第9章　ファイル共有について

この章では、ファイル、フォルダの共有について解説しています。

CONTENTS

9.1　サポートするネットワークファイルシステム

PRIMERGY FileServerは、UNIX/Linuxシステムで一般的なNFS（Network File System ）とWindowsファミリーで一般的なCIFS（Common Internet File System ）、およびApple Macintosh用のAppleTalkプロトコルによるネットワーク上のファイル アクセスをサポートします。どのように異種ファイルシステムを使用するかについては「9.2 ファイルの共有 ～異種システムの混在環境における使用～」をご覧ください。
まずはファイルシステムの特長を簡単に以下に記述します。

9.1.1 CIFSの特長

CIFSは、Microsoft Windows NTクライアントおよびサーバで使用される標準的なネットワーク ファイル共有メカニズムであり、Linuxなどで使われるSMB（Server Message Blocks ）ネットワーク ファイル共有プロトコルのスーパーセットです。

CIFSの代表的な特長は、以下のとおりです。

- 共有アクセス時には、ユーザー名とパスワード入力をし、ネットワークにログインするセッション形式である。
- アクセス権を有するユーザーとグループの管理を基本管理方針とする

9.1.2 NFSの特長

NFSは、UNIXの標準プロトコルで、CIFSとの相違点は、アクセス時に、ユーザー名やパスワードの入力の必要がなく、ホスト名またはクライアント マシンのIP アドレスに基づいてネットワーク ファイル リソースへのアクセスを許可または拒否できることです。
接続過程では、NFS クライアントはNFS 要求の中でユーザー名（UID）とグループ名（GID）が参照されます。
UID とGID をPRIMERGY FileServerで結合する作業を実行しないと、すべてのNFS クライアントは、グループnogroup のユーザーnobody のファイル アクセス許可が参照されます。
NFS は、UNIX のファイル システムを、ネットワークを通じてエキスポートする際に使用するネットワーク プロトコルです。NFSの主な設計目標には、次の3つがあります。

●異なるUNIX マシン間で、ネットワークを介し、ファイルを円滑にエキスポート

NFS は、異なるバージョンのUNIX 間でも、異なるプラットフォーム間でも稼動します。たとえば、Linuxマシンは、Tru64™ UNIXマシン上のファイルにアクセスすることができます。システム管理者とユーザーの両方が、このようなファイルに隔てなくアクセスすることができます。システム管理者やユーザーは、ローカルにあるファイルと、リモート マシン上のファイルに、まったく同様のアクセスができるため、その違いに気付くことがありません。

●可能な限り簡明にした運用管理

リモート ファイル システムは、ローカル ファイル システムとまったく同じ方法で、ローカル マシンにアタッチできます。システム管理者は、他のハード ドライブや、外付けストレージを加える際と同じ方法で、リモート ファイル システムを追加することができます。

●ファイル システムの操作だけに専念

ファイル システムは、ファイル システムをリモート マシンへエキスポートするためだけに使用します。読み込み、書き込み、作成、削除、コピーなどの操作のみサポートします。

また、CIFS クライアントがNFS ファイルに続けてアクセスしても、ユーザーとグループのファイル アクセス権は変換されません。したがって、ユーザーとグループのセットアップは配備の重要な要素になります。

これら二つの特長の比較から分かるとおり、CIFSはユーザー認証に重きを置いた共有プロトコルであり、NFSは簡単な運用管理に重きを置いた共有プロトコルということができます。

■NFS を使うために　–SFU の概要–

PRIMERGY FileServerではNFSを使うために、「Microsoft Windows Services for UNIX 2.1（以下SFU）」のコンポーネントを標準で提供しております。
SFUで最も特徴的な機能は、以下のとおりです。

- NFSファイル共有サービスの提供ができる
- UNIX⇔Windows OS間でのパスワード同期ができる

そのため、たとえばWindows NT/2000サーバを中心にしてネットワークを組んでいる場合、そのサーバ・マシンにSFUをインストールすれば、UNIX/Linuxクライアントを Windowsネットワークに組み入れることができます。つまりWindowsサーバ上に置かれたユーザーごとのホーム・ディレクトリを、Windows系クライアントからも、UNIX系クライアントからもアクセスできます。UNIX系クライアントのために、特別なNFSファイル・サーバを用意したり、2種類のマシンでパスワードを個別に管理したりする必要がなくなります。ファイル共有サービスを一台のマシンだけで集中的に管理したい場合に有用です。

提供されるSFUサービスは以下の２つです。

●NFS 用のサーバおよびNFS認証サーバ

SFU のNFS サーバは、NFS をサポートする本来のファイル システムを提供します。Windows NTファイルは、NFS を通じたエキスポートやアクセスが可能です。

最近まで、UNIXだけがファイルをエキスポートするのにNFS を使用していました。UNIXは、Windowsプラットフォームとファイルを共有することができず、また、Windowsプラットフォームも、UNIX とファイルを共有することができませんでした。

この制限から、UNIXクライアントはUNIX用のファイル サーバが必要で、Windowsクライアントは Windows 用のファイル サーバが必要でした。WindowsプラットフォームとUNIXは、ハードウェアも双方で用意し、オーバーヘッドも労力も双方の環境で生じてしまう完全に切り離された環境でした。

PRIMERGY FileServerではSFUの機能を使うことで、UNIXクライアントは、Windowsベースのマシンをファイル サーバとして使用することができます。SFUのNFSサーバは、NFSバージョン2と3をサポートし、また、TCPとUDPの両ネットワーク プロトコル上での稼動もサポートします。

●ユーザー名のマッピング

その他のSFUコンポーネントに、ユーザー名のマッピング サーバがあります。
ユーザー名のマッピングは、ある1つの環境からユーザーやグループのIDを取り出し、他の環境にあるユーザーID用に変換する処理を指します。

UNIXやNFSの世界では、ユーザーとグループのIDはユーザーID（UID）とグループID（GID）の組み合わせになります。
Windows環境では、ユーザーのIDがセキュリティID（SID）に、また、Windows 2000ではグローバル一意識別子（GUID）になります。

ファイルサーバが異種システムの混在する環境内でファイルをエキスポートするときでも、認証に何ら問題は発生しません。ただ単純に直接照合して、そのユーザーはそのファイルへのアクセス権があるのか、また、アクセス レベルは何かを判断します。
しかし、ファイルサーバが異種システムの混在する環境内で処理する場合、ユーザーのアクセス権を何らかの方法で変換する必要があります。ユーザーのマッピング処理とは、ユーザーのセキュリティ権をある環境から別の環境用に変換する処理になります。

前節で説明したとおり、NFSサーバは、マシン名とIPアドレスに基づいて、エキスポートへのアクセスを許可したり、拒否したりします。しかし、クライアント マシンがエキスポートへアクセスした後は、ユーザーレベルの許可を使用して、ユーザーファイルやディレクトリに対するアクセスの許可や拒否を判断します。

PRIMERGY FileServerは、異種システムが混在する環境で運用する能力があります。これは、UNIXとWindowsの両方のクライアントが稼動できるという意味です。ファイルは純粋なWindows NTファイル システムに格納するため、サーバは、UNIXユーザーをWindowsユーザーにマッピングして、各ファイルに対するユーザーのアクセス レベルを決定する必要があります。

9.1.3 AppleTalkの特長

AppleTalkとは、Apple社のMac OSに標準搭載されているネットワーク機能です。また、AppleTalkのネットワーク機能を実現するプロトコル群の総称のことを言います。
AppleTalkではファイル共有やプリンタ共有などのサービスが提供されます。AppleTalkネットワーク上の、別のコンピュータのアプリケーションソフトを起動することもできます。
AppleTalkの伝送媒体にはEthernet（EtherTalk）の他に、AppleTalk独自のLocalTalkや、ケーブルに電話線を利用したLocalTalk互換のPhoneTalkなどが使われます。

■EtherTalk

EthernetはXerox社とDEC社（現在はCompaq Computer社の一部門）が考案したLAN規格で、PhaseIとPhaseIIと呼ばれる二つの層からなります。

●EtherTalk Phase I

Ethernet上でAppleTalkを動かすためのプロトコルです。AppleTalkセグメントとネットワーク番号は一対一対応します。これによりAppleTalkのルータを介さない限り、ネットワーク番号は保証されます。

●EtherTalk Phase II

AppleTalkでは端末に割り当てられるノード番号は1バイトです。このため、EtherTalk PhaseIでは１セグメントに割り当て可能な端末数に上限があります。これを解決するために開発されたのが PhaseIIです。
１つのAppleTalkセグメントに対して、ネットワーク番号の範囲を割り当てることができます。

9.2　ファイルの共有～異種システムの混在環境における使用～

プラットフォーム間でファイルを授受するPRIMERGY FileServerにおいて、最初に湧き上がる疑問の１つは、ファイルへの同時アクセスをどのように処理するか、ということです。
PRIMERGY FileServerは、クライアントから渡される制御を受け取り、これをファイルシステムレベルで処理することで、この疑問に対応しています。

ネットワーク クライアントがCIFS やNFS を経由してデータにアクセスするとき、クライアントは、POSIX open()コールに似たAPI呼び出しを行います。これは、アプリケーションが既存のファイルを開いたり、新しいファイルを作成する際に、ファイルシステムに、希望するファイルのロック方法を指示するパラメータ渡しを行っているイメージと同じです。このロック方法を指示するパラメータは、次のいずれかの形式になりますが、当てはまらないこともあります。

パラメータ	内容
リード ライト（読み書き）共有	他のアプリケーションも 同時に読み書きする目的で、同じファイルをオープンすることができます。
リード オンリー（読み取り専用）共有	他のアプリケーションも、読み取り専用で、同じファイルを開くことができます。他のアプリケーションがそのファイルに書き込みを試みると、拒否されます。
ライト オンリー（書き込み専用）共有	他のアプリケーションも、書き込み専用で、同じファイルを開くことができます。他のアプリケーションがそのファイルから読み込みを試みると、拒否されます。
排他共有	他のアプリケーションは、読み書きする目的で同じファイルを開くことができません。 他のアプリケーションが同じファイルを開こうとしても、拒否されます。

基本的には、最初にファイルを開いたアプリケーションが、そのファイルのロック方法を決定します。一度ロックされると、該当する共有に関する適切な設定内容が、そのファイル システムで効力を持つようになります。その後、他のアプリケーションが同じファイルを開く場合、その動作は最初のアプリケーションが設定したロック用パラメータに従うことになります。たとえば、最初のアプリケーションがリード オンリー共有として開いたファイルは、2番目のアプリケーションが書き込み目的でそのファイルを開こうとすると、システムがそれを許さないため、失敗に終わります。

これと同じ規則がCIFSやNFSなどのネットワーク ファイル システムにも該当します。
CIFS とNFS の両方が、プロトコル エンティティを含んでおり、これによって希望するオープンモード（たとえばリード、ライト、リード ライト）と、APIから渡されるロック用パラメータの両方を、ネットワーク回線を通じて送信することができます。

PRIMERGY FileServer上に常駐するNFSやCIFSサーバは、このようなロック用パラメータをネットワーク経由で受け取り、パラメータに指示された方法でファイルのオープンを試み、希望するロック方法を適用します。クライアントが最初にファイルを開く場合は、オープンが成功し、指定したロック方法が適用されます。そして、PRIMERGY FileServerのファイル システム上でもそのロック方法が効力を持ちます。クライアントによるファイルのオープンが2番目以降の場合、ロック用パラメータがファイル システム レベルで効力を持っているため、CIFSであるかNFSであるかに関わらず最初にそのファイルをオープンしたクライアントが、ロック用のパラメータを指定し、適用しています。そこで、2番目（または3番目、4番目…）のクライアントは、最初にそのファイルがどのようにロックされたかに従って、アクセスが許可されることになります。
CIFSとNFSの両方が、ネットワーク プロトコル レベルのロック用エンティティをサポートするため、各クライアントがファイルにアクセスする際、どのクライアントが、何のプロトコルを使用しているかは、問題になりません。

ファイルがオープンしている限り、同じファイルのオープンを試みる他のクライアントに対し、本サーバはロック用パラメータを適用します。アクセスしているすべてのクライアント（低レベルのAPIコールで、POSIXの場合close()、Windowsの場合CloseHandle()）が、そのファイルを閉じた（クローズした）時点で、本サーバのファイル システムが直ちにファイルのロックを解除します。
そのあとは、そのファイルのオープンを試みる場合、ファイルがオープンしていなかったように動作します。

9.3　既存のフォルダを共有する

1. プライマリナビゲーションバーで、［共有］をクリックします。
2. セカンダリナビゲーションバーで、［フォルダ］をクリックします。
   次の画面が表示されます。

3. 既にあるフォルダー覧リストから、フォルダを共有するボリュームを選択し、［タスク］ボックスの一覧から［共有］を選択します。
4. プロンプトの指示に従って情報を入力します。
   特定のファイル共有方法で使用するプロパティ ページの設定項目については、「9.4 新しくフォルダを共有する」をご覧ください。

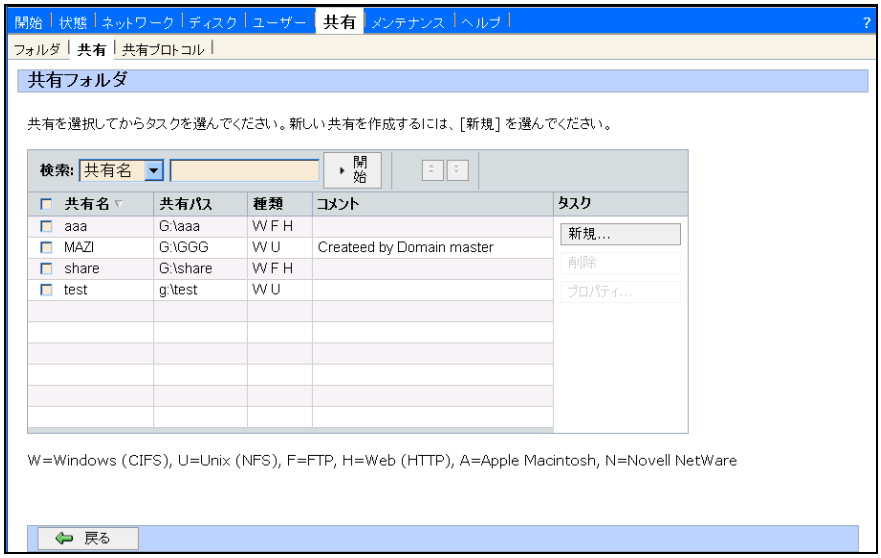
9.4　新しくフォルダを共有する

新しく共有を作成するには、ほかのすべての共有および共有パスと重複しない一意な共有名を指定する必要があります。一部のプロトコルでは、共有に関するコメントまたは簡単な説明を指定することもできます。さらに、使用可能な1つ以上のプロトコルを有効にしなければなりません。

⚠注意

- 同じ1つのユーザー インターフェイスを使用してすべてのプロトコルの共有を作成できますが、実際には、プロトコルごとにそれぞれ個別の共有が作成されます。個々の共有プロトコルを共有から削除しても、共有自体は削除されません。ただし、共有からすべての共有プロトコルを削除すると、すべての種類の共有が削除されます。
- NFSの共有は出荷時はOFFの設定になっています。「9.8章　NFS共有プロトコル」を参照し、プロトコルサービスを［有効］にする必要があります。

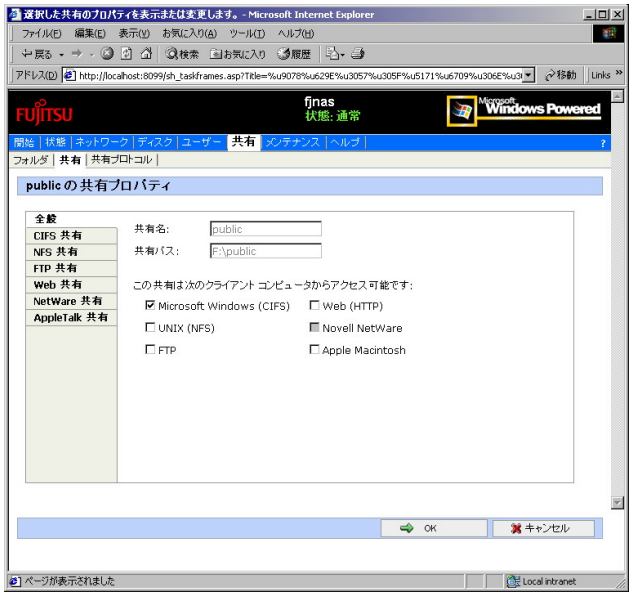
1. プライマリナビゲーションバーで、［共有］をクリックします。
2. セカンダリナビゲーションバーで、［共有］をクリックします。
   共有ページが表示されます。



3. 既にあるフォルダー覧リストから、フォルダを共有するボリュームを選択し、［タスク］ボックスの一覧から［プロパティ］を選択します。
4. 各タブを設定します。

9.4.1 全般

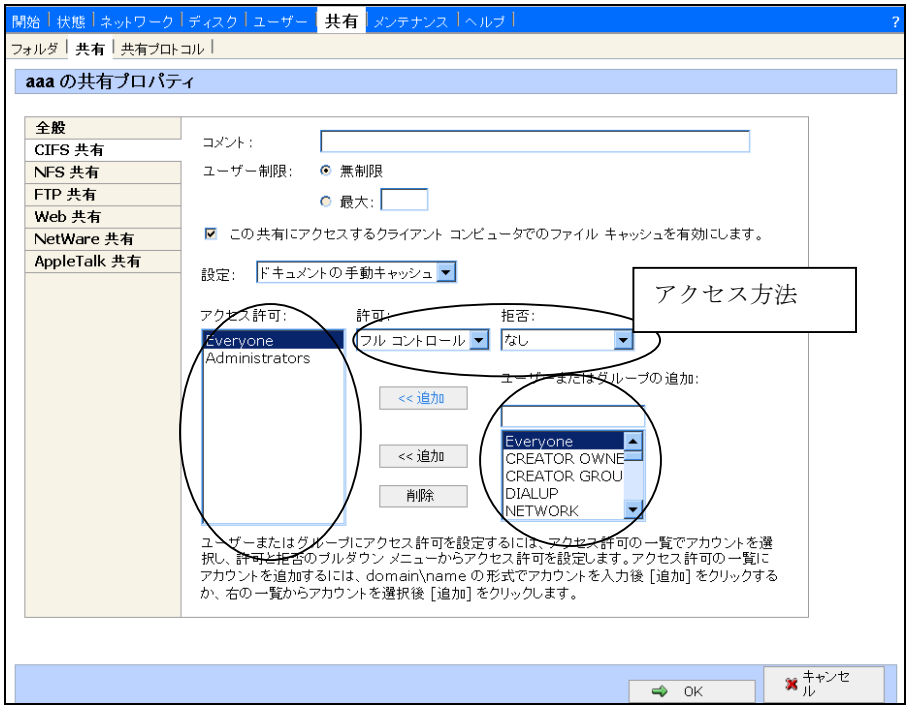
1. プライマリナビゲーションバーで、［共有］をクリックします。
2. セカンダリナビゲーションバーで、［共有］をクリックします。
   共有ページが表示されます。
3. ［タスク］ボックスの一覧で、［新規］をクリックします。
   次の画面が表示されます。



4. ［全般］タブで、共有名と共有パスを入力します。
5. 該当するチェック ボックスを選択して、有効にするプロトコルの種類を指定します。
6. プロトコル タブを使用して、各共有タイプのプロパティを設定します。

9.4.2 CIFS共有

1. プライマリナビゲーションバーで、［共有］をクリックします。
2. セカンダリナビゲーションバーで、［共有］をクリックします。
   共有ページが表示されます。
3. ［タスク］ボックスの一覧で、［新規］をクリックします。
4. ［CIFS］タブをクリックします。
   次の画面が表示されます。



ユーザー制限

ユーザー制限では、共有アクセス可能な最大数のユーザー接続を許可するか、同時に実行できる接続数を指定することができます。

●ユーザー制限を設定するには

以下のいずれかの操作を行います。

- ［無制限］をクリックして、処理可能な最大数のユーザーに本サーバへのログオンを許可します。
- ［最大］をクリックし、接続を許可するユーザー数を指定します。

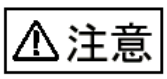
キャッシュ設定

ネットワーク上の共有ファイルをオフラインで使用するには、クライアント コンピュータの「キャッシュ」と呼ばれる予約済みディスク領域にファイルのバージョンを格納します。ネットワークに接続しているかどうかに関係なく、コンピュータはこのキャッシュにアクセスすることができます。ファイルを共有する場合は、次の3つのキャッシュ オプションを使用できます。

- **ドキュメントの手動キャッシュ**
  ドキュメントの手動キャッシュでは、サーバ上の共有フォルダを使用するユーザーが明確に、つまり手動で識別したファイルにのみ、オフラインでアクセスすることができます。このキャッシュ オプションは、限られた数名のユーザーによってアクセスされ修正されるファイルを含むサーバ上のフォルダを共有する場合に適しています。共有フォルダをオフラインで使用するように設定した場合、これが既定のオプションになります。

- **ドキュメントの自動キャッシュ**
  ドキュメントの自動キャッシュでは、サーバ上の共有フォルダ内で開かれたすべてのファイルが、そのファイルを開いたユーザーに対して、オフラインで使用可能になります。つまりクライアント側に指定したファイルをダウンロードさせます。
  自動キャッシュでは、サーバの共有フォルダを使用するユーザーが、ファイルを使用可能に設定したかどうかに関係なく、フォルダのコンテンツをオフラインで使用することができます。
  ユーザーは、ドキュメント、図面、プログラム ファイル、およびその他のすべてのファイルを使用できるようになります。
  オフライン作業時には、そのユーザーが共有フォルダで開いたファイルのみを継続して使用することができます。

- **プログラムの自動キャッシュ**
  プログラムの自動キャッシュは、共有フォルダ ファイルへの読み取り専用のオフライン アクセスを提供します。このキャッシュ オプションは、ファイルをオフラインで実行したり、参照または読み取る際に、これらのファイルを変更できないようにする場合に適しています。プログラムの自動キャッシュによりネットワーク トラフィックが軽減されます。これは、オフライン ファイルをネットワーク バージョンにアクセスせずに直接開くことができ、一般的にネットワーク バージョンよりも高速に起動および実行することができるためです。
  ※プログラムの自動キャッシュは、特に性能を重視する場合に選択してください。



プログラムの自動キャッシュを使用する場合は、必ず共有フォルダ ファイルのアクセス権を読み取り専用アクセスに制限してください。共有に関しては保証されない場合があります。

■ユーザーのアクセス許可を設定する

サーバ へのアクセスを許可または拒否するユーザーまたはグループに対して、アクセス許可を設定することができます。
［ユーザーまたはグループの追加］ボックスで、以下の手順で設定します。

1. 一覧からローカル ユーザーまたはローカル グループを選択します。
   ドメイン ユーザーまたはドメイン グループを追加するには、アカウントを<ドメイン名¥ユーザー名>または<ドメイン名¥グループ名>のように入力します。
2. ［追加］をクリックします。
3. ［許可］ボックスの一覧を使用して、［アクセス許可］ボックスの一覧で選択されたユーザーがサーバ アプライアンス上のファイルに対して持つ制御のレベルを設定します。
   ユーザーに設定できる制御は、フル コントロール、変更アクセス、読み取り専用アクセス、変更および読み取りアクセス、制御なしのいずれかです。
4. ［拒否］ボックスの一覧を使用して、［アクセス許可］ボックスの一覧で選択したユーザーおよびグループに対する制御のレベルを拒否します。
5. ［アクセス許可］の一覧からユーザーまたはグループを削除するには、ユーザーまたはグループを選択して、［削除］をクリックします。
6. ［OK］をクリックします。

⚠注意

［追加］ボタンが二種類ありますが、上はアカウントを直接入力した場合に有効になります。PRIMERGY FileServer に既に登録されているユーザーまたはグループを追加する場合は、下の［追加］ボタンを利用します。

アクセスレベルには以下の種類があります。
アクセス権を設定する場合は、対象とするユーザーおよび対象とするファイルの種類を考え、設定を行ってください。

アクセスレベル	説明
フルコントロール	：全てのアクセスレベルの許可に対して、以下の全てがアクセス許可される。
変更	：次を除く、全ての高度なアクセスプロパティを含む — サブフォルダとファイルの削除 — 許可の変更 — 所有権の取得
読み取りと実行	：次を除く、全ての高度なアクセスプロパティを含む — サブフォルダとファイルの削除 — 削除 — 許可の変更 — 所有権の変更
フォルダ内容と一覧	：次のアクセス許可のみ — フォルダのトラバース/ファイルの実行 — フォルダの一覧/データの読み取り — 属性の読み取り — 拡張属性の読み取り — 読み取り許可

アクセスレベル	説明
読み取り	：次のアクセス許可のみ — フォルダの一覧/データの読み取り — 属性の読み取り — 拡張属性の読み取り — 読み取り許可
書き込み	：次のアクセス許可のみ — ファイルの作成/データの書き込み — フォルダの作成/データの追加 — 属性の書き込み — 書き込み属性の書き込み

9.4.3 NFS共有

NFS共有のページを使用して、各共有へのアクセスを許可するNFSクライアントを指定します。クライアント ホスト名に基づいてアクセスの許可または拒否を設定できます。また、クライアント グループに基づいてアクセスの許可または拒否を設定することもできます。クライアント グループには、1つまたは複数のクライアント ホスト名が含まれています。
WebUIからNFS共有を作成することもできますが、Windows ExplorerによるNFS共有の作成をおすすめします。
操作については、以下の「■Windows Explorerによる共有の作成」をごらんください。

ポイント

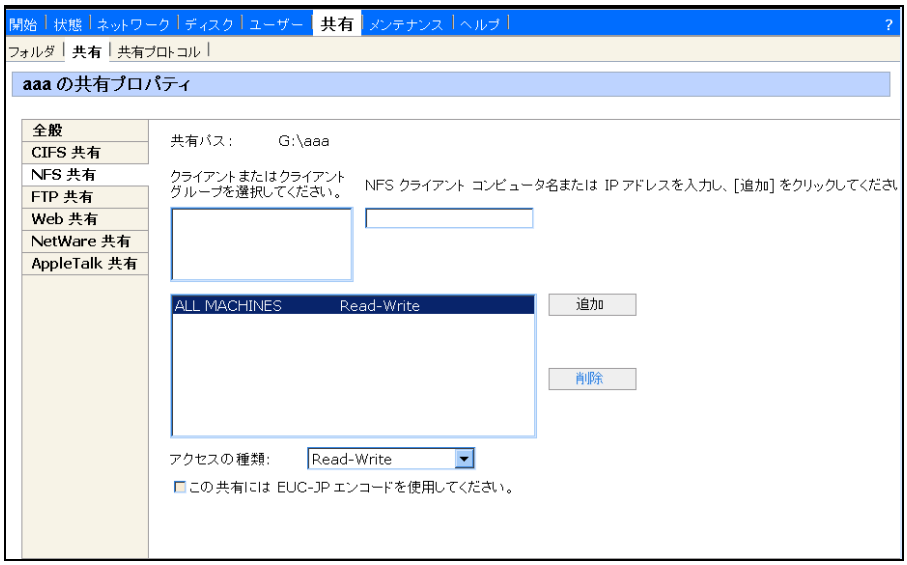
NFSの共有は出荷時はOFFの設定になっています。「9.8章　NFS共有プロトコル」を参照し、プロトコルサービスを［有効］にする必要があります。

■新しいNFS クライアントまたはクライアント グループを共有に追加する

「9.8.1 NFSクライアントグループの管理」をご覧ください。

■既存の NFS クライアントまたはクライアント グループを共有に追加する

1. プライマリ ナビゲーション バーで、［共有］をクリックします。
2. セカンダリ ナビゲーション バーで、［共有］をクリックします。
3. NFSクライアントまたはクライアント グループを追加する共有を選択します。
4. ［タスク］ボックスの一覧で、［プロパティ］をクリックします。
5. ［全般］タブをクリックします。
6. ［UNIX（NFS)］チェック ボックスをオンにします。
7. ［NFS 共有］タブをクリックします。
   NFS 共有のページが表示されます。



8. 左側の一覧から目的のコンピュータまたはグループを選択するか、右側のボックスにNFS クライアント コンピュータ名または IP アドレスを入力して、［追加］をクリックします。
9. ［アクセスの種類］ボックスの一覧から、指定したクライアントが共有のファイルに対して実行できる制御のレベルを選択します。
10. ［OK］をクリックします。

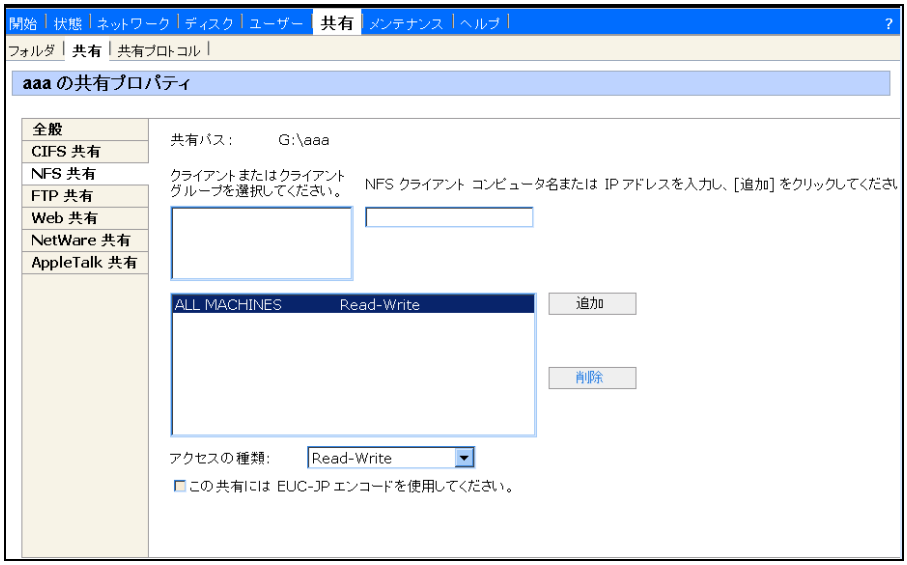
■ Windows Explorer による NFS 共有の作成

1. プライマリナビゲーションバーで、［メンテナンス］をクリックします。
2. セカンダリナビゲーションバーで、［ターミナルサービス］をクリックします。
3. ［スタート］メニューから［プログラム］、［アクセサリ］をポイントし、［エクスプローラ］をクリックします。
4. マイコンピュータのツリーを展開し、共有を作成するドライブへ移動します。
5. NFS共有を開始したいフォルダを右クリックし、［プロパティ］を選択します。
6. NFS共有タブから、共有名と、パーミッションを設定し［OK］ボタンをクリックします。

■NFS クライアントを削除する

1. プライマリ ナビゲーション バーで、［共有］をクリックします。
2. セカンダリ ナビゲーション バーで、［共有］をクリックします。
3. NFSクライアントまたはクライアント グループを削除する共有を選択します。
4. ［タスク］ボックスの一覧で、［プロパティ］をクリックします。
5. ［全般］タブをクリックします。
6. ［UNIX（NFS）］チェック ボックスをオンにします。

7. ［NFS 共有］タブをクリックします。
NFS 共有のページが表示されます。



8. ページの中央にある一覧から、目的のクライアントまたはクライアント グループを選択し、［削除］をクリックします。
9. ［OK］をクリックします。
10. NFS共有がきちんと作成されていることをプロパティページを使って確認します。

アクセス権の設定は、画面上では英語表記されます。
例）No Access : アクセス不可

また、WebUI上からは、Root権限を付与することはできません。

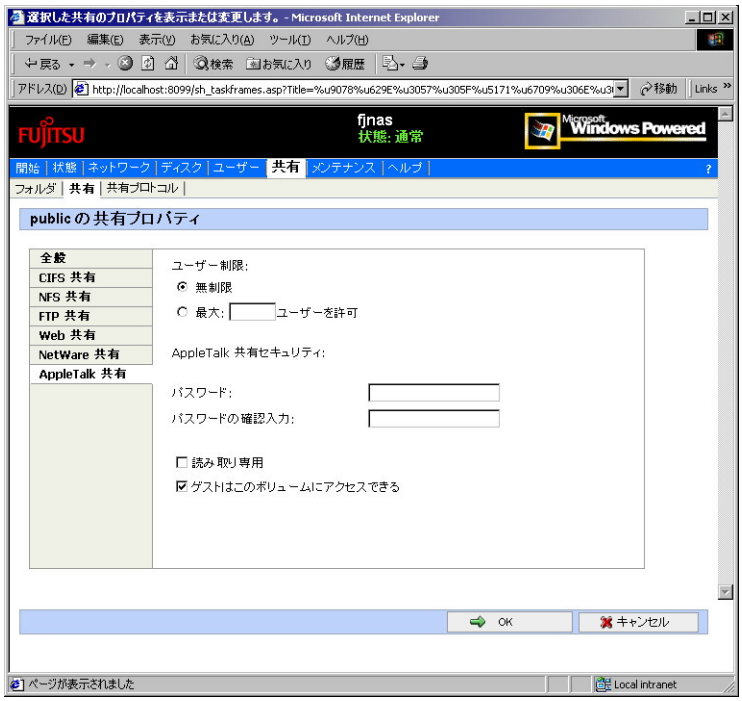
9.4.4 FTP/HTTP

FTP/HTTP設定では、フォルダに対して書き込みまたは読み込みかのどちらかしか設定できません。
特定のユーザーに対して、アクセス許可を付与することはできません。

FTPはアクセスログを採取することが可能です。
設定の詳細に関してはWebUIヘルプをご覧ください。

9.4.5 Apple Macintosh

1. プライマリ ナビゲーション バーで、[共有] をクリックします。
2. セカンダリ ナビゲーション バーで、[共有] をクリックします。
3. AppleTalk クライアント アクセスを追加する共有を選択し、[プロパティ] をクリックします。
4. [全般] タブで、[Apple Macintosh] チェック ボックスをオンにします。
5. [AppleTalk 共有] タブをクリックします。
   次の画面が表示されます。



6. ユーザー制限および共有アクセス パスワードを設定します。
7. 必要に応じて [読み取り専用] およびゲストアクセス許可を設定します。
8. [OK] をクリックします。

9.5　フォルダ/共有を管理する

複数のネットワーク ボリュームを開いたり、共有することができます。

1. プライマリ ナビゲーション バーで、［共有］をクリックします。
2. セカンダリ ナビゲーション バーで、［フォルダ］をクリックします。

次の列で構成された、［オブジェクト/タスク セレクタ］が表示されます。

項目	説明
ボリューム名	すべてのボリュームの名前が一覧表示されます。特定のボリュームを開いたり、ボリュームを作成または削除したり、ボリュームのプロパティを構成するには、目的のボリューム名の横にあるチェックボックスをオンにします。
合計サイズ	ボリュームの合計サイズが表示されます。
空き領域	ボリュームの空き領域のサイズが表示されます。
共有の種類	フォルダに適用される共有の種類を示します。 W = Windows（CIFS）共有 U = UNIX（NFS）共有 F = FTP共有 H = HTTP共有 A = AppleTalk共有

［オブジェクト/タスク セレクタ］には、最大100のフォルダが一覧表示されます。［オブジェクト/タスク セレクタ］に一覧表示されるフォルダ間を移動するには、［検索］ボックスでフィールドを指定した後、［開始］ボタンの左側のボックスに検索条件を入力して、目的のフォルダを検索します。または、一覧をスクロールして目的のフォルダを探します。フォルダ数が100を超える場合は、［開始］ボタンの右側にある［Page Up］をクリックしてその前の100個のフォルダを表示するか、［Page Down］をクリックしてその次の100個のフォルダを表示します。

フォルダの管理情報は以下の情報が表示されます。

項目	説明
フォルダ名	フォルダの名前が一覧表示されます。
変更日	フォルダを最後に修正した日付が表示されます。
属性	次のフォルダ属性が表示されます。 R = 読み取り専用 A = アーカイブ可能 H = 隠しフォルダ C = 圧縮 S = システム フォルダ

9.6　共有プロトコルの概要

共有プロトコルは、PRIMERGY FileServerで提供しているファイル共有プロトコルに対して、以下の操作を行えます。

- プロトコルサービスの開始
- プロトコルサービスの停止
- プロトコルサービスの詳細設定

9.7　CIFS共有プロトコル

CIFS共有プロトコル設定では、サービスのプロパティが表示されます。

9.8　NFS共有プロトコル

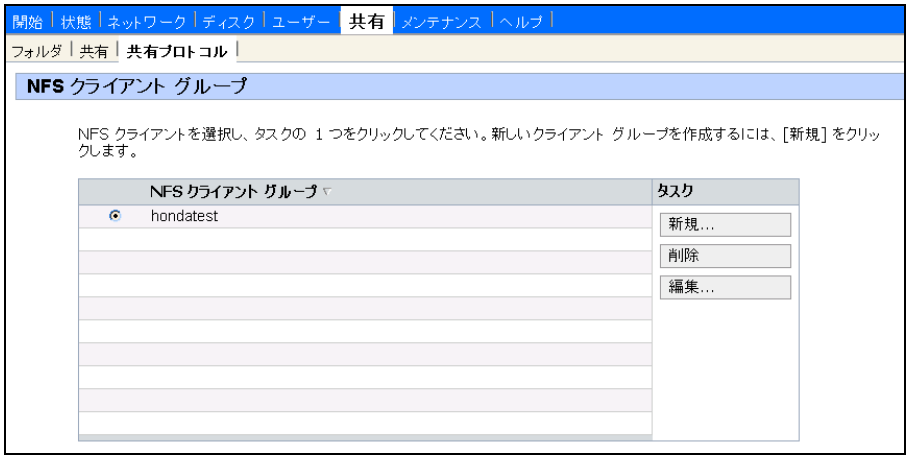
NFS共有プロトコル設定では、サービスの開始・停止の実行が可能であると共に、以下の機能を提供します。

- NFSクライアントグループの管理
- NFSサービスロックの提供
- ユーザーとグループのマッピング管理

9.8.1 NFSクライアントグループの管理

NFSプロトコル設定を行うには、以下の手順で行います。

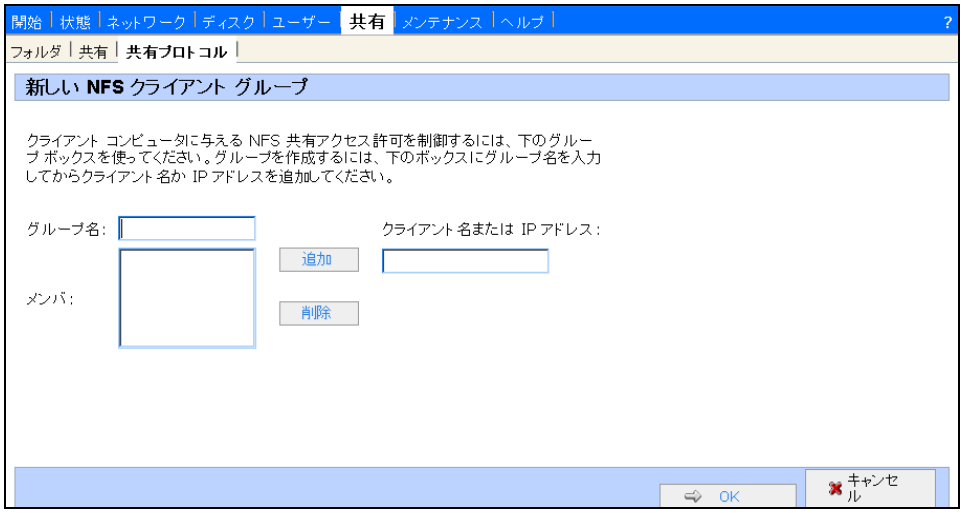
1. プライマリナビゲーションバーから［共有］をクリックします。
2. セカンダリナビゲーションバーから［共有プロトコル］をクリックします。
3. NFSプロトコルを選択し、[プロパティ]をクリックします。NFSサービス画面が表示されます。
4. ［クライアントグループ］をクリックします。
   ［クライアントグループ］のページが表示されます。



既存のNFSクライアントグループ一覧が表示されます。タスクには、NFSクライアントグループの新規・削除・編集があります。

■NFS クライアントグループの新規作成

1. ［クライアントグループ］のページの［タスク］一覧から［新規］をクリックします。
   新規作成画面が表示されます。



2. 必要に応じて項目を設定します。
   新規作成画面では以下の項目が設定できます。

項目名	説明
グループ名	任意のグループ名を設定することができます。 Windowsのグループ作成と同様にクライアントを特定できる、透過的なグループ名を設定することをおすすめします。
クライアントメンバ	クライアントメンバの設定は、クライアント名もしくはIPアドレスを設定することができます。 設定したクライアントは追加ボタンをクリックすることでメンバリストに追加されます。

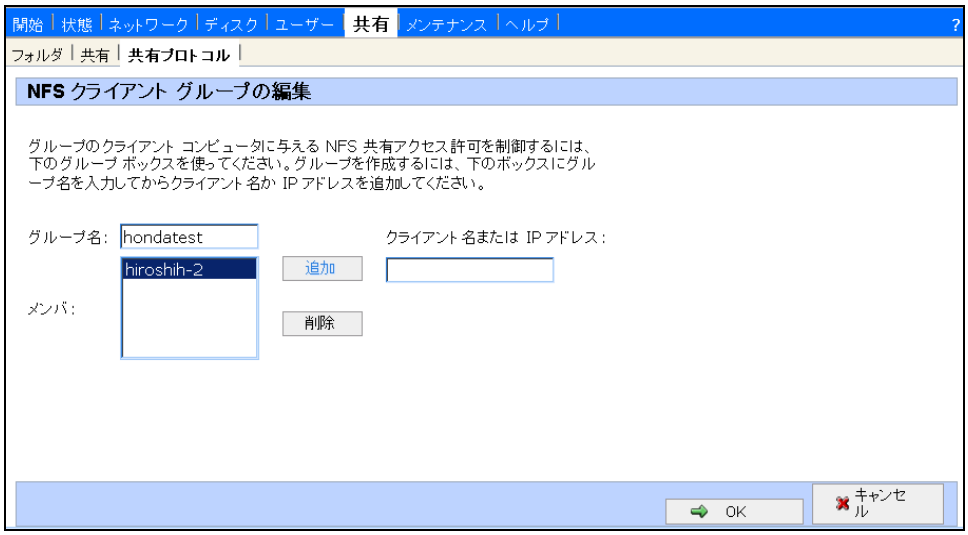
3. ［OK］をクリックします。
   設定したグループ内容がコンピュータに適用されます。

■NFS クライアントグループの削除

1. ［クライアントグループ］のページのグループの一覧表から、削除するグループを選択します。
2. ［タスク］一覧の［削除］をクリックします。
   確認の画面が表示されます。
3. 確認し、問題がなければ、［OK］をクリックします。
   選択したグループが削除されます。

■NFS クライアントグループの編集

1. ［クライアントグループ］のページのグループの一覧表から、編集するグループを選択します。
2. ［タスク］一覧の［編集］をクリックします。
   次の画面が表示されます。



3. 必要に応じて項目を設定します。
   グループ名およびメンバリストを変更できます。
   クライアントの追加と削除は、新規作成時と同様です。
4. ［OK］をクリックします。
   変更内容がコンピュータに適用されます。

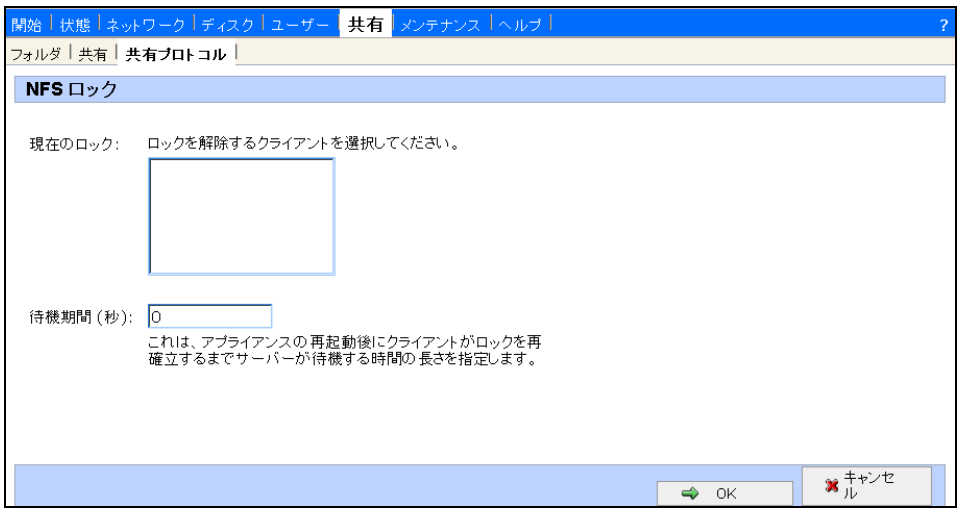
9.8.2 NFSファイルロック

NFSファイルロックを使用すると、ファイル全体またはファイルの一部に排他的にアクセスすることができます。ファイル ロックは、本サーバとクライアントの両方で実現されます。ファイルがロックされると、そのファイルに対してバッファ キャッシュは使用されず、すべての書き込み要求は直ちに本サーバへ送信されます。

システムに障害が発生すると、本サーバは、再起動時にファイルのロック状態を前の状態に復元しようとします。クライアントに障害が発生した場合、本サーバはファイル ロックを解放します。ただし、クライアントの再起動後、少し時間が経過してからファイル ロックは復元要求されます。

NFSロックは次の手順で設定します。

1. プライマリナビゲーションバーから［共有］をクリックします。
2. セカンダリナビゲーションバーから［共有プロトコル］をクリックします。
3. NFSプロトコルを選択し、[プロパティ]をクリックします。NFSサービス画面が表示されます。
4. ［NFSロック］をクリックします。
   ［NFSロック］のページが表示されます。



9.8.3 ユーザーとグループのマッピング管理

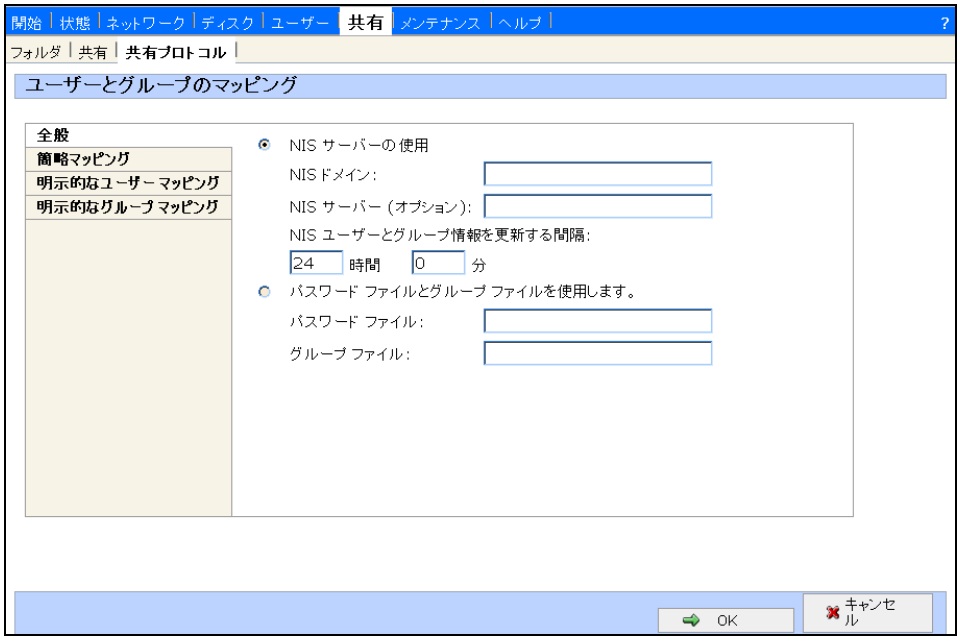
UNIX環境からアクセスされる本サーバ上のファイルのセキュリティを実現するために、NFSプロトコルでは、システム管理者がUNIXユーザーまたはグループ アカウントを、本サーバ上の対応するアカウントに関連付ける必要があります。これによりユーザーは、Microsoft Windowsと同等のアクセス権をUNIX環境において持つことができます。
また、あまり厳格なセキュリティを必要としないWebサイトでは、マッピングを実行せずに、すべてのUNIXユーザーを匿名ユーザーとして扱うことができます。

［ユーザーとグループのマッピング］を使用することにより、以下のように管理できます。

- 両方の環境でユーザーおよびグループ名が異なる場合でも、WindowsユーザーとUNIXユーザーおよびグループ アカウントを関連付けることができます。
- エンタープライズ全体を1つのマッピング データベースで管理できます。
- 同じ名前を持つWindowsアカウントとUNIXアカウントを関連付ける簡略マップを使用できます。
- 異なる名前を持つWindowsアカウントとUNIXアカウントを関連付ける高度なマップを作成し、簡略マップと共に使用することもできます。
- ［ユーザーとグループのマッピング］を使用して、UNIXユーザー、パスワード、およびグループ情報を、1つまたは複数のNIS（Network Information Service）サーバまたはインポートされたパスワードおよびグループ ファイルから取得できます。

［ユーザーとグループのマッピング］は、次の手順で起動します。

1. プライマリナビゲーションバーから［共有］をクリックします。
2. セカンダリナビゲーションバーから［共有プロトコル］をクリックします。
3. NFSプロトコルを選択し、[プロパティ]をクリックします。NFSサービス画面が表示されます。
4. ［ユーザーとグループのマッピング］をクリックします。
   ［ユーザーとグループのマッピング］のページが表示されます。



各タブで、ユーザー管理情報とマッピング方法を設定します。

■ユーザー管理情報

ユーザー管理情報は、［全般］タブで設定します。
NISサーバでユーザー管理をしているかどうかで設定が違いますので、以下の点に注意して設定してください。

●既にNISサーバでユーザー管理が行われている場合

既存のUNIXもしくはLinux環境でネットワークを構築されている場合は、NISサーバがユーザー管理を行っています。

NISはNetwork Information Service の略です。ネットワーク上のすべての計算機で共有すべき情報を提供する目的で用いられます。NISで提供される情報とは、例えば以下のようなものです。

- ログイン名、パスワード、ホームディレクトリ（/etc/passwd）
- グループ情報（/etc/group）

本サーバでは、既存のNISサーバの管理情報をそのまま適応するので、作業は簡単・迅速に行えます。

1. 全般タブの、［NISサーバの使用］ラジオボタンを選択し、［NISドメイン］および［NISサーバ］（これは必須ではありません）を設定します。

●NISサーバを使用していない場合

パスワードファイルおよびグループファイル、いずれもUNIXおよびLinuxマシンの
/etc/passwd, /etc/groupからエクスポートします。
（これらの設定ファイルのパスはディストリビュータによって若干異なる可能性があります。）

1. 既存のUNIXおよびLinuxマシン情報を、あらかじめエクスポートしておきます。
2. ［ユーザーとグループのマッピング］の全般タブで、［パスワードファイルとグループファイルを使用します。］ラジオボタンを選択し、ローカルにインポートしたパスワードファイルとグループファイルのパスを指定します。

ポイント

■/etc/passwd, /etc/groupファイルのエクスポート方法

1. あらかじめ、PRIMERGY FileServer上でNFS共有作業を行っておきます。
2. SU(Super User)権限を持ったユーザーでUNIXまたは、Linuxマシンにログオンします。
3. NFS共有されているフォルダをUNIXまたは、Linuxマシンにマウントします。
4. CPコマンドを使って、/etcから指定のファイルをマウントしたディレクトリにコピーします。

エクスポート作業は以上で終了です。
エクスポート後、上記の手順でPRIMERGY FileServerのWebUIからコピーされた両ファイルを指定します。

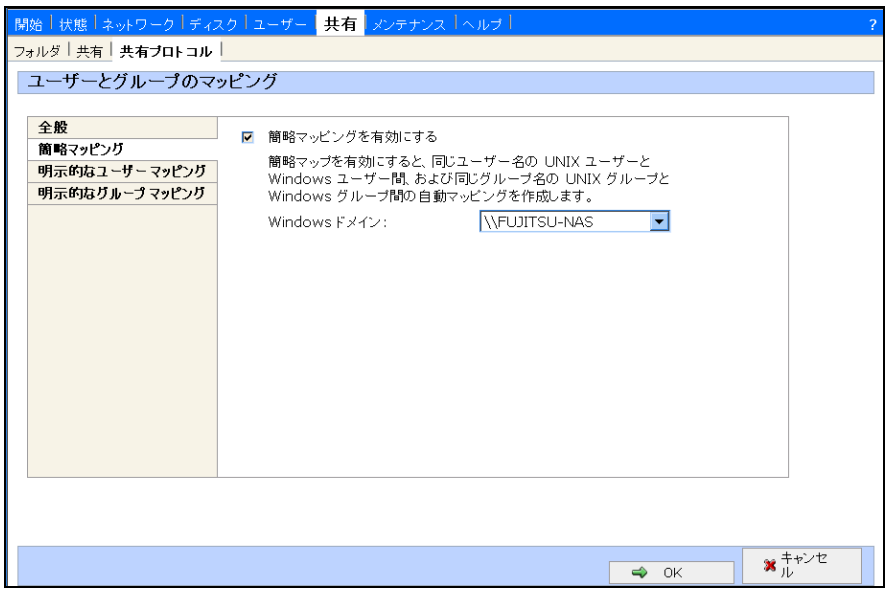
■マッピング方法

マッピング方法には［簡略マッピング］［明示的なユーザーマッピング］［明示的なグループマッピング］の3つのメニューがあります。「9.8.4 簡略マッピング」～「9.8.6 明示的なグループマッピング」をご覧ください。

9.8.4 簡略マッピング

簡略マッピングは、UNIX環境とWindows環境で同一のユーザー名（またはグループ名）を持つユーザー（またはグループ）を、暗黙的にマッピングする方法です。
同一の名前で統合されている環境においては、シームレスな移行作業が行えます。

1. ［ユーザーとグループのマッピング］で［簡略マッピング］をクリックします。
［簡略マッピング］のページが表示されます。

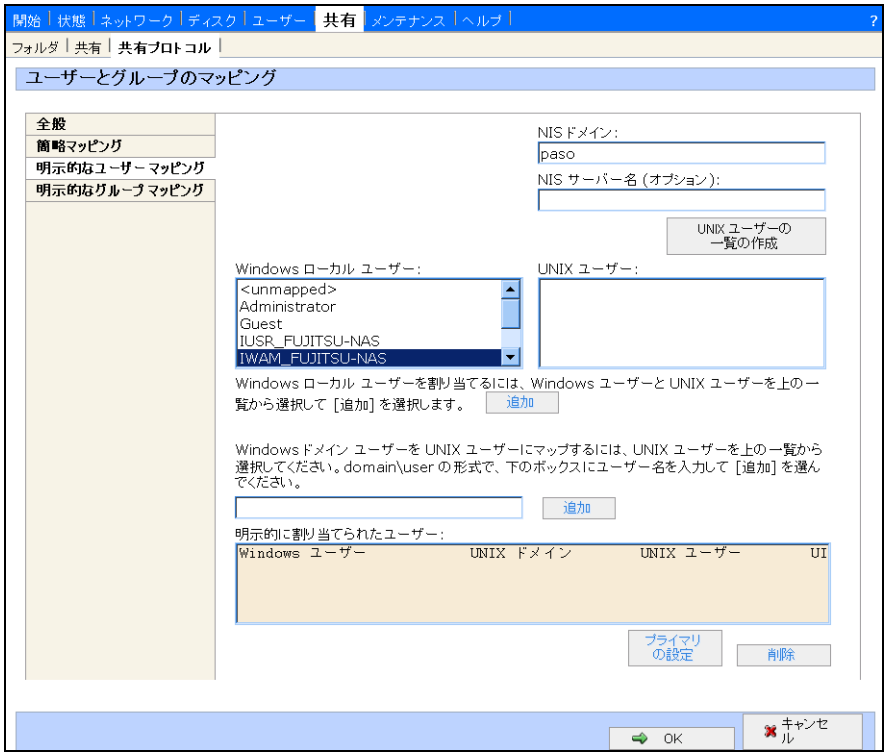


ドメインのプルダウンでは、PRIMERGY FileServerが発見できたドメイン名およびローカルサーバの情報が書き込まれます。（上の図では、ローカルサーバを指定しています。）
本設定を行うためにはNISドメインを指定する必要があります。

9.8.5 明示的なユーザーマッピング

明示的なマッピング方法とは、簡略マップとは異なり、異種OS間のユーザーあるいはグループが同一名で管理されていない場合に、それらの設定を手動で設定する方法です。
［明示的なユーザーマッピング］を使用すると、エンタープライズ全体を1つのマッピング データベースで管理できます。

1. ［ユーザーとグループのマッピング］で［明示的なユーザーマッピング］をクリックします。
   ［明示的なユーザーマッピング］のページが表示されます。



■ユーザーを追加する

1. ［UNIX ユーザーの一覧の作成］ ボタンをクリックして、［UNIX ユーザー］ボックスにすべてのUNIXユーザーを表示します。
2. 各グループからユーザーを選択し、［追加］をクリックします。
   たとえば、DOMAINグループに関連付ける場合は、「DOMAIN¥<ユーザー名>」と入力し、UNIXグループを選択して、［DOMAIN¥<グループ エントリ>］ボックスの横にある［追加］ボタンをクリックします。
   ［明示的に割り当てられたユーザー］ボックスの一覧に、関連付けたユーザーが表示されます。

⚠注意

1つのWindowsドメインのユーザーを複数のUNIXドメインに関連付けることができます。
ただし、1人のUNIXユーザーを複数のWindowsユーザーに関連付けることはできません。

■いずれか1つのマップを特定のユーザーのプライマリ マップとして設定する

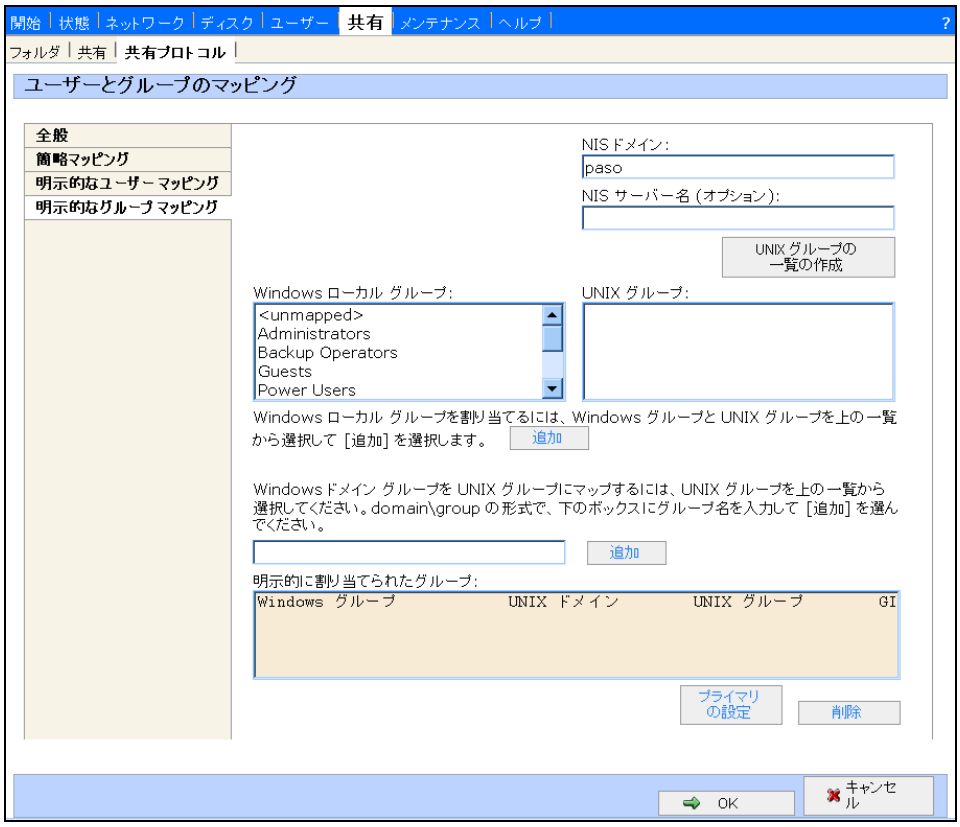
1. ［明示的に割り当てられたユーザー］ボックスの一覧で、マップを選択します。
2. ［プライマリの設定］をクリックします。
3. ［OK］をクリックします。

■明示的なユーザー マップを削除する

1. ［明示的に割り当てられたユーザー］ボックスの一覧で、削除するユーザー マップを選択します。
2. ［削除］をクリックします。
3. ［OK］をクリックします。

9.8.6 明示的なグループマッピング

1. ［ユーザーとグループのマッピング］で［明示的なグループマッピング］をクリックします。
   ［明示的なグループマッピング］のページが表示されます。



図から分かるように、WindowsやUNIXのグループ/ユーザーを明示的に設定します。
これらの情報はドメインから抽出することも可能です。

■明示的なグループマップを作成する

1. ［UNIX グループの一覧の作成］ ボタンをクリックして、［UNIX グループ］ボックスにすべてのUNIXグループを表示します。
2. 各グループからグループを1つ選択し、［追加］をクリックします。
   たとえば、DOMAINグループに関連付ける場合は、「DOMAIN¥<グループ名>」と入力し、UNIXグループを選択して、［DOMAIN¥<グループ エントリ>］ボックスの横にある［追加］ボタンをクリックします。
   ［明示的に割り当てられたグループ］ ボックスに、関連付けたグループが表示されます。

> ⚠注意
> 1つのWindowsドメインのグループを複数のUNIXグループに関連付けることができます。
> ただし、1つのUNIXグループを複数のWindowsグループに関連付けることはできません。

■いずれか1つのマップを特定のグループのプライマリ マップとして設定する

1. ［明示的に割り当てられたグループ］ボックスの一覧で、マップを選択します。
2. ［プライマリの設定］をクリックします。
3. ［OK］をクリックします。

■明示的なグループ マップを削除する

1. ［明示的に割り当てられたグループ］ボックスの一覧で、削除するグループ マップを選択します。
2. ［削除］をクリックします。
3. ［OK］をクリックします。

9.9 FTP共有プロトコル

FTPプロトコル設定では、サービスの開始・停止の実行が可能であると共に、以下の設定が行えます。

- アクセスログの有効化設定
- 匿名アクセスの許可設定
- 接続・切断メッセージの設定

詳細な設定方法はWebUIヘルプなどをご覧ください。

9.10 HTTP共有プロトコル

HTTPプロトコル設定では、以下の設定が行えます。

- IPアドレスの制限
- 使用ポートの設定

詳細な設定方法はWebUIヘルプなどをご覧ください。

9.11　フォルダ

フォルダの作成時には、管理者は詳細なシステム設計ができるようになっています。
ここでは、NTFSの特長とセキュリティについて述べた上で、WebUI上での設定方法を説明します。

9.11.1 NTFSの特長

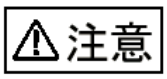
NTFSには、以下の特長があります。

- セキュリティ上の強化
- ドライブ・フォルダを圧縮することができ、ディスクを効率的に使用できる。
- アクセス許可の継承ができ、管理サイドでの有効性が向上する。
- ドライブ毎に使用量の上限（ディスククォータ）を設定することができ、効果的に運用できる。

9.11.2 システムのセキュリティ

ファイルシステムとユーザー管理情報に加えて重要なのがシステムセキュリティです。ここでは、システムセキュリティについて説明します。

本サーバは、Windows 2000のNTFS5を基盤のファイル システムとして使用し、システムのセキュリティモデルとしています。
Windowsで標準的なCIFS共有プロトコルを効果的に運用管理するためには、NTFSのセキュリティの基本的な内容を理解しておくことが重要です。以下ではNTFSセキュリティとCIFSファイル共有プロトコルの関係について説明します。



CIFSは、ファイル システム上に常駐するネットワーク ファイルの共有プロトコルです。
NTFSは、ドライブ システム上に常駐するファイル システムで、ドライブに書き込まれるデータを組織化し、セキュリティを提供します。
CIFSクライアントが、ネットワークを介してリクエストを発行すると、そのリクエストは、サーバのCIFSサービスを通じて処理され、ファイル システムに送信され、データがドライブに書き込まれます。

データをドライブから取得する場合は、ファイル システムとサーバのCIFSサービスを経由して戻され、クライアントに結果を返します。

Windows のファイル システムのセキュリティに関する詳細は、次に示すMicrosoft のWebサイトをご覧ください。

http://www.microsoft.com/

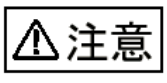
■アクセス制御リスト（ACL）

ファイルシステムのセキュリティを考える上で、アクセス制御リストACL（Access Control List）を理解することが重要です。ACLはファイルへのアクセス権や許可されたアクセスの種類をユーザーやグループに指示する情報を表します。

NTFSファイル システム上の各ファイルには、1つもしくは複数のACLがあります。たとえば、ACLは、ファイルのアクセス権として、ユーザーTaro に読み込みと書き込みを許し、ユーザーJiroに読み込みのみを許し、ユーザーSaburoには、特定のファイルにアクセス権を与えないよう定義することができます。

ACLは、グループに対するアクセス情報を含めることもできるため、作成したグループに所属する全ユーザーに同じアクセス権を適用することも可能です。

NTFS ファイル システム上にある、いかなるファイルやフォルダを選択しても、様々な許可を付与することができます。アクセス権の追加については「9.4.2 CIFS共有」をご覧ください。



ファイルレベルのアクセス制御機能は、WebUIでは提供されません。

9.11.3 割り当て量に上限を設けたスペース利用の管理

ディスククォータというユーザーもしくはグループに対するディスク利用量の制限を行えます。詳細は「第12章　ディスク」をご覧ください。

9.12　アクセス許可の継承のしくみ

親フォルダにアクセス許可を設定すると、そのフォルダに作成された新規ファイルとサブフォルダはこれらのアクセス許可を基本的には継承します。

継承されたアクセス許可により、アクセス許可の管理負担が軽減され、特定コンテナ内の、すべてのオブジェクトのアクセス許可に一貫性が確保されます。

9.13　フォルダの作成方法

フォルダの作成は、以下の手順で行います。

1. プライマリ ナビゲーション バーで、［共有］をクリックします。
2. ［共有］ページで、［フォルダ］をクリックします。

   サーバ配下のドライブ一覧が次のように表示されます。

3. フォルダを新規に作成するドライブをチェックボタンで選択します。

⚠注意

本サーバでは、高可用性・性能が要求されますので、システムディスクドライブには共有ディレクトリを作成しないようにしてください。
リカバリCDを使用したシステムリカバリの場合、システムディスク上のデータは保証されません。

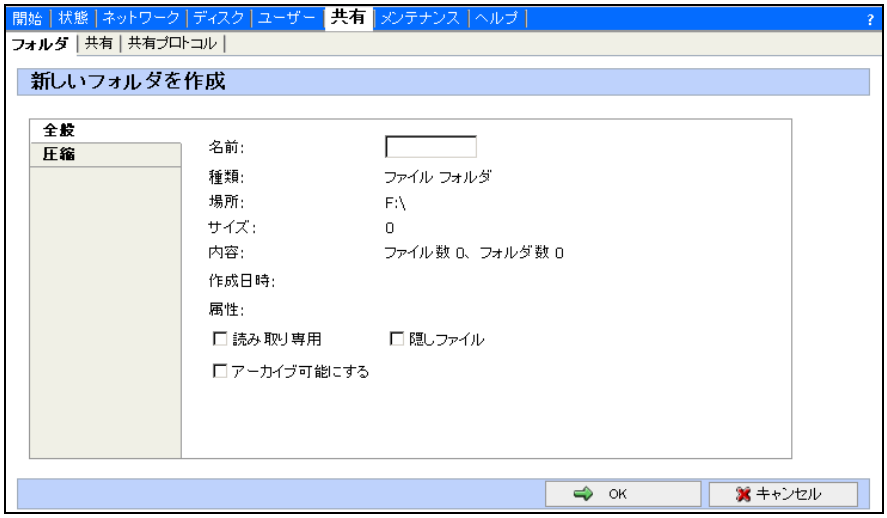
4. ［タスク］一覧で［開く］をクリックします。
ドライブのフォルダ一覧が表示されます。

ここでの実行可能なタスクは、以下の7つです。

項目	説明
上へ	親フォルダに移動します。
新規	新規にフォルダを作成します。 詳しくは、「9.13.1 新規フォルダを作成する」をご覧ください。
削除	フォルダを削除します。 詳しくは、「9.13.2 フォルダを削除する」をご覧ください。
開く	指定したフォルダの配下を閲覧できます。
プロパティ	フォルダの情報を確認できます。 詳しくは、「9.13.3 フォルダの情報を確認する」をご覧ください。
共有	共有を開始します。
共有の管理	「9.5　フォルダ/共有を管理する」をご覧ください。

9.13.1 新規フォルダを作成する

1. フォルダー一覧で［新規］を選択します。
［新しいフォルダを作成］メニューが表示されます。



2. ［全般］タブで、以下の項目を設定します。
— フォルダ名
— フォルダ属性

読み取り専用	：読み取り専用では参照のみ可能です。
隠しファイル	：フォルダをアーカイブ可能にします。

3. ［圧縮］タブをクリックし、必要な項目を設定します。
※［圧縮］タブは、ドライブがNTFSフォーマットされている場合に有効です。
ファイルシステムを変更したい場合は、「第12章 ディスク」をご覧ください。

［圧縮］では、フォルダの内容を圧縮してディスク領域を節約するかどうかと、圧縮の適応範囲の設定を行うことができます。

9.13.2 フォルダを削除する

1. フォルダー一覧で削除するフォルダを選択し、［削除］をクリックします。
削除していいかの確認画面が表示されます。
2. 確認し、削除してもよければ［OK］をクリックします。
選択したフォルダが削除されます。

9.13.3 フォルダの情報を確認する

1. フォルダー一覧でフォルダを選択し、［プロパティ］をクリックします。
フォルダの新規作成画面と同一のものが表示され、同一項目の変更が可能になります。
詳細は「9.13.1 新規フォルダを作成する」をご覧ください。

第10章　PRIMERGY FileServerの様々な使いかた

この章では、PRIMERGY FileServerの代表的な使い方について説明します。

CONTENTS

10.1　共有情報を利用する

Windows系マシンの場合、通常のファイル共有のデータを利用するには、以下の2つの方法があります。

- ネットワークブラウザを使ってサーバを検索する。
- ローカルドライブにマウントする。

ここでは、様々なプロトコルを使って共有を利用するプロセスについて説明します。

10.1.1 ブラウザシステムを使ってサーバを検索する

Windowsマシンでは、Windows エクスプローラを使って簡単にネットワーク上のマシンを検索できます。Windowsエクスプローラおよび検索プロセスに関しては、Windowsのヘルプをご覧ください。

1. 次のいずれかの手順で、Windowsエクスプローラを起動します。
   - ［スタート］→［プログラム］→［アクセサリ］の順にポイントし、［Windowsエクスプローラ］または［エクスプローラ］をクリックします。
   - ［スタート］→［ファイル名を指定して実行］をクリックします。
     表示されたダイアログの［名前］欄に「explorer」と入力し、［OK］をクリックします。
2. Windowsエクスプローラのアドレスバーに、以下のように入力します。

   ¥¥(PRIMERGY FileServer名/IPアドレス)

   ※アドレスバーが表示されない場合は、［表示］メニューの［ツールバー］から［アドレスバー］をチェックしてください。

   サーバが検索されると、共有一覧が表示されます。

上記の方法で成功しない場合は、以下の方法で検索できます。

1. Windowsエクスプローラから［検索］アイコンをクリックし、「コンピュータの検索」を選択します。
2. コンピュータ名またはIPアドレスを指定し、［検索］ボタンをクリックします。

この方法で接続できない場合は、貴部門ネットワーク管理者にお問い合わせください。

⚠注意

出荷時のIPアドレス構成10.0.0.2で検索した場合、環境によっては発見できない可能性があります。
その時は、ローカルなハブとクライアントを一台の環境で、WORKGROUPを構成します。
クライアントのネットワーク環境は以下のように設定してください。

IPアドレス：10.0.0.XX
サブネットマスク：255.255.255.128

10.1.2 ネットワークドライブを割り当てる

ネットワークドライブの利点は、ローカルドライブと同じ操作感で、簡単にサーバのリソースを利用できる点にあります。
特に利用頻度の高いネットワークリソースは、ネットワークドライブとして割り当てるとたいへん便利です。

1. Windowsエクスプローラを起動します。
2. ［ツール］メニューの［ネットワークドライブの割り当て］をクリックします。
3. ［ドライブ］リストボックスで、共有リソースに割り当てるドライブ文字を選択します。
4. ［フォルダ］ボックスに、サーバとリソースの共有名を入力します。
   ［参照］をクリックしてリソースを検索することができます。
   入力時には¥¥<サーバ名>¥<共有名>という書式を使用します。
5. ［完了］をクリックします。

⚠注意

- ログオンするたびに割り当て済みドライブに再接続するには、［ログオン時に再接続する］チェックボックスをチェックします。
- 接続先のサーバが利用できない場合は、割り当て済みドライブも基本的には使えません。
  （ただしオフラインフォルダの場合は一時的に使用することは可能です。）
- 割り当て済みドライブに別のドライブ文字を割り当てることもできます。この場合は、そのドライブとの接続を終了して、新しいドライブ文字を割り当てます。

10.1.3 分散ファイルシステムを利用して、統合的なリソース管理を行う

たとえば、ネットワークドライブをマウントする場合、ドライブ文字の制限があるため、他に有用なリソースが存在しても、最大26台以上のリソースしかマウントすることができません。

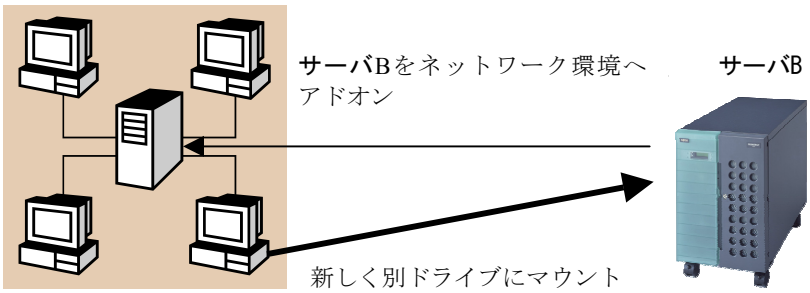
このような事態を防ぐためにネットワーク管理者は、あらかじめ拡張性を持たせたネットワーク設計を行う必要があります。しかし、ハードウェアリソースの問題により、現実的にはベストな解決をはかるのはとても難しいことです。

しかし、分散ファイルシステムを使うことで、これらの問題点を解消することが可能です。
分散ファイルシステムは、ネットワーク上に点在する様々なリソースへのショートカットを提供するWindows 2000の機能です。
詳細な機能はWindowsのヘルプをご覧ください。

分散ファイルシステムを利用することで、ユーザーの利便性は飛躍的にあがります。

●これまでのファイル共有

サーバAがクライアントに対して、ファイル共有を行っています。
ここにPRIMERGY FileServer（ここではサーバBとします）をネットワーク環境へアドオンすると、以下の図のようになります。

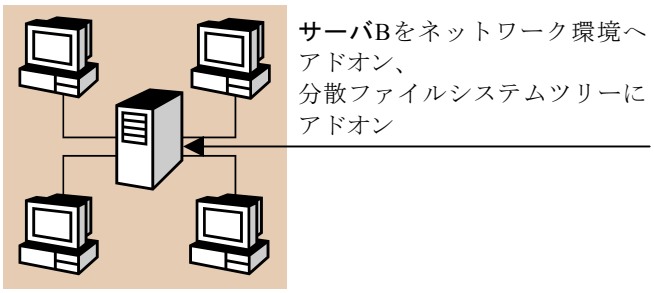


クライアント側では、サーバBのリソースを使う場合は、新たに、別ドライブにサーバBのリソースを、以下のように直接マウントする必要があります。

```
+¥¥ServerA¥ShareA
+¥¥ServerB¥ShareB
```

●分散ファイルシステムを利用したファイル共有

サーバAがクライアントに対して、ファイル共有を行っています。
ただし、ここでサーバAは分散ファイルシステムのルートとします。
（分散ファイルシステムの詳細についてはWindowsのヘルプをご覧ください。）
ここにPRIMERGY FileServer（ここではサーバBとします）をネットワーク環境へアドオンするとともに分散ファイルシステム傘下にアドオンします。



分散ファイルシステムに参加したことで、サーバAの共有の配下にサーバBの共有フォルダへのショートカットが追加されるので、クライアント側では、新たに共有ドライブの割り当てをする必要はありません。

```
+¥¥ServerA¥ShareA
  |- ShareB
```

⚠注意

- ServerB¥ShareBへのアクセス権がないユーザーは接続できません。
- PRIMERGY FileServerが分散ファイルシステムルートになることも可能です。

10.2　IISと連携する

Internet Information Server（以下IIS）はMicrosoft標準のWebサーバ機能を提供します。
以下ではIISのWebデータサーバとして、PRIMERGY FileServerを使った場合の手順を明記します。

IIS自体の設定に関しては、Windowsで［スタート］→［プログラム］→［管理ツール］→［インターネットサービスマネージャ］の順にクリックし、設定が行えます。
IISの詳細な説明に関しては、Windowsのヘルプをご覧ください。

> **⚠注意**
>
> **データベース処理は同期が必要となる場合が多く、外部記憶装置との連携処理では信頼性が問題になります。Webページでデータベース処理を組み合わせた運用には、PRIMERGY FileServerをご利用されませんようお願いします。**
>
> **以下の説明は、Webコンテンツのデータ領域としてPRIMERGY FileServerをお使いになるための設定方法です。**

10.2.1 仮想ディレクトリを利用する

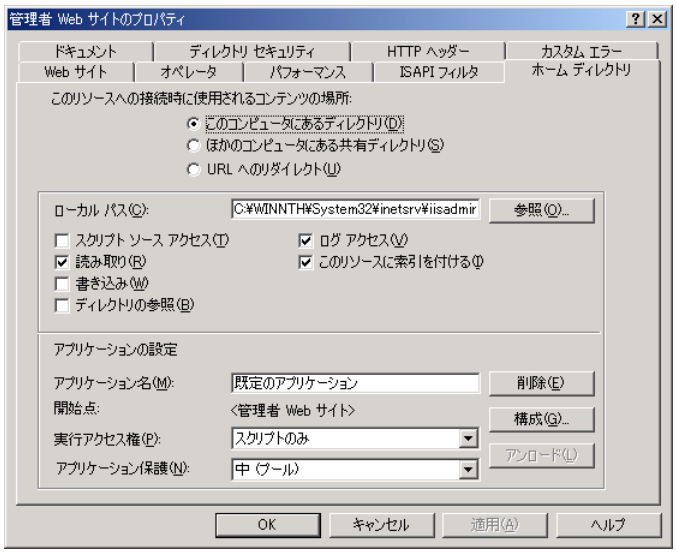
仮想ディレクトリとは、実際のWebツリーに仮想的にマウントしたディレクトリのことです。
通常、IISはシステムドライブに構成されます。
例）c:¥InetPub¥wwwroot

しかし、様々なリソースをwwwroot配下に配置すると、雑多になるばかりでなく、リソースのアクセスも階層が深くなるにつれてパスが長くなるという欠点があり、管理上問題があります。仮想ディレクトリは、これらの問題を解決するために、IIS上のディレクトリ構成上直下に仮想的にディレクトリを配置する機能です。

この機能を使い、PRIMERGY FileServer側でWebデータを参照するには、以下の手順で行います。

1. **PRIMERGY FileServer側でWebデータを保存するための共有フォルダを作成し、共有を開始します。**
2. **IISサーバ（Webを提供するサーバ）側で、ネットワークドライブのマウントを行います。**
3. **IIS管理コンソールから、新規作成→仮想ディレクトリを実行します。**
   仮想ディレクトリ作成ウィザードが起動します。
4. **必要事項を入力します。**

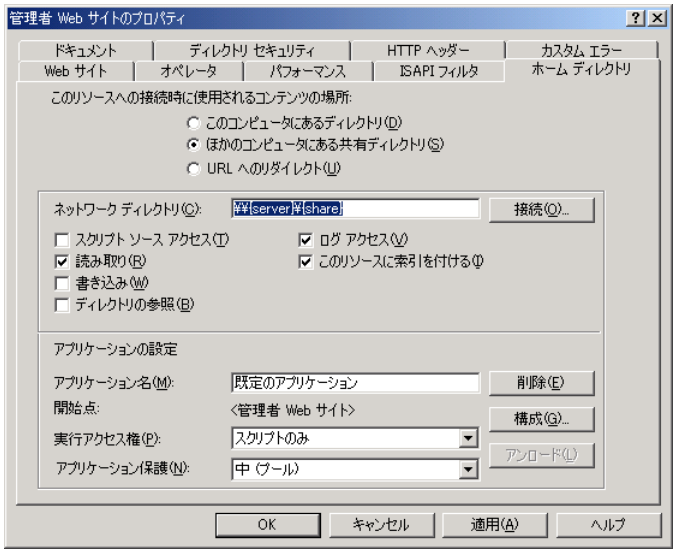
5. プロパティから、次の設定タブを表示します。



6. 「このコンピュータにあるディレクトリ」にチェックを付けます。
7. ローカルパスの指定を、マウントしたPRIMERGY FileServerの共有フォルダパスに変更します。

10.2.2 共有ディレクトリをそのまま使う

1. PRIMERGY FileServer側でWebデータを保存するための共有フォルダを作成し、共有を開始します。
2. IISサーバ側で、ネットワークドライブのマウントを行います。
3. IIS管理コンソールから、新規作成→仮想ディレクトリを実行します。
   仮想ディレクトリ作成ウィザードが起動します。
4. 必要事項を入力します。
5. プロパティから、次の設定タブを表示します。



6. 「ほかのコンピュータにあるディレクトリ」にチェックを付けます。
7. サーバ名と共有名を¥¥Server¥shareの形式で指定します。

⚠注意

設定時には、アカウントとパスワードを入力する必要があります。ドメインに参加している場合は、ドメインコントローラで認証されているユーザーアカウント情報で接続してください。
また、Webコンテンツの改竄などの問題に備えて、接続には一意なユーザーアカウントのみを許可するように設定してください。

10.3　UNIX/Linuxソフトウェアと連携する

UNIXおよびLinuxのソフトウェアは、各ディストリビューションにより設定方法が異なる可能性がありますので、設定の際には、各ソフトウェアのマニュアルをよく読んでから実行してください。

UNIXおよびLinuxのデータバックエンドとして利用する場合は、以下の手順で行います。

1. プライマリナビゲーションバーで、［共有］をクリックします。
2. セカンダリナビゲーションバーで、［共有プロトコル］をクリックし、NFS サービスが実行されていることを確認します。
3. UNIX/Linuxマシンでコマンドを実行して、ファイル共有が可能か確認します。
   以下は、Linuxのコマンド例です。

   ```
   showmount –e PRIMERGY FileServer名
   ```

4. 共有フォルダが確認できたら、Web/mailデータをマウントします。
   以下は、Linuxのコマンド例です。

   ```
   mount　–t　nfs　PRIMERGY FileServer名:/エクスポート名　自サーバ/マウント先
   ```

   以下はSoralisのコマンド例です。

   ```
   mount　–F　nfs　PRIMERGY FileServer名:/エクスポート名　自サーバ/マウント先
   ```

⚠注意

- mount、showmountコマンドの詳細なパラメータの意味は、各ソフトウェアのマニュアルをご覧ください。
- メールの保存先は、一般には/var/mailですが、ディストリビューターによって若干違う可能性があります。各ソフトウェアのマニュアルをよく読んでから、設定を行ってください。

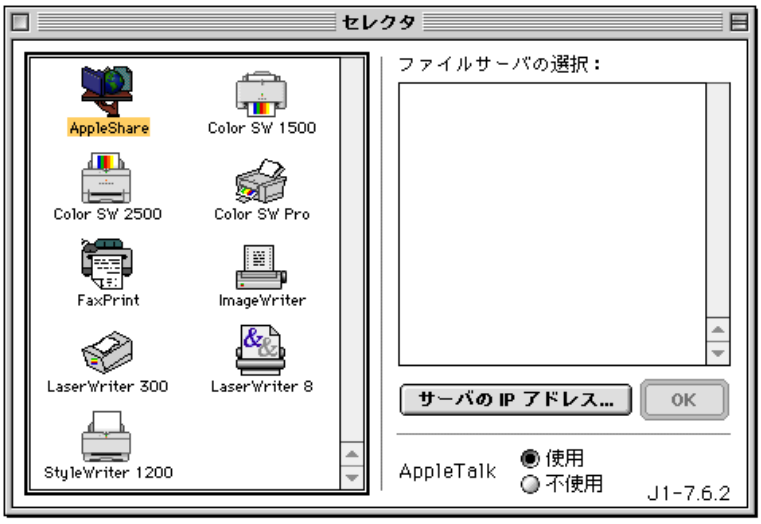
10.4　Apple Macintoshから使う

Apple MachintoshからPRIMERGY FileServerのコンテンツを利用するには以下の様に共有ディスクに接続します。
以下ではMacOS8.6を使った例を示します。
MacOSのバージョンに依っては、接続方法に若干の違いがある可能性があります。詳しくはApple Machintosh添付の説明書を良く読み設定して下さい。

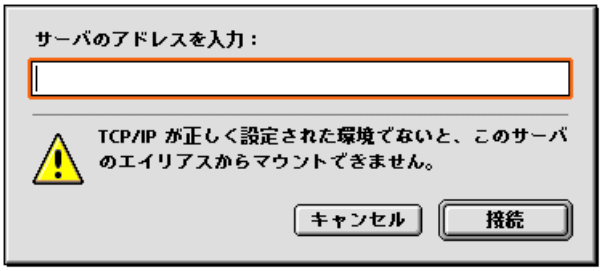
ポイント

- TCP/IPの設定が、正しく行われていることを確認下さい。
  アップルメニューの［コントロールパネル］から［TCP/IP］を選択すると、TCP/IP設定設定画面が表示されます。
- あらかじめ、Apple Macintosh用の共有フォルダをPRIMERGY FileServer上で作成しておく必要があります。

1. アップルメニューから、［セレクタ］をクリックします。
2. 一覧の中からAppleShareを選択します。



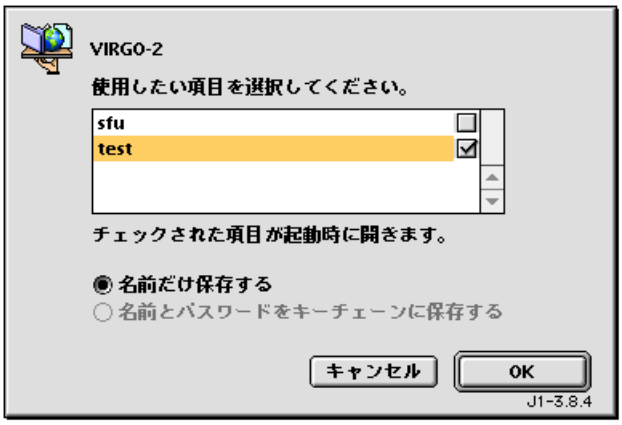
3. ［サーバのIPアドレス］ボタンをクリックします。
4. PRIMERGY FileServerのIPアドレスを指定します。



共有フォルダに接続するための認証画面が表示されます。

5. 接続のための、ID名とパスワードを入力し、［接続］をクリックします。

6. PRIMERGY FileServerに接続が完了すると、解放されている共有フォルダを指定することができます。
利用したいフォルダを指定し、［OK］をクリックします。



7. 画面上にPRIMERGY FileServerへのエイリアスが作成されたことを確認してください。

第11章　バックアップ&リカバリ

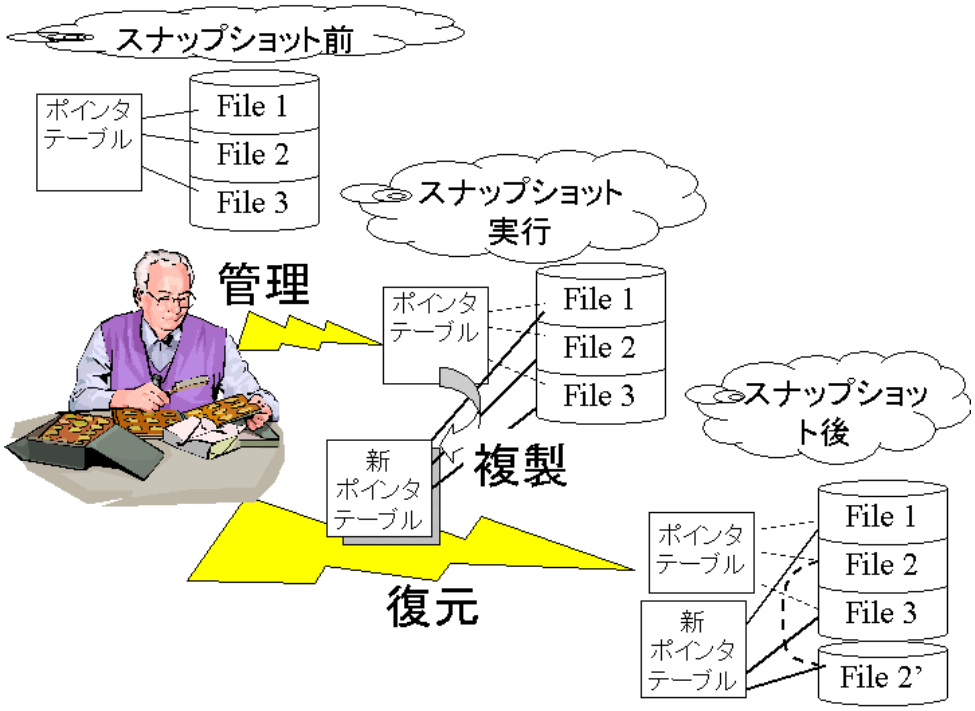
この章では、本サーバにおけるバックアップとリカバリに関する基本的な知識と手段について説明します。

CONTENTS

11.1　固定記憶域

11.1.1 固定記憶域とは？

PRIMERGY FileServerでは、スナップショットと呼ばれる仮想ディスクの複製を、短時間で作ることができます。スナップショットにより、物理的にデータをコピーしなくても、業務運用データの仮想的な複製を簡単に作成することができるため、様々な目的に使用することができます。
スナップショットの概念図を以下に示します。



ファイルシステムでは、すべてのファイルはポインタテーブルとして管理されています。
これを模式的な図で考えると、図の左上のファイル1・2・3の様に、ファイルシステムのポインタテーブルがドライブの状態を管理していることになります。

スナップショットは、この現在の管理しているポインタテーブルの複製を取得することを意味します。
複製された新しいポインタテーブルは、これからのドライブ状態の管理を、複製元のポインタテーブルは、これまでのドライブ状態の管理を行います。

このように、2つ以上のポインタテーブルを作成することで、新しくファイルが更新されたとしても、古いファイルの修正・編集を行うことができるのです。
例えば、スナップショット後に、図の右下の様にファイル2が更新された時（「File 2'」で表しています)、新ポインタでは新しいファイルを操作することができますが、ファイル2の状態に戻すことはできません。

ここで復元オペレーションを行うと、スナップショットで採取したポインタテーブルが復元され、元のファイル2の状態に復帰することが可能なります。

スナップショットは、このようにファイルポインタの複製を採取する為、通常のバックアップが苦手とするオープンファイルのバックアップも可能となります。
復元されたデータは、読み書きができる通常の物理ドライブとまったく同じように機能します。
しかし、スナップショットは、本質的に、短期間で数時間前のデータへ復元できる、一時的措置として考えるべきです。スナップショットの作成詳細については、以降の節をご覧ください。

PRIMERGY FileServer上でのスナップショットにより保護されたデータのことは、瞬間的に固定化されたディスク状態を指していますので、以下「固定記憶域」と呼び、その固定記憶域を管理するプログラムを「固定記憶域マネージャー」と呼びます。

固定記憶域マネージャーは、固定記憶域を、1回限りのイベントあるいは繰り返しのイベントとしてスケジュールすることができます。
作成されたボリュームの固定記憶域は、元のボリュームにディレクトリとして表示されます。このイメージのアクセス権は、元のボリュームから継承されます。イメージは、従来のシステム ボリュームと同様に使用されます。ただし従来のボリュームとは異なり、スナップショットが作成された時点の元のボリュームの正確な内容に復元することが可能です。
固定記憶域マネージャーおよび重大な障害からの復元システムは、Microsoft® Windows® Schedulerに完全に統合されており、定期的な固定復元イメージの作成とローテーションをすべて自動的に管理することができます。

最初に、出荷時状態からお客様の運用形態に応じて、固定記憶域マネージャーを使用して、システム リソースの使用、最適化、および固定記憶域の管理を制御する方法を説明し、次に、固定記憶域の作成方法などについて説明します。

11.1.2 固定記憶域マネージャーのボリューム構成

固定記憶域マネージャーがボリューム単位で固定記憶域を作成することについてはすでに説明しました。固定記憶域マネージャーは、キャッシュファイル領域をボリュームに確保し、その領域を利用しデータをサブフォルダ形式に展開しています。
ボリューム構成の設定では、ボリュームに関連する以下の設定に関して運用環境に応じて、値を設定することができます。
また、本設定は[規定値を復元]ボタンをクリックすることで、出荷時の設定に戻すことができます。

名称	説明
警告しきい値に達する要因	システム イベント ログに警告メッセージを書き込む条件となるキャッシュ領域の使用率を定義します。
イメージを削除する要因	システム上の最も古い固定記憶域を自動的に削除する条件となるキャッシュ領域の使用率を定義します。固定記憶域の自動削除は、システム ログに記録されます。
キャッシュサイズ	キャッシュ ファイルに割り当てられる領域の大きさを指定します。

なお、キャッシュサイズ値を大きくすると、より大きな固定記憶域をより多く管理できるようになりますが、固定記憶域が格納されているドライブのディスク容量を消費します。大きな値を設定する場合は、十分な空き領域があることを確認してください。

11.1.3 スナップショットのおすすめ取得例

スナップショットは、一時的なデータの退避です。短時間で簡単に作成できるのでスナップショットがもたらす利点は多大です。
以下に特長をまとめます。

- 失ったファイルやディレクトリを早急に復旧する際使用できます。
- バックアップソフトが苦手とするオープンファイルのバックアップも行えます。
- 実際のデータに影響させることなく、重要なデータを使用した新しいアプリケーションのテストが行え、データのバックアップ源としても利用可能です。
- スナップショットは、データの一時的なバックアップであり、恒久的なデータを意図した構造にはなっていません。このためバックアップ作業は常に必要となります。
- スナップショットは、各仮想ディスク単位で作成できます。
- スナップショットは、読み取り専用（リード オンリー)、または、読み書きが可能です。
- スナップショットは、仮想ディスクと同じ原則に従った共有が可能です。
- スナップショットは、本質的に一時的なデータとしての使用を意図した設計で作られています。
- プール領域が不足すると、スナップショットを自動的に削除します。
- キャッシュの同一性が確保できないので、システムディスクのリカバリは実現性が低くなります。

⚠注意

スナップショットを利用する際、データを変更する頻度や、各仮想ディスクで維持しているスナップショットの数によっては、仮想ディスクの性能に影響を与えることがあります。お客様サイドで仮想ディスクサイズなどを変更する場合は、運用環境およびヘルプなどを御熟読の上、変更頂けますよう、お願いいたします。

これらの特長を踏まえ、以下の様なスナップショットの使い方を推奨いたします。

■システムディスク

いわゆる惨事復旧という形での復元はできません。オプションソフトであるARCServe2000などをご利用になりシステムバックアップすることをおすすめいたします。詳細に関しては「11.2 バックアップ」をご覧ください。

また、システムディスクではWindows 2000の標準的な機能であるシステムモジュールの監視を行っており、システム状態を含めたリストアが必須になります。この点からもシステムディスクの固定記憶域化はおすすめできません。

■データディスク

サーバデータのご利用の仕方に大きく依存しますが、一般に変更頻度の高い共有フォルダを含むボリュームを固定記憶域マネージャーで管理させるのは、とても効果的です。
管理者は、あらかじめサーバリソースの用途を考慮したボリューム作成を行うことで、簡単にかつ短期間で、信頼性の高いシステムを構築することができます。

11.1.4 固定記憶域の自動作成計画

固定記憶域はその性質から、スケジューリングされた規則によって自動採取することをおすすめします。
以下は1つの管理案です。

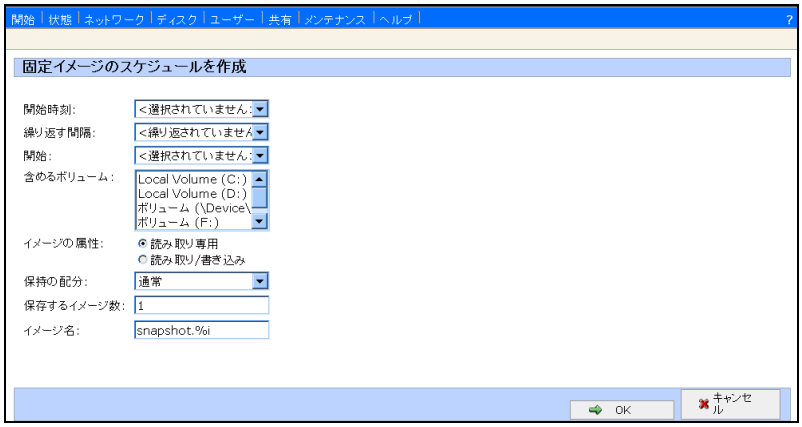
① サイクリックで通常レベル採取する。一日のスナップショットスケジュールは以下の時間で採取します。
0時、6時、12時、18時の一日4回採取します。
② 週末には取得レベル高のスナップショットを週単位で取得します。

このイメージ取得法は、設計に基づいたディスクキャッシュ量に大きく依存する部分があるので、あくまでも一つの案です。また、固定記憶域は一時的なものであるため、バックアップは定期的に行ってください。

11.1.5 固定記憶域の自動作成を行う

固定記憶域を自動作成するには、以下のように行います。

1. プライマリ ナビゲーション バーで、[ディスク] をクリックします。
2. セカンダリ ナビゲーション バーで、[固定記憶域マネージャー] をクリックします。
3. [スケジュール] をクリックします。
4. [タスク] ボックスの一覧で、[新規] をクリックします。
   次の画面が表示されます。



5. スケジュールに必要な以下のパラメータを設定します。

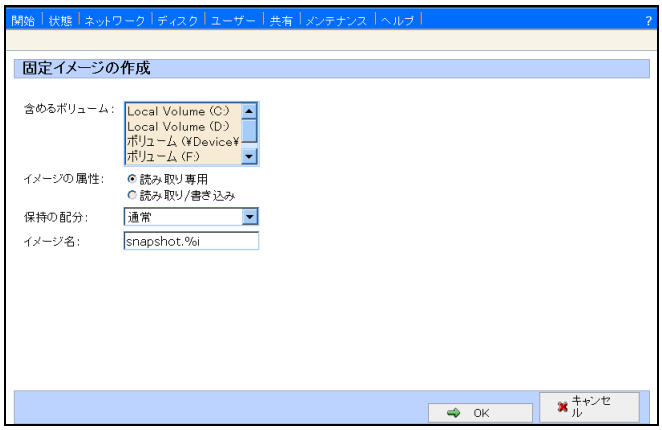
名称	説明
開始時刻	固定記憶域を作成し始める時間を指定します。
繰り返す間隔	固定記憶域の作成間隔を規定します。 時間・日・週単位で指定することが可能です。
開始	固定記憶域を作成し始める日時を指定します。
含めるボリューム	固定記憶域を作成するボリュームを指定します。 プルダウンメニューから択一で選択します。
イメージの属性	作成された固定記憶域の属性を指定することができます。 書き込みを許可した場合のみ、スナップショットで取得されたデータに対して再修正することができます。
保持の配分	保持レベルを指定することができます。 この配分を上げることで採取・削除対象の優先度を指定できます。
保存するイメージ数	ここで保存する固定記憶域数を定義します。
イメージ名	ここで保存する固定記憶域名を定義します。 %iで自動採番されます。

6. ［OK］をクリックします。
固定記憶域が作成され、リストに作成時間を含めたイメージ情報が反映されます。
イメージリストの削除に際しては、複数イメージの削除はできません。

11.1.6 固定記憶域を手動で作成する

固定記憶域を手動で作成するには、以下のように行います。

1. プライマリ ナビゲーション バーで、[ディスク] をクリックします。
2. セカンダリ ナビゲーション バーで、[固定記憶域マネージャー] をクリックします。
3. [固定イメージ] をクリックします。
4. [タスク] ボックスの一覧で、[新規] をクリックします。
   次の画面が表示されます。



5. 次の表を参考にして、固定記憶域情報を入力します。

名称	説明
含めるボリューム	固定記憶域を作成するボリュームを指定します。 プルダウンメニューから択一で選択します。
イメージの属性	作成された固定記憶域の属性を指定することができます。 書き込みを許可した場合のみ、スナップショットで取得されたデータに対して再修正することができます。
保持の配分	保持レベルを指定することができます。 この配分を上げることで採取・削除対象の優先度を指定できます。
イメージ名	ここで保存する固定記憶域名を定義します。 %Iで自動採番されます。

6. [OK] をクリックします。
   固定記憶域が作成されます。

11.1.7 スナップショットデータを復元する

固定記憶域データを復元するには、以下の手順で行います。

1. プライマリナビゲーションバーで、［ディスク］をクリックします。
2. セカンダリナビゲーションバーで、［固定記憶域マネージャー］をクリックします。
3. ［固定イメージの復元］をクリックします。
4. 復元するイメージを選択します。
5. タスクリストから、［復元］を選択します。

11.1.8 特記

オプション製品であるARCServe2000をご使用のお客様は、固定記憶域データをバックアップする場合は以下の点に留意してください。

- 固定記憶域データはボリューム全ての内容を保持しています。このため、ボリュームのフルバックアップと外部メディアにデータを保存する場合は、ディスク容量と同じ容量が必要となります。
- 変更のあった差分や増分バックアップといった、データの蓄積を行うことは固定記憶域マネージャーではできません。
  しっかりしたバックアップを必ず行ってください。

固定記憶域マネージャーには以下の注意事項があります。

- 固定記憶域マネージャーを使った場合、保存領域としてディスク容量を消費します。
- キャッシュ量が制限値を越えると警告が発生します。警告メッセージの削除の仕方は　第5章　を参照ください。この警告メッセージは、スケジュールされてない場合にも発生します。特に、監視ソフトを使っている場合は、イベントのフィルタリングをしてください。
- 固定イメージの時間ソートは正しく行われません。

11.2　バックアップ

バックアップはサーバの運営上必須な管理作業になります。本サーバには、データを瞬間的に保存するスナップショットによるデータのバックアップと、通常のバックアップの形式があります。スナップショットによるデータのバックアップは、「11.1 固定記憶域」をご覧ください。

バックアップはお客様の大切なデータを紛失から保証するための機能です。
本サーバでは、4種類のデータバックアップ方法を例として提案しています。

11.2.1 バックアップの種別と特徴

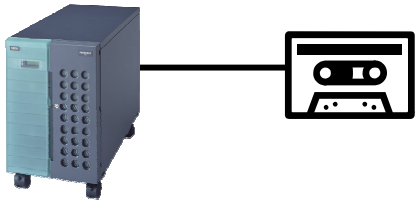
バックアップ計画は、本サーバの設置運用環境の様々なパラメータが依存してきますので、ここでは一般的なおすすめパターンのみを提示します。よりきめ細かな条件でバックアップを実行したい場合は、オプション製品のARCServeのヘルプをご覧ください。
本サーバには次の4種類のデータバックアップ方法が考えられます。

①本機の他のサーバにバックアップフォルダを作成する。

利点：	リソースを浪費しません。
欠点：	ネットワークトラフィックに大きな影響を与えます。

②本サーバ機に、外部記憶装置を用意し、テープバックアップを行う。

利点：	バックアップソフトウェアのソリューションで管理でき、確実にデータを保管できます。
欠点：	バックアップ・リストアに時間が掛かります。



③固定記憶域ディレクトリをテープメディアにバックアップする。

利点：	バックアップには時間がかからず、確実にある時点のバックアップデータが取得できます。
欠点：	リストアに時間がかかり、メディア量が大量に必要となります。

④ 自機データバックアップを自機内に作成する。

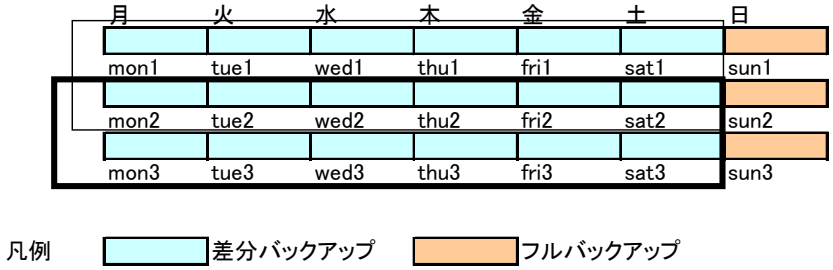
利点：	短時間で多くのデータを保管できます。
欠点：	リソースを多く浪費し、耐障害性に欠きます。

それぞれ長所・短所を兼ね備えていますが、リソース量と利便性、確実性を考えて、推奨は①から④の順番になります。

11.2.2 バックアップのスケジューリング

バックアップジョブは、月・週・および時刻を指定することが可能です。以下に推奨取得案を示します。

週間バックアップの取得例

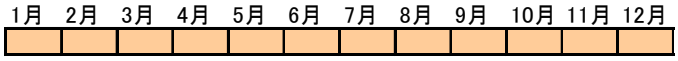


■週間バックアップのサイクル

月曜日～土曜日までは、データを午前2時（サーバのトランザクションの低い他の時間でも構いません）に差分バックアップで取得します。このデータは一週間保存します。

日曜日は午前0時からフルバックアップを実行します、このデータは、一ヶ月間保存します。
（フルバックアップはデータ量に依存しますので、開始時刻などは、データ量を考慮して変更してください。）

また毎月第1日曜日に取得されたフルバックアップデータは、その月のデータとして別ディスクに一年間保存します。
（上図では、sun1に相当）



11.2.3 バックアップ案

これまで、バックアップの種別とスケジュールについてご提案させていただきました。ここでは管理するデータからみたバックアップ方法に関してご提案します。

■システムパーティション

1. 毎週末にフルバックアップを行いこれを一ヶ月間保存します。
2. 保存データはディスク破損に備えて外部バックアップメディアに保存します。

■拡張パーティション

1. ウィークディでスナップショットのバックアップを取得します。
2. バックアップデータの信頼性を要求する場合はテープへ保存します。
3. 統合バックアップ装置がある場合は、ネットワーク経由でのバックアップも可能です。
4. 毎週日曜日にスナップショットデータのフルバックアップを実行し、これを一ヶ月間テープに保存します。
5. 毎月第1日曜日のテープに取得したフルバックアップデータは一年間保存します。

11.2.4 バックアップの実行

バックアップの取得方法に関しては、オプション製品のARCServe2000の取扱説明書をよく読み、上記の様なバックアップ戦略を考案し実行してください。

11.2.5 システムパラメータのバックアップ

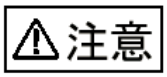
PRIMERGY FileServerのWebUIでは、Web画面を通じて設定されたパラメータに関して、バックアップして保守時に活用することが出来ます。
システムパラメータのバックアップ機能は、以下の場合に有用です。

- システムパラメータを初期化したい場合
- リカバリ時の早期復旧の場合

取得できるパラメータ情報に関しては、「第14章　保守機能について」をご覧ください。

パラメータバックアップを実行するには以下の手順で行います。

1. プライマリナビゲーションバーから［メンテナンス］を選択します。
2. セカンダリナビゲーションバーから［バックアップ／リストア］を選択します。
3. メニューから［バックアップ］を選択します。
   PRIMERGY FileServerの設定情報が取得され、ダウンロード了解のダイアログが表示されます。
4. ［OK］をクリックし、設定情報をバックアップしてください。



システムパラメータの設定情報は、管理者のマシンなど、PRIMERGY FileServerとは別の場所に保存しておくことをお勧めします。
これによって、リカバリ時に有効に利用することが出来ます。

11.3　リカバリ

システムや、データの破壊に伴うリカバリ作業は、非常にコストのかかる作業です。
リストアはサーバの復帰作業上必須な管理作業になります。本サーバはデータを瞬間的に保存するスナップショットによるデータのバックアップと、通常のバックアップの形式があります。スナップショットによるデータのバックアップ・復旧方法は「11.1.7 スナップショットデータを復元する」をご覧ください。

11.3.1 リカバリの種別と方法

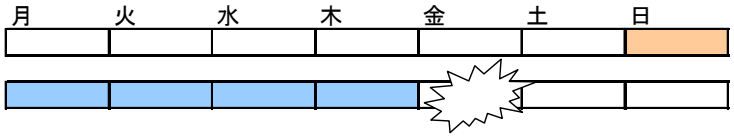
大きく分けて、4種類のリカバリを行う場合があります。

①OS リカバリ

システムパーティションはミラーリングされた設定で出荷されておりますが、故障により復旧できない場合があります。この時は新しいHDDを挿入の上、システムを出荷時設定に戻すリカバリCDを挿入してシステム状態を戻してください。詳細に関しては「第14章　保守機能について」をご覧ください。

②惨事リカバリ（フルデータリカバリ）

なんらかのハード的な故障により、データが完全に崩壊したときは、以下の手順でデータの復旧を行います。ただし、この復旧案は先に提案したようにバックアップがきちんと採取されているという前提にたっています。



1. 一番最近に行ったフルバックアップデータを用意し、これを復旧します。
2. 最新状態への復旧へは、増分バックアップが無事な（外部装置によるデータ保存や、他のネットワークドライブへの保存を行った）場合は、順に（上の図であれば月曜日の増分バックアップから）復旧します。

以上の手順で、データをフルリカバリすることができます。詳細な手順などについては、添付ソフトウェアの説明書をご覧ください。

③データリカバリ-指定したフォルダおよびファイルのリカバリ-

ARCServe2000では、特定のフォルダやファイルの復旧作業を行うことができます。
復旧希望日がわかっている場合は、そのデータファイルを指定し、復旧します。
詳細な方法については、添付ソフトウェアの説明書をよく読み、オペレーションを行ってください。

④システムパラメータの復旧

本サーバでは、WebUIを経由して設定したシステムパラメータを情報ファイルとして保存しておくことができます。
復旧できるシステムパラメータの種類や、復旧方法については、「第14章　保守機能について」をご覧ください。

第12章　ディスク

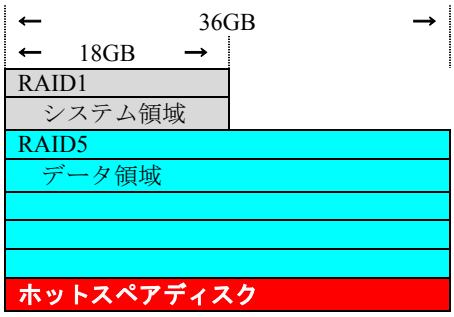
この章では、本サーバのディスクシステムに関する、基本的な知識と操作方法について解説しています。

CONTENTS

12.1　設計コンセプト

本サーバは最大1.7Tバイトまでの容量拡張が可能ですが、初期導入の時点でのディスク見積りが成り立っていない場合、最大構成での購入の必要はありません。
管理者は、現状のディスク使用量とユーザー数・ネットワークトラフィック数を見極めた上で、ディスクの増設を行ってください。

出荷時はハードウェアRAIDシステムを用いて、以下の基本構成で出荷しております。ホットスペアディスクはデータ領域専用です。



8本のディスクをRAID1およびRAID5で構成し、RAID1をシステム用として、RAID5をデータ用とする領域を作成しております。
このためディスク増設時のパーティショニングコンセプトは、ハードディスクキャビネットのディスクに対する操作になります。

12.1.1 ハードディスクキャビネットのディスク構成

本サーバに接続したハードディスクキャビネットには、13本のHDDを格納することができます。スロット13と14はスペアディスク専用スロットです。また、スロット12にはディスクを挿入しないでください。

追加ディスクは、ディスク1本単位での購入が可能ですが、RAID5での拡張を考えるとディスク3本以上で増設してください。
*なお、接続・設定に際してはPRIMERGY S30添付の取扱説明書を参照して下さい。

たとえば、以下のような構成図になります。

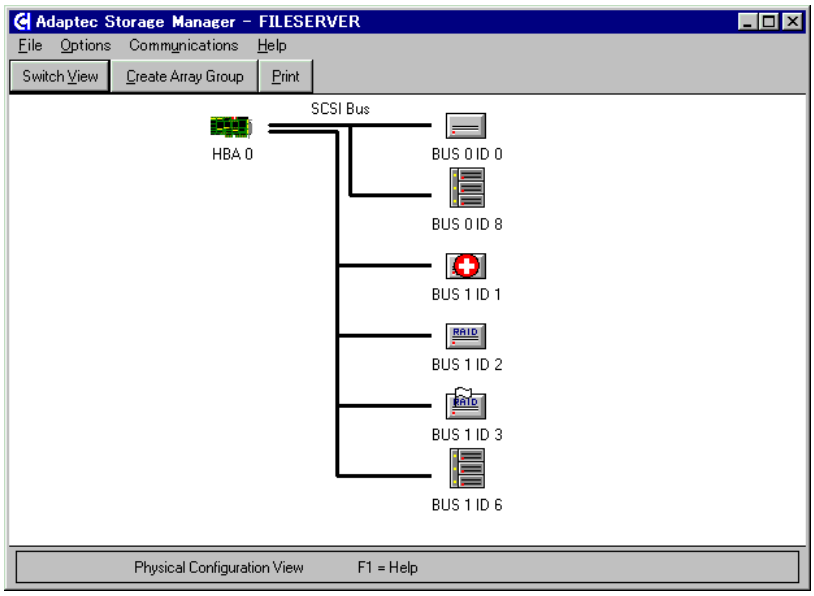
ハードディスクキャビネット 構成略図

12.2　Storage Managerを実行する

本サーバでは、Adaptec Storage ManagerというRAID管理ツールを採用しています。Adaptec Storage ManagerはWebUIから操作できます。

1. プライマリナビゲーションバーから［ディスク］をクリックします。
2. ［Adaptec Storage Manager］をクリックします。
3. 管理者アカウントおよびパスワードを入力し、ログオンします。

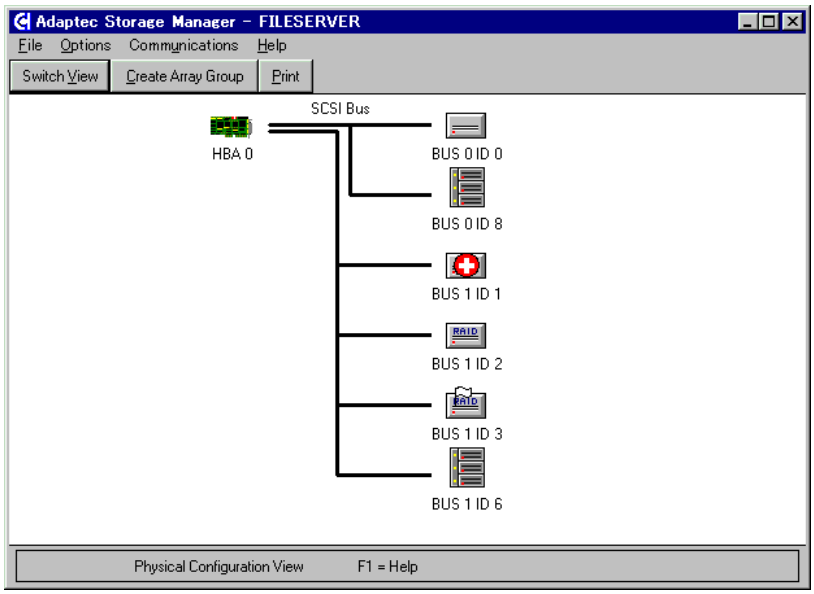
※本ツールはターミナルサービスを経由して起動されます。
次の画面が表示されます。



画面の概要については、「12.2.1 Physical Configuration View」、「12.2.2 Logical Configuration View」を参照してください。
詳細な機能に関しては、Adaptec Storage Managerのヘルプを参照してください。

12.2.1 Physical Configuration View

Adaptec Storage Managerで最初に表示されるウィンドウは、Physical Configuration Viewです。このウィンドウには、システムにインストールされたアレイコントローラが、接続された機器とともに表示されます。



下記以外のアイコンが表示される場合、機器が正しく接続されていません。サーバ本体の電源を切断して接続を再度確認してください。
アイコンの詳細については本製品添付のSCSIアレイコントローラカードの取扱説明書（「付録A.1 アイコン一覧」）を参照してください。

SCSIコントローラ

ハードディスク

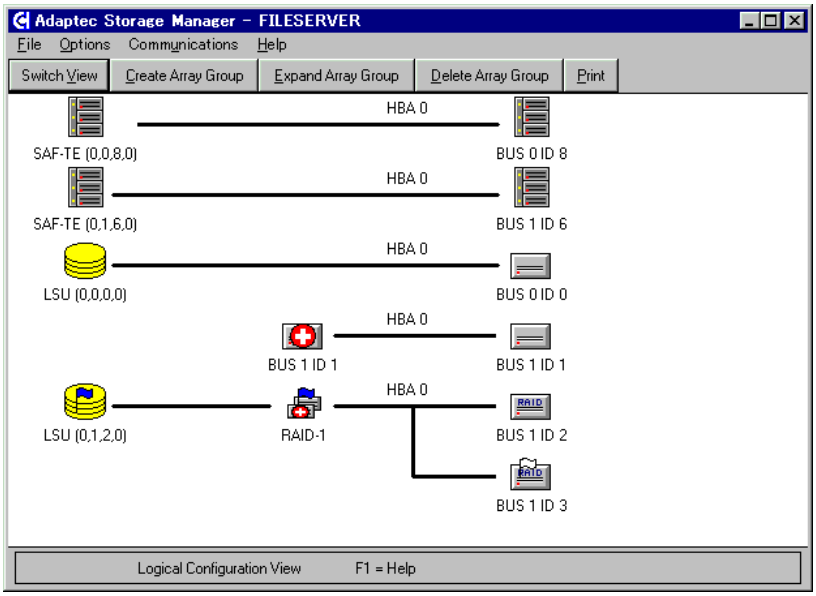
SAF-TE

このウィンドウでは、以下の機能が使用できます。

ボタン	機能
Switch View	Physical Configuration Viewと Logical Configuration Viewを切り替えます。
Create Array Group	ディスクアレイを作成します。 本製品添付のSCSIアレイコントローラカードの取扱説明書（「5.6.1 アレイグループの作成」）を参照してください。
Print	構成情報を印刷します。
コントローラおよび各装置のアイコン	ダブルクリックすると、それぞれの情報が表示されます。

12.2.2 Logical Configuration View

［Switch View］をクリックすると、Logical Configuration Viewウィンドウに切り替わります。
Logical Configuration Viewウィンドウの右側には、アレイコントローラに接続されているすべての機器が表示されます。ウィンドウの左側には、各機器に対応する論理ドライブの情報が表示されます。



ハードディスクは、個別ドライブまたはアレイの構成要素として表示されます。いずれの場合も、ハードディスクまたはアレイは、論理ストレージユニット（LSU:Logical Storage Unit）としてウィンドウの左側に表示されます。マルチレベルRAIDを構成するアレイは、RAID 1アイコンで表され、左側のLSUアイコンと右側のドライブアイコンの間に表示されます。
論理機器アドレスは、Logical Configuration Viewウィンドウの論理機器やLSUのアイコンの下に、括弧付きで表示されます。

項目	内容
HBA	HBA（ホストバスアダプタ）。 機器が接続されているコントローラです。PCIバスのスキャンにより、検出された順に番号が割り当てられます。
BUS	機器が接続されているSCSIバス。
Device ID	その機器のユニークなID。 アレイの場合は、そのアレイを構成するドライブの中の最も値の小さいIDです。
LUN	その機器のロジカルユニット番号（Logical Unit Number）。 通常は0です。

このウィンドウでは、以下の機能が使用できます。

ボタン	機能
Switch View	Physical Configuration Viewと Logical Configuration Viewを切り替えます。
Create Array Group	ディスクアレイを作成します。 本製品添付のSCSIアレイコントローラカードの取扱説明書（「5.6.1 アレイグループの作成」）をご覧ください。
Expand Array Group	ディスクアレイの容量を拡張します。
Delete Array Group	ディスクアレイを削除します。
Print	構成情報を印刷します。
アレイグループおよび各装置のアイコン	ダブルクリックすると、それぞれの情報が表示されます。

12.3 アレイまたはディスクステータスを確認する

アレイやディスクステータスを確認するには、各コントローラや機器のアイコンをダブルクリックします。そのコントローラや機器の情報を示すInformationウィンドウが表示されます。

アレイコントローラは、アレイやハードディスクのステータスをレポートします。いくつかのステータスは、ハードディスクやアレイのアイコン上に、ステータスフラグで示されます。
より詳細なステータス情報を確認するには、そのハードディスクまたはアレイのInformationウィンドウを表示します。ステータス条件の変化はイベントログに記録されます。

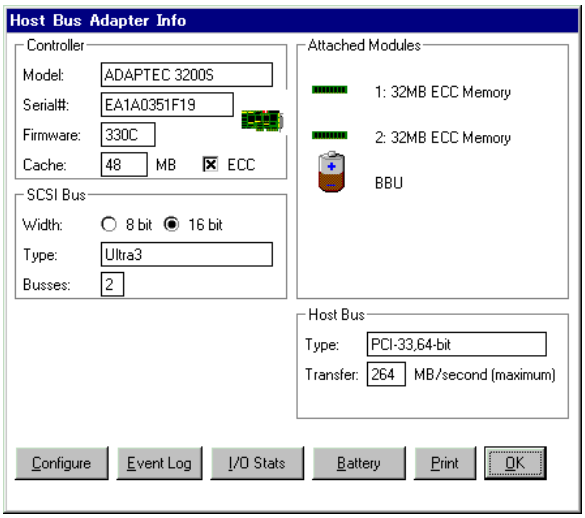
以下の表は、ハードディスクやアレイについて表示される一般的なステータス（状態）の一覧です。実際のステータスメッセージには、さらに詳しい情報が追加される場合があります。

ステータス	状態
Building	アレイの初期化中です。
Created	アレイまたは機器が定義されていますが、初期化されていません。
Dead	アレイ内の複数台のハードディスクが故障しました。この状態から回復することはできません。
Degraded	アレイ内の1台のハードディスクが故障しました。アレイのパフォーマンスが低下しています。
Impacted	アレイのベリファイを実行しています。I/Oパフォーマンスに影響があります。
Optimal	アレイは完全に機能しています。
Pending	アレイは作成済みであり、コントローラによる初期化処理が待機中ですが、まだ開始されていません。 （ステータスの下に表示されます。）
Reconstructing	アレイのリビルド中です。

12.3.1コントローラに関する情報を確認する

1. Physical Configuration Viewで、コントローラのアイコンをダブルクリックします。

Host Bus Adapter Infoウィンドウが表示されます。
このウィンドウでは、コントローラからレポートされる構成情報が表示されます。



項目	内容
Controller	コントローラのモデル、シリアル番号、ファームウェアおよびキャッシュメモリの量が表示されます。ECCは、ECCメモリが搭載されている場合にチェックされます。
Attached Modules	拡張モジュールに関する情報が表示されます。
SCSI Bus、Host Bus	コントローラおよび各バスの仕様が表示されます。

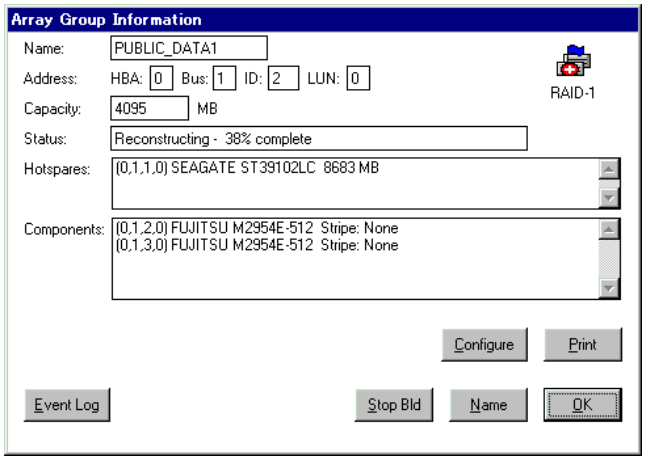
また、アレイコントローラに対し、以下のコマンドを実行することができます。なお、現在の構成や状態により、表示されるボタンが異なります。

ボタン	機能
Configure	キャッシュの設定確認および設定変更を行います。
Event Log	発生したイベント一覧を表示します。
I/O Stats	I/O統計情報を表示します。
Battery	バッテリバックアップモジュールの情報表示および設定変更を行います。
Print	表示されている情報を印刷します。
OK	ウィンドウを閉じます。

12.3.2 アレイに関する情報を確認する

1. Logical Configuration Viewウィンドウで、アレイグループのアイコンをダブルクリックします。

Array Group Informationウィンドウが表示されます。



※ マルチレベルRAIDの構成要素であるアレイのInformationウィンドウを表示するには、それらのアレイのアイコンをダブルクリックします。

Array Group Informationウィンドウには、次の情報が表示されます。

項目	内容
Name	そのアレイに割り当てられた名前が表示されます。ウィンドウの右上隅のアイコンはRAIDレベルを示します。
Address	オペレーティングシステムがアクセスするために使用する論理機器アドレスが表示されます。
Capacity	アレイで使用できる総ストレージ容量（MB）が表示されます。
Status	コントローラからレポートされるアレイのステータスが表示されます。
Hotspares	ハードディスクが故障した場合にアレイを保護するために使用できるホットスペアの一覧を表示します。
Components	アレイを構成する機器の論理アドレス、機種、およびストライプサイズを表示します。マルチレベルRAIDのInformationウィンドウの場合、一覧に表示されるのはマルチレベルRAIDの構成要素である各アレイのアドレス、名前およびストライプサイズです。

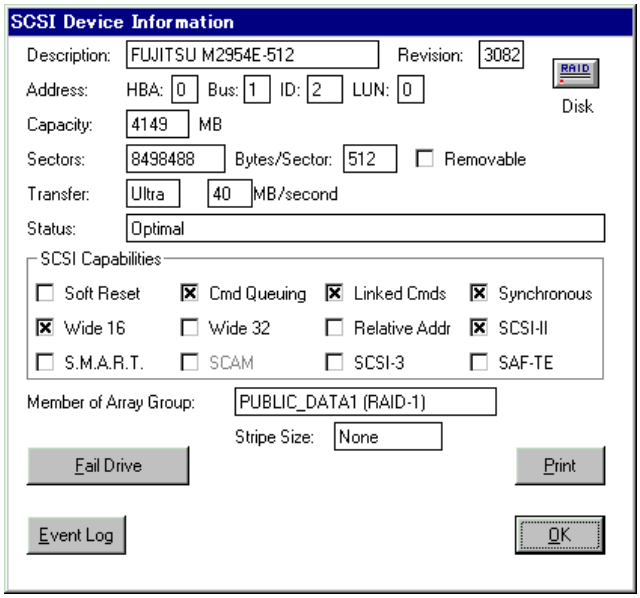
また、アレイに対し、以下のコマンドを実行することができます。なお、アレイの現在の構成や状態により、表示されるボタンが異なります。

ボタン	機能
Configure	設定確認および設定変更を行います。
Event Log	発生したイベント一覧を表示します。
Verify	アレイグループのベリファイを実行します。
Name	アレイグループに名前を付けます。
Rebuild	アレイのリビルドを実行します。 故障したハードディスクを含む冗長アレイで、ホットスペアがない場合に表示されます。
Build	初期化待機中のアレイに対し、初期化を実行します。 初期化待機中のアレイの場合に表示されます。
Stop Bld	アレイの初期化またはリビルドを中断します。 初期化中、リビルド中のアレイの場合に表示されます。
Stop Vfy	ベリファイを中断します。 ベリファイを実行しているアレイの場合に表示されます。
Print	表示されている情報を印刷します。
OK	ウィンドウを閉じます。

12.3.3 SCSI機器に関する情報を確認する

1. Physical Configuration Viewで、ハードディスクやSAF-TEのアイコンをダブルクリックします。

SCSI Device Informationウィンドウが表示されます。



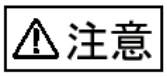
このウィンドウでは、ハードディスクやSAF-TEに関する情報の表示や、設定を行います。

SCSI Device Informationウィンドウには、次の情報が表示されます。

項目	内容
Description	製造元と機種が表示されます。
Revision	ドライブのファームウェアのバージョンが表示されます。
Address	機器の論理アドレスが表示されます。
Capacity	機器のストレージ容量（MB単位）が表示されます。
Stautus	機器の現在のステータス。一般的なステータス（Optimal以外）も、機器のアイコン上にカラーフラグで示されます。
SCSI Capabilities	その特定のSCSI機能をサポートしている場合に「x」マークが表示されます。
Member of Array Group	その機器が属すアレイの名前とRAIDレベル、およびそのアレイのストライプサイズが表示されます。機器のタイプにより、表示されるボタンが異なります。

また、ハードディスクに対し、以下のコマンドを実行することができます。なお、ハードディスクの構成や状態により、表示されるボタンが異なります。

ボタン	機能
Configure	キャッシュの設定確認および設定変更を行います。
Event Log	発生したイベント一覧を表示します。
I/O Stats	I/O統計情報を表示します。
Format	ハードディスクをローレベルフォーマットします。
Make Hotspare	ホットスペアを設定します。
Remove Hotspare	ホットスペアを解除します。
Redirect	ハードディスクのBus/IDのリダイレクトを行います。
Fail Drive	アレイを構成するのハードディスクを強制的に切り離します。
Print	表示されている情報を印刷します。
OK	ウィンドウを閉じます。



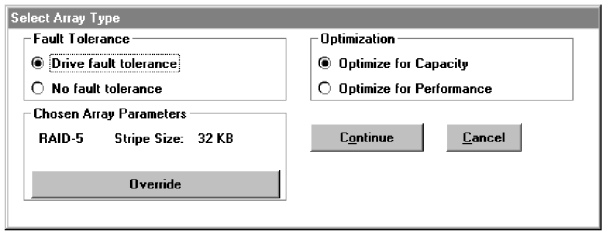
「Fail Drive」ボタンは、担当営業員に指示されるような特別な場合以外は、使用できません。

12.4　アレイグループを作成する

本製品は、RAID 0、1または5のディスクアレイを実現します。また、複数のRAID 1を統合して、マルチレベルRAIDを作成できます。これらのアレイグループは、サーバ側から単一の論理ストレージユニット（LSU）として認識されます。
アレイ内のハードディスクは、すべて同じコントローラに接続されている必要があります。アレイコントローラは、選択された順番にハードディスクを使用してアレイが初期化されます。

アレイグループを作成するには、以下の手順で行います。

1. ［Create Array Group］をクリックします。
   次の画面が表示されます。



2. ［Fault Tolerance］の中で、「Drive fault tolerance（RAID 1または5）」または「No fault tolerance（RAID 0）」を選択します。
   「No fault tolerance（RAID 0）」を選択した場合、手順4.へ進んでください。
3. 「Drive fault tolerance」を選択した場合、Optimizationで、「Optimize for Capacity（RAID 5）」または「Optimize for Performance（RAID 1）」を選択します。
   Chosen Array Parametersに、RAIDレベルとストライプサイズが表示されます。
   ストライプサイズはアレイのタイプにより自動的に設定されます。
   （RAID 0の場合は128KB、RAID 5の場合は64KBとなります）。

⚠注意　ストライプサイズは変更しないでください。

4. 「Continue」をクリックして、使用するハードディスクを選択します。
   ※アレイを作成する場合は、原則として同一型名（同容量、同回転数）のハードディスクを使用してください。
   Logical Configuration Viewウィンドウが、「Choosing Drives for Array （RAID n）」というタイトル文字付きで表示されます（nは、選択されたRAIDレベルです）。

5. アレイを構成するハードディスクを以下の方法で追加、削除します。

— ハードディスクの追加

追加する各ハードディスクをクリックしてマーキングします。緑色のチェックマークは、ハードディスクが選択されていることを示します。マーキングしたハードディスクを新規アレイグループに追加する場合は、「Include Drive」をクリックします。

— ハードディスクの削除

削除するハードディスクのアイコンをクリックし、「Remove Drive」をクリックします。ハードディスクの選択時に、一部のハードディスクが青色で表示される場合があります。これは、構成を変更しないとそのハードディスクをアレイに追加できないことを示しています。さらに多くのハードディスクを選択してアレイに追加するか、1台または複数のハードディスクをアレイから削除する必要があります。

6. 新規アレイグループに追加または削除するハードディスクを選択し終わったら、[Done] をクリックします。

変更内容を保存して初期化処理を開始するまで、そのアレイグループのアイコンのフラグは黒色になります。

7. アレイを作成し終わったら、Storage Managerを終了します。

※［File］メニューから［Set System Configuration］を選択すると、Storage Managerを終了せずに初期化を開始できます。

構成の変更を保存する確認のウィンドウが表示されます。

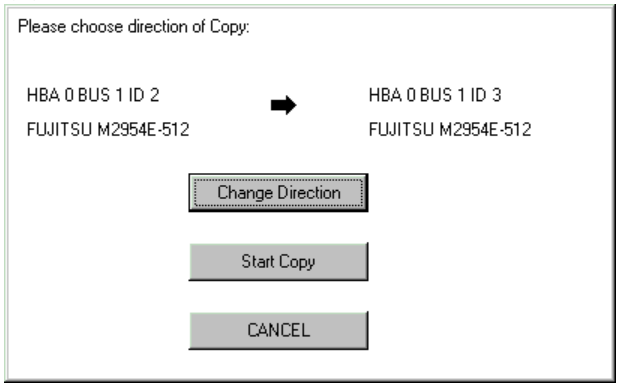
8. 構成を保存します。

初期化処理が自動的に開始されます。

※ 複数のアレイを作成した場合、それらのアレイは、一度にひとつずつ、作成された順番に初期化処理が行われます。

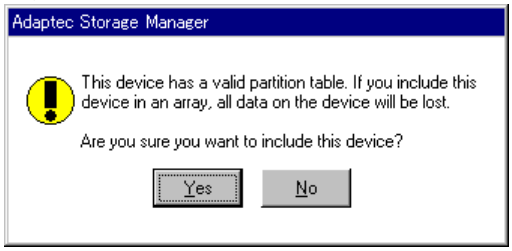
ポイント

- RAID 1アレイを作成する場合、一方のハードディスクからデータをもう一方のハードディスクにコピーします。
  RAID 1アレイを指定した場合は以下の図の矢印ボタンでコピーの方向を設定します。



ポイント

- 大規模な冗長アレイの場合は、初期化処理が完了するまで時間がかかることがあります。初期化処理の実行中でもStorage Managerを終了すればすぐに使用可能になります。
- 初期化開始時に次のようなダイアログが表示されることがあります。この場合、アレイグループを構成しようとしているハードディスクにファイルシステムに関する情報が書き込まれています。消去しても問題ないときのみ初期化を行ってください。初期化を開始すると、元のデータは消去され、既存のデータは復元できません。



- 初期化処理の進行状況をモニタする場合は、そのアレイグループのArray Group Informationウィンドウを表示します。Statusフィールドに、初期化の進行状況が表示されます。また、マルチレベルRAIDの構成要素となっているアレイのInformationウィンドウを表示して、初期化処理の進行状況をモニタすることもできます。

12.5 アレイグループを削除する

アレイグループを削除するには、以下の手順で行います。

1. ［Logical Configuration View］ウィンドウで、削除するアレイのLSUまたはアレイグループアイコンを選択し、［Delete Array Group］をクリックします。
2. 確認メッセージが表示されたら、［OK］をクリックします。
   アレイグループを削除せずに終了する場合は、［Cancel］をクリックします。

アレイが実際に削除されるのは、Storage Managerを終了して変更内容の保存を選択したときか、［File］メニューから［Set System Configuration］を選択したときです。

12.6　容量を拡張する

システム稼動中に、RAID 0アレイまたは RAID 5アレイに1台または複数のハードディスクを追加して、ストレージ容量を増やすことができます。ハードディスクが追加されると、コントローラはデータをアレイに配置し直します。このとき、LSUの最後に空き容量が追加され、システムで認識される論理ドライブのサイズが増えます。

容量の拡張は、NTFSを使用するアレイに対してのみ使用できます。FATファイルシステムでは使用できません。

⚠注意

- ディスクアレイの構成が変更されるような操作を行う場合は、事前にデータをバックアップしておくことをお勧めします。
- アレイの容量拡張処理中は、システムのパフォーマンスが大幅に低下する場合があります。
- 容量の拡張を開始する前のアレイのステータスは、Optimalである必要があります。
- アレイステータスがOptimalでない場合は、既存のアレイをリビルドした後、エクスパンドを続行してください。
- アレイに新しく追加される各ハードディスクは、アレイ内のハードディスクと同一型名（同容量、同回転数）のものを使用してください。

容量の拡張は、以下の手順で行います。

1. 追加するハードディスクを挿入します。
2. Storage Managerを起動し、［Switch View］をクリックしてLogical Configuration Viewに切り替えます。
3. 「RAID 0」アイコンまたは「RAID 5」アイコンをクリックして、ハードディスクを追加するアレイグループを選択します。
4. ［Expand Array Group］をクリックします。
5. アレイに追加するハードディスクアイコンをクリックしてマーキングします。
   緑色のチェックマークはそのハードディスクが容量拡張の対象となることを示しています。
6. 「Inculde Drive」を選択します。
   マーキングされたハードディスクが既存のアレイグループに結合されます。
   追加されるハードディスクにはNewとマーキングされます。
7. ハードディスクを選択し終わったら「Done」をクリックします。
   容量拡張処理が開始されるまで、そのアレイグループのアイコンのフラグは黒色になります。
8. 「File」メニューから「Set System Configuration」を選択します。
   容量拡張処理が開始されます。
   処理中はそのアレイグループのステータスフラグが青色に変わります。
9. 容量拡張処理が完了した後、システムを再起動します。
   追加したスペースがシステム上で認識されます。
10. 容量を拡張した後、プライマリナビゲーションバーで、［ディスク］をクリックします。
11. セカンダリナビゲーションバーで、［ディスクとボリューム］をクリックします。

12. ディスクアドミニストレータを使用してアレイのボリュームセットに空き容量を追加し、システムをシャットダウンして再起動します。

ポイント

- 容量拡張処理の進行状況をモニタする場合は、Storage Managerを使用してArray Group Informationウィンドウを表示します。容量拡張の処理中のステータスはExpandingで、処理が完了するとOptimalになります。
- 容量拡張処理中にドライブが故障すると、問題が修正されるまで対象のアレイグループはDegraded状態になります。そのアレイのホットスペアがある場合は、リビルドを自動的に開始します。ホットスペアがない場合は、故障したハードディスクを交換して、アレイのリビルドを実行してください。
  容量拡張処理中にサーバ本体（およびキャビネット）の電源を切断しないでください。
  容量拡張処理中でもシステムでは通常の処理を実行できます。
- 大規模なアレイの場合や他のI/O処理が実行されている場合は、容量拡張処理が完了するまでに時間がかかる場合があります。
- 再起動時にWindowsのchkdskが実行され、新しく作成された領域が検査される場合があります。大きなアレイの場合は、この検査に時間がかかる場合があります。

12.7 アレイのリビルドを行う

RAID 1アレイまたはRAID 5アレイのハードディスクが故障し、そのアレイにホットスペアが用意されていない場合は、以下の手順でアレイをOptimal状態にします。

1. 「付録B.4.3 内蔵ハードディスクユニットの取り付け／取り外し」に記載されている手順で、故障したハードディスクを交換します。
2. ハードディスクを交換し終わったらStorage Managerを起動してLogical Configuration Viewを選択します。
3. アレイグループのアイコンをダブルクリックしてArray Group Informationウィンドウを開きます。
4. Array Group Informationウィンドウで「Rebuild」をクリックすると、リビルド処理が開始されます。
   — リビルド処理が進行中であれば、そのハードディスクのアイコンに白色のフラグが表示されます。
   — アレイとLSUのアイコンには、青色のフラグが表示されます。
   — リビルドの進行状況は、Array Group Informationウィンドウに表示されます。
5. リビルドが完了するとフラグが消え、アレイステータスがOptimalになります。

ポイント

ホットスワップ可能なハードディスク（SCA-2対応）をご使用の場合、故障ドライブを交換するだけで自動的にリビルドが開始されます（Storage Managerは必要ありません）。

12.8　ディスクの検査を行う

ディスクの検査は「ベリファイ」で行います。
ベリファイはRAID 1アレイとRAID 5アレイに対して冗長情報の整合性を検査します。この処理は、通常のシステム処理と並列で実行されます。ユーザーによる操作やサーバによる処理は不要です。

アレイのデータの検査を開始するには、Array Group Informationウィンドウで［Verify］を選択します。冗長データに不整合が見つかった場合は、それらを整合させることができます。
ベリファイの動作は、RAIDレベルにより次のようになります。

レベル	機能
RAID 0	ディスクメディアのECCチェックを行います。
RAID 1	ミラードライブペアがセクタごとに比較され、両方のハードディスクに含まれるデータが同一であるかどうかを検査します。
RAID 5	パリティが再計算され、ハードディスクに格納されているパリティ情報と比較します。

ポイント

通常の状態ではデータの不整合は発生しません。しかし、電源障害などでアレイの書き込み処理が中断された場合には、不整合が発生している可能性があります。

12.9　アレイグループを新しく命名する

アレイグループやマルチレベルRAIDにユニークな名前を割り当てるには、Array Group Informationウィンドウの［Name］ボタンをクリックします。
この名前は、アレイアイコンの下や、その他のアレイを識別する場所に表示されます。
この名前には最大13文字まで使用できます。

12.10　ホットスペアディスクを作成する

ホットスペアディスクを作成すると、RAID1アレイで発生した障害時に自動的に対応することができます。アレイに割り当てられていないハードディスクをホットスペアに割り当てることができます。ホットスペアは、RAID 1（または0+1）アレイで故障したハードディスクの自動交換用に確保されています。

ホットスペアで保護されているアレイでハードディスクが故障すると、コントローラは自動的にホットスペアを使用して、データのリビルドを開始します。この処理の実行中、Storage ManagerのLogical Configuration Viewでは、故障したハードディスクとホットスペアの位置が入れ替わって表示されます。

- ホットスペアの元の位置には、赤色の故障フラグ付きで故障したハードディスクのアイコンが表示され、ホットスペアはアレイグループの構成要素として表示されます。
- ホットスペアには、リビルド処理が進行中であることを示す白色のフラグが表示されます。
- アレイとLSUのアイコンには、青色のフラグが表示されます。

リビルドが完了すると、ホットスペアのアイコンとフラグが消え、リビルドされたハードディスクはアレイの正式な構成要素として表示されます。
故障したハードディスクのアイコンに表示されている赤色のフラグは、ハードディスクを交換するか、ステータスがOptimalに戻るまで、そのまま表示されます。
複数のアレイグループが存在する場合にホットスペアを割り当てる際は、各アレイグループを構成するハードディスクと同一型名のハードディスクを、それぞれ一台以上ずつ割り当ててください。

■ホットスペアを割り当てる/削除する

ホットスペアの割り当ておよび削除は、以下の手順で行います。

1. ［SCSI Device Information］ウィンドウで、次のいずれかのボタンをクリックします。

ボタン	機能
Make Hotspare	ハードディスクをホットスペアに割り当てる。
Remove Hotspare	既存のホットスペアドライブを削除する。

ホットスペア指定時に次のダイアログが表示されます。

2. 確認し、［OK］をクリックします。

> ⚠注意　ホットスペアに指定すると、そのハードディスクの内容は消去されます。
> 消去しても問題ないときのみ［OK］をクリックしてください。

■ホットスペアを Optimal 状態にする

故障したハードディスクを交換する際、ホットスペアをOptimal状態にする必要があります。これは、以下の手順で行います。

1. 「付録B.4.3 内蔵ハードディスクユニットの取り付け／取り外し」に記載された手順で、故障したハードディスクを取り外して交換します。
2. 新しいハードディスクのInformationウィンドウで［Make Optimal］をクリックします。
   新しいハードディスクがホットスペアになり、前のホットスペアがリビルドされたアレイグループの構成要素になります。
3. ホットスペアを解除する際にリダイレクトをするよう指示される場合があります。
   リダイレクトについては、次の「12.10.1 リダイレクト」をご覧ください。

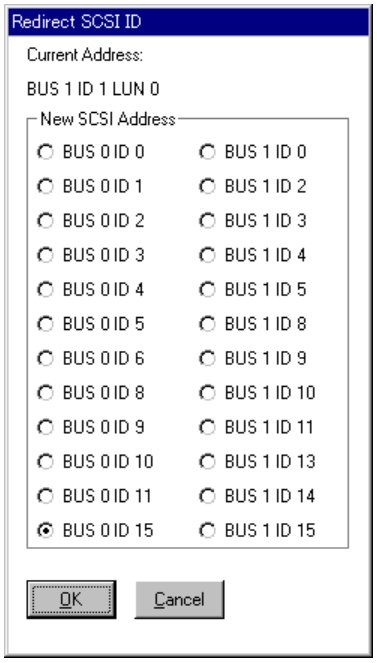
12.10.1 リダイレクト

アレイに含まれていないハードディスクには物理アドレス（Bus/ID）がLSUアドレスとして割り当てられます。しかし、そのLSUアドレスが他のアレイグループなどによりすでに使用されている場合、別のLSUアドレスを割り当てる必要があります。これをリダイレクトといいます。リダイレクトが必要となるのは次のような場合です。

- アレイまたはホットスペアを解除する際、それらのハードディスクの物理アドレス（Bus/ID）と同じLSUアドレスが他のアレイグループなどによりすでに使用されている場合

リダイレクトは、以下の手順で行います。

1. 対象のハードディスクのアイコンをダブルクリックます。
2. ［Redirect］をクリックします。
   次の画面が表示されます。



3. 割り当てられていないBus/IDを選択して、［OK］をクリックします。

12.11　ハードディスクが故障した場合

ハードディスクの故障は、アレイ、マルチレベルRAIDおよび個別のハードディスクに関連付けられたアイコンのフラグで示されます。
アレイグループに属すハードディスクが故障した場合、Physical Configuration ViewとLogical Configuration Viewの両方で、アイコンに赤色のフラグが表示されます。故障の状況は以下のように示されます。

① 故障したハードディスクがRAID 0のアレイに属す場合

故障したハードディスクのアイコンに赤色のフラグが表示されます。
RAID 0アレイのいずれかのハードディスクが故障すると、そのアレイ自体が故障し、そのアレイのデータが失われることになります。

② 故障したドライブがRAID 1、5または0+1のアレイに属す場合

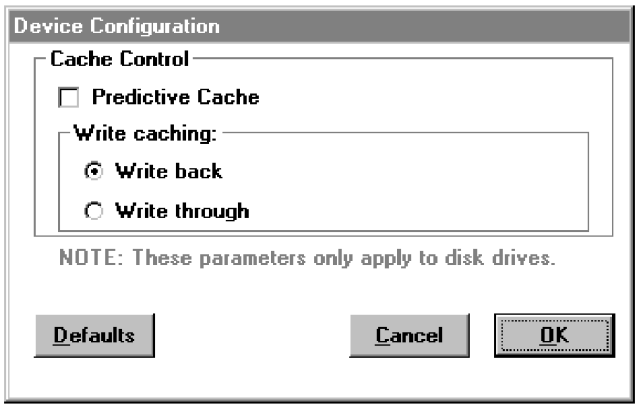
アレイアイコンに黄色のフラグが表示されます。これは、現在アレイがDegraded状態で動作していることを示します。
同じアレイに属す複数のハードディスクに赤色のフラグが表示された場合は、そのアレイのフラグが黄色から赤色に変わります。これは、アレイ自体が故障し、そのデータが失われたことを示しています。
アレイのアイコンが赤色になった場合、そのアレイは使用できません。もう一度アレイを作成し、信頼性のあるデータを復旧しなければなりません。

故障したハードディスクの交換は、以下の手順で行います。

1. **「付録B.4.3 内蔵ハードディスクユニットの取り付け／取り外し」に記載された手順で、故障したハードディスクを取り外して交換します。**
   — ホットスペアを交換する場合は、ツールヘルプの『ホットスペア』をご覧ください。
   — アレイグループに含まれているハードディスクを交換する場合は、ツールヘルプの『ハードディスクの交換手順』をご覧ください。

12.12　アレイおよびハードディスクのキャッシュ設定を変更する

キャッシュ設定を変更するには、Array Group Informationウィンドウおよび SCSI Device Information ウィンドウで［Configure］をクリックします。
Device Configurationダイアログボックスが表示されます。



ここでは、コントローラのキャッシングパラメータを変更できます。

- キャッシュの設定には、Write backとWrite throughがあります。
- Predictive Cacheチェックボックスでは、アレイコントローラの予測キャッシング機能の有効/無効を設定します。工場出荷時には、この機能は無効に設定されています。予測キャッシングを有効にすると、コントローラの全体のパフォーマンスが低下することがあります。
- ［Defaults］をクリックすると、工場出荷時の設定に従ってキャッシュ処理が実行されます。

12.13　イベント

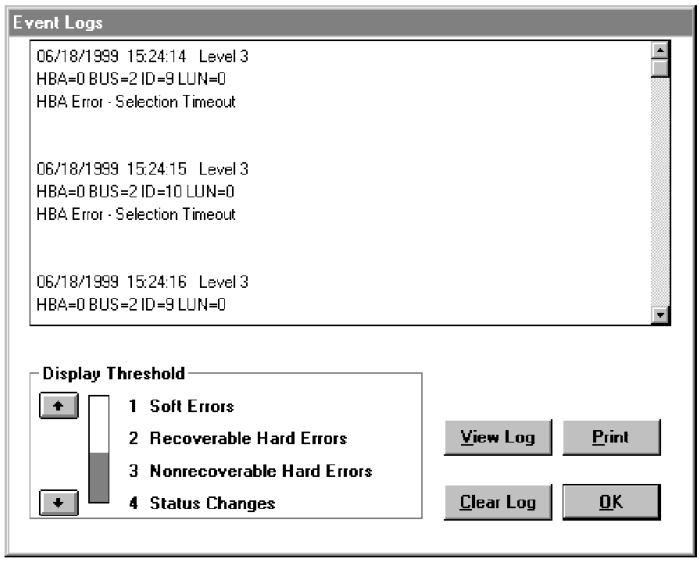
イベントは、エラーの発生やステータスの変化などが発生する場合に生成されます。イベントは、4つのレベルおよびカテゴリに分類されます。

レベル	エラーの種類	意味
1	Soft Error	ハードディスクに対する操作のエラーが発生し、再試行で成功したことを示しています。
2	Recoverable Hard Error	ハードディスク、コントローラまたはPCIバスのエラーで、ECCまたは冗長アレイ情報によってデータが回復されたことを示しています。
3	Nonrecoverable Hard Error	ハードディスク、コントローラまたはPCIバスのエラーで、ECCまたは冗長アレイ情報を使用してもデータを回復できなかったことを示しています。
4	Status Change	アレイまたはディスクドライブのステータスが変化したことを示しています（ハードディスクやアレイの故障、アレイの初期化またはリビルドの開始または完了など）。

12.13.1 イベントロギング

発生したイベントは、イベントが発生したコントローラのNVRAMに自動的に記録されます。さらに、イベントログがハードディスクに保持されるように指定できます。

イベントログの内容を表示するには、コントローラ、ハードディスクまたはアレイのInformationウィンドウの「Event Log」をクリックします。
Event Logsウィンドウが表示され、特定レベル以上（初期値はレベル4）のイベントのみ表示されます。



ボタン	機能
↑ ↓	Display Thresholdのレベルを調整します。 — コントローラには、すべてのイベントが記録されています。 ここで設定するレベルは、表示するイベントのレベルです。
View Log	選択したレベルのイベントメッセージを表示できます。
Print	イベントログ一覧に現在表示されているイベントメッセージを印刷できます。特定のメッセージを印刷する場合は、そのメッセージが表示されるまで一覧をスクロールさせてから、「Print」ボタンをクリックします。

12.14　ソフト的なディスク増加を行う

ここでは、WebUIを通じて追加ディスクを単一ボリュームに見せる方法について説明します。
ただし、この場合、作業中に再起動が必要となります。

以下のようにして、追加されたボリュームをソフトウェア的に拡張することが可能です。

■準備（Disk Management を起動する）

1. プライマリナビゲーションバーから［ディスク］をクリックします。
2. セカンダリナビゲーションバーから［ディスクとボリューム］をクリックします。
   ターミナルサービスを経由して起動されます。
3. 管理者アカウントおよびパスワードを入力してログオンします。
   Disk Managementが起動します。

■スパンボリュームとして拡張する

1. ダイナミックディスクへアップグレードする
   1) Disk Managementの画面でアップグレードする適切なディスクボリュームを選択し、右クリックします。
   2) サブメニューから［ダイナミックディスクにアップグレード］を選択します。
   3) ウィザードに従い作業を終了させてください。
   4) サーバを再起動します。
      本設定はサーバの再起動後有効となります。
2. ディスクを拡張する
   1) 再起動後、再びDisk Managementを起動します。
   2) 拡張するボリュームを右クリックし、［ボリュームの拡張］を選択します。
   3) ［利用可能なダイナミックディスク］一覧から、拡張したいディスクを選択します。
   4) ［追加］をクリックして、選択したディスクを追加し、領域サイズを指定し［次へ］をクリックします。
   5) ［完了］をクリックします。
      拡張は構成済みです。

■ドライブをマウントする

本サーバはWindows 2000テクノロジーに基づいてインテグレートされています。Windows 2000では、ドライブマウントと呼ばれる、パーティション拡張機能があります。これを使うことで物理的には分かれたドライブをシステムドライブに追加することができるようになります。

ローカル ドライブをローカル NTFS ボリュームの空のフォルダに接続したりマウントしたりできます。
ローカルドライブを空の NTFS フォルダにマウントすると、ドライブ文字の代わりに、そのドライブへのパスが割り当てられます。

たとえば、ドライブ文字 D の CD-ROM と、ドライブ文字 C の NTFS ボリュームがある場合、CD-ROM を C:¥CD-ROM という空フォルダにマウントし、C:¥CD-ROM というパスから直接 CD-ROM にアクセスできます。
必要であれば、ドライブ文字 D を削除し、マウントされているドライブのパスを介して引き続き CD-ROM にアクセスできます。

マウントされたドライブを使うと、データに容易にアクセスでき、作業環境およびシステムの使用状況に基づいてデータ記憶域を柔軟に管理できます。

マウントは以下の手順で行います。

1. Disk Managementの画面でマウントするボリュームを右クリックし、［ドライブ文字とパスの変更を選択する］をクリックします。
   現在のドライブ名が表示されます。
2. ［追加］をクリックします。
3. 次画面で、［このNTFSフォルダにマウントする］にチェックし、ドライブ文字とパス（［参照］で検索も可能）を指定します。
4. ［OK］をクリックします。
   マウントポイント作業は完了です。

第13章　サーバ監視について

この章では、本サーバの運用管理・監視の仕方についての、基本的な知識について説明します。

CONTENTS

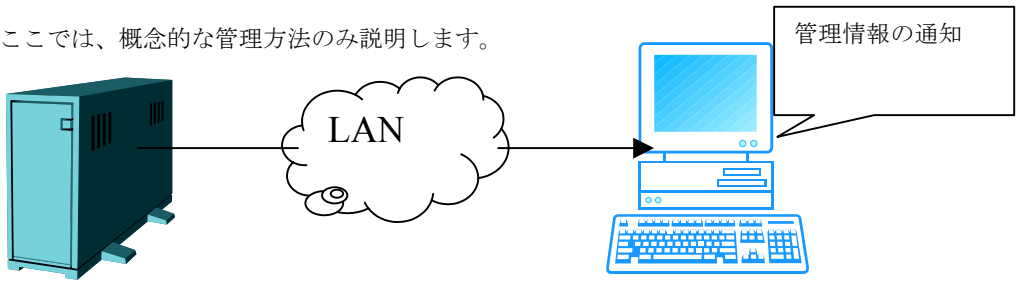
13.1　サーバ監視の概要

サーバ監視には、プレインストールされたサーバ監視ツール「ServerView」を使用します。
ServerView では、ハードディスクドライブ、冷却ファン、電源ユニット、または装置の温度などの重要なサーバ機能をチェックします。これらのパラメータの値が指定した値を超えたりエラーが発生した場合には、メッセージが出力され、必要なときには修正処置が施されます。
注意：ServerViewにおいて、モデル名等が、「PRIMERGY H200」と表示される場合があります。「PRIMERGY H200」を「PRIMERGY FileServer」と読み替えてください。

13.2　配置

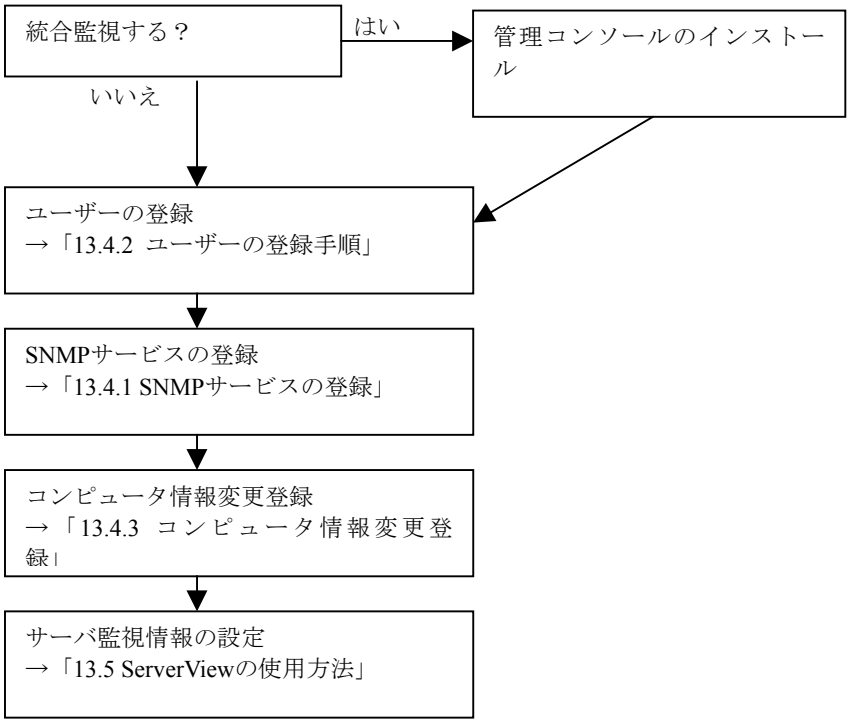
ServerViewを本サーバで使用する場合は、必ず監視・管理コンソールを別マシンに配置することをおすすめします。管理コンソールは添付のServerViewCDに同梱されています。詳しいインストール方法・設定方法に関しては、CD同梱のヘルプをご覧ください。

ここでは、概念的な管理方法のみ説明します。



- 管理サーバを構築することで、複数台のPRIMERGY FileServerを管理することができま
- 弊社の汎用PRIMERGYサーバも合わせて管理することができます。

■ServerView設定までの流れ



13.3 ServerViewの機能

■リカバリ機能

本サーバでは、自身をモニタし、ASR&R （自動サーバ再構成と再起動）の支援により、エラー発生時の対策を指定できます。この方式では、適切なシャットダウンを開始するか、または欠陥部分を自動的に使用不能にしてリブートできます。

■予防保守機能

予防保守機能は、特定のサーバ部品のエラーを早期に検出します。これにより、障害発生前に個々の部品を修理、交換できます。次の部品をモニタします。

- ファン
- CMOS バッテリ
- S.M.A.R.T.標準をサポートするSCSI およびRAID コントローラ上のハードディスク

■モニタ機能

ハードウェアのインベントリ（目録）を作成し、ServerView で利用可能なモニタ機能を使用して、様々なシステムパラメータをモニタできます。このような機能により、特に次のことができます。
- インストールしたハードウェアのインベントリの作成
- サーバオペレーションの稼動時間カウンタを含むすべてのハードウェアコンポーネントのモニタ
- システムがダウンする前に、適切な通知をする全寿命期間にわたるモニタ
- 故障電源ユニットの迅速な認識
- バスシステム、プロセッサ、主記憶装置、ハードディスク（RAID ドライブを含む）、ネットワークコントローラ、およびその他の内蔵コントローラの詳細情報の取得
- 長期モニタの目的で集めた情報の記録（性能分析、エラー頻度率）

■管理機能

ServerView は、次のような管理機能を提供します。

- 簡単に使用できるアラーム管理システムおよび様々なアラーム発信メカニズム
- 長期間にわたり、様々なサーバのパラメータをモニタするためのレポート管理システム
- ネットワーク上の別のサーバにSNMP 構成データをリファレンスサーバから転送するデフォルトの管理システム
- サーバをリモートからメンテナンスするためのリモート管理システム。

ServerView は、リモートメンテナンスのために使用されるRemoteControlService （リモートコントロールサービス）と合わせて機能します。

■S.M.A.R.T. サポート

セルフモニタリングおよびレポーティング技術（S.M.A.R.T.）は、ハードディスクのエラーを早期に検出します。これは、S.M.A.R.T.アルゴリズムによって、実現します。このアルゴリズムは、ディスクのパラメータをモニタし、差し迫った故障を検出し、それをSCSI コントローラまたはホストに通知します。

S.M.A.R.T. の概念は、パラメータ値に基づいて、いわゆる「予測可能なエラー」だけを検出します。たとえば、突然の電源故障または機械故障によるエラーは予測不可能なため、この方式では予期できません。

S.M.A.R.T.は、現在すべてのSCSI ドライブでサポートされており、また数多くのIDE ドライブでも利用できます。

差し迫ったエラーの早期警告の効果は、主にアルゴリズムの効率と、モニタされたパラメータの数に依存します。このようなコンポーネントは、メーカ固有のものなので、ハードディスクのタイプにより異なる可能性があります。

ServerView は、SCSI およびRAID のコントローラ上の S.M.A.R.T.互換のハードディスクをサポートします。S.M.A.R.T.が差し迫ったエラーを検出すると割り込みが発生し、S.M.A.R.T.エラーの発生したドライブが特別な色（マゼンタ）で表示されます。

13.4　管理のための設定（ServerViewを使う前に）

ServerViewを使って管理コンソールに警告情報を通知するには、あらかじめサービスへの登録、ユーザー、サーバの認識設定をしなくてはなりません。

13.4.1　SNMPサービスの登録

1. WebUIに接続し、プライマリナビゲーションバーから［メンテナンス］、セカンダリナビゲーションバーから［ターミナルサービス］を選択し、PRIMERGY FileServerに接続します。
2. コントロール パネルから［管理ツール］アイコンをダブルクリックします。
3. ［コンピュータの管理］アイコンをダブルクリックしてコンピュータの管理ウィンドウを開きます。
4. コンソール ツリーで、［サービスとアプリケーション］－［サービス］をクリックします。
5. 詳細情報のウィンドウ領域で［SNMP Service］をクリックします。
6. ［操作］メニューのプロパティをクリックします。
7. ［トラップ］タブをクリックします。
8. コミュニティ名ボックスに既に「public」がある場合は「public」を選択します。
   存在しない場合はコミュニティ名ボックスに「public 」を入力して［追加］をクリックします。
9. トラップ送信先の［追加］をクリックします。
10. コンソールをインストールするサーバのホスト名、IPアドレスを入力し、［追加］をクリックします。
11. ［セキュリティ］タブを選択します。
12. コミュニティ「public」を選択します。
13. ［編集］をクリックします。
14. ［コミュニティ権利］コンボボックスから「READ_WRITE」または「READ_CREATE」を選択し、［OK］をクリックします。
    ※「READ_WRITE 」を選択することを推奨します。

ポイント

［受け付けるコミュニティ名］ボックスのリストの中に、コミュニティ名「public 」が存在しない場合は、次の操作でコミュニティを追加します。

1) ［追加］をクリックします。
2) ［コミュニティ権利］コンボボックスから、「READ_WRITE 」または「READ_CREATE 」を選択します。（「READ_WRITE 」を推奨します。）
3) ［コミュニティ］ボックスに「public 」と入力します。
4) ［追加...］をクリックします。

15. SNMP パケットを受け付けるホストの設定を行います。

ーすべてのホストのパケットを受け付ける場合

1) ［すべてのホストからのSNMP パケットを受け付ける］をチェックします。

ー指定したホストのパケットのみを受け付ける場合

2) ［次のホストからのSNMP パケットを受け付ける］をチェックします。

3) ［追加］をクリックします。

4) コンソールをインストールするサーバのホスト名、IP アドレスを入力し、［追加］をクリックします。

ポイント

- SNMP トラップ設定では、トラップの送信先を指定します。ここでは、ServerViewコンソールのIP アドレスを入力する必要があります。
  SNMP エージェントをインストール済みのサーバにおいて、独自のIP アドレスとローカルIP アドレス（「127.0.0.1 」または「localhost 」）からのSNMP 要求を受信できるように設定する必要があります。
- SNMP はパスワードで保護されていないオープンプロトコルなので、相応の権限を持つマネージャだけを入力するようにしてください。無許可のネットワークユーザーは、重要なシステムパラメータを変更し、サーバのオペレーションを中断させる可能性があります。

■IPアドレスが複数存在するサーバの監視について

ServerView では、IP アドレスが複数存在する場合（複数枚のLAN カードを持つ等）、ネットワークのバインドで設定された順序にしたがって自サーバのIP アドレスを検索します。管理コンソールとの通信を行うアダプタを最初に検索するようにバインドしてください。

13.4.2 ユーザーの登録手順

1. プライマリナビゲーションバーで、［ユーザー］をクリックします。
2. セカンダリナビゲーションバーで、［ローカルグループ］をクリックします。
3. FUJITSU SVUSER のチェックボックスをオンにし、タスクから［プロパティ］を選択します。
4. タブから［メンバ］をクリックします。
5. 追加するユーザーまたはグループの名前を下のボックスに入力するか、ユーザーまたはグループを上のボックスで選択して［追加］をクリックします。
6. 必要なすべてのユーザーを追加したら、［OK］をクリックします。

13.4.3　コンピュータ情報変更登録

マシンのコンピュータ名、またはIP アドレスを変更した場合、次の操作を行います。
この操作は、PRIMERGY FileServerのIPアドレス設定が変更になるたびに行う必要があります。

1. ServerView およびアラームサービスのウィンドウを起動している場合は、すべて終了します。
2. [スタート]－[プログラム]－[Fujitsu ServerView]－[ChangeComputer Details]の順にクリックします。
3. 新しいコンピュータ情報を設定します。
4. [スタート]－[プログラム]－[Fujitsu ServerView]－[SNMP Agents]－[Restart Services]を実行し、サービスを再開させます。

13.5　ServerViewの使用方法

ServerViewではアラームサービスにより、情報を受信しようとするイベントと運用状態を定義できます。ネットワークにおいてサーバの可用性は非常に重要なので、サーバの可用性を危険にさらす可能性のあるステータスを適切に設定します。アラームはさまざまな段階で起動し、メールなどで通知するように設定することができます。

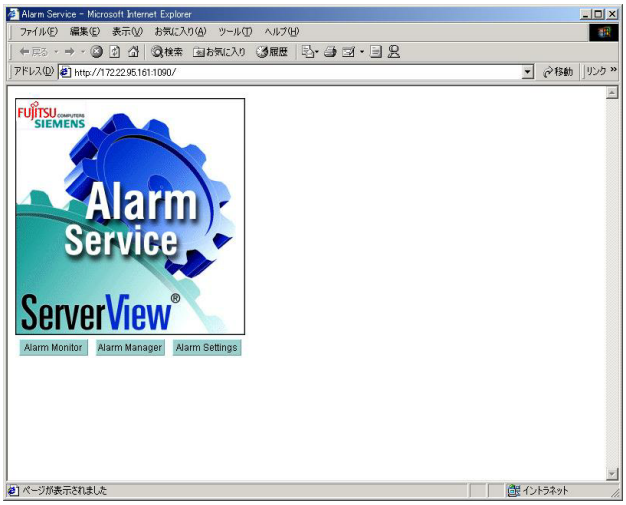
アラームサービスは、監視エージェント群から成り、監視エージェントはサーバの異常な運用ステータスを検出すると、SNMP を経由してアラームサービスにアラーム（割り込み）を送信します。

アラームサービスは、管理コンソールソフトウェアと共に自動的にインストールされていますが、PRIMERGY FileServer内にもプレインストールされているので、WebUIからも設定を行うことができます。
WebUIアラームサービスの起動方法については、次の「13.5.1 アラームサービスを起動する」をご覧ください。

13.5.1 アラームサービスを起動する

WebUIアラームサービスは、以下の手順で起動します。

1. プライマリナビゲーションバーから、[メンテナンス] をクリックします。
2. セカンダリナビゲーションバーから、[Fujitsu Server View] をクリックします。
3. ポート1090を使用して、アラームサービスを起動します。
   次の画面（以後、「アラームメニュー画面」と呼びます）が表示されます。



4. ［Alarm Monitor］［Alarm Manager］［Alarm Settings］の各ボタンをクリックし、編集したい画面を表示します。

アラームサービスは、次のコンポーネントで構成されています。

●Alarm Monitor（アラームモニタ）

Alarm Monitorは、すべてのアラームを参照するために使用します。
詳細は「13.5.3 Alarm Monitor」をご覧ください。

●Alarm Manager（アラームマネージャ）

Alarm Managerは、アラームログリストに格納されたすべてのアラームを参照し編集するために使用します。詳細は「13.5.2 Alarm Manager」をご覧ください。

●Alarm Settings（アラームの設定）

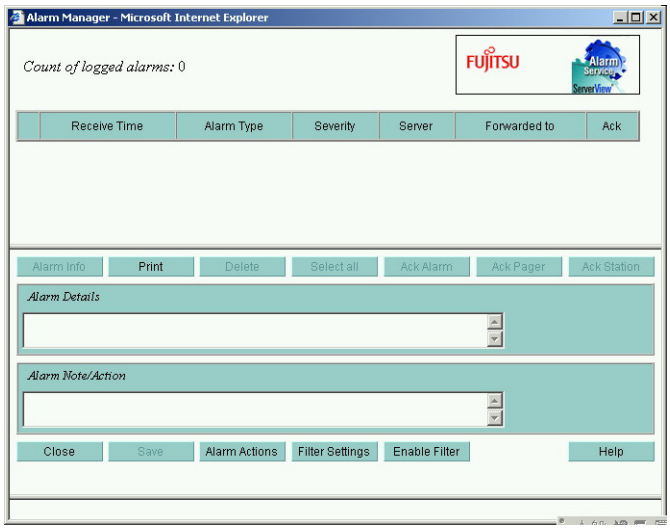
Alarm Settingsは、アラームを設定するために使用します。たとえば、アラームアクションや、アラームメッセージの転送先を定義できます。
詳細は「13.5.4 Alarm Settings」をご覧ください。

13.5.2 Alarm Manager

Alarm Managerを使用すると、アラームログリストにあるすべてのアラームの編集、管理を行えます。

1. アラームメニュー画面で［Alarm Manager］をクリックします。

次の画面が表示されます。



ウィンドウ上部にはアラームの概要が表示されます。
次に、［Count of logged alarm］に記録されたアラームの総数が表示されます。
表の部分にはReceive Time（受信時間）、Alarm Type（アラームタイプ）、Severity（重要度）、Server（サーバ）、Forwarded to（アクション）、Ack（受領）の情報が表示されます。アラームが転送された場合またはエントリが削除された場合には、表示内容が以下のように変わります。

ボタン	機能
Alarm Details	：短いテキストメッセージ（関連するMIBから）が表示されます。これは、選択したアラームの詳細を示すメッセージです。
Alarm Note/Action	：必要なアラームまたはアクションに関する詳細情報を示す短い注を入力できます。
Save	：この情報を保存します。

このエントリは変更できませんが、別のエントリを追加できます。エントリが作成されて初めてアラームは受領されます。

■アラームフィルタ設定を行う

［Setup Alarm Filter］には、アラームの現在のフィルタ設定が表示されます。
［Filter Settings］ボタンを使用して、新しいフィルタ設定を定義します。
アラームマネージャ画面で[Filter Settings]ボタンをクリックします。
[Setup Alarm Filter]画面には以下のフィルタ設定が表示されます。
フィルタ定義を行うことでよりアラームの選別をおこなうことができます。

設定できるフィルタは次のとおりです。

●Select Server（サーバの選択）
選択したサーバのアラームにフィルタをかけます。

●Select Severity（種類の選択）
重大性のレベルが選択したレベル以下か、以上かによってアラームにフィルタをかけます。

●Alarms（アラーム）
未処理か受領済みのアラームに基づいてフィルタをかけます。

●Time（時刻）
アラームが指定した時刻の前と後のいずれに発生したかによって、アラームにフィルタをかけます。

●未処理のマネージメントステーション
トラップを他のマネージメントステーションに送信した未処理のアラームに基づいてフィルタをかけます。

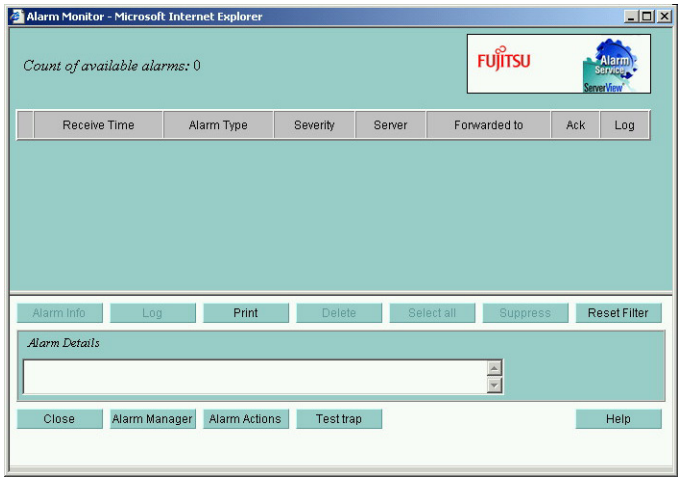
その他動作ボタンの定義は以下の通りです。

ボタン	機能
Alarm Info	：アラームに関する詳細情報を表示するウィンドウが開きます。
Delete	：選択した受領済みのアラームをすべて削除します。
Select all	：すべてのアラームを選択します。
Ack Alarm	：すべてのアラームを受領します。
Alarm Actions	：［Overall settings］ウィンドウを開きます。このウィンドウでアラーム設定を編集できます。

13.5.3 Alarm Monitor

Alarm Monitorでは、受信したすべてのアラームを参照できます。

1. アラームメニュー画面で［Alarm Monitor］をクリックします。
   次の画面が表示されます。



名称	説明
Count of Available alarms	：アラームエントリの数が表示されます。
アラームの概要	：現行セッション中のアラームの［Receive Time］、［Alarm type］、［Severity］、［Server］、［Forwarded to］が表示されます。
Alarm Details	：選択したアラームを多少詳細に説明した短いテキスト（関連するMIB から）情報が表示されます。
Alarm Info	：アラームに関する詳細情報を表示するウィンドウが開きます。
Reset Filter	：フィルタ設定をリセットします。
Alarm Manager	：Alarm Managerを呼び出します。
Alarm Actions	：［Overall settings］ウィンドウを開きます。このウィンドウでアラーム設定を編集できます。
Test trap	：接続テストのためにトラップを送信するサーバを選択できるウィンドウを開きます。［Test trap］ボタンを使用してテストを開始します。 ＊初回設定時には必ずテストトラップを行ってください。

13.5.4 Alarm Settings

アラームアクションや、アラームメッセージの転送先など、アラームの設定を行えます。

■アラームの設定を行う

1. アラームメニュー画面で［Alarm Settings］をクリックします。

アラームサービス自体が実行されていない場合でも、このメニュー項目を呼び出すことができます。

［Start Alarm Settings］画面が表示されます。

［Start Alarm Settings］画面には以下のオプションがあります。

●Use Wizard

ウィザードで表示されるそれぞれのウィンドウに従って、アラームパラメータを設定できます。

特に新しいパラメータ設定を行う場合は、このウィザードに従って設定してください。

●Go to Overall Settings

このオプションでは、アラーム処理の全体的な設定を定義できます。

●Filter Server

このオプションでは、アラームメッセージを受信したくないサーバを非表示にできます。

●Edit／New Alarmgroup

このオプションでは、新しいアラームグループの定義や、既存のアラームグループの編集ができます。

●Set／Edit Destinations

このオプションでは、アラーム転送の設定を定義できます。

●Show Overview of all Groups

このオプションでは、すべてのアラーム定義の概要を表示できます。

ここでは、［Use Wizard］を使って設定する手順を説明します。

2. ［Use Wizard］が選択されているのを確認し、［Go］をクリックします。

［Overall settings］が起動します。

［Overall settings］では、以下のパラメータが設定できます。

●Filter settings

Set time for repetition in sec	：定義時間内に同一サーバから同じアラームが発行された場合にフィルタをかけます。
Filter unknown alarm	：不明なアラームにフィルタをかけます。
Filter unknown server	：不明なサーバにフィルタをかけます。
Filter severity	：エラーの重大性に応じてフィルタをかけます。

●Delete alarm

アラームを削除する時期を指定します。指定の時間が経過した場合またはアラームログリストに指定の数のエントリが作成された場合に、アラームを削除できます。

●Alarm actions／Default alarm handling

トリガされる着信アラームのアクションです。それぞれのエラーカテゴリに応じて、設定できます。任意の組み合わせが可能です。重大なエラーは、必ずアラームログリストに書き込まれます。

Pop up a message	：メッセージを表示する
Store in event log	：アラームログリストに保存する

本サーバは、遠隔管理を目的としたサーバですので、ポップアップの設定はせず、ログの設定のみを行ってください。

・Alarm manager

アラームログリストに書き込めるエントリの最大数を指定し、この最大数に達した場合の動作を指定します。

Pop up warning	：メッセージが出力されます。
Wrap around	：もっとも古いエントリがシステムにより上書きされます。

本サーバは、遠隔管理を目的としたサーバですので、ポップアップの設定はせず、ラップアラウンドの設定を行ってください。

3. ［Next］をクリックし、［Filter Server］を起動します。

［Filter Server］では、アラームにフィルタをかけるサーバを指定できます。

― サーバ上でアラームサービスが実行されておりサーバの一覧に別のサーバが入力されていない場合、アラームサービスが実行されているサーバがローカルホストとして表示されます。この場合、追加設定は必要ありません。

― 上記以外の場合は、サーバの一覧にあるすべてのサーバが［Server list］ウィンドウに表示されます。［>>>］ボタンと［<<<］ボタンを使用して、必要なサーバを選択できます。

一度に選択できるのは1つのサーバだけです。

― ［Info］ボタンをクリックすると、選択したサーバに関する追加情報を表示できます。

4. ［Next］をクリックし、［Edit／New Alarmgroup］を起動します。

［Edit／New Alarmgroup］では、新しいアラームグループの定義や既存のアラームグループの編集を行えます。アラームグループとは、サーバのグループであり、そのグループに対するアラームです。

― アラームグループを定義するには、新しいグループの名前を入力します。

― 既存のアラームグループを編集するには、アラームグループのリストから該当するアラームグループを選択します。

― サーバを選択するには、このアラームグループに入るサーバを指定します。

［Server of alarm group］のリストが空である場合、既知のサーバだけでなく、すべてのサーバがアラームグループに追加されます。

― アラームグループを削除するには、以下の手順で行います。

1) リストからアラームグループの名前を選択するか、手作業で名前を入力します。

2) ［Delete］ボタンをクリックしてアラームグループを削除します。

5. ［Next］をクリックし、［Set／Edit destinations］を起動します。
［Set／Edit destinations］では、アラームのアクションに関する設定を行えます。
アラームグループを選択し、次にこのアラームグループによりトリガできるアクションを定義します。アラーム転送の実際の処理は、［Enable］ボタンで有効または無効にできます。
アラームグループが次のアクションを行うかどうかを指定できます。

Mail	：電子メールでアラームに該当した場合の処理を通知します。
Popup	：ポップアップメッセージを出力します。 ※本機能は使わないでください。
Logging	：イベントログにアラーム情報を書き込みます。
Pager	：ポケットベルまたは、携帯電話によるアラーム処理を行います。
Excute	：修正用のプログラムがある場合には、その指定を行います。
Broadcast	：メッセージをブロードキャスト配信します。
Station	：新しいトラップを設定することができます。

選択したオプションに応じて、追加ウィンドウが表示されます。これらのウィンドウでさらに詳細な設定を行います。これらのウィンドウの説明を見るには、［Help］ボタンをクリックしてください。
設定内容の詳細は、ServerViewCD添付のマニュアルをご覧ください。

■全設定を表示する

1. アラームメニュー画面で［Alarm Monitor］をクリックします。
アラームサービス自体が実行されていない場合でも、このメニュー項目を呼び出すことができます。
［Start Alarm Settings］画面が表示されます。
2. ［Show Overview of all Groups］をクリックします。
［Overview］が起動します。
［Overview］には、アラーム定義の概要が表示されます。表示内容は、［Select root］で選択した並べ替え順序によって異なります。
［Set／Edit destinations］ウィンドウで行った設定によっては、［Enable］ラジオボタンが使用できないことがあります。

13.5.5 アラームメールの設定を行う

メール送信時の設定について説明します。

■メールの転送

MAPIメッセージ設定はおこなうことができません。SMTP設定のみサポートしています。
メールの設定は次の手順で行います。

1. アラーム転送用の［メール］オプションを選択すると、デフォルトのメール設定を示すウィンドウが表示されます。
2. ［プロパティ］を選択し、SMTPのユーザー名とSMTPサーバを［ユーザー名］と［SMTP サーバ］に入力します。
［ポート］にはポート番号を入力します。デフォルト値はPort 25 です。

13.5.6 リモートサービスボードについて

リモートサービスボードは、専用のCPU ・OS ・通信インタフェース・電源により、サーバの状態に依存せずに動作し、サーバを監視するハードウェア製品です。
リモートサービスボードは、ServerViewと連携し、以下の機能を管理者に提供します。

- サーバの状態監視（OS ハング、電源異常、温度異常、電圧異常）
- サーバ異常時の管理者への通知
- サーバ異常時の自動サーバシャットダウン
- サーバの遠隔操作（再起動、電源投入／切断）
- サーバのスケジュール運転

さらに、リモートサービスボードは、RemoteControlService と連携し、以下の機能を管理者に提供します。

- 管理コンソールからのサーバPOST時の画面表示、キーボード操作

また、リモートサービスボードは、以下の通信インタフェースをサポートしています。

- LAN インタフェース

■ 通信インタフェースの設定

お使いになる通信インタフェースに応じて、以下の手順で必要な項目を設定します。
リモートサービスボードの通信インタフェースの設定は、リモートサービスボードのドライバをインストールしてから行ってください。

LAN インタフェースの設定

1. サーバに管理者または管理者と同等の権限をもつユーザー名で、WebUIより［メンテナンス］→［ターミナルサービス］をクリックし、ログインします。
2. 実行中のアプリケーションをすべて終了させます。
3. 次のプログラムを起動します。

```
c:¥Program Files¥Fujitsu¥F5FBAG01¥rsb_uty.exe
```

4. ［LAN Interface ］タブを選択し、各項目を設定します。

項目	説明
Internet Protocol	
IP Address	リモートサービスボードのIP アドレスを設定します。 （設定必須。 デフォルト値：192.168.0.10 ）
Subnet Mask	サブネットマスクを設定します。 （設定必須。 デフォルト値：255.255.255.0 ）
Gateway	デフォルトゲートウェイサーバのIP アドレスを設定します。
Domain Name Server	Use DHCP DHCP を使用するかしないかを設定します。 Enabled：DHCP を使用します。 Disabled：DHCP を使用しません。

5. 各項目を設定後、[Apply]ボタンをクリックします。

LAN インタフェースからのパスワードの変更

1. サーバにログインします。
2. [スタート]ー[プログラム]ー[Fujitsu ServerView]ー[Fujitsu ServerView]をクリックし、ServerView コンソールを起動します。
3. サーバの一覧にあるサーバのアイコンを選択し、[File]メニューの[Server properties]を選択します。
4. [Remote Service Board]タブを選択し、[Apply]ボタンをクリックします。
5. 「ユーザー名（root ）」と「パスワード（fsc ）」を入力し、[OK]ボタンをクリックします。
6. [User Accounts]をクリックします。
7. [root]をクリックします。
   ユーザー名：root の[Account]ページが開きます。
8. 以下の項目を入力し、[Apply]ボタンをクリックします。

項目	説明
Old Password	fsc を入力します。
New Password	新しいパスワードを入力します。
Confirm New Password	新しいパスワードを再度入力します。