Veritas NetBackup™ Appliance セキュリティガイド

リリース 3.1.1

VERITAS™

Veritas NetBackup Appliance セキュリティガイド

法的通知と登録商標

Veritas、Veritas ロゴ、NetBackup は Veritas Technologies LLC または同社の米国とその他の国における関連会社の商標または登録商標です。その他の会社名、製品名は各社の登録商標または商標です。

この製品には、サードパーティの所有物であることを示す必要があるサードパーティソフトウェア(「サードパーティプログラム」)が含まれている場合があります。一部のサードパーティプログラムは、オープンソースまたはフリーソフトウェアライセンスに基づいて提供されています。本ソフトウェアに含まれる本使用許諾契約は、オープンソースまたはフリーソフトウェアライセンスでお客様が有する権利または義務を変更しないものとします。このベリタス製品に付属するサードパーティの法的通知文書は次の場所で入手できます。

https://www.veritas.com/about/legal/license-agreements

本書に記載する製品は、使用、コピー、頒布、逆コンパイルおよびリバースエンジニアリングを制限するライセンスに基づいて頒布されています。Veritas Technologies LLC からの書面による許可なく本書を複製することはできません。

本書は、現状のままで提供され、その商品性、特定目的への適合性、または不侵害の暗黙的な保証を含む、明示的あるいは暗黙的な条件、表明、および保証はすべて免責されるものとします。ただし、これらの免責が法的に無効であるとされる場合を除きます。Veritas Technologies LLC は、本書の提供、内容の実施、また本書の利用によって偶発的あるいは必然的に生じる損害については責任を負わないものとします。本書に記載の情報は、予告なく変更される場合があります。

ライセンス対象ソフトウェアおよび資料は、FAR 12.212 の規定によって商業用コンピュータソフトウェアとみなされ、場合に応じて、FAR 52.227-19「Commercial Computer Software - Restricted Rights」、DFARS 227.7202 以下の「Commercial Computer Software and Commercial Computer Software Documentation」、その後継規制の規定により制限された権利の対象となり、Veritas による納品が内部設置型またはホスト型のサービスのいずれであるかは問いません。米国政府によるライセンス対象ソフトウェアおよび資料の使用、修正、複製のリリース、実演、表示または開示は、本使用許諾契約の条項に従ってのみ行われるものとします。

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

http://www.veritas.com

テクニカルサポート

テクニカルサポートは世界中にサポートセンターを設けています。すべてのサポートサービスは、お客様のサポート契約およびその時点でのエンタープライズテクニカルサポートポリシーに従って提供されます。サポートサービスとテクニカルサポートへの問い合わせ方法については、次の弊社の Web サイトにアクセスしてください。

https://www.veritas.com/support/ja_JP.html

次の URL でベリタスアカウントの情報を管理できます。

https://my.veritas.com

既存のサポート契約に関する質問については、次に示す地域のサポート契約管理チームに電子メールでお問い合わせてください。

世界共通（日本を除く）	CustomerCare@veritas.com
日本	CustomerCare_Japan@veritas.com

マニュアル

最新のマニュアルは、次のベリタス Web サイトで入手できます。

https://sort.veritas.com/documents

マニュアルに対するご意見

お客様のご意見は弊社の財産です。改善点のご指摘やマニュアルの誤謬脱漏などの報告をお願いします。その際には、マニュアルのタイトル、バージョン、章タイトル、セクションタイトルも合わせてご報告ください。ご意見は次のアドレスに送信してください。

APPL.docs@veritas.com

次のベリタスコミュニティサイトでマニュアルの情報を参照したり、質問することもできます。

http://www.veritas.com/community/ja

ベリタスの Service and Operations Readiness Tools (SORT) の表示

ベリタスの Service and Operations Readiness Tools (SORT) は、時間がかかる管理タスクを自動化および簡素化するための情報とツールを提供する Web サイトです。製品によって異なりますが、SORT はインストールとアップグレードの準備、データセンターにおけるリスクの識別、および運用効率の向上を支援します。SORT がお客様の製品に提供できるサービスとツールについては、次のデータシートを参照してください。

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

目次

1

NetBackup appliance セキュリティガイドについて

この章では以下の項目について説明しています。

NetBackup appliance セキュリティガイドについて

NetBackup アプライアンスは、当初からセキュリティを第一に開発されています。Linux オペレーティングシステムや中核的な NetBackup アプリケーションなどのアプライアンスの各要素は、業界標準製品および高度なセキュリティ製品の両方を使って脆弱性がテストされています。これらの評価基準により、不正にアクセスされて、結果として起きるデータの紛失や盗難を最小限にすることができます。

NetBackup アプライアンスのソフトウェアとハードウェアの新しい各バージョンは、リリース前に脆弱性について検証されています。見つかった問題の重大度に応じて、ベリタスは定期的な主要リリースでパッチをリリースするか、修正プログラムを提供します。不明な脅威のリスクを軽減するために、シマンテック社は、定期メンテナンスリリースサイクルの一部となる製品のサードパーティパッケージとモジュールを定期的に更新しています。

このガイドの目的は、NetBackup appliance 3.1.1 リリースに実装されているセキュリティ機能について説明することです。以下の章とサブセクションが含まれます。

NetBackup Appliance ユーザー認証

この章では、NetBackup Appliance の認証機能について説明します。以下のセクションが含まれます。

表 1-1 認証に関するセクション

セクション名	説明	リンク
NetBackup Appliance のユーザー認証について	このセクションでは、アプライアンスにアクセスできるユーザー、ユーザーアカウント、プロセスの種類について説明します。	p.14 の「NetBackup アプライアンスのユーザー認証について」を参照してください。
ユーザー認証の設定について	このセクションでは、アプライアンスで認証できる各種のユーザー用の設定オプションについて説明します。	p.18 の「ユーザー認証の設定について」を参照してください。
LDAP ユーザーの認証について	このセクションでは、LDAP ユーザーを登録、認証するようにアプライアンスを設定するための前提条件とプロセスについて説明します。	p.22 の「LDAP ユーザーの認証について」を参照してください。
Active Directory ユーザーの認証について	このセクションでは、Active Directory（AD）ユーザーを登録、認証するようにアプライアンスを設定するための前提条件とプロセスについて説明します。	p.23 の「Active Directory ユーザーの認証について」を参照してください。
Kerberos-NIS ユーザーの認証について	このセクションでは、Kerberos-NIS ユーザーを登録、認証するようにアプライアンスを設定するための前提条件とプロセスについて説明します。	p.25 の「Kerberos-NIS ユーザーの認証について」を参照してください。
アプライアンスのログインバナーについて	このセクションでは、ユーザーがアプライアンスで認証を試行したときに表示されるテキストバナーを設定できる、ログインバナー機能について説明します。	p.26 の「アプライアンスのログインバナーについて」を参照してください。
ユーザー名とパスワードの仕様について	このセクションでは、ユーザー名とパスワードのクレデンシャルについて説明します。	p.27 の「ユーザー名とパスワードの仕様について」を参照してください。

NetBackup Appliance ユーザーの権限の確認

この章では、NetBackup appliance にアクセスするユーザーを認可するために実装する機能について説明します。以下のセクションが含まれます。

表 1-2 認可のセクション

セクション名	説明	リンク
NetBackup Appliance でのユーザーの権限の確認について	このセクションでは、NetBackup appliance の認可のプロセスの主な特性について説明します。	p.32 の「NetBackup appliance におけるユーザー認可について」を参照してください。

セクション名	説明	リンク
NetBackup Appliance ユーザーの権限の確認について	このセクションでは、アプライアンスユーザーの各種アクセス権限を確認するための管理オプションについて説明します。	p.34 の「NetBackup アプライアンスユーザーの権限の確認について」を参照してください。
管理者ユーザーのロールについて	このセクションでは、管理者のユーザーロールについて説明します。	p.37 の「管理者ユーザーのロールについて」を参照してください。
NetBackupCLI ユーザーロールについて	このセクションでは、NetBackupCLI のユーザーロールについて説明します。	p.38 の「NetBackupCLI ユーザーロールについて」を参照してください。

NetBackup Appliance の侵入防止、侵入検知システム

この章では、以下のセクションで、NetBackup appliance の SDCS（Symantec Data Center Security: Server Advanced）の実装について説明します。

表 1-3 IPS と IDS ポリシーのセクション

セクション名	説明	リンク
NetBackup アプライアンスの Symantec Data Center Security について	このセクションでは、アプライアンスで実装する SDCS 機能を紹介します。	p.42 の「NetBackup appliance の Symantec Data Center Security について」を参照してください。
NetBackup アプライアンスの侵入防止システムについて	このセクションでは、アプライアンスの保護に使う IPS ポリシーについて説明します。	p.44 の「NetBackup appliance の侵入防止システムについて」を参照してください。
NetBackup アプライアンスの侵入検知システムについて	このセクションでは、アプライアンスの監視に使う IDS ポリシーについて説明します。	p.45 の「NetBackup appliance の侵入検知システムについて」を参照してください。
NetBackup アプライアンスの SDCS イベントの見直し	このセクションでは、セキュリティレベルに基づいた SDCS イベントについて説明します。	p.46 の「NetBackup アプライアンスの SDCS イベントの見直し」を参照してください。
NetBackup アプライアンスでのアンマネージモードでの SDCS の実行	このセクションでは、アプライアンスでのデフォルトのセキュリティ管理について簡単に説明します。	p.48 の「NetBackup アプライアンスでのアンマネージモードでの SDCS の実行」を参照してください。

セクション名	説明	リンク
NetBackup アプライアンスでのマネージモードでの SDCS の実行	このセクションでは、集中管理される SDCS 環境の一部としてアプライアンスのセキュリティを管理する方法について説明します。	p.49 の「NetBackup アプライアンスでのマネージモードでの SDCS の実行」を参照してください。
NetBackup アプライアンスの侵入防止システムポリシーの上書き	このセクションでは、アプライアンスに適用する IPS ポリシーを上書きする手順について説明します。	p.50 の「NetBackup appliance の侵入防止システムポリシーの上書き」を参照してください。
NetBackup アプライアンスの侵入防止システムポリシーを再度有効にする	このセクションでは、アプライアンスに適用する IPS ポリシーを再度有効にする手順について説明します。	p.53 の「NetBackup appliance の侵入防止システムポリシーの再有効化」を参照してください。

NetBackup Appliance のログファイル

この章では、以下のセクションで、NetBackup appliance のログファイルとログファイルを表示するためのオプションを一覧表示します。

表 1-4　ログセクションの使用

セクション名	説明	リンク
ログファイルの使用について	この章では、NetBackup appliance に関して表示できる異なる種類のログすべての概要を提供します。	p.56 の「NetBackup appliance のログファイルについて」を参照してください。
Support コマンドの使用によるログファイルの表示	この章では、サポートコマンドを使ってログファイルを表示するための手順について説明します。	p.58 の「Support コマンドの使用によるログファイルの表示」を参照してください。
Browse コマンドを使った NetBackup Appliance のログファイルの検索	この章では、ログファイルを表示するための Browse コマンドの使い方について説明します。	p.60 の「Browse コマンドを使用した NetBackup appliance ログファイルの参照場所」を参照してください。
DataCollect コマンドを使ったデバイスログの収集	この章では、デバイスログを収集するための手順について説明します。	p.61 の「DataCollect コマンドを使ったデバイスログの収集」を参照してください。

NetBackup Appliance オペレーティングシステムのセキュリティ

表 1-5 オペレーティングシステムセクション

セクション名	説明	リンク
NetBackup アプライアンスのオペレーティングシステムのセキュリティについて	このセクションでは、全体的な NetBackup appliance のセキュリティを改善するためにオペレーティングシステムに加える、異なる更新の種類について説明します。	p.65 の「NetBackup アプライアンスのオペレーティングシステムのセキュリティについて」を参照してください。
NetBackup アプライアンスの OS の主要コンポーネント	このセクションでは、NetBackup appliance を搭載する製品とオペレーティングシステムコンポーネントを一覧表示します。	p.67 の「NetBackup appliance の OS の主要コンポーネント」を参照してください。
NetBackup アプライアンスの脆弱性スキャン	このセクションでは、ベリタスがアプライアンスのセキュリティを確認するために使用するセキュリティスキャナの一部を一覧表示します。	p.67 の「NetBackup appliance の脆弱性スキャン」を参照してください。

NetBackup Appliance のデータセキュリティ

この章では、以下のセクションで、NetBackup appliance のデータセキュリティ実装について説明します。

表 1-6 データセキュリティセクション

セクション名	説明	リンク
データセキュリティについて	このセクションでは、データセキュリティの改善のために取られる対策をリストします。	p.68 の「データセキュリティについて」を参照してください。
データ整合性について	このセクションでは、データ整合性の改善のために取られる対策をリストします。	p.69 の「データ整合性について」を参照してください。
データの分類について	このセクションでは、データ分類の改善のために取られる対策をリストします。	p.70 の「データの分類について」を参照してください。
データの暗号化について	このセクションでは、データの暗号化の改善のために取られる対策をリストします。	p.70 の「データの暗号化について」を参照してください。

NetBackup Appliance の Web セキュリティ

この章では、以下のセクションで、NetBackup appliance の Web セキュリティ実装について説明します。

表 1-7 Web セキュリティセクション

セクション名	説明	リンク
SSL 証明書について	このセクションでは、NetBackup Appliance Web Consoleの SSL 証明書の更新を一覧表示します。	p.73 の「SSL の使用について」を参照してください。
サードパーティの SSL 証明書のインストール	このセクションでは、サードパーティの SSL 証明書をインストールするための手順を一覧表示します。	p.74 の「サードパーティの SSL 証明書の実装」を参照してください。

NetBackup Appliance のネットワークセキュリティ

この章では、以下のセクションで、NetBackup appliance のネットワークセキュリティ実装について説明します。

表 1-8 ネットワークセキュリティセクション

セクション名	説明	リンク
IPsec チャネル設定について	このセクションでは、NetBackup Appliance の IPsec 設定について説明します。	p.79 の「IPsec チャネル設定について」を参照してください。
NetBackup appliance ポートについて	このセクションでは、NetBackup Appliance のポート情報について説明します。	p.81 の「NetBackup appliance ポートについて」を参照してください。

NetBackup Appliance のコールホームセキュリティ

この章では、以下のセクションで、NetBackup appliance のコールホームセキュリティ実装について説明します。

表 1-9 コールホームセキュリティセクション

セクション名	説明	リンク
AutoSupport について	このセクションでは、NetBackup appliance の AutoSupport 機能について説明します。	p.84 の「AutoSupport について 」を参照してください。

セクション名	説明	リンク
コールホームについて	このセクションでは、NetBackup appliance のコールホーム機能について説明します。	p.85 の「コールホームについて」を参照してください。
SNMP について	このセクションでは、NetBackup appliance の SNMP 機能について説明します。	p.90 の「SNMP について」を参照してください。

NetBackup Appliance の IPMI セキュリティ

この章の以下のセクションでは、IPMI 設定を保護するために採用するガイドラインについて説明します。

表 1-10 IPMI セキュリティセクション

セクション名	説明	リンク
IPMI 設定の紹介	このセクションでは、IPMI と IPMI がNetBackup applianceで設定される方法について説明します。	p.91 の「IPMI 設定の紹介」を参照してください。
推奨 IPMI 設定の一覧表示	このセクションでは、安全な設定のための推奨 IPMI 設定を一覧表示します。	p.91 の「推奨される IPMI 設定」を参照してください。

対象読者

このガイドは、NetBackup appliance の保守管理業務に従事しているセキュリティ管理者、バックアップ管理者、システム管理者、IT 技術者を含むユーザーを対象としています。

メモ: 本書のタスクや手順は構成済みのアプライアンスで実行する必要があります。アプライアンスの役割を構成する前にローカルユーザーコマンドを問題なく使うことはできません。アプライアンスの役割が構成されていない場合、ユーザー権限の付与などを含むすべてのローカルユーザーコマンドが失敗します。役割を構成する前にローカルユーザーコマンドを実行すると、役割を構成した後に同じコマンドを実行しても失敗します。その他のコマンドは、予期しない動作または望ましくない動作につながることがあります。この状況を防止するには、アプライアンスの構成が完了するまでローカルユーザーコマンドを使わないことがベストプラクティスです。

2

ユーザー認証

この章では以下の項目について説明しています。

NetBackup アプライアンスのユーザー認証について

NetBackup appliance は、ユーザーアカウントを使用して管理します。ローカルユーザーアカウントを作成したり、リモートディレクトリサービスに属するユーザーとユーザーグループを登録したりすることができます。各ユーザーアカウントがアプライアンスにアクセスするには、ユーザー名とパスワードで自己認証する必要があります。ローカルユーザーの場合には、ユーザー名とパスワードはアプライアンス上で管理されます。登録済みのリモートユーザーの場合には、ユーザー名とパスワードはリモートディレクトリサービスによって管理されます。

新しいユーザーアカウントがアプライアンスにログオンしてアクセスするには、最初にそのアカウントとロールを承認する必要があります。デフォルトでは、新しいユーザーアカウントには割り当てられたロールがないので、ロールが認可されるまでログオンできません。

表 2-1 では、アプライアンスで利用可能なユーザーアカウントについて説明します。

表 2-1 NetBackup appliance のアカウントの種類

アカウント名	説明
admin	admin アカウントは NetBackup appliance のデフォルトの管理者ユーザーです。このアカウントは、デフォルトの管理者ユーザーにアプライアンスに対する完全なアクセスと制御を提供します。 NetBackup の新しいアプライアンスには、次のデフォルトのログオンのクレデンシャルが付属しています。 ■ ユーザー名: admin ■ パスワード: P@ssw0rd アプライアンスから共有をマウントまたはマップする場合は、次の内容を記録してください。 ■ Windows: 管理者アカウントと管理者ロールが割り当てられた AD ユーザーは、Windows CIFS 共有のマウントまたはマッピングの権限が付与されています。 ■ Linux: ルートアクセスアカウントを持つユーザーのみが NFS 共有を直接マウントする mount コマンドを実行できます。
AMSadmin	AMSadmin アカウントを使用すると、次のアプライアンスインターフェースにフルアクセスできます。 ■ アプライアンス管理コンソール ■ NetBackup Appliance Web Console ■ NetBackup Appliance Shell Menu ■ NetBackup 管理コンソール このアカウントについて詳しくは、『Veritas Appliance 管理ガイド』を参照してください。
メンテナンス	メンテナンスアカウントは、NetBackup Appliance Shell MenuでVeritasサポートが使用します (管理者用ログオン後)。このアカウントは、メンテナンス活動またはアプライアンスのトラブルシューティング専用として使用します。 **メモ:** このアカウントは、GRUB の変更や、STIG オプションが有効な場合のシングルユーザーモードのブートにも使用します。

内部ユーザーにのみ利用できるアカウントを次に示します。これらのアカウントでは、NetBackup Appliance Web ConsoleまたはNetBackup Appliance Shell Menuを使用してシステムにアクセスすることはできません。

表 2-2 NetBackup appliance の内部アカウントの種類

アカウント名	説明
sisips	`sisips` アカウントは、SDCS ポリシーを実装するための内部ユーザーです。

アカウント名	説明
root	root アカウントは、保守タスクを実行するためにシマンテック社のサポートのみがアクセスする制限されたユーザーです。このアカウントにアクセスしようとすると、次のメッセージが表示されます。 Permission Denied !! Access to the root account requires overriding the Intrusion Security Policy. Please refer to the appliance security guide for overriding instructions. **警告:** 侵入セキュリティポリシー (ISP) を上書きして root アカウントにアクセスできますが、お勧めしません。このポリシーを上書きすると、システムがリスクにさらされ、攻撃に対して脆弱になります。p.50 の「NetBackup appliance の侵入防止システムポリシーの上書き」を参照してください。
nbcopilotxxxx	マスターサーバーからメディアサーバーへのアクセスの認証をサポートします。
AppComm	認証はサポートされません。
nbwebsvc	認証はサポートされません。

p.34 の「NetBackup アプライアンスユーザーの権限の確認について」を参照してください。

NetBackup アプライアンスで認証できるユーザーの種類

アプライアンスのローカルユーザーを直接追加したり、LDAP サーバー、AD（Active Directory）サーバー、または NIS サーバーのユーザーを登録したりできます。リモートユーザーを登録すると、既存のディレクトリサービスを利用してユーザー管理と認証を行うことができるので便利です。表 2-3 は、NetBackup アプライアンスに追加できるユーザーの種類を示します。

メモ: アプライアンスの役割を構成する前にローカルユーザーコマンドを問題なく使うことはできません。アプライアンスの役割が構成されていない場合、ユーザー権限の付与などを含むすべてのローカルユーザーコマンドが失敗します。役割を構成する前にローカルユーザーコマンドを実行すると、役割を構成した後に同じコマンドを実行しても失敗します。一部のコマンドは、予期しない動作または望ましくない動作につながることがあります。この状況を防止するには、アプライアンスの構成が完了するまでローカルユーザーコマンドを使わないことがベストプラクティスです。

表 2-3 NetBackup アプライアンスのユーザーの種類

ユーザーの種類	説明	注意
ローカル（ネーティブユーザー）	ローカルユーザーは、アプライアンスのデータベースに追加され、LDAP サーバーのような外部ディレクトリベースのサーバーに対して参照されることはありません。ユーザーを追加したら、適切なアプライアンスのアクセス権を認可したり取り消せます。	■ NetBackup Appliance Web Consoleから[設定（Settings）] > [認証（Authentication）] > [ユーザー管理（User Management）]の順に開いたページを使ってローカルユーザーを追加、削除、管理できます。 ■ NetBackup Appliance Shell Menuの `Settings > Security > Authentication > LocalUser` コマンドを使用して、ローカルユーザーを追加や削除したり、そのパスワードを変更したりできます。 ■ ローカルユーザーグループは追加できません。 ■ ローカルユーザーは、管理者または NetBackupCLI のロールを持つことができます。 **メモ:** 既存のローカルユーザーに NetBackupCLI ロールを付与することはできません。ただし、ローカル NetBackupCLI ユーザーを作成できます。その場合、`Manage > NetBackupCLI > Create` コマンドを NetBackup Appliance Shell Menuから実行します。
LDAP	LDAP（Lightweight Directory Access Protocol）ユーザーまたはユーザーグループが、外部 LDAP サーバー上に存在します。LDAP サーバーと通信するようにアプライアンスを構成すると、これらのユーザーとユーザーグループをアプライアンスに登録できます。ユーザーを登録（追加）したら、適切なアプライアンスのアクセス権限を認可または取り消しができます。 p.22 の「LDAP ユーザーの認証について」を参照してください。	■ NetBackup Appliance Web Consoleの［設定（Settings）］> ［認証（Authentication）］> ［ユーザー管理（User Management）］の順に開いたページを使って LDAP ユーザーとユーザーグループを追加、削除、管理できます。 ■ NetBackup Appliance Shell Menuの `Settings > Security > Authorization > LDAP` コマンドを使って、LDAP ユーザーとユーザーグループを追加と削除できます。 ■ 管理者または NetBackupCLI ロールを LDAP ユーザーまたはユーザーグループに割り当てることができます。 **メモ:** NetBackupCLI ロールはいつでも最大 9 ユーザーグループに割り当てることができます。

ユーザーの種類	説明	注意
Active Directory	AD（Active Directory）ユーザーまたはユーザーグループは、外部 AD サーバー上に存在します。AD サーバーと通信するようにアプライアンスを構成すると、これらのユーザーとユーザーグループをアプライアンスに登録できます。ユーザーを登録（追加）したら、適切なアプライアンスのアクセス権限を認可または取り消しができます。 p.23 の「Active Directory ユーザーの認証について」を参照してください。	■ NetBackup Appliance Web Consoleの［設定 (Settings)］>［認証 (Authentication)］>［ユーザー管理 (User Management)］ページを使用して、AD ユーザーおよびユーザーグループを追加、削除、管理できます。 ■ NetBackup Appliance Shell Menuの `Settings > Security > Authorization > ActiveDirectory` コマンドを使って、AD ユーザーとユーザーグループを追加および削除できます。 ■ 管理者または NetBackupCLI ロールを AD ユーザーまたはユーザーグループに割り当てることができます。 **メモ:** NetBackupCLI ロールはいつでも最大 9 ユーザーグループに割り当てることができます。
Kerberos-NIS	NIS（ネットワーク情報サービス）ユーザーまたはユーザーグループは、外部 NIS サーバー上に存在します。LDAP や AD の実装とは違って、NIS ドメインと通信するようにアプライアンスを構成する場合は Kerberos 認証が必要です。NIS ユーザーが登録されるようにアプライアンスを構成するには、既存の Kerberos サービスを NIS サーバーに関連付ける必要があります。 NIS サーバーや Kerberos サーバーと通信するようにアプライアンスを構成すると、NIS ユーザーとユーザーグループをアプライアンスに登録できます。ユーザーをアプライアンスに登録（追加）したら、適切なアプライアンスのアクセス権を認可または取り消しができます。 p.25 の「Kerberos-NIS ユーザーの認証について」を参照してください。	■ NetBackup Appliance Web Consoleの［設定 (Settings)］>［認証 (Authentication)］>［ユーザー管理 (User Management)］ページを使用して、NIS ユーザーおよびユーザーグループを追加、削除、管理できます。 ■ NetBackup Appliance Shell Menuの `Settings > Security > Authentication > Kerberos` コマンドを使って、NIS ユーザーとユーザーグループの追加と削除ができます。 ■ 管理者または NetBackupCLI ロールを NIS ユーザーまたはユーザーグループに割り当てることができます。 **メモ:** NetBackupCLI ロールはいつでも最大 9 ユーザーグループに割り当てることができます。

新しいユーザーの構成について詳しくは、『NetBackup Appliance 管理者ガイド』を参照してください。

ユーザー認証の設定について

表 2-4 では、NetBackup Appliance Web Consoleと NetBackup Appliance Shell Menu の機能を利用してアプライアンスを設定し、さまざまな種類のユーザーを認証し、アクセス権限を与える方法について説明します。

表 2-4 ユーザー認証管理

ユーザーの種類	NetBackup Appliance Web Console	NetBackup Appliance Shell Menu
ローカル（ネイティブユーザー）	NetBackup Appliance Web Consoleの［設定（Settings）］>［認証（Authentication）］>［ユーザー管理（User Management）］タブを利用し、ローカルユーザーを追加します。 p.34 の「NetBackup アプライアンスユーザーの権限の確認について」を参照してください。	次のコマンドとオプションは `Settings > Security > Authentication > LocalUser` で利用できます。 ■ `Clean` - すべてのローカルユーザーを削除します。 ■ `List` - アプライアンスに追加されているすべてのローカルユーザーを一覧表示します。 ■ `Password` - ローカルユーザーのパスワードを変更します。 ■ `Users` - 1 人以上のローカルユーザーを追加または削除します。

ユーザーの種類	NetBackup Appliance Web Console	NetBackup Appliance Shell Menu
LDAP	［設定 (Settings)］> ［ユーザー ()］> ［認証 (Authentication)］> ［LDAP］で、次の LDAP 設定タスクを実行できます。 ■ 新しい LDAP 設定を追加します。 ■ XML ファイルから保存済みの LDAP 構成をインポートします。 ■ LDAP サーバーの構成パラメータを追加、編集、削除します。 ■ LDAP サーバーの SSL 証明書を識別し、接続します。 ■ LDAP サーバーの属性マップを追加、編集、削除します。 ■ 既存の LDAP 構成（ユーザーを含む）を XML ファイルとしてエクスポートします。このファイルをインポートし、他のアプライアンスで LDAP を構成できます。 ■ LDAP 構成を無効にして再度有効にします。 ■ LDAP サーバーの構成を解除します。 NetBackup Appliance Web Consoleの［設定 (Settings)］> ［認証 (Authentication)］> ［ユーザー管理 (User Management)］タブを利用し、LDAP ユーザーとユーザーグループを追加します。 p.34 の「NetBackup アプライアンスユーザーの権限の確認について」を参照してください。	次のコマンドとオプションは `Settings > Security > Authentication > LDAP` で利用できます。 ■ `Attribute` - LDAP 構成属性を追加または削除します。 ■ `Certificate` - SSL 証明書を設定、表示、無効化します。 ■ `ConfigParam` - LDAP 構成パラメータを設定、表示、無効化します。 ■ `Configure` - アプライアンスに登録し、認証されることを LDAP ユーザーに許可するようにアプライアンスを設定します。* ■ `Disable` - アプライアンスの LDAP ユーザー認証を無効にします。 ■ `Enable` - アプライアンスの LDAP ユーザー認証を有効にします。 ■ `Export` - 既存の LDAP 構成を XML ファイルとしてエクスポートします。 ■ `Groups` - 1 つ以上の LDAP ユーザーグループを追加または削除します。LDAP サーバーにすでに存在するユーザーグループのみをアプライアンスに追加できます。 ■ `Import` - XML ファイルから LDAP 構成をインポートします。 ■ `List` - アプライアンスに追加されているすべての LDAP ユーザーとユーザーグループを一覧表示します。 ■ `Map` - NSS マップの属性またはオブジェクトクラスを設定、削除、表示します。 ■ `Show` - LDAP 構成の詳細を表示します。 ■ `Status` - アプライアンスの LDAP 認証の状態を表示します。 ■ `Unconfigure` - LDAP 構成を削除します。 ■ `Users` - 1 人以上の LDAP ユーザーを追加または削除します。LDAP サーバーにすでに存在するユーザーグループのみをアプライアンスに追加できます。

ユーザーの種類	NetBackup Appliance Web Console	NetBackup Appliance Shell Menu
Active Directory	[設定 (Settings)] > [ユーザー ()] > [認証 (Authentication)] > [Active Directory]で、次の AD 設定タスクを実行できます。 ■ 新しい Active Directory 設定を行います。 ■ 既存の Active Directory 構成を構成解除します。 NetBackup Appliance Web Consoleの[設定 (Settings)] > [認証 (Authentication)] > [ユーザー管理 (User Management)]タブを利用し、Active Directory ユーザーとユーザーグループを追加します。 p.34 の「NetBackup アプライアンスユーザーの権限の確認について」を参照してください。	次のコマンドとオプションは Settings > Security > Authentication > ActiveDirectory で利用できます。 ■ Configure - アプライアンスに登録し、認証されることを AD ユーザーに許可するようにアプライアンスを設定します。* ■ Groups - 1 つ以上の AD ユーザーグループを追加または削除します。AD サーバーにすでに存在するユーザーグループのみをアプライアンスに追加できます。 ■ List - アプライアンスに追加されているすべての AD ユーザーとユーザーグループを一覧表示します。 ■ Status - アプライアンスの AD 認証の状態を表示します。 ■ Unconfigure - AD 構成を削除します。 ■ Users - 1 人以上の AD ユーザーを追加または削除します。AD サーバーにすでに存在するユーザーのみをアプライアンスに追加できます。
Kerberos-NIS	[設定 (Settings)] > [ユーザー ()] > [認証 (Authentication)] > [Kerberos-NIS]で、次の Kerberos-NIS 設定タスクを実行できます。 ■ 新しい Kerberos-NIS 設定を行います。 ■ 既存の Kerberos-NIS 構成を構成解除します。 NetBackup Appliance Web Consoleの[設定 (Settings)] > [認証 (Authentication)] > [ユーザー管理 (User Management)]タブを利用し、Kerberos-NIS ユーザーとユーザーグループを追加します。 p.34 の「NetBackup アプライアンスユーザーの権限の確認について」を参照してください。	次のコマンドとオプションは Settings > Security > Authentication > Kerberos で利用できます。 ■ Configure - アプライアンスに登録し、認証されることを NIS ユーザーに許可するようにアプライアンスを設定します。* ■ Groups - 1 つ以上の NIS ユーザーグループを追加または削除します。NIS サーバーにすでに存在するユーザーグループのみをアプライアンスに追加できます。 ■ List - アプライアンスに追加されているすべての NIS ユーザーとユーザーグループを一覧表示します。 ■ Status - アプライアンスの NIS と Kerberos の認証の状態を表示します。 ■ Unconfigure - NIS と Kerberos の構成を削除します。 ■ Users - 1 人以上の NIS ユーザーを追加または削除します。NIS サーバーにすでに存在するユーザーのみをアプライアンスに追加できます。

一般的なユーザー認証ガイドライン

アプライアンスでユーザーを認証する場合は次のガイドラインを使ってください。

- アプライアンス上の認証には 1 種類のリモートユーザータイプ (LDAP、Active Directory (AD)、または NIS) のみを設定できます。たとえば、アプライアンスの LDAP ユーザーを認証する場合、AD ユーザー認証に変更する前にアプライアンスの LDAP 構成を削除する必要があります。
- NetBackupCLI ロールはいつでも最大 9 ユーザーグループに割り当てることができます。
- 既存のローカルユーザーに NetBackupCLI ロールを付与することはできません。ただし、ローカル NetBackupCLI ユーザーを作成できます。その場合、`Manage > NetBackupCLI > Create` コマンドを NetBackup Appliance Shell Menuから実行します。
- 既存のアプライアンスユーザーとユーザー名、ユーザー ID、またはグループ ID が同じ場合、新しいユーザーまたはユーザーグループはそのアプライアンスに追加できません。
- アプライアンスローカルユーザーまたは NetBackupCLI ユーザーですでに使用されているユーザーグループ名またはユーザー名は使用しないでください。また、LDAP、AD、または NIS ユーザーに admin または maintenance といったアプライアンスのデフォルト名を使用しないでください。
- アプライアンスは、LDAP または NIS 構成の ID マッピングを処理しません。アプライアンスユーザーの場合に限り、1000～1999 のユーザー ID とグループ ID の範囲を予約することをお勧めします。

p.14 の「NetBackup アプライアンスのユーザー認証について」を参照してください。

p.34 の「NetBackup アプライアンスユーザーの権限の確認について」を参照してください。

LDAP ユーザーの認証について

NetBackup appliance は組み込みのプラグ可能な認証モジュール (PAM) プラグインを使って LDAP (Lightweight Directory Access Protocol) ユーザーの認証をサポートします。この機能により、LDAP ディレクトリサービスに属しているユーザーを NetBackup appliance にログオンできるように追加して認証できます。LDAP は、UNIX サービスによってインストールされるスキーマを持つ別の種類のユーザーディレクトリとして認識されます。

LDAP ユーザー認証を使うための前提条件

アプライアンスで LDAP ユーザー認証を使用するための前提条件と必要条件を以下に示します。

- LDAP ユーザー認証を設定するには NetBackup appliance 2.6 以降をインストールする必要があります。
- LDAP スキーマは RFC 2307 または RFC 2307bis に準拠する必要があります。
- 次のファイアウォールポートを開く必要があります。
  - LDAP 389
  - LDAP OVER SSL/TLS 636
  - HTTPS 443
- LDAP サーバーが利用できること、またそれがアプライアンスに登録するユーザーとユーザーグループで設定されていることを確認します。

  メモ: ベストプラクティスとして、アプライアンスのローカルユーザーまたは NetBackupCLI ユーザーにすでに使われているグループ名またはユーザー名は使わないでください。また、LDAP ユーザーのアプライアンスのデフォルト名 admin または maintenance を使わないでください。

- アプライアンスは、LDAP 構成の ID マッピングを処理しません。アプライアンスユーザーの場合に限り、1000～1999 のユーザー ID とグループ ID の範囲を予約することをお勧めします。

LDAP ユーザー認証の構成方法

新しい LDAP ユーザーとユーザーグループをアプライアンスに登録する前に、LDAP サーバーと通信するようにアプライアンスを構成する必要があります。構成が完了すると、アプライアンスは LDAP サーバーの認証用ユーザー情報にアクセスできます。

LDAP ユーザー認証を構成するには、次のオプションのいずれかを使用します。

- NetBackup Appliance Web Consoleの［設定 (Settings)］>［認証 (Authentication)］>［LDAP］。
- NetBackup Appliance Shell Menuの `Settings > Security > Authentication > LDAP` コマンド

LDAP ユーザー認証をアプライアンス上で構成および管理するための詳細な手順については、『NetBackup Appliance 管理者ガイド』と『NetBackup Appliance コマンドリファレンスガイド』を参照してください。

Active Directory ユーザーの認証について

NetBackup Appliance は組み込みのプラグ可能な認証モジュール (PAM) プラグインを使って、Active Directory (AD) ユーザーの認証をサポートします。この機能により、AD サービスに属しているユーザーを NetBackup appliance にログオンできるように追加し

て認証できます。AD は、UNIX サービスによってインストールされるスキーマを持つ別の種類のユーザーディレクトリとして認識されます。

Active Directory ユーザー認証を使うための前提条件

アプライアンスで AD ユーザー認証を使用するための前提条件と必要条件を以下に示します。

- AD ユーザー認証を設定するには NetBackup appliance 2.6.0.3 以降をインストールする必要があります。
- AD サービスが利用できること、またそれがアプライアンスに登録するユーザーとユーザーグループで設定されていることを確認します。

  メモ: ベストプラクティスとして、アプライアンスのローカルユーザーまたは NetBackupCLI ユーザーにすでに使われているグループ名またはユーザー名は使わないでください。また、admin または maintenance といったアプライアンスデフォルト名を AD ユーザーに使用しないでください。

- 認可されているドメインユーザーの資格情報を利用してアプライアンスで AD サーバーが構成されていることを確認します。
- AD DNS サーバーに DNS 要求を転送できる DNS サーバーを使ってアプライアンスを構成します。または、AD DNS サーバーをネームサービスデータソースとして使うようにアプライアンスを構成します。

Active Directory ユーザー認証の構成方法

新しい AD ユーザーとユーザーグループをアプライアンスに登録する前に、AD サーバーと通信するようにアプライアンスを構成する必要があります。構成が完了すると、アプライアンスは AD サーバーの認証用ユーザー情報にアクセスできます。

次の方法のいずれかを使用して AD 認証を構成します。

- NetBackup Appliance Web Consoleの［設定 (Settings)］>［認証 (Authentication)］>［Active Directory］ページ。
- NetBackup Appliance Shell Menuの `Settings > Security > Authentication > ActiveDirectory` コマンド。

AD ユーザー認証をアプライアンス上で構成および管理するための詳細な手順については、『NetBackup Appliance 管理者ガイド』と『NetBackup Appliance コマンドリファレンスガイド』を参照してください。

Kerberos-NIS ユーザーの認証について

NetBackup appliance は組み込みのプラグ可能な認証モジュール (PAM) プラグインを使ってネットワーク情報サービス (NIS) ユーザーの認証をサポートします。この機能により、NIS ディレクトリサービスに属しているユーザーを NetBackup appliance にログオンできるように追加して認証できます。NIS は、UNIX サービスによってインストールされるスキーマを持つ別の種類のユーザーディレクトリとして認識されます。

NIS ユーザーを認証するようにアプライアンスを構成するには、Kerberos 認証が必要です。NIS ユーザーが登録されるようにアプライアンスを設定するには、既存の Kerberos サービスを NIS ドメインに関連付ける必要があります。

NIS ユーザー認証と Kerberos を併用するための前提条件

アプライアンスで NIS ユーザー認証を使うための前提条件と必要条件を以下に示します。

- Kerberos による NIS ユーザー認証を設定するには NetBackup appliance 2.6.1.1 以降をインストールする必要があります。
- NIS ドメインが利用できること、またそれがアプライアンスに登録するユーザーとユーザーグループで設定されていることを確認します。
- アプライアンスは、NIS 構成の ID マッピングを処理しません。アプライアンスユーザーの場合に限り、1000～1999 のユーザー ID とグループ ID の範囲を予約することをお勧めします。

  メモ: ベストプラクティスとして、アプライアンスのローカルユーザーまたは NetBackupCLI ユーザーにすでに使われているグループ名またはユーザー名は使わないでください。また、NIS ユーザーのアプライアンスのデフォルト名 admin または maintenance を使わないでください。

- Kerberos サーバーが利用できること、またそれが NIS ドメインと通信できるように適切に構成されていることを確認します。
- Kerberos には厳しい時間要件があるため、常に NTP サーバーを利用してアプライアンス、NIS サーバー、Kerberos サーバー間の時間を同期します。

Kerberos による NIS ユーザー認証の構成方法

新しい NIS ユーザーとユーザーグループをアプライアンスに登録する前に、NIS サーバーおよび Kerberos サーバーと通信するようにアプライアンスを構成する必要があります。構成が完了すると、アプライアンスは認証のために NIS ドメインユーザー情報にアクセスできます。

Kerberos-NIS 認証を構成するには、次のいずれかの方法を使います。

- NetBackup Appliance Web Consoleの［設定 (Settings)］>［認証 (Authentication)］>［Kerberos-NIS］ページ
- NetBackup Appliance Shell Menuの `Settings > Security > Authentication > Kerberos` コマンド

Kerberos-NIS ユーザー認証をアプライアンス上で構成および管理するための詳細な手順については、『NetBackup Appliance 管理者ガイド』と『NetBackup Appliance コマンドリファレンスガイド』を参照してください。

アプライアンスのログインバナーについて

NetBackup appliance では、ユーザーがアプライアンスにログオンしようとすると表示されるテキストバナーを設定できます。ログインバナーを使うと、さまざまな種類のメッセージをユーザーに伝えることができます。ログインバナーの一般的な用途には、著作権、警告メッセージ、および会社方針情報の表示があります。

また、NetBackup 管理コンソールもログインバナーをサポートしています。デフォルトでは、アプライアンスのログインバナーを設定しても、NetBackup でそのバナーは使いません。ただし、アプライアンスのログインバナーの設定時に、ユーザーが NetBackup 管理コンソールにログインするときに必ずバナーが表示されるように、バナーを NetBackup に伝播できます。

表 2-5 では、ログインバナーをサポートするアプライアンスインターフェースについて説明します。ログインバナーを設定すると、NetBackup Appliance Shell Menuや SSH などのバナーをサポートするアプライアンスの各インターフェースに表示されます。ただし、必要に応じて、NetBackup 管理コンソールのログインバナーのオンとオフを切り替えることができます。

表 2-5　ログインバナーをサポートするアプライアンスインターフェース

インターフェース	注意
NetBackup Appliance Shell Menu	NetBackup Appliance Shell Menuにログインしようとすると、まずログインバナーが表示されます。
IPMI コンソールセッション	ユーザー名を入力すると、パスワードが要求される前に、ログインバナーが IPMI コンソールセッションで表示されます。
NetBackup Appliance Web Console	Web ブラウザからアプライアンスにアクセスすると、ログインバナーが表示されます。このログインバナーは、［同意 (Agree)］ボタンをクリックした場合のみ非表示にできます。

インターフェース	注意
NetBackup 管理コンソール（オプション）	ユーザーが NetBackup 管理コンソールを使ってアプライアンスにログインするときに、必ずログインバナーが表示されます。この機能は、NetBackup の一部である既存のログインバナー機能を使っています。詳しくは、『NetBackup 管理者ガイド』のボリューム I を参照してください。

ログインバナーを構成するには、NetBackup Appliance Shell Menuの[設定 (Settings)] > [通知 (Notifications)] > [ログインバナー (LoginBanner)]を使います。詳しくは、『NetBackup Appliance コマンドリファレンスガイド』を参照してください。

または、[設定 (Settings)] > [通知 (Notifications)] > [ログインバナー (LoginBanner)]の順に選択して NetBackup Appliance Web Consoleでログインバナーを構成します。詳しくは、『NetBackup appliance 管理者ガイド』を参照してください。

ユーザー名とパスワードの仕様について

NetBackup appliance のユーザーアカウントのユーザー名は選択された認証システムが受け入れる形式である必要があります。表 2-6 に、ユーザーの種類ごとのユーザー名指定を示します。

メモ: `Manage > NetBackupCLI > Create` コマンドを使って、NetBackupCLI ロールを持つローカルユーザーを作成します。すべてのローカルユーザーとパスワードの仕様はこれらのユーザーに適用されます。

表 2-6 ユーザー名の仕様

説明	管理者（ローカルユーザー）	NetBackupCLI（ローカルユーザー）	登録済みのリモートユーザー
最大長	適用される制限なし	適用される制限なし	LDAP、AD、NIS ポリシーによって判断
最小長	2 文字	2 文字	LDAP、AD、NIS ポリシーによって判断
制限	ユーザー名の先頭に次のものを指定することはできません。 ■ 番号 ■ 特殊文字	ユーザー名の先頭に次のものを指定することはできません。 ■ 番号 ■ 特殊文字	LDAP、AD、NIS ポリシーによって判断

説明	管理者（ローカルユーザー）	NetBackupCLI（ローカルユーザー）	登録済みのリモートユーザー
スペースの包含	ユーザー名にスペースを含めることはできません。	ユーザー名にスペースを含めることはできません。	LDAP、AD、NIS ポリシーによって判断

パスワードの仕様

NetBackup appliance パスワードポリシーはアプライアンスのセキュリティを高めるために更新されました。アプライアンスのユーザーアカウントのパスワードは選択された認証システムが受け入れる形式である必要があります。表 2-7 は、各ユーザー形式のパスワードの仕様の一覧を表示します。

表 2-7　　パスワードの仕様

説明	管理者（ローカルユーザー）	NetBackupCLI（ローカルユーザー）	登録済みのリモートユーザー
最大長	適用される制限なし	適用される制限なし	LDAP、AD、NIS ポリシーによって判断
最小長	パスワードは少なくとも 8 文字にする必要があります。	パスワードは少なくとも 8 文字にする必要があります。	LDAP、AD、NIS ポリシーによって判断
必要条件	■ 1 つの大文字 ■ 1 つの小文字（a から z） ■ 1 つの数字（0 から 9） ■ 辞書に記載されている単語は弱いパスワードと見なされ、受け入れられません。 ■ 過去 7 回分のパスワードは再利用できません。以前のパスワードに類似する新しいパスワードも使えません。	■ 1 つの大文字 ■ 1 つの小文字（a から z） ■ 1 つの数字（0 から 9） ■ 辞書に記載されている単語は弱いパスワードと見なされ、受け入れられません。 ■ 過去 7 回分のパスワードは再利用できません。以前のパスワードに類似する新しいパスワードも使えません。	LDAP、AD、NIS ポリシーによって判断
スペースの包含	パスワードにスペースを含めることはできません。	パスワードにスペースを含めることはできません。	LDAP、AD、NIS ポリシーによって判断

説明	管理者（ローカルユーザー）	NetBackupCLI（ローカルユーザー）	登録済みのリモートユーザー
パスワードの最短期限	0 日	0 日 **メモ:** NetBackup Appliance Shell Menuの `Manage > NetBackupCLI > PasswordExpiry` コマンドを使って、ユーザーパスワード保存期間を管理できます。 詳しくは、『NetBackup Appliance コマンドリファレンスガイド』を参照してください。	LDAP、AD、NIS ポリシーによって判断
パスワードの最長期限	99999 日（期限切れになりません）	99999 日（期限切れになりません）	LDAP、AD、NIS ポリシーによって判断
パスワード履歴	過去 7 回分のパスワードは再利用できません。以前のパスワードに類似する新しいパスワードも使えません。	過去 7 回分のパスワードは再利用できません。以前のパスワードに類似する新しいパスワードも使えません。	LDAP、AD、NIS ポリシーによって判断
パスワード有効期限	パスワードの期限が切れませんので、適用されません	`Manage > NetBackupCLI > PasswordExpiry` コマンドを使って、NetBackupCLI ユーザーパスワードを管理します。	LDAP、AD、NIS ポリシーによって判断
パスワードロックアウト	なし	なし	LDAP、AD、NIS ポリシーによって判断
ロックアウトの期間	なし	なし	LDAP、AD、NIS ポリシーによって判断

メモ: アプライアンス環境のセキュリティを強化するには、アプライアンスに初回ログイン時にデフォルトの `admin` と `maintenance` のアカウントパスワードを変更することをお勧めします。NetBackup Appliance Web Consoleの［設定（Settings）］>［パスワード（Password）］ページまたは NetBackup Appliance Shell Menuの `Settings > Password` コマンドを使って、パスワードを変更できます。

警告: NetBackup appliance では、passwd などのコマンドを使ったメンテナンスアカウントのパスワードの設定をサポートしていません。この方法で設定されるパスワードは、システムがアップグレードされると、上書きされます。NetBackup Appliance Shell Menuを使ってメンテナンスのアカウントパスワードを変更してください。

パスワード保護

NetBackup appliance では、次のパスワード保護対策を導入しています。

- NetBackup アプライアンスのソフトウェアバージョン 2.6.1.1 以降では、SHA-512 ハッシュアルゴリズムを使用して、お客様がアクセス可能なすべてのローカルアプライアンスのユーザー (ローカルユーザー、NetBackupCLI のユーザー、管理者ユーザー、メンテナンスユーザー) のパスワードを保護します。新しいローカルアプライアンスユーザーを作成する場合、または既存のローカルアプライアンスユーザーのパスワードを変更する場合、必ず SHA-512 を使ってパスワードがハッシュ化されます。

  メモ: 2.6.1.1 より前は、アプライアンスは SHA-512、SHA-256、Blowfish を含む多様なデフォルトのパスワードハッシュアルゴリズムを使用していました。2.6.1.1 以降のバージョンにアップグレードする場合、新しいデフォルトは SHA-512 になりますが、既存のパスワードハッシュも保持されます。以前のアルゴリズムが機能し、その安全が引き続き保障される場合も、すべてのローカルアプライアンスユーザーが新しいデフォルトを使うように、NetBackup アプライアンスソフトウェアのバージョン 2.6.1.1 以降へのアップグレード後に、最終的にすべてのローカルアプライアンスユーザーのパスワードを変更することをお勧めします。

- パスワード履歴は 7 に設定されているため、過去 7 個までの古いパスワードが保護され、ログに記録されます。新しいパスワードとして古いパスワードを使用しようとすると、アプライアンスにはトークン操作エラーが表示されます。
- 送信中のパスワードには、以下が含まれています。
  - パスワードが SSH プロトコルによって保護されている場所での SSH ログイン。
  - HTTPS 通信によってパスワードが保護されている場所での NetBackup Appliance Web Consoleログイン。

パスワードについて詳しくは、『NetBackup Appliance 管理者ガイド』を参照してください。

STIG 準拠パスワードポリシールールについて

STIG オプションを有効にすると、NetBackup アプライアンスに高度なセキュリティパスワードポリシーが自動的に適用され、STIG (Security Technical Implementation Guide) に準拠できます。

STIG オプションを有効にしても、デフォルトのポリシーを適用して作成した現在のユーザーパスワードはすべて引き続き有効です。ユーザーパスワードを変更する場合は、STIG 準拠ポリシールールに従う必要があります。

STIG 準拠パスワードポリシールールを次に示します。

- 最小文字数: 15
- 数字の最小文字数: 1
- 小文字の最小文字数: 1
- 大文字の最小文字数: 1
- 特殊文字の最小文字数: 1
- 同じ文字が連続する最大数: 2
- 同じクラスの文字が連続する最大数: 4
- 使用する異なる文字の最小数: 8
- 1 つのパスワードを変更するまでの最小日数: 1
- 1 つのパスワードを変更するまでの最大日数: 60
- 辞書にある言葉は無効で、使用できない
- 過去 7 回分のパスワードは再利用できない

ログインのロックアウトの適用

STIG オプションを有効にすると、15 分以内に 3 回連続して誤ったパスワードを入力したユーザーにログインのロックアウトが適用されます。ロックアウトの状態は、7 日間続きます。ロックアウトの状態をクリアするには、テクニカルサポートに連絡してください。

p.98 の「NetBackup アプライアンスのための OS STIG の強化」を参照してください。

3

ユーザー権限の確認

この章では以下の項目について説明しています。

NetBackup appliance におけるユーザー認可について

NetBackup appliance アプライアンスは、ユーザーアカウントを介して管理されます。ローカルユーザーアカウントを作成したり、リモートディレクトリサービスに属するユーザーとユーザーグループを登録したりすることができます。新しいユーザーアカウントがアプライアンスにログオンしてアクセスするには、最初にそのアカウントとロールを承認する必要があります。デフォルトでは、新しいユーザーアカウントには割り当てられたロールがないので、ロールが認可されるまでログオンできません。

表 3-1 NetBackup appliance のユーザー役割

ロール	説明
管理者	管理者役割が割り当てられているユーザーアカウントには、NetBackup appliance を管理するための管理権限が付与されます。管理者ユーザーは、NetBackup Appliance Web Console と NetBackup Appliance Shell Menuのすべての機能のログオン、表示、実行が許可されています。これらのユーザーアカウントには、アプライアンスにログオンし、NetBackup コマンドをスーパーユーザー権限で実行できる権限があります。 p.37 の「管理者ユーザーのロールについて」を参照してください。
NetBackupCLI	NetBackupCLI ロールが割り当てられたユーザーアカウントは、限定的な一連の NetBackup CLI コマンドだけを実行でき、NetBackup ソフトウェアディレクトリの範囲外へのアクセス権はありません。これらのユーザーがアプライアンスにログインすると、NetBackup を管理できる制限付きシェルメニューが表示されます。NetBackupCLI ユーザーには、NetBackup Appliance Web Consoleと NetBackup Appliance Shell Menuへのアクセス権はありません。 p.38 の「NetBackupCLI ユーザーロールについて」を参照してください。
AMSadmin	AMSadmin ロールが割り当てられたユーザーアカウントには、AMS でホストされている Appliance Manager にアクセスするための管理権限が付与されます。AMSadmin ユーザーは Appliance Manager ですべての機能を実行し、複数のアプライアンスを一元管理することができます。AMSadmin ユーザーは AMS の NetBackup Appliance Shell Menuにログオンすることはできません。管理者は、AMSadmin ユーザーを作成できます

次に、NetBackup appliance の認証の特徴の一部の一覧を示します。

- パスワード保護によるログインによってアプライアンスへの意図的でないアクセスを防止する機能。
- 共有データへのアクセス権は、権限があるアプライアンスユーザーと NetBackup 処理のみに提供されます。
- アプライアンス内に格納されているデータは、アプライアンスに対する管理者のクレデンシャルを把握している悪意のあるユーザーによる意図しない修正や削除から自身を保護することは本質的にできません。
- NetBackup Appliance Shell Menuへのネットワークアクセスは、SSH と、HTTPS を介した NetBackup Appliance Web Consoleを通してのみ許可。また、キーボードと

モニターをアプライアンスに直接接続し、管理者のクレデンシャルを使ってログオンすることもできます。

- FTP、Telnet、rlogin へのアクセスは、すべてのアプライアンスで無効になります。

メモ: ソフトウェアバージョン 3.1 以降では、NetBackup appliance はログイン試行を制限して、STIG 機能が有効になっている場合にのみロックアウトポリシーを適用します。詳しくは、次のトピックを参照してください。p.30 の「STIG 準拠パスワードポリシールールについて」を参照してください。

NetBackup アプライアンスユーザーの権限の確認について

表 3-2 では、NetBackup Appliance Web Consoleと NetBackup Appliance Shell Menu を使って新しいユーザーまたはユーザーグループと既存のユーザーまたはユーザーグループを認可するためのオプションについて説明します。

表 3-2　　ユーザー認可管理

タスク	NetBackup Appliance Web Console	NetBackup Appliance Shell Menu
ユーザーの管理	次のオプションは[設定(Settings)] > [認証(Authentication)] > [User Management(ユーザー管理)]にあります。 ■ アプライアンスに追加されているすべてのユーザーを表示する。 ■ 単一のユーザーグループに属しているすべてのユーザーを展開して表示する。 ■ ローカルユーザーを追加または削除する。 ■ LDAP/AD/Kerberos-NIS ユーザーとユーザーグループを追加または削除する。	`Settings > Security > Authentication` コマンドを利用し、アプライアンスユーザーを追加、削除、表示します。 p.18 の「ユーザー認証の設定について」を参照してください。

タスク	NetBackup Appliance Web Console	NetBackup Appliance Shell Menu
ユーザー権限(ロール)の管理	次のオプションは[設定(Settings)] > [認証(Authentication)] > [User Management (ユーザー管理)]にあります。 ■ ユーザーとユーザーグループの管理者ロールを付与し、取り消します。 ■ ユーザーとユーザーグループの NetBackupCLI ロールを付与し、取り消します。 ■ 管理者ロールを持つ登録済みユーザーグループのメンバーを同期します。	次のコマンドとオプションは `Main > Settings > Security > Authorization` にあります。 ■ `Grant` アプライアンスに追加されている特定のユーザーとユーザーグループに管理者ロールと NetBackupCLI ロールを与えます。 ■ `List` アプライアンスに追加されているユーザーとユーザーグループを、それに指定されているロールも含めて、すべて一覧表示します。 ■ **取り消し** アプライアンスに追加されている特定のユーザーとユーザーグループの管理者ロールと NetBackupCLI ロールを取り消します。 ■ `SyncGroupMembers` 登録済みユーザーグループのメンバーを同期します。

ユーザー管理に関するメモ

- 既存のローカルユーザーに NetBackupCLI ロールを付与することはできません。ただし、ローカル NetBackupCLI ユーザーを作成できます。その場合、`Manage > NetBackupCLI > Create` コマンドを NetBackup Appliance Shell Menuから実行します。
- NetBackupCLI ロールはいつでも最大 9 ユーザーグループに割り当てることができます。
- Active Directory (AD) のユーザーグループ名およびユーザー名で、ハイフン文字を使用できます。ハイフンは、ユーザー名またはユーザーグループ名の最初と最後の文字の間で使用される必要があります。AD のユーザー名およびユーザーグループ名の最初と最後にハイフンを使うことはできません。
- NetBackup Appliance Web Consoleからは、グループのすべてのユーザーを最大 2000 ユーザーまでリストできます。2000 を超えるユーザーが含まれるグループのすべてのユーザーをリストするには、NetBackup Appliance Shell Menuから `List` コマンドを使用します。

NetBackup appliance ユーザーロール権限

ユーザーロールにより、システムの操作やシステム設定の変更に対してユーザーが認可されるアクセス権が決まります。このトピックで説明するユーザーロールは LDAP ユーザー、Active Directory（AD）ユーザー、NIS ユーザーに固有です。

次は、アプライアンスユーザーロールとそれに関連付けられる権限の説明です。

表 3-3　　ユーザーロールと権限

ユーザーロール	権限
NetBackupCLI	ユーザーは NetBackup CLI のみにアクセスできます。 p.38 の「NetBackupCLI ユーザーロールについて」を参照してください。
管理者	ユーザーは次にアクセスできます。 ■ NetBackup Appliance Web Console ■ NetBackup Appliance Shell Menu ■ NetBackup 管理コンソール p.37 の「管理者ユーザーのロールについて」を参照してください。
AMSadmin	AMSadmin ロールが割り当てられたユーザーアカウントには、AMS でホストされているアプライアンス管理コンソールにアクセスするために必要な管理者権限が付与されます。AMS ユーザーはアプライアンス管理コンソールですべての機能を実行し、複数のアプライアンスを一元管理することができます。AMS ユーザーは AMS のNetBackup Appliance Shell Menuにログオンすることはできません。管理者は、AMS ユーザーを作成できます。

ロールは個別ユーザーに適用できます。あるいは、複数のユーザーを含むグループに適用できます。

両方のユーザーロールに対する権限をユーザーに与えることはできません。ただし、次のシナリオでは、NetBackupCLI ユーザーには NetBackup Appliance Shell Menuへのアクセス権限も与えられます。

- NetBackupCLI ロールがあるユーザーは、管理者ロールが割り当てられたグループにも入ります。
- 管理者ロールがあるユーザーは、NetBackupCLI ロールが割り当てられたグループにも入ります。

メモ: NetBackupCLI と NetBackup Appliance Shell Menuへの権限をユーザーに与えるとき、追加の手順が必要になります。NetBackup Appliance Shell Menuにアクセスするには、NetBackup CLI から `switch2admin` コマンドを入力する必要があります。

ユーザーとユーザーグループには次のように特権を与えることができます。

- NetBackup Appliance Web Consoleから、[設定(Settings)] > [認証(Authentication)] > [ユーザー管理(User Management)]ページで、[権限の付与(Grant Permissions)]リンクをクリックします。
- NetBackup Appliance Shell Menuから、`Settings > Security > Authorization` ビューで次のコマンドを使用します。

```
Grant Administrator Group
Grant Administrator Users
Grant NetBackupCLI Group
Grant NetBackupCLI Users
Grant AMS Group
Grant AMS Users
```

p.18 の「ユーザー認証の設定について」を参照してください。

p.34 の「NetBackup アプライアンスユーザーの権限の確認について」を参照してください。

管理者ユーザーのロールについて

NetBackup appliance は、アプライアンス上のバックアップデータへの無断アクセスを回避するため、アクセス制御メカニズムを提供しています。これらのメカニズムには、アプライアンスの構成の修正、アプライアンスの監視などのための昇格システム特権を提供する管理用ユーザーアカウントが含まれます。管理者役割が割り当てられているユーザーのみに、NetBackup appliance を構成および管理する権限があります。

管理者役割は、アプライアンスの構成または拡張ディスクストレージに含まれるバックアップデータへの権限のない不適切な改変を防ぐために、権限のあるシステム管理者のみに付与する必要があります。

管理者ユーザーは SSH を通した NetBackup Appliance Shell Menuか、または HTTPS を介した NetBackup Appliance Web Consoleを使ってアプライアンスにアクセスできます。

管理者ユーザーはスーパーユーザーとして次のタスクをすべて実行できます。

- アプライアンスの初期設定の実行。
- ハードウェア、ストレージ、SDCS ログの監視。
- ストレージ構成、追加サーバー、ライセンスなどの管理。

- ［日時（Date and Time）］、［ネットワーク（Network）］、［通知（Notification）］などの設定を更新します。
- アプライアンスのリストア。
- アプライアンスの使用停止。
- アプライアンスへのパッチ適用。
- 共有のマウントまたはマッピング。次の制限事項が適用されます。
  - Windows: Windows CIFS 共有のマウントまたはマップは、ローカルの管理者ユーザーにのみ許可されます。
  - Linux: ルートアクセスアカウントを持つユーザーのみが NFS 共有を直接マウントする mount コマンドを実行できます。

ローカル、LDAP、AD (Active Directory)、または NIS ユーザーがアプライアンスにアクセスして管理するには、管理者ユーザー役割の権限を保有する必要があります。新しいユーザーまたはユーザーグループを追加したら、NetBackup Appliance Web Console の［設定（Settings）> ［認証（Authentication）］> ［ユーザー管理（User Management）］ページを使って、管理者ユーザー権限を認可します。

NetBackupCLI ユーザーロールについて

NetBackupCLI ユーザーは、すべての NetBackup コマンドを実行したり、ログを表示したり、NetBackup タッチファイルを編集したり、NetBackup 通知スクリプトを編集したりすることができます。NetBackupCLI ユーザーは、スーパーユーザー権限による NetBackup コマンドの実行のみに制限されていて、NetBackup のソフトウェアディレクトリの範囲外にはアクセスできません。これらのユーザーがログインすると、NetBackup コマンドを実行できる制限付きシェルが表示されます。NetBackupCLI ユーザーはホームディレクトリを共有し、NetBackup Appliance Web Consoleまたは NetBackup Appliance Shell Menu にはアクセスできません。

表 3-4 に、NetBackupCLI ユーザーの権限と制限を示します。

表 3-4 アプライアンス NetBackupCLI ユーザーの権限と制限

権限	制限
NetBackupCLI ユーザーは、NetBackup Appliance Shell Menuを使って次の操作を実行できます。 ■ NetBackup CLI を実行して、NetBackup ディレクトリとファイルにアクセスする。 ■ cp-nbu-notify コマンドを使って、NetBackup 通知スクリプトを変更または作成する。 **メモ:** 通知スクリプトの制限はバージョン 2.6.0.2 以降に引き上げられました。 ■ 次の NetBackup コマンドを、NetBackup CLI を含む次のディレクトリに対して実行します。 ■ /usr/openv/netbackup/bin/* ■ /usr/openv/netbackup/bin/admincmd/* ■ /usr/openv/netbackup/bin/goodies/* ■ /usr/openv/volmgr/bin/* ■ /usr/openv/volmgr/bin/goodies/* ■ /usr/openv/pdde/pdag/bin/mtstrmd ■ /usr/openv/pdde/pdag/bin/pdcfg ■ /usr/openv/pdde/pdag/bin/pdusercfg ■ /usr/openv/pdde/pdconfigure/pdde ■ /usr/openv/pdde/pdcr/bin/*	NetBackupCLI ユーザーには次の制限があります。 ■ NetBackupCLI ユーザーは、NetBackup ソフトウェアディレクトリの外部へのアクセス権はありません。 ■ エディタを使用して bp.conf ファイルを直接編集することはできません。bpsetconfig コマンドを使用して、属性を設定します。 ■ cp-nbu-config コマンドは、/usr/openv/netbackup/db/config ディレクトリ内でのみ NetBackup タッチ構成ファイルの作成と編集をサポートします。 ■ man または -h コマンドは、他のいずれかのコマンドのヘルプを表示する場合、使用できません。

NetBackupCLI ユーザーとして NetBackup コマンドを実行する方法

次のいずれかの方法で、NetBackupCLI ユーザーとしてコマンドを実行します。

- 制限付きシェル
- 絶対パス [“sudo”]例: bppllist または /usr/openv/netbackup/bin/admincmd/bpplist

特別な指示句の処理を実行する方法

特別な指示句のファイルとコマンドが正しい NetBackup リストまたはパスにない場合、特別な指示句の処理は失敗することがあります。特別な指示句の処理の 1 つの例としては、代替の復元パスを指定する場合があります。

NetBackupCLI ユーザーとして NetBackup コマンドを実行して特別な指示句のファイルにアクセスする必要があるアプライアンスユーザーは、次のことを実行して正常に処理を完了する必要があります。

- NetBackup `bpcd whitelist` に `/home/nbusers` パスを追加します。
- `/home/nbusers` ディレクトリに特別な指示句のコマンドを追加します。

NetBackup `bpcd whitelist` へのエントリの追加について詳しくは、次のドキュメントの `BPCD_WHITELIST_PATH` 構成オプションを参照してください。

NetBackup 管理者ガイド Vol. 1

NetBackup コマンドリファレンスガイド

4

侵入防止、侵入検知システム

この章では以下の項目について説明しています。

NetBackup appliance の Symantec Data Center Security について

メモ: 以前のアプライアンスリリースでは、Symantec Data Center Security（SDCS）は Symantec Critical System Protection（SCSP）という名前でした。NetBackup Appliance 2.7.1 以降へのアップグレードの一部として、アプライアンスの SDCS エージェントが、アンマネージモードに設定されます。アップグレード前にアプライアンスがマネージモードで動作していた場合は、アップグレードの完了後に必ずアプライアンスをマネージモードにリセットしてください。

また、SDCS 管理サーバーでアプライアンスの IPS および IDS のポリシーも更新する必要があります。古いポリシーを使用してソフトウェアバージョン 2.7.1 以降を実行しているアプライアンスを管理することはできません。新しいポリシーは、NetBackup Appliance Web Consoleの［監視 (Monitor)］>［SDCS のイベント (SDCS Events)］ページからダウンロードできます。また、IPS および IDS のポリシーに設定したカスタム規則やサポートの例外は NetBackup Appliance 2.7.1 にアップグレードした後は使用できなくなります。

Symantec Data Center Security: Server Advanced（SDCS）は、データセンターのサーバーを保護するためにシマンテック社が提供するセキュリティソリューションです。SDCS ソフトウェアはアプライアンスに含まれ、アプライアンスソフトウェアのインストール時に自動的に設定されます。SDCS はポリシーベースの保護を提供し、ホストベースの侵入防止と検出技術を使ってアプライアンスを保全します。最小の権限付与による封じ込めで、セキュリティ管理者がデータセンターの複数のアプライアンスを集中的に管理できるようにします。SDCS エージェントは起動時に実行され、カスタマイズされた NetBackup appliance の侵入防止システム (IPS) ポリシーおよび侵入検知システム (IDS) ポリシーをエンフォースします。アプライアンスの SDCS ソリューション全体で次の機能を提供します。

- Linux OS コンポーネントの強化
  OS の脆弱性によりマルウェアが基本ホストシステムの整合性を阻害しないようにするか、またはマルウェアを含めます。
- データ保護
  システム権限に関係なく、アクセスを必要とするプログラムと活動のみにアプライアンスのデータアクセスを限定します。
- アプライアンススタックの強化
  アプリケーションまた信頼されたプログラムおよびスクリプトによって変更が強固に制御されるように、アプライアンスアプリケーションのバイナリと構成の設定がロックダウンされます。
- 検出機能と監査機能の拡張

補正制御として法規制 (PCI など) に対処する有効で完全な監査証跡を確認するために、重要なユーザーやシステムの処理の表示を拡張します。

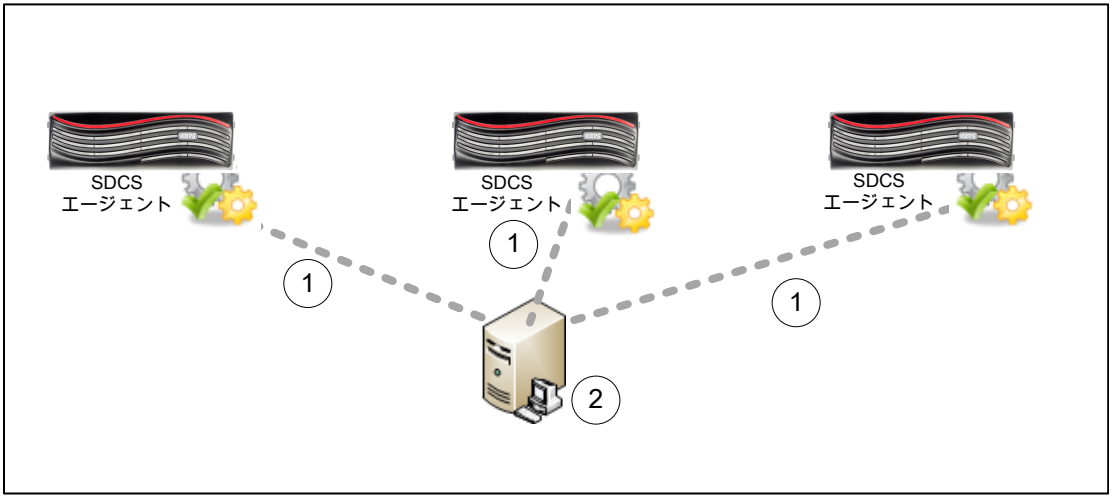
- 集中管理モードによる操作
  ユーザーは、SDCS が管理する複数のアプライアンスや他の企業システム全体のセキュリティを統合的に表示するために集約型 SDCS マネージャを使うことができます。

アプライアンスへの SDCS の実装は、アンマネージモードまたはマネージモードで操作できます。デフォルトでは、SDCS はアンマネージモードで動作して、ホストベースの侵入防止と検出技術を使ってアプライアンスを保全します。NetBackup アプライアンスは、SDCS サーバーに接続していないときはアンマネージモードになります。アンマネージモードでは、NetBackup Appliance Web Consoleから SDCS イベントを監視できます。ログイベントを監視するには、[監視]>[SDCS イベント]を使います。イベントは NetBackup Appliance IPS と IDS ポリシーを使って監視されます。これらのポリシーは初期構成のときに自動的に適用されます。特定のイベントをフィルタ処理して表示するには、[ログのフィルタ]をクリックします。

マネージモードでは、アプライアンスの SDCS エージェントは、アプライアンスの保護を継続し、集中管理およびログ分析のために外部 SDCS サーバーにも接続します。マネージモードでは、アプライアンスは SDCS サーバーに接続され、イベントは SDCS 管理コンソールを使って監視されます。このモードでは、1 つの SDCS サーバーを使って複数のアプライアンスを監視できます。SDCS エージェントは、SDCS サーバーにイベントを送るのに使われる各 NetBackup アプライアンスとともに設定されます。

図 4-1 はマネージモードの SDCS を示します。

図 4-1　　マネージモードでの SDCS 実装



マネージモードを設定するには、SDCS サーバーと管理コンソールをインストールし、次にアプライアンスを SDCS サーバーに接続します。

[監視]>[SDCSイベント]から次を実行します。

- NetBackup Appliance IPS と IDS ポリシーのダウンロード
- SDCS 管理コンソールを使ってこれらのポリシーを適用
- NetBackup アプライアンスをサーバーに接続
- サーバーに接続されたすべての NetBakup アプリケーションのイベントの監視

[監視]>[SDCS イベント]>[SDCSサーバーに接続]から次を実行します。

- SDCS サーバー詳細の追加
- TBD のダウンロード
- SDCS サーバーへの接続

アプライアンスへの SDCS 実装について詳しくは、『NetBackup Appliance セキュリティガイド』を参照してください。

NetBackup appliance の侵入防止システムについて

アプライアンスの侵入防止システム（IPS）は、起動時に自動的に動作する SDCS（Symantec Data Center Security）ポリシーで構成されます。IPS ポリシーは、不要なリソースアクセスの動作がオペレーティングシステムで実行される前に事前に遮断できるインラインのポリシーです。

次のリストには、IPS ポリシー機能の一部が含まれています。

- アプライアンスの OS の処理および共通のアプリケーションのリアルタイムの厳しい制限は以下のとおりです。
  - `nscd` - DNS 要求をキャッシュして、リモート DNS ルックアップを削減します。
  - `cron`
  - `syslog-ng`
  - `klogd`
  - NFS の `rpcd`
    - `rpc.idmapd`
    - `rpc.mountd`
    - `rpc.statd`
    - `rpcbind`
- SDCS エージェント自身のための自己防衛、セキュリティと SDCS の監視機能は損なわれないことを確認します。

- 特定され、信頼されているアプリケーション、ユーザー、ユーザーグループによらない限り、システムバイナリを終了します。
- アプリケーションが sbin などのソフトウェアをインストールしようとしたり、ホストファイルなどのシステム構成の設定を変更しようとしたりすることから、システムを保護する制限です。
- mknod、modctl、link, mount などの重要なシステムコールをアプリケーションで実行することを禁止します。
- /advanceddisk、/cat、/disk、/usr/openv/kms、/opt/NBUAppliance/db/config/data などのバックアップデータに権限のないユーザーやアプリケーションがアクセスすることを禁止します。
- メンテナンスユーザーによってルートアカウントへのアクセスが制限されました。p.50 の「NetBackup appliance の侵入防止システムポリシーの上書き」を参照してください。

NetBackup appliance の侵入検知システムについて

アプライアンスの侵入検知システム（IDS）は、起動時に自動的に動作する SDCS（Symantec Data Center Security）ポリシーで構成されます。IDS ポリシーは、重要なシステムイベントおよび重要な構成の変更を監視し、省略可能なオプションとして対象のイベントに修復操作を実行するリアルタイムポリシーです。

次のリストには、IDS ポリシーが監視するイベントの一部が含まれています。

- ユーザーログイン、ログアウト、試行時に失敗したログオン
- Sudo コマンド
- ユーザーの追加、削除、パスワード変更
- ユーザーグループの追加、削除、メンバーの変更
- システム自動起動オプションの変更
- すべてのシステムディレクトリとファイルに対する変更 (主要システムファイル、主要システム構成ファイル、インストールプログラム、共通デーモンファイルを含む)
- NetBackup のサービス開始と停止
- UNIX ルートキットファイル/ディレクトリ検出、UNIX ワームファイル/ディレクトリ検出、悪意のあるモジュールの検出、疑わしいパーミッション変更の検出などにより検出されたシステムへの攻撃
- 保守、ルートおよび NetBackupCLI ユーザーのためのシェル操作を含めた NetBackup Appliance Web Consoleおよび NetBackup Appliance Shell Menuのすべての動作の監査。

NetBackup アプライアンスの SDCS イベントの見直し

[監視]>[SCSP イベント]ページで、SDCS(Symantec Data Center Security)ログを表示できます。これらの監査ログは、アプライアンスのセキュリティ違反や異常なアクティビティを検出するのに役立ちます。監査ログのイベントには、次の詳細が含まれます。

- 時間 - ログイベントのタイムスタンプを表示します。
- ユーザー - イベントが起きた時ログオンしていたユーザーを表示します。
- 内容 - イベントと関連するリソースの説明を表示します。
- 詳細 - プロセス名、プロセス ID、操作権限、およびサンドボックスの詳細を表示します。
- 重大度 - イベントの重大度を表示します。
- 処理の実施 - イベントが許可されたか拒否されたかを表示します。

SDCS イベントが取り込まれ、表 4-1に記述されている重大度の種類を使って表されます。

表 4-1 SDCS イベントの重大度の種類

重大度の種類	説明	イベントの例

情報 (Information)	重大度が[情報 (Info)]のイベントには、通常のシステム操作についての情報が含まれます。	たとえば、次のメッセージは汎用イベントに関する基本情報を提供します。
		
		`general CLISH message`
		
		`Event source: SYSLOG PID: 30315 Complete message: May 21 06:58:55 nb-appliance CLISH[30315]: User admin executed Return`

重大度の種類	説明	イベントの例

通知 (Notice)	重大度が[通知 (Notice)]のイベントには、通常のシステム操作についての情報が含まれます。	イベントの実行が成功したことを確認する場合に役立つイベントが、[通知 (Notice)]として記録されます。たとえば、次のメッセージによって、ユーザーはイベントが正常に実行されたことを理解できます。
		
		`successful SUDO to root`
		`Event source: SYSLOG [sudo facility]`
		`Command: /bin/su From`
		
		`Username: AppComm To Username: root`
		`Port: unknown`

警告 (Warning)	重大度が[警告]のイベントは、SDCS によってすでに処理された予想外の活動または問題を示します。これらの警告メッセージは、ターゲットコンピュータのサービスまたはアプリケーションが適用済みのポリシーに対して不適切に機能していることを示している可能性があります。ポリシー違反を調査した後、必要に応じて、ポリシーを構成し、サービスまたはアプリケーションが特定のリソースにアクセスできるようにします。	たとえば、次のイベントはローカル IP アドレスからの着信接続のような予想外のアクティビティを特定する場合に役立ちます。 `Inbound connection allowed from <IPaddress> to local address.`

重大度の種類	説明	イベントの例

主要 (Major)	重大度が[主要 (Major)]のイベントは、[警告 (Warning)]のイベントよりも深刻な影響を示しますが、[重要 (Critical)]のイベントほど影響を与えません。	たとえば、次のイベントは認証されていないアクセスを識別するのに役立ちます。
		
		`General luser message`
		
		`Event source:SYSLOG Complete message: Feb 5 21:57 luser Unauthorized user by luser Denying access to system.`

重要 (Critical)	重大度が[重要 (Critical)]のイベントは、管理者による修正が必要になる場合があるアクティビティまたは問題を示します。	たとえば、予想外の方法でアプライアンスに影響を及ぼす可能性のある重要なイベントを特定する場合に、次のイベントが役立つことがあります。 `Group Membership for "group1" CHANGED from 'admin1' to 'admin2'`

SDCS 監査ログの取り込みについて詳しくは、『NetBackup Appliance 管理者ガイド』を参照してください。

syslog や他のアプライアンスログのようなアプライアンスのオペレーティングシステムログについて詳しくは、p.56 の「NetBackup appliance のログファイルについて」を参照してください。を参照してください。

NetBackup アプライアンスでのアンマネージモードでの SDCS の実行

アプライアンスへの Symantec Data Center Security（SDCS）の実装は、アンマネージモードまたはマネージモードで操作できます。アンマネージモードはアプライアンスを構成するデフォルトモードです。アンマネージモードの場合、アプライアンスは外部 SDCS サーバーを使わないで保護され、監査されます。アンマネージモードでも、IDS と IPS の両方のポリシーが適用され、起動時にアプライアンスが保護されます。

アンマネージモードは、アプライアンスの単独の担当者であり、主にバックアップ管理に関係する管理者にお勧めします。

SDCS イベントは、NetBackup Appliance Web Console ([監視 (Monitor)] > [SDCS イベント (SDCS Events)]) と NetBackup Appliance Shell Menu (`Main_Menu > Monitor > SDCS`) から監視できます。

NetBackup アプライアンスでのマネージモードでの SDCS の実行

アプライアンスへの SDCS の実装は、アンマネージモードまたはマネージモードで操作できます。マネージモードでは、外部 SDCS サーバーを使って 1 台以上のアプライアンスの SDCS エージェントと通信し、これを管理することができます。SDCS サーバーはマネージモードで使用されているのと同じ IPS および IDS ポリシーを使用します。NetBackup Appliance Web Consoleから SDCS ポリシーをダウンロードできます。

マネージモードはセキュリティ管理者または SDCS に精通している SDCS の既存のお客様のみが使うことを推奨します。

マネージモード使用の利点:

- バックアップ管理者の役割とセキュリティ管理者の役割に応じたツールを別々に提供できます。
- 単一の SDCS サーバーとコンソールを使用して複数のアプライアンスのセキュリティの集中管理を提供します。
- ログをアーカイブし、エクスポートする機能を提供します。
- 警告の監視、報告、セットアップに使用する共通コンソールを提供します。
- データセンターの基準に合うようにシマンテック社のベースラインを基づいて IPS と IDS ポリシーを拡張します。

SDCS マネージモードでアプライアンスを構成する方法

1. SDCS コンソールを使って SDCS サーバーに接続でき、そのサーバーからアプライアンスに接続できることを確認します。

   SDCS コンソールとサーバーソフトウェアが必要な場合は、https://my.veritas.com からダウンロードできます。

2. SDCS コンソールを使ってアプライアンスから IPS ポリシーと IDS ポリシーをダウンロードしてインポートします。これらのポリシーは、NetBackup Appliance Web Consoleの[監視 (Monitor)] > [SDCS イベント (SDCS Events)]から直接ダウンロードできます。

3 アプライアンスを SDCS サーバーに接続します。NetBackup Appliance Web Consoleの[監視 (Monitor)] > [SDCS イベント (SDCS Events)]または NetBackup Appliance Shell Menuの `Monitor > SDCS` から SDCS サーバーに接続できます。

4 SDCS コンソールを使って、接続されているアプライアンスに IPS ポリシーと IDS ポリシーを適用します。

NetBackup appliance の侵入防止システムポリシーの上書き

ルートアカウントへのアクセスを避けるには、アプライアンスで最初に侵入防止システム (IPS) ポリシーを無効にする必要があります。たとえば、IPS ポリシーを無効にしていないと、`Support > Maintenance` の下の `elevate` コマンドの使用が失敗します。

警告: IPS ポリシーを無効にすると、システムがリスクにさらされ、攻撃に対して脆弱になるため、これは推奨されません。

NetBackupCLI ユーザーの役割を使用すると、IPS ポリシーを上書きすることなく、NetBackup コマンドを実行できます。p.38 の「NetBackupCLI ユーザーロールについて」を参照してください。

メモ: IPS ポリシーを上書きすると、アプライアンスの侵入防止システムのみが無効になります。アプライアンスの侵入検知システム (IDS) のログは有効なままで、メンテナンスアカウントでのあらゆる処理はログに記録されます。

アプライアンスの IPS ポリシーを上書きする方法

1 NetBackup Appliance Shell Menuに管理者としてログオンします。

2 `Support > Maintenance` コマンドを入力し、メンテナンスモードのログインプロンプトが表示されます。保守担当ユーザーアカウントのパスワードを入力して、メンテナンスモードにログインします。

```
app123.Support> Maintenance
<!-- Maintenance Mode --!>
maintenance's password:
```

3 IPS ポリシーを上書きするには、メンテナンスモードで次のコマンドを入力します。

```
/opt/Symantec/sdcssagent/IPS/sisipsoverride.sh
```

次のメッセージが表示されます。

```
Symantec Critical Protection Policy Override

Agent Version: 6.7 (build 1060)

Current Policy: NetBackup Appliance Prevention Policy, r123

Policy Prevention: Enabled

Policy Override: Allowed

Override State: Not overridden

To override the policy and disable protection,
enter your login password.

Password:
```

4 保守担当ユーザーアカウントのパスワードを入力します。以下のオプションが表示されます。

```
Choose the type of override that you wish to perform:

1. Override Prevention except for Self Protection

2. Override Prevention Completely

Choice?
```

5 1 を入力すると、自己防衛以外の防止が上書きされます。

メモ: Veritasはオプション 1 を使用するように推奨しています。[オプション 1 (Option 1)]を選択すると、NetBackup Appliance Shell Menuの変更のみが許可され、SDCS エージェントの変更は許可されません。

以下のオプションが表示されます。

```
Choose the amount of time after which to automatically re-enable:

1. 15 minutes

2. 30 minutes

3. 1 hour

4. 2 hours

5. 4 hours

6. 8 hours
```

6 サポートケースのデバッグに必要な時間に基づいて 1 から 7 までの適切な数字を入力します。

アプライアンスに次のメッセージが表示されます。

```
Enter a comment. Press Enter to continue.
```

7 上書きが必要な理由に関して関連するコメントを入力します。たとえば、

```
Enter a comment. Press Enter to continue.

Disabling the security policy for
debugging support case no - XYZ
```

アプライアンスはポリシーを上書きし、次のメッセージを表示します。

```
Please wait while the policy is being overridden.
........

The policy was successfully overridden.
maintenance - !> elevate
```

アプライアンスをデバッグするには、ここでルートアカウントへのアクセス権が必要になります。

NetBackup appliance の侵入防止システムポリシーの再有効化

次の手順を実行すれば、侵入セキュリティポリシー（IPS）をメンテナンスモードから再び有効にすることができます。

シマンテック社の侵入セキュリティポリシーを再び有効にするには

1. NetBackup Appliance Shell Menuに管理者としてログオンします。
2. `Support > Maintenance` コマンドを入力し、メンテナンスモードのログインプロンプトが表示されます。保守担当ユーザーアカウントのパスワードを入力して、メンテナンスモードにログインします。

```
app123.Support> Maintenance
<!-- Maintenance Mode --!>
maintenance's password:
```

3 IPS ポリシーを再び有効にするには、メンテナンスモードで次のコマンドを入力します。

```
/opt/Symantec/sdcssagent/IPS/sisipsoverride.sh
```

次のメッセージが表示されます。

```
Symantec Critical Protection Policy Override

Agent Version: 6.7 (build 1060)

Current Policy: NetBackup Appliance Prevention Policy, r123

Policy Prevention: Enabled

Policy Override: Allowed

Override State: Overriden

Overide Type: Prevention Overriden except for Self-Protection

Overide User: maintenance

Previous Comment: This is an example.

Auto re-enable in: 13 minutes, 31 seconds


Do you wish to:

1. Re-enable the Policy.
2. Extend the Override Time.
```

4 IPS ポリシーを再び有効にするには、1 を入力します。

次のメッセージが表示されます。

```
Enter a comment. Press Enter to continue.
```

5 次のように、関連するコメントを入力します。

```
Enter a comment. Press Enter to continue.

The policy is re-enabled.
```

アプライアンスはポリシーを再び有効にし、次のメッセージが表示されます。

```
Please wait while the policy is being re-enabled.

......

The policy was successfully re-enabled.
```

5

ログファイル

この章では以下の項目について説明しています。

NetBackup appliance のログファイルについて

ログファイルは、アプライアンスで発生する可能性がある問題の特定と解決に役立ちます。

NetBackup appliance では、ハードウェア、ソフトウェア、システム、パフォーマンス関連のデータを取得できます。ログファイルは、アプライアンス操作などの情報、未構成ボリュームまたはアレイなどの問題、温度またはバッテリに関する問題、およびその他の詳細を取得します。

表 5-1 に、アプライアンスのログファイルにアクセスするために使用できる方法を説明します。

表 5-1 ログファイルの表示

使用する媒体	アクセス方法	ログの詳細
NetBackup Appliance Web Console	NetBackup Appliance Web Consoleの[モニター (Monitor)]>[SDCS 監査ビュー (SCSP Audit View)]画面を使用して、アプライアンスの監査ログを取得できます。p.46 の「NetBackup アプライアンスの SDCS イベントの見直し」を参照してください。	アプライアンスの監査ログ
NetBackup Appliance Shell Menu	`Main > Support > Logs > Browse` コマンドを実行すると、`LOGROOT/>` プロンプトが開きます。`ls` や `cd` コマンドを使用して、アプライアンスのログディレクトリを走査できます。p.58 の「Support コマンドの使用によるログファイルの表示」を参照してください。	■ Appliance の構成ログ ■ Appliance のコマンドログ ■ Appliance のデバッグログ ■ NetBackup ログ、Volume Manager ログ、`openv` ディレクトリに含まれている NetBackup ログ ■ Appliance のオペレーティングシステム (OS) インストールログ ■ NetBackup 管理 Web ユーザーインターフェースログと NetBackup Web サーバーログ ■ NetBackup 52xx アプライアンスのデバイスログ

使用する媒体	アクセス方法	ログの詳細
NetBackup Appliance Shell Menu	`Main > Support > Logs > VxLogView Module` *ModuleName* コマンドを実行して、Appliance VxUL (統合) ログにアクセスすることができます。`Main > Support > Share Open` コマンドを実行し、デスクトップを使用して VxUL ログのマップ、共有、コピーを行うこともできます。 p.58 の「Support コマンドの使用によるログファイルの表示」を参照してください。	Appliance 統合ログ: ■ `All` ■ `CallHome` ■ `Checkpoint` ■ `Commands` ■ `Common` ■ `Config` ■ `CrossHost` ■ `Database` ■ `Hardware` ■ `HWMonitor` ■ `Network` ■ `RAID` ■ `Seeding` ■ `SelfTest` ■ `Storage` ■ `SWUpdate` ■ `Trace` ■ `FTMS` ■ `FTDedup` ■ `TaskService` ■ `AuthService`
NetBackup Appliance Shell Menu	`Main > Support > DataCollect` コマンドを実行して、ストレージデバイスログを収集できます。 p.61 の「DataCollect コマンドを使ったデバイスログの収集」を参照してください。	Appliance ストレージデバイスログ
NetBackup Java アプリケーション	NetBackup Java アプリケーションに関する問題が発生した場合、このセクションのスクリプトを使って、サポートに連絡するために必要な情報を集めることができます。	NetBackup Java アプリケーションに関するログ

Support コマンドの使用によるログファイルの表示

次のセクションを使ってログファイルの情報を表示できます。

Support > Logs > Browse コマンドを使用してログを表示する方法

1. NetBackup Appliance Shell Menuで Main_Menu > Support > Logs を使用して参照モードにしたら、Browse コマンドを実行します。LOGROOT/> プロンプトが表示されます。
2. アプライアンスの利用可能なログディレクトリを表示するには、LOGROOT/> プロンプトで ls と入力します。
3. いずれかのログディレクトリで利用可能なログファイルを参照するには、cd コマンドを使って、選択するログディレクトリにディレクトリを変更します。プロンプトが現在のディレクトリを示すように変わります。たとえば、ディレクトリを OS ディレクトリに変更した場合、プロンプトは LOGROOT/OS/> と表示されます。そのプロンプトから ls コマンドを使うと、OS ログディレクトリの利用可能なログファイルを表示できます。
4. ファイルを表示するには、less <FILE> または tail <FILE> コマンドを使います。ファイルは <FILE> で、ディレクトリは <DIR> でマーク付けされます。

p.60 の「Browse コマンドを使用した NetBackup appliance ログファイルの参照場所」を参照してください。

Support > Logs コマンドを使用して NetBackup appliance 統合 (VxUL) ログを表示する方法

1. Support > Logs > VXLogView コマンドを使用して、NetBackup appliance 統合 (VxUL) ログを表示できます。コマンドをシェルメニューに入力し、次のオプションのうちいずれかを使用します。
   - Logs VXLogView JobID *job_id*
     特定のジョブ ID に関するデバッグ情報の表示に使用します。
   - Logs VXLogView Minutes *minutes_ago*
     特定の時間枠に関するデバッグ情報の表示に使用します。
   - Logs VXLogView Module *module_name*
     特定のモジュールに関するデバッグ情報の表示に使用します。
2. 必要に応じて、Main > Support > Logs > Share Open コマンドを使って統合ログをコピーできます。デスクトップを使ってログのマップ、共有、コピーを行います。

また、Main_Menu > Support > Logs コマンドを使って次のことを実行することもできます。

- ベリタスのテクニカルサポートにログファイルをアップロードする
- ログレベルを設定する
- CIFS 共有と NFS 共有をエクスポートまたは削除する

メモ: NetBackup appliance VxUL ログは、cron ジョブまたはスケジュール済みタスクによってアーカイブされなくなりました。さらに、ログの再利用が有効になり、デフォルトのログファイル数が 50 に設定されました。

上記のコマンドを使う方法について詳しくは『NetBackup Appliance コマンドリファレンスガイド』を参照してください。

p.56 の「NetBackup appliance のログファイルについて」を参照してください。

Browse コマンドを使用した NetBackup appliance ログファイルの参照場所

表 5-2 は、Support > Logs > Browse コマンドを実行することで、アクセス可能なログとログディレクトリの場所を提供します。

表 5-2 NetBackup appliance ログファイルの場所

アプライアンスログ	ログファイルの場所
構成ログ	<DIR> APPLIANCE config_nb_factory.log
セルフテストレポート	<DIR> APPLIANCE selftest_report
ホスト変更ログ	<DIR> APPLIANCE hostchange.log
NetBackup ログ、Volume Manager ログ、openv ディレクトリに含まれている NetBackup ログ	<DIR> NBU ■ <DIR> netbackup ■ <DIR> openv ■ <DIR> volmgr
オペレーティングシステム (OS) インストールログ	<DIR> OS boot.log boot.msg boot.omsg messages
NetBackup 重複排除(PDDE)構成スクリプトのログ	<DIR> PD pdde-config.log

アプライアンスログ	ログファイルの場所
NetBackup 管理 Web ユーザーインターフェースログと NetBackup Web サーバーログ	<DIR> WEBGUI ■ <DIR> gui ■ <DIR> webserver
デバイスログ	/tmp/DataCollect.zip Main > Support > Logs > Share Open コマンドを使うと、DataCollect.zip をローカルフォルダにコピーできます。

p.56 の「NetBackup appliance のログファイルについて」を参照してください。

DataCollect コマンドを使ったデバイスログの収集

Main > Support シェルメニューから DataCollect コマンドを使ってデバイスログを収集できます。これらのデバイスログを ベリタスのサポートチームと共有することで、デバイス関連の問題を解決できます。

DataCollect コマンドは次のログを収集します。

- リリース情報
- ディスクパフォーマンスのログ
- コマンド出力ログ
- iSCSI ログ

メモ: iSCSI ログは /var/log/messages and /var/log/iscsiuio.log にあります。

- CPU 情報
- メモリ情報
- オペレーティングシステムのログ
- Patch ログ
- ストレージログ
- ファイルシステムログ
- Test hardware のログ
- AutoSupport ログ
- ハードウェア情報

- Sysinfo ログ

DataCollect コマンドを使ってデバイスログを収集する方法

1. NetBackup Appliance Shell Menuにログオンします。
2. `Main > Support` ビューから次のコマンドを入力して、デバイスログを収集します。

   ```
   DataCollect
   ```

   アプライアンスは `/tmp/DataCollect.zip` ファイルにデバイスログを生成します。
3. `Main > Support > Logs > Share Open` コマンドを使って、`DataCollect.zip` をローカルフォルダにコピーします。
4. 問題を解決するために、ベリタスのサポートチームに `DataCollect.zip` ファイルを送信できます。

p.56 の「NetBackup appliance のログファイルについて」を参照してください。

ログ転送機能の概要

ログ転送機能を使用すると、外部ログ管理サーバーにアプライアンスのログを送信できます。ソフトウェアバージョン 3.0 以降では、NetBackup アプライアンスで syslog の転送がサポートされます。syslog は、ユーザーレベルやシステムレベルのアクティビティがイベントの形式で格納されている OS システムログのことです。この機能は、セキュリティを高めて、HIPPA、SOX、PCI などの一般的なコンプライアンスイニシアチブを実現する場合に使用します。現在サポートされているログ管理サーバーは HP ArcSight と Splunk です。

NetBackup アプライアンスは、Rsyslog クライアントを使用してログを転送します。HP ArcSight と Splunk 以外に、Rsyslog クライアントをサポートする他のログ管理サーバーを使用してアプライアンスから syslog を受信することもできます。Rsyslog クライアントのサポートの有無を確認するには、ログ管理サーバーのマニュアルを参照してください。

ログ送信の保護

アプライアンスからログ管理サーバーに安全にログを伝送するには、トランスポート層セキュリティ (TLS) オプションを使用します。NetBackup appliance は、現在ログ転送で TLS 匿名認証のみをサポートしています。

TLS を有効にするには、アプライアンスとログ管理サーバーのそれぞれに、次のように個別の準備が必要です。

- アプライアンスの要件
  ログ転送機能を構成して有効にするには、アプライアンスに X.509 ファイル形式で次の証明書ファイルと秘密鍵ファイルが必要になります。
  - `ca-server.pem`
    ログ管理サーバー証明書の元であるルート CA 証明書

- nba-rsyslog.pem
  ログ管理サーバーと通信するために必要なアプライアンスの証明書。すべての中間 CA 証明書も含む
- nba-rsyslog.key
  syslog 管理サーバーと通信するために使用する証明書に対応する秘密鍵

これらのファイルは NFS 共有または CIFS 共有を使用してアプライアンスにアップロードできます。

- HP ArcSight サーバーの構成要件
  アプライアンスから暗号化されたログを受け取るには、HP ArcSight サーバーに TLS を設定して Rsyslog サーバーをセットアップする必要があります。次に、復号化されたログを HP ArcSiight サーバーに転送するように Rsyslog サーバーを構成します。セットアップと構成の手順については、www.rsyslog.com のWeb サイトを参照してください。
- Splunk サーバーの構成要件
  最初にこれらのサーバーで TLS を構成してから、アプライアンスでログ転送機能を構成する必要があります。TLS の適切な構成について詳しくは、Splunk のマニュアルを参照してください。

構成

この機能は、次の Main > Settings > LogFowarding コマンドオプションを使用してシェルメニューから構成する必要があります。

- LogForwarding Enable
  機能を構成します。
- LogForwarding Disable
  構成を削除して機能を無効にします。
- LogForwarding Interval
  ログの転送頻度を設定します。0 (連続)、15、30、45、または 60 分から選択します。
- LogForwarding Share
  必須の証明書ファイルと秘密鍵ファイルを取得するために、アプライアンスで NFS 共有または CIFS 共有を開くかまたは閉じます。共有パスは次のとおりです。
  NFS: <appliance.name>:/inst/logforwarding.
  CIFS: ¥¥<appliance.name>¥logforwarding
- LogForwarding Show
  現在の構成と状態を表示します。

LogForwarding > Enable コマンドを入力すると、次の表に記載されている手順に従って構成をガイドするプロンプトが表示されます。

表 5-3 `LogForwarding > Enable` コマンドのプロンプト

プロンプト	説明
サーバー名または IP (Server name or IP)	外部ログ管理サーバーのは名前または IP アドレスを入力します。
サーバーポート (Server port)	外部ログ管理サーバーの適切なポート番号を入力します。
プロトコル (Protocol)	UDP または TCP を選択します。
間隔 (Interval)	ログの転送頻度を設定します。
TLS の有効化 (Enable TLS)	ログ管理サーバーへのログ送信を保護するために TLS を選択して、有効にします。現時点では X.509 ファイル形式のみがサポートされます。 TLS を使用するには、次の証明書ファイルと秘密鍵ファイルをアプライアンスにアップロードする必要があります。 ■ `ca-server.pem` ■ `nba-rsyslog.pem` ■ `nba-rsyslog.key`

構成とコマンドについて詳しくは、次のドキュメントを参照してください。

NetBackup アプライアンス管理者ガイド

NetBackup アプライアンスコマンドリファレンスガイド

6

オペレーティングシステムのセキュリティ

この章では以下の項目について説明しています。

NetBackup アプライアンスのオペレーティングシステムのセキュリティについて

NetBackup アプライアンスは、カスタマイズされた Linux オペレーティングシステムである VxOS (Veritas オペレーティングシステム) を使用します。NetBackup アプライアンスソフトウェアの各リリースには、最新バージョンの VxOS と NetBackup ソフトウェアが含まれます。定期的なセキュリティパッチと更新に加え、VxOS には次のセキュリティ拡張機能とその他の機能が含まれています。

- 更新され、調整された RHEL (Red Hat Enterprise Linux) ベースの Linux OS プラットフォームによって、すべての必要なソフトウェアコンポーネントを互換性がある堅牢なハードウェアプラットフォームにパッケージし、インストールすることができます。
- NIST (米国標準) と RHEL からのセキュリティ基準に基づいて VxOS のセキュリティを強化します。追加のセキュリティが SDCS (Symantec Data Center Security) によって提供されます。
- Symantec Data Center Security: Server Advanced (SDCS) 侵入防止および侵入検出ソフトウェアは、各プロセスとすべてのシステムファイルを隔離し、サンドボックス化することで、VxOS を強化してバックアップデータを保護します。

- 業界に認められた脆弱性スキャナによるアプライアンスの定期スキャン。検出された脆弱性は、アプライアンスソフトウェアの定期リリースや、Emergency Engineering Binary(EEB)を使用してパッチが適用されます。セキュリティ上の脅威がリリーススケジュールの間に特定された場合、既知の解決法については Veritas サポートまでお問い合わせください。
- 未使用のサービスアカウントは削除されるか無効化されます。
- VxOS にはサービス拒否 (DoS) のような攻撃からアプライアンスを保護するための編集されたカーネルパラメータが含まれます。例えば、`sysctl` 設定、`net.ipv4.tcp_syncookies` は、TCP SYN cookies を実装するため、`/etc/sysctl.conf` 構成ファイルに追加されました。
- 不要な runlevel サービスは無効化されました。VxOS では、runlevel を使用し、実行する必要のあるサービスを判断したり、システム上で実行する特定の作業を許可したりします。
- `FTP`、`telnet`、`rlogin (rsh)` は無効化されました。使用は、`ssh`、`scp`、`sftp` に限定されます。
- `AllowTcpForwarding no` と`X11Forwarding no` の `/etc/ssh/sshd_config` への追加で、SSH の TCP 転送は無効化されました。
- IP 転送が VxOS 上で無効にされ、TCP/IP スタックでのルーティングを許可しなくなりました。この機能により、あるサブネット上のホストがアプライアンスをルーターとして使って、別のサブネット上のホストにアクセスするのを防ぐことができます。
- NetBackup アプライアンスでは、ネットワークインターフェース上での IP エイリアス (複数の IP アドレスの構成) は許可されません。この機能により、1 つの NIC ポート上の複数のネットワークセグメントへのアクセスを防止できます。
- UMASK 値は新しく作成されたファイルのファイル権限を判断します。新しく作成されたファイルにデフォルトでは与えられない権限を指定します。ほとんどの UNIX システムの UMASK のデフォルト値は 022 ですが、NetBackup appliance では UMASK は 077 に設定されています。
- VxOS で検出された万人書き込み可能なすべてのファイルの権限が検索されて修正されました。
- VxOS で検出されたすべての孤立した、あるいは所有者不明のファイルとディレクトリの権限が検索されて修正されました。
- ソフトウェアバージョン 3.1 以降、SMBv1 プロトコルは無効になり、SMBv2 プロトコルに置き換えられています。SMBv1 プロトコルは、`WannaCry` や `Petya` などのランサムウェア攻撃に対する脆弱性があるため、安全と見なされなくなりました。SMBv2 は、NetBackup アプライアンスでサポートされる最低限のプロトコルになりました。

NetBackup appliance の OS の主要コンポーネント

表 6-1 に、アプライアンスのオペレーティングシステム (VxOS) の主要ソフトウェアコンポーネントの一覧を示します。

表 6-1 アプライアンスバージョン 3.1.1 の VxOS に含まれる主要ソフトウェアコンポーネント

ソフトウェアコンポーネント	バージョン
Red Hat Enterprise Linux（RHEL）	7.4
Veritas InfoScale	**メモ:** Veritas InfoScale のインストールが変更されて、アプライアンスで最大限のパフォーマンスを引き出すように調整されています。
SDCS (Symantec Data Center Security): Server 6.7 Advanced	6.7 HF2
Java Runtime Environment (JRE)	8u162
Apache Tomcat	8.0.48
RabbitMQ	3.6.8
MongoDB	3.2.9
Intel IPMI Utils	2.9.5-1

NetBackup appliance の脆弱性スキャン

Veritas 社は、業界に認められた脆弱性スキャナで NetBackup appliance を定期的にテストしています。アプライアンスのセキュリティの脅威となる新しい脆弱性は、定期的なソフトウェアリリースの際にパッチが適用されます。 重大度の高い脆弱性については、Veritas は、セキュリティの脅威の危険性に早急に対処するために、Emergency Engineering Binary（EEB）でパッチを提供します。表 6-2 に、このリリースで使われたソフトウェア製品の一覧を示します。

表 6-2 ソフトウェアスキャンソフトウェアとバージョン

セキュリティスキャナ	バージョン
Nessus™	6.10.5 (ビルド #90)
QualysGuard™	9.9.13-1
Trustwave App Scanner™	OWASP ZAP 2.6.0

7

データセキュリティ

この章では以下の項目について説明しています。

データセキュリティについて

NetBackup appliance は、NetBackup サーバーと同様にクライアント上のデータを保護するためにポリシーに基づいたメカニズムをサポートします。データの漏えいを回避し、保護を強化することによってデータセキュリティを向上させるため、次の手段が実装されています。

- リアルタイムの侵入防止メカニズムが、NetBackup appliance に格納されている機密データへのアクセスを監査するために設置されています。
- すべてのリストアをログに記録し、リアルタイムに追跡します。
- バックアップデータへのアクセスは、アプライアンスユーザーと処理に対してのみ認可されています。
- バックアップの発生時に、重複排除プール（MSDP）のすべてのバックアップデータが巡回冗長検査（CRC）のデジタル署名（CRC）でマーク付けされていることを NetBackup appliance が確認します。メンテナンスタスクが連続的に CRC のデジタル署名を再計算して元の署名と比較し、重複排除プールに不要な改ざんまたは破損があるかどうかを検知します。
- アプライアンスストレージへの意図しないアクセスを、アプライアンスへのログインを保護するパスワードによって回避します。

- 権限があるユーザーのみに限定される共有データとNetBackup 処理にアクセスします。
- HTTPS プロトコルとポート 443 を使って Veritas AutoSupport サーバーに接続し、コールホーム機能を使ってハードウェアとソフトウェアの情報をアップロードします。ベリタスのテクニカルサポートは、報告された問題を解決するためにこの情報を使います。この情報は 90 日間保持され、ベリタスのセキュアオペレーションセンターでパージされます。
- ある時点までシステム全体を容易にロールバックできる「チェックポイント」をサポートしています。この機能により、誤った構成を元に戻すことができます。チェックポイントは次のコンポーネントを取得します。
  - アプライアンスのオペレーティングシステム
  - アプライアンスのソフトウェア
  - NetBackup ソフトウェア
  - マスターサーバーのテープメディアの構成
  - ネットワーク構成
  - LDAP の構成（存在する場合）
  - ファイバーチャネルの構成
  - 前回適用したパッチすべて

メモ: NetBackup カタログや KMS データベースのような重要なコンポーネントは、構成の追加が必要な場合もあります。

NetBackup appliance ソフトウェアには、HTTP (Web サービス)プロトコルでない場合、組み込み伝送 / セッションはありません。アプライアンスのソフトウェアが信頼できないネットワーク環境で実行されている場合、NetBackup ホスト間に IPSec のような VPN (仮想プライベートネットワーク) ソリューションを配備することをお勧めします。

データ整合性について

NetBackup appliance の重複排除プールのストレージは、正常なデータのリストアが確実に行われるように、次のデータ整合性チェックを提供しています。

重複排除プールに格納されているバックアップデータの連続的なエンドツーエンド検証

データ破損が発生する可能性のある不注意なデータ変更でも、可能な場合は、自動的に検出されて修正されます。 修復不能なデータ破損の問題は、NetBackup コンソールのディスクレポート UI（[NetBackup 管理コンソール (NetBackup Administration

Console)] > [レポート (Reports)] > [ディスクのレポート (Disk Reports)]）によって、ストレージ管理者に報告されます。

重複排除プールに格納されているバックアップデータの連続的な巡回冗長検査（CRC）検証

CRC 値は、重複排除プールのバックアップジョブのために作成される各オブジェクトについて計算されます。バックグラウンド処理で連続的に CRC 署名を検証することで、バックアップデータの改ざんを防ぎ、必要な場合に正常にリストアできるようにします。重複排除プールの設計では、破損が重複排除プール全体に広がらないようにするため、プールの破損していない部分からデータ破損を隔離します。

データの分類について

データの分類は、一連のバックアップ要件を表します。これにより、要件の異なるデータのバックアップ構成が容易になります。たとえば、ゴールドの分類のバックアップはゴールドのデータの分類のストレージライフサイクルポリシーに移動する必要があります。NetBackup appliance は、NetBackup と同じデータの分類の属性をサポートします。

NetBackup データの分類の属性は、バックアップを格納するストレージライフサイクルポリシーの分類を指定します。たとえば、ゴールド分類のバックアップはゴールドのデータの分類のストレージユニットに移動する必要があります。

NetBackup は次のデフォルトのデータの分類を提供します。

- プラチナ
- ゴールド
- シルバー
- ブロンズ

この属性はオプションで、バックアップがストレージライフサイクルポリシーに書き込まれる場合のみ適用されます。リストに[データの分類なし (No data classification)]が表示されている場合、ポリシーは[ポリシーストレージ (Policy storage)]リストに表示されるストレージの選択を使用します。データの分類が選択されている場合、ポリシーが作成するすべてのイメージは分類 ID でタグ付けされます。

データの暗号化について

NetBackup appliance は、次の暗号化の方式を提供し、格納中と送信中の両方のデータを保護します。

- セキュアトンネルを使って暗号化形式でデータを転送します。これらの構成はクライアント側の暗号化や複製によっても行うことができます。これらのオプションを使わない

場合、データがアプライアンスから送信された後は、送信中のデータを保護するためにネットワークインフラストラクチャが使われます。

- NetBackup appliance バージョン 3.0 (NetBackup バージョン 8.0) より、MSDP は AES 暗号化を提供します。暗号化された MSDP を使う環境では、新たな受信データは 128 ビット (デフォルト) または 256 ビットの AES を使って暗号化されます。詳しくは、次の NetBackup のマニュアルを参照してください。
  『Veritas NetBackup 重複排除ガイド』
  『Veritas NetBackup セキュリティおよび暗号化ガイド』
- NetBackup Enterprise Server 7.1 に統合されている NetBackup の KMS (Key Management Service) を使った暗号化をサポートします。p.71 の「KMS サポート」を参照してください。

KMS サポート

NetBackup appliance は、NetBackup Enterprise Server 7.1 に統合されている NetBackup の KMS (Key Management Service) によって管理される暗号化をサポートします。アプライアンスのバージョン 2.6 以降では、KMS はマスターサーバーまたはメディアサーバーのアプライアンスでサポートされます。データ暗号化キーを再生成することは、アプライアンスのマスターサーバーで KMS をリカバリする場合にサポートされている唯一の方法です。

次に、KMS の主な機能について説明します。

- 追加のライセンスは必要ありません。
- マスターサーバーベースの対称キー管理サービスです。
- テープデバイスがそれまたは別の NetBackup appliance に接続されているマスターサーバーとして管理できます。
- T10 基準 (LTO4 や LTO5 など) に準拠しているテープドライブの対称暗号化キーを管理します。
- ボリュームプールベースのテープ暗号化を使うように設計されています。
- 組み込みのハードウェア暗号化機能のあるテープハードウェアによって使うことができます。
- NetBackup CLI 管理者が NetBackup Appliance Shell Menuまたは KMS コマンドラインインターフェース (CLI) を使って管理できます。

メモ: 2.6 以前のバージョンのアプライアンスでは、KMS はアプライアンスがメディアサーバーとして構成されている場合のみサポートされます。アプライアンスに接続されているデバイスで KMS を管理するには、非アプライアンスマスターサーバーが必要です。

KMS で使われるキーについて

KMS はパスコードからキーを生成するか、キーを自動生成します。表 7-1 に、キーに関する情報を保持する、関連付けられている KMS ファイルの一覧を示します。

表 7-1 KMS ファイル

KMS ファイル	説明	場所
キーファイルまたはキーデータベース	このファイルにはデータ暗号化キーが含まれるので、KMS にとって重要です。	/usr/openv/kms/db/KMS_DATA.dat
ホストマスターキー	このファイルには、AES 256 を使って KMS_DATA.dat キーファイルを暗号化して保護する暗号化キーが含まれます。	/usr/openv/kms/key/KMS_HMKF.dat
キー保護キー	この暗号化キーは、AES 256 を使って KMS_DATA.dat キーファイルの個別のレコードを暗号化して保護します。現時点では、すべてのレコードを暗号化するために同じ保護キーが使われています。	/usr/openv/kms/key/KMS_KPKF.dat

KMS の構成

アプライアンスで KMS を構成して有効にするには、次の手順を使用します。手順を実行するには、アプライアンスに NetBackupCLI ユーザーとしてログインする必要があります。

アプライアンスで KMS を構成して有効にするには

1. NetBackupCLI ユーザーとしてアプライアンスにログインします。
2. 次のように nbkms コマンドを使用して空のデータベースを作成します。

```
[nbcli@myappliance~]# nbkms -createemptydb
```

3. nbkms を開始します。次に例を示します。

```
[nbcli@myappliance~]# nbkms
```

4. キーグループを作成します。次に例を示します。

```
[nbcli@myappliance~]# nbkmsutil -createkg -kgname test_keygroup
```

5. アクティブなキーを作成します。次に例を示します。

```
[nbcli@myappliance~]# nbkmsutil -createkey -kgname test_keygroup
-keyname test_key
```

8

Web セキュリティ

この章では以下の項目について説明しています。

SSL の使用について

SSL (Secure Socket Layer) プロトコルは、アプライアンスの Web サーバーと Web コンソール、およびその他のローカルサーバー間の接続を暗号化します。この接続の種類では、盗聴、データ改ざん、メッセージの偽造という問題を発生させることなく情報を安全に転送できます。アプライアンスの Web サーバーで SSL を有効にするには、アプライアンスホストを識別する SSL 証明書が必要です。

アプライアンスは、クライアントとホストの検証に自己署名証明書を使用します。SHA256 アルゴリズムでハッシュ化され、RSA 暗号化を使用して署名された 2048 ビット RSA 公開鍵を使用してアプライアンス証明書が生成されます。セキュリティで保護された通信では、アプライアンスは TLS バージョン 1.2 以降のプロトコルのみを使用します。

メモ: デフォルトの自己署名証明書をカスタム CA が発行した証明書に置き換えると、[SSL 証明書は信頼できません (SSL Certificate Cannot be Trusted)]、[SSL 自己署名証明書 (SSL Self-Signed Certificate)]などの警告が表示されないようにすることができます。

SSL 証明書により、アプライアンスと LDAP や Syslog などのさまざまな外部サーバー間の通信もセキュリティで保護できます。

サードパーティの証明書

Web サービスサポート用にサードパーティの証明書を手動で追加して実装できます。証明書は SSL 暗号化と認証で使用されます。

作成したサードパーティの証明書を実装するには、次のトピックを参照してください。

p.74 の「サードパーティの SSL 証明書の実装」を参照してください。

サードパーティの SSL 証明書の実装

Web サービスサポート用にサードパーティの証明書を手動で追加して実装できます。アプライアンスはセキュリティ証明書のリポジトリとして Java KeyStore を使用します。Java KeyStore (JKS) はセキュリティ証明書のリポジトリで、たとえば、SSL 暗号化のインスタンスに使用される認可証明書または公開鍵証明書のようなものです。サードパーティの証明書をアプライアンスに実行するには、ルートアカウントでログインする必要があります。

メモ: この手順についてサポートが必要な場合は、ベリタステクニカルサポートに問い合わせてください。

サードパーティの SSL 証明書を実装するには:

1 Web サービスのための KeyStore ファイルを準備します。

手順は使用する PKCS (公開鍵の暗号化標準) の種類によって異なります。また、選択する PKCS の種類にかかわらず、KeyStore ファイルは次のキーワードを含む必要があります。

SubjectAlternativeName [

DNSName: ホスト名と IP アドレス

*ホスト名*はアプライアンスの完全修飾ドメイン名であり、*IP アドレス*はアプライアンスの完全修飾ドメイン名に対応します。

]

次の表に、PKCS# 7 および PKCS# 12 標準形式を使用する場合の手順を示します。

PKCS の形式	KeyStore ファイルの準備
PKCS#7 または X.509 形式	次のリンクを使用できます。 証明書の変換

PKCS の形式

PKCS#12 形式

KeyStore ファイルの準備

PKCS の形式

KeyStore ファイルの準備

次の手順を実行します。

- PEM 形式の x509 証明書と秘密鍵を PKCS# 12 に変換するには、次のコマンドを入力します。

  ```
  openssl pkcs12 -export -in
  server.crt -inkey server.key
  -out server.p12 -name tomcat
  -CAfile ca.crt -caname root
  ```

  openssl の使用方法について詳しくは、https://www.openssl.org/ を参照してください。

  メモ: PKCS #12 ファイルをパスワードで保護していることを確認してください。ファイルにパスワードを適用しないと、ファイルをインポートするときに NULL 参照例外が発生する可能性があります。

- pkcs12 ファイルを Java KeyStore に変換するには、次のコマンドを入力します。

  ```
  keytool -importkeystore
  -deststorepass appliance
  -destkeypass appliance
  -destkeystore keystore
  -srckeystore server.p12
  -srcstoretype PKCS12
  -srcstorepass some- password
  -alias tomcat
  ```

  メモ: -deststorepass オプションと -destkeypass オプションには、同じパスワードを指定します。異なるパスワードを指定すると、Web サーバーの起動時に例外が発生する可能性があります。パスワードでは、英数字のみがサポートされます。デフォルトのパスワードは *appliance* です。

  -alias オプションには tomcat を指定します。異なるパスワードを指定すると、Web サーバーの起動時に例外が発生する可能性があります。

  メモ: keytool の使用方法について詳しくは、次のリンクを参照してください。

PKCS の形式 **KeyStore ファイルの準備**

http://docs.oracle.com/javase/8/docs/technotes/tools/unix/keytool.html

2 データベースと関連するサービスをシャットダウンするには、次のコマンドを入力します。

```
/opt/IMAppliance/scripts/infraservices.sh database stop

systemctl stop nginx

/opt/IMAppliance/scripts/infraservices.sh database stop

/opt/IMAppliance/scripts/infraservices.sh webserver stop
```

3 既存の keystore ファイルを次のディレクトリにある新しい keystore ファイルに置き換えます。

```
/opt/apache-tomcat/security/
```

4 新しい keystore ファイルに以下のアクセス権を設定します。

```
chmod 700 /opt/apache-tomcat/security

chmod 600 /opt/apache-tomcat/security/keystore

chown -R tomcat:tomcat /opt/apache-tomcat/security
```

5 前の手順で、デフォルト以外の独自のパスワードを使用するように選択した場合は、次のコマンドを入力して Web サーバーの設定を更新します。

```
/opt/apache-tomcat/vrts/scripts/tomcat_instance.py update
--keystore --password <your password>
```

6 `/etc/rc.d/init.d/as-functions` ファイルで Tomcat_Keystore と Tomcat_Keystore_Passwd の設定を更新します。

7 証明書を `mongo_server_part_pam` ファイルにインポートして `/etc/vxos-ssl/cert.conf` から `server_cert` を取得し、証明書をインポートします。

```
/usr/bin/openssl pkcs12 -in server.p12 -out <server_cert> -passin
pass:

<keyPassword> -passout pass: <keyPassword>
```

8 証明書を client_part_pam ファイルにインポートして、/etc/vxos-ssl/cert.conf から client_cert を取得し、証明書をインポートします。

```
/usr/bin/openssl pkcs12 -nokeys -in server.p12 -out <server_cert>
-passin pass:

<keyPassword> -passout pass: <keyPassword>
```

9 カスタマイズしたパスワードが /etc/vxos-ssl/cert.conf の pem_password と異なる場合は、カスタマイズしたパスワードを使用するように /etc/vxos-ssl/cert.conf を変更します。

10 nginx を再起動するには、次のコマンドを入力します。

```
/usr/sbin/update-nginx-conf.sh

service nginx stop

service nginx start
```

11 Web サービスを再起動するには、次のコマンドを入力します。

```
/opt/IMAppliance/scripts/infraservices.sh database start

/opt/IMAppliance/scripts/infraservices.sh webserver start
```

12 AutoSupport サービスを再起動するには、次のコマンドを入力します。

```
service as-alertmanager stop

service as-analyzer stop

service as-transmission stop

service as-alertmanager start

service as-analyzer start

service as-transmission start
```

9

ネットワークセキュリティ

この章では以下の項目について説明しています。

IPsec チャネル設定について

NetBackup appliance は、IPsec チャネルを使用して、2 つのアプライアンス間の通信を保護します。これは、送信中のデータの保護に役立ちます。NetBackup マスターサーバーのような NetBackup appliance と非アプライアンス間の他のすべての通信は非 IPsec です。

IPsec セキュリティは IP レベルで動作し、2 つのホスト間の IP トラフィックのセキュリティ保護を許可します。デバイス証明書はマスターアプライアンスやメディアアプライアンスにプロビジョニングされ、これらの証明書は IPsec チャネルを構成するために有効になります。これはマスターサーバーとメディアサーバーの安全な対話を有効にします。使用されるデバイス証明書は Verisign CA によって発行される x509 証明書です。

アプライアンスは IPsec チャネルを確立する前に次の検証チェックを実行します。

- x509 証明書を使用して証明書の権限を検証します。
- デバイス証明書が IP に対応しているかどうかを検証します。
- 通信の両方向のセキュリティアソシエーションを検証し、更新します。

ホストはデバイスの証明書が認識された後に検出されます。この後にのみ、IPsec チャネルは構成され、有効になります。

IPsec 構成の管理

IPsec チャネルを管理するため、NetBackup Appliance Shell Menuから次のコマンドを使用できます。

表 9-1 IPsec コマンド

コマンド	説明
`Network > Security > Configure`	このコマンドを使って任意の 2 ホスト間の IPsec を設定できます。ホストはホスト名を使って定義できます。また、ユーザー ID とパスワードによってそれらを識別できます。
`Network > Security > Delete`	このコマンドを使ってローカルシステム上にあるリモートホストリストの IPsec ポリシーを削除できます。このコマンドを使ってローカルシステム上にあるリモートホストリストの IPsec ポリシーを削除できます。ローカルシステム上にあるリモートホストリストの IPsec ポリシーを削除します。Hosts 変数を使って 1 つ以上のホスト名を定義します。カンマを使って複数のホスト名を区切ります。
`Network > Security > Export`	このコマンドを使って IPsec クレデンシャルをエクスポートします。*`EnterPasswd`* **フィールドは、[パスワードを入力しますか**`? (Do you want to enter a password?)`**]という質問への回答に使います。**. このフィールドには yes または no の値を入力する必要があります。また、エクスポートしたクレデンシャルを置く場所を定義するパスを指定する必要があります。 **メモ:** IPsec クレデンシャルは再イメージング処理中に削除されます。クレデンシャルはアプライアンスごとに一意であり、元の工場出荷時イメージの一部として含まれています。IPsec クレデンシャルは、アプライアンスの再イメージングに使われる USB ドライブには含まれていません。
`Network > Security > Import`	このコマンドを使って IPsec クレデンシャルをインポートします。 `EnterPasswd` フィールドは、[パスワードを入力しますか? (Do you want to enter a password?)]という質問への回答に使います。.このフィールドには yes または no の値を入力する必要があります。また、インポートしたクレデンシャルを置く場所を定義するパスを指定する必要があります。
`Network > Security > Provision`	このコマンドを使ってローカルシステム上にあるリモートホストリストの IPsec ポリシーをプロビジョニングします。*`Hosts`* **変数を使って** `1` **つ以上のホスト名を定義します。**カンマを使って複数のホスト名を区切ります。
`Network > Security (IPsec) > Refresh`	このコマンドを使って IPsec の構成を再ロードします。`[Auto]` オプションですべての参照されるホスト上の構成を更新するかどうかを定義します。`[Auto]` または `[NoAuto]` **を入力できます。**デフォルト値は `[NoAuto]` です。

コマンド	説明
`Network > Security > Show`	ローカルホストまたは提供されたホストの IPsec ポリシーを表示します。`[[Verbose]]` オプションは、出力を詳細に行うかどうかを定義するために使用します。このフィールドで入力できる値は `[VERBOSE]` または `[NoVERBOSE]` **です。**デフォルト値は `[NoVERBOSE]` です。`[[HostInfo]]` **オプションには、次の情報をカンマで区切って含めることができます。**ホスト名、ユーザー ID (省略可能)、パスワード (省略可能) の情報をカンマで区切って含めることができます。
`Network > Security > Unconfigure`	このコマンドを使って任意の 2 ホスト間の IPsec を設定解除します。*`Host1Info`* **変数には、**ホスト名、ユーザー ID (省略可能)、パスワード (省略可能) の情報をカンマで区切って含めることができます。*`[Host2info]`* 変数にはホスト名、ユーザー ID(省略可能)、パスワード(省略可能)を含めることができます。

NetBackup Appliance Shell Menuの `Main > Network > Security` コマンドを使用して、2 つのホスト間の IPSec チャネルを構成できます。IPsec チャネル構成について詳しくは、『NetBackup Appliance コマンドリファレンスガイド』を参照してください。

NetBackup appliance ポートについて

NetBackup ソフトウェアによって使用されるポートに加えて、NetBackup アプライアンスはインバンドとアウトオブバンドの両方の管理にも対応します。帯域外の管理は別のネットワーク接続、リモート管理のモジュール(RMM)、インテリジェントプラットフォーム管理インターフェース(IPMI)によって行われます。必要に応じてファイアウォールによってこれらのポートを開き、リモートのノートパソコンや KVM(キーボード、ビデオモニタ、マウス)からの管理サービスへのアクセスを許可します。

警告: NetBackup Appliance Web Consoleは現在、デフォルトポート 443 の HTTPS のみを経由して利用可能です。HTTP を経由するポート 80 は無効です。Web コンソールにログインするには、`https://<appliance-name>`を使います。appliance-name はアプライアンスの完全修飾ドメイン名 (FQDN) で、IP アドレスになる場合もあります。

表 9-2 は、NetBackup Appliance へのインバウンド通信用に開いたポートの一覧を示します。

表 9-2 インバウンドポート

ポート	サービス	説明
22	ssh	インバンド管理 CLI
443	HTTPS	インバンド管理 GUI
5900	KVM	CLI アクセス、ISO、CD-ROM リダイレクト
623	KVM	(開いた場合に使用されるオプション)
2049	NFS	NFS
445		CIFS(ログ / 共有をインストール)

+ NetBackup 統合型ストレージマネージャ

*ベリタスリモート管理 – リモートコンソール

表 9-3 に、アプライアンスのアウトバウンドポートを示します。これらのポートは、対象サーバーへの警告や通知の送信を許可します。

表 9-3 送信ポート

ポート	サービス	説明
443	HTTPS	ベリタスへのコールホーム通知 SDCS 証明書のダウンロード
162**	SNMP	アプライアンスの更新のダウンロード
22	SFTP	ベリタスへのログのアップロード
25	SMTP	電子メール警告
389	LDAP	
636	LDAPS	
514	rsyslog	ログ転送

** このポート番号は、リモートサーバーと一致するように、アプライアンス構成内で変更できます。

表 9-4 に、NetBackup Appliance の Out of Band Management ポートを示します。

表 9-4 Out of Band Management ポート

80	HTTP	帯域外の管理（ISM+ または RM*）
443	HTTP	帯域外の管理（ISM+ または RM*）
5900	KVM	CLI アクセス、ISO、CD-ROM リダイレクト
623	KVM	（開いた場合に使用されるオプション）
7578	RMM	CLI アクセス
5120	RMM	ISO と CD-ROM リダイレクト
5123	RMM	フロッピーリダイレクト
7582	RMM	KVM
5124	HTTPS	CD-ROM
5127		USB またはフロッピー
2049	NFS	NFS
445		CIFS（ログ / 共有をインストール）

+ NetBackup 統合型ストレージマネージャ

*ベリタスリモート管理 – リモートコンソール

メモ: ポート 7578、5120、5123 は非暗号化モード用です。ポート 7582、5124、5127 は暗号化モード用です。

適用可能なすべてのポートの一覧は、『NetBackup ネットワークポートリファレンスガイド』で参照できます。

10

コールホームセキュリティ

この章では以下の項目について説明しています。

AutoSupport について

AutoSupport 機能を使うと、Veritasサポート Web サイトでアプライアンスと連絡先の詳細を登録できます。ベリタスのサポートは、報告された問題を解決するためにこの情報を使います。この情報によって、ベリタスは停止時間を最小化し、サポートにプロアクティブなアプローチを提供することが可能になります。

マイアプライアンスポータルは、アプライアンスの登録と登録情報の編集を行う統合ポータルです。

サポートインフラは、ベリタスのサポートが次の方法でサポートできるように設計されています。

- プロアクティブな監視により、ベリタスは自動的にケースを作成し、問題を解決し、リスクを伴う可能性のあるアプライアンスの部品を発送します。
- Veritas内の AutoSupport インフラは、アプライアンスからの Call Home データを分析します。この分析はハードウェア障害に対してプロアクティブなテクニカルサポートを提供するため、バックアップ管理者がサポートケースを開始する必要性が減少します。
- AutoSupport 機能により、ベリタスのサポートは、お客様がアプライアンスを構成して使う方法と、機能強化のメリットが最もあるところを把握できるようになります。
- アプライアンスの状態とアラート通知を送受信します。
- Call Home を使ってハードウェアとソフトウェアの状態を受信します。

- 問題に対してより多くの洞察を提供し、既存の問題の結果としてさらに発生する可能性のある問題を特定します。
- コールホームデータからのレポートを表示して、ハードウェア障害のパターンを分析し、使用状況の傾向を確認します。アプライアンスは 30 分ごとに健全性データを送信します。

アプライアンス登録のために提供された情報は、ベリタスのサポートが報告された問題の解決を開始するのに役立ちます。ただし、二次連絡先、電話番号、ラックの場所などの追加の詳細を提供する場合は、https://my.veritas.com にアクセスしてください。

データセキュリティ基準

アプライアンスからベリタスに伝送するすべてのデータは、業界標準の高度な暗号化方式を使用して伝送されます。クライアントとサーバー間で送信するすべての AutoSupport データと、クライアント内のさまざまなコンポーネント間のデータ通信に、以下のデータセキュリティ基準を適用します。

- RSA 2048 ビットキー (サーバー認証用)
- AES 128/256 ビットキー (データ暗号化用)
- SHA1、SHA2 (256/384 ビット) ハッシュ (メッセージ認証用)

コールホームについて

アプライアンスでは、Veritas AutoSupport コールホームサーバーに接続し、ハードウェアとソフトウェアの情報をアップロードできます。ベリタスのサポートは、報告された問題を解決するためにこの情報を使います。アプライアンスは HTTPS プロトコルとポート 443 を使って、Veritas AutoSupport サーバーに接続します。アプライアンスのこの機能をコールホームと呼びます。この機能はデフォルトで有効です。

アプライアンスの AutoSupport は、コールホームにより収集されたデータを使って、アプライアンスのプロアクティブな監視機能を提供します。コールホームが有効な場合、アプライアンスはデフォルトで 24 時間間隔で定期的に Veritas AutoSupport サーバーに情報 (コールホームデータ) をアップロードします。

アプライアンスに問題があると判断した場合は、Veritasサポートに問い合わせてください。テクニカルサポート技術者は、アプライアンスのシリアル番号を使用してコールホームデータから状態を評価します。

NetBackup Appliance Web Consoleからアプライアンスのシリアル番号を確認するには、[監視 (Monitor)]>[ハードウェア (Hardware)]>[健全性の詳細 (Health details)] ページに移動します。シェルメニューを使ってアプライアンスのシリアル番号を確認するには、`Monitor > Hardware` コマンドを使います。`Monitor > Hardware` コマンドについて詳しくは、『NetBackup Appliance コマンドリファレンスガイド』を参照してください。

[設定 (Settings)]>[通知 (Notification)]メニューを使って、NetBackup Appliance Web Consoleからコールホームを構成します。[警告の構成 (Alert Configuration)]をクリックし、[コールホームの構成 (Call Home Configuration)]ペインで詳細を入力します。

表 10-1 では、本機能が有効または無効な場合、障害がどのように報告されるかを説明します。

表 10-1　　コールホームが有効または無効な場合の処理

監視状態	障害ルーチン
コールホーム有効時	障害が発生すると、以下の警告シーケンスが発生します。 ■ アプライアンスは、すべての監視されているハードウェアとソフトウェアの情報を Veritas AutoSupport サーバーにアップロードします。表の後に続くリストにすべての関連情報が含まれます。 ■ アプライアンスは、設定した電子メールアドレス宛てに次の 3 種類の電子メールアラートを生成します。 　■ エラーが検出されたときに電子メールでエラーを通知するエラーメッセージ。 　■ エラーが解決されると障害について通知する電子メールの解決メッセージ。 　■ 直近の 24 時間以内に発生した現在未解決のすべてのエラーを要約した、電子メール別の 24 時間の概略。 ■ アプライアンスは SNMP トラップも生成します。
コールホーム無効時	データを Veritas AutoSupport サーバーに送信しません。システムは Veritas にエラーを報告しないので問題をより早く解決できます。

次のリストは分析のために Veritas AutoSupport サーバーに監視され、送信されるすべての情報を含んでいます。

- CPU
- ディスク
- ファン
- 電源
- RAID グループ
- 温度
- アダプタ
- PCI
- ファイバーチャネル HBA

- ネットワークカード
- パーティション情報
- MSDP 統計
- ストレージの接続
- ストレージの状態
- 52xx ストレージシェルフ - ディスク、ファン、電源、温度の状態
- 53xx プライマリストレージシェルフ - ディスク、ファン、電源、温度、バッテリバックアップ装置 (BBU)、コントローラ、ボリューム、ボリュームグループの状態
- 53xx 拡張ストレージシェルフ - ディスク、ファン、電源、温度の状態
- NetBackup appliance ソフトウェアのバージョン
- NetBackup のバージョン
- アプライアンスモデル
- アプライアンスの構成
- ファームウェアのバージョン
- アプライアンス、ストレージ、およびハードウェアコンポーネントのシリアル番号

p.87 の「NetBackup Appliance Shell Menuからのコールホームの構成」を参照してください。

p.84 の「AutoSupport について 」を参照してください。

NetBackup Appliance Shell Menuからのコールホームの構成

[設定 (Settings)]>[通知 (Notification)]ページから、コールホームの詳細を構成できます。

NetBackup Appliance Shell Menuから、次のコールホームの設定を構成できます。

- 「アプライアンスシェルメニューからのコールホームの有効化と無効化」
- 「NetBackup Appliance Shell Menuからのコールホームプロキシサーバーの構成」
- `Settings > Alerts > CallHome > Test` コマンドの実行によってコールホームが正しく動作しているかどうかのテスト

`Main > Settings > Alerts > CallHome` コマンドについて詳しくは、『NetBackup Appliance コマンドリファレンスガイド』を参照してください。

警告を引き起こすハードウェア問題のリストについては、次のトピックを参照してください。

p.85 の「コールホームについて」を参照してください。

アプライアンスシェルメニューからのコールホームの有効化と無効化

NetBackup Appliance Shell Menuと Access 3340 Appliance シェルメニューからコールホームを有効または無効にすることができます。コールホームはデフォルトでは有効です。

シェルメニューからコールホームを有効または無効にするには

1. シェルメニューにログオンします。
2. コールホームを有効にするには、`Main > Settings > Alerts > CallHome Enable` コマンドを実行します。
3. コールホームを無効にするには、`Main > Settings > Alerts > CallHome Disable` コマンドを実行します。

`Main > Settings > Alerts > CallHome` コマンドについて詳しくは、『NetBackup Appliance コマンドリファレンスガイド』または『Access 3340 Appliance スタートガイド』を参照してください。

NetBackup Appliance Shell Menuからのコールホームプロキシサーバーの構成

必要に応じて、コールホームのためのプロキシサーバーを構成できます。アプライアンス環境と外部インターネットアクセス間にプロキシサーバーが存在する場合、アプライアンスのプロキシ設定を有効にする必要があります。プロキシ設定には、プロキシサーバーとポートの両方が含まれています。プロキシサーバーは、ベリタスの AutoSupport サーバーからの https 接続を受け入れる必要があります。この機能はデフォルトでは無効です。

NetBackup Appliance Shell Menuからコールホームプロキシサーバーを構成する方法

1. NetBackup Appliance Shell Menuにログオンします。
2. プロキシ設定を有効にするには、`Main > Settings > Alerts > CallHome Proxy Enable` コマンドを実行します。
3. プロキシサーバーを追加するには、`Main > Settings > Alerts > CallHome Proxy Add` コマンドを実行します。
   - プロキシサーバーの名前を入力するように求められます。プロキシサーバーの名前はプロキシサーバーの TCP/IP アドレスまたは完全修飾ドメイン名です。
   - プロキシサーバーの名前を入力した後、プロキシサーバーのポート番号を入力するように求められます。
   - さらに、次の質問に答える必要があります。

     ```
     Do you want to set credentials for proxy server? (yes/no)
     ```

- *yes* と答えると、プロキシサーバーのユーザー名を入力するように求められます。
- ユーザー名を入力した後、ユーザーのパスワードを入力するように求められます。必要な情報を入力すると、次のメッセージが表示されます。

```
Successfully set proxy server
```

4 プロキシ設定を無効にするには、`Main > Settings > Alerts > CallHome Proxy Disable` コマンドを実行します。

さらに、NetBackup Appliance Shell Menuを使って、アプライアンスのプロキシサーバートンネリングの有効と無効を切り替えることもできます。そのためには、`Main > Settings > CallHome Proxy EnableTunnel` と `Main > Settings > Alerts > CallHome Proxy DisableTunnel` コマンドを実行します。プロキシサーバートンネリングを使うと、信頼できないネットワークを通して安全なパスを提供できます。

コールホームワークフローの理解

このセクションでは、アプライアンスから Veritas AutoSupport サーバーにデータをアップロードするためにコールホームが使うメカニズムについて説明します。

コールホームは、Veritas AutoSupport サーバーとのすべての通信で HTTPS（暗号化された安全なプロトコル）とポート番号 443 を使います。コールホームが正しく働くには、アプライアンスがインターネットに直接またはプロキシサーバーを経由してアクセスし、Veritas AutoSupport サーバーに到達する必要があります。アプライアンスをプロアクティブに監視するメカニズムである AutoSupport は、コールホームのデータを使って、アプライアンスで発生する可能性のある問題を分析して解決します。

すべての通信はアプライアンスによって開始されます。アプライアンスは、https://receiver.appliance.veritas.com にアクセスする必要があります。

アプライアンスのコールホーム機能は以下のワークフローを使って、AutoSupport サーバーと通信します。

- https://receiver.appliance.veritas.com のポートに 24 時間ごとにアクセスします。
- https://receiver.appliance.veritas.com に対してセルフテスト操作を実行します。
- アプライアンスでエラー状態が発生した場合は、現在のログと過去 3 日間のすべてのログが収集されます。
- 次に、ログは詳しい分析とサポートのために Veritas AutoSupport サーバーにアップロードされます。これらのエラーログはアプライアンスでも格納されます。`/log/upload/<date>` フォルダからこれらのログにアクセスできます。
- エラー状態が 3 日後も発生した場合は、ログが再アップロードされます。

p.85 の「コールホームについて」を参照してください。

p.84 の「AutoSupport について 」を参照してください。

SNMP について

SNMP は、ネットワークデバイス間における管理情報の交換を支援するアプリケーション層プロトコルです。構成に応じて、伝送制御プロトコル（TCP）またはユーザーデータグラムプロトコル（UDP）を使います。ネットワーク管理者は、SNMP を使うことで、ネットワークパフォーマンスの管理、ネットワーク上の問題の検出と解決、ネットワーク拡張の計画を実行できます。

SNMP はマネージャモデルとエージェントモデルに基づいています。このモデルは、マネージャ、エージェント、管理情報データベース、管理対象オブジェクト、ネットワークプロトコルで構成されています。

マネージャは、ネットワーク管理者と管理システム間のインターフェースを提供します。エージェントは、マネージャと管理対象の物理デバイス間のインターフェースを提供します。

マネージャとエージェントは、MIB (Management Information Base) と、比較的数の少ないコマンドセットを使って情報を交換します。MIB は、状態や説明といった個々の変数を枝の葉として表現するツリー構造で編成されています。数値タグまたはオブジェクト識別子 (OID) によって、MIB と SNMP メッセージの各変数が一意に識別されます。

MIB (Management Information Base) について

SNMP の各要素は、それぞれ独自の特性を備えた特定のオブジェクトを管理します。各オブジェクトと特性には、一意のオブジェクト識別子 (OID) が関連付けられています。各 OID は、小数点によって区切られた数字 (1.3.6.1.4.1.48328.1 など) で構成されています。

これらの OID はツリーを形成します。MIB は、読み取り可能なラベルと、オブジェクトに関連するさまざまなパラメータを持つ各 OID に関連付けられています。MIB は、SNMP メッセージの生成や解釈に使われるデータ辞書として機能します。この情報は MIB ファイルとして保存されます。

Web コンソールの［設定 (Settings)］>［通知 (Notification)］>［アラートの構成 (Alert Configuration)］ページから、SNMP の MIB ファイルの詳細を調べることができます。ハードウェア監視関連のトラップを受信するようにアプライアンスの SNMP マネージャを設定するには、［SNMP サーバーの構成 (SNMP Server Configuration)］ページの［SNMP の MIB ファイルを表示 (View SNMP MIB file)］をクリックします。

アプライアンスのシェルメニューで `Settings > Alerts > SNMP ShowMIB` コマンドを使用して SNMP の MIB ファイルを表示することもできます。

11

IPMI セキュリティ

この章では以下の項目について説明しています。

IPMI 設定の紹介

アプライアンス用の IPMI サブシステムを構成できます。IPMI (Intelligent Platform Management Interface) サブシステムは、予想外の停電によって接続済みのシステムが終了する場合に役立ちます。このサブシステムはオペレーティングシステムとは関係なく動作し、アプライアンスの背面パネルにあるリモート管理ポートを使って接続できます。

IPMI サブシステムとベリタスリモート管理ツールは、BIOS 設定を使って構成できます。ベリタスリモート管理ツールには、リモート管理ポートを使うためのインターフェースがあります。これにより、アプライアンスの監視と管理をリモートから実行することができます。

推奨される IPMI 設定

このセクションでは、安全な IPMI 構成を確認するために推奨される IPMI 設定の一覧を示します。

ユーザー

IPMI ユーザーを作成する場合は、次の推奨事項を使用します。

- Null ユーザー名またはパスワードでアカウントを作成しないでください。
- 管理ユーザーの数を 1 人に制限します。
- 匿名ユーザーを無効にします。

- CVE-2013-4786 の脆弱性を緩和するには
  - オフライン辞書攻撃および総当り攻撃を防止するには強いパスワードを使用します。推奨されるパスワードの長さは 16 ~ 20 文字です。
  - できるだけ早期にデフォルトのユーザーパスワード (sysadmin) を変更します。
  - アクセス制御リスト (ACL) または隔離ネットワークを使って IPMI インターフェースへのアクセスを制限します。

ログイン

IPMI ユーザーにログイン設定を適用する場合は、次の推奨事項を使用します。

表 11-1 ログインセキュリティ設定

設定	推奨される値
ログイン試行に失敗しました	3
ユーザーのロックアウト時間（最短）	60 秒
強制 HTTPS	可 IPMI 接続が常に HTTPS を使用して行われるように[強制 HTTPS (Force HTTPS)]を有効にします。
Web セッションタイムアウト	1800

LDAP 設定

LDAP 認証を有効にすることを推奨します。

SSL アップロード

新規またはカスタム SSL 証明書をインポートすることを推奨します。

リモートセッション

表 11-2 リモートセッションのセキュリティ設定

設定	推奨される値
KVM 暗号化	AES
メディア 暗号化	有効

暗号化の推奨事項

IPMI ユーザーの認証なしの処理またはアクティビティを防止するには、特定の暗号化を無効にする必要があります。詳しい説明が必要な場合は、テクニカルサポートに連絡して、担当者に記事番号 000127964 について問い合わせます。

イーサネット接続設定

IPMI 専用のイーサネット接続を使用し、物理サーバー接続を共有しないようにします。

- 固定 IP を使用してください。
- DHCP を使用しないでください。

デフォルトの IPMI SSL 証明書の置換

IPMI Web インターフェースにアクセスするために使うデフォルトの IPMI SSL 証明書を信頼できる内部または外部の認証局 (PEM 形式)、または自己署名証明書により署名された証明書に置換することを推奨します。次の手順で、Linux コンピュータで最小限の自己署名証明書を作成して IPMI Web インターフェースにインポートできます。

Linux コンピュータに最小限の自己署名証明書を作成して IPMI Web インターフェースにインポートするには、次の操作をします。

1 次のコマンドを実行して ipmi.key と呼ばれるプライベートキーを生成します。

```
$ openssl genrsa -out ipmi.key 2048

Generating RSA private key, 2048 bit long modulus

.....+++

 .+++

 e is 65537 (0x10001)
```

2 各フィールドに適切な値を入力して次のように、ipmi.key を使って ipmi.csr という証明書の署名要求を生成します。

メモ: ブラウザに余分な警告が表示されないようにするには、CN を IPMI インターフェースの完全修飾ドメイン名に設定します。入力するのは識別名（DN）と呼ばれる名前です。

```
$ openssl req -new -key ipmi.key -out ipmi.csr
```

次のガイドラインを参照して、証明書要求に入れる情報を入力します。

国名（2 文字のコード）[AU]:	国の名前を入力します。たとえば、US。
都道府県名（省略しない）[Some-State]:	都道府県の名前を入力します。たとえば、OR。
地域名（たとえば、市区町村）[]:	地域名を入力します。たとえば、Springfield。
組織名（たとえば、会社）[Internet Widgits Pty Ltd]:	組織の名前を入力します。たとえば Veritas です。
組織単位名（たとえば、部署）[]:	組織単位の名前を入力します。
共通名（たとえば、自社名）[]:	hostname.your.company と入力します。
電子メールアドレス []:	電子メールアドレスを入力します。たとえば、email@your.company 。
チャレンジパスワード []:	適切なチャレンジパスワード（証明書要求と共に送信する追加属性）を入力します。
会社名（省略可能）[]:	適切な会社名（証明書要求と共に送信する追加属性）を入力します（省略可能）。

メモ: フィールドを空白のままにするには「.」と入力します。

3 ipmi.key で ipmi.csr に署名し、次のように 1 年間有効な ipmi.crt と呼ばれる証明書を作成します。

```
$ openssl x509 -req -in ipmi.csr

-out ipmi.crt -signkey ipmi.key

-days 365

 Signature ok

 subject=/C=US/ST=OR/L=Springfield

/O=Veritas/OU=Your OU/

CN=hostname.your.company/

emailAddress=email@your.company


Getting Private key
```

4 ipmi.crt と ipmi.key を連結して ipmi.pem と呼ばれる証明書を PEM 形式で作成します。

```
$ cat ipmi.crt ipmi.key > ipmi.pem
```

5 アプライアンスの IPMI Web インターフェースにアクセスできるホストに ipmi.pem をコピーします。

6 ベリタスリモート管理 (IPMI Web インターフェース) にログインします。

7 [設定 (Settings)] > [SSL]をクリックします。

アプライアンスに[SSL のアップロード (SSL Upload)]ページが表示されます。

8 証明書をインポートするには[SSL のアップロード (SSL Upload)]ページで[ファイルを選択 (Choose File)]をクリックします。

9 ipmi.pem を選択して[アップロード (Upload)]をクリックします。

10 SSL 証明書がすでに存在することを示す警告が表示されることがあります。続行するには[OK]をクリックします。

11 キーをインポートするには、再び[ファイルを選択 (Choose File)]をクリックします(このボタンの隣には[新しいプライバシーキー (New Privacy Key)]があります)。

12 ipmi.pem を選択して[アップロード (Upload)]をクリックします。

13 証明書とキーを正常にアップロードしたことを示す確認メッセージが表示されたら、［OK］をクリックして Web サービスを再起動します。

14 ベリタスリモート管理インターフェース (IPMI Web インターフェース) を閉じてから再び開いて、新しい証明書が存在していることを確認します。

12

STIG と FIPS への準拠

この章では以下の項目について説明しています。

NetBackup アプライアンスのための OS STIG の強化

セキュリティ技術導入ガイド (STIG) では、情報システムとソフトウェアのセキュリティを向上するための技術ガイドを提供し、悪質なコンピュータ攻撃を防ぎます。この種のセキュリティは、強化とも呼ばれます。

ソフトウェアバージョン 3.1 以降、セキュリティの向上のため、OS STIG 強化ルールを有効にすることができます。これらのルールは、DISA (Defense Information Systems Agency) からの次のプロファイルに基づいています。

Red Hat Enterprise Linux 7 Server バージョン 0.1.31 用の STIG

これらのルールを有効にするには、次のコマンドを使用します。

`Main_Menu > Settings > Security > Stig Enable` の後に、メンテナンスパスワードを入力します。

STIG の有効化については、次の注意点があります。

- オプションが有効になっていると、強制的に適用されるルールのリストが表示されます。コマンド出力にも、強制的には適用されないすべてのルールの例外が表示されます。
- このコマンドでは、個々のルールの制御は許可されません。
- 高可用性 (HA) 設定のアプライアンス (ノード) の場合、切り替え後に正しく作動するように、各ノードでこの機能を手動で有効にする必要があります。

- オプションを有効にすると、関連付けられたルールを無効にするには、出荷時設定へのリセットが必要です。
- LDAP (Lightweight Directory Access Protocol) を設定する場合は、このオプションを有効にする前に、TLS (Transport Layer Security) を使用するように設定することをお勧めします。

メモ: STIG 機能が有効になっているアプライアンスをアップグレードするか、このアプライアンスに EEB をインストールする必要がある場合、午前 4 時から午前 4 時半の間には計画しないでください。このベストプラクティスに従うと、AIDE データベースと監視対象ファイルの自動更新の中断を防ぐことができます。自動更新が中断されると、アプライアンスで複数の警告メッセージが生成される可能性があります。

このオプションを有効にした後に適用されるセキュリティ強化ルールを次に示します。各ルールは、CCE (Common Configuration Enumerator) 識別子、ルールの短い説明、SCAP (Security Content Automation Protocol) スキャナ重要度レベルによって識別されます。ソフトウェアバージョン 3.1 では、高と中のスキャナ重要度レベルでルールを扱います。

このオプションを有効にした後に適用されるルール

- CCE-27127-0: 仮想アドレス空間のランダムなレイアウトを有効にします。
  スキャナ重要度レベル: 中
- CCE-26900-1: SUID プログラムのコアダンプを無効にします。
  スキャナ重要度レベル: 低
- CCE-27050-4: カーネルメッセージバッファへのアクセスを制限します。
  スキャナ重要度レベル: 低
- CCE-80258-7: kdump カーネルクラッシュアナライザを無効にします。
  スキャナ重要度レベル: 中
- CCE-27220-3: AIDE データベースを構築してテストします。
  スキャナ重要度レベル: 中
- CCE-26952-2: AIDE の定期的な実行を構成します。
  スキャナ重要度レベル: 中
- CCE-27303-7: システムログインバナーを変更します。
  スキャナ重要度レベル: 中
- CCE-27082-7: SSH クライアントライブアカウントを設定します。
  スキャナ重要度レベル: 中
- CCE-27314-4: SSH 警告バナーを有効にします。
  スキャナ重要度レベル: 中

- CCE-27437-3: auditd が特権コマンドの使用に関する情報を収集することを確認します。
  スキャナ重要度レベル: 中
- CCE-27309: ブートローダーのパスワードを設定します。
  スキャナ重要度レベル: 高
- CCE-80374-2: AIDE スキャン結果の通知を構成します。
  スキャナセキュリティレベル: 中
- CCE-80375-9: アクセス制御リスト (ACL) を検証するよう AIDE を構成します。
  スキャナ重要度レベル: 中
- CCE-80376-7: 拡張属性を検証するよう AIDE を構成します。
  スキャナ重要度レベル: 中
- CCE-27375-5: ディスク容量が少ないときの auditd_space_left_action を構成します。
  スキャナ重要度レベル: 中
- CCE-27341-7: auditd が audispd_syslog_plugin を使うように構成します。
  スキャナセキュリティレベル: 中
- CCE-27353-2: システムの任意アクセス制御を変更するイベント (fremovexattr) を記録します。
  スキャナ重要度レベル: 中
- CCE-27410-0: システムの任意アクセス制御を変更するイベント (lremovexattr) を記録します。
  スキャナ重要度レベル: 中
- CCE-27367-2: システムの任意アクセス制御を変更するイベント (removexattr) を記録します。
  スキャナ重要度レベル: 中
- CCE-27204-7: ログオンイベントとログアウトイベントを変更しようとする試みを記録します。
  スキャナ重要度レベル: 中
- CCE-27347-4: ファイルに対する権限のないアクセスの試みを auditd が収集することを確認します。
  スキャナ重要度レベル: 中
- CCE-27447-2: auditd が成功したメディアへのエクスポートに関する情報を収集することを確認します。
  スキャナ重要度レベル: 中
- CCE-27206-2: auditd がユーザーによるファイル削除イベントを収集することを確認します。

スキャナ重要度レベル: 中

- CCE-27129-6: auditd がカーネルモジュールのロードおよびアンロードに関する情報を収集することを確認します。
  スキャナ重要度レベル: 中
- CCE-27333-4: 文字が連続する最大数のパスワードルールを設定します。
  スキャナ重要度レベル: 中
- CCE-27512-3: 同じ文字クラスからの文字が連続する最大数のパスワードルールを設定します。
  スキャナ重要度レベル: 中
- CCE-27214-6: 数字 (数値) の最小文字数のパスワード強度を設定します。
  スキャナ重要度レベル: 中
- CCE-27293-0: 最小長のパスワードルールを設定します。
  スキャナ重要度レベル: 中
- CCE-27200-5: 大文字の最小文字数のパスワード強度を設定します。
  スキャナ重要度レベル: 中
- CCE-27360-7: 特殊文字の最小文字数のパスワード強度を設定します。
  スキャナ重要度レベル: 中
- CCE-27345-8: 小文字の最小文字数のパスワード強度を設定します。
  スキャナ重要度レベル: 中
- CCE-26631-2: 使用する異なる文字の最小文字数のパスワード強度を設定します。
  スキャナ重要度レベル: 中
- CCE-27115-5: USB ストレージドライバの modprobe ロードを無効にします。
  スキャナ重要度レベル: 中
- CCE-27350-8: 失敗したパスワードの試行によってアクセスを拒否する試行回数を設定します。
  スキャナ重要度レベル: 中
- CCE-80353-6: 失敗したパスワードの試行のルートアカウントを構成します。
  スキャナ重要度レベル: 中
- CCE-26884-7: 失敗したパスワードの試行のロックアウト時間を設定します。
  スキャナ重要度レベル: 中
- CCE-27297-1: 失敗したパスワードの試行をカウントする間隔を設定します。
  スキャナ重要度レベル: 中
- CCE-27002-5: パスワードの最短寿命を設定します。
  スキャナ重要度レベル: 中
- CCE-27051-2: パスワードの最長寿命を設定します。

スキャナセキュリティレベル: 中

- CCE-27081-9: 各ユーザーに許可される同時ログインセッションの数を制限します。
  スキャナ重要度レベル: 低

常に適用されるルール

次のルールが常に適用され、無効にすることはできません。これらのルールは、「NIST Special Publication 800-123」で説明されている仕様に準拠するように強化されています。詳しくは、次の文書を参照してください。

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf

- CCE-80165-4: ICMP ブロードキャストエコー要求を無視するようにカーネルパラメータを構成します。
  スキャナ重要度レベル: 中
- CCE-80156-3: デフォルトで ICMP リダイレクトを送信するためのカーネルパラメータを無効にします。
  スキャナ重要度レベル: 中
- CCE-80156-3: すべてのインターフェースで ICMP リダイレクトを送信するためのカーネルパラメータを無効にします。
  スキャナ重要度レベル: 中
- CCE-27212-0: 監査デーモンの前に開始されるプロセスの監査を有効にします。
  スキャナ重要度レベル: 中
- CCE-26957-1: Red Hat GPG キーがインストールされていることを確認します。
  スキャナ重要度レベル: 高
- CCE-27096-7: `AIDE` パッケージがインストールされていることを確認します。
  スキャナ重要度レベル: 中
- CCE-27351-6: `screen` パッケージをインストールします。
  スキャナ重要度レベル: 中
- CCE-27268-2: シリアルポートのルートログインを制限します。
  スキャナ重要度レベル: 低
- CCE-27318-5: 仮想コンソールのルートログインを制限します。
  スキャナ重要度レベル: 中
- CCE-27471-2: パスワードなしでの SSH アクセスを無効にします。
  スキャナ重要度レベル: 高
- CCE-27286-4: パスワードなしでのアカウントへのログインを防止します。
  スキャナ重要度レベル: 高
- CCE-27511-5: Ctrl+Alt+Del キーによる再ブートのアクティブ化を無効にします。
  スキャナ重要度レベル: 高

- CCE-27320-1: SSH プロトコルバージョン 2 のみを許可します。
  スキャナ重要度レベル: 高
- CCE-27294-8: root の直接ログインを許可しません。
  スキャナ重要度レベル: 中
- CCE-80157-1: IP 転送のためのカーネルパラメータを無効にします。
  スキャナ重要度レベル: 中
- CCE-80158-9: すべてのインターフェースで ICMP リダイレクトを受け入れるためのカーネルパラメータを構成します。
  スキャナ重要度レベル: 中
- CCE-80163-9: デフォルトで ICMP リダイレクトを受け入れるためのカーネルパラメータを構成します。
  スキャナ重要度レベル: 中
- CCE-27327-6: Bluetooth カーネルモジュールを無効にします。
  スキャナ重要度レベル: 中
- CCE-80179-5: すべてのインターフェースでソースルーティングパケットを受け入れるためのカーネルパラメータを構成します。
  スキャナ重要度レベル: 中
- CCE-80220-7: GSSAPI 認証を無効にします。
  スキャナ重要度レベル: 中
- CCE-80221-5: Kerberos 認証を無効にします。
  スキャナ重要度レベル: 中
- CCE-80222-3: 厳密モードのチェックの使用を有効にします。
  スキャナ重要度レベル: 中
- CCE-80224-9: 圧縮を無効にするか、圧縮の遅延を設定します。
  スキャナ重要度レベル: 中
- CCE-27455-5: FIPS で承認された MAC のみを使います。
  スキャナ重要度レベル: 中
- CCE-80378-3: `/etc/cron.allow` を所有するユーザーを確認します。
  スキャナ重要度レベル: 中
- CCE-80379-1: `/etc/cron.allow` を所有するグループを確認します。
  スキャナ重要度レベル: 中
- CCE-80372-6: ユーザーが既知のホストの SSH サポートを無効にします。
  スキャナ重要度レベル: 中
- CCE-80373-4: `rhosts` RSA 認証の SSH サポートを無効にします。
  スキャナ重要度レベル: 中

- CCE-27363-1: SSH 環境オプションを許可しません。
  スキャナ重要度レベル: 中
- CCE-26989-4: gpgcheck がグローバルにアクティブになっていることを確認します。
  スキャナ重要度レベル: 高
- CCE-80349--4: 認定済みの OS がインストールされていることを確認します。
  スキャナ重要度レベル: 高
- CCE-27175-9: 0 以外の uid がありません (よりよい説明を取得)。
  スキャナ重要度レベル: 高
- CCE-27498-5: 自動マウンタを無効にします。
  スキャナ重要度レベル: 中
- CCE-80134-0: ユーザーが所有していないファイルはありません。
  スキャナ重要度レベル: 中
- CCE-80135-7: ファイル権限グループが所有していません。
  スキャナ重要度レベル: 中
- CCE-27211-2: sysctl_kernal_exec_shield。
  スキャナ重要度レベル: 中
- CCE-27352-4: すべてのアカウントパスワードハッシュがシャドーイングされていることを確認します。
  スキャナ重要度レベル: 中
- CCE-27104-9: パスワードハッシュアルゴリズム systemauth を設定します。
  スキャナ重要度レベル: 中
- CCE-27124-7: パスワードハッシュアルゴリズム logindefs を設定します。
  スキャナ重要度レベル: 中
- CCE-27053-8: パスワードハッシュアルゴリズム libusercon を設定します。
  スキャナ重要度レベル: 中
- CCE-27078-5: 事前リンクソフトウェアを無効にします。
  スキャナ重要度レベル: 低
- CCE-27116-3: サポートされている 32 ビット x86 システムに PAE カーネルをインストールします。
  スキャナ重要度レベル: 低
- CCE-27503-2: /etc/password で参照されるすべての GID が /etc/group で定義される必要があります。
  スキャナ重要度レベル: 低
- CCE-27160-1: パスワード pam 再試行します。
  スキャナ重要度レベル: 低

- CCE-27275-7: ログインの試行を表示します。
  スキャナ重要度レベル: 低
- CCE-80350-2: sudo の no_authenticate を削除します。
  スキャナ重要度レベル: 中
- CCE-26961-3: SELinux が /etc/default/grub で無効になっていないことを確認します。
  スキャナ重要度レベル: 中

p.105 の「適用外の STIG の強化ルール」を参照してください。

適用外の STIG の強化ルール

このトピックでは、NetBackup アプライアンスに適用されていない STIG (Security Technical Implementation Guide) のルールについて説明します。このリストに含まれるルールが適用されないのは、次に示す理由によると考えられますが、これらに限定されるものではありません。

- 今後のアプライアンスのソフトウェアリリースで、ルールの適用が予定されています。
- 別の方法を使って、ルールで説明されている方法と同等またはそれを超える保護を提供します。
- ルールで説明する方法は、NetBackup アプライアンスでは使用またはサポートされません。

現在適用されていない STIG ルールを次に示します。

- CCE-26876-3: gpgcheck がすべての yum パッケージリポジトリで有効になっていることを確認します。
  スキャナ重要度レベル: 高
- CCE-27209-6: rpm のファイル権限を確認および修正します。
  スキャナ重要度レベル: 高
- CCE-27157-7: rpm でファイルハッシュを確認します。
  スキャナ重要度レベル: 高
- CCE-80127-4: McAfee ウイルス対策ソフトウェアをインストールします。
  スキャナ重要度レベル: 高
- CCE-26818-5: 侵入検知ソフトウェアをインストールします。
  スキャナ重要度レベル: 高
- CCE-27334-2: SELinux 状態が適用されていることを確認します。
  スキャナ重要度レベル: 高
- CCE-80226-4: 暗号化された X11 転送を有効にします。
  スキャナ重要度レベル: 高

- CCE-27386-2: デフォルトの SNMP パスワードが使われていないことを確認します。
  スキャナ重要度レベル: 高
- CCE-80126-6: ACCM (Asset Configuration Compliance Module) をインストールします。
  スキャナ重要度レベル: 中
- CCE-80369-2: PA (Policy Auditor) モジュールをインストールします。
  スキャナ重要度レベル: 中
- CCE-27277-3: USB ストレージドライバの `modprobe` ロードを無効にします。
  スキャナ重要度レベル: 中
- CCE-27349-0: 受信パケットのデフォルト `firewalld` ゾーンを設定します。
  スキャナ重要度レベル: 中
- CCE-80170-4: `libreswan` パッケージをインストールします。
  スキャナ重要度レベル: 中
- CCE-80223-1: 権限分離の使用を有効にします。
  スキャナ重要度レベル: 中
- CCE-80347-8: `gpgcheck` がローカルパッケージで有効になっていることを確認します。
  スキャナ重要度レベル: 高
- CCE-80348-6: `gpgcheck` がリポジトリメタデータで有効になっていることを確認します。
  スキャナ重要度レベル: 高
- CCE-80358-5: `dracut_fips` パッケージをインストールします。
  セキュリティスキャナレベル: 中
- CCE-80359-3: `GRand Unified Bootloader` バージョン 2 (GRUB2) の FIPS モードを有効にします。
  スキャナ重要度レベル: 中
- CCE-27557-8: アイドル状態のセッションを終了する、対話式セッションタイムアウトを設定します。
  スキャナ重要度レベル: 中
- CCE-80377-5: ハッシュを検証するよう、FIPS 140-2 に基づいて AIDE を構成します。
  スキャナ重要度レベル: 中
- CCE-80351-0: 権限のエスカレーション (`sudo_NOPASSWD`) のためにユーザーが再認証することを確認します。
  スキャナ重要度レベル: 中
- CCE-27355-7: アクティブでない状態の後のアカウントの有効期限を設定します。

スキャナ重要度レベル: 中

- CCE-80207-4: スマートカードログインを有効にします。
  スキャナ重要度レベル: 中
- CCE-27370-6: ディスク容量が少ないときの `auditd_admin_space_left_action` を構成します。
  セキュリティスキャナレベル: 中
- CCE-27295-5: 承認された暗号のみを使います。
  スキャナ重要度レベル: 中
- CCE-26548-8: `bootloader` 構成による USB のカーネルサポートを無効にします。
  スキャナ重要度レベル: 低
- CCE-27128-8: パーティションを暗号化します。
  スキャナ重要度レベル: 高
- CCE-26895-3: ソフトウェアのパッチがインストールされていることを確認します。
  セキュリティスキャナレベル: 高
- CCE-27279-9: SE Linux ポリシーを構成します。
  スキャナ重要度レベル: 高
- CCE-27399-5: `ypserv` パッケージをアンインストールします。
  スキャナ重要度レベル: 高
- CCE-80128-2: は、サービス釘を有効にします。
  スキャナ重要度レベル: 中
- CCE-80129-0: ウイルススキャンの定義を更新します。
  スキャナ重要度レベル: 中
- CCE-27288-0: SE Linux によってデーモンの制限がない状態にならないことを確認します。すべてのデーモンが SE Linux で制限されることを確認します。
  スキャナ重要度レベル: 中
- CCE-27326-8: SE Linux によってデバイスファイルにラベルがない状態にならないことを確認します。すべてのデバイスファイルが SE Linux によってラベル付けされていることを確認します。
  スキャナ重要度レベル: 中
- CCE-80354-4: UEFI ブートローダーのパスワードを設定します。
  スキャナ重要度レベル: 中
- CCE-80171-2: 設定済みの `IPSec` トンネル接続を確認します。
  スキャナ重要度レベル: 中
- CCE-26960-5: ブートファームウェアの USB デバイスからのブートを無効にします。
  スキャナ重要度レベル: 低

- CCE-27194-0: ブートファームウェア構成の変更を防ぐためにパスワードを割り当てます。
  スキャナ重要度レベル: 低

p.98 の「NetBackup アプライアンスのための OS STIG の強化」を参照してください。

NetBackup アプライアンスの FIPS 140-2 準拠

連邦情報処理標準 (FIPS) には、米国連邦政府とカナダ政府のコンピュータシステムに対するセキュリティと相互運用性の必要条件が定義されています。米国国立標準技術研究所 (NIST) は、暗号化モジュールの検証に関する必要条件と標準をまとめた FIPS 140 文書シリーズを発行しています。FIPS 140-2 標準には、暗号化モジュールのセキュリティ要件が指定されており、ハードウェアとソフトウェアの両方のコンポーネントに適用されます。対称キー暗号化と非対称キー暗号化、メッセージ認証、ハッシュの承認済みセキュリティ機能についても説明されています。

FIPS 140-2 標準とその検証プログラムについて詳しくは、次のリンクにアクセスしてください。

https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402.pdf

https://csrc.nist.gov/projects/cryptographic-module-validation-program

NetBackup 暗号化モジュールは FIPS によって検証されています。NetBackup MSDP ではこのモジュールを使用しており、NetBackup Appliance リリース 3.1.1 以降では、次のコマンドを使用して NetBackup MSDP で FIPS 140-2 標準を有効にできます。

`Main Menu > Settings > Security > FIPS > Enable` の後に、メンテナンスパスワードを入力します。

メモ: この機能を有効または無効にすると、その時点で進行中のすべてのジョブが自動的に終了し、NetBackup サービスが再起動します。ベストプラクティスとしては、最初にすべてのジョブを手動で停止してから、この機能を有効または無効にすることをお勧めします。

FIPS コマンドについて詳しくは、『NetBackup Appliance コマンドリファレンスガイド』を参照してください。

メモ: 高可用性 (HA) 設定のアプライアンス (ノード) では、現在 FIPS 機能の使用はサポートされていません。

A

セキュリティのリリース内容

この付録では以下の項目について説明しています。

NetBackup Appliance のセキュリティリリース内容

次のリストには、解決された既知のセキュリティの問題およびこのリリースの NetBackup Appliance に含まれている既知の問題が掲載されています。

Spectre と Meltdown の脆弱性

NetBackup Appliance リリース 3.1.1 には、次のバリアントに固有の修正が含まれています。

- バリアント 1 - Spectre、CVE-2017-5753
- バリアント 3 - Meltdown、CVE-2017-5754

これらの修正は、ローカルユーザーがバイナリファイルをインストールして実行し、他のプロセスのメモリにアクセスする潜在的な問題に対処しています。

これらの脆弱性を緩和するために、すべての NetBackup アプライアンスをできるだけ早くバージョン 3.1.1 にアップグレードすることを推奨します。これらの脆弱性について詳しくは、次の記事を参照してください。

https://www.veritas.com/support/en_US/article.100041496

バージョン 3.1.1 で対応された他の脆弱性について以下で説明します。

- Apache Struts の脆弱性
  CVE-2017-5638
- KRACK 用 WPA2 パッケージの更新
  CVE-2017-13077
  CVE-2017-13078
  CVE-2017-13080

CVE-2017-13082
CVE-2017-13086
CVE-2017-13088

- DNS パッケージの更新
  CVE-2017-14491
  CVE-2017-14492
  CVE-2017-14493
  CVE-2017-14494
  CVE-2017-14495
  CVE-2017-14496
- Java の脆弱性
  CVE-2017-10309
  CVE-2017-10274
  CVE-2017-10293
  CVE-2017-10281
  CVE-2017-10347
  CVE-2017-10348
  CVE-2017-10349
  CVE-2017-10350
  CVE-2017-10357
  CVE-2017-10345
  VE-2017-10346
  CVE-2017-10285
- その他
  CVE-2017-8030
  CVE-2017-8046
  CVE-2017-15288
  CVE-2017-5645
  CVE-2017-17485
  CVE-2017-1000253
  CVE-2017-7555
  CVE-2016-10164
  CVE-2017-2625
  CVE-2017-2626
  CVE-2016-10200
  CVE-2017-2647
  CVE-2017-8797
  CVE-2015-8839
  CVE-2015-8970

CVE-2016-9576
CVE-2016-7042
CVE-2016-7097
CVE-2016-8645
CVE-2016-9576
CVE-2016-9588
CVE-2016-9806
CVE-2016-10088
CVE-2016-10147
CVE-2017-2596
CVE-2017-2671
CVE-2017-5970
CVE-2017-6001
CVE-2017-6951
CVE-2017-7187
CVE-2017-7616
CVE-2017-7889
CVE-2017-8890
CVE-2017-9074
CVE-2017-9075
CVE-2017-9076
CVE-2017-9077
CVE-2017-9242
CVE-2014-7970
CVE-2014-7975
CVE-2016-6213
CVE-2016-9604
CVE-2016-9685
CVE-2016-10165
CVE-2016-8399
CVE-2016-9841
CVE-2017-1000111
CVE-2017-1000112
CVE-2017-10274
CVE-2017-10281
CVE-2017-10295
CVE-2017-7558
CVE-2017-10355
CVE-2017-7542
CVE-2017-10356

CVE-2017-10388
CVE-2017-7184
CVE-2017-12617

索引

ら