# *COMPAQ SANworks*

## RAID Array 4000/4100対応
## Windows 2000用セキュア パス3.1

インストレーション/リファレンス ガイド

初版（2000年9月）
製品番号 AA-RN2GA-TE/220959-191
コンパックコンピュータ株式会社

# ご注意



ProLiantは、米国Compaq Computer Corporationの登録商標です。COMPAQ、Compaqロゴ、ROMPaq、SmartStartおよびStorageWorksは、米国Compaq Computer Corporationの商標です。SANworksは、米国Compaq Information Technologies Group, L.P.の商標です。

Microsoft、MS-DOS、WindowsおよびWindows NTは、米国Microsoft Corporationの米国およびその他の国における登録商標です。

IntelおよびPentiumは、米国Intel Corporationの登録商標です。CeleronおよびXeonは、米国Intel Corporationの商標です。

本書に掲載されている会社名、製品名は、それぞれ各社の商標または登録商標です。

本書で取り扱っているコンピュータ ソフトウェアは秘密情報であり、その保有、使用、または複製には、Compaq Computer Corporationから使用許諾を得る必要があります。FAR 12.211および12.212に従って、商業用コンピュータ ソフトウェア、コンピュータ ソフトウェア資料、および商業用製品の技術データは、ベンダ標準の商業用ライセンスのもとで米国政府に使用許諾が付与されます。

本書の内容につきましては万全を期しておりますが、本書中の技術的あるいは校正上の誤り、省略に対して、責任を負いかねますのでご了承ください。本書の内容は、将来予告なしに変更されることがあります。

**本書の内容は、そのままの状態で提供されるもので、いかなる保証も含みません。本書の使用の結果生じるあらゆるリスクはお客様負担となります。いかなる場合もコンパックは、直接損害、結果損害、付随的損害、特別損害、懲罰的損害その他いかなる損害（業務上利益の逸失、業務の中断、業務情報の喪失から生じる損害を含むがこれらに限られません）についても何らの責任も負担しません。コンパックが当該損害の発生の可能性について知らされていた場合でも、また、過失を含め、契約上の行為または不法行為のいずれによる損害についても、同様にコンパックは何らの責任も負担しません。**

**コンパック製品に対する限定保証は、当該製品に付属の資料に記載されたものに限られます。本書のいかなる内容も、当該保証を拡張するものではなく、また新たな保証を追加するものではありません。**

本製品は、日本国内で使用するための仕様になっており、日本国外で使用される場合は、仕様の変更を必要とすることがあります。

本書に掲載されている製品情報には、日本国内で販売されていないものも含まれている場合があります。

Compaq SANworks RAID Array 4000/4100対応Windows 2000用
セキュア パス3.1インストレーション/リファレンス ガイド
初版（2000年9月）
製品番号 AA-RN2GA-TE/220959-191

# 目次

## 第3章
### セキュア パスのインストール



## 第4章
### セキュア パスの管理



## 第5章
### セキュア パスの接続問題のトラブルシューティング

## 図



## 表

# このガイドについて

このガイドは、Compaq SANworks Microsoft Windows用セキュア パス3.1のインストールの手順として、また、操作、トラブルシューティングおよび将来のアップグレードの参考資料としてご使用ください。

## 表記上の規則

このガイドでは、以下の表記規則を採用しています。

| | |
|---|---|
| キー | **Enter**や**F10**などのキーの名前は、太字で、先頭の文字だけを大文字で表記します。2つのキーの間の正符号（+）は、それらのキーを同時に押さえなければならないことを示します。 |
| ユーザ入力 | 別の字体の大文字で表記します。 |
| *ファイル名* | イタリック体の小文字で表記します。 |
| *ユーザ入力変数* | イタリック体で表記します。 |
| メニュー オプション、<br>コマンド名、<br>ダイアログ ボックス名 | [ ]で囲んで表記します。 |
| コマンド、<br>ディレクトリ名<br>およびドライブ名 | すべて大文字で表記します。 |
| タイプ | 「タイプしてください」と指示されている場合、キーボードから情報を入力した後に**Enter**キーを押す必要はありません。 |
| 入力 | 「入力してください」と指示されている場合、情報を入力した後に**Enter**キーを押します。 |

## 本文中の記号

以下の記号は、本文中で安全上重要な注意事項を示します。

**警告:** その指示に従わないと、人体への傷害や生命の危険を引き起こす恐れがある警告事項を表します。

**注意:** その指示に従わないと、装置の損傷やデータの消失を引き起こす恐れがある注意事項を表します。

**重要:** 詳しい説明や具体的な手順を示します。

**注:** 解説、補足または役に立つ情報を示します。

## 装置の記号

安全上の注意が必要な装置の各部には、以下の記号が表示されています。

装置の表面または内部部品に触れると感電の危険があることを示します。カバー内には、一般のユーザが修理できる部品は入っていません。

**警告:** 感電を防止するために、このカバーを開けないようにしてください。

これらの記号が貼付されたRJ-45ソケットはネットワーク インタフェース接続用であることを示します。

**警告:** 感電、火災または装置の損傷を防止するために、電話または電気通信用のコネクタをこのソケットに接続しないようにしてください。

装置の表面または内部部品の温度が非常に高くなる可能性があることを示します。この表面に手を触れるとやけどをする場合があります。

**警告:** 表面が熱くなっているため、やけどをしないように、システムの内部部品が十分に冷めてから手を触れてください。

電源やシステムにこれらの記号が付いている場合、装置の電源が複数あることを示します。

**警告:** 感電しないように、電源コードをすべて抜き取ってシステムの電源を完全に切ってください。

## ラックに関する注意

**警告:** けがや装置の損傷を防止するために、次の点に注意してください。

- ラックの水平脚を床まで延ばしてください。
- ラックの全重量が水平脚にかかるようにしてください。
- 1つのラックだけを設置する場合は、ラックに固定脚を取り付けてください。
- 複数のラックを設置する場合は、ラックを連結してください。
- 一度に複数のコンポーネントを引き出すと、ラックが不安定になる場合があります。コンポーネントは一度に1つずつ引き出してください。

## 困ったときは

問題が発生し、このガイドの情報だけでは解決できない場合、次のところから詳細な情報やその他のヘルプ情報を入手できます。

### コンパックのWebサイト

コンパックのWebサイトでは、最新のドライバやフラッシュROMに関する製品情報を提供しています。コンパックのWebサイト（http://www.compaq.co.jp/またはhttp://www.compaq.com/）にアクセスするには、インターネットにログオンする必要があります。

# 第1章

# 動作説明

## 概要

Compaq SANworks RAID Array 4000/4100対応Windows2000用セキュア パス3.1は高可用性ソフトウェア製品で、次のCompaq StorageWorksストレージ システムへの継続的なデータ アクセスを管理および維持します。

- StorageWorksファイバ チャネルRAID Array 4000
- StorageWorksファイバ チャネルRAID Array 4100

このソフトウェアは、シングル ホスト サーバおよびMicrosoft Cluster Service（MSCS）の高可用性環境内でスタンドアロン構成とクラスタ化構成においてWindows 2000 Advanced Serverオペレーティング システムを実行するIntelベースのプラットフォーム上で動作するように構成されたこれらのStorageWorks RAID Arrayとともに使用できます。

セキュア パスは、ディスク ドライブ、RAIDコントローラ、ホスト バス アダプタ（HBA）、およびインターコネクト ハードウェア（ケーブル、ハブ スイッチ、または接続性デバイス）によるストレージ システム内のsingle point of failure（その障害がシステム全体の障害となる機器）を除去します。

セキュア パスは、リダンダント ハードウェアおよび高度なRAIDテクノロジを使用して、自動化されたフェールオーバ機能を提供することにより、フォールト トレランス機能およびストレージ システムの可用性を向上させます。

リダンダントな物理接続は、セキュア パス ハードウェア コンフィギュレーション内の独立した物理「パス」を定義します。各パスは、サーバ上の固有のHBAポートから開始し、ストレージ システム内の固有のRAIDコントローラ ポートで終了します。

## 特長

セキュア パスには以下の特長があります。

- スイッチ付きデュアル コントローラRAIDシステムと、複数のHBAを装備したホスト サーバの、独立したファイバ チャネル アービトレーテッド ループ（FC-AL）パスを介したリダンダント物理接続管理を可能にします。
- 各パスを監視し、HBA、ケーブル、ハブ、スイッチ、またはコントローラに障害が発生した場合は、I/Oを、機能している代替パスに自動的に経路変更します。
- パスの検証の実装により、物理パスの稼動状態を判定します。
- 障害が発生したパスとフェールオーバされたストレージ ユニットを監視して識別します。
- 複数のストレージ システム間でオンライン（静的）負荷均一化を容易にします。
- 自動フェールバック機能が有効にされている場合、フェールオーバされたストレージ ユニットを修復されたパスに自動的に復元します。
- 限界条件または断続的条件により発生するフェールオーバ/フェールバック反復を防ぎます。
- 誤りや不要なフェールオーバを発生させずに、障害を確実に検出します。
- フェールオーバ/フェールバック動作を、アプリケーションに認識されることも、アプリケーションを中断させることもなしに実行します。
- クライアント/サーバ リモート管理機能、および複数のストレージ システムのサポートを提供します。

## セキュア パスのテクノロジ

セキュア パスの機能にとって重要なのは、StorageWorks RA4000/4100コントローラのアクティブ/パッシブ実装での動作機能です。この実装では、1枚のRA4000コントローラがアクティブにI/O処理を行い、代替コントローラはパッシブの状態のままです。

使用できるストレージ ユニットが、アクティブなコントローラに優先付けされます。これは、システムの起動時に、どのコントローラをアクセスに使用するかを決定します。稼動中は、セキュア パス管理ユーティリティを使用して、いつでもストレージ ユニットをコントローラ パス間で移動させることができます。

セキュア パス ソフトウェアは、障害の発生したパス上のI/O動作の障害を検出して、自動的にトラフィックを代替パスに経路変更します。また、コントローラ、スイッチ、ハブ、HBAまたはその他の接続障害を検出し、障害から復旧することができます。パスのフェールオーバは、プロセスを中断したりデータを消失したりすることなくシームレスに完了します。

アダプタまたはケーブルのコンポーネント、障害の発生したコントローラ、ハブ、またはスイッチのウォームスワップを行った後は、セキュア パス管理ユーティリティを使用してストレージ ユニットを元のパスにフェールバックできます。

セキュア パス環境でのドライブ障害に対する保護のために、ストレージ ユニットはRAIDレベル0、0+1、1、4、または5を使用して構成することができます。セキュア パスは、単一ホスト コンフィギュレーションで、FATまたはNTFSファイル システム フォーマットをサポートしています。MSCSコンフィギュレーションでは、NTFSファイル システムが必要です。

## 自動フェールバック

自動フェールバックを有効にすると、セキュア パスは、障害の発生したパスを監視し、パスが復元されると、フェールオーバされたストレージ ユニットを自動的に元のパスに戻します。反復防止フィルタは、限界条件または断続的条件から発生するピンポン効果（繰り返されるフェールオーバ/フェールバック動作）を防ぎます。ユーザは、セキュア パス管理ユーティリティを使用して、自動または手動のフェールバックを選択できます。

## パスの検証

パスの検証は、使用できるストレージ ユニット パスの稼動状態を定期的に判定する診断機能です。パスの検証により、パスのステータスが正確かつ最新であることが保証されます。アクティブで使用可能なパスについてのこのようなバックグラウンド テストにより、問題を検出し、訂正でき、パスの整合性が保証されます。

## 静的負荷均一化

セキュア パスは、マルチパス アクセスの潜在的機能を活用し、オンライン（静的）負荷均一化機能を使用してI/O性能を改善します。この機能によって、セキュア パスを手動で設定して、複数のストレージ システムにI/O動作を分散します。

# ソフトウェア コンポーネント

セキュア パス ソフトウェア キットには、以下のソフトウェア コンポーネントが含まれています。

- **RDFIL.sys**はWindowsフィルタ ドライバで、LUNへの障害のあるパスをハードウェアの削除とオペレーティング システムが解釈するのを防ぎます。すなわち、ハードウェアの欠落を単に認識しないことによってハードウェアの危険な削除を行えないようにします。
- **RaiDisk.sys**はWindowsフィルタ ドライバで、セキュア パス製品の主要なフェールオーバ機能を提供します。RaiDiskは、StorageWorks RAID Array 4000/4100、マルチパス アクセスをサポートし、I/Oの監視とパス障害の検出のためのすべての機能を提供します。
- **セキュア パス マネージャ**はクライアント/サーバ アプリケーションで、マルチパスStorageWorks RAID Array 4000/4100コンフィギュレーションを管理するために使用します。セキュア パス マネージャは、マルチパス環境をグラフィック表示し、すべての構成済みのストレージ ユニットとパスのステータスを示します。セキュア パス マネージャは、管理対象サーバでローカルに、または管理ワークステーションでリモートに、実行することができます。クライアントは、すべてのWindows 2000オペレーティング システムと互換性があります。

  オンライン（静的）負荷均一化を容易にするために、セキュア パス マネージャは、パス間でストレージセットを移動する機能を提供します。セキュア パス マネージャは、どのパスが構成済みの各ストレージ ユニットに現在サービスを提供しているかを示し、すべての使用可能なパスのモードと状態に関する情報を表示します。
- **セキュア パス エージェント**はWindowsサービスで、ホスト サーバ上のRaiDiskフィルタ ドライバおよびクライアント側のセキュア パス マネージャと、TCP/IPプロトコルおよびWinSock APIを使用して通信します。セキュア パス エージェントは、ホスト サーバに、RaiDiskドライバとともにインストールします。
- **セキュア パス セットアップ**は、Windows 2000 Advanced Serverオペレーティング システムでの、ドライバとアプリケーションのインストールおよびアンインストールをサポートします。

セキュア パスの各ソフトウェア コンポーネントは、必要に応じて、Windowsイベント ログを使用して、エラーと通知メッセージを書き込みます。

# 第2章

# 技術説明

## 概要

Compaq SANworks RAID Array 4000/4100対応Windows 2000用セキュア パスは、サーバ ベースのソフトウェア製品で、サーバとストレージ システム間のコンポーネントの接続障害からの自動復旧を提供することによりこれらのStorageWorks RAID Arrayストレージ システムを強化します。セキュア パスは、ホストとストレージ間のマルチI/Oパスをサポートし、全体的なデータ可用性を向上します。ホストとストレージ間のパス上の任意のコンポーネントで障害が発生した場合、セキュア パスは、ペンディングのI/O要求とそれに続くI/O要求を代替パスに転送します。

この章では、セキュア パスに関する次の項目についての技術的な説明をします。

- 管理対象エンティティ プロファイル
- コントローラ所有権の要件
- パス定義の詳細
- フェールオーバ動作およびオプション
- パス管理動作の要約

## 管理対象エンティティ プロファイル

セキュア パス マネージャの1つのインスタンスによって大規模コンフィギュレーションを管理できます。ただし、1つのグラフィカル ウィンドウに表示して管理できるコンフィギュレーション サイズには、実用上の制限があります。セキュア パス マネージャは、「管理対象エンティティ」または「プロファイル」を使用して、この実用上のコンフィギュレーションの制限を表現します。

セキュア パス マネージャのプロファイルの制限では、最大2台のサーバ（ホスト システム）に、マルチパス フェールオーバ モード用に設定された最大9台のストレージ システムを接続し、共有させることができます。ホスト サーバは、スタンドアロン サーバとするか、クラスタにグループ化することができます。プロファイル内にあるすべてのサーバが、そのプロファイルにリストされているすべてのストレージ システムにアクセスできなければなりません。ストレージセットへのアクセスは、単一のスタンドアロン サーバまたは単一の「クラスタ化」ホスト セットに制限する必要があります。

セキュア パス マネージャにより、同じディレクトリに別々のファイルとして保存される複数のプロファイルを生成できます。上記のプロファイル コンフィギュレーション ルールに従う限り、複数のプロファイルに任意のサーバ、クラスタ、またはストレージ システムを組み込むことができます。

## コントローラの所有権

RA4000/4100ストレージ システムには、1対のリダンダント コントローラが含まれ、アクティブ/パッシブ実装または動作モデルがサポートされます。

アクティブ/パッシブ モデルでは、I/O処理用に一方のメンバーのコントローラにすべてのストレージセットが割り当てられ、もう一方のコントローラは非アクティブです。ただし、このコントローラは、元のコントローラに障害が発生した場合の代替コントローラとして使用できます。

**注**: セキュア パスは、データの整合性を保証するため、所有権の移転に伴い誤って停止されたI/O要求を自動的に再試行します。また、所有権の移転が完了するまで新しいI/O要求を待ち行列に入れます。

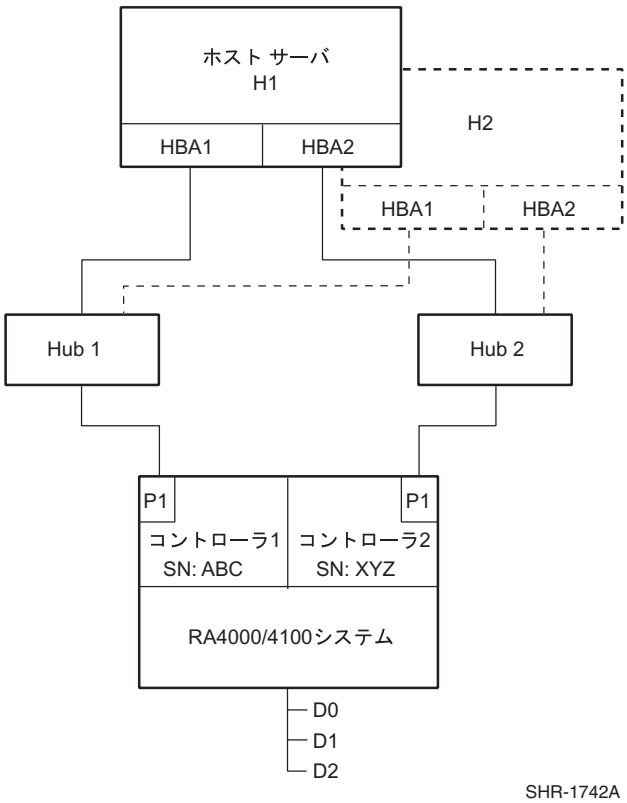
# パスの定義

セキュア パスの中では、パスは、HBA、スイッチまたはハブ、ケーブル、およびRA4000コントローラを含む物理インターコネクト コンポーネントの集合として定義されます。セキュア パスのフィルタドライバ コンポーネントであるRaiDiskは、HBAが生成するSCSI等価アドレスの要素（バス-ターゲット-LUN）によって、物理パスを識別できます。

FC-ALコンフィギュレーションでは、デバイスは、従来のSCSIアドレッシング用語を使用してWindows 2000内でアクセスされます。ファイバ チャネル アダプタはHBAとして表現され、SCSIポートと物理的位置、またはそのどちらかとして名前と番号が設定されます。SCSIアドレスは、RA4000コントローラによりソフト割り当てされたALPA（アービトレーテッド ループ物理アドレス）に基づいています。

LUN番号は、Compaq SmartStart CDに収録されているアレイ コンフィギュレーション ユーティリティ（ACU）を使用してコントローラ内でストレージセットに割り当てられるユニット番号に基づいています。アービトレーテッド ループに接続されている各ノードに、固有のALPAが割り当てられます。

図2-1では、HBA 1、ハブ1、コントローラ1-ポート1が1つのアービトレーテッド ループを構成し、HBA 2、ハブ2、コントローラ2-ポート1がもう1つのアービトレーテッド ループを構成しています。




| | ホスト | コントローラのシリアル番号 | SCSIポート | バス-ターゲット-LUN | HBAスロット |
|---|---|---|---|---|---|
| ドライブD:（D1） | H1 | ABC | 1 | 1 – 1 – 1 | 2 |
| | H1 | XYZ | 2 | 1 – 2 – 1 | 3 |
| | H2 | ABC | 1 | 2 – 1 – 1 | 2 |
| | H2 | XYZ | 2 | 2 – 2 – 1 | 3 |

図2-1. RA4000/4100セキュア パスFC-ALコンフィギュレーションにおけるパスの定義

# パス ステータス

セキュア パスは、パス モード属性とパス状態属性を使用して、パス ステータスを表示します。

## パス モード

パス モードには、優先、代替、優先オフライン、代替オフラインがあります。

- **優先パス モード**は、特定のホストから指定されたストレージセットまでの通信に使用するユーザ指定パスを表します。RaiDiskは、パスを所有権を持つコントローラ上の優先パスと宣言します。ユーザは、セキュア パス マネージャを使用して、デフォルトのドライバ パス設定を変更できます。
- **代替パス モード**は、代替パスを表します。代替パスは、優先パスでの障害に備えて、二重化を提供します。
- **オフライン パス モード**（優先オフラインまたは代替オフライン）は、元のモードと、ユーザがこのパスをI/Oに使用しないように指定したことを表します。パスは、ユーザが介入した場合のみ、オフラインモードになります。

**注**: オフライン モードは、稼動状態のパスには適用できません。

## パスの状態

パスの状態には、稼動、利用可能、障害があり、RaiDiskによって自動的に設定され、パスに発生した障害のためにユーザの予想と異なる可能性がある、現在の実際のパス ステータスを反映します。

- **アクティブ状態**は、関連パスが現在ストレージセットに対してI/Oをサービス中またはサービス可能であることを表します。
- **利用可能状態**は、関連パスがフェールオーバ中に使用できるストレージセットまでのリダンダント パスのセットに属することを表します。
- **障害状態**は、正常動作中またはパスの検証の結果としてパスにエラーが発生したことを表します。

「第4章　セキュア パスの管理」に、パスのモードとパスの状態の詳細な説明と、フェールオーバ、フェールバック、およびユーザ介入の影響の例が示されています。

## フェールオーバ動作

フェールオーバは、特定のエラー状況が検出されると、自動的に実行されます。通常、セキュア パスは、ユーザI/Oがアクティブな場合にのみ、パス フェールオーバを実行します。ただし、セキュア パス マネージャが、障害が発生した共通パスを持つ一部のユニットをフェールオーバ状態と表示し、他のユニットをそのパスを介してアクセス可能なままであると表示する場合があります。

セキュア パスは、フェールオーバの場合に、"優先"パスや"代替"パスのモードを変更しません。このため、ユーザは、修理を行った後で元のパス割り当てを復元できます。セキュア パスは、"優先 - 稼動"パスを故障と記録し、"代替 - 利用可能"パスに切り替えます。

セキュア パスは、もう一方のコントローラ上の"代替 - 利用可能"パスにデバイスを移動しようと試みます。また、その"代替 - 利用可能"パスを"代替 - 稼動"に変更します。

表2-1に、セキュア パスのいくつかのオプション機能によって条件付けられたパス管理動作の要約を示します。

## フェールバック オプション

セキュア パスでは、手動または自動のパス フェールバックが可能です。

手動モードでは、デバイスは、ドラッグ&ドロップ操作（コントローラ フェールバック）またはアクション メニュー項目（他のコントローラへ移動）によって、元のパスに復元されます。この動作は、選択したデバイスに対するシステムI/Oが進行中であるかどうかにかかわらず実行されます。

自動モードに設定すると、セキュア パスは、障害が発生したパスで、影響を受けるデバイスのI/Oが進行中であるかどうかを一定間隔でテストします。パスが正常と見なされる場合、パスの状態が稼動に設定され、I/Oが再びこのパスを介して経路指定されます。

## パスの検証

パスの検証を有効にすると、セキュア パスは、すべてのストレージセットまでのすべてのパスを定期的にテストして、"利用可能"、"障害"、または"稼動"と記録します。ただし、「オフライン」モードにあるパスは、パスの検証の対象外です。

パスの検証は、フェールオーバ機能に影響する前に全体的なパスの二重化に影響する障害を検出する場合に便利です。"優先"パスがパスの検証に合格しない場合、フェールオーバが実行されます。"代替"パスがパスの検証に合格しない場合、その状態が"利用可能"から"障害"に変更されます。

"障害"と記録されているパスがパスの検証に合格すると、パスの状態が"利用可能"に設定されます。自動フェールバックを有効にすると、"優先"パスは"稼動"になります。

## 反復防止フィルタ

セキュア パスは、断続的な障害モードが存在する場合に、デバイスを無限に移動することを防ぐため、反復防止フィルタを実装しています。一定の間隔（現在は1時間）内にデバイスが2回フェールバックされたことをセキュア パスが検出し、元のパスで再びフェールオーバが実行されると、デバイスは、タイマ設定時間の間、フェールオーバされたパスに残ります。タイマ設定時間が経過すると、反復防止フィルタが再初期化され、断続的な障害が継続する場合、フェールオーバ-フェールバック処理が繰り返されます。

反復防止フィルタを使用するには、デフォルトで有効になっているパスの検証を無効にする必要があります。

# パス管理動作の要約

セキュア パスのオプション機能によって条件付けられたパス管理動作の要約については、表2-1を参照してください。

**表2-1**
**パス管理動作の要約**

| | |
|---|---|
| **起動時** | 1） LUNがオンラインになっているコントローラまでのパスが**優先稼動**として選択されます。他のコントローラ上のパスは、**代替利用可能**と記録されます<br>2） オンライン パスが存在しない場合は、使用可能なパスがオンラインにされ、**優先稼動**として使用されます。他のパスは、**代替利用可能**と記録されます |
| **アクティブ パス障害発生時** | 1） パスは**優先（または稼動）障害**と記録され、**代替利用可能**パスにフェールオーバされます。使用される**代替利用可能**パスは、**代替稼動**と記録されます<br>2） 動作は、I/Oまたはバックグラウンド パスの検証と同じです<br>3） LUNが予約されている場合、パスは**障害**と記録されますが、所有権を持たないノード上の他のパスにはフェールオーバされません |
| **使用可能パス障害発生時パスの検証** | 1） 障害が発生したパスは、**障害**と記録されます<br>2） 動作は、バックグラウンド パスの検証の結果です |
| **パス修復後** | 1） パスは、**利用可能**と記録されます<br>2） 自動フェールバックが有効の場合、通常の「自動フェールバック」機能として、**利用可能**パスから**優先**パスにフェールバックされます<br>3） LUNが予約されている場合、パスは**利用可能**と記録されますが、所有権を持たないノードには自動フェールバックされません |

# 第3章

# セキュア パスのインストール

この章では、次のセキュア パス ファイバ チャネル ハードウェアおよびソフトウェアのセットアップ情報を示します。

- 高可用性接続オプションの参照資料
- インストールの前提条件
- セキュア パス ファイバ チャネル スタンドアロン構成とクラスタ構成のインストール手順
  - サーバ ソフトウェアのインストール - RDFILおよびRaiDiskフィルタ ドライバ、Secure Path Agent
  - クライアント ソフトウェアのインストール - セキュア パス マネージャGUI

# RA4000/4100ファイバ チャネル セキュア パスのインストールに必要なコンポーネント

セキュア パス ソフトウェア キットと、インストール用に注文したファイバ チャネル ハードウェアが揃っていることを確認してください。コンポーネントが足りない場合は、サービス エンジニアまでご連絡ください。

表3-1に、セキュア パス動作の基本要件を示します。

**表3-1**
**セキュア パス ファイバ チャネル インストレーションの前提条件**

| ホスト機能 | 要件 |
|---|---|
| プラットフォーム | ProLiantおよびその他のx86 |
| オペレーティング システム | Windows 2000 Advanced Server Edition、Service Pack 1 |
| セキュア パス ソフトウェア キット | SANworks RAID Array 4000/4100対応Windows 2000用セキュア パス3.1 |
| RAIDストレージ システム | StorageWorks RAID Array 4000<br>StorageWorks RAID Array 4100<br>RA4100コントローラ ファームウェア バージョン2.58 |
| ソリューション ソフトウェア キット | Compaq SmartStart and Support Software 4.90<br>Compaq Management Software 4.90 |
| クラスタ キット（オプション） | Compaq ProLiantクラスタHA/F200キット（クラスタ サービス用） |
| ホスト バス アダプタ（およびアダプタ ドライバ） | サポートされているWindows 2000 - IntelおよびRA4000/4100用モデル:<br>StorageWorks 64Bit/66MHzファイバ チャネル アダプタ<br>StorageWorksファイバ チャネル アダプタ/P |
| ファイバ チャネル インターコネクト ハードウェア | 必要に応じて、FC-ALハブ、スイッチ、および接続ハードウェア |
| 作業用具 | 装置の保守に適した工具 |
| 技術資料 | RAIDシステム、HBA、ホスト サーバ、およびWindowsソフトウェアのリファレンス ガイド |

# RA4000/4100セキュア パス コンフィギュレーションのインストール

この項では、ファイバ チャネル ハードウェア インストレーション用に、セキュア パス トポロジをインストールして設定する手順について説明します。

## ハードウェアおよびスタンドアロン ソフトウェアのセットアップ

セキュア パス ファイバ チャネル トポロジをスタンドアロン（非クラスタ化）システム用にインストールして設定するには、以下の手順に従ってください。

1. ハードウェアに付属しているユーザ マニュアルを参照して、すべてのWindowsサーバとすべてのHBAをインストールします。ここでは、ハブまたはスイッチにHBAを接続しないでください。
2. SmartStart 4.90自動インストール ユーティリティを使用して、Windows 2000 Advanced Serverをインストールします。
3. Windowsサーバにセキュア パス ソフトウェアをインストールします。

   セキュア パス ソフトウェアは、セキュア パス セットアップ ウィザードを使用してインストールします。以下に示す「セキュア パス ソフトウェアのインストール」の項を参照して、セキュア パス ソフトウェアのインストレーション セットアップを完了します。
4. サーバをシャットダウンします。
5. ファイバ チャネル装置に付属しているインストレーション マニュアルの手順に従って、新しいRAIDストレージ システム、FC-ALインターコネクト ハードウェア（ハブ/スイッチ）、およびケーブルをすべてインストールします。
6. サーバを再起動します。

   ストレージセットを作成し、SmartStart 4.90に含まれているアレイ コンフィギュレーション ユーティリティ（ACU）を使用して、LUNのユニット属性を指定します。
7. Windows 2000の[ディスクの管理]を起動して、ベーシック ディスク ストレージを構成します。
8. サーバを再起動します。

   システムが再起動したら、Windowsシステム イベント ログで、RaiDiskドライバが正常に起動したことを確認します。

   Windowsアプリケーション イベント ログで、セキュア パス エージェントが正常に起動したことを確認します。

# ハードウェアおよびクラスタ ソフトウェアのセットアップ

ハードウェアおよびクラスタ ソフトウェアのセットアップとコンフィギュレーションについては、Compaq ProLiantクラスタHA/F200キットに付属している『Compaq ProLiantクラスタHA/F200コンフィギュレーション ポスター』を参照してください。

# セキュア パス ソフトウェアのインストール

## サーバ ソフトウェアのインストール

セキュア パス サーバ ソフトウェアは、RAIDストレージ システムが接続されているWindowsホスト システムにインストールしてください。必ず、TCP/IPをホスト システムにインストールしてください。クラスタ コンフィギュレーションでは、セキュア パスをクラスタの各メンバーにインストールしなければなりません。

**重要:** セキュア パスのインストールでは、システム ドライブでTempディレクトリが使用できることが要求されます。たとえば、C:¥Tempが必要です。

以下の手順に従って、セキュア パス サーバ ソフトウェアをインストールしてください。

1. CD-ROMドライブに、Compaq SANworks RAID Array 4000/4100対応Windows 2000用セキュア パス3.1（日本語版）CDを挿入します。
2. サーバで自動実行機能が有効になっている場合、セキュア パス セットアップ プログラムが自動的に起動します。CDの自動実行機能が有効になっていない場合は、[スタート]メニューから[ファイル名を指定して実行]を選択し、次のコマンドを入力します。

   ***drive_letter*:¥spinstall¥setup.exe**

   ここで、*drive_letter*は、CD-ROMドライブに割り当てられるドライブ文字です。
3. セットアップが開始されたら、インストール先パスを選択し、必要なドライバとエージェントをサーバにインストールする[セキュア パス サーバ]オプションを選択します。

ホストを管理できるクライアントを指定するためのプロンプトが表示されます。ローカル ホスト上で実行されるクライアント（セキュア パス マネージャ）からローカル ホストにアクセスするために使用する正しいDNS名のリストが、デフォルトで表示されます。MSCSクラスタ コンフィギュレーションの場合、各クラスタ メンバー用のローカル ホスト名も含まれます。

正しいTCP/IPネットワーク コンフィギュレーションおよびプロトコルについては、システム管理者に確認してください。

4. パスワードを入力します。クラスタ コンフィギュレーションの場合、パスワードが各クラスタ メンバーで同じであることを確認します。

## クライアント ソフトウェアのインストール

セキュア パス クライアント ソフトウェアは、サーバ ソフトウェアと同じWindowsホスト システムにインストールするか、任意のWindows（TCP/IP対応）ワークステーションにインストールできます。

以下の手順に従って、セキュア パス クライアント ソフトウェアをインストールしてください。

1. CD-ROMドライブに、Compaq SANworks RAID Array 4000/4100対応Windows 2000用セキュア パス3.1（日本語版）CDを挿入します。
2. 自動実行機能が有効になっている場合、セキュア パス セットアップ プログラムが自動的に起動します。CDの自動実行機能が有効になっていない場合は、[スタート]メニューから[ファイル名を指定して実行]を選択し、次のコマンドを入力します。

   ***drive_letter*:¥spinstall¥setup.exe**

   ここで、*drive_letter*は、CD-ROMドライブに割り当てられるドライブ文字です。
3. セットアップが開始されたら、インストール先フォルダを選択し、セキュア パス マネージャ ソフトウェアをインストールする[セキュア パス クライアント]オプションを選択します。

これで、新しいセキュア パス環境をサポートするために必要なコンフィギュレーション手順は完了です。セキュア パス マネージャを使用してセキュア パスの動作を監視したり、管理したりするには、「第4章　セキュア パスの管理」を参照してください。

# 第4章

# セキュア パスの管理

この章では、セキュア パス マネージャの次の操作について説明します。

- セキュア パス マネージャの起動
- セキュア パス マネージャへのログオン
- ホスト接続の監視
- ストレージセットおよびパスの管理
- パスとコントローラの障害の検出と識別
- フェールオーバ イベントに対する処置
- MSCSクラスタに関する参照資料

セキュア パス マネージャ（SPM）は、セキュア パス環境の監視および管理に使用できます。SPMは、高可用性ストレージ アクセス用に設定されたRAIDストレージ システムとI/Oパスに関する特定の情報を表示します。SPMを使用すると、管理対象ストレージ プロファイルに関連した各種のプロパティとモードを設定し、フェールバック ポリシーを設定することができます。SPMは、自動的にパス障害を検出して表示します。

# セキュア パス マネージャの起動

SPMを起動するには、以下の手順に従ってください。

1. [スタート]メニューから、[プログラム]、[SecurePath]、[SPM]の順に選択します。
2. セキュア パス マネージャ（SPM）のアプリケーション アイコンをクリックします。

# セキュア パス マネージャへのログオン

SMPへのログオンでは、ログイン ウィンドウからホスト名およびストレージ プロファイルの定義を直接入力します。

## SPMストレージ プロファイルの定義

SPMは、セキュア パスが管理するRAIDストレージ リソースを、ストレージを中心に表示します。特定のホスト（またはホストのセット）に共通する、セキュア パスで保護されたすべてのRA4000/4100ストレージ システムが、SPMディスプレイに表示されます。

SPMのログイン中に、ログイン ウィンドウからストレージ プロファイルを定義する際、これらのRAIDストレージ システムを共有するホスト名を入力します。

- 非クラスタ化ホスト プロファイルを作成するには、まず[ホスト - クラスタ名]フィールドにホスト名を入力します。
- クラスタ化ホスト プロファイルを作成するには、クラスタ化ホスト名のセットを入力します。その際、クラスタ メンバーシップを識別するために、名前の後にハイフンとクラスタ名（たとえば"-clustername"）の定義を付けます。

SPMの1つのインスタンスで、次を管理できます。

- 2つのRA4000/4100ストレージ システムを共有する複数の非クラスタ化ホスト
- 1つのRA4000/4100ストレージ システムを共有するクラスタ化ホストの複数のセット

非クラスタ化ホストとクラスタ化ホストが混在するインストレーションを管理するには、SPMの複数のインスタンスを使用する必要があります。

図4-1に、SPMログイン ディスプレイの例を示します。

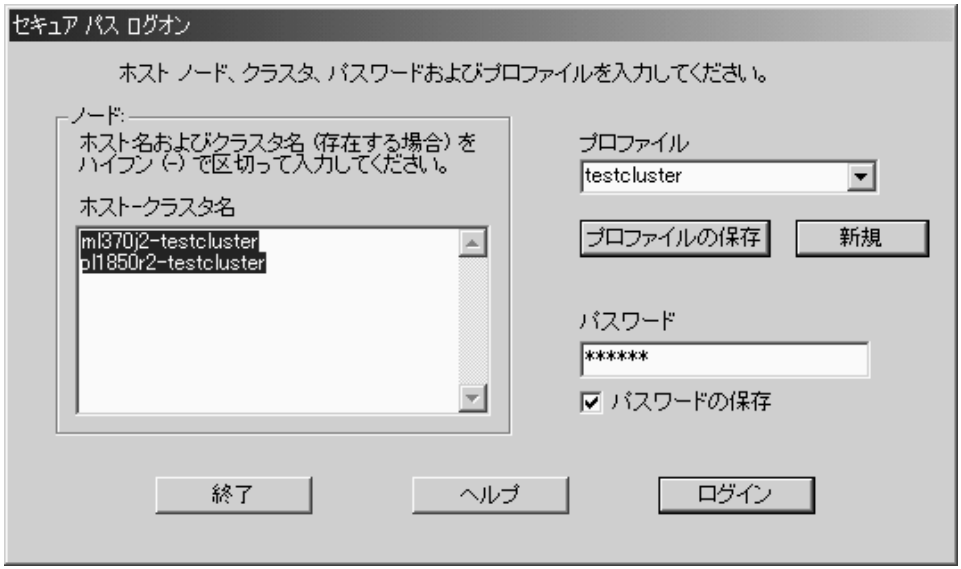



図4-1. クラスタ化ホスト ストレージ プロファイルが表示されている SPMログイン ウィンドウ

ストレージ プロファイルにすべてのホスト名を追加したら、[パスワード]フィールドに接続パスワードを入力します。これは、セットアップ中、またはインストール後にセキュア パス エージェント コンフィギュレーション ユーティリティを実行する際に、セキュア パス エージェント用に定義したパスワードです。

このパスワードは、セキュア パス ホストとのネットワーク接続を確立するために、SPMが使用します。複数のホストを含むストレージ プロファイルの場合、各セキュア パス ホストで接続パスワードが同じでなければなりません。

[パスワードの保存]を選択すると、このストレージ プロファイルでログインするたびに、SPMは保存されたパスワードを自動的に使用します。

## SPMストレージ プロファイルの保存

SPMプロファイルを保存するには、以下の手順に従ってください。

1. ストレージ プロファイルを定義したら、[プロファイル]フィールドに、固有のストレージ プロファイル名を入力します。
2. [プロファイルの保存]をクリックして、プロファイルを保存します。

## 新しいSPMストレージ プロファイルの作成

追加のSPMストレージ プロファイルを作成するには、以下の手順に従ってください。

1. [新規]ボタンをクリックします。
2. [ホスト - クラスタ名]フィールドにホスト名を追加します。
3. [プロファイル]フィールドにプロファイル名を入力します。
4. [プロファイルの保存]ボタンをクリックします。

## 既存のSPMストレージ プロファイルの選択

既存のSPMストレージ プロファイルを選択するには、[プロファイル]ボックスで下向き矢印を使用して目的のプロファイルを表示させ、選択します。

プロファイルを作成したときにパスワードを保存しなかった場合、[パスワード]フィールドにパスワードを入力し、[ログイン]をクリックします。

## 既存のSPMストレージ プロファイルの編集

既存のストレージ プロファイルを編集するには、編集するプロファイルを選択します。プロファイルを修正し、[プロファイルの保存]をクリックします。

## セキュア パス エージェントのパスワードの変更

セキュア パス エージェントのパスワードを変更するには、以下の手順に従ってください。

1. [スタート]メニューから、セキュア パスのプログラム フォルダにあるセキュア パス エージェント コンフィギュレーション ユーティリティを実行する必要があります。
2. コンフィギュレーション ユーティリティを使用してエージェントのクライアント（SPM）アクセス リストやパスワードを変更したら、[コントロール パネル]にある[管理ツール] - [サービス]を使用して、エージェントを終了し、再起動する必要があります。

3. [サービス]リストで[Secure Path Agent]を選択し、[サービスの停止]をクリックします。
4. エージェントが終了したら、もう一度[Secure Path Agent]を選択し、[サービスの開始]をクリックします。

エージェントが再起動し、そのクライアント/パスワード データベースが更新されます。必ず、この手順を、SPMストレージ プロファイル内の各ホストについて行ってください。

## 接続問題のトラブルシューティング

SPMにログオンする際に問題が発生した場合は、詳細について「第8章　セキュア パスの接続問題のトラブルシューティング」を参照してください。

# ホスト接続の監視

SPMは、現在のストレージ プロファイルのメンバーになっている各アクティブ ホストの接続状態を監視します。

**注:** FQDN（完全修飾ドメイン名）を使用したクライアント接続の認証に問題がある場合は、DNS（ドメイン ネーム サービス）による解決の問題の可能性があるため、関連するFQDNとIPアドレスの割り当てを含む*HOSTS*ファイルのエントリによって解決できることがあります。

図4-2に示すように、ツール バーのすぐ下にあるウィンドウ フレームに各ホストのサーバ アイコンが表示されます。ホストがクラスタのメンバーである場合、アイコンの上にホスト名が表示され、アイコンの下にクラスタ名が表示されます。

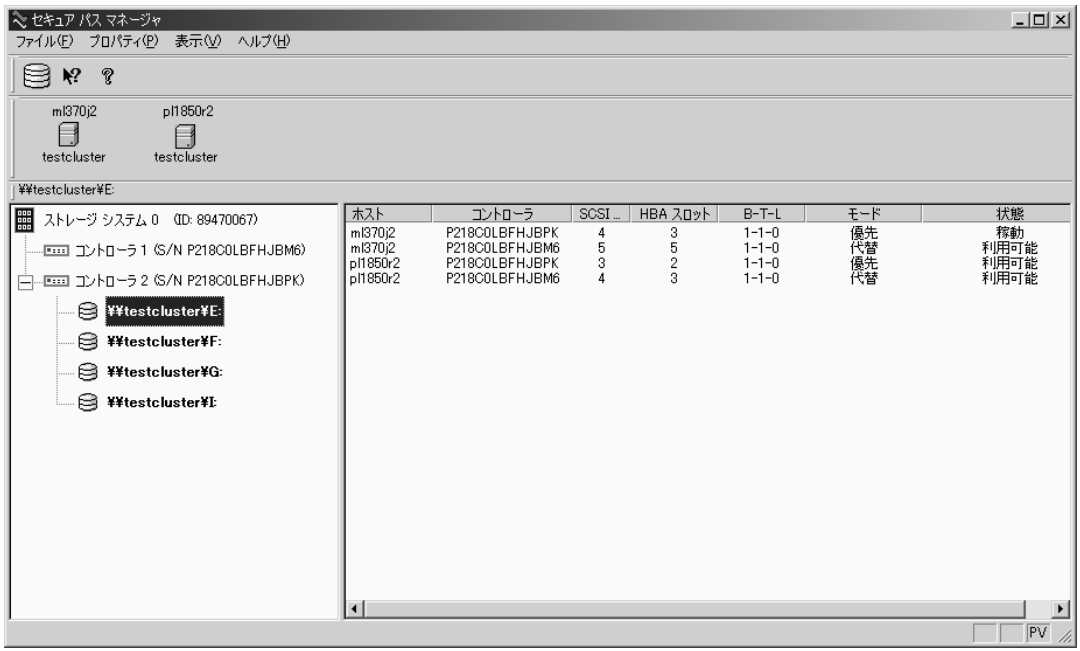



図4-2. ホスト接続の監視

SPMは、ストレージ プロファイルの各メンバーとの接続を監視し、特定のホストとの接続の消失を赤色の"X"で表示します。図4-3に、"testcluster"というクラスタのメンバーの"pl1850r2"との接続が消失した場合の表示を示します。

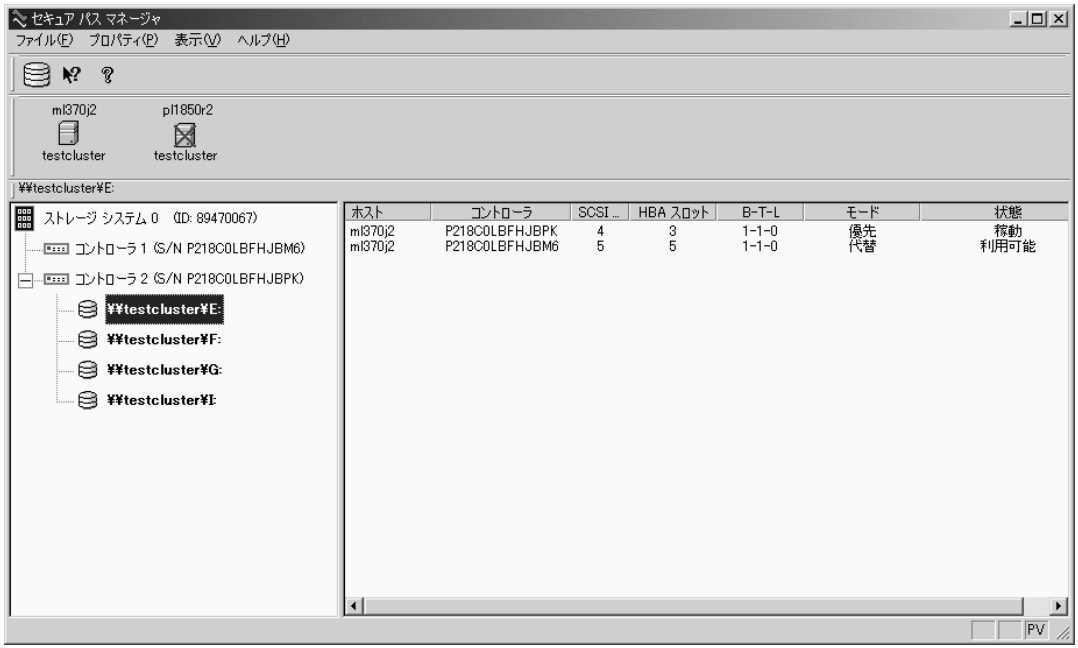



図4-3．ホスト接続消失アイコン

## ホスト接続消失に対する処置

ホスト接続消失について考えられる問題を調べる場合は、以下を検討してください。

- 接続が消失しても、そのホスト上のストレージに対するセキュア パスの保護機能が失われているとは限りません。ホストが稼動している場合は、問題の原因はほぼネットワークの接続問題と考えられるので、失われるのはセキュア パスのリモート管理機能だけです。セキュア パスのRaiDiskマルチパス ドライバによって、ストレージに対する可用性が保護されています。
- ホストがクラスタのメンバーである場合、SPMは、稼動しているホストから受信したデータに基づいて、ストレージ情報の報告を続けます。
- ホストがクラスタのメンバーである場合、クラスタ管理ユーティリティを確認して、稼動しているホストにストレージ リソースがフェールオーバされたかどうかを判定します。
- ホストが稼動中、または再起動後の場合、Windowsイベント ビューアを実行してアプリケーション ログとシステム ログを調べ、接続消失以前と接続消失中に何が起こったかを確認します。特に、ホストとSPMクライアント間の接続問題の原因となる可能性のあるネットワークの問題を確認します。
- SPMは、接続が復旧すると、ホストとの通信を自動的に再確立します。

## ストレージ プロファイルのプロパティの設定

初めてSPMにログオンしたら、現在のストレージ プロファイルの**プロパティ**設定を調べ、調整します。なお、これらの**プロパティ**は、SPMストレージ プロファイルによって管理されるすべてのリソース全体に影響します。[プロパティ]プルダウン メニューを使用すると、以下が可能です。

- **自動フェールバック**の有効化または無効化（デフォルトは無効）。自動フェールバックを有効にすると、代替パスにフェールオーバされたすべてのストレージセットが、優先パスへのアクセスが復元されると、自動的に優先パスにフェールバックされます。ストレージセットが自動フェールバックされるのは、それらのストレージセットに対するI/O動作が進行中の場合だけです。自動フェールバックの有効化とともにパスの検証を有効にすると、停止ストレージセットのフェールバックが行われます。

- **パスの検証**の有効化または無効化（デフォルトは有効）。パスの検証を有効にすると、セキュア パスは、すべての優先パスと代替パスの現在の状態を判定するために、それらのパスに対して定期的に診断を実行します。パスにI/O動作が完了しない問題があると診断された場合、そのパスは障害と記録され、そのパスに対する以後のI/O動作が許可されなくなります。
- **ポーリング間隔**の設定（デフォルトは90秒）。ポーリング間隔は、SPMがセキュア パス エージェントにストレージ プロファイル内のコンフィギュレーション変更情報を要求する間隔です。ポーリング間隔が影響するのは、表示情報の更新間隔だけで、現在のコンフィギュレーションには影響しません。ユーザは、5秒～30分の範囲でポーリング間隔を選択できます。

## ストレージ システム表示

SPMのストレージ システム表示（左側のウィンドウ）に、物理ストレージ オブジェクトが表示されます（図4-4）。この表示内容を展開すると、セキュア パス ストレージ プロファイルを構成する各RAIDストレージ システム、コントローラ、および関連ストレージセットが表示されます。


図4-4. SPMシングル ホスト ストレージ プロファイル - ストレージ システム表示

### ストレージ システムおよびコントローラ

- ストレージ システム**ID -** 各RA4000/4100ストレージ システムは、固有の64ビット値によって識別されます。

  RA4000/4100ストレージ システムの場合、ストレージ システムIDは、製造時に決定され、コントローラのNVRAMに保存されます。ストレージ システムIDは、RAIDストレージ システムの全使用期間にわたって一定です。

- **コントローラのシリアル番号 -** RA4000/4100ストレージ システムの個々のコントローラは、コントローラの製造時に割り当てられる固有の英数字によって識別されます。

### RAID Arrayストレージセット

- **ディスクLUN UUID -** セキュア パスによって割り当てられる固有の128ビット値。
- **ディスク番号 -** Windowsディスク マネージャによって割り当てられる論理ディスク番号。
- **ドライブ文字 -** Windowsディスク マネージャによって割り当てられる論理ドライブ文字。
- **バス/ターゲット/LUN -** ホスト サーバとの接続を表す物理アドレス。
- **ボリューム ラベル -** Windowsエクスプローラまたはディスク マネージャを使用してユーザによってボリュームに割り当てられるラベル。

ツールバーの上にある[表示]プルダウン メニューを使用すると、ストレージセットを識別するためにSPMが使用する方法を選択できます。SPMは、選択したストレージセットIDとともに、常に、所有権を持つホスト名、またはクラスタ名（クラスタ化ホストの場合）を表示します。

## 物理パス表示

ストレージ システム表示でストレージセットを強調表示すると、右側のウィンドウに、そのストレージセットにアクセスするように設定された物理パスに関する情報が表示されます。物理パス表示には、各パスに関する次の情報が表示されます。

- **ホスト -** ストレージセットまでのアクセス パスが確立されているセキュア パス ホスト システム。
- **コントローラ -** パスを提供するRAIDストレージ システム コントローラ。
- **SCSIポート -** パスを提供するホスト バス アダプタの物理ポート番号。HBAは、Windowsがそのホスト上でアダプタを検出する順番によって決まる相対的な番号です。
- **HBAスロット（ホスト バス アダプタ スロット） -** 識別されたHBAを含むホスト ノードのPCIスロットです。
- **B-T-L（バス-ターゲット-LUN） -** ストレージセットのパス アドレスを表す物理バス、ターゲット、およびLUN番号。

- **モード -** 定格状況と障害状況におけるパスの動作を指定する、ユーザが選択できるパラメータ。パス モードは、優先、代替、優先オフライン（優先およびオフライン）、または代替オフライン（代替およびオフライン）に設定できます。
- **状態 -** 現在のパスの動作状況を表す属性。パスの状態には、稼動、障害、および利用可能があります。

次のSPM画面（図4-5）は、"ml370j2"というホストにセキュア パスで保護された複数のRAIDストレージ システムが接続されているシングル ホスト コンフィギュレーションを示しています。

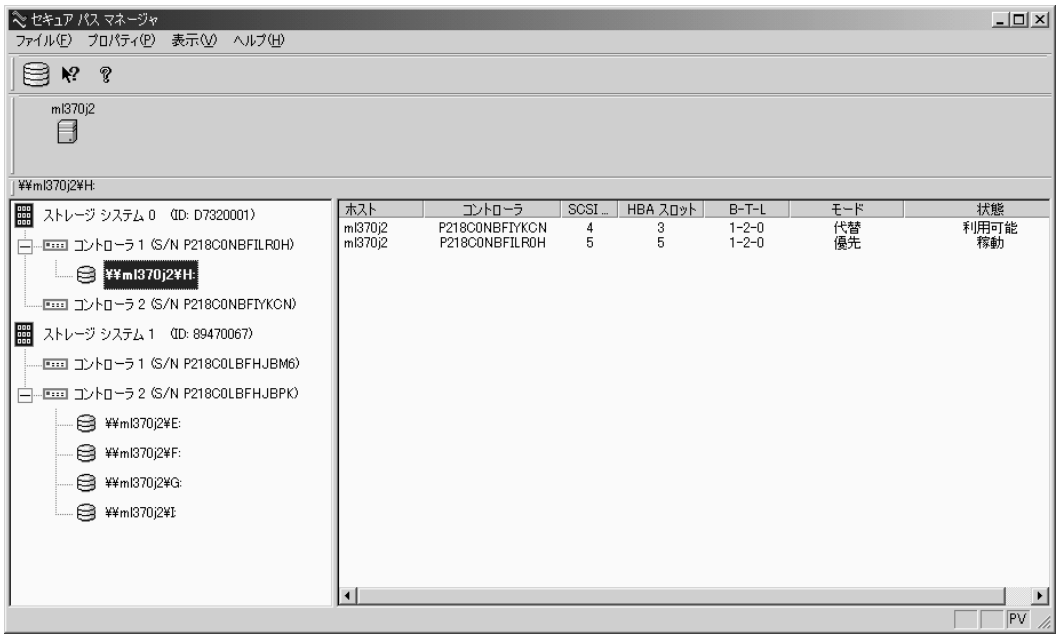



**図4-5. SPMシングル ホスト マルチアレイ ストレージ プロファイル - 物理パス表示**

Windowsの論理ドライブ文字Eを持つストレージセットがストレージ システム表示で強調表示され、対応する物理パス情報が右側のウィンドウに表示されています。物理パス表示の各行は、この特定のストレージセットまでの個別パスを表します。

この例では、ホスト"ml370j2"とドライブEの間に2つのパスが設定されています。両方のパスはそれぞれHBAのポート4とポート5を介して、バス1、ターゲット1、LUN 0にあるストレージセットにアクセスします。1つのパスは優先パスに、もう1つのパスは代替パスになります。

最初の行は、このパスが優先モードで稼動状態にあることを示しています。初期開始状態は、所有していたコントローラに基づきます。優先モードは、正常な状況でのすべてのI/O動作に使用する特定のパスを指定するために、ユーザによってそのパスに対して選択されます。優先モードで稼動状態にあるパスは、正常な動作状況で現在ストレージセットへのアクセスに使用されているパスです。

物理パス表示の2行目は、このパスが代替モードで利用可能状態にあることを示しています。代替モードは、すべての優先パスで障害が発生した後にのみストレージセットへのアクセスに使用する特定のパスを指定するために、ユーザによってそのパスに対して選択されます。代替モードで利用可能状態にあるパスは、優先パスで障害が発生した場合に、ストレージセットへのアクセスにただちに使用できる状態にあるパスです。

優先パスに表示されているコントローラのシリアル番号は、ストレージ システム表示でドライブEを所有しているコントローラのシリアル番号と同じです。

利用可能状態にあるパスのシリアル番号は、優先モードにあるパスのシリアル番号と異なり、この2つのパスがもう一方のコントローラを介してスタンバイアクセスを提供していることを表します。現在優先パスを提供しているコントローラが機能しなくなった場合、稼動しているコントローラ上のパスが優先状態に移行します。

## ポーリング間隔および表示更新

パス状態の表示を最新に保つため、SPMは、定期的にすべてのセキュア パス ホストに対して更新を要求します。ネットワーク トラフィックを最小化するため、SPMは、コンフィギュレーションの変更が報告された場合のみ表示の更新を実行し、変化した情報だけを更新します。状態の変化を要求する間隔は、[プロパティ]メニューから設定したポーリング間隔で決まります。

表示更新動作を[表示]メニューのメニュー項目またはF5ホットキーを使用して起動すると、SPMは、ストレージ プロファイル内のすべてのホストに最新のコンフィギュレーション情報を要求します。SPMは、表示更新の要求に応えて、すべての表示情報を更新します。表示更新動作では表示全体を更新するので、通常のポーリング動作より時間がかかる場合があります。表示更新に要する時間は、監視対象ストレージ プロファイル内のホスト、RAIDストレージ システム、およびストレージセットの数に依存します。

# ストレージセットおよびパスの管理

SPMによって管理されるストレージセットとパスに対して、以下の操作を実行できます。

- コントローラ間でストレージセットを移動する
- パスをオフラインにする
- パスをオンラインにする
- パスを検証する
- パスを修復する

次のSPM動作はSPM GUIに組み込まれていますが、RA4000/4100ストレージ システムには適用されないため、グレイで表示されます。

- パスを代替にする（代替に設定）
- パスを優先にする（優先するに設定）
- 優先パスを変更する（優先を変更）
- 負荷を分散する（負荷分散）

## ストレージセットを移動する

現在のRA4000コントローラから他のコントローラに所有権を移動したい場合は、「ストレージセット移動」操作を実行します。この操作は、自動フェールバックが無効の場合に、フェールオーバされたストレージセットを手動でその優先パスに戻す必要がある場合に便利です。

ストレージセットを移動する方法は、2つあります。

1. ストレージ システム表示でドライブをクリックして強調表示します。
2. ドライブを他のコントローラまでドラッグするか、マウスの右ボタンをクリックして[他のコントローラへ移動]を選択します。

特定のRA4000/4100ストレージ システムのLUNはすべて、コントローラ間でグループとして一緒に移動します。

## パスをオフラインにする

いかなる状況でもパスをI/O動作に使用できないようにしたい場合、「オフライン パス化」操作を実行します。たとえば、ストレージ インターコネクト コンポーネントを交換したり、それらのコンポ―ネントに対する作業をする必要がある場合は、オフライン モードを使用します。パスをオフラインにするには、以下の手順に従ってください。

1. 優先利用可能パスまたは代替パスをクリックします。稼動状態にあるパスをオフライン モードに変更することはできません。
2. マウスの右ボタンをクリックして[オフラインに設定]を選択します。

パスが代替利用可能であった場合、モードは代替オフラインになります。パスが優先利用可能であった場合は、モードは優先オフラインになります。

## パスをオンラインにする

現在オフライン モードにあるパスを元のモードに戻したい場合、「オンライン パス化」操作を実行します。パスをオンラインにするには、以下の手順に従ってください。

1. "代替オフライン"または"優先オフライン"モードにあるパスをクリックします。
2. マウスの右ボタンをクリックして[オンラインに設定]を選択します。

パスが"代替オフライン"であった場合、モードは"代替利用可能"になります。パスが優先オフラインであった場合は、モードは優先利用可能になります。

## パスを検証する

SPMによってパスの現在の状態を確認したい場合、「パスの検証」を実行します。パスを検証するには、以下の手順に従ってください。

1. パスをクリックします。
2. マウスの右ボタンをクリックして[パスの検証]を選択します。

検証が終了すると、操作の結果を示すポップアップ メッセージが表示されます。この操作を実行しても、状態は変化しません。

### パスを修復する

問題を解決した後で、障害状態になっていたパスへのアクセスを復元したい場合、「パス修復」操作を選択します。パスを修復するには、以下の手順に従ってください。

1. 障害状態にあるパスをクリックします。
2. マウスの右ボタンをクリックして[修復]を選択します。

修復が正常に終了すると、パスの状態は、モードが代替であった場合は利用可能に、優先であった場合は稼動に変化します。

## パスとコントローラの障害の検出と識別

SPMは、ポーリング間隔の設定で決まる一定の間隔で、ストレージ プロファイル内のすべてのシステムの状態を監視します。ストレージ システム表示では障害がアイコンで表示され、物理パス表示ではパス状態が障害と記録されます。

さらに、RaiDiskドライバによって、フェールオーバ イベントがWindowsイベント ビューアに記録されます。

SPMステータスを定期的に監視して、ストレージ リソースの性能や可用性を低下させる可能性のあるフェールオーバ イベントの発生を確認してください。

コンフィギュレーションにストレージセットまでのパスが2つしかなく、コンポーネントの障害によって一方のパスが消失すると、可用性が低下します。この状況でさらに障害が発生すると、セキュア パスは、リダンダント パスにフェールオーバできません。

セキュア パスにパスの可用性を保護させるために、SPMクライアントを実行する必要はありません。ホスト上で実行されているRaiDiskデバイス ドライバが、セキュア パスの自動パス保護機能を処理します。

### パス障害の検出

SPMディスプレイには、パス障害の存在を示すいくつかの種類のアイコンが表示されます。これらのアイコンを理解すると、障害に関連する特定のストレージセットとパスを識別するのに役立ちます。以下に示すアイコンがストレージ システム表示に表示され、セキュア パスによってパス障害が検出されたことを表します。

## ストレージ システム パスの障害を検出

図4-6に示すアイコンは、セキュア パスによって、そのRAID Arrayストレージ システムまでの、すべてではないが1つまたは複数のパスで障害が検出されたことを表します。ストレージ システムの表示を展開して、影響を受けるコントローラとストレージセットを特定します。

図4-6. ストレージ システム パスの障害を検出

## ストレージ コントローラ パスの障害を検出

図4-7に示すアイコンは、セキュア パスによって、そのストレージ コントローラまでの、すべてではないが1つまたは複数のパスで障害が検出されたことを表します。ストレージ コントローラの表示を展開して、影響を受けるストレージセットを特定します。

図4-7. ストレージ コントローラ パスの障害を検出

パスの検証プロパティが有効でない場合、セキュア パスは、アクティブI/Oが存在するパスだけで障害を検出します。すなわち、同じコントローラが所有する他のストレージセットまでの1つまたは複数のパスで障害が発生しても、セキュア パスによって検出されない場合があります。ただし、セキュア パスは、これらのドライブのパスまたはコントローラのフェールオーバを実行し、その後それらのストレージセットのどれかまたはすべてに対してI/O動作が行われると障害を示します。

パスの検証が有効の場合、セキュア パスは、コントローラ上の影響を受けるすべてのストレージセットまでのパスの障害を自動的に検出し、可用性を維持するために必要なパスまたはコントローラのすべてのフェールオーバをただちに実行します。

## ストレージセット パスの障害を検出

図4-8に示すアイコンは、セキュア パスによって、そのストレージセットまでの、すべてではないが1つまたは複数のパスで障害が検出されたことを表します。ストレージセットをクリックして強調表示し、物理パス表示の情報を調べて、パス障害の性質を特定します。

図4-8. ストレージセット パスの障害を検出

### すべてのパスの障害

以下に示す各アイコンは、影響を受けるストレージ オブジェクトまでのすべてのパスで障害が発生したことを表します。

図4-9. ストレージ システムの障害を検出

図4-10. ストレージ コントローラの障害を検出

図4-11. ストレージセットの障害を検出

## パス フェールオーバの特定

パス フェールオーバの原因を特定するには、まずストレージ システム表示でパス障害アイコンを確認し、次に影響を受けるストレージセットの物理パス表示を調べます。障害状態にあるパスがないか確認します。特定のストレージセットまでの1つまたは複数のパスが障害状態にあるかどうかは、以下の条件に依存します。

- 影響を受けるストレージセットでI/Oがアクティブだったか

  セキュア パスは、I/O動作の異常終了を検出して、パスの障害を決定します。すなわち、消失した優先パスでI/Oがアクティブでなかった場合、障害は検出されず、I/O動作が行われるまでパスの状態は障害と記録されません。

- パスの検証が有効になっているか

  パスの検証は、定期的にすべてのパスの稼動状況をテストし、自動的に優先パスと代替パスの障害を検出します。すなわち、コントローラ フェールオーバにより、優先パスが障害状態と記録されます。

## コントローラ フェールオーバの特定

RA4000コントローラの障害により、特定のストレージセットの所有権が稼動コントローラに移転されます。フェールオーバは、アクティブI/O動作を持つストレージセットだけに行われます。コントローラ フェールオーバが行われたことが疑われる場合は、パスの検証を使用して、すべての設定済みパスの稼動状況を確認します。パスの検証は任意の時点で有効にすることができますが、ストレージ プロファイル内のすべてのパスの整合性を確認するためにストレージセット当たり約2分かかります。

パスの検証によって、ストレージ システム表示に特定の障害コントローラが示されます。図4-10に示す障害が発生したストレージ コントローラのアイコンがないか確認します。このコントローラ上にあったすべてのストレージセットが、稼動コントローラにフェールオーバされたことが表示されます。パスの検証の結果、障害が発生したコントローラまでのすべての代替パスが障害状態に移行し、稼動コントローラ上の各ストレージセットにストレージセット パス障害アイコンが表示されます。

# フェールオーバ イベントに対する処置

フェールオーバに関連した問題を調べる場合、以下の点を検討してください。

- ストレージセットまでの追加の使用可能パスが残っているか、またはこの障害によって、以後の障害への耐性が完全になくなったか
- 障害の原因は何か

  ほとんどのストレージ チャネル問題の原因は、インターコネクト ハードウェアの障害です。障害以前と障害中に何が起こったかを特定するには、Windowsイベント ビューアを調べ、システム ログにRaiDiskやHBAデバイスドライバによって入力されたイベントがないか確認します。アプリケーション ログで、セキュア パス エージェントとSPMによって入力されたイベントかないか確認します。スイッチまたはハブを見て、LEDやLCDがハードウェア障害を示していないか確認します。

# MSCSクラスタでのSPMの使用

Microsoft Cluster Service（MSCS）環境のSPMディスプレイでは、ストレージシステム表示に、常にストレージセットとともに関連クラスタ名が表示されます。ストレージセットを強調表示すると、物理パス表示に、各クラスタ ホストからそのストレージセットまでのすべての物理パスが表示されます。

MSCSは、ドライブ アクセスを同期化するメカニズムとして、ハードウェア デバイスの予約を使用します。デバイスの予約とは、共有ストレージセットが、実質的に任意の時点で1つのクラスタ ホストによって「所有」されることです。アクティブ状態にあるストレージセット パスをSPMで探すことによって、所有権を持つホストを特定できます。所有権を持たないホストは、優先モードで使用可能状態にあるストレージセット パスによって示されます。

# 第5章

# セキュア パスの接続問題のトラブルシューティング

この章では、次のセキュア パス ネットワーク接続のトラブルシューティングについて説明します。

- クライアント/エージェントに関する注意事項
- ネットワークに関する注意事項

詳しい説明が必要な場合は、サービス エンジニアまでご連絡ください。

## クライアント/エージェントに関する　意　項

次のクライアント/エージェントに関する注意事項は、ネットワークの環境問題のトラブルシューティングに役立ちます。

- エージェント コンフィギュレーション ユーティリティを使用して、エージェントの認証クライアントのリストに各クライアントのNetBIOS名またはFQDN（完全修飾ドメイン名）を追加し、パスワード ダイアログ ボックスでパスワードを設定します。変更を行ったら、[管理ツール]の[サービス]アプレットを使用してセキュア パス エージェントを終了し、再起動して、データベースを更新します。
- セキュア パス クライアントにログインする際は、必ず、エージェントのデータベースに入力した名前タイプ（NetBIOSまたはFQDN）を使用します。
- 使用する各名前は、次のいずれかを使用して、対応するネットワークIPアドレスに割り当てる必要があります。
  - DNS（ドメイン ネーム システム、完全修飾ドメイン名の場合）
  - *HOSTS*ファイル（NetBIOSまたはFQDNをIPアドレスに割り当てる静的なテキスト ファイル）
  - WINS（Windowsインターネット ネーミング サービス、NetBIOS名の場合）

  詳細については、下記の「ネットワークに関する注意事項」を参照してください。
- クラスタ コンフィギュレーションでは、選択したパスワードが、クラスタ内の両方のエージェントに共通していることを確認します。
- セキュア パスは、クライアントを認証するためにWindowsドメイン認証を使用しません。クライアント認証は、エージェントごとに、セキュア パス コンフィギュレーション データベースからの名前-IPアドレス解決とパスワード確認を使用して処理されます。

## ネットワークに関する　意　項

次のネットワークに関する注意事項は、ネットワークの接続問題のトラブルシューティングに役立ちます。

- クライアント名（15文字以内、"."なし）は、クライアント ノードとエージェント ノードが同じサブネット上に構成されている限り、NetBIOSブロードキャスト解決によって解決できます。クライアントとエージェントが異なるサブネット上に存在する場合、DNS、*HOSTS*ファイル、WINS、または*LMHOSTS*ファイルを（この順番で）使用して、アドレスを解決する必要があります。

- *LMHOSTS*ファイルを使用する場合は、クライアント システムのTCP/IPプロトコル プロパティで[LMHOSTSの参照を有効にする]ボックスが選択されていることを確認します。

  クライアント システムで、接続したいエージェントのNetBIOS名とIPアドレスを*LMHOSTS*ファイルに入力し、保存する必要があります。

  [LMHOSTSのインポート]ボタンをクリックして、*LMHOSTS*ファイルの位置を指定します。通常、*LMHOSTS*ファイルと*HOSTS*ファイルは、¥winnt¥system32¥drivers¥etcサブディレクトリにあります。

  最後に、コマンド プロンプトで"NBTSTAT -R"コマンドを発行して、リモート名テーブルをパージし、ロードしなおします。

- 15文字を超えたり、"."を含んでいるクライアント名は、*HOSTS*ファイルに名前を入力するか、DNSサーバによって解決する必要があります。また、DNSサーバが該当する情報で更新されている場合、DNSにNetBIOS名を解決させることもできます。

- ホスト名-IP解決にDNSを使用している場合は、DNSサーバ上のDNSデータベースを該当する情報で更新する必要があります。

- ネットワーク接続を最適化するため、DNSで完全修飾ドメイン名（FQDN）を使用することをおすすめします。

- 管理とセキュリティを重視する実務の環境では、DNS名解決に完全修復ドメイン名を使用することをおすすめします。

- テスト環境や評価環境では、通常、クライアントの*HOSTS*ファイルにサーバの名前を追加し、サーバの*HOSTS*ファイルにクライアントの名前を追加するだけで済みます。

- IPアドレスでなくホスト名を使用して、ローカルで、またリモート ホストから、セキュア パス ホストに対して"ping"を実行できることを確認します。

# 付録A

# 用語集

**HBA**
ホスト システムをSCSIバスまたはファイバ チャネル アービトレーテッド ループに接続するためのインタフェースとして動作するI/Oデバイス。HBAには、Windowsオペレーティング システムによって検出順に相対ポート番号が割り当てられます（「ポート」を参照してください）。

**LUN**
Logical Unit Number（論理ユニット番号）。RAIDシステム コントローラのデバイスに割り当てられる実際のユニット番号です。

**コントローラ**
ホストと、アレイとして編成された1つ以上のLUN間の通信を容易にするハードウェア デバイス。RA4000コントローラが、セキュア パス用にサポートされているアレイ コントローラです。RA4000/4100ストレージ システム内の各コントローラは、セキュア パス マネージャによってコントローラ アイコンの横に表示される固有のシリアル番号により識別されます。セキュア パス マネージャは、サブシステム アイコンの横に表示される固有の64ビットIDによって、マルチパス モードに設定されたコントローラ ペアを識別します。

**状態** パスの現在の動作状況を表す属性。パスは以下のどれかの状態になります。

- **稼動 -** 現在I/O要求のサービスを行っているパス。
- **障害 -** 無効にされ、I/O要求のサービスを行っていないパス。
- **利用可能 -** 稼動状態でも障害状態でもないパス。

**ターゲット** ターゲット番号は、コントローラ レベルの割り当て関数によって割り当てられ、FC-ALトポロジ内のALPA（アービトレーテッド ループ物理アドレス）から得られます。

**バス** ファイバ チャネル コンフィギュレーションでは、HBAは、バス アドレス空間を拡張する人工的な手段として、複数のバス番号を使用できます。

**パス** ホスト サーバとストレージ デバイス間で、データおよびコマンドが通過できるようにする仮想通信経路。

**ポート** HBAの相対番号。特定のポート番号は、Windowsオペレーティング システムによって検出順に決定され、SCSI、ファイバ チャネル、およびIDEアダプタ タイプが含まれます。

**ホスト** セキュア パス サーバ ソフトウェア（RaiDiskドライバおよびエージェント サービス）を実行中のコンピュータ システム。

**モード** 障害のない、および障害のある状況でのパスの動作を指定する、ユーザが選択できるパラメータ。パスは、次のどれかのモードに設定できます。

- **優先 -** 優先させるI/Oパスを表します。パスの検証を有効にすると、すべての優先パスが検証されます。
- **代替 -** デバイスまでのすべてのプライマリ パスで障害が発生した場合のデバイス アクセス用にのみ使用されるパスを表します。このモードにあるパスは、パスの検証に含まれます（パスの検証が有効の場合）。
- **オフライン -** LUNに対するI/Oに使用しないパスを表します。オフライン モードは、他の2つのパス モードのどれかと論理的に組み合わされます。

# 録B

# セキュア パス ソフトウェアの削

この付録では、セキュア パス ソフトウェアをサーバから削除する方法について説明します。これは、シングル パスRAIDストレージ環境に戻す場合に必要になります。

セキュア パス ソフトウェアをシステムから削除するには、以下の手順に従ってください。

1. [コントロール パネル]を起動し、[アプリケーションの追加と削除]を選択します。
2. [SecurePath Client]を選択します。
3. 表示されるウィンドウで、[OK]をクリックします。
4. [SecurePath Server]を選択します。
5. 表示されるウィンドウで、[OK]をクリックします。
6. システムをシャットダウンします。
7. 1対のコントローラから、リダンダント パスを外します。

これで、セキュア パス ソフトウェアの削除は完了です。

**注**: セキュア パスを再インストールできるように、"client.ini"は削除しません。

# 索引

## け



## こ



## さ



## し



## す



## せ

## そ



## て



## と



## は



## ひ



## ふ

## へ



## ほ



## よ



## ろ