

SONY®

OPTICAL DISC ARCHIVE FILE MANAGER2

ODS-FM2



警告

安全のための注意事項を守らないと、火災や人身事故になることがあります。

このインストールガイドには、事故を防ぐための重要な注意事項と製品の取り扱いかたを示してあります。**このインストールガイドをよくお読みのうえ**、製品を安全にお使いください。お読みになったあとは、いつでも見られるところに必ず保管してください。



Optical Disc Archive

INSTALLATION GUIDE Japanese

1st Edition (Revised 3)

権利者の許諾を得ることなく、付属のソフトウェアおよび取扱説明書の内容の全部または一部を複製すること、および付属のソフトウェアを賃貸に使用することは、著作権法上禁止されております。

© 2018 Sony Imaging Products & Solutions Inc.

ソフトウェアを使用したことによるお客様の損害、または第三者からのいかなる請求についても、当社は一切その責任を負い兼ねます。

ハードウェアにトラブルが発生して記録内容の修復が不可能になった場合、当社は一切その責任を負い兼ねます。

万一、製造上の原因による不良がありましたらお取り替えいたします。それ以外の責はご容赦ください。

付属のソフトウェアは、指定された装置以外には使用できません。

付属のソフトウェアの仕様は、改良のため予告なく変更することがありますが、ご了承ください。

商標について

- Microsoft、Windows、Internet Explorer、および Microsoft Edge は、米国 Microsoft Corporation の米国およびその他の国における登録商標です。
- Intel、Intel Core はアメリカ合衆国およびその他の国における Intel Corporation またはその子会社の商標または登録商標です。
- Apple、macOS、OS X および Safari は、米国および他の国々で登録された Apple Inc. の商標です。
- Chrome は、Google Inc. の登録商標です。
- SmartDocs は Teknowmics Co. Inc. の商標または登録商標です。
- その他、本書に記載されている商品名、会社名等は、その会社の登録商標または商標です。

目次

特長	4
システム構成	4
動作環境	6
コントロール PC	6
クライアント PC	6
ネットワークについてのご注意	7
準備	7
オプティカルディスクアーカイブシステムの準備	7
ODS-FM2 の設定	8
ファイアウォールの設定	14
HTTPS 通信の設定	15
Web 画面の表示	18

特長

ODS-FM2は、オプティカルディスクアーカイブシステムでアーカイブやリトリブを行うためのソフトウェアです。オプティカルディスクアーカイブシステムに挿入されているカートリッジだけでなく、棚管理を行っているカートリッジについても管理できます。

ODS-FM2の操作はWeb画面で行います。クライアントPCからWebブラウザを使ってアクセスします。

このインストレーションガイドでは、ODS-L10やODS-L30M¹⁾に接続して使用する場合およびコンピューターにドライブユニットを直接接続して使用する場合のインストール方法について説明します。

1) ODS-L60EやODS-L100Eを接続して使用することもできます。

システム構成

ODS-FM2を使用する場合の基本的なシステム構成を以下に示します。

ODS-FM2をインストールしたコンピューターをコントロールPCと呼びます。コントロールPCをオプティカル

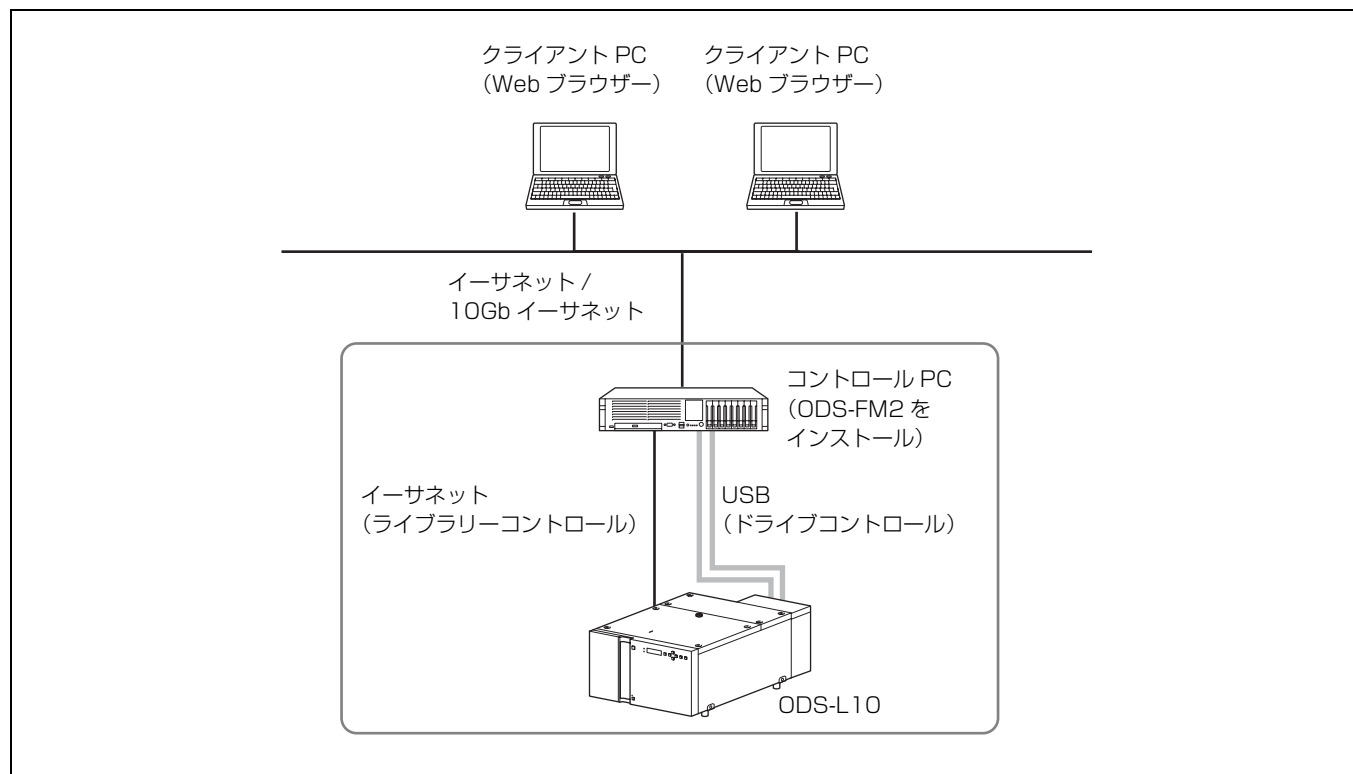
ディスクアーカイブシステムに接続し、オプティカルディスクアーカイブシステムの制御を行います。ODS-FM2の操作は、クライアントPCのWebブラウザからアクセスして行います。

ODS-L10と接続する場合

コントロールPCは、ODS-L10が接続されているネットワークと、クライアントPCやネットワークストレージがあるネットワークの2つのネットワークと接続します。また、ODS-L10に搭載されたドライブユニットとUSBで接続します。

ご注意

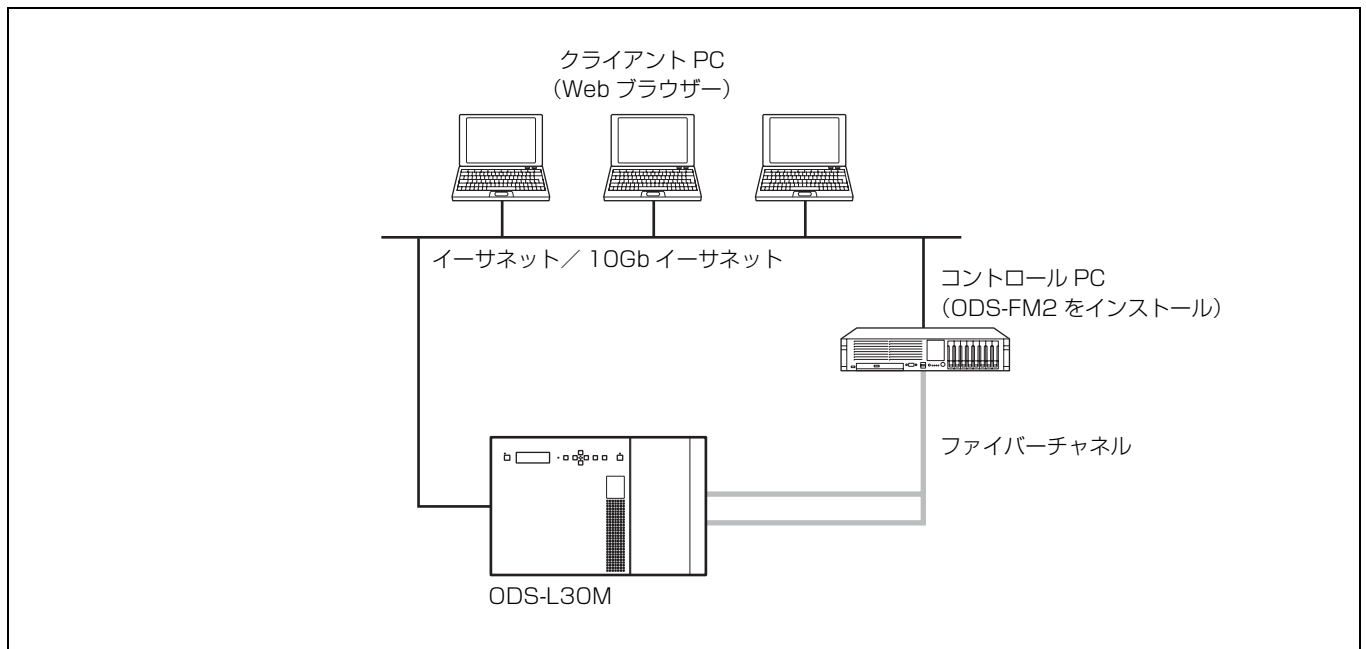
ODS-L10と接続した場合は、Virtual Tapeモードは使用できません。



ODS-L30M と接続する場合

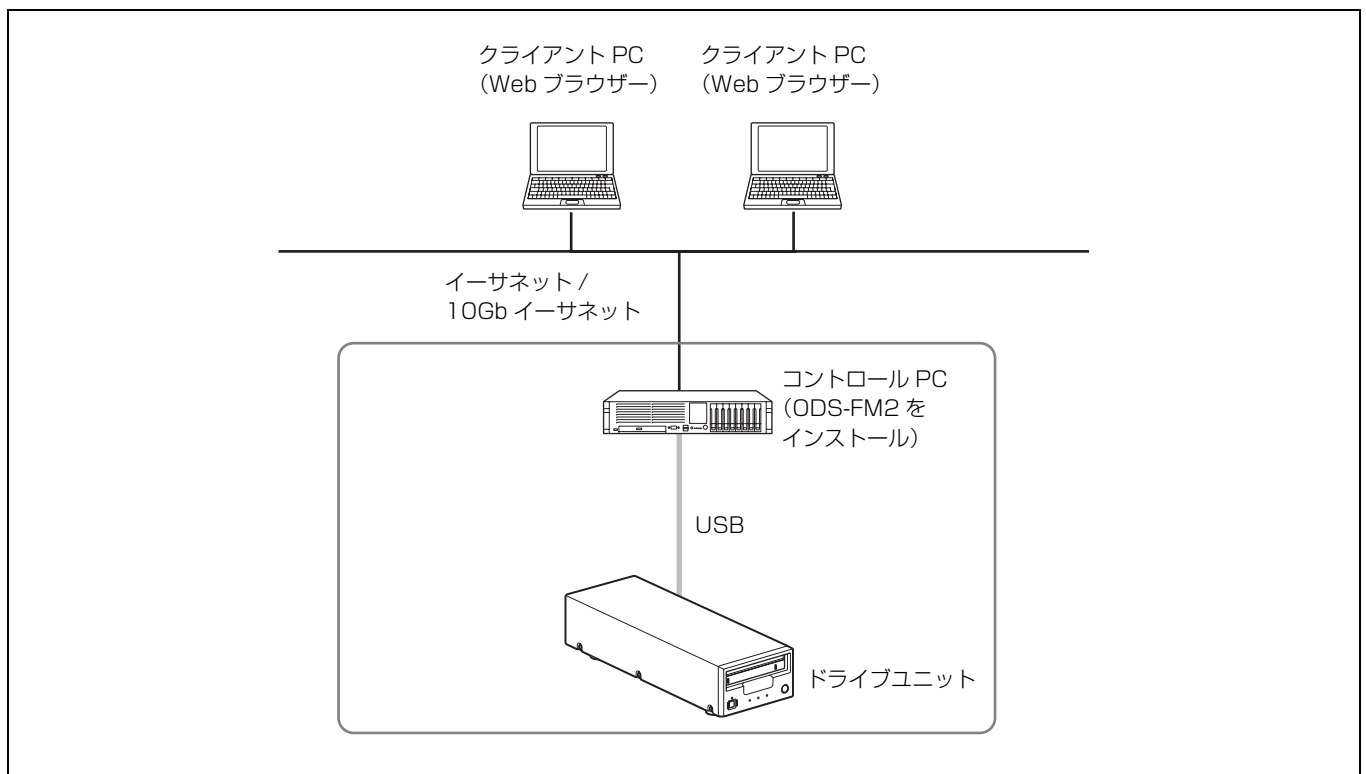
ODS-L30M に搭載されたドライブユニットとコントロール PC (サーバー) をファイバーチャネルで接続します。

また、クライアント PC があるネットワークとコントロール PC を、イーサネット で接続します。



ドライブユニットを直接接続する場合

コントロール PC とドライブユニットを USB で接続します。また、コントロール PC をクライアント PC やネットワークストレージがあるネットワークに接続します。



動作環境

コントロール PC、およびクライアント PC に必要な動作環境を以下に示します。

コントロール PC

選択する動作モードによって、必要な動作環境が異なります。メモリーおよび HDD 容量の要件は、Optical Disc Archive Software に必要な容量を除いた値です。

File Manager モード

CPU	Intel Core i5 3 GHz 以上
メモリー	8 GB
HDD 容量	200 GB (ローカル HDD のファイルをアーカイブしたり、ローカル HDD にリトリーブする場合は、さらに 4TB × ドライブ数の容量が必要)

OS

- ODS-L10 またはドライブユニットと接続する場合：
Windows 10 64 ビット版
- ODS-L30M と接続する場合：
Windows Server 2012
Windows Server 2012 R2
Windows Server 2016
Windows Server 2019

インターフェース

- ODS-L10 と接続する場合：
Ethernet × 2 (クライアント PC および ODS-L10 接続用)
USB × ドライブ数
- ODS-L30M と接続する場合：
Ethernet × 1 (クライアント PC および ODS-L30M 接続用)
ファイバーチャネル HBA (Host Bus Adapter)
- ドライブユニットを直接接続する場合：
Ethernet × 1 (クライアント PC 接続用)
USB × ドライブ数

File Server モード

CPU	Intel Core i5 3 GHz 以上
メモリー	16 GB
HDD 容量	200 GB + (4 TB × ドライブ数)
OS	Windows Server 2012 Windows Server 2012 R2 Windows Server 2016 Windows Server 2019

インターフェース

- ODS-L10 と接続する場合：
Ethernet × 2 (クライアント PC および ODS-L10 接続用)
USB × ドライブ数
- ODS-L30M と接続する場合：
Ethernet × 1 (クライアント PC および ODS-L30M 接続用)
ファイバーチャネル HBA (Host Bus Adapter)
- ドライブユニットを直接接続する場合：
Ethernet × 1 (クライアント PC 接続用)
USB × ドライブ数

Virtual Tape モード

CPU	Intel Core i5 3 GHz 以上
メモリー	4 GB
HDD 容量	なし (Optical Disc Archive Software に必要な容量のみ)
OS	Windows Server 2012 R2 Windows Server 2016 Windows Server 2019

インターフェース

- ODS-L30M と接続する場合：
Ethernet × 1 (クライアント PC および ODS-L30M 接続用)
ファイバーチャネル HBA (Host Bus Adapter)
- ドライブユニットを直接接続する場合：
Ethernet × 1 (クライアント PC 接続用)
USB × ドライブ数

ご注意

各ドライブユニットが対応する USB インターフェースについては、ドライブユニットのオペレーションマニュアルをご覧ください。

クライアント PC

ハードウェア	以下の OS および Web ブラウザーが問題なく動作すること
OS	Windows 7、Windows 8.1、Windows 10 macOS 10.13、10.14、10.15
Web ブラウザー	Microsoft Internet Explorer 11、Microsoft Edge、Google Chrome、Safari 11/12/13

ネットワークについてのご注意

使用環境によってはネットワーク上の意図せぬ第三者からアクセスされる可能性があります。ネットワークに接続する際には、セキュアなネットワークであることをご確認のうえご使用ください。

準備

ここでは、ODS-FM2 をコントロール PC にインストールし、ODS-FM2 でオプティカルディスクアーカイブシステムを使用できるようにするための設定手順を説明します。

ご注意

- ODS-L10/ODS-L30M のファームウェアを最新のものに更新してください。
- Optical Disc Archive Software およびドライブのファームウェアを最新のものに更新してください。

オプティカルディスクアーカイブシステムの準備

コントロール PC を ODS-L10 に接続する場合

- ◆ ODS-L10 の操作について詳しくは、ODS-L10 のインストールマニュアルおよびオペレーションマニュアルをご覧ください。

1 ODS-L10 にドライブユニットを取り付ける。

ODS-L10 には、ODS-D55U または ODS-D77U を 2 台まで取り付けることができます。ODS-D280U/D380U やファイバーチャネルを使用するモデルを取り付けることはできません。

2 ODS-L10 の IP アドレスを設定する。

- ◆ 設定方法について詳しくは、ODS-L10 のオペレーションマニュアルをご覧ください。

3 コントロール PC に Optical Disc Archive Software をインストールする。

4 コントロール PC に ODS-FM2 をインストールする。

インストーラーの指示に従ってインストールしてください。

5 ODS-L10 に取り付けられたドライブユニットとコントロール PC を USB ケーブルで接続する。

ドライブユニットが 2 台取り付けられている場合は、両方のドライブユニットをコントロール PC と接続します。

6 コントロール PC のネットワークポートに ODS-L10 があるネットワークを接続する。

ネットワークの設定について詳しくは、Windows のドキュメントをご覧ください。

- 7 ODS-L10 にオプティカルディスクカートリッジを入れる。

コントロール PC を ODS-L30M に接続する場合

- ◆ ODS-L30M の操作について詳しくは、ODS-L30M のオペレーションマニュアルをご覧ください。

- 1 ODS-L30M にドライブユニット ODS-D77F/D280F/D380F を取り付ける。

ODS-L30M には、ODS-D77F/D280F/D380F を組み合わせて 2 台まで取り付けることができます。3 台以上取り付けたい場合は、ソニーのサービス担当者にご連絡ください。

ご注意

ODS-D77F、ODS-D280F、ODS-D380F が混在している構成では、Virtual Tape モードを使用することができません。Virtual Tape モードを使用する場合は、いずれか 1 機種だけを使った構成にしてください。

- 2 ODS-L30M の IP アドレスを設定する。

- ◆ 設定方法について詳しくは、ODS-L30M のオペレーションマニュアルをご覧ください。

- 3 コントロール PC に Optical Disc Archive Software をインストールする。

- 4 コントロール PC に ODS-FM2 をインストールする。

インストーラーの指示に従ってインストールしてください。

- 5 ODS-L30M に取り付けられたドライブユニットとファイバーチャネルスイッチを接続する。

ドライブユニットが 2 台取り付けられている場合は、両方のドライブをファイバーチャネルスイッチと接続します。

- 6 コントロール PC をファイバーチャネルスイッチと接続する。

- 7 ODS-L30M にオプティカルディスクカートリッジを入れる。

コントロール PC にドライブユニットを直接接続する場合

- 1 コントロール PC に Optical Disc Archive Software をインストールする。

- 2 コントロール PC に ODS-FM2 をインストールする。

インストーラーの指示に従ってインストールしてください。

- 3 コントロール PC とドライブユニットを USB ケーブルで接続する。

- 4 ドライブユニットにオプティカルディスクカートリッジを入れる。

ODS-FM2 の設定

ODS-FM2 の設定およびアクティベーションは、Library Software Configuration Tool で行います。

ご注意

アクティベーションを行う際にインターネットへの接続が必要になります。コントロール PC がインターネットに接続されていない場合は、インターネットに接続できる他の PC を用意してください。

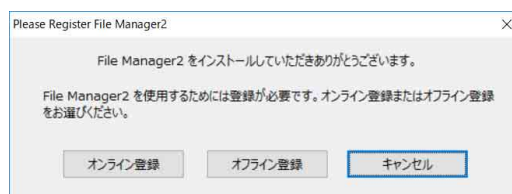
- 1 コントロール PC で、スタートから [Config Tool] を選択するか、C:\Program Files\Sony\ODAFFileManager2\odafm\ConfigTool.exe をダブルクリックして、Library Software Configuration Tool を起動する。

Library Software Configuration Tool は、管理者権限を持つアカウントで実行してください。

- 2 ODS-FM2 のライセンスアクティベーションを行っていない場合は、ライセンスアクティベーションを行う。

コントロール PC がインターネットに接続されている場合

- ① [オンライン登録] をクリックする。



② 必要事項を入力して、[次へ] をクリックする。

③ シリアル番号を入力して、[次へ] をクリックする。
アクティベーションが行われ、Library Software Configuration Tool が起動します。

コントロール PC がインターネットに接続されていない場合

- ① [オフライン登録] をクリックする。
- ② [オフライン登録] ダイアログに表示された URL を、インターネットに接続されている PC の Web ブラウザーで表示させる。

- ③ Web ページにシリアルナンバーとコンピューター ID ([オフライン登録] ダイアログに表示されている) を入力し、認証コードを取得する。
- ④ コントロール PC の [オフライン登録] ダイアログに認証コードを入力し、[登録] ボタンをクリックする。
アクティベーションが行われ、Library Software Configuration Tool が起動します。

3 [次へ] をクリックする。

4 Select System 画面で接続するシステムを選択する。
ドライブユニットと直接接続する場合は、「Direct Mode」を選択します。

5 Select Mode 画面で、利用するモードを選択し、[次へ] をクリックする。

File Server モードを選択した場合は、次の「File Server モードの設定」に進んでください。

Virtual Tape モードを選択した場合は、「Virtual Tape モードの設定」(12 ページ)に進んでください。

File Manager モードを選択した場合は、「全モード共通の設定」(13 ページ)に進んでください。

ご注意

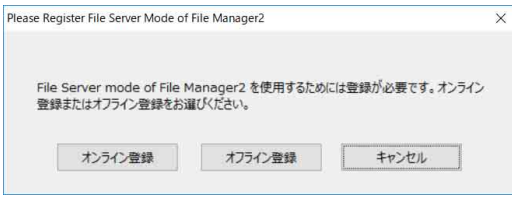
- 手順 4 で ODS-L10 を選択した場合、Virtual Tape モードは選択できません。
- Virtual Tape モードを選択する場合は、[次へ] をクリックする前に仮想テープを使用しているアプリケーションを終了してください。なお、Virtual Tape モードを選択して [次へ] をクリックすると、仮想テープを使用しているアプリケーションが終了しているかどうかにかかわらず、注意を促すダイアログが表示されます。

File Server モードの設定

1 File Server モードのライセンスアクティベーションを行っていない場合は、ライセンスアクティベーションを行う。

コントロール PC がインターネットに接続されている場合

- ① [オンライン登録] をクリックする。



- ② 必要事項を入力して、[次へ] をクリックする。



- ③ シリアル番号を入力して、[次へ] をクリックする。
File Server モードのライセンスアクティベーションが行われます。

コントロール PC がインターネットに接続されていない場合

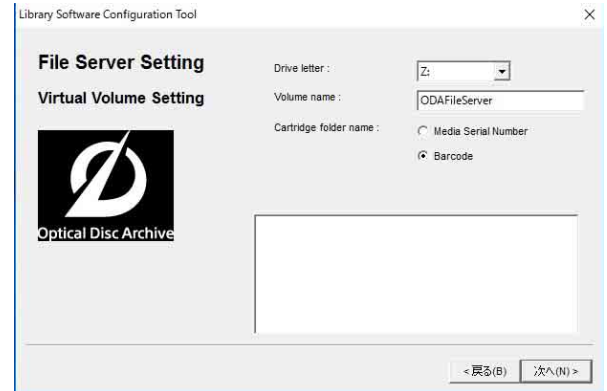
- ① [オフライン登録] をクリックする。
- ② [オフライン登録] ダイアログに表示された URL を、インターネットに接続されている PC の Web ブラウザーで表示させる。



- ③ Web ページにシリアルナンバーとコンピューター ID ([オフライン登録] ダイアログに表示されている) を入力し、認証コードを取得する。

- ④ コントロール PC の [オフライン登録] ダイアログに認証コードを入力し、[登録] ボタンをクリックする。
File Server モードのライセンスアクティベーションが行われます。

- 2 File Server Setting 画面でファイルサーバーのボリュームを設定する。



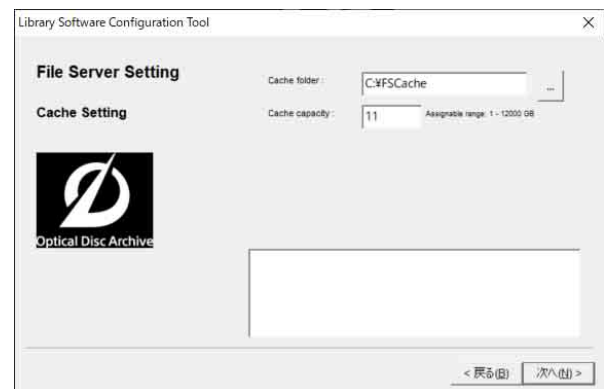
Drive letter : ファイルサーバーのドライブレターを選択します。

Volume name : ボリュームラベルを設定します。

Cartridge folder name : カートリッジフォルダー名を選択します。

- 3 ボリュームの設定が終わったら、[次へ] をクリックする。
- 4 ファイルサーバーのキャッシュフォルダーとキャッシュ容量を設定する。

ファイルサーバーでは書き込まれたファイルを一時的にキャッシュフォルダーに保存します。



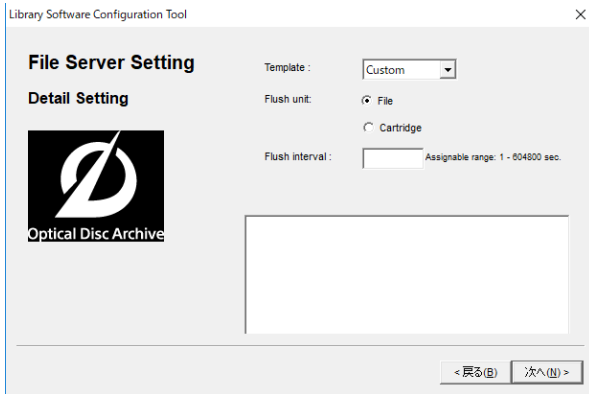
Cache folder : キャッシュフォルダーとして使用するフォルダーを設定します。

Cache capacity : 保存されるキャッシュファイルの上限サイズを設定します。

ご注意

キャッシュフォルダのパスは、ボリュームが他のアプリケーションに使用されないように専用のディスクまたはパーティションを用意することを推奨します。

- 5 キャッシュフォルダとキャッシュ容量の設定が終わったら、[次へ] をクリックする。
- 6 ファイルサーバーの詳細を設定する。



Template：ファイルサーバーを使用するアプリケーションに適した設定テンプレートを選択します。手動で設定する場合は [Custom] を選択してください。

Flush unit：キャッシュからカートリッジへと書き込む同期処理をファイル単位で登録するか、カートリッジ単位で登録するかを設定します。

- File：ファイルが最後に更新されてから経過した時間をファイルごとに管理し、その数値が [Flush interval] を上回ると、そのファイルを同期するためのアーカイブジョブが登録されます。
- Cartridge：ファイルが最後に更新されてから経過した時間をカートリッジごとに管理し、その数値が [Flush interval] を上回ると、更新されたファイルを同期するためのアーカイブジョブがまとめて登録されます。

Flush interval：仮想ボリュームにファイルを書き込み終えてから、あるいは最後に更新されてから、キャッシュ上のファイルをカートリッジに同期するまでの時間を設定します。

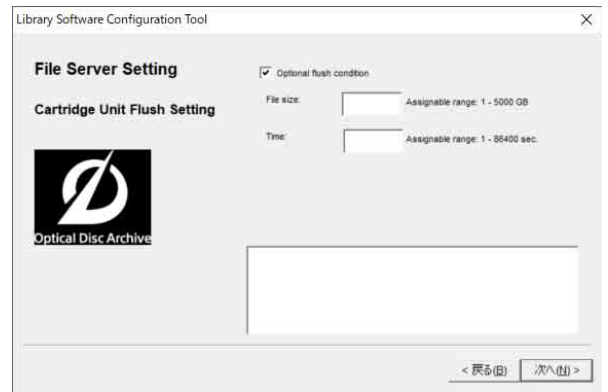
- 7 キャッシュの詳細設定が終わったら、[次へ] をクリックする。

[Flush unit] で [Cartridge] を選択した場合は、手順 8 に進んでください。

[Flush unit] で [File] を選択し、かつ [Template] で [SmartDocs] を選択した場合は、手順 10 に進んでください。

[Flush unit] で [File] を選択し、かつ [Template] で [Custom] を選択した場合は、「全モード共通の設定」(13 ページ) に進んでください。

- 8 カートリッジ単位の同期の設定をする。



Optional flush condition：この設定は同期単位がカートリッジ単位の場合のみ有効です。この設定をオンにすると、[Flush interval] に基づいてアーカイブジョブを登録する通常の条件に加えて、更新されるファイルサイズの総量に応じて早く同期を実施することができるようになります。

同期を開始していないファイルの総サイズが [File size] で設定した値を超え、かつファイルの書き込みや更新が無いまま [Time] で設定した時間が経過した場合に、同期のためのアーカイブジョブを登録します。

- 9 カートリッジ単位の同期の設定が終わったら、[次へ] をクリックする。

[Template] で [SmartDocs] を選択した場合は、手順 10 に進んでください。

[Template] で [Custom] を選択した場合は、「全モード共通の設定」(13 ページ) に進んでください。

- 10 設定テンプレート固有の設定を行います。



Cache capacity for scan：SmartDocs のスキャン機能で使用するキャッシュ容量を設定します。手順 4 の [Cache capacity] とは独立した容量が、同じボリュームに予約されます。

[Cache Clear] ボタン：スキャン用キャッシュ容量の中のファイルを削除し、使用されている領域を解放します。

11 テンプレート固有の設定が終わったら、[次へ] をクリックする。

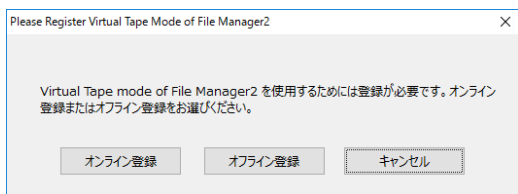
この後は、「全モード共通の設定」(13 ページ)に進んでください。

Virtual Tape モードの設定

1 Virtual Tape モードのライセンスアクティベーションを行っていない場合は、ライセンスアクティベーションを行う。

コントロール PC がインターネットに接続されている場合

① [オンライン登録] をクリックする。



② 必要事項を入力して、[次へ] をクリックする。

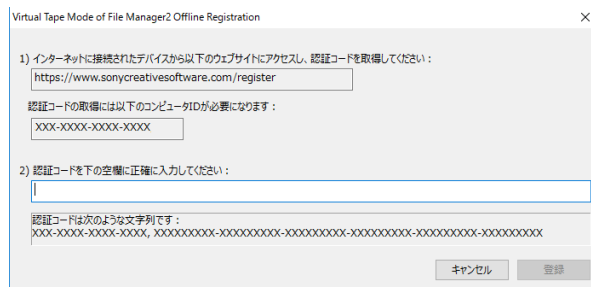


③ シリアル番号を入力して、[次へ] をクリックする。
Virtual Tape モードのライセンスアクティベーションが行われます。

コントロール PC がインターネットに接続されていない場合

① [オフライン登録] をクリックする。

② [オフライン登録] ダイアログに表示された URL を、インターネットに接続されている PC の Web ブラウザーで表示させる。



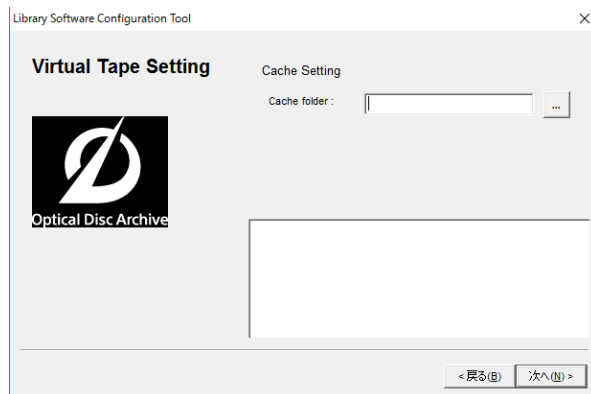
③ Web ページにシリアルナンバーとコンピューター ID ([オフライン登録] ダイアログに表示されている) を入力し、認証コードを取得する。

④ コントロール PC の [オフライン登録] ダイアログに認証コードを入力し、[登録] ボタンをクリックする。
Virtual Tape モードのライセンスアクティベーションが行われます。

2 Virtual Tape Setting 画面でキャッシュフォルダーのパスを設定する。

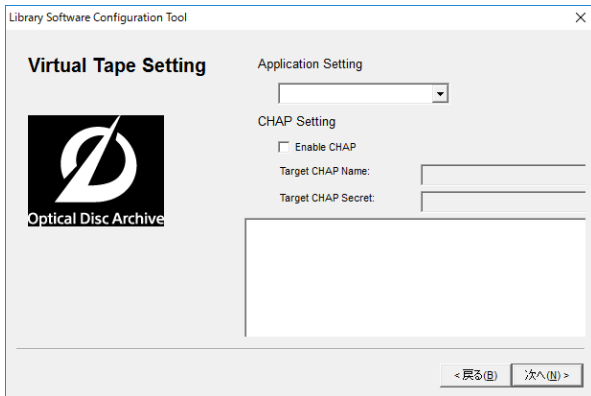
ご注意

キャッシュフォルダーのパスは、ボリュームが他のアプリケーションに使用されないように専用のディスクまたはパーティションを用意することを推奨します。



3 キャッシュフォルダーのパスの設定が終わったら、[次へ] をクリックする。

4 使用するアプリケーションおよびCHAPの設定をする。



Application Setting：仮想テープを使用するアプリケーションをドロップダウンリストから選択します。

Enable CHAP：CHAPによるユーザー認証を有効にする場合は、チェックボックスをチェックします。

Target CHAP Name：認証に使用するユーザー名です。制御文字を除く1文字以上256文字以下のASCII文字列を入力してください。

Target CHAP Secret：認証に使用するパスワードです。制御文字を除く12文字以上16文字以下のASCII文字列を入力してください。

5 アプリケーションとCHAPの設定が終わったら、[次へ]をクリックする。

6 マルチイニシエーターの有効/無効の設定をする。



[Enable Multi-Initiator] をチェックすると、複数クライアントからの同時接続が可能になります。チェックしない場合は、1つのクライアントが接続していると他のクライアントは接続できません。

7 マルチイニシエーターの設定が終わったら、[次へ]をクリックする。

この後は、次の「全モード共通の設定」に進んでください。

全モード共通の設定

1 Database Initialization 画面で [次へ] をクリックする。

データベースの初期設定が自動的に行われます。Select System 画面で「Direct Mode」または「ODS-L30M」を選択した場合は、手順5に進んでください。「ODS-L10」を選択した場合は、次の手順に進んでください。

2 ODS-L10で設定したIPアドレスとODS-L10にログインするためのログイン名(ユーザー名)/パスワードを入力し、[次へ]をクリックする。

ODS-L10と接続します。正常に接続すると、Drive Setting ページが表示されます。

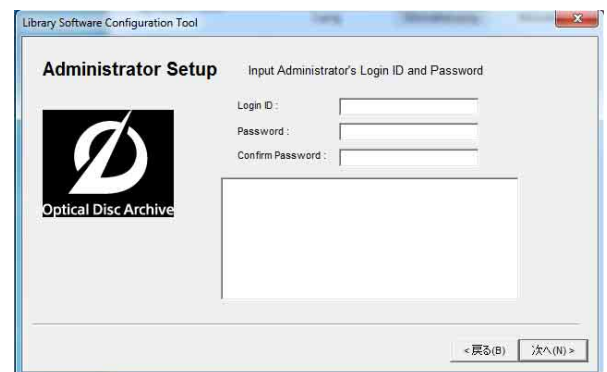
3 ドライブのチェックを行うため、ODS-L10に取り付けられていないドライブユニットがコントロールPCに接続されている場合は、コントロールPCから取り外す。

4 [次へ] をクリックする。

ドライブのチェックが開始されます。ODS-L10に取り付けたドライブユニットが1台だけの場合は、上下どちらのスロットに取り付けたかを確認するメッセージが表示されます。下のスロットに取り付けた場合は「はい」を、上のスロットに取り付けた場合は「いいえ」をクリックしてください。ドライブのチェックが完了すると、Administrator Setup 画面が表示されます。

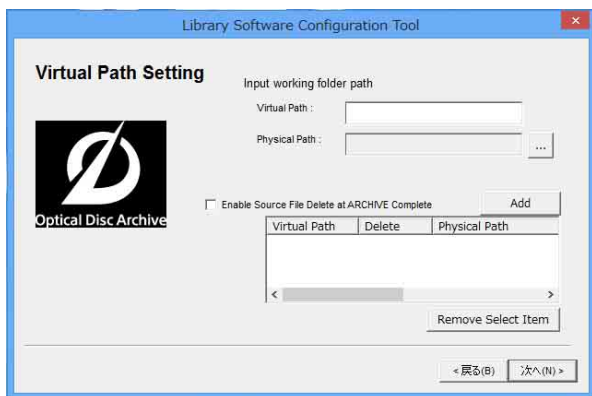
5 ODS-FM2にログインする際に使用するアカウントを作成する。ログインIDとパスワードを入力し、[次へ]をクリックする。

File Manager モードを選択した場合は、手順6、7でルートフォルダー(ベースパス)を設定してください。File Server モードまたはVirtual Tape モードを選択した場合は、手順8に進んでください。



6 ODS-FM2 のアーカイブ画面に表示するルートフォルダー（ベースパス）を設定する。

アーカイブ画面には、指定したベースパス以下のファイル/フォルダーのみが表示されます。公開するフォルダーを制限することで、システムファイルなどを誤って変更することを防げます。ベースパスは複数指定することができます。



Virtual Path：ベースパスをアーカイブ画面に表示するときの名称を入力します。

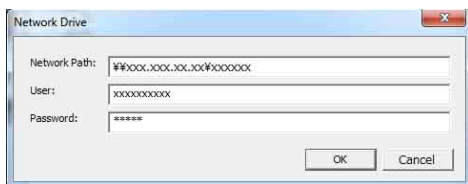
Physical Path：公開するベースパスの物理パスを指定します。ネットワークドライブも指定できます。

Enable Source File Delete at ARCHIVE Complete：アーカイブ後に自動的にファイルを削除する場合に選択します。選択しない場合は、アーカイブされたファイルが削除されずに残るため、必要に応じて手作業で削除してください。

Add ボタン：指定した内容でベースパスを追加します。追加したベースパスは、下のリストに表示されます。

ネットワークドライブを指定するには

- ① [Physical Path] の [...] ボタンをクリックする。
- ② [Reference] ダイアログで [Network Drive] ボタンをクリックする。
- ③ [Network Drive] ダイアログの [Network Path] にネットワークドライブのパスを UNC 形式 (¥¥サーバー名またはサーバーの IP アドレス¥¥フォルダー名) で入力する。



- ④ ユーザー名とパスワードが必要な場合は、[User] [Password] に入力する。
- ⑤ [OK] ボタンをクリックする。追加したネットワークドライブが [Reference] ダイアログに表示されます。

- ⑥ ネットワークドライブを選択し、[Select] ボタンをクリックする。

[Reference] ダイアログが閉じ、選択したネットワークドライブのパスが Virtual Path Setting ページの [Physical Path] に表示されます。

- ⑦ [Virtual Path] を設定し、[Add] ボタンをクリックする。

- 7 ベースパスの設定が終わったら、[次へ] をクリックする。

- 8 完了画面が表示されるので、[完了] をクリックする。

- 9 コントロール PC のネットワークポートに、クライアント PC があるネットワークを接続する。

ODS-L10 と接続している場合は、ODS-L10 のあるネットワークとは別のポートを使用してください。

クライアント PC で Web 画面を表示して、オプティカルディスクアーカイブシステムを操作できるようになります。

ご注意

- コントロール PC にウイルス対策ソフトなどのセキュリティソフトがインストールされている場合、クライアント PC から 8080 ポートへのインバウンドアクセスがブロックされる場合があります。このような場合は、セキュリティソフトでポート 8080 へのインバウンドアクセスを許可するよう設定してください。設定方法については、セキュリティソフトの取扱説明書をご覧ください。
- ハードウェア構成を変更した場合やドライブユニットの接続を変更した場合は、ODS-FM2 が正常に動作しなくなります。Library Software Configuration Tool で再度 ODS-FM2 の設定を行ってください。
- ODS-L10 および ODS-L30M の Web 画面の Setup Menu や本体前面のディスプレイで各種設定を変更した場合は Library Software Configuration Tool で再度 ODS-FM2 の設定を行ってください。
- ODS-FM2 を使用している場合は、Optical Disc Archive Filer を起動できません。Optical Disc Archive Filer を使用する場合は、ODS-FM2 のサービスを停止してから起動してください。(Optical Disc Archive Filer は、Optical Disc Archive Software に含まれています)

ファイアウォールの設定

外部からの MariaDB への接続をブロックするために、以下のファイアウォール設定を行うことを推奨します。

- 1 [コントロールパネル] > [システムとセキュリティ] > [Windows ファイアウォール] > [詳細設定] > [受信の規則] > [新しい規則...] を選択する。

2 新規の受信の規則ウィザードで、以下を設定する。

- 規則の種類：[ポート] を選択
- プロトコルおよびポート：[TCP]、[特定のローカルポート]（ポートに「3306」を指定）を選択
- 操作：[接続をブロックする] を選択
- プロファイル：すべてをチェック
- 名前：「MariaDBPort」を入力

3 [完了] をクリックする。

4 再度、[新しい規則...] を選択して、新規の受信の規則ウィザードを表示し、以下を設定する。

- 規則の種類：[ポート] を選択
- プロトコルおよびポート：[UDP]、[特定のローカルポート]（ポートに「3306」を指定）を選択
- 操作：[接続をブロックする] を選択
- プロファイル：すべてにチェック
- 名前：「MariaDBPort」を入力

5 [完了] をクリックする。

HTTPS 通信の設定

HTTPS 通信の設定をすることで、通信を暗号化できるようになります。

キーストアファイルの生成

1 コマンドプロンプトを起動する。

2 以下のコマンドを入力する。

```
cd C:\Program Files\Zulu\zulu-8-jre\bin
keytool -genkey -alias tomcat -keyalg RSA -keysize 2048
-keystore <キーストアファイル名>
```

キーストアファイル名の例：

```
filemanager2.keystore
```

3 キーストアのパスワードを設定するプロンプトが表示されたら、パスワードを入力する。

```
Enter keystore password: *****
(パスワードは表示されません)
```

4 確認入力を促すプロンプトが表示されたら、同じパスワードを再入力する。

```
Re-enter new password: *****
(パスワードは表示されません)
```

5 CSR に指定する情報を入力する。

入力例：

```
What is your first and last name?
[Unknown]: www.sony.jp
What is the name of your organizational unit?
[Unknown]: File Manager2
What is the name of your organization?
[Unknown]: Sony Imaging Products & Solutions Inc.
What is the name of your City or Locality?
[Unknown]: Minato-ku
What is the name of your State or Province?
[Unknown]: Tokyo
What is the two-letter country code for this unit?
[Unknown]: JP
```

6 入力した情報が下記のように表示されたら、内容を確認して、「yes」と入力する。

```
Is CN=www.sony.jp, OU=File Manager2, O=Sony Imaging
Products & Solutions Inc., L=Minato-ku, ST=Tokyo, C=JP
correct?
[no]: yes
```

7 下記のプロンプトが表示されたら、何も入力せずリターンキーを押す。

```
Enter key password for (RETURN if same as keystore
password):
```

手順 2 で指定したファイル名で、キーストアファイルが作成されます。

CSR の生成

1 コマンドプロンプトを起動する。

2 以下のコマンドを入力する。

```
cd C:\Program Files\Zulu\zulu-8-jre\bin
keytool -certreq -sigalg SHA1withRSA -alias tomcat -file
<CSR ファイル名> -keystore <キーストアファイル名>
```

CSR ファイル名の例：

```
filemanager2.csr
```

3 プロンプトが表示されたら、キーストアファイル作成時に指定したパスワードを入力する。

```
Enter keystore password: *****
```

手順 2 で指定したファイル名で、CSR ファイルが生成されます。

サーバ証明書の発行

生成した CSR を認証局に渡して、署名されたサーバ証明書を発行してもらいます。

アプリケーションで使うサーバ証明書の生成

- 1 署名されたサーバ証明書と中間証明書を任意のディレクトリに配置する。
- 2 コマンドプロンプトを起動する。
- 3 署名されたサーバ証明書と中間証明書を一つのファイルにする。

copy <署名済みのサーバ証明書ファイル名> + <中間証明書ファイル名> <アプリケーションで使うサーバ証明書ファイル名>

アプリケーションで使うサーバ証明書ファイル名の例：
filemanager2.cer

証明書のインストール

- 1 以下のコマンドを入力する。

keytool -import -alias tomcat -keystore <キーストアファイル名> -file <前項の手順 3 で作成したファイル名>
- 2 プロンプトが表示されたら、キーストアファイル作成時に指定したパスワードを入力する。

Enter keystore password: *****
- 3 以下のようなプロンプトが表示された場合には「yes」と入力する。

```
Top-level certificate in reply:
Owner: CN=*****, O=*****, C=**
Issuer: OU=*****, O=*****, C=**
Serial number: *****
Valid from: ***** until: *****
Certificate fingerprints:
MD5: *****
... is not trusted. Install reply anyway? [no]: yes
```

実際には、**には登録されている情報が表示されます。

HTTPSの有効化

- 1 Tomcat サービスを停止する。
 - ① [スタート] メニューから [Windows 管理ツール] > [サービス] をクリックする。
 - ② サービス一覧から「Apache Tomcat」という名前のサービスを探し、クリックする。
 - ③ サービス一覧の左側の [サービスの停止] をクリックする。

- 2 Tomcat の設定ファイル (server.xml) を編集する。

- ① C:\Program Files\Apache Software Foundation\Tomcat 7.0\conf\server.xml を開き、85 行目付近のコメントアウトされている箇所を有効にする。
- ② 「変更後」の内容をコピーする。
- ③ <キーストアファイル名>に実際のキーストアファイル名をフルパスで入力し、<キーストアのパスワード>にキーストアファイル作成時に指定したパスワードを入力する。

変更前

```
<!--
<Connector port="8443" protocol="HTTP/1.1"
SSLEnabled="true"
    maxThreads="150" scheme="https" secure="true"
    clientAuth="false" sslProtocol="TLS" />
-->
```


変更後

```
<Connector port="8443"
  protocol="org.apache.coyote.http11.Http11Protocol"
  SSLEnabled="true"
  maxThreads="150"
  scheme="https"
  secure="true"
  keystoreFile=" <キーストアファイル名> "
  keystorePass=" <キーストアのパスワード> "
  clientAuth="false"
  sslProtocol="TLSv1.2"
  sslEnabledProtocols="TLSv1.1,TLSv1.2"
  ciphers="TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
    TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
    TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384,
    TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384,
    TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
    TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
    TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256,
    TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256,
    TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
    TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,
    TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
    TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA,
    TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384,
    TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384,
    TLS_ECDH_RSA_WITH_AES_256_CBC_SHA,
    TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA,
    TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
    TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,
    TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
    TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,
    TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256,
    TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256,
    TLS_ECDH_RSA_WITH_AES_128_CBC_SHA,
    TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA"
/>
```

HTTP 通信を禁止する場合は、70 行目付近の以下をコメントアウトします。

変更前

```
<Connector port="8080" protocol="HTTP/1.1"
  connectionTimeout="20000"
  redirectPort="8443"
  useBodyEncodingForURI="true" />
```

変更後

```
<!--
<Connector port="8080" protocol="HTTP/1.1"
  connectionTimeout="20000"
  redirectPort="8443"
  useBodyEncodingForURI="true" />
-->
```

3 Tomcat サービスを起動する。

- ① [スタート] メニューから [Windows 管理ツール]
> [サービス] をクリックする。

- ② サービス一覧から「Apache Tomcat」という名前のサービスを探し、クリックする。

- ③ サービス一覧の左側の [サービスの開始] をクリックする。

4 Config Tool を実行する。

5 HTTPS 通信の確認を行なう。

Web ブラウザーを起動して「https:// <ドメイン名> :8443」にアクセスし、ログイン画面が表示されることを確認してください。

Web 画面の表示

HTTPS 通信の設定をしていない場合

クライアント PC で Web ブラウザーを表示し、アドレス欄に「http:// (コントロール PC の IP アドレス) :8080/」を入力します。

Web ブラウザーがコントロール PC に接続されると、ログイン画面が表示されます。Library Software Configuration Tool で設定したユーザー名とパスワードを入力してログインします。

HTTPS 通信の設定が済んでいる場合

クライアント PC で Web ブラウザーを表示し、アドレス欄に「https:// <ドメイン名> :8443/」を入力します。

Web ブラウザーがコントロール PC に接続されると、ログイン画面が表示されます。Library Software Configuration Tool で設定したユーザー名とパスワードを入力してログインします。

