QNAP Turbo NAS

取扱説明書

(バージョン: 3.6.0)

© 2012 QNAP Systems, Inc. All Rights Reserved.

目次

1. 注意.....5

1.1 規制の通知 6
1.2 本書で使用される記号 7
1.3 安全に関する警告 8

2. 始めましょう.....9

2.1 CD-ROM の検索 14
2.2 ハードディスクの推奨リスト 16
2.3 システムステータスのチェック 17
2.4 NAS ネットワーク共有に接続 20
2.5 Web ブラウザを使って NAS に接続 22
2.6 システム移行 29

3. システム管理.....32

3.1 全般設定 33
3.2 ネットワーク 37
3.3 サービスバインディング 56
3.4 ハードウェア 58
3.5 セキュリティ 62
3.6 通知 65
3.7 電源管理 72
3.8 ネットワークごみ箱 74
3.9 設定のバックアップ/復元 75
3.10 システムログ 76
3.11 ファームウェア更新 82
3.12 工場出荷時設定の復元 86

4. ディスク管理.....87

4.1 ボリューム管理 87
4.2 RAID管理 91
4.3 ハードディスクS.M.A.R.T. 116
4.4 暗号化ファイルシステム 117
4.5 iSCSI 127
4.5.1 ポータル管理 127
4.5.2 ターゲット管理 140
4.5.2.1 WindowsのMicrosoft iSCSIイニシエータを使用したNASへの接続..... 151
4.5.2.2 Mac OSのXtend SAN iSCSIイニシエータを使用したNASへの接続..... 157
4.5.2.3 Ubuntu LinuxのOpen-iSCSIイニシエータを使用して接続する..... 164
4.5.3 拡張ACL 166
4.5.4 LUN バックアップ 170

4.6 仮想ディスク 189
5. アクセス権管理.....194
5.1 ドメインのセキュリティ 194
5.1.1 NASをWindows Server 2003/2008 Active Directoryに結合します 195
5.1.2 NAS の LDAP ディレクトリへの接続 209
5.2 ユーザ 216
5.3 ユーザグループ 229
5.4 共有フォルダ 230
5.5 クォータ 260
6. ネットワーク サービス.....261
6.1 Microsoftネットワーク 262
6.2 Appleネットワーク 266
6.3 NFSサービス 269
6.4 FTPサービス 272
6.5 Telnet/SSH 274
6.6 SNMP設定 275
6.7 Webサーバ 277
6.7.1 仮想ホスト 301
6.8 ネットワークサーチサービス 303
7. アプリケーション・サーバー.....305
7.1 Webファイルマネージャ (Web File Manager) 306
7.2 マルチメディアステーション (Multimedia Station) 324
7.2.1 QMobile 356
7.3 Photo Station 384
7.4 Music Station 405
7.5 ダウンロードステーション (Download Station) 425
7.6 監視ステーション (Surveillance Station) 448
7.7 iTunes サービス 456
7.8 UPnPメディアサーバ 459
7.9 MySQLサーバ 461
7.10 QPKG Center 463
7.11 Syslogサーバ 467
7.12 RADIUS サーバ 472
7.13 バックアップサーバー 476
7.14 アンチウイルス 480
7.15 TFTPサーバー 489
7.16 VPN サービス 490
7.17 LDAP サーバー 506
8. バックアップ.....511

8.1 リモートレプリケーション 511
8.2 クラウドバックアップ 536
8.3 Time Machine 546
8.4 外部ドライブ 552
8.5 USBワンタッチコピー 566
9. 外部デバイス.....569
9.1 外部ストレージデバイス 569
9.2 USBプリンタ 579
9.2.1 Windows 7, Vistaユーザー 582
9.2.2 Windows XPユーザー 589
9.2.3 Mac OS 10.6 591
9.2.4 Mac OS 10.5 594
9.2.5 Mac OS 10.4 599
9.2.6 Linux (Ubuntu 10.10) 604
9.3 UPS設定 609
10. MyCloudNAS サービス.....614
10.1 MyCloudNAS ウィザード 615
10.2 MyCloudNAS構成 624
10.3 自動ルータ構成 632
11. システムステータス.....635
11.1 システム情報 635
11.2 システムサービス 636
11.3 リソースモニタ 637
12. LCDパネルの使用.....640
13. インターネットからQNAP NASをアクセスする(DDNSサービス).....647
14. QNAP NASでSMS、電子メール、IM Alertをセットアップします.....656
15. メディアプレーヤー用にUPnPメディアサーバをセットアップする.....668
16. QNAP NASにてPHPBBフォーラムをホストする.....677
17. NAS メンテナンス.....689
17.1 シャットダウン/再起動 690
17.2 システム温度保護 692
18. GNU GENERAL PUBLIC LICENSE.....693

1．注意

QNAP製品をお選びいただき、ありがとうございます。このユーザーマニュアルでは、Turbo NASの使用に関して詳細に説明しています。本書をよく読み、Turbo NASの強力な機能をお楽しみください。

- 「Turbo NAS」または「NAS」と呼ばれます。
- 本書はTurbo NASのすべての機能について説明します。ご購入いただいた製品は特定のモデルに限定されている一部の機能をサポートしていない場合があります。

法的事項

すべての特徴、機能、その他の製品仕様は予告なしに変更されることがあります。この情報は予告なく変更される場合があります。

QNAPおよびQNAPの口ゴはQNAP Systems, Inc.の登録商標です。他のすべてのブランドおよび製品名は、個々の所有者の登録商標です。また、® あるいは ™ の記号は本書では省略します。

保証の制限

いかなる場合も、QNAP Systems, Inc. (QNAP)は直接、間接、特殊、付随的、または結果的ソフトウェア、またはそのマニュアルから製品に対して支払われた価格を超えて責任を負うことはありません。QNAPはその製品に対して返金することはありません。QNAPはその製品または本マニュアルおよび付随するすべてのソフトウェアの内容や使用に関して明示的または黙示的または法的に保証または表明するものではなく、その品質、性能、商業的価値、特定目的への適合性を特定的に表明するものではありません。QNAPは製品、個人または企業への事前の予告なしにソフトウェア、またはマニュアルを改訂または更新する権利を留保します。

データの損失を避けるために、システムのバックアップを定期的にとってください。QNAPはいかなる種類のデータ損失または回復に関して責任を負うことはありません。

NASパッケージのコンポーネントを返品して返金を受ける場合、念入りに輸送用の梱包がなされていることを確認してください。不適切な梱包によるいかなる形の損傷も、補償の対象外となります。

1.1 規制の通知

FCC (連邦通信委員会)通知

この機器はテストの結果、FCC Rules の Part 15 に規定されたクラス B デジタル機器の制限に準拠していることが確認済みです。これらの制限は、住宅地区で使用する際に、有害な電波干渉から適正に保護することを目的としています。この機器は無線周波エネルギーを生成、使用、および放射することがあるため、指示に従わずに取り付けたり使用したりした場合は、有害な干渉を発生させる恐れがあります。ただし、特定の設置環境で干渉が起きないことを保証するものではありません。この機器がラジオやテレビの受信を妨害していることを、機器のオフ / オン切り替えにより確認できる場合、次のいずれかを行って妨害に対処することをお勧めします。

- 受信アンテナの向きを変える、または設置場所を移動する。
- 装置と受信機の距離を離す。
- この機器を受信機が接続されている回線と別のコンセントに接続する。
- 販売代理店か、ラジオ、テレビに詳しい技術者に相談する。

準拠に関する責任当事者の明示的な承認なしに変更や修正を行うと、ユーザーは装置を操作する権利が無効になることがあります。
シールドインターフェイスケーブルが提供されている場合、FCC規制に準拠するためにはそれらを使用する必要があります。

CE通知

クラスBのみ。

1.2 本書で使用される記号

警告	このアイコンは、必ず指示に従うことを示します。指示を遵守しないと人身事故または死亡の原因となることがあります。
注意	このアイコンは、その操作によってディスクの消去または喪失を引き起こすことを示します。指示を遵守しないとデータの損失、ディスクの損傷、または製品の損傷の原因となることがあります。
重要	このアイコンは、提供される情報が重要であるか、あるいは法的規制に関連することを示します。

1.3 安全に関する警告

1. NASは0℃-40℃の温度、および0%-95%の相対湿度で標準作動します。環境がよく換気されていることを確認してください。
2. 電源コードとNASに接続されたデバイスは、正しい供給電圧(100W、90-264V)を提供する必要があります。
3. NASを直射日光にさらしたり、化学物質の傍に設置しないでください。環境温度と湿度が最適レベルに設定されていることを確認してください。
4. クリーニングする前に、電源コードと接続されているすべてのケーブルを抜いてください。乾いたタオルでNASを拭きます。化学薬品やエアゾールでNASをクリーングしないでください。
5. サーバの正常な作動と過熱の原因となるため、NASの上に物を置かないでください。
6. ハードディスクを取り付けるとき、正常に作動するように、製品パッケージ付属の平頭ねじを使用してNASにハードディスクをしっかり留めてください。
7. 液体の傍にNASを設置しないでください。
8. 不安定な表面の上にNASを設置しないでください。落下して負傷の原因となります。
9. NASを使用しているとき、電圧が正しいことを確認してください。不明な場合は、販売店または地域の電力会社にお問い合わせください。
10. 電源コードの上に物を置かないでください。
11. いかなる場合でも、NASを自分で修理することはおやめください。製品を不適切に分解すると、感電またはその他の危険にさらされます。質問がございましたら、販売店にお問い合わせください。
12. シャーシNASモデルはサーバ室に配置し、認定されたサーバ管理者あるいはIT管理者のみメンテナンスしてください。サーバ室は施錠あるいはキーカード· アクセスとされ、認定されたスタッフのみがサーバ室に入室することができます。

警告:

- バッテリーを不適切に交換すると、爆発の危険性があります。製造元により推奨されたものと同一あるいは同等の形式のバッテリーとのみ交換してください。使用済みのバッテリーは製造元の指示に従って廃棄してください。
- システム内のファンにはけして触れないでください。重大な負傷を招く恐れがあります。

2. 始めましょう

ハードウェアのインストール

ハードウェアのインストール情報については、製品パッケージにある「Quick Installation Guide（クイックインストールガイド）」（QIG）を参照してください。QIG は製品 CD-ROM または QNAP Web サイト(http://www.qnap.com)でもご覧いただけます。

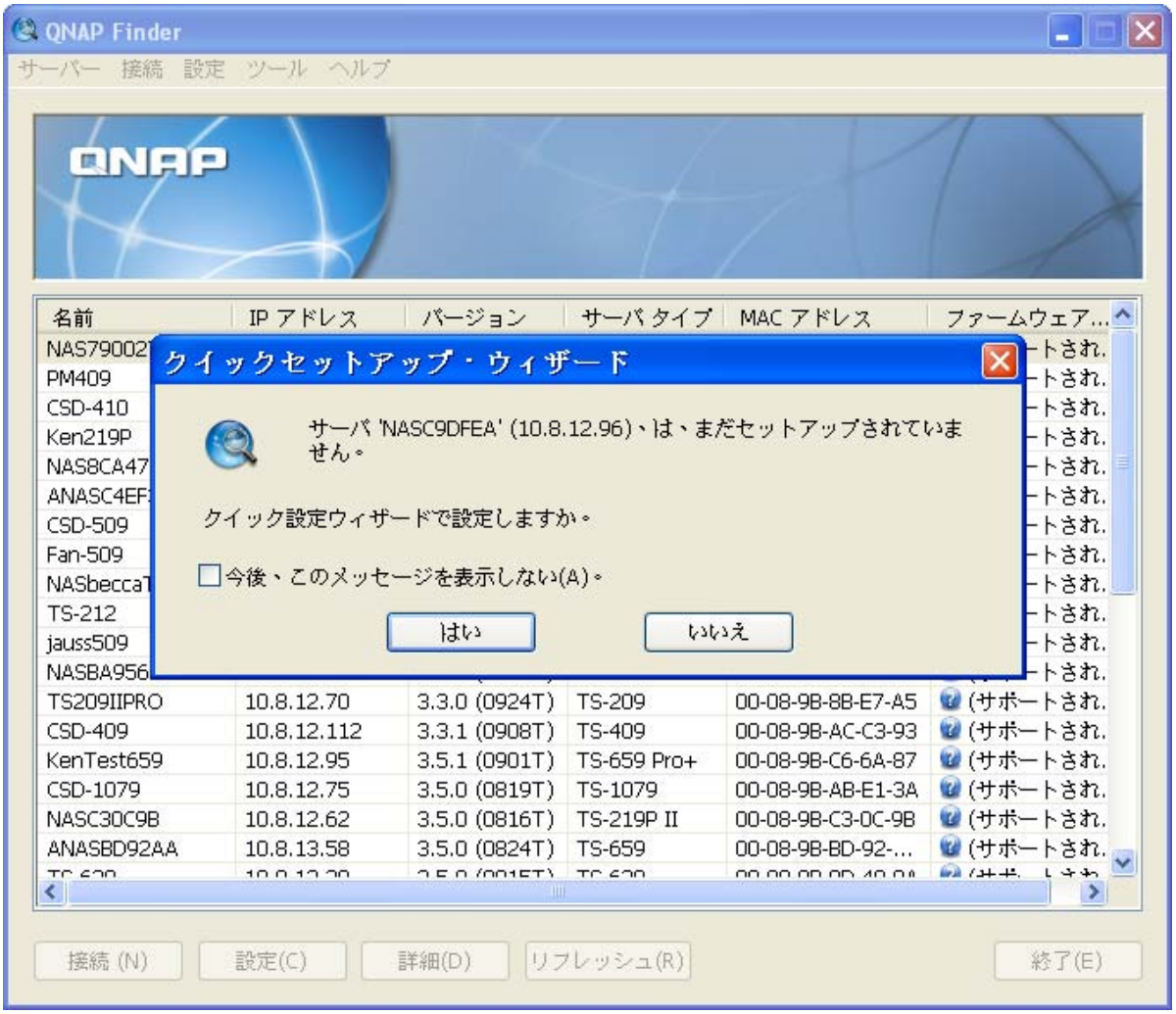
ソフトウェアのインストール

NAS ハードエアをインストールしたら、ソフトウェアのインストールに進みます。次のデモは Windows OS に基づきます。

1. 製品 CD-ROM から QNAP ファインダーをインストールします。

2. QNAP ファインダーを実行します。ファインダーがお使いのファイアウォールでブロックされている場合は、ユーティリティのブロックを解除します。

3. QNAP ファインダーが、構成されていない NAS を検出します。[Yes(はい)] をクリックすると、NAS のクイックセットアップを実行するように指示されます。

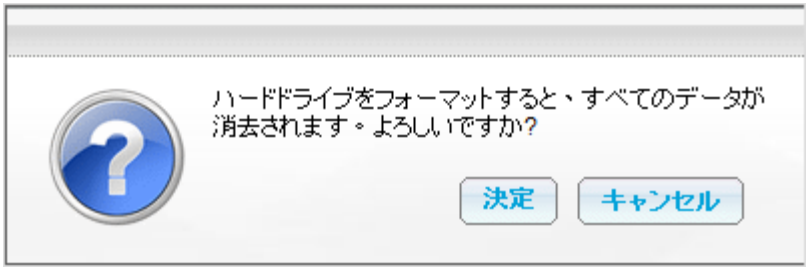


4. ［OK］をクリックして続行します。

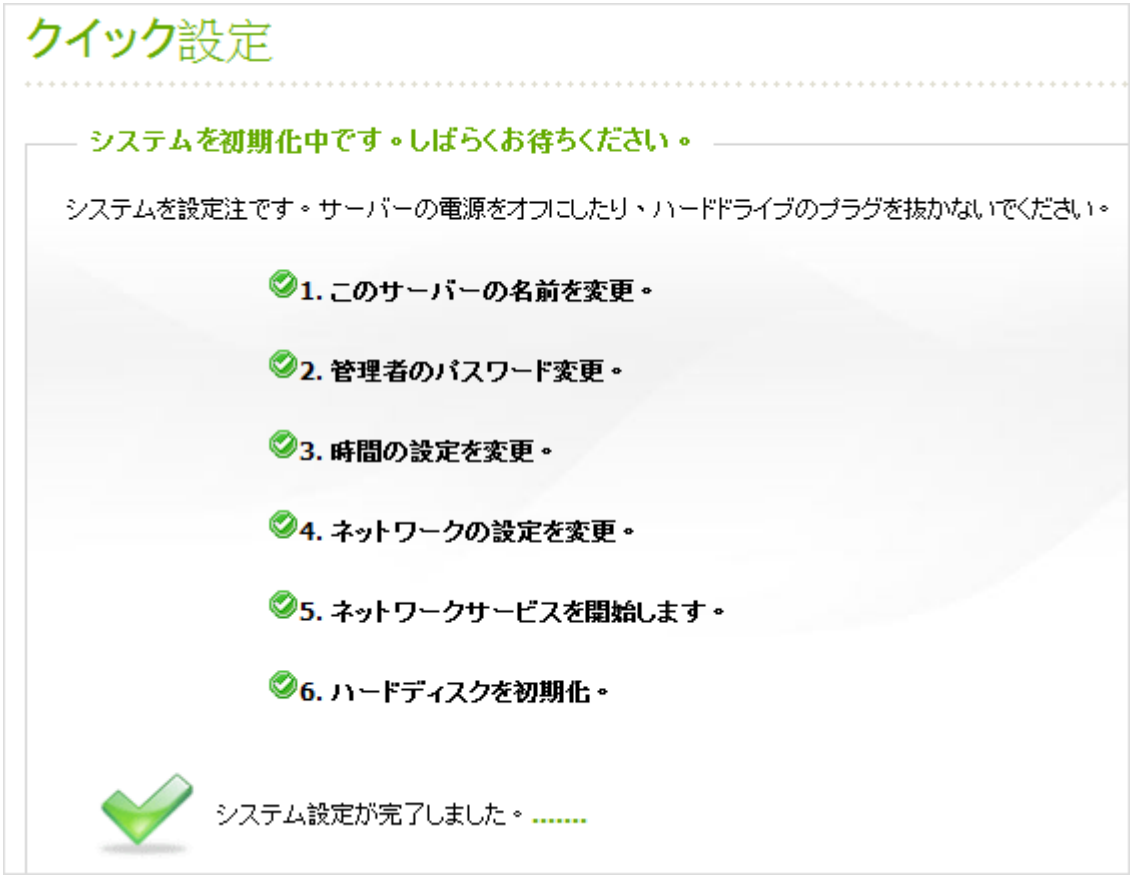
5. お使いのデフォルトの Web ブラウザが開きます。指示に従って NAS を構成します。

6. 最後に [START INSTALLATION（インストールの開始）] をクリックします。

7. インストールされているハードディスクがすべて初期化されて、すべてのデータが消去されます。[OK] をクリックして続行します。



8. 完了したら、「Return to system administration page（システム管理ページに戻る）」をクリックするか、または、Web ブラウザに NAS IP を入力して NAS のウェブ管理ページに接続します。



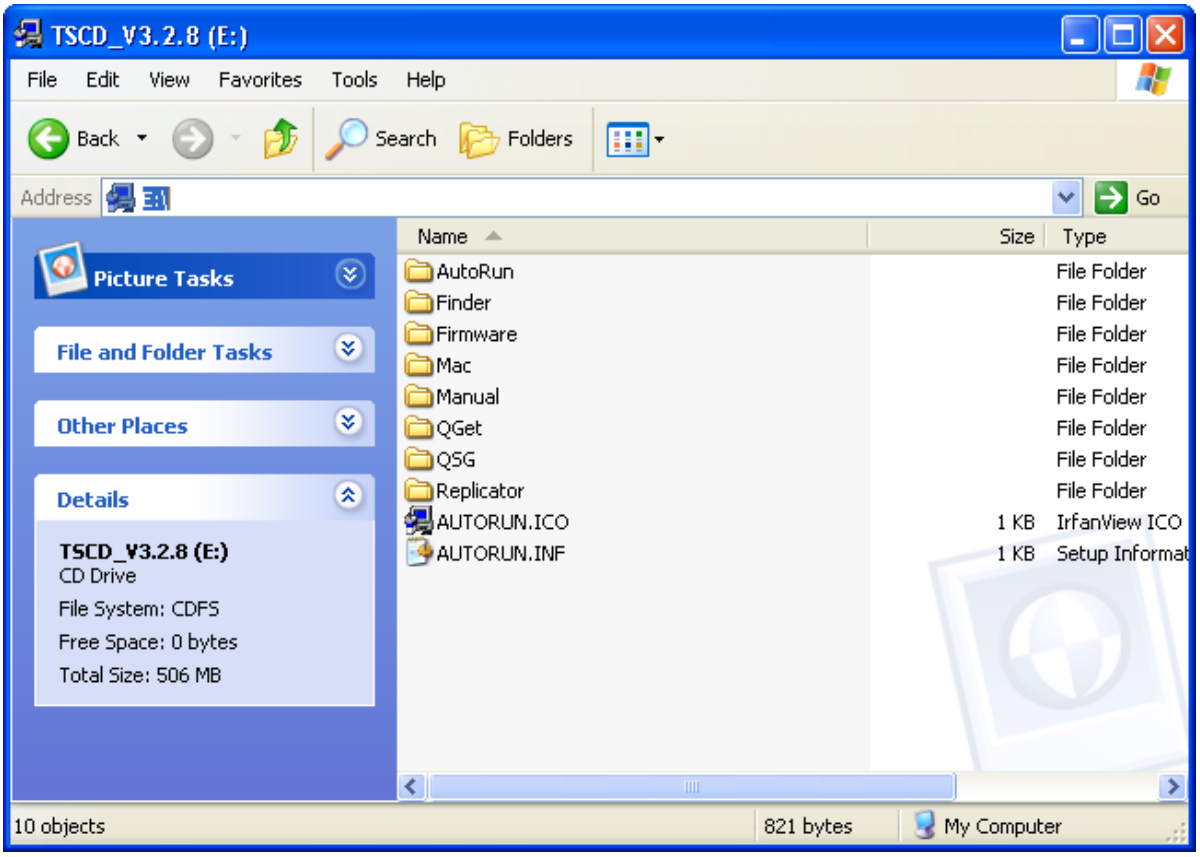
2.1 CD-ROM の検索

NAS CD-ROM には、 Quick Installation Guide（クイックインストールガイド）（QIG）、ユーザーマニュアル、アプリケーションノート、ソフトウェアユーティリティ QNAP ファインダー、NetBak レプリケータ、QGet などのドキュメントが含まれています。

CD-ROM を検索して次のコンテンツにアクセスできます:

- Finder (ファインダー): QNAP ファインダー(Windows OS 用)のセットアッププログラム。
- Firmware (ファームウェア): お買い上げいただいた NAS モデル用のファームウェア IMG ファイル。
- Mac: QNAP ファインダー(Mac OS 用)のセットアッププログラム。
- Manual (マニュアル): Quick Installation Guide(クイックインストールガイド)、ソフトウェアユーザーマニュアル、Turbo NAS のハードウェアマニュアル。
- QGet: QGet ダウンロードユーティリティ(Windows OS 用)のセットアッププログラム。
- QSG: NAS のハードウェアのインストール方法を表示します。
- Replicator (レプリケータ): NetBak レプリケータ(Windows OS から QNAP NAS へのデータバックアップ用 Windows ユーティリティ)のセットアッププログラム。

上記のコンテンツは QNAP Web サイト(http://www.qnap.com)でもご覧いただけます。



2.2 ハードディスクの推奨リスト

当製品は主要なメーカーの2.5/ 3.5インチSATAハードディスクドライバに対応しています。HDD対応表は、http://www.qnap.com にてご覧ください。

QNAPはいかなる理由でもハードディスクの誤使用または不適切な取り付けによる製品の損傷/誤作動またはデータ損失/回復に対していかなる責任も負いません。

NASにこれまで設置されたことのないハードドライブ(新品あるいは中古)を設置する場合は、ハードドライブは自動的にフォーマット及びパーティションされ、すべてのディスクデータは消去されます。

2.3 システムステータスのチェック

LED ディスプレイ & システムステータス概観

LED	色	LED状態	説明
システムステータス	赤/緑	0.5秒ごとに赤と緑に交互に点滅	1) NASのハードドライブのフォーマット中です。 2) NASの初期化中です。 3) システムファームウェアの更新中です。 4) RAID再構築が進行中です。 5) RAIDのオンライン容量拡張が進行中です。 6) オンラインRAIDのレベル転換が進行中です。
		赤	1) ハードドライブが無効です。 2) ディスクボリュームが最大容量に達しました。 3) ディスクボリュームがフルになります。 4) システムファンが故障しています。(TS-119は、スマートファンをサポートしません。) 5) ディスクデータにアクセス中(読み取り/書き込み)エラーが発生しました。 6) ハードドライブのセクタに問題があります。 7) NASは読み取り専用モードに低下しています。(RAID 5あるいはRAID 6 構成において 2 台のメンバードライブに支障あり、データは読み取り可能 8) (ハードウェア自己テストエラー)
		0.5秒ごとに赤く点滅	NASは低下モードです。(RAID 1、RAID 5あるいはRAID 6構成において 1 台のメンバードライブに支障あり)
		0.5秒ごとに緑に点滅	1) NASが起動しています。 2) NASが構成されていません。 3) ハードドライブがフォーマットされていません。
		緑	NASの準備が完了しました。
		オフ	NASの全てのハードドライブがスタンバイモードです。
LAN	オレンジ色	オレンジ色	NASはネットワークに接続しました。
		オレンジ色に点滅	ネットワークがNASにアクセス中です。
10 GbE*	緑	緑	10GbEネットワーク拡張カードが取り付けられています。
		オフ	10GbEネットワーク拡張カードが取り付けられていません。
HDD	赤/緑	赤く点滅	ハードドライブのデータにアクセス中ですが、プロセ

LED	色	LED状態	説明
			スの途中で読み取り/書き込みにエラーが生じました。
		赤	ハードドライブに読み取り/書き込みエラーが生じました。
		緑で点滅	ハードドライブのデータにアクセス中です。
		緑	ハードドライブにアクセスすることが出来ます。
USB	青	0.5秒ごとに青く点滅	1) 前面USBポートに接続されたUSB機器が検出されました。 2) 前面USBポートに接続されたUSB機器はNASから取り外されました。 3) NASの前面USBポートに接続されたUSB機器がアクセスされました。 4) 外部USB/eSATA機器にデータをコピー/コピーされました。
		青	前面USB機器が検出されました。(機器のマウント後)
		オフ	1) USB機器が検出できません。 2) NASは、前面USBポートに接続されたUSB機器へ/からのデータコピーを完了しました。
eSATA**	オレンジ色	点滅	eSATAデバイスにアクセスしています。
		オフ	eSATA機器が検出できません。

* 10 GbEネットワーク拡張機能はTS-879 Pro、TS-1079 Pro、TS-879U-RP、TS-1279U-RP、TS-EC879U-RP、TS-EC1279U-RPでのみサポートされています。

** TS-210、TS-212、TS-219、TS-439U-SP/RP、TS-809 Pro、TS-809U-RPは、eSATAポートをサポートしません。

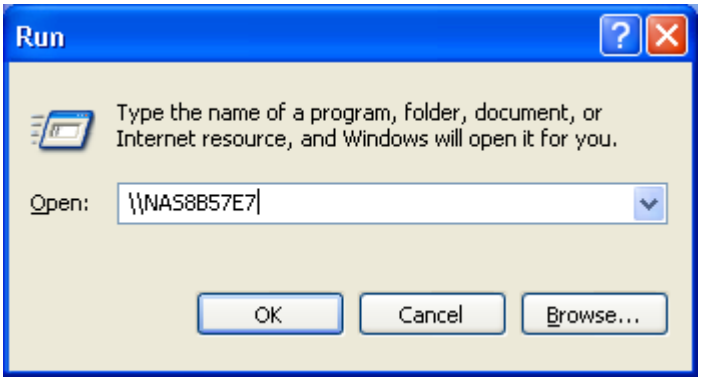
アラームブザー (アラームブザーは 「システムツール」 >「ハードウェア設定」 で無効化できます)

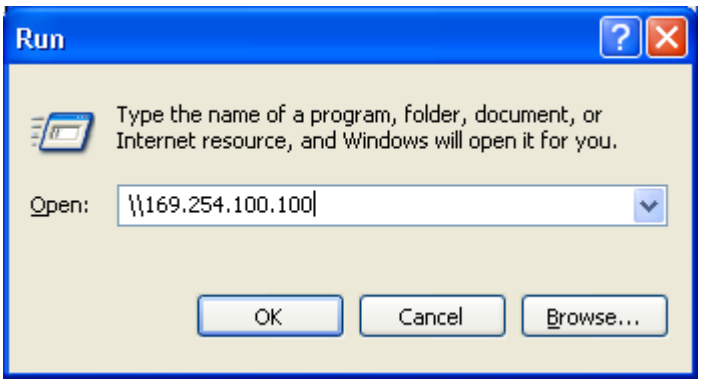
ビープ音	回数	説明
短いビープ(0.5秒)	1回	1) NASが起動しています。 2) NASがシャットダウンしています。 (ソフトウェアシャットダウン) 3) ユーザーにより、NASをリセットするリセットボタンが押されました。 4) システムファームウェアが更新されました。
短いビープ(0.5秒)	3回	ユーザーにより、正面USBポートの外部メモリデバイスへNASのデータコピーが試行されましたが、コピーに失敗しました。
短いビープ(0.5秒)、長いビープ(1.5秒)	3回、5分ごと	システムファンが故障しています。(TS-119は、スマートファンをサポートしません。)
長いビープ(1.5秒)	2回	1) ディスクボリュームがフルになります。 2) ディスクボリュームが最大容量に達しました。 3) NASのハードドライブは低下モードです。 4) ユーザーによりHDD再構築プロセスが開始されました。
	1回	1) NASが強制終了されました。 (ハードウェアシャットダウン) 2) NASの電源投入に成功しました。準備完了です。

2.4 NAS ネットワーク共有に接続

Windows ユーザー

1. 次の手段によって、NASのパブリックフォルダにアクセスできます。
   a. マイネットワークを開き、NASのワークグループを探します。サーバーが見つからない場合、ネットワーク全体を参照してNASを検索してください。NASの名前をダブルクリックして、接続します。
   b. Windowsで[ファイル名を指定して実行]機能を使用します。\\[NAS name] または \\[NAS IP]を入力して、NASの共フォルダにアクセスします。





2. パスワード・フィールドが表示されるので、管理者名とパスワードを入力します。

   デフォルトのユーザー名：admin

   パスワード：admin

3. ネットワーク共にファイルをアップロードできます。

Mac ユーザー

1. "Go" (移動) > "Connect to Server" (サーバに接続)を選択します。
2. ディスクをマウントする方法は2 つあります。
   - AFP:NAS IP あるいは afp://NAS_IPをタイプ
   - SMB:smb://NAS_IP あるいは NAS_名前をタイプ

   例えば、169.254.100.100 あるいはsmb://169.254.100.100
3. "Connect" (接続)をクリックします。

Linuxユーザー

Linuxでは、以下のコマンドを実行します:

mount -t nfs <NAS IP>:/<Network Share Name> <Directory to Mount>

例えば、NASのIPアドレスが192.168.0.1で、/mnt/pubディレクトリ内のネットワーク共フォルダ「public」にリンクする場合、以下のコマンドを使用します:

mount -t nfs 192.168.0.1:/public /mnt/pub

注:上記コマンドを初期化するには、「root」ユーザーでログインしてください。

定義したユーザーIDでログインすると、マウントしたディレクトリを使ってネットワーク共ファイルにアクセスできます。

2.5 Web ブラウザを使って NAS に接続

WindowsあるいはMacのウェブブラウザによりNASへアクセス

1. 次の方法でNAS Web管理ページにアクセスできます。
   a. Finderを使用してNASを検出します。
   b. ウェブブラウザを開いて、http://[NAS IP]:8080 と入力します。

   注:デフォルトNAS IPは169.254.100.100:8080です。NASがDHCPを使用するよう構成してある場合は、Finderを利用してNASのIPアドレスを確認することが出来ます。Finderを実行しているコンピュータとNASが同じサブネットに接続していることを確認してください。NAS IPが検索できない場合、NASをコンピュータに直接接続し、Finderを再度実行してください。

2. NASのログインページのドロップダウンメニューから、あるいはNASにログインした後に、表示言語を選択することが出来ます。

3. NAS UIを参照する場合に、標準表示とフロー表示のどちらを使用するか選択することが出来ます。

標準表示:

フロー表示:

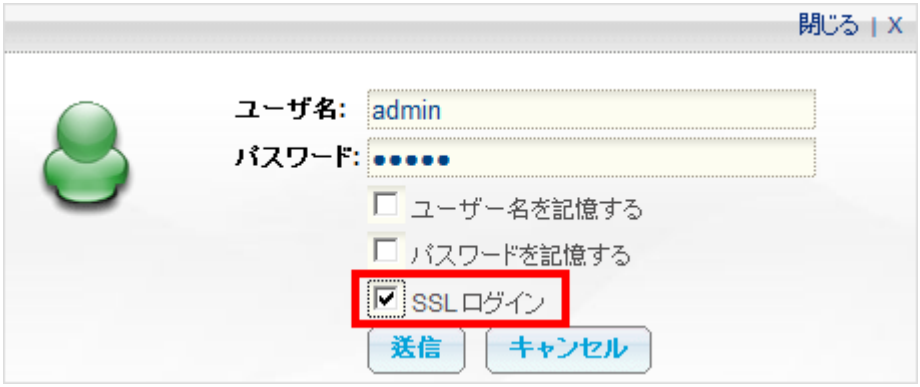
4. NASの管理ページが表示されたら、「管理」をクリックします。ユーザー名およびパスワードを入力してログインします。

デフォルトのユーザー名：admin パスワード：admin

管理者権限のないユーザーアカウントで管理インターフェイスにログインした際は、ログインパスワードの更のみ行うことが可能です。ご注意ください。

5. NASは、暗号化転送によるサーバの設定と管理を可能にするSSLセキュアログインをサポートしています。この機能を使用するには、管理ページのSSLログインボックスをチェックして、サーバにログインします。

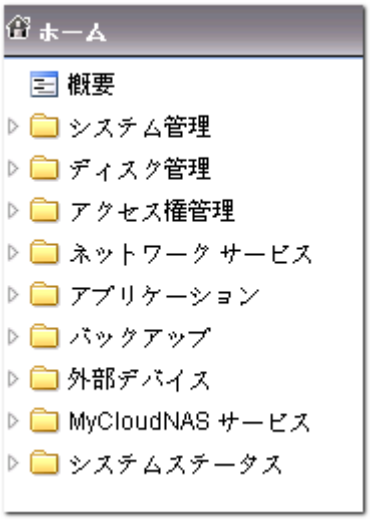
> 注:NASがNATゲートウェイの背後に設置されている場合、イーサネットからセキュアログインでNASにアクセスするためには、NATのポート443を開いて、同ポートをNASのLAN IPにフォワードする必要があります。



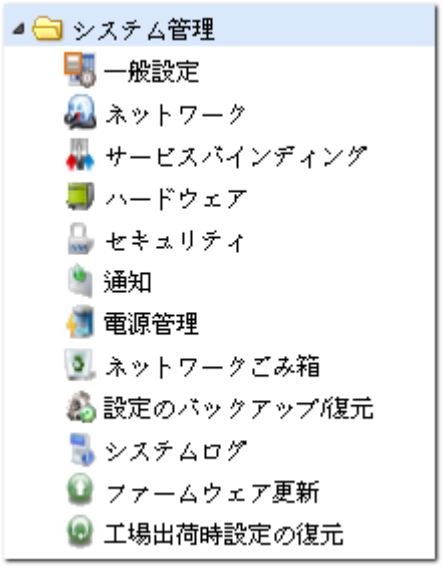
NAS にログインすると、ホームページが表示されます。いくつかの機能の便利なセットアップ用のソフトウェアウィザード、QNAP 技術サポート、フォーラム、Wiki、QNAP からの最新の RSS* ニュースフィードへのリンクが表示されます。

*これらの機能を動作させるには、NAS をインターネットに接続しなければならないことに注意してください。

サーバ管理は次の8 つに分かれています。



セクション名の隣にある参画のアイコンをクリックし、樹状表示を広げ、各セクション下の項目を一覧表示します。



ウェブファイルマネージャ、ダウロードステーション、マルチメディアステーション、および監視ステーションなどのサービスにアクセスするには、ドロップダウンメニューから選択するか、あるいはログインページのアイコンをクリックしてください。

NASにログイン後、ページ上部にあるアイコンをクリックしてサービスにアクセスすることが出来ます。

2.6 システム移行

システム移行により、既存のQNAP NASユーザーは、データ転送やシステムの再構成なしにご使用のNASを他のQNAP NAS新モデルにアップグレードすることができます。オリジナルのハードディスクドライブ(HDD)を、元のHDDの順番に従って新しいNASに設置し、NASを再起動するだけです。

異なるハードウェアデザインに伴い、NASは自動的にファームウェアの更新が必要かどうかをシステム移行前に確認します。移行が完了した後は、設定およびデータは新しいNASにおいて全ての維持され、適用されます。

下記の表はシステム移行をサポートするNASモデルを表記しています。

元のNAS	移行先のNAS	注記
TS-x10、 TS-x19、TS-x39、TS-509、TS-809、SS-x39、TS-x59, TS-x12	TS-x10、TS-x19、TS-x39、TS-509、TS-809、SS-x39, TS-x12	ファームウェア更新が必要です。
TS-x10、TS-x19、TS-x39、TS-509、TS-809、SS-x39、TS-x59, TS-x12, TS-x79	TS-x59, TS-x79	ファームウェア更新は必要ありません。

注:

- 保存先に十分なドライブベイがあり、ソース NAS のディスクボリューム内のハードディスクドライブの数に対応できることを確認します。
- SS-x39 シリーズがサポートするのは 2.5 インチ HDD だけです。
- 暗号化されたディスクボリュームの付いたNASは、ファイルシステム暗号化に対応しないNASに移動できません。ファイルシステム暗号化はTS-110、TS-119、TS-210、TS-219、TS-219P、TS-410、TS-419P、TS-410U、TS-419U、TS-119P+、TS-219P+、TS-419P+、TS-419U+、TS-112、TS-212、TS-412ではサポートされません。
- 非 TS-x79 モデルから TS-x79 モデルに移行した場合、マルチメディアステーション、ダウンロードステーション、iTunes サーバーおよび UPnP メディアサーバー機能は削除されます。ネットワーク共有の Multimedia/Qmultimedia、Download/Qdownload およびすべてのダウンロードされたファイルは保存されます。

移行先NAS	システム移行に対応するディスクボリューム
1 ベイ NAS	1 ドライブシングルディスクボリューム
2 ベイ NAS	1–2 ドライブシングルディスクボリューム/JBOD/RAID 0、 2 ドライブ RAID 1。
4 ベイ NAS	1–4 ドライブシングルディスクボリューム/JBOD/RAID 0、 2 ドライブ RAID 1、 3–4 ドライブ RAID 5、 4 ドライブ RAID 6、 4ドライブRAID 10。
5 ベイ NAS	1–5 ドライブシングルディスクボリューム/JBOD/RAID 0、 2 ドライブ RAID 1、 3–5 ドライブ RAID 5、 4–5ドライブ RAID 6、 4ドライブRAID 10。
6 ベイ NAS	1–6 ドライブシングルディスクボリューム/JBOD/RAID 0、 2 ドライブ RAID 1、 3–6 ドライブ RAID 5、 4–6 ドライブ RAID 6、 4ドライブまたは6ドライブRAID 10。
8 ベイ NAS	1–8 ドライブシングルディスクボリューム/JBOD/RAID 0、 2 ドライブ RAID 1、 3–8 ドライブ RAID 5、 4–8 ドライブ RAID 6、 4ドライブ、6ドライブ、または8ドライブRAID 10。

システム移行を実行するには、以下の手順に従ってください。

> 注：サーバの破損あるいは重大な負傷を防ぐため、システム移行手順は認可を受けたサーバ管理者あるいはIT管理者が行ってください。

1. 元のNASの電源をオフにして、HDDのプラグを抜きます。
2. HDDを元のトレイから取り外し、新しいNASのHDDトレイへと設置します。
3. HDDを移行先のNAS (新しいモデルに接続します。HDDの設置順が元のNASの場合と同じであるよう確認してください。
4. クイックインストールガイド(QIG) の説明に従い、新しいNASの電源およびネットワークケーブルを接続します。
5. 新しいNASの電源を入れます。ウェブ管理インターフェイスに管理者としてログインします。(デフォルトログイン:admin、パスワード:adminとなります)
6. 新しいNASにおいてファームウェアを更新するよう求められた場合は、説明にしたがってファームウェアをダウンロードし、インストールします。
7. "Start Migrating" (移行開始)をクリックします。システム移行後、NASが再起動します。全てのデータおよび設定が維持されます。

システム移行の実行をしない場合は、QIGの説明に従いNASを初期化してください。

システムデザインの相違により、システム移行後いくつかのシステム設定は削除されることがあります。新しいNAS上で以下の設定の再構成が必要な場合があります。

- Windows AD
- いくつかのQPKGの再インストール(例:XDove)

3．システム管理

全般設定 33

ネットワーク 37

サービスバインディング 56

ハードウェア 58

セキュリティ 62

通知 65

電源管理 72

ネットワークごみ箱 74

設定のバックアップ/復元 75

システムログ 76

ファームウェア更新 82

工場出荷時設定の復元 86

3.1 全般設定

システム管理

NASの名前を入力します。サーバ名の長さは最大14文字で、アルファベット、数字、ハイフン(-)を含むことができます。サーバ名にスペース、ピリオド(.)、を含めることはできません。

システムサービスのポート番号を指定します。デフォルトポートは8080です。このポートを使うサービス：システム管理、ウェブファイルマネージャ、マルチメディアステーションおよびダウンロードステーション。

セキュリティ接続(SSL)を効化

ユーザーがNASにhttpsによってアクセスできるよう、セキュリティ接続(SSL) を効化し、ポート番号を入力します。"Force secure connection (SSL) only" (セキュリティ接続(SSL)のみ使用)のオプションを効化した場合、ユーザーはhttps接続でのみウェブ管理ページにアクセスできます。

日付と時刻

本製品が現在時刻として保持する日付、時間を設定し、タイムゾーンを選択します。不正確な日付と時間が設定されている場合は、次のような問題が生じる可能性があります。設置後必ず最初に日付と時刻を設定してください。

- 本製品に保存するファイルの作成/更新日時等が正しく記録されません。結果としてネットワーク上のどのファイルが新しいかを判断できなくなります。
- ログが正しく記録されません。結果としていつどのファイルにアクセスされているかを判断できなくなり、ログを記録する意味がなくなります。

サーバ時間をコンピュータの時間に合わせて設定する

サーバ時間をご使用のコンピュータの時間と同期するには、このオプションの隣にある'Update now(今すぐ更新)'をクリックします。

インターネットタイムサーバで自動的に同期化します

指定したんNTP (ネットワークタイムプロトコルサーバを効または使用して、システムの日付と時刻を自動的に更新できます。時刻を調整する時間間隔を入力します。このオプションは、NASがインターネットに接続されている時のみに使用できます。

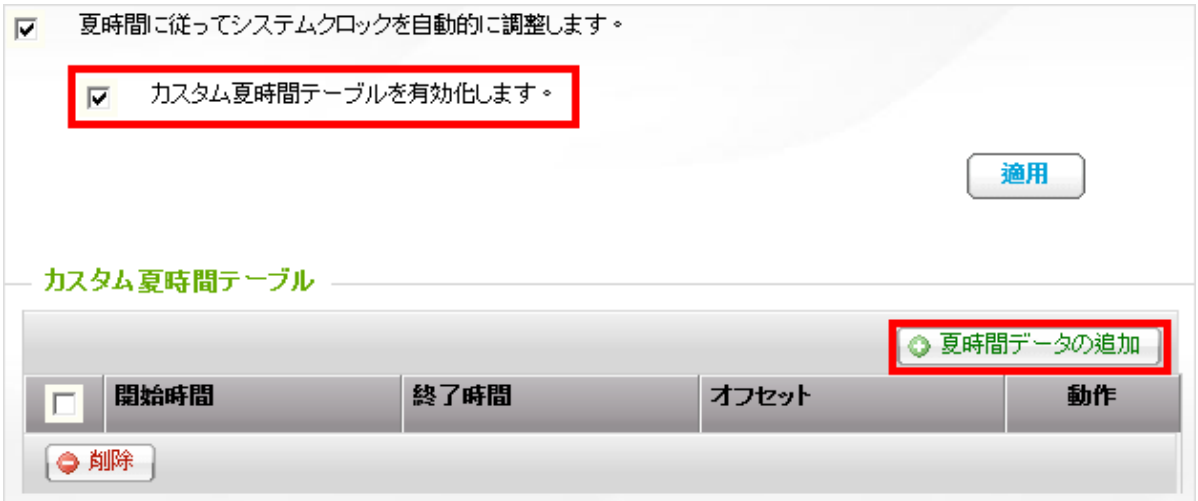
注:初めてNTPサーバを効にするとき、時間が正しく調整されるまで時刻の同期に数分かかることがあります。

夏時間

ご使用の地域が夏時間 (DST: Daylight Saving Time) を採用している場合、「夏時間に従ってシステムクロックを自動的に調整します 」を効にしてください。「適用」をクリックします。「日付と時刻」のセクションで選択したタイムゾーンの最新DSTスケジュールが表示されます。システム時刻はこのDSTに従って自動的に調整されます。

ご使用の地域がDSTを採用しない場合は、このページのオプションが選択できません。

夏時間表を手動で入力するには、「カスタム夏時間テーブルを効化します」オプションにチェックしてください。「夏時間データの追加」をクリックして夏時間スケジュールを入力します。次に「適用」をクリックして夏時間を保存します。



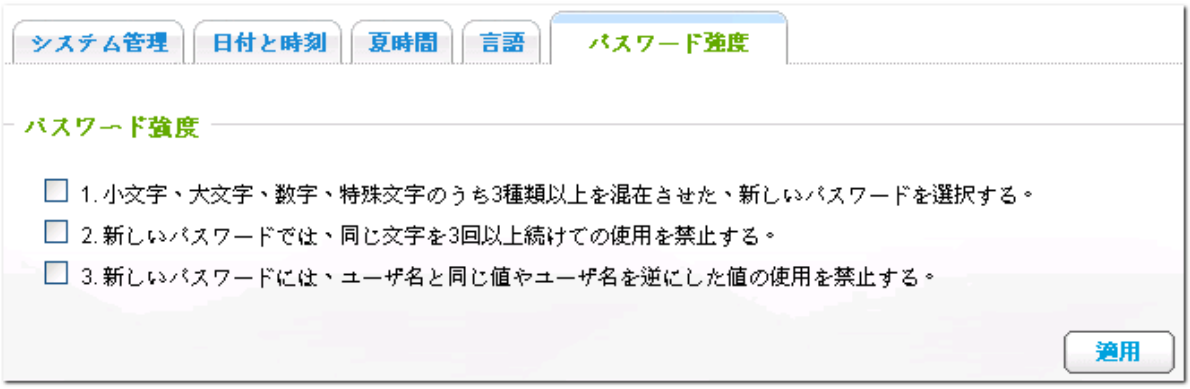
言語

NASがファイルとディレクトリの表示に使用する言語を選択します。

注：NASのすべてのファイルとディレクトリは、ユニコードを使用して作成されます。FTPクライアントまたはPCのOSが例えばWindows 95/98/MEのようにユニコードをサポートしない場合、サーバのファイルとディレクトリを表示するためにこのOSと同じ言語を選択してください。

パスワード強度

パスワード設定規則はここで設定することができます。設定を適用した後、システムは自動的にパスワードの効性を確認します。



3.2 ネットワーク

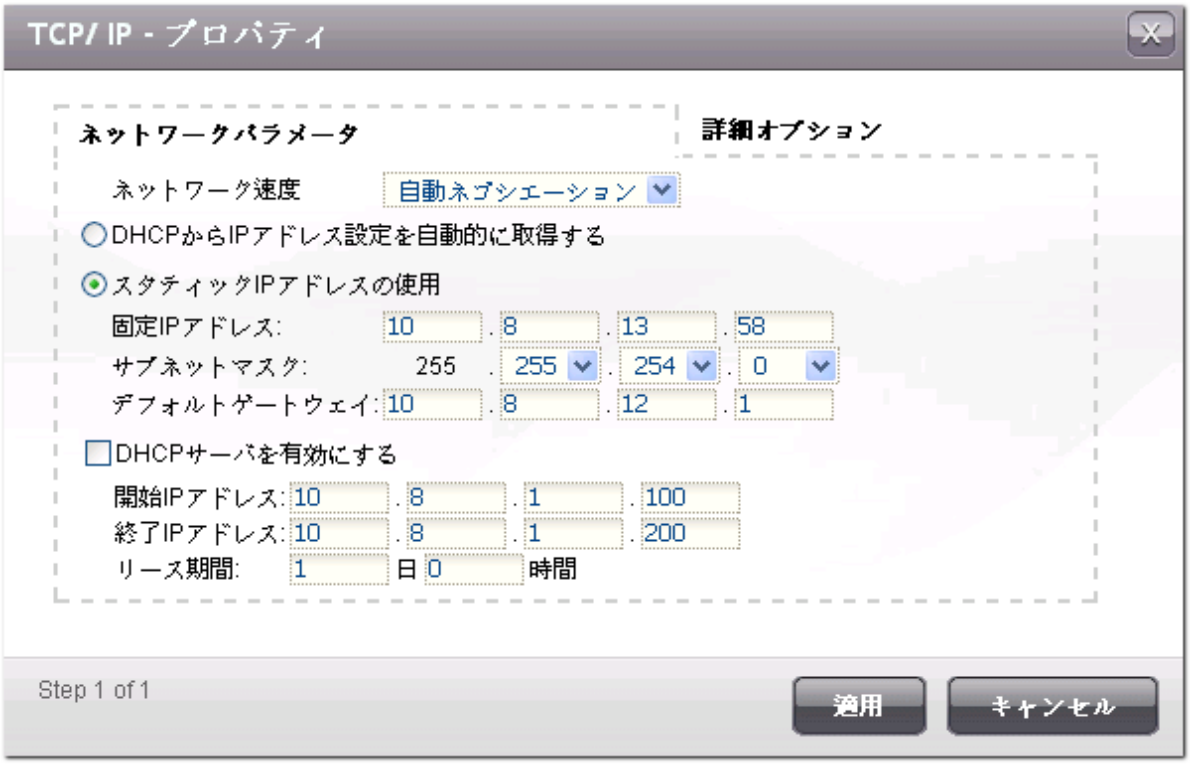
TCP/IP

(i) IPアドレス

NASのTCP/IP 設定をこのページで構成することが出来ます。 をクリックしてネットワーク設定を編集します。

2つのLANポートをサポートするNASでは、両方のネットワークインターフェースを2つの異なるスイッチに接続し、TCP/IP設定を構成できます。NASは2つの異なるサブネットネットからアクセスできるようにする、2つのIPアドレスを取得します。これは複数IPアドレス設定として知られています*。ファインダを使用してNAS IPを検出する場合、Ethernet 1のIPはLAN 1にのみ表示され、Ethernet 2のIPはLAN 2のみに表示されます。デュアルLAN接続のポートトランキングモードを使用するには、セクション(iii)を参照してください。

* TS-110、TS-119、TS-210、TS-219、TS-219P、TS-119P+、TS-219P+、TS-112、およびTS-212は、1つのGiga LANポートのみを提供します。従って、デュアルLAN構成やポートトランキングをサポートしません。



TCP/IPプロパティページで、以下の設定を構成してください。

ネットワーク速度

NASが接続されているネットワーク環境に基づいてネットワーク転送速度を選択します。"Auto negotiation" (自動ネゴシエーション)を選択します。これにより、NASは転送速度を自動的に調整します。

DHCP 設定

DHCP は多くの商業用ブロードバンドネットワークで使用されています。DHCP はIP アドレスを自動的に取得し、自動的に設定をおこないます。

手動設定

ネットワークに適した本製品のIP アドレスを手動で指定します。同じネットワーク内でIP アドレスを重複して設定することはできませんので、必ずネットワーク管理者等に空いているIP アドレスをご確認ください。

DHCP サーバー

DHCP（動的ホスト設定プロトコル）サーバーは、ネットワーク上のクライアントに IP アドレスを割り当てます。「Enable DHCP Server（DHCPサーバを有効にする）」を選択し、NAS の存在するローカルネットワーク上に DHCP サーバーが無い場合、NAS を DHCP サーバーに設定します。

> 注：
>
> - DHCP サーバーがローカルネットワーク上に存在する場合は、IP アドレスの競合またはネットワークアクセスエラーを避けるために、DHCP サーバーを有効化しないでください。
> - DHCP サーバーオプションは、デュアル LAN NAS の両 LAN ポートがネットワークに接続され、スタンドアロン IP 設定がされている場合、イーサネット 1 にのみ有効化します。

開始 IP アドレス、終了 IP アドレス、リース時間： NAS により、DHCP クライアントに割り当てる IP アドレスの範囲およびリース時間を設定します。リース時間とは、クライアントに IP アドレスをリースする期間を表します。その間、IP アドレスは割り当てられたクライアントに予約されます。リース期間が経過すると、IP アドレスは別なクライアントに割り当てられます。

WINS サーバー（オプション）： WINS（Windows Internet Naming Service ： Windows インターネットネーミングサービス）は、Windows ネットワークコンピュータ名（NetBIOS 名）を IP アドレスに解決し、ネットワーク上の Windows コンピュータが相互に検索/通信をしやすくします。利用可能な場合、ネットワーク上の WINS サーバーの IP アドレスを入力します。

DNS サフィックス（オプション）： DNS サフィックスは、無資格または不完全なホスト名を解決するために使用されます。

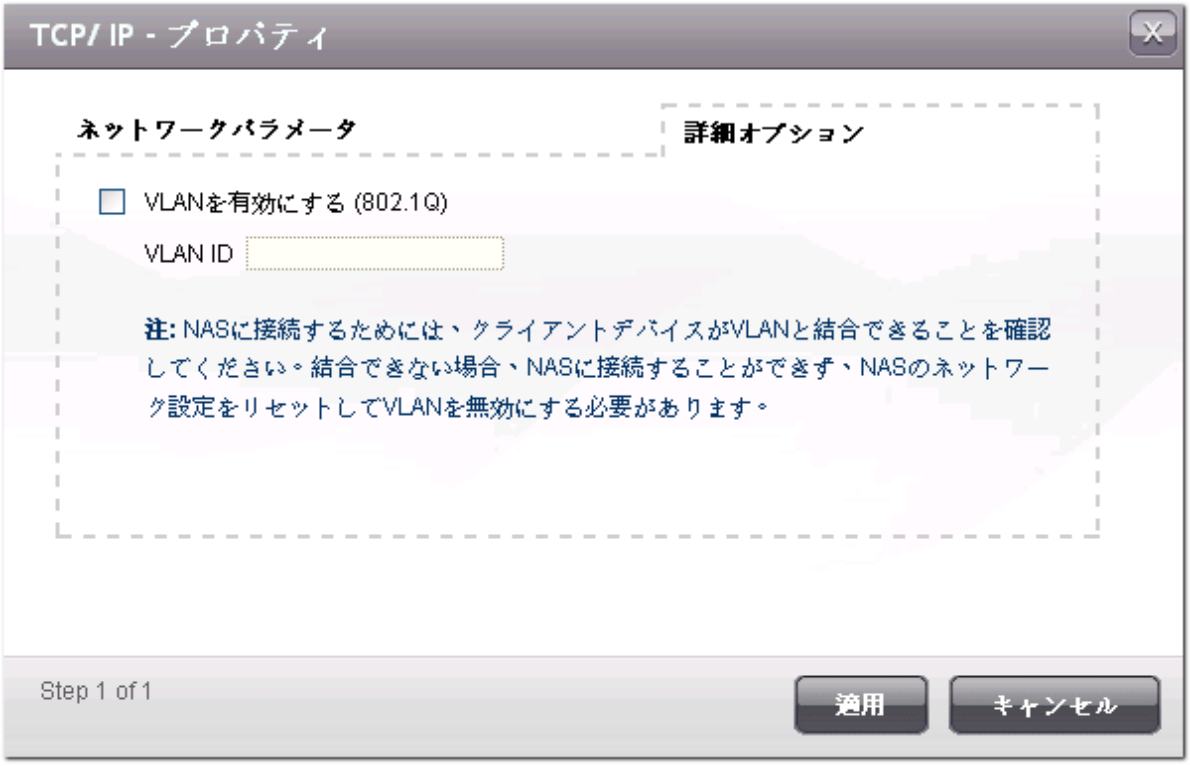
TFTP サーバー（オプション）： NAS は、ネットワークデバイスの PXE ブートをサポートします。TFTP サーバーの IP アドレスおよびブートファイル（TFTP サーバー上のディレクトリおよびファイル名を含む）を入力します。デバイスをリモートブートするには、TFTP サーバーの公開 IP アドレスを入力します。

詳細オプション

VLAN（バーチャルLAN）は異なる物理的場所に置かれていた場合でも、同じブロードキャストドメインに接続されているかのように通信する、ホストのグループです。 NASをVLANに結合し、同じVLAN上の他のデバイスのバックアップストレージとしてNASを設定できます。

NASをVLANに結合するには、「Enable VLAN（VLANを有効にする）」を選択しVLAN ID（0と4094巻の値）を選択します。 VLAN IDを安全な場所に保管し、クライアントデバイスがVLANと結合できることを確認してください。 VLAN IDを忘れNASに接続できなかった場合、NASのリセットボタンを押してネットワーク設定をリセットする必要があります。 NASがリセットされると、VLAN機能は無効になります。 NASが2つのギガビットLANポートをサポートするが、VLANを有効にするために1つのネットワークインターフェースしか設定されない場合、他のネットワークインターフェース経由でNASに接続する必要もあります。

注: VLAN機能はIntelベースのNASモデルでのみサポートされます。詳細はhttp://www.qnap.com にアクセスしてください。



(ii) デフォルトのゲートウェイ

両方のLANポートをネットワークに接続する場合、使用するゲートウェイの設定を選択します(デュアルLAN NASモデルのみ)。

(iii) ポートトランキング (Port Trunking)

ＬＡＮポート2機搭モデルのみ適用。この機能は、TS-110、TS-119、TS-210、TS-219、およびTS-219Pではサポートされません。

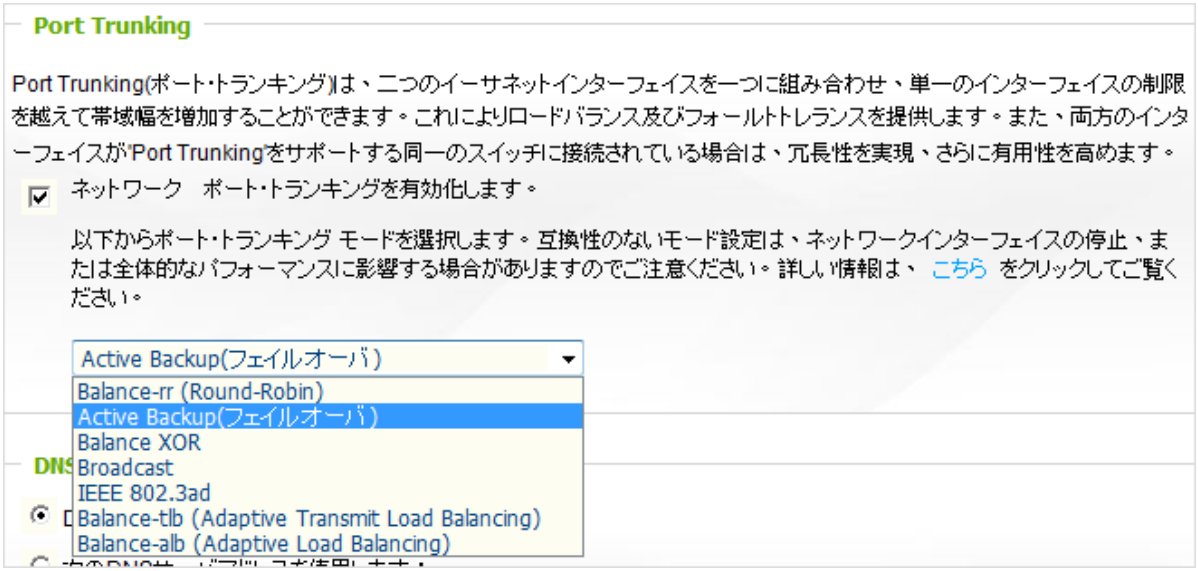
NASは、2つのイーサネットインターフェースを1つに結合し、大域幅を増加し、ロードバランシングと耐障害性(フェイルオーバーとしても知られます)を提供するポートのトランキングをサポートします。ロードバランシングは、2つのイーサネットインターフェースに均一に負荷分散し、冗長性を高める機能です。フェイルオーバーは、プライマリネットワークインターフェース(マスターインターフェースとしても知られます)がハイアベイラビリティを維持するために正しく反応しないときスタンバイネットワークインターフェース(スレーブインターフェースとしても知られます)にスイッチオーバーする機能です。

NASでポートトランキングを使用するには、NASの両方のLANポートを同じスイッチに接続し、セクション(i)と(ii)の説明通りに設定されていることを確認する必要があります。

下の手順に従ってNASのポートトランキングを構成します。

1. "Enable Network Port Trunking" (ネットワーク　ポート・トランキングを有効化します)のオプションを選択します。

2. ドロップダウンメニューからポートトランキングモードを選択します。デフォルトのオプションは、アクティブバックアップ(Failover)です。



3. "Apply" (適用)をクリックします。

4. イーサネットインターフェースはEthernet 1+2として結合されます。"Edit" (編集) ボタン( )をクリックして、ネットワーク設定を編集します。

5. 設定を適用した後、2つのイーサネットインターフェースのネットワークケーブルが正しいスイッチに接続され、スイッチがNASで選択したポートトランキングモードをサポートするように構成されていることを確認します。

NASで使用可能なポートトランキングのオプションについては下の表を参照してください。

項目	解説	必要なスイッチ
バランス-rr (ラウンドロビン)	ラウンドロビンモードは、通常目的における2つのイーサネットインターフェース間のロードバランシングに適しています。このモードは始めから最後までの稼動しているスレーブが順番にパケットを送信します。このモードはロードバランスとフォールトトレランスを提供しま。	静的トランキングをサポートします。スイッチに静的トランキングが効化されていることを確認してください。
アクティブバックアップ	アクティブバックアップは、単一のイーサネットインターフェースのみを使用します。最初のイーサネットインターフェースが適切に機能しない場合、2番目のイーサネットインターフェースに切り換えます。ボンドのインターフェースは1つだけが効になります。ボンドのMACアドレスは1ポート(ネットワークアダプタ)でのみ外部から見ることが可能なため、スイッチの混乱を防ぐことができます。アクティブバックアップモードはフォールトトレランス (耐障害性を提供します。	一般スイッチ
バランスXOR	バランスXORは、指定した各送信先にイーサネットインターフェース間の発信パケットを分割することによってトラフィックのバランス配分を行います。選択した伝送ハッシュポリシーに従って送信します。デフォルトのポリシーは、送信元MACアドレスが送信先MACアドレスと連結したレイヤ2で動作するシンプルスレーブカウントです。オプションによりxmitハッシュポリシーを使用して異なる伝送ポリシーを選択することができます。バランスXORモードはロードバランシングとフォールトトレランスを提供します。	静的トランキングをサポートします。スイッチに静的トランキングが効化されていることを確認してください。
ブロードキャスト	ブロードキャストは両方のネットワークインターフェースにトラフィックを送信します。ブロードキャストモードはフォールトトレランスを提供します。	静的トランキングをサポートします。スイッチに静的トランキングが効化されていることを確認してください。
IEEE 802.3ad (ダイナミックリンクアグリゲーション)	ダイナミックリンクアグリゲーションは複雑なアルゴリズムを使用して速度およびデュプレックス設定によりアダプタを集約させます。802.3ad仕様に従いアクティブアグリゲータ内の全てのスレーブを利用します。ダイナミックリンクアグリゲーションモードはロードバランスおよびフォールトトレランスを提供しますが、IEEE 802.3adをサポートした、LACPモードが適切に構成されているスイッチが必要となります。	802.3ad LACPをサポートします。

バランス-tlb （アダプティブトランスミットロードバランシング	バランス-tlbは、特定のスイッチを必要としないチャンネルボンディングを使用します。各イーサネットインターフェースの現在のロード（速度に対して算出)に基づいて発信トラフィックが配分されます。着信トラフィックは現在のスレーブにより受信されます。受信トラフィックは、現在のイーサネットインターフェースによって受信されます。受信イーサネットインターフェースが故障した場合は、、故障した受信スレーブのMACアドレスを他のスレーブが引き継ぎます。バランス-tlbモードはロードバランシングとフォールトトレランスを提供します。	一般スイッチ
バランス-alb （アダプティブロードバランシング	バランス-albはバランス-tlbと似ていますが、さらにIPV4トラフィックに対し受信を再配分します（受信ロードバランス。セットアップには、特別なスイッチへの対応や構成を必要としません。受信ロードバランシングはローカルシステムによりARPの応答が送信される際に実現され、異なるピアがそれぞれ異なるハードウェアアドレスをサーバ用に使用できるように送信元のハードウェアアドレスをボンド内のイーサネットハードウェアのうちの一つの固有ハードウェアアドレスとして上書きするARPネゴシエーションにより実現されます。バランス-albモードはロードバランシングとフォールトトレランスを提供します。	一般スイッチ

(iv) DNSサーバ

1次DNSサーバ:外部ネットワークでNASに対してDNSサービスを提供する、プライマリDNSサーバのIPアドレスを入力します。

2次DNSサーバ:外部ネットワークでNASに対してDNSサービスを提供する、セカンダリDNSサーバのIPアドレスを入力します。

注:

- プライマリおよびセカンダリDNSサーバのIPアドレスはISPまたはネットワーク管理者にお問い合わせください。NASを端末として使用して、BTのダウンロードなどのように独立した接続を確立する必要がある場合は、正しいURL接続のために少なくとも1つのDNSサーバIPを入力してください。入力しない場合、正しく機能しないことがあります。
- DHCPからIPアドレスを取得するよう選択してある場合、プライマリおよびセカンダリDNSサーバの設定は必要ありません。設定には「0.0.0.0」を入力できます。

(v) ジャンボフレーム設定 (MTU)

この機能はTS-509 Pro、TS-809 Pro、およびTS-809U-RPではサポートされません。

「ジャンボフレーム」は1500バイトを超えるイーサネットフレームのことで、パケットごとにもっと効率的で大量のペイロードを使用することにより、イーサネットネットワークのスループットを向上させ、大容量ファイル転送のためのCPU使用率を低減させるようデザインされています。

最大転送単位 (MTU) とは、通信プロトコルの任意のレイヤーが転送できるパケットの最大サイズ (バイト単位) のことです。

NASはデフォルトで1500バイトの標準的イーサネットフレームを使用します。お使いのネットワーク機器がジャンボフレーム設定に対応している場合は、ネットワーク環境に最適なMTU値を選択してください。NASは4074、7418バイトと 9000バイトのMTUに対応しています。

注: ジャンボフレーム設定はギガビットネットワーク環境でのみ効です。また、接続されているすべてのネットワーク機器はジャンボフレームを効にしており、同一のMTU値を使用していなければなりません。

ワイヤレス

NASをワイヤレスネットワークに接続するには、ワイヤレスドングルをNASのUSBポートに差し込みます。 ワイヤレスアクセスポイントのリストが検出されます。 NASを2つの方法でワイヤレスに接続できます。

注:

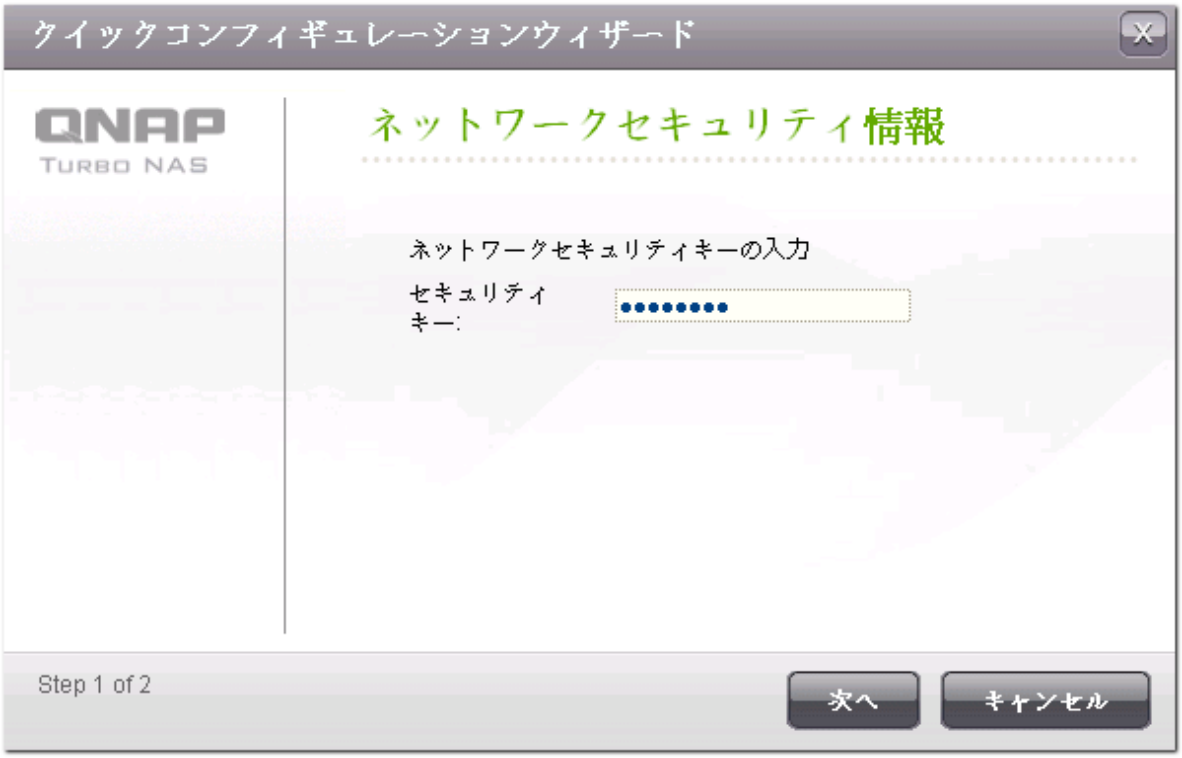
- ワイヤレス接続パフォーマンスは、アダプタモデル、USBアダプタのパフォーマンス、ネットワーク環境などの多くの要因によって異なります。 接続パフォーマンスを高くするには、優先接続を使用することをお勧めします。
- 1つのシステムで同時にご使用頂けるUSB Wi-Fiドングルは、 1 つだけです。

1. 既存のワイヤレスネットワークへの接続：

信号強度のあるワイヤレスアクセスポイントのリストは、「ワイヤレスネットわーっく接続」パネルに表示されます。

アイコンとオプション	説明
再スキャン	範囲内のワイヤレスネットワークを検索します。
(安全なネットワーク)	このアイコンは、ワイヤレスネットワークにネットワークキーが必要なことを示しています。ネットワークに接続するには、キーを入力する必要があります。
(接続)	ワイヤレスネットワークに接続します。 セキュリティキーが要求された場合、キーを入力するように求めるプロンプトが表示されます。
(編集)	接続情報を編集します。 範囲内にあるとき、ワイヤレスネットワークに自動的に接続するように選択できます。
(切断)	ワイヤレスネットワークから切断します。
(削除)	パネルからワイヤレスネットワークプロファイルを削除します。
すべて表示	使用可能なワイヤレスネットワークをすべて表示するには、このオプションを選択します。 構成されたネットワークプロファイルのみを表示するには、このオプションをオフにします。

範囲内の使用可能なワイヤレスネットワークを検索するには、「再スキャン」をクリックします。 接続するワイヤレスネットワークを選択し、Connect（接続）ボタン( )をクリックします セキュリティキー対応ネットワークの場合、セキュリティキーを入力します。「NEXT（次へ）」をクリックすると、NASはワイヤレスネットワークへの接続を試みます。



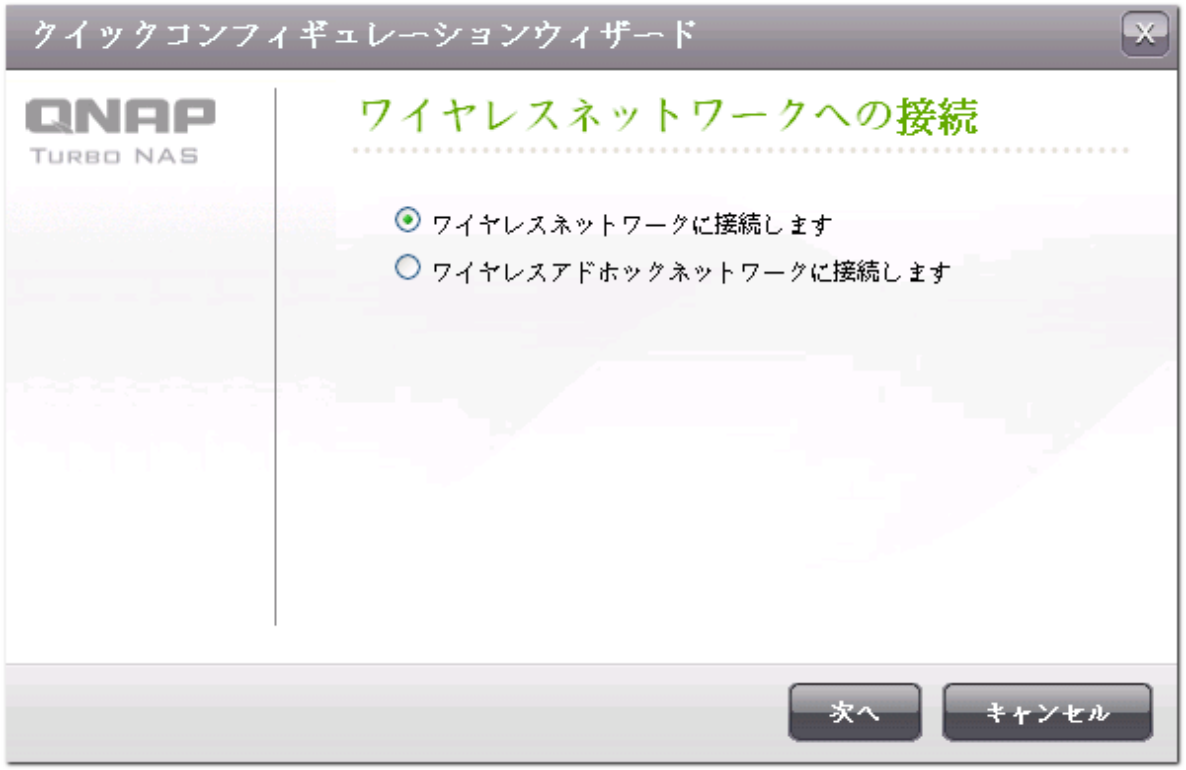
設定されたネットワークプロファイルのステータスを表示できます。

メッセージ	説明
接続済み	NASは現在、ワイヤレスネットワークに接続されています。
接続しています	NASはワイヤレスネットワークに接続を試みています。
範囲外、またはSSIDがステルスモードです。	無線信号が利用不可、またはSSIDが通知されていません。
IPを取得できませんでした	NASはワイヤレスネットワークに接続されていますが、DHCPサーバーからIPアドレスを取得できません。 ルータ設定をチェックしてください。
関連付けに失敗しました	NASは、ワイヤレスネットワークに接続できません。 ルータ設定をチェックしてください。
間違ったキー	入力したセキュリティキーが間違っています。
自動接続	範囲内にある場合、ワイヤレスネットワークに自動的に接続されます。 Wi-FiネットワークのSSIDがブロードキャストでない場合、自動接続機能はサポートされません。

2. ワイヤレスネットワークへ手動で接続：

そのSSID（ネットワーク名）を送信しないワイヤレスネットワークに手動で接続するには、「CONNECT TO A WIRELESS NETWORK（ワイヤレスネットワークに接続する）」をクリックします。

アクセスポイントを必要とせずに、任意のワイヤレスデバイスに接続できるアドホックネットワークへの接続を選択できます。

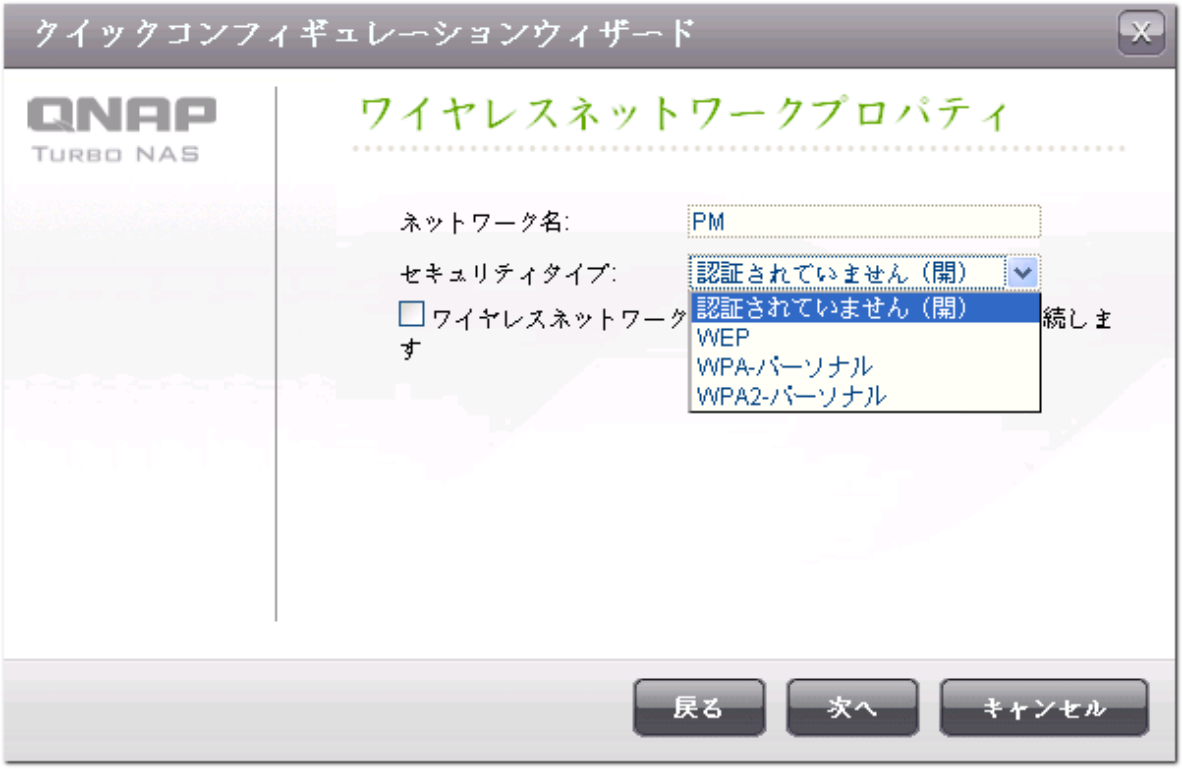


ワイヤレスネットワークのネットワーク名(SSID)を入力し、セキュリティタイプを選択します。

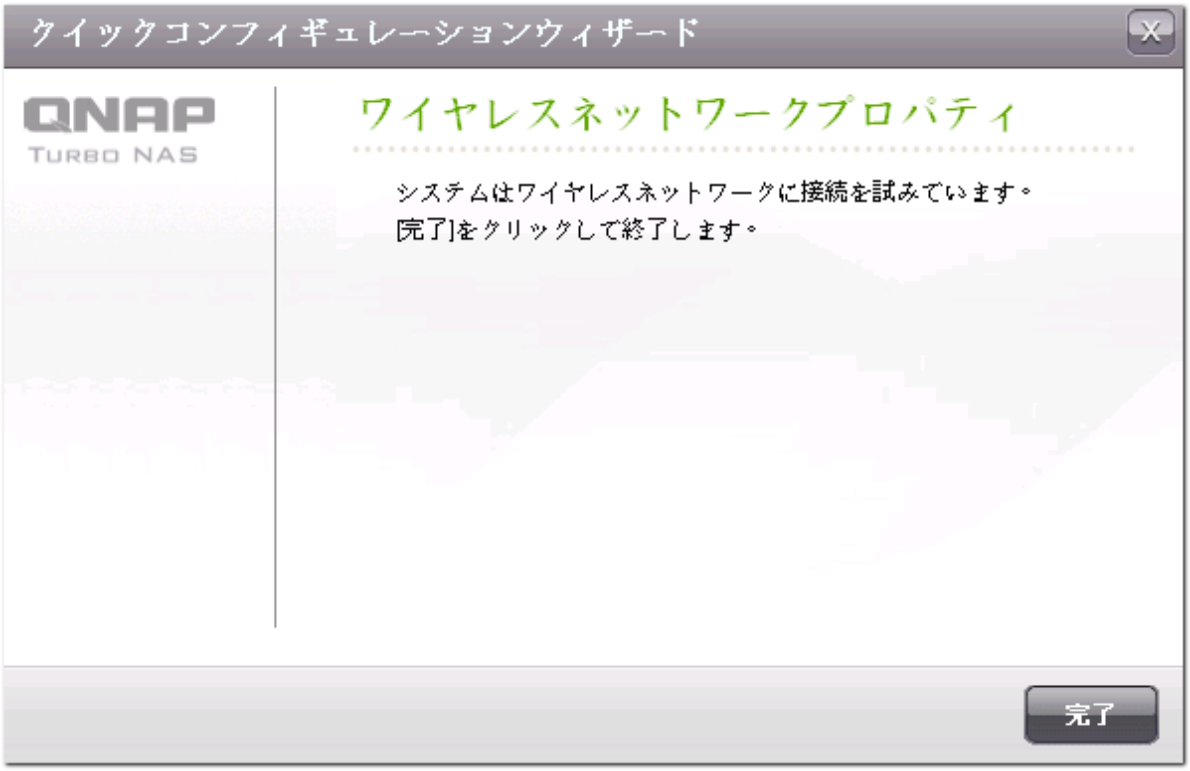
- 認証されていません（開）： セキュリティキーは必要ありません。
- WEP: 最大4つのWEPキーを入力し、認証に使用するキーを1つ選択します。
- WPA-パーソナル： AESまたはTKIP暗号化タイプを選択し、暗号化キーを入力します。
- WPA2-パーソナル： セキュリティキーを入力します。

注:

- WEPキーは5文字か13文字のASCIIキャラクターまたは10文字か26文字の16進数（0-9 / A-F)で記入してください。
- 暗号化されたワイヤレスネットワークへの接続が難しい場合、ワイヤレスルータ/AP設定をチェックし、「Nのみ」モードから「B/G/N混合」または類似設定に転送速度を変更します。
- WPA2で暗号化したWindows 7のユーザーの場合、NASでアドホック接続を確立することはできません。Windows 7でWEP暗号化を使用するように、変更してください。
- アドホック接続を確立するには、ワイヤレスインターフェースに対して固定IPアドレスを使用する必要があります。

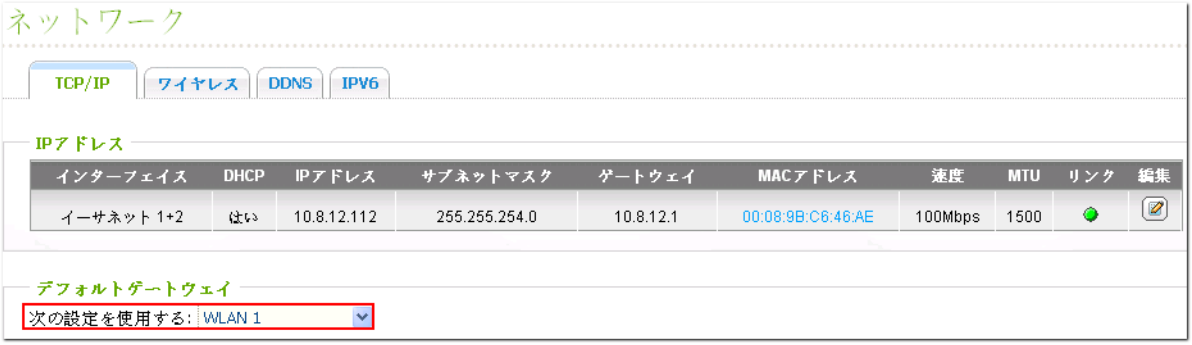


NASがワイヤレスネットワークを追加した後、「FINISH（終了）」をクリックします。



IPアドレス設定を編集するには、Edit（編集）ボタン をクリックします。DHCPでIPアドレスを自動的に取得したり、固定IPアドレスを設定したりできます。

ワイヤレス接続がNASとルータ/AP間の唯一の接続の場合、「Network（ネットワーク）」>「TCP/IP」ページでデフォルトゲートウェイとして「WLAN1」を選択する必要があります。そうしなければ、NASはインターネットに接続したり、別のネットワークと通信したりすることができません。



DDNS

インターネット上にサーバを設定して、同サーバへの容易なアクセスを可能にするには、通常、覚えやすい固のホスト名が必要です。ただし、ISPから提供されているのがダイナミックなIPアドレスだけの場合、サーバのIPアドレスは更されるので、呼び出すのは簡単ではありません。DDNSサービスを使えば、この問題を解決できます。

NASのDDNSサービスを効にした後、NASを再起動するか、IPアドレスを更すると、NASはDDNSプロバイダに直ちに通知して、新しいIPアドレスを記録します。ホスト名を使ってNASに接続しようとすると、DDNSは記録されたIPアドレスをユーザーに送信します。

DDNSサービスを使用する前に、DDNSプロバイダから入手したホスト名を登録してください。NASは以下のDDNSプロバイダに対応しています: DDNS providers: http://www.dyndns.com ，http://update.ods.org ，http://www.dhs.org ，http://www.dyns.cx ，http://www.3322.org ，http://www.no-ip.com ．DDNSサービスの登録方法に関しては、DDNSプロバイダのウェブサイトを参照してください。

NASにおけるDDNSセットアップおよびポート転送の詳細はこちら 64をご覧ください。

IPv6

NASは「ステートレス」アドレス構成を備えたIPv6接続、またIPv6とRFC2461用のRADVD（ルータ通知デーモン、Router Advertisement Daemon）をサポート。これにより、同一のサブネット上のホストはNASからIPv6アドレスを自動的に取得できます。NAS上のIPv6対応サービスは以下を含みます:

- リモートレプリケーション
- ウェブサーバ
- FTP
- iSCSI (仮想ディスクドライブ)
- SSH (putty)

この機能を使用するには、"Enable IPv6" (IPv6を効化) のボックスにチェックをいれ、"Apply" (適用) をクリックします。NASが再起動します。システムが再起動した後、IPv6ページに再度ログインします。IPv6インターフェイスの設定が表示されます。 をクリックして設定を編集します。

IPv6 自動構成

ネットワーク上にIPv6 対応ルータがある場合、このオプションを選択して、NASが自動的にIPv6アドレスを取得し構成するようにします。

静的IPアドレスを使用する

静的IPアドレスを使用するには、IPアドレス(例:2001:bc95:1234:5678)、プレフィックス長(例:64)、およびNASのゲートウェイアドレスを入力してください。プレフィックス及びプレフィックス長の情報をISPに問い合わせる必要があります。

- ルータ通知デーモン (radvd) を効化する

  NASをIPv6ホストとして構成しIPv6アドレスをIPv6対応のローカルクライアントに分配するには、このオプションを効化し、プレフィックス及びプレフィックス長を入力します。

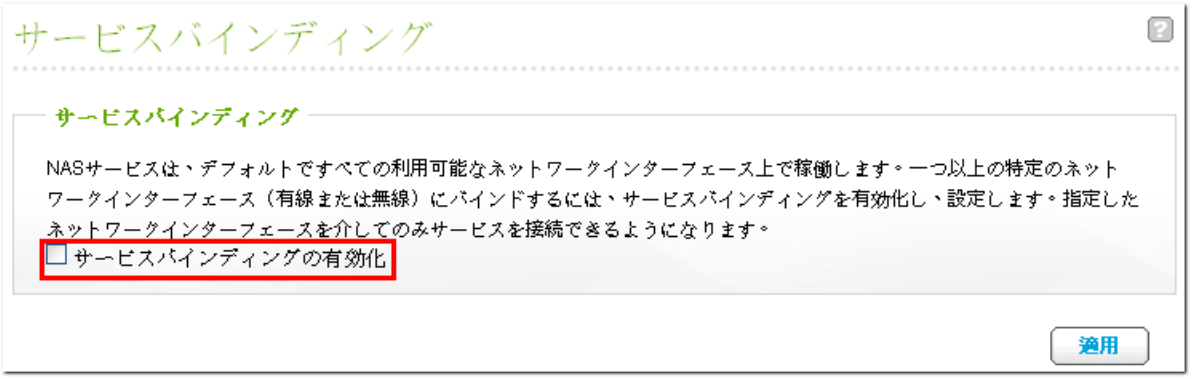
IPv6 DNSサーバ

ご希望のDNSサーバを上の欄に入力し、代替DNSサーバを下の欄に入力します。情報についてはISPあるいはネットワーク管理者にお問い合わせください。IPv6自動構成を選択した場合は、欄は「::」のままにしておいてください。

3.3 サービスバインディング

注：サービスバインディング機能は、2 つ以上のネットワークインターフェース（有線および無線）をもつ NAS でのみ利用可能です。

NAS サービスは、初期設定では、すべての利用可能なネットワークインターフェース上で稼働します。サービスを 1 つ以上のネットワークインターフェース（有線または無線）にバインドするには、サービスバインディングを有効にします。



NAS 上の利用可能なネットワークインターフェースが表示されます。すべての NAS サービスは、初期設定では、すべてのネットワークインターフェース上で稼働します。各サービスにバインドするネットワークインターフェースを少なくとも 1 つ選択します。それから、「Apply（適用）」をクリックします。ユーザーが、指定したネットワークインターフェースを経由して、サービスに接続できるようになります。

設定が適用できない場合は、「Refresh（更新）」をクリックして、サーバー上の現在のネットワークインターフェースを表示して、サービスバインディングを再度設定します。

注：サービスバインディング設定を適用後も、指定したネットワークインターフェースを経由せずに接続しているユーザーの接続は保持されます。指定したネットワークインターフェースは、次回の接続セッションから使用されます。

3.4 ハードウェア

本製品のハードウェア機能を、効あるいは無効に設定できます。

構成リセットスイッチを効にする
このボタンを効にすることにより、リセットボタンを3秒間押して管理者パスワードとシステム設定をリセットしてデフォルトに戻すことができます。ディスクのデータは維持されます。

システム	ベーシックシステムリセット (ビープ音1回)	アドバンスドシステムリセット (ビープ音2回)
すべてのNASモデル	リセットボタンを3秒間押します。	リセットボタンを10秒間押します。

ベーシックシステムリセット(3秒)

リセットボタンを3秒間押すと、ビープ音が発生します。以下の設定はデフォルト値にリセットされます:

- システム管理者のパスワード:admin
- TCP/IP設定: DHCPを通してIPアドレス設定を自動的に取得する
- TCP/IP設定:ジャンボフレームを無効にする
- TCP/ IP 構成:ポートトランキングが効な場合 (デュアルLANモードのみ)、ポートトランキングモードは "Active Backup (Failover)" (アクティブバックアップ(フェールオーバー) にリセットされます。
- システムポート: 8080 (システムサービスポート)
- セキュリティレベル:すべての接続を許可する
- LCDパネルパスワード: (空欄)*
- VLANが無効になります
- サービスバインディング:すべてのNASサービスは、すべての利用可能なネットワークインターフェース上で稼働します。

*この機能はLCDパネルの付いたNASモデルにのみ付属しています。詳細については、http://www.qnap.com にアクセスしてください。

アドバンスドシステムリセット(10秒)

リセットボタンを10秒間押し続けると、3秒後と10秒後の2回発信音が聞こえます。NASは「Administration(管理)」>「Restore to Factory Default(工場出荷時のデフォルト状態に復元)」でネットワークを利用したシステムリセットとして、システム設定内容のすべてを予約済みのデータを除いてデフォルト状態にリセットします。ユーザー、ユーザーグループ、ネットワーク共有フォルダなど、以前作成した設定内容は消去されます。アドバンスシステムのリセット後に古いデータを復元するには、NAS上に同じネットワーク共有フォルダを作成すればデータに再度アクセスできるようになります。

ディスクスタンバイモードを効にする
この機能が効になっているとき、指定した時間アクセスがないとハードディスクはスタンバイモードに入ります。

SATAディスクの空き容量が値より少なくなると、光の信号警報が効になります。
この機能が効になっているときSATAディスクの空き容量が値より少なくなると、ステータスLEDインジケータが赤と緑で点滅します。値の範囲は1-51200 MBです。

ライトキャッシュの効化(EXT4)
NASのディスクボリュームがEXT4形式でフォーマットされている場合、このオプションを選択すると書き込みに高いパフォーマンスが得られます。データの書き込み中に予期しないシステムのシャットダウンが起こると、データ転送が未完了になってしまします。以下のサービスのいずれかが効の場合、このオプションはオフになります。ダウンロードステーション*、MySQLサービス、ユーザークォータ、監視ステーション NASを仮想環境またはクラスター環境での共ストレージとして設定した場合、このオプションをオフにすることをお勧めします。

*この機能は、TS-879 Pro、TS-1079 Pro、TS-879U-RP、TS-EC879U-RP、TS-1279U-RP、TS-EC1279U-RPではサポートされません。

アラームブザーの効化
システム操作(スタートアップおよびファームウェアアップグレード)およびシステムイベント(エラーおよび警告)が起きた際にアラームブザーをオンにするよう選択することができます。

スマートファンコンフィギュレーション

i. スマートファンを効化(推奨)
   デフォルトのスマートファン設定を使用するか、あるいは設定を手動で定義するかを選択します。システムデフォルト設定が選択された場合、サーバ温度、CPU温度、ハードドライブ温度が条件を満たす際はファン回転速度は自動調節されます。このオプションを効化するよう推奨いたします。
ii. ファン回転速度を手動で設定
   ファンの速度を低速、中足、高速から設定します。

ウェブ ベースのインターフェイスで予備電源用の警告アラートを使用可能にする:

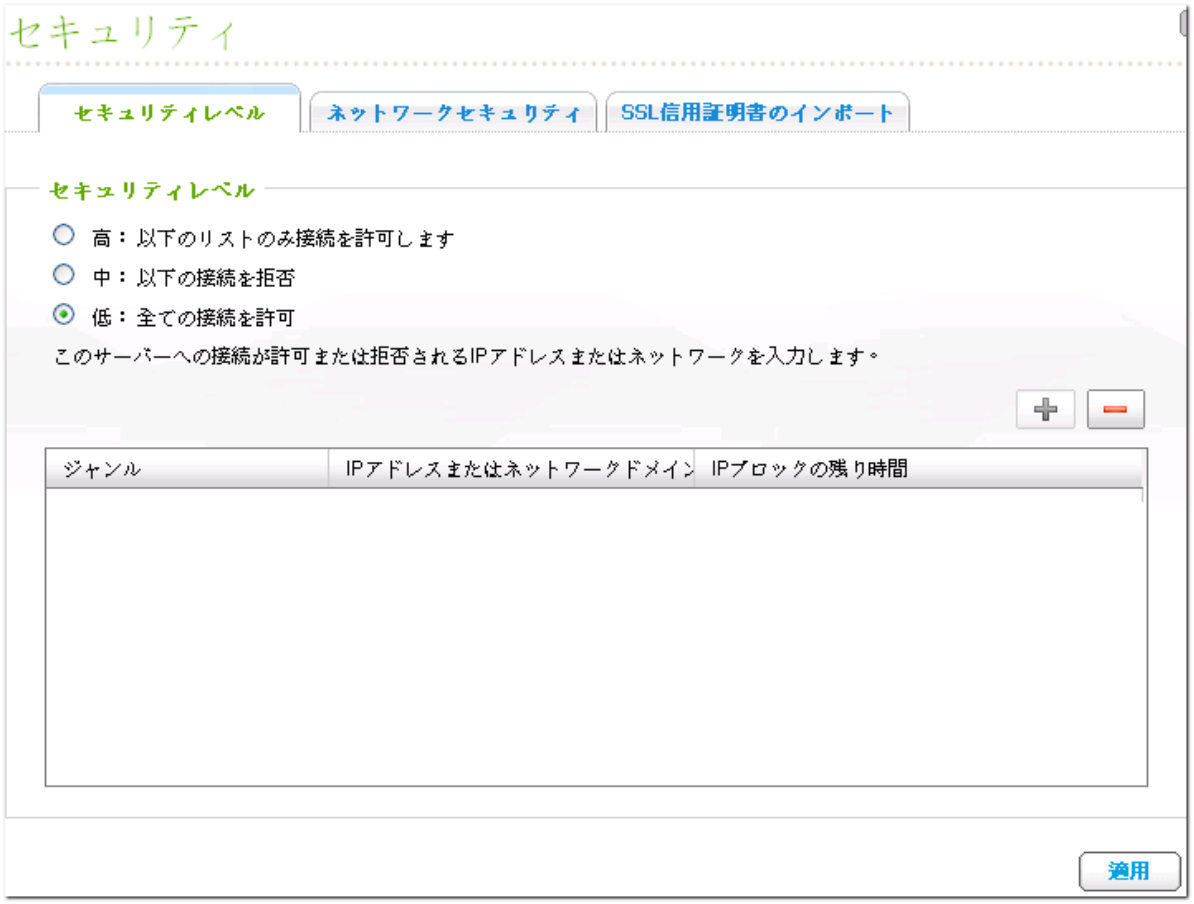
NAS に 2 個の電源ユニット(PSU)を設置して、それらを電源ソケットに接続すると、両方の PSU が NAS に電源を供給します(1U モデルと 2U モデルに適用されます)。"System Administration" (システム管理) > "Hardware" (ハードウェア)で予備電源モードを使用可能にし、予備電源用の警告アラートの受信を可能にすることができます。PSU のプラグが外れるか、故障すると、NAS はビープ音を出し、エラー メッセージを"System Logs" (システム ログ)に記録します。

NAS に電源ユニット(PSU)を 1 個のみ設置した場合には、このオプションを使用可能にしないことをお勧めします。

3.5 セキュリティ

セキュリティレベル

このサーバーへの接続が許可または拒否されるIPアドレスまたはネットワークを入力します。ホストサーバーの接続が拒否されると、そのサーバーのプロトコルはすべてローカルサーバーにアクセスすることができません。設定を更したら、[適用]をクリックして更を保存します。ネットワークサービスが再起動し、サーバへの現在の接続が切断されます。



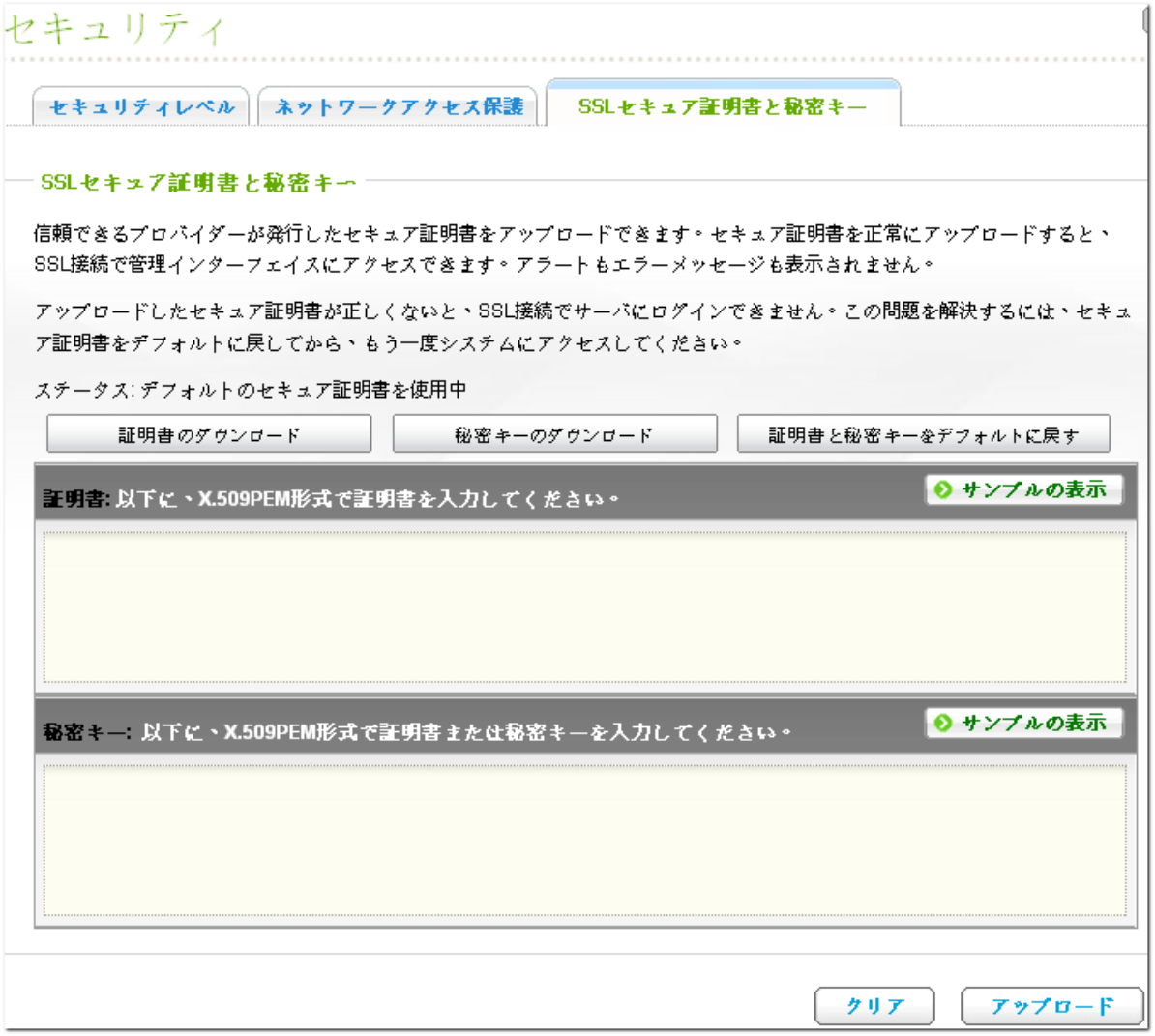
ネットワークアクセスの保護

ネットワークアクセス保護によりシステムのセキュリティが強化され、望ましくない侵入を防ぐことができます。IPが特定の接続方法でサーバにログインできない場合、一定期間または絶えずIPをブロックするようにすることができます。

SSL信用証明書のインポート

Secure Socket Layer（セキュアソケットレイヤー、SSL）はウェブサーバーとブラウザ間のデータ転送の安全確保を目的に開発されたプロトコルです。信用できるプロバイダによって発行された信用証明書をアップロードすることができます。信用証明書を正式にアップロードすると、SSL接続によって管理インターフェースに接続でき、アラートもエラーメッセージも発生しません。システムはX.509証明書とプライベートキーのみをサポートします。

- 証明書のダウンロード：現在使用中の安全な証明書をダウンロードします。
- プライベートキーのダウンロード：現在使用中のプライベートキーをダウンロードします。
- デフォルト証明書およびプライベートキーの復元：安全な証明書およびプライベートキーをシステム初期値に復元します。現在使用中の安全な証明書およびプライベートキーは上書きされます。



3.6 通知

SMTPサーバーの設定

NASは、電子メールアラートをサポート、ユーザーに対しシステムエラーあるいは警告を通知します。電子メールでアラーとを受信するには、SMTPサーバを構成します。

- SMTPサーバ: SMTPサーバ名(例:smtp.gmail.comなど) を入力します。
- ポート番号: SMTPサーバ用のポート番号を入力します。ポート番号の初期設定値は25です。
- 送信者:送信者情報を入力します。
- SMTP認証を効化: この機能を効化すると、システムはメッセージが送信される前にメールサーバの認証を求めます。
- ユーザー名およびパスワード: 電子メールアカウントのログイン情報を入力します。 (例:Gメールログイン名及びパスワードなど)
- SSL/TLSセキュリティ接続を使用: SMTPサーバがこの機能をサポートしている場合、効化することができます。

IM 設定

NAS は、インスタントメッセージ(IM)サービスをサポートし、複数の Windows ライブメッセンジャー連絡機能で、即時システムエラー/警告メッセージを受信し、または、Windows ライブメッセンジャー会話機能で、NAS からリアルタイムでシステム情報を問い合わせることを可能にします。

注:

- この機能を利用するには、NAS をインターネットに接続する必要があります。
- NAS は、Windows ライブメッセンジャー 2009 または、それ以降をサポートします。
- NAS 専用の Windows ライブメッセンジャーのアカウントを登録します。1 台の NAS では、1 つの Windows ライブメッセンジャーのアカウントのみが利用可能です。

これらの機能を実施するには、以下のステップで行います:

1. https://signup.live.com/から、NAS 用の Windows ライブメッセンジャー ID にサインアップします。
2. お使いの Windows オペレーティングシステム用の Windows ライブメッセンジャーをhttp://explore.live.com/からダウンロードします。NAS は、Windows ライブメッセンジャー 2009 または、それ以降をサポートします。
3. ステップ 1 で登録した Windows ライブメッセンジャーのアカウントでログインします。NAS との対話を許可する連絡先を最大 10 件追加します。これらの連絡先を NAS のメッセンジャーアカウントに追加していることを確認します。
4. 「Notification (通知)」>「Configure IM (IM設定)」へ進み、ステップ 1 で登録したログイン情報を入力します。「Apply (適用)」をクリックします。ログインステータスが、「On (オン)」と表示されます。

5. 「Notification（通知）」>「Alert Notification（アラート通知）」と進みます。インスタントメッセージによる警告通知を有効にして、「Instant Messaging Settings（インスタントメッセージの設定）」の下に最大 10 件の許可する連絡先を入力します。「Apply（適用）」をクリックします。

6. 許可された Windows ライブメッセンジャーアカウントでログインして、Windows ライブメッセンジャーを経由し、NAS を対話します。NAS は、イベント発生時に、即時エラー/警告メッセージを許可された連絡先に送信します（英語のみ）。

許可された Windows ライブメッセンジャーの連絡先を使用し、次のコマンドを入力して、NAS からリアルタイムでシステム情報を問い合わせることができます。情報は、英語でのみ利用可能です。

コマンド	説明
help	コマンドのオプション一覧が表示されます。
info-cpu	現在の CPU 温度を問い合わせます。
info-sys	現在のシステム温度および冷却ファンのスピードを問い合わせます。
info-model	NAS のモデル番号と問い合わせます。
info-hd	NAS 上のハードディスクの個数を問い合わせます。
info-hd-[hd#]	ハードディスクの現在の温度およびスマートステータス(自己監視および報告技術によるステータス)を問い合わせます。例、info-hd-1
info-vol	NAS 上のディスクボリュームの個数を問い合わせます。
info-vol-[vol#]	ディスクボリュームの情報を問い合わせます。例、info-vol-1

SMSCサーバーの構成

SMSサーバ設定を構成して、NASからSMSメッセージを送信することができます。デフォルトのSMSサービスプロバイダはClickatellです。ドロップダウンメニューで「SMSプロバイダの追加」を選択することで、専用のSMSサービスプロバイダを追加することもできます。

「SMSサービスプロバイダの追加」を選択するとき、SMSプロバイダの名前とURLテンプレートテキストをを入力する必要があります。

> 注:入力されたURLテンプレートテキストSMSサービスプロバイダの標準に従っていない場合、SMSを適切に受信することができません。

アラート通知

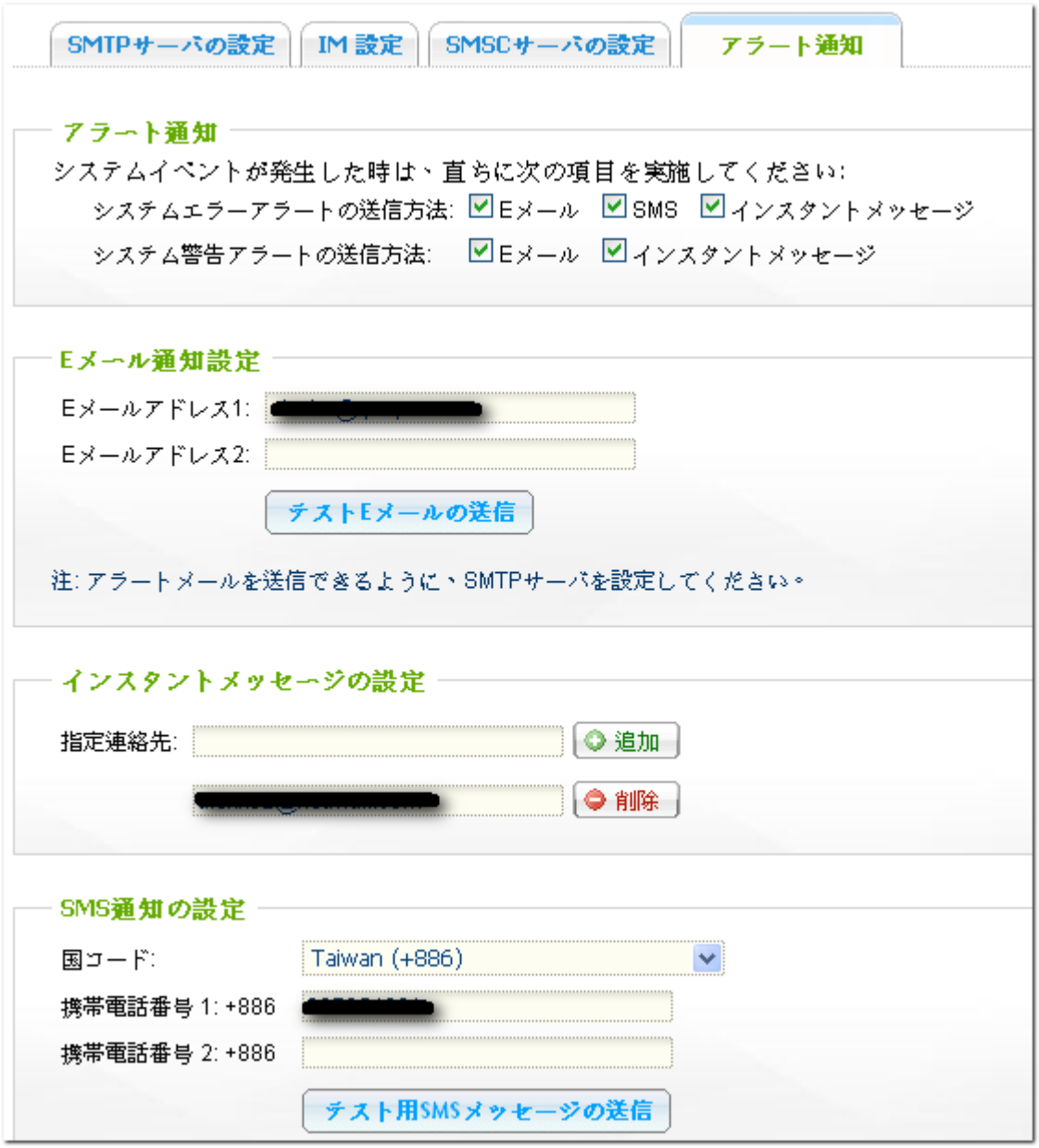
NAS がシステムイベント（警告/エラー）発生時に指定したユーザーに送信する即時警告の種類を選択します。

E メール通知の設定
NAS からの即時システム警告を受信する E メールアドレスを最大 2 件指定します。

インスタントメッセージ設定
NAS からの即時システム警告を受信し、Windows ライブメッセンジャーを経由して NAS からリアルタイムでの情報を問い合わせる Windows ライブメッセンジャーの連絡先を最大 10 件指定します。

Windows ライブメッセンジャーの連絡先は、最初に、「Notification（通知）」>「Configure IM（IM設定）」で、NAS の Windows ライブメッセンジャーアカウントに追加する必要があります。

SMS 通知設定
NAS からの即時システム警告を受信する携帯電話番号を最大 2 件指定します。


SMTPサーバの設定
IM 設定
SMSCサーバの設定
アラート通知
アラート通知
システムイベントが発生した時は、直ちに次の項目を実施してください:
システムエラーアラートの送信方法: Eメール SMS インスタントメッセージ
システム警告アラートの送信方法: Eメール インスタントメッセージ
Eメール通知設定
Eメールアドレス1:
Eメールアドレス2:
テストEメールの送信
注: アラートメールを送信できるように、SMTPサーバを設定してください。
インスタントメッセージの設定
指定連絡先:
追加
削除
SMS通知の設定
国コード:
Taiwan (+886)
携帯電話番号 1: +886
携帯電話番号 2: +886
テスト用SMSメッセージの送信

3.7 電源管理

このセクションによりサーバの即時再起動またはシャットダウンが可能です。また、停電後に電力が復旧した場合のサーバの動作を定義、さらに自動システム電源オン/オフ/再起動のスケジュールの設定をすることができます。

再起動/シャットダウン

システムの再起動/シャットダウンを直ちに実行する。
リモートレプリケーションジョブの進行中に、ウェブベースのインターフェイスまたはLCDパネルからNASを再起動あるいは電源オフにしようとした場合、システムは進行中のリモートレプリケーションジョブを無視するかどうか確認するメッセージが表示されます。

「レプリケーションジョブの実行中は、再起動/シャットダウンのスケジュールを延期する」のオプションを効化すると、進行中のレプリケーションジョブが完了した後に、スケジュール済みのシステム再起動あるいはシャットダウンが実行されます。そうでない場合、システムは進行中のレプリケーションジョブを無視し、スケジュール済みのシステム再起動/シャットダウンを実行します。

EuP の設定

EuP（または、エネルギー使用製品）とは、電気機器のエネルギー効率の向上、有害物質の使用の削減、製品リサイクルの容易さの向上、および製品の環境への優しさを改善するために設計された欧州連合（EU）の指令です。

EuP が有効になっている場合は、以下の設定は、サーバの電源が切れている場合、低消費電力（1W 未満）を維持するように影響を受けます。

- ウェイクオン LAN：無効になります。
- AC 電源再供給：電源が停電から復旧後も、サーバーはオフのままになります。
- スケージュル電源オン/オフ/再起動設定：無効になります。

EuP が無効になると、サーバーの電源がオフの場合の電源消費量は 1W より少し大きくなります。EuP は、初期設定では無効になっており、ウェイクオン LAN、AC 電源再供給、電源スケジュール設定機能を正しく利用できます。

この機能は、一部の NAS モデルでのみサポートされます。詳細は、http://www.qnap.com を参照してください。

Wake on LAN (ウェイクオンLAN)

このオプションを効にすると、Wake on LANにより遠隔操作でNASの電源を入れることが出来ます。NASがオフの間に電源接続が実際に引き抜かれた場合、Wake on LANは電源がその後再接続されたかどうかに関わらず、機能しません。

この機能は、TS-110、TS-119、TS-210、TS-219、TS-219P、TS-410、TS-419P、TS-410U、TS-419U、TS-112、TS-212、TS-412およびTS-412Uではサポートされません。詳細はhttp://www.qnap.com　にアクセスしてください。

電源回復設定

停電号にAC電源が回復した際、NASが以前のオンまたはオフ状態に戻る、または電源を入れる、あるいはオフのままにするよう構成します。

電源オン/オフ/再起動スケジュール

毎日、平日、週末、あるいは週のうちのいずれかの曜日を選んび、特定の時間に自動システム電源オン、オフ、あるいは再起動するよう設定することができます。平日とは月曜日から金曜日までのことです。週末とは、土曜日と日曜日のことです。最大15スケジュールまで設定することができます。

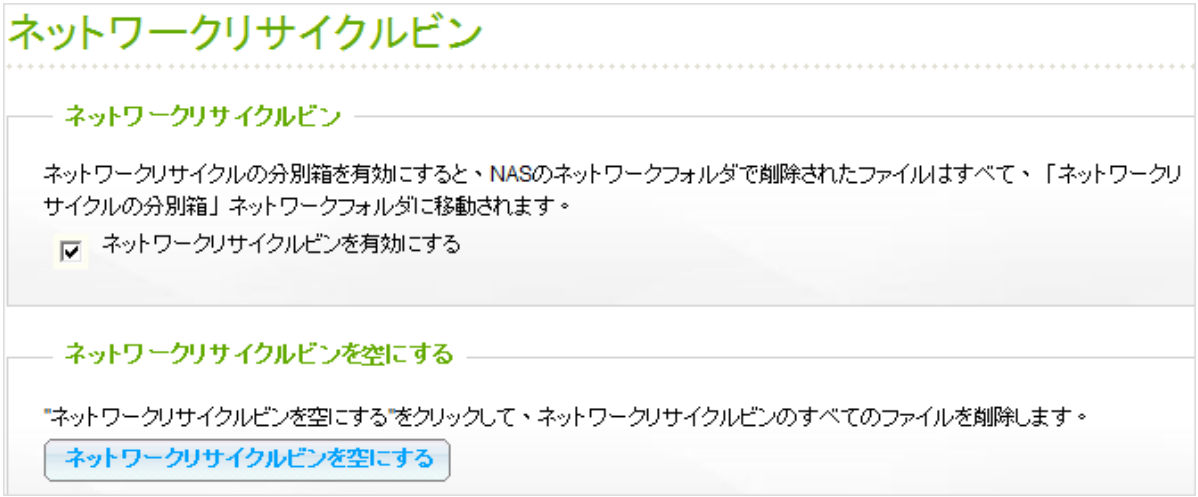
3.8 ネットワークごみ箱

ネットワークごみ箱を使用する

この機能を使用すると、NASの共部分で削除されたファイルはネットワークごみ箱に一時的に保存されます。この機能を効にするには、「ネットワークごみ箱を使用する」のボックスをチェックして、適用をクリックします。システムは「ネットワークごみ箱」というネットワークシェアを自動的に作成します。
ネットワークごみ箱はSAMBAおよびAFPを使用してのファイル削除のみサポートしていますのでご注意ください。

ネットワークごみ箱を空にする

ネットワークごみ箱内のすべてのファイルを削除するには、「ネットワークごみ箱を空にする」をクリックします



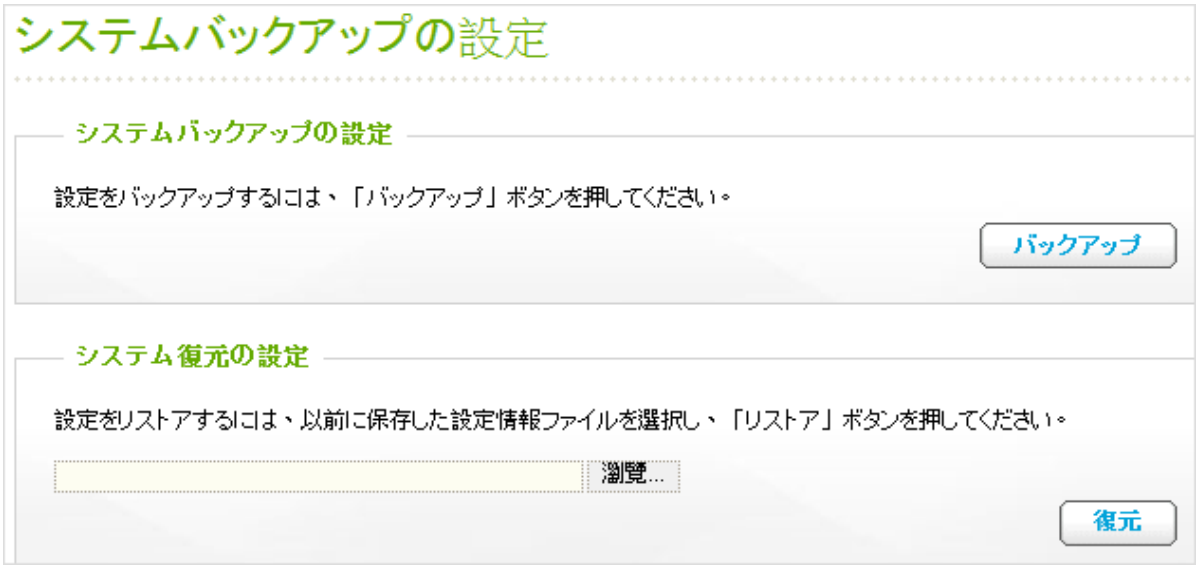
3.9 設定のバックアップ/復元

システムバックアップの設定

設定をバックアップするには、「バックアップ」ボタンを押してください。

システム復元の設定

設定をリストアするには、以前に保存した設定情報ファイルを選択し、「リストア」ボタンを押してください。



3.10 システムログ

システムイベントのログ

NASは警告、エラーおよび情報メッセージを含む最近10,000件のイベントログを保存できます。情報単なるメッセージです。通常は無視してください。警告この動作には、問題がある可能性があります。ネットワークやセキュリティの設定によっては、何らかの対処が必要でエラー何らかの対処が必要です。

ヒント：ログを右クリックして記録を削除することができます。すべてのログを消去するには、「Clear(クリア)」をクリックします。

システム接続のログ

システムはHTTP、FTP、Telnet、SSH、AFP、NFS、SAMBA、および iSCSIの接続のログをサポートします。「オプション」をクリックしてログする接続タイプを選択します。

ヒント：接続ログのリストのログを右クリックし選択して、レコードを削除するかIPを禁止するリストに追加し、IPの禁止期間を選択できます。すべてのログを消去するには、「Clear(クリア)」をクリックします。

アーカイブログ：このオプションは接続ログのアーカイブを効化します。システムは、csvファイルを自動的に生成し、ログ回数が上限に達するとファイルを指定のフォルダに保存します。

このページでファイルレベルのアクセスログを表示することもできます。「Options(オプション)」で指定した接続タイプ経由でファイルやフォルダにユーザーがアクセス、作成、削除、移動、または名前の変更を行うと、NASはログを記録します。この機能を無効にするには、「Stop logging(ロギングの停止)」をクリックします。

タイプ	日付	時刻	ユーザ	送信元IP	コンピュータ名	接続タイプ	アクセスしたリソース	アクション
	2011-01-24	10:18:54	guest	10.8.12.7	reinb	SAMBA	---	Login OK
	2011-01-24	10:18:54	admin	10.8.12.7	reinb	SAMBA	Public/temp/New Microsoft Office Access A	Write
	2011-01-24	10:18:45	admin	10.8.12.7	reinb	SAMBA	Public/temp/New Bitmap Image.bmp	Delete
	2011-01-24	10:18:40	admin	10.8.12.7	reinb	SAMBA	Public/New Bitmap Image.bmp -> Public/t	Move
	2011-01-24	10:18:28	admin	10.8.12.7	reinb	SAMBA	Public/New Text Document.txt	Delete
	2011-01-24	10:18:09	admin	10.8.12.7	reinb	SAMBA	Public/tem -> Public/temp	Rename
	2011-01-24	10:18:06	admin	10.8.12.7	reinb	SAMBA	Public/temp -> Public/tem	Rename
	2011-01-24	10:18:00	admin	10.8.12.7	reinb	SAMBA	---	Login OK
	2011-01-24	10:17:59	guest	10.8.12.7	reinb	SAMBA	---	Login OK
	2011-01-24	10:17:41	admin	10.8.12.7	reinb	SAMBA	---	Login OK

オンラインユーザー

ネットワーキングサービス経由でシステムにアクセスするオンラインユーザーの情報は、このページに表示されます。

ヒント：ログを右クリックしてIP接続の切断を選択し、IPをブロックリストに追加することができます。

Syslog

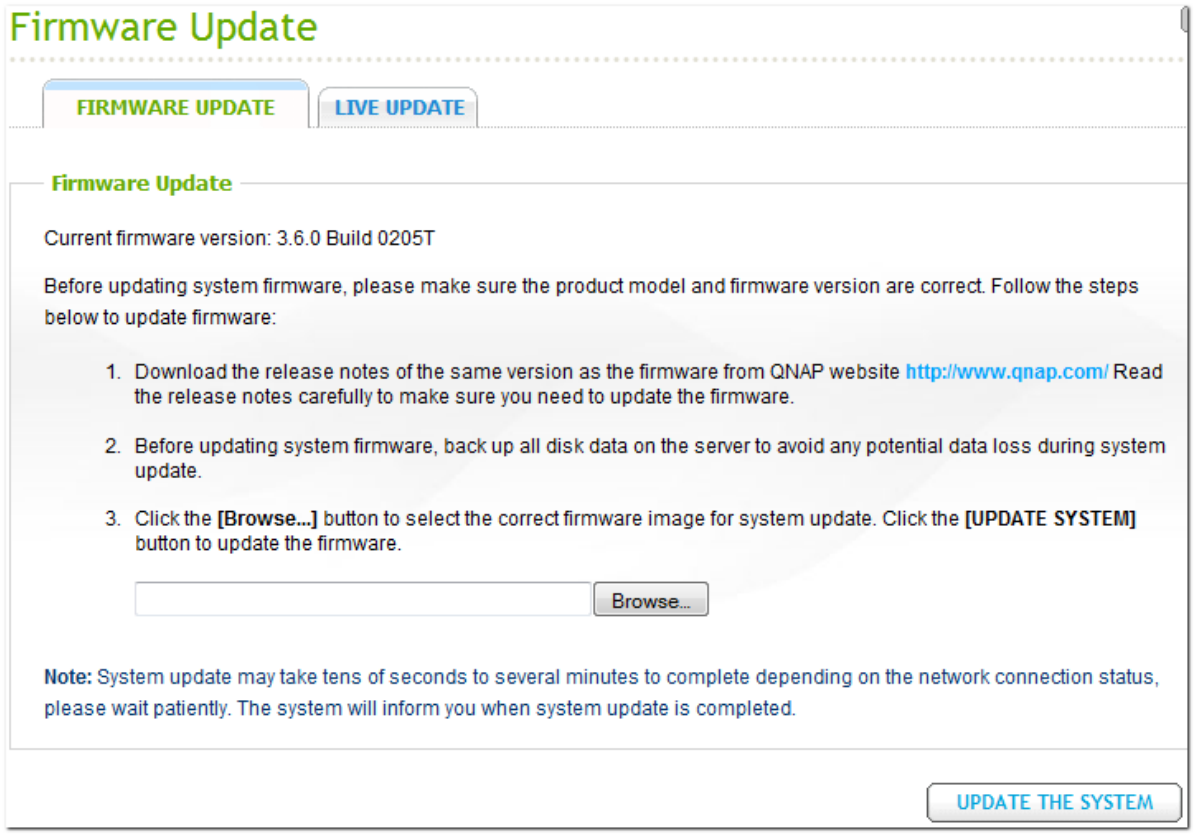
SyslogはIPネットワークでログメッセージを転送するための標準規格です。このオプションを使用可能にすることで、イベント・ログや接続ログをリモートのSyslogに保存することができます。

接続ログをCSVファイルに変換する場合、接続タイプとアクションはコード（番号）になります。コードの意味については、下の表を参照してください。

接続タイプコード	アクションコード
0 – UNKNOWN	0 – UNKNOWN
1 – SAMBA	1 – DEL
2 – FTP	2 – READ
3 – HTTP	3 – WRITE
4 – NFS	4 – OPEN
5 – AFP	5 – MKDIR
6 – TELNET	6 – NFSMOUNT_SUCC
7 – SSH	7 – NFSMOUNT_FAIL
8 – ISCSI	8 – RENAME
	9 – LOGIN_FAIL
	10 – LOGIN_SUCC
	11 – LOGOUT
	12 – NFSUMOUNT
	13 – COPY
	14 – MOVE
	15 – ADD

3.11 ファームウェア更新

ウェブ管理ページによるファームウェア更新



注:システムが正常に動作している場合にはファームウェアのアップデートは必要ありません。

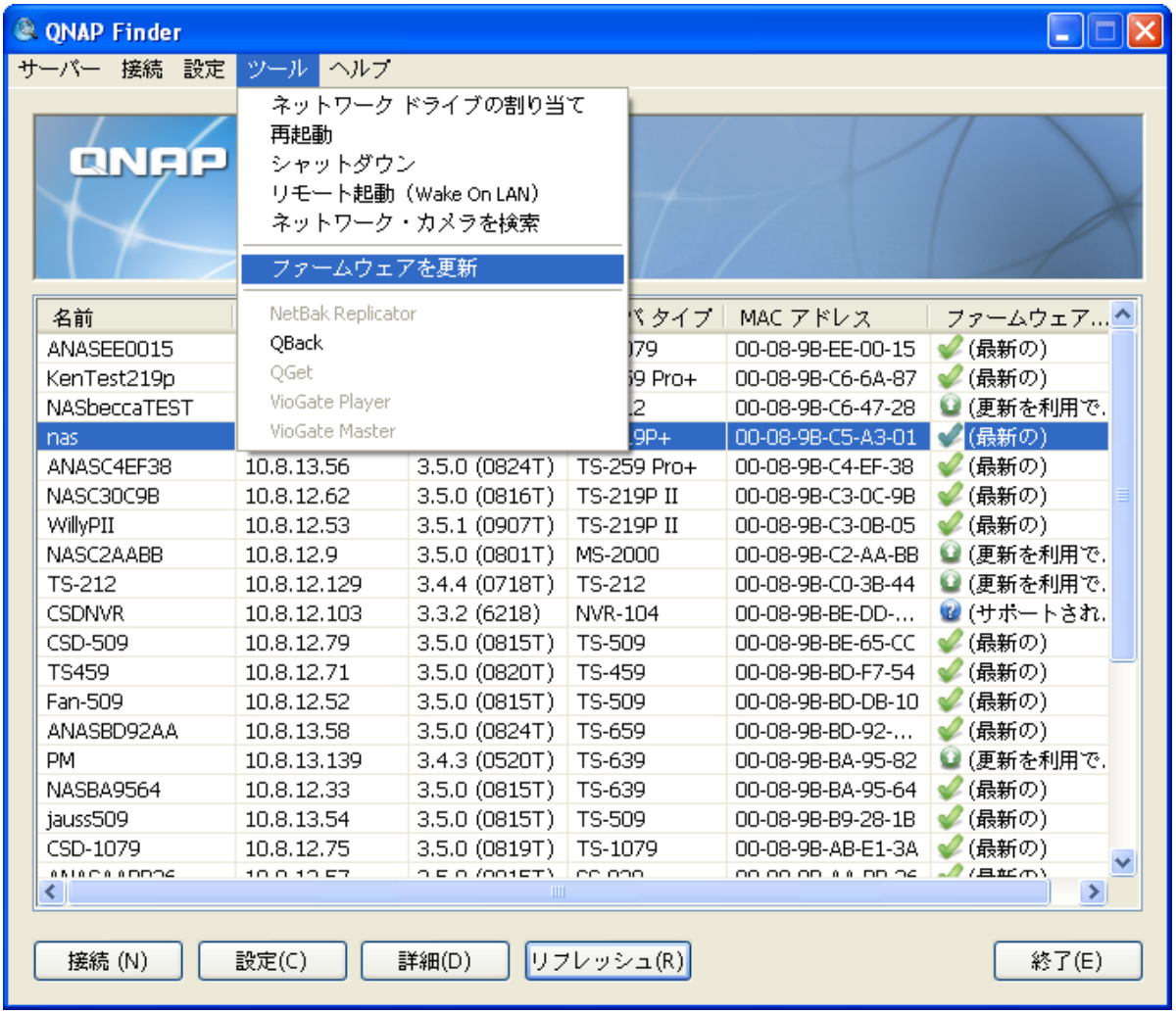
ファームウェアのアップデートを開始する前に、製品名およびファームウェアバージョンをご確認ください。ファームウェアのアップデートは下記の手順に従って進めてください。

手順1:QNAP ウェブサイトからファームウェアと同じバージョンのリリースノートをダウンロードしてください。http://www.qnap.com　リリースノートを注意してお読みください。更にファームウェアをアップデートする必要があるかどうかご確認ください。
手順2:NASファームウェアをダウンロードし、IMGファイルをご使用のコンピュータに解凍してください。
手順3:ファームウェアのアップデート前には、データの紛失を避けるためにサーバー上の全データのバックアップをとってください。
手順4:ファームウェアのアップデートには [参照…] ボタンをクリックした後、[更新] ボタンをクリックしてください。

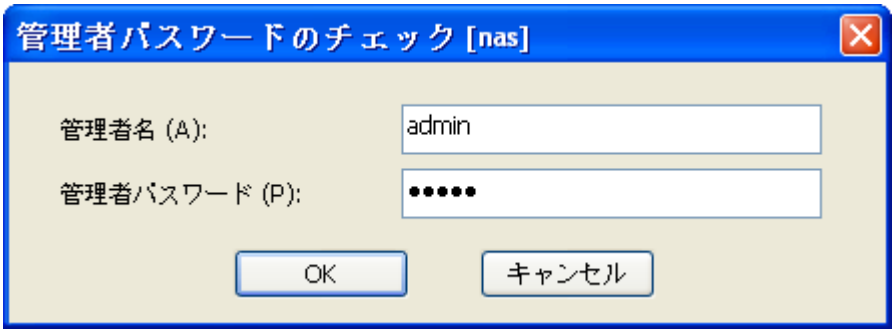
注:アップデートには数十秒から数分かかることがあります。アップデートの完了が通告されたら終了です。

Finderによるシステムファームウェアの更新

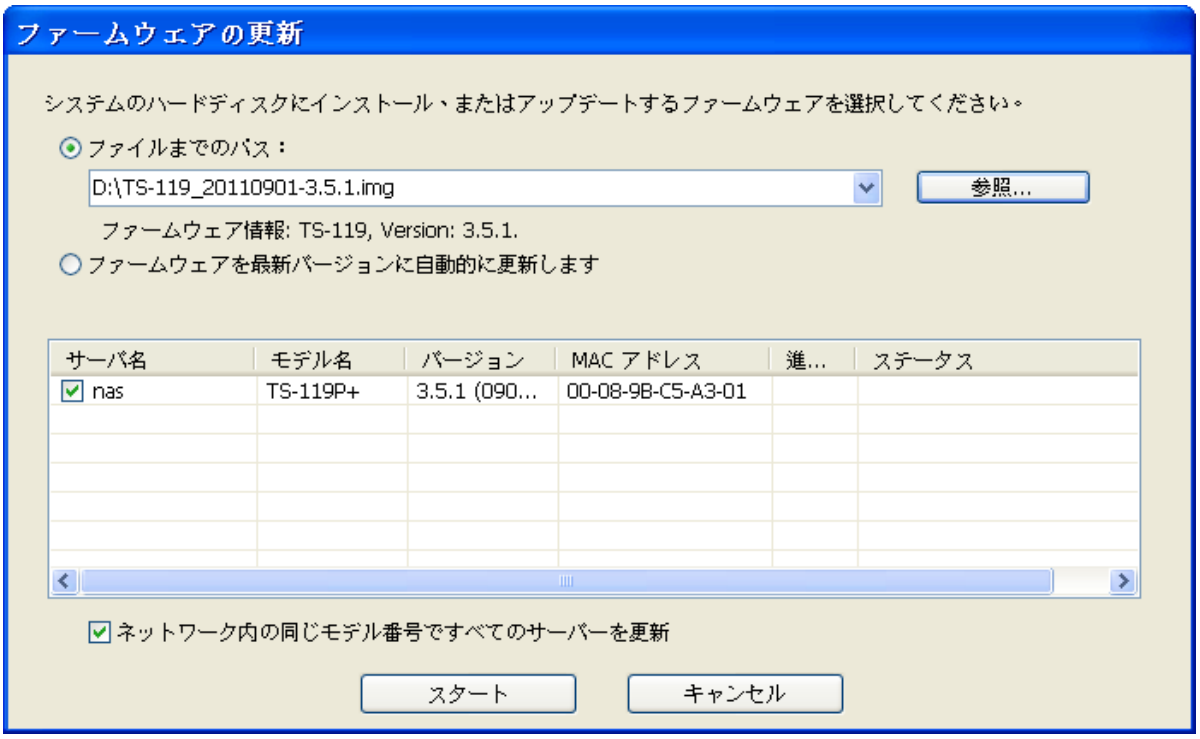
QNAP Finderによりシステムファームウェアを更新することができます。"Tools" (ツール)メニューからNASモデルを選択し"Update Firmware" (ファームウェアを更新) を選択してください。



管理者としてログインします。



NASのファームウェアを参照し選択します。"Start"（開始）をクリックしシステムを更新します。



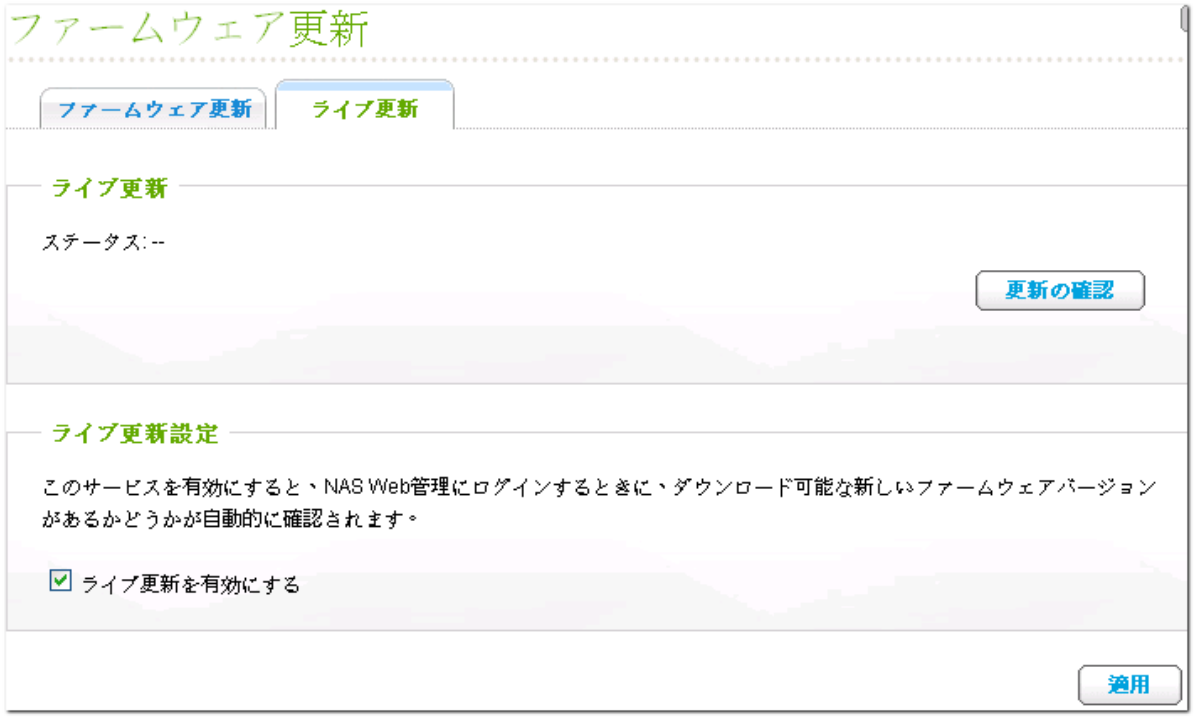
注：Finderを使用して、同じローカルネットワーク上にある同じモデルのサーバをすべて更新することができます。更新したいすべてのサーバに対し管理者権限があることを確認してください。

ライブ・アップデート

"Enable QNAP live update" (QNAPライブ・アップデートを効化)を選択すると、新規ファームウェアバージョンがインターネットからダウンロードできるかどうかをNASが自動的に確認します。ファームウェアが見つかると、NASに管理者としてログインした際にその旨が通知されます。

"CHECK FOR UPDATE" (更新を確認する)をクリックすると、いつでもファームウェアの更新について確認することができます。

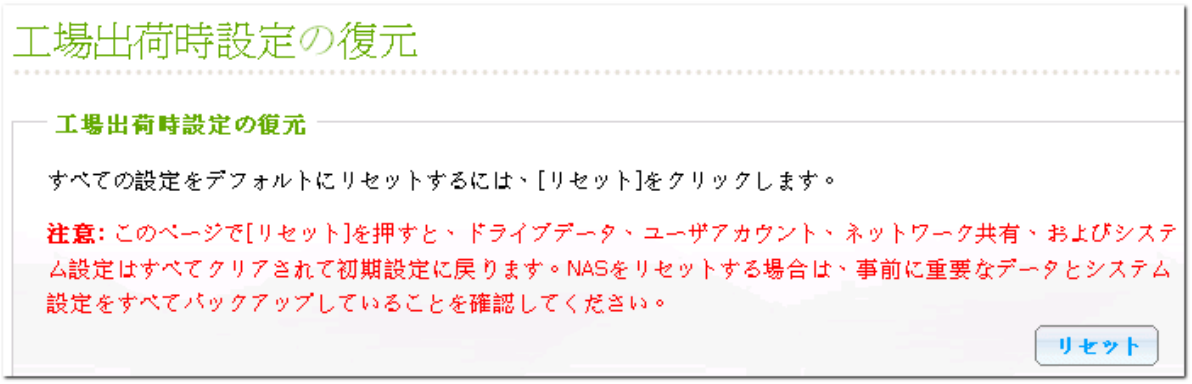
これらの機能が動作するには、NASがインターネットに接続されていることが必要となりますのでご注意ください。



3.12 工場出荷時設定の復元

設定情報を工場出荷値に戻すには、「リセット」ボタンを押してください。

注:このページで[リセット]を押すと、ドライブデータ、ユーザーアカウント、ネットワーク共およびシステム設定はすべて消去され、デフォルトに復元されます。NASをリセットする前に、すべての重要なデータとシステム設定をバックアップしていることを確認してください。



4. ディスク管理

ボリューム管理 87
RAID管理 91
ハードディスクS.M.A.R.T. 116
暗号化ファイルシステム 117
iSCSI 127
仮想ディスク 189

4.1 ボリューム管理

このページにはNASのSATAディスクのモデル、サイズ、現在のステータスが表示されます。ディスクをフォーマットしてチェックし、ディスクの不良ブロックをスキャンできます。SATAディスクをフォーマットするとき、NASは次のデフォルトの共フォルダを作成します。

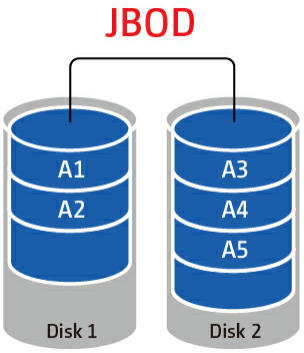
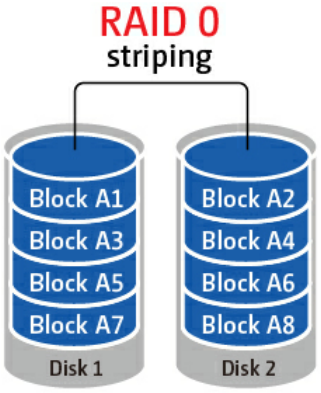
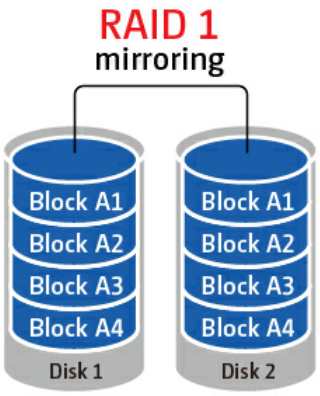
- Public:ファイルを共するためのネットワーク共
- Qdownload/ Download*:ダウンロードステーションのためのネットワーク共#
- Qmultimedia/ Multimedia*:マルチメディアステーションのためのネットワーク共#
- Qusb/ Usb*:USBケーブルを通したデータコピー機能のためのネットワーク共
- Qweb/ Web*:Webサーバ用のネットワーク共
- Qrecordings/ Recordings* は監視ステーションのデフォルトのネットワーク共です

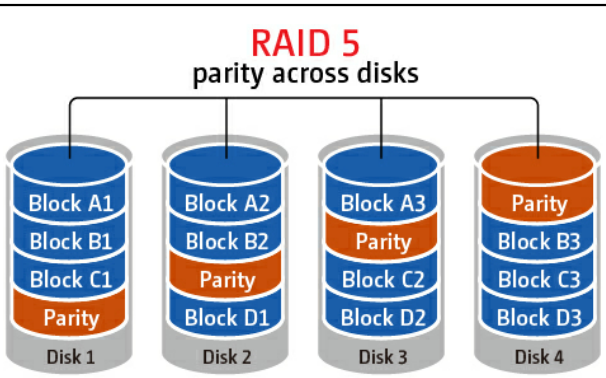
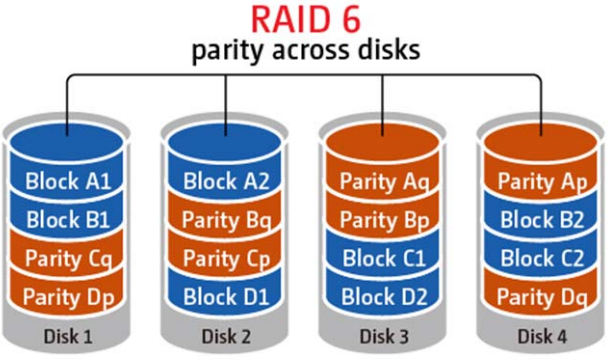
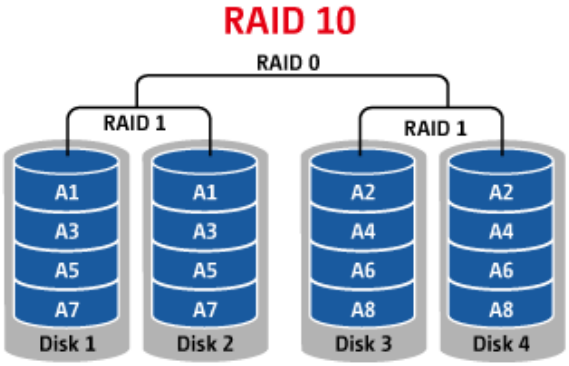
*TS-x59 シリーズのみ

#これらの機能は、TS-879 Pro、TS-1079 Pro、TS-879U-RP、TS-EC879U-RP、TS-1279U-RP、TS-EC1279U-RP ではサポートされません。

> 注:最初のディスクボリュームおよびディレクトリに作成されているデフォルトの共有は変更することはできません。

ディスク構成	対応するNAS モデル
シングルディスクボリューム	すべてのモデル
RAID 1、JBOD (Just a bunch of disks(ただのディスクの束)の略;スパニング)	2ベイモデル以上
RAID 5、RAID 6、RAID 5+ホットスペア、	4ベイモデル以上
RAID 6+ホットスペア	5ベイモデル以上
RAID 10	4ベイモデル以上
RAID 10+ホットスペア	5ベイモデル以上

シングルディスクボリューム 各ハードディスクドライブはスタンドアローンディスクとして使用されます。ディスクが損傷した場合、すべてのデータが失われます。	
JBOD (Just a bunch of disks (ディスク束) JBODは、RAID保護を行わないハードディスクドライブの集まりです。データは物理ディスクに順番に書き込まれます。合計ストレージ容量は、すべてのメンバードライブの容量の合計となります。	
RAID 0 ストライピングディスクボリューム RAID 0 (ストライピングディスク) は二つ以上のハードディスクドライブを一つの大きなボリュームにまとめます。データはパリティ情報なしにハードディスクに書き込まれ、冗長性はありません。合計ストレージ容量は、すべてのメンバードライブの容量の合計となります。	
RAID 1 ミラーリングディスクボリューム RAID 1 はディスクミラーリングによりデータを2つのハードディスクドライブの間で複製します。RAID 1アレイを作成するには、2機以上のハードドライブが必要となります。 RAID 1ディスクボリュームのストレージ容量は最小ハードドライブのサイズ。	

RAID 5ディスクボリューム データはRAID 5アレイ内のすべてのドライブにストライプされます。パリティ情報は各ドライブに分配され保管されます。メンバードライブが停止した際は、アレイは低下モードに入ります。停止したドライブに替えて新規ドライブを設置した後、データはパリティ情報を持つ他のメンバードライブから再構築することができます。 RAID 5 ディスクボリュームを作成するには、3機以上のハードドライブが必要となります。 RAID 5 アレイのストレージ容量は（N-1）x (最小ハードドライブのサイズ)と同じです。 Nは、アレイのハードドライブメンバーの総数です。	
RAID 6ディスクボリューム データはRAID 6アレイ内のすべてのドライブにストライプされます。RAID 6がRAID 5と違う点は、パリティ情報の二つ目のセットがアレイ内のメンバードライブに保管されることです。これでメンバードライブ2機の停止に備えることができます。 RAID 6ディスクボリュームを作成するには、4機以上のハードドライブが必要となります。RAID 6アレイのストレージ容量は（N-2）x (最小ハードドライブのサイズ)と同じです。Nは、アレイのハードドライブメンバーの総数です。	
RAID 10ディスクボリューム RAID 10は、1つのシステムのRAID 0およびRAID 1の利点を結合しています。 ディスクの2次セットのデータをすべてミラーリングすることでセキュリティを提供する一方で、ディスクの各セットにまたがってストライプを使用してデータ転送を加速します。 RAID 10は偶数のハードドライブを必要とします（最低4台のハードドライブ）。 RAID 10ディスクボリュームのストレージ容量は(アレイの最小容量ディスクのサイズ) *N/2と同じです。 Nは、ボリュームのハードドライブの数です。 RAID 10では、異なるペアのディスクの故障は最大2台まで許可されます。	

4.2 RAID管理

*オンラインRAID容量拡張、オンラインRAIDレベル移行、RAID復旧は、1ベイNASモデルおよびTS-210、TS-212ではサポートされません。

このページで、オンラインRAID容量拡大(RAID 1、5、6、10)とオンラインRAIDレベル移行(1台のディスク、RAID 1、5、10)を実行し、ハードドライブメンバーをRAID 5、6、または10設定に追加し、予備のハードドライブ(RAID 5、6、10)を保存されたデータで設定し、ビットマップを有効にし、RAID設定を回復することができます。

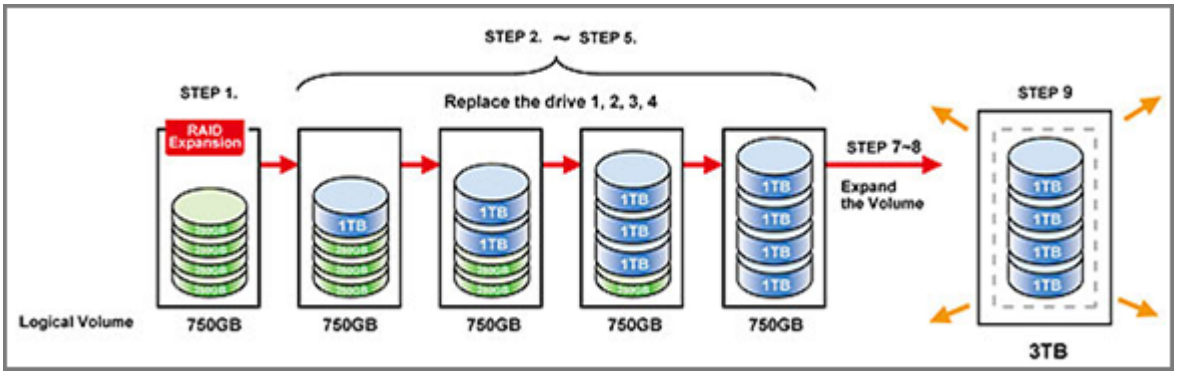
RAID 10ボリュームのストレージ容量を拡大するには、オンラインRAID容量拡大を実行するか、同じ数のハードディスクドライブをボリュームに追加します。

オンラインRAID容量拡張

使用例

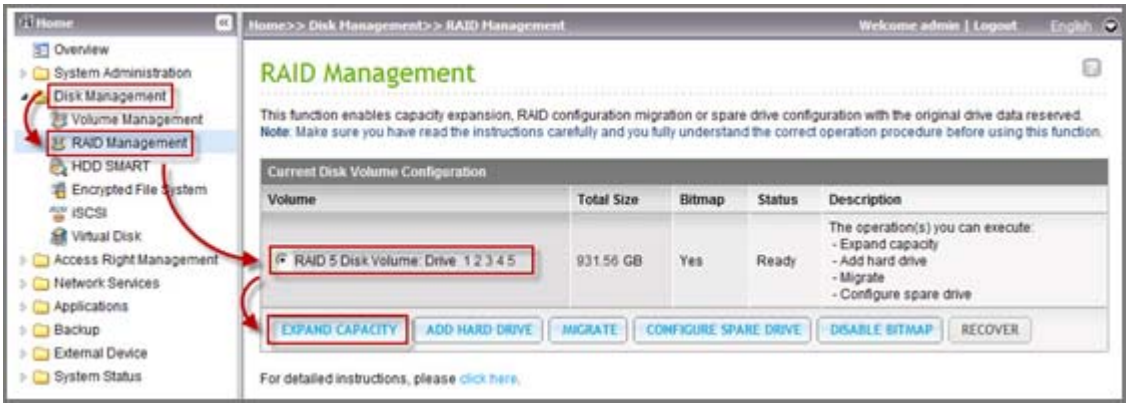
あなたはTS-509Proの初期設定のために4台の250GBハードドライブを購入し、RAID 5ディスク構成を構成しました。

半年後、部署のデータサイズは大きく増大し、1.5TBに達しました。 つまり、TS-509Proの容量はほぼフルの状態なのです。 それと同時に、 1TBハードドライブの価格は大幅に下がっています。

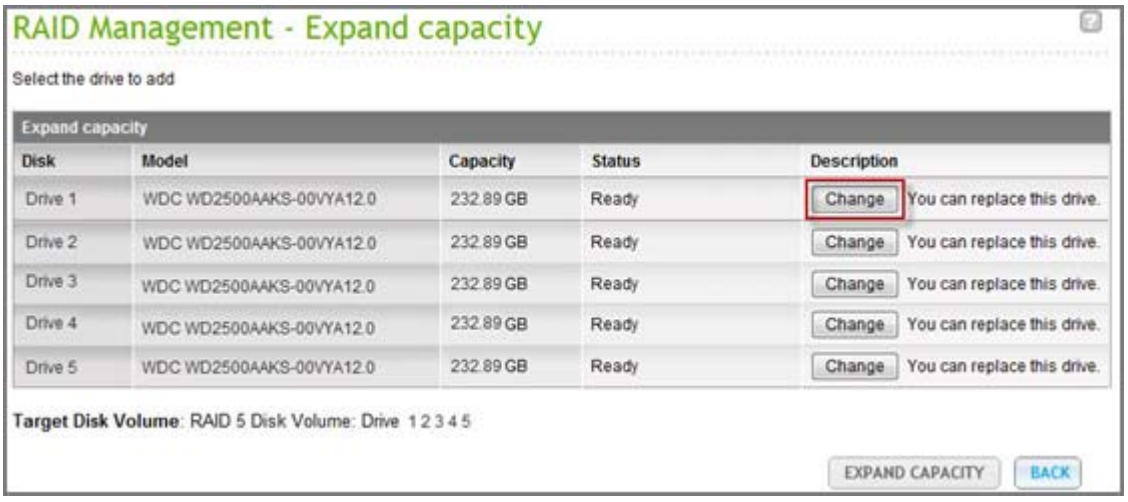


操作手順

"Disk Management" (ディスク管理) > "RAID Management" (RAID管理)ページにて、拡張するドライブボリュームを選択し、"Expand Capacity" (容量を拡張)をクリックします。



交換したい最初のハードドライブに対し"Change" (変更)をクリックします。 指示に従い続行します。

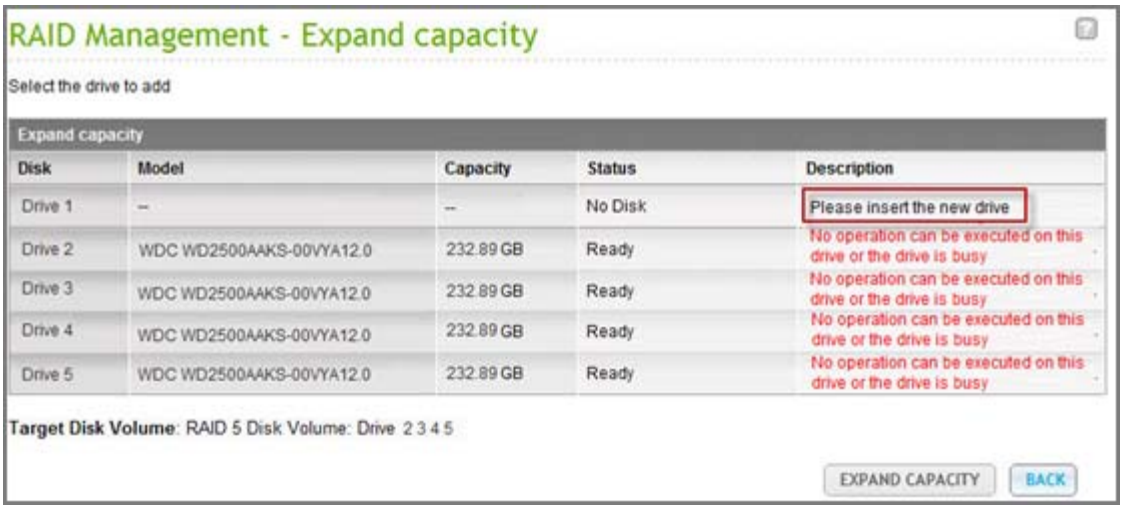


ヒント: ハードドライブを交換した後、説明の欄には"You can replace this drive" (このドライブを交換できます) のメッセージが表示されます。これは、ハードドライブをより容量が大きいものに交換できる、あるいはハードドライブが既に交換されている場合はこのステップをスキップできるということを表しています。

> 注：ハードドライブの同期が進行中の際は、ハードドライブのプラグを差し込む、または抜く、あるいはNASの電源を切る、といったことは絶対にお止めください。

説明が"Please remove this drive" (このドライブを取り外してください）と表示されたら、NASからハードドライブを取り外します。 ハードドライブを取り外した後、NASがビープ音を2回鳴らすまでお待ちください。

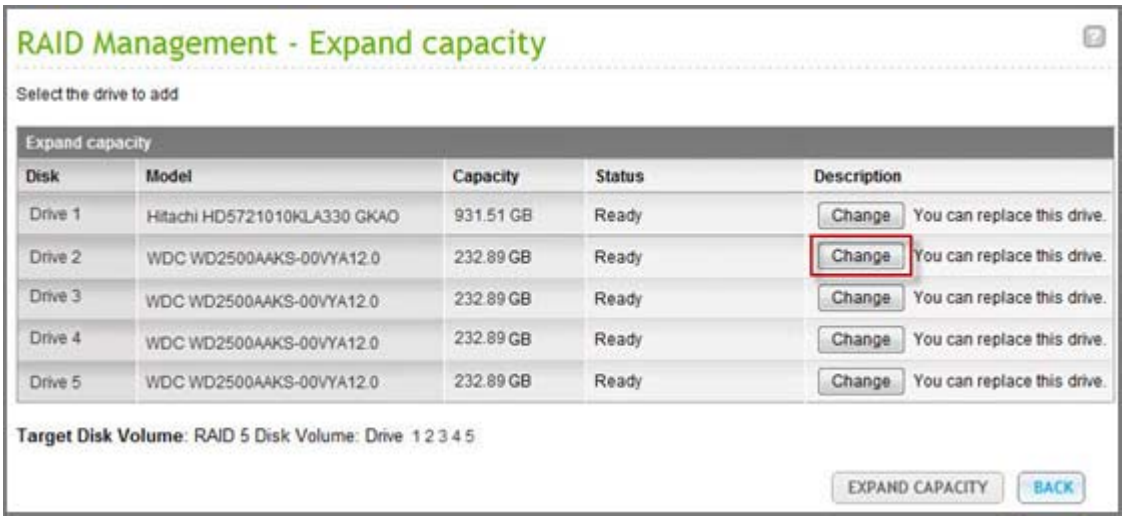
説明が"Please insert the new drive" (新しいドライバを挿入してください）と表示されたら、ドライブスロットに新しいドライブを挿入します。



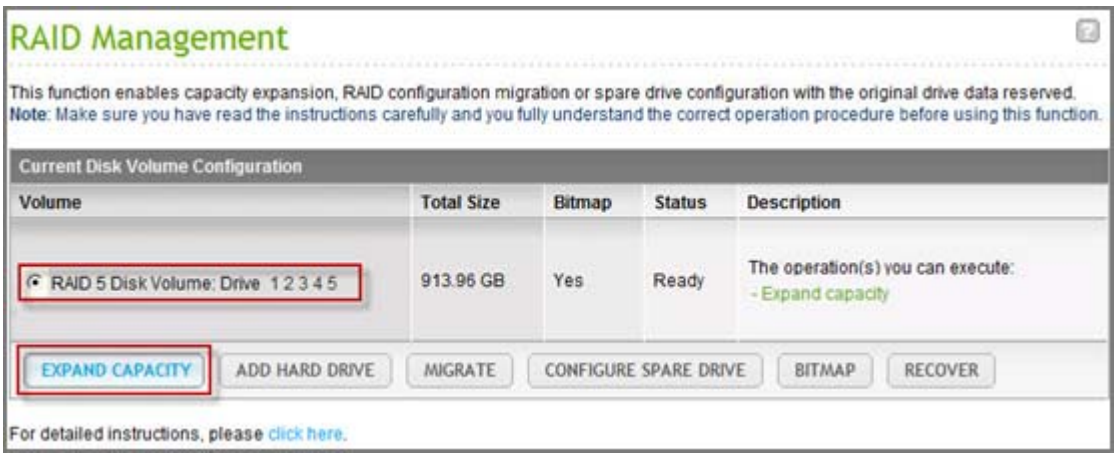
ハードドライブの挿入後、NASがビープ音を発するのをお待ちください。 システムが再構築を開始します。

Status	Description
Rebuilding... (0%)	No operation can be executed on this drive or the drive is busy
Rebuilding... (0%)	No operation can be executed on this drive or the drive is busy
Rebuilding... (0%)	No operation can be executed on this drive or the drive is busy
Rebuilding... (0%)	No operation can be executed on this drive or the drive is busy
Rebuilding... (0%)	No operation can be executed on this drive or the drive is busy

再構築が終了したら、上記のステップに従って他のハードドライブを交換します。

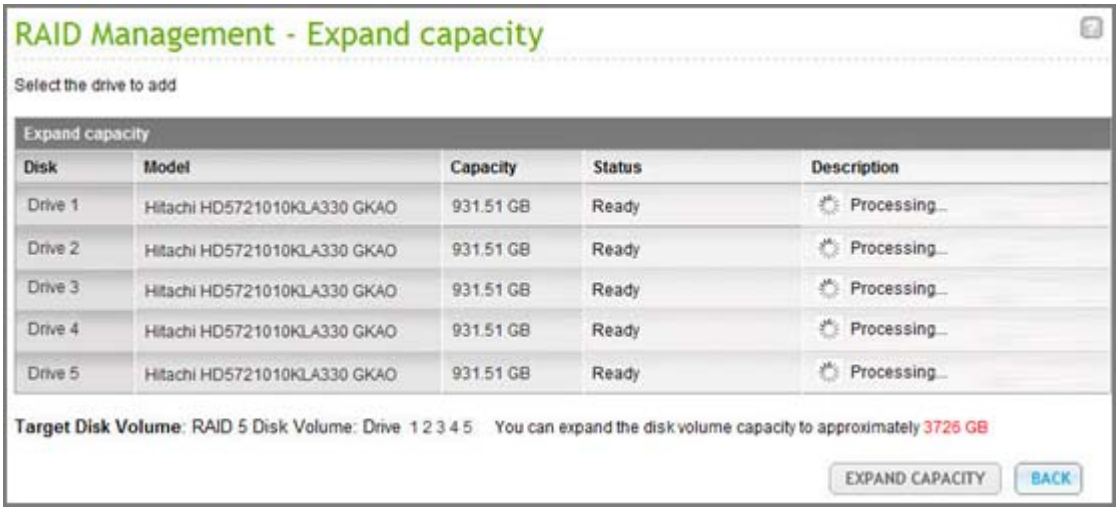


ハードドライブの交換および再構築が完了した後、"EXPAND CAPACITY"（容量を拡張）をクリックしてRAID拡張を実行します。



"OK"をクリックして続行します。

NASがビープ音を発し、容量の拡張を開始します。



ドライブのサイズにより、プロセスの完了には数時間から数十時間かかる場合があります。 プロセスが完了するまでお待ちください。 NASの電源は絶対に切らないでください。

Current Disk Volume Configuration: Physical Disks

Disk	Model	Capacity	Status	Bad Blocks Scan	SMART Information
Drive 1	Hitachi HD5721010KLA330 GKAO	931.51 GB	Ready	SCAN NOW	GOOD
Drive 2	Hitachi HD5721010KLA330 GKAO	931.51 GB	Ready	SCAN NOW	GOOD
Drive 3	Hitachi HD5721010KLA330 GKAO	931.51 GB	Ready	SCAN NOW	GOOD
Drive 4	Hitachi HD5721010KLA330 GKAO	931.51 GB	Ready	SCAN NOW	GOOD
Drive 5	Hitachi HD5721010KLA330 GKAO	931.51 GB	Ready	SCAN NOW	GOOD

Current Disk Volume Configuration: Logical Volumes

Volume	File System	Total Size	Free Size	Status
RAID 5 Disk Volume: Drive 1 2 3 4 5	EXT3	3726.04 GB	3315.36 GB	Ready

RAID拡張が完了した後、新しい容量が表示され、ステータスは"Ready"（準備完了）となります。 これで拡張された容量を使用することができます。（この例では、3TB論理ボリュームに拡張されたということです）

RAID Management

This function enables capacity expansion, RAID configuration migration or spare drive configuration with the original drive data reserved.
Note: Make sure you have read the instructions carefully and you fully understand the correct operation procedure before using this function.

Current Disk Volume Configuration

Volume	Total Size	Bitmap	Status	Description
RAID 5 Disk Volume: Drive 1 2 3 4 5	3726.04 GB	Yes	Ready	The operation(s) you can execute: - Expand capacity

EXPAND CAPACITY | ADD HARD DRIVE | MIGRATE | CONFIGURE SPARE DRIVE | BITMAP | RECOVER

For detailed instructions, please click here.

ヒント: 説明が "You can replace this hard drive"（このハードドライブを交換できます）と表示され、ドライブのボリュームステータスが "Ready"（準備完了）のままの場合、このRAIDボリュームはさらに拡張することができます。

オンラインRAIDのレベル移行

使用例

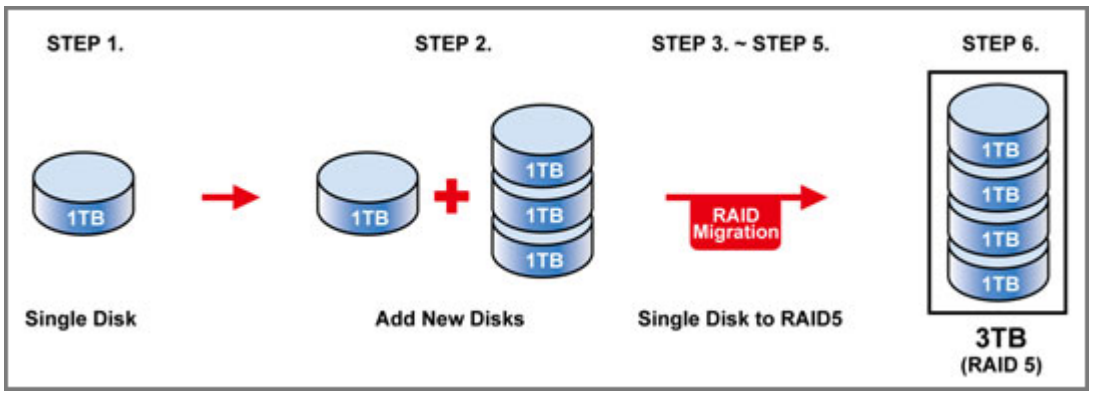
TS-509 Proの初期設定の間に、あなたは1TBハードドライブを購入し、Single Disk(シングルディスク）モードで構成しました。 TS-509 Proは部署間のデータ共有のためのファイルサーバとして使用されています。

半年後、TS-509 Proに重要なデータが大量に保管されています。 ハードドライブのクラッシュまたはデータ損失の恐れが出てきました。そこで、あなたはディスク構成をRAID 5にアップグレードすることにしました。

オンラインRAIDレベル移行により、ユーザーはTS-509 Prのセットアップのためにハードドライブを一機取り付け、後ほどRAID冗長性レベルを移行してデータ保護を向上することができます。 移行プロセスはサーバの電源を切ることなしに実行することができます。 オリジナルのデータはすべて保持されます。

オンラインRAIDレベル移行で次を実行できます。

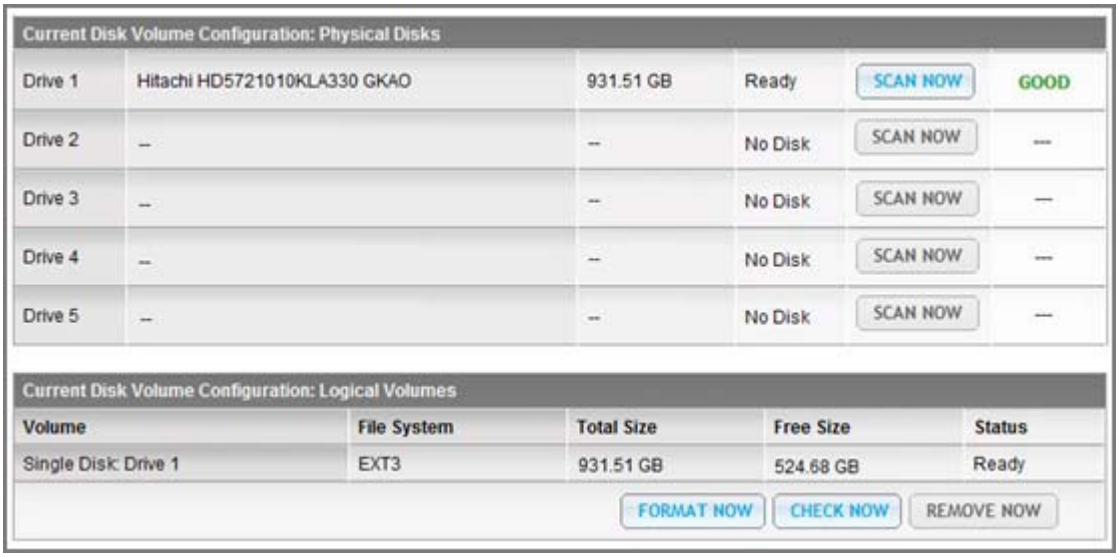
- 1台のディスクからRAID 1、RAID 5、RAID 6またはRAID 10にシステムを移行します
- RAID 1からRAID 5、RAID 6またはRAID 10にシステムを移行します
- 3台のハードドライブを持つRAID 5からRAID 6にシステムを移行します。



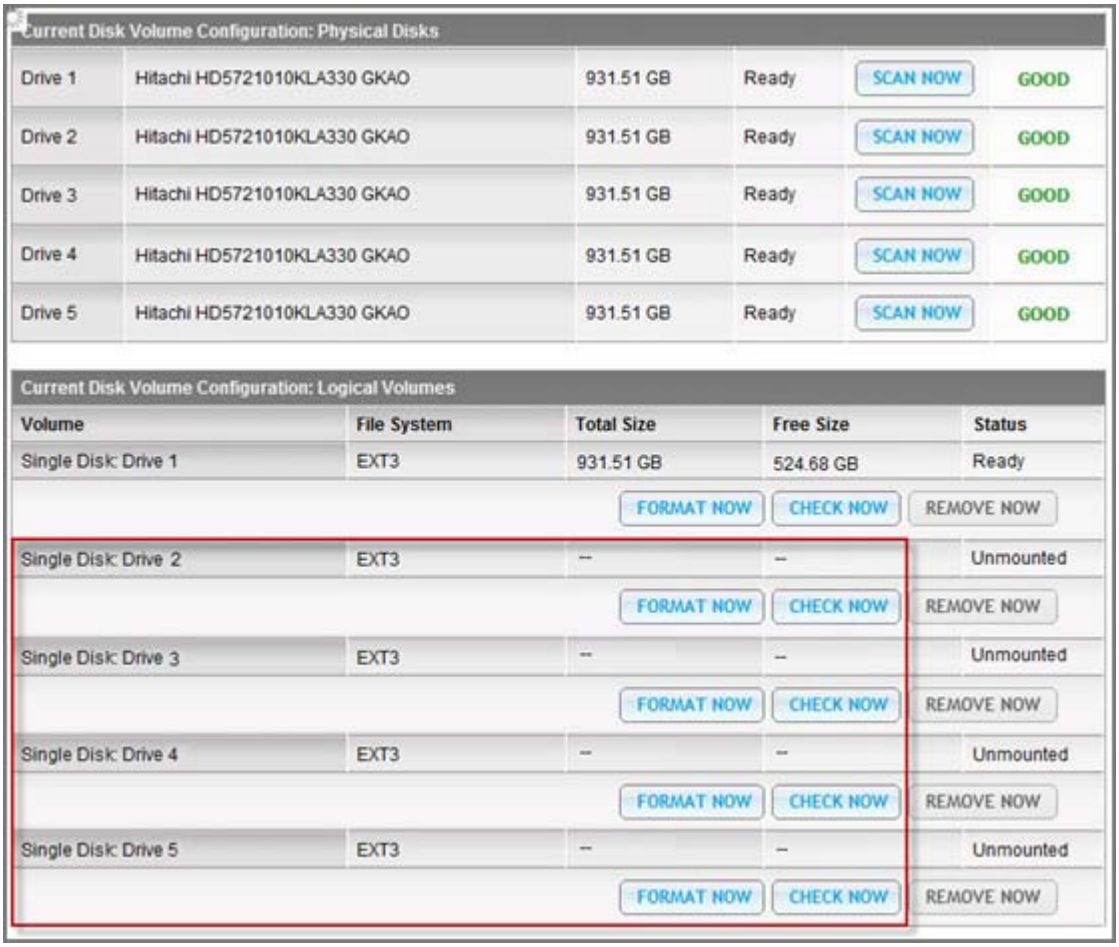
以下を行ってください

- 既存のドライブと同等またははより容量が大きいRAID構成のハードドライブを準備します。
- RAID移行（シングルディスクモードからハードディスク4台のRAID 5にシステムを移行）。

"Device Management"（デバイス管理） > "Volume Management"（ボリューム管理）ページに移動します。 ページに表示される現在のディスクボリューム構成はシングルディスク(容量1TB）です。



NASのドライブスロット2、3、4、5に1TB容量の新規ハードドライブを挿入します。 NASが新規バードディスクを検出します。 新規ディスクのステータスは"Unmounted"（マウント解除）です。



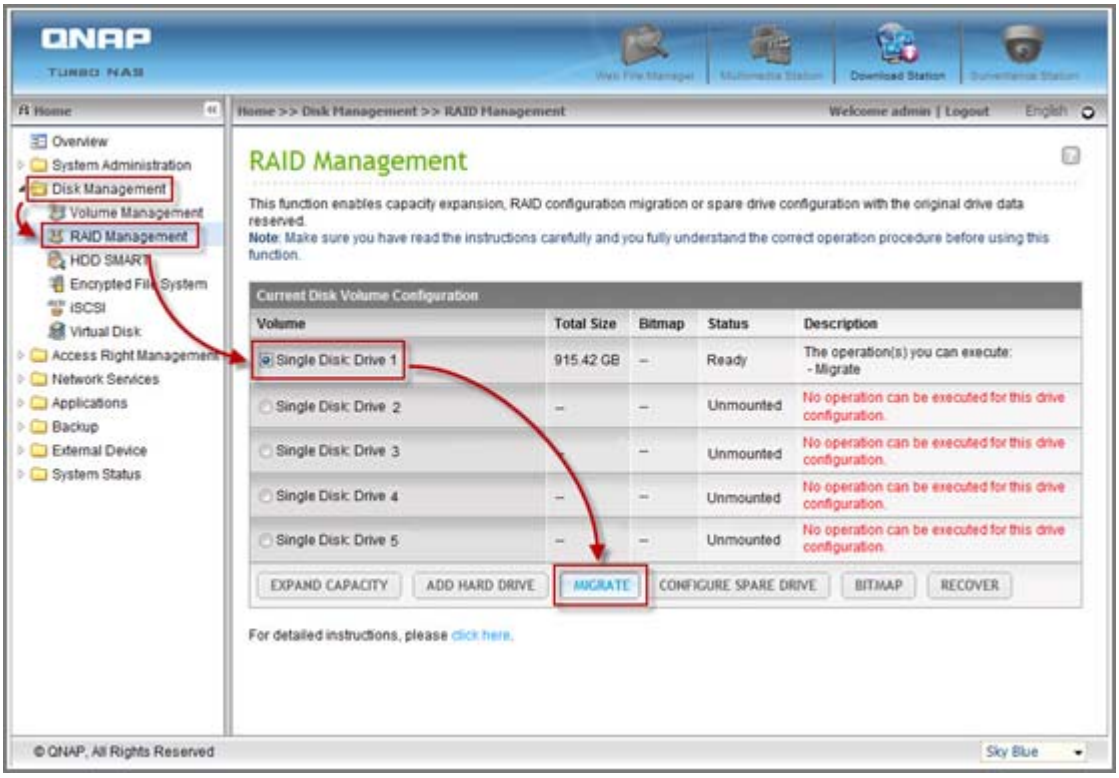
Current Disk Volume Configuration: Physical Disks

Drive 1	Hitachi HD5721010KLA330 GKAO	931.51 GB	Ready	SCAN NOW	GOOD
Drive 2	Hitachi HD5721010KLA330 GKAO	931.51 GB	Ready	SCAN NOW	GOOD
Drive 3	Hitachi HD5721010KLA330 GKAO	931.51 GB	Ready	SCAN NOW	GOOD
Drive 4	Hitachi HD5721010KLA330 GKAO	931.51 GB	Ready	SCAN NOW	GOOD
Drive 5	Hitachi HD5721010KLA330 GKAO	931.51 GB	Ready	SCAN NOW	GOOD

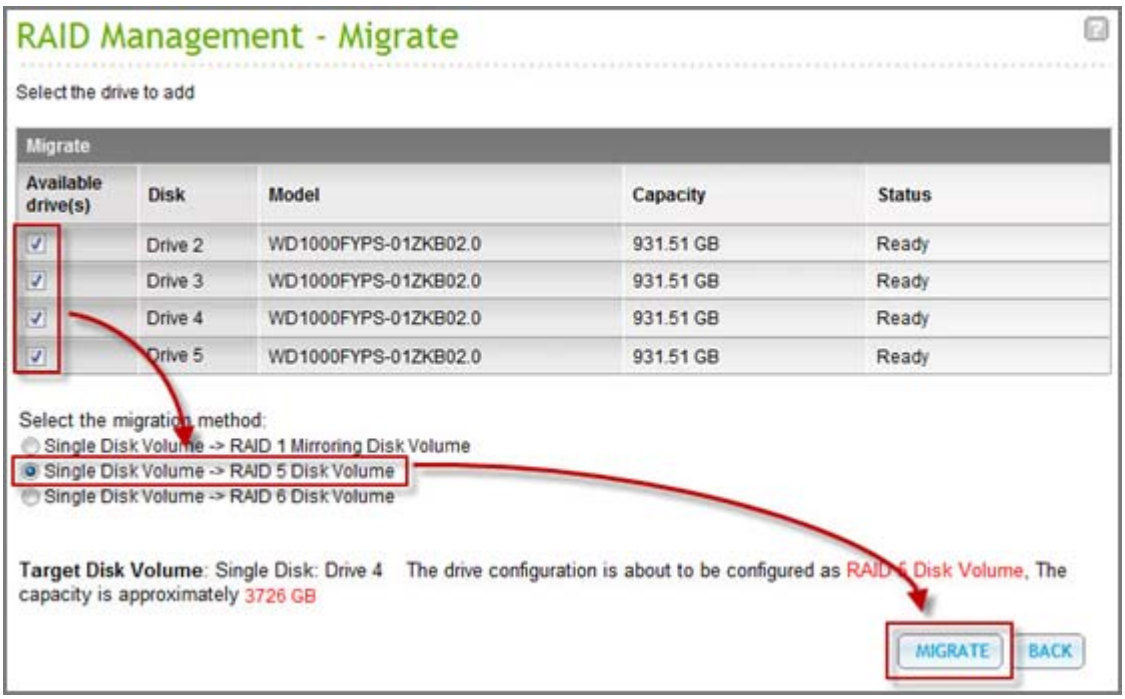
Current Disk Volume Configuration: Logical Volumes

Volume	File System	Total Size	Free Size	Status			
Single Disk Drive 1	EXT3	931.51 GB	524.68 GB	Ready			
				FORMAT NOW	CHECK NOW	REMOVE NOW	
Single Disk Drive 2	EXT3	--	--	Unmounted			
				FORMAT NOW	CHECK NOW	REMOVE NOW	
Single Disk Drive 3	EXT3	--	--	Unmounted			
				FORMAT NOW	CHECK NOW	REMOVE NOW	
Single Disk Drive 4	EXT3	--	--	Unmounted			
				FORMAT NOW	CHECK NOW	REMOVE NOW	
Single Disk Drive 5	EXT3	--	--	Unmounted			
				FORMAT NOW	CHECK NOW	REMOVE NOW	

"Disk Management"（ディスク管理） > "RAID Management"（RAID管理）ページにて、移行するドライブ構成を選択し、"Migrate"（移行）をクリックします。

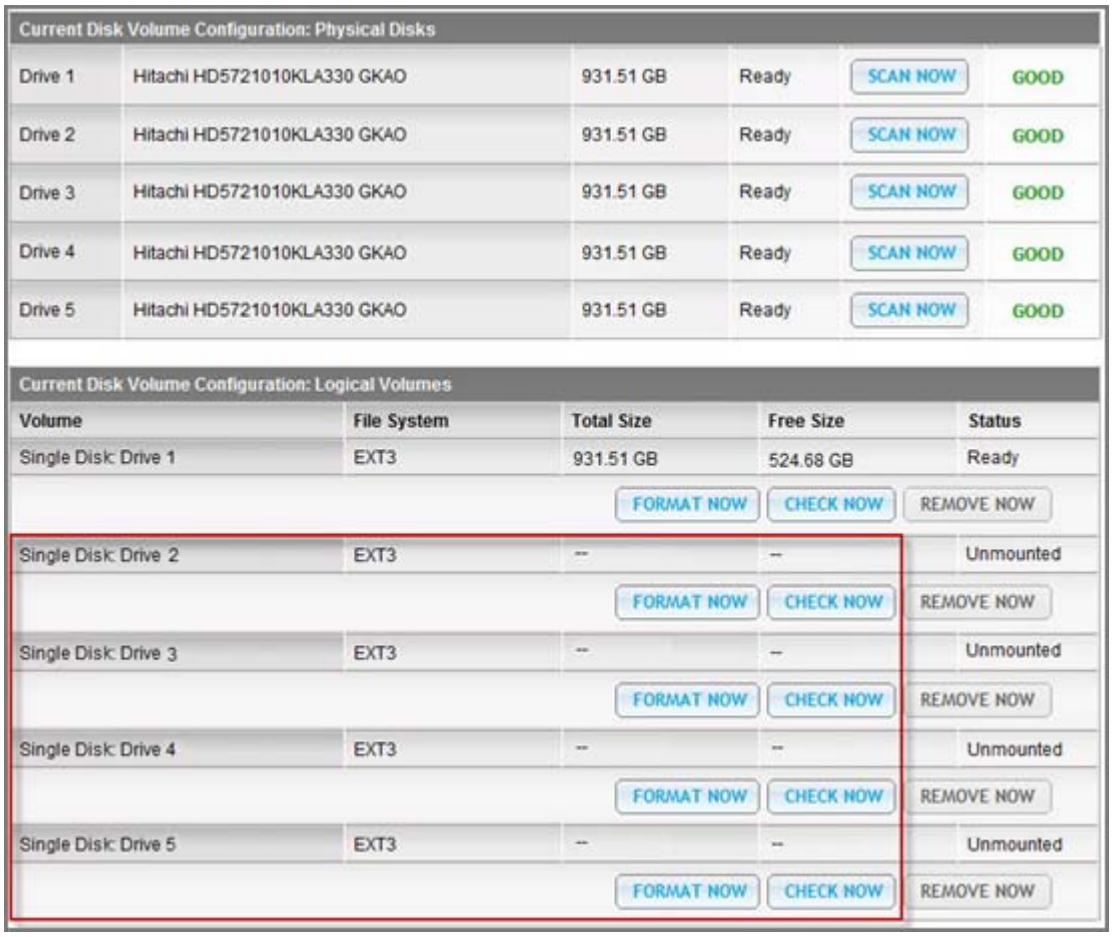


1つ以上の使用可能なドライブおよび移行方法を選択してください。 移行後のドライブ容量が表示されます。"Migrate"（移行）をクリックして続行します。



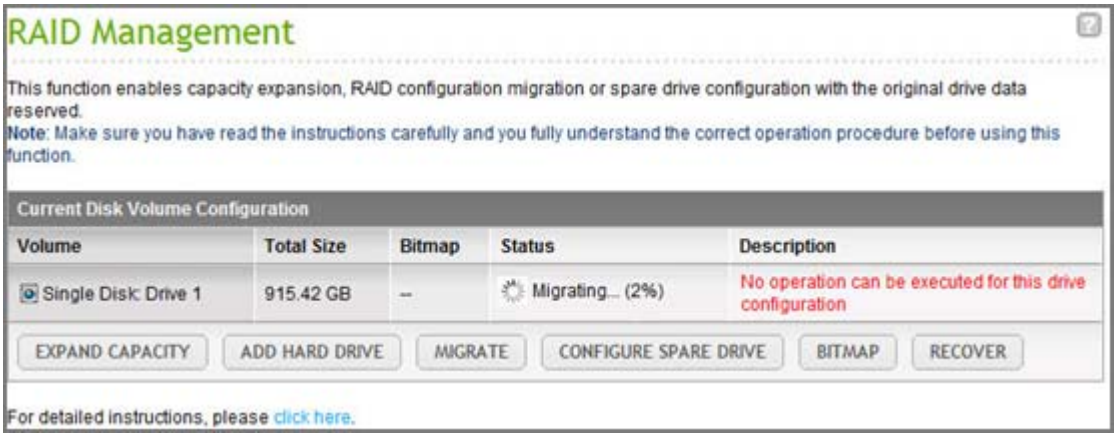
選択したドライブのすべてのデータは消去されます。"OK"をクリックして確定します。

移行が進行中の際は、説明の欄に必要な時間と移行後のドライブ容量が表示されます。



注: RAID構成のデータがRAID移行完了後も確実に一致するよう、NASシステムは、移行が11%~49%進行中の際に"Read only" (読み取り専用）モードに入ります。

移行が完了した後、新しいドライブ構成が表示され(この場合RAID 5）、ステータスはReady(準備完了）となります。これで新しいドライブ構成を使用することができます。

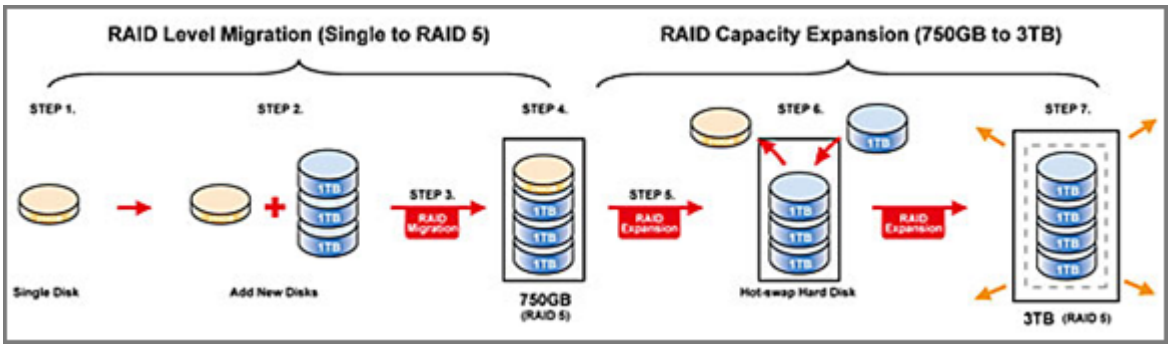


ドライブのサイズにより、プロセスの完了には数時間から数十時間かかる場合があります。後で、NASのWebページに接続してステータスを確認することができます。

オンラインRAID容量拡張およびオンラインRAIDレベル移行を併用する

使用例
あなたははとても多忙で、ファイルサーバとFTPサーバをセットアップする時間が見つかりませんでした。しかし、あなたがお持ちのドライブは250GBのハードドライブ一台だけでした。 そこで、TS-509 Proをシングルディスク構成でセットアップしました。

元のプランは、TS-509 Proを3TB RAID 5ネットワークデータセンターにてセットアップすることでした。
あなたは今、TS-509 Proのディスク構成をRAID 5に移行し、総ストレージ容量を3TBに拡張、すべてのオリジナルのデータはハードドライブを購入した後に保持、というプランを立てています。



システムをシングルディスクからRAID 5へ移行するため、オンラインRAIDレベル移行を実行します。RAID 5の総ストレージ容量は750GBになります(250GBドライブ1台、 1TBドライブ3台、RAID 5のディスク使用は250GB*4となります)。 操作手順についての詳細は前のステップを参照してください。

250GBドライブを新規 1TBドライブと交換するためオンラインRAID容量拡張を実行します。そしてRAID 5の論理ボリュームを750GBから3TBに拡張します。詳細な操作手順についてはケース1を参照してください。

ハードドライブの追加

以下の手順に従ってHDDメンバーをRAID 5またはRAID 6ディスク設定に追加します。

1. RAID 5またはRAID 6設定の状態が「Ready（準備OK）」になっていることを確認します。
2. NASにHDDを取り付けます。 お使いのHDDがNASの1台のディスクボリュームとしてすでにフォーマットされている場合、HDDをRAID 5またはRAID 6設定に追加できます。 RAID設定の場合、同じストレージ容量のハードディスクドライブを使用するようにお勧めします。
3. 「RAID管理」ページでRAID 5またはRAID 6設定を選択し、「ハードドライブの追加」をクリックします。
4. 新しいHDDメンバーを選択します。 ドライブを追加した後の合計ドライブ容量が表示されます。 「ハードドライブの追加」をクリックします。
5. 新しいHDDメンバーのすべてのデータが、このプロセス中に削除されます。 元のRAID 5またはRAID 6設定のデータが保存されます。 [OK] をクリックします。 NASが2回ビープ音を出します。

RAID 10ディスクボリュームにハードドライブのメンバーを追加するには、上の手順を繰り返します。 RAID 10ボリュームに、偶数のハードディスクドライブを追加する必要があります。 正常に設定されると、RAID 10ボリュームのストレージ容量が増加します。

このプロセスでは終了するまでに、ハードドライブの数とサイズによって、数時間から数十時間かかります。 プロセスが終了するまで、しばらくお待ちください。 このプロセスの間、NASをオフにしないでください。 プロセス後、大容量のRAID設定を使用することができます。

予備のドライブの設定

予備のドライブをRAID 5、6、または10設定に追加したり、この設定から取り外したりできます。

この機能を使用するには、以下の手順に従ってください。

1. RAID 5、6、10設定の状態が「Ready（準備OK）」になっていることを確認します。
2. 予備のドライブを追加するには、NASにハードドライブを取り付けます。 NASにシングルディスクボリュームとしてフォーマット済みのハードドライブを取り付けている場合、予備のドライブとしてこのハードドライブを設定できます。 RAID設定の場合、同じストレージ容量のハードディスクドライブを使用するようにお勧めします。
3. RAID設定を選択し、「CONFIGURE SPARE DRIVE（予備のドライブの設定）」をクリックします。
4. 選択した設定に予備のドライブを追加するには、ハードドライブを選択し「CONFIGURE SPARE DRIVE（スペアドライブの設定）」をクリックします。予備のドライブを取り外すには、予備のドライブを選択解除し、「CONFIGURE SPARE DRIVE（予備のドライブの設定）」をクリックします。
5. 選択したハードドライブのデータがすべて削除されます。「OK」をクリックして続行します。

RAID 5、RAID 6、または10ディスクボリュームの元のデータが保存されます。 設定が完了すると、ディスクボリュームの状態が「Ready（準備OK）」になります。

Bitmap

Bitmap(ビットマップ)は、クラッシュやRAID構成のメンバードライブの削除または再追加の後のRAID再構築の時間を縮小します。配列内にビットマップが存在する場合、メンバードライブは削除または再追加が可能であり、削除移行に更されたブロックのみ (ビットマップに記録されているとおり再同期されます。

> 注：ビットマップサポートは、RAID1、5、6構成でのみ使用可能です。

RAID復旧

NASがRAID 1、RAID 5あるいはRAID 6で構成されており、機のハードドライブがサーバから誤ってプラグを抜かれた場合、そのハードドライブを同じドライブスロットにプラグインして「回復」をクリックすることで、ボリュームステータスを「起動していません(Not active) 」から「格下げモード(Degraded mode) 」 に戻すことができます。

ディスクボリュームがRAID 0あるいはJBODで構成されている場合に、1台以上のドライブメンバーがNASから接続を切断されたり、プラグを抜かれた場合、この機能を使用してボリュームステータスを「起動していません(Not active) 」から「一般(Normal) 」に回復することができます。 回復が完了すると、ディスクボリュームは正常に使用することができます。

ディスクボリューム	RAID回復をサポート	ディスク削除が可能な最大数
シングル	いいえ	–
JBOD	はい	1台以上
RAID 0	はい	1台以上
RAID 1	はい	1台あるいは2台
RAID 5	はい	2台以上
RAID 6	はい	3台以上
RAID 10	いいえ	–

注：

- RAID回復によってRAID 1、RAID 5 あるいはRAID 6ディスクボリュームを非アクティブから低下モードに回復した場合は、通常通りボリュームの読取り/書込みが可能になります。ボリュームステータスは、同期の後に正常に回復されます。
- 切断されたドライブメンバーに障害がある場合、RAID回復機能は動作しません。

	標準RAID 5	QNAP RAID5	標準RAID 6	QNAP RAID6
低下モード	N-1	N-1	N-1 & N-2	N-1 & N-2
読み取り専用保護 (即時データバックアップ & HDD 交換)	適用なし	N-1、不良ブロックがアレイ中の残存ドライブに存在	適用なし	N-2、不良ブロックがアレイ中の残存ドライブに存在
RAID復旧 (RAIDステータス:非アクティブ)	適用なし	元のハードディスクドライブをすべてNAS に挿入しなおした場合に、ドライブが起動し、認識され、アクセスできる場合、HDD スーパーブロックは破損していません。	適用なし	元のハードディスクドライブをすべてNASに挿入しなおした場合に、ドライブが起動し、認識され、アクセスできる場合、HDD スーパーブロックは破損していません。
RAIDキャッシュ	N-2	N-2 停止したHDDおよびその他すべてのHDDが起動/ 認識/ アクセスできない。	N-3	N-3 およびその他すべてのHDDが起動/ 認識/ アクセスできない。

N = アレイ中のハードディスクドライブの数

グローバルスペアの設定/解除

グローバルスペアドライブは、NAS 上の RAID 1、5、6、10 ディスクボリュームの故障したハードドライブに自動的に置き換わります。同じグローバルスペアが NAS 上の複数の RAID ボリュームで共有されている場合、スペアドライブは、RAID ボリュームで最初に故障したドライブに置き換わります。

グローバルスペアドライブとして、ディスクドライブを設定するには、1 台のディスクボリュームを選択し、「Set Global Spare（グローバルスペアの設定）」をクリックします。**ハードドライブ上のすべてのデータが消去されます。**

注：グローバルスペアドライブの容量は、RAID ディスクボリュームのドライブの容量と等しいか、または、それより大きくなければなりません。

グローバルスペアドライブを解除するには、ドライブを選択し、「Cancel Spare Drive（スペアドライブの解除）」をクリックします。

NASは、サポートされるハードドライブの数とディスクの構成に従って以下の操作をサポートします。詳細は、下表を参照してください。

最初のディスクの構成 * ハードディスクの数	新規ハードディスクの数	操作	新規ディスクの構成 * HDDの数
RAID 5 * 3	1	ハードディスクメンバーの追加	RAID 5 * 4
RAID 5 * 3	2	ハードディスクメンバーの追加	RAID 5 * 5
RAID 5 * 3	3	ハードディスクメンバーの追加	RAID 5 * 6
RAID 5 * 3	4	ハードディスクメンバーの追加	RAID 5 * 7
RAID 5 * 3	5	ハードディスクメンバーの追加	RAID 5 * 8
RAID 5 * 4	1	ハードディスクメンバーの追加	RAID 5 * 5
RAID 5 * 4	2	ハードディスクメンバーの追加	RAID 5 * 6
RAID 5 * 4	3	ハードディスクメンバーの追加	RAID 5 * 7
RAID 5 * 4	4	ハードディスクメンバーの追加	RAID 5 * 8
RAID 5 * 5	1	ハードディスクメンバーの追加	RAID 5 * 6
RAID 5 * 5	2	ハードディスクメンバーの追加	RAID 5 * 7
RAID 5 * 5	3	ハードディスクメンバーの追加	RAID 5 * 8
RAID 5 * 6	1	ハードディスクメンバーの追加	RAID 5 * 7
RAID 5 * 6	2	ハードディスクメンバーの追加	RAID 5 * 8
RAID 5 * 7	1	ハードディスクメンバーの追加	RAID 5 * 8
RAID 6 * 4	1	ハードディスクメンバーの追加	RAID 6 * 5
RAID 6 * 4	2	ハードディスクメンバーの追加	RAID 6 * 6

RAID 6 * 4	3	ハードディスクメンバーの追加	RAID 6 * 7
RAID 6 * 4	4	ハードディスクメンバーの追加	RAID 6 * 8
RAID 6 * 5	1	ハードディスクメンバーの追加	RAID 6 * 6
RAID 6 * 5	2	ハードディスクメンバーの追加	RAID 6 * 7
RAID 6 * 5	3	ハードディスクメンバーの追加	RAID 6 * 8
RAID 6 * 6	1	ハードディスクメンバーの追加	RAID 6 * 7
RAID 6 * 6	2	ハードディスクメンバーの追加	RAID 6 * 8
RAID 6 * 7	1	ハードディスクメンバーの追加	RAID 6 * 8
RAID 10 * 4	2	ハードディスクメンバーの追加	RAID 10 * 6
RAID 10 * 4	4	ハードディスクメンバーの追加	RAID 10 * 8
RAID 10 * 6	2	ハードディスクメンバーの追加	RAID 10 * 8
RAID 1 * 2	1	オンラインRAID容量拡張	RAID 1 * 2
RAID 5 * 3	1	オンラインRAID容量拡張	RAID 5 * 3
RAID 5 * 4	1	オンラインRAID容量拡張	RAID 5 * 4
RAID 5 * 5	1	オンラインRAID容量拡張	RAID 5 * 5
RAID 5 * 6	1	オンラインRAID容量拡張	RAID 5 * 6
RAID 5 * 7	1	オンラインRAID容量拡張	RAID 5 * 7
RAID 5 * 8	1	オンラインRAID容量拡張	RAID 5 * 8
RAID 6 * 4	1	オンラインRAID容量拡張	RAID 6 * 4
RAID 6 * 5	1	オンラインRAID容量拡張	RAID 6 * 5
RAID 6 * 6	1	オンラインRAID容量拡張	RAID 6 * 6
RAID 6 * 7	1	オンラインRAID容量拡張	RAID 6 * 7
RAID 6 * 8	1	オンラインRAID容量拡張	RAID 6 * 8
RAID 10 * 4	1	オンラインRAID容量拡張	RAID 10 * 4

RAID 10 * 6	1	オンラインRAID容量拡張	RAID 10 * 6
RAID 10 * 8	1	オンラインRAID容量拡張	RAID 10 * 8
シングル * 1	1	オンラインRAIDレベル移行	RAID 1 * 2
シングル * 1	2	オンラインRAIDレベル移行	RAID 5 * 3
シングル * 1	3	オンラインRAIDレベル移行	RAID 5 * 4
シングル * 1	4	オンラインRAIDレベル移行	RAID 5 * 5
シングル * 1	5	オンラインRAIDレベル移行	RAID 5 * 6
シングル * 1	6	オンラインRAIDレベル移行	RAID 5 * 7
シングル * 1	7	オンラインRAIDレベル移行	RAID 5 * 8
シングル * 1	3	オンラインRAIDレベル移行	RAID 6 * 4
シングル * 1	4	オンラインRAIDレベル移行	RAID 6 * 5
シングル * 1	5	オンラインRAIDレベル移行	RAID 6 * 6
シングル * 1	6	オンラインRAIDレベル移行	RAID 6 * 7
シングル * 1	7	オンラインRAIDレベル移行	RAID 6 * 8
シングル * 1	3	オンラインRAIDレベル移行	RAID 10 * 4
シングル * 1	5	オンラインRAIDレベル移行	RAID 10 * 6
シングル * 1	7	オンラインRAIDレベル移行	RAID 10 * 8
RAID 1 * 2	1	オンラインRAIDレベル移行	RAID 5 * 3
RAID 1 * 2	2	オンラインRAIDレベル移行	RAID 5 * 4
RAID 1 * 2	3	オンラインRAIDレベル移行	RAID 5 * 5
RAID 1 * 2	4	オンラインRAIDレベル移行	RAID 5 * 6
RAID 1 * 2	5	オンラインRAIDレベル移行	RAID 5 * 7
RAID 1 * 2	6	オンラインRAIDレベル移行	RAID 5 * 8
RAID 1 * 2	2	オンラインRAIDレベル移行	RAID 6 * 4
RAID 1 * 2	3	オンラインRAIDレベル移行	RAID 6 * 5
RAID 1 * 2	4	オンラインRAIDレベル移行	RAID 6 * 6
RAID 1 * 2	5	オンラインRAIDレベル移行	RAID 6 * 7
RAID 1 * 2	6	オンラインRAIDレベル移行	RAID 6 * 8
RAID 1 * 2	2	オンラインRAIDレベル移行	RAID 10 * 4
RAID 1 * 2	4	オンラインRAIDレベル移行	RAID 10 * 6

RAID 1 * 2	5	オンラインRAIDレベル移行	RAID 10 * 8
RAID 5 * 3	1	オンラインRAIDレベル移行	RAID 6 * 4
RAID 5 * 3	2	オンラインRAIDレベル移行	RAID 6 * 5
RAID 5 * 3	3	オンラインRAIDレベル移行	RAID 6 * 6
RAID 5 * 3	4	オンラインRAIDレベル移行	RAID 6 * 7
RAID 5 * 3	5	オンラインRAIDレベル移行	RAID 6 * 8

4.3 ハードディスクS.M.A.R.T.

S.M.A.R.T.（セルフモニタリング・アナリシス・アンド・リポーティング・テクノロジー）によって、ハードディスクの状態、温度、使用状況を監視することができます。

ハードドライブを選択すると、対応するボタンをクリックすることで次の情報を表示できます。

項目	説明
概要	ハードドライブのスマートサマリと最新のテスト結果を表示します。
ハードディスク情報	ハードドライブの詳細、たとえばモデル、シリアル番号、ドライブ容量などが表示されます。
SMART情報	ハードドライブのS.M.A.R.T.が表示されます。しきい値より値が低いアイテムは、すべて異常と見なされます。
テスト	ハードドライブのS.M.A.R.T.テストを素早く完璧に実施し、結果を表示します。
設定	温度アラームを設定します。ハードドライブの温度がプリセット値を超えるとき、システムはエラーログを記録します。 素早く完璧なテストスケジュールも設定できます。最新のテスト結果は、サマリページに表示されます。

4.4 暗号化ファイルシステム

この機能は、TS-110、TS-119、TS-210、TS-219、TS-219P、TS-410、TS-419P、TS-410U、TS-419U、TS-119P+、TS-219P+、TS-419P+、TS-112、TS-212、TS-412、TS-419U+、およびTS-412Uではサポートされません。

このページでNASの暗号化されたディスクボリュームを管理できます。暗号化された各ディスクボリュームは特定のキーでロックされます。暗号化されたボリュームは以下の方法でロックを解除できます。

- 暗号化パスワード： 暗号化パスワードを入力してディスクボリュームのロックを解除します。デフォルトのパスワードは「admin」に設定されています。パスワードは、8～16文字にしてください。記号 (! @ # $ % ^ & * ( )_+ = ?) はサポートされています。
- 暗号化キーファイル： 暗号化ファイルをサーバーにアップロードしてディスクボリュームのロックを解除します。ディスクボリュームのロックが正常に解除されると、「暗号化キーの管理」ページからキーをダウンロードできます。

データ暗号化機能は、一部の国では法規制に従って利用できないことがあります。

QNAP Turbo NASのデータ暗号化機能を使用するには

Turbo NASのデータ暗号化機能により、NASのディスクボリュームを256ビットAES暗号により暗号化し、データ漏洩を防ぎます。暗号化されたディスクボリュームは認証されたパスワードによってのみ、通常の読取り/書込みアクセス用にマウントすることができます。暗号化により、ハードドライブあるいはサーバ自体が盗難されても機密データを保護することができます。

AES 暗号化について：

"暗号技術において、新暗号規格 (AES) は米国政府に採用されている暗号規格です。この規格は3つのブロック暗号、AES-128, AES-192 and AES-256 […] によって構成されています。各AES暗号は128ビットのブロックサイズで、それぞれ128、192、256ビットの鍵長となります。AES暗号は広範囲にわたって分析され、現在は世界中で利用されています。" http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

AESボリュームベース暗号化は特定のQNAP NASモデルにのみ適用されます。
詳しくはこちらの対応表をご参照ください: http://www.qnap.com/images/products/comparison/Comparison_NAS.html

始める前に

Turbo NASのデータ暗号化機能の使用を始める前に、以下の点にご注意ください。

- Turbo NASの暗号化機能はボリュームベースです。ボリュームはシングルディスク、JBOD構成、あるいはRAIDアレイが使用できます。
- ディスクボリュームをNAS上に作成する際に、データを暗号化するかどうかを選択する必要があります。つまり、ディスクを作成した後には暗号化を実行できません。実行するには、ディスクボリュームを初期化する必要があります。ディスクボリュームを初期化すると、そのボリューム上の既存のデータはすべて消去されます。
- ディスクボリュームの暗号化を除去するには、初期化する必要があります。ディスクボリュームの暗号化を除去するには、ディスクボリュームを初期化し、すべてのデータを消去しなくてはなりません。
- 暗号化パスワードあるいはキーは安全に保管してください。パスワードを忘れたり、あるいは暗号化キーを紛失すると、データを取り戻すことができません!
- 始める前に、本書類を注意深く読み、説明に正しく従うようご注意ください。

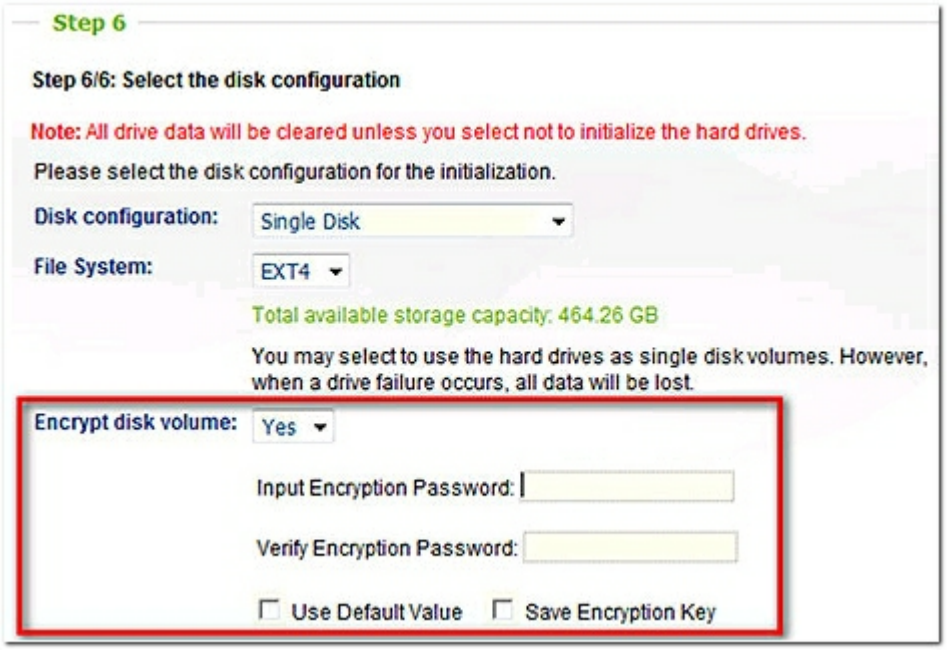
Turbo NAS上でディスクボリューム暗号化を起動する

NAS設置時にディスクボリュームを暗号化する

クイックインストールガイド (QIG) の説明に従い、ウェブベースのインターフェイスを使用してNASを初期化します。クイック構成のステップ 6 にて、"Encrypt disk volume" (ディスクボリュームを暗号化する) オプションで "Yes" (はい) を選択します。

クイックインストールガイド (QIG) の説明に従い、ウェブベースのインターフェイスを使用してNASを初期化します。クイック構成のステップ 6 にて、"Encrypt disk volume" (ディスクボリュームを暗号化する) オプションで "Yes" (はい) を選択します。

ディスクボリュームの暗号化を選択すると、暗号化設定が表示されます。



暗号化パスワードを入力します。このパスワードは暗号化されたボリュームのロックを解除する際に必要となります。暗号化パスワードは8-16文字以内で設定してください。スペース（ ）は使用できません。文字と数字を混合した長いパスワードを作成するようにしてください。

- デフォルト値を使用する:デフォルトの暗号化パスワード "admin" の使用を選択します。
- 暗号化キーの保存:暗号化キーをNAS上に保存するよう選択します。 (このオプションは後からの変更が可能です)
  - チェックを入れた場合: NASの起動時に、保存されたパスワードを使用して暗号化ディスクボリュームを自動的にロック解除します。
  - チェックを入れない場合: NASの起動時に、暗号化ディスクボリュームはロックされています。NASに管理者としてログインし、暗号化パスワードを入力してディスクボリュームのロックを解除する必要があります。

その後、次の手順に進んでNASの設置を完了します。

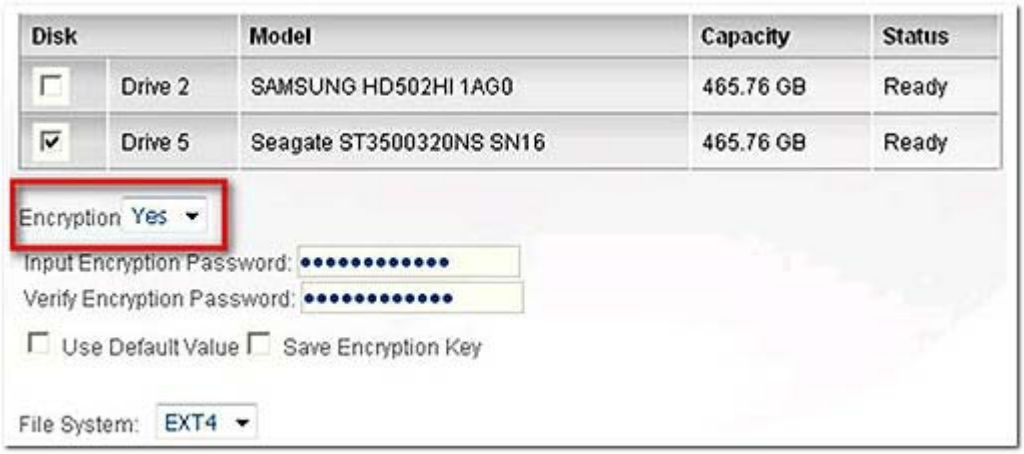
新規ハードドライブに新規暗号化ディスクボリュームを作成する

ご使用のNASが設置済みの場合に、新規ハードドライブをサーバに設置して新規暗号化ディスクボリュームを作成したい場合は、以下の手順に従ってください。

1. 新規ハードドライブをNASに設置します。
2. NASに管理者としてログインします。"Disc Management" (ディスク管理) > "Volume Management" (ボリューム管理) を開きます。
3. NASに管理者としてログインします。"Disc Management" (ディスク管理) > "Volume Management" (ボリューム管理) を開きます。

4. ディスクボリュームを作成するハードドライブを選択します。この例では、シングルドライブの作成を選択します。手順はRAID構成の場合も同様です。

5. "Encryption" (暗号化) オプションにて "Yes" (はい) を選択し、暗号化設定を入力します。



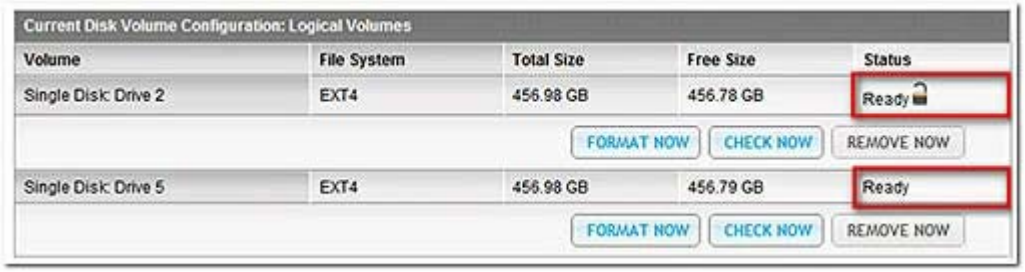
6. 続いて "CREATE" (作成) をクリックして、新規暗号化ボリュームを作成します。選択したドライブのすべてのデータは消去されますのでご注意ください! 暗号化ボリュームを作成する前にデータをバックアップしてください。

NAS上に暗号化ディスクボリュームが作成されました。

ディスクボリュームが暗号化されたことを確認する

ディスクボリュームが暗号化されていることを確認するには、まずNASに管理者としてログインします。続いて、"Disc Management"（ディスク管理）> "Volume Management"（ボリューム管理）を開きます。

ディスクボリュームのステータス欄に鍵のアイコンが表示されている場合、暗号化されていることを表します。
暗号化ボリュームのロックが解除されると、鍵が開いたアイコンになります。ステータス欄に鍵のアイコンがないディスクボリュームは暗号化されていません。

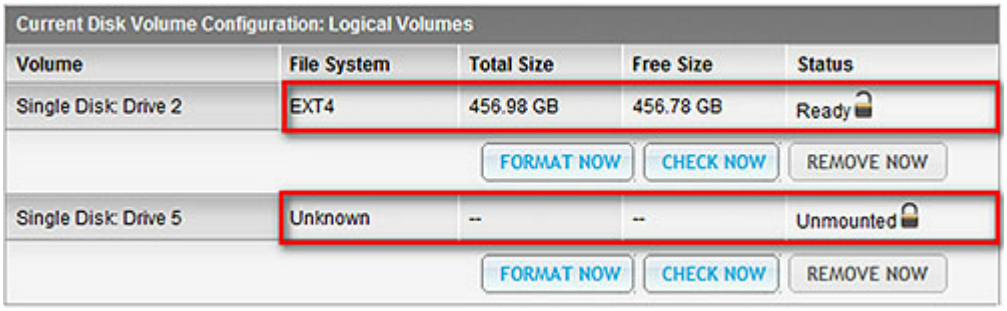


システム再起動時の暗号化ボリュームの動作

システム再起動時の暗号化ボリュームの動作

1つ目のボリューム（シングルディスクドライブ2）は "Save Encryption Key"（暗号化キーを保存）オプションを有効化して作成されています。
2つ目のボリューム（シングルディスクドライブ5）は "Save Encryption Key"（暗号化キーを保存）オプションを無効化して作成されています。

NASの再起動後、ボリュームステータスを確認します。1つ目のドライブのロックは解除されマウントされていますが、2つ目のドライブはロックされています。2つ目のディスクボリュームでは暗号化キーが保存されていないため、ユーザーは手動で暗号化パスワードを入力し、ロックを解除する必要があります。



- NAS上にキーを保管すると、ハードドライブのみが盗難された場合はデータを保護することができます。NAS全体が盗難された場合は、NASを再起動することでデータにアクセスが可能となるため、データ漏洩の危険性があります。
- NASに暗号化キーを保存しないよう選択した場合は、サーバが盗難された際にもデータ漏洩を防ぐことができます。唯一不都合となる点は、システム再起動のたびにディスクボリュームを手動でロック解除する必要があるということです。

暗号化キー管理:新規パスワード/暗号化キーの保存/暗号化キーのエクスポート

暗号化キー設定を管理するには、NASに管理者としてログインし、"Disk Management" (ディスク管理) > "Encrypted File System" (暗号化ファイルシステム) を開きます。

ロック解除されているディスクボリュームの"Action" (動作) 行にある"ENCRYPTION KEY MANAGEMENT" (暗号化キー管理) をクリックします。

以下の動作を実行することができます:

- 暗号化キーの変更
- NAS上に暗号化キーを保存
- 暗号化キーファイルのダウンロード

- 暗号化キーの変更:
  現在の暗号化パスワードを入力し、続いて新しいパスワードを入力します。(パスワードの変更後は、以前にエクスポートされたキーは無効となりますのでご注意ください。必要に応じて新しい暗号化キーをダウンロードする必要があります。その手順については以下をご覧ください。)
- 暗号化キーの保存:
  暗号化キーをNASに保存し、NASが再起動する際に暗号化ディスクボリュームを自動的にロック解除しマウントします。
- 暗号化キーファイルのダウンロード:
  暗号化パスワードを入力して暗号化キーファイルをダウンロードします。暗号化キーファイルをダウンロードすることで暗号化キーをファイルに保存することができます。ファイル自体も暗号化されており、実際のパスワードを知らない場合にもボリュームのロック解除が可能です。(下記の"ディスクボリュームを手動でロック解除する"をご覧ください) 暗号化キーファイルは安全な場所に保管してください!

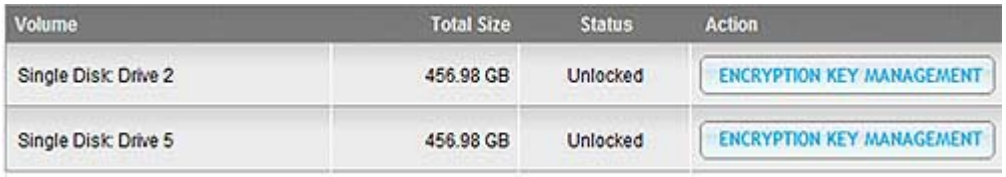
ディスクボリュームを手動でロック解除する

ボリュームをロック解除するには、NASに管理者としてログインします。続いて、"Disc Management" (ディスク管理) > "Encrypted File System" (暗号化ファイルシステム) を開きます。

暗号化ボリューム及びそのステータスが表示されます:ロック/ロック解除。

ボリュームをロック解除するには、暗号化パスワードを入力するか、あるいは前にエクスポートされた暗号化キーファイルを使用します。

暗号化パスワードあるいはキーファイルが正しい場合、ボリュームはロック解除され使用可能となります。



4.5 iSCSI

ポータル管理 127
ターゲット管理 140
拡張ACL 166
LUN バックアップ 170

4.5.1 ポータル管理

NASはサーバクラスタリングおよび仮想環境向けの内蔵iSCSIサービスをサポートしています。

iSCSIターゲットサービス

コンピュータとストレージデバイスの相互関係では、コンピュータはデバイスへの接続を開始するため イニシエータ（initiator）と呼ばれ、デバイス（target）はターゲットと呼ばれます。

NASはビルトインISCSIサービスをサポートします。この機能を使用するには、以下の手順に従ってください。

1. iSCSIイニシエータをコンピュータ（Windows PC、Mac、またはLinux）にインストールします。
2. iSCSIターゲットサービスをNAS上に有効にし、新しいiSCSIターゲットを作成します。
3. iSCSIイニシエータを実行し、iSCSIターゲット (NAS) に接続します。
4. ログイン完了後、iSCSIターゲット（ディスクボリューム）をフォーマットします。ディスクボリュームをご使用のコンピュータの仮想ドライブとしてNAS上で使用開始できます。

注: 同じiSCSIターゲットを2つの異なるクライアント（iSCSIイニシエータに同時に接続することは避けてください。データのクラッシュまたはディスク損傷の原因となる場合があります。

以下の説明は、3.3.0**以前の**バージョンのファームウェアを実行する非IntelベースのNASモデルと、3.2.0**以前の**バージョンのファームウェアを実行するIntelベースのNASモデルにのみ適用されます。NASモデルが一覧にない場合、http://www.qnap.com にアクセスして詳細をご確認ください。

IntelベースのNAS	TS-x39シリーズ、TS-x59シリーズ、TS-509、TS-809、TS-809 Pro、TS-809U-RP、SS-439 Pro、SS-839 Pro、TS-x59 Pro+、TS-879 Pro、TS-1079 Pro、TS-879U-RP、TS-EC879U-RP、TS-1279U-RP、TS-EC1279U-RP
非IntelベースのNAS	TS-109、TS-209、TS-409、TS-409U、TS-x10、TS-x12、TS-x19シリーズ

iSCSIターゲットとLUNをNAS上に作成するには、以下の手順に従ってください。

ロジカルユニット番号(LUN)は作成する各iSCSIターゲットに対して作成されます。最大4つのターゲットと4つのLUNを作成できます。

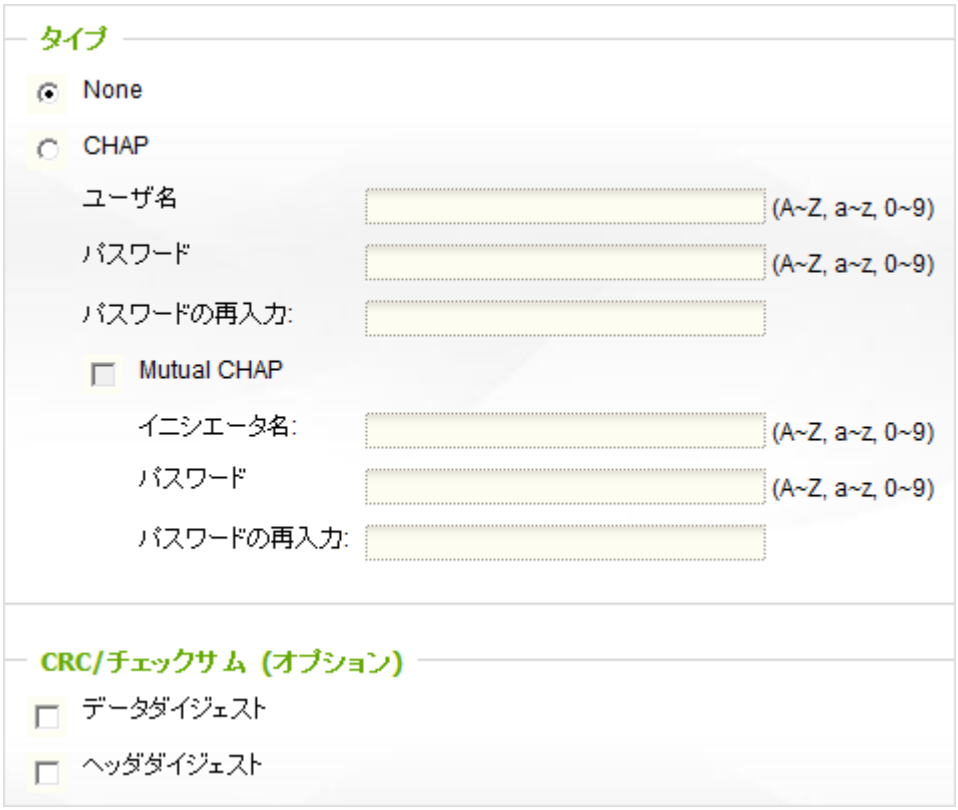
"iSCSI TARGET LIST" (iSCSIターゲットリスト)タブの下にある、"Create New iSCSI Target" (新規iSCSIターゲットの作成)をクリックします。

必要な情報を入力します。ターゲット名を指定します。iSCSIターゲットが作成されるボリューム、ターゲットのサイズ、またディスク領域を事前に割り当てるかどうかを指定します。

NASが公共ネットワークや信頼されないネットワークに接続される場合、CHAP認証設定を入力します (オプション。"CHAP"下にユーザー名とパスワード設定を入力した場合にのみ、iSCSIターゲットはイニシエータを認証します。つまり、イニシエータは、ユーザー名とパスワードを入力しないとターゲットに接続されません。

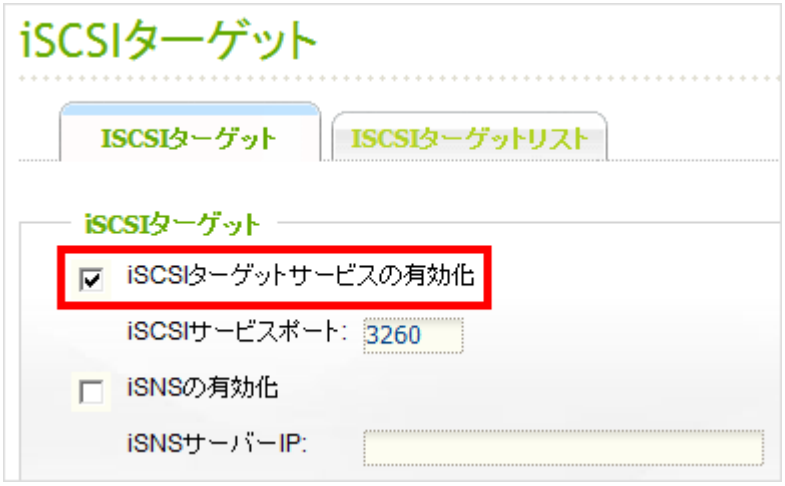
相互CHAP: このオプションを効化すると、iSCSIターゲットとイニシエータの間で二方向の認証が行われます。ターゲットははじめのユーザー名とパスワードのセットを使用してイニシエータを認証します。イニシエータは"Mutual CHAP" (相互CHAP)設定を使用してターゲットを認証します。

欄	ユーザー名制限	パスワード制限
CHAP認証を使用	• 効な文字は0-9, a-z, A-Zのみ • 最長: 256文字まで	• 効な文字は0-9, a-z, A-Zのみ • 最長: 12-16文字まで
相互CHAP	• 効な文字は0-9, a-z, A-Z, : (コロン), . (ドット), および - (ダッシュ) • 最長: 12-16文字まで	• 効な文字は0-9, a-z, A-Z, : (コロン), . (ドット), および - (ダッシュ) • 最長: 12-16文字まで



作成が完了すると、iSCSIターゲットは、iSCSIターゲットリストに表示されます。

"iSCSI TARGET"（iSCSIターゲット）タブにある"Enable iSCSI Target Service" (iSCSIターゲットサービスの有効化)オプションを選択して、"Apply"（適用）をクリックします。iSCSIターゲットの準備が完了しました。



クイック構成ウィザード

以下の説明は3.3.0**以降の**バージョンのファームウェアを実行する非IntelベースのNASモデルと、3.2.0**以降の**バージョンのファームウェアを実行するIntelベースのNASモデルにのみ適用されます。

最大256のiSCSIターゲットとLUNを作成できます。例えば、NASに100のターゲットを作成する場合、作成できるLUNの最大数は156になります。複数のLUNを各ターゲット用に作成できます。ただし、NASによってサポートされるiSCSIターゲットへの最大同時接続数はご使用のネットワークインフラとアプリケーションの性能によって異なります。同時接続が多すぎると、NASのパフォーマンスが低下する場合があります。

NASにおいてiSCSIターゲットサービスを構成するには以下の手順に従ってください。

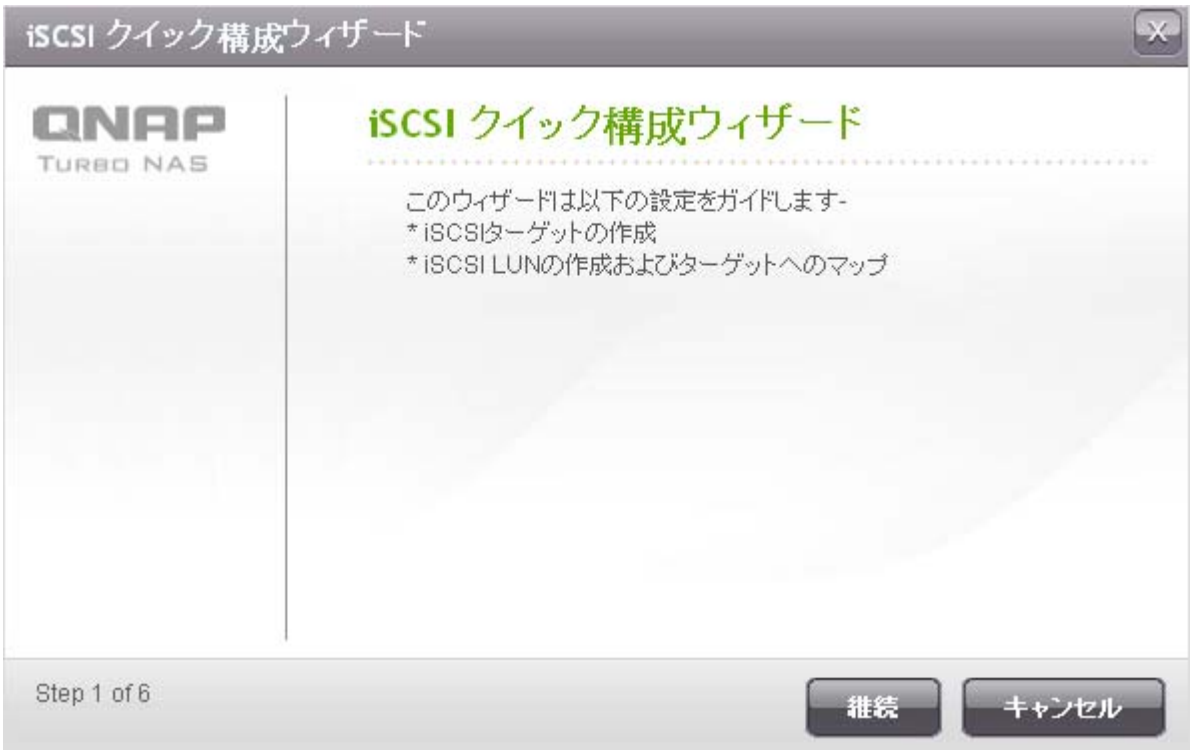
1. "Portal Management"（ポータル管理）表をクリックしiSCSIターゲットサービスを効化します。設定を適用します。

2. サービスが効の状態で、"Target Management"（ターゲット管理）タブを開き、iSCSIターゲットをNAS上で作成します。iSCSIターゲットを初めて作成する場合、Quick Installation Wizard（クイックインスールウィザード）が表示され、iSCSI ターゲットまた/あるいは LUN（論理ユニット番号）の作成を求めます。「OK」をクリックします。

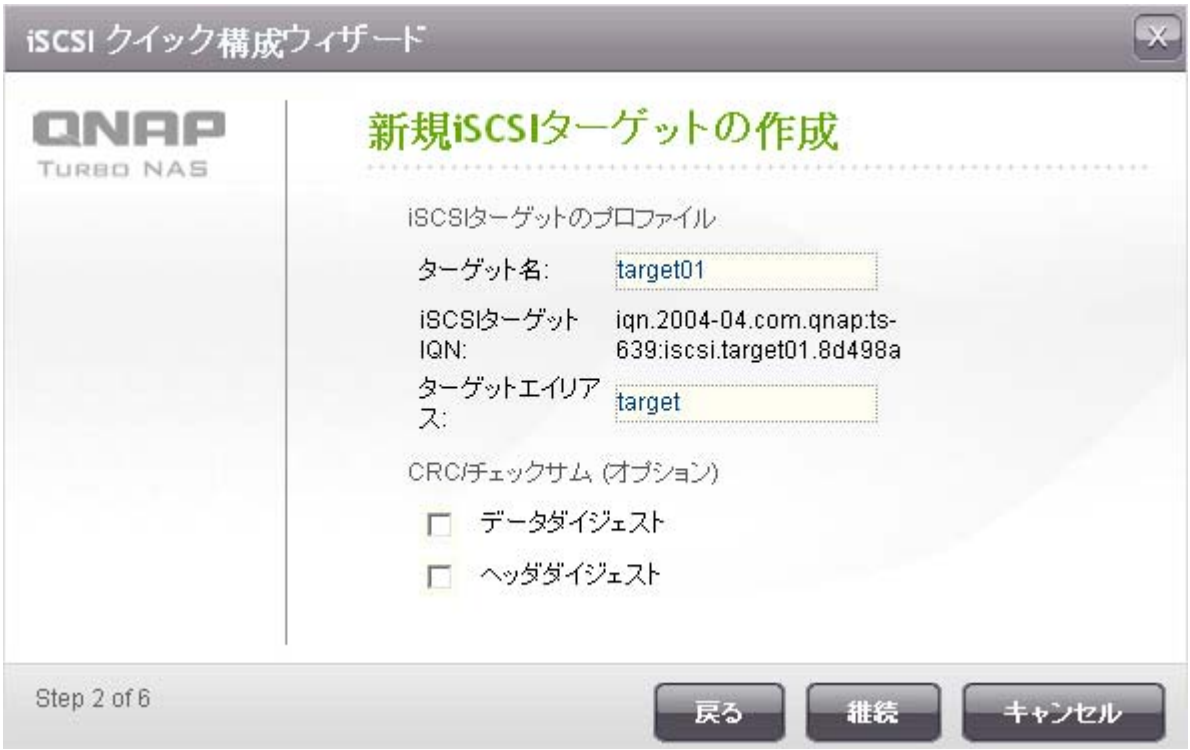
3. ウィザードが表示された際に、マップされた LUN と iSCSI ターゲット、iSCSI ターゲットのみ、あるいは iSCSI LUN のみの作成を選択します。"Next"（次へ）をクリックします。

4. マップされた LUNとiSCSI ターゲットを作成します:

"Next"(次へ)をクリックします。



5. ターゲット名及びターゲットエイリアスを入力します。"Data Digest"（データダイジェスト）また/あるいは"Header Digest"（ヘッダーダイジェスト）のオプションにチェックを入れます。(オプション) これらは、iSCSIイニシエータがiSCSIターゲットに接続しようとする際に確認をおこなうパラメータです。



6. CHAP認証設定に入ります。ユーザー名及びパスワード設定を"Use CHAP authentication" (CHAP認証を使用する) 下でのみ入力すると、iSCSI ターゲットのみがイニシエータを認証することになります。つまり、イニシエータはターゲットにアクセスするためにユーザー名及びパスワード設定をここで入力する必要があります。

相互CHAP: このオプションを効化すると、iSCSI ターゲットとイニシエータの間で二方向の認証が行われます。ターゲットははじめのユーザー名とパスワードのセットを使用してイニシエータを認証します。イニシエータは"Mutual CHAP" (相互CHAP) 設定を使用してターゲットを認証します。

欄	ユーザー名制限	パスワード制限
CHAP認証を使用	• 効な文字は0-9, a-z, A-Zのみ • 最長: 256文字まで	• 効な文字は0-9, a-z, A-Zのみ • 最長: 12-16文字まで
相互CHAP	• 効な文字は0-9, a-z, A-Z, : (コロン), . (ドット), および - (ダッシュ) • 最長: 12-16文字まで	• 効な文字は0-9, a-z, A-Z, : (コロン), . (ドット), および - (ダッシュ) • 最長: 12-16文字まで

7. iSCSI LUNを作成します

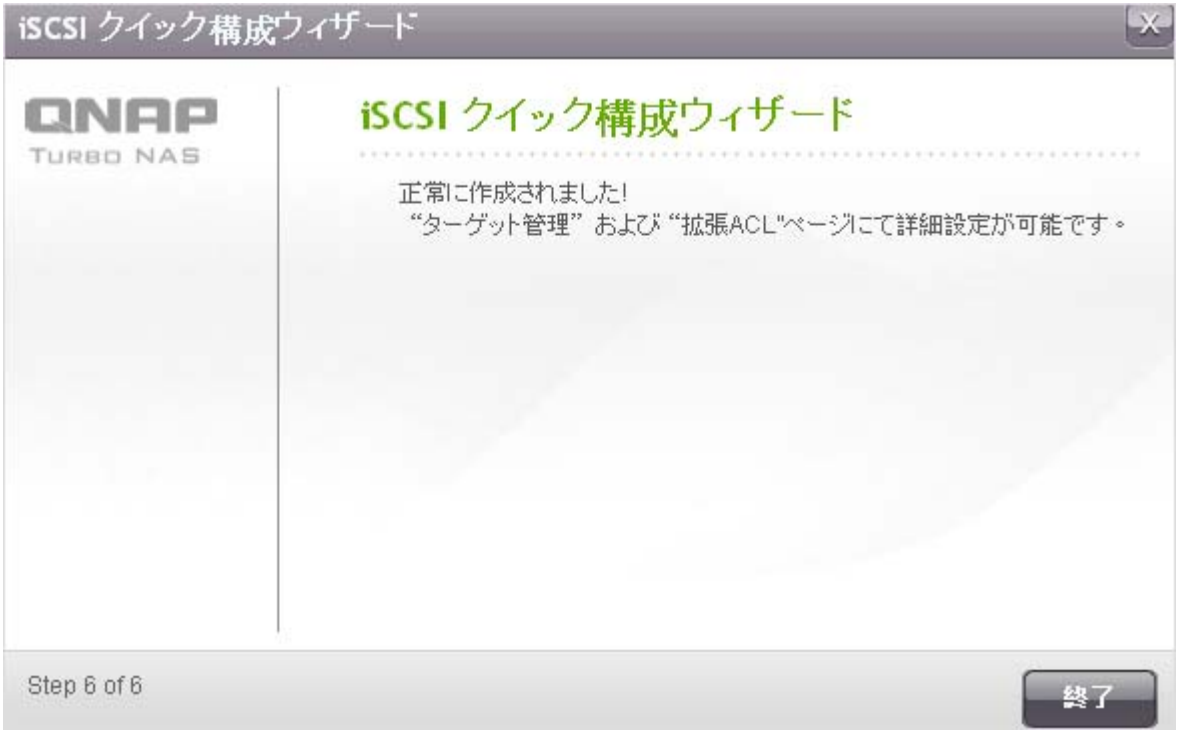
iSCSI LUNはiSCSIターゲットにマップされた論理ボリュームです。以下のうちいずれかのモードを選択してディスク容量をLUNに配分します:

- Thin Provisioning: このオプションを選択すると、ディスク容量を柔軟に配分することができます。NAS上で使用できる現在のストレージ容量に関わらず、ディスク容量をターゲットにいつでも配分することができます。NASのストレージ容量は、オンラインRAID容量拡張により拡大できるため、割り当て超過も可能です。
- 即時配分: このオプションを選択すると、ディスク容量をLUNに即時配分することができます。このオプションはLUNに対してディスク容量割当を保証するものですが、LUNの作成に時間がかかるようになる場合があります。

LUN名を入力し、LUNの場所を指定します。(NAS上のディスクボリューム) LUN 用の容量を入力します。"Next"(次へ)をクリックします。

8. 設定を確定し、"Next"（次へ）をクリックします。

9. ターゲットとLUNが作成された後に、"Finish"（終了）をクリックします。



10. ターゲットとLUNが"Target Management"（ターゲット管理）タブ内の一覧に表示されます。

4.5.2 ターゲット管理

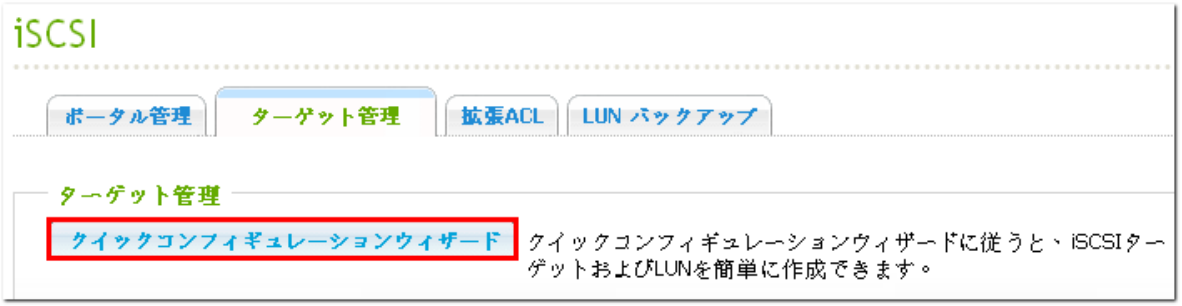
---

iSCSIターゲットの作成

以下の説明は3.3.0以降のバージョンのファームウェアを実行する非IntelベースのNASモデルと、3.2.0以降のバージョンのファームウェアを実行するIntelベースのNASモデルにのみ適用されます。

単独のiSCSIターゲットに複数のLUNを作成することができます。iSCSIターゲットにさらにLUNを作成するには以下の手順に従ってください。

1. "Target Management"（ターゲット管理）から"Quick Configuration Wizard"（クイック構成ウィザード）をクリックします。



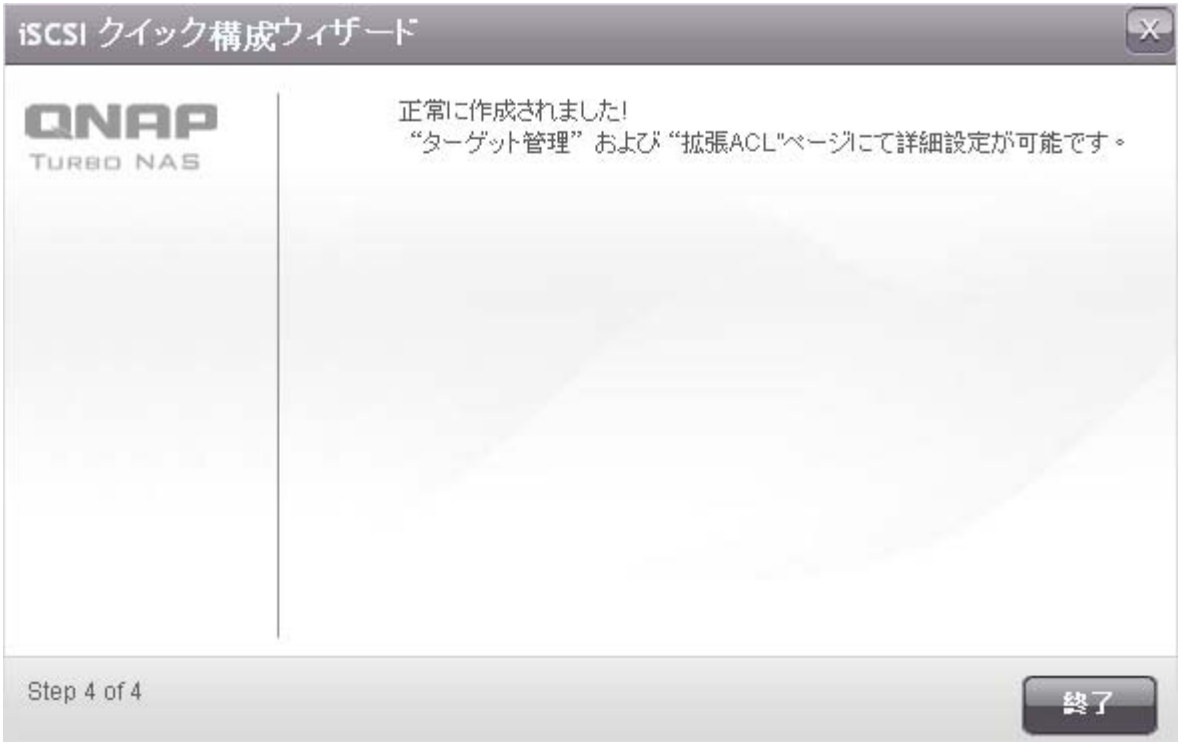
2. "iSCSI LUN only"（iSCSI LUNのみ）を選択し、"Next"（次へ）をクリックします。

3. LUN配分方法を選択します。LUN名を入力し、LUNディレクトリを選択し、LUN用の容量を指定します。"Next"（次へ)をクリックします。.

4. LUNをマップするターゲットを選択します。LUNを今はマップしないよう選択することも可能です。

5. 設定を確定し、"Next" (次へ)をクリックします。

6. LUNが作成された後に、"Finish"（終了）をクリックしてウィザードを終了します。



7. 作成されたLUNはいつでも iSCSI ターゲットにマップ、あるいは iSCSI ターゲットからアンマップすることができます。また、1つのターゲットからLUNをアンマップして他のターゲットにマップすることも可能です。

項目	ステータス	説明
iSCSI ターゲット	準備完了	iSCSIターゲットは準備完了していますが、イニシエータは接続されていません。
	接続済み	iSCSIターゲットはイニシエータにより接続されました。
	切断	iSCSIターゲットは切断されました。
	オフライン	iSCSIターゲットは無効化され、イニシエータにより接続することができません。
LUN	効化	LUNは接続に対し効で、認証されたイニシエータから見ることができます。
	無効化	LUNは無効であり、イニシエータからは見えません。

ボタン	説明
	準備完了あるいは接続済みのターゲットを非アクティブにします。イニシエータによる接続は切断されますのでご注意ください。
	オフラインのターゲットをアクティブ化します。
	以下のターゲット設定を更します: ターゲットエイリアス、CHAP情報、チェックサム設定。 以下のLUN設定を更します: LUN配分、名前、ディスクボリュームディレクトリなど。
	iSCSIターゲットを削除します。すべての接続が切断されます。
	LUNを無効化します。すべての接続が切断されます。
	LUNを効化します。
	LUNをターゲットからアンマップします。LUNのアンマップの前にLUNを無効化するようご注意ください。このボタンをクリックすると、LUNは「Un-Mapped iSCSI LUN List」 (アンマップ済みiSCSI LUN 一覧) に移動されます。
	LUNをiSCSIターゲットにマップします。"Un-Mapped iSCSI LUN List" (アンマップ済みiSCSI LUN一覧) 上でのみこのオプションを使用できます。
	iSCSIターゲットの接続状況を表示します。

LUNのマッピングを切り替える

以下の説明は3.3.0以降のバージョンのファームウェアを実行する非IntelベースのNASモデルと、3.2.0以降のバージョンのファームウェアを実行するIntelベースのNASモデルにのみ適用されます。

LUNのマッピングを切り替えるには、以下の手順に従ってください。

1. iSCSI ターゲットからアンマップするLUNを選択し、 （無効化）をクリックします。

2. 続いて、 をクリックしてLUNをアンマップします。"Un-Mapped iSCSI LUN List"（アンマップ済みiSCSI LUN 一覧）にLUNが表示されます。 をクリックしてLUNを他のターゲットにマップします。

3. LUNをマップするターゲットを選択し、"Apply"（適用）をクリックします。

4. LUNをターゲットにマップします。

iSCSIターゲットおよびLUNをNAS上に作成すると、ご使用のコンピュータ（Windows PC, Mac, Linux）にインストールされたiSCSI initiator を使用してiSCSIターゲットおよびLUNに接続し、ディスクボリュームをコンピュータの仮想ドライブとして使用することができます。

iSCSI LUNの容量の拡張

NAS は、iSCSI LUNの容量の拡張をサポートしています。それを実施するには、次のステップに従います。

1. 「iSCSI」>「Target Management（ターゲット管理）」のiSCSIターゲットリスト上でiSCSI LUNを指定します。 をクリックします。

2. スライドバーを使って、LUNの容量を指定するか、フィールド内に容量を入力します。LUNの容量は最大限界値まで何回でも増やすことはできますが、減らすことはできないことに注意してください。

LUNのアロケーションタイプ	LUNの最大容量
シンプロビジョニング	32テラバイト
即時配分	ディスクボリューム上の空き容量

3. 「Apply（適用）」をクリックして、設定を保存します。

注：容量を増やす前に、NAS上のiSCSI LUNをiSCSIターゲットにマッピングする必要があります。

4.5.2.1 WindowsのMicrosoft iSCSIイニシエータを使用したNASへの接続

---

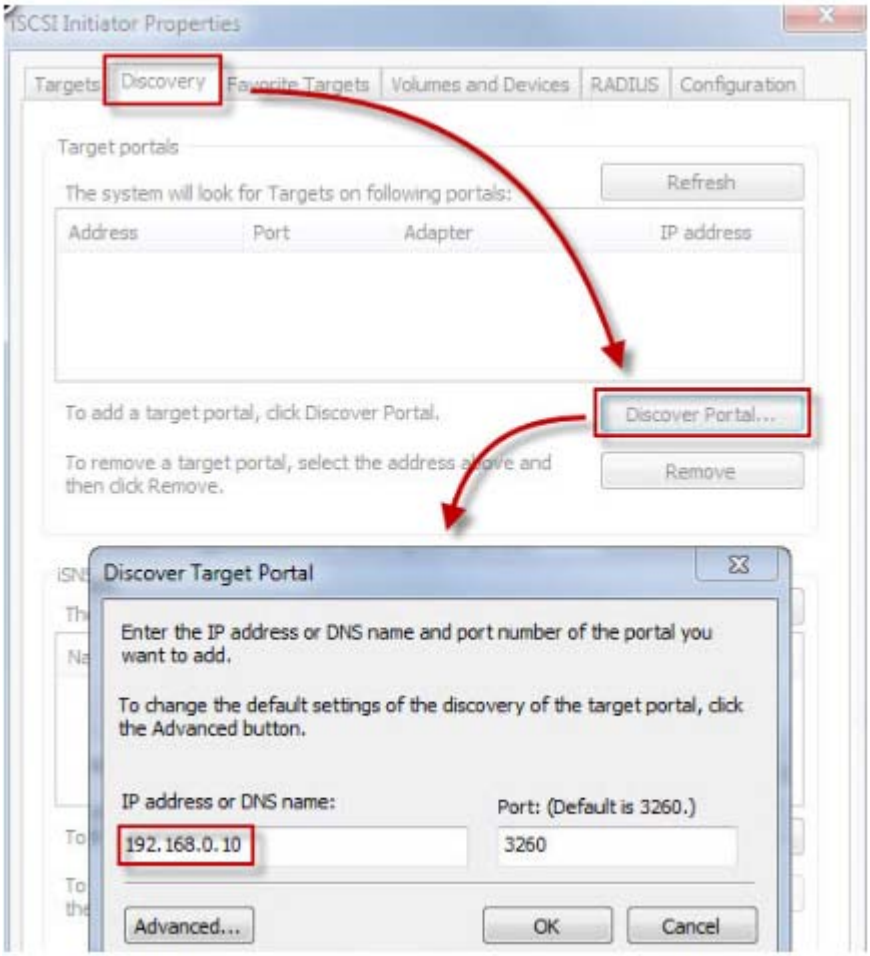
iSCSIターゲットサービスの使用を開始する前に、NAS上のLUNを使用してiSCSIターゲットを作成し、ご使用のOSに適した正しいiSCSIイニシエータをインストールしておく必要があります。

WindowsのiSCSIイニシエータ

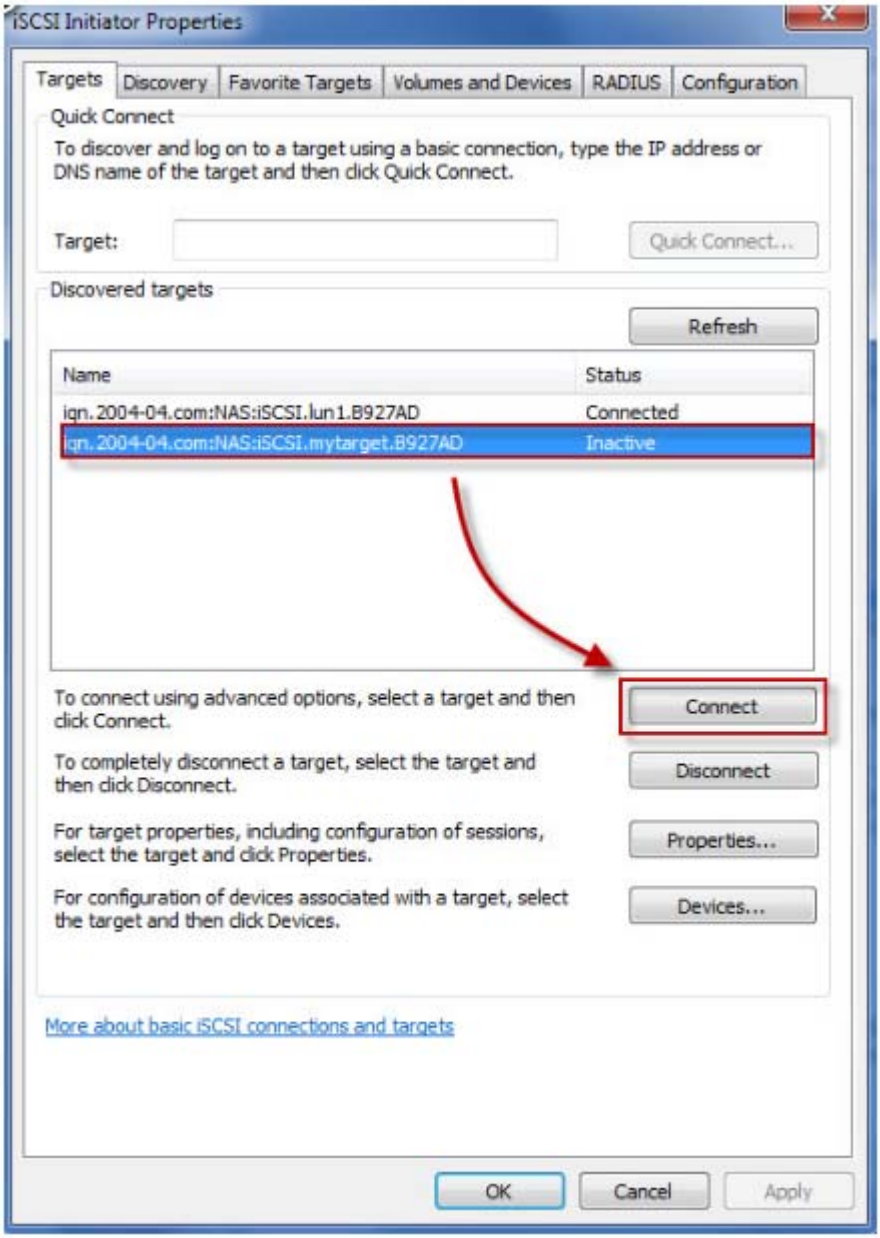
Microsoft iSCSI Software Initiator v2.07はWindows OS 2003、XP、および2000の公式アプリケーションで、ネットワーク上で外部iSCSIストレージアレイの実装を可能にします Windows VistaまたはWindows Server 2008には、Microsoft iSCSI Software Initiatorが含まれています。詳細およびダウンロードの場所については、以下のリンクからアクセスしてください。

http://www.microsoft.com/downloads/details.aspx?familyid=12cb3c1a-15d6-4585-b385-befd1319f825&displaylang=en

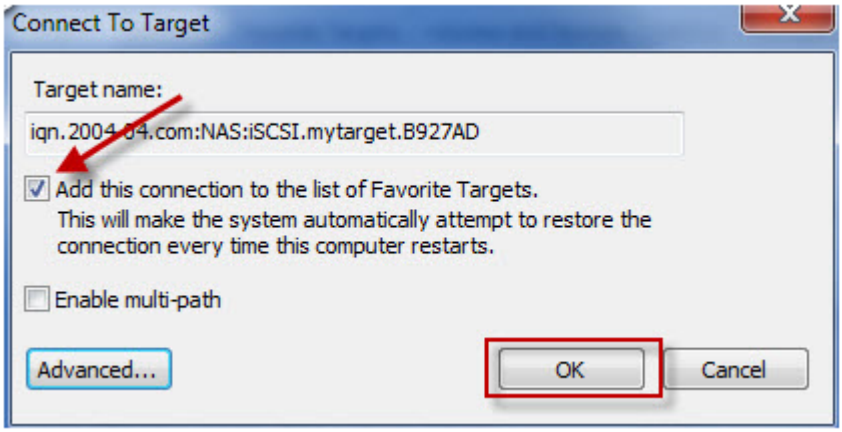
"Control Panel"（コントロールパネル） > "Administrative Tools"（管理ツール）からiSCSIイニシエータを開始します。"Discovery"（探索）タブ下の "Add Portal"（ポータルを追加）をクリックします。NAS IPおよびiSCSIサービスのためのポート番号を入力します。



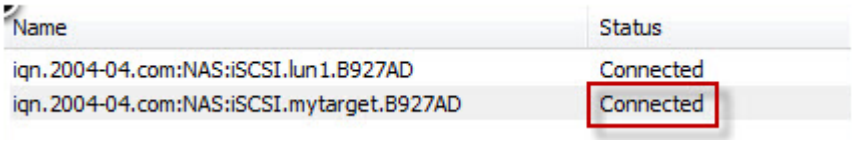
使用可能なiSCSIターゲットおよびそのステータスは"Targets"（ターゲット）タブ下にて表示されます。 接続を希望するターゲットを選択し、"Log on"（ログオン）をクリックします。



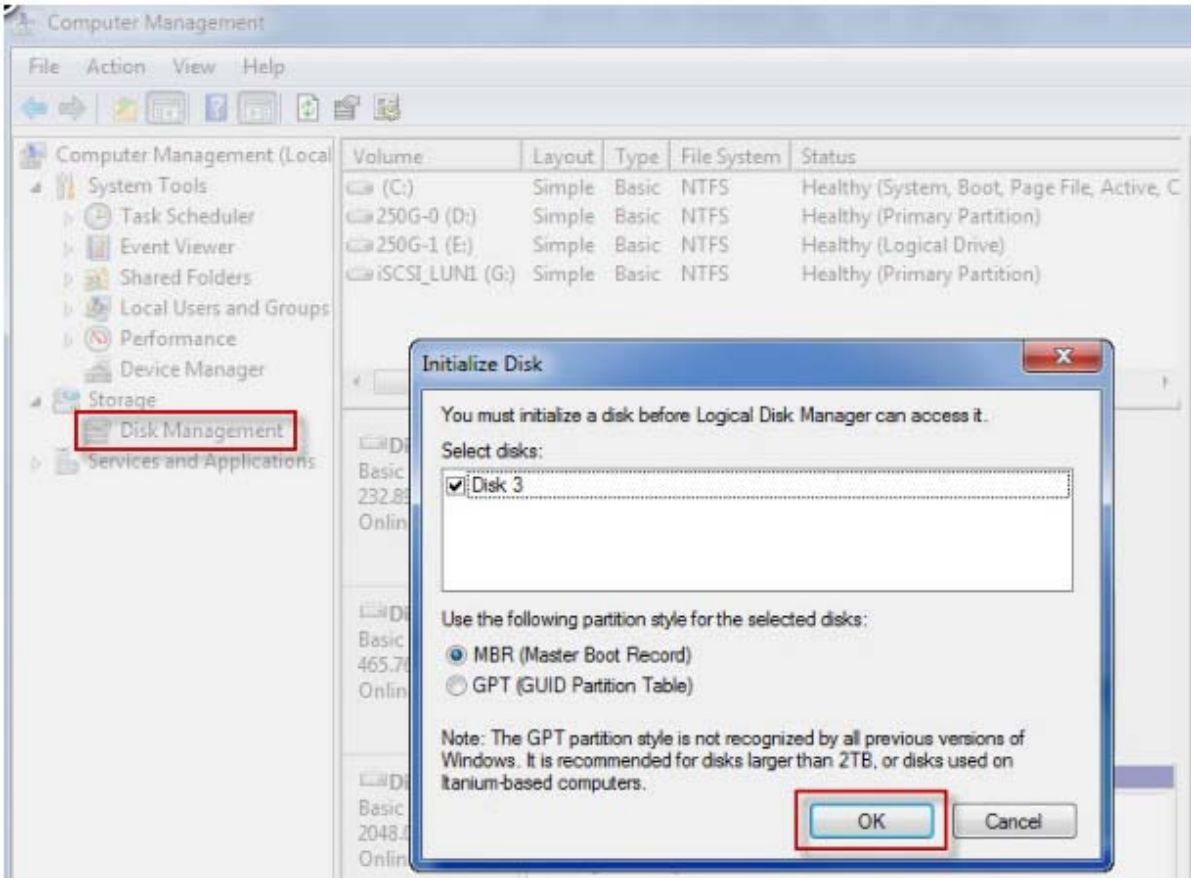
認証を構成してある場合は"Advanced"（詳細）をクリックすると口グオン情報を特定することができます。構成を行っていない場合は"OK"をクリックして続行します。



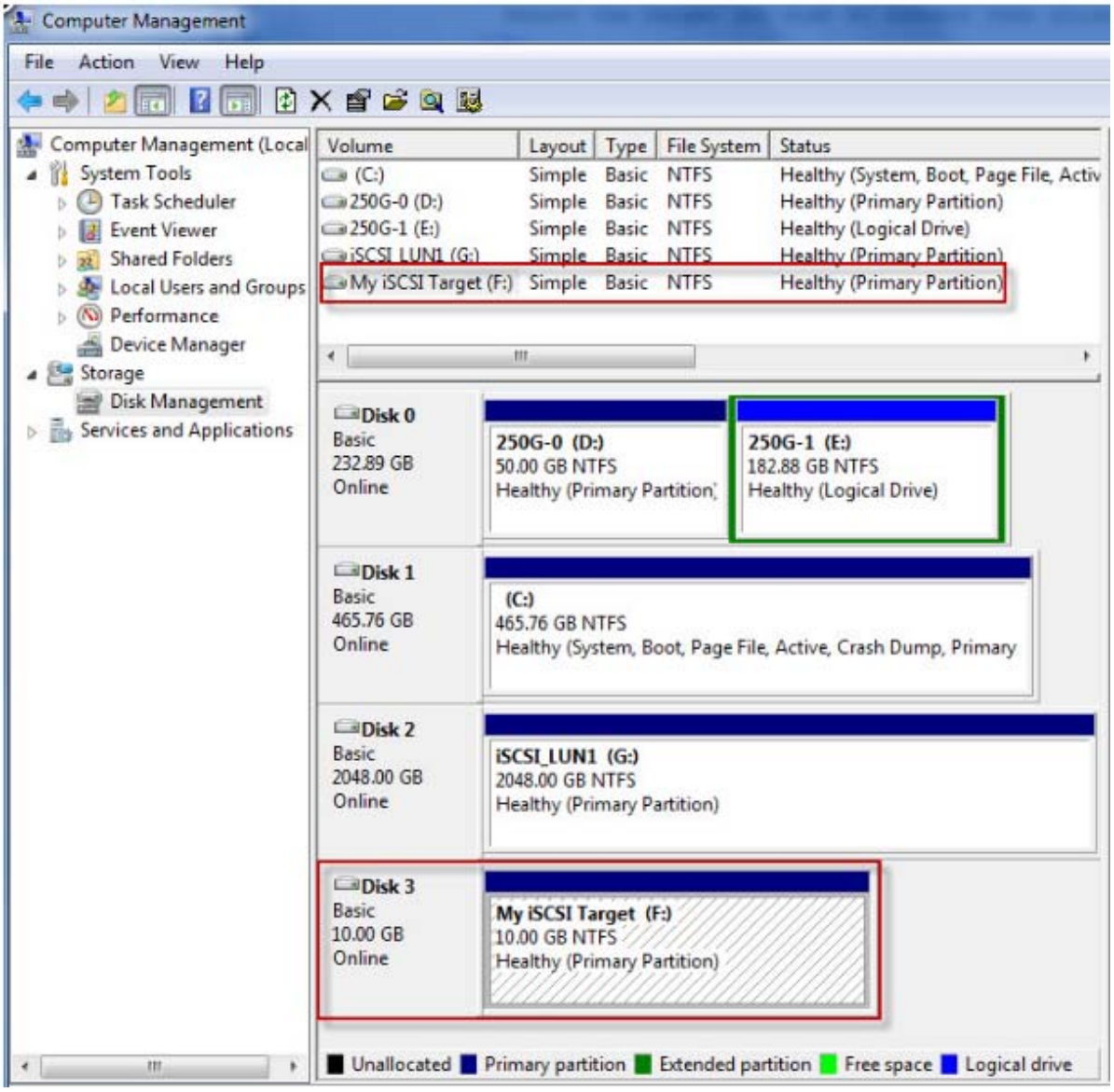
問題なく口グオンすると、ターゲットのステータスは "Connected"（接続済み）となります。



Windowsは接続されたターゲットを検出し、追加された新規ハードドライブは使用前に初期化とフォーマットが必要であると認識します。右クリックして "My Computer"（マイコンピュータ）> "Manage"（管理）と移動し、"Computer Management"（コンピュータ管理）ウィンドウを開きます。"Disk Management"（ディスク管理）に進むと、ウィンドウが自動的にポップアップし、新たに検出されたハードドライブを初期化するかどうか選択を求めます。"OK"をクリックし、新規ディスクを追加する際と同様にこのドライブをフォーマットします。



ディスク初期化とフォーマットが済んだら、新しいドライブがPCに接続されます。PCとターボステーションとが同一のLANに接続されていることを確認してください。



4.5.2.2 Mac OSのXtend SAN iSCSIイニシエータを使用したNASへの接続

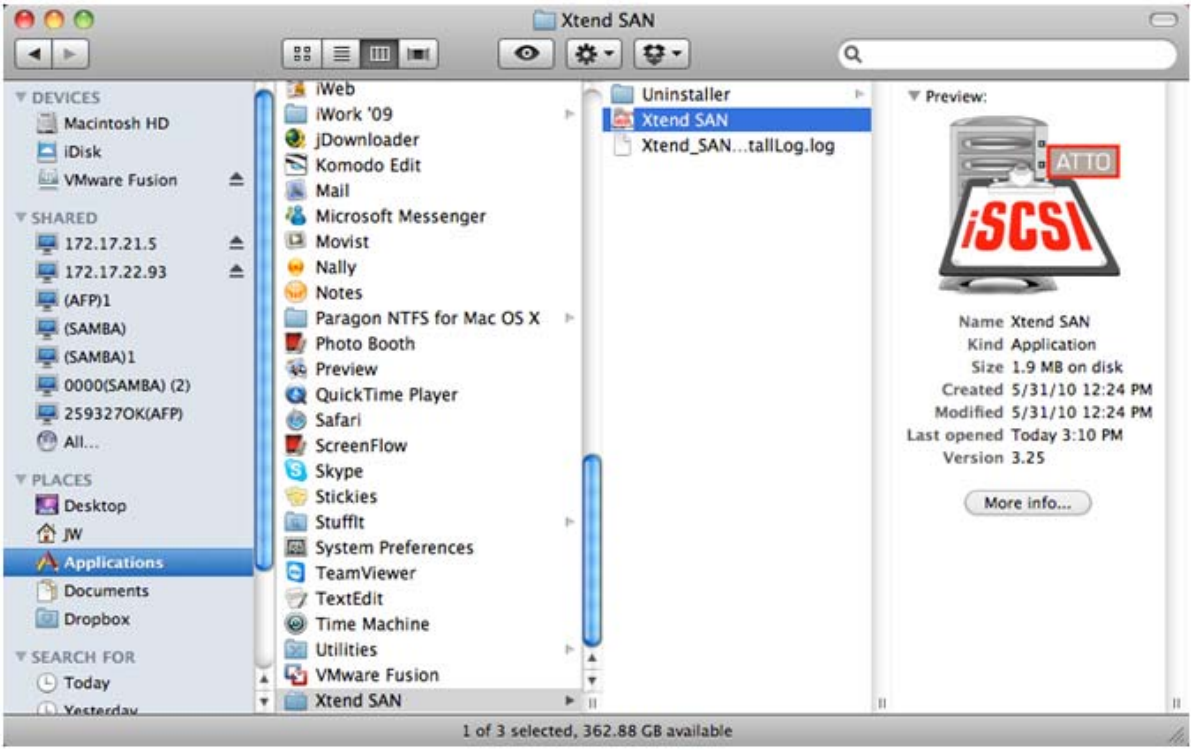
このセクションでは、Mac OSのXtend SAN iSCSIイニシエータを使用してiSCSIターゲット(QNAP NAS)を追加パーティションとして追加する方法をご紹介します。iSCSIターゲットサービスの使用を始める前に、NAS上のLUNを使用してiSCSIターゲットを作成し、ご使用のOSに適した正しいiSCSIイニシエータをインストールしておく必要があります。

Xtend SAN iSCSI イニシエータについて

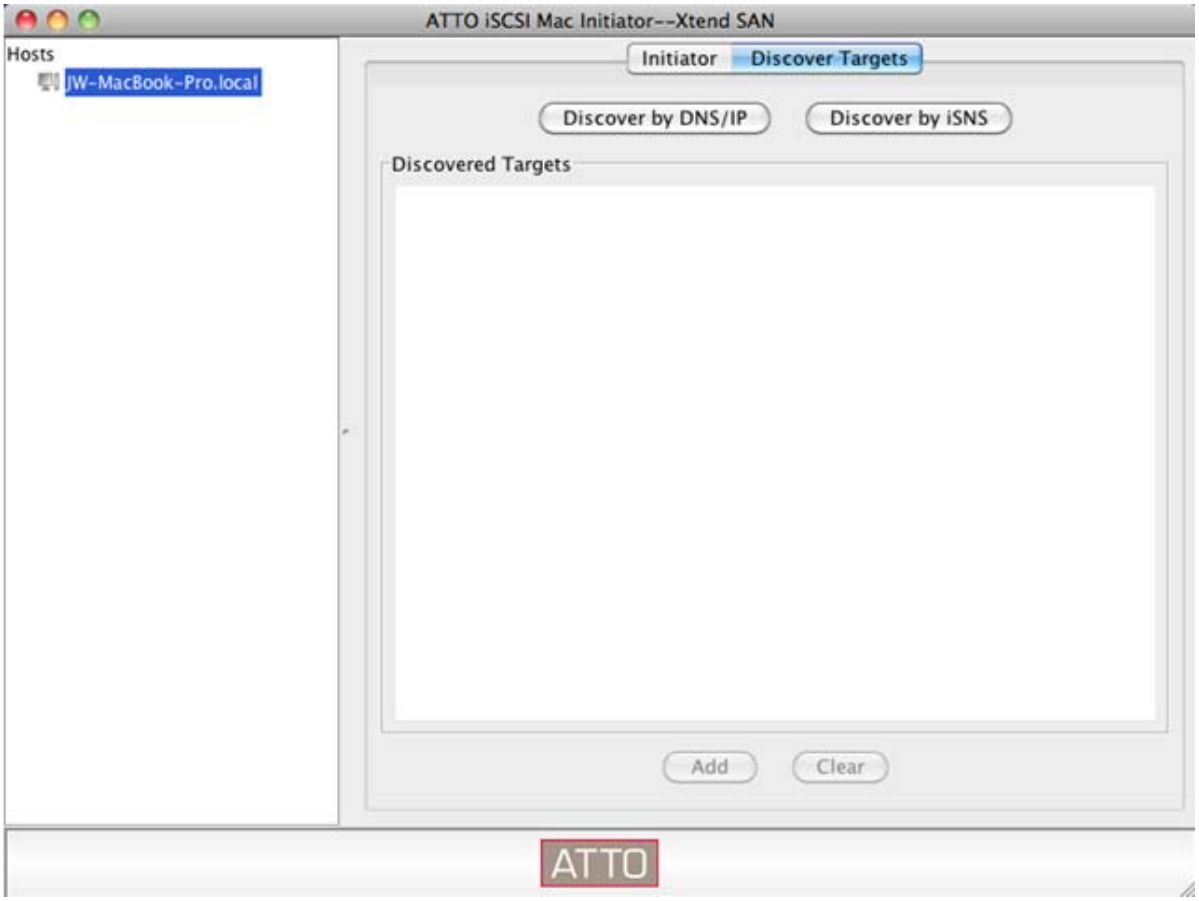
MAC OS X向けATTOのXtend SAN iSCSIイニシエータにより、Macユーザーはi SCSIを使用しその利点を活用することができます。Mac OS X 10.4.x to 10.6.xと互換しています。

詳しくは、こちらのページをご覧ください: http://www.attotech.com/products/product.php?sku=INIT-MAC0-001

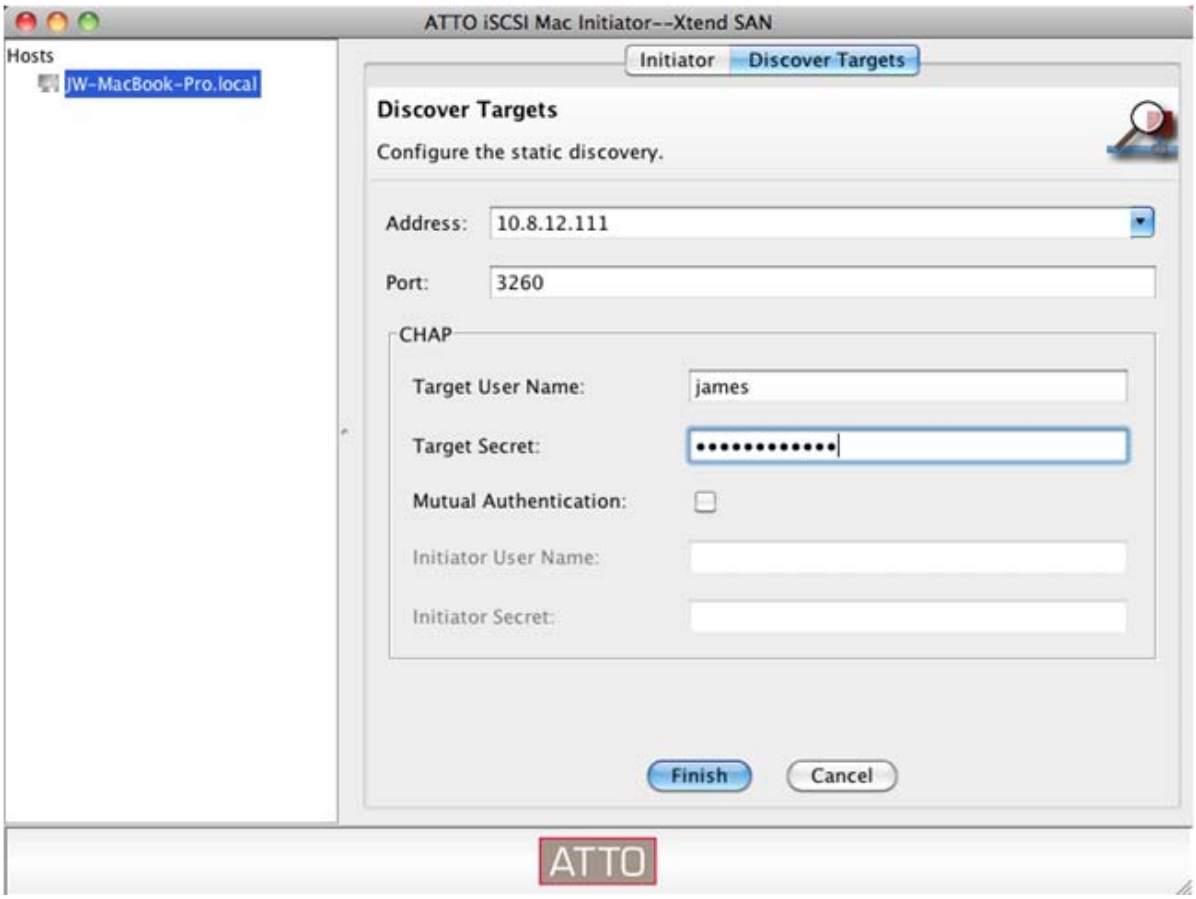
Xtend SAN iSCSIイニシエータは、インストール後は "Applications" (アプリケーション) から表示することができます。



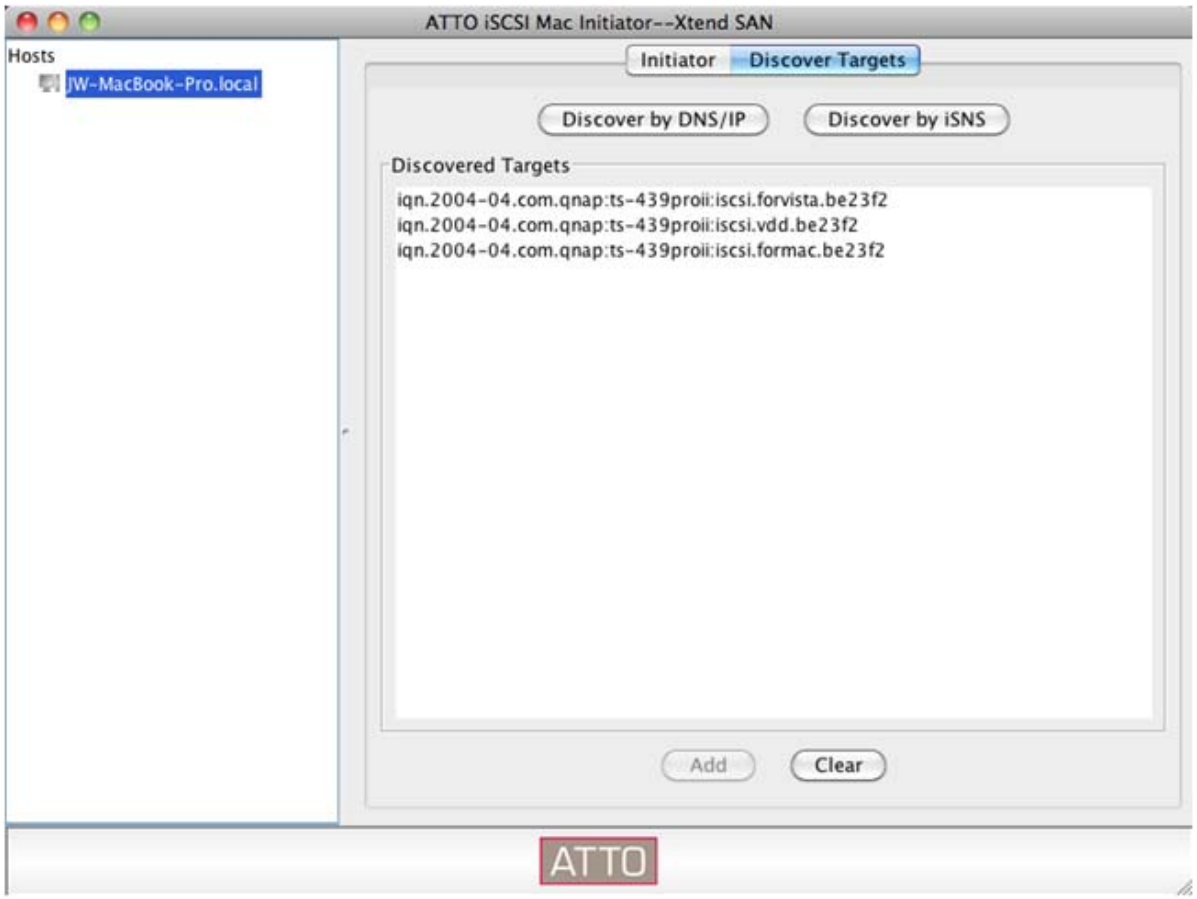
"Discover Targets" (ターゲットの検出) タブをクリックすると、ネットワークトポロジーに応じて"Discover by DNS/IP" (DNS/IPにより検出) あるいは "Discover by iSNS" (iSNSにより検出) のどちらかを選択することができます。この例では、IPアドレスを使用してiSCSIターゲットを検出します。



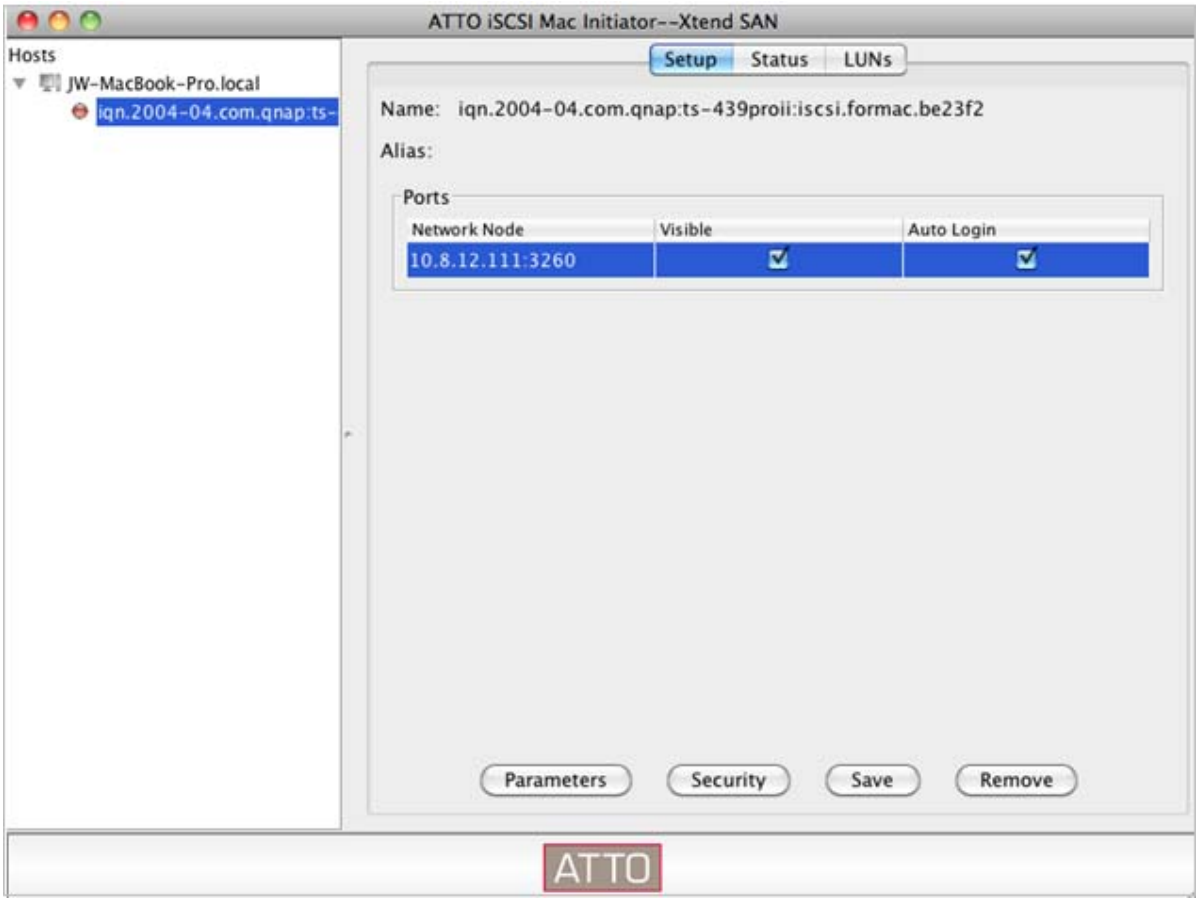
画面の指示に従い、サーバアドレス、iSCSIターゲットポート番号 (デフォルト:3260)、CHAP情報(該当する場合)を入力します。全てのデータが正しく入力された後、"Finish" (終了) をクリックしてターゲット一覧を取得します。



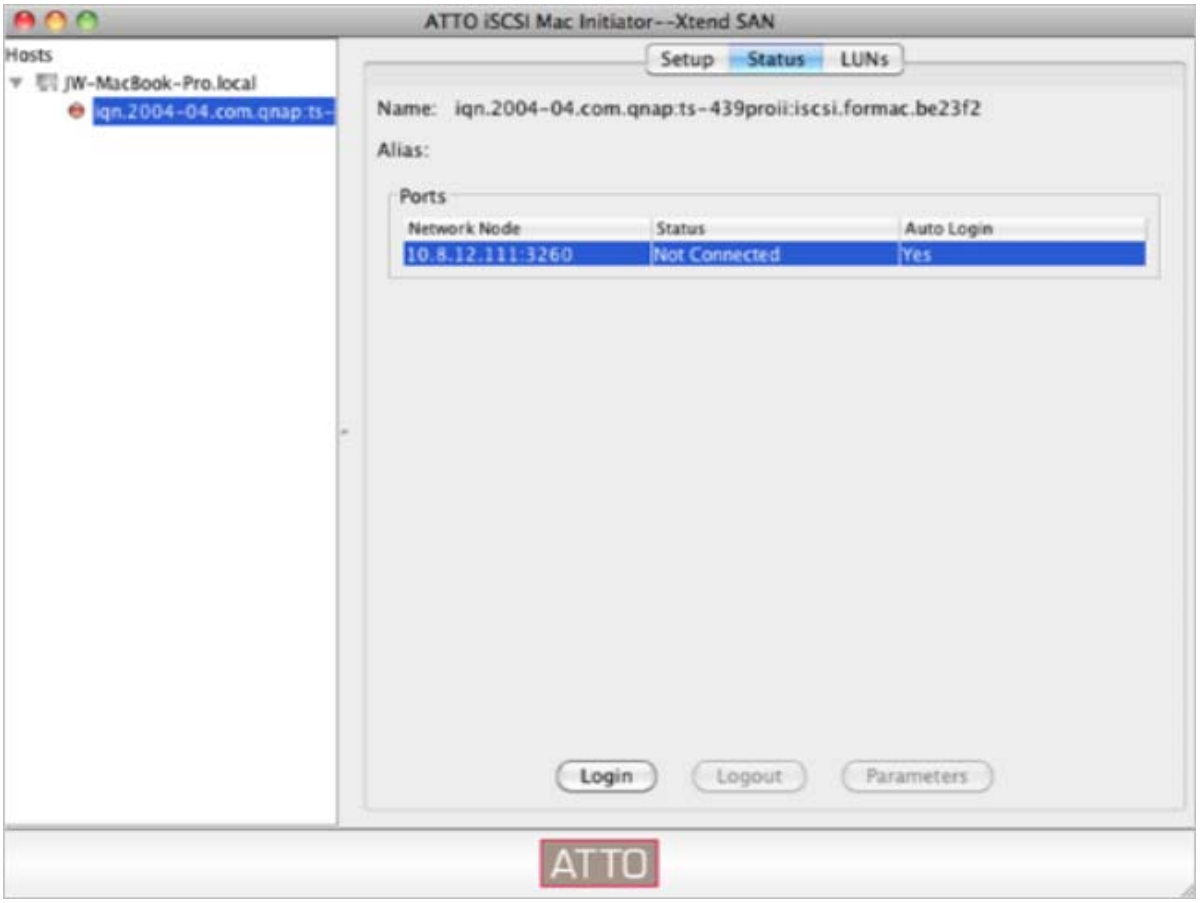
NASサーバにおいて使用可能なiSCSIターゲットが全て表示されます。接続するターゲットを選択し、"Add" (追加) をクリックします。



選択したiSCSIターゲットの接続プロパティは、"Setup" (セットアップ) タブにて構成することができます。



"Status" (ステータス) タブをクリックして接続するターゲットを選択します。"Login" (ログイン)をクリックして続行します。



iSCSIターゲットに初めてログオンするとき、ディスクが初期化されていないことを指摘するポップアップメッセージが表示されます。"Initialize..."（初期化）をクリックしてディスクをフォーマットします。"Disk Utilities"（ディスクユーティリティ）アプリケーションを開いて、初期化を実行することもできます。

これで、Macの外部ドライブとしてiSCSIを使用できるようになりました。

4.5.2.3 Ubuntu LinuxのOpen-iSCSIイニシエータを使用して接続する

ここでは、UbuntuのLinux Open-iSCSIイニシエータを使用してiSCSIターゲット(QNAP NAS)を追加パーティションとして追加する方法をご紹介します。iSCSIターゲットサービスの使用を始める前に、NAS上のLUNを使用してiSCSIターゲットを作成し、ご使用のOSに適した正しいiSCSIイニシエータをインストールしておく必要があります。

LinuxのOpen-iSCSIイニシエータについて

LinuxのOpen-iSCSIイニシエータはUbuntu 8.04 LTS以降の組み込みパッケージです。シェルプロンプトで2、3のコマンドを入力するだけで、iSCSIボリュームに接続することができます。Ubuntuに関する詳細は、http://www.ubuntu.com/ でご覧いただけます。Open-iSCSIの詳細とダウンロード場所については、 http://www.open-iscsi.org/ を参照してください。

始める前に

Open-iSCSIパッケージをインストールします。パッケージはLinux Open-iSCSIイニシエータしても知られています。

```
# sudo apt-get install open-iscsi
```

以下のステップに従い、LinuxのOpen-iSCSIイニシエータでiSCSIターゲット(QNAP NAS)に接続します。node.session.auth.username & node.session.auth.password などのCHAPログイン情報に対して、iscsid.confを更する必要があります。

```
# vi /etc/iscsi/iscsid.conf
```

ファイルを保存して終了し、open- iscsiサービスを再起動します。

```
# /etc/init.d/open-iscsi restart
```

デフォルトポートが3260である「10.8.12.31」などの特定ホスト(この例では、QNAP NAS)で iSCSIターゲットを見つけます。

```
# iscsiadm -m discovery -t sendtargets -p 10.8.12.31:3260
```

接続する使用可能なiSCSIノードにチェックマークを付けます。

```
# iscsiadm -m node
```

** サービスが次のコマンドで実行されるとき、接続を望まないノードを削除することができます。

```
# iscsiadm -m node --op delete --targetname THE_TARGET_IQN
```

open-iscsiを再起動して、使用可能なすべてのノードにログインします。

```
# /etc/init.d/open-iscsi restart
```

以下のようなログインメッセージが表示されます。

Login session [iface: default, target: iqn.2004-04.com:NAS:iSCSI.ForUbuntu.B9281B, portal: 10.8.12.31,3260]

[OK]

dmesgでデバイスステータスをチェックします。

```
# dmesg | tail
```

次のコマンドを入力してパーティションを作成します。/dev/sdbはデバイス名です。

```
# fdisk /dev/sdb
```

パーティションをフォーマットします。

```
# mkfs.ext3 /dev/sdb1
```

ファイルシステムをマウントします。

```
# mkdir /mnt/iscsi
```

```
# mount /dev/sdb1 /mnt/iscsi/
```

次のコマンドを使用してI/O速度をテストすることができます。

```
# hdparm -tT /dev/sdb1
```

以下は、"iscsiadm"関連のコマンドの一部です。

ホストでターゲットを見つけます。

```
# iscsiadm -m discovery --type sendtargets --portal HOST_IP
```

ターゲットにログインします:

```
# iscsiadm –m node --targetname THE_TARGET_IQN --login
```

ターゲットからログアウトします:

```
# iscsiadm –m node --targetname THE_TARGET_IQN --logout
```

ターゲットを削除します:

```
# iscsiadm –m node --op delete --targetname THE_TARGET_IQN
```

4.5.3 拡張ACL

拡張ACL

以下の説明は3.3.0**以降の**バージョンのファームウェアを実行する非IntelベースのNASモデルと、3.2.0**以降の**バージョンのファームウェアを実行するIntelベースのNASモデルにのみ適用されます。

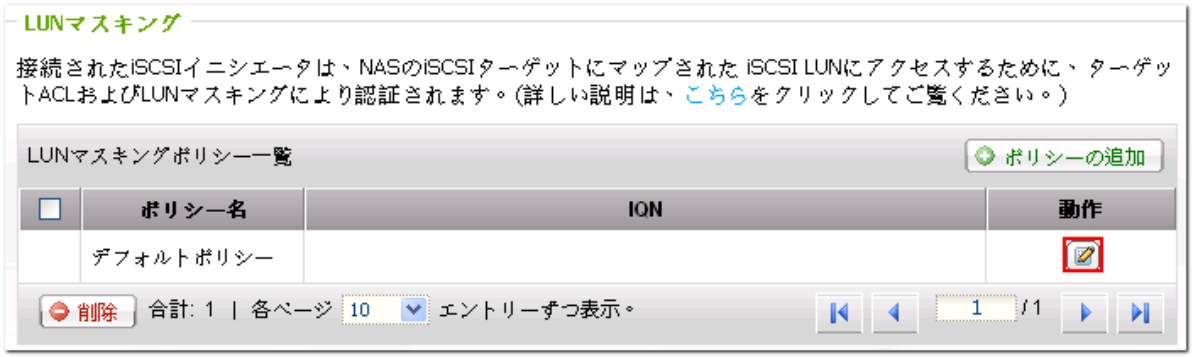
LUNマスキングポリシーを作成して、NASのiSCSIターゲットにマッピングされたLUNへのアクセスを試行するiSCSIイニシエータの許可が設定できます。この機能を使用するには、「拡張ACL」の「ポリシーの追加」をクリックします。

ポリシー名、イニシエータIQNを入力し、NASで作成した各LUNへのアクセス権を割り当てます。

- 読み取り専用: 接続されたイニシエータはLUNからのデータを読み取ることだけが可能です。
- 読み取り/書き込み: 接続されたイニシエータはLUNの読み取りと書き込みアクセス権が許可されます。
- Deny Access (アクセスの拒否: LUNは、接続されたイニシエータに非表示となります。

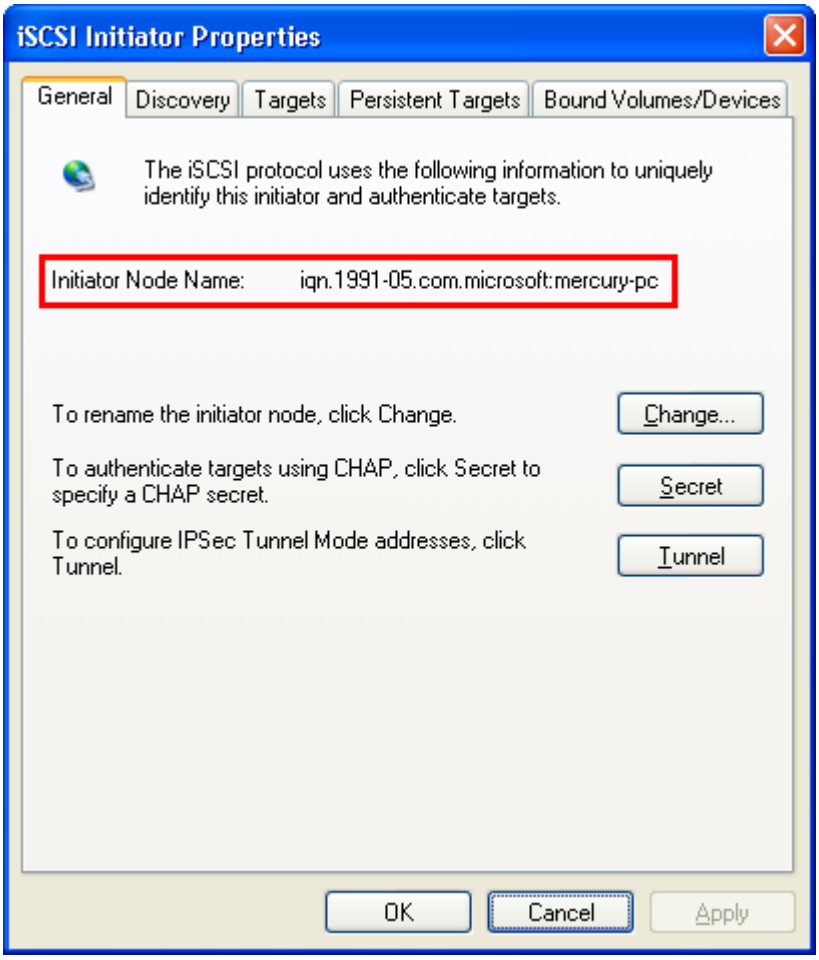
接続されたiSCSIイニシエータに特定のLUNマスキングポリシーを指定しない場合、デフォルトのポリシーが適用されます。システムのデフォルトのポリシーでは、接続された全iSCSIイニシエータからの読み取りと書き込みアクセスを許可します。LUNマスキングリストにある をクリックすると、デフォルトのポリシーを編集できます。

注: デフォルトのLUNポリシーを編集する前にNAS上のLUNを最低1つは作成しておく必要があります。



ヒント:イニシエータIQNはどこにありますか？

Microsoft iSCSIイニシエータを開始し、"General" (全般)をクリックします。イニシエータのIQNは下図のように表示されます。



4.5.4 LUN バックアップ

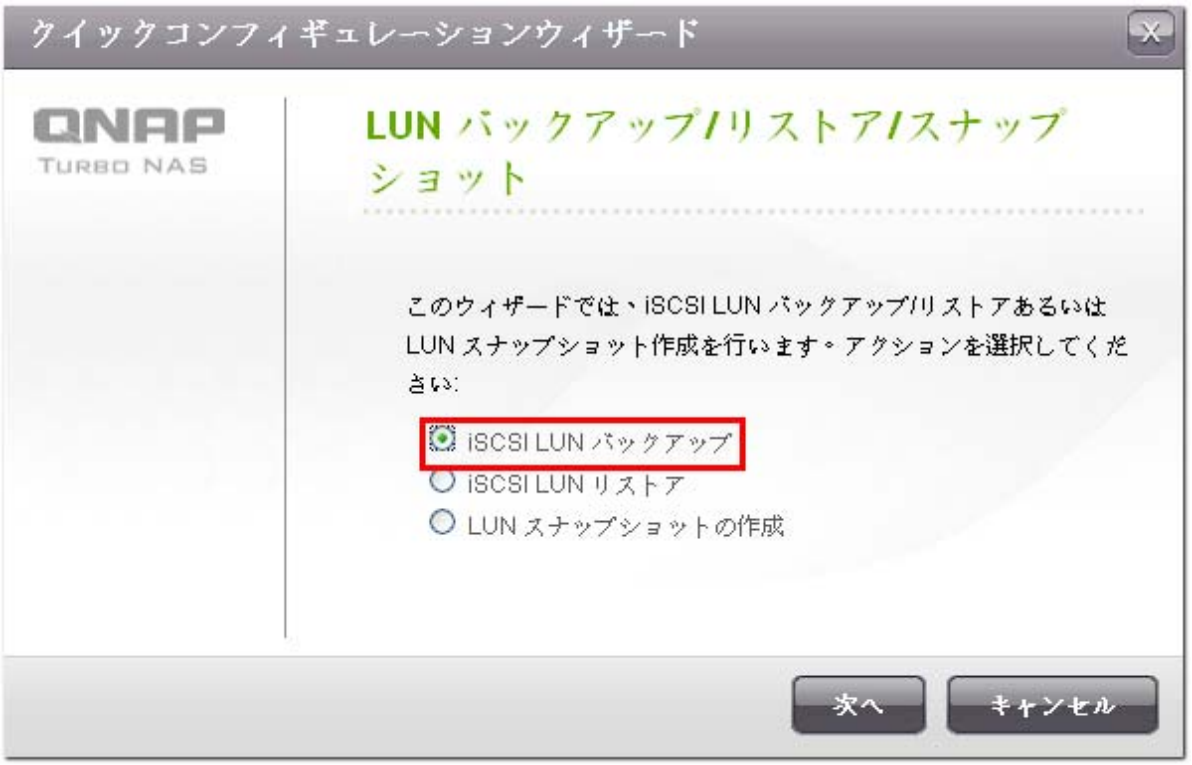
NAS は、iSCSI LUN の異なるストレージロケーション（Windows、Linux、またはローカルネットワーク共有）へのバックアップ、LUN の NAS への復元、LUN スナップショットを作成し、iSCSI ターゲットにマッピングする機能をサポートします。

iSCSI LUN のバックアップ

iSCSI LUN バックアップを行う前に、NAS 上に少なくとも一つの iSCSI LUN が作成されていることを確認してください。iSCSI ターゲットおよび LUN を作成するには、「Disk Management（ディスク管理）」>「iSCSI」>「Target Management（ターゲット管理）」に進みます。

1. 「Disk Management（ディスク管理）」>「iSCSI」>「LUN BACKUP（LUN バックアップ）」に進みます。「Create a new job（新しいジョブの作成）」をクリックします。

2. 「Back up an iSCSI LUN（iSCSI LUNバックアップ）」を選択し、「NEXT（次へ）」をクリックします。

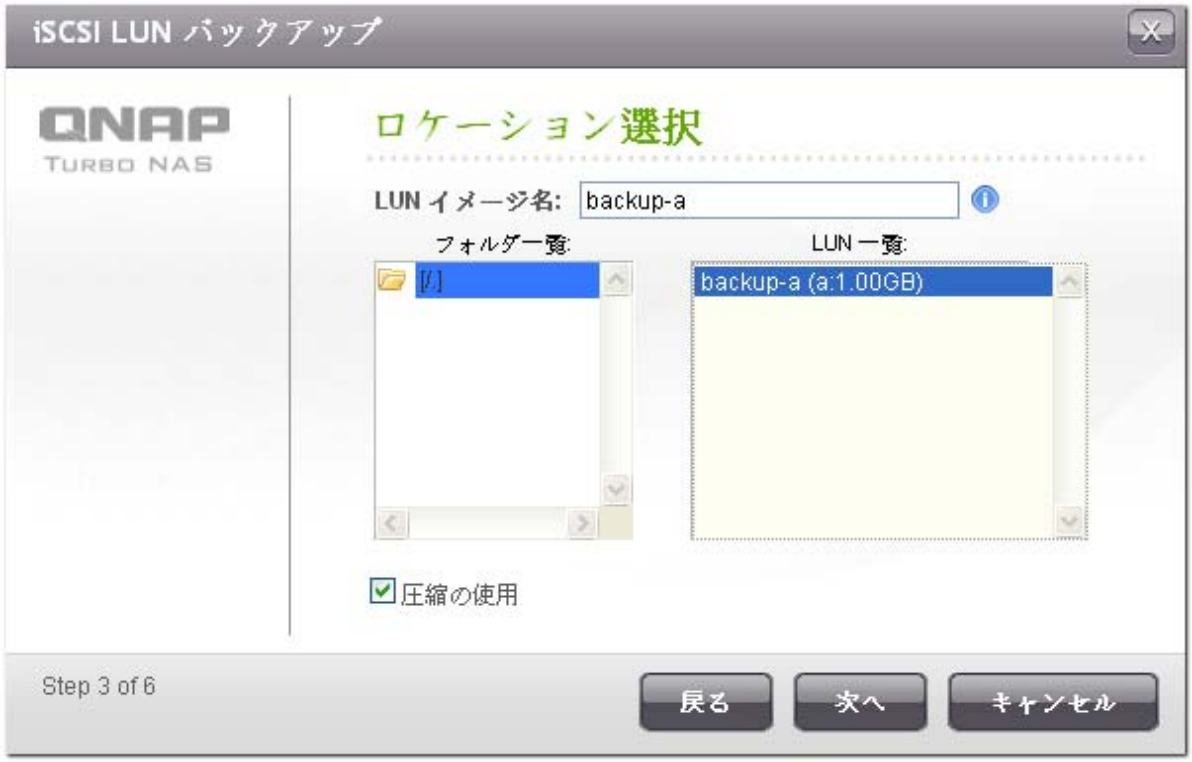


3. バックアップを行う LUN を選択します。オンライン LUN を選択した場合、LUN に対し自動的に非常に短時間にスナップショットを作成します。

4. LUN のバックアップ先を指定します。NAS は、LUN のバックアップ先として、Linux 共有（NFS）、Windows 共有（CIFS/SMB）、および NAS 上のローカルフォルダをサポートします。「TEST（テスト）」をクリックして、指定したパスへの接続をテストします。それから、「NEXT（次へ）」をクリックします。

5. LUN バックアップのイメージ名を入力するか、NAS により生成されたものを使用します。イメージファイルを格納するサブフォルダを選択します。「Use compression*（圧縮の使用）」または「not（使用しない）」を選択します。「NEXT（次へ）」をクリックします。

*Use Compression（圧縮の使用）：このオプションを有効にした場合、NAS 上の CPU リソースはたくさん消費されますが、LUN バックアップサイズは小さくなります。バックアップ時間は、iSCSI LUN の大きさにより変化します。

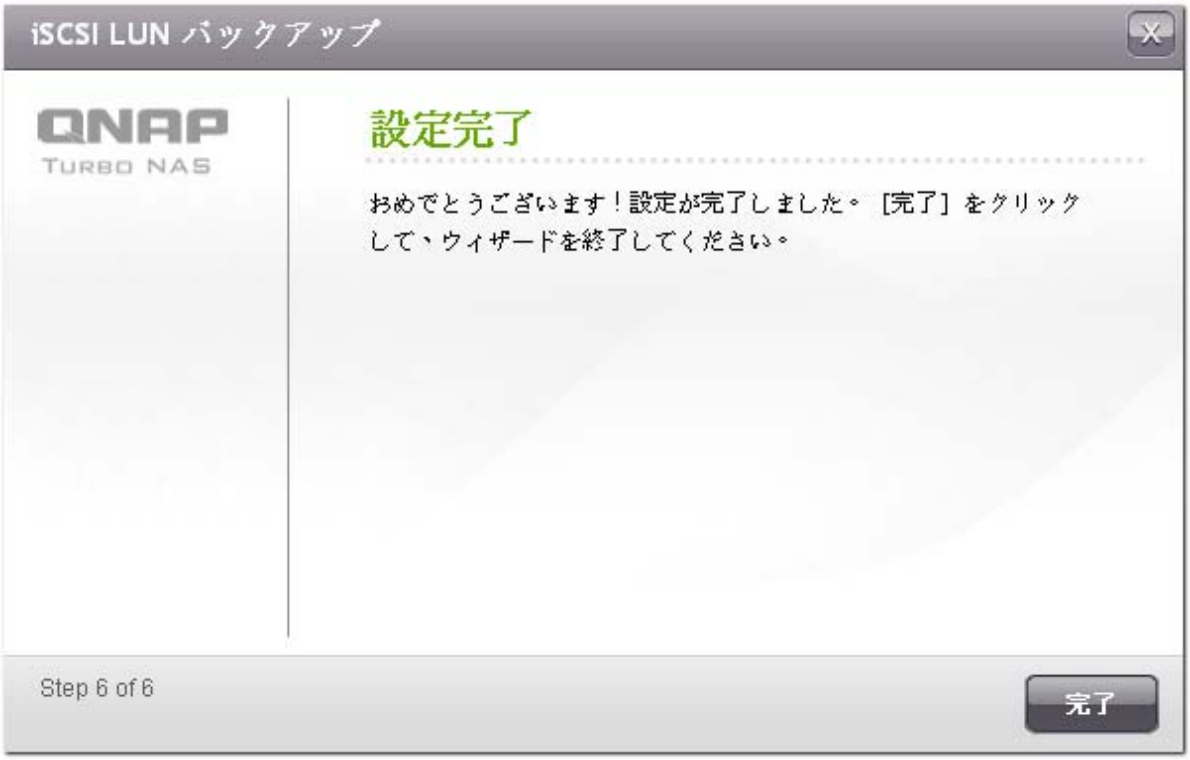


6. バックアップスケジュールを指定します。次のオプションが利用可能です:
   - すぐ
   - 毎時
   - 毎日
   - 毎週
   - 毎月

「NEXT（次へ）」をクリックします。

7. 設定が表示されます。ジョブ名を入力するか、NAS により生成されたものを使用します。「NEXT（次へ）」をクリックします。

8. 「FINISH（完了）」をクリックして終了します。

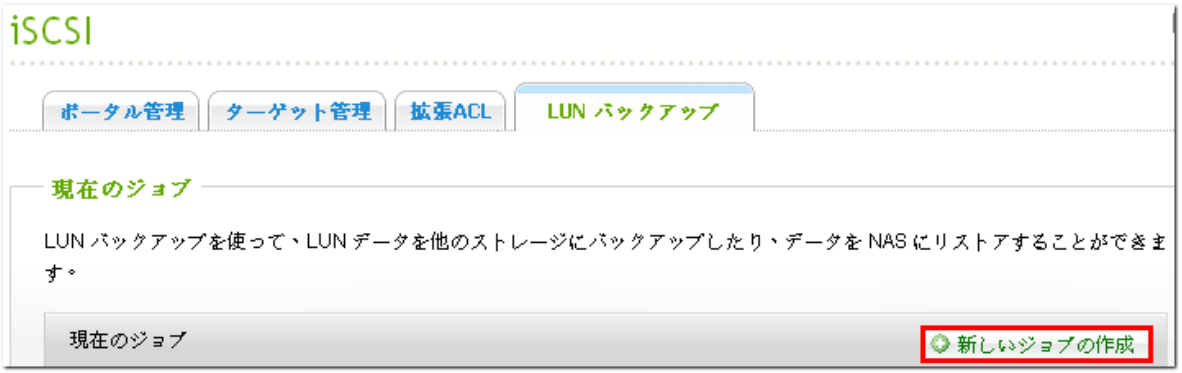


9. バックアップジョブがリスト上に表示されます。

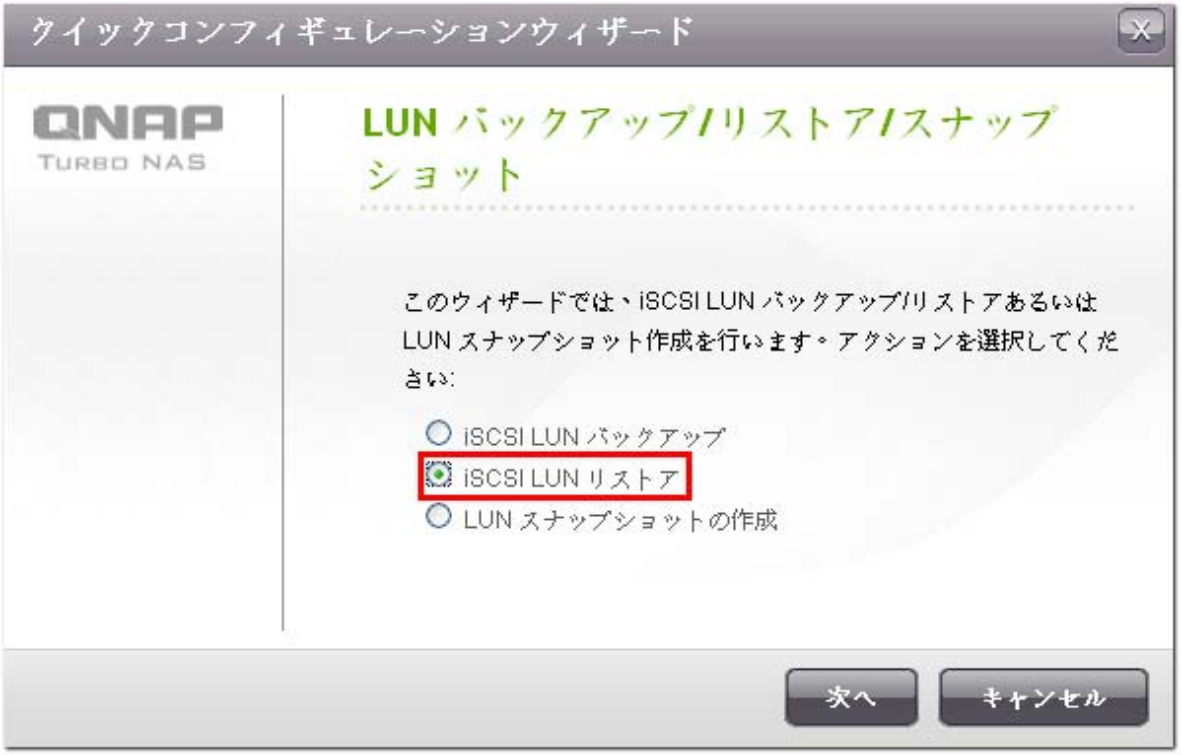
ボタン	説明
	ジョブを直ちに開始します。
	稼働中のジョブを停止します。
	ジョブの設定を編集します。
	ジョブのステータスおよびログを表示します。

iSCSI LUN のリストア

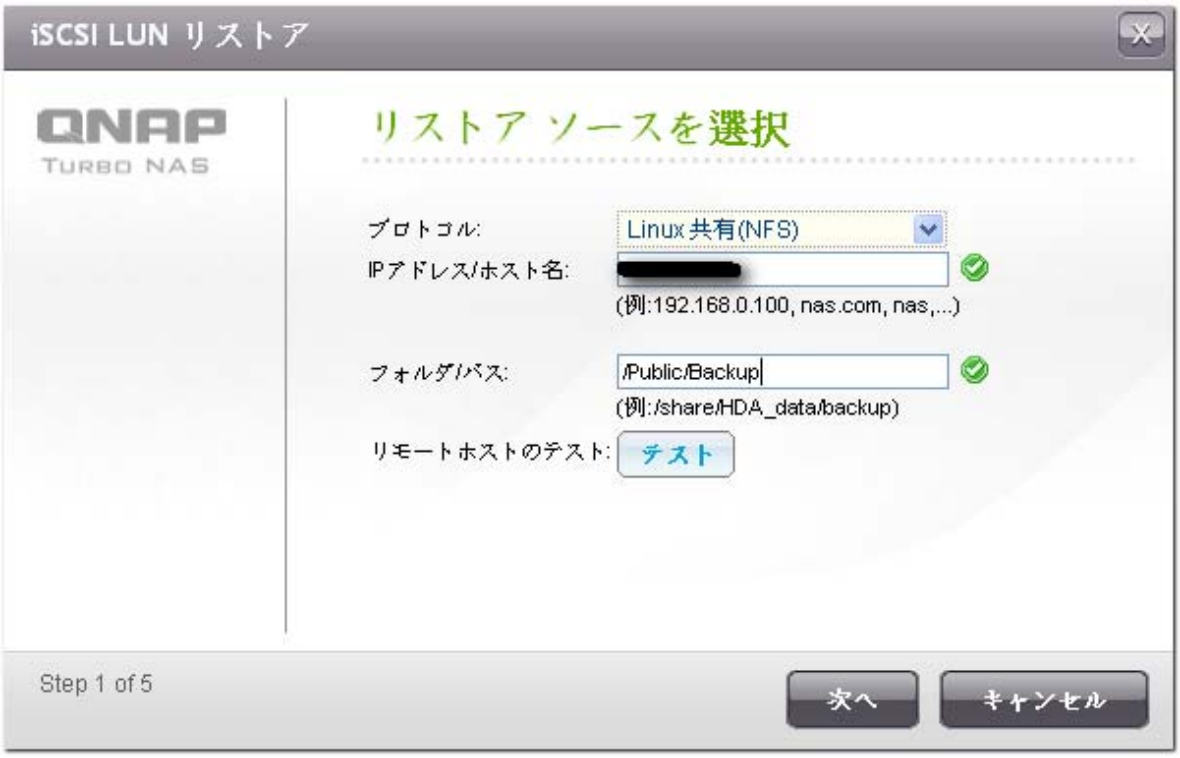
1. iSCSI LUN を NAS にリストアするには、「Disk Management（ディスク管理）」>「iSCSI」>「LUN Backup（LUN バックアップ）」に進みます。「Create a new job（新しいジョブの作成）」をクリックします。



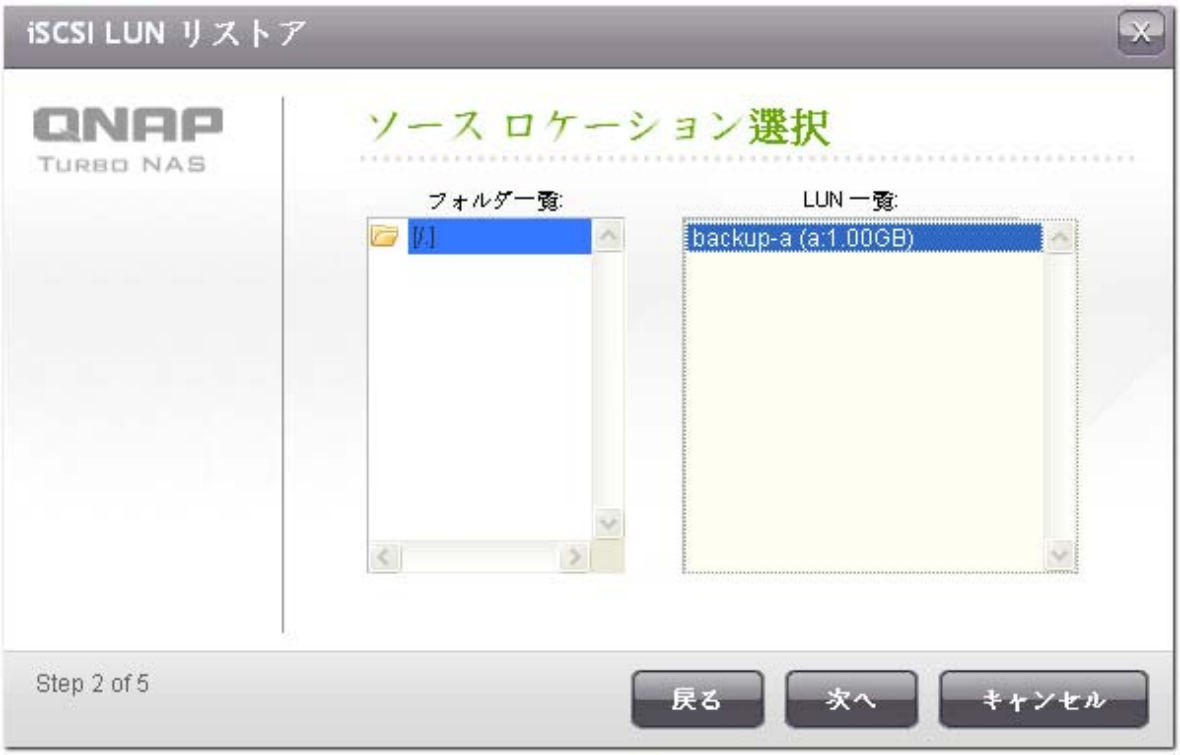
2. 「Restore an iSCSI LUN（iSCSI LUNリストア）」を選択し、「NEXT（次へ）」をクリックします。



3. リストア元のプロトコル、IP アドレス/ホスト名、およびフォルダ/パスを指定します。「TEST（テスト）」をクリックして、接続をテストします。それから、「NEXT（次へ）」をクリックします。

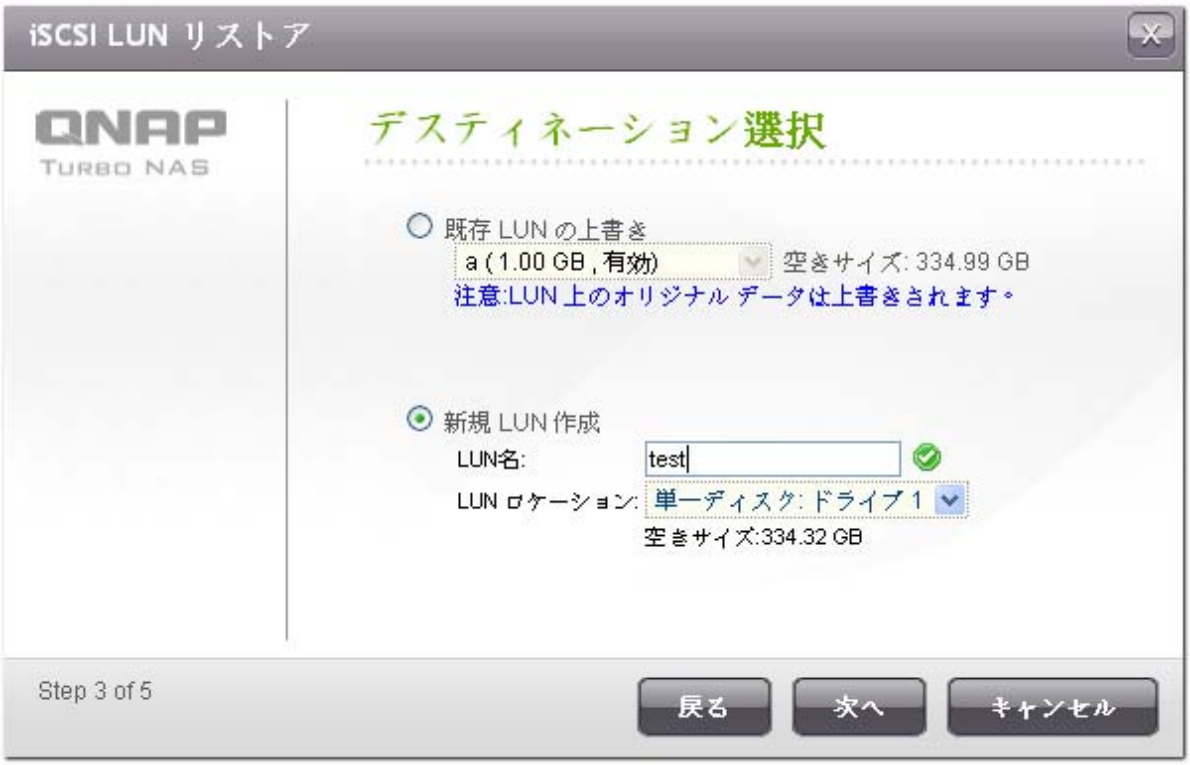


4. LUN イメージファイルを表示し、選択します。「NEXT（次へ）」をクリックします。



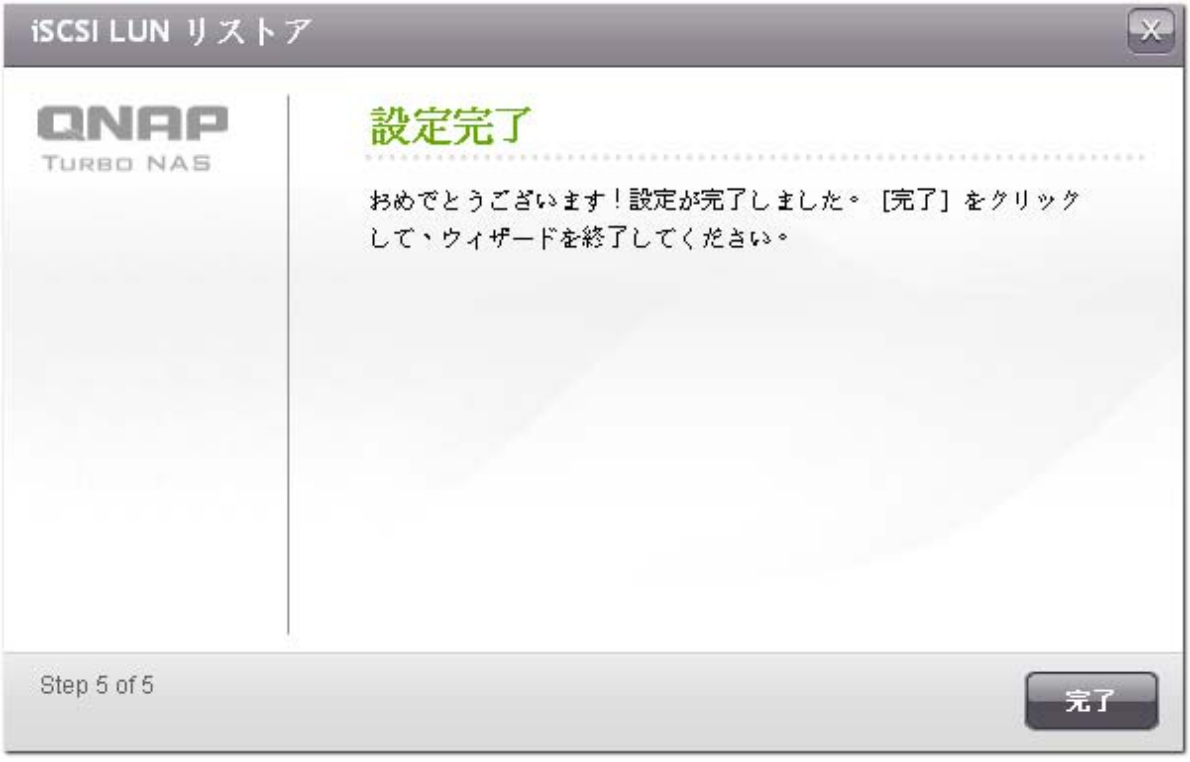
5. リストア先を選択します。
   - 既存 LUNの上書き：iSCSI LUN をリストアし、NAS 上の既存 LUN を上書きします。元の LUN 上のすべてのデータが上書きされます。
   - 新規 LUN作成：iSCSI LUN を NAS 上に新規 LUN としてリストアします。新規 LUN の名称を入力し、ロケーションを選択します。

「NEXT（次へ）」をクリックします。



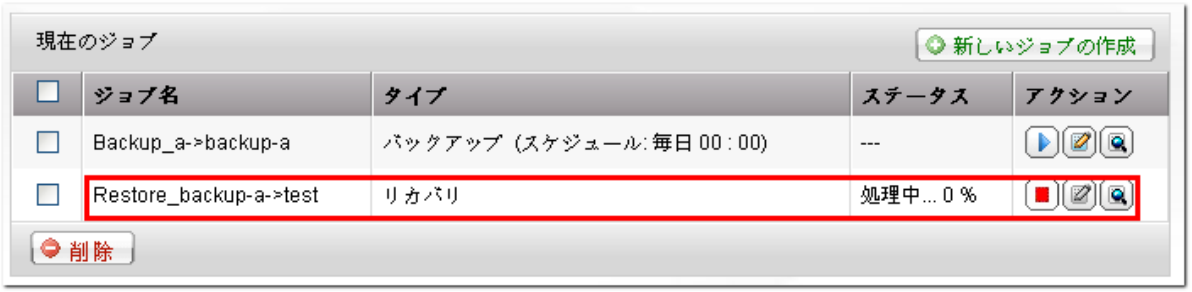
6. 設定が表示されます。ジョブ名を入力するか、NAS により生成されたものを使用します。「NEXT（次へ）」をクリックします。

7. 「FINISH（完了）」をクリックして終了します。



8. リストアジョブは、直ちに実行されます。

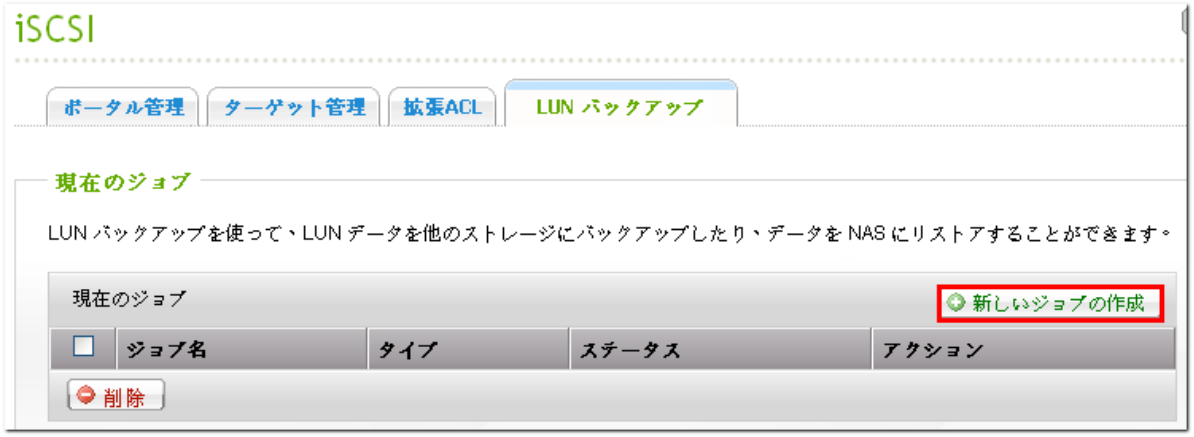
ボタン	説明
	稼働中のジョブを停止します。
	ジョブの設定を編集します。
	ジョブのステータスおよびログを表示します。



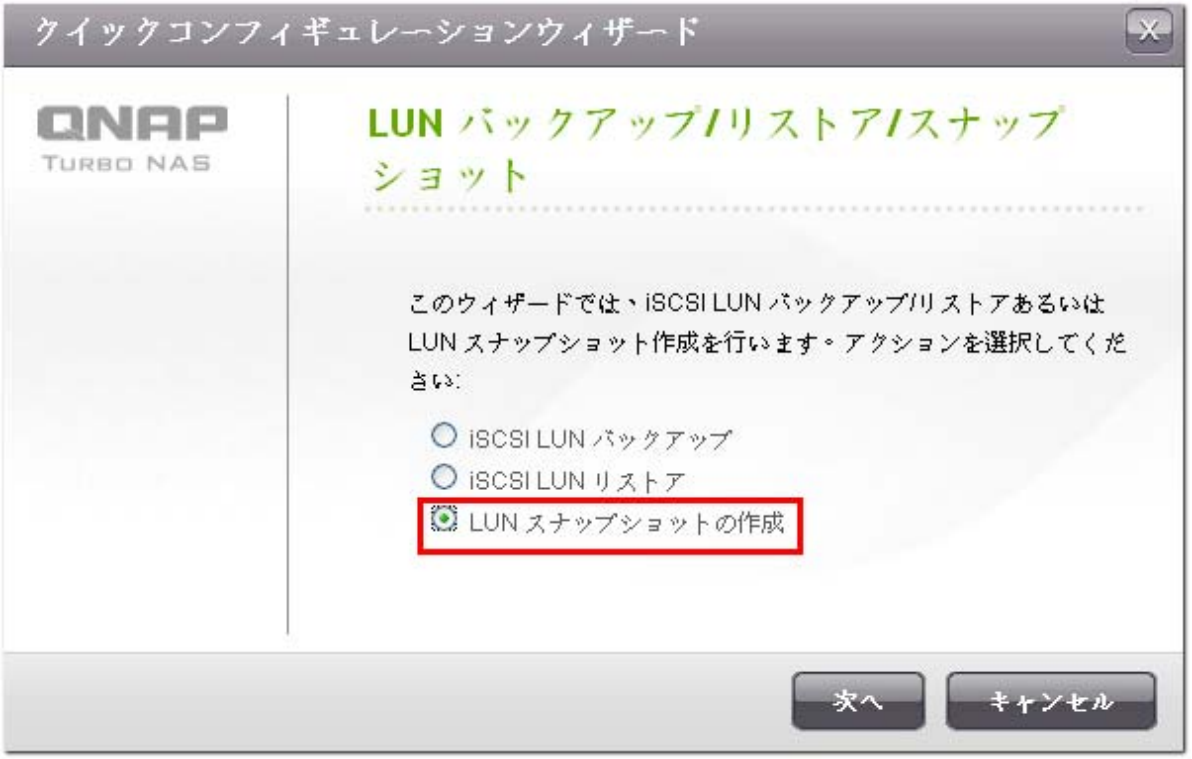
iSCSI LUN スナップショットの作成

iSCSI LUN スナップショットを作成する前に、NAS 上に少なくとも一つの iSCSI LUN および一つの iSCSI ターゲットが作成されていることを確認します。iSCSI ターゲットおよび LUN を作成するには、「Disk Management（ディスク管理）」>「iSCSI」>「Target Management（ターゲット管理）」に進みます。

1. iSCSI LUN スナップショットを作成するには、「Disk Management（ディスク管理）」>「iSCSI」>「LUN Backup（LUN バックアップ）」に進みます。「Create a new job（新しいジョブの作成）」をクリックします。



2. 「Create a LUN Snapshot（LUN スナップショットの作成）」を選択し、「NEXT（次へ）」をクリックします。

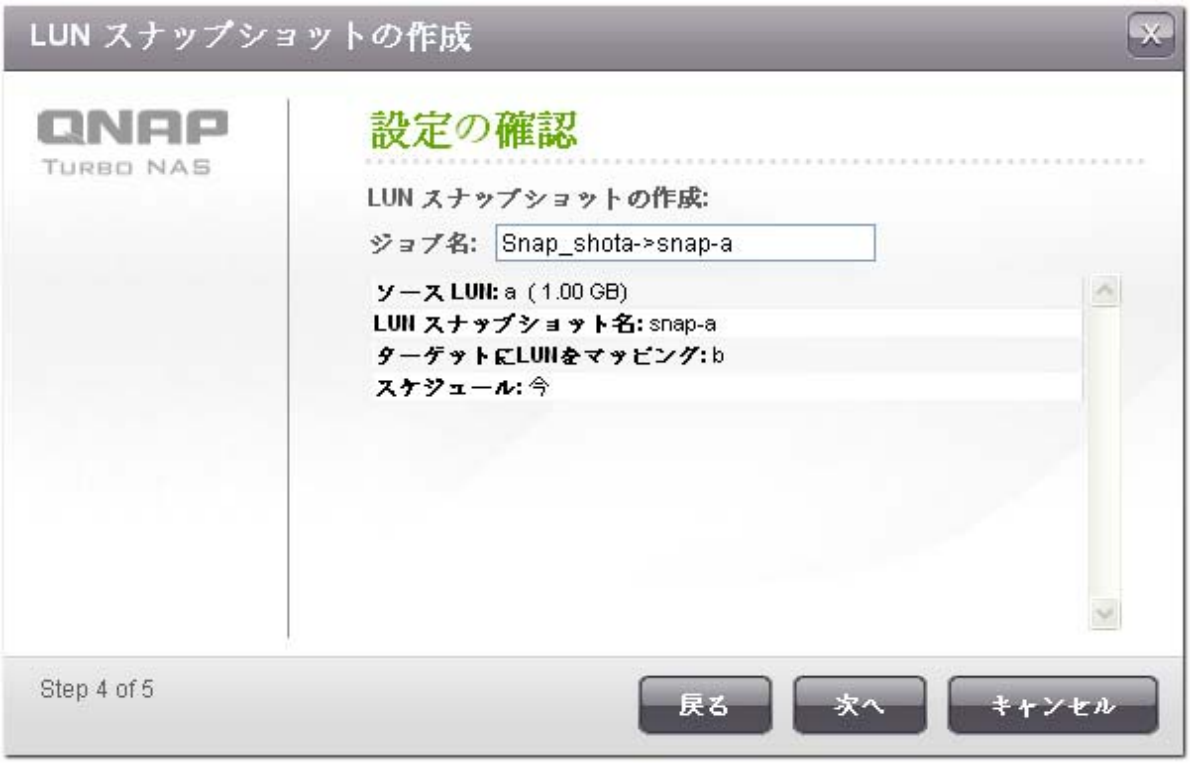


3. NAS 上の iSCSI LUN を選択します。「NEXT（次へ）」をクリックします。

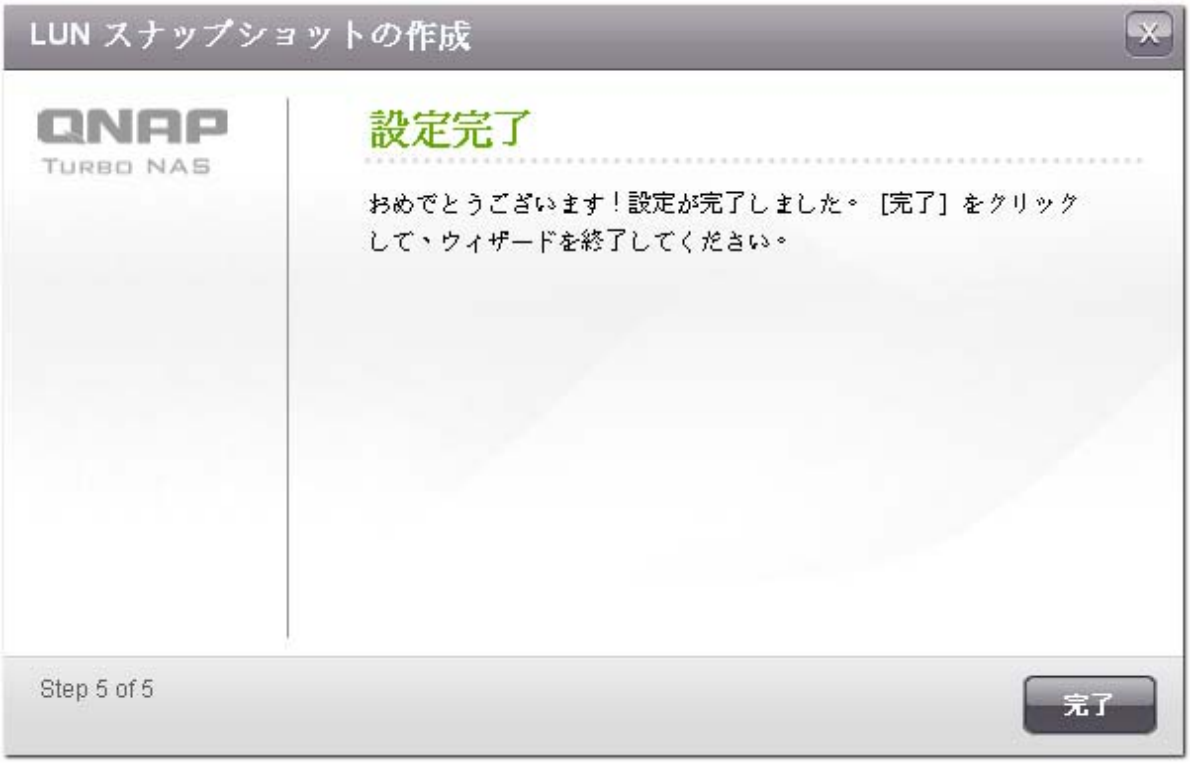
4. LUN スナップショット名を入力するか、NAS により生成されたものを使用します。LUN スナップショットをマッピングする iSCSI ターゲットを選択します。「NEXT（次へ）」をクリックします。

5. スナップショットのスケジュールおよび存続期間を指定します。スナップショットは、存続期間に達した時に自動的に消去されます。

6. 設定が表示されます。ジョブ名を入力するか、NAS により生成されたものを使用します。「NEXT（次へ）」をクリックします。



7. 「FINISH（完了）」をクリックして終了します。



8. スナップショットは直ちに作成されます。ステータスおよび存続期間がリスト上に表示されます。

9. 「iSCSI」>「Target Management（ターゲット管理）」と進めて、iSCSI ターゲットリスト内にスタップショットの LUN を表示します。iSCSI イニシエーターソフトウェアと使って、iSCSI ターゲットに接続し、LUN スナップショット上の瞬時データにアクセスします。QNAP NAS 上の iSCSI ターゲットへの接続に関する詳細な情報は、http://www.qnap.com/pro_application.asp?ap_id=135 を参照してください。

注: ソースLUNとスナップショットLUNは、Windows 7やWindows 2008 R2などの特定オペレーティングシステム上の同じサーバーにマウントすることは⇂できません。そのような場合、LUNを異なるサーバーにマウントしてください。

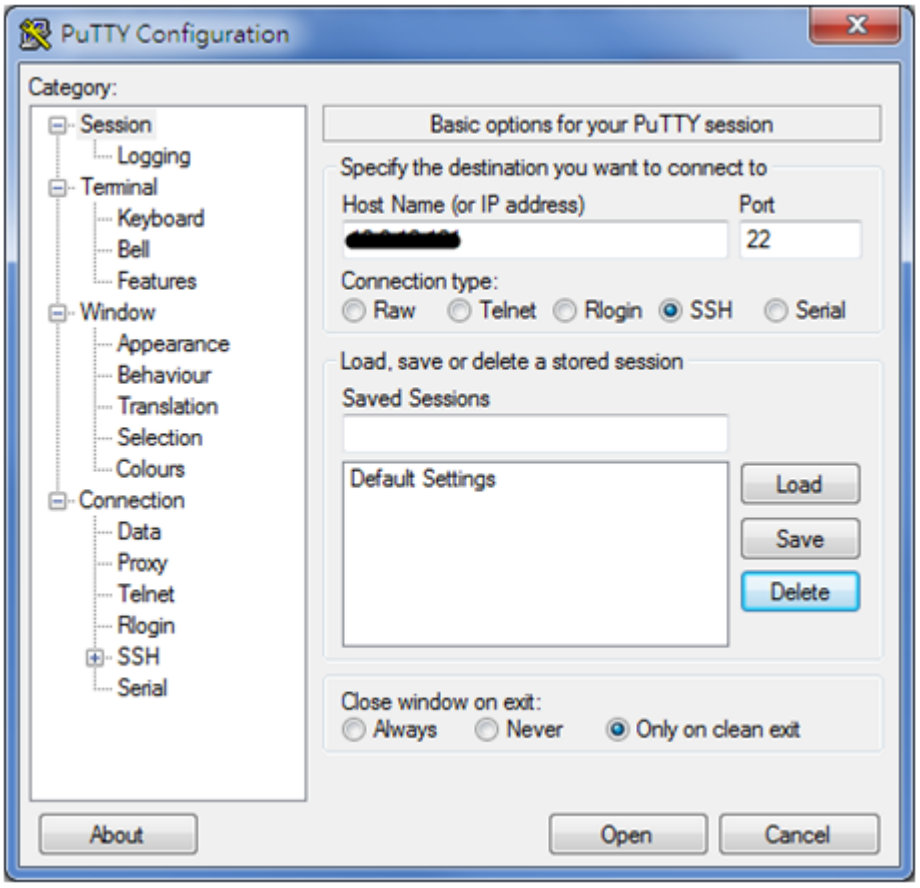
コマンドラインでの LUN バックアップ/リストア/スナップショットの管理

QNAP NAS ユーザーは、コマンドラインで、NAS 上の iSCSI LUN バックアップ、リストア、スナップショットジョブを実行/停止することができます。次の操作を行い、この機能を利用します。

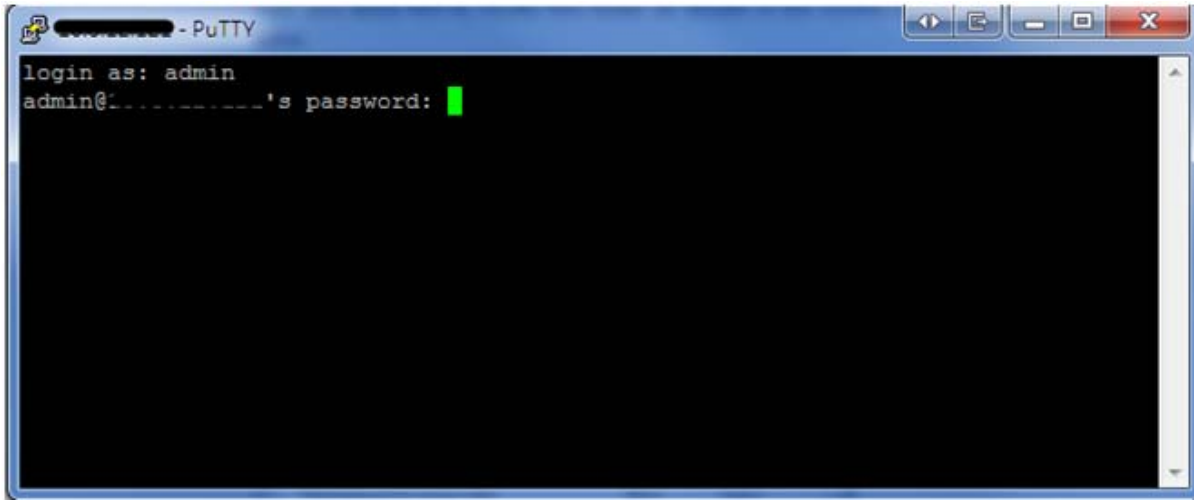
> 注：以下の操作はコマンドラインに慣れた IT 管理者のみが実行するようにしてください。

1. 最初に、iSCSI LUN バックアップ、リストア、スナップショットジョブが NAS 上に作成されていることを「Disk Management（ディスク管理）」>「iSCSI」>「LUN Backup（LUN バックアップ）」で確認します。

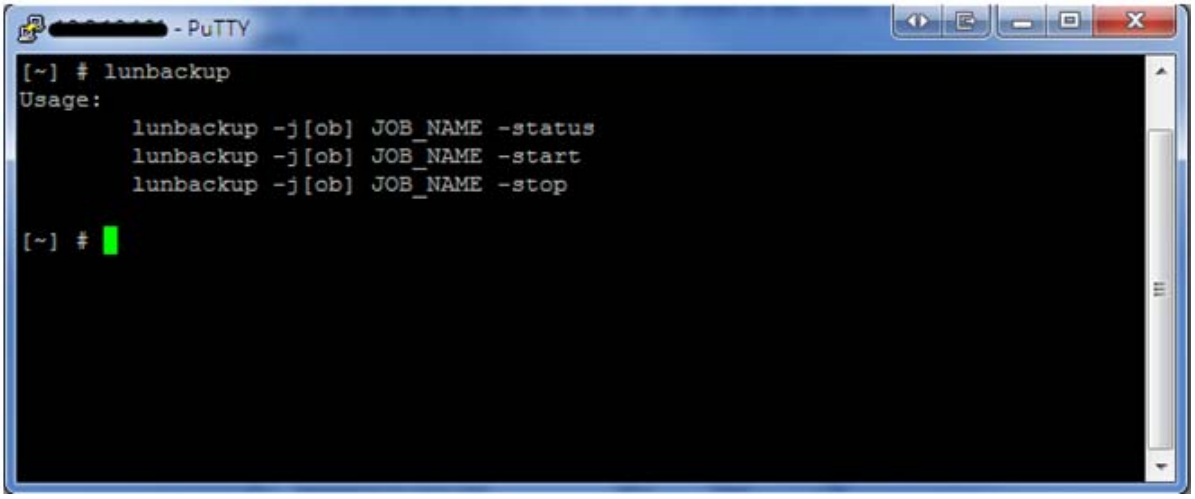
2. NAS に Putty などの SSH ユーティリティを使用して接続します。



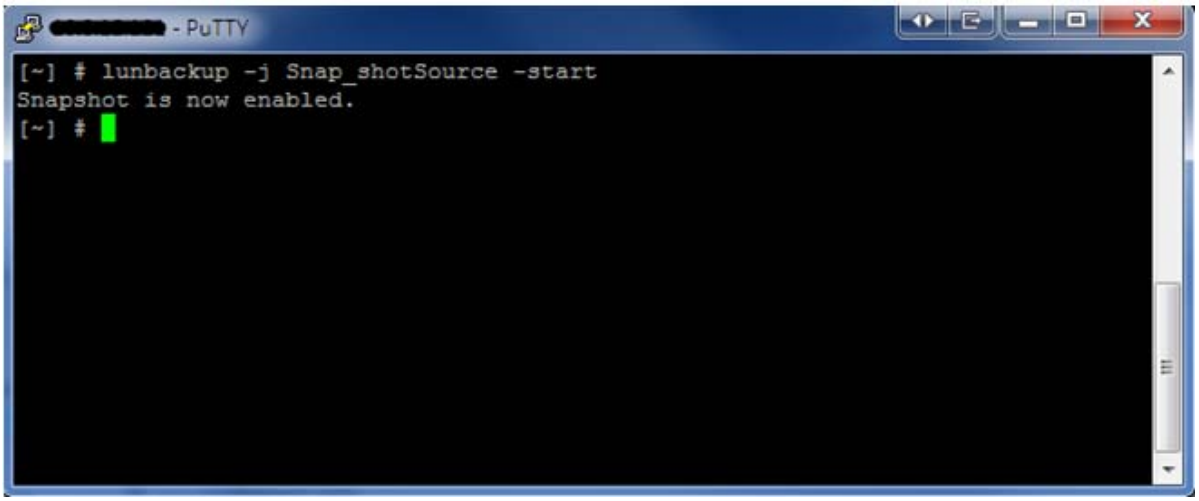
3. NAS に管理者としてログインします。



4. コマンド「lunbackup」を入力します。コマンドの使用方法が表示されます。



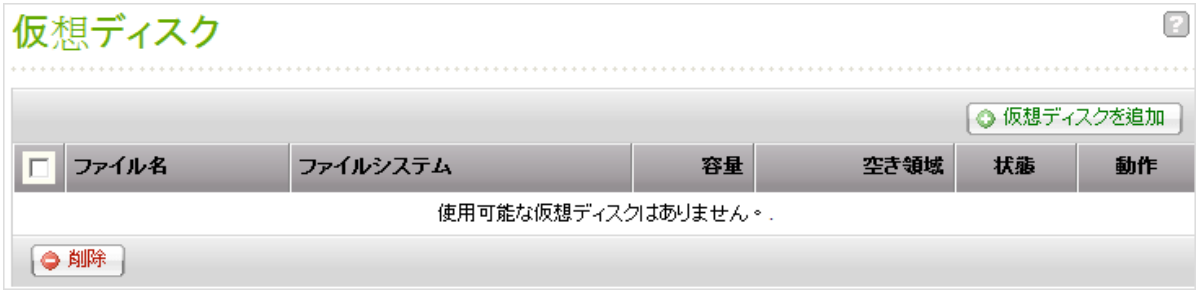
5. lunbackup コマンドを使用して、NAS 上の iSCSI LUN バックアップ、リストア、スナップショットジョブを開始/終了します。



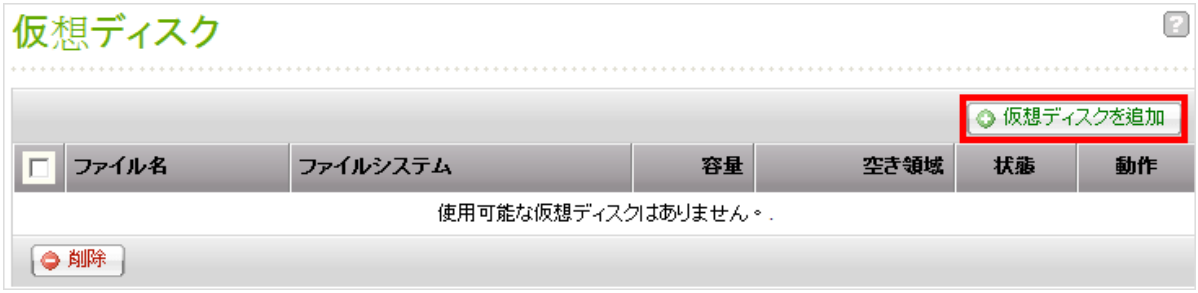
4.6 仮想ディスク

この機能を使用して、他のQNAP NASまたはストレージサービスのiSCSIターゲットを、ストレージ容量拡張のため仮想ディスクとしてNASに追加することができます。NASは最大8仮想ディスクまでサポートしています。

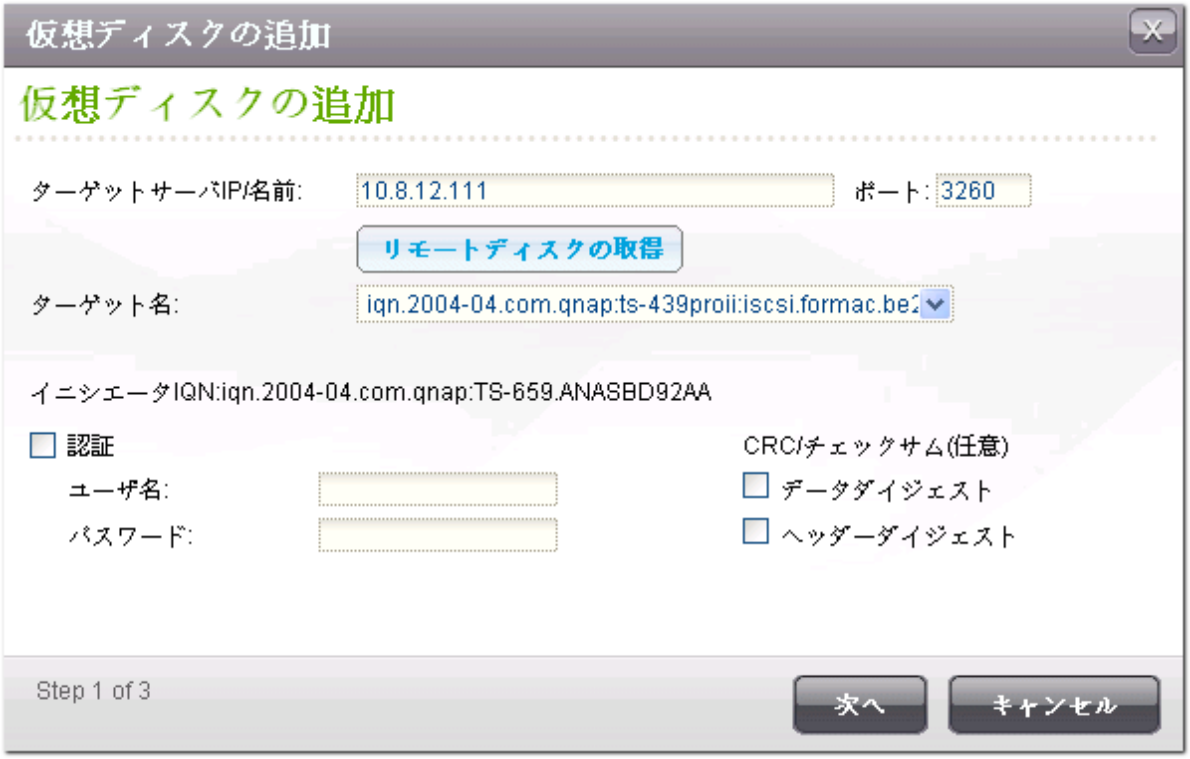
> 注：NASがサポートする仮想ディスクの最大サイズは16テラバイトです。



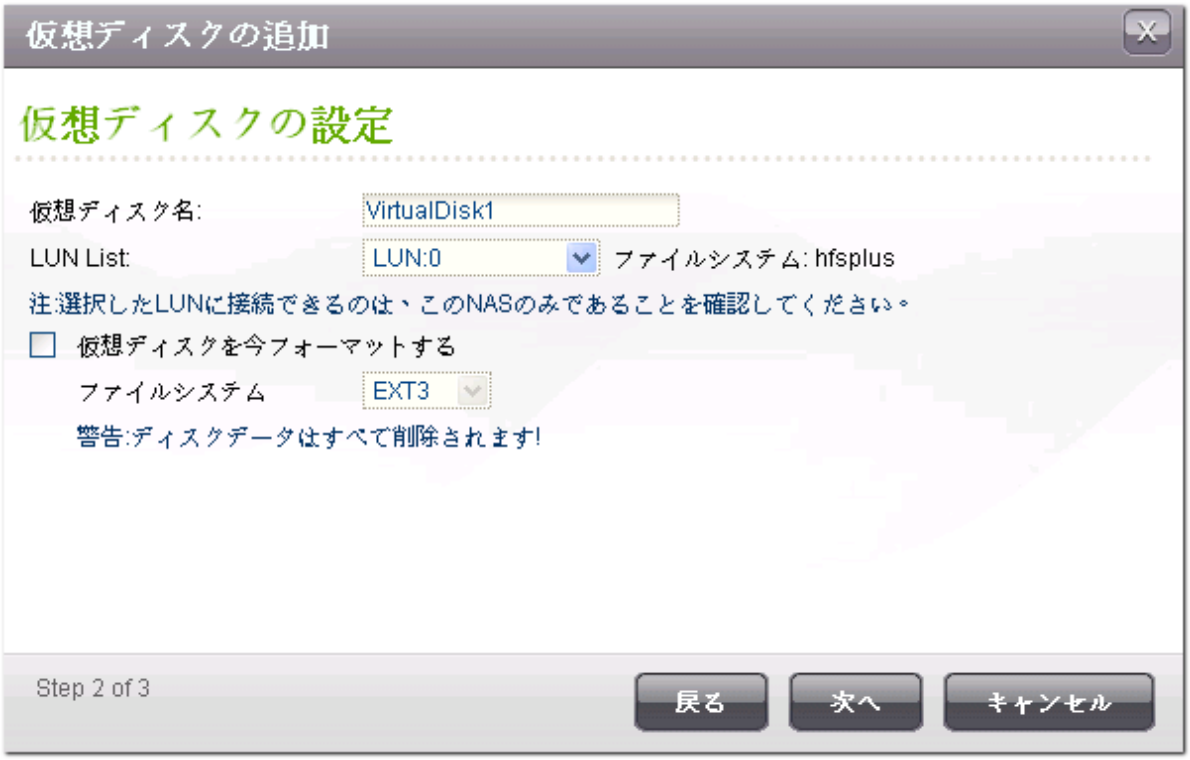
仮想ディスクをNASに追加するには、iSCSIターゲットが作成されていることを確認してください。「仮想ディスクの追加」をクリックします。



ターゲットのサーバーIPとポート番号を入力します（デフォルト: 3260）。「Get Remote Disk（リモートディスクの取得）」をクリックします。ターゲットリストからターゲットを選択します。認証が要求されたら、ユーザー名とパスワードを入力します。オプションの「データダイジェスト」と「ヘッダダイジェスト」を選択することができます。これらのオプションは、iSCSIターゲットへの接続を試みるときに、イニシエータを検証するパラメータです。「NEXT（次へ）」をクリックします。



バーチャルディスクの名前を入力します。 ターゲットが複数のLUNでマップされる場合、リストからLUNを選択します。 このNASのみがLUNに接続できることを確認します NASはEXT3、EXT4、FAT32、NTFS、HFS+ファイルシステムのマウントに対応しています。 LUNのファイルシステムが「不明」な場合、「Format virtual disk now（仮想ディスクを今フォーマットする）」とファイルシステムを選択します。 EXT3、EXT4、FAT32、NTFS、HFS+としてバーチャルディスクをフォーマットできます。 「Format virtual disk now（仮想ディスクを今フォーマットする）」を選択することで、LUNのデータが削除されます。



「FINISH（終了）」をクリックしてウィザードを終了します。

NASのストレージ容量は、バーチャルディスクにより拡張されています。「Access Right Management（アクセス権の管理）」>「Share Folders（共有フォルダ）」をポイントすることで、バーチャルディスクの新しい共有フォルダを作成できます。

アイコン	説明
（編集）	iSCSIターゲットのバーチャルディスク名または認証情報を編集します。
（接続）	iSCSIターゲットに接続します。
（切断）	iSCSIターゲットに接続します。
（フォーマット）	EXT3、EXT 4、FAT 32、NTFS、HFS+ファイルシステムとしてバーチャルディスクをフォーマットします。
（削除）	iSCSIターゲットのバーチャルディスクを削除します。

5. アクセス権管理

ドメインのセキュリティ 194
ユーザ 216
ユーザグループ 229
共フォルダ 230
クォータ 260

5.1 ドメインのセキュリティ

NAS は、ローカルでのアクセス権管理、Microsoft アクティブディレクトリ(Windows Server 2003/2008)、および、LDAP (Lightweight Directory Access Protocol : ライトウェイトディレクトリアクセスプロトコル)ディレクトリによるユーザー認証をサポートします。NAS をアクティブディレクトリまたは LDAP ディレクトリに参加させることにより、アクティブディレクトリまたは LDAP ディレクトリのユーザーは、NAS 上に設定された余分なユーザーアカウントではなく、自身のユーザーアカウントで NAS にアクセスすることができます。

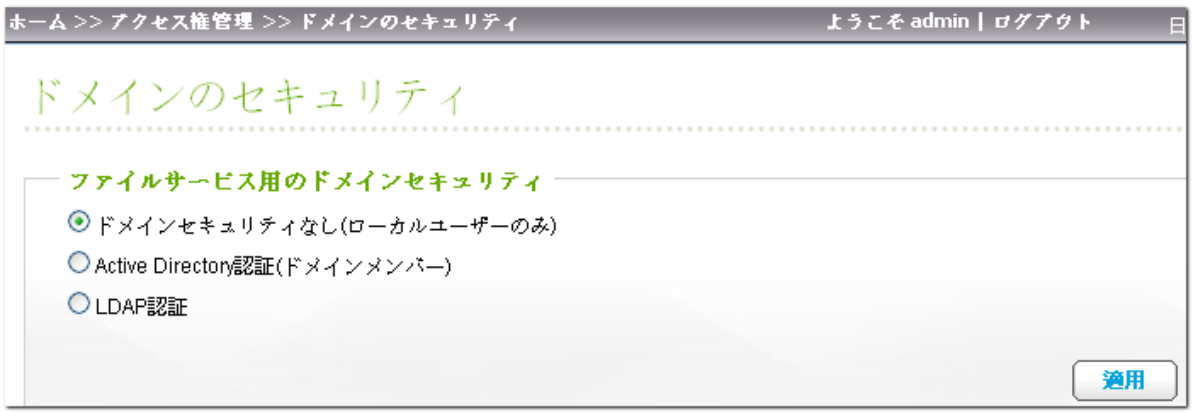
ドメインセキュリティなし
ローカルユーザーのみが NAS にアクセス可能です。

Active Directory認証(ドメインメンバー)
NAS をアクティブディレクトリに参加させます。ドメインユーザーは、NAS により認証されます。NAS をアクティブディレクトリドメインに参加させた後は、ローカル NAS ユーザーおよびアクティブディレクトリユーザーは、次のプロトコル/サービス経由で NAS にアクセスします:

- Samba (Microsoft ネットワーク方式)
- AFP
- FTP
- Web ファイルマネージャ
- WebDAV

LDAP 認証
NAS を LDAP ディレクトリに接続します。LDAP ユーザーは、NAS により認証されます。NAS を LDAP ディレクトリに接続した後は、ローカル NAS ユーザー、または、LDAP ユーザーは Samba (Microsoft ネットワーク方式)経由で認証され、アクセスします。ローカル NAS ユーザーおよび LDAP ユーザーは、次のプロトコル/サービス経由で NAS にアクセスします:

- AFP
- FTP
- Web ファイルマネージャ



5.1.1 NASをWindows Server 2003/2008 Active Directoryに結合します

Active Directory® は、Windows環境で使用されるMicrosoftのディレクトリです。このディレクトリを使用してネットワーク上で情報やリソースを中央集中的に保存、共、及び管理できます。 これは、ユーザー、ユーザーグループ、コンピュータの情報を中央集中的に保持しセキュアなアクセス管理が可能な階層的データセンターです。

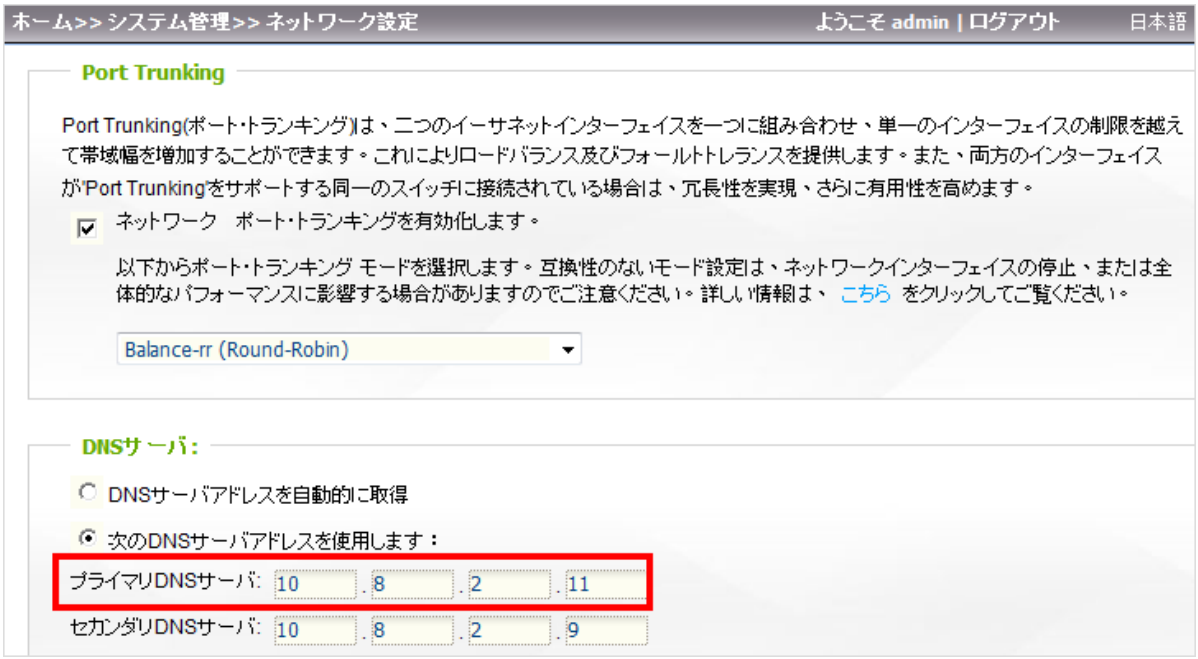
NASは、Active Directory (AD) をサポートします。 ＮＡＳとActive Directoryを連結させることによって、ADサーバーのユーザーアカウントは全て、自動的にNASへインポートされます。 ADユーザーは、ユーザー名およびパスワードを使用してNASにログインできます。

アクティブディレクトリをWindows Server 2008 R2上で使用している場合、NASをアクティブディレクトリに連携させるには、NASファームウェアをV3.2.0またはそれ以降にアップデートさせる必要があります。

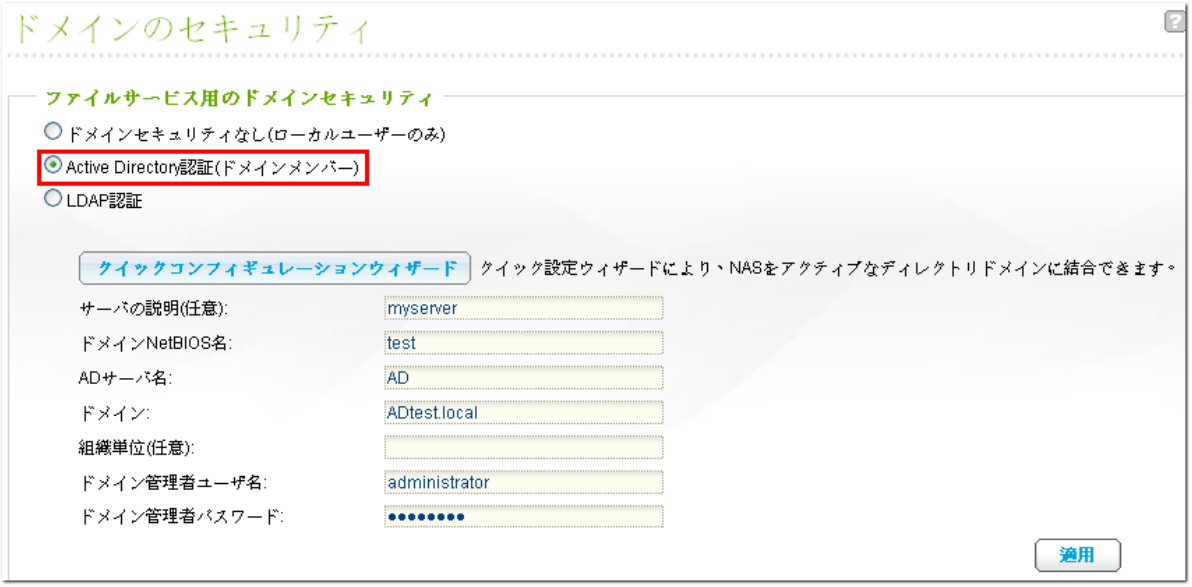
QNAP NASをWindows Active Directoryに連結するには、以下の手順に従ってください。

1. NASに管理者としてログインします。"System Administration" (システム管理) > "General Settings" (一般設定) > "Date and Time" (日付) に移動します。 NASの日付を設定します。この日付は、ADサーバーの日付と一致させる必要があります。 最大許容誤差時間は5分です。

2. "System Administration" (システム管理) > "Network" (ネットワーク) > "TCP/IP" に移動します。プライマリDNSサーバーのIPアドレスをActive Directoryサーバーの IPアドレスとして入力します。外部DNSサーバーを使用する場合、ドメインに連携することはできません。



3. 「Access Right Management（アクセス権管理）」 > 「Domain Security（ドメインのセキュリティ）」と進みます。「Active Directory authentication (domain member)（Active Directory認証(ドメインメンバー)）」を有効化し、アクティブディレクトリドメインの情報を入力します。



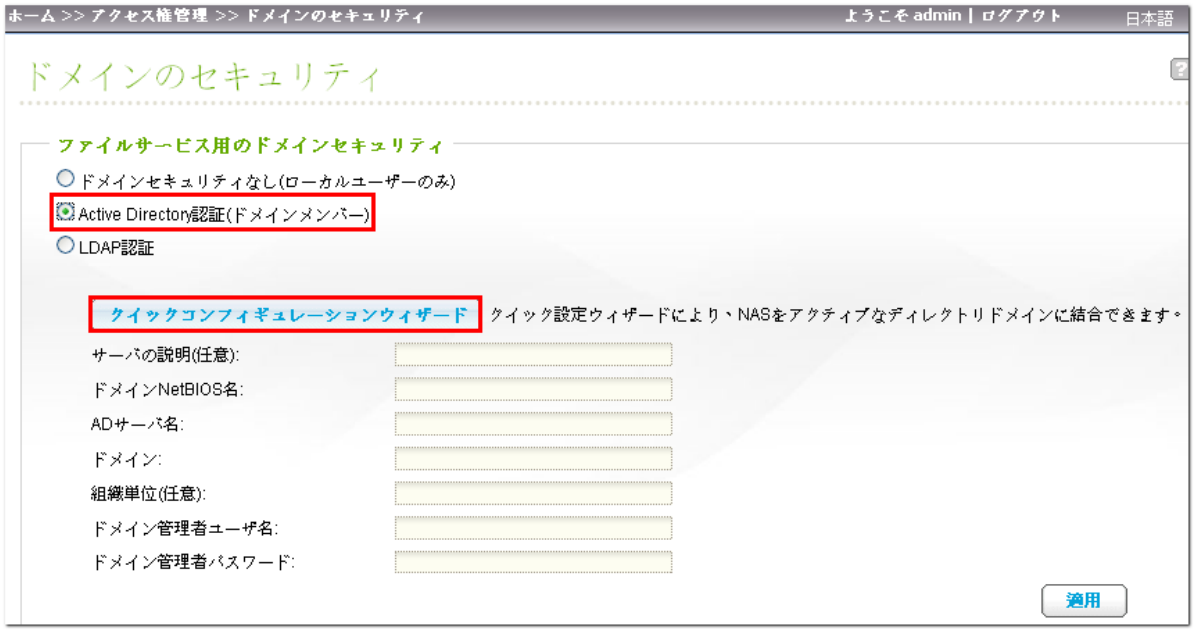
注:

- 正式に認可されたADドメイン名 (例: qnap-test.com) を入力します。
- ここに入力したADユーザーはADドメインへの管理者アクセス権を所持している必要があります。
- WINS サポート:WINSサーバをネットワークでご使用の際に、ワークステーションをWINSサーバを名前解決に使用するよう構成してある場合、WINSサーバIPをNAS上にセットアップする必要があります。(特定のWINSサーバを使用)。

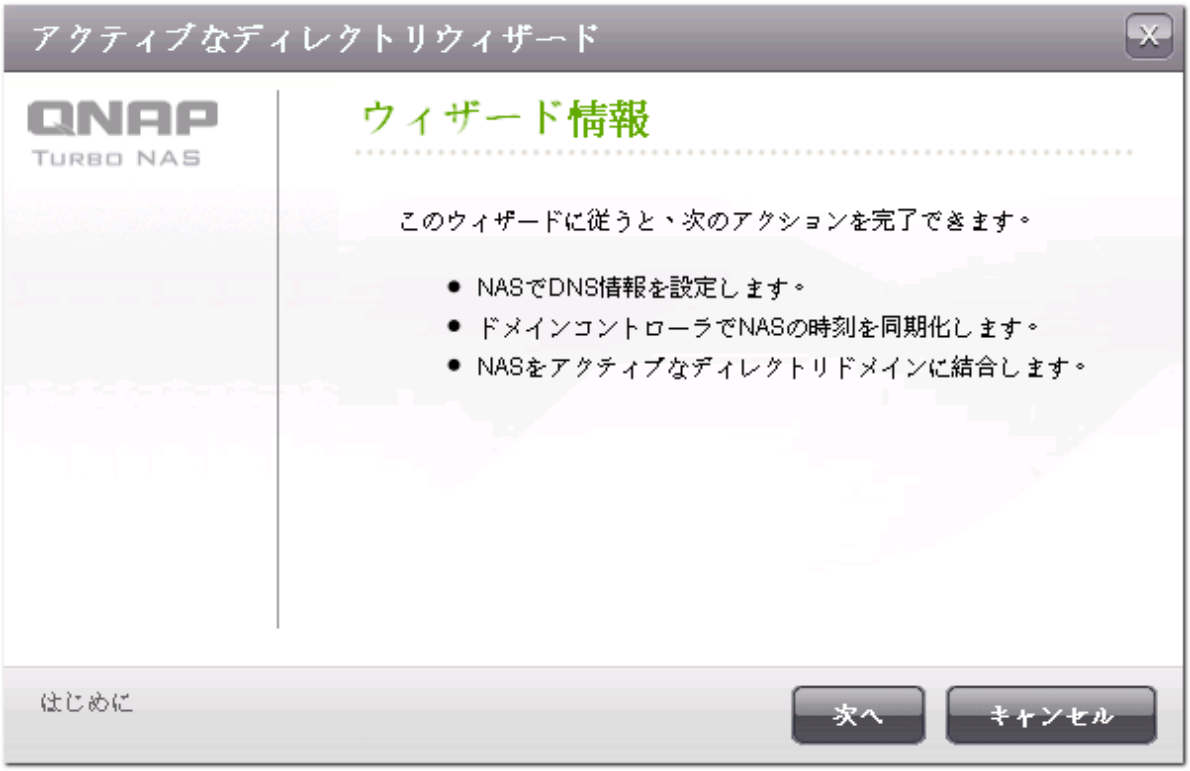
クイック設定ウィザードによりAD（アクティブディレクトリ）にQNAP NASを結合する

クイック設定ウィザードで、NAS をアクティブディレクトリドメインに参加させるには、次のステップを行います。

1. 「Access Right Management（アクセス権管理）」>「Domain Security（ドメインのセキュリティ）」と進みます。「Active Directory authentication (domain member)（Active Directory認証(ドメインメンバー)）」を選択し、「Quick Configuration Wizard（クイックコンフィギュレーションウィザード）」をクリックします。

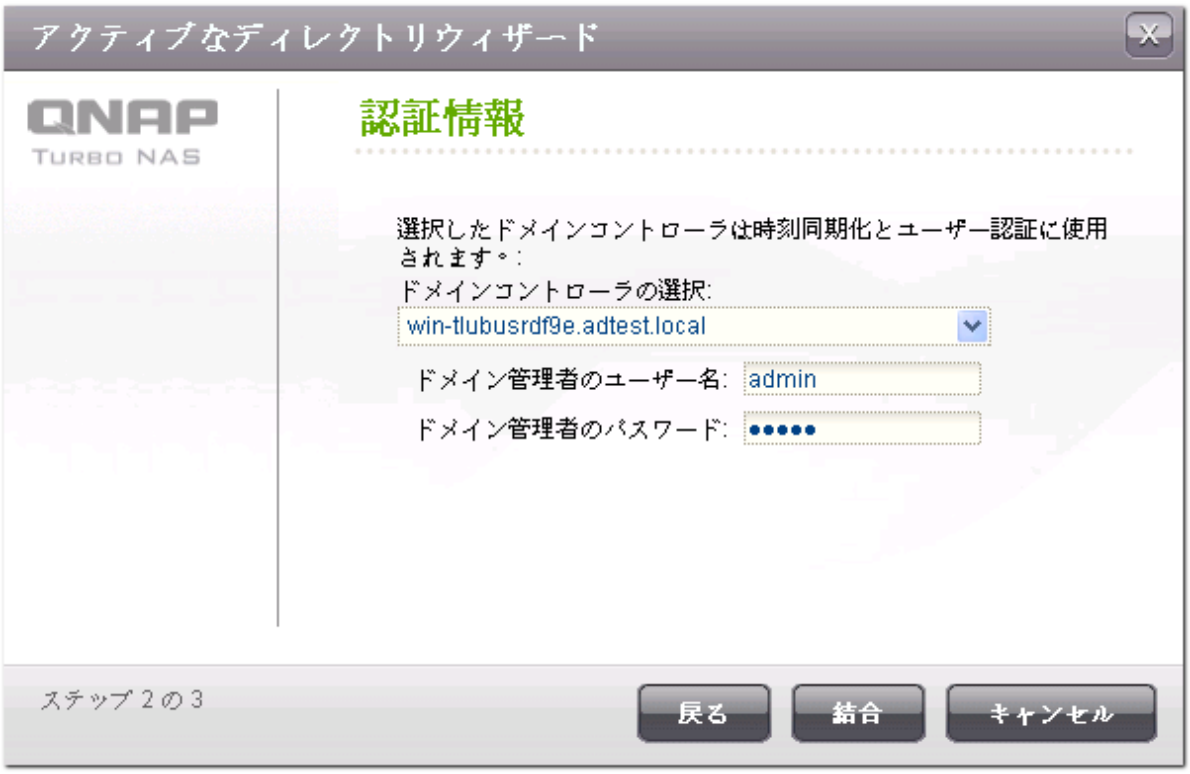


2. ウィザードの紹介を読みます。「Next（次へ）」をクリックします。

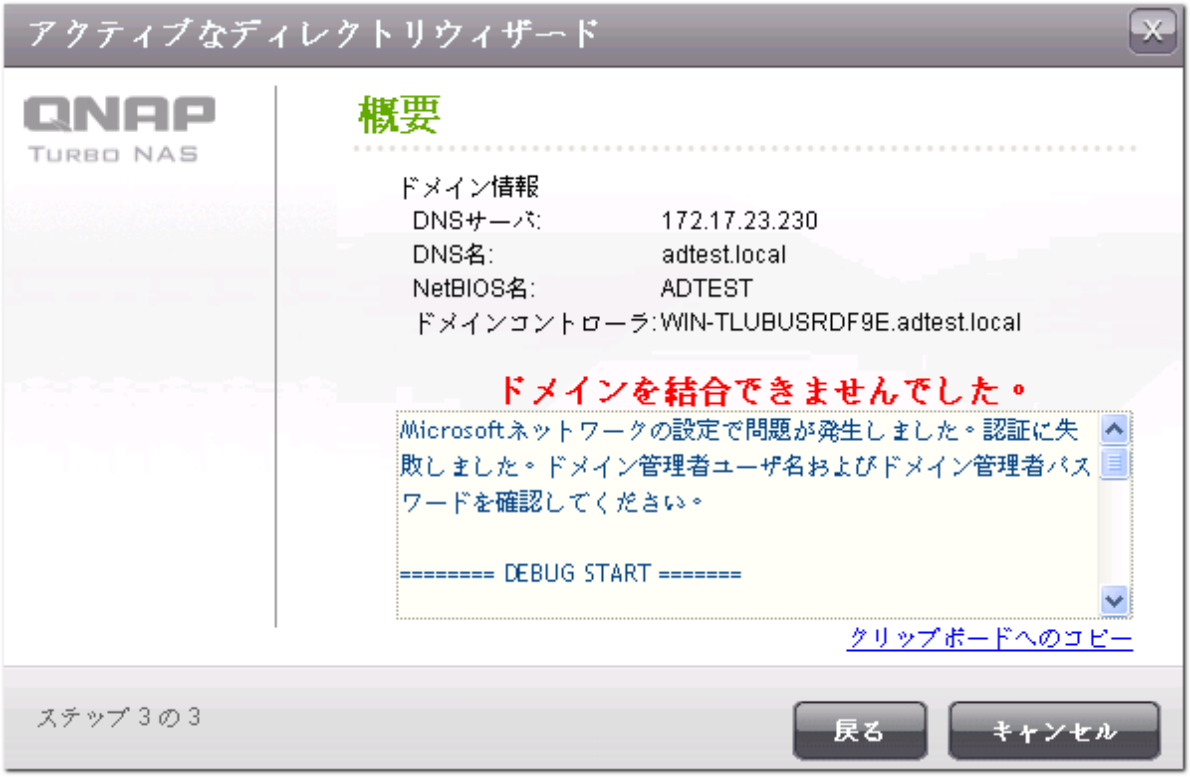


3. DNS（ドメイン名サービス）のドメイン名を入力します。ドメイン名を入力すると、NetBIOS名が自動的に生成されます。ドメインコントローラのDNSサーバーIPを指定します。IPは、アクティブディレクトリのDNSサーバーと同じにする必要があります。「NEXT（次へ）」をクリックします。

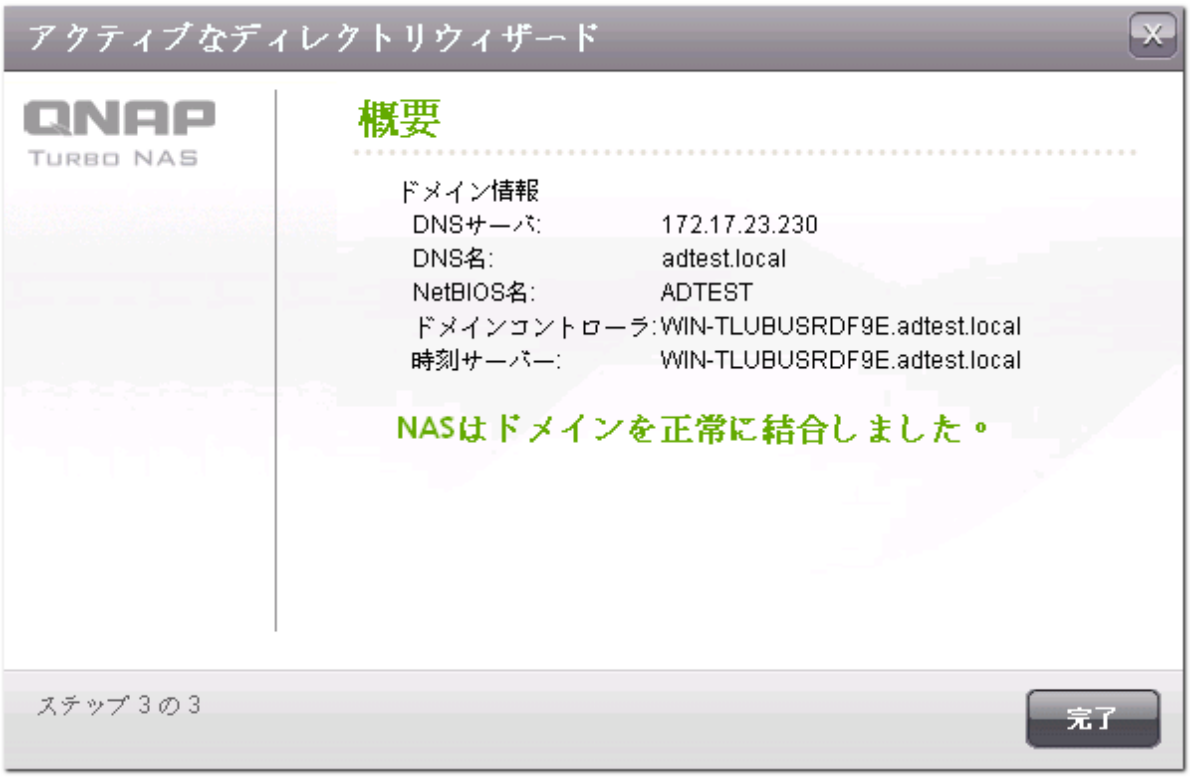
4. ドロップダウンメニューからドメインコントローラを選択します。ドメインコントローラは、NASとドメインサーバーおよびユーザー認証間の時刻同期に関与しています。ドメインの管理者名とパスワードを入力します。「JOIN（結合）」をクリックします。



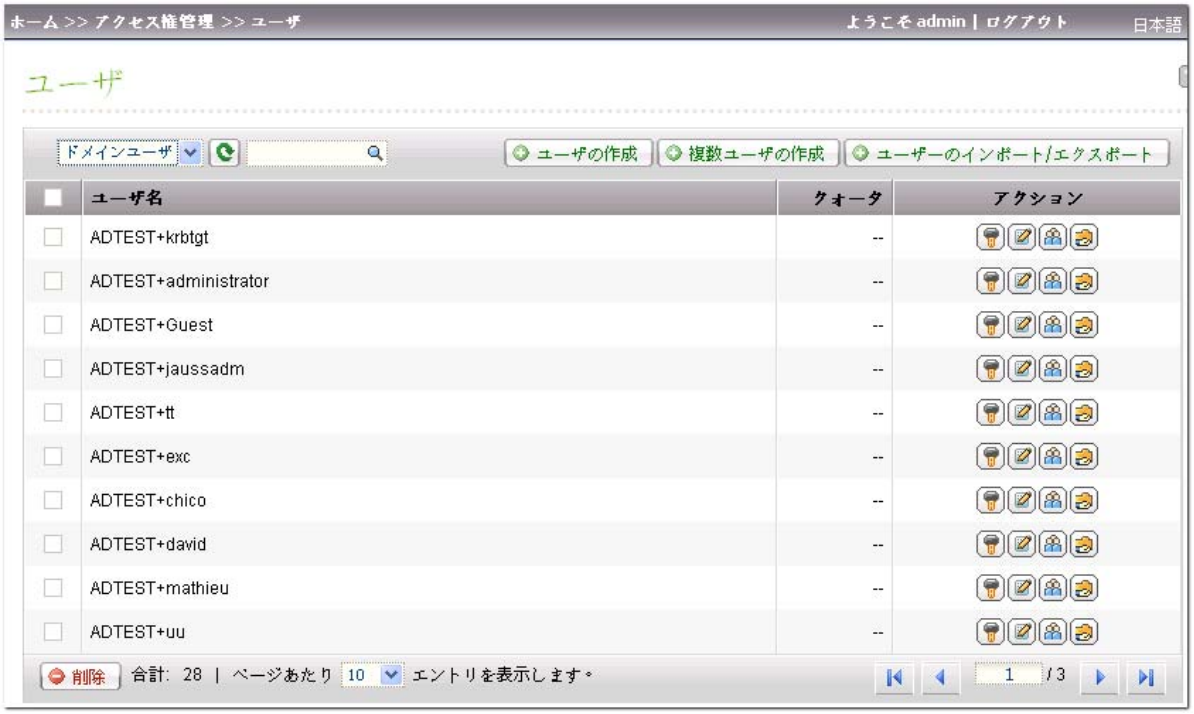
5. NAS がドメインへの参加に失敗した場合、エラーメッセージが表示されます。前のステップに戻り、設定を変更してください。



6. ドメインサーバーへのログインに成功すると、NAS はドメインに参加します。「Finish（完了）」をクリックして、ウィザードを終了します。

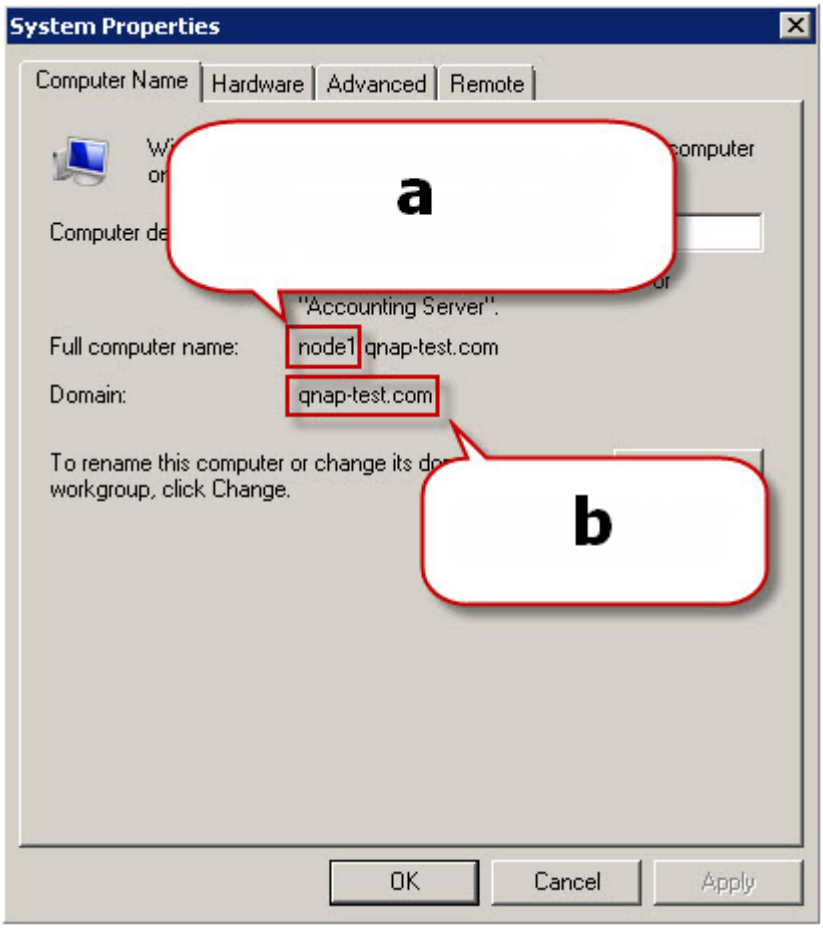


7. 「Access Right Management（アクセス権管理）」>「Users（ユーザー）」または「User Groups（ユーザーグループ）」にアクセスして、ドメインユーザーまたはユーザーグループをNASにロードできます。



Windows 2003

ADサーバ名およびADドメイン名を"System Properties" (システムプロパティ)内で確認できます。

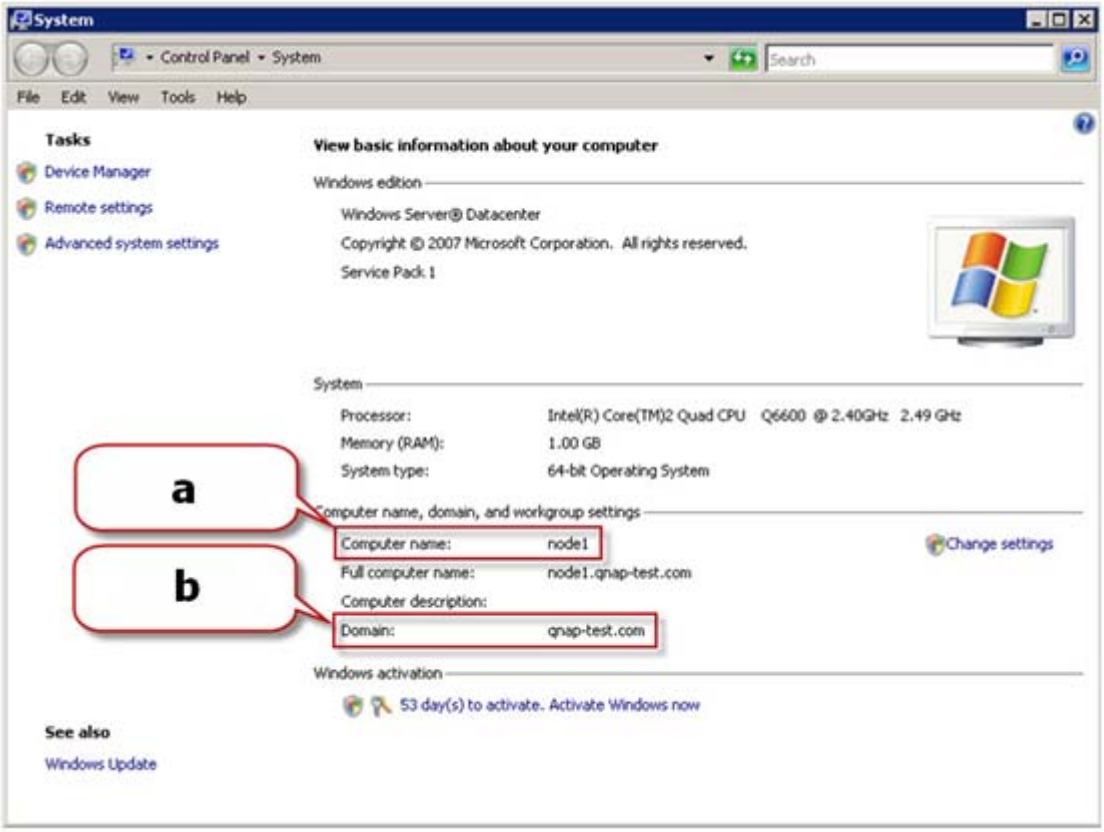


a. Windows 2003 サーバでは、ADサーバ名は "node 1" ,であり、"node1.qnap-test.com" ではありません。

b. ドメイン名は同じです。

Windows Server 2008

ADサーバ名およびADドメイン名を "Control Panel" (コントロールパネル) > "System" (システム) で確認できます。



a. これはユーザーの "AD server name" (ADサーバ名) です。
b. これはユーザーの "Domain name" (ドメイン名) です。

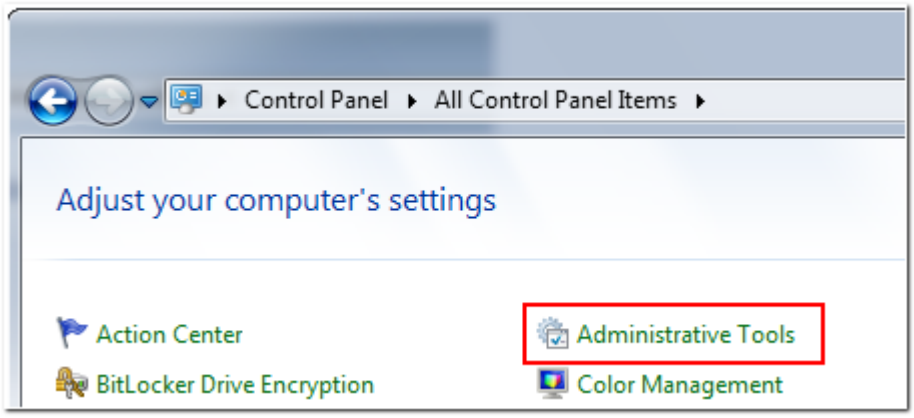
注:

- NASをActive Directoryに連結させた後、ADサーバーへのアクセス権を持つローカルのNASユーザーは、"NASname\username" (NAS名\ユーザー名) を使用してログインします。ADユーザーは、ご自分のユーザー名を使用してADサーバーにログインする必要があります。
- ローカルのNASユーザーおよびADユーザー (ドメイン名 + ユーザー名のユーザー名を使用します) は、AFP、FTP、Web File Manager、およびWebDAVを介して、NAS (ファームウェアバージョン 3.2.0以降) にアクセスできます。 ただし、NASのファームウェアバージョンが、3.2.0よりも前のバージョンである場合は、ローカルのNASユーザーのみがWeb File ManagerおよびWebDAVを介してNASにアクセスできます。
- TS-109/209/409/509シリーズTurbo NASについては、ADドメインがWindows 2008 Serverに基づく場合、NASのファームウェアは、バージョン2.1.2以降にアップデートする必要があります。

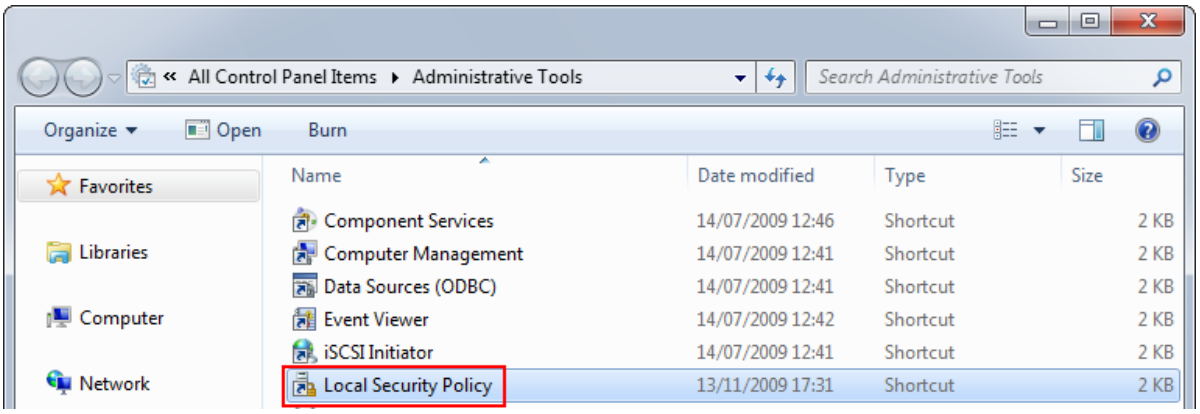
Windows 7

Active DirectoryのメンバーではないWindows 7 PCをご使用で、あなたのNASがADドメインメンバーであり、ファームウェアバージョンがv3.2.0より前のバージョンである場合は、PC設定を以下のように更して、ご使用のPCをNASにアクセスできるようにします。

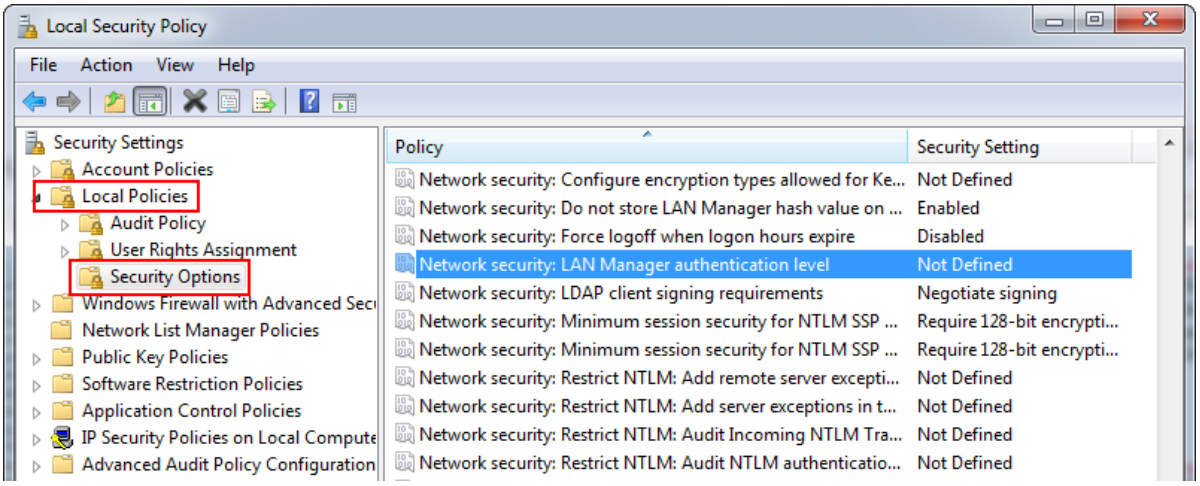
a. "Control Panel" (コントロールパネル) に移動し、"Administrative Tools" (管理ツール) をクリックします。



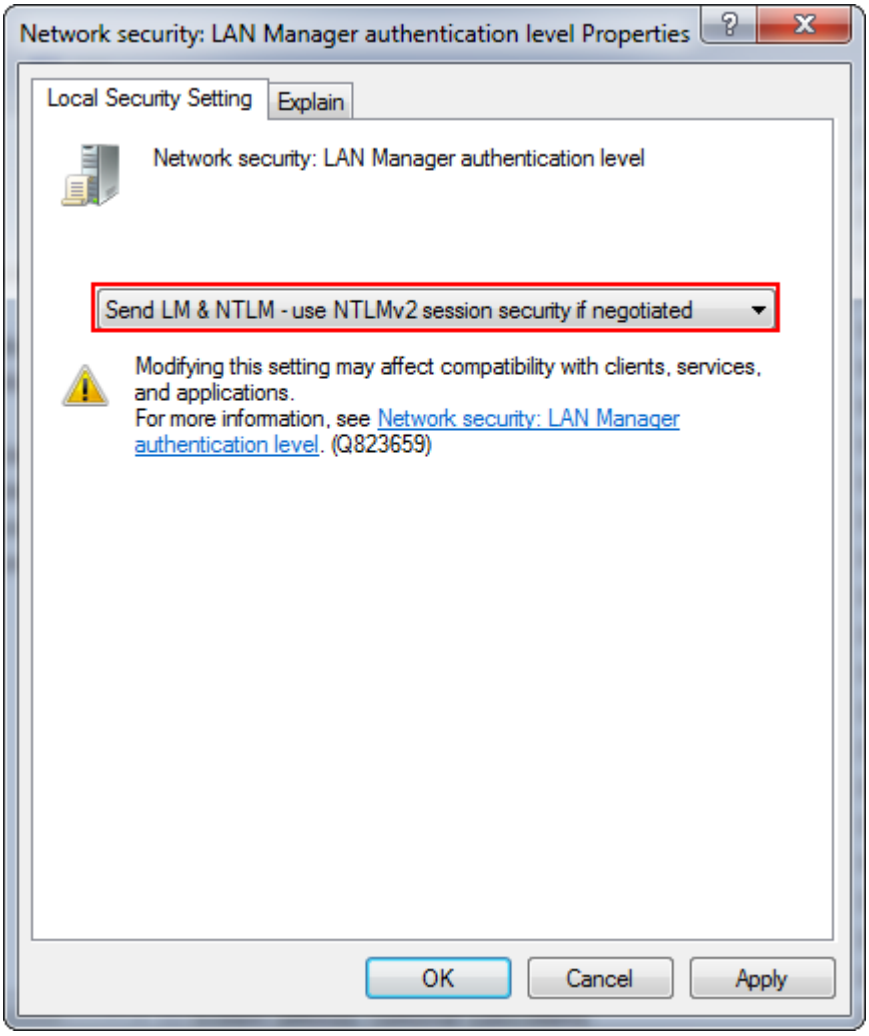
b. "Local Security Policy" (ローカルセキュリティポリシー) をクリックします。



c. "Local Policies" (ローカルセキュリティポリシー) > "Security Options" (セキュリティオプション) に移動します。 次に、"Network security: LAN Manager authentication level" (ネットワークセキュリティ: LAN Manager 認証レベル) を選択します。



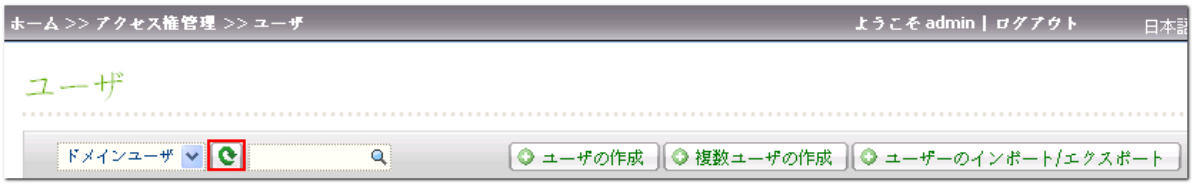
d. "Local Security Setting" (ローカル セキュリティの設定) タブを選択し、リストから "Send LM & NTLMv2 – use NTLMv2 session security if negotiated" (LM と NTLM を送信する - ネゴシエーションの場合、NTLMv2 セッション セキュリティを使う) を選択します。"OK"–をクリックします。



設定の確認

NASが正しくアクティブディレクトリに連携されているかどうかを確認するには、"Access Right Management"（アクセス権管理）> "Users"（ユーザー)に移動します。ユーザーとユーザーグループの一覧が、"Domain Users"（ドメインユーザー)および"Domain Groups"（ドメイングループ)のリストの中に表示されます。

ドメインに新しいユーザーまたはユーザーグループを作成した場合、"Access Right Management"（アクセス権管理）> "Users"（ユーザー)の "Domain Users"（ドメインユーザー)ドロップダウンメニュー、または"Access Right Management"（アクセス権管理）> "User Groups"（ユーザーグループ)の"Domain Groups"（ドメイングループ)ドロップダウンメニューの隣に位置する再ロードボタンをクリックすることができます。これによりアクティブディレクトリからNASにユーザーおよびユーザーグループリストを再ロードできます。ユーザー権限設定はドメインコントローラーを使用してリアルタイムで同期化されます。



5.1.2 NAS の LDAP ディレクトリへの接続

LDAP とは、ライトウェイトディレクトリアクセスプロトコルを表しています。 中央サーバー内に、すべてのユーザーおよびグループの情報を格納できるディレクトリです。 LDAP を使って、管理者は、LDAP ディレクトリ内のユーザーを管理することができ、ユーザーは、複数の NAS サーバーに同じユーザー名とパスワードで接続することができます。

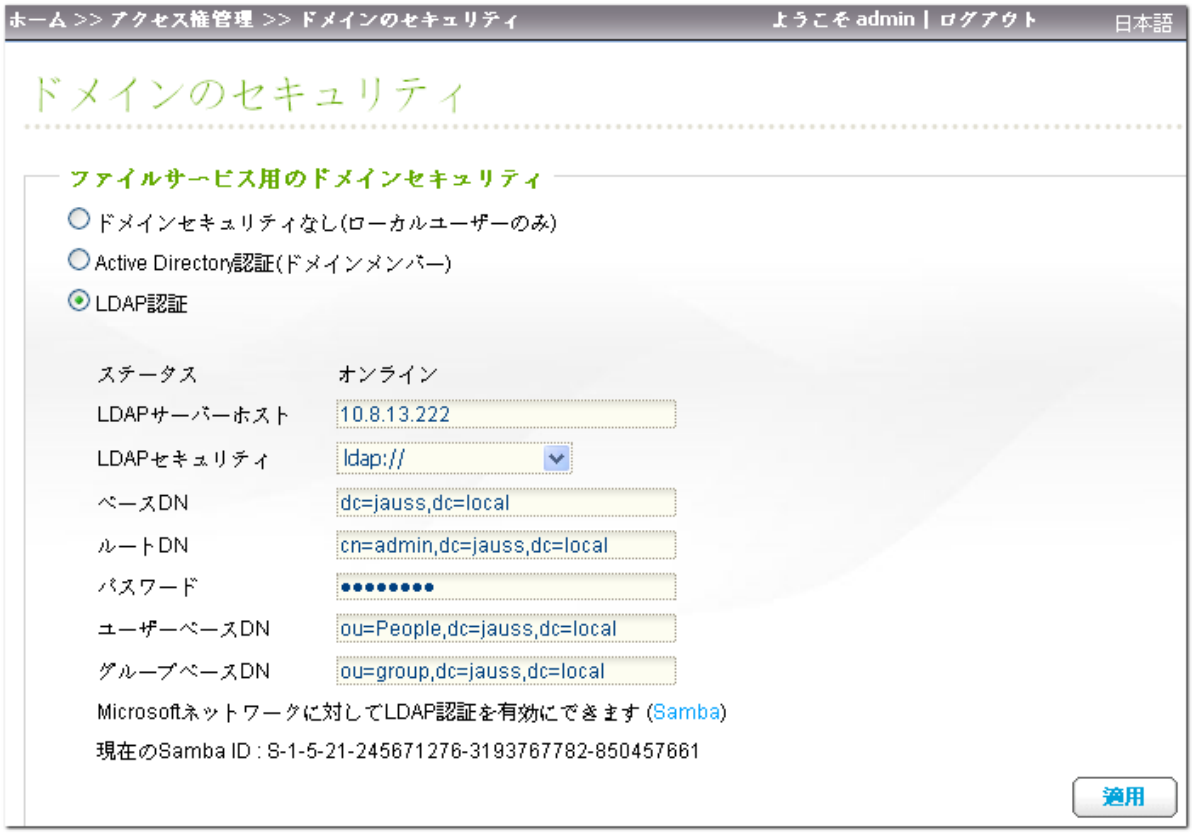
この機能は、Linux サーバー、LDAP サーバー、および Samba にいくらか知識のある管理者およびユーザーを対象にしています。 QNAP NAS の LDAP 機能を利用するには、稼働している LDAP サーバーが必要です。

必要な情報/設定:

- LDAP サーバーの接続情報および認証情報
- ユーザーおよびグループが格納される LDAP の構造
- LDAP サーバーのセキュリティ設定

次のステップを行い、QNAP NAS を LDAP ディレクトリに接続します。

1. NAS のウェブインターフェースに管理者としてログインします。
2. 「Access Right Management（アクセス権管理）」>「Domain Security（ドメインのセキュリティ）」と進みます。初期設定では、「No domain security（ドメイン無しのセキュリティ）」オプションが有効になっています。これは、ローカル NAS ユーザーのみが NAS にアクセスできることを意味します。
3. 「LDAP authentication（LDAP 認証）」を選択し、設定を行います。

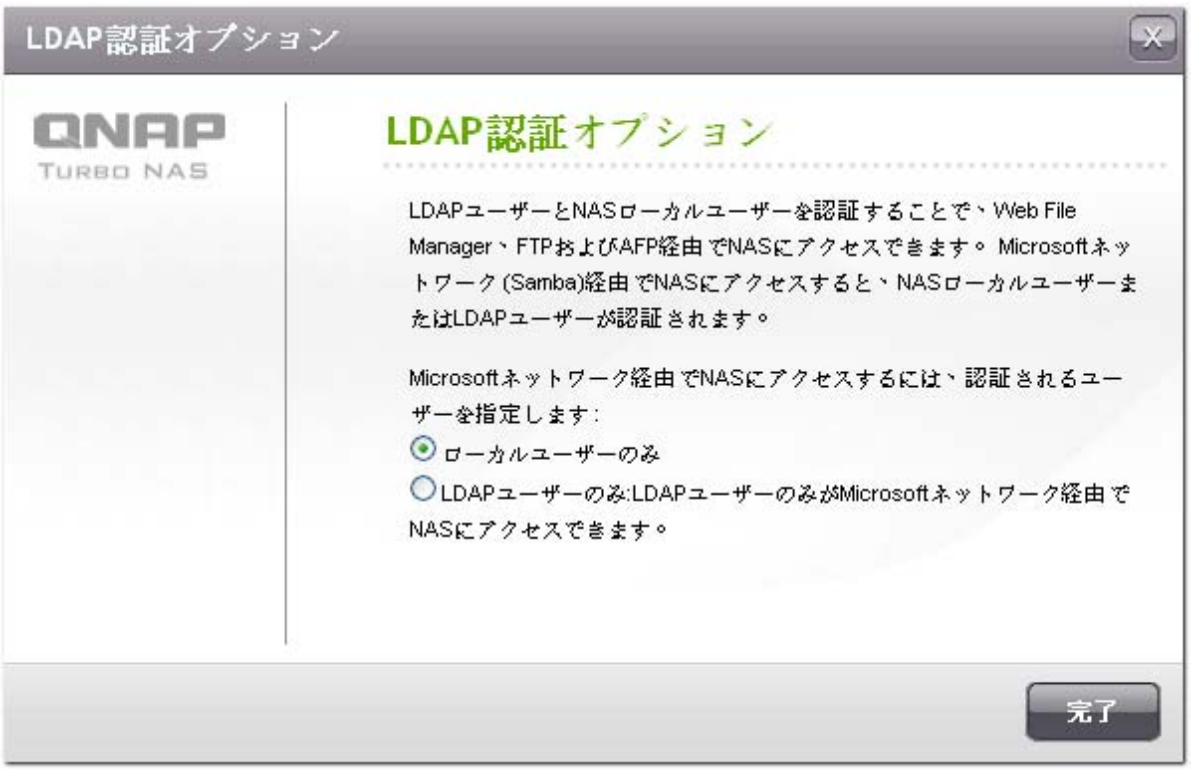


- LDAP サーバーホスト: LDAP サーバーのホスト名または IP アドレスです。
- LDAP セキュリティ: NAS の LDAP サーバーとの通信方法を指定します:
  - ✓ ldap:// = 標準 LDAP 接続を使用します (デフォルトポート: 389)。
  - ✓ ldap:// (ldap + SSL) = SSL で暗号化された接続を使用します (デフォルトポート: 686)。通常、旧バージョンの LDAP サーバーで使用します。
  - ✓ ldap:// (ldap + TLS) = TLS で暗号化された接続を使用します (デフォルトポート: 389)。通常、新バージョンの LDAP サーバーで使用します。
- BASE DN: LDAP ドメインです。例: dc=mydomain,dc=local
- Root DN: LDAP ルートユーザーです。例: cn=admin, dc=mydomain,dc=local
- パスワード: ルートユーザーのパスワードです。
- Users Base DN: ユーザーが格納されている OU (組織単位)です。例: ou=people,dc=mydomain,dc=local
- Groups Base DN: グループが格納されている OU (組織単位)です。例: ou=group,dc=mydomain,dc=local
- パスワード暗号化タイプ: LDAP サーバーがパスワードを格納する際の暗号化タイプを選択します。LDAP サーバーの設定と同一である必要があります。

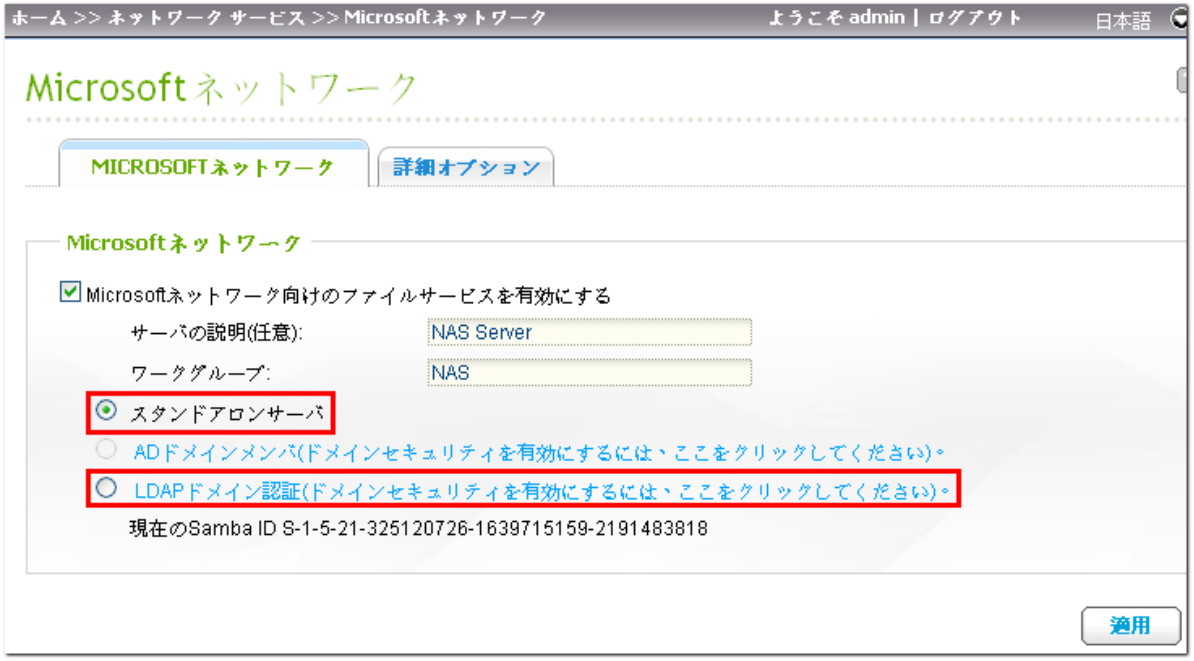
4. 「Apply (適用)」をクリックして、設定を保存します。設定に成功すると、NAS は、LDAP サーバーに接続できるようになります。

5. LDAP 認証オプションを設定します。
   - Microsoft ネットワーク方式が有効になっている場合（ネットワークサービス > Microsoft ネットワーク方式）、LDAP 設定を有効にする際、Microsoft ネットワーク方式（Samba）を経由して NAS にアクセスできるユーザーを指定します。
     - ✓ ローカルユーザーのみ：ローカル NAS ユーザーのみが、Microsoft ネットワーク方式を経由して NAS にアクセスできます。
     - ✓ LDAP ユーザーのみ：LDAP ユーザーのみが、Microsoft ネットワーク方式を経由して NAS にアクセスできます。.

注：LDAP ユーザーおよびローカル NAS ユーザーは、両者ともに、Web ファイルマネージャー、FTP、および AFP を経由して NAS にアクセスすることが可能です。



- Microsoft ネットワーク方式が有効な場合、NAS を LDAP サーバーに接続後、Microsoft ネットワーク方式用の認証タイプを選択します。
  - ✓ スタンドアロンサーバー：ローカル NAS ユーザーのみが、Microsoft ネットワーク方式を経由して NAS にアクセスできます。
  - ✓ LDAP ドメイン認証：LDAP ユーザーのみが、Microsoft ネットワーク方式を経由して NAS にアクセスできます。



6. NAS が LDAP ユーザーに接続されると、管理者は次を実行できます：
   - 「Access Right Management（アクセス権管理）」>「Users（ユーザ）」と進み、ドロップダウンメニューから「Domain Users（ドメインユーザ）」を選択します。LDAP ユーザーの一覧が表示されます。
   - 「Access Right Management（アクセス権管理）」>「User Groups（ユーザグループ）」と進み、ドロップダウンメニューから「Domain Groups（ドメイングループ）」を選択します。LDAP グループの一覧が表示されます。
   - 「Access Right Management（アクセス権管理）」>「Shared Folders（共有フォルダ）」>「Folder Permissions（フォルダ許可）」で、LDAP ドメインのユーザーまたはグループのフォルダ権限を指定します。

Microsoft ネットワークの LDAP 認証に関する技術的要件：

LDAP ユーザーを Microsoft ネットワーク（Samba）で認証するには次の項目が必要です：

1. LDAP サーバー内で LDAP と Samba 間のパスワードを同期させるサードパーティのソフトウェア。
2. Samba スキーマの LDAP ディレクトリへのインポート。

1） サードパーティソフトウェア：

Samba パスワードを含む LDAP ユーザーを管理できるソフトウェアはいくつかあります。例：

- LDAP Account Manager (LAM) ウェブベースのインターフェースで、以下で取得できます：http://www.ldap-account-manager.org/
- smbldap-tools（コマンドラインツール）
- webmin-ldap-useradmin - Webmin 用 LDAP ユーザー管理モジュール。

2） Samba スキーマ：

Samba スキーマを LDAP サーバーにインポートする方法は、LDAP サーバーの文書または FAQ を参照してください。
samba.schema ファイルが必要で、Samba ソース配布物の examples/LDAP ディレクトリ内にあります。

LDAP サーバーが稼働している Linux サーバー内の open-ldap の例（Linux のディストリビューションによって異なります）：

Samba スキーマをコピーします：

```
zcat /usr/share/doc/samba-doc/examples/LDAP/samba.schema.gz > /etc/ldap/schema/samba.schema
```

/etc/ldap/slapd.conf（openldap サーバー設定ファイル）を編集し、ファイル内に次の行があることを確認します：

```
include /etc/ldap/schema/samba.schema

include /etc/ldap/schema/cosine.schema

include /etc/ldap/schema/inetorgperson.schema

include /etc/ldap/schema/nis.schema
```

設定例:
以下は、設定の例です。これらは必須ではありませんし、LDAP サーバの設定と一致するように適応させる必要があります:

1. Linux OpenLDAP Server(Linux OpenLDAP サーバー)

Base DN: dc=qnap,dc=com
Root DN: cn=admin,dc=qnap,dc=com
Users Base DN: ou=people,dc=qnap,dc=com
Groups Base DN: ou=group,dc=qnap,dc=com

2. Mac Open Directory Server(Mac オープンディレクトリサーバー)

Base DN: dc=macserver,dc=qnap,dc=com
Root DN: uid=root,cn=users,dc=macserver,dc=qnap,dc=com
Users Base DN: cn=users,dc=macserver,dc=qnap,dc=com
Groups Base DN: cn=groups,dc=macserver,dc=qnap,dc=com

5.2 ユーザ

デフォルトでは、次のユーザがあらかじめ登録されています。

- admin

  フォルトのユーザadmin は、グループAdministrators のメンバで、システムを管理できます。ユーザadmin は削除できません。

- guest

  登録されていないユーザ名が使用された場合、本製品はそれをゲストと認め、限定的なアクセスを許可します。ユーザGuest はどのグループにも所属しません。ユーザguest は削除できません。またパスワードも更できません。「guest」のログインパスワードはguestです。

- Anonymous

  FTP サービスによってサーバに接続する場合、Guest としてログインすることができます。ユーザAnonymous は削除できません。またパスワードも更できません。

NASで作成できるユーザー数は、NAS機種によって異なります。NASモデルが一覧にない場合、http://www.qnap.com にアクセスして詳細をご確認ください。

最大ユーザー数	NASモデル
1,024	TS-110、TS-210
2,048	TS-112, TS-119, TS-119P+, TS-212, TS-219P+, TS-410, TS-239 Pro II+, TS-259 Pro+
4,096	TS-412, TS-419P+, TS-410U, TS-419U, TS-412U, TS-419U+, SS-439 Pro, SS-839 Pro, TS-439 Pro II+, TS-459U-RP/SP, TS-459U-RP+/SP+, TS-459 Pro+, TS-459 Pro II, TS-559 Pro+, TS-559 Pro II, TS-659 Pro+, TS-659 Pro II, TS-859 Pro+, TS-859U-RP, TS-859U-RP+, TS-809 Pro, TS-809U-RP, TS-879 Pro, TS-1079 Pro, TS-879U-RP, TS-EC879U-RP, TS-1279U-RP, TS-EC1279U-RP

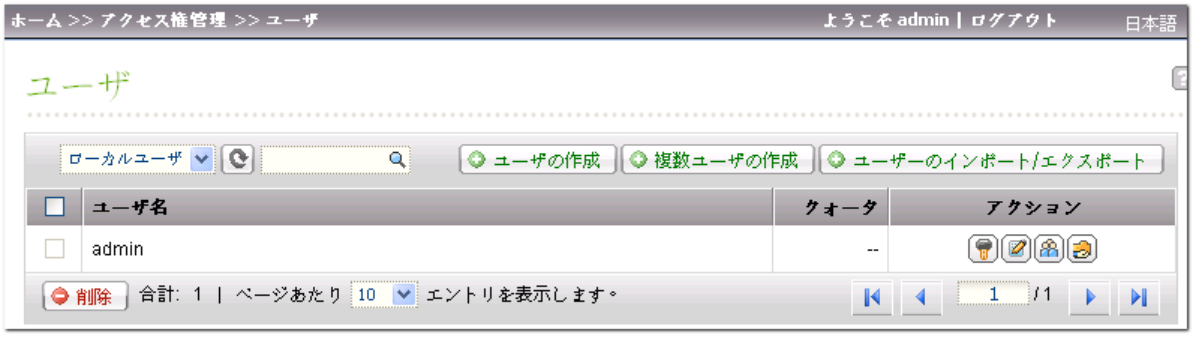
ユーザ名

ユーザ名は、大文字小文字を区別しません。2 バイト文字 (例えば、日本語、国語、韓国語等は使用できます。半角32 文字以内の文字です。次の特殊文字は使用できません。

" / \ [ ] : ; | = , + * ? < > ` '

パスワード

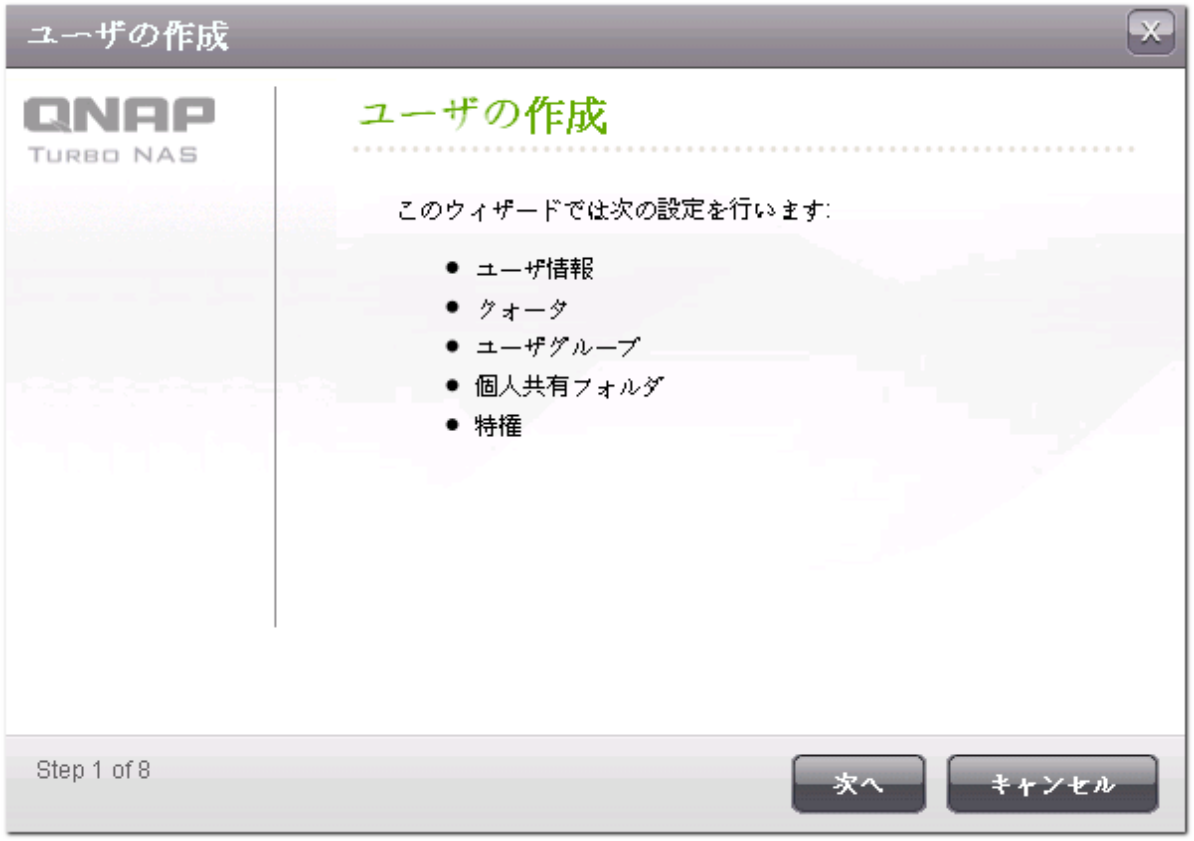
大文字小文字を区別します16 文字以内の文字です。セキュリティのため、少なくともパスワード6 文字以上を設定してください。



ユーザの作成

NASでユーザーを作成するには、「Create a User（ユーザの作成）」をクリックします。

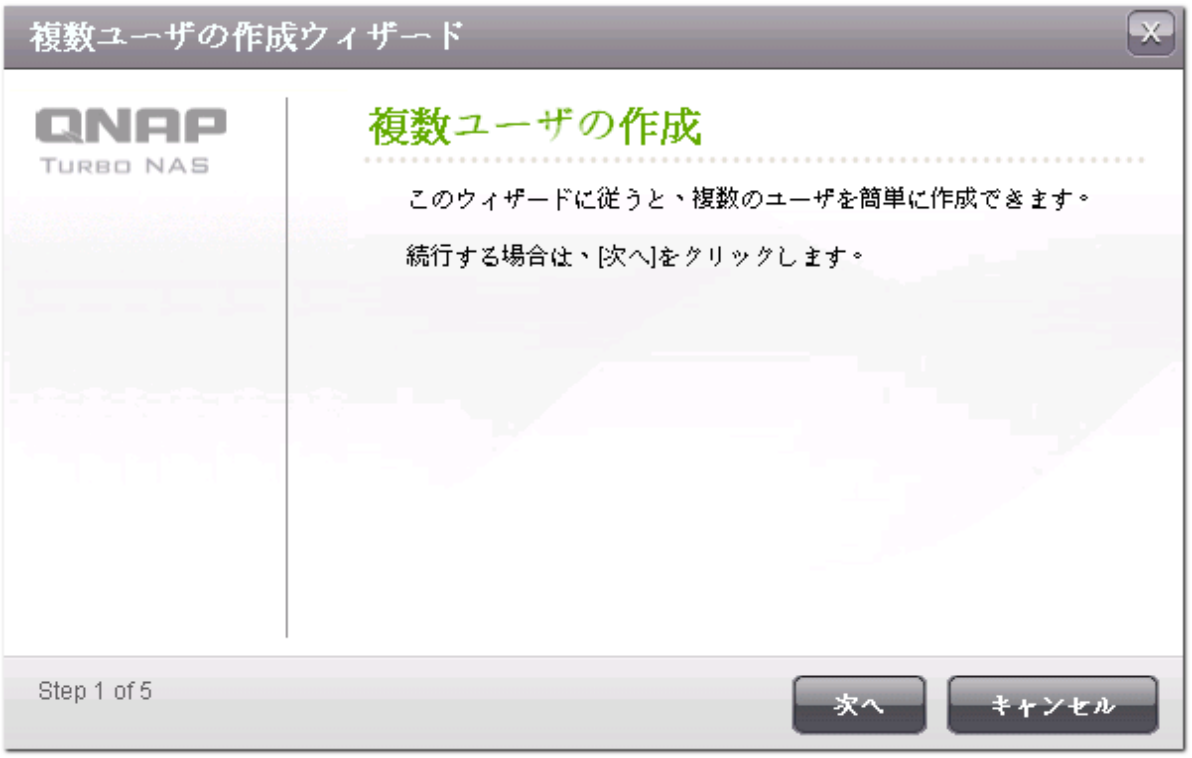
ウィザードの指示に従い、詳細を完成します。



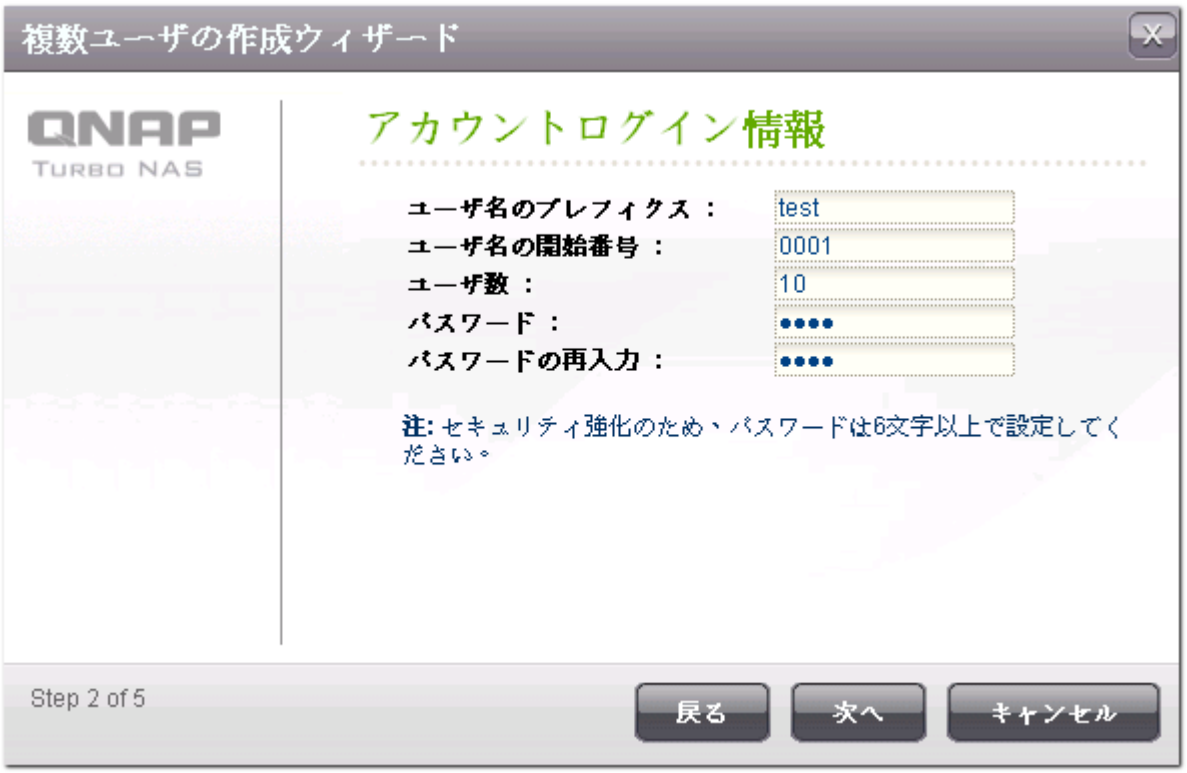
複数のユーザーの作成

NASで複数のユーザーを作成するには、「Create Multiple Users（複数ユーザの作成）」をクリックします。

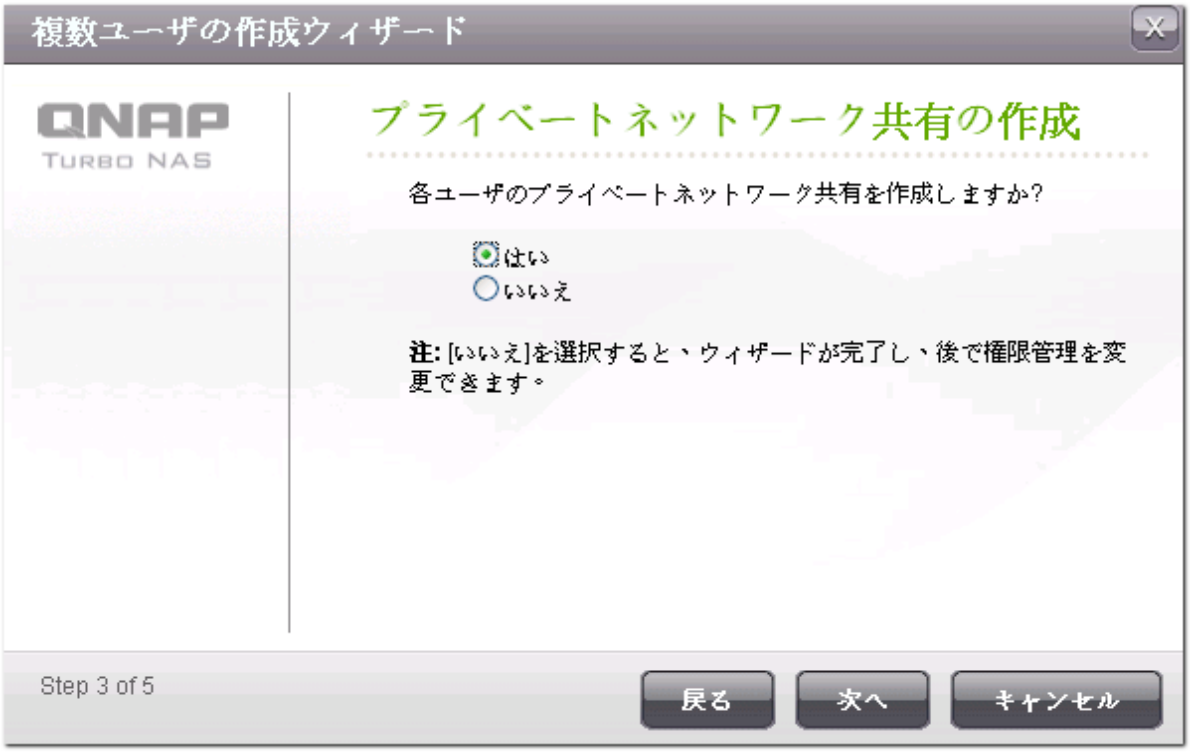
「Next（次へ」をクリックします。



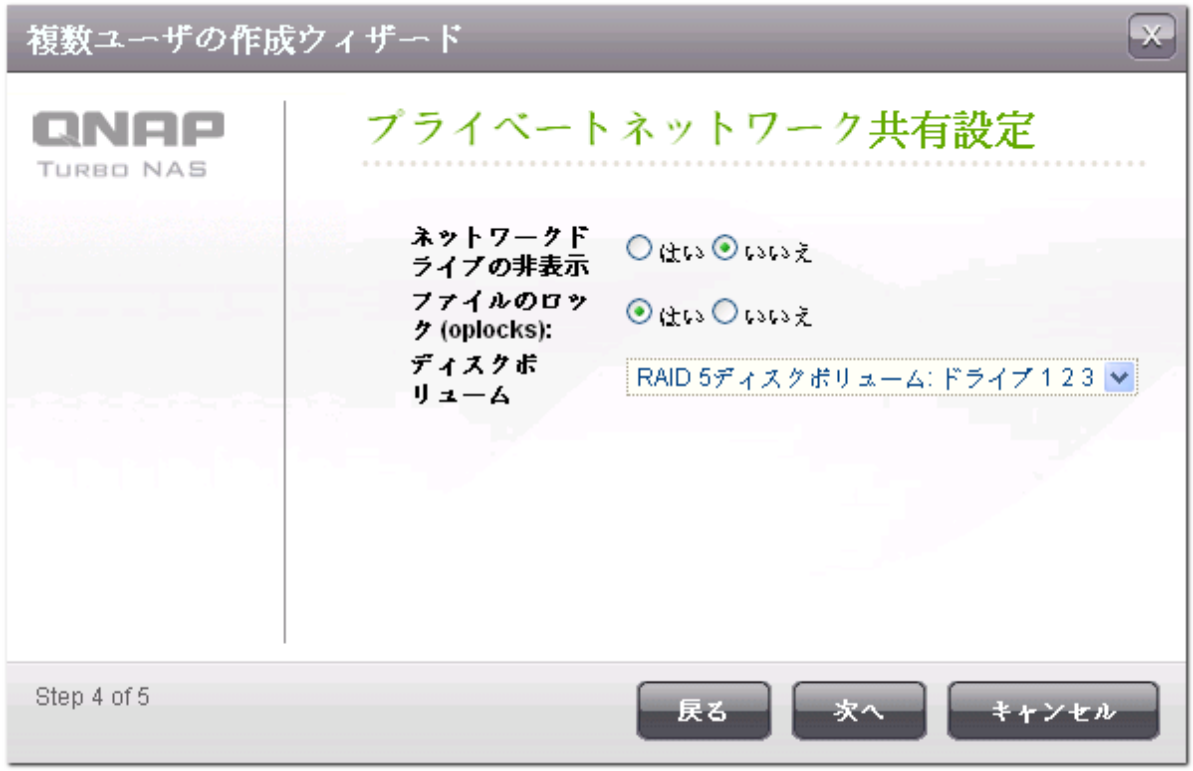
名前の接頭辞、たとえばtestを入力します。ユーザー名の開始番号、たとえば0001、および作成するユーザーの番号、たとえば10を入力します。NASはtest0001、test0002、test0003…test0010という名前のユーザーを作成します。ここに入力するパスワードは、すべての新しいユーザーに対して同じです。



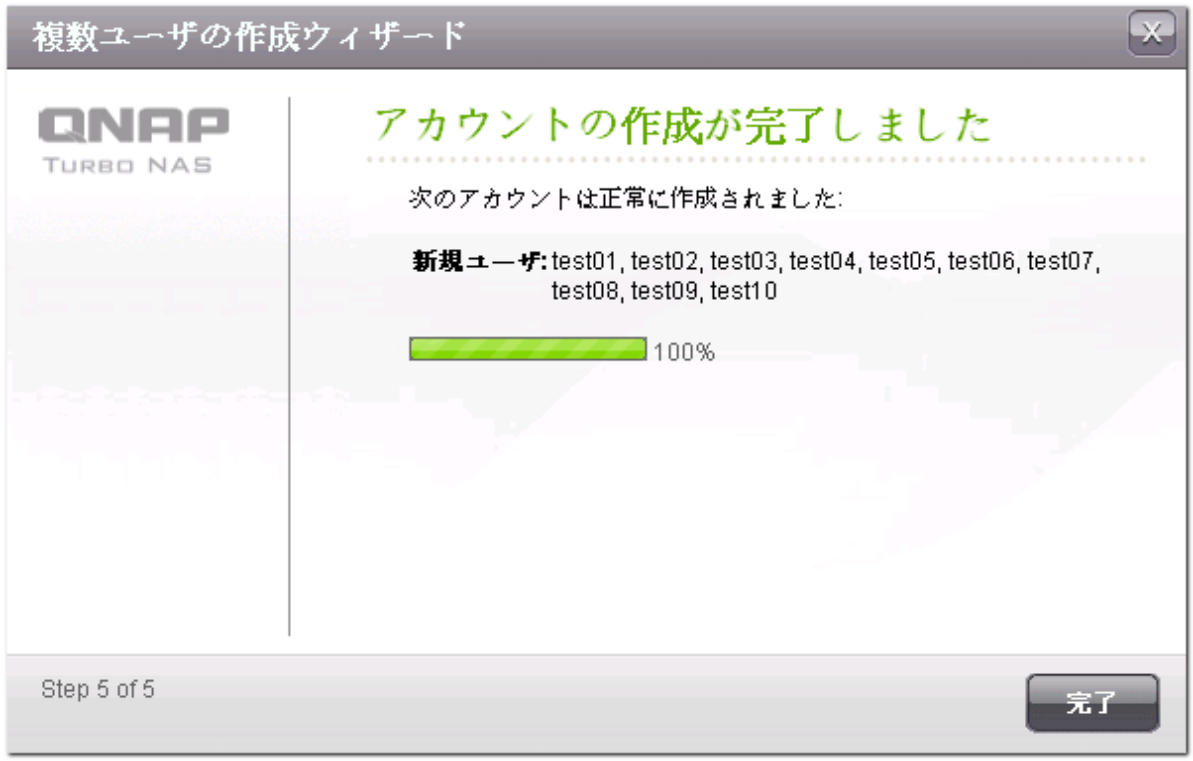
各ユーザーのプライベートネットワーク共有を作成するかしないかを選択します。ネットワーク共有はユーザー名の後で名前が付けられます。同じ名前のネットワーク共有がすでに存在する場合、NASはフォルダを作成しません。



フォルダ設定を指定します。



最後の手順で作成した新規ユーザーを表示できます。「FINISH（終了）」をクリックしてウィザードを終了します。



ユーザーが作成されたことを確認します。

ユーザーのネットワーク共有が作成されたことを確認します。

ユーザーのインポート/エクスポート

このシステムでは、NASとユーザー間でインポート/エクスポートを実行できます。

注: ユーザーリストをインポートしているとき、パスワード規則（適用可能な場合）は適用されません。

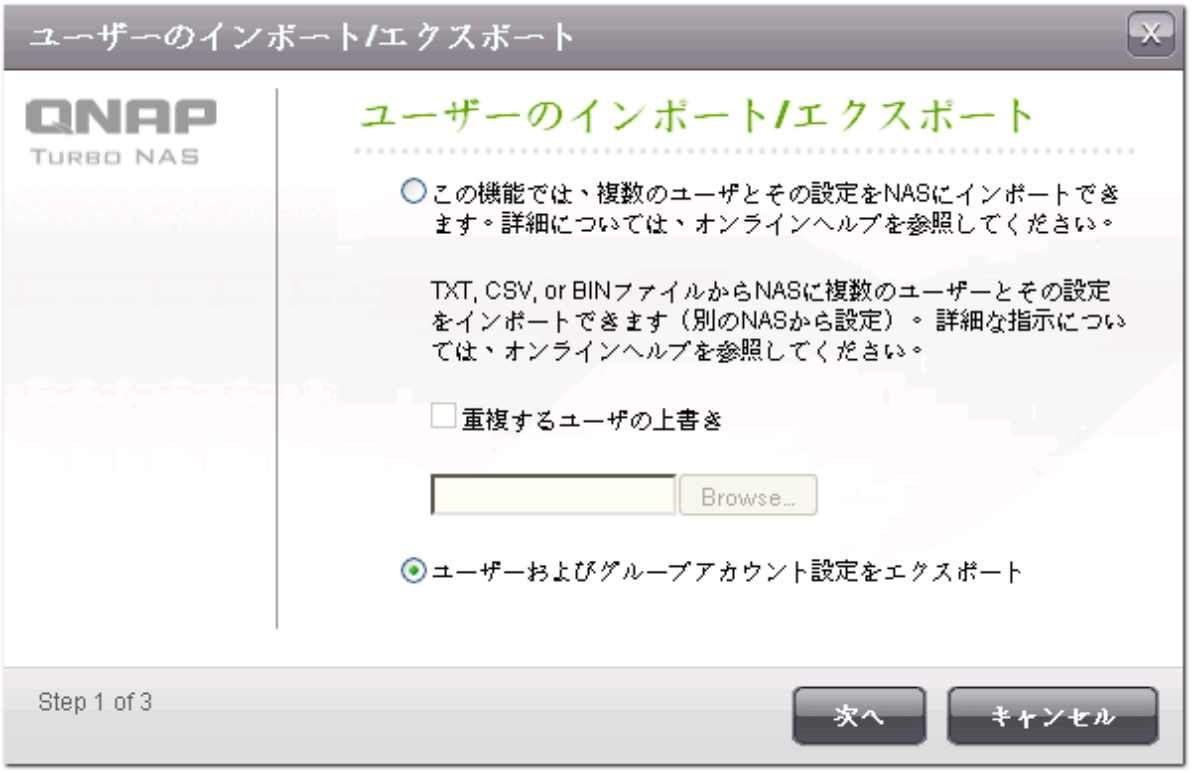
ユーザーのエクスポート

以下の手順に従って、NASからユーザーをエクスポートします。

1. 「Import/Export Users（ユーザーのインポート/エクスポート）」をクリックします。

2. 「Export user and user group settings（ユーザーとユーザーグループ設定のエクスポート）」のオプションを選択します。

3. 「NEXT（次へ）」をクリックして、アカウント設定ファイル(*.bin)をダウンロードし保存します。アカウントセットアップの場合、ファイルは別のNASにインポートできます。



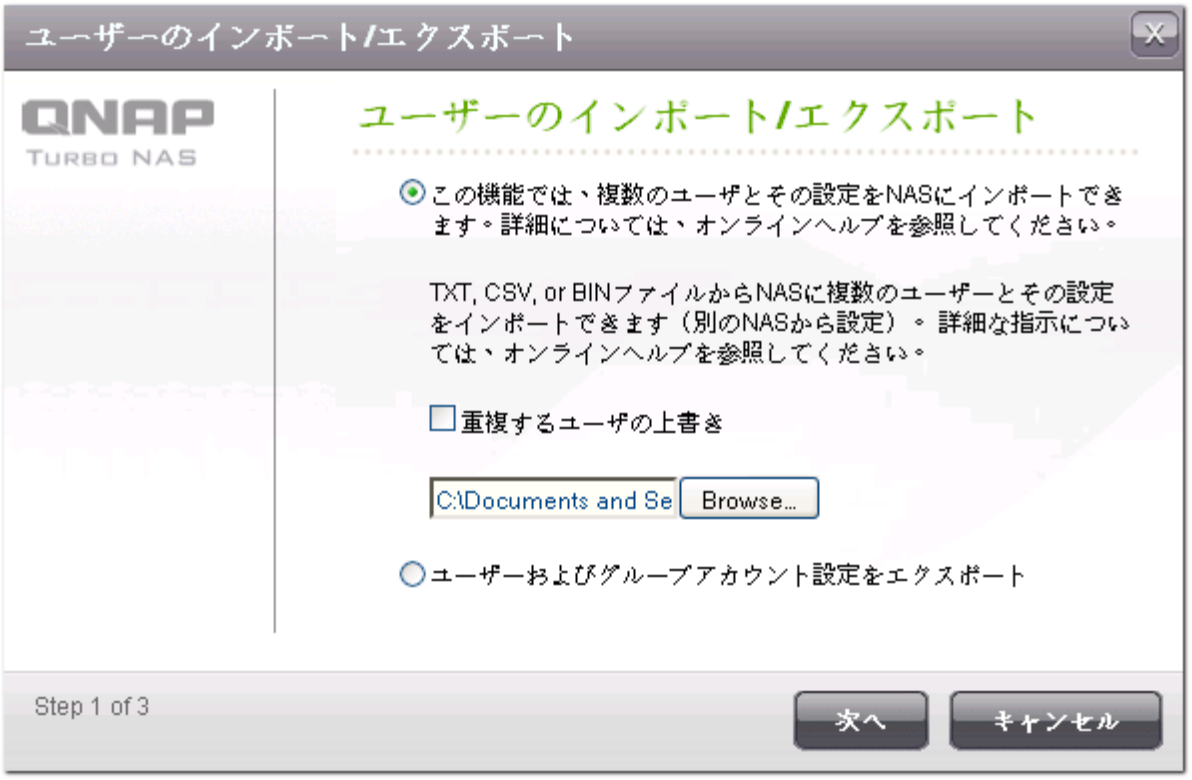
クォータ機能が「Access Right Management（アクセス権管理）」>「Quota（クォータ）」で有効になっているとき、クォータ設定をエクスポートできます。

ユーザーのインポート

NASにユーザーをインポートする前に、ユーザーをエクスポートすることでユーザー設定をバックアップしていることを確認してください。以下の手順に従って、NASにユーザーをインポートします。

1. 「Import/Export Users（ユーザーのインポート/エクスポート）」をクリックします。

2. 「Import user and user group settings（）」のオプションを選択します。「Overwrite duplicate users（重複ユーザーの上書き）」オプションを選択して、NASに既存のユーザーを上書きします。

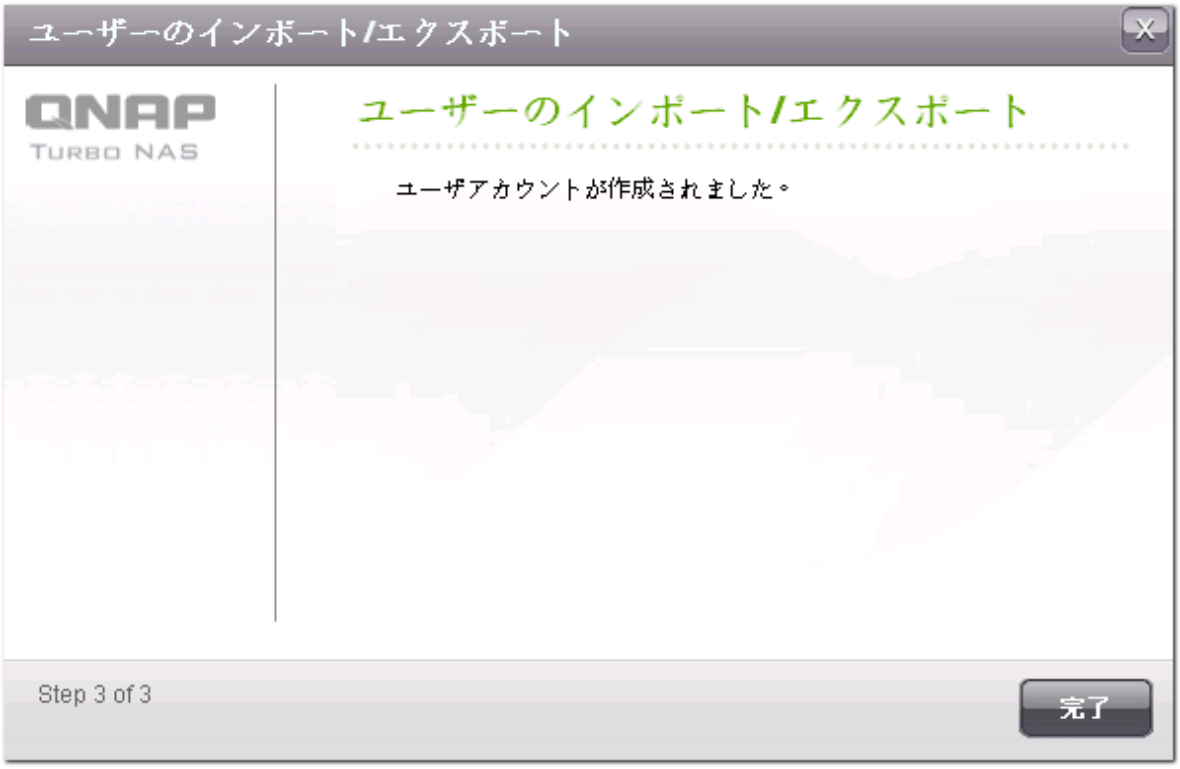


3. 「Browse（閲覧）」をクリックして、ユーザー情報を含むファイル(*.TXT、*.CSV、*.BIN)を選択します。「NEXT（次へ）」をクリックしてユーザーをインポートします。

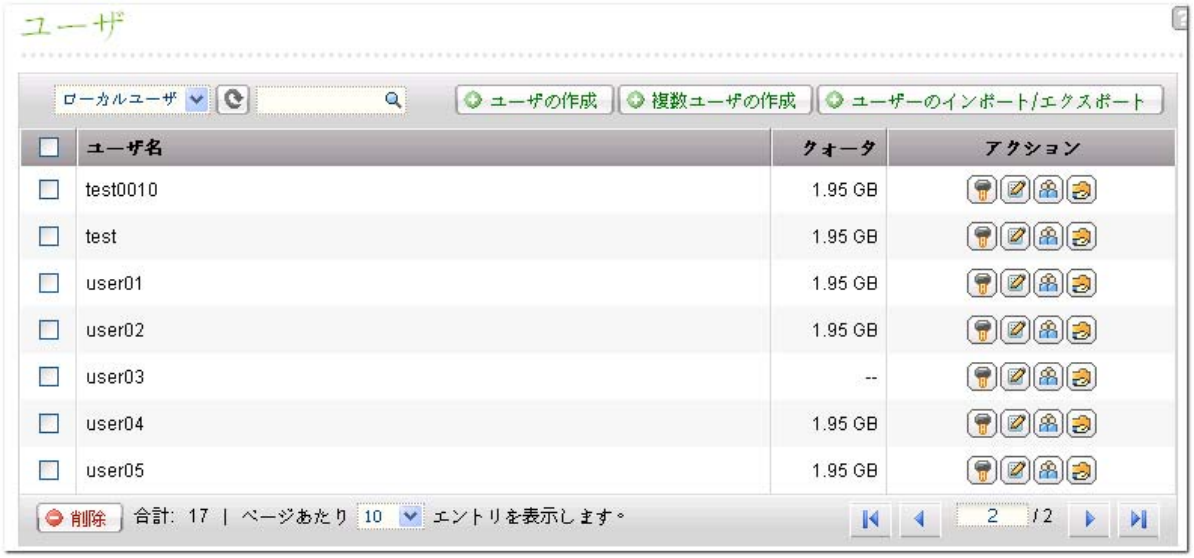
4. インポートされたユーザーのリストが表示されます。赤でハイライトされた、異常な状態のユーザーは、スキップされます。BINファイルによりユーザーをインポートする場合、この手順は表示されません。

5. 「NEXT（次へ）」をクリックしてユーザーアカウントを作成します。

6. ユーザーが作成されたら、「Finish（終了）」をクリックします。



7. インポートしたユーザーアカウントが表示されます。

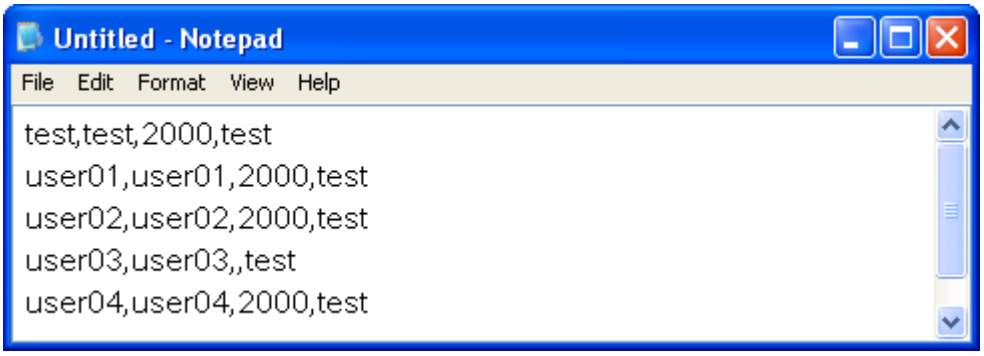


NASはTXT、CSVまたはBINファイルからユーザーアカウントのインポートをサポートします。これらのファイルタイプでユーザーアカウントのリストを作成するには、以下の手順に従います。

TXT

1. テキストエディターで新規ファイルを開きます。
2. ユーザーの情報を以下の情報で入力し、"," で区切ります: ユーザー名、パスワード、クォータ(MB)、グループ名
3. 次の行に移動し、前のステップを繰り返して他のユーザーアカウントを作成します。各行一人ずつのユーザーの情報を示します。
4. 全角文字を含むファイルはUTF-8エンコードで保存します。

下記はその例です。 クォータが空白のままの場合、ユーザーはNASのディスク容量を無制限に使用することができます。



CSV (Excel)

1. Excelで新規ファイルを開きます。
2. ユーザーの情報を同じ列に以下の順番で入力します:
   行A: ユーザー名
   行B: パスワード
   行C: クォータ(MB)
   行D: グループ名
3. 次の列に移動し、前のステップを繰り返して他のユーザーアカウントを作成します。各列一人ずつのユーザーの情報を示します。ファイルをcsv形式で保存します。
4. 全角文字を含むcsvファイルはノートパッドで開き、UTF-8エンコードで保存します。

下記はその例です:

	A	B	C	D
1	test	test	2000	test
2	user01	user01	2000	test
3	user02	user02	2000	test
4	user03	user03		test
5	user04	user04	2000	test
6	user05	user05	2000	test

BIN (NASからエクスポート)
BINファイルは、QNAP NASからエクスポートされます。ユーザー名、パスワード、クォータ、ユーザーグループを含む情報が含まれます。クォータ機能が「Access Right Management(アクセス権管理)」>「Quota(クォータ)」で有効になっているとき、クォータ設定をエクスポートできます。

5.3 ユーザグループ

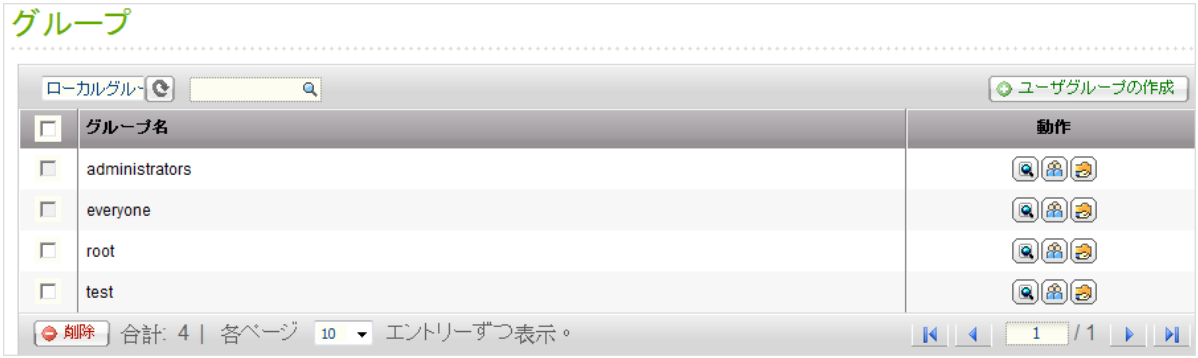
簡単にアクセス権を設定、更できるように、ユーザを作成したら、グループ化します。ファイルまたはフォルダへの同じアクセス権を与えるユーザを1つのグループにまとめます。デフォルトでは、次のグループがあらかじめ登録されています。

Administrators
グループAdministrators の全メンバは、システムを管理できます。グループAdministrators は削除できません。
Everyone
全てのユーザはグループEveryone に所属します。グループEveryone に所属しないような設定はできませんし、グループEveryone は削除できません。

NASで作成できるユーザーグループ数は、NAS機種によって異なります。NASモデルが一覧にない場合、http://www.qnap.com にアクセスして詳細をご確認ください。

最大ユーザーグループ数	NASモデル
128	TS-110、TS-210
256	TS-112, TS-119, TS-119P+, TS-212, TS-219P+, TS-410, TS-239 Pro II+, TS-259 Pro+
512	TS-412, TS-419P+, TS-410U, TS-419U, TS-412U, TS-419U+, SS-439 Pro, SS-839 Pro, TS-439 Pro II+, TS-459U-RP/SP, TS-459U-RP+/SP+, TS-459 Pro+, TS-459 Pro II, TS-559 Pro+, TS-559 Pro II, TS-659 Pro+, TS-659 Pro II, TS-859 Pro+, TS-859U-RP, TS-859U-RP+, TS-809 Pro, TS-809U-RP, TS-879 Pro, TS-1079 Pro, TS-879U-RP, TS-EC879U-RP, TS-1279U-RP, TS-EC1279U-RP

グループ名は半角256 以内の文字です。2 バイト文字 (例えば、日本語、国語、韓国語等は使用できます。次の特殊文字は使用できません。
" / \ [ ] : ; | = , + * ? < > ` '



5.4 共有フォルダ

共フォルダ

ファイルの共により、OS やマシンの違いを超えて同じ情報にアクセスしたり、同じ環境で作業したりできます。

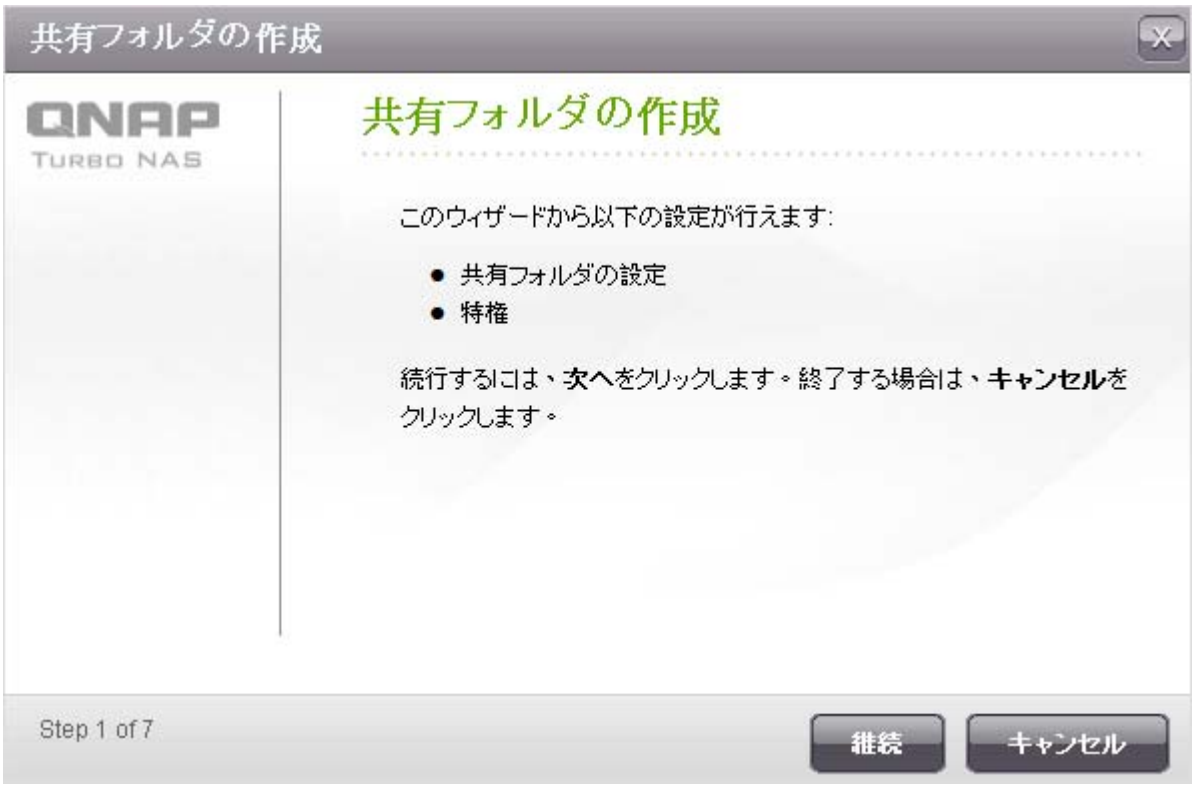
NASで作成できる共フォルダ数は、NAS機種によって異なります。NASモデルが一覧にない場合、http://www.qnap.com にアクセスして詳細をご確認ください。

最大共有フォルダ数	NASモデル
256	TS-110, TS-210, TS-112, TS-119, TS-119P+, TS-212, TS-219P+, TS-410, TS-239 Pro II+, TS-259 Pro+
512	TS-412, TS-419P+, TS-410U, TS-419U, TS-412U, TS-419U+, SS-439 Pro, SS-839 Pro, TS-439 Pro II+, TS-459U-RP/SP, TS-459U-RP+/SP+, TS-459 Pro+, TS-459 Pro II, TS-559 Pro+, TS-559 Pro II, TS-659 Pro+, TS-659 Pro II, TS-859 Pro+, TS-859U-RP, TS-859U-RP+, TS-809 Pro, TS-809U-RP, TS-879 Pro, TS-1079 Pro, TS-879U-RP, TS-EC879U-RP, TS-1279U-RP, TS-EC1279U-RP

共フォルダ一覧にて、現在のデータサイズ、サブフォルダおよびネットワーク共有内に作成されたファイルの数、またフォルダステータス(非表示かどうか)を表示することができます。

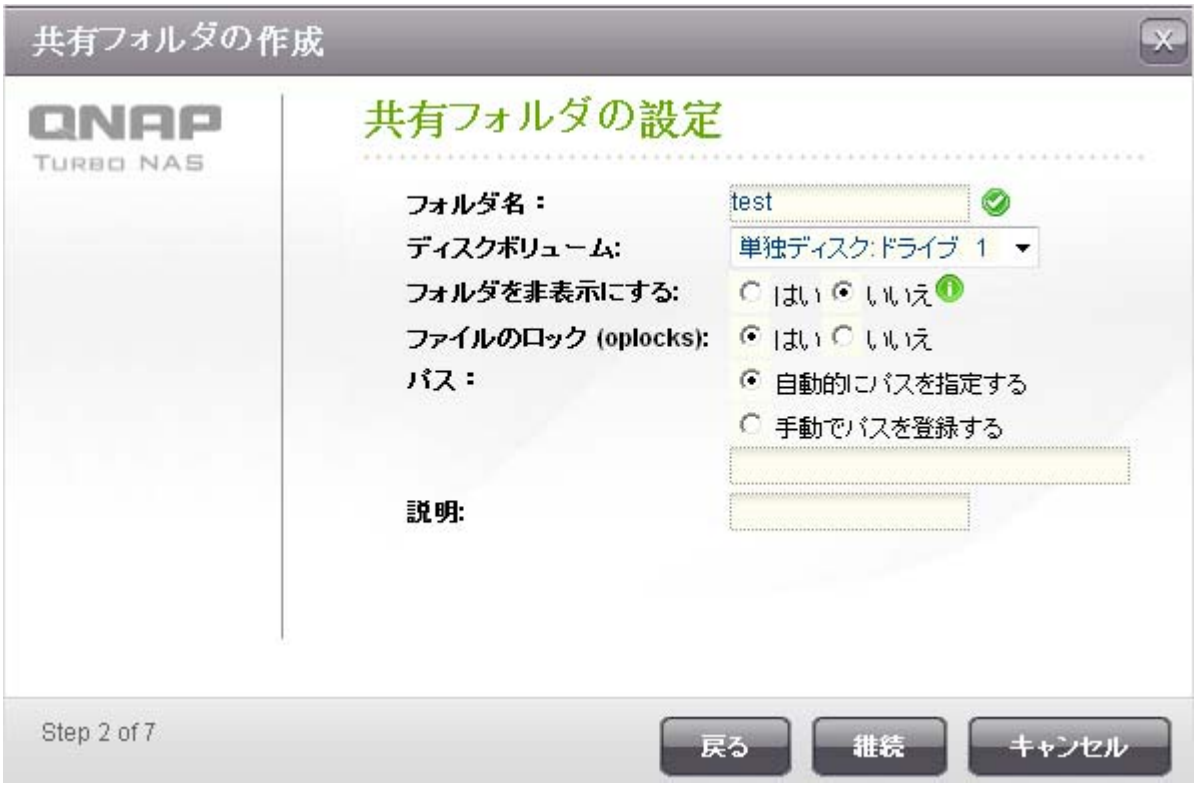
共フォルダを作成するには、"New Share Folder" (新規共有フォルダ)をクリックします。

"Next" (次へ)をクリックします。

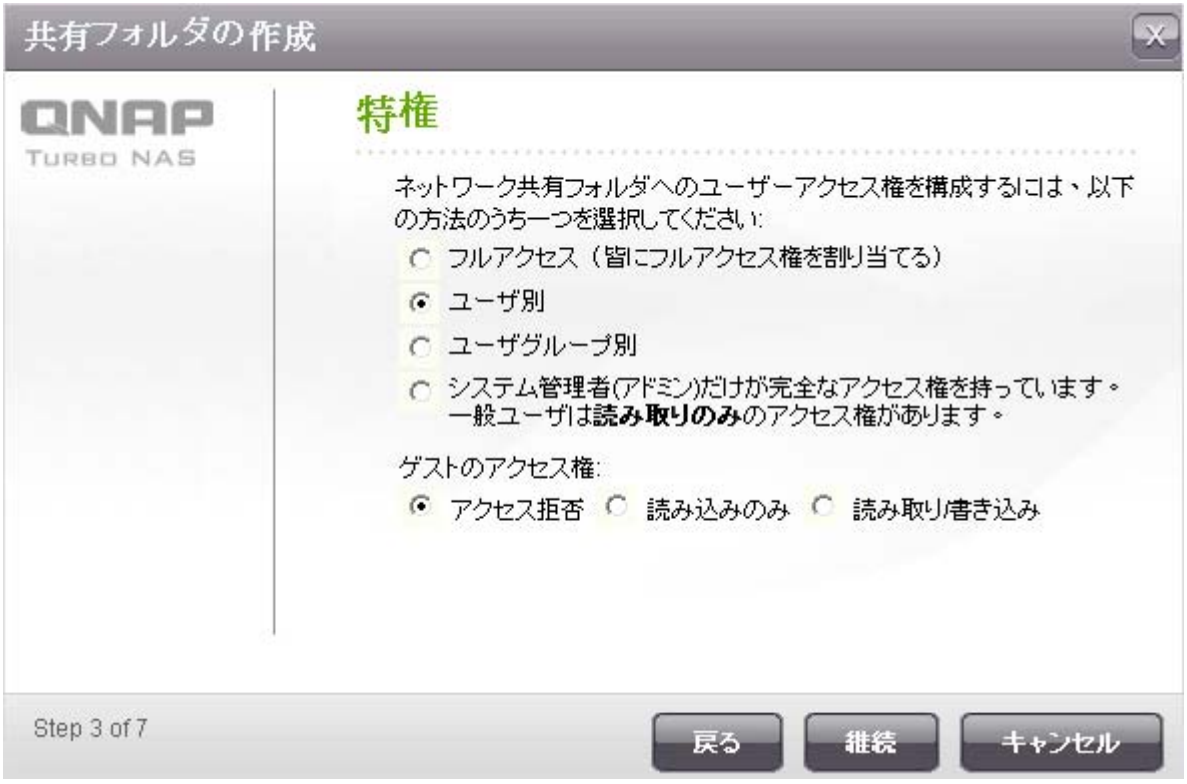


共フォルダ設定を入力します。

- フォルダ名:共フォルダ名を入力します。共フォルダ名には以下の記号は使用できません。" / ¥ [ ] : ; | = , + * ? < > ` '
- フォルダの非表示:Microsoft ネットワークにて、フォルダを非表示にするかを選択します。フォルダが非表示の場合は、フォルダにアクセスする際は完全なディレクトリ¥¥NAS_IP¥フォルダ_名　を入力する必要があります。
- ファイルプロテクト(oplocks): Opportunistic LockingはWindowsによる機構です。クライアントはopportunistic lock (oplock) をサーバ上のファイルに設定し、データをローカルでキャッシュしてパフォーマンスを向上させることができます。デフォルトでは、日常使用において効となっています。データベースなど、複数のユーザーが同時に同一のファイルへアクセスする必要があるネットワークに対しては、oplocksは無効にしてください。
- パス:フォルダのパスを特定、あるいはNASが自動的にパスを特定するよう選択します。
- 説明:オプションでこのフォルダの説明を入力します。

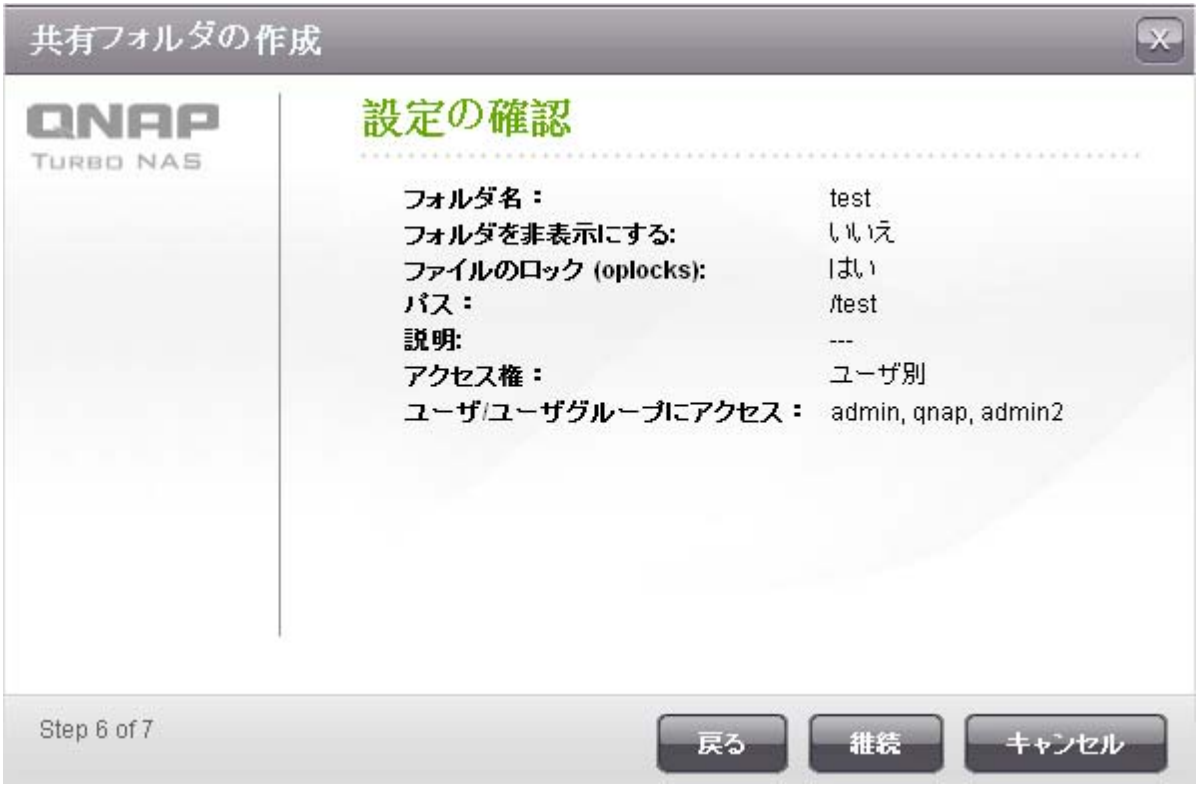


フォルダへのアクセス権限をどのように特定するかを選択し、ゲストのアクセス権限を特定します。

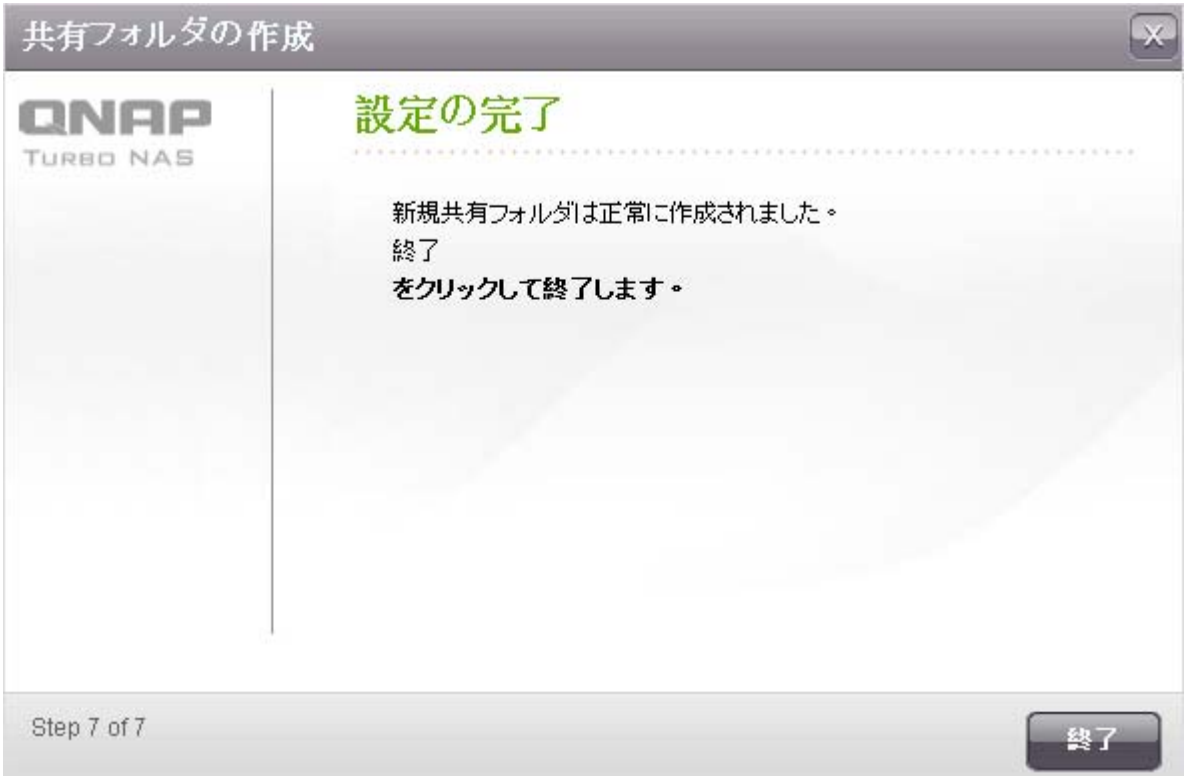


ユーザーあるいはユーザーグループ毎にアクセス権限を特定するよう選択した場合は、読込のみ、読込み/書込み、あるいはアクセス拒否をユーザーあるいはユーザーグループに割当てることができます。

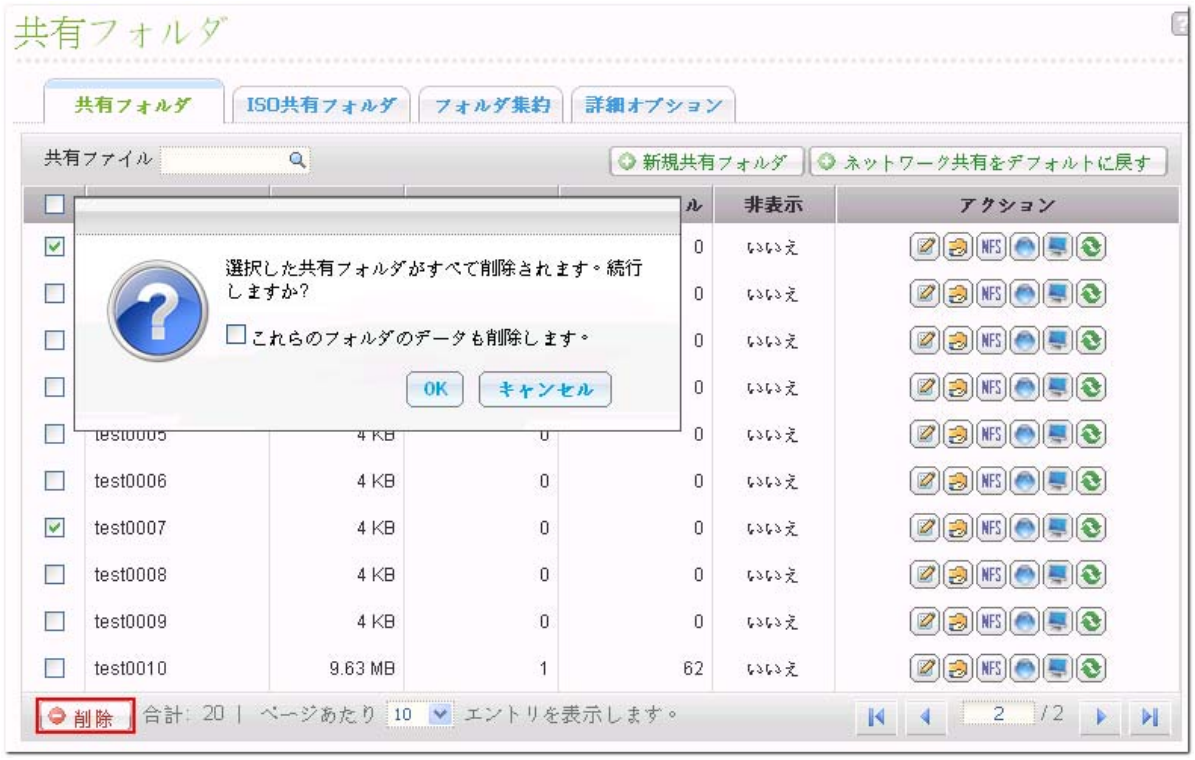
設定を確定し、"Next"（次へ)をクリックします。



"Finish"（終了）をクリックしてセットアップを完了します。



共フォルダを削除するには、フォルダのチェックボックスにチェックを入れ、"Delete"（削除）をクリックします。"Also delete the data in these folder(s)"（これらのフォルダのデータも削除する）のオプションを選択して、フォルダおよびその中のファイルを削除することができます。フォルダデータを削除しないよう選択した場合は、データはNASに保持されます。データにアクセスするには、同じ名前のフォルダを再度作成します。

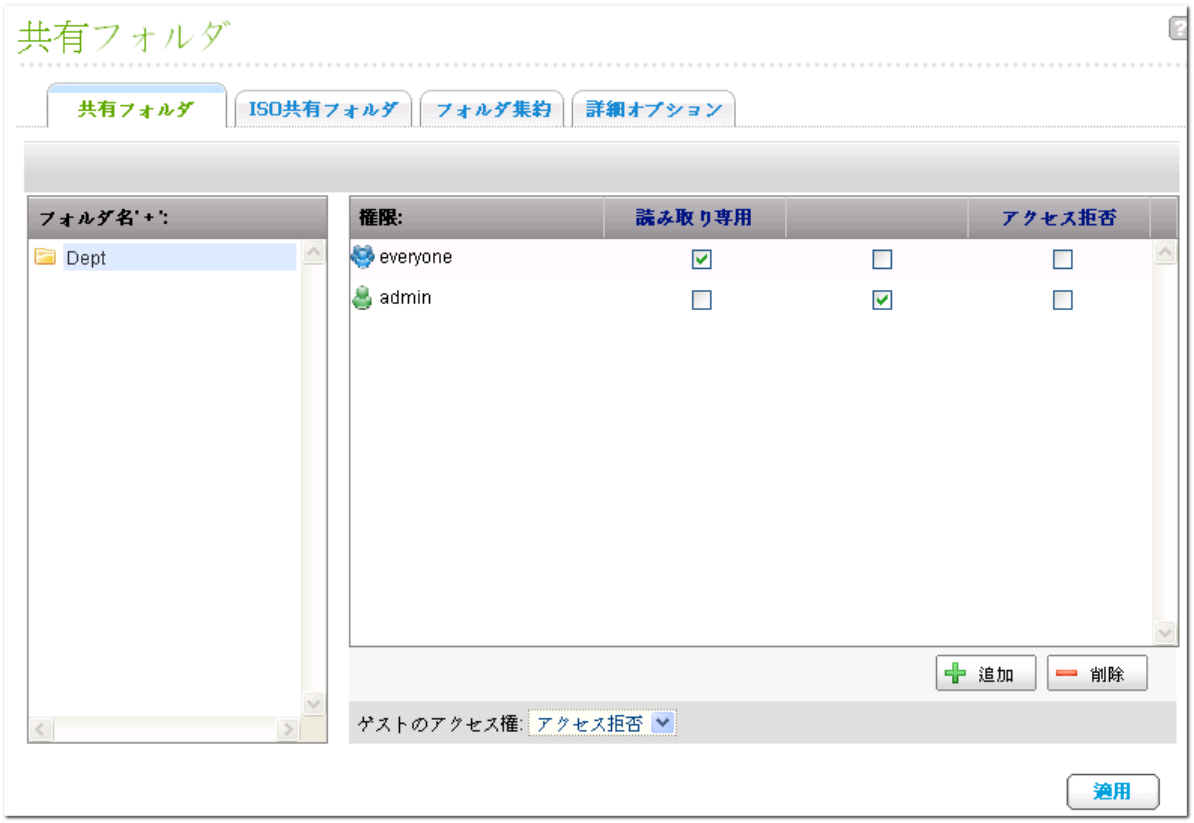


アイコン	説明
（フォルダプロパティ）	フォルダのプロパティを編集します。 フォルダの表示または非表示、便宜的ロック、フォルダパス、コメントの有効または無効、FTP接続で書き込み専用アクセスの有効または無効を指定します。
（フォルダアクセス権）	フォルダ許可およびサブフォルダ許可を編集します。
（NFSアクセス制御）	NASへのNFSアクセス権を指定します。 アスタリスク(*)はすべての接続を意味します。
（WebDAVアクセス制御）	フォルダへのWebDAVアクセス権を指定します。
（Microsoft Networkingホストアクセス制御）	Microsoft Networking経由でフォルダへの接続を許可されたホスト名またはIPアドレスを入力します。 Microsoft Networking経由でフォルダにアクセスするために、ユーザーは正しいログイン名とパスワードが必要です。
（リフレッシュ）	フォルダの詳細をリフレッシュします。

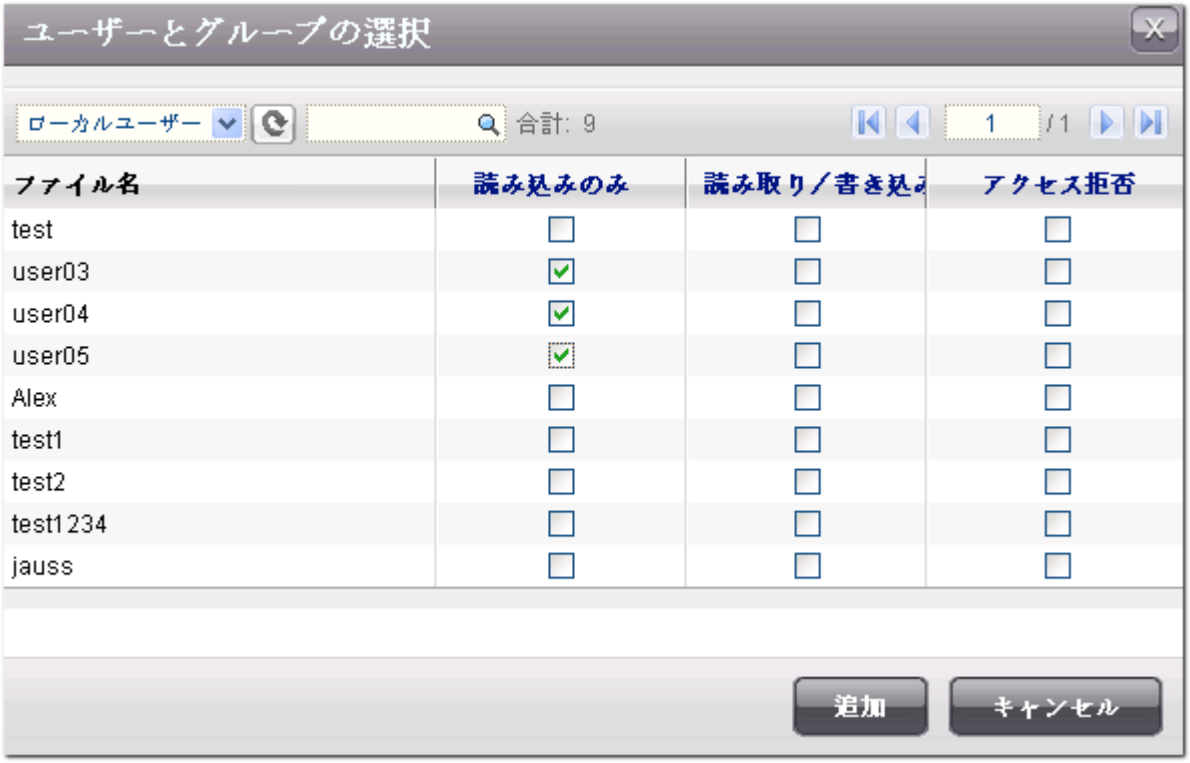
フォルダアクセス権

NASでフォルダ許可またはサブフォルダ許可を設定できます。 基本フォルダ許可を編集するには、「アクセス権利管理」 > 「共有フォルダ」でフォルダ名を検索し、 をクリックします。

フォルダ名は左に表示され、設定済みアクセス権利を持つユーアーはパネルに表示されます。 パネル下部でゲストアクセス権利を指定することもできます。

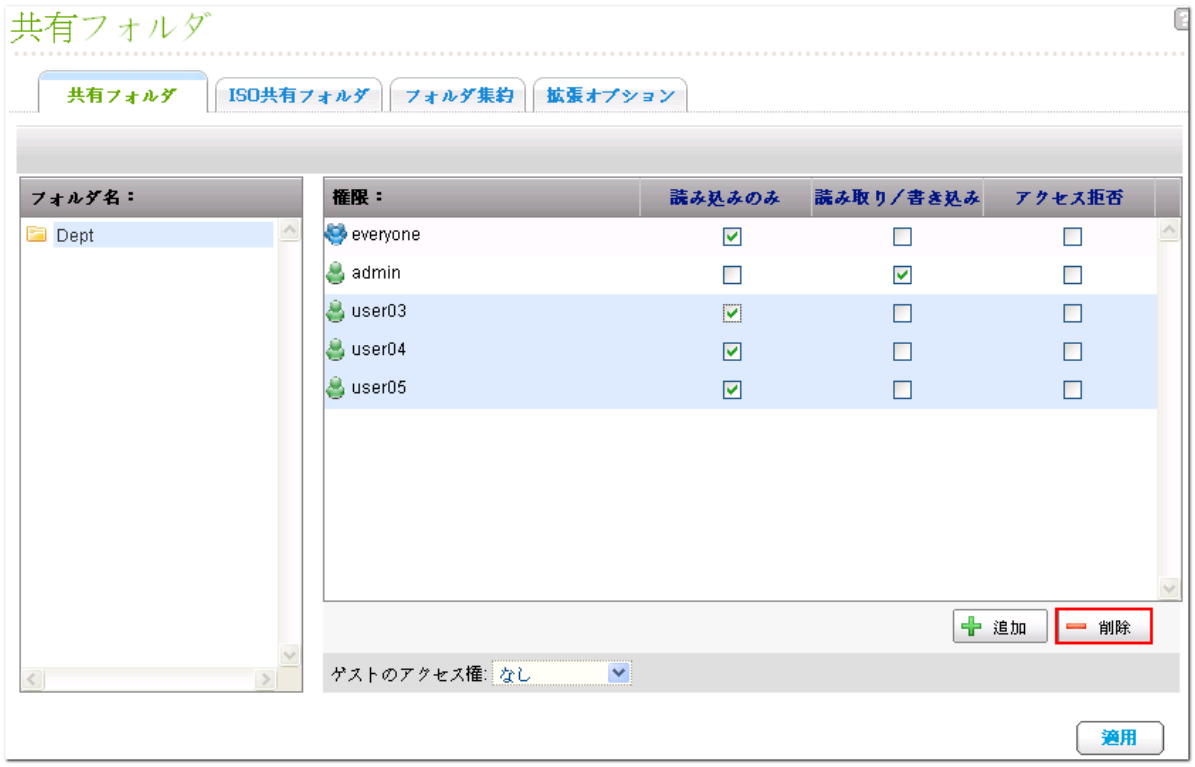


「+ Add (+ 追加) 」をクリックしさらに多くのユーザーとユーザーグループを選択し、フォルダへのアクセス権を指定します。 「ADD (追加) 」をクリックして確認します。



「– Remove（除去）」をクリックして設定された許可を取り外します。 Ctrlキーを押したままマウスを左クリックすることで、複数の項目を選択できます。 「APPLY（適用）」をクリックして設定を保存します。

「Read/Write（読み取り/書き込み）」アクセス権をユーザーに与えると、フォルダとサブフォルダを完全に制御できます。



サブフォルダ許可

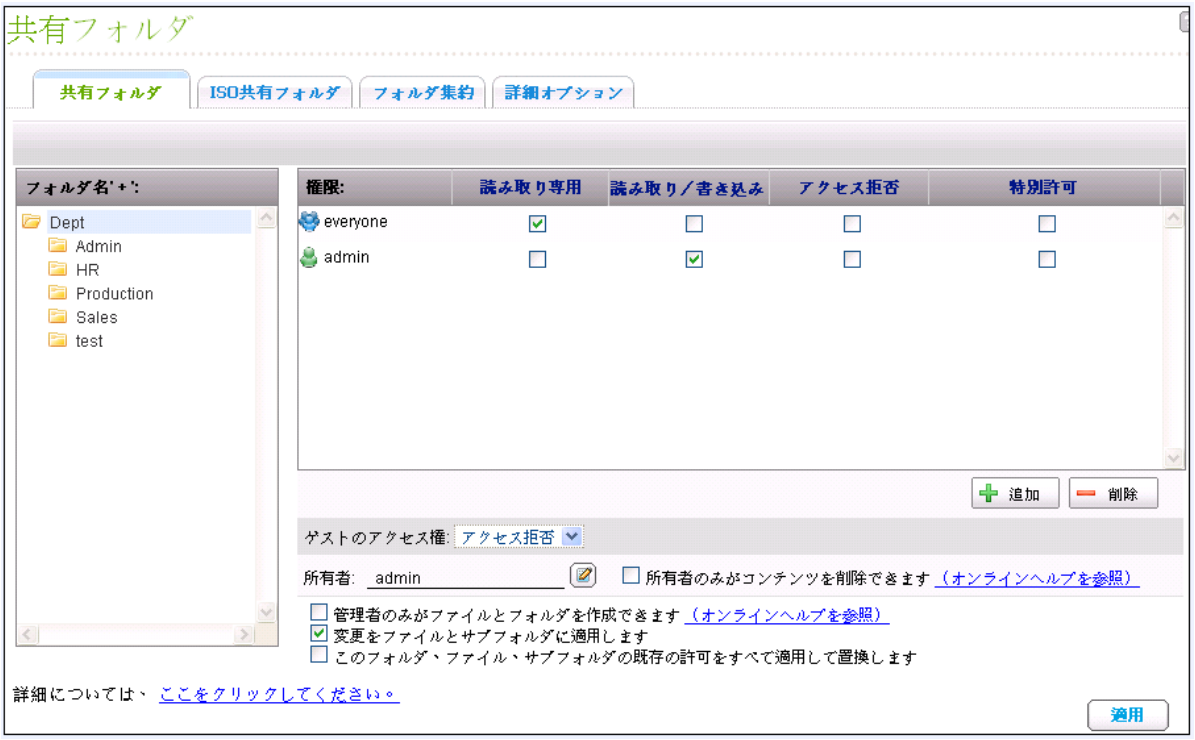
NASは、フォルダとサブフォルダの安全な管理のためにサブフォルダ許可をサポートします。 各フォルダとサブフォルダに対して、個別ユーザーの読み取り、読み取り/書き込み、および拒否アクセス権を指定できます。

サブフォルダ許可を設定するには、「Access Right Management（アクセス権管理）」 > 「Share Folders（共有フォルダ）」 > 「Advanced Options（詳細オプション）」タブを順にポイントします。 「Enable Advanced Folder Permissions（詳細フォルダ許可を有効にする）」を選択し、「APPLY（適用）」をクリックします。

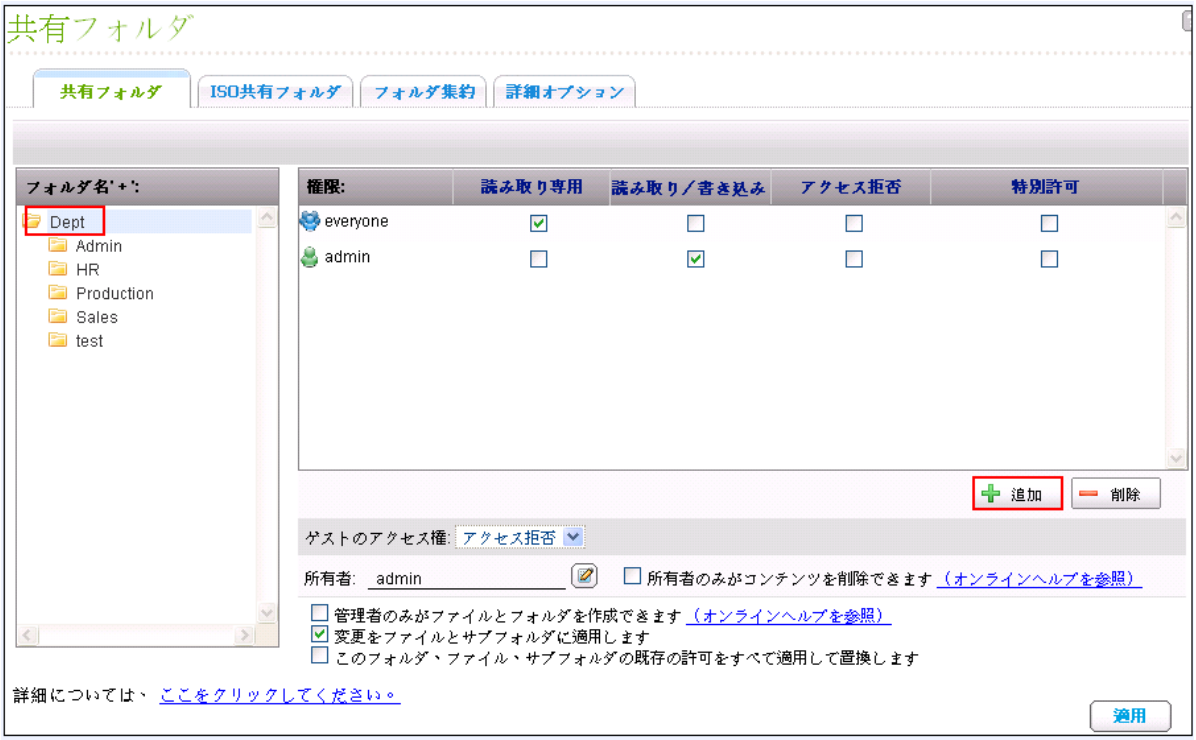
注: 詳細フォルダ許可が有効になっているとき、各フォルダに対して最大230の許可エントリを作成できます。

「Access Right Management（アクセス権利管理）」 > 「Share Folders（共有フォルダ）」 > 「Share Folders（共有フォルダ）」タブを順にポイントします。 ルートフォルダ、例えばDeptを選択し、 をクリックします。

フォルダ名とそのファーストレベルのサブフォルダが左に表示されます。 設定したアクセス権を持つユーザーが、以下の特別な許可と共にパネルに表示されます。 ファーストレベルのサブフォルダをダブルクリックして、セカンドレベルのサブフォルダを表示します。



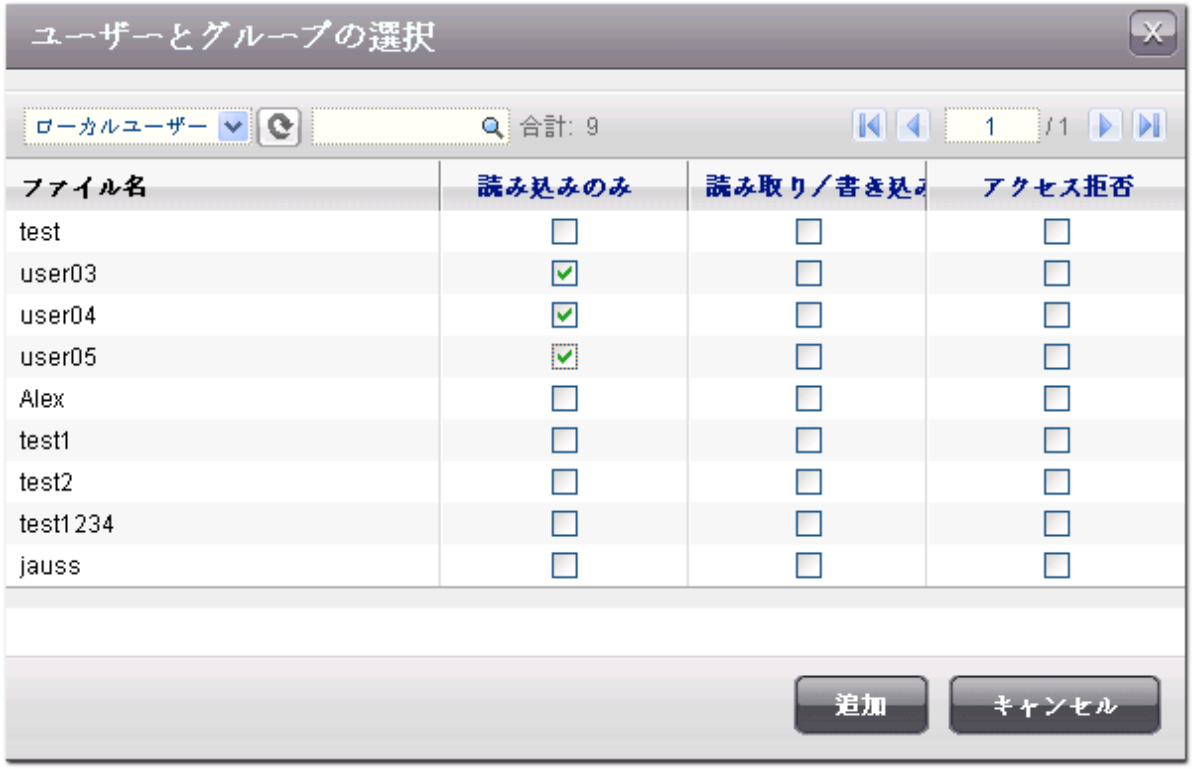
ルートフォルダ(Dept)を選択します。 「+ Add (+追加) 」をクリックして、ユーザー及びユーザーグループの読み取り専用、読み取り/書き込み、または拒否アクセス権を指定します。



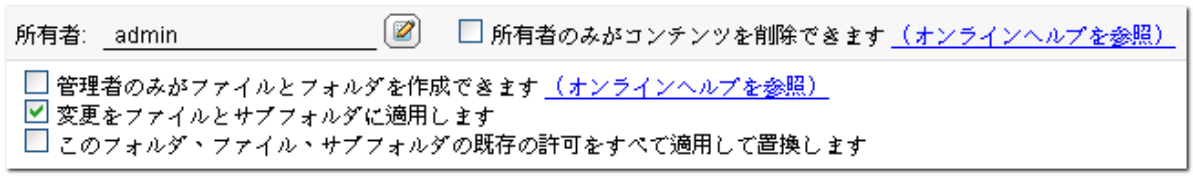
注:

- ルートフォルダのユーザーに対して「拒否アクセス権」を指定した場合、あなたがサブフォルダへの読み取り/書き込みアクセス権を選択した場合でも、ユーザーはフォルダとサブフォルダへのアクセスを許可されません。
- ルートフォルダのユーザーに対して「読み取り専用アクセス権」を指定した場合、あなたがサブフォルダへの読み取り/書き込みアクセス権を選択した場合、ユーザーはすべてのサブフォルダに対して読み取り専用アクセス件を与えられます。
- ルートフォルダに読み取り専用許可を、サブフォルダに読み取り/書き込み許可を指定するには、ルートフォルダで読み取り/書き込み許可を設定し、「管理者のみがファイルとフォルダを作成できる」（後述）オプションを使用する必要があります。

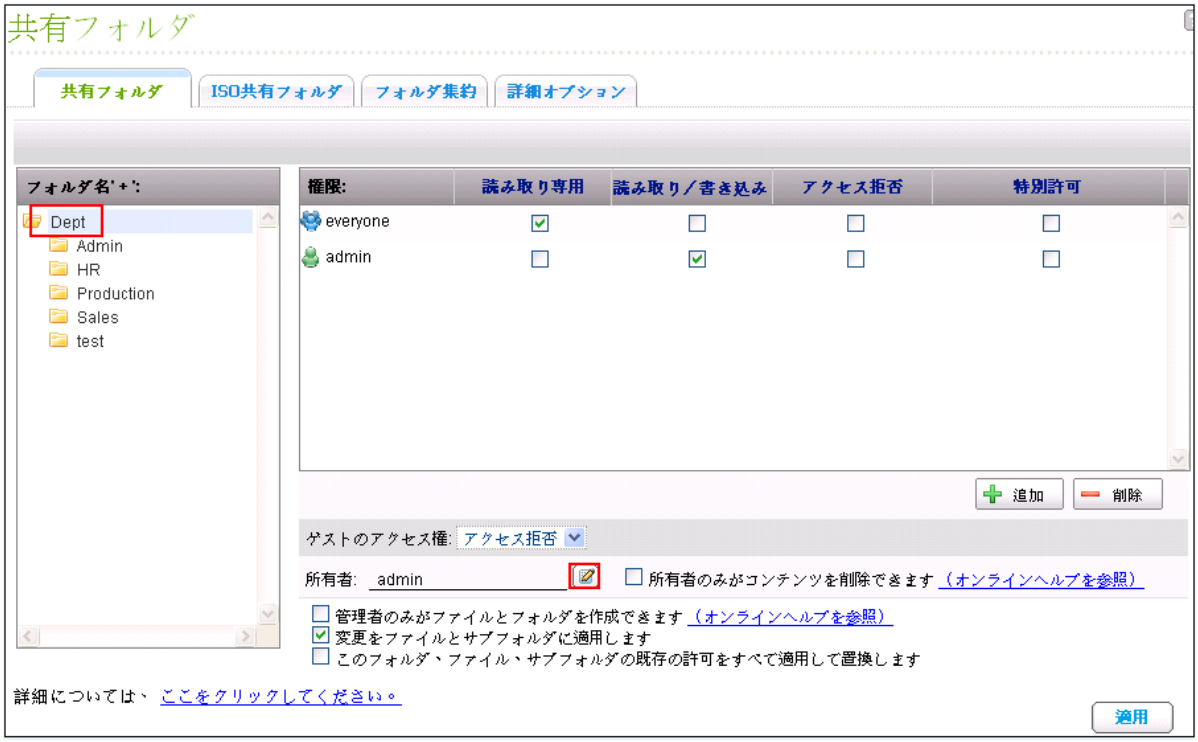
設定を終了したら「ADD（追加）」をクリックします。



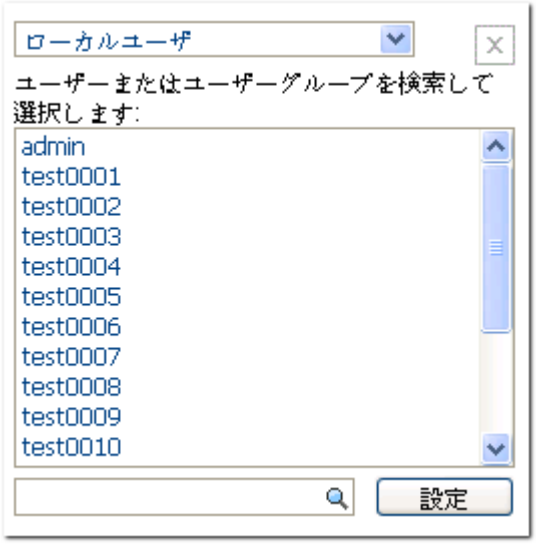
フォルダ許可パネルの下で、他の許可設定を指定します。



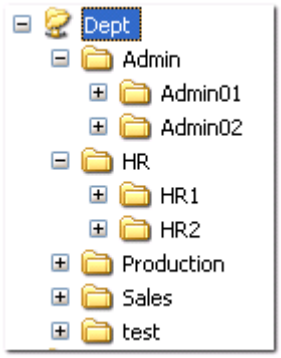
- ゲストアクセス権： 完全または読み取り専用アクセス権を与えるように、またはゲストアクセス権を拒否するように指定します。
- オーナー： フォルダのオーナーを指定します。 デフォルトで、フォルダオーナーは作成者です。 フォルダオーナーを変更するには、 をクリックします。



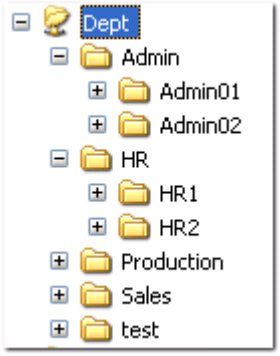
リストからユーザーを選択するか、ユーザー名を検索します。 「Set（設定）」をクリックします。



- オーナーのみがコンテンツを削除できる
  このオプションをフォルダ、例えばDeptに適用するとき、フォルダオーナーのみがファーストレベルのサブフォルダとファイルを削除できます。 オーナーではないがフォルダへの読み取り/書き込み許可を持つユーザーは、この例のAdmin、HR、Production、Sales、testを削除できません。 このオプションは、「ファイルとサブフォルダに変更を適用する」と「このフォルダ、ファイル、およびサブフォルダのすべての既存の許可を適用し置換する」オプションが選択されている場合でも、選択したフォルダのサブフォルダには適用されません。



- 管理者のみがファイルとフォルダを作成できる： このオプションは、ルートフォルダでのみ使用できます。このオプションを選択すると、管理者は選択したフォルダでのみファーストレベルのサブフォルダとファイルを作成できます。 例えば、フォルダ「Dept」では、管理者のみがファイルとサブフォルダAdmin、HR、Productionなどを作成できます。 Deptに対して読み取り/書き込みアクセス権を持つ他のユーザーはAdmin01、Admin02、HR1、HR2などのセカンドおよびファーストレベルのサブフォルダにファイルとフォルダのみを作成できます。



- ファイルとサブフォルダに変更を適用する： 選択したフォルダ内部のすべてのファイルとサブフォルダに対するオーナー保護とルートフォルダの書き込み保護設定を除き、許可設定を適用します。 これらの設定には新規ユーザー、削除されたユーザー、変更された許可、フォルダオーナーが含まれます。 「オーナーのみがコンテンツを削除できる」と「管理者のみがファイルとフォルダを作成できる」のオプションはサブフォルダには適用されません。

- このフォルダ、ファイル、およびサブフォルダの既存の許可をすべて適用し、交換する： オーナー保護とルートフォルダの書き込み保護設定を除き、選択したフォルダとそのファイルおよびサブフォルダのそれまでに設定された許可をすべて無効にするには、このオプションを選択します。「オーナーのみがコンテンツを削除できる」と「管理者のみがファイルとフォルダを作成できる」のオプションはサブフォルダには適用されません。

- 特殊許可： このオプションは、ルートフォルダでのみ使用できます。 ユーザーにフ事前設定された許可に関わりなく、フォルダのすべてのコンテンツへのアクセス権を許可するには、このオプションを選択し、「読み取り専用」または「読み取り/書き込み」から選択します。 特殊な許可を持つユーザーは、Microsoft Networking経由でフォルダに接続するとき「admin」として確認されます。 ユーザーに「読み取り/書き込み」アクセス権のある特殊な許可を与えた場合、そのユーザーは完全アクセス権を持ち、Windowsのフォルダ許可を設定することができるようになります。 このユーザーにより作成されたファイルは、すべて「admin」に属します。 「admin」はNASの割当が制限されていないため、特殊な許可を持つユーザーが作成したファイルの数とサイズは事前設定された割当設定により制限されません。 このオプションは、管理とバックアップタスクにしか使用できません。

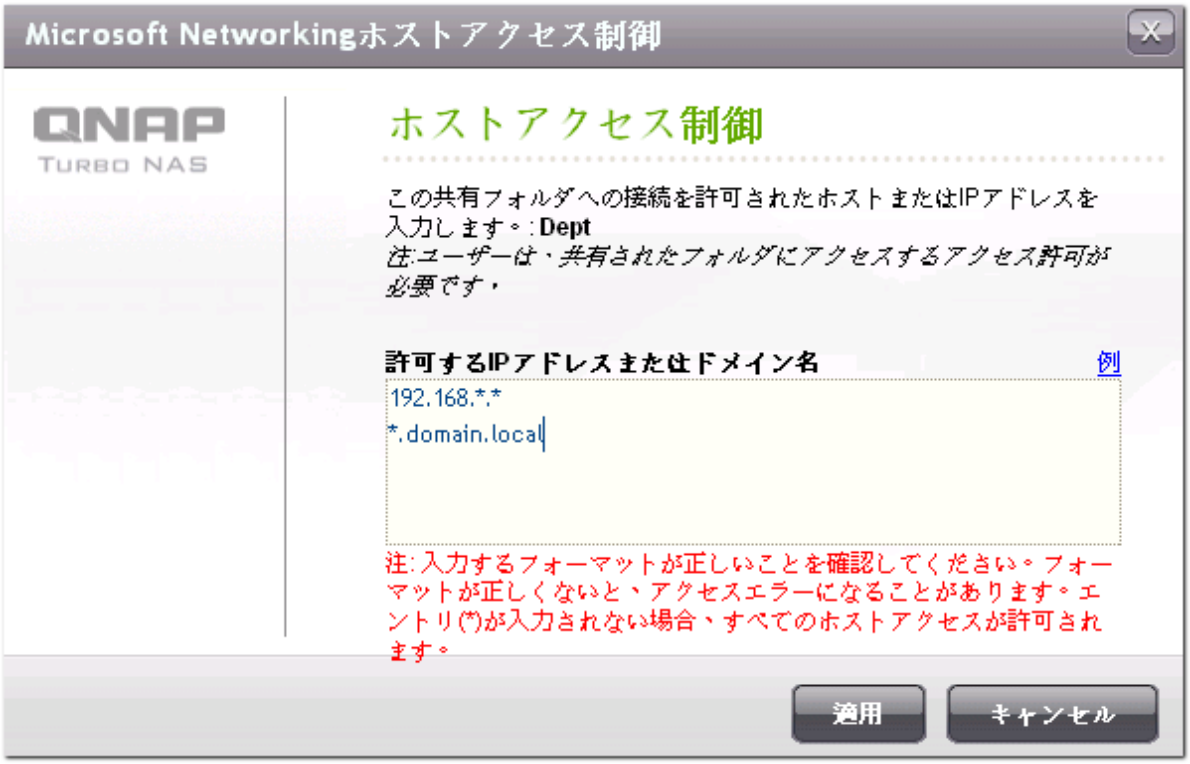
許可の変更後、「APPLY（適用）」、「YES（はい）」の順にクリックして確認します。

Microsoft Networkingホストアクセス制御

NASフォルダは、デフォルトではSamba接続(Windows)経由でアクセスできます。 Microsoft Networking経由でNASへのアクセスを許可された、IPアドレスまたはホストを指定できます。 フォルダのホストアクセス制御を編集するには、 をクリックします。

ウィザードが示されます。許可されたIPアドレスとホスト名を入力します。例:

IPアドレス	192.168.12.12 192.168.*.*
ホスト名	dnsname.domain.local *.domain.local



ワイルドカード文字

不明な文字を表すために、IPアドレスまたはホスト名エントリにワイルドカード文字を入力できます。

アスタリスク(*)

ゼロ以上の文字数の場合、代替文字としてアスタリスク(*)を使用します。 例えば、*.domain.localと入力した場合、次の項目が含まれます。

a.domain.local

cde.domain.local

test.domain.local

疑問符(?)

1文字だけの場合、代替文字として疑問符(?)を使用します。 例えば、test?.domain.localには次が含まれます。

test1.domain.local

test2.domain.local

testa.domain.local

有効なホスト名にワイルドカード文字を使用するとき、ドット(.)がワイルドカード文字に含まれます。 例えば、*.example.com、「one.example.com」および「one.two.example.com」が含まれます。

ISO共有フォルダ

ISO画像ファイルをNASにISO共フォルダとしてマウントし、ディスクにコピーを焼き付けることなくコンテンツにアクセスすることができます。NASは最大で256*のISO共フォルダをサポートしています。

*TS-110、TS-119、TS-210、TS-219、TS-219P、TS-410、TS-119P+、TS-219P+、TS-112、およびTS-212は最大256のネットワーク共フォルダのみサポートしています。そのため、これらのモデルでサポートされるISO画像ファイルの最大数は256以下となります。

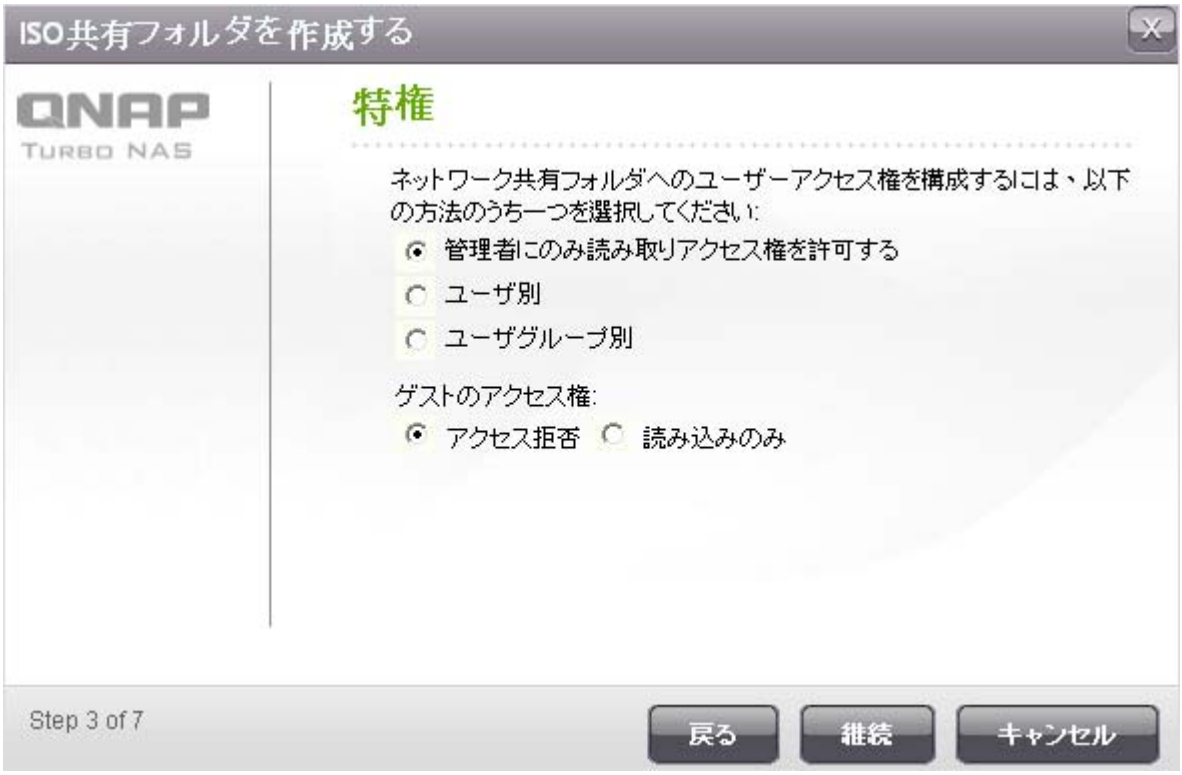
下記の手順に従い、ウェブインターフェイスを使用してNASにISOファイルをマウントしてください。

1. NASに管理者として ログインします。"Share Folders" (共フォルダ) > "ISO SHARE FOLDERS" (ISO共フォルダ)を開きます。"Mount An ISO File" (ISOファイルをマウントする)をクリックします。

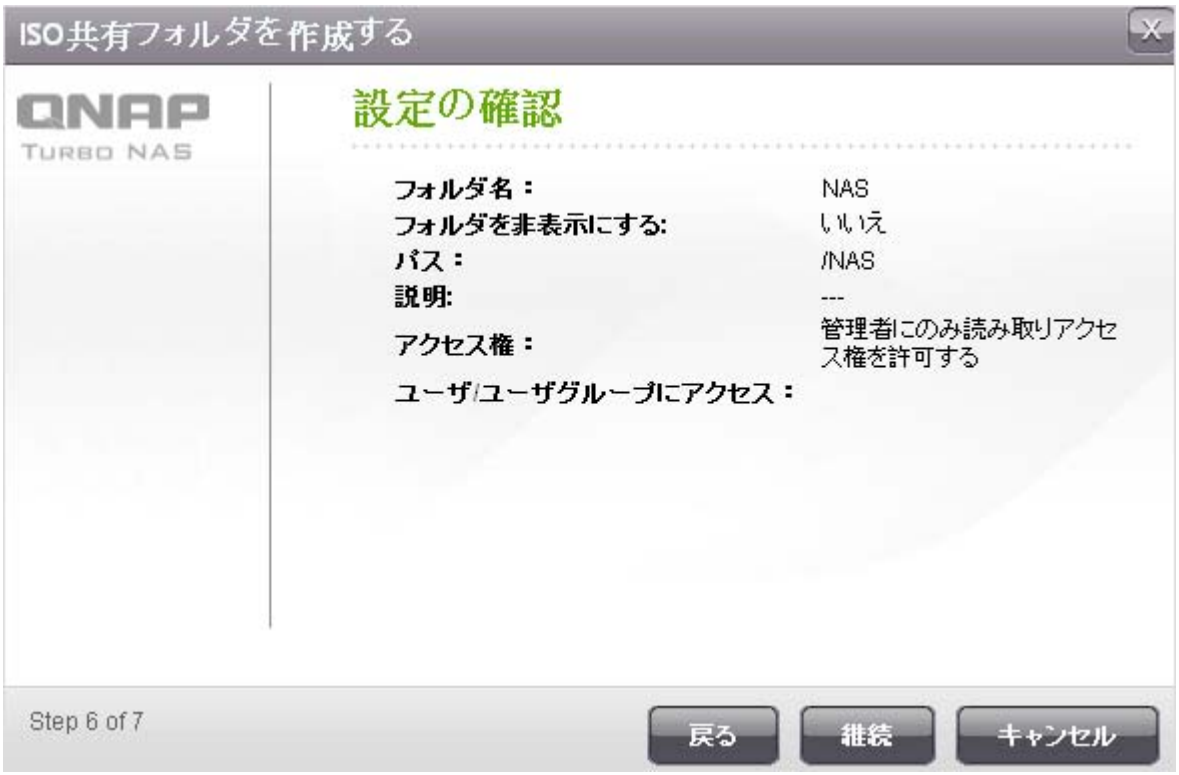
2. NASのISO画像ファイルを選択します。"Next" (次へ) をクリックします。

3. 画像ファイルはNASの共フォルダとしてマウントされます。フォルダ名を入力します。

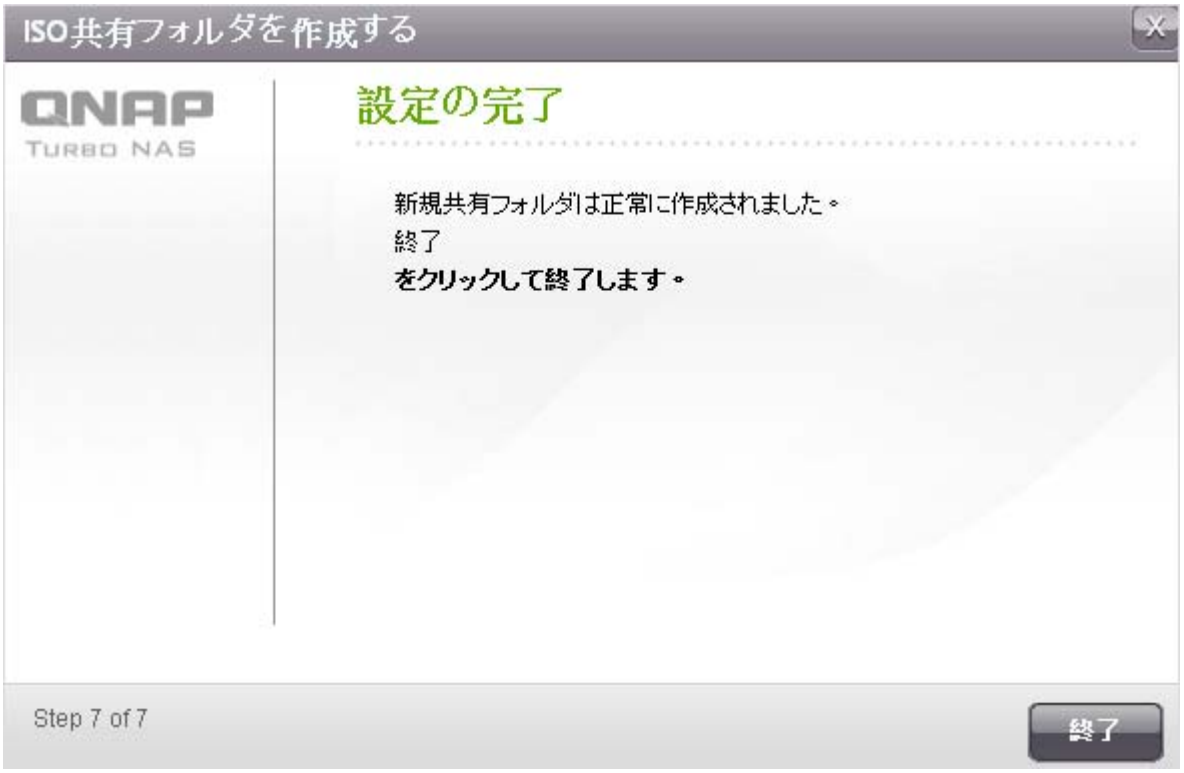
4. NASユーザーあるいはユーザーグループの共フォルダに対するアクセス権限を指定します。ゲストアクセス権限に "Deny Access" (アクセス拒否) あるいは "Read only" (読込のみ)を選択することもできます。"Next" (次へ)をクリックします。



5. 設定を確定し、"Next" (次へ)をクリックします。



6. "Finish" (終了)をクリックします。



7. 画像ファイルのマウント後、異なるネットワークプロトコル(SMB、AFP、NFS、WebDAVなど)からのユーザーにおけるアクセス権限を指定することができます。"Action" (操作)列のアイコンをクリックしてください。

8. NASはWeb File Manager(ウェブファイルマネージャ)によるISO画像ファイルのマウントもサポートしています。詳細はこちら をご覧ください。

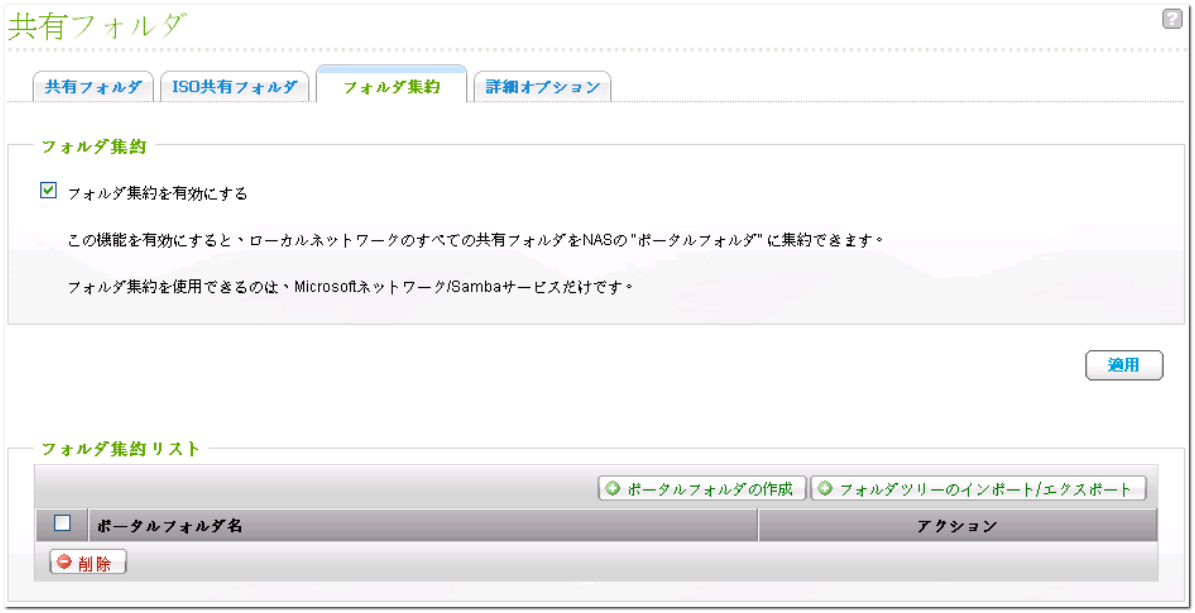
フォルダ集約

Microsoftネットワークの共フォルダをNASのポータルフォルダとして集約し、ご使用のNASを通してNASユーザーがアクセスできるようにすることができます。最大10個の共フォルダまでNAS上のポータルフォルダにリンクすることができます。

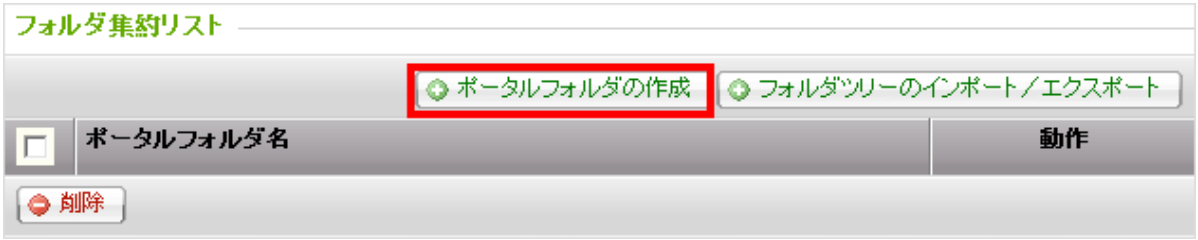
> 注: この機能は、Microsoftネットワークサービスでのみサポートされています。

この機能を使用するには、以下の手順に従ってください。

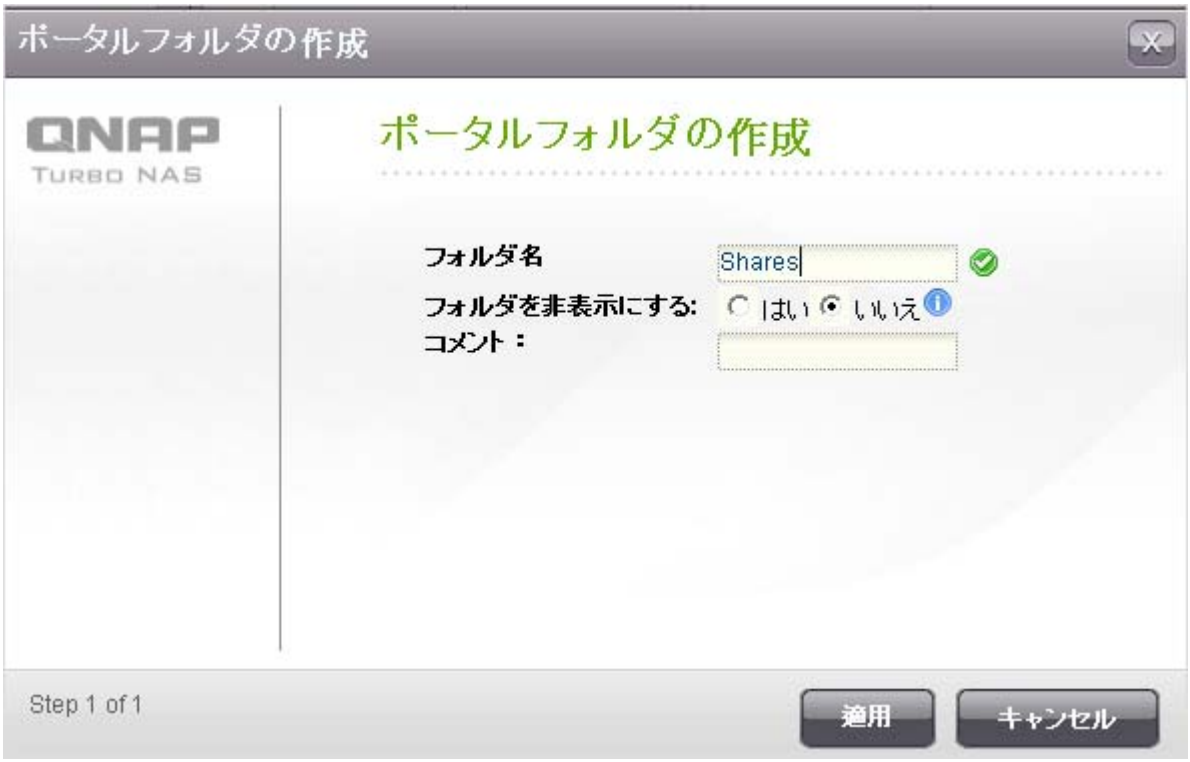
1. フォルダ集約を効化します。



2. "Create A Portal Folder" (ポータルフォルダの作成) をクリックします。



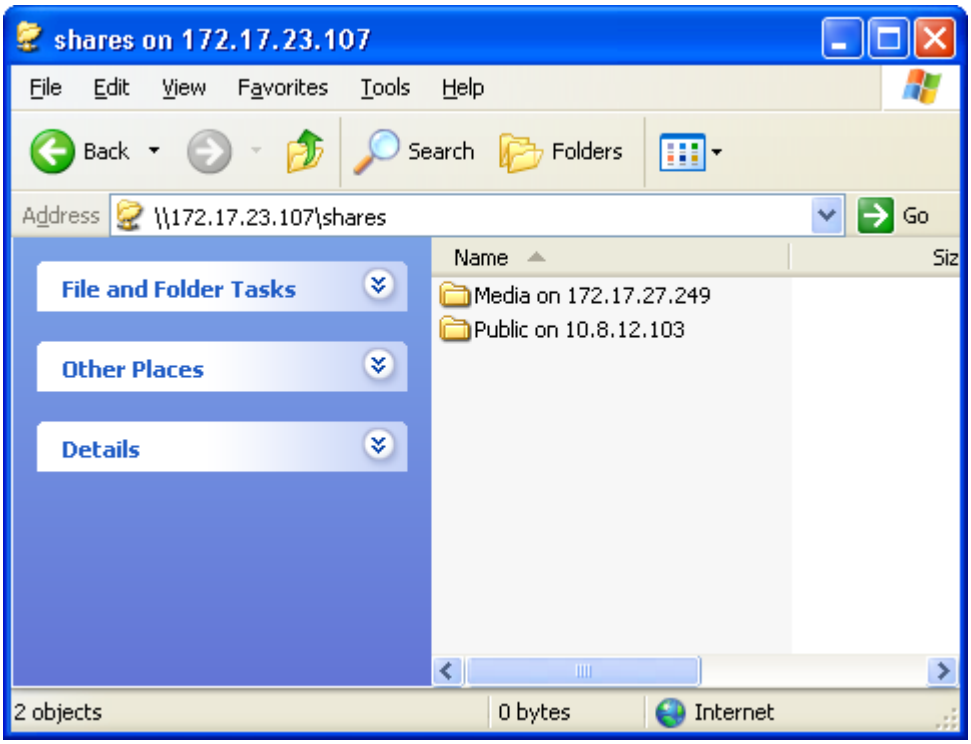
3. ポータルフォルダ名を入力します。 フォルダを表示するかどうかを選択し、ポータルフォルダのオプションのコメントを入力します。



4. をクリックし、リモートフォルダ設定を入力します。 共フォルダがパブリックアクセスに開かれていることを確認してください。

注: 共フォルダに許可制限がある場合、同じADドメインのNASとリモートサーバに参加する必要があります。

5. 正常に接続されると、NASを通じてリモートフォルダにアクセスすることができます。



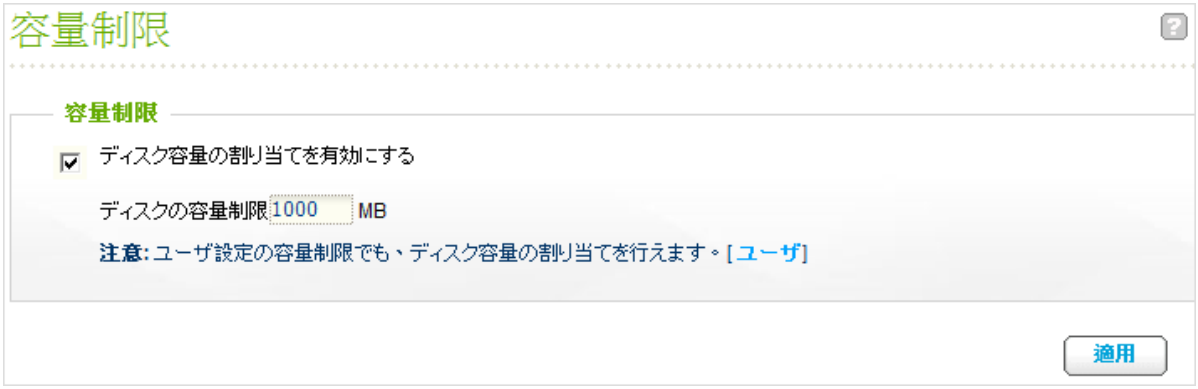
詳細オプション

NASでサブフォルダ許可を設定するには、「詳細フォルダ許可を有効にする」を選択し、「共有フォルダ」>「フォルダ許可」の順にポイントして許可を指定します。

5.5 クォータ

ディスク容量を効果的に使用、運用するためにユーザが使用できるディスク容量を制限できます。設定が適用されたとき制限値以上のデータを利用できません。これにより少数のユーザがディスク容量を独占するのを防止できます。初期設定では制限は設けられていません。

- すべてのユーザーに対してクォータを効にします
- 各ディスクボリュームのクォータサイズ



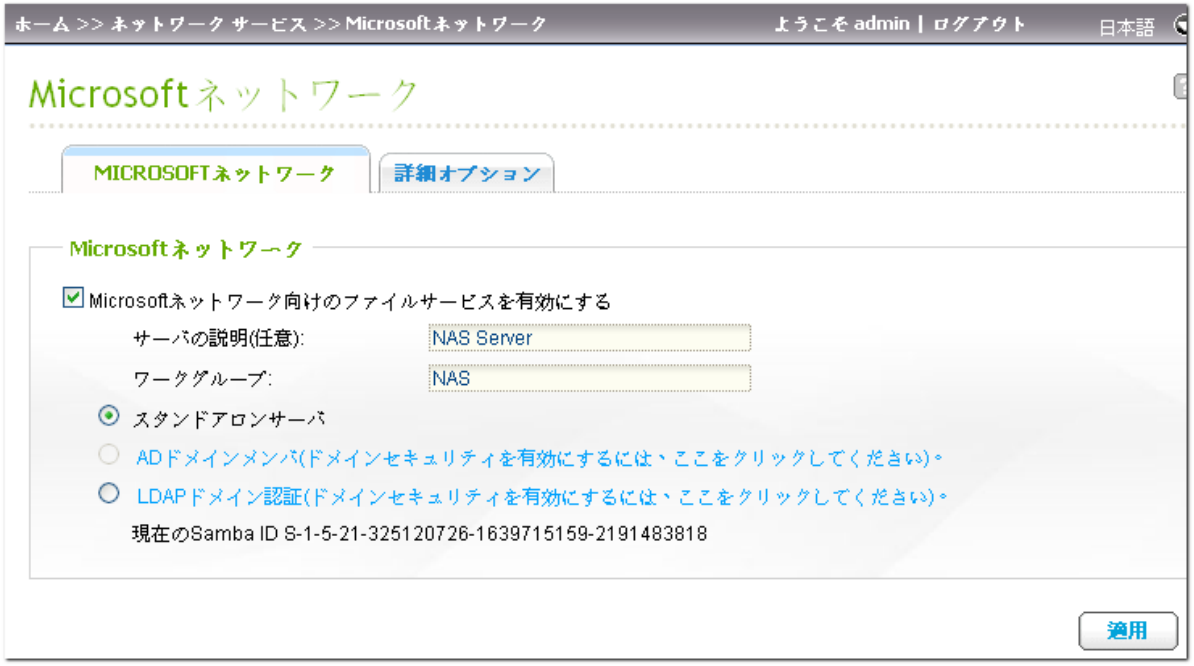
更の適用後、クォータ設定が表示されます。"GENERATE" (生成)をクリックし、クォータ設定ファイルをCSV形式で生成します。ファイルが生成された後、"DOWNLOAD" (ダウンロード)をクリックして指定した場所に保存します。

6．ネットワーク サービス

Microsoftネットワーク 262
Appleネットワーク 266
NFSサービス 269
FTPサービス 272
Telnet/ SSH 274
SNMP設定 275
Webサーバ 277
ネットワークサーチサービス 303

6.1 Microsoftネットワーク

Microsoft Windows NetworkでNASへのアクセスを許可するには、Microsoftネットワーキング用のファイルサービスを有効にします。ユーザーの認証方法も指定してください。



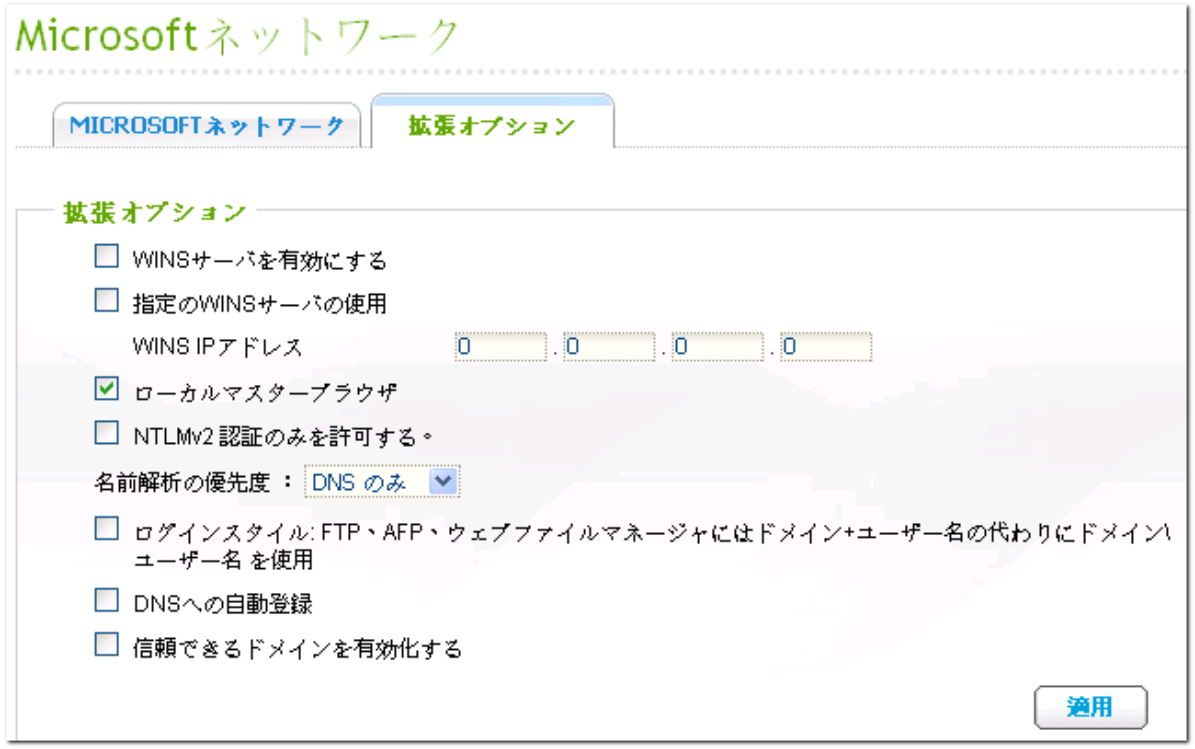
スタンドアロンサーバ
認証にはローカルユーザーを使用します。NASはローカルのユーザーアカウント情報(「Access Right Management (アクセス権管理)」>「Users (ユーザ)」で作成)を使用して、NASにアクセスするユーザーを認証します。

- サーバの説明(オプション): ユーザーがMicrosoft Networkのサーバーを容易に識別できるように、NASを説明します。
- ワークグループ: NASが属するワークグループを指定します。ワークグループ名は15文字までサポートされますが、以下を含むことはできません。
  " + = / ¥ : | * ? < > ; [ ] % , `

ADドメインメンバ
AD(Microsoft Active Directory)を使ってユーザーを認証します。このオプションを使用するには、「Access Right Management (アクセス権管理)」>「Domain Security (ドメインのセキュリティ)」でActive Directory認証を有効にし、NASをActive Directoryに結合します。

LDAPドメイン認証
LDAP (Lightweight Directory Access Protocol): ライトウェイト・ディレクトリ・アクセス・プロトコル)ディレクトリを使って、ユーザーを認証します。このオプションを使うには、LDAP認証を有効にして、「Access Right Management (アクセス権管理)」>「Domain Security (ドメインのセキュリティ)」で設定を指定します。このオプションが有効になっている場合、ローカルのNASユーザーを選択する必要があります。選択しないと、LDAPユーザーがMicrosoft Networkingを通してNASにアクセスできます。

拡張オプション



WINSサーバ

ローカルネットワークにWINSサーバが取り付けられていない場合、IPアドレスを指定してください。NASはWINSサービスにその名前とIPアドレスを自動的に登録します。ネットワーク内にWINSサーバがあって、そのサーバを使用する場合は、WINSサーバのIPを入力します。この設定について確信がないときは、このオプションを効にしないでください。

ドメインマスター

リソースとサービスを収集しレコードするために、独特なドメインマスタブラウザをネットワークまたはWindowsのワークグループ内のそれぞれのPCに対して使用できます。ドメインマスタブラウザ(Windows NT/ 200x/ XP PC)がネットワークにすでに存在する場合、ドメインマスタとしてNASを設定する必要はありません。

ネットワークコンピュータにアクセスするための待機時間が長すぎる場合、既存のマスタブラウザに障害があるか、またはマスタブラウザを使用できないことが原因であると考えられます。原因が後者である場合、このセクションでボックスドメインマスタをチェックし、NASをマスタブラウザとして設定すると、ネットワークコンピュータの情報へのアクセス速度を向上することができます。この設定について確信がないときは、このオプションを効にしないでください。

NTLMv2認証のみ許可する

NMLMv2とはNT LAN Manager version 2の略です。このオプションがオンの場合、NTLMv2認証がある場合に限りMicrosoft Networking（Microsoftネットワーク）を使用しての共フォルダへのログインが可能になります。オプションがオフの場合は、デフォルトでNTLM（NT LAN Manager）が使用され、NTLMv2はクライアントによってネゴシエートされます。デフォルト設定は無効です。

名前解決優先度

DNSサーバまたはWINSサーバを選択して、IPアドレスからクライアントホスト名を取得することができます。NASがWINSサーバを使用するようセットアップするか、あるいはWINSサーバとなるようセットアップすると、名前解決のためにDNSとWINSのどちらをはじめに使用するかを選択することができます。WINSが効の場合、デフォルト設定は‘Try WINS then DNS’（まずWINSを試行し続いてDNS）となります。WINSが効でない場合は、デフォルトでDNSが名前解決に使用されます。

ログインスタイル:FTP、AFP、ウェブファイルマネージャにはドメイン+ユーザー名の代わりにドメイン¥ユーザー名 を使用。
アクティブディレクトリ環境では、ドメインユーザーのデフォルトログイン形式は以下のとおりです:
Windows共:ドメイン¥ユーザー名
FTP:ドメイン+ユーザー名
Web File Manager（ウェブファイルマネージャ):ドメイン+ユーザー名
AFP:ドメイン+ユーザー名

このオプションがオンの場合は、ユーザーは同一のログイン名形式（ドメイン¥ユーザー名）を使用してサービスに接続することができます。

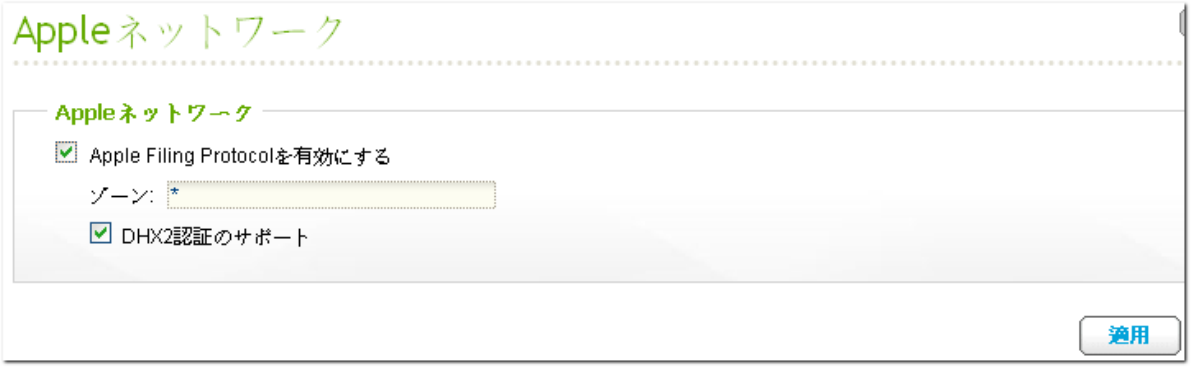
DNSにて自動登録：このオプションがオンの際にNASがアクティブディレクトリと結合されている場合、NASはドメインDNSサーバに自動的に登録されます。これにより、DNSサーバ内でのNASのDNSホストエントリが作成されます。NAS IPが更された場合は、NASは自動的に新IPをDNSサーバに対し更新します。

信頼ドメインを有効にする：このオプションを選択して信頼できるアクティブディレクトリドメインからユーザーをロードし、「Access Right Management（アクセス権管理）」>「Share Folders（共有フォルダ）」でユーザーのアクセス許可をNASに指定します。（ドメイン信頼は、NASではなく、アクティブディレクトリでのみセットアップされます）。

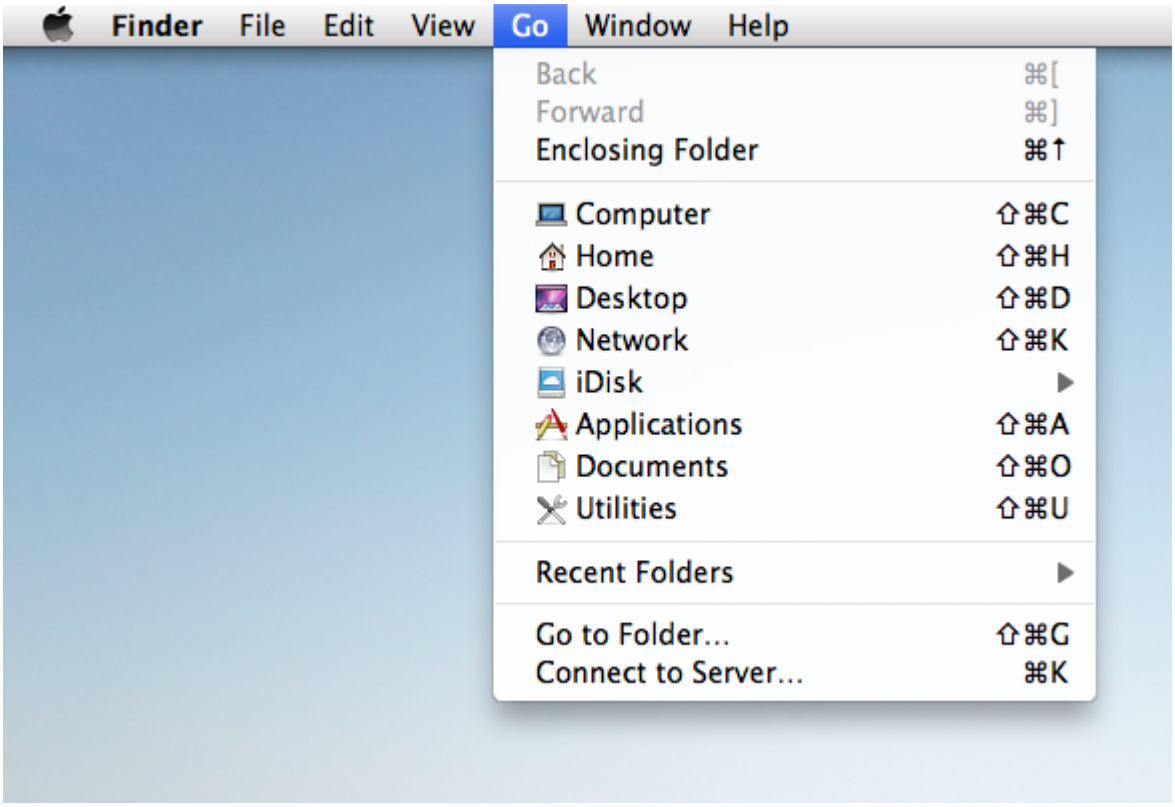
6.2 Appleネットワーク

Mac から NAS に接続するには、Apple ファイリングプロトコルを有効にします。AppleTalk ネットワークが拡張ネットワークを使用し、複数ゾーンに割り当てられている場合、NAS にゾーン名を割り当てます。アスタリスク(*)を入力して、初期設定を使用します。この設定は初期設定では無効になっています。

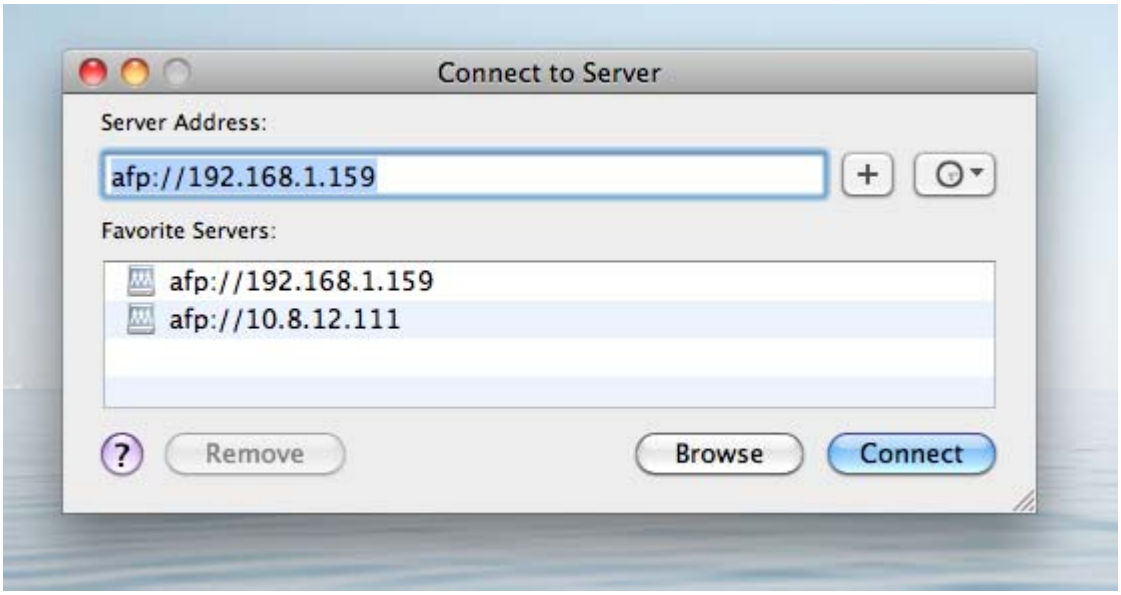
Mac OS X 10.7 Lion から NAS へのアクセスを許可するには、「DHX2 Authentication Support (DHX2 認証のサポート)」を有効にします。「Apply (適用)」をクリックして、設定を保存します。



ファインダーを使ってMacから共有フォルダに接続できます。「Go（移動）」>「Connect to Server（サーバーに接続）」をポイントするか、デフォルトのキーボードショートカット「Command+k」を使用します。



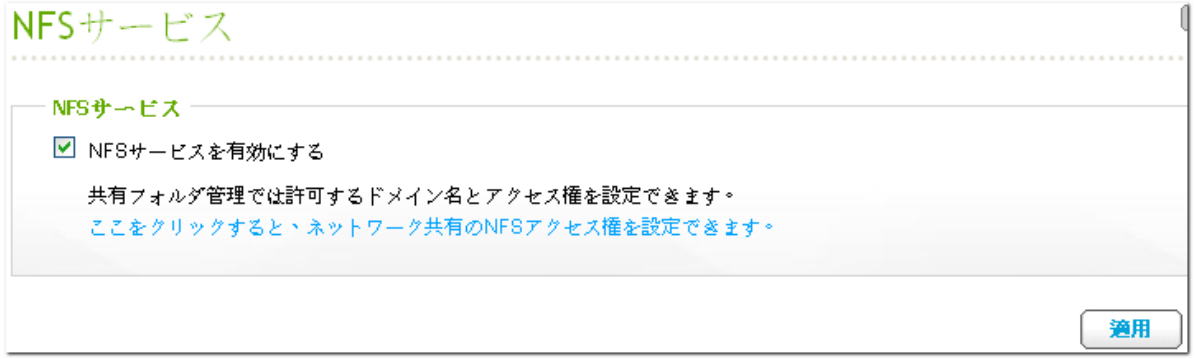
「afp://YOUR_NAS_IP_OR_HOSTNAME」などの、「Server Address (サーバーアドレス)」フィールドに接続情報を入力します。 以下に例を上げます:
afp://10.8.12.111
afp://NAS-559
smb://192.168.1.159



注: Mac OS XはApple Filing ProtocolとMicrosoft Networkingをどちらもサポートします。 Apple Filing ProtocolによってNASに接続するには、サーバーアドレスが「afp://」で始まる必要があります。 Microsoft NetworkingによってNASに接続するには、「smb://」を使用してください。

6.3 NFSサービス

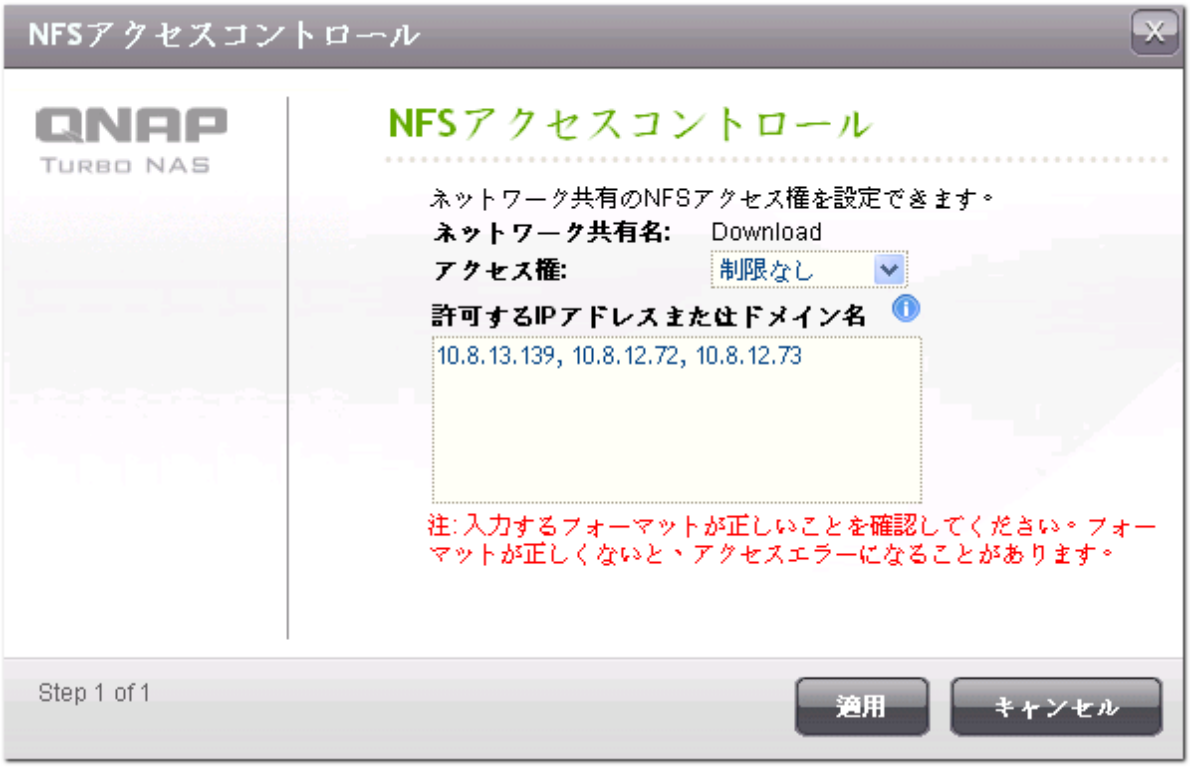
LinuxからNASにアクセスするには、NFSサービスを効にします。



NAS上の共フォルダのNFSアクセス権設定を構成するには、"Access Right Management" (アクセス権管理) > "Share Folders" (共フォルダ) を開いてください。"Action" (アクション) 列のNFSボタンをクリックします。

ネットワーク共に対するアクセス権限を特定します。"No limit" (制限なし) あるいは "Read only" (読込のみ) を選択した場合は、NFSによって共ファイルに接続することのできるIPアドレスあるいはドメインを特定することができます。

- 制限なし:ネットワーク共およびその全てのサブディレクトリ内にて、ユーザーはファイルあるいはフォルダを作成、読込み、書込み、および削除することができます。
- 読込のみ:ネットワーク共およびその全てのサブディレクトリ内にて、ユーザーはファイルあるいはフォルダを読込むことができますが、書込み、作成、あるいは削除することはできません。
- アクセス拒否:ネットワーク共に対する全てのアクセスを拒否します。



NFSを使用してNASに接続

Linuxでは、以下のコマンドを実行します:

mount -t nfs <NAS IP>:/<Network Share Name> <Directory to Mount>

例えば、NASのIPアドレスが192.168.0.1で、/mnt/pubディレクトリ内のネットワーク共フォルダ「public」にリンクする場合、以下のコマンドを使用します:

mount -t nfs 192.168.0.1:/public /mnt/pub

> 注：上記コマンドを初期化するには、「root」ユ–ザーでログインしてください。

定義したユーザーIDでログインすると、マウントしたディレクトリを使ってネットワーク共ファイルにアクセスできます。

6.4 FTPサービス

FTPサービスを効にするとき、サービスのポート数とFTPに同時に接続されているユーザーの最大数を定義できます。

NASのFTPサービスを使用するには、この機能を効化します。IEブラウザを開き、ftp://[NAS IP]と入力します。ユーザー名及びパスワードを入力しFTPサービスにログインします。

プロトコルタイプの選択
標準のFTP接続またはSSL/TLS暗号化FTPの使用を選択します。お使いのクライアントFTPソフトウェアで対応するプロトコルタイプを選択し、正常に接続されることを確認します。

ユニコードのサポート
ユニコードサポートを効/無効を選択します。初期設定は無効です。ほとんどのFTPクライアントは現在ユニコードに対応していないため、ここでユニコードサポートを無効にし、FTPのフォルダとファイルが正しく表示されるように、「システム管理」>「全般設定」ページでOSと同じ言語を選択することをお勧めします。FTPクライアントがユニコードに対応している場合、クライアントとNASの両方に対してユニコードを効にしていることを確認してください。

自動ログオン
anonymousログインを使用すれば、NASのFTPサーバに匿名でアクセスできます。ユーザーは公共アクセス用のファイルとフォルダに接続できます。このオプションをオフにした場合、ユーザーは認証済みユーザー名とパスワードを入力しないとサーバーに接続できません。

パッシブFTPポート範囲
デフォルトのポート範囲(55536-56559)を使用するか、または1024より大きなポート範囲を定義できます。この機能を使用しているとき、ルータまたはファイアウォールで、設定されたポート範囲が開いていることを確認してください。

FTP転送制限
すべてのFTP接続の最大数、単一アカウントの最大接続および単一接続の最大アップロード/ダウンロード速度を設定することができます。

受動FTP接続要求に対して外部IPアドレスで応答
受動FTP接続が使用中でFTPサーバーがルータ下で設定されているとき、リモートコンピュータがWAN経由でFTPサーバーに接続できない場合、この機能を効にできます。この機能を効にすることによって、FTPサービスは指定されたIPアドレスに手動で応答したり、外部IPアドレスを自動で検出できるため、リモートコンピュータはFTPサーバーに正常に接続できます。

6.5 Telnet/SSH

このログインを効にした後、TelnetまたはSSH暗号化接続を介してこのサーバーにアクセスできます(アカウント「admin」のみがリモートでログインできます)。接続に対して特定のTelnetまたはSSH接続クライアント、たとえばputtyを使用できます。この機能を使用しているとき、ルータまたはファイアウォールで設定されたポートを開いていることを確認してください。

SFTP (SSH File Transfer Protocol (SSHファイル転送プロトコル)あるいは Secure File Transfer Protocol (セキュリティファイル転送プロトコル)として知られます) を使用するには、"Allow SSH connection" (SSH接続を許可) のオプションをオンにするよう注意してください。

6.6 SNMP設定

SNMP(シンプルネットワークマネジメントプロトコル)サービスをNASにて効化し、SNMP管理ステーション(SNMPマネージャ、例えばSNMPソフトウェアがインストールされているPC)のトラップアドレスを入力することができます。NASにてイベント、警告、またはエラーが生じた際、(SNMPエージェントとしての)NASはSNMP管理ステーションにリアルタイムでアラートを報告します。

フィールドの説明は以下の通りです:

フィールド	説明
SNMPトラップレベル	SNMP管理ステーションに送信される情報の種類を選択します。
イベント送信	SNMPマネージャに報告するイベントのタイプを選択します。詳細ログは「システムログ」のページで表示することができます。
SNMP MIB(管理情報ベース)	MIBはASCIIテキスト形式のデータベースのタイプで、SNMPネットワーク内のNASの管理に使用されます。SNMPマネージャはMIBを使用することでネットワーク内のエージェント(NAS)によって送信されたメッセージを理解、または価値判断することができます。すべてのワードプロセッサあるいはテキストエディターによって、MIBをダウンロードし表示することができます。
コミュニティ(SNMP V1/V2)	SNMPコミュニティストリングは、パスワードとして機能するテキストストリングです。これは、管理ステーションとNASの間で送信されたメッセージの認証に使用されます。コミュニティストリングは、SNMPマネージャとSNMPエージェントとの間で送信される各パケットに含まれています。
SNMP V3	NASはSNMPバージョン3をサポートしています。 使用可能な場合、認証及びプライバシー設定を入力することができます。

SNMP設定
SNMP
このサービスを有効化した後、NASはSNMPを経由して管理システムに情報を報告することができるようになります。
SNMPサーバを有効にする
ポート番号：
161
SNMPトラップレベル:
情報
警告
エラー
トラップアドレス 1:
トラップアドレス 2:
トラップアドレス 3:
SNMPバージョン：
SNMP V1/V2
コミュニティ:
public
SNMP MIB
MIBを管理システムにインストールするには、[ダウンロード]をクリックしてください。
ダウンロード

6.7 Webサーバ

NASを使えば、ウェブサーバ機能により、ウェブページをアップロードして独自のウェブサイトを管理するのが容易にできます。また、インタラクティブなウェブサイトを確立するJoomla! 、PHPやSQLiteにも対応しています。

ウェブサーバを使用するには、以下の手順に従ってください。

1. サービスを効化し、ポート番号を入力してください。初期設定値は80です。

2. その他の設定を構成します:

   - register_globals の設定

   register_globalsを効または無効にするように選択します。設定は、デフォルトでは無効になっています。ウェブプログラムがPHP register_globalsを効にするように要求する場合は、register_globalsを効にしてください。ただ、システムセキュリティ上、このオプションは無効にすることを推奨します。

   - php.iniを編集する

   php.ini メンテナンスがphp.ini を効にして、編集、アップロードおよび修復できます。

   > 注:PHP mail()機能を使用するには、「システム管理」 > 「通知」 をポイントしてSMTPサーバーを設定します

   - セキュリティ接続(SSL)

   SSL接続用のポート番号を入力します。

3. HTMLファイルをNAS上の共フォルダ (Qweb/ Web) にアップロードします。ウェブページのホームパスは、file index.html、index.htm、あるいはindex.php となります。

4. "Web Server" (ウェブサーバ) ページ上のリンク(http://NAS IP/)をクリックするか、あるいはNASの口グインページ上の"Web Server" (ウェブサーバ) をクリックしてアップロードしたウェブページにアクセスします。Web Server (ウェブサーバ) が効な際は、NASの口グインページにアクセスするには、ウェブブラウザに [http://NAS IP アドレス:8080] と入力する必要があります。

WebDAV

WebDAV (Web-based Distributed Authoring and Versioning)はHTTPプロトコル向けの拡張子のセットで、これによりユーザーはリモートウェブサーバ上のファイルの編集または管理を行うことができます。この機能を効化すると、インターネットを通してNASの共フォルダをリモートPC のネットワークドライブとしてマップすることができます。アクセス権設定を編集するには、"Access Right Management" (アクセス権管理) > "Share Folders" (共フォルダ) ページに移動してください。

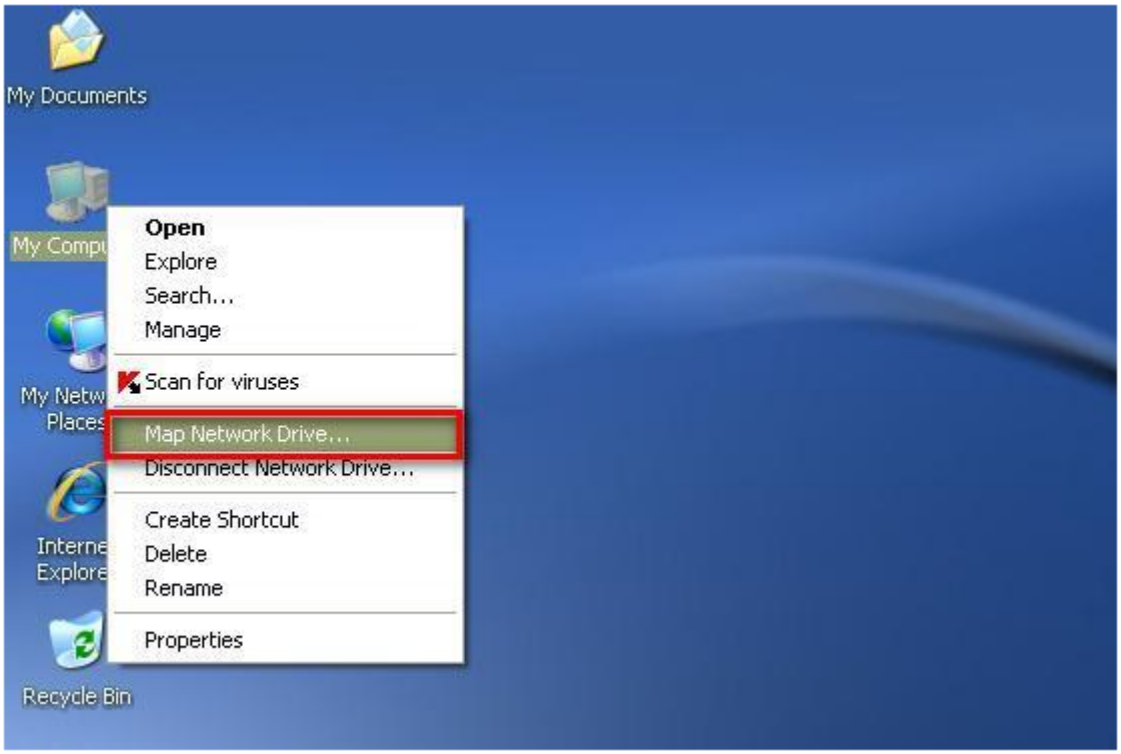
ご使用のPCのネットワークドライブとしてNAS上の共フォルダをマップするには、NAS上のWebDAVを効化し、以下の手順に従ってください。

「アクセス権管理」>「共フォルダ」>「共フォルダ」をクリックします。「動作」カラムにある「WebDAVアクセスコントロール」ボタン をクリックして、ユーザーの共フォルダへのWebDAVアクセス権を設定します。

次に、WebDAVによって、ご使用のオペレーティングシステム上のネットワーク共フォルダとしてNASのネットワーク共フォルダをマウントします。

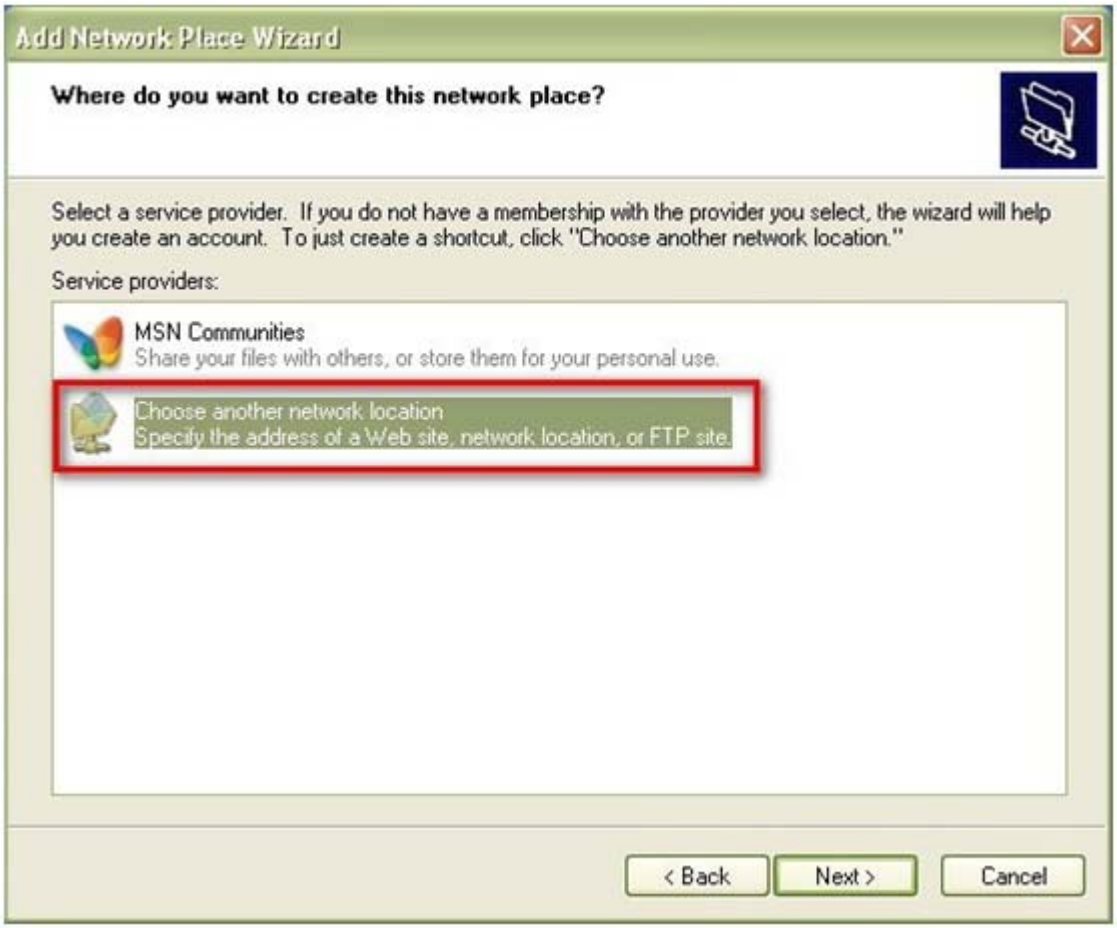
Windows XP:

1. "My Computer" (マイコンピュータ) を右クリックし"Map Network Drive..." (ネットワークドライブをマップする) を選択します。



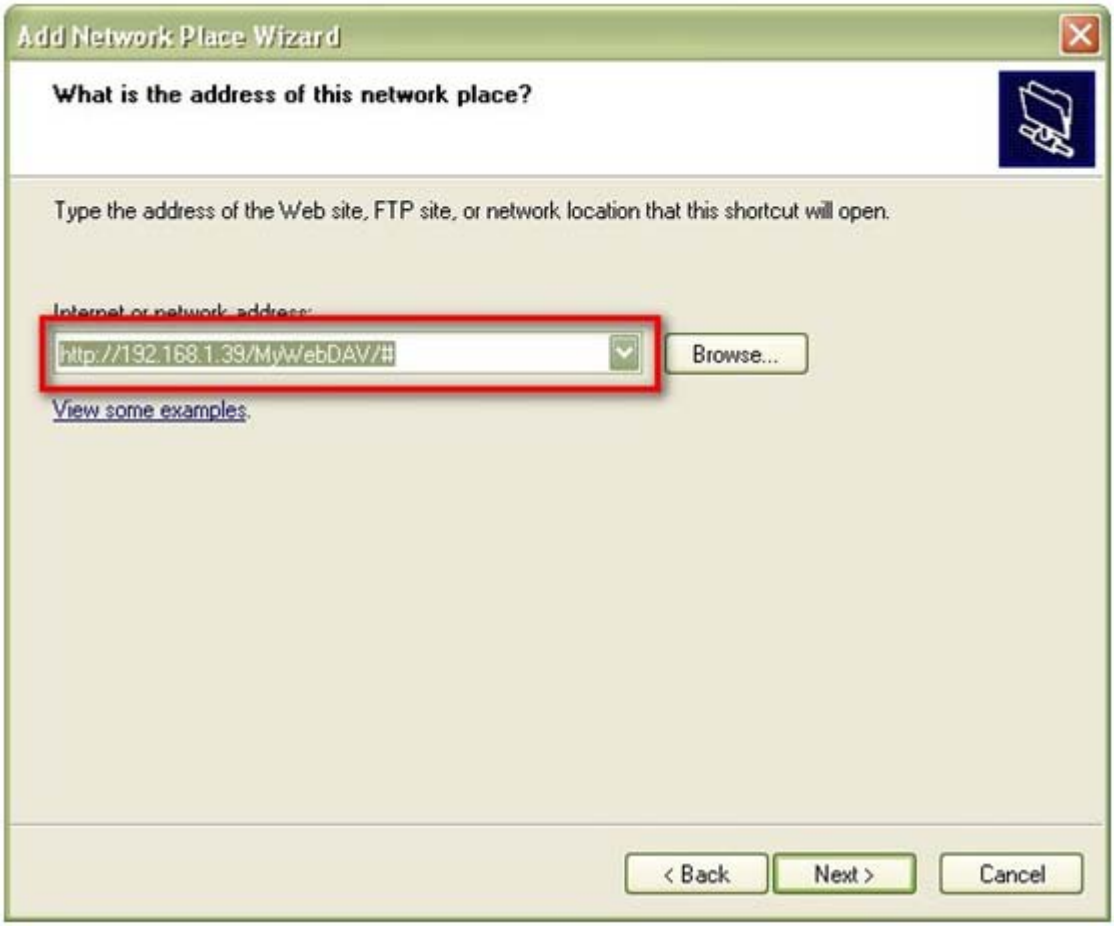
2. "Sign up for online storage or connect to a network server" (オンラインストレージへサインアップ、またはネットワークサーバへ接続) をクリックします。

3. "Choose another network location" (他のネットワークの場所を選択する) を選択します。



4. NASのURLを共フォルダ名と共に入力します。URLの終わりに "#" を入力するようご注意ください。"Next" (次へ)をクリックします。

フォーマット： http://NAS_IP_or_HOST_NAME/SHARE_FOLDER_NAME/# (http://NAS_IP_またはホスト名/共フォルダ名/#)

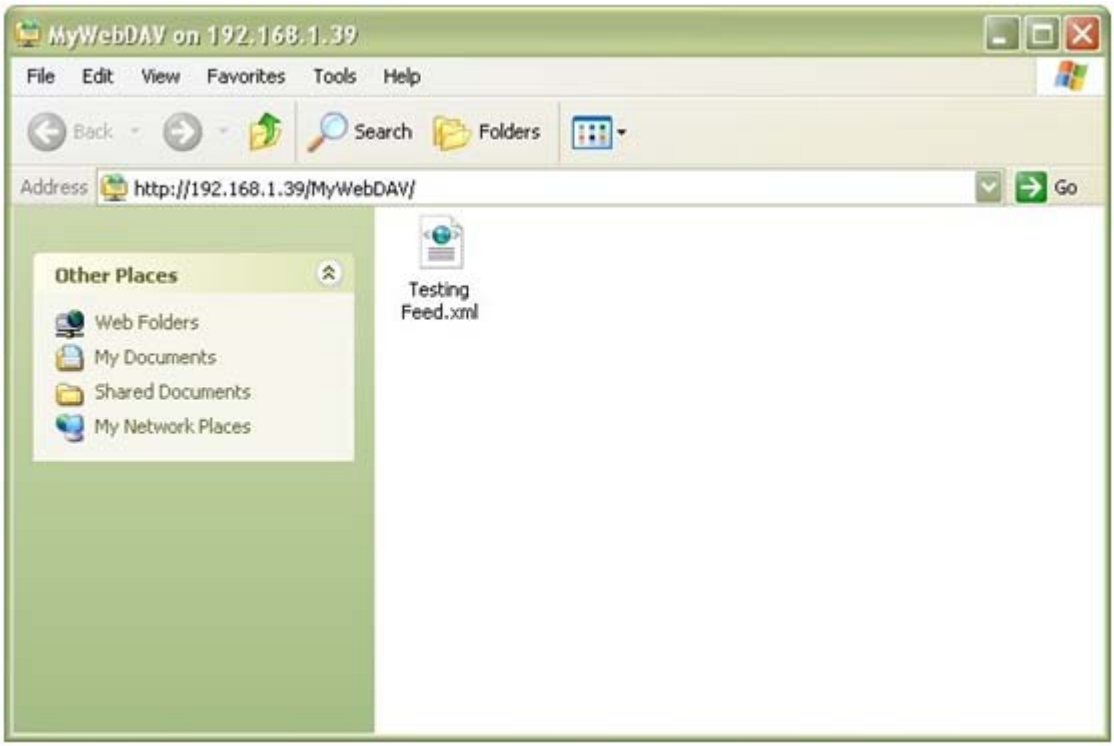


5. 共フォルダにアクセスするWebDAV権限を持つユーザー名とパスワードを入力します。

6. このネットワークプレースの名前を入力します。

7. ネットワークプレースが作成され、使用準備が整っています。

8. これでこの共フォルダにいつでもWebDAVを使用してアクセスすることができます。"My Network Places" (マイネットワークプレース) にショートカットも作成されています。

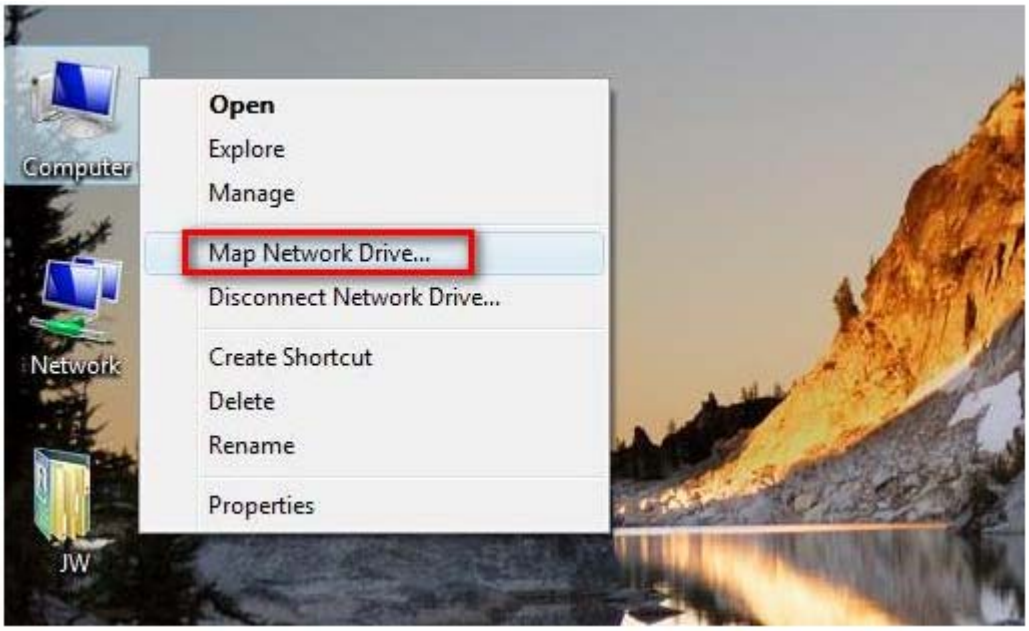


Windows Vista

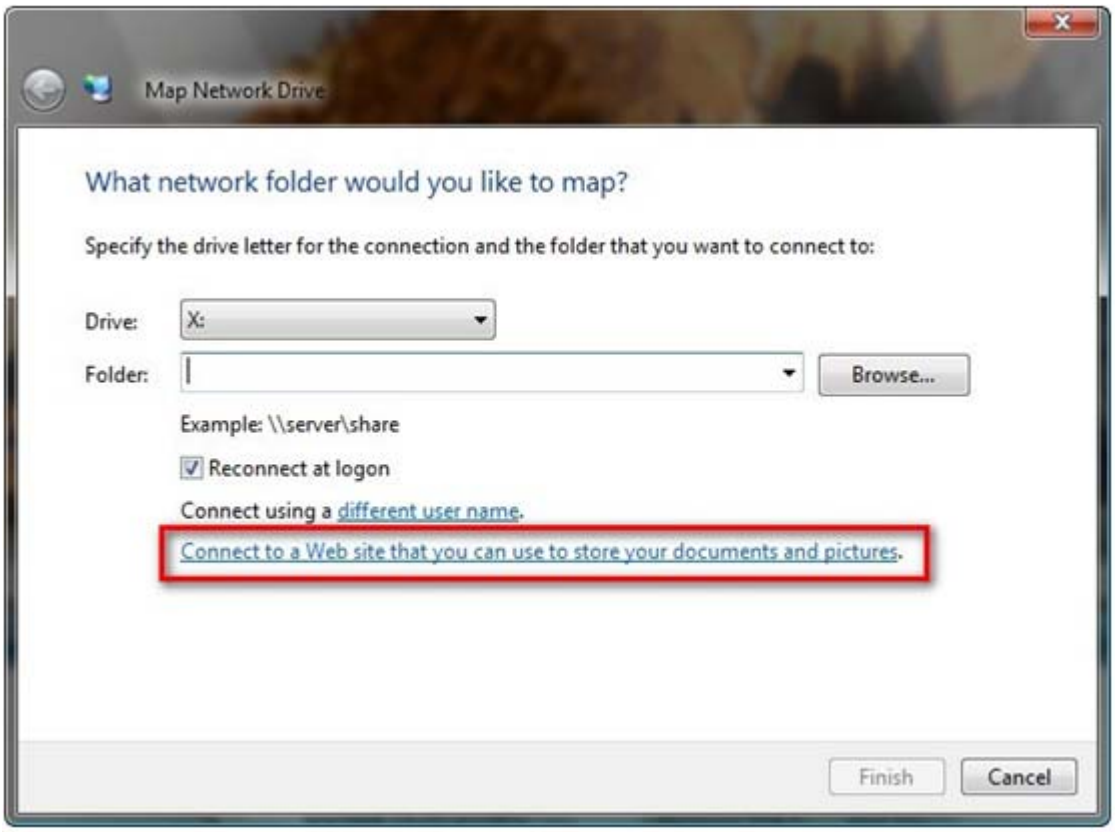
Windows Vistaをご使用の場合は、"Software Update for Web Folders" (ウェブフォルダのソフトウェア更新) (KB907306) のインストールが必要な場合があります。この更新は32ビットのWindows OSにのみ行われます。

http://www.microsoft.com/downloads/details.aspx?FamilyId=17c36612-632e-4c04-9382-987622ed1d64&displaylang=en

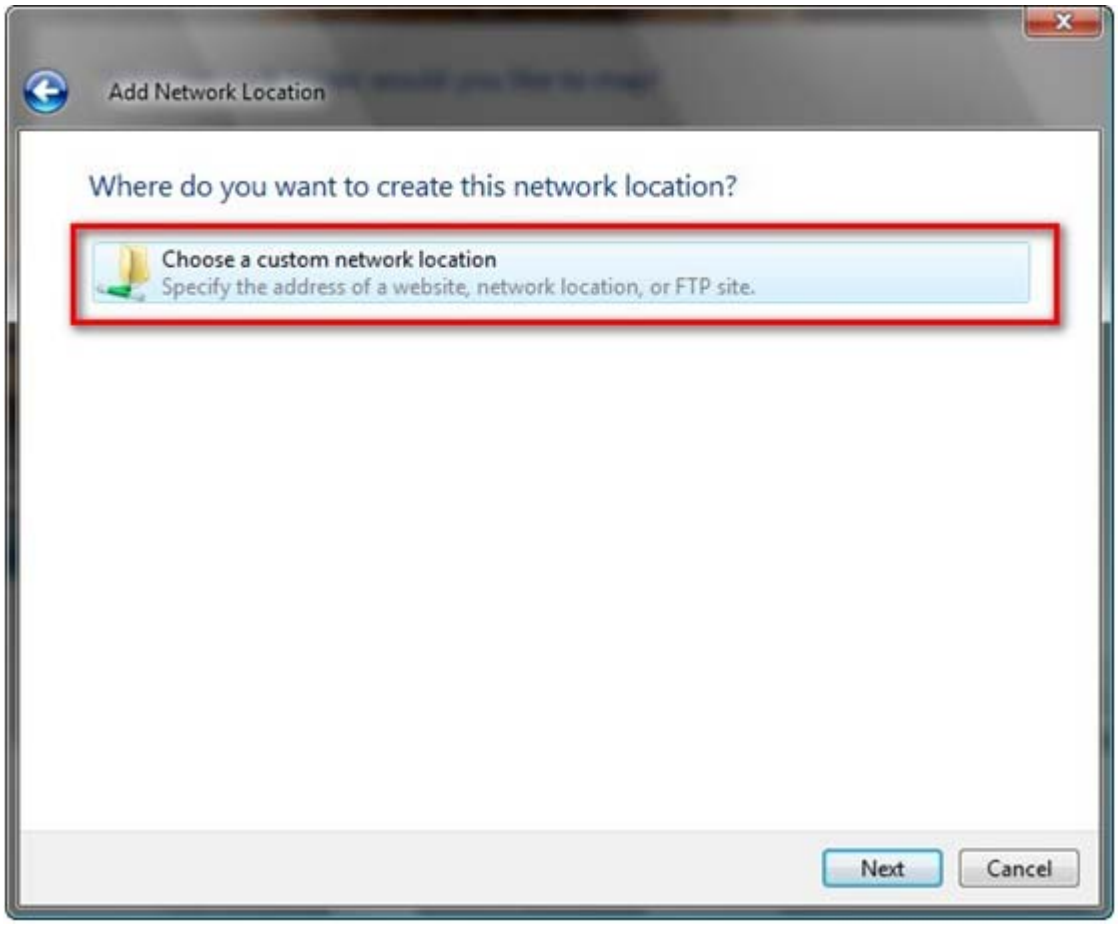
1. "Computer" (コンピュータ) を右クリックし "Map Network Drive..." (ネットワークドライブをマップする...) を選択します。



2. "Connect to a web site that you can use to store your documents and pictures" 書類や写真を保管するのに使用できるウェブサイトに接続する ） をクリックします。

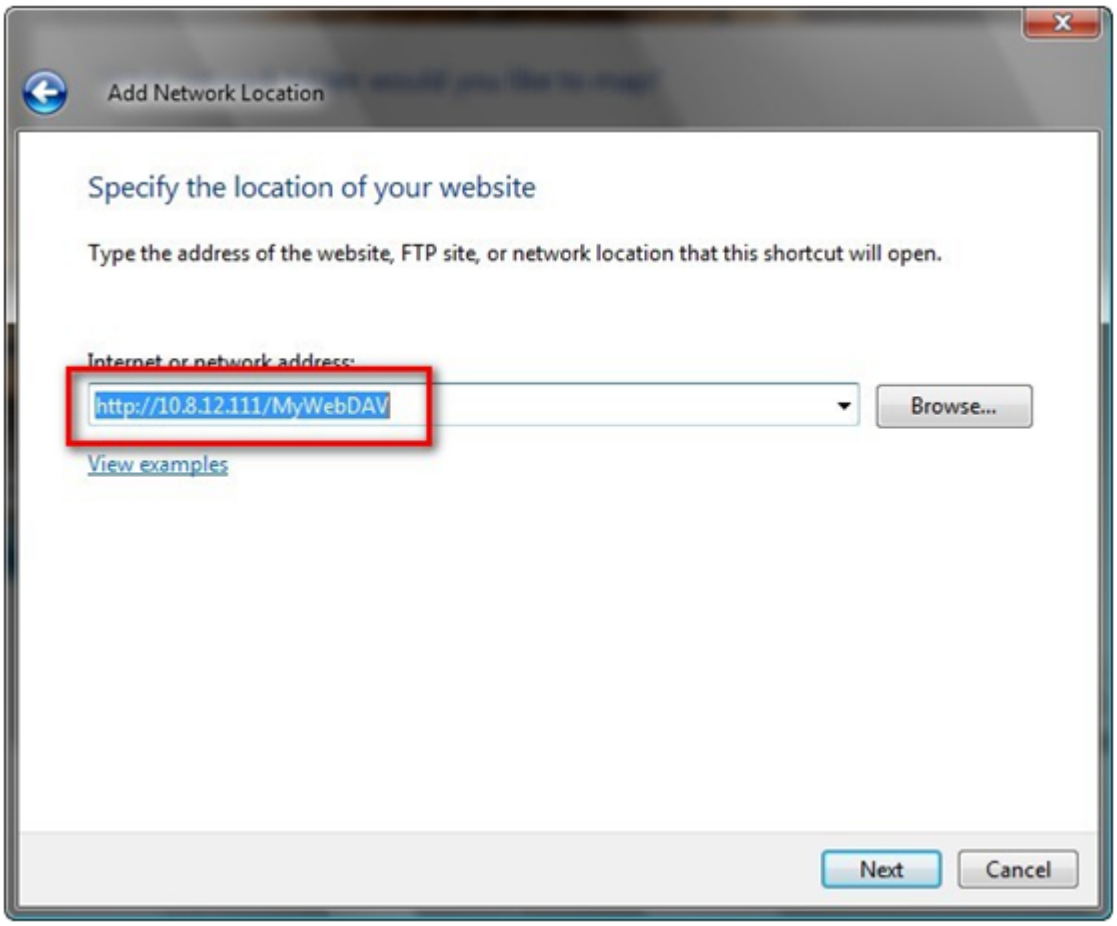


3. "Choose a custom network location" (カスタムのネットワークの場所を選択する) を選択します。



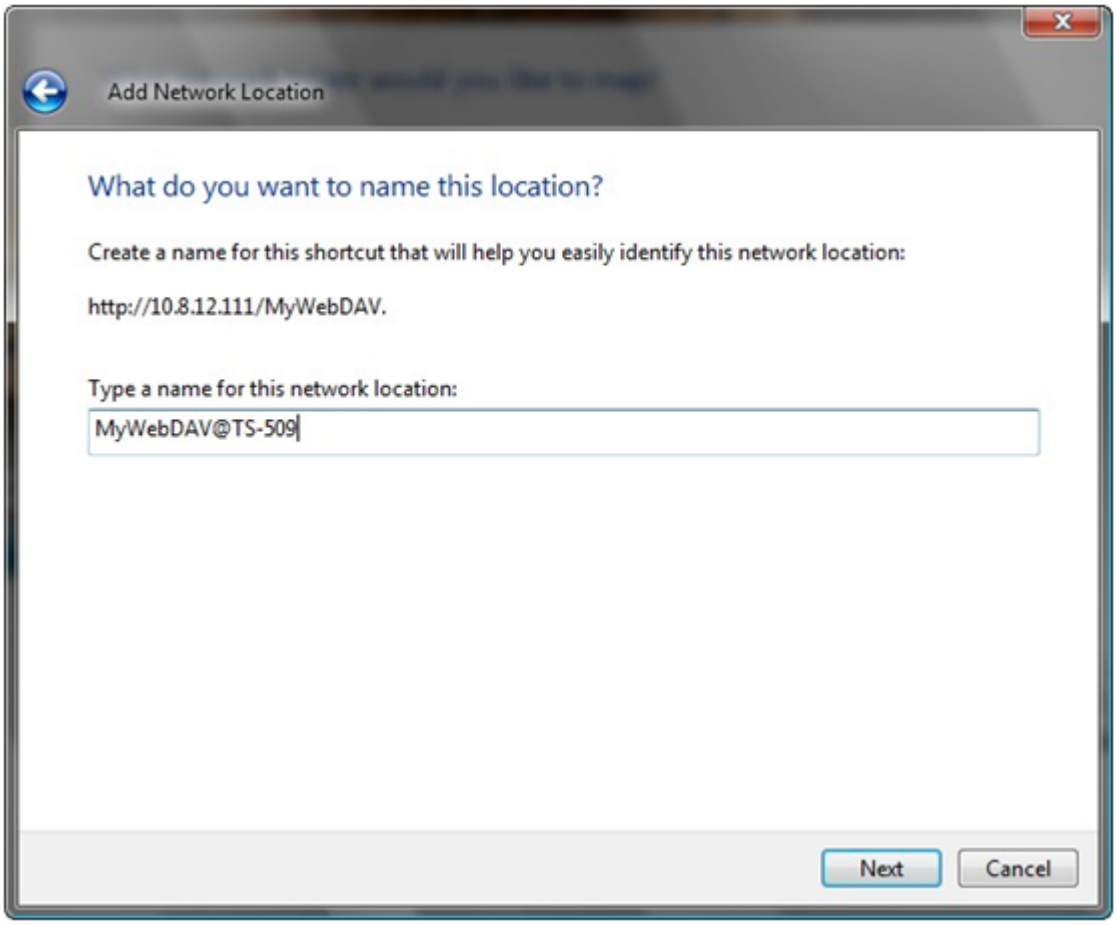
4. NASのURLを共フォルダ名と共に入力します。

フォーマット：http://NAS_IP_or_HOST_NAME/SHARE_FOLDER_NAME (http://NAS_IPまたはホスト名/共フォルダ名/)

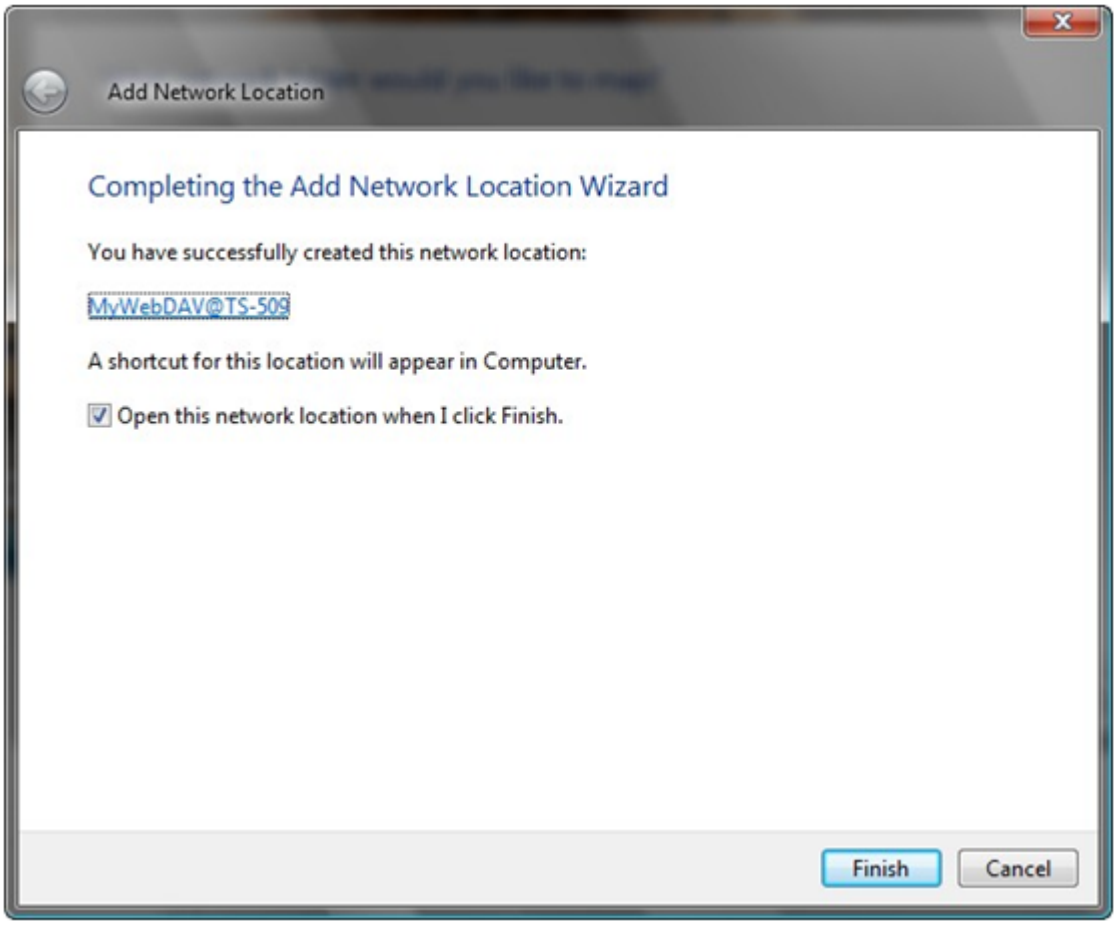


5. この共フォルダにアクセスするWebDAV権限を持つユーザー名とパスワードを入力します。

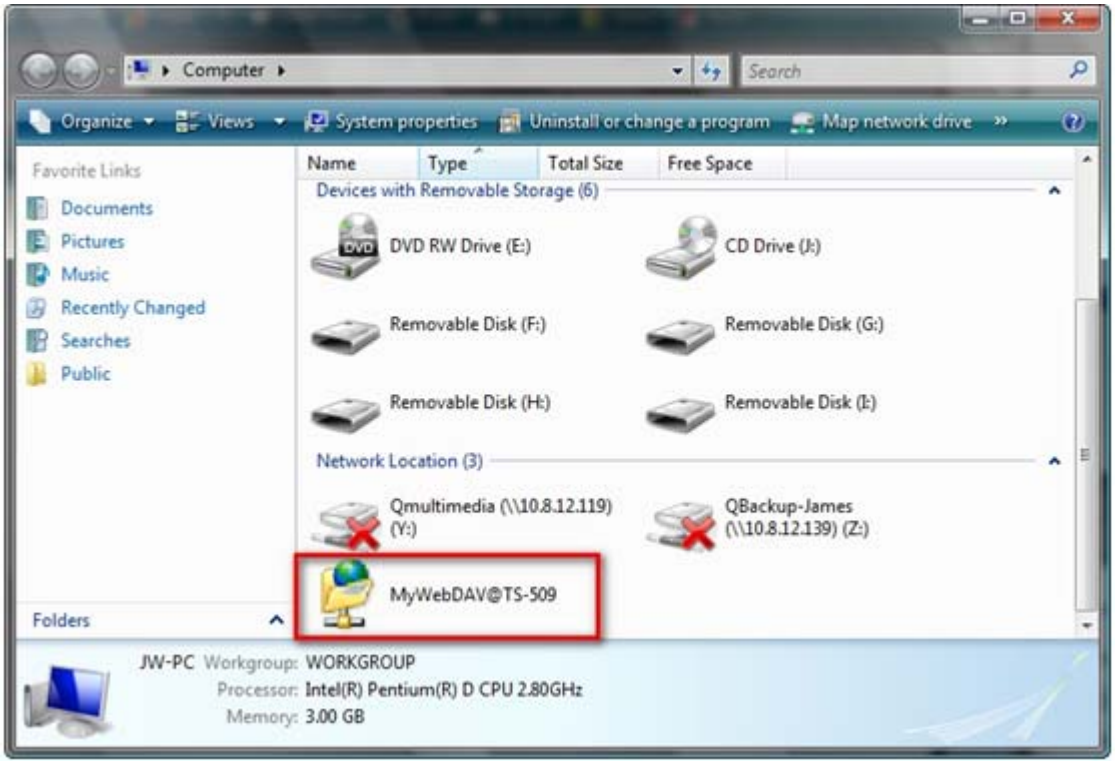
6. このネットワークの場所の名前を入力します。



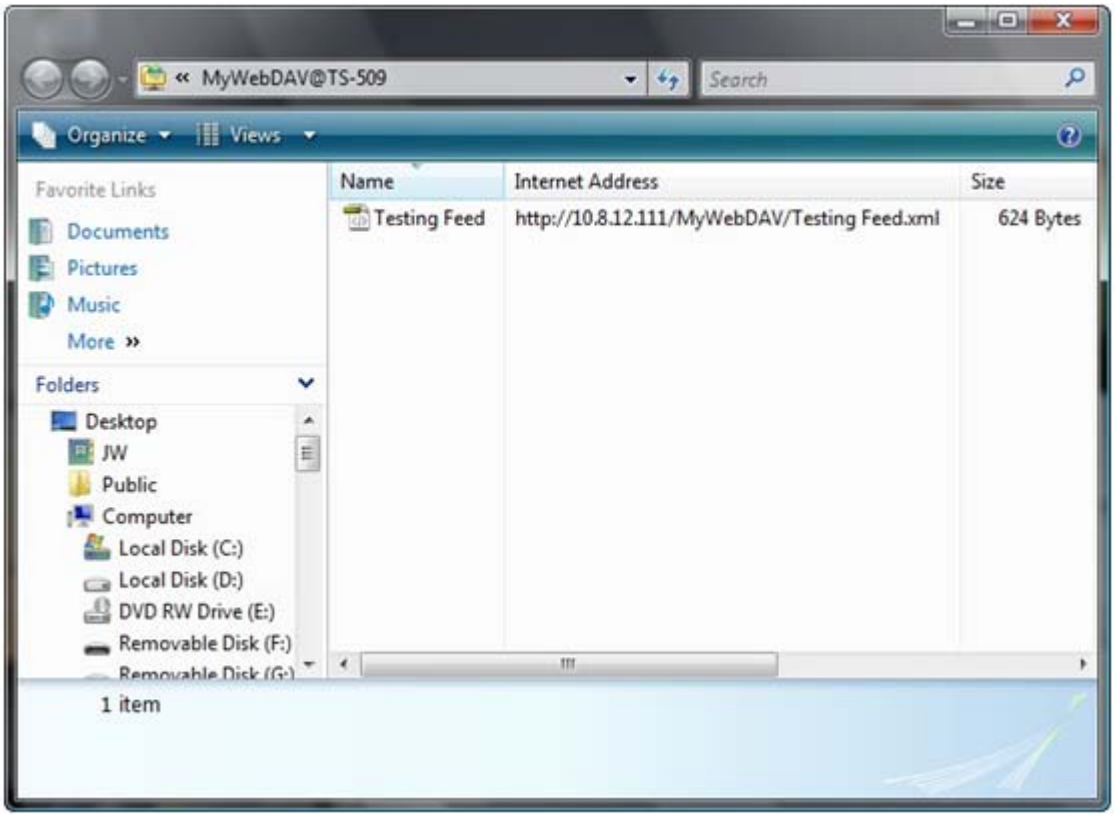
7. ウェブフォルダが正常に作成されました。



8. ウェブフォルダは "Computer" (コンピュータ) の"Network Location" (ネットワークの場所) セクションに作成されています。



9. この共フォルダにはこのリンクからHTTP/WebDAV経由でアクセスすることができます。



Mac OS X

Mac OS XのWebDAVを通してNASに接続するには以下の手順に従ってください。

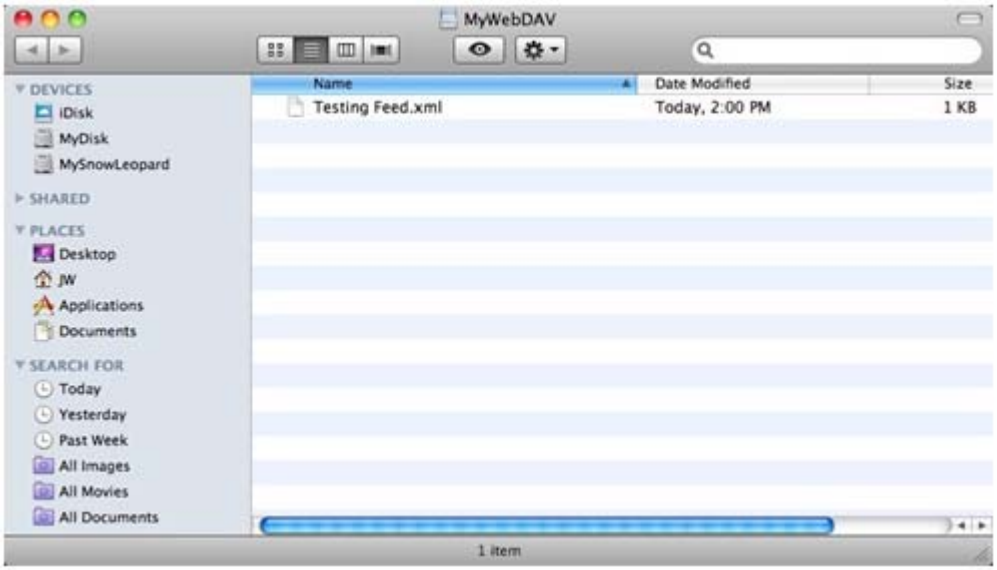
クライアントオペレーティングシステム： Mac OS X Snow Leopard (10.6.1)

1. "Finder" (ファインダ) > "Connect to Server" (サーバに接続) を開き、共フォルダのURLを入力します。

フォーマット: http://NAS_IP_or_HOST_NAME/SHARE_FOLDER_NAME (http://NAS_IPまたはホスト名/共フォルダ名/)

2. この共フォルダにアクセスするWebDAV権限を持つユーザー名とパスワードを入力します。

3. この共フォルダにはこのリンクから HTTP/WebDAV 経由でアクセスすることができます。



4. ファインダの "SHARED" (共) カテゴリからマウントポイントを確認し、これをログイン項目の一つにすることも可能です。

上記の説明はMac OS X 10.6に基づいたものです。10.4 以降に適用できます。

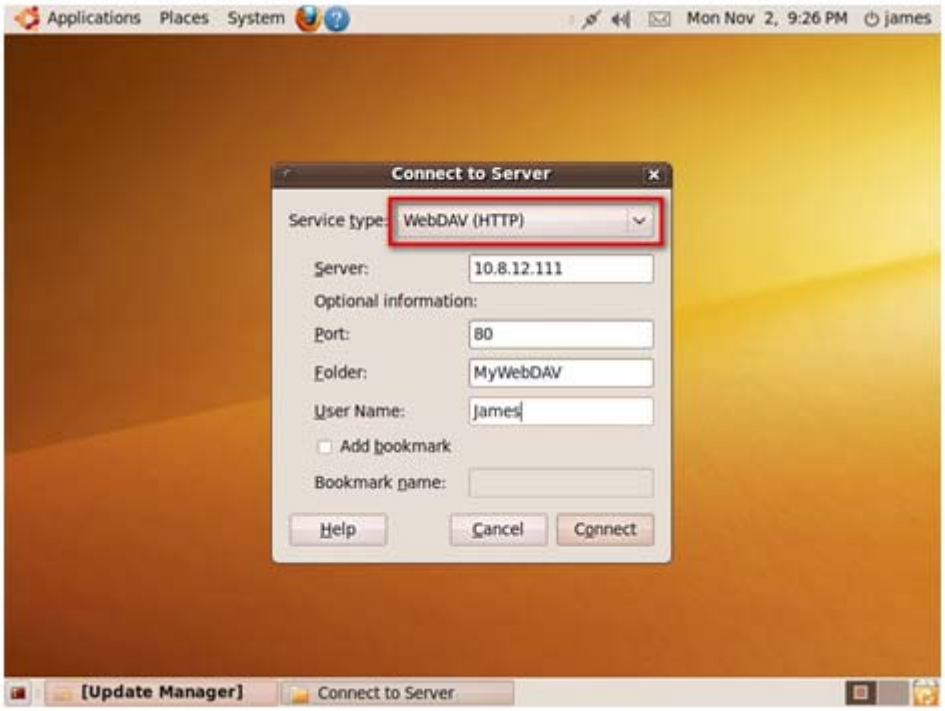
Ubuntu

Ubuntu の WebDAVを通してNASに接続するには以下の手順に従ってください。

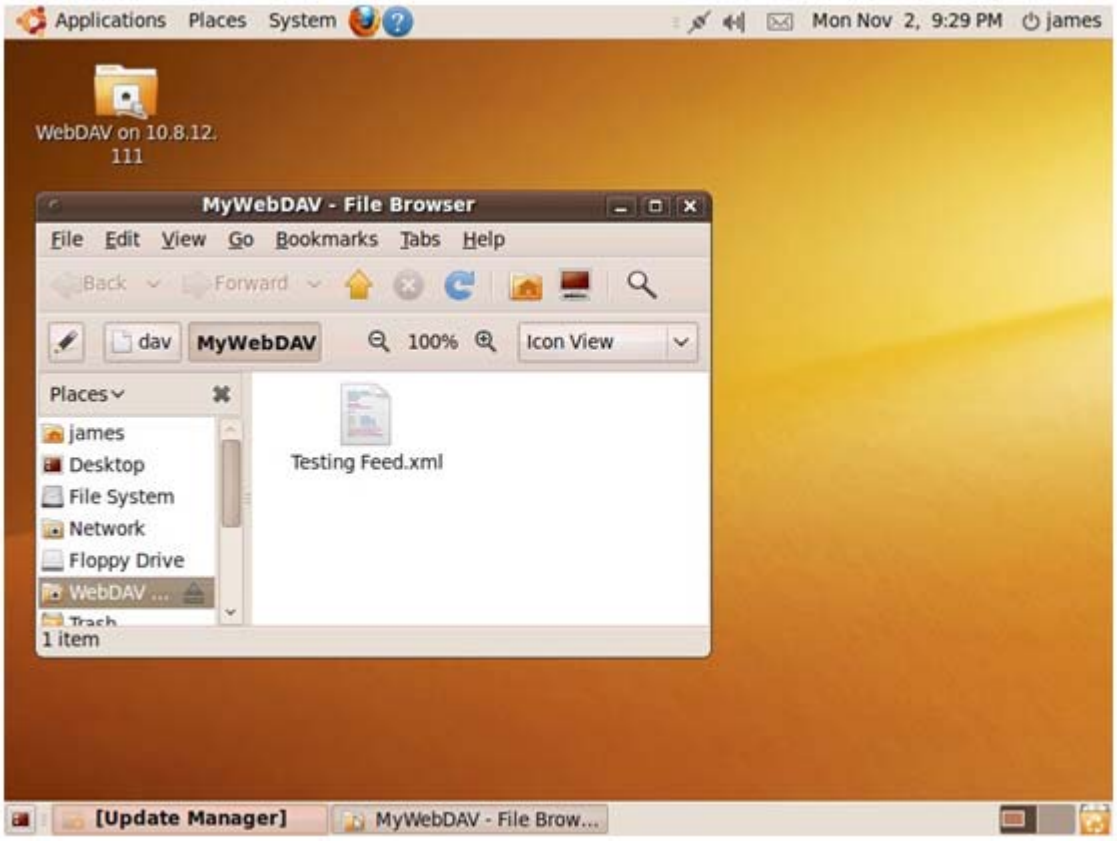
クライアントオペレーティングシステム: Ubuntu 9.10 Desktop

1. "Places" (場所) > "Connect to Server..." (サーバに接続) を開きます。

2. ご使用のNAS設定に合わせてService type (サービスタイプ) にて "WebDAV (HTTP)" あるいは "Secure WebDAV (HTTPS)" (セキュリティ保護WebDAV) を選択し、ホスト情報を入力します。この共フォルダにアクセスするWebDAV権限を持つユーザー名とパスワードを入力します。"Connect" (接続) をクリックして接続を初期化します。



3. このWebDAV接続は正常に確立されました。リンク先フォルダはデスクトップに自動的に作成されます。



MySQL管理

システムを初めてインストールするとき、phpMyAdminソフトウェアはMySQL管理ツールとして自動的にインストールされます。将来ファームウェアを更新するとき、phpMyAdminは再インストールされず、データベースのデータは上書きまたは更されません。
phpMyAdminプログラムファイルはQweb/ Web共フォルダに作成されます。ブラウザにURLを入力することで、フォルダ名を更しデータベースにアクセスできます。しかし、Web管理インターフェイスのリンクは更されません。

> 注: MySQLのデフォルトのユーザー名は「root」です。パスワードは「admin」です。phpMyAdmin管理インターフェイスにログインした後、直ちにルートパスワードを更してください。

SQLite管理

SQLiteManagerはSQLiteデータベースを管理する多言語のウェブベースツールで、http://www.sqlitemanager.org/ からダウンロードできます。
以下の手順に従うか、ダウンロードしたSQLiteManager-*.tar.gz? に含まれるINSTALLファイルを参照して、SQLiteManagerをインストールします。

- ダウンロードファイルSQLiteManager-*.tar.gzをアンパックします。
- アンパックしたフォルダSQLiteManager-*を\\NAS IP\Qweb\あるいは\\NAS IP\Web\にアップロードします。
- ウェブブラウザを開いて、http://NAS IP/SQLiteManager-*/にアクセスします。

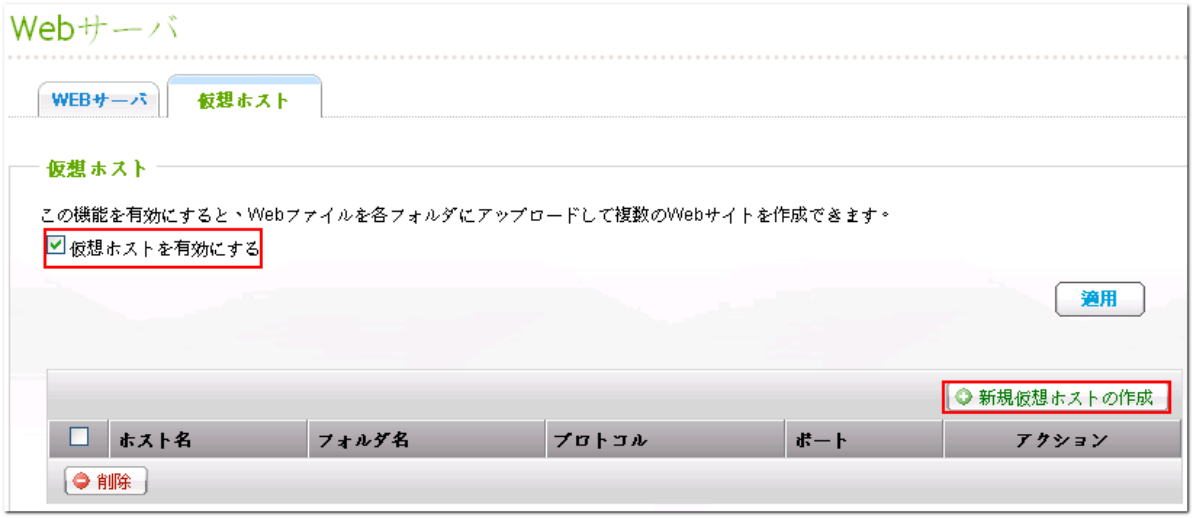
?: 「*」の記号はSQLiteManagerのバージョン番号を指しています。

6.7.1 仮想ホスト

この機能により、複数のウェブサイト(最大32)をNASにてホストすることができます。

仮想ホストを使用する前に、NASのWebサーバを効化してあることを確認してください。仮想ホストを使用するには、以下の手順に従ってください。

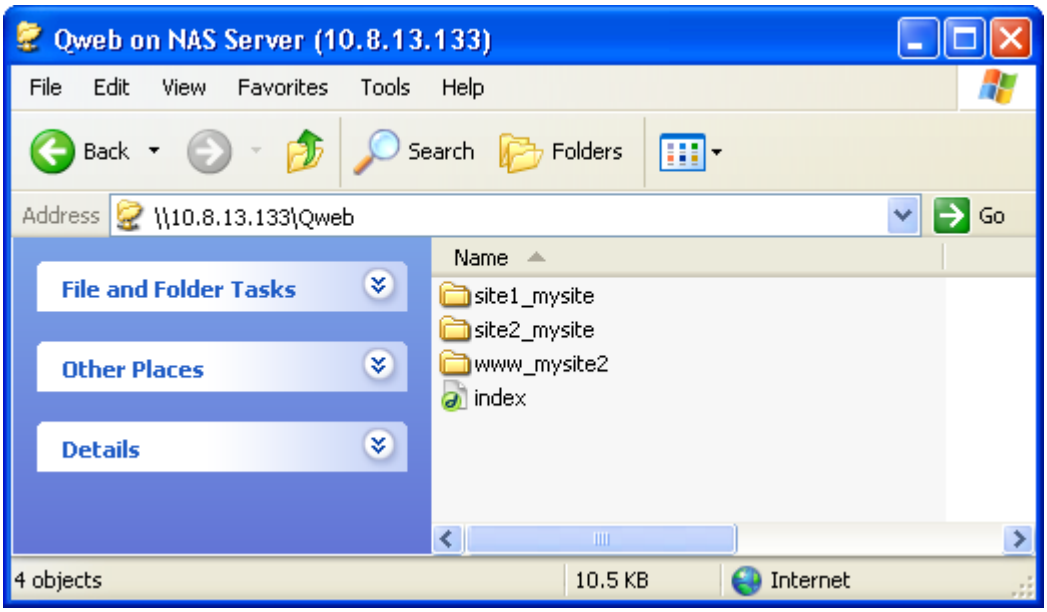
1. "Enable Virtual Host" (仮想ホストを有効にする)を選択し、"Apply" (適用) をクリックします。
2. 続いて "Create New Virtual Host" (新規仮想ホストの作成) をクリックします。



3. ホスト名を入力し、ウェブファイルをアップロードするフォルダ*(WebあるいはQweb下)を指定します。
4. 接続用プロトコル(HTTPまたはHTTPS)を指定します。HTTPSを選択した場合、Webサーバーのオプションの "Enable Secure Connection (SSL)" (セキュア接続(SSL)を効にする)がオンになっていることを確認してください。
5. 接続用ポート番号を指定します。
6. "Apply" (適用)をクリックします。

*ウェブファイル用には、"Access Right Management" (アクセス権限管理) > "Share Folders" (共フォルダ) のWeb あるいはQweb下に専用ファイルを作成するよう注意してください。

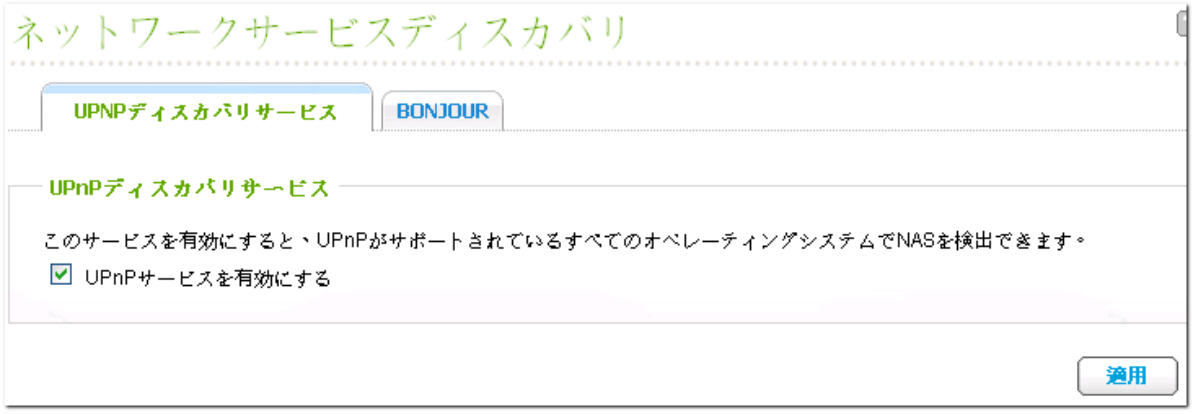
仮想ホストの作成後は、ウェブファイルを特定のフォルダにアップロードし、自分のウェブサイトをNAS上で公開することができます。その後、ウェブページにはその設定によりhttp://NAS_IP:ポート_番号 あるいは https://NAS_IP:ポート_番号 にて接続することができます。



6.8 ネットワークサーチサービス

UPnP探索サービス

ネットワークにデバイスが追加された際、ネットワーク上のコントロール ポイントに対し、デバイスはUPnP検出プロトコルによりそのサービスを提供することが出来ます。
UPnP検出サービスを効化することで、UPnPをサポートする全てのオペレーティングシステムがNASを検出できるようになります。



Bonjour

ご使用のMacは、Bonjourによりネットワークサービスを配信することで、NAS上で実行されているネットワークサービス(例:FTP)を、IPアドレスの入力やDNSサーバの構成の必要なしに、自動的に検出することが出来ます。

注:各サービス(例:FTP)をセットアップページにて効化し、その後Bonjourページにてまたサービスを効化します。これにより、NASはこのサービスをBonjourを通して提供できます。

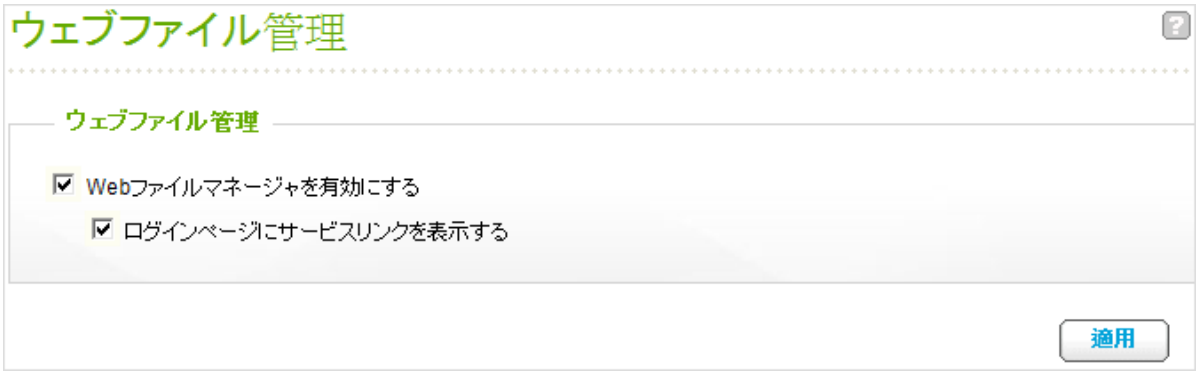
7. アプリケーション・サーバー

Webファイルマネージャ (Web File Manager) 306
マルチメディアステーション (Multimedia Station) 324
Photo Station 384
Music Station 405
ダウンロードステーション (Download Station) 425
監視ステーション (Surveillance Station) 448
iTunes サービス 456
UPnPメディアサーバ 459
MySQL サーバ 461
QPKG Center 463
Syslogサーバ 467
RADIUS サーバ 472
バックアップサーバー 476
アンチウイルス 480
TFTPサーバー 489
VPN サービス 490
LDAP サーバー 506

7.1 Webファイルマネージャ (Web File Manager)

この項目を効にすると、標準のサポートプロトコル以外に、Web ブラウザでファイルにアクセスできます。本製品がインターネットに接続され、インターネットで効なグローバルIP アドレスが設定されていれば、世界のどこからでもWeb ブラウザ経由でファイルにアクセスできます。

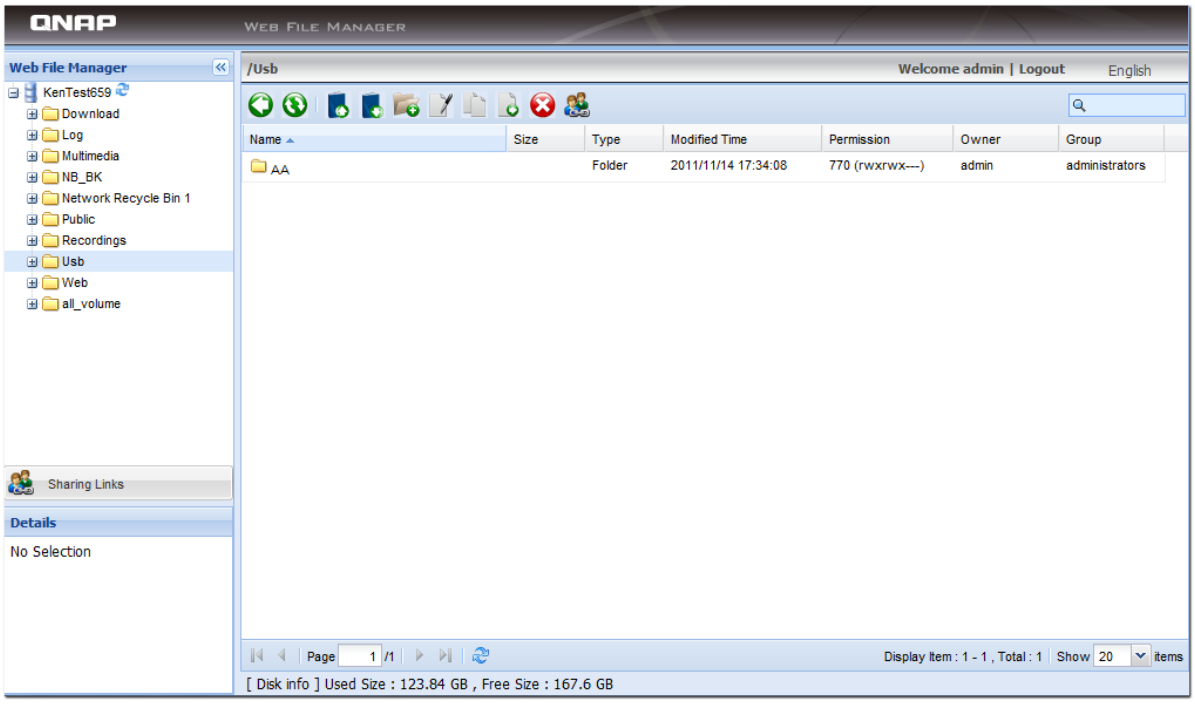
ウェブファイルマネージャを使用するには、「アプリケーション」 > 「ウェブファイルマネージャ」に移動し、サービスを効化します。



ページ上部あるいはNASログインページの"Web File Manager"をクリックし、ウェブファイルマネージャにアクセスします。NASログインページからサービスにログインする場合、ユーザー名およびパスワードを入力する必要があります。

> 注：Webファイルマネージャを使用する前に、ネットワーク共が作成されていることを確認してください。

NASのネットワーク共フォルダを整理することができます。ウェブファイルマネージャにより、ネットワーク共内のファイル及びフォルダを、アップロード、ダウンロード、名前更、移動、コピー、あるいは消去することができます。

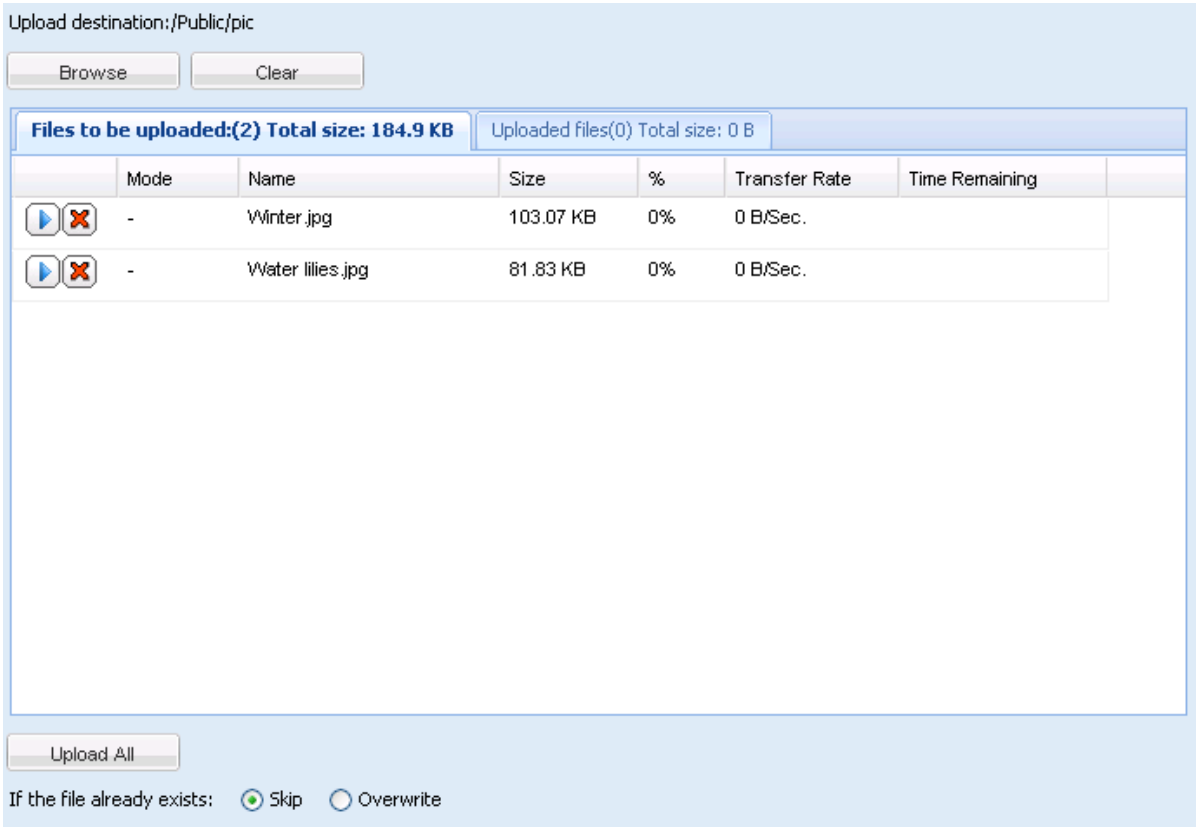


ファイルのアップロード

> 注：Web ファイルマネージャーを介して NAS にアップロードできるファイルの最大サイズは 2 ギガバイトです。

この機能を使用するには、Adobe Flash プラグインをご使用のウェブブラウザにインストールしてください。

i. フォルダを選択し、 をクリックします。
ii. 「Browse（参照）」をクリックして、ファイルを選択します。
iii. フォルダ内の既存ファイルの「Skip（スキップ）」または「Overwrite（上書き）」を選択します。
iv. をクリックしてファイルをアップロードするか、「Upload All（すべてアップロード）」をクリックして選択したファイルをすべてアップロードします。



ファイルをダウンロードする

1. ダウンロードしたいファイルあるいはフォルダを選択します。
2. マウスを右クリックして"Download" (ダウンロード) を選択、あるいは をクリックしてファイルをダウンロードします。

フォルダの作成

1. 新しいフォルダを作成するネットワーク共またはフォルダを選択します。
2. ツールバーで (フォルダの作成)をクリックします。
3. 新しいフォルダ名を入力し、OKをクリックします。

ファイルまたはフォルダの名称更

1. 名称更するファイルまたはフォルダを選択します。
2. ツールバーで (名称変更) をクリックします。
3. 新しいファイルまたはフォルダ名を入力し、OKをクリックします。

ファイルまたはフォルダをコピーする

1. コピーしたいファイルまたはフォルダを選択します。
2. (コピー) をクリックします。
3. コピー先フォルダを選択します。
4. コピー先フォルダ内の既存のファイルをスキップするか上書きするかを選択します。"OK" をクリックします。

ファイルまたはフォルダを移動する

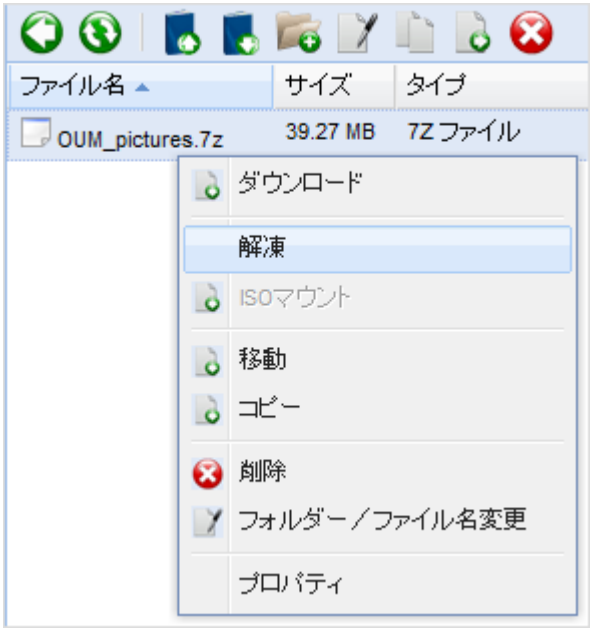
1. 移動したいファイルまたはフォルダを選択します。
2. (移動) をクリックします。
3. 移動先フォルダを選択します。
4. 移動先フォルダ内の既存のファイルをスキップするか上書きするかを選択します。"OK" をクリックします。

ファイルまたはフォルダの削除

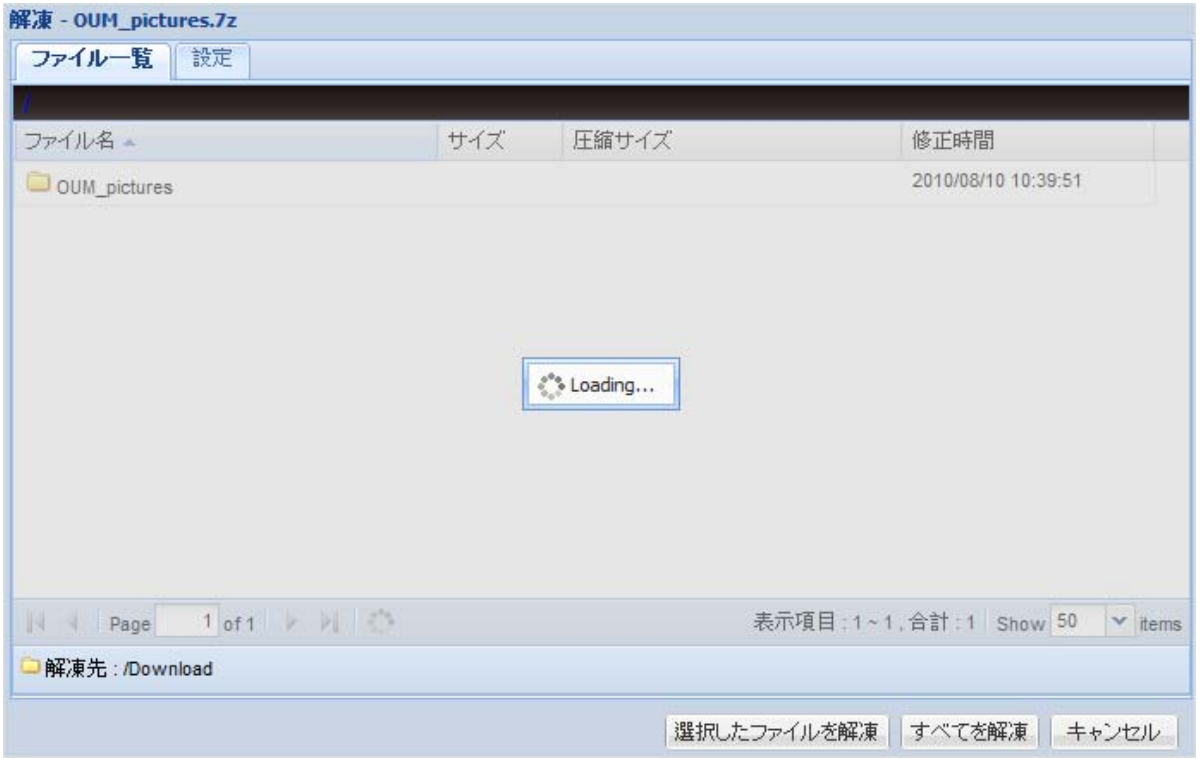
1. 削除するファイルまたはフォルダを選択します。
2. ツールバーで (削除)をクリックします。
3. ファイルまたはフォルダの削除を確認します。

ファイルを解凍する

1. ZipファイルをNAS上で解凍するには、Zipファイル上で右クリックし、"Extract" (解凍) を選択します。

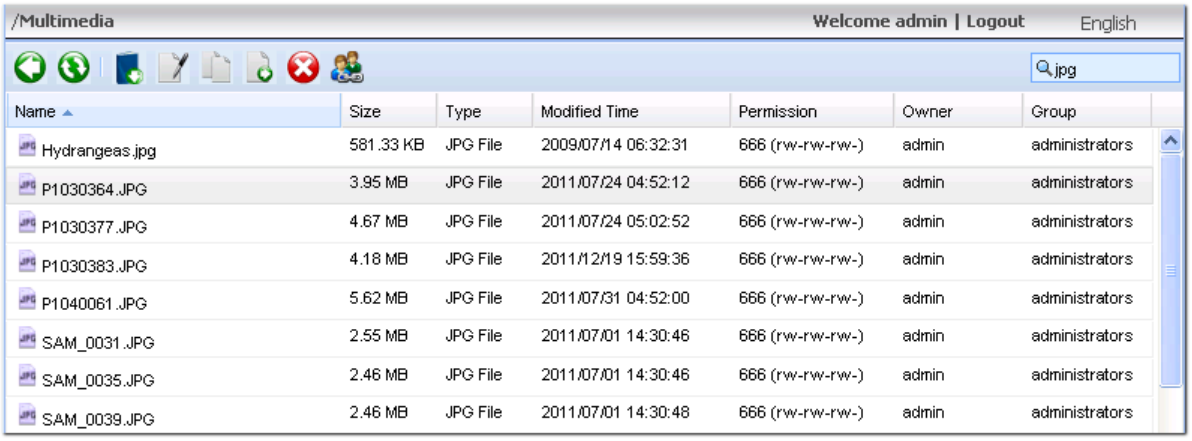


2. 解凍するファイルを選択し、解凍設定を構成します。



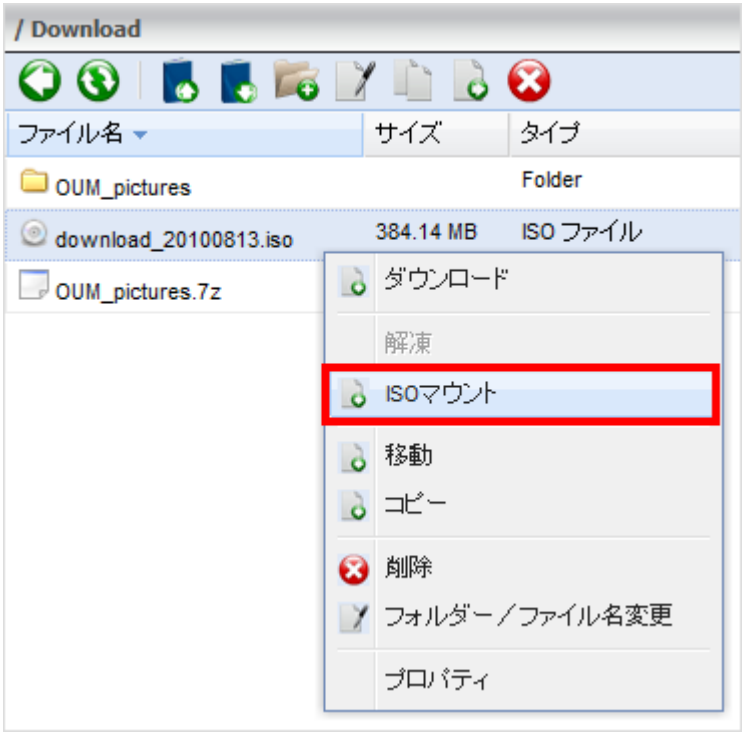
ファイル/フォルダ検索

Web File Manager (ウェブファイルマネージャ)は、NAS上にあるファイル、サブフォルダ、フォルダのスマート検索をサポートしています。ファイルまたはフォルダ名のすべてあるいは一部、またファイルの拡張子(AVI、MP3など)によってファイルやフォルダを検索することができます。

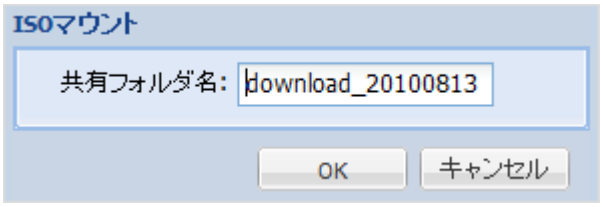


ISO共有のマウント

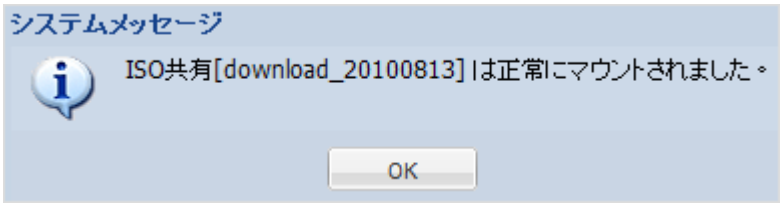
NASにISOファイルを共フォルダとしてマウントするには、下記の手順に従ってください。
NAS上のISOファイルを検索します。ファイルを右クリックし、"Mount ISO" (ISOをマウント)を選択します。



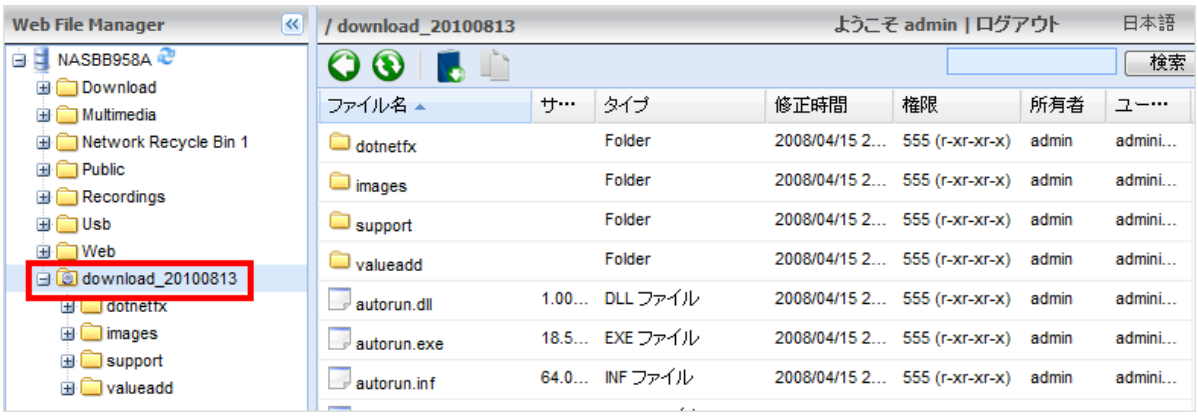
共フォルダ名を入力し、"OK"をクリックします。



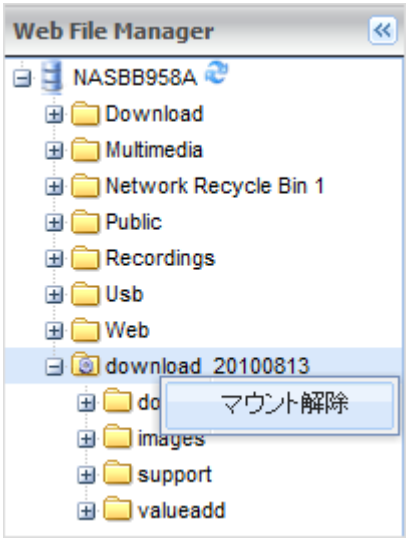
"OK"をクリックして確定します。



共フォルダリストにISO共フォルダが表示されます。ISO画像ファイルのコンテンツにアクセスすることもできます。NASウェブインターフェイスに管理者アカウントでログインし、ユーザーのアクセス権限を"Access Right Management"（アクセス権限管理）> "ISO Share Folders"（ISO共フォルダ)にて特定します。

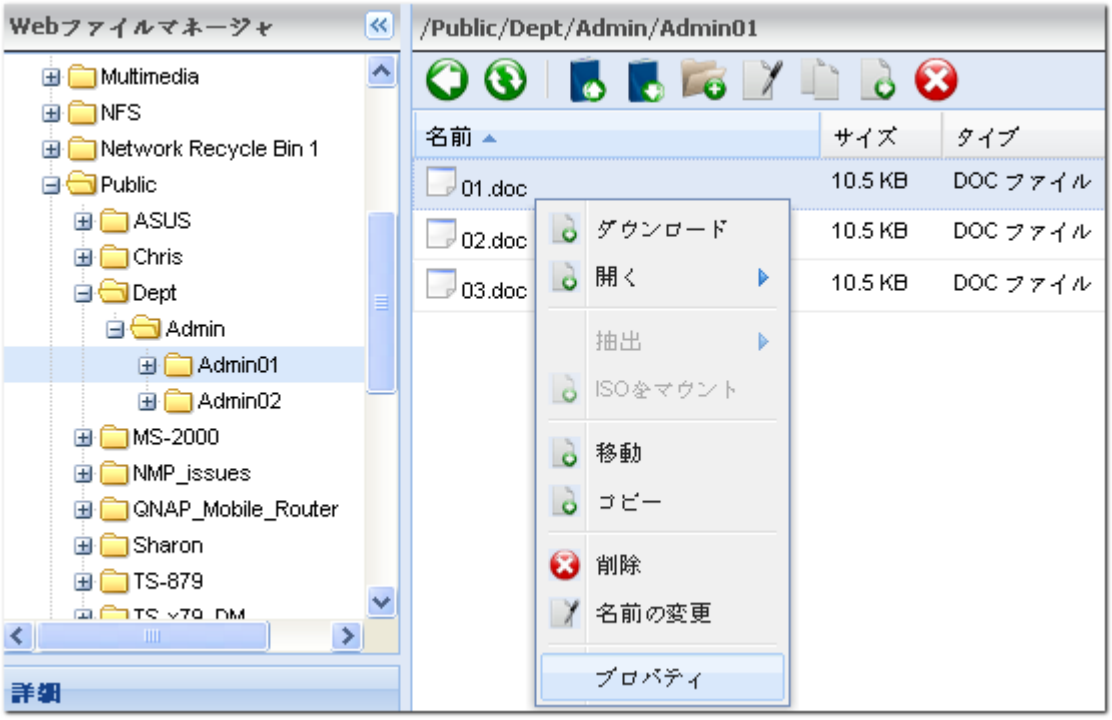


共フォルダをマウント解除するには、フォルダ名を右クリックし、"Unmount"（マウント解除)を選択します。 続いて"OK"をクリックします。



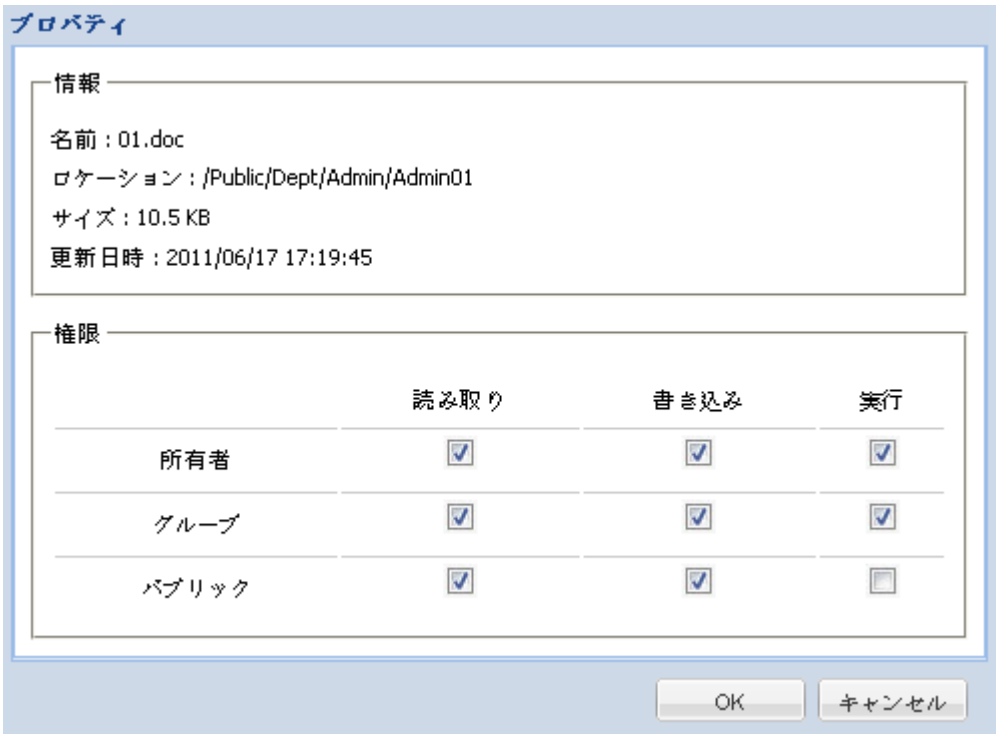
ファイル/フォルダレベル許可

Web File Managerにより、NASでファイルレベルまたはフォルダレベル許可を設定できます。ファイルまたはフォルダを右クリックして、「Properties(プロパティ)」を選択します。



「Advanced Folder Permissions(拡張フォルダ許可)」オプションが「Access Right Management(アクセス権管理)」>「Share Folder(フォルダの共有)」>「Advanced Options(拡張オプション)」で無効になっている場合、次の設定が表示されます。オーナー、グループ、およびパブリックに対してアクセス権の読み取り、書き込み、実行を定義します。

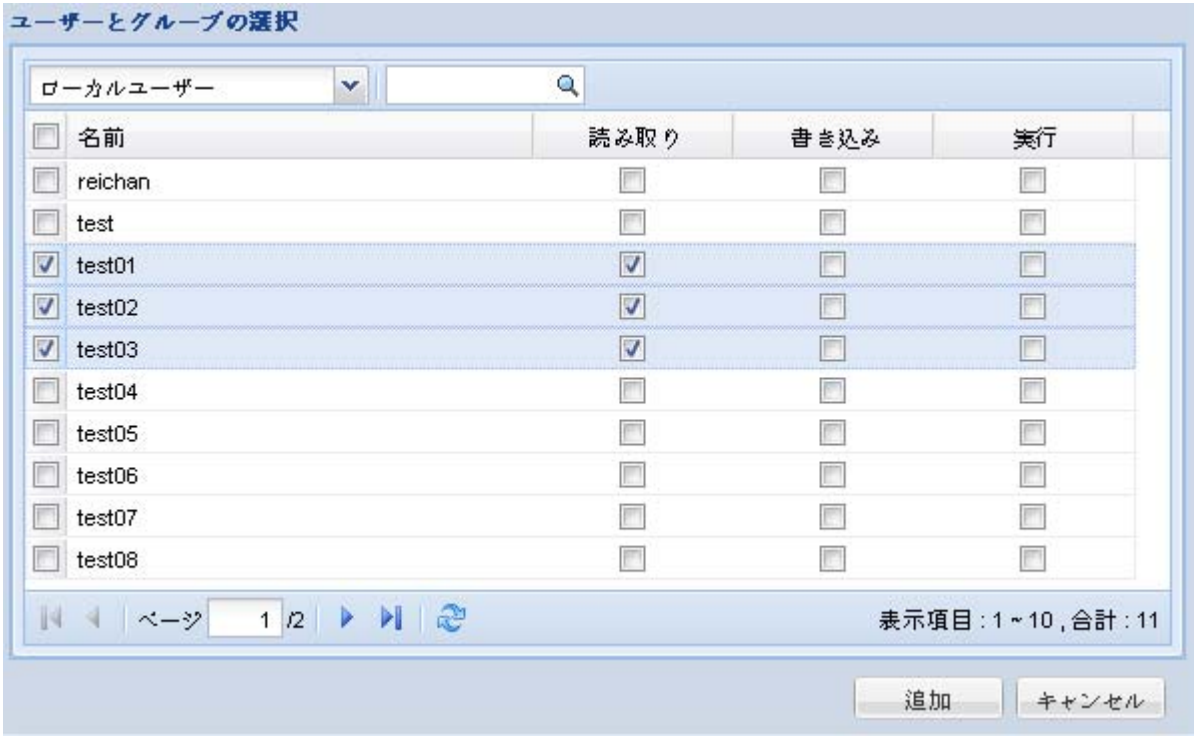
- オーナー: ファイルまたはフォルダのオーナー。
- グループ: ファイルまたはフォルダのグループオーナー。
- パブリック: グループオーナーのオーナーまたはメンバーでない他のすべての(ローカルまたはドメインメンバー)ユーザー。



フォルダが選択されている場合、「Apply changes to folder(s), subfolder(s) and file(s)(変更をフォルダ、サブフォルダおよびファイルに適用する)」を選択して設定を選択したフォルダ内部のすべてのファイルやサブフォルダに適用できます。「OK」をクリックして確認します。

「拡張フォルダ許可」オプションが「Access Right Management（アクセス権管理）」>「Share Folder（フォルダの共有）」>「Advanced Options（拡張オプション）」で有効になっている場合、ユーザーとユーザーグループでファイルとフォルダ許可を指定することができます。 をクリックします。

ユーザーとユーザーグループを選択し、読み取り、書き込み、および実行権利を指定します。「Add（追加）」をクリックします。



リストの許可を削除するには、ユーザーまたはユーザーグループを選択し、 をクリックします。

をクリックすることで、ファイルとフォルダオーナーを定義することもできます。リストからユーザーを選択するか、ユーザー名を検索します。「Set（設定）」をクリックします。

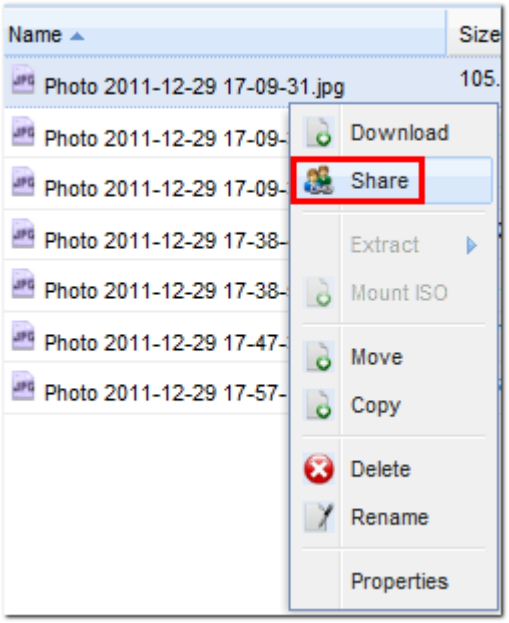
フォルダ許可設定に対して、次のオプションを利用できます。「Access Right Management（アクセス権管理）」>「Share Folders（フォルダの共有）」 230でフォルダ許可とサブフォルダ許可を設定することをお勧めします。

- Only the owner can delete the contents（所有者のみがコンテンツを削除できます）。このオプションをフォルダに適用すると、第一レベルのサブフォルダとファイルはそのオーナーでのみ削除できます。
- Apply changes to files and subfolders（変更をファイルとサブフォルダに適用します）：オーナー保護以外の変更済み許可設定を、選択したフォルダ内部のすべてのファイルとサブフォルダに適用します。オプション「Only the owner can delete the contents（所有者のみがコンテンツを削除できます）」はサブフォルダに適用されません。
- Apply and replace all existing permissions of this folder, files, and subfolders（このフォルダ、ファイル、サブフォルダの既存の許可をすべて適用して置換します）：オーナー保護を除き、選択したフォルダとそのファイルおよびサブフォルダのそれまでに設定された許可をすべて無効にするには、このオプションを選択します。オプション「Only the owner can delete the contents(所有者のみがコンテンツを削除できます)」はサブフォルダに適用されません。

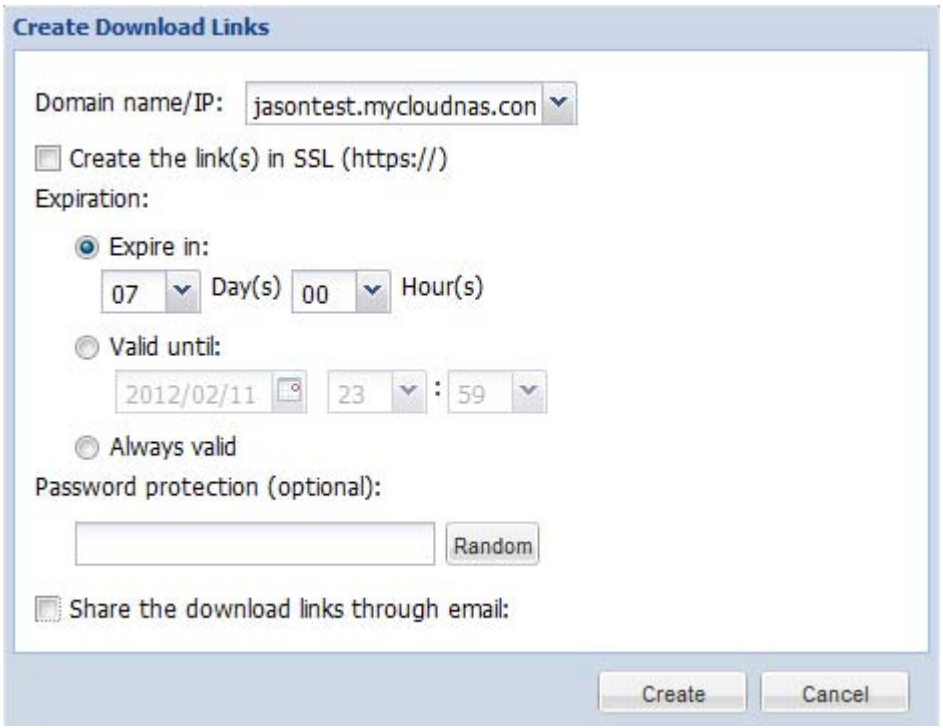
ファイル共有

注：この機能は、admin でのみ利用できます。

Web ファイルマネージャを使って NAS 上でファイル共有を行うには、 をクリックするか、ファイルを右クリックして、「Share（共有）」を選択します。

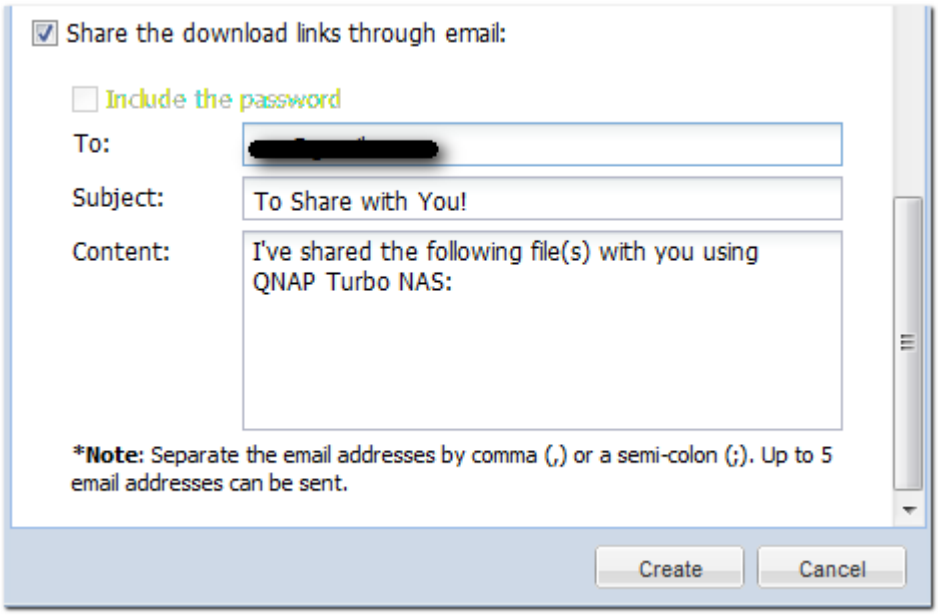


NAS の IP または「Domain name（ドメイン名）」を選択します。「Create the link(s) in SSL（SSL によるリンクを作成する）」（オプション）を選択し、「Expiration（有効期限）」を指定して、「Password（パスワード）」を入力します（オプション）。

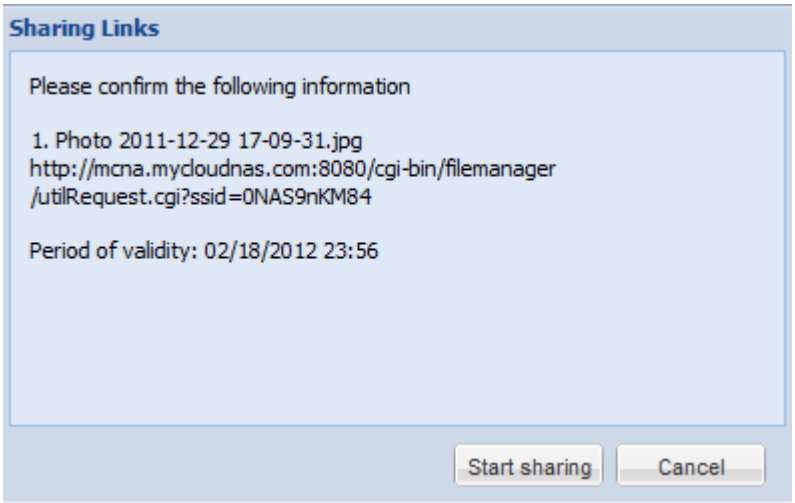


電子メールでリンクを共有するには、「Share the download links through email（電子メールを通してダウンロードリンクを共有する）」を選択し、コンテンツを入力します。「Create（作成）」をクリックします。

注：この機能を使用するには、「System Administration（システム管理）」>「Notification（通知）」>「Configure SMTP Server（SMTP サーバーの設定）」でメールサーバー設定を適切に行う必要があります。



情報を確認し、「Start Sharing（共有開始）」をクリックします。



7.2 マルチメディアステーション (Multimedia Station)

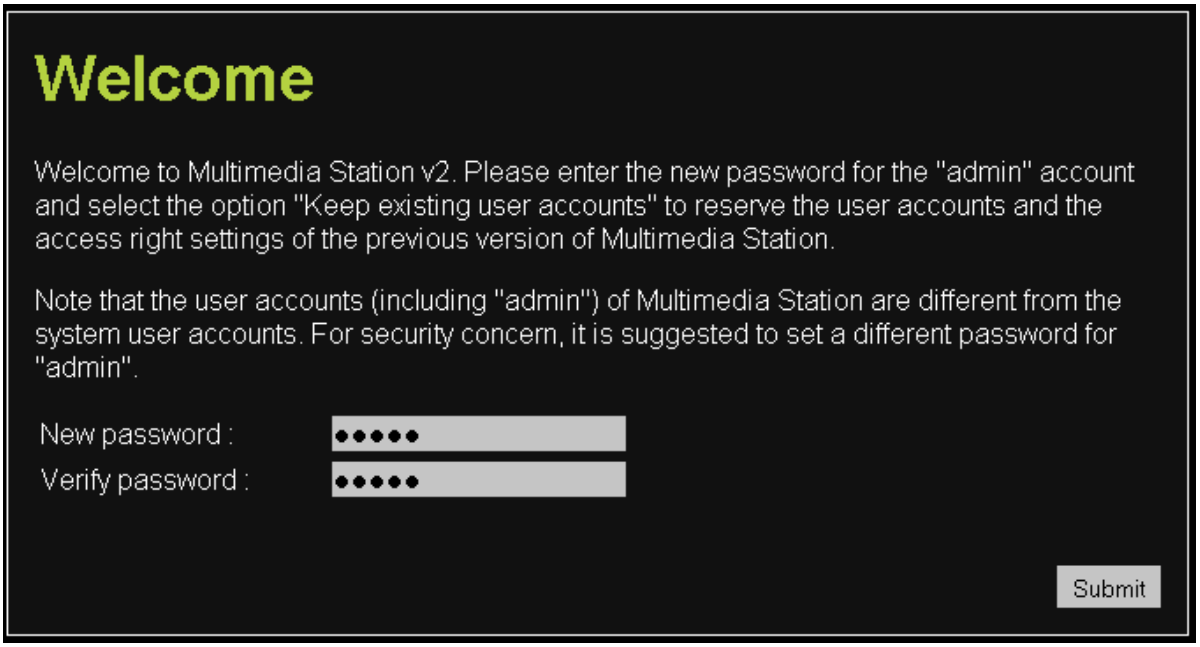
Multimedia Station (マルチメディアステーション) はウェブベースのアプリケーションで、ご自分の写真、音楽、ビデオをウェブブラウザによりNAS上で再生できるようにします。マルチメディアファイルをお友達と共したり、写真をFacebook、Plurk、Twitter、Bloggerなどの人気のソーシャルネットワークにて公開することもできます。

Multimedia Stationを使用するには、以下の手順に従ってください。

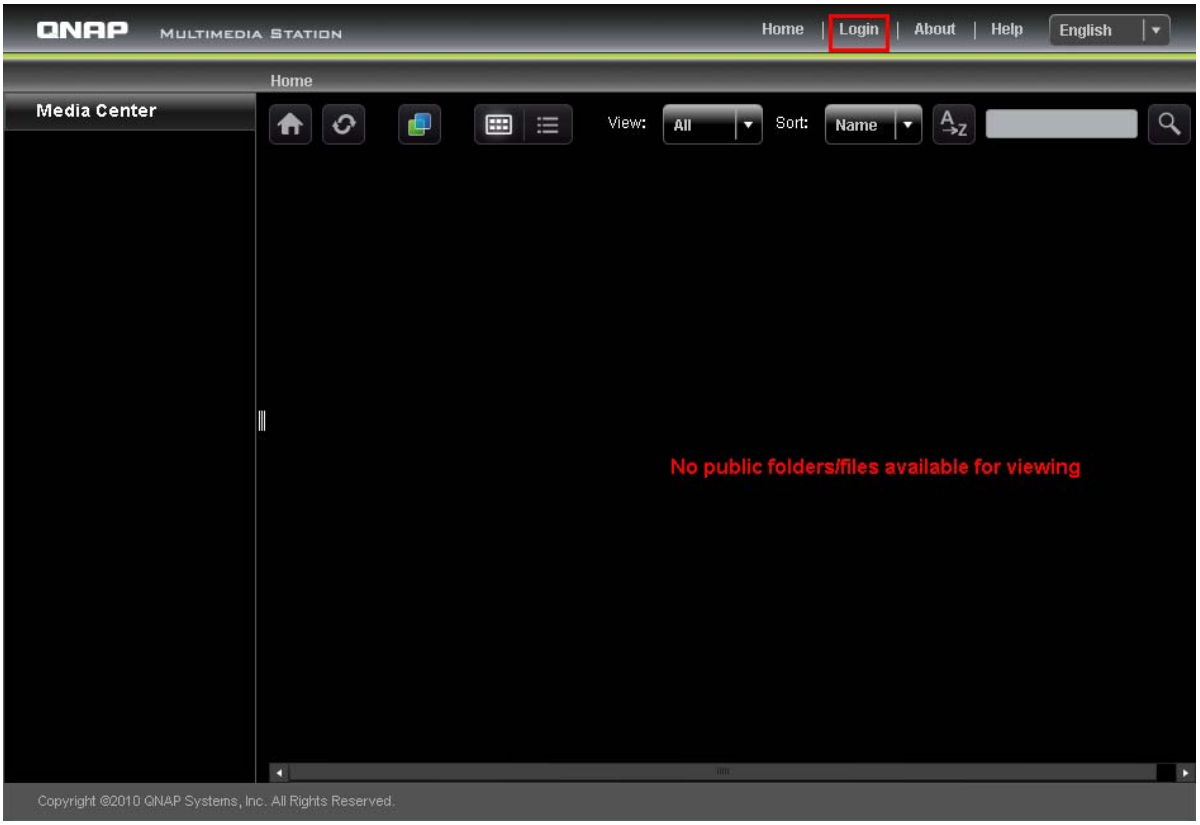
1. "Network Services" (ネットワークサービス) > "Web Server" (Webサーバ)に移動します。ウェブサーバ機能をオンにします。Multimedia StationへのHTTPSによるアクセスを許可するには、"Enable Secure Connection" (SSL) (セキュリティ接続(SSL)を効化する) のオプションをオンにします。

2. "Application Servers" (アプリケーション・ サーバー) > "Multimedia Station" を開きます。サービスを効にします。その後、Multimedia Stationのウェブページに http://NAS_IP:80/MSV2/ あるいは https://NAS_IP:8081/MSV2/ (セキュリティ接続) にて移動します。設定によりポート番号は異なる場合があります。

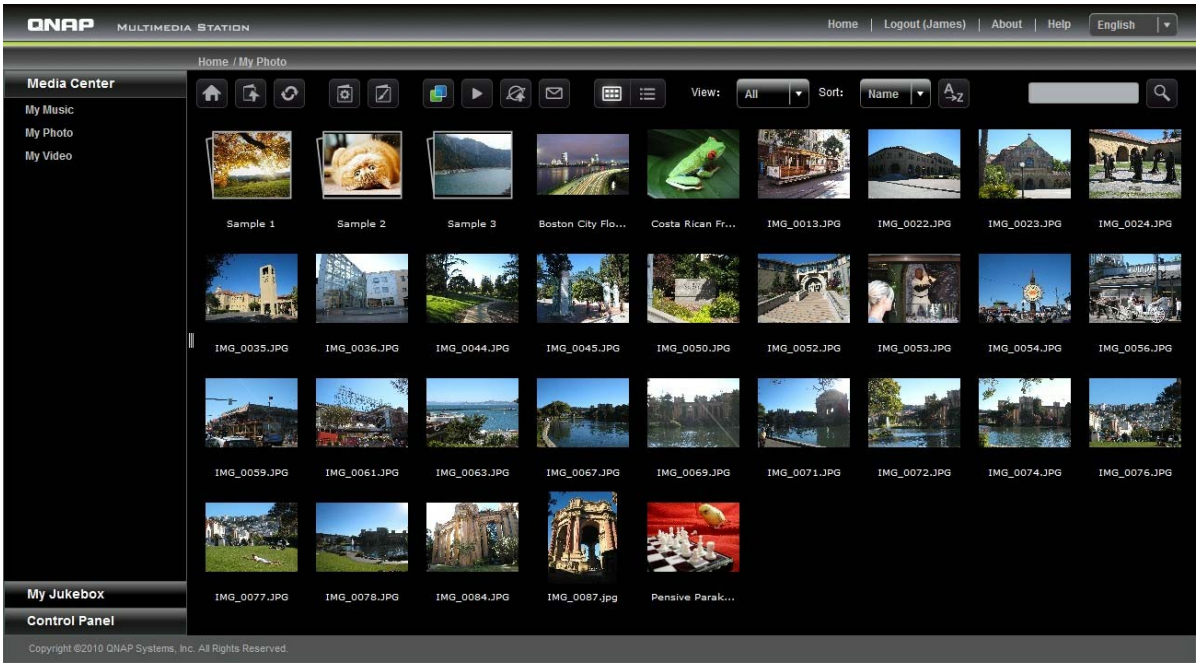
3. Multimedia Stationに初めて接続する際は、"admin" (管理者) アカウントに新しいパスワードを入力します。続いて "Submit" (送信) をクリックします。前バージョンのMultimedia Stationにてユーザーアカウントを既に作成してある場合は、"Keep existing user accounts" (既存のユーザーアカウントを維持する) を選択してユーザーアカウントを保持することができます。 Multimedia Stationのユーザーアカウント (管理者を含む) はNASのシステムユーザーアカウントとは異なりますので注意してください。安全性の問題から、管理者には異なるパスワードを設定するよう強く推奨いたします。パスワードには1-16文字まで使うことができます。パスワードに効な文字はA-Z, a-z, 0-9, -, !, @, #, $, %, _です。



4. Multimedia Station のページが表示されたら、"Login" (ログイン) をクリックします。このサービスにアクセス権のあるユーザー名及びパスワードを入力します。管理者 (admin) としてログインした場合は、新しいユーザーを作成し、その他の詳細設定を構成することができます。



Multimedia Stationは、Media Center (メディアセンター)、My Jukebox (マイ·ジュークボックス)、およびControl Panel (コントロールパネル)により構成されます。



Media Center (メディアセンター)

Multimedia Stationのデフォルトネットワーク共 (Qmultimedia / Multimedia) のフォルダおよびマルチメディアファイルは、Media Center (メディアセンター) にて表示されます。NAS上のマルチメディアコンテンツ(画像、ビデオ、およびオーディオファイル)を、LANあるいはWAN経由でウェブブラウザにて表示または再生することができます。

サポートされているファイル形式

タイプ	ファイル形式
オーディオ	MP3
画像	JPG/JPEG, GIF, PNG (アニメーションGIFファイルではアニメーションは表示されません)
ビデオ	再生:FLV, MPEG-4 ビデオ (H.264 + AAC) トランスコード:AVI, MP4, M4V, MPG, MPEG, RM, RMVB, WMV (ファイルはFLVに換されます)

	ホーム Multimedia Stationのホームディレクトリに戻ります。
	親ディレクトリ 親ディレクトリに戻ります。
	更新 現在のディレクトリを更新します。
	アルバムの管理* 以下の内容が可能です: 1. 現在のディレクトリ下に新規アルバムを作成、および 2. このディレクトリにファイルをコピーあるいはアップロードすることで、このアルバムに新規ファイルを追加
	アルバムカバーの設定* 各アルバム/ディレクトリに対して、そのアルバム/ディレクトリ内から写真を一枚指定してアルバムカバーとして設定することができます。
	Cooliris Coolirisを使って写真を3D表示することができます。はじめにCoolirisプラグインのインストールが必要です。
	スライドショー スライドショーを開始します。フォトフレーム、バックグラウンドミュージック、およびアニメーションをスライドショーモードにて設定することができます。
	公開* 選択した写真 (最大5枚まで) を人気のソーシャルネットワークサイトに公開します。現在のサポート先は以下のとおりです:Twitter, Facebook, MySpace, Plurk, Windows Live, および Blogger.公開の前に、アルバムをパブリック (コントロールパネル > Set Folder Public (フォルダをパブリック(公開)に設定) に設定し、またインターネットからMultimedia Stationにアクセスできる必要があります。この機能を使用する前に、NAS向けにDDNSをセットアップすることが推奨されます。
	電子メール* 写真(最大5枚まで)をお友達に電子メールで送信します。この機能を使用する前に、NAS管理コンソール内でSMTPサーバをセットアップする必要がありますので注意してください。
	サムネイル ファイルをサムネイル表示できます。Multimedia Stationでは、これはデフォルト設定です。
	詳細 ファイルを詳細表示できます。以下の機能をサポートしています:開く、名前の更、削除、ダウンロード、全画面表示
	分類 ファイルをアルファベットの昇順あるいは降順で分類するよう選択することができます。
	検索

	この機能によりファイルを検索することができます。現在のディレクトリ内での検索のみサポートしています。

*管理者のみ操作できるオプション

音楽を再生

NASはウェブブラウザ上の音楽ファイルの再生をサポートしています。ウェブページ上でファイル(MP3) をクリックするだけで、NASが再生します。フォルダ内の音楽ファイルをクリックした場合は、フォルダ内にある他の音楽ファイルも、サポートされる場合に限り、再生リストに表示され、再生されます。'X'をクリックし、再生ページを終了します。

画像ファイルの表示

画像ファイルを表示している際に "EXIF" をクリックすると、ファイル名、サイズ、日付、および効口径などの詳細情報が表示されます。ファイルにキャプションを追加するには、"Edit caption" (キャプションの編集)をクリックし説明を入力します。 説明は512文字まで可能です。

画像ファイルに対するコメントを送信し、また他のユーザーからのコメントを"All comments" (全てのコメント)にて表示することができます。各コメントは128文字まで可能です。

バックグランドミュージックの設定

画像ファイルあるいは画像ファイルのフォルダにバックグランドミュージックを設定するには、Multimedia Station の "Control Panel" (コントロールパネル) > "Playlist Editor" (再生リストエディタ) (後ほど説明) にて再生リストを作成しておく必要があります。

Media Center にて画像ファイルを開き、 をクリックします。

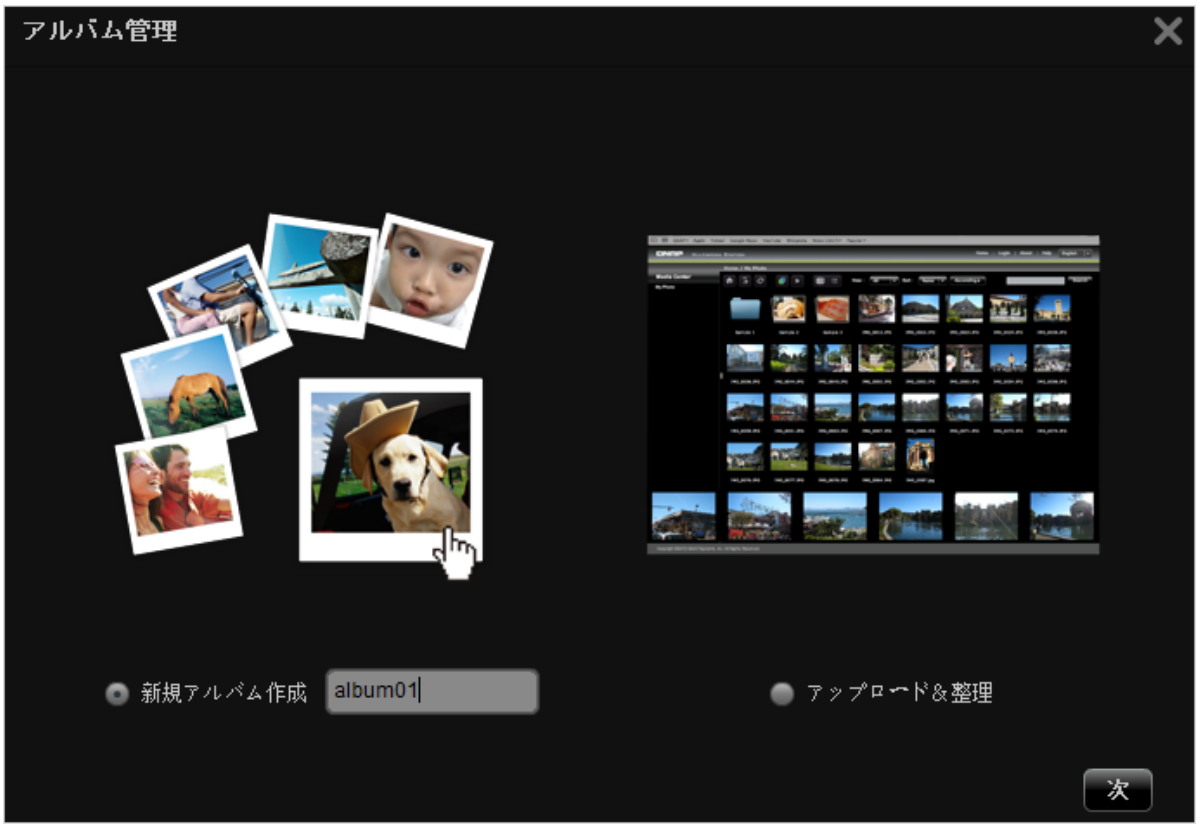
再生リストを選択し、"Save" (保存)をクリックします。バックグラウンドミュージックを削除するには、"No music" (音楽なし) を選択します。

アルバムの作成

Multimedia Station のウェブベースのインターフェイスを使用してアルバム (フォルダ) を作成するには、Media Center にてディレクトリを作成します。 (Create Album)(アルバム作成) をクリックします。

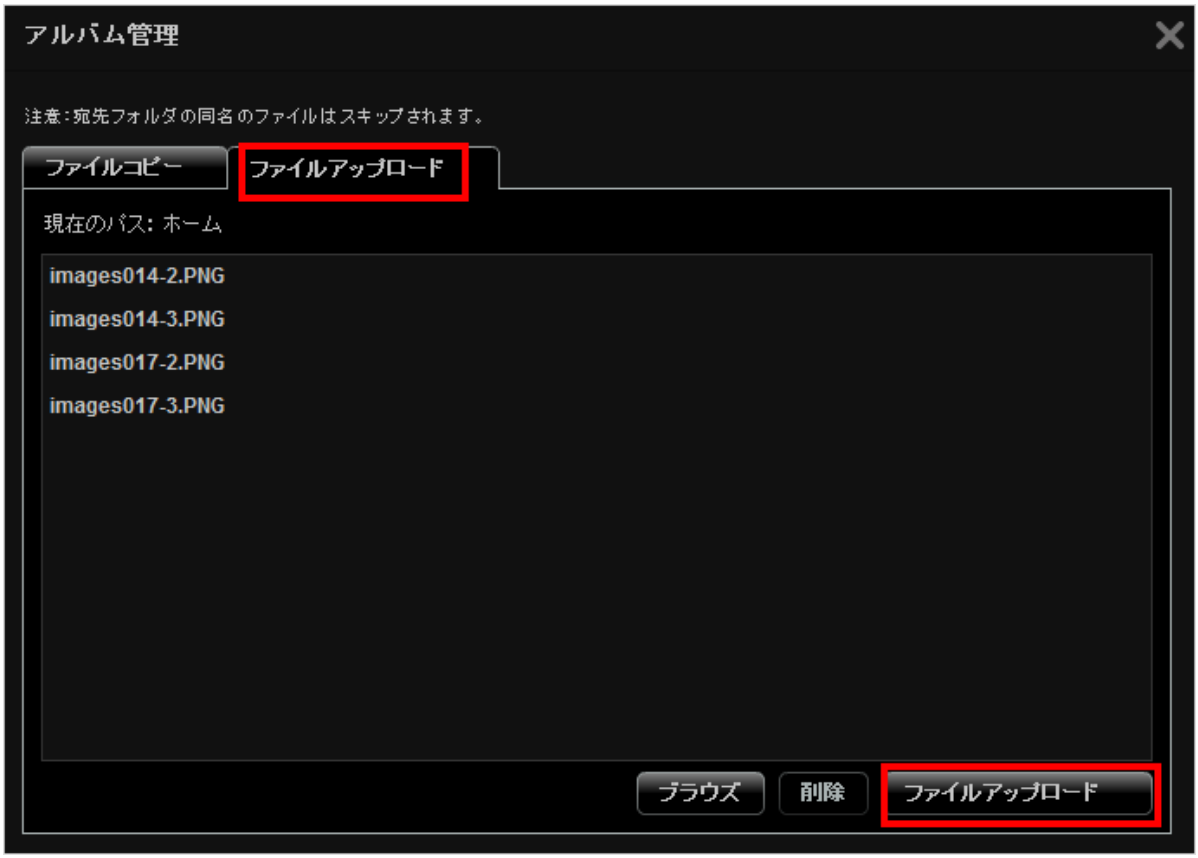
"Create New Album" (新アルバムの作成)を選択し、アルバム名を入力します。"Next" (次へをクリックします。

アルバム名は1-64文字以内で設定してください。また以下の記号は使用できません。 | \ : ? " < > *



Media Center内の他の場所からアルバムにファイルをコピーしたい場合は、"File Copy"（ファイルのコピー)を選択し、コピーするファイルを選んで＞をクリックします。続いて"File Copy"（ファイルのコピー）をクリックしてファイルのコピーを開始します。

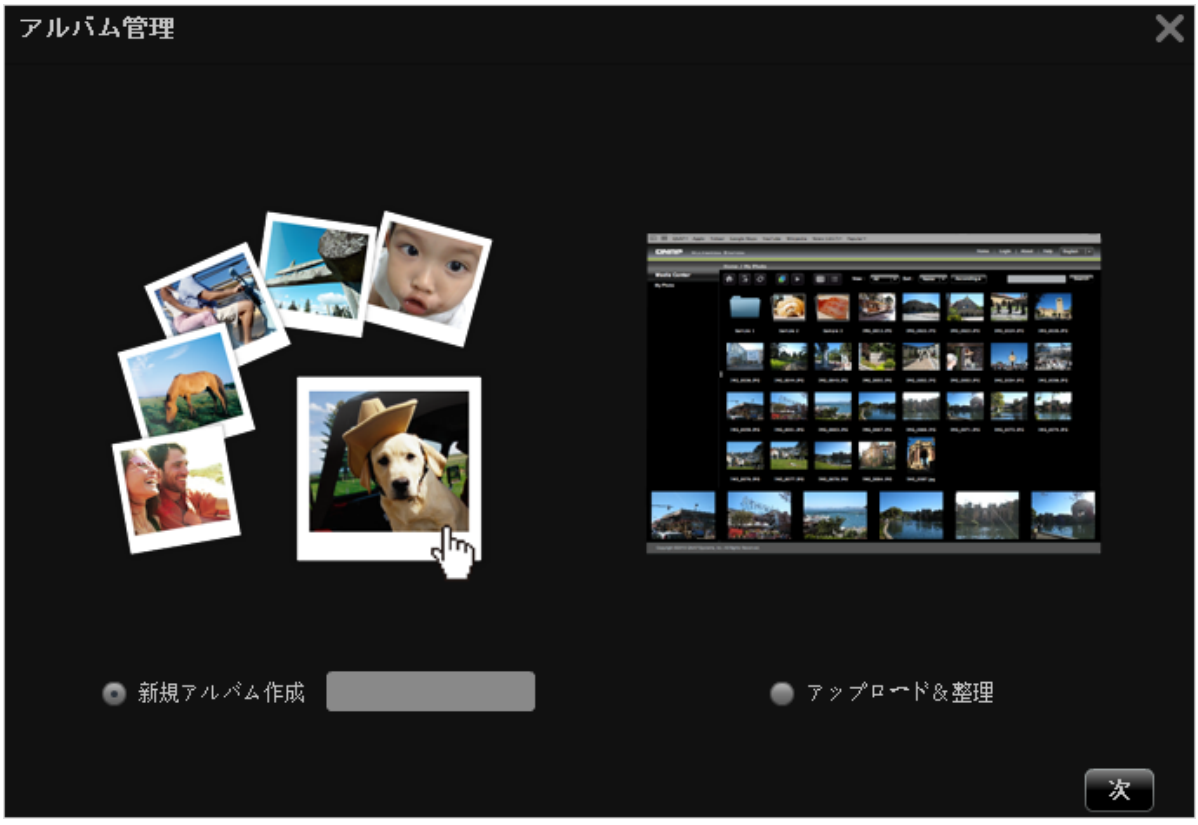
アルバムにファイルをアップロードするには、"Browse" (参照) をクリックしてファイルを選択し、"File Upload" (ファイルのアップロード) をクリックします。



アルバムの管理

Multimedia Station のウェブベースのインターフェイスを使用してアルバム（フォルダ）を管理するには、Media Center にてディレクトリを作成します。 （Create Album）（アルバム作成）をクリックします。

"Upload & Organize"（アップロード＆整理）を選択し、"Next"（次へ）をクリックします。



Media Center 内の他の場所からアルバムにファイルをコピーしたい場合は、"File Copy" (ファイルのコピー)を選択し、コピーするファイルを選んで＞をクリックします。続いて"File Copy" (ファイルのコピー)をクリックしてファイルのコピーを開始します。アルバムにファイルをアップロードするには、"Browse" (参照)をクリックしてファイルを選択し、"File Upload" (ファイルのアップロード)をクリックします。

をクリックしてマルチメディアコンテンツの詳細を表示し、アイコンをクリックしてファイルあるいはフォルダを開く、名前を更する、削除する、あるいはダウンロードすることができます。

アルバムカバーの設定

画像ファイルをアルバムカバーとして設定するには、 をクリックします。

画像ファイルを選択し、"Save"（保存）をクリックします。

スライドショー

をクリックし、複数の画像ファイルをスライドショーで表示します。再生速度(3秒/6秒/9秒/15秒)を選択し、またスライドショーの効果（全画面表示用）をドロップダウンメニューから選びます。画像ファイルの表示のためのフォトフレームも選択することができます。3次元表示(3D)で画像ファイルを表示するには、 をクリックします。

画像ファイルの公開

Multimedia Station上の画像ファイルを、FacebookやTwitterなどの人気のソーシャルネットワークサイトにて公開することができます。

をクリックします。

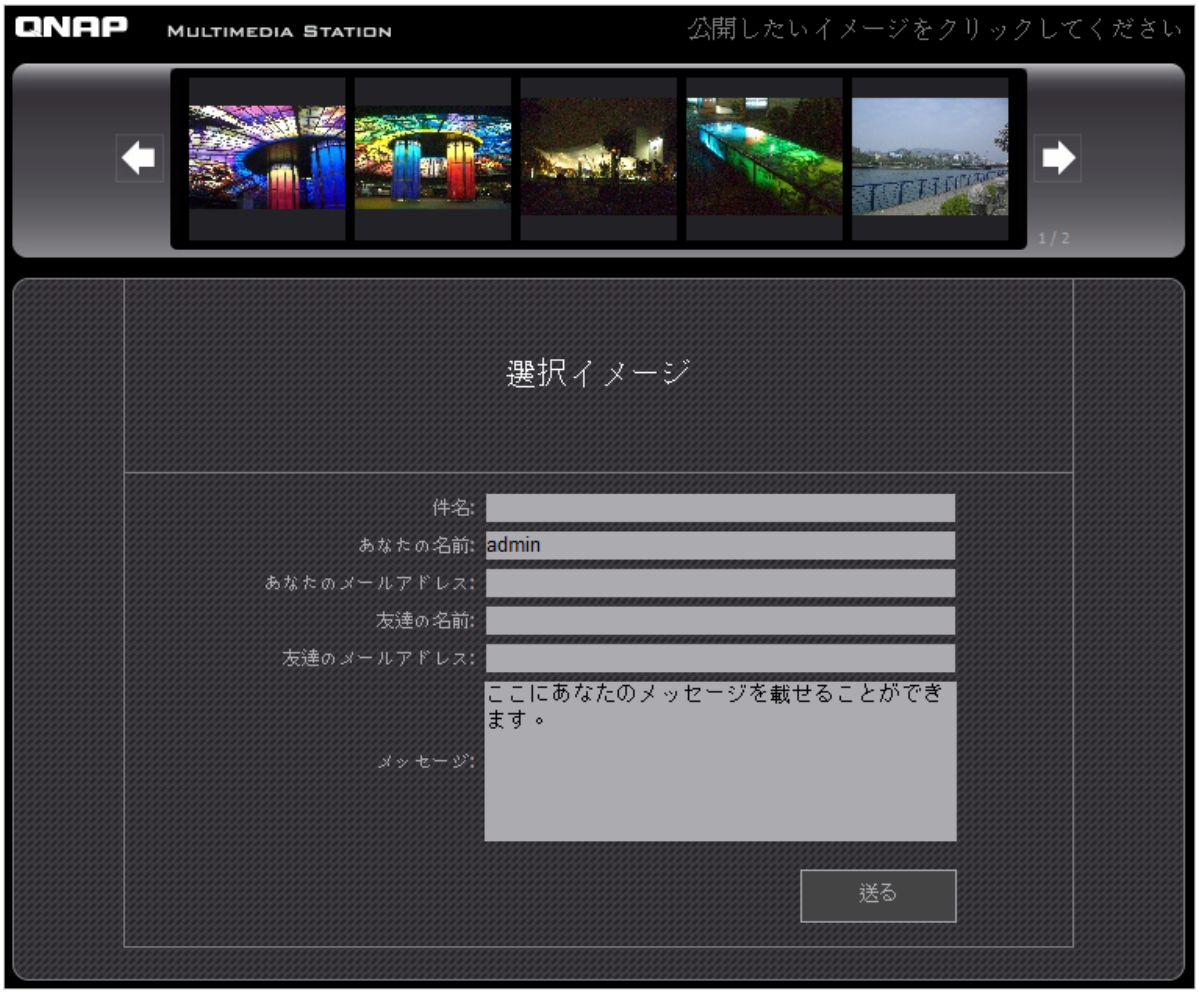
公開する画像ファイルを選択します。1度につき5枚まで公開できます。タイトルおよび説明を入力します。続いてファイルを公開するウェブサイトを選択し、ウェブサイトのログイン情報を入力します。公開の前に、アルバムをパブリック (コントロールパネル > Set Folder Public (フォルダをパブリック(公開)に設定)に設定し、またインターネットからMultimedia Stationにアクセスできる必要があります。この機能を使用する前に、NAS向けにDDNSをセットアップすることが推奨されます。

記入欄	制限
タイトル	最大文字数: 256
リンク(NASのIPアドレスあるいはホスト名)	アルファベット、数字、ドット(.)、スラッシュ(/)のみ。 最大文字数: 256
説明	最大文字数: 1024

画像ファイルの電子メール送信

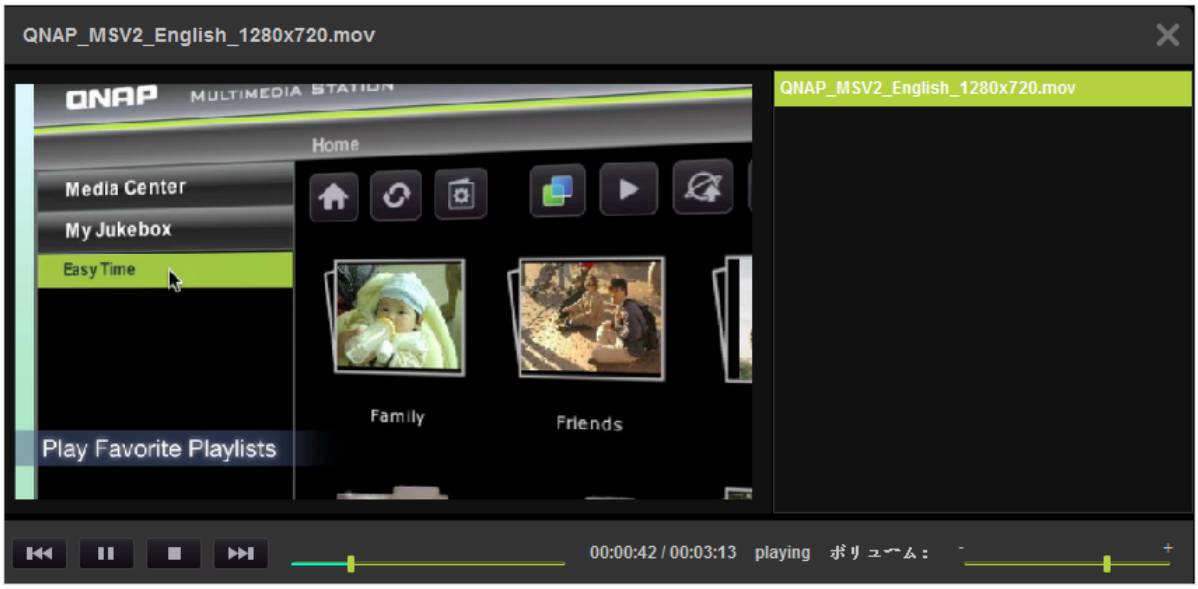
画像ファイルを電子メールで送信するには、NASのSMTPサーバ設定が適切に構成されているよう確認してください。 をクリックします。
情報を入力して、"Send" (送信)をクリックします。

記入欄	制限
題名	最大文字数: 128
私の名前	名前にはアルファベット(A-Zおよびa-z)、数字 (0-9、ハイフン(-)、およびアンダースコア(_)のみ使用できます。
私の電子メール	最大文字数: 128
友人の名前	最大文字数: 128
友人の電子メール	最大文字数: 128
メッセージ	最大文字数: 1024



ビデオの再生

NASはウェブブラウザ上のビデオファイルの再生をサポートしています。ウェブページ上でビデオファイルをクリックするだけで、NASが再生します。フォルダ内のビデオファイルをクリックした場合は、フォルダ内にある他のビデオファイルも、サポートされる場合に限り、再生リストに表示され、再生されます。'X'をクリックし、再生ページを終了します。



トランスコードビデオ

ビデオファイルがAVI、M4V、MPG/MPEG、RM/RMVB、WMV形式の場合、Multimedia Stationで正しく再生するためにファイルをトランスコードする必要があります。トランスコードが可能なビデオファイルには、サムネイル表示の際に下のようなアイコンが表示されています。

アイコンをクリックし、ビデオトランスコードの実行を確定します。トランスコードが進行中の間、お待ちください。

ビデオはFLV形式に換されます。これでウェブブラウザ上で再生することができます。ビデオのトランスコードは管理者のみ実行することができます。

QNAPは全てのビデオ形式またはコーデックがサポートされていることを保証するものではありません。ビデオファイルをNASにアップロードする前に、ファイルをMultimedia Stationがサポートする形式に換するよう強く推奨いたします。

My Jukebox（マイ・ジュークボックス）

音楽ファイルの再生リストを作成し、My Jukebox（マイ・ジュークボックス）で再生することができます。アルバムアートおよび情報は、該当する場合、ID3タグから自動的に読込まれます。

My Jukeboxにて自分の再生リストを作成したり編集するには、"Control Panel"（コントロールパネル）> "Playlist Editor"（再生リストエディタ）を開いてください。管理者のみが再生リストを編集することができます。My Jukebox内の再生リストは、Multimedia Stationのユーザー全てと共されます。

Control Panel (コントロールパネル)

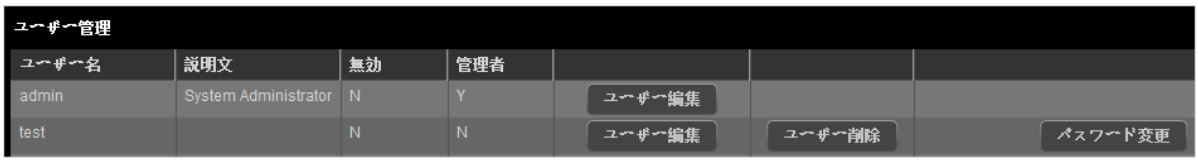
User Management (ユーザー管理)

Multimedia Station にて複数のユーザーアカウントを作成することができます。ここで作成されるユーザーアカウントはNAS上で作成する "Access Right Management" (アクセス権限管理) > "Users" (ユーザー)システムユーザーアカウントとは異なりますので注意してください。"Add User" (ユーザーの追加)をクリックしてユーザーを作成します。Multimedia Station がサポートするユーザーの最大数は、"admin" (管理者)を含め128です。

ユーザー情報を入力します。ユーザー名はアルファベット(A-Zおよびa-z)、数字(0-9、ハイフン(-)、およびアンダースコア(_)のみ使用できます。 ユーザー名は32文字まで可能です。

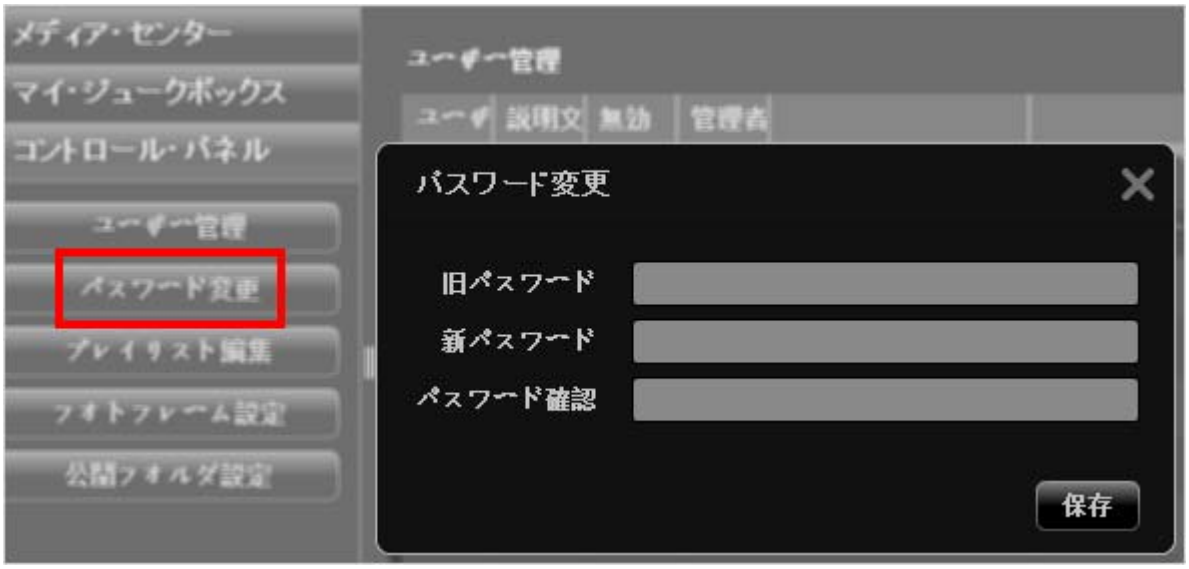
ユーザーが管理者かどうかを特定し、ユーザーがアクセスできるフォルダを指定します。"Save" (保存)をクリックします。パスワードには1-16文字まで使うことができます。パスワードに効な文字はA-Z, a-z, 0-9, -, !, @, #, $, %, _です。

リストの中に、そのユーザーが表示されます。ユーザー情報の編集、ユーザーの削除、またログインパスワードの更が可能です。デフォルトアカウントである "admin" は削除できません。ご注意ください。



Change Password (パスワードの更)

管理者のパスワードをこのセクションで更することができます。パスワードには1-16文字まで使うことができます。パスワードに効な文字は A-Z, a-z, 0-9, -, !, @, #, $, %, _です。



Playlist Editor（再生リストエディタ）

再生リストを作成するには、Playlist Editor（再生リストエディタ）を開きます。既存の再生リストをドロップダウンメニューから選択するか。"Add"（追加)をクリックして再生リストを作成します。
次に、左の行（Multimedia Station上のファイル）から音楽ファイルを選択し、> をクリックしてファイルを再生リストに追加します。
"Save"（保存)、続いて "Close"（閉じる）をクリックします。

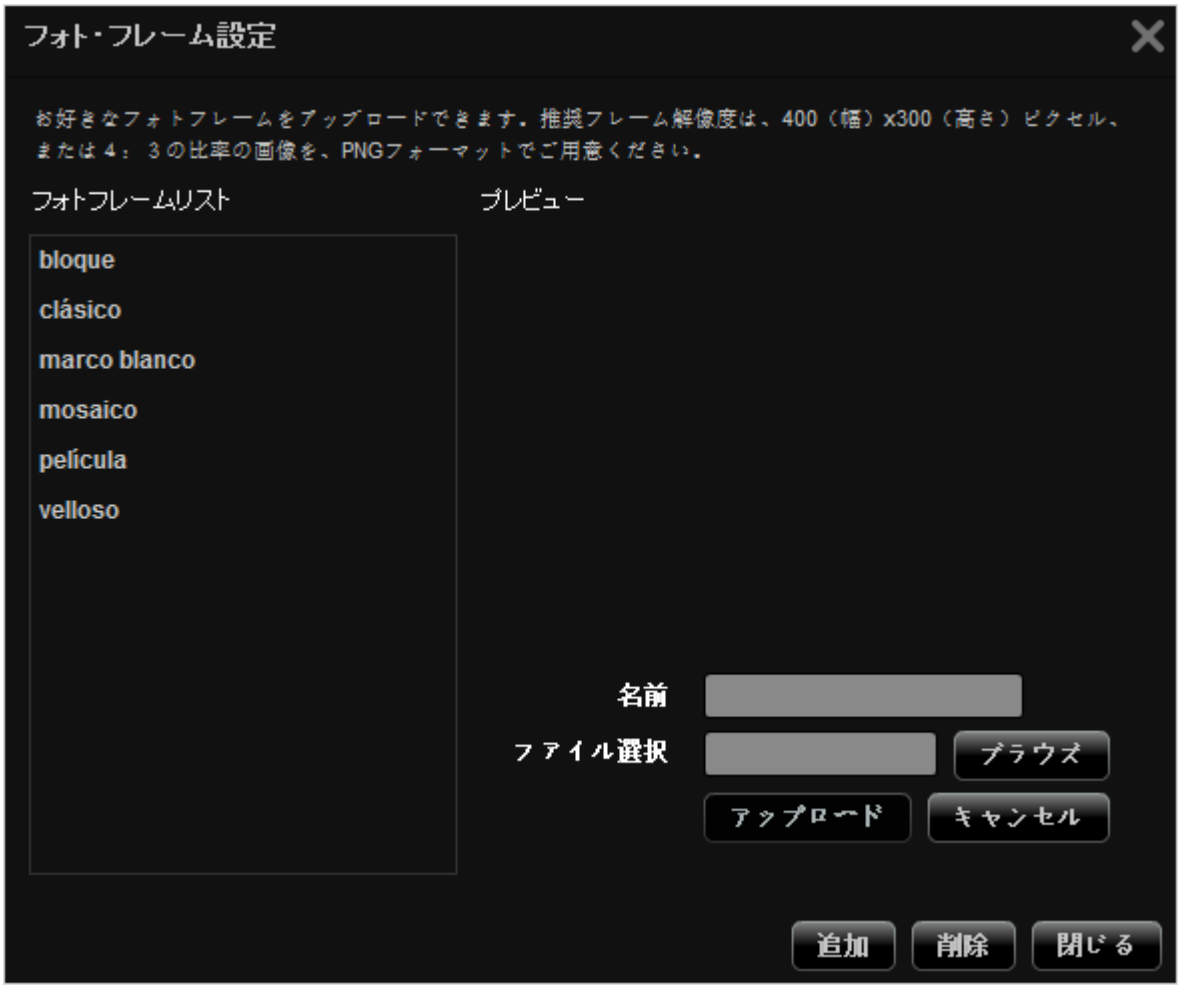
再生リストの作成後、このリストをMy Jukeboxで再生することができます。

再生リスト内の最大文字数	24
再生リスト内の最大曲数	512
再生リストの最大保管数	128

Photo Frame Settings (フォトフレーム設定)

フォトフレームをアップロードして画像表示に使用することができます。推奨解像度は400(幅x300(高ピクセルか、画像を4:3アスペクト比で使用します。サポートする形式はPNGです。フォトフレームを追加するには、"Add" (追加) をクリックしてファイルをアップロードします。

フォトフレーム名には1–16文字まで使うことができます。Multimedia Stationがサポートするフォトフレームの最大数は、システムデフォルトのフォトフレームを含め64です。デフォルトのフォトフレームは削除できません。ご注意ください。



Set Folder Public（フォルダをパブリックに設定）

画像ファイルをウェブに公開するには、フォルダをパブリックにする必要があります。パブリックアクセスを許可するフォルダを選択し、>をクリックします。続いて"Save"（保存)をクリックします。パブリックフォルダには、Multimedia Stationにログインすることなく全ての人がアクセスすることができますのでご注意ください。

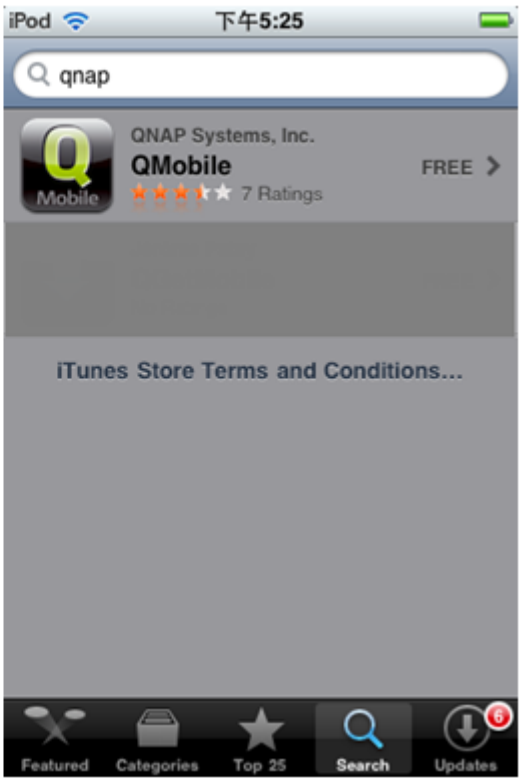
7.2.1 QMobile

QMobile は、iPhone、iPod touch、iPad、および、Android 電話などのハンドヘルドデバイスを使って、音楽、デジタル写真、および、ビデオを、QNAP NAS サーバーからストリームして、どこにいても、ファイルをデバイス上で直接再生できるアプリケーションです。インターネットアクセスがあれば、NAS 上のすべてのコンテンツにリモートアクセスできます。

注: QMobile は、ファームウェアバージョン 3.3.0 またはそれ以降を実行する QNAP Turbo NAS に適用できます。マルチメディアステーションと Web サーバーが有効になっていること、および、QMobile が QNAP NAS 上のマルチメディアファイルにアクセスできるように共有コンテンツが構成されていることを確認します。（NAS 上とマルチメディアステーション上に作成したユーザーアカウントは相互依存性はありません。認証されたユーザーアカウントを使って、マルチメディアステーションにアクセスしてください。）

QMobile のステップバイステップインストールガイド:

App Store（iPhone）または Android Market（Android 電話）から QMobile をダウンロードします。

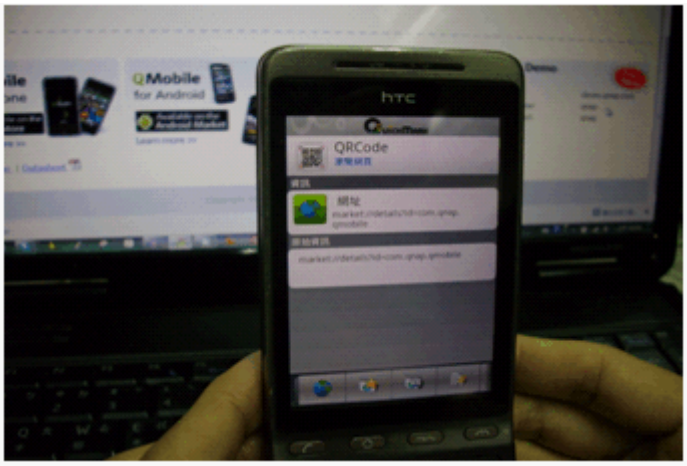


Android電話ユーザーは、以下のWebサイトからQRコードの写真を撮ることでQmobileのダウンロードリンクを取得することもできます。

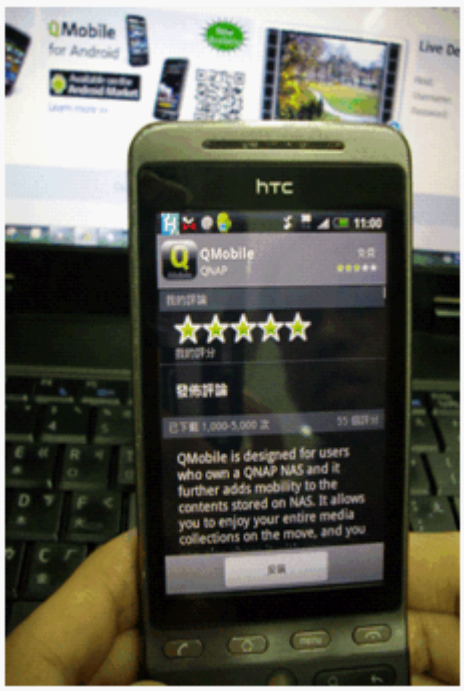
1. http://www.qnap.com/QMobile/Default.aspx?lang=eng
2. http://www.doubletwist.com/apps/android/qmobile/-6558955796410604679/

QRコードの写真を撮ります。

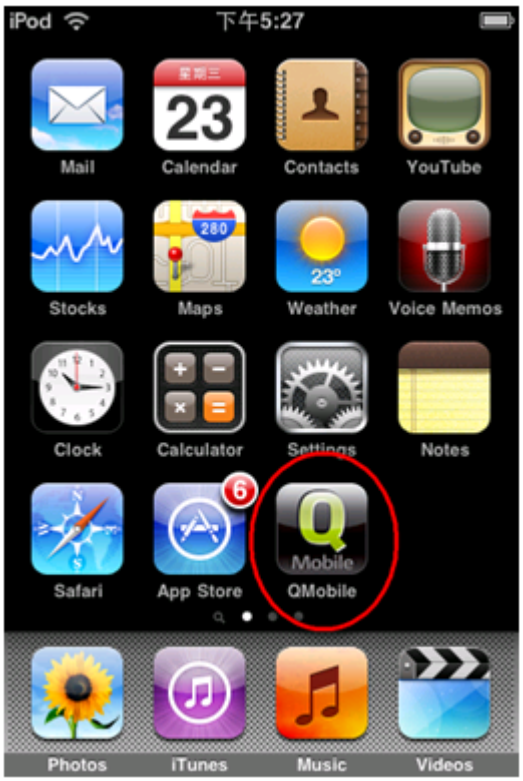
QRコードからダウンロードを自動的に取得します。



QMobileをAndroid電話にダウンロードします。



インストールが完了すると、QMobile が画面上に表示されます。



ハンドヘルドデバイス上で NAS 設定を構成します

QMobile アプリケーションを起動して QNAP NAS を追加します。「Automatic Discovery（オートディスカバリ）」または「Add Server Manually（サーバーを手動で追加）」で NAS を QMobile に追加できます。

Automatic Discovery（オートディスカバリ）

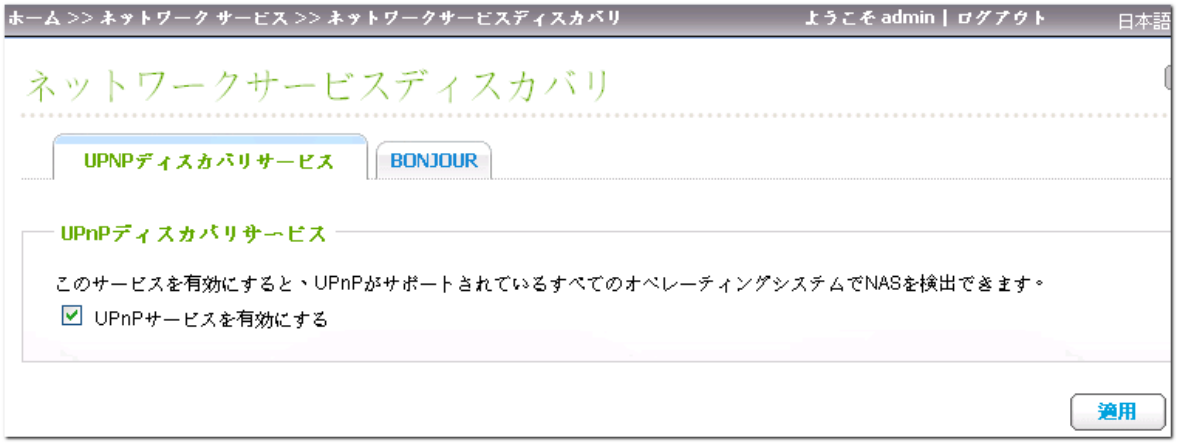
注:

1. iPhone の場合

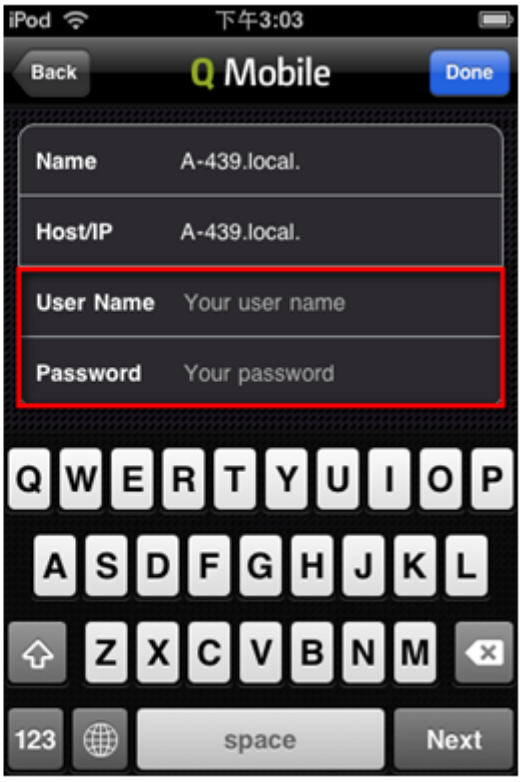
この機能を使用できるのは、「Network Services（ネットワークサービス）」>「Network Service Discovery（ネットワークサービスディスカバリ）」>「Bonjour」で「QMobile for iPhone/iPod Touch（iPhone/iPod touch 用の QMobile）」を有効にした場合だけです。

2. Android デバイスの場合

この機能を使用できるのは、「Network Services（ネットワークサービス）」>「Network Service Discovery（ネットワークサービスディスカバリ）」>"UPnP Discovery Service（UPnP ディスカバリサービス）"で NAS 上の「Enable UPnP Service（UPnP サービスを有効にする）」を有効にした場合だけです。

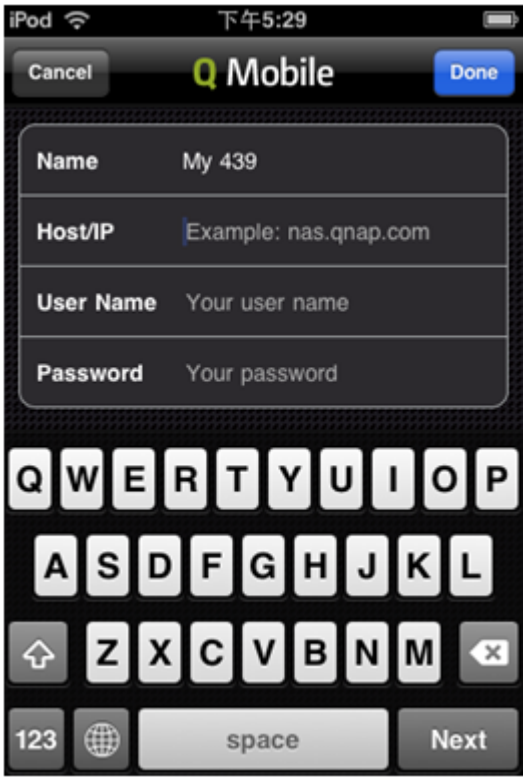


QMobile がローカルネットワーク上で Bonjour/UPnP を有効にした NAS サーバーをすべて検索します。NAS を選択し、ユーザー名とパスワードを使ってログインします。

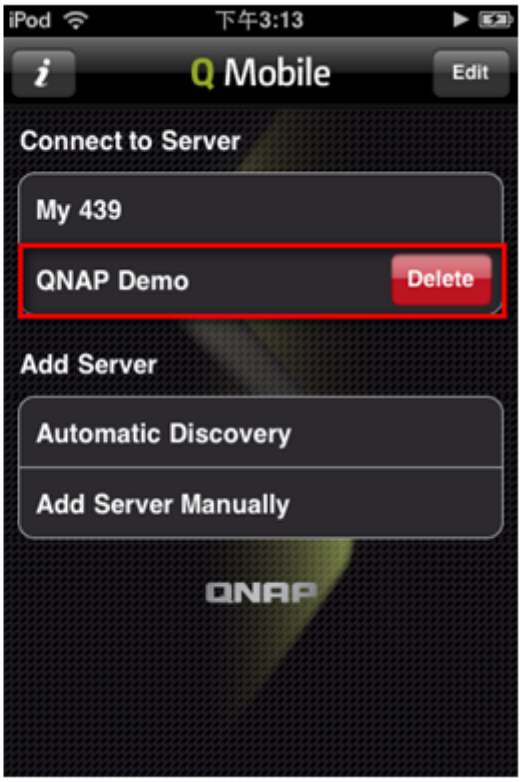


Add Server Manually (サーバーを手動で追加)

NAS の名前、ホスト/IP、ユーザー名、および、パスワードを入力します。



接続したい NAS を選択します。QMobileからNASを削除するには、NAS名をスワイプし[Delete(削除)]をタップします。



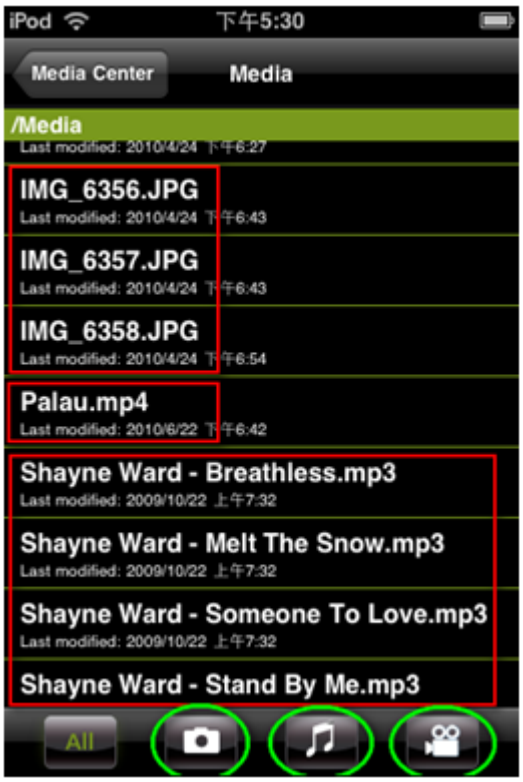
QMobile を使って NAS 上のメディアセンターを管理する

1. Media Center (メディアセンター)

NAS のマルチメディアステーション上に保存したマルチメディアファイルを表示したり、再生できます。
注: QMobile が再生できるのはハンドヘルドデバイスがサポートするファイル形式だけです。

NAS に接続して、Media Center(メディアセンター)アイコンをタップします。

「Qmultimedia/Multimedia」デフォルト共有フォルダで、マルチメディアファイルを検索できます。または、一番下にある対応するアイコンをタップして、特定の写真、音楽、または、ビデオファイルを選択できます。

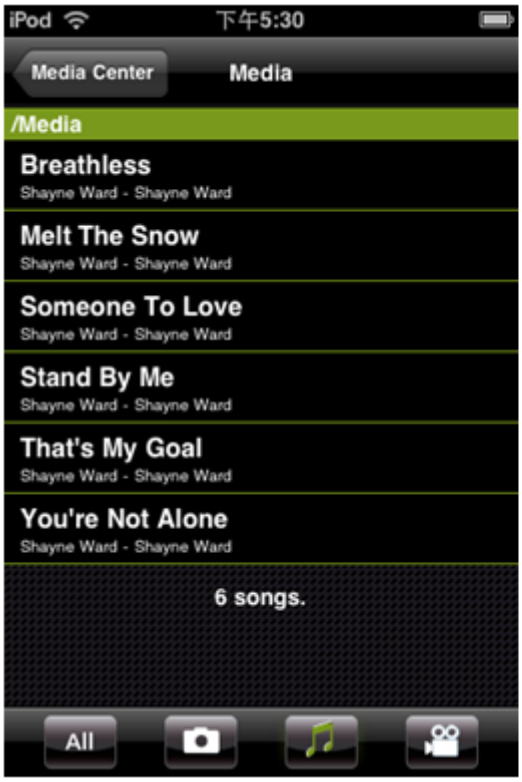


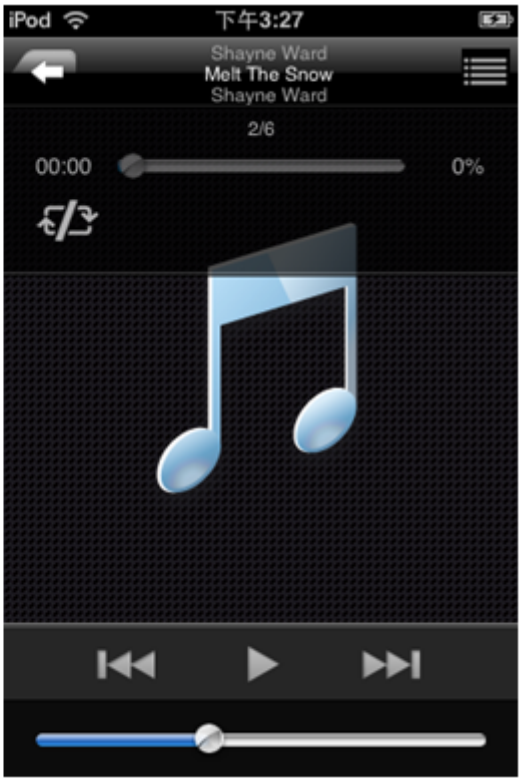
フォトビュー

iPod
下午5:30
Media Center
Media
/Media
All

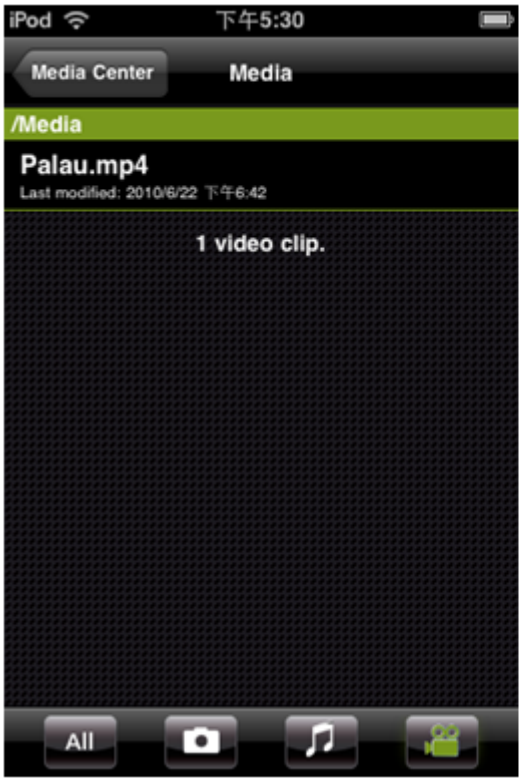
iPod
下午3:24
Media
3 of 12
See All
IMG_0027.jpg

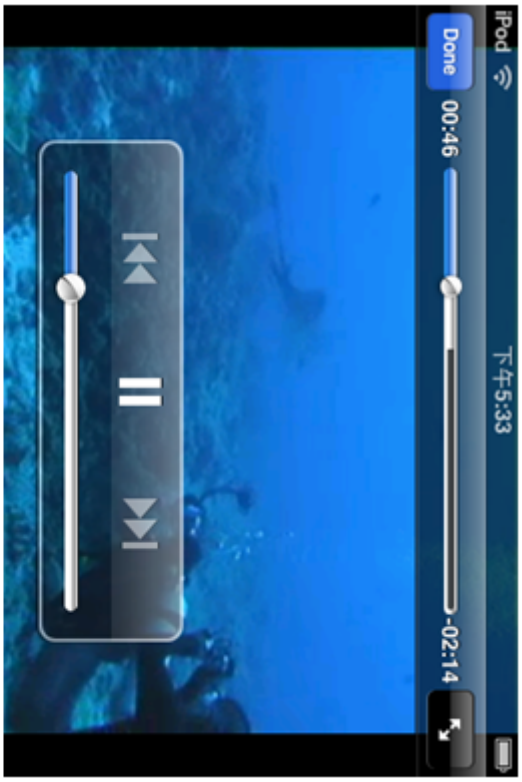
ミュージックビュー


iPod
下午5:30
Media Center
Media
/Media
Breathless
Shayne Ward - Shayne Ward
Melt The Snow
Shayne Ward - Shayne Ward
Someone To Love
Shayne Ward - Shayne Ward
Stand By Me
Shayne Ward - Shayne Ward
That's My Goal
Shayne Ward - Shayne Ward
You're Not Alone
Shayne Ward - Shayne Ward
6 songs.
All


iPod
下午3:27
Shayne Ward
Melt The Snow
Shayne Ward
2/6
00:00
0%

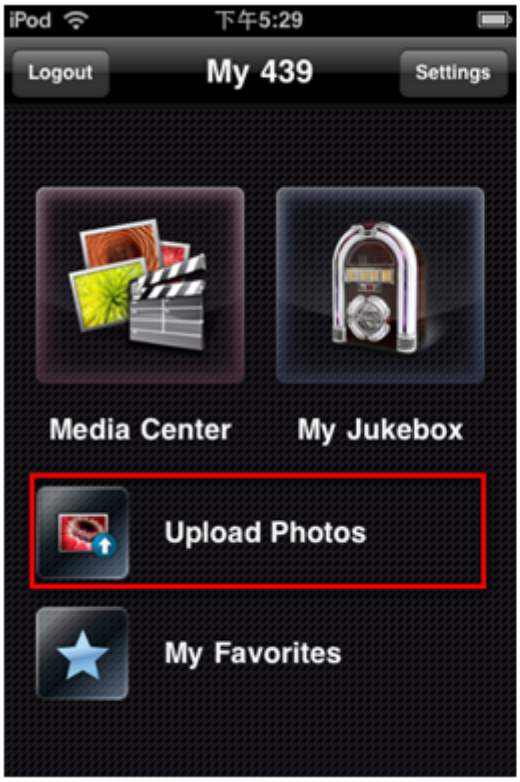
ビデオビュー


iPod
下午5:30
Media Center
Media
/Media
Palau.mp4
Last modified: 2010/6/22 下午6:42
1 video clip.
All

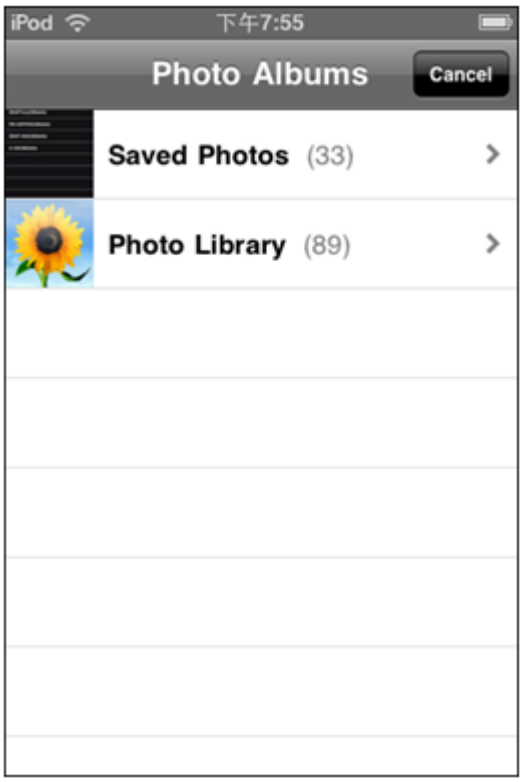

Done
00:46
-02:14
iPod
下午5:33

2. 写真を NAS にアップロードする

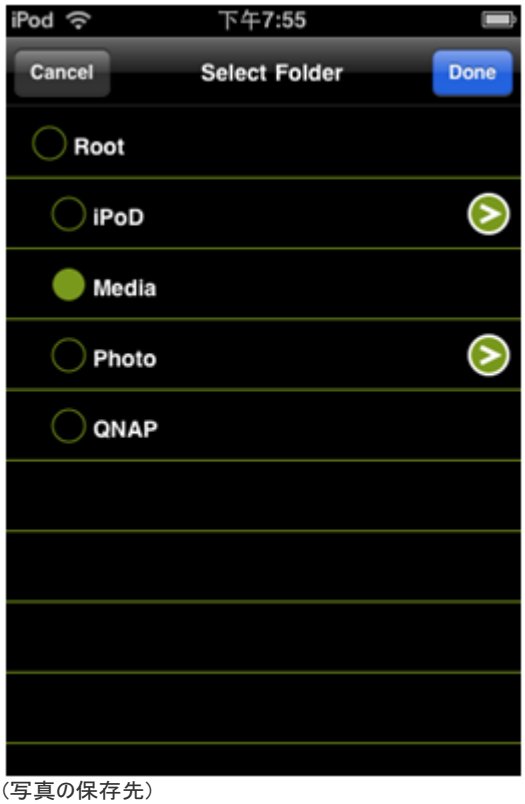
QMobile 経由でハンドヘルドデバイス上の写真ファイルを NAS に直接アップロードできます。 をタップして、ファイルソースを選択します。 をタップして、NAS のファイルのアップロード先を選択します。



写真のソース: ハンドヘルドデバイスから写真を選択します。
写真の保存先: 写真の保存先となるルートフォルダ（NAS の「Qmultimedia/Multimedia」フォルダ）、または、サブフォルダを選択します。

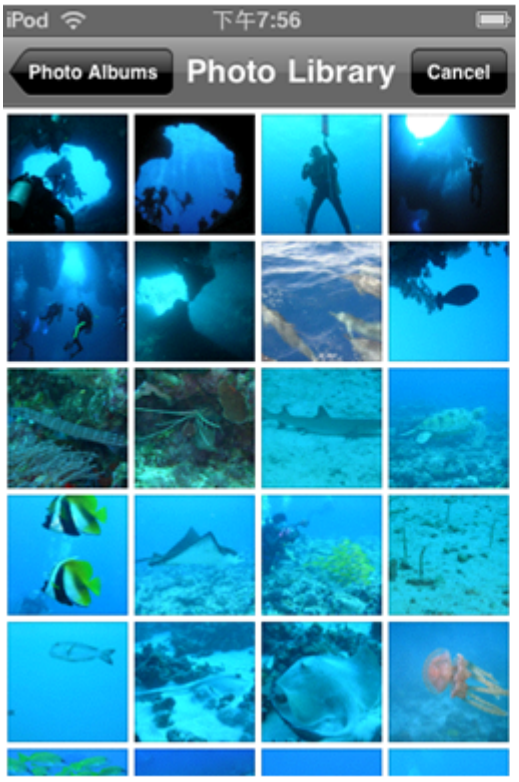


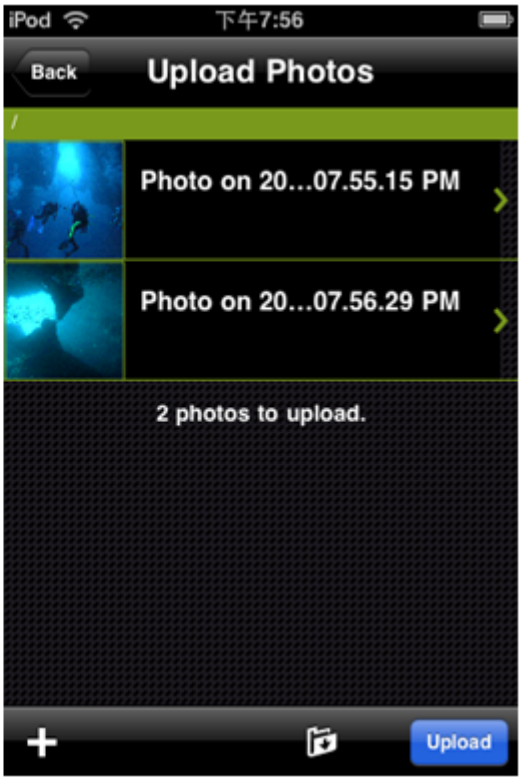
（写真のソース）



（写真の保存先）

写真を選択し、「Upload（アップロード）」アイコンをタップして、写真を NAS にアップロードします。

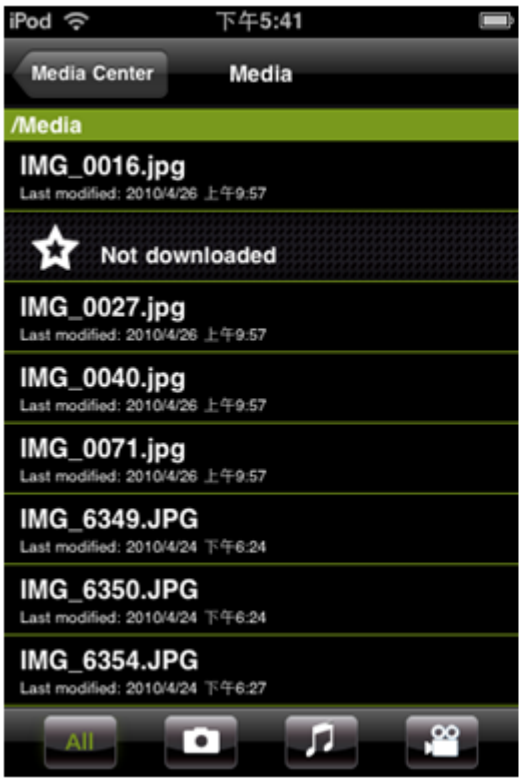


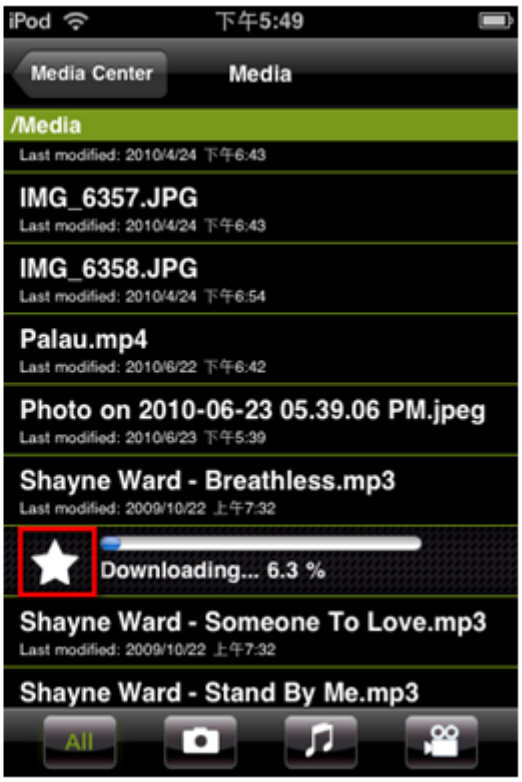


3. My Favorites (お気に入り)

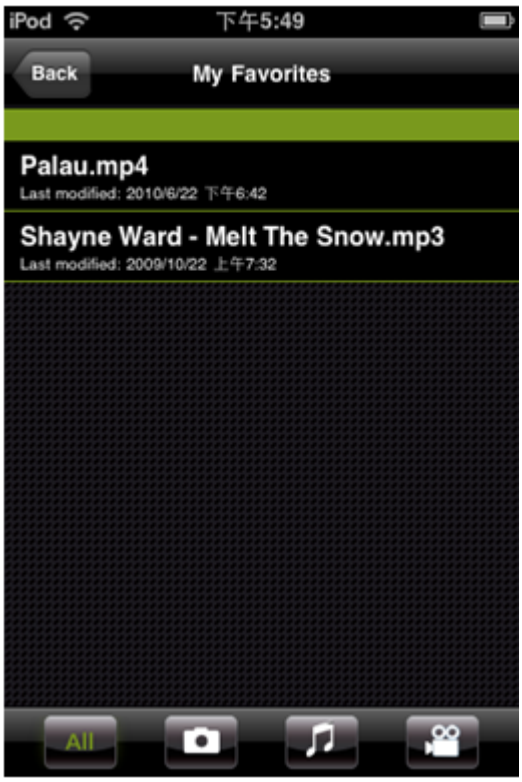
「My Favorites（お気に入り）」で、マルチメディアファイルを NAS からハンドヘルドデバイスにダウンロードして、オフラインで再生できます。

Media Center（メディアセンター）でファイルをスワイプし、星印をタップしてダウンロードを開始します。
（ダウンロードされていないファイルは「Not downloaded（ダウンロードされていません）」と表示されます。）





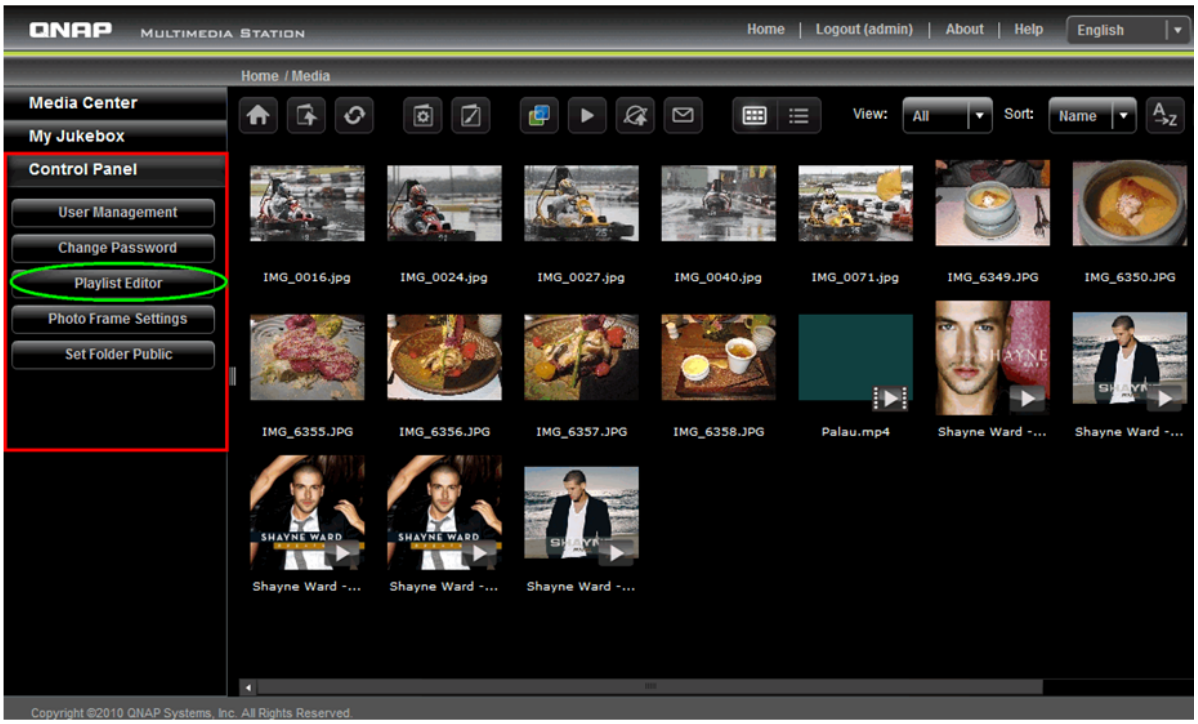
ダウンロードしたファイルが「My Favorites（お気に入り）」に表示されます。NAS に接続する度に、QMobile が、ダウンロードしたファイルのソースが更新されたかどうか、または、NAS から削除されたかどうかを確認します。NAS を使って変更を同期化するように選択できます。



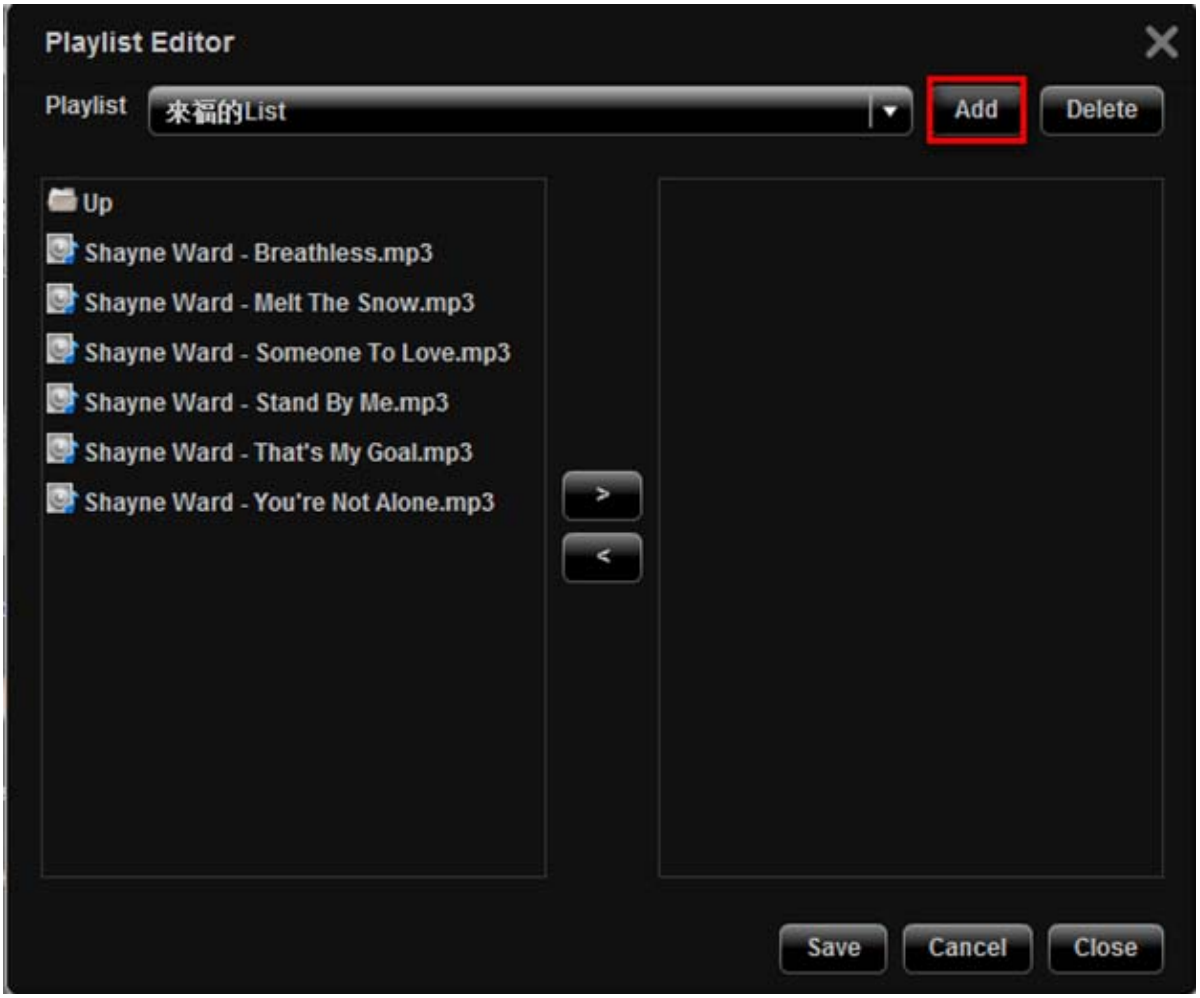
4. My Jukebox (マイ ジュークボックス)

メディアステーション上で構成したプレイリストを表示、ストリーム、再生できます。

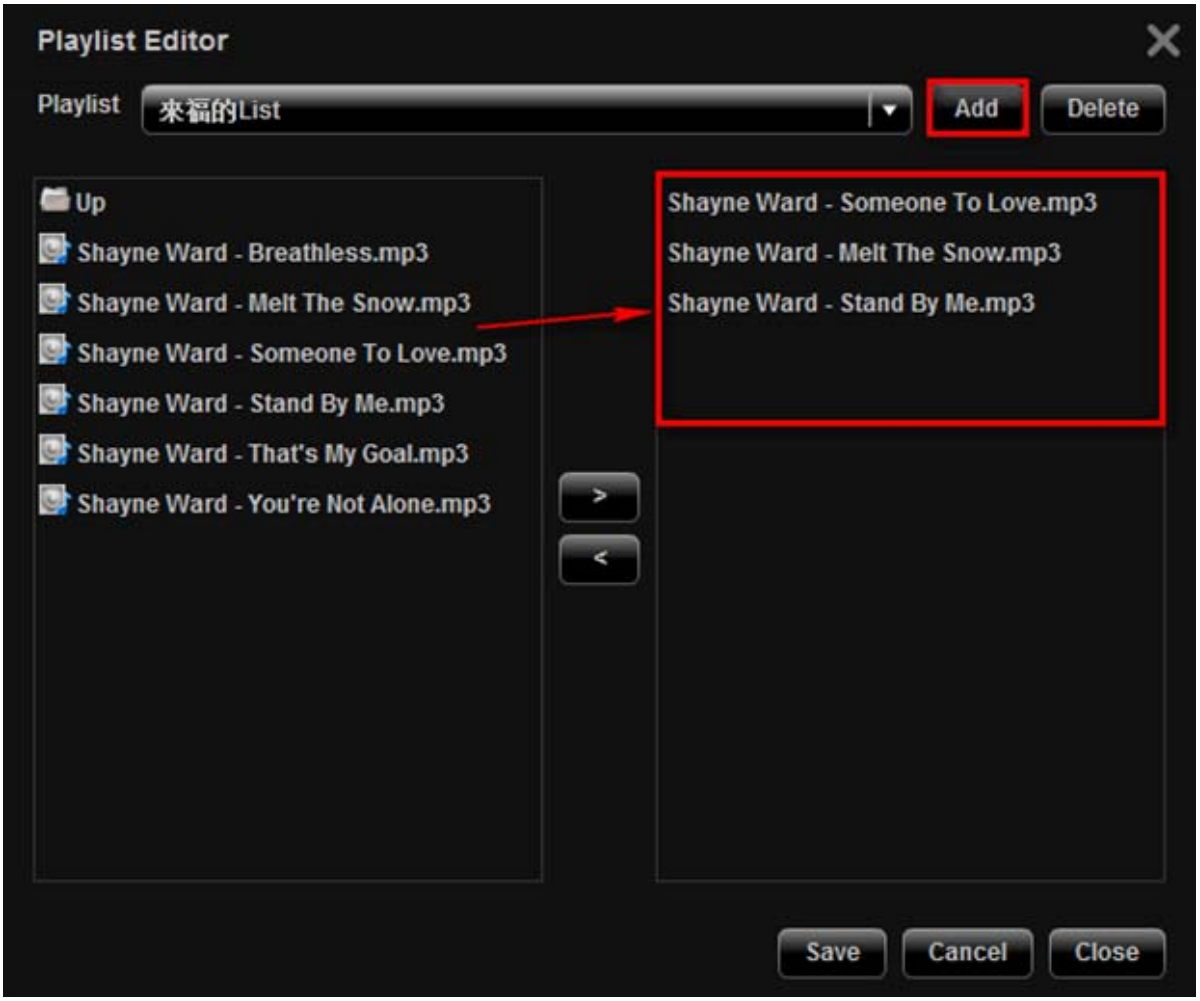
メディアステーションに管理者としてログインします。「Control Panel（コントロール パネル）」>「Playlist Editor（プレイリストエディタ）」の順に選択します。



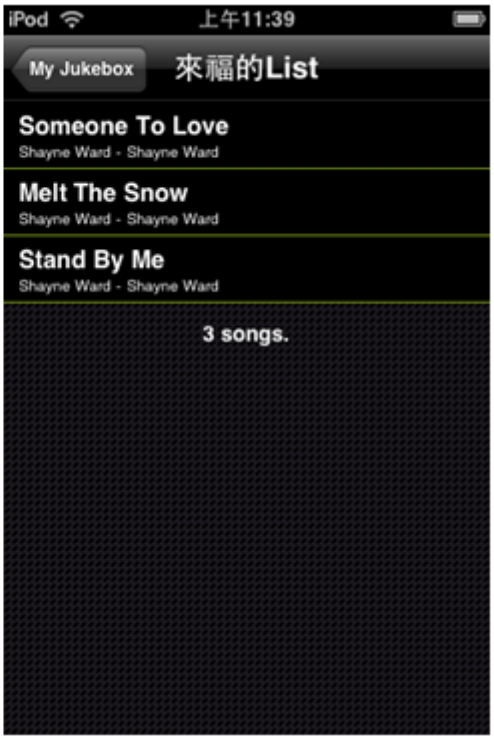
[Add（追加）] をクリックして、プレイリストを作成します。プレイリスト名を入力して、[Save（保存）] をクリックします。



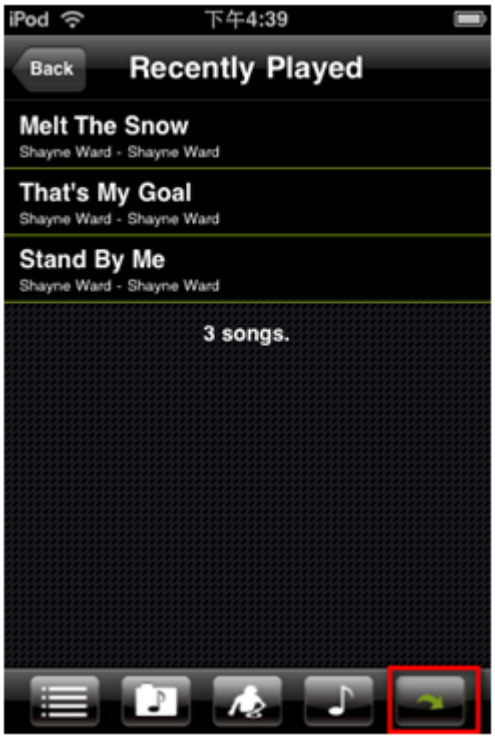
ドロップダウンメニューからプレイリストを選択し、次に、プレイリストに追加する音楽ファイルを選択して、[>] をクリックします。[Save（保存）] をクリックして、プレイリストを保存します。



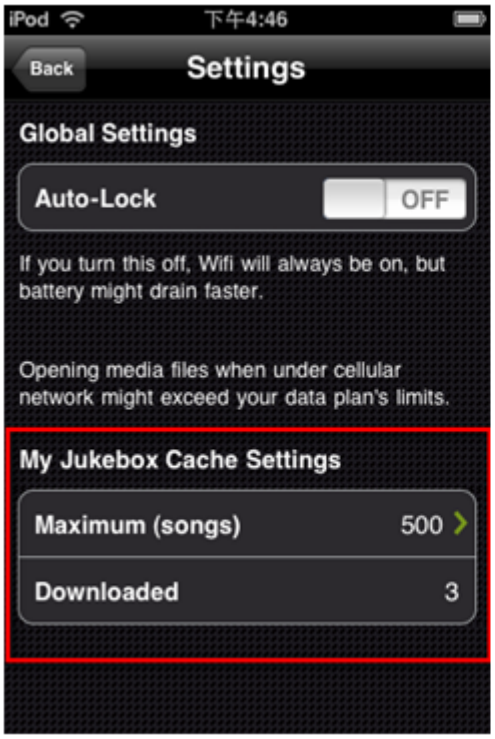
ハンドヘルドデバイス上の「My Jukebox（マイ ジュークボックス）」で、NAS 上に作成したプレイリストを再生できます。

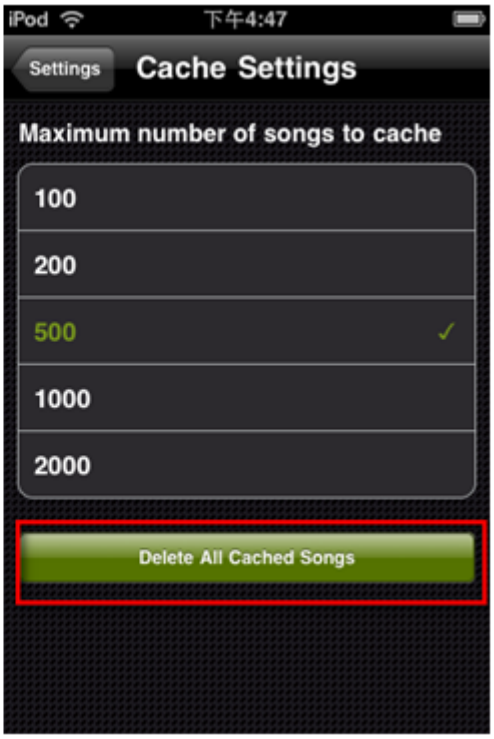


オーディオファイルのストリームが完了すると、「Recently Played（最近再生したファイル）」内のキャッシュに保存されます。



「Settings（設定）」でキャッシュ設定を編集できます。





7.3 Photo Station

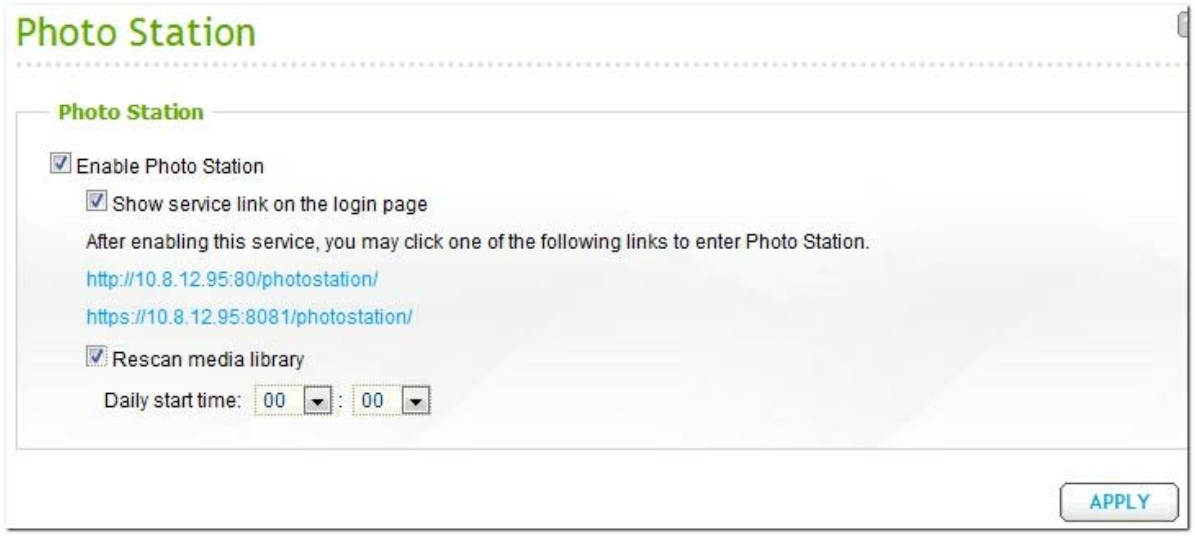
Photo Station とは、インターネット上で写真およびビデオを整理し共有するウェブアルバムです。

要件:

- NAS の Web サーバーおよびマルチメディアステーションを有効にします。Photo Station は、マルチメディアステーションのメディアライブラリを使用します。Photo Station を有効にすると、マルチメディアステーションが自動的に有効化されます（無効な場合）。
- Adobe Flash Player 9 またはそれ以降が必要です。

Photo Station を使用するには、以下を行います。

1. NAS に「admin」としてログインします。「Application Servers（アプリケーションサーバー）」 > 「Photo Station」に移動し、この機能を有効にします。「Rescan media library（メディアライブラリの再スキャン）」オプションを有効にし、NAS が毎日メディアライブラリをスキャンする時刻を指定します。NAS は、毎日指定した時刻に新しく追加されたファイルに対してサムネイルを生成し、メディア情報を取得して、ビデオをトランスコードします。



2. 写真およびビデオファイルを NAS の Qmultimedia または Multimedia フォルダにアップロードします。

Photo Station は、次のファイルフォーマットをサポートします：

画像	BMP（Intel ベース NAS のみ）、GIF、PNG、JPG および JPEG
ビデオ	FLV および H.264（AAC）

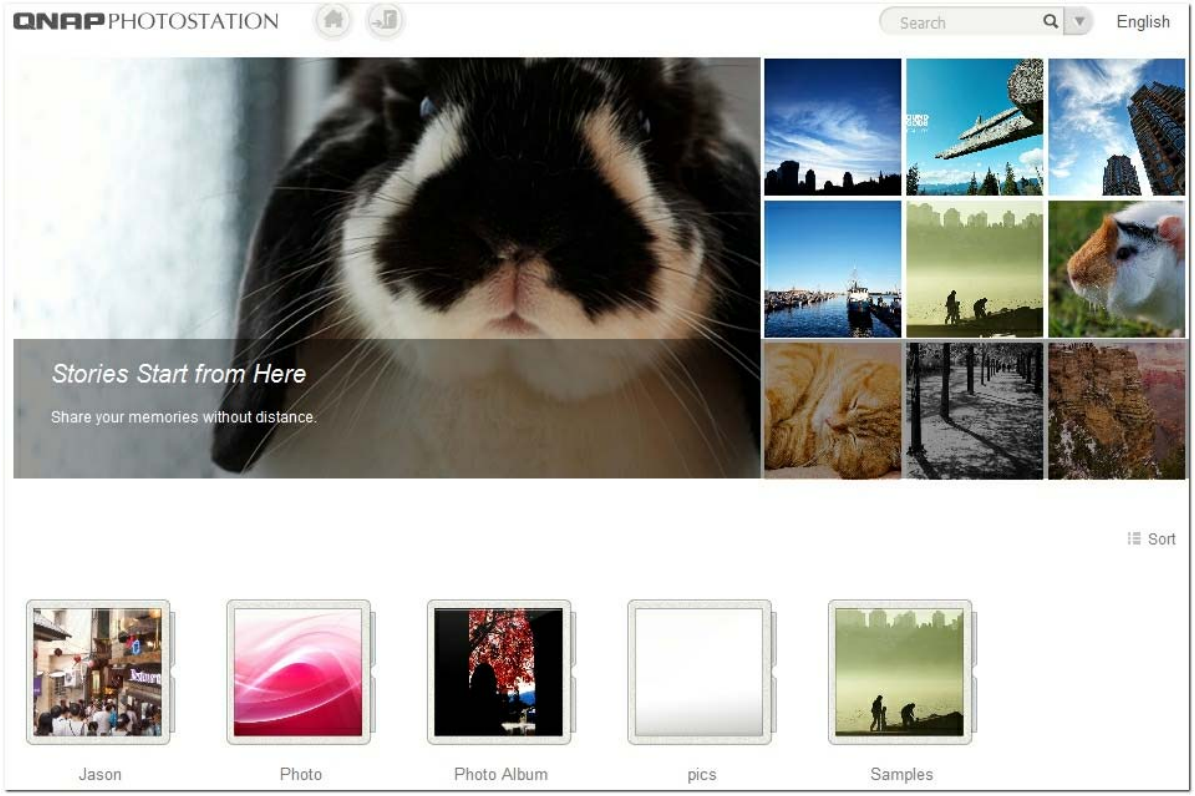
ファイルアップロードのヒント：

- 画像ファイルの最大サイズは 32MByte です。
- 同時にアップロードできるファイルの最大サイズは 2GByte です。

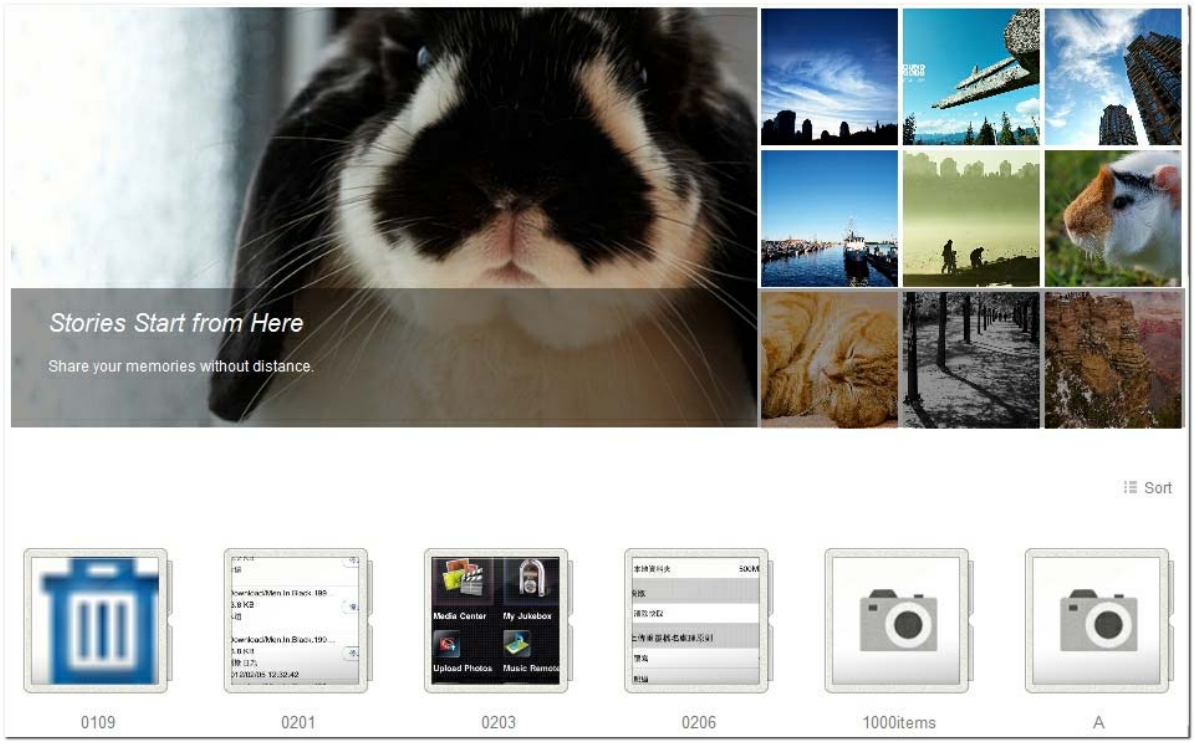
3. Photo Station のログインページに移動します。これを行うには、NAS のログインページ上の Photo Station アイコンをクリックするか、「Application Servers（アプリケーションサーバー）」>「Photo Station」上のリンクをクリックするか、または、ウェブブラウザ（Internet Explorer、Mozilla Firefox または Google Chrome）で http://NAS IP/photostation を入力します。

4. ログインページの上部に Photo Station のバナーと説明が表示されます。以下が、公開アルバムのバナーです。右上のドロップダウンメニューから表示言語を選択します。

5. をクリックし、ユーザー名とパスワードを入力して、Photo Station にログインします。管理者のログイン資格情報は、NAS の ウェブ管理者と同じです。



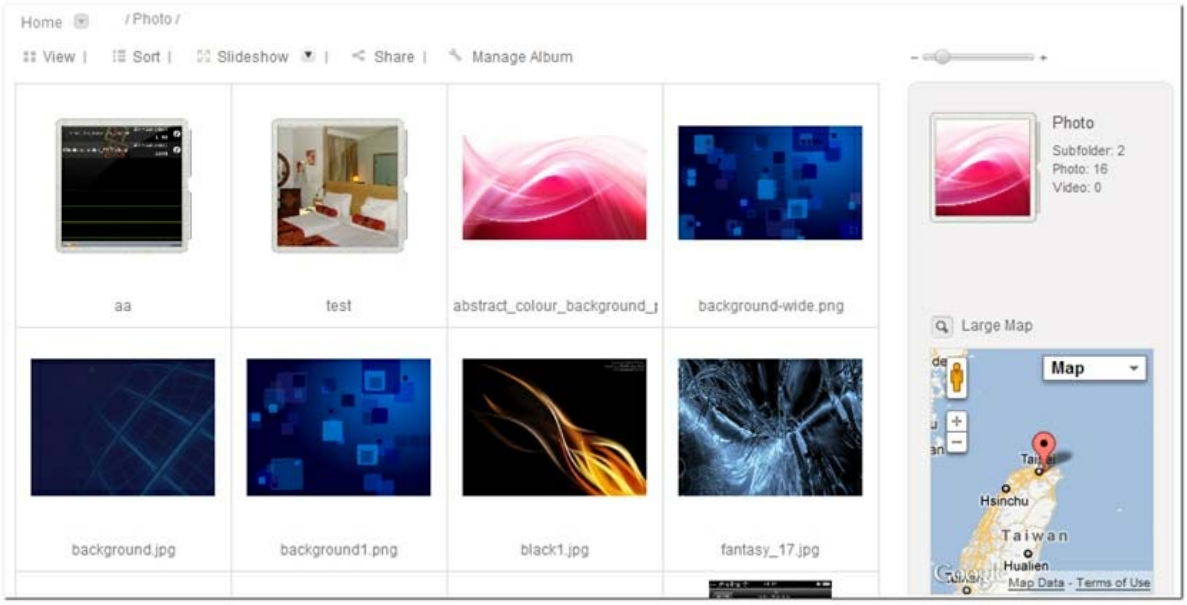
ログインに成功すると、Photo Station 内の全フォルダ（アルバム）が表示されます。



アイコン	説明
	Photo Station のホームページに移動します。Qmultimedia/Multimedia 上のフォルダのみが表示されます。
	ログアウトします。
	「Settings（設定）」ページに移動します。
	現在ディレクトリの下のフォルダ、写真またはビデオを検索します。高度な検索を行うには、三角アイコンをクリックします。
	コンテンツをファイル名、サイズ、ファイル作成日、写真撮影日、アルファベットの昇順または降順でソートします。

1. アルバム（フォルダ）の参照

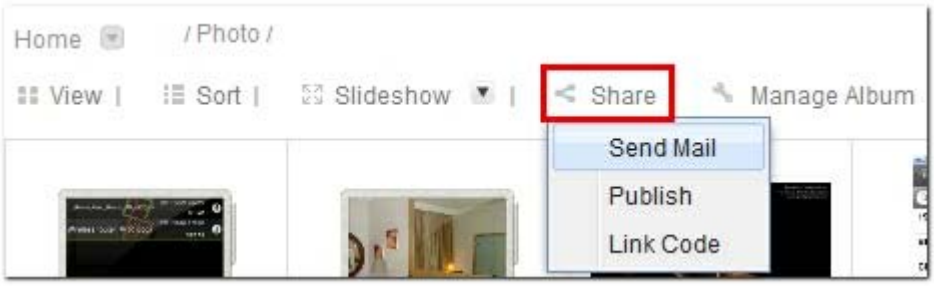
アルバム（フォルダ）を参照すると、サブフォルダおよびサポートされる画像とビデオファイルが表示されます。



アイコン/オプション	説明
Home（ホーム）	Photo Station（Qmultimedia/Multimedia フォルダ）内の全フォルダとファイルが表示されるページに移動します。
/ディレクトリ/	アルバム（フォルダ）内のディレクトリに対するクイックリンクです。
View（表示）	サムネイルまたは写真壁内から表示するコンテンツを選択します。サムネイル表示では、画像ファイル名またはビデオファイル名のみが表示されます。
Sort（ソート）	コンテンツをファイル名、サイズ、ファイル作成日、写真撮影日、アルファベットの昇順または降順でソートします。
Slideshow（スライドショー）	写真をスライドショーで表示します。三角アイコンをクリックして、表示モード、スピード、プレイリスト（背景音楽）を選択します。プレイリストは、Music Station（「Application Servers（アプリケーションサーバー）」 > Music Station）で作成および編集することができます。
Share（共有）	コンテンツを他の人と電子メール、ソーシャルネットワークへの公開、またはリンクコードにより共有します。
Manage Album（アルバム管理）	既存アルバムにアルバムを追加したり、ファイルをアップロード/コピーします。
	サムネイルサイズを調整します。

2. 写真およびビデオファイルの共有

Photo Station 上の画像を電子メール、ソーシャルネットワークへの公開、またはリンクコードによりインターネット上で共有することができます。「Share（共有）」をクリックし、オプションを選択します。

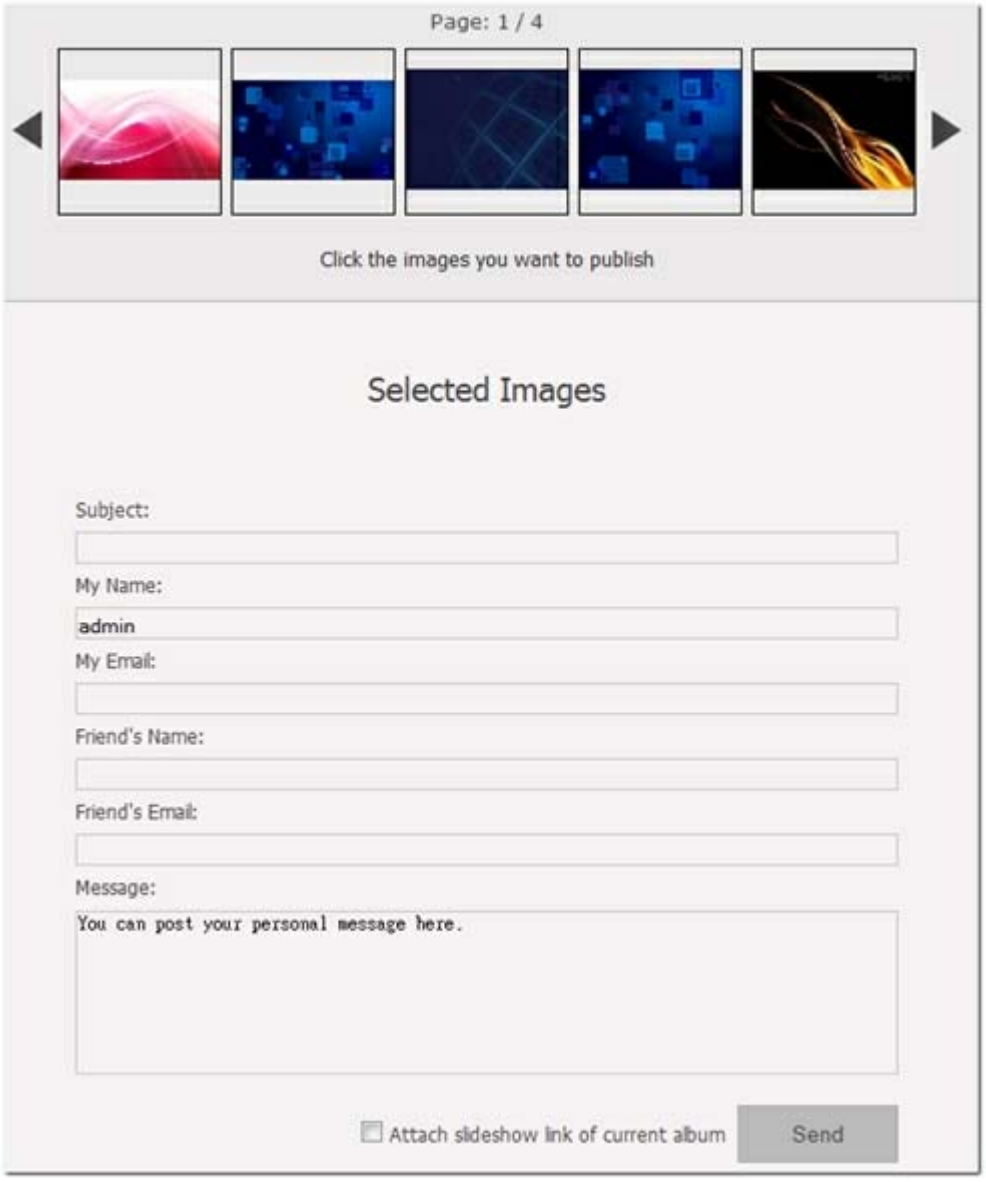


2.1 Send Mail（メールの送信）

電子メールで友達に送信する最大 5 件の画像を選択します。件名（最大 128 文字）、送信者名（最大 128 文字）とメールアドレス、受信者名（最大 128 文字）とメールアドレス、およびメッセージ（最大 1024 文字）を入力します。「Attach slideshow link of current album（カレントアルバムのスライドショーリンクを添付する）」を選択し、電子メールにアルバムスライドショーのリンクを添付します。「Send（送信）」をクリックします。

注：

- この機能を使用するには、「System Administration（システム管理）」>「Notification（通知）」>「Configure SMTP Server（SMTP サーバーの設定）」でメールサーバー設定を適切に行う必要があります。
- 画像の共有を行う前に、「Settings（設定）」>「Set Folder Public（フォルダ公開設定）」でアルバムを公開する必要があります。

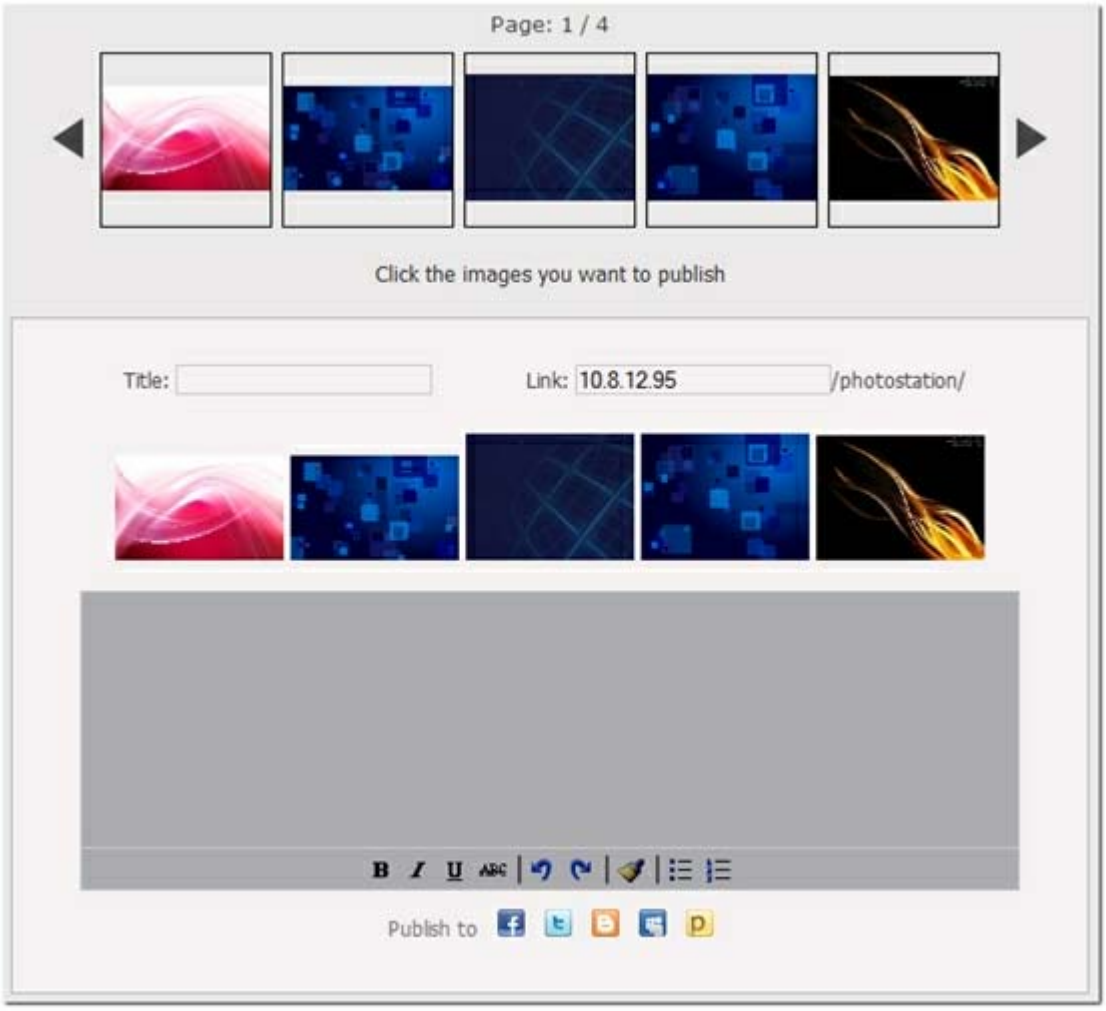

Page: 1 / 4
Click the images you want to publish
Selected Images
Subject:
My Name:
admin
My Email:
Friend's Name:
Friend's Email:
Message:
You can post your personal message here.
Attach slideshow link of current album
Send

2.2 Publish（公開）

ソーシャルネットワークに公開する最大 5 件の画像を選択します：Twitter、Facebook、MySpace、Plurk または Blogger。タイトル（最大 256 文字）とメッセージ（最大 1024 文字）を入力し、URL を指定します。ソーシャルネットワークアイコンをクリックし、ログイン情報を入力して、画像を公開します。

注：

- 画像の共有を行う前に、「Settings（設定）」>「Set Folder Public（フォルダ公開設定）」でアルバムを公開する必要があります。
- Photo Station をインターネット上でアクセス可能にする必要があります。NAS 上で DDNS（「System Administration（システム管理）」>「Network（ネットワーク）」）または MyCloudNAS サービスをセットアップすることを推奨します。



2.3 Link Code（リンクコード）

ソーシャルネットワーム、電子メール、またはフォーラムに公開するコンテンツのアルバムスライドショーのリンクをコピーします。

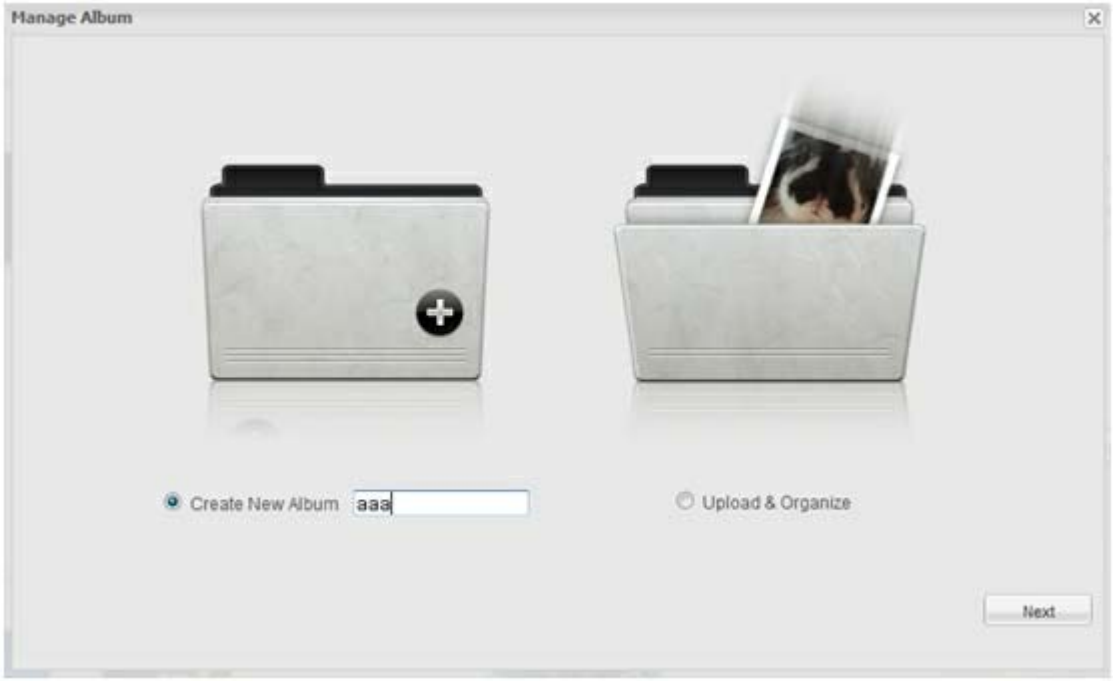
注：

- 画像の共有を行う前に、「Settings（設定）」>「Set Folder Public（フォルダ公開設定）」でアルバムを公開する必要があります。
- Photo Station をインターネット上でアクセス可能にする必要があります。NAS 上で DDNS または MyCloudNAS サービスをセットアップすることを推奨します。

3. アルバムの作成

フォルダ内にアルバムを作成するには、「Manage Album（アルバムの管理）」をクリックします。

「Create an Album（アルバムの作成）」を選択し、アルバム名を入力します。「Next（次へ）」をクリックします。

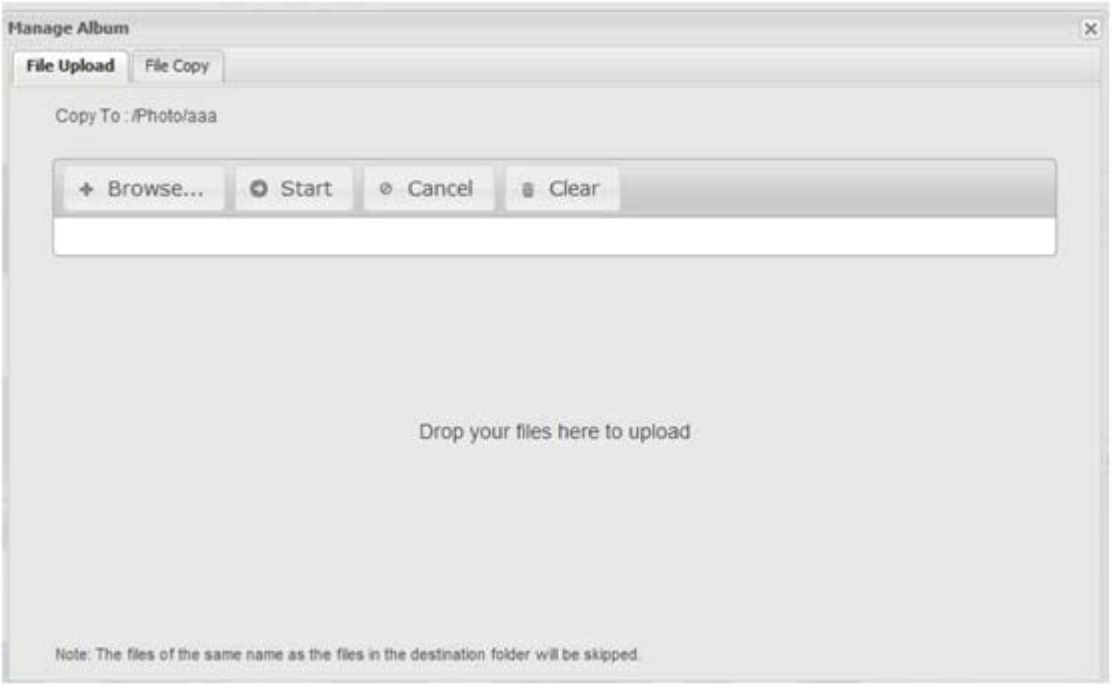


3.1 File Upload（ファイルアップロード）

「File Upload（ファイルアップロード）」タブの下で、画像またはビデオファイルを参照し、「Start（開始）」をクリックしてファイルをアップロードします。Mozilla Firefox または Google Chrome のユーザーは、ファイルをドラッグアンドドロップしてアルバムにアップロードすることができます。アルバム内に同一名称のファイルが存在する場合、操作はスキップされます。

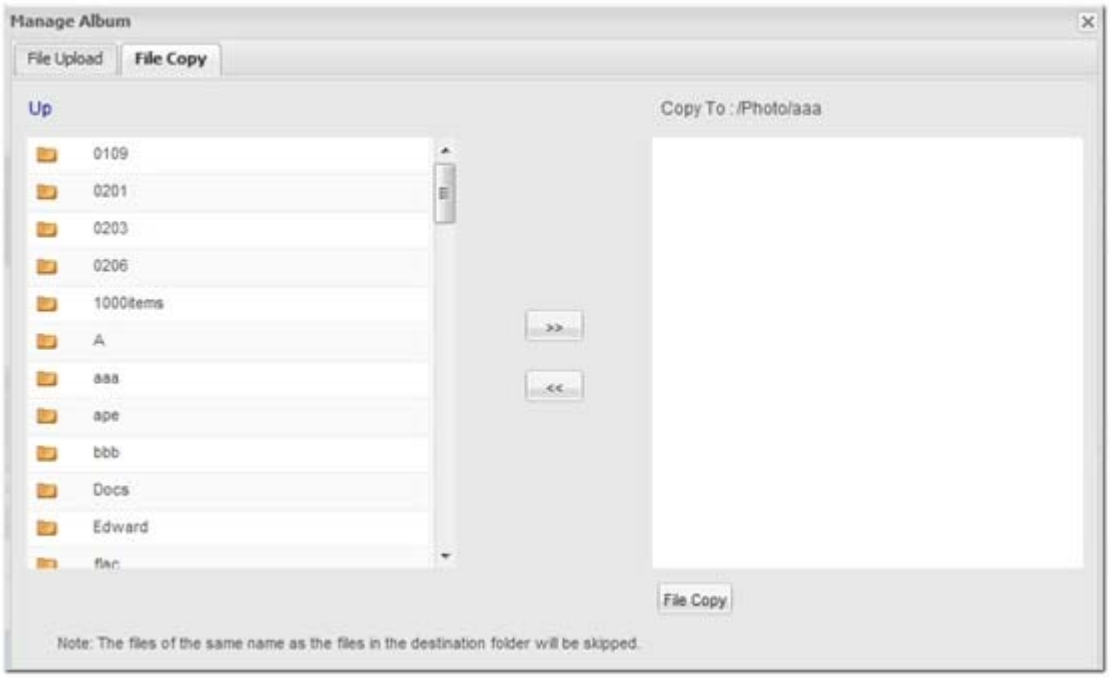
注：

- サポートされる画像ファイルの最大サイズは 32MByte です。
- 同時にアップロードできるファイルの最大サイズは 2GByte です。



3.2 File Copy（ファイルコピー）

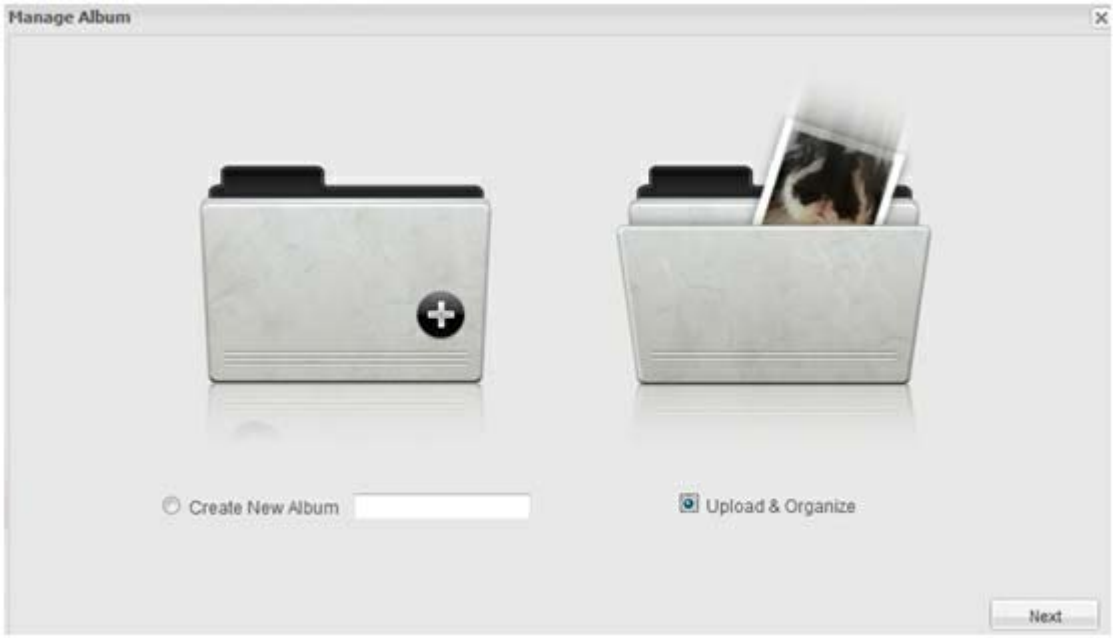
Photo Station 上のフォルダから画像またはビデオファイルを選択したアルバムにコピーするには、「File Copy（ファイルコピー）」タブの下でフォルダとファイルを選択して「 >>」をクリックします。その後、「File Copy（ファイルコピー）」をクリックします。アルバム内に同一名称のファイルが存在する場合、操作はスキップされます。



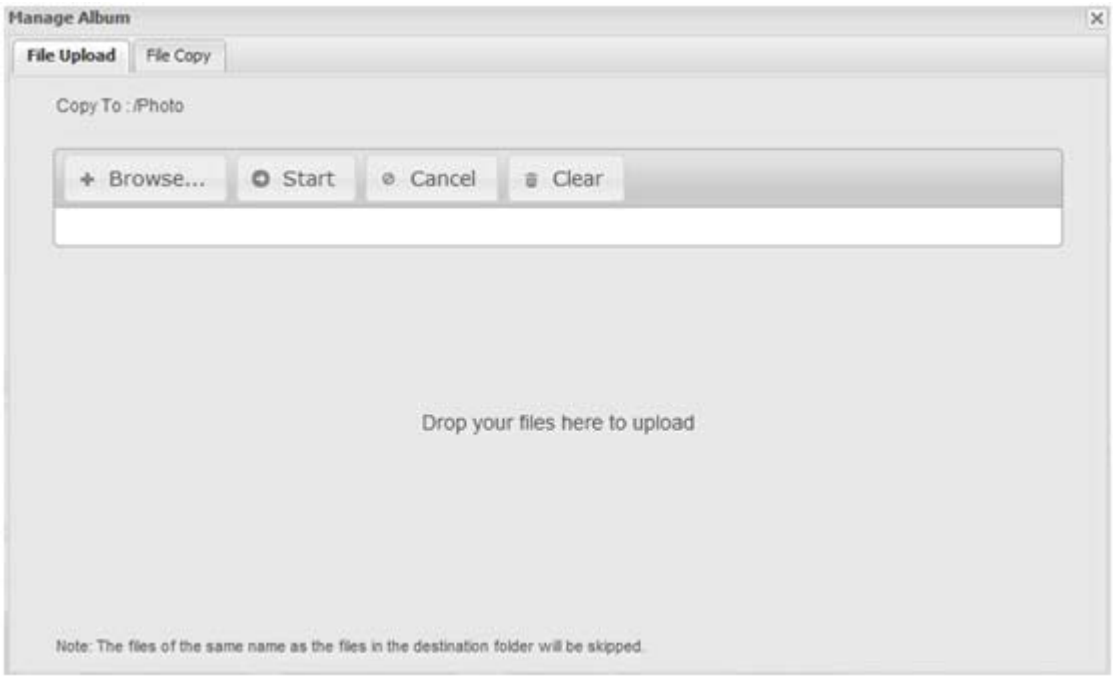
4. アルバムの編集

Photo Station 上の既存アルバムのファイルをアップロードまたはファイルをコピーするには、「Manage Album（アルバム管理）」をクリックします。

「Upload & Organize（アップロード＆整理）」を選択します。「Next（次へ）」をクリックします。



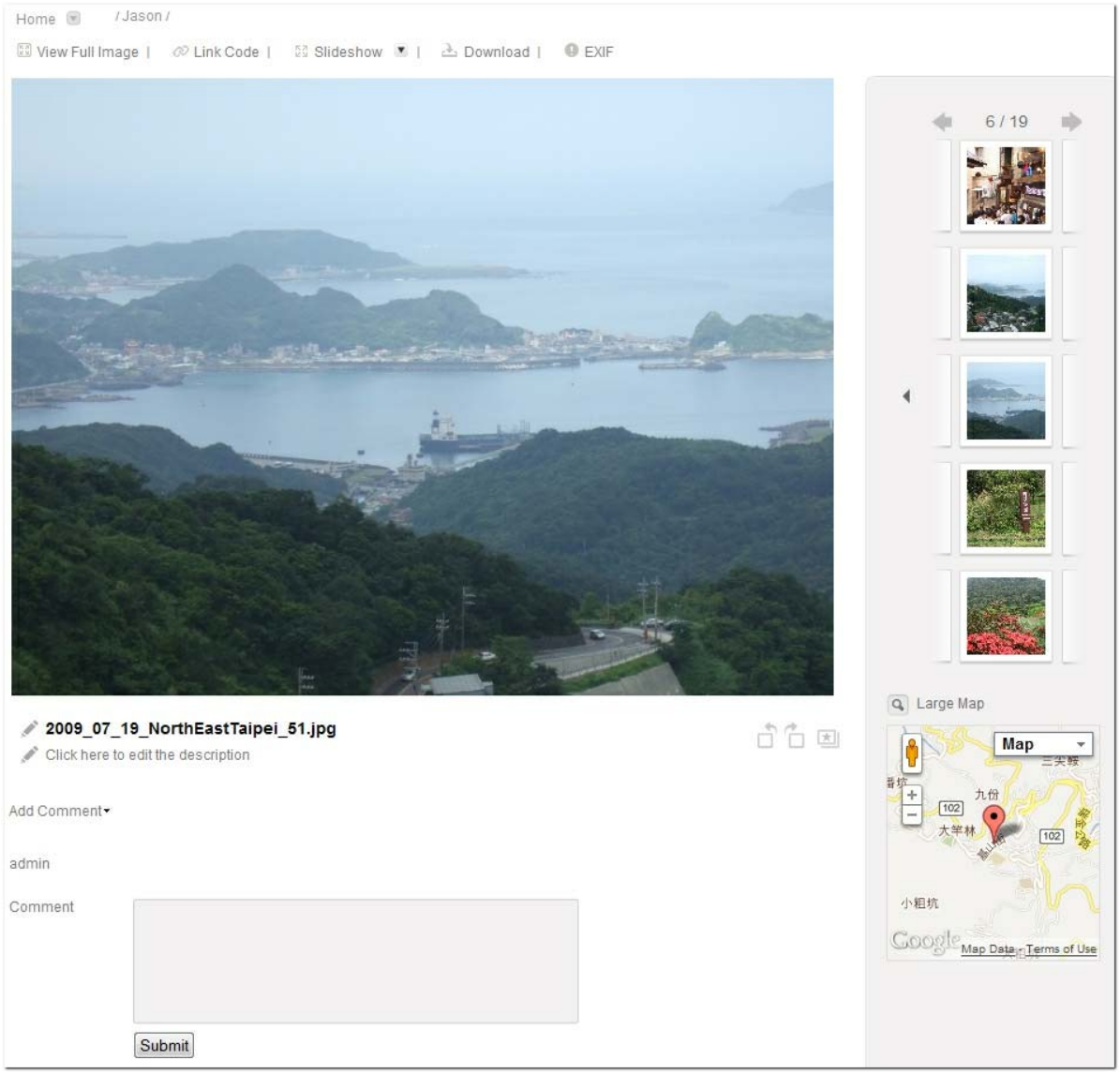
既存アルバムからアルバムにアップロードするファイルまたはコピーするファイルを選択します。



5. 写真の表示

Photo Station は、画像ファイルの表示に次のオプションをサポートします。

アイコン/オプション	説明
View Full Image （フルイメージ表示）	画像をオリジナルサイズで表示します。
Link Code（リンクコード）	インターネット上で公開するために、異なるサイズの画像のリンクをコピーします。
Slideshow （スライドショー）	アルバム内の画像をスライドショー形式で表示します。 三角アイコンをクリックして、表示モード、スピード、プレイリスト（背景音楽）を選択します。 プレイリストは、Music Station（「Application Servers（アプリケーションサーバー）」 > Music Station）で作成および編集することができます。
Download（ダウンロード）	画像をダウンロードします。
EXIF	画像の EXIF 情報を表示します。
	画像を反時計回りに 90 度回転します。
	画像を時計回りに 90 度回転します。
	画像をアルバム表紙として設定します。
File name（ファイル名）	クリックして、画像のファイル名を編集します。「Submit（実行）」をクリックして、変更を保存します。
Description（説明）	画像の説明（最大 512 文字）を入力します。
Add Comment （コメントの追加）	クリックして、画像上にコメント（最大 128 文字）を追加します。
Comment（コメント）	クリックして、画像上の全コメントを表示します。

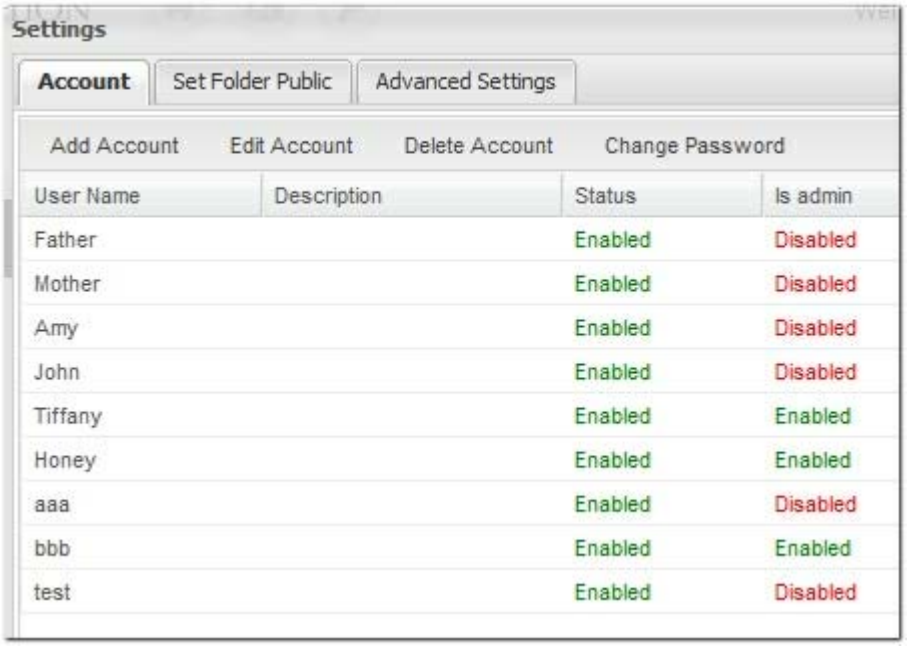

Home
/ Jason /
View Full Image |
Link Code |
Slideshow |
Download |
EXIF
6 / 19
2009_07_19_NorthEastTaipei_51.jpg
Click here to edit the description
Add Comment
admin
Comment
Submit
Large Map
Map
九份
大竿林
小粗坑
102
Google
Map Data
Terms of Use

6. ビデオの表示

ウェブブラウザで表示するビデオをクリックします。ファイルをダウンロードするには、「Download（ダウンロード）」をクリックします。

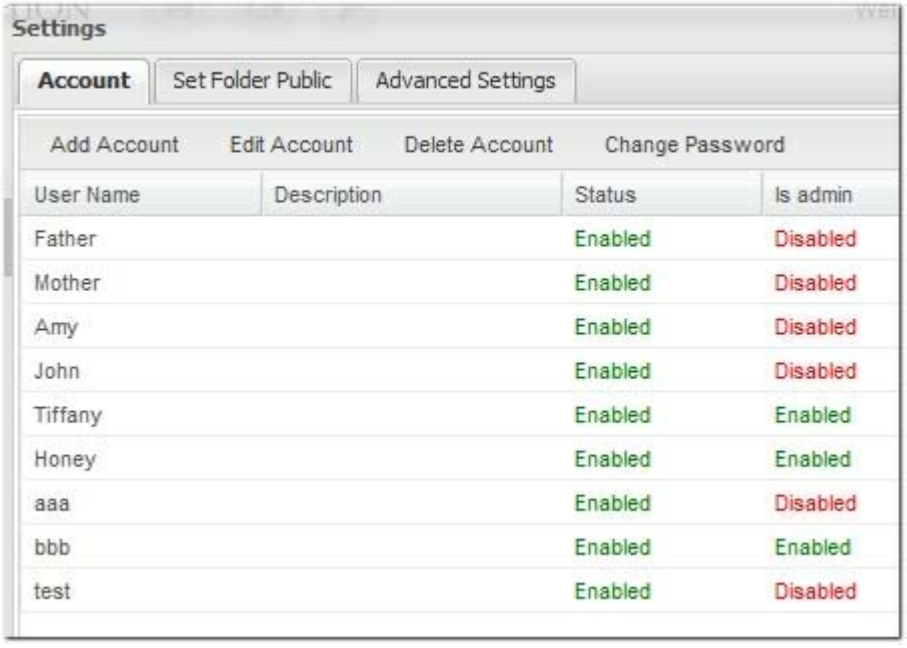
7. Settings（設定）

をクリックして、「Settings（設定）」ページに移動します。



7.1 Account（アカウント）

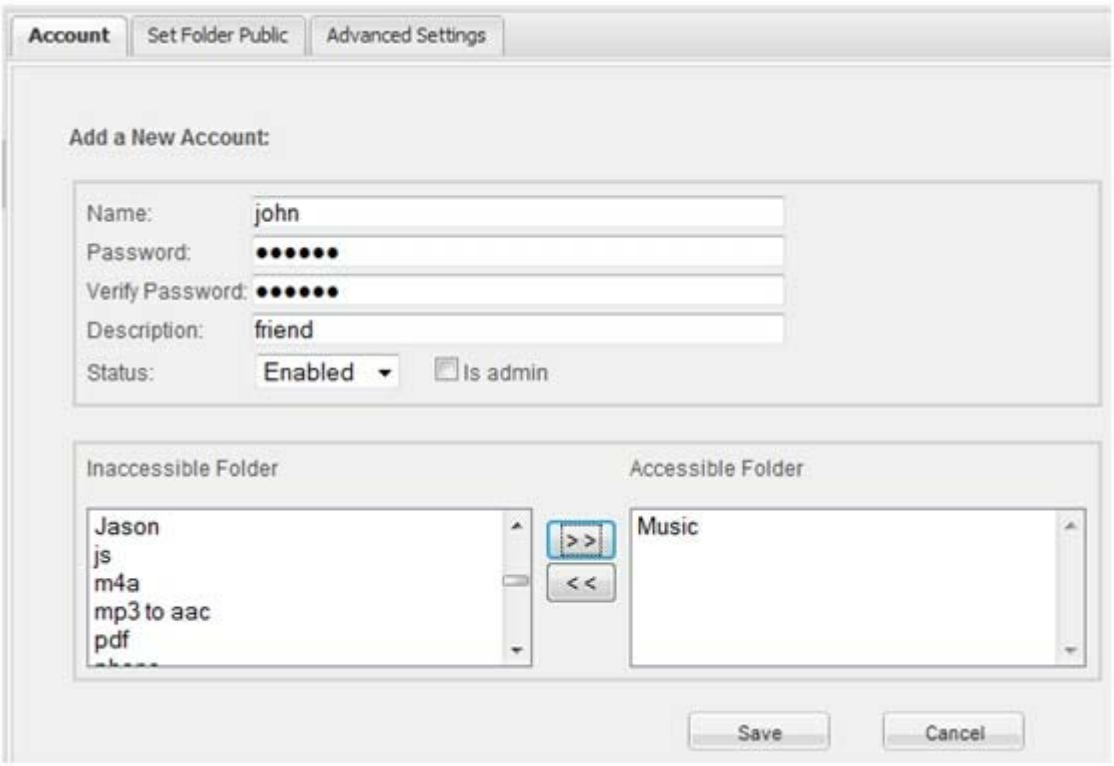
ユーザーを作成するには、「Account（アカウント）」タブの下で、「Add Account（アカウントの追加）」をクリックします。



ユーザー名（最大 32 文字）、パスワード（1 ～ 16 文字）および説明（最大 512 文字）を入力します。ユーザーのステータス（enable（有効）またはdisable（無効））を選択し、ユーザーが管理者であるかどうかを指定します。その後、ユーザーにアクセスを許可するフォルダをアクセス可能フォルダリストに追加することで選択します。「Save（保存）」をクリックします。

注：

- ユーザー名には、A ～Z、a ～ z、0 ～9、ダッシュ（-）およびアンダースコア（_）のみが利用可能です。
- パスワードには、A ～ Z、a ～ z、0 ～ 9、-、!、@、#、$、%、_ のみが利用可能です。

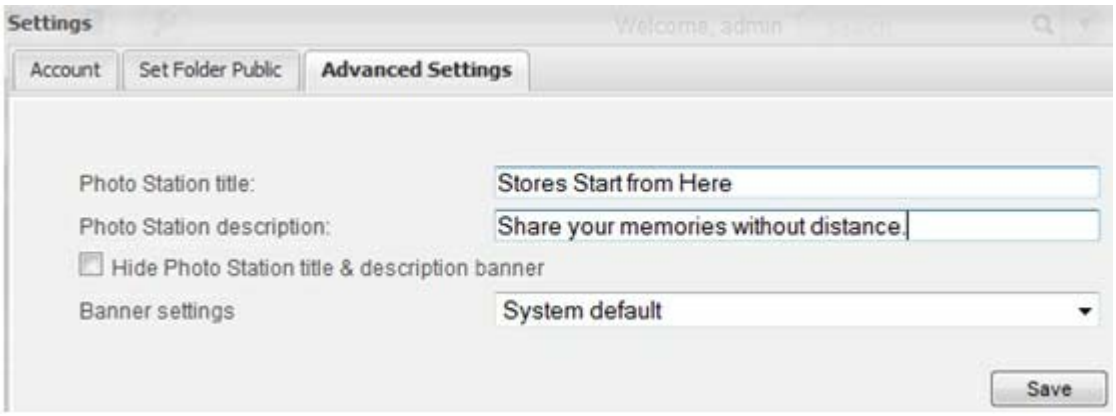


7.2 Set folder public（フォルダ公開設定）

Photo Station 内の全フォルダは初期設定では非公開です。公開するフォルダを選択します。非公開フォルダは、承認済 Photo Station ユーザーのみがアクセス可能です。「Save（保存）」をクリックして、変更を保存します。

7.3 Advanced Settings（詳細設定）

「Advanced Settings（詳細設定）」でホームページ上の Photo Station のバナーをカスタマイズします。

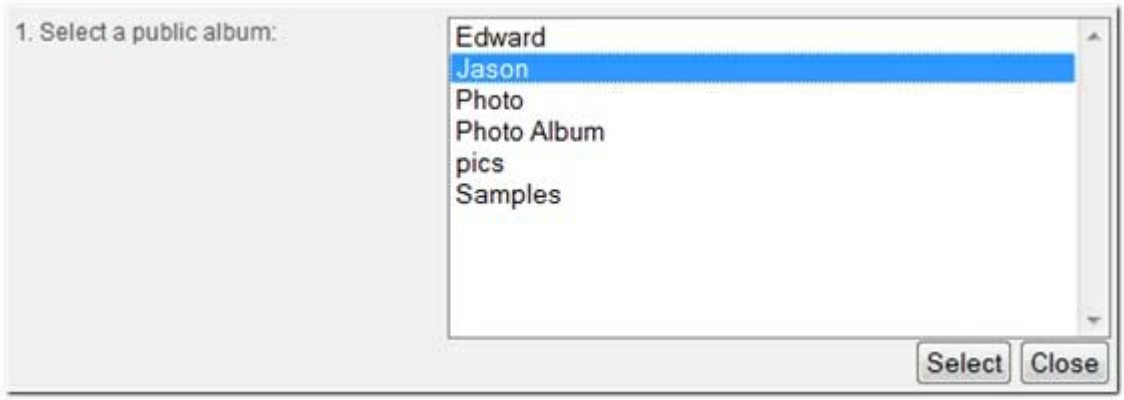


1. Photo Station のタイトル（最大 35 文字）と説明（最大 120 文字）を入力し、非表示にする情報を選択します。

2. バナー設定を選択します。2x2、3x3、または 4x4 写真壁バナーを選択し、「Browse（参照）」をクリックして、公開アルバムを選択します。

3. 「Select（選択）」をクリックします。

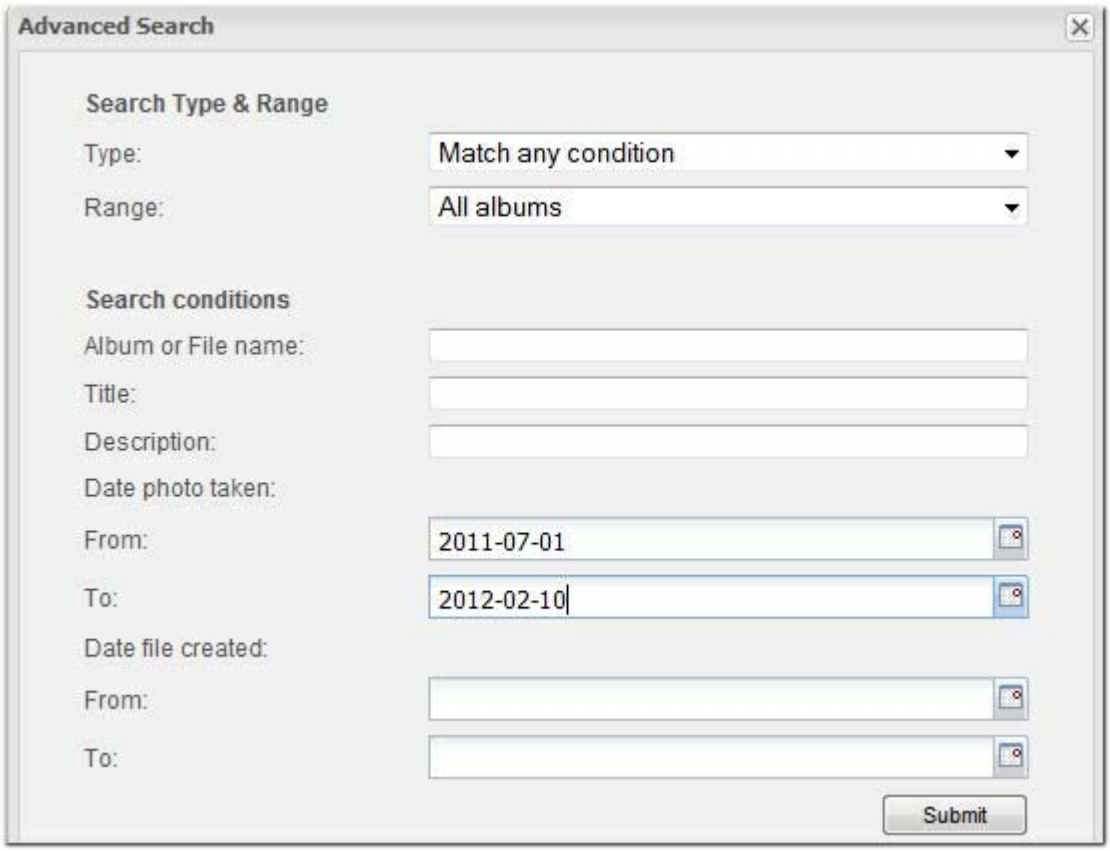
4. 公開アルバム内の写真が下に表示されます。バナーブロック（赤くハイライト表示される）を選択し、画像ファイルを選びます。システムの初期画像を伴う空ブロックが表示されます。「Save（保存）」をクリックして、変更を保存します。



8. 「Advanced search（高度な検索）」

「Advanced search（高度な検索では）」、フォルダ（アルバム）およびファイル（写真またはビデオ）を検索するためのより多くのオプションを提供します。 検索ボックスの横の三角アイコンをクリックして、「Advanced search（高度な検索）」ページに移動します。

検索条件を入力し、「Submit（実行）」をクリックします。



7.4 Music Station

Music Station とは、NAS またはメディアサーバー上の音楽ファイルの再生、ウェブブラウザを介するリモートストリーミングあるいは NAS に接続された USB サウンドカードを介するローカル再生により、インターネットラジオを行うウェブベースのアプリケーションです。また、ローカル再生では音楽アラームを設定できます。

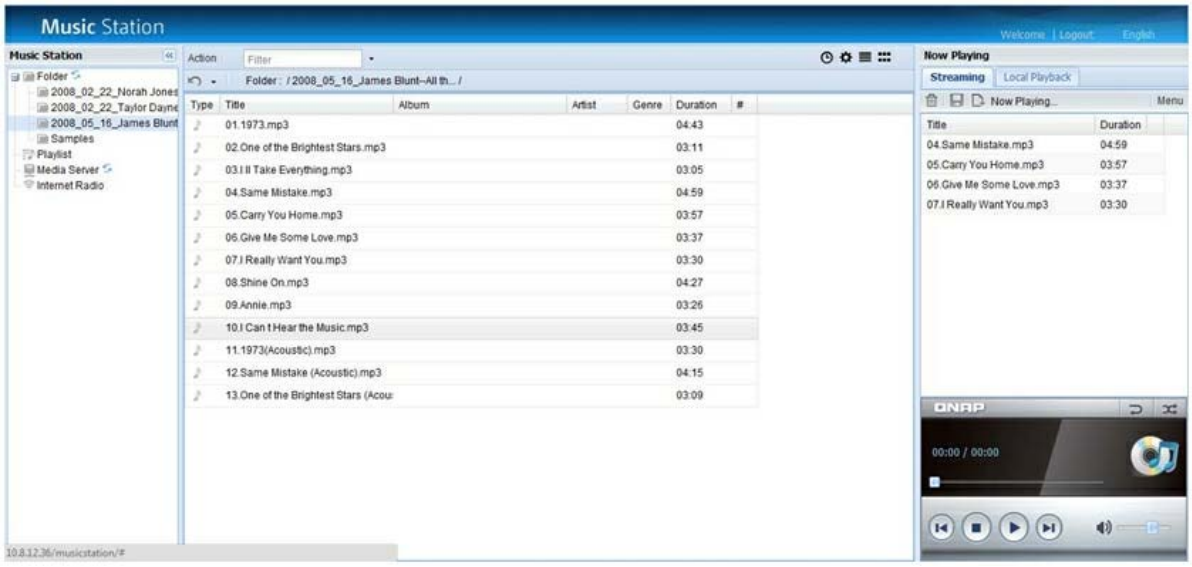
以下のステップに従って、Music Station を有効にし、再生する音楽ファイルを準備します。

1. NAS に「admin」としてログインします。「Application Servers（アプリケーションサーバー）」 > 「Music Station」に移動し、この機能を有効にします。

2. 音楽ファイルを NAS の「Multimedia」または「Qmultimedia」フォルダにアップロードします。Music Station にアップロードされたフォルダは初期設定では非公開で、管理者または承認済管理グループのみが管理できます。

3. Music Station に管理者としてログインします。Music Station の管理者ログイン情報は、NAS ウェブ管理者のそれと同じです。

注：Music Station は、マルチメディアステーションと同一のユーザーアカウント情報を使用します。Music Station のユーザーを作成するには、マルチメディアステーションに「admin」としてログインし、「Control Panel（コントロールパネル）」>「User Management（ユーザー管理）」でアカウントを作成します。



A. 音楽ソース

再生可能な音楽ファイルは左パネル上に表示されます。以下に項目を説明します:

1. Folder(フォルダ): NAS の Multimedia または Qmultimedia フォルダ上のフォルダおよびサポートされる音楽ファイルが表示されます。「Folder(フォルダ)」をクリックし、リストの読込みまたは再読込みを行います。

> 注: Music Station は、MP3、MP4、OGG、WAV、AIFF、AU、FLAC、M4A、APE フォーマットのオーディオファイルのみをサポートします。

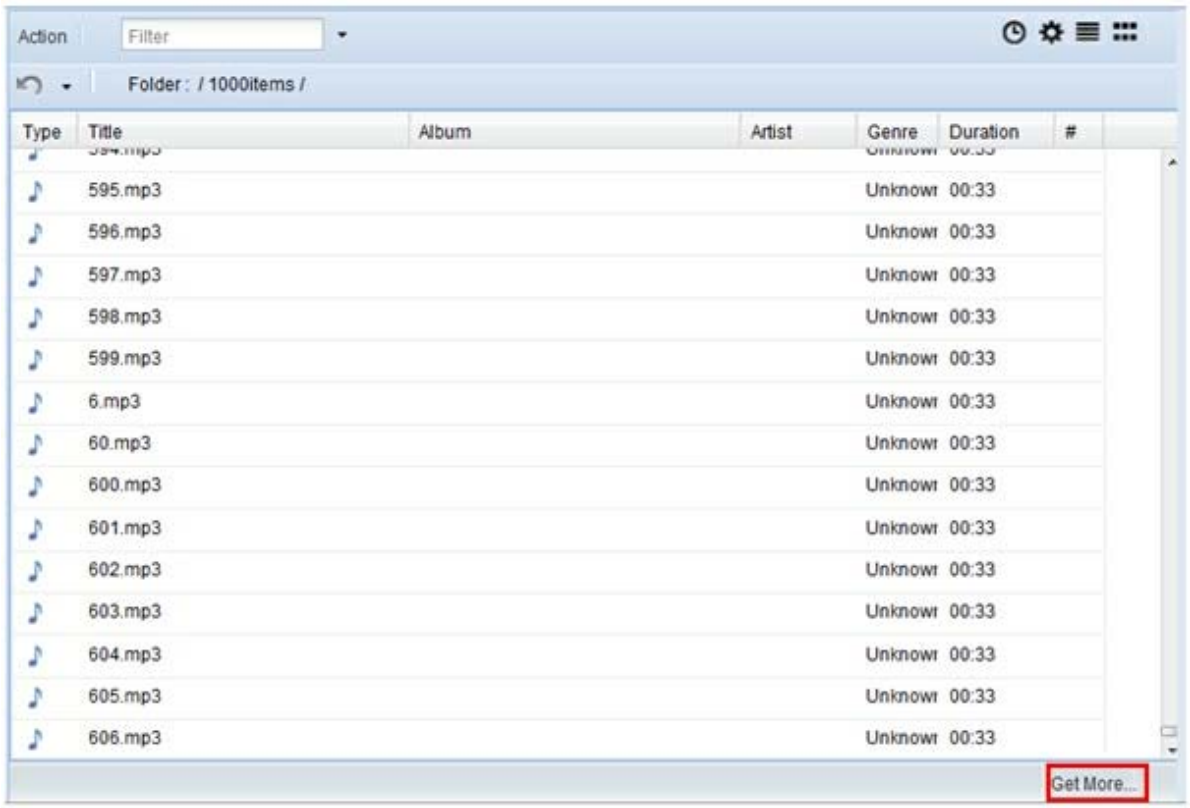
2. Playlist(プレイリスト): Music Station 上で利用可能なプレイリストです。各プレイリストは、NAS またはメディアサーバー上の音楽ファイルおよびインターネットラジオを含む 512 項目を含むことができます。最大 128 件のプレイリストがサポートされます。

3. Media server(メディアサーバー):「Media Server(メディアサーバー)」をクリックすると NAS は、自動的にローカルネットワーク上の利用可能な全 DLNA メディアサーバーを検索します。サポートされる音楽ファイルのみが表示されます。

4. Internet radio(インターネットラジオ): インターネットラジオ局のリンクです。最大 1024 項目をサポートします。ラジオ局タイプが MP3 である必要があることに注意してください。

フォルダ内の 600 項目を超える表示

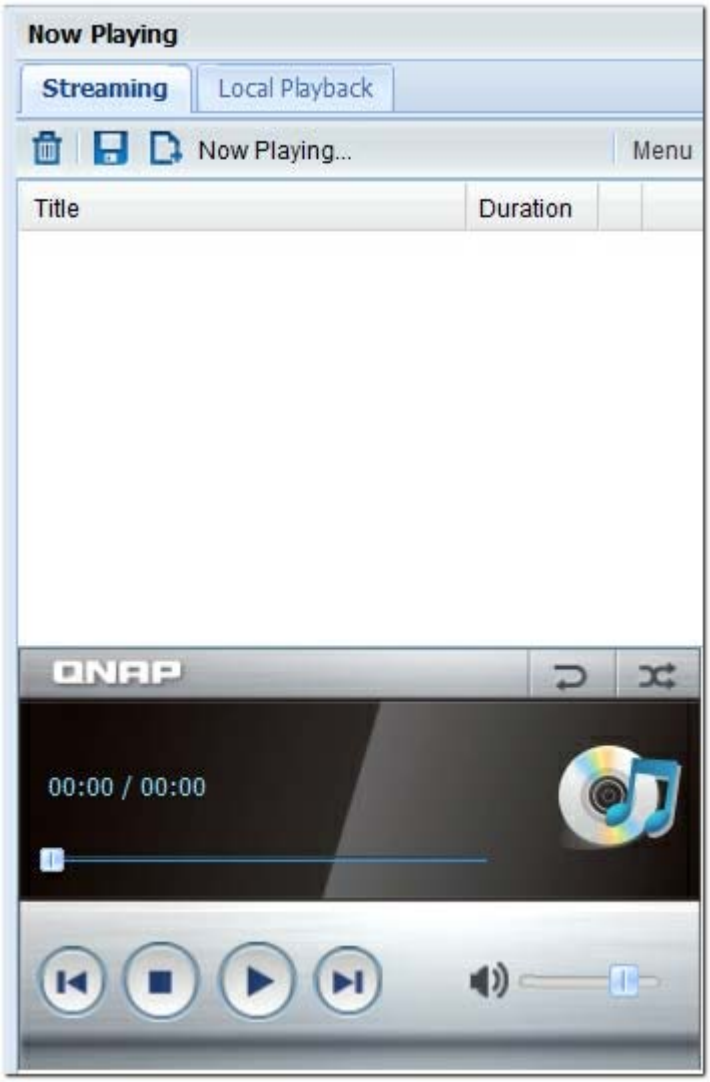
フォルダに 600 を超える項目が含まれる場合、Music Station は、アルファベット順に最初の 600 項目を表示します。画面上の右下の「Get more（次項目）」をクリックして、次の 500 項目を読み込みます。



B. 音楽再生

右側の「Now Playing（現在再生中）」パネルには、2 つの再生モードがあります：

1. Streaming（ストリーミング）（ウェブブラウザによる音楽再生）
2. Local playback（ローカル再生）（NAS に接続された USB スピーカーまたはサウンドカードによる音楽再生）



プレイヤー

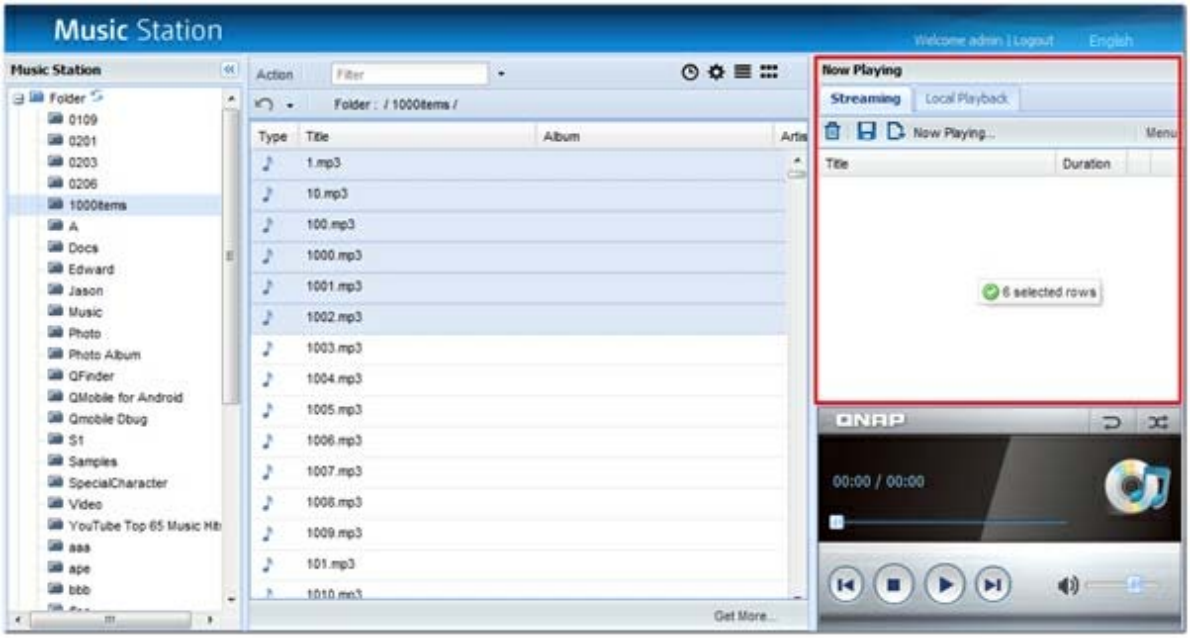
アイコン	説明
	現在のプレイリストを繰り返します。
	プレイリスト内の項目順を並べ替えます。
	再生。
	一時停止。
	停止。
	前項目を再生します。
	次項目を再生します。
	音量を調整します。

音楽ファイルの再生

1. 「Folder（フォルダ）」、「Playlist（プレイリスト）」、「Media Server（メディアサーバー）、または「Internet Radio（インターネットラジオ）」内のコンテンツを参照します。
2. ファイル名をダブルクリックして、ファイルを再生中リストに追加し直ちに再生するか、1 つまたは複数ファイルを右クリックして、「Add Selected Entries to Playlist（選択済エントリをプレイリストに追加）」をクリックします。

または

1. をクリックして、コンテンツを詳細表示します。
2. 1 つまたは複数のマルチメディアファイルを「Now Playing（現在再生中）」の下のプレイリストにドラッグアンドドロップします。



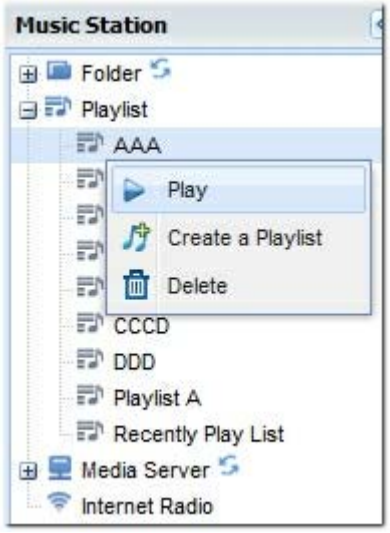
フォルダの再生

フォルダを右クリックして、「Add Selected Entries to Playlist（選択済エントリをプレイリストに追加）」を選択するか、フォルダを「Now Playing（現在再生中）」にドラッグアンドドロップします。

注：フォルダに 100 件を超える音楽ファイルが含まれている場合、最初の 100 件のファイルのみがプレイリストに追加されます。

プレイリストの再生

1. 「Playlist（プレイリスト）」の下のエントリを参照します。
2. プレイリストを右クリックして、「Play（再生）」を選択します。



「Create a Playlist（プレイリストの作成）」

1. 「Playlist（プレイリスト）」を右クリックして、「Create a Playlist（プレイリストの作成）」を選択します。

2. プレイリスト名（最大 24 文字）を入力し、「OK」をクリックします。

または

1. 「Now Playing（現在再生中）」の下の　をクリックします。
2. ファイルまたはフォルダをプレイリストに追加します。
3. をクリックするか、「Menu（メニュー）」＞「Save（保存）」で、プレイリスト名を入力します。
4. 「OK」をクリックします。

注：最大 128 件のプレイリストがサポートされます。各プレイリストは、最大 512 項目を含むことができます。

プレイリストの編集

1. 左パネルからプレイリストを「Now Playing（現在再生中）」にドラッグアンドドロップします。
2. プレイリストにファイルまたはフォルダを追加し、項目順の並べ替えまたは項目の削除を行います。
3. をクリックするか、「Menu（メニュー）」>「Save（保存）」で変更を保存するか、「Menu（メニュー）」>「Save as（名前を付けて保存）」でプレイリストを新規保存します。

プレイリスト内の項目順の並べ替え

1. プレイリストを「Now Playing（現在再生中）」にドラッグアンドドロップします。
2. 並べ替える項目をドラッグアンドドロップします。
3. をクリックして、変更を保存します。

インターネットラジオ局の追加

1. 「Internet Radio（インターネットラジオ）」を右クリックします。
2. 「Add an Internet Radio（インターネットラジオの追加）」をクリックします。
3. 名称（最大 512 文字）、URL（最大 1024 文字）、および説明（最大 512 文字）を入力します。
4. 「OK」をクリックします。

注：インターネットラジオ局のタイプは MP3 である必要があります。

インターネットラジオ局の編集

1. インターネットラジオ局を右クリックします。
2. 「Edit Internet Radio Settings（インターネットラジオ設定の編集）」をクリックします。
3. コンテンツを編集し、「OK」をクリックして、変更を保存します。

インターネットラジオ局の編集

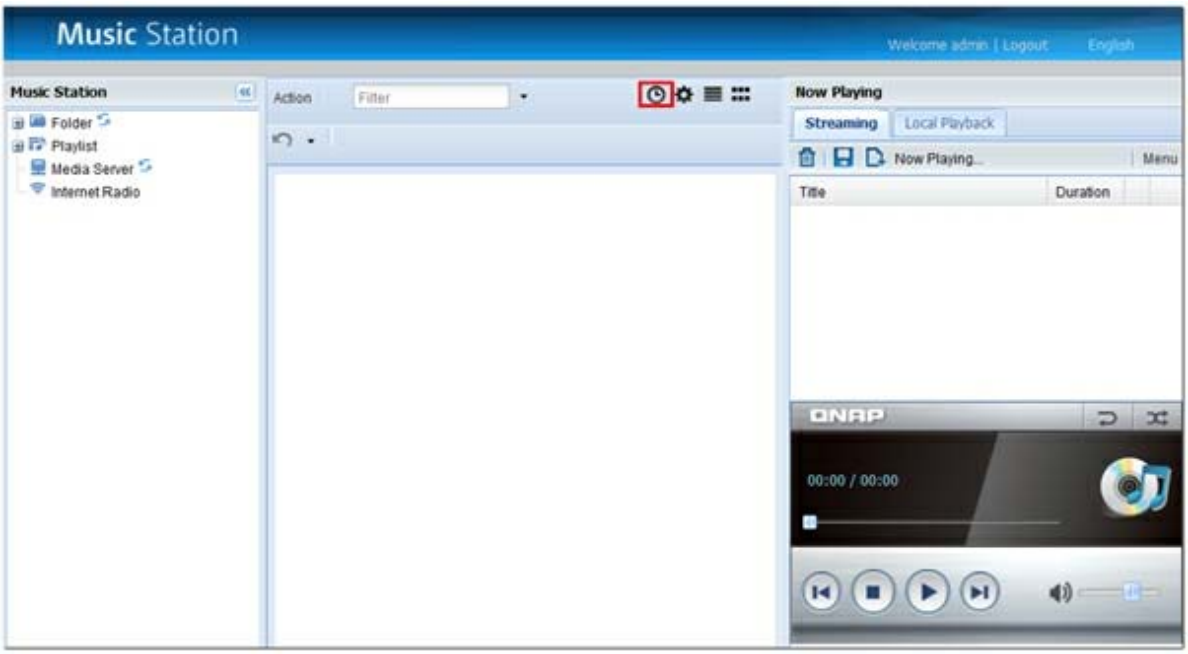
1. インターネットラジオ局を右クリックします。
2. 「Remove（削除）」をクリックします。

C. Music Alarm（音楽アラーム）

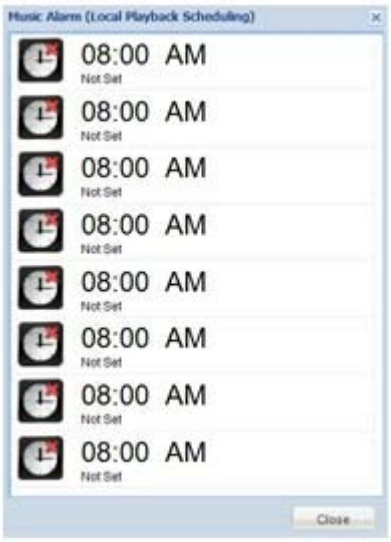
Music Station は、ローカル再生モードでは音楽アラーム設定をサポートします。この機能を使用するには、NAS に USB スピーカーまたは USB サウンドカードを接続する必要があります。

音楽アラームの設定

1. をクリックします。

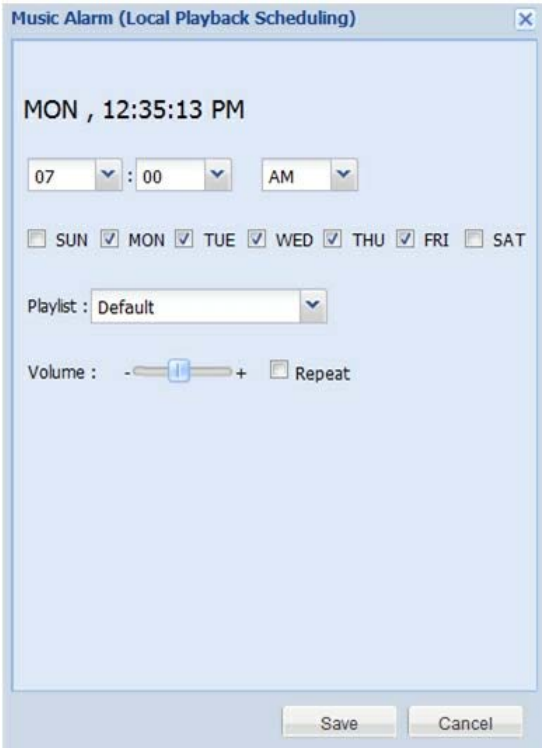


2. スケジュールをクリックします。



3. アラームスケジュールを設定します。
4. デフォルトアラームの使用または Music Station 上のプレイリストを選択します。
5. アラーム音量を調整します。
6. アラームがオンの時、プレイリストを繰り返し再生するには、「Repeat（繰り返し）」を選択します。

7. 「Save（保存）」をクリックします。



音楽アラームの有効/無効

アイコン	説明
	アラームは有効です。
	アラームは無効です。

アイコンをクリックして、アラームを有効または無効にします。

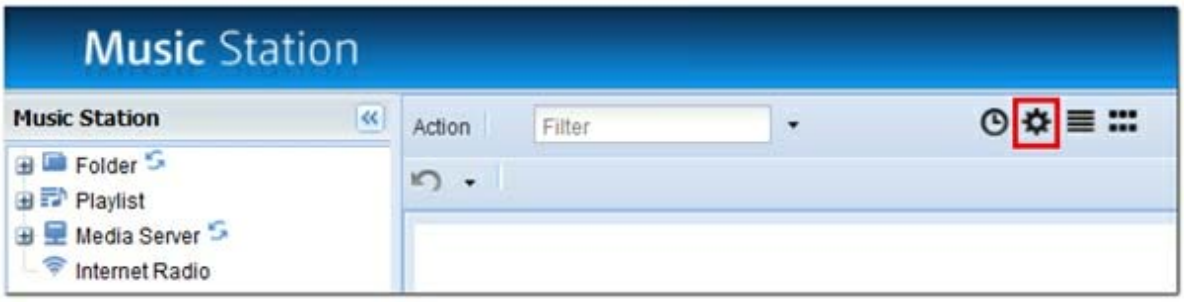
音楽アラームの停止

音楽アラームを停止するには、NAS の前面のワンタッチコピーボタンを押すか、ローカル再生モード画面の停止ボタン をクリックします。

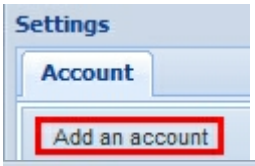
D. アカウントおよびアクセス管理

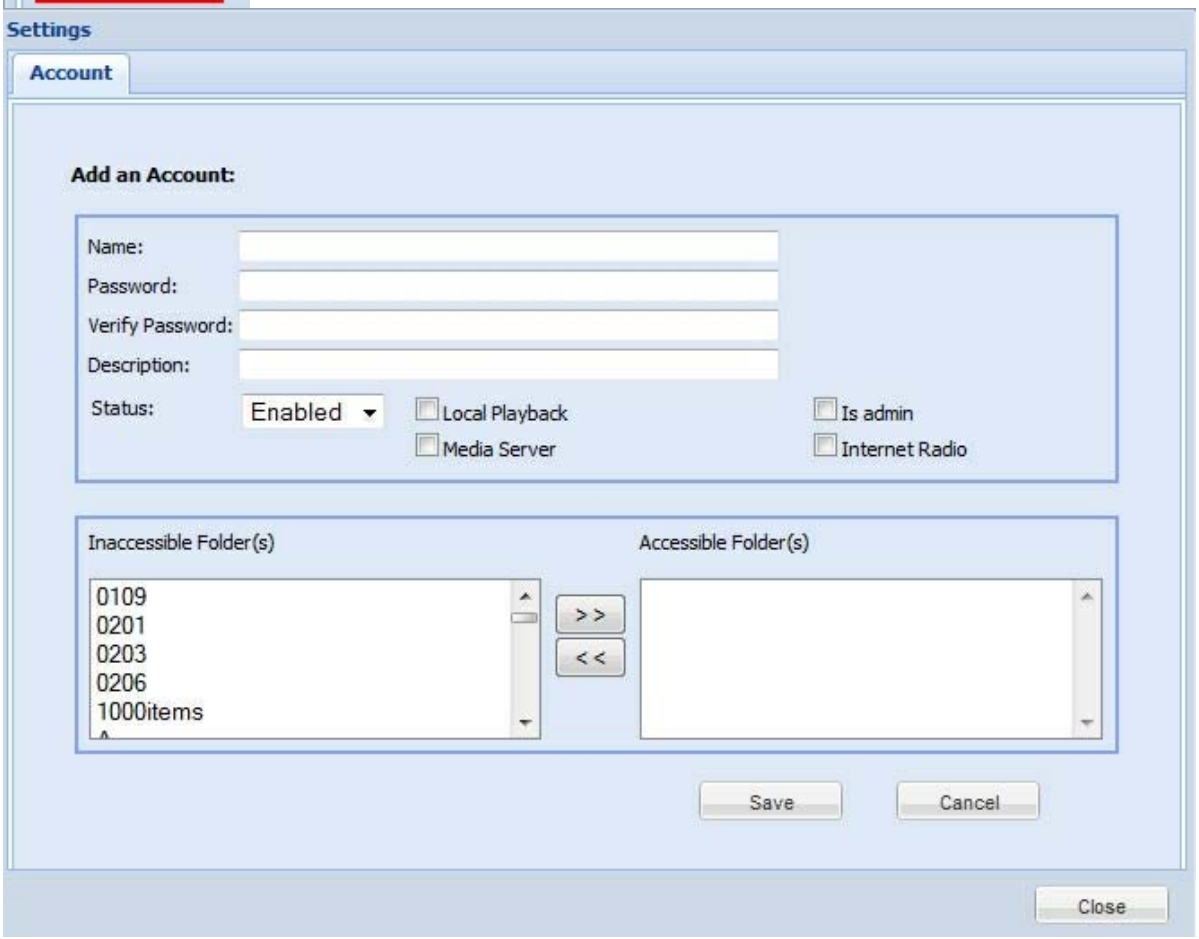
アカウントの作成

1. をクリックします。



2. 「Add an account（アカウントの追加）」をクリックします。





3. ユーザー名（最大 32 文字）、パスワード（最大 16 文字）および説明（最大 512 文字）を入力します。アルファベット（A ～ Z および a ～ z）、数字（0 ～ 9）、ダッシュ（-）、およびアンダースコア（_）のみをサポートします。

4. アカウントを有効または無効にし、権限を付与します。
   - Local Playback（ローカル再生）：ユーザーにローカル再生を介する音楽ファイルの再生を許可します。
   - Is admin（管理者である）：ユーザーにプレイリストの管理および音楽アラームの設定を許可します。
   - Media Server（メディアサーバー）：ユーザーにメディアサーバーコンテンツへのアクセスを許可します。
   - Internet Radio（インターネットラジオ）：ユーザーにインターネットラジオ局へのアクセスを許可します。ユーザーに管理者権限とインターネットラジオへのアクセス権が付与されている場合、インターネットラジオのコンテンツを編集できます。

5. ユーザーにアクセスを許可するフォルダを選択します。

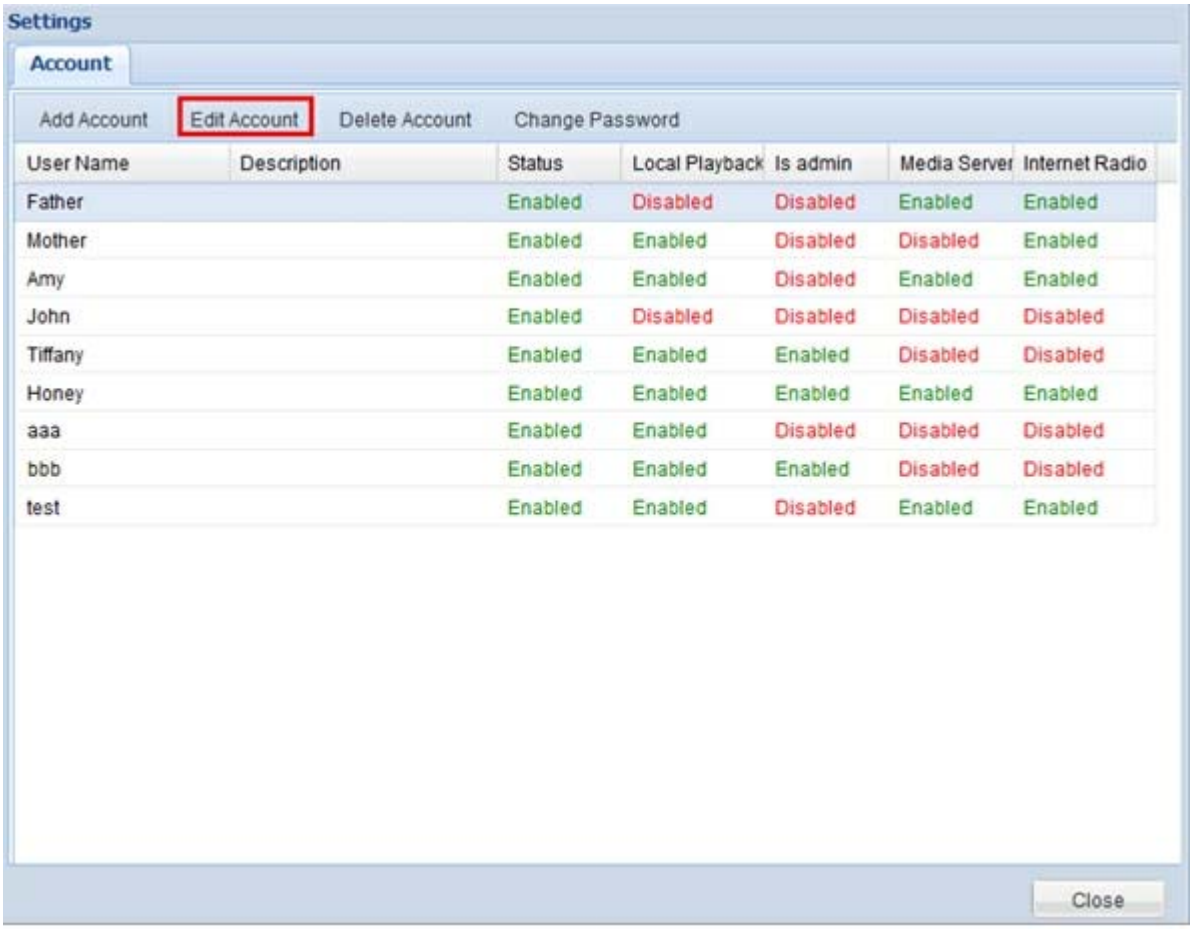
6. 「Save（保存）」をクリックします。

注：

- マルチメディアステーション、Music Station、および Photo Station でサポートされる合計ユーザー数は、「admin」を含めて最大 1024 件です。
- ユーザーはアクセス不能フォルダ内のプレイリストと音楽ファイルを参照することは可能ですが、それらを再生することはできません。

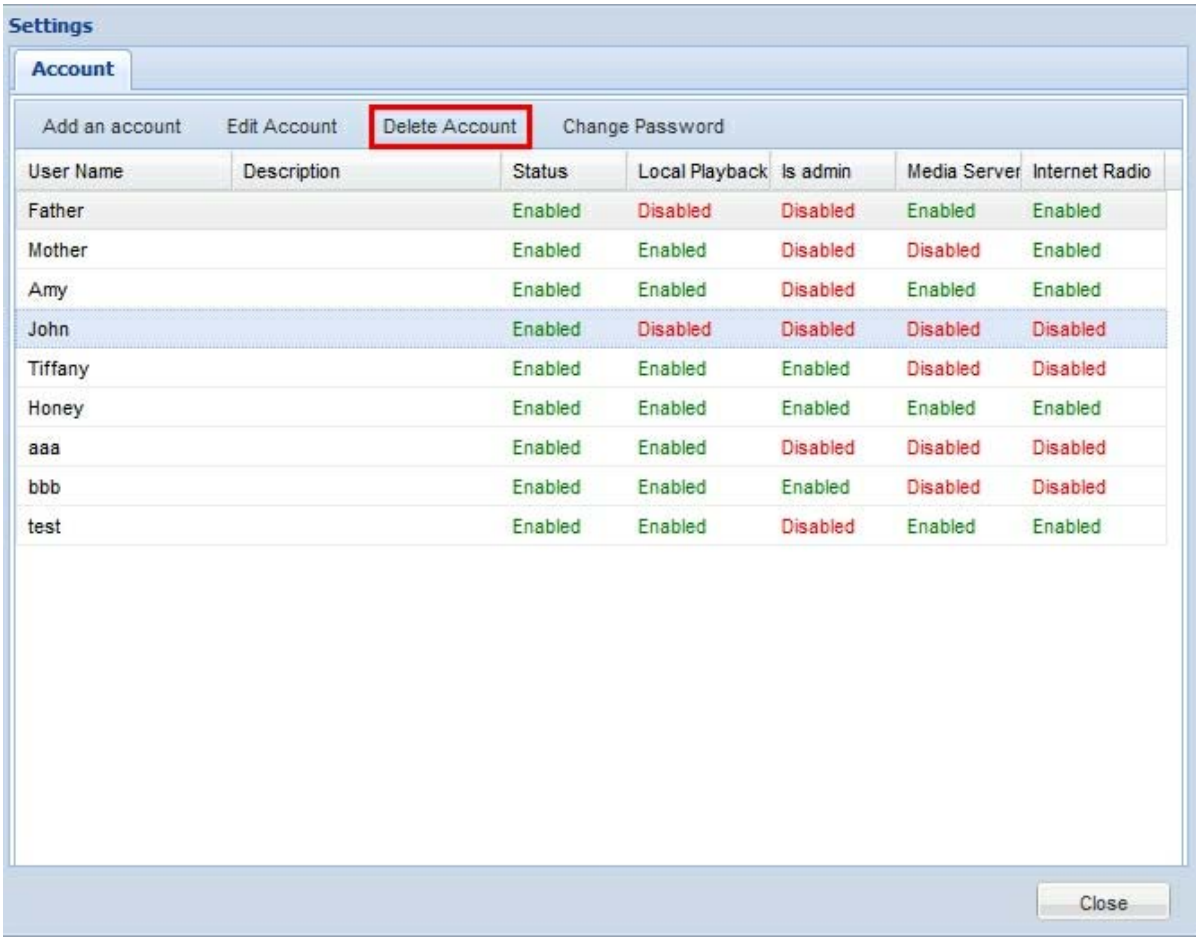
アカウントの編集

1. をクリックします。
2. アカウントを選択します。
3. 「Edit Account（アカウントの編集）」をクリックします。
4. 設定を編集し、「Save（保存）」をクリックします。



アカウントの削除

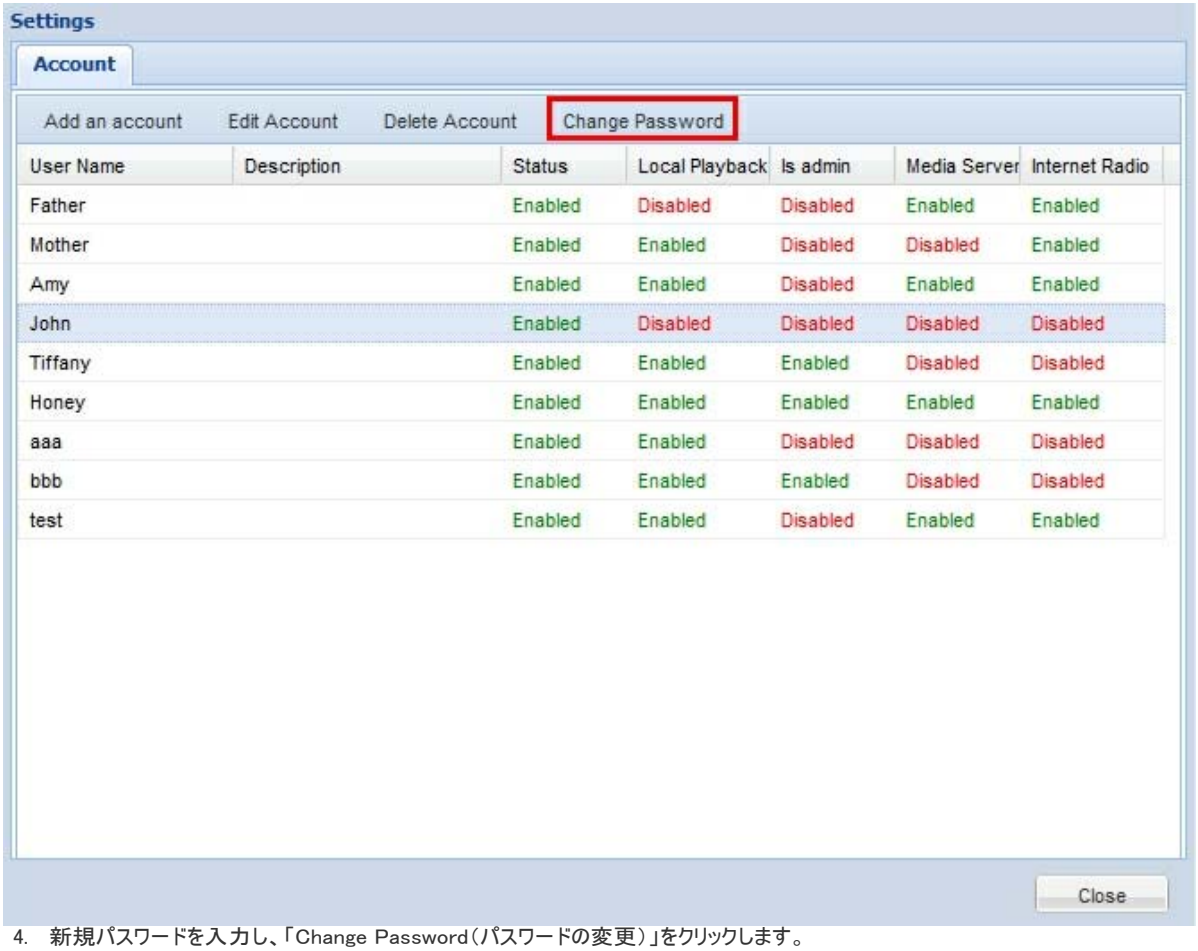
1. をクリックします。
2. アカウントを選択します。
3. 「Delete Account（アカウントの削除）」をクリックします。



4. 「OK」をクリックして、確認します。

Change Password（パスワードの変更）

1. をクリックします。
2. アカウントを選択します。
3. 「Change Password（パスワードの変更）」をクリックします。



4. 新規パスワードを入力し、「Change Password（パスワードの変更）」をクリックします。

7.5 ダウンロードステーション (Download Station)

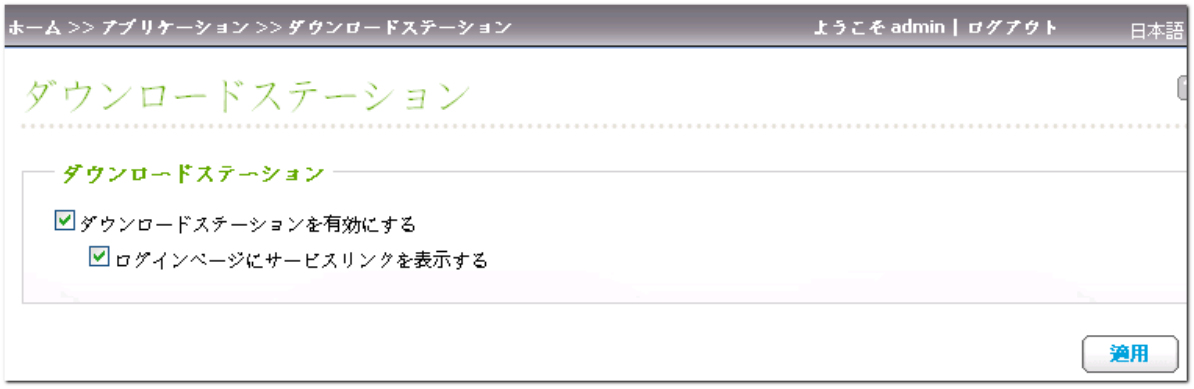
NASはBT、HTTP、FTP、RapidShareダウンロードに対応しています。NASにダウンロードタスクを追加し、PCとは無関係にダウンロードサーバーの側でダウンロードを終了できます。

重要：著作権のある資料のダウンロードは違法です。 Download Stationの機能は、ダウンロードを認可されたファイルに対してのみ有効です。 認可されていない資料のダウンロードまたは配布は、民事罰および刑事罰の対象となります。 ユーザーは著作権法に制約され、すべての結果を受け入れなければなりません。

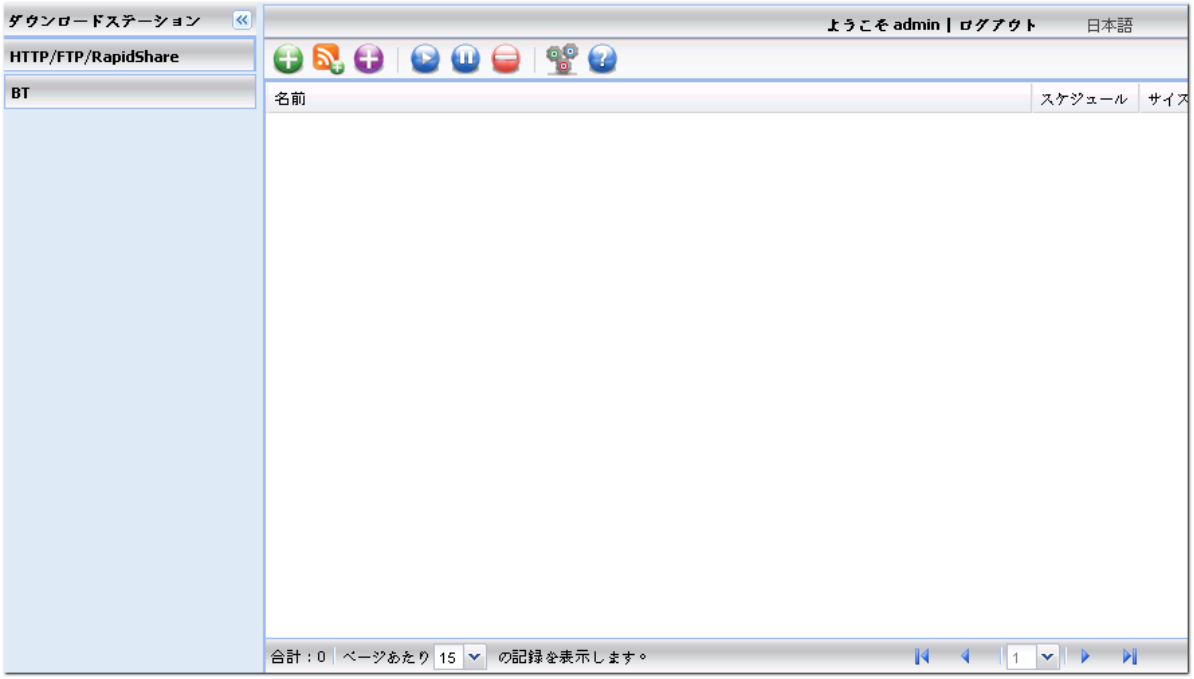
注:

- バージョン3.3.x以下から3.4.0以上にNASファームウェアを更新することで、Download Stationはv1からv2にアップグレードされます。 Run（実行）、Pause（一時停止）、およびFinish（終了）リストのタスクはすべて停止され、消去されます。 ダウンロードされたファイルはそのまま維持されます。
- Download Station v2はQGet 2.0以降と互換性があります。

1. 「Application Servers（アプリケーション・サーバー）」 > 「Download Station」に移動します。 サービスを有効にします。



2. NASのログインページ上部の「Download Station」をクリックして、Download Stationに接続します。NASのログインページからサービスにログインする場合、ユーザー名とパスワードを入力するように求められます。



ファイルのダウンロードを開始する前に、 をクリックしてダウンロード設定を設定してください。

グローバル設定

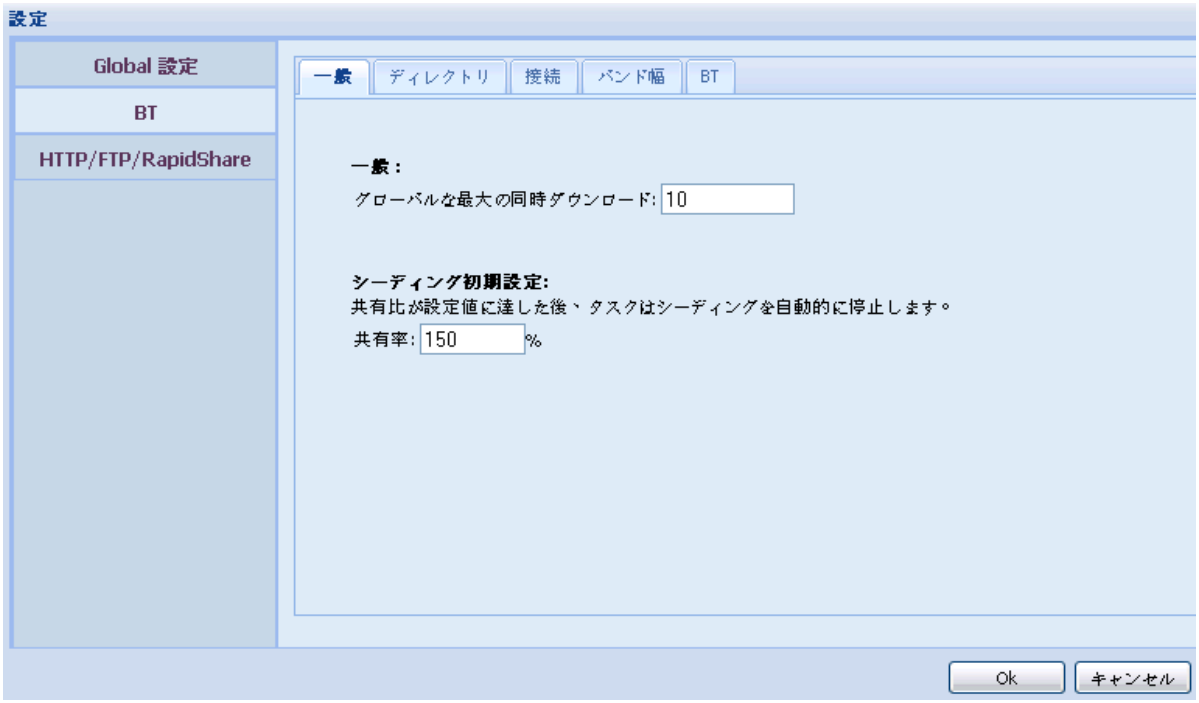
連続ダウンロードを選択するか、タスクのダウンロードスケジュールを指定します。

BT設定

1. 全般：

NASと共有比率に対して許可された同時BTダウンロードの最大数を指定します。共有比率は、アップロードされたデータの量をダウンロードされたデータの量で割ることで計算されます。 比率がその制限に達すると、アップロードは自動的に停止します。

NASモデル	同時ダウンロードの最大数
IntelベースのNAS	30
ARMベース（非Intelベース）NAS	10



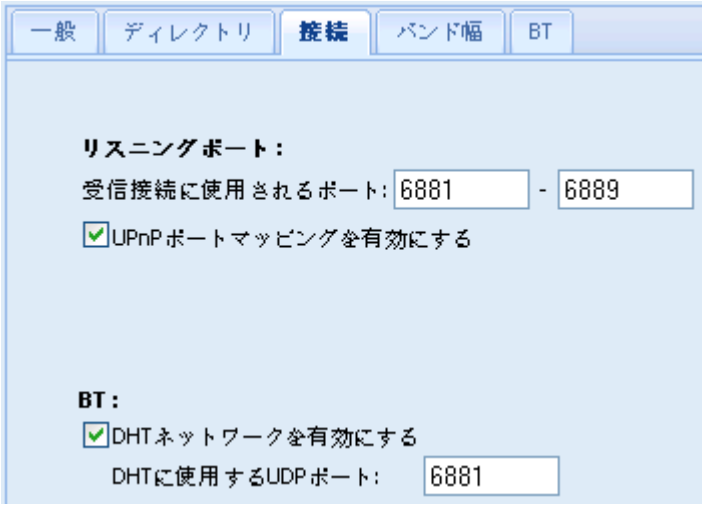
2. ディレクトリ

ダウンロードしたファイルを保存するための、デフォルトフォルダを選択します。 ダウンロードが完了したファイルの移動先フォルダを指定することもできます。

3. 接続

BT Download用のポートを指定します。 デフォルトのポート番号は6881-6889です。 UPnPポートマッピングを選択することで、UPnPサポートゲートウェアでパートマッピングが自動的に有効になります。

DHTネットワークの有効化： torrentのトラッカを接続できない場合でもNASでファイルをダウンロードできるようにするには、DHT（分散ハッシュテーブル）ネットワークを有効にしてDHTのUDPポート番号を指定します。

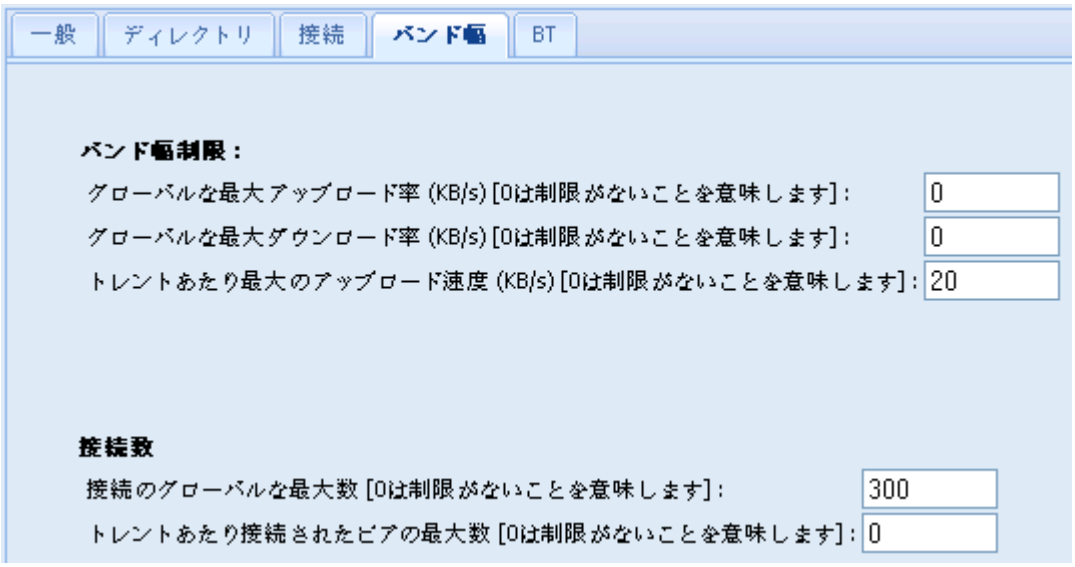


4. バンド幅

すべてのBT Downloadタスクに対して、最大のアップロードおよびダウンロード比率を指定します。 0は制限がないことを意味します。

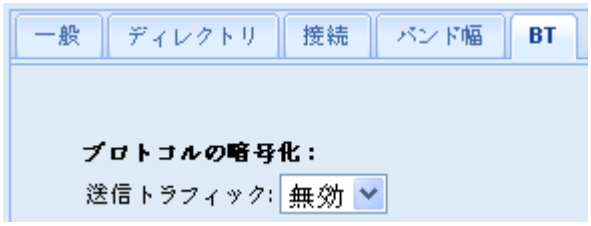
接続のグローバル最大数： これは、torrentに対して許可された最大の接続数を指します。

torrent当たりの接続されたピアの最大数： これは、torrentに接続するピアの許可された最大の接続数を指します。



5. BT

プロトコルの暗号化： 暗号化されたデータ転送に対してこのオプションを有効にします。

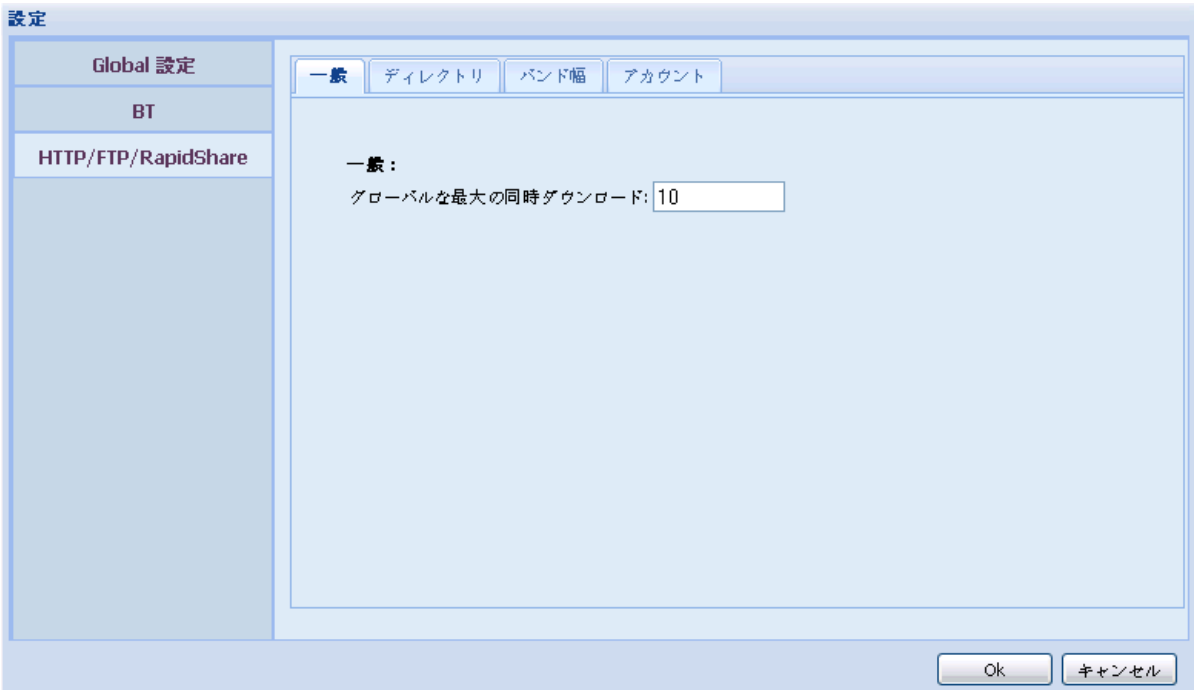

一般
ディレクトリ
接続
バンド幅
BT
プロトコルの暗号化：
送信トラフィック:
無効

HTTP、FTP、RapidShare設定

1. 全般：

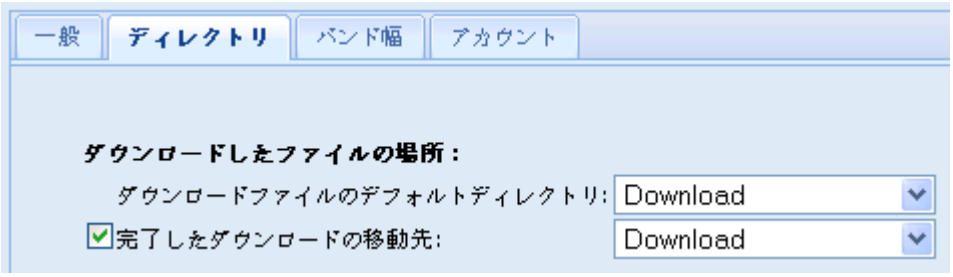
NASに対して許可された同時HTTP、FTP、RapidShareダウンロードの最大数を指定します。「OK」をクリックして変更を保存します。

NASモデル	同時ダウンロードの最大数
IntelベースのNAS	30
ARMベース（非Intelベース）NAS	10



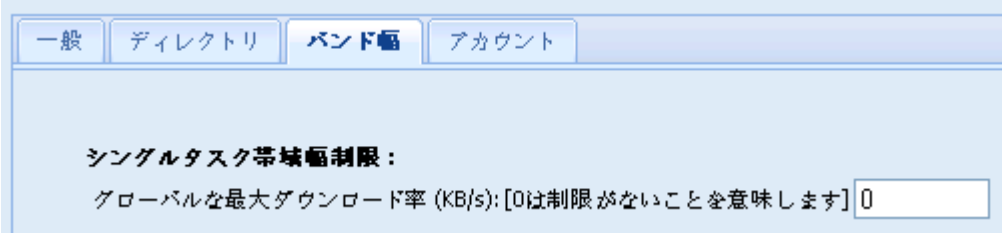
2. ディレクトリ

ダウンロードしたファイルを保存するための、デフォルトフォルダを選択します。 ダウンロードが完了したファイルの移動先フォルダを指定することもできます。 「OK」をクリックして変更を保存します。



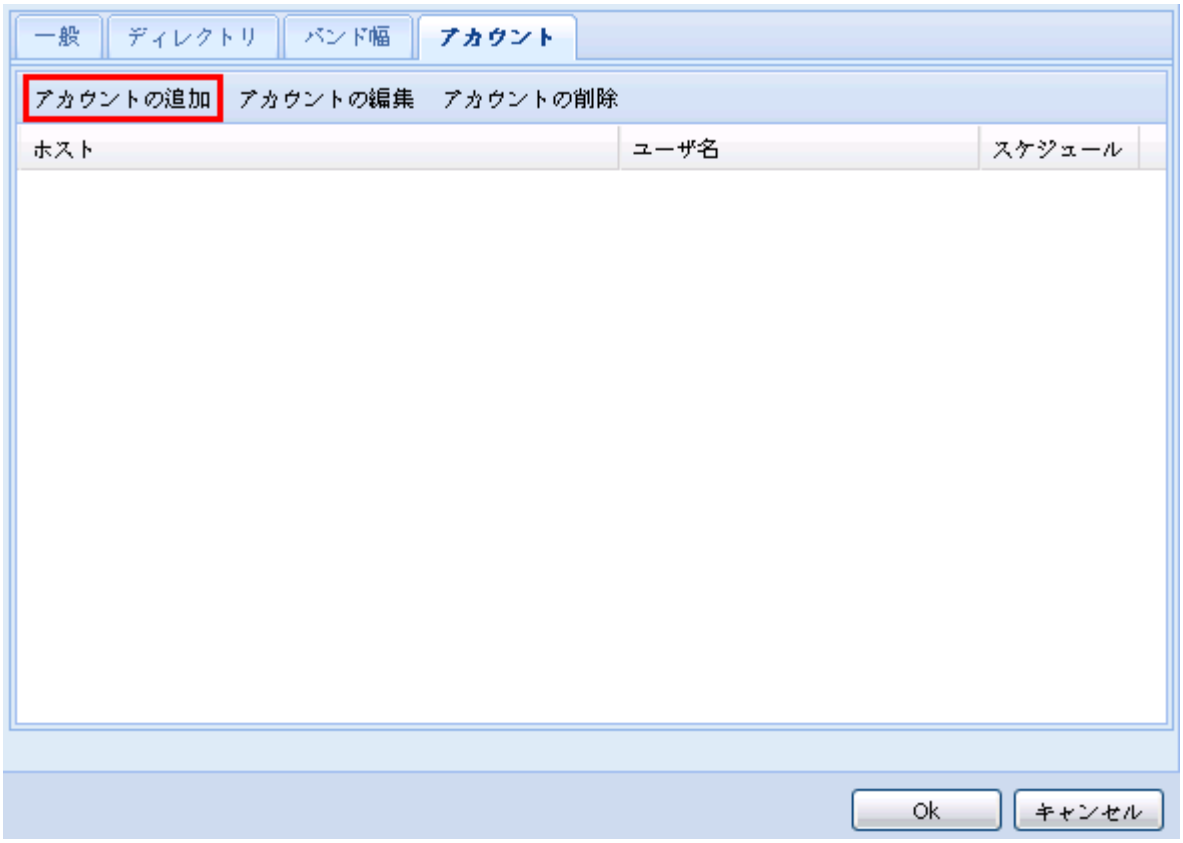
3. バンド幅

単一HTTP、FTP、またはRapidShareダウンロードの最大ダウンロード比率を指定します。 0は制限がないことを意味します。 「OK」をクリックして変更を保存します。



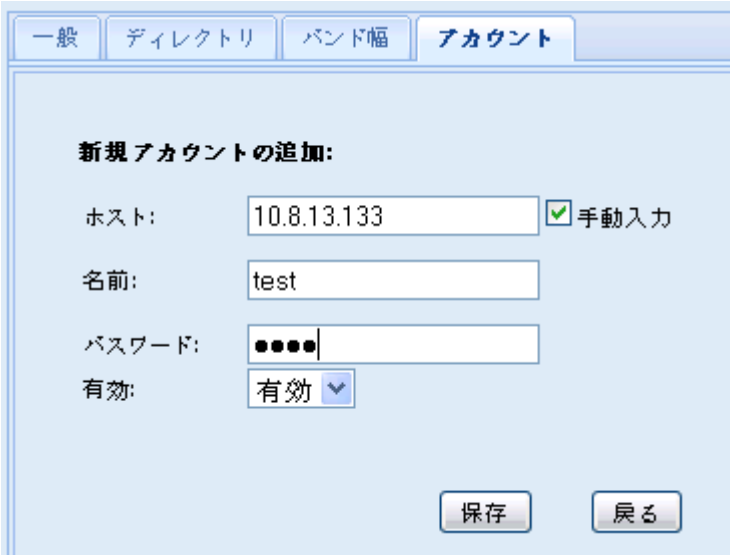
4. アカウント

HTTP、FTP、RapidShareアカウントのログイン情報を最大64保存できます。 ログイン情報を追加するには、「Add Account (アカウントの追加) 」をクリックします。

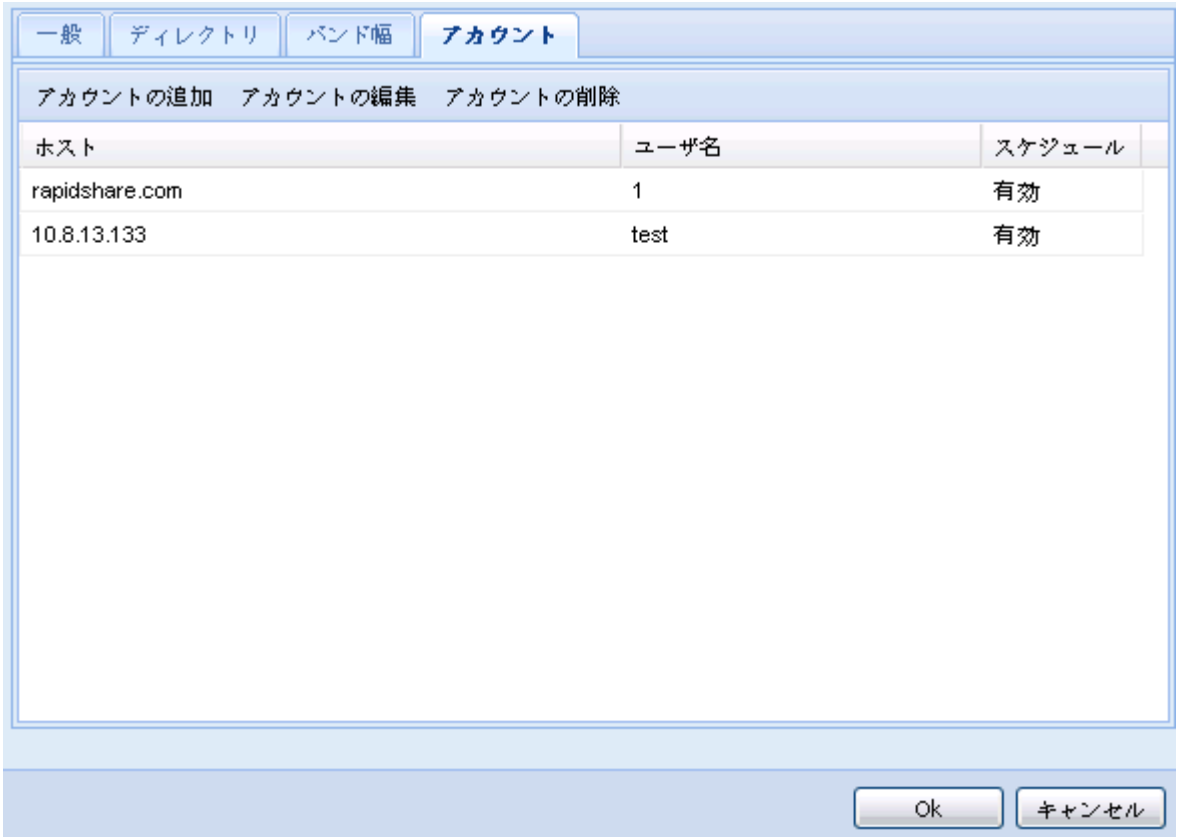


デフォルトのホストはrapidshare.comです。 HTTPまたはFTPサーバーのログイン情報を入力するには、「Input manually (手動で入力) 」を選択します。

ホスト名またはIP、ユーザー名とパスワードを入力します。 HTTP、FTP、またはRapidShareダウンロードを設定しているときアカウント選択に対してログイン情報を表示できるようにするには、ドロップダウンメニューから「Enabled（有効）」を選択します。 「Save（保存）」をクリックして確認するか、「Back（戻る）」でキャンセルします。

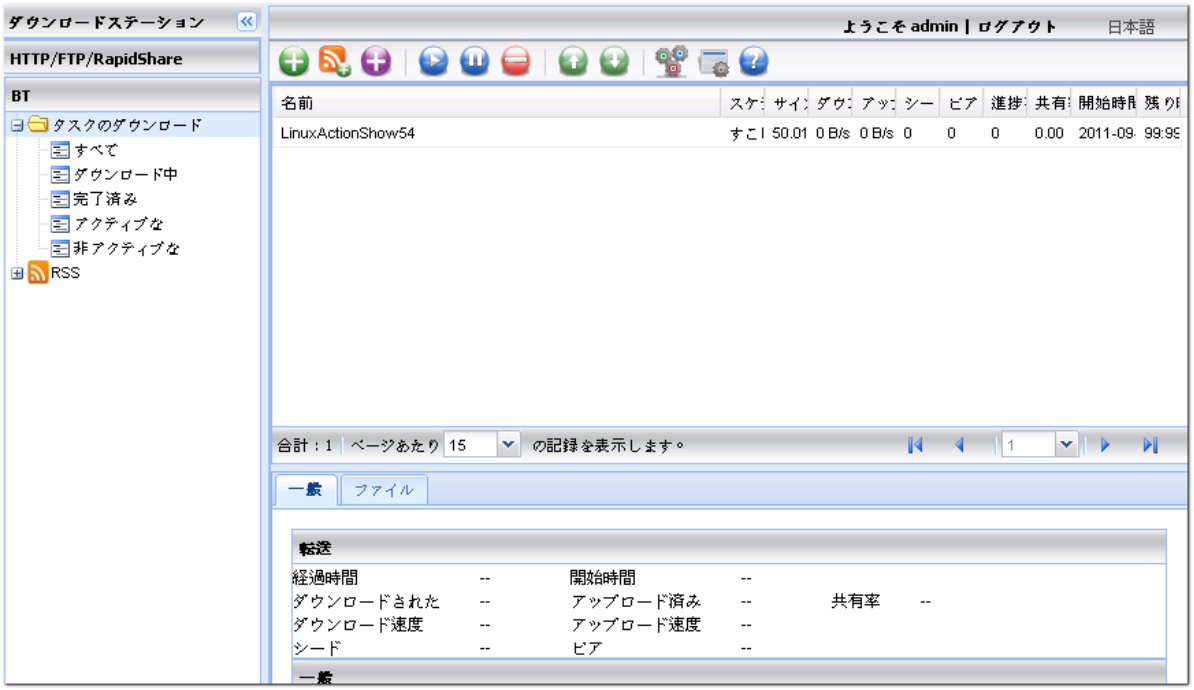


アカウントの設定を編集するには、リストのエントリを選択し「Edit Account（アカウントの編集）」をクリックします。 アカウントを削除するには、リストのエントリを選択し「Delete Account（アカウントの削除）」をクリックします。 「OK」をクリックして変更を全般、ディレクトリ、およびバンド幅に保存します。

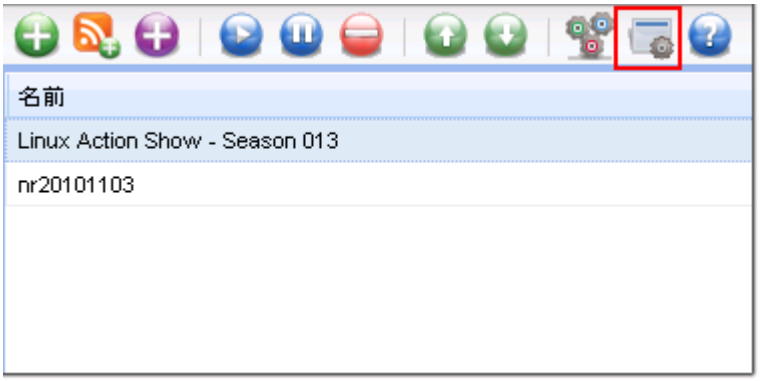


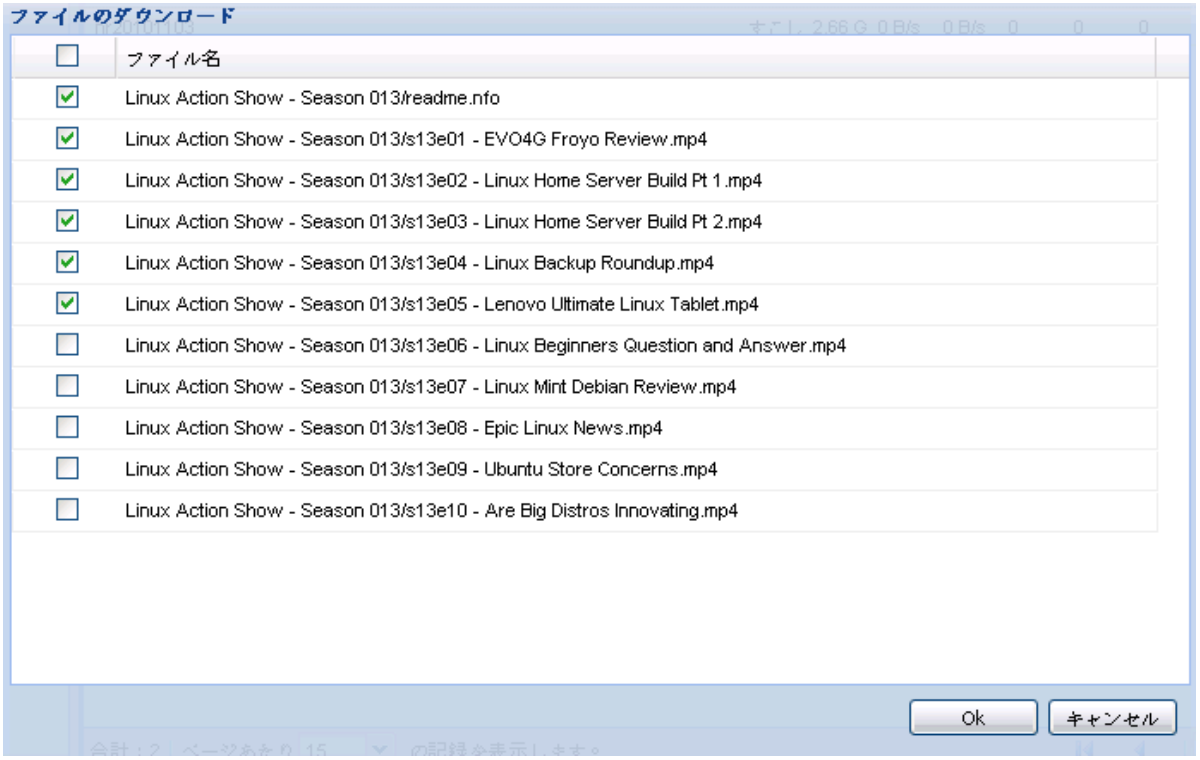
BTダウンロード

BTによってファイルをダウンロードするには、 をクリックします。 torrentファイルを閲覧して選択し、「OK」をクリックします。 ダウンロードタスクが示されます。 タスクの詳細とダウンロードステータスが表示されます。



torrentファイルからダウンロードする特定ファイルを選択できます。リストでBTダウンロードタスクを選択します。 をクリックして、ダウンロードするファイルを選択します。





ダウンロードしたタスクを表示し、タスクを右クリックしてタスクの開始、一時停止、優先順位付け、または削除を行うことができます。ダウンロードタスクとそのすべてのダウンロードされたデータを取り除くには、「Remove and Delete Data（データの除去と削除）」を選択します。

RSSフィード

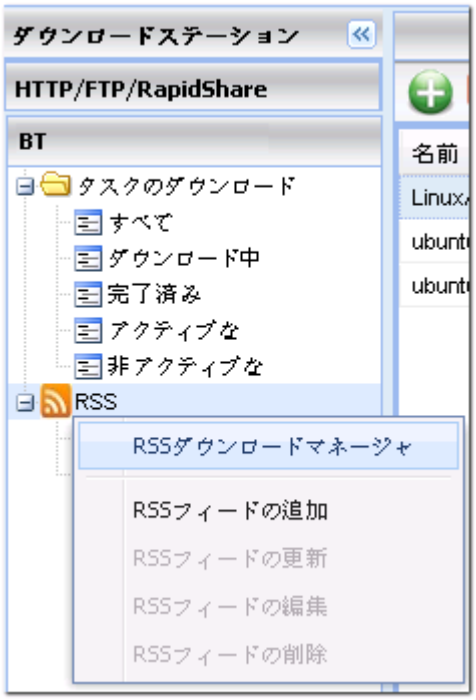
Download StationでRSSフィードを予約購読したり、フィードにtorrentファイルをダウンロードしたりできます。 をクリックしてRSSフィードを追加します。

URLとラベルを入力します。

RSSフィードからtorrentファイルをダウンロードするには、フィードを右クリックし「Download（ダウンロード）」を選択します。

NASはファイルのダウンロードを自動的に開始します。 BT Downloadにダウンロードステータスを表示できます。

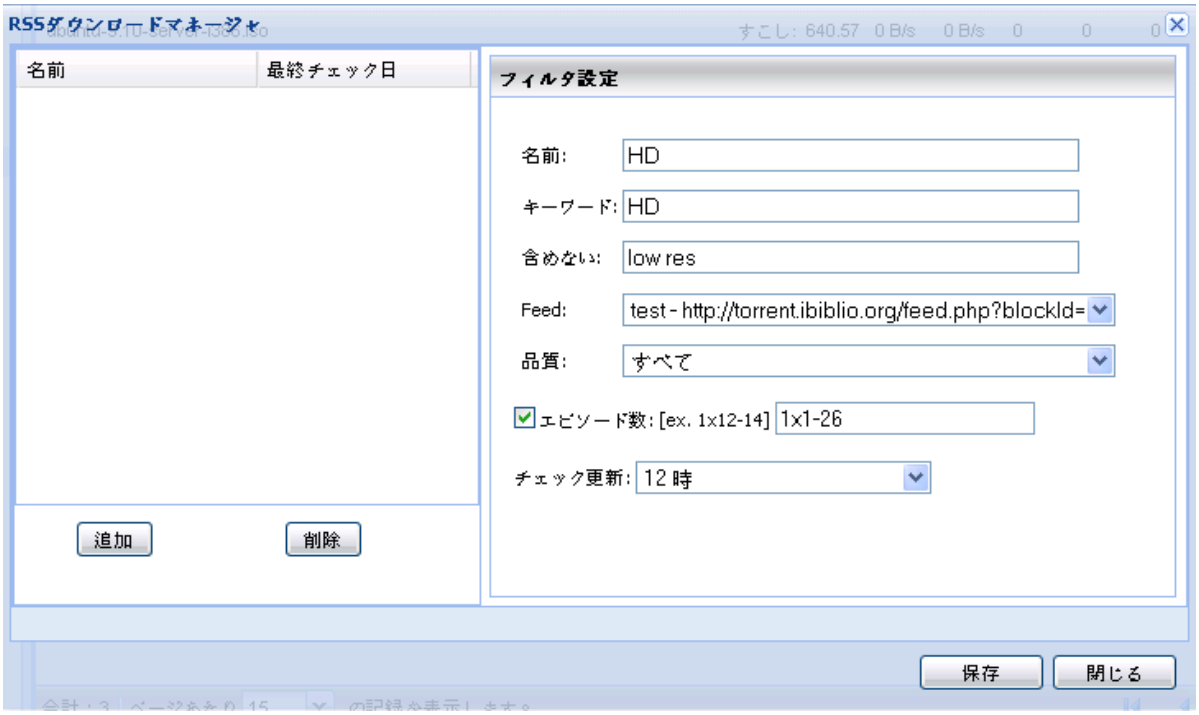
RSSフィード予約購読を管理するには、RSSフィードラベルを右クリックします。 RSS Download Managerを開き、RSSフィードを追加、更新、編集、削除することができます。



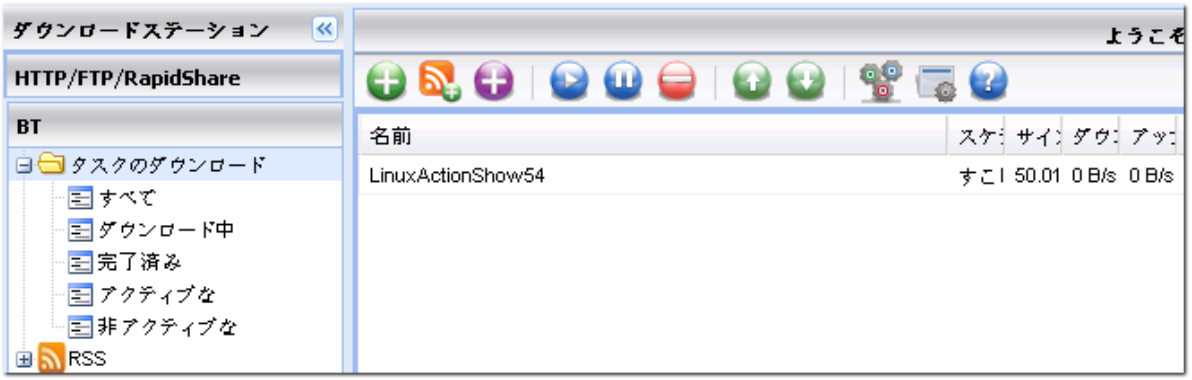
RSSダウンロードマネージャ

RSSダウンロードマネージャ を使用してフィルタを作成および管理し、BTダウンロードの特定のtorrentファイルをダウンロードすることができます。

1. フィルタを追加するには、「Add（追加）」をクリックします。
2. フィルタ名を入力し、含めたり除外したりするフィーワードを指定します。
3. フィルタ設定を適用するRSSフィードを選択します。
4. ビデオtorrentファイルの品質を指定することもできます（この機能が必要ない場合、またはtorrentファイルがビデオでない場合、ファイルの品質を「All（すべて）」のままにしておきます）。
5. エピソード番号： このオプションを選択して、ドラマ作品の特定エピソードまたは一連のエピソードを指定します。 例えば、TV番組のシーズン1のエピソード1～26をダウンロードするには、1x1-26と入力します。 シーズン1のエピソード1のみをダウンロードするには、1x1と入力します。
6. RSSフィードの自動更新の時間間隔を選択します。 NASはRSSフィードを更新し、フィルタに一致する新しいコンテンツが使用できるかどうかを確認します。
7. 「Save（保存）」をクリックしてフィルタを保存するか、「Close（閉じる）」をクリックしてキャンセルまたは終了します。
8. フィルタを削除するには、リストからフィルタを選択し「Delete（削除）」をクリックします。



左列の「BT」をクリックすることで、すべてのBTダウンロードタスクのステータスを表示できます。

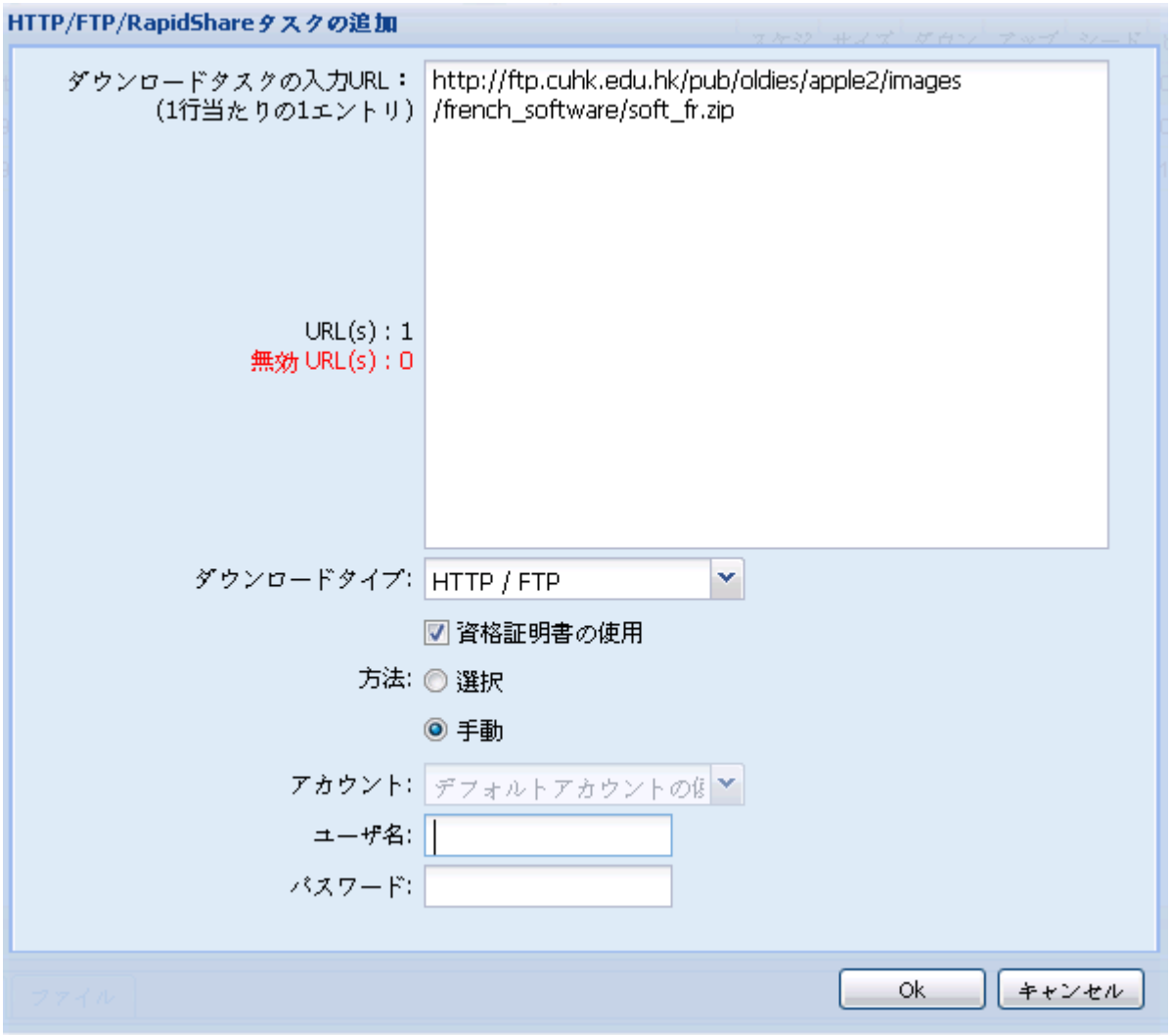


HTTP/FTP/RapidShareダウンロード

HTTP、FTP、またはRapidShareダウンロードを追加するには、 をクリックします。

ダウンロードタスクのURLを入力します（1行あたり1つのエントリ）。 次に、ダウンロードタイプ: HTTP/FTPまたはRapidShareを選択します。 ファイルへのアクセスにユーザー名とパスワードが要求される場合、「Use credentials（クリデンシャルの使用ｓ）」を選択し、事前設定されたアカウントを選択するか（Settings（設定）> HTTP/FTP/RapidShare > Account（アカウント））、ユーザー名とパスワードを入力します。 [OK]をクリックします。 NASはファイルを自動的にダウンロードします。

> 注: 一度に最大30のエントリしか入力できません。



左列の「HTTP/FTP/RapidShare」をクリックすることで、すべてのHTTP、FTP、またはRapidShareダウンロードタスクのステータスを表示できます。

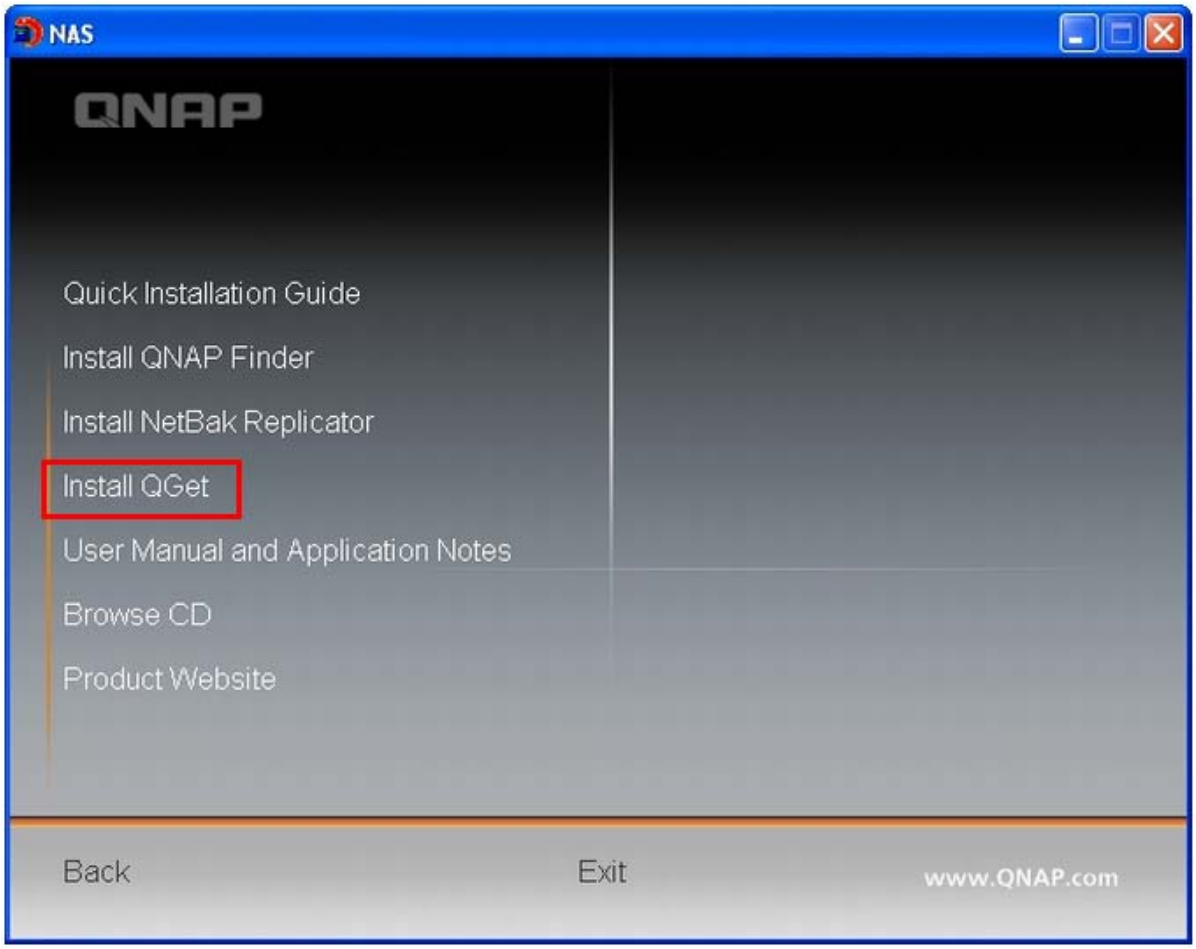
BTダウンロード速度が遅かったり、ダウンロードエラーが発生したりする一般的な理由は以下の通りです:

1. トレントファイルが期限切れか、ピアがこのファイルの共を停止したか、ファイルにエラーがあります。
2. NASは固定IPを使用するように設定していても、DNSサーバが設定されていないか、DNSサーバがダウンしています。
3. ダウンロード速度が最適になるよう同時ダウンロードの最大数が3-5に設定されています。
4. NASがNATルータの背後に配置されています。ポート設定により、BTのダウンロード速度が遅くなっているか、反応がありません。以下の手順に従って問題を解決できるかもしれません:
   - NATルータのBTポートの範囲を手動で開きます。それらのポートをNASのLAN IPにフォワードします。
   - NASの新しいファームウェアはUPnP NATポートのフォワーディングをサポートしています。NATルータがUPnPに対応している場合、NATのこの機能を効にします。その後、NASのUPnP NATポートのフォワーディングを効にします。BTのダウンロード速度は改善されるはずです。

ダウンロードソフトウェアQGetを使用する

QGetはLANまたはインターネット上で複数のNASサーバーでダウンロードタスクを管理するユーティリティです。複数のPCまたはMacにソフトウェアをインストールすることができます。ライセンスは必要ありません。 QGetはDownload Station v1およびv2と互換性があります。

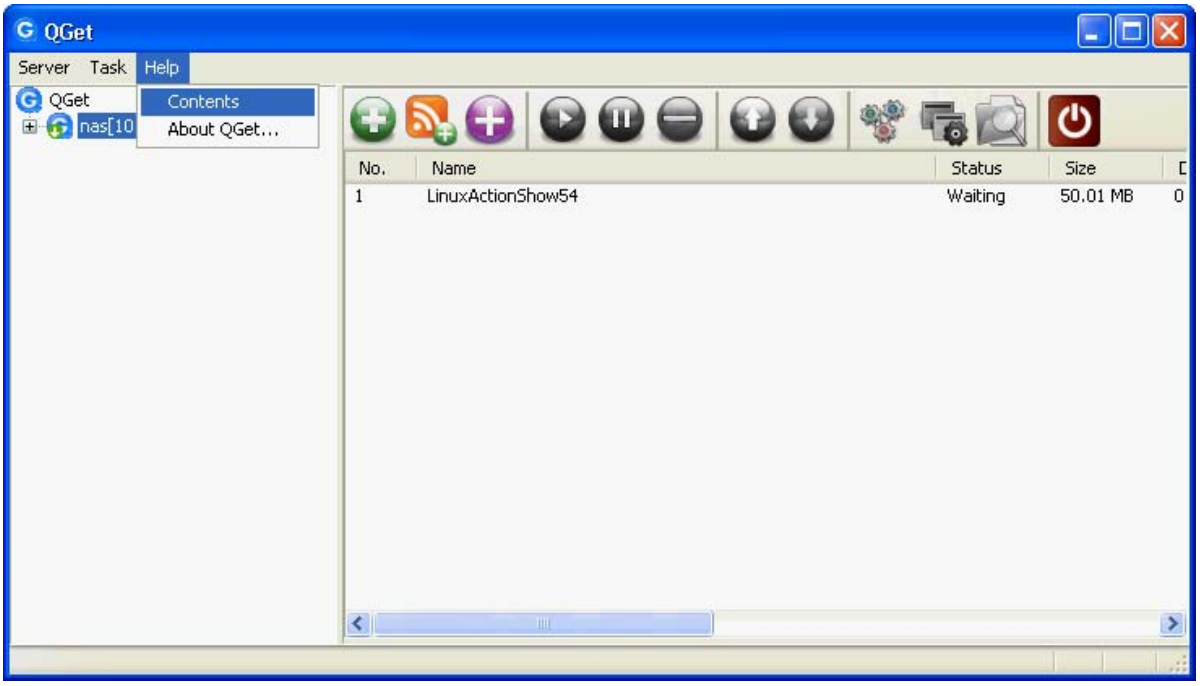
1. QGetを使用するには、製品CD-ROMから同ソフトウェアをインストールします。



2. 指示に従ってQGetをインストールします。

3. インストールした場所からQGetを実行します。

4. QGetを使用すれば、WebベースのDownload Stationを使用しているかのごとく、複数のNASサーバ上でダウンロードタスクを管理することができます。 QGetの概要とボタンの説明については、「Help（ヘルプ）」>「Contents（コンテンツ）」のオンラインヘルプを参照してください。



7.6 監視ステーション (Surveillance Station)

監視ステーションでは、ネットワーク (LAN または WAN) で最大 2-4 つのネットワークカメラを使って、ライブビデオを監視し記録することができます。NASモデルが一覧にない場合、http://www.qnap.com にアクセスして詳細をご確認ください。

最大数のIPカメラをサポート	NASモデル
2	TS-110, TS-210, TS-112, TS-119, TS-119P+, TS-210, TS-212, TS-219P+, TS-239 Pro II+, TS-259 Pro+
4	TS-410, TS-412, TS-419P+, TS-410U, TS-419U, TS-412U, TS-419U+, SS-439 Pro, SS-839 Pro, TS-439 Pro II+, TS-459U-RP/SP, TS-459U-RP+/SP+, TS-459 Pro+, TS-459 Pro II, TS-559 Pro+, TS-559 Pro II, TS-659 Pro+, TS-659 Pro II, TS-859 Pro+, TS-859U-RP, TS-859U-RP+, TS-809 Pro, TS-809U-RP, TS-879 Pro, TS-1079 Pro, TS-879U-RP, TS-EC879U-RP, TS-1279U-RP, TS-EC1279U-RP

注:TS-x39/509/809シリーズにてこの機能を使用するには製品CDに含まれている画像ファイルを使用してシステムファームウェアを更新するか、あるいは最新システムファームウェアをダウンロードしてください。

ページ上部あるいはNASログインページの"Surveillance Station"をクリックし、監視ステーションにアクセスします。NASログインページからサービスにログインする場合、ユーザー名およびパスワードを入力する必要があります。

> 注:監視ステーションは、IE ブラウザ 6.0 以降でのみサポートされます。

NAS によるネットワーク監視システムをセットアップするには、以下のステップに従います。

1. ホームネットワーク接続状態を計画します
2. IP カメラをセットアップします
3. NAS でカメラを設定します
4. NAT ルータを設定します (インターネット上でのリモート監視用)

ホームネットワーク接続状態を計画します

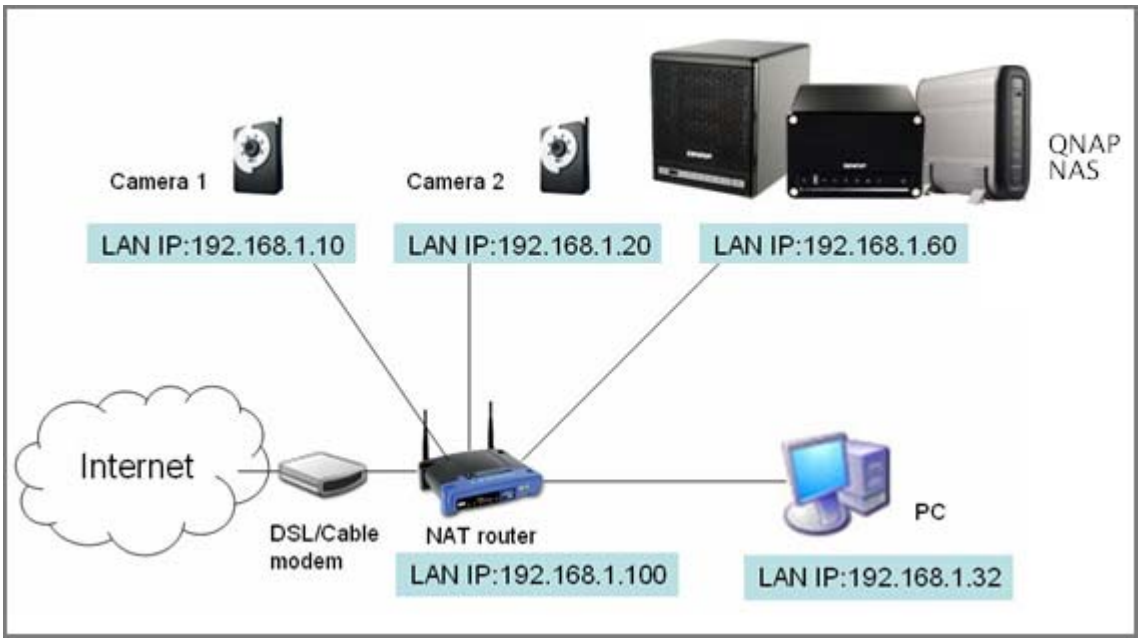
監視システムのセットアップを開始する前に、ホームネットワークの計画を書き留めます。その際、以下の点を考慮してください。

i. NAS の IP アドレス
ii. カメラの IP アドレス

この例では、2 つの IP カメラがインストールされています。

コンピュータ、NAS、IP カメラは LAN の同じルータにインストールする必要があります。固定 IP アドレスを NAS と IP カメラに割り当てます。例:

- ホームルータの LAN IP: 192.168.1.100
- カメラ 1 IP: 192.168.1.10 (固定 IP)
- カメラ 2 IP: 192.168.1.20 (固定 IP)
- NAS IP: 192.168.1.20 (固定 IP)



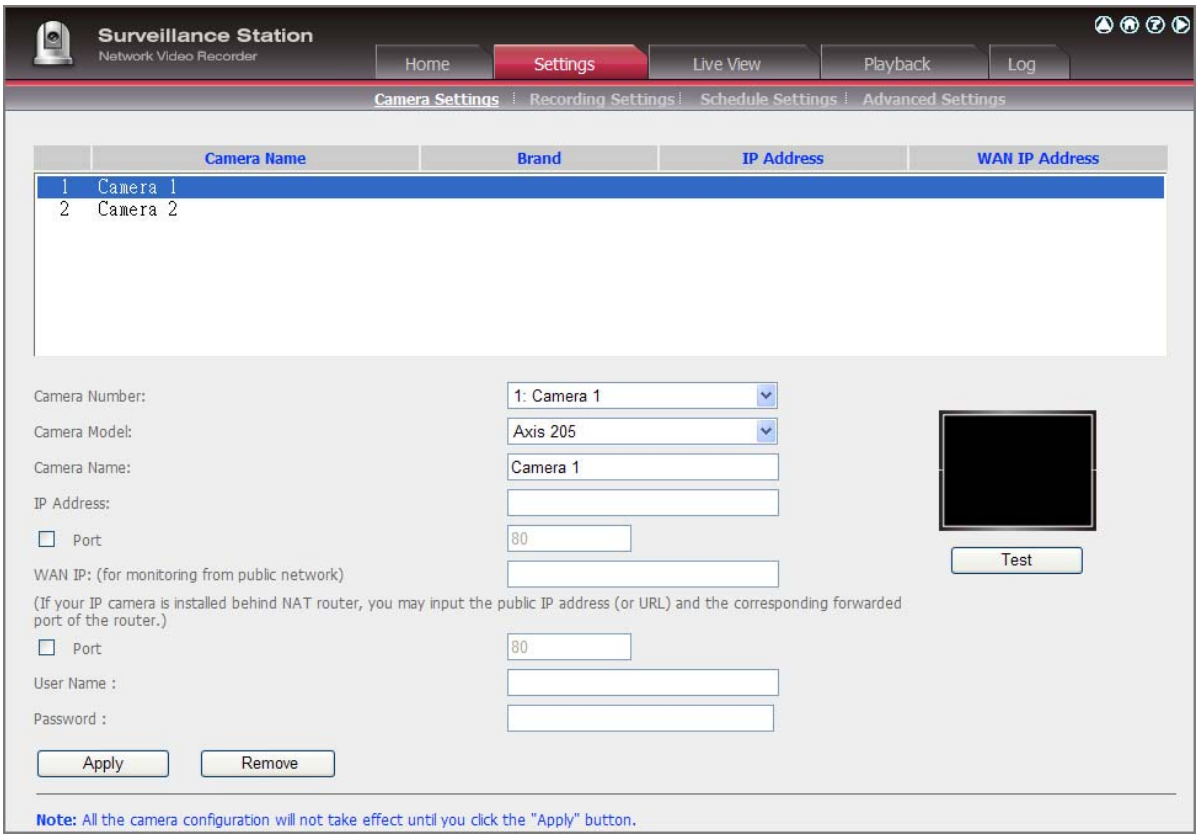
IP カメラをセットアップします

IP カメラをホームネットワークに接続します。次に、カメラがコンピュータと同じ LAN に入るようにカメラの IP アドレスを設定します。IE ブラウザによるカメラ 1 の設定ページにログインします。最初のカメラの IP アドレスを 192.168.1.10 と入力します。デフォルトのゲートウェイはルータの LAN IP として設定する必要があります (この例では、192.168.1.100)。2 台目のカメラの IP アドレスを 192.168.1.20 と設定します。
カメラによっては、IP 設定に対してユーティリティを提供するものもあります。詳細については、カメラのユーザーマニュアルを参照してください。

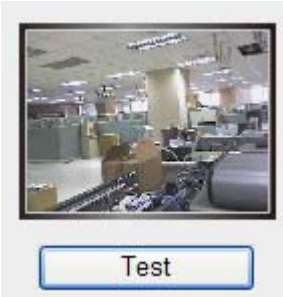
サポートされるネットワークカメラリストについては、http://www.qnap.com を参照してください。

NAS でカメラを設定します

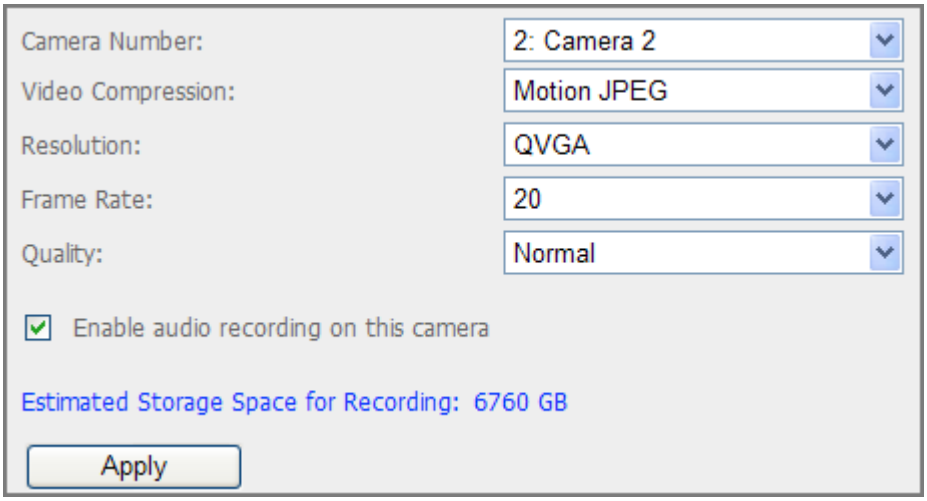
IE ブラウザにより監視ステーションにログインして IP カメラを設定します。「設定>カメラ設定」ページに進みます。カメラ情報 (名前、モデル、IP アドレスなど) を入力します。



右の「接続テスト」をクリックして、IP カメラへの接続が正常に行われていることを確認します。



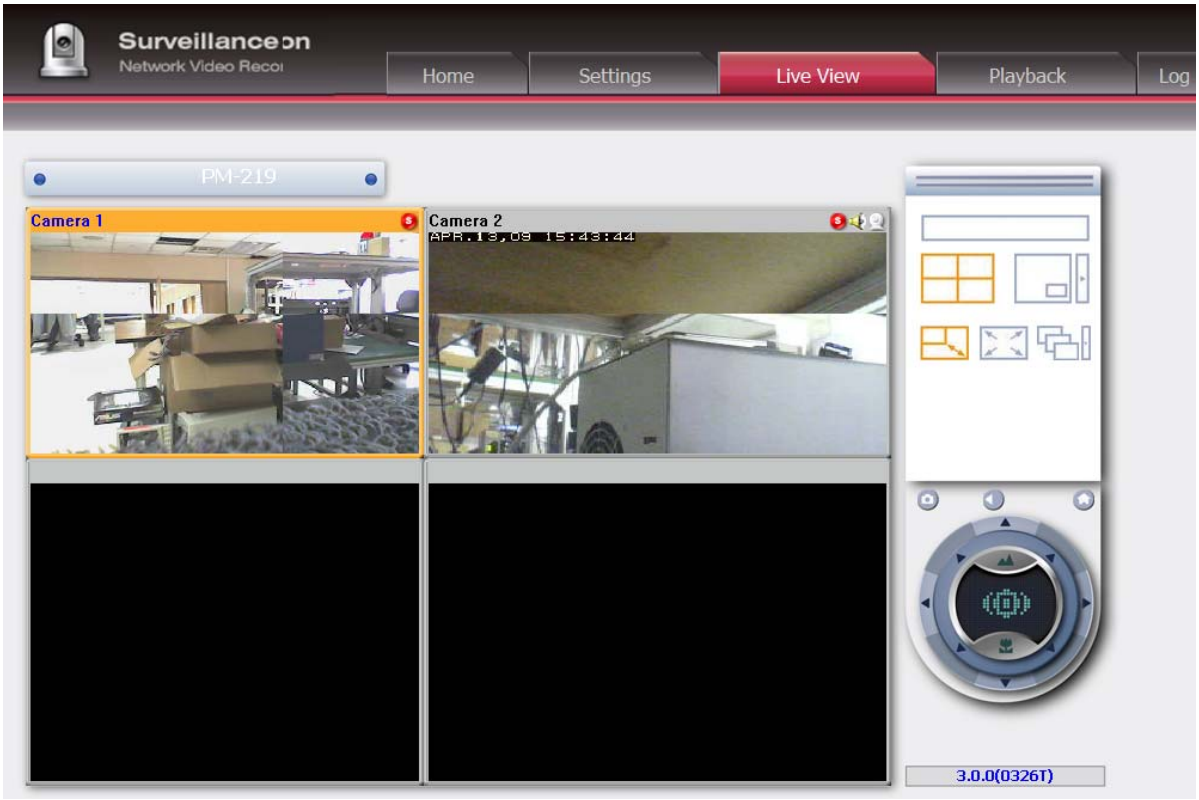
カメラで音声録音がサポートされている場合、「記録設定」ページでオプションを効にすることができます。「適用」をクリックして更を保存します。



上のステップに従ってカメラ 2 の設定を行います。

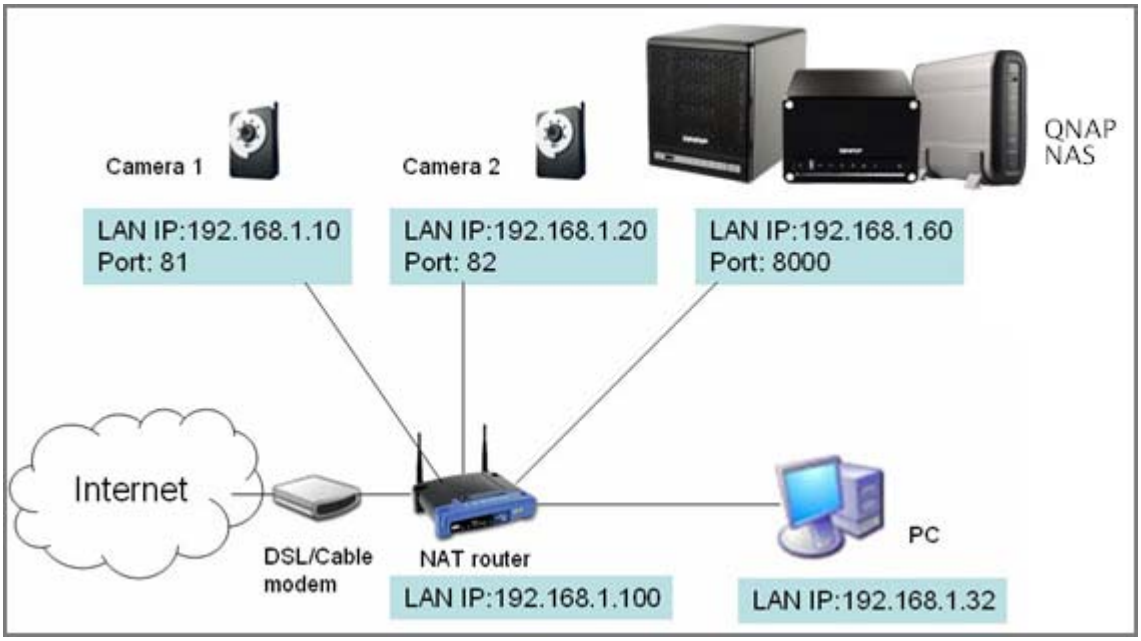
ネットワークカメラを NAS に追加した後、「ライブビュー」ページに進みます。IE ブラウザによりこのページに初めてアクセスするとき、カメラ 1 とカメラ 2 の画像を表示するには、ActiveX コントロールをインストールする必要があります。監視ステーションの監視および記録機能を使用できるようになります。

モーション検出記録、スケジュール記録、ビデオ再生など、監視ステーションのその他の機能を使用するには、オンラインヘルプを参照してください。



NAT ルータを設定します (インターネット上でのリモート監視用)

監視ビデオを表示し NAS にリモートでアクセスするには、NAT ルータの対応する LAN IP に異なるポートを転送することで、ネットワーク設定を更する必要があります。



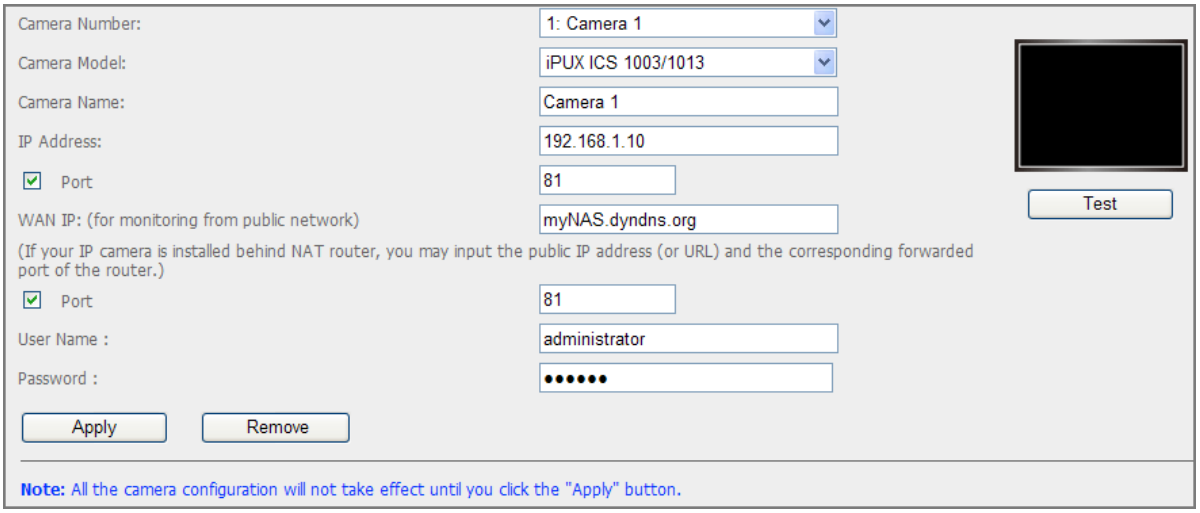
NAS および IP カメラのポート設定を更する

NAS のデフォルトの HTTP ポートは 8080 です。この例で、ポートは 8000 に更されます。従って、設定を適用した後、**http://NAS IP:8000** を通して NAS にアクセスする必要があります。

次に、IP カメラのネットワーク設定ページにログインします。カメラ 1 の HTTP ポートを 80 から 81 に更します。カメラ 2 のポートを 80 から 82 に更します。

次に、監視ステーションにログインします。「設定>カメラ設定」に進みます。カメラ 1 とカメラ 2 のポート番号をそれぞれ 192.168.1.10 **port 81** とおよび 192.168.1.20 **port 82** として入力します。両方のカメラに対してログイン名とパスワードを入力します。

また、WAN IP アドレス (または、パブリックネットワークのドメインアドレス。MyNAS.dyndns.org など) とインターネットから接続用の WAN サイドのポートを入力します。設定の終了後、「Test」をクリックして、カメラへの接続が正常に行われていることを確認します。



ルータの設定ページに移動し、以下のようにポート転送を設定します。

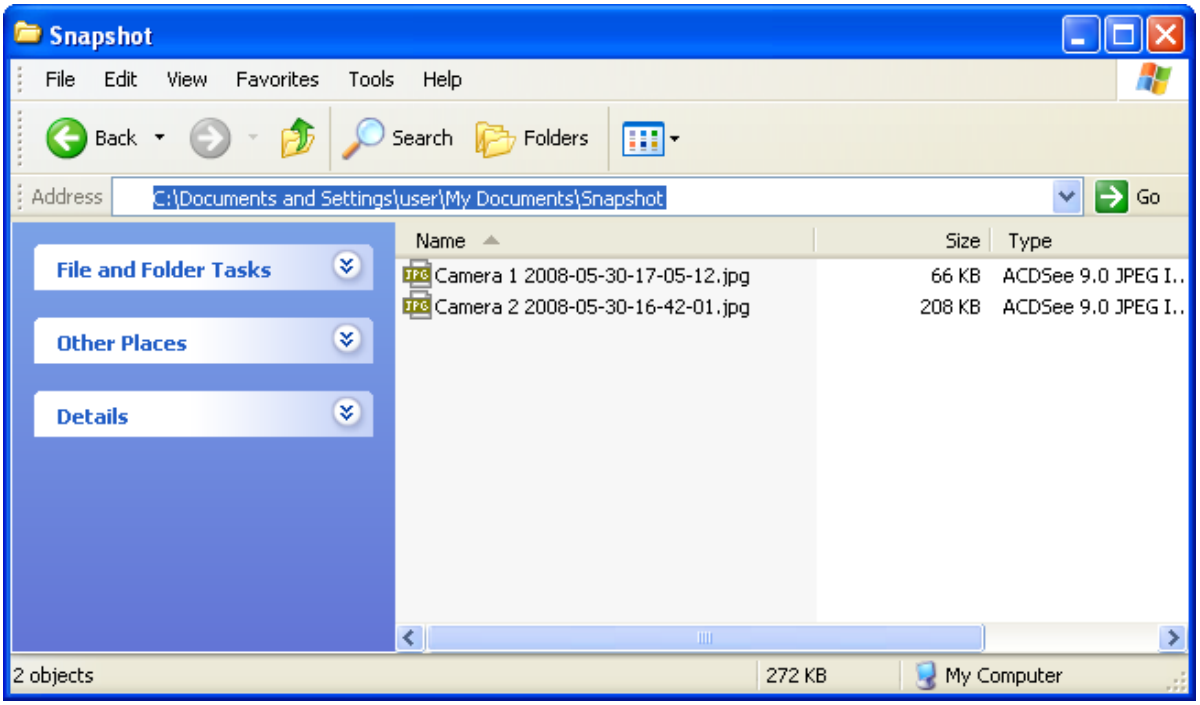
- 転送ポート 8000 対 NAS LAN IP: 192.168.1.60
- 転送ポート 81 対カメラ 1 の LAN IP: 192.168.1.10
- 転送ポート 82 対カメラ 2 の LAN IP: 192.168.1.20

> 注:ポート設定を更するとき、リモートアクセスが許可されていることを確認します。たとえば、オフィスのネットワークがポート 8000 をブロックする場合、オフィスから NAS にアクセスすることはできません。

ポート転送とルータ設定を設定した後、インターネット上で監視ステーションを使ってリモート監視を開始できます。

監視ステーションのスナップショットとビデオ記録にアクセスする

すべてのスナップショットは、ご使用のコンピュータの "My Documents" (マイドキュメント) > "Snapshot" (スナップショット) (Windows XP) に保存されます。Windows 7 あるいは Vistaをご使用の場合は、デフォルトのディレクトリは "Documents" (ドキュメント) > "Snapshot" (スナップショット)です。

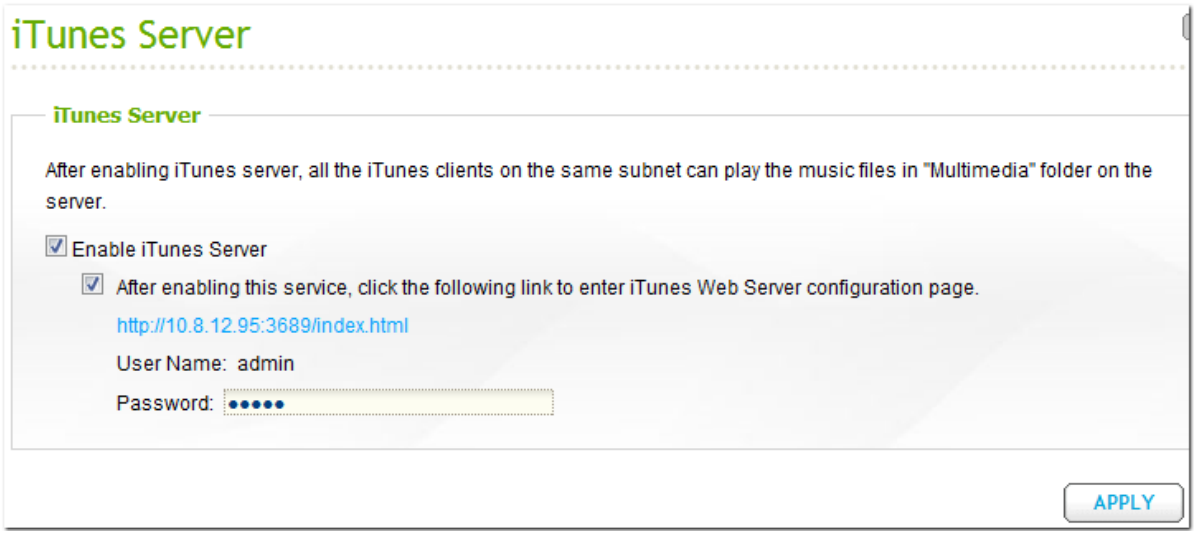


ビデオ録画は \\NASIP\Qrecordings あるいは \\NASIP\Recordings に保存されます。通常の記録はフォルダ「record_nvr」に保存され、アラーム記録はネットワーク共のフォルダ「record_nvr_alarm」に保存されます。

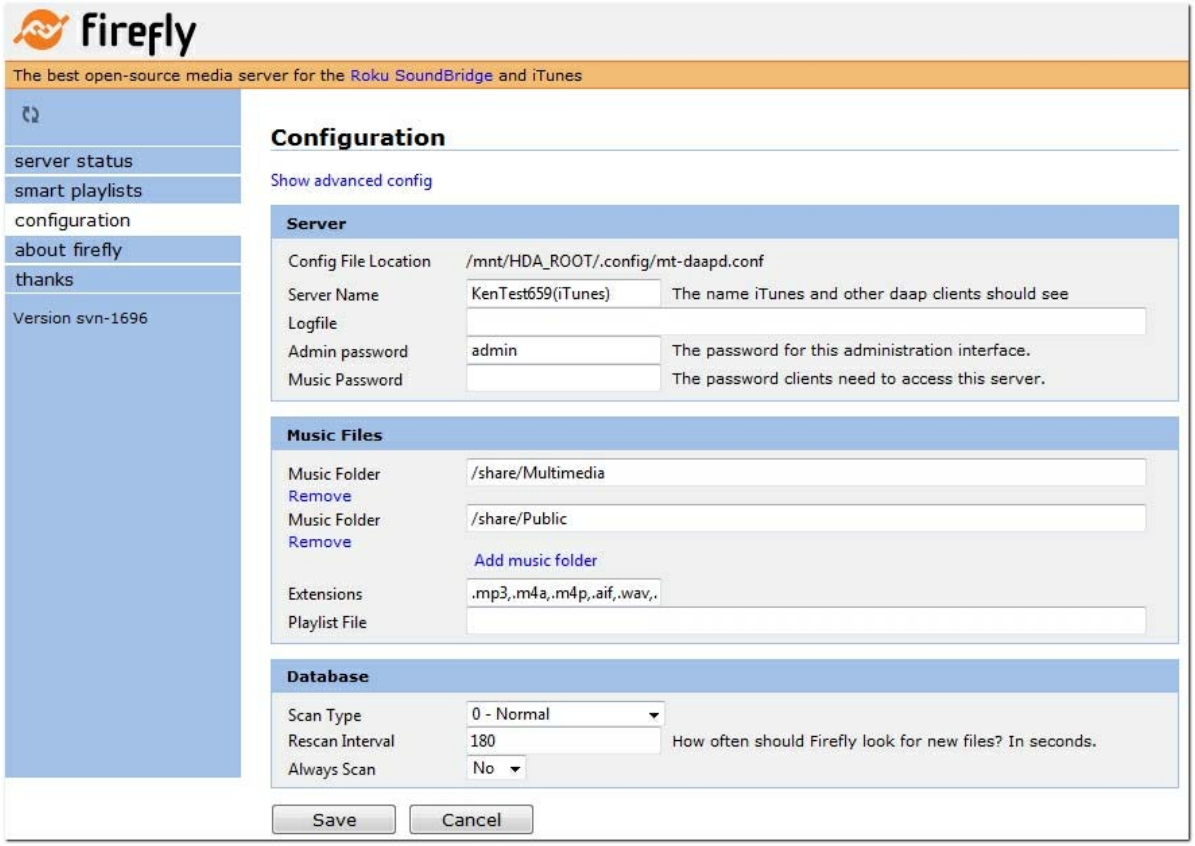
7.7 iTunes サービス

NASのQmultimedia/ Multimediaフォルダのmp3ファイルは、このサービスを効にすることによってiTunesと共できます。iTunesがインストールされているLAN上のすべてのコンピュータから、NASの音楽ファイルの検出、参照、再生が可能となります。

iTunes サーバーを使用するには、お使いのコンピュータ上に iTunes（http://www.apple.com/itunes/ ）をインストールします。この機能を有効にし、NAS の Qmultimedia/Multimedia フォルダに音楽ファイルをアップロードします。



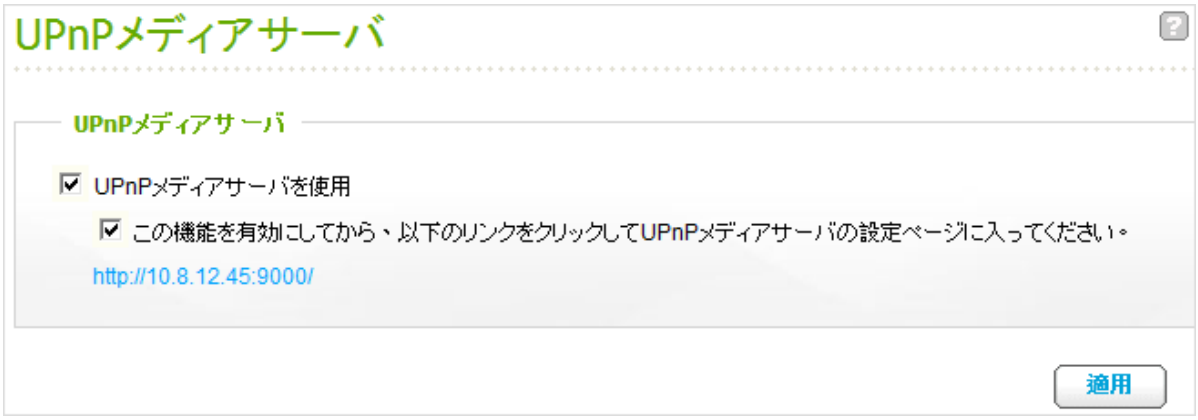
iTunes サーバーを設定し、スマートプレイリストを追加するには、iTunes サーバーのウェブページにログインします：
http://NAS-IP:3689/index.html



PC および NAS を同一 LAN 上に接続し、PC 上の iTunes を起動します。「SHARED（共有中）」の下で NAS 名を探し、音楽ファイルまたはプレイリストの再生を開始します。

7.8 UPnPメディアサーバ

UPnPメディアサーバを使用するには、この機能を効にしてから、以下のリンク (http://NAS IP:9000/をクリックして、UPnPメディアサーバのページに入ってください。



http://NAS IP:9000/のリンクをクリックし。"TwonkyMedia Settings" (TwonkyMedia設定) > "Basic Setup" (基本セットアップ)に移動し、基本サーバ設定を構成します。

デフォルトではNASのQmultimedia (Qマルチメディア) あるいはMultimedia (マルチメディア) フォルダのコンテンツはデジタルメディアプレーヤーに共されます。"Basic Setup" (基本セットアップ) > "Sharing" (共) > "Content Locations" (コンテンツの場所) に移動し、共フォルダの更、または共フォルダを追加することができます。

設定の構成後、mp3、写真、ビデオファイルをNAS上の特定の共フォルダにアップロードすることができます。

> 注：マルチメディアファイルをデフォルトの共フォルダにアップロードしても、ファイルがメディアプレーヤーに表示されない場合は、メディアプレーヤーの設定ページの「コンテンツディレクトリの再スキャン」または「サーバの再起動」をクリックできます。

この機能に関する情報は、詳細はこちらをご覧ください 668。

UPnPについて

ユニバーサルプラグアンドプレイ (UPnP) はUPnPフォーラムが普及を進めているコンピュータネットワークプロトコルのセットです。UPnPの目的はデバイスのシームレスな接続を可能にし、ホームおよび企業環境でのネットワークの実装を簡略化することです。UPnPはオープンなインターネットベースの通信規格上に構築されたUPnPデバイスのコントロールプロトコルを定義および公開することによりこれを達成しています。

UPnPという用語は、デバイスをコンピュータに直接ダイナミックに接続するテクノロジーであるPlug-and-Playから来ています。

7.9 MySQLサーバ

注：TS-x39/509/809シリーズにてこの機能を使用するには製品CDに含まれている画像ファイルを使用してシステムファームウェアを更新するか、あるいは最新システムファームウェアをダウンロードしてください。

MySQLサーバをウェブサイトデータベースとして効にすることができます。

TCP/IPネットワークを効にします

リモート接続を効にし、他のウェブプロブラムがインターネット経由でこのサーバのMySQLサーバにアクセスし、データベースサーバとして使うことができるようになります。無効にすると、ローカルウェブプログラムからの接続のみが許可されます。

リモート接続を効にした場合、MySQLサーバのリモート接続サービスに1つのポートを割り当ててください。デフォルトポートは3306です。
NASをはじめてインストールした後、phpMyAdminというフォルダがQweb/ Webネットワークフォルダに作成されます。Webブラウザにhttp://NAS IP/phpMyAdmin/を入力してphpMyAdminページに入りMySQLデータベースを管理できます。

注:

- phpMyAdminフォルダは削除しないでください。このフォルダの名前を変更することはできますが、MySQLサーバーページは更新されません。名前を変更したフォルダにアクセスするには、Webブラウザのhttp://NAS IP/renamedフォルダのリンクに入ります。
- はじめてインストールした後に、phpMyAdminフォルダが作成されます。ファームウェアを更新しても、フォルダは変更されません。

データベースメンテナンス

- ロートパスワードをリセットします:MySQLルートのパスワードは、この機能実行後、 "admin" にリセットされます。
- データベースを初期化します:この機能実行後、MySQL データベースのすべてのデータは消去されます。

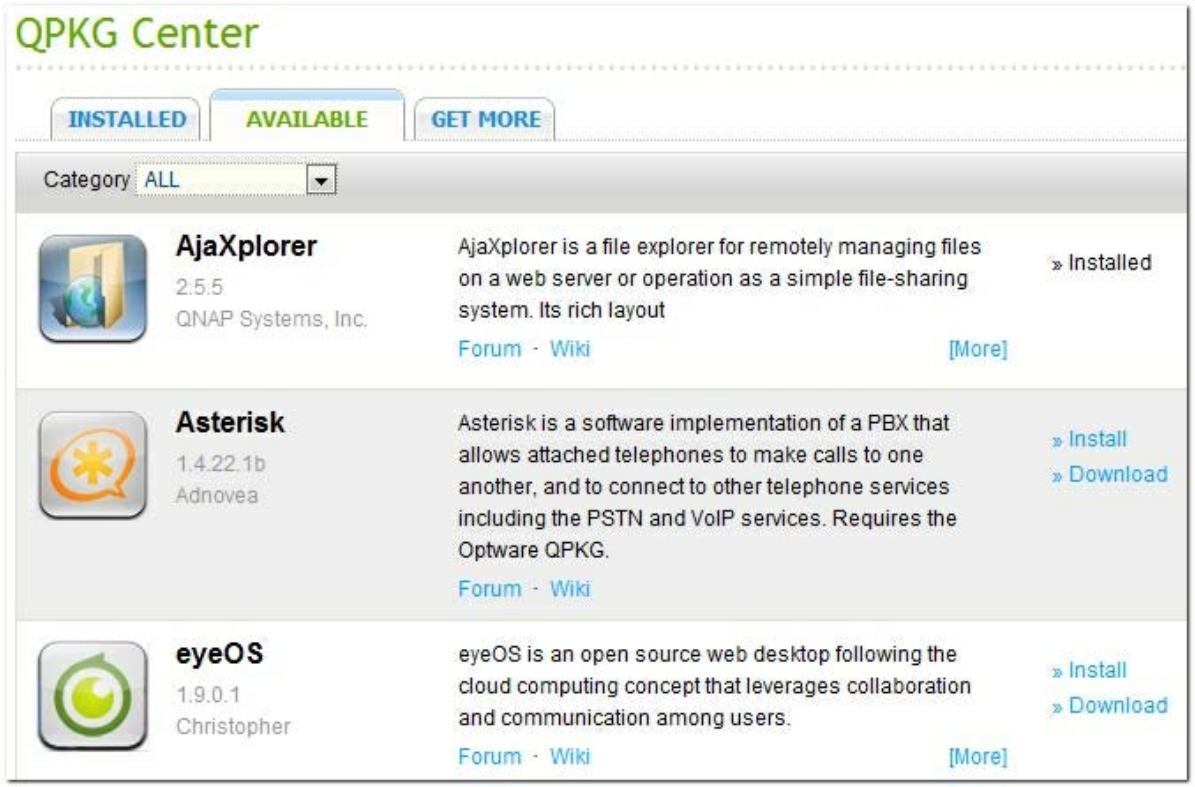
この機能に関する情報は、詳細はこちらをご覧ください 677。

7.10 QPKG Center

QPKG センターとは、NAS 上にサードパーティ製アドオンソフトウェアをインストールするための管理プラットホームです。「QPKG Center（QPKG センター）」>「Available（利用可能）」に移動して、アドオンを参照します。「Install（インストール）」をクリックして、それらをインストールします。

注：

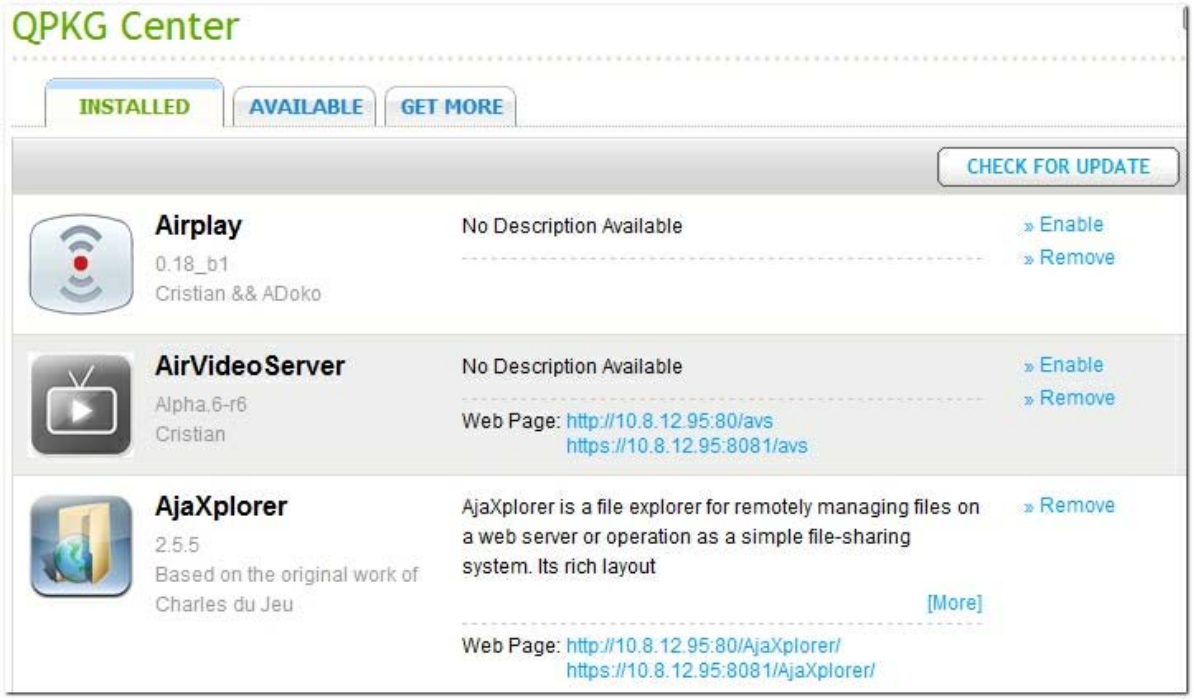
- NAS がインターネットに接続されていることを確認します。
- QNAP 社は、オープンソースソフトウェア/アドオンにより引き起こされる問題のトラブル対応の責任を負いません。ユーザーが、問題解決のために QNAP コミュニティフォーラムのディスカッションに参加するか、オープンソースソフトウェアの元の開発者に連絡することを推奨します。



選択済のアドオンとインストールの進行状況が表示されます。

注：前提条件となる QPKG を必要とする QPKG アドオンをインストールする場合、前提条件となるアドオンは依存するアドオンの前に自動的にインストールキューに追加されます。

「Installed（インストール済）」タブに移動し、インストール済アドオンの参照、有効化、無効化、または削除を行います。「Check for update（更新の確認）」をクリックして、アドオンの利用可能な更新バージョンをチェックします。 利用可能な場合、ダウンロードリンクをクリックして、更新をインストールします。



オフラインでのインストール

NAS がオフライン時に QPKG アドオンをインストールする場合、または、QNAP 社の QPKG サーバーで正式に利用可能でなベータ版のアドオンをインストールする場合、ユーザーは、QPKG ファイルを QNAP 社ウェブサイト（http://www.qnap.com/QPKG.asp ）またはフォーラム（http://forum.qnap.com/ ）からをダウンロードし、ファイルを解凍して、「QPKG Center（QPKG センター）」>「Get More（追加）」でアドオンを手動でインストールします。

7.11 Syslogサーバ

サーバ設定

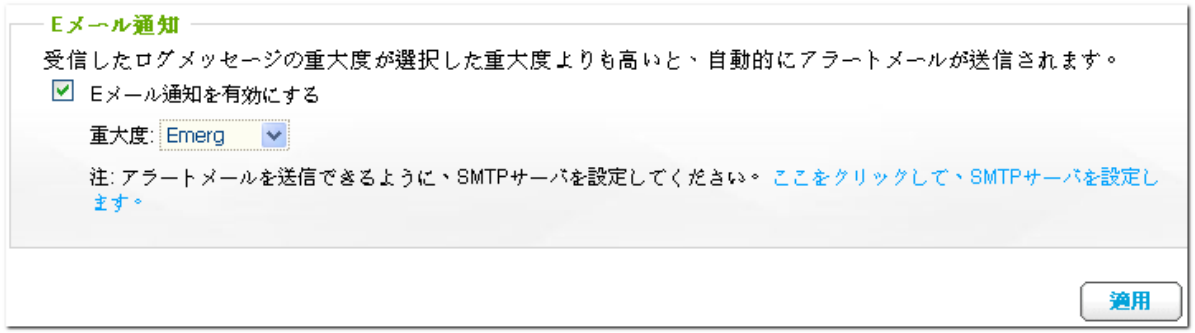
NAS をシステムログサーバーとして設定し、クライアントからシステムログメッセージを受信するには、システムログサーバーを有効にします。NAS がシステムログメッセージを受信するために使用するプロトコル（TCP/UDP）を選択します。必要に応じてポート番号を指定するか、デフォルトポート番号 514 を使用します。「Apply（適用）」をクリックして、設定を保存します。NAS をシステムログサーバーとして有効にした後、システムログクライアント上のシステムログサーバー IP アドレスに NAS の IP アドレスを入力して、クライアントからシステムログメッセージを受信できるようにします。

ログ設定：
システムログメッセージの最大ログサイズ（1 ～ 100MB）、ログを保存するロケーション（NAS ネットワーク共有）、およびファイル名を指定します。ログが最大サイズに達すると、ログは自動的にアーカイブされ、名称が MyLogFile_yyyy-mm-dd に変更されます（例 MyLogFile_2011-12-31）。複数ログファイルが同じ日にアーカイブされる場合、ファイル名は MyLogFile_yyyy_mm_dd.[番号] になります。例えば、MyLogFile_2011_12_31.1、MyLogFile_2011_12_31.2 などです。「Apply（適用）」をクリックして、設定を保存します。

E メール通知：

NASは、受信したシステムログメッセージの重大度が指定されたレベルと一致するとき、専用の E メールアドレス（「System Administration（システム管理）」>「Notification（通知）」>「Alert Notification（アラート通知）」で設定された最大 2 件）への電子メール警告の送信をサポートしています。この機能を利用するには、「System Administration（システム管理）」>「Notification（通知）」>「Configure SMTP Server（SMTP サーバーの設定）」で、SMTP サーバーの設定を行います。次に、E メール通知を有効にし、「Application Servers（アプリケーション）」>「Syslog Server（Syslogサーバ）」>「Server Settings（サーバ設定）」で、重大度のレベルを選択します。「Apply（適用）」をクリックして、設定を保存します。

重大度	レベル（最小の数字が最高の重大度を表します）	説明
Emerg	0	緊急：システムは利用不能です。 レベル 0 ～ 4 のシステムログメッセージを受信した時に、警告 E メールを送信します。
Alert	1	警告：直ちにアクションが必要です。 レベル 1 ～ 4 のシステムログメッセージを受信した時に、警告 E メールを送信します。
Crit	2	危険：危険な状態です。 レベル 2 ～ 4 のシステムログメッセージを受信した時に、警告 E メールを送信します。
Err	3	エラー：エラー状態です。 レベル 3 ～ 4 のシステムログメッセージを受信した時に、警告 E メールを送信します。
Warning	4	注意：注意が必要な状態です。 レベル 4 のシステムログメッセージを受信した時に、警告 E メールを送信します。



フィルタ設定

この機能は、システムログのフィルタに慣れたシステム管理者のみが操作するようにします。

次のステップに従い、条件に一致するシステムログメッセージを受信するように NAS のシステムログフィルタを作成します。

1. 「Add a New Filter（新規フィルタの追加）」をクリックします。

2. フィルタ設定を定義し、「Add（追加）」をクリックします。フィルタを手動で編集/追加するには、「Manual Edit（手動編集）」をクリックし、ダイアログで内容を変更します。「Apply（適用）」をクリックして、フィルタを保存します。

3. フィルタがリスト上に表示されます。NAS は、使用するフィルタに一致するシステムログメッセージのみを受信します。

ボタン	説明
	フィルタを有効にします
	フィルタを無効にします
	フィルタ設定を編集します
削除	1 つ以上のフィルタを削除します

Syslogビューア

ウェブベースのシステムログビュワーを使って、NAS 上で利用可能なシステムログメッセージを閲覧します。最新のログを閲覧するか、または、特定のアーカイブされたファイル内のログを閲覧するかを選択します。「Syslog Server（Syslogサーバ）」>「Server Settings（サーバ設定）」>「Log Settings（ログ設定）」で、設定したディレクトリ上のログファイルに直接アクセスします。

日付	時刻	ファシリティ	重大度	ホスト名	アプリケーション	P.ID	M.ID	メッセージ
2011-09-08	14:12:30 +08:00	auth	Info	nas	qlogd	5853	-	qlogd[5853]: conn log: Users: admin, Source IP: 10.8.13.134, Computer name: ---, Connection type: HTTP, Accessed resources: Administration, Action: Login OK
2011-09-08	14:11:48 +08:00	daemon	Info	nas	qlogd	5853	-	qlogd[5853]: event log: Users: admin, Source IP: 10.8.13.134, Computer name: ---, Content: [Syslog Server] Filter deleted.
2011-09-08	14:11:44 +08:00	daemon	Info	nas	qlogd	5853	-	qlogd[5853]: event log: Users: admin, Source IP: 10.8.13.134, Computer name: ---, Content: [Syslog Server] Filter deleted.

7.12 RADIUS サーバ

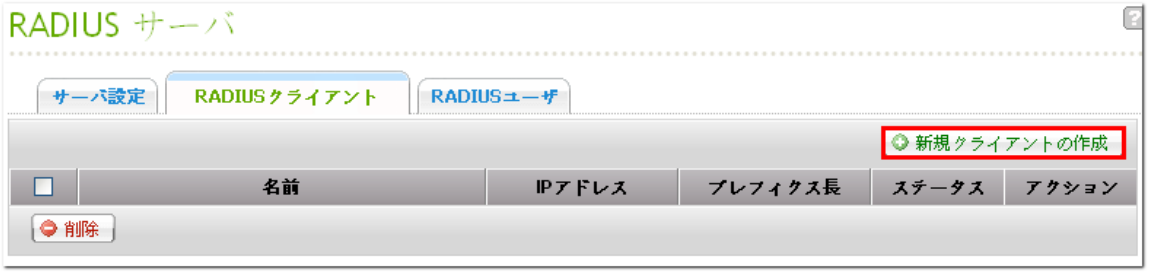
NAS を、RADIUS（Remote Authentication Dial In User Service：ユーザーサービスにおけるリモート認証ダイヤル）サーバーとして設定し、ネットワークサービスに接続/使用するコンピュータに対する集中化認証および認証管理機能を提供します。

この機能を利用するには、以下のステップに従います：

1. 「RADIUS Server（RADIUS サーバー）」>「Server Settings（サーバ設定）」で、NAS 上の RADIUS サーバーを有効化します。「Apply（適用）」をクリックします。

2. 「RADIUS Server（RADIUS サーバ）」>「RADIUS Clients（RADIUS クライアント）」で、NAS 上に、Wi-Fi アクセスポイントおよび VPN などの RADIUS クライアントを追加します。最大 10 の RADIUS クライアントをサポートします。

   a. 「Create a New Client（新規クライアントの作成）」をクリックします。



b. クライアントの情報を入力し、「Apply（適用）」をクリックします。

c. クライアントがリスト上に表示されます。

3. 「RADIUS Server（RADIUS サーバ）」>「RADIUS Users（RADIUS ユーザ）」で、RADIUS ユーザーおよびパスワードを作成します。ユーザーは、RADIUS クライアントを通して、ネットワークにアクセスしようとする時に認証されます。NAS がサポートする RADIUS ユーザーの最大数は、サポートされる最大ローカル NAS ユーザーと同じです。詳細は、http://docs.qnap.com/nas/en/index.html?users.htm を参照してください。

   a. 「Create a New User（新規ユーザの作成）」をクリックします。

   b. ユーザー名およびパスワードを入力します。ユーザー名は、アルファベット（a ～ z および A ～ Z）と数字（0 ～ 9）のみが利用可能です。パスワードは、8 ～ 32 文字でなければなりません（a ～ z、A ～ Z、および 0 ～ 9 のみ）。「Apply（適用）」をクリックします。

4. ダイアルアクセス権を付与するローカル NAS ユーザーを指定します。このオプションを有効にして、ローカル NAS ユーザーが、NAS へのログイン名とパスワードを使用して RADIUS クライアントを通し、ネットワークサービスにアクセスできるようにします。「Apply（適用）」をクリックします。

注：RADIUS サーバーは、ローカル NAS ユーザーの認証に、PAP、EAP-TLS/PAP、および EAP-TTLS/PAP のみをサポートします。

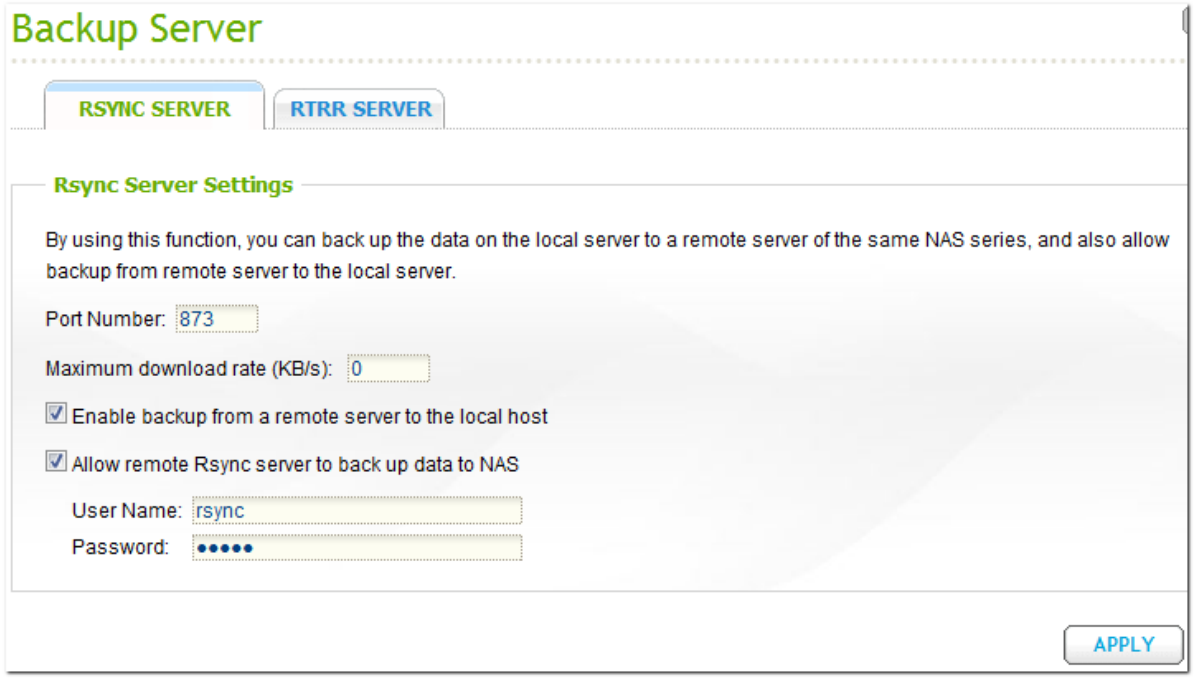
7.13 バックアップサーバー

再同期サーバー

再同期サーバーを有効にしてNASをバックアップサーバーとして設定することで、リモート再同期サーバーまたはNASサーバーからデータをバックアップすることができます。 再同期経由でのリモートレプリケーションに対するデフォルトのポート番号は、873です。帯域幅制御のため最大ダウンロードレートを指定します。 0 は、無制限を意味します。

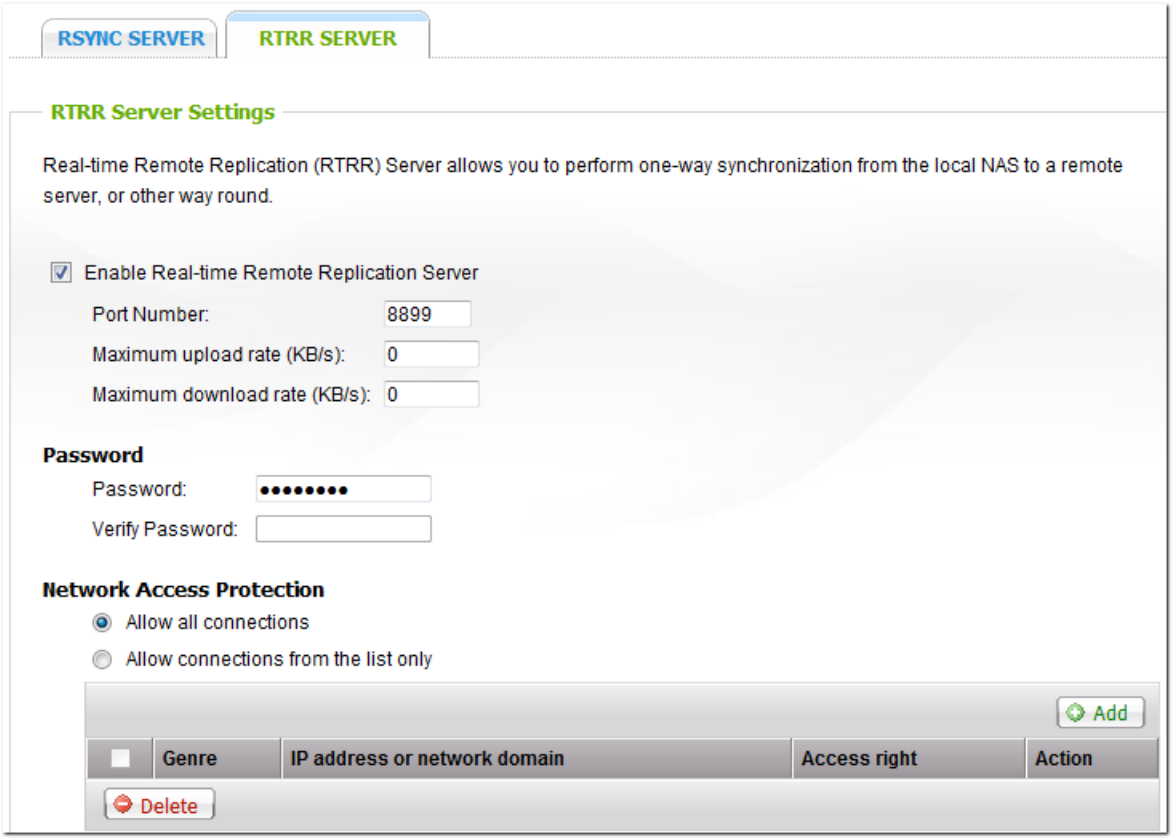
- リモートサーバーからローカルホストへのバックアップを有効にする: このオプションを選択すると、リモートサーバー（NAS）からローカルサーバー（NAS）にデータをバックアップすることができます。
- リモート再同期サーバーがNASにデータをバックアップできるようにする: このオプションを選択すると、再同期サーバーからローカルサーバー（NAS）にデータをバックアップすることができます。

ユーザー名とパスワードをセットアップすると、再同期サーバーから認証されたアクセスのみを許可して、NASにデータをバックアップすることができます。

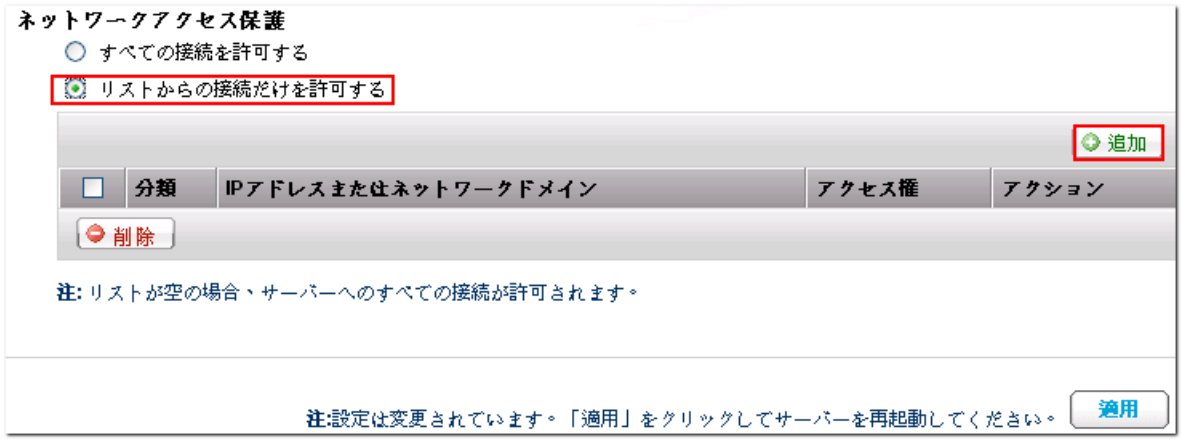


RTRRサーバー

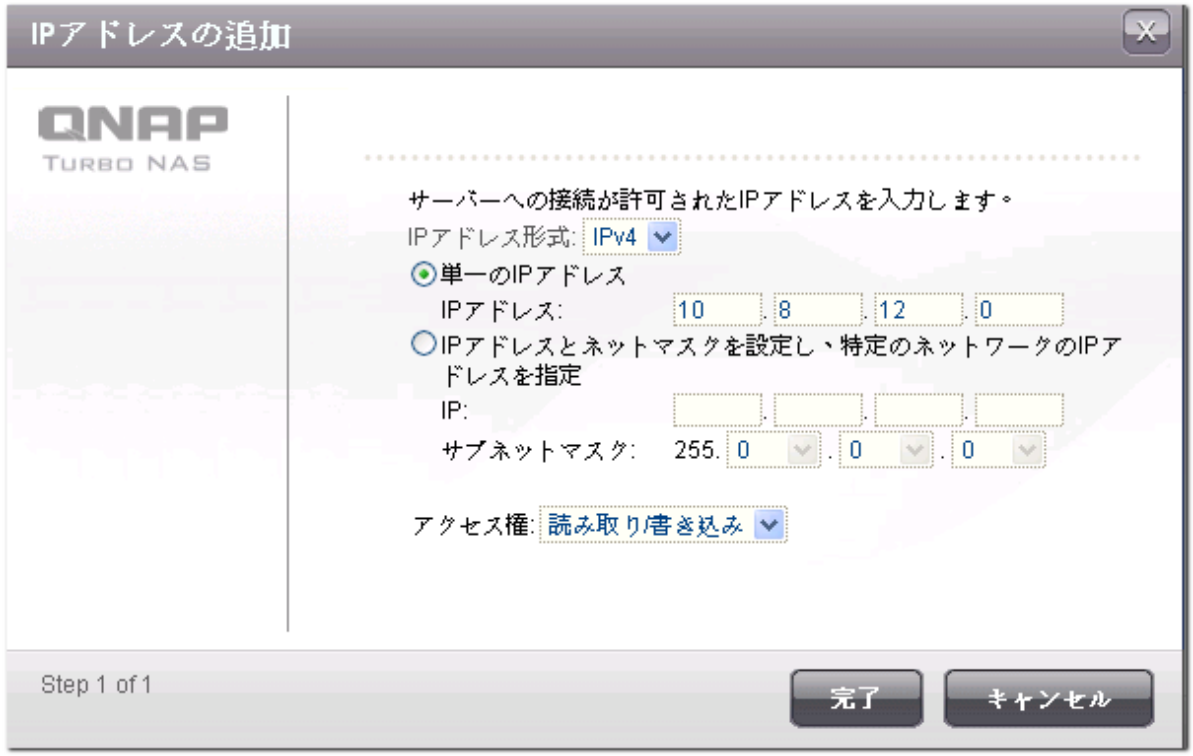
リモートサーバーからローカルNASにリアルタイムまたはスケジュールのデータレプリケーションを可能にするには、「Enable Real-time Remote Replication Server（リアルタイムのリモートレプリケーションサーバーを有効にする）」を選択します。リモートレプリケーションに対して、ポート番号を指定できます。デフォルトのポート番号:は8899です。帯域幅制御のため最大アップロードレートとダウンロードレートを指定します。0 は、無制限を意味します。認証されたアクセスのみを許可してローカルNASにデータをバックアップするには、アクセスパスワードを指定します。パスワードを入力し、RTRR経由でNASにデータをバックアップするように求めるプロンプトが、クライアントサーバーに対して出されます。



リモートレプリケーションのためにNASへのアクセスを許可する、IPアドレスまたはホスト名を指定できます。規則は、**最大10件まで設定できます**。すべての接続を許可するには、「Allow all connections（すべての接続を許可する）」を選択します。IPアドレスまたはホスト名を指定するには、「Allow connections from the list only（リストのみから接続を許可する）」を選択し「Add（追加）」をクリックします。



IPとサブネットマスクを入力することで、IPアドレスを入力したりIPアドレスの範囲を指定します。「読み込みのみ」または「読み込み/書き込み」のアクセス権を選択します。「読み込み/書き込み」を選択することで、クライアントサーバーはローカルNASのファイルを削除できます。「FINISH（終了）」をクリックして終了します。



アクセス規則を保存した後、「APPLY（適用）」をクリックするとNASが再起動して設定を適用します。

7.14 アンチウイルス

ステータス

ウィルス対策機能を使用して、NAS を手動または定期的なスケジュールでスキャンし、ウイルス、マルウェア、トロイの木馬、および、その他の悪意のある脅威に感染したファイルを削除または隔離します。この機能を利用するには、「Enable antivirus（アンチウイルスを有効にする）」を選択し、「Apply（適用）」をクリックします。

更新:
「Check and update automatically（自動的に確認して更新します）」を選択し、ウィルス対策定義を自動的に更新する間隔日数を指定します。オンライン更新の横の「Update Now（今すぐ更新）」をクリックして、ウィルス対策定義を直ちに更新します。また、http://www.clamav.net から更新ファイルをダウンロードして、ウィルス対策定義を手動で更新することも可能です。
この機能を使用するには、インターネットにNASを接続する必要があります。

隔離:
NAS 上のディスクボリュームの隔離情報を表示します。詳細は、「Application Servers（アプリケーション）」>「Antivirus（アンチウイルス）」>「Quarantine（隔離）」で参照します。

スキャンジョブ

NAS は、手動またはスケジュールでの全共有あるは指定した共有のスキャンをサポートします。最大 64 件のスキャンジョブを作成し、同時に 5 スキャンジョブを起動できます。スキャンジョブを作成するには、次のステップを行います。

1. 「Application Servers（アプリケーション）」>「Antivirus（アンチウイルス）」>「Scan Jobs（スキャンジョブ）」に進みます。「New Scan Job（新規スキャンジョブ）」をクリックします。

2. ジョブ名を入力して、スキャンするネットワーク共有を選択します。スキャンするネットワーク共有を指定するには、共有を選択して、「Add（追加）」をクリックします。

3. 複数のネットワーク共有を選択可能です。ネットワーク共有を削除するには、共有名の横の をクリックします。「Next（次へ）」をクリックします。

4. スキャンジョブのスクジュールを定義します。「Next（次へ）」をクリックします。

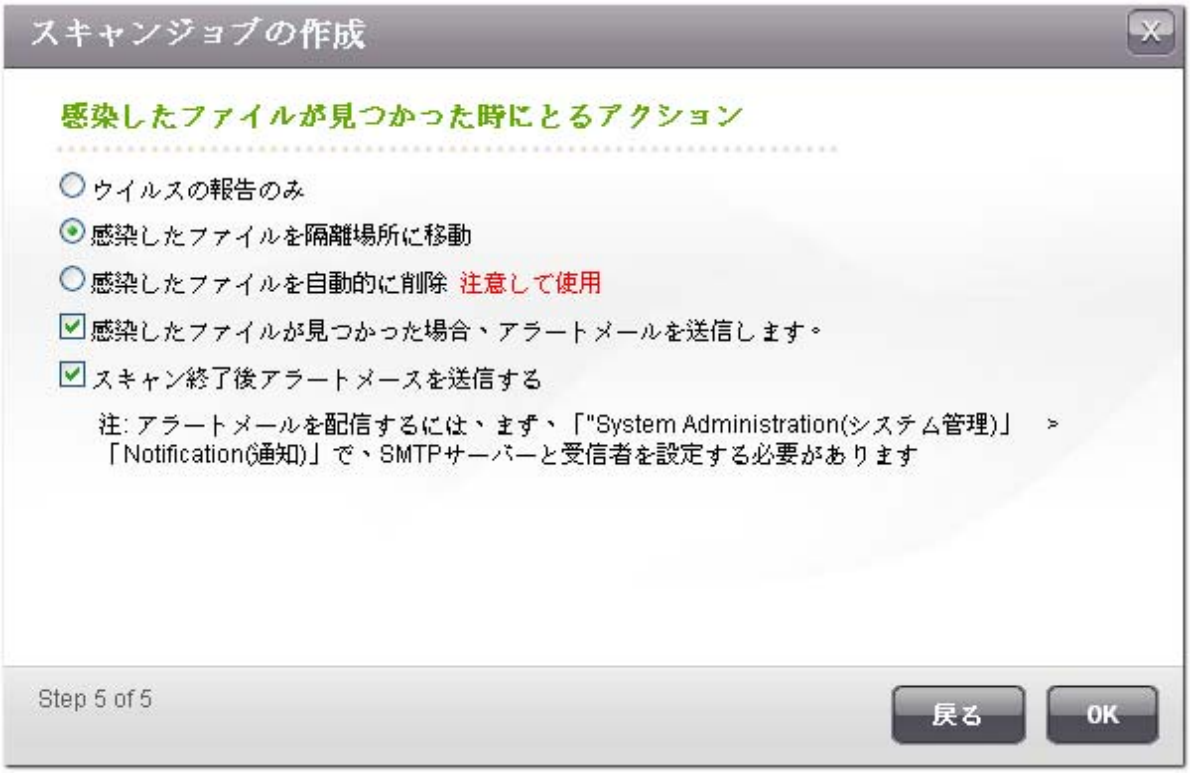
5. ネットワーク共有内の全ファイルをスキャンするか、感染の可能性のあるファイルだけをクイックスキャンするかを選択します。「Exclude files or folders（除外するファイルまたはフォルダ）」を選択し、ウィルススキャンを実行しないファイル、フォルダ、またはファイル拡張子を指定します。同一行にスペース区切りで入力するか、行ごとに入力します。例：
/Public/testfile.txt
/Download
*.log
*.exe *.com
*.txt
「Next（次へ）」をクリックします。

6. 他のスキャンオプションの有効化：
   - スキャニングを行う最大ファイルサイズ（1 ～ 4096 MB）を指定します。
   - ネットワーク共有内の圧縮ファイルをスキャンするには、「Scan compressed files（圧縮したファイルをスキャン）」を有効にします。該当する場合は、圧縮ファイル大きさの最大値（1 ～ 4096 MB）を指定します。
   - MS オフィスおよび Mac オフィスファイル、RTF、PDF、および HTML ファイルをスキャンするには、「Scan documents（ドキュメントをスキャン）」を選択します。

「Next（次へ）」をクリックします。

7. 感染したファイルを検出したときのアクションを指定します。
   - ウィルスの報告のみ：「Reports（レポート）」タブの下にウィルススキャンの結果が記録されます。感染ファイルに対して、アクションを実施しません。
   - 感染したファイルを隔離場所に移動：感染したファイルは隔離され、元のネットワーク共有からはアクセスできなくなります。「Reports（レポート）」タブの下にウィルススキャンの結果が表示され、ユーザーは「Quarantine（隔離）」タブの下の感染ファイルを削除/復元できます。
   - 感染したファイルを自動的に削除：感染したファイルは削除され、復元できなくなります。

感染ファイルの検出時、または、スキャン完了後に、E メールを受信するには、「System Administration（システム管理）」>「Notification（通知）」>「Configure SMTP Server（SMTP サーバの設定）」で、SMTP サーバーを設定します。「OK」をクリックして、スキャンジョブを作成します。



8. スキャンジョブは指定したスケジュールにより起動します。

ボタン	説明
	スキャンジョブを今すぐ起動します。
	スキャンジョブを停止します。
	スキャンジョブの設定を編集します 。
	最新のウィルススキャンのサマリをダウンロードします。ファイルは、WordPad などのテキストエディタで開くことができます。
	スキャンジョブを削除します。

レポート

NAS 上の最新のスキャンジョブのレポートを表示/ダウンロードします。

ボタン	説明
	ウィルススキャンのレポートをダウンロードします。ファイルは、WordPad などのテキストエディタで開くことができます。
	リスト上のエントリを削除します。
ダウンロード	リスト上の全ウィルススキャンのログを zip ファイルとしてダウンロードします。

レポートオプション

- ログを保存する日数(1 ～ 999)を指定します。
- 「Archive logs after expiration (有効期限切れにログをアーカイブします)」オプションを有効化し、保存日数に達したログを保存するネットワーク共有を指定します。「Apply (適用)」をクリックして、変更を保存します。

隔離

このページには、NAS 上の隔離ファイルが表示されます。ユーザーは、手動で隔離ファイルを削除/復元し、または、除外リストにファイルを復元/追加できます。

ボタン/オプション	説明
	感染ファイルを削除します。ファイルは復元できません。
	感染ファイルを元のネットワーク共有に復元します。
	感染ファイルを復元し、除外リスト(スキャンフィルタ)に追加します。
選択したファイルを復元	リスト上の複数ファイルを復元します。
選択したファイルを削除	リスト上の複数ファイルを削除します。ファイルは復元できません。
すべてのファイルを削除	リスト上の全ファイルを削除します。ファイルは復元できません。

7.15 TFTPサーバー

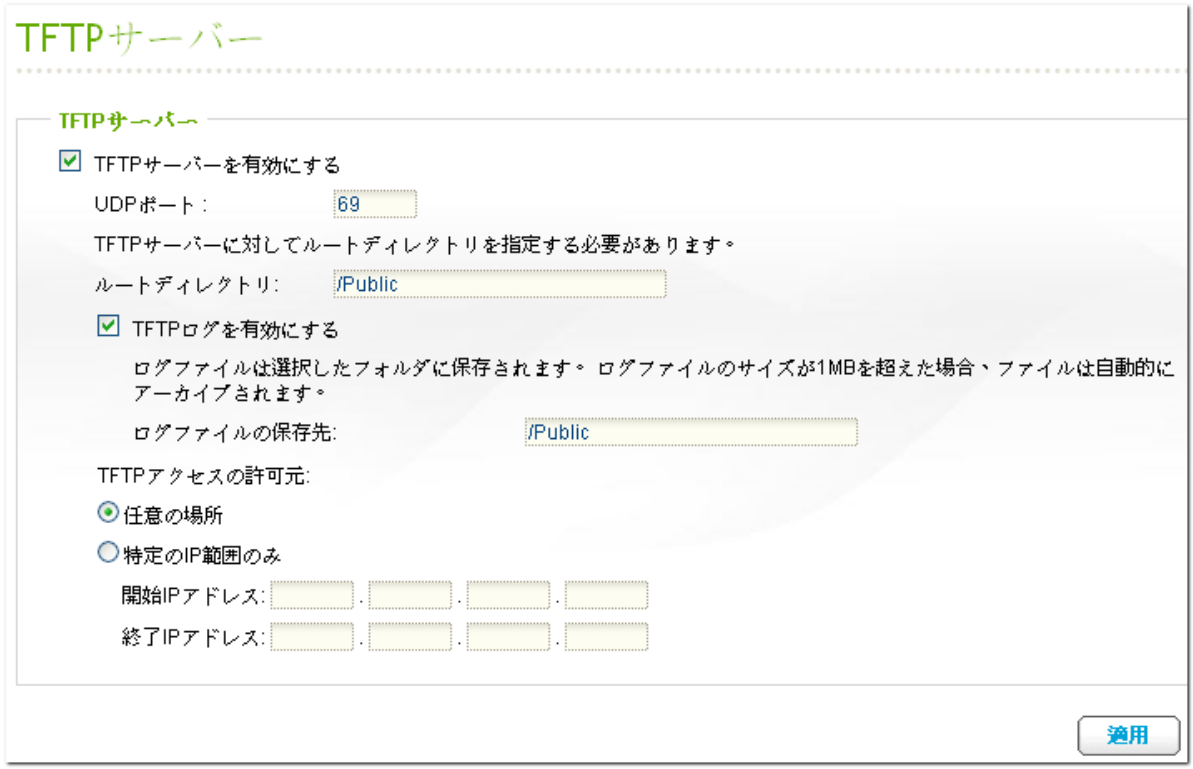
NAS を TFTP（Trivial File Transfer Protocol：トリビアル ファイル トランスファー プロトコル）サーバーとして設定し、ネットワークデバイスの設定管理およびシステムイメージおよびシステムリカバリでのコンピュータのリモートネットワークブートを行います。TFTP は、FTP の非常に基本的な機能であるファイル転送プロトコルです。 TFTP は、ユーザー認証を提供せず、標準 FTP クライアントにより接続できません。

この機能を利用するには、「Enable TFTP Server（TFTPサーバーを有効にする）」を選択します。ファイル転送アクティビティには、デフォルト UDP ポート（番号 69）が使用されます。 必要がある場合のみ、ポート番号を変更します。
TFTP サーバーのルートディレクトリとして、NAS 上のフォルダを指定します。

Enable TFTP Logging（TFTPログを有効にする）: このオプションを有効にして、TFTP ログファイル（opentftpd.log）を保存するディレクトリを指定します。ログファイルを閲覧するには、Windows OS では、Microsoft Excel または、WordPad、Mac OS では、TextEdit の利用を推奨します。

IP アドレスの範囲を指定して、TFTP クライアントアクセスを制限するか、「Anywhere（どこでも）」を選択して、任意の TFTP クライアントアクセスを許可します。「Apply（適用）」をクリックして、設定を保存します。

.



7.16 VPN サービス

NAS は、仮想プライベートネットワーク（VPN）サービスをサポートしており、ユーザーは、インターネットからプライベートネットワーク上で NAS およびリソースにアクセスすることができます。 次の指示に従って、NAS 上の VPN サービスの初期設定を行います。

1. 接続するネットワークインターフェースを選択します
2. PPTP サービスまたは OpenVPN サービスを有効にします
3. 自動ルーター設定により、ポートフォワーディングを設定します
4. MyCloudNAS サービスを登録します
5. VPN ユーザーを追加します
6. VPN クライアントにより、プライベートネットワークに接続します

1. 接続するネットワークインターフェースを選択します

NAS に「admin」としてログインし、「Application Servers（アプリケーションサーバー）」>「VPN Service（VPN サービス）」>「VPN Server Settings（VPN サーバー設定）」に移動します。「General Settings（一般設定）」の下で、NAS が所属するネットワークに接続するネットワークインターフェースを選択します。

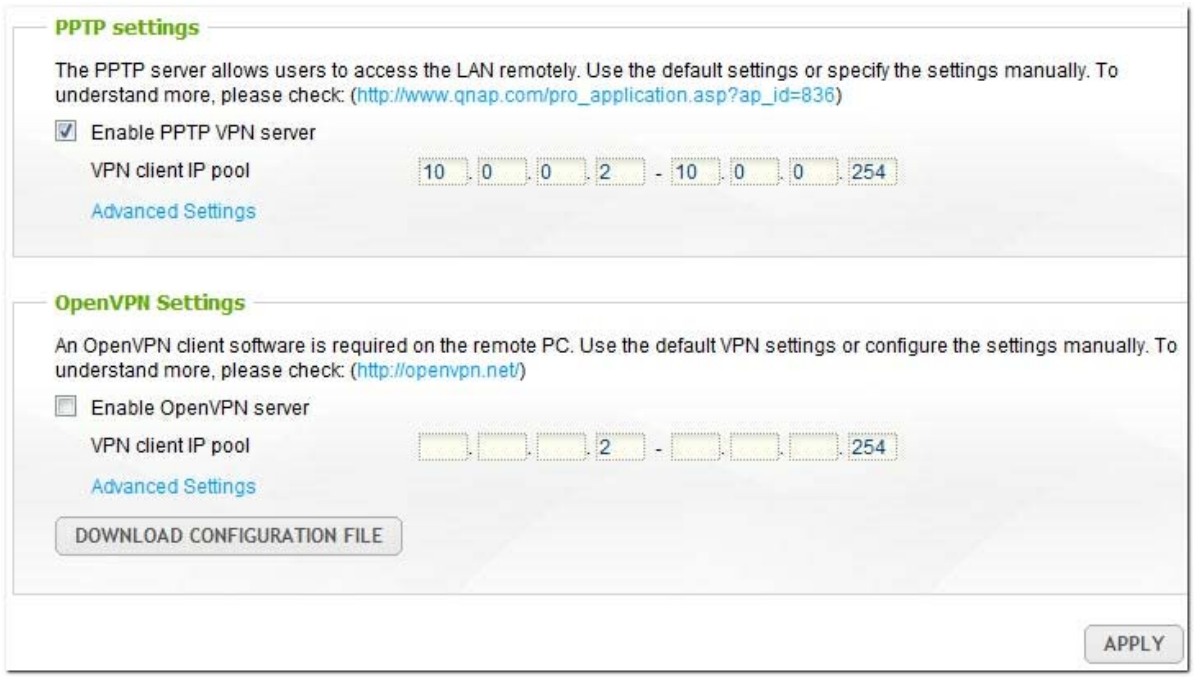
2. PPTP サービスまたは OpenVPN サービスを有効にします

NAS は、VPN 接続に対して、PPTP および OpenVPN をサポートします。いずれかのオプションを選択し、設定を行います。

PPTP：ポイントツーポイントトンネルプロトコル（PPTP）は、VPN 接続の最も良く使用される方法の一つです。Windows、Mac、Linux、Android、および iPhone でネイティブにサポートされます。

OpenVPN：OpenVPN とは、セキュア接続に SSL 暗号化を使用するオープンソースの VPN ソリューションです。OpenVPN サーバーに接続するには、お使いの PC 上に OpenVPN クライアントをインストールする必要があります。「Download Configuration File（設定ファイルのダウンロード）」とクリックし、NAS から VPN クライアント設定、認証/キーおよびインストールガイドをダウンロードして、ファイルを OpenVPN クライアントにアップロードします。

> 注：OpenVPN 設定、MyCloudNAS 名またはセキュア証明書が変更される場合は必ず OpenVPN クライアントに設定ファイルをアップロードする必要があります。



3. 自動ルーター設定により、ポートフォワーディングを設定します

NAS は、UPnP（ユニバーサルプラグアンドプレイネットワークプロトコル）ルーターに対して、自動ポートフォワーディングをサポートしています。「MyCloudNAS Service（MyCloudNAS サービス）」>「Auto Router Configuration（自動ルーター設定）」に移動し、UPnP ポートフォワーディングを有効にして、ルーター上で PPTP サービスまたは OpenVPN サービス用のポートを開きます。

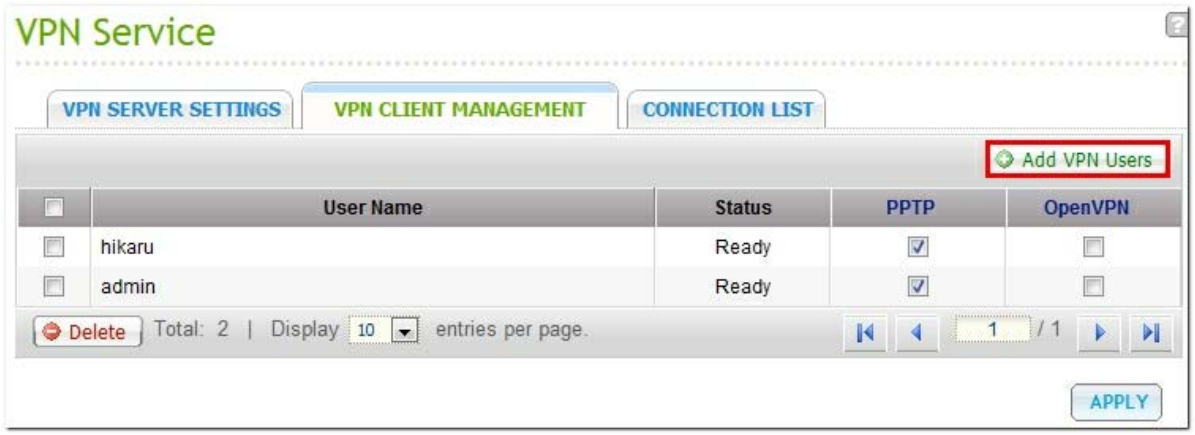
> 注：インターネット上で PPTP サーバーに接続するには、一部のルーターでは PPTP パススルーオプションを開く必要があります。PPTP は、ポート TCP-1723 のみを使用します。お使いのルーターが UPnP をサポートしていない場合、このポートを手動でフォワーディングする必要があります。

4. MyCloudNAS サービスを登録します

WAN IP または MyCloudNAS 名で NAS に接続することができます。MyCloudNAS サービスを有効にするには、「MyCloudNAS Service（MyCloudNAS サービス）」>「Configure MyCloudNAS（MyCloudNAS 設定）」に移動します。更に詳しい情報は、http://www.qnap.com/pro_application.asp?ap_id=637 を参照してください

5. Add VPN Users（VPN ユーザーを追加します）

「Application Servers（アプリケーションサーバー）」>「VPN Service（VPN サービス）」>「VPN Client Management（VPN クライアント管理）」に移動し、「Add VPN Users（VPN ユーザーの追加）」をクリックします。ローカル NAS ユーザーが表示されます。VPN サービスの使用を許可するユーザーとその接続方法（PPTP、OpenVPN または両方）を選択します。「Add（追加）」をクリックします。



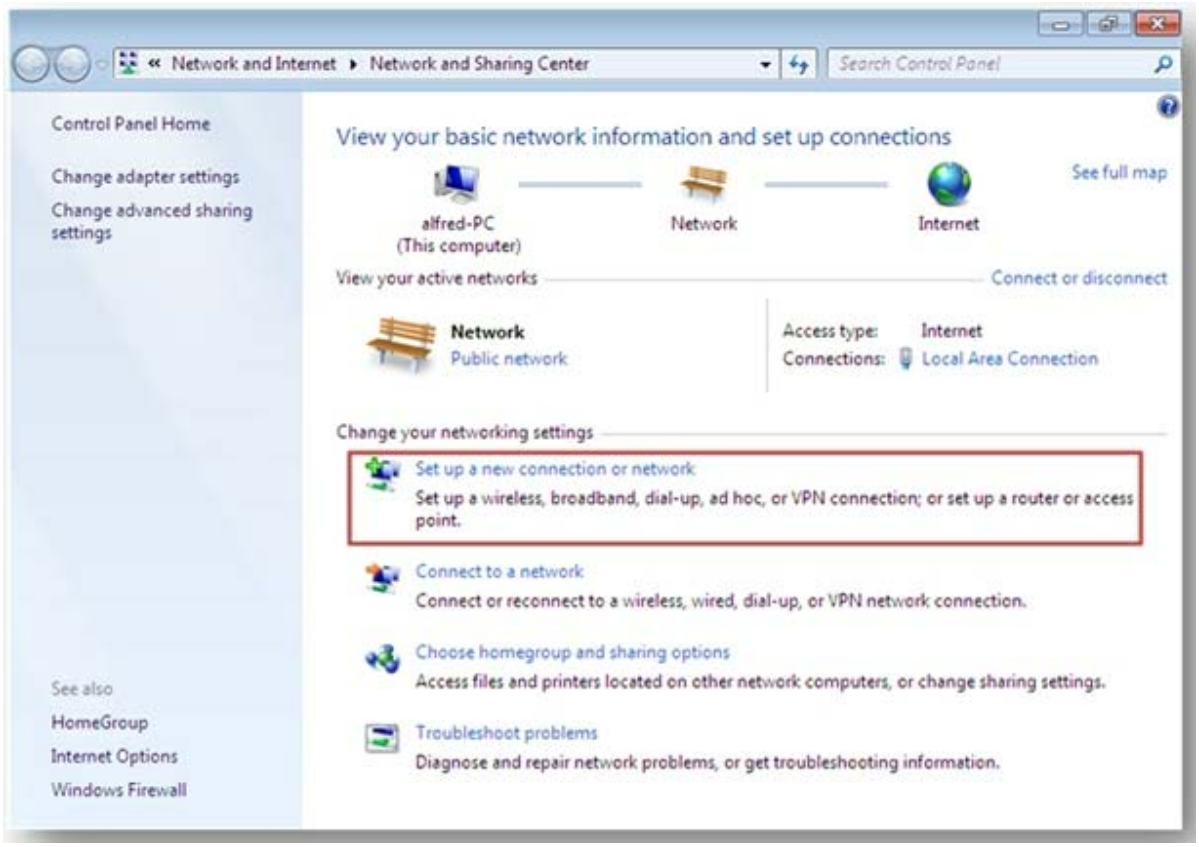
Select users and their privileges
Create a User
Total: 3
1 / 1
User Name
PPTP
OpenVPN
bbb
jason
rr
Step 1 / 1
ADD
CANCEL

6. VPN クライアントにより、プライベートネットワークに接続します

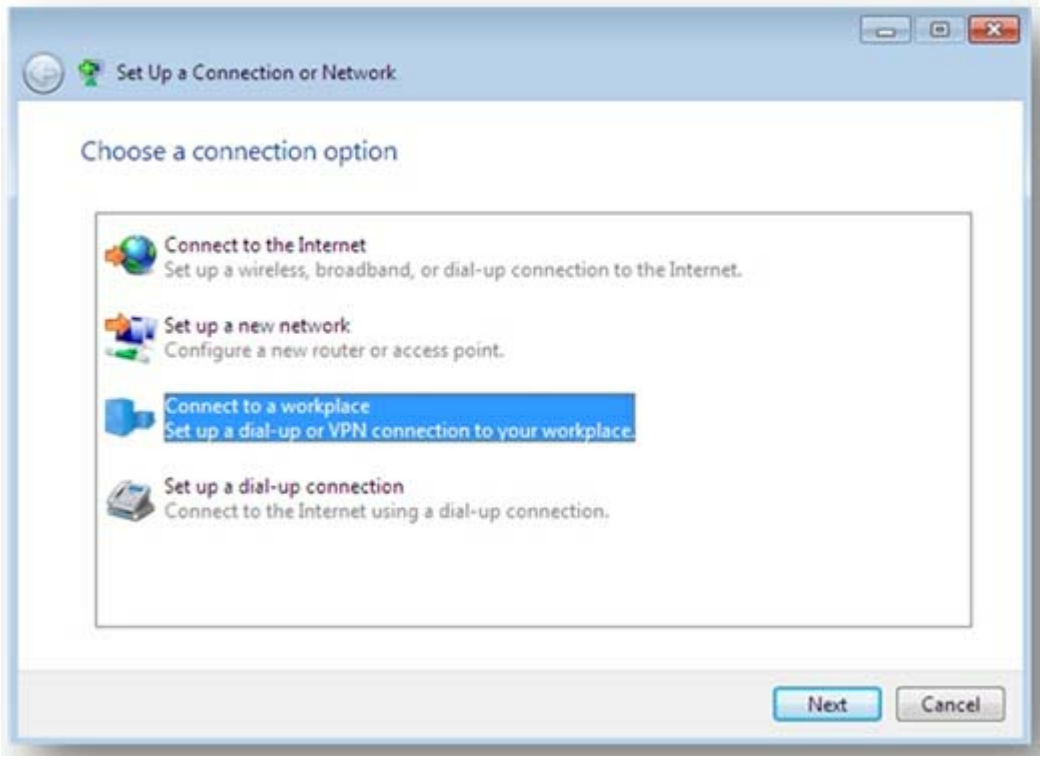
VPN クライアントを使用して、VPN サービスを介して NAS に接続できるようになりました。

Windows 7 上の PPTP

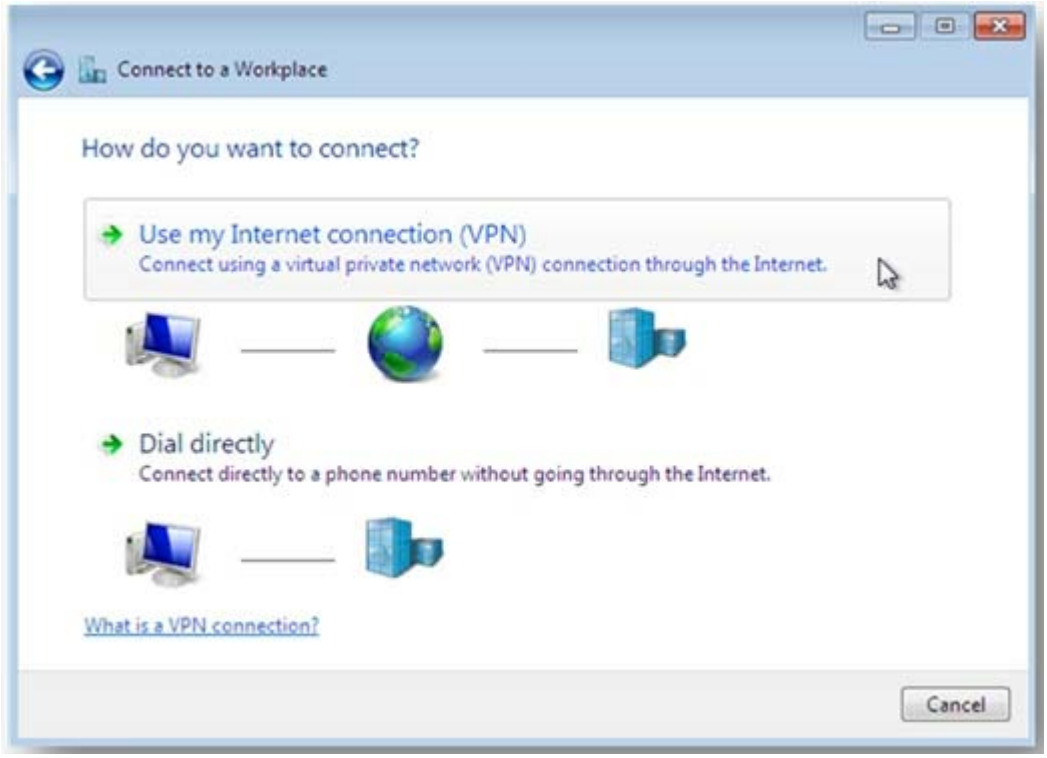
1. 「Control Panel（コントロールパネル）」>「Network and Sharing Center（ネットワークおよび共有センター）」に移動します。「Set up a new connection or network（新規接続またはネットワークの設定）」を選択します。



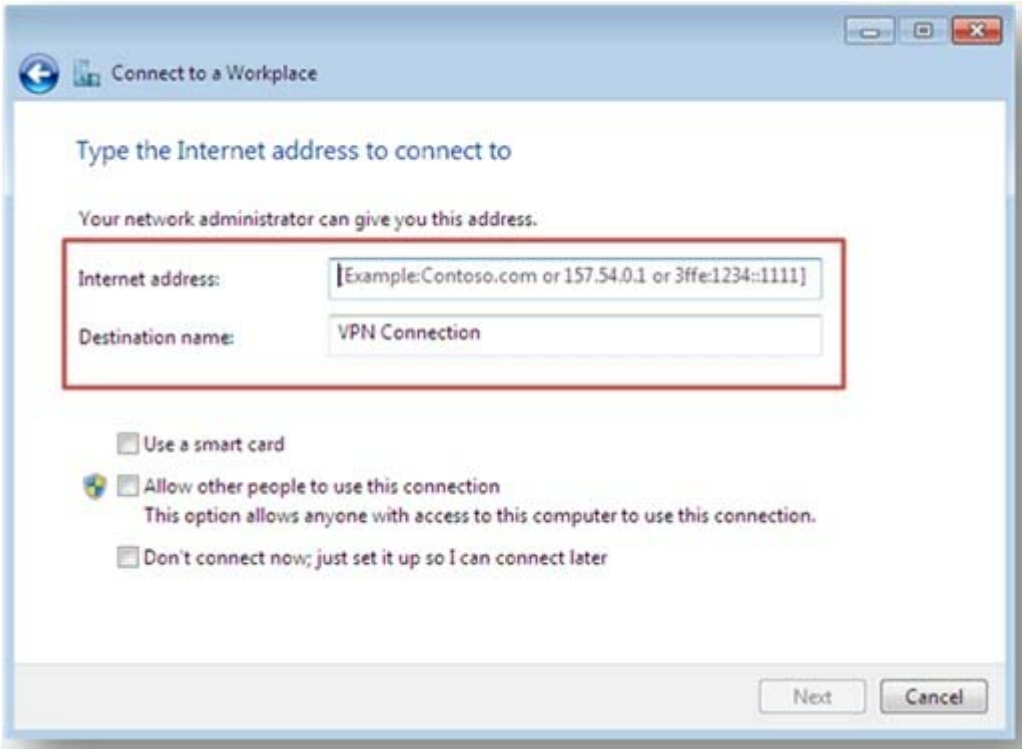
2. 「Connect to a workplace（ワークプレイスに接続する）」を選択し、「Next （次へ）」をクリックします。



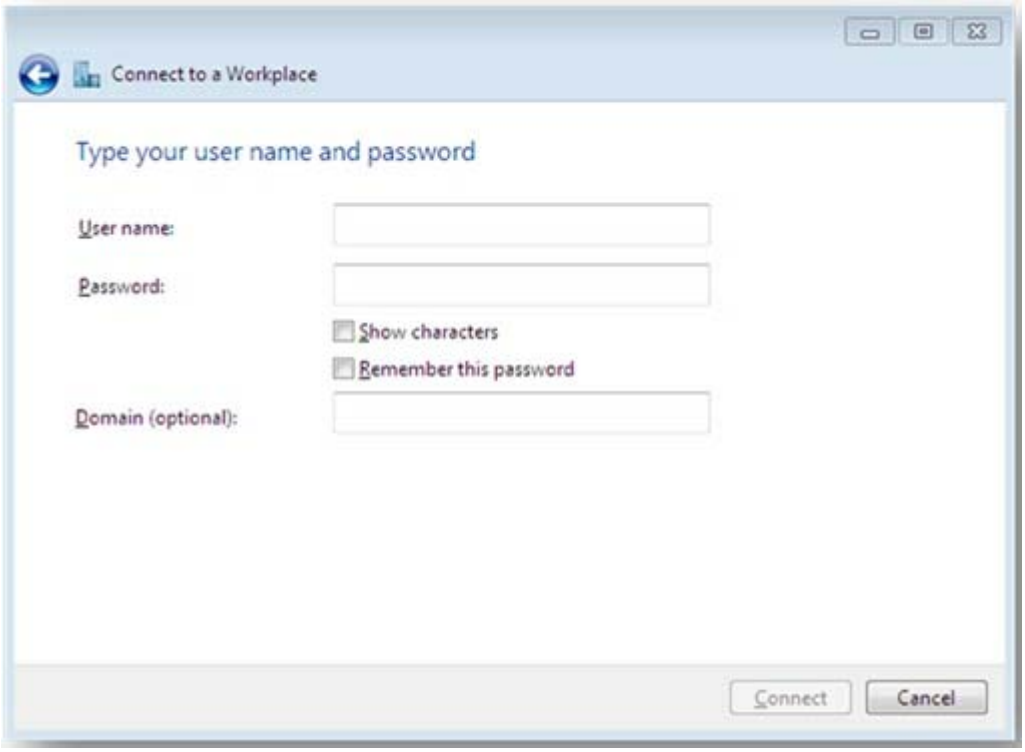
3. 「Use my Internet connection (VPN)（マイインターネット接続（VPN）の使用」を選択します。



4. MyCloudNAS 名または NAS の WAN IP を入力し、接続名を入力します。その後、「NEXT（次へ）」をクリックします。



5. VPN アクセス用に NAS から追加されたユーザー名とパスワードを入力します。「Connect（接続）」をクリックします。

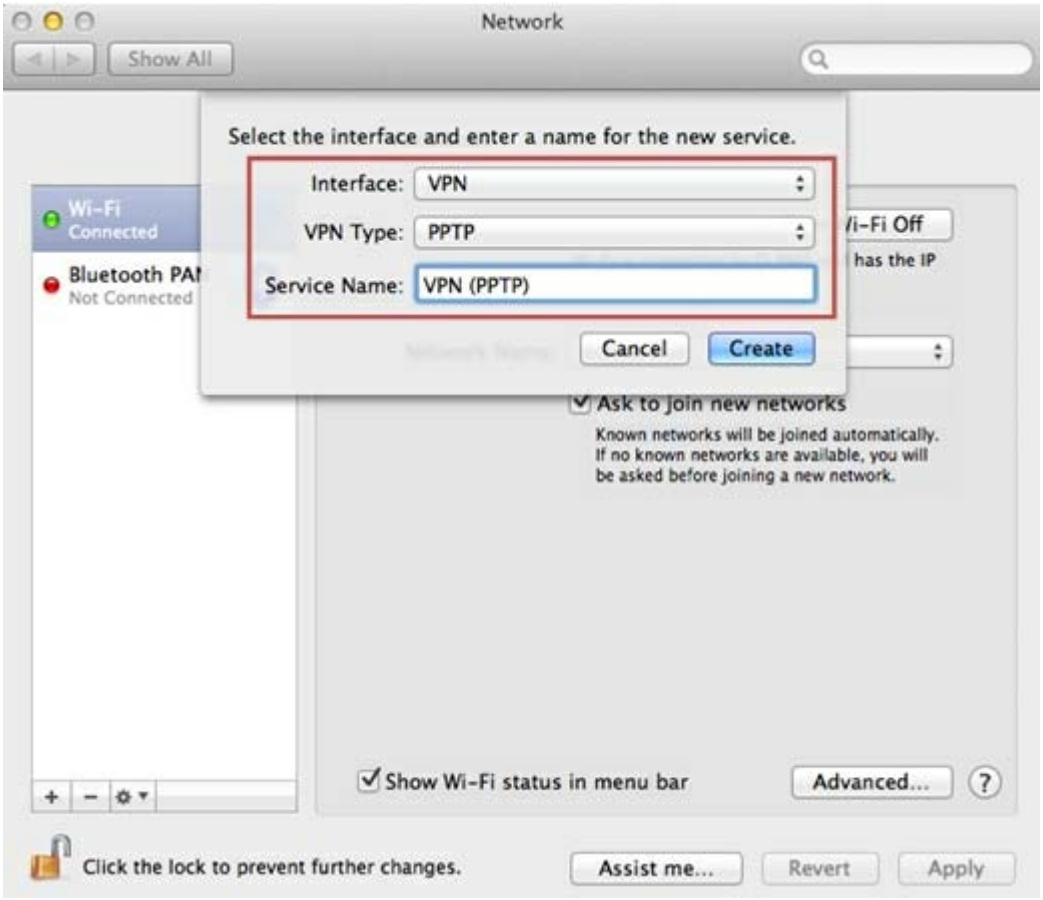


Mac OS X 10.7 上の PPTP

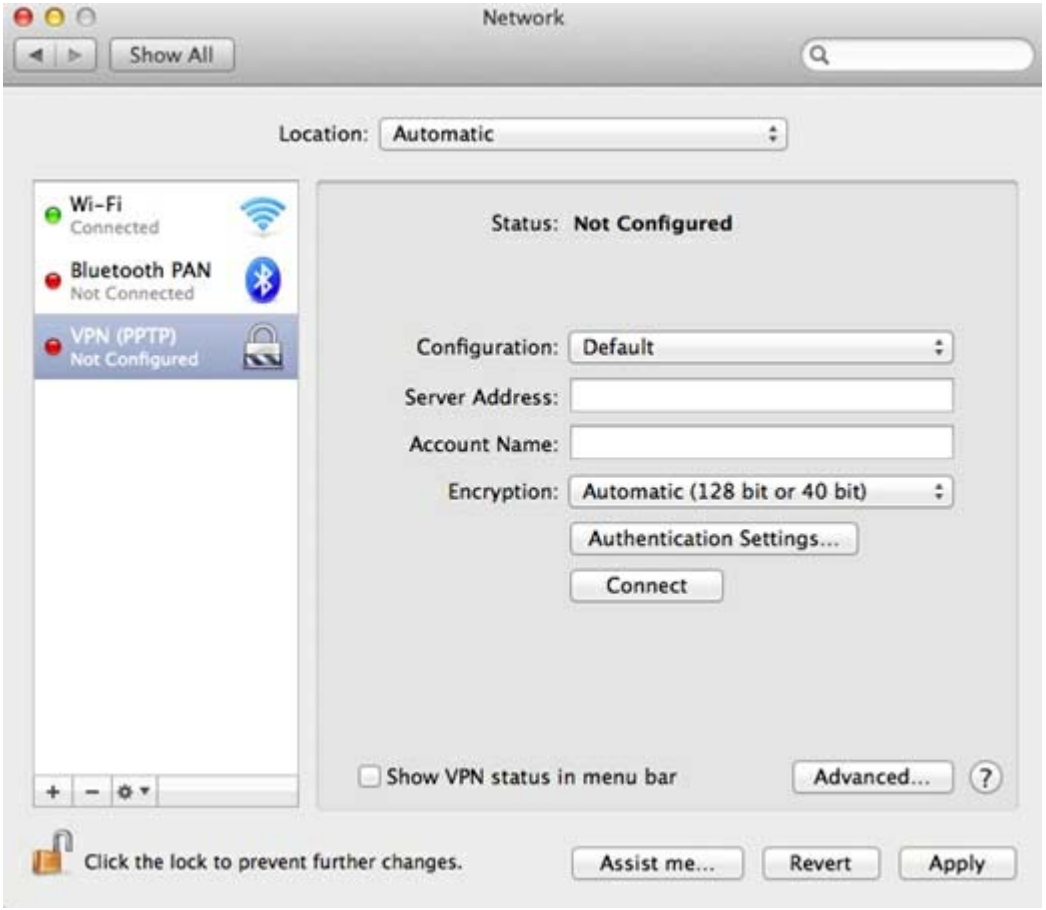
1. 「Apple menu（Apple メニュー）」>「System Preferences（システム設定）」に移動し、「Network（ネットワーク）」をクリックします。

2. リストの下の「Add (+)（追加（+））」をクリックし、インターフェースとして「VPN」を選択します。

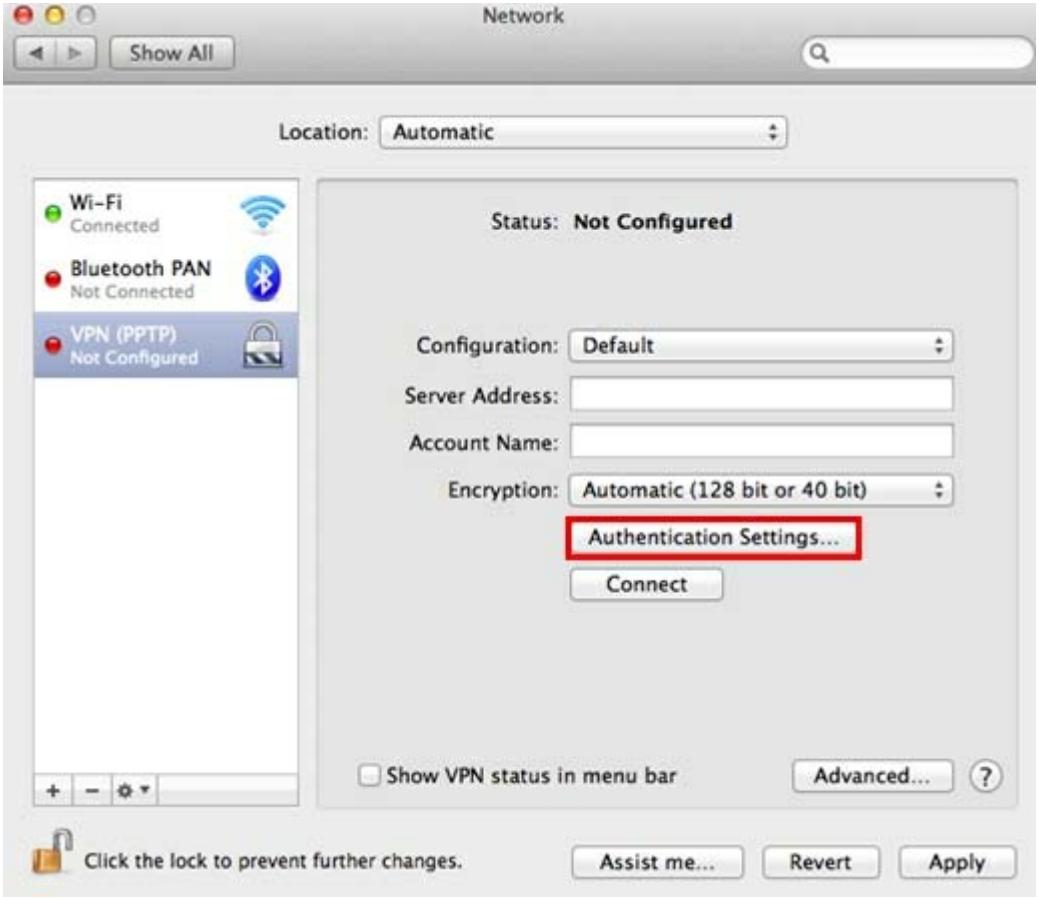
3. 接続する NAS の設定により VPN タイプを選択します。サービス名を入力します。



4. 「Server Address（サーバーアドレス）」で、MyCloudNAS 名または NAS の WAN IP を入力します。「Account Name（アカウント名）」で、NAS から追加されたユーザー名を入力します。


Network
Show All
Location: Automatic
Wi-Fi
Connected
Bluetooth PAN
Not Connected
VPN (PPTP)
Not Configured
Status: Not Configured
Configuration: Default
Server Address:
Account Name:
Encryption: Automatic (128 bit or 40 bit)
Authentication Settings...
Connect
Show VPN status in menu bar
Advanced...
Click the lock to prevent further changes.
Assist me...
Revert
Apply

5. 「Authentication Settings（認証設定）」をクリックし、ネットワーク管理者から与えられたユーザー認証情報を入力します。



6. ユーザー認証情報を入力後、「OK」をクリックし、その後「Connect（接続）」をクリックします。

iOS 5 上の PPTP

1. 「Settings（設定）」>「General（一般）」>「Network（ネットワーク）」> を選択し、「VPN」をクリックします。

2. 「Add VPN Configuration（VPN 設定の追加）」をクリックします。

3. 「PPTP」をクリックし、Description（説明）、Server（サーバー）、接続用のAccount（アカウント）およびPassword（パスワード）を入力します。

4. 「Settings（設定）」>「General（一般）」>「Network（ネットワーク）」>「VPN」に戻り、「VPN」を有効にします。

Windows 上の OpenVPN

1. http://openvpn.net/index.php/open-source/downloads.html から OpenVPN をダウンロードします
2. Windows 上に OpenVPN クライアントをインストールします。デフォルトインストールディレクトリは、C:¥Program Files¥OpenVPN です。
3. 管理者として OpenVPN GUI を起動します。
4. NAS から OpenVPN 設定ファイルと証明書をダウンロードします（「Application Servers（アプリケーションサーバー）」>「VPN Service（VPN サービス）」>「VPN Server Settings（VPN サーバー設定）」>「OpenVPN Settings（OpenVPN 設定）」）。
5. openvpn.ovpn ファイルを編集し、「OPENVPN_SERVER_IP」を OpenVPN サーバー IP で置き換えます。
6. 「ca.crt」および「openvpn.ovpn」を OpenVPN 設定サブディレクトリの下の設定フォルダ（C:¥Program Files¥OpenVPN¥config）に配置します。

注：Windows 7 上で OpenVPN クライアントを起動する場合は、OpenVPN の詳細設定内でファイアウォールルールを追加します。

Linux 上の OpenVPN

1. http://openvpn.net/index.php/open-source/downloads.html から OpenVPN をダウンロードします
2. Linux 上に OpenVPN クライアントをインストールします。
3. NAS から OpenVPN 設定ファイルと証明書をダウンロードします（「Application Servers（アプリケーションサーバー）」 > 「VPN Service（VPN サービス）」 > 「VPN Server Settings（VPN サーバー設定）」 > 「OpenVPN Settings（OpenVPN 設定）」）。
4. openvpn.ovpn ファイルを編集し、「OPENVPN_SERVER_IP」を OpenVPN サーバー IP で置き換えます。
5. 「ca.crt」および「openvpn.ovpn」を OpenVPN 設定サブディレクトリの下の設定フォルダに配置します。
6. OpenVPN を起動します。

Mac 上の OpenVPN

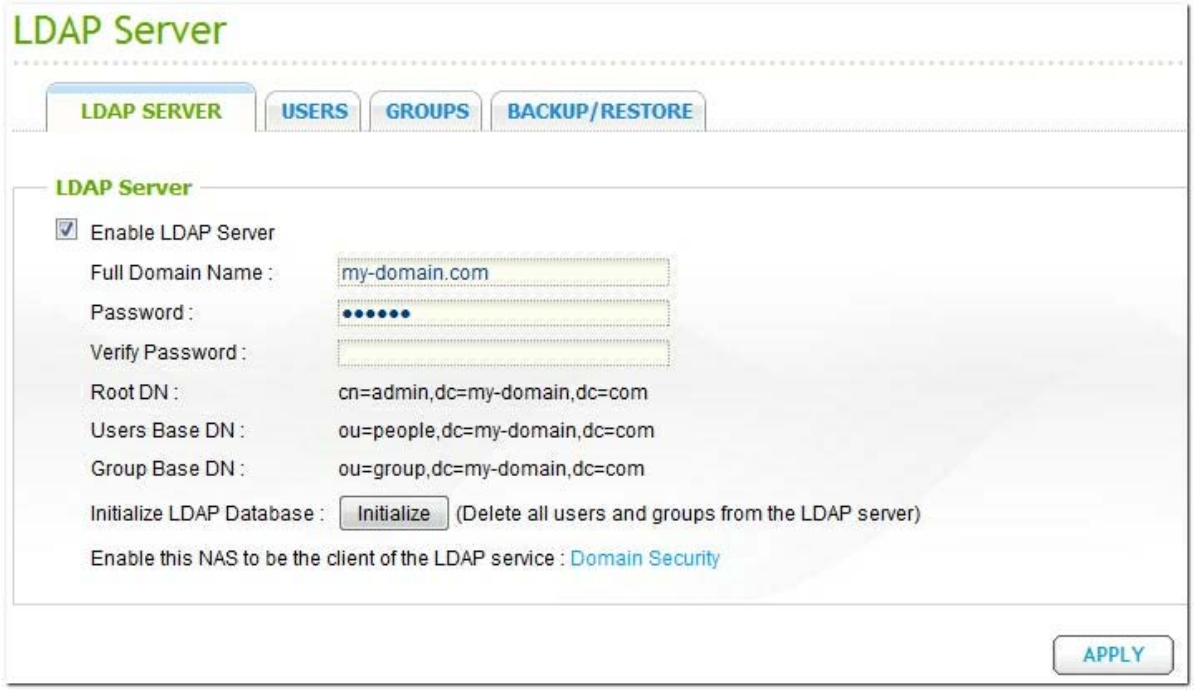
1. http://code.google.com/p/tunnelblick/ から OpenVPN クライアントのディスクイメージをダウンロードします
2. Tunnelblick を起動します。
3. NAS から OpenVPN 設定ファイルと証明書をダウンロードします（「Application Servers（アプリケーションサーバー）」 > 「VPN Service（VPN サービス）」 > 「VPN Server Settings（VPN サーバー設定）」 > 「OpenVPN Settings（OpenVPN 設定）」）。
4. openvpn.ovpn ファイルを編集し、「OPENVPN_SERVER_IP（alfred.myqnapnas.com）」を OpenVPN サーバー IP で置き換えます。
5. 「ca.crt」および「openvpn.ovpn」を OpenVPN 設定サブディレクトリの下の設定フォルダに配置します。
6. OpenVPN を起動します。

7.17 LDAP サーバー

NAS の LDAP サーバーを使用することで、管理者は、同一ユーザー名とパスワードで複数 NAS サーバーにアクセスできるユーザーを作成することができます。 以下の指示に従って、LDAP サーバーを設定します。

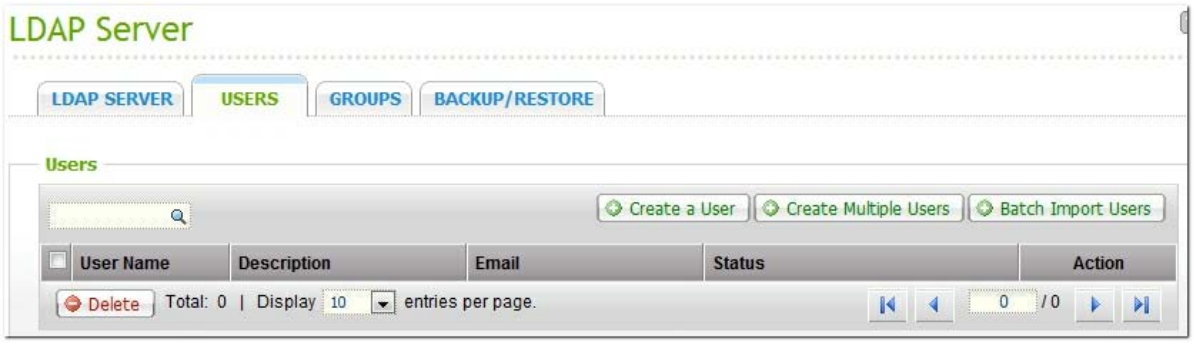
LDAP サーバーを有効にする

NAS に「admin」としてログインします。「Application Servers（アプリケーションサーバー）」 > 「LDAP Server（LDAP サーバー）」に移動し、LDAP サーバーを有効にします。フル LDAP ドメイン名と LDAP サーバーに対するパスワードを入力し、「Apply（適用）」をクリックします。



LDAP ユーザーの作成

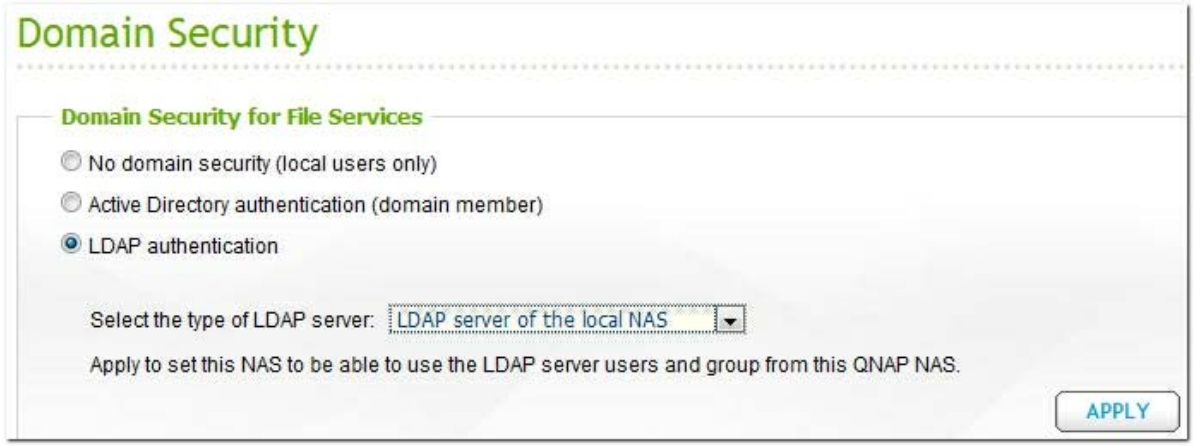
「Users（ユーザー）」タブの下で、「Create a User（ユーザーの作成）」、「Create Multiple Users（複数ユーザーの作成）」または「Batch Import Users（ユーザーの一括インポート）」をクリックします。ウィザードの指示に従って、LDAP ユーザーを作成します。



LDAP ユーザーを作成すると、NAS をドメインに参加させることができます。LDAP ユーザーの権限を設定し、NAS により認証することができます。

NAS の LDAP ドメインへの参加

LDAP ユーザーの NAS への接続を許可するには、NAS を LDAP ドメインに参加させます。「Access Right Management（アクセス権管理）」>「Domain Security（ドメインセキュリティ）」に移動します。「LDAP authentication（LDAP 認証）」を選択し、サーバータイプとして、「LDAP server of local NAS（ローカル NAS の LDAP サーバー）」を選びます。その後、「Apply（適用）」をクリックします。



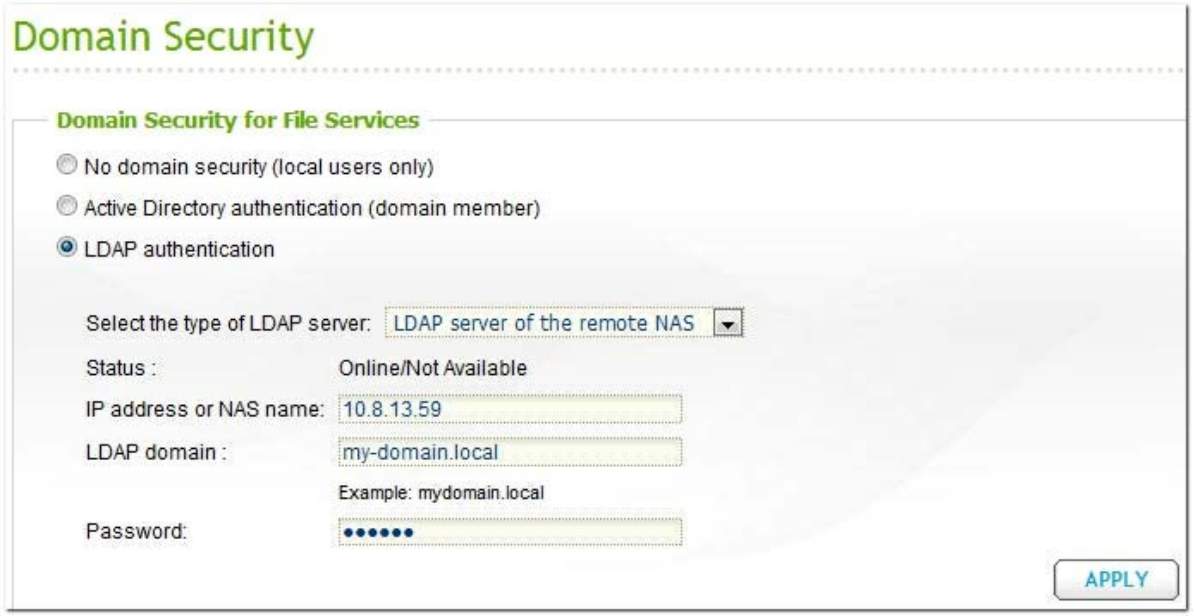
NAS は、LDAP サーバーのクライアントになりました。ドメインユーザーまたはグループを表示するには、「Access Right Management（アクセス権管理）」>「Users（ユーザー）」または「User Groups（ユーザーグループ）」に移動し、「Domain Users（ドメインユーザー）」あるいは「Domain Groups（ドメイングループ）」を選択します。また、ドメインユーザーあるいはグループにフォルダ権限を設定することもできます。

セカンダリ NAS の LDAP ドメインへの参加

複数 NAS サーバーを同一 LDAP ドメインに参加させ、LDAP ユーザーに同一ログイン情報を使用して NAS サーバーへの接続を許可することができます。

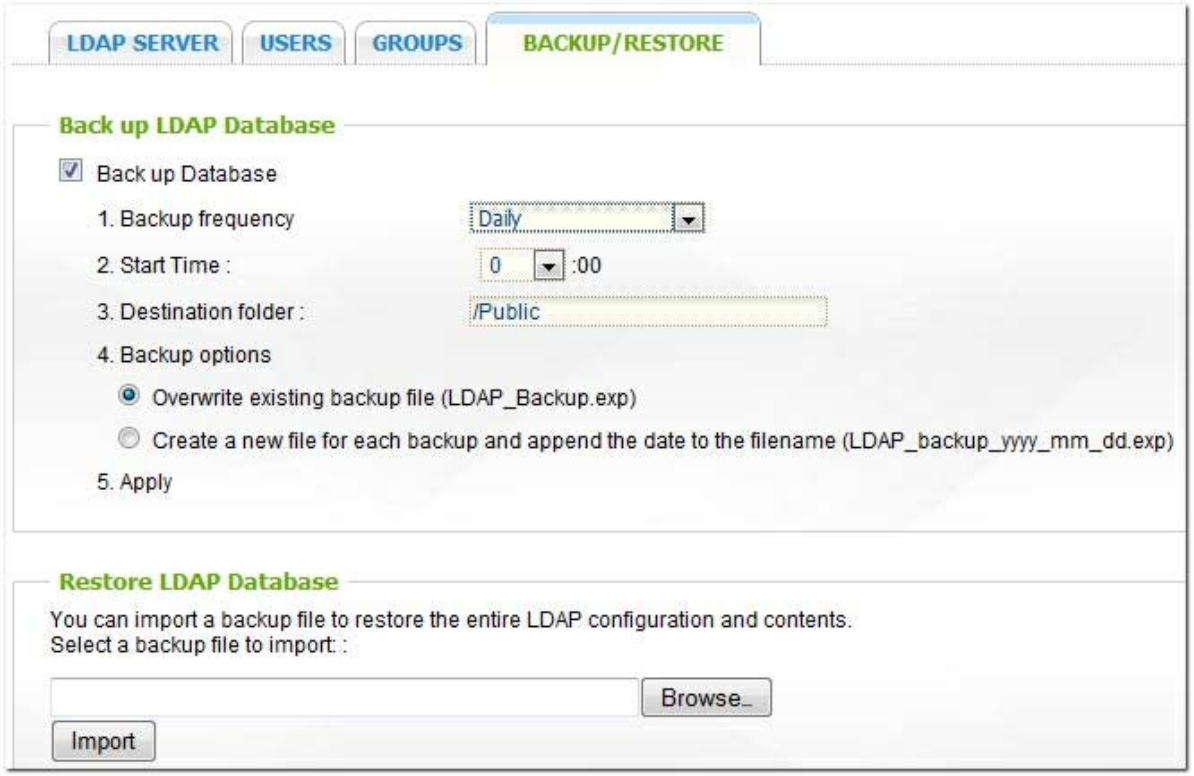
別な NAS を LDAP ドメインに参加させるには、「Access Right Management（アクセス権管理）」>「Domain Security（ドメインセキュリティ）」に移動します。「LDAP authentication（LDAP 認証）」を選択し、サーバータイプとして、「LDAP server of a remote NAS（リモート NAS の LDAP サーバー）」を選びます。

リモード NAS の DNS 名または IP アドレスを、事前に作成した LDAP ドメイン名を入力し、LDAP サーバーのパスワードを入力します。「Apply（適用）」をクリックします。



LDAP データベースのバックアップ/リストア

NAS 上の LDAP データベースをバックアップするには、「Back up Database（データベースのバックアップ）」を選択し、バックアップ周期、NAS 上の宛先フォルダおよびその他のオプションを指定します。 LDAP データベースをリストアするには、*.exp ファイルを参照し、選択して「Import（インポート）」を選びます。「Apply （適用）」をクリックして、設定を適用します。



8. バックアップ

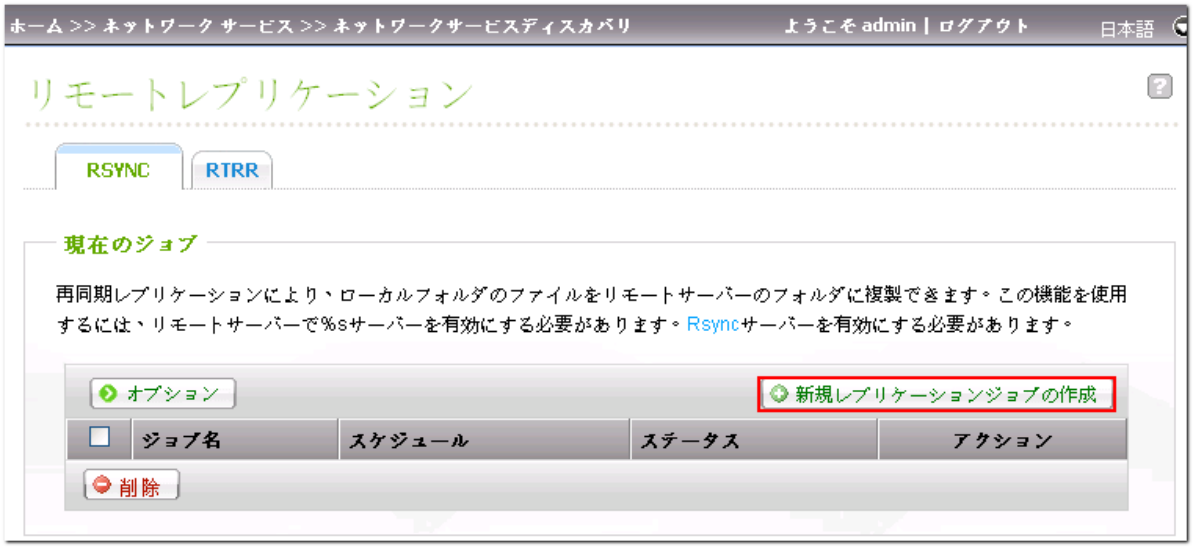
リモートレプリケーション 511
クラウドバックアップ 536
Time Machine 546
外部ドライブ 552
USBワンタッチコピー 566

8.1 リモートレプリケーション

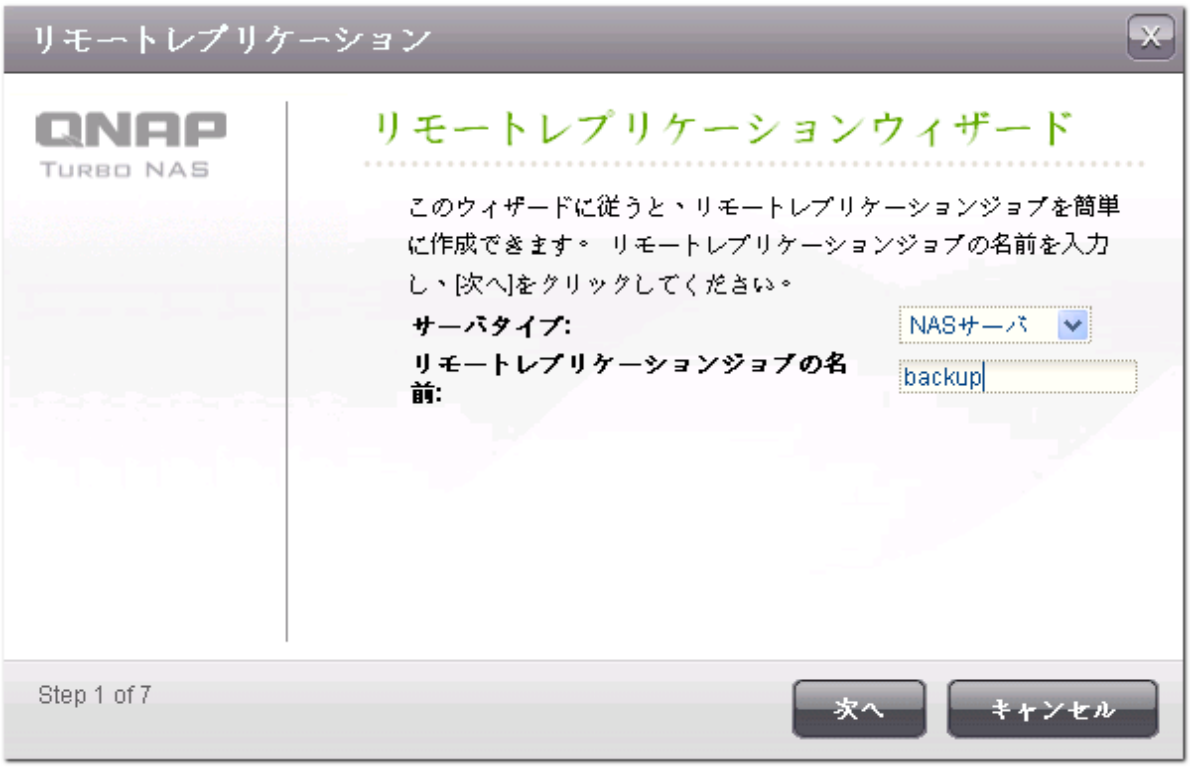
再同期レプリケーション

再同期リモートレプリケーションにより、リモートNASまたは再同期サーバーに対してNASデータを複製できます。バックアップ先がNASの場合、まず「アプリケーションサーバー」>「バックアップサーバー」>「再同期サーバー」に移動し、再同期バックアップサーバーとしてリモートNASを有効にします。

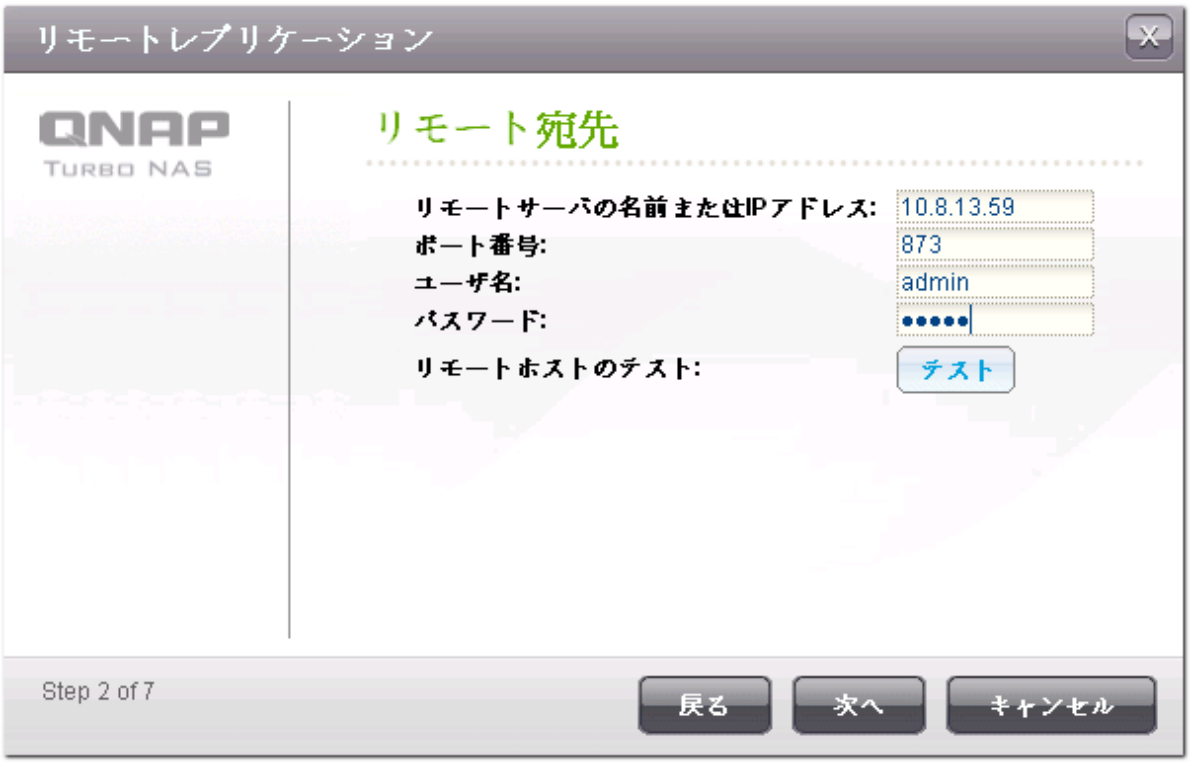
レプリケーションジョブを作成するには、「新規レプリケーションジョブの作成」をクリックします。



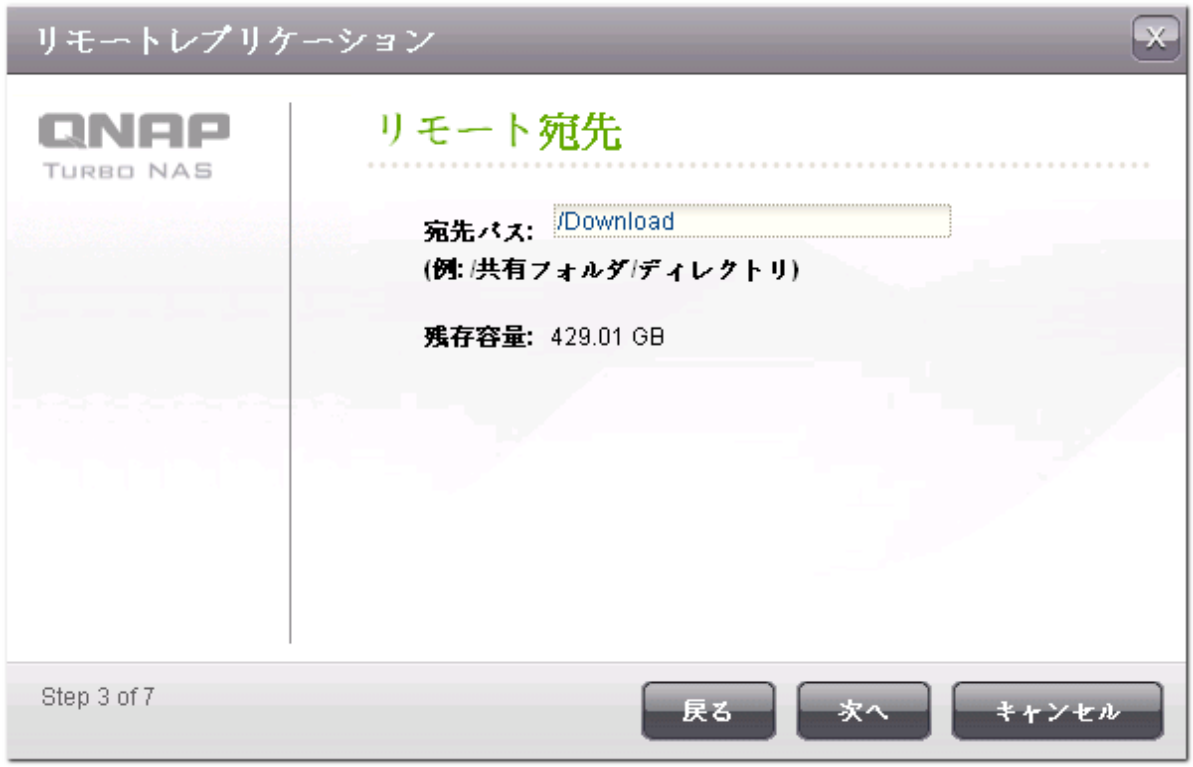
リモートサーバーのサーバータイプ、NASまたは再同期サーバーを指定します。ジョブ名を入力します。「NEXT（次へ）」をクリックします。



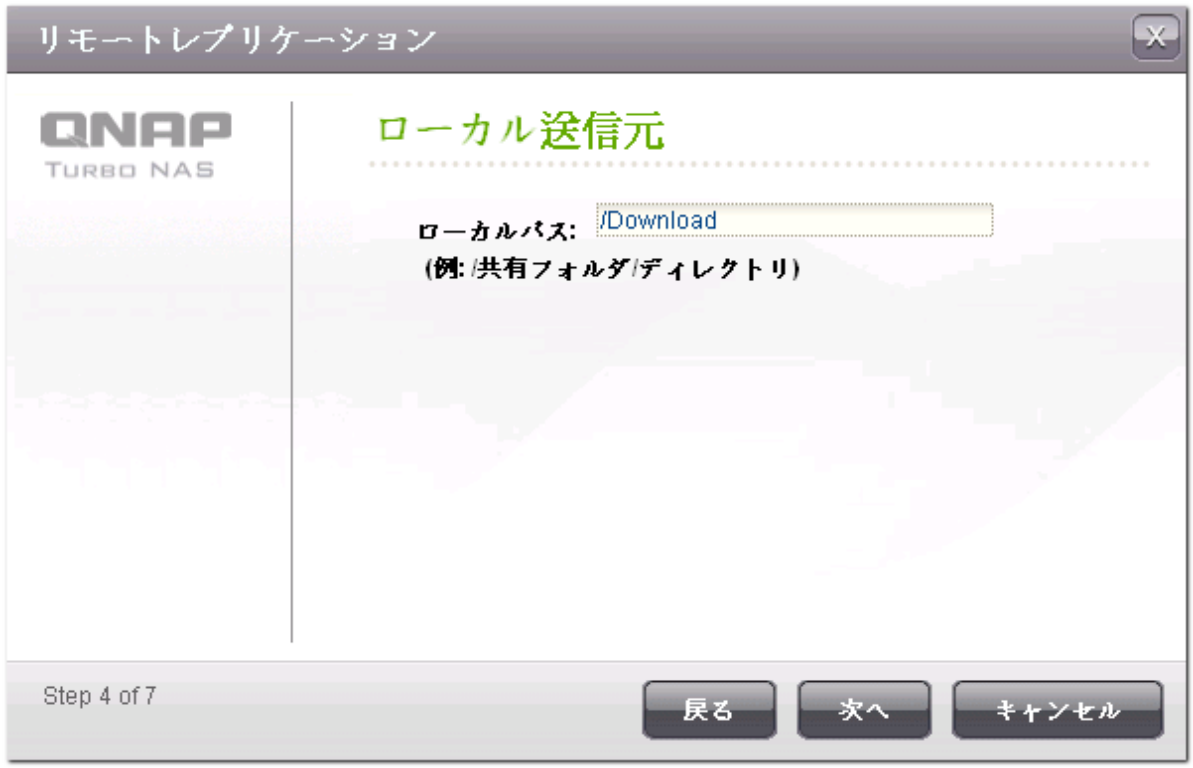
IPアドレス、ポート番号、ユーザー名、パスワードを入力してリモートサーバーにログインします。デフォルトのポート番号:は873です。ログインユーザー名はリモートサーバーに対して読み込み/書き込みアクセス権、およびサーバー上での十分な割当制限を持つ必要があります。「TEST（テスト）」をクリックして接続を確認します。「NEXT（次へ）」をクリックします。



データを複製する、宛先フォルダを指定します。



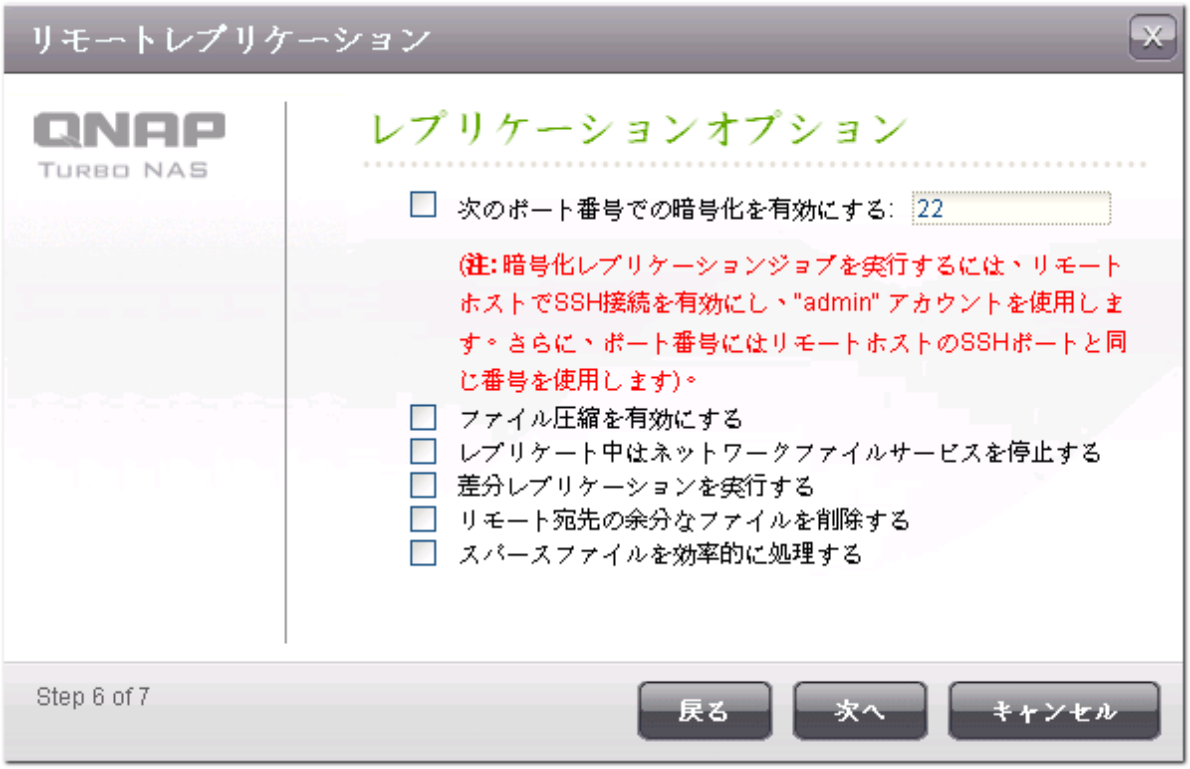
データの複製元となる、ローカルフォルダを指定します。



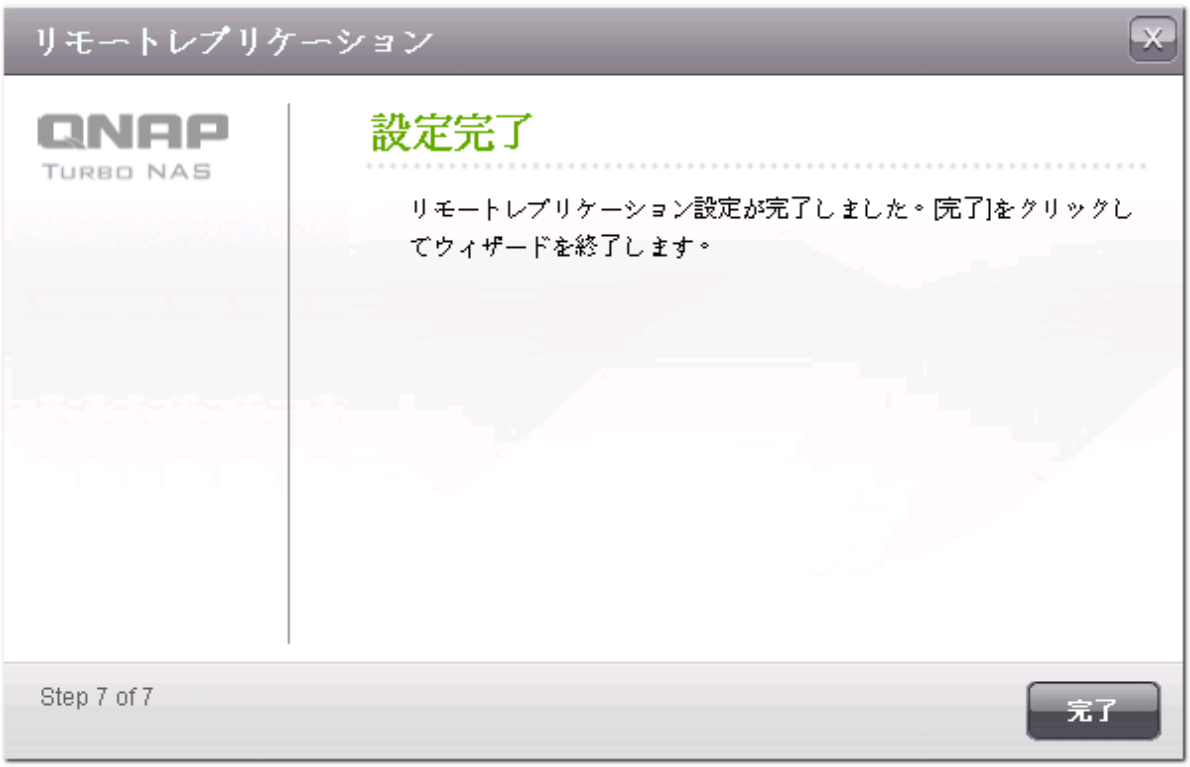
直ちにデータを複製するように選択するか、バックアップスケジュールを指定します。

リモートレプリケーションジョブに対して、他のオプションを指定します。

- 暗号の有効化：このオプションを選択して、暗号化されたリモートレプリケーションを実行します。「ネットワークサービス」>「テルネット/SSH」で「SSH接続を許可する」をオンにし、SSHと暗号化されたリモートレプリケーションに対して同じポート番号を指定する必要があります。
- ファイル圧縮のアクティブ化：データ転送プロセスの間圧縮を可能にするには、このオプションをオンにします。低バンド幅環境またはWAN上でのリモートレプリケーションに対して、このオプションを推奨します。
- 複製中は、ネットワークファイルサービスを停止してください。リモートレプリケーションの進行中は、Samba（SMB）、AFP、およびFTP経由でのNASへの接続をすべて停止してください。
- 増分レプリケーションの実施：このオプションがオンになっているとき、最初のレプリケーション後、NASは最後のバックアップ以後に変更されたファイルのみをバックアップします。同じ名前、サイズ、変更された時間のファイルは再びコピーされません。バックアップ時間を短縮するために、何回も実行されるレプリケーションジョブに対してこのオプションをオンにするようにお勧めします。
- リモート宛先の余分なファイルを削除します。ソースデータを宛先データと同期するオプションを選択します（一方向の同期化）。宛先の余分なファイルは削除されます。ソースデータは変更されません。
- スパースファイルの効率的な処理：スパースファイルは、ゼロタイプのデータの大きなブロックを含む一種のコンピュータファイルです。このオプションをオンにすると、リモートレプリケーションに必要な時間が短縮されます。



「FINISH（終了）」をクリックします。ジョブは、スケジュールに従って実行されます。ジョブは繰り返し用いられます。リモートレプリケーションの実行中は、ローカルNASとリモートサーバーをオフにしないでください。

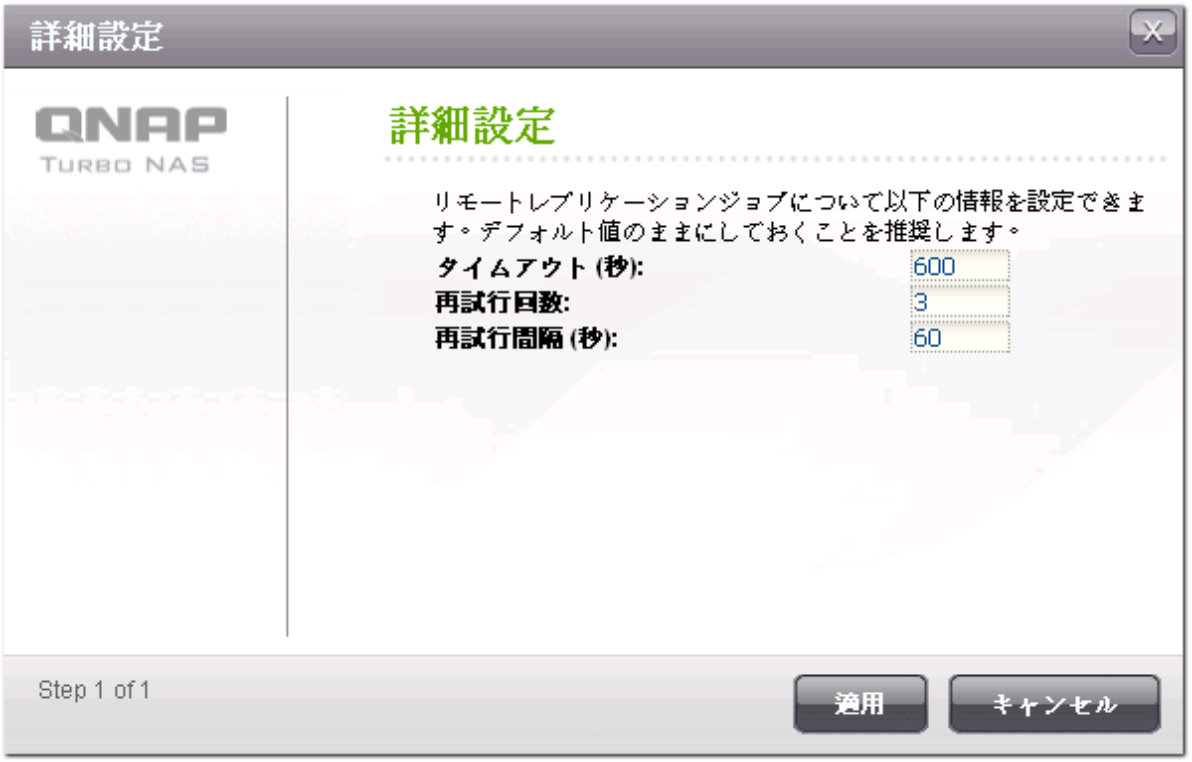


アイコン	説明
	直ちに、レプリケーションジョブを開始します。
	実行中のレプリケーションジョブを停止します。
	再同期ログを表示します（レプリケーション結果）。
	レプリケーションジョブを編集します。
	レプリケーションスケジュールを無効にします。
	レプリケーションスケジュールを有効にします。

レプリケーションジョブのタイムアウトと再試行設定を設定するには、「Options（オプション）」をクリックします。

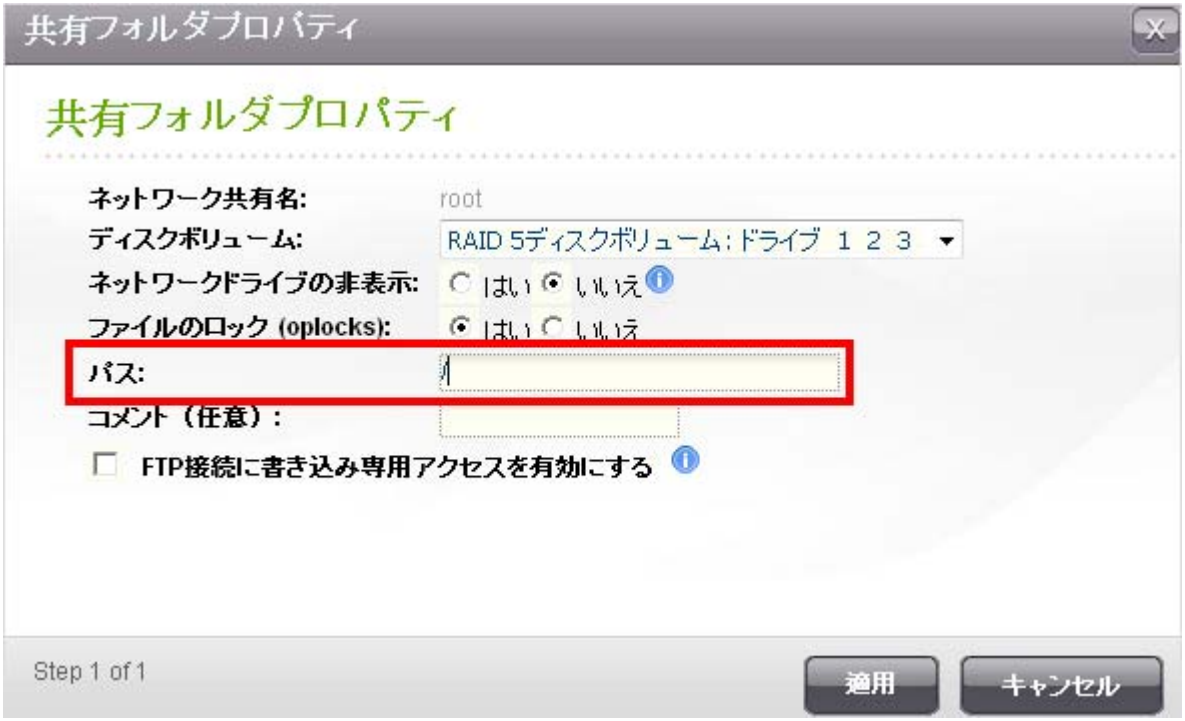
- タイムアウト（秒）：レプリケーションジョブごとのタイムアウト値を指定します。これは、データが届かない場合、レプリケーションジョブがキャンセルされるまで待つ最大の秒数です。
- 再試行回数：NASがレプリケーションジョブが失敗した場合、再試行する回数を指定します。
- 再試行間隔（秒）：各試行間に待つ秒数を指定します。

例えば、タイムアウトに対して600秒、3回の再試行、再試行間隔に対して60秒を入力した場合、データを受け取らなければレプリケーションジョブは600秒でタイムアウトになります。NASは60秒待ち、2度目のジョブを試みます。ジョブが再びタイムアウトになると、NASはさらに60秒間待ち、ジョブの実行をさらに試みます。



リモートアプリケーション(rsync)によりディスクボリュームにすべての共有をバックアップするには、どうすればいいのですか?

リモートレプリケーション(rsync)でディスクボリュームにすべての共有をバックアップするには、ルートディレクトリとして(例えば、root)同じボリュームにすべてのフォルダを含むネットワーク共有を作成し、「/」にパスを指定します。 次に、リモートレプリケーションジョブを作成してこの共有(root)をコピーします。 すべてのフォルダとサブフォルダが複製されます。



RTRRレプリケーション

リアルタイムリモートレプリケーション(RTRR)は、ローカルNASとリモートNAS、FTPサーバー、または外部ドライブ間でリアルタイムのまたはスケジュールされたデータレプリケーションを、または2つのローカル共有フォルダ間のレプリケーションを提供します。リアルタイムモードでは、ソースフォルダがモニタされ、新規の、変更された、名前を変更されたファイルが直ちにターゲットフォルダに複製されます。スケジュールモードでは、事前定義されたスケジュールに従ってソースフォルダがターゲットフォルダに複製されます。

バックアップ宛先がNASの場合、まずリモートNASでRTRRサーバー(「アプリケーションサーバー」>「バックアップサーバー」>「RTRRサーバー」) またはFTPサービス(「ネットワークサービス」>「FTPサービス」)を有効にする必要があります。

NASモデル	**ファームウェア**	**サポートされるレプリケーションジョブの最大数**
IntelベースのNAS	v3.5.0以前	64*
	v3.5.0以降	32*
ARMベース(非Intelベース)NAS	v3.5.0以前	RTRRレプリケーションはサポートされていません。
	v3.5.0以降	8*

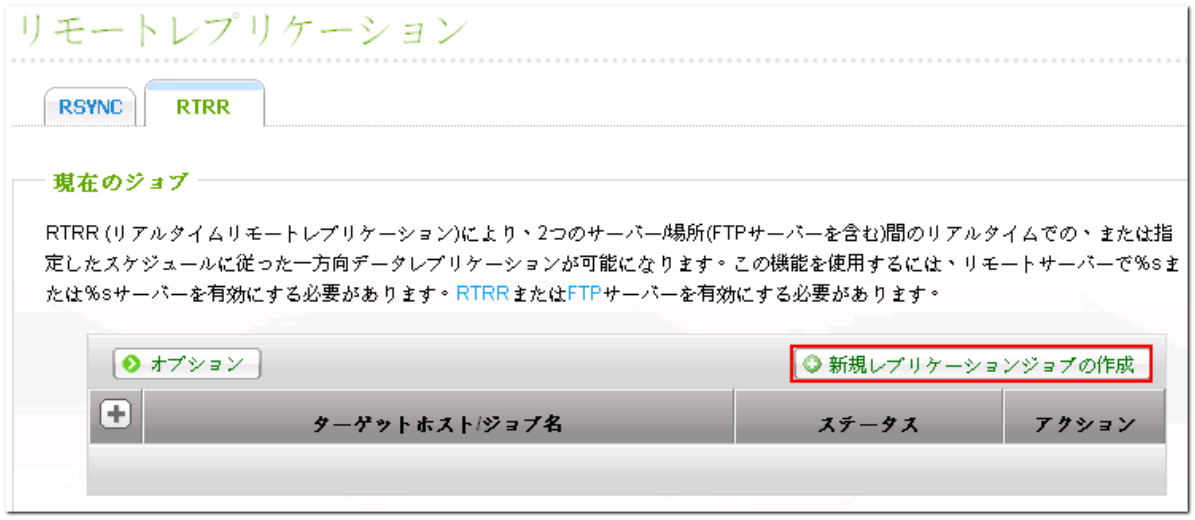
*各ジョブは、最大5つのホルダペアをサポートします。

NASモデルが以下に一覧されていない場合、http://www.qnap.com にアクセスして詳細をご確認ください。

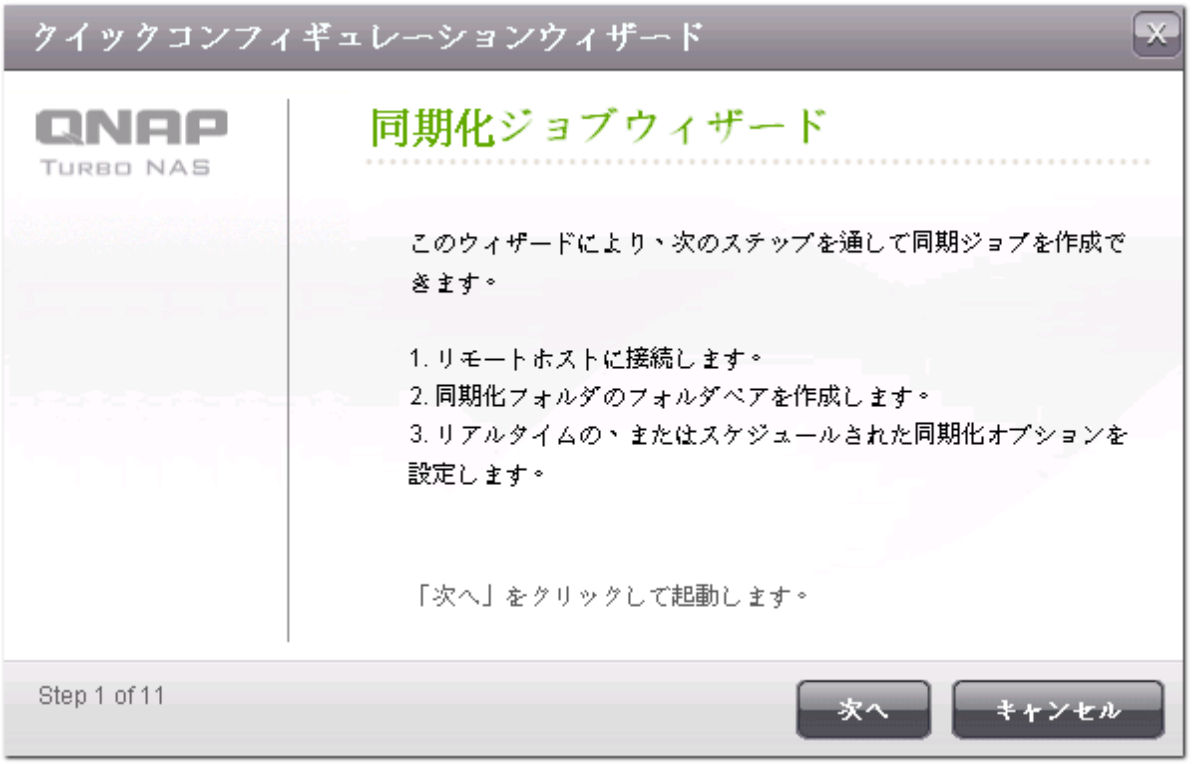
IntelベースのNAS	TS-x39シリーズ、TS-x59シリーズ、TS-509、TS-809、TS-809 Pro、TS-809U-RP、SS-439 Pro、SS-839 Pro、TS-x59 Pro+、TS-879 Pro、TS-1079 Pro、TS-879U-RP、TS-EC879U-RP、TS-1279U-RP、TS-EC1279U-RP
ARMベース(非Intelベース)NAS	TS-109、TS-209、TS-409、TS-409U、TS-x10、TS-x12、TS-x19シリーズ

以下のステップに従ってレプリケーションジョブを作成します。

リアルタイムまたはスケジュールされたリモートレプリケーションを作成するには、「新規レプリケーションジョブの作成」をクリックします。



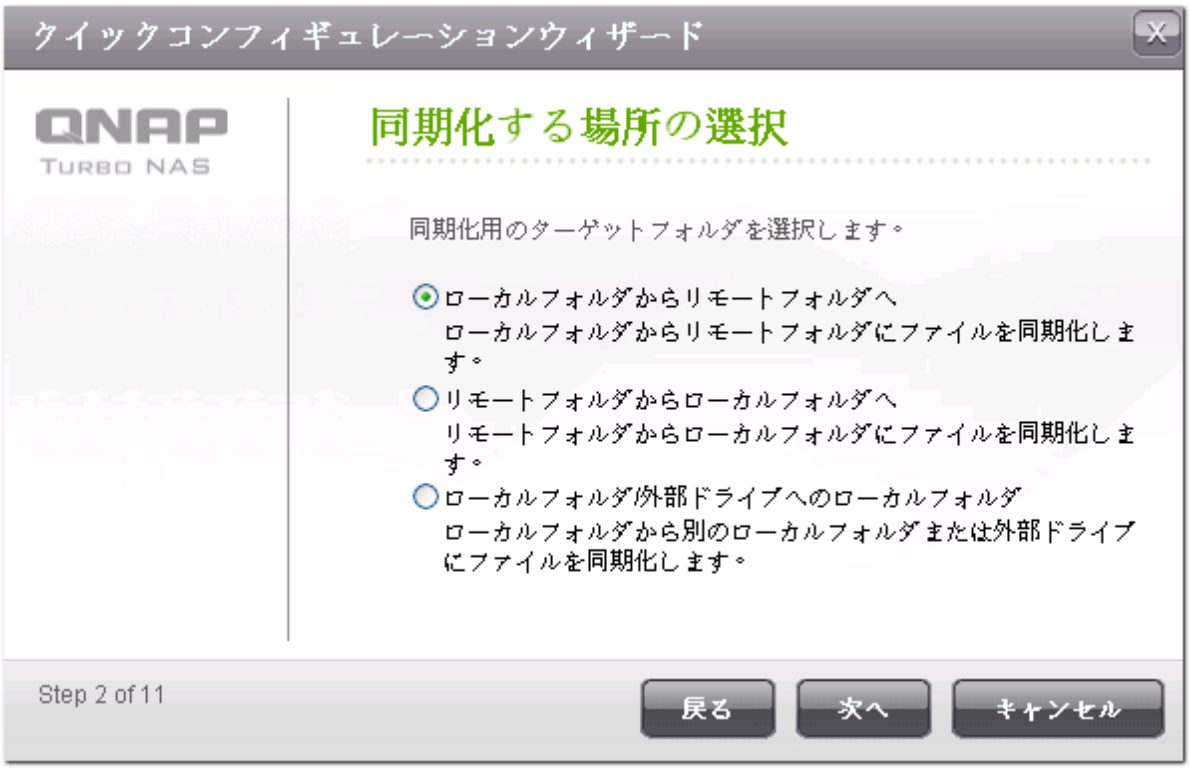
ウィザードが表示されたら、「NEXT（次へ）」をクリックします。



同期場所を選択します。宛先デバイスがフォーマットされ、共有フォルダが作成されていることを確認してください。NASは、以下をサポートします。

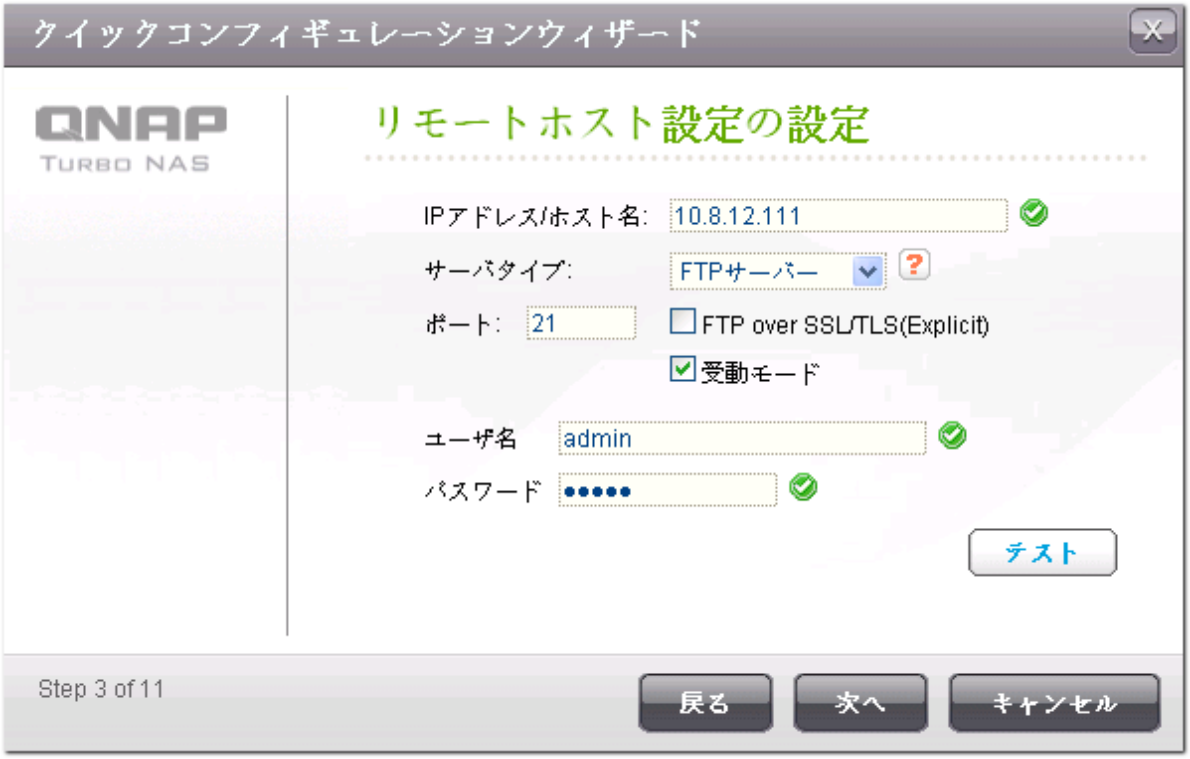
- ローカルフォルダからリモートフォルダ（NASまたはFTPサーバー）に対してデータを同期化します。
- リモートフォルダ（NASまたはFTPサーバー）からローカルフォルダに対してデータを同期化します。
- ローカルフォルダから別のローカルフォルダまたは外部ドライブに対してデータを同期化します。

「NEXT（次へ）」をクリックします。

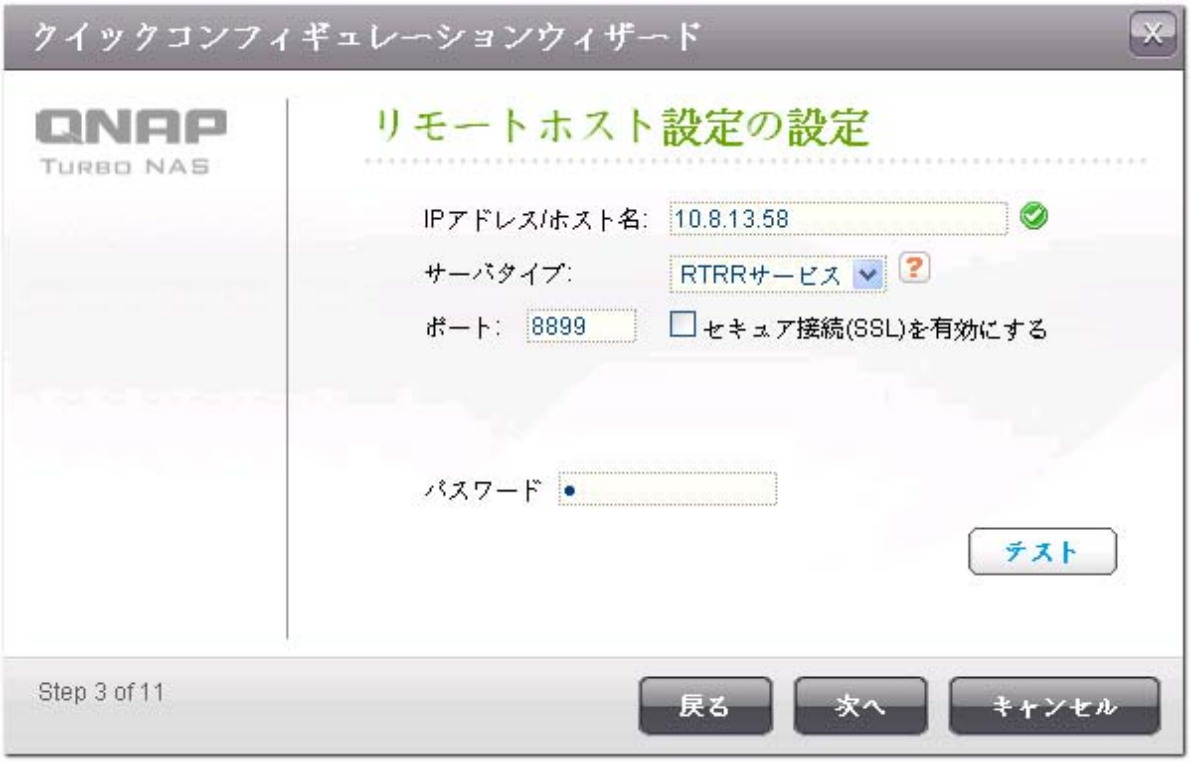


IPアドレスまたはホスト名を入力します。サーバータイプを選択します（RTRRサービスを有効にしたFTPサーバーまたはNASサーバー）。

FTPサーバーへのリモートレプリケーション:
暗号化されたデータを転送するために、ポート番号および、FTPをSSL/TLS (Explicit)でFTPを有効にするかどうかを指定します。FTPサーバーがファイアウォールの背後にある場合、パッシブモードを有効にします。サーバーに対して読み込み/書き込みアクセス権を持つユーザー名とパスワードを入力します。「NEXT(次へ)」をクリックします。



NASとRTRRサービスに対するリモートレプリケーション:
RTRRサービス対応サーバーのIPアドレスを入力します。接続ポートを指定し、安全な接続を有効にするかどうかを選択します。RTRR接続用のパスワードを入力します。「NEXT(次へ)」をクリックします。



データ同期化用のフォルダペアを選択します。

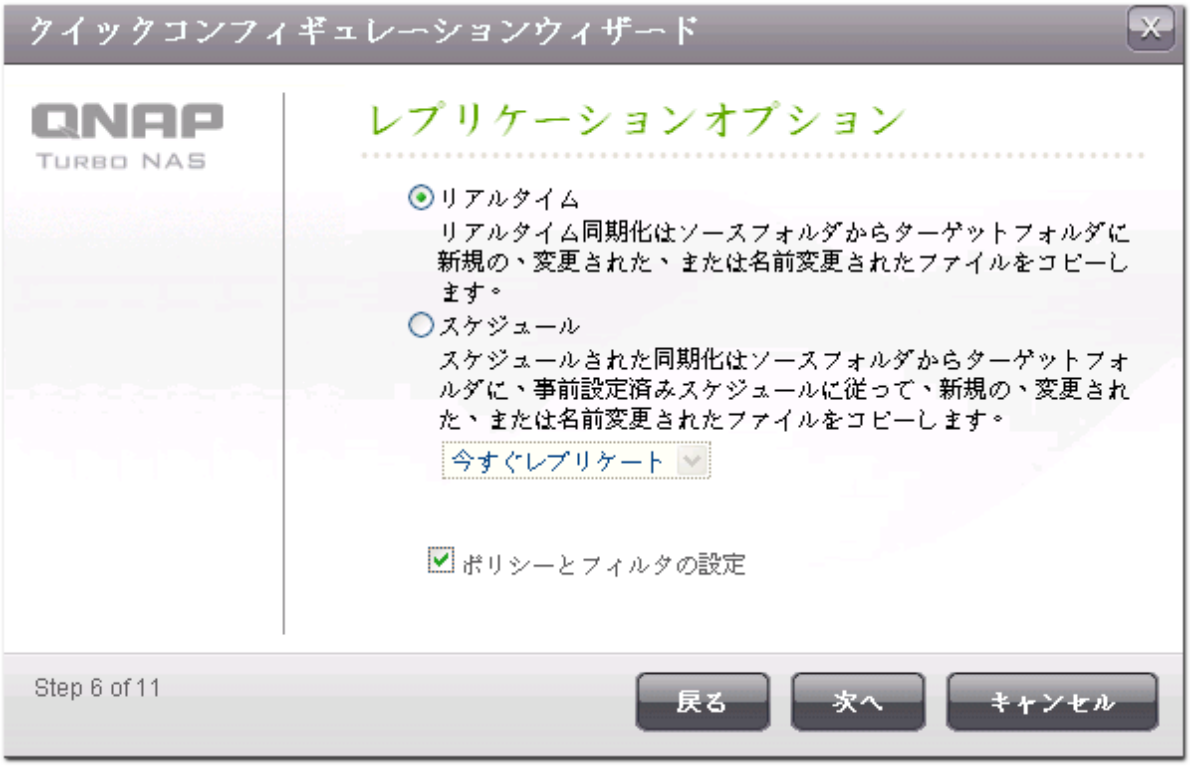
注: レプリケーションジョブのフォルダペアでソースまたは宛先としてあるフォルダまたはその親フォルダまたは子フォルダが選択されている場合、同じジョブの別のフォルダペアのソースまたは宛先としてフォルダを選択できません。

バックアップに対してさらに多くのフォルダペアを追加するには、「さらにフォルダペアを追加する」を選択します。
各同期ジョブは、最大5つのフォルダペアをサポートします。フォルダペアを選択し、「ADD（追加）」をクリックします。「NEXT（次へ）」をクリックします。

リアルタイムとスケジュールされた同期化から選択します。 最初のバックアップ後変更が行われると直ちに、リアルタイム同期化は、新しいファイル、またソースフォルダからターゲットフォルダに変更または名称変更されたファイルをコピーします。

スケジュールされた同期化は、事前設定されたスケジュールに従って、ソースフォルダからターゲットフォルダにファイルをコピーします。 オプションは以下の通りです:

- 今複製する: データを直ちに複製します。
- 周期的に: バックアップが実行される間隔を、時間と分で入力します。 最小の時間間隔は5分です。
- 毎時: 毎時のバックアップスケジュールを実行するときの分を指定します。例えば、01を入力すると、1時間ごとに最初の分のバックアップを入力します。1:01、2:01、3:01...
- 毎日: 毎日のバックアップを実行する時刻を指定します。例えば、毎日の02:02。
- 毎週: 毎週のバックアップを実行する曜日と時刻を選択します。
- 毎月: 毎月のバックアップを実行する日と時刻を選択します。



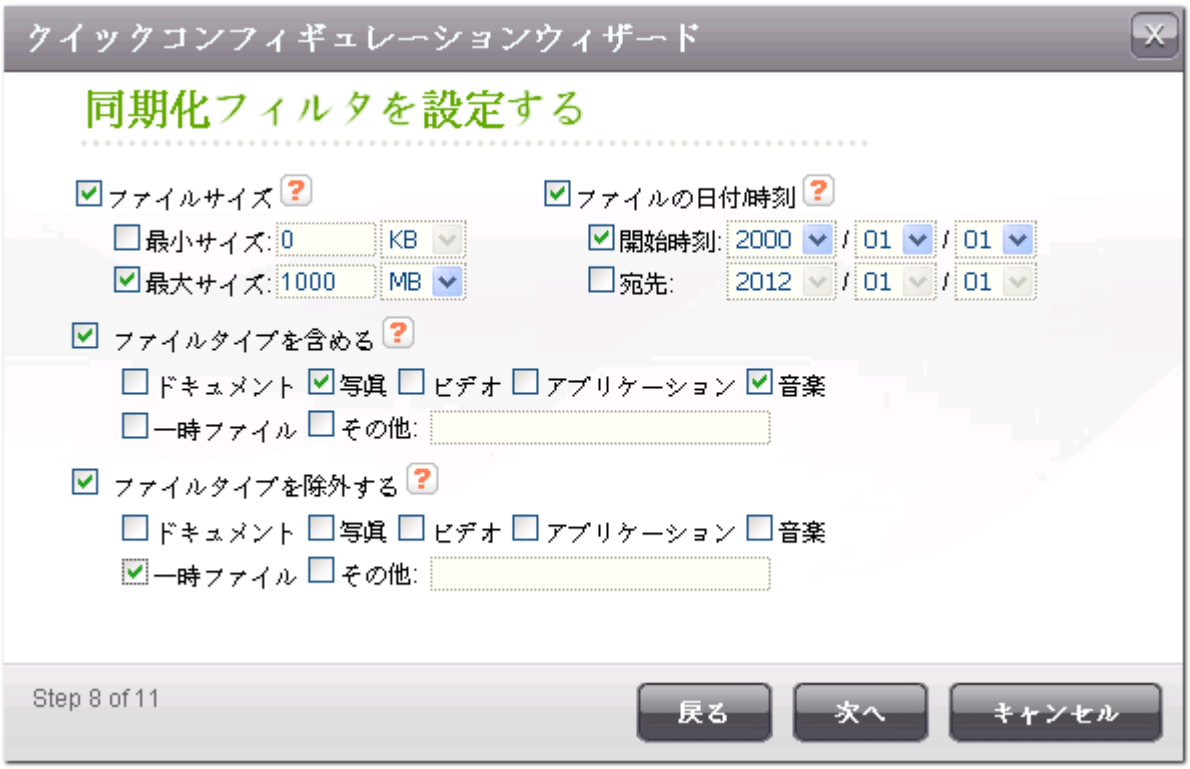
同期化ポリシーを設定するには、「ポリシーとフィルタの設定」を選択し、「NEXT（次へ）」をクリックします。

次のオプションを有効にするかどうかを選択します。

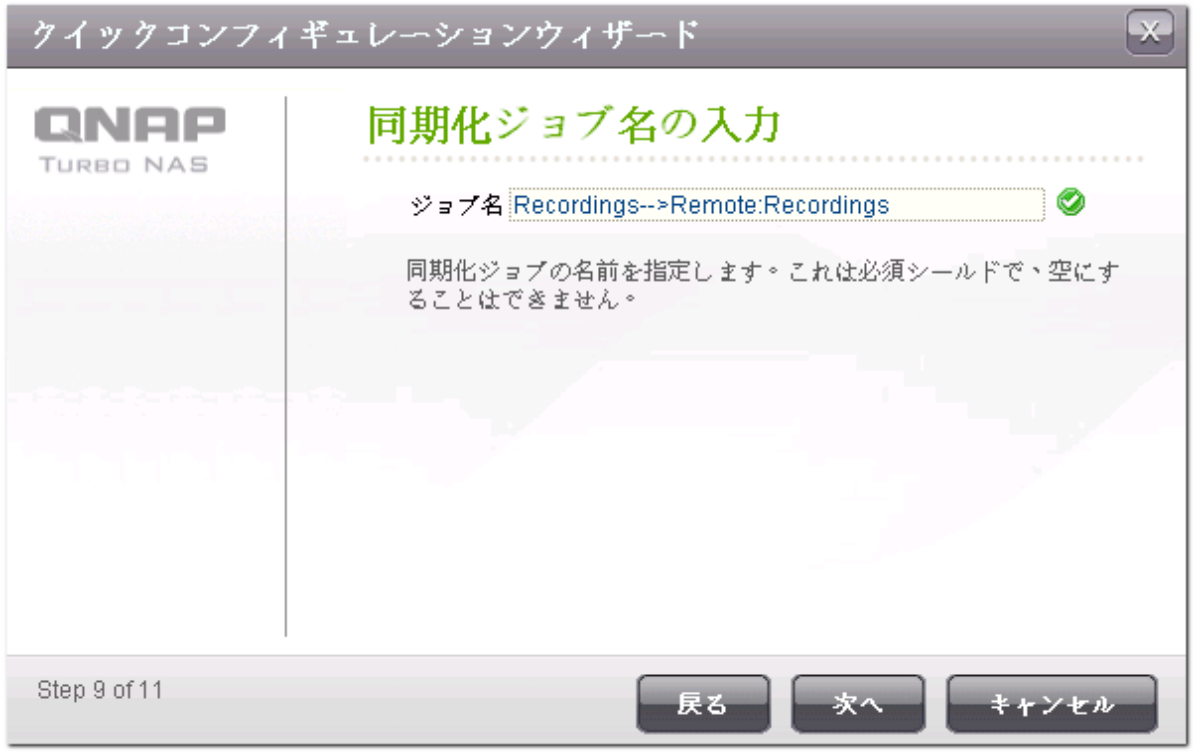
- 余分のファイルの削除：ターゲットフォルダの余分なファイルを削除します。ソースフォルダで実行された削除は、ターゲットフォルダで繰り返されます。リアルタイム同期化の場合、このオプションは使用できません。
- スパースファイルの削除：ヌルデータのファイルを無視するには、このオプションを選択します。
- ファイルコンテンツの確認：2つのファイルが同じかどうかを判断するには、ファイルコンテンツ、日付、サイズ、名前の検査を指定します。リアルタイム同期化の場合、このオプションは使用できません。
- 送信間のファイルの圧縮：同期操作用にファイルを圧縮するかどうかを指定します。多くのCPUリソースが消費されることにご注意ください。
- シンボリックリンクの無視：ペアフォルダのシンボリックリンクを無視するには、このオプションを選択します。
- 拡張属性：拡張属性で情報を維持するには、このオプションを選択します。
- タイムアウトと再試行設定：同期操作が失敗した場合、タイムアウト期間と再試行設定を指定します。

ファイルサイズ、含有/除外するファイルタイプ、データ同期化をフィルタするファイル日付/時刻を指定できます。

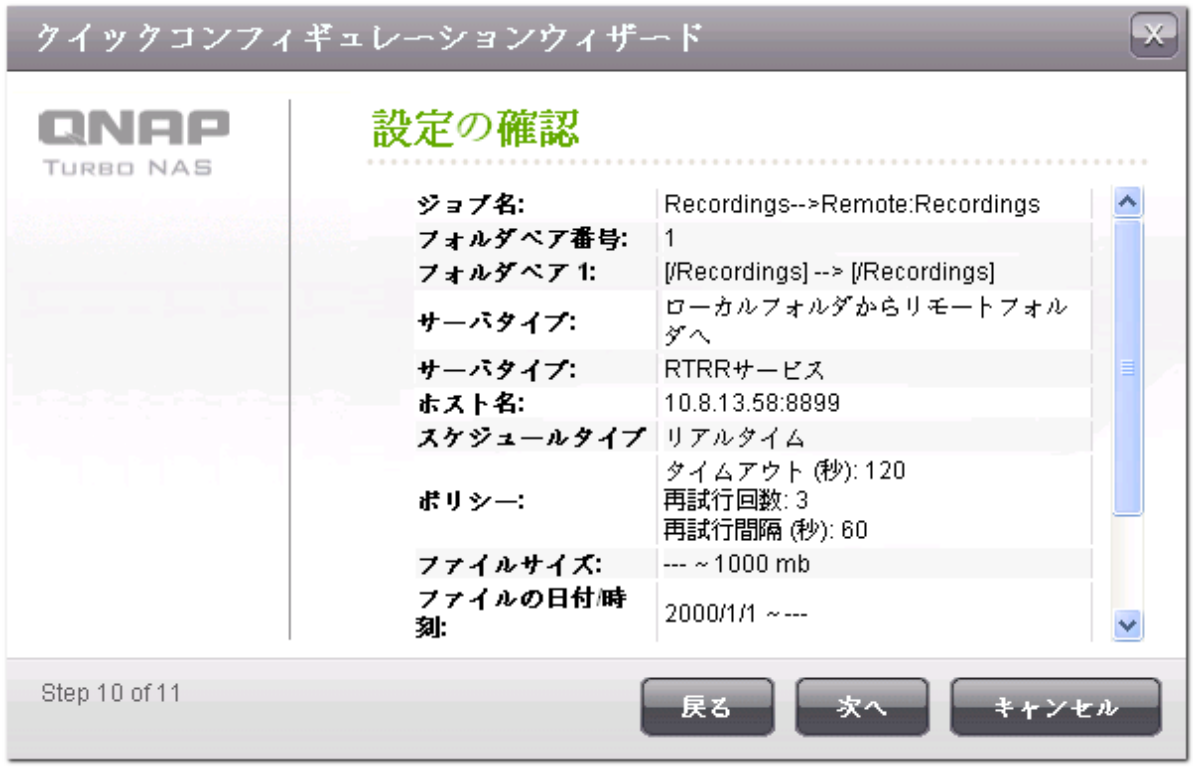
- ファイルサイズ：複製するファイルの最小および最大サイズを指定します。
- ファイルタイプの含有：複製するファイルタイプを指定します。
- ファイルタイプの除外：レプリケーション用に除外するファイルタイプを指定します。
- ファイル日付/時刻：複製するファイルの日付と時刻を指定します。



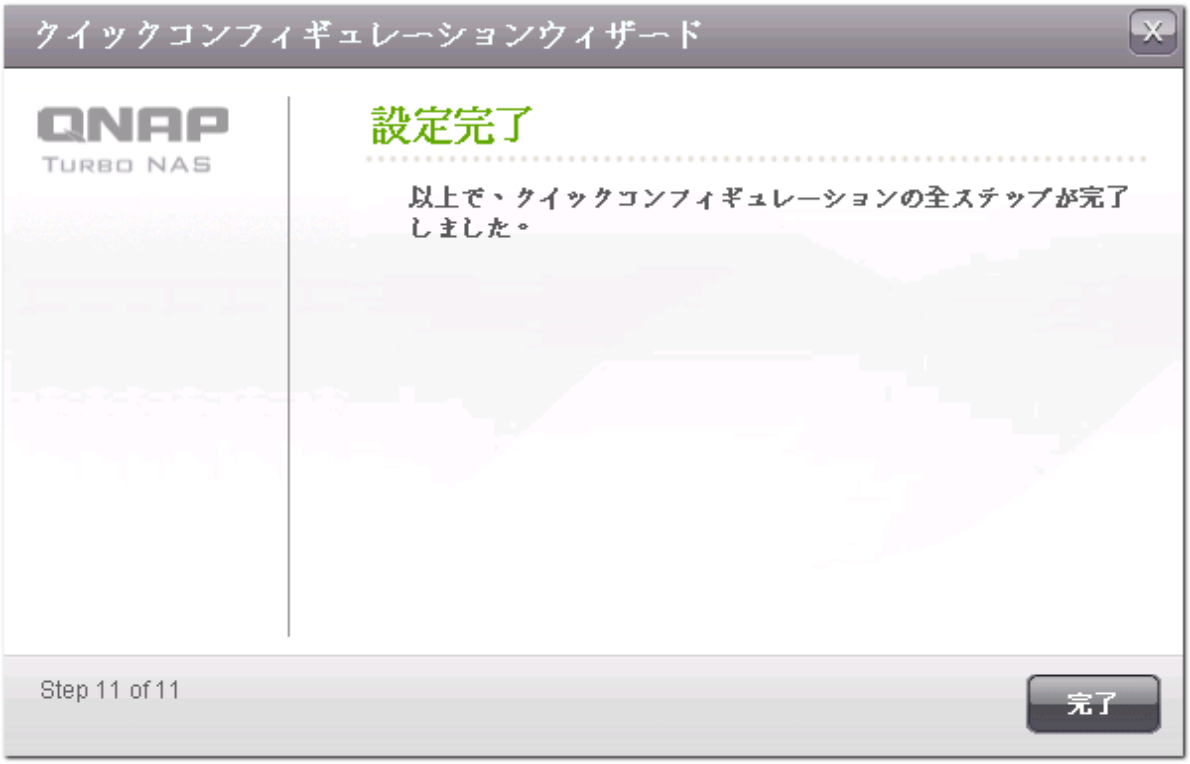
ジョブ名を入力します。「NEXT（次へ）」をクリックします。



設定を確認し、「NEXT（次へ）」をクリックします。



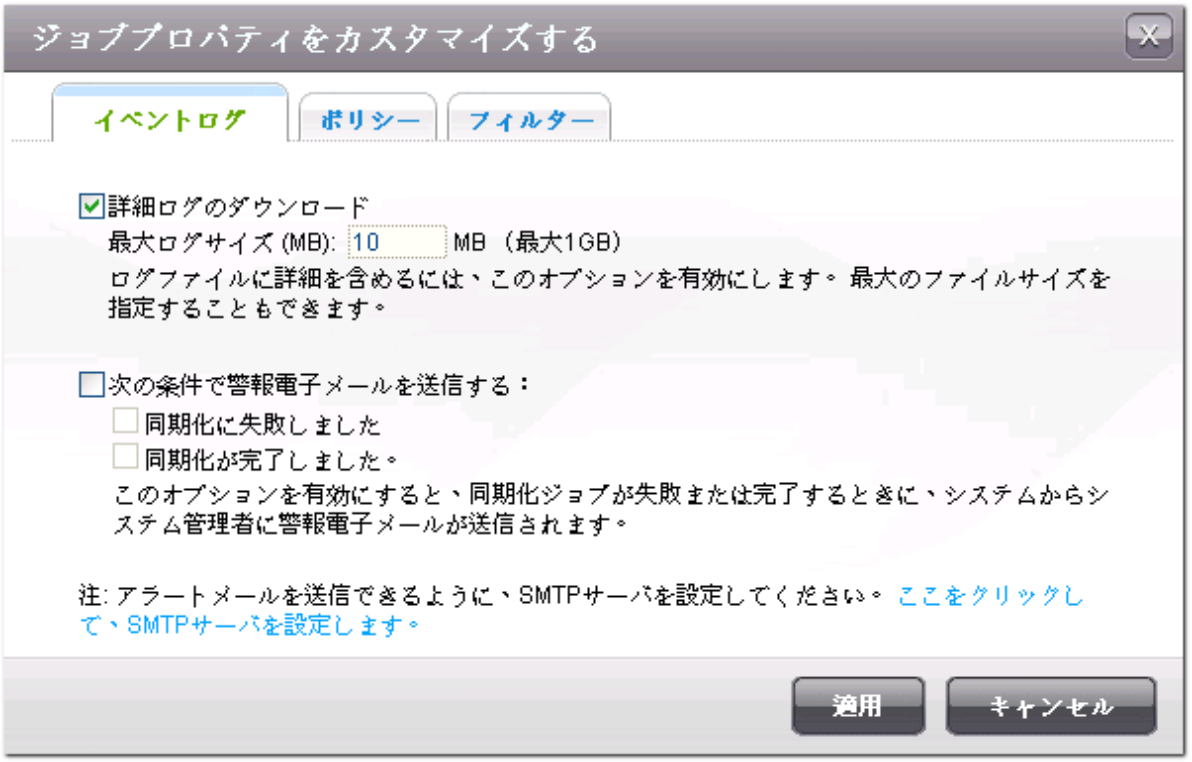
「FINISH（終了）」をクリックしてウィザードを終了します。



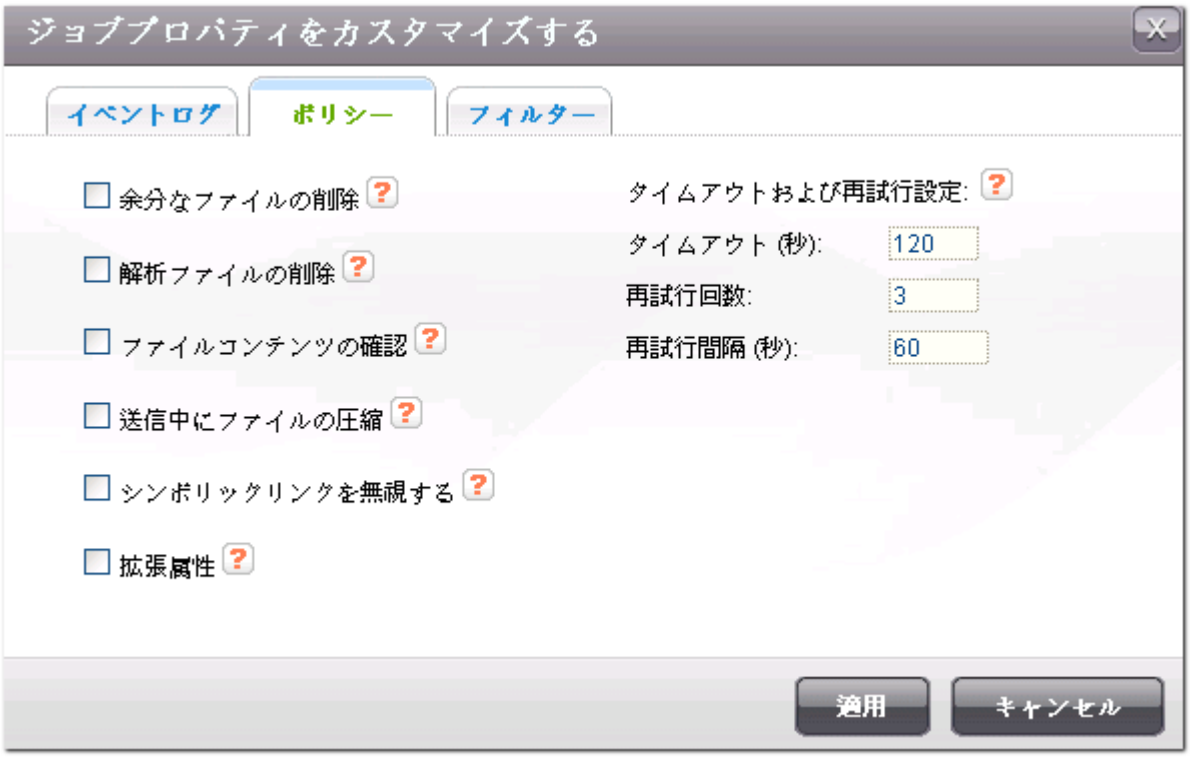
アイコン	説明
	• リモートサーバーへの接続を有効にします。 • レプリケーションジョブを開始します。
	リモートサーバーまたは外部ドライブへの接続を停止します。
	レプリケーションジョブを停止します。
	ジョブステータスとログ、ダウンロードログを表示します。
	• リモートサーバーの接続設定を編集します。 • レプリケーションジョブの設定を編集します。
	• リモートサーバーへの接続設定を削除します。 • レプリケーションジョブを削除します。 このボタンは、レプリケーションジョブがまたはリモートサーバーへの接続が停止した後でのみ使用できます。

レプリケーションジョブプロパティを編集するには、「Options(オプション)」をクリックします。

「Event Logs(イベントログ)」の下で、「詳細ログのダウンロード」を選択して有効にし、ログファイルの最大のファイルサイズを指定することができます。同期化の失敗や完了時に電子メールアラートを送信するように、選択することもできます。SMTPサーバー設定をNAS(「Download Detailed Logs(システム管理)」>「Notification(通知)」)で適切にセットアップする必要があることにご注意ください。



「Policy(ポリシー)」でレプリケーションポリシーを、「Filter(フィルタ)」でフィルタ設定を指定します。これらはすべてのRTRRレプリケーションジョブでデフォルトの設定です。



レプリケーションジョブログのダウンロード:

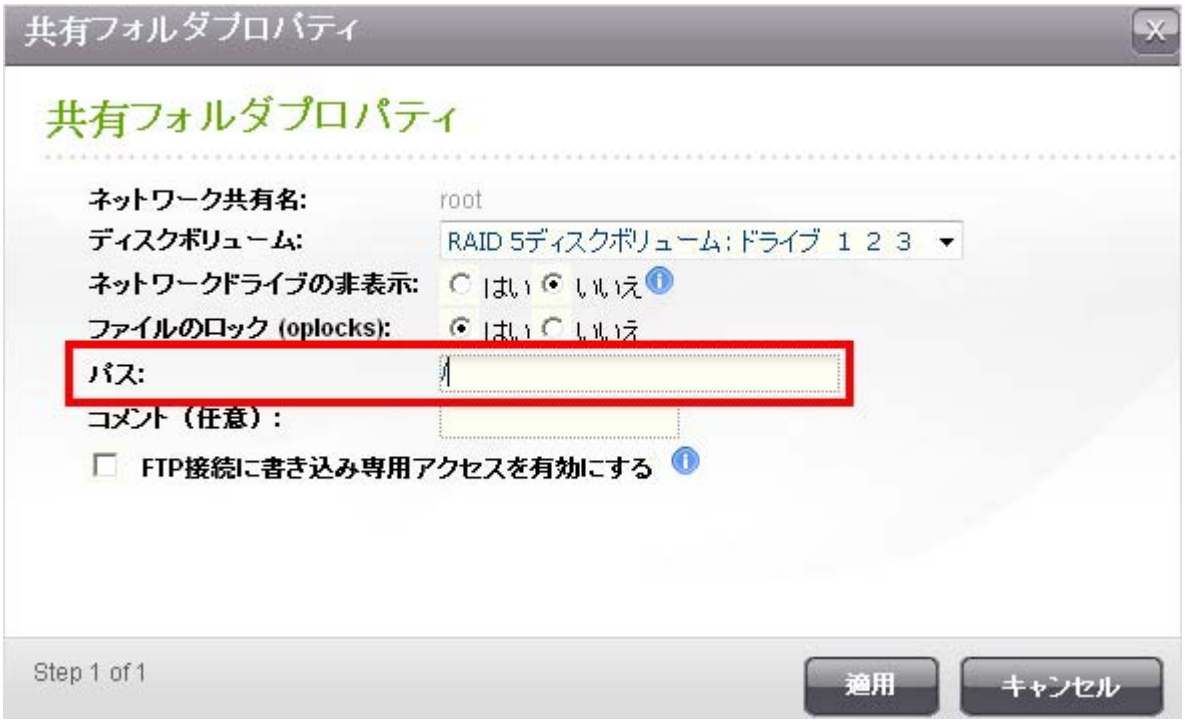
レプリケーションジョブのステータスとログを表示するには、 をクリックします。

レプリケーションジョブの詳細を表示できます。

「Download Logs（ログをダウンロードする）」をクリックすることで、ジョブログを表示したり、ログをダウンロードしたりできます。ログファイルは、Microsoft Excelまたはその他のテキストエディタソフトウェアで開くことができます。このボタンは「Download Detailed Logs(オプション)」 > 「Options(イベントログ)」で「Event Logs(詳細ログのダウンロード)」を有効にし、レプリケーションジョブを一度実行した後でのみ利用できることにご注意ください。

ディスクボリューム全体のリモートレプリケーションジョブの作成方法

リモートレプリケーションによってディスクボリュームの全体をバックアップするには、同じボリュームにすべての共フォルダを含むをルートディレクトリとして新しい共フォルダ(例えば、ルート)を作成し、パスを '/' に指定します。次にリモートレプリケーションジョブを作成し、この共フォルダ (ルート) をコピーします。共フォルダとサブフォルダのすべてが複製されます。

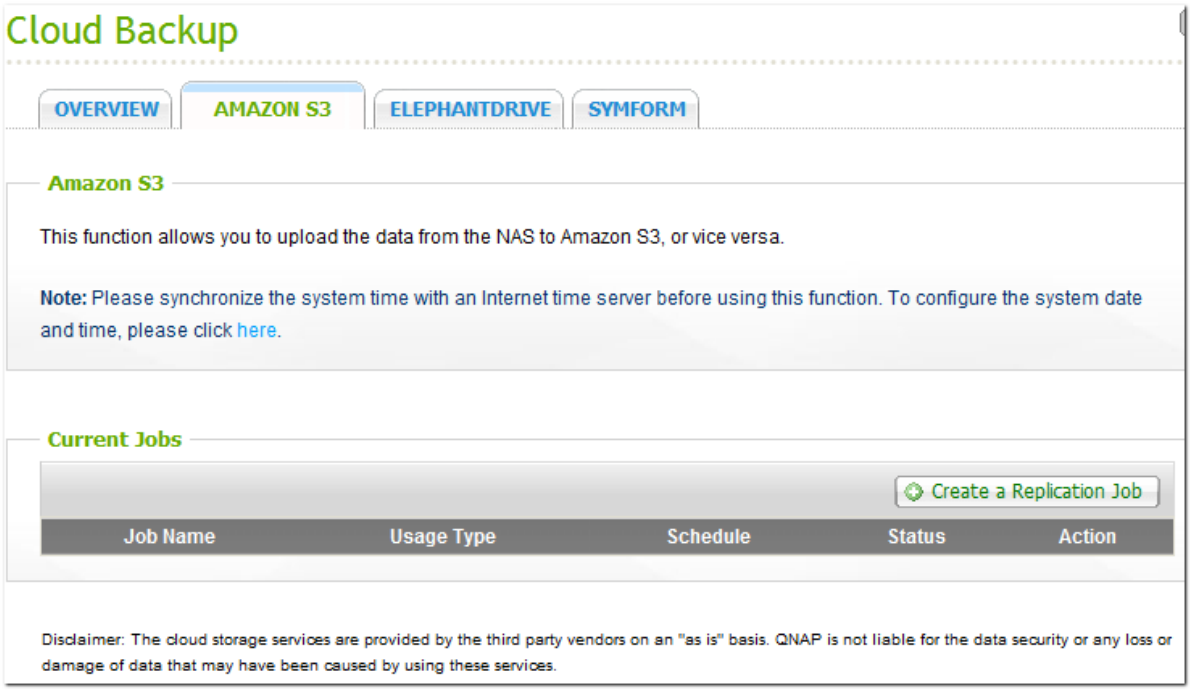


8.2 クラウドバックアップ

Amazon S3

Amazon S3 (シンプルストレージサービス、Simple Storage Service) はAWS (Amazonウェブサービス、Amazon Web Services) が提供するオンラインストレージウェブサービスです。明快なウェブサービスインターフェイスにより、ウェブ上のどこからでもデータを保管または取得することができます。Amazon S3により、NASからAmazon S3 へのデータアップロード、またはAmazon S3 からNASへのデータダウンロードが可能です。

http://aws.amazon.com よりAWSアカウントに登録し、サービスを購入する必要があります。ご注意ください。アカウントにサインアップした後、一つ以上のバケット (ルートフォルダ) をAmazon S3アプリケーションによりAmazon S3に作成する必要があります。初心者の方には、Mozilla Firefoxのアドオン "S3Fox" をお勧めします。



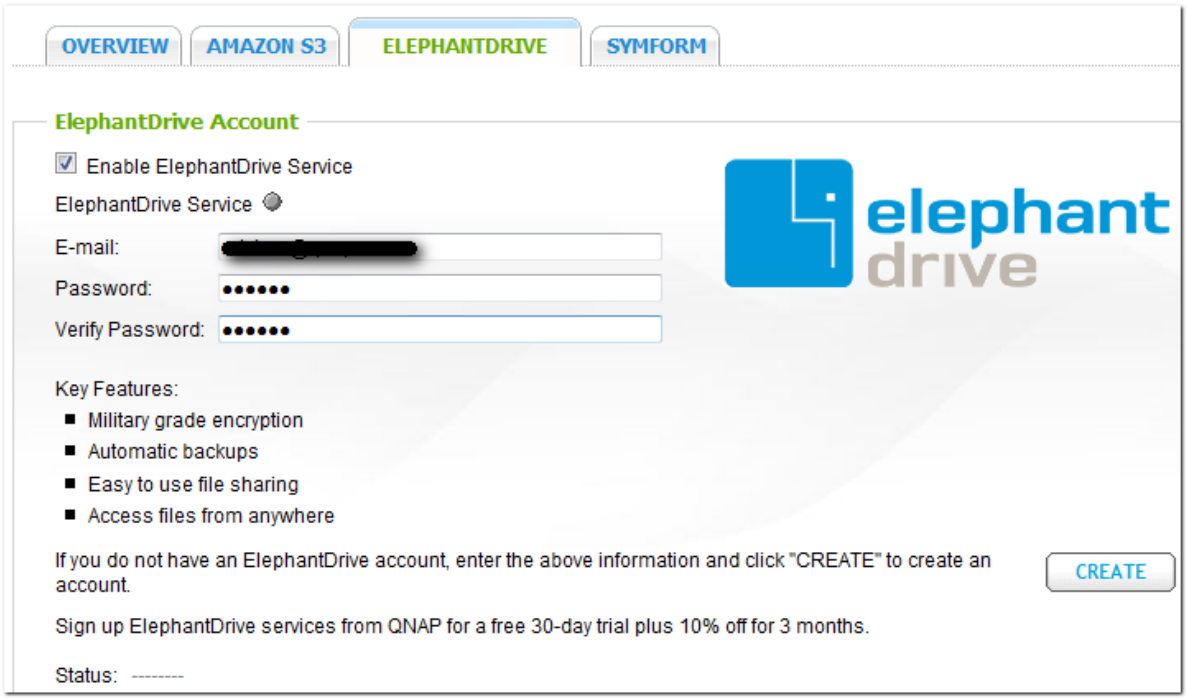
Amazon S3アカウントをセットアップした後、以下の手順に従い、NASを使用してAmazon S3へデータのバックアップ、またはAmazon S3からデータを取得してください。

1. "Create New Replicating Job" (新規レプリケーションジョブの作成)をクリックします。
2. リモートレプリケーションジョブ名を入力します。
3. 使用タイプを選択します: "Upload" (アップロード) あるいは "Download" (ダウンロード) を選択肢、その他の設定を入力します。バケットとはAmazon S3のルートディレクトリのことです。"TEST" (テスト) をクリックすると、リモートホストテストが可能です。その他の設定はオプションとなります。

4. レプリケーション用のNASのローカルディレクトリを指定します。
5. レプリケーションスケジュールを入力します。
6. "Finish" (終了) をクリックします。 スケジュールに合わせてレプリケーションジョブが実行されます。

ElephantDrive

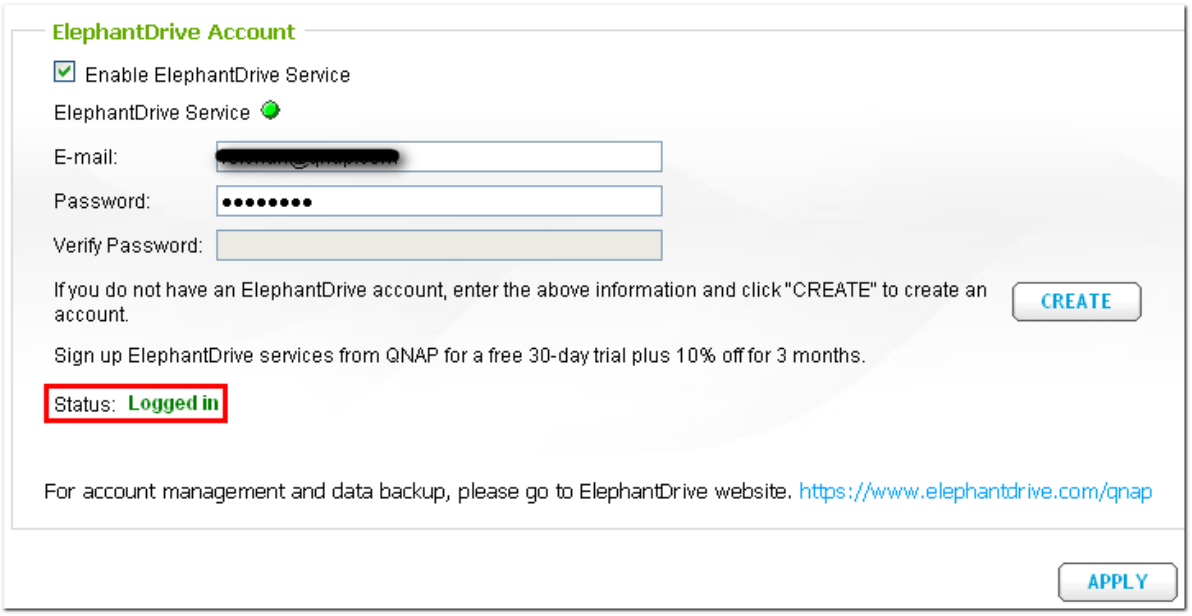
ElephantDriveサービスを使用するには、「ElephantDriveサービスを有効にする」を選択してください。ElephantDriveサービスの電子メールとパスワードを入力します。 アカウントをお持ちでない場合、情報を入力し、「Create（作成）」をクリックします。



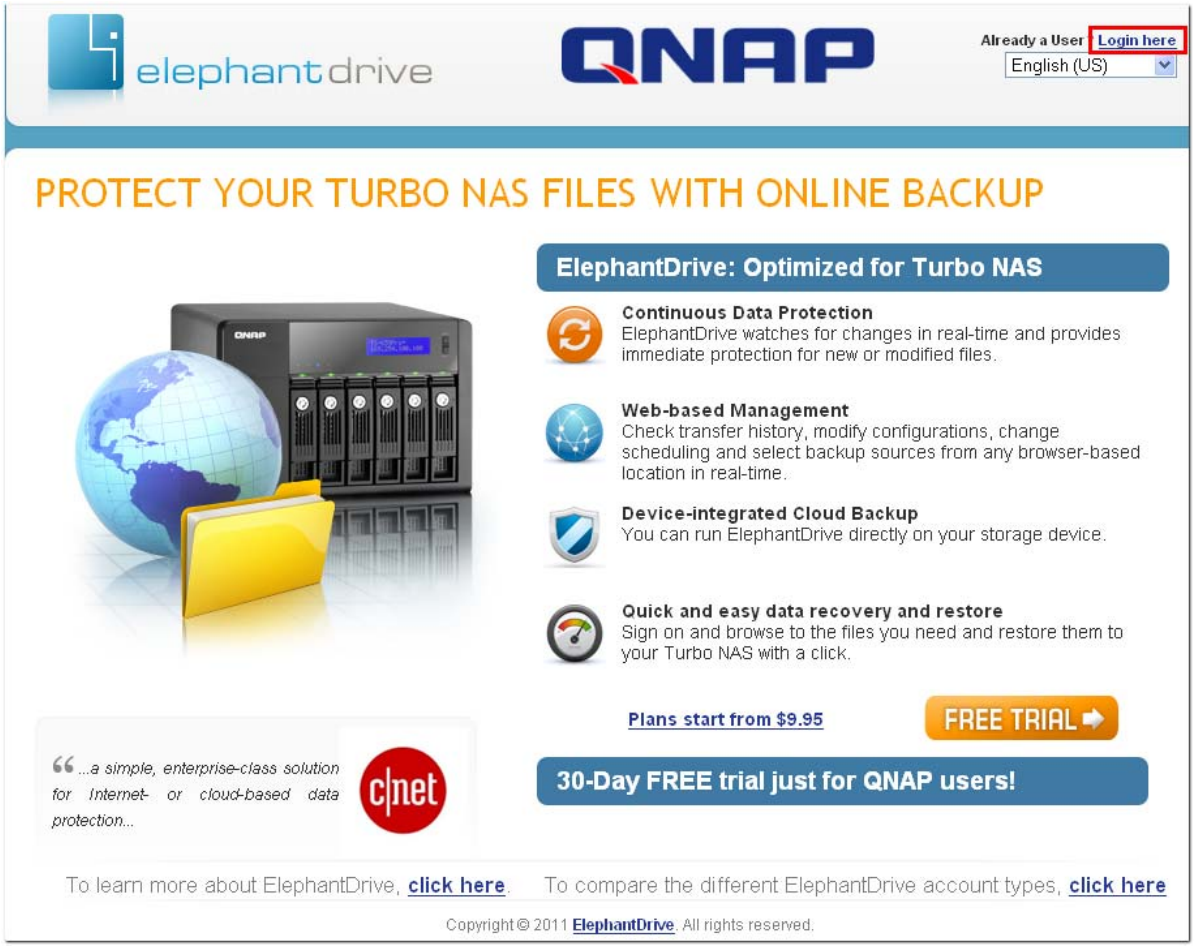
「OK」をクリックして確認します。

アカウントの作成後、「APPLY（適用）」をクリックします。 NASは、ElephantDriveサービスへのログインをお手伝いいたします。

NASのElephantDriveサービスにログインした後、ElephantDrive Webサイト（http://www.elephantdrive.com/qnap　）にアクセスしてバックアップを管理することができます。

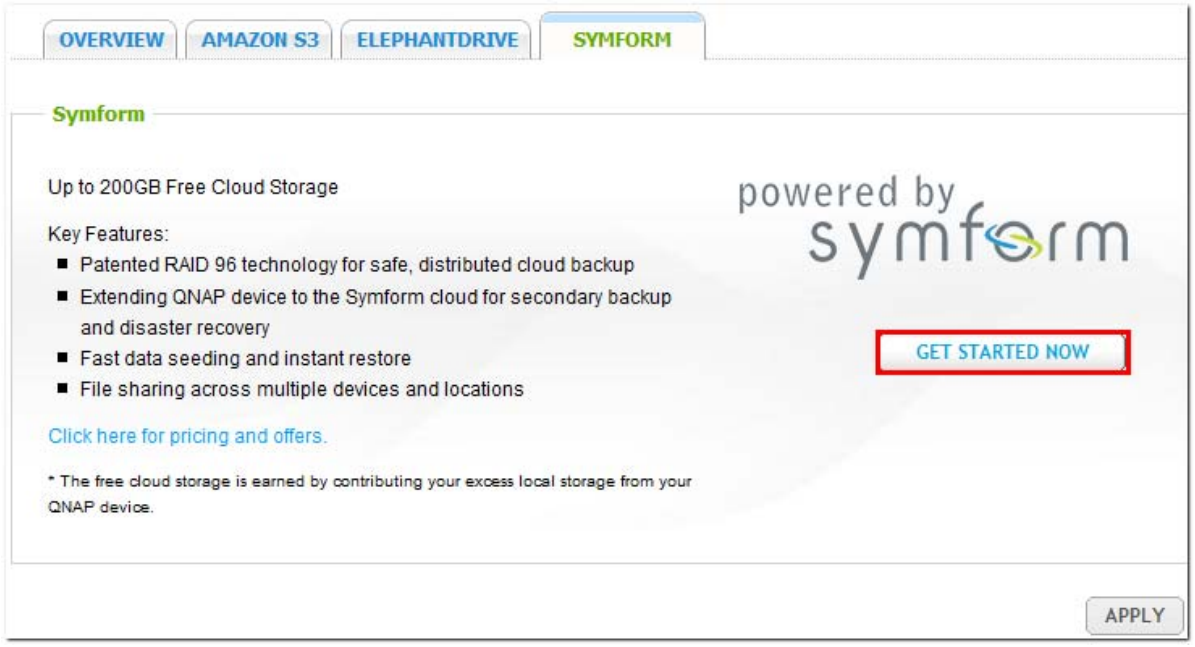


ElephantDriveアカウントにログインします。 バックアップを管理し、Webサイトでジョブを復元することができます。

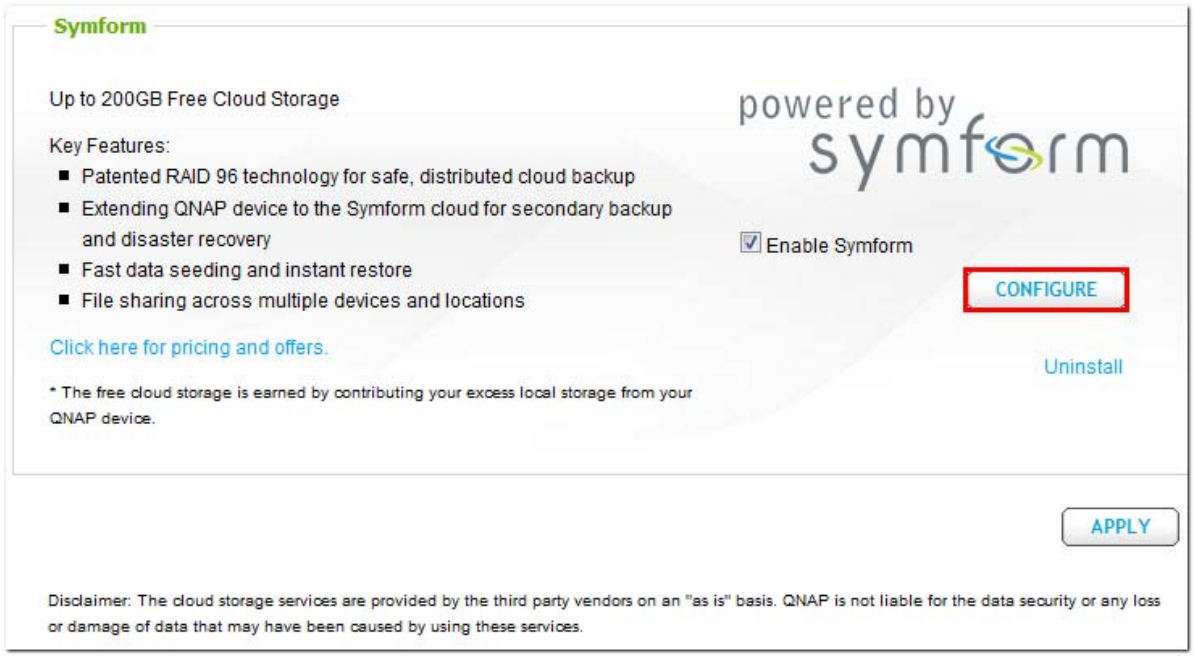


Symform

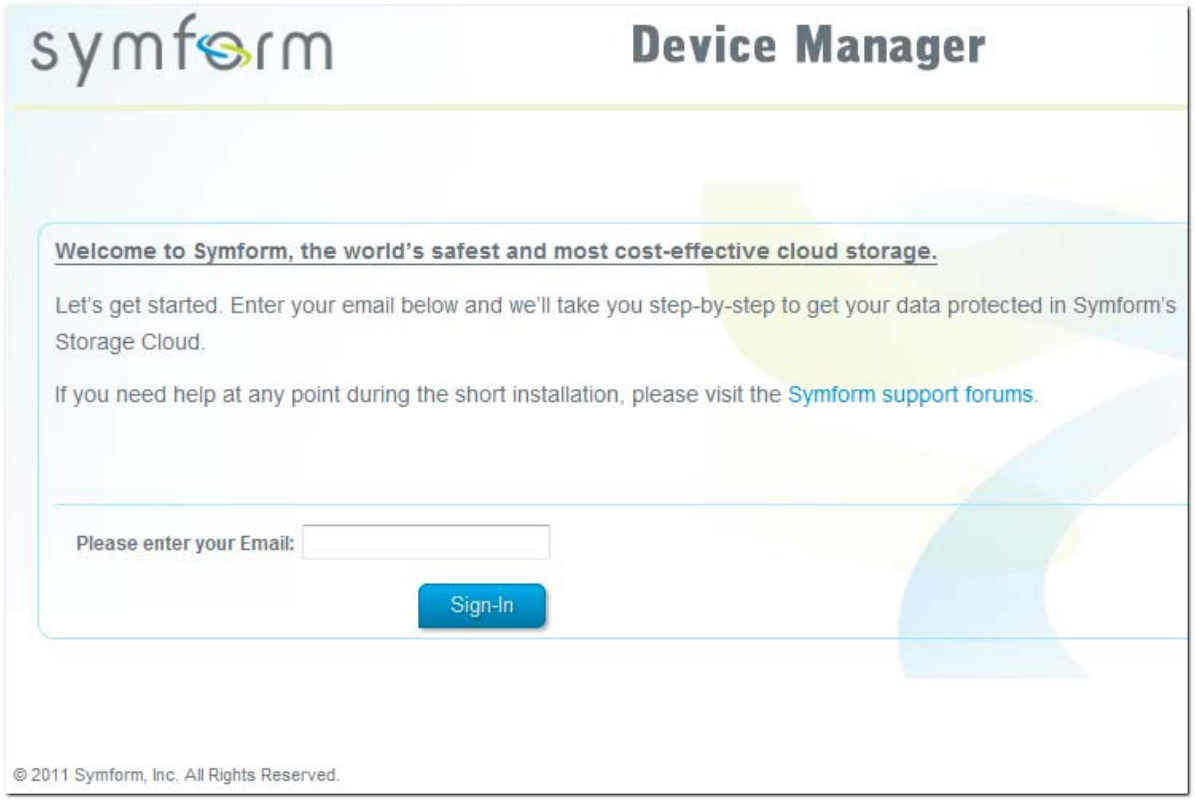
Symform クラウドバックアップを使用するには、「Backup（バックアップ）> Cloud Backup（クラウドバックアップ）> Symform」に移動します。「Get Started Now（今すぐ開始）」をクリックして、Symform をインストールします。NAS がパッケージを自動的にダウンロード、検証、インストールします。



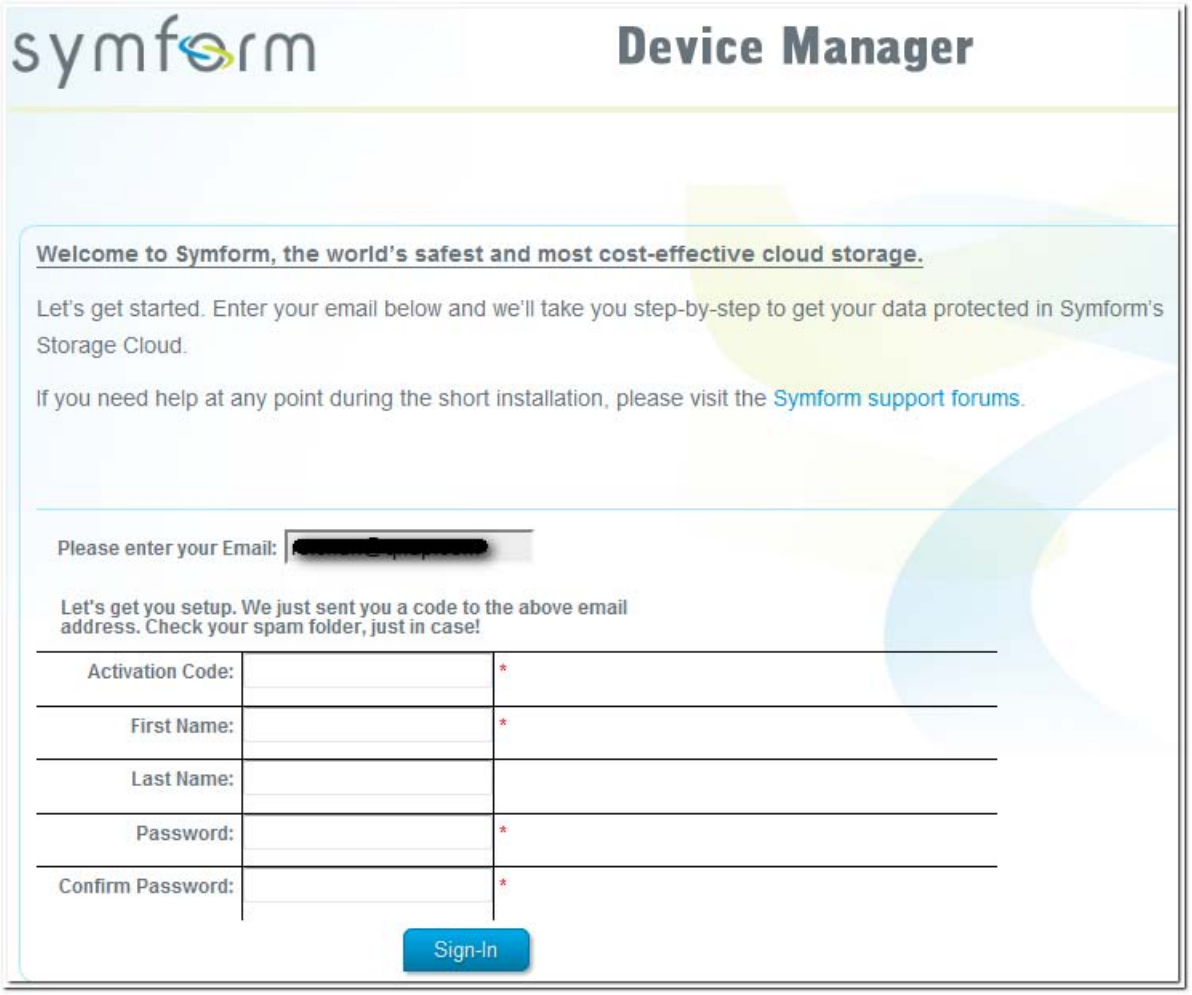
「Configure（設定）」をクリックします。



電子メールアドレスを入力し、「Sign-In（サインイン）」をクリックして、NAS 上の Symform をアクティブにします。アクティベーションコードが、このメールアドレスに送信されます。



アクティベーションコードを受信するメールアドレスを確認し、セットアップを完了します。


symform
Device Manager
Welcome to Symform, the world's safest and most cost-effective cloud storage.
Let's get started. Enter your email below and we'll take you step-by-step to get your data protected in Symform's Storage Cloud.
If you need help at any point during the short installation, please visit the Symform support forums.
Please enter your Email:
Let's get you setup. We just sent you a code to the above email address. Check your spam folder, just in case!
Activation Code:
First Name:
Last Name:
Password:
Confirm Password:
Sign-In

指示に従い、Symform を設定します。

完了後、セットアップ時に選択したフォルダが、Symform ストレージクラウドにバックアップされます。

Symform がアクティブになると、デバイス設定が表示されます。「Cloud Dashboard（クラウドダッシュボード）」をクリックして Symform クラウドダッシュボードにアクセスし、Symform ストレージクラウド稼働中の全デバイスのステータスを確認します。

Symform サービスに関する注意事項：

- ウェブ管理インターフェースの TCP ポート：59234
- コントリビューション TCP ポート：Symform セットアップ時にランダムに定義され、必要な場合は変更できます。
- 全 TCP アウトバウントポートは必須です。
- コントリビューション使用時は、NAS のハードドライブのスタンバイ機能は、Symform サービスが常にハードドライブ上のデータを読み書きするため機能しません。
- コントリビューション付 Symform は、ネットワーク帯域幅が必要です。コントリビューションが有効な場合、NAS と Symform クラウド間に常に通信が発生します。これによりネットワークが使用され、必要な場合、帯域幅を制限することができます。

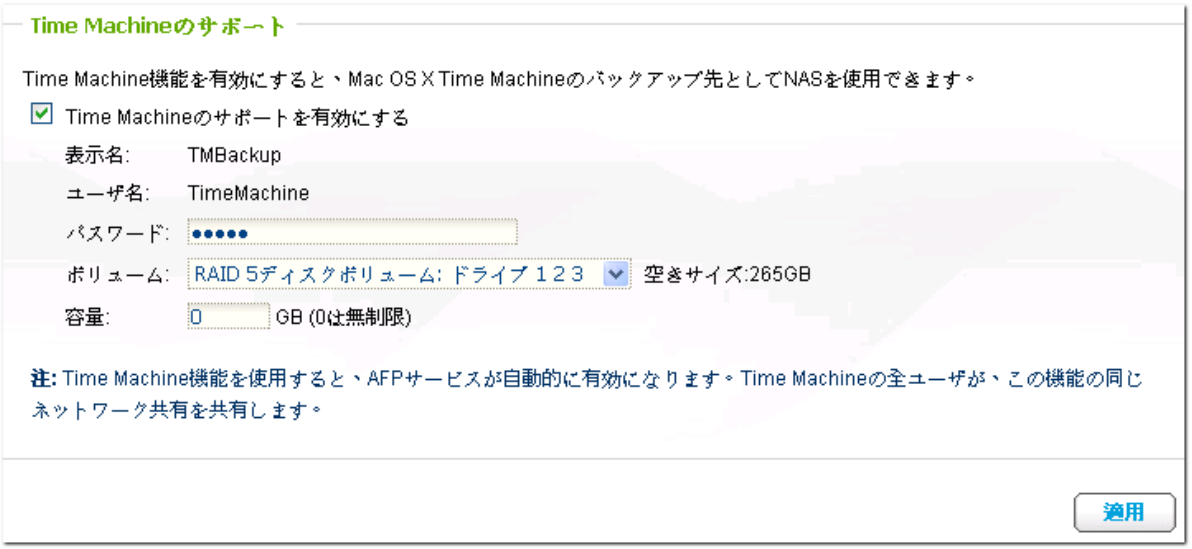
8.3 Time Machine

Time Machineサポートを効化して、OS XのTime Machine機能により複数のMacのバックアップ先としてNASを使用することができます。

この機能を使用するには、以下の手順に従ってください。

NAS上の設定を構成します:

1. Time Machineサポートを効化します。



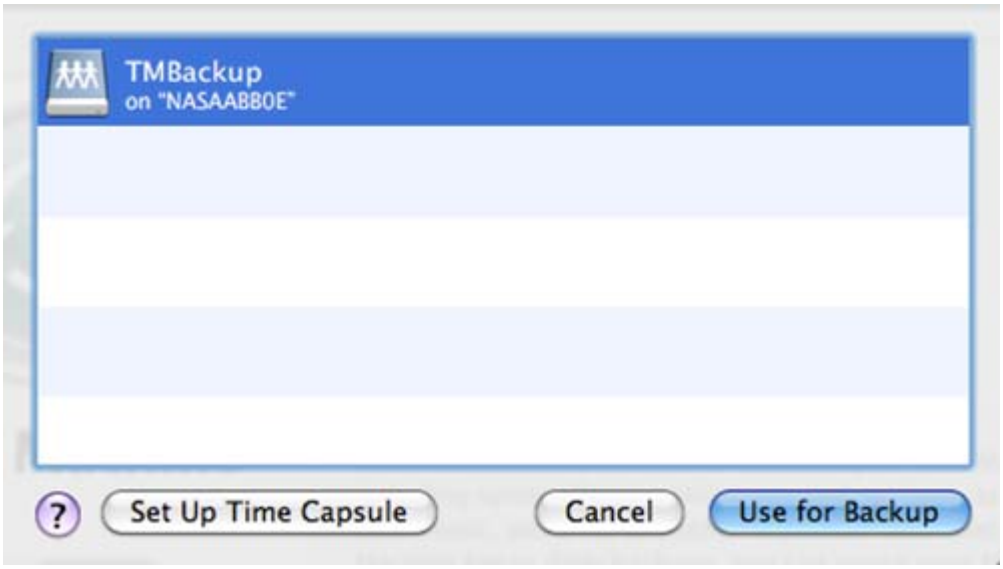
2. Time Machineパスワードを入力します。パスワードはデフォルトでは空欄になっています。
3. バックアップ先としてNAS上のボリュームを選択します。
4. Time Machineバックアップが使用できるストレージ容量を入力します。
5. "Apply" (適用) をクリックし設定を保存します。

すべてのTime Machineユーザーは、この機能用に同一のネットワーク共有を共有します。

Mac上のバックアップ設定を構成します:

1. Mac上でTime Machineを開き、"Select Backup Disk" (バックアップディスクの選択) をクリックします。

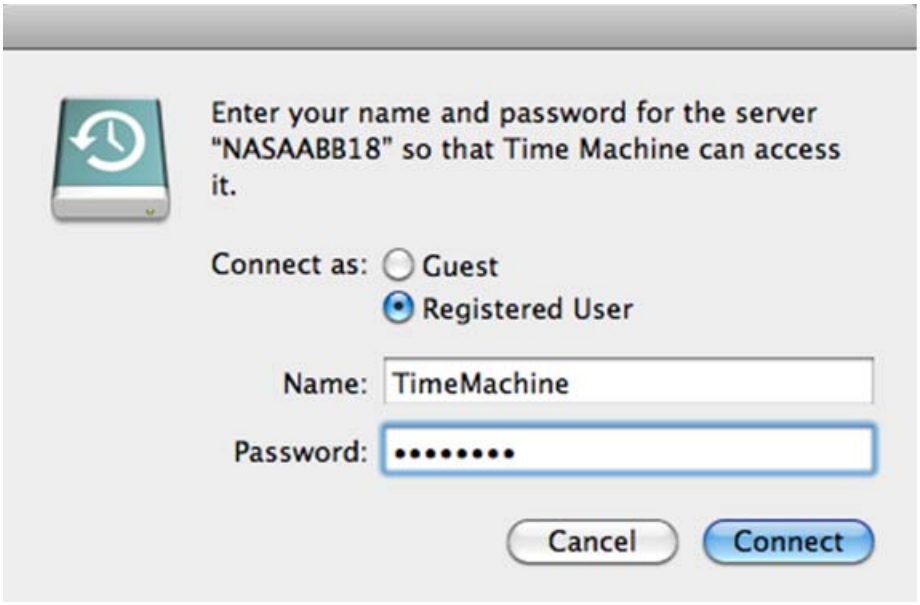
2. NASのTMBackupをリストから選択し、"Use for Backup" (バックアップに使用) をクリックします。



3. QNAP NASにアクセスするユーザー名及びパスワードを入力します。 続いて"Connect" (接続) をクリックします。

登録したユーザー名: TimeMachine

パスワード: NASで構成したパスワードです。パスワードはデフォルトでは空欄になっています。



4. 正常に接続されると、Time Machineは "ON" (オン) に切り替わります。 バックアップに使用可能な容量が表示され、バックアップは120秒後に開始されます。

初めてバックアップを実行する際は、Mac上のデータサイズにより、時間が通常より長くかかる場合があります。

Mac OSにデータを回復するには、http://www.apple.com のチュートリアルを参照してください。

バックアップ管理

このページで既存のバックアップを管理することができます。

Volume (ボリューム):ボリュームに保管されたTi Name (名前):Time Machineバックアップの名前(Time Machineが作成したスパースバンドルディスク画像)

Size (サイズ) : このTime Machineバックアップのサイズ

Date Modified (修正日時):このTime Machineバックアップが最後に修正された日時

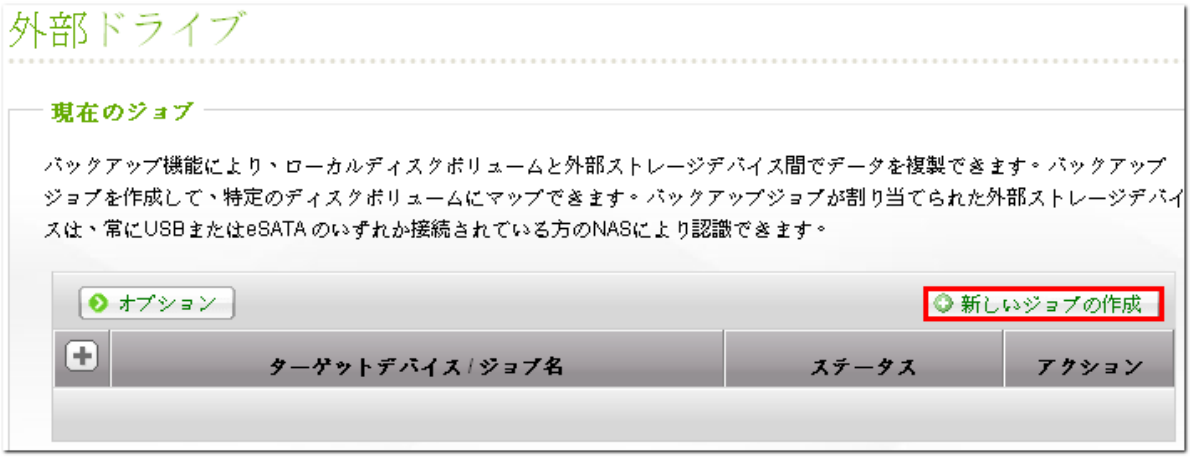
Delete (削除):このTime Machineバックアップの削除me Machine バックアップタスクを表示します。

8.4 外部ドライブ

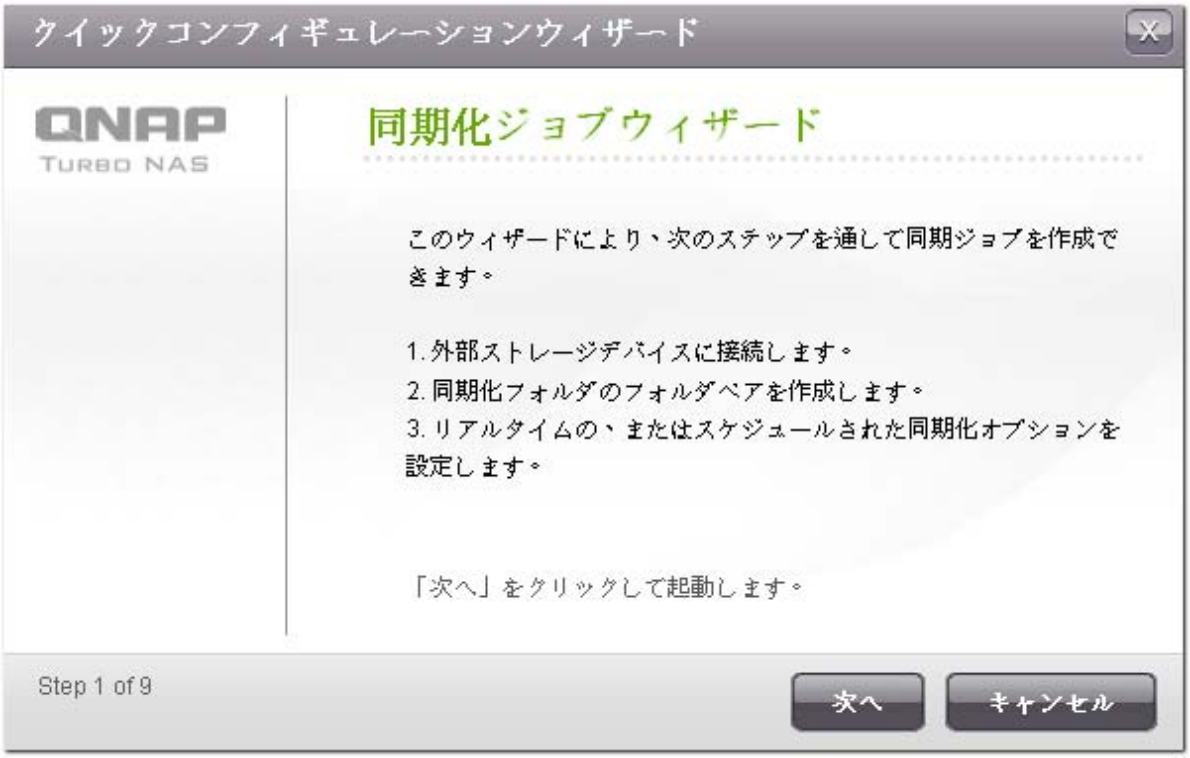
NAS は、内部ディスクボリュームと外部 USB/eSATA ストレージデバイス間のリアルタイムおよびスケジュール設定でのデータバックアップをサポートします。この機能を利用するには、次のステップを行います。

> 注：外部ストレージデバイスがNASによって暗号化されている場合、バックアップジョブを作成する前に「External Device（外部デバイス）」>「External Storage Device（外部ストレージデバイス）」でロックされていないことを確認します。

1. NAS の USB/eSATA インターフェースに 1 台以上の外部ストレージデバイスを接続します（利用可能な場合）。
2. 「Create a new job（新しいジョブの作成）」をクリックします。

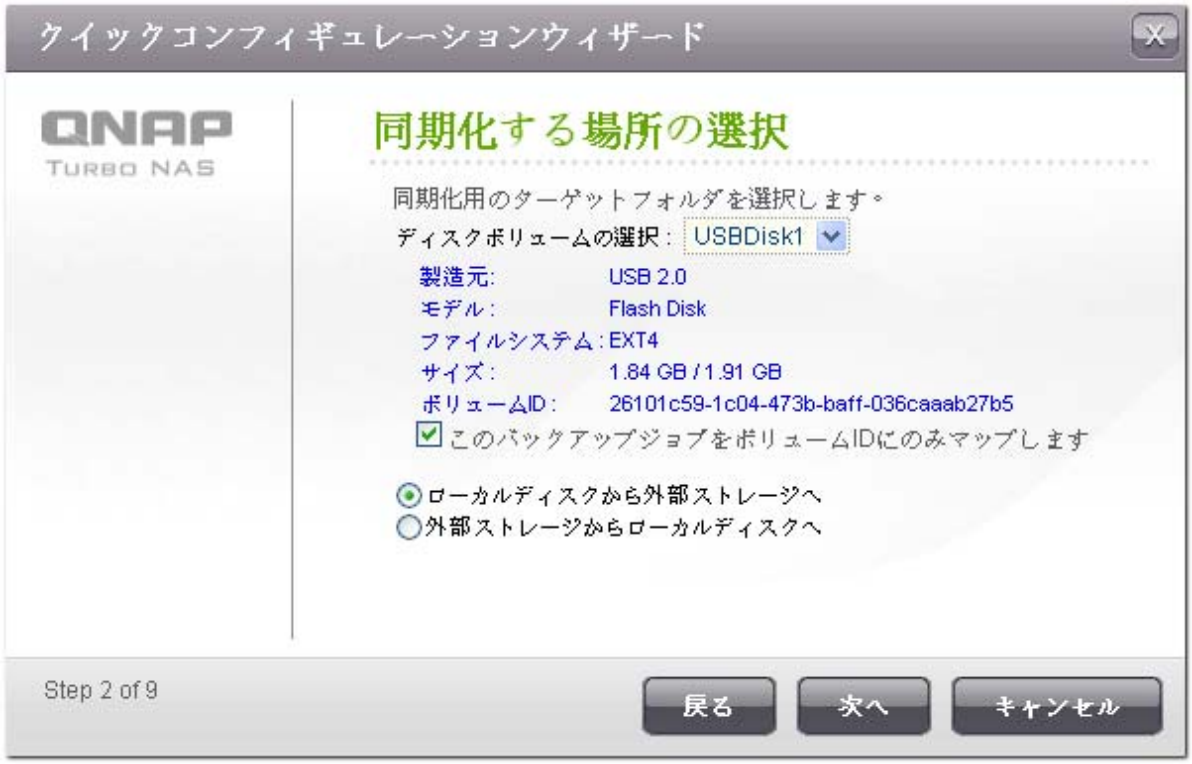


3. ウィザードが表示されたら、説明を注意深く読んで、「NEXT（次へ）」をクリックします。



4. バックアップ先を選択します。
   a. ドロップダウンメニューから外部ディスクボリューム* を選択します。NAS は、EXT3、EXT4、FAT、NTFS、および HFS+ ファイルシステムをサポートします。ストレージデバイスの一般的な情報が表示されます。
   b. 「Map this backup job to the volume ID only（このバックアップジョブをボリュームIDにのみマップします）」を選択し、バックアップジョブを特定の外部ストレージデバイスにマッピングします。USB/eSATA インターフェースで、デバイスが NAS に接続されると、NAS が、デバイスを認識し、自動的に設定によりバックアップジョブを実行します。
   c. ローカルディスクボリュームから外部ストレージ、または、その逆に外部ストレージからローカルディスクボリュームにデータをバックアップするを選択します。
   d. 「NEXT（次へ）」をクリックします。

* 外部ストレージデバイス上の複数パーティションは、別々のディスクボリュームとして認識されます。



5. バックアップの元と先のフォルダを選択します。それから、「ADD（追加）」をクリックします。最大 5 フォルダのペアを作成できます。「NEXT（次へ）」をクリックします。

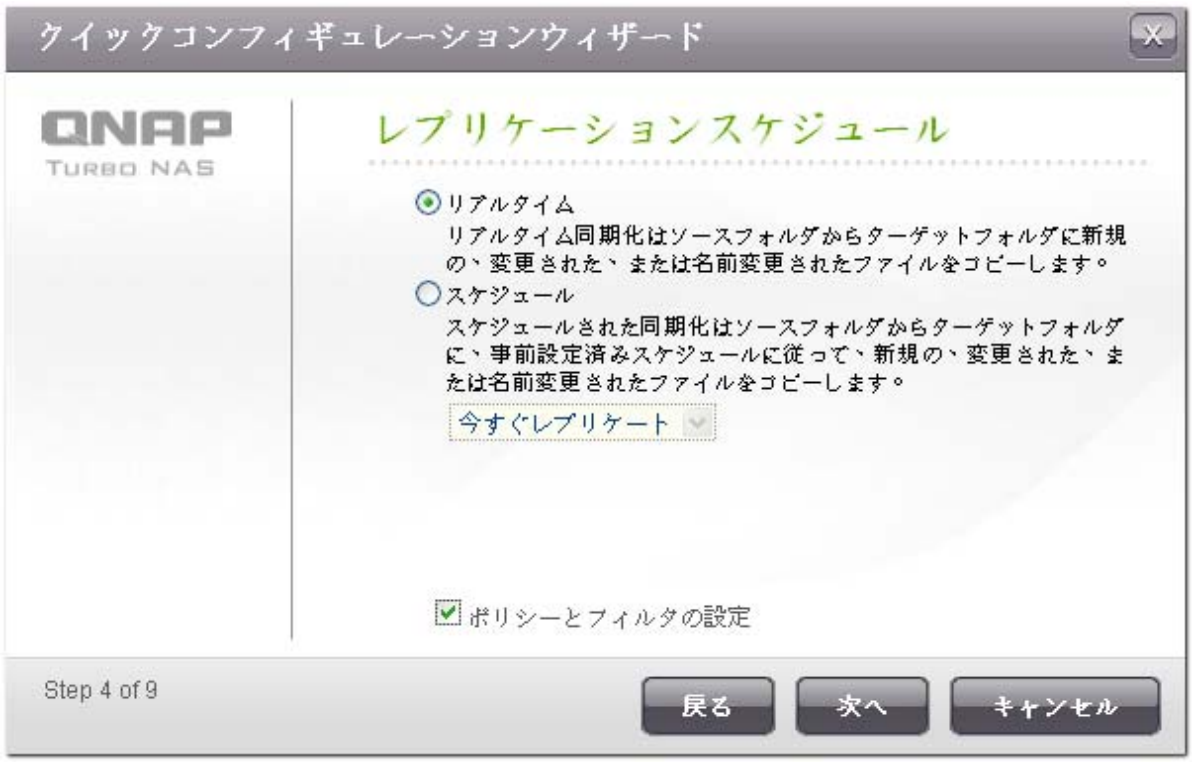
注：バックアップジョブのフォルダペアで、親フォルダまたは子フォルダが元フォルダまたは先フォルダとして選択された場合、同じバックアップジョブのフォルダペアで同じフォルダを別なフォルダペアの元フォルダまたは先フォルダとして選択することはできません。

6. リアルタイムバックアップおよびスケジュールバックアップを選択します。リアルタイムバックアップは、新しいファイル、変更されたファイル、名称が変更されたファイルを元フォルダから先フォルダに、バックアップ後変更された場合直ちにコピーします。

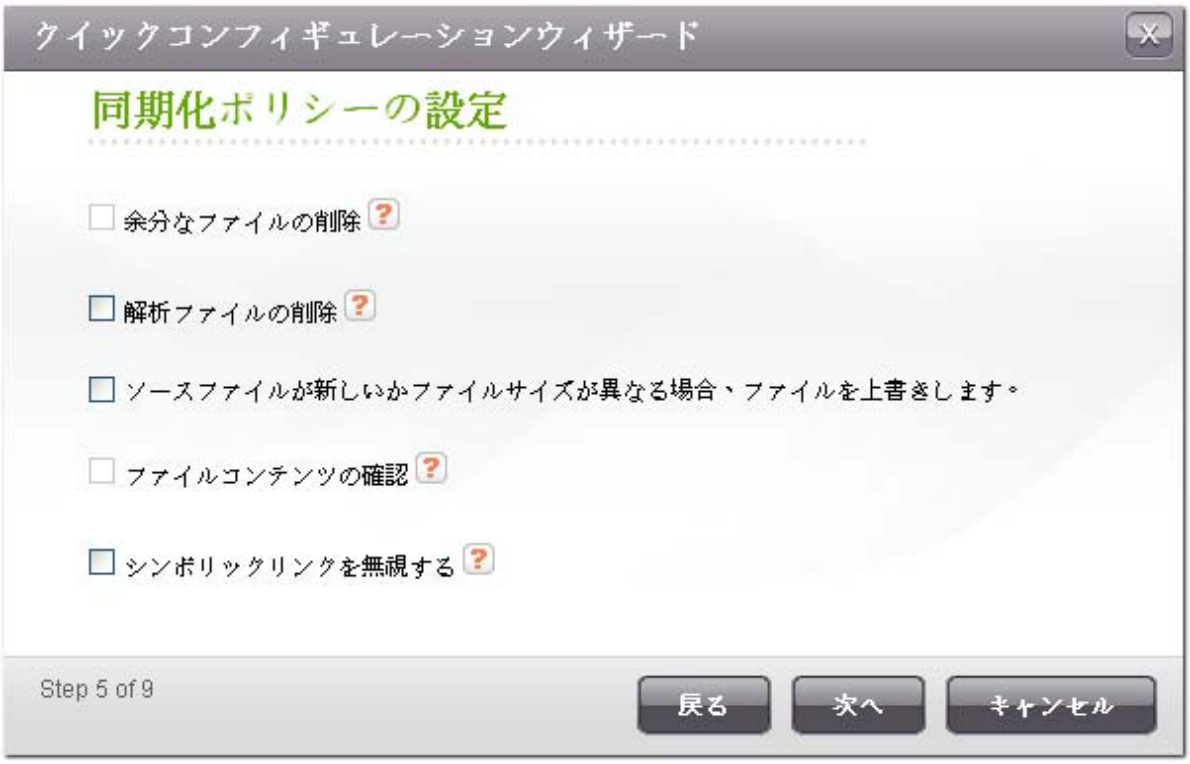
スケジュールバックアップは、スケジュールに従い、元フォルダから先フォルダにファイルをコピーします。オプションは次の通りです：

- 今すぐコピー：データを直ちにコピーします。
- 周期的：バックアップジョブを実行する間隔を時分単位で入力します。最小時間間隔は 5 分です。
- 毎時：バックアップジョブを実行する分を選択します。例えば、01 を選択した場合、バックアップジョブは毎時 1分（1 時 1 分、2 時 1 分、3 時 1 分…）に実行されます。
- 毎日：バックアップジョブを実行する時刻を指定します（例えば、毎日 2 時 2 分）。
- 毎週：週毎のバックアップを実行する曜日と時刻を選択します。
- 毎月：月毎のバックアップを実行する日付と時刻を選択します。
- 自動バックアップ：デバイスが接続され、NAS が検出した時に自動的に毎回データバックアップを実行します。

バックアップポリシーおよびフィルタ設定を行うには、「Configure policy and filter（ポリシーとフィルタの設定）」を選択します。「NEXT（次へ）」をクリックします。

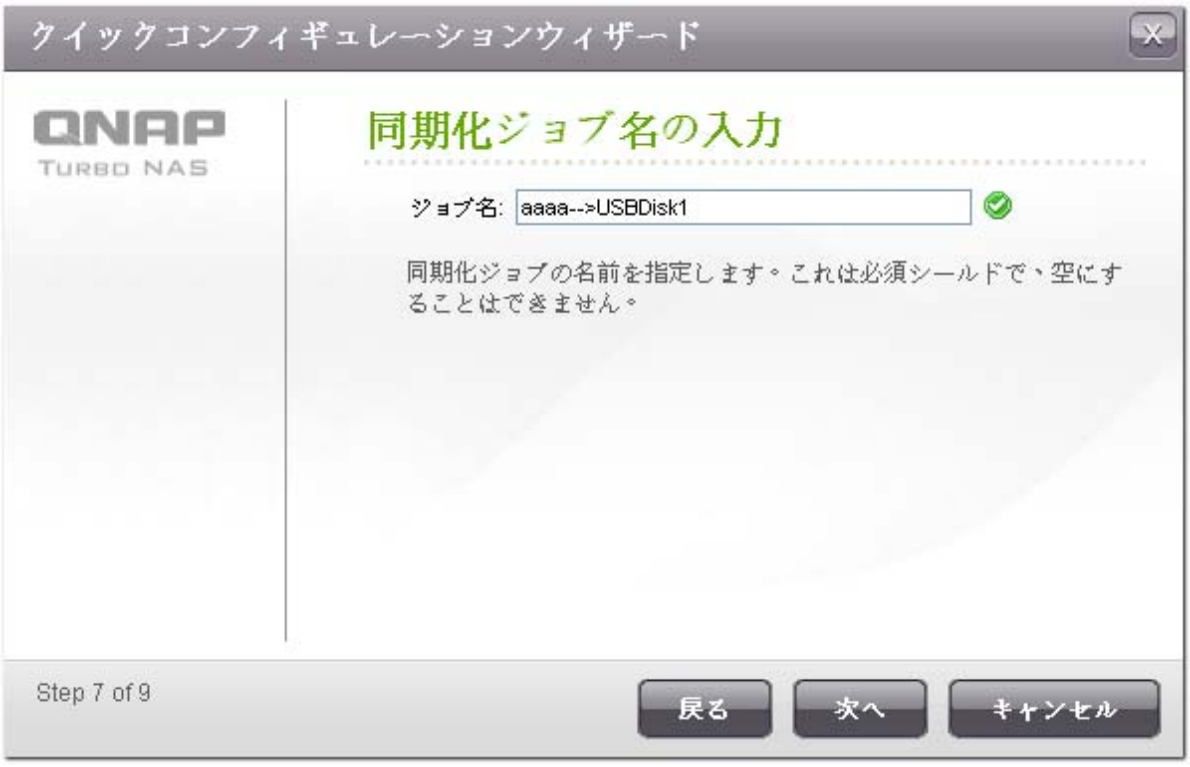


7. 次のオプションを有効にするかどうかを選択します：
   - Delete extra files（余分なファイルの削除）：先フォルダ内の余分なファイルを削除します。元フォルダ上の削除が、先フォルダに反映されます。このオプションは、リアルタイムバックアップでは利用できません。
   - Detect sparse files（解析ファイルの削除）：このオプションを選択して、NULL データのファイルを無視します。
   - Overwrite the file if the source file is newer or the file size is different（ソースファイルが新しいかファイルサイズが異なる場合、ファイルを上書きします）。
   - Check file contents（ファイルコンテンツの確認）：ファイルコンテンツ、日付、サイズ、名称を検査して、2 つのファイルが同一であるかどうか決定します。このオプションは、リアルタイムバックアップでは利用できません。
   - Ignore symbolic links（シンボリックリンクを無視する）：このオプションを選択して、フォルダペア内のシンボリックリンクを無視します。

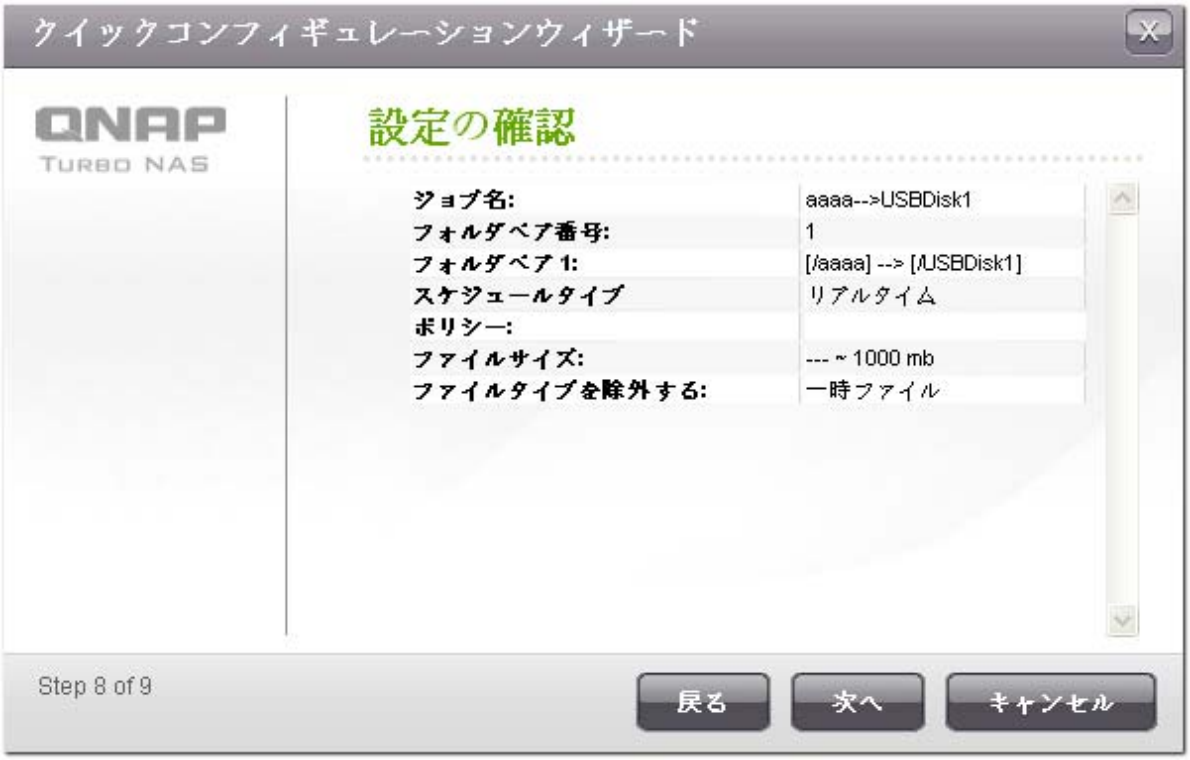


8. バックアップジョブ用のフィルタを作成します。
   - File size（ファイルサイズ）：コピーするファイルの最小サイズおよび最大サイズを指定します。
   - Include file types（ファイルタイプを含める）：コピーするファイルタイプを指定します。
   - Exclude file types（ファイルタイプを除外する）：データコピーから除外するファイルタイプを指定します。
   - File date/time（ファイルの日付/時刻）：コピーするファイルの日付および時刻を指定します。

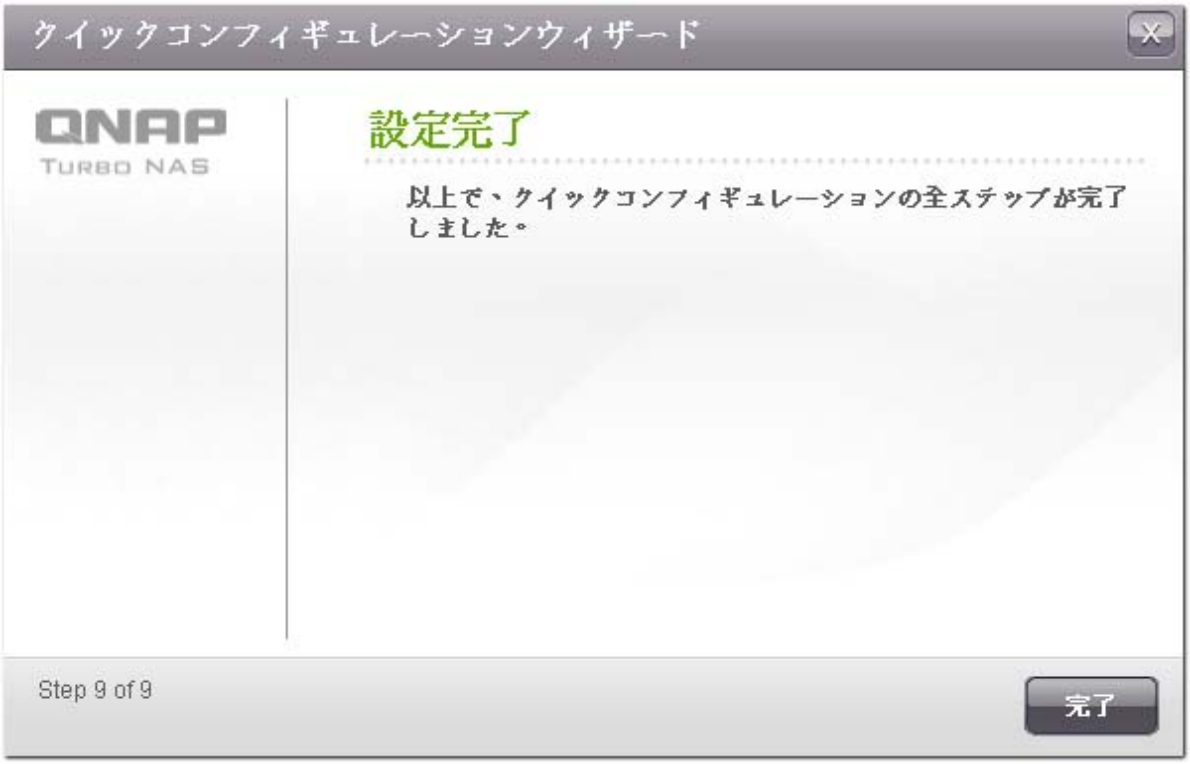
9. バックアップジョブの名称を入力します。ジョブ名は最大 63 文字をサポートします。スペースで開始/終了することはできません。「NEXT（次へ）」をクリックします。



10. 設定を確認し、「NEXT（次へ）」をクリックします。



11. 「FINISH（完了）」をクリックして、ウィザードを終了します。



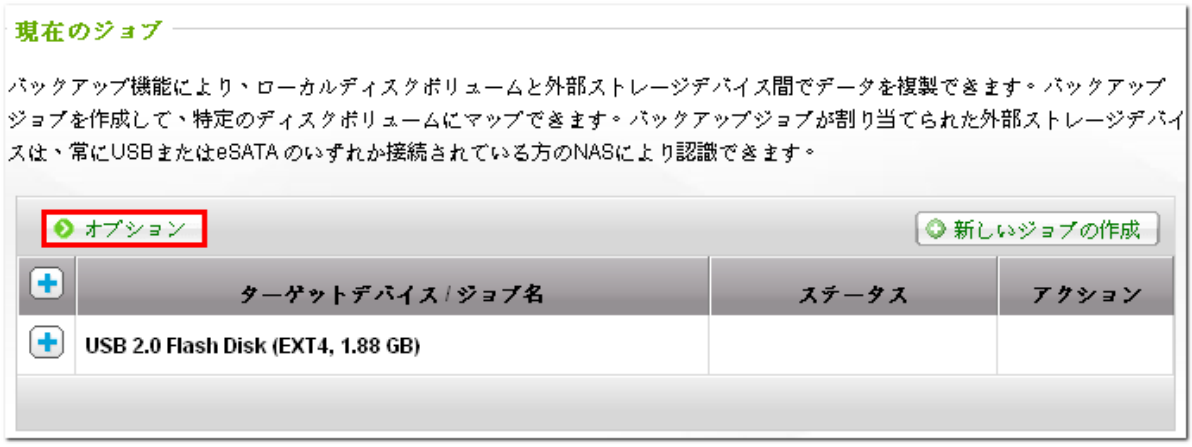
12. バックアップジョブおよびステータスがリスト上に表示されます。

ボタン	説明
	バックアップジョブを開始します。
	バックアップジョブを停止します。
	バックアップジョブの設定を編集します。
	ジョブのステータスおよびログを表示します バックアップジョブのログをダウンロードします。
	バックアップジョブを削除します。 このボタンは、バックアップジョブが停止後、利用可能です。

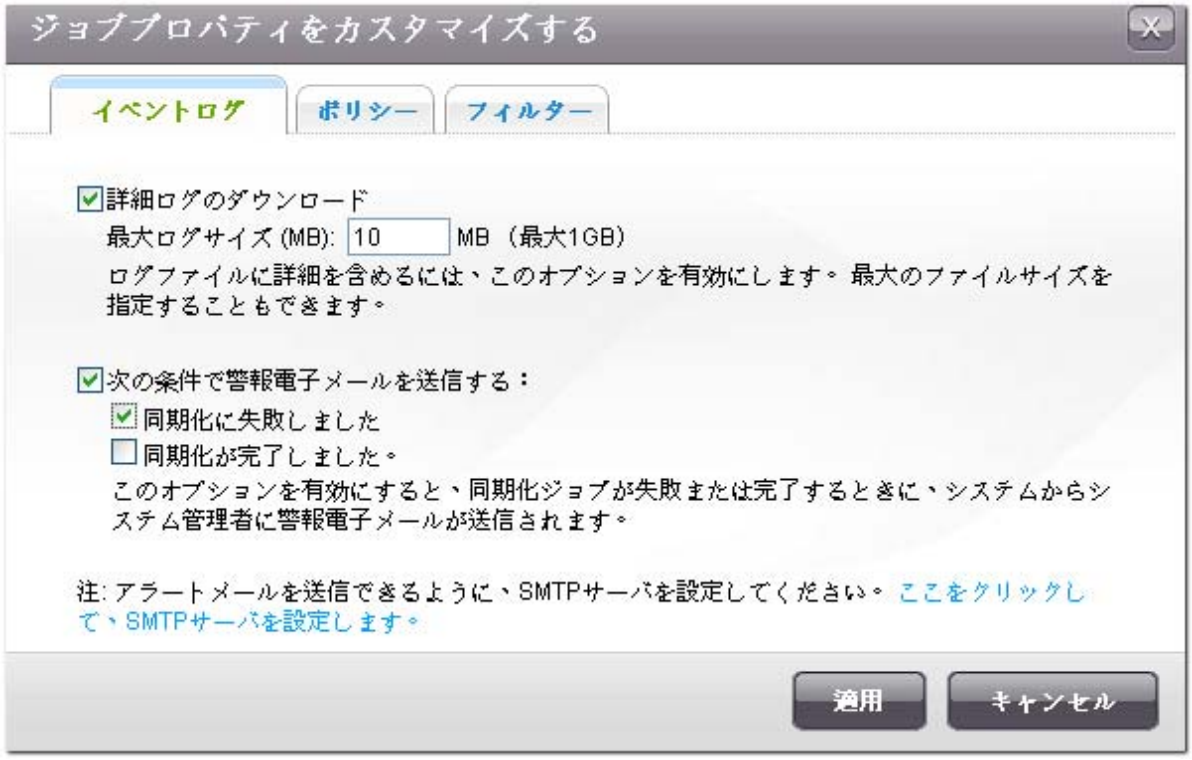
バックアップジョブのバックアップスケジュールを無効にするには、 をクリックし、「Settings（設定）」>「Schedule Type（スケジュールタイプ）」の下の「Disabled（無効）」を選択して、「APPLY（適用）」をクリックします。

デフォルトバックアップジョブ設定

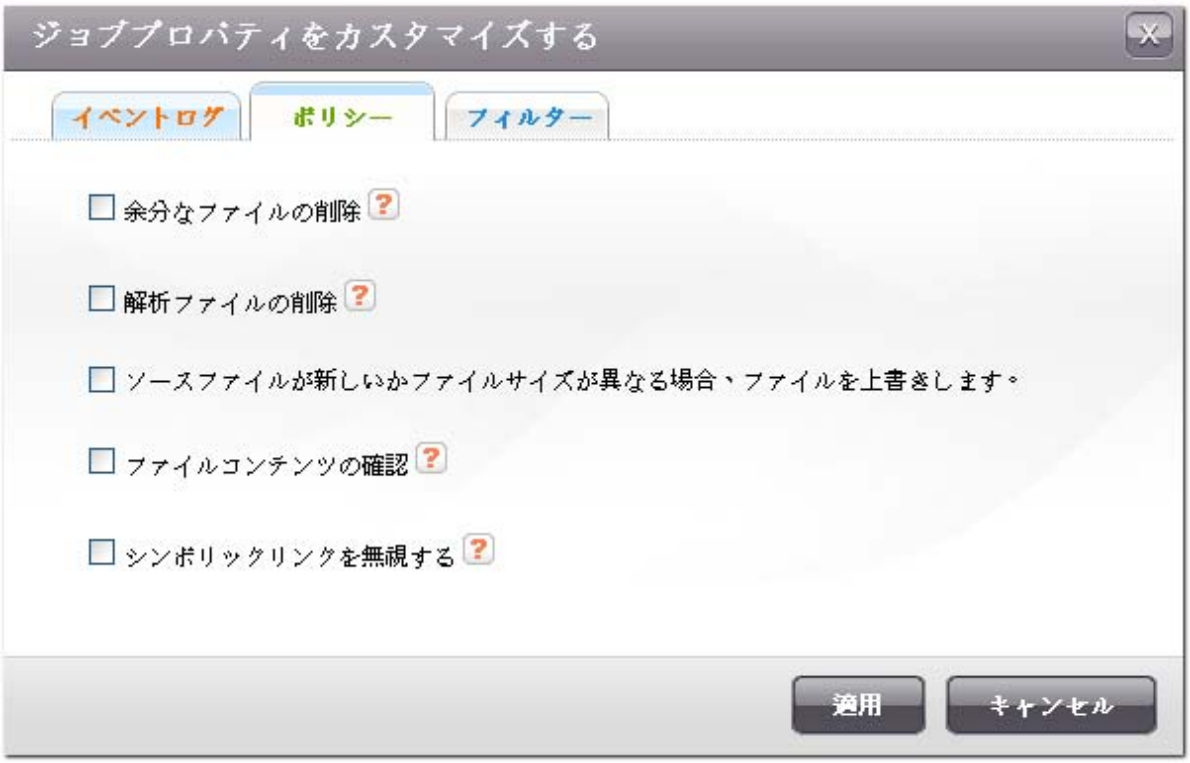
デフォルトバックアップジョブのプロパティを編集するには、「Options（オプション）」をクリックします。



「Event Logs（イベントログ）」の下の「Download Detailed Logs（詳細ログのダウンロード）」を選択/有効にし、ログファイルの最大ファイルサイズを指定します。バックアップジョブが失敗または完了した時の E メール通知を送信するよう選択します。「System Administration（システム管理）」>「Notification（通知）」で、SMTP サーバー設定が適切に行う必要があることに注意してください。

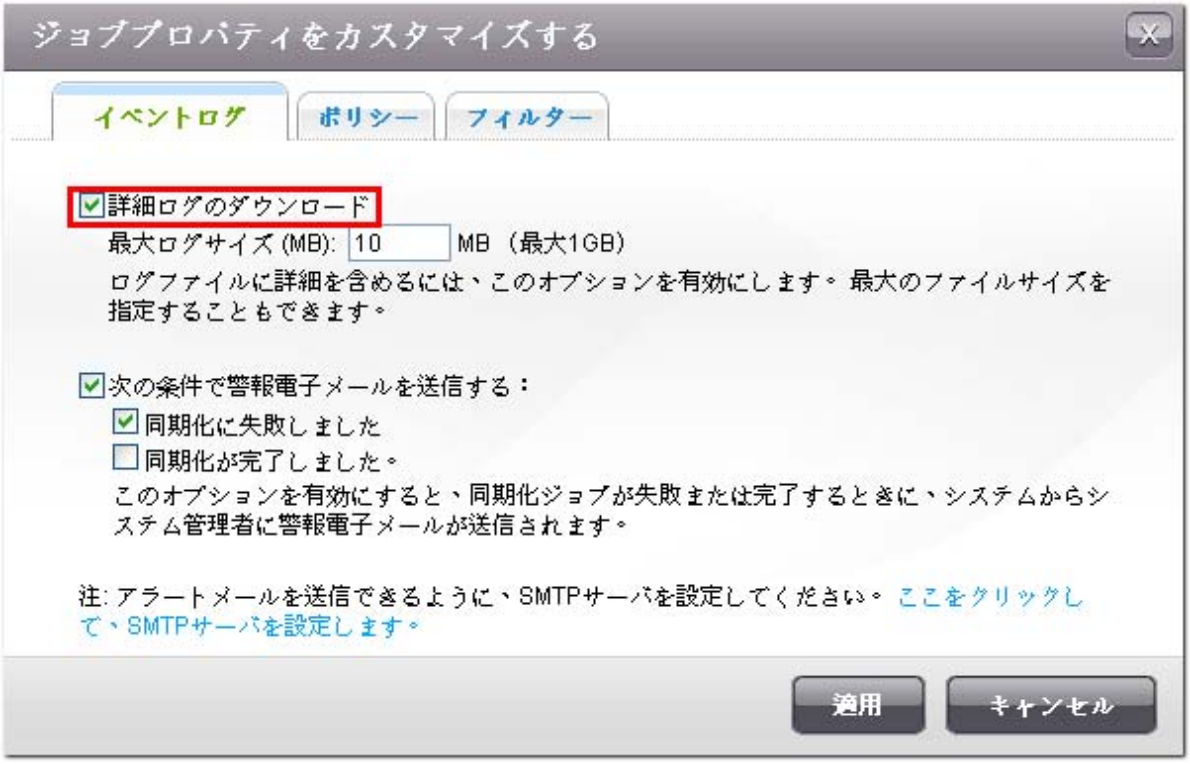


「Policy（ポリシー）」で、バックアップポリシーを、「Filter（フィルター）」で、フィルタ設定を指定します。これらが、すべてのバックアップジョブのデフォルト設定になります。



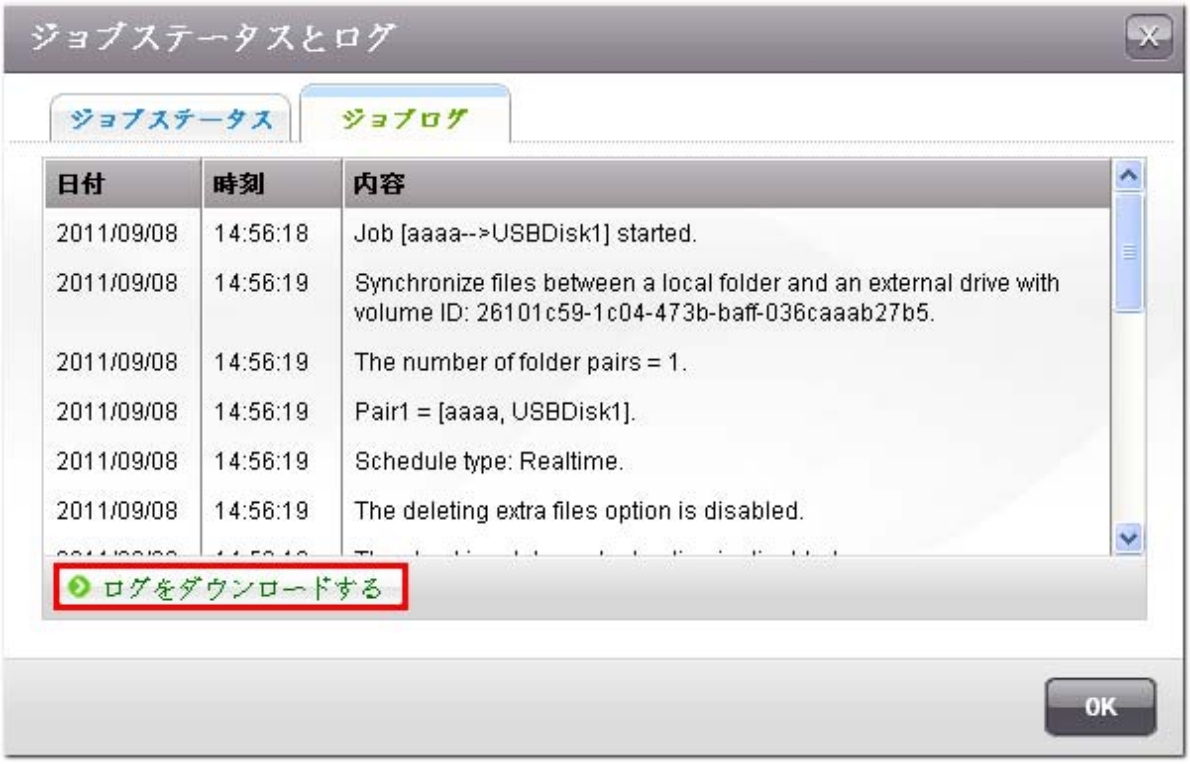
バックアップログのダウンロード

1. バックアップログをダウンロードするには、「Options（オプション）」>「Event Logs（イベントログ）」内の「Download Detailed Logs（詳細ログのダウンロード）」オプションが有効になっていることを確認します。



2. バックアップジョブの「Action（アクション）」カラムの をクリックします。

3. 「Job Logs（ジョブログ）」に進み、「Download Logs（ログのダウンロード）」をクリックします。ログファイルは、Microsoft Excel または他のテキストエディタで開くことができます。このボタンは、「Options（オプション）」>「Event Logs（イベントログ）」の「Download Detailed Logs（詳細ログのダウンロード）」を有効にし、バックアップジョブを一度実行した後でのみ、利用可能になります。



8.5 USBワンタッチコピー

この機能はTS-809U-RP, TS-879U-RP, TS-EC879U-RP, TS-1279U-RP, TS-EC1279U-RPではサポートされません。

このページでUSBワンタッチコピーの機能を設定できます。次の3つの機能を使用できます。

オプション	説明
前面のUSBストレージからNASの内蔵HDDへコピーする	1. ディレクトリの作成:コピー先に新たなディレクトリが作成され、ソースデータはこのディレクトリにコピーされます。新たなディレクトリはバックアップの日付で名前が付けられます(年(4桁)月(2桁)日(2桁)同日中に二つ以上のバックアップがある場合、ディレクトリは年(4桁)月(2桁)日(2桁)-1、年(4桁)月(2桁)日(2桁)-2…というように名付けられます。 2. コピー:データをコピー先の共フォルダにバックアップします。同一のファイルが存在する場合、コピー先のファイルは上書きされます。 3. 同期化:データをコピー先の共フォルダにバックアップし、冗長ファイルを削除します。同一のファイルが存在する場合、コピー先のファイルは上書きされます。
NASの内蔵HDDのディレクトリから前面のUSBストレージへコピーする	1. コピー:データをコピー先の共フォルダにバックアップします。同一のファイルが存在する場合、コピー先のファイルは上書きされます。 2. 同期化:データをコピー先の共フォルダにバックアップし、冗長ファイルを削除します。同一のファイルが存在する場合、コピー先のファイルは上書きされます。
ワンタッチコピーボタンを無効化	コピーボタンを無効化するにはこのオプションを選択してください。

注:ソースのストレージ機器に複数のパーティションが存在する場合、バックアップ先には、バックアップフォルダとして各パーティションに対し新規フォルダが作成されます。バックアップフォルダはバックアップの日付およびパーティション用の数値が名付けられます。パーティション1用には年(4桁)月(2桁)日(2桁)-1、パーティション2用には年(4桁)月(2桁)日(2桁)-2…のようになります。ソースのストレージ機器にはパーティションが1つしかない場合、バックアップフォルダは年(4桁)月(2桁)日(2桁)として名付けられます。

USBワンタッチコピー
USBワンタッチコピー
USBワンタッチコピーボタンの機能を設定する
前面USBストレージデバイスから内部ディスクの Qusb ディレクトリにコピーする
バックアップ方法: ディレクトリの追加 宛先の共有フォルダにディレクトリを新規作成し、データをバックアップする
前面USBストレージデバイスに内部ディスクの Qusb ディレクトリからコピーする
ワンタッチコピーボタンを無効にする
適用

フロントUSBポートによるデータコピー

NASは外付けUSBデバイスからNASに、またはフロント[USBコピー]ボタンによるその他の方法によるインスタントデータコピーのバックアップをサポートします。この機能を使用するには、以下のステップに従ってください。

1. ハードドライブが取り付けられ、NASでフォーマットされていることを確認します。デフォルトのネットワーク共Qusb/ Usbが作成されます。
2. NASをオンにします。
3. 「データのバックアップ」 > 「USBのワンタッチコピーバックアップ」ページで、[コピー]ボタンの動作を構成します。
4. デジタルカメラやフラッシュなどのUSBデバイスをNASのフロントUSBポートに接続します。
5. Copy (コピーボタンを一度押します。NASの設定に従って、データがコピーされます。

注:増分バックアップがこの機能に使用されます。初回のデータバックアップの後は、NASは前回のバックアップ以降に変更があったファイルのみコピーします。

注:ファイルはソースからコピー先へとコピーされます。コピー先にあるその他のファイルは削除され、同一の名前のファイルはソースのファイルにより上書きされます。ソースのデータには変更はありません。

9. 外部デバイス

外部ストレージデバイス 569
USBプリンタ 579
UPS設定 609

9.1 外部ストレージデバイス

NAS は、ストレージ拡張用に、外部 USB および eSATA ストレージデバイス* をサポートします。ストレージデバイスを NAS の USB または eSATA インターフェースに接続し、デバイスの検出に成功すると、詳細がこのページに表示されます。

*サポートする USB および eSATA インターフェースの数は、モデルによって異なります。詳細は、http://www.qnap.com を参照してください。

NAS サーバーが、外部 USB デバイスを検出するには数十秒かかる場合もあります。辛抱強くお待ちください。

外部ストレージデバイスは、FAT32、NTFS、EXT3、または、HFS+（Mac のみ）ファイルシステムとしてフォーマットが可能です。「Format As（指定フォーマット）」の横のドロップダウンメニューからオプションを選択します。

高度なフォーマットオプション:
NAS は、外部ドライブの暗号化をサポートします。外部ストレージデバイスを暗号化するには、「Advanced format options（高度なフォーマットオプション）」をクリックします。暗号化方式を選択します：AES 128-、192- または 256- ビット。そして、パスワード（8 ～ 16 文字）を入力します。「Save encryption key（暗号化キーの保存）」を選択して、パスワードを NAS のハードドライブの隠された場所に保存します。NAS は、暗号化された外部ストレージデバイスが接続されると、毎回自動的にロック解除します。

「Format Now（指定フォーマット）」をクリックします。全データが消去されます。ディスクの初期化が完了後、デバイスは「Ready（準備完了）」になります。

暗号化管理

NAS により外部ストレージデバイスが暗号化されると、「Encryption Management（暗号化管理）」ボタンが表示されます。このボタンをクリックして、暗号化パスワード/キーを管理し、または、デバイスをロック/ロック解除します。

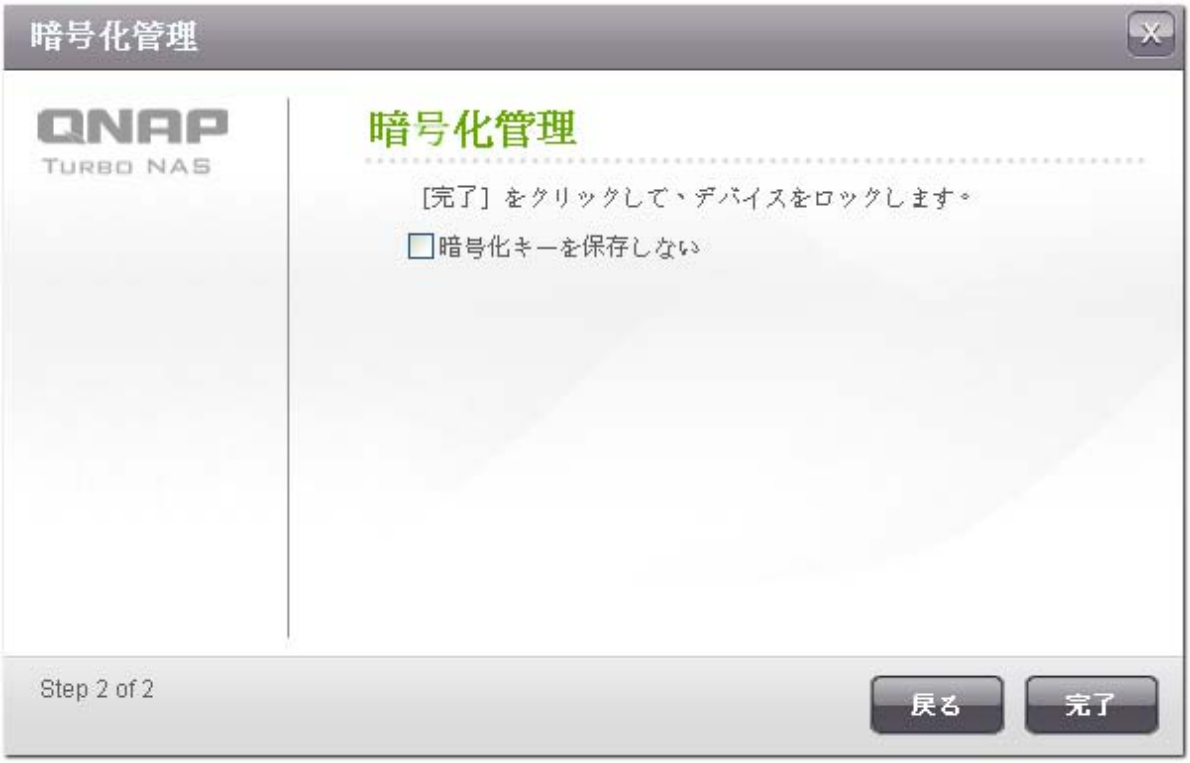
デバイスのロック

注：リアルタイムのまたは定期的なバックアップジョブが実行中は、外部ストレージでバイスをロックできません。バックアップジョブを無効にするには、「Backup（バックアップ）」>「External Drive（外部ドライブ）」に移動します。

1. 暗号化された外部ストレージデバイスをロックするには、「Encryption Management（暗号化管理）」をクリックします。

2. 「Lock this device（このデバイスをロックする）」を選択し、「Next（次へ）」をクリックします。

3. 「Finish（完了）」をクリックして、デバイスをロックします。



デバイスのロック解除

1. 暗号化された外部ストレージデバイスをロック解除するには、「Encryption Management（暗号化管理）」をクリックします。

2. 「Unlock the device（このデバイスをロック解除する）」を選択し、「Next（次へ）」をクリックします。

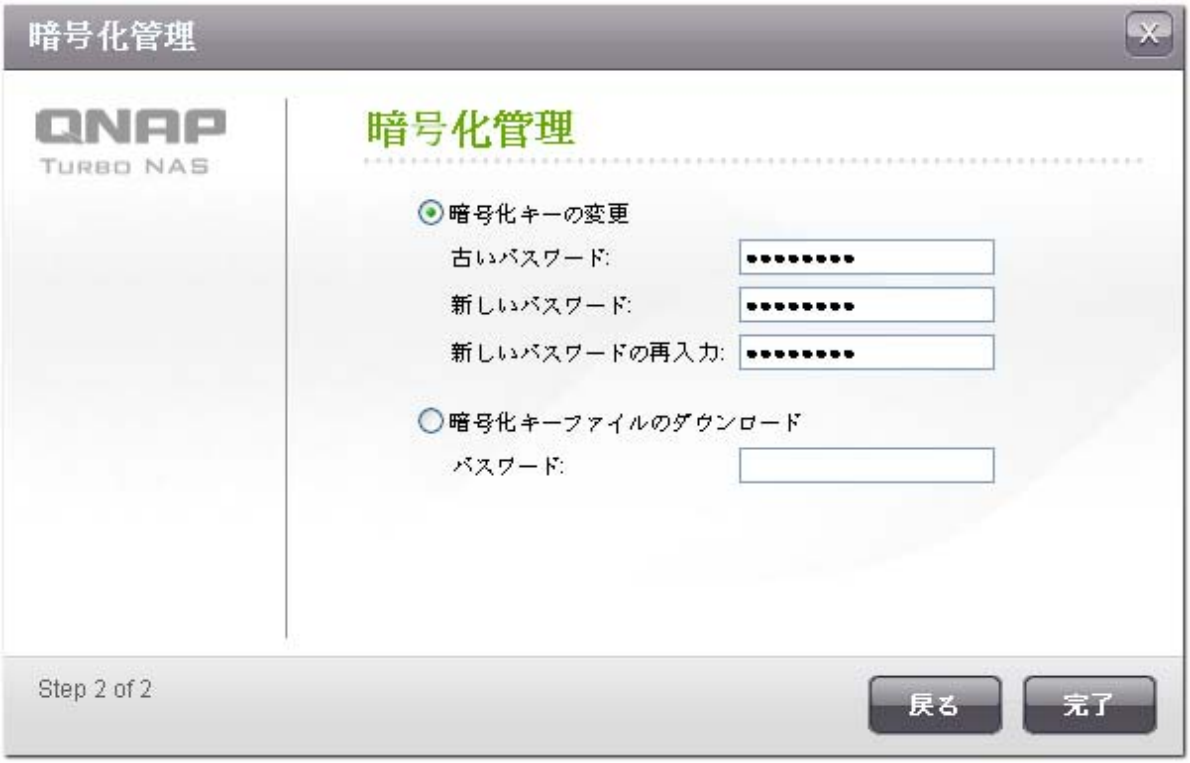
3. 暗号化パスワードを入力するか、キーファイルをアップロードします。「Save encryption key（暗号化キーの保存）」を選択して、パスワードを NAS のハードドライブの隠された場所に保存します。NAS は、暗号化された外部ストレージデバイスが接続されると、毎回自動的にロック解除します。「Finish（完了）」をクリックします。

暗号化キーの管理

1. 暗号化パスワードの変更、または、暗号化キーファイルをダウンロードするには、「Encryption Management（暗号化管理）」をクリックします。

2. 「Manage encryption key（暗号化キーの管理）」を選択します。「Next（次へ）」をクリックします。

3. 暗号化キーの変更または、暗号化キーファイルのダウンロードを選択します。「Finish（完了）」をクリックします。



1 ドライブモデル用ディスク利用設定

1 ドライブモデルの NAS へ外部ストレージデバイスを接続するには次のうち 1 つの設定を選択します:

- データ共有: 外部ドライブを NAS のストレージ拡張用に使用します。
- Q-RAID 1: 外部ドライブと NAS 上のローカルハードドライブを Q-RAID 1 として設定します。Q-RAID 1 は、NAS から外部ストレージデバイスへの一方向のデータ同期を可能にしますが、RAID 冗長性には影響を与えません。**Q-RAID 1が実行されているとき、外部ドライブはフォーマットされません。**

Q-RAID 1 が一度実行され、NAS に外部ストレージデバイスが接続されると、自動的に NAS のデータが外部ストレージデバイスにコピーされます。

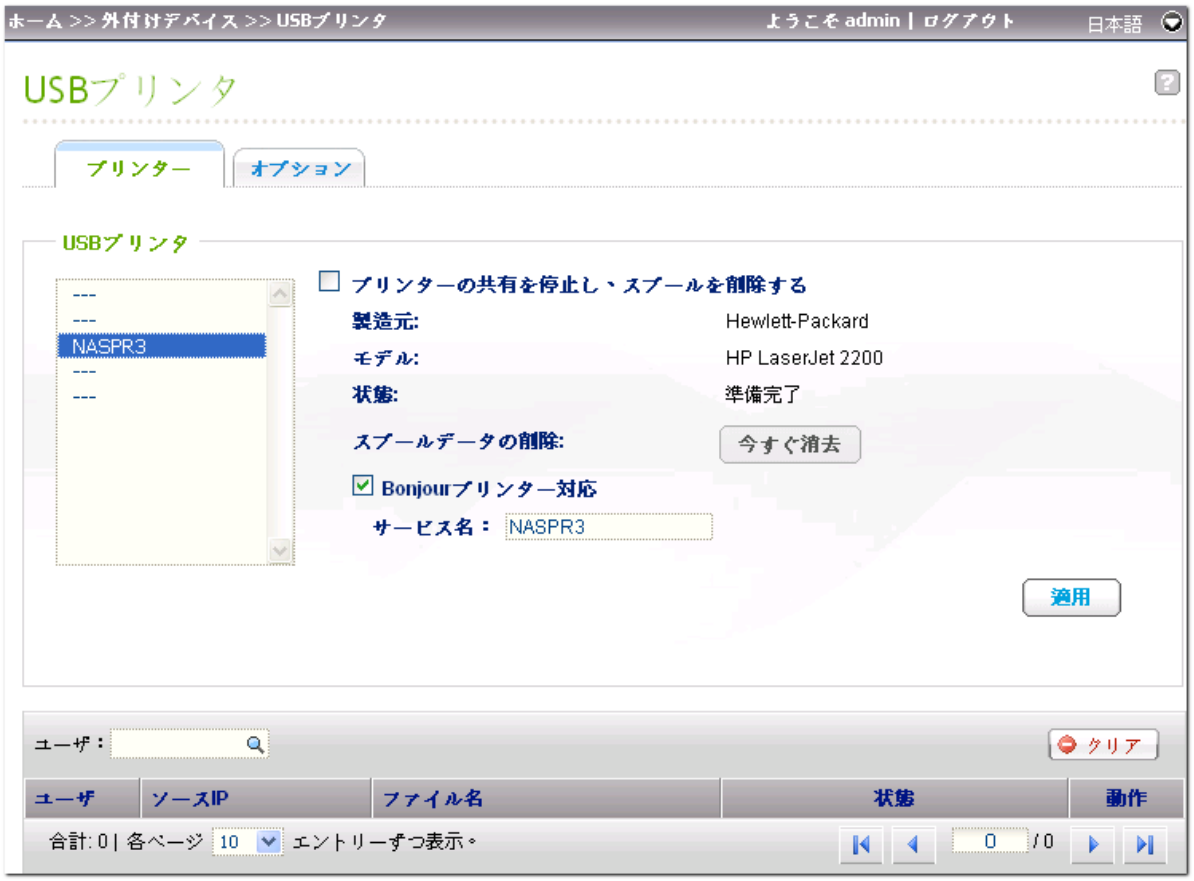
注:

- 一度に Q-RAID 1 として設定できる外部ハードディスクは 1 台のみです。
- NAS の内部ハードドライブと同じ容量の外部ストレージデバイスの利用を推奨します。外部ストレージデバイスのストレージ容量が内部ハードドライブの同期用に小さ過ぎる場合、デバイスはデータ共有用にのみ利用可能です。

9.2 USBプリンタ

NASは、Windows、Mac、Linux (Ubuntu)環境のローカルネットワークおよびインターネット上で、ネットワーク印刷共有サービスをサポートします。 最大3台のUSBプリンタがサポートされます。

NASでUSBプリンタを共有するには、プリンタをNASのUSBポートに接続します。 プリンタは自動的に検出され、プリンタの情報が表示されます。



注：

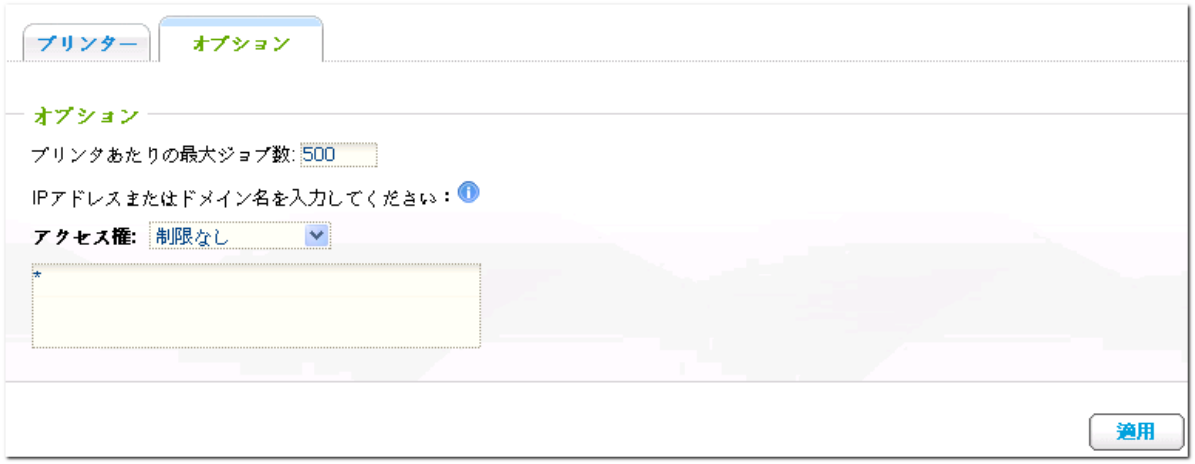
- USBプリンタをサーバに接続する前に、ソフトウェアの設定を完了してください。
- NASは一般のUSBプリンタだけでなく、多機能プリンタにも対応しています。
- プリンタジョブテーブルのファイル名表示は、IPP（インターネット印刷プロトコル）接続経由で送信されるプリンタジョブでのみ使用できます。
- 対応しているUSBプリンタの型番情報については、http://www.qnap.com を参照してください。

プリンタ共有の停止と印刷スプールのクリア
このオプションを選択すると、接続したプリンタの印刷共有が一時的に無効になります。プリンタスプールのすべてのデータも消去されます。

プリンタのスプールスペースの除去
[Clean Now(今消去する)]をクリックしてプリンタスプールに保存したデータを除去します。

Bonjourプリンタサポート
このオプションを選択して、Bonjour経由でMacユーザーに印刷サービスを送信します Bonjourでプリンタを見つけられるサービス名を入力します。 名前には、「a-z」、「A-Z」、「0-9」、ドット(.)、コンマ (,)、ダッシュ (-)のみを含めることができます。

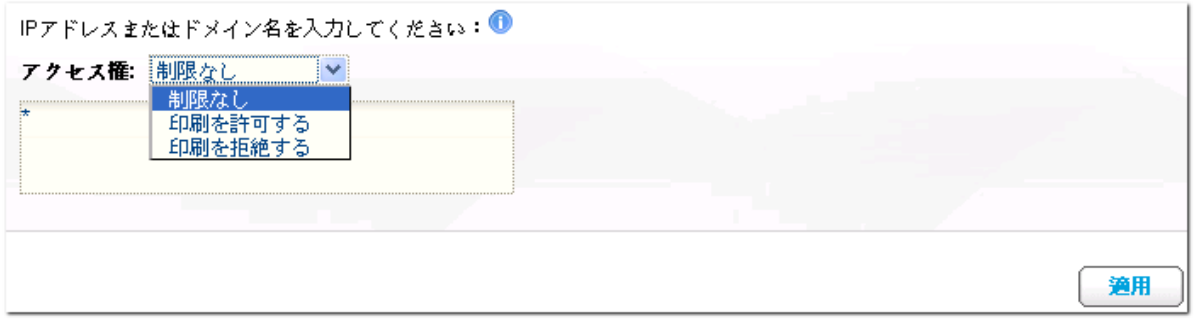
「Options(オプション)」タブで他のプリンタオプションを設定できます。



プリンタあたりの最大プリンタジョブ
プリンタあたりのプリンタジョブの最大数を指定します。プリンタは1,000までのプリンタジョブをサポートします。プリンタジョブの最大数に達すると、もっとも古いプリンタジョブは最新ジョブに置き換えられます。

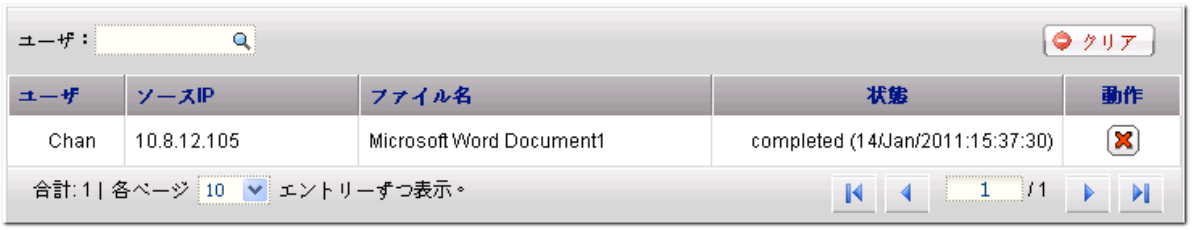
印刷アクセスを許可または拒否するIPアドレスまたはドメイン名を入力する
NASの印刷サービスを使用するために特定のIPアドレスまたはドメイン名を許可または拒否するには、「Allow printing(印刷の許可)」または「Deny printing(印刷の拒否)」を選択し、IPアドレスまたはドメイン名を選択します。アスタリスク(*)はすべての接続を意味します。 すべてのユーザーがプリンタを使用できるようにするには、「No limit(制限なし)」を選択します。「Apply(適用)」をクリックして設定を保存します。

> 注:この機能は、Sambaではなく、IPPとBonjour経由で設定された印刷サービスでのみ作動します。



プリンタジョブの一時停止、再開、削除

進行中または保留中のジョブの一時停止またはキャンセル、一時停止中ジョブの再開、または完了または保留中ジョブの削除を行うことができます。

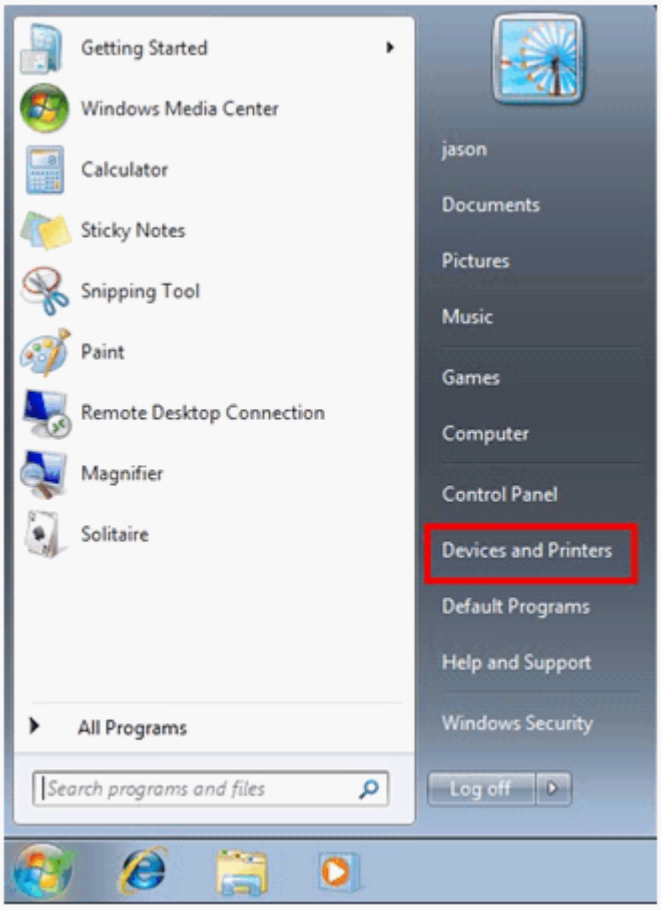


注:印刷が進行中のときまたは待ち行列のジョブがあるとき、NASを再起動したりシステムファームウェアを更新したりしないでください。これを守らないと、シーケンスジョブはキャンセルされ削除されます。

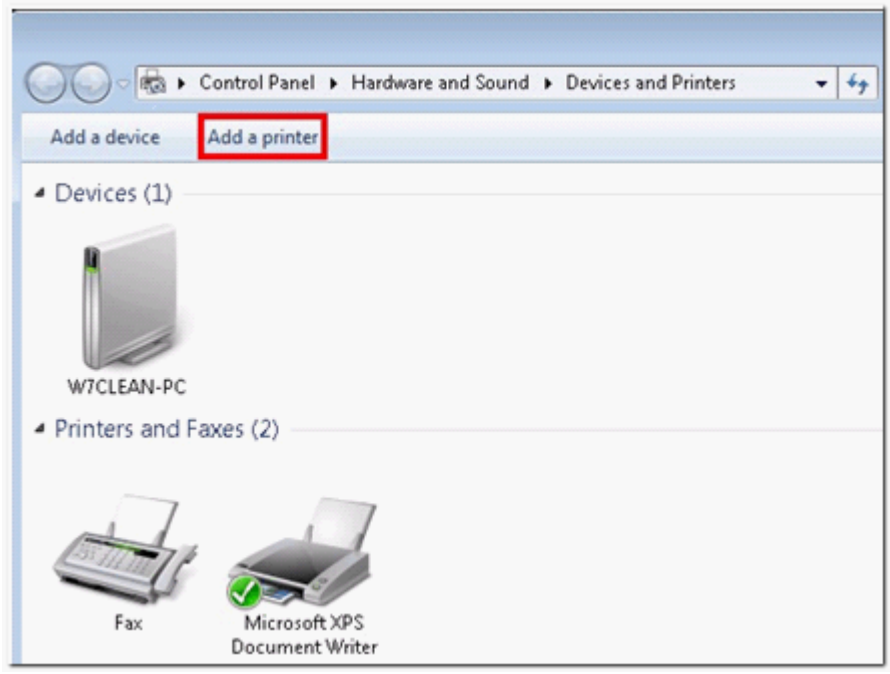
9.2.1 Windows 7, Vistaユーザー

次の説明はWindows 7に適用されます。

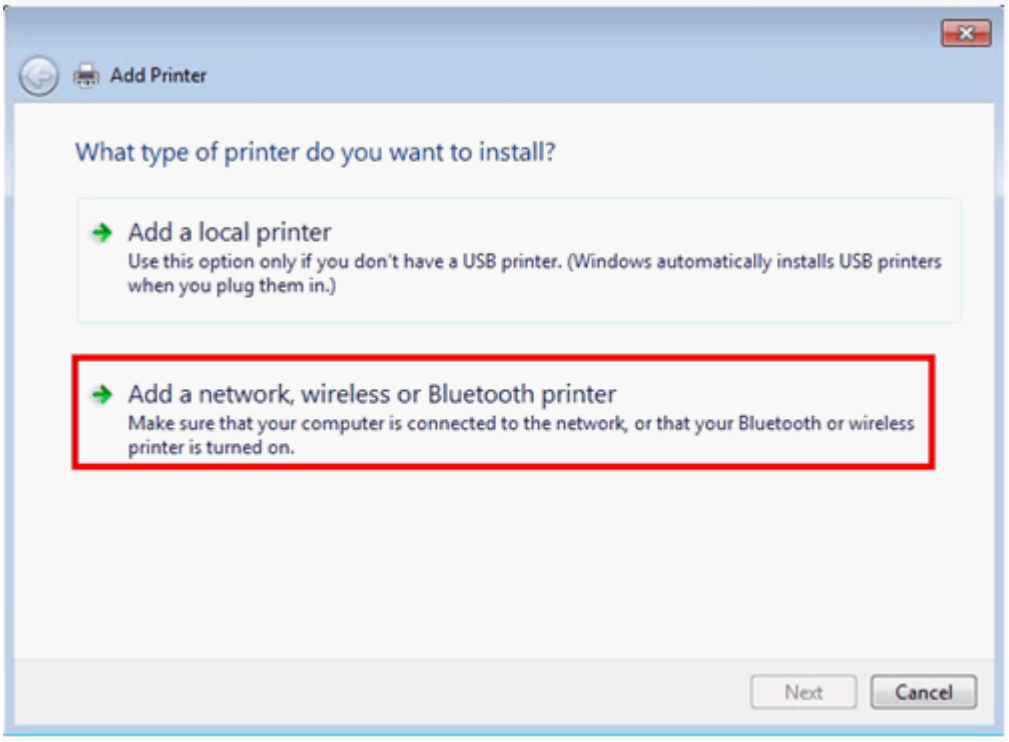
1. 「Devices and Printers（デバイスとプリンタ）」に進んでください。



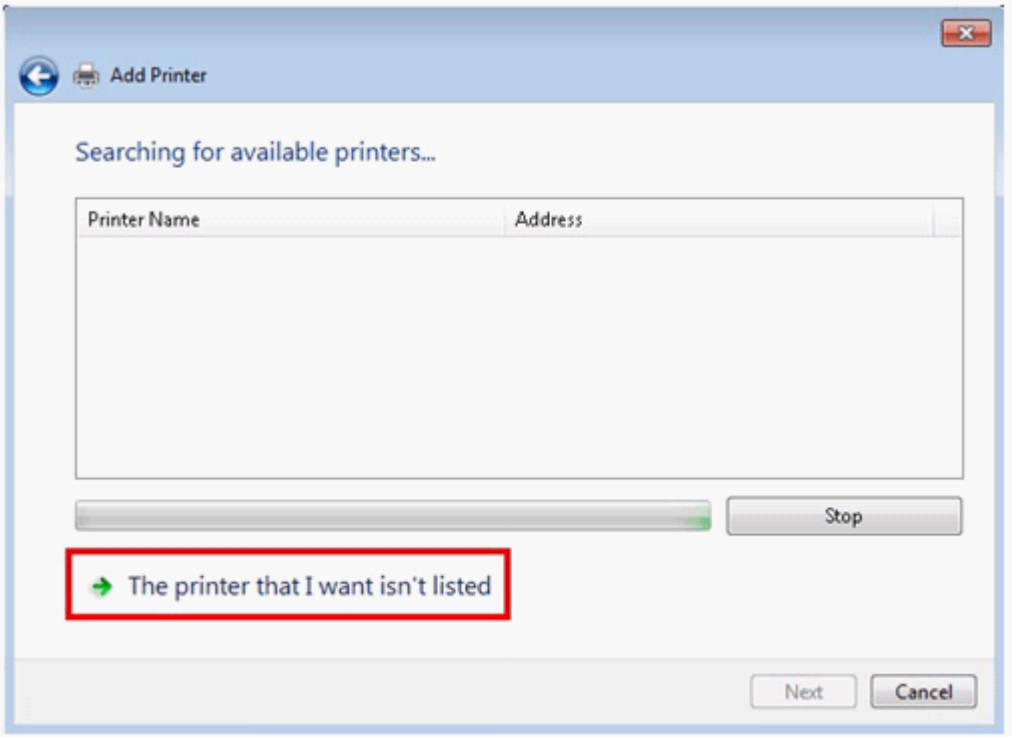
2. 「Add a printer（プリンタの追加）」をクリックします。



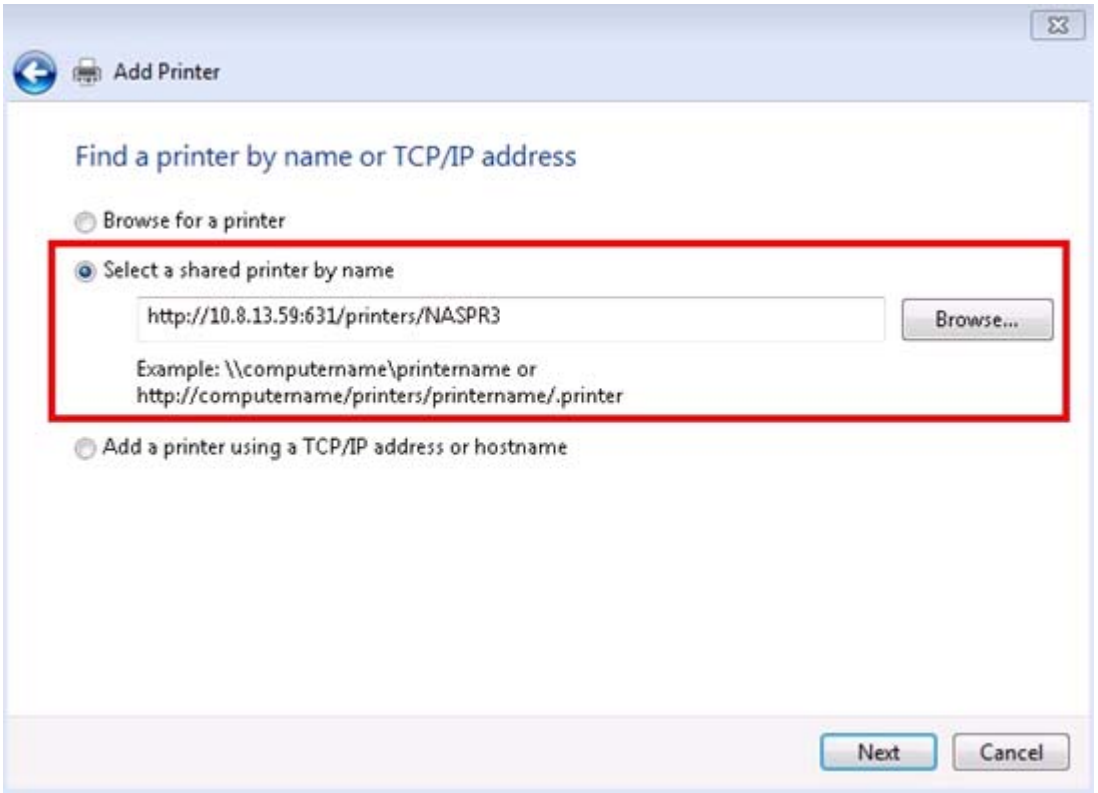
3. 「Add printer（プリンタの追加）」ウィザードで、「Add a network, wireless or Bluetooth printer（ネットワーク、ワイヤレスまたはBluetoothの追加）」をクリックします。



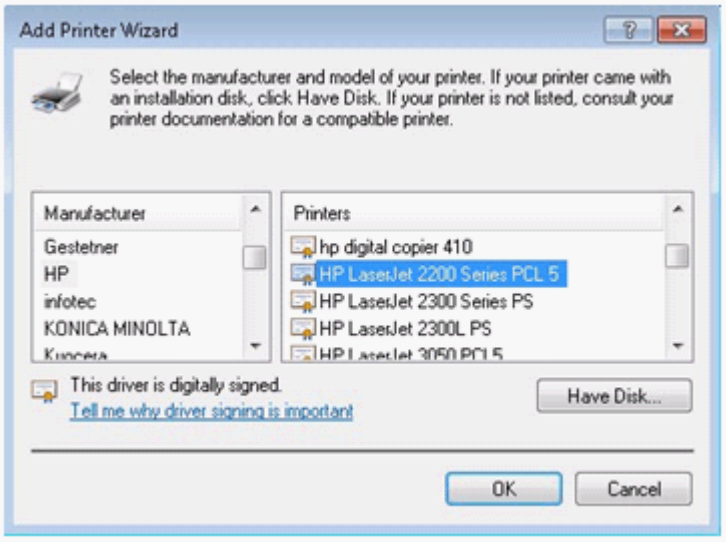
4. Windowsが利用可能なネットワークプリンタを検索している間、「希望するプリンタが一覧にありません」をクリックします。



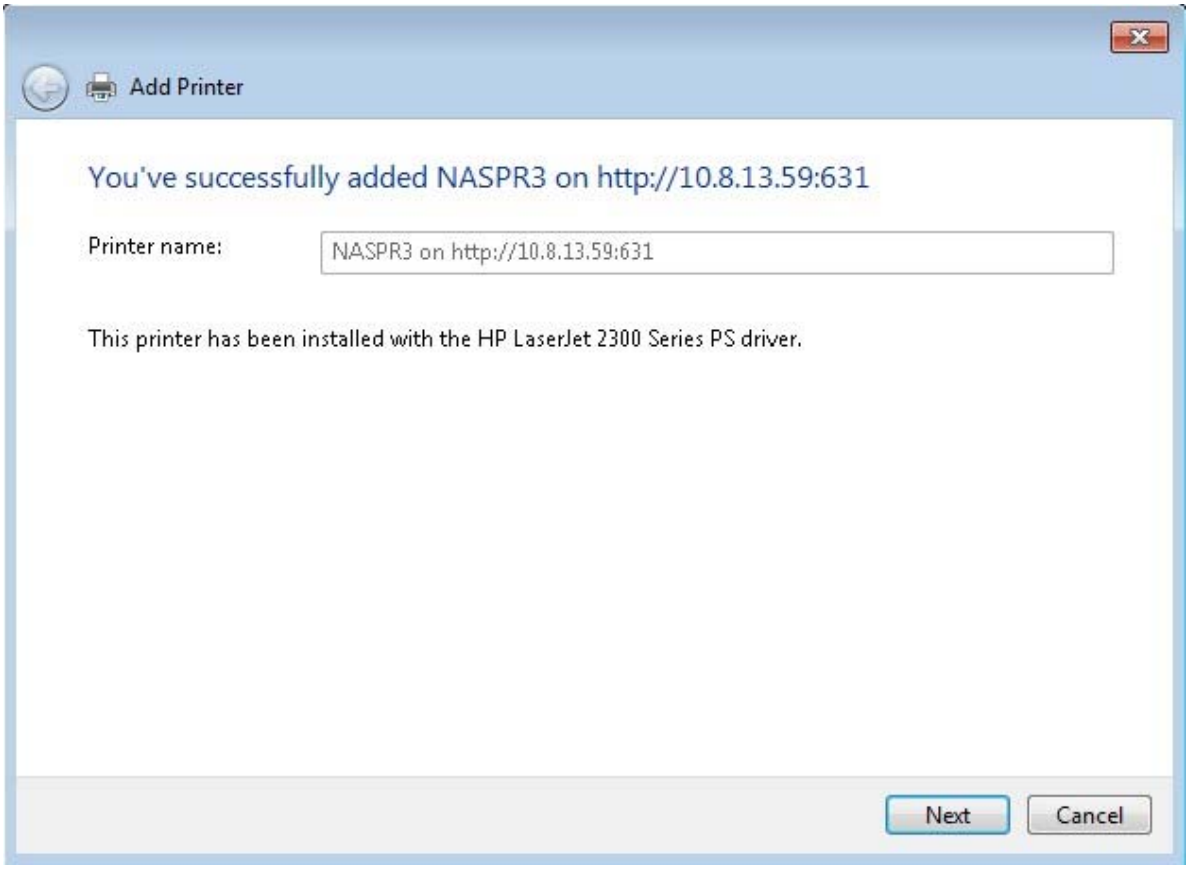
5. 「名前で共有されたプリンタを選択する」をクリックしてから、ネットワークプリンタのアドレスを入力します。アドレスは次の形式です – http://NAS_IP:631/printers/ServernamePR。プリンタをリモートで印刷する場合、NAS_IPをドメイン名アドレスにすることもできます。例えば、http://10.8.13.59:631/printers/NASPR3



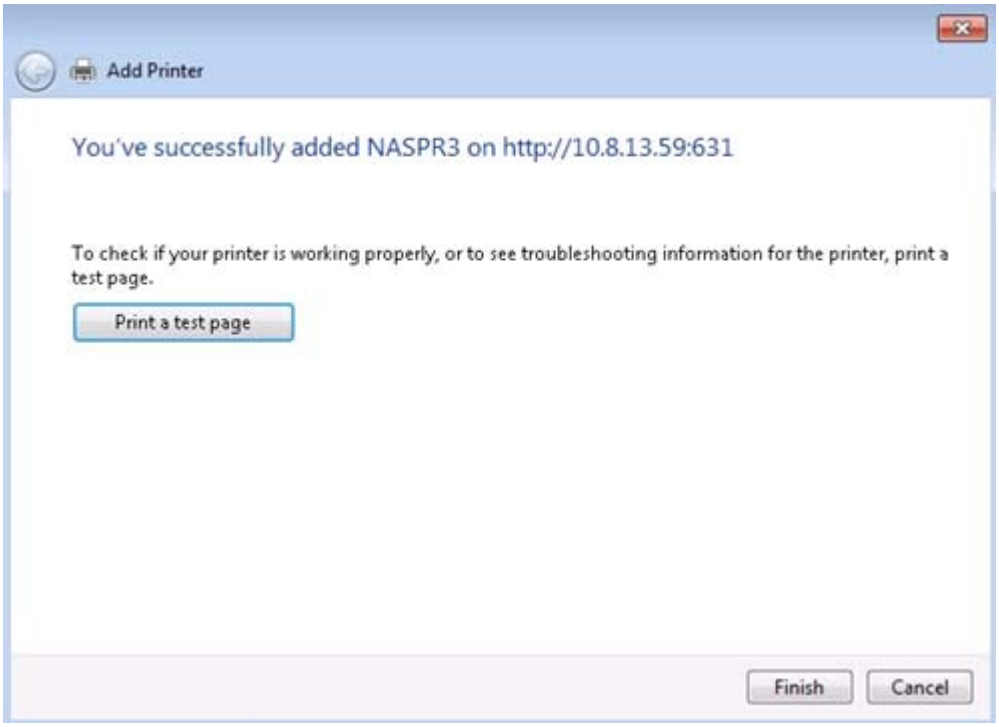
6. 正しいプリンタドライバを求めるプロンプトが表示されます。Windowsオペレーティングシステムに組み込まれていない場合、メーカーのWebサイトから最新のプリンタドライバをダウンロードすることもできます。



7. 正しいプリンタドライバをインストールした後、新しいネットワークプリンタのアドレスとドライバが表示されます。



8. デフォルトのプリンタとしてネットワークプリンタをセットアップしたり、テストページを印刷することもできます。「FINISH（終了）」をクリックしてウィザードを終了します。

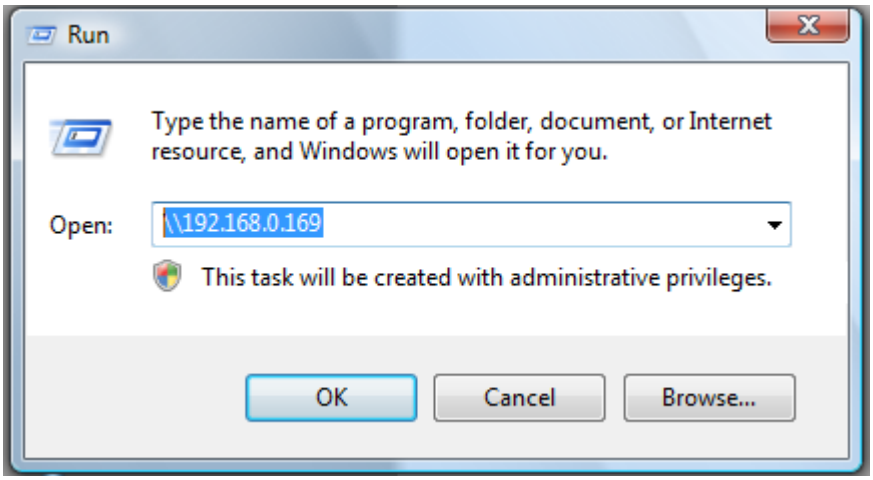


9. 新しいネットワークプリンタが印刷できるようになります。

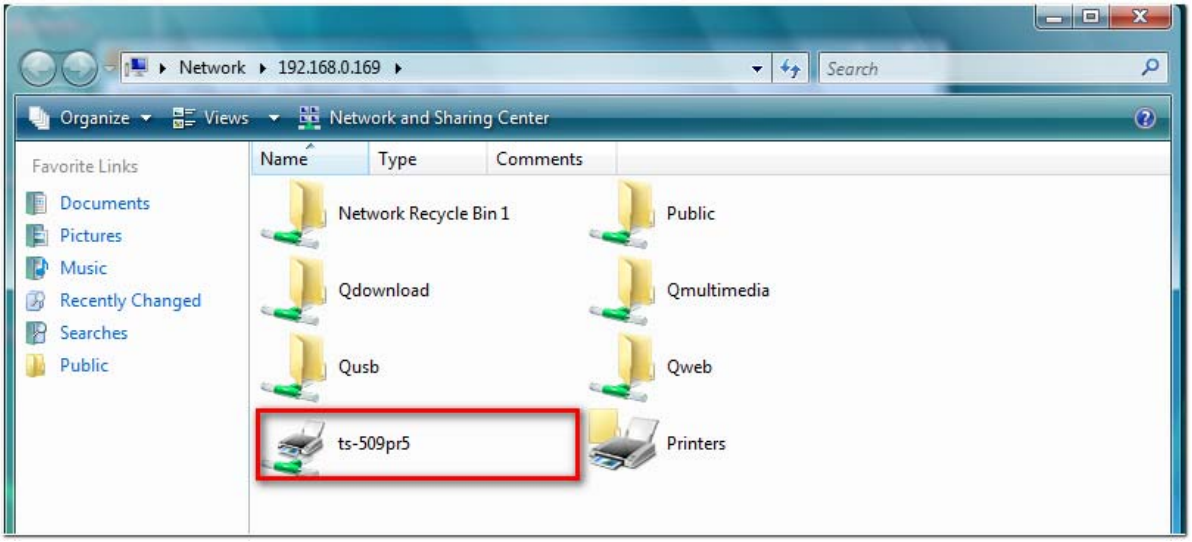
次の説明はWindows 7とVista OSに適用されます。

以下の手順に従ってNASのプリンタ機能を構成してください。

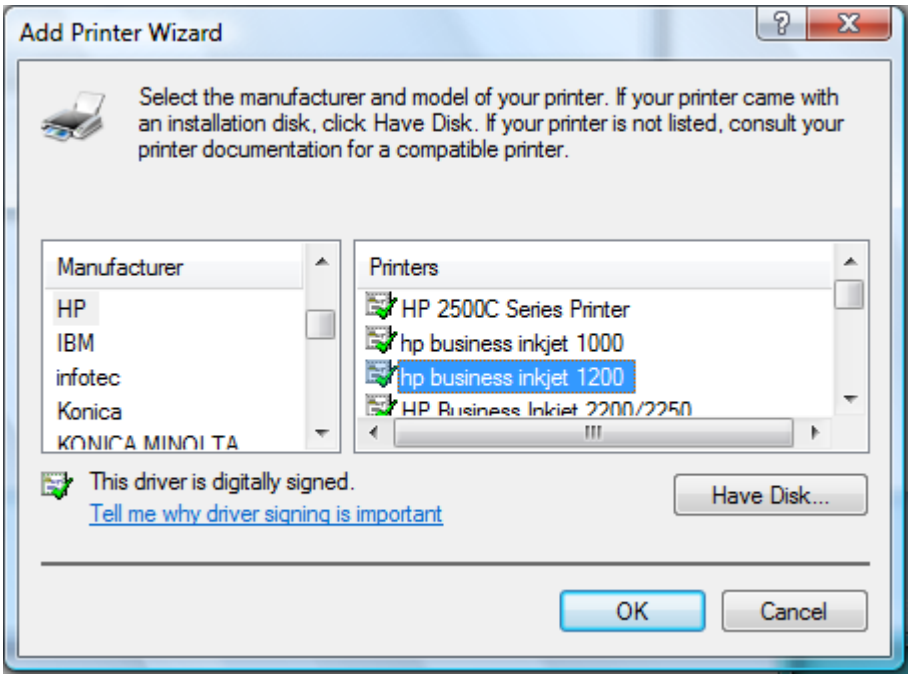
1. "Run" (ファイル名を指定して実行)メニューで、\\NAS IPを入力します。



2. ネットワークプリンタアイコンを見つけ、それをダブルクリックします。



3. 正しいプリンタドライバをインストールします。



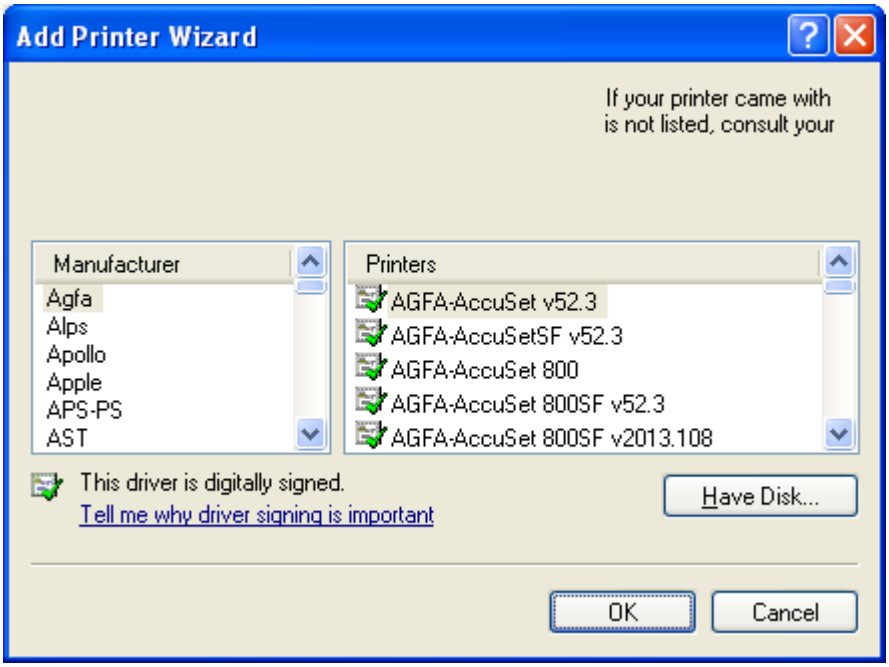
4. 完了したら、テストページを印刷してプリンタの使用準備ができていることを確認します。

9.2.2 Windows XPユーザー

以下の手順に従ってNASのプリンタ機能を構成してください。

方式1

1. Windows Explorerで\\NAS IPを入力します。
2. プリンタアイコンが、サーバの共フォルダに表示されます。アイコンをダブルクリックします。
3. プリンタドライバをインストールします。



4. 終了すると、NASのネットワークプリンタサービスを使用できるようになります。

方式2

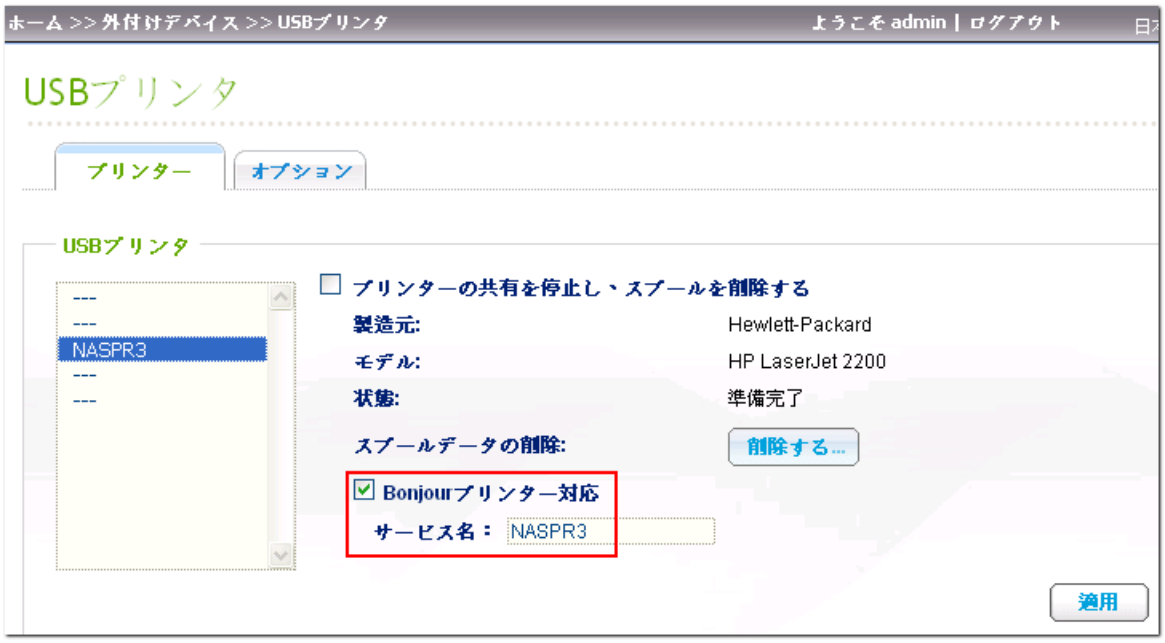
次の設定方式はWindows XPでのみ確認されています：

1. [プリンタとFAXを開きます]。
2. 既存のネットワークプリンタがある場合、それを削除します。
3. プリンタとFAXウィンドウでブランク領域を右クリックします。[サーバーのプロパティ]を選択します。
4. [ポート]タブをクリックし、以前のネットワークプリンタに対して設定されていたポートがあれば、それを削除します。
5. PCを再起動します。
6. プリンタとFAXを開きます。
7. [プリンタの追加をク]リックし、[次へ]をクリックします。
8. [このコンピュータに接続されたローカルプリンタ]を選択します。[次へ]をクリックします。
9. [新規ポートの作成]をクリックし、ドロップダウンメニューから[ローカルポート]を選択します。[次へ]をクリックします。
10. ポート名を入力します。形式は\\NAS IP\NAS名prです。たとえば、NAS IP= 192.168.1.1, NAS名= myNAS、リンクは\\192.168.1.1\myNASprです。
11. プリンタドライバをインストールします。
12. テストページを印刷します。

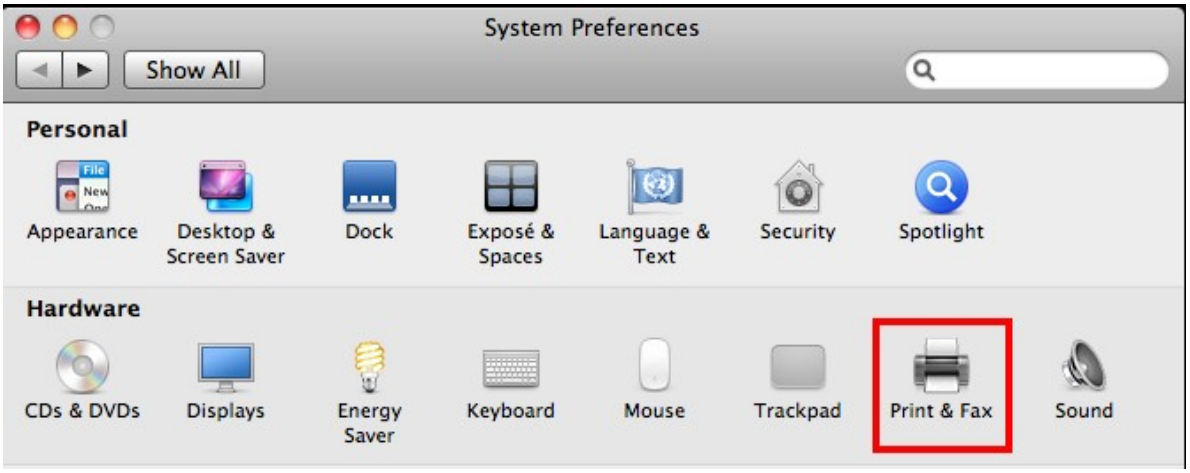
9.2.3 Mac OS 10.6

Mac OS X 10.6をご使用の場合は、以下の手順に従ってNASのプリンタ機能を構成してください。

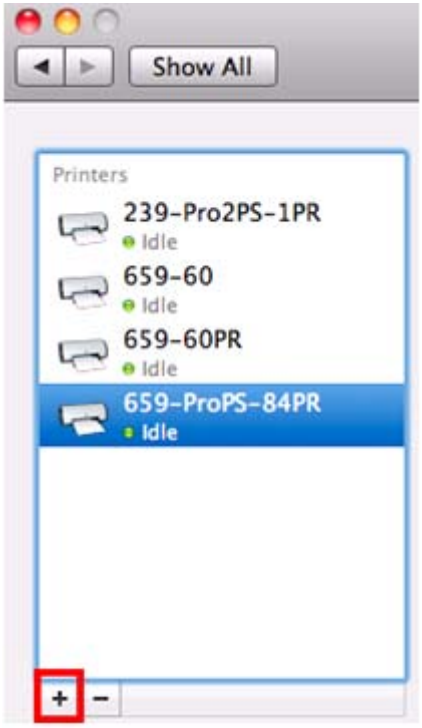
1. まず、「External Device（外部デバイス）」>「USB Printer（USBプリンタ）」を順にクリックして、Bonjourプリンタサポートが NASで有効になっていることを確認します。サーバー名をプリンタによりふさわしい名前に変更することができます。



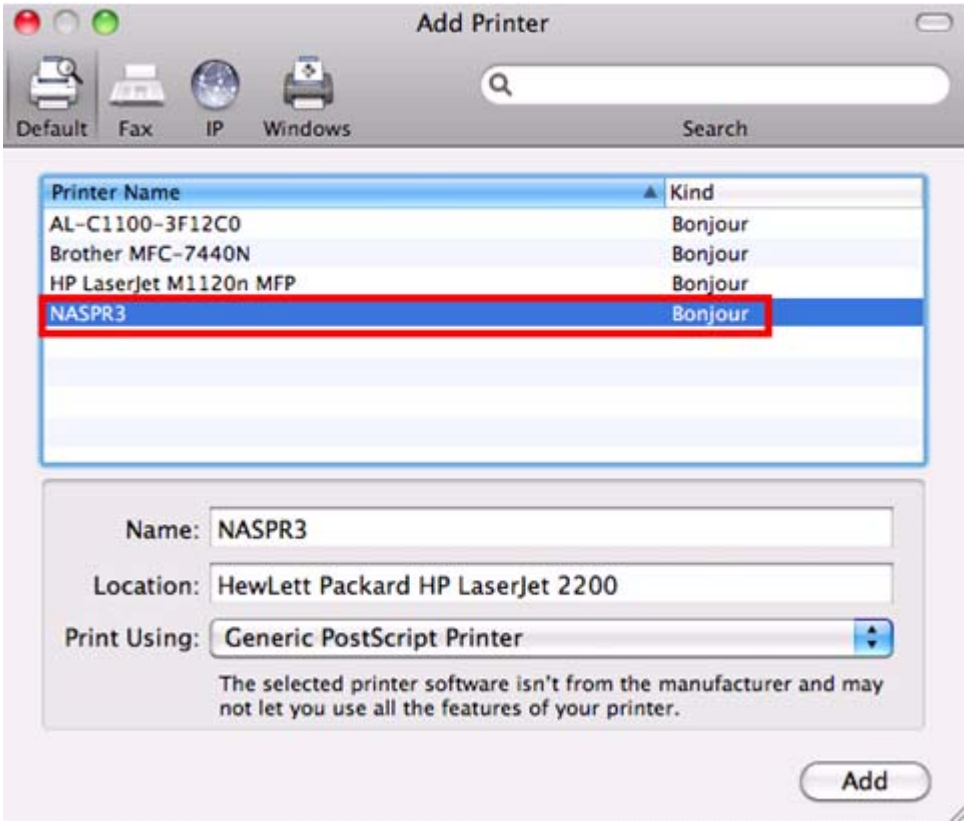
2. Macの場合、「System Preferences（システム初期設定）」をポイントし、「Print & Fax（プリンタとファックス）」をクリックします。



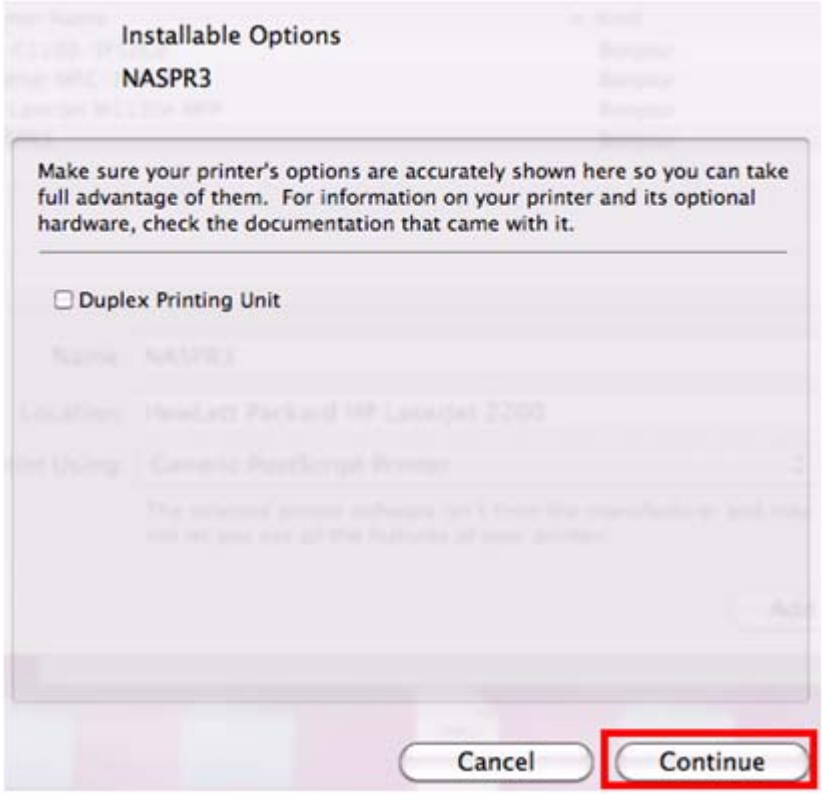
3. 「Print & Fax（プリンタとファックス）」ウィンドウで、+ をクリックして新しいプリンタを追加します。



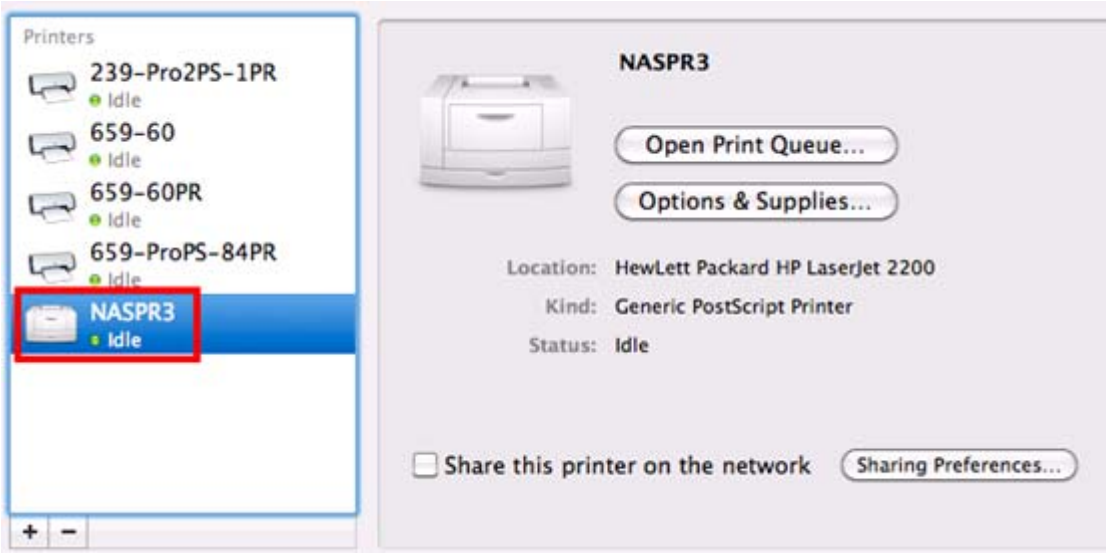
4. USBネットワークプリンタは、Bonjour経由で一覧表示されます。デフォルトのプリンタドライバを選択するか、プリンタメーカーのWebサイトから最新のドライバをダウンロードしてインストールすることができます。「Add（追加）」をクリックしてこのプリンタを追加します。



5. お使いのプリンタで追加オプションが利用できるようになります。「Continue（続行）」をクリックします。



6. 新しいネットワークプリンタが印刷できるようになります。

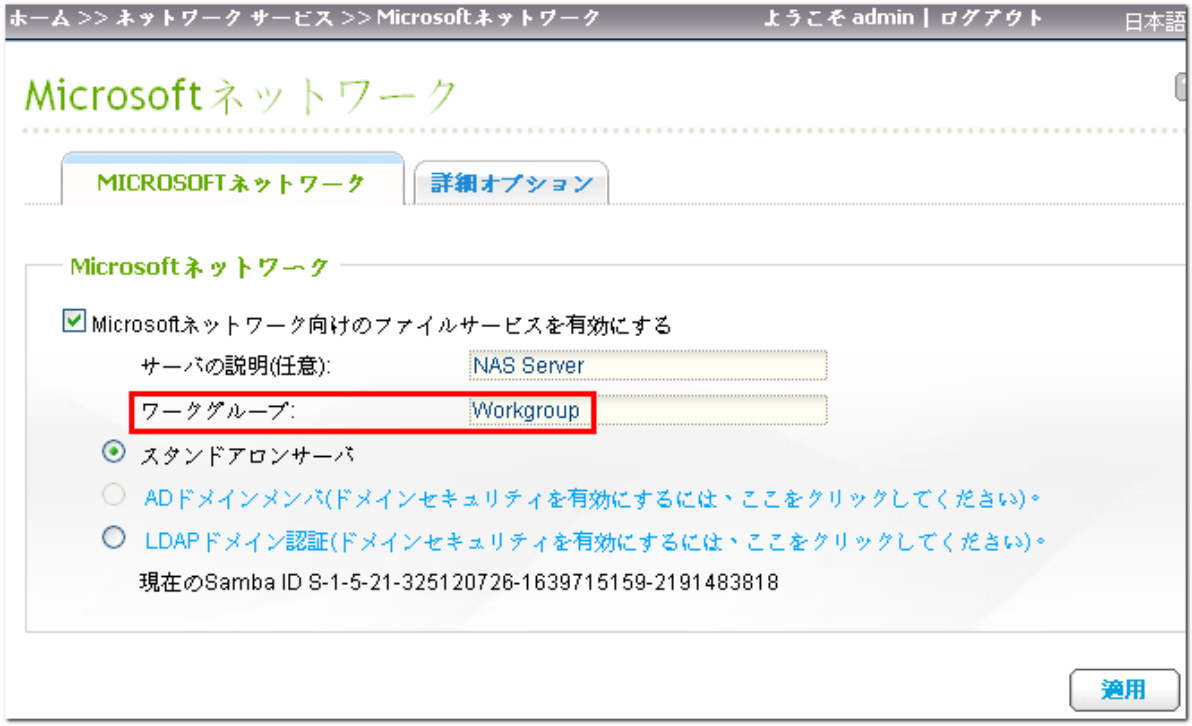


9.2.4 Mac OS 10.5

Mac OS X 10.5をご使用の場合は、以下の手順に従ってNASのプリンタ機能を構成してください。

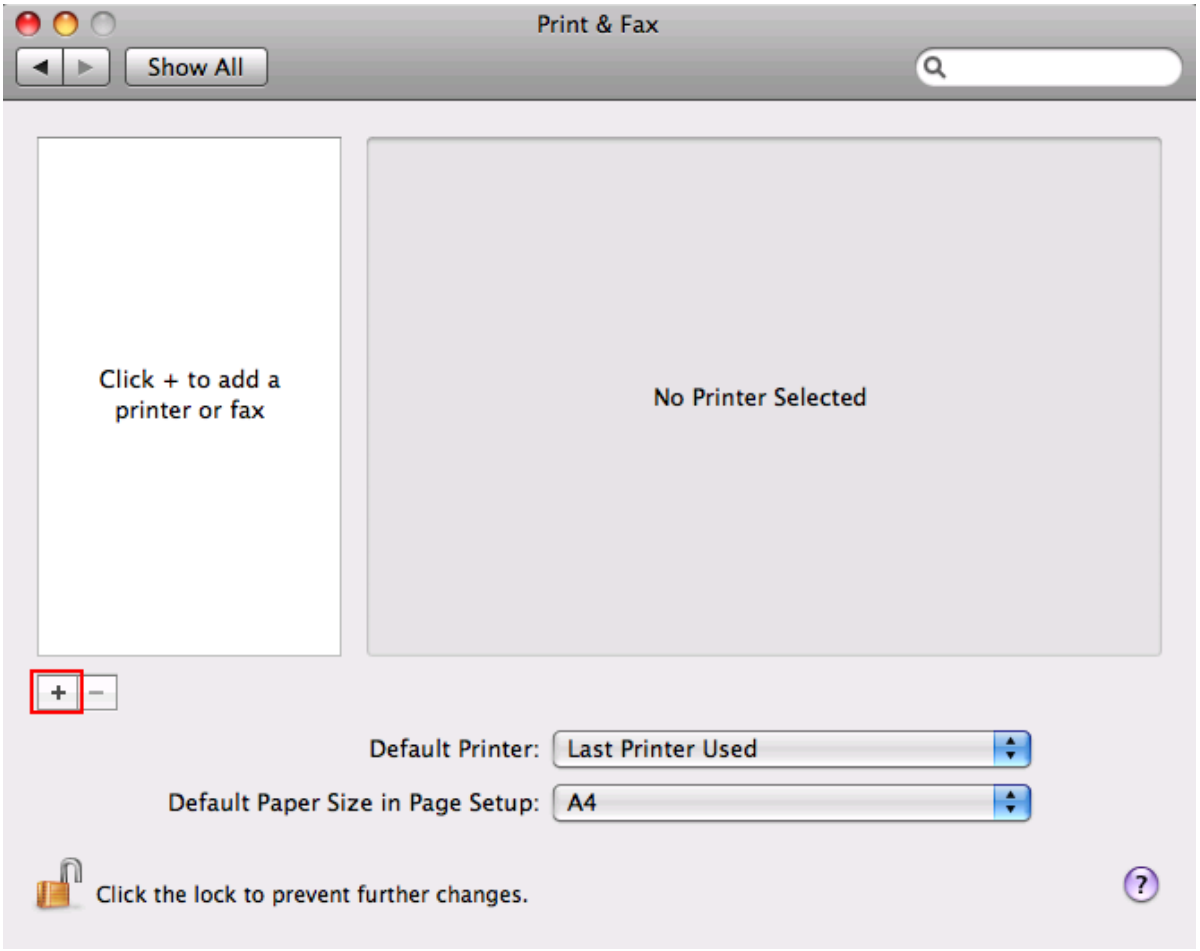
1. プリンタがNASに接続され、"USBプリンタ"ページに情報が正しく表示されている ことを確認してください。

2. 「ネットワーク設定」 >「Microsoftネットワーク 」に移動します。NAS用のワークグループ名を入力します。この情報は後に必要となります。

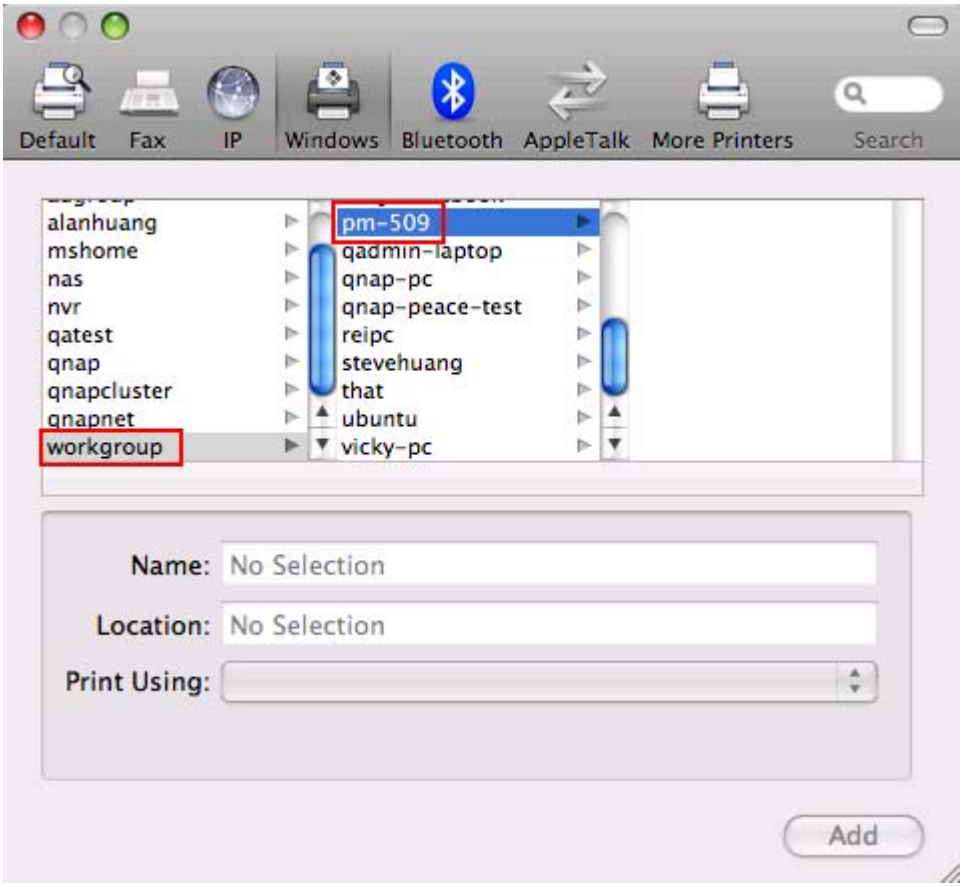


3. Macの「印刷とファックス」に移動します。

4. + をクリックして新規プリンタを追加します。

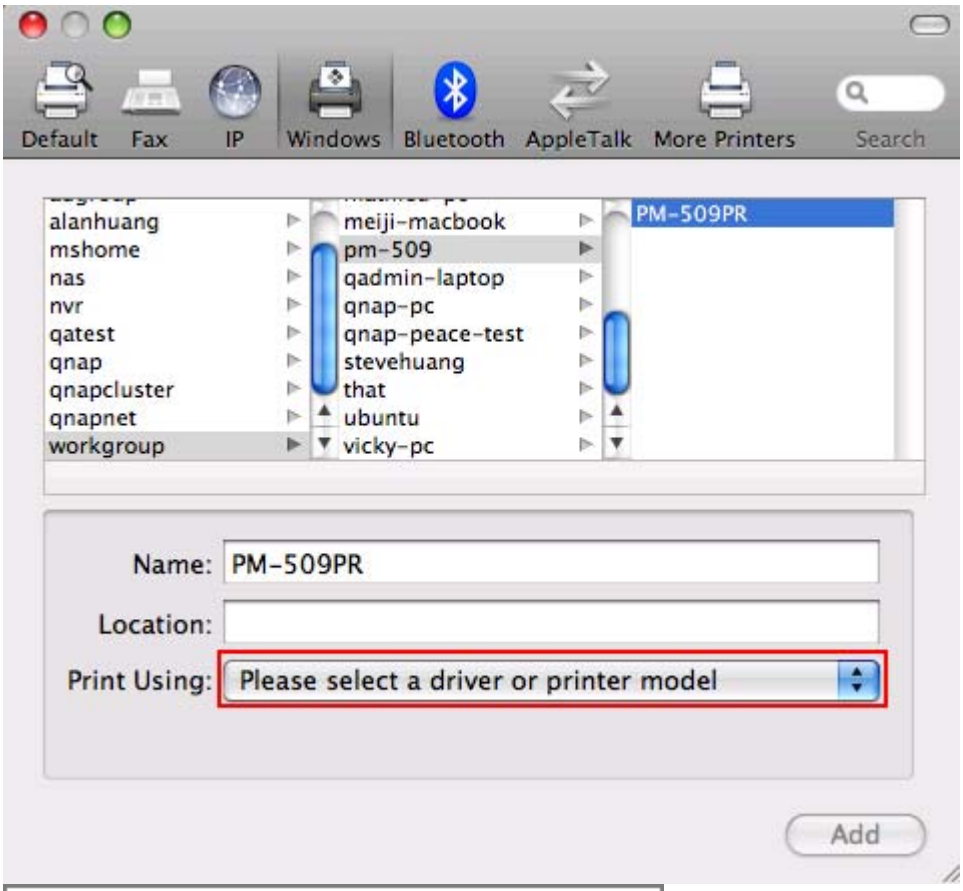


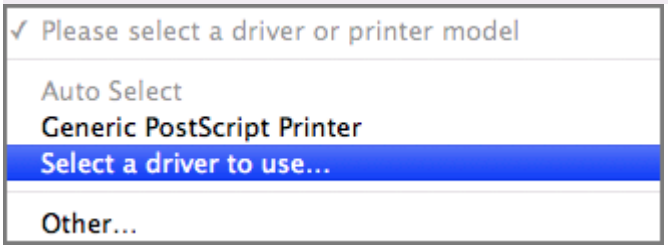
5. NASワークグループを選択し、続いてプリンタ名を選択します。



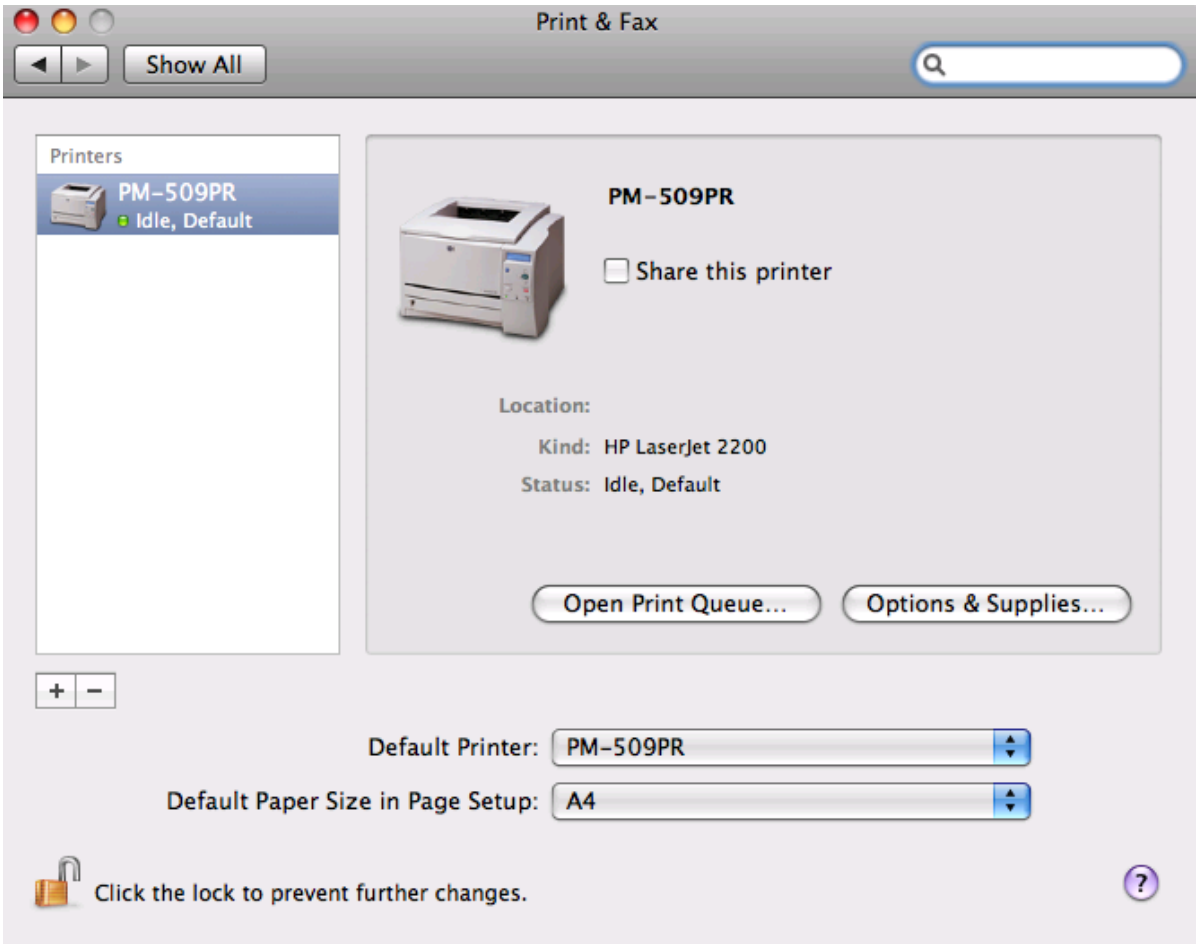
6. ユーザー名及びパスワードを入力し、NAS上のプリンタサーバにアクセスします。

7. プリンタドライバを選択します。





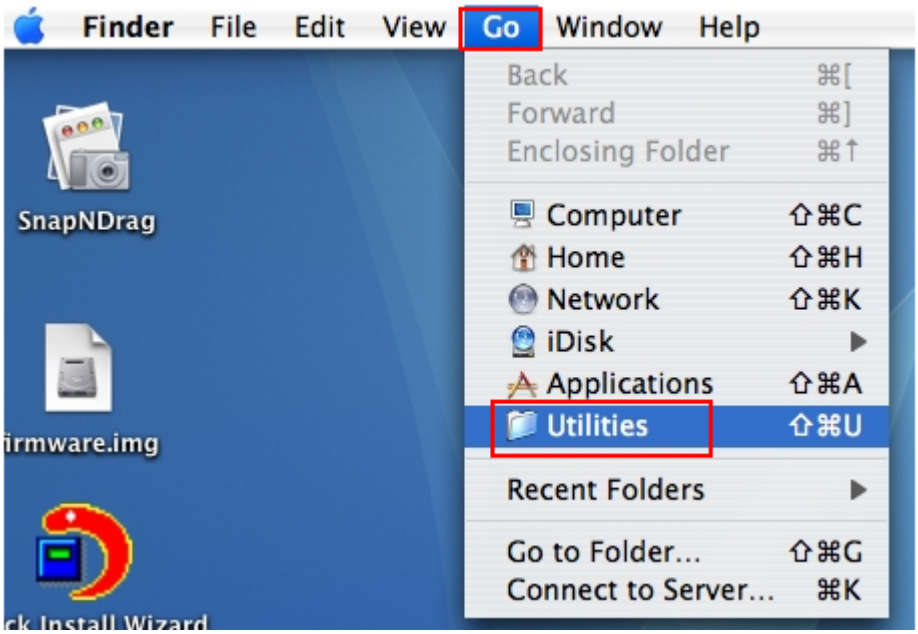
8. プリンタドライバが正常にインストールされると、プリンタの使用を開始することができます。



9.2.5 Mac OS 10.4

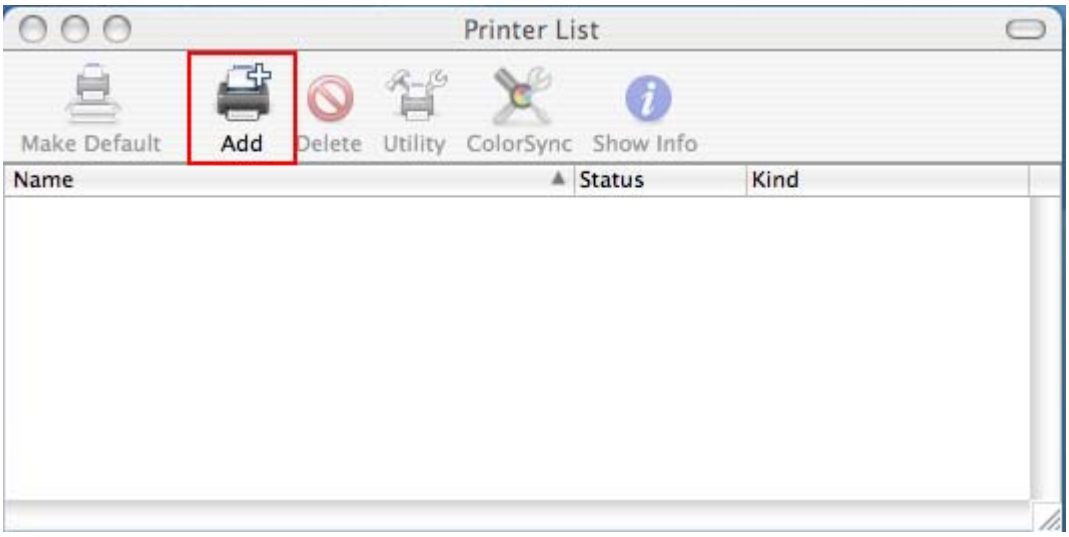
Mac OS X 10.4をご使用の場合は、以下の手順に従ってNASのプリンタ機能を構成してください。

1. ツールバーで、[移動/ ユーティリティ]をクリックします。



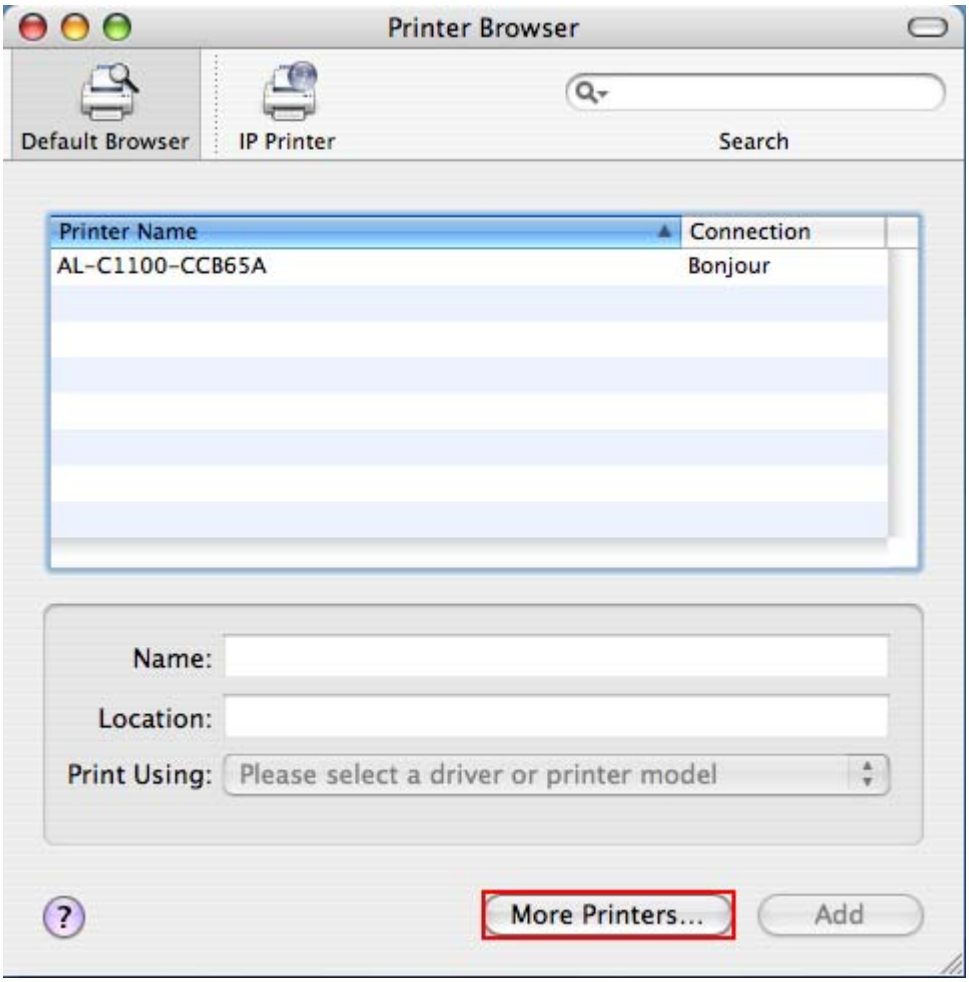
2. [プリンタセットアップユーティリティ]をクリックします。

3. [追加]をクリックします。



4. キーボードでaltキー

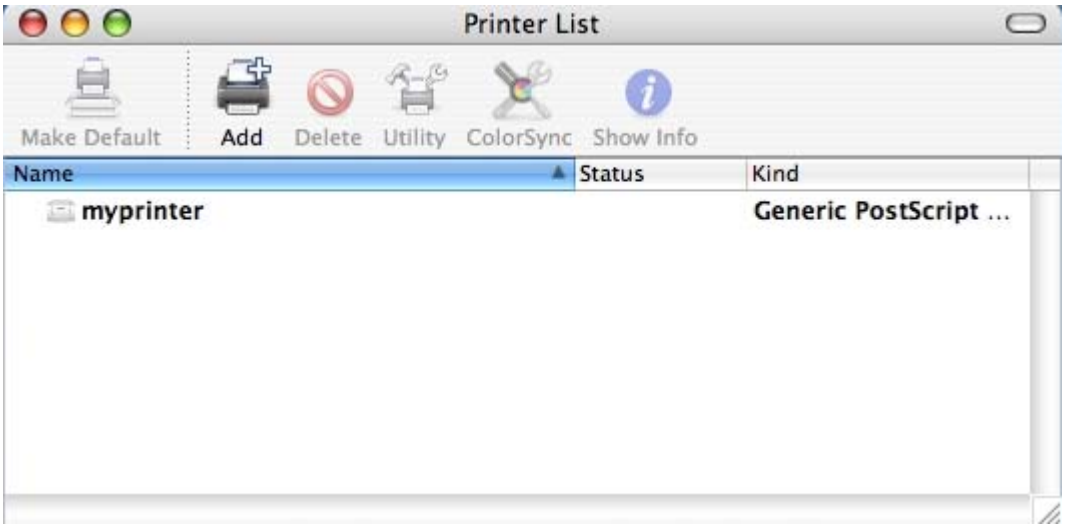
を押し下げながら、同時に[プリンタの追加]をクリックします。



5. ポップアップウィンドウで、次の操作を実行します。
   a. [詳細設定]を選択します。
   b. [SAMBAを組み込んだWindowsプリンタ]を選択します。
   c. プリンタ名を入力します。
   d. プリンタのURIを入力します。形式はsmb://NAS IP/printer名です。プリンタ名はデバイス設定/ USBプリンタページに出ています。
   e. プリンタモデルで[汎用]を選択します。
   f. [追加]をクリックします。

拡張プリンタ設定を表示するには、altキーを押し下げながら、同時に[プリンタの追加]をクリックする必要があります。それ以外の場合、このオプションは表示されません。

6. プリンタはプリンタリストに表示されます。これで使用する準備が整いました。



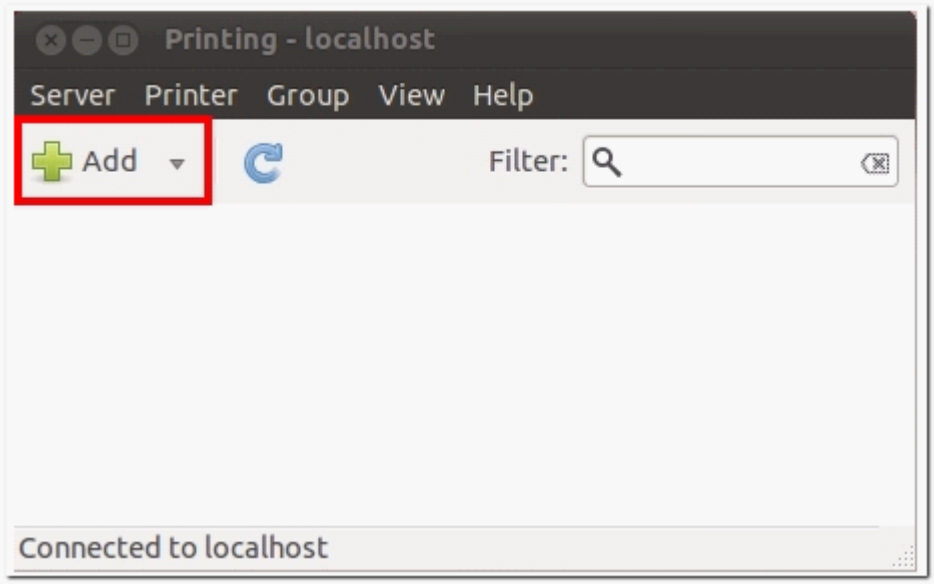
注: NASネットワークプリンタサービスは、Mac OSのPostscriptプリンタのみをサポートします。

9.2.6 Linux (Ubuntu 10.10)

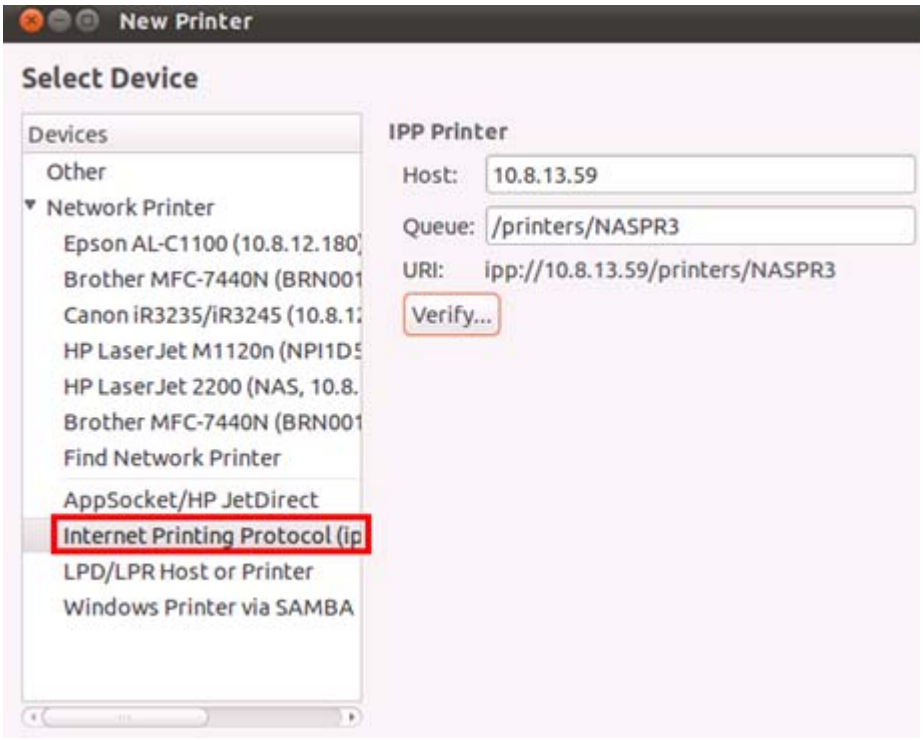
Linux (Ubuntu 10.10)をご使用の場合は、以下の手順に従ってNASのプリンタ機能を構成してください。

1. 「System（システム）」タブをクリックし、「Administration（管理）」を選択します。「Printing（印刷する）」を選択します。

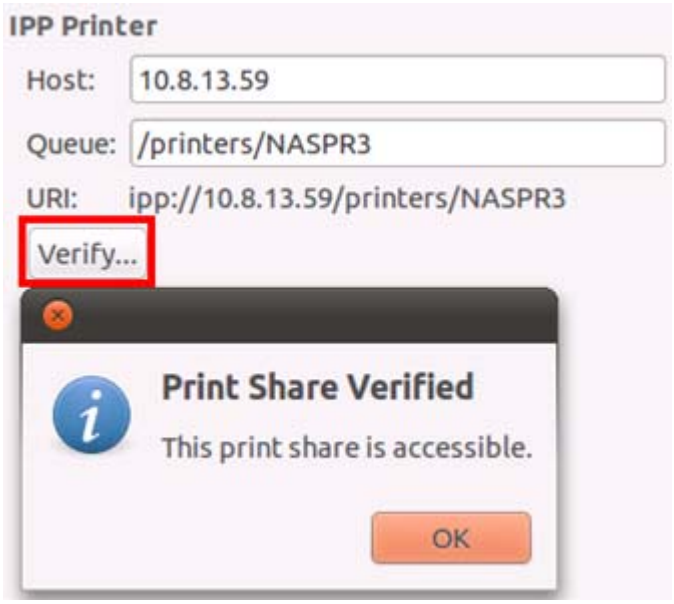
2. 「Add（追加）」をクリックして新しいプリンタを追加します。



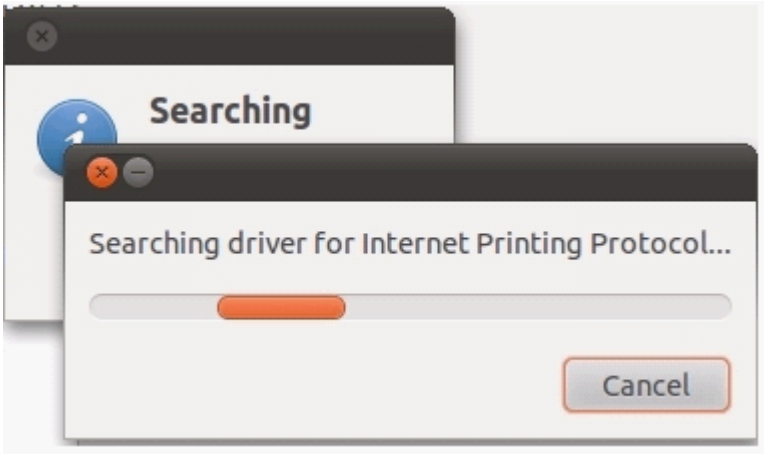
3. 「Network Printer（ネットワークプリンタ）」をクリックしてから、「Internet Printing Protocol (ipp)（インターネット印刷プロトコル (ipp)）」を選択します。「Host（ホスト）」にNAS IPアドレスを入力します。「/printers」がすでに存在します。「Queue（待ち行列）」フィールドの「printers/」の後にプリンタ名を入力します。



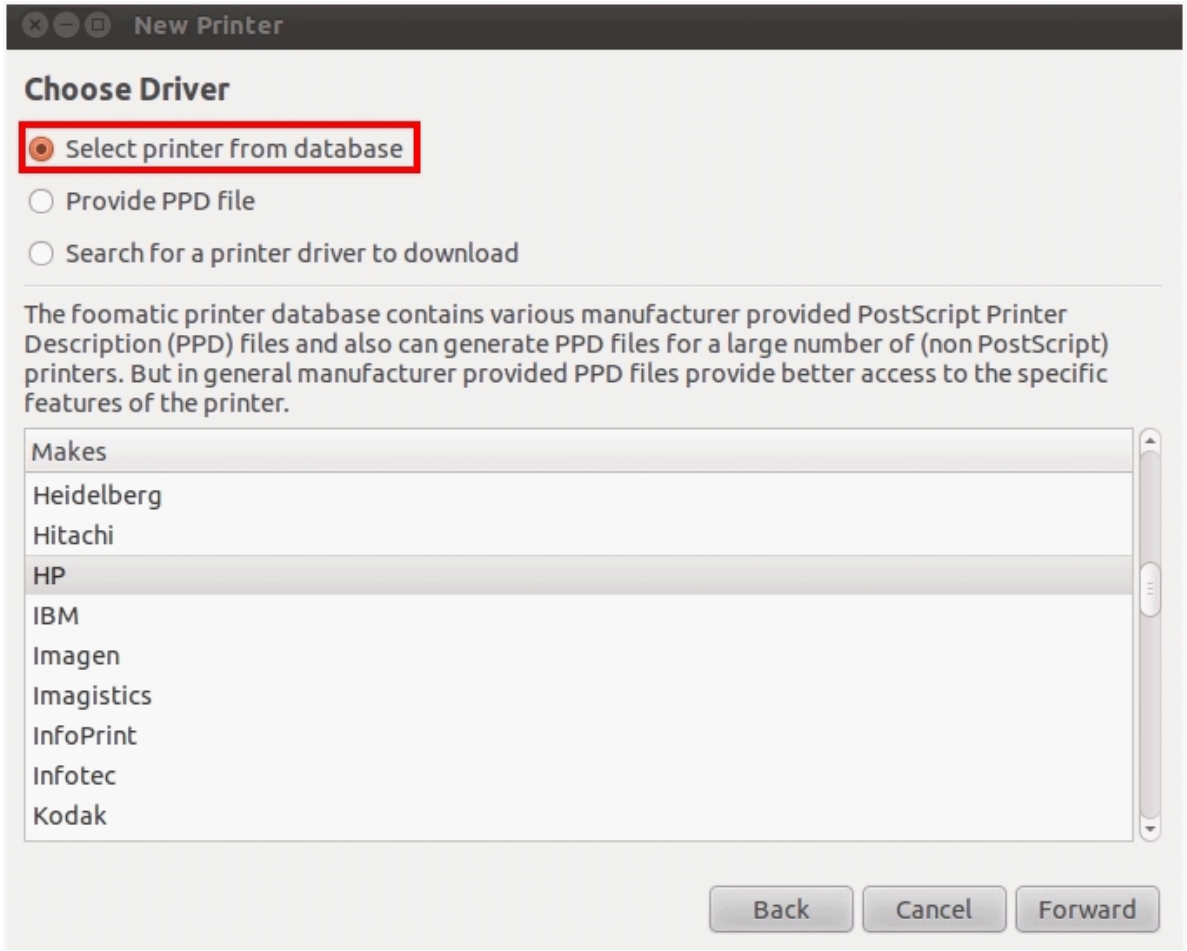
4. 続ける前に、「Verify（検証）」をクリックしてプリンタ接続をテストできます。



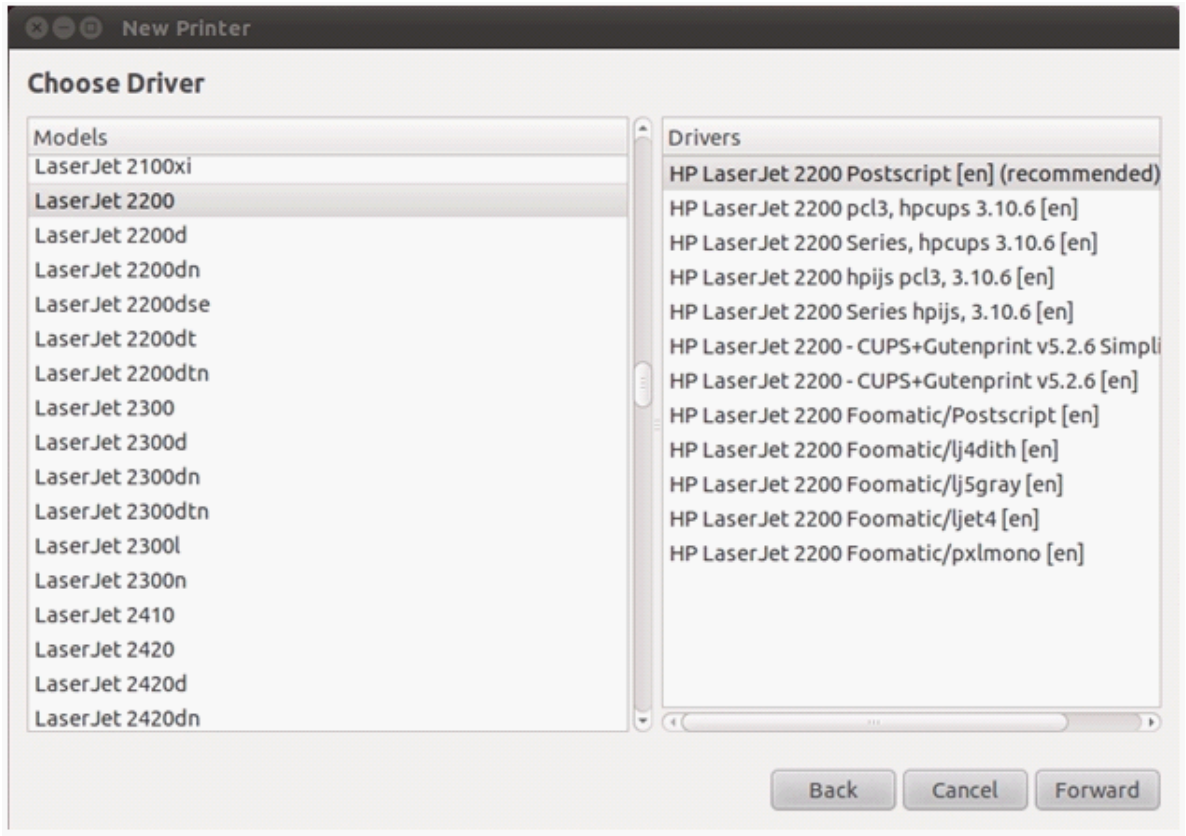
5. オペレーティングシステムは、可能なドライバリストの検索を開始します。



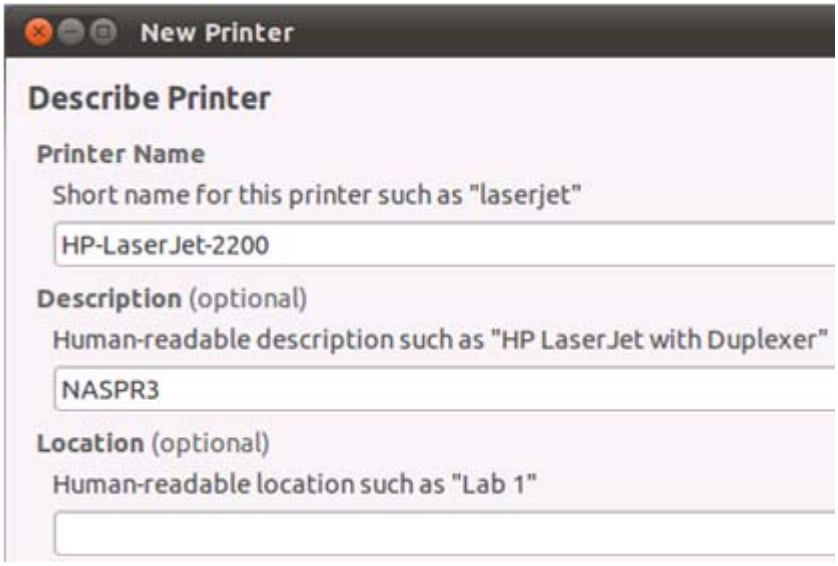
6. 組み込みデータベースからプリンタドライバを選択するか、オンライン検索します。



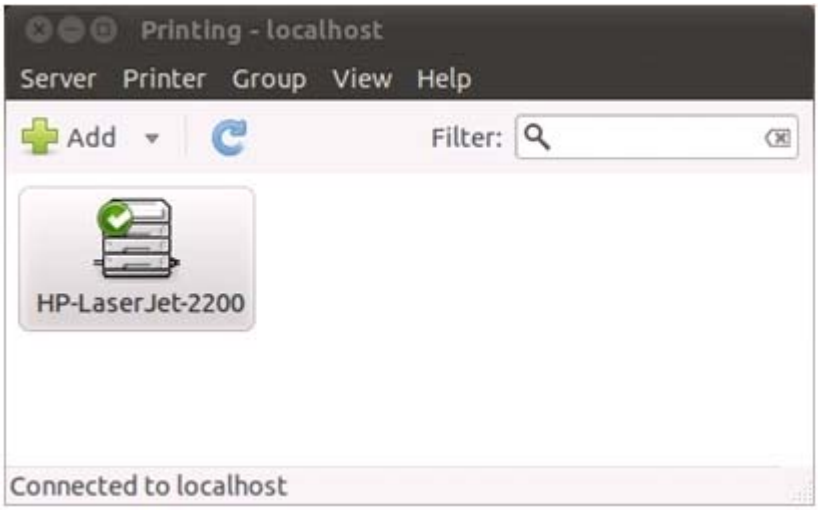
7. 正しいプリンタモデルとドライバを選択します。プリンタによっては、次の手順で追加プリンタオプションを利用できるものもあります。



8. このプリンタの名前を変えたり、追加情報を入力できます。「Apply（適用）」をクリックして終了します。



9. ネットワークプリンタが印刷できるようになります。



9.3 UPS設定

UPS (無停電電源装置) サポートを有効化することにより、電源遮断によるNASの異常なシステムシャットダウンを防ぐことができます。電源が停止した場合、NASは自動的にシャットダウンするか、あるいは接続されたUPSユニットの電源ステータスを検出し自動保護モードに入ります。

スタンドアローン・モード–USB

USBスタンドアローン·モードで操作するには、以下の手順に従ってください。

1. UPSのUSBケーブルをNASに挿し込みます。
2. "Enable UPS Support" (UPSサポート効化) オプションを選択します。
3. AC電源停止の際に、NASがシャットダウンするか自動保護モードに入るかを選択します。選択したオプションをNASが実行するまでの待ち時間を分単位で指定します。NASが自動保護モードに入った後に電源が復旧した際には、NASはもとの操作ステータスに戻ります。
4. "Apply" (適用) をクリックして確定します。

スタンドアローン・モード–SNMP

SNMPスタンドアローン·モードで操作するには、以下の手順に従ってください。

1. NASがSNMPベースのUPSと同一の物理ネットワークに接続されていることを確認してください。
2. "Enable UPS Support" (UPSサポート効化) オプションを選択します。
3. AC電源停止の際に、NASがシャットダウンするか自動保護モードに入るかを選択します。選択したオプションをNASが実行するまでの待ち時間を分単位で指定します。NASが自動保護モードに入った後に電源が復旧した際には、NASはもとの操作ステータスに戻ります。
4. "Protocol" (プロトコル) ドロップダウンメニューから"SNMP"を選択します。
5. SNMPベースのUPSのIPアドレスを入力します。
6. "Apply" (適用)をクリックして確定します。

ネットワークマスター·モード

ネットワークUPSマスターは、同一の物理ネットワーク上のネットワークUPSスレーブに対し、重要な電源ステータスについてコミュニケーションをとる責任を担っています。UPSを備えたNASをネットワークマスター·モードにセットアップするには、UPSのUSBケーブルをNASに接続し、以下の手順に従ってください。

1. NASがネットワークUPSスレーブと同一の物理ネットワークに接続されていることを確認してください。
2. "Enable UPS Support" (UPSサポート効化)オプションを選択します。
3. AC電源停止の際に、NASがシャットダウンするか自動保護モードに入るかを選択します。選択したオプションをNASが実行するまでの待ち時間を分単位で指定します。NASが自動保護モードに入った後に電源が復旧した際には、NASはもとの操作ステータスに戻ります。
4. "Enable network UPS master" (ネットワークUPSマスター効化)オプションをクリックします。このオプションは、NASがUPSにUSBケーブルを通して接続されている場合にのみ表示されます。
5. 他のネットワークUPSスレーブの "IP address" (IPアドレス)を入力し、電源停止の際に通知が届くようにします。
6. "Apply" (適用)をクリックして確定し、下記のネットワークスレーブ·モードで操作するNASシステムのセットアップに進みます。

ネットワークスレーブ·モード

ネットワークUPSスレーブはネットワークUPSマスターとコミュニケートし、UPSステータスを受信します。UPSを備えたNASネットワークスレーブモードでセットアップするには、以下の手順に従ってください。

1. NASがネットワークUPSマスターと同一の物理ネットワークに接続されていることを確認してください。
2. "Enable UPS Support" (UPSサポート効化)オプションを選択します。
3. AC電源停止の際に、NASがシャットダウンするか自動保護モードに入るかを選択します。選択したオプションをNASが実行するまでの待ち時間を分単位で指定します。NASが自動保護モードに入った後に電源が復旧した際には、NASはもとの操作ステータスに戻ります。
4. "Protocol" (プロトコル)ドロップダウンメニューから "USB slave mode" (USBスレーブモード)を選択します。
5. ネットワークUPSマスターのIPアドレスを入力します。
6. "Apply" (適用)をクリックして確定します。

注:電力喪失の際に、ご使用のUPS機器がSNMPアラートをQNAP NASに送信するには、UPS機器の構成ページにてNASのIPアドレス入力が必要な場合があります。

NASのUPS機能の動作:

電力喪失および電力復旧の際、これらのイベントは "System Event Logs" (システムイベントログ) に記録されます。

電力喪失の間、NASは "UPS Settings" (UPS設定) にて特定された時間が経過するのを待ち、その後電源オフ、あるいは自動保護モードに入ります。
この待ち時間経過以前に電力が復旧した場合は、NASは操作状態を保持し、電源オフあるいは自動保護の動作をキャンセルします。

電源が復旧した後には:

- NASが自動保護モードに入っていた場合には、通常の操作に戻ります。
- NASが電源オフになっていた場合は、オフのままとなります。

自動保護モードと電源オフモードの違い

モード	利点	不利な点
自動保護モード	電源の回復後、NASは動作を再開する。	UPSがオフになるまで停電が続く場合、NASは異常シャットダウンを起こす。
電源オフモード	NASは、正常なシャットダウンで終了する。	電源の回復後、NASは電源がオフのままである。手動でサーバーの電源をオンにする必要がある。

NASがシャットダウンし、UPSデバイスの電源がオフになる前に電源が回復した場合、Wake on LAN*機能を使用してNASの電源をオンにすることができます (NASとUPSデバイスがWake on LAN機能をサポートし、Wake on LANがNASで効になっている場合。

*この機能は、TS-110、TS-119、TS-210、TS-219、TS-219P、TS-410、TS-419P、TS-410U、TS-419U、TS-112、TS-212、TS-412およびTS-412Uではサポートされません。詳細はhttp://www.qnap.com にアクセスしてください。

NASとUPSの両機器がシャットダウンした後に電源が回復した場合、NASは「システム管理」 > 「パワーマネジメント」で設定したとおりに動作します。

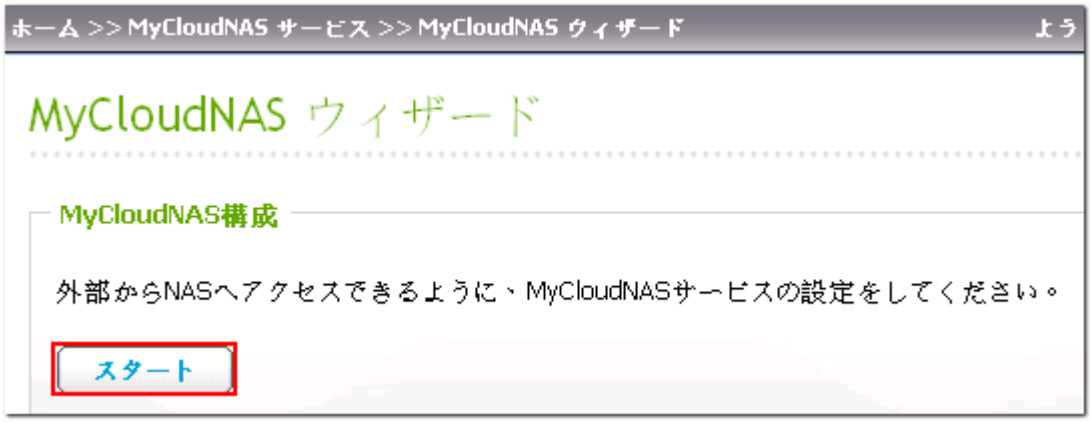
10. MyCloudNAS サービス

MyCloudNASサービスは、ホスト名登録、ホスト名への動的NAS IPの自動マッピング、ローカルネットワークでUpnPルータの自動ポートマッピングを提供する機能です。MyCloudNASウィザードを使用してNASで固有ホスト名の登録、UpnPルータの自動ポート転送の設定、インターネット上のリモートアクセスに対するNASサービスの公開を行います。

MyCloudNASサービスを使用するには、NASをUPnPルータとインターネットに接続していることを確認してください。

10.1 MyCloudNAS ウィザード

MyCloudNASサービスを初めて使用するとき、MyCloudNASウィザードを使用して設定を完了するようにお勧めします。それまで設定を行ったことがない場合、ウィザードが自動的に表示されます。「Start（スタート）」をクリックしてウィザードを使用することもできます。



以下の手順に従ってMyCloudNASサービスをセットアップします。MyCloudNASサービスを使用するには、NASをUPnPルータとインターネットに接続していることを確認してください。

1. エクスプレスセットアップ(デフォルト)または手動セットアップの使用を選択します。エクスプレスセットアップはHTTP (8080)、HTTP (80)、FTP (21)、FTPS (20)サービス用のポートを自動的に開きます。開くNASサービスのポートを選択するには、「Manual Setup（手動セットアップ）」を選択します。「Next（次へ）」をクリックします。

2. NAS用のホスト名(MyCloudNAS名)を入力し、ドメイン名を選択します。「Check(チェック)」をクリックして、ホスト名の可用性をチェックします。次に「Next(次へ)」をクリックします。

3. UPnPルータで開くポートを選択します。ルータは、NASサービスに対してポートを自動的に開いたり転送するように設定されます。「Next（次へ）」をクリックします。

ポート番号:	NASサービス
HTTP (8080)	Web管理、Webファイルマネージャ
HTTP (80)	Webサーバー、マルチメディアステーション、QMobile
FTP, FTPS (21, 20)	FTP, FTPS
SSL (443)	安全なWeb管理
Telnet (13131)	テルネットサーバー
SSH (22)	SSHサーバー、SFTPサーバー
SSL (8081)	安全なWebサーバー
再同期 (873)	リモートレプリケーション

4. 公開サービス。

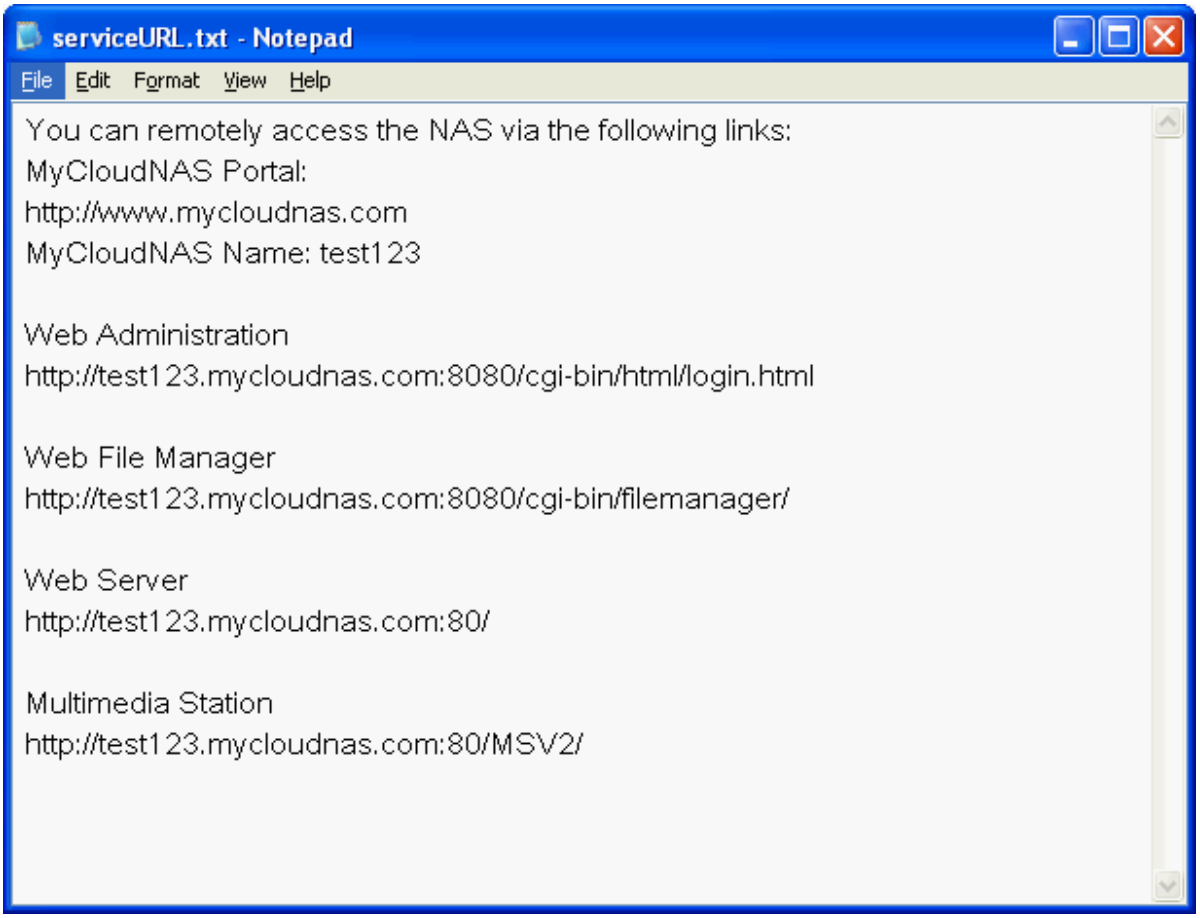
前の手順で開いたポートを使用するNASサービスが表示されます。現在無効になっているサービスを有効にし、Web管理、Webサーバー、マルチメディアサーバー、Webファイルマネージャなどの Webベースの NASサービスを http://www.mycloudnas.com に公開することができます。「Next（次へ）」をクリックします。

この手順でNASサービスを有効にすることで、公開された場合でもリモートアクセスに対して公開されます。NASサービスを有効にし公開することで、http://www.mycloudnas.com からアクセスできます。

NAS サーバーを MyCloudNAS Access Code を所有するユーザーのみに MyCloudNAS ウェブサイト（http://www.mycloudnas.com）から閲覧できるようにプライベートに公開することができます。この機能を利用するには、「MyCloudNAS Service（MyCloudNAS サービス）」>「Configure MyCloudNAS（MyCloudNAS構成）」>「Publish Services（公開サービス）」へ進みます。

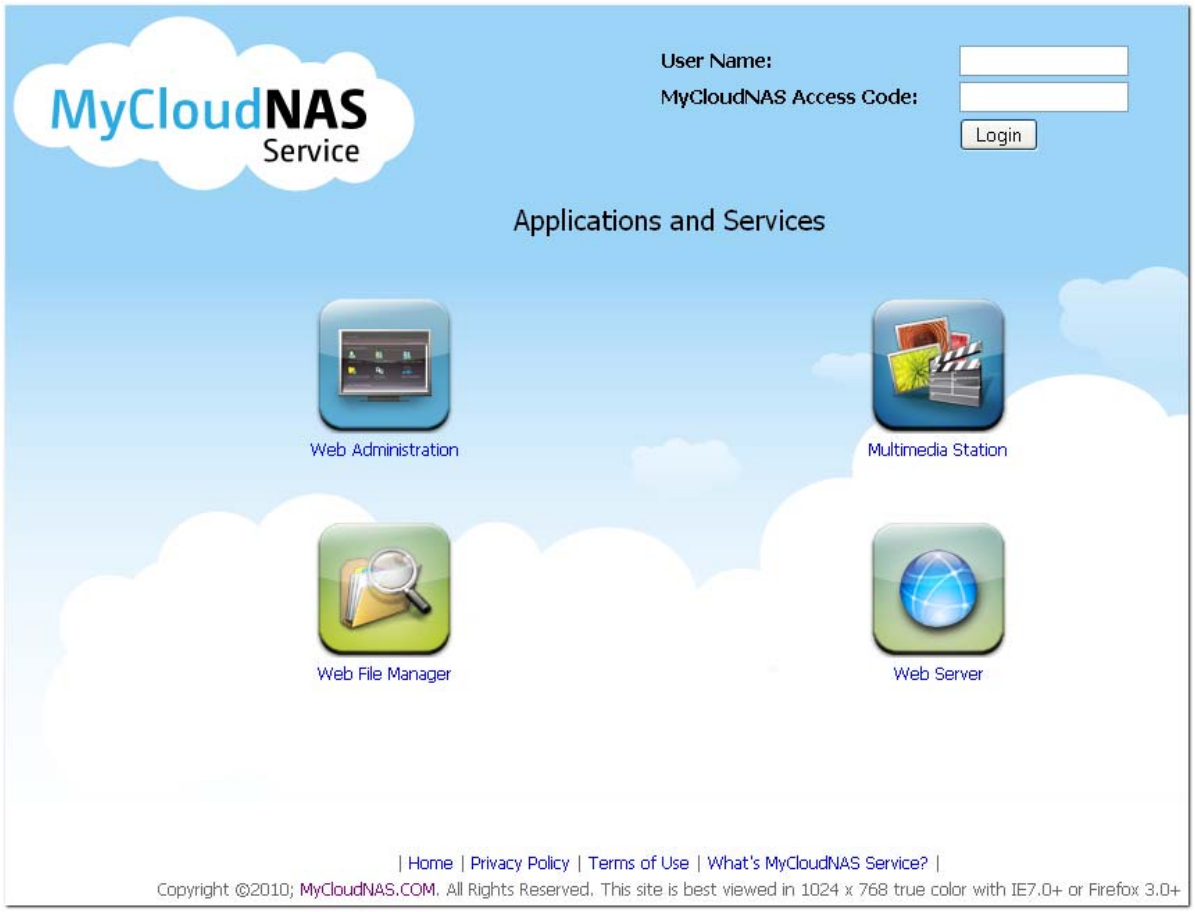
5. サマリが表示されます。MyCloudNAS 名で NAS に接続し、公開サービスの URL をダウンロードします。「Finish（完了）」をクリックして終了します。

URLをコピーし、WebブラウザによりNASサービスにアクセスします。



6. MyCloudNAS ウェブサイトを経由して NAS サービスにアクセスするには、http://www.mycloudnas.com に進み、NAS の MyCloudNAS 名を入力し、正しいドメイン名を選択します。「Go（実行）」をクリックして、公開された NAS サービスにアクセスします。

7. サービスアイコンをクリックして、ウェブベースの NAS サービスにログインします。



8. MyCloudNAS ウェブサイト上に公開されたプライベート NAS サービスを閲覧するには、ユーザー名と MyCloudNAS Access Code を入力して、「Login（ログイン）」をクリックします。

NAS サービスをプライベートに公開し、MyCloudNAS Access Code を設定するには、「MyCloudNAS Service（MyCloudNAS サービス）」>「Configure MyCloudNAS（MyCloudNAS構成）」>「Publish Services（公開サービス）」と進みます。

9. ログインに成功すると、MyCloudNAS ウェブサイト上に公開されたプライベート NAS サービスが表示されます。サービスアイコンをクリックして、ウェブベースの NAS サービスにログインします。

10.2 MyCloudNAS構成

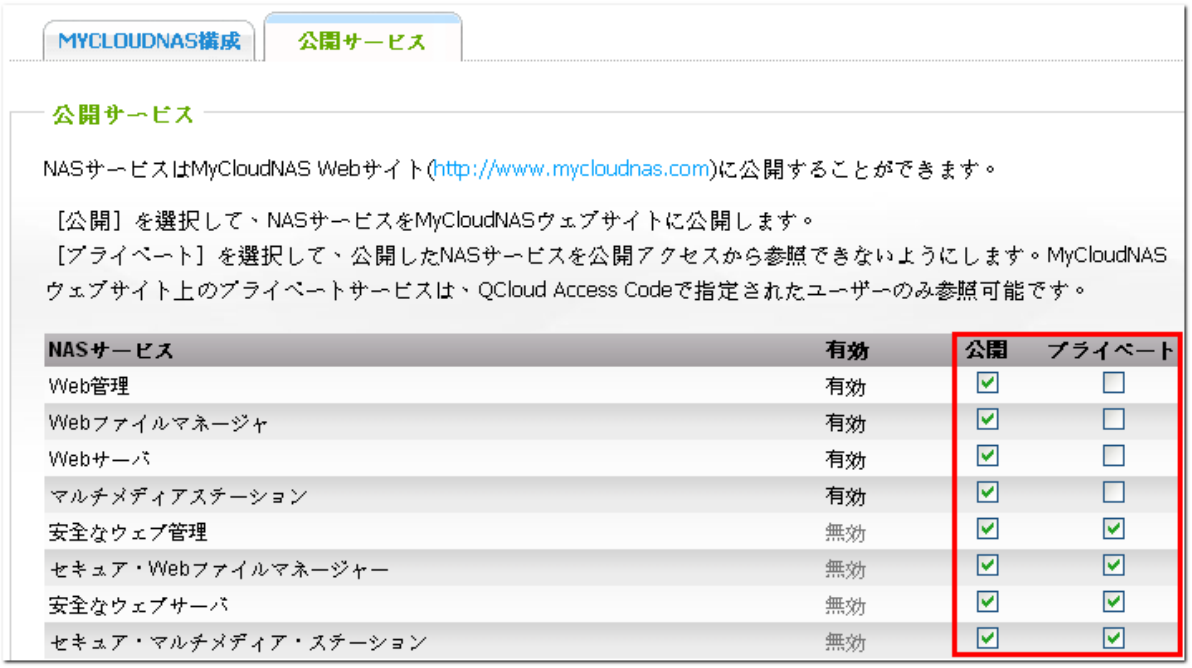
「MyCloudNASサービス」>「MyCloudNASの設定」を順に選択して、MyCloudNASサービスを有効にするように選択できます。NASのホスト名を登録したり、ホスト名をいつでも変更できます。時間間隔を指定し、NASの外部IPアドレスをチェックします。NASのWAN IPアドレスが変更されると、NASはMyCloudNASサービスを自動的に通知します。MyCloudNASサービスを使用するには、NASをUPnPルータとインターネットに接続していることを確認してください。

注:

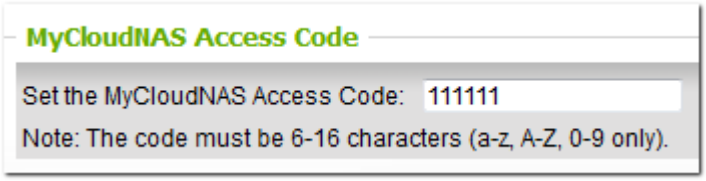
- 各QNAP NASのMyCloudNAS名は一意です。1つのNASでは、1つのMyCloudNAS名のみを使用できます。
- NASが期間内にオンラインに接続されなければ、登録されたMyCloudNAS名は120日で有効期限が切れます。名前の有効期限が切れると、他のユーザーによって新しい登録用に公開されます。

「Configure MyCloudNAS（MyCloudNAS構成）」>「Publish Services（公開サービス）」に、ウェブベースの NAS サービスが表示されます。「Publish（公開）」を選択して、NAS サービスを MyCloudNAS ウェブサイトに公開します。「Private（プライベート）」を選択して、公開した NAS サービスを公開アクセスから非表示にします。MyCloudNAS ウェブサイト上のプライベートサービスは、MyCloudNAS Access Code を所有する指定したユーザーのみが閲覧できます。

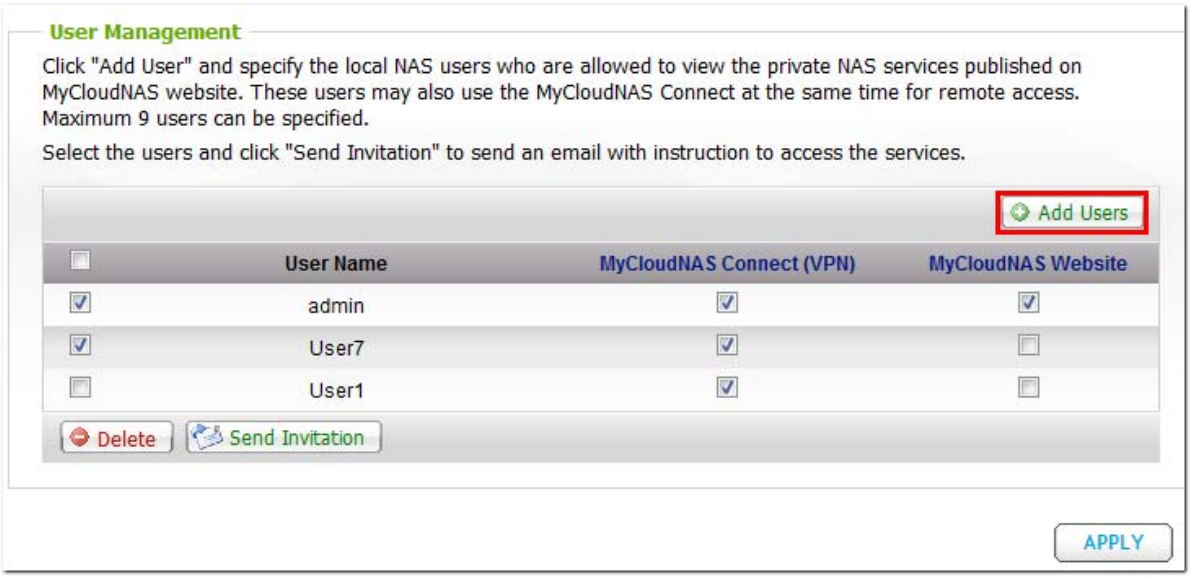
NAS サービスの公開を無効化すると、MyCloudNAS ウェブサイト（http://www.mycloudnas.com ）上に対応するアイコンが表示されていても、サービスにアクセスできなくなります。

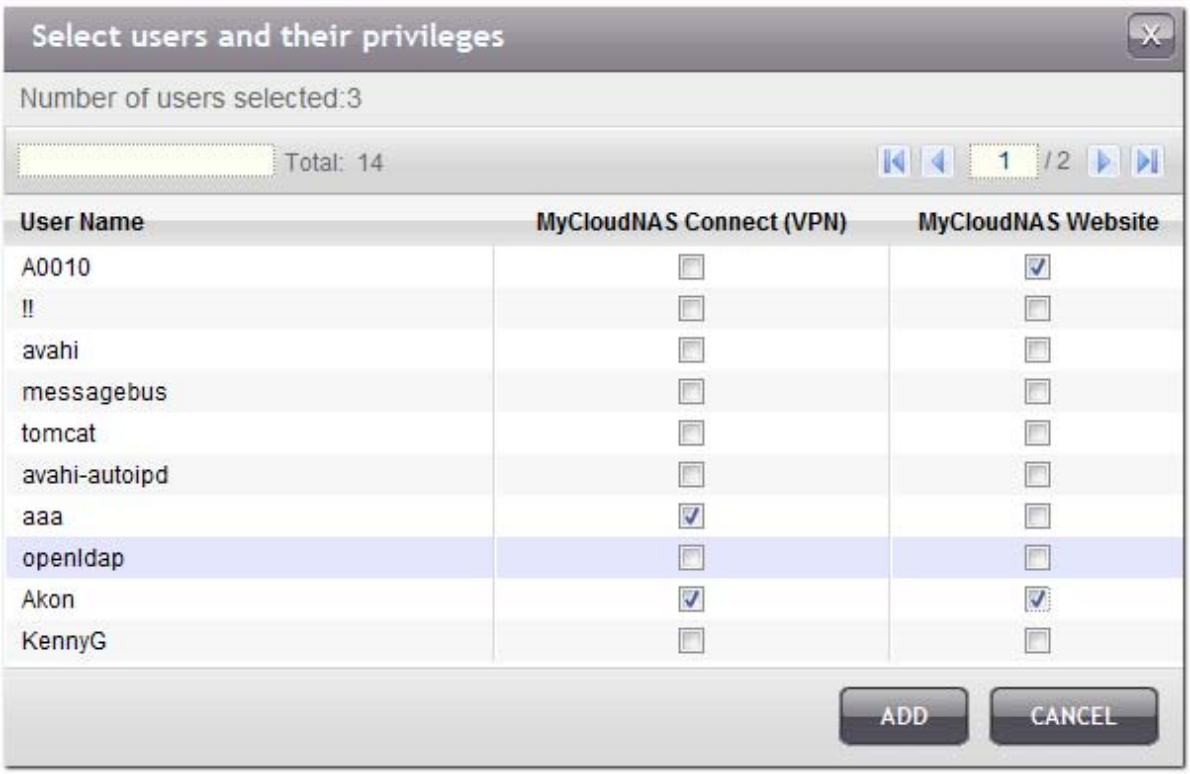


Set MyCloudNAS Access Code（MyCloudNAS Access Code の設定）: 6 ～ 16 文字のコード(a ～ z、A ～ Z、0 ～ 9 のみ)を入力します。コードは、NAS ユーザーが、MyCloudNAS ウェブサイト上のプライベート NAS サービスを閲覧しようとするときに必要になります。

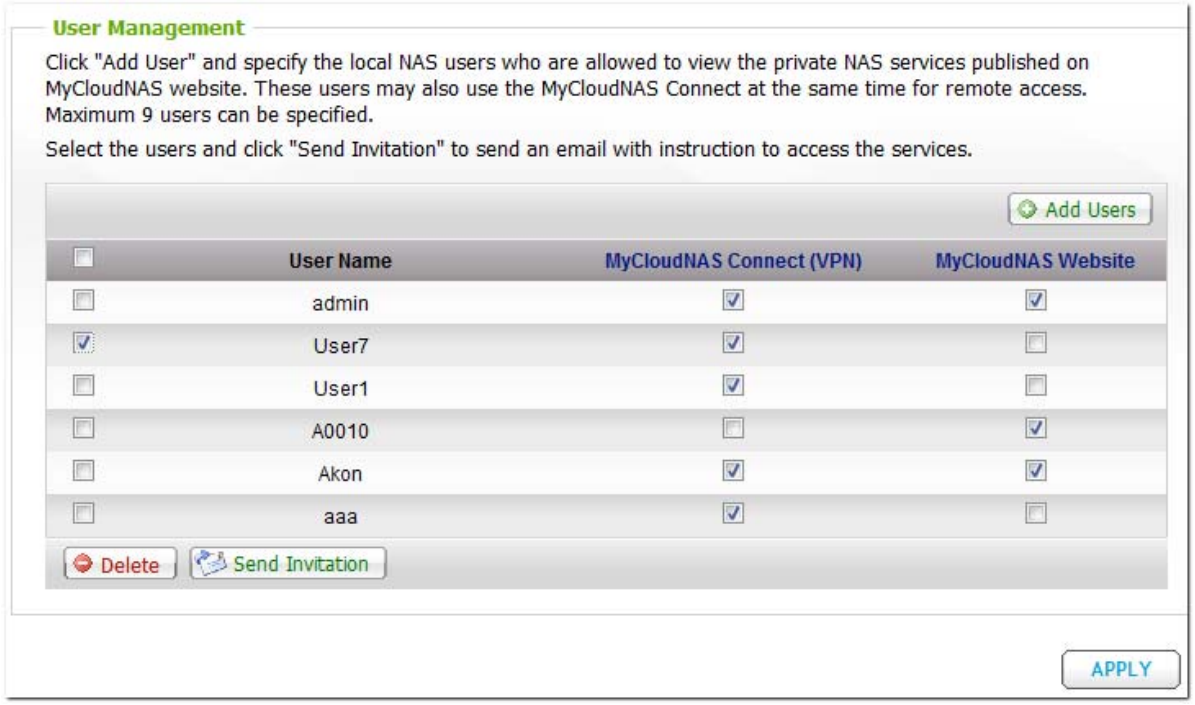


ユーザー管理: 「Manage Users（ユーザー管理）」をクリックし、MyCloudNAS ウェブサイト上に公開されたプライベート NAS サービスの閲覧を許可する最大 9 件の NAS ユーザーを指定します。「Apply（適用）」をクリックします。

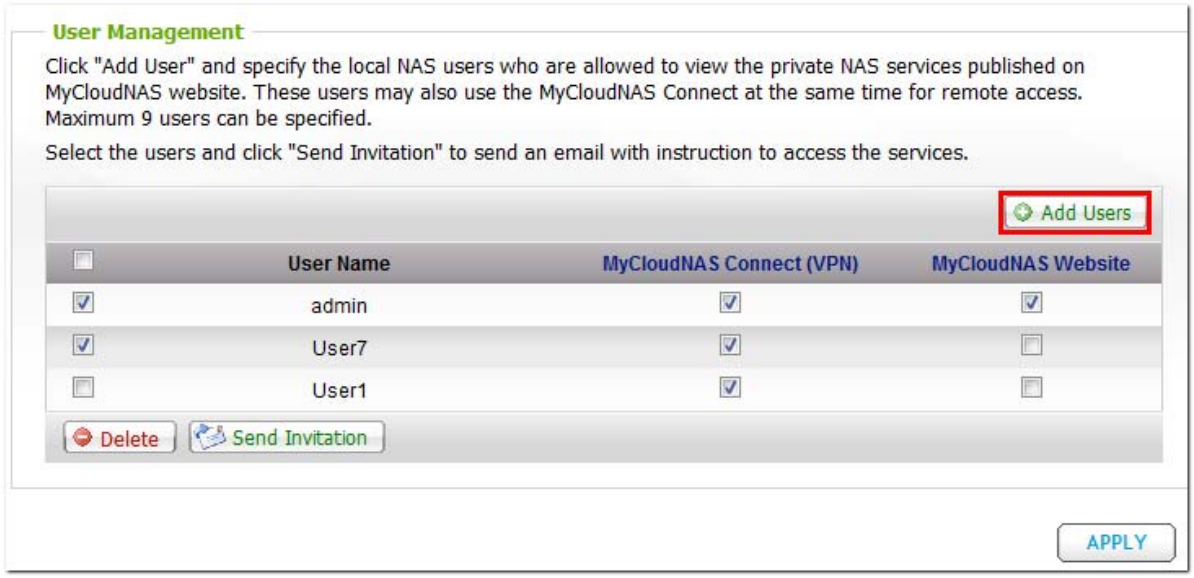




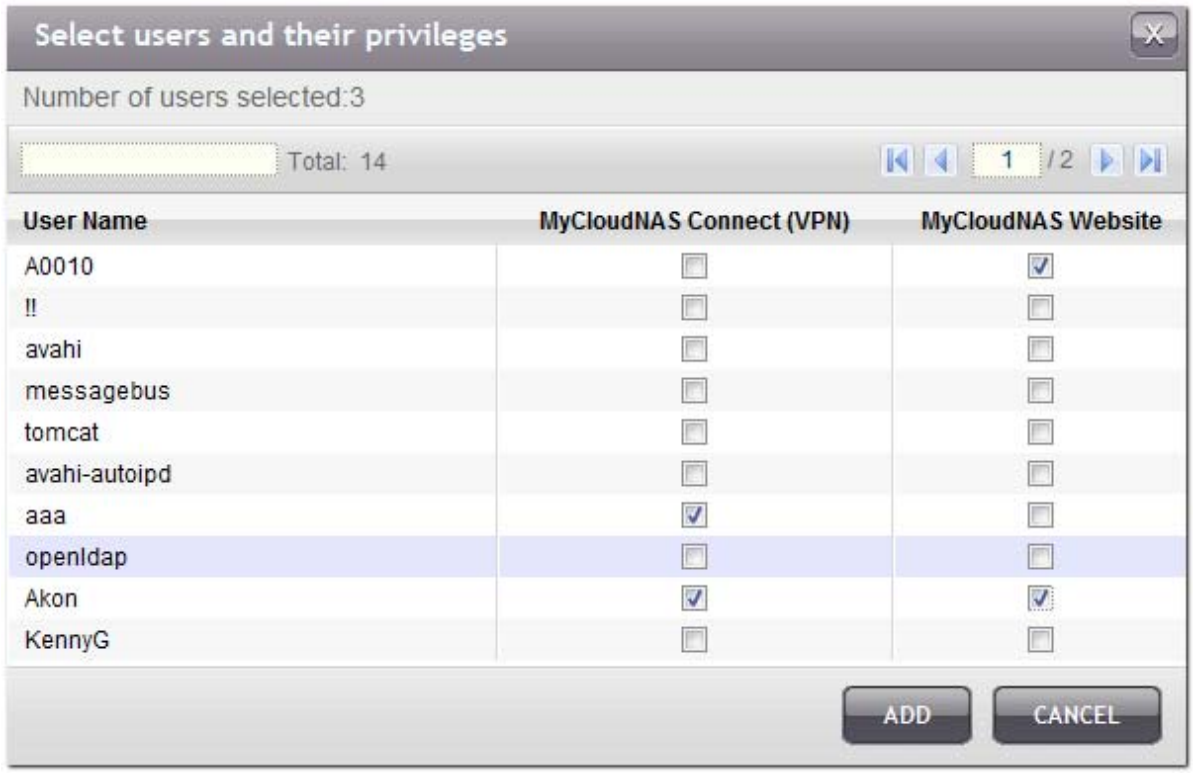
「Apply（適用）」クリックして、「Publish Services（公開サービス）」ページ上の設定を保存します。



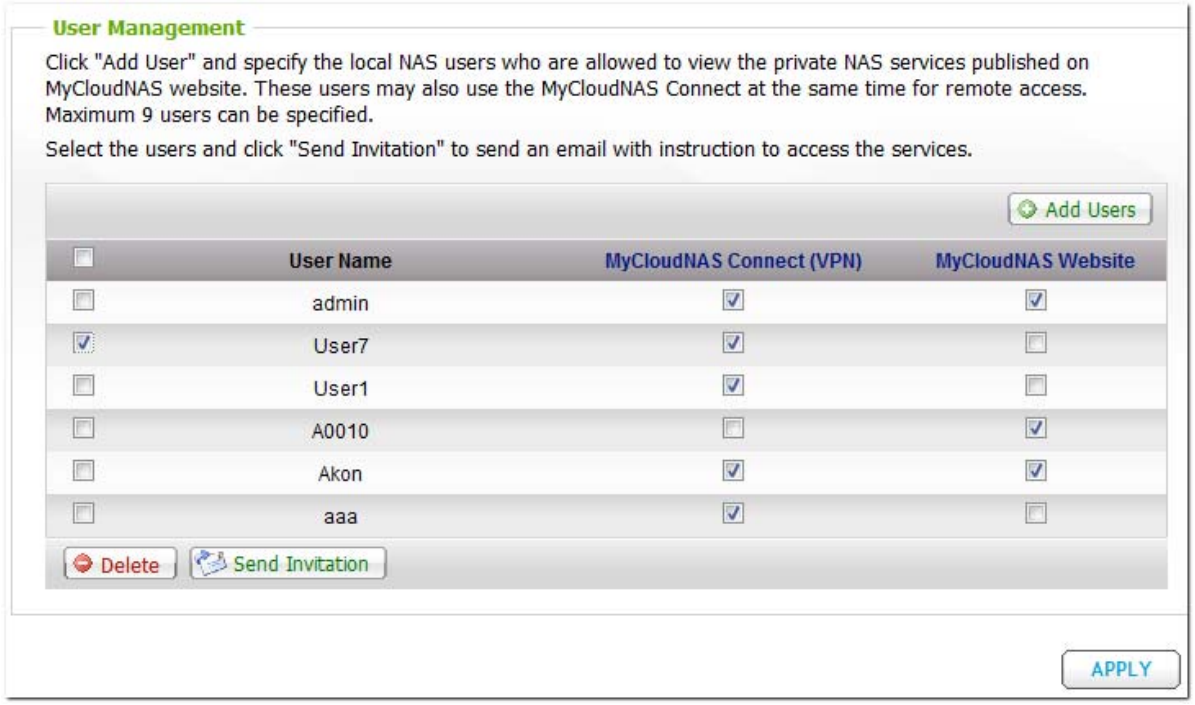
「Add Users（ユーザー追加）」をクリックし、MyCloudNAS ウェブサイトに公開されたプライベート NAS サービスの参照を許可する最大 9 件のローカル NAS ユーザーを指定します。



接続方法を選択します：MyCloudNAS 接続（VPN）ユーティリティおよび/または MyCloudNAS ウェブサイト。「Add（追加）」をクリックします。

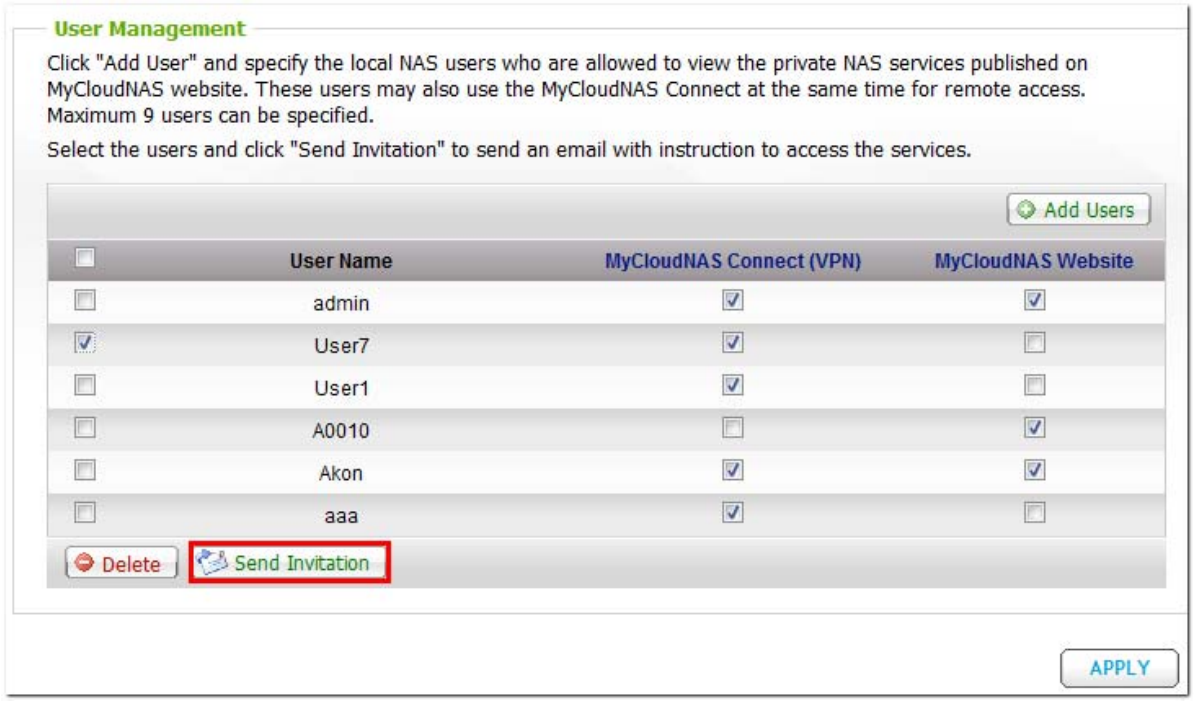


「Apply（適用）」をクリックして、設定を保存します。



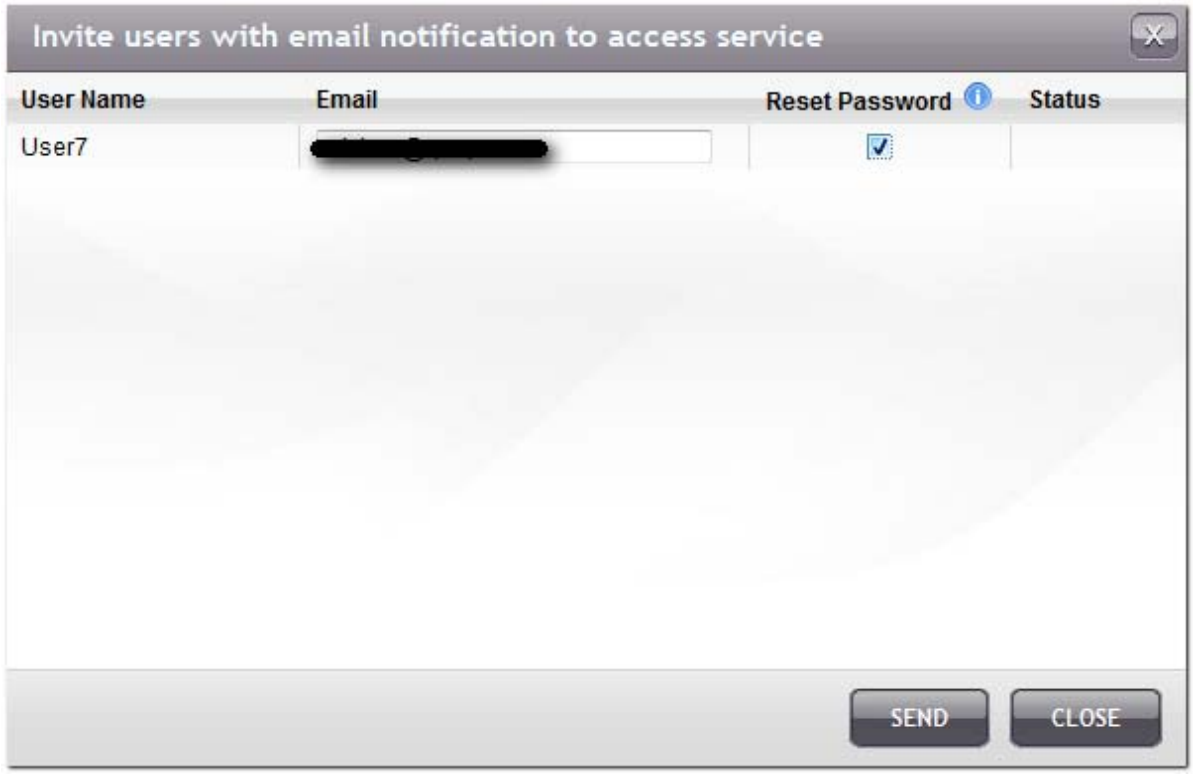
MyCloudNAS サービスの使用方法を電子メールを介してユーザーに送信するには、ユーザーを選択し、「Send Invitation（招待の送信）」をクリックします。

注：この機能を使用するには、「System Administration（システム管理）」>「Notification（通知）」>「Configure SMTP Server（SMTP サーバーの設定）」でメールサーバー設定を適切に行う必要があります。



メールアドレスを入力します。ユーザーに MyCloudNAS パスワードを再設定するリンクを伴う操作方法を送信するには、「Reset Password（パスワードの再設定）」を選択します。「Send（送信）」をクリックします。

注：パスワード再設定用のリンクは、電子メール送信後 24 時間を経過するか、ユーザーがパスワードを再設定した後、無効になります。

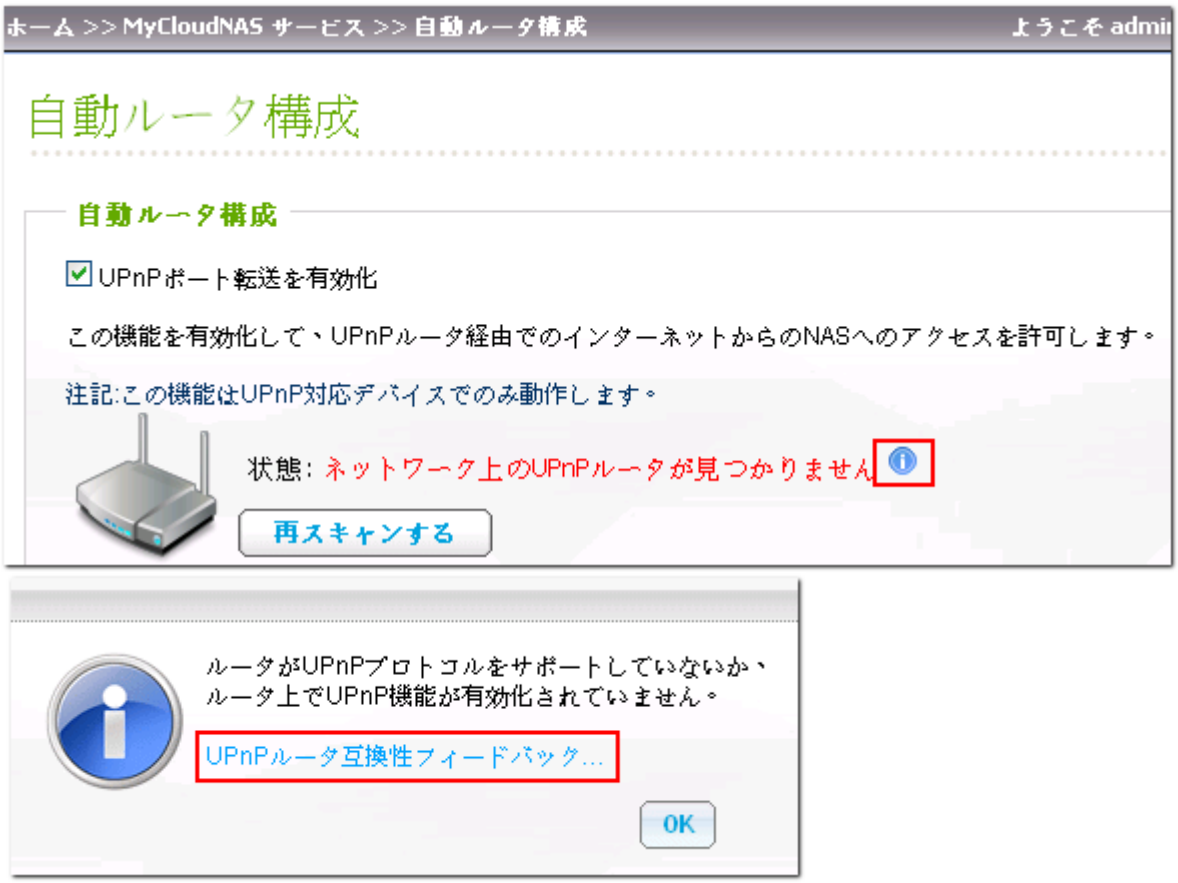


10.3 自動ルータ構成

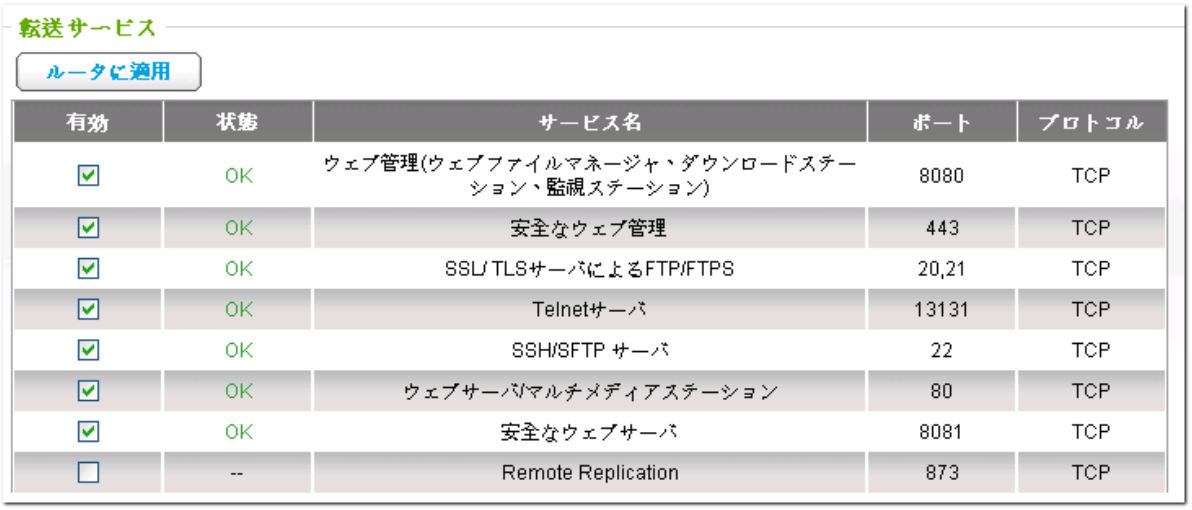
「MyCloudNASサービス」>「自動ルータ設定」を順に選択すると、UPnPポート転送の有効/無効を切り替えることができます。このオプションが有効になると、NASにUpnPルータ経由でインターネットからアクセスできます。UPnPルータがローカルネットワークに見つからない場合、「Rescan(再スキャン)」をクリックしてルータを検出します。ルータ情報を表示するには、「view details(詳細を見る)」をクリックします。

注: ネットワークに複数のルータがある場合、NASのデフォルトゲートウェイとして設定されるルータのみが検出されます。

UPnPルータにNASと互換性がない場合、 アイコンをクリックし、「UPnPルータ互換性フィードバック…」(http://www.qnap.com/onlinesupport.aspx)をクリックして技術サポートに連絡してください。



リモートアクセスを許可されたNASサービスを選択します。「Apply to router（ルータに適用）」をクリックします。UpnPルータでポート転送が自動的に設定されます。これらのNASサービスには、インターネットからアクセスが可能です。



注: ルータがUPnP機能に対応していない場合、ルータでポート転送を手動設定する必要があります。以下のリンクを参照してください。

- アプリケーションメモ: http://www.qnap.com/pro_application.asp?ap_id=111
- FAQ: http://www.qnap.com/faq.asp
- UPnPルータ互換性リスト: http://www.qnap.com/pro_compatibility.asp

11. システムステータス

システム情報 635
システムサービス 636
リソースモニタ 637

11.1 システム情報

CPU使用率およびメモリなどのシステム情報は、このページに表示できます。

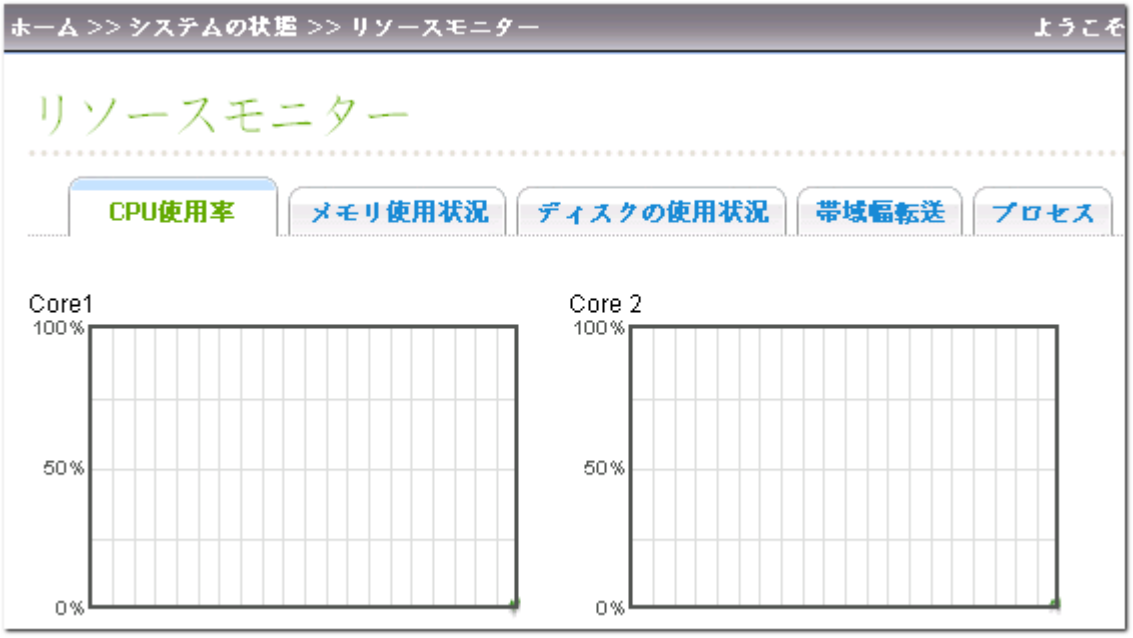
11.2 システムサービス

このセクションで、NASの現在のネットワーク設定とステータスを表示できます。

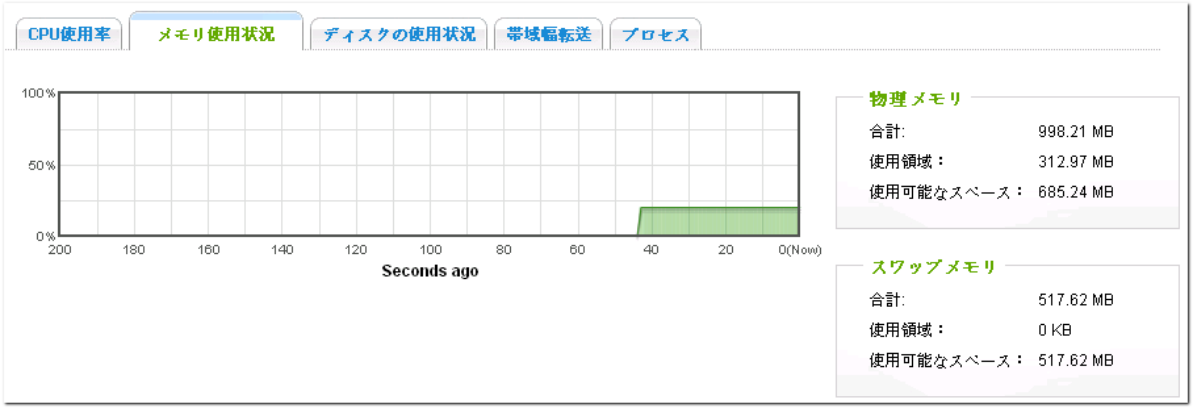
11.3 リソースモニタ

CPU使用率、ディスク使用率、NASの帯域幅伝送統計をこのページで表示することができます。

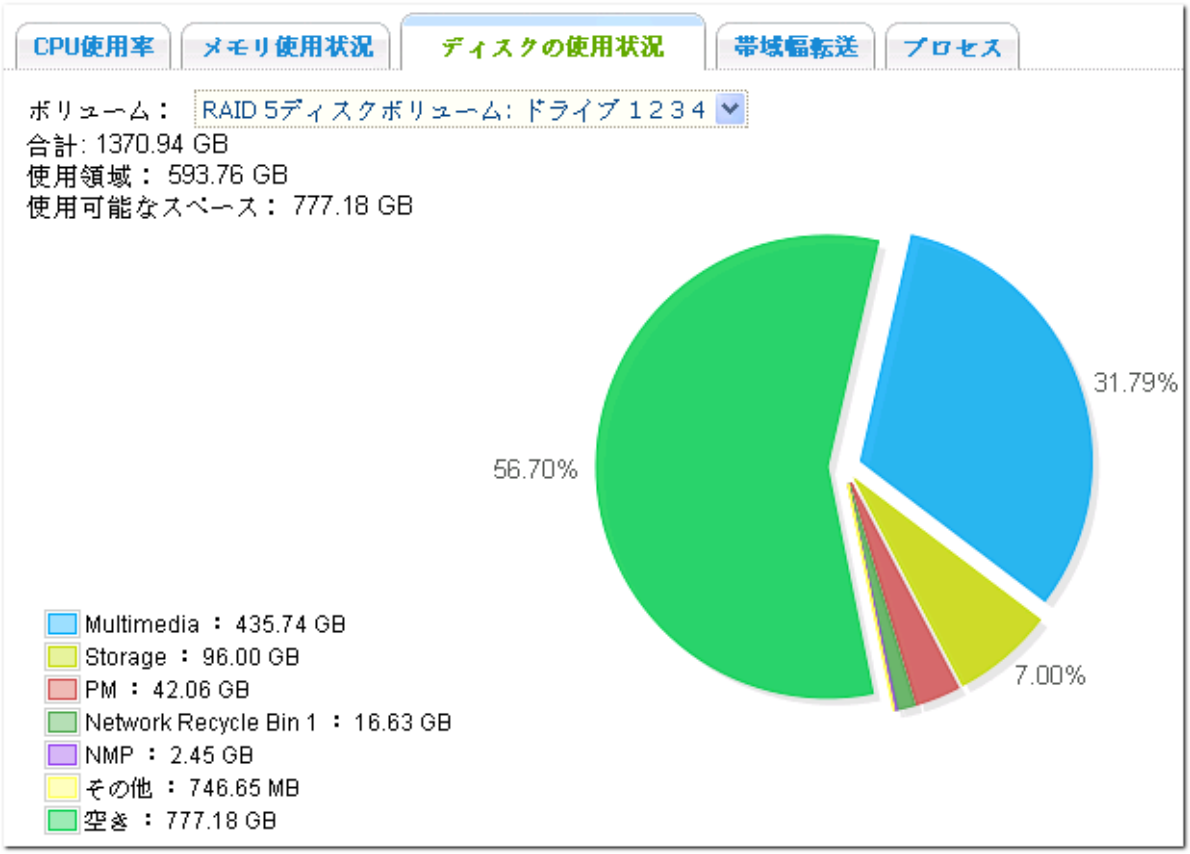
CPU 使用状況:このタブではNASのCPU使用状況を表示します。



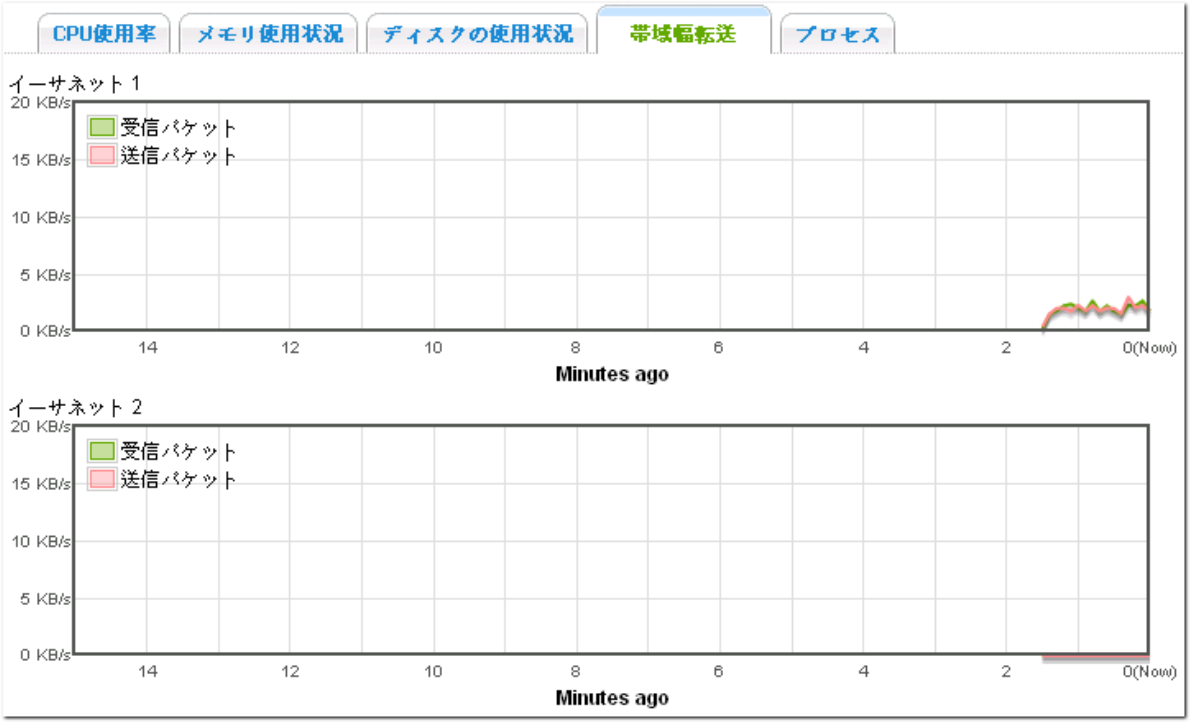
メモリ使用状況:このタブではNASのメモリ使用状況をリアルタイムの動的グラフで表示します。



ディスク使用状況:このタブは、各ディスクボリュームおよびその共フォルダのディスク容量の使用状況を示します。



帯域幅伝送:このタブは、NASの各LANポートにおける帯域幅伝送についての情報を示します。



プロセス:このタブではNASで実行中のプロセスの情報を表示します。

プロセス名	ユーザ	PID	CPU使用率	物理メモリ
top	admin	1118	2.9%	872 K
top	admin	1121	1.9%	872 K
hd_util	admin	4782	0.9%	1220 K
init	admin	1	0	624 K
manaRequest.cgi	admin	1116	0	1288 K
thttpd	admin	1117	0	540 K
manaRequest.cgi	admin	1119	0	1288 K
thttpd	admin	1120	0	540 K
daemon_mgr	admin	1535	0	536 K
qWatcodogd: keeping alive ever	admin	1610	0	476 K
modagent	admin	1854	0	420 K
hotswap	admin	2249	0	1036 K
qsmartd	admin	2257	0	820 K
dhcpcd	admin	2540	0	256 K
mDNSResponderPosix	admin	2607	0	708 K

12. LCDパネルの使用

この機能はLCDパネルの付いたNASモデルにのみ付属しています。詳細については、http://www.qnap.com にアクセスしてください。

NASでは、便利なLCDパネルにより、ディスクを構成を実行したり、システム情報を表示することができます。

NASを開始すると、サーバー名とIPアドレスを表示することができます。

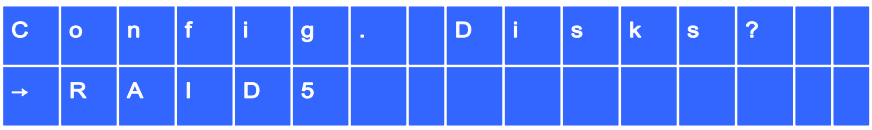
N	A	S	5	F	4	D	E	3					
1	6	9	.	2	5	4	.	1	0	0	.	1	0	0

初めてインストールする場合、LCDパネルには検出されたハードドライブの数とIPアドレスが表示されます。ハードドライブを構成するよう選択することもできます。

検出されたハードドライブ数	デフォルトのディスク構成	利用可能なディスク構成オプション*
1	シングル	シングル
2	RAID 1	シングル -> JBOD -> RAID 0 -> RAID 1
3	RAID 5	シングル -> JBOD -> RAID 0 -> RAID 5
4以上	RAID 5	シングル -> JBOD -> RAID 0 -> RAID 5 -> RAID 6

*「Select」ボタンを押しオプションを選択、「Enter」ボタンを押し承認します。

例えば、インストールされた5つのハードドライブのあるNASのスイッチをオンにした場合、LCDパネルには以下のように表示されます：



「Select」ボタンを押し、RAID6などの詳細オプションを表示します。「Enter」ボタンを押すと次のメッセージが表示されます。「Select」ボタンを押し、「Yes」を選択します。再度「Enter」ボタンを押し、承認します。

RAID 1、RAID 5、RAID 6構成を実行する際、システムはハードドライブを初期化し、またRAIDデバイスを作成及びフォーマットし、NASにボリュームとしてマウントします。進行はLCDパネルに表示されます。100％に達すると、RAIDボリュームにアクセスすることができます。例えば、共フォルダの作成、NAS上のファイルにファイルをアップロード、といったことが可能になります。その間、すべてのRAIDコンポーネントデバイスのストライプ及びブロックの準備が完了していることを確認するため、NASはRAID同期を実行します。その進行は"Disk Management" (ディスク管理) > "Volume Management" (ボリューム管理) のページで表示することができます。同期率は約30-60MB/秒です。(ハードドライブモデル、システムリソース使用率などにより異なる)

注：RAID構成のメンバードライブが同期中に失われた場合、RAIDデバイスは低下モードに入ります。その際もボリュームデータへのアクセスは可能です。デバイスに新規メンバーを追加すると、再構築が開始されます。"Volume Management" (ボリューム管理) ページにてステータスを確認することができます。

ディスクボリュームを暗号化するには*、LCD パネルに<Encrypt Volume?>が表示されたら"Yes"を選択します。デフォルトの暗号化パスワードは"admin"です。パスワードを更するには、管理者としてWebベースの管理インターフェイスにログインし、「デバイス設定」 > 「ディスクボリューム暗号化の管理」で設定を更します。

E	n	c	r	y	p	t		V	o	l	u	m	e	?	
→	Y	e	s			N	o								

構成が終了すると、サーバー名、IPアドレスが表示されます。NASがディスク容量の作成に失敗した場合、次のメッセージが表示されます。

C	r	e	a	t	i	n	g	.	.	.					
R	A	I	D	5		F	a	i	l	e	d				

この機能は、TS-110、TS-119、TS-210、TS-219、TS-219P、TS-410、TS-419P、TS-410U、TS-419U、TS-119P+、TS-219P+、TS-419P+、TS-112、TS-212、TS-412、TS-419U+、およびTS-412Uではサポートされません。

データ暗号化機能は、一部の国では法規制に従って利用できないことがあります。

LCDパネルによるシステム情報の表示

LCDパネルがサーバー名、IPアドレスを表示した場合、「Enter」ボタンを押し、Main Menuを入力します。Main Menuでは以下で構成されます。

1. TCP/IP
2. Physical disk
3. Volume
4. System
5. Shut down
6. Reboot
7. Password
8. Back

TCP/ IP

TCP/ IP では、以下のオプションを表示することができます。

1. LAN IP Address
2. LAN Subnet Mask
3. LAN Gateway
4. LAN PRI. DNS
5. LAN SEC. DNS
6. Enter Network Settings
    - Network Settings – DHCP
    - Network Settings – Static IP*
    - Network Settings – BACK
7. Back to Main Menu

*Network Settings – Static IPでは、IPアドレス、サブネットマスク、ゲートウェイ、LAN 1 と LAN 2のDNSを構成することができます。

Physical disk

Physical diskでは、以下のオプションを表示することができます。

- Disk Info
- Back to Main Menu

ディスク情報では、ハードドライブの温度、容量が表示されます。

D	i	s	k	:	1		T	e	m	p	:	5	0	°	C
S	i	z	e	:		2	3	2		G	B				

Volume

このセクションでは、NASのディスク情報が表示されます。1行目には、RAID構成、ストレージ容量、2行目には構成のメンバードライブ数が表示されます。

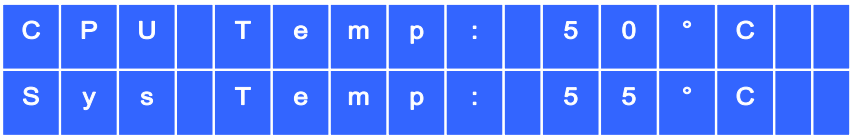
R	A	I	D	5							7	5	0	G	B
D	r	i	v	e		1	2	3	4						

1つ以上のボリュームがある場合、「Select」ボタンを押し情報を表示します。以下の表に、RAID5構成用のLCDメッセージの表示を示します。

LCDディスプレイ	ドライブ構成
RAID5+S	RAID5+スペア
RAID5 (D)	RAID 5低下モード
RAID 5 (B)	RAID 5 再構築
RAID 5 (S)	RAID 5 再同期化
RAID 5 (U)	RAIDのマウントが解除されました。
RAID 5 (X)	RAID 5 が非アクティブです。

System

このセクションでは、システムのオ温度、システムファンの回転速度を表示します。



Shut down

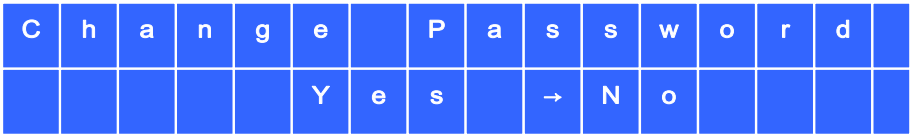
このオプションを使用し、NASのスイッチをオフにします。「Select」ボタンを押し、「Yes」を選択します。次に、「Enter」ボタンを押し、承認します。

Reboot

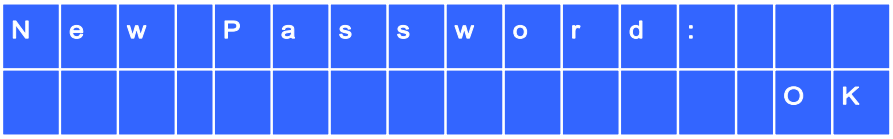
このオプションを使用し、NASを再起動します。「Select」ボタンを押し、「Yes」を選択します。次に、「Enter」ボタンを押し、承認します。

Password

LCDパネルのデフォルトのパスワードはblankです。このオプションを入力し、パスワードを更します。「Yes」を選択し、続行します。



最大8文字までの数字（０～９でパスワードを入力することができます。カーソルを「OK」まで移動し、「Enter」ボタンを押します。パスワードを確認し、更します。

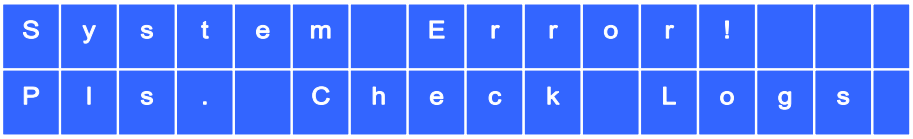


Back

このオプションを選択し、メインメニューに戻ります。

システムメッセージ

NASがシステムエラーになった場合、エラーメッセージがLCDパネルに表示されます。「Enter」を押し、メッセージを表示します。「Enter」ボタンを押し、再度次のメッセージを表示します。

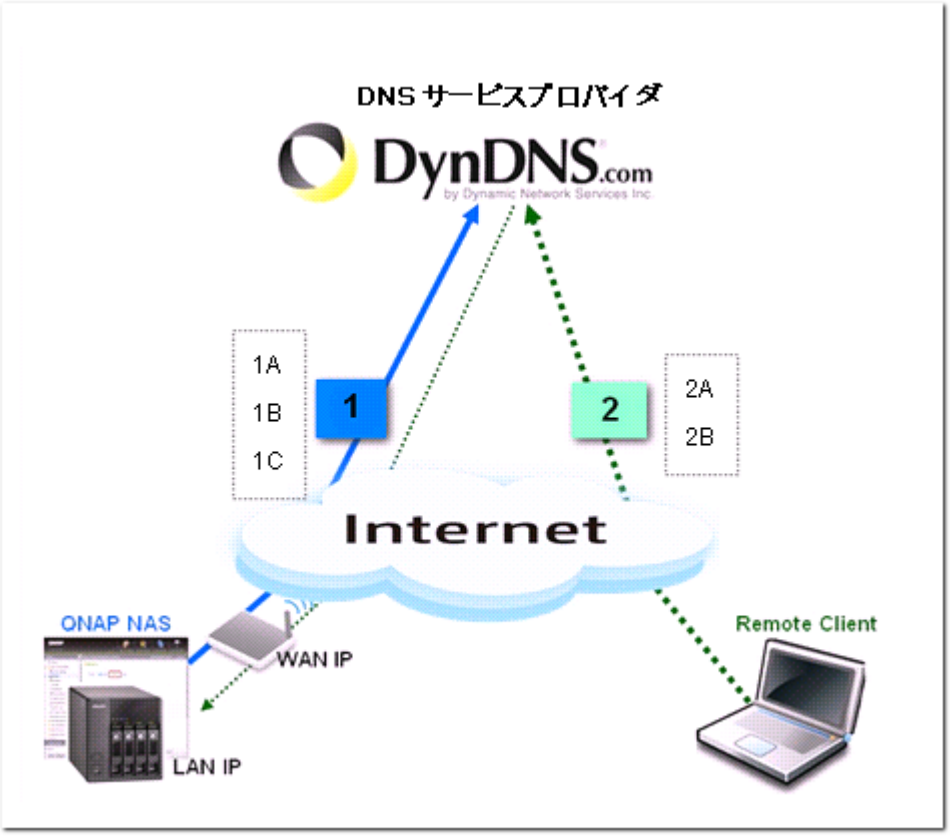


システムメッセージ	表記
Sys. Fan Failed	システムファンのエラー
Sys. Overheat	システムのオーバーヒート
HDD Overheat	ハードドライブのオーバーヒート
CPU Overheat	CPUのオーバーヒート
Network Lost	LAN 1 と LAN 2が、フェールオーバー、または負荷バランシングモードで接続が切断されました。
LAN1 Lost	LAN 1の接続が切断されました。
LAN2 Lost	LAN 2の接続が切断されました。
HDD Failure	ハードドライブエラー
Vol1 Full	容量がいっぱいです。
HDD Ejected	ハードドライブが取り出されました。
Vol1 Degraded	容量が低下モードです。
Vol1 Unmounted	容量のマウントが解除されました。
Vol1 Nonactivate	容量が非アクティブです。

13．インターネットからQNAP NASをアクセスする(DDNSサービス)

リモートでインターネットにアクセスするために、QNAP NASに対してDDNSサービスをセットアップする

DDNS (ダイナミックドメイン名サービス) は、ドメイン名をネットワークデバイスのダイナミックIPアドレスにマップするために使用されるサービスです。 QNAP NASはDDNSをサポートして、長ったらしいIPアドレスの代わりに覚えやすいドメイン名(URL)でインターネットのサーバーにすばやくアクセスできるようにしています。 IPが変更されると、NASはいつでもリモートでアクセスできるように、DDNSプロバイダへの情報を自動的に更新します。



1A: DDNSプロバイダからドメイン名、例えばqnap.dyndns-office.comを登録します。
1B: DDNSサービスを有効にし、NASでDDNSアカウント情報を入力します。
1C: QNAP NASでは、DDNSプロバイダへのWAN IP情報を自動的に更新します。

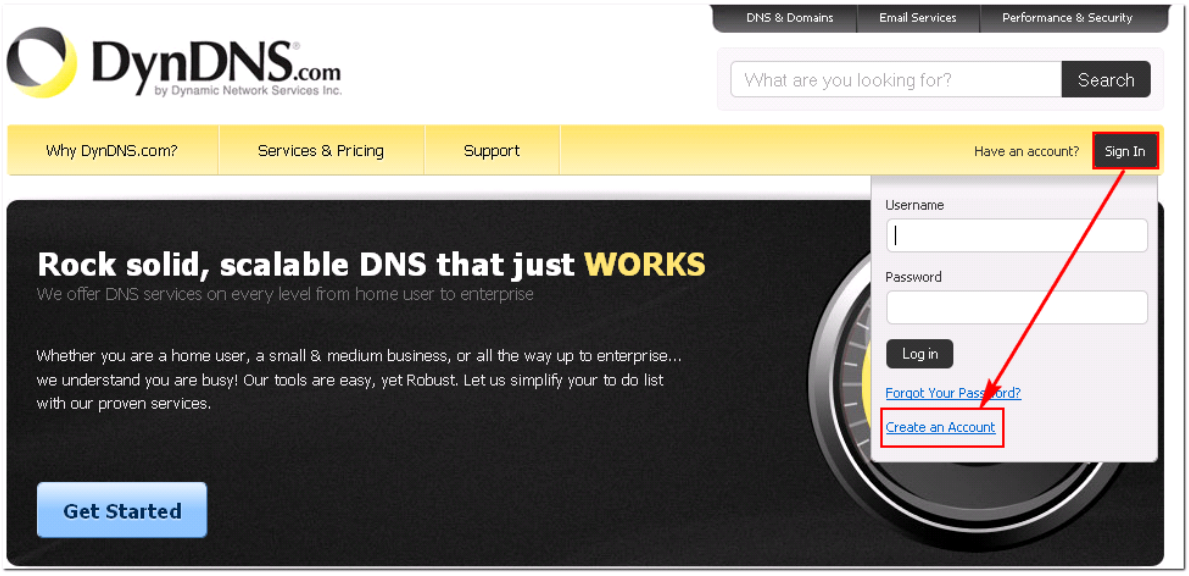
2A: 任意のPCから登録したドメイン名: http://qnap.dyndns-office.com:8080により、NASにリモートで接続します。
2B: IPが変更されると、DDNSはQNAP NASにより更新されたWAN IPをドメイン名にマップします。

DDNSサービスの登録

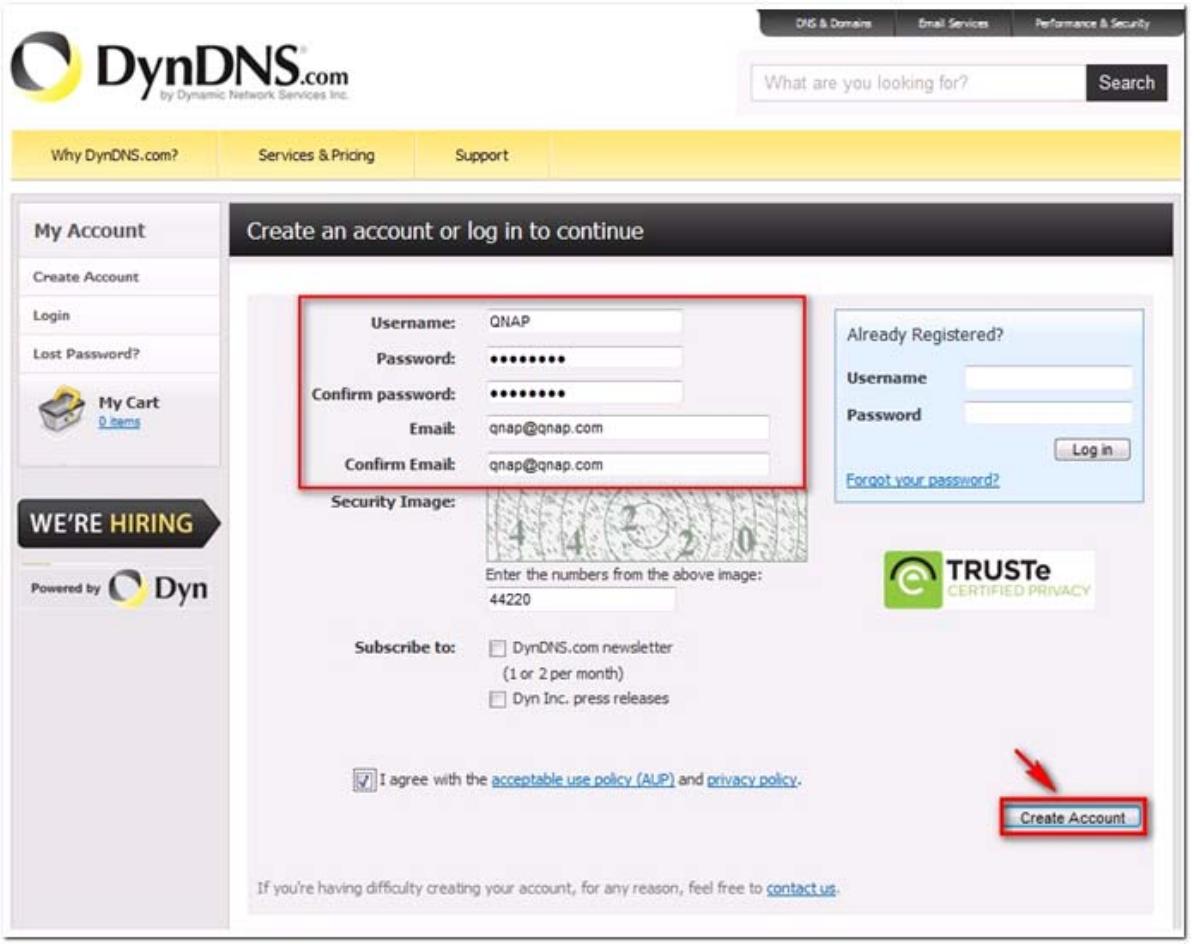
NASがダイナミックIPアドレスを使用するようにセットアップされている場合、DNSサービスプロバイダからDDNS（ダイナミックDNS）アカウントを登録し一意のホスト名を割り当てて、インターネット上でNASに容易にアクセスすることができます。DDNSアカウントを登録するには、以下のステップを参照してください。

1. DNSサービスプロバイダを選択します。QNAP NASは現在、次のDDNSサービスプロバイダをサポートしています。
   http://www.dyndns.com
   http://update.ods.org
   http://www.dhs.org
   http://www.dyns.cx
   http://www.3322.org
   http://www.no-ip.com

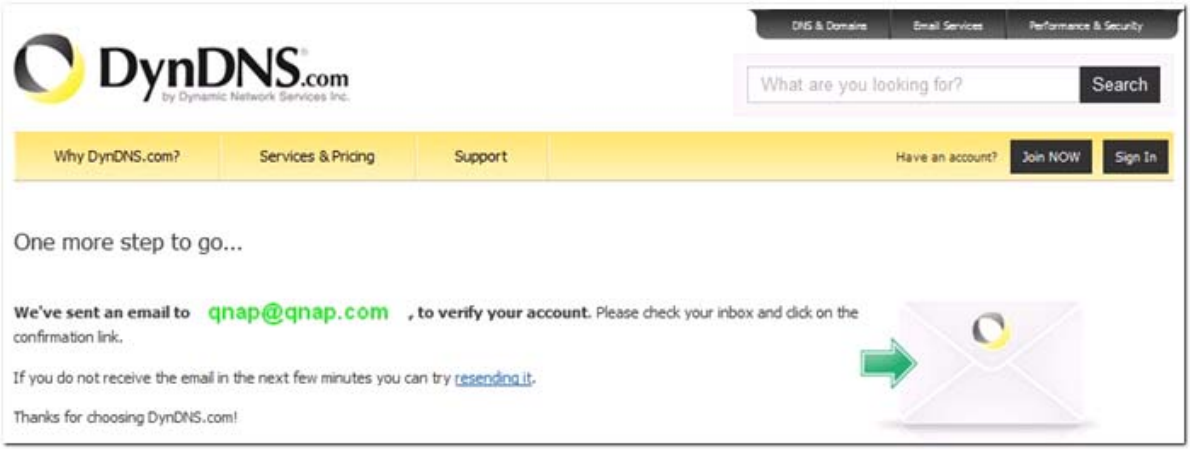
2. アカウントを作成します。ここでは、http://www.dyndns.org を例に取ります。http://www.dyndns.org にアクセスします。「Sign In 」と「Create an Account」をクリックしてDynDNSアカウントを登録します。



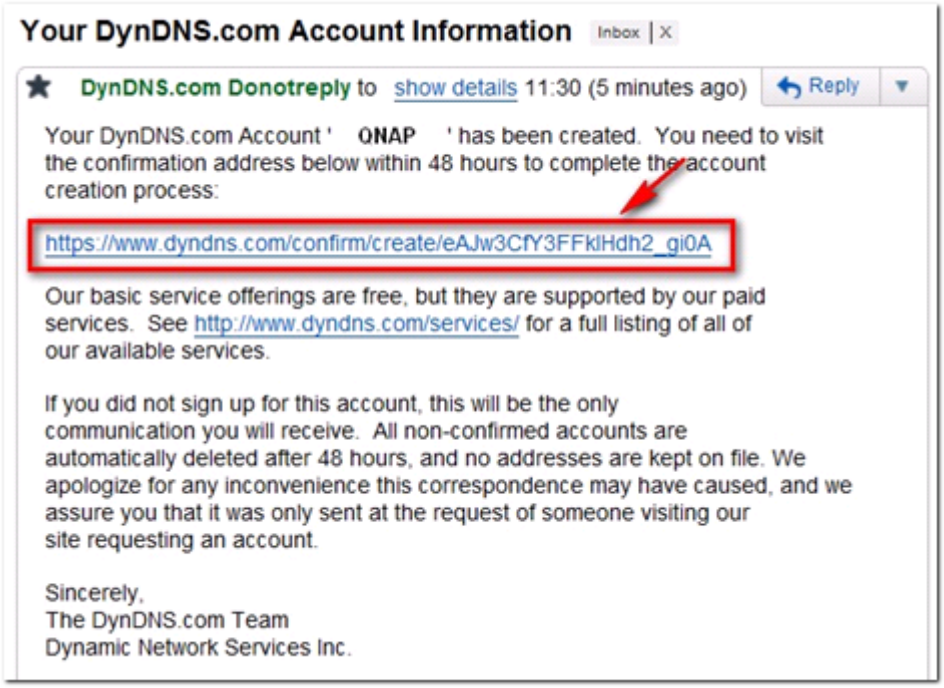
3. 書式に必要事項を記入して無料アカウントを作成します。



4. 確認電子メールがお客様の電子メールアドレスに送信されます。

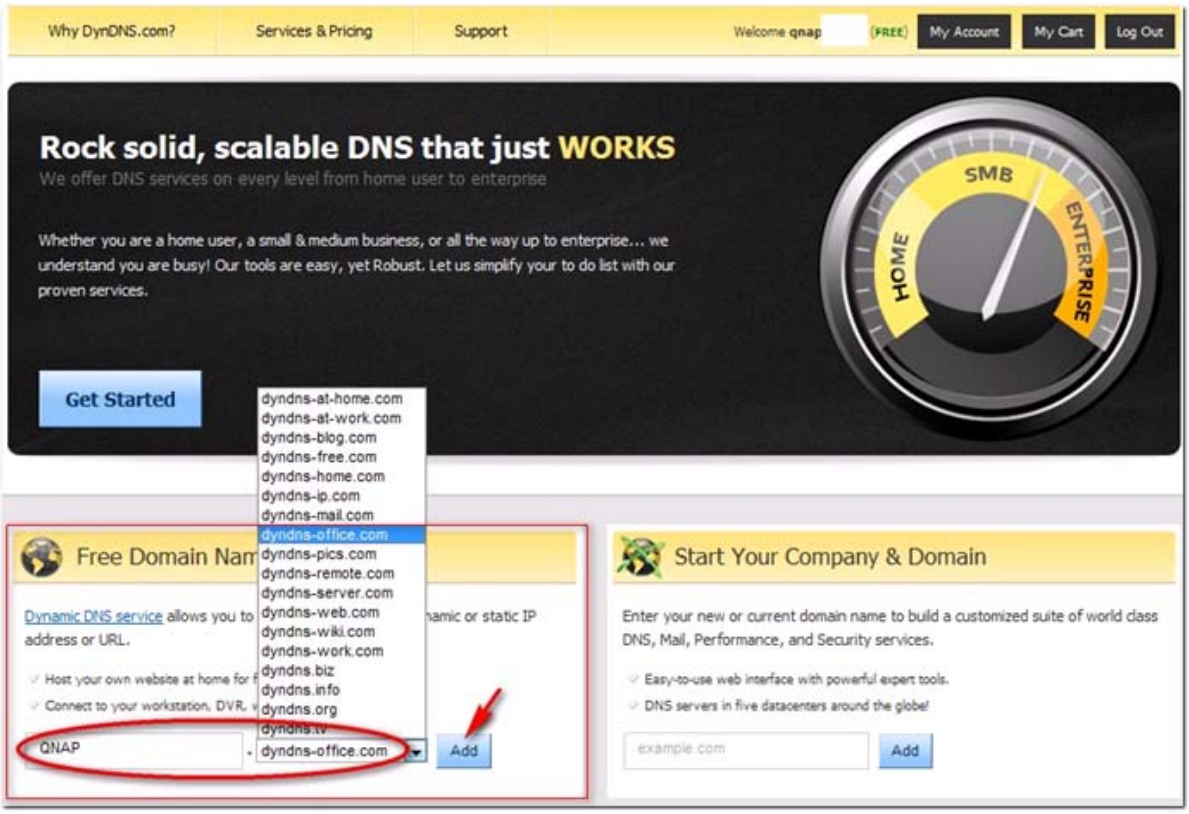


5. 電子メールのリンクをクリックして確認します。



6. 「Confirm Account（アカウントの確認）」をクリックしてDynDNSにログインします。

7. NASのホスト名を登録します。ホスト名は、ご利用のサーバーを特定する一意の名前です。覚えやすい名前を選んでください。例えば、「QNAP」と記入し「dyndns-office.com」を選択します。「Add」をクリックします。

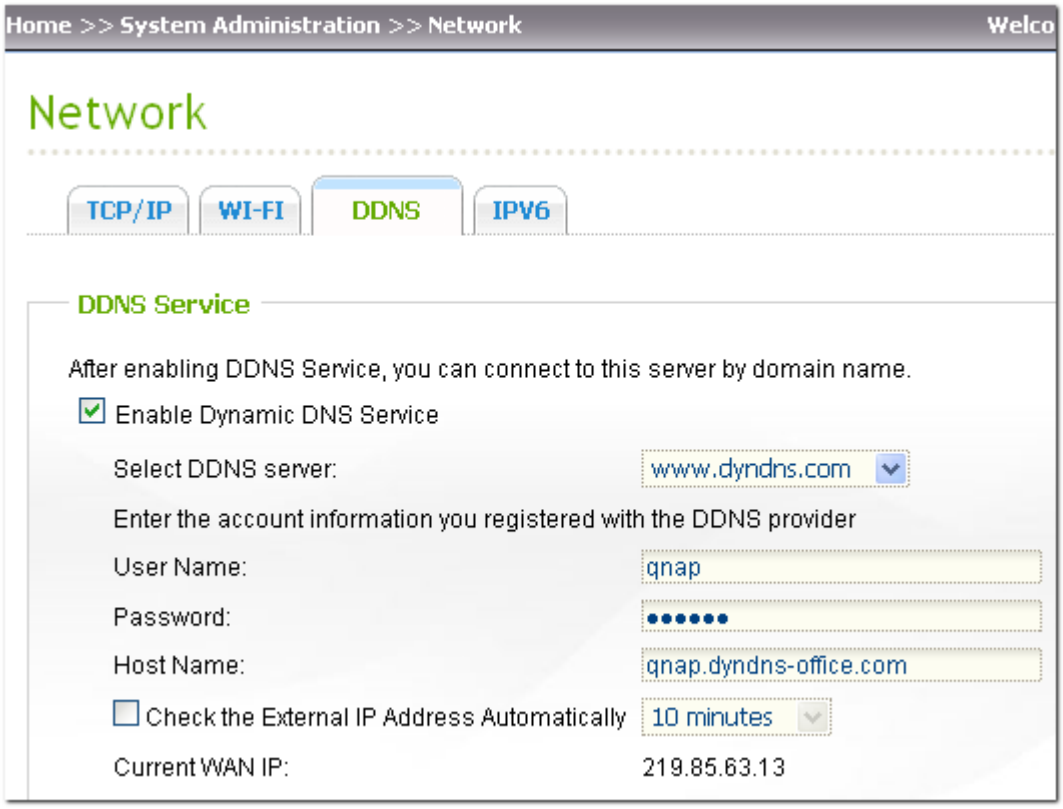


8. ホスト名を有効にします。

NASにログインし、DDNSサービスをセットアップできるようになりました。

QNAP NASでDDNSサービスを設定する

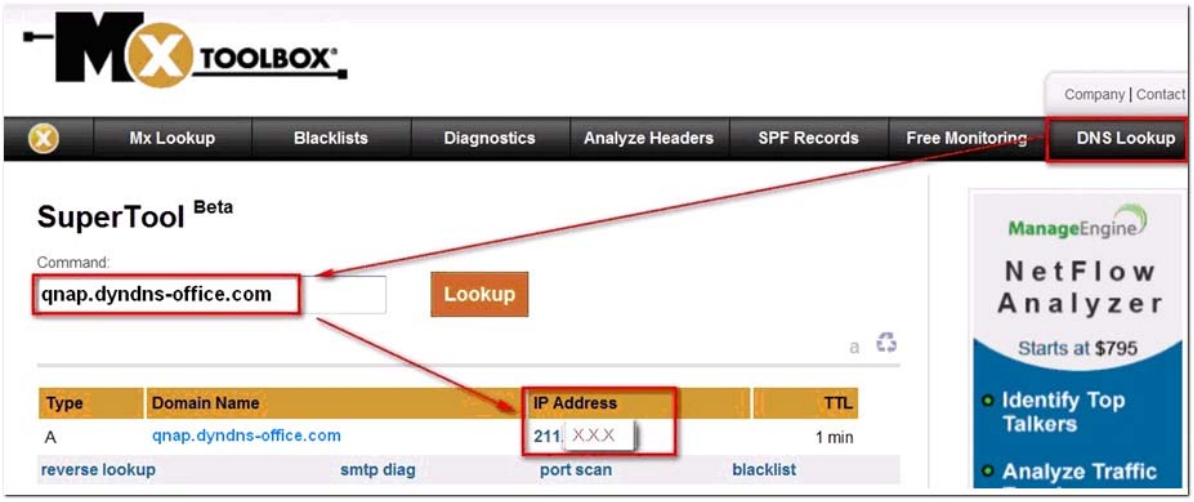
NASにログインし、「System Administration(システム管理)」 > 「Network(ネットワーク)」 > 「DDNS」の順にポイントします。DNSサービスプロバイダから登録したDDNS情報を入力します。「Check the External IP Address Automatically(外部IPアドレスを自動的に確認する)」オプションを設定することで、DDNS記録を周期的に更新するようにNASをスケジュールに入れることができます。



設定を終了すると、NASはDDNSプロバイダに対してWAN IPの更新を開始しドメイン名をマッピングします。インターネットで上で、ドメイン名(qnap.dyndns-office.com)によりNASに接続できるようになります。

確認が必要な場合、DNSを検索する:

NASのドメイン名がそのWAN IPに正しくマップされていることを確認するには、http://www.mxtoolbox.com/DNSLookup.aspx にアクセスする必要があります。DNS検索のドメイン名を入力すると、IPアドレスが戻されます。



ポートの転送

ご使用のNASがNATルーターの背後に配置されている場合、NATルーター上のいくつかのサービスのポートを開け、NASの固定LAN IPにこれらのポートを転送する必要があります。この機能は市場のほとんどのルーターに搭載されており、"Port Forwarding" (ポート転送)、"NAT Server" (NAT サーバ)あるいは"Virtual Server" (仮想サーバ) といった名称で知られています。 例えば、NASシリーズの管理インターフェースに接続するには、ポート8080を開ける必要があります。

QNAP NASの現在開いているサービスポート	
NASサービス	**デフォルトのポート**
Webベースシステム管理	8080 (全てのモデル、TS-101/201ファームウェアバージョン 2.3.0以降)
Webベースシステム管理	6000 (TS-100/101/201ファームウェアバージョン 2.3.0以前)
FTP	21
パッシブFTP	55536–56559
Webサーバー	80
ダウンロードステーション (BTダウンロード)	6881–6999
リモートレプリケーション (Rsync)	873
Telnet	13131
SSH	22
SSL	443
SMTP	25
Samba	445
MySQL	3306
TwonkyMedia	9000

14. QNAP NASでSMS、電子メール、IM Alertをセットアップします

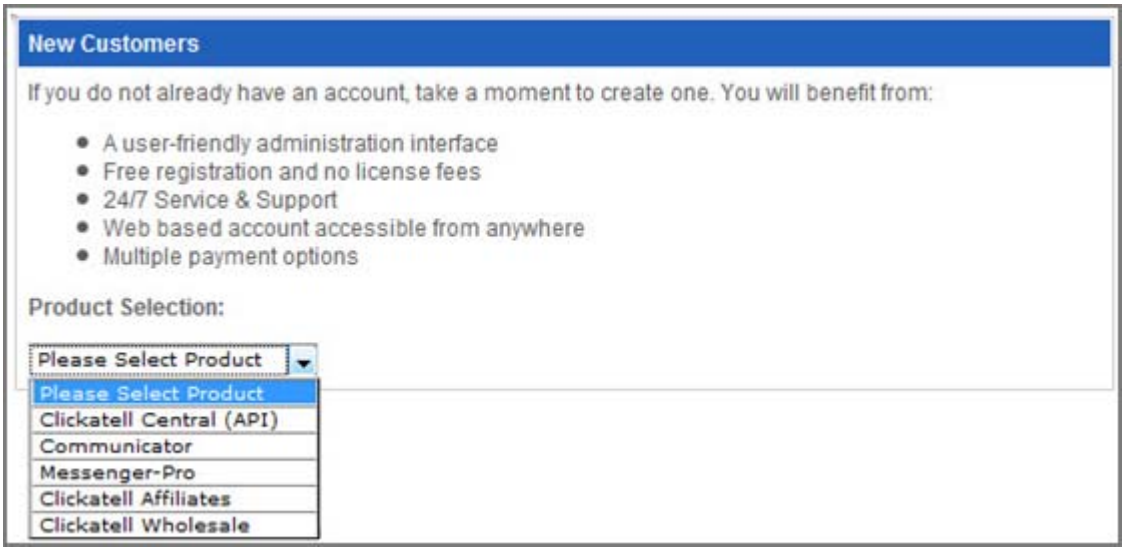
QNAP NASはSMS（ショートメッセージサービス）、電子メール、インスタントメッセージング(IM) Alertをサポートして、ユーザーにシステムエラーまたは警告を通知します。

注: TS-109/ 209/ 409/ 409U シリーズはメールアラートのみサポートしています。

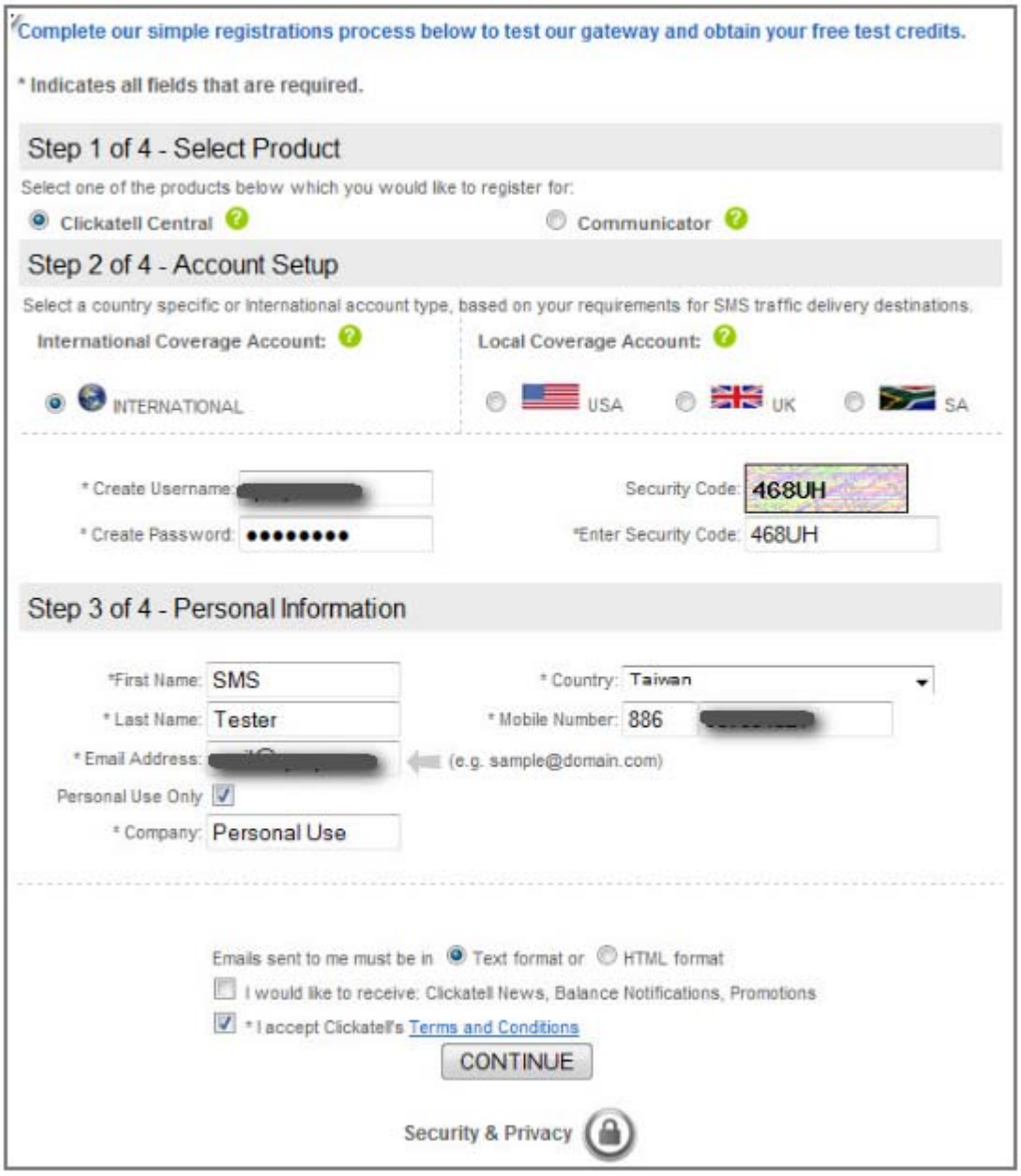
SMS Alertのセットアップ

1. **SMSサービスアカウントに加入し、セットアップする**

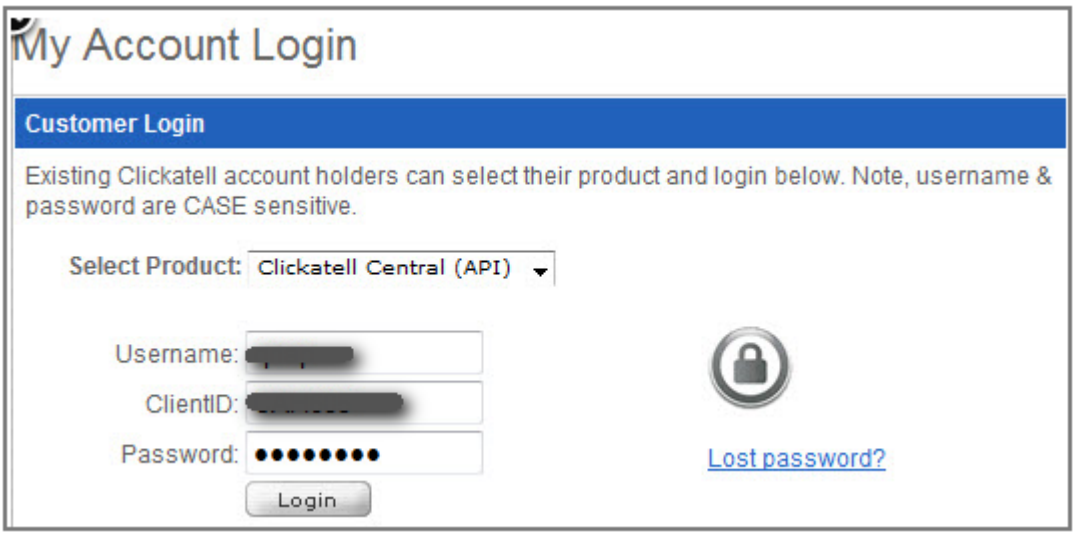
ここではClickatellを例に使
用します。 ClickatellのWebサイトhttp://www.clickatell.com/login.php にアクセスします。"New Customers"（新規顧客)から"Clickatell Central (API)"を選択します。



個人情報を入力し、 "Continue" (続行)をクリックします。 利用規定をよく読み、内容が適当と判断されれば同意します。

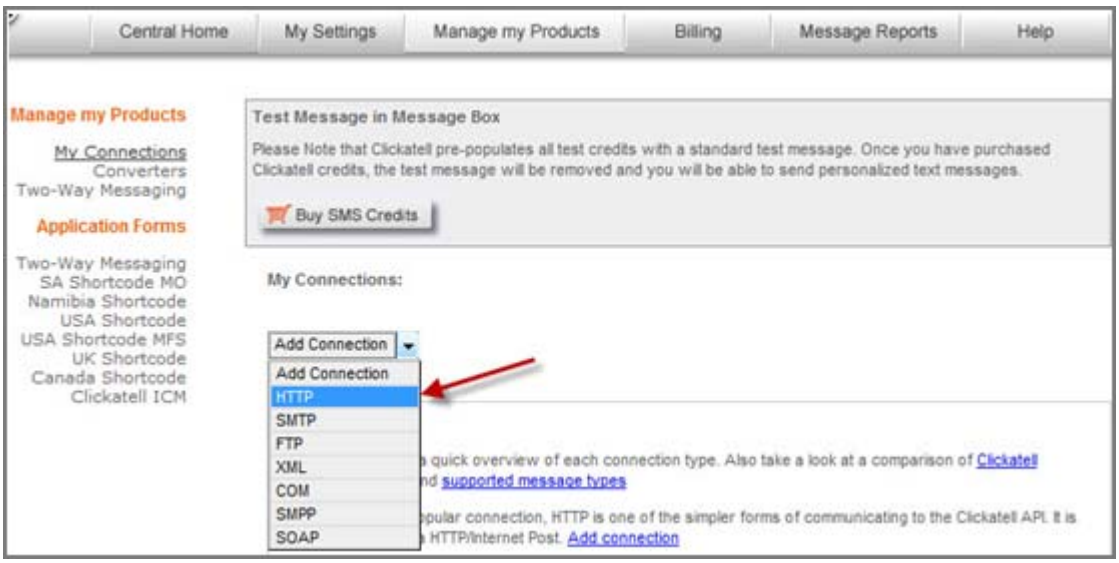


登録が完了すると、アカウント効化のためのリンクを含んだメールを受信できます。 アカウントの効化を完了するため、メールの受信箱を確認してください。 効化のリンクから、下図のようなログイン画面に進みます。 パスワードを入力し、"Login" (ログイン)をクリックして進みます。



ご使用の携帯電話番号を入力し、"SEND ACTIVATION CODE" (アクティベーションコードを送信する) をクリックします。その後、Clickatellから送信されたアクティベーションコードを入力し、ご使用の携帯電話番号を確認します。

Clickatellにログインしたまま、"Manage my Products"（製品の管理）に移動、"My Connections"（接続）のドロップダウンリストから"HTTP"を選択します。



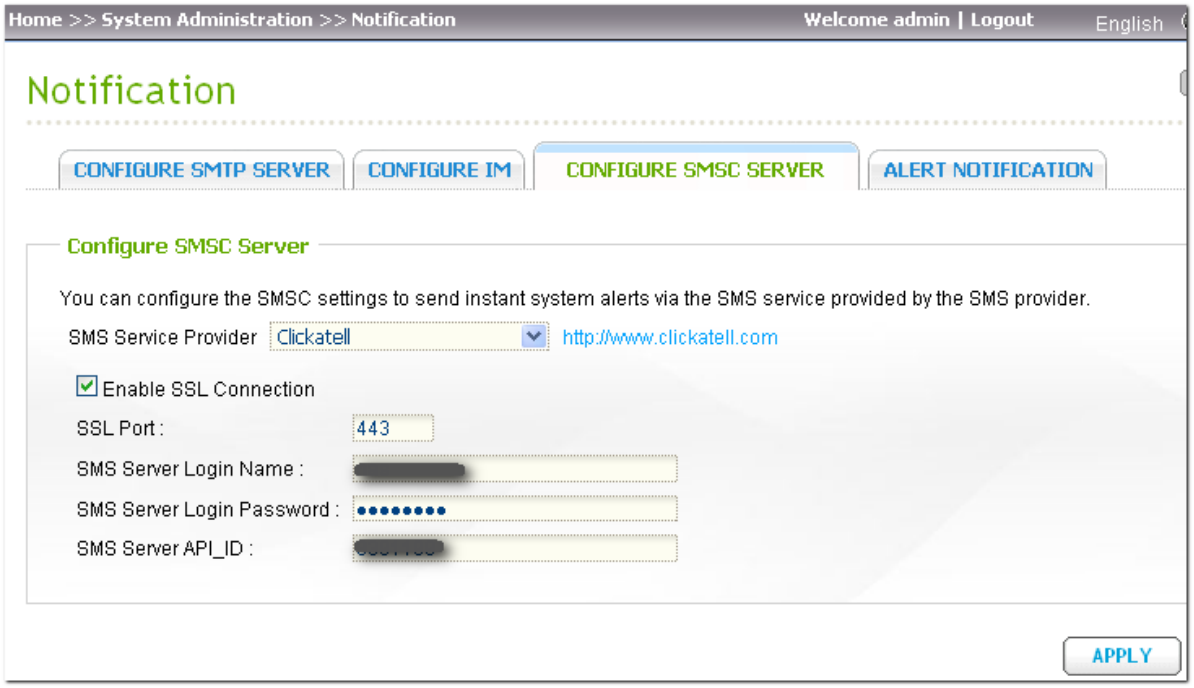
以下の図に示されるように、最小限必要な "Name"（名前）、 "Dial Prefix"（ダイヤルのプレフィックス）および "Callback Type"（コールバックのタイプ）xの情報を入力して "HTTP API"をセットアップします。"Submit"（送信）をクリックすると完了です。

SMSサービスの使用前に必要となる"API ID"が表示されます。次のステップでNAS管理でのセットアップに使用できるよう、書き取っておいてください。

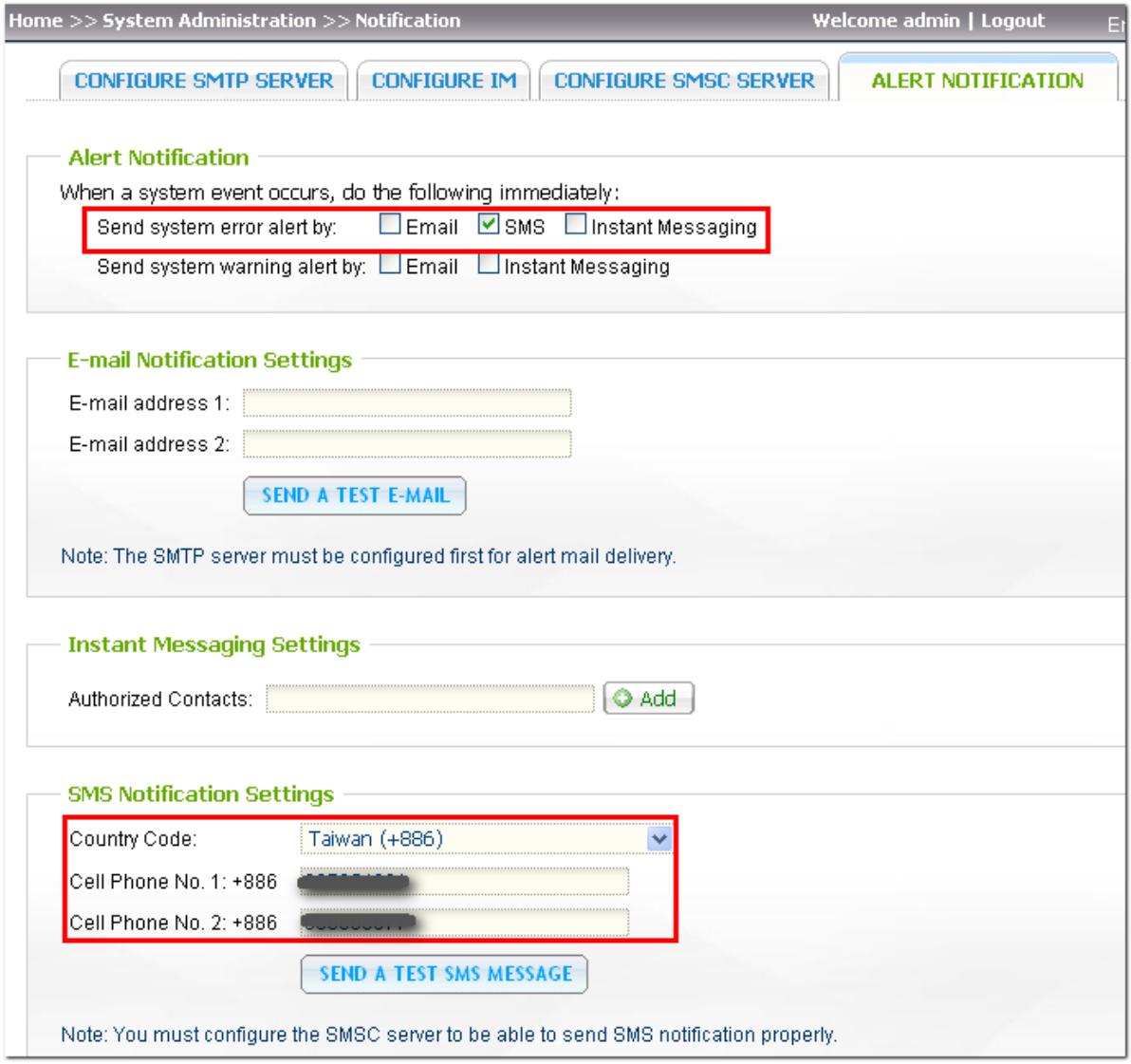
ここまでで、Clickatellにおけるアカウント登録、携帯電話番号の確認、"API ID"の取得が完了しました。 ステップ2に進みましょう。

2. NAS上のSMSCおよびSMSアラート通知を設定する

"System Administration"（システム管理）> "Notification"（通知）> "Configure SMSC server"（SMSCサーバの構成）と移動し、前のステップで取得した情報を入力してSMSCサーバを構成します。



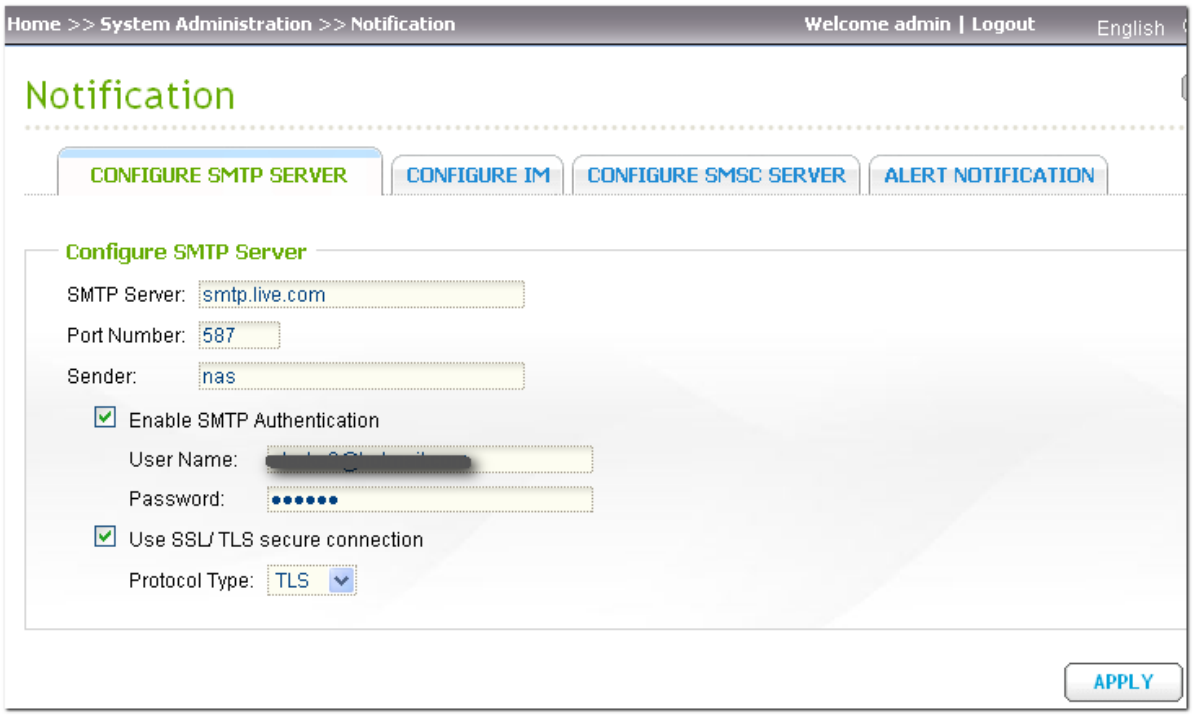
次に、"System Administration"（システム管理）> "Notification"（通知）> "Alert Notification"（アラート通知）に移動し、携帯電話番号を入力します。



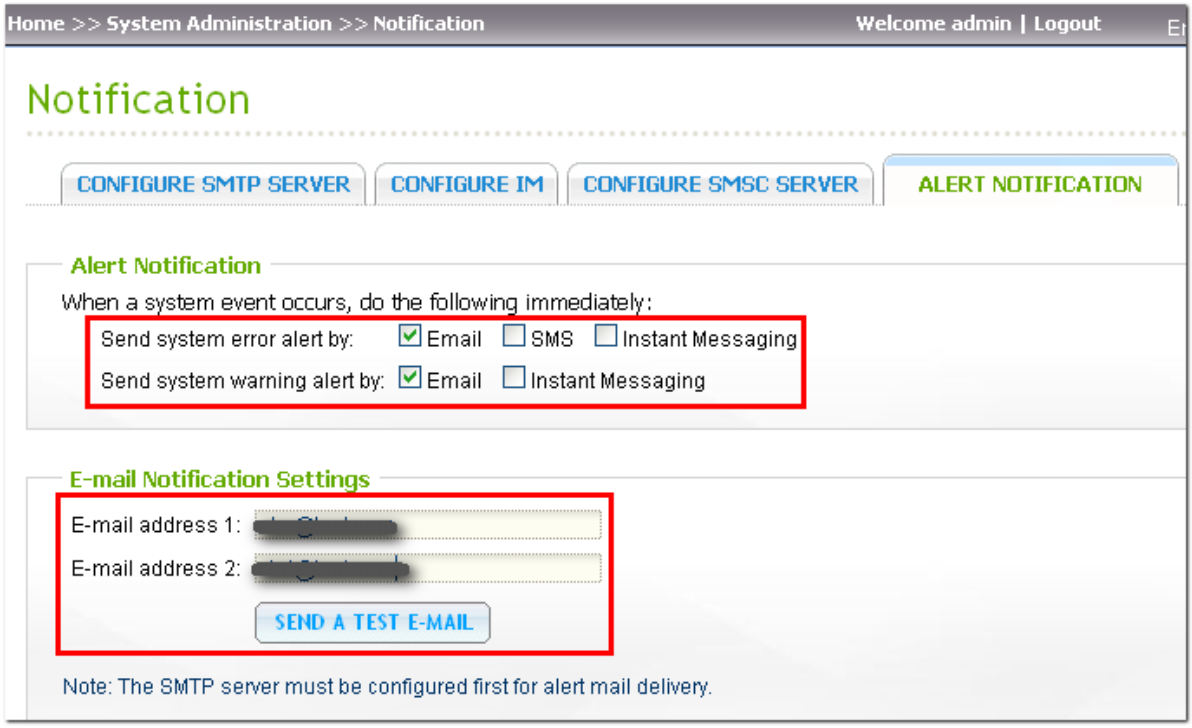
これですべてのセットアップは終了です。"SEND A TEST SMS MESSAGE"（テストSMSメッセージを送信する）をクリックし、SMS通知が正しく構成されたかテストしてみましょう。 正しく構成されている場合、10秒以内に通知を受信するはずです。

Email Alertのセットアップ

"System Administration"（システム管理）> "Notification"（通知）> "Configure SMTP server"（SMTPサーバを構成）と移動し、正しいSMTP情報を入力します。 この例では、SMTPサービスプロバイダとしてGmailを使用しています。



次に、"System Administration"（システム管理）> "Notification"（通知）> "Alert Notification"（アラート通知）と移動しメールアドレスを入力します。また、システムエラーアラートだけでなくシステム警告アラートも受信するかどうかを指定します。"SEND A TEST E-MAIL"（テストメールを送信する）をクリックするとメール送信プロセスをテストすることもできます。



IM(インスタントメッセージング) Alertのセットアップ

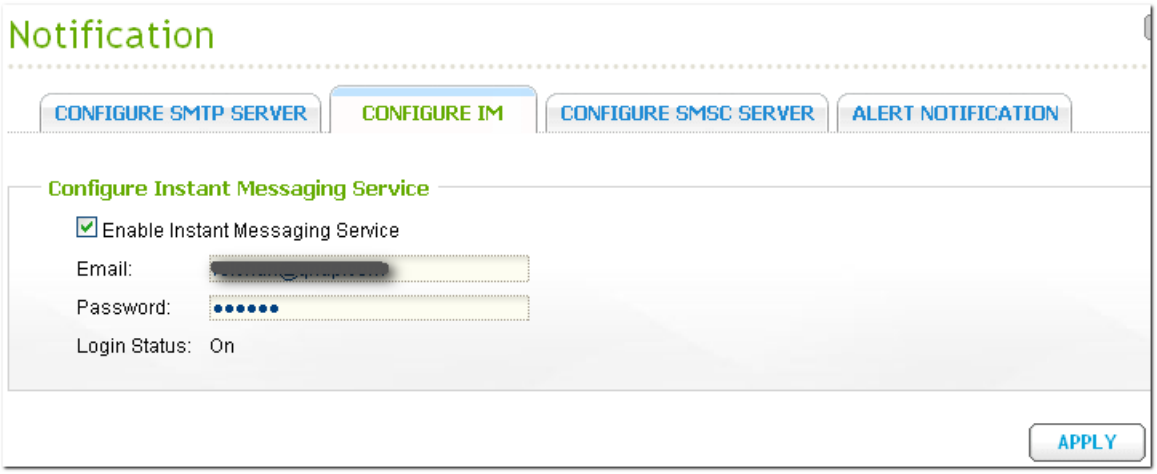
これらの機能を実施するには、以下のステップで行います:

1. https://signup.live.com/ から、NAS 用の Windows ライブメッセンジャー ID にサインアップします。

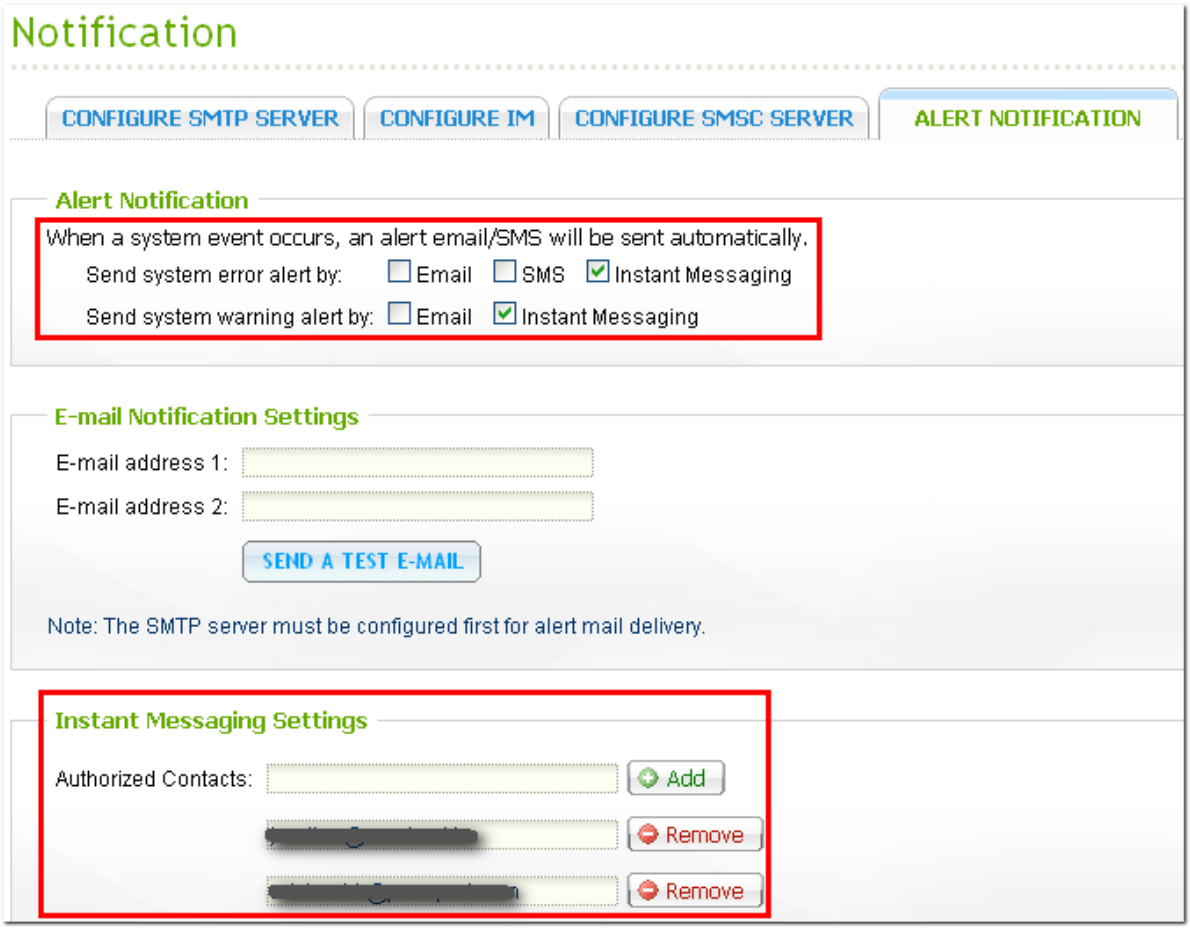
2. お使いの Windows オペレーティングシステム用の Windows ライブメッセンジャーをhttp://explore.live.com/ からダウンロードします。NAS は、Windows ライブメッセンジャー 2009 または、それ以降をサポートします。

3. ステップ 1 で登録した Windows ライブメッセンジャーのアカウントでログインします。NAS との対話を許可する連絡先を最大 10 件追加します。これらの連絡先を NAS のメッセンジャーアカウントに追加していることを確認します。

4. 「Notification (通知)」>「Configure IM (IM設定)」へ進み、ステップ 1 で登録したログイン情報を入力します。「Apply (適用)」をクリックします。ログインステータスが、「On (オン)」と表示されます。



5. 「Notification（通知）」>「Alert Notification（アラート通知）」と進みます。インスタントメッセージによる警告通知を有効にして、「Instant Messaging Settings（インスタントメッセージの設定）」の下に最大 10 件の許可する連絡先を入力します。「Apply（適用）」をクリックします。



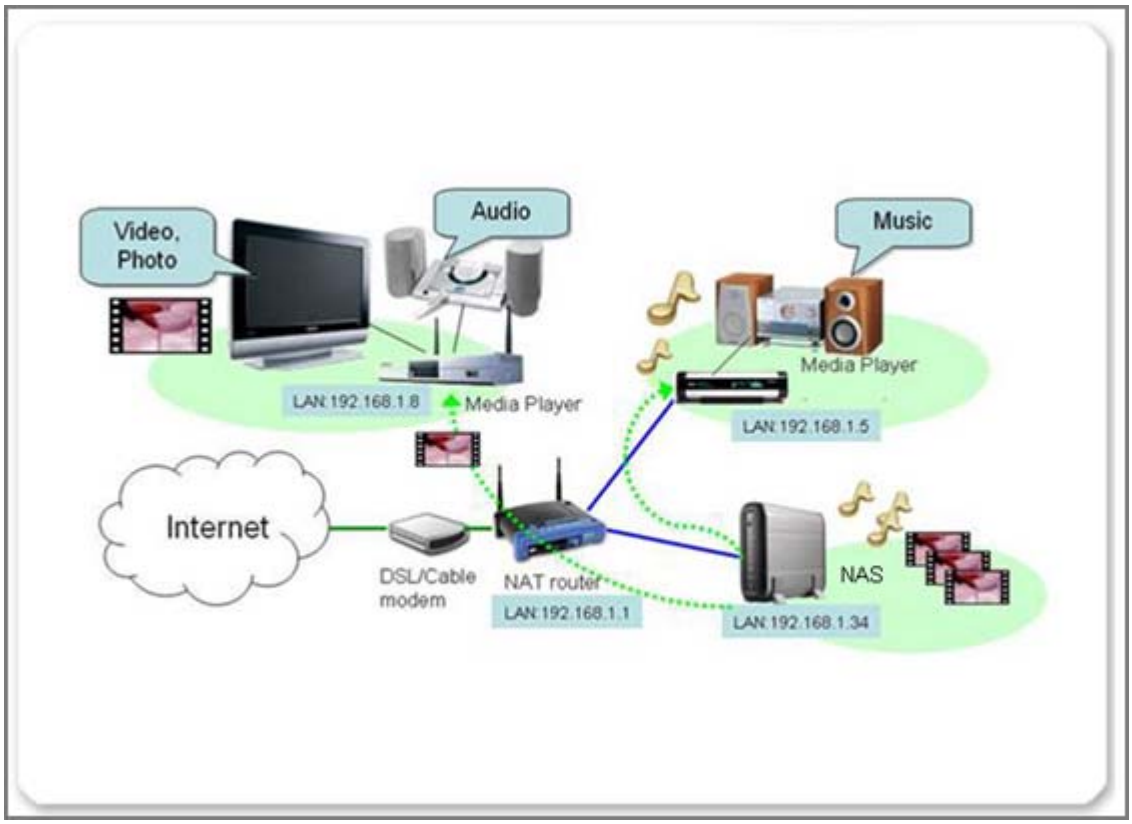
6. 許可された Windows ライブメッセンジャーアカウントでログインして、Windows ライブメッセンジャーを経由し、NAS を対話します。NAS は、イベント発生時に、即時エラー/警告メッセージを許可された連絡先に送信します（英語のみ）。

許可された Windows ライブメッセンジャーの連絡先を使用し、次のコマンドを入力して、NAS からリアルタイムでシステム情報を問い合わせることができます。情報は、英語でのみ利用可能です。

コマンド	説明
help	コマンドのオプション一覧が表示されます。
info-cpu	現在の CPU 温度を問い合わせます。
info-sys	現在のシステム温度および冷却ファンのスピードを問い合わせます。
info-model	NAS のモデル番号と問い合わせます。
info-hd	NAS 上のハードディスクの個数を問い合わせます。
info-hd-[hd#]	ハードディスクの現在の温度およびスマートステータス(自己監視および報告技術によるステータス)を問い合わせます。例、info-hd-1
info-vol	NAS 上のディスクボリュームの個数を問い合わせます。
info-vol-[vol#]	ディスクボリュームの情報を問い合わせます。例、info-vol-1 の情報

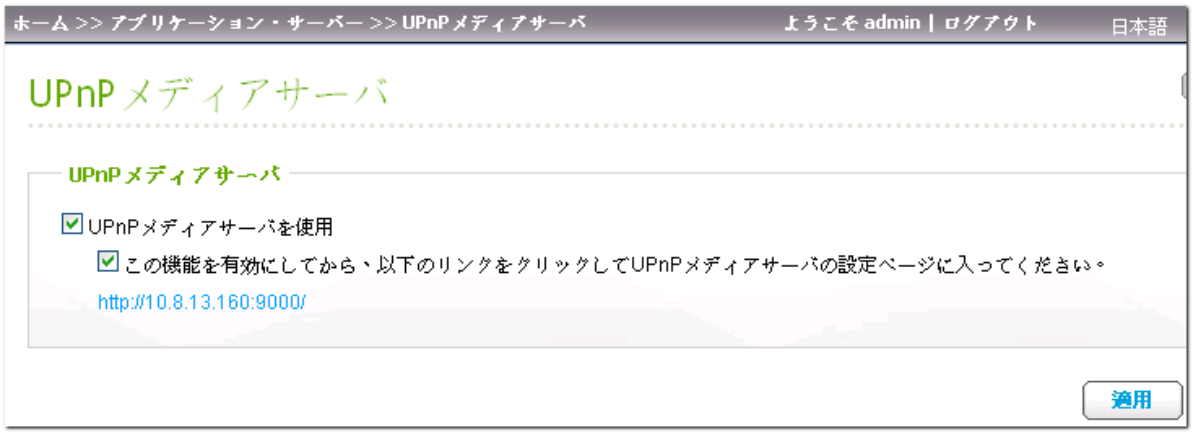
15．メディアプレーヤー用にUPnPメディアサーバをセットアップする

このセクションでは、マルチメディアファイルをローカルネットワーク上のメディアプレーヤーと共して、ご自宅のホームエンターテーメントシステムで再生するためのQNAP NASのUPnPメディアサーバのセットアップ法を説明します。



UPnPメディアサーバの効化

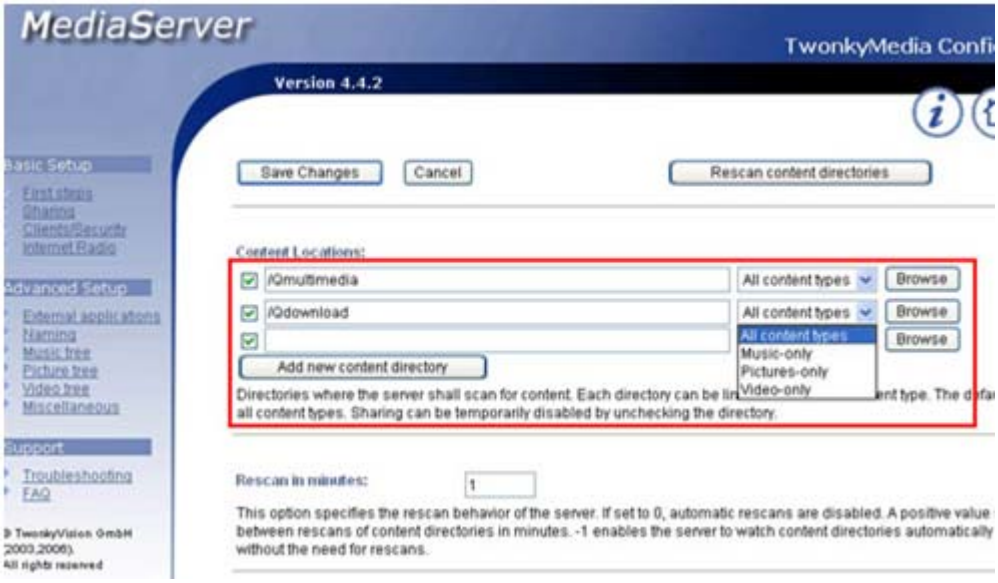
"Applications"（アプリケーション）> "UPnP Media Server"（UPnPメディアサーバ）に移動し、 "Enabled UPnP Media Server"（UPnP メディアサーバを有効化する）のチェックボックスにチェックマークを入れ、"Apply"（適用）をクリックします。 UPnPメディアサーバ機能はこれで準備完了です。



TwonkyMediaサーバのセットアップ

この例でご紹介するTwonkyMediaのバージョンは、4.4.2です。NASがサポートする実際のバージョンは、予告なく更されることがあります。

ブラウザから http://NAS IP:9000/ に移動すると、構成ページに入ります。"Content Locations" (コンテンツの場所下で、ホームネットワーク内で共したいコンテンツの場所を指定することができます。 QNAP NAS上のコンテンツのパスを入力します。(デフォルトのフォルダはQmultimediaです。 この例では、共/Qdownload (Qダウンロードを追加しています。



多量のメディアコンテンツを所している際は、閲覧を容易にするために、写真、動画、および音楽のナビゲーションツリーを構成することが出来ます。 このパワフルな機能により、TV上でメディアコンテンツを選択するのが容易になります。

構成が完了した際に、Save Changes (更を保存のボタンをクリックして設定を保存するよう確認してください。

これで、QmultimediaフォルダやMutimediaフォルダあるいはWindowsのマップ済みドライブまたはFTPからNASにメディアプレーヤー用として追加したあらゆるカスタムフォルダへ、mp3、画像、動画を移動することができます。

メディアプレーヤーとの接続をセットアップ

実際の配線について:
この例では、ハイディフィニション(HDメディアプレーヤをQNAP NASと併用しています。 メディアプレーヤはNASのUPnPメディアサーバによって送信されたストリーム·マルチメディアファイルを受信するのに使用されます。そしてこれらのファイルを換し、TVあるいはHi-Fiシステムにより再生できるようにします。 これらのインターフェイスにおけるケーブルの長さの限界により、メディアプレーヤは通常、TVやHi-Fiシステムの側に配置する必要があります。

TCP/IP設定について:
ご家庭のLANにメディアプレーヤーを接続し、DHCPによりIPアドレスを取得するよう設定します。 (ほとんどのメディアプレーヤーはDHCPクライアントとして定義されており、ホームネットワークに接続した際に自動的にIPアドレスを割り当てられます。

メディアプレーヤーのビデオおよびオーディオ出力をご使用のTVに接続する

複合ビデオ/オーディオ出力、ビデオ出力用のS-ビデオ、S/PDIFデジタルオーディオ、あるいはビデオとオーディオの両方の信号を処理できる最新のHDMIインターフェイスなど、異なるビデオおよびオーディオインターフェイスがメディアプレーヤーに付属している場合があります。

例1（Buffalo LinkTheaterを使用)

この例では、TVにビデオおよびオーディオ出力ケーブルが接続されています。 オーディオ出力をステレオ音響システムに接続することもできます。

メディアプレーヤーに接続されているTVの電源を入れます。メディアプレーヤーのリモートコントロールによりオプションを選択することができます。 メディアプレーヤーがネットワーク上のNASを検出します。 NASの名前が画面に表示されます。

NASの特定のフォルダにより共されている写真、ビデオ、および音楽を検出することができます。 メディアプレーヤーのリモートコントロールを使用してファイルを選択、再生することができます。

例2 (ZyXEL’s DMA-1000W)

ZyXEL DMA-1000WはSigmaDesignsのプラットフォームを基礎としたモデルの一つです。

ご使用のTVがHDMIインターフェイス搭の場合、オーディオとビデオの両方は一本のケーブルだけで処理できます。 メディアプレーヤーとTVをHDMIケーブルを使用して接続してください。

TVがHDMIインターフェイスに対応していない場合、ビデオ出力にはS-ビデオケーブルを使用してTVに接続、オーディオ出力には複合左/右オーディオインターフェイスで接続することができます。 音楽をより高音質でお楽しみいただくには、ご使用のHi-FiシステムにS/PDIFケーブルを使用して接続してください。

TVの電源をいれ、選択したインターフェイスにあわせTVをスイッチします(例:HDMIあるいはS-ビデオ）。メディアプレーヤーのリモートコントロールをご使用いただき、"Server"（サーバ）のページに入るよう選択します。メディアプレーヤーはNASを自動的に検出します。 これで、NASからマルチメディアファイルを再生したり、インターネットラジオを聴くことができます。

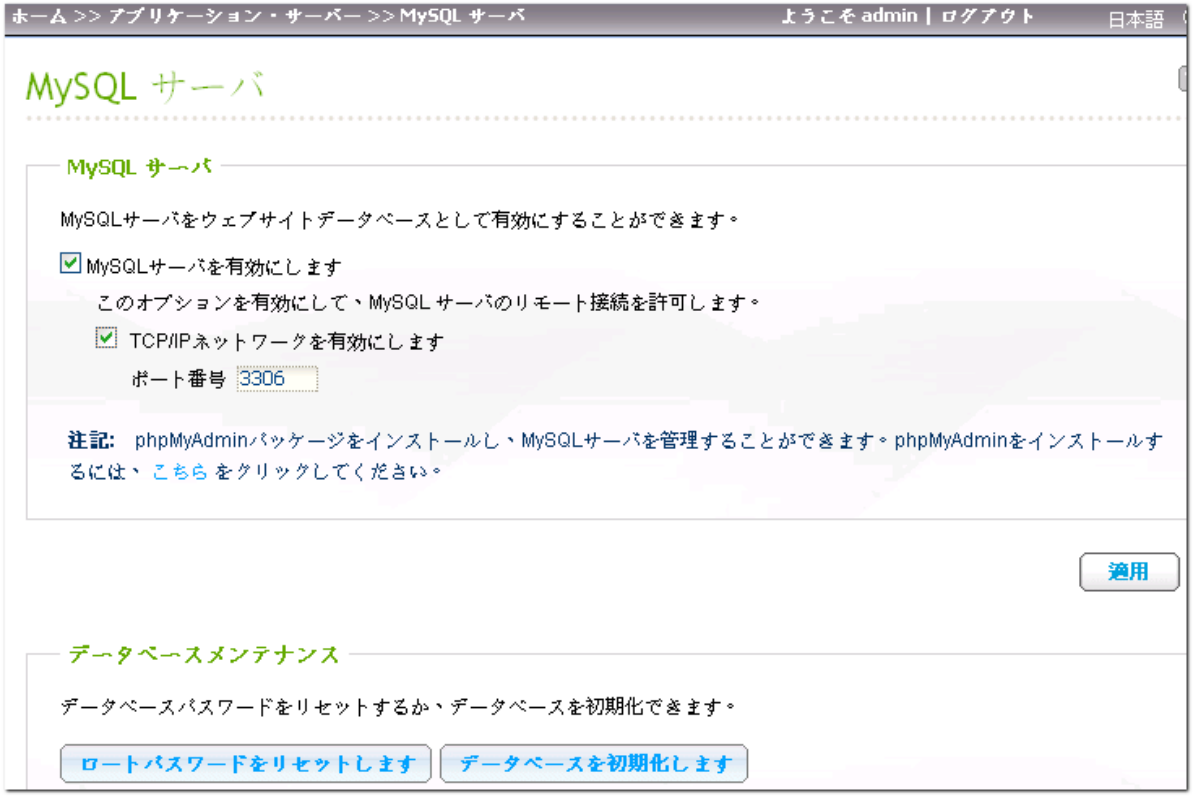
16. QNAP NASにてPHPBBフォーラムをホストする

本セクションでは、QNAP NASで人気の高いオープンソースフォーラムソフトウェアのphpBBを使用してフォーラムをホストする方法を説明します。

WebサーバおよびMySQLデータベースサーバの効化

NASの管理ページにログインし、"Network Services"（ネットワークサービス）> "Web Server"（Webサーバ）に移動します。"Enable Web server"（Webサーバを有効化）のオプションを選択し、"Apply"（適用）をクリックします。

次に、 "Applications"（アプリケーション） > "MySQL Server"（MySQLサーバ）と移動し、"Enable MySQL Server"（MySQLサーバを有効化）および"Enable TCP/IP Networking"（TCP/IPネットワークを有効化）のオプションにチェックマークを入れ、"Apply"（適用）をクリックします。



phpMyAdminにてphpBB3用データベースを作成

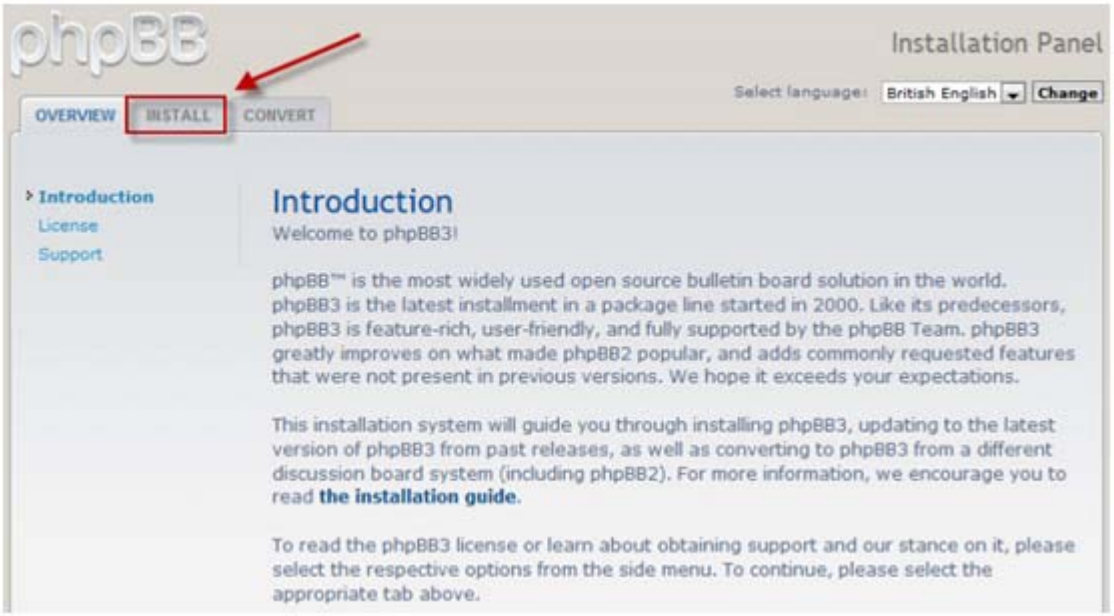
phpBB3のインストール前に、そのための新規データベースを作成する必要があります。データベース作成にはphpMyAdminを使用しますので、phpMyAdmin QPKGをNASでまだ実行していない場合は、これをまずインストールしてください。インストール終了後、ブラウザからhttp://NAS-IP/phpMyAdmin/に移動し、ユーザー名およびパスワードを入力してログインします。(デフォルトのユーザー名およびパスワードはroot/adminです）。ご希望の言語を選択することもできます。

ログイン後、"Create new database"（新規データベースを作成）の欄にデータベース名 "phpBB3"を入力します。ご希望のデフォルトのエンコード言語(最も互換性があるのはUTF-8です）を選択し、"Create"（作成）をクリックします。では、次のステップに進みましょう。

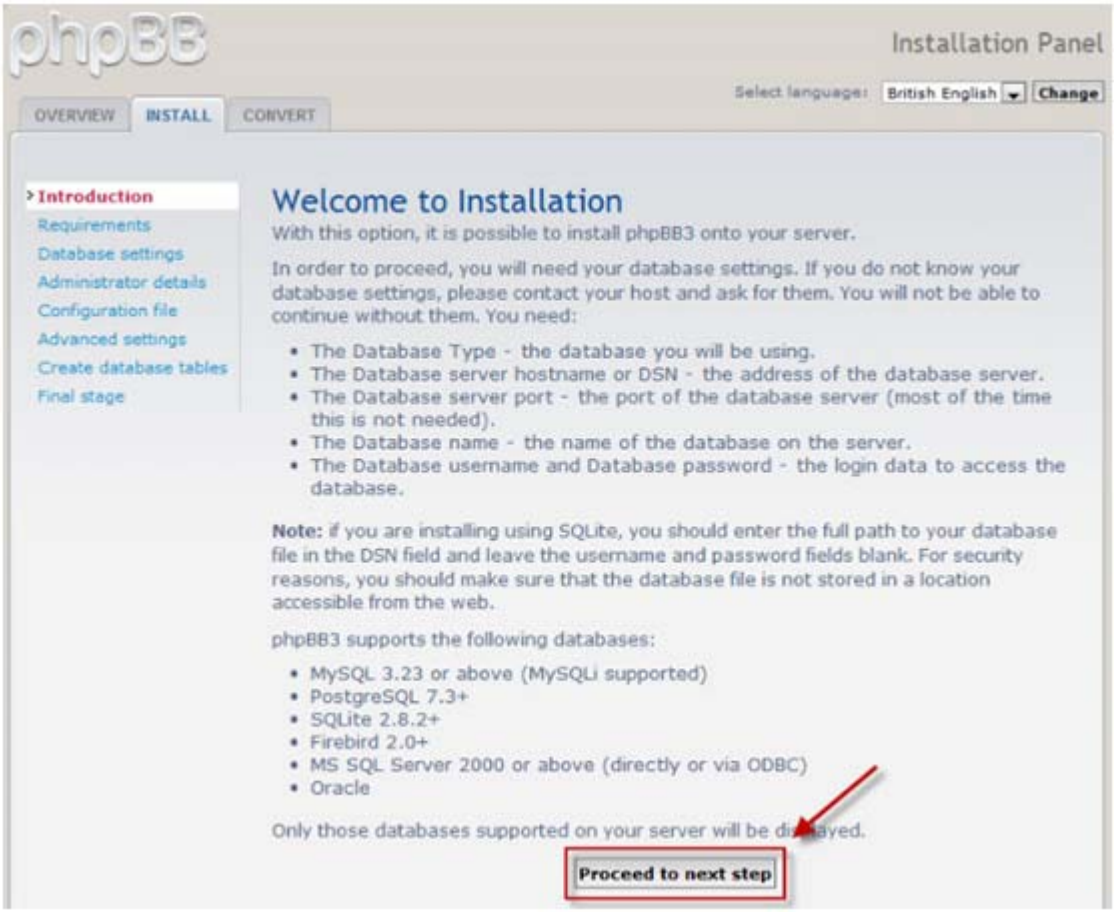
phpBB3 Webベースインストールを開始する

phpBB3ソースアーカイブを http://www.phpbb.com/downloads/olympus.php からダウンロードします。[Full Package]（フルパッケージ）をダウンロードし、QwebまたはWeb共有フォルダにzip解凍します。

ブラウザから http://NAS-IP/phpBB3 に移動すると、下のようなphpBB3 Webベース インストールページが表示されます。"INSTALL" (インストール）タブをクリックして開始します。

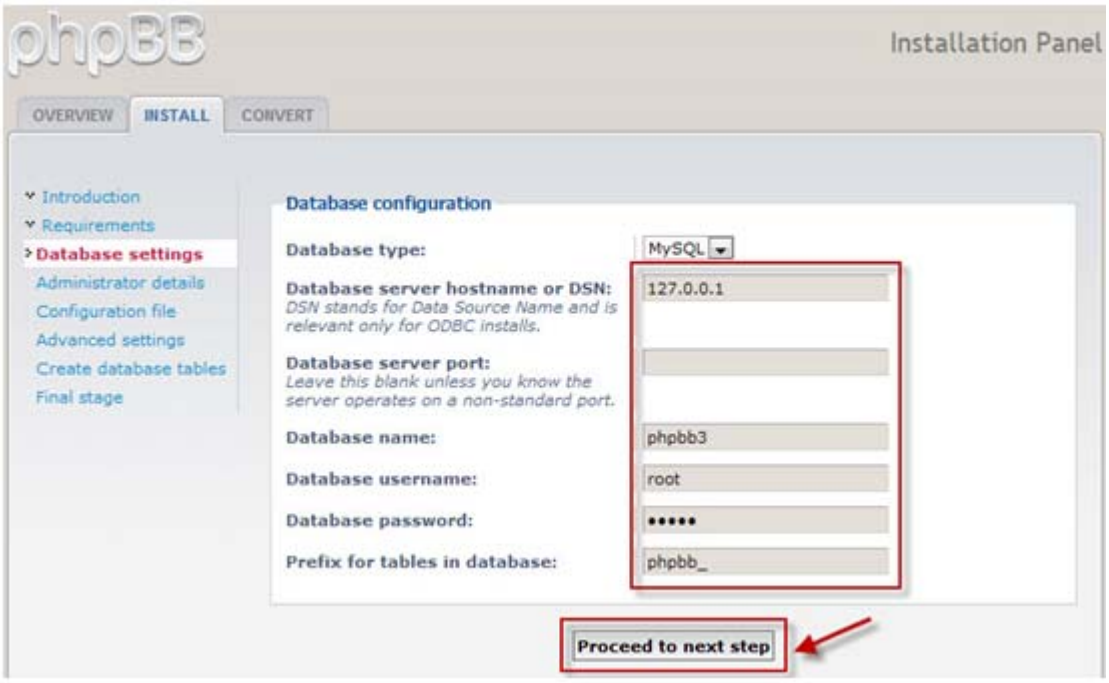


"Proceed to next step"（次のステップに進む）をクリックして次のステップに進みます。

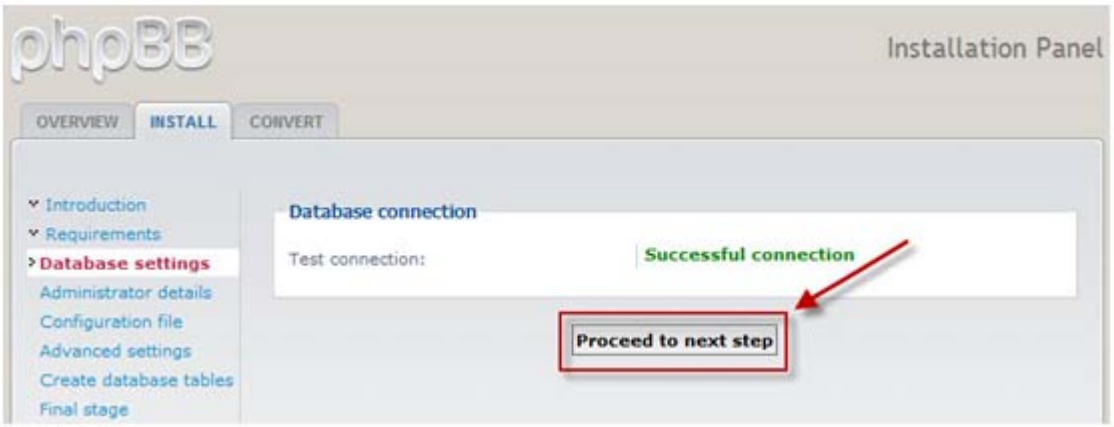


インストールの互換性ページが表示されます。 ほとんどの場合、ご使用のWebサーバは必要条件と互換しているはずです。"Start install"（インストールを開始）をクリックして次のステップに進みます。

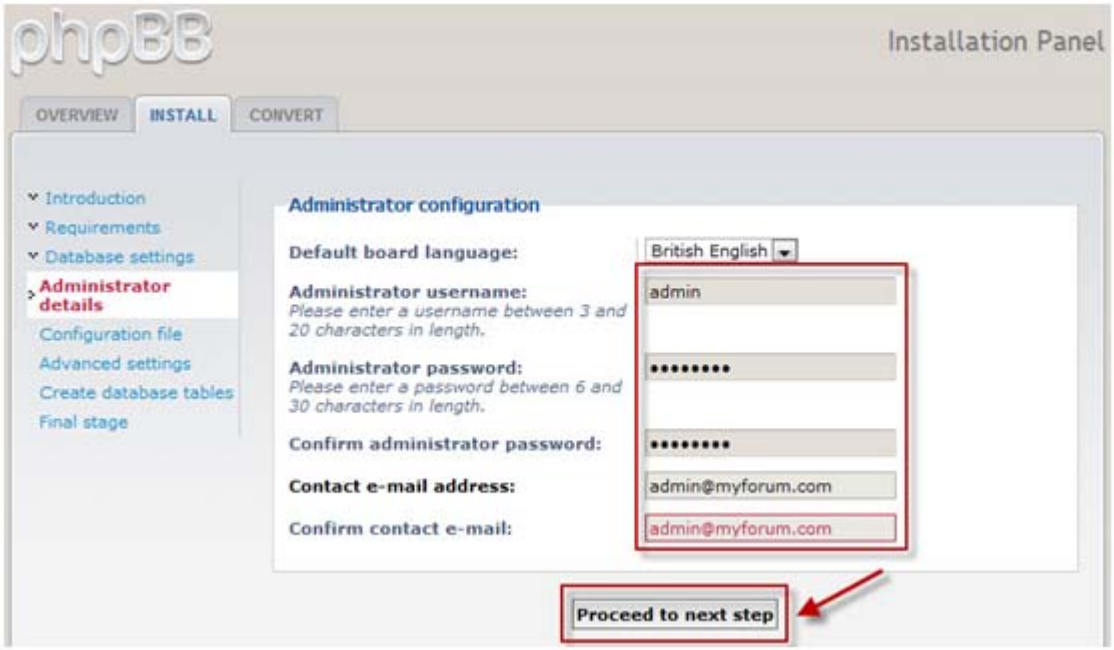
ホスト名、データベース名、データベースのユーザー名およびパスワードなどのMySQL情報を空欄に入力し、"Proceed to next step"（次のステップに進む）をクリックして続行します。



MySQLサーバが実行され、先に作成したデータベース "phpBB3" が正しく存在している場合、"Successful connection"（接続成功）と表示されます。"Proceed to next step"（次のステップに進む）をクリックして次のステップに進みます。

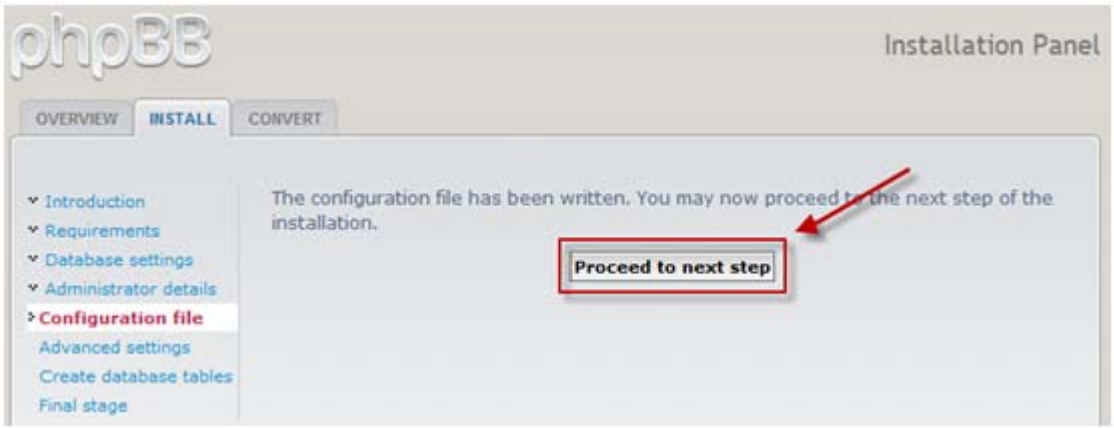


phpBB3管理者ユーザー名およびパスワード、また有効なメールアドレスを指定します。 その後、"Proceed to next step"（次のステップに進む）をクリックします。

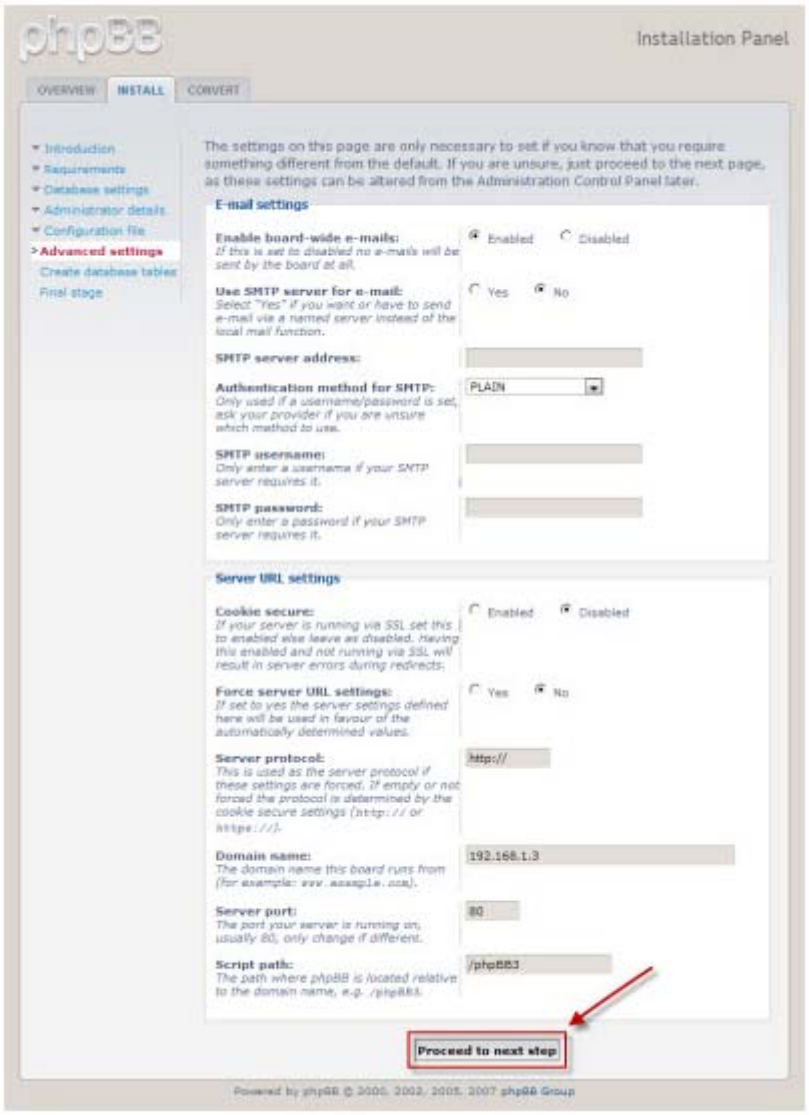


"Tests passed"（テスト成功）と表示されたら、"Proceed to next step"（次のステップに進む）をクリックして続行します。

phpBB3はここで構成ファイル(config.php）にすべての設定情報を書き込みます。"Proceed to next step"（次のステップに進む）をクリックして次のステップに進みます。

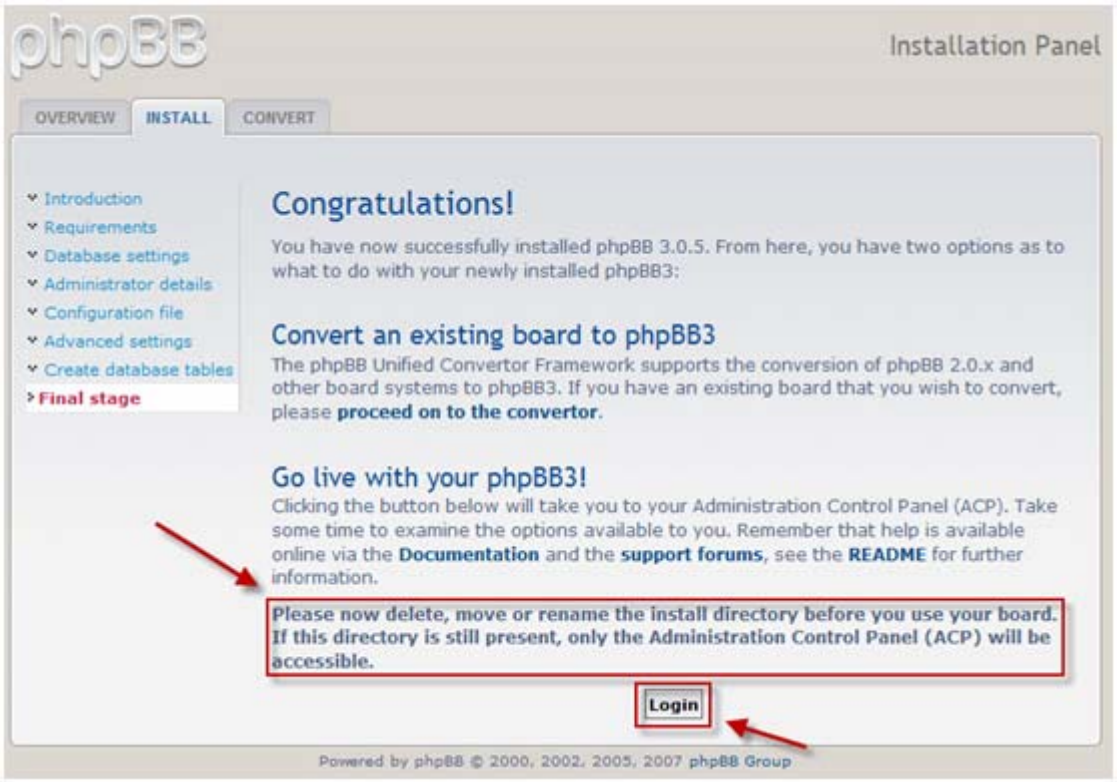


ご希望にあわせ詳細を指定し、その後"Proceed to next step"（次のステップに進む）をクリックして続行します。

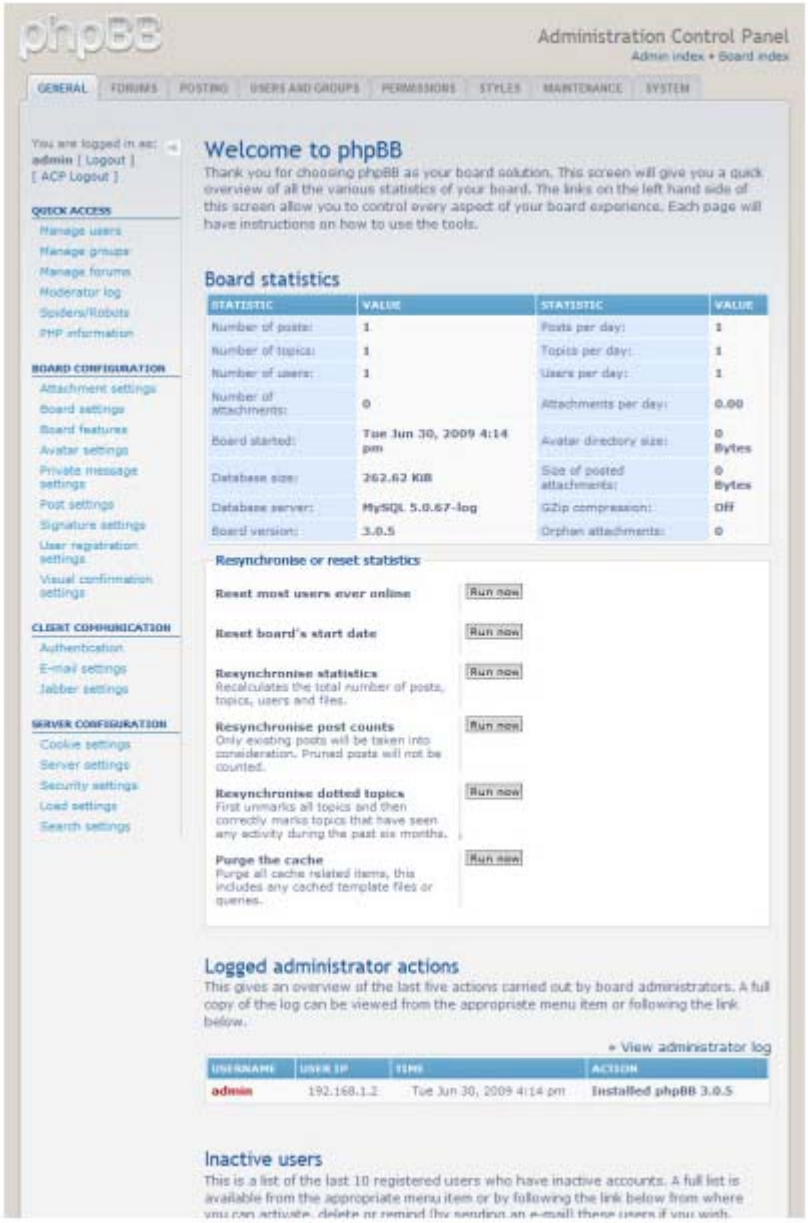


phpBB3はすべてのデータベーステーブルおよびいくつかの初期データをここで作成します。"Proceed to next step"（次のステップに進む）をクリックして次のステップに進みます。

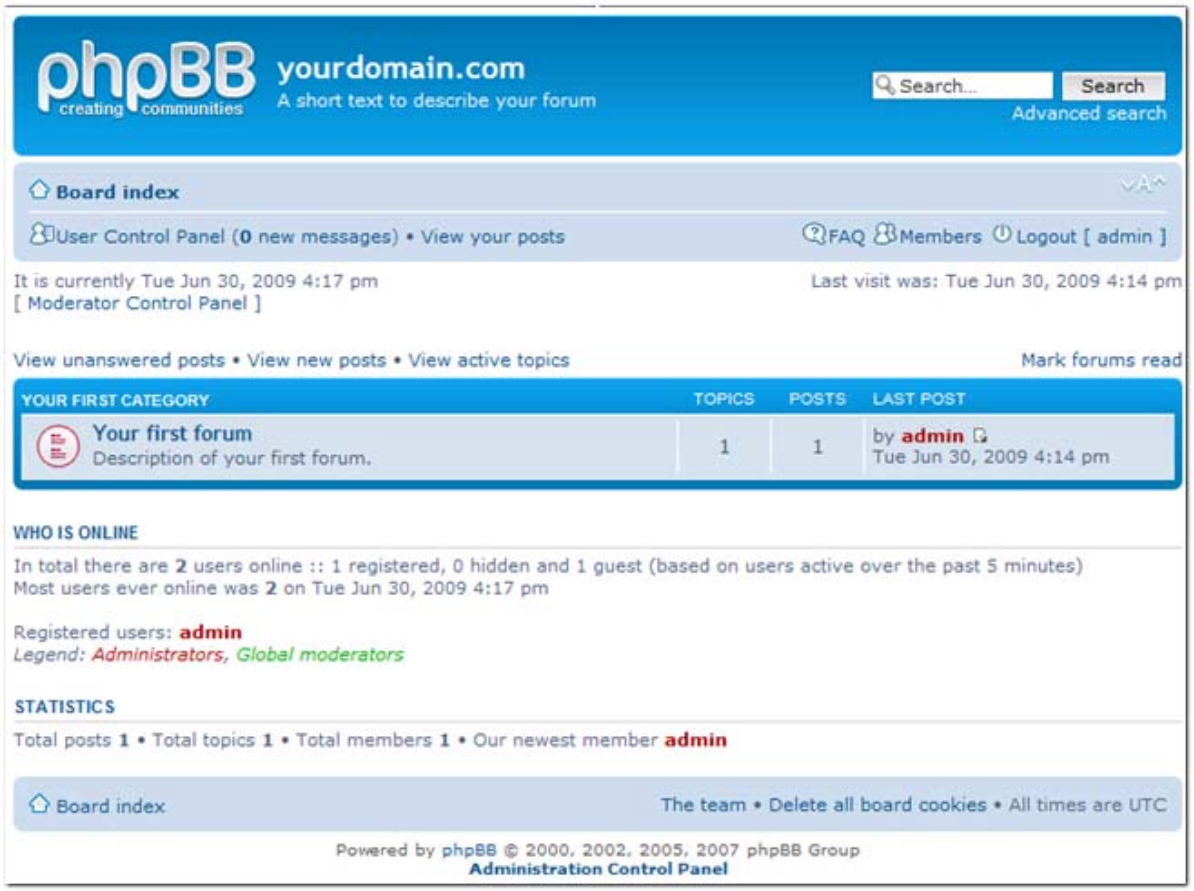
最後の手順として一つだけ残っていることは、phpBB3フォルダ内のインストールフォルダを削除することです。削除後は、"Login"（ログイン）をクリックすればphpBB3の管理ページに入ることができます。



これがphpBB3のAdministration Control Panel（管理コントロールパネル）です。すべての管理タスクをここで行うことができます。



これが新しく設置したphpBB3フォーラムの最初のページとなります。オンラインコミュニティを作り上げるため、フォーラム招待状の送信を始めましょう。



17. NAS メンテナンス

シャットダウン/再起動 690
システム温度保護 692

17.1 シャットダウン/再起動

シャットダウン/再起動の手順は次の通りです。

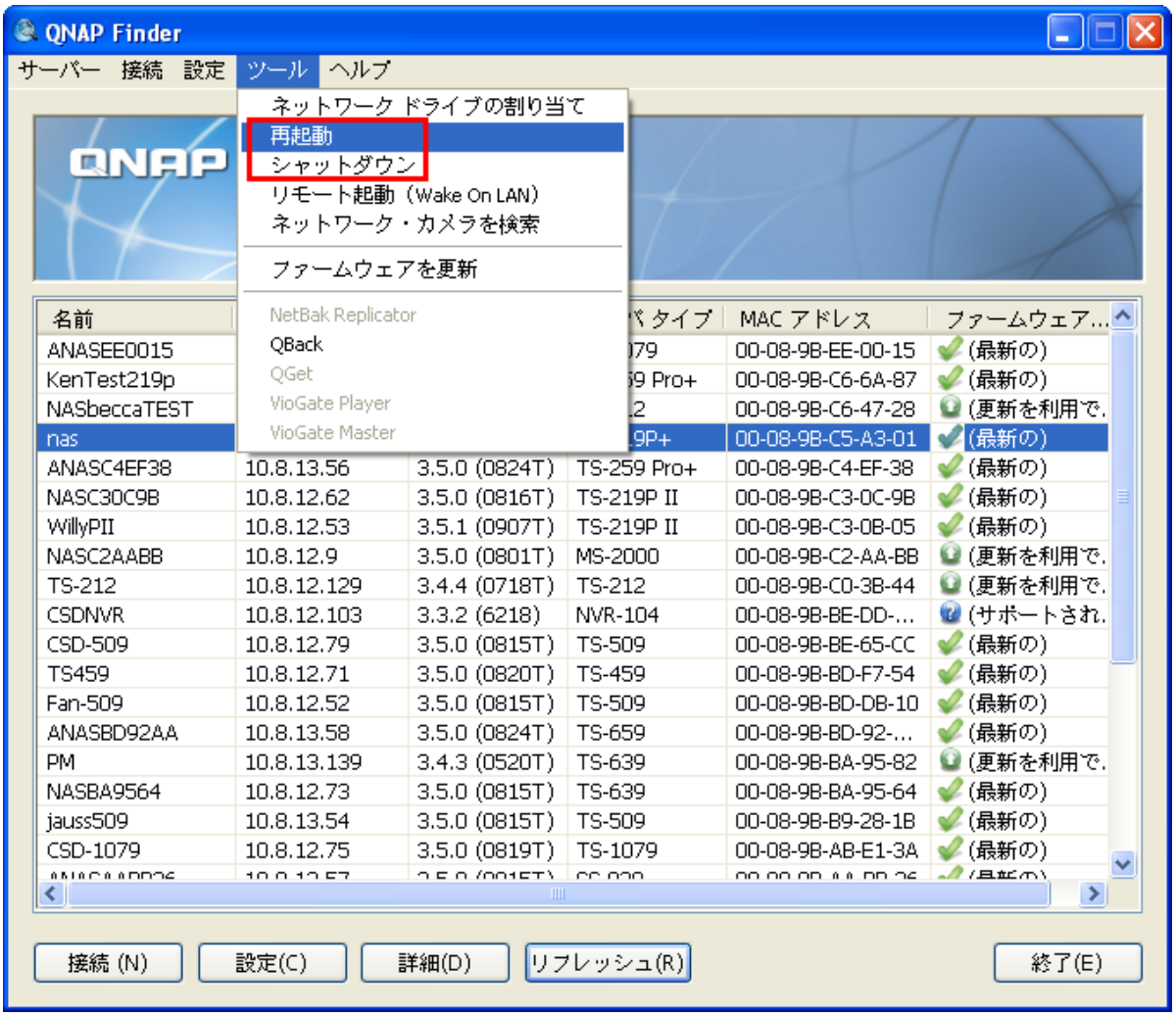
a. NASにログインします。「システム管理」>「パワーマネジメント」に進みます。

b. 「再起動」をクリックしてサーバを再起動するか、「シャットダウン」をクリックしてサーバの電源をオフにします。

電源ボタンを1.5秒間*押すとNASの電源がオフになります。NASを強制終了にするには、電源ボタンを5秒間以上押し続けます。ビープ音が一度鳴ると、サーバーは直ちにシャットダウンします。

*TS-109I/II、TS-109 Pro I/II、TS-209 I/II、TS-209 Pro I/II、TS-409/ TS-409 Pro/ TS-409Uの電源をオフにするには、電源ボタンを4秒間押してください。

Finder を使用してサーバーの再起動やシャットダウンを行えます (管理者権限が必要となります)。



17.2 システム温度保護

以下の条件のうちいずれかが発生した場合、システムはハードウェア保護のため自動的にシャットダウンします:

- システム温度が70°C (158°F)を超える
- CPU温度が85℃ (185°F)を超える
- ハードドライブ温度が65°C (149°F)を超える*

* NASのいずれかのハードドライブの温度が65°C (149°F)を超えた場合、NASはスタンバイ時間（「システム管理」 >「ハードウェア」で設定）まで待ち、その後10分間経過すると、自動的にシャットダウンします。例えば、休止状態になってから5分間後にスタンバイモードになるようにNASを設定すると、いずれかのハードドライブの温度が継続して65°C (149°F)を超える場合、NASは15分（5 + 10分）後に自動的にシャットダウンします。

18. GNU GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright © 2007 Free Software Foundation, Inc. <http://fsf.org/>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble
The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this

provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS
0. Definitions.
'This License' refers to version 3 of the GNU General Public License.

'Copyright' also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

'The Program' refers to any copyrightable work licensed under this License. Each licensee is addressed as 'you'. 'Licensees' and 'recipients' may be individuals or organizations.

To 'modify' a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a 'modified version' of the earlier work or a work 'based on' the earlier work.

A 'covered work' means either the unmodified Program or a work based on the Program.

To 'propagate' a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To 'convey' a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays 'Appropriate Legal Notices' to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.
The 'source code' for a work means the preferred form of the work for making modifications to it. 'Object code' means any non-source form of a work.

A 'Standard Interface' means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The 'System Libraries' of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A 'Major Component', in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The 'Corresponding Source' for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.
All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.
No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to

the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.
You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.
You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.
b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to 'keep intact all notices'.
c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.
d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.
A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an 'aggregate' if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.
You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.
b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical

medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.
c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.
d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.
e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.
A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A 'User Product' is either (1) a 'consumer product', which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, 'normally used' refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

'Installation Information' for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the

network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.
'Additional permissions' are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or
b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or
c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or
d) Limiting the use for publicity purposes of names of licensors or authors of the material; or
e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or
f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.
All other non-permissive additional terms are considered 'further restrictions' within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.
You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.
Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An 'entity transaction' is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.
A 'contributor' is a copyright holder who authorizes use under this License of the Program or a work on which the

Program is based. The work thus licensed is called the contributor's 'contributor version'.

A contributor's 'essential patent claims' are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, 'control' includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a 'patent license' is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To 'grant' such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. 'Knowingly relying' means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is 'discriminatory' if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.
If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.
Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.
The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License 'or any later version' applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.
THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM 'AS IS' WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.
IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY

COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.
If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS