CHAPTER 17

DLP A1 ～ A99

DLP-A1 シェルフ アセンブリの開梱と確認

目的	この作業では、パッケージからシェルフ アセンブリを取り出します。
工具 / 機器	なし
事前準備手順	なし
必須 / 適宜	必須
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

ステップ 1 設置場所で ONS 15454 システム機器を受け取ったら、箱の上部を開きます。Cisco Systems のロゴがある側が箱の上部です。

ステップ 2 箱から発砲スチロールを取り出します。箱には、ONS 15454 シェルフ（ビニールで包装されています）と、設置に必要な部品を含む小さい箱が入っています。

ステップ 3 シェルフを取り出します。その際、シェルフ取り出しストラップの両方のリングを持って、シェルフを箱の外にゆっくりと持ち上げます。

ステップ 4 設置用の部品が入った小さな箱を開き、「シスコが提供する部品」（p.1-3）に示されている品目がすべて揃っていることを確認します。

（注） ファン トレイ アセンブリは、同梱されていません。

ステップ 5 元の NTP（手順）に戻ります。

DLP-A2 シェルフ アセンブリの検査

目的	この作業では、シェルフ アセンブリのすべての部品が適切な状態であることを確認します。
工具 / 機器	前面扉用ピン付き六角（アレン）キー
事前準備手順	「DLP-A1 シェルフ アセンブリの開梱と確認」（p.17-1）
必須 / 適宜	必須
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

ステップ 1　ピン付き六角キーを使用してシェルフを開きます。詳細については、「DLP-A8 前面扉のオープン」（p.17-10）を参照してください。

ステップ 2　次の点を確認します。

- ピンが曲がっていたり、壊れていたりしない。
- フレームが曲がっていない。

ステップ 3　ピンが曲がっているか壊れている場合やフレームが曲がっている場合は、シスコの販売担当者に連絡して交換してください。

ステップ 4　設置する前に、前面扉を閉じます。

ステップ 5　元の NTP（手順）に戻ります。

DLP-A3 19 インチ（482.6 mm）ラックに適合させるためのマウント ブラケットの反転

目的	この作業では、マウント ブラケットを取り付けて、23 インチ（584.2 mm）ラックを 19 インチ（482.6 mm）ラックに変換します。
工具 / 機器	#2 プラス ドライバ 中型スロット ヘッド ネジ用ドライバ 小型スロット ヘッド ネジ用ドライバ
事前準備手順	なし
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

注意　圧着部品は ONS 15454 の付属品のみを使用し、ハードウェアおよび結合部の緩み、劣化、電気機械的な腐食がないよう注意してください。

注意　ONS 15454 を不導体コーティング（塗料、ラッカー、またはエナメルなど）を施したフレームに取り付ける場合は、ONS 15454 梱包キットに付属の溝付きネジを使用するか、または溝からコーディングを除去して、電位差が生じないようにします。

ステップ 1　シェルフ アセンブリの片側から、マウント ブラケットの取り付けネジを取り外します。

ステップ 2　取り外したマウント ブラケットを上下逆さまにします。

マウント ブラケットに刻まれた文字も逆さまになります。

ステップ 3　マウント ブラケットの幅広の面がシェルフ アセンブリと接するように合わせます（図17-1を参照）。

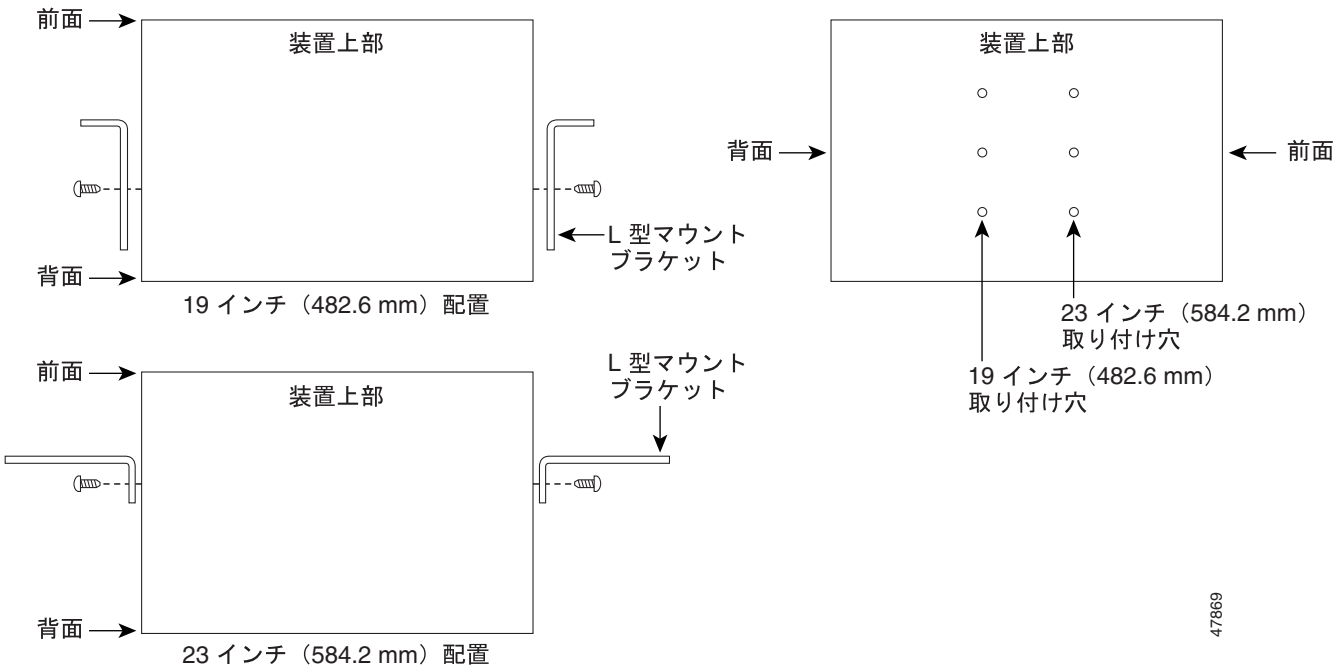
マウント ブラケットの幅が狭い面が、シェルフ アセンブリの前面を向くようにします。マウント ブラケットに刻まれた文字が逆さまに見える位置になります。

ステップ 4　マウント ブラケットのネジ穴をシェルフ アセンブリのネジ穴に合わせます。

ステップ 5　ステップ 1 で取り外したネジを差し込んで、締めます。

ステップ 6　反対側のマウント ブラケットにもこの作業を繰り返します。

図 17-1　マウント ブラケットの反転（23 インチ［584.2-mm］配置から 19 インチ［482.6-mm］配置へ）



ステップ 7　元の NTP（手順）に戻ります。

DLP-A4 外部ブラケットおよびエアー フィルタの取り付け

目的	この作業では、ファン トレイ アセンブリの下でなくシェルフの底部に、外部ブラケットおよびエアー フィルタを取り付けます。シェルフの底部に外部ブラケットおよびエアー フィルタを取り付けると、エアー フィルタを扱うときに、ファン トレイ アセンブリを取り外す必要がなくなります。
工具 / 機器	#2 プラス ドライバ 中型スロット ヘッド ネジ用ドライバ 小型スロット ヘッド ネジ用ドライバ
事前準備手順	DLP-A3 19 インチ（482.6 mm）ラックに適合させるためのマウント ブラケットの反転（p.17-3）（必要に応じて）
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

（注） ブラケットを取り付けない場合は、エアー フィルタをシェルフ アセンブリの底部にあるコンパートメントにスライドさせて、取り付けます。これ以降は、エアー フィルタを取り外して取り付け直すたびに、まずファン トレイ アセンブリを取り外す必要があります。シェルフ アセンブリのいずれのフィルタ位置にも、エアー フィルタを取り付けないでください。

ステップ 1　ファン トレイ アセンブリを取り外した状態のまま、ONS 15454 を水平な場所に逆さまに置きます。

（注） フィルタはどちらの側を正面にして取り付けても機能しますが、フィルタの表面を保護するために、押え金具を表向きにしてフィルタを取り付けることを推奨します。

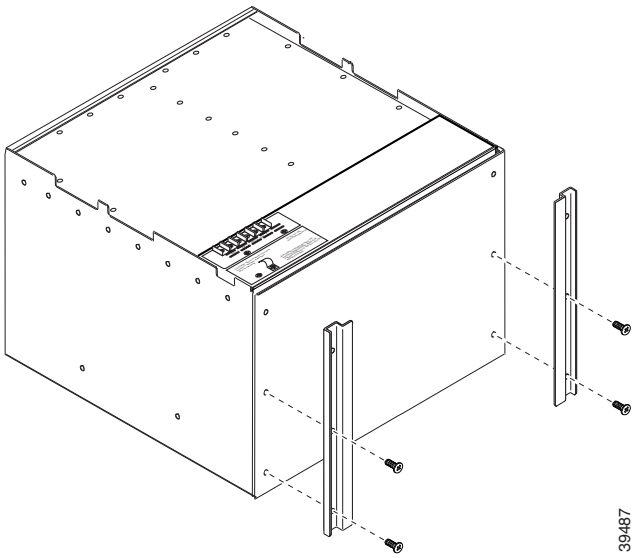
ステップ 2　シェルフ アセンブリ底部の左右両側に並んでいる 3 つのネジ穴を確認します。

ステップ 3　バックプレーン スタンドオフ キット（53-0795-XX）に付属のネジ（48-0003）を使用して、シェルフ アセンブリの底部に各ブラケットを固定します。

各ブラケットの一端には、フィルタ ストッパとフランジがあります。ストッパとフランジがシェルフ アセンブリの背面（取り付け時に ONS 15454 を逆さまにした場合は、上部）を向くようにブラケットを取り付けます

図 17-2 に、底部ブラケットの取り付け方法を示します。これ以降、ブラケットを使用しない場合は、ファン トレイ アセンブリを取り外してから、エアー フィルタを取り外す必要があります。ブラケットを使用すると、ファン トレイ アセンブリを取り外さなくても、エアー フィルタを清掃したり、交換することができます。

図 17-2　外部ブラケットの取り付け



ステップ 4　エアー フィルタをシェルフ アセンブリにスライドします。

ステップ 5　元の NTP（手順）に戻ります。

DLP-A5 ラックへのシェルフ アセンブリの取り付け（1 人で作業する場合）

目的	この作業では、シェルフ アセンブリを 1 人でラックに取り付けます。
工具 / 機器	ピン付き六角レンチ 固定ネジ（48-1003-XX）（2） 取り付け用プラスなべネジ（48-1004-XX、48-1007-XX）（8） #2 プラス ドライバ
事前準備手順	「DLP-A3 19 インチ（482.6 mm）ラックに適合させるためのマウント ブラケットの反転」（p.17-3）（必要に応じて） 「DLP-A4 外部ブラケットおよびエアー フィルタの取り付け」（p.17-5）（必要に応じて）
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

ステップ 1　上部取り付けスペースに、適切なヒューズ アラーム パネルが取り付けられていることを確認します。ヒューズ アラーム パネルが取り付けられていない場合は、メーカーの指示に従って取り付けます。

- 15454-SA-ANSI または 15454-SA-HD シェルフ アセンブリを取り付ける場合は、100 A ヒューズ パネル（シェルフごとに最低 30 A のヒューズ）が必要。
- 15454-SA-NEBS3 シェルフ アセンブリを取り付ける場合は、標準の 80 A ヒューズ パネル（シェルフごとに最低 20 A のヒューズ）が必要。

ステップ 2　シェルフ アセンブリが、適切なラック サイズに合わせてあることを確認します（23 インチ［584.2 mm］または 19 インチ［482.6 mm］）。

ステップ 3　アセンブリに付属している六角レンチを使用して、シェルフの取り付けに使用しないネジ穴に 2 本の固定ネジを取り付けます。ネジをしっかりと差し込んで、マウント ブラケットを固定します。

ステップ 4　シェルフ アセンブリを目的のラック位置まで持ち上げて、固定ネジの上に置きます。

ステップ 5　マウント ブラケットのネジ穴をラックの取り付け穴の位置に合わせます。

ステップ 6　プラス ドライバを使用して、アセンブリの両側にそれぞれ取り付けネジを 1 本取り付けます。

ステップ 7　シェルフ アセンブリをラックに固定したら、残りの取り付けネジを取り付けます。

（注）　1 組以上の水平ネジ穴を使用して、ONS 15454 が滑らないようにします。

ステップ 8　六角レンチを使用して、仮留め用のネジを取り外します。

ステップ 9　元の NTP（手順）に戻ります。

DLP-A6 ラックへのシェルフ アセンブリの取り付け（2 人で作業する場合）

目的	この作業では、シェルフ アセンブリを 2 人でラックに取り付けます。
工具 / 機器	ピン付き六角レンチ 固定ネジ（48-1003-XX）（2） 取り付け用プラスなべネジ（48-1004-XX、48-1007-XX）（8） #2 プラス ドライバ
事前準備手順	「DLP-A3 19 インチ（482.6 mm）ラックに適合させるためのマウント ブラケットの反転」（p.17-3）（必要に応じて） 「DLP-A4 外部ブラケットおよびエアー フィルタの取り付け」（p.17-5）（必要に応じて）
必須 / 適宜	必須
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

ステップ 1　上部取り付けスペースに、適切なヒューズ アラーム パネルが取り付けられていることを確認します。ヒューズ アラーム パネルが取り付けられていない場合は、メーカーの指示に従って取り付けます。

- 15454-SA-ANSI または 15454-SA-HD シェルフ アセンブリを取り付ける場合は、100 A ヒューズ パネル（シェルフごとに最低 30 A のヒューズ）が必要。
- 15454-SA-NEBS3 シェルフ アセンブリを取り付ける場合は、標準の 80 A ヒューズ パネル（シェルフごとに最低 20 A のヒューズ）が必要。

ステップ 2　シェルフ アセンブリが、適切なラック サイズに合わせてあることを確認します（23 インチ［584.2 mm］または 19 インチ［482.6 mm］）。

ステップ 3　シェルフ アセンブリに付属している六角レンチを使用して、シェルフの取り付けに使用しないネジ穴に 2 本の固定ネジ（48-1003-XX）を取り付けます。固定ネジを差し込んで、マウント ブラケットをしっかり固定します。

ステップ 4　シェルフ アセンブリを目的のラック位置まで持ち上げます。

ステップ 5　マウント ブラケットのネジ穴をラックの取り付け穴の位置に合わせます。

ステップ 6　1 人がシェルフ アセンブリを適切な位置に保持している間に、もう 1 人がプラス ドライバを使用して、アセンブリの両側へ取り付けネジを 1 本ずつ取り付けます。

ステップ 7　シェルフ アセンブリをラックに固定したら、残りの取り付けネジを取り付けます。

（注）　1 組以上の水平ネジ穴を使用して、ONS 15454 が滑らないようにします。

ステップ 8　六角レンチを使用して、仮留め用のネジを取り外します。

ステップ 9　元の NTP（手順）に戻ります。

DLP-A7 ラックへの複数のシェルフ アセンブリの取り付け

目的	この作業では、複数のシェルフをラックに取り付けます。
工具 / 機器	#2 プラス ドライバ 中型スロット ヘッド ネジ用ドライバ 小型スロット ヘッド ネジ用ドライバ
事前準備手順	「DLP-A3 19 インチ（482.6 mm）ラックに適合させるためのマウント ブラケットの反転」（p.17-3）（必要に応じて） 「DLP-A4 外部ブラケットおよびエアー フィルタの取り付け」（p.17-5）（必要に応じて）
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

（注） ONS 15454 のファン吸気口にエアフローを取り入れるには、設置されたシェルフ アセンブリの下に 1 インチ（25.4 mm）の隙間が必要です。シェルフ アセンブリの下に別の ONS 15454 を設置する場合は、下部シェルフ アセンブリの上にあるエアー ランプによって必要なスペースが確保されます。ただし、サードパーティ製の機器の上に ONS 15454 を取り付けた場合は、サードパーティ製シェルフ アセンブリと ONS 15454 の底部との間に、1 インチ（25.4 mm）以上の隙間を確保する必要があります。サードパーティ製の機器から ONS 15454 に熱気が排出されないようにしてください。

ステップ 1　上部取り付けスペースに、適切なヒューズ アラーム パネルが取り付けられていることを確認します。ヒューズ アラーム パネルが取り付けられていない場合は、メーカーの指示に従って取り付けます。

- 15454-SA-ANSI または 15454-SA-HD シェルフ アセンブリを取り付ける場合は、100 A ヒューズ パネル（シェルフごとに最低 30 A のヒューズ）が必要。
- 15454-SA-NEBS3 シェルフ アセンブリを取り付ける場合は、標準の 80 A ヒューズ パネル（シェルフごとに最低 20 A のヒューズ）が必要。

ステップ 2　最初の ONS 15454 を、ヒューズ アラーム パネルの下に直接取り付けます。「DLP-A5 ラックへのシェルフ アセンブリの取り付け（1 人で作業する場合）」（p.17-7）または「DLP-A6 ラックへのシェルフ アセンブリの取り付け（2 人で作業する場合）」（p.17-8）に従ってください。

ステップ 3　残りのシェルフにこの作業を繰り返します。

ステップ 4　元の NTP（手順）に戻ります。

DLP-A8 前面扉のオープン

目的	この作業では、キャビネット コンパートメントの前面扉を開く方法を示します。
工具 / 機器	ピン付き六角キー
事前準備手順	なし
必須 / 適宜	必須
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

（注） ONS 15454 には静電気防止用リスト ストラップが付属していて、その差し込み口があります。リスト ストラップのプラグ差し込み口は、シェルフ アセンブリの右下外側の端にあります。上部および下部に［ESD］というラベルが付いています。ONS 15454 で作業をする際は、必ず静電気防止用リスト ストラップを着用し、ストラップを ESD プラグに接続してください。

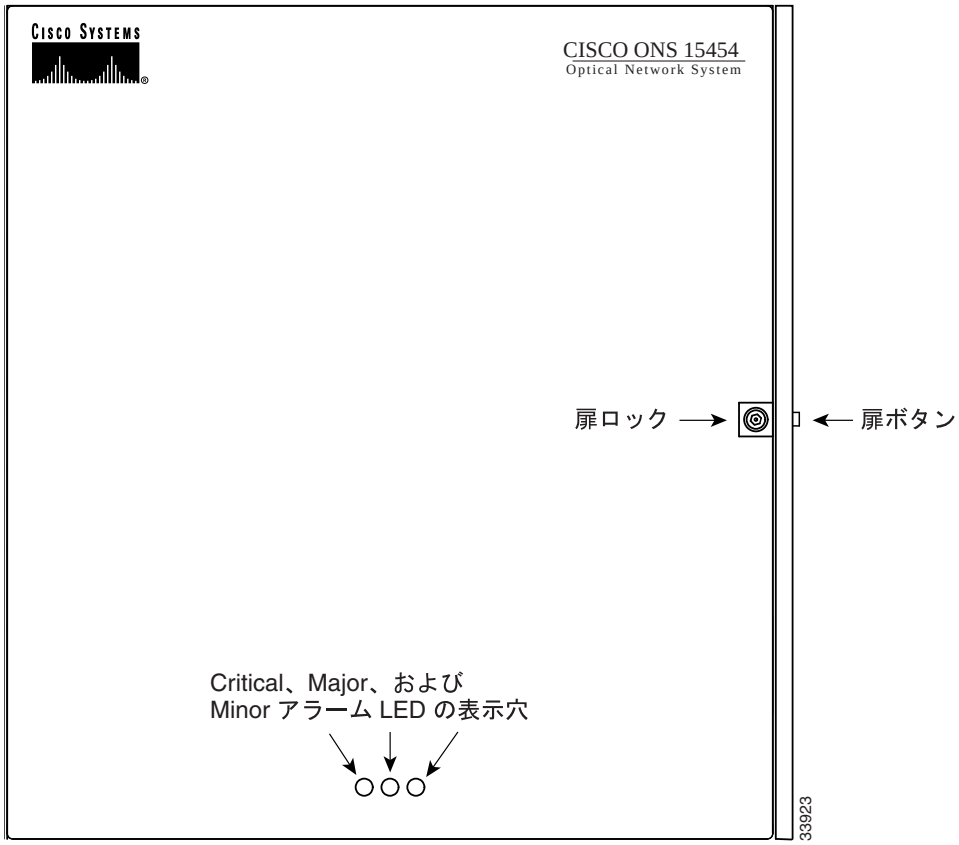
ステップ 1　前面扉のロックを解除します（図 17-3）。

ONS 15454 には、前面扉の鍵を開閉するためのピン付き六角キーが付属しています。キーを左回りに回転させると扉がロック解除され、右回りに回転させるとロックされます。

ステップ 2　扉のボタンを押して、ラッチをリリースします。

ステップ 3　扉を開きます。

図 17-3　Cisco ONS 15454 の前面扉



ステップ 4　元の NTP（手順）に戻ります。

DLP-A9 前面扉の取り外し

目的	この作業では、キャビネット コンパートメントの前面扉を取り外します。
工具 / 機器	オープンエンド レンチ
事前準備手順	DLP-A8 前面扉のオープン（p.17-10）
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

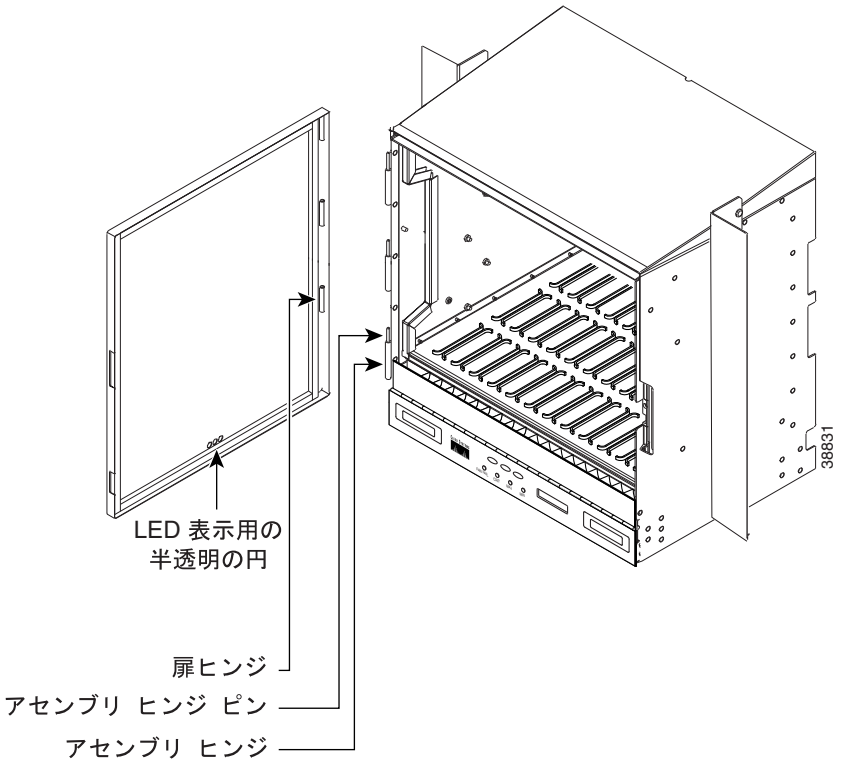
ステップ 1　扉のアース ストラップ（リリース 3.3 以降で使用可能）を取り外す手順は、次のとおりです。

a. 前面扉からアース ストラップを取り外すには、オープンエンド レンチを使用して #6 ケプナット（49-0600-01）を緩めます。扉内のオス スタッドから、アース ストラップ圧着端子（72-3622-01）の一端を取り外します。

b. ファイバ ガイドの長い方のネジからアース ストラップの反対側を取り外すには、オープンエンド レンチを使用して、圧着端子の #4 ケプナット（49-0337-01）を緩めます。圧着端子およびロック ワッシャを取り外します。

ステップ 2　扉の左上隅にあるヒンジから扉を持ち上げます（図 17-4）。

図 17-4　ONS 15454 前面扉の取り外し



ステップ 3　元の NTP（手順）に戻ります。

DLP-A10 下部バックプレーン カバーの取り外し

目的	この作業では、下部バックプレーン カバーを取り外します。
工具 / 機器	#2 プラス ドライバ 中型スロット ヘッド ネジ用ドライバ 小型スロット ヘッド ネジ用ドライバ
事前準備手順	なし
必須 / 適宜	必須
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

ステップ 1　カバーを所定位置に固定している 5 本の固定ネジを外します。

ステップ 2　カバーの両側を持ちます。

ステップ 3　カバーをバックプレーンから静かに引き抜きます。

ステップ 4　元の NTP（手順）に戻ります。

DLP-A11 金属製バックプレーン カバーの取り外し

目的	この作業では、EIA が取り付けられていない場合に、バックプレーンに取り付けられた金属製バックプレーン カバーを取り外します。
工具 / 機器	#2 プラス ドライバ 中型スロット ヘッド ネジ用ドライバ 小型スロット ヘッド ネジ用ドライバ
事前準備手順	「DLP-A10 下部バックプレーン カバーの取り外し」（p.17-13）
必須 / 適宜	必須
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

ステップ 1　クリア プラスチック製の下部バックプレーン カバーを取り外すには、ONS15454 を固定している 5 本のネジを緩めて、シェルフ アセンブリから引き出します。

ステップ 2　金属製バックプレーン カバーを所定位置に固定している 9 本の周辺ネジを緩めます。

ステップ 3　パネルを底部から持ち上げて、シェルフ アセンブリから取り外します。

ステップ 4　あとで使用できるようにパネルを保管しておきます。EIA　を取り付けない場合は、必ずバックプレーン カバーを取り付けます。

ステップ 5　元の NTP（手順）に戻ります。

DLP-A12 BNC または 高密度 BNC EIA の取り付け

目的	この作業では、BNC または高密度 BNC EIA を取り付けます。DS3-12、DS3XM-6、または EC-1 カードを使用していて、SMB インターフェイスよりも BNC インターフェイスが必要な場合は、この作業を実行します。
工具 / 機器	#2 プラス ドライバ 中型スロット ヘッド ネジ用ドライバ 小型スロット ヘッド ネジ用ドライバ 周辺ネジ（9） 内側に取り付けるネジ（12） バックプレーン カバー ネジ（5） BNC または 高密度 BNC カード
事前準備手順	「NTP-A4 バックプレーン カバーの取り外し」（p.1-8）
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

ステップ 1　パッケージから BNC または 高密度 BNC カードを取り出します。カードのコネクタをバックプレーンの対応するコネクタに合わせます。カードを静かに押し込んで、両方のコネクタ セットをしっかり噛み合わせます。

ステップ 2　金属製 EIA パネルをカードに合わせます。

ステップ 3　9 本の周辺ネジ（部品番号 48-0358）を差し込んで締め（8 ～ 10 lb［3.6 ～ 4.5 kg］）、カバー パネルをバックプレーンに固定します。

ステップ 4　12 本（BNC）または 9 本（高密度 BNC）の内側ネジ（部品番号 48-0004）を差し込んで締め（8 ～ 10 lb［3.6 ～ 4.5 kg］）、カバー パネルをカードおよびバックプレーンに固定します。

図 17-5 に、BNC EIA の取り付け方法を示します。

図 17-5　BNC EIA の取り付け

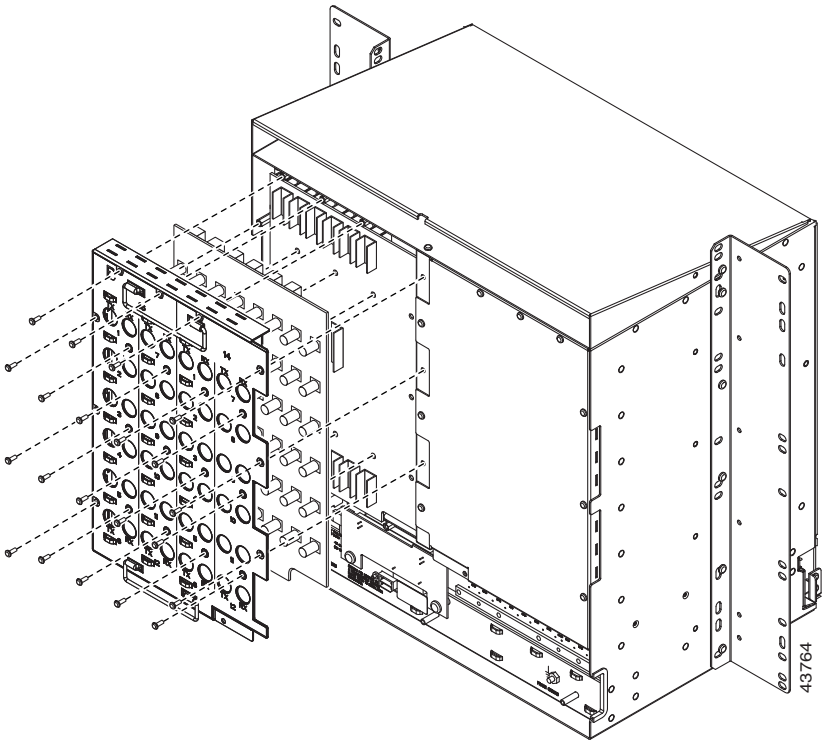
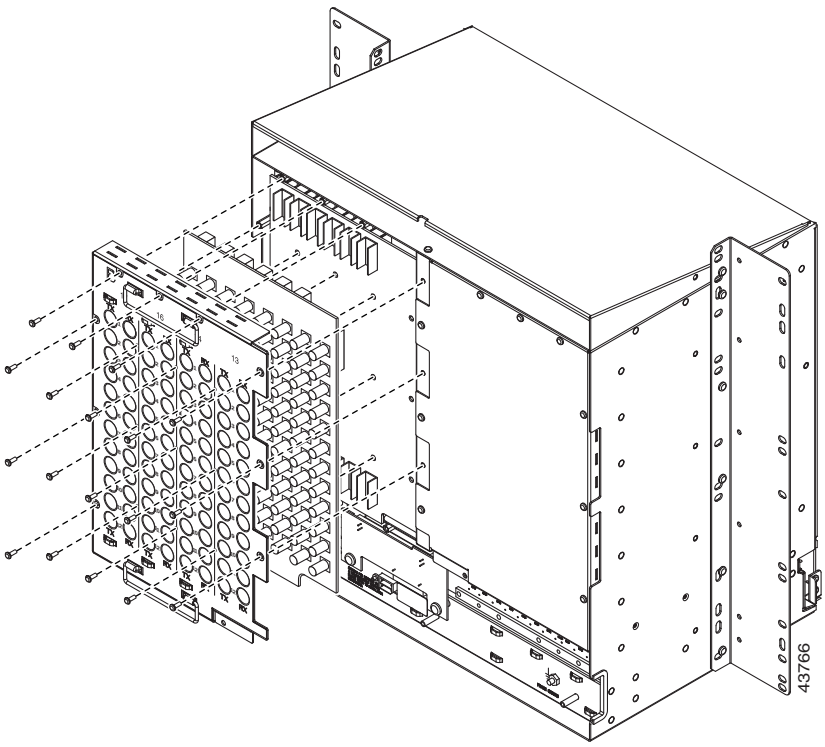


図 17-6 に、高密度 BNC EIA の取り付け方法を示します。

図 17-6　高密度 BNC EIA の取り付け



ステップ 5　元の NTP（手順）に戻ります。

DLP-A13 SMB EIA の取り付け

目的	この作業では、SMB EIA を取り付けます。DS1-14 カードを使用していて、AMP インターフェイスよりも SMB インターフェイスが必要な場合、または DS3-12、DS3XM-6、または EC-1 カードを使用していて、BNC インターフェイスよりも SMB インターフェイスが必要な場合は、SMB EIA を使用します。
工具 / 機器	#2 プラス ドライバ 中型スロット ヘッド ネジ用ドライバ 小型スロット ヘッド ネジ用ドライバ 周辺ネジ（9） 内側に取り付けるネジ（12） バックプレーン カバー ネジ（5） SMB カード フォイル EMI ガスケット（SMB EIA アセンブリによってはすでに取り付けられていることがある） 金属製 SMB カバー パネル
事前準備手順	なし
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

ステップ 1　パッケージから SMB カードを取り出します。カードのコネクタをバックプレーンの対応するコネクタに合わせます。カードを静かに押し込んで、両方のコネクタ セットをしっかり噛み合わせします。

ステップ 2　フォイル EMI ガスケットを SMB カードに合わせて、フォイル EMI ガスケットの穴を SMB コネクタの穴に合わせます。

注意　SMB EIA アセンブリが取り付けられた状態でフォイル EMI ガスケットが出荷される場合があります。そうでない場合は、フォイル EMI ガスケットを取り付けて、EMI（電磁波干渉）に関する注意事項に適合させる必要があります。

ステップ 3　金属製 SMB カバー パネルをカードに合わせます。

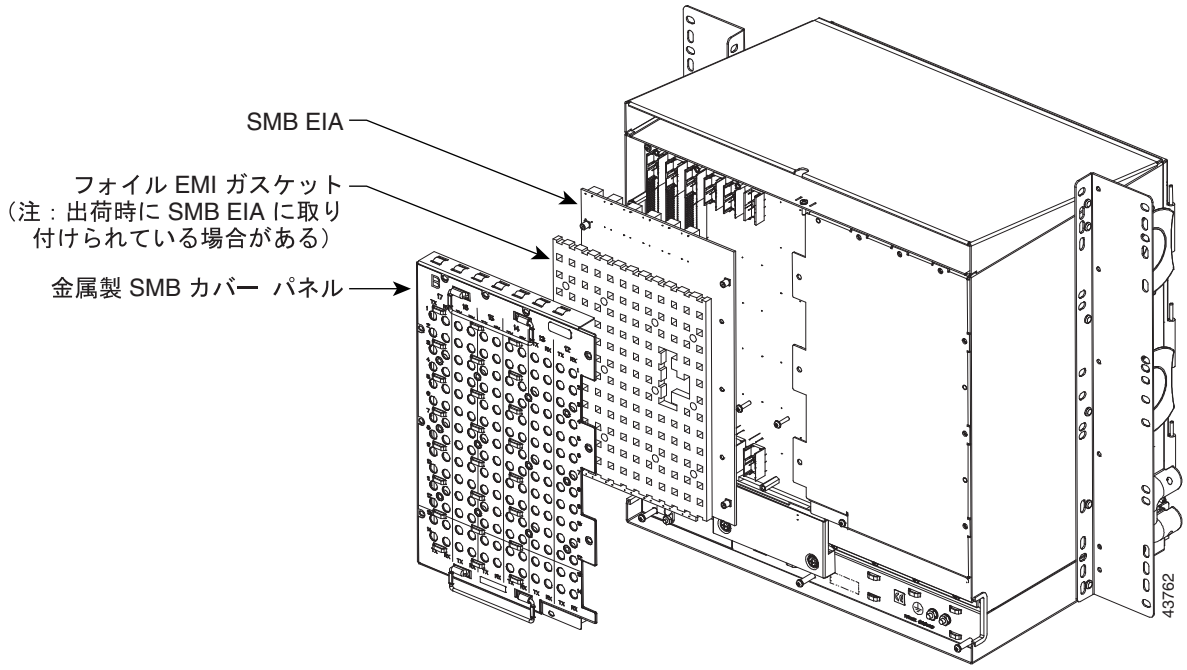
ステップ 4　12 本の内側ネジ（部品番号 48-0004）を差し込んで締め（8 ～ 10 lb［3.6 ～ 4.5 kg］）、カバー パネルをカードおよびバックプレーンに固定します。

ステップ 5　9 本の周辺ネジ（部品番号 48-0358）を差し込んで締め（8 ～ 10 lb［3.6 ～ 4.5 kg］）、カバー パネルをバックプレーンに固定します。

SMB EIA を使用して DS-1 接続を行っている場合は、DS-1 電気インターフェイス アダプタが必要です。このアダプタは通常、バラン（部品番号 15454-WW-14=）といいます。

図 17-7 に、SMB EIA の取り付け方法を示します。

図 17-7　SMB EIA の取り付け（DS-1 接続にバランを使用）



ステップ 6　元の NTP（手順）に戻ります。

DLP-A14 AMP Champ EIA の取り付け

目的	この作業では、AMP Champ EIA を取り付けます。DS1-14 カードを使用していて、SMB インターフェイスより AMP インターフェイスが必要な場合は、AMP Champ EIA を使用します。
工具 / 機器	#2 プラス ドライバ 中型スロット ヘッド ネジ用ドライバ 小型スロット ヘッド ネジ用ドライバ 周辺ネジ（9） 内側に取り付けるネジ（12） バックプレーン カバー ネジ（5） AMP Champ カード（6） EIA パネル
事前準備手順	なし
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

ステップ 1　AMP Champ パネルをバックプレーンに合わせ、9 本の周辺ネジ（部品番号 48-0358）を差し込んで締めます（8 ～ 10 lb［3.6 ～ 4.5 kg］）。

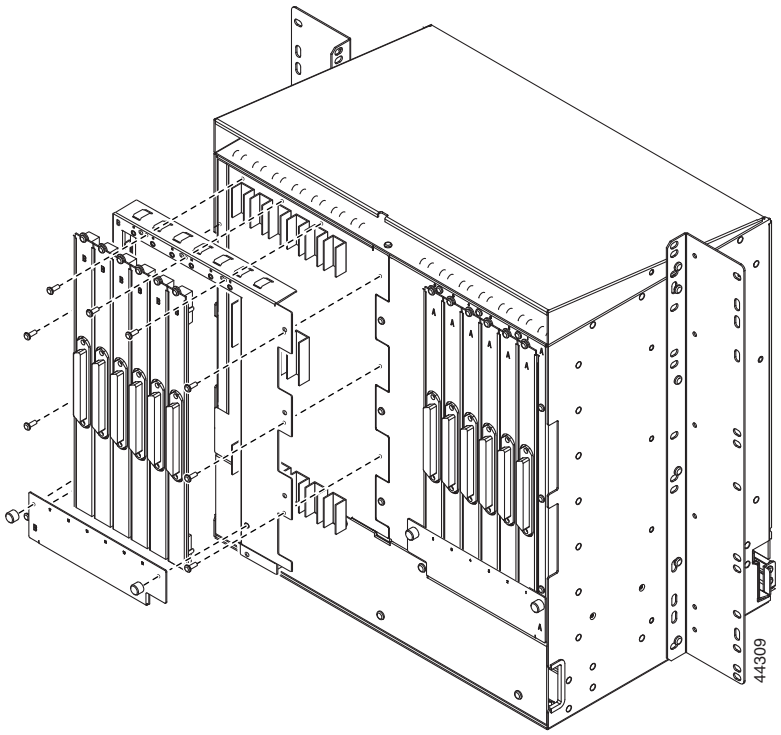
ステップ 2　AMP Champ カードをバックプレーン コネクタに合わせて、押し込み、しっかり装着します。6 つの AMP Champ カードをすべて取り付けるまで、この手順を繰り返します。

ステップ 3　各 AMP Champ カードをカバー パネルに固定するには、各カードの上部にネジ（部品番号 48-003）を差し込んで締めます（8 ～ 10 lb［3.6 ～ 4.5 kg］）。

ステップ 4　AMP Champ 固定プレートをカバー パネルの底部に合わせて、2 本の取り付けネジを手で締めます。

図 17-8 に、AMP Champ EIA の取り付け方法を示します。

図 17-8　AMP Champ EIA の取り付け



ステップ 5　元の NTP（手順）に戻ります。

DLP-A16 ONS 15454 へのオフィス アースの接続

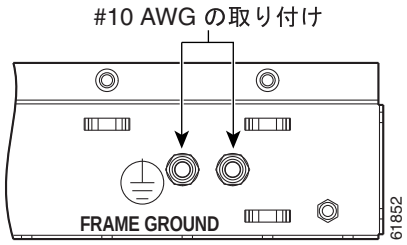
目的	この作業では、ONS 15454 シェルフにアースを接続します。
工具 / 機器	#2 プラス ドライバ 中型スロット ヘッド ネジ用ドライバ 小型スロット ヘッド ネジ用ドライバ ネジ 電源コード（ヒューズ アラーム パネルとアセンブリを接続）、#10 AWG、銅コンダクタ、90°C（194°F） ストランド アース ケーブル（機器フレームとオフィス アースを接続）、#6 AWG リストされている圧着端子コネクタ（通常はデュアル端子タイプ）。コネクタは、スタッド サイズおよび間隔が装置ラックの仕様に基づいている、#6 AWG 銅コンダクタに適したものを使用する必要があります。オフィス アース接続には、通常、現地の規約に従って H-TAP 圧着コネクタを使用します。 ワイヤ カッター ワイヤ ストリッパ 圧着工具
事前準備手順	「DLP-A10 下部バックプレーン カバーの取り外し」（p.17-13）
必須 / 適宜	必須
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

ステップ 1　オフィス アース ケーブル（#6 AWG ストランド）が、現地の規約に従って、ベイ上部およびオフィス アースに接続されていることを確認します。

ステップ 2　指定された 2 穴圧着端子コネクタを使用して、シェルフ アース ケーブル（#10 AWG）の一端をシェルフのフレーム アース支柱に取り付けます。バックプレーンのアース場所については、図 17-9 を参照してください。

（注）　フレーム アースを終端する場合は、ONS 15454 に付属のケプナットを使用して、31 インチ / ポンドの指定トルクで締めます。ケプナットを使用すると、フレーム アース接続が可能になり、取り付け時およびメンテナンス作業中の回転による緩みを最小限に抑えることができます。ケプナットがフレーム アース接続で実現する防止タイプは、本来、バッテリ接続およびバッテリ リターン接続の端子ブロックで提供されます。

図 17-9　バックプレーンのアース場所



ステップ 3　装置ベイ フレーム仕様に従って、2 穴コネクタ圧着端子を使用し、シェルフ アース ケーブルの反対側を装置ベイ フレームに接続します。

ステップ 4　元の NTP（手順）に戻ります。

DLP-A17 ONS 15454 シェルフへのオフィス電源の接続

目的	この作業では、ONS 15454 シェルフに電源を接続します。
工具 / 機器	#2 プラス ドライバ 中型スロット ヘッド ネジ用ドライバ 小型スロット ヘッド ネジ用ドライバ ワイヤ カッター ワイヤ ストリッパ 圧着工具 ヒューズ パネル 電源コード（ヒューズ アラーム パネルとアセンブリを接続）、#10 AWG、銅コンダクタ、90°C（194°F） ストランド アース ケーブル #6 AWG
事前準備手順	「DLP-A16 ONS 15454 へのオフィス アースの接続」（p.17-20）
必須 / 適宜	必須
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

警告　**装置の取り付けまたは交換を行う場合は、必ずアース線を最初に接続し、最後に取り外す必要があります。**

（注）　バッテリ リターン接続は、Telcordia GR-1089-CORE Issue 3 の定義に従って、DC-I として処理されます。

（注）　Network Time Protocol/Simple Network Time Protocol（NTP/SNTP）サーバから時刻を取得するようにプロビジョニングされていないシステムで、電源が切断されるか、または TCC2/TCC2P の両方のカードがリセットされた場合は、ONS 15454 クロックをリセットする必要があります。電源切断後の日付のデフォルト値は、1970 年 1 月 1 日の 00:04:15 です。クロックをリセットする場合は、「NTP-A25 名前、日付、時刻、連絡先情報の設定」（p.4-7）を参照してください。
TCC2/TCC2P カードを使用している場合は、システム クロックが最大 3 時間動作し続けます。この場合、対応は不要です。

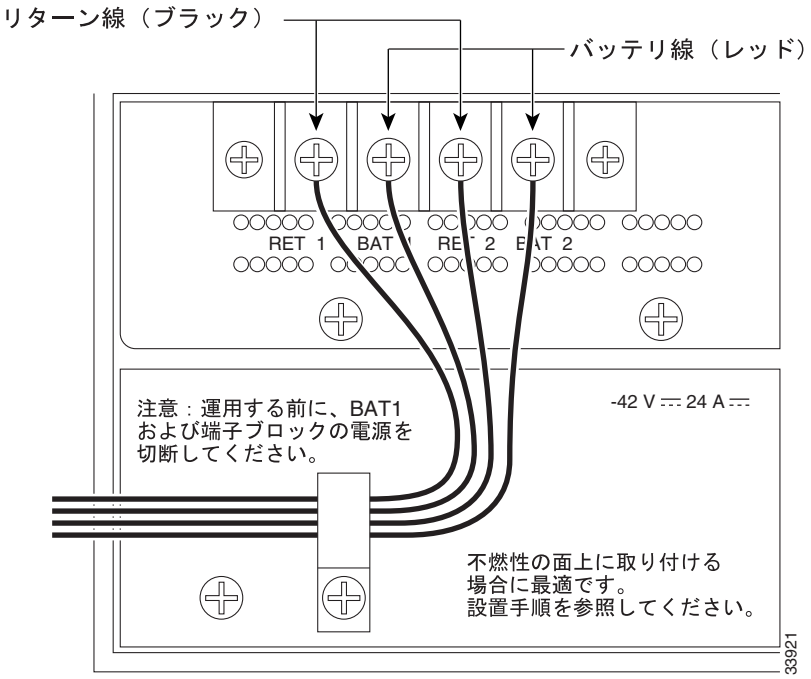
（注）　電源装置に問題が発生した場合は、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。

ステップ 1　ヒューズ パネルのエンジニアリング仕様に従って、オフィス電源を接続します。

ステップ 2　ヒューズ パネルから ONS 15454 まで到達するようにケーブルを測定し、必要に応じて切断します。図 17-10 に、ONS 15454 の電源端子を示します。

ステップ 3　現地の規約に従って、電源コードに印を付けます。

図 17-10　Cisco ONS 15454 の電源端子



ステップ 4　ONS 15454 の #8 電源端子ネジを取り外すか、または緩めます。混乱を避けるために、BAT1/RET1（A）電源端子に接続されたケーブルに 1 のラベルを付け、BAT2/RET2（B）電源端子に接続されたケーブルに 2 のラベルを付けます。

（注）　バッテリ、バッテリ リターン、およびフレーム アース コンダクタを終端する場合は、リング、フォーク、デュアル端子タイプなどの圧着端子コネクタのみを使用します。

注意　圧着接続を行う場合は、むき出しのすべての導体（バッテリ、バッテリ リターン、およびフレーム アース）を、適切な酸化防止剤でコーティングします。めっきしていないすべてのコネクタ、ブレード ストラップ、およびバス バーを接続する前に、光沢仕上げを施し、酸化防止剤でコーティングします。コネクタにスズめっき、はんだめっき、または銀めっきを施したり、接続面にその他のめっき処理を施す必要はありません。ただし、これらを常に清潔な状態に保ち、汚れが付着しないようにしてください。

注意　電源、リターン、フレーム アースを終端する場合は、はんだ付け端子、ネジなし（押し込み）コネクタ、クイック接続コネクタ、または他の摩擦式コネクタを使用しないでください。

ステップ 5　使用するすべての電源コードから、絶縁被膜を 1/2 インチ（12.7 mm）はぎ取ります。

ステップ 6　すべての電源コードの両端に圧着端子を圧着します。

（注）　バッテリ接続およびバッテリ リターン接続を終端する場合は（図 17-10 を参照）、10 インチ / ポンドのトルク仕様に従います。

ステップ 7　リターン 1 導線を RET1 バックプレーン端子に終端します。酸化防止用グリースを使用して、接続の腐食を防止します。

ステップ 8　マイナス 1 導線をマイナス BAT1 バックプレーン電源端子に終端します。酸化防止用グリースを使用して、接続の腐食を防止します。

ステップ 9　冗長電源コードを使用している場合は、リターン 2 導線を ONS 15454 のプラス RET2 端子に終端します。マイナス 2 導線を ONS 15454 のマイナス BAT2 端子に終端します。酸化防止用グリースを使用して、接続の腐食を防止します。

ステップ 10　プラスチックのケーブル クランプを使用して、電源端子の下にケーブルを配線します（図 17-10 [p.17-23] を参照）。

ステップ 11　元の NTP（手順）に戻ります。

DLP-A18 オフィス電源の投入と検証

目的	この作業では、電力を測定して正しい電源およびリターンであることを確認します。
工具 / 機器	電圧計
事前準備手順	「DLP-A16 ONS 15454 へのオフィス アースの接続」（p.17-20） 「DLP-A17 ONS 15454 シェルフへのオフィス電源の接続」（p.17-22）
必須 / 適宜	必須
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

ステップ 1　電圧計を使用して、ヒューズ アラーム パネルの次のポイントでオフィス バッテリとアースを検証します。

a. 電源を検証するには、電圧計のブラックのテスト線をフレーム アースに接続します。レッドのテスト線を A 側接続に接続し、–40.5 VDC から –57 VDC の間であることを確認します。レッドのテスト線を B 側接続に接続し、–40.5 VDC から –57 VDC の間であることを確認します。

（注）　–40.5 VDC と –57 VDC という電圧は、それぞれシャーシに電力を供給するために必要な最小および最大電圧です。

b. アースを確認するには、電圧計のブラックのテスト線をフレーム アースに接続します。レッドのテスト線を A 側リターン アースに接続し、電圧が存在しないことを確認します。レッドのテスト線を B 側リターン アースに接続し、電圧が存在しないことを確認します。

ステップ 2　次のいずれかの手順を実行して、ノードに電力を供給します。

- 80 A のヒューズ パネルを使用している場合は、現地の規約に従ってヒューズ位置に 20 A ヒューズを挿入します。
- 100 A のヒューズ パネルを使用している場合は、現地の規約に従ってヒューズ位置に 30 A ヒューズを挿入します。

ステップ 3　電圧計を使用して、シェルフで –48 VDC バッテリとアースを確認します。

a. シェルフの A 側を確認するには、電圧計のブラックのテスト線をフレーム アースに接続します。レッドのテスト線を BAT1（A 側バッテリ接続）のレッド ケーブルに接続します。–40.5 VDC から –57 VDC の間になることを確認します。その後、電圧計のレッドのテスト線を RET1（A 側リターン アース）ブラック ケーブルに接続し、電圧が存在しないことを確認します。

（注）　–40.5 VDC と –57 VDC という電圧は、それぞれシャーシに電力を供給するために必要な最小および最大電圧です。

b. シェルフの B 側を確認するには、電圧計のブラックのテスト線をフレーム アースに接続します。レッドのテスト線を BAT2（B 側バッテリ接続）のレッド ケーブルに接続します。–40.5 VDC から –57 VDC の間になることを確認します。その後、電圧計のレッドのテスト線を RET2（B 側リターン アース）ブラック ケーブルに接続し、電圧が存在しないことを確認します。

ステップ 4　元の NTP（手順）に戻ります。

DLP-A19 バックプレーンへのアラーム ケーブルの取り付け

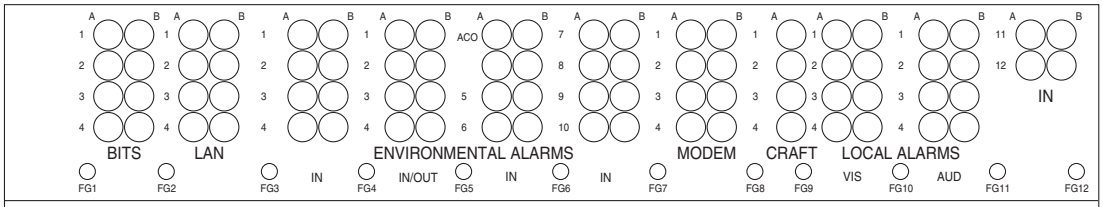
目的	この作業では、バックプレーンにアラーム ケーブルを取り付けることにより、Alarm Interface Controller-International（AIC-I）カードを使用して外部（環境）のアラームおよび制御をプロビジョニングできるようにします。Alarm Extension Panel（AEP）を使用している場合は、この作業を実行しないでください。
工具 / 機器	ワイヤ ラッパー #22 または #24 AWG（0.51 mm^2 または 0.64 mm^2）ケーブル 100 Ω シールド Building Integrated Timing Supply（BITS）クロック ケーブル ペア #22 または #24 AWG（0.51 mm^2 または 0.64 mm^2）、ツイストペア T1 タイプ
事前準備手順	なし
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

ステップ 1　100 Ω シールド BITS クロック ケーブル ペア #22 または #24 AWG（0.51 mm^2 または 0.64 mm^2）ツイストペア T1 タイプ ケーブルを使用して、現地の規約に従って、適切なワイヤラップ ピンにアラーム ケーブルをラップします。BITS 側で、BITS 入力ケーブルのシールドをアースします。BITS 出力の場合は、BITS ケーブルのアース シールドを、BITS ピンの列の下にあるフレーム アース ピン（FG1）にラップします。

図 17-11 に、リリース 3.4 以上の ONS 15454 バックプレーンの AIC-I に対応するアラーム ピン割り当てを示します。

（注）　AIC-I を使用する場合は、シェルフ アセンブリで 3.4.0 以降のソフトウェア リリースが稼働している必要があります。ANSI シェルフのバックプレーンには、図 17-11 のレイアウトに従ってピンが割り当てられたワイヤラップ フィールドがあります。シェルフ アセンブリの既存のシェルフが、R3.4 以降にアップグレードされている場合には、バックプレーン ピンのラベルが図 17-13（p.17-28）のようになりますが、図 17-11 に示された AIC-I のピン割り当てを使用する必要があります。

図 17-11　Cisco ONS 15454 バックプレーンのピン割り当て（リリース 3.4 以降）



フィールド	ピン	説明
BITS	A1	BITS 出力 2 マイナス（–）
	B1	BITS 出力 2 プラス（+）
	A2	BITS 入力 2 マイナス（–）
	B2	BITS 入力 2 プラス（+）
	A3	BITS 出力 1 マイナス（–）
	B3	BITS 出力 1 プラス（+）
	A4	BITS 入力 1 マイナス（–）
	B4	BITS 入力 1 プラス（+）
LAN	ハブまたはスイッチに接続	
	A1	RJ-45 ピン 6 RX–
	B1	RJ-45 ピン 3 RX+
	A2	RJ-45 ピン 2 TX–
	B2	RJ-45 ピン 1 TX+
	PC/ワークステーションまたはルータに接続	
	A1	RJ-45 ピン 2 RX–
	B1	RJ-45 ピン 1 RX+
	A2	RJ-45 ピン 6 TX–
	B2	RJ-45 ピン 3 TX+
ENVIR ALARMS IN	A1	アラーム入力ペア番号 1：接続ケーブルが閉じているかどうかをレポート
	B1	
	A2	アラーム入力ペア番号 2：接続ケーブルが閉じているかどうかをレポート
	B2	
	A3	アラーム入力ペア番号 3：接続ケーブルが閉じているかどうかをレポート
	B3	
	A4	アラーム入力ペア番号 4：接続ケーブルが閉じているかどうかをレポート
	B4	
	A5	アラーム入力ペア番号 5：接続ケーブルが閉じているかどうかをレポート
	B5	
	A6	アラーム入力ペア番号 6：接続ケーブルが閉じているかどうかをレポート
	B6	
	A7	アラーム入力ペア番号 7：接続ケーブルが閉じているかどうかをレポート
	B7	
	A8	アラーム入力ペア番号 8：接続ケーブルが閉じているかどうかをレポート
	B8	
	A9	アラーム入力ペア番号 9：接続ケーブルが閉じているかどうかをレポート
	B9	
	A10	アラーム入力ペア番号 10：接続ケーブルが閉じているかどうかをレポート
	B10	
	A11	アラーム入力ペア番号 11：接続ケーブルが閉じているかどうかをレポート
	B11	
	A12	アラーム入力ペア番号 12：接続ケーブルが閉じているかどうかをレポート
	B12	

フィールド	ピン	説明
ENVIR ALARMS IN/OUT N/O	A1/A13	通常開いている出力ペア番号 1
	B1/B13	
	A2/A14	通常開いている出力ペア番号 2
	B2/B14	
	A3/A15	通常開いている出力ペア番号 3
	B3/B15	
	A4/A16	通常開いている出力ペア番号 4
	B4/B16	
ACO	A1	通常開いている ACO ペア
	B1	
CRAFT	A1	受信（PC ピン #2）
	A2	送信（PC ピン #3）
	A3	アース（PC ピン #5）
	A4	DTR（PC ピン #4）
LOCAL ALARMS AUD (Audible) N/O	A1	アラーム出力ペア番号 1：リモート音声アラーム
	B1	
	A2	アラーム出力ペア番号 2：Critical 音声アラーム
	B2	
	A3	アラーム出力ペア番号 3：Major 音声アラーム
	B3	
	A4	アラーム出力ペア番号 4：Minor 音声アラーム
	B4	
LOCAL ALARMS VIS (Visual) N/O	A1	アラーム出力ペア番号 1：リモート ビジュアル アラーム
	B1	
	A2	アラーム出力ペア番号 2：Critical ビジュアル アラーム
	B2	
	A3	アラーム出力ペア番号 3：Major ビジュアル アラーム
	B3	
	A4	アラーム出力ペア番号 4：Minor ビジュアル アラーム
	B4	

AIC-I カードを使用している場合は、 ピン 1～4 が OUT としてプロビジョニングされています。また、ピン 13～16 が IN としてプロビジョニングされています。

83020

図 17-12 に、リリース 3.4 以降のバックプレーンの環境アラーム ピン割り当てを示します。

図 17-12　環境アラーム（強調表示）

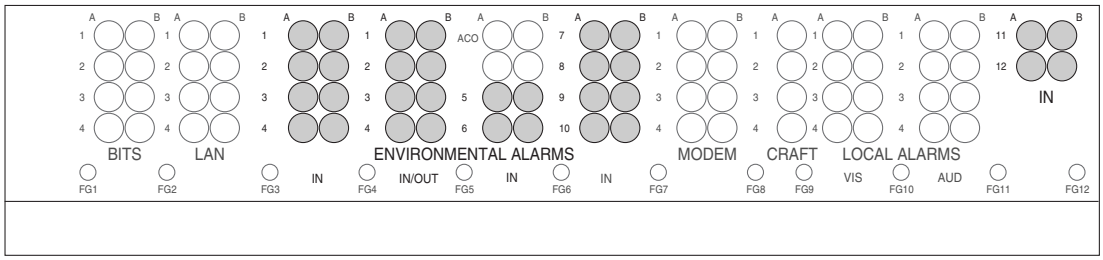
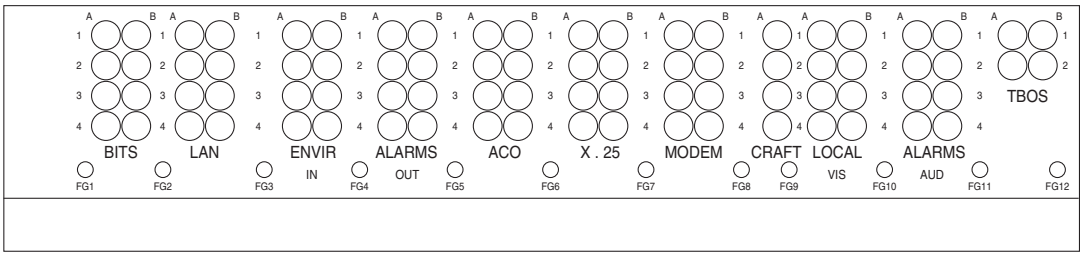


図 17-13 に、リリース 3.3 以前のシェルフのアラーム ピン割り当てを示します。AIC-I は 3.3 以前のリリースのシェルフと互換性がありません。

図 17-13　Cisco ONS 15454 バックプレーンのピン割り当て（リリース 3.3 以前）



フィールド	ピン	説明
BITS	A1	BITS 出力 2 マイナス（–）
	B1	BITS 出力 2 プラス（+）
	A2	BITS 入力 2 プラス（+）
	B2	BITS 入力 2 プラス（+）
	A3	BITS 出力 1 マイナス（–）
	B3	BITS 出力 1 プラス（+）
	A4	BITS 入力 1 マイナス（–）
	B4	BITS 入力 1 プラス（+）
LAN	ハブまたはスイッチに接続	
	A1	RJ-45 ピン 6 RX–
	B1	RJ-45 ピン 3 RX+
	A2	RJ-45 ピン 2 TX–
	B2	RJ-45 ピン 1 TX+
	PC/ワークステーションまたはルータに接続	
	A1	RJ-45 ピン 2 RX–
	B1	RJ-45 ピン 1 RX+
	A2	RJ-45 ピン 6 TX–
	B2	RJ-45 ピン 3 TX+
ENVIR ALARMS IN	A1	アラーム入力ペア番号 1：接続ケーブルが閉じているかどうかをレポート
	B1	
	A2	アラーム入力ペア番号 2：接続ケーブルが閉じているかどうかをレポート
	B2	
	A3	アラーム入力ペア番号 3：接続ケーブルが閉じているかどうかをレポート
	B3	
	A4	アラーム入力ペア番号 4：接続ケーブルが閉じているかどうかをレポート
	B4	

フィールド	ピン	説明
ENVIR ALARMS OUT N/O	A1	通常開いている出力ペア番号 1
	B1	
	A2	通常開いている出力ペア番号 2
	B2	
	A3	通常開いている出力ペア番号 3
	B3	
	A4	通常開いている出力ペア番号 4
	B4	
ACO	A1	通常開いている ACO ペア
	B1	
CRAFT	A1	受信（PC ピン #2）
	A2	送信（PC ピン #3）
	A3	アース（PC ピン #5）
	A4	DTR（PC ピン #4）
LOCAL ALARMS AUD (Audible) N/O	A1	アラーム出力ペア番号 1：リモート音声アラーム
	B1	
	A2	アラーム出力ペア番号 2：Critical 音声アラーム
	B2	
	A3	アラーム出力ペア番号 3：Major 音声アラーム
	B3	
	A4	アラーム出力ペア番号 4：Minor 音声アラーム
	B4	
LOCAL ALARMS VIS (Visual) N/O	A1	アラーム出力ペア番号 1：リモート ビジュアル アラーム
	B1	
	A2	アラーム出力ペア番号 2：Critical ビジュアル アラーム
	B2	
	A3	アラーム出力ペア番号 3：Major ビジュアル アラーム
	B3	
	A4	アラーム出力ペア番号 4：Minor ビジュアル アラーム
	B4	

38533

（注）　X.25、Modem、および TBOS ピン フィールドは無効です。

ステップ 2　元の NTP（手順）に戻ります。

DLP-A20 バックプレーンへのタイミング ケーブルの取り付け

目的	この作業では、バックプレーンに BITS タイミング ケーブルを取り付けます。
工具 / 機器	ワイヤ ラッパー 100 Ω シールド BITS クロック ケーブル ペア #22 または #24 AWG（0.51 mm^2 または 0.64 mm^2）、ツイストペア T1 タイプ
事前準備手順	なし
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

ステップ 1　100 Ω シールド BITS クロック ケーブル ペア #22 または #24 AWG（0.51 mm^2 または 0.64 mm^2）ツイストペア T1 タイプ ケーブルを使用して、現地の規約に従って、適切なワイヤラップ ピンにクロック線をラップします

BITS 側で、BITS 入力ケーブルのシールドをアースします。BITS 出力の場合は、BITS ケーブルのアース シールドを、BITS ピンの列の下にあるフレーム アース ピン（FG1）にラップします。表 17-1 に、BITS タイミング ピン フィールドのピン割り当てを示します。

表 17-1　BITS の外部タイミング ピン割り当て

BITS ピン	Tip/Ring	CTC/TL1 名	説明
A4	Ring	BITS-1	BITS デバイス 1 からの入力
B4	Tip	BITS-1	BITS デバイス 1 からの入力
A3	Ring	BITS-1	外部デバイス 1 への出力
B3	Tip	BITS-1	外部デバイス 1 への出力
A2	Ring	BITS-2	BITS デバイス 2 からの入力
B2	Tip	BITS-2	BITS デバイス 2 からの入力
A1	Ring	BITS-2	外部デバイス 2 への出力
B1	Tip	BITS-2	外部デバイス 2 への出力

（注）　タイミングの詳細については、『*Cisco ONS 15454 Reference Manual*』にある「Timing」の章を参照してください。システム タイミングの設定については、「NTP-A28 タイミングの設定」（p.4-12）を参照してください。

ステップ 2　元の NTP（手順）に戻ります。

DLP-A21 バックプレーンへの LAN ケーブルの取り付け

目的	この作業では、バックプレーンに LAN ケーブルを取り付けます。
工具 / 機器	ワイヤ ラッパー #22 または #24 AWG（0.51 mm^2 または 0.64 mm^2）ケーブル（CAT-5 UTP を推奨）
事前準備手順	なし
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

（注） 必要であれば、LAN ケーブルを使用しないで、TCC2/TCC2P の LAN 接続ポートを使用することもできます。バックプレーン接続または TCC2/TCC2P 前面接続を使用します。LAN バックプレーン ピンと TCC2/TCC2P の LAN 接続ポートを同時に使用することはできません。ただし、TCC2/TCC2P に直接接続しているコンピュータが LAN に接続していない場合に限って、LAN バックプレーン ピンが使用されているときに、コンピュータから TCC2/TCC2P の LAN 接続ポートに直接接続することができます。

ステップ 1 #22 または #24 AWG（0.51 mm^2 または 0.64 mm^2）ケーブルまたは CAT-5 UTP イーサネット ケーブルを使用し、現地の規約に従って、適切なワイヤラップ ピンにケーブルをラップします。

注意 受信（Rx）および送信（Tx）ピンが CAT-5 ケーブルの同じツイストペア線に接続されている場合は、漏話が発生することがあります。2 つの Tx ピンと 2 つの Rx ピンをそれぞれ異なるツイストペアに接続する必要があります。

フレーム アース ピンは各ピン フィールドの下にあります（LAN ピン フィールドの場合は FG2）。LAN インターフェイス ケーブルのアース シールドを、フレーム アース ピンにラップします。表 17-2 に、LAN ピン割り当てを示します。

表 17-2　LAN ピン割り当て

ピン フィールド	バックプレーン ピン	RJ-45 ピン	機能 / 色
LAN 1 Date Circuit-terminating Equipment（DCE*; データ回線終端装置）（ハブまたはスイッチ）。ONS 15454 は DCE。	B2	1	TX+ ホワイト / グリーン
	A2	2	TX– グリーン
	B1	3	RX+ ホワイト / オレンジ
	A1	6	RX– オレンジ
LAN 1 Data Terminal Equipment（DTE; データ端末装置）に接続（PC/ ワークステーションまたはルータ）	B1	1	RX+ ホワイト / グリーン
	A1	2	RX– グリーン
	B2	3	TX + ホワイト / オレンジ
	A2	6	TX– オレンジ

（注）　TCC2/TCC2P はイーサネット極性検出をサポートしません。イーサネット接続の極性が正しくない場合は（ケーブルの受信線ペアがフリップしている場合のみ発生することがある）、［Lan Connection Polarity Reversed］状態が生じます。この状態は通常、アップグレード中または最初のノード配置中に発生します。この状況を改善するには、イーサネット ケーブルにワイヤラップ ピンが正しく対応付けられているか確認します。

ステップ 2　元の NTP（手順）に戻ります。

DLP-A22 TL1 クラフト インターフェイスの取り付け

目的	この作業では、クラフト バックプレーン ピンを使用して、TL1 クラフト インターフェイスを取り付けます。TCC2/TCC2P カードの EIA/TIA-232 ポートに接続された LAN ケーブルを使用して、TL1 クラフト インターフェイスにアクセスすることもできます。
工具 / 機器	ワイヤ ラッパー #22 または #24 AWG（0.51 mm^2 または 0.64 mm^2）アラーム ケーブル
事前準備手順	「NTP-A4 バックプレーン カバーの取り外し」（p.1-8）
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

（注） クラフト ピンを使用しないで、TCC2/TCC2P カードの EIA/TIA-232 ポートに接続された LAN ケーブルを使用して、TL1 クラフト インターフェイスにアクセスすることもできます。

ステップ 1　#22 または #24 AWG（0.51 mm^2 または 0.64 mm^2）ケーブルを使用し、現地の規約に従って、適切なワイヤラップ ピンにクラフト インターフェイス ケーブルをラップします。

ステップ 2　クラフト インターフェイス ケーブルのアース シールドを、フレーム アース ピンにラップします。

コンピュータ ケーブルのアース線をクラフト ピン フィールドのピン A3 にラップします。表 17-3 に CRAFT ピン フィールドのピン割り当てを示します。

（注） クラフト バックプレーン ピンと TCC2/TCC2P カードの EIA/TIA-232 ポートを同時に使用することはできません。同時に使用すると、ノードにアクセスできなくなったり、接続が切断されたりします。

表 17-3　クラフト インターフェイス ピンの割り当て

ピン フィールド	ピン	説明
Craft	A1	受信
	A2	送信
	A3	アース
	A4	DTR

ステップ 3　元の NTP（手順）に戻ります。

DLP-A23 電気インターフェイス アダプタ（バラン）を使用した DS-1 ケーブルの取り付け

目的	この作業では、電気インターフェイス アダプタを使用して、SMB EIA に DS-1 ケーブルを取り付けます。
工具 / 機器	ワイヤ ラッパー ツイストペア ケーブル
事前準備手順	「DLP-A13 SMB EIA の取り付け」（p.17-16）
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

（注） ONS 15454 DS-1 ポートに接続されたすべての DS-1 ケーブルは、ツイストペア ケーブルを使用して終端し、DS-1 電気インターフェイス アダプタに接続する必要があります。DS-1 電気インターフェイス アダプタは、SMB EIA よりも 1.72 インチ（43.7 mm）突き出ています。詳細については、『*Cisco ONS 15454 Reference Manual*』の「Shelf and Backplane Hardware」の章を参照してください。

ステップ 1　バックプレーンのポート送信ペアの SMB コネクタに、アダプタの SMB コネクタを接続します。

ステップ 2　バックプレーンのポート受信ペアの SMB コネクタに、アダプタの SMB コネクタを接続します。

ステップ 3　ポートの DS-1 送受信ケーブルをアダプタのワイヤラップ ポートに終端します。

a. ワイヤラップ工具を使用して、受信ケーブルを、目的のポートに対応したバックプレーン コネクタの受信アダプタ ピンに接続します。

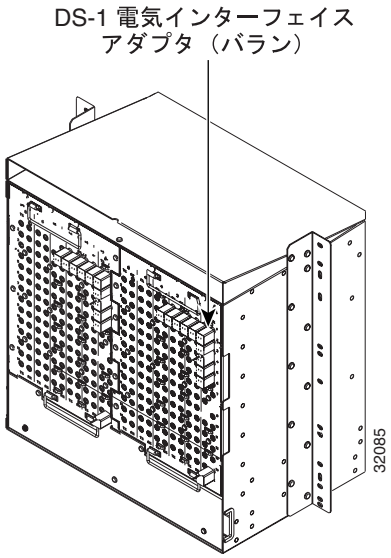
b. 送信ケーブルを、目的のポートに対応したバックプレーン コネクタの送信アダプタ ピンに接続します。

c. 現地の規約に従って、DS-1 ケーブルのシールド アース ケーブルをアースに終端します。

（注） DS1N-14 カードをスロット 3 および 15 に装着して 1:N 保護グループを形成する場合は、DS-1 電気インターフェイス アダプタのスロット 3 および 15 をラップしないでください。

図 17-14 に、SMB EIA が取り付けられた ONS 15454 バックプレーンを示します。シェルフ アセンブリの両側に DS-1 電気インターフェイス アダプタが取り付けられていて、DS-1 ツイストペア終端ポイントを形成しています。

図 17-14　DS-1 ケーブルに対応する SMB EIA が取り付けられたバックプレーン



ステップ 4　元の NTP（手順）に戻ります。

DLP-A24 AMP Champ EIA への DS-1 AMP Champ ケーブルの取り付け

目的	この作業では、AMP Champ EIA に DS-1 AMP Champ ケーブルを取り付けます。
工具 / 機器	ワイヤ ラッパー ツイストペア ケーブル
事前準備手順	「DLP-A14 AMP Champ EIA の取り付け」（p.17-18）
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

ステップ 1　シェルフ アセンブリに取り付ける DS1-14/DS1N-14 カードごとに、56 線ケーブルを 1 本準備します。

ステップ 2　ケーブルのオス AMP Champ コネクタを、ONS 15454 バックプレーンのメス AMP Champ コネクタに接続します。

ステップ 3　オス AMP Champ コネクタのクリップを使用して、接続を固定します。

メス コネクタの外側エッジには、クリップを所定位置に合わせるための溝があります。

表 17-4 に、ONS 15454 AMP Champ EIA の AMP Champ コネクタのピン割り当てを示します。

（注）　表 17-4 の影のついた領域は、ホワイト / オレンジ バインダ グループに対応します。バインダ グループは、業界標準の色分け方式によって色分けされた 25 のケーブル ペアで構成されています。

表 17-4　AMP Champ コネクタのピン割り当て

信号 / 線	ピン	ピン	信号 / 線	信号 / 線	ピン	ピン	信号 / 線
Tx Tip 1 ホワイト/ブルー	1	33	Tx Ring 1 ブルー/ホワイト	Rx Tip 1 イエロー/オレンジ	17	49	Rx Ring 1 オレンジ / イエロー
Tx Tip 2 ホワイト/オレンジ	2	34	Tx Ring 2 オレンジ/ホワイト	Rx Tip 2 イエロー/グリーン	18	50	Rx Ring 2 グリーン / イエロー
Tx Tip 3 ホワイト/グリーン	3	35	Tx Ring 3 グリーン/ホワイト	Rx Tip 3 イエロー/ブラウン	19	51	Rx Ring 3 ブラウン / イエロー
Tx Tip 4 ホワイト/ブラウン	4	36	Tx Ring 4 ブラウン/ホワイト	Rx Tip 4 イエロー/ブルーグレー	20	52	Rx Ring 4 ブルーグレー/イエロー
Tx Tip 5 ホワイト/ブルーグレー	5	37	Tx Ring 5 ブルーグレー/ホワイト	Rx Tip 5 バイオレット/ブルー	21	53	Rx Ring 5 ブルー / バイオレット
Tx Tip 6 レッド / ブルー	6	38	Tx Ring 6 ブルー / レッド	Rx Tip 6 バイオレット/オレンジ	22	54	Rx Ring 6 オレンジ/バイオレット

表 17-4　AMP Champ コネクタのピン割り当て（続き）

信号 / 線	ピン	ピン	信号 / 線	信号 / 線	ピン	ピン	信号 / 線
Tx Tip 7 レッド/オレンジ	7	39	Tx Ring 7 オレンジ/レッド	Rx Tip 7 バイオレット/グリーン	23	55	Rx Ring 7 グリーン/バイオレット
Tx Tip 8 レッド/グリーン	8	40	Tx Ring 8 グリーン/レッド	Rx Tip 8 バイオレット/ブラウン	24	56	Rx Ring 8 ブラウン/バイオレット
Tx Tip 9 レッド/ブラウン	9	41	Tx Ring 9 ブラウン/レッド	Rx Tip 9 バイオレット/ブルーグレー	25	57	Rx Ring 9 ブルーグレー/バイオレット
Tx Tip 10 レッド/ブルーグレー	10	42	Tx Ring 10 ブルーグレー/レッド	Rx Tip 10 [1] ホワイト/ブルー	26	58	Rx Ring 10 ブルー/ホワイト
Tx Tip 11 ブラック/ブルー	11	43	Tx Ring 11 ブルー/ブラック	Rx Tip 11 ホワイト/オレンジ	27	59	Rx Ring 11 オレンジ/ホワイト
Tx Tip 12 ブラック/オレンジ	12	44	Tx Ring 12 オレンジ/ブラック	Rx Tip 12 ホワイト/グリーン	28	60	Rx Ring 12 グリーン/ホワイト
Tx Tip 13 ブラック/グリーン	13	45	Tx Ring 13 グリーン/ブラック	Rx Tip 13 ホワイト/ブラウン	29	61	Rx Ring 13 ブラウン/ホワイト
Tx Tip 14 ブラック/ブラウン	14	46	Tx Ring 14 ブラウン/ブラック	Rx Tip 14 ホワイト/ブルーグレー	30	62	Rx Ring 14 ブルーグレー/ホワイト
Tx Spare0+ 使用しない	15	47	Tx Spare0– 使用しない	Rx Spare0+ 使用しない	31	63	Rx Spare0– 使用しない
Tx Spare1+ 使用しない	16	48	Tx Spare1– 使用しない	Rx Spare1+ 使用しない	32	64	Rx Spare1– 使用しない

1. ピン 26、27、28、29、30、58、59、60、61、および 62 は、ホワイト / オレンジ バインダ グループに対応します。バインダ グループは、業界標準の色分け方式によって色分けされた 25 のケーブル ペアで構成されています。

表 17-5 に、シールド付き DS-1 ケーブルに対応する、ONS 15454 AMP Champ EIA の AMP Champ コネクタのピン割り当てを示します。

表 17-5　AMP Champ コネクタのピン割り当て（シールド付き DS-1 ケーブル）

64 ピン ブルー バンドル				64 ピン オレンジ バンドル			
信号 / 線	**ピン**	**ピン**	**信号 / 線**	**信号 / 線**	**ピン**	**ピン**	**信号 / 線**
Tx Tip 1 ホワイト/ブルー	1	33	Tx Ring 1 ブルー/ホワイト	Rx Tip 1 ホワイト/ブルー	17	49	Rx Ring 1 ブルー/ホワイト
Tx Tip 2 ホワイト / オレンジ	2	34	Tx Ring 2 オレンジ/ホワイト	Rx Tip 2 ホワイト/オレンジ	18	50	Rx Ring 2 オレンジ/ホワイト
Tx Tip 3 ホワイト/グリーン	3	35	Tx Tip 3 グリーン/ホワイト	Rx Tip 3 ホワイト/グリーン	19	51	Rx Ring 3 グリーン/ホワイト

表 17-5　AMP Champ コネクタのピン割り当て（シールド付き DS-1 ケーブル）（続き）

64 ピン ブルー バンドル				64 ピン オレンジ バンドル			
信号 / 線	ピン	ピン	信号 / 線	信号 / 線	ピン	ピン	信号 / 線
Tx Tip 4 ホワイト/ブラウン	4	36	Tx Ring 4 ブラウン/ホワイト	Rx Tip 4 ホワイト/ブラウン	20	52	Rx Ring 4 ブラウン/ホワイト
Tx Tip 5 ホワイト/ブルーグレー	5	37	Tx Ring 5 ブルーグレー/ホワイト	Rx Tip 5 ホワイト/ブルーグレー	21	53	Rx Ring 5 ブルーグレー/ホワイト
Tx Tip 6 レッド / ブルー	6	38	Tx Ring 6 ブルー / レッド	Rx Tip 6 レッド / ブルー	22	54	Rx Ring 6 ブルー / レッド
Tx Tip 7 レッド/オレンジ	7	39	Tx Ring 7 オレンジ/レッド	Rx Tip 7 レッド/オレンジ	23	55	Rx Ring 7 オレンジ/レッド
Tx Tip 8 レッド/グリーン	8	40	Tx Ring 8 グリーン/レッド	Rx Tip 8 レッド/グリーン	24	56	Rx Ring 8 グリーン/レッド
Tx Tip 9 レッド/ブラウン	9	41	Tx Ring 9 ブラウン/レッド	Rx Tip 9 レッド/ブラウン	25	57	Rx Ring 9 ブラウン/レッド
Tx Tip 10 レッド/ブルーグレー	10	42	Tx Ring 10 ブルーグレー/レッド	Rx Tip 10 レッド/ブルーグレー	26	58	Rx Ring 10 ブルーグレー/レッド
Tx Tip 11 ブラック/ブルー	11	43	Tx Ring 11 ブルー/ブラック	Rx Tip 11 ブラック/ブルー	27	59	Rx Ring 11 ブルー/ブラック
Tx Tip 12 ブラック/オレンジ	12	44	Tx Ring 12 オレンジ/ブラック	Rx Tip 12 ブラック/オレンジ	28	60	Rx Ring 12 オレンジ/ブラック
Tx Tip 13 ブラック/グリーン	13	45	Tx Ring 13 グリーン/ブラック	Rx Tip 13 ブラック/グリーン	29	61	Rx Ring 13 グリーン/ブラック
Tx Tip 14 ブラック/ブラウン	14	46	Tx Ring 14 ブラウン/ブラック	Rx Tip 14 ブラック/ブラウン	30	62	Rx Ring 14 ブラウン/ブラック
Tx Tip 15 ブラック/ブルーグレー	15	47	Tx Tip 15 ブルーグレー/ブラック	Rx Tip 15 ブラック/ブルーグレー	31	63	Rx Tip 15 ブルーグレー/ブラック
Tx Tip 16 イエロー/ブルー	16	48	Tx Tip 16 ブルー/イエロー	Rx Tip 16 イエロー/ブルー	32	64	Rx Tip 16 ブルー/イエロー

ステップ 4　元の NTP（手順）に戻ります。

DLP-A25 BNC コネクタを使用した同軸ケーブルの取り付け

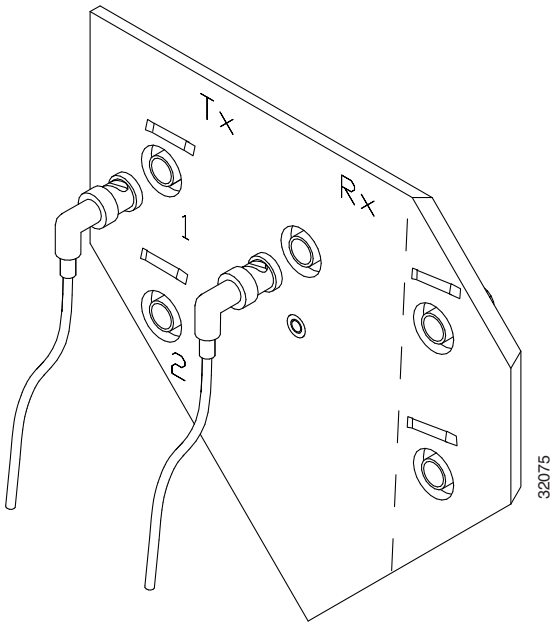
目的	この作業では、BNC コネクタを使用して同軸ケーブルを取り付けます。
工具 / 機器	なし
事前準備手順	「DLP-A12 BNC または 高密度 BNC EIA の取り付け」（p.17-14）
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

警告　**外部プラント回線（T1/E1/T3/E3　など）に接続するための金属製インターフェイスは、CSU/DSU（チャネル サービス ユニット / データ サービス ユニット）や NT1（ネットワーク終端 1）などの登録済みデバイスや承認済みデバイスを介して接続する必要があります。**

ステップ 1　バックプレーンの目的の接続ポイントに BNC ケーブル コネクタを合わせます。

図 17-15 に、直角 BNC ケーブル コネクタを使用して BNC EIA に同軸ケーブルを接続する方法を示します。

図 17-15　直角 BNC コネクタを使用した 同軸ケーブルの取り付け



ステップ 2　ケーブル コネクタのスロットがバックプレーン接続ポイントの対応するノッチの上にくるように、コネクタを合わせます。

ステップ 3　コネクタを静かに押し下げて、バックプレーン コネクタのノッチをケーブル コネクタのスロットにスライドさせます。

ステップ 4　ケーブル コネクタを右に回して、所定の位置にロックします。

ステップ 5　Telcordia 標準（GR-1275-CORE）または現地の規約に従って、ケーブルを EIA にタイ ラップするか、または撚り合わせます。

ステップ 6　現地の規約に従って、ケーブルをシェルフ アセンブリの最も近い側面の穴に通して、この側面に配線します。側面開口部のゴムで覆われたエッジが、ケーブルの摩擦を防ぎます。

ステップ 7　接続の両側ですべてのケーブルにラベルを付け、外見の似たケーブルが混同しないようにします。

ステップ 8　元の NTP（手順）に戻ります。

DLP-A26 高密度 BNC コネクタを使用した同軸ケーブルの取り付け

目的	この作業では、高密度 BNC コネクタを使用して同軸ケーブルを取り付けます。
工具 / 機器	BNC 取り付け工具
事前準備手順	「DLP-A12 BNC または 高密度 BNC EIA の取り付け」（p.17-14）
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

ステップ 1　バックプレーンの目的の接続ポイントにケーブル コネクタを合わせます。

ステップ 2　BNC 取り付け工具を使用して、ケーブル コネクタのスロットがバックプレーン接続ポイントの対応するノッチの上にくるように、コネクタを合わせます。

ステップ 3　コネクタを静かに押し下げて、バックプレーン コネクタのノッチをケーブル コネクタのスロットにスライドさせます。

ステップ 4　ケーブル コネクタを右に回して、ロックします。

ステップ 5　Telcordia 標準（GR-1275-CORE）または現地の規約に従って、ケーブルを EIA にタイ ラップするか、または撚り合わせます。

ステップ 6　現地の規約に従って、ケーブルをシェルフ アセンブリの最も近い側面の穴に通して、この側面に配線します。

側面開口部のゴムで覆われたエッジが、ケーブルの摩擦を防ぎます。

ステップ 7　元の NTP（手順）に戻ります。

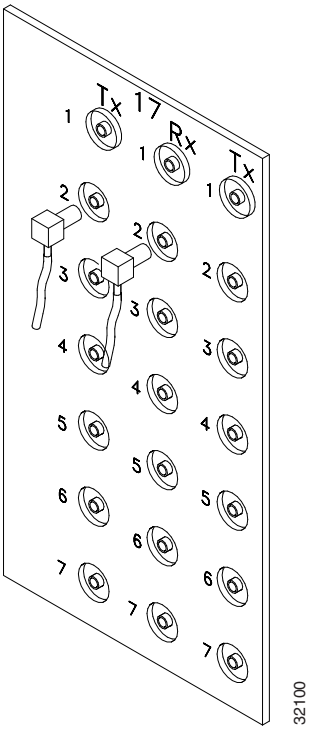
DLP-A27 SMB コネクタを使用した同軸ケーブルの取り付け

目的	この作業では、SMB コネクタを使用して同軸ケーブルを取り付けます。
工具 / 機器	SMB ケーブル コネクタ
事前準備手順	「DLP-A13 SMB EIA の取り付け」（p.17-16）
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

警告　**外部プラント回線（T1/E1/T3/E3　など）に接続するための金属製インターフェイスは、CSU/DSU や NT1 などの登録済みデバイスや承認済みデバイスを介して接続する必要があります。**

ステップ 1　バックプレーンの目的の接続ポイントに SMB ケーブル コネクタを合わせます（図 17-16）。

図 17-16　SMB コネクタを使用した同軸ケーブルの取り付け



ステップ 2　カチッという音がするまでコネクタを静かに押して、コネクタを固定します。

ステップ 3　Telcordia 標準（GR-1275-CORE）または現地の規約に従って、ケーブルを EIA にタイ ラップするか、または撚り合わせます。

ステップ 4　現地の規約に従って、ケーブルをシェルフ アセンブリの最も近い側面に這わせて、ラックに配線します。

ステップ 5　接続の両側で終端ケーブル、受信ケーブル、現用ケーブル、および保護ケーブルにラベルを付け、外見の似たケーブルと混同しないようにします。

ステップ 6　元の NTP（手順）に戻ります。

DLP-A28 同軸ケーブルの配線

目的	この作業では、同軸ケーブルを配線します。
工具 / 機器	RG179、RG59（735A）#26 AWG ケーブル、または RG59（734A）#20 AWG ケーブル
事前準備手順	必要に応じて次の作業を 1 つまたは複数実行します。 • 「DLP-A25 BNC コネクタを使用した同軸ケーブルの取り付け」（p.17-38） • 「DLP-A26 高密度 BNC コネクタを使用した同軸ケーブルの取り付け」（p.17-39） • 「DLP-A27 SMB コネクタを使用した同軸ケーブルの取り付け」（p.17-40）
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

ステップ 1　現地の規約に従って同軸ケーブルをタイ ラップするか撚り合わせて、ONS 15454 のいずれかの側面の穴を通してケーブルを配線します。側面開口部のゴムで覆われたエッジが、ケーブルの摩擦を防ぎます。

ステップ 2　短いピグテール RG179 を使用して、シェルフ アセンブリを終端します。

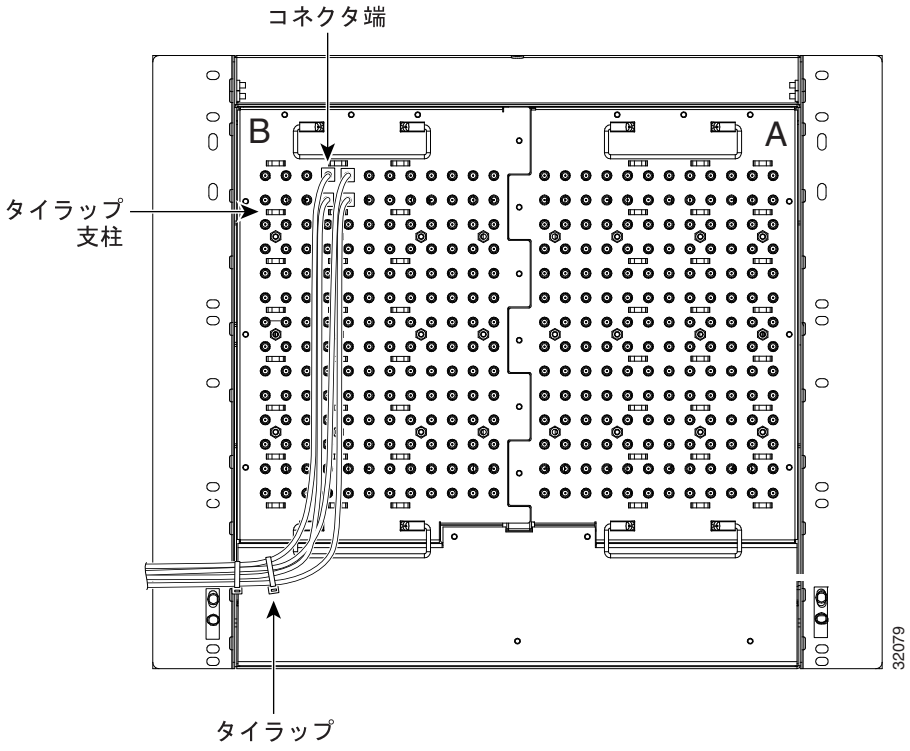
ステップ 3　RG179 に接続された標準 RG59（735A）ケーブルを使用して、残りのケーブルを配線します。10 フィート（3.05 m）の RG179 を使用した場合は、最大 437 フィート（133 m）の RG59（735A）を接続できます。30 フィート（9.1 m）の RG179 を使用した場合は、最大 311 フィート（94.8 m）の RG59（735A）を接続できます。

RG179 ケーブルを使用した場合の最大距離（122 フィート、37.2 m）は、標準 RG59（735A）ケーブルの最大距離（306 フィート、93.3 m）よりも短くなります。RG59（734A）ケーブルを使用した場合の最大距離は、450 フィート（137.2 m）です。RG179 の最大距離が短くなるのは、ケーブルが細いために減衰率が大きくなるからです。減衰率の計算には、DS-3 信号を使用します。

- RG179 の減衰率は、22 MHz で 59 dB/kft（dB/ キロ フィート）です。
- RG59（735A）の減衰率は、22 MHz で 23 dB/kft です。

計算するときは、ケーブル全体の損失に 5.0 を使用します。図 17-17 に、適切な同軸ケーブル配線例を示します。

図 17-17　同軸ケーブルの配線（SMB EIA バックプレーン）



ステップ 4　元の NTP（手順）に戻ります。

DLP-A29 DS-1 ツイストペア ケーブルの配線

目的	この作業では、DS-1 ツイストペア ケーブルを配線します。
工具 / 機器	なし
事前準備手順	「DLP-A23 電気インターフェイス アダプタ（バラン）を使用した DS-1 ケーブルの取り付け」（p.17-33）
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

ステップ 1　次の点を確認します。

- DS-1 ポートのすべての送受信コネクタに、DS-1 電気インターフェイス アダプタが取り付けられている。
- DS-1 電気インターフェイス アダプタのワイヤラップ支柱が、終端された着信ケーブルの接続に使用されている。

ステップ 2　現地の規約に従ってツイストペア ケーブルをタイ ラップするか撚り合わせて、ONS 15454 のいずれかの側面の穴を通してケーブルを配線します。

（注）　SMB EIA には、ケーブルをカバー パネルにタイ ラップしたり、撚り合わせるためのケーブル マネジメント アイレットがあります。

ステップ 3　元の NTP（手順）に戻ります。

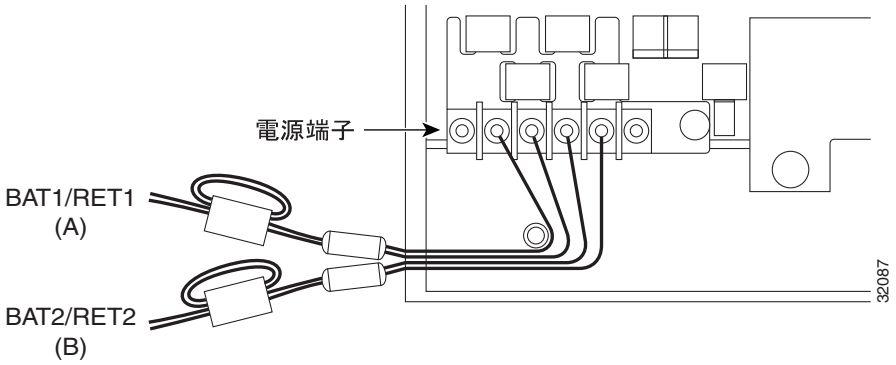
DLP-A30 電源コードへのフェライトの取り付け

目的	この作業では、電源コードにフェライトを取り付けます。ケーブル ペア（BAT1/RET1［A］および BAT2/RET2［B］）ごとに、クランプ型フェライト（TDK ZCAT2035-0930）とブロック フェライト（Fair Rite 0443164151）を 1 つずつ使用します。
工具 / 機器	クランプ型フェライトおよびブロック フェライト
事前準備手順	なし
必須 / 適宜	必須
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

ステップ 1　ケーブルをブロック フェライトの周りに 1 回巻いてブロック フェライトに通してから、クランプ型フェライトにまっすぐ通します。

ステップ 2　ONS 15454 とブロック フェライトの間の、電源端子にできるだけ近い位置に、クランプ型フェライトを配置します（図 17-18 を参照）。ブロック フェライトは電源端子の 5 ～ 6 インチ（127 ～ 152 mm）以内になければなりません。

図 17-18　ブロック フェライトとクランプ型フェライトおよび電源コードの接続



ステップ 3　元の NTP（手順）に戻ります。

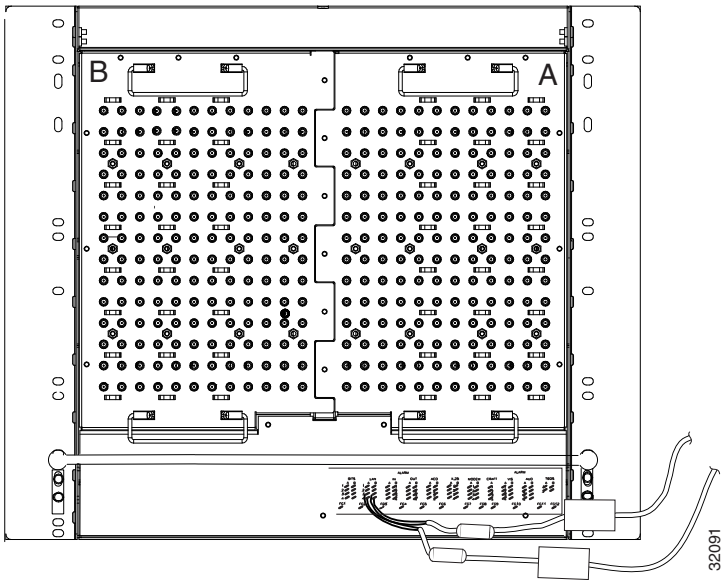
DLP-A31 ワイヤラップ ピン フィールドへのフェライトの接続

目的	この作業では、ワイヤラップ ピン フィールドにフェライトを接続します。ケーブル ペアごとに、クランプ型フェライト（TDK ZCAT1730-0730）とブロック フェライト（Fair Rite 0443164151）を 1 つずつ使用します。
工具 / 機器	クランプ型フェライトおよびブロック フェライト
事前準備手順	「NTP-A8 アラーム、タイミング、LAN、およびクラフト ピン接続のための配線」（p.1-19）
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

ステップ 1　ケーブルをブロック フェライトの周りに 1 回巻いてブロック フェライトに通してから、クランプ型フェライトにまっすぐ通します。

ステップ 2　ONS 15454 とブロック フェライトの間の、ワイヤラップ ピン フィールドにできるだけ近い位置に、クランプ型フェライトを配置します（図 17-19 を参照）。ブロック フェライトはワイヤラップ ピン フィールドの 5 ～ 6 インチ（127 ～ 152 mm）以内になければなりません。

図 17-19　ワイヤラップ ピン フィールドへのフェライトの接続



ステップ 3　元の NTP（手順）に戻ります。

DLP-A32 シェルフの取り付けおよび接続の検査

目的	この作業では、シェルフの取り付けおよび接続を検査し、すべてが正しく取り付けられ、接続されていることを確認します。
工具 / 機器	なし
事前準備手順	表 1-5（p.1-34）の作業を行います。
必須 / 適宜	必須
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

ステップ 1　各ワイヤおよびケーブル接続を調べ、すべてのケーブルがしっかりと固定されていることを確認します。ワイヤまたはケーブルが緩んでいる場合は、該当する取り付け手順に戻って直します。

ステップ 2　バックプレーンが正しく装着されているか調べるには、ネジ穴とバックプレーン インターフェイス カードの穴が正しく合っていること、および A コネクタと B コネクタがかみ合っていることを確認します。

ステップ 3　元の NTP（手順）に戻ります。

DLP-A33 電圧の測定

目的	この作業では、電力を測定して正しい電源およびリターンであることを確認します。
工具 / 機器	電圧計
事前準備手順	表 1-5（p.1-34）の作業を行います。
必須 / 適宜	必須
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

ステップ 1　電圧計を使用して、オフィス アースおよび電源を確認します。図 17-10（p.17-23）に電源端子を示します。

a. ブラックの線（プラス）を、ベイのフレーム アースに接続します。ステップ b が完了するまでそのままにします。

b. レッドの線（マイナス）を、ヒューズ電源ポイントおよびアラームパネルに接続し、–40.5 ～ –57 VDC（電源）または 0（リターン アース）となることを確認します。

ステップ 2　電圧計を使用して、シェルフ アースおよび電源の配線を確認します。

a. ブラックの線（プラス）を RET1 に、レッドの線を BAT1 ポイントに接続します。–40.5 ～ –57 VDC になることを確認します。電圧が存在しない場合は、次の点を調べ、必要に応じて修正します。

- バッテリおよびアースがシェルフに逆方向に流れていないか。
- バッテリが開いていたり、なくなっていたりしないか。
- リターンが開いていたり、なくなっていたりしないか。

b. B 電源装置が装備されている場合は、RET2 および BAT2 について、ステップ 2 を繰り返します。

ステップ 3　元の NTP（手順）に戻ります。

DLP-A34 最適化 1+1 保護グループの作成

目的	この作業では、OC3-4 および OC3-8 カードの最適化 1+1 保護グループを作成します。
工具 / 機器	取り付けられた OC3-4 カード、OC3-8 カード、または事前にプロビジョニングされたスロット
事前準備手順	「DLP-A60 CTC へのログイン」（p.17-79）
必須 / 適宜	適宜。この機能を使用する前に、ネットワーク管理者に問い合わせてください。
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　表 4-1（p.4-13）に示す、最適化 1+1 の要件に応じたカードが取り付けられていることを確認します。

ステップ 2　最適化 1+1 保護グループをプロビジョニングする OC3-4 または OC3-8 カードの該当するポートごとに、ポート タイプを SONET から SDH に変更します。

a.　ノード ビューで、該当するカードをダブルクリックします。

b.　**Provisioning > Line** タブをクリックします。

c.　ポートの横にある Type カラムのドロップダウン リストから **SDH** を選択して、**Apply** をクリックします。

ステップ 3　ノード ビューで、**Provisioning** > **Protection** タブをクリックします。

ステップ 4　Protection Groups 領域で、**Create** をクリックします。

ステップ 5　Create Protection Group ダイアログボックスで次の情報を入力します。

- Name — 保護グループの名前を入力します。保護グループ名には、32 文字までの英数字（a ～ z、A ～ Z、0 ～ 9）を使用します。特殊文字も使用できますが、TL1 と互換性を持たせるために、疑問符（?）、バックスラッシュ（\）、二重引用符（"）は使用しないでください。
- Type — ドロップダウン リストから **1+1 Optimized** を選択します。
- Protect Card — ドロップダウン リストから保護ポートを選択します。ドロップダウン リストには、使用可能な OC3-4 または OC3-8 ポートが表示されます。OC3-4 または OC3-8 カードが取り付けられていないと、ドロップダウン リストにポートは表示されません。

保護カードを選択すると、保護に使用できるカードのリストが Available Ports リストに表示されます（図 17-33 を参照）。使用可能なカードがないと、カードは表示されません。その場合は、この作業を行う前に、物理カードを取り付けるか、「DLP-A330 カード スロットの事前プロビジョニング」（p.20-24）を行って ONS 15454 スロットを事前にプロビジョニングする必要があります。

ステップ 6　Available Ports リストから、Protect Port フィールドで選択したポートで保護するポートを選択します。上にある矢印ボタンをクリックして、各ポートを Working Ports リストに移動します。

ステップ 7　残りのフィールドを次のように設定します。

- Reversion time — Revertive をオンにした場合に、ドロップダウン リストから復元時間を選択します。選択できる範囲は 0.5 ～ 12.0 分です。デフォルトは 5.0 分です。復元時間は、プライマリ チャネルがセカンダリに、セカンダリ チャネルがプライマリに自動変更されるまでの経過時間です。切り替えの原因になった状態が解消されると、復元タイマーが動き始めます。

- Verification guard time ― ドロップダウン リストから検証ガード時間を選択します。指定できる範囲は 500 ミリ秒 ～ 1 秒です。検証ガード タイマーは、遠端ノードからの強制切り替えコマンドを受け入れるように設定する場合に使用します。強制コマンドの着信時に、ロックアウトが存在しない場合、またはセカンダリ セクションに障害が発生していない場合は、発信 K1 バイトが強制を示すように変更され、検証ガード タイマーが開始します。検証ガード タイマーの有効期限内に、遠端側で強制切り替えコマンドが受け入れられない場合は、強制コマンドがクリアされます。
- Recovery guard time ― ドロップダウン リストから回復ガード時間を選択します。指定できる範囲は 0 ～ 10 秒です。デフォルトは 1 秒です。回復ガード タイマーは、信号劣化（SD）、または信号障害（SF）が原因で発生する短時間での切り替えを防止する場合に使用します。回線の SD/SF 障害がクリアされると、回復ガード タイマーが開始します。回復ガード時間は、SD/SF 障害が検出されてから、状態がクリアされたとシステムが宣言するまでの経過時間です。
- Detection guard time ― ドロップダウン リストから検出ガード時間を選択します。指定できる範囲は 0 ～ 5 秒です。デフォルトは 1 秒 です。検出ガード タイマーは、SD、SF、Loss of Signal（LOS; 信号損失）、Loss of Frame（LOF; フレーム損失）、Alarm Indication Signal - Line（AIS-L）障害が検出されると開始します。検出ガード時間は、アクティブ カードで SD、SF、LOS、LOF、AIS-L 障害が検出されてから、スタンバイ カードにトラフィックが切り替わるまでの経過時間です。

ステップ 8　**OK** をクリックします。

ステップ 9　元の NTP（手順）に戻ります。

DLP-A35 最適化 1+1 保護グループの変更

目的	この作業では、OC3-4 および OC3-8 カードの最適化 1+1 保護グループを変更します。
工具 / 機器	なし
事前準備手順	「DLP-A34 最適化 1+1 保護グループの作成」（p.17-48） 「DLP-A60 CTC へのログイン」（p.17-79）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　ノード ビューで、**Provisioning** > **Protection** タブをクリックします。

ステップ 2　Protection Groups 領域で、変更する最適化 1+1 保護グループをクリックします。

ステップ 3　Selected Group 領域で、次の情報を必要に応じて変更します。

- Name — 保護グループの名前を変更するときは、ここに新しい名前を入力します。保護グループの名前には、32 文字までの英数字が指定できます。
- Reversion time — Revertive をオンにした場合に、ドロップダウン リストから復元時間を選択します。選択できる範囲は 0.5 ～ 12.0 分です。デフォルトは 5.0 分です。復元時間は、プライマリ チャネルがセカンダリに、セカンダリ チャネルがプライマリに自動変更されるまでの経過時間です。
- Verification guard time — ドロップダウン リストから検証ガード時間を選択します。指定できる範囲は 500 ミリ秒 ～ 1 秒です。検証ガード タイマーは、遠端ノードからの強制切り替えコマンドを受け入れるように設定する場合に使用します。強制コマンドの着信時に、ロックアウトが存在しない場合、またはセカンダリ セクションに障害が発生していない場合は、発信 K1 バイトが強制を示すように変更され、検証ガード タイマーが開始しします。検証ガード タイマーの有効期限内に、遠端側で強制ユーザ コマンドが受け入れられない場合は、強制コマンドがクリアされます。
- Recovery guard time — ドロップダウン リストから回復ガード時間を選択します。指定できる範囲は 0 ～ 10 秒です。デフォルトは 1 秒です。回復ガード タイマーは、SD または SF 障害が原因で発生する短時間での切り替えを防止する場合に使用します。回線の SD/SF 障害がクリアされると、回復ガード タイマーが開始します。回復ガード時間は、SD/SF 障害が検出されてから、状態がクリアされたとシステムが宣言するまでの経過時間です。
- Detection guard time — ドロップダウン リストから検出ガード時間を選択します。指定できる範囲は 0 ～ 5 秒です。デフォルト値は 1 秒です。検出ガード タイマーは、SD、SF、LOS、LOF、または AIS-L 障害が検出されると開始します。検出ガード時間は、アクティブ カードで SD、SF、LOS、LOF、AIS-L 障害が検出されてから、スタンバイ カードにトラフィックが切り替わるまでの経過時間です。

ステップ 4　**Apply** をクリックします。変更内容を確認し、完了していなければ作業を繰り返します。

ステップ 5　元の NTP（手順）に戻ります。

DLP-A36 TCC2/TCC2P カードの取り付け

目的	この作業では、冗長 TCC2/TCC2P カードを取り付けます。ONS 15454 に取り付ける最初のカードは、TCC2/TCC2P カードでなければなりません。他のクロスコネクト カードやトラフィック カードを取り付ける前に、この TCC2/TCC2P カードを初期化しておく必要があります。
工具 / 機器	TCC2/TCC2P カード（2）
事前準備手順	なし
必須 / 適宜	必須
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

（注） カードを取り付ける場合は、各カードのブートが完了してから、次のカードを取り付けてください。

ステップ 1　取り付ける TCC2/TCC2P カードのラッチまたはイジェクタを開きます。

ステップ 2　ラッチまたはイジェクタを使用して、ガイド レールに沿ってカードをスライドさせ、スロット（スロット 7 または 11）の後ろのレセプタクルにカードを確実に取り付けます。

ステップ 3　カードが正しく挿入されていることを確認して、カードのラッチまたはイジェクタを閉めます。

（注） カードがバックプレーンに完全に取り付けられていない状態でも、ラッチまたはイジェクタが閉まることがあります。カードをそれ以上挿入できないことを確かめてください。

別のカード用にプロビジョニングされたスロットにカードを挿入すると、すべての LED が消灯します。

ステップ 4　TCC2 カードの場合は、ステップ a を実行して LED の動作を確認します。TCC2P カードの場合は、ステップ b を実行します。

a. TCC2 カードの場合

- すべての LED が短時間点灯します。
- レッドの FAIL LED、イエローの ACT/STBY LED、レッドの REM LED、グリーンの SYNC LED、およびグリーンの ACO LED が約 10 秒間点灯します。
- レッドの FAIL LED とグリーンの ACT/STBY LED が約 40 秒間点灯します。
- レッドの FAIL LED が約 10 秒間点滅します。
- レッドの FAIL LED が約 5 秒間点灯します。
- グリーンの 2 つの PWR LED がともに 5 秒間点灯します。その後、その PWR LED は 2 ～ 3 分間レッドに変わってから、グリーンになります。
- すべての LED（CRIT、MAJ、MIN、REM、SYNC、および ACO LED を含む）が一度点滅してから、約 10 秒間消灯します。
- イエローの ACT/STBY LED が点灯します（Data Communication Channel［DCC; データ通信チャネル］プロセッサのブート中は、ACT/STBY LED が点灯するのに数分かかることがあります）。

（注）　A 電源アラームと B 電源アラームがクリアされるまでに、最大 3 分かかる場合があります。

（注）　アラーム LED が点灯することがありますが、Cisco Transport Controller（CTC）にログインしてアラーム タブを表示できるようになるまでは、アラーム LED を無視してください。

（注）　CTC にログインしている場合は、TCC2 カードの初期化中に SFTWDOWN アラームが 2 回表示されます。このアラームは、カードのブートが完了するとクリアされます。

（注）　FAIL LED が連続して点灯する場合は、TCC2 カードの自動アップロードと関係している可能性があります。ステップ 8 のヒントを参照してください。

b. TCC2P カードの場合

- すべての LED が短時間点灯します。
- レッドの FAIL LED、イエローの ACT/STBY LED、レッドの REM LED、グリーンの SYNC LED、およびグリーンの ACO LED が約 10 秒間点灯します。
- レッドの FAIL LED とグリーンの ACT/STBY LED が約 40 秒間点灯します。
- レッドの FAIL LED が約 10 秒間点滅します。
- レッドの FAIL LED が約 5 秒間点灯します。
- レッドの FAIL LED が約 5 秒間点滅してから点灯します。
- すべての LED（CRIT、MAJ、MIN、REM、SYNC、および ACO LED を含む）が一度点滅してから、約 10 秒間消灯します。
- グリーンの 2 つの PWR LED がともに 5 秒間点灯します。その後、その PWR LED は 2 ～ 3 分間レッドに変わってから、グリーンになります。
- イエローの ACT/STBY が点灯し、PWR LED が 2、3 分の間レッドに点灯します（この時点で Sync LED はグリーンになっている可能性があります）。
- イエローの ACT/STBY LED が点灯します（DCC プロセッサのブート中は、ACT/STBY LED が点灯するのに数分かかることがあります）。

（注）　A 電源アラームと B 電源アラームがクリアされるまでに、最大 3 分かかる場合があります。

（注）　アラーム LED が点灯することがありますが、CTC にログインしてアラーム タブを表示できるようになるまでは、アラーム LED を無視してください。

（注）　CTC にログインしている場合は、TCC2P カードの初期化中に SFTWDOWN アラームが 2 回表示されます。このアラームは、カードのブートが完了するとクリアされます。

（注） FAIL LED が連続して点灯する場合は、TCC2P カードの自動アップロードと関係している可能性があります。ステップ 8 のヒントを参照してください。

ステップ 5　TCC2/TCC2P カードの ACT/STBY LED を見て、そのカードが最初に電源を入れたカードであれば、LED の色がグリーン（アクティブ）になっていることを確認します。また、そのカードが 2 番めに電源を入れたカードであれば、LED の色がイエロー（スタンバイ）になっていることを確認します。IP アドレス、ノードの温度、および日時が LCD に表示されます。デフォルトの日付と時刻は、1970 年 1 月 1 日 12:00 AM です。

ステップ 6　LCD に、IP アドレス、ノード名、およびソフトウェア バージョンが順番に繰り返されて表示されます。正しいソフトウェア バージョンが LCD に表示されていることを確認します。

ステップ 7　LCD に正しいソフトウェア バージョンが表示されている場合は、ステップ 8 へ進みます。LCD に正しいソフトウェア バージョンが表示されていない場合は、ソフトウェアをアップグレードするか、または TCC2/TCC2P カードを取り外して交換用カードを取り付けてください。

ソフトウェアを交換する場合は、そのリリース専用のソフトウェア アップグレード マニュアルを参照してください。TCC2/TCC2P カードの交換については、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。

ステップ 8　冗長 TCC2/TCC2P カードに対してステップ 1 ～ 7 を繰り返します。

ヒント　アクティブ カードとソフトウェア バージョンの異なるスタンバイ TCC2/TCC2P カードを取り付けると、新たに取り付けたそのスタンバイ TCC2/TCC2P カードにアクティブ TCC2/TCC2P カードのソフトウェア バージョンが自動的にコピーされます。この自動処理に対しては、特に対応する必要はありません。ただし、ソフトウェアをロードしている TCC2/TCC2P カードの起動の様子は、通常とは異なります。スタンバイ カードを最初に挿入したとき、LED はステップ 4 に列挙されているシーケンスにほぼ従って動作します。レッドの FAIL LED が約 5 秒間点灯したあと、新しいソフトウェアをアクティブ TCC2/TCC2P カード上でロードしている間、FAIL LED と ACT/STBY LED が最大 30 分間交互に点滅を始めます。新しいソフトウェアをロードしたあと、アップグレードされた TCC2/TCC2P カードの LED が ステップ 4 のシーケンスを繰り返し、オレンジの ACT/STBY LED が点灯します。

（注） 別のカード用にプロビジョニングされたスロットにカードを挿入すると、すべての LED が消灯します。

（注） アラーム LED が点灯することがありますが、CTC にログインしてアラーム タブを表示できるようになるまでは、アラーム LED を無視してください。

ステップ 9　ACT/STBY LED がスタンバイを示すオレンジになっていることを確認します。

ステップ 10　元の NTP（手順）に戻ります。

DLP-A37 XCVT、XC10G、または XC-VXC-10G カードの取り付け

目的	この作業では、クロスコネクト（XCVT/XC10G/XC-VXC-10G）カードを取り付けます。
工具 / 機器	XCVT/XC10G/XC-VXC-10G（クロスコネクト）カード
事前準備手順	「DLP-A36 TCC2/TCC2P カードの取り付け」（p.17-51）
必須 / 適宜	必須
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

（注） クロスコネクト カードをアップグレードする場合は、この手順を使用しないでください。XCVT カードを XC10G カードに、または XC10G カードを XC-VXC-10G カードにアップグレードする場合は、第 12 章「カードとスパンのアップグレード」を参照してください。

（注） カードを取り付ける場合は、各カードのブートが完了してから、次のカードを取り付けてください。

ステップ 1　取り付ける 1 つめの XCVT、XC10G、または XC-VXC-10G カードのラッチまたはイジェクタを開きます。

ステップ 2　ラッチまたはイジェクタを使用して、ガイド レールに沿ってカードをスライドさせ、スロット（スロット 8 または 10）の後ろのレセプタクルにカードを確実に取り付けます。

ステップ 3　カードが正しく挿入されていることを確認して、カードのラッチまたはイジェクタを閉めます。

（注） カードがバックプレーンに完全に取り付けられていない状態でも、ラッチまたはイジェクタが閉まることがあります。カードをそれ以上挿入できないことを確かめてください。

ステップ 4　LED の動作を確認します。

- レッドの FAIL LED が 20 ～ 30 秒間点灯します。
- レッドの FAIL LED が 35 ～ 45 秒間点滅します。
- レッドの FAIL LED が 5 ～ 10 秒間点灯します。
- すべての LED が一度点滅してから点灯します。
- ACT/STBY LED が点灯します。

（注） 別のカード用にプロビジョニングされたスロットにカードを挿入すると、すべての LED が消灯します。

（注） レッドの FAIL LED が点灯しない場合は、電源を調べてください。

（注）　レッドの FAIL LED が連続して点灯する場合や、LED の動作が異常な場合は、カードが正しく取り付けられていません。カードを取り外して、ステップ 1 ～ 4 を繰り返してください。

ステップ 5　ACT/STBY LED がアクティブを示すグリーンになっていることを確認します。

ステップ 6　ラッチまたはイジェクタを使用して、ガイド レールに沿って 2 つめのクロスコネクト カードをスライドさせ、スロット（スロット 8 または 10）の後ろのレセプタクルにカードを確実に取り付けます。

ステップ 7　カードが正しく挿入されていることを確認して、カードのラッチまたはイジェクタを閉めます。

（注）　カードがバックプレーンに完全に取り付けられていない状態でも、ラッチまたはイジェクタが閉まることがあります。カードをそれ以上挿入できないことを確かめてください。

ステップ 8　LED の動作を確認します。

- レッドの FAIL LED が 20 ～ 30 秒間点灯します。
- レッドの FAIL LED が 35 ～ 45 秒間点滅します。
- レッドの FAIL LED が 5 ～ 10 秒間点灯します。
- すべての LED が一度点滅してから点灯します。
- ACT/STBY LED が点灯します。

（注）　別のカード用にプロビジョニングされたスロットにカードを挿入すると、すべての LED が消灯します。

（注）　レッドの FAIL LED が点灯しない場合は、電源を調べてください。

（注）　レッドの FAIL LED が連続して点灯する場合や、LED の動作が異常な場合は、カードが正しく取り付けられていません。カードを取り外して、ステップ 6 ～ 8 をやり直してください。

ステップ 9　ACT/STBY LED がスタンバイを示すオレンジになっていることを確認します。

ステップ 10　元の NTP（手順）に戻ります。

DLP-A39 イーサネット カードの取り付け

目的	この作業では、イーサネット カード（E100T-12、E100T-G、E1000-2、E1000-2-G、G1K-4、ML100T-12、ML1000-2、ML100X-8、および CE-100T-8）を取り付けます。
工具 / 機器	イーサネット カード
事前準備手順	「NTP-A15 共通コントロール カードの取り付け」（p.2-3）
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

ステップ 1　カードのラッチまたはイジェクタを開きます。

ステップ 2　ラッチまたはイジェクタを使用して、ガイド レールに沿ってカードをしっかりとスライドさせ、スロットの後方のレセプタクルにカードを取り付けます。

ステップ 3　カードが正しく挿入されていることを確認して、カードのラッチまたはイジェクタを閉めます。

（注）　カードがバックプレーンに完全に取り付けられていない状態でも、ラッチまたはイジェクタが閉まることがあります。カードをそれ以上挿入できないことを確かめてください。

ステップ 4　LED の動作を確認します。

- レッドの FAIL LED が 20 ～ 30 秒間点灯します。
- レッドの FAIL LED が 35 ～ 45 秒間点滅します。
- すべての LED が一度点滅してから、1 ～ 5 秒間消灯します。
- ACT または ACT/STBY LED が点灯します。SF LED は、すべてのカード ポートがそれぞれの遠端の相手先に接続されて、信号が発生するまで点灯し続けます。

（注）　レッドの FAIL LED が点灯しない場合は、電源を調べてください。

（注）　別のカード用にプロビジョニングされたスロットにカードを挿入すると、すべての LED が消灯します。

ステップ 5　元の NTP（手順）に戻ります。

DLP-A41 AIC-I カードの取り付け

目的	この作業では、AIC-I カードを取り付けます。AIC-I カードは、外部アラームおよび制御（環境アラーム）の接続に使用します。
工具 / 機器	AIC-I カード
事前準備手順	「DLP-A36 TCC2/TCC2P カードの取り付け」（p.17-51） 「DLP-A37 XCVT、XC10G、または XC-VXC-10G カードの取り付け」（p.17-54）
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

（注） カードを取り付ける場合は、各カードのブートが完了してから、次のカードを取り付けてください。

ステップ 1　カードのラッチまたはイジェクタを開きます。

ステップ 2　ラッチまたはイジェクタを使用して、ガイド レールに沿ってカードをスライドさせ、スロット（スロット 9）の後ろのレセプタクルにカードを確実に取り付けます。

ステップ 3　カードが正しく挿入されていることを確認して、カードのラッチまたはイジェクタを閉めます。

（注） カードがバックプレーンに完全に取り付けられていない状態でも、ラッチまたはイジェクタが閉まることがあります。カードをそれ以上挿入できないことを確かめてください。

ステップ 4　次の点を確認します。

- レッドの FAIL LED が 1 秒間点灯したあと、1 ～ 5 秒間点滅します。
- PWR A LED と PWR B LED がレッドになり、2 つの INPUT/OUTPUT LED が約 3 秒間グリーンになります。
- PWR A LED がグリーンになってから、INPUT/OUTPUT LED が消灯し、次に ACT LED が点灯します。レッドの FAIL LED が点灯しない場合は、電源を調べてください。

（注） PWR A LED と PWR B LED が更新されるまでに、最大 3 分かかる場合があります。

（注） 別のカード用にプロビジョニングされたスロットにカードを挿入すると、すべての LED が消灯します。

（注） レッドの FAIL LED が連続して点灯する場合や、LED の動作が異常な場合は、カードが正しく取り付けられていません。カードを取り外して、ステップ 1 ～ 4 を繰り返してください。

ステップ 5　元の NTP（手順）に戻ります。

DLP-A43 UPSR 構成での光ファイバ ケーブルの取り付け

目的	この作業では、各ノードのイーストおよびウェスト Unidirectional Path Switched Ring（UPSR; 単方向パス スイッチ型リング）ポートに光ファイバ ケーブルを接続します。UPSR 構成のプロビジョニングとテストについては、第 5 章「ネットワークの起動」を参照してください。
工具 / 機器	光ファイバ ケーブル
事前準備手順	「NTP-A112 ファイバ コネクタの清掃」（p.15-19）
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

（注）　間違いを防止するために、右端のスロットをイースト ポートとし、左端のスロットをウェスト ポートとして、光ファイバ ケーブルを接続します。あるノードのイースト ポートに接続されたファイバは、隣接ノードのウェスト ポートに接続する必要があります。

注意　UPSR のイースト ポートとウェスト ポートは、同じ OC-N カードにプロビジョニングしないでください。

ステップ 1　ファイバの接続関係を計画します。すべての UPSR ノードに対して同じ計画を使用します。

ステップ 2　ファイバをあるノードの OC-N カードの送信（Tx）コネクタに接続し、もう一方の端を隣接ノードの OC-N カードの受信（Rx）コネクタに接続します。送信用のファイバと受信用のファイバが一致していない（1 本のファイバが、あるカードの受信ポートと他のカードの受信ポートを接続している、あるいは送信ポートで同様の状況になっている）と、カードの SF LED が点灯します。

ステップ 3　リングの構成が完了するまで、ステップ 2 を繰り返します。

図 17-20 に、スロット 5（ウェスト）とスロット 12（イースト）にトランク（スパン）カードを備えた、4 ノード UPSR のファイバ接続を示します。

図 17-20　4 ノード UPSR へのファイバ接続

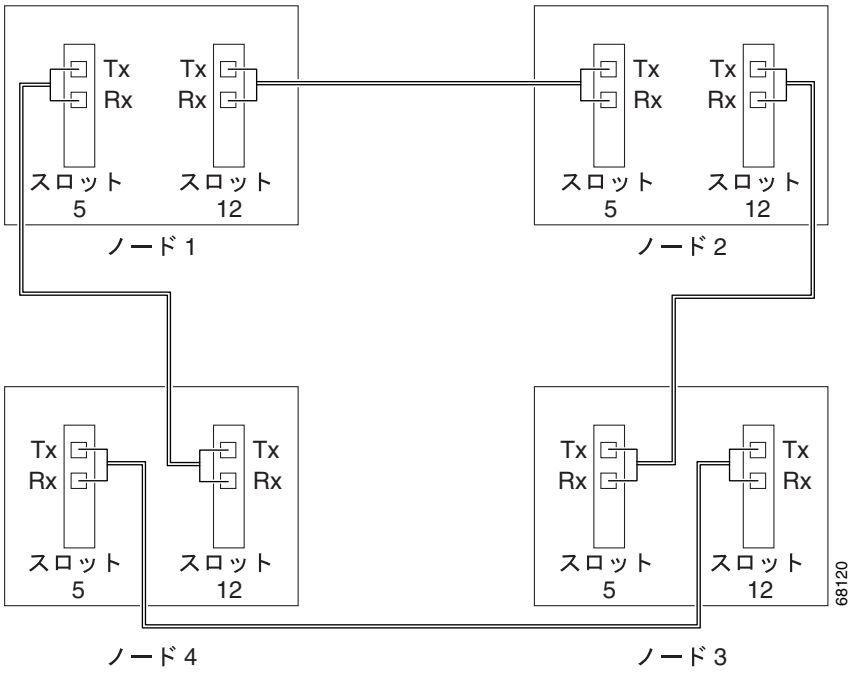


図 17-21 に、従来型 UPSR デュアル リング相互接続（DRI）の例を示します。

図 17-21　8 ノードの従来型 UPSR DRI へのファイバ接続

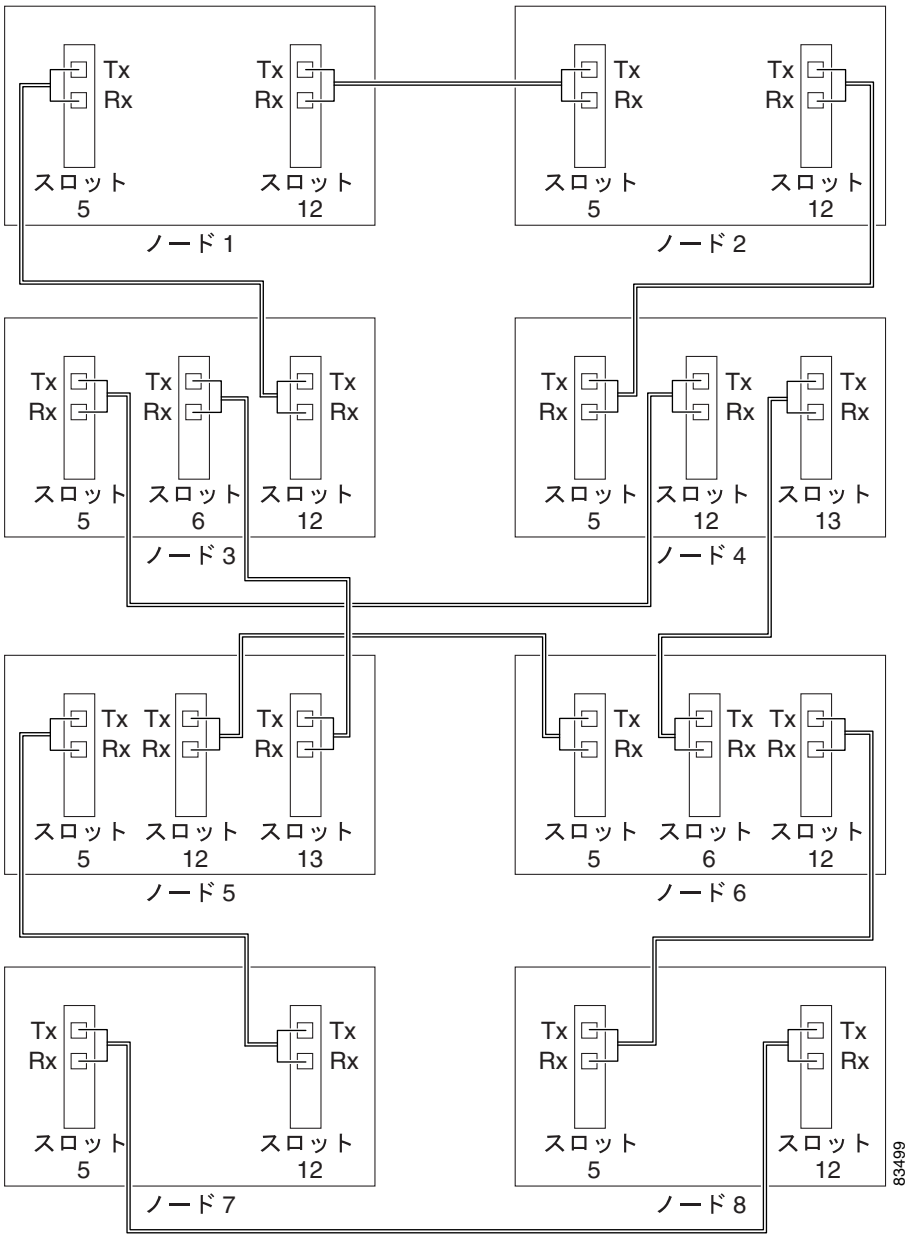
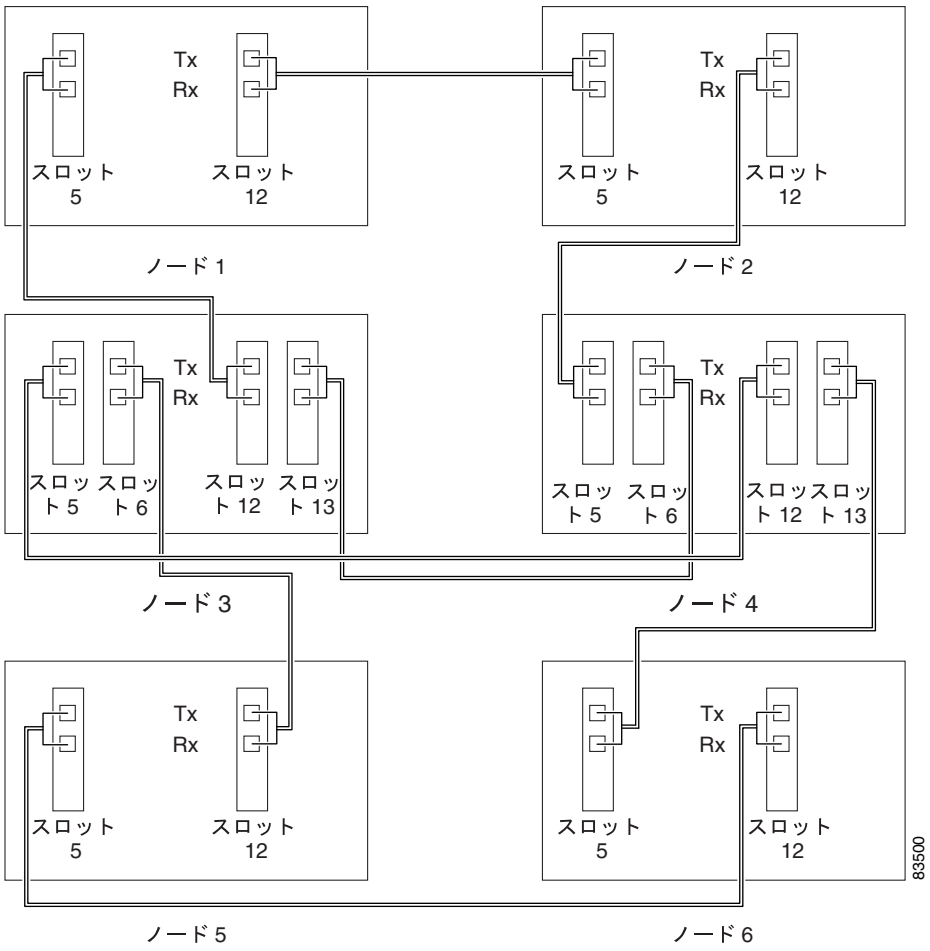


図 17-22 に、統合 DRI の例を示します。

図 17-22　6 ノードの統合 UPSR DRI へのファイバ接続



ステップ 4　元の NTP（手順）に戻ります。

DLP-A44 BLSR 構成での光ファイバ ケーブルの取り付け

目的	この作業では、各ノードのイーストおよびウェスト Bidirectional Line Switched Ring（BLSR; 双方向ライン スイッチ型リング）ポートに光ファイバ ケーブルを接続します。BLSR 構成のプロビジョニングとテストについては、第 5 章「ネットワークの起動」を参照してください。
工具 / 機器	光ファイバ ケーブル
事前準備手順	「NTP-A112 ファイバ コネクタの清掃」（p.15-19）
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

（注） 間違いを防止するために、右端のスロットをイースト ポートとし、左端のスロットをウェスト ポートとして、光ファイバ ケーブルを接続します。あるノードのイースト ポートに接続されたファイバは、隣接ノードのウェスト ポートに接続する必要があります。

注意 BLSR のイースト ポートとウェスト ポートは、同じ OC-N カードにプロビジョニングしないでください。

ステップ 1　ファイバの接続関係を計画します。すべての BLSR ノードに対して同じ計画を使用します。

ステップ 2　ファイバをあるノードの OC-N カードの送信（Tx）コネクタに接続し、もう一方の端を隣接ノードの OC-N カードの受信（Rx）コネクタに接続します。送信用のファイバと受信用のファイバが一致していないと、カードの SF LED が点灯します。

（注） 4 ファイバ BLSR を接続する場合は、現用カードと保護カードの接続を混在させないでください。現用カードと保護カードが相互接続されていると、BLSR は機能しません。4 ファイバ BLSR の正しいケーブル接続の例については、図 17-24（p.17-63）を参照してください。

ステップ 3　リングの構成が完了するまで、ステップ 2 を繰り返します。

図 17-23 に、スロット 5（ウェスト）とスロット 12（イースト）にトランク（スパン）カードを備えた、2 ファイバ BLSR のファイバ接続を示します。

図 17-23　4 ノード、2 ファイバ BLSR でのファイバ接続

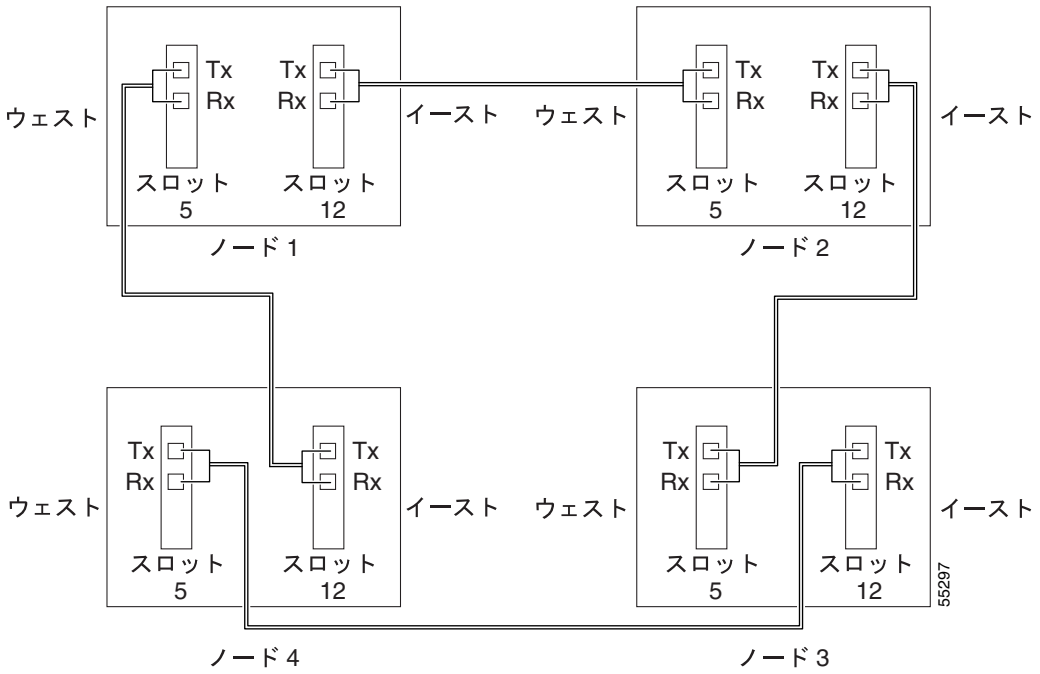
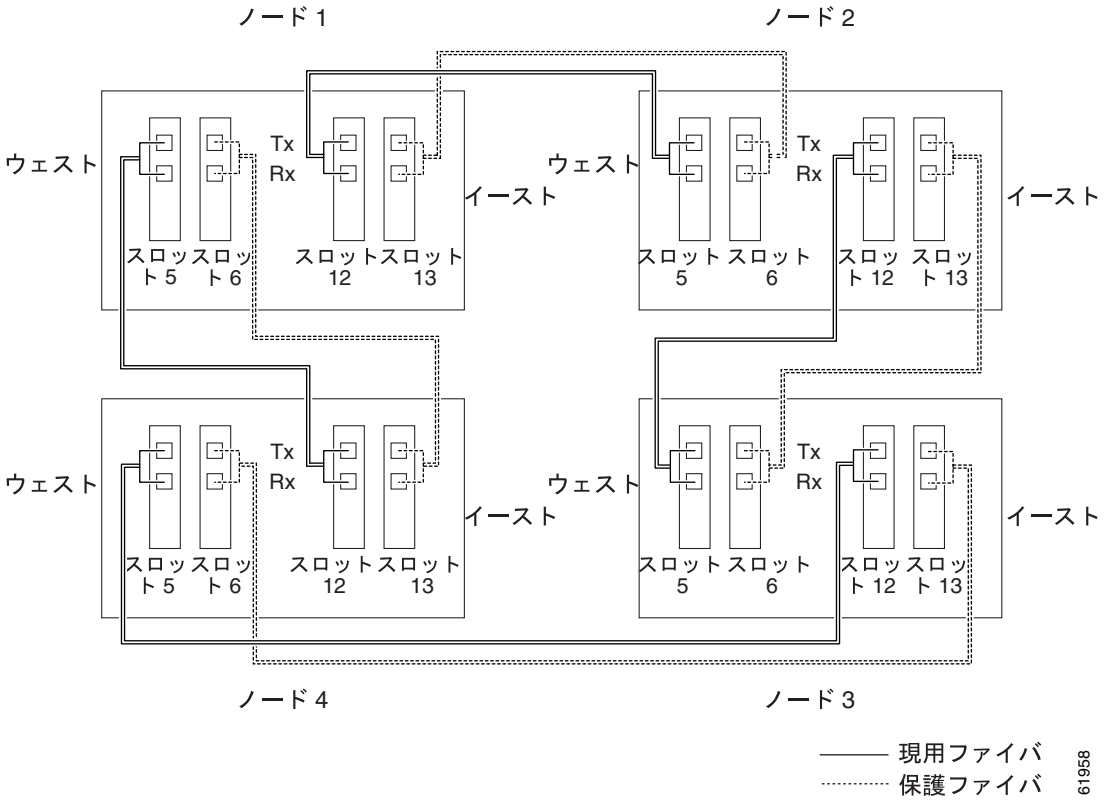


図 17-24 に、4 ファイバ BLSR のファイバ接続を示します。スロット 5（ウェスト）とスロット 12（イースト）は現用トラフィックを伝送します。スロット 6（ウェスト）とスロット 13（イースト）は保護トラフィックを伝送します。

図 17-24　4 ノード、4 ファイバ BLSR でのファイバ接続



ステップ 4　元の NTP（手順）に戻ります。

DLP-A45 ファイバ ブーツの取り付け

目的	この作業では、ファイバが屈曲し過ぎないように保護するファイバ ブーツを取り付けます。OC-192、OC192-XFP、および OC-48 AS カードでは、角度の付いた SC コネクタを使用しているためブーツは必要ありませんが、これらを除くすべての OC-N カードに、ファイバ ブーツが必要です。
工具 / 機器	ファイバ ブーツ
事前準備手順	「NTP-A16 光カードおよびコネクタの取り付け」（p.2-8）
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

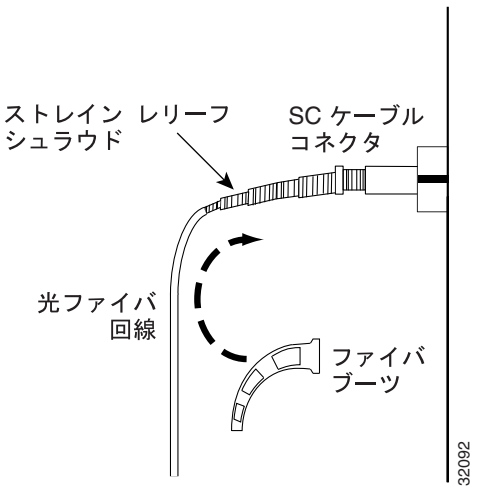
（注）　光ファイバ ケーブルを OC-N カードに取り付ける前、または取り付けたあとに、光ファイバ ケーブルにファイバ ブーツを取り付けることができます。

（注）　OC3IR/STM1SH 1310-8 カードを取り付ける場合は、ポート 8 の Rx ファイバ コネクタに、ファイバ ブーツの代わりにファイバ クリップを使用する必要があります。

ステップ 1　光ファイバ ケーブルの下にファイバ ブーツの開いたスロットを位置合わせします。

ステップ 2　光ファイバ ケーブルをファイバ ブーツに押し込みます。図 17-25 にファイバ ブーツの取り付けを示します。

図 17-25　ファイバ ブーツの取り付け



ステップ 3　ファイバ ブーツをひねって、光ファイバ ケーブルをファイバ ブーツの末端に固定します。

ステップ 4　光ファイバ ケーブルに沿ってファイバ ブーツを前方にスライドさせて、SC ケーブル コネクタの端にファイバ ブーツをぴったりとはめ込みます。

ステップ 5　元の NTP（手順）に戻ります。

DLP-A50 スタティック IP アドレスを使用して同一サブネット上の ONS 15454 にクラフト接続するための Windows PC の設定

目的	この作業では、次のような場合に ONS 15454 にローカル クラフト接続するようにコンピュータを設定します。 • リリース 3.3 より前のソフトウェア リリースが稼働するノードにアクセスする。 • 1 つの ONS 15454 に接続する。複数の ONS 15454 に接続する場合は、ONS 15454 へ接続するたびにコンピュータの IP を設定しなければならないことがあります。 • ONS 15454 には備わっていないアプリケーション（ping や tracert［トレース ルート］など）を使用する必要がある。
工具 / 機器	なし
事前準備手順	「NTP-A260 CTC 用コンピュータのセットアップ」（p.3-2）
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

ステップ 1　コンピュータにインストールされている OS（オペレーティング システム）を確認してください。

a.　Windows の［スタート］メニューから、［**設定**］>［**コントロール パネル**］の順に選択します。

b.　［コントロール パネル］ウィンドウ内の［**システム**］アイコンをダブルクリックします。

c.　［システムのプロパティ］ウィンドウの［全般］タブで、Windows の OS が Windows 98、Windows NT 4.0、Windows 2000、または Windows XP のいずれかであることを確認します。

ステップ 2　コンピュータにインストールされている Windows の OS に応じて、次のステップのいずれかを実行してください。

- Windows 98 の場合は、ステップ 3 を実行します。
- Windows NT 4.0 の場合は、ステップ 4 を実行します。
- Windows 2000 の場合は、ステップ 5 を実行します。
- Windows XP の場合は、ステップ 6 を実行します。

ステップ 3　PC に Windows 98 がインストールされている場合は、次のステップを実行して TCP/IP の設定を変更してください。

a.　Windows の［スタート］メニューから、［**設定**］>［**コントロール パネル**］の順に選択します。

b.　［コントロール パネル］ダイアログボックス内で［**ネットワーク**］アイコンをクリックします。

c. ［ネットワーク］ダイアログボックスで、使用している NIC カード用の **TCP/IP** を選択し、［**プロパティ**］をクリックします。

d. ［TCP/IP のプロパティ］ダイアログボックスで、［**DNS 設定**］タブをクリックし、［**DNS を使わない**］を選択します。

e. ［**WINS 設定**］タブをクリックし、［**WINS の解決をしない**］を選択します。

f. ［**IP アドレス**］タブをクリックします。

g. ［IP アドレス］ウィンドウ内の［**IP アドレスを指定**］をクリックします。

h. ［IP アドレス］フィールドに、最後のオクテットを除いて ONS 15454 の IP アドレスと同じ IP アドレスを入力します。最後のオクテットは、1 または 3 ～ 254 の値にする必要があります。ノードをプロビジョニングしているときに LCD の表示を無効にしていなければ、その LCD にこの IP アドレスが表示されます。

i. ［**サブネット マスク**］フィールドに、ONS 15454 と同じサブネット マスクを入力します。デフォルトは **255.255.255.0**（24 ビット）です。

j. ［**OK**］をクリックします。

k. TCP/IP のダイアログボックス内で［**ゲートウェイ**］タブをクリックします。

l. ［新しいゲートウェイ］フィールドに ONS 15454 の IP アドレスを入力します。［**追加**］をクリックします。

m. その IP アドレスが［インストールされているゲートウェイ］フィールドに表示されていることを確認してから［**OK**］をクリックします。

n. PC を再起動するよう求めるプロンプトが表示されたら、［**はい**］をクリックします。

ステップ 4　PC に Windows NT 4.0 がインストールされている場合は、次のステップを実行して TCP/IP の設定を変更してください。

a. Windows の［スタート］メニューから、［**設定**］>［**コントロール パネル**］の順に選択します。

b. ［コントロール パネル］ダイアログボックス内で［**ネットワーク**］アイコンをクリックします。

c. ［ネットワーク］ダイアログボックスで、［**プロトコル**］タブをクリックし、［**TCP/IP のプロトコル**］を選択してから［**プロパティ**］をクリックします。

d. ［**IP アドレス**］タブをクリックします。

e. ［IP アドレス］ウィンドウ内の［**IP アドレスを指定**］をクリックします。

f. ［IP アドレス］フィールドに、最後のオクテットを除いて ONS 15454 の IP アドレスと同じ IP アドレスを入力します。最後のオクテットは、1 または 3 ～ 254 の値にする必要があります。ノードをプロビジョニングしているときに LCD の表示を無効にしていなければ、その LCD にこの IP アドレスが表示されます。

g. ［サブネット マスク］フィールドに **255.255.255.0** と入力します。

h. ［**詳細**］をクリックします。

i. ［ゲートウェイ］で［**追加**］をクリックします。［TCP/IP ゲートウェイ アドレス］ダイアログボックスが表示されます。

j. ［ゲートウェイ アドレス］フィールドに ONS 15454 の IP アドレスを入力します。

k. ［**追加**］をクリックします。

l. ［**OK**］をクリックします。

m. ［**適用**］をクリックします。

n. Windows NT 4.0 の場合は、PC をリブートするように求めるプロンプトが表示されることがあります。このプロンプトが表示されたら、［**はい**］をクリックします。

ステップ 5　PC に Windows 2000 がインストールされている場合は、次のステップを実行して TCP/IP の設定を変更してください。

a. Windows の［スタート］メニューから、［**設定** ］>［**ネットワークとダイヤルアップ接続** ］>［**ローカル エリア接続**］の順に選択します。

b. ［ローカル エリア接続の状態］ダイアログボックス内の［**プロパティ**］をクリックします。

c. ［全般］タブで、［**インターネット プロトコル（TCP/IP）**］を選択し、［**プロパティ**］をクリックします。

d. ［**次の IP アドレスを使う**］をクリックします。

e. ［IP アドレス］フィールドに、最後のオクテットを除いて ONS 15454 の IP アドレスと同じ IP アドレスを入力します。最後のオクテットは、1 または 3 ～ 254 の値にする必要があります。ノードをプロビジョニングしているときに LCD の表示を無効にしていなければ、その LCD にこの IP アドレスが表示されます。

f. ［サブネット マスク］フィールドに **255.255.255.0** と入力します。

g. ［デフォルト ゲートウェイ］フィールドに ONS 15454 の IP アドレスを入力します。

h. ［**OK**］をクリックします。

i. ［ローカル エリア接続のプロパティ］ダイアログボックス内で［**OK**］をクリックします。

j. ［ローカル エリア接続の状態］ダイアログボックス内で［**閉じる**］をクリックします。

ステップ 6　PC に Windows XP がインストールされている場合は、次のステップを実行して TCP/IP の設定を変更してください。

a. Windows の［スタート］メニューから、［**コントロール パネル**］>［**ネットワーク接続**］の順に選択します。

（注）　［ネットワーク接続］メニューが有効になっていない場合は、［**クラシック表示に切り替える**］をクリックします。

b. ［ネットワーク接続］ダイアログボックス内の［**ローカル エリア接続**］アイコンをクリックします。

c. ［ローカル　エリア接続のプロパティ］ダイアログボックスで、［**インターネット　プロトコル（TCP/IP）**］を選択し、［**プロパティ**］をクリックします。

d. ［IP アドレス］フィールドに、最後のオクテットを除いて ONS 15454 の IP アドレスと同じ IP アドレスを入力します。最後のオクテットは、1 または 3 ～ 254 の値にする必要があります。ノードをプロビジョニングしているときに LCD の表示を無効にしていなければ、その LCD にこの IP アドレスが表示されます。

e. ［サブネット マスク］フィールドに **255.255.255.0** と入力します。

f. ［デフォルト ゲートウェイ］フィールドに ONS 15454 の IP アドレスを入力します。

g. ［**OK**］をクリックします。

h. ［ローカル エリア接続のプロパティ］ダイアログボックス内で［**OK** ］をクリックします。

i. ［ローカル エリア接続の状態］ダイアログボックス内で［**閉じる**］をクリックします。

ステップ 7　元の NTP（手順）に戻ります。

DLP-A51 DHCP を使用して ONS 15454 にクラフト接続するための Windows PC の設定

目的	この作業では、Dynamic Host Configuration Protocol（DHCP）を使用して ONS 15454 へクラフト接続するようにコンピュータを設定します。
工具 / 機器	なし
事前準備手順	「NTP-A260 CTC 用コンピュータのセットアップ」（p.3-2）
	「NTP-A169 CTC ネットワーク アクセスの設定」（p.4-10）
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

（注） 最初にノードを起動するときには、この作業を行わないでください。この作業は、ONS 15454 で DHCP フォワーディングがイネーブルになっている場合にだけ使用してください。デフォルトでは、DHCP がディセーブルになっています。イネーブルにする場合は、「NTP-A169 CTC ネットワーク アクセスの設定」（p.4-10）を参照してください。

（注） ONS 15454 からは IP アドレスが提供されません。DHCP フォワーディングをイネーブルにすると、ONS 15454 は DHCP の要求を外部 DHCP サーバに送ります。

ステップ 1　コンピュータにインストールされている OS を確認してください。

a. Windows の［スタート］メニューから、［**設定**］>［**コントロール パネル**］の順に選択します。
b. ［コントロール パネル］ウィンドウ内の［**システム**］アイコンをダブルクリックします。
c. ［システムのプロパティ］ウィンドウの［全般］タブで、Windows の OS が Windows 98、Windows NT 4.0、Windows 2000、または Windows XP のいずれかであることを確認します。

ステップ 2　コンピュータにインストールされている Windows の OS に応じて、次のステップのいずれかを実行してください。

- Windows 98 の場合は、ステップ 3 を実行します。
- Windows NT 4.0 の場合は、ステップ 4 を実行します。
- Windows 2000 の場合は、ステップ 5 を実行します。
- Windows XP の場合は、ステップ 6 を実行します。

ステップ 3　PC に Windows 98 がインストールされている場合は、次のステップを実行して TCP/IP の設定を変更してください。

a. Windows の［スタート］メニューから、［**設定**］>［**コントロール パネル**］の順に選択します。
b. ［コントロール パネル］ダイアログボックス内で［**ネットワーク**］アイコンをクリックします。
c. ［ネットワーク］ダイアログボックスで、使用している NIC 用の **TCP/IP** を選択し、［**プロパティ**］をクリックします。

d. ［TCP/IP のプロパティ］ダイアログボックスで、［**DNS 設定**］タブをクリックし、［**DNS を使わない**］を選択します。

e. ［**WINS 設定**］タブをクリックし、［**WINS の解決をしない**］を選択します。

f. ［**IP アドレス**］タブをクリックします。

g. ［IP アドレス］ウィンドウ内の［**IP アドレスを自動的に取得**］をクリックします。

h. ［**OK**］をクリックします。

i. PC を再起動するよう求めるプロンプトが表示されたら、［**はい**］をクリックします。

ステップ 4　PC に Windows NT 4.0 がインストールされている場合は、次のステップを実行して TCP/IP の設定を変更してください。

a. Windows の［スタート］メニューから、［**設定**］>［**コントロール パネル**］の順に選択します。

b. ［コントロール パネル］ダイアログボックス内で［**ネットワーク**］アイコンをクリックします。

c. ［ネットワーク］ダイアログボックスで、［**プロトコル**］タブをクリックし、［**TCP/IP のプロトコル**］を選択してから［**プロパティ**］をクリックします。

d. ［**IP アドレス**］タブをクリックします。

e. ［IP アドレス］ウィンドウ内の［**DHCP サーバから IP アドレスを取得する**］をクリックします。

f. ［**OK**］をクリックします。

g. ［**適用**］をクリックします。

h. Windows により PC を再起動するよう求めるプロンプトが表示されたら、［**はい**］をクリックします。

ステップ 5　PC に Windows 2000 がインストールされている場合は、次のステップを実行して TCP/IP の設定を変更してください。

a. Windows　の［スタート］メニューから、［**設定**］>［**ネットワークとダイヤルアップ接続**］>［**ローカル エリア接続**］の順に選択します。

b. ［ローカル エリア接続の状態］ダイアログボックス内の［**プロパティ**］をクリックします。

c. ［全般］タブで、［**インターネット プロトコル（TCP/IP）**］を選択し、［**プロパティ**］をクリックします。

d. ［**DHCP サーバから IP アドレスを取得する**］をクリックします。

e. ［**OK**］をクリックします。

f. ［ローカル エリア接続のプロパティ］ダイアログボックス内で［ **OK**］をクリックします。

g. ［ローカル エリア接続の状態］ダイアログボックス内で［**閉じる**］をクリックします。

ステップ 6　PC に Windows XP がインストールされている場合は、次のステップを実行して TCP/IP の設定を変更してください。

a. Windows の［スタート］メニューから、［**コントロール パネル**］>［**ネットワーク接続**］の順に選択します。

（注）　［ネットワーク接続］メニューが有効になっていない場合は、［**クラシック表示に切り替える**］をクリックします。

b. ［ネットワーク接続］ダイアログボックス内の［**ローカル エリア接続**］をクリックします。

c. ［ローカル エリア接続の状態］ダイアログボックス内の［**プロパティ**］をクリックします。

d. ［全般］タブで、［**インターネット プロトコル（TCP/IP）**］を選択し、［**プロパティ**］をクリックします。

e. ［**DHCP サーバから IP アドレスを取得する**］をクリックします。

f. ［**OK**］をクリックします。

g. ［ローカル エリア接続のプロパティ］ダイアログボックス内で［**OK**］をクリックします。

h. ［ローカル エリア接続の状態］ダイアログボックス内で［**閉じる**］をクリックします。

ステップ 7　元の NTP（手順）に戻ります。

DLP-A52 自動ホスト検出を使用して ONS 15454 にクラフト接続するための Windows PC の設定

目的	この作業では、次のような場合に ONS 15454 にローカル クラフト接続するようにコンピュータを設定します。 • ONS 15454 イーサネット ポートまたは バックプレーン ピンに直接接続するか、ハブを介して接続する。 • アクセスするすべてのノードで、ソフトウェア リリース 3.3 以降が実行されている。 • 複数の ONS 15454 に接続し、接続のたびに毎回 IP アドレスを再設定しなくてもよいようにしたい。 • ONS 15454 には備わっていないアプリケーション（ping や tracert［トレース ルート］など）へアクセスする必要がない。
工具 / 機器	なし
事前準備手順	「NTP-A260 CTC 用コンピュータのセットアップ」（p.3-2）
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

ステップ 1　コンピュータにインストールされている OS を確認してください。

a. Windows の［スタート］メニューから、［**設定**］>［**コントロール パネル**］の順に選択します。

（注） Windows XP の場合は、［スタート］メニューから直接［コントロール パネル］を選択できます。クラシック表示になっていることを確認した上で、この手順を実行してください。

b. ［コントロール パネル］ウィンドウ内の［**システム**］アイコンをダブルクリックします。

c. ［システムのプロパティ］ウィンドウの［全般］タブで、Windows の OS が Windows 98、Windows NT 4.0、Windows 2000、または Windows XP のいずれかであることを確認します。

ステップ 2　コンピュータにインストールされている Windows の OS に応じて、次のステップのいずれかを実行してください。

- Windows 98 の場合は、ステップ 3 を実行します。
- Windows NT 4.0 の場合は、ステップ 4 を実行します。
- Windows 2000 の場合は、ステップ 5 を実行します。
- Windows XP の場合は、ステップ 6 を実行します。

ステップ 3　PC に Windows 98 がインストールされている場合は、次のステップを実行して TCP/IP の設定を変更してください。

a. Windows の［スタート］メニューから、［**設定**］>［**コントロール パネル**］の順に選択します。

b. ［コントロール パネル］ダイアログボックス内で［**ネットワーク**］アイコンをクリックします。

c. ［ネットワーク］ダイアログボックスで、使用している NIC 用の **TCP/IP** を選択し、［**プロパティ**］をクリックします。

d. ［TCP/IP のプロパティ］ダイアログボックスで、［**DNS 設定**］タブをクリックし、［**DNS を使わない**］を選択します。

e. ［**WINS 設定**］タブをクリックし、［**WINS の解決をしない**］を選択します。

f. ［**IP アドレス**］タブをクリックします。

g. ［IP アドレス］ウィンドウ内の［**IP アドレスを指定**］をクリックします。

h. ［IP アドレス］フィールドに、ノード IP アドレスとは別の正規の IP アドレスを入力します。

i. ［**サブネット マスク**］フィールドに、ONS 15454 と同じサブネット マスクを入力します。デフォルトは **255.255.255.0**（24 ビット）です。

j. ［**OK**］をクリックします。

k. ［TCP/IP］ダイアログボックス内で［**ゲートウェイ**］タブをクリックします。

l. ［新しいゲートウェイ］フィールドに、ステップ h で指定したアドレスを入力します。［**追加**］をクリックします。

m. その IP アドレスが［インストールされているゲートウェイ］フィールドに表示されていることを確認してから［**OK**］をクリックします。

n. PC を再起動するよう求めるプロンプトが表示されたら、［**はい**］をクリックします。

ステップ 4　PC に Windows NT 4.0 がインストールされている場合は、次のステップを実行して TCP/IP の設定を変更してください。

a. Windows の［スタート］メニューから、［**設定**］>［**コントロール パネル**］の順に選択します。

b. ［コントロール パネル］ダイアログボックス内で［**ネットワーク**］アイコンをクリックします。

c. ［ネットワーク］ダイアログボックスで、［**プロトコル**］タブをクリックし、［**TCP/IP のプロトコル**］を選択してから［**プロパティ**］をクリックします。

d. ［**IP アドレス**］タブをクリックします。

e. ［IP アドレス］ウィンドウ内の［**IP アドレスを指定**］をクリックします。

f. ［IP アドレス］フィールドに、ノード IP アドレスとは別の正規の IP アドレスを入力します。

g. ［**サブネット マスク**］フィールドに、ONS 15454 と同じサブネット マスクを入力します。デフォルトは **255.255.255.0**（24 ビット）です。

h. ［**詳細**］をクリックします。

i. ［ゲートウェイ］で［**追加**］をクリックします。［TCP/IP ゲートウェイ アドレス］ダイアログボックスが表示されます。

j. ステップ f で指定した IP アドレスを［ゲートウェイ アドレス］フィールドに入力します。

k. ［**追加**］をクリックします。

l. ［**OK**］をクリックします。

m. ［**適用**］をクリックします。

n. PC をリブートします。

ステップ 5　PC に Windows 2000 がインストールされている場合は、次のステップを実行して TCP/IP の設定を変更してください。

a. Windows　の［スタート］メニューから、［**設定**］>［**ネットワークとダイヤルアップ接続**］>［**ローカル エリア接続**］の順に選択します。

b. ［ローカル エリア接続の状態］ダイアログボックス内の［**プロパティ**］をクリックします。

c. ［全般］タブで、［**インターネット プロトコル（TCP/IP）**］を選択し、［**プロパティ**］をクリックします。

d. ［**次の IP アドレスを使う**］をクリックします。

e. ［IP アドレス］フィールドに、ノード IP アドレスとは別の正規の IP アドレスを入力します。

f. ［**サブネット マスク**］フィールドに、ONS 15454 と同じサブネット マスクを入力します。デフォルトは **255.255.255.0**（24 ビット）です。

g. ステップ e で指定した IP アドレスを［ゲートウェイ アドレス］フィールドに入力します。

h. ［**OK**］をクリックします。

i. ［ローカル エリア接続のプロパティ］ダイアログボックス内で［**OK**］をクリックします。

j. ［ローカル エリア接続の状態］ダイアログボックス内で［**閉じる**］をクリックします。

ステップ 6　PC に Windows XP がインストールされている場合は、次のステップを実行して TCP/IP の設定を変更してください。

a. Windows の［スタート］メニューから、［**コントロール パネル**］>［**ネットワーク接続**］の順に選択します。

（注）　［ネットワーク接続］メニューが有効になっていない場合は、［**クラシック表示に切り替える**］をクリックします。

b. ［ネットワーク接続］ダイアログボックス内の［**ローカル エリア接続**］アイコンをクリックします。

c. ［ローカル　エリア接続のプロパティ］ダイアログボックスで、［**インターネット　プロトコル（TCP/IP）**］を選択し、［**プロパティ**］をクリックします。

d. ［IP アドレス］フィールドに、ノード IP アドレスとは別の正規の IP アドレスを入力します。

e. ［**サブネット マスク**］フィールドに、ONS 15454 と同じサブネット マスクを入力します。デフォルトは **255.255.255.0**（24 ビット）です。

f. ステップ d で指定した IP アドレスを［ゲートウェイ アドレス］フィールドに入力します。

g. ［**OK**］をクリックします。

h. ［ローカル エリア接続のプロパティ］ダイアログボックス内で［**OK**］をクリックします。

i. ［ローカル エリア接続の状態］ダイアログボックス内で［**閉じる**］をクリックします。

ステップ 7　元の NTP（手順）に戻ります。

DLP-A53 ONS 15454 にクラフト接続するための Solaris ワークステーションの設定

目的	この作業では、ONS 15454 へクラフト接続するように Solaris ワークステーションを設定します。
工具 / 機器	なし
事前準備手順	「NTP-A260 CTC 用コンピュータのセットアップ」（p.3-2）
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

ステップ 1　root ユーザとしてワークステーションにログインします。

ステップ 2　次のように入力して、インターフェイスがプラミングされていることを確認します。

 # ifconfig *device*

たとえば、次のようになります。

 # ifconfig hme1

インターフェイスがプラミングされている場合は、次のようなメッセージが表示されます。

```
hme1:flags=1000842<BROADCAST,RUNNING,MULTICAST,IPv4>mtu 1500 index 2 inet 0.0.0.0
netmask 0
```

このようなメッセージが表示されたら、ステップ 4 へ進みます。

インターフェイスがプラミングされていない場合は、次のようなメッセージが表示されます。

```
ifconfig: status: SIOCGLIFFLAGS: hme1: no such interface.
```

このようなメッセージが表示されたら、ステップ 3 へ進みます。

ステップ 3　次のように入力して、インターフェイスをプラミングします。

 # ifconfig *device* **plumb**

たとえば、次のようになります。

 # ifconfig hme1 plumb

ステップ 4　次のように入力して、インターフェイス上に IP アドレスを設定します。

 # ifconfig *interface ip-address* **netmask** *netmask* **up**

たとえば、次のように入力します。

 # ifconfig hme0 192.1.0.3 netmask 255.255.255.0 up

（注）　ONS 15454 の IP アドレスと同じ IP アドレスを入力します（ただし、最後のオクテットを除く）。最後のオクテットは必ず 1 または 3 ～ 254 でなければなりません。

ステップ 5　Subnet Mask フィールドに **255.255.255.0** と入力します。Provisioning > Network > General > Gateway Settings タブを順にクリックして Craft Access Only をオンにした場合は、このステップを省略してください。

ステップ 6　接続をテストします。

a. Netscape Navigator を起動します。

b. Web アドレス（URL）のフィールドに ONC 15454 の IP アドレスを入力します。接続が確立されると、Java Console ウィンドウ、CTC キャッシング メッセージ、および Cisco Transport Controller Login ダイアログボックスが表示されます。このあと、「DLP-A60 CTC へのログイン」（p.17-79）のステップ 2 へ進んでログインを実行します。Login ダイアログボックスが表示されない場合は、ステップ c と d を実行してください。

c. プロンプトが表示されたら、次のように入力します。

ping *ONS-15454-IP-address*

たとえば、デフォルト IP アドレスの 192.1.0.2 を使用した ONS 15454 に接続する場合は、次のように入力します。

ping 192.1.0.2

ワークステーションが ONS 15454 に接続されている場合は、次のようなメッセージが表示されます。

```
IP-address is alive
```

（注）　Provisioning > Network > General > Gateway Settings タブを順にクリックして Craft Access Only チェックボックスをオンにした場合は、このステップを省略してください。

d. CTC からの応答がない場合は、［Request timed out］（Windows の場合）メッセージまたは［no answer from *x.x.x.x*］（UNIX の場合）メッセージが表示されます。IP とサブネット マスクに関する情報を確認します。ワークステーションと ONS 15454 との間を接続しているケーブルが確実に取り付けられていることを確認します。次のように入力して、リンクの状態を確認します。

 # ndd -set/dev/*device* **instance 0**

 # ndd -get/dev/*device* **link_status**

たとえば、次のようになります。

 # ndd -set/dev/hme instance 0

 # ndd -get/dev/hme link_status

結果が「1」の場合は、このリンクが稼働しています。結果が「0」の場合は、このリンクがダウンしています。

（注）　ndd については、マニュアル ページを確認してください。たとえば、次のように入力します。`# man ndd`.

ステップ 7　元の NTP（手順）に戻ります。

DLP-A54 CTC を使用した CE-100T-8 カードのハードリセット

目的	この作業では、CE100T-8 イーサネット カードをハードリセットします。
工具 / 機器	なし
事前準備手順	「DLP-A60 CTC へのログイン」（p.17-79）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	スーパーユーザ

注意　CE100T-8 カードをハードリセットすると、トラフィックの中断が発生します。

（注）　ハードリセット オプションがイネーブルになるのは、カードが OOS-MA,MT サービス状態の場合のみです。

ステップ 1　ノード ビューで、**Inventory** タブをクリックします。インベントリ ペインで適切なカードを検索します。

ステップ 2　**Admin State** ドロップダウン メニューをクリックして、**OOS-MT,MA** を選択します。**Apply** をクリックします。

ステップ 3　［Action may be service affecting. Are you sure?］ダイアログボックスで、**Yes** をクリックします。

ステップ 4　カードのサービス状態が［Locked enabled, loopback & maintenance］になります。CTC ではカードの前面プレートがブルーで表示され、SRV LED はオレンジになります。

ステップ 5　カードを右クリックして、ポップアップ メニューを表示します。

ステップ 6　**Hard-reset Card** をクリックします。

ステップ 7　［Are you sure you want to hard-reset this card?］ダイアログボックスで、**Yes** をクリックします。

ステップ 8　元の NTP（手順）に戻ります。

DLP-A56 Internet Explorer によるプロキシ サービスのディセーブル化（Windows）

目的	この作業では、Internet Explorer を実行している PC に対してプロキシ サービスをディセーブルにします。
工具 / 機器	なし
事前準備手順	「NTP-A260 CTC 用コンピュータのセットアップ」（p.3-2）
必須 / 適宜	コンピュータがネットワーク コンピュータのプロキシ サーバに接続されており、かつブラウザが Internet Explorer である場合は必須
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	なし

ステップ 1　Windows の［スタート］メニューから、［**設定**］>［**コントロール パネル**］の順に選択します。

（注）　コンピュータが Windows XP を実行している場合は、［スタート］メニューから直接コントロール パネルを選択できます。クラシック表示になっていることを確認した上で、この手順を実行してください。

ステップ 2　［コントロール パネル］ウィンドウから、［**インターネット オプション**］を選択します。

ステップ 3　［インターネットのプロパティ］ダイアログボックスで、［**接続**］>［**LAN の設定**］の順にクリックします。

ステップ 4　［ローカル エリア ネットワーク（LAN）の設定］ダイアログボックスで、次のいずれかを実行します。

- ［LAN にプロキシ サーバを使用する］をオフにして、このサービスをディセーブルにします。
- ［LAN にプロキシ サーバを使用する］をオンのままにして、［**詳細設定**］をクリックします。［プロキシの設定］ダイアログボックスの［例外］の下に、アクセスする ONS 15454 ノードの IP アドレスを入力します。アドレスの間はセミコロンで区切ります。ホスト番号にアスタリスク（*）を入れると、ネットワーク上のすべての ONS 15454 ノードを含めることができます。［**OK**］をクリックして、開いた状態の各ダイアログボックスを閉じます。

（注）　TCC2P カードが取り付けられた ONS 15454 ノードで、TCC2P のセキュア モード オプションがイネーブルになっている場合は、バックプレーン LAN ポートの IP アドレスを入力します。

ステップ 5　元の NTP（手順）に戻ります。

DLP-A57 Netscape によるプロキシ サービスのディセーブル化（Windows および UNIX）

目的	この作業では、Netscape を実行している PC と UNIX ワークステーションに対してプロキシ サービスをディセーブルにします。コンピュータがネットワーク コンピュータのプロキシ サーバに接続されており、かつブラウザが Netscape である場合は、この作業を実行する必要があります。
工具 / 機器	なし
事前準備手順	「NTP-A260 CTC 用コンピュータのセットアップ」（p.3-2）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	なし

ステップ 1　Netscape を開きます。

ステップ 2　［**編集**］メニューから［**設定**］を選択します。

ステップ 3　［設定］ダイアログボックスのカテゴリの中で、［**詳細**］>［**プロキシ**］の順に選択します。

ステップ 4　［設定］ダイアログボックスの右側の、［プロキシ］の下で、次のいずれかを実行します。

- ［**インターネットに直接接続する**］を選択して、プロキシ サーバをバイパスします。
- ［**手動でプロキシを設定する**］を選択し、プロキシ　サーバに例外を追加してから［**表示**］をクリックします。［手動でプロキシを設定］ダイアログボックスの［例外］の下に、アクセスする ONS 15454 ノードの IP アドレスを入力します。アドレスの間はカンマで区切ります。［**OK**］をクリックして、開いた状態の各ダイアログボックスを閉じます。

（注）　TCC2P カードが取り付けられた ONS 15454 ノードで、TCC2P のセキュア モード オプションがイネーブルになっている場合は、バックプレーン LAN ポートの IP アドレスを入力します。

ステップ 5　元の NTP（手順）に戻ります。

DLP-A60 CTC へのログイン

目的	この作業では、CTC にログインします。
工具 / 機器	なし
事前準備手順	「NTP-A260 CTC 用コンピュータのセットアップ」（p.3-2）
	次の手順のいずれか • 「NTP-A234　ONS　15454　へローカルにクラフト接続するための CTC コンピュータのセットアップ」（p.3-4） • 「NTP-A235 ONS 15454 に社内 LAN で接続するための CTC コンピュータのセットアップ」（p.3-6） • 「NTP-A236 ONS 15454 へのリモート アクセス接続のセットアップ」（p.3-7）
必須 / 適宜	必須
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	検索以上のレベル

（注） CTC のビューとナビゲーションについては、付録 A「CTC の情報とアクセスのためのショートカット」を参照してください。

ステップ 1　ONS 15454 に接続されているコンピュータから Netscape（PC または UNIX の場合）または Internet Explorer（PC の場合のみ）を起動します。

- PC を使用してる場合は、Windows の［スタート］メニューまたはショートカット アイコンから Netscape または Internet Explorer を起動します。
- UNIX を使用している場合は、コマンド ラインに次のように入力して Netscape を起動します。
  - Netscape を使用するための Netscape の色をインストールするには、次のように入力します。

    ```
    # netscape -install
    ```

  - Netscape の色を 32 色に制限して、希望の色が利用できない場合に Netscape に最も近い色を選択させるには、次のように入力します。

    ```
    netscape -ncols 32
    ```

（注） CTC が正常に動作するには、24 色フルカラー パレットが必要です。UNIX 版の Netscape のように色の種類が重要なアプリケーションでは、CTC を使用するには色が足りない可能性があります。-install または -ncols 32 のコマンド ライン オプションにより、Netscape が使用する色の数を制限できます。

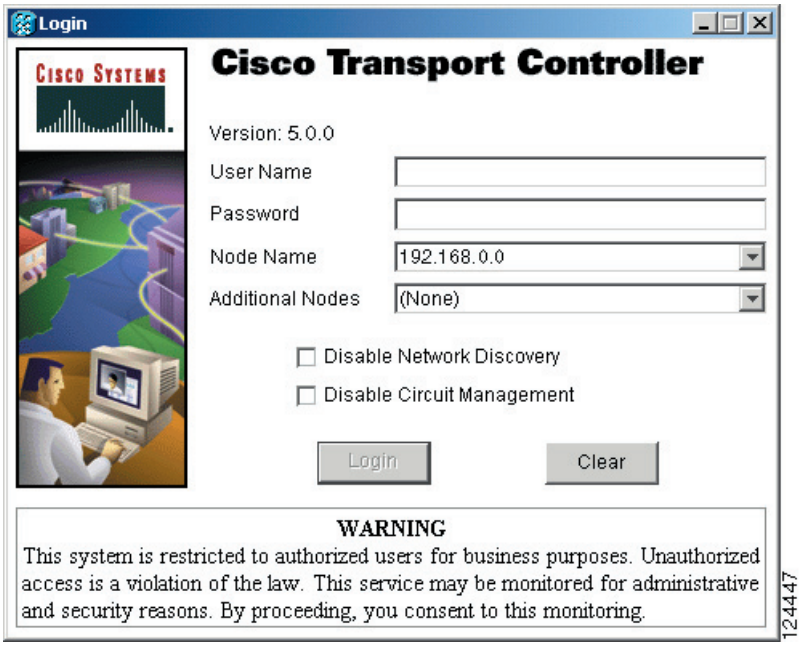
ステップ 2　Netscape または Internet Explorer の Web アドレス（URL）フィールドに、ONS 15454 の IP アドレスを入力します。初期設定の場合、デフォルトの IP アドレスは 192.1.0.2 です。この IP アドレスは LCD に表示されます。CTC を使用すれば LCD の IP アドレスを非表示にできます。詳細については、「DLP-A266 IP 設定の変更」（p.19-64）を参照してください。**Enter** キーを押します。

（注）　ログインしようとしている ONS 15454 ノードの CTC ソフトウェアにリリースの異なるものがある場合は、最新のリリースを実行しているノードにログインしてください。以前のリリースを実行しているノードにログインすると、新しいリリースを実行している各ノードで INCOMPATIBLE-SW アラームが発生し、CTC でそれらのノードを管理できなくなります。ノードのソフトウェア バージョンを確認するには、CTC Help メニューから About CTC を選択します。このようにすれば、ネットワーク ビューに表示されている各ノードで ONS 15454 のソフトウェア バージョンが表示されます。表示されていないノードについては、LCD ディスプレイの表示で調べられます。アラームを解決する方法については、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。

Java Plug-in Security Warning ダイアログボックスが表示されたら、「DLP-A418 公開鍵セキュリティ証明書のインストール」（p.21-6）を実行して、ソフトウェア リリース 4.1 以降で必要となる公開鍵のセキュリティ証明書をインストールしてください。

セキュリティ証明書ダイアログボックスでの操作が終了すると（または証明書がすでにインストールされている場合は）、Java Console ウィンドウに CTC ファイルのダウンロード ステータスが表示されます。Web ブラウザには、使用している Java の環境とシステムの環境に関する情報が表示されます。今回のログインが初めての場合は、コンピュータへ CTC のファイルがダウンロードされているときに CTC のキャッシング メッセージが表示されます。ONS 15454 に初めて接続する場合は、この処理に数分かかることがあります。ダウンロードが終了すると、CTC Login ダイアログボックス（図 17-26）が表示されます。

図 17-26　CTC へのログイン



ステップ 3　Login ダイアログボックスにユーザ名とパスワード（いずれも大文字と小文字を区別する）を入力します。初めて設定する場合は、ユーザ名として **CISCO15** を入力し、パスワードとして **otbu+1** を入力してください。

（注）　すべての ONS 15454 に ユーザ CISCO15 が設定されています。ユーザ CISCO15 にはスーパーユーザの権限があるので、他のユーザを作成できます。ユーザ CISCO15 を削除する場合は、その前に別のスーパーユーザを作成する必要があります。ユーザ CISCO15 には otbu+1 というパスワードが付与されています。ユーザ CISCO15 のパスワードを変更する場合は、ログインしたあとに Provisioning > Security タブを順にクリックしてから、パスワードを変更します。ONS 15454 のユーザを設定してセキュリティを割り当てる場合は、「NTP-A30 ユーザの作成とセキュリティの割り当て」（p.4-6）へ進みます。セキュリティの詳細については、『*Cisco ONS 15454 Reference Manual*』にある「Security」の章を参照してください。

ステップ 4　ONS 15454 にログインするたびに、次のようなログイン オプションを選択できます。

- Node Name — Web ブラウザに入力した IP アドレスとともに、以前に入力した ONS 15454 の IP アドレスがドロップダウン リスト形式で表示されます。リストにあるいずれかの ONS 15454 をログイン用に選択するか、または新しくログインするノードの IP アドレス（またはノード名）を入力できます。
- Additional Nodes — 現在のログイン ノード グループをリストで表示します。ログイン ノード グループの作成方法と新規グループの追加方法については、「DLP-A61 ログイン ノード グループの作成」（p.17-82）を参照してください。
- Disable Network Discovery — このボックスをオンにすると、Node Name フィールドに入力した ONS 15454（および、存在する場合は、ログイン ノード グループ メンバー）だけが表示されます。DCC を介してこのノードにリンクされているノードは検出されないので、CTC のネットワーク ビューに表示されません。このオプションを使用すると、ネットワークに DCC で接続されているノードが多数ある場合の CTC の起動時間を短縮できます。
- Disable Circuit Management — このボックスをオンにすると、既存回線の検出が行われなくなります。このオプションを使用すると、ネットワークに回線が多数存在する場合の CTC の起動時間を短縮して、メモリの消費を削減できます。このオプションによって新規回線の作成と管理が妨害されることはありません。

ステップ 5　**Login** をクリックします。

ログインに成功すると、CTC のウィンドウが表示されます。このウィンドウから、他の CTC ビューに移動して、ONS 15454 のプロビジョニングと管理を行うことができます。初めてシェルフを起動する必要がある場合は、第 4 章「ノードの起動」を参照してください。また、ログインで問題が発生した場合は、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。

ステップ 6　元の NTP（手順）に戻ります。

DLP-A61 ログイン ノード グループの作成

目的	この作業では、ログイン ノード グループを作成して、ログイン ノードに DCC ではなく IP で接続している ONS 15454 を表示します。
工具 / 機器	なし
事前準備手順	「DLP-A60 CTC へのログイン」（p.17-79）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　ノード ビューの Edit メニューから **Preferences** を選択します。

ステップ 2　**Login Node Group** と **Create Group** をクリックします。

ステップ 3　Create Login Group Name ダイアログボックスにグループの名前を入力します。**OK** をクリックします。

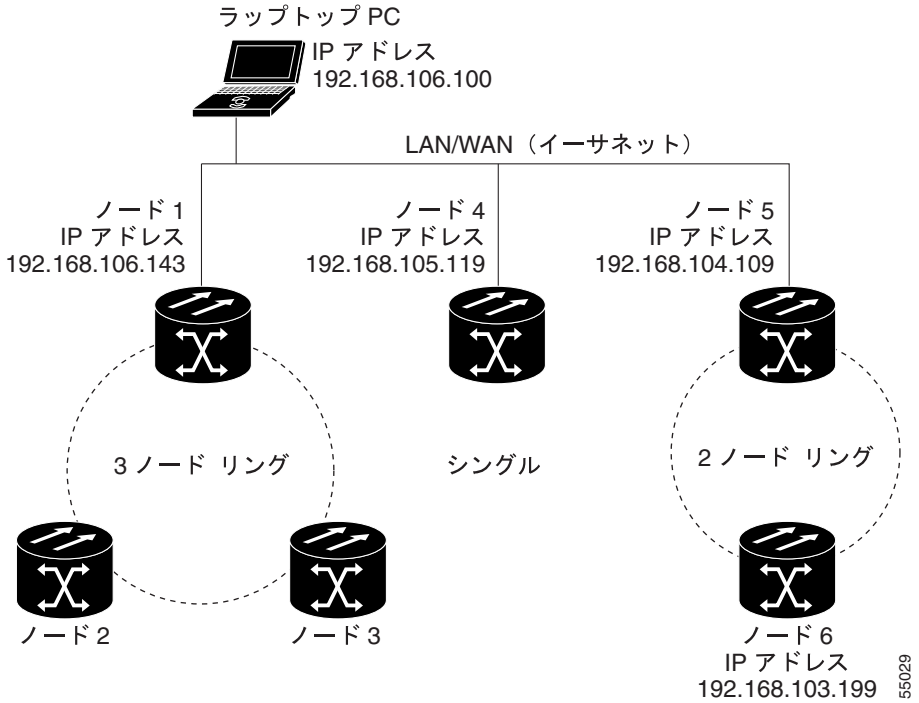
ステップ 4　Members 領域に、このグループに追加するノードの IP アドレス（またはノード名）を入力します。**Add** をクリックします。グループに追加するノードごとに、このステップを繰り返します。

（注）　ログイン ノード グループに追加する ONS 15454 に TCC2P カードが取り付けられていて、TCC2P のセキュア モード オプションがイネーブルになっている場合は、バックプレーン LAN ポートの IP アドレスを入力します。

ステップ 5　**OK** をクリックします。

ONS 15454 へ次回ログインするときに、このログイン ノード グループが Login ダイアログボックスの Additional Nodes リストで利用可能となります。たとえば、図 17-27 では、ノード 1、4、および 5 の IP アドレスを含むログイン ノード グループが作成されます。ログイン時に Additional Nodes リストからこのグループを選択して、Disable Network Discovery を選択しないと、図の中のすべてのノードが表示されます。ログイン グループと Disable Network Discovery を両方とも選択すると、ノード 1、4、および 5 が表示されます。ログイン グループは必要な数だけ作成できます。これらのグループは、CTC のプリファレンス ファイルに保存され、他のユーザに対しては表示されません。

図 17-27　ログイン ノード グループ



ステップ 6　元の NTP（手順）に戻ります。

DLP-A62 現在のセッションまたはログイン グループへのノードの追加

目的	この作業では、現在の CTC セッションまたはログイン ノード グループへノードを追加します。
工具	なし
事前準備手順	「DLP-A60 CTC へのログイン」（p.17-79）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　CTC File メニューから **Add Node** をクリックします。

ステップ 2　Add Node ダイアログボックスにノード名（または IP アドレス）を入力します。

追加する ONS 15454 に TCC2P カードが取り付けられていて、TCC2P のセキュア モード オプションがイネーブルになっている場合は、バックプレーン LAN ポートの IP アドレスを入力します。

ステップ 3　現在のログイン グループにノードを追加する場合は、**Add node to current login group** をオンにします。それ以外の場合は、このチェックボックスをオフのままにします。このチェックボックスは、CTC へのログイン時にログイン グループを選択した場合にだけ、アクティブとなります。

ステップ 4　**OK** をクリックします。

数秒が経過すると、新規ノードがネットワーク ビュー マップに表示されます。

ステップ 5　元の NTP（手順）に戻ります。

DLP-A64 LCD による IP アドレス、デフォルト ルータ、ネットワーク マスクの設定

目的	この作業では、ファントレイ アセンブリの LCD を使って ONS 15454 の IP アドレス、デフォルト ルータ、およびネットワーク マスクを変更します。この作業は、CTC へログインできない場合に使用します。
工具 / 機器	なし
事前準備手順	「DLP-A36 TCC2/TCC2P カードの取り付け」（p.17-51）
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

（注） ノード ビューの Provisioning > Network タブで LCD IP Display が Display Only または Suppress Display に設定されている場合は、この作業を行えません。LCD IP Display フィールドの表示方法と変更方法については、「DLP-A249 IP 設定のプロビジョニング」（p.19-39）を参照してください。

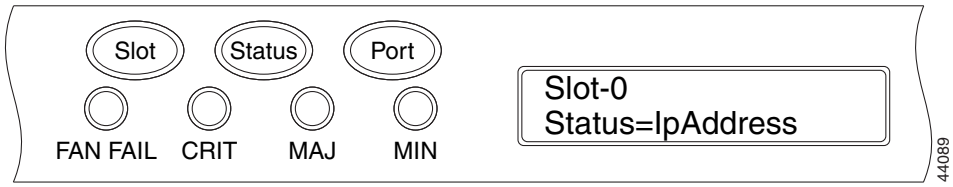
（注） 5 秒間ボタン操作がないと、LCD は通常の表示モードに戻ります。

ステップ 1　ONS 15454 の前面パネルで、LCD に Node の文字が表示されるまで **Slot** ボタンを繰り返し押します。

ステップ 2　次の表示が現れるまで、**Port** ボタンを繰り返し押します。

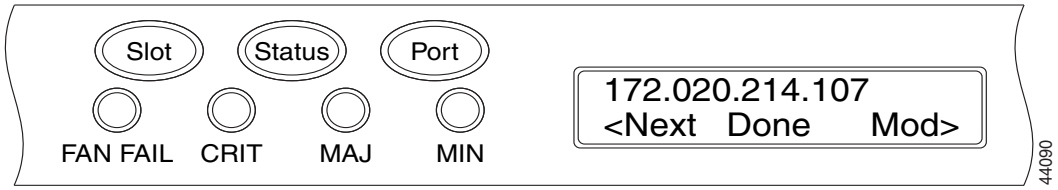
- ノードの IP アドレスを変更する場合は、Status=IpAddress（図 17-28）
- ノードのネットワーク マスクを変更する場合は、Status=Net Mask
- デフォルト ルータの IP アドレスを変更する場合は、Status=Default Rtr

図 17-28　IP アドレス オプションの選択



ステップ 3　**Status** ボタンを押して、ノードの IP アドレス（図 17-29）、ノードのサブネット マスク長、またはデフォルト ルータの IP アドレスを表示します。

図 17-29　IP アドレスの変更



ステップ 4　**Slot** ボタンを押して、変更が必要な IP アドレスまたはサブネット マスクのディジットに移動します。選択したディジットがフラッシュします。

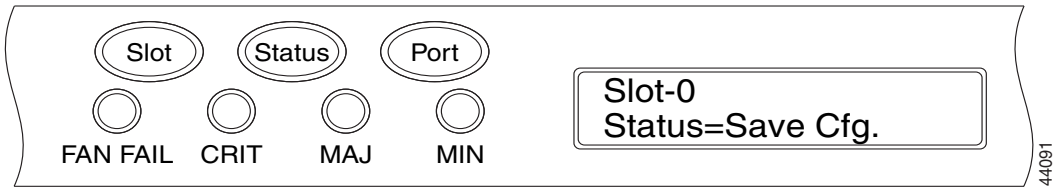
ヒント　Slot、Status、および Port の各ボタンの位置は、LCD のコマンドの位置に対応しています。たとえば、図 17-29 では、Slot ボタンを押して Next コマンドを呼び出し、Port ボタンを押して Done コマンドを呼び出します。

ステップ 5　**Port** ボタンを押して IP アドレスまたはサブネット マスクの該当するディジットへ進みます。

ステップ 6　変更が完了したら、**Status** ボタンを押して Node メニューに戻ります。

ステップ 7　Save Configuration オプションが表示されるまで、**Port** ボタンを繰り返し押します（図 17-30）。

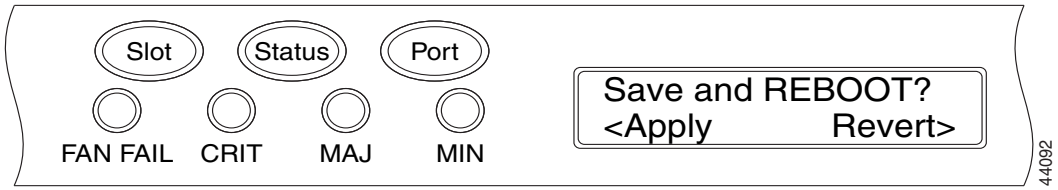
図 17-30　Save Configuration オプションの選択



ステップ 8　**Status** ボタンを押して、Save Configuration オプションを選択します。

［Save and REBOOT］というメッセージが表示されます（図 17-31）。

図 17-31　TCC2/TCC2P の保存とリブート



ステップ 9　**Slot** ボタンを押して新しい IP アドレス設定を適用するか、**Port** を押して設定をキャンセルします。

新しい設定を保存すると、TCC2/TCC2P カードがリブートされます。リブート中に、［Saving Changes - TCC Reset］というメッセージが LCD に表示されます。TCC2/TCC2P のリブートが完了すると、LCD は通常の交互表示に戻ります。

（注）　IP アドレスとデフォルト ルータは、同じサブネット上に設定する必要があります。サブネットが異なる場合は、設定を適用できません。

ステップ 10　元の NTP（手順）に戻ります。

DLP-A65 スタティック ルートの作成

目的	この作業では、別のネットワークにあるコンピュータとの間で CTC 接続を確立するために、スタティック ルートを作成します。
工具 / 機器	なし
事前準備手順	「DLP-A60 CTC へのログイン」（p.17-79）
必須 / 適宜	次のいずれかの条件に該当する場合は必須です。 • あるサブネット内の CTC コンピュータを、ルータを介して別のサブネット内の ONS 15454 に接続されている ONS 15454 と接続する必要がある。また OSPF がディセーブルで、しかも、ENE のゲートウェイ設定がイネーブルになっていない。 • 同じサブネット内の ONS 15454 間で複数の CTC セッションをイネーブルにする必要がある。また、ENE のゲートウェイ設定がイネーブルになっていない。
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　ノード ビューで、**Provisioning** > **Network** タブをクリックします。

ステップ 2　**Static Routing** タブをクリックします。**Create** をクリックします。

ステップ 3　Create Static Route ダイアログボックスで次の情報を入力します。

- Destination — CTC が稼働しているコンピュータの IP アドレスを入力します。アクセス先を 1 つのコンピュータに制限する場合は、完全な IP アドレスとサブネット マスク 255.255.255.255 を入力します。192.168.1.0 サブネット上のすべてのコンピュータへアクセスできるようにするには、192.168.1.0 とサブネット マスク 255.255.255.0 を入力します。宛先として 0.0.0.0 を入力すると、ルータに接続しているすべての CTC コンピュータへアクセスできるようになります。
- Mask — サブネット マスクを入力します。宛先がホスト ルート（つまり、1 つの CTC コンピュータ）の場合は、32 ビットのサブネット マスク（255.255.255.255）を入力します。宛先がサブネットの場合は、255.255.255.0 のようにサブネット マスクを調整します。宛先が 0.0.0.0 の場合は CTC によって自動的にサブネット マスク 0.0.0.0 が入力され、すべての CTC コンピュータへアクセスできるようになります。この値は変更できません。
- Next Hop — CTC コンピュータがノードに直接接続されている場合は、ルータ ポートまたはノードの IP アドレスを入力します。
- Cost — ONS 15454 とコンピュータの間のホップ数を入力します。

ステップ 4　**OK** をクリックします。Static Route ウィンドウにスタティック ルートが表示されることを確認します。

（注）　スタティック ルートを使用したネットワーキングの例は、『*Cisco ONS 15454 Reference Manual*』にある「Management Network Connectivity」の章に記載されています。

ステップ 5　元の NTP（手順）に戻ります。

DLP-A67 ONS 15454 での IIOP リスナー ポートのプロビジョニング

目的	この作業では、ONS 15454 上で Internet Inter-ORB Protocol（IIOP）リスナー ポートを設定し、ファイアウォールの背後にある ONS 15454 ノードにアクセスできるようにします。
工具 / 機器	LAN 管理者またはファイアウォール管理者が指定する IIOP リスナー ポート番号
事前準備手順	「DLP-A60 CTC へのログイン」（p.17-79）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

（注） ポート 1080 の Enable SOCKS Proxy Server チェックボックスがオンになっている場合、CTC ではポート 1080 が使用され、ここで設定した IIOP ポート設定は無視されます。あとで Enable SOCKS Proxy Server チェックボックスをオフにした場合は、ここで設定した IIOP リスナー ポートが使用されます。

ステップ 1　ノード ビューで、**Provisioning** > **Network** > **General** タブをクリックします。

ステップ 2　TCC CORBA (IIOP) Listener Port 領域で、次のリスナー ポート オプションを選択します。

- TCC Fixed（デフォルト）— ONS 15454 が CTC コンピュータと同じファイアウォール側にある場合、またはファイアウォールを使用しない場合（デフォルト）に、このオプションを選択します。このオプションは、ONS 15454 リスナー ポートをポート 57790 に設定します。ポート 57790 が開いている場合は、ファイアウォールを介したアクセスにこのオプションを使用することもできます。
- Standard Constant — ONS 15454 リスナー ポートとしてポート 683（CORBA のデフォルト ポート番号）を使用する場合は、このオプションを選択します。
- Other Constant — ポート 683 を使用しない場合は、ファイアウォール管理者が指定する IIOP ポートを入力します。

ステップ 3　**Apply** をクリックします。

ステップ 4　［Change Network Configuration］というメッセージが表示されたら、**Yes** をクリックします。

両方の ONS 15454 TCC2/TCC2P カードは、一度に 1 つずつリブートします。リブートには約 15 分かかります。

ステップ 5　元の NTP（手順）に戻ります。

DLP-A68 CTC コンピュータにおける IIOP リスナー ポートのプロビジョニング

目的	この作業では、CTC 上で IIOP リスナー ポートの選択を行います。CTC を実行しているコンピュータがファイアウォールの背後にある場合は、この作業を実行する必要があります。
工具 / 機器	LAN 管理者またはファイアウォール管理者が指定する IIOP リスナー ポート番号
事前準備手順	「NTP-A323 カードの取り付けの確認」（p.4-3） 「DLP-A60 CTC へのログイン」（p.17-79）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　Edit メニューから **Preferences** を選択します。

ステップ 2　Preferences ダイアログボックスで **Firewall** タブをクリックします。

ステップ 3　CTC CORBA (IIOP) Listener Port 領域で、リスナー ポート オプションを選択します。

- Variable（デフォルト）— ONS 15454 が CTC コンピュータと同じファイアウォール側にある場合、またはファイアウォールを使用しない場合（デフォルト）に、このオプションを選択します。このオプションは、CTC リスナー ポートをポート 57790 に設定します。ポート 57790 が開いている場合は、ファイアウォールを介したアクセスにこのオプションを使用することもできます。
- Standard Constant — CTC コンピュータのリスナー ポートとしてポート 683（CORBA のデフォルト ポート番号）を使用する場合は、このオプションを選択します。
- Other Constant — ポート 683 を使用しない場合は、管理者が定義した IIOP ポートを入力します。

ステップ 4　**Apply** をクリックします。ポートの変更は次回の CTC ログイン時に適用される旨の警告メッセージが表示されます。

ステップ 5　**OK** をクリックします。

ステップ 6　Preferences ダイアログボックスで **OK** をクリックします。

ステップ 7　IIOP ポートを使用して ONS 15454 にアクセスする場合は、CTC からログアウトしてから、ログインしなおします（ログアウトするには、File メニューから **Exit** を選択します）。

ステップ 8　元の NTP（手順）に戻ります。

DLP-A69 外部タイミングまたはライン タイミングの設定

目的	この作業では、ONS 15454 の SONET タイミング ソース（外部またはライン）を定義します。
工具 / 機器	なし
事前準備手順	「DLP-A60 CTC へのログイン」（p.17-79）
必須 / 適宜	必須
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　ノード ビューで、**Provisioning > Timing** > **General** タブをクリックします。

ステップ 2　General Timing 領域で、次の情報を入力します。

- Timing Mode — ONS 15454 がタイミングをバックプレーン ピンに接続された BITS ソースから得る場合は **External** を選択し、タイミング ノードに光接続された OC-N カードから得る場合は **Line** を選択します。3 番めのオプション Mixed を選択すると、ユーザは外部タイミング基準とライン タイミング基準を設定できます

（注） Mixed タイミングではタイミング ループが発生することがあるので、使用しないことを推奨します。このモードを使用するときは注意してください。

- SSM Message Set — 同期ステータス メッセージング（SSM）メッセージ セットを選択します。すべての ONS 15454 は Generation 2 メッセージ セットを変換できるため、ONS 15454 がほかの ONS 15454 に接続されている場合は、Generation 2 を選択します。Generation 1 を選択するのは、Generation 2 をサポートしない機器に ONS 15454 が接続されている場合に限定してください。SSM メッセージ セットが Generation 1 に設定されているノードが Generation 2 メッセージを受信すると、メッセージは次に使用可能な Generation 1 メッセージにマッピングされます。Transit Node Clock（TNC）および ST3E（Stratum 3E）は、ST3（Stratum 3）クロックになります。
- Quality of RES — タイミング ソースが予約済みの S1 バイトをサポートしている場合は、タイミング品質をここで設定します（ほとんどのタイミング ソースは RES を使用しません）。品質は降順で、範囲として表示されます。たとえば、ST3<RES<ST2 は、タイミング基準が Stratum 3 より大きく、Stratum 2 より小さいことを示します。SONET タイミング レベルの定義など、SSM の詳細については、『*Cisco ONS 15454 Reference Manual*』の「Timing」の章を参照してください。
- Revertive — セカンダリ タイミング基準へ切り替わる要因となった状態が修正されたあとで、ONS 15454 をプライマリ基準ソースに戻す場合は、このチェック ボックスをオンにします。
- Revertive Time — Revertive がオンになっている場合に、プライマリ タイミング ソースに戻るまでに ONS 15454 が待つ時間を選択します。デフォルトは 5 分です。

ステップ 3　Reference List 領域で、次の情報を入力します。

（注） ノードのタイミング基準を最大 3 つまでと、BITS Out 基準を最大 6 つまで定義できます。BITS Out 基準は、バックプレーン上にあるノードの BITS Out ピンに接続可能な機器で使用されるタイミング基準を定義します。機器を BITS Out ピンに接続する場合、外部タイミング基準の近くにある機器はその基準に直接配線できるため、通常、機器をライン モードのノードに接続します。

- NE Reference — 3 つのタイミング基準（Ref 1、Ref 2、Ref 3）を定義できます。その基準で障害が発生しないかぎり、ノードは Reference 1 を使用します。障害が発生した場合は、Reference 2 を使用します。Reference 2 が失敗すると、ノードは、通常内部クロックに設定されている Reference 3 を使用します。内部クロックは、TCC2/TCC2P に提供される Stratum 3 クロックです。表示されるオプションは、Timing Mode の設定により異なります。
- Timing Mode が External に設定されている場合に選択できるオプションは、BITS1、BITS2、および Internal Clock です。
- Timing Mode が Line に設定されている場合に選択できるオプションは、ノードの現用 OC-N カードおよび Internal Clock です。BITS ソース、すなわちノードのトランク（スパン）カードに配線されたノードに直接または間接的に接続されたカードやポートを選択します。Reference 1 は BITS ソースに一番近いトランク カードに設定されています。たとえば、スロット 5 が BITS ソースに配線されたノードに接続されている場合、スロット 5 を Reference 1 として選択します。
- Timing Mode が Mixed に設定されている場合は、BITS カードと OC-N カードの両方を使用できます。これにより、外部 BITS カードと OC-N トランク（スパン）カードを組み合わせたものをタイミング基準として設定できます。
- BITS-1 Out/BITS-2 Out — バックプレーンの BITS Out ピンに接続された機器のタイミング基準を定義します。BITS-1 Out および BITS-2 Out は、BITS-1 および BITS-2 ファシリティがイン サービス状態の場合にイネーブルになります。Timing Mode が External に設定されている場合は、タイミング設定に使用する OC-N カードを選択します。Timing Mode が Line に設定されている場合は、OC-N カードを選択できます。または、NE Reference を選択して、BITS-1 Out または BITS-2 Out（またはその両方）が NE と同じタイミング基準に従うように設定することもできます。

ステップ 4　**BITS Facilities** サブタブをクリックします。

BITS Facilities セクションには、BITS1 タイミング基準と BITS2 タイミング基準のパラメータを設定します。これらの設定は、そのほとんどがタイミング ソースのメーカーによって決まっています。機器のタイミングを BITS Out から取得していれば、その機器の要件を満たすようにタイミング パラメータを設定できます。

ステップ 5　BITS In 領域で、次の情報を入力します。

- Facility Type — （TCC2P カードのみ）BITS クロックでサポートされている BITS 信号タイプを選択します（DS1 または 64Khz+8Khz.）。
- BITS In State — Timing Mode を External または Mixed に設定した場合は、MIC 上の BITS 入力 ピン ペアが外部タイミング ソースに 1 つだけ接続されているか、または両方とも接続されているかによって、BITS-1 または BITS-2（またはその両方）の BITS In State を **IS**（インサービス）に設定します。Timing Mode を Line に設定した場合は、BITS In State を **OOS**（アウト オブ サービス）に設定します。

ステップ 6　BITS In State を OOS に設定した場合は、ステップ 7 に進みます。BITS In State を IS に設定した場合は、次の情報を入力します。

- Coding — BITS 基準で使用される符号化として、Binary 8-Zero Substitution（B8ZS; バイナリ 8 ゼロ置換）または Alternate Mark Inversion（AMI; 交互マーク反転）を選択します。
- Framing — ご使用の BITS 基準で使用されるフレーミングを、Extended Super Frame（ESF; 拡張スーパ フレーム）または Super Frame（SF）（D4）から選択します。
- Sync Messaging — SSM をイネーブルにする場合は、このチェックボックスをオンにします。Framing が Super Frame に設定されている場合は、SSM を使用できません。
- Admin SSM — Sync Messaging チェックボックスがオフになっていれば、ドロップダウン リストから SSM Generation 2 タイプを選択できます。

ステップ 7　BITS Out 領域で、次の情報を入力します。

- Facility Type — BITS Out 信号タイプとして、DS1 または 64 KHz を選択します。

- BITS Out State — 機器がバックプレーンにあるノードの BITS 出力ピンに接続されていて、ノード基準から機器のタイミングを取るようになっている場合は、外部機器に使用されている BITS Out ピンに応じて、BITS-1 と BITS-2 のいずれかまたは両方の BITS Out State を **IS** に設定します。機器が BITS 出力ピンに接続されていない場合は、BITS Out State を **OOS** に設定します。

ステップ 8　BITS Out State を OOS に設定した場合は、ステップ 9 へ進みます。BITS Out State を IS に設定した場合は、次の情報を入力します。

- Coding — BITS 基準で使用される符号化として、B8ZS または AMI を選択します。
- Framing — ご使用の BITS 基準で使用されるフレーミングを、ESF または SF（D4）から選択します。
- AIS Threshold — SSM がディセーブルの場合、または SF が使用されている場合は、ノードが BITS1 Out や BITS2 Out バックプレーン ピンから Alarm Indication Signal（AIS; アラーム表示信号）を送信するときの品質レベルを設定します。BITS 基準の光ソースが このフィールドで定義された SSM 品質レベル以下に低下すると、AIS アラームが発生します。
- LBO — BITS Out ピンに接続された外部デバイスのタイミングを取る場合は、デバイスと ONS 15454 の間の距離を選択します。選択できるオプションは、0 ～ 133 フィート（デフォルト）、124 ～ 266 フィート、267 ～ 399 フィート、400 ～ 533 フィート、および 534 ～ 655 フィートです。Line Build Out（LBO）は BITS ケーブル長に関係します。

ステップ 9　**Apply** をクリックします。

（注）　タイミング関連のアラームについては、『*Cisco ONS 15454 Procedure Guide*』を参照してください。

ステップ 10　元の NTP（手順）に戻ります。

DLP-A70 内部タイミングの設定

目的	この作業では、ONS 15454 の内部タイミング（Stratum 3）を設定します。BITS ソースを使用できない場合のみ、実行してください。
工具 / 機器	なし
事前準備手順	「DLP-A60 CTC へのログイン」（p.17-79）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

注意　内部タイミングは Stratum 3 なので、一時的にしか使用しません。ONS 15454 のタイミングは、すべて Stratum 2 以上のプライマリ基準ソースに合わせる必要があります。

ステップ 1　ノード ビューで、**Provisioning > Timing** > **General** タブをクリックします。

ステップ 2　General Timing 領域で、次の情報を入力します。

- Timing Mode — **External** を選択します。
- SSM Message Set — **Generation 1** に設定します。
- Quality of RES — 内部タイミングには適用されません。
- Revertive — 内部タイミングには適用されません。
- Revertive Time — 内部タイミングには適用されません。

ステップ 3　Reference Lists 領域で、次の情報を入力します。

- NE Reference
  - Ref 1 — **Internal Clock** に設定します。
  - Ref 2 — **Internal Clock** に設定します。
  - Ref 3 — **Internal Clock** に設定します。
- BITS-1 Out/BITS-2 Out — **None** に設定します。

ステップ 4　**Provisioning > Timing** > **BITS Facilities** タブをクリックします。

ステップ 5　BITS Facilities 領域で、BITS In State および BITS Out State を **OOS** に変更します。その他の BITS Facilities 設定は無視してください。内部タイミングには関係しません。

ステップ 6　**Apply** をクリックします。

ステップ 7　元の NTP（手順）に戻ります。

DLP-A71 1:1 保護グループの作成

目的	この作業では、1:1 電気回路カード保護グループを作成します。
工具 / 機器	冗長的な DS-1、DS-3、EC-1、または DS3XM カードをシェルフに取り付けるか、またはこれらのカードのうちの 2 枚に対して ONS 15454 スロットをプロビジョニングする必要があります。
事前準備手順	「DLP-A60 CTC へのログイン」（p.17-79）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　表 4-1（p.4-13）に示す、1:1 保護の要件に応じたカードが取り付けられていることを確認します。

ステップ 2　ノード ビューで、**Provisioning** > **Protection** タブをクリックします。

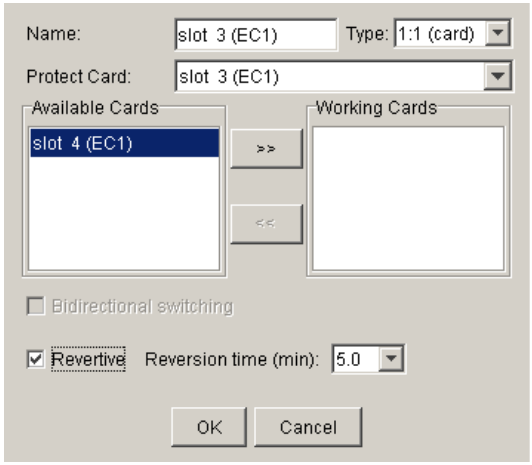
ステップ 3　**Create** をクリックします。

ステップ 4　Create Protection Group ダイアログボックスで次の情報を入力します。

- Name — 保護グループの名前を入力します。保護グループ名には、32 文字までの英数字（a ～ z、A ～ Z、0 ～ 9）を使用します。特殊文字も使用できますが、TL1 と互換性を持たせるために、疑問符（?）、バックスラッシュ（\）、二重引用符（"）は使用しないでください。
- Type — ドロップダウン リストから **1:1** を選択します。
- Protect Card — ドロップダウン リストから保護カードを選択します。ドロップダウン リストには、1:1 保護で使用可能なカードが表示されます。使用可能なカードがないと、リストにカードは表示されません。

保護カードを選択すると、保護に使用できるカードが Available Cards リストに表示されます（図 17-32 を参照）。使用可能なカードがないと、カードは表示されません。その場合は、この作業を行う前に、物理カードを取り付けるか、「DLP-A330 カード スロットの事前プロビジョニング」（p.20-24）を行って ONS 15454 スロットを事前にプロビジョニングする必要があります。

図 17-32　1:1 保護グループの作成



ステップ 5　Available Cards リストから、Protect Card ドロップダウン リストで選択したカードで保護するカードを選択します。上にある矢印ボタンをクリックして、各カードを Working Cards リストに移動します。

ステップ 6　残りのフィールドを次のように設定します。

- Bidirectional switching — 1:1 保護では使用できません。
- Revertive — 障害状態が修正されたあと Reversion Time フィールドに入力された時間でトラフィックを現用カードに復帰させる場合、このボックスをオンにします。
- Reversion time — Revertive をオンにした場合に、ドロップダウン リストから復元時間を選択します。選択できる範囲は 0.5 ～ 12.0 分です。デフォルトは 5.0 分です。これは、切り替えの原因になった状態が解消されたあと、トラフィックが現用カードに復帰するまでに経過する時間です。切り替えの原因になった状態が解消されると、復元タイマーが動き始めます。

ステップ 7　**OK** をクリックし、確認用ダイアログボックスで **Yes** をクリックします。

ステップ 8　元の NTP（手順）に戻ります。

DLP-A72 1:N 保護グループの作成

目的	この作業では、DS-1 または DS-3 の 1:N 保護グループを作成します。
工具 / 機器	スロット 3 または スロット 15 に装着された DS1N-14、DS3N-12、DS3N-12E、DS3/EC1-48、または DS1/E1-56（保護カード）。対応する保護カードのいずれかの側に取り付けられた DS1-14、DS3-12、または DS3-12E（現用カード）。
事前準備手順	「DLP-A60 CTC へのログイン」（p.17-79）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　表 4-1（p.4-13）に示す、1:N の要件に応じたカードが取り付けられていることを確認します。

ステップ 2　**Provisioning** > **Protection** タブをクリックします。

ステップ 3　Protection Groups 領域で、**Create** をクリックします。

ステップ 4　Create Protection Group ダイアログボックスで次の情報を入力します。

- Name — 保護グループの名前を入力します。保護グループ名には、32 文字までの英数字（a ～ z、A ～ Z、0 ～ 9）を使用します。特殊文字も使用できますが、TL1 と互換性を持たせるために、疑問符（?）、バックスラッシュ（\）、二重引用符（"）は使用しないでください。
- Type — ドロップダウン リストから **1:N** を選択します。
- Protect Card — ドロップダウン リストから保護カードを選択します。リストには、スロット 3 またはスロット 15 に装着された DS1N-14、DS3N-12、DS3/EC1-48、DS3N-12E、または DS1/E1-56 カードが表示されます。これらのカードが装着されていない場合は、ドロップダウン リストにカードは表示されません。

保護カードを選択すると、保護に使用できるカードのリストが Available Cards リストに表示されます。使用可能なカードがないと、カードは表示されません。その場合は、この作業を行う前に、物理カードを取り付けるか、「DLP-A330 カード スロットの事前プロビジョニング」（p.20-24）を行って ONS 15454 スロットを事前にプロビジョニングする必要があります。

ステップ 5　Available Cards リストから、Protect Card ドロップダウン リストで選択したカードで保護するカードを選択します。上にある矢印ボタンをクリックして、各カードを Working Cards リストに移動します。

ステップ 6　残りのフィールドを次のように設定します。

- Bidirectional switching — 1:N 保護では使用できません。
- Revertive — 1:N 保護グループの場合は必ずイネーブルになります。
- Reversion time — **Reversion time** をクリックし、ドロップダウン リストから復元時間を選択します。選択できる範囲は 0.5 ～ 12.0 分です。デフォルトは 5.0 分です。これは、切り替えの原因になった状態が解消されたあと、トラフィックが現用カードに復帰するまでに経過する時間です。切り替えの原因になった状態が解消されると、復元タイマーが動き始めます。

ステップ 7　**OK** をクリックし、確認用ダイアログボックスで **Yes** をクリックします。

ステップ 8　元の NTP（手順）に戻ります。

DLP-A73 1+1 保護グループの作成

目的	この作業では、任意の OC-N カードまたはポート（OC-3、OC3-8、OC-12、OC12-4、OC-48、OC-48 AS、OC-192、MRC-12、OC192SR1/STM64IO Short Reach、および OC192/STM64 Any Reach カード）の 1+1 保護グループを作成します。
工具 / 機器	取り付け済みの OC-N カードまたは事前にプロビジョニングされたスロット
事前準備手順	「DLP-A60 CTC へのログイン」（p.17-79）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　表 4-1（p.4-13）に示す、1+1 の要件に応じたカードが取り付けられていることを確認します。

ステップ 2　ノード ビューで、**Provisioning** > **Protection** タブをクリックします。

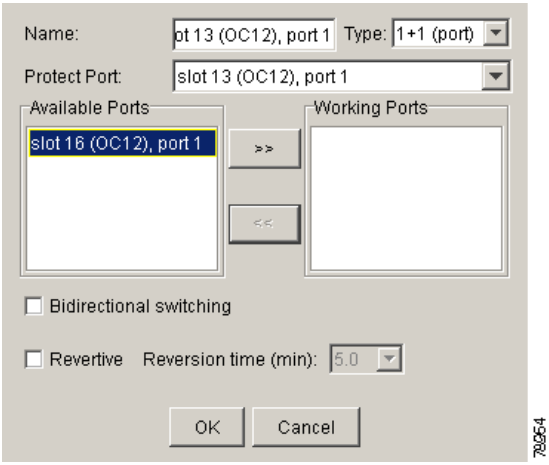
ステップ 3　Protection Groups 領域で、**Create** をクリックします。

ステップ 4　Create Protection Group ダイアログボックスで次の情報を入力します。

- Name — 保護グループの名前を入力します。保護グループ名には、32 文字までの英数字（a ～ z、A ～ Z、0 ～ 9）を使用します。特殊文字も使用できますが、TL1 と互換性を持たせるために、疑問符（?）、バックスラッシュ（\）、二重引用符（"）は使用しないでください。
- Type — ドロップダウン リストから **1+1** を選択します。
- Protect Card — ドロップダウン リストから保護ポートを選択します。ドロップダウン リストには、使用可能な OC-N ポートが表示されます（図 17-33 [p.17-97] を参照）。OC-N カードが取り付けられていないと、ドロップダウン リストにポートは表示されません。

保護ポートを選択すると、保護に使用できるポートのリストが Available Ports リストに表示されます（図 17-33 を参照）。使用可能なカードがないと、ポートは表示されません。その場合は、この作業を行う前に、物理カードを取り付けるか、「DLP-A330 カード スロットの事前プロビジョニング」（p.20-24）を行って ONS 15454 スロットを事前にプロビジョニングする必要があります。

図 17-33　1+1 保護グループの作成



ステップ 5　Available Ports リストから、Protect Port フィールドで選択したポートで保護するポートを選択します。上にある矢印ボタンをクリックして、各ポートを Working Ports リストに移動します。

ステップ 6　残りのフィールドを次のように設定します。

- Bidirectional switching — いずれかの信号に障害が発生した際に Tx と Rx の信号を両方とも保護ポートに切り替える場合は、このボックスをオンにします。障害が発生した信号だけを保護ポートに切り替える場合は、オフにします。
- Revertive — 障害状態が修正されたあと Reversion Time フィールドに入力された時間でトラフィックを現用カードに復帰させる場合、このボックスをオンにします。
- Reversion time — Revertive をオンにした場合に、ドロップダウン リストから復元時間を選択します。選択できる範囲は 0.5 ～ 12.0 分です。デフォルトは 5.0 分です。復元時間は、切り替えの原因になった状態が解消されたあと、トラフィックが現用カードに復帰するまでに経過する時間です。切り替えの原因になった状態が解消されると、復元タイマーが動き始めます。

ステップ 7　**OK** をクリックします。

ステップ 8　元の NTP（手順）に戻ります。

DLP-A74 新規ユーザの作成：単一ノード

目的	この作業では、単一の ONS 15454 ノードに対して新しいユーザを作成します。
工具 / 機器	なし
事前準備手順	「DLP-A60 CTC へのログイン」（p.17-79）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	スーパーユーザ

ステップ 1　ノード ビューで、**Provisioning** > **Security** > **Users** タブをクリックします。

ステップ 2　Users ウィンドウで、**Create** をクリックします。

ステップ 3　Create User ダイアログボックスで次の情報を入力します。

- Name — ユーザ名を入力します。ユーザ名は、6 ～ 20 文字以内の英数字（a ～ z、A ～ Z、0 ～ 9）で指定します。TL1 との互換性を保つには、ユーザ名を 6 ～ 10 文字にする必要があります。
- Password — ユーザ パスワードを入力します。パスワードは、6 ～ 20 文字以内の英数字（a ～ z、A ～ Z、0 ～ 9）および特殊文字（+、#、%）で指定します。少なくとも 2 文字は英字以外の文字、少なくとも 1 文字は特殊文字を使用する必要があります。TL1 との互換性を保つには、パスワードを 6 ～ 10 文字にする必要があります。パスワードには、ユーザ名を含めないでください。
- Confirm Password — 確認のためにパスワードをもう一度入力します。
- Security Level — ユーザのセキュリティ レベルを RETRIEVE、MAINTENANCE、PROVISIONING、SUPERUSER から選択します。各レベルで提供される機能については、『*Cisco ONS 15454 Reference Manual*』の「Security」の章を参照してください。

（注）　各セキュリティ レベルには、それぞれ異なるアイドル時間があります。アイドル時間とは、CTC がアイドル状態になってからパスワードが再入力されるまでの時間です。デフォルトのアイドル時間は、検索ユーザは無制限、メンテナンス ユーザは 60 分、プロビジョニング ユーザは 30 分、スーパーユーザは 15 分です。アイドル時間の変更方法については、「NTP-A205 ユーザの変更とセキュリティの変更」（p.11-10）を参照してください。

ステップ 4　**OK** をクリックします。

ステップ 5　元の NTP（手順）に戻ります。

DLP-A75 新規ユーザの作成：複数ノード

目的	この作業では、複数の ONS 15454 ノードに対して新しいユーザを作成します。
工具 / 機器	なし
事前準備手順	「DLP-A60 CTC へのログイン」（p.17-79）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	スーパーユーザ

（注） ユーザを追加するすべてのノードに、ネットワーク　ビューでアクセスできるようにする必要があります。

ステップ 1　View メニューから **Go to Network View** を選択します。

ステップ 2　**Provisioning** > **Security** > **Users** タブをクリックします。

ステップ 3　Users ウィンドウで、**Create** をクリックします。

ステップ 4　Create User ダイアログボックスで次の情報を入力します。

- Name — ユーザ名を入力します。ユーザ名は、6 ～ 20 文字以内の英数字（a ～ z、A ～ Z、0 ～ 9）で指定します。TL1 との互換性を保つには、ユーザ名を 6 ～ 10 文字にする必要があります。
- Password — ユーザ パスワードを入力します。パスワードは、6 ～ 20 文字以内の英数字（a ～ z、A ～ Z、0 ～ 9）および特殊文字（+、#、%）で指定します。少なくとも 2 文字は英字以外の文字、少なくとも 1 文字は特殊文字を使用する必要があります。TL1 との互換性を保つには、パスワードを 6 ～ 10 文字にする必要があります。パスワードには、ユーザ名を含めないでください。
- Confirm Password — 確認のためにパスワードをもう一度入力します。
- Security Level — ユーザのセキュリティ レベルを RETRIEVE、MAINTENANCE、PROVISIONING、SUPERUSER から選択します。各レベルで提供される機能については、『*Cisco ONS 15454 Reference Manual*』の「Security」の章を参照してください。

（注） 各セキュリティ レベルには、それぞれ異なるアイドル時間があります。アイドル時間とは、CTC がアイドル状態になってからロックアップしてパスワードが再入力されるまでの時間です。デフォルトのアイドル時間は、検索ユーザは無制限、メンテナンス ユーザは 60 分、プロビジョニング ユーザは 30 分、スーパーユーザは 15 分です。アイドル時間の変更方法については、「NTP-A205 ユーザの変更とセキュリティの変更」（p.11-10）を参照してください。

ステップ 5　［Select applicable nodes］で、ユーザを追加しないノードの選択を解除します（デフォルトでは、すべてのネットワーク ノードが選択されます）。

ステップ 6　**OK** をクリックします。

ステップ 7　User Creation Results ダイアログボックスで、ステップ 5 で選択したすべてのノードにユーザが追加されたことを確認します。ユーザが追加されていない場合は、**OK** をクリックしてステップ 2 ～ 6 を繰り返します。すべてのノードにユーザが追加されていたら、**OK** をクリックして次のステップへ進みます。

ステップ 8　元の NTP（手順）に戻ります。

DLP-A83 オーダーワイヤのプロビジョニング

目的	この作業では、AIC-I カードのオーダーワイヤをプロビジョニングします。
工具 / 機器	AIC-I カードがスロット 9 に取り付けられている必要があります。 OC-N カードが取り付けられている必要があります。
事前準備手順	「NTP-A323 カードの取り付けの確認」（p.4-3） 「DLP-A60 CTC へのログイン」（p.17-79）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　ネットワーク ビューで、**Provisioning > Overhead Circuits** タブをクリックします。

ステップ 2　**Create** をクリックします。

ステップ 3　Overhead Circuit Creation ダイアログボックスの Circuit Attributes 領域で次のフィールドを指定します。

- Name — 回線に名前を付けます。名前には、48 文字（スペースを含む）以下の英数字を指定します。
- Circuit Type — 作成するオーダーワイヤ パスに応じて、**Local Orderwire** または **Express Orderwire** を選択します。ONS 15454 ノード間でリジェネレータが使用されていない場合は、ローカル オーダーワイヤ チャネルまたはエクスプレス オーダーワイヤ チャネルを使用します。リジェネレータが存在する場合は、エクスプレス オーダーワイヤ チャネルを使用します。オーダーワイヤ パスごとに 4 つまでの ONS 15454 OC-N ポートをプロビジョニングできます。
- PCM — Pulse Code Modulation（PCM; パルス符号変調）音声符号化およびコンパンディングの標準として、Mu_Law（北米、日本）または A_Law（ヨーロッパ）のいずれかを選択します。プロビジョニングの手順は、どちらの種類のオーダーワイヤでも同じです。

注意　リングにある ONS 15454 ノードのオーダーワイヤをプロビジョニングする場合は、オーダーワイヤ ループ全体をプロビジョニングしないでください。たとえば、4 つのノードがあるリングでは、通常、4 つのノードすべてにプロビジョニングされたイースト ポートとウェスト ポートがありますが、オーダーワイヤ ループを防止するには、1 つのリング ノードを除いたすべてのノードで、2 つのオーダーワイヤ ポート（イーストとウェスト）をプロビジョニングしてください。

ステップ 4　**Next** をクリックします。

ステップ 5　Circuit Source 領域で次の項目を指定します。

- Node — 送信元ノードを選択します。
- Slot — 送信元スロットを選択します。
- Port — 表示された場合は、送信元ポートを選択します。

ステップ 6　**Next** をクリックします。

ステップ 7　Circuit Destination 領域で、次の項目を指定します。

- Node — 宛先ノードを選択します。
- Slot — 宛先スロットを選択します。
- Port — 表示された場合は、宛先ポートを選択します。

ステップ 8　**Finish** をクリックします。

ステップ 9　元の NTP（手順）に戻ります。

DLP-A88 1+1 光保護のテスト

目的	この作業では、1+1 保護グループでトラフィックが正しく切り替えられることを確認します。1+1 保護グループを作成した場合は、この手順を実行する必要があります。
工具 / 機器	受け入れテストの手順で指定したテスト セット
事前準備手順	「DLP-A60 CTC へのログイン」（p.17-79）、トポロジーの受け入れテストで作成したテスト回線
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　View メニューから **Go to Network View** を選択します。

ステップ 2　**Alarms** タブをクリックします。

a. アラーム フィルタの機能がオフであることを確認します。必要に応じて、「DLP-A227 アラーム フィルタリングのディセーブル化」（p.19-24）を参照してください。

b. 説明のつかないアラームがネットワーク上に表示されていないことを確認します。表示されている場合は、作業を進める前に解決してください。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。

ステップ 3　**Conditions** タブをクリックします。説明のつかない状態がネットワーク上に表示されていないことを確認します。表示されている場合は、作業を進める前に解決してください。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。

ステップ 4　ネットワーク マップ上でテスト対象の 1+1 保護グループがあるノードをダブルクリックし、ノード ビューで開きます。

ステップ 5　**Maintenance > Protection** タブをクリックします。

ステップ 6　次のようにして、現用ポートで強制切り替えを開始します。

a. Protection Groups 領域で、1+1 保護グループをクリックします。

b. 現用ポートをクリックします。Switch Commands の隣にある **Force** をクリックします。

c. Confirm Force Operation ダイアログボックスで、**Yes** をクリックします。

d. Selected Group 領域で、次のように表示されることを確認します。

- Protect port: Protect/Active［FORCE_SWITCH_TO_PROTECT］,［PORT STATE］
- Working port: Working/Standby［FORCE_SWITCH_TO_PROTECT］,［PORT STATE］

ステップ 7　ノードに接続されたテスト　セットのトラフィックが動作していることを確認します。ビット　エラーはあってもかまいませんが、トラフィック フローが中断する場合は問題があります。トラフィックの中断が発生する場合は、ステップ 8 を実行して、上位レベルのサポートに連絡します。トラフィックの中断が発生しない場合は、ステップ 8 ～ 12 を実行します。

ステップ 8　現用ポートで切り替えをクリアします。

a. Switch Commands の隣にある **Clear** をクリックします。

b. Confirm Clear Operation ダイアログボックスで、**Yes** をクリックします。

ステップ 9　保護ポートで強制切り替えを開始します。

a. Selected Group 領域で、保護ポートをクリックします。Switch Commands の隣にある **Force** をクリックします。

b. Confirm Force Operation ダイアログボックスで、**Yes** をクリックします。

c. Selected Group 領域で、次のように表示されることを確認します。

- Protect port: Protect/Active［FORCE_SWITCH_TO_WORKING］,［PORT STATE］
- Working port: Working/Standby［FORCE_SWITCH_TO_WORKING］,［PORT STATE］

ステップ 10　ノードに接続されたテスト セットのトラフィックが動作していることを確認します。トラフィックの中断が発生する場合は、ステップ 11 を実行し、上位レベルのサポートに連絡します。トラフィックの中断が発生しない場合は、ステップ 11 および 12 を実行します。

ステップ 11　保護ポートで切り替えをクリアします。

a. Switch Commands の隣にある **Clear** をクリックします。

b. Confirm Clear Operation ダイアログボックスで、**Yes** をクリックします。

c. Selected Group 領域で、次の状態を確認します。

- 保護ポート：Protect/Standby
- 現用ポート：Working/Active

ステップ 12　元の手順（NTP）に戻ります。

DLP-A89 K3 バイトの再マップ

目的	この作業では、K3 バイトをプロビジョニングします。ONS 15454 の BLSR をサードパーティ製機器経由で運用する必要がない場合は、K3 バイトを再マップしないでください。特別なユーザでないかぎり、この作業は不要です。
工具 / 機器	再マップする BLSR スパンに OC48 AS カードが取り付けられている必要があります。
事前準備手順	「DLP-A60 CTC へのログイン」（p.17-79）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

注意　K3 バイトを再マップする場合は、スパンの両端で同じ拡張バイト（Z2、E2、または F1）に再マップします。

ステップ 1　ノード ビューで、サードパーティ製機器に接続する OC48 AS カードをダブルクリックします。

ステップ 2　**Provisioning > Line** タブをクリックします。

ステップ 3　**BLSR Ext Byte** をクリックして、別のバイト（Z2、E2、または F1）を選択します。

ステップ 4　**Apply** をクリックします。

ステップ 5　（4 ファイバ BLSR のみ）保護カードごとにステップ 2 ～ 4 を繰り返します。

ステップ 6　BLSR スパンの他端にあるノードとカードで、この作業を繰り返します。

（注）　ステップ 3 で選択した拡張バイトは、スパンの両端で一致している必要があります。

ステップ 7　元の NTP（手順）に戻ります。

DLP-A91 BLSR 切り替えテスト

目的	この作業では、BLSR で保護切り替えが正しく実行されることを確認します。
工具 / 機器	なし
事前準備手順	「DLP-A60 CTC へのログイン」（p.17-79）
必須 / 適宜	必須
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　View メニューで、**Go to Network View** を選択します。

ステップ 2　**Provisioning > BLSR** タブをクリックします。

ステップ 3　切り替える BLSR の行をクリックし、**Edit** をクリックします。

ステップ 4　ウェスト ポートで強制リング切り替えを開始します。

a. 任意の BLSR ノードのウェスト ポートを右クリックし、**Set West Protection Operation** を選択します。図 19-2（p.19-14）に例を示します（グラフィック アイコンを移動するには、そのアイコンをクリックし、**Ctrl** キーを押しながら新しい場所にドラッグ アンド ドロップします）。

（注）　2 ファイバの BLSR の場合、ノード アイコンの四角形は、BLSR の現用チャネルと保護チャネルを表します。いずれかのチャネルを右クリックします。4 ファイバ BLSR の場合、四角形はポートを表します。現用ポートまたは保護ポートを右クリックします。

b. Set West Protection Operation ダイアログボックスで、ドロップダウン リストから **FORCE RING** を選択します。

c. **OK** をクリックします。

d. 表示される 2 つの Confirm BLSR Operation ダイアログボックスで、**Yes** をクリックします。

ネットワーク ビューの図で、強制リング切り替えを呼び出した BLSR チャネルに F が表示されます。強制リング切り替えが呼び出された BLSR スパン ラインがパープルに変わり、他の BLSR ノード間のスパン ラインはすべてグリーンに変わります。

ステップ 5　次の状態を確認します。

a. **Conditions** タブをクリックします。

b. **Retrieve** をクリックします。

c. ウェスト ポートで強制リング切り替えを呼び出したノードで、次の状態が報告されることを確認します。

- FORCE-REQ-RING — ノードのウェスト側にあるスパンの現用スロットに対して、Force Switch Request On Ring 状態が報告されます。
- RING-SW-EAST — ノードのイースト側にある現用スパンに対して、イースト側で Ring Switch Active 状態が報告されます。

（注）　ウィンドウの右下にある Filter ボタンがオフになっていることを確認します。ノードをキーにして状態をソートする場合は、Node カラムをクリックします。

d. 切り替えを実行したノードのウェスト ラインに接続されたノードで、次の状態が報告されることを確認します。

- FE-FRCDWKSWPR-RING　—　ノードのイースト側にある現用スパンに対して、Far-End Working Facility Forced to Switch to Protection 状態が報告されます。
- RING-SW-WEST　—　ノードのウェスト側にある現用スパンに対して、ウェスト側で Ring Switch Active 状態が報告されます。

ステップ 6　（任意）ONS 15454 の BLSR をサード パーティ製機器経由で運用するために K3 バイトを再マップしている場合は、次の状態が報告されていることを確認します。強制リング切り替えを実行したノードのウェスト側に接続されていない他のノードで、FULLPASSTHR-BI 状態が報告されていることを確認します。

ステップ 7　各ノードで BLSR のライン ステータスを確認します。

a. View メニューから、**Go to Node View** を選択します。

b. **Maintenance > BLSR** タブをクリックします。

c. 次の点を確認します。

- 強制リング切り替えを呼び出したノードのライン ステータスが、ウェスト側では Stby/Stby、イースト側では Act/Act と表示されること。
- 強制リング切り替えを呼び出したノードのウェスト　ラインに接続されたノードのライン ステータスが、イースト側では Stby/Stby、ウェスト側では Act/Act と表示されること。
- リング内の残りのノードのライン ステータスが、イースト側とウェスト側の両方で Act/Act と表示されること。

ステップ 8　View メニューから **Go to Network View** を選択します。

ステップ 9　**Alarms** タブをクリックします。

a. アラーム フィルタの機能がオフであることを確認します。必要に応じて、「DLP-A227 アラーム フィルタリングのディセーブル化」（p.19-24）を参照してください。

b. 説明のつかないアラームがネットワーク上に表示されていないことを確認します。表示されている場合は、作業を進める前に解決してください。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。

ステップ 10　強制リング切り替えを呼び出した BLSR ウィンドウを表示します（このウィンドウは、CTC ウィンドウの下に隠れていることがあります）。

ステップ 11　ウェスト ポートで切り替えをクリアします。

a. 強制リング切り替えを実行した BLSR ノードのウェスト ポートを右クリックし、**Set West Protection Operation** を選択します。

b. Set West Protection Operation ダイアログボックスで、ドロップダウン リストから **CLEAR** を選択します。

c. **OK** をクリックします。

d. Confirm BLSR Operation ダイアログボックスで **Yes** をクリックします。

ネットワーク ビューの図では、強制リング切り替えが削除され、切り替えを表す F も表示されなくなっています。BLSR ノード間のスパン ラインはパープルとグリーンで表示されます。スパン ラインの色が変わるまでには、数秒かかることがあります。

ステップ 12 ネットワーク ビューで、**Conditions** タブをクリックします。この手順を実行して表示されたすべての状態がネットワークからクリアされていることを確認します。説明のつかない状態が表示されている場合は、作業を進める前に解決してください。

ステップ 13 各ノードで BLSR のライン ステータスを確認します。

a. View メニューから、**Go to Node View** を選択します。

a. **Maintenance > BLSR** タブをクリックします。

b. リング内にある各ノードのライン ステータスが、イースト側とウェスト側の両方で Act/Stby と表示されることを確認します。

ステップ 14 イースト ポートで強制リング切り替えを開始します。

a. BLSR ノードのイースト ポートを右クリックし、**Set East Protection Operation** を選択します。

b. Set East Protection Operation ダイアログボックスで、ドロップダウン リストから **FORCE RING** を選択します。

c. **OK** をクリックします。

d. 表示される 2 つの Confirm BLSR Operation ダイアログボックスで、**Yes** をクリックします。

ネットワーク ビューの図で、強制リング切り替えを呼び出した現用 BLSR チャネルに F が表示されます。強制リング切り替えが呼び出された BLSR スパン ラインがパープルに変わり、他の BLSR ノード間のスパン ラインはすべてグリーンに変わります。スパン ラインの色が変わるまでには、数秒かかることがあります。

ステップ 15 次の状態を確認します。

a. **Conditions** タブをクリックします。

b. **Retrieve** をクリックします。

c. イースト ポートで切り替えを呼び出したノードで、次の状態が報告されることを確認します。

- FORCE-REQ-RING — ノードのイースト側にあるスパンの現用スロットに対して、Force Switch Request On Ring 状態が報告されます。
- RING-SW-WEST — ノードのイースト側にある現用スパンに対して、ウェスト側で Ring Switch Active 状態が報告されます。

（注） ウィンドウの右下にある Filter ボタンがオフになっていることを確認します。ノードをキーにして状態をソートする場合は、Node カラムをクリックします。

d. 切り替えを実行したノードのイースト ラインに接続されたノードで、次の状態が報告されることを確認します。

- FE-FRCDWKSWPR-RING — ノードのウェスト側にある現用スパンに対して、Far-End Working Facility Forced to Switch to Protection 状態が報告されます。
- RING-SW-EAST — ノードのウェスト側にある現用スパンに対して、イースト側で Ring Switch Active 状態が報告されます。

ステップ 16（任意）K3 バイトを再マップして ONS 15454 の BLSR をサード パーティ製機器経由で運用している場合は、強制リング切り替えを実行したノードのウェスト側に接続されていない他のノードで、FULLPASSTHR-BI 状態が報告されていることを確認します。

ステップ 17 各ノードで BLSR のライン ステータスを確認します。

a. View メニューから、**Go to Node View** を選択します。

b. **Maintenance > BLSR** タブをクリックします。

- 次の点を確認します。
- 強制リング切り替えを呼び出したノードのライン ステータスが、イースト側では Stby/Stby、ウェスト側では Act/Act と表示されること。
- 強制リング切り替えを呼び出したノードのイースト　ラインに接続されたノードのライン ステータスが、ウェスト側では Stby/Stby、イースト側では Act/Act と表示されること。
- リング内の残りのノードのライン ステータスが､イースト側とウェスト側の両方で Act/Act と表示されること。

ステップ 18 View メニューから **Go to Network View** を選択します。

ステップ 19 **Alarms** タブをクリックします。

a. アラーム フィルタの機能がオフであることを確認します。必要に応じて、「DLP-A227 アラーム フィルタリングのディセーブル化」（p.19-24）を参照してください。

b. 説明のつかないアラームがネットワーク上に表示されていないことを確認します。表示されている場合は、作業を進める前に解決してください。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。

ステップ 20 強制リング切り替えを呼び出した BLSR ウィンドウを表示します（このウィンドウは、CTC ウィンドウの下に隠れていることがあります）。

ステップ 21 イースト ポートで切り替えをクリアします。

a. 強制リング切り替えを呼び出した BLSR ノードのイースト ポートを右クリックし、**Set East Protection Operation** を選択します。

b. Set East Protection Operation ダイアログボックスで、ドロップダウン リストから **CLEAR** を選択します。

c. **OK** をクリックします。

d. Confirm BLSR Operation ダイアログボックスで **Yes** をクリックします。

ネットワーク ビューの図では、強制リング切り替えが削除され、切り替えを表す F も表示されなくなっています。BLSR ノード間のスパン ラインはパープルとグリーンで表示されます。スパン ラインの色が変わるまでには、数秒かかることがあります。

ステップ 22 ネットワーク ビューで、**Conditions** タブをクリックします。この手順を実行して表示されたすべての状態がネットワークからクリアされていることを確認します。説明のつかない状態が表示されている場合は、作業を進める前に解決してください。

ステップ 23 各ノードで BLSR のライン ステータスを確認します。

a. View メニューから、**Go to Node View** を選択します。

b. **Maintenance > BLSR** タブをクリックします。

c. リング内にある各ノードのライン ステータスが、イースト側とウェスト側の両方で Act/Stby と表示されることを確認します。

ステップ 24 File メニューから **Close** を選択して、BLSR ウィンドウを閉じます。

ステップ 25 元の NTP（手順）に戻ります。

DLP-A92 4 ファイバ BLSR のスパン負荷テスト

目的	この作業では、4 ファイバ BLSR のスパンに対して負荷テストを実行します。リング試験の状態（K バイトのパススルーなど）が報告され、10 ～ 15 秒以内にクリアされます。
工具 / 機器	なし
事前準備手順	「DLP-A60 CTC へのログイン」（p.17-79）
必須 / 適宜	必須
オンサイト / リモート	オンサイト
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　View メニューから **Go to Network View** を選択します。

ステップ 2　**Provisioning > BLSR** タブをクリックします。

ステップ 3　負荷テストをする BLSR をクリックして、**Edit** をクリックします。

ステップ 4　ウェスト スパンの負荷テストを実行します。

a. 負荷テストを行う 4 ファイバ BLSR ノードのウェスト ポートを右クリックし、**Set West Protection Operation** を選択します（グラフィック アイコンを移動するには、**Ctrl** キーを押しながら、そのアイコンを新しい場所にドラッグ アンド ドロップします）。

（注）　ネットワーク　マップ上の四角形は、ポートを表します。現用ポートを右クリックします。

b. Set West Protection Operation ダイアログボックスで、ドロップダウン リストから **EXERCISE SPAN** を選択します。

c. **OK** をクリックします。Confirm BLSR Operation ダイアログボックスで、**Yes** をクリックします。

ネットワーク ビューの図で、試験を呼び出した BLSR チャネルに E が表示されます。E は、10 ～ 15 秒間表示され、そのあとでクリアされます。

ステップ 5　次の状態を確認します。

a. **Conditions** タブをクリックしてから、**Retrieve** をクリックします。

b. 次の状態を確認します。

- EXERCISING-SPAN — スパンの負荷テストを実行したノードで Exercise Ring Successful 状態が報告されます。
- FE-EX-SPAN — スパンの負荷テストを実行したノードのウェスト側に接続されたノードのイースト スパンに対して Far-End Exercise Span Request 状態が報告されます。
- KB-PASSTHR — 該当する場合に K Byte Pass Though Active 状態が報告されます。

（注）　ウィンドウの右下にある Filter ボタンがオフになっていることを確認します。ノードをキーにして状態をソートする場合は、Node カラムをクリックします。

ステップ 6　**Alarms** タブをクリックします。

a. アラーム フィルタの機能がオフであることを確認します。必要に応じて、「DLP-A227 アラーム フィルタリングのディセーブル化」（p.19-24）を参照してください。

b. 説明のつかないアラームがネットワーク上に表示されていないことを確認します。表示されている場合は、作業を進める前に解決してください。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。

ステップ 7　イースト スパンの負荷テストを実行します。

a. 負荷テストを行う 4 ファイバ BLSR ノードのイースト ポートを右クリックし、**Set East Protection Operation** を選択します

b. Set East Protection Operation ダイアログボックスで、ドロップダウン リストから **EXERCISE SPAN** を選択します。

c. **OK** をクリックします。

d. Confirm BLSR Operation ダイアログボックスで、**Yes** をクリックします。

ネットワーク ビューの図で、試験を呼び出した BLSR チャネルに E が表示されます。E は、10 ～ 15 秒間表示され、そのあとでクリアされます。

ステップ 8　File メニューから、**Close** を選択します。

ステップ 9　次の状態を確認します。

a. **Conditions** タブをクリックしてから、**Retrieve** をクリックします。

b. 次の状態を確認します。

- EXERCISING-SPAN — スパンの負荷テストを実行したノードで Exercise Ring Successful 状態が報告されます。
- FE-EX-SPAN — スパンの負荷テストを実行したノードのウェスト側に接続されたノードのイースト スパンに対して Far-End Exercise Span Request 状態が報告されます。
- KB-PASSTHR — 該当する場合に K Byte Pass Though Active 状態が報告されます。

（注）　ウィンドウの右下にある Filter ボタンがオフになっていることを確認します。ノードをキーにして状態をソートする場合は、Node カラムをクリックします。

ステップ 10　**Alarms** タブをクリックします。

a. アラーム フィルタの機能がオフであることを確認します。必要に応じて、「DLP-A227 アラーム フィルタリングのディセーブル化」（p.19-24）を参照してください。

b. 説明のつかないアラームがネットワーク上に表示されていないことを確認します。表示されている場合は、作業を進める前に解決してください。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。

ステップ 11　File メニューから **Close** を選択して、BLSR ウィンドウを閉じます。

ステップ 12　元の NTP（手順）に戻ります。

DLP-A93 4 ファイバ BLSR のスパン切り替えテスト

目的	この作業では、4 ファイバ BLSR のスパンでトラフィックが現用ファイバから保護ファイバに切り替わることを確認します。
工具 / 機器	なし
事前準備手順	「DLP-A60 CTC へのログイン」（p.17-79）
必須 / 適宜	必須
オンサイト / リモート	オンサイト
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　View メニューから **Go to Network View** を選択します。

ステップ 2　**Provisioning > BLSR** タブをクリックします。

ステップ 3　**Edit** をクリックします。BLSR ウィンドウが開き、BLSR の図が表示されます。

（注）　BLSR の図にノード アイコンが重ねて表示されている場合は、Ctrl キーを押しながら各アイコンを新しい場所にドラッグ アンド ドロップし、BLSR ポートの情報を見やすくできます。

ステップ 4　ウェスト スパンを切り替えます。

a.　テストする 4 ファイバ BLSR ノードのウェスト ポートを右クリックし、**Set West Protection Operation** を選択します。図 19-2（p.19-14）に例を示します。

（注）　ネットワーク マップ上の四角形は、ポートを表します。現用ポートを右クリックします。

b.　Set West Protection Operation ダイアログボックスで、ドロップダウン リストから **FORCE SPAN** を選択します。

c.　**OK** をクリックします。

d.　表示される 2 つの Confirm BLSR Operation ダイアログボックスで、**Yes** をクリックします。

ネットワーク ビューの図で、保護切り替えを呼び出した BLSR チャネルに F が表示されます。強制スパン切り替えが呼び出された BLSR スパン ラインがパープルに変わり、他の BLSR ノード間のスパン ラインはすべてグリーンに変わります。

ステップ 5　次の状態を確認します。

a.　**Conditions** タブをクリックします。

b.　**Retrieve** をクリックします。

c.　強制スパン切り替えを呼び出したノードで SPAN-SW-WEST（Span Switch West）状態が報告され、切り替えを実行したノードのウェスト ラインに接続されたノードで SPAN-SW-EAST（Span Switch East）状態が報告されることを確認します。ウィンドウの右下にある Filter ボタンがオフになっていることを確認します。ノードをキーにして状態をソートする場合は、Node カラムをクリックします。

ステップ 6　**Alarms** タブをクリックします。

a. アラーム フィルタの機能がオフであることを確認します。必要に応じて、「DLP-A227 アラーム フィルタリングのディセーブル化」（p.19-24）を参照してください。

b. 説明のつかないアラームがネットワーク上に表示されていないことを確認します。表示されている場合は、作業を進める前に解決してください。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。

ステップ 7　強制スパン切り替えを呼び出した BLSR ウィンドウを表示します（このウィンドウは、CTC ウィンドウの下に隠れていることがあります）。

ステップ 8　ウェスト切り替えをクリアします。

a. 強制スパン切り替えを呼び出した BLSR ノードのウェスト ポートを右クリックし、**Set West Protection Operation** を選択します。

b. Set West Protection Operation ダイアログボックスで、ドロップダウン リストから **CLEAR** を選択します。

c. **OK** をクリックします。

d. Confirm BLSR Operation ダイアログボックスで **Yes** をクリックします。

ネットワーク ビューの図では、強制スパン切り替えが削除され、F が表示されなくなり、BLSR ノード間のスパン ラインはパープルとグリーンで表示されます。スパン ラインの色が変わるまでには、数秒かかることがあります。

ステップ 9　イースト スパンを切り替えます。

a. BLSR ノードのイースト ポートを右クリックし、**Set East Protection Operation** を選択します。

b. Set East Protection Operation ダイアログボックスで、ドロップダウン リストから **FORCE SPAN** を選択します。

c. **OK** をクリックします。

d. 表示される 2 つの Confirm BLSR Operation ダイアログボックスで、**Yes** をクリックします。

ネットワーク ビューの図で、強制スパン切り替えを呼び出した BLSR チャネルに F が表示されます。強制スパン切り替えが呼び出された BLSR スパン ラインがパープルに変わり、他の BLSR ノード間のスパン ラインはすべてグリーンに変わります。スパン ラインの色が変わるまでには、数秒かかることがあります。

ステップ 10　次の状態を確認します。

a. **Conditions** タブをクリックします。

b. **Retrieve** をクリックします。

c. 強制スパン切り替えを呼び出したノードで SPAN-SW-EAST（Span Switch East）状態が報告され、切り替えを実行したノードのウェスト ラインに接続されたノードで SPAN-SW-WEST（Span Switch West）状態が報告されることを確認します。ウィンドウの右下にある Filter ボタンがオフになっていることを確認します。

ステップ 11　**Alarms** タブをクリックします。

a. アラーム フィルタの機能がオフであることを確認します。必要に応じて、「DLP-A227 アラーム フィルタリングのディセーブル化」（p.19-24）を参照してください。

b. 説明のつかないアラームがネットワーク上に表示されていないことを確認します。表示されている場合は、作業を進める前に解決してください。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。

ステップ 12 強制スパン切り替えを呼び出した BLSR ウィンドウを表示します（このウィンドウは、CTC ウィンドウの下に隠れていることがあります）。

ステップ 13 イースト切り替えをクリアします。

a. 強制スパン切り替えを呼び出した BLSR ノードのイースト ポートを右クリックし、**Set East Protection Operation** を選択します。

b. Set East Protection Operation ダイアログボックスで、ドロップダウン リストから **CLEAR** を選択します。

c. **OK** をクリックします。

d. Confirm BLSR Operation ダイアログボックスで **Yes** をクリックします。

ネットワーク ビューの図では、強制スパン切り替えが削除され、F が表示されなくなり、BLSR ノード間のスパン ラインはパープルとグリーンで表示されます。スパン ラインの色が変わるまでには、数秒かかることがあります。

ステップ 14 File メニューから **Close** を選択して、BLSR ウィンドウを閉じます。

ステップ 15 元の NTP（手順）に戻ります。

DLP-A94 UPSR の保護切り替えテスト

目的	この作業では、UPSR スパンが正しく切り替わることを確認します。
工具 / 機器	なし
事前準備手順	「DLP-A60 CTC へのログイン」（p.17-79）
必須 / 適宜	必須
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

（注） 60 ミリ秒未満の間サービスが中断することがありますが、テスト回線は、切り替えの実行前、実行中、実行後に関係なく同様に機能します。回線が停止した場合は、作業を中断し、次のレベルのサポートに問い合わせます。

ステップ 1　View メニューから **Go to the Network View** を選択します。

ステップ 2　ネットワークのスパンを右クリックして、**Circuits** を選択します。

Circuits on Span ダイアログボックスが開き、UPSR 回線（回線名、場所、スパンでアクティブな回線の色分けなど）が表示されます。

ステップ 3　次のようにして、スパンのすべての回線で強制切り替えを開始します。

a. **Perform UPSR span switching** フィールドをクリックします。
b. ドロップダウン リストから **FORCE SWITCH AWAY** を選択します。
c. **Apply** をクリックします。
d. Confirm UPSR Switch ダイアログボックスで、**Yes** をクリックします。
e. Protection Switch Result ダイアログボックスで **OK** をクリックします。

Circuits on Span ダイアログボックスにあるすべての回線の Switch State 値が FORCE になります。保護されていない回線は、切り替わりません。

ステップ 4　次の手順を実行して、強制切り替えをクリアします。

a. **Perform UPSR span switching** フィールドをクリックします。
b. ドロップダウン リストから **CLEAR** を選択します。
c. **Apply** をクリックします。
d. Confirm UPSR Switch ダイアログボックスで、**Yes** をクリックします。
e. Protection Switch Result ダイアログボックスで **OK** をクリックします。

Circuits on Span ウィンドウで、すべての UPSR 回線の Switch State が CLEAR になります。

ステップ 5　元の NTP（手順）に戻ります。

DLP-A95 DS-1 回線の送信元と宛先のプロビジョニング

目的	この作業では、DS-1 回線の電気回線の送信元と宛先をプロビジョニングします。
工具 / 機器	なし
事前準備手順	「DLP-A60 CTC へのログイン」（p.17-79）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

（注） Circuit Source ダイアログボックスで特定の回線作成手順に従って回線プロパティを選択すると、回線の送信元をプロビジョニングする準備ができます。

ステップ 1　Node ドロップダウン リストから、始点となるノードを選択します。

ステップ 2　Slot ドロップダウン リストから、回線の送信元となる DS1-14、DS1N-14、DS1/E1-56、DS3XM-6、または DS3XM-12 カードが存在するスロットを選択します。

（注） VT 回線の送信元および宛先は、ポートレス集約回線の STS グルーミング エンドポイント上に設定できます。

ステップ 3　カードとして DS3XM-6 または DS3XM-12 を選択した場合は、Port ドロップダウン リストからポートを選択します。

ステップ 4　DS-1 ドロップダウン リストから送信元 DS-1 を選択します。

ステップ 5　セカンダリ送信元を作成する場合は（マルチベンダー UPSR における UPSR ブリッジまたはセレクタ回線の入り口ポイントなど）、**Use Secondary Source** をクリックし、ステップ 1 ～ 4 を繰り返してセカンダリ送信元を定義します。セカンダリ送信元を作成する必要がない場合は、ステップ 6 へ進みます。

ステップ 6　**Next** をクリックします。

ステップ 7　Node ドロップダウン リストから、宛先（終端）ノードを選択します。

ステップ 8　Slot　ドロップダウン　リストから、宛先カードが存在するスロットを選択します。宛先は、通常、DS-1 カードです。OC-N 転送の場合は、OC-N カードを選択して DS-1 を VT1.5 にマップすることもできます。

ステップ 9　ステップ 8 で選択したカードに対応して表示されるドロップダウン リストから、宛先カードに応じて宛先ポート、STS、VT、または DS1 を選択します。有効なオプションのリストは、表 6-2（p.6-4）を参照してください。ほかの回線で使用されているポート、STS、VT、または DS1 は、CTC に表示されません。同じネットワークで作業している 2 人のユーザが、同じポート、STS、VT、ポート、または DS1 を同時に選択した場合は、一方のユーザに［Path in Use］のエラーが表示され、回線を完成させることができません。回線が不完全な方のユーザは、新しい宛先パラメータを選択する必要があります。

ステップ 10 セカンダリ宛先を作成する場合は（マルチベンダー UPSR における UPSR ブリッジまたはセレクタ回線の出口ポイントなど）、**Use Secondary Destination** をクリックし、ステップ 7 ～ 9 を繰り返してセカンダリ宛先を定義します。

ステップ 11 **Next** をクリックします。

ステップ 12 元の NTP（手順）に戻ります。

DLP-A96 DS-1 または DS-3 回線ルートのプロビジョニング

目的	この作業では、手動でルーティングした DS-1 または DS-3 回線の回線ルートをプロビジョニングします。
工具 / 機器	なし
事前準備手順	「DLP-A60 CTC へのログイン」（p.17-79） Circuit Creation ウィザードの Route Review and Edit ページを開く必要があります。
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　Circuit Creation ウィザードの Route Review/Edit 領域で送信元ノードのアイコンがまだ選択されていない場合は、そのアイコンをクリックして選択します。

ステップ 2　最初に、送信元ノードにあるスパンの中から回線を通過させるスパンを選択して、その矢印をクリックします。矢印がホワイトになります。Selected Span 領域の From フィールドと To フィールドに、スパンの情報が表示されます。送信元 STS および VT（DS-1 回線のみ）が表示されます。

ステップ 3　送信元 STS を変更する場合は、Source STS フィールドを変更します。変更しない場合は、ステップ 4 へ進みます。

ステップ 4　DS-1 回線の送信元 VT を変更する場合は、Source VT フィールドを変更します。変更しない場合は、ステップ 5 へ進みます。

（注）　DS-3 回線の VT はグレー（使用不可）です。

ステップ 5　**Add Span** をクリックします。Included Spans リストにスパンが追加され、スパンの矢印がブルーになります。

ステップ 6　Circuit Routing Preferences パネルで Fully Protect Path チェックボックスがオンになっている場合は、次の作業を行います。

- 送信元から宛先までの回線ルートにあるすべての UPSR 部分または保護されていない部分に対しては、2 つのスパンを追加します。
- 始点から終点までのルートにあるすべての BLSR 部分または 1+1 部分に対しては、1 つのスパンを追加します。
- UPSR DRI トポロジーの中でルーティングされる回線については、DRI ノード間のスパンと同様に、現用パスと保護パスをプロビジョニングします。

ステップ 7　中継ノードも含めて回線が送信元から宛先まですべてプロビジョニングされるまで、ステップ 2 ～ 6 を繰り返します。

ステップ 8　元の NTP（手順）に戻ります。

DLP-A97 OC-N 回線の送信元と宛先のプロビジョニング

目的	この作業では、OC-N 回線の送信元と宛先をプロビジョニングします。
工具 / 機器	なし
事前準備手順	「DLP-A60 CTC へのログイン」（p.17-79）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

（注） Circuit Source ダイアログボックスで特定の回線作成手順に従って回線プロパティを選択すると、回線の送信元と宛先をプロビジョニングする準備ができます。

ステップ 1　Node ドロップダウン リストから、回線の始点となるノードを選択します。

ステップ 2　Slot ドロップダウン リストから、回線の始点になる OC-N カードが取り付けられているスロットを選択します。（伝送容量を使い切っているカードは、リストに表示されません）。

ステップ 3　回線の送信元カードに応じて、Port リストと STS リストから送信元ポートまたは STS またはその両方を選択します。Port リストは、カードに複数のポートがある場合にだけ使用できます。STS は、別の回線によってすでに使用されている場合は、表示されません。

（注） 表示される STS は、カード、回線のサイズ、および保護方式によって異なります。たとえば、UPSR の OC-12 カードに STS-3c 回線を作成する場合は、4 つの STS しか使用できません。また、BLSR の OC-12 カードに STS-3c 回線を作成する場合は、BLSR の保護特性のため、2 つの STS しか使用できません。

ステップ 4　セカンダリ送信元を作成する場合は（マルチベンダー UPSR における UPSR ブリッジまたはセレクタ回線の入りロポイントなど）、**Use Secondary Source** をクリックし、ステップ 1 ～ 3 を繰り返してセカンダリ送信元を定義します。

ステップ 5　**Next** をクリックします。

ステップ 6　Node ドロップダウン リストから宛先ノードを選択します。

ステップ 7　Slot ドロップダウン リストから、回線の宛先となる OC-N カード（宛先カード）が存在するスロットを選択します（伝送容量を使い切っているカードは、リストに表示されません）。

ステップ 8　ステップ 2 で選択したカードに合わせて、Port ドロップダウン リストと STS ドロップダウン リストから、宛先ポートまたは STS またはその両方を選択します。Port ドロップダウン リストは、カードに複数のポートがある場合にだけ使用できます。表示される STS は、カード、回線のサイズ、および保護方式によって異なります。

ステップ 9　セカンダリ宛先を作成する場合は（マルチベンダー UPSR における UPSR ブリッジまたはセレクタ回線の入りロポイントなど）、**Use Secondary Destination** をクリックし、ステップ 6 ～ 8 を繰り返してセカンダリ宛先を定義します。

ステップ 10　**Next** をクリックします。

ステップ 11　元の NTP（手順）に戻ります。

DLP-A99 使用可能な VLAN の判別

目的	この作業では、E シリーズ回線の作成に必要な新しい VLAN（仮想 LAN）に対して、ネットワークに十分な伝送容量があることを確認します。この手順は、ポートマップ モードの E シリーズ カードには適用できません。
工具 / 機器	E シリーズ イーサネット カード（E100T-12/E100T-G、E1000-2/E1000-2-G）がイーサネット回線の両端に取り付けられている必要があります。
事前準備手順	「NTP-A127 ネットワークの起動の確認」（p.6-6） 「DLP-A60 CTC へのログイン」（p.17-79）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　CTC のいずれかのビューで、**Circuits** タブをクリックします。

ステップ 2　既存のイーサネット回線をクリックします。

ステップ 3　**Edit** をクリックしてから、**VLANs** タブをクリックします。

Edit Circuit ダイアログボックスに、回線で使用されている VLAN の数と使用可能な VLAN の合計数が表示されます。

ステップ 4　表示された使用可能な VLAN の数が、作成する E シリーズ イーサネット回線の数だけ十分にあるかどうかを判別します。

注意　スパニングツリーがイネーブルになっている複数の E シリーズ イーサネット回線が、同じ E シリーズ イーサネット カードを通過していて、しかも同じ VLAN を使用していると、それらの回線は互いにブロックしあいます。

ステップ 5　元の NTP（手順）に戻ります。