



パッケージ管理

パッケージ（追加機能）

メニューからご利用のパッケージ（追加機能）をお選びください。

事前にご利用のパッケージを追加してください

設定画面の [システム] → [パッケージ管理] → [追加] から追加できます。

製品によっては、非対応のパッケージがあります

各パッケージの対応情報については、[弊社サイト](#)をご確認ください。

本製品でのFTP共有機能

FTP共有を有効に設定した共有フォルダーに、FTPクライアントよりアクセスすることができます。
FTP共有サービスを利用して本製品にアクセスする際の権限は、共有フォルダーに設定した詳細アクセス権設定により以下ようになります。

本製品のFTP共有サービスに、「anonymous」ユーザーでアクセスする場合	・共有フォルダーの詳細アクセス権設定を無効にした共有フォルダーにアクセスできません。 ・共有フォルダーの読み取り専用オプションをチェックしている場合は、ダウンロードのみ可能です。 ・共有フォルダーの読み取り専用オプションを未チェックの場合は、ダウンロード/アップロードが できます。
本製品のFTP 共有サービスに、 本製品に登録したユーザーでアクセスする場合	・本製品に登録したユーザー名とパスワードでFTP共有に接続できます。 ・登録したユーザー名、もしくは、登録したユーザーが含まれるグループ名に設定したアクセス権にしたがってアクセスできます。 読み取り → ダウンロードのみ可能 読み書き → ダウンロード/ アップロードが可能 ただし、共有フォルダーの読み取り専用オプションをチェックしている場合は、上記の設定にかかわらず、ダウンロードのみ可能です。

FTP共有を有効にする

あらかじめ作成済みの共有フォルダーをFTP共有可能にする設定を説明します。
共有フォルダーの作成方法は、本体の【画面で見るマニュアル】をご覧ください。

ご注意

ファイル数の多い共有フォルダーを変更すると、変更が完了するまでに時間がかかる場合があります。また、変更が完了するまで共有フォルダーにはアクセスできません。

- 1. [共有] → [フォルダー] → [一覧] をクリック
- 2. FTP用に変更する共有フォルダーの[変更] をクリック

一覧

名前	基本設定	操作
LAN DISK Log		<button>変更</button>
disk1		<button>変更</button> <button>削除</button>
usb1		<button>変更</button>
usb2		<button>変更</button>

詳細アクセス権設定が無効になっている共有フォルダーの名前は赤色で表示されます。

追加へ

- 3. [基本設定] の [FTP共有] にチェックをつけ、[変更] をクリック

変更

名前	share
コメント	
基本設定	☐ 読み取り専用 ☐ 非登録ユーザーからのアクセスを拒否 ☐ Amazon S3 同期 ☐ Dropbox 同期 ☒ FTP共有 ☒ Microsoftネットワーク共有 ☐ ごみ箱 ☐ 隠し 使用量制限値 0.0 GB ☐ レプリケーション機能
詳細アクセス権	☐ 有効 ☒ 無効
情報	●現在下記サービスは無効です。設定ページへ移動。 ・使用量制限

変更

一覧へ

FTP共有設定をする

- 1. [共有] → [方式] → [FTP共有設定] をクリック
- 2. ①FTP共有に関する設定をする
- ② [適用] をクリック

FTP共有設定

FTP共有

ポート

エンコード

☒ 有効 ☐ 無効

☐ Shift-JIS ☒ UTF-8

適用

FTP共有	FTP共有設定の有効/無効を選びます。
ポート	ネットワーク環境に応じて変更します。通常は変更する必要はありません。
エンコード	接続するFTPクライアントによっては、ファイル名が文字化けする場合があります。使用するクライアントに合わせてエンコードを選択します。

FTPクライアントから接続する

[FTPクライアントからのご利用について](#)

[公開フォルダーについて](#)

[FTPクライアントソフトについて](#)

[Windows標準のFTP機能を使用する場合](#)

FTPクライアントからのご利用について

●詳細アクセス権を設定している場合

作成したFTP用の共有フォルダーに保存されているファイルをFTP経由でダウンロードできます。アクセス許可設定したユーザー/グループに限りアクセスできます。FTPクライアントから接続するには、下記のユーザー名、パスワードでログオンしてください。

ユーザー名	設定したユーザー名
パスワード	設定したパスワード

アップロードしたファイルの使用量は、ログオンしたユーザーおよび、ユーザーのプライマリーグループに加算されます。

●詳細アクセス権を設定していない場合

作成したFTP用の共有フォルダーはネットワーク経由で誰でもデータをダウンロード/アップロードできるようになります。FTPクライアントから接続するには、下記のユーザー名、パスワードでログオンしてください。

ユーザー名	anonymous または ftp
パスワード	任意

公開フォルダーについて

●ログイン直後はフォルダーの最上位階層(/)が見えます。このフォルダーやsataraid1フォルダーには、フォルダーを作成したりファイルを保存することはできません。

●内蔵ボリューム上に作成した共有フォルダーは、以下のフォルダーに公開されます。
/sataraid1/作成した共有名

●USBポートx（xはポート番号）に接続したUSB HDDは、FTPで公開すると、以下のようにアクセスできます。
/usbx（xはポート番号）

```
├── sataraid1 ── 作成した共有名 1
│
│           ── 作成した共有名 2
│           ── ...
├── usb1
├── usb2
```

FTPクライアントソフトについて

本製品にFTPでアクセスするには、FTPクライアントソフトが必要となります。別途ご用意ください。

ご注意

ご使用になるFTPクライアントソフトのサポートする文字コードにあわせて、エンコードを選択してください。[FTP共有設定をする](#)
日本語ファイル名を取り扱う場合は、Shift-JIS もしくはUTF-8の文字コードに対応したFTPクライアントソフトをご利用ください。

Windows標準のFTP機能を使用する場合

ここでは、WindowsのFTPコマンドによるアクセスの例を説明します。

※Windows標準のFTP機能の詳細な操作方法や不明点は、各パソコンメーカーへお問い合わせください。

1. あらかじめ、本製品の[FTP共有設定](#)のエンコードを「Shift-JIS」に変更する
2. [スタート]→[すべてのプログラム]→[アクセサリ]→[コマンドプロンプト]をクリック
3. コマンドプロンプトのカレントディレクトリをFTPでアップロードするファイルを保存したフォルダー、またはFTPでダウンロードしたファイルを保存するフォルダーに移動する
C: ¥ FTPフォルダーにカレントディレクトリを移動する場合
>cd c: ¥ ftp
4. コマンドプロンプトに以下のように入力
>ftp xxx.xxx.xxx.xxx
※「xxx.xxx.xxx.xxx」の部分は、同一LAN内から接続する場合は本製品のIPアドレスを入力します。
5. ユーザー名、パスワードを入力
アクセスする共有フォルダーへのアクセス権限を持ったユーザー名とパスワードを入力してください。
※詳細アクセス権設定していない共有フォルダーへのアクセスには以下のユーザー名とパスワードを入力します。

ユーザー名	anonymousまたはftp
パスワード	任意

※ファイルをバイナリモードで転送する場合は、ログイン後、binコマンドを実行してください。

6. FTPでアクセスする
以下は内蔵ボリューム上の共有フォルダー「disk1」に対する操作例です。
 - ファイルのアップロード
ftp > cd /sataraid1/disk1
ftp > put アップロードするファイル名
 - ファイルのダウンロード
ftp > cd /sataraid1/disk1
ftp > get ダウンロードするファイル名
 - FTPアクセスを終了
ftp > bye

ご注意

●エクスプローラまたは、Internet Explorerのアドレスバーでftp://xxx.xxx.xxx.xxx/（xxx.xxx.xxx.xxxの部分は、本製品のIPアドレス）や ftp://LAN DISKの名前/ でアクセスした場合、全角文字が文字化けした状態で表示される場合があります。

●FTP共有機能を使用すると、フォルダーやファイル名が文字化けしてしまう場合は、以下をご覧ください。

UTF-8	FFFTPやFileZilla 3.2.8などUTF-8対応のFTPクライアントソフトを利用する場合に設定します。ファイル名、フォルダー名に日本語が使用できます。
Shift-JIS	コマンドプロンプトのFTPコマンドなどShift-JIS対応のFTPクライアントソフト利用の場合に設定します。ファイル名、フォルダー名に一部の日本語が使用できない場合があります。※

※Shift-JISエンコード設定の場合、以下の文字は使用しないようにしてください。

炳倅同哇翫嶠懷晒葉榆洵煨琯皖淨墓間都銑銷鏽飼鷄 I
 倍伺冷咏禽律憚昂柰櫟森煜瑋益靖茹誦郎鉅釧鑠飯鶴
 葩恍宜叱萌崎愠昉杓操虎煮肆嗽鵒成詹違鉀鋹鎡顛鵬 ∴
 銈佞燼夔參嵩惕昂朗櫪清亟珣晶竝芋諄逸鈺鈺鏹顛鵬 i Tel
 鐸秘允坂爰松愀昕聆舞湊炫玼皁禎茁訥返鈇鋒鏘璜鰲 No.
 襲但做屢撫屹慙昀曹橫淦吳珉臨福羽襄軋鈴鏐鎖青鯨 x 侏
 續仔閭匡增岑悅敦噶槽泣瀾均皂禔羨螻赴鈆銕錕霸鮭 ix 一
 U 公儂邵塚立劫擎暄褶活瀟獮駿祥躡牲赶鈇鍋錦霸鮭 viii X
 O 任偷匡塔寮恣搗嵩渠涇滢猪瓶神繒穉賢鈇銀鍍霍鮪 vii IX
 ∴ 伋匱勾埔寬德摠暗榷回濱狹環礼緒葉賴鈇鉸鏐靈魴 vi VIII
 Z 一僭勻埃眞或鍵哲楨泚漸狄璉礪綠蔭瞻釘鉸鏐露鬬 v VII
 上彈掠勛堪甯弭柄晴栢泓澈執瓖礫綽董譚鈇銑鎬騰高 iv VI
 J 昇僂劬坦案亞或唆得沆澌壽琮硤絜蕙諶釧鋤鋳鴈麟 iii V
 S 銀捷荔莖孖靚愜吟枕汜漢燁瑁砌紮藝謀鈇鉸鏐鋳鴈醇 ii IV
 ≡ 精俠加詰妹嶠悒皖柳汎涕熙琪砭精蒨諸鄧鉅鑿隆館 i III
 三昱俚荔哥好嶠愷吟披步湜輝琦劬箬菓謔鄉釵鉸鉤閒饒黑 II

一括登録をする

※その他の内容については、本体の【画面で見るマニュアル】をご確認ください。

●設定書式カスタマイズ

・共有フォルダー設定項目定義

▼フィールド名と設定項目の対応

Ftp	FTP共有	1->有効,0->無効,空->無効/無効
-----	-------	----------------------

●CSVファイルの記述例

▼ケース1

共有フォルダー追加	Share1を追加	FTP共有が有効 MSネットワーク共有が有効 読み取り専用が無効
-----------	-----------	--

上記設定内容のCSV ファイル

addshare,Share1,コメント,,,,,1,,,1,,,,,0

▼ケース2

共有フォルダー追加	Share2を追加	FTP共有が有効 MSネットワーク共有が有効 読み取り専用が無効
-----------	-----------	--

上記設定内容のCSV ファイル

#share_config,Name,Comment,Ftp,Win,ReadOnly

addshare,Share2,コメント,1,1,0

CSV一括登録で「設定が不正です。」と表示される場合

設定値として以下の例のような不正な値が設定されています。CSVファイルを修正してください。

例1：使用量制限を0.1以上、かつFTP共有を有効で設定している。

例2：ゲストユーザー禁止を有効、かつFTP共有を有効で設定している。

Amazon S3と同期する

[Amazon S3同期について](#)

[Amazon S3の設定を確認する](#)

[Amazon S3との同期を有効にする](#)

[任意のタイミングでダウンロードする場合](#)

Amazon S3同期について

本製品の共有フォルダーとAmazonが運営するインターネット用の有償ストレージサービスAmazon S3のバケットを同期させることができます。

Amazon S3に関する詳細は、<http://aws.amazon.com/jp/s3/>をご覧ください。

同期動作は本製品からAmazon S3へのアップロードと、Amazon S3から本製品へのダウンロードに分けられ、アップロードは1分ごとに、ダウンロードは設定した時間ごとにおこなわれます。

※本機能をご利用いただくには、本製品がインターネット環境に接続されている必要があります。

※実際にアップロードが開始されるのは、フォルダー内のファイルが更新されなくなってから約2分後になります。

※本製品のAmazon S3連携機能は、署名バージョン2のみに対応しています。一部の署名バージョン4を必要とするリージョンには対応しておりません。

ご注意

- 1つの共有フォルダーには、各クラウドサービスのうち1つを有効に設定できます。同時に複数では設定できません。
- 本機能を有効にした共有フォルダー内のファイルを直接編集しないでください。
※編集中に一時ファイルを作るソフトで編集している場合、その一時ファイルまでアップロードされます。
- 同期する前に本製品の時刻設定をNTP同期有効(毎日同期有効)に設定してください。時刻がずれると正常に同期できなくなります。
- USB HDDは、専用フォーマットで共有モードの場合のみ同期が実行されます。
- Amazon S3のGlacierストレージクラスには対応しておりません。
- Amazon S3は保存容量・通信量に応じて課金されます。頻繁に更新されるデータがある場合、請求額が大きくなる場合があります。Amazon S3ご契約サイトなどで料金を確認しながら運用することをおすすめします。
- 同期の通信において、プロキシ設定が必要な場合は、あらかじめプロキシ設定をしてください。方法は、本体の【画面で見るマニュアル】をご覧ください。
- 共有フォルダーの設定変更・削除をする場合は、本製品を利用しているユーザーがいらないことを確認してから、作業することをおすすめします。共有フォルダーの設定変更・削除をすると、その内容が反映されるまで、すべての共有フォルダーにアクセスできなくなります。特に、共有フォルダー内のファイル数が多く、使用量制限がかかっている場合に、内容反映の時間がかかります。
- USB HDDの共有フォルダーを同期する場合、その共有フォルダーのトップに"__tmp_file_for_Copy_..." という名前のファイルが一時的に作成される場合があります。そのファイルを削除や変更しないでください。同期処理に必要です。

Amazon S3の設定を確認する

事前に、<http://aws.amazon.com/jp/s3/>にアクセスし、AWSアカウントを作成してください。

アカウント作成後、そのアカウントにてバケットおよびアクセスキーを作成し、以下をメモしてください。

- ・バケット名
- ・作成したアカウントのアクセスキーID
- ・シークレットキー

※バケット名は、3文字以上63文字以内で作成してください。

※アクセスキーは、「セキュリティ証明書」または「Security Credentials」から作成します。

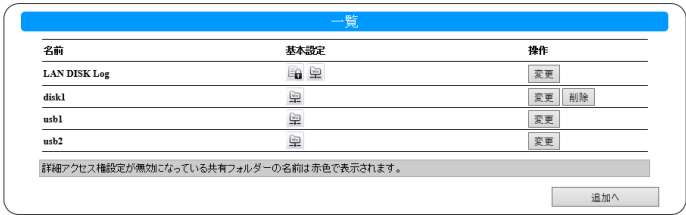
※アクセスキーID とシークレットキーについては、そのアカウントでのAWS サインアップ後、Amazon S3ホームページ画面右上の「アカウ

ント/コンソール] の [セキュリティ証明書] を開いた先の [アクセス証明書] の [アクセスキー] タブをご参照ください。
※Amazon S3についての不明点、通信料金、規約については、Amazon S3のホームページにてご確認ください。

Amazon S3との同期を有効にする

あらかじめ作成済みの共有フォルダーを同期する設定を説明します。共有フォルダーの作成方法は、本体の【画面で見るマニュアル】をご覧ください。

- 1. [共有] → [フォルダー] → [一覧] をクリック
- 2. 変更する共有フォルダーの [変更] をクリック



3. ① [基本設定] の [Amazon S3同期] にチェック
※リンクをクリックすると、Amazon S3に関する現在の利用料金などの契約情報が確認できます。
②契約情報を入力する

変更

名前

share

コメント

☐ 読み取り専用

☐ 非登録ユーザーからのアクセスを拒否

☒ Amazon S3 同期

Amazon S3にアクセスしてアカウントやバケットの作成、使用料金の確認を行います。

アクセスキー

シークレットキー

バケット名

プロトコル

☐ http

☒ https

ストレージクラス

☒ STANDARD

☐ RRS

クラウド側更新監視間隔

1時間

基本設定

詳細設定

エンドポイント

ポート

アップロード最大ファイルサイズ

10240

MB

☒ Multipart Upload

アクセスキー	作成した [アクセスキー] を入力します。
シークレットキー	作成した [シークレットアクセスキー] を入力します。
バケット名	作成した [バケット名] を入力します。
プロトコル	Amazon S3との通信プロトコルを選びます。 [https] を選んだ場合、本製品とAmazon S3間の通信は暗号化されます。 ※ [http] を選び、かつ本製品のプロキシ設定を利用する場合、使用するプロキシサーバーの機能によっては同期に失敗することがあります。その場合は、[https] をお試しください。
ストレージクラス	Amazon S3のバケットに保存するファイルのストレージクラスを選びます。 ※ストレージクラスについてはAmazon S3のホームページをご確認ください。
クラウド側更新監視間隔	Amazon S3のバケットのファイルの更新監視間隔を選びます。 ※ [更新監視しない] を設定した場合は、自動での定期ダウンロードはおこなわれません。

▼詳細設定

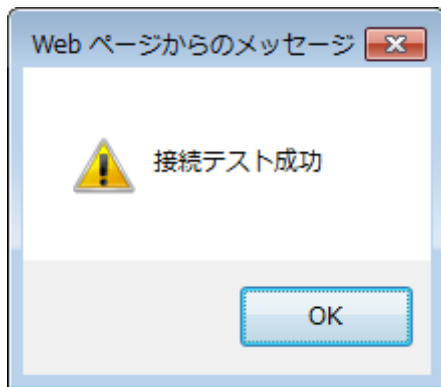
エンドポイント	エンドポイント名（ホスト名）を直接入力する場合に設定します。 ※空白の場合は、Amazon S3のエンドポイントが利用されます。
ポート番号	Amazon S3にアクセスする際のポート番号（TCP）を入力します。 ※空白の場合は、プロトコルで [http] を選ぶと80、[https] を選ぶと443を使います。
アップロード最大ファイルサイズ	ファイルをアップロードする際の最大ファイルサイズを入力します。これを超えるファイルはアップロードされません。 ※Mバイト単位で設定します。 [最大5242880MB（5TB）]
Multipart Upload	Multipart Uploadを使うかどうかを選びます。 ※ただし、100MB未満のファイルをアップロードする際は、SinglePart Uploadを使います。 ※チェックしない場合、5GB以上のファイルはアップロードできません。

4. [接続テスト] をクリック
しばらく後に「接続テスト成功」と出ることを確認します。

☒ Multipart Upload

接続テスト開始

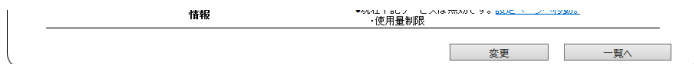
5. [OK] をクリック



接続テストに失敗した場合

- 入力した契約情報がすべて正しいか確認してください。（特に、エンドポイントやポート番号を初期値から変更している場合は、ご注意ください。）
- 本製品がインターネットに接続可能な環境に設置されているか、確認してください。（本製品のプロキシ設定を有効にしている場合、プロキシ設定が正しいかも確認してください。）

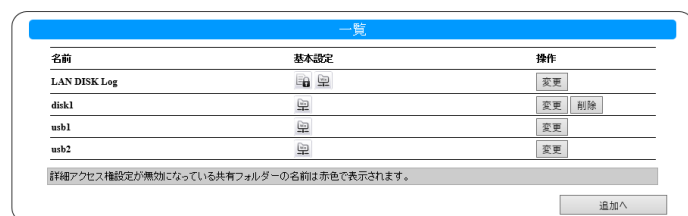
6. 接続テストに成功したら、[変更] をクリック



任意のタイミングでダウンロードする場合

1. [共有] → [フォルダー] → [一覧] をクリック

2. 変更する共有フォルダーの [変更] をクリック



3. [ダウンロード開始] をクリック



結果を確認する

本製品のログ記録用の共有フォルダー「LAN DISK Log」の「Amazon S3」フォルダー以下に同期の結果を記録を残します。

「[同期実行日時]_summary.log」というファイル名のログファイルで内容を確認してください。

失敗した場合は「[同期実行日時]_failed.log」というファイル名のログファイルで、内容を確認してください。

成功した場合は「[同期実行日時].log」というファイル名のログファイルも保存されます。また、同期中に本機能の設定を追加や変更した場合や本製品を再起動した場合など、同期処理が中断された場合「[同期実行日時]_stopped.log」という名前のログファイルが保存されます。

「[同期実行日時].log」および「[同期実行日時]_stopped.log」というファイル名のログファイルはあわせて最大10 個まで保存されま

す。それ以上のログファイルが保存される場合は、その中で最も古い実行日時のファイルが同じ実行日時の「[[同期実行日時]_summary.log]」と一緒に自動的に削除されます。

なお、「[[同期実行日時]_failed.log]」は自動的に削除されませんので必要に応じて削除してください。

(共有フォルダー「LAN DISK Log」へのアクセス方法は本体の【画面で見るマニュアル】をご覧ください。)

▼詳細設定

ログ内容	意味	対処
SizeTooLargeError	アップロードのファイルサイズの上限を超えています。	該当するファイルをアップロード元の共有フォルダーから別の場所に移動してください。
NoSpaceError	ローカルの共有フォルダーまたはサーバーのファイル・フォルダー数またはファイルの合計サイズが制限値を超えています。	制限値を超えているファイル・フォルダーの移動または削除が必要です。
NoEntryError	フォルダーやファイルが見つかりません。	同期中に設定やファイル・フォルダーを変更しないようにしてください。
PermissionError	サーバー側に権限がないためファイル操作ができませんでした。	サーバー側の権限設定を確認してください。
ExistsError	以下のうちいずれかに該当します。 ・アップロード元にあるファイルと同名のフォルダーがアップロード先のサーバーに存在します。 ・アップロード元にあるフォルダーと同名のファイルがアップロード先のサーバーに存在します。 ・ダウンロード元にあるファイルと同名のフォルダーがダウンロード先のサーバーに存在します。 ・ダウンロード元にあるフォルダーと同名のファイルがダウンロード先のサーバーに存在します。	同名のファイル、フォルダーのうち片方の名称を変更してください。
NameTooLongError	ファイル名の長さが制限値を超えています。	該当するファイルの名称を変更してください。
ServerCommunicationError	サーバーへの同時接続数が多すぎるか、BOX IDもしくはパスワードの設定が間違っています。	BOX IDもしくはパスワードに誤りがないか確認してください。BOX IDもしくはパスワードに誤りがない場合、本機以外に同じBOX IDでサーバーに接続している機器が存在するなら接続台数を減らすことを検討してください。
ForbiddenNameError	ファイル名が不正です。	該当するファイルの名称を変更してください。

Microsoft Azureと同期する

[Microsoft Azure同期について](#)

[Microsoft Azureの設定を確認する](#)

[Microsoft Azureとの同期を有効にする](#)

[任意のタイミングでダウンロードする場合](#)

Microsoft Azure同期について

本製品の共有フォルダーと、Microsoftが運営するインターネット用の有償ストレージサービスAzure Blob Storage (<http://azure.microsoft.com/>) のコンテナを同期させることができます。

同期動作は本製品からAzureへのアップロードと、Azure から本製品へのダウンロードに分けられ、アップロードは1分ごとに、ダウンロードは設定した時間ごとにおこなわれます。

※本機能をご利用いただくには、本製品がインターネット環境に接続されている必要があります。

※実際にアップロードが開始されるのは、フォルダー内のファイルが更新されなくなってから約2分後になります。

ご注意

- 1つの共有フォルダーには、各クラウドサービスのうち1つを有効に設定できます。同時に複数設定できません。
- 本機能を有効にした共有フォルダー内のファイルを直接編集しないでください。
※編集中に一時ファイルを作るソフトで編集している場合、その一時ファイルまでアップロードされます。
- 同期する前に本製品の時刻設定をNTP同期有効(毎日同期有効)に設定してください。時刻がずれると正常に同期できなくなります。
- アップロード可能なファイルは、1ファイル200GBまでです。
- USB HDDは、専用フォーマットで共有モードの場合のみ同期が実行されます。
- Azure上のBlobはブロックBlobのみが同期対象となり、ページBlobは同期対象外となります。
- Microsoft AzureのBlob Storageは保存容量・通信量に応じて課金されます。頻繁に更新されるデータがある場合、請求額が大きくなる場合があります。Microsoft Azureご契約サイトなどで料金を確認しながら運用することをおすすめします。
- 同期の通信において、プロキシ設定が必要な場合は、あらかじめプロキシ設定をしてください。方法は、本体の【画面で見るマニュアル】をご覧ください。
- USB HDDの共有フォルダーを同期する場合、その共有フォルダーのトップに"__tmp_file_for_Copy_..." という名前のファイルが一時的に作成される場合があります。そのファイルを削除や変更しないでください。同期処理に必要です。
- 共有フォルダーの設定変更・削除をする場合は、本製品を利用しているユーザーがいらないことを確認してから、作業することをおすすめします。共有フォルダーの設定変更・削除をすると、その内容が反映されるまで、すべての共有フォルダーにアクセスできなくなります。特に、共有フォルダー内のファイル数が多く、使用量制限がかかっている場合に、内容反映の時間がかかります。
- 共有フォルダー内にある空のフォルダーは、同期の対象となりません。

Microsoft Azureの設定を確認する

事前にAzure Blob Storage (<http://azure.microsoft.com/>) にアクセスし、Microsoftアカウントを作成してください。アカウント作成後、そのアカウントにてさらにストレージアカウントやコンテナを作成、およびプライマリアクセスキーを確認し、以下をメモしてください。

- ・コンテナ名
- ・ストレージアカウント名
- ・作成したストレージアカウントのプライマリアクセスキー

※ストレージアカウントは、Microsoftアカウントでサインイン後、Microsoft Azureホームページ画面左下の「新規」の「データサービス」の「ストレージ」の「簡易作成」から作成します。

※コンテナは、上記で作成したストレージアカウントをクリックし、Microsoft Azureホームページ画面上の「コンテナ」の「追加」から作成します。

※プライマリアクセスキーは、上記で作成したストレージアカウントをクリックし、Microsoft Azure ホームページ画面下の「アクセスキーの

管理」から確認します。

※ Microsoft Azureについての不明点、通信料金、規約については、Microsoft Azureのホームページにてご確認ください。

Microsoft Azureとの同期を有効にする

あらかじめ作成済みの共有フォルダーを同期する設定を説明します。共有フォルダーの作成方法は、【画面で見るマニュアル】をご覧ください。

- 1. [共有] → [フォルダー] → [一覧] をクリック
- 2. 変更する共有フォルダーの [変更] をクリック

一覧

名前	基本設定	操作
LAN DISK Log		<button>変更</button>
disk1		<button>変更</button> <button>削除</button>
usb1		<button>変更</button>
usb2		<button>変更</button>

詳細アクセス権設定が無効になっている共有フォルダーの名前は赤色で表示されます。

追加へ

- 3. ① [基本設定] の [Microsoft Azure同期] にチェック
※リンクをクリックすると、Microsoft Azureに関する現在の利用料金などの契約情報が確認できます。
- ②契約情報を入力する

変更

名前

share

コメント

☐ 読み取り専用

☐ 非登録ユーザーからのアクセスを拒否

☐ Amazon S3 同期

☒ Microsoft Azure 同期

Microsoft Azureにアクセスしてアカウントやコンテナの作成、使用料金の確認を行います。

アカウント名

アクセスキー

コンテナ名

プロトコル

☐ http ☒ https

クラウド側更新監視間隔

1時間

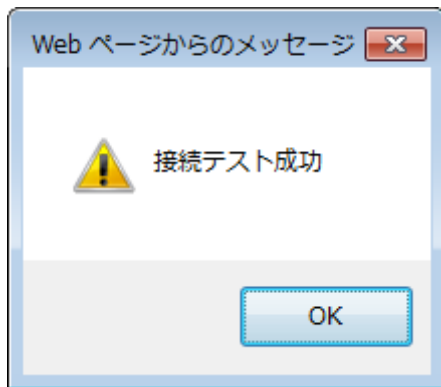
アカウント名	作成したストレージアカウント名を入力します。
アクセスキー	確認したアクセスキーを入力します。
コンテナ名	作成したコンテナ名を入力します。
プロトコル	Microsoft Azureとの通信プロトコルを選びます。 [https]を選んだ場合、本製品とMicrosoft Azure間の通信は暗号化されます。 ※ [http] を選び、かつ本製品のプロキシ設定を利用する場合、使用するプロキシサーバーの設定が必要です。HTTPのCONNECTメソッドでのトンネル通信で、許可するポートにhttp（ポート80番）を追加してください。
クラウド側更新監視間隔	Microsoft Azureのコンテナのファイルの更新監視間隔を選びます。 ※ [更新監視しない] を設定した場合は、自動での定期ダウンロードはおこなわれません。

- 4. [接続テスト] をクリック
しばらく後に「接続テスト成功」と出ることを確認します。

接続テスト

接続テスト開始

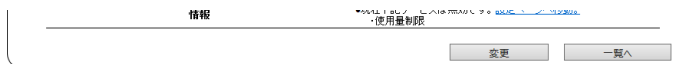
5. [OK]をクリック



接続テストに失敗した場合

- 入力した契約情報がすべて正しいか確認してください。（特に、エンドポイントやポート番号を初期値から変更している場合は、ご注意ください。）
- 本製品がインターネットに接続可能な環境に設置されているか、確認してください。（本製品のプロキシ設定を有効にしている場合、プロキシ設定が正しいかも確認してください。）

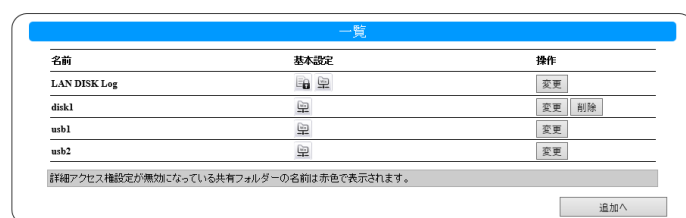
6. 接続テストに成功したら、[変更] をクリック



任意のタイミングでダウンロードする場合

1. [共有] → [フォルダー] → [一覧] をクリック

2. 変更する共有フォルダーの [変更] をクリック



3. [ダウンロード開始] をクリック



結果を確認する

本製品のログ記録用の共有フォルダー「LAN DISK Log」の「Microsoft Azure」フォルダー以下に同期の結果を記録を残します。

「[同期実行日時]_summary.log」というファイル名のログファイルで内容を確認してください。

失敗した場合は「[同期実行日時]_failed.log」というファイル名のログファイルで、内容を確認してください。

成功した場合は「[同期実行日時].log」というファイル名のログファイルも保存されます。また、同期中に本機能の設定を追加や変更した場合や本製品を再起動した場合など、同期処理が中断された場合「[同期実行日時]_stopped.log」という名前のログファイルが保存されます。

「[同期実行日時].log」および「[同期実行日時]_stopped.log」というファイル名のログファイルはあわせて最大10個まで保存されま

す。それ以上のログファイルが保存される場合は、その中で最も古い実行日時のファイルが同じ実行日時の「[[同期実行日時]_summary.log]」と一緒に自動的に削除されます。

なお、「[[同期実行日時]_failed.log]」は自動的に削除されませんので必要に応じて削除してください。（共有フォルダー「LAN DISK Log」へのアクセス方法は本製品の【画面で見るマニュアル】をご覧ください。）

▼詳細設定

ログ内容	意味	対処
SizeTooLargeError	アップロードのファイルサイズの上限を超えています。	該当するファイルをアップロード元の共有フォルダーから別の場所に移動してください。
NoSpaceError	ローカルの共有フォルダーまたはサーバーのファイル・フォルダー数またはファイルの合計サイズが制限値を超えています。	制限値を超えているファイル・フォルダーの移動または削除が必要です。
NoEntryError	フォルダーやファイルが見つかりません。	同期中に設定やファイル・フォルダーを変更しないようにしてください。
PermissionError	サーバー側に権限がないためファイル操作ができませんでした。	サーバー側の権限設定を確認してください。
ExistsError	以下のうちいずれかに該当します。 ・アップロード元にあるファイルと同名のフォルダーがアップロード先のサーバーに存在します。 ・アップロード元にあるフォルダーと同名のファイルがアップロード先のサーバーに存在します。 ・ダウンロード元にあるファイルと同名のフォルダーがダウンロード先のサーバーに存在します。 ・ダウンロード元にあるフォルダーと同名のファイルがダウンロード先のサーバーに存在します。	同名のファイル、フォルダーのうち片方の名称を変更してください。
NameTooLongError	ファイル名の長さが制限値を超えています。	該当するファイルの名称を変更してください。
ServerCommunicationError	サーバーへの同時接続数が多すぎるか、BOX IDもしくはパスワードの設定が間違っています。	BOX IDもしくはパスワードに誤りがないか確認してください。BOX IDもしくはパスワードに誤りがない場合、本機以外に同じBOX IDでサーバーに接続している機器が存在するなら接続台数を減らすことを検討してください。
ForbiddenNameError	ファイル名が不正です。	該当するファイルの名称を変更してください。

Boxと同期する

Box同期について

Boxとの同期を有効にする

任意のタイミングでダウンロードする場合

Box同期について

本製品の共有フォルダーと、Box社が運営する法人向けクラウドストレージサービスBox (https://www.box.com/ja_JP/front/) を同期させることができます。

同期動作は本製品からBox へのアップロードと、Box から本製品へのダウンロードに分けられ、アップロードは1分ごとに、ダウンロードは設定した時間ごとにおこなわれます。

※本機能をご利用いただくには、本製品がインターネット環境に接続されている必要があります。

※実際に同期が開始されるのは、フォルダー内のファイルが更新されなくなってから約2分後になります。

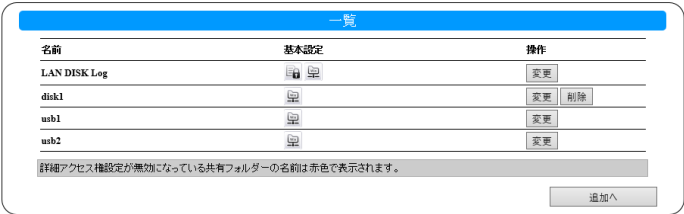
ご注意

- 1つの共有フォルダーには、各クラウドサービスのうち1つを有効に設定できます。同時に複数設定できません。
 - 同期する前に本製品の時刻設定をNTP 同期有効に設定してください。時刻がずれると正常に同期できなくなります。
 - 本機能を有効にした共有フォルダー内のファイルを直接編集しないでください。
- ※編集中に一時ファイルを作るソフトで編集している場合、その一時ファイルまでアップロードされます。
- USB HDDは、専用フォーマットで共有モードの場合のみ同期が実行されます。
 - アップロード可能なファイルは1 ファイルのサイズや使用可能容量は契約によって異なります。
(フリーアカウントはアップロード可能な1 ファイルのサイズは250MB、使用可能容量は10GB)
 - 同期の通信において、プロキシ設定が必要な場合は、あらかじめプロキシ設定をしてください。方法は、本体の【画面で見るマニュアル】をご覧ください。
 - 共有フォルダーの設定変更・削除をする場合は、本製品を利用しているユーザーがいらないことを確認してから、作業することをおすすめします。共有フォルダーの設定変更・削除をすると、その内容が反映されるまで、すべての共有フォルダーにアクセスできなくなります。特に、共有フォルダー内のファイル数が多く、使用量制限がかかっている場合に、内容反映の時間がかかります。
 - USB HDDの共有フォルダーを同期する場合、その共有フォルダーのトップに"__tmp_file_for_Copy_..." という名前のファイルが一時的に作成される場合があります。そのファイルを削除や変更しないでください。同期処理に必要です。

Boxとの同期を有効にする

あらかじめ作成済みの共有フォルダーを同期する設定を説明します。共有フォルダーの作成方法は、【画面で見るマニュアル】をご覧ください。

1. [共有] → [フォルダー] → [一覧] をクリック
2. 変更する共有フォルダーの[変更]をクリック



3. ① [基本設定] の [Box同期] にチェック
② 契約情報を入力する

変更

名前

boxshare

コメント

☐ 読み取り専用

☐ 非登録ユーザーからのアクセスを拒否

☐ Amazon S3 同期

☐ Microsoft Azure 同期

☒ Box 同期

メールアドレス

パスワード

アップロード最大ファイルサイズ

MB

クラウド側更新監視間隔

更新監視しない

接続テスト開始

ダウンロード開始

☐ Clouda 同期

☐ Dropbox 同期

☒ Microsoftネットワーク共有

☐ ごみ箱

☐ 隠し

使用量制限値

0

GB

(小数点第一位で入力してください)

詳細なアクセス権

☒ 有効 ☐ 無効

禁止ユーザー

読み取りユーザー

メールアドレス	Boxに登録したメールアドレスを入力します。
パスワード	Boxに登録したパスワードを入力します。
アップロード最大ファイルサイズ	Boxサーバーへのアップロードをおこなう最大サイズを入力します。（初期設定値は「250」、「0」は制限なし）
クラウド側更新監視間隔	Boxのコンテナのファイルの更新監視間隔を選びます。 ※ [更新監視しない] を設定した場合は、自動での定期ダウンロードはおこなわれません。

※Box同期を有効に設定すると、入力されたメールアドレス/パスワードによりサーバーと通信がおこなわれ、アプリケーション"nasdsync" によるアクセスが自動で許可されます。

4. [接続テスト開始] をクリック
しばらく後に「接続テスト成功」と表示されることを確認します。

更新監視しない

接続テスト開始

ダウンロード開始

☐ Clouda 同期

5. [OK]をクリック

接続テストに失敗した場合

- 入力した契約情報がすべて正しいか確認してください。
- 本製品がインターネットに接続可能な環境に設置されているか、確認してください。（本製品のプロキシ設定を有効にしている場合、プロキシ設定が正しいかも確認してください。）
- パスワード間違いで何度か失敗した場合、ログイン認証情報が無効になった可能性があります。Boxのホームページからサインインし、「ログイン認証情報が無効です」と表示されたら、画面の指示にしたがってサインインを完了させてください。

6. 接続テストに成功したら、[変更] をクリック

情報

▼共有フォルダの共有設定を参照してください。使用量制限

変更

一覧へ

任意のタイミングでダウンロードする場合

1. [共有] → [フォルダー] → [一覧] をクリック
2. 変更する共有フォルダーの[変更]をクリック

一覧

名前	基本設定	操作
LAN DISK Log		変更
disk1		変更 削除
usb1		変更
usb2		変更

詳細アクセス権設定が無効になっている共有フォルダーの名前は赤色で表示されます。

追加へ

3. [ダウンロード開始] をクリック

1時間

▼

接続テスト開始

ダウンロード開始

結果を確認する

本製品のログ記録用の共有フォルダー「LAN DISK Log」の「Box」フォルダー以下に同期の結果を記録を残します。

「[同期実行日時]_summary.log」というファイル名のログファイルで内容を確認してください。

失敗した場合は「[同期実行日時]_failed.log」というファイル名のログファイルで、内容を確認してください。

成功した場合は「[同期実行日時].log」というファイル名のログファイルも保存されます。また、同期中に本機能の設定を追加や変更した場合や本製品を再起動した場合など、同期処理が中断された場合「[同期実行日時]_stopped.log」という名前のログファイルが保存されます。

「[同期実行日時].log」および「[同期実行日時]_stopped.log」というファイル名のログファイルはあわせて最大10 個まで保存されます。それ以上のログファイルが保存される場合は、その中で最も古い実行日時のファイルが同じ実行日時の「[同期実行日時]_summary.log」と一緒に自動的に削除されます。

なお、「[同期実行日時]_failed.log」は自動的に削除されませんので必要に応じて削除してください。

(共有フォルダー「LAN DISK Log」へのアクセス方法は本製品の【画面で見るマニュアル】をご覧ください。)

▼詳細設定

ログ内容	意味	対処
SizeTooLargeError	アップロードのファイルサイズの上限を超えています。	該当するファイルをアップロード元の共有フォルダーから別の場所に移動してください。
NoSpaceError	ローカルの共有フォルダーまたはサーバーのファイル・フォルダー数またはファイルの合計サイズが制限値を超えています。	制限値を超えているファイル・フォルダーの移動または削除が必要です。
NoEntryError	フォルダーやファイルが見つかりません。	同期中に設定やファイル・フォルダーを変更しないようにしてください。
PermissionError	サーバー側に権限がないためファイル操作ができませんでした。	サーバー側の権限設定を確認してください。

ror		
Exists Error	以下のうちいずれかに該当します。 ・アップロード元にあるファイルと同名のフォルダーがアップロード先のサーバーに存在します。 ・アップロード元にあるフォルダーと同名のファイルがアップロード先のサーバーに存在します。 ・ダウンロード元にあるファイルと同名のフォルダーがダウンロード先のサーバーに存在します。 ・ダウンロード元にあるフォルダーと同名のファイルがダウンロード先のサーバーに存在します。	同名のファイル、フォルダーのうち片方の名称を変更してください。
NameTooLongError	ファイル名の長さが制限値を超えています。	該当するファイルの名称を変更してください。
ServerCommunicationError	サーバーへの同時接続数が多すぎるか、BOX IDもしくはパスワードの設定が間違っています。	BOX IDもしくはパスワードに誤りがないか確認してください。BOX IDもしくはパスワードに誤りがない場合、本機以外に同じBOX IDでサーバーに接続している機器が存在するなら接続台数を減らすことを検討してください。
ForbiddenNameError	ファイル名が不正です。	該当するファイルの名称を変更してください。

Cloudⁿ と同期する

[Cloudⁿ 同期について](#)

[Cloudⁿ の設定を確認する](#)

[Cloudⁿ との同期を有効にする](#)

[任意のタイミングでダウンロードする場合](#)

Cloudⁿ 同期について

本製品の共有フォルダーと、NTTコミュニケーションズが運営するパブリッククラウドサービスCloudⁿ (<https://www.ntt.com/cloudn/>)のObject Storageのバケットを同期させることができます。

同期動作は本製品から Cloudn へのアップロードと、Cloudn から本製品へのダウンロードに分けられ、アップロードは1 分ごとに、ダウンロードは設定した時間ごとにおこなわれます。

※本機能をご利用いただくには、本製品がインターネット環境に接続されている必要があります。

※実際にアップロードが開始されるのは、フォルダー内のファイルが更新されなくなってから約2 分後になります。

ご注意

- 1つの共有フォルダーには、各クラウドサービスのうち1つを有効に設定できます。同時に複数設定できません。
- 本機能を有効にした共有フォルダー内のファイルを直接編集しないでください。
※編集中に一時ファイルを作るソフトで編集している場合、その一時ファイルまでアップロードされます。
- 同期する前に本製品の時刻設定をNTP 同期有効(毎日同期有効)に設定してください。時刻がずれると正常に同期できなくなります。
- USB HDDは、専用フォーマットで共有モードの場合のみ同期が実行されます。
- Cloudⁿ のObject Storageは保存容量に応じて課金されます。Cloudⁿ ご契約サイトなどで料金を確認しながら運用することをおすすめします。
- 同期の通信において、プロキシ設定が必要な場合は、あらかじめプロキシ設定をしてください。方法は、本体の【画面で見るマニュアル】をご覧ください。
- USB HDDの共有フォルダーを同期する場合、その共有フォルダーのトップに"__tmp_file_for_Copy_..." という名前のファイルが一時的に作成される場合があります。そのファイルを削除や変更しないでください。同期処理に必要です。
- 共有フォルダーの設定変更・削除をする場合は、本製品を利用しているユーザーがいらないことを確認してから、作業することをおすすめします。共有フォルダーの設定変更・削除をすると、その内容が反映されるまで、すべての共有フォルダーにアクセスできなくなります。特に、共有フォルダー内のファイル数が多く、使用量制限がかかっている場合に、内容反映の時間がかかります。

Cloudⁿ の設定を確認する

事前に、Cloudⁿ (<https://www.ntt.com/cloudn/>) にアクセスし、アカウントを作成してください。

アカウント作成後、そのアカウントにてバケットおよびアクセスキーを作成し、バケット名とそのアカウントのアクセスキーID とシークレットアクセスキーをメモしてください。

※アクセスキーID とシークレットキー（秘密鍵）については、そのアカウントでのログイン後、Cloudⁿ ホームページ画面右上の［ようこそ（アカウント名）さん］右側の▼から［APIアクセスキー・秘密鍵管理］を開いた先の［Query API］をご参照ください。

※Cloudⁿ についての不明点、通信料金、規約については、Cloudⁿ のホームページにてご確認ください。

Cloudⁿ との同期を有効にする

あらかじめ作成済みの共有フォルダーを同期する設定を説明します。共有フォルダーの作成方法は、【画面で見るマニュアル】をご覧ください。

- 1. [共有] → [フォルダー] → [一覧] をクリック
- 2. 変更する共有フォルダーの[変更] をクリック

一覧

名前	基本設定	操作
LAN DISK Log	 	<button>変更</button>
disk1		<button>変更</button> <button>削除</button>
usb1		<button>変更</button>
usb2		<button>変更</button>

詳細アクセス権設定が無効になっている共有フォルダーの名称は赤色で表示されます。

追加へ

3. ① [基本設定] の [Cloudn同期] にチェック

※リンクをクリックすると、Microsoft Azureに関する現在の利用料金などの契約情報が確認できます。

②契約情報を入力する

変更

名前

share

コメント

☐ 読み取り専用

☐ 非登録ユーザーからのアクセスを拒否

☐ Amazon S3 同期

☐ Microsoft Azure 同期

☒ Cloudn 同期

アクセスキー

シークレットキー

バケット名

プロトコル

☐ http ☒ https

ストレージクラス

☒ STANDARD ☐ RRS

クラウド側更新監視間隔

1時間

詳細設定

エンドポイント

str.cloudn-service.com

ポート

アップロード最大ファイルサイズ

10240

MB

☒ Multipart Upload

基本設定

アクセスキー	作成した [アクセスキー] を入力します。
シークレットキー	作成した [シークレットアクセスキー] を入力します。
バケット名	作成した [バケット名] を入力します。
プロトコル	Cloud ⁿ との通信プロトコルを選びます。 [https] を選んだ場合、本製品とCloud ⁿ 間の通信は暗号化されます。 ※ [http] を選び、かつ本製品のプロキシ設定を利用する場合、使用するプロキシサーバーの機能によっては同期に失敗することがあります。その場合は、 [https] をお試しください。
ストレージクラス	設定しません。Cloud ⁿ のバケットに保存するファイルのストレージクラスを選びます。 ※この項目は、Cloud ⁿ との同期では使いません。
クラウド側更新監視間隔	Cloud ⁿ のバケットのファイルの更新監視間隔を選びます。 ※ [更新監視しない] を設定した場合は、自動での定期ダウンロードはおこなわれません。

▼詳細設定

エンドポイント	エンドポイント名（ホスト名）を直接入力する場合に設定します。 ※最初から「str.cloudn-service.com」が入力されています。
ポート番号	Cloud ⁿ にアクセスする際のポート番号（TCP）を入力します。 ※空白の場合は、プロトコルで [http] を選ぶと80、 [https] を選ぶと443を使います。
アップロード最大ファイルサイズ	ファイルをアップロードする際の最大ファイルサイズを入力します。これを超えるファイルはアップロードされません。 ※MB単位で設定します。 [最大5242880MB（5TB）]
Multipart Upload	Multipart Upload を使うかどうかを選びます。 ※ただし、100MB未満のファイルをアップロードする際は、SinglePart Upload を使います。 ※チェックしない場合、500MB以上のファイルはアップロードできません。

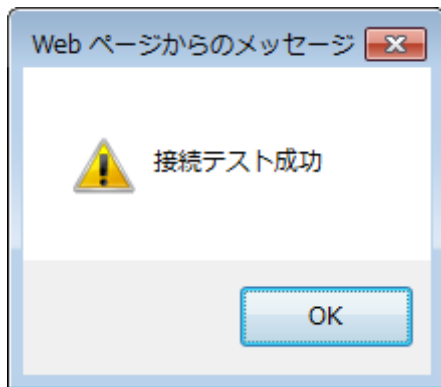
4. [接続テスト] をクリック

しばらく後に「接続テスト成功」と出ることを確認します。

▼

接続テスト開始

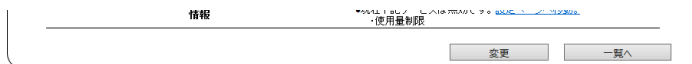
5. [OK] をクリック



接続テストに失敗した場合

- 入力した契約情報がすべて正しいか確認してください。（特に、エンドポイントやポート番号を初期値から変更している場合は、ご注意ください。）
- 本製品がインターネットに接続可能な環境に設置されているか、確認してください。（本製品のプロキシ設定を有効にしている場合、プロキシ設定が正しいかも確認してください。）

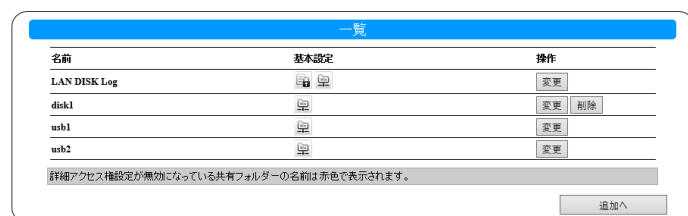
6. 接続テストに成功したら、[変更] をクリック



任意のタイミングでダウンロードする場合

1. [共有] → [フォルダー] → [一覧] をクリック

2. 変更する共有フォルダーの [変更] をクリック



3. [ダウンロード開始] をクリック



結果を確認する

本製品のログ記録用の共有フォルダー「LAN DISK Log」の「Cloudn」フォルダー以下に同期の結果を記録を残します。

「[同期実行日時]_summary.log」というファイル名のログファイルで内容を確認してください。

失敗した場合は「[同期実行日時]_failed.log」というファイル名のログファイルで、内容を確認してください。

成功した場合は「[同期実行日時].log」というファイル名のログファイルも保存されます。また、同期中に本機能の設定を追加や変更した場合や本製品を再起動した場合など、同期処理が中断された場合「[同期実行日時]_stopped.log」という名前のログファイルが保存されます。

「[同期実行日時].log」および「[同期実行日時]_stopped.log」というファイル名のログファイルはあわせて最大10個まで保存されま

す。それ以上のログファイルが保存される場合は、その中で最も古い実行日時のファイルが同じ実行日時の「[[同期実行日時]_summary.log]」と一緒に自動的に削除されます。

なお、「[[同期実行日時]_failed.log]」は自動的に削除されませんので必要に応じて削除してください。（共有フォルダー「LAN DISK Log」へのアクセス方法は本製品の【画面で見るマニュアル】をご覧ください。）

▼詳細設定

ログ内容	意味	対処
SizeTooLargeError	アップロードのファイルサイズの上限を超えています。	該当するファイルをアップロード元の共有フォルダーから別の場所に移動してください。
NoSpaceError	ローカルの共有フォルダーまたはサーバーのファイル・フォルダー数またはファイルの合計サイズが制限値を超えています。	制限値を超えているファイル・フォルダーの移動または削除が必要です。
NoEntryError	フォルダーやファイルが見つかりません。	同期中に設定やファイル・フォルダーを変更しないようにしてください。
PermissionError	サーバー側に権限がないためファイル操作ができませんでした。	サーバー側の権限設定を確認してください。
ExistsError	以下のうちいずれかに該当します。 ・アップロード元にあるファイルと同名のフォルダーがアップロード先のサーバーに存在します。 ・アップロード元にあるフォルダーと同名のファイルがアップロード先のサーバーに存在します。 ・ダウンロード元にあるファイルと同名のフォルダーがダウンロード先のサーバーに存在します。 ・ダウンロード元にあるフォルダーと同名のファイルがダウンロード先のサーバーに存在します。	同名のファイル、フォルダーのうち片方の名称を変更してください。
NameTooLongError	ファイル名の長さが制限値を超えています。	該当するファイルの名称を変更してください。
ServerCommunicationError	サーバーへの同時接続数が多すぎるか、BOX IDもしくはパスワードの設定が間違っています。	BOX IDもしくはパスワードに誤りがないか確認してください。BOX IDもしくはパスワードに誤りがない場合、本機以外に同じBOX IDでサーバーに接続している機器が存在するなら接続台数を減らすことを検討してください。
ForbiddenNameError	ファイル名が不正です。	該当するファイルの名称を変更してください。

Dropboxと同期する

[Dropbox同期について](#)

[Dropboxとの同期を有効にする](#)

Dropbox同期について

共有フォルダーとオンラインストレージサービスDropbox (<https://www.dropbox.com/>) 間でデータを同期させることができます。

※本機能をご利用いただくには、本製品がインターネット環境に接続されている必要があります。

※実際に同期が開始されるのは、同期対象共有フォルダー内のファイルが更新されなくなってから最短で約2分後となります。また、同期開始までの所要時間は、同期対象の共有フォルダー内のサブフォルダー数が多くなればなるほど長くなります。

Dropboxの同期に失敗する場合

本パッケージを最新版に更新してください。

ご注意

- 1つの共有フォルダーには、各クラウドサービスのうち1つを有効に設定できます。同時に複数は設定できません。
- 同期する前に本製品の時刻設定をNTP 同期有効に設定してください。時刻がずれると正常に同期できなくなります。
- 本機能を有効にした共有フォルダー内のファイルを直接編集しないでください。
※編集中に一時ファイルを作るソフトで編集している場合、その一時ファイルまでアップロードされます。
- USB HDDは、専用フォーマットで共有モードの場合のみ同期が実行されます。
- 本機能で使用する共有フォルダー、Dropboxアカウントのフォルダーにはどちらも、以下の制限があります。必ず制限範囲内でお使いください。1フォルダーの直下に置けるファイル・フォルダー数の合計は10000 まで
※Dropbox上の1フォルダーの直下に10000ファイルを配置すると、Dropboxのブラウザー版では開けない場合があります。
- 同期の通信において、プロキシ設定が必要な場合は、あらかじめプロキシ設定をしてください。方法は、本体の【画面で見るマニュアル】をご覧ください。
- 共有フォルダーの設定変更・削除をする場合は、本製品を利用しているユーザーがいないことを確認してから、作業することをおすすめします。共有フォルダーの設定変更・削除をすると、その内容が反映されるまで、すべての共有フォルダーにアクセスできなくなります。特に、共有フォルダー内のファイル数が多く、使用量制限がかかっている場合に、内容反映の時間がかかります。
- USB HDDの共有フォルダーを同期する場合、その共有フォルダーのトップに"__tmp_file_for_Copy..." という名前のファイルが一時的に作成される場合があります。そのファイルを削除や変更しないでください。同期処理に必要です。
- 複数の共有フォルダーを一つのDropboxフォルダー(アカウント) と同期させた場合、各共有フォルダー内のデータが互いに同期されます。共有フォルダーの使い分けをしている場合、各共有フォルダーごとに異なるDropbox フォルダー (アカウント) をご用意ください。
- ファイル・フォルダー名に特殊な文字を使用した場合、ファイル・フォルダー名が一部変更される場合があります。

Dropboxとの同期を有効にする

あらかじめ作成済みの共有フォルダーを同期する設定を説明します。共有フォルダーの作成方法は、【画面で見るマニュアル】をご覧ください。

1. [共有] → [フォルダー] → [一覧] をクリック

2. 変更する共有フォルダーの[変更]をクリック

名前	基本設定	操作
LAN DISK Log		変更
disk1		変更 削除
usb1		変更
usb2		変更

詳細アクセス権設定が無効になっている共有フォルダーの名前は赤色で表示されます。

追加へ

3. ① [Dropbox同期] にチェック

② リンクをクリック

名前: dbtest

コメント:

基本設定

- ☐ 読み取り専用
- ☐ 非登録ユーザーからのアクセスを拒否
- ☐ Amazon S3 同期
- ☐ Microsoft Azure 同期
- ☐ Box 同期
- ☐ Cloudn 同期
- ☒ **Dropbox 同期**
- ☐ アップロードのみ実行する
本共有フォルダーは I/O DATA Cloud Developer さんの Dropbox にアクセス可能です。
本共有フォルダーを別の Dropbox アカウントと同期する場合のみ、以下の手順を実行してください。
1. https://www.dropbox.com/oauth2/authorize?response_type=code&client_id=av49kj4ir28xk65 にアクセスし、nasdsync のアクセスを許可してください。
2. 表示されたコードを入力してください。

☒ Microsoft ネットワーク共有

【アップロードのみ実行する】について

チェックをつけると、サーバー上の更新検出がおこなわれなくなり、アップロードのみ実行されます。(ダウンロードはおこなわれません)

Dropbox上の更新検出をおこなわないことにより、LAN DISKのファイル更新時に、Dropbox上へアップロードされるまでの時間を短縮できます。

ただし、LAN DISKの起動直後や共有フォルダーの設定変更時など、Dropbox上のファイルの情報取得をおこないますので、このときはフォルダー・ファイル数に応じて同期に時間がかかる場合があります。

4. Dropboxログイン画面では、本製品と同期させたいアカウントでログインする

5. [許可] をクリック

nasdsync が Dropbox 内のファイル/フォルダへのアクセスをリクエストしています。
詳しくはこちら

キャンセル 許可

The screenshot shows the nadsync website interface. At the top left is a blue puzzle icon, and at the top right is a smiley face icon next to a progress bar. In the center, there is a large blue square containing a white puzzle piece icon. Below this, the text reads: "このプロセスを完了するには **nadsync** にこのコードを入力してください。" (To complete this process, please enter this code in **nadsync**.) Below the text is a text input field with a placeholder "nadsync-xxxx-xxxx-xxxx-xxxx" and a "コピー" (Copy) button to its right.

- 以下の手順を実行してください。

 - 以下のリンク先にアクセスしてください。
https://www.dropbox.com/oauth2?authorize?response_type=code&client_id=ad494d428ac655nasdevncのアカウントでログインしてください。
 - 表示されたコードを入力してください。**

☐ FTP共有
☒ Microsoftネットワーク共有

☐ ゴミ箱
 本機能を有効から無効にする場合、ゴミ箱用フォルダーが削除されます。
 ゴミ箱用フォルダーに大量のファイルが存在する場合、ゴミ箱用フォルダーの消滅に時間がかかります。

☐ 隠し
 使用量制限

☐ レプリケーション機能

詳細アクセス権

情報

 - 現在下記サービスは無効です。設定ページへ移動。
 - 使用量制限

変更 一覧へ

同期先の変更について

☒ Dropbox 同期

☐ アップロードのみ実行する

本共有フォルダーは [] さんのDropboxにアクセス可能です。

本共有フォルダーを別のDropboxアカウントと同期する場合のみ、以下の手順を実行してください。

1. 以下のリンク先にアクセスしてください。
https://www.dropbox.com/oauth2/authorize?response_type=code&client_id=av49kj4lr28xk65
2. 本共有フォルダーと同期させるDropboxアカウントでログインし、nasdsyncのアクセスを許可してください。
3. 表示されたコードを入力してください。

Dropbox同期の設定を無効にしても、本製品に保存されたアクセスのための情報は保存されたままとなり、次にDropbox同期を有効にした場合に、この保存された情報が利用されます。

この情報を破棄する場合は、「Dropboxのアクセス権を削除する」にチェックを付けて共有フォルダーの設定を変更してください。

結果を確認する

本製品のログ記録用の共有フォルダー「LAN DISK Log」の「Dropbox」フォルダー以下に同期の結果を記録を残します。

「[同期実行日時]_summary.log」というファイル名のログファイルで内容を確認してください。

失敗した場合は「[同期実行日時]_failed.log」というファイル名のログファイルで、内容を確認してください。

成功した場合は「[同期実行日時].log」というファイル名のログファイルも保存されます。また、同期中に本機能の設定を追加や変更した場合や本製品を再起動した場合など、同期処理が中断された場合「[同期実行日時]_stopped.log」という名前のログファイルが保存されます。

「[同期実行日時].log」および「[同期実行日時]_stopped.log」というファイル名のログファイルはあわせて最大10個まで保存されます。それ以上のログファイルが保存される場合は、その中で最も古い実行日時のファイルが同じ実行日時の「(同期実行日時)_summary.log」と一緒に自動的に削除されます。

なお、「[同期実行日時]_failed.log」は自動的に削除されませんので必要に応じて削除してください。（共有フォルダー「LAN DISK Log」へのアクセス方法は本製品の【画面で見るマニュアル】をご覧ください。）

▼詳細設定

SizeTooLargeError

意味

アップロードのファイルサイズの上限を超えています。

対処

該当するファイルをアップロード元の共有フォルダーから別の場所に移動してください。

NoSpaceError

意味

ローカルの共有フォルダーまたはサーバーのファイル・フォルダー数またはファイルの合計サイズが制限値を超えています。

対処

制限値を超えているファイル・フォルダーの移動または削除が必要です。

NoEntryError

意味

フォルダーやファイルが見つかりません。

対処

同期中に設定やファイル・フォルダーを変更しないようにしてください。

PermissionError

意味

サーバー側に権限がないためファイル操作ができませんでした。

対処

サーバー側の権限設定を確認してください。

ExistsError

意味

以下のうちいずれかに該当します。

- ・アップロード元にあるファイルと同名のフォルダーがアップロード先のサーバーに存在します。
- ・アップロード元にあるフォルダーと同名のファイルがアップロード先のサーバーに存在します。
- ・ダウンロード元にあるファイルと同名のフォルダーがダウンロード先のサーバーに存在します。
- ・ダウンロード元にあるフォルダーと同名のファイルがダウンロード先のサーバーに存在します。

対処

同名のファイル、フォルダーのうち片方の名称を変更してください。

NameTooLongError

意味

ファイル名の長さが制限値を超えています。

対処

該当するファイルの名称を変更してください。

ServerCommunicationError

意味

サーバーへの同時接続数が多すぎるか、BOX IDもしくはパスワードの設定が間違っています。

対処

BOX IDもしくはパスワードに誤りがないか確認してください。BOX IDもしくはパスワードに誤りがない場合、本機以外に同じBOX IDでサーバーに接続している機器が存在するなら接続台数を減らすことを検討してください。

ForbiddenNameError

意味

ファイル名が不正です。

対処

該当するファイルの名称を変更してください。

一括登録をする

※その他の内容については、本体の【画面で見るマニュアル】をご確認ください。

Dropbox同期を有効にする場合

●Dropbox同期を有効にする場合は、一括登録を実行した後、[Dropboxとの同期を有効にする](#)の作業をおこなってください。

●設定書式カスタマイズ

・共有フォルダー設定項目定義

▼フィールド名と設定項目の対応

AmazonS3	AmazonS3同期	1->有効,0->無効,空->無効/無効
AmazonS3AccessKey	アクセスキー	文字列 / 空 (AmazonS3 が有効の場合指定必須)
AmazonS3SecretKey	シークレットキー	文字列 / 空 (AmazonS3 が有効の場合指定必須)
AmazonS3Bucket	バケット	文字列 / 空 (AmazonS3 が有効の場合指定必須)
AmazonS3HttpMethod	プロトコル	http またはhttps / https
AmazonS3StorageClass	ストレージクラス	STANDARD またはRRS / STANDARD
AmazonS3DownloadInterval	更新監視間隔	0->更新監視なし,1~24->時間 / 1
AmazonS3EndPoint	エンドポイント	文字列 / 空
AmazonS3Port	ポート	数字文字列 / 空
AmazonS3UploadMaxFileSize	アップロード最大ファイルサイズ	数字文字列 / 10240
AmazonS3Mpupload	Multipart Upload	1->有効,0->無効,空->無効/無効
Cloudn	Cloudn同期	1->有効,0->無効,空->無効/無効
CloudnAccessKey	アクセスキー	文字列 / 空 (Cloudn が有効の場合指定必須)
CloudnSecretKey	シークレットキー	文字列 / 空 (Cloudn が有効の場合指定必須)
CloudnBucket	バケット	文字列 / 空 (Cloudn が有効の場合指定必須)
CloudnHttpMethod	プロトコル	http またはhttps / https
CloudnStorageClass	ストレージクラス	STANDARD またはRRS / STANDARD
CloudnDownloadInterval	更新監視間隔	0->更新監視なし,1~24->時間 / 1
CloudnEndPoint	エンドポイント	文字列 / str.cloudn-service.com
CloudnPort	ポート	数字文字列 / 空
CloudnUploadMaxFileSize	アップロード最大ファイルサイズ	数字文字列 / 10240
CloudnMpupload	Multipart Upload	1->有効,0->無効,空->無効/無効
Azure	Microsoft Azure同期	1->有効,0->無効,空->無効/無効
AzureAccountName	アカウント名	文字列 / 空 (Azure が有効の場合指定必須)
AzureAccessKey	アクセスキー	文字列 / 空 (Azure が有効の場合指定必須)
AzureContainer	コンテナ名	文字列 / 空 (Azure が有効の場合指定必須)
AzureHttpMethod	プロトコル	http またはhttps / https
AzureDownloadInterval	更新監視間隔	0->更新監視なし,1~24->時間 / 1

※各項目の設定形式と指定しない場合のデフォルト値を“設定形式/デフォルト値”の形で示しています。

●CSVファイルの記述例

▼ケース1

共有フォルダー追加	Share1を追加	AmazonS3同期が有効 アクセスキーが"example-accesskey" シークレットキーが"example-secretkey" バケットが"example-bucket" プロトコルが"https" ストレージクラスが"STANDARD" 更新監視間隔が"1" 時間 エンドポイントが空 MS ネットワーク共有が有効 読み取り専用が無効
-----------	-----------	---

上記設定内容のCSV ファイル

```
#share_config,Name,Comment,AmazonS3,AmazonS3AccessKey,AmazonS3SecretKey,AmazonS3Bucket,AmazonS3HttpMethod,AmazonS3StorageClass,AmazonS3DownloadInterval,AmazonS3EndPoint,Win,ReadOnly
addshare,Share1, コメント,1,example-accesskey,example-secretkey,example-bucket,https,STANDARD,1,,1,0
```

※上記の#share_config行は1行で記述してください。
※上記の"example-accesskey" と"example-secretkey" と"example-bucket" はAmazonS3 アカウントにて作成したものを記述してください。

▼ケース2

共有フォルダー追加	Share2を追加	Dropbox同期が有効 MSネットワーク共有が有効 読み取り専用が無効
-----------	-----------	--

上記設定内容のCSV ファイル

```
#share_config,Name,Comment,Dropbox,Win,ReadOnly
addshare,Share2, コメント,1,1,0
```

▼ケース3

共有フォルダー追加	Share3を追加	Cloudn同期が有効 アクセスキーが"example-accesskey" シークレットキーが"example-secretkey" バケットが"example-bucket" プロトコルが"https" ストレージクラスが"STANDARD" 更新監視間隔が"1" 時間 MSネットワーク共有が有効 読み取り専用が無効
-----------	-----------	---

上記設定内容のCSV ファイル

```
#share_config,Name,Comment,Cloudn,CloudnAccessKey,CloudnSecretKey,CloudnBucket,CloudnHttpMethod,CloudnStorageClass,CloudnDownloadInterval,Win,ReadOnly
addshare,Share3, コメント,1,example-accesskey,example-secretkey,example-bucket,https,STANDARD,1,1,0
```

※上記の#share_config 行は1 行で記述してください。
※上記のexample-accesskey と"example-secretkey" と"example-bucket" はCloudn アカウントにて作成したものを記述してください。

▼ケース4

共有フォルダー追加	Share4を追加	Microsoft Azure同期が有効 アカウント名が"example-account" アクセスキーが"example-accesskey" コンテナ名が"example-container" プロトコルが"https" 更新監視間隔が"1" 時間
-----------	-----------	---

	MS ネットワーク共有が有効 読み取り専用が無効
--	-----------------------------

上記設定内容のCSV ファイル

```
#share_config,Name,Comment,Azure,AzureAccountName,AzureAccessKey,AzureContainer,AzureHttpMethod,AzureDownloadInterval,Win,ReadOnly  
addshare,Share4, コメント,1,example-account,example-accesskey,example-container,https,1,1,0
```

※上記の#share_config 行は1 行で記述してください。

※上記のexample-accesskey と"example-secretkey" と"example-bucket" はCloudn アカウントにて作成したものを記述してください。

CSV一括登録で「設定が不正です。」と表示される場合

設定値として以下の例のような不正な値が設定されています。CSVファイルを修正してください。

例1：Amazon S3 同期を有効、かつDropbox 同期を有効で設定している。

ソフトウェアライセンス情報

[クラウドストレージ パッケージで使用するソフトウェアライセンス情報 \(zip形式 : 6.14KB\)](#)

レプリケーションについて

レプリケーション元に設定したメイン機の共有フォルダーと、レプリケーション先に指定した予備機の共有フォルダーを同期し、同じ状態に保ちます。

※LAN環境により遅延が発生します。遠隔地へのレプリケーションにより、メイン機側での災害・事故によるデータ損失のリスク低減ができません。

※レプリケーション機能はメイン機に保存したデータをファイル単位で予備機にコピーするため、同一の状態になるまでにタイムラグが発生します。

クローンパッケージについて

レプリケーションでは、データのみの同期となります。設定情報も保存したい場合は、クローンパッケージをご利用ください。

ご注意

- レプリケーション先とする予備機には本パッケージを追加する必要はありません。
- 予備機に使用できる機器は以下の機種のみです。
 - ・ HDL-Hシリーズ
 - ・ HDL-AAシリーズ
 - ・ HDL-Xシリーズ
- レプリケーション機能でコピーされるのは、「レプリケーション元共有フォルダー」に指定した共有フォルダー上に保存された、ファイル・フォルダーのデータのみです。アクセス権はコピーされません。
- 予備機をメイン機に接続する前に、予備機の管理者パスワードを4文字以上で設定しておいてください。
- VPN経由でレプリケーションを利用する場合は、十分なスループットを確保できる光回線をご使用ください。
- レプリケーション先に設定された共有フォルダーのデータは、レプリケーション実施後に消去されます。
- ネットワーク(ルーター)を超えるレプリケーションを行う場合のご注意
 - ・ 本製品はレプリケーション通信に「IPv4 TCP : 873 番」を使用します。レプリケーション先の本製品を接続しているルーターがNAT設定されている場合は、「IPv4 TCP : 873番」宛の通信がレプリケーション先の予備機に届くように、ポートフォワード設定が必要です。
 - ・ レプリケーション通信は暗号化をおこなっておりませんので、インターネットを経由するレプリケーションをおこなう場合は、VPN 環境下でのご利用をおすすめします。
- 一時的に予備機を切り離した場合、1時間以内は1分ごと、それ以降は1時間ごとに接続を再試行し、接続できた段階で再開します。（メイン機を再起動した場合でも再開されます。）この場合、レプリケーションの再設定は不要です。
- ファイル数の多い共有フォルダーを変更すると、変更が完了するまでに時間がかかる場合があります。また、変更が完了するまで共有フォルダーにはアクセスできません。
- レプリケーション元共有フォルダーとして指定可能な共有フォルダーは300個です。

レプリケーションを設定する

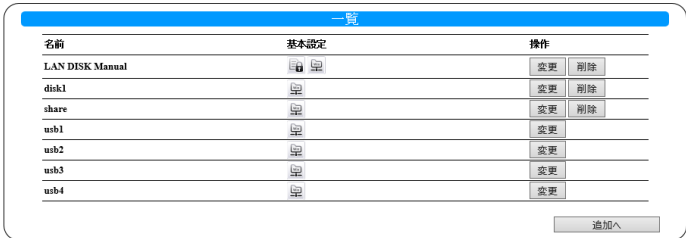
①レプリケーション先(予備機) を設定する

- 1. レプリケーション先の予備機で、管理者パスワードを 4 文字以上で設定する
※詳しくは、本体の【画面で見るマニュアル】をご覧ください。
- 2. レプリケーション先の予備機で、レプリケーション先と する共有フォルダーを作成する
※詳しくは、本体の【画面で見るマニュアル】をご覧ください。

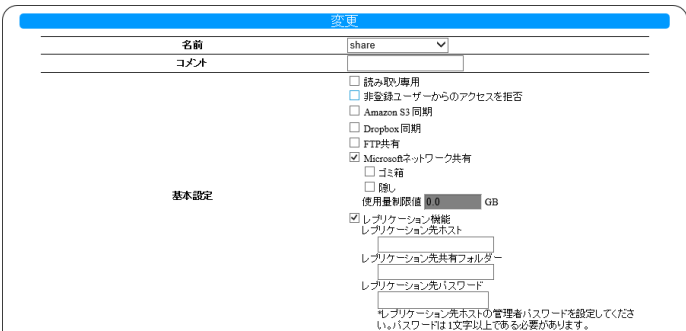
②レプリケーション元（メイン機）を設定する

あらかじめ作成済みの共有フォルダーを同期する設定を説明し ます。

- 1. レプリケーション元のメイン機で、[共有] → [フォルダー] → [一覧] をクリック
- 2. レプリケーション元にする共有フォルダーの[変更] をクリック



- 3. ① [レプリケーション機能] にチェックをつける
- ②レプリケーション先の予備機の情報を入力
- ③ [変更] をクリック



レプリケーション先ホスト	レプリケーション先（予備機）の「LAN DISKの名前」または「IPアドレス(IPv4アドレスまたはIPv6 アドレス(コロン区切り))」を入力します。
レプリケーション先共有フォルダー名	レプリケーション先とする共有フォルダーの名前を入力します。
レプリケーション先パスワード	レプリケーション先（予備機）の管理者パスワードを入力します。パスワードは1文字以上で設定する必要があります。

マスターで共有フォルダーを削除した場合

スレーブの共有フォルダーは削除されません。

一括登録をする

※その他の内容については、本体の【画面で見るマニュアル】をご確認ください。

- 設定書式カスタマイズ
 - ・共有フォルダー設定項目定義
- ▼フィールド名と設定項目の対応

Replication	レプリケーション機能	1->有効,0->無効,空->無効/無効
ReplicationHost	レプリケーション先ホスト	文字列/空(レプリケーション機能が有効の場合指定必須)
ReplicationShare	レプリケーション先共有フォルダー	文字列/空(レプリケーション機能が有効の場合指定必須)
ReplicationPassword	レプリケーション先パスワード	文字列/空(レプリケーション機能が有効の場合指定必須)

- CSVファイルの記述例
- ▼ケース1

共有フォルダー追加	Share1を追加	レプリケーション機能が有効 レプリケーション先ホストが"example-host" レプリケーション先共有フォルダーが"example-share" レプリケーション先管理者パスワードが"example-password" MSネットワーク共有が有効 読み取り専用が無効
-----------	-----------	--

上記設定内容のCSVファイル
#share_config,Name,Comment,Replication,ReplicationHost,ReplicationShare,ReplicationPassword,Win,ReadOnly
addshare,Share1,コメント,1,example-host,example-share,example-password,1,0

CSV一括登録で「設定が不正です。」と表示される場合

設定値として以下の例のような不正な値が設定されています。CSVファイルを修正してください。
例1：USB共有フォルダーに対してレプリケーション機能を有効で設定している。

結果を確認する

レプリケーションの結果を確認する方法を説明します。

1. レプリケーション元のメイン機で、[情報・ログ表示] → [レプリケーション動作状況] をクリック
2. レプリケーション処理の結果を確認する

レプリケーション動作状況			
フォルダー		最終更新検出時刻	結果
dsk1		2016年9月30日 13:39:29	NG
			ログ
			表示 ダウンロード

レプリケーション処理の結果

共有フォルダーごとに、最後に実行したレプリケーション処理の検出時刻[最終更新検出時刻]と、その結果が表示されます。

結果がOKの場合

ログの列には何も表示されません。

結果がNGの場合

[表示] :

レプリケーションのログを確認できます。

[ダウンロード] :

ログをファイルとしてダウンロードできます。

ログがすべて表示されない場合はダウンロードしてご確認ください。

「（共有フォルダー名）のレプリケーション先に接続できませんでした」 または、「（共有フォルダー名）がタイムアウトしました。」 というログが記録された

一時的な通信障害の可能性があります。

レプリケーション元の[自己診断](#)を使用し、その結果、「問題ありません。」であれば対処不要です。

自己診断結果が上記とログと同結果の場合は以下をご確認ください。

- ・レプリケーション先と元が物理的にネットワーク接続されていること
- ・レプリケーション先と元、途中経路のネットワーク設定が正しくされていること

「（共有フォルダー名）を認証できませんでした」というログが記録された

- ・レプリケーション先の管理者パスワードが1文字以上で設定されているか確認してください。
- ・レプリケーション元に設定した、レプリケーション先管理者パスワードが正しいか確認してください。

自己診断する

レプリケーション元（メイン機）で[システム] → [自己診断] をクリックすると、レプリケーション機能についての自己診断をすることができます。

詳しくは、『画面で見るマニュアル』をご覧ください。

自己診断内容

レプリケーション機能について、本製品に設定したレプリケーション先と接続 / 認識できることを確認します。

クローン機能について

本製品※ 2台をそれぞれマスター/ スレーブとして構成し、マスターの設定やファイルをスレーブに保存します。

※ファイルの保存はレプリケーション機能を利用しておこなわれます。 万一のマスター故障時に、スレーブを切り替えることで、迅速に復旧できます。

[クローンを設定する](#)

※同じ機種に限ります。

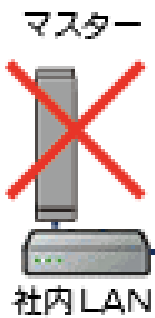
保存先がHDL-AAシリーズの場合



マスター故障時

スレーブを切り替え

マスターと同等サービスを開始



レプリケーションパッケージについて

クローンでは、自動的にマスターの共有フォルダーのデータがスレーブへ同期されます。

共有フォルダー単位で同期設定をおこなう場合は、レプリケーションパッケージをご利用ください。

また、スレーブの代わりにUSB HDDを利用しての設定やファイルの保存・復元もできます。

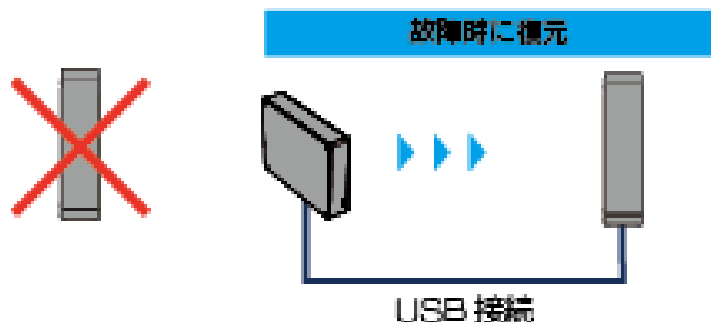
※USB HDDを利用した復元では、対象ファイルをコピーするため、その分時間がかかります。

[USB HDDを利用する](#)

保存先が USB HDD の場合



HDL-AA シリーズ故障時



ご注意

- 事前に、クローン機能を使用する本製品（マスター、スレーブ）に本パッケージを追加してください。
 - 事前に、クローン機能を使用する本製品（マスター）にレプリケーションパッケージ(Ver.1.03 以降)を追加してください。（スレーブには不要です。）
 - 使用できるLAN DISKは本製品のみです。マスターとスレーブは、同じシリーズであれば使用できます。ただし、スレーブにはファイル保存のため十分な空き容量が必要です。
 - 設定の前に、マスターとスレーブの管理者パスワードを4文字以上で設定しておいてください。
 - VPN経由で利用する場合は、十分なスループットを確保できる光回線をご使用ください。
 - スレーブにマスターにあるフォルダーと同名のフォルダーがある場合は、ファイルが削除される可能性があります。必要に応じてバックアップしてください。
 - スレーブの設置がネットワーク(ルーター)を超える場合のご注意
 - ・本製品はクローン通信に「TCP : 873 番」「TCP : 51055番」を使用します。スレーブの本製品を接続しているルーターがNAT設定されている場合は、「TCP : 873番」「TCP : 51055番」宛の通信がスレーブに届くように、ポートフォワード設定が必要です。
 - ・通信は暗号化をおこなっておりませんので、インターネットを経由する場合は、VPN環境下でのご利用をおすすめします。
 - 一時的にスレーブを切り離した場合、レプリケーションエラーがシステムログに記録され、1時間以内は1分ごと、それ以降は1時間ごとに接続を再試行し、接続できた段階で再開します。（マスターを再起動した場合でも再開されます。）この場合、再設定は不要です。ただし、スレーブを切り離された状態でマスターの設定変更をした場合、スレーブへの設定保存が失敗します。この場合は自動で保存はされませんので、再度マスターで設定変更をしてください。
 - ファイル数の多い共有フォルダーを変更すると、変更が完了するまでに時間がかかる場合があります。また、変更が完了するまで共有フォルダーにはアクセスできません。
 - ファイルの保存は、「外付けボリューム共有フォルダー」など削除できない共有フォルダーは対象外です。
 - マスターでのレプリケーションの設定変更はできなくなります。
 - 次の設定項目は保存されません。
 - ・ログのフィルター設定
 - ・暗号化設定
 - ・管理者設定
 - ・以下を除くパッケージ設定
- ※以下の設定は保存対象となります。
- Dropbox以外のクラウド同期設定（Dropboxを有効にした場合は、切替後に再設定が必要です。）
 - FTP
- 共有フォルダーの削除はスレーブ側に反映されません。
- 切り替え後、必要に応じて別途共有フォルダーの削除を実行してください。

クローンを設定する

①スレーブを設定する

1. クローンパッケージを追加する

※方法は、【画面で見るマニュアル】をご覧ください。

2. スレーブで、管理者パスワードを4文字以上で設定する

※管理者パスワードは、【システム】→【管理者設定】で設定できます。詳しくは、本体の【画面で見るマニュアル】をご覧ください。

※他のマスターから設定を保存したことがある場合は、一度クローンパッケージを削除し、再度追加してください。方法は、【画面で見るマニュアル】をご覧ください。

3. スレーブをマスターと同じネットワークに設置し、通信可能な状態にする

マスターをActive Directoryに参加させる場合

スレーブはマスター昇格時にマスターの設定情報を元にActive Directoryに参加します。

通常はマスターのみをActive Directoryに参加させてご利用ください。

マスターとスレーブの接続方法について

LANポートを複数搭載している機種では、ネットワークへの負荷を抑えるため、マスターとスレーブをLAN 2ポート同士で接続することもできます。

この場合、LAN 2ポート同士が通信可能となるように適切なネットワーク設定をおこなってください。

※設置/設定方法は、本体の【画面で見るマニュアル】をご覧ください。

②マスターを設定する

1. クローンパッケージを追加する

※方法は、【画面で見るマニュアル】をご覧ください。

2. レプリケーションパッケージ（ver.1.03以降）を追加する

※方法は、【画面で見るマニュアル】をご覧ください。

3. マスターの設定画面で、【データバックアップ】→【クローン機能】→【マスター設定】をクリック

4. ① [有効] を選択
②スレーブの情報を入力
③ [適用] をクリック

マスター設定

マスターとして動作

☒ 有効

☐ 無効

スレーブ

パスワード

適用

スレーブ	スレーブの「LAN DISKの名前」または「IPアドレス(IPv4アドレスまたはIPv6アドレス(コロン区切り))」を入力します。
パスワード	スレーブの管理者パスワードを入力します。パスワードは1文字以上で設定する必要があります。

ご注意

●スレーブにマスターにあるフォルダーと同名のフォルダーがある場合は、ファイルが削除される可能性があります。必要に応じてバックアップしてください。

設定後の動作について

- これ以降は、マスターで共有フォルダー/ファイルを作成すると、自動で同期されます。同期中にスレーブに共有フォルダーを作成できない場合、マスターでの共有フォルダーの作成は失敗します。この場合、スレーブの容量などをご確認ください。
- マスターで共有フォルダーを削除した場合でも、スレーブの共有フォルダーは削除されません。
- 保存対象の設定を変更すると、最後の設定変更から10分後にスレーブに最新設定が保存されます。スレーブへの設定保存に失敗した場合は、システムログにエラーが記録されます。この場合、再度マスターで設定してください。
- クローン設定後スレーブに対して設定情報も同期されますが、実際にスレーブ側の設定として反映されるのはスレーブからマスターへ切り替わった後となるため、クローン動作中にスレーブの設定画面を確認しても設定内容は変化ありません。
- 同期や切り替え失敗など予期せぬトラブルを防ぐため、クローン中はスレーブへのアクセスはおこなわないようにしてください。
- 各共有フォルダーの同期状況の確認は、マスターの設定画面の [情報] → [レプリケーション機能] で確認できます。

スレーブを切り替える

万一のマスターの故障の際は、スレーブを以下の手順で切り替えます。

マスターをActive Directory環境下でご利用の場合

スレーブはマスター昇格時にマスターの設定情報を元にActive Directoryに参加します。

1. マスターをネットワークから取り外す
- ※マスターがネットワーク上に存在している場合、切り替えが実行できない場合があります。
2. スレーブの設定画面で、[データバックアップ] → [クローン機能] → [切り替え] をクリック
3. 内容を確認し、[実行] をクリック

切り替え

保存設定の情報		
保存日時	2014/11/05 10:51:44	
LAN DISKの名前	landisk-	
LAN1	IPv4	192.168.
	IPv6	-
LAN2	IPv4	-
	IPv6	-

実行

4. Webブラウザ（設定画面）を閉じる
- STATUSランプが点滅から点灯に変わったなら、切り替えは完了です。

マスターの故障を監視し、自動で切り替える場合

スレーブからマスターを監視し、故障を感知した場合に自動で切り替える設定です。

1. スレーブの設定画面で、[データバックアップ] → [クローン機能] → [スレーブ設定] をクリック
2. ① [有効] を選択
- ② マスターの情報を入力
- ③ [適用] をクリック

スレーブ設定

マスター 監視による自動切り替え	☒ 有効 ☐ 無効
故障判定時間	10 分
マスター	landisk- ×

適用

故障判定時間	マスターの稼働状態を確認する時間間隔を設定します。 ※1分ごとに通信し、30秒以内に応答がない状態が[故障判定時間]継続した場合に故障と判定し、切り替えます。
マスター	マスターの「LAN DISKの名前」または「IPアドレス(IPv4アドレスまたはIPv6アドレス(コロン区切り))」を入力します。

切り替え後の本製品の設定について

クローン機能の【ご注意】に記載の移行されない設定を再設定してください。

スレーブを切り替えた場合

スレーブを切り替えた場合、クローン機能は解除されます。再度クローン機能を構築する場合は以下の手順にしたがってください。

※故障した旧マスターを修理などして利用可能な状態にしてから、スレーブとして再利用できます。

- ①旧マスターを修理などして利用可能状態にする
※新しい本製品も使用できます。
- ②旧マスターを出荷時状態に戻す（リセット）
- ③旧マスターにクローンパッケージを追加する
- ④新マスターにレプリケーションパッケージ(Ver.1.03以降)を追加する
- ⑤旧マスターをスレーブに設定する

スレーブが故障した場合

以下の手順で、新しいスレーブに入れ替えてください。

- ①マスターの［データ保守］→［クローン機能］→［マスター設定］で無効にする
- ②新しいスレーブ用の本製品を設置し、クローンパッケージをインストールする
- ③再度クローン設定をする

USB HDDへのクローンを設定する

① USB HDDを設定する

USB HDDへのクローンには、「最後のUSBポート」を使います

各LAN DISKの該当するUSBポートは以下のとおりです。

HDL-AAシリーズ	USBポート2
HDL-AAWシリーズ	USBポート2
HDL2-AAシリーズ	USBポート3
HDL2-AAWシリーズ	USBポート3
HDL2-Xシリーズ	USBポート4
HDL4-Xシリーズ	USBポート4

見ただ目で探す

背面の青いUSBポートが「最後のUSBポート」です。

青いUSBポートが2つある場合は、上にある方が「最後のUSBポート」です。

1. 最後のUSBポートの設定が「共有モード」（初期設定）であることを確認する

※ モード設定は、[ボリューム] → [USBx] → [モード設定] で設定できます。

詳しくは、本体の【画面で見るマニュアル】をご覧ください。

2. USB HDDを最後のUSBポートに接続する

※ 他のUSBポートで、クローン機能は利用できません。

3. USB HDDが専用フォーマットでない場合はフォーマットする

※ [ボリューム] → [USBx] → [フォーマット] でフォーマットできます。暗号化の設定も可能です。詳しくは、本体の【画面で見るマニュアル】をご覧ください。

② 保存する

1. クローンパッケージを追加する

※ 方法は、【画面で見るマニュアル】をご覧ください。

2. レプリケーションパッケージ（ver.1.03以降）を追加する

※ 方法は、【画面で見るマニュアル】をご覧ください。

3. 設定画面で、[データバックアップ] → [クローン機能] → [システム保存設定] をクリック

4. [システム保存(フル)] をクリック
→システム保存を開始します。
STATUSランプが点滅から点灯に変わったら、システム保存は完了です。しばらくお待ちください。

システム保存設定

ステータス	未実行
履歴数	0 0は「制限なし」になります USB4に十分な容量があるかご確認ください ジョーム情報
スケジュール	☐ 有効 ☒ 無効
曜日	日: なし 月: なし 火: なし 水: なし 木: なし 金: なし 土: なし
時刻	00 : 00

適用

システム保存(差分)

システム保存(フル)

システム保存停止

履歴数	保存する履歴の数を設定できます。「0」に設定すると、無制限に保存されますので、USB HDD の容量にご注意ください。指定可能な最大数は「31」です。
スケジュール、曜日、時刻	定期的に保存をおこないます。スケジュール設定をおこなう場合は、[有効]を選択し、曜日・時刻で設定します。
[適用]	設定を保存するのみなど、すぐに保存をしない場合にクリックします。
[システム保存(差分)]	一度フル保存をした後など、前回の保存部分からの差分のみを保存します。
[システム保存(フル)]	すべての内容を保存します。
[システム保存停止]	開始されたシステム保存を停止します。

設定後の動作について

- これ以降は、本製品の設定を変更すると、USB HDDに保存されます。
 - 共有フォルダーやファイルは、以下の操作で保存されます。
 - ・[システム保存(フル)] または [システム保存(差分)] をクリックした時
 - ・スケジュール設定した時刻になった時
 - システム保存の結果は、マスターの設定画面の [情報] → [システムログ] や、マスターの共有フォルダー [LAN DISK Log] の [Backup] → [ジョブ名] 以下で確認できます。
- ※バックアップ結果の詳細は、【画面で見るマニュアル】をご覧ください。

ログが記録されます

システム保存を実行すると、バックアップ（ジョブ名: SystemRestore）に関するシステムログが記録されます。

最後のUSBポートへのアクセス権限が変更されます

システム保存を実行すると最後のUSBポートの共有フォルダーは、管理者だけがアクセスできるように設定変更されます。

※ ご購入時、USBポートは管理者だけがアクセスできる状態です。

ご注意

システム保存したUSB HDDの扱いにご注意ください。

- ◆ 他のNASも含め、管理者以外もアクセスできるように設定変更されたUSBポートにつないだ場合、意図しないユーザーにアクセスされるおそれがあります。
管理者だけがアクセスできるように設定された、最後のUSBポートにつなぐことをおすすめします。

- ◆ パソコンにつないで、保存したデータを閲覧されるおそれがあります。
システム保存したUSB HDDは厳重に保管してください。

USB HDDから復元する

USB HDDに保存したシステムから復元する方法を説明します。

①復元する本体にUSB HDDをつなぐ

USB HDDへのクローンには、「最後のUSBポート」を使います

各LAN DISKの該当するUSBポートは以下のとおりです。

HDL-AAシリーズ	USBポート2
HDL-AAWシリーズ	USBポート2
HDL2-AAシリーズ	USBポート3
HDL2-AAWシリーズ	USBポート3
HDL2-Xシリーズ	USBポート4
HDL4-Xシリーズ	USBポート4

見ただ目で探す

背面の青いUSBポートが「最後のUSBポート」です。
青いUSBポートが2つある場合は、上にある方が「最後のUSBポート」です。

- 1. 最後のUSBポートの設定が[共有モード]（初期設定）であることを確認する
※ モード設定は、[ボリューム] → [USBx] → [モード設定] で設定できます。
詳しくは、本体の【画面で見るマニュアル】をご覧ください。

- 2. システム保存したUSB HDDを最後のUSBポートに接続する

②復元する

- 1. 設定画面で、[データバックアップ] → [クローン機能] → [システム復元] をクリック
- 2. [実行] をクリック
⇒ システム復元を開始します。
STATUSランプが点滅から点灯に変わったら、システム復元は完了です。しばらくお待ちください。
※ [バックアップ履歴] では、保存した履歴から復元するデータを選びます。

システム復元

保存設定の情報

保存日時

保存されていません

LAN DISKの名前

-

LAN1

IPv4

-

IPv6

-

LAN2

IPv4

-

IPv6

-

バックアップ履歴

保存されていません▼

実行

ログが記録されます

システム復元を実行すると、バックアップ(ジョブ名: SystemRestore)に関するシステムログが記録されます。

切り替え後の本製品の設定について

[クローン機能の【ご注意】](#)に記載の移行されない設定を再設定してください。

移行前の確認

本パッケージは、HDL-H、XR、XVの各シリーズ(以後、移行元と呼びます)の共有フォルダーの構成、各共有フォルダー、一部の設定を本製品(以後、移行先と呼びます)に移行するために使用します。

ユーザー、グループ、共有フォルダーの設定

ユーザー、グループ、共有フォルダーの各設定について、移行元と移行先それぞれに設定がおこなわれている場合、いない場合により処理が異なります。

移行元	移行先	処理内容
設定あり	設定なし	移行元の構成を新規作成
設定なし	設定あり	処理なし(移行先の構成は削除されない)
設定あり	設定あり	移行元の構成に設定変更

移行されない設定

- 以下の設定は移行されません。
 - ・RAIDモード(暗号化設定含む)
 - ・NarSuS設定
 - ・管理者設定
 - ・クラウド同期、FTPを除くパッケージ設定(ただし、Dropboxの設定は保存されません)
 - ・USBポート1以外のモード設定
- 以下の設定が有効に設定されている場合は無効に変更します。
 - ・バックアップ/データコピーのスケジュール設定
 - ・共有フォルダーのレプリーケーション設定
 - ・電源のスケジュール終了設定
- HDL-XR、XVシリーズから移行する場合、以下の設定も移行されません。
 - ・バックアップ
 - ・共有フォルダーのクラウド同期設定
 - ・iobb.net
 - ・リモートリンク
 - ・DLNA設定
 - ・net.USB設定
 - ・レプリーケーション

移行されないフォルダー

- ・LAN DISK Manual
- ・LAN DISK Log
- ・usb1～4
- ・esata1
- ・tmadmin
- ・削除できない共有フォルダー（移行元がHDL-Hシリーズの場合のみ）

ご注意

- 移行先には、移行元のファイルをコピーするため十分な空き容量が必要です。
- 移行元と移行先に同名のファイル・フォルダーが存在する場合、移行元のファイル・フォルダーで上書きされます。移行先にのみ存在

するファイル・フォルダーは削除されません。

移行する

1. 移行元、移行先が同じネットワークに接続されていることを確認する
2. 移行先の設定画面を開き、[データバックアップ] → [H/XR/XV移行] をクリック
3. ①設定情報を入力
- ② [設定保存] または [設定保存して今すぐ実行] をクリック

H/XR/XV移行

移行状態

未実行

移行元

Ⓜ 候補検索

移行元の管理者パスワード

スケジュール実行

☐ 有効 ☒ 無効

強制フルコピー

☐ 有効 ☒ 無効

移行を実行しただけでは本機のネットワーク設定(LAN1設定、LAN2設定、Microsoftネットワーク設定、名前設定)は変更されません。ネットワーク設定を移行する場合は、移行元をネットワークから切り離してから「移行元のネットワーク設定を反映」を行ってください。

移行元のネットワーク設定を反映

設定保存

設定保存して今すぐ実行

移行状態	移行状態を表示します。
移行元	移行元のHDL-H、XR、XVのコンピューター名またはIPアドレスを入力します。 [候補検索] をクリックすると、再検索します。
移行元の管理者パスワード	移行元のHDL-H、XR、XVのパスワードを入力します。
スケジュール実行	設定したスケジュールでの移行をおこなう場合は、[有効] を選択します。
日時	スケジュール実行を[有効]にした場合、日時を設定します。
強制フルコピー	[無効] を選択すると、差分コピーとなり、変更のあったファイルのみコピーします。 ※通常は[無効] を選択します。 [有効] を選択すると、常にすべてのファイルをコピーします。
移行元のネットワーク設定反映	移行実行後に、移行元のネットワーク設定を移行先に反映する場合にクリックします。以下の項目が移行されます。 ・LAN1設定 ・LAN2設定 ・Microsoftネットワーク設定 ・名前設定 ・Active Directory参加時のアクセス権限 ネットワーク設定反映をおこなう場合は、移行元のLAN DISKはネットワークから取り外してください。 移行元のネットワーク設定を反映する

移行元を運用しながら、移行する場合

移行元のLAN DISKを運用しながら移行したい場合は、次のように実行します。

①上記手順を参照し、[強制フルコピー] が[無効] の設定で移行を実行します。

②ログファイルを確認しコピーされたファイルが“0”になるまで、①を実行します。

※ログファイルの確認方法については、[移行結果を確認する](#)をご覧ください。

移行結果を確認する

[LAN DISK Log] 共有の [Data Copy] の [移行_(共有フォルダー名)] 以下に移行結果を記録します。

「(移行実行日時)_summary.log」というファイル名のログファイルで内容を確認してください。

※移行中に移行元のファイルを更新した場合などは、[強制フルコピー] を [無効] にした状態での移行実行後、コピーしたファイルが“0”であれば、移行が完了したことになります。

失敗した場合は「(移行実行日時)_failed.log」というファイル名のログファイルで、内容を確認してください。

■ ログファイルの内容と対処

※ログ内容を「Error」で検索し、検索に掛かった場合は対処をご覧ください。

ログ内容	意味	対処
NoSpaceError	データコピー先の容量が足りません。	データコピー先の容量を確保してください。
NoEntryError	フォルダーやファイルが見つかりません。	データコピー中にファイル・フォルダーを変更しないようにしてください。
ExistsError	以下のうちいずれかに該当します。 ・データコピー元にあるファイルと同名のフォルダーがデータコピー先に存在します。 ・データコピー元にあるフォルダーと同名のファイルがデータコピー先に存在します。	同名のファイル、フォルダーのうち片方の名称を変更してください。
TimeOutError	ネットワーク上のデータコピー元への接続がタイムアウトしました。	データコピー元や本製品のネットワーク設定を確認してください。
UnMountedError	対象のボリュームがマウントされていません。	対象のボリュームがマウントされているか確認してください。
ShareNotExistsError	対象の共有フォルダーが存在していません。	対象の共有フォルダーが存在しているか確認してください。

移行中に移行元のデータを削除した場合

移行中に移行元のファイルの移動や削除をおこなうと、移行が失敗となる場合があります。
この場合、ファイルの移動や削除をおこなわないようにして、再度移行を実行してください。

移行元のネットワーク設定を反映する

- 1. 移行処理が完了したことを確認する
- 2. 移行元のLAN DISKをネットワークから取り外す
- 3. 移行先の設定画面を開き、[データバックアップ] → [H/XR/XV移行] をクリック
- 4. [移行元のネットワーク設定反映] をクリック

H/XR/XV移行

移行状態	未実行
移行元	詳細検索
移行元の管理者パスワード	
スケジュール実行	☐ 有効 ☒ 無効
強制フルコピー	☐ 有効 ☒ 無効

移行を実行しただけでは本機のネットワーク設定(LAN設定、LAN2設定、Microsoftネットワーク設定、名前設定)は変更されません。ネットワーク設定を移行する場合は、移行元をネットワークから取り離してから「移行元のネットワーク設定を反映」を行ってください。

移行元のネットワーク設定を反映

設定保存

設定保存して今すぐ実行

移行後の作業（パッケージの削除）

移行後に、誤って移行を実行してしまうことを防ぐため、H/XR/XV移行パッケージを削除します。

- 1. 移行先の設定画面を開く
- 2. [システム] → [パッケージ管理] → [一覧] をクリック
- 3. ① [H/XR/XV移行] にチェック
② [削除] をクリック

一覧

☐ 全てチェック全て解除

パッケージ名	バージョン	操作	
☐ [パッケージ名]	1.00	☐ 削除	☐ 詳細
☐ [パッケージ名]	1.00	☐ 削除	☐ 詳細
☐ [パッケージ名]	1.00	☐ 削除	☐ 詳細

削除

更新

追加へ

本製品のメディアサーバー機能

パソコンやテレビなどのメディアプレーヤーを利用して、ネットワーク経由で本製品内の指定したフォルダー内のコンテンツを楽しむことができます。

再生できるファイルフォーマット

ファイルサイズによる制限はありませんが、本製品は以下の拡張子のファイルのみに対応しています。
※ファイル編集ソフトなどで拡張子を変更した場合などファイルによっては、下記ファイル拡張子でも再生できない場合があります。
以下の形式のファイルの本製品内の公開するフォルダーに保存してください。

動画	mpe mpeg mpg m2p tts m2ts mts m1v m2v mp1v mp2v mpv mpgv m4v mp4 mov wmv avi divx asf dvr-ms vob 3gp mkv
写真	jpg jpeg mpo jps png bmp gif tif tiff m3u
音楽	mp3 wma wav lpcm pcm ogg m4a m4b 3gp flac aif aiff aac ac3

メディアプレーヤーからの再生方法

メディアプレーヤーからの再生方法は、お使いのメディアプレーヤーのマニュアルをご覧ください。

ご注意

- 公開フォルダー内のファイル数は、合計1万ファイル以内でご利用ください。
- メディアサーバー設定の変更や公開フォルダー内のファイルに変化があると、データベースの構築がおこなわれます。この間、再生できない場合があります。また、公開している共有フォルダーへのファイルコピーは、公開していないものより遅くなります。
- 公開する共有に含まれるファイル数が多い場合には、メディアプレーヤーからの接続に時間がかかります。また、公開中の共有にファイルをコピーしたり削除した場合にも、データベース構築がおこなわれるため、時間がかかる場合があります。ファイル数によっては、数時間かかることもあります。
- 本製品の設定中は、メディアプレーヤーからアクセスしないでください。
- ネットワークメディアプレーヤーで再生中のファイルや、再生中のファイルがある共有フォルダーを削除したり移動させたりしないでください。
- 同時再生をおこなったり、再生中にパソコンから本製品へファイルコピーなどの操作をした場合やバックアップ処理中などの場合、再生するファイルがコマ落ちしたり、音飛びしたりすることがあります。
- Windowsのネットワークに表示されるアイコンについて
本製品のメディアサーバーは、Windowsのネットワーク画面に追加アイコンとして表示される場合があります。ダブルクリックするとメディアプレーヤーが起動する場合がありますが、お使いのパソコンのメディアプレーヤーがDLNAに準拠していない場合は、本製品の共有フォルダー内のコンテンツの再生はできません。
- コンテンツ再生時にMP3ファイルのタイトル名・アーティスト名などの情報が文字化けして表示される場合があります。その場合は、ID3タグ情報を編集可能なソフトウェアで、文字コードをUnicodeへ変更してください。文字コード変更しても改善しない場合は、ご利用のメディアプレーヤーの仕様によって文字化けが発生している場合があります。

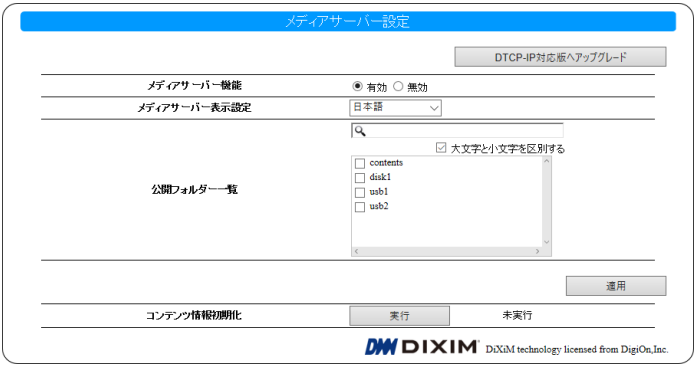
メディアサーバーを設定する

メディアサーバーとして公開するフォルダーを設定します。

ご注意

コンテンツ再生中の設定変更やコンテンツ情報の初期化はおこなわないでください。

- 1. [共有] → [メディアサーバー設定]
- 2. ① [メディアサーバー機能] の [有効] にチェック
②メディアサーバーの公開フォルダーなどを設定をする
③ [適用] をクリック



DTCP-IP対応版へアップグレード	メディアサーバーをDTCP-IP対応版にアップグレードします。 詳しくは、メディアサーバー（DTCP-IP対応版）の アップグレードする をご覧ください。
メディアサーバー機能	本製品のメディアサーバー機能の有効/無効を設定します。
メディアサーバー表示設定	再生時のフォルダー構成の言語を設定します。 例えば、「英語」に設定すると、再生時のフォルダー名称などが英語表示になります。（フォルダー→Folder、アルバム→Albumなど）
公開フォルダー一覧	メディアサーバーとして公開するフォルダーを選択します。選択したフォルダー内のコンテンツをメディアプレーヤーから再生することができます。
コンテンツ情報の初期化	本製品で管理するコンテンツ情報を初期化します。 通常はおこなう必要はありません。メディアプレーヤーに本製品のコンテンツが表示されない場合に実行してください。

ソフトウェアライセンス情報

[メディアサーバー パッケージで使用するソフトウェアライセンス情報 \(zip形式 : 43.0KB\)](#)

アップグレードする

ここでは、パッケージ「メディアサーバー」を追加済みの方が、DTCP-IP対応版にアップグレードする方法をご案内します。

DTCP-IP 対応版へのアップグレード

DTCP-IP 対応版へアップグレードすると、地上デジタル / BSデジタル / CSデジタル等の著作権保護されたコンテンツを本製品に保存し、テレビなどの別の機器から利用できます。

[注意事項](#)

[アップグレード方法](#)

注意事項

- ◆ ご利用の録画機器がDTCP-IP対応版に対応しているかどうか、[「対応表 \(Webページ\)」](#)をご確認ください。
- ◆ アップグレードには、別途ioPLAZAで購入したライセンスキーが必要です。
- ◆ 本製品をインターネットに常時接続できる環境が必要です。
- ◆ DTCP-IP機能で録画・保存したコンテンツについて
コンテンツと本製品の基板が紐付管理されています。
そのため、以下のような使い方はできません。
 - ・ 取り外した内蔵ディスクを別の筐体に入れて、コンテンツを利用する
 - ・ 本体部分だけが交換修理になった場合、今までのコンテンツを利用する
 - ・ バックアップ機能などによるコンテンツのバックアップ
- ◆ **パッケージ「メディアサーバー」を削除した場合、アップグレード時に作成される「recorded」フォルダーとその中のコンテンツは削除されます。（「recorded」には録画コンテンツ等が保存されます。）**

アップグレード方法

1. パッケージ「メディアサーバー」を最新の状態にする

パッケージを更新する

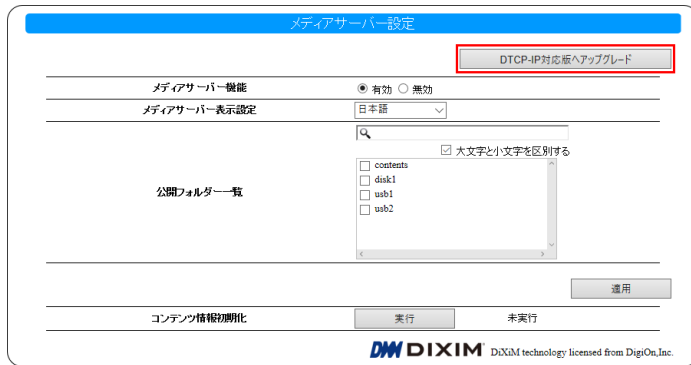
〔システム〕→〔パッケージ管理〕→〔一覧〕をクリックし、「メディアサーバー」をチェックしてから〔更新〕をクリックしてください。

〔更新〕をクリックできない場合は、すでに最新版です。

※ 本製品をインターネットに接続できる環境が必要です。

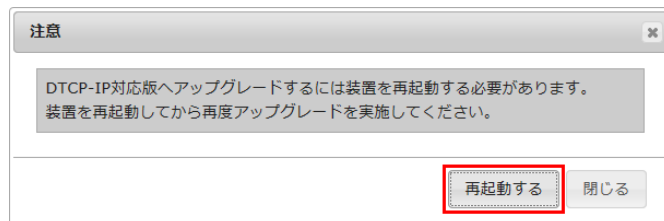
2. 設定画面の〔共有〕→〔メディアサーバー設定〕をクリック

3. [DTCP-IP対応版へアップグレード] をクリック

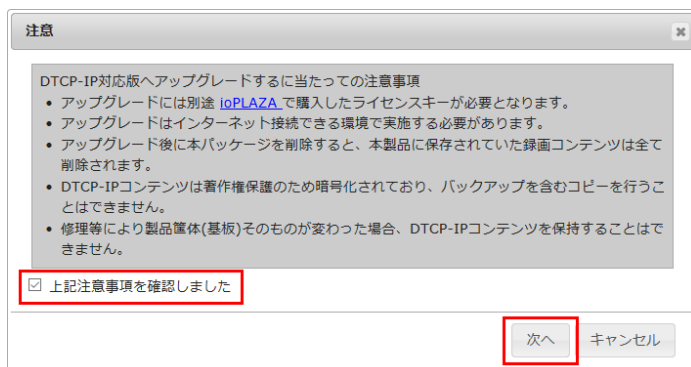


再起動を要求された場合は

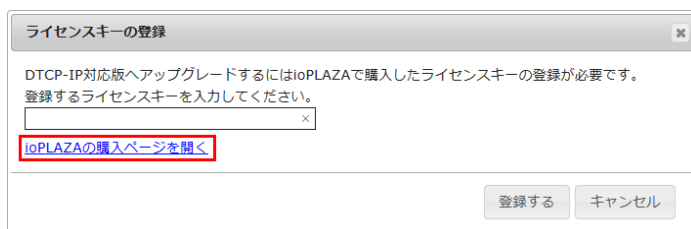
[再起動する] をクリックし、再起動してください。
その後、上の手順2からやり直してください。



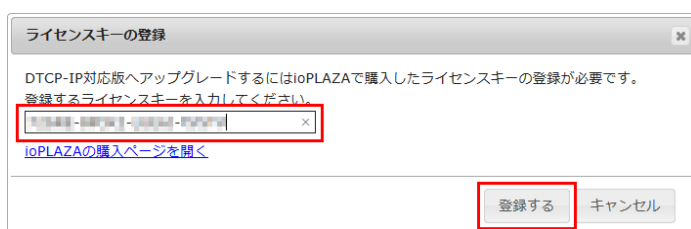
4. 表示された注意をよく読み、[上記注意事項を確認しました] にチェックしてから、[次へ] をクリック



5. [ioPLAZAの購入ページを開く] をクリックし、ioPLAZAからライセンスキーを購入する ※ ライセンスキーを購入済みの場合は、この手順を飛ばしてください。



6. ライセンスキーを入力し、[登録する] をクリック ※ ライセンスキーは「-」（ハイフン）も含めて入力してください。



7. 「DTCP-IP対応版へのアップグレードが完了しました。」と表示されれば、アップグレードは完了です。
⇒ [共有] → [メディアサーバー設定] を開いた場合、今度からこの画面が表示されます。

メディアサーバー設定

DTCP-IP対応版へのアップグレードが完了しました。

登録されたライセンスキー: [不明] [不明] [不明] [不明]

メディアサーバー管理画面

[管理画面を開く](#)

公開フォルダー一覧

検索

☒ 大文字と小文字を区別する

☐ contents

☐ disk1

☐ usb1

☐ usb2

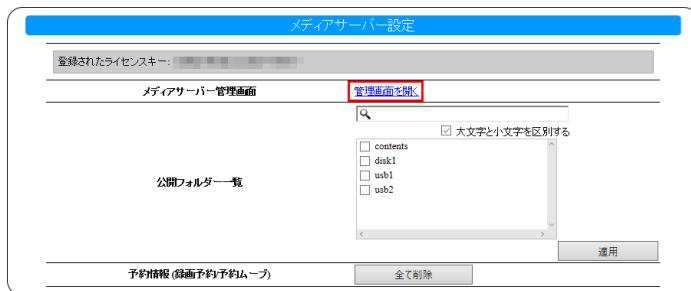
予約情報 (録画予約予約ムーフ)

全て削除

適用

使い方

1. 設定画面の［共有］→［メディアサーバー設定］をクリック
2. 〔管理画面を開く〕をクリック
⇒ メディアサーバー（DTCP-IP対応版）の設定画面が表示されます。



この画面の設定方法については、別マニュアル『パッケージ メディアサーバー（DTCP-IP対応版）画面で見るマニュアル』をご覧ください。
http://www.iodata.jp/lib/manual/hdl-aa_pkg-dtcpip/index.html（別ウィンドウ）

ソフトウェアライセンス情報

[メディアサーバーを参照](#)

利用可能にする（アクティベート）

[アクティベートについて](#)

[管理画面を開く](#)

[プロキシを設定する場合](#)

[利用可能にする（アクティベート）](#)

「ESET File Security」と共存できません

- ・「ESET File Security」パッケージが追加されている場合は、本パッケージの追加はできません。
- ・本パッケージが追加されている場合は、「ESET File Security」パッケージの追加はできません。

本パッケージの追加に必要な容量

本パッケージを追加すると、NASの保存容量が約5GB使用されます。

アクティベートについて

本パッケージをご利用いただくためには、「アクティベート」が必要です。
アクティベートを実行することにより、以下の機能が利用可能になります。

- ・リアルタイム検索機能
- ・ウイルスパターンの自動更新機能
- ・スパイウェア/グレーウェアパターンの自動更新機能
- ・検索エンジンの自動更新機能

ご注意

- 本製品をインターネットに接続してください。
設置方法は、本製品の管理マニュアルをご覧ください。
インターネットに接続できない場合、パターンファイルが更新できなくなり、新しいウイルスなどが検出できない可能性があります。
- インターネット接続にプロキシサーバーを利用する場合は、アクティベートの前にプロキシサーバーを設定してください。
方法は、[プロキシを設定する場合](#) をご覧ください。
- 管理者は、Trend Micro NAS Security の管理画面や、隔離されているウイルスファイルにアクセスできます。
- 「Trend Micro NAS Security」のシリアル番号をご用意ください。
[「LDOP-LS/TML1」](#) を購入することで、1年間のシリアル番号（ライセンス）を購入できます。
※ HDL-AAW、HDL2-AAWは3年間のライセンスが標準添付しています。

管理画面を開く

1. 本製品の設定画面を開く
※ 設定画面の開き方は、本製品の管理マニュアルを参照
2. [ウイルス対策] → [TMNAS] をクリック

3. 以下のどちらかをクリック

- ・ Trend Micro NAS Security 管理画面(https)
- ・ Trend Micro NAS Security 管理画面(http)

Web ブラウザーで下記URL に直接アクセスして開くこともできます

https://[LAN DISK の名前かIP アドレス]:14943/

または

http://[LAN DISK の名前かIP アドレス]:14942/

- ① 「ユーザー名」に [admin] と入力
- ② 「パスワード」に設定した管理者パスワードを入力
- ③ [ログオン] をクリック



ログオン

ユーザー名とパスワードを入力してWebコンソールにアクセスしてください。

ユーザー名:

パスワード:

下の画面が表示された場合

[このサイトの閲覧を続行する] をクリックしてください。

 この Web サイトのセキュリティ証明書には問題があります。

この Web サイトで提示されたセキュリティ証明書は、信頼された証明機関から発行されたものではありません。
この Web サイトで提示されたセキュリティ証明書は、別の Web サイトのアドレス用に発行されたものです。

セキュリティ証明書の問題によって、詐欺や、お使いのコンピューターからサーバーに送信される情報を盗み取る意図が示唆されている場合があります。

このページを閉じて、この Web サイトの閲覧を続行しないことを推奨します。

☒ [ここをクリックしてこの Web ページを閉じる。](#)

☐ [このサイトの閲覧を続行する \(推奨されません\)。](#)

[詳細情報](#)

これで、管理画面が開きます。

プロキシを設定する場合

1. [管理画面を開く](#)

2. ① [管理] をクリック
- ② [プロキシ設定] をクリック



3. ① [プロキシサーバを使用してインターネットにアクセスする] にチェックを付ける
- ② プロキシ設定をする
- ③ [保存] をクリック

プロキシの設定

コンポーネントのアップデート

☒ プロキシサーバを使用してインターネットにアクセスする (ライセンスアップデート)

サーバ名またはIPアドレス:

ポート:

プロキシサーバ認証

ユーザ名:

パスワード:

サーバ名またはIP アドレス	プロキシサーバの名前またはIP アドレスを入力します。IPv4 アドレスのみ入力可能です。(IPv6 は未対応)
ポート	プロキシ接続する際に利用する通信ポート番号を入力します。
プロキシサーバ認証 ユーザ名 パスワード	利用するプロキシサーバがユーザー認証を必要とする場合、[ユーザ名] [パスワード] を入力します。 ユーザー認証が必要ない場合は空欄のままご利用ください。

※ [コンポーネントのアップデート] タブでは、パターンファイル更新時に利用するプロキシを設定することができます。

これで、プロキシ設定は完了です。

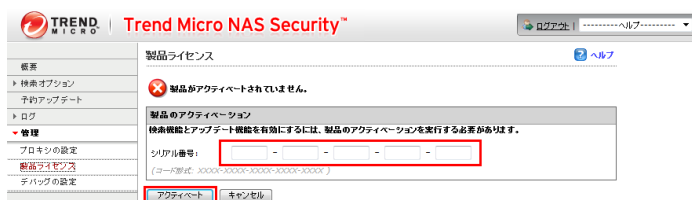
利用可能にする (アクティベート)

1. [管理画面を開く](#)

2. ① [管理] をクリック
② [製品ライセンス] をクリック



3. ① 「Trend Micro NAS Security」のシリアル番号を入力
② [アクティベート] をクリック



4. [OK] をクリック



以上で、アクティベートは完了です。

ウイルスが発見されたら…

本製品内にウイルスが発見された場合、設定にしたがって処理されます。
初期設定では、以下のように処理されます。

駆除された場合

ファイルのウイルス挙動部分が削除され、ファイルは健全な状態で残ります。
駆除される前のファイルは拡張子を変更してバックアップフォルダー「TMNAS.Backup」へコピーされます。

駆除できなかった場合

対象ファイルは拡張子を変更して隔離フォルダー「TMNAS.Quarantine」へ移動されます。

※ バックアップフォルダー・隔離フォルダーは、本製品の隠し共有フォルダー「tmadmin」に作成されています。
「tmadmin」にアクセスできるのは、ユーザー「admin」だけです。
アクセス方法については、[こちら](#)をご覧ください。

ご注意

- バックアップフォルダー・隔離フォルダーへコピー・移動されたファイルは自動で削除されません。
定期的に削除することをおすすめします。
- バックアップフォルダー・隔離フォルダーの容量が増加すると、駆除・隔離によるファイルのコピー・移動ができないことがあります。
 - ◆ バックアップフォルダーへコピーできない場合でもウイルスは駆除されます。
駆除される前のファイルは残りません。
またこのとき、駆除される前のファイルがあった場所に、「元のファイル名.RB●.BAK(●は数字)」のファイルが作られます。
このファイルは削除してください。
 - ◆ 隔離フォルダーへ移動できない場合、対象ファイルは削除されてしまいます。
- ウイルスが発見されファイルが削除された場合、ファイルがあった共有フォルダーに以下の名前のファイルが作成されます。
ウイルスが検出されたため削除されました_XXXX
(XXXX は元のファイル名)
- ウイルスが発見されファイルが隔離された場合、ファイルがあった共有フォルダーに以下の名前のファイルが作成されます。(XXXX は元のファイル名)
ウイルスが検出されたため隔離されました_XXXX
- ウイルスが発見された場合、処理結果にしたがって以下のメッセージがログに記録されます。またお知らせにも表示されます。
ウイルスが削除されました。共有:XXXX 上のファイル:YYYY
ウイルスが隔離されました。共有:XXXX 上のファイル:YYYY
ウイルスが駆除されました。共有:XXXX 上のファイル:YYYY
ウイルスファイルの拡張子を変更されました。共有:XXXX 上のファイル:YYYY
ウイルスが放置されました。共有:XXXX 上のファイル:YYYY
ウイルスファイルを適切に処理できませんでした。共有:XXXX 上のファイル:YYYY
(XXXX は共有名、YYYY はディレクトリ含むファイル名)

バックアップフォルダー・隔離フォルダーへのアクセス手順例（Windows）

1. エクスプローラーを開く



2. 「\\¥landisk-xxxxxx¥tadmin」 にアクセスする

※ xxxxxxは、LAN ポートのMAC アドレス下6桁

※ 本製品の名前を変更した場合は、「landisk-xxxxxx」のところを変更した名前に変えて入力します。

3. ログオン画面が表示されたら、ユーザー「admin」でログオンする

ユーザー名	admin
パスワード	設定した管理者パスワード

エラーが表示された場合

- パソコンを再起動してください。
- 再起動してもだめな場合は、以下を確認してください。
 - ・ 手順前に本製品の共有フォルダーを開かないこと
 - ・ LAN DISK コネクトを開かないこと
 - ・ 本製品の共有フォルダーをネットワークドライブに割り当てていないこと

管理画面のリファレンス

- 検索オプション → リアルタイム検索
- 検索オプション → 予約検索
- 検索オプション → 手動検索
- 予約アップデート
- ログ → ウイルスログ
- ログ → スパイウェアログ
- ログ → 検索ログ
- ログ → システムログ
- ログ → 手動削除
- ログ → 自動削除
- 管理 → プロキシの設定
- 管理 → 製品ライセンス
- 管理 → デバッグの設定

検索オプション → リアルタイム検索

ファイルを保存したときに即座にウイルス検索を実施する「リアルタイム検索」に関するオプションを設定します。
オプションを設定したら「保存」ボタンをクリックし、設定内容を適用します。

- ☒ リアルタイム検索を有効にする
- リアルタイム検索を有効にする：
ファイルが保存された際に自動的にウイルス検索を実施する場合にチェックを付けます。（推奨）

出荷時設定 有効

リアルタイム検索

リアルタイム検索

☒ 入力ファイル

☐ 出力ファイル

- 入力ファイル：
NAS に保存されるファイルについて、リアルタイム検索を実施します。（推奨）

出荷時設定 有効
- 出力ファイル：
NAS から出力されるファイルについて、リアルタイム検索を実施します。

出荷時設定 無効

次のファイルタイプを検索

次のファイルタイプを検索

☒ すべてのファイルタイプ

☐ IntelliScan: 実際のファイルタイプによる識別

☐ 指定のファイル拡張子:

☐ トレンドマイクロが推奨する拡張子を検索

注意: これらの拡張子は、新しいバージョンファイルが公開されるたびにアップデートされます。

☐ 選択した拡張子を検索:

使用可能な拡張子:

ARJ

BAT

BIN

BOO

CAB

CHM

追加 >

< 削除

検索するファイルタイプ:

他の拡張子 :

拡張子ごとにコロンの (:) またはセミコロン (;) で区切って入力してください。

- すべてのファイルタイプ：
デフォルト設定値です。保存されるファイル形式にかかわらず、すべてのファイルについてウイルス検索を実施します。

- IntelliScan：実際のファイルタイプによる識別：
ファイルヘッダを調べて実際のファイルタイプを判断します。
- 指定のファイル拡張子：

トレンドマイクロが推奨する拡張子を検索

パターンファイルとともに配信されるトレンドマイクロが推奨する拡張子一覧にしたがってウイルス検索を実施します。

「推奨する拡張子」をクリックすると、実際に検索される拡張子を確認することができます。

選択した拡張子を検索

ユーザが設定した拡張子を持つファイルについてウイルス検索を実施します。
 ここで指定されていない拡張子を持つファイルがウイルス感染している場合には、排除できません。
 ※「他の拡張子」は、拡張子選択リストに表示されていない拡張子を指定する場合に利用します。

圧縮ファイル検索の設定

圧縮ファイル検索の設定

☒ 圧縮ファイルを検索する
注意: 大きなサイズの圧縮ファイルを検索すると、システムのパフォーマンスが低下する可能性があります。
 圧縮の階層数が次の値より小さい:

1

 圧縮解除されたファイルのサイズが次の値より小さい:

30

 MB

- 圧縮ファイルを検索する：
zip 形式など、圧縮されたファイルもウイルス検索を実施します。

出荷時設定

 有効
- 圧縮の階層数が次の値より小さい：
複数段階圧縮されたファイルに対し、どこまで検索対象とするかを指定します。

出荷時設定

 1
- 圧縮解除されたファイルのサイズが次の値より小さい：
圧縮されたファイルの元のサイズに対し、どこまで検索対象とするかを指定します。

出荷時設定

 30

セキュリティリスクが見つかった時の処理

セキュリティリスクが見つかったときの処理

☒ 処理を実行する前に、セキュリティリスクが存在するファイルをバックアップする。

セキュリティリスクが検出されたときの処理を選択：

☐
 トレンドマイクロの推奨処理 - ファイルタイプ別の推奨処理

☒
 カスタム処理

種類	1次処理	2次処理
ジョークプログラム	隔離	
トロイの木馬	隔離	
ウイルス	ウイルス駆除	隔離
テラウイルス	放置	
スパイウェア/グレーウェア	隔離	
バット	ウイルス駆除	隔離
その他	ウイルス駆除	隔離

☒
 すべての種類に同じ処理を使用

種類	1次処理	2次処理
すべての種類	ウイルス駆除	隔離

- 処理を実行する前に、セキュリティリスクが存在するファイルをバックアップする。：
検出した際、指定の動作を行う前にファイルをバックアップするかどうか指定します。

出荷時設定

 有効
- セキュリティリスクが検出されたときの処理を選択：

トレンドマイクロの推奨処理 - ファイルタイプ別の推奨処理

トレンドマイクロの推奨処理方法にしたがってファイルタイプ別に処理を行います。

カスタム処理

種類ごとに処理方法を指定します。

すべての種類に同じ処理を使用

すべての種類について一律に処理します。

予約した時刻にLAN DISK 内をウイルス検索する「予約検索」に関するオプションを設定します。
オプションを設定したら「保存」ボタンをクリックし、設定内容を適用します。

予約検索は無効になりました。
☐ 予約検索を有効にする

- 予約検索を有効にする：
ファイルが保存された際に自動的にウイルス検索を実施する場合にチェックを付けます。

出荷時設定 無効

検索周期

検索周期

開始時刻：

00

：

00

 (hh:mm)

アップデートの周期：

☒ 毎日

☐ 毎週

金曜日

☐ 毎月

1

- 開始時刻：
予約検索を実行する時刻を設定します。

出荷時設定 00:00
- アップデートの周期：
検索を実施する周期を設定します。

出荷時設定 毎日

次のファイルタイプを検索

次のファイルタイプを検索

☒ すべてのファイルタイプ

☐ IntelliScan: 実際のファイルタイプによる識別

!

☐ 指定のファイル拡張子：

☐ トレンドマイクロが推奨する拡張子を検索
注意: これらの拡張子は、新しいパターンファイルが公開されるたびにアップデートされます。

☐ 選択した拡張子を検索：

使用可能な拡張子：

ARJ

BAT

BIN

BOO

CAB

CHM

検索するファイルタイプ：

追加 >

< 削除

他の拡張子

!

:

拡張子ごとにコロン (:) またはセミコロン (;) で区切って入力してください。

- すべてのファイルタイプ：
デフォルト設定値です。保存されるファイル形式にかかわらず、すべてのファイルについてウイルス検索を実施します。
- IntelliScan：実際のファイルタイプによる識別：
ファイルヘッダを調べて実際のファイルタイプを判断します。
- 指定のファイル拡張子：

トレンドマイクロが推奨する拡張子を検索

パターンファイルとともに配信されるトレンドマイクロが推奨する拡張子一覧にしたがってウイルス検索を実施します。
「推奨する拡張子」をクリックすると、実際に検索される拡張子を確認することができます。

選択した拡張子を検索

ユーザが設定した拡張子を持つファイルについてウイルス検索を実施します。
ここで指定されていない拡張子を持つファイルがウイルス感染している場合には、排除できません。
※「他の拡張子」は、拡張子選択リストに表示されていない拡張子を指定する場合に利用します。

圧縮ファイル検索の設定

圧縮ファイル検索の設定

☒ 圧縮ファイルを検索する

圧縮の階層数が次の値より小さい：

5

圧縮解凍されたファイルのサイズが次の値より大きい：

60

 MB

- 圧縮ファイルを検索する：
zip 形式など、圧縮されたファイルもウイルス検索を実施します。

出荷時設定 有効

- 圧縮の階層数が次の値より小さい：

複数段階圧縮されたファイルに対し、どこまで検索対象とするかを指定します。

出荷時設定 5

- 圧縮解除されたファイルのサイズが次の値より小さい：

圧縮されたファイルの元のサイズに対し、どこまで検索対象とするかを指定します。

出荷時設定 60

セキュリティリスクが見つかった時の処理

セキュリティリスクが見つかったときの処理

☒ 処理を実行する前に、セキュリティリスクが存在するファイルをバックアップする。 ⓘ

セキュリティリスクが検出されたときの処理を選択：

☐ トレンドマイクロの推奨処理 - ファイルタイプ別の推奨処理 ⓘ

☐ カスタム処理

種類	1次処理	2次処理
ジョークプログラム	隔離	
トロイの木馬	隔離	
ウイルス	ウイルス検除	隔離
テラ-ウイルス	放置	
スパイウェア/グレーウェア	隔離	
バグカー	ウイルス検除	隔離
その他	ウイルス検除	隔離

☒ すべての種類に同じ処理を使用

種類	1次処理	2次処理
すべての種類	ウイルス検除	隔離

- 処理を実行する前に、セキュリティリスクが存在するファイルをバックアップする。：

検出した際、指定の動作を行う前にファイルをバックアップするかどうか指定します。

出荷時設定 有効

- セキュリティリスクが検出されたときの処理を選択：

トレンドマイクロの推奨処理 - ファイルタイプ別の推奨処理

トレンドマイクロの推奨処理方法にしたがってファイルタイプ別に処理を行います。

カスタム処理

種類ごとに処理方法を指定します。

すべての種類に同じ処理を使用

すべての種類について一律に処理します。

検索オプション → 手動検索

手動でLAN DISK 内をウイルス検索する「手動検索」に関するオプションを設定します。

〔検索開始〕ボタンをクリックすると、設定内容にしたがってウイルス検索を実施します。

オプションを設定したら〔保存〕ボタンをクリックし、設定内容を適用します。

次のファイルタイプを検索

次のファイルタイプを検索

☒ すべてのファイルタイプ

☐ IntelliScan: 実際のファイルタイプによる識別 ⓘ

☐ 指定のファイル拡張子：

☐ トレンドマイクロが推奨する拡張子を検索

注意: これらの拡張子は、新しいバージョンファイルが公開されるたびにアップデートされます。

☐ 選択した拡張子を検索：

使用可能な拡張子：

ARJ
BAT
BIN
BOO
CAB
CHM

追加 >

< 削除

検索するファイルタイプ：

他の拡張子 ⓘ：

拡張子ごとにコロンの (:) またはセミコロンの (;) で区切って入力してください。

- すべてのファイルタイプ：

デフォルト設定値です。保存されるファイル形式にかかわらず、すべてのファイルについてウイルス検索を実施します。

- IntelliScan：実際のファイルタイプによる識別：
ファイルヘッダを調べて実際のファイルタイプを判断します。
- 指定のファイル拡張子：

トレンドマイクロが推奨する拡張子を検索

パターンファイルとともに配信されるトレンドマイクロが推奨する拡張子一覧にしたがってウイルス検索を実施します。
「推奨する拡張子」をクリックすると、実際に検索される拡張子を確認することができます。

選択した拡張子を検索

ユーザが設定した拡張子を持つファイルについてウイルス検索を実施します。
ここで指定されていない拡張子を持つファイルがウイルス感染している場合には、排除できません。
※「他の拡張子」は、拡張子選択リストに表示されていない拡張子を指定する場合に利用します。

圧縮ファイル検索の設定

圧縮ファイル検索の設定

☒ 圧縮ファイルを検索する

検索する圧縮ファイルの階層数：

5

解凍されたファイルのサイズが次の値より小さい：

60

 MB

- 圧縮ファイルを検索する：
zip 形式など、圧縮されたファイルもウイルス検索を実施します。

出荷時設定

 有効
- 圧縮の階層数が次の値より小さい：
複数段階圧縮されたファイルに対し、どこまで検索対象とするかを指定します。

出荷時設定

 5
- 圧縮解除されたファイルのサイズが次の値より小さい：
圧縮されたファイルの元のサイズに対し、どこまで検索対象とするかを指定します。

出荷時設定

 60

セキュリティリスク検出時の処理

セキュリティリスク検出時の処理

☒ 処理を実行する前に、セキュリティリスクが存在するファイルをバックアップする。

セキュリティリスク検出時の処理を選択：

トレンドマイクロの推奨処理 - ファイルタイプ別の推奨処理

カスタム処理

種類	1次処理	2次処理
ジョークプログラム	隔離	
トロイの木馬	隔離	
ウイルス	ウイルス排除	隔離
デタウウイルス	放置	
スパイウェア/グレーウェア	隔離	
バッカー	ウイルス排除	隔離
その他	ウイルス排除	隔離

☒ すべての種類に同じ処理を使用

種類	1次処理	2次処理
すべての種類	ウイルス排除	隔離

- 処理を実行する前に、セキュリティリスクが存在するファイルをバックアップする。：
検出した際、指定の動作を行う前にファイルをバックアップするかどうか指定します。

出荷時設定

 有効
- セキュリティリスクが検出されたときの処理を選択：

トレンドマイクロの推奨処理 - ファイルタイプ別の推奨処理

トレンドマイクロの推奨処理方法にしたがってファイルタイプ別に処理を行います。

カスタム処理

種類ごとに処理方法を指定します。

すべての種類に同じ処理を使用

すべての種類について一律に処理します。

ウイルスパターンファイル、スパイウェア／グレーウェアパターンファイル、およびウイルス検索エンジンを自動的にアップデートできます。

☒ 予約アップデートを有効にする

- 予約アップデートを有効にする：
予約アップデートを実施する場合にチェックを付けます。

無効

アップデート周期

アップデート周期

開始時刻: 00 : 00 (hh:mm)

アップデートの周期:

- ☐ 毎時間
- ☒ 開始時刻から次の時間内にアップデート: 2時間
- ☐ 毎週 日曜日

開始時刻から次の時間内にアップデート: 2時間

- 開始時刻：
アップデートを開始する時刻を設定します。
 00:00
- アップデートの周期：
アップデートを開始する周期を設定します。
アップデートは指定した時間の範囲内でランダムに開始されます。
 開始時刻から次の時間内にアップデート（毎日）、2時間

アップデートするコンポーネント

アップデートするコンポーネントを選びます。

すべて有効

アップデートするコンポーネント		
☒ コンポーネント	現在のバージョン	前回のアップデート
☒ ウイルスパターンファイル		
☒ スパイウェア/グレーウェアパターンファイル		
☒ 検索エンジン		

ログ → ウィルスログ

ウィルス検出ログを参照します。
設定し、[ログの表示] ボタンをクリックすると、ログが表示されます。最大 1,000 件まで表示できます。

0個のログが保存されました

データの範囲:

今日

開始日:

2016-02-10

終了日:

2016-02-10

表示順:

開始日/時刻

降順

ページあたりの表示件数

25

件

注意: 指定のデータ範囲における最新の1000個のログのみが表示されます。

- データの範囲：
あらかじめ設定された範囲（開始日、終了日）を選んで設定できます。

ログ → スパイウェアログ

スパイウェア検出ログを参照します。
設定し、[ログの表示] ボタンをクリックすると、ログが表示されます。最大 1,000 件まで表示できます。

0個のログが保存されました

データの範囲:

今日

▼

開始日:

2016-02-10

終了日:

2016-02-10

表示順:

開始日/時刻

▼

降順

▼

ページあたりの表示件数

25

▼

件

注意: 指定のデータ範囲における最新の1000個のログのみが表示されます。

ログの表示

- データの範囲:
- あらかじめ設定された範囲（開始日、終了日）を選んで設定できます。

ログ → 検索ログ

セキュリティリスクの検索記録を参照します。
設定し、[ログの表示] ボタンをクリックすると、ログが表示されます。最大 1,000 件まで表示できます。

0個のログが保存されました

データの範囲:

今日

▼

開始日:

2016-02-10

終了日:

2016-02-10

表示順:

開始日/時刻

▼

降順

▼

ページあたりの表示件数

25

▼

件

注意: 指定のデータ範囲における最新の1000個のログのみが表示されます。

ログの表示

- データの範囲:
- あらかじめ設定された範囲（開始日、終了日）を選んで設定できます。

ログ → システムログ

Trend Micro NAS Security のシステムログを参照します。
設定し、[ログの表示] ボタンをクリックすると、ログが表示されます。最大 1,000 件まで表示できます。

1個のログが から に保存されました

データの範囲:

今日

▼

開始日:

2016-02-10

終了日:

2016-02-10

表示順:

日付/時刻

▼

降順

▼

ページあたりの表示件数

25

▼

件

注意: 指定のデータ範囲における最新の1000個のログのみが表示されます。

ログの表示

- データの範囲:
- あらかじめ設定された範囲（開始日、終了日）を選んで設定できます。

ログ → 手動削除

ログを手動で削除します。
設定し、[削除] ボタンをクリックすると、該当のログが削除されます。
※ 削除したログデータは復旧できません。ご注意ください。

保存されたログ

ウイルスログ：0

スパイウェア/グレーウェアログ：0

検索ログ：0

システムログ：1

合計ログ：1

削除

すべてのログ

次の日付より以前のログ：2012-02-10

削除

ログ → 自動削除

ログを自動的に削除します。

チェックして保持する日数を設定し、〔保存〕ボタンをクリックします。

保持する日数を過ぎたログデータが自動的に削除されるようになります。

※ 削除したログデータは復旧できません。ご注意ください。

保存されたログ

ウイルスログ：0

スパイウェア/グレーウェアログ：0

検索ログ：0

システムログ：1

合計ログ：1

ログを自動削除する

ログを保持する日数：60日

保存

キャンセル

管理 → プロキシの設定

インターネット接続時にプロキシサーバーを経由する必要がある場合に設定します。

設定の必要性や有無が分からない場合は、システム管理者に確認してください。

一般

ライセンスのアップデートに関するプロキシ情報を設定します。

必要な場合は、〔プロキシサーバを使用してインターネットにアクセスする（ライセンスアップデート）〕にチェックを付け、プロキシサーバーを指定してください。

一般コンポーネントのアップデート

プロキシサーバを使用してインターネットにアクセスする（ライセンスアップデート）

サーバ名またはIPアドレス：

ポート：

プロキシサーバ認証

ユーザ名：

パスワード：

保存

キャンセル

コンポーネントのアップデート

パターンファイル更新時に利用するプロキシを設定します。

通常は〔一般と同じ〕に設定しておいてください。必要に応じて〔カスタマイズ〕をお選びください。

一般

コンポーネントのアップデート

プロキシを設定して、ウイルスパターンファイルおよびスバイウェア/グレーウェアパターンファイルをアップデートします。

☐ [一般]と同じ

☒ カスタマイズ

☐ プロキシサーバを使用してインターネットにアクセスする

サーバ名またはIPアドレス:

ポート:

プロキシサーバ認証

ユーザ名:

パスワード:

保存

キャンセル

管理 → 製品ライセンス

ライセンス状況を確認できます。有効期限が近付いている場合は更新ライセンスをご用意ください。
[新しいシリアル番号]をクリックすることで、[新しいシリアル番号画面](#)が表示されます。
更新ライセンスを組み合わせることにより、最長 5 年間本製品の検索機能をご利用いただくことができます。

サポート契約期間は に終了します。

サポート契約期間が終了するまで、あと189日です。

ライセンス情報	
製品:	Trend Micro NAS Security
製品ライセンス:	製品版
シリアル番号:	新しいシリアル番号
ステータス:	アクティベート済み
有効期限:	

新しいシリアル番号画面

準備した更新ライセンスに同梱されているシリアル番号を入力します。
入力後、[アクティベート] ボタンをクリックすると、有効期限が更新されます。

新しいシリアル番号を入力して、製品をアクティベートしてください。

新しいシリアル番号	
製品:	Trend Micro NAS Security
現在のシリアル番号:	
新しいシリアル番号:	- - - -

アクティベート

キャンセル

更新用ライセンス

[「LDOP-LS/TML1」](#)をご用意ください。

管理 → デバッグの設定

デバッグモードを有効にすると、不具合が発生した場合に、製品の動作状況を細かく記録できます。
ただし、システムへの負荷が高くなりますので、通常は無効にしてください。
[保存] ボタンをクリックするとデバッグモードを設定できます。

デバッグログを収集するための設定を指定します。トラブル対応などに使用するため、通常利用では有効にする必要はありません。

デバッグログの設定	
☐	デバッグモードを有効にする
☐	カーネルデバッグモードを有効にする
デバッグログをエクスポートする	
デバッグログが含まれるファイルを生成します。 エクスポート	

保存

キャンセル

デバッグログの設定

- デバッグモードを有効にする：
デバッグモードの有効／無効を設定します。
☐ 出荷時設定 ☐ 無効
- カーネルデバッグモードを有効にする：
より細かなログ記録を行う場合にチェックします。
☐ 出荷時設定 ☐ 無効

デバッグログをエクスポートする

「エクスポート」をクリックすると、デバッグモードを有効にして記録した情報を取得します。
デバッグログの格納場所は隠しフォルダーとなっています。アクセス方法は、[バックアップフォルダー・隔離フォルダーへのアクセス手順例 \(Windows\)](#) をご覧ください。

ソフトウェアライセンス情報

[Trend Micro NAS Security パッケージで使用するソフトウェアライセンス情報 \(zip形式 : 175KB\)](#)

利用可能にする（アクティベート）

[アクティベートについて](#)

[利用可能にする（アクティベート）](#)

「Trend Micro NAS Security」と共存できません

- ・「Trend Micro NAS Security」パッケージが追加されている場合は、本パッケージの追加はできません。
- ・本パッケージが追加されている場合は、「Trend Micro NAS Security」パッケージの追加はできません。

アクティベートについて

本パッケージをご利用いただくためには、「アクティベート」が必要です。
アクティベートを実行することにより、本パッケージが利用可能になります。

ご注意

- 本製品をインターネットに接続してください。
設置方法は、本製品の管理マニュアルをご覧ください。
インターネットに接続できない場合、アクティベートやウイルス定義データベースが更新できなくなり、新しいウイルスなどが検出できない可能性があります。
- インターネット接続にプロキシサーバーを利用する場合は、アクティベートの前にプロキシサーバーを設定してください。
方法は、本製品の『画面で見るマニュアル』をご覧ください。
- 「ESET File Security」の「購入コード」をご用意ください。（添付の『ESET File Security はじめにお読みください』参照）

利用可能にする（アクティベート）

1. 本製品の設定画面を開く
※ 設定画面の開き方は、本製品の管理マニュアルを参照
2. [ウイルス対策] → [ESET] → [ライセンス管理] をクリック
3. 「1.」の登録ページアイコンをクリック

The screenshot shows the 'ライセンス管理' (License Management) window. It has two tabs: '新規アクティベーション' (New Activation) and '更新アクティベーション' (Update Activation). The '新規アクティベーション' tab is active. It contains three numbered steps: 1. 'ESETのユーザー登録' (ESET user registration) with a document icon, 2. 'ユーザーサイトにログイン' (Login to user site) with a document icon, and 3. '以下の項目に入力したライセンスキーファイルとユーザー名、パスワードを入力して[適用]を押してください' (Enter license key file, username, and password, then click [Apply]). Below the steps is a section titled '有効期限' (Valid Period) with a dropdown menu. At the bottom, there are input fields for 'ライセンスキーファイル' (License key file), 'ユーザー名' (Username), and 'パスワード' (Password), followed by an '適用' (Apply) button.

4. ① [購入コード] を入力する
- ② [登録用メールアドレス] と [登録用メールアドレス (確認用)] を入力する
- ③ [メール送信] をクリック

Canon キヤノン ITソリューションズ株式会社

ESET製品 新規登録

このたびは、ESETセキュリティソフトウェアシリーズをご購入いただき誠にありがとうございます。
下記のフォームに「購入コードまたはシリアル番号(※)」とメールアドレスを入力していただき、[メール送信] ボタンをクリックしてください。
入力いただいたメールアドレス宛に、「ライセンス情報取得案内」(ユーザー登録のご案内)をお送りします。

※ 購入コードまたはシリアル番号とは・・・
パッケージ製品に同梱されている「購入コードのご案内」または「シリアル番号のご案内」用紙、もしくはダウンロード製品購入後に販売店より配信されるメールに記載されています。シリアルキー「ライセンスキー」と記載されている場合もございますので、ご注意ください。

購入コードまたはシリアル番号 (半角入力)		※ 大文字・小文字の区別がされます。 ※ 全角で入力した場合は登録に失敗しますので、ご注意ください。
登録用メールアドレス (半角入力)		
登録用メールアドレス(確認用) (半角入力)		※ 確認のため、もう一度ご入力ください。

5. 登録したメールアドレスに届いたメールを確認し、そこに記載されたURLのWebページを開く

6. 画面の指示に従って、ユーザー登録する
⇒ 登録が終わると、メールを受信します。

7. 登録したメールアドレスに届いたメールを開き、そこに記載された「ユーザー名」「パスワード」「シリアル番号」を確認する

8. 本製品の設定画面に戻り、「2.」のユーザーズサイトアイコンをクリック

ライセンス管理

新規アクティベーション / 更新アクティベーション

1. ESETのユーザー登録を完了し、送付されたメールに記載されている「ユーザー名」、「パスワード」、「シリアル番号」を確認してください。

2. ユーザーズサイトにログインし、「ライセンス情報」タブをクリックして「ライセンスキーファイル」をダウンロードしてください。

3. 以下の項目に入手した「ライセンスキーファイル」と「ユーザー名」「パスワード」を入力して「適用」を押してください。(10分程度時間がかかる場合があります。)

↓

有効期限: ...

ライセンスキーファイル		変更
ユーザー名		
パスワード		

9. ① メールに記載の「シリアル番号」「ユーザー名」を入力する
- ② 内容を確認し、[同意する] にチェック
- ③ [ログイン] をクリック

Canon キヤノン ITソリューションズ株式会社

ユーザーズサイト

ユーザーズサイトについて

ユーザーズサイトは、ESET File Security for Linux / Windows Server (旧製品名: ESET File Security for Microsoft Windows Server, ESET NOD32アンチウイルス サーバー) をご購入いただいたお客様が専用のWebサイトです。同サイトでは、以下の各種情報を入手いただけます。

- 最新のプログラムやマニュアル
- お客様のライセンス情報
- 最新の製品サポート情報

<ユーザーズサイトへのログインについて>

- ログインする際に、シリアル番号・ユーザー名を30分以内に連続して5回以上誤って入力された場合、不正な入力等が疑われるため、ログイン機能を一時的にロックさせていただきます。
- ロックは30分後に解除されますので、解除後に再度、ログイン操作をお願いします。
- シリアル番号・ユーザー名をお忘れになった際、ログインに際してのお問い合わせは[こちら](#)

ログイン

シリアル番号
JM

※ NOD32またはJMでは半角英数字を入力してください。

ユーザー名
EAV-

※ EAV-では半角英数字を入力してください。

ソフトウェア使用に際してのエンドユーザーライセンス契約書

☒ 同意する

© Canon IT Solutions Inc.

10. ① [ライセンス情報] をクリック
- ② 「ライセンスキーファイル」内の [Download] をクリック
⇒ ライセンスキーファイルをダウンロードします。
- ※ ライセンスキーファイル以外のファイルなどをダウンロードする必要はありません。

Canon キヤノン IT ソリューションズ株式会社

ログアウト

トップ ライセンス情報 プログラム/マニュアル ウィルス定義データベース

サポート情報

ライセンス情報

ライセンス情報(保有状況)

お客様名(英語)	
ライセンス種別	ESET File Security for Linux / Windows Server 6年パック
総ライセンス数	1
シリアル番号	JM
ユーザー名	EAV
パスワード	
契約終了日	2021年9月29日

※ 現在登録されているメールアドレスの変更を希望される場合は[こちら](#)からお手続きください。

ライセンスキーファイル

ライセンスキーファイルを取得するには [Download] ボタンをクリックして、ファイルを保存してください。

Download

※ ライセンスキーファイルは、Linuxサーバー用プログラムESET File Security for Linuxをご利用の際に必要となります。ESET File Security for Microsoft Windows Serverをご利用の際は必要ありません。

© Canon IT Solutions Inc.

11. ① 本製品の設定画面に戻る
- ② [参照] をクリックし、手順10.で入手した「ライセンスキーファイル」を選ぶ
- ③ 手順7.で入手した「ユーザー名」「パスワード」を入力する
- ④ [適用] をクリック

ライセンス管理

新規アクティベーション 更新アクティベーション

1. ESETのユーザー登録を行い、送付されてきたメールに記載されている「ユーザー名」「パスワード」、シリアル番号を確認してください。

2. ユーザーサイトにログインし、「ライセンス情報」タブをクリックして「ライセンスキーファイル」をダウンロードしてください。

3. 以下の項目に入力した「ライセンスキーファイル」と「ユーザー名」「パスワード」を入力して「適用」を押してください。(10分程度時間がかかる場合があります。)

有効期限 -

ライセンスキーファイル **参照**

ユーザー名

パスワード

適用

以上で、アクティベートは完了です。（設定反映には数分から10分程度かかります。）

※ ネットワーク環境によって、「ウィルス定義データベース更新」の完了まで時間がかかる場合があります。

ウイルススキャン

1. 本製品の設定画面を開く

※ 設定画面の開き方は、本製品の管理マニュアルを参照

2. [ウイルス対策] → [ESET] → [ウイルススキャン] をクリック

3. 今すぐにウイルススキャンする場合 [ウイルススキャン実行] をクリック

スキャンのスケジュールを設定する場合

① スケジュールを設定する

② [適用] をクリック

スケジュールの設定

毎週

毎週チェックした曜日の指定時刻に実行されます。

毎日

毎日指定時刻に実行されます。

繰り返し

指定した時間毎に繰り返し実行されます。

以上で、ウイルススキャンをすることができます。

スキャンオプション設定

「ヒューリスティックスキャン」「リアルタイムスキャン」の有効/無効を設定できます。

1. それぞれの有効/ 無効を選ぶ

2. [適用] をクリック

ヒューリスティックスキャン

ウイルス定義データベースに基づく検出に加えて、ヒューリスティック機能による検出※ がおこなわれます。

※ ヒューリスティック機能による検出では、パターン照合ではなくウイルスに特徴的な挙動があるかどうかを調べます。新種や亜種のウイルスも検出することが可能です。ただし、正規のアプリケーションを、ウイルスとして検知する場合があります。

リアルタイムスキャン

Windows からLAN DISK の共有フォルダーにファイルを作成した時にウイルスに感染していないかスキャンがおこなわれます。ウイルスが発見されると対象のファイルが削除され、ウイルスによる被害を未然に防ぐことができます。

※ リアルタイムスキャンの対象はWindows共有だけです。

ウイルスが発見されたら…

本製品内にウイルスが発見された場合、駆除が実行されます。

ウイルスが発見され削除された場合

ファイルがあったフォルダーに以下の名前のファイルが作成されます。

– ウイルスが検出されたため削除されました_XXXX

※ XXXX は元のファイル名

ウイルスが発見された場合

処理結果にしたがって以下のメッセージがログに記録されます。

また、お知らせにも表示されます。

– ウイルスが削除されました。共有:XXXX 上のファイル:YYYY

– ウイルスが発見されましたが削除できませんでした。共有:XXXX 上のファイル:YYYY

※ XXXX は共有名、YYYY はディレクトリ含むファイル名

ウイルス定義データベース更新

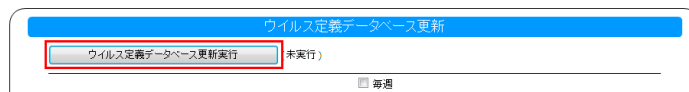
1. 本製品の設定画面を開く

※ 設定画面の開き方は、本製品の管理マニュアルを参照

2. [ウイルス対策] → [ESET] → [ウイルス定義データベース更新] をクリック

3. 今すぐに更新する場合

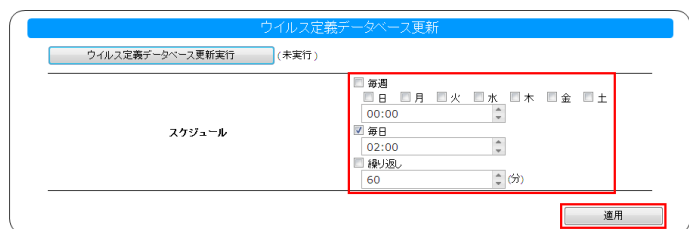
[ウイルス定義データベース更新実行] をクリック



更新のスケジュールを設定する場合

① スケジュールを設定する

② [適用] をクリック



スケジュールの設定

毎週

毎週チェックした曜日の指定時刻に実行されます。

毎日

毎日指定時刻に実行されます。

繰り返し

指定した時間毎に繰り返し実行されます。

※ 初期設定では、毎日02:00に更新されるようになっています。

以上で、ウイルススキャンをすることができます。

Webユーザインターフェース

ご注意

ESET File Security Web インターフェースを利用すると、ESET File Security が提供するすべての設定を変更することができます。ただし、ご利用方法等については、サポート対象外となります。

1. 本製品の設定画面を開く

※ 設定画面の開き方は、本製品の管理マニュアルを参照

2. [ウイルス対策] → [ESET] → [詳細設定ページ] をクリック

3. ①「Webインターフェース」の[有効]を選ぶ

②「接続ポート番号」を入力

※ ESET File Security Web インターフェースにアクセスするポート番号を指定します。

③ [適用] をクリック

以上で、設定は完了です。

ESET File Security Web インターフェースを利用するには

Web ブラウザーを起動し、以下にアクセスします。

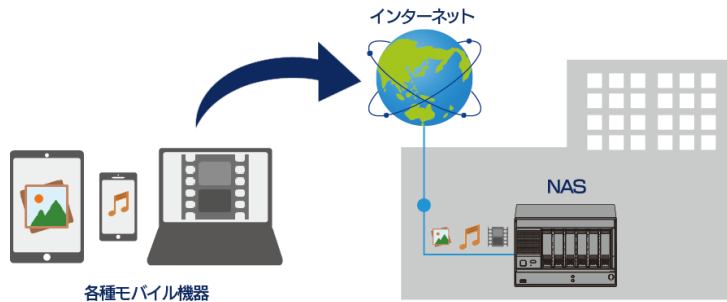
[https://LAN DISK のホスト名: ポート番号/](https://LAN_DISKのホスト名:ポート番号/)

その後、Username にはadmin、Password には管理者パスワードを入力します。

Remote Link 3とは？

外出先のモバイル機器からインターネットを介して、NASに保存してあるデータを見ることができる機能です。

アプリ「Remote Link Files」を利用すると、スマートフォン/タブレット/パソコンからNASに保存した写真、動画、音楽などが楽しめます。



スマホアプリ「Remote Link Files」について

ダウンロードなど詳しくは、以下の弊社Webサイトをご覧ください。

<http://www.iodata.jp/product/app/nas/remotelinkFiles/>

パソコン版「Remote Link Files for PC」について

ダウンロードなど詳しくは、[「Remote Link Files for PC」画面で見るマニュアル](#)をご覧ください。

ご注意

Remote Link 3機能を利用するには、インターネット環境が必要です。インターネット接続にプロキシが必要な環境ではご利用いただけません。

Remote Link 3パッケージを削除する際はインターネット環境が必要です。また、本パッケージを追加した状態でNASを初期化する際もインターネット環境が必要です。

パソコン用自動同期アプリ「Remote Link PC Sync」

Remote Link PC Sync は、Remote Link 3 をベースにしたパソコン用アプリです。

パソコンとNASとの間でファイルの自動同期ができます。詳しくは、以下のWeb サイトをご覧ください。

<http://www.iodata.jp/r/4877>

同時アクセスできる端末数の制限について

Remote Link 3で同時アクセス端末数は、3台までです。

Remote Link 3の設定をする

NAS側で「Remote Link 3設定」をおこない、接続する端末側のアプリ「Remote Link Files」に設定すると、NASへのリモートアクセスができるようになります。

Remote Link 3機能を利用するには

Remote Link 3機能を利用するには、事前に会員情報サービス「IOPortal」での会員登録が必要です。
以下のWeb サイトで登録してください。

<https://ioportal.iodata.jp/>

①Remote Link 3の初期設定をおこなう

②端末の接続設定をおこなう

①Remote Link 3の初期設定をおこなう

1. [共有] → [Remote Link 3] をクリック
2. ①「Remote Link 3利用規約」を確認し、[同意する] にチェックをつける
② [利用規約に同意して次へ進む] をクリック

3. ①会員登録をしていない場合は、[IOPortal]をクリックして登録する
②会員登録した内容を入力
③ [本製品をIOPortalに登録する] をクリック

4. [Remote Link 3] の[有効] を選ぶ

※ [端末認証機能]、[一時公開機能] については、必要に応じて変更してください。

Remote Link 3

接続情報更新: 成功

Remote Link 3 ☒ 有効 ☐ 無効

端末認証機能 ☒ 有効 ☐ 無効

一時公開機能 ☐ 有効 ☒ 無効

[詳細項目を開く](#)

共有フォルダ名	Remote Link 3	端末認証機能
LAN DISK Log	☐ 有効	☐ 有効
LAN DISK Manual	☐ 有効	☐ 有効
disk1	☐ 有効	☐ 有効
disk2	☐ 有効	☐ 有効
usb1	☐ 有効	☐ 有効
usb2	☐ 有効	☐ 有効
usb3	☐ 有効	☐ 有効
usb4	☐ 有効	☐ 有効

適用

端末認証機能、一時公開機能とは？

各機能について詳しくは、[端末認証機能](#)、[一時公開機能](#)をご覧ください。

詳細項目について

「詳細項目を開く」をクリックすると、以下の設定ができます。

通常は設定を変更する必要はありません。内容については、以下の一覧をご覧ください。

ポート番号 1、2

Remote Link 3で使用するポート番号を設定します。

UPnP機能

UPnP機能の使う/使わないを設定します。アクセスできない場合などに「使わない」にすると改善することがあります。

外部ポートを変更する

外部ポートを変更する場合は、「はい」を選択し、「外部ポート番号」を入力します。

外部ポート番号 1、2

外部ポートを変更する場合に、変更するポート番号を入力します。

「接続情報更新」について

Remote Link 3を利用するためのサーバーへの接続状態を表示します。

「失敗」と表示されている場合、NASが正常にインターネットへ接続できる状態であるか確認してください。

5. ①アクセスを許可するフォルダーを選ぶ
② [適用] をクリック

共有フォルダー名	Remote Link 3	端末認証機能
LAN DISK Log	☒ 有効	☐ 有効
LAN DISK Manual	☒ 有効	☐ 有効
disk1	☒ 有効	☐ 有効
usb1	☒ 有効	☐ 有効
usb2	☒ 有効	☐ 有効
usb3	☒ 有効	☐ 有効
usb4	☒ 有効	☐ 有効

① ② 適用

Remote Link 3適用フォルダーの設定について

Remote Link 3

Remote Link 3機能を有効にするフォルダーにチェックをつけます。

端末認証機能

端末認証機能で認証した端末のみアクセス許可するフォルダーを選びます。

[端末認証機能](#)をご覧ください。

※フォルダーの数が多い場合は、[共有フォルダー名] 欄にフォルダー名の一部を入力すると、探しやすくなります。

以上で、初期設定は完了です。

次に端末のアクセス設定をおこないます。

IOPortalの会員登録情報を変更した場合

会員登録情報を変更した場合は、[Remote Link 3] → [IOPortal] で更新してください。

初期設定の内容を変更する場合

アクセスを許可するフォルダーを変更する場合など、再度設定を変更する場合は、[Remote Link 3] → [設定] をクリックします。

② 端末のアクセス設定をおこなう

本製品にインターネット経由でアクセスします。

アクセス可能な端末は、アプリ「Remote Link Files」が動作するスマートフォン、タブレット、パソコンです。

1. インターネット経由でのアクセスを許可するユーザーをNASに追加する
設定方法は、【画面で見えるマニュアル】の【共有設定する】の項をご確認ください。
2. [共有] → [Remote Link 3] → [接続用PINコード] をクリック

3. 接続用PINコード（QRコード）が表示されるので、端末の「Remote Link Files」で読み取る



QRコードが読み取れない端末は、PINコードをご利用ください

PINコード（QRコード）は端末にメールで送ることができます。受け取ったメールから、コピー＆ペーストするなどで利用できます。

アクセスする端末宛のメールアドレスを入力し、［PINコードをメールで送る］ボタンをクリックします。この機能を利用するには、事前にLAN DISKの［メール設定］をおこなってください。

※メール設定をおこなう場合は、［メール設定ページへ移動］をクリックします。設定内容については、【画面で見るマニュアル】の【本製品の動きを通知する】をご覧ください。

［接続用PINコードを変更する］について

有効になるPINコード（QRコード）を変更します。

接続用PINコードを変更すると、これ以前に読み取ったPINコード（QRコード）はすべて無効になり、アクセスできなくなりますのでご注意ください。

また、これまでに登録された［端末管理］、［一時公開一覧］の情報もすべて削除されます。

Remote Link Filesでのアクセス方法は以下をご覧ください。

▶ スマートフォン・タブレットアクセスする場合

1. スマートフォン・タブレットに「Remote Link Files」をインストールする

Remote Link Filesのインストール方法

PlayストアやApp Storeで「Remote Link Files」を検索してください。

2. Remote Link Filesをタップ

3. 「登録を開始する」をタップ



4. 「QRコードで登録」をタップ



5. [読み取り開始] をタップし、QR コードを読み取る

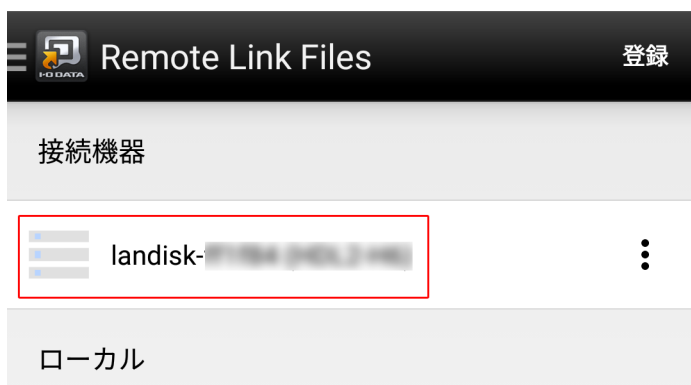


QRコードを読み込んでください



読み取り開始

6. 接続機器をタップ



iOS の場合

証明書のインストールを求められます。パスコードを求められたときは、端末のものを入力してください。

-  手動で登録

表示名：

landisk-

71194 (HOL2-H6)

PINコード：

52F7EEBDA09711E6B5BA34

① ユーザー名

パスワード

② 完了

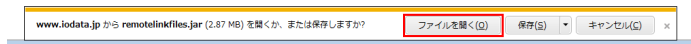
データの参照などの操作方法

▶ パソコンからアクセスする場合

- ## Javaランタイムが必要です

※Microsoft Edgeではご利用いただけません。Edge右上の  → [Internet Explorerで開く] の順にクリックし、Internet Explorerでご利用ください。

3. ダウンロードした「remotelinkfiles.jar」を開く



「remotelinkfiles.jar」を開けない

開くのにかかる場合があります。しばらくお待ちください。しばらく待っても次の画面が表示されない場合は、以下をお試しください。

- ① 「remotelinkfiles.jar」を右クリックし、[プロパティ] をクリック
- ② [全般] タブの「プログラム」が「Java(TM) ~」になっているかを確認する
- ③ 「Java(TM) ~」でない場合は[変更] をクリックし、一覧から「Java(TM) ~」を選ぶ
- ④ [この種類のファイルを開くときは、選択したプログラムをいつも使う] をチェックする
- ⑤ [OK] をクリック

便利な使い方

「remotelinkfiles.jar」を保存しておけば、次からは保存したファイルを開くだけで起動できます。

※接続できない場合は、バージョンアップされている可能性があります。この場合、再ダウンロードしてお試しください。

4. ①NASに設定した [ユーザー名] [パスワード] を入力

※入力するユーザー名/パスワードは、IOPortalの会員登録情報ではありません。

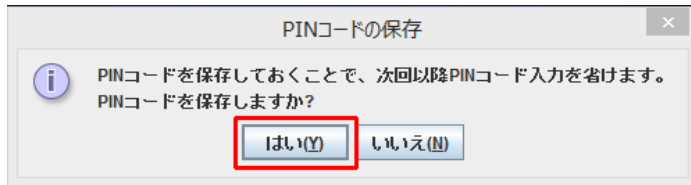
- ② 設定画面に表示のPINコードを入力
- ③ [ログイン] ボタンをクリック



ログインできない

- PINコード/ユーザー名/パスワードが間違っていないか、ご確認ください。
- ルーターのUPnPが有効になっていることを確認してください。方法は、ルーターの取扱説明書をご確認ください。

5. [はい] をクリック



次回からのPINコード入力

手順4の画面に自動的にPINコードが入力されます。

※「remotelinkfiles.jar」と同じ場所に「remotelinkfiles.bin」が保存されています。これを削除すると、PINコードの情報が消えてしまいます。

これでアクセスできるようになります。

データの参照などの操作方法について

[「Remote Link Files for PC」画面で見るマニュアル](#)をご覧ください。

端末認証機能

NASに登録された端末だけがアクセスできる共有フォルダーを設定する機能です。
端末認証用PINコード（QRコード）を発行し、端末からこの端末認証用PINコード（QRコード）で接続することで端末登録・認証がおこなわれます。

「端末認証機能」を「有効」にしたフォルダーは、端末認証機能で登録をした端末だけが参照可能になります。

Remote Link 3

接続情報更新: 成功

Remote Link 3

☒ 有効 ☐ 無効

端末認証機能

☒ 有効 ☐ 無効

一時公開機能

☐ 有効 ☒ 無効

[詳細項目を開く](#)

共有フォルダー名	Remote Link 3	端末認証機能
LAN DISK Log	☐ 有効	☐ 有効
LAN DISK Manual	☐ 有効	☐ 有効
disk1	☐ 有効	☐ 有効
disk2	☐ 有効	☐ 有効
usb1	☐ 有効	☐ 有効
usb2	☐ 有効	☐ 有効
usb3	☐ 有効	☐ 有効
usb4	☐ 有効	☐ 有効

適用

端末認証機能を有効にした場合

- ・ 端末認証機能が有効なフォルダーは、接続用PINコード（QRコード）で設定をした端末（[②端末の接続設定をおこなう](#)参照）で接続した場合、アクセスできません。
- ・ 端末認証用PINコード（QRコード）で接続した場合、他の端末への一時公開含むアクセス許可はできません。

[①認証した端末のみがアクセス可能なフォルダーを指定する](#)

[②端末を登録する](#)

① 認証した端末のみがアクセス可能なフォルダーを指定する

1. 「共有」 → 「Remote Link 3」 → 「設定」 をクリック

2. ① [端末認証機能] の [有効] を選ぶ
- ② 端末認証機能でアクセスを許可するフォルダーを選ぶ
- ③ [適用] をクリック

【端末認証機能】適用フォルダーの設定について

端末認証機能により登録した端末だけアクセスを認めるフォルダーにチェックをつけます。

端末認証機能を有効にしても、リストでチェックが外れているフォルダーは、端末認証制限がかかりません。

※ [端末認証機能] を [有効] にしたフォルダーは、[Remote Link 3] も [有効] にしてください。

※ フォルダーの数が多い場合は、[共有フォルダー名] 欄にフォルダー名の一部を入力すると、探しやすくなります。

▼ 設定による動作の違い

Remote Link 3	端末認証機能	動作
有効	有効	接続用PINコードの端末は、アクセス不可 端末認証用PINコードの端末は、アクセス可能
有効	無効	接続用PINコードの端末は、アクセス可能 端末認証用PINコードの端末は、アクセス可能
無効	有効	接続用PINコードの端末は、アクセス不可 端末認証用PINコードの端末は、アクセス不可

次に、[端末認証機能] による端末登録をおこないます。

② 端末を登録する

1. [共有] → [Remote Link 3] → [端末管理] をクリック
2. [端末登録用PINコードを生成する] をクリック

3. 登録する端末でRemote Link Filesを起動する
- ※ Remote Link Filesのヘルプをご確認ください。

4. 登録する端末で、QRコードを読み込むか、PINコードを入力する

※端末認証用PINコード（QRコード）は、1台だけ登録できます。2台目以降も登録する場合は、[続けて端末登録用PINコードを生成する]をクリックしてください。

その他の設定項目について

登録名

リスト表示時にわかりやすい名前をつけます。

メールアドレス

PINコードをメールで送ることができます。

登録する端末宛のメールアドレスを入力し、[PINコードをメールで送る] ボタンをクリックします。

この機能を利用するには、事前にLAN DISKの[メール設定]をおこなってください。

※メール設定をおこなう場合は、[メール設定ページへ移動]をクリックします。設定内容については、【画面で見るマニュアル】の【本製品の動きを通知する】をご覧ください。

[保存する] ボタンをクリックすると、設定した[登録名]と[メールアドレス]が保存されます。

登録したら、端末管理画面に[登録済]と表示されます。

[詳細] ボタンをクリックすると、登録名の変更やPINコードの再表示ができます。

登録を解除する場合は、チェックをつけ、[選択した対象を削除する]をクリックしてください。

一時公開機能

有効期限をつけて、ファイルやフォルダーのアクセスを制限する機能です。また、端末数や1ファイルあたりのアクセス回数でも制限ができます。

例えば、パーティー会場などでお客様に本日限定で写真を見られるようにするなど、一時的なアクセスを許可するような使い方ができます。接続用PINコードで設定したスマートフォン・タブレットからだけ設定可能です。設定方法は、Remote Link Filesのヘルプをご覧ください。

端末認証機能で認証されている端末からは設定できません

接続用PINコード（QRコード）で設定をした端末（[②端末の接続設定をおこなう](#)）から設定できます。

端末認証用PINコード（QRコード）で接続した場合、他の端末への一時公開含むアクセス許可はできません。

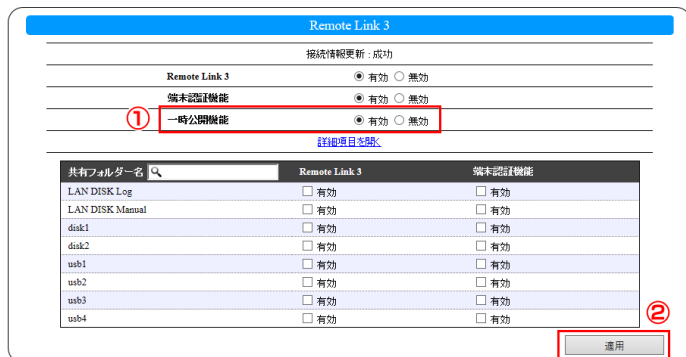
[一時公開機能を有効にする](#)

[一時公開の状況を確認する](#)

一時公開機能を有効にする

1. [共有] → [Remote Link 3] → [設定] をクリック

2. ① [一時公開機能] の [有効] を選ぶ
② [適用] をクリック



以上で、NAS側の設定は完了です。

一時公開の設定方法について

一時公開は、iOS版/Android版のRemote Link Filesで設定できます。設定方法は、Remote Link Filesのヘルプをご確認ください。

一時公開の状況を確認する

1. [共有] → [Remote Link 3] → [一時公開一覧] をクリック

2. 確認する接続の「詳細」をクリック

一時公開一覧

現在、一時公開機能は有効です。[設定ページへ移動](#)

公開パス	公開日時	公開ユーザー名	有効期限	アクセス可能端末台数	アクセス可能回数	操作
☐ disk1:photo/IMG...	2016/12/08 14:45:49	admin	2016/12/08	無制限	無制限	詳細

選択した対象を削除する

一時公開を解除する場合

解除する接続の☐にチェックをつけ、「選択した対象を削除する」をクリックしてください。

一時公開の詳細情報が表示されます。

一時公開

設定	
公開パス	disk1:photo
公開期限	2016/12/09
アクセス可能端末台数	無制限
アクセス可能回数	無制限

アクセス状況	
アクセス端末	
アクセス回数	disk1:photo/IMG_20160811_131504.jpg (1)

一覧へ戻る

AppleShareとは？

本パッケージを追加すると、Mac からAppleShare ネットワーク共有へのアクセスが可能になります。

アクセス権限の優先順位について

AppleShare ネットワーク共有

アクセス権の設定の優先順位は、以下の①②③の順に優先される設定になります。

- ① 共有フォルダーの読み取り専用設定
- ② 詳細アクセス権設定の読み取り設定（グループ・ユーザー）
- ③ 詳細アクセス権設定の読み書き設定（グループ・ユーザー）

AppleShare ネットワーク共有と他の共有サービスを組み合わせて使用する場合に、詳細アクセス権設定でグループ、ユーザーごとに個別にアクセス権を設定するには、以下のいずれかの方法ですべての共有サービスからのアクセス権限を統一できます。

- ◆ ユーザーとユーザーが属するグループに対して異なるアクセス権を設定しない
- ◆ 詳細アクセス権設定をすべてユーザーで指定する

設定例

以下のグループにアクセス権を設定する場合（※ user2 が重複していることに注意）

グループ名	所属するユーザー
ROgroup	user1,user2
RWgroup	user2,user3

例 1

グループ全体を読み取り権限に設定するが、グループ内の特定ユーザーのみを読み書き権限とする場合

共有フォルダー

share1（フォルダーの読み取り専用チェックなし、詳細設定有効）

許可したユーザー

〔読み書き〕 user1

許可したグループ

〔読み取り〕 ROgroup（user1、user2がメンバー）

結果

user1 読み取り

user2 読み取り

※ user1 は、読み書き指定よりも読み取り指定の方が優先のため、読み取りのアクセスとなります。

例 2

ユーザーおよびユーザが属するグループに異なるアクセス権を付与した場合

共有フォルダー

share1（フォルダーの読み取り専用チェックなし、詳細設定有効）

許可したユーザー

〔読み書き〕 user1

〔読み書き〕 user3

許可したグループ

- 〔読み取り〕 ROgroup (user1、user2がメンバー)
- 〔読み書き〕 RWgroup (user2、user3がメンバー)

結果

user1 読み取り
user2 読み取り
user3 読み書き

※ user1、user2 は、読み書き指定よりも読み取り指定の方が優先のため、読み取りのアクセスとなります。

例 3

複数グループにまたがるユーザーが存在し、かつ、それぞれのグループに異なるアクセス権を付与した場合

共有フォルダー

share1 (フォルダーの読み取り専用チェックなし、詳細設定有効)

許可したグループ

- 〔読み取り〕 ROgroup (user1、user2がメンバー)
- 〔読み書き〕 RWgroup (user2、user3がメンバー)

結果

user1 読み取り
user2 読み取り
user3 読み書き

※ user2 は、読み書き指定よりも読み取り指定の方が優先のため、読み取りのアクセスとなります。

例 4

共有フォルダーの読み取り専用チェックをつけた場合

共有フォルダー

share1 (フォルダーの読み取り専用チェックあり、詳細設定有効)

結果

すべてのユーザー 読み取り

※ 詳細アクセス権の設定なし、および、詳細アクセス権設定でユーザー、グループに対してどのような設定を実施しても、共有フォルダーの読み取り専用チェックが優先されます。

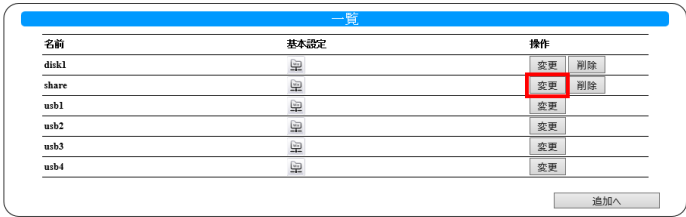
Mac からアクセス可能にする

あらかじめ作成済みの共有フォルダーをMac からのアクセス可能にする設定を説明します。
共有フォルダーの作成方法は、【画面で見るマニュアル】をご覧ください。

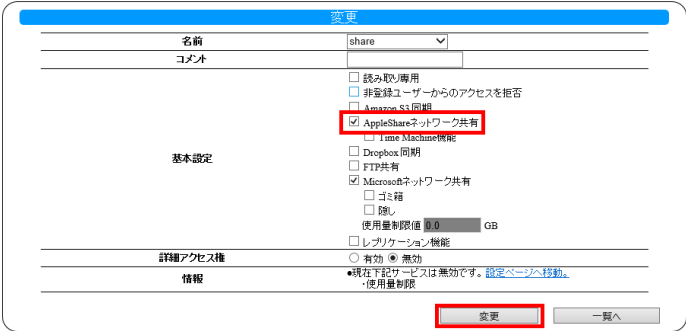
ご注意

ファイル数の多い共有フォルダーを変更すると、変更が完了するまでに時間がかかる場合があります。
また、変更が完了するまで共有フォルダーにはアクセスできません。

- 1. [共有] → [フォルダー] → [一覧] をクリック
- 2. 変更する共有フォルダーの [変更] ボタンをクリック



- 3. 「基本設定」の [AppleShare ネットワーク共有] にチェックをつけ、[変更] をクリック



以上で、AppleShare ネットワーク共有が有効になりました。

Mac から共有フォルダーにアクセスする

同じネットワークにあるMac から、本製品の共有フォルダーにアクセスする方法を説明します。

アクセス方法

1. Finder を開く

2. ①「共有」の [landisk-xxxxxx] をクリック

※ xxxxxx は、本製品のシールに記載のMAC アドレス下6 桁です。

② [別名で接続] をクリック



[landisk-xxxxxx]が見つからない、もしくは、接続できない

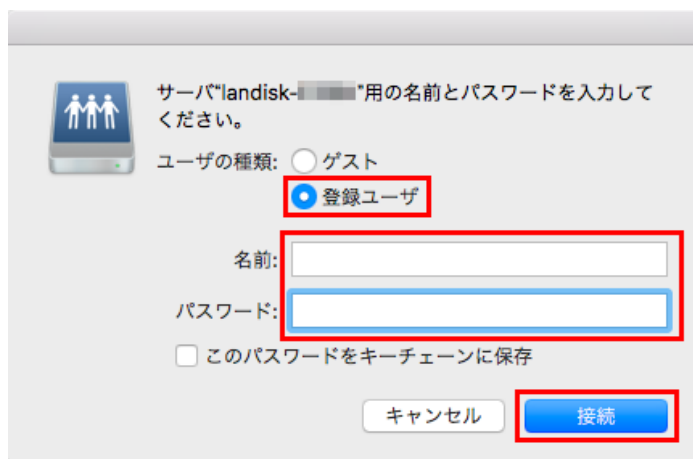
下の [\[LANDISK-xxxxxx\] が見つからない、接続できない](#) をご覧ください。

3. ① [登録ユーザ] を選ぶ

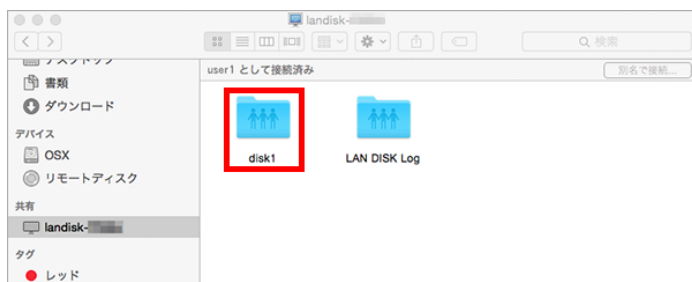
② アクセスのためのユーザー名（名前）とパスワードを入力

③ [接続] をクリック

⇒ 入力したユーザーで接続されます。



4. [disk1] をダブルクリック



これで、データを読み書きできます。

〔LANDISK-xxxxxx〕が見つからない、接続できない

- ◆ 正しく接続されていない可能性があります。
本製品の電源（ランプが緑点灯）、LANケーブルの接続、本製品を接続したブロードバンドルーターやハブ、LANポートのランプが点いていることをご確認ください。
- ◆ ファイアウォールソフトで、本製品のコンピューター名（初期値は「LANDISK-xxxxxx」）や本製品のIPアドレス（DHCPから自動取得）を使用できるように設定してください。（詳しくは、お使いのソフトウェアの取扱説明書をご覧ください。）
- ◆ 以下の操作をしてください。

① Finder の〔移動〕メニュー→〔サーバへ接続〕をクリック

② 〔サーバアドレス〕に〔landisk-xxxxxx〕をクリック

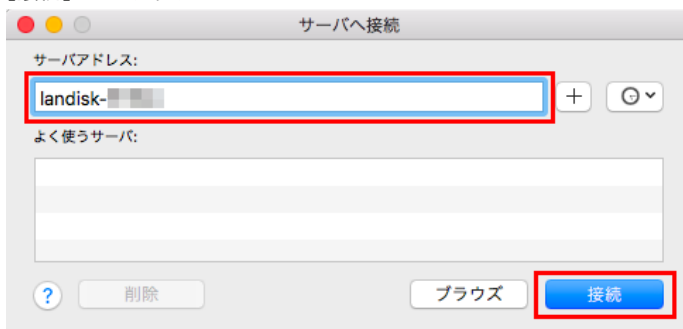
※ xxxxxx は、本製品のシールに記載のMAC アドレス下6 桁です。

※ 〔landisk-xxxxxx〕で接続できなかった場合は、代わりに「afp://（本製品のIPアドレス）」と入力してください。

入力例 afp://192.168.0.200/

本製品のIPアドレスは「Magical Finder」画面上に表示されます。

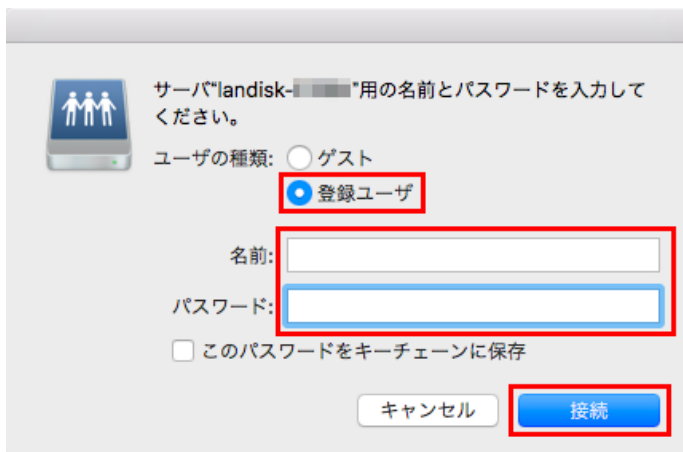
③ 〔接続〕をクリック



④ 〔登録ユーザ〕を選ぶ

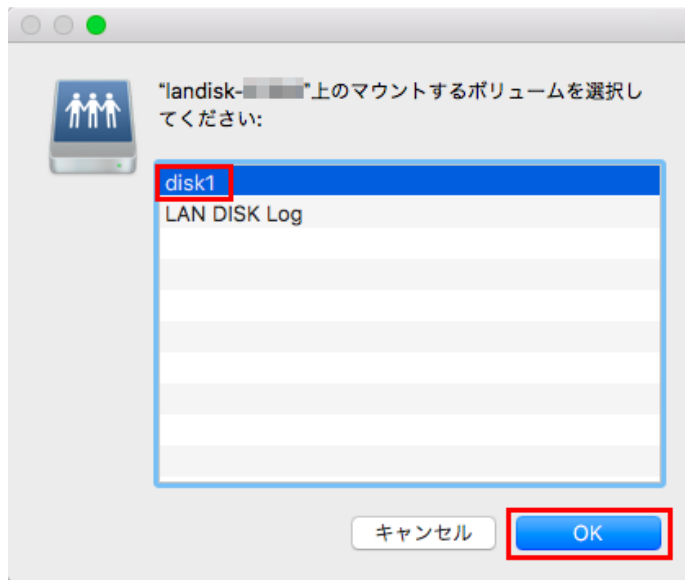
⑤ アクセスのためのユーザー名（名前）とパスワードを入力

⑥ 〔接続〕をクリック



⑦ 〔disk1〕を選ぶ

⑧ [OK] をクリック



Time Machine 設定をする

Mac のTime Machine 機能のバックアップディスクとして、NASの特定の共有フォルダーを使うことができます。

ご注意

- ◆ Time Machine設定をおこなうと、設定した保存先共有フォルダーに次のファイル・フォルダーが自動的に作成されます。
.com.apple.timemachine.supported (コンピューター名)_(MAC アドレス).sparsebundle
これらのファイル・フォルダーは Time Machine を動作させるために必要ですので、削除しないでください。
※ Time Machine設定を無効にした場合は、上記のファイル・フォルダーは削除しても問題ありません。
- ◆ ファイル数の多い共有フォルダーを変更すると、変更が完了するまでに時間がかかる場合があります。また、変更が完了するまで共有フォルダーにはアクセスできません。

NAS側の設定をする

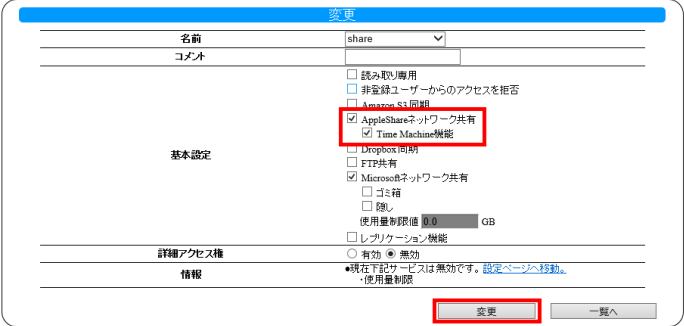
Mac 側の設定をする

NAS側の設定をする

1. [共有] → [フォルダー] → [一覧] をクリック
2. 変更する共有フォルダーの [変更] ボタンをクリック



3. 「基本設定」の [AppleShare ネットワーク共有] と [Time Machine 機能] にチェックをつけ、[変更] をクリック



以上で、NAS側の設定は完了です。

Mac 側の設定をする

1. [システム環境設定] → [Time Machine] を開く

2. スイッチを [入] にする

3. 保存先ディスクを選択する画面が開くので、NASの保存先共有フォルダーを指定する

以上で、設定は完了です。

一括登録をする

AppleShare に関する一括登録の記述例を説明します。

※ AppleShare 以外の一括登録の記述例や一括登録の方法については、【画面で見るマニュアル】をご覧ください。

設定書式カスタマイズ

共有フォルダー設定項目定義

フィールド名

AppleShare

設定項目

AppleShareネットワーク共有

値

1→有効、0→無効、（空）→無効

デフォルト値

無効

フィールド名

TimeMachine

設定項目

TimeMachine機能

値

1→有効、0→無効、（空）→無効

デフォルト値

無効

CSV ファイルの記述例

ケース 1

共有フォルダー項目定義レコードを使わない場合

設定内容

「Share1」という共有フォルダーを追加。
そのフォルダーは、
AppleShareネットワーク共有が有効、
TimeMachine機能が有効、
MSネットワーク共有が有効、
読み取り専用が無効
という設定にする。

上記設定内容のCSVファイル

addshare,Share1,コメント,,,,,1,,,1,,,,1,,,,,0

ケース 2

共有フォルダー項目定義レコードを使う場合

設定内容

「Share2」という共有フォルダーを追加。
そのフォルダーは、
AppleShareネットワーク共有が有効、

TimeMachine機能が有効、
MSネットワーク共有が有効、
読み取り専用が無効
という設定にする。

上記設定内容のCSVファイル

```
#share_config,Name,Comment,AppleShare,TimeMachine,Win,ReadOnly  
addshare,Share2,コメント,1,1,1,0
```

CSV一括登録でエラーが表示される場合

原因

「設定が不正です。」と表示される。

対処

設定値として以下の例のような不正な値が設定されています。CSV ファイルを修正してください。

例 1 :

使用量制限を0.1以上、かつAppleShareネットワーク共有を有効で設定している。

例 2 :

ゲストユーザー禁止を有効、かつAppleShareネットワーク共有を有効で設定している。

お問い合わせ

重要

- 本製品の修理対応、電話やメール等によるサポート対応、ソフトウェアのアップデート対応、本製品がサーバー等のサービスを利用する場合、そのサービスについては、弊社が本製品の生産を完了してから5年間を目途に終了とさせていただきます。ただし状況により、5年以前に各対応を終了する場合があります。
- 個人情報、株式会社アイ・オー・データ機器の[プライバシーポリシー](#)に基づき、適切な管理と運用をおこないます。

[弊社サポートページ](#)にて、以下をご確認ください

- ・「Q&A よくあるご質問」を参照
- ・最新のソフトウェアをダウンロード

それでも解決できない場合は、サポートセンターへ

電話:050-3116-3025

※受付時間 9:00～17:00 月～金曜日（祝祭日をのぞく）

インターネット: <http://www.iodata.jp/support/>

※ご用意いただく情報▷製品情報（製品名、シリアル番号など）、PCや接続機器の情報（型番、OSなど）

ソフトウェアライセンス情報

●本マニュアルで使用しているソフトウェアライセンス情報

jquery.min.js

jQuery v1.10.2 | (c) 2005, 2013 jQuery Foundation, Inc. | jquery.org/license
@ sourceMappingURL=jquery.min.map

jquery.cookie.js

jQuery Cookie Plugin v1.4.1
<https://github.com/carhartl/jquery-cookie>

Copyright 2006, 2014 Klaus Hartl
Released under the MIT license

jquery.easing.1.3.js

jQuery Easing v1.3 - <http://gsgd.co.uk/sandbox/jquery/easing/>

Uses the built in easing capabilities added In jQuery 1.1
to offer multiple easing options

TERMS OF USE - jQuery Easing

Open source under the BSD License.

Copyright c 2008 George McGinley Smith
All rights reserved.

jquery.lazyload.js

Lazy Load - jQuery plugin for lazy loading images
Copyright (c) 2007-2015 Mika Tuupola

Licensed under the MIT license:
<http://www.opensource.org/licenses/mit-license.php>

Project home:
<http://www.appelsiini.net/projects/lazyload>

Version: 1.9.5

jquery.hashchange.min.js

jQuery hashchange event, v1.4, 2013-11-29
<https://github.com/georgekosmidis/jquery-hashchange>

lity.js

Copyright (c) 2015-2016 Jan Sorgalla

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation Files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

本マニュアルのご利用について

● Google アナリティクスを利用した計測について

本マニュアルではサービス向上のため、Google アナリティクス を使用しております。

これによって、データ収集のためにGoogleがお使いのWebブラウザーにcookie を設定したり、既存のcookie を読み取ったりする場合があります。

また、本マニュアルをご利用中のWebブラウザーは、Googleに特定の非個人情報（IPアドレスやアクセスしたウェブページのアドレスなど）を自動的に送信します。

弊社はそれらの情報を、マニュアル利用状況の把握やユーザー体験の改善といった用途で利用いたします。

利用者は、本マニュアルを利用することで、上記方法および目的においてGoogleと弊社がおこなう、こうしたデータ処理に対して許可を与えたものとみなします。

※ なお「cookie」は、お客様がWebブラウザーを設定することで拒否できる場合があります。

その場合、本マニュアルの機能が一部利用できなくなるおそれがあります。

設定方法については、Webブラウザーのヘルプなどをご覧ください。

