



IBM Systems - iSeries

iSeries Windows 環境





IBM Systems - iSeries

iSeries Windows 環境

ご注意！

本書および本書で紹介する製品をご使用になる前に、 291 ページの『特記事項』に記載されている情報をお読みください。

本書は、IBM i5/OS (製品番号 5722-SS1) のバージョン 5、リリース 4、モディフィケーション 0 に適用されます。また、改訂版で断りがない限り、それ以降のすべてのリリースおよびモディフィケーションに適用されます。このバージョンは、すべての RISC モデルで稼働するとは限りません。また CISC モデルでは稼働しません。

本マニュアルに関するご意見やご感想は、次の URL からお送りください。今後の参考にさせていただきます。

<http://www.ibm.com/jp/manuals/main/mail.html>

なお、日本 IBM 発行のマニュアルはインターネット経由でもご購入いただけます。詳しくは

<http://www.ibm.com/jp/manuals/> の「ご注文について」をご覧ください。

(URL は、変更になる場合があります)

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原 典： IBM Systems - iSeries
Windows environment on iSeries
Version 5 Release 4

発 行： 日本アイ・ピー・エム株式会社

担 当： ナショナル・ランゲージ・サポート

第1刷 2006.2

この文書では、平成明朝体™W3、平成明朝体™W7、平成明朝体™W9、平成角ゴシック体™W3、平成角ゴシック体™W5、および平成角ゴシック体™W7を使用しています。この(書体*)は、(財)日本規格協会と使用契約を締結し使用しているものです。フォントとして無断複製することは禁止されています。

注* 平成明朝体™W3、平成明朝体™W7、平成明朝体™W9、平成角ゴシック体™W3、平成角ゴシック体™W5、平成角ゴシック体™W7

© Copyright International Business Machines Corporation 1998, 2006. All rights reserved.

© Copyright IBM Japan 2006

目次

第 1 章 iSeries Windows 環境	1	サービス・プロセッサ構成	49
第 2 章 V5R4 での新機能	3	接続セキュリティ構成	49
第 3 章 印刷可能な PDF	5	証明書ストア	49
第 4 章 概念	7	高可用性の概念	50
統合サーバーの概要	7	セキュリティの概念	51
利点	8	IXS および IXA 接続システムのセキュリティ	51
用語集	10	iSCSI 接続システムのセキュリティ	51
ハードウェアの概念	14	ユーザーおよびグループの概念	54
IXS および IXA 接続サーバー	15	ユーザー構成の種類	56
iSCSI 接続サーバー	18	ユーザー登録テンプレート	58
iSCSI 接続サーバーの概要	19	パスワードについての考慮事項	59
基本的な単一サーバー・サポート	19	第 5 章 iSeries での Windows 環境の インストールと構成	61
複数サーバー・サポート	21	ハードウェア要件	62
拡張 iSCSI サポート	22	ソフトウェア要件	64
iSCSI を使用したディスクレス・ブート	23	統合 Windows サーバーのインストールの準備	64
Windows コンソール	24	マシン・プール・サイズ要件	66
考慮事項	25	時刻合わせ	67
パフォーマンス	26	i5/OS TCP/IP を統合 Windows サーバー用に構成 する	67
iSeries 記憶域スペースと専用ディスクの比較	26	統合 Windows サーバー上の iSeries Access for Windows	68
記憶域スペースのバランス化	27	iSeries NetServer の使用可能化	68
iSCSI 接続サーバーのパフォーマンス	28	iSeries NetServer 用のゲスト・ユーザー・プロフ ァイルの作成	68
仮想イーサネット	29	IBM i5/OS 統合サーバー・サポートのインストール	69
ネットワークングの概念	29	Windows サーバーのインストールの計画	70
サービス・プロセッサ接続	30	iSCSI ハードウェアのインストールの計画	70
iSCSI ネットワーク	31	ホストされるシステムのブート・モードの計画	70
Point-to-Point 仮想イーサネット	33	サービス・プロセッサ構成およびリモート・ システム構成の作成	71
仮想イーサネット・ネットワーク	34	サービス・プロセッサ接続の計画	72
外部ネットワーク	38	iSeries サーバーにおけるサービス・プロセッ サーのディスカバリー方法の構成	73
ソフトウェアの概念	38	ネットワーク・サーバー記述	73
統合 xSeries サーバー (IXS) と統合 xSeries アダ プター (IXA) 接続 xSeries サーバー	38	i5/OS パラメーターのインストール・ワークシ ート	73
ネットワーク・サーバー記述	41	FAT、FAT32、および NTFS ファイル・システム の比較	96
ハードウェア・リソース名	41	ヒント: 複数の統合サーバーがある場合のリソー ス名の検索	97
ネットワーク・サーバー記憶域スペース	41	サポートされている言語バージョン	97
仮想イーサネット回線記述	42	Windows 2000 Server または Windows Server 2003 のインストール	98
TCP/IP インターフェース	42	Windows のインストールのための iSCSI ハード ウェアの準備	99
システム・バスおよび HSL データ・フロー	43	サービス・プロセッサ・セキュリティの初 期化	99
iSCSI 接続の xSeries および IBM BladeCenter サ ーバー	43	ネットワーク・サーバー・ホスト・アダプター の作成と開始	99
ネットワーク・サーバー・ホスト・アダプター	45		
リモート・システム構成	45		
サービス・プロセッサ構成	46		
ネットワーク・サーバー記述	46		
ネットワーク・サーバー記憶域スペース	47		
データ・フロー	47		
セキュリティのある iSCSI 接続の xSeries およ び BladeCenter サーバー	47		
リモート・システム構成	49		

i5/OS コンソールからのインストールの開始	100	統合 Windows サーバーへのネットワーク・アダ プター・デバイス・ドライバのインストール と、アダプター・アドレス情報の追加	127
統合 Windows サーバー・コンソールからのイン ストールの続行	104	ネットワーク・アダプターの除去	128
サーバーのインストールの完了	105		
IBM iSeries Integration for Windows Server ライ センス・プログラムのアップグレード	106	第 7 章 iSCSI 接続サーバーへの接続の 管理	129
IBM i5/OS 統合サーバー・サポートの統合サー バー側のアップグレード	108	iSCSI 構成オブジェクトの処理	129
285x または 661x から 2890 統合 xSeries サー バー・ハードウェアへの移行	109	ネットワーク・サーバー・ホスト・アダプターの 管理	129
iSCSI 接続サーバーへの移行	109	ネットワーク・サーバー・ホスト・アダプタ ー・オブジェクトの作成	129
Windows クラスタ・サービス	109	別のオブジェクトを基にしてネットワーク・ サーバー・ホスト・アダプター・オブジェク トを作成する	130
Windows クラスタ・サービスのインストール	110	ネットワーク・サーバー・ホスト・アダプタ ーのプロパティの表示	131
新しい統合 Windows サーバーへの Windows クラスタ・サービスのインストール	110	ネットワーク・サーバー・ホスト・アダプタ ーのプロパティの変更	131
既存のサーバーへの Windows クラスタ・ サービスのインストール	111	ネットワーク・サーバー・ホスト・アダプタ ーの開始	131
Windows クラスタ・サービスをインストール する前の Windows システムの準備	112	ネットワーク・サーバー・ホスト・アダプタ ーの停止	132
Windows への Windows クラスタ・サービ スのインストール	113	ネットワーク・サーバー・ホスト・アダプタ ーの削除	132
Windows 2000 Server へのクラスタ・サー ビスのインストール	114	リモート・システム・ネットワーク・サーバー構 成の管理	132
Windows Server 2003 へのクラスタ・サー ビスのインストール	114	リモート・システム構成オブジェクトの作成	133
Windows Server 2003 Active Directory Server を 使用して Kerberos を使用可能にする	116	別のオブジェクトを基にしてリモート・シス テム構成オブジェクトを作成する	134
2892-002 または 4812-001 統合 xSeries サーバ ーに ATI Radeon 7000M の Windows 2000 用ビ デオ・デバイス・ドライバをインストールする	116	リモート・システム構成プロパティの表示	134
2892-002 または 4812-001 統合 xSeries サーバ ー上の Windows Server 2003 のハードウェアの 加速を調整する	117	リモート・システム構成プロパティの変更	134
インストール中のエラー・メッセージへの応答	117	リモート・システムの状況の表示	135
TCP/IP に応じた統合 Windows サーバーのオンへの 自動変更の設定	118	リモート・システム構成オブジェクトの削除	135
コード修正	119	サービス・プロセッサ・ネットワーク・サーバ ー構成の管理	135
コード修正のタイプ	119	サービス・プロセッサ構成オブジェクトの 作成	136
Windows サーバー・コンソールによる統合ソフ トウェア・レベルの同期化	120	別のオブジェクトを基にしてサービス・プロ セッサ構成オブジェクトを作成する	136
iSeries ナビゲーターによる統合ソフトウェア・ レベルの同期化	120	サービス・プロセッサ構成プロパティの 表示	137
リモート・コマンドによる統合ソフトウェア・レ ベルの同期化	121	サービス・プロセッサ構成プロパティの 変更	137
		サービス・プロセッサの初期化	138
		サービス・プロセッサ構成オブジェクトの 削除	138
第 6 章 仮想イーサネットおよび外部ネ ットワークの管理	123	接続セキュリティ・ネットワーク・サーバー構 成の管理	138
IP アドレス、ゲートウェイ、および MTU 値の構 成	123	接続セキュリティ構成オブジェクトの作成	139
仮想イーサネット・ネットワークの構成	123	別のオブジェクトを基にして接続セキュリテ ィー構成オブジェクトを作成する	139
区画間仮想イーサネット・ネットワークの構成	124	接続セキュリティ構成プロパティの表示	140
Point-to-Point 仮想イーサネット・ネットワークにつ いて	126	接続セキュリティ構成プロパティの変更	140
外部ネットワーク	127	接続セキュリティ・オブジェクトの削除	141

	i5/OS とホストされるシステムとの間のセキュリテ	
	ィーの構成	141
	CHAP の構成	141
	IPSec の構成	142
	サービス・プロセッサ SSL の構成	143
	SSL の自動初期化	144
	SSL の手動初期化	144
	サービス・プロセッサ・パスワード	145
	ファイアウォールの構成	145
	iSCSI ホスト・バス・アダプターの管理	146
	iSCSI ローカル・ホスト・アダプター間のホッ	
	ト・スペア	146
	iSCSI HBA 使用法の管理	147
	複数のホストされるサーバー間での iSCSI	
	HBA の共用	147
	ワークロードを複数の iSCSI HBA に分散す	
	る	148
	冗長度を確保するための複数の iSCSI HBA	
	の使用	149
	iSCSI ネットワークの Windows 側での iSCSI	
	HBA 割り振りの管理	150
	最大伝送単位 (MTU) の考慮事項	151
	1500 バイトを超えるフレームをサポートする	
	iSCSI ネットワークで最高のパフォーマンス	
	を得るための仮想イーサネットの構成	151
	最大フレーム・サイズが 1500 バイト未満の	
	iSCSI ネットワーク用仮想イーサネットの構	
	成	152
	MTU をネゴシエーションしない、通常と異	
	なる非 TCP アプリケーションをサポートす	
	るよう仮想イーサネットを構成する	152
	統合 DHCP サーバー	153
	リモート・サーバーのディスカバリーおよび管理	154
	IBM Director のインストールおよび構成	154
	リモート・サーバーおよびサービス・プロセッサ	
	ーのディスカバリー	155
	サービス・プロセッサのディスカバリー構	
	成	155
	動的 IP アドレッシング (DHCP)	157
	サービス・プロセッサのディスカバリー方	
	式	157
	マルチキャスト・アドレッシングを使用す	
	る Service Location Protocol (SLP)	158
	IP アドレスによるディスカバリー	159
	ホスト名によるディスカバリー	159
	管理モジュールまたは RSA II の Web イン	
	ターフェースの使用	160

第 8 章 統合 Windows サーバーの管理 163

統合サーバーの開始と停止	163
統合 Windows サーバーの開始と停止 (iSeries ナ	
ビゲーターを使用する場合)	164
統合 Windows サーバーの開始と停止 (文字ベー	
スのインターフェースを使用する場合)	164
Windows サーバーのコンソールからの統合サー	
バーのシャットダウン	164

統合 Windows サーバーが存在する場合に		
iSeries を安全にシャットダウンする方法	165	
4812 IXS 仮想シリアル・コンソールへの接続	165	
統合 Windows サーバーの構成情報の表示または変		
更	166	
メッセージ・ログ	167	
統合 Windows サーバーのコマンドのリモート実行	168	
リモート・コマンド実行に関するガイドライン	169	
SBMNWSCMD と、Kerberos v5 および EIM の		
ファイル・レベルのバックアップのサポート	171	
	サーバー・ハードウェア間のホット・スペア	172

第 9 章 記憶域の管理 175

i5/OS の記憶域管理	175
統合 Windows サーバーのディスク・ドライブ	176
統合 Windows サーバーの事前定義ディスク・ド	
ライブ	179
i5/OS からの統合 Windows サーバー・ディスク・	
ドライブの管理	180
統合サーバーからの i5/OS 統合ファイル・シス	
テムへのアクセス	180
統合サーバー・ディスク・ドライブについての情	
報の取得	180
統合 Windows サーバーへのディスク・ドライブ	
の追加	181
統合サーバー・ディスク・ドライブの作成	181
ディスク・ドライブと統合サーバーのリンク	182
統合サーバー・ディスク・ドライブのフォー	
マット	183
ディスク・ドライブのコピー	184
ディスク・ドライブの拡張	184
システム・ドライブの拡張	185
統合 Windows サーバー・ディスク・ドライブの	
リンク解除	186
統合 Windows サーバー・ディスク・ドライブの	
削除	186
統合 Windows サーバーでの Windows ディスク管	
理プログラムの使用	187

第 10 章 装置の共用 189

iSeries 装置の装置記述とハードウェア・リソース名	
の確認	189
統合 Windows サーバーでの iSeries 光ディスク装	
置の使用	189
統合 Windows サーバーでの iSeries 磁気テープ・	
ドライブの使用	190
磁気テープ装置のドライバーのインストール	191
i5/OS での統合 Windows サーバー用のテープの	
フォーマット	191
統合 Windows サーバーに対する iSeries テー	
プ・ドライブの割り振り	192
統合 Windows サーバーから iSeries へのテー	
プ・ドライブの制御の返還	193
サポートされている iSeries 磁気テープ・ドライ	
ブ	193

アプリケーション用の iSeries 磁気テープ装置の 識別	194
統合 Windows サーバー間での iSeries テープ・ド ライブと光ディスク装置の制御権移動	194
統合 Windows サーバーから iSeries 印刷装置への 印刷	195

第 11 章 i5/OS からの統合 Windows サーバー・ユーザーの管理 197

iSeries ナビゲーターによる Windows 環境への単一 i5/OS ユーザーの登録	197
iSeries ナビゲーターによる Windows 環境への i5/OS グループの登録	198
文字ベースのインターフェースによる Windows 環 境への i5/OS ユーザーの登録	198
ユーザー・テンプレートの作成	199
テンプレートでのホーム・ディレクトリーの指定	200
LCLPDMGT ユーザー・プロファイル属性の変更	201
エンタープライズ識別マッピング (EIM)	201
Windows 環境に対するユーザーの登録の終了	203
Windows 環境に対するグループの登録の終了	204
QAS400NT ユーザー	204
統合 Windows サーバーへの登録と伝搬の禁止	206

第 12 章 統合 Windows サーバーのバ ックアップと回復 209

統合 Windows サーバーに関連付けられた NWSD およびその他のオブジェクトのバックアップ	209
統合 Windows サーバーの NWSD のバックアッ プ	210
iSCSI 接続の統合 Windows サーバーの NWSH のバックアップ	210
iSCSI NWSCFG および妥当性検査リストのバッ クアップ	210
統合 Windows サーバー用事前定義ディスク・ド ライブのバックアップ	211
統合 Windows サーバー用ユーザー定義ディス ク・ドライブのバックアップ	212
ユーザー登録情報の保管と復元	213
保管するオブジェクトと i5/OS でのその保管位 置	213
統合 Windows サーバーの個々のファイルおよびデ ィレクトリーのバックアップ	215
ファイル・レベルのバックアップの制約事項	215
予備的な管理者セットアップ・タスク	216
統合 Windows サーバーでの共有の作成	217
QAZLCSAVL ファイルへのメンバーの追加	217
iSeries NetServer と統合 Windows サーバーを 同じドメインに置く	218
ファイルの保管	218
例: 統合 Windows サーバーの各部分のアドレ スを指定する方法	219
Windows バックアップ・ユーティリティ	220
統合 Windows サーバーの NWSD およびディス ク・ドライブの復元	220

統合 Windows サーバー用事前定義ディスク・ド ライブの復元	221
統合 Windows サーバー用ユーザー定義ディス ク・ドライブの復元	222
統合 Windows サーバー NWSD の復元	222
iSCSI 接続サーバー用の統合 Windows サーバー NWSH の復元	223
iSCSI 接続サーバー用の統合 Windows サーバー NWSCFG の復元	223
統合 Windows サーバー・ファイルの回復	224

第 13 章 統合サーバー・ハードウェア から Windows サーバー・オペレーティ ング・システムをアンインストールする . 225

統合 Windows サーバーの NWSD の削除	225
統合 Windows サーバーの回線記述の削除	226
統合 Windows サーバーに関連した TCP/IP インタ ーフェースの削除	226
統合 Windows サーバーに関連した制御装置記述の 削除	227
統合 Windows サーバーに関連した装置記述の削除	227
iSCSI 統合 Windows サーバーに関連したネットワ ーク・サーバー構成の削除	227
IBM i5/OS 統合サーバー・サポート、i5/OS オプシ ョン 29 (5722-SS1) の削除	228

第 14 章 統合 Windows サーバーのト ラブルシューティング 229

メッセージ・ログとジョブ・ログのチェック	230
モニター・ジョブ	231
iSCSI 接続のサーバーの追加ログおよびメッセ ージ	232
統合 Windows サーバーの問題	232
STOP またはブルー・スクリーン・エラー	233
統合サーバーでのシステム・ドライブ空き容量不 足	234
光ディスク装置の問題	235
障害が起きたサーバーのロックされた光ディ スク装置	235
磁気テープ関連の問題	235
磁気テープ・ドライブの装置ドライバーがロ ードされていることの確認	236
統合 Windows サーバーの始動に関する問題	237
サーバー間のホット・スペアリングに関する問題	239
ホストされるシステム・ハードウェアの共用に関 する問題	240
ホストされる同じシステム・ハードウェアを 使用するよう定義された複数の NWSD	240
iSCSI 接続のシステムに関する特別な考慮事 項	240
NWSD 構成ファイルのエラー	242
NWSD 構成ファイルの修正	242
NWSD 構成ファイル・パラメーターのリセッ ト	242

以前のバージョンの統合サーバー・ファイルの使用	242	NWSD 構成ファイルの作成	276
IXA または iSCSI 接続のサーバーの DASD	243	例: NWSD 構成ファイル	277
ユーザーおよびグループの登録時の障害	243	CLEARCONFIG 項目タイプによる既存の統合サーバー・ファイルからの行の削除	277
ユーザー登録権限の問題	244	TARGETDIR キーワード	278
パスワードの問題	245	TARGETFILE キーワード	278
IBM iSeries 統合サーバー・サポート・スナップイン・プログラム	246	ADDCONFIG 項目タイプによる統合サーバー・ファイルの変更	278
iSCSI 接続のサーバーの問題	247	VAR キーワード	279
ブートおよび記憶域パス・ネットワークの分析	249	ADDSTR キーワード	279
パス証明書の管理	250	ADDWHEN キーワード	279
IBM Director のトラブルシューティング	250	ADDWHEN および DELETEWHEN 式演算子	280
ディスクバリエーションの問題	251	DELETEWHEN キーワード	280
SSL 接続の問題	252	LINECOMMENT キーワード	281
iSCSI 接続のサーバーの仮想イーサネットの問題	254	LOCATION キーワード	281
IXS および IXA 接続のサーバーの仮想イーサネットの問題	257	LINESEARCHPOS キーワード	281
回線記述およびアイコンの両方がある	258	LINESEARCHSTR キーワード	281
回線記述があり、アイコンがない	258	LINELOCATION キーワード	281
回線記述がなく、アイコンがある	259	FILESEARCHPOS キーワード (ADDCONFIG 項目タイプ)	281
回線記述およびアイコンの両方がない	259	FILESEARCHSTR キーワード	281
外部ネットワークに関する問題	260	FILESEARCHSTROCC キーワード	282
統合 Windows サーバーでの LAN ドライバーの手動アップデート	261	REPLACEOCC キーワード	282
LAN ドライバーのインストールまたは更新を開始する	261	TARGETDIR キーワード	282
インストールまたは更新したいアダプターを選択する	261	TARGETFILE キーワード	282
LAN ドライバーのインストールまたは更新を完了する	262	UNIQUE キーワード	283
Point-to-Point 仮想イーサネット IP アドレスの競合	263	VAROCC キーワード	283
Point-to-Point 仮想 IP アドレスの割り当て	265	VARVALUE キーワード	283
仮想イーサネット上の TCP/IP の問題	265	UPDATECONFIG 項目タイプによる統合 Windows サーバー・ファイルの変更	283
QNTC ファイル・システムによる Windows Server 2003 共用へのアクセス時の問題	266	FILESEARCHPOS キーワード (UPDATECONFIG 項目タイプ)	284
IFS アクセスの問題	267	FILESEARCHSTR キーワード (UPDATECONFIG 項目タイプ)	284
統合 Windows サーバー・ファイルの保管の問題	267	FILESEARCHSTROCC キーワード (UPDATECONFIG 項目タイプ)	284
サーバー・メッセージ待ち行列の判読不能メッセージ	268	SETDEFAULTS 項目タイプによる構成デフォルトの設定	284
Windows システム・メモリー・ダンプを取る際の問題	268	ADDWHEN	285
統合 Windows サーバーの再インストール	269	DELETEWHEN	285
統合 Windows サーバーのサービス・データの収集	270	FILESEARCHPOS キーワード (SETDEFAULTS 項目タイプ)	286
i5/OS での統合 Windows サーバーのメモリー・ダンプの作成	270	FILESEARCHSTR キーワード (SETDEFAULTS 項目タイプ)	286
i5/OS でのネットワーク・サーバー記述 (NWSD) ダンプ・ツールの使用	271	TARGETDIR	286
		TARGETFILE	286
		キーワード値に対する置換変数の使用	287
第 15 章 ネットワーク・サーバー記述構成ファイル	275	第 16 章 関連情報	289
NWSD 構成ファイル形式	275	付録. 特記事項	291
		商標	292
		使用条件	292

第 1 章 iSeries Windows 環境

iSeries Windows[®] 環境は、ハードウェアやソフトウェアの一部というより、むしろ 1 つのアイデアです。これは iSeries[™] サーバーとパーソナル・コンピュータ (PC) とを共存させるための手段であり、さらに、iSeries サーバーが PC を制御してその管理を容易にするための手段となります。

iSeries Windows 環境の最初の部分は、iSeries に追加する必要がある PC ハードウェアです。その基本的な方法としては、次の 3 つがあります。

- iSeries は、統合 xSeries[®] アダプター (IXA) を使用することにより、IBM[®] xSeries サーバーを制御します。IBM は PC xSeries サーバーの回線呼び出します。
 - iSeries サーバーは、Internet SCSI ホスト・バス・アダプター (iSCSI HBA) を使用することにより、イーサネットでの接続を行い、IBM xSeries サーバーまたは IBM BladeCenter[™] サーバーを制御することができます。
 - 統合 xSeries サーバー (IXS) は、ランダム・アクセス・メモリー (RAM) および Intel[™] プロセッサーを含む、iSeries 拡張カードです。これは、iSeries サーバー本体の内部に組み込まれた PC と考えることができます。
- 2 番目の部分は IBM i5/OS オプション 29 (5722-SS1) であり、これを iSeries サーバー上にインストールすることにより PC を制御する機能が iSeries に付与されます。それらの PC は統合 Windows サーバーと呼ばれます。

最後に、Microsoft の Windows 2000 Server または Windows Server 2003 ソフトウェアをインストールする必要があります。

この文書は、以下のセクションに分かれています。

3 ページの『第 2 章 V5R4 での新機能』

このリリースでの変更点および改善点。

5 ページの『第 3 章 印刷可能な PDF』

この文書の PDF を印刷します。

7 ページの『第 4 章 概念』

iSeries ソリューションにおける Windows 環境について理解します。

61 ページの『第 5 章 iSeries での Windows 環境のインストールと構成』

新しい統合 Windows サーバーを最初からインストールするには、この指示に従います。

123 ページの『第 6 章 仮想イーサネットおよび外部ネットワークの管理』

統合サーバーで利用可能な 3 つの異なるタイプのネットワークを使用する方法について学びます。

129 ページの『第 7 章 iSCSI 接続サーバーへの接続の管理』

iSeries を構成して、iSCSI を使用する xSeries または IBM BladeCenter サーバーへ接続します。

163 ページの『第 8 章 統合 Windows サーバーの管理』

サーバーの開始と停止、リモートでの統合サーバー・コマンドの実行、構成情報の表示と変更、およびメッセージとエラー・ログのモニターを実行します。

175 ページの『第 9 章 記憶域の管理』

統合サーバーのハード・ディスクに関する情報。

189 ページの『第 10 章 装置の共用』

統合サーバー上で、iSeries の装置を使用します。

197 ページの『第 11 章 i5/OS からの統合 Windows サーバー・ユーザーの管理』

i5/OS[®] ユーザーを Windows 環境に統合します。

209 ページの『第 12 章 統合 Windows サーバーのバックアップと回復』

このセクションでは、統合サーバー・ファイルを磁気テープ・ドライブまたは iSeries ハード・ディスクにバックアップする方法を説明します。

225 ページの『第 13 章 統合サーバー・ハードウェアから Windows サーバー・オペレーティング・システムをアンインストールする』

統合サーバー・ソフトウェアをシステムから除去する際に考慮すべきこと。

229 ページの『第 14 章 統合 Windows サーバーのトラブルシューティング』

よくある質問に対する答えが記載されています。

275 ページの『第 15 章 ネットワーク・サーバー記述構成ファイル』

独自の構成ファイルを作成すれば、統合サーバーをカスタマイズできます。



289 ページの『第 16 章 関連情報』

第 2 章 V5R4 での新機能

- V5R4 では、iSeries Windows 環境において、以下に示すいくつかの新機能があります。
- xSeries システムおよび IBM BladeCenter システムを iSCSI ホスト・バス・アダプター (iSCSI HBA) 経由で iSeries サーバーと統合する場合のサポートが提供されます。このサーバー統合テクノロジーは、既存の統合 xSeries サーバーのテクノロジーと xSeries アダプターのテクノロジーを補完するものです。ここでサポートするのは、iSCSI プロトコルと iSeries サーバーおよび xSeries サーバーの両方でサポートされるアダプターを使用する拡張が容易なギガビット・イーサネット・ネットワークで接続されたサーバーです。iSCSI テクノロジーを使用して IBM xSeries システムと BladeCenter システムを iSeries サーバーと統合する方法についての詳細は、7 ページの『第 4 章 概念』を参照してください。iSCSI 接続サーバーを管理し、構成する方法についての詳細は、129 ページの『第 7 章 iSCSI 接続サーバーへの接続の管理』および 163 ページの『第 8 章 統合 Windows サーバーの管理』を参照してください。
 - IBM iSeries Integration for Windows Server (5722-WSV) 製品は、i5/OS™ Integrated Server Support (5722-SS1 オプション 29) に再パッケージされました。
- 注: 以前のリリースから、i5/OS V5R4 にアップグレードする場合、製品 5722-WSV は自動的に除去され、製品 5722-SS1 オプション 29 がその場所にインストールされます。
- iSCSI 接続 Windows サーバーの記憶容量が増えました。最大 64 のディスク・ドライブ (ネットワーク・サーバーの記憶域) を iSCSI 接続の Windows サーバーに接続可能です。1 台のサーバーにつき 60 TB を超えるディスク装置が使用できます。
 - ディスク・ドライブのサイズ (ネットワーク・サーバーの記憶域) の拡張のサポートが追加されています。184 ページの『ディスク・ドライブの拡張』を参照してください。
 - Windows Server 2003 Volume Shadow Copy Service のサポートが追加されました。Windows で実行するバックアップ・アプリケーションで使用することができます。この機能を使用すると、Volume Shadow Copy Service をサポートするアプリケーションのデータを、アプリケーションを停止せずにバックアップできるようになりました。これにより、アプリケーションの可用性が向上します。209 ページの『第 12 章 統合 Windows サーバーのバックアップと回復』を参照してください。
 - iSCSI 接続サーバーの管理、統合 Linux® サーバーおよび統合 AIX® サーバーの管理、および統合サーバーの仮想イーサネットの・ポートの構成を含む iSeries ナビゲーター GUI サポートが追加されました。
 - 200 MHz および 333MHz の IBM 統合 PCサーバー AS/400®用 (IPCS) と IBM 統合 Netfinity® サーバー AS/400用 (INS) のサポートが取り下げられました。取り下げられた IPCS および INS ハードウェアのリソース・タイプは、6617 および 2850 で、フィーチャー・コードは 2854、2857、2865、2866、6617 および 6618 です。IPCS サーバーおよび INS サーバーのみがホスト LAN サポートを提供していた (i5/OS と Windows 間で LAN アダプターを共用している) 統合サーバー・タイプなので、ホスト LAN 機能も取り下げられます。
 - 本書に以前に記載されていた Windows NT® 4.0 サーバー (V5R3 以降サポートされていません)、IPCS ハードウェアまたは INS ハードウェア (タイプ 6617 および 2850)、共用ネットワーク・アダプター (ホスト LAN)、および V4R5 以前にインストールされたサーバーの考慮事項に関連する情報は、本書から削除されました。これらのトピックに関連した情報については、V5R3 iSeries Information Center の『iSeries Windows 環境』のトピックを参照してください。

新規または変更箇所を見分ける方法

技術変更が加えられた部分分かるように、以下の情報を使用しています。

-  マークは、新しい情報または変更された情報が開始する位置を示します。
-  マークは、新しい情報または変更された情報が終了する位置を示します。

このリリースでの新規箇所または変更箇所に関するその他の情報については、「プログラム資料説明書」を参照してください。

第 3 章 印刷可能な PDF

この文書の PDF 版をダウンロードして表示するには、iSeries Windows 環境 を選択します。


関連資料および Redbooks™ の PDF は、289 ページの『第 16 章 関連情報』から表示または印刷できます。

PDF ファイルの保存

表示用または印刷用の PDF ファイルをワークステーションに保存するには、次のようにします。

1. ブラウザーで PDF を右マウス・ボタン・クリックします (上記のリンクを右マウス・ボタン・クリックします)。
2. Internet Explorer を使用している場合、「対象をファイルに保存...」をクリックします。Netscape Communicator を使用している場合、「リンクを名前を付けて保存...」をクリックします。
3. PDF ファイルを保存するディレクトリーを指定します。
4. 「保存」をクリックします。

Adobe Reader のダウンロード

- | これらの PDF を表示または印刷するには、Adobe Reader がご使用のシステムにインストールされている
- | 必要があります。これは、Adobe Web サイト (www.adobe.com/products/acrobat/readstep.html)  から無償
- | でダウンロードできます。

第 4 章 概念

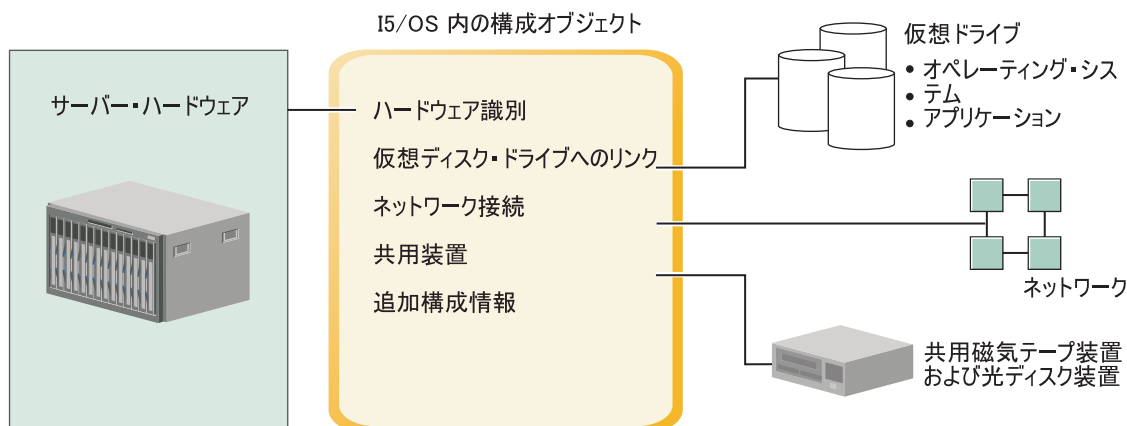
この資料において、統合 Windows サーバー または単に統合サーバー という用語は、統合 xSeries サーバー上、統合 xSeries アダプターによって iSeries に接続された xSeries サーバー上、または iSCSI ホスト・バス・アダプターによって iSeries サーバーに接続された xSeries または IBM BladeCenter サーバー上で実行される、Microsoft® Windows 2000 Server または Windows Server 2003 のインスタンスを指しています。PC という語が、Intel ベースのマイクロプロセッサおよび関連ハードウェア上で実行される Microsoft の Windows オペレーティング・システム・ソフトウェアを指してしばしば使用されるように、統合 Windows サーバーは、製品全体を構成するハードウェアおよびソフトウェアの組み合わせを指します。

概念に関する以下の情報を参照してください。

- 『統合サーバーの概要』
- 8 ページの『利点』
- 10 ページの『用語集』
- 14 ページの『ハードウェアの概念』
- 25 ページの『考慮事項』
- 26 ページの『パフォーマンス』
- 29 ページの『ネットワーキングの概念』
- 38 ページの『ソフトウェアの概念』
- 50 ページの『高可用性の概念』
- 51 ページの『セキュリティの概念』
- 54 ページの『ユーザーおよびグループの概念』

統合サーバーの概要

統合サーバーは、いくつかのハードウェアとソフトウェアを組み合わせることにより構成されます。



RZAHQ507-1

図 1. 統合サーバーの概要

サーバー・ハードウェアとは、統合サーバーが実行される物理的なハードウェア（プロセッサやメモリーなど）のことです。統合サーバーのために使用できるサーバー・ハードウェアには、必要に応じて、いくつかのタイプがあります。サーバー・ハードウェアは、iSeries サーバーに差し込まれたカードであることも、統合 xSeries アダプターを使用して iSeries サーバーに接続された外部 IBM xSeries サーバーであることも、または iSCSI ホスト・バス・アダプターを使用して iSeries サーバーに接続された外部 IBM xSeries または IBM BladeCenter サーバーである場合もあります。統合サーバーは、ホストする i5/OS パーティションに接続された磁気テープおよび光ディスク装置を使用することも可能です。統合サーバーのために使用できるハードウェアのタイプについて詳しくは、14 ページの『ハードウェアの概念』を参照してください。

それぞれの統合サーバーは、ネットワークへの接続を 1 つ以上持っています。ネットワーク・アダプターを使用した物理的ネットワーク接続と iSeries 仮想イーサネット・ネットワーク接続の両方がサポートされています。統合サーバーで使用できるネットワーク接続のタイプについて詳しくは、29 ページの『ネットワークングの概念』を参照してください。

それぞれの統合サーバーは、サーバーのオペレーティング・システム、アプリケーション、およびデータを保持する仮想ディスク・ドライブを使用します。これらの仮想ディスク・ドライブは、i5/OS ディスク記憶域から割り振られます。統合サーバーは、これらのドライブをサーバー内に含まれる物理ディスク・ドライブとして扱います。しかし、実際には、統合サーバーはそれ自体の物理ディスク・ドライブを持ちません。仮想ディスク・ドライブについて詳しくは、38 ページの『ソフトウェアの概念』を参照してください。

共用装置には、統合サーバーにとってローカルであるかのように統合サーバーがアクセスできる、サポートされるすべての磁気テープ装置と光ディスク装置が含まれます。デフォルトでは、すべての iSeries 磁気テープおよび光ディスク装置が自動的に統合サーバーからアクセス可能になります。これらの iSeries 装置のうち統合サーバーがアクセスできるものを制限することもできます。

i5/OS 内の構成オブジェクトは、各統合サーバーを記述します。i5/OS 構成オブジェクトは、統合サーバーが実行されるハードウェア、統合サーバーが使用する仮想ディスク・ドライブ、統合サーバーが使用する仮想イーサネット接続、およびサーバーの他の多くの属性を識別します。統合サーバーを記述する i5/OS 構成オブジェクトについて詳しくは、38 ページの『ソフトウェアの概念』を参照してください。

利点

iSeries Windows 環境は、Microsoft Windows を PC ベースのサーバー上で実行する際の機能のほとんどを提供し、他のコンピューター・システムと比較して以下の利点があります。

スペースの節約

- 管理するハードウェアの数が少なくなるので、必要な物理スペースも少なくなります。

データ・アクセス能力の増強とデータ保護

- 統合 Windows サーバーは、iSeries ディスク装置を使用します。一般的にこのほうが、PC サーバーのハード・ディスクよりも信頼性が高くなります。
- 統合サーバーのバックアップのために、より高速な iSeries 磁気テープ装置にアクセスできます。
- Windows サーバー全体を、iSeries サーバー・バックアップの一部としてバックアップすることができ、これにより、障害を起こしたサーバーのリカバリーを、Windows での通常のファイル・レベル・リカバリーに比べてはるかに速く簡単に行えます。
- 統合サーバーは、i5/OS に存在する RAID やドライブ・ミラーリングなどのより優れたデータ保護方式を暗黙のうちに利用します。

- 通常の統合サーバー構成では、記憶域スペース・データが、スタンドアロン (非統合) Windows サーバー・インストール済み環境の場合より多くの iSeries ディスク・ドライブに分散して存在します。多くの場合、これによってピーク・ディスク入出力能力が向上します。各サーバーが少数の専用ドライブに制限されないためです。
 - サーバーをシャットダウンしなくても、統合サーバーにディスク記憶域を追加できます。
 - iSeries Access を使用すれば、拡張 ODBC (Open Database Connectivity) を介して、DB2[®] UDB for iSeries データにアクセスできます。統合サーバーと i5/OS の間でサーバー間アプリケーションを使用するには、このデバイス・ドライバを使用します。
 - 統合サーバーを、3 層クライアント/サーバー・アプリケーションの第 2 層として使用することができます。
- 仮想ネットワーキングは追加の LAN ハードウェアを必要とせず、iSeries 論理区画、統合 xSeries サーバー (IXS)、統合 xSeries アダプター (IXA)、および iSCSI HBA 相互間の通信を提供します。

管理の簡素化

- パスワードなどのユーザー・パラメーターを i5/OS からさらに容易に管理できます。ユーザーとグループを作成し、それらを i5/OS から統合サーバーに登録できます。つまり、i5/OS からのパスワードや他のユーザー情報の更新がさらに簡単になりました。
- i5/OS 環境と Microsoft Windows 環境の間で、ユーザー管理機能、セキュリティー、サーバー管理、バックアップおよび回復計画が統合されるので、コンピューター・システムの複雑さが軽減されます。他の i5/OS データと同じメディアに統合サーバー・データを保管することができ、また i5/OS オブジェクトだけでなく個々のファイルを復元することができます。

リモート管理機能および問題分析

- リモート・ロケーションから i5/OS にサインオンして、統合サーバーをシャットダウンまたは再始動する機能があります。
- 統合サーバーのイベント・ログ情報を i5/OS にミラーリングできるので、Microsoft Windows のエラーをリモート分析できます。

統合 xSeries アダプター (IXA) または iSCSI HBA による xSeries サーバーとの接続

- フルサイズの xSeries を構成する際の柔軟性は、IXS やカード上の xSeries を構成する場合よりもかなり大きくなります。
- フルサイズの xSeries モデルはより頻繁にリリースされるので、最新の Intel プロセッサーなどのハードウェアを利用できます。
- フルサイズの xSeries サーバーでは、IXS よりも多くの PCI 機能カードを使用できます。

iSCSI ホスト・バス・アダプターによる IBM BladeCenterサーバーとの接続

- 高密度な IBM BladeCenter のパッケージ化
- IBM BladeCenter の新モデルは、IXS より頻繁にリリースされます。

複数のサーバー

- Microsoft クラスタ・サービスにより、複数のサーバーを接続してサーバー・クラスターにすることができます。サーバー・クラスターは、クラスター内で実行されるデータおよびプログラムの高可用性および管理の容易性を提供します。
- LAN ハードウェアを使用しないで同じ iSeries 上で実行するサーバーおよび論理区画は、高性能でセキュアな仮想ネットワーキング通信を実現します。

- 複数の統合サーバーを単一の iSeries 上で実行できます。これは便利で効果的だけでなく、ハードウェアに障害が生じた場合に稼働中の別のサーバーに簡単に切り替えることが可能になります。
- iSeries に複数の統合サーバーをインストールすると、簡単にユーザー登録およびアクセスできるように Windows ドメイン役割を定義できます。たとえば、これらのサーバーの 1 つをドメイン・コントローラーとしてセットアップできます。そのようにすれば、ユーザーをドメイン・コントローラーに登録するだけで、ユーザーは任意の Microsoft Windows マシンからそのドメインにログオンできます。
- iSeries 上で実行される複数の統合サーバーは、iSeries サーバーの光ディスク・ドライブおよび磁気テープ・ドライブを共用できます。

ホット・スペアのサポート

- サーバー統合と記憶域仮想化は、Windows サーバー環境の信頼性と復元可能性を向上させる革新的なオプションを提供します。
- Windows サーバー・ハードウェアに障害が発生した場合、そのサーバーの構成を他のホット・スペア xSeries サーバーか IBM BladeCenter サーバーに、iSeriesサーバーを再始動しなくても迅速かつ簡単に切り替えることができます。これは、より高い可用性を提供するのに必要な PC サーバーの全体数の削減につながる場合があります。
- ホット・スペアのサポートにより、1 台のスペア・サーバーを使用して複数の実動サーバーを保護できるので、柔軟性が増し加わります。

用語集

以下の用語は、iSeries Windows 環境に関連したものです。その他の iSeries 用語および定義については、「Information Center 用語集」を参照してください。

- **ベースボード管理コントローラー (BMC)**. xSeries システムを制御するのに使用される基本低機能サービス・プロセッサ。
- **証明書**. ID を公開鍵と結びつけ、認証局による署名を付す標準形式。指定された開始日時から指定された終了日時まで有効です。証明書内の ID (証明書の「サブジェクト」とも呼ばれる) には、この証明書が発行されている対象が示されます。構文にはさまざまなものがありますが、通常は "CN=common name, O=organization, OU=organizational unit" のような属性付き識別名が含まれます。公開鍵は、秘密鍵/公開鍵ペアの一部で、通常は RSA 公開鍵暗号方式で使用するために作成されるものです。これに対して、対応する秘密鍵は証明書の一部ではなく、表示することは意図されていません。
- **認証局**. 証明書が本当に発行元からのものかどうかを判断するなど、認証目的で他の証明書に署名できる秘密鍵/公開鍵ペア。認証局は、識別情報を検査し署名付きデジタル証明書を発行する第三者機関が所有する場合もあれば、ローカルで私用である場合もあります。証明書はいったんデジタル署名されると、検出されずに変更することができなくなります。
- **チャレンジ・ハンドシェイク認証プロトコル (CHAP)**. 認証元と認証されるものの両者に既知の機密事項を扱う認証プロトコル。機密事項は、伝送中の盗聴から保護されます。
- **接続セキュリティ・ネットワーク・サーバー構成**. iSCSI HBA SCSI および仮想イーサネット LAN のデータをネットワーク上で保護する方法を制御するセキュリティ関連の値を構成するために使用する i5/OS 構成オブジェクト。対応する i5/OS オブジェクト・タイプは、サブタイプ *CNNSEC を持つ *NWSCFG です。このオブジェクトは、短く**接続セキュリティ構成**という用語で呼ばれることもあります。
- **格納装置 ID**. サービス・プロセッサを収容している格納装置の識別用シリアル番号、タイプ、およびモデル。標準の xSeries サーバーの場合、サービス・プロセッサと xSeries サーバーは共通の格納装置 ID を使用します。IBM BladeCenter サーバーの場合、これは制御する IBM BladeCenter サーバーを含む管理モジュールを識別します。

エンタープライズ識別マッピング (EIM). 人またはエンティティをマッピング/関連付けして、複数のオペレーティング・システム上にあるさまざまなレジストリー内のユーザー ID を訂正するメカニズム。ユーザー管理機能は、EIM Windows ソース関連の自動作成をサポートすることにより、ユーザー登録を EIM に統合します。さらに、管理者が EIM Windows ソース関連を手動で定義する場合には、登録する i5/OS ユーザー・プロファイルでは、Windows ユーザー・プロファイルを i5/OS ユーザー・プロファイルとは異なるものにすることができます。

EIM ID. EIM 内で実際の人またはエンティティを表します。EIM ID を作成すると、それはその人のユーザー ID と関連付けられます。

EIM ID マッピング関連. レジストリー内でユーザー ID を EIM ID と関連付けることにより、単一のサインオン環境が可能になります。関連には、ソース、ターゲット、および管理の 3 つのタイプがあります。ターゲット i5/OS 関連とソース Windows 関連とが定義されると、ユーザー登録に EIM と統合されます。関連は、ユーザー・プロファイル属性 EIMASSOC を使用して自動的に、または iSeries ナビゲーターを使用して手動で定義されます。ターゲット関連は、主に既存のデータを保護するために使用されます。ソース関連は、主に認証目的で使用されます。

| **外部ネットワーク.** 物理ネットワーク・ハードウェアを経由し、統合サーバーがアクセスするネットワーク。**仮想ネットワーク**も参照してください。

| **ホスト・バス・アダプター (HBA).** ホスト・バス・アダプター (HBA) とは、ホスト・システムのバスに接続するアダプター・カードです。たとえば、イーサネット・アダプターや iSCSI アダプターなどです。

| **ホット・スペア.** ホット・スペアにより、1 つ以上のサーバーで使用される、サーバー・ハードウェアのバックアップ専用のスペア・サーバー・ハードウェア (アイドル IXS など) を持つことが可能になります。アクティブ・サーバーの 1 つにサーバー・ハードウェア障害が発生した場合、そのサーバーはすぐに障害が発生したサーバー・ハードウェアからスペア・サーバー・ハードウェアに切り替えられ、再始動されます。これにより、サーバー・ハードウェアの障害に関連したサーバー・ダウン時間は大幅に短縮されます。詳しくは、172 ページの『サーバー・ハードウェア間のホット・スペア』を参照してください。

| **IBM Director.** リモート xSeries および IBM BladeCenter のディスカバリー、電源制御、および管理を提供するアプリケーション。IBM Director は、Virtualization Engine™ Standard Edition を通じて入手することができます。iSeries iSCSI 接続サーバーの場合、これは単に iSCSI 接続サーバーをホストする i5/OS 区画上で実行される IBM Director のホスト部分のことです。

IBM i5/OS 統合サーバー・サポート. iSeries にインストールされた i5/OS オペレーティング・システムを拡張したものの。統合 Windows および Linux サーバーと共に機能することを可能にします。統合サーバー上で実行される製品のコンポーネントもあります。

統合 Windows サーバー. 「統合サーバー」とも呼ばれるもの。IXS または IXA 接続の xSeries サーバー上、あるいは iSCSI HBA 接続の xSeries または IBM BladeCenter サーバー上で実行される Windows 2000 Server または Windows Server 2003 のインスタンス。

統合 xSeries サーバー (IXS). iSeries サーバーの内部に取り付ける PCI 拡張カード上の PC (Intel ベースのコンピューター)。

統合 xSeries アダプター (IXA). iSeries サーバーへの高速リンクを提供するために、IBM eServer™ xSeries サーバーのうちの特定のモデルの内部に取り付ける PCI 拡張カード。

| **Internet Protocol Security (IPSec).** iSCSI ネットワーク上のトラフィックを暗号化します。

| **IP マルチキャスト.** 単一のマルチキャスト・グループを構成するシステムのセットに対するインターネット・プロトコル (IP)・データグラムの伝送。

| **IPSec.** 「Internet Protocol Security」を参照。

| **IQN.** 「iSCSI 修飾名」を参照。

l **iSCSI**. Internet SCSI. TCP/IP パケット内の SCSI プロトコルのカプセル化。既存のインターネット・インフラストラクチャー、インターネット管理機能、およびアドレス距離制限を利用できる相互運用可能なソリューションを提供します。

l **iSCSI 接続**. 接続は TCP 接続です。イニシエーターとターゲットの間のコミュニケーションは、1 つ以上の TCP 接続上で行われます。

l **iSCSI イニシエーター・アダプター**. iSCSI 要求を開始するホスト・バス・アダプター (HBA)。iSCSI イニシエーターは、ターゲットであるサーバーのコンポーネントや論理装置からのサービスを要求する SCSI コマンドを発行します。iSCSI イニシエーターは、xSeries または BladeCenter サーバーの iSCSI HBA です。

l **iSCSI 修飾名 (IQN)**. iSCSI 規格 (RFC 3722)によって定義される iSCSI ターゲット・アダプターまたは iSCSI イニシエーター・アダプターを識別する固有の名前。

l **iSCSI ターゲット・アダプター**. iSCSI イニシエーター要求に対してサービスを提供するホスト・バス・アダプター (HBA)。iSCSI ターゲットは記憶域コントローラーとして機能し、論理装置 (LUN) をホストします。iSeries iSCSI 接続サーバーの場合、iSCSI ターゲットは iSeries の iSCSI HBA です。

Kerberos. MIT が作成したネットワーク・セキュリティ・プロトコル。企業全体の情報システムをセキュアにするために役立つ、ネットワークの認証および強力な暗号化ツールを提供します。iSeries ナビゲーターには、Kerberos 認証のサインオンが備わっています。ユーザー管理では、i5/OS ユーザー・プロファイル・パスワードを *NONE に定義したり、登録された Windows ユーザーがパスワードを Windows 内で設定したりできるようになっています。それにより単一のサインオン環境がサポートされます。このサポートは、登録されたユーザー・プロファイル属性が LCLPWDMGT(*NO) に指定されている場合に提供されます。

l **ローカル・インターフェース**. ローカル・インターフェースは、iSeries サーバーにある iSCSI ターゲット・アダプターを記述する構成パラメーターを表します。

l **MAC**. 「メディア・アクセス制御」を参照。

l **管理モジュール**. IBM BladeCenter シャーシおよびその中の個々のサーバーを制御するのに使用される高機能サービス・プロセッサ。

l **メディア・アクセス制御 (MAC)**. ローカル・エリア・ネットワークにおいて、ある時点でどの装置が伝送メディアにアクセスできるかを決定するプロトコル。

Microsoft Windows クラスタ・サービス (MSCS). 複数のサーバーをリンクして共通のタスクを実行可能にするための、Microsoft Windows のサービス。

l **ネットワーク・サーバー構成 (NWSCFG)**. iSCSI 接続のリモート統合サーバーで使用される属性を記述する、i5/OS 構成オブジェクト。属性には、リモート・システム (*RMTSYS)、リモート・システム上のサービス・プロセッサ (*SRVPRC)、あるいはサーバーとの通信に使用する構成セキュリティ値 (*CNNSEC) が含まれます。対応する i5/OS オブジェクト・タイプは *NWSCFG です。

ネットワーク・サーバー記述 (NWS D). 統合サーバーを記述する i5/OS 構成オブジェクト。対応する i5/OS オブジェクト・タイプは *NWS D です。

l **ネットワーク・サーバー・ホスト・アダプター (NWSH)**. ネットワーク・サーバー・ホスト・アダプター(NWSH) とは、iSeries サーバーの iSCSI HBA 装置を構成するのに使用する i5/OS 構成オブジェクトです。対応する i5/OS 装置タイプは *NWSH です。

ネットワーク・サーバー記憶域スペース (NWSSTG). 統合サーバーに割り振られた i5/OS ディスク記憶域。

l **NWSH**. 「ネットワーク・サーバー・ホスト・アダプター (NWSH)」を参照。

Point-to-Point 仮想イーサネット. インストール中に、iSeries と統合 Windows サーバーとの間に構成される仮想イーサネット・ネットワーク。これは、iSeries と統合サーバーとの間の通信に使用されるリンクです。

リモート・インターフェース。リモート・インターフェースは、xSeries サーバーまたは IBM BladeCenter サーバーにある iSCSI イニシエーター・アダプターを記述する構成パラメーターを表します。リモート・インターフェースには、アダプターの SCSI 機能と LAN 機能の両方が含まれます。

リモート・システム ID。xSeries サーバーまたは IBM BladeCenter サーバーの識別シリアル番号、タイプ、およびモデル。標準の xSeries サーバーの場合、サービス・プロセッサと xSeries サーバーは共通の ID を使用します。IBM BladeCenter サーバーの場合、これはシャーシ内のサーバーを識別します。

リモート・システム・ネットワーク・サーバー構成。特定のリモート xSeries または IBM BladeCenter サーバーに固有の属性を構成するために使用する i5/OS 構成オブジェクト。このオブジェクトには、リモート・システムを識別してブートするのに必要な情報と、リモート・システムが使用する iSCSI イニシエーター・アダプターに関する情報が含まれます。対応する i5/OS オブジェクト・タイプは、サブタイプ *RMTSYS を持つ *NWSCFG です。このオブジェクトは、短くリモート・システム構成という用語で呼ばれることもあります。

リモート監視プログラム・アダプター (RSA)。xSeries システムを制御するのに使用される高機能サービス・プロセッサ。

サービス・プロセッサ。システムのメイン CPU とは別のプロセッサ。サービス・プロセッサは、システムの電源を制御し、他の管理や診断機能を実行するために使用されます。統合 xSeries および IBM BladeCenter システムで使われるサービス・プロセッサには、いくつかのタイプがあります。リモート監視プログラム・アダプター (RSA)、ベースボード管理コントローラー (BMC)、および管理モジュールを参照してください。

サービス・プロセッサ・ネットワーク・サーバー構成。リモート・システム上のサービス・プロセッサに関連したパラメーターのセットを保持する i5/OS 構成オブジェクト。IBM BladeCenter サーバーの場合、これは IBM BladeCenter 格納装置を表します。対応する i5/OS オブジェクト・タイプは、サブタイプ SRVPRC を持つ *NWSCFG です。このオブジェクトは、短くサービス・プロセッサ構成という用語で呼ばれることもあります。

記憶域パス。記憶域パスは、記憶域スペースが使用できるネットワーク・サーバー・ホスト・アダプター (NWSH) と、データ・トラフィックを保護するのに使用する IP セキュリティ規則を定義します。

ターゲット・ノード。iSCSI セッションおよび接続を管理する iSeries iSCSI ファームウェア・オブジェクト。

ユニキャスト。単一の宛先へのデータの伝送。

仮想ネットワーク。i5/OS 論理区画、Linux 論理区画、および統合 Windows サーバーの相互間のネットワークを作成できるようにするために iSeries 内部でエミュレートされるイーサネット・ネットワーク。

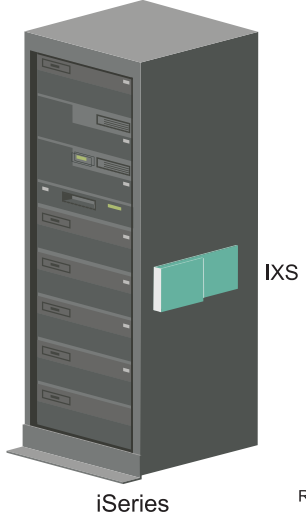
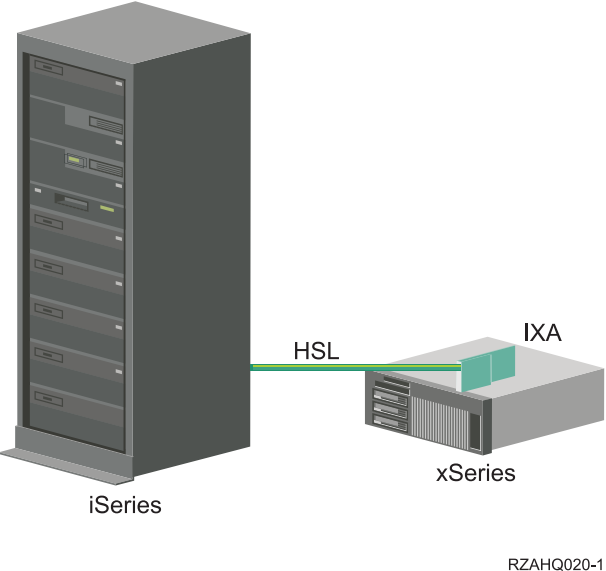
Windows サーバー。Microsoft Windows 2000 Server または Windows Server 2003

Windows Server 2003 Volume Shadow Copy Service。アプリケーションを終了せずにアプリケーション・データをバックアップできるようにするためのサポート。このサービスは、アプリケーションの可用性を向上させます。

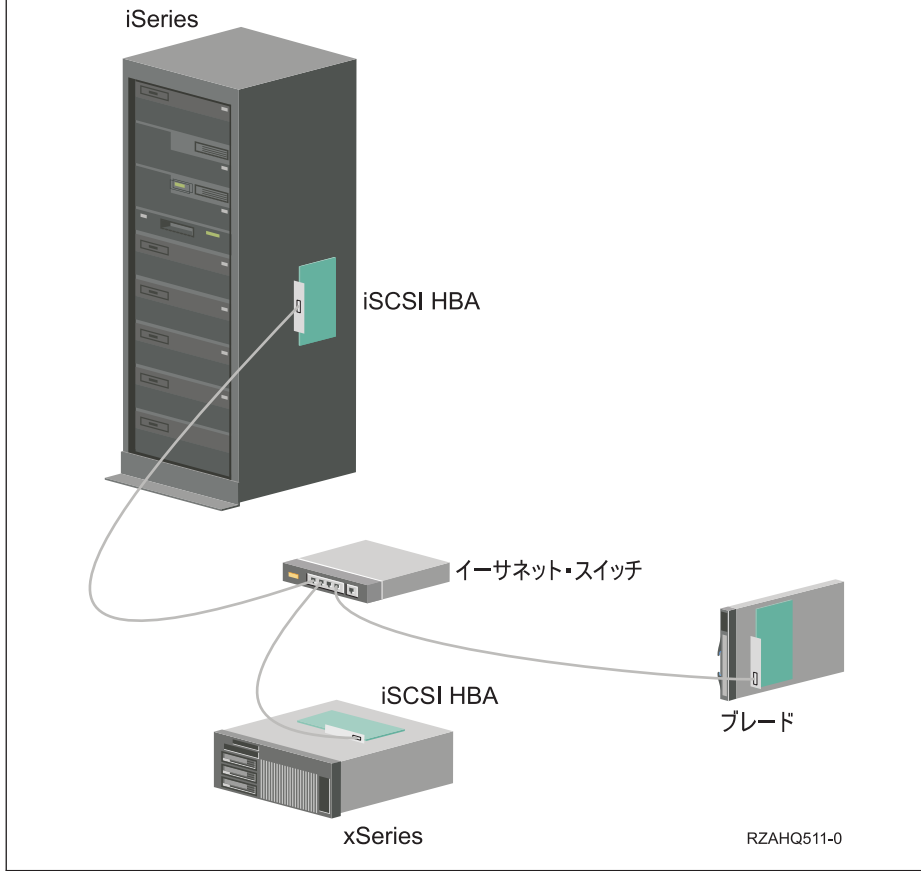
ハードウェアの概念

iSeries サーバーは、IBM xSeries サーバーや BladeCenter サーバーを統合するために、いくつかのハードウェア構成をサポートしています。次の表は、統合 xSeries サーバー (IXS)、統合 xSeries アダプター (IXA) 接続 xSeries サーバー、および iSCSI 接続サーバーの間の本質的な違いを説明しています。

IXS、IXA、および iSCSI HBA 接続の各 xSeries サーバーの比較。

	<p>IXS は、プロセッサとメモリーを持ち、iSeries サーバーの内部にインストールされるディスクレス PC サーバーです。</p>
	<p>IXA は、サポートされる xSeries サーバー内に取り付けられる高速リンク (HSL) バス・アダプターです。iSeries サーバーにとって xSeries サーバーは、HSL で接続された拡張装置に見えます。</p>

IXS、IXA、および iSCSI HBA 接続の各 xSeries サーバーの比較。

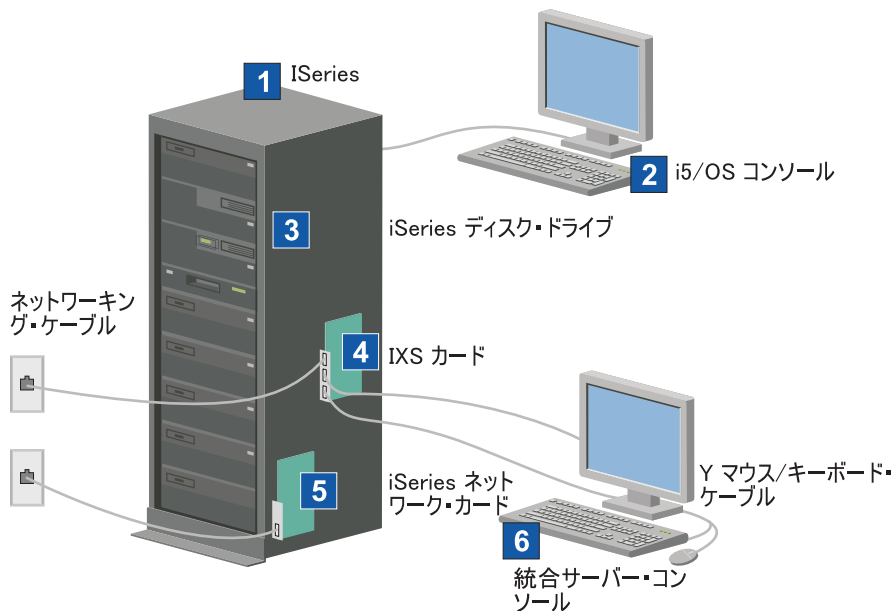


iSCSI テクノロジーが、ディスクレス xSeries サーバーと IBM BladeCenter サーバーの両方を、低価格で拡張が容易なイーサネット・ネットワークを使用して iSeries システムに接続します。iSeries サーバー、関係する各 xSeries サーバー、および関係する各 IBM BladeCenter サーバーに iSCSI ホスト・バス・アダプター (HBA) があります。

IXS および IXA 接続サーバー

1 典型的な IXS サーバー・システム

1 以下の図は、典型的な IXS システムを示しています。



RZAHQ025-0

図 2. 典型的な IXS システム

1. 互換性のある iSeries サーバーが必要です。(互換性については、62 ページの『ハードウェア要件』を参照。)
2. i5/OS コンソールが示されています。そこから iSeries ナビゲーターまたは文字ベースのインターフェースを使用して iSeries サーバーに接続することになります。これは、統合サーバー・コンソールとは違うものです。
3. 統合サーバーに専用のハード・ディスク・ドライブはありません。iSeries ハード・ディスク・ドライブの一部を使用するため、i5/OS がハード・ディスク・スペースをエミュレートします。
4. IXS カードは、独自の RAM を含む Intel プロセッサを PCI ボードに取り付けたものであり、それを iSeries 拡張スロットに差し込みます。IXS は、物理的に 2 つのスロットを使用します。
5. 通常、iSeries サーバーには、ネットワーク・カードが装着されています。
6. 統合サーバー・コンソールを使用して、統合サーバーと対話することができます。統合サーバー・コンソールは通常、IXS カードに直接接続されたモニター、キーボード、およびマウスから構成されます。これについて、また他のタイプの統合サーバー・コンソールについて詳しくは、24 ページの『Windows コンソール』を参照してください。

注: IXS タイプによってはネットワークへの別の接続方法もあります。IXS のタイプの中には、iSeries ネットワーク・カードの制御を可能にするために、隣接した PCI スロットを「占有」するものがあります(サポートされるネットワーク・カードについては、62 ページの『ハードウェア要件』のセクションで説明します)。この方法で 3 つまでネットワーク・カードを取り付けることができます。さらに、ネットワーク・コントローラーを内蔵し、隣接したスロットのネットワーク・カードをサポートしない IXS のタイプもあります。

1 典型的な IXA 接続サーバー・システム

IXA 接続の統合サーバーは、プロセッサ、メモリー、および拡張カードを含む標準の xSeries サーバー・モデルですが、ディスクは含まれていません。すべてのディスク・スペースは iSeries サーバー内にあり、IXS モデルの場合と同じ方法で管理されます。

IXA 接続の統合 Windows サーバーのインストール手順は、IXS 統合サーバーのインストール手順とほとんど同じです。それらの間の主な違いは、新しい xSeries サーバーは IXS よりも頻繁にリリースされるため、更新された機能がより迅速に使用可能になることです。さらに、IXA 接続の xSeries サーバーには独自の拡張スロットがあるので、IXS に比べてはるかに拡張性が高くなっています。

1 以下の図は、典型的な IXA 接続サーバー・システムを示しています。

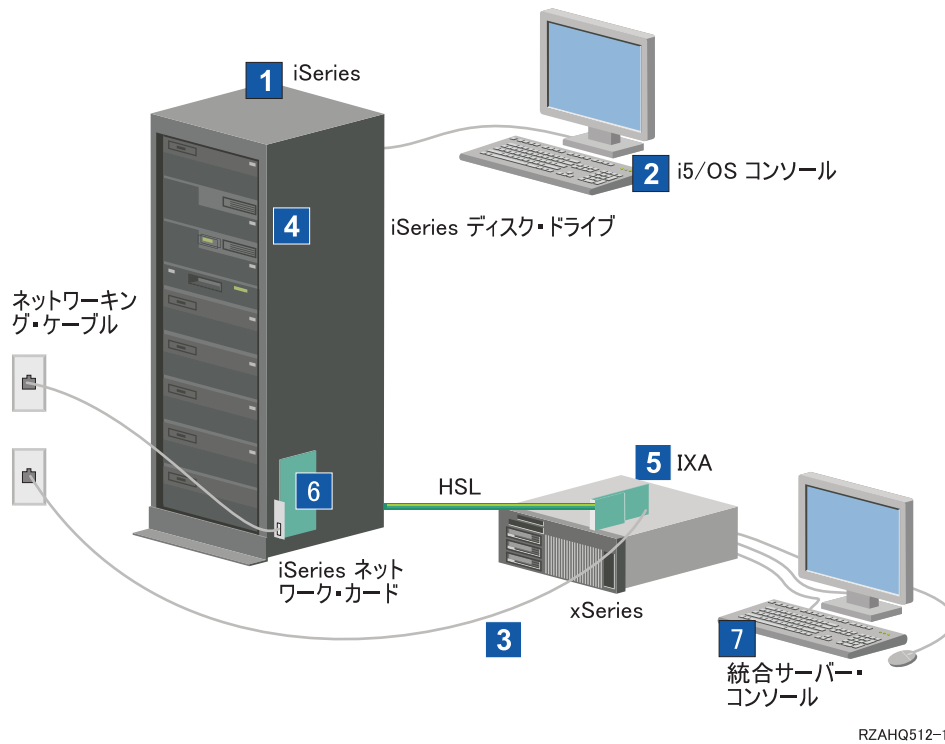


図 3. 典型的な IXA 接続サーバー・システム

1. 互換性のある iSeries サーバーが必要です。(互換性については、62 ページの『ハードウェア要件』を参照。)
2. i5/OS コンソールが示されています。そこから iSeries ナビゲーターまたは文字ベースのインターフェースを使用して iSeries に接続することになります。これは、Windows コンソールとは違うものです。
3. 典型的な xSeries サーバーには、少なくとも 1 つの統合ネットワーク・コントローラーがあります。ほとんどの xSeries サーバーには、ネットワーク接続を拡張するために追加のネットワーク・カードを付加することが可能です。xSeries ネットワーク・カードの互換性に関する情報は、統合 xSeries ソリューション (英語) という Web サイトにあります。
4. IXA 接続 xSeries サーバーには、専用のハード・ディスク・ドライブはありません。iSeries ハード・ディスク・ドライブの一部を使用するため、i5/OS がハード・ディスク・スペースをエミュレートします。
5. IXA カードは、xSeries サーバーの特定のスロットに差し込まれ、HSL ケーブルで iSeries に接続されます。
6. 通常、iSeries サーバーには、ネットワーク・カードが装着されています。

- | 7. 統合サーバー・コンソールを使用して、IXA 接続 xSeries と対話することができます。統合サーバー・コンソールは通常、xSeries サーバーに直接接続されたモニター、キーボード、およびマウスから構成されます。これについて、また他のタイプの統合サーバー・コンソールについて詳しくは、24 ページの『Windows コンソール』を参照してください。

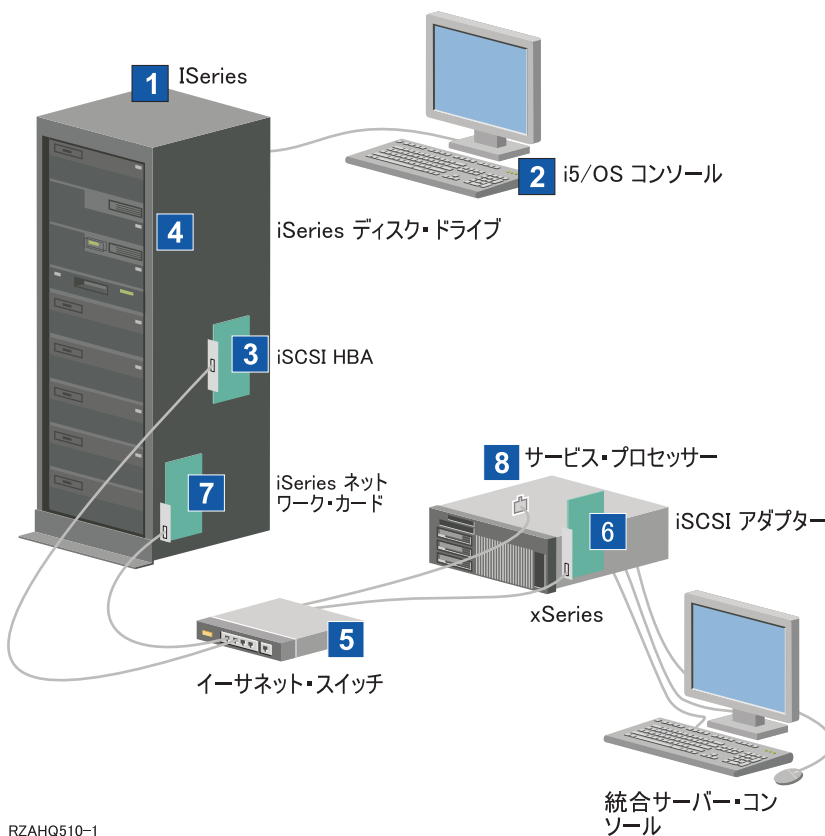
| iSCSI 接続サーバー

| 典型的な iSCSI 接続の IBM xSeries または BladeCenter サーバー・システム

- | iSCSI 接続のサーバーは、プロセッサ、メモリー、および拡張カードを持つ標準の xSeries または IBM BladeCenter サーバー・モデルですが、ディスクはありません。すべてのディスク・スペースは iSeries サーバー内にあり、IXS モデルや IXA モデルの場合と同じ方法で管理されます。

- | iSCSI 接続の統合 Windows サーバーのインストール手順では、iSeries と xSeries または IBM BladeCenter サーバーにハードウェアがインストールされて構成されていることが必要です。IXA の場合と同様、iSCSI HBA 接続の xSeries サーバーには独自の拡張スロットがあり、追加のオプションをインストールしてサーバーの機能を拡張することができます。

- | 以下の図は、典型的な iSCSI HBA システムを示しています。




RZAHQ510-1

| 図 4. 典型的な iSCSI 接続サーバーまたは IBM BladeCenter システム

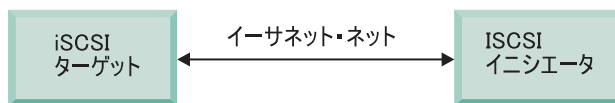
- | 1. 互換性のある iSeries が必要です。互換性については、62 ページの『ハードウェア要件』を参照してください。
- | 2. i5/OS コンソールが示されています。そこから iSeries ナビゲーターまたは文字ベースのインターフェースを使用して iSeries に接続することになります。これは、Windows コンソールとは違うものです。

- 3. 物理的ネットワークのタイプに応じて、銅線またはファイバーの iSCSI HBA が使用可能です。この iSCSI アダプターはターゲット装置として機能し、標準イーサネット・ケーブルを使用してイーサネット・ネットワークに接続します。
- 4. 統合サーバーに専用のハード・ディスク・ドライブはありません。iSeries ハード・ディスク・ドライブの一部を使用するため、i5/OS がハード・ディスク・スペースをエミュレートします。これらのドライブや他の iSeries 記憶装置には、iSCSI HBA 経由でアクセスします。
- 5. iSCSI HBA ネットワーク・ケーブルは、標準のギガビット・イーサネット・スイッチに接続されます。
- 6. xSeries サーバーには、追加の iSCSI HBA が必要です。このアダプターは、iSeries に iSCSI HBA への接続を提供します。このアダプターは、xSeries サーバーからは記憶域アダプターとみなすことができ、ネットワーク経由でディスクを見ることができます。
- 7. 通常、iSeries サーバーには、ネットワーク・カードが装着されています。IBM Director は、リモートの xSeries または IBM BladeCenter サーバーを発見して管理するために、iSeries LAN 接続を必要とします。
- 8. サービス・プロセッサは、iSeries サーバーがリモート・システムを発見して管理できるようにします。このサービス・プロセッサは、リモート監視プログラム・アダプター (RSA II) の場合もあり、ベースボード管理コントローラー (BMC) や IBM BladeCenter の管理モジュールの場合もあります。RSA II、BMC、または管理モジュールは、イーサネット・ネットワークを経由して iSeries サーバーに接続します。

その他のハードウェア情報については、IBM iSeries 統合 xSeries ソリューション  Web サイト (英語) (www.ibm.com/servers/eserver/series/integratedxseries) を参照してください。

iSCSI 接続サーバーの概要

基本的な iSCSI ネットワークは、iSCSI ターゲット (iSeries サーバーにインストールされた iSCSI HBA) と iSCSI イニシエーター (xSeries または IBM BladeCenter サーバーにインストールされた iSCSI HBA) で構成されます。これらのターゲット装置とイニシエーター装置は、イーサネット・ローカル・エリア・ネットワーク (LAN) 経由で接続されます。iSeries 用 iSCSI HBA は、iSCSI イニシエーターの記憶域および取り外し可能メディア装置を提供します。図 5 は、基本的な iSCSI ネットワークを示しています。



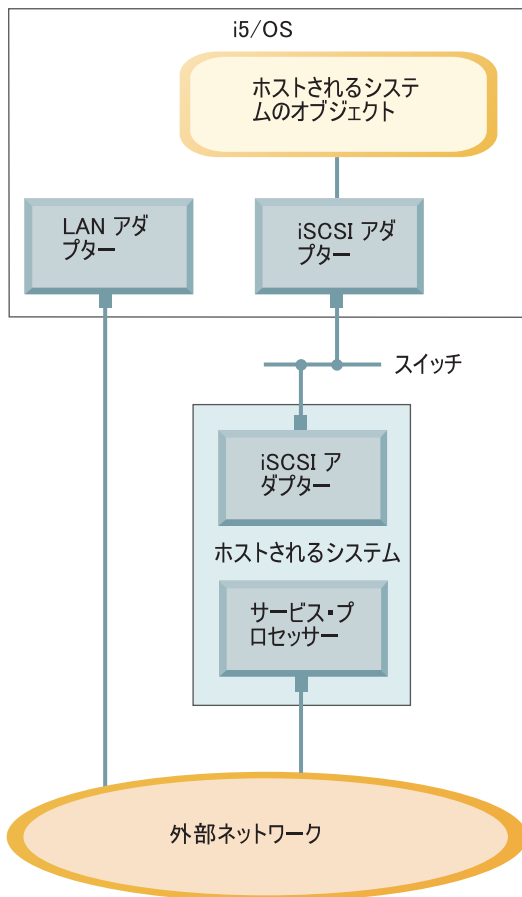
RZAHQ509-0

図 5. 基本的な iSCSI の概念

iSCSI ターゲットとイニシエーターは、両方とも iSeries サーバー上で発行するコマンドを使用して構成しなければなりません。iSCSI ネットワークは iSCSI HBA トラフィックのためだけに使用されます。

基本的な単一サーバー・サポート

xSeries または IBM BladeCenter サーバーを iSCSI 経由で iSeries に接続またはホストするには、iSeries とホストされるシステムの両方にハードウェアをインストールしなければなりません。両端に必要なハードウェアは、iSCSI ホスト・バス・アダプター (HBA) または iSCSI アダプターです。これらの 2 つのアダプターは、標準のイーサネット・ケーブルを使用して、イーサネット・スイッチ経由で接続されます。ホストされるシステムと iSeries サーバーの物理接続の最も単純な形を、20 ページの図 6 に示します。



RZAHQ501-1

図 6. 単一 iSCSI 接続サーバー

ホストされるシステムである xSeries または IBM BladeCenter サーバーには、イニシエーター iSCSI HBA がインストールされます。このアダプターは、イーサネット・ネットワーク・インターフェースを持ち、イーサネット・スイッチを介して、iSeries サーバーにインストールされているターゲット iSCSI HBA に接続されます。ホストされるシステムはディスクレス・サーバーです。仮想ディスクおよび仮想取り外し可能メディア装置は、iSeries 用 iSCSI HBA によってホストまたは提供されます。これらの装置にアクセスするための SCSI コマンドは TCP/IP フレームにパッケージされ、イーサネット・ネットワークを通じて、ホストされるシステムから iSeries 用 iSCSI HBA に送られます。この通信のモードを Internet SCSI、または iSCSI と呼びます。

iSCSI 接続サーバーは、i5/OS オブジェクト内で構成されます。これらのオブジェクトについて詳しくは、38 ページの『ソフトウェアの概念』を参照してください。

i5/OS は、イーサネット・ネットワークを介してリモート・システムのサービス・プロセッサにコマンドを送信して、リモート・システムの検出と管理を行うことができます。これらの機能のために、IBM Director が使用されるので、iSCSI 接続ホスト・バス・アダプター (HBA) に接続されたすべての区画にそれがインストールおよび実行されていなければなりません。詳しくは、154 ページの『リモート・サーバーのディスカバリーおよび管理』を参照してください。

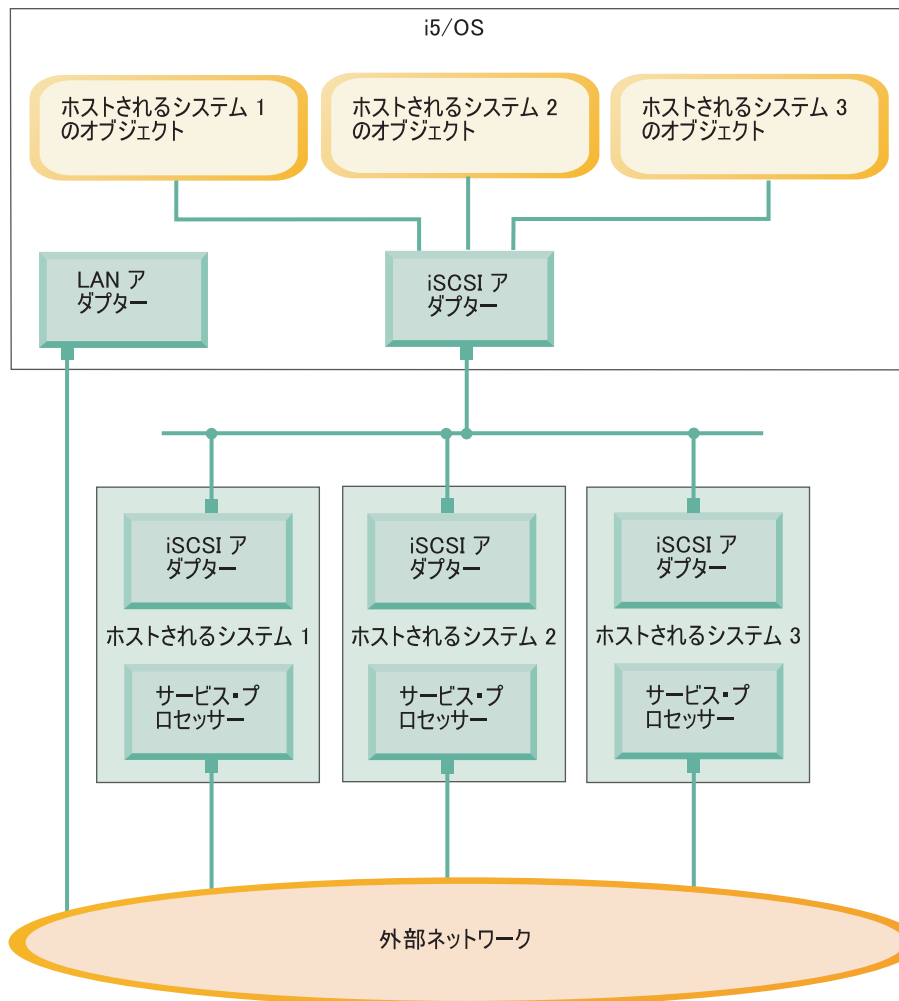
図 6 には、2 つの異なるネットワークが示されています。iSCSI ネットワークは、専用のスイッチを使用しています。サービス・プロセッサの接続は、外部ネットワーク (共用ネットワーク) を使用しています。2 つの別個のネットワークが必ず存在する必要はありません。たとえば、サービス・プロセッサの

| 接続に iSCSI ネットワークと同じ専用スイッチを使用することもできます。これは、サービス・プロセッ
| サー接続を保護する 1 つの方法です。しかし、外部ネットワーク上の他のアプリケーションで i5/OS LAN
| アダプターを使用することができなくなります。

| 両方のタイプのネットワークは保護される必要があります。iSCSI 接続サーバーのセキュリティーについ
| て詳しくは、51 ページの『セキュリティーの概念』を参照してください。

| 複数サーバー・サポート

| 単一の iSeries 用 iSCSI HBA で、複数の xSeries または IBM BladeCenter サーバーをホストすることが
| できます。図 7 は、この概念を示しています。



RZAHQ502-3

| 図 7. 複数の iSCSI 接続サーバー

| ホストされるシステムごとに、サーバーに少なくとも 1 つの iSCSI HBA がインストールされていること
| が必要です。ホストされるシステムの iSCSI HBA はそれぞれ、イーサネット・ネットワークを通じて
| iSeries 用 iSCSI HBA に接続されます。物理的にセキュアなモデルを実装する場合、このネットワークは
| 物理的にセキュアな、つまり分離されたネットワークにすることが可能です。i5/OS では、ホストされる
| システムとリモート・システムはそれぞれ、オブジェクトのセットで表されます。これらのオブジェクトに
| ついては、38 ページの『ソフトウェアの概念』で詳しく説明します。

ホストされるシステムにはそれぞれ、リモート・ディスクバリーと電源管理のためのサービス・プロセッサーがインストールされていなければなりません。複数のサービス・プロセッサーは、外部ネットワークを通じて単一の iSeries LAN アダプターに接続することができます。

拡張 iSCSI サポート

iSeries の単一の iSCSI HBA で、複数のサーバーまたはホストされるシステムをサポートすることができます。また、ホストされるシステムはそれぞれ複数の iSeries 用 iSCSI HBA に接続することが可能です。図 8 は、複数の iSeries 用 iSCSI HBA に接続されている、ホストされるシステムを示します。

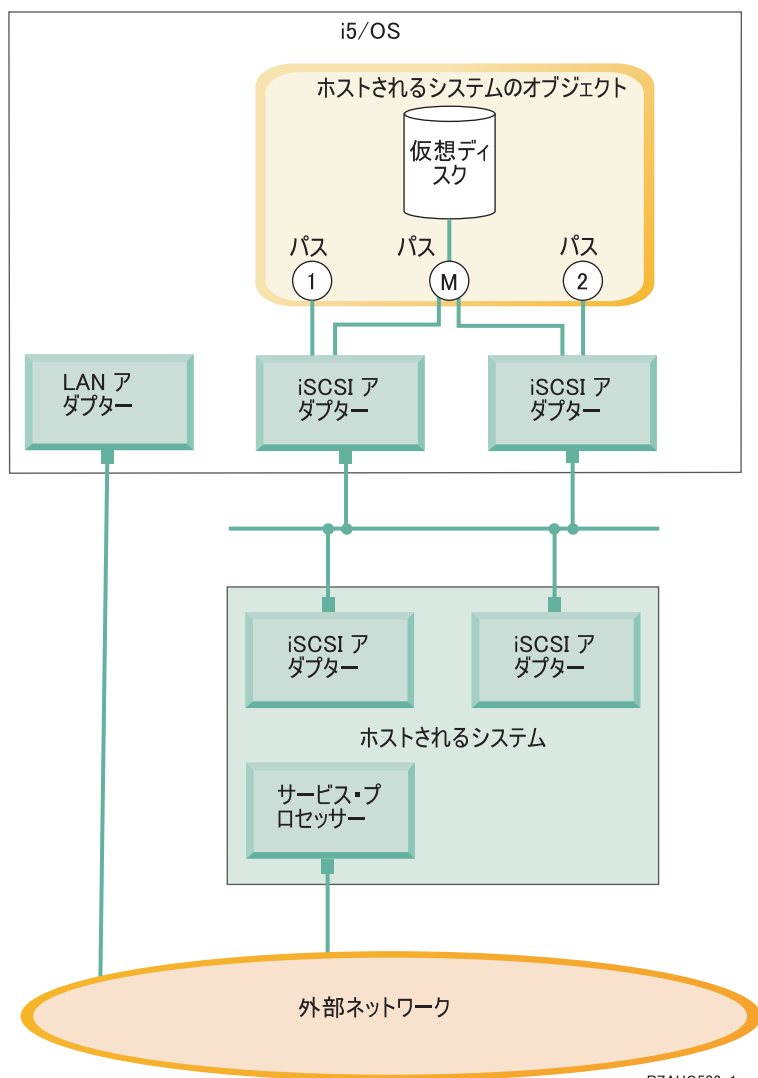


図 8. 拡張構成

図 8 は、ホストされるシステムにインストールされた複数の iSCSI HBA を示しています。

パス定義

ホストされるシステムが iSeries 用 iSCSI HBA に接続されるときに、ホストされるシステムと iSeries 用 iSCSI HBA の間にはパスが定義されます。

22 ページの図 8 では、いくつかの別個のパスが定義されています。それらには 1、2、および M というラベルが付けられています。

iSeries サーバーでホストされる仮想装置は、パスに検出されるということができません。iSeries 用 iSCSI HBA または NWSH アダプターによって i5/OS 内にホストされる、構成された仮想ディスク (たとえばドライブ C:) は、その NWSH アダプターに検出されます。

22 ページの図 8 では、パス 1 およびパス 2 はそれぞれ別個の iSeries 用 iSCSI HBA に対して定義されています。パス 1 に定義されている装置は、そのパスが定義されている iSCSI アダプターに検出することができます。同様に、パス 2 に定義されている装置は、そのパスが定義されている iSCSI アダプターに検出することができます。パス 1 や 2 にある装置は、特定の iSCSI HBA に排他的に検出されるということができます。

マルチパスの概要

ホストされるシステムは、i5/OS がホストする仮想ディスクにアクセスするための冗長パスを持つことができます。最も包括的なのは、各終端に冗長パスがある場合です。ある仮想ディスクには、ホストされるシステムにインストールされている 2 つの iSCSI HBA のいずれかを使用してアクセスでき、2 つの iSeries 用 iSCSI HBA のいずれかを使用して iSeries に検出することができます。これをマルチパスといいます。

22 ページの図 8 では、マルチパスは M として定義されています。マルチパスに検出される仮想ディスクには、iSeries サーバーにインストールされている iSCSI HBA のいずれかによってアクセスすることができます。マルチパスは、パス M にアクセスする、つまりそれを使用する iSeries 用 iSCSI HBA のグループとして定義されます。1 つのホストされるシステムに定義できるマルチパス・グループは 1 つだけです。このグループには、複数の iSeries 用 iSCSI HBA を含めることができます。

注: 取り外し可能メディア装置は、マルチパス・グループに定義できません。

専用帯域幅

冗長パスが望ましくない、または不要な場合もありますが、より高い性能が必要な仮想ディスクでは、専用パスを必要とする場合があります。


22 ページの図 8 の場合、ホストされるシステムの構成で、仮想ディスクをパス M にではなくパス 1 か 2 に定義することが可能です。このようにすると、iSCSI アダプターの帯域幅は特定の仮想ディスク専用にすることができます。

iSCSI を使用したディスクレス・ブート

iSCSI 接続のスタンドアロンまたは IBM BladeCenter サーバーはすべてディスクレスで、xSeries または IBM BladeCenter iSCSI ホスト・バス・アダプター (HBA) がブート装置として必要です。

新しい統合 Windows サーバーをインストールして使用する前に、i5/OS リモート・システム構成とリモート・サーバー iSCSI HBA の両方を構成しなければなりません。45 ページの『リモート・システム構成』を参照してください。

iSCSI HBA は、xSeries や IBM BladeCenter のブート・プロセス中にアダプターの CTRL-Q ユーティリティーを使用して構成しなければなりません。初期サーバー・セットアップの一部として構成することをお勧めします。ホストされるサーバーの iSCSI HBA で構成する必要があるパラメーターの最小限のセットがあります。これらのパラメーターは、リモート・システムの構成オブジェクトで構成されるパラメーターと一致する必要があります。これらのパラメーターは、選択されたブート・モードによって異なります。

- ホストされるシステムの iSCSI HBA を iSCSI ブート装置として構成する方法については、iSCSI インストール、最初にお読みください  の Web ページ (英語) を参照してください。リモート・システムの構成オブジェクト内のパラメーターのセットを構成する方法については、134 ページの『リモート・システム構成プロパティの変更』を参照してください。

ホストされるサーバーのブート装置の使用可能化

- xSeries または IBM BladeCenter にインストールされた iSCSI HBA は、構成されたパラメーターに基づいて、ブート・プロセス中にブート装置として機能します。
- xSeries の iSCSI HBA が 1 つだけである場合、このアダプターをブート装置として構成する必要があります。iSCSI ブートはすべての iSCSI HBA でデフォルトで使用可能になりますが、追加情報を構成しなければなりません。
- xSeries サーバーに複数の iSCSI HBA がインストールされている場合、その内の 1 つだけをブート装置として構成しなければなりません。
- IBM BladeCenter サーバーの iSCSI HBA は、デュアル・ポート・アダプターです。1 つのポートだけをブート装置として構成する必要があります。

ブート・モードとパラメーター

- iSeries iSCSI ソリューションは、いくつかの異なるブート・モードをサポートします。選択されたブート・モードに応じて、ホストされるシステムの iSCSI HBA で異なるブート・パラメーターを構成する必要があります。
- パラメーターは、アダプターの CTRL-Q ユーティリティを使用して構成されます。ブート装置は、サーバーを初めてデプロイする際に選択して構成しなければなりません。必要なパラメーターは、この初期セットアップ・プロセスの一部として構成することをお勧めします。

統合 DHCP サーバー

- iSCSI 接続サーバーは、デフォルトまたは DHCP ブート・モードを使用するように構成した場合、統合 DHCP サーバーを使用します。この統合 DHCP サーバーは汎用サーバーではありません。これは、ホストされるサーバーの iSCSI HBA にブート・パラメーターをデプロイすることだけを目的としたものです。ネットワーク・サーバー記述 (NWS) がオンに変更されている場合、サーバーはリモート・システム構成に提供されているパラメーターで自動的に構成されます。詳しくは、153 ページの『統合 DHCP サーバー』を参照してください。

Windows コンソール

統合サーバーとの対話は、Windows コンソールを使用して行います。ハードウェアおよびソフトウェアの構成次第で、以下のいずれかの方法で接続されているモニター、キーボード、およびマウスを使用することができます。

モニター、キーボード、マウスを直接接続

- IXS カード、IXA 接続 xSeries サーバー、または iSCSI 接続 xSeries または BladeCenter サーバーに直接接続されているモニター、キーボード、およびマウスを使用できます。これらは、統合サーバー・コンソールを形成します。これらの装置によって統合サーバーと対話する方法は、通常のパーソナル・コンピューター (PC) と対話する方法とまったく同じです。

iSCSI 接続サーバーには、いくらかのプリインストール・ハードウェア・セットアップが必要です。このセットアップは、直接接続されたモニター、キーボード、およびマウスを使用して行います。

リモート GUI デスクトップ・アプリケーション

Microsoft Terminal Services、Remote Desktop、その他のサード・パーティー・アプリケーションを使用して、リモート・ワークステーション上でサーバーのグラフィカル・ユーザー・インターフェース (GUI) デスクトップを表示することができます。サーバーに直接接続されたコンソールで普通に実行できる管理タスクのほとんどは、リモート・デスクトップでも実行できます。サーバー・コンソールに対してリモート・デスクトップを構成し、使用方法については、Microsoft Terminal Services または他のサード・パーティー・アプリケーションの資料を参照してください。

仮想シリアル・コンソール

i5/OS は、タイプ 4812 IXS の仮想シリアル・コンソールに接続することができます。これは、iSeries 論理区画に対して提供されている i5/OS 仮想シリアル・コンソール・サポートに似ています。これは 4812 IXS サーバー用のテキスト・モード・コンソールを提供し、これを使用することにより、グラフィカル・ユーザー・インターフェース (GUI) デスクトップにアクセスすることなくさまざまな管理タスクを行えます。特定の 4812 IXS の仮想シリアル・コンソールとのセッションを確立する方法は、165 ページの『4812 IXS 仮想シリアル・コンソールへの接続』を参照してください。

仮想シリアル・コンソールは現在 Windows Server 2003 でのみサポートされています。このコンソールを使用すると、サーバー・エラーを表示したり、LAN 通信を復元したりできます。このコンソールの接続は、サーバーで TCP/IP を構成する前に使用できます。仮想シリアル・コンソール

を使用して実行できるタスクについては、Microsoft Emergency Management Services の資料  (www.microsoft.com/whdc/system/platform/server/default.mspx) を参照してください。次の点に注意してください。

- i5/OS では仮想シリアル・コンソールに関する構成のほとんどが自動的に行われるため、Microsoft の文書で言及される構成タスクの中には i5/OS 仮想シリアル・コンソールで行う必要のないものもあります。
- iSeries の実装では、(Microsoft の資料では言及されていますが) 追加のハードウェア、たとえばモデム、コンセントレーター、ケーブルなどは必要ありません。

リモート監視プログラム・アダプター II グラフィカル・コンソール転送

RSA II を装備した xSeries サーバーの場合、RSA II も完全にハードウェア・ベースのグラフィカル・コンソール転送を提供します。つまり、ローカル・デスクトップを使用してリモート・サーバーへのアクセスとその制御が可能です。

考慮事項

統合 Windows サーバーは PC ベースの Windows サーバーとよく似ていますが、考慮する必要のあるいくつかの相違点もあります。

- ディスケット・ドライブは使用できません。つまり、スタートアップ・ディスクや緊急修復ディスクを使用できないということです。しかし、iSeries ディスク・スペースを使用してファイルや全ディスク・イメージをバックアップすることはできます。
- iSeries の磁気テープ装置およびディスク装置を使用できます。
- 仮想ネットワーキングを使用する場合、iSeries サーバーまたは他の統合サーバーでの TCP/IP 通信に、LAN アダプター、ケーブル、ハブ、またはスイッチは必要ありません。

- Microsoft Windows オペレーティング・システムを iSeries Windows 環境にインストールする方法は、標準的な PC サーバーのインストール方法と異なります。まず IBM i5/OS 統合サーバー・サポートをインストールしてから、Microsoft Windows のインストールを行います。ほとんどの構成情報は、i5/OS の WINDOWS サーバー導入 (INSWNTSVR) コマンドを使用して入力するため、通常のインストール・パネルのいくつかは表示されません。また、このコマンドには、日付および時刻の同期化など、サーバーを i5/OS に統合することに固有の追加パラメーターが含まれています。
- i5/OS 側のサーバー管理では、統合 Windows サーバーはネットワーク・サーバー記述 (NWS) によって表され、ネットワーク・インターフェースは回線記述によって表されます。i5/OS からサーバーを終了および再始動するには、NWS をオフそしてオンに変更します。
- i5/OS から、Windows ユーザーの作成などの多くのユーザー管理作業を実行できます。
- i5/OS が記憶域を管理する方法は PC とは異なるため (175 ページの『i5/OS の記憶域管理』を参照)、統合サーバーの場合は、PC サーバーでの記憶域管理に必要な一部の技法は必要ありません。


パフォーマンス


IXS、IXA、および iSCSI 接続サーバーはそれ自体のメモリーと 1 つ以上のプロセッサーを持っています。仮想 (シミュレートされた) ディスク・ドライブを通して、iSeries ハード・ディスク・ドライブ記憶域を共有します。ディスク・ドライブは、iSeries 上の記憶域スペース・オブジェクトを作成することにより、Windows に割り振られます。統合サーバーとスタンドアロン・サーバーの主な違いは、スタンドアロン・サーバーが多くの場合に専用のディスク・ドライブを使用するのに対して、統合サーバーは iSeries 記憶域スペースを仮想ディスクとして使用することです。また、iSeries 統合サーバーには、iSeries 磁気テープ・ドライブ、CD および DVD ドライブを共有するためのドライバーや高速仮想イーサネット・アダプターなどのオプション機構が含まれます。

iSeries 記憶域スペース (仮想ドライブ) を使用すると、大きな記憶域ファブリックへの投資や保守コストなしに、スタンドアロン環境では通常利用できないパフォーマンス上の利点が提供されます。しかし、それに伴う制限もあります。統合サーバーの計画と構成に当たっては、それらの制限も考慮に入れるべきです。以下の情報は、パフォーマンスに影響する考慮事項を中心に説明しています。

パフォーマンスに関連した情報の詳細は、以下のリンクを参照してください。

- 『iSeries 記憶域スペースと専用ディスクの比較』
- 27 ページの『記憶域スペースのバランス化』
- 28 ページの『iSCSI 接続サーバーのパフォーマンス』
- 29 ページの『仮想イーサネット』

- IBM iSeries 統合 xSeries ソリューション (英語) 
(www.ibm.com/servers/eserver/iseries/integratedxseries)

- iSeries パフォーマンス管理 (英語) 
(www.ibm.com/eserver/iseries/perfmgmt)

- iSeries Performance Capabilities Reference  の第 17 章

iSeries 記憶域スペースと専用ディスクの比較

統合サーバーでは、プロセッサーまたはメモリー集中の処理を実行できるように、そのパフォーマンス特性は専用ディスク・ドライブを使用するスタンドアロン・サーバーと同等です。統合サーバーのディスク・ドライブは iSeries 記憶域から割り振られるので、そのディスク・パフォーマンスは iSeries に依存します。

1 iSeries 共用ディスクではより大きなディスク・パフォーマンス能力が必要

1 ほとんどのスタンドアロン・サーバーでは、2、3 個のディスクが各サーバーに専用になります。ディスク
1 負荷の小さいアプリケーションの場合、そのパフォーマンスは十分です。しかしながら、これら 2、3 個の
1 専用ディスクの能力でサーバーのパフォーマンスが制限される時があります。

1 同じサーバーのグループを iSeries に統合した場合、仮想ディスクはもっと多くの iSeries ハード・ディス
1 クに分散することになります。全体の平均ディスク負荷は、専用ディスクを持つサーバーのグループの場合
1 より大きくなる必要はありません。しかし、個々のサーバーが余分のディスク・パフォーマンス容量を一時的
1 的に必要とする場合、iSeries ディスクのより大きなセットによって、それを使用可能にできます。

1 専用ディスクを持つサーバーの場合、ディスク応答時間は比較的に安定している傾向があります。たとえ
1 ば、予測可能な応答時間を利用して、Windows パフォーマンス・モニターを構成し、ディスク応答時間が
1 標準的なしきい値を越えたときにアラートを生成して、注意が必要な例外状態が起きていることを示すこと
1 ができます。

1 統合サーバーの場合は、iSeries の記憶域、CPU、およびメモリーは統合サーバーと iSeries アプリケーショ
1 ンの間で共有されます。通常、Windows のディスク応答はより大きな範囲で変動します。複数の統合サー
1 ーバーや他の iSeries 操作からの入出力操作が同じディスクで競合する短い期間が生じることがあります。デ
1 ィスク集中の iSeries アプリケーション (SAV や RST など) が、Windows サーバーで見られるディス
1 ク・パフォーマンスをある期間にわたって悪くしてしまう可能性があります。このため、短期間のためのし
1 きい値を選ぶのがもっと難しくなることがあります。

1 記憶域ボトルネックを評価する際には、ディスクのグループ全体を考慮する

1 iSeries サーバーの記憶域スペースは、Windows 内では 1 つのディスク・ドライブのように見えます。物
1 理ディスクの平均待ち行列長 (Windows パフォーマンス・モニターにおいて) が 2 を超える場合、サーバ
1 ー・パフォーマンスはディスクに制限されているとは限りません。メモリー・ページングの問題が計算に含
1 まれないと想定すると、待ち行列長が 2 になることや Windows ディスク使用率が 100% になることは、
1 操作を実行する物理ディスク・ドライブが 1 個しかない場合に記憶域ボトルネックがあることを示すにす
1 ぎません。記憶域スペース ASP が並列に作動している iSeries サーバーには通常、複数のディスクがあり
1 ます。通常、ASP 内のディスクの数の 2 倍がディスク・ボトルネックを示す可能性があります。また、記
1 憶域 ASP を使用しているすべてのサーバーの平均待ち行列長を計算に入れる必要があるかもしれません。

1 記憶域スペースのバランス化

1 記憶域スペースが作成されると、データはユーザーが指定した補助記憶域プール (ASP) または独立補助記
1 憶域プール (IASP) 内のディスクに分散されます。プール内のディスクは、無保護、パリティ保護
1 (RAID-5)、またはミラー保護のいずれかに構成できます。無保護のディスクは、ディスク障害が起きても保
1 護されません。パリティ保護されたディスクは、パリティ・セットを維持し、ディスクに障害が起こっ
1 た場合に回復できるようにします (パフォーマンスは犠牲になります)。ミラーリングはディスク障害に対
1 する保護を提供しますが、パリティよりもパフォーマンスが良くなります。ASP や IASP の構成方法に
1 関係なく、統合サーバーでは、効率的な iSeries 記憶域アーキテクチャーの利点を活用できます。

1 iSeries サーバーには、データがディスク間で効率的に分散されるようにするための機能があります。1 つ
1 の例は、ディスク再編成の開始 (STRDSKRGZ) 操作で、この操作はディスク記憶域使用率をバランス化し
1 ます。もう 1 つの例は、ハード・ディスク・リソースを ASP に割り当てる際に使用可能な「ASP への装
1 置の追加およびデータのバランス化」です。統合サーバーでは、リンクされているサーバーがオフに変更さ
1 れた場合、記憶域スペースのディスク間での移動、または再バランス化のみが行われます。

記憶域スペースに関連したデータの場所は、通常 iSeries によって自動的に管理されます。Windows オペレーティング・システム内でディスクのストライピングされたボリュームやソフトウェア RAID を構成する必要はありません。Windows オペレーティング・システムでこれらの機能を構成すると、実質のディスク操作を遅くしてしまう場合があります。記憶域が iSeries ディスクにそれほど分散していない場合でも、Windows 上で継続的に関連したディスクのデフラグを行って、効率的なファイル・システム・データ構造を維持するようにしてください。

iSeries が統合サーバーのディスク要件をどれほど実現しているかについては、ディスク状況の処理 (WRKDSKSTS)、ネットワーク・サーバー記憶域スペースの処理 (WRKNWSSTG)、およびネットワーク・サーバー状況の処理 (WRKNWSSTS) コマンドを使用してモニターすることができます。パフォーマンス上のその他の考慮事項については、統合サーバーが Microsoft Windows サーバーであることに注意してください。Microsoft の Windows パフォーマンス・モニターは、他のサーバーの場合と同じ方法で使用できます。パフォーマンス・モニターの使用については、Microsoft Windows の資料を参照してください。

iSCSI 接続サーバーのパフォーマンス

iSCSI 接続サーバーの場合、必要に応じてより良いパフォーマンス能力のために調整を行う複数の構成オプションがあります。オプションによっては、統合サーバー上で異なるターゲット・ディスク構成やボリュームが必要です。

Windows ディスク構成

iSCSI 接続統合サーバーでは、仮想ディスク・ドライブは以下の構成に最適化されます。

- 仮想ドライブ当たり 1 ディスク区画
- 1 ギガバイト以上の記憶域スペース
- 4 キロバイト以上のクラスター・サイズでフォーマットされた NTFS ファイル・システム

これらのガイドラインにより、iSeries は記憶域スペース・メモリーを効率的に管理し、ディスク・パフォーマンスを向上させることができます。これらのガイドラインは IXS および IXA 接続のサーバーにも使えますが、その影響ははるかに小さくなります。

ネットワーク・サーバー記憶域スペースの変更 (CHGNWSSTG) CL コマンドを使用して記憶域スペース・サイズを増やす場合、必ず Windows Server 2003 の DISKPART コマンドを使用して Windows 上のパーティションのサイズも増やしてください。

注: パフォーマンスを良くするため、新規スペースに別のディスク区画を追加するのではなく、サーバーに記憶域スペースを追加してください。

iSeries メモリー・プール

iSCSI 接続サーバーの場合、記憶域操作は iSeries メモリー・プールを通じて行われます。このメモリーは、実質的にはディスク操作のキャッシュとして機能するので、このメモリーのサイズは Windows のディスク・パフォーマンスに影響を与る場合があります。この I/O が直接ベース・プール内のページ不在を引き起こすことはありません。しかし、プール・メモリーは他の i5/OS アプリケーションと共用されるので、Windows ディスク操作が他のアプリケーションのページ不在を引き起こしたり、他のアプリケーションが iSCSI ディスク操作のページングを引き起こしたりする場合があります。極端な場合には、メモリーの問題を軽減するために、メモリー・プール・サイズの調整やアプリケーションに他のメモリー・プールを割り当てる必要がある場合もあります。

IXS および IXA 接続のサーバーは、ディスク操作にベース・メモリー・プールを使用しません。それらは、マシン・プール (システム・プール ID 1) 内の予約メモリーを使用します。このため、ディスク操作で他のアプリケーションとメモリーを共有することはありません。

iSCSI パフォーマンス構成

iSCSI 接続統合サーバーの場合、単一のネットワーク・ファブリックが容量の限界に達した場合、追加の iSCSI HBA を持つチャンネルを xSeries サーバーと iSeries サーバーの両方に追加することが可能です (相互接続ネットワークの帯域幅も使用可能と想定した場合)。

iSCSI およびネットワーク・トラフィックを別々のチャンネルに分散するには、以下のようないくつかの方法があります。

- SCSI 操作を 1 つのチャンネル専用、仮想イーサネット操作を別のチャンネル専用にします。
- 2 つの記憶域ターゲットを使用します。各ターゲットは別の HBA パスにリンクしなければなりません。146 ページの『iSCSI ホスト・バス・アダプターの管理』を参照してください。
 - Windows 上で、可能であればアプリケーションが両方のドライブを使用するようにするか、ドライブをそれぞれ別々のアプリケーション専用にして全体のディスク操作がドライブ間で分散するようにします。
 - データが 2 つのドライブにわたってストライピングされるように、2 つのディスクを Windows ダイナミック・ボリューム・セットに構成します。アプリケーションがボリュームを使用すると、ディスク操作はボリューム・セット内のドライブ間で自動的にバランスを取ります。

仮想イーサネット

仮想イーサネットの Point-to-Point 接続は、iSeries ホスト区画と各統合 Windows サーバーの間のデフォルト仮想ネットワーク接続です。統合環境の一部である管理操作には、基本的にこの Point-to-Point 接続が使用されます。

Point-to-Point 接続を使用した場合の iSeries および Windows の CPU 使用コストは、ハードウェア・ネットワーク・アダプターを使用した場合の使用コストと同様です。接続は高速ですが、その合計帯域幅は常に IXS および IXA アダプター上のディスク、磁気テープ、その他の操作と共有されます。Internet SCSI (iSCSI) を使用する場合、もう一つの iSCSI HBA チャンネルを使用することにより、仮想イーサネット操作を分離することができます。

複数の統合サーバー間の仮想イーサネット接続では、iSeries サーバーがトラフィックのエンドポイントではない場合でも、サーバー間のトラフィックの切り替えに iSeries CPU を使用します。ほとんどの接続において、この使用量は大きなものではありません。しかし、統合サーバー間の仮想イーサネット接続に持続して高いネットワーク負荷が予想される場合、仮想イーサネット内部スイッチと統合サーバー上の外部ネットワーク・アダプターの使用コストのバランスを取る必要があるかもしれません。

ネットワークキングの概念

ホストされるシステムには、いくつかの異なるタイプのネットワーク接続が関係しています。

以下の接続タイプは、iSCSI 接続システムにだけ使用されます。

- 30 ページの『サービス・プロセッサ接続』
 - この物理接続により、ホストする i5/OS 区画はホストされるシステムのサービス・プロセッサと通信することができます。

1 • 31 ページの『iSCSI ネットワーク』

1 この物理ネットワークは、ホストする i5/OS 区画の iSCSI アダプターをホストされるシステムの iSCSI
1 アダプターと接続します。

すべてのタイプの統合 Windows サーバーでは、以下の接続タイプを使用することができます。

• 仮想イーサネット

これは、追加のネットワークング・カードやケーブルを必要としないシミュレートされたイーサネット
接続です。仮想イーサネットには 2 つのタイプがあります。

– 33 ページの『Point-to-Point 仮想イーサネット』

この接続は、ホストされるシステムとホストする i5/OS の間の汎用通信を提供します。

– 34 ページの『仮想イーサネット・ネットワーク』

ホストされるシステム、i5/OS 区画、および他の区画 (Linux など) の間に作成されるネットワークで
す。

• 38 ページの『外部ネットワーク』

すべてのサーバーが使用し、ホストされるシステムが制御する物理ネットワーク・カードによるネット
ワークングによって作成される、通常の Windows ネットワークです。

1 サービス・プロセッサ接続

1 注: このセクションは iSCSI 接続のシステムにのみ関係します。

1 この物理接続は、ホストする i5/OS がホストされるシステムのサービス・プロセッサと通信できるよう
1 にするために必要です。この接続は、単純なスイッチ接続されたネットワークで構成されることも、もっと
1 複雑な経路を通ったネットワークで構成されることもあります。iSeries Windows 環境は、この接続に対
1 して IBM Director を使用して、ホストされるシステムの状態を管理します。

1 接続の一方の終端には、LAN アダプターつまり i5/OS が制御するアダプターがあります。この LAN アダ
1 プターは他の目的のためにも使用可能です。このアダプターの IP アドレスやその他の属性は、i5/OS の標
1 準の構成方法を使用して制御します。iSeries Windows 環境では、このアダプターの構成を行いません。
1 IBM Director および既に構成されている 1 つ以上の i5/OS TCP インターフェースを使用して、自動的に
1 サービス・プロセッサを発見することができます。

1 接続のもう一方の終端には、サービス・プロセッサがあります。サービス・プロセッサには、それ自体
1 のイーサネット・ポートと TCP/IP スタックがあります。この TCP/IP スタックは、サーバーの電源コード
1 が通電されている AC コンセントに差し込まれていれば、サーバーが電源の入った状態になくてもアクテ
1 ィブになります。ある xSeries のモデルでは、Windows とベースボード管理コントローラー (BMC) と呼
1 ばれる特定のタイプのサービス・プロセッサが単一のイーサネット・ポートを共有します。この場合、ホ
1 ストされるシステムの同じ物理ポートが、サービス・プロセッサ接続と外部ネットワーク接続の両方を提
1 供します。

1 サービス・プロセッサ用の DHCP サーバー

1 サービス・プロセッサの IP アドレスを設定すると、ネットワーク上にサービス・プロセッサ接続を提
1 供する外部 DHCP サーバーが必要になる場合があります。この DHCP サーバーは、ホストされるシステ
1 ムの電源コードを通電された AC コンセントに差し込む前に、アクティブにしておかなければなりませ
1 ん。(この DHCP サーバーは、ホストされるオペレーティング・システムの iSCSI ブートを支援するため
1 に iSCSI ネットワークの i5/OS 側に組み込まれている DHCP サーバーとは別のものです。) 詳しくは、
1 157 ページの『動的 IP アドレッシング (DHCP)』を参照してください。

IP マルチキャスト

サービス・プロセッサの発見のために iSeries Windows 環境が提供するオプションがいくつかあります。最大の自動化を提供する選択では、ネットワークが IP マルチキャストをサポートしている必要があることにご注意ください。スイッチやネットワークの中には、デフォルトでは IP マルチキャストをサポートしないものがあります。詳しくは、157 ページの『サービス・プロセッサのディスクバリー方式』を参照してください。

パフォーマンスと最大伝送単位 (MTU)

サービス・プロセッサ接続に高速ネットワークを使用したり、大規模 MTU を使用することは、必要ではありません。また、利点もありません。

セキュリティ

使用するサービス・プロセッサ・ハードウェアのセキュリティ機能が、サービス・プロセッサ接続を提供するのに分離されたネットワークと共用ネットワークのどちらを使用するかに決定に影響する場合があります。詳しくは、143 ページの『サービス・プロセッサ SSL の構成』を参照してください。

iSCSI ネットワーク

この物理ネットワークは、ホストする i5/OS のイーサネット iSCSI アダプターをホストされるシステムのイーサネット iSCSI アダプターと接続します。通常は、単純なスイッチ接続されたギガビット・イーサネット・ネットワークです。2 種類のトラフィック、記憶域 (SCSI) および仮想イーサネット (LAN) がこの接続を通じて流れます。

このネットワークの一方の側には、iSCSI アダプターつまり i5/OS が制御するアダプターがあります。iSCSI アダプターにはそれぞれ 2 つの IP アドレスがあり、1 つは SCSI 用、もう 1 つは LAN 用です。アダプターの IP アドレスやその他の属性は、ネットワーク・サーバー・ホスト・アダプターとして知られる i5/OS 装置記述オブジェクトで構成します。詳しくは、45 ページの『ネットワーク・サーバー・ホスト・アダプター』を参照してください。i5/OS が制御する iSCSI アダプターそれぞれに、それ自体のオブジェクトが必要です。すべての iSCSI アダプターには、通常の i5/OS TCP/IP スタックとは別の TCP/IP スタックがハードウェア内にインプリメントされています。ネットワーク・サーバー・ホスト・アダプターをオンに変更すると、i5/OS が制御する iSCSI アダプターは構成された値を使用します。別の値を有効にしたい場合は、構成を変更して、サーバー・ホスト・アダプターをもう一度オンに変更しなければなりません。i5/OS TCP/IP スタックからは、iSCSI アダプターに構成されている IP アドレスが分かりません。

ネットワークのもう一方の側には、iSCSI アダプターつまりホストされるシステム用のアダプターがあります。これらのアダプターの IP アドレスやその他の属性は、リモート・システム構成として知られる i5/OS オブジェクトで構成します。詳しくは、45 ページの『リモート・システム構成』を参照してください。この構成は、以下のいくつかの点で、i5/OS ネットワーク・サーバー・アダプター・オブジェクトと異なります。

- ホストされるシステム内の iSCSI アダプター・ポートは、1 つか 2 つの IP アドレス (SCSI、LAN、または両方) で構成することができます。構成されたアダプターすべての中に、少なくとも 1 つの SCSI と 1 つの LAN IP アドレスがなければなりません。
- ホストされるシステムの iSCSI アダプターの IP アドレスを構成するときは、対応するアダプター MAC アドレスも必ず構成しなければなりません。アダプターにはそれぞれ、その MAC アドレスを示すラベルがあります。MAC アドレスの構成は正しく行うように注意してください。
- ホストされるシステムの iSCSI アダプターすべての構成は、同じ i5/OS リモート・システム構成オブジェクトで行います。その後統合サーバーをオンに変更すると、製品は自動的に、ホストされるシステムの iSCSI アダプターが i5/OS リモート・システム構成の値を使用するようにします。別の値を有効にしたい場合は、構成を変更して、サーバーをもう一度オンに変更しなければなりません。

・ SCSI トラフィックは iSCSI アダプターのハードウェア TCP/IP スタックを使用しますが、LAN トラフィックは Windows TCP/IP スタックを使用します。したがって、Windows TCP/IP スタックからは SCSI IP アドレスが分かりませんが、LAN IP アドレスは分ります。

注:

1. i5/OS 構成オブジェクトでは、ネットワーク・インターフェース情報にはローカルまたはリモートというラベルが付きます。これらの用語は i5/OS に対するものです。ローカル・インターフェース情報は i5/OS 側に関する情報です。リモート・インターフェース情報は Windows のホストされるシステム側に関する情報です。
2. ネットワーク・サーバー・ホスト・アダプターとリモート・システム構成は、iSCSI ネットワークの両側の IP アドレス情報を定義します。単純な交換網で接続する際には、以下の規則が適用されます。
 - ・ スイッチによって接続されたこれら 2 つのオブジェクトの SCSI インターネット・アドレスは、同一のサブネットになければなりません。例えば、a.b.x.y という形式の IP アドレスと 255.255.255.0 というサブネット・マスクの場合、両方のオブジェクトの a.b.x は同じ値でなければなりません。
 - ・ スイッチによって接続されたこれら 2 つのオブジェクトの LAN インターネット・アドレスは、同一のサブネットになければなりません。
 - ・ ネットワーク内にゲートウェイがない場合、ネットワーク・サーバー・ホスト・アダプターのゲートウェイ・エレメントは、任意のサブネット内の任意の未割り当ての IP アドレスにすることができます。
 - ・ ネットワーク内にゲートウェイがない場合、リモート・システム構成のゲートウェイ・エレメントは、ブランクにする必要があります。

DHCP および DHCP リレー

ホストされるシステムにブート情報を配信するには、いくつかの方法があります。Windows をブートするための IP および 記憶域情報を配信するデフォルトの方法では、iSCSI ネットワークの i5/OS 側の統合動的ホスト構成プロトコル (DHCP) サーバーを使用します。DHCP を使用しても、DHCP サーバーは単一の IP アドレスを MAC アドレスと関連付けるので、IP アドレスは静的なものとして扱われる場合があります。詳しくは、23 ページの『iSCSI を使用したディスクレス・ブート』を参照してください。

統合 DHCP サーバーは、iSCSI ネットワーク上に存在する可能性のある任意の DHCP サーバーと共存できるように設計されています。

iSeries サーバーとホストされるシステムの間ルーターが iSCSI ネットワークに含まれていて、ブート情報の配信方法が DHCP である場合、適切に構成された DHCP リレー・エージェント (BOOTP リレー・エージェントとしても知られる) がネットワークに必要です。

パフォーマンスおよび最大伝送単位 (MTU)

iSCSI ネットワークでは、帯域幅が高く、待ち時間が短いことが望まれます。ネットワークが大きな MTU をサポートする場合、仮想イーサネットは最大 9000 バイトの MTU の「ジャンボ」フレームを利用することができます。これによって仮想イーサネットのパフォーマンスが向上します。

i5/OS iSCSI アダプター使用率の管理

ネットワーク・サーバー記述に構成されるパスは、i5/OS iSCSI アダプターを流れることができる記憶域トラフィック (存在する場合) と仮想イーサネット・トラフィック (存在する場合) を制御します。詳しくは、147 ページの『iSCSI HBA 使用法の管理』を参照してください。

複数のネットワーク・サーバー記述が同じネットワーク・サーバー・ホスト・オブジェクトを使用する場合、複数のホストされるシステムが 1 つの i5/OS iSCSI アダプターを同時に使用することができます。

ホストされるシステムの iSCSI アダプター使用率の管理

ホストされるシステム内の iSCSI アダプターは、SCSI IP アドレス、LAN IP アドレス、または両方の種類の IP アドレスで構成することができます。SCSI IP アドレスがあれば記憶域トラフィックが使用可能になり、LAN IP アドレスがあれば仮想イーサネット・トラフィックが使用可能になります。Windows の仮想イーサネット・アダプターは通常、自動的に物理 iSCSI アダプターに割り当てられます。各仮想イーサネット・アダプターの拡張プロパティ・タブには、特定の物理 iSCSI アダプターを選択することができます。150 ページの『iSCSI ネットワークの Windows 側での iSCSI HBA 割り振りの管理』を参照してください。

IBM は、汎用外部ネットワーク接続として iSCSI アダプターを使用することをサポートしません。外部ネットワーク接続の詳細については、38 ページの『外部ネットワーク』を参照してください。

他の考慮事項

- iSCSI ネットワークはインターネット・プロトコルのバージョン 4 だけを使用します。
- フレーム形式はイーサネット・バージョン 2 です。
- iSCSI ネットワークはネットワーク・アドレス変換をサポートしません。

セキュリティ

記憶域トラフィックと仮想イーサネット・トラフィックのセキュリティを確保するには、いくつかの方法があります。詳しくは、51 ページの『セキュリティの概念』を参照してください。

Point-to-Point 仮想イーサネット

i5/OS には、その統合 Windows サーバーとの通信手段が必要です。この通信は、Point-to-Point 仮想イーサネット・ネットワークによってなされます。統合サーバーがインストールされると、それを制御する i5/OS 区画との間に特殊な仮想ネットワークが作成されます。このネットワークには統合サーバーと iSeries の 2 つのエンドポイントしかなく、仮想イーサネット・ネットワークと同じく追加の物理ネットワーク・アダプターまたはケーブルを使用しないで iSeries 内でエミュレートされるため、Point-to-point と呼ばれます。i5/OS では、ポート番号値 *VRTETHPTP のイーサネット回線記述として構成されます。

WINDOWS サーバー導入 (INSWNTSVR) コマンドを使用すると、Point-to-Point 仮想イーサネットが構成されます。

Point-to-Point 仮想イーサネット接続と仮想イーサネット・ネットワークは、何が違うのかと思われるかもしれませんが、Point-to-Point 仮想イーサネットは構成方法が異なっており、エンドポイントとしては iSeries と統合サーバーの 2 つだけが可能です。Point-to-Point 仮想イーサネットでは、TCP/IP プロトコルだけがサポートされており、プライベート・ドメイン内の制限付き IP アドレスがデフォルトで使用されるため、アドレスがゲートウェイまたはルーターを通過することはありません。

統合 xSeries サーバー (IXS) と統合 xSeries アダプター (IXA) 接続 xSeries サーバーの場合、これらのアドレスの形式は 192.168.xxx.yyy (xxx と yyy は 1 から 2 桁にすることができます) です。たとえば、ハードウェア・リソースの番号が LIN03 として定義された IXS の場合、IP アドレスは 192.168.3.yyy です。

iSCSI ハードウェアの場合、これらのアドレスの形式は 192.168.xxx.yyy (xxx は 100 から 254 の範囲) で、結果として固有のクラス C ネットワークになります。この例では、Point-to-Point ネットワークの i5/OS 側には IP アドレス 192.168.100.1 が割り当てられ、Windows 側は 192.168.100.2 になります。同一のハードウェア・リソースに複数の回線記述を定義するにつれて、yyy の値は大きくなっていきます。

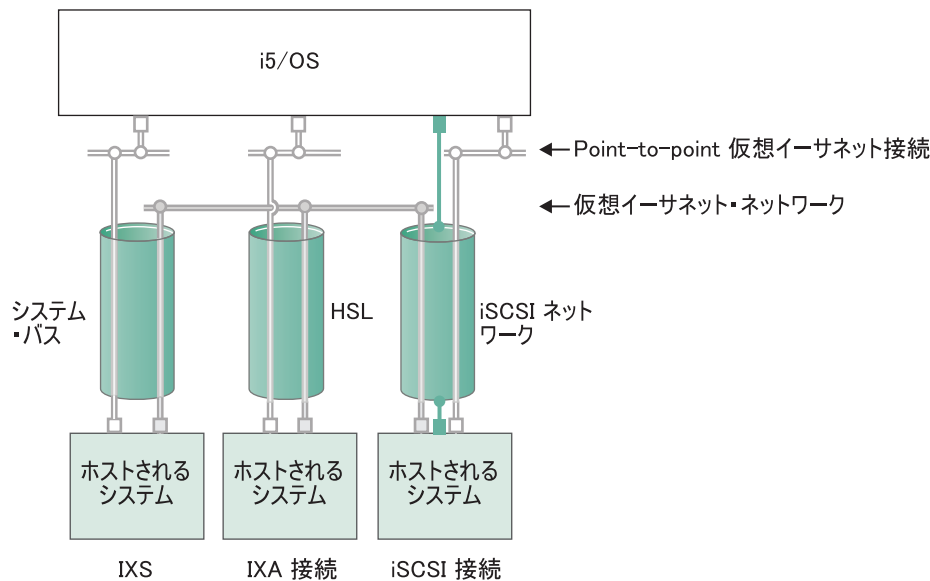
それらの IP アドレスは、INSWNTSVR コマンドで自動的に割り当てるか、またはシステム上の他のホストとの間で TCP/IP アドレス衝突が発生しないように手動で構成することができます。

仮想イーサネット・ネットワーク

仮想イーサネット・ネットワークは柔軟性があり、さまざまな構成が可能です。

複数の論理区画を含まない仮想イーサネット・ネットワーク

仮想イーサネット・ネットワークを作成する手順については、123 ページの『仮想イーサネット・ネットワークの構成』を参照してください。



- または
- 仮想アダプター上の IP アドレス
 - iSCSI アダプター上の LAN IP アドレス

RZAHQ500-5

図9. システム・バス、HSL、iSCSI ネットワーク・トンネル

IXS、IXA 接続システム、および iSCSI HBA 接続システムは皆、仮想イーサネット・ネットワークに参加でき、互いに通信することができます。

- IXS の場合、仮想イーサネットのトラフィックは iSeries システム・バスを流れます。
- IXA 接続のホストされるシステムの場合、仮想イーサネットのトラフィックは HSL ケーブルを流れます。
- iSCSI 接続のホストされるシステムの場合、仮想イーサネットのトラフィックは物理 iSCSI ネットワークのトンネルを通り抜けます。iSCSI ネットワークが存在する場合でも、仮想イーサネットは以下のいくつかの理由が必要です。
 - 仮想イーサネットは、iSeries サーバーの他の仮想イーサネット・サポートと共に機能できます。
 - 仮想イーサネットは、iSCSI ネットワーク内のスイッチが IEEE 802.1Q VLAN をサポートしなくても、分離された複数の仮想ネットワークを各 iSCSI HBA を通じて提供できます。

- IPSec を有効にすれば、iSCSI ネットワークを通るトラフィックは暗号化されます。仮想イーサネットは、強力な仮想プライベート・ネットワーク (VPN) とみなすことができます。通常の VPN には 2 つのエンドポイントがあるだけなのに対して、IPSec を伴った仮想イーサネットは仮想ネットワーク全体を保護することができます。

注: 各 iSCSI HBA インターフェースは、2 つの IP アドレス (1 つは記憶域、もう 1 つは LAN 機能で仮想イーサネットのトンネルを通り抜けるのに使用されます) を持つことができます。i5/OS TCP/IP はこれらの IP アドレスを知りません。iSCSI HBA の場合、仮想イーサネットは物理エンドポイントにある iSCSI HBA を使用した物理ネットワークのトンネルを通り抜けます。

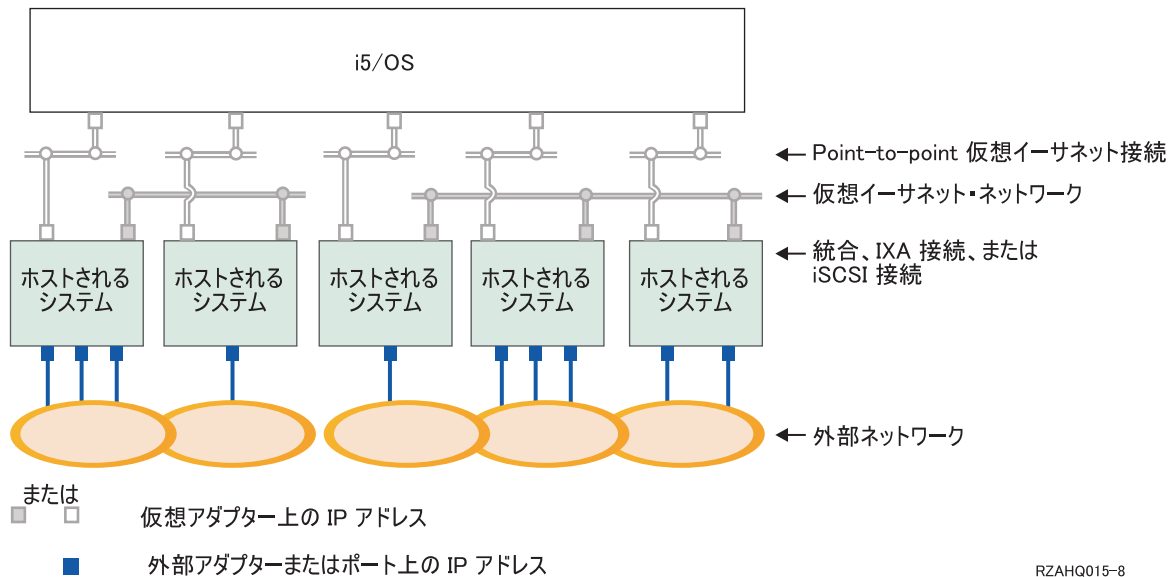


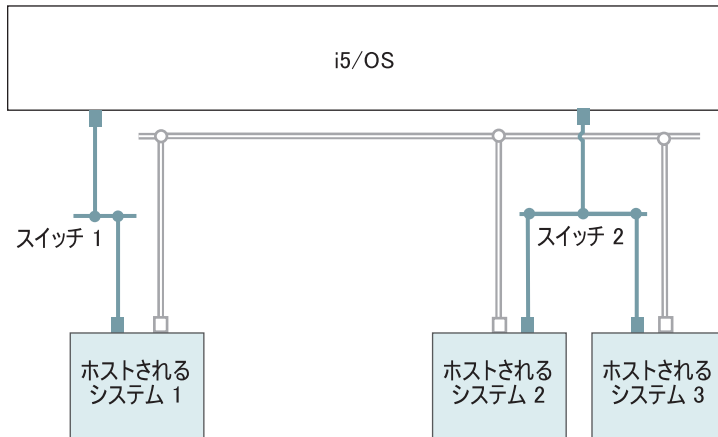
図 10. 同じ iSeries サーバー上にある統合 Windows サーバーの 2 つの分離されたグループ。各グループにはそれぞれ 1 つの複数ポイント仮想イーサネット・ネットワークがあります。

図 10 は、仮想ネットワークが iSeries 内でどのように機能するかを説明するものです。5 つの異なる統合 Windows サーバーがあります。それらはすべて、Point-to-Point 仮想イーサネット・ネットワーク (白色) によって単一の i5/OS 区画に接続されて、その制御を受けます。統合サーバーの下にある青色の四角は、マシンを外部ネットワークに接続するための物理ネットワーク・アダプター・カードです。その接続先の楕円形は、外部ネットワークを表します。最後に、2 つの分離した仮想イーサネット・ネットワーク (グレー) があります。各統合サーバーは、同時に最大 4 つの仮想イーサネット・ネットワークに参加できます。

クラスター化のために統合サーバーのグループを構成する際には、このタイプの接続が必要です。

Point-to-Point 仮想イーサネットと同じように、仮想イーサネット・ネットワークもイーサネット回線記述によって構成されます。統合サーバーが仮想イーサネット・ネットワークに接続されるのは、イーサネット回線記述のポート番号に *VRTETH0 から *VRTETH9 までの値を指定するように i5/OS 構成 (NWSD) が構成された場合です。NWSD のポート番号値が同じになるよう構成された統合サーバーは、同じ仮想イーサネット・ネットワークに接続されます。新しい統合サーバーをインストールする場合、WINDOWS サーバー導入 (INSWNTSVR) コマンドを実行することにより、必要な回線記述を自動的に作成して、それらに IP アドレスを割り当てることができます。上図には、回線記述の i5/OS 側が示されていません。仮想イー

サネットを使用する場合とは異なり、仮想イーサネット・ネットワークで使用される回線記述の i5/OS 側の TCP/IP アドレスは構成しなければなりません。



□ 仮想アダプター上の IP アドレス

■ iSCSI アダプター上の LAN IP アドレス

RZAHQ513-2

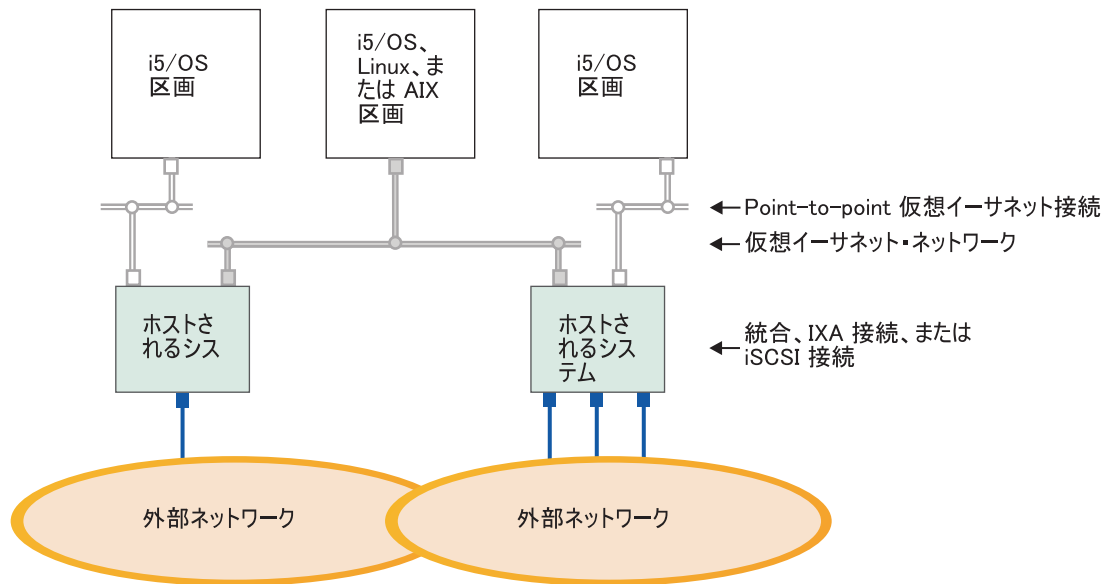
図 11. iSCSI ネットワークのトンネルを通り抜ける仮想イーサネット

iSCSI ネットワークのトンネルを通り抜ける仮想イーサネットには、図 11 に示されるいくつかの特性があります。

- 別々の iSCSI ネットワーク (別々の物理スイッチ) が関係しているにも関わらず、ホストされるシステム 1 はホストされるシステム 2 およびホストされるシステム 3 と通信することができます。
- ホストされるシステム 2 とホストされるシステム 3 は同一のスイッチに接続されていますが、これらのホストされるシステム間の仮想イーサネット通信には iSeries システムが関係します。
- それぞれのホストされるシステムの仮想イーサネット通信に関する、物理 iSCSI ネットワーク上の LAN IP アドレスのペアがあります。ホストされるシステム 2 のためのペアとホストされるシステム 3 のためのペアは、i5/OS 側で共通に IP アドレスを持ちます。

複数の論理区画を含む仮想イーサネット・ネットワーク

仮想イーサネット・ネットワークを作成する手順については、124 ページの『区画間仮想イーサネット・ネットワークの構成』を参照してください。



- または □ 仮想アダプター上の IP アドレス
- 外部アダプターまたはポート上の IP アドレス

RZAHQ016-9

図 12. 単純な区画間仮想イーサネット・ネットワーク

今回は、iSeries は区画に分割され、3 つの異なる仮想 i5/OS 論理区画が iSeries 内に作成されました。この図には、3 つの仮想ネットワークが示されています。Point-to-Point 仮想イーサネット・ネットワーク (白色) が 2 つと仮想イーサネット・ネットワーク (グレー) が 1 つです。各統合サーバーには、その制御区画との通信のための Point-to-Point 仮想イーサネット・ネットワークがあります。この例では、仮想イーサネット・ネットワークに 3 つの参加者がいます。それらは、それぞれ異なる i5/OS 区画によって制御される 2 つの統合サーバー、および i5/OS または他のオペレーティング・システムが実行されている第 3 の区画です。これを区画間イーサネット・ネットワークと言います。

ハードウェア管理コンソール (HMC) のないサーバーでは、同じネットワーク番号を使用する複数の区画の間に区画間接続が存在し、統合サーバーが接続されるのは制御 i5/OS 区画が接続された場合だけです。ネットワーク番号の 0 から 9 までは、統合サーバーのためのものです。たとえば、i5/OS 区画がネットワーク 1 と 5 で区画間接続用に構成されている場合、その区画によって制御される統合サーバーは、ポート *VRTETH1 と *VRTETH5 で区画間通信に参加できます。その手順については、iSeries ナビゲーターのオンライン・ヘルプを参照してください。概要を知るには、「論理区画の概念」を参照することもできます。

ハードウェア管理コンソール (HMC) のあるサーバーの場合、同じ仮想 LAN ID を使用する複数の区画または統合サーバーの間に区画間接続が存在します。参加している統合サーバーは、仮想 LAN ID を直接サポートしていません。その代わりに、参加している各統合サーバーには、*VRTETH1 などのポート値を、仮想 LAN ID のある仮想アダプターに関連付けるイーサネット回線記述が必要になります。仮想アダプターは、HMC を使用して作成します。詳細については、「eServer i5 による区画化」トピックと、IBM Systems Hardware Information Center 内の『i5/OS 用の仮想イーサネット・アダプターの構成 (Configuring a virtual Ethernet adapter for i5/OS)』を参照してください。HMC を持たないサーバーから HMC を持つサーバーに区画間仮想イーサネットを移行する場合、HMC を使用する仮想イーサネット・アダプターを作成し、イーサネット回線記述を追加して、該当する関連を提供する必要があります。同じ区画の中であれば、単に同じ仮想イーサネット・ポート番号を使用するだけで引き続き Windows サーバー間の相互通信が可能です。

外部ネットワーク

統合 Windows サーバーは、通常の PC サーバーの場合と同じように外部ネットワークに参加することができます。その方法には、いくつかあります。IXA または iSCSI 接続の統合サーバーでは PCI 拡張スロットが使用可能なので、PC の場合と同じように、統合ネットワーク・アダプターのいずれかを使用したリ、ネットワーク・アダプター・カードを取り付けたりできます。IXS は iSeries 内の PCI スロットに取り付けたカード上の PC サーバーです。IXS には PCI 拡張スロットがありませんが、中には、取り付け位置に隣接した iSeries PCI スロットを制御することができるものがあり、それによって、iSeries ネットワーク・アダプターを「占有」します。さらに、タイプ 2892 および 4812 IXS モデルには統合イーサネット・ネットワーク・アダプターが搭載されています。

ネットワーク・アダプター・カードを IXS または xSeries 用に物理的にインストールする方法、および統合サーバーと共に使用するためにそれらのカードを構成する方法については、127 ページの『外部ネットワーク』を参照してください。

ソフトウェアの概念

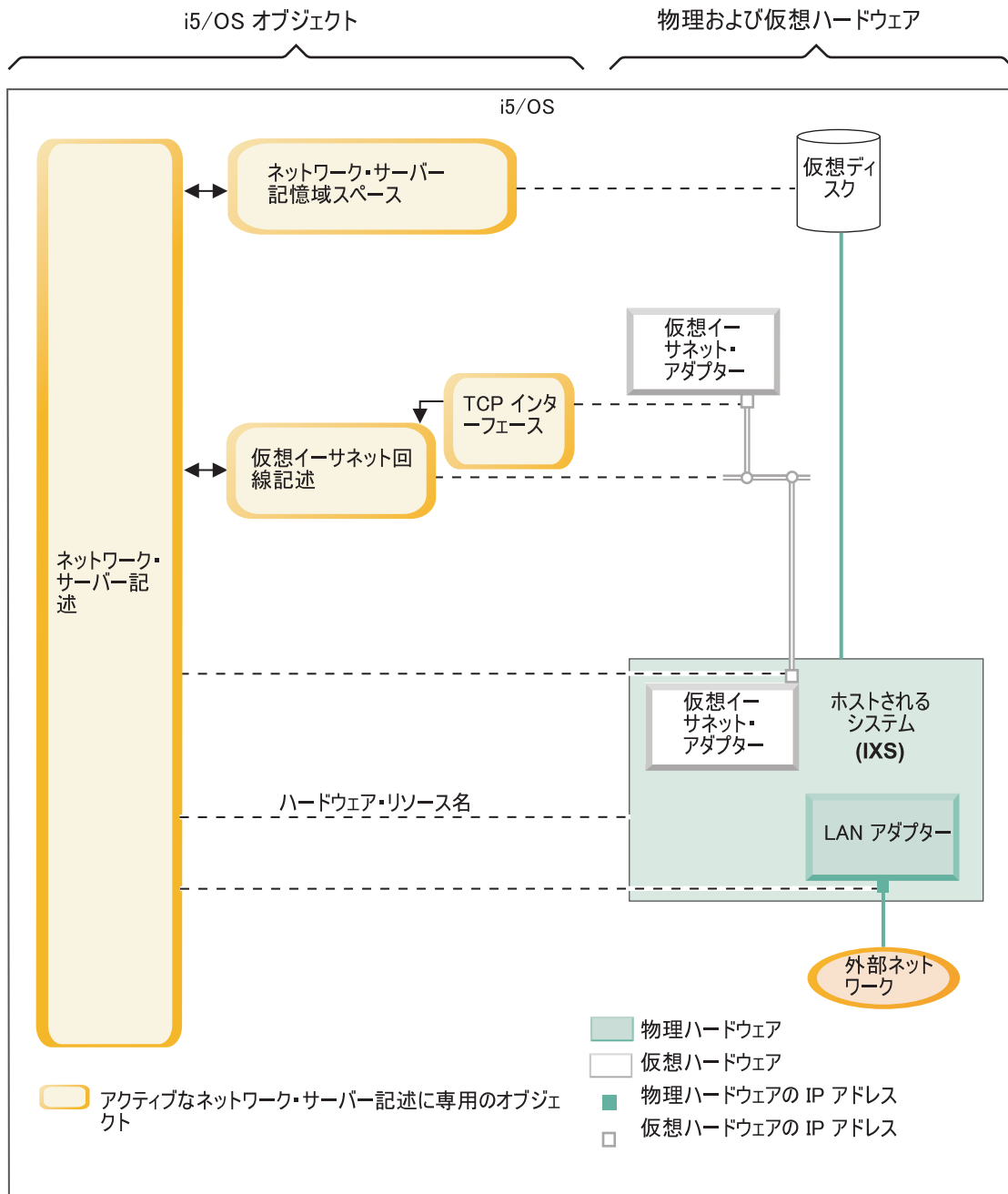
i5/OS は、統合サーバー・ハードウェアのタイプに関わりなく、統合サーバーの定義、構成、および管理を行うためのサポートを提供します。さまざまなハードウェア構成に使用される i5/OS オブジェクトの説明については、以下の図をご覧ください。サポートされるハードウェア構成の説明については、14 ページの『ハードウェアの概念』を参照してください。

i5/OS ソフトウェア構成に関する詳細については、以下の情報を参照してください。

- 『統合 xSeries サーバー (IXS) と統合 xSeries アダプター (IXA) 接続 xSeries サーバー』
- 43 ページの『iSCSI 接続の xSeries および IBM BladeCenter サーバー』
- 47 ページの『セキュリティーのある iSCSI 接続の xSeries および BladeCenter サーバー』

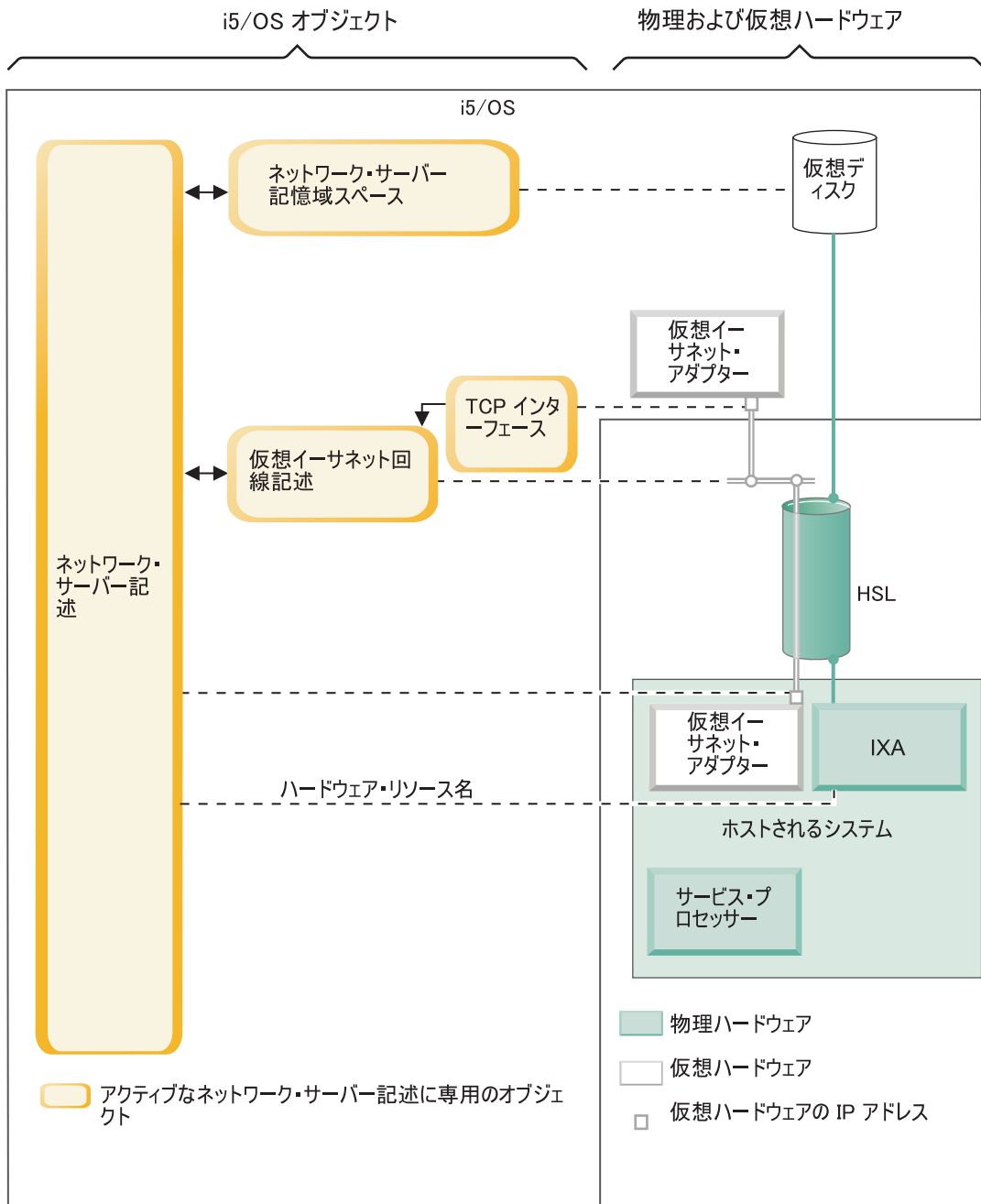
統合 xSeries サーバー (IXS) と統合 xSeries アダプター (IXA) 接続 xSeries サーバー

i5/OS は、IXS 接続と IXA 接続の xSeries サーバーを同様の方法で表します。



RZAHQ508-3

図 13. i5/OS 内の IXS 構成オブジェクト



RZAHQ504-2

図 14. i5/OS 内の IXA 構成オブジェクト

図 14 は、IXS 接続および IXA 接続の xSeries サーバーのための重要な i5/OS オブジェクトと重要なハードウェア・コンポーネントを示します。

39 ページの図 13 と 図 14 のオブジェクトを説明する以下のセクションを参照してください。

- 41 ページの『ネットワーク・サーバー記述』
- 41 ページの『ハードウェア・リソース名』
- 41 ページの『ネットワーク・サーバー記憶域スペース』
- 42 ページの『仮想イーサネット回線記述』
- 42 ページの『TCP/IP インターフェイス』

43 ページの『システム・バスおよび HSL データ・フロー』

ネットワーク・サーバー記述

39 ページの図 13 と 40 ページの図 14 のネットワーク・サーバー記述 (NWS D) は、すべてのタイプの統合サーバーの重要な i5/OS 構成オブジェクトです。NWS D オブジェクトは、統合サーバーに関係した他のすべての i5/OS オブジェクトを結合するために使用されます。このオブジェクトには、たとえばサーバーが実行されるハードウェアへの参照、サーバーが使用する仮想ディスク・ドライブへのリンク、サーバーが使用するネットワーク・ポートへの参照など、他にも多くのサーバーの属性が入っています。i5/OS の WINDOWS サーバー導入 (INSWNTSVR) コマンドを使用して、サーバーの NWS D とサーバーが必要とする他のいくつかの i5/OS オブジェクトを作成します。

NWS D 内の値の説明については、i5/OS のネットワーク・サーバー記述の作成 (CRTNWS D) コマンドを参照してください。

統合サーバーでは、IXS 接続および IXA 接続の xSeries サーバー・ハードウェアは i5/OS によって制御されます。

- 統合サーバーは、そのサーバー用の NWS D をオンに変更することにより、開始されます。これにより、Windows オペレーティング・システムのブート・プロセスが始動されます。

- 統合サーバーは、そのサーバー用の NWS D をオフに変更することにより、シャットダウンされます。これにより、Windows オペレーティング・システムのシャットダウン・プロセスが始動されます。

- IXS の場合、i5/OS は IXS ハードウェアと直接に通信して、始動およびシャットダウン・タスクを実行します。

- IXA 接続 xSeries サーバーの場合、i5/OS は高速リンク (HSL) バスを通して xSeries サーバーにインストールされている IXA と通信し、始動およびシャットダウン・タスクを開始します。IXA が今度は xSeries システムのサービス・プロセッサ (SP) と通信して始動およびシャットダウン・タスクを実行します。

注: IXA は xSeries サービス・プロセッサに配線して接続されているので、xSeries サービス・プロセッサの特性を構成するのに i5/OS オブジェクトは必要ありません。

ハードウェア・リソース名

IXS 接続と IXA 接続両方の xSeries サーバーにおいて、i5/OS はハードウェア・リソース名 (たとえば LIN23) でサーバー・ハードウェアを表します。IXS または IXA 接続の xSeries サーバーのためのハードウェア・リソース名への参照は NWS D オブジェクトに保管されます。39 ページの図 13 および 40 ページの図 14 を参照してください。

注: IXS または IXA 接続の xSeries サーバーが実行されるハードウェアは NWS D のハードウェア・リソース名を使って定義されるので、統合サーバーが実行されるハードウェアを切り替えるのは容易です。これは、IXS または IXA 接続の xSeries サーバーのハードウェアに障害が起こる状況で便利です。統合サーバーを障害が起こったハードウェアから互換性のある「ホット・スペア」ハードウェアにすぐに切り替えて、予備のハードウェアを使用して再始動できるからです。この「ホット・スペア」機能に関する詳細については、172 ページの『サーバー・ハードウェア間のホット・スペア』を参照してください。

ネットワーク・サーバー記憶域スペース

ネットワーク・サーバー記憶域スペース (NWSSTG) は、サーバーが使用する仮想ディスク・ドライブを表します。39 ページの図 13 および 40 ページの図 14 を参照してください。仮想ディスク・ドライブのサイズは各 1 MB から 1000 GB までさまざまです。サーバー構成に応じて最大 64 個の仮想ディスク・ドライ

1 ブを 1 台のサーバーにリンクすることができるので、統合サーバーの記憶容量は数ギガバイトから数十テ
1 ラバイトに及びます。仮想ディスク・ドライブはまずスタンドアロン・オブジェクトとして作成され、それ
1 を使用する統合サーバーの NWSD を識別することにより統合サーバーにリンクされます。

1 サーバーにはそれぞれ最低 2 つの INSWNTSVR コマンドによって自動的に作成される仮想ディスク・ド
1 ライブがありますが、ユーザー定義の仮想ディスク・ドライブも持つことができます。

1 • システム・ドライブ (通常 C: ドライブ) には、Windows サーバーのオペレーティング・システム
1 (Windows Server 2003 など) があります。

1 • インストール・ドライブ (通常 D: ドライブ) には、Windows サーバーのインストール・メディアのコ
1 ピーと Windows サーバーで実行される i5/OS 統合サーバー・サポート (製品 5722-SS1 オプション 29)
1 コードの一部があります。インストール・ドライブは Windows インストール・プロセス中に使用され、
1 サーバーが起動されるたびに構成情報を i5/OS からサーバーに渡すためにも使用されます。

1 • 追加のユーザー定義ドライブは通常サーバー・アプリケーションとデータのために使用されます。

1 仮想ディスク・ドライブのための実際のディスク記憶域は、i5/OS 統合ファイル・システム (IFS) から割り
1 振られます。仮想ディスク・ドライブは、デフォルト・システム・ディスク・プール (システム補助記憶域
1 プールまたはシステム ASP と呼ばれます) やユーザー定義ディスク・プールや独立ディスク・プール
1 (IASP) から割り振ることができます。

1 仮想ディスク・ドライブについて詳しくは、175 ページの『第 9 章 記憶域の管理』を参照してください。

1 注:

1 1. 仮想ディスク・ドライブは i5/OS IFS 内のオブジェクトなので、仮想ディスク・ドライブ・イメージ全
1 体は i5/OS 保管 (SAV) および復元 (RST) コマンドを使用してバックアップおよび復元することができ
1 ます。仮想ディスク・ドライブ上の個々のファイルは、i5/OS から IFS のネットワーク・クライアント
1 (QNTC) ファイル・システムのファイル・レベル・バックアップを使用して、またはネイティブの
1 Windows バックアップ・アプリケーションを使用して バックアップすることができます。詳しくは、
1 209 ページの『第 12 章 統合 Windows サーバーのバックアップと回復』を参照してください。

1 2. 記憶域スペースが IFS から割り振られていますが、統合サーバーがオンに変更されている間は記憶域操
1 作は IFS によって実行されません。つまり、ジャーナリングのような操作は使用可能ではないというこ
1 とです。

1 仮想イーサネット回線記述

1 仮想イーサネット回線記述は、統合サーバーが参加する iSeries 仮想イーサネット・ネットワークを構成す
1 るのに使用されます。39 ページの図 13 および 40 ページの図 14 を参照してください。回線記述は、統
1 合サーバーがサーバーの Point-to-Point 仮想イーサネット・ネットワークを通じて i5/OS と通信するよう
1 に構成するのに使用されます。回線記述は、統合サーバーが区画内もしくは区画間仮想イーサネット・ネット
1 ワークを通じて他の統合サーバーや他の論理区画と通信するように構成するのにも使用されます。仮想イー
1 サネット・ネットワークについての詳細は、29 ページの『ネットワークングの概念』を参照してくださ
1 い。

1 注: 統合サーバーにある物理ネットワーク・アダプターのために LIND を使用することはありません。物
1 理アダプターは、Windows から通常の Windows ネットワーク・アダプター構成方法を使用して構成し
1 ます。

1 TCP/IP インターフェース

1 TCP/IP インターフェースは、Point-to-Point 仮想イーサネット・ネットワークの i5/OS 側の終端の TCP/IP
1 アドレスを構成するのに使用されます。39 ページの図 13 および 40 ページの図 14 を参照してくださ
1 い。

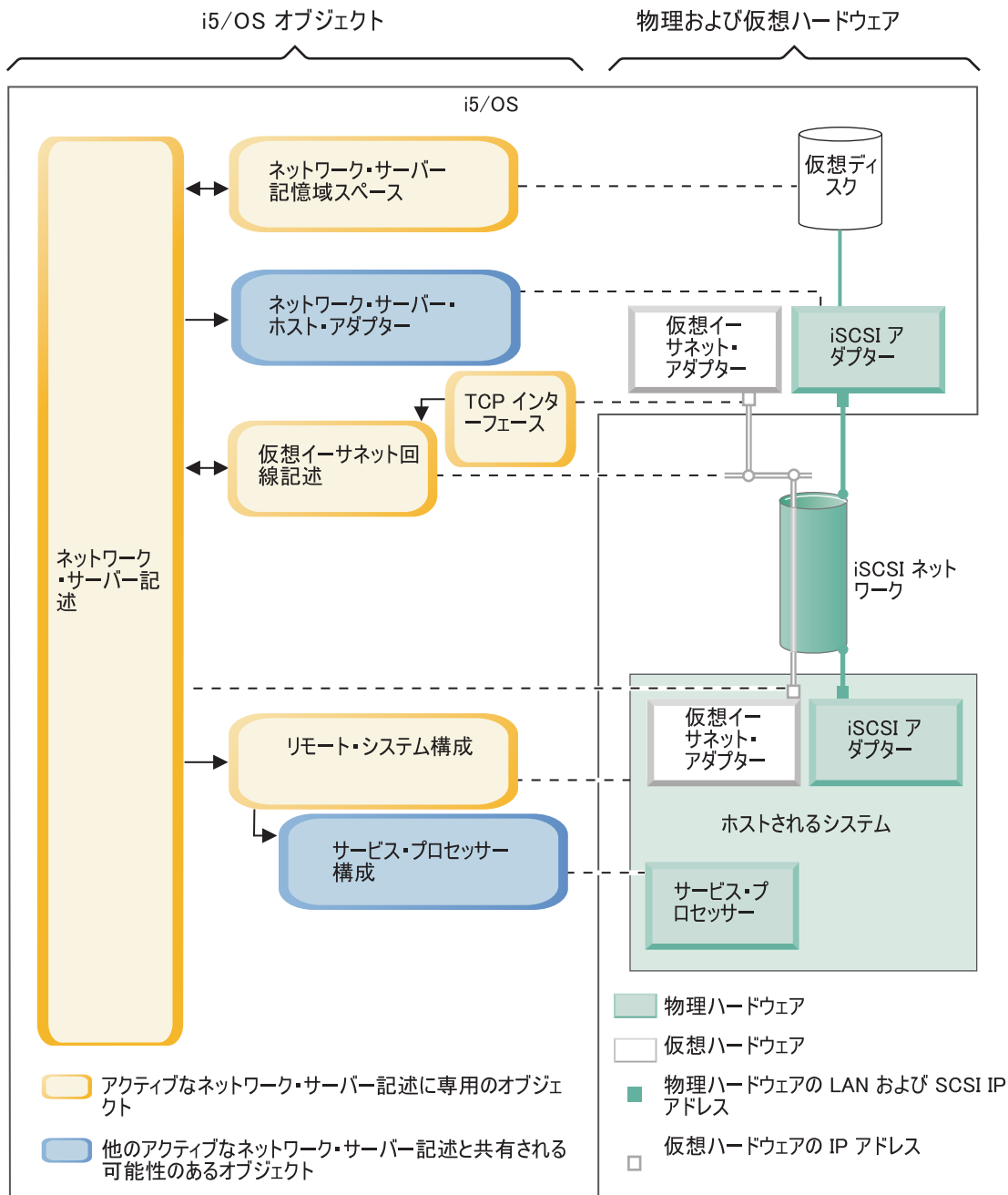
注: Point-to-Point 仮想イーサネット・ネットワークの Windows 側終端の TCP/IP アドレスは、NWSD の「TCP/IP ポート構成 (TCPPORTCFG)」パラメーターを通して構成されます。

システム・バスおよび HSL データ・フロー

i5/OS と統合サーバーの間のディスク・ドライブ SCSI および仮想イーサネットのデータは、iSeries システム・バス (IXS の場合) または I/O と iSeries システム間的高速リンク (HSL) 接続 (IXA の場合) を通じて流れます。39 ページの図 13 および 40 ページの図 14 を参照してください。実質的には、ディスク・ドライブ SCSI および仮想イーサネットのプロトコルは、通常の iSeries システム・バス/HSL データ転送プロトコル内にカプセル化またはトンネル化されます。

iSCSI 接続の xSeries および IBM BladeCenter サーバー

i5/OS は、IXS および IXA 接続の xSeries サーバーを表すのと同様の方法で、iSCSI 接続の xSeries および IBM BladeCenter サーバーを表します。しかし、iSCSI テクノロジーでは、IXS および IXA 接続の xSeries サーバーの場合には必要でない追加の i5/OS オブジェクトと構成情報が必要です。iSCSI 接続サーバーは (IXS および IXA の場合に使用されるシステム・バス / HSL 接続ではなく) イーサネット・ネットワークを使用して iSeries システムに接続されるので、ネットワーク上の xSeries または IBM BladeCenter サーバーを識別し通信するのに追加の構成情報が必要です。さらに、iSCSI 接続サーバーはイーサネット・ネットワーク上で他のシステムと共存できるので、i5/OS と iSCSI 接続サーバー間の通信およびデータ・フローのセキュリティーは懸念材料になり得ます。以下の図は、iSCSI 接続サーバーが i5/OS によってどのように表されるかを示します。



RZAHQ505-1

図 15. ネットワーク・セキュリティのない i5/OS iSCSI 構成オブジェクト

図 15 は、ネットワーク・セキュリティを使用しない場合に、iSCSI 接続 xSeries または IBM BladeCenter サーバーのために使用される重要な i5/OS オブジェクトと重要なハードウェア・コンポーネントを示します。

図 15 のオブジェクトを説明する以下のセクションを参照してください。

- 45 ページの『ネットワーク・サーバー・ホスト・アダプター』
- 45 ページの『リモート・システム構成』
- 46 ページの『サービス・プロセッサ構成』
- 46 ページの『ネットワーク・サーバー記述』

- 47 ページの『ネットワーク・サーバー記憶域スペース』
- 47 ページの『データ・フロー』
- 42 ページの『仮想イーサネット回線記述』
- 42 ページの『TCP/IP インターフェース』

ネットワーク・セキュリティーがある iSCSI 接続の xSeries および IBM BladeCenter サーバーのために使用される i5/OS オブジェクトに関する詳細については、48 ページの図 16 を参照してください。

ネットワーク・サーバー・ホスト・アダプター

44 ページの図 15 に示されるネットワーク・サーバー・ホスト・アダプター (NWSH) 装置記述オブジェクトは、以下のようにして、iSCSI 接続の iSeries 側が使用する iSCSI ホスト・バス・アダプター (HBA) を表します。

- iSCSI HBA の iSeries ハードウェア・リソース名 (たとえば LIN33) を識別します。
- 通信エラーを記録する方法と通信回復情報を定義します。
- iSCSI HBA の SCSI および LAN インターフェースのためのインターネット・アドレス、ポートなどを定義します。

iSeries はそれぞれ関連した NWSH オブジェクトがある iSCSI HBA を複数持つことができます。

- NWSH はそれぞれ複数の統合サーバーで共用できます。帯域幅が問題にならない構成の場合、これはコストのかからないソリューションになります。
- 統合サーバーはそれぞれ複数の NWSH を使用することができます。こうすると、iSeries と xSeries または IBM BladeCenter システムの間で複数の SCSI および仮想イーサネットのデータ・パスが使えるようになり、帯域幅と接続冗長度を大きくすることができます。

リモート・システム構成

リモート・システム・ネットワーク・サーバー構成 (NWSCFG タイプ RMTSYS) オブジェクト (44 ページの図 15 に示されている) は、以下のようにして、iSCSI 接続 xSeries または IBM BladeCenter サーバーを表します。

- シリアル番号、タイプ、およびモデルによってサーバー・ハードウェアを識別します。
- xSeries または IBM BladeCenter サーバーが使用する iSCSI ホスト・バス・アダプター (HBA) の構成情報を含みます。
- サーバーをブートするのに必要な値 (どの iSCSI アダプターからブートするかを指定するなど) を含みます。
- xSeries または IBM BladeCenterサーバーを制御するのに使用されるサービス・プロセッサ NWSCFG オブジェクト (以下参照) への参照を含みます。
- リモート・システム構成には、サーバー・ブート・プロセスを保護するのに使用される値をオプションで含めることができます。

xSeries または IBM BladeCenter サーバーは複数の iSCSI HBA を持つことができます。こうすると、iSeries と xSeries または IBM BladeCenter システムの間で複数の SCSI および仮想イーサネットのデータ・パスが使えるようになり、帯域幅と接続冗長度を大きくすることができます。

統合サーバーのためのリモート・システム構成オブジェクトは、NWSD のパラメーターを使って参照されます。

サービス・プロセッサ構成

サービス・プロセッサ構成(NWSCFG タイプ SRVPRC) オブジェクト (44 ページの図 15 に示されている) は、以下のようにして、xSeries サービス・プロセッサまたは IBM BladeCenter 管理モジュールを表します。

- シリアル番号、タイプ、およびモデルでサービス・プロセッサまたは管理モジュールのハードウェアを識別します。
- インターネット・アドレスやホスト名を使用して、イーサネット・ネットワーク上でサービス・プロセッサや管理モジュールを検出する方法を定義します。
- サービス・プロセッサ・オブジェクトには、i5/OS からサービス・プロセッサへの通信を保護するために使用される値をオプションで含めることができます。

注: iSCSI 接続 xSeries サーバーの場合、サービス・プロセッサが制御するのはそれぞれ 1 台の xSeries サーバーだけなので、サービス・プロセッサ・オブジェクトとリモート・システム構成の間には 1 対 1 の関係があります。しかしながら、iSCSI 接続 IBM BladeCenter サーバーの場合、各管理モジュールは IBM BladeCenter シャーシ内部にある IBM BladeCenter サーバーのどれでも制御できるので、サービス・プロセッサ・オブジェクトとリモート・システム構成の間関係は 1 対多になる場合があります。そのため、iSCSI 接続 IBM BladeCenter サーバーでは、いくつかのリモート・システム構成が同じサービス・プロセッサ・オブジェクトを共用 (参照) するのが一般的です。

ネットワーク・サーバー記述

44 ページの図 15 に示されるネットワーク・サーバー記述 (NWS) オブジェクトは、基本的に、40 ページの図 14 での説明と以下の点を除いて同じです。

- 含まれるのは iSeries ハードウェア・リソース名ではなく、リモート・システム構成オブジェクトへの参照です。
- xSeries システム内の 1 つの IXA カードを使用して SCSI および仮想イーサネット・データ・フローのすべてを管理する IXA 接続サーバーと違い、iSCSI 接続サーバー・ソリューションでは iSeries および xSeries の両方が複数の iSCSI ホスト・バス・アダプター (HBA) を持つことができます。こうすると、iSeries と xSeries または IBM BladeCenter システムの間で複数の SCSI および仮想イーサネットのデータ・パスが使えるようになり、帯域幅と接続冗長度を大きくすることができます。
- 1 つ以上の記憶域パスを定義できます。これらの記憶域パスは、統合サーバーが使用する iSCSI HBA と関連した NWSH オブジェクトを参照します。仮想ディスク・ドライブごとに SCSI データ・フローのためにどの記憶域パスを使用するかを選ぶことができます。仮想ディスク・ドライブを異なる記憶域パスに関連付けることにより、サーバー SCSI データ・フローの負荷全体を記憶域パスの iSCSI HBA に分散させて帯域幅を高めることができます。
- マルチパス・グループを定義できますが、これは構成された記憶域パスのサブセットです。それから、仮想ディスク・ドライブを特定の記憶域パスと関連付けるのではなく、このマルチパス・グループと関連付けることができます。仮想ディスク・ドライブのためにマルチパス・グループを使用することには、マルチパス内の NWSH の 1 つのための iSCSI HBA に障害が起きたり、iSCSI HBA へのネットワーク接続に障害が起きた場合、その仮想ディスク・ドライブのための SCSI データ・フロー作業負荷は自動的にマルチパス・グループ内に構成された他の iSCSI HBA の 1 つに経路指定されるという利点があります。これにより、接続が冗長になり、可用性が向上します。
- 1 つ以上の仮想イーサネット・パスを定義できます。これらの仮想イーサネット・パスも、統合サーバーが使用する NWSH オブジェクトを参照します。統合サーバーが使用する仮想イーサネット・ポートのそれぞれにどの NWSH を使用するかを選ぶことができます。異なる仮想イーサネット・ポートを異なる NWSH と関連付けることにより、サーバー仮想イーサネット・データ・フローの作業負荷全体を仮想イーサネット・パスの iSCSI HBA に分散させて帯域幅を高めることができます。

- | • IXS または IXA 接続サーバーがそうであるように、iSCSI 接続の xSeries または IBM BladeCenter サーバー・ハードウェアは i5/OS によって制御されます。
 - | - iSCSI 接続サーバーは、IXS または IXA 接続サーバー（40 ページの図 14 を参照）と同じように、そのサーバー用の NWS D をオンまたはオフに変更することにより始動したりシャットダウンしたりできます。
 - | - iSCSI 接続の xSeries または IBM BladeCenter サーバーの場合、i5/OS はイーサネット・ネットワークを通じて xSeries システム用のサービス・プロセッサ（SP）や IBM BladeCenter サーバー用の IBM BladeCenter 管理モジュールと通信を行い、始動およびシャットダウン・タスクを実行します。
- | サーバー・ハードウェアの電源制御に関して、IXS/IXA 構成と iSCSI 構成の間の主な違いは、IXS または IXA 接続サーバーの場合、サーバー・ハードウェアは iSeries ハードウェア・リソース名によって識別されるのに対し、iSCSI 接続サーバーではサーバー・ハードウェアはリモート・システム構成オブジェクトによって識別されるということです。

| 注: iSCSI 接続サーバーが実行される xSeries または IBM BladeCenter サーバーは単純に NWS D のリモート・システム構成名を使って定義されるので、iSCSI 接続統合サーバーが実行されるハードウェアを切り替えるのは容易です。リモート・システム構成名を変更することにより、既存の NWS D でブートされた xSeries または IBM BladeCenter サーバーのホット・スワップを行うことができます。詳しくは、172 ページの『サーバー・ハードウェア間のホット・スワップ』を参照してください。

| ネットワーク・サーバー記憶域スペース

| 44 ページの図 15 に示されるネットワーク・サーバー記憶域スペース (NWSSTG) は、基本的に、40 ページの図 14 (上記) での説明と以下の点を除いて同じです。

- | • 仮想ディスク・ドライブを NWS D にリンクする際に、どの NWS D の記憶域パスをその仮想ディスク・ドライブのための SCSI データ・フローに使用するかを識別することが必要です。
- | • 特定のパスやマルチパス・グループを選択することも、デフォルトの記憶域パスが使用されるようにすることもできます。

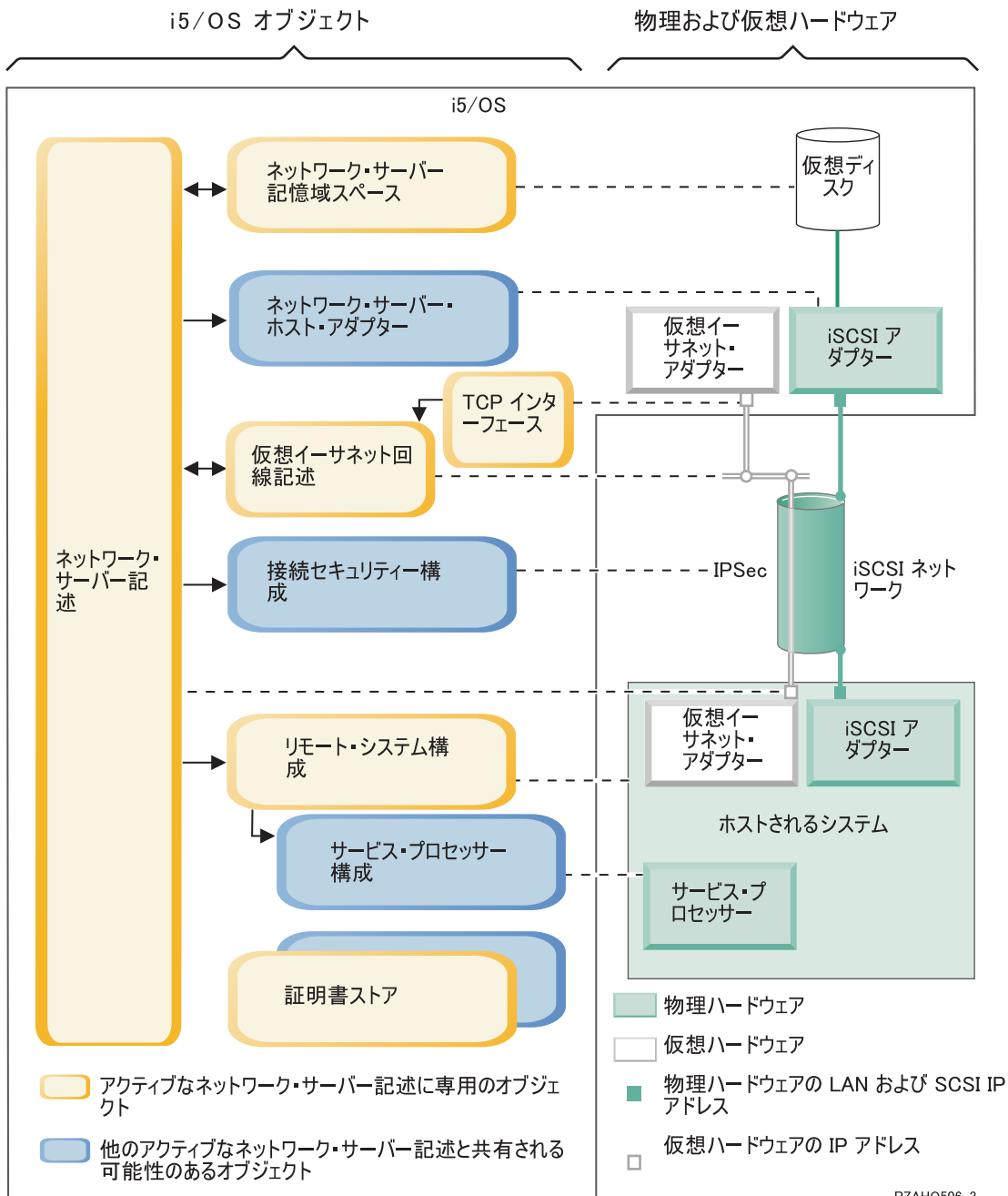
| 詳しくは、41 ページの『ネットワーク・サーバー記憶域スペース』を参照してください。

| データ・フロー

| 44 ページの図 15 において、i5/OS と iSCSI 接続統合サーバーの間のディスク・ドライブ SCSI および仮想イーサネットのデータは、イーサネット・ネットワークを通して流れます。実質的には、ディスク・ドライブ SCSI および仮想イーサネットのプロトコルは、通常のイーサネット・ネットワーク・プロトコル内にカプセル化またはトンネル化されます。

| セキュリティーのある iSCSI 接続の xSeries および BladeCenter サーバー

| iSCSI 接続サーバーは他のシステムとネットワークを共用できるので、iSCSI およびサービス・プロセッサのネットワーク接続を保護することが必要な場合があります。次の図は、i5/OS が iSCSI 接続サーバーのネットワーク・セキュリティを構成するのに使用するオブジェクトを示します。



RZAHQ506-3

図 16. ネットワーク・セキュリティーのある i5/OS 内の iSCSI 構成オブジェクト

図 16 は、ネットワーク・セキュリティーを使用する場合に、iSCSI 接続 xSeries または IBM BladeCenter サーバーのために使用される重要な i5/OS オブジェクトと重要なハードウェア・コンポーネントを示します。

図 16 内のオブジェクトを説明する以下のセクションを参照してください。

- 49 ページの『リモート・システム構成』
- 49 ページの『サービス・プロセッサ構成』
- 49 ページの『接続セキュリティー構成』
- 49 ページの『証明書ストア』

- 46 ページの『ネットワーク・サーバー記述』
- 47 ページの『ネットワーク・サーバー記憶域スペース』
- 47 ページの『データ・フロー』
- 42 ページの『仮想イーサネット回線記述』
- 42 ページの『TCP/IP インターフェース』

リモート・システム構成

48 ページの図 16 に示されるリモート・システム・ネットワーク・サーバー構成 (NWSCFG タイプ RMTSYS) オブジェクトは、記憶域に最初にアクセスする際にリモート・システムを認証するのに使用されるチャレンジ・ハンドシェイク認証プロトコル (CHAP) 構成値を持っていることを除けば、44 ページの図 15 に関する 45 ページの『リモート・システム構成』の説明と同じです。

サービス・プロセッサ構成

48 ページの図 16 に示されるサービス・プロセッサ・ネットワーク・サーバー構成 (NWSCFG タイプ SRVPRC) オブジェクトは、44 ページの図 15 に関する 46 ページの『サービス・プロセッサ構成』での説明と以下の点を除いて同じです。

- サービス・プロセッサにサインオンするために使用されるサービス・プロセッサ・ユーザー名とパスワードを持っています。
- i5/OS からサービス・プロセッサへの通信の保護に使用されるオプションの SSL 証明書を管理するために必要な情報を持っています。

接続セキュリティ構成

接続セキュリティ・ネットワーク・サーバー構成 (NWSCFG タイプ CNNSEC) オブジェクト (48 ページの図 16 に示されている) は、以下のように、i5/OS と iSCSI 接続 xSeries または IBM BladeCenter サーバーの間の SCSI および仮想イーサネットデータ・フローを保護するのに使用されます。

- さまざまな記憶域および仮想イーサネット接続とともに使用される IP セキュリティ (IPSec) 規則のセットを識別します。
- どのデータ・フローを保護して、どのデータ・フローを保護しないかを定めることができます。記憶域または仮想イーサネット接続を保護しない、一部保護する、またはすべて保護することを選択できます。たとえば、記憶域 (SCSI) データ・フローだけ、または仮想イーサネット接続の 1 つだけを保護するように選択できます。
- NWSD の記憶域パスおよび仮想イーサネット・パスに適切なセキュリティ規則を指定することにより、どの SCSI および仮想イーサネットのデータ・フローを保護するかを識別します。
- IPSec を使用する場合、i5/OS と iSCSI 接続統合サーバーの間の SCSI および仮想イーサネットのデータ・フローは暗号化され、通常のイーサネット・ネットワーク・プロトコル内のカプセル化 (トンネル化) の追加層を持つようになります。

証明書ストア

証明書は、さまざまな機能に関して i5/OS とホストされるシステム間の通信を保護するのに使用されます。証明書は以下の i5/OS 証明書ストアに保持されます。

- i5/OS システム証明書ストア。** ホストされるシステムのサービス・プロセッサに外部ソースから証明書を手動でインポートする場合、この証明書ストアが対応するトラステッド・ルート CA 証明書を保管する場所です。システム証明書ストアは、多くの i5/OS アプリケーションによって共有されます。
- サービス・プロセッサ構成と関連付けられた証明書ストア。** この証明書ストアは自動的に作成されません。この証明書ストアの証明書は、対応するサービス・プロセッサ構成を使用するホストされるシス

- | テムと通信する場合にだけ使用されます。複数のホストされるシステム (たとえば、IBM BladeCenter プ
- | レード) が同じサービス・プロセッサ構成を使用している場合、この証明書ストアは共有されます。以
- | 下の場合に、証明書はこの証明書ストアに置かれます。
- |- サービス・プロセッサ構成オプションを使用して、証明書を生成する。
- |- ホストされるシステムのサービス・プロセッサからの証明書を、対応するサービス・プロセッサ
- | 構成に同期する。
- **ネットワーク・サーバー記述と関連付けられた証明書ストア。** この証明書ストアは自動的に作成・保守
- | されます。i5/OS 統合サーバー・サポートが内部的に生成・使用する証明書 (たとえば、ユーザーをホ
- | ストされるシステムに登録するとき使用される証明書) を保管するのに使用されます。この証明書スト
- | アの証明書は、対応するネットワーク・サーバー記述を使用するホストされるシステムと通信する場合
- | だけに使用されます。

高可用性の概念

| iSeries と xSeries の統合と記憶域仮想化は、Windows サーバー環境の信頼性と復元可能性を向上させるこ
| とを可能にする革新的なオプションを提供します。ホストされるシステムは、以下のテクノロジーのうちの
| 1 つ以上を使用して、可用性を向上させることができます。

ホット・スペア・ハードウェア

| ホット・スペア・ハードウェアは、ある種のハードウェア障害から迅速に回復する手段を提供します。これ
| により、サーバー・ダウン時間は、時間や日の単位から分の単位に短くすることができます。ホストされる
| システムの場合、ハードウェア障害が引き起こしたダウン時間を最小にするためにホット・スペア・ハード
| ウェアを使用するための 2 つの方法があります。

1. 統合 xSeries サーバー、統合 xSeries アダプターを使って接続された xSeries サーバー、および iSCSI
| ホスト・バス・アダプターを通じて接続された xSeries または IBM BladeCenter サーバーを含むホスト
| されるシステムのハードウェアはホット・スペアすることができます。ホストされるサーバーを実行す
| るのに使用するハードウェアに障害が起こると、すぐにホストされるシステムのディスク・イメージを
| 互換性のあるスペア・ハードウェアに切り替えて、ホストされるシステムを再始動することができます
| す。詳しくは、172 ページの『サーバー・ハードウェア間のホット・スペア』を参照してください。
2. iSCSI 接続サーバーの場合、iSeries ターゲット iSCSI ホスト・バス・アダプター (iSCSI HBA) をホッ
| ト・スペアすることができます。ホストされるシステムが使用している iSCSI HBA に障害が起こった
| ら、ホストされるシステムをすぐにスペアの iSCSI HBA を使用するように切り替え、ホストされるシ
| ステムを再始動することができます。詳しくは、146 ページの『iSCSI ローカル・ホスト・アダプター
| 間のホット・スペア』を参照してください。

iSCSI マルチパス

| ホストされるシステムは、i5/OS がホストする仮想ディスクにアクセスする冗長 iSCSI データ・パスを使
| 用することができます。これは、複数の iSCSI HBA のグループを定義してから、特定の仮想ディスクが単
| 一の iSCSI HBA ではなくグループを使用してアクセスするように指定することによって、実現することが
| できます。この構成にすると、仮想ディスク上のデータにはグループ内の iSCSI HBA のいずれかを使用し
| てアクセスできるようになります。

| マルチパス構成の 1 つの利点は、マルチパス・グループ内の iSCSI HBA に障害が起こった場合、ホスト
| されるシステムはマルチパス・グループを使用するように構成されたディスクに、マルチパス・グループ内
| 構成された他の iSCSI HBA のいずれかを使用して、中断無しでアクセスし続けられるということです。詳
| しくは、22 ページの『拡張 iSCSI サポート』を参照してください。

Microsoft Windows クラスタ・サービス (MSCS)

ホストされるサーバーは、MSCS を使用して、ホストされるシステムのハードウェアまたはソフトウェア障害が起きた場合にリアルタイム・アプリケーション・フェイルオーバーを提供することができます。ユーザーが開始したフェイルオーバーは、クラスタ内の他のサーバーでアプリケーションの実行を続けながら、保守やバックアップを実行することができるように、サーバーをオフラインにするのに使用することができます。詳しくは、109 ページの『Windows クラスタ・サービス』を参照してください。

セキュリティの概念

このセクションに説明されているセキュリティの概念をインプリメントする手順については、141 ページの『i5/OS とホストされるシステムとの間のセキュリティの構成』を参照してください。考慮すべきセキュリティのタイプがいくつかあります。

- 『IXS および IXA 接続システムのセキュリティ』
- 『iSCSI 接続システムのセキュリティ』

IXS および IXA 接続システムのセキュリティ

IXS および IXA 接続システムの記憶域データと仮想イーサネット通信は、物理的にセキュアな iSeries システム・バスと HSL ケーブルを通じて流れます。

iSCSI 接続システムのセキュリティ

iSCSI テクノロジーは、低コストで広く使われているイーサネットと IP ネットワーキングを活用します。イーサネットと IP ネットワーキングは柔軟なので、iSCSI 接続システムはハードウェアを共用し、範囲を拡張し、ハードウェアの追加によって帯域幅を高めることができます。しかし、このように広く使用されていることと柔軟性のために、ふさわしいネットワーク・セキュリティが必要になります。

iSCSI 接続システムが使用するさまざまなネットワークのタイプごとに、異なるセキュリティ上の考慮事項があります。

サービス・プロセッサ接続のセキュリティ

サービス・プロセッサのセキュリティには、以下のメカニズムの 1 つ以上が関係する場合があります。

- サービス・プロセッサ・パスワード
- Secure Sockets Layer (SSL)
- ネットワーク分離と物理的セキュリティ

iSCSI ネットワークのセキュリティ

考慮すべき iSCSI ネットワーク・トラフィックには以下の 2 つのタイプがあります。

- 記憶域のセキュリティには、以下のメカニズムの 1 つ以上が関係する場合があります。
 - チャレンジ・ハンドシェイク認証プロトコル (CHAP)
 - IP セキュリティ (IPSec)
 - ファイアウォール
 - ネットワーク分離、物理的セキュリティ、およびセキュリティ・ゲートウェイ
- 仮想イーサネットのセキュリティには、以下のメカニズムの 1 つ以上が関係する場合があります。
 - IP セキュリティ (IPSec)
 - ファイアウォール

- ネットワーク分離、物理的セキュリティ、およびセキュリティ・ゲートウェイ
- さらに、Point-to-Point 仮想イーサネットを使ってユーザー登録やリモート・コマンド投入が機密データを送信する場合、これらのアプリケーションは i5/OS と Windows の間で Secure Sockets Layer (SSL) 接続を使用します。ユーザー登録について詳しくは、54 ページの『ユーザーおよびグループの概念』を参照してください。

サービス・プロセッサ・パスワード

このパスワードは i5/OS によって管理され、iSeries サーバーがホストされるシステムのサービス・プロセッサと会話を開始するときに使用されます。サービス・プロセッサはパスワードを検査して、i5/OS 構成が信頼できることを確認します。新規のサービス・プロセッサはデフォルトの名前とパスワードを持っています。i5/OS がパスワードの変更方法を提供します。

サービス・プロセッサ Secure Sockets Layer (SSL)

このタイプの SSL は、それにながったタイプのサービス・プロセッサ・ハードウェアがある場合だけ、使用可能にすることができます。使用可能にされると、SSL はサービス・プロセッサ接続のトラフィックを暗号化し、サービス・プロセッサが信頼できることを確認します。認証は、自動的にまたは手動で i5/OS にインストールされているサービス・プロセッサからのデジタル証明書に基づいて行われます。この証明書は、i5/OS と Windows の間の SSL 接続に使用されるデジタル証明書とは別のものです。

i5/OS と Windows の間の Secure Sockets Layer (SSL) 接続

iSeries 上の Windows 環境には、ユーザー登録とリモート・コマンド投入機能が含まれますが、これらの機能は Point-to-Point 仮想イーサネットを通して機密データを転送する場合があります。これらのアプリケーションは自動的に SSL 接続をセットアップしてその機密ネットワーク・トラフィックを暗号化し、自動的にインストールされたデジタル証明書に基づいて、会話の両方の側が信頼できることを確認します。これらの証明書は、サービス・プロセッサ SSL に使用されるデジタル証明書とは別のものです。このセキュリティ機能はデフォルトで提供され、構成可能ではありません。ファイル・データ、コマンド結果、および他のアプリケーションのトラフィックは、この SSL 接続によって保護されません。

チャレンジ・ハンドシェイク認証プロトコル (CHAP)

CHAP は、記憶域にアクセスするのに無許可システムが許可されたシステムの iSCSI 名を使用する可能性に対する保護を行います。CHAP はネットワーク・トラフィックの暗号化は行いませんが、i5/OS 記憶域パスにどのシステムがアクセスできるかを制限します。

CHAP には、i5/OS とホストされるシステムの両方が知らなければならない機密事項を構成することが関係します。短い CHAP 機密事項は、CHAP パケット交換が LAN 盗聴プログラムによって記録されオフラインで分析されれば、明らかになってしまいます。CHAP 機密事項は、十分ランダムで長いために、この方法による攻撃が実際的でないようにしなければなりません。i5/OS は適切な機密事項を生成することができます。ホストされるシステムは、同じ CHAP 機密事項を使用して、その構成された i5/OS 記憶域パスのすべてにアクセスします。

CHAP はデフォルトでは使用可能ではありませんが、その使用を強くお勧めします。

IP セキュリティ (IPSec)

IPSec は iSCSI ネットワーク上の記憶域および仮想イーサネット・トラフィックを暗号化します。関連したプロトコルである Internet Key Exchange (IKE) が、通信を行う IP エンドポイントが信頼できることを確認します。

IPSec を使用可能にするには、以下の 2 つの条件が必要です。

1. iSeries とホストされるシステムの両方に、高速 IPSec サポートを持った特別の iSCSI HBA がなければなりません。

2. 事前共有キーを構成しなければなりません。i5/OS は適切な事前共有キーを生成することができます。iSeries またはホストされるシステムで複数の iSCSI HBA が関係している場合、異なる IP アドレス・ペアに異なる事前共有キーを割り当てることができます。IPSec と IKE の他の詳細はすべて自動的に処理されます。i5/OS TCP/IP および Windows TCP/IP の IPSec サポートは関係しません。

IPSec HBA は、構成されていない IP アドレスとの通信をブロックするフィルター機能を提供します。事前共有キーを提供することによって IPSec 暗号化を使用可能にしていなくても、IPSec HBA はこのフィルタリングを実行します。

仮想イーサネットで使用されると、IPSec は仮想イーサネットのエンドポイントに直接は適用されず、iSCSI ネットワークを通り抜けるトンネルになる iSCSI HBA に適用されます。したがって、複数の iSCSI 接続 Windows サーバーが仮想イーサネットでお互いと通信する場合、各サーバーの IPSec は他のものから独立しています。たとえば、あるサーバーが IPSec を使用可能にして、IPSec ではなく物理的セキュリティを使用している他の Windows サーバーと通信するようにすることが可能です。サーバーは、お互いに通信するのに、同じ IPSec 事前共有キーを使用する必要はありません。

ファイアウォール

ファイアウォールは、iSeries を望ましくないネットワーク・トラフィックから保護するために、共用ネットワークと iSeries の間に使用することができます。同様に、ファイアウォールはホストされるシステムを望ましくないネットワーク・トラフィックから保護するために、共用ネットワークとホストされるシステムの間にも使用することもできます。

iSCSI 接続システムのトラフィックには、ファイアウォールを構成する場合に助けになる以下の属性があります。

- iSCSI HBA は静的 IP アドレスを持っています (DHCP ブート・モードがありますが、実際には関係する IP アドレスは静的に事前構成されています)。
- 決定論で、構成可能な UDP および TCP ポート。ホストされるシステムの仮想イーサネット・アダプターはそれぞれ異なる UDP ポートを使用して iSCSI ネットワークを通り抜けるトンネルとします。仮想イーサネット・パケットは、外部ヘッダーから内部ヘッダーまで以下のようにカプセル化されます。
 - LAN (SCSI でなく) アドレスを使用する iSCSI HBA 用の MAC および IP ヘッダー。
 - UDP ヘッダー。オプションとして UDP ポート選択を制御することに関する情報については、145 ページの『ファイアウォールの構成』を参照してください。
 - 仮想イーサネット・アダプター用の MAC および IP ヘッダー。

IPSec HBA は、事前共有キーを提供することによって IPSec を使用可能にしていなくても、構成されていない IP アドレスとの通信をブロックするファイアウォールのような機能を提供します。

ネットワーク分離と物理的セキュリティ

ネットワーク分離は、ネットワークを全探索するにあたり、無許可の装置によってデータがアクセスされたり、変更されたりするリスクを最小にします。分離されたネットワークの作成は、専用のイーサネット・スイッチを使用するか、物理的 VLAN スイッチ/ネットワーク上で専用の仮想ローカル・エリア・ネットワーク (VLAN) を使用することによって行えます。VLAN スイッチを構成する場合、iSeries サーバーにインストールされている iSCSI HBA を、VLAN に気付かない装置として扱います。

物理的セキュリティには、ネットワーク装置やネットワーク・エンドポイントへのアクセスをなんらかのレベルで制限する物理的バリア (ロックされる格納装置、ロックされる部屋、ロックされる建物など) が含まれます。

ユーザーおよびグループの概念

iSeries Windows 環境を使用する主な利点の 1 つは、i5/OS と Windows のユーザー・プロファイルのユーザー管理機能です。ユーザー管理機能によって管理者は、既存の i5/OS ユーザーおよびグループ・プロファイルを Microsoft Windows に登録することができます。このセクションでは、この機能の詳細を説明します。

登録

登録 (enrollment) とは、i5/OS ユーザーまたはグループ・プロファイルを統合ソフトウェアに登録する処理です。

登録処理は、ユーザーまたはグループを登録する CHGNWSUSRA コマンドの実行、登録済み Windows ユーザーによる i5/OS ユーザー・プロファイル・パスワードまたはユーザー属性の更新、または統合サーバーの再始動など、イベントによってトリガーされることにより自動的に実行されます。統合 Windows サーバーがアクティブであれば、変更は即時に実行されます。統合サーバーがオフに変更されていれば、変更は次回サーバーが始動する際に実行されます。

Windows ドメインおよびローカル・サーバー

登録は、Windows ドメインまたはローカル・サーバーのいずれかに対して実行できます。Windows ドメインは、ネットワークによって相互に連結したリソース (アプリケーション、コンピューター、プリンター) の集まりです。ユーザーはドメイン全体に対して 1 つのアカウントを持ち、そのドメインにログオンするだけですべてのリソースにアクセスできます。統合サーバーは Windows ドメインのメンバー・サーバーとなって、複数の i5/OS ユーザー・アカウントを Windows ドメインに統合できます。

一方、i5/OS ユーザーをそのドメインの一部ではない統合サーバーに登録した場合、それは**ローカル・サーバー**と呼ばれ、ユーザー・アカウントはその統合サーバー上だけで作成されます。

注: Windows ネットワーキングでは、Windows ワークグループを使用することによって、ローカル・サーバーのグループを自由に参加させることができます。例えば、「マイ ネットワーク」を開いて「近くのコンピュータ」をクリックすると、同じワークグループにあるコンピューターのリストが表示されます。

Microsoft Windows i5/OS グループ

2 つのグループのユーザーが、Microsoft Windows 内での統合サーバーへのインストールの一部として作成されます。

- **AS400_Users** すべての i5/OS ユーザーが Windows 環境に最初に登録されると、そのユーザーは AS400_Users グループに入れられます。Windows 環境ではユーザーをこのグループから除去することができますが、iSeries サーバーからアップデートが次回実行された時点で、そのユーザーは復元されます。このグループは、どの i5/OS ユーザー・プロファイルが Windows 環境に登録されたかを調べるための場所として役立ちます。
- **AS400_Permanent_Users** iSeries サーバーはこのグループ内のユーザーを Windows 環境から除去することはできません。これは、i5/OS 内のアクションにより Windows ユーザーが間違って除去されてしまうことを防止するためです。ユーザー・プロファイルが i5/OS から削除された場合でも、そのユーザーは Windows 環境内には引き続き存在しています。AS400_Users グループとは異なり、このグループ内のメンバーシップは Windows 環境から制御されます。このグループからユーザーを削除した場合、i5/OS のアップデートを実行してもそのユーザーは復元されません。

i5/OS ユーザー・プロファイル LCLPWDMGT 属性の使用

ユーザー・プロファイルのパスワードを管理する方法には、次の 2 つがあります。

- **従来のユーザー** i5/OS パスワードと Windows パスワードとを同じにすることができます。i5/OS パスワードと Windows パスワードとを同じにするには、i5/OS ユーザー・プロファイル属性値を LCLPWDMGT(*YES) に指定します。LCLPWDMGT(*YES) と指定すると、登録されている Windows ユーザーはパスワードを i5/OS で管理することになります。LCLPWDMGT 属性を設定するには、i5/OS のユーザー・プロファイルの作成 (CRTUSRPRF) またはユーザー・プロファイルの変更 (CHGUSRPRF) コマンドを使用します。
- **Windows ユーザー** 登録された Windows プロファイル・パスワードを Windows 内で管理する方法もあります。LCLPWDMGT(*NO) を指定すると、i5/OS ユーザー・プロファイル・パスワードが *NONE に設定されます。そのように設定すると、登録された Windows ユーザーはパスワードを Windows 内で管理できるようになります。i5/OS がそのパスワードを上書きすることはありません。

56 ページの『ユーザー構成の種類』を参照してください。

i5/OS エンタープライズ識別マッピング (EIM) の使用

i5/OS EIM サポートを利用する 2 つの方法があります。EIM Windows レジストリー内の機能を使用して、自動的に EIM 関連を作成することができます。EIM 関連を定義すると、i5/OS で、Kerberos などの認証方式を使用する Windows シングル・サインオンがサポートされるようになります。Windows EIM ソース関連の自動作成および自動削除は、i5/OS のユーザー・プロファイルの作成 (CRTUSRPRF)、ユーザー・プロファイルの変更 (CHGUSRPRF)、またはユーザー・プロファイルの削除 (DLTUSRPRF) コマンドを使用し、その EIMASSOC パラメーター値に *TARGET、*TGTSRC、または *ALL を指定すると実行されます。

EIM 関連を EIM Windows レジストリーに手動で定義することもできます。EIM i5/OS ターゲット関連および Windows ソース関連が i5/OS ユーザー・プロファイルに定義される際、登録された i5/OS ユーザー・プロファイルは Windows 内の異なるユーザー・プロファイル名として定義されることがあります。

注: SBMNWSCMD、QNTC、およびファイル・レベル・バックアップ操作は EIM Kerberos 関連とだけ連動します。EIM Windows レジストリーを使用して異なる Windows ユーザー名にマップされた i5/OS ユーザー・プロファイルは認識されません。これらの操作は依然として同じ名前を使用するようになっています。

詳しくは、201 ページの『エンタープライズ識別マッピング (EIM)』を参照してください。

既存の Windows ユーザー・プロファイルの登録

Windows 環境に既に存在しているユーザーを登録することもできます。その場合、ユーザーのパスワードは、i5/OS 上でも、既存の Windows のユーザーまたはグループのパスワードと同じでなければなりません。59 ページの『パスワードについての考慮事項』を参照してください。

ユーザー登録テンプレート

ユーザー登録テンプレートを使用すると、登録時にユーザーが受け取る権限とプロパティをカスタマイズできます。58 ページの『ユーザー登録テンプレート』を参照してください。ユーザー登録時にテンプレートを使用しない場合、各ユーザーの設定値は、デフォルトで以下のようになります。

- ユーザーは、AS400_Users グループのメンバーになり、ローカル統合 Windows サーバー上の Users グループあるいは Windows ドメイン上の Domain Users グループのどちらかのメンバーになります。
- i5/OS は、ユーザーの i5/OS パスワード、パスワード満了日、記述、および使用可能または使用不可の状況を追跡します。

i5/OS グループの登録

- 1 ここまでは、Windows 環境への個々の i5/OS ユーザー・プロファイルの登録について説明してきました。
- 1 i5/OS グループの全体を登録することもできます。その後、ユーザーを Windows 環境に登録されているそれらの i5/OS グループに追加するなら、それらのユーザーも Windows 環境に自動的に作成および登録されます。

複数ドメインへの登録

ユーザーとグループは複数のドメインに登録できますが、通常はその必要はありません。ほとんどの Windows 環境では、複数ドメインについて相互に信頼関係が設定されています。そのような場合、信頼関係があるとユーザーは自動的に他のドメインへアクセスできるため、ユーザーを 1 つのドメインに登録するだけで済みます。信頼関係については、ご使用の Windows の資料を参照してください。

登録情報の保管と復元

ユーザーおよびグループ登録を定義したなら、その登録定義を保管する必要があります。登録情報を保管するには、「GO SAVE」メニューのオプション 21 または 23、SAVSECDTA コマンド、または QSRSAVO API を使用します。ユーザー・プロファイルを復元するには、RSTUSRPRF コマンドで USRPRF(*ALL) または SECDTA(*PWDGRP) 値を指定します。

PRPDMNUSR パラメーターの使用

複数のサーバーが同じドメインのメンバーである場合には、それぞれのメンバー・サーバー上で重複するドメイン登録が生じることを防止することができます。ネットワーク・サーバー記述の変更 (CHGNWD) またはネットワーク・サーバー記述の作成 (CRTNWS) コマンドで、「ドメイン・ユーザーの伝搬 (PRPDMNUSR) パラメーター」を使用してください。詳しくは、204 ページの『QAS400NT ユーザー』を参照してください。

ユーザー構成の種類

統合 Windows ユーザーは、以下の 3 つの基本タイプに分類して考えると便利です。

- **従来型ユーザー (パスワードは i5/OS によって管理される)**
デフォルトで、ユーザーはこのタイプに設定されます。このユーザーは、Windows および i5/OS の両方で作業します。i5/OS パスワードと Windows パスワードとは同期されます。統合 Windows サーバーが再始動されるたびに、ユーザーのパスワードは i5/OS パスワードにリセットされます。パスワードは、i5/OS 内でのみ変更できます。ファイル・レベル・バックアップおよびリモート Windows コマンドを実行する際には、このユーザー・タイプが推奨されています。Windows ユーザーをこの構成に設定するには、WRKUSRPRF を使用してユーザー・プロファイル属性 LCLPWDMGT を *YES に設定します。
- **Windows パスワード管理ユーザー**
このユーザーは、作業のすべてまたはほとんどを Windows 内で実行し、i5/OS にはまったくまたはほとんどサインオンしません。ユーザーが i5/OS にサインオンする場合、i5/OS にアクセスするには Kerberos などの認証方式を使用する必要があります。これについては、次のセクション『エンタープライズ識別マッピング (EIM) が構成された Windows ユーザー』で説明します。

i5/OS ユーザーに対してユーザー・プロファイル属性 LCLPWDMGT(*NO) が定義されているなら、i5/OS ユーザー・プロファイル・パスワードは *NONE に設定されます。i5/OS 登録パスワードは、Windows 登録が正常に完了するまで保管されます。i5/OS ユーザーが Windows に登録された後、Windows ユーザーは Windows 内でパスワードを変更および管理できます。i5/OS がそのパスワードを上書きすることはありません。この方法を使用すると、管理対象のパスワード数が少なくなるので、よ

りセキュアな環境を実現できます。このタイプのユーザーを作成する方法については、201ページの『LCLPWDMGT ユーザー・プロファイル属性の変更』を参照してください。

• **エンタープライズ識別マッピング (EIM) 関連が自動的に構成された Windows ユーザー**

ユーザー・プロファイル属性の EIMASSOC を *TGT、TGTSRC、または *ALL に指定すると、統合サーバーは EIM Windows ソース関連を自動的に定義します。関連の自動定義を使用すると、EIM の構成が容易になります。このタイプのユーザーを作成する方法については、201ページの『エンタープライズ識別マッピング (EIM)』を参照してください。

• **エンタープライズ識別マッピング (EIM) 関連が手動で構成された Windows ユーザー**

ユーザーは、EIM Windows ソース関連を手動で定義することもできます。この方法によって、i5/OS ユーザー・プロファイルを、異なる Windows ユーザー・プロファイル名に対して登録するように設定できます。ユーザーは、i5/OS ユーザー・プロファイルの i5/OS ターゲット関連、および同じ EIM ID の Windows ソース関連を手動で定義する必要があります。

表 1. ユーザー構成の種類

ユーザーの種類	提供される機能	ユーザー・プロファイル定義
従来型	<ul style="list-style-type: none"> • i5/OS および Windows の両方が完全に機能する。 • 構成が容易。 • パスワードは i5/OS から変更される。 • i5/OS および Windows のユーザー ID とパスワードは同じ。 • システム管理者、i5/OS を頻繁に使用するユーザー、または i5/OS を使用してユーザー・プロファイルのバックアップと回復を実行するシステムで推奨される。 	LCLPWDMGT(*YES)、および EIM Windows ソース関連は定義されない。
Windows パスワード管理ユーザー	<ul style="list-style-type: none"> • パスワードは Windows から変更可能。 • 単純な構成。 • i5/OS パスワードは *NONE であるため、この構成は Windows パスワード管理により安全性が高い。 • i5/OS にサインオンするには、iSeries ナビゲーターにおいて Kerberos を使用した i5/OS サインオンのサポートで提供されている方式など、なんらかの認証方式を必要とする。 	LCLPWDMGT(*NO)
エンタープライズ識別マッピング (EIM) 関連が自動構成された Windows ユーザー	Windows ソース関連の自動作成機能により、Kerberos が使用可能なアプリケーションのセットアップと構成が容易。	例: EIMASSOC(*CHG *TARGET *ADD *CRTEIMID)

表 1. ユーザー構成の種類 (続き)

ユーザーの種類	提供される機能	ユーザー・プロファイル定義
エンタープライズ識別マッピング (EIM) 関連が手動で構成された Windows ユーザー	ユーザーは、登録された i5/OS ユーザー・プロファイルの EIM 関連を、Windows 内では異なるユーザー・プロファイルとして定義することが可能。	iSeries ナビゲーターを使用して、EIM i5/OS ターゲット関連および Windows ソース関連を手動で定義する。

ユーザー登録テンプレート

ユーザー登録テンプレートを使用すれば、ユーザーを i5/OS から Windows 環境により効率的に登録できます。同じ設定値でたくさんの新しいユーザーを登録する場合は、手動で構成する代わりに、ユーザー登録テンプレートを使用して自動的に構成してください。各テンプレートは、グループ・メンバーシップ、ディレクトリー・パス、および組織単位コンテナなどのユーザー特権を定義する Windows ユーザー・プロファイルです。

ユーザーとグループを i5/OS から Windows 環境に登録する際には、新しい Windows ユーザーのベースとなるユーザー・テンプレートを指定できます。たとえば、ユーザー・テンプレートを作成して USRTEMP という名前を付けたとします。USRTEMP は Windows サーバー・グループ NTG1 と NTG2 のメンバーです。一方、i5/OS 上には MGMT というグループがあります。この MGMT グループとそのメンバーを Windows サーバーに登録することにします。登録プロセスの間、ユーザー・テンプレートとして USRTEMP を指定します。すると、登録時に MGMT グループのメンバーすべてが、NTG1 および NTG2 グループに自動的に追加されます。

ユーザー・テンプレートを使用すれば、ユーザーごとにグループのメンバーシップを設定する作業をする必要はありません。さらに、登録ユーザーの属性の一貫性が保たれます。

Windows グループを i5/OS から登録したかどうかに関係なく、ユーザー・テンプレートをそのグループのメンバーにすることができます。i5/OS から登録していないグループのメンバーであるテンプレートを使用して、ユーザーを登録することができます。ただし、そのようにすると、ユーザーは、登録されていないそのグループのメンバーにもなってしまいます。i5/OS 側では、i5/OS から登録されていないグループについては認識しません。つまり、そのグループからのユーザーの削除は、Windows 上で「ユーザー マネージャ」プログラムを使用しなければ不可能であるということです。

新しいユーザーの登録を定義するのにテンプレートを使用し、そのテンプレートにフォルダーまたはディレクトリーの「パス (Path)」や「接続先 (Connect to)」が定義されている場合には、新しく作成された Windows ユーザーも同じ定義になります。フォルダー定義を使用すると、ユーザー管理者はフォルダー・リダイレクトの活用や、端末サービスのサインオンの管理が可能になります。


新しいユーザーの登録を定義する際にテンプレートを使用し、そのテンプレートが Windows Active Directory の組織単位コンテナ内のユーザー・オブジェクトの場合には、新しく作成された Windows ユーザー・オブジェクトは同じ組織単位コンテナ内に配置されます。組織単位は、リソースに対するユーザー管理制御を与えるための手段になります。

既存のユーザー・テンプレートは変更することができます。その変更は、テンプレート変更後に登録するユーザーだけに反映されます。

テンプレートを使用するのは、新たに登録するユーザーを Windows 環境に作成する場合だけです。既存の Windows 側のユーザーと i5/OS 側のユーザーの同期を取るために登録を実行する場合、Windows はテンプレートを無視します。

その手順については、199 ページの『ユーザー・テンプレートの作成』を参照してください。





パスワードについての考慮事項

1. i5/OS QRETSVRSEC システムが 1 に設定されていることを確認します。これは、システム値の処理 (WRKSYSVAL) コマンドを使用して行うことができます。これを行わないと、統合 Windows サーバー上のユーザーの登録が、そのユーザーが i5/OS にサインオンするまで行えなくなります。
- 1 注: このシステム値は、iSCSI 統合サーバー・サポートのためにも必要です。
2. ユーザーがユーザー登録を実行するには、Windows のパスワードで使用できる文字とパスワードの長さだけを使った i5/OS パスワードを使用する必要があります。1 文字以上 10 文字以下のユーザー・プロファイル・パスワード、または 1 文字以上 128 文字以下のユーザー・プロファイル・パスワードを使えるように i5/OS のパスワード・レベルを設定することができます。システム値 QPWDLVL を i5/OS パスワード・レベルで変更するには、IPL が必要です。
3. i5/OS パスワード・レベル 0 または 1 では、1 文字以上 10 文字以下のパスワードがサポートされ、文字セットは制限されます。パスワード・レベル 0 または 1 では、i5/OS のパスワードは、Windows サーバー用にすべての文字が小文字に変換されます。
4. i5/OS パスワードのレベル 2 または 3 では、1 文字以上 128 文字以下のパスワードがサポートされ、大文字小文字を含め、使用できる文字が多くなります。レベル 2 または 3 の場合、i5/OS は Windows 用にパスワードでの大文字小文字の区別を保ちます。
5. 登録ユーザーの i5/OS パスワードが期限切れになると、そのユーザーの Windows パスワードも期限切れになります。ユーザーは Windows 上で自分のパスワードを変更できますが、i5/OS 上でもパスワードを変更するようにしなければなりません。最初に i5/OS パスワードを変更した場合、Windows サーバー・パスワードは自動的に変更されます。
6. i5/OS システム値 QSECURITY が 10 である場合、作成された Windows サーバー・ユーザーは、パスワードなしでサインオンできます。その他の i5/OS QSECURITY レベルでは、ユーザー・オブジェクトごとに、サインオン用パスワードが必要です。セキュリティー・レベルについては、「iSeries 機密保護解説書 」に記載されています。
7. 英語以外の言語を使用する場合は、ユーザー・プロファイルとパスワードで不変文字以外の文字を使用すると、予測不能な結果になる可能性があるので、注意してください。グローバリゼーションのトピックには、不変文字セットに入っている文字についての詳細が記載されています。これが該当するのは、QPWDLVL が 0 または 1 の場合だけです。QPWDLVL が 2 または 3 の場合は、不変文字を使っても何も問題は起きません。

第 5 章 iSeries での Windows 環境のインストールと構成

iSeries Windows 環境のセットアップには、ハードウェアおよび 2 つのソフトウェアをインストールすることが含まれます。それらのソフトウェアは、IBM i5/OS 統合サーバー・サポートおよび Microsoft の Windows 2000 Server または Windows Server 2003 オペレーティング・システムです。


iSeries Windows 環境のインストールおよび構成は、以下の手順で行います。


1. 「IBM iSeries 統合 xSeries ソリューション」  Web サイト (英語) (www.ibm.com/servers/eserver/series/integratedxseries) を調べます。最新のニュースや情報に通じていることを確認してください。
2. インストールするハードウェアの最新のニュースや情報を確認してください。
 - IXA インストール、最初にお読みください (英語)  (www.ibm.com/servers/eserver/series/integratedxseries/ixareadme)
 - iSCSI インストール、最初にお読みください (英語)  (www.ibm.com/servers/eserver/series/integratedxseries/iscsireadme)
 - IXS インストール、最初にお読みください (英語)  (www.ibm.com/servers/eserver/series/integratedxseries/ixsreadme)
3. 適切なハードウェアおよびソフトウェアがあることを確認します。
 - a. 62 ページの『ハードウェア要件』。
 - b. 64 ページの『ソフトウェア要件』。
4. IXS 接続サーバーまたは IXA 接続サーバーの場合、必要であれば、ハードウェアをインストールします。「iSeries フィーチャーの取り付け」を参照してください。iSeries サーバーのモデルを選択します。IXS には、「PCI アダプター」を選択し、IXA には、「統合 xSeries アダプター」を選択します。iSCSI HBA をインストールしている場合、ハードウェアを 6b のステップでインストールするように指示されます。
5. IBM iSeries 統合サーバー・サポートをインストールします。
 - a. 64 ページの『統合 Windows サーバーのインストールの準備』
 - b. 69 ページの『IBM i5/OS 統合サーバー・サポートのインストール』
6. Microsoft Windows 2000 Server または Windows Server 2003 を統合サーバーにインストールします。
 - a. 70 ページの『Windows サーバーのインストールの計画』
 - b. 98 ページの『Windows 2000 Server または Windows Server 2003 のインストール』
7. インストールが完了したので、統合 Windows サーバーを構成します。
 - a. 119 ページの『コード修正』。これらのコード・フィックスは、ライセンス・プログラムがリリースされた後に検出されたエラーを修正します。
 - b. 123 ページの『第 6 章 仮想イーサネットおよび外部ネットワークの管理』
 - c. 118 ページの『TCP/IP に応じた統合 Windows サーバーのオンへの自動変更の設定』

ハードウェア要件

統合 Windows サーバーを実行するには、以下のハードウェアが必要です。

- 以下の統合 xSeriesサーバー (IXS)、統合 xSeriesアダプター (IXA)、または、iSCSI HBA のいずれか。

説明	フィーチャー・コード	タイプ - モデル
2.0 GHz 統合 xSeries サーバー	4811 48124813	4812-001
2.0 GHz 統合 xSeries サーバー	4710	2892-002
2.0 GHz 統合 xSeries サーバー	4810	2892-002
1.6 GHz 統合 xSeries サーバー	2792	2892-001
1.6 GHz 統合 xSeries サーバー	2892	2892-001
1.0 GHz 統合 xSeries サーバー	2799	2890-003
1.0 GHz 統合 xSeries サーバー	2899	2890-003
850 MHz 統合 xSeries サーバー	2791	2890-002
850 MHz 統合 xSeries サーバー	2891	2890-002
700 MHz 統合 xSeries サーバー	2790	2890-001
700 MHz 統合 xSeries サーバー	2890	2890-001
統合 xSeries アダプター・モデル 100	0092 ^{2,3}	2689-001
統合 xSeries アダプター・モデル 200	0092 ^{2,4}	2689-002
注:		
1. IXA には xSeries サーバーが必要です。xSeries サーバーでは、要件が追加される場合があります。詳しくは、 統合 xSeries ソリューション Web サイト (英語) (www.ibm.com/servers/eserver/iserics/integratedxseries)  を参照してください。		
2. ハードウェアは、マシン・タイプ 1519-100 として AAS または WTAAS を介して注文します。		
3. ハードウェアは、マシン・タイプ 1519-200 として AAS または WTAAS を介して注文します。		

注: 上記の表にリストされていない統合サーバー・ハードウェアがある場合、IBM 統合 xSeries ソリューション  Web サイト (英語) で仕様を参照してください。

ハードウェアをインストールする方法については、『「iSeries フィーチャーの取り付け」』のトピックを参照してください。IXS、IXA、および iSCSI HBA の説明は、14 ページの『ハードウェアの概念』を参照してください。

- iSeries サーバー。IBM i5/OS 統合サーバー・サポートのコーディング用に 100 MB、Windows システム・ドライブまたはネットワーク・サーバー記憶域スペース用に 2,047 MB を含む、十分な空きディスク・スペースが必要です。
- IXS の場合、1 つ以上の承認されている LAN ポートまたは PCI アダプター。

説明	フィーチャー・コード	IXS ハードウェア・タイプ 4812 によるサポート	IXS ハードウェア・タイプ 2892 によるサポート	IXS ハードウェア・タイプ 2890 によるサポート
iSeries 1000/100/10 Mbps Ethernet Adapter (銅線 UTP)	5701		X	

説明	フィーチャー・コード	IXS ハードウェア・タイプ 4812 によるサポート	IXS ハードウェア・タイプ 2892 によるサポート	IXS ハードウェア・タイプ 2890 によるサポート
iSeries Gigabit (1000 Mbps) Ethernet Adapter (光ファイバー)	5700		X	
iSeries Gigabit (1000/100/10 Mbps) Ethernet Adapter (銅線 UTP)	2760			X
iSeries Gigabit (1000 Mbps) Ethernet Adapter (光ファイバー)	2743			X
iSeries 2892 10/100 Mbps イーサネット・ポート	2892		X	
IBM iSeries 10/100 Mbps Ethernet Adapter	2838			X
高速 100/16/4 Mbps トークンリング PCI アダプター	2744		X	X
iSeries 4812 1000/100/10 Mbps イーサネット・ポート	4812	X		

4. SVGA 互換モニター、マウス、およびキーボード。IXS にあるキーボード/マウスのポートは 1 つだけなので、両方を同時に接続するにはキーボード/マウスの Y ケーブルも必要です。複数の統合サーバーがあり、一度に 1 つずつ管理することを計画している場合、複数の統合サーバーの間で 1 セットの I/O ハードウェアを切り替えることを検討してください。
5. 最低限 128 MB のランダム・アクセス・メモリー (RAM)、または Windows 2003 Server を使用する場合は最低限 256 MB の RAM。このメモリーは統合サーバー内にインストールされて、別個に配列されている必要があります。
6. Microsoft Windows および iSeries Access (iSeries ナビゲーターを含む) がインストールされている PC。

注: iSeries ナビゲーターは iSeries Windows 環境のほとんどの構成タスクで優先されます。

追加のハードウェア要件については、以下を参照してください。

- 66 ページの『マシン・プール・サイズ要件』
- 29 ページの『ネットワーキングの概念』

ソフトウェア要件

以下のソフトウェアが必要です。

1. i5/OS 5722-SS1 バージョン 5 リリース 4。

リリース・レベルを調べるには、次のようにします。

- a. i5/OSコマンド行で Go LICPGM と入力し、Enter キーを押します。
- b. オプション・フィールドに 10 と入力し、インストールされている製品を表示します。
- c. 5722SS1 を探します。この横に表示されているリリースが、ご使用のバージョンです。(リリースによっては、F11 を押してバージョン番号を表示しなければならない場合もあります。)

2. IBM i5/OS 統合サーバー・サポート (5722-SS1 オプション 29) V5R4。69 ページの『IBM i5/OS 統合サーバー・サポートのインストール』を参照してください。

3. IBM iSeries ナビゲーター。IBM iSeries Access for Windows (5722-XE1) に同梱されています。

注:

- a. Windows PC に iSeriesナビゲーターをインストールする場合、フルインストールを行うか、カスタム・インストールを行って、オプションの「統合サーバー管理」コンポーネントを選択します。
- b. iSeries ナビゲーターは iSeries Windows 環境のほとんどの構成タスクで優先されます。

4. TCP/IP Connectivity Utilities for i5/OS V5R4 (5722-TC1)

5. IXS 接続サーバーおよび IXA 接続サーバーの場合、Microsoft Windows 2000 Server または Windows Server 2003 が必要です。iSCSI 接続サーバーの場合、Windows Server 2003 が必要です。

6. 必要な Microsoft Windows サービス・パック。i5/OS 統合サーバー・サポートを使用した IBM によるテスト済みかつ入手可能なサービス・パックの最新情報については、IBM 統合 xSeries ソリューション



Web サイト (英語) の『Applications』の項を参照してください。

- iSCSI サーバーの場合は、以下のソフトウェアも必要です。

1. IBM Director 5.10

注: IBM Director は、Virtualization Engine (5733-VE2) の費用のかからないオプションで、追加のソフトウェア要件があります。詳細については、IBM Systems Software Information Center の『IBM Director の i5/OS へのインストール (Installing IBM Director on i5/OS)』を参照してください。

2. IBM i5/OS Digital Certificate Manager (5722-SS1 オプション 34) V5R4

3. xIBM HTTP Server for iSeries (5722-DG1)

必要なソフトウェアのインストールについては、「iSeries ソフトウェアの導入」 を参照してください。

統合 Windows サーバーのインストールの準備

いくつかの事前の作業を実行しておく、インストールがスムーズになります。

1. インストールを実行するのに必要な権限があることを確認します。i5/OS上で *IOSYSCFG、*ALLOBJ、および *JOBCTL 特殊権限を持っていないなりません。このチェックリストのステップ 8 を行うためには、*SECADM 特殊権限が必要です。特殊権限については、「iSeries

機密保護解説書  」を参照してください。


2. 66 ページの『マシン・プール・サイズ要件』を確認します。
3. 時刻合わせが正しく構成されていることを確認します。 67 ページの『時刻合わせ』を参照してください。
4. 67 ページの『i5/OS TCP/IP を統合 Windows サーバー用に構成する』。
5. 特定の業務に必要な統合 Windows サーバーとサブネットの数を決めます。

iSCSI 接続サーバーをインストールする場合、各 iSeries 用の iSCSI HBA は 2 つの固定 IP アドレスを必要とし、それぞれのホストされる xSeries システムまたは IBM BladeCenter は、iSCSI 用に少なくとも 2 つの IP アドレスを必要とします。IP アドレスの要件については、29 ページの『ネットワークングの概念』を参照してください。

組織が固定 IP アドレスを使用する場合 (DHCP を使用する組織では、通常の PC サーバーと同様に統合 Windows サーバーに IP アドレスが自動的に割り当てられるように構成できます)、ネットワーク管理者から TCP/IP アドレスを取得してください。TCP/IP アドレスには以下のものが含まれます。




- すべての外部 TCP/IP ポートの IP アドレス
- サブネット・マスク
- ドメイン名またはワークグループ名
- ドメイン・ネーム・システム (DNS) サーバーの IP アドレス (ある場合)
- ローカル・エリア・ネットワーク (LAN) のデフォルト・ゲートウェイの IP アドレス (ある場合)

TCP/IP を iSeries システムで実行している場合、上記のリストにある最後の 2 つの項目は、システムに供給済みです。Windows サーバー導入 (INSWNTSVR) コマンドを実行する際に、それらのパラメーターに *SYS を指定します。

6. iSeries Access for Windows を使用するかどうかを決定します。このソフトウェアでは、iSeries ナビゲーターを使用して、Open Database Connectivity (ODBC) を Windows サービスとして実行することができます。Information Center の「iSeries NetServer™ と iSeries Access for Windows」トピックを参照してください。
7. NetServer を使用可能化にし、ゲスト・ユーザー・プロファイルをセットアップします。これで、統合サーバーで保守タスクを実行できます。68 ページの『iSeries NetServer の使用可能化』および 68 ページの『iSeries NetServer 用のゲスト・ユーザー・プロファイルの作成』を参照してください。
8. 実際に CD-ROM がなくてもインストールできます。そうすれば、たとえば、サーバーを再インストールする必要がある場合に遠隔地に CD-ROM を配送する時間や費用を節約したり、Microsoft サービス・パックまたは hotfix をインストール・ソースに統合し、ウィルス感染を防ぐことができます (MS サポート技術資料 828930)。インストール CD のイメージを保管してから、インストール時に「Windows ソース・ディレクトリー」フィールドでそのイメージへのパス名を指定してください。この点に関する説明が必要な場合、レッドブック「Microsoft Windows Server 2003 Integration with iSeries」(SG24-6959)  を参照してください。


注: インストール CD の内容は、それぞれの作成者および配布者に所属するライセンスの対象になっていません。ライセンス条項を必ず順守してください。また、この機能を公開しても、CD ライセンスご使用条件の順守または行使に関連した責任を IBM が負担するというわけではありません。

9. 構成ファイルを使用して、Windows 不在インストール・セットアップ・スクリプト・ファイル (unattend.txt) のデフォルト値を変更し、インストールをカスタマイズできます。275 ページの『第 15 章 ネットワーク・サーバー記述構成ファイル』を参照してください。

- 10. 統合 xSeries アダプターを使って外部 xSeries サーバーにサーバーをインストールする場合は、以下のリンクを参照してください。
 - IXA インストール、最初にお読みください (英語) 
 - iSeries フィーチャーの取り付け
- 11. サーバーを統合 xSeries サーバー上にインストールする場合は、IXS インストール、最初にお読みください (英語)  を参照してください。
- 12. iSCSI HBA を使って外部 xSeries サーバーまたは IBM BladeCenter サーバーにサーバーをインストールする場合は、xSeries サーバーまたは IBM BladeCenter サーバーを準備する必要があります。詳細については、iSCSI インストール、最初にお読みください (英語)  を参照してください。
- 13. iSCSI HBA を使って外部 xSeries サーバーまたは IBM BladeCenter サーバーにサーバーをインストールする場合は、i5/OS QRETSVRSEC システムが 1 に設定されていることを確認します。これは、システム状況の処理 (WRKSYSVAL) コマンドを使用して行うことができます。
- 14. iSeries サーバーで論理区画を使用する場合、サーバーをオンに変更するのに使用する論理区画にだけ、IBM i5/OS 統合 xSeries サーバー・サポートをインストールする必要があります。すべての論理区画にライセンス・プログラムをインストールする必要はありません。たとえば、ある論理区画には i5/OS 統合 xSeries サーバー・サポートと 1 つ以上の統合 Windows サーバーがインストールされており、別の論理区画には i5/OS 統合 xSeries サーバー・サポート も統合サーバーもインストールされていないという場合もあります。
- 15. i5/OS に Windows サーバーをインストールする場合、Windows のバージョンや使用するハードウェア・リソースなどの構成情報を含むネットワーク・サーバー記述 (NWS) オブジェクトが作成されます。ただし、指定されたハードウェア・リソースに関して、一度にオンに変更 (実行中) にできるのは、1 つの NWS だけです。

マシン・プール・サイズ要件

マシン記憶域プールは、高度共用マシンおよびオペレーティング・システム・プログラムのために使用されます。マシン記憶域プールは、システムが実行する必要のある、ユーザーによる操作を必要としないジョブのための記憶域を提供します。それらの記憶域プールに対して設定するサイズが小さすぎると、システム・パフォーマンスの低下を招きます。QMCHPOOL を 256 KB より小さい値に設定することはできません。この記憶域プールのサイズは、マシン記憶域プール・サイズのシステム値 (QMCHPOOL) で指定されます。この記憶域プール内では、ユーザー・ジョブは実行しません。

- サポートされるすべての IXS 接続および IXA 接続の統合サーバー・ハードウェアには、少なくとも 856 KB のメモリーが必要です。iSCSI 接続サーバーのメモリー所要量について詳しくは、iSCSI インストール、最初にお読みください (英語)  を参照してください。

システム状況の処理 (WRKSYSSTS) コマンドを使用して、マシン・プール・サイズを表示したり変更したりできます。WRKSYSSTS 画面の 1 番目の記憶域プールは、マシン・プールです。

システムがシステム・プール・サイズを自動的に調整するように、システム値 QPFRADJ を変更することができます。ただし、自動パフォーマンス調整に起因して使用中のシステムがスローダウンする可能性があるため、使用を以下のいずれかの期間に制限したほうがよいかもしれません。

- インストール後 2 日間
- システム負荷が日中 (対話式が主体) から夜間 (バッチが主体) に、またその逆に代わる際の約 1 時間

時刻合わせ

i5/OS および Windows 環境の時刻合わせをするには、次のようにします。

1. Windows サーバー導入 (INSWNTSVR) コマンドまたは CHGNWSD コマンドで、日付と時刻の時刻合わせに対して *YES を選択します。*YES を選択すると、i5/OS および統合 Windows サーバーの時刻合わせが 30 分ごとに行われます。*NO を選択すると、サーバーの始動時だけに時刻合わせが行われます。
2. iSeries の時刻、日付、およびタイム・ゾーンが正しいことを確認します。これらの値が設定されると、その後は 6 カ月ごとに夏時間調整のために自動的に更新されます。QTIMZON システム値により、QUTCOFFSET システム値を年に 2 回手動で変更する必要がなくなります。
3. Windows コンソールで、「コントロール パネル」→「日付と時刻」をクリックしてから、「タイムゾーン」タブを選択してドロップダウン・リストからタイム・ゾーンを選択します。
4. 「自動的に夏時間の調整をする」チェック・ボックスを選択します。次に「OK」をクリックします。

時刻合わせで問題が生じた場合は、LOCALE の i5/OS システム値を調べて、正しく設定されているかどうかを確かめます。

- 注: Windows アクティブ・ドメイン・サーバーおよびドメイン・メンバー・サーバーの場合、時刻合わせは *NO に設定する必要があります。Windows Active Directory には、固有の時刻合わせ機能があるので、時刻合わせを *YES に設定すると、競合が生じます。

i5/OS TCP/IP を統合 Windows サーバー用に構成する

iSeries に Windows 環境をインストールするときには、選択によっては、統合サーバーを構成するデフォルト値として i5/OS TCP/IP 構成で指定した値を使用できます。そのように選択したい場合に、TCP/IP をまだ構成していないときは、先に構成してから IBM i5/OS 統合サーバー・サポートをインストールする必要があります。ゲートウェイ・アドレスを i5/OS に追加する必要もあります。TCP/IP の構成の詳細は、「TCP/IP」のトピックを参照してください。

iSeries ナビゲーターがインストールされている場合、それを使用して TCP/IP 接続を構成することができます。iSeries ナビゲーターのオンライン・ヘルプに、TCP/IP の構成方法が示されています。iSeries ナビゲーターがインストールされていない場合には、次のステップを実行します。

1. i5/OS コンソールでコマンド CFGTCP を入力し、Enter キーを押します。「TCP/IP の構成」メニューが表示されます。
2. オプション 12「TCP/IP ドメイン情報の変更」を選択し、Enter キーを押します。「TCP/IP ドメインの変更 (CHGTCPDMN)」画面が表示されます。
3. ローカル・ドメイン名を 73 ページの『i5/OS パラメーターのインストール・ワークシート』から指定します。
4. 「ドメイン・ネーム・サーバー」フィールドに、Windows サーバー・インストール・アドバイザーまたは 73 ページの『i5/OS パラメーターのインストール・ワークシート』から得た IP アドレス (最大 3 つ) を指定し、Enter キーを押します。

以下のようにして、ゲートウェイ IP アドレスを i5/OS に追加します。

5. 「TCP/IP の構成」メニューから、オプション 2「TCP/IP 経路の処理」を選択します。「TCP/IP 経路の処理」画面が表示されます。
6. TCP/IP 経路指定を追加するには、「Opt」フィールドに 1 を入力します。「TCP/IP 経路の追加」画面が表示されます。
7. 該当するフィールドに、ゲートウェイ・アドレスの情報を入力します。

統合 Windows サーバー上の iSeries Access for Windows

IBM iSeries Access for Windows を使用すると、ローカル・エリア・ネットワーク (LAN)、平衡型接続、またはリモート・リンクを介してパーソナル・コンピュータ (PC) を iSeries サーバーに接続できます。これは一連の機能の全統合を特徴としますが、それによって、デスクトップを使う場合のローカル PC 機能の利用と同じように簡単に i5/OS リソースを使用できます。iSeries Access を使ってユーザーおよびアプリケーション・プログラマーは、社内全体の情報、アプリケーション、およびリソースを迅速に処理できます。

統合サーバーに iSeries Access for Windows サーバーをインストールすれば、Open Database Connectivity (ODBC) を Windows サービスとして実行できます。このようにして、DB2 for iSeries にアクセスするために ODBC デバイス・ドライバを呼び出すサーバー・アプリケーションを作成できるようになります。

Windows サービスから ODBC を起動できるようにするには、iSeries Access をインストールしてから、/s オプションを指定した CWBCFG コマンドを実行します。

Windows にサインオンした単一ユーザーとして、他のすべての iSeries Access 機能に対するサポートが提供されます。

参考資料:

- iSeries Access for Windows と iSeries NetServer を比較してください。

iSeries NetServer の使用可能化

- 1 iSeries NetServer を使って Windows クライアントは、TCP/IP を介して i5/OS 共用ディレクトリー・パス
- 1 および共用出力待ち行列に接続することができます。サービス・パックをインストールするには、同じパス
- 1 ワードの iSeries ユーザー・プロファイルに対応する Windows アカウントでサインオンするか、ゲスト
- 1 NetServer ユーザー・プロファイルを構成する必要があります。

保守タスクの実行のときだけ iSeries NetServer を使用する予定であれば、iSeries ナビゲーターを使用しないでこのセットアップを実行することもできます。その場合、『iSeries NetServer を使用するように iSeries サーバーを構成する』トピックに示されているクイック・スタート方式を使用できます。iSeries NetServer の全機能を使いたい場合は、iSeries ナビゲーターが必要です。この場合は、管理に使用している PC 上で iSeries アクセスをセットアップしなければなりません (『統合 Windows サーバー上の iSeries Access for Windows』を参照)。いずれかのバージョンをセットアップしたら、ゲスト・ユーザー・プロファイルをセットアップしなければなりません。『iSeries NetServer 用のゲスト・ユーザー・プロファイルの作成』を参照してください。

iSeries NetServer 用のゲスト・ユーザー・プロファイルの作成

- 1 コード修正とシステム更新を iSeries Windows 環境に適用できるようにするには、同じパスワードの
- 1 Windows アカウントおよび iSeries ユーザー・プロファイルでサインオンするか、ゲスト NetServer ユー
- 1 ザー・プロファイルを iSeries NetServer 用に構成しておく必要があります。この作業を実行するため
- 1 は、*SECADM 特殊権限が必要です。

システムに iSeries ナビゲーターがあれば、グラフィカル・インターフェースを使用して iSeries NetServer のゲスト・ユーザー・プロファイルを設定することができます。その場合、特殊権限やパスワードは必要ありません。

iSeries ナビゲーターがない場合は、以下のステップを行って iSeries NetServer のゲスト・ユーザー・プロファイルを設定します。

1. i5/OS 上で、特殊権限とパスワードを持たないユーザー・プロファイルを作成します。

```
CRTUSRPRF USRPRF(username) PASSWORD(*NONE) SPCAUT(*NONE)
```

注:

ユーザー・プロファイルについては、「iSeries 機密保護解説書 」を参照してください。

2. 次のコマンドを入力します。 *username* は、作成したユーザー・プロファイルの名前です。

```
CALL QZLSCHSG PARM(username X'00000000')
```

3. iSeries NetServer を終了するには、以下のコマンドを入力してください。

```
ENDTCPSVR SERVER(*NETSVR)
```

4. iSeries NetServer を再始動するには、以下のコマンドを入力してください。

```
STRTCPSVR SERVER(*NETSVR)
```

68 ページの『iSeries NetServer の使用可能化』または 64 ページの『統合 Windows サーバーのインストールの準備』に戻ることができます。

IBM i5/OS 統合サーバー・サポートのインストール

IBM i5/OS 統合サーバー・サポートをインストールするには、以下のステップを iSeries で実行してください。

1. IBM iSeries Integration for Windows Server を V5R2 または V5R3 からアップグレードする場合、106 ページの『IBM iSeries Integration for Windows Server ライセンス・プログラムのアップグレード』のトピックを参照してください。『アップグレードを準備します』の下にある手順を実行してから、ここに戻ってください。
2. 5722-SS1 オプション 29 の入った i5/OS CD を挿入します。
3. GO LICPGM と入力し、Enter キーを押します。
4. 「ライセンス・プログラムの処理」メニューから、オプション 11 を選択して、Enter キーを押します。
5. 「統合サーバー・サポート」が表示されるまで、次ページ・キーを押して、ライセンス・プログラムのリストを下に移動します。
6. 記述の左側の「オプション」フィールドに 1 と入力します。
7. Enter キーを押します。
8. i5/OS CD を挿入した装置の名前を「インストール装置」に入力します。
9. Enter キーを押します。統合ソフトウェアがインストールされます。
10. IBM i5/OS 統合サーバー・サポートをインストールし終わったら、IBM の最新の累積プログラム一時修正 (PTF) パッケージをインストールしてください。PTF のインストールは、iSeries 上にユーザーがいないときに行います。システムで論理区画が使用されている場合、i5/OS 統合サーバー・サポートのインストール先の 2 次区画に PTF をロードし、適用の遅延を設定してください。後で 1 次区画にロードします。『論理区画を持つシステムでのプログラム一時修正のインストール』を参照してください。
11. 最新の PTF をインストールするには、次のようなステップを行います。
 - a. i5/OS コマンド行で GO PTF と入力し、Enter キーを押します。
 - b. プログラム一時修正パッケージをインストールするには、8 と入力し、Enter キーを押します。
 - c. 「装置」フィールドに、光ディスク装置の名前を入力します。

- d. システムが論理区画を使用しなければ、「自動 IPL」にはデフォルトの *YES を使用します。Enter キーを押すと、すべての PTF がインストールされます。値を *NO に変更しなければ、システムは自動的にシャットダウンし、それから再始動します。

PTF の詳細は、『iSeries の概要』の『プログラム修正』を参照してください。

12. IBM iSeries Integration for Windows Server を V5R2 または V5R3 からアップグレードする場合、106 ページの『IBM iSeries Integration for Windows Server ライセンス・プログラムのアップグレード』を参照してください。『i5/OS をアップグレードしたら』の下にある手順を実行してから、ここに戻ってください。
13. i5/OS 統合サーバー・サポートを以前のリリースからアップグレードする場合、既存の統合 Windows サーバーを新しいレベルにアップグレードする必要があります。108 ページの『IBM i5/OS 統合サーバー・サポートの統合サーバー側のアップグレード』を参照してください。

Windows サーバーのインストールの計画

- ネットワーク上の最初の統合 Windows サーバーをドメイン・コントローラーにし、慎重に名前を付けるようにお勧めします。(名前を変更する場合、まず役割を変更しなければなりません。)ドメイン・コントローラーには、マスター・セキュリティ・データベースが含まれています。どのドメイン・コントローラーも変更することができ、その変更は他のすべてのドメイン・コントローラーに複製されます。

- iSCSI 接続サーバーをインストールする場合、『iSCSI ハードウェアのインストールの計画』も参照してください。

- Windows 2000 Server または Windows Server 2003 をインストールする前に、「Windows サーバー・インストール・アドバイザー」によって生成されたコマンドを完了して保管する必要があります。またはその代わりに、73 ページの『i5/OS パラメーターのインストール・ワークシート』を記入することもできます。

続行するには、98 ページの『Windows 2000 Server または Windows Server 2003 のインストール』を参照してください。

iSCSI ハードウェアのインストールの計画

- Windows サーバーのインストールを開始する前に、iSCSI ハードウェアの構成を行う必要があります。
- 『ホストされるシステムのブート・モードの計画』
 - 71 ページの『サービス・プロセッサ構成およびリモート・システム構成の作成』
 - 72 ページの『サービス・プロセッサ接続の計画』
 - 73 ページの『iSeries サーバーにおけるサービス・プロセッサのディスカバリー方法の構成』

ホストされるシステムのブート・モードの計画

- ブート・モードは、Windows のブートに必要な IP および記憶域情報をホストされるシステムの iSCSI HBA に配信する方法を決定します。

DHCP を介してリモート・システムへ動的に送達

- これは、デフォルト・モードです。iSeries サーバーの DHCP サーバーは、構成済みの NWSH アダプター経由の構成情報を自動的に提供します。23 ページの『iSCSI を使用したディスクレス・ブート』を参照してください。

- 複数の NWSH は、ホストされるシステムをそれぞれ別の機会に使用できます。
- このモードは、スイッチ接続されたネットワークおよび DHCP リレーで接続された経路指定ネットワークで使用できます。

・ IPsec が使用可能になると、DHCP トラフィックが iSCSI HBA 間で流れることが可能になります。

リモート・システムに手動で構成

・ 1 つの NWSD だけがホストされるシステムを使用できます。

・ この設定は、DHCP リレーのないネットワーク上で作動します。

・ IPsec が iSCSI HBA 間で使用できる場合、DHCP トラフィックは iSCSI ネットワーク上でブロックされます。

サービス・プロセッサ構成およびリモート・システム構成の作成

サーバーをインストールする前に、オプションでサービス・プロセッサ構成およびリモート・システム構成を作成することができます。そうすることにより、この構成の名前を Windows サーバー導入 (INSWNTSVR) コマンドのパラメーターとして使用できます。この手順は、ホストされるシステムのハードウェアのセットアップ前に実行することができます。また、INSWNTSVR はパラメーターと同一の情報すべてが与えられた場合、これらのオブジェクトを生成することができるため、これはオプションです。サービス・プロセッサ構成およびリモート・システム構成の作成は、以下の条件のいずれかを満たす場合、INSWNTSVR コマンドの実行前に行うことをお勧めします。

・ 以前に iSCSI 接続サーバーをインストールしたことがなく、できるだけ多くの手引きが必要である。

・ できるだけ、グラフィカル・インターフェースを使用したい。

・ リモート・システムの製造番号または iSCSI HBA ラベルには、後からアクセスできないことがある。

サービス・プロセッサ構成およびリモート・システム構成を作成するには、次のステップを実行します。

1. 新規サーバーで使用するサービス・プロセッサ構成をまだ作成していない場合は、それをすぐに作成します。このオブジェクトは、後で変更できます。

a. 「統合サーバー管理」を展開します。

b. 「iSCSI 接続」を展開します。

c. 「サービス・プロセッサ」を右マウス・ボタンでクリックします。

d. 「新規サービス・プロセッサ構成」を選択します。

e. 「一般」タブで以下のようにします。

・ 「名前」 および 「記述」を入力します。

・ 格納装置「製造番号」を指定して、ネットワーク上のサービス・プロセッサを識別します。システム格納装置を参照して、この値を決定します。

・ 「オブジェクト権限」を選択します。

f. 「セキュリティ」タブで、「(物理的セキュリティが必要な) 証明書を使用しない (Do not use a certificate (requires physical security))」を指定します。

g. 「OK」をクリックします。

2. リモート・システム構成をまだ作成していない場合は、それをすぐに作成します。

a. 「統合サーバー管理」を展開します。

b. 「iSCSI 接続」を展開します。

c. 「リモート・システム」を右マウス・ボタンでクリックします。

d. 「新規リモート・システム構成」を選択します。

e. 「一般」タブで以下のようにします。

・ 「名前」 および 「記述」を入力します。

- サービス・プロセッサ構成の場合、ステップ 1 から既存または新規のサービス・プロセッサを選択します。
- 「リモート・システムの識別」を指定します。

注: IBM BladeCenter ブレードのリモート・システム ID を指定する場合、「次の値を使用」オプションを指定し、IBM BladeCenter ブレードの製造番号を指定します。他のサーバーの場合、「格納装置 ID を使用 (Use enclosure identity)」オプションが選択された状態にします。

- 「オブジェクト権限」を選択します。
- f. 「ネットワーク インターフェース」タブで、ホストされるシステムで使用する iSCSI HBA ポートごとに次のステップを実行します。
- 1) 「追加」をクリックします。
 - 2) 「ネットワーク・インターフェース・プロパティ (Network Interface Properties)」パネルで、iSCSI HBA にあるラベルから少なくとも 1 つの「アダプター (MAC) アドレス (adapter (MAC) address)」を指定します。リモート SCSI インターフェースおよびリモート LAN インターフェースのアドレスの指定を判別する場合は、31 ページの『iSCSI ネットワーク』を参照してください。どちらかわからない場合は、両方のアドレスを指定してください。各アドレスは、12 個の 16 進文字で構成されています。
 - リモート SCSI インターフェース の場合、ラベルにある語「iSCSI」を検索し、対応するアドレスを指定します。
 - リモート LAN インターフェースの場合、ラベルにある語「TOE」を検索し、対応するアドレスを指定します。

注: 2 つのポートを持つ iSCSI HBA の場合、ラベルは 4 つのアドレスを示します。各ポートには 1 つの iSCSI アドレスと、1 つの TOE アドレスがあります。

- 3) 指定する各アダプター (MAC) アドレスごとに、1 つの IP アドレスと iSCSI ネットワークに適切なサブネット・マスクを入力します。iSCSI ネットワークにゲートウェイがない場合、「ゲートウェイ」フィールドは空白のままにしておきます。
 - 4) 「ネットワーク・インターフェース・プロパティ (Network Interface Properties)」で「OK」をクリックします。
- g. 「ブート・パラメーター (Boot parameters)」タブで以下のようになります。
- ブート・モードを構成します。70 ページの『ホストされるシステムのブート・モードの計画』を参照してください。ほとんどの場合、これは、「DHCP を介してリモート・システムへ動的に送達」のデフォルト・オプションとなります。詳しくは、23 ページの『iSCSI を使用したディスクレス・ブート』を参照してください。「リモート・システム内の 1 つ以上の iSCSI インターフェース (More than one iSCSI interface in remote system)」チェック・ボックスは無視します。
- h. 「CHAP 認証」タブで以下のようになります。
- 「CHAP を使用しない (Do not use CHAP)」を選択します。詳しくは、51 ページの『iSCSI 接続システムのセキュリティ』を参照してください。
- i. このオブジェクトの追加の情報を構成する場合は、すぐに構成します。
- j. 「OK」をクリックします。

サービス・プロセッサ接続の計画

新規のサービス・プロセッサ構成を作成して、新規サーバーと一緒に使用する場合、以下に示すそれぞれのサービス・プロセッサによってサポートされる方法と、どのサポート済みの方法を使用するかを決定する必要があります。

- | • 構成方法
- | • 静的または動的 IP アドレス
- | • ディスカバリー方法
- | • セキュリティー方法

| ハードウェアを準備し、サービス・プロセッサの構成を変更する場合、次のステップにあるこの情報が必要になります。使用する方法的決定について、30 ページの『サービス・プロセッサ接続』および 155 ページの『サービス・プロセッサのディスカバリー構成』を参照してください。ただし、構成のステップはまだ実行しないでください。

| iSeries サーバーにおけるサービス・プロセッサのディスカバリー方法の構成

| サービス・プロセッサのディスカバリー方法を構成します。この場合、ホストされるシステムで実行されるステップは飛ばしてください。このステップは後ほど、ハードウェアの準備の一部として実行されるからです。詳しくは、157 ページの『サービス・プロセッサのディスカバリー方式』を参照してください。

ネットワーク・サーバー記述

統合 Windows サーバーは iSeries 上で、ネットワーク・サーバー記述 (NWSD) によって表されます。Windows サーバー導入 (INSWNTSVR) コマンドは、インストールする統合サーバーごとに自動的に NWSD を作成します。通常、その NWSD にはサーバーと同じ名前が付きます。NWSD 上でアクションを実行すると、サーバー上でもアクションを実行します。たとえば、NWSD をオンに変更するとサーバーが始動され、NWSD をオフに変更するとサーバーがシャットダウンされます。

i5/OS パラメーターのインストール・ワークシート

Windows 2000 Server または Windows Server 2003 をインストールする前に、Windows サーバー・インストール・アドバイザーまたはこのインストール・ワークシートのいずれかを完了してください。

このワークシートを使用すると、システムのインストールと構成に役立ちます。

フィールド	説明および指示	値
ネットワーク・サーバー記述 (NWSD)	<p>統合 Windows サーバーを制御するネットワーク・サーバーの操作特性と通信接続を定義します。『ネットワーク・サーバー記述』を参照してください。</p> <p>覚えやすい名前を使用してください。名前の長さは最高 8 文字までです。名前には A から Z の文字および 0 から 9 のみを使用し、先頭は文字にしてください。ネットワーク・サーバー記述名は、コンピューター名、および統合サーバーの TCP/IP ホスト名でもあります。</p>	

フィールド	説明および指示	値
インストール・タイプ (INSTYPE)	<p>実行するインストールのタイプを指定します。次の 1 つを選んでください。</p> <p>*FULL</p> <p>内部統合 xSeries(R) サーバー (IXS) へのインストールでは必須ですが、統合 xSeries アダプター (IXA) または iSCSI HBA によって接続された外部 xSeries サーバーでのインストールではオプションです。</p> <p>*BASIC</p> <p>外部接続された、IXA または iSCSI HBA の接続した xSeries サーバーでインストールするときのオプションのインストール・タイプ。このオプションを指定すると、インストール・プロセスの最初の部分は i5/OS の Windows サーバー導入 (INSWNTSVR) コマンドによって制御されます。その後、ServerGuide™ CD を使用する xSeries インストール・プロセスでインストールが完了します。</p>	
リソース名 (RSRCNAME)	<p>Windows サーバー・ハードウェアを識別します。</p> <p>iSCSI 接続 xSeries および IBM BladeCenter サーバーの場合、*ISCSI のリソース名を指定します。</p> <p>IXS および IXA の両方に接続されている xSeries サーバーの場合、ファイル・サーバー IOA リソース名を入力します。名前を確かめるには、i5/OS コマンド行で DSPHDWRSC *CMN (通信ハードウェア・リソースの表示) を入力します。リソース名は、LINxx で表されます。xx は数値です。</p> <p>97 ページの『ヒント: 複数の統合サーバーがある場合のリソース名の検索』</p>	

フィールド	説明および指示	値
TCP/IP ポート構成 (TCPPOORTCFG)	<p>ローカルで制御される各アダプター・ポートに固有の Windows TCP/IP 構成値を指定してください。それ以外の場合は、このステップをスキップして、デフォルト値 *NONE を使用します。</p> <p>注: TCPPOORTCFG パラメーターを使用して構成できるのは、iSeries によって直接管理され、IXS により論理的に制御されているアダプターだけです。IXA または iSCSI HBA と接続されており、xSeries サーバーによって管理されている LAN アダプターはこのパラメーターで構成することはできません。</p>	<ul style="list-style-type: none"> • ポート 1 <ul style="list-style-type: none"> - IP アドレス - サブネット・マスク - ゲートウェイ (オプション) • ポート 2 <ul style="list-style-type: none"> - IP アドレス - サブネット・マスク - ゲートウェイ (オプション) • ポート 3 <ul style="list-style-type: none"> - IP アドレス - サブネット・マスク - ゲートウェイ (オプション) • ポート 4 <ul style="list-style-type: none"> - IP アドレス - サブネット・マスク - ゲートウェイ (オプション)

フィールド	説明および指示	値
仮想イーサネット・ポート (VRTETHPORT)	<p>ファイル・サーバーによって使用される仮想イーサネット・ネットワークの TCP/IP 構成を指定します。</p> <p>Windows クラスタ・サービスをインストールするには、それに一致している仮想イーサネット・ポートが必要です。</p> <p>*NONE: 仮想イーサネット・ポート構成はないことを指定します。</p> <p>要素 1: ポート</p> <ul style="list-style-type: none"> • *VRTETHx: ネットワーク・サーバーの仮想イーサネット・ポート <i>x</i> が構成されます (<i>x</i> の値は 0 から 9 まで)。 <p>要素 2: Windows IP アドレス ポートの Windows IP アドレス。形式は <i>nnn.nnn.nnn.nnn</i> で、<i>nnn</i> は、0 から 255 の範囲の 10 進数です</p> <p>要素 3: Windows サブネット・マスク <i>nnn.nnn.nnn.nnn</i> の形式の Windows IP アドレスのサブネット・マスク。ただし <i>nnn</i> は、0 から 255 の範囲の 10 進数です。</p> <p>要素 4: 関連ポート Windows ネットワーク・サーバーとネットワークとの間に接続を確立するために使用される、ポートを説明するためのリソース名。</p> <ul style="list-style-type: none"> • *NONE 関連ポート・リソース名は、回線と関連していません。 • resource-name リソース名。 	<ul style="list-style-type: none"> • 仮想ポート 1 <ul style="list-style-type: none"> - *VRTETHx - IP アドレス - サブネット・マスク - 関連するポート (オプション) • 仮想ポート 2 <ul style="list-style-type: none"> - *VRTETHx - IP アドレス - サブネット・マスク - 関連するポート (オプション) • 仮想ポート 3 <ul style="list-style-type: none"> - *VRTETHx - IP アドレス - サブネット・マスク - 関連するポート (オプション) • 仮想ポート 4 <ul style="list-style-type: none"> - *VRTETHx - IP アドレス - サブネット・マスク - 関連するポート (オプション)
TCP/IP ローカル・ドメイン名 (TCPDMNNAME)	統合サーバーに関連した TCP/IP ローカル・ドメイン名を指定します。i5/OS システムが使用するものと同じ値を使用するには、*SYS を指定できます。	
TCP/IP ネーム・サーバー・システム (TCPNAMSVR)	統合サーバーが使用するネーム・サーバーの IP アドレスを指定します。IP アドレスは最高 3 つまで指定できます。また、*SYS を指定すれば、i5/OS が使用するのと同じ値を使用することもできます。	
ワークグループ用 (TOWRKGRP)	サーバーが関与する Windows サーバー・ワークグループの名前を指定します。	
ドメイン用 (TODMN)	サーバーが関与する Windows ドメインの名前を指定します。	

フィールド	説明および指示	値
サーバー・メッセージ待ち行列とライブラリー (MSGQ)	<p>メッセージ待ち行列の名前とそれが入っているライブラリーを指定します。メッセージ待ち行列がない場合、INSWNTSVR コマンドで作成します。メッセージ待ち行列には、このサーバーに関連したすべてのイベント・ログおよびエラーが送信されます。MSGQ 名およびライブラリーを指定する必要があります。また、*JOBLOG も指定できます。その指定によって、重大でないエラーはユーザー管理モニターのジョブ・ログに送信され、重大エラーは QSYSOPR に送信されます。</p> <p>*NONE を指定すると、重大でないエラーは i5/OS には送信されず、重大エラーは QSYSOPR に送信されます。</p>	<p>待ち行列: ライブラリー:</p>
イベント・ログ (EVTLOG)	<p>i5/OS がイベント・ログ・メッセージを統合サーバーから受け取るかどうかを指定します。選択できるのは、すべて (all)、システム (system)、セキュリティー (security)、アプリケーション (application) またはなし (none) のいずれかです。</p> <p>*ALL i5/OS はすべてのイベント・ログ・メッセージを受け取ります。</p> <p>*NONE イベント・ログ・メッセージは受け取りません。</p> <p>*SYS i5/OS はシステム・イベント・ログ・メッセージを受け取ります。</p> <p>*SEC i5/OS はセキュリティー・イベント・ログ・メッセージを受け取ります。</p> <p>*APP i5/OS はアプリケーション・イベント・ログ・メッセージを受け取ります。</p> <p>注: 統合サーバーがセキュリティー・ログを (*ALL または *SEC を指定することによって) iSeries に送信するようにした場合は、メッセージ待ち行列を必ず適切なセキュリティーとともにセットアップしてください。</p>	

フィールド	説明および指示	値
インストール・ソースとシステム・ドライブのサイズおよび補助記憶域プール (ASP) (SVRSTGSIZE) (SVRSTGASP) (STGASPDEV)	<p>インストール・ソースおよびシステム・ドライブ用のネットワーク・サーバー記憶域スペースのサイズを指定します。また、必要な ASP (1 から 255) の指定も行います。ASP 装置名は、記憶域スペースを独立した補助記憶域プール内に作成する必要があるとき、ASP 番号 33 から 255 の代わりに指定できます。しかし、名前を使用した場合は、ASP 番号フィールドはデフォルト値の 1 またはプレースホルダー値の *N のままにしておく必要があります。</p> <p>インストール・ソース・ドライブ (ドライブ D) は、Windows サーバー・インストール CD イメージ上の I386 ディレクトリーと、IBM i5/OS Integrated Server コードを保持するための十分な大きさがなければなりません。</p> <p>システム・ドライブ (ドライブ C) は、Windows サーバー・オペレーティング・システムを保持するのに十分な大きさでなければなりません。限度は、リソースの容量に応じて 1,024 MB 以上 1,024,000 MB 以下になります。次の要素を考慮してください。</p> <ul style="list-style-type: none"> • Windows サーバーのバージョン (オペレーティング・システムの要件については、Microsoft の資料を参照してください。) • 主な使用法 (印刷/ファイル処理) と端末サーバー数。 • システム・ドライブのフリー・スペース。 • アプリケーション・リソースの所要量。 • クラッシュ・ダンプ・ファイルの必要。 • サーバーにインストール済みのメモリー <p>i5/OSは FAT32 または NTFS ネットワーク・サーバー記憶域スペースとしてドライブを作成し、リンクします。</p> <p>これらのドライブについての詳細は、179 ページの『統合 Windows サーバーの事前定義ディスク・ドライブ』を参照してください。</p> <p>注:</p> <ol style="list-style-type: none"> 1. INSWNTSVR コマンドはシステム・ドライブのサイズを自動的に最小サイズに設定します。その一部は、Windows バージョンやインストール済みメモリーのような要因に基づいて決定されます。 2. それぞれのドライブのサイズを決定する場合、新しいアプリケーションや Windows サーバー製品のアップグレードなどの、将来に必要な見越した余裕をとっておいてください。SVRSTGSIZE に *CALC を指定する場合、i5/OS は、Windows のインストールに必要な最小限のディスク・サイズを割り振るということに注意してください。アプリケーションまたはデータのスペースがさらに必要な場合は、手動で追加のディスク・サイズを指定することを考慮する必要があります。 3. 独立 ASP (33 から 255) のサポートは、iSeries ナ 	インストール・ソース・ドライブ: サイズ: ASP: ASPDEV: システム・ドライブ: サイズ: ASP: ASPDEV:

フィールド	説明および指示	値
ライセンス・モード (LICMODE)	<p>Microsoft Windows サーバーをインストールするときのライセンス・モードを決定します。</p> <p>要素 1 ライセンス・タイプ:</p> <p>*PERSEAT サーバーにアクセスするマシンごとにクライアント・ライセンス料が支払われていることを示します。</p> <p>*PERSERVER サーバー用のクライアント・ライセンス料が支払われていて、そのサーバーに特定数の並行接続が可能であることを示します。</p> <p>要素 2 クライアント・ライセンス:</p> <p>*NONE クライアント・ライセンスがインストールされていないことを示します。 *PERSEAT が指定されるときには、*NONE が指定されます。</p> <p>クライアント・ライセンスの数: インストールするサーバー用に購入したクライアント・ライセンスの数を指定します。</p> <p>要素 3 Windows Terminal Services:</p> <p>*TSENABLE Windows 2000 の場合、Windows Terminal Services と Terminal Services ライセンスをインストールします。</p> <p>*PERDEVICE *PERDEVICE Windows 2003 Terminal Services をインストールして、接続された各装置が有効な Windows Terminal Server アクセス・ライセンスを持つことを必要とするように構成します。クライアントが Terminal Server アクセス・ライセンスを持つ場合、複数の Terminal Server にアクセスできます。</p> <p>*PERUSER Windows 2003 Terminal Server をインストールして、アクティブ・ユーザーごとに 1 つの Terminal Server アクセス・ライセンスを与えるように構成します。</p> <p>*NONE このサーバーには Terminal Server デスクトップ・ライセンスはありません。</p>	<p>ライセンス・タイプ:</p> <p>クライアント・ライセンス:</p> <p>Terminal Services:</p>

フィールド	説明および指示	値
ドメイン・ユーザーの伝搬 (PRPDMNUSR)	<p>Windows ドメインまたは Active Directory に対してユーザーを伝搬および同期するのにこのサーバーを使用する必要があるかどうかを指定します。</p> <p>*YES このサーバーを介して、ユーザーの更新内容を Windows ドメインまたは Active Directory に送信します。</p> <p>*NO このサーバーを介して、ユーザーの更新内容を Windows ドメインまたは Active Directory に送信しません。</p>	
シャットダウン・タイムアウト (SHUTDTIMO)	i5/OSが 統合サーバーをシャットダウンする前に、プログラムを終了させるために待機する時間を決める値。遅延として、2 分以上 45 分以下を指定できます。値を指定しないなら 15 分に設定されます。	シャットダウン・タイムアウト:
制約付きの装置リソース (RSTDEVRSC)	<p>統合サーバーでの iSeries テープ装置と光ディスク装置の使用を制限します。</p> <p>*NONE 統合サーバーでのテープ装置または光ディスク装置の使用を制限しません。</p> <p>*ALL 統合サーバーでのすべてのテープ装置と光ディスク装置の使用を制限します。</p> <p>*ALLTAPE 統合サーバーでのすべてのテープ・リソースの使用を制限します。</p> <p>*ALLOPT 統合サーバーでのすべての光ディスク・リソースの使用を制限します。</p> <p>restricted-device 統合サーバーでの使用を不能にしたい最大 10 個の装置リソースを指定します。</p>	
時間帯	(オプション) インストールの Windows サーバーの段階で使用する iSeries の時間帯を記録します。67 ページの『時刻合わせ』を参照してください。	

フィールド	説明および指示	値
仮想イーサネット Point-to-Point (VRTPTPPORT)	<p>ローカル・エリア・ネットワーク (29 ページの『ネットワークの概念』を参照) は、i5/OS と Windows サーバーとの間に存在します。この LAN の i5/OS 側と Windows サーバー側の両方に IP アドレスとサブネット・マスクがあります。</p> <p>注: デフォルトでは、INSWNTSVR コマンドでこれらのアドレスは自動的に設定されます。アドレスは 192.168.xx.yy の形式になっています。クラス C アドレスを使用するサイトの場合、重複した IP アドレスが生成される可能性があります。</p> <p>競合が生じないようにするため、システム全体を通して固有アドレスとなる IP アドレスを指定することもできます。a.b.x.y の形式のアドレスを使用してください (a.b.x は Point-to-Point 仮想イーサネットの両端で同じ値になります)。また、その Point-to-Point 仮想イーサネットが i5/OS で独自のサブネットを占有していることを確認してください。</p> <p>INSWNTSVR コマンドの追加パラメーターの下にある仮想 PTP イーサネット・ポート・パラメーターを使用してください。</p> <p>サブネット・マスクは必ず 255.255.255.0 です。</p>	<p>i5/OS 側の IP アドレス:</p> <p>Windows サーバー側の IP アドレス:</p>
構成ファイル (CFGFILE)	<p>インストール中に、カスタマイズされた NWSD を作成して指定します (275 ページの『第 15 章 ネットワーク・サーバー記述構成ファイル』を参照)。</p> <p>デフォルトは *NONE です。すでに作成されている構成ファイルを指定する場合、ファイルの名前およびそのファイルが保管されているライブラリーの名前 (*LIBL、*CURLIB、またはそのライブラリーの名前) と置き換えます。</p>	

追加の Internet SCSI (iSCSI) パラメーターのインストール・ワークシート

フィールド	説明および指示	値
活動化タイマー (ACTTMR)	<p>リモート・サーバーのサービス・プロセッサへの接続が確立されて、それによってリモート・サーバーの電源がオンになるまでシステムが待機する時間 (秒) を指定します。デフォルト値は 120 です。値 (秒) を 30 から 1800 の範囲で指定します。</p>	活動化タイマー:

フィールド	説明および指示	値
通信メッセージ待ち 行列 (CMNMSGQ)	<p>通信状況メッセージを受信するメッセージ待ち行列名を指定します。</p> <p>修飾子 1:</p> <ul style="list-style-type: none"> • *SYSOPR メッセージをシステム・オペレーター・メッセージ待ち行列に入れます。 • name 通信状況メッセージを受信するメッセージ待ち行列名を指定します。 <p>修飾子 2:</p> <ul style="list-style-type: none"> • *LIBL 最初の一致が見つかるまで、ジョブのライブラリー・リストのすべてのライブラリーが検索されます。 • *CURLIB ジョブの現行ライブラリーが検索されます。ジョブの現行ライブラリーとしてライブラリーを指定しない場合には、QGPLライブラリーが使用されます。 • library-name 使用するライブラリーの名前を指定してください。 	<p>メッセージ待ち行列:</p> <p>ライブラリー:</p>
記憶域パス (STGPTH)	<p>記憶域スペースが使用できる記憶域パスを指定します。この情報は、ネットワーク・サーバー・ホスト・アダプター (NWSH) 記述から成っています。</p> <p>注: サーバーのインストール後に、さらに記憶域パスを追加できます。</p> <p>name 既存のネットワーク・サーバー・ホスト・アダプター (NWSH) 記述の名前を指定します。</p>	NWSH 名:

フィールド	説明および指示	値
仮想イーサネット・パス (VRTETHPTH)	<p>イーサネット回線記述が使用できる仮想イーサネット・パスを指定します。この情報は、仮想イーサネット・ポートおよびネットワーク・サーバー・ホスト・アダプター (NWSH) 記述を含む 2 つの部分から構成されています。このパラメーターには最大 5 つの値を入力できます。*VRTETHPTH 回線記述名が使用するパスである仮想イーサネット・パスを少なくとも 1 つ入力しなければなりません。</p> <p>注: サーバーのインストール後に、仮想イーサネット・パスを追加できます。</p> <p>要素 1: ポート</p> <p>*VRTETHPTH</p> <p>ネットワーク・サーバーの仮想イーサネット Point-to-Point ポートが構成されます。</p> <p>*VRTETH_x ネットワーク・サーバーの仮想イーサネット・ポート <i>x</i> が構成されます (<i>x</i> の値は 0 から 9 まで)。</p> <p>要素 2: ネットワーク・サーバー・ホスト・アダプター</p> <p>name 既存のネットワーク・サーバー・ホスト・アダプター (NWSH) 記述の名前を指定します。ネットワーク・サーバー・ホスト・アダプター名は、この NWSH の各 VRTETHPTH パラメーターごとに固有である必要はありません。</p>	仮想イーサネット・パス: ポート: NWSH:
シャットダウン TCP ポート (SHUTDPORT)	<p>シャットダウンに使用する TCP ポートを指定します。</p> <p>注: これは、拡張パラメーターで、iSCSI ネットワーク内にファイアウォールがある場合に役に立ちます。</p> <p>8700 TCP ポート番号 8700 を使用します。</p> <p>integer</p> <p>シャットダウンに使用されるポートを識別するポート番号を指定します。有効値は、1024 から 65,535 の範囲になります。</p>	
仮想イーサネット制御ポート (VRTETHCTLP)	<p>仮想イーサネット制御に使用する TCP ポートを指定します。</p> <p>注: これは、拡張パラメーターで、iSCSI ネットワーク内にファイアウォールがある場合に役に立ちます。</p> <p>8800 TCP ポート番号 8800 を使用します。</p> <p>integer</p> <p>仮想イーサネット制御に使用されるポートを識別するポート番号を指定します。有効値は、1024 から 65,535 の範囲になります。</p>	

フィールド	説明および指示	値
リモート・システム NWSCFG (RMTNWSCFG)	<p>このサーバーで使用するリモート・システム・ネットワーク・サーバーの構成を指定します。</p> <p>注: INSWNTSVR コマンドの実行前にリモート・システムの構成を作成するのが望ましい場合があり、必要でさえある場合があります。 71 ページの『サービス・プロセッサ構成およびリモート・システム構成の作成』を参照してください。</p> <p>*DFT システム生成されたデフォルトのリモート・システム・ネットワーク・サーバー構成名、 'nwsdnameRM' を使用します。ここで nwsdname は、このネットワーク・サーバー記述の名前です。</p> <p>name 既存のリモート・システム・ネットワーク・サーバー構成の名前を指定します。</p>	
サービス・プロセッサ NWSCFG (SPNWSCFG)	<p>このサーバーで使用するサービス・プロセッサ・ネットワーク・サーバーの構成を指定します。</p> <p>注: INSWNTSVR コマンドの実行前にサービス・プロセッサの構成を作成するのが望ましい場合があり、必要でさえある場合があります。 71 ページの『サービス・プロセッサ構成およびリモート・システム構成の作成』を参照してください。</p> <p>*DFT システム生成されたデフォルトのサービス・プロセッサ・ネットワーク・サーバー構成名、 'nwsdnameSP' を使用します。ここで nwsdname は、このネットワーク・サーバー記述の名前です。</p> <p>name 既存のサービス・プロセッサ・ネットワーク・サーバー構成の名前を指定します。</p>	
接続機密保護 NWSCFG (CNNNWSCFG)	<p>このサーバーで使用する接続機密保護ネットワーク・サーバーの構成を指定します。</p> <p>*DFT システム生成されたデフォルトの接続機密保護ネットワーク・サーバー構成名、 'nwsdnameCN' を使用します。ここで nwsdname は、このネットワーク・サーバー記述の名前です。</p> <p>name 既存の接続機密保護ネットワーク・サーバー構成の名前を指定します。</p>	

フィールド	説明および指示	値
省略時 IP 機密保護規則 (DFTSECRULE)	<p>ホスト側とリモート・システム間で使用するデフォルトの IP 機密保護 (IPSEC) 規則を指定します。</p> <p>注: CNNNWSCFG パラメーターの既存の接続機密保護構成を指定した場合、このパラメーターの値を指定することはできません。</p> <p>*NONE IP 機密保護規則は構成されません。</p> <p>*GEN システムがランダム事前共用キーを自動的に生成します。</p> <p>pre-shared-key 事前共用キーを指定します。事前共用キーは、32 文字までの長さの非単純ストリングです。</p>	
IP 機密保護規則 (IPSECRULE)	<p>既存の接続機密保護ネットワーク・サーバー構成に定義され、ホスト側とリモート・システム間の初期 IP 機密保護設定として使用される IP 機密保護規則 (IPSECRULE) パラメーターの相対項目を指定します。</p> <p>*DFTSECRULE 省略時 IP 機密保護規則 (DFTSECRULE) パラメーターに指定された値を使用します。</p> <p>*NONE リモート・インターフェースで、機密保護規則は使用されません。</p> <p>1-16 リモート・インターフェースで、指定された機密保護規則が使用されます。</p>	

フィールド	説明および指示	値
サービス・プロセッサの初期化 (INZSP)	<p>リモート・システムのサービス・プロセッサの保護方法を指定します。</p> <p>注: サービス・プロセッサ構成がすでに存在する場合、*SYNC を指定することはできません。サービス・プロセッサ構成がない場合、*MANUAL、*AUTO、および *NONE だけが使用されます。</p> <p>*MANUAL これは、最も保護された方式です。サービス・プロセッサのユーザー名、パスワードおよび証明書を手動で構成する必要があります。証明書管理が必要となります。サービス・プロセッサのパスワードを保護するために、公衆ネットワーク上で接続する時には、この方式が適切です。</p> <p>*AUTO リモート・システムのサービス・プロセッサにあるパラメーターを手動で構成する必要はありません。リモート・システムのサービス・プロセッサが証明書を自動的に生成します。この接続は、いったん初期化されれば保護されます。物理的に保護されているか、あるいはファイアウォールによって保護されているサービス・プロセッサにネットワーク上で接続する場合には、このオプションが適切です。</p> <p>*SYNC このネットワーク・サーバー構成は、ユーザー、パスワードおよび自己署名証明書をサービス・プロセッサと同期します。</p> <p>*NONE サービス・プロセッサのパスワードに対する機密保護はありません。物理的に安全なネットワーク上でサービス・プロセッサに接続するまでは、これを使用しないでください。</p>	
ユニキャストを使用可能にする (ENBUNICAST)	<p>ユニキャストとは、パケットが指定されたサービス・プロセッサ名 (SPNAME) またはサービス・プロセッサ・アドレス (SPINTNETA) パラメーターに直接送信される送信方式です。*AUTO が指定されて、システム・ハードウェアがそれをサポートしている場合には、格納装置 ID (EID) パラメーターのシステム識別が自動的に検索されます。</p> <p>注: SPNWSCFG パラメーターの既存のサービス・プロセッサ構成を指定した場合、このパラメーターの値を指定することはできません。</p> <p>*NO ユニキャストを使用不可にします</p> <p>*YES ユニキャストを使用可能にします。</p>	

フィールド	説明および指示	値
格納装置 ID (EID)	<p>サービス・プロセッサが入っている格納装置の識別製造番号、タイプおよび型式を指定します。</p> <p>ENBUNICAST(*NO) が指定された場合には、ネットワーク上のリモート・システムの場所を探索するために、これが必要となります。システムのラベルにあるこれらの値を調べてください。</p> <p>注: SPNWSCFG パラメーターの既存のサービス・プロセッサ構成を指定した場合、このパラメーターの値を指定することはできません。</p> <p>*AUTO ENBUNICAST(*YES) が指定された場合には、自動的に ID を検索します。</p> <p>要素 1: 製造番号 リモート・システムのマシン製造番号をダッシュを除く英数字のみを使用して指定します。</p> <p>要素 2: 製造元のタイプおよび型式 リモート・システムのマシン・タイプおよび型式を ttttmmm の形式で指定します。この tttt はマシン・タイプであり、mmm はマシン型式番号です。</p>	
サービス・プロセッサ名 (SPNAME)	<p>リモート・システムのサービス・プロセッサ・ホスト名を指定します。</p> <p>注: SPNWSCFG パラメーターの既存のサービス・プロセッサ構成を指定した場合、このパラメーターの値を指定することはできません。</p> <p>*SPINTNETA リモート・システムは、サービス・プロセッサ・アドレス (SPINTNETA) パラメーターに指定された値によって識別されます。</p> <p>host-name: リモート・システムのサービス・プロセッサ・ホスト名を指定します。</p>	
サービス・プロセッサ・アドレス (SPINTNETA)	<p>リモート・システムのサービス・プロセッサ IP アドレスを指定します。IP アドレスは nnn.nnn.nnn.nnn の 10 進数形式で表現され、ここで nnn は 0 から 255 の範囲の 10 進数です。</p> <p>注: SPNWSCFG パラメーターの既存のサービス・プロセッサ構成を指定した場合、このパラメーターの値を指定することはできません。</p> <p>internet-address: サービス・プロセッサの IP アドレスを指定します。</p>	

フィールド	説明および指示	値
SP 認証 (SPAUT)	<p>サービス・プロセッサのユーザー名およびパスワードを指定します。</p> <p>注: SPNWSCFG パラメーターの既存のサービス・プロセッサ構成を指定した場合、このパラメーターの値を指定することはできません。</p> <p>*DFT デフォルトのサービス・プロセッサのユーザー ID およびパスワードが使用されます。</p> <p>要素 1: ユーザー名 リモート・システムのサービス・プロセッサ・ユーザー名を指定します。</p> <p>要素 2: ユーザー・パスワード リモート・システムのサービス・プロセッサ・パスワードを指定します。パスワードは少なくとも 5 文字の長さで、少なくとも 1 つの英字と 1 つの数値またはシンボリック文字が含まれていなければなりません。</p>	<p>名前:</p> <p>パスワード:</p>

フィールド	説明および指示	値
SP 証明書 ID (SPCERTID)	<p>SP 証明書 ID は、サービス・プロセッサの証明書を識別する可能な 3 つのフィールドの 1つを指定します。このパラメーターを指定して、証明書がサービス・プロセッサからのものであることの追加検証を提供します。選択したフィールドの内容は、証明書が生成されたか、あるいは認証局から要求された時に入力したフィールドの値と正確に一致していなければなりません。</p> <p>注: SPNWSCFG パラメーターの既存のサービス・プロセッサ構成を指定した場合、このパラメーターの値を指定することはできません。</p> <p>単一値:</p> <p>*NONE サービス・プロセッサ証明書は構成されません。</p> <p>要素 1: コンポーネント</p> <p>*COMMONNAME 証明書が生成されたか、あるいは認証局から要求された時に指定される証明書共通名を選択します。リモート監視プログラム・アダプター II では、これを自己署名証明書の生成または証明書署名要求の生成に使用される「ASM ドメイン名」フィールドに相互に関連付けます。</p> <p>*EMAIL 証明書が生成されたか、あるいは認証局から要求された時に指定される証明書の E メール・アドレスを選択します。リモート監視プログラム・アダプター II では、これを自己署名証明書の生成または証明書署名要求の生成に使用される「E メール・アドレス」フィールドに相互に関連付けます。</p> <p>*ORGUNIT 証明書が生成されたか、あるいは認証局から要求された時に指定される証明書の組織単位を選択します。リモート監視プログラム・アダプター II では、これを自己署名証明書の生成または証明書署名要求の生成に使用される「組織単位」フィールドに相互に関連付けます。</p> <p>要素 2: 比較値</p> <p>compare-value 証明書コンポーネントの比較値を指定します。255 文字以内のテキストをアポストロフィで囲んで指定します。</p>	<p>コンポーネント:</p> <p>比較値:</p>

フィールド	説明および指示	値
リモート・システム ID (RMTSYSID)	<p>リモート・システムの識別製造番号、タイプおよび型式を指定します。指定された場合には、これは、ネットワーク上のリモート・システムの場所を探索するために使用されます。リモート・システムのラベルにあるこれらの値を調べてください。</p> <p>注: RMTNWSCFG パラメーターの既存のリモート・システム構成を指定した場合、このパラメーターの値を指定することはできません。</p> <p>単一値:</p> <p>*EID サービス・プロセッサ格納装置 ID を使用します。</p> <p>要素 1: 製造番号</p> <p>serial-number リモート・システムのマシン製造番号を指定します。</p> <p>要素 2: 製造元のタイプおよび型式</p> <p>type-model</p> <p>リモート・システムのマシン・タイプおよび型式を <code>ttttmmm</code> の形式で指定します。この <code>tttt</code> はマシン・タイプであり、<code>mmm</code> はマシン型式番号です。</p>	<p>製造番号:</p> <p>製造元のタイプおよび型式:</p>
配信方法 (DELIVERY)	<p>リモート・システムの構成に必要なパラメーターの配信方法を指定します。</p> <p>注: RMTNWSCFG パラメーターの既存のリモート・システム構成を指定した場合、このパラメーターの値を指定することはできません。</p> <p>*DYNAMIC</p> <p>パラメーターは、DHCP を使用してリモート・システムに動的に配信されます。</p> <p>*MANUAL</p> <p>パラメーターは、BIOS ユーティリティ (システム BIOS またはアダプター BIOS - CTRL-Q) を使用してリモート・システム上に手動で構成されます。</p>	

フィールド	説明および指示	値
CHAP 認証 (CHAPAUT)	<p>リモート・システムの起動側ノードを認証するための、ホスト・システム iSCSI ターゲットの Challenge Handshake Authentication Protocol (CHAP)を指定します。</p> <p>注: RMTNWSCFG パラメーターの既存のリモート・システム構成を指定した場合、このパラメーターの値を指定することはできません。</p> <p>単一値:</p> <p>*NONE CHAP 認証は使用可能ではありません。</p> <p>要素 1: CHAP 名 CHAP 名を指定します。</p> <p>要素 2: CHAP 機密事項 Challenge Handshake Authentication Protocol で使用したい機密事項を、24 文字までの長さの値として指定します。</p>	<p>CHAP 名:</p> <p>CHAP 機密事項:</p>
ブート装置 ID (BOOTDEVID)	<p>ブート元に使用するリモート・システム中の iSCSI アダプターの PCI 機能アドレス (バス/装置/機能) を指定します。この情報は、BIOS ユーティリティ (システム BIOS またはアダプター BIOS - CTRL-Q) を使用してアクセスすることができます。</p> <p>注: RMTNWSCFG パラメーターの既存のリモート・システム構成を指定した場合、このパラメーターの値を指定することはできません。</p> <p>単一値:</p> <p>*SINGLE 単一の iSCSI アダプターがリモート・システムで使用されます。注: サーバーに複数の iSCSI アダプターが導入されているリモート・システムでは、どのアダプターをブート元を使用するかを指定する必要があります。</p> <p>要素 1: バス番号 ブートに使用するリモート・システムの iSCSI アダプターのバス番号を指定します。</p> <p>要素 2: 装置番号 ブートに使用するリモート・システムの iSCSI アダプターの装置番号を指定します。</p> <p>要素 3: 機能 function-number ブートに使用するリモート・システムの iSCSI アダプターの機能番号を指定します。</p>	<p>バス番号:</p> <p>装置:</p> <p>機能:</p>

フィールド	説明および指示	値
動的ブート・オプション (DYNBOOTOPT)	<p>これは拡張機能です。</p> <p>このパラメーターは、iSCSI ターゲット・ホスト・バス・アダプターのファームウェアの一部である内部 DHCP サーバーを構成するために使用され、リモート iSCSI 起動側の IP アドレスおよびディスクレス・ブート・パラメーターの指定が必要となります。</p> <p>注: RMTNWSCFG パラメーターの既存のリモート・システム構成を指定した場合、このパラメーターの値を指定することはできません。</p> <p>要素 1: ベンダー ID クライアントおよびサーバーは固定されたベンダー ID に対して事前構成されます。ネットワーク管理者はクライアントを構成して、ハードウェア、オペレーティング・システムまたはその他の識別情報を伝達するためのそれぞれに固有の識別値を定義することができます。IETF RFC 2132 に記述された DHCP オプション 60 がこの機能で使用されます。</p> <p>*DFT デフォルトのベンダー ID が使用されます。</p> <p>vendor-id リモート・システムの iSCSI アダプターのベンダー ID が使用されます。</p> <p>要素 2: 代替クライアント ID サーバーに対して固有の ID を指定するためにクライアントによって使用されます。それぞれのクライアントの ID は、クライアントの接続先である有効な DHCP ネットワーク（すなわち、クライアントのローカル・サブネットおよび DHCP リレーを使用して到達可能なリモート・サブネット）で使用されるその他すべてのクライアント ID の間で固有のものでなければなりません。この固有性の要件を満たすクライアント ID を選択する責任は、ベンダーおよびシステム管理者にあります。IETF RFC 2132 に記述された DHCP オプション 61 がこの機能で使用されます。</p> <p>*ADPT デフォルトのクライアント ID は、リモート・システムの iSCSI アダプターのアダプター・アドレスから構成されます。この値はリモート・システムを識別するために使用されます。</p> <p>client-id ブートに使用するリモート・システムの iSCSI アダプターのクライアント ID を指定してください。</p>	<p>ベンダー ID:</p> <p>代替クライアント ID:</p>

フィールド	説明および指示	値
リモート・インターフェース (RMTIFC)	<p>リモート・システム・インターフェースを指定します。この情報は、リモート・システムのインターフェースの識別して構成するために使用されます。各アダプターには、SCSI および LAN インターフェースをサポートするための 2 つの機能があります。</p> <p>注: RMTNWSCFG パラメーターの既存のリモート・システム構成を指定した場合、このパラメーターの値を指定することはできません。</p> <p>要素 1: SCSI インターフェース</p> <p>要素 1: アダプター・アドレス リモート・システムの SCSI インターフェースの 12 文字の 16 進数アダプター・アドレスを指定します。</p> <p>要素 2: IP アドレス</p> <p>internet-address リモート・システムの SCSI インターフェース用。</p> <p>要素 3: サブネット・マスク</p> <p>subnet-mask リモート・システムの SCSI インターフェース用。</p> <p>要素 4: ゲートウェイ・アドレス</p> <p>gateway-address リモート・システムの SCSI インターフェース用。</p> <p>要素 5: iSCSI 修飾名</p> <p>*GEN</p> <p>システムが iSCSI 修飾名を自動的に生成します。</p> <p>iqn-name</p> <p>リモート・システムの SCSI インターフェースの iSCSI 修飾名。</p>	<p>SCSI インターフェース</p> <ul style="list-style-type: none"> • アダプター・アドレス: • IP アドレス: • サブネット・マスク: • ゲートウェイ・アドレス (オプション): • iSCSI 修飾名:
リモート・インターフェース (RMTIFC) 続き	<p>要素 2: LAN インターフェース</p> <p>要素 1: アダプター・アドレス</p> <p>リモート・システムの LAN または TCP Offload Engine (TOE) インターフェースの 12 文字の 16 進アダプター・アドレス。</p> <p>要素 2: IP アドレス</p> <p>リモート・システムの LAN インターフェース用。</p> <p>要素 3: サブネット・マスク</p> <p>リモート・システムの LAN インターフェース用。</p> <p>要素 4: ゲートウェイ・アドレス</p> <p>リモート・システムの LAN インターフェース用。</p>	<p>LAN インターフェース</p> <ul style="list-style-type: none"> • アダプター・アドレス: • IP アドレス: • サブネット・マスク: • ゲートウェイ・アドレス (オプション):

Windows クラスタ・サービスの情報

- 注:
1. クラスタ化された統合サーバーをインストールするときで、ハードウェア・モデルが Windows クラスタ・サービスをサポートしている場合のみ、このワークシートに記入してください。(統合 Netfinity サーバーは Windows クラスタ・サービスをサポートしていません。)
 2. ネットワーク・アダプターのことを i5/OS では「ポート」と言います。

項目	説明および指示	値
クラスタ名	<p>クラスタの名前を指定します。管理者はこの名前をクラスタへの接続で使用します。クラスタ名は、ドメイン名、ドメイン内のすべてのコンピューター名、およびドメイン内の他のクラスタ名のいずれとも異ならなければなりません。</p> <p>Windows クラスタのクォーラム・リソースとして使用されるネットワーク・サーバー記憶域スペースの作成でもクラスタ名を使用します。</p> <p>*NONE: Windows クラスタを形成したり結合したりしません。</p> <p>cluster-name: クラスタの名前を指定します。</p>	

項目	説明および指示	値
クラスターの構成: (要素 1 から 4)	<p>新規の Windows クラスターを構成するのに必要なパラメーターを指定します。</p> <p>注: このパラメーターは、i5/OS クラスター構成の検証に使用されます。クラスター・サービスのインストールには、Microsoft の構成ウィザードを使用します。</p> <p>このパラメーターが必要なのは、クラスター名 (CLU) パラメーターを使って新規の Windows クラスターを作成する場合のみです。</p> <p>要素 1: クラスターのドメイン名 クラスターが所属するドメインを指定します。クラスターがすでに存在する場合、そのクラスターに結合されますが、存在しない場合はクラスターが作成されます。クラスターを作成するには、クラスターの構成 (CLUCFG) パラメーターを指定しなければなりません。</p> <p>cluster-domain-name: 新規のクラスターの作成時に、クラスターが属するドメイン名を指定します。</p> <p>要素 2: クォーラム・リソース・サイズ Windows クォーラム・リソースとして使用する記憶域スペースのサイズをメガバイト単位で指定します。</p> <p>*CALC サイズを Windows サーバー・バージョン (WNTVER) パラメーターに基づくデフォルト値として計算することを指定します。</p> <p>quorum-size Windows クォーラム・リソース・サイズをメガバイト単位で指定します。サイズは 550 メガバイト以上、1024000 メガバイト以下でなければなりません。</p> <p>要素 3: クォーラム・リソース ASP Windows のクォーラム・リソースとして使用する記憶域スペース用の補助記憶域プールを指定します。以下の値のうちのいずれか 1 つを指定します。</p> <p>1: 記憶域スペースは、補助記憶域プール 1 (システム補助記憶域プール (ASP)) 内に作成されます。</p> <p>quorum-ASP: ASP の ID として 2 から 255 までの範囲の値を指定します。有効値は、システムでいくつの ASP が定義されているかによって異なります。</p> <p>要素 4: クォーラム ASP 装置 Windows のクォーラム・リソースとして使用する独立した記憶域スペース用の補助記憶域プールの装置名を指定します。注: クォーラム・リソース ASP とクォーラム ASP 装置値との両方を指定することはできません。</p>	クラスターのドメイン名: クォーラム・リソース・サイズ: クォーラム・リソース ASP: クォーラム ASP 装置:

項目	説明および指示	値
クラスター構成: (要素 5 から 7)	<p>要素 5: クラスター接続ポート クラスター・サービスの通信に使用する接続ポートを指定します。</p> <p>*VRTETH_x: ネットワーク・サーバーの仮想イーサネット・ポート x が構成されます。ただし x は、0 から 9 の値を持ちます。</p> <p>注: 仮想イーサネット・ポートは、この値に一致するように構成されていなければなりません。要素 6: クラスター IP アドレス クラスターの IP アドレスを指定します。</p> <p>IP アドレス $xxx.yyy.zzz.nnn$ の形式のクラスターの IP アドレスを指定します。ただし xxx、yyy、zzz、および nnn は、0 から 255 までの 10 進数です。</p> <p>注: 選択する IP アドレスは、すべての NWS D オブジェクトと i5/OS TCP/IP 構成を通して固有でなければなりません。</p> <p>要素 7: クラスター・サブネット・マスク</p> <p>subnet-mask: $nnn.nnn.nnn.nnn$ の形式のクラスターのサブネット・マスクを指定します。ただし nnn は、0 から 255 までの 10 進数です。</p>	<p>接続ポート:</p> <p>クラスターの IP アドレス:</p> <p>クラスター・サブネット・マスク:</p>

FAT、FAT32、および NTFS ファイル・システムの比較

- Windows 2000 Server または Windows Server 2003 では、NTFS および FAT32 ファイル・システムの中から選ぶことができます。IBM i5/OS 統合サーバー・サポートは、ハードウェア・リソースの諸機能、Windows のバージョン、および使用目的に合った適切なファイル・システムを使ってシステム・ドライブをインストールします。インストール・コマンドは、CVTNTFS(*NO) が指定されない場合には、FAT32 ドライブを NTFS に変換します。

注: D ドライブを NTFS に変換しないでください。FAT のままでなければなりません。

C ドライブを変換するオプションはありません。使用するファイル・システムの決定に役立つように、以下にそれらの比較を示します。

FAT	FAT32	NTFS
ボリュームはフロッピー・ディスクットのサイズから最大 4 GB まで。	ボリュームは 512 MB から 2 TB まで。	ボリュームは 10 MB から 2 TB まで。
最大ファイル・サイズは 2 GB。	最大ファイル・サイズは 4 GB。	ファイル・サイズはボリュームのサイズによって制限されます。
Windows 2000 または Windows Server 2003 Active Directory をサポートしていません。	Windows 2000 または Windows Server 2003 Active Directory をサポートしていません。	Windows 2000 または Windows Server 2003 Active Directory または共用クラスター・ドライブを使用するのに必要です。

FAT	FAT32	NTFS
PC-DOS を使用してハード・ディスク上のファイルにアクセスできます。	PC-DOS を使用してハード・ディスク上のファイルにアクセスできます。	PC-DOS を使用してハード・ディスク上のファイルにアクセスすることはできません。
NWSD 構成ファイルを使用してサーバーをカスタマイズできます。	NWSD 構成ファイルを使用してサーバーをカスタマイズできます。	NWSD 構成ファイルを使用できません。
NWSD ダンプ・ツール (QFPDMP) を使用して、ディスクからファイルを取り出して、サービスを得ることができます。	NWSD ダンプ・ツールを使用して、ディスクからファイルを取り出して、サービスを得ることができます。	ダンプ・ツールを使用して、ファイルをディスクから取り出すことはできません。

ヒント: 複数の統合サーバーがある場合のリソース名の検索

同一タイプの複数の統合サーバーを iSeries にインストールすることができます。その場合でも、「通信リソースの表示」画面で、それぞれを区別することはできない場合があります。

リソース名が表す統合サーバーがどれかを検索するには、次のステップを実行します。

- 「通信リソースの表示」画面が表示されていない場合は、DSPHDWRSC *CMN を入力し、Enter キーを押します。
- 「ファイル・サーバー IOA」のリソース名の左側にある「Opt」フィールドに 7 と入力します。「リソース明細の表示」画面が表示されます。iSCSI 接続サーバーの場合、「ネットワーク・サーバー・ホスト・アダプター」を探索します。これは、NWSH オブジェクトを作成する場合に使用するリソースです。NWSH オブジェクト名は、NWSD をインストールする場合に使用します。
- 「設置場所」の見出しの下の「カード位置」を調べます。
- iSeries のスロットのラベルを調べます。1 つのスロットのラベルは、「カード位置」フィールドと同じ数字、または同じ文字と数字の組み合わせになっているはずですが、このスロットには、リソース名が表す統合 xSeries サーバー・ハードウェアが入っています。

73 ページの『i5/OS パラメーターのインストール・ワークシート』に戻ります。

サポートされている言語バージョン

以下の言語が、Windows サーバー導入 (INSWNTSVR) コマンドの、言語バージョン (LNGVER) パラメーターでサポートされています。

LNGVER	国語
*PRIMARY	iSeriesに既にインストールされている基本言語の言語バージョンを使用します。
2911	スロベニア語
2922	ポルトガル語
2923	オランダ語
2924	英 大文字小文字
2925	フィンランド語
2926	デンマーク語
2928	フランス語
2929	ドイツ語
2931	スペイン語

LNGVER	国語
2932	イタリア語
2933	ノルウェー語
2937	スウェーデン語
2938	英大文字 DBCS
2939	ドイツ語 MNCS
2940	フランス語 MNCS
2942	イタリア語 MNCS
2950	英大文字
2962	日本語 DBCS
2963	オランダ語 MNCS
2966	ベルギー・フランス語
2975	チェコ語
2976	ハンガリー語
2978	ポーランド語
2979	ロシア語
2980	ブラジル・ポルトガル語
2981	カナダ・フランス語 MNCS
2984	英大文字小文字 DBCS
2986	韓国語 DBCS
2987	中国語 (繁体字)
2989	中国語 (簡体字)
2994	スロバキア語
2996	ポルトガル語 MNCS


IBM i5/OS 統合サーバー・サポートは Windows 複数言語ユーザー・インターフェースをサポートします。

Windows 2000 Server または Windows Server 2003 のインストール




以下が必要になります。

- Windows 2000 Server または Windows Server 2003 ソフトウェアを含む CD (または CD のイメージ)。
- Windows のライセンス・キー (インストール CD ケースの裏面または認証文書に印刷してあります)。
- 完成および印刷した 73 ページの『i5/OS パラメーターのインストール・ワークシート』、またはインストール・アドバイザーによって生成されたコマンド・ストリング。

注: Windows Server のインストールまたはアップグレードを行う前に、ディスク・ミラーリングを使用不可にする方法および無停電電源装置を切る方法については、Microsoft の資料を参照してください。これは iSeries 上でのディスク・ミラーリングまたは無停電電源装置には適用されないことに注意してください。

注: 62 ページの『ハードウェア要件』セクションにリストされていない統合 xSeries サーバー、統合 xSeries アダプター、または iSCSI HBA がある場合、インストール方法については、IBM 統合 xSeries ソリューション  Web サイト (英語) を参照してください。

以下のステップを実行してください。

1. 統合 xSeries ハードウェアを準備します。詳しくは、以下のリンクを参照してください。
 - IXA インストール、最初にお読みください (英語) 
(www.ibm.com/servers/eserver/series/integratedxseries/ixareadme)
 - iSCSI インストール、最初にお読みください (英語) 
(www.ibm.com/servers/eserver/series/integratedxseries/iscsireadme)
 - IXS インストール、最初にお読みください (英語) 
(www.ibm.com/servers/eserver/series/integratedxseries/ixsreadme)
2. iSCSI 接続サーバーの場合、『Windows のインストールのための iSCSI ハードウェアの準備』を参照してください。
3. 100 ページの『i5/OS コンソールからのインストールの開始』。
4. 104 ページの『統合 Windows サーバー・コンソールからのインストールの続行』。
5. 105 ページの『サーバーのインストールの完了』。

インストール中にエラー・メッセージが出た場合、117 ページの『インストール中のエラー・メッセージへの応答』を参照してください。

Windows のインストールのための iSCSI ハードウェアの準備

iSCSI 接続サーバーの場合、ハードウェアの準備後に構成する追加事項もあります。

- 『サービス・プロセッサ・セキュリティーの初期化』
- 『ネットワーク・サーバー・ホスト・アダプターの作成と開始』

サービス・プロセッサ・セキュリティーの初期化

新規サービス・プロセッサ用に新規サービス・プロセッサ構成を作成する場合、サービス・プロセッサのデフォルトのユーザー名およびパスワードから選択する新規ユーザー名およびパスワードにセキュリティー設定を変更する必要があります。

使用することに決定したセキュリティー・メソッドに対応する手順を以下のリストから選択します。

- SSL のないサービス・プロセッサ・パスワードの場合、145 ページの『サービス・プロセッサ・パスワード』で記述された手順を使用します。
- SSL 付きのサービス・プロセッサ・パスワードの場合、143 ページの『サービス・プロセッサ SSL の構成』で記述された手順を使用します。

ネットワーク・サーバー・ホスト・アダプターの作成と開始

iSCSI 接続サーバーに Windows をインストールする前に、iSeries サーバーにあるターゲット iSCSI HBA を構成する必要があります。この構成はネットワーク・サーバー・ホスト・アダプター (NWSH) 装置と呼ばれます。

- NWSH 装置は 1 つ以上のアクティブ・サーバーで使用することができます。新規サーバーが既存の NWSH 装置を使用する場合には、既存の NWSH 装置が開始されていることを検証します。

- | 新規 NWSH 装置を作成し、開始 (オンに変更) するには、以下のステップのようにします。
- | 1. iSeries ナビゲーターを使用して次のように NWSH ハードウェア・リソースを確認します。
 - | a. 「構成およびサービス」 → 「ハードウェア」 → 「通信」を展開します。
 - | b. ネットワーク・サーバー・ホスト・アダプターの記述があるリソース用のリソース名をメモします。
 - | c. CL コマンドが使用したい場合は、WRKHDWRSC TYPE(*CMN) を使用します。
- | 2. NWSH 装置を作成します。129 ページの『ネットワーク・サーバー・ホスト・アダプター・オブジェクトの作成』を参照してください。
- | 3. NWSH 装置を開始します。131 ページの『ネットワーク・サーバー・ホスト・アダプターの開始』を参照してください。

i5/OS コンソールからのインストールの開始

Windows 2000 Server または Windows Server 2003 を iSeries にインストールするには、*IOSYSCFG、*ALLOBJ、および *JOBCTL 特殊権限が必要です。使用可能な Windows サーバー・ライセンス・キーを持っていないければなりません。ほとんどの場合、キーはインストール CD ケースの裏面に印刷してあります。

- 1. *FULL のインストール・タイプを実行するときは、インストール CD を iSeries サーバー光ディスク装置に入れます (インストール CD のイメージを使用する場合を除く)。

*BASIC のインストール・タイプを実行するときは、接続されている xSeries サーバー CD-ROM ドライブに ServerGuide CD を装着します。

- 2. 以下の方法のいずれかを使用して、インストールを開始します。

- Windows サーバー・インストール・アドバイザーで生成した Windows サーバー導入 (INSWNTSVR) コマンドを使用できる場合は、次のようにします。
 - a. i5/OS コマンド行で QCMD を呼び出してコマンド入力プロンプトを開始し、「F11=全表示 (F11=Display Full)」を選択します。
 - b. Windows サーバー・インストール・アドバイザーで生成された INSWNTSVR コマンドを i5/OS コマンド行に貼り付けて、Enter キーを押してコマンドを実行します。
 - c. インストールが開始して、その過程は最大 1 時間かかります。追加の情報入力を要求するプロンプトが出されることがあります。その後、104 ページの『統合 Windows サーバー・コンソールからのインストールの続行』に移動してください。
- あるいは、i5/OS コマンド行から、INSWNTSVR と入力してから F4 キーを押してコマンドを実行し、インストールを行うこともできます。73 ページの『i5/OS パラメーターのインストール・ワークシート』の値を以下の各フィールドに入力します。

- | 3. 「ネットワーク・サーバー記述」フィールド (詳しくは 73 ページの『ネットワーク・サーバー記述』を参照) に、73 ページの『i5/OS パラメーターのインストール・ワークシート』のサーバー名を入力して、Enter キーを押します。
- | 4. 73 ページの『i5/OS パラメーターのインストール・ワークシート』で記入した値 (*FULL または *BASIC) を「インストール・タイプ (Install type)」フィールドに入力します。
- | 5. 「リソース名」フィールドに、73 ページの『i5/OS パラメーターのインストール・ワークシート』で記入した情報を入力します。
- | 6. インストールする Windows サーバーのバージョンを選択し、Enter キーを押します。

注: iSCSI 接続サーバーには Windows Server 2003 が 必要です。

7. 実際の CD ではなく格納イメージからサーバーをインストールする場合には、「Windows ソース・ディレクトリー」フィールドにイメージへのパスを指定します。
8. 「導入オプション」フィールドで、デフォルトの *INSTALL を使用します。
9. インストール・プログラムが TCP/IP プロパティを、新規の統合サーバーによって制御される、iSeries にインストール済みのネットワーク・アダプター向けに構成するようにするには、Windows TCP/IP 構成値を 73 ページの『i5/OS パラメーターのインストール・ワークシート』から指定します。それ以外の場合は、このステップをスキップして、デフォルト値 *NONE を使用します。
10. オプションの仮想イーサネット・ポートをインストールおよび構成するには、仮想イーサネット・ポート・フィールドの Windows TCP/IP 構成値を 73 ページの『i5/OS パラメーターのインストール・ワークシート』から指定します。
11. 73 ページの『i5/OS パラメーターのインストール・ワークシート』の値を以下のようなフィールドに入力します。
 - TCP/IP ローカル・ドメイン名
 - TCP/IP ネーム・サーバー・システム
 - サーバー・メッセージ待ち行列
 - ライブラリー
12. サーバーからのどのイベント・ログ・メッセージを i5/OS で受け取りたいかを「イベント・ログ」フィールドに指定します。
13. 「サーバー記憶域スペース」のフィールドに、73 ページの『i5/OS パラメーターのインストール・ワークシート』の値を入力します。
 - 「ソース導入サイズ」および「システム・サイズ」フィールドの値を指定するか、デフォルトの *CALC を選択すると、システムは最小サイズを計算することができます。
 - インストール・ソースおよびシステム・ドライブに別の補助記憶域プール (ASP) を選択する場合、「記憶スペース ASP」または「サーバー記憶域 ASP 装置」フィールドのいずれかと対応する要素に指定します。
 - システムが 32 GB 以下の場合には「NTFS への変換」フィールドで *NO を指定すれば、統合サーバーのシステム・ドライブがファイル割り振りテーブル (FAT32) ファイル・システムでフォーマットされることになります。そうでない場合には、デフォルトの *YES を使用して、インストール時にシステム・ドライブを New Technology File System (NTFS) に変換します。この決定に役立つ情報については、96 ページの『FAT、FAT32、および NTFS ファイル・システムの比較』を参照してください。必要であれば、INSWNTSVR コマンドは、32 GB 以上のシステム・ドライブを自動的に NTFS に変換します。
14. オプション: 「ワークグループ用」または「ドメイン用」パラメーターに対応する Windows ワークグループまたはドメインを指定します。
15. オプション: 「フルネーム」フィールドに、インストール中の Windows サーバー・ライセンスを所有しているユーザーの名前を指定します。
16. オプション: 「編成」フィールドに、インストール中の Windows サーバー・ライセンスを所有している組織の名前を指定します。
17. IBM i5/OS 統合サーバー・サポートがユーザーの 1 次言語を使用するようにするには、「言語バージョン」フィールドに *PRIMARY を指定します。登録不可能な事前定義名の問題が起きないようにするため、統合ライセンス・プログラムと Windows サーバーとが同じ言語を使用することを確認してください。どの言語がコマンドをサポートしているかを知る必要がある場合は、97 ページの『サポートされている言語バージョン』を参照してください。

18. i5/OS が 30 分ごとに統合サーバーと日付と時刻の同期をとるようになるには、「日付と時刻の同期化」フィールドに *YES を指定します。それをオンに変更したときだけ i5/OS が統合サーバーと日付と時刻の同期を取るようになるには、*NO を入力します。
19. 「ドメイン・ユーザーの伝搬」フィールドで、Windows ドメインまたは Active Directory に対してユーザーを伝搬および同期するのにこのサーバーを使用する必要があるかどうかを指定します。
20. 「Windows ライセンス・キー」フィールドに、Microsoft 提供の CD キー (ダッシュも含めて) を指定します。ほとんどの場合、この CD キーは Windows インストール CD ケースの裏面に印刷してあります。
21. 「ライセンス・タイプ」フィールドに、購入した Windows サーバー・ライセンスのタイプを指定します。
22. 「ライセンス・タイプ」フィールドに *PERSERVER を指定した場合、次に「クライアント・ライセンス」フィールドに、購入したクライアント・ライセンスの数を指定します。
23. 「Terminal services」オプションを入力して、「Terminal services」フィールドにインストールします。
24. 「制限された装置リソース」フィールドに、73 ページの『i5/OS パラメーターのインストール・ワークシート』から値を入力します。
25. 「シャットダウン・タイムアウト (Shutdown timeout)」フィールドで、統合サーバーのシャットダウン・タイムアウト値を分単位で入力します。この値は、サーバーをオフに変更する前に、統合サーバーのオペレーティング・システムがシャットダウンするために与えられる時間を制限するために使用されます。
26. IXA 接続サーバーまたは IXS サーバーをインストールしている場合、ステップ34 (104 ページ)を継続し、追加パラメーターを記入します。iSCSI 接続サーバーをインストールしている場合、以下のフィールドの 73 ページの『i5/OS パラメーターのインストール・ワークシート』から iSCSI パラメーターの値を入力します。
 - 活動化タイマー
 - 通信メッセージ待ち行列
27. 「記憶域パス」フィールドで、ネットワーク・サーバー・ホスト・アダプター名を指定して、iSCSI 記憶域の通信に使用します。詳しくは、45 ページの『ネットワーク・サーバー・ホスト・アダプター』を参照してください。
28. 「仮想イーサネット・パス」フィールドで、1 つ以上のネットワーク・サーバー・ホスト・アダプターを入力し、iSCSI LAN の通信に使用します。
 - 「仮想イーサネット・ポート」フィールドに *VRTETHPTP ポートおよび上で指定した別のポートで少なくとも 1 つの値を指定します。
29. オプション: 「シャットダウン TCP ポート」および「仮想イーサネット制御ポート」を指定します。
30. 以下のフィールドに既存のネットワーク・サーバー構成名を入力するか、デフォルト値を選択します。
 - リモート・システム NWSCFG
 - サービス・プロセッサ NWSCFG
 - 接続機密保護 NWSCFGEnter キーを押します。
31. IP 機密保護 (IPSec) 規則を入力して、以下を使用します。
 - 既存の接続機密保護 NWSCFG の場合は、次のようにします。
 - a. 構成済みの機密保護規則を指定して、「IP 機密保護規則」フィールドを使用します。
 - b. Enter キーを押します。

- | • デフォルトの接続機密保護 NWSCFG の場合は、次のようにします。
- | a. デフォルトの IP 機密保護 (IPSec) 規則を指定して、「省略時の IP 機密保護規則」フィールド
- | で使用します。
- | b. Enter キーを押します。
- | 32. プロンプトが出されたら、デフォルトの「サービス・プロセッサ NWSCFG 名 (Service processor
- | NWSCFG name)を使用している場合、このフィールドに 73 ページの『i5/OS パラメーターのインストール
- | ル・ワークシート』からサービス・プロセッサ構成情報を入力します。
- | • 「サービス・プロセッサの初期化」フィールドで、次のようにします。
- | – a. サービス・プロセッサの初期化が *NONE 以外の値である場合、「SP 証明書 ID」フィール
- | ドでコンポーネント比較値を入力します。
- | • 「ユニキャストを使用可能にする」フィールドで、使用するユニキャスト・オプションを選択しま
- | す。
- | a. ユニキャストを使用しない場合、「格納装置 ID」フィールドに値を入力し、製造番号と、オブ
- | ションの製造元のタイプおよび形式の値を指定します。
- | b. ユニキャストを使用する場合、「サービス・プロセッサ名」フィールドの値を指定するか、
- | 「SP IP アドレス」フィールドに IP アドレスを入力します。
- | • デフォルトのリモート・システム NWSCFG 名を使用する場合、およびサービス・プロセッサを
- | 初期化すると *NONE 以外の値になる場合、ユーザー名およびユーザー・パスワードの SP 認証値
- | を指定します。
- | 33. プロンプトが出されたら、デフォルトの「リモート・システム NWSCFG 名 (Remote system NWSCFG
- | name)」を使用している場合、このフィールドに 73 ページの『i5/OS パラメーターのインストール・
- | ワークシート』からリモート・システム構成情報を入力します。
- | • 「リモート・システム ID」フィールドで、以下のいずれかを指定します。
- | a. サービス・プロセッサ NWSCFG の「格納装置 ID」フィールドで識別された製造番号を使用
- | します。
- | b. 「リモート・システム ID」フィールドの製造番号とオプションの製造元のタイプおよび形式の
- | 値を指定します。
- | • 「配送方式」フィールドで、リモート・システムの構成に使用される方式を入力します。
- | • 「CHAP 認証」フィールドで、リモート・システムの認証に使用される Challenge Handshake
- | Authentication Protocol (CHAP) 値を入力します。
- | • 「ブート装置 ID」フィールドで、リモート・システムのブートに使用される iSCSI アダプターを識
- | 別します。リモート・システムに iSCSI ブート装置が 1 つしかない場合、デフォルト値 *SINGLE
- | を使用します。
- | • *DYNAMIC 配送方式を使用する場合、「動的ブート・オプション」フィールドで追加のオプション
- | を任意で指定します。
- | • 「リモート・インターフェース」フィールドで、リモート・システムで使用するインターフェース
- | の値を入力します。
- | a. 「SCSI インターフェース」フィールドで、以下のものを含む SCSI 機能の値を入力します。
- | 1) SCSI アダプター・アドレス
- | 2) SCSI IP アドレス
- | 3) SCSI サブネット・マスク
- | 4) オプション: SCSI ゲートウェイ・アドレスの入力

- 5) iSCSI 修飾名、または *GEN を入力してシステムが自動的にアドレスを生成するように許可。
- b. 「LAN インターフェース」フィールドで、以下のものを含む LAN 機能の値を入力します。
 - 1) LAN (TOE) アダプター・アドレス
 - 2) LAN IP アドレス
 - 3) LAN サブネット・マスク
 - 4) オプション: LAN ゲートウェイ・アドレスの入力

34. 追加のパラメーターを使用すると、以下を行うことができます。

- 統合サーバーにデフォルト以外のキーボード・タイプをインストールする。(有効なキーボード・スタイル ID は、Windows サーバー・インストール・ソースの I386 ディレクトリーにある TXTSETUP.SIF ファイルにリストされています。)
- Point-to-Point 仮想イーサネット用の自分独自の IP アドレスを使用する。
- NWSD 構成ファイルを使用する。 275 ページの『第 15 章 ネットワーク・サーバー記述構成ファイル』を参照してください。
- 新規または既存の Windows クラスタ構成の構成。

特に必要と思われる他の情報ごとに、入力して Enter キーを押してください。

統合 Windows サーバーはインストールを開始します。インストール処理の 2 番目の段階は、『統合 Windows サーバー・コンソールからのインストールの続行』です。このプロセスは、ハードウェア構成によって異なりますが、約 1 時間かかります。

統合 Windows サーバー・コンソールからのインストールの続行

i5/OS 側のインストールが完了すると、統合サーバーが始動されます。ここで、Windows サーバー側のインストールを開始します。64 ページの『統合 Windows サーバーのインストールの準備』のステップを完了してインストール属性を Windows サーバー導入 (INSWNTSVR) コマンドに指定した場合、インストールのこの段階は簡単になります。

Windows サーバーのインストールを完了するには、ServerGuide を実行していないときに、次のタスクを実行します。

1. 「ライセンス契約」ステップ (「Windows Server セットアップ」ウィンドウ) で、「同意します」ラジオ・ボタンをクリックします。それから「次へ」をクリックします。
2. エラー・メッセージを受け取る場合、「OK」をクリックして、インストール・プログラムに従って、状態を訂正するかまたは必要な情報を提供してください。それらのエラー・メッセージの例や、その応答方法については、117 ページの『インストール中のエラー・メッセージへの応答』を参照してください。
3. 「コンピュータ名と Administrator のパスワード」ウィンドウで、パスワードを入力して確認します。
4. 「日付と時刻の設定」パネルで以下のようにします。
 - a. i5/OS の時間帯が正確で、『Windows サーバー・インストール・アドバイザー』に示す時間帯システム値と一致することを確認します。67 ページの『時刻合わせ』を参照してください。
 - b. 夏時間を採用している地域の場合は、「自動的に夏時間の調整をする」ボックスをチェックしたままにします。

夏時間を採用していない地域の場合は、「自動的に夏時間の調整をする」チェック・ボックスのチェックをはずしてください。

5. 「Windows セットアップ・ウィザードの完了」画面で、「完了」をクリックします。
6. 「Windows セットアップ」ウィンドウで、「すぐに再起動する」ボタンをクリックします。クリックしなくても、15 秒後に自動的にサーバーが再起動します。

注: ドメイン・コントローラー Windows サーバーをインストールする場合、DCPROMO コマンドを実行して、この時点で Active Directory をインストールしてください。Active Directory のインストールについての詳細は、Microsoft 社の資料を参照してください。

Windows サーバーのインストールを完了するには、ServerGuide を実行しているときに、次のタスクを実行します。


- HSL 接続のサーバーのローカル光ディスク・ドライブに ServerGuide CD を挿入します。(IXA の接続した xSeries サーバー。)
- メッセージ NTA100C 「Insert ServerGuide CD-ROM into &2 optical device (C G)」に G と応答します。
- ServerGuide ウィザードの指示に従ってインストール・プロセスをたどります。

『サーバーのインストールの完了』を参照してください。

サーバーのインストールの完了

Windows 2000 Server または Windows Server 2003 を i5/OS にインストールした後でいくつかの最終的な作業を実行して、それが正しくインストールされていて使用できることを確認します。

1. サポートされる最新の Microsoft Service Pack をインストールすることをお勧めします。IBM 統合

xSeries ソリューション Web サイト (英語)  の『Service Information』に載せられている、サポートされる最新の Service Pack のリストについて、Microsoft サービス・パックのページを参照し、Windows Update を実行してください。

2. TCP/IP の開始時に統合 Windows サーバーが自動的にオンに変更されるようにしたい場合は、118 ページの『TCP/IP に応じた統合 Windows サーバーのオンへの自動変更の設定』を参照してください。
3. QRETSVRSEC システム値で iSCSI 接続サーバーのインストールがまだ使用可能になっていない場合、i5/OS 上の QRETSVRSEC システム値を変更して、パスワードが確実に i5/OS に保存します (こうすれば、ユーザーのサインオンに時間がかからないようにすることができます)。

- i5/OS コマンド行で以下のコマンドを入力します。

```
WRKSYSVAL SYSVAL(QRETSVRSEC)
```

- 値を変更するには、「Option」フィールドに 2 と入力して、Enter キーを押します。

- 「サーバー機密保護データの保存」の値を 1 に変更します。

4. サーバーが NWSD 名とは別の名前を持つようにしたい場合 (例えば、8 文字以上の名前) は、Windows コンソールでコンピューター名を変更することができます。詳しくは、Windows の資料を参照してください。
5. アプリケーションとデータをシステム・ドライブに保管しないで、これらの項目用に追加のディスク・ドライブを作成することができます。詳しくは、181 ページの『統合 Windows サーバーへのディスク・ドライブの追加』を参照してください。
6. サーバーに追加の仮想イーサネット LAN を定義できるので、同一の区画または別の区画にある他のサーバーに接続することができます。詳しくは、123 ページの『第 6 章 仮想イーサネットおよび外部ネットワークの管理』を参照してください。
7. Windows サーバーまたはドメインに i5/OS ユーザーを登録することもできます。詳しくは、197 ページの『第 11 章 i5/OS からの統合 Windows サーバー・ユーザーの管理』を参照してください。

8. ユーザー記憶域スペースをサーバーにリンクした時に、光ディスク・ドライブのドライブ名が変更されないようにすることができます。「ディスク管理」を使って統合サーバーの光ディスク・ドライブ名を割り当てます。(たとえば、ドライブ X に割り当てることができます。)
9. 独自の NWSD 構成ファイルを作成すれば、サーバーをカスタマイズすることができます。275 ページの『第 15 章 ネットワーク・サーバー記述構成ファイル』を参照してください。
10. Windows をクラスター化したい場合は、109 ページの『Windows クラスタ・サービス』を参照してください。
11. サーバーが Windows Server 2003 と共にインストールされていて、Active Directory がインストール済みの場合 (ドメイン・コントローラーの場合など)、116 ページの『Windows Server 2003 Active Directory Server を使用して Kerberos を使用可能にする』を参照してください。
12. 2892-002 または 4812-001 IXS ハードウェア・タイプを Microsoft Windows 2000 Server と共に使用する場合、特殊なビデオ・デバイス・ドライバーをインストールして、2892-002 および 4812-001 IXS 上の ATI Radeon ビデオ・チップを利用してください。116 ページの『2892-002 または 4812-001 統合 xSeries サーバーに ATI Radeon 7000M の Windows 2000 用ビデオ・デバイス・ドライバーをインストールする』を参照してください。
13. Microsoft Windows Server 2003 で 2892-002 または 4812-001 IXS ハードウェア・タイプを使用している場合、ハードウェアの加速設定を調整して、最良のパフォーマンスを発揮できるようにします。117 ページの『2892-002 または 4812-001 統合 xSeries サーバー上の Windows Server 2003 のハードウェアの加速を調整する』を参照してください。

重要: ファイアウォールを統合サーバーと共に使用することを計画している場合は、Point-to-Point 仮想イーサネット用の IP アドレスが、ファイアウォールとして稼働している SOCKS サーバーを経由しないようにしてください。経由すると、接続障害の原因となります。ファイアウォールの設定についての詳細は、『ファイアウォールご使用に際して』を参照してください。

- | iSCSI 接続サーバーの場合、以下のステップを実行することもできます。
- | 1. サーバーを構成して、追加の iSCSI HBA を使用し、パフォーマンスまたは可用性を向上させることができます。詳しくは、147 ページの『iSCSI HBA 使用法の管理』を参照してください。
- | 2. iSCSI ネットワークが大規模フレーム・サイズをサポートしている場合、ご使用の仮想イーサネットのパフォーマンスを向上させることができるかもしれません。詳しくは、151 ページの『最大伝送単位 (MTU) の考慮事項』を参照してください。

IBM iSeries Integration for Windows Server ライセンス・プログラムのアップグレード

i5/OS and IBM iSeries Integration for Windows Server を V5R4 にアップグレードする場合、5722-SS1 を収めた CD が必要です。新しい統合 xSeries サーバー・ハードウェアのインストールも計画している場合、最初にこのソフトウェア・インストールを完了するようにします。「iSeries ソフトウェアの導入




」のアップグレード手順に従って、以下の追加ステップを行ってください。

アップグレードを準備します:

1. i5/OSに対してだけでなく、既存の統合 Windows サーバーすべてに対して、最新のコード修正をインストールしたことを確認します。119 ページの『コード修正』を参照してください。
2. 使用可能なシステム・バックアップがあり、それぞれの統合サーバーに割り当てられた記憶域も用意されていることを確認します。
3. 念のため、各ハードウェアの関連リソースについて記録しておきます。

- a. i5/OS コマンド行で WRKCFGSTS *NWS と入力し、Enter キーを押します。
 - b. ネットワーク・サーバー記述の横のオプション列に 8 と入力します。「ネットワーク・サーバー記述の処理」画面が表示されます。
 - c. ネットワーク・サーバー記述の横のオプション列に 5 と入力します。
 - d. 「リソース名」フィールドが表示されるまでページ送りをして、このネットワーク・サーバーの値 (たとえば、LIN05) を記録します。
 - e. F12 を 2 度押して、このコマンドを終了します。
 - f. i5/OS コマンド行で WRKHDWRSC TYPE(*CMN) と入力し、Enter キーを押します。
 - g. ステップ 3 d で識別したリソース名の横のオプション列に、7 (リソース詳細の表示) と入力します。入力列には統合 xSeries サーバー・ハードウェアの CCIN 番号が示されており、テキスト記述は「ファイル・サーバー I0P」か「ファイル・サーバー I0A」です。
 - h. iSeries に同一タイプの統合 xSeries サーバーを複数インストールしてある場合、以下のカード位置によって該当するカードを識別できます。
 - 1) 「設置場所」の見出しの下の「カード位置」を調べます。
 - 2) iSeries のスロットのラベルを調べます。1 つのスロットのラベルは、「カード位置」フィールドと同じ数字、または同じ文字と数字の組み合わせになっているはずですが、このスロットには、リソース名が表す統合 xSeries サーバーが入っています。
 - i. 「タイプ/型式」および「製造番号」フィールドの情報を記録します。
 - j. F12 を 2 度押して、コマンドを終了します。
4. すべての統合サーバーをオフに変更します。163 ページの『統合サーバーの開始と停止』を参照してください。

新しいバージョンの i5/OS を iSeries にインストールするには、「iSeries ソフトウェアの導入 」の手順に戻ってください。

i5/OS をアップグレードしたら、以下のステップを完成させます。

1. 統合サーバーを始動して (163 ページの『統合サーバーの開始と停止』を参照)、同じリソース名であることを確認します。
 - a. i5/OS コマンド行で WRKHDWRSC TYPE(*CMN) と入力し、Enter キーを押します。
 - b. ステップ 3d で識別したリソース名の横のオプション列に、7 (リソース詳細の表示) と入力します。「タイプ/型式」および「製造番号」フィールドの情報が、このリソースについて記録した内容と一致することを確認します。
 - c. これらのフィールドと記録した内容が一致しない場合、以下のようになります。
 - 1) F12 を押して、前の画面を終了します。
 - 2) 「タイプ/型式」および「製造番号」の値が、記録した値と一致することを確認できるまで、オプション 7 を使用して、リスト中の他のリソース名のリソース詳細を表示します。i5/OS がこの統合 xSeries サーバー・ハードウェアに関連付けたリソース名を記録します。F12 を押して、このコマンドを終了します。
 - 3) i5/OS コマンド行で WRKNWSD と入力し、Enter キーを押します。「ネットワーク・サーバー記述の処理」画面が表示されます。
 - 4) ネットワーク・サーバー記述の横のオプション列に 2 (変更) と入力し、Enter キーを押します。「ネットワーク・サーバー記述の変更」画面が表示されます。
 - 5) このネットワーク・サーバーのリソース名を、新しい適切なリソース名に変更します。

2. IBM i5/OS 統合サーバー・サポートを既存の統合サーバーにインストールします。 69 ページの『IBM i5/OS 統合サーバー・サポートのインストール』を参照してください。

IBM i5/OS 統合サーバー・サポートの統合サーバー側のアップグレード

IBM i5/OS 統合サーバー・サポートは、iSeries と統合 Windows サーバーとを組み合わせるソフトウェアです。これは翻訳プログラムであると考えてください。プログラムの半分は iSeries 上で実行して、Windows 言語を i5/OS 言語に翻訳し、他の半分は統合サーバー上で実行して i5/OS 言語を Windows 言語に翻訳します。

IBM i5/OS 統合サーバー・サポートの新規バージョンが i5/OS にインストールされます。その後、ライセンス・プログラムの統合サーバーの部分を統合サーバーにコピーしてインストールする必要があります。

以下のものをインストールする場合、既存の統合 Windows サーバーのライセンス・プログラムをアップグレードしなければなりません。

- IBM i5/OS 統合サーバー・サポートの新規バージョン。
- Microsoftによる、Windows サーバーの新規バージョン。

IBM i5/OS 統合サーバー・サポートの新規バージョン

IBM i5/OS 統合サーバー・サポートの新しいバージョンをインストールする場合、既存の統合サーバーすべてをそのレベルまでアップグレードする必要があります。複数の統合サーバーがある場合、それらのサーバーを i5/OS からリモートでアップグレードすることができます。

この手順では、統合 Windows サーバーと i5/OS とで同じユーザー ID とパスワードがなければなりません。

統合サーバーを更新するには、以下のステップを実行してください。

1. 実行しているアプリケーションをすべて終了します。
2. 統合サーバーにログオンしているユーザーがないことを確認します。

重要: 統合サーバーは、インストール完了後、自動的に再始動します。したがって、ステップ 1 と 2 を省略すると、データを失う危険があります。

3. 「スタート」メニューから、「プログラム」、「IBM iSeries」、「Integration for Windows Server」、「ソフトウェア・レベル (Software level)」の順に選択します。

注: 新しいレベルのライセンス・プログラムがインストールに使用可能な場合、統合サーバーに管理者としてログオンするとソフトウェア・レベルは自動的に開始します。

4. V5R3 以降からアップグレードする場合、オプション「同期 (Synchronize)」を選択します。それ以外の場合、オプション「iSeries からのリリースのインストール (Install release from iSeries)」を選択します。
5. ユーザー・インターフェースの指示に従って、インストールを完了します。
6. **ヒント:** 後で、このサーバーの事前定義されたインストールおよびシステム・ドライブのバックアップを実行してください。それらのドライブのバックアップについては、211 ページの『統合 Windows サーバー用事前定義ディスク・ドライブのバックアップ』を参照してください。サーバーのすべての記憶域を同時にバックアップの方が安全なので、関係するユーザー作成記憶域スペースもバックアップするようにします (212 ページの『統合 Windows サーバー用ユーザー定義ディスク・ドライブのバックアップ』を参照)。

Windows Server の新バージョン

サーバーを Windows NT 4.0 から Windows 2000 にアップグレードするには、V5R3 iSeries Information Center の「Windows NT 4.0 から Windows 2000 サーバーへのサーバーのアップグレード」を参照してください。

285x または 661x から 2890 統合 xSeries サーバー・ハードウェアへの移行

IPCS または INS サーバー (タイプ 2850 および 6617) はより新しいハードウェア上にインストールするか、V5R4 のインストール前に 2890 ハードウェアに移行する必要があります。V5R3 iSeries Information Center の「2890 統合 xSeries サーバー・ハードウェアへの移行」トピックを参照してください。

I iSCSI 接続サーバーへの移行

- I iSCSI 接続サーバーへの移行はサポートされていません。すべての iSCSI 接続サーバーには新規でインストールしなければなりません。

Windows クラスタ・サービス

Windows クラスタ・サービスは、個々のサーバーをリンクして共通のタスクを実行可能にします。いずれかのサーバーの機能が停止した場合、そのワークロードをフェイルオーバーと呼ばれるプロセスが他のサーバーに自動的にシフトするので、サービスは継続します。フェイルオーバーに加えて、一部の形式のクラスタリングではロード・バランシングも採用しています。これにより、コンピューターのワークロードは相互にリンクされたコンピューターのネットワークに分散されます。

Windows 2000 Advanced Server は、2 つのノードのクラスタをサポートし、Windows Server 2003 Enterprise Edition は 8 つのノードのクラスタをサポートします。Windows の Datacenter 版はサポートされていません。

Windows クラスタ・サービス・サポートは、Windows 2000 Advanced Server または Windows Server 2003 Enterprise Edition を実行する統合 Windows サーバーのいずれかでサポートされます。

注:

1. Windows クラスタ化ネットワーク・サーバー・ノードをクラスタ化するには、それが単一の iSeries 区画内になければなりません。
- I 2. iSCSI 接続 xSeries を IXS/IXA 接続サーバーとクラスタ化することはできません。

従来の Windows クラスタ化サーバーのソリューションでは共用物理 SCSI またはファイバー・チャネル装置が必要でしたが、統合 Windows サーバー・ソリューションでは仮想ファイバー・チャネル・バスを使用して、クラスタのノード間で仮想ディスク装置を共有します。

また、仮想イーサネットの新しいサポートにより、ハイパフォーマンスかつ安全な、クラスタ化ノードの間の内部ノード間通信が可能になりました。

サーバー・クラスタに関する Microsoft のオンライン・ヘルプから、サーバー・クラスタの計画および作成用の詳細チェックリストを入手できます。これは、Windows クラスタ・サーバーのインストールおよび構成を行う前に参照してください。クラスタ・サービスのインストールの段階的な手引きなどの追加

情報は、「Microsoft Web サイト 」から入手可能です。

Windows クラスタ・サービスのサポートについて詳しくは、以下のトピックを参照してください。

『Windows クラスタ・サービスのインストール』


統合 Windows サーバー上で Windows クラスタ・サービスをインストールおよび構成する方法が記されています。

111 ページの『既存のサーバーへの Windows クラスタ・サービスのインストール』

既存の統合 Windows サーバーでクラスタを作成する方法が記されています。

l iSCSI 接続サーバーにおけるクラスタ・サポート

l iSCSI 接続サーバーでの Microsoft クラスタ・サービス (MSCS) 用の iSeries サポートについては、統合

l xSeries ソリューション Web サイト (英語) の『MSCS on an iSCSI attached server』

l (www.ibm.com/servers/eserver/iseries/integratedxseries/windows/iscsiclusters.html) を参照してください。

Windows クラスタ・サービスのインストール

将来計画やインストールの際に問題が起きないようにするために、クラスタ・サービスをインストールする前に、サーバー・クラスタのインストールに関するすべての Microsoft チェックリストをお読みください。

注: 最初のノードでのクラスタ・サービスをインストールする際、Windows を始動する前に、クラスタに含まれる他のすべてのノードをオフに変更してください。

サーバー・クラスタ情報における共用 SCSI またはファイバー・チャネル装置の言及はすべて、共用ネットワーク・サーバー記憶域スペースへのアクセスで使用される仮想ファイバー・チャネルの実装を指します。

Windows クラスタ・サービスをインストールし、実行するには、以下のタスクを完了してください。

1. 統合 xSeries サーバー上に Windows クラスタ・サービスをインストールする。
 - 『新しい統合 Windows サーバーへの Windows クラスタ・サービスのインストール』
 - 111 ページの『既存のサーバーへの Windows クラスタ・サービスのインストール』
2. 113 ページの『Windows への Windows クラスタ・サービスのインストール』

新しい統合 Windows サーバーへの Windows クラスタ・サービスのインストール

Windows クラスタ・サーバーのインストールと構成は、最初の統合サーバーの構成時が最も簡単です。Windows サーバー導入 (INSWNTSVR) コマンドを、クラスタ構成情報を指定する以下のパラメーターとともに使用します。

- 「クラスタ名 (CLU)」パラメーター
- 「クラスタ構成 (CLUCFG)」パラメーター

統合サーバーのインストール方法について詳しくは、98 ページの『Windows 2000 Server または Windows Server 2003 のインストール』を参照してください。

INSWNTSVR コマンドを実行し、(Windows インストールが完了した後、) Windows クラスタ・サービスを Windows 側にインストールする前に、統合サーバーのコンソールで追加の構成ステップを実行しなければなりません。詳しくは、112 ページの『Windows クラスタ・サービスをインストールする前の Windows システムの準備』を参照してください。

クラスタ名:

「クラスター名 (CLU)」パラメーターは、クラスターを判別するための名前を提供します。管理者はこの名前を使用してクラスターに接続し、単一システムとして協働する独立ネットワーク・サーバー・ノードのグループを表します。クラスター名に入力された名前は、ネットワーク・サーバー記憶域スペース (クラスターのクォーラム・リソースとして作成され、機能する) の名前としても使用されます。

クラスターの構成:

「クラスター構成パラメーター (CLUCFG)」は、クラスターを定義し、クォーラム・リソースのネットワーク・サーバー記憶域スペースを構成するために使用されます。また、この情報は、プライベート・クラスター化内部接続で使用される、共用記憶域装置および仮想イーサネット・ポートの仮想クラスター接続を作成するのに必要な、適切な i5/OS 構成がどの 2 次ノードにもあるかを確認するためにも使用されます。
*CLU のクラスター構成値は、CLU パラメーターで指定された既存のクォーラム・リソースのネットワーク・サーバー記憶域スペースからクラスター構成を取得します。

注: 接続ポートをクラスター化するには、一致した仮想イーサネット・ポートの構成が必要です。仮想イーサネット・ポートの構成の詳細については、123 ページの『仮想イーサネット・ネットワークの構成』を参照してください。

既存のサーバーへの Windows クラスター・サービスのインストール

Windows クラスター・サービスは、既存の Windows 2000 Advanced Server または Windows Server 2003 Enterprise Edition サーバー上にインストールできます。

サーバーの統合サーバー・サポート・レベルが i5/OS と同期していることを確認します。108 ページの『IBM i5/OS 統合サーバー・サポートの統合サーバー側のアップグレード』を参照してください。それによって、Windows クラスター・サービスのインストールに必要なすべてのサービス機能を確実に使用できるようになります。

既存のサーバーに Windows クラスター・サービスをインストールするには、以下のタスクを行います。

- 記憶域スペース (クォーラム・リソース) の作成
- 仮想イーサネット接続ポートの構成
- ネットワーク・サーバー記述へのクォーラム・リソース・ドライブのリンク

上記のステップを完了しても、統合 Windows サーバー側に Windows クラスター・サービスをインストールする前にさらにいくつかの別の構成ステップを統合 Windows サーバーのコンソールで実行する必要があります。詳しくは、112 ページの『Windows クラスター・サービスをインストールする前の Windows システムの準備』を参照してください。

記憶域スペース (クォーラム・リソース) の作成

最初のステップでは、クォーラム・リソースとして使用する記憶域スペースを作成します。記憶域スペースを作成するには、「NWS 記憶域の作成 (Create NWS Storage space)」(CRTNWSSTG) と CL コマンドを使用して、特殊フォーマット *NTFSQR を指定します。

ネットワーク・サーバーの記憶域スペースの名前は、作成しようとしているクラスターの名前に一致していなければなりません。推奨サイズは 550 MB 以上です。以下のようなクラスター情報を尋ねられるので、入力しなければなりません。

- クラスターのドメイン名
- 仮想イーサネット接続ポート
- Windows クラスターの IP アドレス

- Windows クラスターのサブネット・マスク

仮想イーサネット接続ポートの構成

次のステップでは、プライベート・クラスター通信で使用する予定の仮想イーサネット接続ポートを構成します。123 ページの『仮想イーサネット・ネットワークの構成』を参照してください。使用する仮想イーサネット・ポートは、クォーラム・リソース・ネットワーク・サーバーの記憶域スペースで指定する接続ポートに一致していなければなりません。

ネットワーク・サーバー記述へのクォーラム・リソース・ドライブのリンク

クォーラム・リソースの記憶域スペースをネットワーク・サーバーにリンクします。それには、ACCESS(*SHRUPD)、DYNAMIC(*YES)、および DRVSEQNBR(*QR) を指定した「サーバー記憶域リンクの追加 (Add Server Storage Link)」(ADDNWSSTGL) コマンドを使用します。

注: 最初のノードにクラスター・サービスをインストールするときは、統合サーバーを始動する前に、他のノードをすべてオフに変更しておく必要があります。さらに別の共用記憶域装置をこの時点で作成してリンクすることができます。すべての共用記憶域は、*NTFS でなければならず、ACCESS(*SHRUPD) を指定してリンクしなければなりません。

Windows クラスター・サービスをインストールする前の Windows システムの準備

統合サーバーのインストールが完了したら、Windows クラスター・サービスをインストールするためのサーバーの準備を行う必要があります。

Windows クラスター・サービスのインストールの前に Windows を準備するには、次のようなタスクを実行します。

1. クォーラム・リソースのフォーマット
2. プライベート・ネットワーク・アダプターの構成

このステップを完了すれば、Windows クラスター・サービスをインストールするための Windows の準備は整います。詳しくは、113 ページの『Windows への Windows クラスター・サービスのインストール』を参照してください。

クォーラム・リソースのフォーマット

Windows クラスターのインストールのための Windows の準備の最初のステップでは、NTFS としてクォーラム・リソースをフォーマットします。クォーラム・リソースのフォーマットは、Windows クラスター・サービスのインストールのために必要であるだけでなく、クラスターの最初のノードをインストールするときの最初のステップでもあります。詳しくは、183 ページの『統合サーバー・ディスク・ドライブのフォーマット』を参照してください。

- | IXS または IXA 接続サーバーの場合、クォーラム・リソースは、通常は論理装置ドライブ文字 E が指定された未フォーマットのディスク・ドライブとして表示されます。クォーラム・リソースの位置はバス番号が 1、ターゲット ID が 0、論理装置番号 (LUN) が 0 です。

ボリュームのフォーマットとラベル付けを行う際は、クラスターと同じ名前を使用しなければなりません。その名前は、クォーラム・リソース・ネットワーク・サーバーの記憶域スペース名でもあります。また、他のすべての共用記憶域スペースもこの時点でフォーマットします。さらに、このクォーラム・ドライブと他のすべての共用記憶域ドライブに固定のドライブ名を割り当てることをお勧めします。

注: 共用記憶域バス上の記憶域スペースにドライブ名を割り当てる場合は、クラスターのどのノードでも同じドライブ名にならなければなりません。

プライベート・ネットワーク・アダプターの構成

次に、クラスター内の最初のノード上で次のようなステップを行って、Windows クラスター・サービスで使用するためのプライベート・ネットワーク・アダプターを構成します。

1. 統合 Windows サーバーのコンソールで、「マイ ネットワーク」を右マウス・ボタン・クリックしてから、「プロパティ」を選択します。
2. 「ローカル エリア接続 2」アイコンを右マウス・ボタンでクリックします。

注: どのネットワーク・アダプターがプライベートでどれが共通になるかは、サーバーの構成方法によって決まります。ここに述べている解説では、以下を前提としています。

- 最初のネットワーク・アダプター (Local Area Connection) は、統合 Windows サーバーの下の物理 LAN アダプターを介して公衆ネットワークに接続されます。
- 2 番目のネットワーク・アダプター (Local Area Connection 2) は、プライベート・クラスター・ネットワークとして使用する予定のクラスター構成接続ポートとして構成された仮想イーサネット・アダプターです。
- 3 番目のネットワーク・アダプター (Local Area Connection 3) は、i5/OSへの Point-to-Point 仮想イーサネット接続です。これは、どのクラスターでも使用してはなりません。

サーバーとネットワークの物理および仮想の構成によっては、ネットワーク・アダプターの数と配列は同じでない可能性もあります。

3. 「状況 (Status)」をクリックして、接続状況と接続速度を示す「ローカル・エリア接続 2 の状況 (Local Area Connection 2 Status)」ウィンドウを表示します。
4. 「ローカル・エリア接続 2 の状況 (Local Area Connection 2 Status)」ウィンドウの「プロパティ」をクリックします。
5. 「プロパティ」ダイアログ・ボックスで、「接続での使用 (Connect using)」フィールドに「IBM iSeries 仮想イーサネット x (IBM iSeries Virtual Ethernet x)」が入っていることを確認します。ただし x は、クラスターの構成接続ポート用に指定した *VRTETHx に符合します。
6. 「閉じる」をクリックし、もう一度「閉じる」をクリックします。

分かりやすく言うと、「ローカル・エリア・ネットワーク (Local Area Network)」アイコンの名前を変更する必要があるということです。たとえば、「ローカル エリア接続 2 (Local Area Connection 2)」という名前を、「プライベート・クラスター接続 (Private Cluster Connection)」などの名前に変更することができます。

Windows への Windows クラスター・サービスのインストール

Windows クラスター・サービスの実際のインストールは、iSeries Windows 環境のインストール時にインストールした Windows のバージョンによって異なります。基本的に、Windows クラスター・サービスのインストールの詳細については、Microsoft の資料を参照してください。以下の項では、統合 Windows サーバーへの Windows クラスター・サービスのインストールに必要な個々のステップが取り上げられています。

- 114 ページの『Windows 2000 Server へのクラスター・サービスのインストール』
- 114 ページの『Windows Server 2003 へのクラスター・サービスのインストール』

注: クラスター内のサーバーで Windows を始動する場合は、別のサーバーで Windows クラスター・サービスがインストール済みで稼働していることを確認してください。任意のサーバーで Windows クラスター・サービスを実行する前に、複数のサーバーでオペレーティング・システムを始動すると、クラスター記憶域が破壊されることがあるからです。最初のサーバーの構成が完了したら、残りのサーバーをすべて同時にインストールすることができます。

Windows 2000 Server へのクラスター・サービスのインストール: Windows クラスター・サービスをインストールするには、「クラスタ サービスの構成」ウィザードを使用します。クラスター構成のすべての初期情報をこのウィザードに入力します。

Windows クラスター・サービスをインストールするには、以下のタスクを行います。

1. 「クラスタ サービスの構成」ウィザードの開始
2. このウィザードによるクラスター・サービスの構成

「クラスタ サービスの構成」ウィザードの開始

「クラスタ サービスの構成」ウィザードを開始するには、次のようなステップを行います。

1. Windows の「スタート」メニューで「設定」を選択し、次に「コントロール パネル」をクリックします。
2. 「コントロール パネル」ウィンドウの「アプリケーションの追加と削除」をダブルクリックします。
3. 「アプリケーションの追加と削除」ウィンドウで、「Windows コンポーネントの追加と削除」をクリックします。
4. 「Windows コンポーネント ウィザード」ダイアログ・ボックスで、「クラスタ サービス」を選択してから「次へ」をクリックします。

Windows クラスター・サービスの構成

「クラスタ サービスの構成」ウィザードを開始したら、画面の説明に従って、Windows クラスター・サービスをインストールします。クラスターの作成に必要なクラスター構成のすべての初期情報をこのウィザードに入力します。

クォーラム・リソースに関する画面が表示されたら、フォーマットとラベル付けを終えたドライブを選択します。新規のインストールの場合はそのドライブは通常は E: ドライブですが、ディスク・マネージャーによってドライブは別の文字に固定化されていることもあります。

ネットワーク接続では、次のような特別な配慮が必要です。

注: 「クラスタ サービスの構成」ウィザードに表示されるネットワーク構成情報の順序は変動することがあります。

- IBM iSeries 仮想イーサネット Point-to-Point (通常はローカル エリア接続 3) の「クラスタ使用のためにこのネットワークを有効にする」のチェック・マークを外します。
- 「IBM iSeries 仮想イーサネット x (IBM iSeries Virtual Ethernet x)」用にオプション「内部クラスタ通信のみ」を選択します。なお x は、クラスター構成接続ポート (通常はローカル エリア接続 2) で指定した *VRTETHx に一致します。
- 必要に応じて、残りのネットワーク接続も構成します。

IBM iSeries virtual Ethernet x アダプター (Local Area Connection 2) を内部クラスタ通信の 1 次ネットワークと指定します。

Windows Server 2003 へのクラスター・サービスのインストール: Windows クラスター・サービスを Windows Server 2003 にインストールして既存のクラスターに結合するには、「クラスタ アドミニストレータ」を使用します。クラスター・サービスのインストールと既存のクラスターへの結合のどちらでも、「クラスタ アドミニストレータ」を開く必要があります。Windows 「スタート」メニューから「クラスタ アドミニストレータ」を開きます。それには、「すべてのプログラム」を選択し、次に「管理ツール」を選択してから、「クラスタ アドミニストレータ」を選択します。

以下のステップを行って、Windows クラスタ・サービスをインストールして構成します。

1. 「**クラスタ アドミニストレータ**」を開きます。
2. 表示された「**クラスタへの接続を開く**」ダイアログ・ボックスの「**アクション**」で、「**クラスタの新規作成 (Create new cluster)**」を選択します。
3. 「**OK**」をクリックして「**新規サーバー・クラスタ (New Server Cluster)**」ウィザードを表示します。画面の説明に従って、最初のノードのクラスタ・サービスをインストールします。
4. 「**次へ**」をクリックします。
5. 「**ドメイン**」(デフォルト) および「**クラスタ名**」を入力します。
6. 「**コンピューター名**」(デフォルト) を入力します。
7. クラスタ管理用の「**IP アドレス**」を入力します。
8. 「**クラスタ・サービス・アカウント・ユーザー名**」、「**パスワード**」、および「**ドメイン**」を入力します。
9. 「**クラスタの構成案 (Proposed Cluster Configuration)**」を検証します。

既存のクラスタの結合:


次のようなステップを行って、既存のクラスタを結合します。

1. 「**クラスタ アドミニストレータ**」を開きます。
2. 「**クラスタへの接続を開く**」ダイアログ・ボックスの「**アクション**」で、「**クラスタへのノードの追加 (Add nodes to cluster)**」を選択します。
3. 次に「**クラスタまたはサーバー名**」で、既存のクラスタの名前の入力、リスト中の名前の選択、または「**参照**」のクリックを介した使用可能クラスタの選択のいずれかを行います。
4. 「**OK**」をクリックして「**サーバー・クラスタの追加 (Add Server Cluster)**」ウィザードを表示します。
5. クラスタに追加する 1 つ以上のコンピューター名を選択して「**追加**」をクリックします。
6. クラスタ・サービスのドメイン・アカウント・パスワードを入力します。
7. クラスタ・サービスのインストールが完了した後、作成したばかりのクラスタを「**クラスタ アドミニストレータ**」を使用して、見つけて選択します。
8. 「**クラスタの構成**」、「**ネットワーク インターフェイス**」を拡張表示します。すると、すべての「**ローカル・エリア接続 (Local Area Connections)**」のリストが右のパネルに開きます。
9. 仮想 IBM iSeries virtual Ethernet x のネットワーク名 (Local Area Connection x) を入力します。ただし x は、「**クラスタの構成**」の接続ポートで指定した *VRTETHx に一致します。このネットワークは後で指定する必要があるので、名前を忘れないでください。
10. 仮想 IBM iSeries virtual Ethernet Point-to-Point のネットワーク名 (Local Area Connection x) を特定します。このネットワークは後で指定する必要があるので、名前を忘れないでください。
11. 「**クラスタ アドミニストレータ**」ウィンドウで、「**クラスタの構成**」、「**ネットワーク**」を拡張表示します。
12. 仮想 IBM iSeries virtual Ethernet x のネットワーク名 (Local Area Connection x) を右マウス・ボタンでクリックして、「**プロパティ**」を選択します。
13. 該当するネットワーク用にオプション「**内部クラスタ通信のみ**」を選択します。
14. 仮想 IBM iSeries virtual Ethernet Point-to-Point のネットワーク名 (Local Area Connection x) を右マウス・ボタンでクリックして、「**プロパティ**」を選択します。

15. 該当するネットワークの「クラスタ使用のためにこのネットワークを有効にする」ボックスのチェック・マークを外します。

必要に応じて、残りのネットワーク接続も構成します。

Windows Server 2003 Active Directory Server を使用して Kerberos を使用可能にする

QNTC、SBMNWSCMD、およびファイル・レベル・バックアップは、Kerberos を使用して、Windows Active Domain メンバー・サーバーへ認証することができます。Kerberos を使用するために、Microsoft Active Directory コントローラー・サーバーで Windows Server 2003 のアップデートをインストールする必要があるかもしれません。このアップデートは、Service Pack 1 または Microsoft Hot Fix KB833708 で入手可能です。サービス・パックおよび Hot Fix のインストール情報などの追加情報は、「Microsoft Web サイト 」で入手可能です。

Hot Fix または Service Pack 1 をインストールした後、Windows Server 2003 のレジストリーをアップデートする必要もあります。以下のステップを実行してください。

1. 「スタート」>「ファイル名を指定して実行」をクリックします。
2. 「開く」ボックスで regedit と入力します。
3. 「OK」をクリックします。
4. **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kdc** レジストリー・サブキーを選択します。
5. 「Kdc」を右マウス・ボタン・クリックします。
6. 「新規」を選択します。
7. 「DWORD 値 (DWORD Value)」をクリックします。
8. KdcUseRequestedEtypesForTickets を新規の値として入力します。
9. **KdcUseRequestedEtypesForTickets** を右マウス・ボタン・クリックします。
10. 「変更」を選択します。
11. **KdcUseRequestedEtypesForTickets** レジストリー値を 1 に設定します。
12. 「OK」をクリックします。
13. レジストリー・エディターを終了します。
14. 変更をアクティブにするには、鍵配布センター・サービスを再始動するか、サーバーをリブートします。

2892-002 または 4812-001 統合 xSeries サーバーに ATI Radeon 7000M の Windows 2000 用ビデオ・デバイス・ドライバーをインストールする

2892-002 および 4812-001 統合 xSeries サーバーには、ATI Radeon 7000M ビデオ・チップが含まれます。必要なドライバーは、Microsoft Windows 2000 Server 配布 CD には含まれていません。ATI ビデオ・チップの機能を十分に活用するためには、ATI ビデオ・ディスプレイ・ドライバーを統合 Windows サーバーにインストールする必要があります。

ATI ビデオ・ドライバーをインストールする前に、システムには DirectX 8.1 以降をインストールする必要があります。

Windows 2000 用の ATI ビデオ・ドライバーをインストールするには、次のステップを行います。

1. DirectX バージョン 8.1 以降をインストールします。Windows 2000 には DirectX 7.0 が同梱されていますが、DirectX バージョン 8.1 以降が ATI ビデオ・ドライバーに必要であり、それを ATI ビデオ・ドライバーをインストールするよりも前にインストールしなければなりません。Microsoft は、DirectX の情報とダウンロードのための Web サイトを保守しています。
<http://www.microsoft.com/directx> を参照してください。
2. ATI ビデオ・ドライバーをインストールする方法:
 - a. すべてのプログラムをクローズします。
 - b. 「スタート」ボタンをクリックして、「ファイル名を指定して実行」メニュー項目を選択します。
 - c. 「参照」ボタンをクリックします。
 - d. %SystemDrive%\WSV ディレクトリーまでブラウズします。ここに、atidrvr.exe があります。
 - e. atidrvr.exe を選択して、「OK」をクリックし、プログラムを実行します。
 - f. 画面に表示されるインストールの指示に従ってください。
3. オプションで、「Advanced ATI」コントロール・パネル・タブもインストールできます。
 - a. すべてのプログラムをクローズします。
 - b. 「スタート」ボタンをクリックして、「ファイル名を指定して実行」メニュー項目を選択します。
 - c. 「参照」ボタンをクリックします。
 - d. %SystemDrive%\WSV ディレクトリーまでブラウズします。ここに、aticp.exe があります。
 - e. aticp.exe を選択して、「OK」をクリックし、プログラムを実行します。
 - f. 画面に表示されるインストールの指示に従ってください。

2892-002 または 4812-001 統合 xSeries サーバー上の Windows Server 2003 のハードウェアの加速を調整する

Windows Server 2003 を 2892-002 または 4812-001 IXS でインストールする場合、最適なビデオ・パフォーマンスを得るために、いくつかの追加セットアップが必要になります。パフォーマンスを調整するには、以下の作業を行ってください。

1. Windows の「スタート」メニューで、「設定」->「コントロール パネル」->「画面」をクリックします。
2. 「画面のプロパティ」パネルで、「設定」タブをクリックします。
3. 「詳細設定」をクリックします。
4. 「トラブルシューティング」タブをクリックします。
5. 「ハードウェア アクセラレータ」スライダーを必要に応じて調整します。
6. 「適用」をクリックします。
7. 「OK」をクリックします。
8. 再び「OK」をクリックして、変更を受け入れます。

インストール中のエラー・メッセージへの応答

統合 Windows サーバーのインストール段階では、i5/OS のインストール段階で入力しなかったために欠落している情報にフラグを付け、その情報を提供できるようにします。このセクションには、これらのエラー・メッセージとその応答方法の例が記載されています。

エラー (サーバーのインストール時)

i5/OS上の「Windows サーバーのインストール」画面の、「ワークグループ用」または「ドメイン用」フィールドに値を設定していないことがあります。そうでない場合、以下のエラー・メッセージが表示されま

Error (Installing Server)

A setup parameter specified by your system administrator or computer manufacturer is missing or invalid. Setup must therefore ask you to provide this information now.

Once you have furnished the required information, unattended Setup operation will continue.

You may wish to inform your system administrator or computer manufacturer that the "JoinWorkgroup" value is missing or invalid.

「OK」をクリックします。

インストール・プログラムは、ワークグループまたはドメインのメンバーをコンピューターに作成するように指示します。

TCP/IP に応じた統合 Windows サーバーのオンへの自動変更の設定

TCP/IP の開始時に統合サーバーが自動的にオンに変更されるように設定できます。ただし、1 つのファイル・サーバー・リソースを複数の統合サーバーが使用する場合、そのうちの 1 つだけを自動開始するように構成します。同時にファイル・サーバー・リソースを使用できるネットワーク・サーバーは 1 つだけです。同じリソースを共有するネットワーク・サーバーで自動開始されるように、複数の TCP/IP インターフェースを構成すると、予期しない結果が生じる場合があります。

TCP/IP の開始時に統合サーバーを自動的にオンに変更するには、次のステップを行います。

1. i5/OS コマンド行で、「TCP/IP の構成 (CFGTCP)」コマンドを入力します。
2. オプション 1 「TCP/IP インターフェースの処理」を選択して、Enter キーを押します。
3. サーバーについての Point-to-Point 仮想イーサネット (仮想イーサネット Point-to-Point) 回線記述のインターフェースの横の「Opt」フィールドで 2 (変更) を指定して、Enter キーを押します。

注: Point-to-Point 仮想イーサネット回線記述の名前は、ネットワーク・サーバー記述 (NWS) 名の後に、仮想イーサネット Point-to-Point LAN の場合は 'PP' が続きます。たとえば、NWS 名が MYSVR である場合、Point-to-Point 仮想イーサネット LAN 回線記述は MYSVRPP です。

4. 自動開始パラメーター値を *YES に変更して、Enter キーを押します。統合サーバーは、TCP/IP の開始時に自動的にオンに変更されます。

注: V5R1 以後は、システムの IPL 属性を変更すれば、IPL 時に TCP/IP を自動始動することができます。そのため、始動手順はもう不要になります。自動開始パラメーターを *YES に設定された TCP インターフェースは、IPL 時に TCP/IP と一緒に始動します。

注: TCPPRTCFG パラメーター *VRTETHPTP ポートの NWS で設定された値を、Point-to-Point 仮想イーサネットの統合コンソールで入力された IP アドレスがオーバーライドすることに注意してください。しかし、SBMNWSCMD のような操作は、NWS で設定される値を使ってサーバーを検索します。両方の値は一貫していなければなりません。

コード修正

IBM iSeries 統合サーバー・サポートのコード修正を使えば、次のソフトウェア・リリースまで待たなくても、可能な限りエラーのない最新のコードを利用することができます。これらは、Microsoft Windows サーバーを統合サーバー上で実行可能にする iSeries 統合サーバー・サポート・コードを更新します。これらは、Microsoft 社から入手しなければならない Windows 自体のサービス・パックとは別個のものです。

『コード修正のタイプ』を参照してください。

統合サーバーにコード修正をインストールするプロセスは、同期と呼ばれます。統合サーバーを同期するとき、統合ソフトウェアは統合サーバー上の統合ソフトウェアが i5/OS 統合ソフトウェアと同じサービス・パックとリリース・レベルであることを確認します。Windows 側のコードのレベルは、i5/OS 側のコードのレベルに依存します。

統合ソフトウェアを使用して統合サーバーを同期するとき、「マシンの内側で」実行可能な 4 つのアクションがあります。

1. i5/OS が新規リリースにアップグレード (V5R3 から V5R4 など) されているとき、新規リリースのソフトウェアは旧リリースのソフトウェアに置き換わります。
2. 新規の IBM iSeries 統合サーバー・サポートのサービス・パックが i5/OS 上にインストールされた場合、それは統合サーバーにコピーされます。
3. IBM iSeries 統合サーバー・サポートのサービス・パックが i5/OS 上から除去された場合、それは統合サーバーからも除去されて、i5/OS に現在存在するコードに置き換わります。
4. i5/OS 統合コードと統合サーバー・コードとが同じレベルの場合でも、同期操作は実行できます。これは、統合サーバー上の削除または損傷したファイルを復元するために許可されています。

どの場合でも、統合サーバーは i5/OS に存在するソフトウェアと同じレベルになります。

同期を実行する方法は、次の 3 つあります。

- 120 ページの『Windows サーバー・コンソールによる統合ソフトウェア・レベルの同期化』。
- 120 ページの『iSeries ナビゲーターによる統合ソフトウェア・レベルの同期化』。
- 121 ページの『リモート・コマンドによる統合ソフトウェア・レベルの同期化』。


同期を実行する際に問題があれば、246 ページの『IBM iSeries 統合サーバー・サポート・スナップイン・プログラム』を参照してください。

コード修正のタイプ


コード修正には、次の 4 つのタイプがあります。

1. i5/OS 統合コードに適用されるコード修正。**通常のプログラム一時修正 (PTF)** と呼ばれます。

- これらは、i5/OS にインストールするだけで、適用できます。
- これらのコード修正は、IBM サポートまたはインターネット

(<http://www.ibm.com/servers/eserver/series/integratedxseries>)  から入手できます (左のナビゲーション・バーから、サービス・サポートをたどってください)。

2. 統合サーバーのドライブにコピーされて、統合サーバー上で実行するコード修正。**サービス・パック PTF** と呼ばれます。

- | • IBM iSeries 統合サーバー・サポート・ライセンス・プログラムには、i5/OS 側からコピーされる統合サーバー部分があります。i5/OS 累積 PTF パッケージを適用すると、そこに統合サーバーに適用可能な統合サーバー・サポートのサービス・パックが含まれていることがあります。これは、統合サーバーを同期することによって行います。
- | • これらのコード修正も IBM サポートまたはオンライン
 - | (<http://www.ibm.com/servers/eserver/iseries/integratedxseries/>)  から入手できます (左のナビゲーション・バーから、サービス・サポートをたどってください)。
- | 3. Microsoft Windows サーバー自体に適用されるコード修正。サービス・パックと呼ばれます。
 - | • これらは、Microsoft から入手します。Windows Update Web サイトからダウンロードすることができます。
 - | • Microsoft からのコード修正で、IBM iSeries 統合サーバー・サポートによって使用される Windows サーバーの部分を変更する可能性のあるものは、適用しないでください。例えば、SCSI ストレージ・デバイス・ドライバーや LAN デバイス・ドライバーを Windows Update からダウンロードしないでください。
 - | • その他の分野のものは、一般に安全です。例えば、USB デバイス・ドライバーは Windows Update から自分の責任でダウンロードできます。
- | 4. Hot Fix。Microsoft Windows サーバーそれ自体または、Windows Update を使用して適用されます。

Windows サーバー・コンソールによる統合ソフトウェア・レベルの同期化

iSeries 統合サーバー・サポート・スナップインを使ってソフトウェア・レベルを同期するには、Windows のシステム管理者でなければなりません。インストールの開始前に、実行しているアプリケーションをすべて終了し、統合サーバーにログオンしているユーザーがいらないことを確認してください。この作業を行わないと、インストールの完了後に統合サーバーの再始動が必要になることがあるので、データが失われる場合があります。

1. 「スタート」->「プログラム」->「IBM iSeries」->「IBM iSeries 統合サーバー・サポート (IBM iSeries Integrated Server Support)」をクリックします。
2. 統合サーバーの名前をクリックしてから、「ソフトウェア・レベル (Software level)」をクリックします。
3. i5/OS統合ソフトウェアおよび Windows 統合ソフトウェアのソフトウェア・レベルが表示されます。「同期 (Synchronize)」をクリックして、Windows 統合ソフトウェアを i5/OS 統合ソフトウェアと同じレベルにします。
4. インストールが正常に行われると、確認メッセージが表示されます。

注: 統合 Windows サーバーのコンソールに管理者としてログオンして、ソフトウェア・レベルの不一致が存在する場合、ソフトウェアを同期するように自動的に求められます。

iSeries ナビゲーターによる統合ソフトウェア・レベルの同期化

1. iSeries ナビゲーターで、「統合サーバー管理」->「サーバー」をクリックします。
2. 同期する統合サーバーを右マウス・ボタンでクリックして、「iSeries 統合ソフトウェアの同期化 (Synchronize iSeries Integration Software)」を選択します。(アクセスしている i5/OS サーバーが V5R3 以降のサーバーでなければ、サービス・パックを個別にインストールまたはアンインストールするかまたはリリース更新だけを実行するための、以前のオプションのリストが表示されます)。
3. 「同期 (Synchronize)」をクリックして、操作を確定します。

- 同期化が進行中であることを示すメッセージが表示されてから、すぐにリポートが行われることを示す完了メッセージが表示されます。すぐにリポートするかどうかは選択できません。

i5/OS および統合サーバーにインストールされているソフトウェアのレベルを調べるには、以下の手順に従います。

- iSeries ナビゲーターで、「統合サーバー管理」->「サーバー」をクリックします。
- 調べたい統合サーバーを右マウス・ボタンでクリックして、「プロパティ」を選択します。
- 「ソフトウェア」タブをクリックします。そこに、ソフトウェア・レベルが表示されます。

リモート・コマンドによる統合ソフトウェア・レベルの同期化

統合 Windows サーバーのコンソールのコマンド・プロンプトにコマンド `lvlsync` を入力すると、統合サーバーは同期します。このコマンド行プログラムの主な利点は、リモート側でコマンドを出して統合サーバーを同期できることです。例えば、統合サーバーを定期的に同期する CL プログラムを作成するときなど、この機能が役立ちます。リモート側で出されるコマンドについては、168 ページの『統合 Windows サーバーのコマンドのリモート実行』を参照してください。

`lvlsync` コマンドを i5/OS コンソールからリモートで出して統合サーバーをリモート側で同期するための、簡単な手順を示します。

- i5/OS文字ベースのインターフェースで、`SBMNWSCMD` と入力して **F4** を押します。
- 「コマンド」フィールドに `lvlsync` と入力して、**Tab** を押します。
- 統合サーバーの `NWSD` 名を「サーバー」フィールドに入力して、**Enter** キーを押します。

過去には、`lvlsync` プログラムにオプション・パラメーターを指定できました。それらのパラメーターは機能なくなっていますが、コマンドに指定されていても機能には影響しません。

`lvlsync` は、以下のエラー・コードを戻します。

lvlsync エラー・コード

エラー・コード	エラー
0	エラーなし
01	<code>lvlsync</code> を実行するのは、管理者でなければならない
02	統合 Windows サーバー上のリリース・レベルが i5/OS 上のものより高い
03	統合サーバー上のサービス・パック・レベルが i5/OS 上のものより高い
04	i5/OS からリリースをインストールできない - 言語ファイルが i5/OS にない
05	構文が無効
06	i5/OS 上のサービス・パック情報にアクセスできない
07	ネットワーク・ドライブをマッピングできない
08	レジストリー内のサービス・パック情報にアクセスできない
09	<code>qvnacfg.txt</code> ファイルをオープンできない
10	i5/OS 上にサービス・パックがインストールされていない
11	<code>NWSD</code> を検出できない
13	<code>NWSD</code> が非活動状態
20	i5/OS 上で使用できるサービス・パックがない。
21	<code>InstallShield</code> アプリケーションが開始できない

エラー・コード	エラー
31	lvlsync の開始時に予期しないエラー
44	lvlsync 処理中の予期しないエラー

注: エラー・メッセージ NTA0218 は、構文エラー、権限エラー、NWSD を検出できないというエラーの診断 (*DIAG) メッセージです。

第 6 章 仮想イーサネットおよび外部ネットワークの管理

このセクションでは、29 ページの『ネットワークングの概念』で説明された仮想イーサネットおよび外部ネットワークを作成して理解するために役立つ手順を示します。

- 『IP アドレス、ゲートウェイ、および MTU 値の構成』
- 『仮想イーサネット・ネットワークの構成』
- 124 ページの『区画間仮想イーサネット・ネットワークの構成』
- 126 ページの『Point-to-Point 仮想イーサネット・ネットワークについて』
- 127 ページの『外部ネットワーク』
- 128 ページの『ネットワーク・アダプターの除去』

IP アドレス、ゲートウェイ、および MTU 値の構成

ホストされるシステムにおける仮想および物理ネットワーク・アダプターの IP アドレス、ゲートウェイ、および最大伝送単位 (MTU) 値は、以下の場合を除き、Windows オペレーティング・システムから管理されます。

- 新規仮想イーサネット回線記述の IP アドレスおよびサブネット・マスクは、i5/OS の Windows サーバー導入 (INSWNTSVR) コマンドにより任意指定で割り当てることができます。サーバーのインストールの後には、これらの値は、Windows オペレーティング・システム内からしか変更できません。
- IP アドレスおよびサブネット・マスクは、仮想イーサネット回線が既存のサーバーに追加される時に割り当てることができます。回線記述が追加された後は、これらの値は、Windows オペレーティング・システム内からしか変更できません。
- 仮想イーサネット Point-to-Point IP アドレスの変更は、Windows オペレーティング・システムおよび i5/OS の両方で構成する必要があります。263 ページの『Point-to-Point 仮想イーサネット IP アドレスの競合』を参照してください。
- iSCSI ネットワークの Windows 側の IP アドレスおよびゲートウェイ値は常に、i5/OS リモート・システム構成から構成および変更されます。134 ページの『リモート・システム構成プロパティの変更』を参照してください。
- IXS 外部 LAN アダプターの IP アドレス、サブネット・マスク、ゲートウェイ、および MTU 値は、i5/OS の Windows サーバー導入 (INSWNTSVR) コマンドで任意指定で設定することができます。サーバーのインストールの後には、これらの値は、Windows オペレーティング・システム内からしか変更できません。

仮想イーサネット・ネットワークの構成

このセクションでは、統合サーバー間で仮想イーサネット・ネットワークを構成する方法について説明します。(なお、統合サーバーを最初からインストールする場合は、インストール・コマンド (INSWNTSVR) を実行することで仮想イーサネット・ネットワークを構成できます。)他の iSeries 論理区画に仮想イーサネット・ネットワークを拡張する方法については、124 ページの『区画間仮想イーサネット・ネットワークの構成』を参照してください。手順は、以下の基本的なステップから構成されています。

1. 統合サーバーのための仮想イーサネット・ポートおよび回線記述を構成します。iSeries ナビゲーターを使用して、以下のようになります。

- a. 「統合サーバー管理」 → 「サーバー」を展開します。
 - b. 統合サーバーを右マウス・ボタンでクリックして、「プロパティ」を選択します。
 - c. サーバー・プロパティ・パネルで、「仮想イーサネット」タブをクリックします。
 - d. 「追加...」ボタンをクリックして新しい仮想イーサネット・ポートを追加します。
 - e. 「仮想イーサネット・プロパティ」パネルで、新しい仮想イーサネット・ポートの値を指定します。
 - 1) 仮想イーサネットのポート番号を選択します。
 - 2) 統合サーバーで使用する IP アドレスを入力します。
 - 3) 統合サーバーで使用するサブネット・マスクを入力します。
 - 4) デフォルトの回線記述名のままにするか、それを別の名前に変更することができます。デフォルトの回線記述名は、NWSD 名の次に v、その次にポート番号が付きます。たとえば、Mynwsd という名前の NWSD にポート 3 を追加する場合、デフォルトの回線記述名は Mynwsdv3 となります。
 - 5) 関連したポートを「なし」の設定のままにします。
 - 6) 最大フレーム・サイズをデフォルトの 8996 の設定のままにします。
 - 7) サーバーが iSCSI 接続サーバーの場合、この仮想イーサネット構成で、ホストされるシステムへ i5/OS が到達するために使用する iSCSI HBA に対応するネットワーク・サーバー・ホスト・アダプターを選択します。
 - 8) 「OK」をクリックし、新しいポートを、サーバー・プロパティ・パネルの「仮想イーサネット」タブに追加します。
 - f. サーバー・プロパティ・パネルで、「OK」をクリックして変更を保管します。これで NWSD が更新され、新しい仮想イーサネット・ポートの回線記述が作成されます。
 - g. この統合サーバーを複数の仮想イーサネット・ネットワークに接続したい場合は、上の一連のステップを繰り返して、ネットワークごとに別の仮想イーサネット・ポート番号を使用して仮想イーサネット・ポートおよび回線記述を作成します。
2. ネットワークに接続するすべての統合サーバーに関し、それぞれに同じ仮想イーサネット・ポートを指定して、上記の手順を繰り返します。
 3. 統合サーバーを再始動させます。仮想イーサネット・アダプターのデバイス・ドライバーが自動的にインストールされ、NWSD で指定されている Windows TCP/IP アドレスに設定されます。ただし、統合サーバー・コンソールで IP アドレスが入力されると、NWSD で設定されている値は指定変更されません。
 4. テストを実行し、仮想イーサネット・ネットワークが機能しているかどうかを確認します (たとえば、特定のサーバーから別のサーバーに指定している IP アドレスに ping します)。

区画間仮想イーサネット・ネットワークの構成

ハードウェア管理コンソールを使用する区画間ネットワーク

統合サーバーで他の論理区画と通信する場合や、他の i5/OS 区画で制御されている統合サーバーと通信する場合は、1 つ以上の区画間ネットワークを構成する必要があります。iSeries システムでは、ハードウェア管理コンソール (HMC) を使用して他のシステムの場合とは異なる方法で、区画間ネットワークを構成します。iSeries HMC システムでは、区画間や同一の VLAN ID を使用する統合サーバー間に区画間接続が存在します。参加している統合サーバーは、VLAN ID を直接サポートしていません。その代わりに、参加している各統合サーバーには、仮想イーサネット・ポート値を、VLAN ID のある仮想アダプターに関連付けるイーサネット回線記述が必要になります。構成手順は、以下のステップから構成されています。

1. ハードウェア管理コンソール (HMC) を使用し、区画間ネットワークに参加する各区画および各統合サーバーに仮想イーサネット・アダプターを作成します。詳しくは、eServer i5 による区画化および区画間仮想イーサネット・ネットワークの構成を参照してください。統合サーバーや i5/OS 区画を区画間ネットワークに接続する各仮想アダプターごとに、一貫性のあるポート仮想 LAN ID を指定し、「**IEEE 802.1Q compatible adapter (IEEE 802.1Q 互換アダプター)**」のチェック・マークを外してください。
2. 使用したいポート (0 から 9) に回線記述がまだ作成されていない場合は、123 ページの『仮想イーサネット・ネットワークの構成』の、1 (123 ページ) のステップに説明されているように仮想イーサネット・ポートおよび回線記述を構成します。該当する 268C リソース用の関連したポート名 (Cmnxx) を選択します。
3. 続けて、123 ページの『仮想イーサネット・ネットワークの構成』のステップ 2 (参加する統合サーバーを制御するすべての i5/OS 区画で)、および 123 ページの『仮想イーサネット・ネットワークの構成』のステップ 3 を実行します。
4. 区画を完全に参加させるためには、区画内に適切にプロトコルを構成する必要があります。各 i5/OS 区画では、該当する専用 268C ポート・リソースにイーサネット回線記述を作成します。TCP/IP 通信に参加する各区画に、適切な固有 IP アドレスを構成します。
5. 区画間ネットワークが機能しているかどうかを確認するテストを実行します (たとえば、接続されている統合サーバーや区画の間で ping を実行します)。

ハードウェア管理コンソールを使用しない区画間ネットワーク

- iSeries HMC システム以外のシステムでは、同一のネットワーク番号を使用する区画の間に区画間接続が存在し、統合サーバーは、制御を行う i5/OS 区画が接続されている場合のみ接続されます。ネットワーク番号の 0 から 9 までは、統合サーバーのためのものです。たとえば、i5/OS 区画がネットワーク 1 と 5 で区画間通信用に構成されている場合、その区画によって制御される統合サーバーは、仮想イーサネット・ポート 1 と 5 で区画間通信に参加できます。構成手順は、以下のステップで構成されています。
1. 各区画を接続させるネットワーク番号を構成します。『論理区画の概念』および iSeries ナビゲーターのオンライン・ヘルプ情報を参照してください。統合サーバーは、制御している i5/OS 区画が接続される場合のみ接続されるという点にご注意ください。
 2. 使用したいポート (0 から 9) に回線記述がまだ作成されていない場合は、説明されているように仮想イーサネット・ポートおよび回線記述を構成します。123 ページの『仮想イーサネット・ネットワークの構成』のステップ 1 を参照してください。関連したポート名を「なし」の設定のままにします。
 3. 続けて、123 ページの『仮想イーサネット・ネットワークの構成』のステップ 2 (参加する統合サーバーを制御するすべての i5/OS 区画で)、および 123 ページの『仮想イーサネット・ネットワークの構成』のステップ 3 を実行します。
 4. 区画を完全に参加させるためには、区画内に適切にプロトコルを構成する必要があります。参加させる各 i5/OS 区画で、WRKHDWRSC *CMN コマンドを使用し、自動的に作成されたハードウェア・タイプ 268C の該当ポートの名前を検索してください。123 ページの『仮想イーサネット・ネットワークの構成』のステップ 1 を参照してください。次いで、その 268C ポート・リソースにイーサネット回線記述を作成します。TCP/IP 通信に参加する各区画に、適切な固有 IP アドレスを構成します。
 5. 区画間ネットワークが機能しているかどうかを確認するテストを実行します (たとえば、接続されている統合サーバーや区画の間で ping を実行します)。

Point-to-Point 仮想イーサネット・ネットワークについて

各統合サーバーには、iSeries による統合サーバーの制御を可能にする、iSeries との Point-to-Point 仮想イーサネット・ネットワーク接続があります。これらの接続はインストール時に自動的に構成されますが、ここではこれらを表示または変更する方法について説明します。

i5/OS からの Point-to-Point イーサネット接続の表示

i5/OS の Point-to-Point イーサネット接続は、回線記述と、統合サーバーの NWSD のエントリーで構成されています。

1. 回線記述を表示するには、i5/OS の文字ベースのインターフェースからコマンド WRKCFGSTS *NWS を発行します。
2. 統合サーバーに対応するエントリーのカスケードを検索してください。「回線記述」列のエントリーの 1 つに、NWSD と同じ名前を持ち、文字 PP で終わるエントリーがあります。その左側に 8 と入力し、Enter キーを押してください。
3. 「回線記述の処理」メニューが開かれます。使用する回線記述の左側に 5 と入力して Enter キーを押すと、情報が表示されます。
4. 基本メニューに戻るまで F3 を押します。
5. この状態でコマンド CFGTCP を発行し、オプション 1、「TCP/IP インターフェースの処理」を選択します。
6. 「回線記述」列のエントリーの 1 つに、NWSD と同じ名前を持ち、文字 PP で終わるエントリーがあるはずですが。
7. オプション 5 では TCP/IP インターフェース情報が表示され、オプション 9 および 10 で、これを使用可能および使用不可に設定できます。インターネット・アドレスを記録しておいてください。これは後で使用します。
8. ここで、統合サーバーの NWSD にあるエントリーを簡単に見てみます。コマンド WRKNWSD を発行してください。統合サーバーの NWSD を探し、5 を入力してこれを表示します。Enter を押して、NWSD 属性のページを順に表示します。
9. 画面の 1 つは「接続されている回線 (Attached lines)」というタイトルで、ここに、そのネットワークで使用しているポート番号 *VRTETHPTP と回線記述の名前が表示されます。
10. 「ネットワーク・サーバー記述の処理」メニューに戻ると、オプション 2 を使用してこの情報を変更できます。

統合 Windows サーバー・コンソールからの Point-to-Point イーサネット接続の表示

1. 統合サーバーのコンソールで、「スタート」→「設定」→「コントロール パネル」をクリックします。次に「ネットワークとダイヤルアップ接続」を選択します。
2. アイコンの 1 つに、「仮想イーサネット Point-to-Point」というものがあります。これをダブルクリックしてください。
3. 表示されるダイアログ・ボックスで「プロパティ」をクリックします。
4. 次のテキスト・ダイアログ・ボックスの「インターネット・プロトコル (TCP/IP)」をダブルクリックします。
5. この最後のダイアログ・ボックスには、Point-to-Point 仮想イーサネット接続の統合サーバー側に関連した IP アドレスが表示されるはずですが。これは i5/OS の IP アドレスに 1 を加算して、奇数ではなく偶数でなければなりません。

6. 開いているウィンドウをすべて閉じ、「スタート」→「ファイル名を指定して実行」をクリックして、コマンド `cmd` を入力します。Enter キーを押します。すると、Windows コマンド・プロンプトのインスタンスが開始されます。
7. 表示されている `C:\>` コマンド・プロンプトで、`ping` コマンドを入力し、直前のステップの `i5/OS` IP アドレスをその後に入力します。たとえば、`ping 192.168.3.1` のようにです。コマンドは、「Reply from」を戻すはずで、そうであれば良好です。`ping` コマンドは、特定の IP アドレスにデータの packets を送信し、往復するのにどれほどの時間がかかるかを計測します。
8. (オプション) `i5/OS` 文字ベース・インターフェースに戻り、コマンド `call qcnd` を入力します。(これにより、コマンドの結果を表示できるよう、表示スペースが拡張されます。) `i5/OS` コマンドを使用して統合サーバーを `ping` してください。たとえば、`ping '192.168.3.2'` のようにします。おめでとうございます。以上がすべて適切に行われたなら、Point-to-Point 仮想イーサネット・ネットワークが適切に機能していることとなります。

外部ネットワーク

空いている PCI スロットには、新しいネットワーク・アダプター・カードをインストールできます。これを行う場合は、統合 Windows サーバー上で新しいアダプターを構成する必要があります。

新規ネットワーク・アダプター・カードのインストールについては、`iSeries` フィーチャーの取り付けを参照してください。`iSeries` のモデルを選択して、「**Install PCI Card and Integrated xSeries Adapter Card**」という題名の指示を検索します。

新規ネットワーク・アダプターをセットアップする場合は、『統合 Windows サーバーへのネットワーク・アダプター・デバイス・ドライバのインストールと、アダプター・アドレス情報の追加』を参照してください。

仮想イーサネット接続を作成する場合は、123 ページの『仮想イーサネット・ネットワークの構成』を参照してください。

ネットワーク・アダプターを除去する場合は、128 ページの『ネットワーク・アダプターの除去』を参照してください。

統合 Windows サーバーへのネットワーク・アダプター・デバイス・ドライバのインストールと、アダプター・アドレス情報の追加


ここで、統合 Windows サーバーにアダプター・デバイス・ドライバをインストールし、新しいアダプターのアダプター・アドレス情報を追加することができます。

Windows 2000 Server および Windows Server 2003 のアダプターおよびデバイス・ドライバでは、Plug-n-Play がサポートされています。アダプターを物理的に設置したら、アダプターを有効にするため、統合サーバーをオンに変更することによりリブートしてください。必ず、アダプター (接続) ごとに IP アドレスを構成するようにします。

統合 `xSeries` サーバーを Windows NT 4.0 から Windows 2000 Server にアップグレードする場合は、新しいアダプターを追加する前に古いアダプターを除去してください。128 ページの『ネットワーク・アダプターの除去』を参照してください。

Windows 2000 Server または Windows Server 2003 は、新しいアダプターを認識します。所定のアダプター用の IP アドレスを構成するには、以下のようにします。

1. 「マイネットワーク」を右クリックして、プルダウン・メニューから「プロパティ」をクリックします。
2. 適切なアダプター (ローカル・エリア接続) をダブルクリックし、IP アドレスを構成します。
3. 「プロパティ」ボタンをクリックします。
4. 「インターネット・プロトコル (TCP/IP)」を選択し、「プロパティ」ボタンをクリックします。
5. まだ選択していなければ、「次の IP アドレスを使う」ラジオ・ボタンをクリックします。
6. 「IP アドレス」フィールドに、IP アドレスを指定します。
7. 「サブネット マスク」フィールドに、サブネット・マスクを指定します。
8. 「デフォルト ゲートウェイ」フィールドに、デフォルトのゲートウェイ・アドレスを指定します。
9. 「OK」、「OK」、「閉じる」の順にクリックして、IP アドレスの設定を完了します。

注: IP アドレスが他のアダプター用に構成済みであることを Windows が示しているものの、そのアドレスをすでに使用しているアダプターを見つけることができない場合、Windows はそのアドレスを使用していた直前のハードウェア環境を認識している可能性があります。IP アドレスを解放できるように直前のハードウェア環境の LAN アダプターを表示するには、Microsoft Knowledge Base 資料 Q241257 Device Manager Does Not Display Devices Not Currently Present in Windows 2000  を参照してください。

ネットワーク・アダプターの除去

- 統合 Windows サーバーからネットワーク・アダプター・カードを取り外す場合、これを取り外す前に、Windows 内からアダプターをアンインストールする必要があります。
- 統合サーバーからネットワーク・アダプターをアンインストールする場合は、以下のステップを実行します。
 1. 「スタート」、「設定」、「コントロール パネル」の順にクリックします。
 2. 「ハードウェアの追加と削除」ウィザードを開始し、最初のパネルで「次へ」をクリックします。
 3. 「デバイスの削除/取り外し」をクリックします。
 4. 「削除操作の選択」パネルで「次へ」をクリックして、デフォルト（「デバイスの取り外し」）を使用します。
 5. アンインストールする装置 (たとえば、IBM PCI Token-Ring Adapter) をリストから選択します。
 6. そのアダプターが除去したいアダプターであることを確認して、「はい」をクリックします。
 7. Windows 2000 Server および Windows Server 2003 はプラグ・アンド・プレイのオペレーティング・システムであるため、サーバーの再始動前に、アダプターを i5/OS から物理的に除去するか、または使用不可にする必要があります。アダプターがプラグインされたまま統合サーバーを再始動させると、オペレーティング・システムは、これを新しいハードウェアとして認識し、デバイス・ドライバを再インストールしてしまいます。アダプターを除去せずに使用不可にする場合は、次のステップを行います。
 - a. 「コントロール パネル」で、「ネットワークとダイヤルアップ接続」を選択します。
 - b. LAN アダプターを選択します。
 - c. 右クリックし、「無効にする」を選択します。
 8. サーバーを再始動してこの手順を完了します。

第 7 章 iSCSI 接続サーバーへの接続の管理

以下のセクションでは、iSCSI HBA 統合サーバー上で実行する作業について説明します。

- 『iSCSI 構成オブジェクトの処理』
- 141 ページの『i5/OS とホストされるシステムとの間のセキュリティーの構成』
- 146 ページの『iSCSI ホスト・バス・アダプターの管理』
- 154 ページの『リモート・サーバーのディスカバリーおよび管理』

iSCSI 構成オブジェクトの処理

iSeries 用の iSCSI HBA、リモート xSeries または IBM BladeCenter システム、リモート・システムのサービス・プロセッサ、および iSCSI ネットワークのセキュリティー属性を構成および管理するには、i5/OS オブジェクトを使用します。詳細については、以下を参照してください。

- 『ネットワーク・サーバー・ホスト・アダプターの管理』
- 132 ページの『リモート・システム・ネットワーク・サーバー構成の管理』
- 135 ページの『サービス・プロセッサ・ネットワーク・サーバー構成の管理』
- 138 ページの『接続セキュリティー・ネットワーク・サーバー構成の管理』

ネットワーク・サーバー・ホスト・アダプターの管理

iSeries ターゲット iSCSI ホスト・バス・アダプター (iSCSI HBA) を構成するには、ネットワーク・サーバー・ホスト・アダプター (NWSH) オブジェクトを使用します。統合サーバーが記憶域または仮想イーサネット・データ・フロー用の iSCSI HBA を使用するには、対応する NWSH オブジェクトを開始 (オンに変更) しなければなりません。NWSH オブジェクトを停止 (オフに変更) すると、これに対応する iSCSI HBA は、この iSCSI HBA を使用するよう定義された記憶域または仮想イーサネット・バスを持つ統合サーバーから使用不可になります。詳しくは、45 ページの『ネットワーク・サーバー・ホスト・アダプター』を参照してください。

NWSH オブジェクトに対して以下のタスクを実行できます。

- 『ネットワーク・サーバー・ホスト・アダプター・オブジェクトの作成』
- 130 ページの『別のオブジェクトを基にしてネットワーク・サーバー・ホスト・アダプター・オブジェクトを作成する』
- 131 ページの『ネットワーク・サーバー・ホスト・アダプターのプロパティの表示』
- 131 ページの『ネットワーク・サーバー・ホスト・アダプターのプロパティの変更』
- 131 ページの『ネットワーク・サーバー・ホスト・アダプターの開始』
- 132 ページの『ネットワーク・サーバー・ホスト・アダプターの停止』
- 132 ページの『ネットワーク・サーバー・ホスト・アダプターの削除』

ネットワーク・サーバー・ホスト・アダプター・オブジェクトの作成

iSeries ターゲット iSCSI ホスト・バス・アダプター (iSCSI HBA) のそれぞれに対して、ネットワーク・サーバー・ホスト・アダプター (NWSH) オブジェクトを作成しなければなりません。

1 iSeries ナビゲーターを使用してネットワーク・サーバー・ホスト・アダプターを作成するには、以下のステップを行います。

1. 「統合サーバー管理」を展開します。
2. 「iSCSI 接続」を展開します。
3. 「ローカル・ホスト・アダプター」を右マウス・ボタンでクリックします。
4. 「新規のネットワーク・サーバー・ホスト・アダプター」を選択します。
5. 「一般」タブで、以下のようになります。
 - NWSH 装置の名前を「名前」に、説明を「記述」に入力します。
 - 「ハードウェア・リソース」を選択します。
 - 「オブジェクト権限」を選択します。
6. 「ローカル・インターフェース」タブで、iSCSI HBA の SCSI および LAN インターフェース属性を定義する情報を入力します。
7. 「OK」をクリックします。

注: ネットワーク・サーバー・ホスト・アダプターとリモート・システム構成は、iSCSI ネットワークの両側の IP アドレス情報を定義します。単純な交換網で接続する際には、以下の規則が適用されます。

- スイッチによって接続されたこれら 2 つのオブジェクトの SCSI インターネット・アドレスは、同一のサブネットになければなりません。例えば、a.b.x.y という形式の IP アドレスと 255.255.255.0 というサブネット・マスクの場合、両方のオブジェクトの a.b.x は同じ値でなければなりません。
- スイッチによって接続されたこれら 2 つのオブジェクトの LAN インターネット・アドレスは、同一のサブネットになければなりません。
- ネットワーク内にゲートウェイがない場合、ネットワーク・サーバー・ホスト・アダプターのゲートウェイ・エレメントは、任意のサブネット内の任意の未割り当ての IP アドレスにすることができます。
- ネットワーク内にゲートウェイがない場合、リモート・システム構成のゲートウェイ・エレメントは、ブランクにする必要があります。

CL コマンドを使用する場合は、CRTDEVNWSH または WRKDEVD を参照してください。

別のオブジェクトを基にしてネットワーク・サーバー・ホスト・アダプター・オブジェクトを作成する

新しいネットワーク・サーバー・ホスト・アダプター (NWSH) オブジェクトを作成する際に、既存のオブジェクトをコピーできます。新しい NWSH 属性の一部が既存の NWSH の属性と同じ場合や似ている場合は、こうすることで時間を節約できます。

iSeries ナビゲーターを使用し、既存のネットワーク・サーバー・ホスト・アダプターを基にして別のアダプターを作成するには、以下のステップを行います。

1. 「統合サーバー管理」を展開します。
2. 「iSCSI 接続」を展開します。
3. 「ローカル・ホスト・アダプター」を選択します。
4. 表示されたリストで、コピーするローカル・ホスト・アダプターを右マウス・ボタンでクリックします。
5. 「既存のものを基にした新規作成」を選択します。
6. 新しい NWSH 装置の名前を「名前」に入力します。

- | 7. その他の属性のうち、コピー元の NWSH と違っていなければならないものを指定します。
- | 8. 「OK」をクリックします。
- | CL コマンドを使用する場合は、WRKDEVD を参照してください。

| ネットワーク・サーバー・ホスト・アダプターのプロパティの表示

- | ネットワーク・サーバー・ホスト・アダプター (NWSH) オブジェクトには、iSeries ターゲット iSCSI ホスト・バス・アダプター (iSCSI HBA) に関する構成情報が含まれています。
- | iSeries ナビゲーターを使用して、ネットワーク・サーバー・ホスト・アダプターの属性を表示するには、以下のステップを行います。
- | 1. 「統合サーバー管理」を展開します。
- | 2. 「iSCSI 接続」を展開します。
- | 3. 「ローカル・ホスト・アダプター」を選択します。
- | 4. 表示されたりストで、ローカル・ホスト・アダプターを右マウス・ボタンでクリックします。
- | 5. 「プロパティ」を選択します。
- | 6. 表示するプロパティに該当するタブをクリックします。
- | 7. 「キャンセル」をクリックし、パネルをクローズします。
- | CL コマンドを使用する場合は、DSPDEVD または WRKDEVD を参照してください。

| ネットワーク・サーバー・ホスト・アダプターのプロパティの変更

- | ネットワーク・サーバー・ホスト・アダプター (NWSH) オブジェクトには、iSeries ターゲット iSCSI ホスト・バス・アダプター (iSCSI HBA) に関する構成情報が含まれています。
- | iSeries ナビゲーターを使用して、ネットワーク・サーバー・ホスト・アダプターの属性を変更するには、以下のステップを行います。
- | 1. 「統合サーバー管理」を展開します。
- | 2. 「iSCSI 接続」を展開します。
- | 3. 「ローカル・ホスト・アダプター」を選択します。
- | 4. 表示されたりストで、ローカル・ホスト・アダプターを右マウス・ボタンでクリックします。
- | 5. 「プロパティ」を選択します。
- | 6. 変更を加えるプロパティに該当するタブをクリックします。
- | 7. 「OK」をクリックして、変更内容を保管します。
- | CL コマンドを使用する場合は、CHGDEVNWSH または WRKDEVD を参照してください。

| ネットワーク・サーバー・ホスト・アダプターの開始

- | 統合サーバーが記憶域または仮想イーサネット・データ・フロー用の iSeries ターゲット iSCSI ホスト・バス・アダプター (iSCSI HBA) を使用するには、対応するネットワーク・サーバー・ホスト・アダプター (NWSH) オブジェクトを開始 (オンに変更) しなければなりません。
- | iSeries ナビゲーターを使用してネットワーク・サーバー・ホスト・アダプターを開始するには、以下のステップを行います。
- | 1. 「統合サーバー管理」を展開します。
- | 2. 「iSCSI 接続」を展開します。

- | 3. 「ローカル・ホスト・アダプター」を選択します。
 - | 4. 表示されたリストで、ローカル・ホスト・アダプターを右マウス・ボタンでクリックします。
 - | 5. 「開始」を選択します。
- | CL コマンドを使用する場合は、VRYCFG または WRKCFGSTS を参照してください。

| ネットワーク・サーバー・ホスト・アダプターの停止

| ネットワーク・サーバー・ホスト・アダプター (NWSH) オブジェクトを停止 (オフに変更) すると、これ
| に対応する iSeries ターゲット iSCSI ホスト・バス・アダプター (iSCSI HBA) は、このアダプターを使用
| するよう定義された記憶域または仮想イーサネット・バスを持つ統合サーバーから使用不可になります。

| 活動状態のサーバーによって使用されている NWSH を停止することは、この NWSH に対応する iSCSI
| HBA を使用しないと重要な記憶域リソースにアクセスできなくなるようになっている場合に、サーバーの
| 障害の原因となることがあります。通常は、NWSH を停止する前に、NWSH を使用している統合サーバー
| をシャットダウンする必要があります。詳しくは、164 ページの『統合 Windows サーバーの開始と停止
| (iSeries ナビゲーターを使用する場合)』を参照してください。

| iSeries ナビゲーターを使用してネットワーク・サーバー・ホスト・アダプターを停止するには、以下のス
| テップを行います。

- | 1. 「統合サーバー管理」を展開します。
- | 2. 「iSCSI 接続」を展開します。
- | 3. 「ローカル・ホスト・アダプター」を選択します。
- | 4. 表示されたリストで、ローカル・ホスト・アダプターを右マウス・ボタンでクリックします。
- | 5. 「停止」を選択します。
- | 6. 確認パネルで「停止」をクリックします。
- | 7. 活動状態のサーバーが現在 NWSH を使用している場合は、警告メッセージが表示されます。「続行」
| をクリックします。

| CL コマンドを使用する場合は、VRYCFG または WRKCFGSTS を参照してください。

| ネットワーク・サーバー・ホスト・アダプターの削除

| iSeries ナビゲーターを使用してネットワーク・サーバー・ホスト・アダプターを削除するには、以下のス
| テップを行います。

- | 1. 「統合サーバー管理」を展開します。
- | 2. 「iSCSI 接続」を展開します。
- | 3. 「ローカル・ホスト・アダプター」を選択します。
- | 4. 表示されたリストで、ローカル・ホスト・アダプターを右マウス・ボタンでクリックします。
- | 5. 「削除」を選択します。
- | 6. 確認パネルで「削除」をクリックします。

| CL コマンドを使用する場合は、DLTDEVD または WRKDEVD を参照してください。

| リモート・システム・ネットワーク・サーバー構成の管理

| iSCSI 接続リモート xSeries または IBM BladeCenter ブレード・サーバーの属性を構成するには、リモー
| ト・システム・ネットワーク・サーバー構成 (NWSCFG サブタイプ RMTSYS) オブジェクトを使用しま
| す。リモート・システム構成は、統合サーバーを実行する特定の xSeries または IBM BladeCenter ハード

ウェアの識別に使用します。また、リモート・システムがブートする方法や、iSeries システムと通信する方法も定義します。詳しくは、45 ページの『リモート・システム構成』を参照してください。

リモート・システム構成オブジェクトに対して以下のタスクを実行できます。

- 『リモート・システム構成オブジェクトの作成』
- 134 ページの『別のオブジェクトを基にしてリモート・システム構成オブジェクトを作成する』
- 134 ページの『リモート・システム構成プロパティの表示』
- 134 ページの『リモート・システム構成プロパティの変更』
- 135 ページの『リモート・システムの状況の表示』
- 135 ページの『リモート・システム構成オブジェクトの削除』

リモート・システム構成オブジェクトの作成

iSCSI 接続の統合サーバーの実行に使用する xSeries または IBM BladeCenter サーバーごとに、リモート・システム・ネットワーク・サーバー構成 (NWSCFG サブタイプ RMTSYS) オブジェクトを作成しなければなりません。

iSeries ナビゲーターを使用してリモート・システム構成を作成するには、以下のステップを行います。

1. 「統合サーバー管理」を展開します。
2. 「iSCSI 接続」を展開します。
3. 「リモート・システム」を右マウス・ボタンでクリックします。
4. 「新規リモート・システム構成」を選択します。
5. 「一般」タブで、以下のようになります。
 - 「名前」および「記述」に入力します。
 - 「サービス・プロセッサ構成」を選択します。
 - 「リモート・システムの識別」を指定します。
 - 「オブジェクト権限」を選択します。
6. 「ネットワーク・インターフェース」タブで、リモート・システムの SCSI および LAN インターフェース属性を定義する情報を入力します。
7. 必要に応じて、「ブート・パラメーター」および「CHAP 認証」タブで値を指定します。
8. 「OK」をクリックします。

注: ネットワーク・サーバー・ホスト・アダプターとリモート・システム構成は、iSCSI ネットワークの両側の IP アドレス情報を定義します。単純な交換網で接続する際には、以下の規則が適用されます。

- スイッチによって接続されたこれら 2 つのオブジェクトの SCSI インターネット・アドレスは、同一のサブネットになければなりません。例えば、a.b.x.y という形式の IP アドレスと 255.255.255.0 というサブネット・マスクの場合、両方のオブジェクトの a.b.x は同じ値でなければなりません。
- スイッチによって接続されたこれら 2 つのオブジェクトの LAN インターネット・アドレスは、同一のサブネットになければなりません。
- ネットワーク内にゲートウェイがない場合、ネットワーク・サーバー・ホスト・アダプターのゲートウェイ・エレメントは、任意のサブネット内の任意の未割り当ての IP アドレスにすることができます。
- ネットワーク内にゲートウェイがない場合、リモート・システム構成のゲートウェイ・エレメントは、ブランクにする必要があります。

1 CL コマンドを使用する場合は、CRTNWSCFG または WRKNWSCFG を参照してください。

1 別のオブジェクトを基にしてリモート・システム構成オブジェクトを作成する

1 新しいリモート・システム・ネットワーク・サーバー構成 (NWSCFG サブタイプ RMTSYS) オブジェクトを作成する際に、既存のオブジェクトをコピーできます。新しいリモート・システム構成の属性の一部が既存のリモート・システム構成の属性と同じ場合や似ている場合は、こうすることで時間を節約できます。

1 iSeries ナビゲーターを使用し、既存のリモート・システム構成を基にして別の構成を作成するには、以下のステップを行います。

1. 「統合サーバー管理」を展開します。
2. 「iSCSI 接続」を展開します。
3. 「リモート・システム」を選択します。
4. 表示されたリストで、コピーするリモート・システム構成を右マウス・ボタンでクリックします。
5. 「既存のものを基にした新規作成」を選択します。
6. 新しいリモート・システム構成の名前を「名前」に入力します。
7. その他の属性のうち、コピー元のリモート・システム構成と違っていなければならないものを指定します。
8. 「OK」をクリックします。

1 注: このタスクに相当する CL コマンドはありません。

1 リモート・システム構成プロパティの表示

1 リモート・システム・ネットワーク・サーバー構成 (NWSCFG サブタイプ RMTSYS) オブジェクトには、iSCSI 接続の統合サーバーの実行に使用する IBM xSeries または BladeCenter サーバーに関する構成情報が含まれています。

1 iSeries ナビゲーターを使用して、リモート・システム構成の属性を表示するには、以下のステップを行います。

1. 「統合サーバー管理」を展開します。
2. 「iSCSI 接続」を展開します。
3. 「リモート・システム」を選択します。
4. 表示されたリストで、リモート・システム構成を右マウス・ボタンでクリックします。
5. 「プロパティ」を選択します。
6. 表示するプロパティに該当するタブをクリックします。
7. 「OK」をクリックし、パネルをクローズします。

1 CL コマンドを使用する場合は、DSPNWSCFG または WRKNWSCFG を参照してください。

1 リモート・システム構成プロパティの変更

1 リモート・システム・ネットワーク・サーバー構成 (NWSCFG サブタイプ RMTSYS) オブジェクトには、iSCSI 接続の統合サーバーの実行に使用する xSeries または IBM BladeCenter サーバーに関する構成情報が含まれています。

1 iSeries ナビゲーターを使用して、リモート・システム構成の属性に変更を加えるには、以下のステップを行います。

1. 「統合サーバー管理」を展開します。

- | 2. 「iSCSI 接続」を展開します。
 - | 3. 「リモート・システム」を選択します。
 - | 4. 表示されたリストで、リモート・システム構成を右マウス・ボタンでクリックします。
 - | 5. 「プロパティ」を選択します。
 - | 6. 変更を加えるプロパティに該当するタブをクリックします。
 - | 7. 「OK」をクリックして、変更内容を保管します。
- | CL コマンドを使用する場合は、CHGNWSCFG または WRKNWSCFG を参照してください。

| リモート・システムの状況の表示

- | xSeries または IBM BladeCenter サーバーのハードウェアの状況を表示できます。これは、たとえば、このハードウェアが iSCSI 接続の統合サーバーで使用できるかどうかを判断するのに役立つ場合があります。
- | iSeries ナビゲーターを使用してリモート・システムの状況を表示するには、以下のステップを行います。
- | 1. 「統合サーバー管理」を展開します。
 - | 2. 「iSCSI 接続」を展開します。
 - | 3. 「リモート・システム」を選択します。
 - | 4. 表示されたリストで、リモート・システム構成を右マウス・ボタンでクリックします。
 - | 5. 「状況」を選択します。
 - | 6. リモート・システム・ハードウェアの状況が表示されます。
 - | 7. 「キャンセル」をクリックし、パネルをクローズします。
- | CL コマンドを使用する場合は、WRKNWSCFG を参照してください。

| リモート・システム構成オブジェクトの削除

- | iSeries ナビゲーターを使用してリモート・システム構成を削除するには、以下のステップを行います。
- | 1. 「統合サーバー管理」を展開します。
 - | 2. 「iSCSI 接続」を展開します。
 - | 3. 「リモート・システム」を選択します。
 - | 4. 表示されたリストで、リモート・システム構成を右マウス・ボタンでクリックします。
 - | 5. 「削除」を選択します。
 - | 6. 確認パネルで「削除」をクリックします。
- | CL コマンドを使用する場合は、DLTNWSCFG または WRKNWSCFG を参照してください。

| サービス・プロセッサ・ネットワーク・サーバー構成の管理

- | 各 iSCSI 接続リモート xSeries または IBM BladeCenter サーバーのサービス・プロセッサまたは管理モジュールの属性を構成するには、サービス・プロセッサ・ネットワーク・サーバー構成 (NWSCFG サブタイプ SRVPRC) オブジェクトを使用します。サービス・プロセッサ構成は、ネットワーク上のサービス・プロセッサまたは管理モジュールを発見して、これに安全に接続するのに使用する属性を定義します。リモート・システム・ネットワーク・サーバー構成オブジェクトには、リモート・システム・ハードウェアの制御に使用される、対応するサービス・プロセッサ構成オブジェクトへの参照が含まれています。詳しくは、46 ページの『サービス・プロセッサ構成』を参照してください。

注: BladeCenter シャーシの中の各 IBM BladeCenter サーバーごとにサービス・プロセッサ構成が必要なわけではありません。必要なサービス・プロセッサ構成は、IBM BladeCenter シャーシに対して 1 つだけです。

サービス・プロセッサ構成オブジェクトに対して以下のタスクを実行できます。

- 『サービス・プロセッサ構成オブジェクトの作成』
- 『別のオブジェクトを基にしてサービス・プロセッサ構成オブジェクトを作成する』
- 137 ページの『サービス・プロセッサ構成プロパティの表示』
- 137 ページの『サービス・プロセッサ構成プロパティの変更』
- 138 ページの『サービス・プロセッサの初期化』
- 138 ページの『サービス・プロセッサ構成オブジェクトの削除』

サービス・プロセッサ構成オブジェクトの作成

iSCSI 接続の統合サーバーの実行に使用する、各 xSeries または IBM BladeCenter のサービス・プロセッサまたは管理モジュールのために、サービス・プロセッサ・ネットワーク・サーバー構成 (NWSCFG サブタイプ SRVPRC) オブジェクトを作成しなければなりません。

注: IBM BladeCenter シャーシの中の各ブレードごとにサービス・プロセッサ構成が必要なわけではありません。必要なサービス・プロセッサ構成は、BladeCenter シャーシに対して 1 つだけです。

iSeries ナビゲーターを使用してサービス・プロセッサ構成を作成するには、以下のステップを行います。

1. 「統合サーバー管理」を展開します。
2. 「iSCSI 接続」を展開します。
3. 「サービス・プロセッサ」を右マウス・ボタンでクリックします。
4. 「新規サービス・プロセッサ構成」を選択します。
5. 「一般」タブで、以下のようになります。
 - 「名前」および「記述」に入力します。
 - 「ホスト名」、「インターネット・アドレス」、または「製造番号」のいずれかを指定して、ネットワーク上のサービス・プロセッサを識別します。
 - 「オブジェクト権限」を選択します。
6. 「セキュリティ」タブで、サービス・プロセッサへの接続時に使用するセキュリティのタイプを定義します。
7. 「OK」をクリックします。

CL コマンドを使用する場合は、CRTNWSCFG または WRKNWSCFG を参照してください。

別のオブジェクトを基にしてサービス・プロセッサ構成オブジェクトを作成する

新しいサービス・プロセッサ・ネットワーク・サーバー構成 (NWSCFG サブタイプ SRVPRC) オブジェクトを作成する際に、既存のオブジェクトをコピーできます。新しいサービス・プロセッサ構成の属性の一部が既存のサービス・プロセッサ構成の属性と同じ場合や似ている場合は、こうすることで時間を節約できます。

iSeries ナビゲーターを使用して、既存のサービス・プロセッサ構成を基にして別の構成を作成するには、以下のステップを行います。

1. 「統合サーバー管理」を展開します。

- | 2. 「iSCSI 接続」を展開します。
- | 3. 「サービス・プロセッサ」を選択します。
- | 4. 表示されたリストで、コピーするサービス・プロセッサ構成を右マウス・ボタンでクリックします。
- | 5. 「既存のものを基にした新規作成」を選択します。
- | 6. 新しいサービス・プロセッサ構成の名前を「名前」に入力します。
- | 7. その他の属性のうち、コピー元のサービス・プロセッサ構成と違っていなければならないものを指定します。
- | 8. 「OK」をクリックします。

| 注: このタスクに相当する CL コマンドはありません。

| サービス・プロセッサ構成プロパティの表示

| サービス・プロセッサ・ネットワーク・サーバー構成 (NWSCFG サブタイプ SRVPRC) オブジェクトには、iSCSI 接続の統合サーバーの実行に使用する xSeries または IBM BladeCenter サーバーのサービス・プロセッサまたは管理モジュールに関する構成情報が含まれています。

| iSeries ナビゲーターを使用して、サービス・プロセッサ構成の属性に変更を加えるには、以下のステップを行います。

- | 1. 「統合サーバー管理」を展開します。
- | 2. 「iSCSI 接続」を展開します。
- | 3. 「サービス・プロセッサ」を選択します。
- | 4. 表示されたリストで、サービス・プロセッサ構成を右マウス・ボタンでクリックします。
- | 5. 「プロパティ」を選択します。
- | 6. 表示するプロパティに該当するタブをクリックします。
- | 7. 「OK」をクリックし、パネルをクローズします。

| CL コマンドを使用する場合は、DSPNWSCFG または WRKNWSCFG を参照してください。

| サービス・プロセッサ構成プロパティの変更

| サービス・プロセッサ・ネットワーク・サーバー構成 (NWSCFG サブタイプ SRVPRC) オブジェクトには、iSCSI 接続の統合サーバーの実行に使用する IBM xSeries または BladeCenter のサービス・プロセッサまたは管理モジュールに関する構成情報が含まれています。

| iSeries ナビゲーターを使用して、サービス・プロセッサ構成の属性に変更を加えるには、以下のステップを行います。

- | 1. 「統合サーバー管理」を展開します。
- | 2. 「iSCSI 接続」を展開します。
- | 3. 「サービス・プロセッサ」を選択します。
- | 4. 表示されたリストで、サービス・プロセッサを右マウス・ボタンでクリックします。
- | 5. 「プロパティ」を選択します。
- | 6. 変更を加えるプロパティに該当するタブをクリックします。
- | 7. 「OK」をクリックして、変更内容を保管します。

| CL コマンドを使用する場合は、CHGNWSCFG または WRKNWSCFG を参照してください。

サービス・プロセッサの初期化

サービス・プロセッサ・ネットワーク・サーバー構成 (NWSCFG サブタイプ SRVPRC) オブジェクトには、iSCSI 接続の統合サーバーの実行に使用する xSeries または IBM BladeCenter のサービス・プロセッサまたは管理モジュールに関する構成情報が含まれています。サービス・プロセッサを統合サーバーと併用できるようにするには、その前にこれを初期化する必要があります。サービス・プロセッサ接続の保護に使用するユーザー、パスワード、および証明書の再生成か同期化を行ったり、サービス・プロセッサへの接続に使用するユーザーまたはパスワードを変更したりすることもできます。

iSeries ナビゲーターを使用してサービス・プロセッサを初期化するには、以下のステップを行います。

1. 「統合サーバー管理」を展開します。
2. 「iSCSI 接続」を展開します。
3. 「サービス・プロセッサ」を選択します。
4. 表示されたリストで、サービス・プロセッサ構成を右マウス・ボタンでクリックします。
5. 「初期化」を選択します。
6. 以下のオプションのうち 1 つを選択します。
 - 「新規サービス・プロセッサの初期化」
 - 「サービス・プロセッサ証明書の再生成」
 - 「サービス・プロセッサからの証明書の同期化」
 - 「サービス・プロセッサ・ユーザー ID およびパスワードの変更」
7. 必要に応じて、「ユーザー」および「パスワード」に入力します。
8. 「初期化」をクリックして、選択したオプションを実行します。

CL コマンドを使用する場合は、INZNWSCFG または WRKNWSCFG を参照してください。

サービス・プロセッサ構成オブジェクトの削除

iSeries ナビゲーターを使用してサービス・プロセッサ構成を削除するには、以下のステップを行います。

1. 「統合サーバー管理」を展開します。
2. 「iSCSI 接続」を展開します。
3. 「サービス・プロセッサ」を選択します。
4. 表示されたリストで、サービス・プロセッサ構成を右マウス・ボタンでクリックします。
5. 「削除」を選択します。
6. 確認パネルで「削除」をクリックします。

CL コマンドを使用する場合は、DLTNWSCFG または WRKNWSCFG を参照してください。

接続セキュリティ・ネットワーク・サーバー構成の管理

iSeries と xSeries または IBM BladeCenter ブレード・サーバーとの間の、iSCSI ネットワークを介した記憶域および仮想イーサネット・データ・フローを保護するために使用する IP セキュリティ (IPSec) ルールを定義するには、接続セキュリティ・ネットワーク・サーバー構成 (NWSCFG サブタイプ CNNSEC) オブジェクトを使用します。詳しくは、49 ページの『接続セキュリティ構成』を参照してください。

注: iSCSI 接続の iSeries 側か xSeries/Center 側のどちらかの iSCSI HBA ハードウェアが IPSec をサポートしていない場合、iSCSI ネットワークを介したデータ・フローを保護するために IPSec を使用する

ことはできません。iSCSI HBA ハードウェアが IPSec をサポートしていない場合でも、接続セキュリティ・オブジェクトを作成する必要があるありますが、IP セキュリティ・ルールは定義しないでください。

接続セキュリティ構成オブジェクトに対して以下のタスクを実行できます。

- 『接続セキュリティ構成オブジェクトの作成』
- 『別のオブジェクトを基にして接続セキュリティ構成オブジェクトを作成する』
- 140 ページの『接続セキュリティ構成プロパティの表示』
- 140 ページの『接続セキュリティ構成プロパティの変更』
- 141 ページの『接続セキュリティ・オブジェクトの削除』

接続セキュリティ構成オブジェクトの作成

iSeries と xSeries または IBM BladeCenter ブレード・サーバーとの間の、iSCSI ネットワークを介した記憶域および仮想イーサネット・データ・フローを保護するために使用する IP セキュリティ (IPSec) ルールを定義するには、接続セキュリティ・ネットワーク・サーバー構成 (NWSCFG サブタイプ CNNSEC) オブジェクトを作成しなければなりません。

注: iSCSI 接続の iSeries 側か、xSeries または IBM BladeCenter 側の iSCSI HBA ハードウェアが IPSec をサポートしていない場合、iSCSI ネットワークを介したデータ・フローを保護するために IPSec を使用することはできません。iSCSI HBA ハードウェアが IPSec をサポートしていない場合でも、接続セキュリティ・オブジェクトを作成する必要があるありますが、IP セキュリティ・ルールは定義しないでください。

iSeries ナビゲーターを使用して接続セキュリティ構成を作成するには、以下のステップを行います。

1. 「統合サーバー管理」を展開します。
2. 「iSCSI 接続」を展開します。
3. 「接続セキュリティ」を右マウス・ボタンでクリックします。
4. 「新規接続セキュリティ構成」を選択します。
5. 「一般」タブで、以下のようになります。
 - 「名前」および「記述」に入力します。
 - 「オブジェクト権限」を選択します。
6. 「IP セキュリティ・ルール」タブで、以下のようになります。
 - iSCSI HBA ハードウェアが IPSec をサポートしている場合は、iSCSI ネットワークを介した記憶域および仮想イーサネット・データ・フローの保護に使用する IP セキュリティ・ルールを定義します。
 - サポートしていない場合は、IP セキュリティ・ルールを定義しないでください。
7. 「OK」をクリックします。

CL コマンドを使用する場合は、CRTNWSCFG または WRKNWSCFG を参照してください。

別のオブジェクトを基にして接続セキュリティ構成オブジェクトを作成する

新しい接続セキュリティ・ネットワーク・サーバー構成 (NWSCFG サブタイプ CNNSEC) オブジェクトを作成する際に、既存のオブジェクトをコピーできます。新しい接続セキュリティ構成の属性の一部が既存の接続セキュリティ構成の属性と同じ場合や似ている場合は、こうすることで時間を節約できます。

1 iSeries ナビゲーターを使用して、既存の接続セキュリティ構成を基にして別の構成を作成するには、以下のステップを行います。

1. 「統合サーバー管理」を展開します。
2. 「iSCSI 接続」を展開します。
3. 「接続セキュリティ」を選択します。
4. 表示されたリストで、コピーする接続セキュリティ構成を右マウス・ボタンでクリックします。
5. 「既存のものを基にした新規作成」を選択します。
6. 新しい接続セキュリティ構成の名前を「名前」に入力します。
7. その他の属性のうち、コピー元の接続セキュリティ構成と違っていなければならないものを指定します。
8. 「OK」をクリックします。

注: このタスクに相当する CL コマンドはありません。

接続セキュリティ構成プロパティの表示

接続セキュリティ・ネットワーク・サーバー構成 (NWSCFG サブタイプ CNNSEC) オブジェクトには、iSeries と xSeries または IBM BladeCenter ブレード・サーバーとの間の、iSCSI ネットワークを介した記憶域および仮想イーサネット・データ・フローの保護に使用される IP セキュリティ (IPSec) ルールが含まれています。

iSeries ナビゲーターを使用して、接続セキュリティ構成の属性を表示するには、以下のステップを行います。

1. 「統合サーバー管理」を展開します。
2. 「iSCSI 接続」を展開します。
3. 「接続セキュリティ」を選択します。
4. 表示されたリストで、接続セキュリティ構成オブジェクトを右マウス・ボタンでクリックします。
5. 「プロパティ」を選択します。
6. 表示するプロパティに該当するタブをクリックします。
7. 「OK」をクリックし、パネルをクローズします。

CL コマンドを使用する場合は、DSPNWSCFG または WRKNWSCFG を参照してください。

接続セキュリティ構成プロパティの変更

接続セキュリティ・ネットワーク・サーバー構成 (NWSCFG サブタイプ CNNSEC) オブジェクトには、iSeries と xSeries または IBM BladeCenter ブレード・サーバーとの間の、iSCSI ネットワークを介した記憶域および仮想イーサネット・データ・フローの保護に使用される IP セキュリティ (IPSec) ルールが含まれています。

注: iSCSI 接続の iSeries 側か xSeries/IBM BladeCenter 側のどちらかの iSCSI HBA ハードウェアが IPSec をサポートしていない場合、iSCSI ネットワークを介したデータ・フローを保護するために IPSec を使用することはできません。iSCSI HBA ハードウェアが IPSec をサポートしていない場合は、IP セキュリティ・ルールを定義しないでください。

iSeries ナビゲーターを使用して、接続セキュリティ構成の属性に変更を加えるには、以下のステップを行います。

1. 「統合サーバー管理」を展開します。

- | 2. 「iSCSI 接続」を展開します。
 - | 3. 「接続セキュリティ」を選択します。
 - | 4. 表示されたリストで、接続セキュリティ構成オブジェクトを右マウス・ボタンでクリックします。
 - | 5. 「プロパティ」を選択します。
 - | 6. 変更を加えるプロパティに該当するタブをクリックします。
 - | 7. 「OK」をクリックして、変更内容を保管します。
- | CL コマンドを使用する場合は、CHGNWSCFG または WRKNWSCFG を参照してください。

| 接続セキュリティ・オブジェクトの削除

- | iSeries ナビゲーターを使用して接続セキュリティ構成を削除するには、以下のステップを行います。
- | 1. 「統合サーバー管理」を展開します。
 - | 2. 「iSCSI 接続」を展開します。
 - | 3. 「接続セキュリティ」を選択します。
 - | 4. 表示されたリストで、接続セキュリティ構成オブジェクトを右マウス・ボタンでクリックします。
 - | 5. 「削除」を選択します。
 - | 6. 確認パネルで「削除」をクリックします。
- | CL コマンドを使用する場合は、DLTNWSCFG または WRKNWSCFG を参照してください。

| i5/OS とホストされるシステムとの間のセキュリティの構成

- | 以下のセキュリティ・アクションのうち、ご使用の環境に該当するものを判別するには、51 ページの『iSCSI 接続システムのセキュリティ』を参照してください。
- | • 『CHAP の構成』
 - | • 142 ページの『IPSec の構成』
 - | • 143 ページの『サービス・プロセッサ SSL の構成』
 - | • 145 ページの『サービス・プロセッサ・パスワード』
 - | • 145 ページの『ファイアウォールの構成』

| CHAP の構成

- | 注: CHAP 情報の作成、変更、または表示には、セキュリティ管理者 (*SECADM) 特殊権限が必要です。
- | CHAP を構成するか、または CHAP 信用証明情報に変更を加えるには、以下のステップを行います。
- | 1. サーバーをシャットダウン (NWS D をオフに変更) し、134 ページの『リモート・システム構成プロパティの変更』で説明されている手順を使用して、サーバーのリモート・システム構成のプロパティに変更を加えます。「CHAP 認証」タブに進みます。
 - | • CHAP を使用可能にするには、「CHAP 認証に次の値を使用」オプションを選択して、「CHAP 名」を指定し、「CHAP 機密事項を一度だけ生成」オプションを選択します。
 - | • CHAP を使用不可にするには、「CHAP を使用しない」オプションを選択します。
 - | 2. 134 ページの『リモート・システム構成プロパティの表示』で説明されている手順を使用して、サーバーのリモート・システム構成のプロパティを表示します。
 - | • 「CHAP 認証」タブで、「CHAP 名」と「CHAP 機密事項」をメモします。

- ・ 「ブート・パラメーター」タブで、ブート・パラメーターの送達方法をメモします。
3. このステップは、ブート・パラメーターの送達方法が「リモート・システムに手動で構成」または「Dynamically delivered to remote system via CHAP (CHAP を介してリモート・システムへ動的に送達)」の場合に必須です。次回のサーバー開始 (NWS D のオンに変更) 時、ホストされるシステムのコンソールに注意し、CTRL-Q を押すようにとのプロンプトが出のを待ちます。プロンプトが表示されたら即時に CTRL-Q を押します。CTRL-Q ユーティリティーで、ホストされる OS をブートするよう構成されているアダプターを選択します。リモート・システム構成プロパティーの CHAP の名前と機密事項を、CTRL-Q ターゲット・セキュリティー構成パネルの CHAP の名前と機密事項のフィールドに入力します。この情報を CTRL-Q イニシエーター構成パネルに入力しないでください。

注: ホストされるシステムの非ブート iSCSI HBA は、i5/OS 構成から自動的に構成されます。

IPSec の構成

注: iSCSI ネットワークを介したデータ・フローを保護するために IPSec を使用するには、IPSec をサポートしている iSeries 用 iSCSI HBA が必要です。iSCSI HBA ハードウェアが IPSec をサポートしていない場合でも、接続セキュリティー・オブジェクトを作成する必要がありますが、IP セキュリティー・ルールは定義しないでください。

IPSec を構成するか、または IPSec 信用証明情報に変更を加えるには、以下のステップを行います。

1. 1 つ目の事前共用キーをまだ生成していない場合、このステップを実行することが必要です。また、いつでもこのステップを実行して事前共用キーを変更することができます。サーバーをシャットダウン (NWS D をオフに変更) し、140 ページの『接続セキュリティー構成プロパティーの変更』で説明されている手順を使用して、サーバーの接続セキュリティー構成のプロパティーに変更を加えます。
 - ・ 「IP セキュリティー・ルール」タブに進みます。
 - ・ 「追加」ボタンをクリックして、「事前共用キーを一度だけ生成」オプションを選択します。
 - ・ 「OK」をクリックして、新しい IP セキュリティー・ルールを表に追加します。次いで再度「OK」をクリックして、接続セキュリティー構成を保管し、事前共用キーが生成されるようにします。

注: 事前共用キーの作成、変更、または表示には、セキュリティー管理者 (*SECADM) 特殊権限が必要です。

2. 140 ページの『接続セキュリティー構成プロパティーの表示』で説明されている手順を使用して、サーバーの接続セキュリティー構成のプロパティーを表示します。
 - ・ 「IP セキュリティー・ルール」タブに進みます。
 - ・ 表値の最初の行をメモします。この行には、i5/OS によって生成されたランダム事前共用キーが含まれます。この情報は、5 (143 ページ) のステップで使用されます。
3. iSeries ナビゲーターを使用して、以下のようにします。
 - ・ 「統合サーバー管理」->「サーバー」を選択します。
 - ・ 統合サーバーを右マウス・ボタンでクリックして、「プロパティー」を選択します。
 - ・ 「iSCSI セキュリティー」タブに進みます。
 - ・ 「デフォルトの IP セキュリティー・ルール」の場合、「1」を選択してから、「OK」をクリックして、変更内容を保管します。これは i5/OS に対して以下の事柄を行うよう指示するということです。すなわち、サーバー・プロパティーの IP セキュリティー・ルールが「デフォルト」値の場合は、必ず接続セキュリティー構成内の最初の値 (サーバー・プロパティーの「iSCSI セキュリティー」タブでサーバーの「接続セキュリティー構成」値として指定されている) を使用する、ということです。

4. このステップを実行する必要があるのは、サーバーの NWSH の接続すべてに対して IPSec を使用可能にするわけではない場合、あるいはサーバー・プロパティのリモート・インターフェース・ルールがデフォルト値から変更されている場合だけです。

iSeries ナビゲーターを使用して、以下のようにします。

- 「統合サーバー管理」->「サーバー」を選択します。
- 統合サーバーを右マウス・ボタンでクリックして、「プロパティ」を選択します。
- 「記憶域パス」タブに進みます。
- 個々の「リモート・インターフェース IP セキュリティ規則」は、iSeries 用 iSCSI HBA ポートとホストされるシステムの iSCSI HBA ポートとで構成される、iSCSI HBA の対に対応しています。

「記憶域パス」および「Virtual Ethernet Paths (仮想イーサネット・パス)」タブのすべての「リモート・インターフェース IP セキュリティ規則」列で以下の作業を繰り返します。

注: ある NWSH が NWSH の中で複数回使用されている場合、この NWSH を参照する記憶域または仮想イーサネット・パスそれぞれの「リモート・インターフェース IP セキュリティ規則」の値のセットは同一でなければなりません。

それぞれの「リモート・インターフェース IP セキュリティ規則」を、「なし」または「デフォルト」のうち、この特定の iSCSI HBA ポートの対を使用する方法に該当する方に設定します。

- iSCSI HBA のいずれかが IPSec をサポートできるかどうかに関係なく、ネットワーク・トラフィックが iSCSI HBA ポート間を自由に流れるようにしたい場合は、「なし」を使用します。
- 対応する iSeries 用 iSCSI HBA が IPSec をサポートしており、暗号化されたトラフィックのみ許可する (つまり、ホストされるシステムの iSCSI HBA ポートが IPSec をサポートしていない場合はトラフィックを許可しない) 場合は、「デフォルト」を使用します。

5. このステップを実行する必要があるのは、リモート・システム構成の送達方法が「リモート・システムに手動で構成」または「Dynamically delivered to remote system via CHAP (CHAP を介してリモート・システムへ動的に送達)」の場合だけです。次回のサーバー開始 (NWSH のオンに変更) 時、ホストされるシステムのコンソールに注意し、CTRL-Q を押すようにとのプロンプトが出るのを待ちます。プロンプトが表示されたら即時に CTRL-Q を押します。CTRL-Q ユーティリティで、ホストされる OS をブートするよう構成されているアダプターを選択します。接続セキュリティ構成のプロパティの事前共用キーを、ターゲットのセキュリティ構成パネルの事前共用キーに入力します。CTRL-Q ユーティリティについて詳しくは、23 ページの『iSCSI を使用したディスクレス・ブート』を参照してください。

注: ホストされるシステムの非ブート iSCSI HBA は、i5/OS 構成から自動的に構成されます。

サービス・プロセッサ SSL の構成

SSL とサービス・プロセッサ・パスワードは、iSeries システムの LAN アダプターとホストされるシステムのサービス・プロセッサとの間のシステム管理トラフィックを保護するためにともに働きます。

以下のどちらかの方式を使用して、サービス・プロセッサ SSL 接続を初期化できます。

- 144 ページの『SSL の自動初期化』
- 144 ページの『SSL の手動初期化』

サービス・プロセッサ・パスワードについて詳しくは、145 ページの『サービス・プロセッサ・パスワード』を参照してください。

SSL の自動初期化

SSL を自動的に初期化するには、以下のステップを行います。

1. サービス・プロセッサと iSeries の間の接続に共用回線網を使用している場合は、一時的にサービス・プロセッサと iSeries とを分離されたネットワークで接続することを考慮してください。さもないと、ステップ 3 で初期化タスクを実行する短い期間中、自動方式の安全性は手動方式に比べて若干劣ることになります。
2. 137 ページの『サービス・プロセッサ構成プロパティの変更』で説明されている手順を使用して、サーバーのサービス・プロセッサ構成のプロパティに変更を加えます。「セキュリティ」タブに進み、「自動的にユーザーをセットアップして証明書を生成」オプションを選択します。「OK」を押して、変更内容を保管します。
3. 138 ページの『サービス・プロセッサの初期化』で説明されている手順を使用して、サービス・プロセッサを初期化します。
 - a. 「新規サービス・プロセッサの初期化」オプションを指定します。


注：別の統合サーバーとともに使用する目的で以前に初期化を済ませたサービス・プロセッサ用に、追加のサービス・プロセッサ構成を行うという場合は、「サービス・プロセッサからの証明書の同期化」オプションを使用してください。

- b. 「ユーザー」および「パスワード」値を指定します。
- c. 「初期化」を押して、操作を実行します。

注：サービス・プロセッサは自己署名証明書を自動的に生成し、この証明書は i5/OS によって保管されます。この証明書は、サービス・プロセッサ構成の名前と一致するファイル名で、統合ファイル・システムのディレクトリー /QIBM/UserData/Director/classes/com/ibm/sysmgmt/app/iide/ に保管されます。このファイルの拡張子は「kdb」になります。

SSL の手動初期化

信頼できる認証局によって署名された証明書を使用して SSL を手動で初期化するには、以下のステップを行います。

1. サービス・プロセッサの Web インターフェースを使用して、信頼できる認証局に SSL 証明書を要求します。詳細な手順については、IBM Remote Supervisor Adapter II SlimLine and Remote Supervisor Adapter II User's Guide  (www.ibm.com/pc/support/site.wss/) を参照してください。「Browse (ブラウズ)」の下で「Servers (サーバー)」を選択し、「Family: (ファミリー:)」に「xSeries 236」、次いで「publications (資料)」を選択します。

注：認証局の証明書が i5/OS *SYSTEM 証明書ストアに入っていないとなりません。

2. 認証局から新しい証明書を受け取ったら、サービス・プロセッサの Web インターフェースを使用して、証明書をサービス・プロセッサにインポートします。
3. 137 ページの『サービス・プロセッサ構成プロパティの変更』で説明されている手順を使用して、サーバーのサービス・プロセッサ構成のプロパティに変更を加えます。「セキュリティ」タブに進み、以下のステップを行います。
 - a. 「手動でユーザーおよび証明書をセットアップ」オプションを選択します。
 - b. 「コンポーネント」オプションでは、「共通名」、「電子メール・アドレス」、または「組織単位」のいずれかを選択します。

- | c. 「比較値」では、新しい証明書の中の対応する情報を指定します。こうすると、SSL がこの証明書を、認証局によって署名された i5/OS *SYSTEM 証明書ストア内の他の証明書と区別できます。例えば、既知の認証局から証明書を受信するのに使用した電子メール・アドレスを指定できます。
- | d. 「OK」を押して、変更内容を保管します。
- | 4. パスワードを変更して、初期化を完了します。『サービス・プロセッサ・パスワード』を参照してください。

| SSL を使用不可にするには、上記の手順を使用しますが、「証明書を使用しない (物理的セキュリティーが必要)」オプションを選択します。

| サービス・プロセッサ・パスワード

- | サービス・プロセッサ・パスワードを変更するには、138 ページの『サービス・プロセッサの初期化』で説明されている手順を使用します。
- | 1. 「サービス・プロセッサ・ユーザー ID およびパスワードの変更」オプションを選択します。
 - | 2. 新しく「ユーザー」、「パスワード」を指定し、「Confirm new password values (新規パスワード値の確認)」を指定します。
 - | 3. 「初期化」を押して、操作を実行します。

| ファイアウォールの構成

| iSeries と iSCSI ネットワークとの間にファイアウォールがある場合は、iSCSI および仮想イーサネットの着信トラフィックが通過できるようにファイアウォールを構成しなければなりません。ファイアウォールの構成に影響する値を以下にリストします。

| ファイアウォールによって保護されている記憶域バスおよび仮想イーサネット接続関連:

- | • **リモート IP アドレス:** 134 ページの『リモート・システム構成プロパティの表示』で説明されている手順を使用して、サーバーのリモート・システム構成のプロパティを表示します。「ネットワーク・インターフェース」タブに進み、「SCSI インターネット・アドレス」および「LAN インターネット・アドレス」の値をメモします。
- | • **ローカル IP アドレスおよび TCP ポート:** 131 ページの『ネットワーク・サーバー・ホスト・アダプターのプロパティの表示』で説明されている手順を使用して、ネットワーク・サーバー・ホスト・アダプター (NWSH) のプロパティを表示します。「ローカル・インターフェース」タブに進み、NWSH で使用されている情報を表示します。以下の値を記録します。
 - | – ローカル SCSI インターフェース: インターネット・アドレス
 - | – ローカル SCSI インターフェース: TCP ポート
 - | – ローカル LAN インターフェース: インターネット・アドレス
 - | – ローカル LAN インターフェース: 基本仮想イーサネット・ポート
 - | – ローカル LAN インターフェース: 上位仮想イーサネット・ポート

| **注:** 仮想イーサネット・トラフィックは UDP パケットの中にカプセル化されます。各仮想イーサネット・アダプターにはそれぞれ自動的に 1 つの UDP ポートが割り当てられます。その範囲は、指定された基本仮想イーサネット・ポート番号から、基本仮想イーサネット・ポート番号と構成済みの仮想イーサネット・アダプター数を加算したものであります。各仮想イーサネット・アダプターには、Windows サーバーで割り当てられた UDP ポートもあります。通常、仮想イーサネットに関する UDP ポートは Windows によって自動的に割り振られます。自動割り振りをオーバーライドするには、Windows コンソールで以下のステップを実行して、UDP ポートを手動で割り振ることができます。

1. 「ネットワーク接続」ウィンドウにナビゲートします。
2. 構成する「**IBM iSeries Virtual Ethernet x (IBM iSeries 仮想イーサネット x)**」アダプターをダブルクリックします。
3. 「プロパティ」をクリックします。
4. 「構成」をクリックします。
5. 「詳細設定」をクリックします。
6. 「**Initiator LAN UDP Port (イニシエーター LAN UDP ポート)**」をクリックします。
7. 仮想イーサネット・アダプターが使用する UDP ポートを入力します。

• **すべてのローカル IP アドレスに関連した TCP ポート:**

iSeries ナビゲーターを使用して、以下のようにします。

1. 「統合サーバー管理」を展開します。
2. 「サーバー」を選択します。
3. 表示されたリストでサーバーを右マウス・ボタンでクリックして、「プロパティ」を選択します。
4. 「システム」タブに進み、「拡張」ボタンをクリックします。
5. 以下の値をメモします。
 - 「シャットダウン TCP ポート」
 - 「仮想イーサネット制御ポート」

IPSec を使用する場合は、iSCSI HBA と iSCSI ネットワークの間のファイアウォールに関する追加の考慮事項があります。

- 「**Allow IPSec: (IPSec の許可:)**」このオプションが使用可能でないファイアウォールもあります。
- ファイアウォールを構成する際に考慮する必要があるのは IP アドレスだけです。TCP ポートと UDP ポートは IPSec によって暗号化されるので、ファイアウォールはこの情報に基づいて稼働できません。

iSCSI ホスト・バス・アダプターの管理

以下のタスクを使用して、iSCSI ホスト・アダプター (NWSH) を管理します。

- 『iSCSI ローカル・ホスト・アダプター間のホット・スペア』
- 147 ページの『iSCSI HBA 使用法の管理』
- 151 ページの『最大伝送単位 (MTU) の考慮事項』
- 153 ページの『統合 DHCP サーバー』

iSCSI ローカル・ホスト・アダプター間のホット・スペア

iSeries iSCSI ローカル・ホスト・アダプター・ハードウェアは、Windows サーバー環境の信頼性および回復可能性を向上させるためのホット・スペア機能を備えています。Windows サーバーが使用している iSCSI ローカル・ホスト・アダプターが故障した場合、迅速かつ容易にサーバーを切り替えて、別の「ホット・スペア」iSCSI ローカル・ホスト・アダプターを使用することができます。さらに、1 つの「スペア」iSCSI ローカル・ホスト・アダプターを使用して複数の実動 iSCSI ローカル・ホスト・アダプターを保護することができるので、柔軟性も向上します。

注: この iSCSI ローカル・ホスト・アダプターのホット・スペア機能は、統合サーバー・ハードウェア用に提供されているホット・スペア機能を補完するものです。詳しくは、172 ページの『サーバー・ハードウェア間のホット・スペア』を参照してください。

1 iSeries ナビゲーターを使用して iSCSI ローカル・ホスト・アダプター・ハードウェアをホット・スペアリングするためには、以下のステップを実行します。

1. 「統合サーバー管理」を展開します。
2. 「iSCSI 接続」を展開します。
3. 「ローカル・ホスト・アダプター」を選択します。
4. ハードウェアを交換したいネットワーク・サーバー・ホスト・アダプター (NWSH) がまだ停止していない場合には、以下のようにします。
 - NWSH を右クリックし、「停止」を選択します。
 - 確認パネルで「停止」をクリックします。
 - 活動状態のサーバーが現在 NWSH を使用している場合は、警告メッセージが表示されます。「続行」をクリックします。
5. ホット・スペア iSCSI ローカル・ホスト・アダプターを指すように NWSH を変更するためには、以下のようにします。
 - NWSH を右クリックし、「プロパティ」を選択します。
 - 「一般」タブを選択し、「ハードウェア・リソース」プロンプトに新しい値を選択します。
 - 「OK」をクリックします。
6. NWSH を開始するには、NWSH を右クリックして「開始」を選択します。

構成変更 (VRYCFG) を使用して、NWSH をオフに変更することもできます。その後、装置記述変更 (NWSH) (CHGDEVNWSH) CL コマンドを使用して資源名 (RSRCNAME) パラメーターの値を変更し、新しいハードウェア・リソース名を指定します。

1 iSCSI HBA 使用法の管理

単一の iSeries iSCSI ホスト・バス・アダプター (iSCSI HBA) を使用して、複数のホストされるシステム (xSeries システムまたは IBM BladeCenter ブレード) を iSeries に接続することができます。さらに、iSeries 用の複数の iSCSI HBA を使用して、ホストされる単一のシステムを iSeries に接続することもできます。さらに、iSeries 用の複数の iSCSI HBA を使用するよう、ホストされるシステムを構成する方法がいくつかあります。これらの技法を組み合わせることもできます。

いくつかの一般的な構成については、以下のセクションを参照してください。

- 『複数のホストされるサーバー間での iSCSI HBA の共用』
- 148 ページの『ワークロードを複数の iSCSI HBA に分散する』
- 149 ページの『冗長性を確保するための複数の iSCSI HBA の使用』
- 150 ページの『iSCSI ネットワークの Windows 側での iSCSI HBA 割り振りの管理』

1 複数のホストされるサーバー間での iSCSI HBA の共用

SCSI および仮想イーサネット LAN のトラフィックに高帯域幅を必要としない複数のサーバーのワークロードを、iSeries 用の単一の iSCSI HBA で処理できる場合があります。ワークロードが軽ければ、たとえば複数の開発およびテスト・サーバーで 1 つの iSeries 用の iSCSI HBA を共用できます。

1 つの iSCSI HBA でサポートできる記憶域および仮想イーサネット・バスの数には限界があります。各アクティブ・サーバー記憶域バスはそれぞれ、iSCSI HBA に対応するネットワーク・サーバー・ホスト・アダプター (NWSH) オブジェクト内のファイル・サーバー・リソースを使用します。同様に、各アクティブ・サーバー仮想イーサネット・バスはそれぞれ、NWSH オブジェクト内の仮想イーサネット・リソース

を使用します。特定の NWSH によりサポートされるファイル・サーバーおよび仮想イーサネットのリソースの数には限界があるため、NWSH を使用できるアクティブ・サーバーの数も制限されます。

iSeries ナビゲーターを使用して NWSH ファイル・サーバーおよび仮想イーサネットのリソースの限界を調べるには、以下のステップを実行します。

1. 「統合サーバー管理」を展開します。
 2. 「iSCSI 接続」を展開します。
 3. 「ローカル・ホスト・アダプター」を選択します。
 4. 表示されたリストで NWSH を右クリックします。
 5. 「プロパティ」を選択します。
 6. 「リソース使用」タブをクリックします。
 7. 現在 NWSH を使用しているアクティブ・サーバー、およびそれらが現在使用しているファイル・サーバーおよび仮想イーサネットのリソースが表に表示されます。表の下には、非アクティブ・サーバーのためにまだ使用可能なファイル・サーバーおよび仮想イーサネットのリソース数、および NWSH がサポートするファイル・サーバーおよび仮想イーサネットのリソースの総数が表示されます。
 8. NWSH プロパティ・パネルで「キャンセル」をクリックしてパネルをクローズします。
- CL コマンドを使用する場合は、WRKDEVD または DSPDEVD コマンドを参照してください。

iSCSI HBA がサポートできるサーバーの数には、あまり明確ではない実際上の限界もあります。実際上の限界は、使用可能な iSCSI HBA の帯域幅と、iSCSI HBA によって実行されるワークロードによって決まります。上述のファイル・サーバーおよび仮想イーサネットのリソースの限界に達する前に、おそらく実際上の限界により、iSCSI HBA がサポートできるホストされるシステムの数も制限されてしまいます。実際上の限界は、ご使用の特定のサーバー構成およびワークロードにより異なります。

ワークロードを複数の iSCSI HBA に分散する

高帯域幅が必要なサーバーでは、ワークロードを処理するために iSeries 用の複数の iSCSI HBA が必要になる場合があります。仮想ディスクおよび仮想イーサネット LAN のうち、高帯域幅を必要とするものものとを識別することにより、これをさらにセグメント化できます。たとえば、ある iSCSI HBA を高帯域幅が必要なディスク専用にし、別の iSCSI HBA を高帯域幅が不要なディスクまたは他のサーバー間で共用することができます。

サーバーの SCSI および仮想イーサネットのワークロードを複数の iSCSI HBA に分散する方法に従って、複数の記憶域または仮想イーサネット・パスがネットワーク・サーバー記述 (NWSH) に定義され、それぞれのパスをどの仮想ディスクおよびどの仮想イーサネットが使用するかが割り当てられることとなります。

iSeries ナビゲーターを使用して追加の記憶域パスを定義するには、まずサーバーをシャットダウンし (163 ページの『統合サーバーの開始と停止』を参照)、次に以下のステップに従います。

1. 「統合サーバー管理」を展開します。
2. 「サーバー」を展開します。
3. 表示されたリストからサーバーを右クリックします。
4. 「プロパティ」を選択します。
5. 「記憶域パス」タブをクリックします。
6. 「追加」ボタンをクリックして、新しい記憶域パスを定義します。

7. 記憶域パスとして使用したい iSCSI HBA に対応するネットワーク・サーバー・ホスト・アダプター (NWSH) を選択します。
8. 「OK」をクリックして、記憶域パスをサーバー・プロパティ・パネルに追加します。
9. 新しいパスに割り当てられるパス番号をメモしておきます。パス番号は、後でディスクをリンクするときこのパスを識別するために使用されます。
10. サーバー・プロパティ・パネルで「OK」をクリックして、NWSH に新しい記憶域パスを保管します。

CL コマンドを使用する場合は、CHGNWSD コマンドの STGPTH キーワードを参照してください。

新しい記憶域パスを定義したので、次に、新しい記憶域パスを使用するために、サーバーの 1 つ以上の仮想ディスクを再リンクする必要があります。まず、ディスクをリンク解除します (186 ページの『統合 Windows サーバー・ディスク・ドライブのリンク解除』を参照)。次に、上述の手順で追加された新しい記憶域パス番号を使用して、ディスクをサーバーに再度リンクします (182 ページの『ディスク・ドライブと統合サーバーのリンク』を参照)。

iSeries ナビゲーターを使用して追加の仮想イーサネット・パスを定義するには、まずサーバーをシャットダウンし (163 ページの『統合サーバーの開始と停止』を参照)、次に以下のステップに従います。

1. 「統合サーバー管理」を展開します。
2. 「サーバー」を展開します。
3. 表示されたリストからサーバーを右クリックします。
4. 「プロパティ」を選択します。
5. 「仮想イーサネット (Virtual Ethernet)」タブをクリックします。
6. 新しいパスを使用する仮想イーサネット・ポートを選択し、「プロパティ」ボタンをクリックします。
7. 仮想イーサネット・ポートで使用する NWSH を選択します。
8. 「OK」をクリックして、サーバー・プロパティ・パネルの仮想イーサネット・ポート情報を更新します。ポートの仮想イーサネット・パスも自動的に更新されます。
9. サーバー・プロパティ・パネルで「OK」をクリックして、NWSH の変更を保管します。

CL コマンドを使用する場合は、CHGNWSD コマンドの VRTETHPTH キーワードを参照してください。

冗長性を確保するための複数の iSCSI HBA の使用

サーバーの帯域幅の要件上は iSeries 用の iSCSI HBA が複数必要ない場合でも、フォールト・トレランスおよび冗長性を確保するために複数の iSCSI HBA を使用したいと思うかもしれません。これにより、ホストされるシステムへ iSeries を接続する iSCSI HBA またはネットワーク・コンポーネントの 1 つ (スイッチ、ケーブルなど) の障害が原因でサーバー障害の発生する可能性が減少します。冗長性は、マルチパス I/O が可能という iSCSI の機能によって提供されます (22 ページの『拡張 iSCSI サポート』を参照)。マルチパス I/O を活用するためには、複数の iSCSI HBA を識別するマルチパス・グループを作成します。その後、どの仮想ディスクがマルチパス・グループを使用するかを定義します。任意指定で、マルチパス・グループを、ディスク・ドライブをリンクするときのデフォルト・パスとして使用することができます。

iSeries ナビゲーターを使用してマルチパス・グループを定義するには、まずサーバーをシャットダウンし (163 ページの『統合サーバーの開始と停止』を参照)、次に以下のステップに従います。

1. 「統合サーバー管理」を展開します。
2. 「サーバー」を展開します。

- 1 3. 表示されたリストからサーバーを右クリックします。
 - 1 4. 「プロパティ」を選択します。
 - 1 5. 「記憶域パス」タブをクリックします。
 - 1 6. 少なくとも 2 つの記憶域パスを定義します (必要ならば「追加」ボタンを使用します)。
 - 1 7. 記憶域パス・テーブルの下で、マルチパス・グループの「プロパティ」ボタンをクリックします。
 - 1 8. チェック・ボックスを使用して、複数の定義済み記憶域パスをマルチパス・グループのメンバーとして示します。
 - 1 9. 「OK」をクリックして、サーバー・プロパティ・パネルのマルチパス・グループ情報を更新します。
 - 1 10. オプション: マルチパス・グループを、ディスク・ドライブのデフォルト・パスとして選択します。
 - 1 11. サーバー・プロパティ・パネルで「OK」をクリックして、NWS D の変更を保管します。
- 1 CL コマンドを使用する場合は、CHGNWSD コマンドの MLTPHGRP および DFTSTGPTH キーワードを参照してください。

1 マルチパス・グループを定義したので、次に、マルチパス・グループを使用するために、サーバーの 1 つ
1 以上の仮想ディスクを再リンクする必要があります。まず、ディスクをリンク解除します (186 ページの
1 『統合 Windows サーバー・ディスク・ドライブのリンク解除』を参照)。その後、マルチパス・グループ
1 を明示的に指定するか、デフォルト・パスを指定 (ディスク・ドライブのデフォルト・パスがマルチパス・
1 グループを使用するように定義されている場合) するかのいずれかを行って、ディスクを再度サーバーにリ
1 ンクします (182 ページの『ディスク・ドライブと統合サーバーのリンク』を参照)。

1 iSCSI ネットワークの Windows 側での iSCSI HBA 割り振りの管理

1 Windows サーバーは、複数の物理 iSCSI HBA ポートを持つ場合があります。1 つの iSCSI HBA ポート
1 は、iSeries 記憶域パス、あるいは仮想イーサネット・ネットワーク、またはその両方のトラフィックを搬
1 送する可能性があります。Windows サーバー上の各 iSCSI HBA ポートを流れるトラフィックの性質は、
1 いくつかの要因に影響されます。

1 IP アドレス

1 iSCSI HBA ポートは、SCSI IP アドレスまたは LAN IP アドレス、またはその両方をもつ場合がありま
1 す。SCSI IP アドレスを持つポートは、記憶域トラフィック搬送の候補となります。LAN IP アドレスを
1 持つポートは、仮想イーサネット・トラフィック搬送の候補となります。

1 ブート記憶域構成

1 Windows をブートするために使用される iSCSI HBA ポートを、CTRL-Q ユーティリティで選択しま
1 す。Windows がブートされた後も、選択された iSCSI HBA ポートは、システム・ドライブに対応する
1 iSeries 記憶域パスへの接続を継続して提供します。

1 仮想イーサネットおよび非ブート記憶域パスへの iSCSI HBA ポートの自動割り振り

1 iSeries Windows 環境には、サーバー構成情報の入った i5/OS オブジェクトを自動的に読み取る、Windows
1 で実行されるプログラムが含まれます。iSeries 用の iSCSI HBA は i5/OS オブジェクトの中で構成され
1 ますが、ホストされるシステム用の iSCSI HBA ポートはそうではありません。代わりに、プログラムが
1 iSCSI HBA ポートを仮想イーサネットおよび非ブート記憶域パスへ自動的に割り振ります。

1 物理 iSCSI HBA ポートへの仮想イーサネット・アダプターの手動割り振り

- | 自動割り振りをオーバーライドするには、Windows コンソールで以下のステップを実行して、iSCSI HBA
- | ポートを手動で割り振ることができます。
- | 1. 「ネットワーク接続」ウィンドウにナビゲートします。
- | 2. 構成する「IBM iSeries Virtual Ethernet x (IBM iSeries 仮想イーサネット x)」アダプターをダブルク
- | リックします。
- | 3. 「プロパティ」をクリックします。
- | 4. 「構成」をクリックします。
- | 5. 「詳細設定」をクリックします。
- | 6. 「Initiator LAN IP Address」をクリックします。
- | 7. 仮想イーサネット・アダプターがその物理接続用に使用する iSCSI HBA ポートの IP アドレスを
- | Windows で入力します。

| 最大伝送単位 (MTU) の考慮事項

| 注: ここで説明されているフレーム・サイズには、イーサネットの 14 バイトの MAC ヘッダーは含まれ

| ません。

| IXS および IXA 接続のサーバーで提供される 9000 バイトのジャンボ・フレームとは対照的に、iSCSI ネットワークにより接続されたシステムの仮想イーサネットのデフォルトは、標準的な 1500 バイトのイーサネット・フレームで伝送できるより小さなフレーム・サイズになります。

| iSCSI ネットワークがより大きなフレーム・サイズに対応している場合には、仮想イーサネットがより大きなサイズ (最大で 9000 バイト) を使用するように構成できます。これにより、パフォーマンスは向上します。複雑な iSCSI ネットワークの場合、ネットワーク・トポロジーおよび関係する装置に応じて、複数の最大フレーム・サイズが混在する可能性があります。

| 注: Windows サーバー導入 (INSWNTSVR) コマンドの MTU プロンプトは、IXS で使用される外部 LAN アダプター以外では効果がありません。

| MTU 構成については、以下のトピックを参照してください。

- | • 『1500 バイトを超えるフレームをサポートする iSCSI ネットワークで最高のパフォーマンスを得るための仮想イーサネットの構成』
- | • 152 ページの『最大フレーム・サイズが 1500 バイト未満の iSCSI ネットワーク用仮想イーサネットの構成』
- | • 152 ページの『MTU をネゴシエーションしない、通常と異なる非 TCP アプリケーションをサポートするよう仮想イーサネットを構成する』

| 1500 バイトを超えるフレームをサポートする iSCSI ネットワークで最高のパフォーマンスを得るための仮想イーサネットの構成

| Windows コンソールで、以下のステップを実行します。

- | 1. 「ネットワーク接続」ウィンドウにナビゲートします。
- | 2. 1500 バイトを超えるフレームをサポートする iSCSI ネットワークに接続されている iSCSI アダプターをダブルクリックします。
- | 3. 「プロパティ」をクリックします。
- | 4. 「構成」をクリックします。
- | 5. 「詳細設定」をクリックします。

6. 「Ethernet Frame Size」をクリックします。
7. iSCSI ネットワークの最大フレーム・サイズを超えない範囲で可能なかぎり大きな値を選択します。

注: 以下に挙げる関連した構成項目は、デフォルト値のままにしておく必要があります。

- Windows 仮想イーサネット・アダプターでは、「Maximum Frame Size」のデフォルトは「自動」です。「自動」にすると、使用される iSCSI HBA ポートの「Ethernet Frame Size」を基にして仮想イーサネットが最大フレーム・サイズを計算します。iSCSI HBA ポートの使用法については、150 ページの『iSCSI ネットワークの Windows 側での iSCSI HBA 割り振りの管理』を参照してください。
- i5/OS 仮想イーサネット回線記述では、「最大フレーム・サイズ (MAXFRAME)」のデフォルトは 8996 です。
- 仮想イーサネット用 i5/OS TCP/IP インターフェースでは、「最大伝送単位 (MTU)」のデフォルトは *LIND です。

最大フレーム・サイズが 1500 バイト未満の iSCSI ネットワーク用仮想イーサネットの構成

Windows コンソールで、以下のステップを実行します。

1. 「ネットワーク接続」ウィンドウにナビゲートします。
2. 最大フレーム・サイズが 1500 バイト未満の iSCSI ネットワークに接続される iSCSI HBA を使用する「IBM iSeries Virtual Ethernet x (IBM iSeries 仮想イーサネット x)」アダプターをダブルクリックします。
3. 「プロパティ」をクリックします。
4. 「構成」をクリックします。
5. 「詳細設定」をクリックします。
6. 「最大フレーム・サイズ」をクリックします。
7. iSCSI ネットワークの最大フレーム・サイズを超えない範囲で可能なかぎり大きな値を選択します。

MTU をネゴシエーションしない、通常と異なる非 TCP アプリケーションをサポートするよう仮想イーサネットを構成する

注: MTU をネゴシエーションする通常のアプリケーションへの影響を回避するため、この手順を実行する前に、MTU をネゴシエーションしないアプリケーションのための別個の仮想イーサネット・ネットワークまたは別個の IP アドレスを定義しておくこともできます。

1. 以下のいずれかを実行してください。
 - a. Windows のすべてのエンドポイントで、最大フレーム・サイズが 1500 バイト以上の iSCSI ネットワークを使用する場合は、Windows のすべてのエンドポイントで iSCSI HBA の「Ethernet frame size」を、iSCSI ネットワークの最も制約の大きな最大フレーム・サイズを超えない範囲で可能なかぎり大きな値に構成します。
 - b. Windows のいずれかのエンドポイントで、最大フレーム・サイズが 1500 バイト未満の iSCSI ネットワークを使用する場合は、Windows のすべてのエンドポイントで仮想イーサネットの「Maximum frame size」を、iSCSI ネットワークの最も制約の大きな最大フレーム・サイズを超えない範囲で可能なかぎり大きな値に構成します。
2. 他のエンドポイントでは、Windows iSCSI HBA の「Ethernet frame size」と仮想イーサネットの「Maximum frame size」のうち、いずれか小さい方から 116 を引いて決定される値に MTU を設定します。i5/OS のエンドポイントの場合、以下の手順を実行してこれを行います。

- a. iSeries ナビゲーターを使用して、「ネットワーク」→「TCP/IP 構成」→「IPv4」→「インターフェイス」を展開します。
- b. 該当する IP アドレスおよび回線記述名を持つインターフェイスを右クリックし、「プロパティ」を選択します。
- c. 「詳細設定」タブで、計算値を「最大伝送単位」フィールドに入力し、「OK」をクリックして変更を保管します。

注: コマンド行インターフェイスを使用する場合、CFGTCP を使用してオプション 1、「TCP/IP インターフェイスの処理」を選択します。


統合 DHCP サーバー

iSeries iSCSI 接続のサーバー・ソリューションでは、統合 DHCP サーバーが提供されています。i5/OS リモート・システム構成オブジェクトに「DHCP を介してリモート・システムへ動的に送達」オプションが指定されており、ホストされるサーバーの iSCSI HBA に AUTO または DHCP モードが指定されている場合、このサーバーが、ホストされるシステムの iSCSI HBA にブート・パラメーターをデプロイするために使用されます。

統合 DHCP サーバーは、汎用サーバーではありません。これは、ホストされるサーバーの iSCSI HBA にブート・パラメーターをデプロイすることだけを目的としたものです。このサーバーは、ネットワーク・サーバー記述 (NWS D) がオンに変更される時、リモート・システム構成で規定されるパラメーターで自動的に構成されます。

DHCP サーバーは、ホストされるサーバーの iSCSI HBA DHCP クライアントのみに応答します。iSCSI HBA DHCP クライアントのすべての要求では、IBM の定義したベンダー ID が使用されます。サーバーは、デフォルトのベンダー ID を使用する要求に応答するようにプログラムされています。DHCP サーバーは、ネットワーク内の他の装置からの要求をすべて無視します。

ホストされるサーバーの iSCSI HBA の MAC アドレスをリモート・システム構成オブジェクトで指定することは非常に重要です。統合 DHCP サーバーは、ブート・パラメーターを正しくデプロイするために、上述のベンダー ID に加えて MAC アドレスを使用します。MAC アドレスは、パラメーターを正しくデプロイするために必要な特定のスコープの一部です。

ベンダー ID および MAC アドレスにより規定されたスコープは変更できます。上級の、技術力に富むユーザーがこの設定値を必要に応じてより具体的に構成することを可能にする機能が、拡張機能として備えられています。デフォルトのベンダー ID を他の値に構成することができます。構成画面は、ホストされるサーバーの iSCSI HBA アダプターの CTRL-Q セットアップ・ユーティリティーおよびそれに対応するリモート・システム構成オブジェクトから使用可能です。この拡張機能は、RFC 2132 仕様に準拠しています。拡張構成の詳細については、iSCSI インストールの最初にお読みください (英語)  を参照してください。

統合 DHCP サーバーが着信 DHCP 要求を受け取り、必要なすべてのスコープが一致する場合、統合 DHCP サーバーは、DHCP クライアントにブート・ターゲット装置の IP アドレスを提供します。ブート・ターゲット装置は、ブート仮想ディスクが構成されているネットワーク・サーバー・ホスト・アダプター (NWS H) です。サーバーは、イニシエーターまたは DHCP クライアントの IP アドレスも提供します。イニシエーターは、iSCSI を介したブートに使用される、ホストされるサーバーの iSCSI HBA です。

さらに統合 DHCP サーバーは、ホストされるシステムの iSCSI HBA へのターゲットおよびイニシエーター装置を表す、グローバルに固有の iSCSI 修飾名 (IQN) を提供します。

IP アドレスと IQN のこれらのセットは両方とも、ホストされるサーバーを定義するために使用される iSeries 構成オブジェクトの中にあります。ターゲット IP アドレスは、NWSH オブジェクトで定義されます。イニシエーター IP アドレスおよびイニシエーター IQN は、リモート・システム構成オブジェクトで定義されます。ターゲット IQN は、NWSH オブジェクトで自動的に構成および定義されます。これらのオブジェクトについての詳細は、46 ページの『ネットワーク・サーバー記述』を参照してください。

統合 DHCP サーバーは、ホット・スペアをインプリメントするときのかぎを握る不可欠な構成要素です。DHCP ブート・モードは、iSeries ソフトウェア・オブジェクトで定義される必須パラメーターの自動デプロイメントを使用可能にします。こうして、ブート・パラメーター (IP アドレスおよび IQN) の変更の際にサーバーを手動で構成する必要がなくなります。

リモート・サーバーのディスカバリーおよび管理

IBM Director、および i5/OS リモート・システム構成オブジェクトおよびサービス・プロセッサ構成オブジェクトの情報は、接続されるサーバーを見つけて管理するために使用されます。以下の情報を参照してください。

- 『IBM Director のインストールおよび構成』
- 155 ページの『リモート・サーバーおよびサービス・プロセッサのディスカバリー』
 - 155 ページの『サービス・プロセッサのディスカバリー構成』
 - 157 ページの『動的 IP アドレッシング (DHCP)』
 - 157 ページの『サービス・プロセッサのディスカバリー方式』
- 160 ページの『管理モジュールまたは RSA II の Web インターフェースの使用』

IBM Director のインストールおよび構成

IBM Director は、リモート・サーバーのディスカバリーおよび iSCSI 接続のサーバーの管理のために使用されます。IBM Director をインストールして起動するとき以外には、IBM Director インターフェースを使用する必要はありません。IBM Director のインストールについては、64 ページの『ソフトウェア要件』を参照してください。

iSeries Windows 環境では、以下の目的で IBM Director を使用します。

- リモート・サーバーおよびサービス・プロセッサのディスカバリー
ネットワーク上のサーバーの検出します。
- 電源制御
サーバーの電源オン、または該当する i5/OS の構成変更コマンド用のオペレーティング・システムのシャットダウンの実行を行います。
- 電源状況の取得
- リモート・サーバーの構成
リモート・サーバー機能の一部は、リモート・サーバーのサービス・プロセッサを介して iSeries からリモート側で構成できます。

IBM Director は TCP/IP に依存します。IBM Director を機能させるには TCP/IP を開始する必要があります。IBM Director は i5/OS TCP サーバーであるため、TCP が開始する時に自動始動するように構成することができます。IBM Director TCP サーバーを自動的に始動するように構成することをお勧めします。そうすることにより、iSeries 用の iSCSI HBA が必要とするときに、IBM Director が確実に使用可能であるようにできます。

1 TCP/IP が開始する時に IBM Director TCP サーバーが自動的に始動するように構成するには、iSeries ナビゲーターを使用して以下のステップを実行します。

1. 「ネットワーク」->「サーバー」->「ユーザー定義」を選択します。
2. 「IBM DIRECTOR」を右クリックして「プロパティ」を選択します。
3. 「TCP/IP の開始時に開始」オプションを選択します。
4. 「OK」をクリックします。

1 TCP/IP サーバー変更 (CHGTCPSVR) コマンドを使用することもできます。

1 IBM Director が自動的に始動しない場合は、以下のように iSeries ナビゲーターを使用して IBM Director TCP サーバーを始動します。

1. 「ネットワーク」->「サーバー」->「ユーザー定義」を選択します。
2. 「IBM DIRECTOR」を右クリックして「開始」を選択します。

1 注: IBM Director サーバーが始動するまでには数分以上かかります。iSeries ナビゲーターのリストを最新表示することにより、開始プロセスの状況を表示することができます。最終的に、IBM DIRECTOR サーバーは「開始済み」の状況を表示します。

1 リモート・サーバーおよびサービス・プロセッサのディスカバリー

1 i5/OS は IBM Director を使用してリモート・サーバーのサービス・プロセッサと通信することにより、ローカル・エリア・ネットワーク (LAN) 上のリモート・サーバーを見つけ、識別します。リモート・システムは、iSeries サーバー上のリモート・システム構成オブジェクトおよびサービス・プロセッサ構成オブジェクトに保管されている情報により識別されます。

1 これは、iSeries iSCSI ターゲット・アダプターと、リモート・サーバーの iSCSI イニシエーター・アダプターとの間の接続とは異なる接続です。リモート・サーバーのサービス・プロセッサ用の LAN アダプターは、iSeries サーバーの LAN アダプターから到達できるネットワークに接続される必要があります。

1 i5/OS オブジェクトとサービス・プロセッサの両方を構成する必要があります。i5/OS ネットワーク・サーバー構成オブジェクトで、使用するディスカバリー方式を構成できます。

1 以下の情報を参照してください。

- 1 • 『サービス・プロセッサのディスカバリー構成』
- 1 • 157 ページの『動的 IP アドレッシング (DHCP)』
- 1 • 157 ページの『サービス・プロセッサのディスカバリー方式』
- 1 • 160 ページの『管理モジュールまたは RSA II の Web インターフェースの使用』

1 サービス・プロセッサのディスカバリー構成

1 サービス・プロセッサの IP 情報は、i5/OS 構成と一致するように構成する必要があります。構成オプションは、サービス・プロセッサのタイプに依存します。ご使用の xSeries サーバーのサービス・プロセッサのタイプの識別については、iSCSI でサポートされる xSeries および BladeCenter のモデル (英語)





1 (www.ibm.com/servers/eserver/iseries/integratedxseries/iscsiservermodels/) を参照してください。

1 ベースボード管理コントローラー (BMC)

1 BMC サービス・プロセッサは、一部の xSeries モデルで使用できます。


- | • BMC を構成するためには、システム BIOS セットアップ・メニューを使用します。
- | • BMC は、静的 IP アドレッシングをサポートします。
- | • BMC は、IP アドレスによるディスカバリーをサポートします。159 ページの『IP アドレスによるディスカバリー』を参照してください。
- | • BMC は、パスワードを使用するセキュリティーをサポートします。145 ページの『サービス・プロセッサ・パスワード』を参照してください。

| リモート監視プログラム・アダプター II (RSA II)

- | RSA II サービス・プロセッサは、一部の xSeries モデルで使用できます。
- | • RSA II を構成するには、以下のいずれかを実行してください。
 - | – システム BIOS セットアップ・メニューを使用します。この方法は、ホスト名を構成するためには使用できません。
 - | – 160 ページの『管理モジュールまたは RSA II の Web インターフェースの使用』を参照してください。
- | • RSA II は以下のいずれかの方法を使用して IP アドレス情報を取得できます。ご使用のネットワークに最適の方法を使用してください。
 - | – 157 ページの『動的 IP アドレッシング (DHCP)』。これは出荷時のデフォルト値です。
 - | – 静的 IP アドレッシング。
- | • RSA II は、以下のディスカバリー方式をサポートします。ご使用のネットワークに最適の方法を使用してください。
 - | – 158 ページの『マルチキャスト・アドレッシングを使用する Service Location Protocol (SLP)』。
 - | – 159 ページの『IP アドレスによるディスカバリー』。
 - | – 159 ページの『ホスト名によるディスカバリー』。
- | • RSA II は、以下のセキュリティー方式をサポートします。
 - | – パスワード。構成手順については、145 ページの『サービス・プロセッサ・パスワード』を参照してください。
 - | – SSL とパスワード。143 ページの『サービス・プロセッサ SSL の構成』を参照してください。
- | • RSA II についての詳細は、以下の情報を参照してください。
 - | – 「IBM リモート監視プログラム・アダプター II SlimLine およびリモート監視プログラム・アダプター II のインストール・ガイド - サーバー (英語)」  (www.ibm.com/pc/support/site.wss/)。「Browse (ブラウズ)」の下で「Servers (サーバー)」を選択し、「Family: (ファミリー)」に「xSeries 236」、「Type: (タイプ:)」に「All Types (すべてのタイプ)」を選択し、「Continue (続行)」を選択します。「Publications (資料)」を選択します。
 - | – 「IBM リモート監視プログラム・アダプター II SlimLine およびリモート監視プログラム・アダプター II のユーザーズ・ガイド - サーバー(英語)」  (www.ibm.com/pc/support/site.wss/)。「Browse (ブラウズ)」の下で「Servers (サーバー)」を選択し、「Family: (ファミリー)」に「xSeries 236」、「Type: (タイプ:)」に「All Types (すべてのタイプ)」を選択し、「Continue (続行)」を選択します。「Publications (資料)」を選択します。

| 管理モジュール

- | 管理モジュールは、IBM BladeCenter サーバーから使用できます。

- | • 管理モジュールを構成するには、160 ページの『管理モジュールまたは RSA II の Web インターフェースの使用』を参照してください。
- | • 管理モジュールは以下のいずれかの方法を使用して IP アドレス情報を取得できます。ご使用のネットワークに最適の方法を使用してください。
 - | – 『動的 IP アドレッシング (DHCP)』。これは出荷時のデフォルト値です。
 - | – 静的 IP アドレス情報。
- | • 管理モジュールは、以下のディスカバリー方式をサポートします。ご使用のネットワークに最適の方法を使用してください。
 - | – 158 ページの『マルチキャスト・アドレッシングを使用する Service Location Protocol (SLP)』
 - | – 159 ページの『IP アドレスによるディスカバリー』。
 - | – 159 ページの『ホスト名によるディスカバリー』
- | • IBM BladeCenter サーバーには、ディスカバリーに関する付加的な考慮事項があります。リモート・システム構成のリモート・システム ID は常に、IBM BladeCenter サーバーのシリアル番号に設定する必要があります。シリアル番号はサーバーのラベルに記載されています。リモート・システム構成の変更については、134 ページの『リモート・システム構成プロパティの変更』を参照してください。サービス・プロセッサ構成の格納装置 ID は、ブレードごとに IBM BladeCenter 格納装置 (シャーンシ) シリアル番号に設定することができます。IBM BladeCenter の管理モジュール・サービス・プロセッサがディスカバリーされなければ、サーバー・ブレードをディスカバリーすることはできません。サービス・プロセッサ構成のパラメーターで、管理モジュールのディスカバリーの方式が決定されます。これらのプロパティの変更については、137 ページの『サービス・プロセッサ構成プロパティの変更』を参照してください。管理モジュールがディスカバリーされた後、IBM Director は、格納装置内のサーバー・ブレードについての情報を収集します。個々のサーバー・ブレードをディスカバリーするという 2 番目のディスカバリー・フェーズを実行する際は、リモート・システムのリモート・システム ID が使用されます。
- | • 管理モジュールは、以下のセキュリティー方式をサポートします。
 - | – パスワード。詳しくは、145 ページの『サービス・プロセッサ・パスワード』を参照してください。
 - | – SSL とパスワード。143 ページの『サービス・プロセッサ SSL の構成』を参照してください。
- | • IBM eServer BladeCenter のシステム管理については、「IBM BladeCenter Systems Management」
Redpaper 
(www.redbooks.ibm.com/abstracts/redp3582.html) を参照してください。

| 動的 IP アドレッシング (DHCP)

- | DHCP を使用するサービス・プロセッサは、サーバーの電源がオンになると即時に初期化され、DHCP プロセスを開始します。DHCP でアドレスを取得できない場合、サービス・プロセッサはデフォルトの静的 IP アドレスである 192.168.70.125 を使用します。

| 注: サービス・プロセッサが DHCP での IP アドレスの取得に失敗した場合、電源をオフにして電源を再投入しないとプロセスを再開できません。

| サービス・プロセッサのディスカバリー方式

- | サービス・プロセッサのディスカバリーの方式はいくつかあります。
 - | • 158 ページの『マルチキャスト・アドレッシングを使用する Service Location Protocol (SLP)』
 - | • 159 ページの『IP アドレスによるディスカバリー』

159 ページの『ホスト名によるディスカバリー』

マルチキャスト・アドレッシングを使用する Service Location Protocol (SLP): ネットワークでサーバーのディスカバリーをするためにサービス・プロセッサのホスト名または IP アドレスを使用しない場合には、Service Location Protocol (SLP) でのマルチキャスト・アドレッシングが使用されます。SLP ディスカバリーを構成するには、iSeries サーバーを構成する必要があります。以下のステップを実行してください。

1. 137 ページの『サービス・プロセッサ構成プロパティの変更』で説明されている手順を使用して以下のようにします。
 - a. 「リモート・システムの格納装置識別を判別するためにサービス・プロセッサ接続を使用」オプションが選択されていないことを確認します。
 - b. 「シリアル番号」フィールドで、スタンドアロン・サーバー格納装置または IBM BladeCenter シャーシのシリアル番号を指定します。
2. 134 ページの『リモート・システム構成プロパティの変更』で説明されている手順を使用して、以下のようにリモート・システム ID が正しく設定されていることを確認します。
 - a. スタンドアロン・サーバーの場合、「サービス・プロセッサ構成からの格納装置識別を使用」オプションを選択します。
 - b. IBM BladeCenter ブレードの場合、「次の値を使用」オプションを選択し、ブレードのシリアル番号を指定します。

サービス・プロセッサは、マルチキャスト・アドレッシングを使用してネットワークに発信される SLP パケットで、自分自身について通知します。このパケットには、リモート・サーバーのシリアル番号、タイプ、モデルなどの属性が含まれています。IBM Director はこのパケットを受信し、サーバーについての情報を保管します。サービス・プロセッサ構成の格納装置 ID またはリモート・システム構成のリモート・システム ID から取得したシリアル番号は、SLP ディスカバリー・プロセスで確認した属性にマップされ、固有のリモート・サーバーを識別します。

利点:

- リモート・サーバーのディスカバリーに必要なのは、サーバーのラベルから入手できるシリアル番号だけです。
- サービス・プロセッサがその IP アドレスを DHCP サーバーから取得し、ネットワークが IP マルチキャストをサポートする場合には、サービス・プロセッサの出荷時のデフォルト設定値を使用できます。

欠点:

- SLP をサポートしているのは、リモート監視プログラム・アダプター II サービス・プロセッサおよび IBM BladeCenter 管理モジュール・サービス・プロセッサだけです。これはベースボード管理コントローラー (BMC) サービス・プロセッサではサポートされていません。
- サービス・プロセッサと iSeries LAN アダプターの間には置かれているルーターおよびスイッチを、マルチキャスト・アドレッシングをサポートするように構成する必要があります。正しく構成されていない場合、ルーターはマルチキャスト・パケットを伝搬しません。マルチキャスト・アドレッシングが可能になるようにルーターを構成する方法を判別するには、ご使用のルーター資料を参照してください。Service Location Protocol では、239.255.255.253 の IP アドレスと 427 のポート番号を使用します。マルチキャスト SLP パケットをサポートするようにルーターを構成するために、この情報が必要になるかもしれません。

IP アドレスによるディスカバリー: このディスカバリーの方式では、ユニキャスト・アドレッシングを使用します。IP アドレスによるディスカバリーを構成するには、以下のステップを実行します。

1. ホストされるシステムにおいて、ネットワークに適切な静的 IP アドレスをサービス・プロセッサ内で構成します。可能ならば、サービス・プロセッサを LAN に接続する前にこのステップを行います。システム BIOS セットアップ・メニューまたは Web インターフェースのいずれか、ご使用のサービス・プロセッサによりサポートされる方を使用します。Web ブラウザーの接続および使用についての詳細は、160 ページの『管理モジュールまたは RSA II の Web インターフェースの使用』を参照してください。
2. iSeries サーバーにおいて、サービス・プロセッサ構成を構成します。
 - a. 「リモート・システムの格納装置識別を判別するためにサービス・プロセッサ接続を使用」オプションがチェックされていることを確認します。
 - b. 「IP アドレス」オプションを選択して、サービス・プロセッサの IP アドレスを指定します。
 - c. (オプション) スタンドアロン・サーバーのシリアル番号または IBM BladeCenter シャーシのシリアル番号を指定します。IP アドレスによりディスカバリーされるサービス・プロセッサのシリアル番号が、構成されたシリアル番号とは異なる場合、エラーが発生します。
137 ページの『サービス・プロセッサ構成プロパティの変更』を参照してください。
3. 134 ページの『リモート・システム構成プロパティの変更』で説明されている手順を使用して、以下のようにリモート・システム ID が正しく設定されていることを確認します。
 - スタンドアロン・サーバーの場合、「サービス・プロセッサ構成からの格納装置識別を使用」オプションを選択します。
 - IBM BladeCenter ブレードの場合、「次の値を使用」オプションを選択し、ブレードのシリアル番号を指定します。

利点:

- このディスカバリー方式は、サービス・プロセッサの IP アドレスが既知であり、サービス・プロセッサ内に構成されている場合には非常に単純です。

欠点:

- IP アドレスをサービス・プロセッサ内で構成する必要があります。

ホスト名によるディスカバリー: このディスカバリーの方式では、ユニキャスト・アドレッシングを使用します。ホスト名によるディスカバリーを構成するには、以下のステップを実行します。

1. ホストされるシステムにおいて、ホスト名をサービス・プロセッサ内で構成します。可能ならば、サービス・プロセッサを LAN に接続する前にこのステップを行います。
 - a. このステップでは、Web インターフェースを使用する必要があります。現行 IP アドレスを使用して、RSA II Web インターフェースに接続します。Web ブラウザーの接続および使用についての詳細は、160 ページの『管理モジュールまたは RSA II の Web インターフェースの使用』を参照してください。
 - b. ブラウザーを使用して、ホスト名をネットワークに適切な名前に変更します。
 - c. **オプション:** ネットワークに適切な静的 IP アドレスを構成することもできます。
2. iSeries サーバーにおいて、サービス・プロセッサを構成します。
 - a. 「リモート・システムの格納装置識別を判別するためにサービス・プロセッサ接続を使用」オプションがチェックされていることを確認します。
 - b. 「ホスト名」オプションを選択して、サービス・プロセッサのホスト名を指定します。

l c. **オプション:** スタンドアロン・サーバーのシリアル番号または IBM BladeCenter シャーシのシリアル番号を指定します。ホスト名によりディスカバリーされるサービス・プロセッサのシリアル番号が、構成されたシリアル番号とは異なる場合、エラーが発生します。

l 137 ページの『サービス・プロセッサ構成プロパティの変更』を参照してください。

l 3. 134 ページの『リモート・システム構成プロパティの変更』で説明されている手順を使用して、以下のようにリモート・システム ID が正しく設定されていることを確認します。

l • スタンドアロン・サーバーの場合、「サービス・プロセッサ構成からの格納装置識別を使用」オプションを選択します。

l • IBM BladeCenter ブレードの場合、「次の値を使用」オプションを選択し、ブレードのシリアル番号を指定します。

l 利点:

l • DNS サーバーが使用可能な場合、特定の IP アドレスを i5/OS リモート・システム構成で保持する必要がありません。

l 欠点:

l • サービス・プロセッサの Web インターフェースを介してホスト名をサービス・プロセッサ内に構成する必要があります。

l • ドメイン・ネーム・システム (DNS) サーバーが必要です。

l 管理モジュールまたは RSA II の Web インターフェースの使用

l リモート監視プログラム・アダプター II (RSA II) または管理モジュールの Web インターフェースを使用して、以下のタスクを実行することができます。

l • サービス・プロセッサの IP ホスト名を変更する

l • サービス・プロセッサ構成の手動セキュリティ設定の証明書を管理する

l - Verisign などの認証局から証明書を取得するために証明書署名要求を実行する

l - 証明書をサービス・プロセッサにインポートする

l • 静的 IP アドレスを構成する


l • RSA II ファームウェアを更新する

l **重要:** Web インターフェースを使用してサービス・プロセッサのユーザー名またはパスワードを変更しないでください。Web インターフェースを使用してユーザー名またはパスワードを変更すると、i5/OS オブジェクトには古いユーザー名とパスワードが含まれることになり、i5/OS はサービス・プロセッサに接続できなくなります。

l 138 ページの『サービス・プロセッサの初期化』の方法を使用してユーザー名およびパスワードを変更するか、または NWS 構成初期化 (INZNWSCFG) コマンドに *CHGSPAUT オプションを付けて実行します。これにより、i5/OS オブジェクトと、サービス・プロセッサのユーザー名およびパスワードとの同期を保ちます。

l サービス・プロセッサの Web インターフェースの使用については、以下のリンクを参照してください。

l • 「IBM リモート監視プログラム・アダプター II SlimLine およびリモート監視プログラム・アダプター

l II のユーザーズ・ガイド - サーバー(英語)」の 2 章 

l (www.ibm.com/pc/support/site.wss/)。「Browse (ブラウズ)」の下で「Servers (サーバー)」を選択し、

l 「Family: (ファミリー)」に「xSeries 236」、「Type: (タイプ:)」に「All Types (すべてのタイプ)」を

l 選択し、「Continue (続行)」を選択します。「Publications (資料)」を選択します。

・ 「IBM xSeries and BladeCenter Server Management」、SG24-6495 

Web ブラウザーによる RSA II または IBM BladeCenter 管理モジュールへの接続

1. **オプション:** ルーターを介してブラウザーを RSA II に接続する必要がある場合には、まず BIOS インターフェイスを使用して RSA II の IP アドレスを構成します。
2. 最初に、Web ブラウザーのアドレス (URL) 領域に、RSA II または管理モジュールの IP アドレスまたはホスト名を入力します。
3. RSA II または管理モジュールのユーザー名およびパスワードを入力するためのプロンプトが表示されるはずですが、RSA II または管理モジュールのユーザー名およびパスワードを入力します。RSA II または管理モジュールは、デフォルト・ユーザー名は「USERID」、デフォルト・パスワードは「PASSWORD」(0 はゼロ) になっています。RSA II または管理モジュールの出荷時のデフォルト値は以下のようにになっています。

DHCP「DHCP を試行。失敗した場合、静的 IP 構成を使用。」静的 IP アドレスは 192.168.70.125。これはルーティングできないアドレスであることに注意してください。つまり、このアドレスを使用しても、ルーターを介してブラウザーを RSA II または管理モジュールに接続できないということを意味します。ほとんどの (すべてではない) ブランドのスイッチ、およびほとんどのイーサネット・ハブで、デフォルトの IP アドレスを使ってブラウザーを RSA II または管理モジュールに接続できる可能性があります。

RSA II/管理モジュールの Web インターフェースへ接続すると、以下のタスクを実行できます。

- ・ ASM コントロールの下の「ネットワーク・インターフェース」を選択する。ホスト名を入力します。ホスト名フィールドに、IP ホスト名の非修飾部分を設定することをお勧めします。非修飾 IP ホスト名は、完全修飾 IP ホスト名の最初のピリオドまでで構成されています。たとえば、完全修飾 IP ホスト名 asmcard1.us.company.com の場合、非修飾 IP ホスト名は asmcard1 です。
- ・ ASM コントロールの下の「Login Profiles (ログイン・プロファイル)」を選択し、ユーザー名およびパスワードを変更する。これは、「手動」セキュリティー・モードでは必須です。
- ・ 「タスク」の下の「Firmware Update (ファームウェアの更新)」を選択して、RSA II または管理モジュールのファームウェアを最新のレベルに更新する。

第 8 章 統合 Windows サーバーの管理

以下のセクションでは、統合サーバー上で実行する日常の一般的な作業について説明します。

- 『統合サーバーの開始と停止』
 - 164 ページの『統合 Windows サーバーの開始と停止 (iSeries ナビゲーターを使用する場合)』
 - 164 ページの『統合 Windows サーバーの開始と停止 (文字ベースのインターフェースを使用する場合)』
 - 164 ページの『Windows サーバーのコンソールからの統合サーバーのシャットダウン』
 - 165 ページの『統合 Windows サーバーが存在する場合に iSeries を安全にシャットダウンする方法』
- 165 ページの『4812 IXS 仮想シリアル・コンソールへの接続』
- 166 ページの『統合 Windows サーバーの構成情報の表示または変更』
- 167 ページの『メッセージ・ログ』
- 168 ページの『統合 Windows サーバーのコマンドのリモート実行』
 - 169 ページの『リモート・コマンド実行に関するガイドライン』
 - 171 ページの『SBMNWSCMD と、Kerberos v5 および EIM のファイル・レベルのバックアップのサポート』
- 172 ページの『サーバー・ハードウェア間のホット・スペア』

統合サーバーの開始と停止

統合 Windows サーバーには電源ボタンがありません。統合 Windows サーバーの状態は iSeries が管理します。通常、統合サーバーの開始とシャットダウンは、iSeries ナビゲーターまたは文字ベースのインターフェースから実行します。統合サーバーの部分的なシャットダウンは、「スタート」→「シャットダウン」メニューからも実行できますが、再び開始するには、iSeries ナビゲーターまたは文字ベースのインターフェースからの操作が必要です。

iSeries をシャットダウンする前に、必ず統合サーバーをオフに変更してください。そうしない場合は、データが破損する可能性があります。iSeries のシャットダウン用のいくつかのコマンドは、接続している統合サーバーのシャットダウンを開始して、統合サーバーの電源遮断を待ってから iSeries をシャットダウンします。その他のコマンドは、iSeries をただちにシャットダウンします。

電源オフ/オンのスケジュール設定プログラム QEZPWROFFP を使用する場合は、統合サーバー用に構成する作業が必要です。

以下のセクションでは、開始とシャットダウンの方法について説明します。

- 164 ページの『統合 Windows サーバーの開始と停止 (iSeries ナビゲーターを使用する場合)』
- 164 ページの『統合 Windows サーバーの開始と停止 (文字ベースのインターフェースを使用する場合)』
- 164 ページの『Windows サーバーのコンソールからの統合サーバーのシャットダウン』
- 165 ページの『統合 Windows サーバーが存在する場合に iSeries を安全にシャットダウンする方法』

統合 Windows サーバーの開始と停止 (iSeries ナビゲーターを使用する場合)

1. iSeries ナビゲーターで統合サーバーを停止するには、「統合サーバー管理」->「サーバー」を選択します。
2. 停止するサーバーを右マウス・ボタンでクリックして、「シャットダウン (Shut Down)」を選択します。すべての統合サーバーをシャットダウンする場合は、左側のナビゲーションで統合 xSeries サーバーのアイコンを右マウス・ボタンでクリックしてから、「すべてシャットダウン (Shut Down All)」を選択します。状況が「シャットダウン中... (Shutting down...)」、「一部シャットダウン済み (Partially shut down)」に変わり、最後に「シャットダウン済み (Shutdown)」になります。
3. 統合サーバーを開始するには、対象のサーバーを右マウス・ボタンでクリックしてから、「開始」を選択します。状況が「開始中 (Starting)」に変わり、最後に「開始済み (Started)」になります。

統合 Windows サーバーの開始と停止 (文字ベースのインターフェースを使用する場合)

1. 文字ベースのインターフェースを使用して統合サーバーを停止するには、コマンド WRKCFGSTS *NWS を入力します。
2. 対象の統合サーバーを見つけ、2 と入力してオフに変更します。
3. 状況が **ACTIVE** から **SHUTDOWN** に変わり、最後に **VARIED OFF** になります。F5 を押して画面を更新できます。

注: iSCSI 接続のサーバーでは、状況が **ACTIVE** から **VARIED OFF** に変更されます。

4. 統合サーバーを開始するには、同じコマンド WRKCFGSTS *NWS を使用し、1 と入力してオンに変更します (つまり、統合サーバーを開始します)。
5. 統合サーバーを再始動するには、手動でオフに変更してからオンに戻す必要があります。文字ベースのインターフェースから統合サーバーを自動的に再始動するためのコマンドはありません。

Windows サーバーのコンソールからの統合サーバーのシャットダウン

統合 Windows サーバーをそれ自体のコンソールからシャットダウンするには、Windows の「スタート」メニューから、「スタート」->「シャットダウン」を選択します。ただし、この場合は、統合サーバーが部分的にシャットダウンするだけなので、この方法は推奨ではありません。Windows オペレーティング・システムは停止し、コンピュータの電源を切る準備ができました というメッセージを表示しますが、完全に電源を切って再始動するには、iSeries ナビゲーターまたは文字ベースのインターフェースを使用してオフに変更する必要があります。

シャットダウンの場合とは異なり、再始動の場合は、統合サーバーのコンソールから実行するのが効率的な方法です。

次のステップを実行してください。

1. 「スタート」メニューから「シャットダウン」を選択します。
2. ドロップダウン・メニューから「再起動」を選択して、「OK」をクリックします。

注: iSCSI 接続のサーバーでは、サーバーが Windows サーバー・コンソールからシャットダウンされる時、NWS はオフに変更されません。NWS は **ACTIVE** から **VARIED ON** に移行します。サーバーの状況は、iSeries ナビゲーターまたはネットワーク・サーバー状況処理 (WRKNWSSTS) を使用して照会することができます。状況は、このコマンドを実行するたびに取得されます。Windows サーバーはその状態を自動的にレポートしません。

統合 Windows サーバーが存在する場合に iSeries を安全にシャットダウンする方法

統合サーバーを安全にシャットダウンするための一番簡単な方法は、iSeries をシャットダウンする前に統合サーバーを常に手動でシャットダウンすることです。ただし、このような面倒な作業を繰り返していると、だんだん嫌気がさしてくる可能性もあります。CL コマンド PWRDWN SYS *CNTRL D は、それぞれの統合サーバーのシャットダウンに一定の時間 (NWS D 属性 SHUTDTIMO のデフォルト値は 15 分) を見込んで各サーバーの電源遮断を試みます。ただし、その時間内にシャットダウンが終了するという保証はありません。

注: CL コマンド PWRDWN SYS *IMMED はお勧めしません。このコマンドは統合サーバーのシャットダウンを試みずに、iSeries の電源遮断をただちに実行します。

表 2.

処置	結果
統合サーバーの手動シャットダウン	統合サーバーは正しくオフに変更され、データ損失の危険はありません。
CL コマンド pwrdw nsys *cntrl d の実行	統合サーバーには、NWS D のシャットダウン・タイムアウト属性で一定のシャットダウン時間が与えられ、それから iSeries の電源遮断に移っていきます。
CL コマンド pwrdw nsys *immed の実行	統合サーバーのシャットダウンなしで、iSeries の電源遮断がただちに実行されます。データ破損の危険がありません。

1 i5/OS システムで電源オン/オフ・スケジュールの機能を使用している場合は、電源オフ出口プログラム
1 (QEZPWROFFP) を変更して、PWRDWN SYS コマンドの呼び出し前にすべての NWS D をオフに変更する
1 ようにしてください。サーバーの数や各サーバーのアクティビティーによって、各サーバーを完全にオフに
1 変更するために必要な時間は違ってくるので、スケジュール設定については慎重な検討が必要です。パッチ
1 で複数のサーバーを同時に変更するには、構成変更 (VRYCFG) コマンドの複数ジョブ実行依頼
1 (SBMMLTJOB) およびジョブ記述 (JOB D) パラメーターを使用します。システムがすべてのサーバーをオ
1 フに変更してから PWRDWN SYS を実行する前に、スケジュール電源投入が発生するようであってはなり
1 ません。システムのシャットダウンおよび再始動をスケジュールするを参照してください。

4812 IXS 仮想シリアル・コンソールへの接続

仮想シリアル・コンソールは、4812 統合 xSeries サーバー (IXS) 上で実行される Windows Server 2003 サーバーに、Windows コンソールの機能を提供します。Windows コンソールについての詳細は、24 ページの『Windows コンソール』を参照してください。このコンソールの接続は、サーバーで TCP/IP を構成する前に使用できます。

Telnet クライアントはすべて、仮想シリアル・コンソールとして使用できます。複数の Telnet クライアントが同じ仮想シリアル・コンソールに同時にアクセスすることができます。コンソールに接続するには、Telnet を使用して、そのリソースを共有している i5/OS 区画のポート 2301 に接続します。i5/OS 論理区画で、TCP/IP が構成済みで、実行されていなければなりません。

IBM パーソナル・コミュニケーションズ・クライアントを使用して仮想シリアル・コンソールに接続するには、次のステップを実行します。

1. 「スタート」 -> 「プログラム」 -> 「IBM Personal Communications (IBM パーソナル・コミュニケーションズ)」 -> 「Start or Configure Session (セッションの開始または構成)」をクリックします。
2. 「Customize Communication (通信のカスタマイズ)」ダイアログ・ボックスの「Type of Host (ホストのタイプ)」フィールドで、ASCII を選択します。
3. 「Link Parameters (パラメーターのリンク)」をクリックします。
4. 「TelnetASCII」ダイアログ・ボックスの「Primary Host Name or IP Address (1 次ホスト名または IP アドレス)」フィールドに、接続先の i5/OS 区画のホスト名または IP アドレスを入力します。
5. 「Primary Port Number (1 次ポート番号)」フィールドに 2301 を入力します。
6. 「OK」をクリックします。
7. 「OK」をクリックします。セッション・ダイアログ・ボックスがオープンします。
8. 「i5/OS Virtual Consoles (i5/OS 仮想コンソール)」メニューで、「Integrated xSeries Server Consoles (統合 xSeries サーバー・コンソール)」を選択します。
9. 「Integrated xSeries Server Consoles (統合 xSeries サーバー・コンソール)」ダイアログ・ボックスで、コンソールとして接続する 4812 IOA のハードウェア・リソース名を選択します。4812 IOA ハードウェア・リソース名を決定するには、サーバーのネットワーク・サーバー記述 (NWSD) を表示し、リソース名パラメーターの値を使用します。
10. i5/OS 保守ツール ID およびパスワードを入力して、統合 xSeries サーバー仮想コンソールに接続します。

DOS コマンド・プロンプトから Telnet を使って仮想シリアル・コンソールに接続するには、次のステップに従います。

1. 「コマンド・プロンプト」ダイアログ・ボックスで、telnet *partitionname* 2301 を入力します。ここで、*partitionname* は、接続先の i5/OS 区画の名前です。
2. Enter キーを押します。
3. 「i5/OS Virtual Consoles (i5/OS 仮想コンソール)」メニューで、「Integrated xSeries Server Consoles (統合 xSeries サーバー・コンソール)」を選択します。
4. 「Integrated xSeries Server Consoles (統合 xSeries サーバー・コンソール)」ダイアログ・ボックスで、コンソールとして接続する 4812 IOA のハードウェア・リソース名を選択します。4812 IOA ハードウェア・リソース名を決定するには、サーバーのネットワーク・サーバー記述 (NWSD) を表示し、リソース名パラメーターの値を使用します。
5. i5/OS 保守ツール ID およびパスワードを入力して、統合 xSeries サーバー仮想コンソールに接続します。

統合 Windows サーバーの構成情報の表示または変更

iSeries ナビゲーターでは、統合サーバーのほとんどの構成情報を表示して変更できます。

1. iSeries ナビゲーターで、「統合サーバー管理」->「サーバー」を選択します。
2. 統合サーバーを右マウス・ボタンでクリックして、「プロパティ」を選択します。

l iSCSI 接続のサーバーでは、以下のように iSeries ナビゲーターを使用して、追加の構成情報を表示または変更することができます。

- l 1. iSeries ナビゲーターで、「統合サーバー管理」->「iSCSI 接続」を選択します。

2. 以下のいずれかのフォルダーを選択し、対応するオブジェクトのリストを表示します。リスト内でオブジェクトを右クリックし、「プロパティ」を選択します。
 - ・ ローカル・ホスト・アダプター
 - ・ リモート・システム
 - ・ サービス・プロセッサ
 - ・ 接続セキュリティ

文字ベースのインターフェースを使用する場合は、統合サーバーのすべての構成情報を表示して変更できません。以下の表に、関連する CL コマンドをまとめておきます。

表 3.

タスク	CL コマンド
統合サーバーのオン/オフを切り替えて、統合サーバーと、ネットワーク・サーバー記述 (NWSD) に関連するオブジェクトの状況を検査するタスク。	WRKCFGSTS CFGTYPE(*NWS)
統合サーバーを管理するタスク。	WRKNWSD
統合サーバーのインストール時に作成された回線記述を管理するタスク。	WRKLIND
サーバーのインストール時に作成された TCP/IP インターフェースを管理するタスク。	「TCP/IP ネットワーク状況の処理」のオプション 1: NETSTAT TCP/IP の構成、オプション 1 CFGTCP
ネットワーク・サーバー記憶域をモニターするタスク。	WRKNWSSTG
ネットワーク・サーバー構成を管理するタスク。	WRKNWSCFG
ネットワーク・サーバーのホスト・アダプターを管理するタスク。	WRKDEVD DEVD(*NWSH)

メッセージ・ログ

統合 Windows サーバーでは、ログ情報がさまざまな場所に格納されます。問題が発生した場合は、その原因を突き止めるのにここでの情報が役立ちます。以下のセクションでは、メッセージ・ログについて説明します。

統合サーバーに問題が発生した場合のトラブルシューティングに役立つ主な情報源は、**モニター・ジョブ・ログ**です。このログには、通常の処理イベントから詳細なエラー・メッセージまでさまざまなメッセージが記録されます。モニター・ジョブは、常に統合サーバーと同じ名前で QSYSWRK サブシステムで実行されます。

iSeries ナビゲーターでジョブ・ログを見つけるには

1. 「実行管理機能」→「アクティブ・ジョブ」をクリックします。
2. QSYSWRK セクションの下に表示されるジョブの 1 つが、統合サーバーと同じ名前になっているはずです。そのジョブを右マウス・ボタンでクリックしてから、「ジョブ・ログ」を選択します。
3. 統合サーバーのジョブ・ログのウィンドウがオープンします。メッセージ ID をダブルクリックすると、詳細が表示されます。

文字ベースのインターフェースでジョブ・ログを見つけるには

1. i5/OS コマンド行で、WRKACTJOB SBS(QSYSWRK) と入力します。

2. 表示されるジョブの 1 つが、統合サーバーと同じ名前になっているはずですが、オプション 5 (ジョブの処理) を選択します。
3. 10 と入力してから Enter を押して、ジョブ・ログを表示します。
4. F10 を押して詳細なメッセージを表示します。

関連する他のジョブ・ログも確認できます。レッドブック「Microsoft Windows Server 2003 Integration

with iSeries」(SG24-6959)  には、i5/OS および Windows コンソールの統合サーバー・イベント・ログについて詳しく載っているセクションがあります。

統合 Windows サーバーのコマンドのリモート実行

i5/OS を使用して、統合サーバーのバッチ・コマンドをリモートで実行できます。ユーザー対話なしでバッチ・モードで実行できる Windows サーバー・コマンドが実行されます。リモート・コマンドを実行する前に、以下の条件を満たしているかどうかを確認してください。

- サーバーがこの i5/OS 上の統合 Windows サーバーであり、アクティブであること。
- ユーザー・プロファイルが統合 Windows サーバーまたはドメインに登録されているか、コマンドの実行者が QSECOFR プロファイルにサインオンしていること。
- SBMNWSCMD を実行する権限がある (*JOBCTL 特殊権限が必要)。また、QSYS/SBMNWSCMD *CMD オブジェクトに対して少なくとも *USE 権限がなければなりません。
- ユーザー・プロファイルの *LCLPWDMGT 値が *YES の場合に、システム値 QRETSVRSEC が 1 に設定されていて、ユーザー・パスワードが変更されているか、ユーザーが QRETSVRSEC の変更後にサインオンしていること。
- ユーザー・プロファイルの *LCLPWDMGT 値が *NO の場合に、ネットワーク認証 (Kerberos) を使用していること。ユーザーは、Kerberos 対応アプリケーション (iSeries ナビゲーターのシングル・サインオンなど) によって iSeries オペレーションにアクセスする必要があります。詳しくは、171 ページの『SBMNWSCMD と、Kerberos v5 および EIM のファイル・レベルのバックアップのサポート』を参照してください。
- i5/OS ユーザー・プロファイル・パスワードと Windows パスワードが等しくなければならないこと。これらを整合した状態にしておく最も簡単な方法は、ユーザーおよびグループの登録を使用することです。

以下の 169 ページの『リモート・コマンド実行に関するガイドライン』も参考になります。

iSeries ナビゲーターから統合サーバーのコマンドを実行するには

1. iSeries ナビゲーターで、「統合サーバーの管理」 → 「サーバー」の順に選択します。
2. バッチ・コマンドを実行するサーバーを右マウス・ボタンでクリックして、「コマンドを実行する」を選択します。
3. 「コマンドを実行する」パネルで、実行する Windows コマンド (dir ¥ など) を入力します。

ヒント: コマンドは、サーバーでそれまでに実行した 10 個のコマンドのリストから選択することもできます。

4. 「実行」をクリックしてコマンドを実行します。

注: 「コマンドを実行する」パネルを使用するコマンドでは、認証ドメインとして *PRIMARY が使用されます。代替ドメインとしては SBMNWSCMD が使用されます。

文字ベースのインターフェースから統合 Windows サーバーのコマンドを実行するには

1. CALL QCMD と入力して、Enter を押します。
2. SBMNWSCMD と入力して、F4 を押します。
3. リモート・サーバーで実行するコマンドを入力します。次ページ・キーを押します。
4. コマンドを実行するサーバーの NWSD を入力して、Enter を押します。
5. リモート・コマンドを実行するための認証を受けるには、使用する i5/OS アカウントを統合サーバーに登録しておく必要があります。認証ドメインのフィールドでは、ユーザー ID の認証を受けるための場所を指定できます。
6. コマンドから戻された出力がコンソールに表示されます。F10 を押してすべてのメッセージを表示します。

リモート・コマンド実行に関するガイドライン

統合 Windows サーバーのコマンドをリモートで実行する場合は、次の指針に留意してください。

注: このセクションで取り上げている SBMNWSCMD パラメーターの多くは、iSeries ナビゲーターから Windows コマンドを実行するときには使用できません。iSeries ナビゲーターがサポートしていないパラメーターを使用する必要がある場合は、SBMNWSCMD (ネットワーク・サーバー・コマンドの投入) を直接使用する必要があります。

- 要求コマンドは、Windows コンソール・コマンド "cmd.exe." のもとで実行されます。SBMNWSCMD は、Windows 上での実行を終了して cmd.exe プログラムが終了するまで、その呼び出し側に制御を戻しません。
- SBMNWSCMD の「認証ドメイン」フィールドは、ユーザー ID が認証される Windows ドメインを示します。サーバーがドメイン・メンバーの場合、デフォルトの *PRIMARY のときはサーバーの 1 次ドメインにログオンします。*LOCAL の場合はそのサーバー自体にログオンします。トラステッド・ドメインの名前を指定しても構いません。
- QSECOFR ユーザー・プロファイルは、他のすべてのユーザー・プロファイルとは別に処理されます。SBMNWSCMD が QSECOFR プロファイルによって実行されるときは、Windows でのユーザー認証は行われません。Windows 要求コマンドは、Windows のローカル・システム・アカウントのもとで実行されます。ローカル・システム・アカウントは QSECOFR プロファイルが登録されていても使用されません。ローカル・システム・アカウントにはパスワードがなく、ネットワーク・アクセス権限がありません。
- "/u" パラメーターは、Windows "cmd" コマンドと一緒に使用しないでください。
- SBMNWSCMD は、Kerberos v5 の認証を限定的にしかサポートしていません。Kerberos は、LCLPDMGT ユーザー・プロファイル属性が *NO の場合にのみ使用されます。171 ページの『SBMNWSCMD と、Kerberos v5 および EIM のファイル・レベルのバックアップのサポート』を参照してください。
- リモート・コマンド・サービスと SBMNWSCMD は、ASCII マルチバイトと Unicode 出力データを区別して、それらを必要に応じて変換できます。
- Windows の "cmd.exe" コマンド・インタープリターの機能を使用して、複数の統合 Windows サーバー・コマンドを 1 つのコマンド・ストリングに結合できます。たとえば、SBMNWSCMD コマンド行に、net statistics workstation && net statistics server と入力して統計を収集できます。しかし、1 つの SBMNWSCMD 要求に結合するコマンドは、混合データ (ASCII および Unicode データの組み合わせ) や、または混合コード・セットのデータを戻すことはできません。コマンドが異なるタイプのデータを戻すと、SBMNWSCMD は「データ出力変換で問題が発生した」ことを示すメッセージを出して異常終了します。この場合には、コマンドを別々に実行してください。

- 統合サーバー・キーボードで通常使用することのできない文字は使用しないでください。まれなケースでは、アクティブ・ジョブのコード化文字セットにある EBCDIC 文字の中には、同等の文字が Windows のアクティブ・コード・ページ内にもあります。Windows アプリケーションが異なると、変換結果も異なってきます。
- ネットワーク・サーバー・コマンドの投入で、ログオン環境が完全に初期化されるわけではありません。ユーザーの環境変数が設定されても、対話式ログオンで指定するものとまったく同じになるとは限りません。したがって、対話式のログオンで通常はユーザー固有の値に設定される環境変数は、存在しないこともありますし、システム・デフォルト値に設定することもできます。ユーザー固有の環境変数に依存するスクリプトまたはアプリケーションは、正しく実行されない可能性があります。
- 統合サーバーでのユーザー ID のホーム・ディレクトリーがローカル・サーバーに設定されている場合は、ネットワーク・サーバー・コマンドの投入によって、現行ディレクトリーがホーム・ディレクトリーに設定されます。そうでない場合には、/home/default またはローカル・システム・ドライブを使用しようとします。
- ユーザー・プロファイルのロード (LODUSRPRF) キーワードが *YES の場合や、ユーザー・プロファイルがある場合は、SBMNWSCMD は Windows プロファイルをロードしようとします。その後、プロファイルの依存関係を使用または変更するコマンドを使用することができます。ただし、プロファイルのロードに失敗しても、そのことは Windows によって作成されるイベント・ログ・メッセージ以外では示されません。1 つの Windows ログオン・セッションで活動状態にできる Windows プロファイルは 1 つのみです。
- ユーザーの介入を必要としないかぎり、SBMNWSCMD を使用して統合サーバー・アプリケーションを実行できます。コマンドは、統合サーバー・コンソール上ではなく、バックグラウンド・ウィンドウで実行されます。メッセージ・ウィンドウのポップアップのような形でアプリケーションがユーザー介入を要求すると、SBMNWSCMD はハングし、コマンドの完了待ちになります。ただし、介入することはできません。i5/OS 上で SBMNWSCMD を終了すると、ハングしている Windows コマンドの終了が試みられます。バックグラウンド・コマンドは、GUI またはコンソールのどちらであっても終了します。
- 先に進むには **yes** または **no** の応答の必要なコマンドを実行することもできます。これは、入力パイプ構文を使用して応答を出せば実行できます。たとえば、`echo y|format f: /fs:ntfs` と入力すると、`format` コマンドを実行すると出される「フォーマットを続行しますか」の質問の後に、フォーマットがそのまま継続するようにできます。「y」とパイプ記号「|」の間にはスペースを入れないことに注意してください。しかし、すべての Windows バッチ・コマンドが、入力のパイピングをサポートしているわけではありません (たとえば `net` コマンド)。デフォルトの応答を渡そうとしてもできない場合があります。
- SBMNWSCMD がコマンドをログに記録しないようにすることができます。エラー・メッセージに記録しないようにしたい機密データ (パスワードなど) がコマンド・ストリングに入っている場合には、以下のステップを実行してください。
 1. コマンド・ストリングとして *NOLOGCMD を指定します。
 2. 「コマンド (ログに記録されない)」フィールドが表示されたら、実行するコマンドをそのフィールドに入力します。

ただし、*NOLOGCMD オプションを指定しても、このコマンドが戻すデータには影響を与えないことに注意してください。このコマンドが機密データを戻す場合は、コマンド標準出力 (CMDSTDOUT) パラメーターを使用して、統合ファイル・システム・ファイルなどの安全な場所に出力を保管できます。
- このコマンドからの標準出力は、ジョブ・ログ (*JOBLOG)、スプール・ファイル (*PRINT)、統合ファイル・システム (IFS) オブジェクトのいずれかに送信できます。標準エラー・データは、常にジョブ・ログに入ります。

*PRINT を指定すると、「スプール・ファイルの処理 (WRKSPLF)」画面のスプール・ファイルの「ユーザー・データ」フィールドに SBMNWSCMD が表示されます。オプション 8 を選択して属性を表示すると、指定された統合サーバーおよび Windows コマンドの名前がユーザー定義のデータ・フィールドに表示されます。

統合ファイル・システム・オブジェクトを指定するときは、そのパス名がすでに存在していなければなりません。統合ファイル・システム・オブジェクト名が存在していない場合は、SBMNWSCMD がその名前を作成します。

- 「標準出力の変換」フィールドで (*YES) を指定すると、Windows コード・セットからの出力を i5/OS ジョブのコード化文字セット ID (CCSID) に変換できます。

ジョブ CCSID とともに新しい IFS ファイルが作成されます。既存の IFS オブジェクトに送信する出力は、IFS オブジェクトの CCSID に変換されます。/QSYS.LIB ファイル・システム内の既存ファイルの新しいメンバーに送信する出力は、その既存ファイルの CCSID に変換されます。

- 「標準出力の変換」が (*NO) の場合、Windows の標準出力は CCSID に変換されて IFS オブジェクトからスプール・ファイルに書き込まれます。

SBMNWSCMD と、Kerberos v5 および EIM のファイル・レベルのバックアップのサポート

統合 Windows サーバーに対するファイル・レベルのバックアップ・オペレーションでは、iSeries の NetClient 機能と SBMNWSCMD (ネットワーク・サーバー・コマンドの投入) 機能を使用します。i5/OS V5R3 以降の場合、これらの機能には、Kerberos v5 のサポート (iSeries ネットワーク認証ともいう) が限定的にしか用意されていません。したがって、これらの機能でネットワーク認証を使用する場合は、以下の注意点を押さえておく必要があります。

1. iSeries で Kerberos 認証を使用するには、iSeries サーバーで以下の機能やオプションを構成する必要があります。
 - iSeries ナビゲーターのセキュリティー・オプション
 - ネットワーク認証サービス
 - エンタープライズ識別マッピング (EIM)
 - 暗号アクセス・プロバイダー (5722-AC2 または AC3)
2. iSeries NetServer でパスワード認証と Kerberos v5 認証を使用するように構成し、NetServer をアクティブにする必要があります。
3. Windows Active Directory のドメイン・コントローラー (Windows 2000 Server または Windows Server 2003) を Kerberos KDC にする必要があります。詳しくは、116 ページの『Windows Server 2003 Active Directory Server を使用して Kerberos を使用可能にする』を参照してください。
4. Kerberos 認証は、i5/OS ジョブのユーザー・プロファイルの LCLPWDMGT 属性が *NO に設定されている場合にのみ使用されます。LCLPWDMGT が *YES に設定されている場合は、パスワード認証が常に使用されます。
5. ユーザー登録機能では、EIM を使用して、Windows ユーザー名を別の i5/OS プロファイル名にマッピングできます。したがってユーザー登録では、必要に応じて、Windows Active Directory ドメイン名に由来する EIM レジストリーを検索したり、統合サーバー名に由来する EIM レジストリーを検索したりできます。このように、ユーザー登録機能は、Kerberos 認証を使用できるかどうかにかかわらず EIM マッピングを使用しますが、SBMNWSCMD と NetClient は、Kerberos 認証を使用する場合のみ、EIM マッピングに基づく名前を使用します。つまり、ユーザー登録機能は、EIM マッピングによって指定されている i5/OS プロファイルとは異なる名前でローカル Windows ユーザーを作成すること

がありますが、SBMNWSCMD と NetClient は、Kerberos 認証を実行している場合 (LCLPDMGT = *NO の場合) にのみ、別の Windows 名を使用します。そうでない場合は、i5/OS プロファイル名と同じ Windows 名によって認証を受けようとします。

6. Kerberos 認証が使用されている場合に、SBMNWSCMD から実行する Windows コマンドが他のネットワーク・サーバーに接続するには、ターゲットの Windows サーバーが委任に対して信頼されている必要があります。Windows 2000 の場合、ドメイン・コントローラーについてはこの設定がデフォルトで有効になりますが、ドメインのメンバー・サーバーについてはデフォルトで無効になります。この設定を有効にするには、ドメイン・コントローラーで、「Active Directory ユーザーとコンピュータ」管理ツールを使用します。このツールで、「Computers」をクリックして、対象のコンピューターを選択します。「プロパティ」->「全般」をクリックします。「コンピューターを委任に対して信頼する」にチェック・マークを付けます。

サーバー・ハードウェア間のホット・スペア

iSeries と xSeries を統合し、記憶域の仮想化を行うと、Windows サーバー環境の信頼性と回復可能性を向上させるために使用可能にできるオプションが提供されます。Windows サーバーに障害が起きた場合、iSeries サーバーを再始動せずに、サーバーの記憶域スペースを別のホット・スペアの xSeries サーバーに即時かつ簡単に切り替えることができます。この場合、可用性を向上させるために必要な Intel サーバーの総数を少なくできる可能性があります。さらに、1 つのスペア・サーバーを使用して複数の実動サーバーを保護することができるので、柔軟性も向上します。

注: iSCSI 接続サーバーの場合、iSCSI ローカル・ホスト・アダプターもホット・スペア・サポートの利点を活用できます。146 ページの『iSCSI ローカル・ホスト・アダプター間のホット・スペア』を参照してください。

統合サーバーのハードウェアをホット・スペアリングする手順を以下に示します。

iSeries ナビゲーターを使用する場合:

1. 「統合サーバー管理」を展開します。
2. 「サーバー」を選択します。
3. ハードウェアを交換するサーバーをまだシャットダウンしていない場合は、以下のようになります。
 - サーバーを右マウス・ボタンでクリックして、「シャットダウン」を選択します。
 - 確認パネルで「シャットダウン」をクリックします。
4. ホット・スペアのサーバーのハードウェアを指すようにサーバー構成を変更します。
 - a. サーバーを右マウス・ボタンでクリックして、「プロパティ」を選択します。
 - b. 「システム」タブを選択して、次の 1 つを選びます。
 - iSCSI 以外のサーバーの場合、新しい「リソース名およびタイプ」を選択します。
 - iSCSI サーバーの場合、新しい「リモート・システム構成名」を選択します。
- 「OK」をクリックします。
5. 統合サーバーを開始するには、サーバーを右マウス・ボタンでクリックして、「開始」を選択します。

文字ベースのインターフェースを使用する場合:

1. ハードウェアを交換するサーバーをまだオフに変更していない場合は、構成変更 (VRYCFG) コマンドを使用してオフに変更します。
2. ホット・スペアのサーバーのハードウェアを指すようにサーバー構成を変更するには、ネットワーク・サーバー記述変更 (CHGNWSD) コマンドを使用して以下のいずれかに変更を加えます。

- | • iSCSI 以外のサーバーの場合、**資源名 (RSRCNAME)** パラメーターの値を変更して、新しい IXS または IXA ハードウェア・リソース名を指定します。
 - | • iSCSI サーバーの場合、**ネットワーク・サーバー構成 (NWSCFG)** パラメーターのリモート・システム名エレメントの値を変更して、新しいリモート・システム・ネットワーク・サーバー構成オブジェクト名を指定します。
- | 3. 統合サーバーを開始するには、**構成変更 (VRYCFG)** コマンドを使用します。

第 9 章 記憶域の管理

統合 Windows サーバーは、クライアント・データの格納とネットワーク・ファイルの共用のために、自身のハード・ディスク・ドライブではなく i5/OS のディスク記憶域を使用します。統合サーバーに割り振られた i5/OS のディスク記憶域をネットワーク・サーバー記憶域といいます。統合サーバーにおいて、PC サーバーに新規ハード・ディスクをインストールすることに相当するのは、i5/OS にネットワーク・サーバー記憶域を作成してそれを統合サーバーにリンクすることです。統合サーバーのディスク記憶域が i5/OS によって管理されることを踏まえると、ドライブ・サイズ、区分化、およびディスク・ボリュームに関する決定に影響を与えるはず değildir。『i5/OS の記憶域管理』を参照してください。さらに、179 ページの『統合 Windows サーバーの事前定義ディスク・ドライブ』および 176 ページの『統合 Windows サーバーのディスク・ドライブ』をお読みになることもできます。

iSeries 用の Windows 環境により、以下の方法でデータ記憶域を扱う助けが得られます。

- i5/OS を使用して 180 ページの『i5/OS からの統合 Windows サーバー・ディスク・ドライブの管理』を行うことができます。
- 187 ページの『統合 Windows サーバーでの Windows ディスク管理プログラムの使用』を行うオプションが与えられます。

i5/OS の記憶域管理

ここに記載されている i5/OS 記憶域管理の概念に関する簡単な概要は、Windows サーバーの記憶域管理に精通している管理者を対象としています。i5/OS が記憶域管理を処理する方法は PC サーバーとは異なるため、PC サーバーで必要な一部の技法は iSeries 上の Windows 環境では不必要です。

i5/OS とディスク・ドライブ

i5/OS (iSeries 上で実行されるオペレーティング・システム) では、ディスク・ドライブを直接処理する必要はありません。このオペレーティング・システムでは、あるレベルのソフトウェア (システム・ライセンス内部コード (SLIC)) がディスク・ドライブを隠し、それらのディスク・ドライブ上のオブジェクトの記憶域を管理します。仮想アドレス領域が既存のディスク記憶域にマップされ、ディスク・ドライブ ID、シリンダー、およびセクターの代わりにオブジェクトのアドレス指定に使用されます。必要なオブジェクトは、ディスク上のこのアドレス領域から、メイン・メモリーのアドレス領域に複写 (ページイン) されます。

i5/OS がディスク・データを管理するため、統合サーバー上では、肥大化するデータベースの区分化、ディスクのデフラグ、またはディスクのストライピングについて心配する必要はありません。統合サーバーは、デバイス・ドライバを使用して i5/OS のディスク・ドライブを共用します。これらのデバイス・ドライバは、i5/OS 記憶域管理サブシステムとの間でディスク・データを送受信します。ハード・ディスクの処理は i5/OS 記憶域管理が行い、Windows ディスク・ドライブのイメージを複数のハード・ディスク・ドライブに分けて分散させたり、RAID とファイルのミラーリング (構成されている場合) を適用したりします。ディスク・デフラグ・ソフトウェアは、ハード・ディスク・イメージの論理ファイル断片化を管理します。i5/OS 記憶域管理がこれらの作業を扱うため、統合サーバー上でデフラグ・プログラムを実行するのが役立つのは、主に「重要なファイル・システム構造」のデフラグが可能な場合です。

ディスク・プール (ASP)

i5/OS では、いくつかの物理ハード・ディスクが、ディスク・プール (または、補助記憶域プール (ASP)) と呼ばれる 1 つのストレージ・スペースにまとめてプールされます。ファイル・システムがスペースを使い尽くした場合、ディスク・プールに新規ハード・ディスクを追加することができます。そうすれば、新しいストレージ・スペースがすぐに使用可能になります。どのシステムにも、システム・ディスク・プールというディスク・プールが少なくとも 1 つあります。システム・ディスク・プールは常に ASP 1 になります。2 から 255 までの番号の追加ユーザー・ディスク・プールを構成できます。ディスク・プールを使用すると、異なるディスク・グループにまたがって i5/OS データを分散させることができます。また、この概念を使用すると、重要度の低いアプリケーションやデータを、より旧式で処理速度が遅いディスク・ドライブに移動することもできます。独立 ASP (33 から 255 まで) のサポートは、iSeries ナビゲーターを使って実現します。Information Center と iSeries ナビゲーターではどちらも、ASP はディスク・プールという名称になっています。

ディスク保護:

i5/OS のディスクは、以下の 2 つの方法で保護できます。

1 • サイト間ミラーリング

1 オペレーティング・システムの IASP のリモート・ミラーリングを使用した、サイト間ミラーリングは、距離がかなり離れている場所にあるディスク上にデータをミラーリングします。

• RAID-5

RAID-5 技法では、複数のディスクを 1 つの配列にまとめます。それぞれのディスクには、同じ配列にある他のディスクのチェックサム情報があります。いずれかのディスクで障害が発生した場合は、RAID-5 ディスク・コントローラーで他のディスクに関するチェックサム情報を活用して、障害が発生したディスクのデータを再作成できます。障害が発生したディスクを新しいものに置き換える場合、i5/OS は、障害が発生したディスクの情報を新しい (空の) ディスク上に再構築できます。

• ミラーリング

ミラーリングでは、2 つの異なるディスクに 2 つのデータ・コピーを保持します。i5/OS では、同時に両方のディスクへの書き込み操作を実行し、ミラーリングの対になっている 2 つのディスクに対して 2 つの異なる読み取り操作を同時に実行できます。1 つのディスクで障害が発生した場合、i5/OS はもう 1 つのディスクの情報を使用します。障害が発生したディスクを置き換える場合、i5/OS は障害がないほうのディスクのデータを新しいディスクに複写します。

保護のレベルをさらに強化するには、ミラーリングされたディスクを 2 つの異なるディスク・コントローラーに接続することができます。どちらかのコントローラーとそのディスク・セットで障害が発生した場合は、もう一方のコントローラーでシステムを機能させることができます。もっと大きな iSeries モデルでは、複数のバスにコントローラーを接続することができます。ミラーリングされた対を形成する 2 つのディスク・コントローラーを 2 つの異なるバスにつなぐと、さらに可用性を高めることができます。

i5/OS 上のディスク・プールに対してさまざまな保護レベルを定義することができますが、保護をまったく定義しないようにすることもできます。こうすると、それぞれの使用に関する重要度に応じた保護を定義されたディスク・プールにアプリケーションとデータを入れることができます。i5/OS のディスク保護および可用性オプションについては、バックアップおよび回復の手引きをお読みください。

統合 Windows サーバーのディスク・ドライブ

統合サーバー自体にはディスク・ドライブがありません。i5/OS が自身のファイル・システム内にネットワーク・サーバー記憶域を作成し、統合サーバーはあたかもそれらが通常のハード・ディスク・ドライブであるかのように使用します。

統合 Windows サーバーが統合サーバー・ディスク・ドライブ (ネットワーク・サーバー記憶域) をハード・ディスク・ドライブとして認識できるようにするために、それらを一緒にリンクする必要があります。その前にディスク・ドライブを作成しておかなければなりません。181 ページの『統合サーバー・ディスク・ドライブの作成』および 182 ページの『ディスク・ドライブと統合サーバーのリンク』を参照してください。新しい統合サーバー・ディスク・ドライブを作成してリンクすると、それは統合サーバーには新規ハード・ディスク・ドライブとして示されます。その後、それを使用できるようにするために、フォーマットする必要があります。183 ページの『統合サーバー・ディスク・ドライブのフォーマット』を参照してください。

次の方法のどちらかでディスク・ドライブをサーバーにリンクすることができます。

1. 固定の (静的) ディスク・ドライブ・リンクを使用すると、ユーザー指定のリンク順序位置でディスク・ドライブをサーバーにリンクすることができます。サーバーで認識されるドライブの順序は、リンク順序位置の相対順序で決まります。固定の (静的) ディスク・ドライブ・リンクを追加するときは、サーバーをオフに変更しておかなければなりません。

注: 静的ドライブ・リンクは、iSCSI 接続 xSeries サーバーでは使用されません。

2. クラスタ・クォーラム・リソースのディスク・ドライブをクラスタ内のサーバーにリンクする場合は、クラスタ・クォーラム・リソース・ディスク・ドライブ・リンクを使用します。

3. クラスタ共用ディスク・ドライブ・リンクを使用すると、クラスタ化されている統合サーバーの間でディスク・ドライブを共用することができます。共用ドライブをリンクできるのは、共通クォーラム・リソース・ドライブを共用するノードに対してのみです。このタイプのドライブは、クラスタ・クォーラム・リソースのリンクによって結合しているすべてのノードで使用できます。各ノードは、その上で動作する Windows クラスタ・サービスの制御下にある共用ドライブに対してアクセスすることができます。

注: 共用としてリンクされるドライブは、一緒にクラスタ化されているすべてのノードにリンクする必要があります。

4. 動的ディスク・ドライブ・リンクを使用すると、動的に割り当てられるリンク順序位置に従って、さらに別のディスク・ドライブを統合サーバーにリンクすることができます。ディスク・リンク順序位置は、活動中のサーバーにディスク・ドライブがリンクされるときに動的に割り当てられます。ディスク・リンク順序位置を指定することができますが、それが使用されるのはサーバーの再始動後です。動的ディスク・ドライブ・リンクを追加するときは、統合サーバーはシャットダウン済みまたは活動中のどちらでも可能です。

iSCSI 以外の統合サーバーを始動すると、次の順序でディスク・ドライブを認識します。

1. 静的にリンクされたディスク・ドライブ
2. クラスタ・クォーラム・リソース・ディスク・ドライブ
3. クラスタ共用ディスク・ドライブ
4. 動的にリンクされたディスク・ドライブ

iSCSI 接続サーバーの場合、クラスタ・クォーラム・ディスクはディスク・ドライブのリストの最後に表示されます。動的にリンクされたディスクおよびクラスタ共用ディスクは混用することができます。

これらのリンク・タイプの各カテゴリー内では、ユーザーが指定したリンク順序位置の順にディスクを認識します。ディスク・ドライブを活動中のサーバーに動的にリンクすると、他のすべてのリンク済みディスク・ドライブの後にその新規のディスク・ドライブを認識します。

以下の表では、i5/OS V5R4 以降のさまざまなタイプのサーバー・ネットワーク・サーバー記述 (NWS D) でサポートされる、iSeries 仮想ディスク・ドライブ機能について説明します。

サポートされるディスク機能

機能	NWS D タイプ ⁵ *WINDOWSNT または *IXSVR (OS タイプ *WIN32)	NWS D タイプ ⁵ *ISCSI (OS タイプ *WIN32)
固定の (静的) リンク数	16	0
動的リンク数	16	63 ¹
クラスター・クォーラム・リンク数	1	1
クラスター共用リンク数	15	61 ¹
サーバーにリンク可能な仮想ディスクの最大数	48 (クラスタリングを使用した場合) ² または 32 (それ以外の場合)	64 (クラスタリングを使用した場合) ² または 63 (それ以外の場合)
仮想ディスクごとの最大容量	1000 GB	1000 GB
仮想ディスクの合計最大容量 (ディスクごとに 1000 GB と仮定した場合)	46.9 TB (クラスタリングを使用した場合) ² または 31.3 TB (それ以外の場合)	62.5 TB (クラスタリングを使用した場合) ² または 61.5 TB (それ以外の場合)
サーバーがアクティブである間に仮想ディスクのリンクが可能か	はい 例外: 固定リンク	はい 例外: 動的リンク 1-2
サーバーがアクティブである間に仮想ディスクのリンク解除が可能か	はい 例外: 固定リンク (ディスクをボリューム・セットの一部にしたり、ディレクトリーにマウントされたボリュームにすることはできません)	はい 例外: 動的リンク 1-2 (ディスクをボリューム・セットの一部にしたり、ディレクトリーにマウントされたボリュームにすることはできません)
リンク ³ 時に許可される仮想ディスク・フォーマットのタイプ	*NTFS、 *NTFSQR、 *FAT、 *FAT32、 *OPEN	*NTFS、 *NTFSQR、 *FAT、 *FAT32、 *OPEN
リンク時に許可される仮想ディスク・アクセスのタイプ	排他的更新、共有更新 ⁴	排他的更新、共有更新 ⁴
排他的更新アドレス・タイプに必要なディスク・リンク	すべてのハード・ディスク・リンクおよび動的リンク	すべての動的リンク
共有更新アドレス・タイプに必要なディスク・リンク	クラスター・クォーラム・リンクおよびクラスター共用ディスク・リンク	クラスター・クォーラム・リンクおよびクラスター共用ディスク・リンク

注:

- iSCSI Windows サーバーの場合、動的共用ディスクおよびクラスター共用ディスクは同じ範囲の順序位置を使用し、混用することができます。組み合わせた動的共用ディスクおよびクラスター共用ディスクの合計数は 63 です。
- Windows サーバー・クラスタリングでは、クラスター内で共用ディスクへのアクセスを制御するために Microsoft クラスター・サービス (MSCS) の使用が必要になります。
- フォーマット・タイプの説明については、NWS 記憶スペースの作成 (CRTNWSSTG) コマンドのヘルプ・テキストを参照してください。
- 複数のサーバーが共有更新を使用してディスクをリンクする場合、1 つのサーバーだけが任意の時点でそのディスクに対する書き込みアクセスを持つことができます。たとえば、Windows サーバーの場合、クラスター内でディスクへの書き込みアクセスを持つサーバーを制御するのに Microsoft クラスター・サービス (MSCS) が使用されます。

5. NWSD タイプおよび関連したオペレーティング・システム (OS) タイプの説明については、ネットワーク・サーバー記述の作成 (CRTNWSD) コマンドのヘルプ・テキストを参照してください。

ネットワーク・サーバー記憶域は、i5/OS システム・ディスク・プール (ASP 1) またはユーザー・ディスク・プール内に置くことができます。ディスク・ドライブを別のディスク・ドライブにコピーして、異なるディスク・プールに移動することができます。

- ネットワーク・サーバー記憶域が作成され、統合サーバーにリンクされた後、Windows コンソールからそれをフォーマットする必要があります。3種類のディスク・フォーマットから選択することができます。NTFS が最も効率のよい安全なフォーマットなので、おそらく NTFS を選択することでしょう。NTFS でフォーマットされた区画は、最大 1,024,000 MB です。もう 1 つのフォーマット・タイプは FAT-32 です。FAT-32 でフォーマットされた区画は 512 MB 以上 32,000 MB 以下です。最も古いフォーマット・タイプは FAT です。FAT 区画の考えられる最大サイズは 2,047 MB です。事前定義インストール・ソース・ドライブ区画 (ドライブ D) は FAT 形式のままであればならず、そのため、2,047 MB までに限定されます。

ネットワーク・サーバー記憶域は、統合サーバーが使用する 2 種類のネットワーク記憶域の 1 つです。統合サーバーは、iSeries NetServer を使用することにより、管理者がネットワークと共用している i5/OS 上のリソースにもアクセスできます。

IBM iSeries 統合サーバー・サポートのインストール・プロセスでは、統合 Windows サーバーをインストールして実行するのに使われるディスク・ドライブがいくつか作成されます。『統合 Windows サーバーの事前定義ディスク・ドライブ』のトピックを参照してください。

- ドライブの作成については、181 ページの『統合サーバー・ディスク・ドライブの作成』を参照してください。

統合 Windows サーバーの事前定義ディスク・ドライブ

IBM iSeries 統合サーバー・サポートのインストール・プロセスで、統合サーバーのインストールおよび実行に使用される 2 つのディスク・ドライブ (ネットワーク・サーバー記憶域) が作成されます。176 ページの『統合 Windows サーバーのディスク・ドライブ』を参照してください。デフォルトでは、これらのディスク・ドライブは i5/OS によってシステム・ディスク・プール (ASP) 内に作成されますが、インストール中に別の場所を選択することもできます。i5/OS では、統合サーバーのロードと開始にもこれらのディスク・ドライブが使われます。

サーバーには、以下のような事前定義ディスク・ドライブがあります。

ブートおよびシステム・ドライブ (C)

このドライブはシステム・ドライブとして機能します。i5/OS はこのドライブに *server1* という名前を付けます。ここで、*server* はネットワーク・サーバー記述 (NWSD) の名前です。このディスク・ドライブは、統合ファイル・システム内に置かれ、自動的に最初のドライブとしてリンクされます。

C ドライブは 1,024 MB 以上 1,024,000 MB 以下の範囲です。ドライブ FAT のままにしておくことも選択できます。記憶域のサイズによって必要とされる場合には、C ドライブは自動的に NTFS に変換されます。

注: NWSD 構成ファイルを作成する場合は、NWSD 構成ファイルがサポートされているのは、FAT または FAT32 としてフォーマットされたディスク・ドライブだけであることに注意してください。275 ページの『第 15 章 ネットワーク・サーバー記述構成ファイル』を参照してください。NTFS に変換されたシステム・ドライブには、アクセスして NWSD 構成ファイル

を取得することはできません。別のファイル・システムの詳細については、96 ページの『FAT、FAT32、および NTFS ファイル・システムの比較』を参照してください。

インストール・ソース・ドライブ (D)

D ドライブは 200 から 2,047 MB で、Windows サーバー・インストール・コードと IBM iSeries 統合サーバー・サポート・コードのコピーが保持されています。i5/OS はこのドライブに *server2* という名前を付けます。ここで、*server* は NWSD の名前です。このディスク・ドライブは、統合ファイル・システム内に置かれ、自動的に 2 番目のドライブとしてリンクされます。D ドライブは、i5/OS によってファイル割り振りテーブル (FAT) ディスクとしてフォーマットされます。

重要: このドライブは必ず FAT ドライブのままにしておかなければなりません。このドライブを変更しないでください。i5/OS は更新を行うためにこのドライブを使用するので、ドライブの変更を行うと更新が不可能になります。

注: V4R5 以前の i5/OS システムからアップグレードされたサーバーについては、V5R3 iSeries Information Center の『統合 Windows サーバーの事前定義ディスク・ドライブ』を参照してください。

i5/OS からの統合 Windows サーバー・ディスク・ドライブの管理

i5/OS からの統合サーバー・ディスク・ドライブ (ネットワーク・サーバー記憶域) の管理には、以下のタスクが含まれています。

- 『統合サーバーからの i5/OS 統合ファイル・システムへのアクセス』
- 『統合サーバー・ディスク・ドライブについての情報の取得』
- 181 ページの『統合 Windows サーバーへのディスク・ドライブの追加』
- 184 ページの『ディスク・ドライブのコピー』
- 184 ページの『ディスク・ドライブの拡張』
- 185 ページの『システム・ドライブの拡張』
- 186 ページの『統合 Windows サーバー・ディスク・ドライブのリンク解除』
- 186 ページの『統合 Windows サーバー・ディスク・ドライブの削除』

統合サーバーからの i5/OS 統合ファイル・システムへのアクセス

統合サーバーから IBM iSeries Support for Windows Network Neighborhood (iSeries NetServer) を介して、i5/OS 統合ファイル・システムにアクセスすることができます。これによって、i5/OS 上のファイル・システム・リソースの処理が容易になります。iSeries NetServer の使用については、以下を参照してください。

- iSeries NetServer ファイル共有の作成
- iSeries NetServer を使用するための PC クライアントのセットアップ
- Windows クライアントによる iSeries NetServer ファイル共有へのアクセス

詳しくは、68 ページの『iSeries NetServer の使用可能化』を参照してください。

統合サーバー・ディスク・ドライブについての情報の取得

統合サーバー・ディスク・ドライブ (ネットワーク・サーバー記憶域) の使用中の割合やそのフォーマットを知りたい場合は、i5/OS から情報を入手することができます。

ディスク・ドライブ情報を入手するには、以下のステップを行います。

1. iSeries ナビゲーターで、「統合サーバー管理」 → 「すべての仮想ディスク」を選択します。
2. 示されたリストでディスク・ドライブを選択します。
3. ディスク・ドライブを右マウス・ボタンでクリックして「プロパティ」を選択するか、または iSeries ナビゲーターのツールバーで該当するアイコンをクリックします。

CL コマンドを使用する場合は、Work with Network Server Storage Spaces (WRKNWSSTG) を参照してください。

統合 Windows サーバーへのディスク・ドライブの追加

統合サーバーがアプリケーションおよびデータ用のディスク・ドライブと見なすものを作成しフォーマットする作業の一環として、ネットワーク・サーバー記憶域を i5/OS 上に作成します。ネットワーク・サーバー記憶域の概念情報については、176 ページの『統合 Windows サーバーのディスク・ドライブ』を参照してください。統合サーバー・ディスク・ドライブ (ネットワーク・サーバー記憶域) を追加するには、以下のタスクを実行します。

1. 『統合サーバー・ディスク・ドライブの作成』。
2. 182 ページの『ディスク・ドライブと統合サーバーのリンク』。
3. 183 ページの『統合サーバー・ディスク・ドライブのフォーマット』。

統合サーバー・ディスク・ドライブの作成

統合 Windows サーバーにディスク・スペースを追加するための最初のステップとして、統合サーバー・ディスク・ドライブ (ネットワーク・サーバー記憶域) を作成します。ディスク・ドライブの作成に要する時間は、作成するドライブのサイズに比例します。ディスク・ドライブを作成したら、統合サーバーのネットワーク・サーバー記述にそれをリンクし (182 ページの『ディスク・ドライブと統合サーバーのリンク』を参照)、それをフォーマットする必要があります。183 ページの『統合サーバー・ディスク・ドライブのフォーマット』を参照してください。

統合サーバー・ディスク・ドライブを作成するには、以下のステップを行います。

1. iSeries ナビゲーターで、「統合サーバー管理」を選択します。
2. 「すべての仮想ディスク」フォルダーを右マウス・ボタンでクリックして「新規ディスク」をクリックするか、または iSeries ナビゲーターのツールバーで該当するアイコンをクリックします。
3. ディスク・ドライブの名前と記述を指定します。
4. 別のディスクからデータを複写する場合は、「別のディスクのデータを使ったディスクの初期設定 (Initialize disk with data from another disk)」を選択します。次に、複写するデータの入っているソース・ディスクを選択します。
5. ディスク容量を指定します。
6. ディスクを収めるディスク・プール (補助記憶域プール) を選択します。
7. ディスク用の計画ファイル・システムを選択します。

注: Windows でディスクをフォーマットする場合、必要に応じて別のファイル・システムを選択することができます。

8. Windows クラスタ・クォーラム・リソース・ディスクを作成する場合には、クラスタ属性を指定します。
9. ディスクの作成後すぐにそれをサーバーにリンクする場合、「サーバーへのディスクのリンク」をチェックしてリンク属性を入力します。

10. 「OK」をクリックします。

CL コマンドを使用する場合は、CRTNWSSTG を参照してください。

注:

1. 別個の操作として新規のディスク・ドライブをリンクするには、『ディスク・ドライブと統合サーバーのリンク』を参照してください。
2. 作成されるディスクは、Windows の「ディスク管理」または DISKPART コマンド行ユーティリティーを使用して、区画化およびフォーマットする必要があります。
3. 独立ディスク・プール (ASP) 内のディスク・ドライブを使用してサーバーを作成または始動する場合は、そのディスク・プール・デバイスが使用可能である必要があります。

ディスク・ドライブと統合サーバーのリンク

統合 Windows サーバーが統合サーバー・ディスク・ドライブ (ネットワーク・サーバー記憶域) をハード・ディスク・ドライブとして認識できるようにするために、それら 2 つを一緒にリンクする必要があります。その前にディスク・ドライブを作成しておかなければなりません。181 ページの『統合サーバー・ディスク・ドライブの作成』を参照してください。新しい統合サーバー・ディスク・ドライブを作成してリンクすると、それは統合サーバーには新規ハード・ディスク・ドライブとして示されます。その後、それを使用できるようにするために、フォーマットする必要があります。183 ページの『統合サーバー・ディスク・ドライブのフォーマット』を参照してください。

ディスク・ドライブを統合サーバーにリンクするには、以下のステップを行います。

1. ディスク・ドライブを動的にリンクしない場合は、統合サーバーをシャットダウンします。163 ページの『統合サーバーの開始と停止』を参照してください。
2. iSeries ナビゲーターで、「**統合サーバー管理**」 → 「**すべての仮想ディスク**」を選択します。
3. 使用可能なディスク・ドライブを右マウス・ボタンでクリックして「**リンクの追加**」を選択するか、またはドライブを選択して iSeries ナビゲーターのツールバーから該当するアイコンをクリックします。
4. ディスクのリンク先にしたいサーバーを選択します。
5. 使用可能なリンク・タイプを 1 つと、リンク順序位置を選択します。
6. ディスクを iSCSI 接続サーバーにリンクする場合、使用可能な記憶域パスの 1 つを選択します。
7. 使用可能なデータ・アクセス・タイプを 1 つ選択します。
8. 「OK」をクリックします。
9. ディスク・ドライブを動的にリンクしない場合は、統合サーバーを始動します。163 ページの『統合サーバーの開始と停止』を参照してください。

CL コマンドを使用する場合は、ADDNWSSTGL を参照してください。

そのディスク・ドライブが、まだフォーマットされていない新規のディスク・ドライブの場合は、183 ページの『統合サーバー・ディスク・ドライブのフォーマット』を参照してください。

ドライブの英字を使い切った場合のディスク・ドライブの管理:

統合サーバーにリンクできるディスク・ドライブの最大数は、Windows で使用可能なドライブ名の数より大きくなります。すべてのドライブにドライブ文字が付くのではないため、サーバーにリンクしたすべての記憶域を利用するには他のオプションを使う必要があります。以下に、サーバーにリンクされたすべてのディスク・ドライブを利用するためのオプションを 2 つ示してあります。

1. スパン・ボリューム・セットを使って複数のディスク・ドライブでディスク・ドライブ文字を構成することができます。

- 注: ボリューム・セットを作成すると、新規のボリューム・セットに使用するパーティション上にある既存のデータはすべて消去されます。サーバーのセットアップ時にボリューム・セットについて考慮しなければなりません。
- a. 「**ディスクの管理**」で各ディスク・ドライブ番号を右マウス・ボタンでクリックしてから、ポップアップ・メニューで「**動的ディスクへのアップグレード... (Upgrade to Dynamic Disk...)**」を選択します。
 - b. ディスク・ドライブの区画を右マウス・ボタンでクリックしてから、ポップアップ・メニューで「**ボリュームの作成... (Create Volume...)**」を選択します。
 - c. ボリュームの作成ウィザードに従って、確実に複数のディスクを追加しながらスパン・ボリュームを作成します。注: このフィーチャーが便利なのは、ボリュームがいっぱいになったときに、サーバーをリブートしなくても、ディスクを動的に追加して、ただちにスパン・ボリュームに結合できるからです。
2. 既存のディスク・ドライブ文字のサブディレクトリの上にディスク・ドライブをマウントすることができます。
- a. NTFS でフォーマットされているディスク・ドライブ文字の上にディレクトリを作成します。たとえば、MD C:¥MOUNT1 を作成します。
 - b. 「**ディスクの管理**」で、フォーマットしようとするディスク・ドライブ区画をクリックし、ポップアップ・メニューで「**フォーマット (Format)**」を選択します。
 - c. ドライブのフォーマットが完了したら、もう一度ディスク・ドライブ区画を右マウス・ボタンでクリックし、ポップアップ・メニューで「**ドライブの英字とパスの変更... (Change Drive Letter and Path...)**」を選択します。
 - d. 「**追加**」を選択します。
 - e. 「**この NTFS フォルダーにマウント (Mount in this NTFS folder:)**」ラジオ・ボタンを選択します。
 - f. 「**ブラウズ**」ボタンを使って、ステップ 1 で作成した C:¥MOUNT1 ディレクトリを探します。
 - g. 「**OK**」をクリックし、そのディレクトリをこのディスク・ドライブのマウント・ポイントにします。

統合サーバー・ディスク・ドライブのフォーマット

統合 Windows サーバー・ディスク・ドライブ (ネットワーク・サーバー記憶域) を使用するには、フォーマットしなければなりません。フォーマットする前に、まずディスク・ドライブを作成 (181 ページの『統合サーバー・ディスク・ドライブの作成』を参照) およびリンク (182 ページの『ディスク・ドライブと統合サーバーのリンク』を参照) してから、i5/OS から Windows サーバーを開始しなければなりません (163 ページの『統合サーバーの開始と停止』を参照)。

- 注: サーバー記憶域リンクの追加 (ADDNWSSTGL) コマンドの動的記憶域リンク・パラメーターを使用してサーバーをオンにしている間は、サーバーはディスク・ドライブを動的にリンクすることができません。

ディスク・ドライブをフォーマットするには、次のステップを実行します。

1. 統合 Windows サーバー・コンソールで、「**スタート**」メニューから、「**プログラム**」、「**管理ツール**」、「**コンピュータの管理**」の順に選択します。
2. 「**記憶域**」をダブルクリックします。
3. 「**ディスクの管理**」をダブルクリックします。

- | 4. 新規区画を作成するには、区画を作成する基本ディスク上の未割り振りスペースを右マウス・ボタンでクリックしてから、「**新規区画**」をクリックします。
- | 5. プロンプトに従って、新しいドライブをフォーマットします。
 - | a. ボリューム・ラベルの記憶域名を指定します。
 - | b. ディスク・ドライブの作成時に指定したファイル・システムを選択します。
 - | c. 今作成された記憶域に対してクイック・フォーマットを選択します。これは、割り振り時に i5/OS によってロー・レベル・フォーマットされています。

ディスク・ドライブのコピー

既存のディスク・ドライブからデータをコピーすれば、新規の統合 Windows サーバー・ディスク・ドライブ (ネットワーク・サーバー記憶域) を作成することができます。

ディスク・ドライブをコピーするには、以下のステップを行います。

- 1. 「**統合サーバー管理**」 -> 「**すべての仮想ディスク**」を展開します。
- 2. 示されたリストでディスク・ドライブを選択します。
- 3. ディスク・ドライブを右マウス・ボタンでクリックして「**新規のベース (New Based On)**」を選択するか、または iSeries ナビゲーターのツールバーから該当するアイコンをクリックします。
- 4. ディスク・ドライブの名前と記述を指定します。
- 5. ディスク容量を指定します。個々のファイル・システム形式別の有効なディスク・サイズに関する詳細は、オンライン・ヘルプを参照してください。コピーの際にディスクのサイズを増やしたい場合は、もっと大きいサイズを指定することができます。ディスクの拡張した部分は、区画化されていない空きスペースとなります。

| **注:** DISKPART コマンド行ユーティリティーは、追加のフリー・スペースを使用するために既存の区画
| を拡張するのに使用できます。詳細および制限については、DISKPART 用の Microsoft サポート技
| 術情報にある資料を参照してください。

- 6. ディスクを収めるディスク・プール (補助記憶域プール) を選択します。
- 7. 「**OK**」をクリックします。

CL コマンドを使用する場合は、Create Network Storage Space (CRTNWSSTG) を参照してください。

ディスク・ドライブの拡張

| ディスク・ドライブをコピーせずに、仮想ディスク・ドライブ (ネットワーク・サーバー記憶域) を拡張す
| ることができます。ブート・ディスクの拡張について詳しくは、185 ページの『システム・ドライブの拡
| 張』を参照してください。


| ディスク・ドライブを拡張するには、以下のステップを行います。

- | 1. 「**統合サーバー管理**」 -> 「**すべての仮想ディスク**」を展開します。
- | 2. 示されたリストでディスク・ドライブを選択します。
- | 3. ディスク・ドライブを右マウス・ボタンでクリックして「**プロパティ**」を選択するか、または iSeries
| ナビゲーターのツールバーで該当するアイコンをクリックします。
- | 4. ディスク・ドライブのプロパティ・シートの「**容量**」タブをクリックします。
- | 5. 「**新規容量**」フィールドで、増大したディスク・サイズを指定します。個々のファイル・システム形式
| 別の有効なディスク・サイズに関する詳細は、オンライン・ヘルプを参照してください。ディスクの拡
| 張した部分は、区画化されていない空きスペースとなります。

6. 「OK」をクリックします。
7. ディスクがアクティブなサーバーにリンクされている場合、ディスクの拡張時に、サーバーでディスク・ドライブが一時的に使用不可になることを示す確認パネルが表示されます。「変更」をクリックしてこれが受け入れ可能であることを確認するか、「キャンセル」をクリックしてディスク拡張操作をキャンセルします。

注:


1. ディスクは拡張時に、アクティブなサーバーへリンクすることはできません。サーバーがディスク・ドライブの動的リンク解除をサポートしている場合、サーバーがアクティブである間は上記の手順を実行できます。この場合、ディスクは動的にリンク解除され、その後拡張されてから、サーバーに再リンクされます。このため、ディスクの拡張時には、サーバーでディスク・ドライブが一時的に使用不可になります。
2. DISKPART コマンド行ユーティリティーは、追加のフリー・スペースを使用するために既存の区画を拡張するのに使用できます。

注: DISKPART は、Windows Server 2003 ではデフォルトで使用可能です。これは、Microsoft  Web ページ (www.microsoft.com) からダウンロードすることもできます。詳細および制限については、DISKPART 用の Microsoft サポート技術情報にある資料を参照してください。

3. 既存のネットワーク・サーバー記憶域の拡張には、記憶域が最初に割り振られた方法に応じて幾つかの制限があります。

CL コマンドを使用する場合は、ネットワーク記憶域スペースの変更 (CHGNWSSTG) を参照してください。CHGNWSSTG を使用してディスクを拡張する場合、ディスクをアクティブなサーバーにリンクすることはできません。サーバーがアクティブである場合、CHGNWSSTG は自動的にディスクのリンク解除および再リンクを行いません。

システム・ドライブの拡張

重要: システム・ドライブは拡張する前にバックアップしなければなりません。DISKPART ユーティリティーの使用について詳しくは、Microsoft  Web ページ (www.microsoft.com) を参照してください。

システム・ドライブを拡張するには、以下のステップを実行します。

1. サーバーをシャットダウンします。163 ページの『統合サーバーの開始と停止』を参照してください。
2. サーバーからシステム・ドライブ・ディスクをリンク解除します。186 ページの『統合 Windows サーバー・ディスク・ドライブのリンク解除』を参照してください。
3. ディスクのサイズを変更します。184 ページの『ディスク・ドライブの拡張』を参照してください。
4. ディスクを一時サーバーのネットワーク・サーバー記述にデータ・ディスクとしてリンクします。182 ページの『ディスク・ドライブと統合サーバーのリンク』を参照してください。
5. 一時サーバーを始動します。163 ページの『統合サーバーの開始と停止』を参照してください。
6. 一時サーバーの Windows コンソールで、DISKPART ユーティリティーを使用してディスクの区画を拡張します。
7. 一時サーバーをシャットダウンします。163 ページの『統合サーバーの開始と停止』を参照してください。
8. 一時サーバーからディスクをリンク解除します。186 ページの『統合 Windows サーバー・ディスク・ドライブのリンク解除』を参照してください。

- 1 9. 拡張されたディスクをシステム・ディスクとして元のサーバーにリンクします。182 ページの『ディスク・ドライブと統合サーバーのリンク』を参照してください。
- 1 10. 元のサーバーを始動します。163 ページの『統合サーバーの開始と停止』を参照してください。

統合 Windows サーバー・ディスク・ドライブのリンク解除

- 1 統合サーバー・ディスク・ドライブ (ネットワーク・サーバー記憶域) のリンクを解除すると、統合サーバーとのリンクが切断されるため、ユーザーはアクセスできなくなります。動的にリンク解除できる場合の詳細については、176 ページの『統合 Windows サーバーのディスク・ドライブ』を参照してください。

ディスク・ドライブをリンク解除するには、以下のステップを行います。

- 1 1. ディスク・ドライブを動的にリンク解除しない場合は、統合サーバーをシャットダウンします。163 ページの『統合サーバーの開始と停止』を参照してください。
- 1 2. iSeries ナビゲーターで、「**統合サーバー管理**」 → 「**すべての仮想ディスク**」を選択するか、「**統合サーバー管理**」 → 「**サーバー**」 → 「**servername**」 → 「**リンクされた仮想ディスク**」を選択します。ここで、**servername** はディスクのリンク先であるサーバーの名前です。
- 1 3. リンク解除するディスク・ドライブを右マウス・ボタンでクリックして「**リンクの除去**」を選択するか、またはドライブを選択して iSeries ナビゲーターのツールバーから該当するアイコンをクリックします。
4. **オプション:** ドライブの順序を変更するには、「**リンク順序の圧縮**」をクリックします。
5. 「**除去**」をクリックします。

CL コマンドを使用する場合は、サーバー記憶域リンク除去 (RMVNWSSTGL) を参照してください。

統合 Windows サーバー・ディスク・ドライブの削除

ディスク・ドライブ (ネットワーク・サーバー記憶域) を削除するとディスク・ドライブ上のデータが破棄されて、他の目的に使用できるように iSeries ディスク記憶域を解放します。

ディスク・ドライブを削除する場合、事前に統合サーバーからリンク解除しなければなりません。『統合 Windows サーバー・ディスク・ドライブのリンク解除』を参照してください。リンク解除を完了した後で削除することができます。

ディスク・ドライブを削除するには、次のステップを行います。

- 1 1. iSeries ナビゲーターで、「**統合サーバー管理**」 → 「**すべての仮想ディスク**」を選択します。
2. 示されたリストでディスク・ドライブを選択します。
3. そのディスク・ドライブを右マウス・ボタンでクリックして「**削除**」を選択するか、または iSeries ナビゲーターのツールバーで該当するアイコンをクリックします。
4. 確認パネルで「**削除**」をクリックします。

CL コマンドを使用する場合は、NWS 記憶スペース削除 (DLTNWSSTG) を参照してください。

統合サーバーの除去時のディスク・ドライブの削除

統合サーバーを手動で除去する時は、そのサーバーのネットワーク・サーバー記述 (NWSD) に関連したディスク・ドライブ (ネットワーク・サーバー記憶域) を削除する必要があります。ご自分が所有するユーザー作成のディスク・ドライブも削除します。

Windows サーバー導入 (INSWNTSVR) コマンドで作成されたオブジェクトを除去するために、Windows サーバーの削除 (DLTWNTSVR) コマンドが用意されています。これによって、ネットワーク・サーバー記述 (NWS)、回線記述 (LIND)、記憶域 (NWSSTG)、TCP インターフェース、制御装置記述 (CTLD)、および装置記述 (DEVD) が除去されます。システムから統合サーバーを永続的に除去する場合は、この方法をお勧めします。

- | サーバー用のシステム・ドライブおよびインストール・ドライブとして i5/OS が事前定義したディスク・ドライブもすべて削除する必要があります。

サーバーに関連付けられているディスク・ドライブを確認するには、180 ページの『統合サーバー・ディスク・ドライブについての情報の取得』の項を参照してください。

統合 Windows サーバーでの Windows ディスク管理プログラムの使用

Windows ディスク管理プログラムを使用すれば、ディスク・ドライブ (ネットワーク・サーバー記憶域) をそれぞれ個別の物理ディスク・ドライブであるものとして管理することができます。ドライブ名の割り当て、区分化の実行、ボリューム・セットの作成などの機能を十分に活用できます。

Windows ディスク管理プログラムを使用する場合には、以下に配慮してください。

- ディスク・ドライブをリンクする場合、ドライブの相対順序位置を割り当てることができますが、これを i5/OS で自動的に実行させることもできます。
- Windows ディスク管理を使用して光ドライブ名を割り当てないと、統合サーバー上のすべてのディスク・ドライブの後の次に使用できるドライブ名として光ドライブが表示されます。どのユーザー定義ディスク・ドライブも NWS にリンクしていないと、一般的に光ドライブはドライブ E として表示されます。

第 10 章 装置の共用

iSeries 装置を使用できるのが、統合 Windows サーバーの利点の 1 つです。Windows サーバーから iSeries 光ディスク装置、磁気テープ・ドライブ、および印刷装置を使用することができます。

iSeries 装置にアクセスするには、以下のようなタスクを行います。

- i5/OS と Windows サーバーでは装置を呼ぶ名称が異なるので、まず使用しようとしている正しい装置記述とハードウェア・リソース名を知る必要があります。『iSeries 装置の装置記述とハードウェア・リソース名の確認』を参照してください。
- 統合サーバー上で光ディスク・ドライブを使用するには、i5/OS からそのドライブをオンに変更します。『統合 Windows サーバーでの iSeries 光ディスク装置の使用』を参照してください。
- 統合 Windows サーバーへのドライブの割り振り、テープのフォーマット、サーバーどうしのドライブの相互転送、元の i5/OS へのドライブの返送に関する詳細は、190 ページの『統合 Windows サーバーでの iSeries 磁気テープ・ドライブの使用』の項を参照してください。
- 195 ページの『統合 Windows サーバーから iSeries 印刷装置への印刷』の項を参照してください。

iSeries 装置の装置記述とハードウェア・リソース名の確認

i5/OS 上で iSeries 装置を参照するには、装置記述名を使う必要があります。統合 Windows サーバーからそのような装置を参照するには、ハードウェア・リソース名を使う必要があります。名前が違っていたり、誤った名前を使用したりすると、誤った装置が参照されます。

ハードウェア・リソース名を判別し、装置記述名と同じであるかどうかを確認する場合、次のステップを行います。

1. i5/OS コマンド行で `DSPDEV device_description_name` と入力して、Enter を押します。
2. 「リソース名」フィールドには、この装置のハードウェア・リソース名が入っています。この名前が「装置記述」フィールドと同じになっているかどうかを確かめてください。名前が違う場合は、統合 Windows サーバーと i5/OS のどちらから作業するかに応じて、必ず適切な名前を使用してください。

一部の磁気テープ装置は複数の装置記述で報告されます。テープ・ライブラリー (3590、3570 など) は、装置 (TAPxx) に加えてテープ・ライブラリー (TAPMLBxx) としても報告されます (xx は数値)。IBM 統合サーバーはテープ・ライブラリーをサポートしていません。このため、装置にテープ・ライブラリー記述がある場合は、Windows サーバーでその装置をロックするときは、あらかじめその磁気テープ装置とテープ・ライブラリー装置の両方をオフに変更してください。

統合 Windows サーバーでの iSeries 光ディスク装置の使用

Windows サーバーは、ローカル光ディスク装置と同じように iSeries 光ディスク装置を使用することができます。Windows サーバーの「マイ コンピュータ」フォルダーでは、この iSeries 光ディスク装置は通常のローカル光ディスク装置として示されます。

iSeries に論理区画がある場合、光ディスク装置は単一の区画に割り振られます。別々の区画にある統合サーバーどうしがこの装置を共用することはできません。また、光ディスク装置は、使用する NWSD に割り振る (ロックする) 必要があります。

光ディスク装置を統合 Windows サーバーに割り振るには、先にオンに変更しなければなりません。光ディスク装置がオンに変更されていない場合には、以下のステップに従ってオンにしてください。

1. i5/OS コマンド行で WRKCFGSTS *DEV *OPT と入力し、実行キーを押します。
2. 正しい光ディスク装置 (通常は OPT01) の横の Opt 欄に 1 と入力して、光ディスク装置をオンに変更します。
3. 実行キーを押すと、光ディスク装置はオンに変更されます。

光ディスク装置をロックするには、以下のステップを行います。

1. 「スタート」、「プログラム」、「IBM iSeries」、「IBM iSeries 統合サーバー・サポート」を順にクリックします。
2. 「IBM iSeries 統合サーバー・サポート」を展開します。
3. 「ネットワーク・サーバー記述」名を拡張表示します。
4. 「iSeries 装置」を選択します。
5. 装置名を選択します。
6. 「全タスク (All Tasks)」、「装置のロック (Lock Device)」を右マウス・ボタンでクリックして選択します。

統合 Windows サーバーから iSeries 光ディスク装置を使用して問題が生じた場合は、235 ページの『光ディスク装置の問題』を参照してください。

- 注: 光ディスク装置をアンロックする前に統合サーバーに障害が起きた場合、i5/OS またはその他の統合サーバーはこの光ディスク装置を使えなくなります。その場合、WRKCFGSTS *DEV *OPT を使用していったん光ディスク装置をオフに変更してから、再びオンに変更してロックを外します。

統合サーバーから iSeries への光ディスク装置の制御の返還

光ディスク装置を i5/OS から使用するには、まず統合サーバーからアンロックします。統合サーバーから光ディスク装置をアンロックできるのは、そのドライブにロックをかけたユーザーか、管理者またはバックアップ・オペレーターの権限を保有しているユーザーだけです。

iSeries 光ディスク装置の制御を統合サーバーから iSeries に渡すには、次のステップを行います。

1. 「スタート」、「プログラム」、「IBM iSeries」、「IBM iSeries 統合サーバー・サポート」を順にクリックします。
2. 「IBM iSeries 統合サーバー・サポート」を展開します。
3. 「ネットワーク・サーバー記述」名を拡張表示します。
4. 「iSeries 装置」を選択します。
5. アンロックしたい装置を選択します。
6. 「全タスク (All Tasks)」、「装置のアンロック (Unlock Device)」を右マウス・ボタンでクリックして選択します。

統合 Windows サーバーでの iSeries 磁気テープ・ドライブの使用

iSeries 磁気テープ・ドライブは、PC サーバーに通常接続されるドライブよりはるかに高速に稼働するので、統合サーバーにそのドライブを割り振れば、PC サーバーで利用できるものより迅速なテープ・アクセス手段になります。193 ページの『サポートされている iSeries 磁気テープ・ドライブ』を参照してください。

同じ iSeries システム内の複数の統合 Windows サーバーがすべて (ただし同時ではない) 1 つの磁気テープ・ドライブにアクセスできるため、複数の統合サーバーに 1 つの磁気テープ・ドライブを割り振るだけで済みます。

注:

1. 磁気テープ・ドライブを統合 Windows サーバーと i5/OS の専用にすることはできても、両方のシステムが同時に同じ磁気テープ・ドライブを使用することはできません。この 2 つのオペレーティング・システムには、テープの異なるフォーマットを必要とします。統合サーバーと i5/OS の両方で、同じテープを再フォーマットせずに使用することはできません。
2. iSeries に論理区画がある場合は、磁気テープ・ドライブは単一の区画に割り振られます。他の区画にある複数の統合サーバーがこのドライブを共用することはできません。

統合サーバーから iSeries 磁気テープ・ドライブを使用するには、以下のタスクを実行する必要があります。


- 『i5/OS での統合 Windows サーバー用のテープのフォーマット』。
- i5/OS から磁気テープ・ドライブをオフに変更してから統合サーバー上でロックすることによって、iSeries 磁気テープ・ドライブを統合サーバーに割り振ります。192 ページの『統合 Windows サーバーに対する iSeries テープ・ドライブの割り振り』を参照してください。
- iSeries 磁気テープ・ドライブの制御権を別の統合サーバーに渡します。194 ページの『統合 Windows サーバー間での iSeries テープ・ドライブと光ディスク装置の制御権移動』を参照してください。
- 統合サーバーから磁気テープ・ドライブに制御権を戻して、i5/OS が使用できるようにします。正しくフォーマットされた磁気テープを使用してください。193 ページの『統合 Windows サーバーから iSeries へのテープ・ドライブの制御の返還』を参照してください。

iSeries 磁気テープ・ドライブに問題が生じた場合は、235 ページの『磁気テープ関連の問題』を参照してください。

磁気テープ装置のドライバーのインストール

サポートされる磁気テープ装置のドライバーについて詳しくは、『Windows サーバー用のサポートされる磁気テープ装置 (英語)』を参照してください。

ドライバーのインストールには、特別なアクションは全く必要ありません。ドライバー提供者によって提供される説明で十分なはずですが、新規の磁気テープ・ドライブを使用する場合、その磁気テープ・ドライブは xSeries サーバーで使用可能なドライブと同じに見えます。その装置は、装置のロック/アンロック・ユーティリティーで依然としてタイプ・モデル番号別にリストされています。

磁気テープ装置が一度ロックされ、サーバーがリブートされると、取り外し可能な Storage Manager、および一部のバックアップ・アプリケーションにおいて、装置の余分なインスタンスが存在しているように見える場合があります。これは通常の動作です。これら余分のインスタンスを削除するほうが安全かもしれません。ご使用の資料を調べてください。最新の情報については、iSeries 統合 xSeries ソリューションの Web サイト (www.ibm.com/servers/eserver/iseries/integratedxseries/windows/tape_driver_migration.html) にある「磁気テープ・ドライバーのマイグレーション (英語)」 を参照してください。

i5/OS での統合 Windows サーバー用のテープのフォーマット

統合 Windows サーバーで iSeries 磁気テープ・ドライブを使用するには、サーバーが認識するテープ・フォーマットを使用する必要があります。Windows で受け入れられるラベルなしのテープを作成するには、i5/OS テープの初期化 (INZTAP) コマンドを使用します。

テープをフォーマットするには、以下のステップを実行してください。

- 使用したいテープを iSeries 磁気テープ・ドライブに入れます。
- i5/OS コマンド行に、次のように入力します。

```
INZTAP DEV(tap01) NEWVOL(*NONE) NEWOWNID(*BLANK) VOL(*MOUNTED)
CHECK(*NO) DENSITY(*CTGTYPE) CODE(*EBCDIC)
```

tap01 は磁気テープ・ドライブの名前です。 Enter キーを押します。

統合 Windows サーバーに対する iSeries テープ・ドライブの割り振り

統合 Windows サーバー・コンソールから iSeries 磁気テープ・ドライブを使用するには、i5/OS 上でオフに変更してから、統合サーバー上でロックしなければなりません。装置のロックは、アプリケーションまたはそのサービスを開始する前に実行してください。

注: 一部の磁気テープ装置は複数の装置記述で報告されます。テープ・ライブラリー (3590、3570 など) は、装置 (TAPxx) に加えてテープ・ライブラリー (TAPMLBxx) としても報告されます (xx は数値)。 IBM iSeries 統合サーバーはテープ・ライブラリーをサポートしていません。このため、装置にテープ・ライブラリー記述がある場合は、統合サーバーでその装置をロックする前に、その磁気テープ装置とテープ・ライブラリー装置の両方をオフに変更してください。

iSeries 磁気テープ・ドライブの制御を integrated サーバーに渡すには、次のステップを行います。

1. i5/OS 上の磁気テープ・ドライブをオフに変更します。

- 「iSeries ナビゲーター」からこれを行うには、次のようにします。
 - a. 「構成およびサービス」 → 「ハードウェア」 → 「テープ・デバイス」をクリックします。
 - b. 「スタンドアロン装置」または「テープ・ライブラリー」をクリックします。
 - c. 装置またはライブラリーを右マウス・ボタンでクリックしてから、「使用不可にする」を選択します。
- i5/OS 文字ベース・インターフェースからこれを行うには、次のようにします。
 - a. i5/OS のコマンド行に WRKCFGSTS *DEV *TAP と入力して、Enter キーを押します。「構成状況処理」画面が表示されます。

注: WRKCFGSTS *DEV *TAPMLB と入力すると、テープ・ライブラリー装置の一覧が表示されます。

- b. 磁気テープ・ドライブの装置名の横の Opt 欄に 2 と入力して、磁気テープ・ドライブをオフに変更します。
- c. Enter キーを押します。磁気テープ・ドライブはオフに変更されます。

2. 次のようにして、統合サーバー上の磁気テープ装置をロックします。

- a. Windows コンソールから、「スタート」 → 「プログラム」 → 「IBM iSeries」 → 「IBM iSeries 統合サーバー・サポート」をクリックします。
- b. 「IBM iSeries 統合サーバー・サポート」を展開します。
- c. 「ネットワーク・サーバー記述」名を拡張表示します。
- d. 「iSeries 装置」を選択します。
- e. ロックしたいテープ・オブジェクトを選択します。
- f. 「全タスク (All Tasks)」、「装置のロック (Lock Device)」を右マウス・ボタンでクリックして選択します。

3. 磁気テープ装置をアプリケーションが認識できるようにするのに他の情報が必要な場合は、194ページの『アプリケーション用の iSeries 磁気テープ装置の識別』を参照してください。問題がある場合、235ページの『磁気テープ関連の問題』を参照してください。

統合 Windows サーバーから iSeries へのテープ・ドライブの制御の返還

現在統合サーバー上でロックのかかっている磁気テープ・ドライブを i5/OS から使用するには、まず統合サーバーからその磁気テープ・ドライブをアンロックし、次に i5/OS からオンに変更します。Windows サーバーから磁気テープ・ドライブをアンロックできるのは、そのドライブにロックをかけたユーザーか、管理者またはバックアップ・オペレーターの権限を保有しているユーザーだけです。

iSeries 磁気テープ・ドライブの制御を統合 Windows サーバーから iSeries に渡すには、次のステップを行います。

1. 統合 Windows サーバーのコンソールから、磁気テープ装置をアンロックします。
 - a. 「スタート」、「プログラム」、「IBM iSeries」、「IBM iSeries 統合サーバー・サポート」を順にクリックします。
 - b. 「IBM iSeries 統合サーバー・サポート」を展開します。
 - c. 「ネットワーク・サーバー記述」名を拡張表示します。
 - d. 「iSeries 装置」を選択します。
 - e. ロックしたいテープ・オブジェクトを選択します。
 - f. 「アクション (Action)」 「全タスク (All Tasks)」、「装置のアンロック (Unlock Device)」を選択します。
2. i5/OS コンソールから、装置を i5/OS で使用できるようにします。
 - 「iSeries ナビゲーター」から、次のようにします。
 - a. 「構成およびサービス」→「ハードウェア」→「テープ・デバイス」をクリックします。
 - b. 「スタンドアロン装置」または「テープ・ライブラリー」をクリックします。
 - c. 装置またはライブラリーを右マウス・ボタンでクリックしてから、「使用可能にする」を選択します。
 - i5/OS コマンド行インターフェースから、次のようにします。
 - a. i5/OS のコマンド行に WRKCFGSTS *DEV *TAP と入力して、Enter キーを押します。「構成状況処理」画面が表示されます。
 - b. テープ・ドライブ装置名 (たとえば TAP01) の横の「Opt」欄に、1 と入力して磁気テープ・ドライブをオンに変更します。
 - c. Enter キーを押すと、磁気テープ・ドライブはオンに変更されます。
 - d. テープを i5/OS 用にフォーマットされたテープに替えます。

サポートされている iSeries 磁気テープ・ドライブ

統合 Windows サーバーから iSeries 磁気テープ・ドライブを使用できるかどうかは、磁気テープ装置モデル、磁気テープ・コントローラー、およびメディア・タイプによって決まります。

どの装置がサポートされているかの詳細は、「統合 xSeries ソリューション (英語)」 Web サイトを参照してください。

テープ・ライブラリーはライブラリーとしてはサポートされませんが、単一装置としてサポートされている場合があります。

自動カートリッジ機能 (ACF) および自動カートリッジ・ローダー (ACL) では、手動と自動モードの両方がサポートされます。ACL または ACF が自動モードの場合、バックアップ・アプリケーションがいっぱいになったテープを排出すると、次のテープが自動的にロードされます。Windows バックアップ・ユーティリティは、ユーザーが介入しなくても自動的にこれを実行します。Veritas の Backup Exec では、「ドライブからメディアを取り外し、「OK」を押してください。(Please remove the media from the drive, and respond OK.)」と表示されたダイアログ・ボックスが現れます。このダイアログ・ボックスで「OK」を押してください (Respond OK)」をクリックすると、バックアップは通常の仕方で行われます。

アプリケーション用の iSeries 磁気テープ装置の識別

i5/OS とは異なり、アプリケーションは、磁気テープ装置を参照する際に装置記述やハードウェア・リソース名を使用しません。磁気テープ装置は、アプリケーションでは以下の 3 通りのうちのいずれかの方法で表示されます。

- 製造機能型式番号
- 装置マップ
- Port-bus-target id-lun

これらの値が必要な場合は、以下のようにしてください。

1. 統合 Windows サーバーのコンソールで、「スタート」 → 「プログラム」 → 「管理ツール」 → 「コンピュータの管理」をクリックします。
2. 「システム ツール」をクリックします。
3. 「デバイス マネージャ」をクリックします。
4. 「テープ・デバイス」をダブルクリックします。
5. テープ装置を右マウス・ボタンでクリックします。
6. 「プロパティ」を選択します。
7. プロパティ・ボックスには、「全般」とマークされたタブと、「ドライバー」とマークされたタブの 2 つのタブがあります。「全般」タブには、装置の名前とバス番号、ターゲットの ID と LUN が表示されます。

iSeries 上のすべての磁気テープ装置のタイプが異なる場合、この情報だけで Windows アプリケーション内で各装置を区別できます。同じ製造機能型式番号の磁気テープ装置が複数ある場合は、どの磁気テープ装置がどれかを試してみても判別する必要があります。

統合 Windows サーバー間での iSeries テープ・ドライブと光ディスク装置の制御権移動

複数の統合サーバーがある場合、一度に 1 つだけが iSeries 磁気テープ・ドライブまたは光ディスク装置を使用できます。磁気テープ・ドライブと光ディスク装置の制御をサーバーからサーバーに移すには、それを一方のサーバー上でアンロックし、他方のサーバー上でロックする必要があります。

注: iSeries に論理区画がある場合は、磁気テープ・ドライブおよび光ディスク装置は単一の区画に割り振られ、他の区画にある複数の統合サーバーと共用することはできません。

iSeries 磁気テープ・ドライブまたは光ディスク装置の制御を統合サーバーどうしに移行するには、次のステップを行います。

ドライブの制御権をもつ統合サーバー・コンソール上で、次のようにします。

1. 「スタート」、「プログラム」、「IBM iSeries」、「IBM iSeries 統合サーバー・サポート」を順にクリックします。
2. 「IBM iSeries 統合サーバー・サポート」を展開します。
3. 「ネットワーク・サーバー記述」名を拡張表示します。
4. 「iSeries 装置」を選択します。
5. アンロックしたい装置を選択します。
6. 「アクション (Action)」 「全タスク (All Tasks)」、「装置のアンロック (Unlock Device)」を選択します。


制御を渡す先の統合サーバー・コンソール上で、磁気テープ・ドライブまたは光ディスク装置をロックします。

1. 「スタート」、「プログラム」、「IBM iSeries」、「IBM iSeries 統合サーバー・サポート」を順にクリックします。
2. 「IBM iSeries 統合サーバー・サポート」を展開します。
3. 「ネットワーク・サーバー記述」名を拡張表示します。
4. 「iSeries 装置」を選択します。
5. ロックしたい装置を選択します。
6. 「アクション (Action)」 「全タスク (All Tasks)」、「装置のロック (Lock Device)」を選択します。

統合 Windows サーバーから iSeries 印刷装置への印刷

印刷ジョブを i5/OS へ送るには、TCP/IP 印刷ができるように i5/OS 印刷装置を設定する必要があります。さらに、LPD/LPR プロトコル経由でその印刷装置を使用するよう統合サーバーを設定しなければなりません。ご使用の統合サーバーには、**Microsoft TCP/IP Printing Network Service** もインストールされていなければなりません。TCP/IP 印刷の詳細は、Windows の資料を参照してください。

i5/OS 印刷装置で印刷するように統合サーバーを設定するには、以下の作業を行ってください。

1. TCP/IP 印刷を行うために i5/OS 印刷装置を設定します。詳細は、「eServer iSeries TCP/IP 構成および解説書 」を参照してください。
2. i5/OS 印刷装置で印刷するように統合サーバーを設定するには、次のようにします。
 - a. Windows 2000 Server または Windows Server 2003 の「スタート」メニューから、「設定」、「プリンタ」をクリックします。「プリンタ」ウィンドウが表示されます。
 - b. 「プリンタの追加」アイコンをダブルクリックします。「プリンタの追加ウィザード」が起動します。
 - c. 「ネットワーク プリンタ」ボタンをクリックします。
 - d. 「プリンタの検索」パネルで印刷装置の名前を入力するか、または「次へ」をクリックして印刷装置を表示します。

第 11 章 i5/OS からの統合 Windows サーバー・ユーザーの管理


iSeries 上の Windows 環境の主な利点の 1 つは、ユーザー管理が同期されて単純化されることです。既存の i5/OS ユーザー・プロファイルとプロファイル・グループを統合 Windows サーバーに登録することができます。これは、それらのユーザーは、i5/OS へのログオンに使用するのと同じユーザー ID とパスワードのペアを使って Windows サーバーにログオンできることを意味します。i5/OS パスワードを変更した場合、Windows のパスワードも同じく変更されます。

この概念の詳細は、54 ページの『ユーザーおよびグループの概念』の項を参照してください。

以下に、実行できるタスクを一覧で示してあります。

- 『iSeries ナビゲーターによる Windows 環境への単一 i5/OS ユーザーの登録』
- 198 ページの『iSeries ナビゲーターによる Windows 環境への i5/OS グループの登録』
- 198 ページの『文字ベースのインターフェースによる Windows 環境への i5/OS ユーザーの登録』
- 199 ページの『ユーザー・テンプレートの作成』
- 200 ページの『テンプレートでのホーム・ディレクトリーの指定』
- 201 ページの『LCLPDMGT ユーザー・プロファイル属性の変更』
- 201 ページの『エンタープライズ識別マッピング (EIM)』
- 203 ページの『Windows 環境に対するユーザーの登録の終了』
- 204 ページの『Windows 環境に対するグループの登録の終了』
- 204 ページの『QAS400NT ユーザー』
- 206 ページの『統合 Windows サーバーへの登録と伝搬の禁止』

iSeries ナビゲーターによる Windows 環境への単一 i5/OS ユーザーの登録

ユーザーの i5/OS ユーザー・プロファイルが存在していなければ、それを作成します。i5/OS ユーザー・プロファイルの作成の詳細については、「iSeries 機密保護解説書 」を参照してください。

単一のユーザーを Windows 環境に登録するには、次のステップを行います。

1. 「iSeries ナビゲーター」で、「統合サーバー管理」→「サーバー」または「ドメイン」を展開します。
2. 示されたリスト中の選択可能な Windows ドメインまたはサーバーを右マウス・ボタンでクリックしてから、「ユーザー登録 (Enroll Users)」を選択します。


注: Windows ワークグループを選択しないでください。ワークグループへの登録はサポートされていません。

3. ユーザー名を選択して入力するか、またはリストでユーザー名を選択します。

- (オプション) ユーザー設定のベースとしてユーザー・テンプレートを使用する場合は、Windows でユーザーを作成するときにテンプレートとして活用する Windows ユーザーを指定します。ユーザーの登録後にユーザー・テンプレートを変更しても、その変更はユーザーに影響を与えないことに注意してください。
- 「登録 (Enroll)」をクリックします。

ユーザーの登録で問題が生じた場合は、243 ページの『ユーザーおよびグループの登録時の障害』を参照してください。

iSeries ナビゲーターによる Windows 環境への i5/OS グループの登録

以下の手順は、i5/OS グループのすべてのユーザーを Windows 環境に登録します。i5/OS ユーザーおよびグループ・プロファイルの作成の詳細については、「iSeries 機密保護解説書」を参照してください。

i5/OS グループとそのメンバーを Windows 環境に登録するには、次のステップを行います。

- 「統合サーバー管理」 → 「サーバー」または「ドメイン」を展開します。
- 示されたリスト中の選択可能な Windows ドメインまたはサーバーを右マウス・ボタンでクリックしてから、「グループの登録 (Enroll Groups)」を選択します。

注: Windows ワークグループを選択しないでください。ワークグループへの登録はサポートされていません。

- グループ名を入力するか、または未登録のグループをリストで選択します。
- (オプション) テンプレートを使用して新しいユーザーを作成するには、Windows でグループ内にユーザーを作成するときにテンプレートとして使用する Windows ユーザーを指定します。ユーザーの登録後にユーザー・テンプレートを変更しても、その変更はユーザーには影響を与えません。
- グループをドメインに登録しようとしていて、そのグループがドメインから認識されなければならない場合は、「グローバル (Global)」を選択します。それ以外の場合、「ローカル (Local)」を選択します。Windows サーバー・ローカル・グループには、ユーザーと Windows サーバー・グローバル・グループを入れることができますが、Windows サーバー・グローバル・グループに入れられるのはユーザーだけです。グループ・タイプについての詳細は、Windows のオンライン・ヘルプを参照してください。
- 「登録 (Enroll)」をクリックします。

グループ登録で問題が生じた場合は、243 ページの『ユーザーおよびグループの登録時の障害』を参照してください。

文字ベースのインターフェースによる Windows 環境への i5/OS ユーザーの登録

Windows 環境へのユーザーの登録

- i5/OS 文字ベースのインターフェースで、CHGNWSUSRA と入力して **F4** を押します。
- 「ユーザー・プロファイル」フィールドに、Windows 環境に登録する i5/OS ユーザー・プロファイルの名前を入力します。
- Enter** キーを 2 回押します。追加のフィールドが表示されます。
- Page Down** を押して、ユーザーを登録する対象の Windows ドメインと Windows ローカル・サーバーを入力します。

5. **Enter** を押して、変更内容を受け入れます。

関連する CL コマンド

表 4.

WRKUSRPRF	i5/OS ユーザー・プロファイルを処理します。
WRKNWSEN	Windows 環境に登録された i5/OS ユーザー・プロファイルを処理します。
CHGNSWUSRA	i5/OS ユーザーを Windows 環境に登録します。

ユーザー・テンプレートの作成

ユーザー登録テンプレートを使用すれば、ユーザーを i5/OS から Windows 環境により効率的に登録できます。同じ設定値を使って多数の新規ユーザーを手動で構成する代わりに、ユーザー登録テンプレートを使用すれば、自動構成を行うことができます。ユーザー登録テンプレートについての詳細は、『ユーザー登録テンプレート』を参照してください。

Windows テンプレートを作成するには、以下のステップに従います。

Windows 2000 Server または Windows Server 2003 のドメイン用:

1. 統合サーバー・コンソールで、「スタート」→「プログラム」→「管理ツール」→「**Active Directory ユーザーとコンピュータ**」をクリックします。
2. ドメイン名をクリックします。
3. 「**ユーザー**」を右クリックして、「**新規作成**」→「**ユーザー**」を選択します。
4. 「**ユーザー名**」および「**ログオン名**」フィールドに、テンプレート名として、*stduser* や *admtemp* のような明確な名前を入力します。「**次へ**」をクリックします。
5. さらに、「**ユーザーは次回ログオン時にパスワードの変更が必要**」チェック・ボックスを選択解除して、「**ユーザーはパスワードを変更できない**」、「**パスワードを無期限にする**」、および「**アカウントを無効にする**」チェック・ボックスを選択することを推奨します。これによって、いずれかのユーザーがテンプレートそのものを使って統合サーバーにアクセスするのを防げます。
6. テンプレート・アカウントのパスワードを入力しないでください。
7. 「**完了**」をクリックします。
8. グループ・メンバーシップを設定するには、右側のペインに表示されるドメイン・ユーザーおよびグループのリストの中にあるテンプレート名をダブルクリックします。「**所属するグループ**」タブをクリックし、「**追加**」をクリックして、必要なグループを追加します。

Windows 2000 Server または Windows Server 2003 のサーバー用:

1. 統合サーバー・コンソールから、次のようにします。
 - Windows 2000 Server で、「スタート」→「プログラム」→「管理ツール」→「**コンピュータの管理**」→「**ローカル ユーザーとグループ**」をクリックします。
 - Windows Server 2003 で、「スタート」→「プログラム」→「管理ツール」→「**コンピュータの管理**」→「**システム ツール**」→「**ローカル ユーザーとグループ**」をクリックします。
2. 「**システム ツール**」→「**ローカル ユーザーとグループ**」を選択します。
3. 「**ユーザー**」を右クリックして、「**新しいユーザー**」を選択します。
4. 「**ユーザー名**」フィールドに、テンプレート名として、*stduser* や *admtemp* のような明確な名前を入力します。

5. さらに、「ユーザーは次回ログオン時にパスワードの変更が必要」チェック・ボックスを選択解除して、「パスワードを無期限にする」、「ユーザーはパスワードを変更できない」、および「アカウントを無効にする」チェック・ボックスを選択することを推奨します。これによって、いずれかのユーザーがテンプレートそのものを使って Windows サーバーにアクセスするのを防げます。
6. 「作成」そして「閉じる」の順にクリックします。
7. 「ユーザー」をクリックするか、最新表示することにより、新規ユーザー・テンプレートが表示されません。
8. グループ・メンバーシップを設定するには、右側のペインに表示されるドメイン・ユーザーおよびグループのリストの中にあるテンプレート名をダブルクリックします。「所属するグループ」タブをクリックし、「追加」をクリックして、必要なグループを追加します。

i5/OS から登録したサーバー・グループかどうかにかかわらず、ユーザー・テンプレートを任意の Windows サーバー・グループのメンバーにすることができます。i5/OS から登録していないグループのメンバーであるテンプレートを使用して、ユーザーを登録することができます。その場合、グループからユーザーを削除する唯一の方法は、Windows サーバー上で「ユーザー マネージャ」プログラムを使用することです。

管理者の登録に使うテンプレートを作成している場合には、テンプレートを Windows サーバー・グループ *Administrators* のメンバーにするのが適切かもしれません。同様に、Windows ユーザーが偶発的に i5/OS を削除してしまうのを防ぐには、*AS400_Permanent_Users* (または *OS400_Permanent_Users*) グループ内にテンプレートを登録するのが適切です。

テンプレートでのホーム・ディレクトリーの指定

iSeries 上の Windows 環境において、可能な限り移植可能な方法でユーザーを管理するには、アプリケーションが作成するユーザー固有情報を保管するためのホーム・ディレクトリーを各ユーザーごとにセットアップすることができます。作業量を最小化するために、テンプレート・アカウントの中でホーム・ディレクトリーを指定することにより、登録プロセスで作成されるそれぞれの新規プロファイルのホーム・ディレクトリーを自動生成することができます。スケーラビリティのために、ホーム・ディレクトリーを特定の 1 つのディスク・ドライブに限定しないことが重要です。移植性を実現するには、汎用命名規則 (UNC) による名前を使用します。

テンプレート・プロファイルをカスタマイズしてホーム・ディレクトリーを含めるには、統合 Windows サーバー・コンソールから、以下のステップに従います。

1. ホーム・ディレクトリー・フォルダーを適切なサーバー上に作成して、それを共有にします。
2. ドメイン内で、Windows サーバー・コンソールから、「スタート」->「プログラム」->「管理ツール」->「Active Directory ユーザーとコンピュータ」をクリックします。ローカル・サーバーで、「スタート」->「プログラム」->「管理ツール」->「コンピュータの管理」->「ローカル ユーザーとグループ」をクリックします。
3. テンプレート (モデル・ユーザー) をダブルクリックして、プロパティを表示します。
4. 「プロファイル」タブをクリックします。
5. 「ホーム フォルダ」で、「接続ドライブ」をクリックします。ドライブ名 (たとえば Z:) を選択します。「パス」ダイアログには、UNC 名を使ってホーム・ディレクトリーのディレクトリー・パスを入力します (たとえば、`¥¥iSeriesWin¥¥homedirs¥¥username%`)。この例の場合、**iSeriesWin** はホーム・ディレクトリー・フォルダーが格納されているサーバー名、**homedirs** はホーム・ディレクトリー・フォルダーの名前です。ログオン名やユーザー名の代わりに変数 `%username%` を使用すると、新規

Windows サーバー・アカウントが作成されるたびに、Windows サーバーは変数名をユーザー名に自動的に置き換えます。さらに、そのユーザーのホーム・ディレクトリーを自動的に作成します。

LCLPWDMGT ユーザー・プロファイル属性の変更

ここでは、ユーザー・プロファイル属性「ローカル・パスワード管理 (LCLPWDMGT)」を変更する方法について説明します。LCLPWDMGT 属性についての説明は、54 ページの『ユーザーおよびグループの概念』および 56 ページの『ユーザー構成の種類』を参照してください。

LCLPWDMGT ユーザー・プロファイル属性を変更するには、i5/OS の文字ベースの環境で、以下の手順に従います。

1. CHGUSRPRF と入力し、変更する対象のユーザー・プロファイル名を入力します。
2. F4 キー (プロンプト) を押します。
3. すべての属性を表示するには **F9**、属性の省略形を表示するには **F11** を押します。
4. 属性 LCLPWDMGT を見つけて、*YES または *NO に設定します。
5. Enter キーを押します。

エンタープライズ識別マッピング (EIM)

EIM とは

エンタープライズ識別マッピング (EIM) は、各ユーザーの持つさまざまな UserID やパスワードを単一アカウントで一括管理する方法です。EIM を使用すれば、ユーザーはシステムに 1 度ログオンするだけで、EIM と他のサービスがバックグラウンドで連動することにより、そのユーザーのすべてのアカウントへの認証が行われます。

このメカニズムは、シングル・サインオン環境と呼ばれます。ユーザーが新しいシステムにアクセスを試行するたびに認証が行われますが、ユーザーはパスワードの入力を要求されません。EIM によって、ユーザーはネットワーク内の他のシステムにアクセスするために、多数のユーザー名とパスワードを記憶したり管理したりする必要がほとんどなくなります。ユーザーがいったんネットワークで認証されると、システムごとに異なるパスワードを入力しなくても、企業内のさまざまなサービスやアプリケーションにアクセスできます。

Information Center には、EIM について詳しく説明したトピックがあります。『エンタープライズ識別マッピング』を参照してください。

ユーザーを Windows 環境に登録するさまざまな方法については、56 ページの『ユーザー構成の種類』を参照してください。

EIMASSOC ユーザー・プロファイル属性

EIMASSOC は、EIM の構成を支援するためのユーザー・プロファイル属性です。i5/OS コマンド・プロンプトで、CHGUSRPRF に続いてユーザー・プロファイル名を入力して、F4 キーを押してコマンドを実行します。次に、ページの下端までスクロールダウンして、「EIM 関連」というセクションを見つけます。ここに含まれる各フィールドの意味の要約は、次のとおりです。

- **要素 1: EIM 識別子** EIM がユーザーを識別するために使用する UserID。これは、他のすべてのユーザー ID を保管するマスター ID と見なすことができます。ここに *USRPRF と指定した場合、自分の

i5/OS ユーザー・プロファイル名が EIM 識別子として使用されます。または、任意の有効な文字ストリングを指定することもできます。このフィールドに *DLT と入力して Enter キーを押すと、EIM 関連を削除するいくつかのオプションが表示されます。

- **要素 2: 関連タイプ** この値は、編集対象の i5/OS ユーザー・プロファイルが EIM 識別子に関連付けられる方法を指定します。iSeries 上の Windows 環境では、値 *TARGET、*TGTSRC、または *ALL によって i5/OS ターゲット関連および Windows ソース関連が自動作成または削除されます。
- **要素 3: 関連アクション** 以下のような特殊値があります。
 - *REPLACE - このユーザー・プロファイルに関連しているすべての EIM 識別子の Windows ソース関連が削除されます。登録済みユーザーの場合、指定した EIM 識別子に新しい Windows ソース関連が追加されます。
 - *ADD - 登録済みユーザーの場合、Windows ソース関連が追加されます。
 - *REMOVE - Windows ソース関連が削除されます。
- **要素 4: EIM 識別子の作成** この値は、EIM 識別子がまだ存在しない場合に作成するかどうかを指定します。使用できる特殊値には、*NOCRTEIMID (EIM 識別子を作成しない) または *CRTEIMID (EIM 識別子が存在しない場合、作成する) があります。

自動および手動の EIM 関連

シングル・サインオンを使用する典型的な EIM 環境では、通常、i5/OS ターゲット関連および Windows ソース関連が定義されます。統合 Windows サーバーのユーザー管理では、登録済み Windows ユーザーの EIM 関連を自動的に定義するようシステム管理者が決定する場合があります。たとえば、ある登録済みユーザーに関して EIMASSOC(*USRPRF *TARGET *ADD *CRTEIMID) を指定した場合、i5/OS は自動的に i5/OS のターゲット関連と Windows のソース関連を作成します。EIMASSOC 情報はユーザー・プロファイルに保管されません。また、この情報をユーザー・プロファイルとともに保存および復元することもできません。さらに、i5/OS システムで EIM が構成されていない場合、関連は処理されず、EIMASSOC 情報は無視されます。

i5/OS で EIM が構成され、登録済みユーザーに関する EIMASSOC 処理が定義されている場合、統合 Windows サーバーのユーザー管理でもまた、Windows EIM レジストリー内でユーザーの Windows ソース関連が自動的に作成または削除されます。Windows 環境にローカルに登録されているユーザーの場合、Windows EIM レジストリー名は、完全修飾されたローカルの Domain Name System (DNS) 名です。Windows EIM レジストリー・タイプは Windows 2000 として定義します。Windows ドメインに登録されているユーザーの場合、Windows レジストリー名は完全修飾されたドメイン DNS 名です。Windows レジストリー・タイプは Kerberos (大文字小文字を区別しない) として定義します。あるユーザーの EIMASSOC が定義され、i5/OS で EIM が構成されていて、Windows EIM レジストリーが存在しない場合には、統合 Windows サーバーのユーザー管理によって Windows EIM レジストリーが作成されます。

EIM 関連を使って、さまざまな Windows ユーザー・プロファイル名を使用可能にする

EIM は、複数のユーザー・プロファイルを 1 つのディレクトリー・システムに関連付けるメカニズムです。それぞれの EIM 識別子ごとに、i5/OS ユーザー・プロファイルのターゲット関連と Windows ユーザー・プロファイルのソース関連を定義することができます。ユーザー管理者は、i5/OS ターゲット関連のユーザー・プロファイル名とは異なる Windows ユーザー・プロファイル名を使用して Windows ソース関連を定義することができます。統合された Windows ユーザー管理では、定義済みの EIM Windows ソース関連 Windows ユーザー・プロファイルが存在すれば、それを使って Windows ユーザー登録を実行します。i5/OS ターゲット関連を定義する必要があります。管理者は EIM 識別子を使って Windows ソース関連を定義する必要があります。Windows ソース関連を定義するとき、同じ EIM 識別子に関して、正しい Windows EIM レジストリー名およびタイプを使用する必要があります。Windows にローカルに登録され

ているユーザーの場合、Windows EIM レジストリー名は、完全修飾されたローカルの Domain Name Server (DNS) 名です。Windows EIM レジストリー・タイプは EIM_REGTYPE_WIN2K として定義します。Windows ドメインに登録されているユーザーの場合、Windows レジストリー名は完全修飾されたドメイン DNS 名です。Windows レジストリー・タイプは EIM_REGTYPE_KERBEROS_IG として定義します。

Windows 環境に対するユーザーの登録の終了

Windows 環境ドメインおよびサーバーへのユーザーの登録を終了するには、統合 Windows サーバー・コンソールで次のステップを実行します。

1. 「統合サーバー管理」 → 「サーバー」または「ドメイン」を展開します。
2. 登録を解除したいユーザーが入っているドメインまたはサーバーを展開します。
3. 「ユーザー登録 (Enroll Users)」を選択します。
4. 登録を解除したいユーザーを右マウス・ボタンでクリックします。
5. 「登録解除 (Unenroll)」を選択します。
6. 確認ウィンドウで「登録解除 (Unenroll)」をクリックします。

Windows 環境へのユーザーの登録の終了の影響

Windows 環境からユーザー登録を終了すると、Windows サーバー・グループの AS400_Users (または OS400_Users) からだけではなく、登録された Windows サーバー・ユーザーのリストからもユーザーを除去することになります。ユーザーが Windows サーバー・グループの AS400_Permanent_Users (または OS400_Permanent_Users) のメンバーでなければ、Windows 環境からもユーザーを削除することになります。

Windows サーバー・グループの AS400_Permanent_Users (または OS400_Permanent_Users) のメンバーであるユーザーは、登録を終了したり、i5/OS からユーザーを削除しても、Windows サーバーから削除することはできません。しかし、登録が終了すると、そのユーザーは登録された Windows サーバー・ユーザーのリストと、Windows サーバー・グループの AS400_Users (OS400_Users) から除去されます。

1. i5/OS でのユーザー登録が終了した後、そのユーザーを Windows 環境上に保持しておくことができます。
1. これにより、それらのユーザーを i5/OS 上のグループに追加したり、i5/OS 上でパスワードを変更したり
1. することが可能になりますが、そのような更新が実行されても Windows 環境に反映されないため、これを
1. 実行することは推奨されていません。このような矛盾があると、どちらのシステムでもユーザーの追跡が難
1. しくなる可能性があります。

ユーザーの登録は、数々の方法で終了させることができます。ユーザー登録を終了させるアクションには、以下のものが含まれます。

- 意図的にユーザーの登録を終了する。
- i5/OS ユーザー・プロファイルを削除する。
- ユーザーが属するすべての i5/OS グループの登録を終了する。
- 登録された i5/OS グループからそのユーザーを除去する。そのユーザーが他の登録済みグループに属することはありません。

Windows 環境に対するグループの登録の終了

Windows 環境へのグループ登録を終了すると、登録がそのグループに制限されているすべてのユーザーは、自分の登録も終了させられてしまいます。そのグループ内に、そのグループ経由で登録されたメンバーがいる場合、そのグループは Windows 環境から削除されます。

しかし、そのグループ内に、i5/OS から登録されたメンバーではなく Windows 環境から追加したメンバーがいる場合、そのグループは削除されません。グループ内に残っているメンバーだけが、非登録ユーザーになります。

Windows 環境ドメインおよびサーバーへのグループの登録を終了するには、iSeries ナビゲーターで次のステップを実行します。

1. 「統合サーバー管理」 → 「サーバー」または「ドメイン」を展開します。
2. 登録を解除したいグループが入っているドメインまたはサーバーを展開します。
3. 「登録済みグループ」を選択します。
4. 登録を解除したいグループを右マウス・ボタンでクリックします。
5. 「登録解除 (Unenroll)」を選択します。
6. 確認ウィンドウで「登録解除 (Unenroll)」をクリックします。

QAS400NT ユーザー

次の場合、ドメインまたローカル・サーバー上に i5/OS ユーザーまたはグループ・プロファイルを正常に登録するには、QAS400NT ユーザーをセットアップする必要があります。

- メンバー・サーバーを経由してドメイン上に登録されている。
- 200 ページの『テンプレートでのホーム・ディレクトリーの指定』のセクションで説明されているように、ホーム・ディレクトリー・パスを指定しているテンプレートを使用して、ローカル・サーバー上に登録されている。
- 同一ドメイン上にドメイン・コントローラーおよびメンバー・サーバーの両方を含んでいる i5/OS 区画を経由して、ドメイン上に登録されている。

次の場合、ドメインまたローカル・サーバー上に i5/OS ユーザーまたはグループ・プロファイルを正常に登録するには、QAS400NT ユーザーをセットアップする必要はありません。

- 同一ドメイン上にドメイン・コントローラーは含まれているが、メンバー・サーバーが含まれていない i5/OS 区画を経由して、ドメイン上に登録されている。
- ホーム・ディレクトリー・パスを指定していないテンプレートを使用して、ローカル・サーバー (またはメンバー・サーバー上のローカル部分) に登録されている。

QAS400NT ユーザーをセットアップする必要がある場合、次のステップを実行します。

1. ユーザー・クラス *USER を使用して、i5/OS 上に QAS400NT ユーザー・プロファイルを作成する。パスワードは、次のステップで必要となりますので、メモしておいてください。ドメイン上に登録されている場合には、パスワードが Windows パスワード規則に従っていることを確認します。59 ページの『パスワードについての考慮事項』を参照してください。
2. 登録する際に経由した統合 Windows サーバーの Windows コンソール上に、QAS400NT ユーザー・アカウントを作成する。i5/OS ユーザー・プロファイル・パスワードおよび Windows ユーザー・アカウント・パスワードは、QAS400NT のパスワードと同じでなければならないことに注意してください。
 - a. ドメイン・コントローラー上の QAS400NT のセットアップ

登録をセットアップするドメインのドメイン・コントローラー上に、QAS400NT ユーザー・アカウントを次のように作成します。

1) 統合サーバー・コンソールから、次のようにします。

a)

- Windows 2000 Server で、「スタート」->「プログラム」->「管理ツール」->「コンピュータの管理」->「ローカル ユーザーとグループ」をクリックします。
- Windows Server 2003 で、「スタート」->「プログラム」->「管理ツール」->「コンピュータの管理」->「システム ツール」->「ローカル ユーザーとグループ」をクリックします。

b) 「システム ツール」->「ローカル ユーザーとグループ」を選択します。

2) 「ユーザー」フォルダー (またはユーザーが属するフォルダー) を右マウス・ボタン・クリックし、「新しいユーザー」を選択します。

3) 次の設定値を入力します。

Full name: qas400nt
User logon name: qas400nt

4) 「次へ」をクリックします。次の設定値を入力します。

Password: (the same password as you used for QAS400NT on i5/OS)
Deselect: User must change password at next logon
Select: User cannot change password
Select: Password never expires

5) 「次へ」、そして「完了」の順にクリックします。

6) 「QAS400NT ユーザー」アイコンを右マウス・ボタン・クリックして、「プロパティ」を選択します。

7) 「所属するグループ」タブ、「追加」の順にクリックします。

8) ボックスに Domain Admins と入力して、「OK」をクリックしてから、もう一度「OK」をクリックします。これで、QAS400NT ユーザー・アカウントにユーザーを作成するための権限が付与されます。

b. ローカル・サーバー上の QAS400NT のセットアップ

ローカル・サーバー (または、ローカルに登録している場合にはメンバー・サーバー) 上に、QAS400NT ユーザー・アカウントを次のように作成します。

1) 統合サーバー・コンソールから、次のようにします。

- Windows 2000 Server で、「スタート」->「プログラム」->「管理ツール」->「コンピュータの管理」->「ローカル ユーザーとグループ」をクリックします。
- Windows Server 2003 で、「スタート」->「プログラム」->「管理ツール」->「コンピュータの管理」->「システム ツール」->「ローカル ユーザーとグループ」をクリックします。

2) 「ユーザー」フォルダーを右マウス・ボタン・クリックして、「新しいユーザー...」を選択します。

3) 次の設定値を入力します。

User name: qas400nt
Full name: qas400nt
Password: (the same password as you used for QAS400NT on i5/OS)
Deselect: User must change password at next logon
Select: User cannot change password
Select: Password never expires

- 4) 「作成」そして「閉じる」の順にクリックします。
 - 5) 「QAS400NT ユーザー」アイコンを右マウス・ボタン・クリックして、「プロパティ」を選択します。
 - 6) 「所属するグループ」タブ、「追加」の順にクリックします。
 - 7) ボックスに Administrators と入力して「OK」をクリックしてから、もう一度「OK」をクリックします。これで、QAS400NT ユーザー・アカウントにユーザー管理サービスに対する権限が付与されます。
3. iSeries ナビゲーターまたは CHGNWSUSRA コマンドを使用して、ドメインまたはローカル・サーバーに i5/OS QAS400NT ユーザー・プロファイルを登録します。この実行方法については、197 ページの『iSeries ナビゲーターによる Windows 環境への単一 i5/OS ユーザーの登録』を参照してください。QAS400NT の登録の際には、テンプレートを使用しないでください。
4. iSeries ナビゲーターまたは WRKNWSENR コマンドを使用して、QAS400NT が正常に登録されたことを確認します。これで、ドメイン上のドメイン・コントローラーまたはメンバー・サーバーを介して、i5/OS ユーザー・プロファイルを登録できます。

注:

- i5/OS が登録ユーザーになっているため、QAS400NT パスワードを OS/400 側から変更できます。
- 同じ i5/OS 区画上の別のドメインに属する複数の統合サーバーがある場合には、ドメインごとに QAS400NT をセットアップする必要があります。すべての QAS400NT ユーザー・アカウントには、i5/OS ユーザー・プロファイルと同じパスワードがなければなりません。あるいはドメイン間の Active Directory または信頼関係を使用することを検討して、ユーザーを 1 つのドメインだけに登録します。
- 複数の i5/OS 区画があり統合サーバーも複数ある場合には、各ドメインが複数の i5/OS 区画上にある統合サーバーを含んでいない限りは、別の i5/OS 区画上の QAS400NT パスワードが異なっても構いません。すべての i5/OS QAS400NT ユーザー・プロファイルおよび対応する Windows ユーザー・アカウントは、1 つのドメインに対しては同じパスワードを持っている必要があるというのがルールです。
- i5/OS 上の QAS400NT ユーザー・プロファイルを削除したり、パスワードを失効させたりしないように注意してください。同一 Windows ドメインの複数の i5/OS 区画のいずれかにある QAS400NT パスワードが失効するというリスクを最小限にするには、変更を QAS400NT ユーザー・プロファイルに伝搬する i5/OS 区画を 1 つだけにしておくことをお勧めします。この実行方法については、『統合 Windows サーバーへの登録と伝搬の禁止』を参照してください。
- 同一ドメインにある統合 Windows サーバーがそれぞれに存在する i5/OS 区画が複数ある場合、すべての i5/OS 区画で QAS400NT パスワードが一致していないと、登録で問題が生じる可能性があります。この問題を最小限に抑えるには、QAS400NT パスワードへの変更の伝搬を 1 つのみの i5/OS 区画に制限することをお勧めします。他の区画に対してはユーザーを登録する権限は引き続き許可します。このようにすれば、他の区画でパスワードの変更に失敗しても、ユーザー登録できないのはその区画だけです。この実行方法については、『統合 Windows サーバーへの登録と伝搬の禁止』を参照してください。

統合 Windows サーバーへの登録と伝搬の禁止

特定の統合サーバーへの i5/OS ユーザー・プロファイル伝搬の回避を望む場合もあります。幾つかの理由が考えられます。

- 同じドメインに属する複数の統合サーバーがあり、それらすべてが同一の i5/OS 区画にある場合、デフォルトではユーザー・プロファイル登録は、その区画のすべての統合サーバーで実行されます。ネット

ワーク・トラフィックを減らすには、1つの統合サーバー以外では、そのドメイン上のすべての統合サーバーでの登録をオフに変更できます。登録する1つの統合サーバーはドメイン・コントローラーになります(同じ区画にある場合)。

- 同じドメインに属する複数の統合サーバーがあり、それらすべてが別個の i5/OS 区画にある場合には、QAS400NT パスワードが同期されずに、ユーザー・プロファイルの登録の際に問題が生じる危険があります。QAS400NT ユーザー・プロファイルを1つ以外の i5/OS 区画すべてに伝搬しないようにして、登録で問題が生じる危険を減らすことができます。他の i5/OS 区画には、ユーザーを登録するための権限が十分にあることに注意してください。このようにすれば、他の区画でパスワードの変更に失敗しても、ユーザー登録できないのはその区画だけです。

特定の統合サーバーへの i5/OS ユーザー・プロファイル伝搬を回避するには、2つの方法があります。

- 「ドメイン・ユーザーの伝搬 (PRPDMNUSR)」パラメーターを使用します。この実行方法については、下記の説明を参照してください。
- データ域の作成 (CRTDTAARA) コマンドを使ってデータ域を作成します。この実行方法については、下記の説明を参照してください。

特定の統合サーバーを経由してのドメインへの登録を回避するための PRPDMNUSR パラメーターの使用

ネットワーク・サーバー記述の変更 (CHGNWSD) コマンドの「ドメイン・ユーザーの伝搬 (PRPDMNUSR)」パラメーターは、特定の統合サーバーを介してのドメインへのユーザー登録を回避するのに使用できます。このパラメーターは、Windows サーバー導入 (INSWNTSVR) コマンドを使用して統合サーバーをインストールする際にも設定できます。同じドメインに属する複数の統合 Windows サーバーを制御する単一の i5/OS 区画では、1つ以外のすべての統合サーバーで登録をオフに変更できるので、このオプションが役に立ちます。

PRPDMNUSR パラメーターを使用してユーザー登録を回避するには、次のようにします。

1. ネットワーク・サーバー記述の処理 (WRKNWSD) コマンドを使用して、登録を停止する統合サーバーを選択します。(サーバーをオフに変更する必要はありません。)
2. 次のコマンドを入力します。CHGNWSD NWSD(newsdname) PRPDMNUSR(*NO)

注:

- ドメイン上のすべての統合サーバーの登録をオフにしないでください。オフにすると、すべてのユーザーが更新保留 (*UPDPND) 状況になってしまう可能性があり、まったく伝搬しなくなります。
- ユーザーの登録用に2つの使用可能な統合サーバーを用意し、サーバーの1つがダウンしてしまう場合にも変更を可能にしておくとう便利です。

特定の統合サーバーへの QAS400NT の登録を回避するための CRTDTAARA コマンドの使用

データ域の作成 (CRTDTAARA) コマンドは、指定された統合サーバーに対して、QAS400NT ユーザー・プロファイルのみの登録を回避するのに使用できます。他のユーザー・プロファイルの伝搬には影響しません。同じドメインに属する複数の統合サーバーがあり、それらすべてが別個の i5/OS 区画にある場合に、このオプションが役に立ちます。異なる i5/OS 区画からユーザー・プロファイルを登録しますが、複数の QAS400NT ユーザー・プロファイルではパスワードをドメインに伝搬しません。次のステップを実行してください。

1. QAS400NT の登録に使用するドメイン上の i5/OS 区画を1つ選択します。QAS400NT がこの i5/OS 区画に登録されるようにします。
2. QAS400NT が他の i5/OS 区画に登録される場合には、次のステップを実行します。
 - a. ドメイン・コントローラーで、QAS400NT ユーザー・アカウントを OS400_Permanent_Users グループに追加して、削除されていないことを確認します。

- b. QAS400NT の登録を行わない i5/OS 区画で、QAS400NT ユーザー・プロフィールを削除します。
3. QAS400NT の登録を行わない i5/OS 区画で、次のコマンドを使用してデータ域を作成します。

```
CRTDTAARA DTAARA(QUSRSYS/nwsdnameAU) TYPE(*CHAR) LEN(10) VALUE( *NOPROP )
```

ここで、**nwsdname** は統合サーバーのネットワーク・サーバー記述で、***NOPROP** は QAS400NT ユーザー・プロフィール・パラメーター (パスワードも含む) がこの i5/OS 区画から伝搬されないことを示すキーワードです。

4. データ域を作成した各 i5/OS 区画に、QAS400NT ユーザー・プロフィールを作成して登録します。その後のユーザー・プロフィール (QAS400NT 以外) の登録のためには、すべての i5/OS 区画上に現行の QAS400NT パスワード (失効していない) がなければならないことに注意してください。QAS400NT パスワードは伝搬されないの、失効していない限りどのようなパスワードでも問題ありません。


第 12 章 統合 Windows サーバーのバックアップと回復

iSeries の Windows 環境は 2 つのオペレーティング・システム (Windows 2000 Server または Windows Server 2003 with i5/OS) を結合したものであるため、バックアップの管理は i5/OS か Windows サーバー・ユーティリティを使用し、または両方を組み合わせて行うことができます。バックアップ・ストラテジーを計画する場合は、『Backup and recovery』のトピックと、Microsoft 資料を参照してください。

iSeries の統合サーバーをバックアップするには、以下の基本的なオプションがあります。

- i5/OS 上で全システム・バックアップを行う。トピック『Back up your server』を参照してください。
- ネットワーク・サーバー記述 (NWSD) と、iSeries 統合サーバーとに関連したディスク・ドライブのバックアップをとる。『統合 Windows サーバーに関連付けられた NWSD およびその他のオブジェクトのバックアップ』を参照してください。
- i5/OS SAV および RST コマンドと i5/OS NetServer がバックアップ・ユーティリティを使って、個々の統合サーバー・ファイルのバックアップをとる。215 ページの『統合 Windows サーバーの個々のファイルおよびディレクトリーのバックアップ』を参照してください。

使用する回復オプションは、システムをバックアップした方法と、何をリカバリーする必要があるかによって異なります。

- システム全体を回復するには、『Backup and Recovery』 を参照してください。
- ネットワーク・サーバー記述とそれに関連した i5/OS ディスク・ドライブを復元する必要がある場合は、220 ページの『統合 Windows サーバーの NWSD およびディスク・ドライブの復元』を参照してください。
- 保管 (SAV) コマンドでバックアップした統合サーバー・データ (ファイル、ディレクトリー、共用、および Windows レジストリー) を復元するには、224 ページの『統合 Windows サーバー・ファイルの回復』を参照してください。
- Windows バックアップ・ユーティリティまたは他のユーティリティを使用して保管したファイルを復元するには、そのユーティリティを使用します。

統合 Windows サーバーに関連付けられた NWSD およびその他のオブジェクトのバックアップ

統合サーバーをインストールすると、バックアップをとる必要のあるサーバーのネットワーク・サーバー記述と事前定義ディスク・ドライブが i5/OS で作成されます。179 ページの『統合 Windows サーバーの事前定義ディスク・ドライブ』を参照してください。ディスク・ドライブには、システム関連のもの (インストールおよびシステム・ドライブ) と、ユーザー関連のものがあります。Windows サーバーはそれらを 1 つのシステムであると思なすため、適切に復元できるように、すべてのディスク・ドライブとネットワーク・サーバー記述を保管する必要があります。

Microsoft Windows サーバー・オペレーティング・システムと、統合サーバーの始動に必要なファイルは、サーバーの C および D ドライブにあります。iSeries の Windows 環境を使用すれば、これらのドライブを i5/OS ネットワーク・サーバー記憶域オブジェクトとして保管し、復元することができます。これらのオブジェクトは、i5/OS 全システム・バックアップを実行する際に、i5/OS システムの一部として保管され

ます。また、ネットワーク・サーバー記述や関連した記憶域についても、それぞれを個別に保管することが可能です。システム・ドライブのバックアップを毎日取るようにするとよいでしょう。

記憶域を保管してしまえば最も手早いのですが、そうすると個々のファイルを復元できないので、統合サーバーをバックアップする方法としては最も柔軟性に欠けています。特定のファイルおよびディレクトリーのバックアップを個別に作成すると、PC ベースの Windows サーバーで、BOOT ディスク、RDISK、およびレジストリーのバックアップを作成せずに済みます。215 ページの『統合 Windows サーバーの個々のファイルおよびディレクトリーのバックアップ』を参照してください。

ネットワーク・サーバー記述および統合サーバーに関連したディスク・ドライブオブジェクトをバックアップするには、以下のトピックを参照してください。

- 『統合 Windows サーバーの NWSD のバックアップ』。
- 『iSCSI NWSCFG および妥当性検査リストのバックアップ』
- 211 ページの『統合 Windows サーバー用事前定義ディスク・ドライブのバックアップ』。
- 212 ページの『統合 Windows サーバー用ユーザー定義ディスク・ドライブのバックアップ』。
- 213 ページの『ユーザー登録情報の保管と復元』。
- 213 ページの『保管するオブジェクトと i5/OS でのその保管位置』で、保管するユーザー・オブジェクトとシステム・オブジェクトの表を表示することができます。

統合 Windows サーバーの NWSD のバックアップ

統合 Windows サーバーに関連した記憶域オブジェクトを保管する場合、ネットワーク・サーバー記述 (NWSD) も保管する必要があります。そうしないと、Windows サーバーは Windows サーバー・ファイル・システム許可などの項目を再確立できなくなります。NWSD を保管するには、構成の保管 (SAVCFG) コマンドを使用します。

1. i5/OS コマンド行に、SAVCFG と入力します。
2. Enter キーを押して、i5/OS で NWSD 構成を保管します。

注: 構成の保管 (SAVCFG) コマンドは、NWSD に関連したオブジェクトを保管します。

iSCSI 接続の統合 Windows サーバーの NWSH のバックアップ

NWSH を保管するには、構成の保管 (SAVCFG) コマンドを使用します。

1. i5/OS コマンド行に、SAVCFG と入力します。
2. Enter キーを押して、i5/OS で NWSH 構成を保管します。

iSCSI NWSCFG および妥当性検査リストのバックアップ

iSCSI HBA で接続されたサーバーの場合、追加の構成オブジェクトが QUSRSYS ライブラリーに保管されます。これには、ネットワーク・サーバー構成オブジェクト (タイプ *NWSCFG) および関連した妥当性検査リスト・オブジェクト (タイプ *VLDL) が含まれます。

注: *NWSCFG オブジェクトと *VLDL オブジェクトは同じ名前を共有します。

ネットワーク・サーバー構成オブジェクトと妥当性検査リスト・オブジェクトを保管するには、**オブジェクトの保管 (SAVOBJ)** コマンドを使用します。

1. 磁気テープに保管する場合は、i5/OS 用にフォーマットされた磁気テープがマウントされていることを確認してください。
2. Windows サーバーをシャットダウンして、オブジェクト・ロックを解放します。

3. i5/OS コマンド行で、SAV0BJ と入力し、F4 を押します。
4. 「オブジェクト」フィールドで、NWSCFG 名を指定します。デフォルト名が使用されている場合は、総称名 nwsdname* を指定します。
5. 「ライブラリー」フィールドで、QUSRSYS と指定します。
6. オブジェクトを磁気テープに保管する場合、「装置」フィールドに磁気テープ装置 (たとえば、TAP01) の名前を指定します。磁気テープのかわりに保管ファイルを使用する場合、装置として *SAVF を指定し、データ圧縮オプションを使用可能にします。
7. 「オブジェクトの種類」に、*NWSCFG と *VLDL の両方を指定します。
8. 保管ファイルを使用する場合、F10 を押して、追加のパラメーターを表示します。
9. 「保管ファイル」フィールドに、保管ファイルへのパス (たとえば、winbackup/nwscfg) を指定します。
10. 保管ファイルを使用する場合、次ページ・キーを押し、「データ圧縮」の値を「*はい」に変更します。

統合 Windows サーバー用事前定義ディスク・ドライブのバックアップ

統合サーバーをインストールすると、保管を必要とするシステムおよびインストール・ソース (C および D) ドライブが事前定義ドライブとして i5/OS で作成されます。 179 ページの『統合 Windows サーバーの事前定義ディスク・ドライブ』を参照してください。

注:

1. Windows ネットワーク・サーバー記述、その事前定義されたディスク・ドライブ、およびこれにリンクされているすべてのユーザー定義のディスク・ドライブは、一まとまりのユニットとして扱ってください。これらはまとめて保管および復元してください。どちらも 1 つの完全なシステムを構成するもので、そのように扱わなければなりません。そうしないと、統合サーバーは Windows サーバー・ファイル・システム許可などの項目を再確立できなくなります。
2. サーバーが V4R5 より前の OS/400 システムで作成されている場合、V5R3 iSeries Information Center の『V4R5 より前の OS/400 システムで作成した統合 Windows サーバー用事前定義ディスク・ドライブのバックアップ』を参照してください。

i5/OS 上のシステム・ディスク・プール (ASP) 内のディスク・ドライブ (ネットワーク・サーバー記憶域) を保管するには、次のようにします。

1. 磁気テープに保管する場合は、i5/OS 用にフォーマットされた磁気テープがマウントされていることを確認してください。
2. 統合サーバーをシャットダウンし、バックアップ時にユーザーがファイルを更新できないようにします。 163 ページの『統合サーバーの開始と停止』を参照してください。
3. i5/OS コマンド行で、SAV と入力し、F4 を押します。
4. 記憶域を磁気テープに保管する場合、「装置」フィールドに磁気テープ装置の名前 (たとえば、/QSYS.LIB/TAP01.DEVD) を指定します。

記憶域を磁気テープではなく保管ファイルに保管する場合は、装置として使う保管ファイルへのパスを指定してください。たとえば、ライブラリー WINBACKUP の MYSAVF という保管ファイルを使用するには、装置を表す '/QSYS.LIB/WINBACKUP.LIB/MYSAVF.FILE' を指定します。

5. 「オブジェクト:」の下の「名前」フィールドには、'/QFPNWSSTG/stgspc' を指定してください。stgspc は、ネットワーク・サーバー記憶域の名前です。
 - システム (C) ドライブの場合は、/QFPNWSSTG/nwsdname1 を使用します。

- D ドライブを保管するには、 /QFPNWSSTG/newsdname2 を使用します。
 - ユーザー・ディスク・プールに作成される記憶域の場合は、 /QFPNWSSTG/stgspc および dev/QASPnn/stgspc.UDFS を使用してください。 stgspc は、ネットワーク・サーバー記憶域の名前で、nn はユーザー・ディスク・プールの番号です。
 - 独立ディスク・プールの場合には、 /QFPNWSSTG/stgspc および dev/independent ASP name/stgspc.UDFS を使用してください。 independent ASP name は独立ディスク・プールの名前で、stgspc はネットワーク・サーバー記憶域の名前です。
6. 指定したい他のすべてのパラメーターに値を指定してから、Enter キーを押して記憶域を保管します。
 7. それから統合サーバーを始動します。 163 ページの『統合サーバーの開始と停止』を参照してください。

次の部分に詳細が示されています。 213 ページの『保管するオブジェクトと i5/OS でのその保管位置』。

統合 Windows サーバー用ユーザー定義ディスク・ドライブのバックアップ

統合サーバー用に作成するディスク・ドライブは、統合ファイル・システム内にあります。これらの記憶域を i5/OS 上のユーザー・ディスク・プール (ASP) から保管するには、保管 (SAV) コマンドを使用します。

注: ネットワーク・サーバー記述 (NWSR)、その事前定義されたディスク・ドライブ、およびこれにリンクされているすべてのユーザー定義のディスク・ドライブは、一まとまりのユニットとして扱ってください。これらはまとめて保管および復元してください。それらは 1 つの完全なシステムを構成するもので、そのように扱わなければなりません。そうしないと、統合サーバーは Windows サーバー・ファイル・システム許可などの項目を再確立できなくなります。

i5/OS 上のユーザー・ディスク・プール (ASP) 内にディスク・ドライブを保管するには、次のようにします。

1. 磁気テープに保管する場合は、i5/OS 用にフォーマットされた磁気テープがマウントされていることを確認してください。
2. 独立ディスク・プール内に作成したネットワーク・サーバー記憶域の場合、'dev/independent ASP name/stgspc.UDFS' オブジェクトを保管する前に補助記憶域プール (ASP) がオンに変更されていることを確認してください。
3. ネットワーク・サーバー記述をオフに変更して統合サーバーをシャットダウンし、バックアップ時にユーザーがファイルを更新できないようにします。 163 ページの『統合サーバーの開始と停止』を参照してください。
4. i5/OS コマンド行で、SAV と入力し、F4 を押します。
5. 記憶域を磁気テープに保管する場合、「装置」フィールドに磁気テープ装置の名前 (たとえば、/QSYS.LIB/TAP01.DEVD) を指定します。

記憶域を磁気テープではなく保管ファイルに保管する場合は、装置として使う保管ファイルへのパスを指定してください。(たとえば、ライブラリー WINBACKUP の MYSAVF という保管ファイルを使用するには、装置を表す '/QSYS.LIB/WINBACKUP.LIB/MYSAVF.FILE' を指定します。)あるいは、使用する装置の名前 (たとえば、/QSYS.LIB/TAP01.DEVD) を使用します。

6. 「オブジェクト:」の下の「名前」フィールドには、'/QFPNWSSTG/stgspc' および 'dev/QASPnn/stgspc.UDFS' を指定してください。 stgspc はネットワーク・サーバー記憶域の名前、xx はディスク・プールの番号です。

- ユーザー・ディスク・プールに作成される記憶域の場合は、/QFPNWSSTG/stgspc および dev/QASPnn/stgspc.UDFS を使用してください。 stgspc は、ネットワーク・サーバー記憶域の名前で、xx はユーザー・ディスク・プールの番号です。
- 独立ディスク・プールの場合には、/QFPNWSSTG/stgspc および dev/independent ASP name/stgspc.UDFS 使用してください。 independent ASP name は独立ディスク・プールの名前で、stgspc はネットワーク・サーバー記憶域の名前です。

7. 指定したい他のすべてのパラメーターに値を指定してから、Enter キーを押して記憶域を保管します。


8. Windows サーバーを始動します。 163 ページの『統合サーバーの開始と停止』を参照してください。

システム・オブジェクトのバックアップと適切な保管コマンドの詳細については、バックアップ、回復、および可用性 (Backup, recovery, and availability) を参照してください。

上記の方法を使用すると、ネットワーク・サーバー記憶域全体をバックアップして回復できるようになります。個々のファイルをバックアップして回復するには、次の新しい機能を使用できます。 215 ページの『統合 Windows サーバーの個々のファイルおよびディレクトリーのバックアップ』

ユーザー登録情報の保管と復元

場合によっては、ユーザー・プロファイルとその登録情報を復元する必要があることがあります。以下の項では、統合 Windows サーバー登録に使われるユーザー・プロファイルを保管および復元するための i5/OS コマンドと API について説明しています。i5/OS のバックアップと回復のセキュリティに関する

詳細は、「iSeries 機密保護解説書」 中の『セキュリティ情報のバックアップおよび回復』の項を参照してください。

ユーザー・プロファイルを保管するには、SAVSECDTA コマンドまたは QRSAVO API を使います。統合 Windows サーバー登録サポートの場合、i5/OS システム値 QRETSVRSEC を 1 に設定しなければなりません。SAVSECDTA コマンドまたは QRSAVO API を使って保管したユーザー・プロファイルは、USRPRF(*ALL) を指定した RSTUSRPRF コマンドを使って復元することができます。パラメーター USRPRF(*ALL) を指定しなくても、パラメーターと値 SECDTA(*PWDGRP) を指定すればユーザー・プロファイルを復元することができます。

QRSAVO API を使用し、以前のターゲット・リリース値を使ってユーザー・プロファイルを保管した場合、ユーザー・プロファイル登録定義は復元されません。ユーザー・プロファイルを復元した後、登録を定義する必要があります。登録を定義するには、iSeries ナビゲーターまたは「ネットワーク・サーバー・ユーザー属性の変更」(CHGNWSUSRA) コマンドを使用してください。

統合 Windows サーバーの登録の場合は、上記の方法を使ってユーザー・プロファイルを保管および復元する必要があります。他のコマンドや API を使って保管および復元されたユーザー・プロファイルは、Windows ではサポートされません。

保管するオブジェクトと i5/OS でのその保管位置

Windows environment for iSeries をインストールすると、多くのオブジェクトが作成されます。これらのオブジェクトには、システム関連のものとユーザー関連のものがあります。正常に復元を行うには、すべてのオブジェクトを保管する必要があります。これらのオブジェクトの保管には、i5/OS GO SAVE コマンドのオプションを使用します。オプション 21 は、システム全体を保管します。オプション 22 は、システム・データを保管します。オプション 23 は、ユーザー・データ (QFPNWSSTG のオブジェクトを含む) を保管します。

特定のオブジェクトを保管する場合は、以下の表のいずれかを使って、i5/OS 上でのそのオブジェクトの保管位置と使用するコマンドを参照してください。トピック『Manually saving parts of your system』には、保管コマンドの使用についての詳細が掲載されています。ドライブ全体 (記憶域) を保管するだけでなく、個々のファイルおよびディレクトリーを保管して復元することも可能です。215 ページの『統合 Windows サーバーの個々のファイルおよびディレクトリーのバックアップ』を参照してください。

保管するオブジェクト

オブジェクトの内容	オブジェクト名	オブジェクトの位置	オブジェクト・タイプ	保管コマンド
統合サーバー・ブートおよびシステム・ドライブ	nwsdname1	/QFPNWSSTG	システム・ディスク・プール (ASP) 内の事前定義ネットワーク・サーバー記憶域	GO SAVE、オプション 21 または 23 SAV OBJ('/QFPNWSSTG/nwsdname1') DEV('/QSYS.LIB/TAP01.DEVD')
統合サーバー・ブートおよびシステム・ドライブ	nwsdname1	/QFPNWSSTG	ユーザー・ディスク・プールの事前定義ネットワーク・サーバー記憶域	SAV OBJ('/QFPNWSSTG/nwsdname1') (/dev/QASPnn/nwsdname1.UDFS)) DEV('/QSYS.LIB/TAP01.DEVD')
統合サーバー・インストール・ソース・ドライブ	nwsdname2	/QFPNWSSTG	システム・ディスク・プールの事前定義ネットワーク・サーバー記憶域	GO SAVE、オプション 21 または 23 SAV OBJ('/QFPNWSSTG/nwsdname2') DEV('/QSYS.LIB/TAP01.DEVD')
統合サーバー・インストール・ソース・ドライブ	nwsdname2	/QFPNWSSTG	ユーザー・ディスク・プールの事前定義ネットワーク・サーバー記憶域	GO SAVE、オプション 21 または 23 SAV OBJ('/QFPNWSSTG/nwsdname2') (/dev/QASPnn/nwsdname2.UDFS)) DEV('/QSYS.LIB/TAP01.DEVD')
統合サーバー・インストール・ソース・ドライブ	nwsdname2	/QFPNWSSTG	独立ディスク・プール (ASP) 内の事前定義ネットワーク・サーバー記憶域	GO SAVE、オプション 21 または 23 SAV OBJ('/QFPNWSSTG/nwsdname2') (/dev/independent ASP name/nwsdname2.UDFS)) DEV('/QSYS.LIB/TAP01.DEVD')
ユーザー・データおよびアプリケーション	各種	/QFPNWSSTG	システム・ディスク・プールのユーザー定義ネットワーク・サーバー記憶域	GO SAVE、オプション 21 または 23 SAV OBJ('/QFPNWSSTG/stgspc') DEV('/QSYS.LIB/TAP01.DEVD')
ユーザー・データおよびアプリケーション	各種	/QFPNWSSTG	ユーザー・ディスク・プールのユーザー定義ネットワーク・サーバー記憶域	GO SAVE、オプション 21 または 23 SAV OBJ('/QFPNWSSTG/stgspc') (/dev/QASPnn/stgspc.UDFS)) DEV('/QSYS.LIB/TAP01.DEVD')
ユーザー・データおよびアプリケーション	各種	/QFPNWSSTG	独立ディスク・プールのユーザー定義ネットワーク・サーバー記憶域	GO SAVE、オプション 21 または 23 SAV OBJ('/QFPNWSSTG/stgspc') (/dev/independent ASP name/stgspc.UDFS)) DEV('/QSYS.LIB/TAP01.DEVD')
統合サーバーからのメッセージ	各種	各種	メッセージ待ち行列	GO SAVE、オプション 21 または 23 SAVOBJ OBJ(msgq) LIB(library) DEV(TAP01) OBJTYPE(*MSGQ)
統合サーバー用の i5/OS 構成オブジェクト	各種	QSYS	装置構成オブジェクト	GO SAVE、オプション 21、22、または 23 SAVCFG DEV(TAP01)
i5/OS ベースおよび Windows ベースの IBM iSeries 統合サーバー・サポート・コード	QNTAP、NTAP、およびサブディレクトリー	QSYS および /QIBM/ProdData/NTAP	ライブラリーおよびディレクトリー	SAVLICPGM LICPGM(5722SS1) OPTION(29)
Windows サーバー・ファイル共有	QNTC およびサブディレクトリー	/QNTC/servername /sharename	ディレクトリー	GO SAVE、オプション 21 または 22 SAV
i5/OS TCP インターフェース	QATOCIFC	QUSRSYS	物理ファイル	GO SAVE、オプション 21 または 23 SAVOBJ OBJ(QATOCIFC) LIB(QUSRSYS) DEV(TAP01) OBJTYPE(*FILE)
i5/OS TCP インターフェース	QATOCLIFC	QUSRSYS	論理ファイル	GO SAVE、オプション 21 または 23 SAVOBJ OBJ(QATOCLIFC) LIB(QUSRSYS) DEV(TAP01) OBJTYPE(*FILE)
iSCSI NWSCFG および関連した妥当性検査リスト	各種	QUSRSYS	ネットワーク・サーバー構成および関連した値	SAVOBJ LIB(QUSRSYS) OBJTYPE(*NWSCFG *VLDL)

オブジェクトの内容	オブジェクト名	オブジェクトの位置	オブジェクト・タイプ	保管コマンド
iSCSI バス証明書ストア	nwsdname.*	/QIBM/UserData/NWSDCert	証明書ストア・ファイル	GO SAVE、オプション 21 または 23 SAV OBJ('/QIBM/UserData/NWSDCert/nwsdname.*')
iSCSI サービス・プロセッサ証明書ストア	nwscfgname.kdb	/QIBM/UserData/Director /classes/com/ibm /sysmgt/app/iide	証明書ストア・ファイル。セキュリティー初期化メソッドが「自動的に証明書を生成」の場合は、保管する。	GO SAVE、オプション 21 または 23 SAV OBJ('/QIBM/UserData/Director/classes/com/ibm/sysmgt/app/iide/nwscfgname.kdb')

注: V4R5 より前のシステムで作成された統合 Windows サーバーについては、V5R3 iSeries Information Center の『保管するオブジェクトと OS/400 上のそのオブジェクトの位置』を参照してください。

統合 Windows サーバーの個々のファイルおよびディレクトリーのバックアップ

IBM iSeries 統合サーバー・サポートを使用すると、統合サーバー・データ (ファイル、ディレクトリー、共用、および Windows レジストリー) をその他の i5/OS データと一緒に、磁気テープ、光ディスク、またはディスクに保管 (*SAVF) して、そのデータを個々に復元することができます。ただし、この方法は、主なバックアップ手順としては使わないようにしてください。災害回復に備え、システム全体と Windows サーバーに関連した NWSD を周期的に保管する必要があります。それから、変更された統合サーバー・ファイルだけの日常のバックアップを行うようにすることができます。209 ページの『統合 Windows サーバーに関連付けられた NWSD およびその他のオブジェクトのバックアップ』を参照してください。

ファイル・レベルのバックアップ機能の詳細については、以下のトピックを参照してください。

- 最初に、『ファイル・レベルのバックアップの制約事項』をお読みください。
- 統合サーバーのファイル・レベルのバックアップを行うには、まず 216 ページの『予備的な管理者セットアップ・タスク』を参照してください。
- 218 ページの『ファイルの保管』

Windows 付属のバックアップ・プログラムなどのユーティリティー (220 ページの『Windows バックアップ・ユーティリティー』を参照) も使用できます。統合 Windows サーバー・ファイルのバックアップおよびリカバリーの詳細については、IBM Integrated xSeries Solutions Web サイトの『Windows サーバーのバックアップ (英語)』を参照してください。

ファイル・レベルのバックアップの制約事項

ファイル・レベルのバックアップを使用する際は、以下の制限および制約事項に注意する必要があります。

制限:

- コードが IBM i5/OS 統合サーバー・サポートと一緒にパッケージされているので、このサポートはスタンドアロン Windows サーバーでは使用できません。
- この方法では、IBM iSeries 統合サーバー・サポート・コードの一部であるファイルはバックアップされません。
- 保管 (SAV) または復元 (RST) コマンドの実行中に、ユーザーがサーバーにサインオンしたりサーバー上のデータにアクセスするのを妨げることはできません。IBM iSeries 統合サーバー・サポートは、読み取ることさえできれば、使用中のファイルを保管することができます。したがって、システムにアクセスするユーザーがいると思える場合は、統合サーバー・ファイルをバックアップする必要があります。サーバーにアクセスしないようユーザーに事前に通知しておくとうよいでしょう。

- 1 • Windows Server 2003 はその Volume Shadow copy Service (VSS) に機能を提供します。このサービスにより、ファイル・レベルのバックアップを使用するときに、アプリケーションはまだ使用中のファイルを保管することができるようになります。
- QSECOFR ユーザー・プロファイルを、ファイル・レベルのバックアップを実行するために使用しないでください。統合サーバーに登録されている場合でも、QSECOFR はファイルのバックアップには使用されません。Windows ローカル・システム・アカウントが代わりに使用されます。それには、すべての要求されるファイルをバックアップするのに必要な権限がない可能性があります。
- ユーザー・プロファイルの *LCLPWDMGMT 値が *YES の場合に、システム値 QRETSVRSEC が 1 に設定されていて、ユーザー・パスワードが変更されているか、ユーザーが QRETSVRSEC の変更後にサインオンしていること。
- ユーザー・プロファイルの *LCLPWDMGMT 値が *NO の場合に、ネットワーク認証 (Kerberos) を使用していること。ユーザーは、EIM 対応アプリケーション (iSeries ナビゲーターのシングル・サインオンなど) を使用して、iSeries 操作にアクセスする必要があります。詳しくは、171 ページの『SBMNWSCMD と、Kerberos v5 および EIM のファイル・レベルのバックアップのサポート』を参照してください。

要件:

- 1 • 統合サーバーが活動状態にあり、i5/OS との TCP/IP Point-to-Point 仮想イーサネット接続が機能している必要があります。統合サーバー・ファイルは、残りの i5/OS ファイルをバックアップするためにシステムを制限状態にする前か、制限状態操作が完了した後で、バックアップする必要があります。
- この手順では、統合サーバーと i5/OS 上で同じユーザー ID とパスワードがなければなりません。
- 統合サーバー・ユーザー・アカウントは、Administrators グループのメンバーでなければなりません。
- ファイル・レベルのバックアップでは、保管するファイルのリストを作成するのに、QNTC ファイル・システム (NetClient) を使用します。QNTC は、ドメインの中のサーバーを見つけるのに iSeries NetServer を使用します。ファイルを保管したいと思っている統合サーバーと同じドメイン (218 ページの『iSeries NetServer と統合 Windows サーバーを同じドメインに置く』を参照) に iSeries NetServer があるようにしてください。
- 以前に QNTC ファイル・システムで保管した、すべてのドライブ上のすべてのファイルを復元するには、注意が必要です。Windows システム・ファイル (たとえば、Recycle Bin のファイル) によっては、復元後に予期しない結果を引き起こすものもあります。
- Windows 2000 Server または Windows Server 2003 では、Windows システム・ファイルのバックアップと回復を行う際に、システム・ファイル保護について特別に考慮する必要があります。Microsoft の資料を参照してください。

予備的な管理者セットアップ・タスク

いくつかの予備的なセットアップ・タスクを行ってからでなければ、統合 Windows サーバー・ファイルをファイル・レベルでバックアップすることはできません。

1. ファイルの保管と復元を行っている人が、i5/OS と統合サーバー上で同じパスワードを持っているようにしてください。最も簡単な方法が、197 ページの『iSeries ナビゲーターによる Windows 環境への単一 i5/OS ユーザーの登録』に掲載されています。ユーザーが Administrators グループのメンバーになるようにもしてください。199 ページの『ユーザー・テンプレートの作成』を参照してください。
2. Windows サーバー上のすべてのファイルを保管するよう要求する際に保管したい、それぞれのドライブまたはボリューム用の共用を作成します。IBM iSeries 統合サーバー・サポートはファイル・システムをアクセスして、これらの共用をパス名に変換します。217 ページの『統合 Windows サーバーでの共有の作成』を参照してください。

3. QUSRSYS の中の QAZLCSAVL ファイルにメンバーを追加します。ここには保管できるようにしたい共有名がリストされています。『QAZLCSAVL ファイルへのメンバーの追加』を参照してください。
4. ファイルを保管したいと思っている統合サーバーと同じドメインに iSeries NetServer があるようにしてください。218 ページの『iSeries NetServer と統合 Windows サーバーを同じドメインに置く』を参照してください。
5. 保管または復元を実行するユーザーが *ALLOBJ 権限を持つようにしてください。この権限は、保管または復元プロセスに必要なプログラムおよび装置に対する全アクセス権限をユーザーに与えるものです。*ALLOBJ 権限を提供できない場合、ユーザーはオブジェクト QNTAP/QVNASBM に対して少なくとも *USE 権限を持っている必要があります。これによって、バックアップまたは復元要求を Windows サーバーとやりとりできます。

統合 Windows サーバーでの共有の作成

i5/OS 上の統合サーバー・ファイルのファイル・レベルでのバックアップおよび回復を可能にするには、保管したいデータをもったそれぞれのディレクトリーにまたがる共有を作成します。統合サーバーに共有を作成するには、統合サーバーのコンソールから次を実行します。

1. 「マイ コンピュータ」アイコンをオープンして、「Windows エクスプローラ」を開きます。
2. ドライブまたはボリュームを右クリックします。
3. ポップアップ・メニューから、「共有」を選択します。
4. 「フォルダーを共有」をクリックします。「共有名」(共有名の文字は、制限のより厳しいコード・ページ 500 文字セットの文字でなければなりません)を指定します。デフォルト共有名は、ディレクトリー名の後半部分と同じ名前になっています。共有名の長さは 12 文字までで、組み込みブランクも使用できます。
5. 無制限のアクセスか、一度に共有をアクセスするユーザーの数を制限するか選ぶことができます。「アクセス許可」ボタンを使用して、共有したいレベル(アクセス権なし、読み取り、変更、またはフルコントロール)を設定することもできます。
6. 「適用」をクリックして、共有を作成します。

QAZLCSAVL ファイルへのメンバーの追加

i5/OS からのファイル・レベルのバックアップおよびリカバリーを可能にするには、それぞれの統合 Windows サーバーのメンバーを、QUSRSYS の中の QAZLCSAVL ファイルに追加します。メンバー名には、サーバーの NWSD 名 (*nwsdname*) を使用してください。

メンバーを追加するには、次のようにします。

1. i5/OS コマンド行に、次のように入力します。


```
ADDPFM FILE(QUSRSYS/QAZLCSAVL) MBR(nwsdname)
TEXT('description') EXPDATE(*NONE) SHARE(*NO) SRCTYPE(*NONE)
```
2. 作成したばかりのファイル・メンバーに、保管できるようにしたいすべての共有がリストされています。サーバーに定義したそれぞれの共有名が別々の行にリストされます。Windows 共有名の最大長は 12 文字です。共有名には、組み込みブランクを使用できます。たとえば、cshare、dshare、eshare、fshare、gshare、および my share を WINSVR1 上の共有として定義した場合は、メンバー名 WINSVR1 は、以下のようになります。

```

                                QUSRSYS/QAZLCSAVL
                                WINSVR1

0001.00  cshare
0002.00  dshare
```

0003.00 eshare
0004.00 fshare
0005.00 gshare
0006.00 my share

注: 同じ統合サーバー・ディレクトリーを指す複数の共有名を指定すると、i5/OS は 1 つの「すべてを保管」要求についてデータを複数回保管します。保管の際にデータが重複しないようにするため、同じディレクトリーまたはデータが関与する複数個の共有を組み込まないでください。

iSeries NetServer と統合 Windows サーバーを同じドメインに置く

ファイル・レベルのバックアップ用に統合サーバー・ファイルを保管するには、保管したいファイルと同じドメインに iSeries NetServer を置くようにしなければなりません。

1. 統合サーバーのドメインを調べます。
 - a. iSeries ナビゲーターで、「**統合サーバーの管理**」 → 「**サーバー**」の順に選択します。
 - b. 右方のペインにあるリストの中で統合サーバーを見つけて、「**ドメイン**」列を見てそのサーバーのドメインを検出します。
2. iSeries NetServer のドメインを調べます。
 - a. iSeries ナビゲーターで、「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」を選択します。
 - b. TCP/IP サーバーのリストの中で iSeries NetServer を見つけます。
 - c. 「**iSeries NetServer**」を右クリックして、「**プロパティ**」を選択します (または、「**iSeries NetServer**」をダブルクリックしてから、「**ファイル**」、「**プロパティ**」を順に選択します)。iSeries NetServer のドメイン名は、「**一般情報**」ファイル・タブに表示されます。
3. iSeries NetServer が統合サーバーと同じドメインにない場合は、次のようにして iSeries NetServer のドメインを変更します。
 - a. 「**次の開始**」ボタンをクリックします。
 - b. 「**ドメイン名**」フィールドに、Windows サーバー・ドメインの名前を入力します。
 - c. iSeries NetServer を停止してから開始します (iSeries NetServer を右マウス・ボタン・クリックして、「**停止**」、「**開始**」を順に選択します)。

ファイルの保管

必要な事前作業 (216 ページの『予備的な管理者セットアップ・タスク』を参照) が終了したら、i5/OS 上の統合サーバー・ファイルをバックアップする準備が整いました。ディレクトリーまたはファイルを共有名で保管できるようにするには、SAV コマンドでそのファイルまたは共有名を明確に指定する必要があります。

注: データが重複しないようにするため、何を保管するかを SAV コマンドで指定する際には注意してください。統合サーバー上の同じディレクトリーを指す複数の共有名を指定すると、i5/OS はデータを複数回保管します。

i5/OS で保管する対象を指定するには、次のようにします。

1. 統合サーバーが活動状態であることを確認します (163 ページの『統合サーバーの開始と停止』に説明されている)。さらに、QSYSWRK サブシステム、QSERVER、および TCP/IP が活動状態であることも確認します (これは、活動ジョブの処理 (WRKACTJOB) コマンドで行うことができます)。
2. i5/OS コマンド行で、SAV と入力し、F4 を押します。
3. 「**装置**」フィールドに、i5/OS がデータを保管する装置を指定します。たとえば、'QSYS.LIB/TAP01.DEVD' と指定すると、データは磁気テープに保管されます。

- 「オブジェクト」フィールドには、i5/OS で保管するものを '/QNTC/servername/sharename' という形式で指定します。

ワイルドカード文字を使用できます。統合サーバーの特定の部分を指定する方法は、『例: 統合 Windows サーバーの各部分のアドレスを指定する方法』を参照してください。

- 「ディレクトリー・サブツリー」フィールドを使用して、ディレクトリーの下のサブツリーを保管するかどうかを指定します。デフォルトでは、すべてのディレクトリーが保管されます。
- 最後に保管した時からの変更を保管するよう指定するには、「期間の変更」フィールドに *LASTSAVE を指定します。特定の範囲の日時を指定することもできます。
- Enter キーを押して、指定した共有を保管します。

例: 統合 Windows サーバーの各部分のアドレスを指定する方法

以下の例では、SAV または RST コマンドを使用して、server1 というサーバーにおける統合サーバーの特定部分を参照する方法について示されます。

保管または復元する対象	指定
すべての統合サーバー・オブジェクト。	OBJ('/QNTC/*') SUBTREE(*ALL)
server1 のすべてのオブジェクト	OBJ('/QNTC/server1/*') SUBTREE(*ALL)
ファイルを最後に保管した時から変更された server1 のすべてのオブジェクト。	OBJ('/QNTC/server1/*') SUBTREE(*ALL) CHGPERIOD(*LASTSAVE)
特定の期間 (この場合は 10/19/99 から 10/25/99 までの間) に変更された server1 のすべてのオブジェクト。	OBJ('/QNTC/server1/*') SUBTREE(*ALL) CHGPERIOD('10/19/99' '00:00:00' '10/25/99' '23:59:59')
すべてのディレクトリー、ファイル、および特定の共有 (たとえば、'fshare') が参照している共有。i5/OS は、共有が作成されているディレクトリーの保管と復元は行いません。	OBJ('/QNTC/server1/fshare/*') SUBTREE(*ALL)
指定したパターン (pay*) と一致する、指定した共有 (たとえば、'fshare') が参照するファイルのみ。i5/OS は、ディレクトリーおよび共有を保管しません。	OBJ('/QNTC/server1/fshare/pay*')
'fshare' のディレクトリーおよび共有と、その直下の子のみ (オブジェクトは除く)。	OBJ('/QNTC/server1/fshare') SUBTREE(*DIR)
'terry' のディレクトリー、共有、およびファイルとそのサブツリー (ディレクトリー 'terry' ではない)。	OBJ('/QNTC/server1/fdrive/terry/*') SUBTREE(*ALL)
特定のファイル 'myfile.exe' のみ。	OBJ('/QNTC/server1/gdrive/myfile.exe')
統合サーバー・レジストリー。	OBJ('/QNTC/server1/\$REGISTRY')

Windows バックアップ・ユーティリティー

Windows バックアップ・ユーティリティーと iSeries 磁気テープ・ドライブを使用して、統合 Windows サーバーからバックアップを実行できます。190 ページの『統合 Windows サーバーでの iSeries 磁気テープ・ドライブの使用』を参照してください。

バックアップ・ユーティリティーを始動するには、以下のように実施します。

1. 統合サーバー・コンソールで、「スタート」をクリックします。
2. 「アクセサリ」→「システム ツール」→「バックアップ」を選択します。

LAN 接続の大容量記憶装置を使ったバックアップまたは回復についての詳細は、Microsoft 提供の Windows サーバー資料を参照してください。

統合 Windows サーバーの NWSD およびディスク・ドライブの復元

統合サーバー・データを復元する 1 つの方法は、i5/OS がサーバーと関連付けるネットワーク・サーバー記述 (NWSD) およびディスク・ドライブを復元することです。この方法は、現在でも大量のデータを復元するための一番速い方法です。ファイル・レベルのバックアップを実行した場合には、特定の統合サーバー・ファイルを復元することもできます。

i5/OS から保管したオブジェクトを復元するとき、以下の考慮事項に注意してください。

注:

1. ネットワーク・サーバー記述 (NWSD)、その事前定義されたディスク・ドライブ (179 ページの『統合 Windows サーバーの事前定義ディスク・ドライブ』を参照)、およびこれにリンクされているすべてのユーザー定義のディスク・ドライブは、一まとまりのユニットとして扱ってください。これらは同時にまとめて保管および復元してください。そうしないと、統合サーバーは Windows サーバー・ファイル・システム許可などの項目を再確立できなくなります。
2. 統合ファイル・システム内に復元したディスク・ドライブが i5/OS で適切な NWSD に自動的に再リンクされるようにするには、ディスク・ドライブを復元した後に NWSD を復元します。
3. 統合ファイル・システムの事前定義ディスク・ドライブおよびユーザー定義ディスク・ドライブを復元する前に NWSD を復元する場合、それらのディスク・ドライブを再リンクする必要があります。そうするには、NWSD に関連したディスク・ドライブごとに、ネットワーク・サーバー記憶域の追加 (ADDNWSSTGL) コマンドを使います。

```
ADDNWSSTGL NWSSTG(Storage_Name) NWSD(NWSD_Name)
```

4. ドメイン・コントローラーを復元するときは、サーバーに保持されているドメイン・データベースが他のドメイン・コントローラーと同期していることを確かめてください。Windows クラスタ・ノードが使用する共用ドライブを復元するとき、共用ドライブを手動で再リンクする必要があるかもしれません。その場合、最初に共用クォーラム・リソース・ドライブをリンクしてください。共用クォーラム・リソース・ドライブをリンクするには、以下のコマンドを使用できます。

```
ADDNWSSTGL NWSSTG(Quorum_name) NWSD(NWSD_Name) ACCESS(*SHRUPD) DYNAMIC(*YES) DRVSEQNBR(*QR)
```

共用クォーラムの再リンクが完了した後、残りの共用ドライブを再リンクすることができます。残りの共用ドライブを再リンクするには、以下のコマンドを使用します。

```
ADDNWSSTGL NWSSTG(Shared_name) NWSD(NWSD_Name) ACCESS(*SHRUPD) DYNAMIC(*YES) DRVSEQNBR(*CALC)
```

この作業を行うには、通常の Windows 手順に従います。必要に応じて Microsoft の資料を参照してください。

5. 特定のハードウェア・タイプにインストールされた NWSD を別のハードウェア・タイプに復元する場合、制限が存在する可能性があります。詳しくは、222 ページの『統合 Windows サーバー NWSD の復元』を参照してください。

統合サーバーの NWSD およびディスク・ドライブを復元するには、以下のページを参照してください。

- 『統合 Windows サーバー用事前定義ディスク・ドライブの復元』
- 222 ページの『統合 Windows サーバー用ユーザー定義ディスク・ドライブの復元』
- 222 ページの『統合 Windows サーバー NWSD の復元』

統合 Windows サーバー用事前定義ディスク・ドライブの復元

Windows オペレーティング・システムおよびレジストリーを格納するディスク・ドライブは、統合ファイル・システムに置かれます。そのような事前定義ディスク・ドライブは、ユーザー定義のディスク・ドライブの場合と同じように復元します。i5/OS 上の統合ファイル・システムの中のディスク・ドライブを復元するには、次のように復元 (RST) コマンドを使用します。

1. 保管メディアから復元する場合は、メディアがマウントされていることを確認してください。
2. ネットワーク・サーバー記憶域が現在システムに存在しない場合 (WRKNWSSTG コマンドを使用しても何も表示されない場合) は、まず /QFPNWSSTG ディレクトリーを作成し、それからそのディレクトリーの下に保管したネットワーク・サーバー記憶域を復元する必要があります。/QFPNWSSTG ディレクトリーを作成するには、以下のステップを完成させてください。
 - a. i5/OS コマンド行で、CRTNWSSTG を入力してネットワーク・サーバー記憶域を作成し、F4 を押しします。
 - b. 記憶域の名前を入力します。
 - c. 許可されている最小のサイズを使い、適切なディスク・プール (ASP) を指定します。
 - d. Enter キーを押して記憶域を作成します。i5/OS は /QFPNWSSTG ディレクトリー内に記憶域を作成します。
3. 記憶域を復元するには、RST と入力し F4 を押しします。
4. 「オブジェクト:」の下の「名前」フィールドには、'/QFPNWSSTG/stgspc' および 'dev/QASPnn/stgspc.UDFS' を指定してください。stgspc はネットワーク・サーバー記憶域の名前、nn はディスク・プールの番号です。

注: 独立ディスク・プールに対して .UDFS オブジェクトを復元するには、ディスク・プール装置をオンに変更する必要があります。dev/independent ASP name/stgspc.UDFS を指定します。
independent ASP name は独立ディスク・プールの名前で、stgspc はネットワーク・サーバー記憶域の名前です。

システム (C) ドライブを復元する場合は、/QFPNWSSTG/nwsdname1 を使用します。D ドライブを復元するには、/QFPNWSSTG/nwsdname2 を使用します。

5. 指定したい他のすべてのパラメーターに値を指定してから、Enter キーを押して記憶域を復元します。
6. さらに、サーバーに関連付けられたすべてのユーザー定義ディスク・ドライブ、および NWSD を復元する必要があります。222 ページの『統合 Windows サーバー用ユーザー定義ディスク・ドライブの復元』を参照してください。NWSD および関連したディスク・ドライブすべての復元が完了したら、統合サーバーをオンに変更してください。

注: サーバーが V4R5 より前にインストールされている場合、V5R3 iSeries Information Center の『V4R5 より前のシステムで作成した統合 Windows サーバー用事前定義ディスク・ドライブの復元』を参照してください。

統合 Windows サーバー用ユーザー定義ディスク・ドライブの復元

現在では、個々のファイルおよびディレクトリーのバックアップが可能です (215 ページの『統合 Windows サーバーの個々のファイルおよびディレクトリーのバックアップ』を参照)、大量のデータを復元する最も速い方法は、記憶域全体を復元することです。ユーザー記憶域を ¥QFPNWSSTG ディレクトリーからバックアップした場合は、記憶域全体の復元のみが可能です。212 ページの『統合 Windows サーバー用ユーザー定義ディスク・ドライブのバックアップ』を参照してください。個々のファイルは、このバックアップからは復元できません。

統合ファイル・システムの中のディスク・ドライブを復元するには、次のようにします。

1. 保管メディアから復元する場合は、メディアがマウントされていることを確認してください。
2. ネットワーク・サーバー記憶域が現在システムに存在しない場合 (WRKNWSSTG コマンドを使用しても何も表示されない場合) は、まず /QFPNWSSTG ディレクトリーを作成し、それからそのディレクトリーの下に保管したネットワーク・サーバー記憶域を復元する必要があります。/QFPNWSSTG ディレクトリーを作成するには、以下のステップを完成させてください。
 - a. i5/OS コマンド行で、CRTNWSSTG を入力してネットワーク・サーバー記憶域を作成し、F4 を押します。
 - b. 記憶域の名前を入力します。
 - c. 許可されている最小のサイズを使い、適切なディスク・プール (ASP) を指定します。
 - d. Enter キーを押して記憶域を作成します。i5/OS は /QFPNWSSTG ディレクトリー内に記憶域を作成します。
3. 記憶域を復元するには、RST と入力し F4 を押します。
4. 「オブジェクト:」名フィールドには、'/QFPNWSSTG/stgspc' および 'dev/QASPnn/stgspc.UDFS' を指定してください。stgspc はネットワーク・サーバー記憶域の名前、nn はディスク・プールの番号です。

注: 独立ディスク・プールに対して .UDFS オブジェクトを復元するには、ディスク・プール装置をオンに変更する必要があります。'dev/independent ASP name/stgspc.UDFS' を指定します。independent ASP name は独立ディスク・プールの名前、stgspc はネットワーク・サーバー記憶域の名前です。
5. 指定したい他のすべてのパラメーターに値を指定してから、Enter キーを押して記憶域を復元します。
6. また、サーバーと関連した事前定義ディスク・ドライブや、NWS D も復元する必要があります。『統合 Windows サーバー NWS D の復元』を参照してください。NWS D および関連したディスク・ドライブすべての復元が完了したら、統合サーバーをオンに変更してください。

統合 Windows サーバー NWS D の復元

災害回復を行う状況では、すべての構成オブジェクトを復元します。その 1 つが、統合 Windows サーバーのネットワーク・サーバー記述 (NWS D) です。場合によっては (たとえば、新しい統合 xSeries サーバー・ハードウェアへ移行する場合)、NWS D を個別に復元する必要があります。i5/OS が統合ファイル・システム内のディスク・ドライブを、復元された NWS D に自動的に再リンクするようにするには、まずこれらのディスク・ドライブを復元します。NWS D を復元するには、構成の復元 (RSTCFG) コマンドを使用します。

1. i5/OS コマンド行で、RSTCFG と入力し、F4 を押します。
2. 「オブジェクト」フィールドで、NWS D の名前を指定します。
3. メディアから復元する場合、「装置」フィールドに、装置名を指定します。保管ファイルから復元する場合、*SAVF を指定し、保管ファイルの名前とライブラリーを該当するフィールドに指定します。

4. Enter キーを押して、i5/OS で NWS D を復元します。
5. NWS D および関連した記憶域すべての復元が完了したら、統合サーバーを始動してください。 163 ページの『統合サーバーの開始と停止』を参照してください。

注: NWS D を復元するときは、その NWS D に関連したすべての回線および装置記述オブジェクトも復元する必要があります。さらに、TCP/IP インターフェースが定義されていたすべての回線記述を復元する必要もあります。

ISCSI 接続サーバー用の統合 Windows サーバー NWSH の復元

災害回復を行う状況では、すべての構成オブジェクトを復元します。その 1 つが、ネットワーク・サーバーホスト・アダプター (NWSH) です。NWSH を復元するには、構成の復元 (RSTCFG) コマンドを使用します。

1. i5/OS コマンド行で、RSTCFG と入力し、F4 を押します。
2. 「オブジェクト」フィールドで、NWSH の名前およびタイプを指定します。
3. メディアから復元する場合、「装置」フィールドに、装置名を指定します。保管ファイルから復元する場合、*SAVF を指定し、保管ファイルの名前とライブラリーを該当するフィールドに指定します。
4. Enter キーを押して、i5/OS で NWSH を復元します。

注:

1. NWSH を復元する場合、それを開始してから、統合サーバーを開始する必要があります。

ISCSI 接続サーバー用の統合 Windows サーバー NWSCFG の復元

iSCSI HBA で接続されたサーバーの場合、追加の構成オブジェクトを QUSRSYS ライブラリーに復元する必要があります。これには、ネットワーク・サーバー構成オブジェクト (タイプ *NWSCFG) および関連した妥当性検査リスト・オブジェクト (タイプ *VLDL) が含まれます。

注: *NWSCFG オブジェクトと *VLDL オブジェクトは同じ名前を共有します。

サーバー記憶域を復元するには、次のようにオブジェクトの復元 (RSTOBJ) コマンドを使用します。

1. i5/OS コマンド行で、RSTOBJ と入力し、F4 を押します。
2. 保管メディアから復元する場合は、メディアがマウントされていることを確認してください。
3. 「オブジェクト」フィールドで、ネットワーク・サーバー構成の名前を指定します。(複数の NWSCFG を復元する場合は、総称名 『nwsdname*』 を入力します。また、+ を入力して Enter キーを押すことにより、オブジェクト名を明示的に識別することもできます。)
 - デフォルトの接続セキュリティ・ネットワーク・サーバー構成を復元するには、NWS D の名前の後に CN を指定します。
 - デフォルトのサービス・プロセッサ・ネットワーク・サーバー構成を復元するには、NWS D の名前の後に SP を指定します。
 - デフォルトのリモート・システム・ネットワーク・サーバー構成を復元するには、NWS D の名前の後に RM を指定します。
4. 「ライブラリーの保管」フィールドで、QUSRSYS と指定します。
5. 「装置」フィールドに、保管メディアを備えた装置の名前を指定します。保管ファイルから復元している場合は、このフィールドに *SAVF と指定します。
6. オブジェクトの種類」フィールドに、*NWSCFG と *VLDL の両方を指定します。

- l 7. 保管ファイルから復元する場合、保管ファイルの名前とライブラリーを指定します。
- l 8. Enter キーを押して、ネットワーク・サーバー構成と関連した妥当性検査リストを復元します。

統合 Windows サーバー・ファイルの回復

IBM iSeries 統合サーバー・サポートでは、ファイル・レベルのバックアップおよびファイルの回復がサポートされています。ディスク・ドライブ全体を復元しなくても、個々のファイルを i5/OS バックアップから回復できるようになりました。ただし、この方法を使用する前に、復元する必要があるデータの量を考慮してください。データの量が多いと、ディスク・ドライブ全体の復元オブジェクトを使用した方が、ディスク・ドライブの中のすべての個別のファイルを復元するよりもずっと早くなります。少ない量のデータを復元するには、この方法は大いに役立ちます。

最初にディレクトリー、次にファイル、その次にレジストリーを復元してから、新しいレジストリー項目が有効になるようにリポートする必要があります。この方法で保管したファイルを復元するには、次のように RST コマンドを使用します。

1. 統合 Windows サーバーと TCP/IP が実行されていることを確認してください。
2. i5/OS コマンド行で、RST と入力し、F4 を押します。
3. 「装置」フィールドに、データが使用可能になっている装置を指定します。(たとえば、'QSYS.LIB/TAP01.DEVD' と指定すると、データが磁気テープから復元されます。)
4. 「オブジェクト」フィールドには、i5/OS で保管するものを '/QNTC/servername/sharename' という形式で指定します。

ワイルドカード文字を使用できます。統合 Windows サーバーの特定の部分を指定する方法は、219 ページの『例: 統合 Windows サーバーの各部分のアドレスを指定する方法』を参照してください。復元したファイルの動作を予測できなくなる可能性があるため、この方法を使って Windows システム・ファイルを復元しないようにしてください。

5. 「名前」フィールドに、復元するオブジェクトのパス名を指定します。
6. 「組み込みまたは除外」フィールドを使用して、「オブジェクト」パラメーターの「名前」の部分に指定したパターンをもつオブジェクトを、組み込むか除外することができます。
7. 「新規オブジェクト名」フィールドには、オブジェクト名をそのまま残すか、新しいパス名を指定します。新しいパス名は、統合 Windows サーバーに存在する共用名によって参照されます。

注: 共有されているディレクトリーを保管するときは、i5/OS は共有情報をディレクトリーと一緒に保管します。ディレクトリーを復元するときに新しいオブジェクト名を指定する場合には、i5/OS はこれらの共有を再作成しません。

8. 「ディレクトリー・サブツリー」フィールドを使用して、ディレクトリーの下サブツリーを復元するかどうかを指定します。デフォルトでは、すべてのディレクトリーが復元されます。
9. 特定の期間に保管されたファイルを復元するよう指定するには、「期間の変更 (Change period)」フィールドに開始日時と終了日時を指定します。
10. i5/OS がファイルを復元するのに使用する他の情報についても、入力して Enter キーを押してください。
11. ファイルが復元されたら、統合サーバーをリポートして新しいレジストリー項目が有効になるようにします。

第 13 章 統合サーバー・ハードウェアから Windows サーバー・オペレーティング・システムをアンインストールする

Windows サーバーの削除 (DLTWNTSVR) コマンドを使用して、統合 xSeries サーバーから Windows サーバーをアンインストールできます。Windows サーバーの削除コマンドを実行する前に、i5/OS から統合 Windows サーバーをシャットダウンしてください。163 ページの『統合サーバーの開始と停止』を参照してください。

Windows サーバーの削除 (DLTWNTSVR) コマンドは、指定された Windows ネットワーク・サーバー記述、および関連オブジェクトを削除します (これらは、Windows サーバー導入 (INSWNTSVR) コマンドで作成されたものです)。これらのオブジェクトには、ネットワーク・サーバー記述、回線記述、TCP/IP インターフェース、およびシステムの作成したネットワーク・サーバー記憶域が含まれます。このコマンドを発行する前に、ネットワーク・サーバーをオフラインに構成変更しておく必要があります。

- | DLTWNTSVR コマンドを使用できない場合 (たとえば、サーバーの NWSD オブジェクトはすでに存在し
- | ていないが、関連したオブジェクトのいくつかをクリーンアップする必要がある場合)、以下の手順を使用
- | して、サーバーおよび関連したオブジェクトを手動で削除することができます。
 1. 統合サーバーをシャットダウンし、163 ページの『統合サーバーの開始と停止』を参照してください。
 2. 186 ページの『統合 Windows サーバー・ディスク・ドライブのリンク解除』。
 3. 186 ページの『統合 Windows サーバー・ディスク・ドライブの削除』。
 4. 『統合 Windows サーバーの NWSD の削除』。
 5. 226 ページの『統合 Windows サーバーの回線記述の削除』。
 6. 226 ページの『統合 Windows サーバーに関連した TCP/IP インターフェースの削除』。
 7. 227 ページの『統合 Windows サーバーに関連した制御装置記述の削除』。
 8. 227 ページの『統合 Windows サーバーに関連した装置記述の削除』。
 - | 9. 227 ページの『iSCSI 統合 Windows サーバーに関連したネットワーク・サーバー構成の削除』

特定のネットワーク・サーバー・ホスト・アダプター (NWSH) オブジェクトを使用する、すべての Windows サーバーおよび Linux サーバーを i5/OS から除去し、それ以降は NWSH を使用するサーバーをインストールしない予定である場合、NWSH を削除できます。132 ページの『ネットワーク・サーバー・ホスト・アダプターの削除』を参照してください。

すべての Windows サーバーおよび Linux サーバーを i5/OS から除去し、それ以降はインストールしない予定である場合、IBM iSeries 統合サーバー・サポートを削除して、製品が使用する記憶域を解放することができます。228 ページの『IBM i5/OS 統合サーバー・サポート、i5/OS オプション 29 (5722-SS1) の削除』を参照してください。

統合 Windows サーバーの NWSD の削除

ネットワーク・サーバー記述 (NWSD) を削除する前に、そのディスク・ドライブをリンク解除し (186 ページの『統合 Windows サーバー・ディスク・ドライブのリンク解除』を参照)、その NWSD に関連した記憶域を削除する (186 ページの『統合 Windows サーバー・ディスク・ドライブの削除』を参照) 必要があります。その後で NWSD を削除できます。

1. V4R5 およびそれ以降で作成された NWSD のシステム・ドライブの記憶域をリンク解除するには、i5/OS コマンド行で `RMVNWSSSTGL NWSSTG(nwsdname1) NWSD(nwsdname)` と入力します。Enter キーを押します。
2. インストール・ソース・ドライブの記憶域をリンク解除するには、`RMVNWSSSTGL NWSSTG(nwsdname2) NWSD(nwsdname)` と入力し、Enter キーを押します。
3. NWSD にリンクしていたユーザー定義の記憶域もすべてここで除去することができます。それには、必要な回数だけ `RMVNWSSSTGL NWSSTG(nwsstgname) NWSD(nwsdname)` を使ってから Enter キーを押します。
4. システム・ドライブのネットワーク・サーバー記憶域を削除するには、`DLTNWSSSTG NWSSTG(nwsdname1)` コマンドを入力し、Enter キーを押します。
5. インストール・ソース・ドライブのネットワーク・サーバー記憶域を削除するには、`DLTNWSSSTG NWSSTG(nwsdname2)` を入力し、Enter キーを押します。
6. もう必要のないそれ以外の記憶域も除去します。それには、`DLTNWSSSTG NWSSTG(nwsstgname)` コマンドを入力してから Enter キーを押します。

統合サーバーのネットワーク・サーバー記述 (NWSD) を削除するには、次のステップを行います。

1. i5/OS 上で、コマンド `WRKNWSD` を入力して、Enter キーを押します。
2. 「ネットワーク・サーバー」の左側の「Opt」フィールドに 8 を入力して、Enter キーを押します。「構成状況処理」画面が表示されます。
3. NWSD の状況がオフに構成変更されていない場合、「ネットワーク・サーバー」の左側の「Opt」フィールドに 2 を入力して、Enter キーを押します。それ以外の場合、次のステップへ進みます。
4. F3 キーを押して直前のダイアログに戻ります。
5. 「ネットワーク・サーバー」の左側の「Opt」フィールドに 4 を入力して、Enter キーを押します。
6. 「ネットワーク・サーバー記述の削除の確認」画面で、Enter キーを押します。

注: V4R5 より前に作成された NWSD を削除する場合、V5R3 iSeries Information Center の『統合 Windows サーバーの NWSD の削除』を参照してください。

統合 Windows サーバーの回線記述の削除

統合サーバーのすべての回線記述を削除するには、以下のステップに従います。

1. i5/OS 上で、コマンド `WRKLIND` を入力して、Enter キーを押します。
2. 削除したい回線記述が表示されるまで、次ページ・キーを押します。

注: 回線記述の名前は、ネットワーク・サーバー記述 (NWSD) の名前の後に 00、01、02、PP、V0、V1、V2、V3、V4、V5、V6、V7、V8 または V9 が付いたものです。これは、回線を接続したポート番号に依存しています。

3. 回線記述の左側の「Opt」フィールドに 4 を入力して、Enter を押します。NWSD に関連したその他のすべての回線記述について、このステップを繰り返します。

注: ステップ 1 および 2 に代わる方法として `WRKLIND nwsdname*` コマンドを使用することができます。nwsdname は、関連したネットワーク・サーバー記述の名前です。

統合 Windows サーバーに関連した TCP/IP インターフェースの削除

統合サーバーに関連した TCP/IP インターフェースを削除するには、次のステップを行います。

1. i5/OS コンソールで、`CFGTCP` コマンドを入力します。

2. 「TCP/IP メニューの構成」画面から、オプション 1「TCP/IP インターフェースの処理」を選択します。
3. 削除したい TCP/IP インターフェースの横にある「Opt」フィールドに 4 を入力して、Enter キーを押します。

付けられた回線記述の名前を検索すれば、ネットワーク・サーバー記述 (NWS D) に関連した TCP/IP インターフェースを識別できます。この名前は NWS D 名で構成されており、その後には数字が付けられます。

4. NWS D に関連した TCP/IP インターフェースごとに、ステップ 3 を繰り返します。

統合 Windows サーバーに関連した制御装置記述の削除

統合サーバーの制御装置記述をすべて削除するには、次のステップを行います。

1. i5/OS 上で、コマンド WRKCTLD を入力して、Enter キーを押します。
2. 削除したい制御装置記述が表示されるまで、次ページ・キーを押します。

注: 制御装置記述の名前は、NWS D 名の 5 文字で始まり、それに「NET」および 2 つの数字が続きます。たとえば、NWS D 名が MYSERVER である場合、制御装置名は MYSERNET01 とすることができます。

3. 制御装置記述の左側の「Opt」フィールドに 4 を入力して、Enter を押します。NWS D に関連したその他のすべての制御装置記述について、このステップを繰り返します。

注: ステップ 1 および 2 に代わる方法として WRKCTLD MYSER* コマンドを使用することができます。MYSER は NWS D 名の最初の 5 文字です。

重要: この方法を使用する場合、これらの 5 文字で始まる、システム上の NWS D をすべて削除するか確認してください。

統合 Windows サーバーに関連した装置記述の削除

統合サーバーの装置記述をすべて削除するには、次のステップを行います。

1. i5/OS 上で、コマンド WRKDEVD を入力して、Enter キーを押します。
2. 削除したい装置記述が表示されるまで、次ページ・キーを押します。

注: 装置記述の名前は、NWS D 名の 5 文字で始まり、それに「TCP」および 2 つの数字が続きます。たとえば、NWS D 名が MYSERVER である場合、装置名は MYSERTCP01 とすることができます。

3. 装置記述の左側の「Opt」フィールドに 4 を入力して、Enter を押します。NWS D に関連したその他のすべての装置記述について、このステップを繰り返します。

注: システムには多数の装置が装備されていることがあります。削除する必要があるネットワーク装置の全リストを見るには、WRKDEVD MYSERTCP* または WRKDEVD *NET コマンドを使います。

iSCSI 統合 Windows サーバーに関連したネットワーク・サーバー構成の削除

統合サーバーに関連したネットワーク・サーバー構成を削除するには、次のステップを行います。

1. i5/OS コンソールで、WRKNWSCFG コマンドを入力します。

- 1 2. NWS D に関連したネットワーク・サーバー構成を見つけます。通常、これは一般的に nwsdname* で識別されます。
- 1 3. 削除したいネットワーク・サーバー構成の横にある「Opt」フィールドに 4 を入力します。
- 1 4. **Enter** キーを押します。

IBM i5/OS 統合サーバー・サポート、i5/OS オプション 29 (5722-SS1) の削除

- 1 iSeries からすべての統合 Windows サーバーおよび非区画 Linux サーバーを除去し、他のものを再インストールする計画がない場合には、i5/OS から IBM i5/OS 統合サーバー・サポート、オプション 29 を削除することもできます。プログラムを削除すると、i5/OS 上で占有されていた記憶域が解放されます。


注: プログラムを削除しても、既存のネットワーク・サーバー記述、あるいはユーザー定義のディスク・ドライブは自動的に削除されません。しかし、オプションを削除するとそれらは使用不能になります。ネットワーク・サーバー記述およびディスク・ドライブの削除についての詳細は、225 ページの『第 13 章 統合サーバー・ハードウェアから Windows サーバー・オペレーティング・システムをアンインストールする』を参照してください。

IBM i5/OS 統合サーバー・サポートを削除するには、以下のステップを実行してください。

1. i5/OS 上で、コマンド GO LICPGM を入力して、Enter キーを押します。
2. 「ライセンス・プログラムの処理」メニューから、オプション 12 を選択して、Enter キーを押します。
- 1 3. 「統合サーバー・サポート」が表示されるまで、次ページ・キーを押して、ライセンス・プログラムのリストを下に移動します。
- 1 4. オプションの左側の「オプション」フィールドに 4 を入力します。 Enter キーを押します。 i5/OS によってオプションが削除されます。




第 14 章 統合 Windows サーバーのトラブルシューティング

統合サーバーが正しく動作しない場合、以下のステップに従って問題を修正してください。

1. 統合サーバーを再始動してみます。 163 ページの『統合サーバーの開始と停止』を参照してください。
2. NWSD とそれに関連する回線、制御装置、および装置についての情報を表示します。 166 ページの『統合 Windows サーバーの構成情報の表示または変更』を参照してください。
3. 問題が解決しない場合は、ログから有用な情報を探してください。 230 ページの『メッセージ・ログとジョブ・ログのチェック』を参照してください。
4. 次に、232 ページの『統合 Windows サーバーの問題』で特定の問題を探してください。
5. また、最新のヒントおよびサービス情報については、情報 APAR をチェックしてください。これは、
IBM 統合 xSeries ソリューション (英語) Web サイト  にあります。
6. 統合サーバーが損傷を受けている場合、それを再インストールすることによって、インストールしてあるアプリケーションおよびユーザー・データを保護できます。 269 ページの『統合 Windows サーバーの再インストール』を参照してください。
7. サービス・データを収集してサポート担当者に送ることについては、 270 ページの『統合 Windows サーバーのサービス・データの収集』を参照してください。

問題解決のためのその他のオプション

発生した問題に対するソリューションがこの章のトラブルシューティングの項に解説されていない場合、他のサービス・オプションを使えばその問題を解決できることがあります。

- 統合 xSeries ソリューション (英語) Web サイト
(www.ibm.com/servers/eserver/series/integratedxseries/troubleshooting.html) の トラブルシューティング (英語)  を参照してください。
- 個々のアプリケーションで起きた問題の場合、そのアプリケーションの提供者に問い合わせてください。
- 統合 xSeries サーバーのハードウェアのエラーの場合や、サーバーのインストールでの問題の場合、IBM 技術部にご連絡ください。
- サーバーの回復不能エラー (ブルー・スクリーンなど) の場合、以下の Web サイトに追加情報が載っているかもしれません。
 - iSeries ファミリーのサポート (英語)  (www.ibm.com/servers/eserver/support/series/)。
 - Microsoft サポート オンライン  (<http://support.microsoft.com>)。

さらに解説が必要な場合は、IBM サービス契約に沿って問題解決のための正しい方策を特定するための助言を IBM 技術部門が行います。必要があれば IBM Support Line にご連絡ください。

メッセージ・ログとジョブ・ログのチェック

統合 Windows サーバーについての情報は、いくつかの場所にログとして記録されます。問題が発生した場合は、その原因を突き止めるのにこの情報を役立てることができます。

ジョブ・ログのモニター

モニター・ジョブ・ログ (231 ページの『モニター・ジョブ』のトピックを参照) には、通常の処理イベントから詳細なエラー・メッセージまでさまざまなメッセージが記録されます。このログをチェックするには、以下のようにします。

1. i5/OS コマンド行で、活動ジョブの処理 (WRKACTJOB) コマンドを使用して、ネットワーク・サーバーと同じ名前の QSYSWRK サブシステム内でジョブを検索します。この画面にジョブが表示されない場合は、ジョブは終了したか開始されていないかのどちらかです。
2. ジョブが表示されているなら、ジョブを処理する場合はオプション 5、ジョブ・ログを表示するにはオプション 10 を使用します。
3. 詳細なメッセージを表示するには、F10 を押します。
4. ログ内の有用な情報を見つけるには、ジョブ ID (3 つの部分全部: 名前、ユーザー、および番号) を入力します。その後、次のコマンドを使用してそのログを印刷します。DSPJOBLOG JOB(number/user/name) OUTPUT(*PRINT)

注: 問題が発生したためにモニター・ジョブが終了した場合や、現在のモニター・ジョブの前に発生した問題をデバッグする場合は、直前のジョブ・ログの情報が収められているスプール・ファイルを検索してください。使用しているネットワーク・サーバーを処理するスプール・ファイルを検索するには、次のコマンドを使います。WRKSPLF SELECT(QSYS *ALL *ALL nwsd_name)

QVNAVARY ジョブ・ログ

QVNAVARY ジョブ・ログには、Windows サーバーのシャットダウンおよび再始動時に、IXS または IXA 接続のネットワーク・サーバー記述をオンに変更、またはオフに変更する操作に関するメッセージが入っています。このログをチェックしてシャットダウンおよび再始動時のエラーを調べるには、以下のようにします。

1. i5/OS コマンド行で、活動ジョブの処理 (WRKACTJOB) コマンドを使用して、QSYSWRK サブシステム内で QVNAVARY ジョブを検索します。
2. ジョブを処理する場合はオプション 5、ジョブ・ログを表示するにはオプション 10 を使用します。

また、WRKJOB JOB(QVNAVARY) を使用することもできます。

IXS または IXA 接続の xSeries サーバーの場合、サーバーの「リポート」に必要なオフおよびオンへの変更を実行するために、BTnwsdname という名前を使用したバッチ・ジョブがサブミットされます。

QVNAVARY ジョブ・ログでサブミットされたジョブの修飾名を識別します。WRKSPLF SELECT(*ALL) JOB(qualjobname) を使用してジョブ名を完全に修飾することにより、サブミットされた「リポート」ジョブがないか、ジョブ・ログを探します。

WRKSPLF SELECT(*ALL) JOB(BTnwsdname) ですべての「リポート」ジョブをリストします。

オンまたはオフへの変更を開始したジョブのジョブ・ログ

バッチ・ジョブまたは対話式ユーザーが i5/OS から NWS D のオンまたはオフへの変更を開始した場合は、そのジョブのログを見れば役立つ情報が見つかることがあります。たとえば、VRYCFG または WRKCFGSTS コマンドを使用した場合は、ジョブの表示 (DSPJOB) コマンドとオプション 10 を使用して、そのジョブ・ログを参照することができます。

サーバー・メッセージ待ち行列

インストール時にネットワーク・サーバーのメッセージ待ち行列を指定した場合は、そのメッセージ待ち行列に役立つ情報が見つかることがあります。

1. メッセージ待ち行列を指定したかどうかを確認する必要がある場合は、i5/OS コマンド行で DSPNWS D NWS D(nwsd_name) と入力して、Enter を押します。*none に設定されていれば、重要なメッセージだけが QSYSOPR メッセージ待ち行列に入れられます。
2. メッセージ待ち行列が指定されている場合は、i5/OS で次のコマンドを使用してメッセージを表示します。DSPMSG MSGQ(library/queue)

システム・オペレーターのメッセージ待ち行列

統合サーバーでは、システム・オペレーターのメッセージ待ち行列 (QSYSOPR) が、通常の始動およびシャットダウン時のメッセージと障害メッセージによって更新されます。これらのメッセージを文字ベースのインターフェースで表示するには、DSPMSG QSYSOPR と入力します。

通信メッセージ待ち行列

iSCSI 接続のサーバーには、通信メッセージ待ち行列パラメーターが含まれます。インストール時にネットワーク・サーバーの通信メッセージ待ち行列を指定した場合は、そのメッセージ待ち行列に通信状況メッセージに関する役立つ情報が見つかることがあります。

1. 指定されたメッセージ待ち行列を確認する必要がある場合、i5/OS コマンド行で DSPNWS D NWS D(nwsd_name) と入力して、Enter を押します。通信メッセージ待ち行列が *SYSOPR に設定されている場合、メッセージは QSYSOPR メッセージ待ち行列に入れられます。
2. 通信メッセージ待ち行列が指定されている場合は、i5/OS で次のコマンドを使用してメッセージを表示します。DSPMSG MSGQ(library/queue)

プロファイル同期ジョブ・ログ

プロファイル同期ジョブ・ログには、EIM およびユーザー・プロファイル登録メッセージが記されます。このログをチェックするには、WRKJOB QPRFSYNCH と入力します。

モニター・ジョブ

活動状態のすべての統合 Windows サーバーには、サーバー起動時に開始されるモニター・ジョブがあります。モニター・ジョブは、QSYS ユーザー・プロファイルの下の QSYSWRK サブシステムの中で実行されます。ジョブ名は、モニター対象のネットワーク・サーバー記述の名前です。

モニター・ジョブが開始されると、i5/OS は通知メッセージ、CPIA41B を QSYSOPR メッセージ待ち行列に送信します。このメッセージには、モニター・ジョブのジョブ ID が示されています。このジョブ ID はジョブの処理 (WRKJOB) コマンドと一緒に使用して、モニター・ジョブ・ログとモニター・ジョブのジョブに関連したその他の情報を見つけることができます。

■ iSCSI 接続のサーバーの追加ログおよびメッセージ

■ ネットワーク・サーバー・ホスト・アダプター・ジョブ・ログ

■ ネットワーク・サーバー・ホスト・アダプターは、i5/OS によって特定のシステム・ジョブに割り当てられます。ネットワーク・サーバー・ホスト・アダプターに関連したシステム・ジョブのジョブ・ログに、役立つ情報が見つかることがあります。

- 1. システム・ジョブの名前を判別するには、i5/OS コマンド行で DSPDEV DEVD(nwshname) と入力して、Enter を押します。次ページ・キーを押して、ジョブ名の値に移動します。
- 2. ジョブの表示 (DSPJOB) コマンドを使用し、オプション 10 を選択して、上記で識別されるジョブのジョブ・ログを参照します。

■ ネットワーク・サーバー・ホスト装置メッセージ待ち行列

■ ネットワーク・サーバー・ホスト・アダプターには、メッセージ待ち行列パラメーターが含まれます。このメッセージ待ち行列に、役立つ情報がみつかることがあります。

- 1. 使用されているメッセージ待ち行列を判別する必要がある場合は、131 ページの『ネットワーク・サーバー・ホスト・アダプターのプロパティの表示』を参照してください。「通信」タブをクリックし、メッセージ待ち行列名およびライブラリーをメモします。
- 2. iSeries ナビゲーターを使用してメッセージ待ち行列を表示するには、以下のステップを行ってください。
 - a. 「基本操作」→「メッセージ」と展開します。
 - b. 「メッセージ」を右クリックし、「このビューをカスタマイズ」→「組み込み...」と選択します。
 - c. 「メッセージ待ち行列」オプションを選択し、「ネットワーク・サーバー・ホスト・アダプターのプロパティ」パネルにメッセージ待ち行列名およびライブラリーを入力します。

■ 注: 「NWSH プロパティ」パネルに「システム・オペレーター」が表示される場合は、メッセージ待ち行列名に QSYSOPR を指定してください。

■ プロダクト・アクティビティ・ログ (PAL)

■ iSCSI ネットワークに関連したエラーの一部 (CHAP 認証障害など) は、PAL に記録されます。PAL にアクセスするには、以下のステップを行ってください。

- 1. システム保守ツールの開始 (STRSST) CL コマンドを実行します。
- 2. 「保守ツールの開始」を選択します。
- 3. 「プロダクト・アクティビティ・ログ」を選択します。

統合 Windows サーバーの問題

統合 Windows サーバーが正常に機能していない場合は、発生している問題が以下のいずれかに当てはまるかどうかを確かめてください。

- 233 ページの『STOP またはブルー・スクリーン・エラー』
- ソフトウェア保守プログラムの使用に関連した問題。246 ページの『IBM iSeries 統合サーバー・サポート・スナップイン・プログラム』を参照してください。
- **ドライブ関連の問題**
 - 234 ページの『統合サーバーでのシステム・ドライブ空き容量不足』
- **装置関連の問題**
 - 235 ページの『光ディスク装置の問題』
 - 235 ページの『磁気テープ関連の問題』

- 始動/停止時の問題

- 237 ページの『統合 Windows サーバーの始動に関する問題』
- 239 ページの『サーバー間のホット・スペアリングに関する問題』
- 242 ページの『NWS D 構成ファイルのエラー』

- 外部接続された xSeries サーバー

- 243 ページの『IXA または iSCSI 接続のサーバーの DASD』

- ユーザーおよびグループの登録に関連した問題

- 243 ページの『ユーザーおよびグループの登録時の障害』
- 244 ページの『ユーザー登録権限の問題』
- 245 ページの『パスワードの問題』

- | • iSCSI 接続の xSeries または IBM BladeCenter サーバー

- | - 247 ページの『iSCSI 接続のサーバーの問題』
- | - 249 ページの『ブートおよび記憶域パス・ネットワークの分析』
- | - 250 ページの『パス証明書の管理』
- | - 250 ページの『IBM Director のトラブルシューティング』
- | - 251 ページの『ディスカバリーの問題』
- | - 252 ページの『SSL 接続の問題』
- | - 254 ページの『iSCSI 接続のサーバーの仮想イーサネットの問題』


- ネットワーキング関連の問題

- 257 ページの『IXS および IXA 接続のサーバーの仮想イーサネットの問題』
- 260 ページの『外部ネットワークに関する問題』
- 261 ページの『統合 Windows サーバーでの LAN ドライバーの手動アップデート』
- 263 ページの『Point-to-Point 仮想イーサネット IP アドレスの競合』
- 267 ページの『IFS アクセスの問題』
- 265 ページの『仮想イーサネット上の TCP/IP の問題』
- 266 ページの『QNTC ファイル・システムによる Windows Server 2003 共用へのアクセス時の問題』

- | • 240 ページの『ホストされるシステム・ハードウェアの共用に関する問題』

- 267 ページの『統合 Windows サーバー・ファイルの保管の問題』
- 268 ページの『サーバー・メッセージ待ち行列の判読不能メッセージ』
- 268 ページの『Windows システム・メモリー・ダンプを取る際の問題』

- | 調査中の問題を上記のトピックで扱っていない場合、統合 xSeries ソリューション Web サイト **トラブル**

- | **シューティング** (英語)  のページ




- | (<http://www.ibm.com/servers/eserver/series/integratedxseries/troubleshooting.html>) を参照してください。この

- | Web ページは、トラブルシューティング情報の追加ソースを参照しています。

STOP またはブルー・スクリーン・エラー

ブルー・スクリーン・エラーが表示される場合、以下のアクションを実行して、エラーの原因を判別し、修正してください。

1. i5/OS コマンド行に、DSPMSG QSYSOPR と入力します。
2. Enter キーを押します。QSYSOPR メッセージ待ち行列が表示されます。

3. ブルー・スクリーンを引き起こした原因を判別するのに役立つ情報がないかどうか、メッセージを調べます。
4. i5/OS で統合サーバーをオフに変更してからもう一度オンにして、再起動します (163 ページの『統合サーバーの開始と停止』を参照してください)。
5. Windows のイベント・ログで、エラー、停止コードのタイプ、その他の診断情報を調べます。
6. PAL 項目および VLOG を調べます。
7. 問題が続く場合には、 [IBM iSeries サポート Web ページ \(英語\)](#)  の技術情報データベースをチェックしてください。それでも解決しない場合には、テクニカル・サポート・プロバイダーに連絡してください。
8. iSCSI 接続のサーバーの場合、iSCSI トラブルシューティング (英語)  (www.ibm.com/servers/eserver/series/integratedxseries/iscsireadme/troubleshooting.html) を参照してください。



統合サーバーでのシステム・ドライブ空き容量不足

システム・ドライブには、Windows サーバー・オペレーティング・システムが含まれるほか、場合によってはアプリケーションとデータが含まれます。このドライブのスペースがなくなった場合、ドライブのスペースがなくなったことを示すメッセージや、ページング・ファイルのエラーが起こります。

システム・ドライブのスペースがなくならないようにするために、以下のステップの 1 つまたは複数を行ってください。



- Windows サーバーのインストール時に、システム・ドライブのサイズを増やしてください。
- アプリケーションをインストールするときには、システム・ドライブへのインストール (デフォルト) ではなく、ユーザー定義の記憶域にインストールしてください。
- Windows サーバー・ページング・ファイルを、デフォルトの場合のシステム・ドライブではなく、ユーザー定義の記憶域に移動してください。ページング・ファイルを移動すると、STOP エラーまたはブルー・スクリーンが発生したときに、システム・メモリー・ダンプを収集できなくなります。それでもこれを実行したい場合は、次のステップを行います。
 1. 「マイ コンピュータ」アイコンを右マウス・ボタン・クリックして、「プロパティ」を選択します。
 2. 「詳細」タブを選択します。
 3. 「パフォーマンス」オプション・ボタンをクリックします。
 4. 「仮想メモリ」で「変更」ボタンをクリックします。
 5. 必要なフリー・スペースが十分にあるユーザー定義の記憶域を選択します。
 6. 「OK」をクリックします。
- Windows サーバー・メモリー・ダンプを、デフォルトの場合のシステム・ドライブではなく、ユーザー定義の記憶域に移動してください。そうするには、次のステップを行います。
 1. 「スタート」、「設定」、「コントロール パネル」の順に選択します。
 2. 「スタートアップ/シャットダウン」タブをクリックします。
 3. 画面の「回復」セクションで、「デバッグ情報を次へ書き込む」ボックスを選択します。
 4. 十分なフリー・スペース (RAM サイズに 12 MB を加えたサイズ) のあるユーザー定義記憶域を選択します。ページ・サイズの補足的な勧告や要件については、Windows の資料を参照してください。
 5. 「OK」をクリックします。

注: Windows サーバー・メモリー・ダンプをユーザー定義の記憶域に移動する場合には、そのダンプ・ファイルをテープに複写して、テクニカル・サポートに送る必要があります。

- 問題が続く場合には、 IBM iSeries サポート Web ページ (英語)  の技術情報データベースをチェックしてください。それでも解決しない場合には、テクニカル・サポート・プロバイダーに連絡してください。

光ディスク装置の問題

統合 Windows サーバーで i5/OS 光ディスク装置が機能しない場合、以下の措置をとってください。

1. i5/OS 上で光ディスク装置をオンに変更していることを確認します。光ディスク装置のオンへの変更について、詳細は 189 ページの『統合 Windows サーバーでの iSeries 光ディスク装置の使用』をご覧ください。
2. 光ディスク装置が統合サーバーに割り振られていることを確かめます。
3. ドライブ内に光メディアが入っていることを確かめます。
4. システムに論理区画がある場合は、統合サーバーと同じ区画に光ディスク装置が割り振られていることを確認します。
5. 光ディスク装置エラーのイベント・ログを調べます。
6. 統合 Windows サーバーの「マイ コンピュータ」に、その光ディスク装置が示されていることを確認します。
7. 光ディスク装置を回復するステップは次のとおりです。
 - a. IBM iSeries 統合サーバー・サポート・スナップイン・プログラムをクローズします。
 - b. iSeries 上の光ディスク装置をオフに変更します。
 - c. 光ディスク装置をオンに変更します。
 - d. 装置を統合サーバーに割り振りし直します。
8. 問題が続く場合には、 IBM iSeries サポート Web ページ (英語)  の技術情報データベースをチェックしてください。
9. それでも解決しない場合には、テクニカル・サポート・プロバイダーに連絡してください。

光ディスク装置をアンロックする前に統合サーバーに障害が起きた場合、i5/OS やその他の統合サーバーはこの装置を使えなくなります。詳しくは、『障害が起きたサーバーのロックされた光ディスク装置』を参照してください。



障害が起きたサーバーのロックされた光ディスク装置

光ディスク装置をアンロックする (またはサーバーをオフに変更する) 前に統合サーバーに障害が起きたら、i5/OS またはその他の Windows サーバーは光ディスク装置を使えなくなります。その場合、WRKCFGSTS *DEV *OPT を使用していったん光ディスク装置をオフに変更してから、再びオンに変更してロックを外します。

磁気テープ関連の問題

統合 Windows サーバーで iSeries 磁気テープ・ドライブが機能しない場合、以下の処置をとってください。

1. i5/OS で磁気テープ・ドライブをオフに変更していること、および統合サーバーでこれをロックしていることを確認します。192 ページの『統合 Windows サーバーに対する iSeries テープ・ドライブの割り振り』を参照してください。次のいずれかの理由で、装置がロックに失敗することがあります。

- 磁気テープ装置またはそのテープ・ライブラリーがオンに変更されている。
 - デバイス・ドライバーがロードされていない。
 - 磁気テープ装置がサポートされていない。
 - 装置のロックに問題がある場合は、デバイス・ドライバーが統合サーバーにロードされていることを確認してください。通常、これは自動的に行われます。『磁気テープ・ドライブの装置ドライバーがロードされていることの確認』を参照してください。
 - ご使用の磁気テープ・ドライブがサポートされていることを確認します。 193 ページの『サポートされている iSeries 磁気テープ・ドライブ』を参照してください。
2. より高機能のアプリケーションでは、アプリケーション・インターフェースを終了した後も続行するサービスに対して装置をロックする場合があります。このようにすると、他のアプリケーションがその装置を使うことができなくなります。システムを再始動すると、これらのサービスは、アプリケーションが装置を使用できないようにロックした状態で、自動的に開始します。アプリケーションのサービス (Seagate、Computer Associates など) を表示するには、以下のようになります。
 - a. 「スタート」、「プログラム」、「管理ツール」、「コンポーネント サービス」の順にクリックします。
 - b. 「サービス」をダブルクリックします。
 - c. 必要であれば、「サービス」ウィンドウからサービスを停止できます。
 3. 複数の統合サーバーが所有できます。その場合、磁気テープを使用するサーバー以外のすべてのサーバーで、磁気テープ・ドライブがアンロックされていることを確認してください。 194 ページの『統合 Windows サーバー間での iSeries テープ・ドライブと光ディスク装置の制御権移動』を参照してください。
 4. システムに論理区画がある場合は、磁気テープ・ドライブを統合サーバーと同じ区画に割り振ってあることを確認してください。
 5. ドライブに、適切にフォーマットされた磁気テープが入っていることを確認します。 191 ページの『i5/OS での統合 Windows サーバー用のテープのフォーマット』を参照してください。
 6. NWSD コマンドの表示 (DSPNWSD) コマンドを使用することによって、i5/OS 上で制限されている装置のリストに、このドライブが含まれていないことを確認します。
 7. 磁気テープ・エラーのイベント・ログを調べます。
 8. 磁気テープ装置が装置リストに表示されていることを確かめます。
 - a. 「スタート」、「プログラム」、「管理ツール」、「コンピュータの管理」の順にクリックします。
 - b. 「システム ツール」、「デバイス マネージャ」の順に選択します。
 - c. この磁気テープ・ドライブが装置リストに表示されていることを確認します。
 9. 問題が続く場合には、 IBM iSeries サポート Web ページ (英語)  の技術情報データベースをチェックしてください。それでも解決しない場合には、テクニカル・サポート・プロバイダーに連絡してください。

磁気テープ・ドライブの装置ドライバーがロードされていることの確認

- 1 統合サーバーで実行されるアプリケーションが iSeries 磁気テープ・ドライブを使用できるようにする前
- 1 に、装置ドライバーを統合サーバーにロードしなければなりません。通常、この作業は自動的に実行されま
- 1 す。サポートされる磁気テープ・ドライブについての詳細は、193 ページの『サポートされている iSeries
- 1 磁気テープ・ドライブ』を参照してください。

磁気テープ装置のドライバーがロードされていることを確認するには、以下のステップに従います。

1. Windows サーバーのタスクバーで、「スタート」、「プログラム」、「管理ツール」の順にクリックします。
2. 「コンピュータの管理」、「システム ツール」、「デバイス マネージャ」の順にクリックします。
3. 使用しているマシンの名前が付いたアイコンを展開します。磁気テープ装置がロードされている場合、「テープ デバイス」アイコンが表示されます。
4. 「テープ デバイス」アイコンを展開し、ロードされている磁気テープ・デバイス・ドライバーを確認します。

サード・パーティーのドライバーを必要としない IBM iSeries 磁気テープ・ドライブを持っており、デバイス・ドライバーを手動でロードする必要がある場合、統合サーバー・コンソールで以下のステップを行ってください。

1. 「スタート」、「設定」、「コントロール パネル」の順にクリックします。
2. 「ハードウェアの追加と削除」をクリックします。
3. 「ハードウェアの追加と削除ウィザード」で、「次へ」をクリックします。
4. 「デバイスの追加/トラブルシューティング」を選択し、「次へ」をクリックします。
5. 「ハードウェアの追加と削除ウィザード」ウィンドウの「ハードウェア デバイスの選択」セクションで、「新しいデバイスの追加」を選択し、「次へ」をクリックします。
6. 「ハードウェアの追加と削除ウィザード」ウィンドウの「新しいハードウェアの検出」セクションで、「いいえ、一覧からハードウェアを選択します」を選択し、「次へ」をクリックします。
7. 「ハードウェアの種類」セクションで、コンボ・ボックスを「テープ ドライブ」までスクロールダウンして選択し、「次へ」をクリックします。
8. 「デバイス ドライバの選択」セクションの「製造元」ペインで、「IBM」を選択します。「モデル」ペインで、「IBM iSeries テープ装置」を選択し、「次へ」をクリックします。
9. このウィンドウの「IBM iSeries テープ装置」セクションで、「次へ」をクリックします。
10. 「ファイルが必要」ボックスが表示される場合、「コピー元」ボックスに、`%SystemRoot%\%System32%\drivers` と入力します。C はそれぞれのシステム・ドライブです。「OK」をクリックします。
11. 「ハードウェアの追加と削除」ウィザード・ウィンドウの「ハードウェアの追加と削除ウィザードの完了」セクションで、「完了」をクリックします。磁気テープ装置がすべてロードされます。
12. コンピューターを再始動したら、ステップ 1 から 4 までを繰り返し、装置がロードされたことを確認します。

その他の磁気テープ装置ドライバーのロードについての詳細は、191 ページの『磁気テープ装置のドライバーのインストール』を参照してください。

統合 Windows サーバーの始動に関する問題

統合サーバーが始動しない場合、以下のステップを行って、問題を判別してください。

1. サーバーの状況をチェックします。NWSD の現在の状況が「VARIED OFF」(オフに構成変更) されていることを確認します。そうでない場合は、NWSD をオフに変更してから、もう一度サーバーを始動してみます。163 ページの『統合サーバーの開始と停止』を参照してください。統合サーバーが起動しなくても、サーバーの状況が「VARY ON 保留中」であれば、デバイス・ドライバーに問題がある可能性があります。
2. NWSD のオンへの構成変更を実行したジョブ・ログを調べ、エラー・メッセージと取りうる訂正アクションを探します。

3. QSYSOPR メッセージ待ち行列を調べて、障害メッセージおよび可能な修正処置を探します。
 4. 問題の原因となる可能性のあるサーバー構成ファイルを作成した場合は、そのサーバー構成ファイルを修正するか、リセットしてください。 242 ページの『NWSD 構成ファイルのエラー』を参照してください。
 5. 統合サーバーの再始動が開始したなら、以下のステップを実行してください。
 - a. i5/OS 上で、WRKACTJOB SBS(QSYSWRK) コマンドを入力します。
 - b. Enter キーを押します。
 - c. ジョブ QVNAVARY を探し出します。
 - d. オプション 5 を選択してジョブを処理します。
 - e. ジョブがアクティブであるかジョブ待ち行列にある場合、オプション 10 を選択してそのジョブ・ログを表示します。障害メッセージおよび可能な修正処置を探します。
 - f. ジョブを終了したら、WRKSPLF SELECT(*CURRENT *ALL *ALL QVNAVARY) と入力して、スプール・ファイルを表示します。
 6. コマンド WRKPRB を入力して、ログ記録された問題を表示します。
- | IXS または IXA 接続の xSeries サーバーの場合、サーバーの「リポート」に必要なオフおよびオンへの変更を実行するために、BTnwsdname という名前を使用したバッチ・ジョブがサブミットされます。
- | QVNAVARY ジョブ・ログでサブミットされたジョブの修飾名を識別します。 WRKSPLF SELECT(*ALL)
- | JOB(qualjobname) を使用してジョブ名を完全に修飾することにより、サブミットされた「リポート」ジョブがないか、ジョブ・ログを探します。
- | WRKSPLF SELECT(*ALL) JOB(BTnwsdname) ですべての「リポート」ジョブをリストします。

緊急修理

障害のあるシステム・ドライブが原因で問題が続く場合で、そのドライブの正常なバックアップがある場合は、この緊急修理を試してください。破損したデータを回復してシステムを機能状態に戻すには、次のステップを行います。

注: これらの例では、NWSD 名 *ERS* および *ERS1* という名前のシステム・ドライブが使用されます。

1. 次のコマンドを使用して、障害のあるシステム・ドライブ (通常は C ドライブ) をリンク解除します。 RMVWNSSTGL NWSSTG(*ERS1*) NWSD(*ERS*)
2. 次のコマンドを使用して、障害のあるシステム・ドライブを新しい名前にコピーします。 CRTNWSSTG NWSSTG(*ERSBKP*) FROMNWSSTG(*ERS1*)
3. システム・ドライブの最新のバックアップを復元します。
4. 次のコマンドを使用して、復元されたシステム・ドライブをリンクします。 ADDNWSSTGL NWSSTG(*ERS1*) NWSD(*ERS*)
5. 次のコマンドを使用して、ステップ 1 の障害のあるシステム・ドライブをリンクします。 ADDNWSSTGL NWSSTG(*ERS1BKP*) NWSD(*ERS*)
6. 次のコマンドを使用して、NWSD をオンに変更します。 VRYCFG CFGOBJ(*ERS*) CFGTYPE(*NWS) STATUS(*ON)
7. 最新のバックアップから変更された、障害のあるシステム・ドライブから、データ・ファイルなどの主要ファイルをすべてコピーします。
8. 最新のバックアップから追加または更新されたすべてのアプリケーションをインストールします。

9. 次のコマンドを使用して、NWSD をオフに変更します。 VRYCFG CFGOBJ(ERS1) CFGTYPE(*NWS) STATUS(*OFF)
10. 次のコマンドを使用して、ステップ 5 の障害のあるシステム・ドライブをリンク解除します。 RMVNWSTGL NWSSTG(ERS1BKP) ERS(ERS1)
11. 障害のあるシステム・ドライブからすべてのデータを確実に除去するまで、ドライブを再リンクして (ステップ 5)、復元先ドライブに追加のファイルをコピーすることができます。障害のあるシステム・ドライブからすべてのデータを確実に除去できたら、すべての記憶域の新しいバックアップを作成します。記憶域をバックアップするステップについては、211 ページの『統合 Windows サーバー用事前定義ディスク・ドライブのバックアップ』を参照してください。その後、次のコマンドを使用して、障害のあるシステム・ドライブを削除します。 DLTNWSSTG NWSSTG(ERS1BKP)

サーバー間のホット・スペアリングに関する問題

統合サーバー間でホット・スペアリングが失敗する主な理由は、ハードウェアの互換性です。Windows Server 2003 のアクティベーションによって問題が生じる場合もあります。詳細については、以下を参照してください。

ホット・スペア・ハードウェアの互換性

1 つの統合サーバー・ハードウェアのセットから別のセットへの Windows サーバーの切り替えは、1 つの PC から 2 番目の PC への Windows システム・ドライブの移行に類似しています。必要なハードウェア分離層 (HAL)、基本入出力システム (BIOS) レベル、または 2 つの PC に取り付けられている装置の違いが、移行の際の問題の原因となる場合があります。2 番目の PC 上の Windows の初期ブートの際にハードウェアの相違が検出され、以下の方法のうちのいずれかによって処理されます。

- 一部のハードウェアの相違はプラグ・アンド・プレイによる自動処理が可能です。
- 一部のハードウェアの相違は手操作による介入を必要とする場合があります。たとえば、新しいデバイス・ドライバーをインストールしなければならないかもしれません。
- ハードウェアの相違が非常に大きい場合、2 番目の PC はブートできない可能性があります。たとえば、2 つの PC に必要な HAL のバージョンに互換性がない場合があります。

これらの同じハードウェアの互換性に関する考慮事項は、IXS サーバー同士、IXA 接続の xSeries サーバー同士、および iSCSI 接続の IBM xSeries または BladeCenter サーバー同士のホット・スペアリングに当てはまります。ホット・スペアの移行を正常に機能させるには、2 つのサーバーのハードウェア構成の一致度が高くなければなりません。

統合 xSeries サーバー (IXS) ホット・スペア

IXS サーバー間でホット・スペアを使用するには、それらが互換タイプであり、LAN アダプターの構成などに互換性がある必要があります。Web ページ http://www.ibm.com/eserver/iserries/integratedxseries/ixs_system_config.html にある統合 xSeries サーバーの構成表には、サポートされる特定の IXS ホット・スペア構成が示されています。

xSeries または IBM BladeCenter サーバー・ホット・スペア

IXA 接続の xSeries サーバー間、または iSCSI 接続の xSeries または IBM BladeCenter サーバー間でホット・スペアを使用する場合は、同じタイプの xSeries または IBM BladeCenter プレード・サーバーを使用することを強くお勧めします。たとえば、xSeries モデル 236 を別の xSeries モデル 236 のホット・スペアとすることができます。加えて、xSeries サーバー同士は PCI アダプター構成などが類似していなければなりません。

注: タイプの異なる 2 つの xSeries またはブレード・サーバー・モデル間でホット・スペアを使用することも可能です。しかし、xSeries またはブレードのモデル同士のハードウェアの相違が大きい場合もしばしばあります。そのため、この場合、ホット・スペア用に使用を計画している xSeries またはブレード・サーバーのモデルの特定の組み合わせをテストする必要があります。それらを実稼働環境のホット・スペア・サーバー・バックアップで使用する前に、xSeries またはブレード・サーバー・モデルのハードウェア構成に互換性があるかどうか、また相互のシームレスな移行が可能かどうかを確認する必要があります。

Windows Server 2003 のアクティベーション

Windows Server 2003 サーバーの記憶域スペースが別のホット・スペア統合サーバーに切り替わるたびに、Windows のアクティベーションがトリガーされます。各ライセンス・キーに対する無料のアクティベーションの回数は限られています。アクティベーションが何度もトリガーされる場合、再度アクティベーションをするために Microsoft に電話をかける必要が生じるかもしれません。これによりサーバーの再アクティベーションの速度が制限される恐れがあります。Windows Server 2003 のボリューム・ライセンスはアクティベーションが不要なため、この場合に役立つかもしれません。

ホストされるシステム・ハードウェアの共用に関する問題

ホストされるシステム・ハードウェアの共用に関する問題について詳しくは、以下のリンクを参照してください。

- 『ホストされる同じシステム・ハードウェアを使用するよう定義された複数の NWSD』
- 『iSCSI 接続のシステムに関する特別な考慮事項』

ホストされる同じシステム・ハードウェアを使用するよう定義された複数の NWSD

特定の統合 xSeries サーバー (IXS)、xSeries システム、または IBM BladeCenter ブレードのハードウェアを制御するために、複数のネットワーク・サーバー記述 (NWSD) を定義することが可能です。iSCSI 接続のサーバー以外の場合、これらの NWSD は同じ iSeries 区画になければなりません。しかし、iSCSI 接続のサーバーの場合は、NWSD を同じ iSeries 区画に定義することも、同じ iSeries システムの別の区画に定義することも、あるいはまったく別の iSeries システムに定義することもできます。たとえば、通常の営業時間中の実動作業では xSeries システムを使用するように特定の NWSD を定義し、その他の時間は同じ xSeries システムを使用するように別の NWSD を定義することもできます。

サーバー・ハードウェアの特定の部分を使用できる NWSD はいつでも 1 つのみです。したがって、同じハードウェア上で実行されるように複数の NWSD が定義されており、現在そのうちの 1 つがそのハードウェアを使用している場合、それ以外の NWSD は、現在ハードウェアを使用中の NWSD がシャットダウンされるまで (オフになるまで) 開始することができません。これにより、ある NWSD が使用しているハードウェアを不用意に別の NWSD が引き継ぐことがないよう保護されます。

NWSD の開始に問題が生じ、サーバー・ハードウェアが現在別の NWSD によって使用されている場合、ある NWSD から別の NWSD へ制御権移動する正しい方法は、現在ハードウェアを使用している NWSD をまずシャットダウンしてから、次にハードウェアを使用する必要がある NWSD を開始することです。

iSCSI 接続のシステムに関する特別な考慮事項

iSCSI 接続のサーバーの場合、ハードウェアへのアクセスを制御し、いつでも 1 つの NWSD だけがハードウェアが使用するようになるために、サーバー・ハードウェアの状態が使用されます。NWSD を開始したとき (オンに変更したとき) の iSCSI 接続のサーバーの特定の動作は、サーバーが持つサービス・プロセッサのタイプに応じて異なります。

- | • BMC サービス・プロセッサを持つ xSeries サーバーの場合、最初ハードウェアを電源オフの状態にしておかなければなりません。
- | • RSA II を持つ xSeries サーバー、または管理モジュールを持つ IBM BladeCenter の場合、ハードウェアをオペレーティング・システム (たとえば DOS または Windows) にブートしてはなりません。
- | xSeries システムがディスク挿入プロンプトの状態に留まることは許可されていますが、システムは一定時間に渡って待機し、他のシステムがこのシステムを使用しようとしていないか確認します。
- | それ以外の場合、開始操作は失敗します。NWSD をシャットダウンするとき (オフに変更するとき) に、NWSD の xSeries または BladeCenter ブレード・ハードウェアは電源オフの状態のままにされます。
- | サーバー・ハードウェアが電源オン状態であることの理由として考えられるのは、現在このサーバー・ハードウェアを使用している NWSD があるというケース以外に、ほかにもあります。たとえば、ファームウェアのロードや BIOS 設定の変更など、ハードウェアのセットアップを実行するためにサーバー・ハードウェアの電源がオンにされたかもしれません。別の例としては、サーバー・オペレーティング・システムに回復不能エラーが生じてサーバー障害になったものの、ハードウェアは電源オン状態のままという場合があります。このような場合に通常の方法で NWSD を開始すると、サーバー・ハードウェアが電源オフの状態になっていないため、あるいはオペレーティング・システムがまだ実行中であることをサービス・プロセッサが示すために、失敗する場合があります。
- | この状況から回復するための方法がいくつかあります。
- | • NWSD が現在ハードウェアを使用しており、サーバー・オペレーティング・システムが失敗した場合、サーバーのシャットダウンを試みてください。ほとんどの場合、これによってサーバー・ハードウェアの電源がオフになり、同じ、または別の NWSD で使用可能になります。NWSD をシャットダウンしても問題が解決されない場合は、以下で説明する方法を試してみてください。
- | • NWSD を開始するときにはシステムのリセット・オプションがあります。これは NWSD の開始中にサーバー・ハードウェアを強制的にリセットするものです。通常ならサーバーの開始 (オンに変更) が失敗してしまうはずの状態にあるサーバー・ハードウェアでも、このオプションを使用することによって、このサーバー・ハードウェアを使用する NWSD を開始することができます。
- | **重要:** システムのリセット・オプションは、サーバー・ハードウェアが現在他の NWSD によって使用されていないことが確実な場合にのみ使用してください。別の NWSD がハードウェア上で実行されている状態でシステムのリセット・オプションを使用して NWSD を開始すると、その別の NWSD は失敗し、データ損失またはデータ破損を招く可能性があります。
- | iSeries ナビゲーターを使用してリモート・システムをリセットするには、以下のステップに従ってください。
- | 1. 「統合サーバー管理」を展開します。
- | 2. 「サーバー」を展開します。
- | 3. 表示されたリストからサーバーを右クリックします。
- | 4. 「オプションで始動...」を選択します。
- | 5. 「リモート・システムのリセット」オプションをチェックします。
- | 6. 「開始」をクリックします。確認パネルが表示されます。
- | 7. 確認パネルで「開始」をクリックし、リモート・システムをリセットします。
- | CL コマンドを使用する場合は、構成の変更 (VRYCFG) コマンドのシステムのリセット (RESETSYS) キーワードを参照してください。

NWSD 構成ファイルのエラー

独自に作成した NWSD 構成ファイルがエラーの原因と思われる場合は、NWSD 構成ファイル・パラメーターを *NONE にリセットしてみてください。『NWSD 構成ファイル・パラメーターのリセット』を参照してください。これでエラーがなくなったら、NWSD 構成ファイルに問題がある可能性が高いと判断されます。

NWSD 構成ファイルが原因でエラーが発生している場合は、以下の方法を実行することができます。

- 独自の NWSD 構成ファイルを使用しないで作業を続行する。
- 『以前のバージョンの統合サーバー・ファイルの使用』
- 『NWSD 構成ファイルの修正』

NWSD 構成ファイルの修正

NWSD 構成ファイルを修正してエラーを除去する場合、以下のオプションを考慮してください。

1. ログをチェックして、エラーと回復の情報を探します。 230 ページの『メッセージ・ログとジョブ・ログのチェック』を参照してください。
2. NWSD 構成ファイルを編集します。
3. 再始動します。 163 ページの『統合サーバーの開始と停止』を参照してください。

NWSD 構成ファイル・パラメーターのリセット

NWSD の構成ファイル・パラメーターを *NONE に設定すると、統合サーバー・ファイルに、エラーの原因となる変更が加えられないようにすることができます。i5/OS が問題の NWSD 構成ファイルを使用しないようにするには、以下のようになります。

1. i5/OS コマンド行に WRKNWSD (ネットワーク・サーバー記述 (NWSD) の処理) を入力します。
2. 問題のネットワーク・サーバーの横にある行で、オプション 2 (変更) を選びます。
3. 「構成ファイル」フィールドで、*NONE を選択します。
4. ネットワーク・サーバーをオンに変更し、エラーがなくなるかどうかを見ます。

注: 構成ファイルによって処理されるいずれかのファイルに対してなされた既存の変更は、そのまま変わりません。サーバーがオンに変更されることによって実行される最後の変更の前のファイルの内容が .BKU ファイルとして保管されています。このファイルを使って、変更後のバージョンを元の内容に置換できます。または、以前のバックアップ・ファイルが存在する場合には、それを復元することもできます。

以前のバージョンの統合サーバー・ファイルの使用

機能するバージョンの統合サーバー・ファイルが存在する場合は、ファイルを変更して、この機能するバージョンに戻せます。変更するには、次のステップを行います。

1. エラーの原因となる変更が統合サーバー・ファイルに加えられないようにするために、NWSD の構成ファイル・パラメーターを *NONE に再設定します。『NWSD 構成ファイル・パラメーターのリセット』を参照してください。
2. 以前のバージョンにリセットするファイルを選びます。
3. サーバーが機能中でオンに変更されている場合は、サーバーにログオンするか、i5/OS コンソールからリモート・コマンドを実行して (168 ページの『統合 Windows サーバーのコマンドのリモート実行』を参照)、以下のようにファイル名を変更します。
 - 問題の原因となっているファイル名を別の名前に変更します。
 - 以前のバージョンのファイルを元の名前に変更します。

4. 以前のバージョンのファイルを使用するために、統合サーバーをオフに変更して、オンに戻します。

IXA または iSCSI 接続のサーバーの DASD

ローカル・ハード・ディスク・ドライブは、統合 xSeries アダプターを使って iSeries に直接接続されると、xSeries サーバーではサポートされません。ローカル・ハード・ディスク・ドライブは、iSCSI HBA を使って iSeries に接続されると、IBM xSeries または BladeCenter サーバーでサポートされません。たいの場合、そのようなローカル・ハード・ディスク・ドライブは表示されません。もしそのようなドライブが表示された場合にそれを使用すると、想定外の結果が起きる可能性があります。直接接続モードの xSeries または IBM BladeCenter サーバーを使って、IXA または iSCSI HBA 経由で iSeries に接続するときは、どのローカル・ハード・ディスク・ドライブも取り外されていることを確かめてください。

ユーザーおよびグループの登録時の障害

グループまたはユーザーを iSeries の Windows 環境に登録できない場合、以下の手順を実行して問題を判別してください。

i5/OS から:

- このネットワーク・サーバー記述 (NWS D) (サーバーのインストール中に QSYSOPR、ユーザー定義のメッセージ・ログ、またはユーザー・ジョブ・ログになるよう指定されている) のメッセージ・ログにエラーがないかチェックします。エラー・メッセージの回復処置に従って、問題を修正します。さらに、「NWS ユーザー登録の処理 (WRKNWSENR)」画面でエラー・コードを見つけることもできます。
- メッセージ・ログに User Admin error NTA0282 が含まれる場合には、244 ページの『ユーザー登録権限の問題』を参照してください。
- サーバーの状況がオンに構成変更 (VARIED ON) であることを確認します。
- 登録状況をチェックして (197 ページの『iSeries ナビゲーターによる Windows 環境への単一 i5/OS ユーザーの登録』を参照)、エラー・メッセージがあるかどうかを調べます。F5 を押して状況を最新表示します。
- i5/OS がパスワードを保持するように設定されている (QRETSVRSEC が 1 に設定されている) ことを確かめます。さらに、登録を試行するユーザーが、この値の設定後に i5/OS へのサインオンを試行していることを確かめてください。
- NWS D のメッセージ待ち行列を指定して作成します。その待ち行列にメッセージがないかどうかをチェックします。
- i5/OS で、WRKACTJOB コマンドを入力します。QSYSWRK サブシステムで QPRFSYNCH ジョブをチェックします。詳細なメッセージについては、F10 を押してジョブ・ログをチェックしてください。
- i5/OS 上で、WRKJOB *nwsdname* コマンドを入力します (*nwsdname* は統合サーバーの NWS D の名前)。そのジョブがアクティブである場合、ジョブ・ログを表示します (メッセージの詳細は F10 を押す)。ジョブを終了する場合、スプール・ファイルを表示してください。

統合 Windows サーバーから:

さらに、以下のステップを試行して、問題を判別することもできます。

- ユーザー管理サービスが稼働していることを確認します。
 - 統合サーバーの「スタート」メニューから、「プログラム」、「管理ツール」、「コンポーネントサービス」の順に選択します。
 - 「システム ツール」、「サービス」の順に選択します。
 - サービスのリストに「iSeries ユーザー管理」が含まれていることを確認します。

4. 「iSeries ユーザー管理」サービスがリストされていても、このサービスの状況が開始済みでない場合には、「iSeries ユーザー管理」を右マウス・ボタン・クリックして、メニューから「開始」を選択します。
5. 「iSeries ユーザー管理」がリストされない場合は、以下を行ってこれを再インストールしてください。
 - a. 「スタート」から、「ファイル名を指定して実行」を選択し、`command` と入力してコマンド・プロンプト・ウィンドウをオープンします。
 - b. C: ドライブ (または現行の Windows ドライブ) に移動します。
 - c. `%SystemRoot%\as400wsv\admin\qvnadaem /install` と入力し、Enter を押します。
 - d. 「サービス」ウィンドウをクローズします。
 - e. もう一度「サービス」をオープンします。
 - f. 「iSeries ユーザー管理」をまだ開始していない場合は、「開始」をクリックします。

Windows ドメイン制御装置が見つからないことを示すエラー・メッセージが表示される場合、ユーザーを Windows ワークグループに登録しようとしている可能性があります。Windows ネットワーキングでは、ローカル・サーバーのグループを、Windows ワークグループを使用することで自由に加入させられます。例えば、「マイ ネットワーク」を開いて「近くのコンピュータ」をクリックすると、同じワークグループにあるコンピューターのリストが表示されます。iSeries ナビゲーターでは、i5/OS ユーザーをそれらのワークグループに登録できますが、そうしようとするとエラーになってしまう場合もあります。Windows ドメインに存在しているような、Windows ワークグループ・ユーザーの個別のリストはありません。

ユーザー登録権限の問題

統合サーバー・ユーザーの作成および更新を行う十分な権限がないことを示すエラー (NTA0282) が出たら、以下のアクションを行ってください。

- 初めてユーザーおよびグループをドメインに登録しようとしている場合には、QAS400NT ユーザー ID に必要な権限が提供されるように設定します。204 ページの『QAS400NT ユーザー』のトピックに、その方法が説明されています。さらに、ユーザーが従来のユーザーとして構成されていることも確認してください。これはつまり、ユーザーは iSeries パスワードを指定しなければならず、ローカル・パスワード管理が可能でなければならないということです。56 ページの『ユーザー構成の種類』を参照してください。
- ユーザーおよびグループを正常に登録してから時間が経過している場合には、QAS400NT ユーザーの i5/OS パスワードの有効期限が切れていないかどうかをチェックします。QAS400NT ユーザー・パスワードの有効期限が切れると、統合サーバーのアカウントも期限切れになります。この状況を修正するには、以下のことを行ってください。
 1. 統合サーバー・アカウントを使用可能にします。

ドメイン制御装置では:

- a. 「スタート」→「プログラム」→「管理ツール」をオープンします。
- b. 「Active Directory ユーザーとコンピュータ」を選択します。
- c. 「ユーザー」を右マウス・ボタン・クリックして、「QAS400NT」をダブルクリックします。
- d. 「ユーザーのプロパティ」画面の上部の「アカウント」タブをクリックします。
- e. 「アカウントの期限」の日付を将来の日付に変更し、「無期限」をクリックします。

ローカル統合 Windows サーバーでは:



- a. 「スタート」、「プログラム」、「管理ツール」をオープンします。

- b. 「コンピュータの管理」を選択します。
 - c. 「システム ツール」を展開してから、「ローカル ユーザーとグループ」を展開します。
 - d. リストから「QAS400NT」を右マウス・ボタン・クリックします。
 - e. 「ユーザーのプロパティ」画面の上部の「アカウント」タブをクリックします。
 - f. 「アカウントの期限」の日付を将来の日付に変更し、「無期限」をクリックします。
2. i5/OS 上で、ユーザー・プロファイルの変更 (CHGUSRPRF) またはパスワードの変更 (CHGPWD) コマンドを使用して、QAS400NT ユーザー・パスワードを変更します。
 3. iSeries ユーザー管理サービスを再始動します。
 - a. 「スタート」、「プログラム」、「管理ツール」、「コンポーネント サービス」の順にクリックします。
 - b. 「サービス」をクリックします。
 - c. 「iSeries ユーザー管理」をクリックし、「停止」を右クリックしてサービスを停止します。
 - d. 「iSeries ユーザー管理」をクリックし、「開始」を右クリックしてサービスを再始動します。

サービスを再始動すると、ユーザーおよびグループの登録は自動的に再試行されます。


この問題が起きないようにするには、ご使用の i5/OS システムで QAS400NT パスワードを定期的に変更して、パスワードの有効期限が切れないようにします。

Windows ドメインに加入する複数の統合サーバーで複数の iSeries を使用している場合は、204 ページの『QAS400NT ユーザー』で説明されているステップを実行することで、パスワード満了の問題を最小限にとどめることができます。

- 問題が続く場合には、IBM  server iSeries Support Web ページ  の技術情報データベースをチェックしてください。それでも解決しない場合には、テクニカル・サポート・プロバイダーに連絡してください。

パスワードの問題

これまでは i5/OS パスワードに使える文字はすべて、Windows パスワードでも使用しても差し支えありませんでした。現在 i5/OS では、Windows でサポートされる以上の長さのパスワードと、Windows でサポートされるより多くの数の文字の文字をできるようになりました。ユーザー登録を行いたい場合、Windows パスワードで使用できる数の文字とパスワード長だけを使った i5/OS パスワードを使用する必要があります。



i5/OS パスワード・レベルのセキュリティに関する詳しい解説は、「iSeries 機密保護解説書」 の『パスワード・レベルの変更計画』にあります。

統合サーバーのコンソールから変更された後でパスワードの有効期限が毎日切れる場合は、ユーザーは i5/OS からパスワードを変更するのを忘れていました。i5/OS パスワードを変更すれば、問題はなくなります。

i5/OS パスワードと Windows サーバー・パスワードが一致しない場合、以下の作業を行って、その理由を判別してください。

1. ユーザーが Windows ユーザーとして構成されていることを確認します。56 ページの『ユーザー構成の種類』を参照してください。
 - a. i5/OS コマンド行に、WRKUSRPRF と入力します。
 - b. 正しいユーザー ID を入力します。

- c. 属性 LCLPDMGT (ローカル・パスワード管理) が *NO に設定されていることを確認します。そのように設定されていれば、ユーザーは、*NONE の i5/OS パスワードを持つよう構成されていて、i5/OS および Windows パスワードは同じものではありません。
2. 次のようにして、i5/OS がパスワードを保管するよう設定されていることをチェックします。
 - a. i5/OS コマンド行に、WRKSYSVAL SYSVAL(QRETSVRSEC) と入力します。
 - b. 「Option」フィールドに 2 と入力して、Enter キーを押します。
 - c. 「サーバー機密保護データの保存」に 1 が設定されていることを確認します。1 に設定されていない場合は、1 に変更してください。
3. 統合 Windows サーバー上で、ユーザー管理サービス (User Administration Service) が稼働していることを確認します。関連情報は、243 ページの『ユーザーおよびグループの登録時の障害』を参照してください。
4. 次のようにして、i5/OS パスワードのサポート・レベルをチェックして確かめます。
 - a. i5/OS コマンド行に WRKSYSVAL SYSVAL(QPWDLVL) と入力します。
 - b. オプション・フィールドに 5 を入力してから Enter キーを押します。

1 文字以上 10 文字以下のユーザー・プロファイル・パスワード、または 1 文字以上 128 文字以下のユーザー・プロファイル・パスワードを使えるよう、i5/OS のパスワード・レベルを設定できます。0 または 1 の i5/OS パスワード・レベルでは、1 文字以上 10 文字以下のパスワードがサポートされ、文字セットが制限されます。レベル 0 または 1 では、i5/OS のパスワードは Windows サーバー用にすべて小文字に変換されます。i5/OS パスワードのレベル 2 または 3 では、1 文字以上 128 文字以下のパスワードがサポートされ、大文字小文字を含め、使用できる文字が増えます。レベル 2 または 3 では、Windows サーバー用にパスワードでの大/小文字の区別が順守されます。i5/OS パスワード・レベルに加えた変更は、IPL の実行後に有効化されます。
5. ユーザーの登録状況をチェックします。ユーザーを登録する前に、そのユーザーが違うパスワードで Windows 環境にすでに登録されていないことを確認します (197 ページの『iSeries ナビゲーターによる Windows 環境への単一 i5/OS ユーザーの登録』を参照)。ユーザーが違うパスワードで登録されていれば、この登録は失敗します。Windows パスワードを i5/OS パスワードと一致するよう変更してから、もう一度登録手順を実行してください。
6. 問題が続く場合には、 IBM iSeries サポート Web ページ (英語)  の技術情報データベースをチェックしてください。それでも解決しない場合には、テクニカル・サポート・プロバイダーに連絡してください。

IBM iSeries 統合サーバー・サポート・スナップイン・プログラム

IBM iSeries 統合サーバー・サポート・スナップイン・プログラムを実行しようすると、エラーになることがあります。プログラムが起動しなかったり、予期しない情報が示されたり、あるいは使用時にエラーが発生する可能性があります。

IBM iSeries 統合サーバー・サポート・スナップイン・プログラム画面が表示されない場合には、以下のステップを実行すると問題判別に役立ちます。



- システム上にすでに IBM iSeries 統合サーバー・サポート・スナップインまたは Lvlsync プログラムのインスタンスがあることを確認します。プログラムのインスタンスは 1 度に 1 つだけ実行できます。いずれかのプログラムのインスタンスがすでに稼働している場合、そのプログラムに対する新しい呼び出しが戻されます。新しいインスタンスを開始する前に、現在のプログラムを完了してください。

- ユーザーが管理者レベルのアクセス権限および特殊権限を持っていることを確認します。 IBM iSeries 統合サーバー・サポート・スナップイン・プログラムは、これらの権限を必要とします。管理者権限を使用して、プログラムの起動を再試行してください。
- iSeries NetServer を起動してあることを確認してください。 iSeries NetServer は、i5/OS 上の QSERVER サブシステムと一緒に自動的に始動します。 i5/OS でまだ iSeries NetServer を始動していないければ、これを始動してください。
- iSeries NetServer 上でゲスト・ユーザー・プロファイルを使用可能にしたことを確認します。 使用可能になっていなければ、ゲスト・ユーザー・プロファイルを使用可能にして、ゲストが iSeries NetServer にアクセスできるようにします (68 ページの『iSeries NetServer 用のゲスト・ユーザー・プロファイルの作成』を参照)。ゲスト・アクセスを使用可能である場合、iSeries NetServer を停止してから再起動し、 IBM iSeries 統合サーバー・サポート・スナップイン・プログラムを再試行してください。
- IBM iSeries 統合サーバー・サポート・スナップイン・プログラムに関するメッセージがないかどうか、Windows サーバーのシステム・イベント・ログをチェックします。

IBM iSeries 統合サーバー・サポート・スナップイン画面が表示されますが、i5/OS には予期しない情報が表示される場合があります。そのような場合、以下のステップで問題を判別してください。

- 最新のサービス・パック PTF が使用可能であり、i5/OS 上でアクティブ状態になっていることを確認します。 PTF の表示 (DSPPTF) コマンドを使用して、これを行えます。
- すでにインストールしたと思われるサービス・パックが、実際に統合サーバー上にインストールされていることを確認します。
- 統合サーバー・サポート・スナップイン・プログラムに関するメッセージがないかどうか、統合サーバーのシステムおよびアプリケーションのイベント・ログをチェックします。

IBM iSeries 統合サーバー・サポート・スナップイン・プログラムを使用してアクションを実行すると、問題が発生することがあります。以下のリストは、「OK」ボタンをクリックした後に生じた問題を解決するときに役立ちます。

- IBM iSeries 統合サーバー・サポート・スナップイン・プログラムを続けるため、特定のドライブ名が使用できなければなりません。このドライブ名は、一時的に使用可能にする必要があります。すべてのドライブ名が使用中の場合、 IBM iSeries 統合サーバー・サポート・スナップインのためにドライブ名を 1 つ解放してから、プログラムを再試行してください。
- IBM iSeries 統合サーバー・サポート・スナップイン・プログラムは、指定されたアクションを行います。システムは、更新された一群のファイルに応じて再始動されることもありますしされないこともあります。システムをシャットダウンし起動するときには、時間が少しかかることがあります。
- IBM iSeries 統合サーバー・サポート・スナップイン・プログラムに関するメッセージがないかどうか、統合サーバーのシステムおよびアプリケーションのイベント・ログをチェックします。
- 問題が続く場合には、  IBM iSeries サポート Web ページ (英語)  の技術情報データベースをチェックしてください。それでも解決しない場合には、テクニカル・サポート・プロバイダーに連絡してください。

1 iSCSI 接続のサーバーの問題

1 以下にリストする問題のいずれかが起こった場合、リストされているアクションを実行することにより、ト
1 ラブルシューティングを開始できます。これは包括的なリストではないので、問題によっては、ここでリス
1 トされている以外のアクションが必要になる場合もあるかもしれません。問題のトラブルシューティングに
1 役立つ情報については、230 ページの『メッセージ・ログとジョブ・ログのチェック』を参照してくださ
1 い。

サービス・プロセッサ構成の初期化に失敗する

システム・オペレーターのメッセージ待ち行列 (QSYSOPR) にメッセージ CPDC4xx または CPFC4xx がある場合、またはバッチ・ジョブか対話式ユーザーのジョブ・ログが関係している場合は、250 ページの『IBM Director のトラブルシューティング』を参照してください。

サーバーのインストール時または開始時に NWSD 状況が VARIED OFF から変わらない

サーバーをインストールまたは開始する前に、サーバーで構成されている必要なネットワーク・サーバー・ホスト・アダプターがすべてオンに変更されているか確認してください。ネットワーク・サーバー・ホスト・アダプターがオンに変更されない場合、ネットワーク・サーバー・ホスト装置のメッセージ待ち行列の中にメッセージがないか調べてください。

システム・オペレーターのメッセージ待ち行列 (QSYSOPR) にメッセージ CPDC4xx または CPFC4xx がある場合、またはバッチ・ジョブか対話式ユーザーのジョブ・ログが関係している場合は、250 ページの『IBM Director のトラブルシューティング』を参照してください。

ホストされるシステムの電源がオンになっているとサーバーが始動しない

240 ページの『ホストされるシステム・ハードウェアの共用に関する問題』を参照してください。

ホストされるシステムのコンソールに「iSCSI 装置が見つかりません」が表示される、またはディスクレットの挿入を求めるプロンプトが出る

ホストされるシステムでブート用に構成された iSCSI HBA で、これを行うことができませんでした。

iSCSI の構成に問題がある可能性があります。iSCSI トラブルシューティング (英語)  (www.ibm.com/servers/eserver/iseries/integratedxseries/iscsireadme/troubleshooting.html) を参照してください。

メッセージ CPPC056 がプロダクト・アクティビティ・ログにある場合、CHAP 構成に問題がある可能性があります。

ブート用に構成された、ホストされるシステムの iSCSI HBA と、NWSD のシステム・ドライブ記憶域スペース用に構成されたパスに対応する iSeries HBA との間に、ネットワーク問題がある可能性があります。249 ページの『ブートおよび記憶域パス・ネットワークの分析』を参照してください。

NWSD の状況が VARIED ON なのに Windows がブートを開始しない

iSCSI の構成に問題がある可能性があります。iSCSI トラブルシューティング (英語)  (www.ibm.com/servers/eserver/iseries/integratedxseries/iscsireadme/troubleshooting.html) を参照してください。

メッセージ CPPC056 がプロダクト・アクティビティ・ログにある場合、CHAP 構成に問題がある可能性があります。

ブート用に構成された、ホストされるシステムの iSCSI HBA と、NWSD のシステム・ドライブ記憶域スペース用に構成されたパスに対応する iSeries HBA との間に、ネットワーク問題がある可能性があります。249 ページの『ブートおよび記憶域パス・ネットワークの分析』を参照してください。


NWSD の状況が DEGRADED である

サーバーで構成されている必要なネットワーク・サーバー・ホスト・アダプターがすべてオンに変更されているか確認してください。ネットワーク・サーバー・ホスト・アダプターがオンに変更されない場合、ネットワーク・サーバー・ホスト装置のメッセージ待ち行列の中にメッセージがないか調べてください。

ブート・パス以外のパスを使用する記憶域が Windows で表示されない

- ホストされるシステムと、非ブート・パスに対応する iSeries 内の iSCSI HBA との間に、ネットワーク問題がある可能性があります。『ブートおよび記憶域パス・ネットワークの分析』を参照してください。
- メッセージ CPPC056 がプロダクト・アクティビティ・ログにある場合、CHAP 構成に問題があります。この場合、最も可能性が高いのは、iSeries 上の Windows 環境が自分独自の機密データを i5/OS と Windows の間で安全に転送するために必要とする、デジタル証明書の問題です。250 ページの『パス証明書の管理』を参照してください。

ブート・パス以外のパスを使用する記憶域が Windows でときどき遅れて表示される

- これは特定の i5/OS 構成情報 (ネットワーク・サーバー・ホスト・アダプターの SCSI ローカル・インターフェース情報、またはリモート・システム構成の CHAP 情報など) を変更した後、最初にサーバーを始動する際の正常な動作です。
- 以前に、ホストされるシステムの iSCSI HBA をこの特定の NWSD とともに使用したことがない場合、これは正常な動作です。ホストされるシステムで iSCSI HBA を取り替えた場合や、別のホストされるシステムをホット・スワップとして使用する場合などにこれが当てはまる場合があります。
- 上記の状況の影響を受けやすい自動開始サービスがアプリケーションに含まれている場合、拡張 iSCSI タスク (英語)  Web ページ (www.ibm.com/servers/eserver/iseries/integratedxseries/iscsireadme/advancedtasks.html) を参照してください。

ユーザー登録またはリモート・コマンドのサブミットが NTA02BB、NTA028A、NTA028B で失敗する


- iSeries 上の Windows 環境が自分独自の機密データを i5/OS と Windows の間で安全に転送するために必要とする、デジタル証明書に問題があります。250 ページの『パス証明書の管理』を参照してください。
- NTA028A および NTA028B の場合、ホストされるシステムの時刻と日付が iSeries の日付と大幅に違ってないか確認してください。これはデジタル証明書が無効と認識される原因となる場合があります。

ブートおよび記憶域パス・ネットワークの分析

これらのステップと追加のトラブルシューティングの手順については、iSCSI トラブルシューティング

(英語)  (www.ibm.com/servers/eserver/iseries/integratedxseries/iscsireadme/troubleshooting.html) を参照してください。

- ホストされるシステム上で、CTRL-Q ユーティリティを使用して、ホストされるシステムの iSCSI HBA MAC アドレスを表示してください。これらが i5/OS リモート・サーバー構成の SCSI インターフェース・アダプター・アドレス値と一致するようにしてください。手動構成されたブートが失敗した場合、このステップはスキップできます。
- CTRL-Q ユーティリティまたは SCSI ドライバーの「デバイス マネージャ」ビューを使用して、iSeries 用の該当する iSCSI HBA の SCSI IP アドレスを PING します。
- PING が失敗する場合、以下のステップを実行してください。
 - 物理ネットワークが正しく接続されていること、またスイッチなどのネットワーク内の装置が機能していることを確認します。
 - 31 ページの『iSCSI ネットワーク』で定義されている要件が満たされていることを確認します。
 - ファイアウォールまたは同種のパケット・フィルター機能が関係している場合、ファイアウォールが Internet Control Message Protocol (ICMP) パケットを通すようになっていることを確認します。SCSI IP アドレスとは異なり、LAN IP アドレスは Windows で実行されるファイアウォール・ソフトウェアの影響を受ける場合があります。

- | - NWS D が *NONE 以外の IP セキュリティー (IPSec) 規則を使用する場合、iSCSI トラブルシューティング (英語)  (www.ibm.com/servers/eserver/iseries/integratedxseries/iscsireadme/troubleshooting.html) を参照してください。
- | • ping が成功する場合、以下のステップを実行してください。
 - | - ファイアウォールまたは同種のパケット・フィルター機能が関係している場合、145 ページの『ファイアウォールの構成』を参照してください。SCSI IP アドレスとは異なり、LAN IP アドレスは Windows で実行されるファイアウォール・ソフトウェアの影響を受けます。
 - | - DHCP ブートが失敗し、かつルーティングされるネットワークが関係する場合、適切に構成された DHCP リレー・エージェント (BOOTP リレー・ブートとも呼ばれる) がネットワーク内に存在することを確認します。

| パス証明書の管理

| 注: このセクションは iSCSI 接続のシステムにのみ関係します。

| 通常、iSeries 上の Windows 環境は、自分独自の機密データを i5/OS と Windows の間で安全に転送するために必要となるデジタル証明書を自動的に生成します。これらはパス証明書と呼ばれます。パス証明書に問題があると思われる場合、以下を行うことができます。

- | • 5722-SS1 オプション 34 (デジタル証明書マネージャー) がインストール済みであることを確認します。
- | • サーバーの開始時に新規デジタル証明書を生成することにより、i5/OS と Windows が互換性のあるデジタル証明書を持つようにします。これは例外的な状況でのみ行うべきです (たとえば Windows システム・ドライブの古いバージョンの記憶域スペースを復元し、対応する i5/OS 証明書ストアは復元しない場合など)。iSeries ナビゲーターを使用して新規パス証明書を生成するには、以下のステップに従ってください。
 - | 1. 「統合サーバー管理」を展開します。
 - | 2. 「サーバー」を展開します。
 - | 3. 表示されたリストからサーバーを右クリックします。
 - | 4. 「オプションで始動...」を選択します。
 - | 5. 「パス証明書の再生成」オプションをチェックします。
 - | 6. 「開始」をクリックします。

| CL コマンドを使用する場合は、構成の変更 (VRYCFG) コマンドのパス証明書の生成 (GENPTHCERT) キーワードを参照してください。

| IBM Director のトラブルシューティング

| 注: このセクションは iSCSI 接続のシステムにのみ関係します。

| IBM Director に接続できない場合 (たとえばサーバーの開始時またはシャットダウン時) は、以下のアクションを取ってください。

- | • 5 分待ってから操作を再試行します。
- | • IBM Director を停止し、再始動します。
 - | - i5/OS コマンド行で ENDTCPVSR SERVER(*DIRECTOR) を入力します。

- | - Director サーバーが停止するまでに数分かかります。停止プロセスの状況は、qsh から /qibm/userdata/director/bin/twgstat を実行することにより入手できます。数分たつと、最終的に「非アクティブ」状態を報告するはずですが。
- | - i5/OS コマンド行で qsh を入力することにより、qsh インタープリターを開始します。
- | - qsh から /qibm/userdata/director/bin/twgstart を実行します。
- | • IBM Director プロパティ・ファイルの構成を確認します。

| IBM Director プロパティ・ファイルは IBM Director のインストール時に /QIBM/ProdData/Director/classes/com/ibm/sysmgmt/app/iide/IIDETask.properties にインストールされます。

| IBM Director プロパティ・ファイルが存在するかどうかを確認します。存在しない場合、IBM Director を再インストールするか、またはサービス担当者に連絡してください。

- | • IBM Director プロパティ・ファイルにポートが指定されているかどうかを確認します。

| このファイルには『port = **xxxxx**』を指定する行が含まれているはずですが。**xxxxx** はポート番号です。この行が存在しない場合、以下のステップを行ってください。

- | 1. ファイルを編集し、『port = 5779』を含む行を追加します。5779 は IBM Director への i5/OS 接続に使用されるデフォルトのポートです。
- | 2. IBM Director を再始動します。

- | • IBM Director によって使用されているポートが別のアプリケーションで使用されていないかどうかを確認します。


| IBM Director を開始した後、IBM Director プロパティ・ファイルで指定されているポートが別のアプリケーションで使用されていないかどうかを確認します。

- | 1. iSeries ナビゲーターを使用して、「ネットワーク」→「TCP/IP 構成」→「IPv4」→「接続」を展開します。
- | 2. IBM Director プロパティ・ファイルで指定された同じポート番号を「ローカル・ポート」列に持つリスト項目を右クリックし、「ジョブ」を選択します。
- | 3. ジョブ・リストから、ジョブ名 **Qcpmgtsvr**、ユーザー **Qcpmgtdir** を持つジョブを探します。これは指定のポートを使用している唯一のジョブであるはずですが。

| 他のジョブがポートを使用している場合、以下のステップを使用して、IBM Director によって使用されているポートを変更する必要があります。

- | 1. IBM Director プロパティ・ファイルの行『port = **xxxxx**』で指定されているポート番号を変更します。**xxxxx** はポート番号です。
- | 2. IBM Director を再始動します。

| **ディスクバリーの問題:** リモート・サーバーまたは格納装置が見つからないことを示すメッセージがログに記録される場合、IBM Director インターフェイスがネットワーク上でターゲットとなるサービス・プロセッサを見つけることができなかったことを示します。154 ページの『リモート・サーバーのディスクバリーおよび管理』を参照してください。

| リモート監視プログラム II サービス・プロセッサを使用している場合、最新のファームウェアを使用しているかどうかを確認してください。iSCSI インストールについて最初にお読みください (英語) 

| (www.ibm.com/servers/eserver/iseries/integratedxseries/iscsireadme) を参照してください。

サービス・プロセッサのディスカバーにユニキャスト・アドレッシングを使用していない場合、以下のステップを行ってください。

- iSeries サービスにリモート・システムのサービス・プロセッサへの物理的なネットワーク接続があるかどうか確認してください。

- TCP/IP のトラブルシューティング・トピック・コレクションの iSeries ナビゲーターから Ping するを参照してください。

- iSeries サーバーにサーバー・プロセッサへの物理的なネットワーク接続がある場合、iSCSI ネットワーク上のルーターまたはスイッチのファイアウォール設定を確認してください。 iSeries LAN インターフェースとサービス・プロセッサの間のネットワーク・ルーターまたはスイッチがマルチキャスト・アドレッシングをサポートしていないか、またはマルチキャスト・アドレッシングを許容するように構成されていない可能性があります。

ネットワーク・ルーターまたはファイアウォールは SLP マルチキャスト・パケットをブロックする場合があります。 Service Location Protocol IP アドレスの 239.255.255.253 またはポート番号 427 を許容して SLP パケットの受け渡しができるようにルーターまたはファイアウォールを構成する必要があるかもしれません。

- ユニキャスト・アドレッシングを使用するようにサービス・プロセッサを構成します。

サービス・プロセッサの静的ホスト名または IP アドレスは構成済みでなければなりません。これは RSA II 用の BIOS ユーティリティまたはサービス・プロセッサ Web インターフェースを使用して行えます。サービス・プロセッサ Web インターフェースを使用してサービス・プロセッサを構成する方法については、160 ページの『管理モジュールまたは RSA II の Web インターフェースの使用』を参照してください。

ユニキャスト・アドレッシングを使用するようにサービス・プロセッサ構成を変更します。このユニキャスト・アドレッシングは、サービス・プロセッサに接続するために上記のサービス・プロセッサで設定済みのホスト名または IP アドレスを使用します。 137 ページの『サービス・プロセッサ構成プロパティの変更』を参照してください。

サービス・プロセッサのディスカバーにユニキャスト・アドレッシングを使用している場合

- サービス・プロセッサ IP アドレスまたはホスト名が、リモート・システム・サービス・プロセッサと i5/OS 上のサービス・プロセッサ構成の両方で正しく構成されているかどうか確認してください。

- 一般的な TCP/IP のトラブルシューティングの手順については、TCP/IP トラブルシューティングのトピックを参照してください。

SSL 接続の問題: サービス・プロセッサへの Secure Socket Layer (SSL) 接続が構成されると、多様な問題が発生する場合があります。 143 ページの『サービス・プロセッサ SSL の構成』を参照してください。

正しい i5/OS 証明書ストアに証明書がインポートされない。

手動のセキュリティー・モードを使用している場合、iSeries *SYSTEM 証明書ストアにサービス・プロセッサ認証局 (CA) ルートがあるかどうか確認してください。

1. サービス・プロセッサ Web インターフェースに接続します。

2. 証明書を表示します。証明書の「発行元」フィールドの認証局をメモします。

3. CA が *SYSTEM 証明書ストアの証明書としてリストされるかどうかを判別するために、iSeries デジタル証明書マネージャー (DCM) インターフェースに接続します。

- a. サービス・プロセッサにインストール済みの証明書のルート CA を判別します。

- 1) `http://hostname` (*hostname* はサービス・プロセッサのホスト名) または `http://ipaddress` (*ipaddress* はサービス・プロセッサの IP アドレス) に移動して Web ブラウザーでサービス・プロセッサ Web インターフェースに接続します。
 - 2) Web サイトの ID を確認したセキュリティ証明書を表示するためにブラウザーのヘルプの説明に従います。
 - 3) 証明書階層を表示するためにブラウザーのヘルプの説明に従います。
 - 4) 階層の最上位の項目がルート CA 証明書になります。
 - 5) 以下のステップ h で使用するためにルート CA 証明書に関して表示される名前をメモします。
- b. iSeries デジタル証明書マネージャー (DCM) インターフェースに接続します。デジタル証明書マネージャーのトピックのデジタル証明書のはじめてのセットアップを参照してください。
 - c. 「証明書ストアの選択 (Select Certificate Store)」をクリックします。
 - d. *SYSTEM を選択し、「続行」をクリックします。
 - e. *SYSTEM 証明書ストアの証明書ストア・パスワードを入力します。
 - f. 左側のペインで、「ファースト・パス」をクリックします。
 - g. 「CA 証明書の処理」を選択し、「続行」をクリックします。
 - h. 「CA 証明書の処理」ページで、ステップ a で判別されたルート CA 証明書の名前と一致する「認証局 (CA)」フィールドの項目を探します。
 - i. この項目の「状況」フィールドが「使用可能」の場合、CA は正しく構成されていることになります。
 - j. この項目の「状況」フィールドが「使用不可」の場合、以下のステップを実行して使用可能にする必要があります。
 - 1) 使用可能にする必要のある「認証局 (CA)」項目の左にあるラジオ・ボタンを選択します。
 - 2) 表の下の「使用可能」プッシュボタンを選択します。
 - 3) これで CA は正しく構成されます。
 - k. ステップ a) で判別されたルート CA 証明書の名前と一致する項目が「認証局 (CA)」フィールドに存在しない場合、以下のステップを行って CA を追加してください。
 - 1) 認証局 (CA) から受け取ったオリジナルの E メールを参照します。この E メールに証明書 (サービス・プロセッサにインポートされたもの) および関連したトラステッド・ルート証明書が含まれてははずです。
 - 2) iSeries 上の IFS ファイル・システムのディレクトリーにトラステッド・ルート証明書を FTP でファイル転送し、絶対パスおよびファイル名をメモします。
 - 3) 左側のペインで「証明書の管理」を選択し、タスクのリストを表示します。
 - 4) タスク・リストから、「証明書のインポート」を選択します。
 - 5) 証明書タイプとして「認証局 (CA)」を選択し、「続行」をクリックします。
 - 6) CA 証明書ファイルの完全修飾パスおよびファイル名を指定し、「継続」をクリックします。インポート・プロセスが成功したことを確認するメッセージか、またはプロセスが失敗した場合にはエラー情報を提供するメッセージが表示されます。
 - 7) これで CA は正しく構成されます。

サービス・プロセッサ構成が初期化されていない。

自動セキュリティ・モードを使用している場合、そのモードの構成後にサービス・プロセッサ構成を初期化する必要があります。

以下のステップを実行してください。

- リモート・システムのサービス・プロセッサを初めて初期化する場合、138 ページの『サービス・プロセッサの初期化』で説明されている手順に従って、新規サービス・プロセッサを初期化します。
- リモート・システムのサービス・プロセッサを以前に初期化した場合は、138 ページの『サービス・プロセッサの初期化』で説明されている手順に従って、リモート・システムのサービス・プロセッサからサービス・プロセッサ構成へ、ユーザー、パスワード、および証明書を同期します。

サービス・プロセッサの証明書 ID が認識されない。

手動のセキュリティーを使用している場合、サービス・プロセッサの証明書フィールドが、サービス・プロセッサ構成で構成されているサービス・プロセッサ証明書 ID と一致しているかどうか確認します。

1. サービス・プロセッサ構成を表示し (137 ページの『サービス・プロセッサ構成プロパティの表示』を参照)、「**セキュリティー**」タブをクリックします。サービス・プロセッサの証明書 ID コンポーネントの値および比較値をメモします。コンポーネントの値は、次のように証明書フィールドにマップします。

- 共通名 - (サブジェクト) 共通名 (CN) に発行
- E メール・アドレス - (サブジェクト) (E) に発行
- 組織単位 - (サブジェクト) 組織単位 (OU) に発行

2. サービス・プロセッサの Web インターフェースにアクセスします。

3. サービス・プロセッサのセキュリティー証明書を表示します。

4. 証明書フィールドを、サービス・プロセッサ構成に現れる比較値と比較します。

5. これらの値が一致しない場合は、137 ページの『サービス・プロセッサ構成プロパティの変更』で説明されている方法を使用して、正しい値を入力します。その後、リモート・システムのサービス・プロセッサからサービス・プロセッサ構成へ証明書を同期する方法について、138 ページの『サービス・プロセッサの初期化』を参照してください。

注: サービス・プロセッサ構成で、サービス・プロセッサ証明書を使用しないことを指定できます。

サービス・プロセッサが SSL をサポートしない。

• セキュア接続を必要としない場合、137 ページの『サービス・プロセッサ構成プロパティの変更』を参照してください。「**セキュリティー**」タブで、「**証明書を使用しない (物理的セキュリティーが必要)**」オプションを選択し、変更を保管します。

• サービス・プロセッサが SSL をサポートしているかどうかを確認します。

1. 155 ページの『リモート・サーバーおよびサービス・プロセッサのディスクバリー』を参照してください。

2. サービス・プロセッサが SSL に対応している場合、SSL サポートを追加するにはファームウェアまたはハードウェアの更新が必要かどうかを確認するためにサービス担当者に連絡してください。

iSCSI 接続のサーバーの仮想イーサネットの問題

Windows TCP/IP スタックで使用可能な接続に関する情報を参照するには、Windows コマンド・プロンプトで **ipconfig /all** と入力します。以下に関する情報が表示されるはずですが。

- 外部ネットワーク・アダプター
- iSCSI HBA ポートの LAN インターフェース
- iSeries サーバーの仮想イーサネット・アダプター

ipconfig コマンドの結果を、以下のいずれかのトラブルシューティングのケースと突き合わせ、そのケースに対して提案されるアクションを問題が解決されるまで実行します。

ipconfig で構成済み LAN IP アドレスが欠落している

このケースは、i5/OS リモート構成の LAN インターフェースのインターネット・アドレスと、ipconfig が任意の iSCSI HBA に関して表示する IP アドレスとが一致しない場合に当てはまります。リモート・システム構成の表示については、134 ページの『リモート・システム構成プロパティの表示』を参照してください。

- iSCSI HBA の物理アドレス (MAC アドレス) を知るために、ipconfig の結果を調べます。ipconfig によって表示される物理アドレスが、i5/OS リモート・システム構成の LAN インターフェース用のアダプター・アドレスと異なる場合、以下のステップを行ってください。

1. Windows コンソールからサーバーをシャットダウンします。
2. i5/OS から NWS D をオフに変更します。163 ページの『統合サーバーの開始と停止』を参照してください。
3. リモート・システム構成の LAN インターフェース用のアダプター・アドレスを変更します。
4. i5/OS を使用して、NWS D を開始 (オンに変更) します。163 ページの『統合サーバーの開始と停止』を参照してください。

- 「コントロール パネル」、「管理ツール」、「サービス」の順に選択します。「iSeries Shutdown Manager」がサービスのリストにあり、その状態が「開始」であることを確認します。このサービスは、LAN IP インターフェース情報を、i5/OS リモート・システム構成から構成済み MAC アドレスを持つポートに自動的に割り当てます。

- Windows の「アプリケーション」イベント・ログで、iSeries Shutdown Manager のソースを持つイベントがないか調べます。

- 「一般」タブ、「認証」タブ、および「詳細」タブを持つネットワーク・プロパティ・ウィンドウはすべてクローズします。このタイプのウィンドウは、IP アドレスの割り当てに必要なリソースをロックするからです。このタイプのウィンドウをクローズしたら、欠落している IP アドレスを iSeries Shutdown Manager が割り当ててのを 30 秒待ち、ipconfig /all を再び入力します。

- ipconfig の結果のいずれにもインストール済みの iSCSI HBA が記載されていない場合、Windows の「デバイス マネージャ」を開き、iSCSI HBA のネットワーク・ドライバーがインストール済みで使用可能になっていることを確認します。ドライバーに黄色の「！」が付いているかまたはグレー化されている場合、Windows の「システム」イベント・ログで、QL40xx のソースを持つイベントがないか調べ、システム BIOS セットアップ・メニューによって iSCSI HBA が使用不可になっていないことを確認します。


ipconfig がメディア切断状態の構成済み iSCSI HBA 接続を表示する

このケースは、ipconfig が、メディア切断状態で、かつ i5/OS リモート・システム構成のアダプター・アドレスに一致する物理アドレスを持つ iSCSI HBA 接続を表示する場合に当てはまります。

- 物理ネットワークが正しく接続されていること、またスイッチなどのネットワーク内の装置が、ホストされるシステムの iSCSI HBA への物理リンクで機能していることを確認します。

ipconfig がメディア切断状態の IBM iSeries 仮想イーサネット接続を表示する

- 仮想イーサネットは機能中の iSCSI ネットワークを必要とするため、iSCSI HBA の問題は最初に解決する必要があります。先に進む前に、ipconfig が i5/OS リモート・システム構成の LAN アドレスを表示することを確認します。

- 物理ネットワークが正しく接続されていること、またスイッチなどのネットワーク内の装置が、ホストされるシステムの iSCSI HBA への物理リンクを越えて機能していることを確認します。
- 31 ページの『iSCSI ネットワーク』で定義されている要件が満たされていることを確認します。
- 「コントロール パネル」、「管理ツール」、「サービス」の順に選択します。「iSeries Manager」、「iSeries Shutdown Manager」、および「iSeries Virtual Ethernet Manager」がサービスのリストにあり、その状態が「開始」であることを確認します。
- Windows の「アプリケーション」イベント・ログで、「iSeries Virtual Ethernet Manager」のソースを持つイベントがないか調べます。
- ファイアウォールまたは同種のパケット・フィルタ機能が関係している場合、145 ページの『ファイアウォールの構成』を参照してください。i5/OS リモート・システム構成の LAN IP インターフェースは、Windows で実行されるファイアウォール・ソフトウェアの影響を受ける場合があります。
- NWSD が *NONE 以外の IPSec 規則を使用する場合、iSCSI トラブルシューティング (英語) Web ページ  (www.ibm.com/servers/eserver/iseries/integratedxseries/iscsireadme/troubleshooting.html) を参照してください。

ipconfig が不正 IP アドレスを持つ IBM iSeries 仮想イーサネット接続を表示する

- Windows で IP アドレスを手動で構成します。Point-to-Point 仮想イーサネットの場合は、263 ページの『Point-to-Point 仮想イーサネット IP アドレスの競合』を参照してください。それ以外の仮想イーサネット・ネットワークの場合は、この手順のステップ 1 からステップ 5 のみが適用されます。

i5/OS で「仮想ネットワーク x」が構成されているのに、ipconfig に「IBM iSeries 仮想ネットワーク x」が欠落している

- i5/OS で、対象の仮想イーサネットの回線記述が存在するかどうか確認します。Point-to-Point 仮想イーサネットの場合は、126 ページの『Point-to-Point 仮想イーサネット・ネットワークについて』を参照してください。
- 「コントロール パネル」、「管理ツール」、「サービス」の順に選択します。「iSeries Virtual Ethernet Manager」がサービスのリストにあり、その状態が「開始」であることを確認します。このサービスにより、i5/OS の回線記述の構成が一致するように、IBM iSeries 仮想イーサネットのアダプターが自動的に作成および除去されます。
- 未署名のドライバーのインストールをブロックするようにシステムが設定されていないことを確認します。詳しくは、261 ページの『LAN ドライバーのインストールまたは更新を開始する』のステップ 1 からステップ 4 を参照してください。設定を「ブロック」から変更する場合、「iSeries Virtual Ethernet Manager」サービスを再開し、30 秒待ち、`ipconfig /all` と再び入力します。
- Windows で「デバイス マネージャ」を開き、対象の IBM iSeries 仮想イーサネット・アダプターのネットワーク・ドライバーがインストール済みで使用可能になっていることを確認します。ドライバーの横に黄色の「！」が表示されている場合、Windows の「システム」イベント・ログで、`Qvndvimp` のソースを持つイベントがないか調べます。

ipconfig の結果は正常と思えるのに、大容量の転送に失敗する

- IBM iSeries 仮想イーサネット・アダプターおよび iSCSI HBA ポートの 'LAN' 側が、iSCSI ネットワーク・サポートより大きな最大伝送単位を使用するように構成されていないことを確認します。たとえば、一部のスイッチは 9000 バイトのジャンボ・フレームをサポートしません。ネットワーク装置の仕様を確認してください。詳しくは、151 ページの『最大伝送単位 (MTU) の考慮事項』を参照してください。

IXS および IXA 接続のサーバーの仮想イーサネットの問題

このセクションでは、仮想イーサネットの Point-to-Point LAN および仮想イーサネット・ポート 0 から 9 までは、すべて仮想イーサネット・アダプターまたは仮想イーサネット・ポートとみなします。

仮想イーサネット・アダプター (VE) および仮想イーサネット・データ転送 (DT) という、2 種類の仮想イーサネット・デバイス・ドライバがあります。

- 仮想イーサネット・アダプターは、NIC ハードウェアと関連していないため、「仮想」というアダプターとして表示されるドライバに対応しています。
- 仮想イーサネット・データ転送は、すべての仮想イーサネット・ネットワークに接続するシステム・バスへの接続を行うドライバです。

VE ポートがシステム・バスと通信できない時には、VE ポートは、ポートのケーブルのプラグが接続されていない (ケーブルが非接続) ことを報告します。これは、仮想イーサネット・エラーのトラブルシューティングのための大切な概念です。

Windows での仮想イーサネット・ポートは、仮想イーサネット・ユーティリティー (VEU) により自動的にインストールおよびアンインストールされます。そのユーティリティーは、構成ファイルを通して NWSD からの信号を受け取ります。たとえば、ユーザーが NWSD の下で、与えられた仮想イーサネット・ポートのための回線記述を作成する時には、VEU は、対応する VE ポートをインストールします。Windows サーバーをリブートすると、VE ポート・アドレスが構成されます。

以下の仮想イーサネット・コンポーネントは、リストにあるドライバを使用します。

- 仮想イーサネット・アダプター: qvndvemp.sys
- 仮想イーサネット・データ転送: qvndvedt.sys
- 仮想イーサネット・インストール・ユーティリティー: qvndveu.exe

仮想イーサネットの問題のトラブルシューティング

いずれかの VE ポート間の通信が機能していない時には、問題のトラブルシューティングをするために、2 つの一般的な作業を行う必要があります。

1. VE ポートの状況を判別する
2. 観察された結果を次のトラブルシューティングの事例に突き合わせる

VE のポート状況を判別する

VE ポートの状況を判別する方法は、以下の通りです。

- iSeries コンソールを使用して、VE ポートの回線記述が NWSD の下で作成されているかを判別する。
- Windows コンソールを使用して、「ネットワークとダイヤルアップ接続」フォルダーを開き、VE ポート・アイコンがあるかを判別する。

ポート状況をトラブルシューティングの事例に突き合わせる

VE ポートの状況を判別した結果を、次のトラブルシューティングの事例の 1 つに突き合わせます。

- 258 ページの『回線記述およびアイコンの両方がある』。
- 258 ページの『回線記述があり、アイコンがない』。
- 259 ページの『回線記述がなく、アイコンがある』。
- 259 ページの『回線記述およびアイコンの両方がない』。

いずれの場合においても、まず i5/OS 側を検証し、その後 Windows 側を検証します。Windows 側を検証するためには、「イベント ログ」および「デバイス マネージャ」を開く必要があるかもしれません。

- 「イベント ログ」を開くには、Windows の「スタート」メニューから、「プログラム」を選択した後、「管理ツール」、「イベント ビューア」の順に選択します。
- 「デバイス マネージャ」を開くには、Windows の「スタート」メニューから、「設定」を選択した後、「コントロール パネル」、「管理ツール」、「コンピューターの管理」、「デバイス マネージャ」の順に選択します。

回線記述およびアイコンの両方がある

i5/OS 側を検証する

回線記述を検査します。回線記述が「失敗」の状態の時、次のステップを実行してください。

1. PAL 項目および VLOG を収集する
2. サポートに連絡する
3. Windows 側を検証する

それ以外の時は、回線記述が「オンに変更保留」、「オンに変更」、または「RCYPND」の状態の時には、Windows 側を検証してください。

Windows 側を検証する

「ネットワークとダイヤルアップ接続」ウィンドウを開き、VE アイコンをチェックします。

- VE アイコンが機能している様子であり、回線記述が「オンに変更」の状態の時、IP アドレスが正しく構成されていることを検証します。問題が続く場合には、サポートに連絡してください。
- VE アイコンが機能している様子であり、回線記述が「オンに変更保留」または「RCYPND」の状態の時には、PAL 内の項目を検証し、サポートに連絡してください。
- VE アイコンに赤い X (ケーブルが非接続) が付いている時は、「イベント ログ」を開き、qvndvemp.sys ドライバーの項目を見つけます。
 - qvndvemp.sys の項目を見つけた時は、それらを記録し、サポートに連絡します。おそらくドライバーの初期化が失敗しており、問題の判別には IOP ダンプが必要になるかもしれません。
 - qvndvemp.sys の項目が見つからない時には、サポートに連絡して、回線記述の状態を知らせてください。その問題は、i5/OS LIC の問題に関係していると思われる。

回線記述があり、アイコンがない

i5/OS 側を検証する

回線記述を検査します。回線記述が「失敗」の状態の時、次のステップを実行してください。

1. PAL 項目および VLOG を収集する
2. サポートに連絡する
3. Windows 側を検証する

それ以外の時は、回線記述が「オンに変更保留」、「オンに変更」、または「RCYPND」の状態の時には、Windows 側を検証してください。

Windows 側を検証する

「デバイス マネージャ」を開き、「ネットワーク アダプタ」をクリックしてインストール済みアダプターのリストを表示させ、VE ポートの項目を見つけます。

- VE ポートの横に感嘆符 (!) がある場合、以下のステップを実行してください。
 1. 「イベント ログ」を開き、qvndvemp.sys ドライバーの項目のどれかを見つけ、それらを記録します。
 2. サポートに連絡します。ドライバーの初期化は失敗しました。原因を診断するためにはアシスタンスを必要とします。
- VE ポートに赤い X が付いている場合には、以下のステップを行ってください。
 1. VE ポートを右マウス・ボタン・クリックし、「有効」を選択します。
 2. 「ネットワークとダイヤルアップ接続」ウィンドウを開き、VE アイコンを見つけます。
 3. VE ポート・アイコンがないか、それが灰色 (グレー) のままの場合には、「イベント ログ」を開きます。
 4. qvndvemp.sys ドライバーの項目を見つけ、見つかったすべての項目を記録し、サポートに連絡します。VE ポートは、ロードまたは開始に失敗しました。

回線記述がなく、アイコンがある

i5/OS 側を検証する

現行において、NWSD の下で VE ポートに回線記述がないことを検証した後、Windows 側を検証してください。

Windows 側を検証する

「ネットワークとダイヤルアップ接続」ウィンドウを開き、VE アイコンをチェックします。インストール VEU が VE ポートの除去に失敗した時には、統合サーバーをリブートし、この状態を消去します。問題が続く場合には、以下のステップを行ってください。

1. VEU を使用して、次のコマンドを使用することにより手動で VE ポートを除去します。

```
qvndveu -a -R -x [port_id]
```

ここで、[port_id] は、除去されるポートに対応する 10 進数 (0 から 9 まで)、または Point-to-Point (Point-to-Point 仮想イーサネット) の場合は p のいずれかです。

2. コマンドの実行後、VE ポート・アイコンがなくなった場合には、処理は完了しました。しかしながら、VEU が VE ポートのアンインストールおよび除去に失敗した場合には、残りのステップを続けます。
3. VEU ログ・ファイル (D:\%as400nt%\qvndveu.log) を収集します。
4. 「イベント ログ」を開き、qvndvemp.sys ドライバーの項目のどれかを見つけ、それらを記録します。
5. サポートに連絡します。以下のものが手元にあることを確認してください。
 - 記録した qvndvemp.sys の項目
 - 直前に収集した VEU ログ・ファイル

回線記述およびアイコンの両方がない

i5/OS 側を検証する

VE ポートをインストールするためには、NWSD 内に回線記述がなくてはなりません。123 ページの『仮想イーサネット・ネットワークの構成』に示されている指示を使用して、回線記述を作成してください。

注: 回線記述を追加するには、NWSD をオフに変更する必要があります。回線記述を作成し、統合 Windows サーバーをリブートした後は、インストール VEU は、Windows 内に VE ポートを自動的に作成します。

回線記述の作成および統合サーバーのリブートを正常に行った後に VE ポートの問題が続く時には、このトラブルシューティングのセクションに戻り、新しく一致する障害の事例の指示に従ってください。

Windows 側を検証する

i5/OS 回線記述がない時には、VE ポートは Windows でリスト表示されないはずですが。123 ページの『仮想イーサネット・ネットワークの構成』で説明されているとおりに回線記述をインストールし、統合サーバーを再始動して、問題が修正されたことを確認してください。

外部ネットワークに関する問題

統合サーバーの外部ネットワークに問題がある場合、次のようにします。

- 統合 Windows サーバーのイベント・ログを調べて、通信エラーまたはデバイス・ドライバー・エラーのいずれかが生じていないかどうかを確認します。そのために、Windows イベント ビューアを使用することができます。2890、2892、および 4812 統合 xSeries サーバーでサポートされる外部アダプターに関連したイベント・ログ Source フィールドには、IBMTRP、PCNET、ALTND5、E100B、または E1000 のいずれかが示されている可能性があります。IBMTRP トークンリング・サービスのイベント・ログの中にテキストが見つからない場合には、Windows のレジストリーに変更をする必要があります。

注: Windows のレジストリーを変更する処理に精通しておられない方は、サービス担当者に連絡してください。



この処理に精通しておられるならば、イベント・ログ内のテキストを表示可能にするために、以下のステップを行ってください。

1. Windows の「スタート」メニューから、「ファイル名を指定して実行」をクリックします。
 2. 「regedit」と入力します。
 3. 「レジストリ エディタ」で、
「HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\System\IBMTRP」に進みます。
 4. 「EventMessageFile」を選択します。
 5. 「レジストリ エディタ」の「編集」メニューから、「変更」を選択します
 6. 「%SystemRoot%\System32\netevent.dll;%SystemRoot%\System32\ibmsgnet.dll」と入力します。
 7. 「レジストリ エディタ」を閉じ、統合サーバーを再始動します。
- イーサネット・アダプターの場合には、**iSeries Ethernet Adapter (PCI)** または **AMD PCNET Family Ethernet Adapter (PCI)** という名前が付いたドライバーがリストされており、「開始済み」の状況であることを次のようにして確認します。
 1. 「スタート」、「管理ツール」、「コンピュータの管理」、「システム ツール」、「デバイス マネージャ」、「ネットワーク アダプタ」の順にクリックします。
 2. **iSeries Ethernet Adapter (PCI)** または **AMD PCNET Family Ethernet Adapter (PCI)** という名前が付いたドライバーがリストされており、「開始済み」の状況であることを確認します。
 - トークンリング・ネットワークの場合には、「デバイス マネージャ」でも、**IBM High-Speed 100/16/4 Token-Ring PCI Adapter** または **IBM PCI Token-Ring Adapter** を開始していることを確認します。

注: 起動の設定は、「使用する」でなければなりません。
 - トークンリング・ネットワークの場合には、「ネットワーク・データ転送速度」の設定が実際のネットワークに適切な値になっていることを確認してください。
 - イーサネット・ネットワークの場合には、「リンク速度」および「二重」の設定が実際のスイッチまたはハブに適切な値になっていることを確認してください。4812 または 5701 の接続速度が 1 億ビット/

秒以下の場合、スイッチの仕様が IEEE 802.3ab 規格に準拠しているかどうかを調べてください。

4812 または 5701 のギガビット・イーサネット・ポートの Windows LAN ドライバーは、規格に準拠していない古いモデルのスイッチに接続されていると、接続速度が 1 億ビット/秒までしかでないことがあります。

- 2892 統合 xSeries サーバーの 10/100 Mbps イーサネット・ポートは、自動極性機能のない特定の 10 Mbps ハブおよびルーターへの直接接続をサポートしていません。2892 10/100 ポートを 10 Mbps ハブまたはルーターで完全に機能させることが難しい場合、自動極性サポートの仕様を確認してください。さらに、2892 10/100 ポートが他の装置でも機能するか確認してください。
- 問題が続く場合には、 IBM iSeries サポート Web ページ (英語)  の技術情報データベースをチェックしてください。それでも解決しない場合には、テクニカル・サポート・プロバイダーに連絡してください。

統合 Windows サーバーでの LAN ドライバーの手動アップデート

Windows 2000 Server および Windows Server 2003 は、一般的には LAN アダプターおよびポートに適切な LAN ドライバーを自動的にインストールします。しかしながら、特別の状況の場合には、LAN ドライバーを手動でインストールまたは更新することができます。

仮想イーサネット以外のアダプター用の LAN ドライバーを、手動で外部に接続された Netfinity または xSeries サーバーにインストールまたは更新するためには、IBM パーソナル・コンピューター・サポート

(英語) Web サイト  に進み、「Servers」、「Device driver file matrix」の順に選択します。

統合 xSeries サーバー内のアダプターまたはポート用、または仮想イーサネット用の LAN ドライバーを手動でインストールまたは更新するためには、次の作業を行います。

1. 『LAN ドライバーのインストールまたは更新を開始する』。
2. 『インストールまたは更新したいアダプターを選択する』。
3. 262 ページの『LAN ドライバーのインストールまたは更新を完了する』。

LAN ドライバーのインストールまたは更新を開始する

統合 xSeries サーバー内の LAN ドライバーまたはポート、または仮想イーサネットの場合に手動インストールまたは更新を開始するためには、次のステップを行ってください。

1. Windows の「スタート」メニューで、「設定」、「コントロール パネル」の順に選択します。
2. 「システム」をダブルクリックします。
3. 「システムのプロパティ」ウィンドウで、「ハードウェア」タブを選択します。
4. 新規 LAN ドライバーにデジタル署名がない場合、あるいは LAN ドライバーにデジタル署名があるか不明な場合には、ドライバー署名ポリシーが「無視」に設定されていることを確認してください。
 - a. 「システムのプロパティ」ウィンドウで、「ドライバの署名」をクリックします。
 - b. 現行の設定をメモし、「無視」をクリックした後、「OK」をクリックします。
5. 「デバイス マネージャ」をクリックします。
6. 『インストールまたは更新したいアダプターを選択する』。

インストールまたは更新したいアダプターを選択する

統合 xSeries サーバー内の LAN ドライバーまたはポート、または仮想イーサネットの LAN ドライバーまたはポートのインストールまたは更新 (『LAN ドライバーのインストールまたは更新を開始する』を参照) を開始するためのステップを完了した後、アダプターを選択する必要があります。

インストールまたは更新したいアダプターを選択するためには、次のステップを行ってください。

1. 「デバイス マネージャ」ウィンドウで、「ネットワーク アダプタ」を開きます。
2. 「ネットワーク アダプタ」内で更新したいアダプターを右マウス・ボタン・クリックし、「プロパティ」を選択します。
3. アダプターの「プロパティ」ウィンドウで、「ドライバ」タブをクリックします。
4. 「ドライバの更新」または「ドライバのインストール」をクリックします (片方だけが表示されます)。
5. 「デバイス ドライバのアップグレード ウィザードの開始」ダイアログ・ボックスで、「次へ」をクリックします。
6. 『LAN ドライバーのインストールまたは更新を完了する』。

LAN ドライバーのインストールまたは更新を完了する

統合 xSeries サーバー内の LAN ドライバーまたはポート、または仮想イーサネットの場合に手動インストールまたは更新をするために必要な、最初の 2 つの作業を完了したことを確認してください。

- 261 ページの『LAN ドライバーのインストールまたは更新を開始する』。
- 261 ページの『インストールまたは更新したいアダプターを選択する』。

LAN ドライバーまたはポートのインストールまたは更新を完了するには、実際の状況に適合する以下の手順の 1 つを使用してください。

- Windows 2000 Server を使用している、または Windows Server 2003 の場合に特定のフォルダーから LAN ドライバーをインストールするように指図された。
- Windows Server 2003 を使用しており、特定の場所から LAN ドライバーをインストールするように指図されていない。

Windows 2000 Server を使用している、または **Windows Server 2003** の場合に特定のフォルダーから LAN ドライバーをインストールするように指図された場合。

LAN ドライバーのインストールまたは更新を完了するには、以下のステップを行ってください。

1. 「このデバイスの既知のドライバを表示して、その一覧から選択する」を選択して、「次へ」をクリックします。
2. 「ディスク使用」をクリックして、「フロッピー ディスクからインストール」ダイアログ・ボックスを開き、ドライバの場所を指定します。
 - 特定のドライブおよびフォルダーからドライバをインストールするように指図された場合には、「参照」をクリックし、場所を指定した後、「開く」をクリックします。
 - それ以外の時には、「参照」をクリックして、インストールまたは更新しようとするアダプターに対応するドライバのシステム・ドライブ (通常は C:) 上の場所を指定します。次のリストを使用して、特定のハードウェアのためのドライバを含むフォルダーを見つけてください。
 - ￥sv￥ibm ハードウェア・タイプ 2744 用
 - ￥sv￥alt ハードウェア・タイプ 2743 および 2760 用
 - ￥sv 仮想イーサネット用
 - ￥sv￥amd Windows 2000 のハードウェア・タイプ 2838
 - ￥windows￥inf Windows Server 2003 のハードウェア・タイプ 2723 および 2838 用
 - ￥sv￥itl Windows 2000 のハードウェア・タイプ 2892 用
 - ￥sv Windows Server 2003 のハードウェア・タイプ 2892 用
 - ￥sv￥alt Windows 2000 のハードウェア・タイプ 4812、5700、および 5701 用

- ¥wsv¥itg Windows Server 2003 のハードウェア・タイプ 4812、5700、および 5701 用

3. 「OK」をクリックします。
4. 「デバイス ドライバのアップグレード ウィザードの開始」ダイアログ・ボックスで、適切なドライバがまだ強調表示されていない場合には、リストから選択し、「次へ」をクリックします。
5. 「次へ」を再びクリックします。
6. 「ドライバの更新」手続きが完了した時にリターン・コード 22 がある場合には、アダプターが使用不可になっているかもしれません。この場合にアダプターを使用可能にするには、「デバイス マネージャ」ウィンドウで、使用不可になっているアダプターを右マウス・ボタン・クリックし、「有効」を選択します。
7. さらにアダプターをインストールまたは更新したい場合には、261 ページの『インストールまたは更新したいアダプターを選択する』を参照してください。

注: ドライバの更新の後に再起動が必要であるという指示を Windows がする場合は、更新するアダプターがもうなくなるまでそれを後回しにします。

8. インストールまたは更新 (261 ページの『LAN ドライバのインストールまたは更新を開始する』を参照) を開始した時に、ドライバの署名ポリシーを変更した場合は、元のポリシーに戻します。

Windows Server 2003 を使用しており、特定の場所から LAN ドライバをインストールするように指図されていない場合。

LAN ドライバのインストールまたは更新を完了するには、以下のステップを行ってください。

1. 「デバイスに最適なドライバを検索する」を選択して、「次へ」をクリックします。
2. 「次へ」をクリックして、互換性のあるハードウェアを表示させます。
3. 「検索場所のオプション」の選択をすべて解除し、「次へ」をクリックし、「次へ」を再びクリックします。
4. 「ドライバの更新」手続きが完了した時にリターン・コード 22 がある場合には、アダプターが使用不可になっているかもしれません。この場合にアダプターを使用可能にするには、「デバイス マネージャ」ウィンドウで、使用不可になっているアダプターを右マウス・ボタン・クリックし、「有効」を選択します。
5. さらにアダプターをインストールまたは更新したい場合には、261 ページの『インストールまたは更新したいアダプターを選択する』を参照してください。

注: ドライバの更新の後に再起動が必要であるという指示を Windows がする場合は、更新するアダプターがもうなくなるまでそれを後回しにします。

6. ドライバのインストールまたは更新 (261 ページの『LAN ドライバのインストールまたは更新を開始する』を参照) を開始した時に、ドライバの署名ポリシーを変更した場合は、元のポリシーに戻します。

Point-to-Point 仮想イーサネット IP アドレスの競合

IBM iSeries 統合サーバー・サポートは、統合サーバーの Point-to-Point イーサネット・ネットワークで、192.168.x.y の範囲の IP アドレスを使用します。デフォルトでは、実アドレスは i5/OS の Windows サーバーのインストール (INSWNTSVR) コマンドで選択されます。詳細と例は、265 ページの『Point-to-Point 仮想 IP アドレスの割り当て』を参照してください。ネットワークによっては、すでに使用中のアドレスと競合が起きる可能性があります。競合の可能性を避けるために、統合 xSeries サーバーか統合 xSeries アダプター付属の xSeries サーバーの VRTPTPPORT パラメーターを使用できます。

競合が起きた場合には、アドレスを変更しなければなりません。このとき、Point-to-Point 仮想イーサネットが i5/OS 上で固有のサブネットを占有していることを確認しなければなりません。使用されているサブネット・マスクは、255.255.255.0 です。Point-to-Point 仮想イーサネットが固有のサブネットにあることを確認するには、a.b.x.y の形式 (a.b.x は Point-to-Point 仮想イーサネットの両側で同じ値になります) の IP アドレスを使用します。また、値 a.b.x がご使用のネットワーク上で固有であることを検査します。

競合が原因で Point-to-Point 仮想イーサネット・アドレスを変更するには、以下のアクションを行ってください。

1. i5/OS コンソールで、DSPNWSN NWSN(name) OPTION (*PORTS) コマンドを入力します。ポート番号「*VRTETHPTP」に、付加されている回線をメモします。これは、回線記述とも呼ばれます。
2. TCP の構成 (CFGTCP) コマンドおよびオプション 1 を使用して、TCP インターフェースを表示します。ステップ 1 にある回線記述に関連する IP アドレスおよびサブネット・マスクをメモします。

注: Point-to-Point 仮想イーサネット用に Windows コンソールに入力された IP アドレスは、TCP/IPCFG パラメーターである *VRTETHPTP のために NWSN に設定された値を指定変更しません。

1. 「スタート」→「設定」→「コントロール パネル」→「ネットワークとダイヤルアップ接続」をクリックします。
2. Point-to-Point 仮想イーサネット のための「ローカル エリア接続」を右マウス・ボタン・クリックして、メニューから「プロパティ」を選択します。
3. インストールされているプロトコルから「TCP/IP プロトコル」を選択し、「プロパティ」ボタンを押して、TCP/IP のプロパティを表示します。
4. IP アドレスを、選択した新しい値に変更します。
5. 「OK」、次に「クローズ」をクリックして、アプリケーションをクローズします。
6. 統合 Windows サーバーをシャットダウンして、再始動しません。
7. i5/OS で、NWSN をオフに変更します。
8. ステップ 2 で記録した IP アドレスを使用して、TCP/IP インターフェースの除去 (RMVTCPIFC) コマンドを使用します。
9. TCP/IP インターフェースの追加 (ADDTCPIFC) コマンドを使用して、新しいインターフェースを追加します。Point-to-Point 仮想イーサネットの i5/OS 側で選択した IP アドレスを使用します。また、ステップ 1 およびステップ 2 で記録したサブネット・マスクおよび回線記述も入力する必要があります。
10. i5/OS コマンド行に CHGNWSN NWSN(name) と入力し、F4 を押します。
 - a. 「TCP/IP ポート構成」のラベルのあるセクションまでページを送ります。
 - b. ポート「*VRTETHPTP」の「インターネット・アドレス」フィールドの IP アドレスを、ステップ 3 で使用した値に変更します。変更を有効にするために Enter キーを押します。
 - c. NWSN をオンに変更します。

注: 複数のサーバーをインストールする場合、さらに競合が起きないようにするには、INSWNTSVR コマンドで IP アドレスを生成するのではなく、Point-to-Point 仮想イーサネットの IP アドレスを割り当ててください (265 ページの『Point-to-Point 仮想 IP アドレスの割り当て』を参照)。「仮想 PTP イーサネット・ポート」パラメーターを使用すると、システム上で固有であることが分かっている IP アドレスを入力できます。

Point-to-Point 仮想 IP アドレスの割り当て

デフォルトでは、Windows サーバーのインストール (INSWNTSVR) コマンドは、192.168.x.y の形式の Point-to-Point 仮想イーサネット IP アドレスを割り当てます。起きる可能性のある競合を防止するには、このコマンドで VRTPTPPORT パラメーターを使用して、システム上で固有であることが分かっている IP アドレスを割り当てます。

このコマンドにアドレスを割り当てさせて競合が検出された場合は、IP アドレスを変更できます。IXS および IXA 接続の統合サーバーの場合、このコマンドは、統合 xSeries サーバーのリソース番号に基づいた値を x に割り当てます。コマンドは、その i5/OS で使用されていない値 y と y+1 (y=1 から始まる) の組のアドレスを探します。コマンドは、Point-to-Point 仮想イーサネットの i5/OS 側に小さいほうの番号を、Windows サーバー側に大きいほうの番号を割り当てます。



たとえば、LIN03 というリソース名の 2892 統合 xSeries サーバーがあるとします。Windows Server のインストール (INSWNTSVR) コマンドを実行した後は、Point-to-Point 仮想イーサネットで以下のアドレスを使用して終了しなければなりません。

192.168.3.1 (i5/OS 側)
192.168.3.2 (Windows サーバー側)

インストールしたサーバー上で競合が発生する場合には、特定の置換値 (例、192.168.17) がご使用のネットワークで使用されていないことを確認し、IP アドレスをその値に変更します。

192.168.17.1 (i5/OS 側)
192.168.17.2 (Windows サーバー側)

TCPPORTCFG パラメーター *VRTETHPTP ポートの NWSD で設定された値を、Point-to-Point 仮想イーサネットの Windows コンソールに入力された IP アドレスがオーバーライドすることに注意してください。

問題が続く場合には、 IBM iSeries サポート Web ページ (英語)  の技術情報データベースをチェックしてください。それでも解決しない場合には、テクニカル・サポート・プロバイダーに連絡してください。問題が続く場合には、IBM に連絡してサポートを要請してください。

仮想イーサネット上の TCP/IP の問題

Point-to-Point 仮想イーサネットの TCP/IP 構成が正しいかどうか確認します。i5/OS TCP/IP 構成が新規であるか、または変更された場合、以下の手順を実行して、Windows の TCP/IP 構成が正しいかどうかを確認してください。

1. 「スタート」 → 「コントロール パネル」 → 「ネットワーク接続」または「スタート」 → 「設定」 → 「ネットワークとダイヤルアップ接続」とクリックします。
2. 「ネットワーク接続」または「ネットワークとダイヤルアップ接続」を右クリックしてポップアップメニューを表示し、「開く」を選択します。
3. 「IBM iSeries 仮想イーサネット Point-to-Point 接続 (IBM iSeries Virtual Ethernet point to point Connection)」をダブルクリックします。
4. 「プロパティ」ボタンをクリックします。
5. 「インターネット・プロトコル (TCP/IP)」を選択します。
6. 「プロパティ」ボタンをクリックします。「次の IP アドレスを使う」を選択し、i5/OS コンソールにその IP アドレスが表示される場合、ここから先のステップは行う必要はありません。「IP アドレスの自動取得 (Obtain an IP address automatically)」を選択した場合、次のステップに進みます。
7. ラジオ・ボタン「次の IP アドレスを使う」を選択します。

8. i5/OS コマンド行で DSPNWSN NWSD(nwsd) OPTION(*TCPIP) というコマンドを入力します。 nwsd は、ご使用のサーバーの NWSD です。次に Enter キーを押します。
 - DSPNWSN ダイアログ・ボックスで *VRTETHPTP という名前のポートを見つけ出します。これに、Point-to-Point 仮想イーサネット の IP アドレスとサブネット・マスク値が示されています。
 - 統合サーバー・コンソールに、DSPNWSN コマンドで示された Point-to-Point 仮想イーサネットの IP アドレスとサブネット・マスク値を入力します。
9. 「OK」をクリックします。
10. 「OK」をクリックします。
11. 「閉じる」をクリックします。

i5/OS および Windows での TCP/IP 構成の確認については、126 ページの『Point-to-Point 仮想イーサネット・ネットワークについて』を参照してください。

それぞれのアクティブ・サーバーによって使用される Point-to-Point 仮想イーサネットは、別個の IP サブネットを使用しなければなりません。サブネットの要件の詳細、および TCP/IP 構成を変更する方法については、263 ページの『Point-to-Point 仮想イーサネット IP アドレスの競合』を参照してください。

iSeries 仮想イーサネット・アダプターが正しく構成されているかどうか、また機能しているかどうかを確認します。

仮想イーサネット・アダプターのトラブルシューティングについては、以下のいずれかのトピックを参照してください。

- 254 ページの『iSCSI 接続のサーバーの仮想イーサネットの問題』。
- 257 ページの『IXS および IXA 接続のサーバーの仮想イーサネットの問題』

仮想イーサネット・アダプターの回線記述が正しく構成されていることを確認するには、123 ページの『第 6 章 仮想イーサネットおよび外部ネットワークの管理』を参照してください。

ファイアウォールが干渉していないことを確認します。

ファイアウォール (たとえば Windows で実行されているソフトウェア・ファイアウォールなど) が関係している場合、必要なトラフィックを許容するようにそれを構成する必要があります。

- IBM iSeries 仮想イーサネット Point-to-Point 接続の IP アドレスについては、統合サーバー管理アプリケーションの失敗を防止するために、TCP 動的ポートを許可します。ネットワーク・アドレス変換 (NAT) は使用しないでください。
- IBM iSeries 仮想イーサネット接続の IP アドレスについては、アプリケーションに必要なプロトコルおよびポートを許可します。
- iSCSI HBA 接続の IP アドレス については、145 ページの『ファイアウォールの構成』を参照してください。

QNTC ファイル・システムによる Windows Server 2003 共用へのアクセス時の問題

i5/OS QNTC ファイル・システムを使用して、Active Directory がインストールされている Windows Server 2003 サーバー上の共用にアクセスできない場合 (たとえば、ドメイン制御装置である場合)、さらに別のセットアップ作業を行わなければならない可能性があります。116 ページの『Windows Server 2003 Active Directory Server を使用して Kerberos を使用可能にする』を参照してください。

IFS アクセスの問題

iSeries NetServer を介して統合 Windows サーバーから i5/OS 統合ファイル・システム (IFS) にアクセスしようとする、以下の状況でアクセスが失敗する可能性があります。

- 汎用命名規則 (UNC) 名を IP アドレス付きで使用しており、
- Point-to-Point 仮想イーサネットおよび外部 LAN の両方のパスが、統合 Windows サーバーと i5/OS との間

に存在する
UNC 名を変更して代わりに iSeries NetServer 名を使用するようにするか、または外部 LAN パスを使用不可にしてから失敗した操作を再試行してください。

統合 Windows サーバー・ファイルの保管の問題

統合サーバー・ファイルのファイル・レベルのバックアップを行うことに問題がある場合は、Windows イベント・ログとメッセージの i5/OS QSYSOPR メッセージ待ち行列をチェックしてください。

- ファイルを保管しようとするときに、セッション初期化エラー (CPDB050) またはセッション通信エラー (CPDB055) が起こる場合は、次のようにしてください。
 1. ファイルを保管したいと思っている統合サーバーと同じドメイン (218 ページの『iSeries NetServer と統合 Windows サーバーを同じドメインに置く』を参照) に i5/OS NetServer があるようにしてください。
 2. 217 ページの『統合 Windows サーバーでの共有の作成』と 217 ページの『QAZLCSAVL ファイルへのメンバーの追加』のステップを完了したことを確認してください。
 3. QSERVER サブシステムが実行されていることを確認してください。
 4. TCP/IP が活動状態になっていることを確認してください。
 - a. CFGTCP コマンドのオプション 1 を使用します。
 - b. 「F11」を押してインターフェースの状況を表示します。
 - c. 適切なネットワーク・サービスのとなり 9 を入力して、TCP/IP インターフェースを開始します。
 - d. 「F5」を押して画面を最新表示します。適切な TCP/IP サービスがアクティブになっているはず です。
 5. その後、ファイルの保管を再度試みてください。
- セキュリティ情報の交換に問題があることを示すエラー・メッセージ (CPDB053)、またはサーバーへのログオンに問題があることを示すエラー・メッセージ (NTA02AE) を受け取る場合は、次のようにしてください。
 1. Administrators グループの一部として自分が統合サーバーに登録されていることを確認してください。
 2. i5/OS と統合サーバーで同じパスワードがあることを確認してください。
 3. その後、ファイルの保管を再度試みてください。
- 共有ファイル・メンバーの処理に問題があることを示すエラー・メッセージ (CPDB058) を受け取る場合は、QAZLCSAVL ファイルが正しく設定されていることを確認してください。
 1. 217 ページの『統合 Windows サーバーでの共有の作成』のステップを完了したことを確認してください。
 2. 217 ページの『QAZLCSAVL ファイルへのメンバーの追加』のステップを完了したことも確認してください。保管 (SAV) コマンドで指定した共有をそのファイル内にリストしたことを確認してください。

- NTSAV での通信に問題があることを示すエラー・メッセージ (NTA02A3) を受け取る場合は、リモート・プロシージャー呼び出しが実行されていることを確認してください。
 1. 統合サーバーのタスクバーで、「スタート」→「プログラム」→「管理ツール」をオープンします。
 2. 「サービス」をダブルクリックします。
 3. リモート・コマンド・サービスが実行されていることを確認します。
- SAV を実行すると、以下のエラーが表示される場合があります。
 - CPFA09C Not authorized to object
 - CPD3730 Cannot save directory /qntc/(server)/(share)/System Volume Information

これらのエラーは、**System Volume Information** ディレクトリーが保管されなかったことを示します。これは隠しシステム・ディレクトリーであり、Windows SYSTEM アカウントによってのみアクセスできます。このメッセージを無視すると、ディレクトリーとその内容は保管されません (ここには、ファイル暗号化時に使用する中間ログ・ファイルが置かれます)。無視しなければ、SAV を実行しているユーザーへの許可をこのディレクトリーに追加できます。許可を設定するには、ディレクトリーを見える状態にしておく必要があります (つまり、隠しファイルを隠さず、プロテクトされたオペレーティング・システム・ファイルを隠さない)。フォルダー許可の設定についての詳細は、Windows 2000 Server または Windows Server 2003 のヘルプを参照してください。



さらに、ファイル・レベルでのバックアップを QSECOFR として実行した場合には、QSECOFR がサーバーに登録されていなくても、CPFA09C エラーも発生するかもしれません。統合サーバーにバックアップされた、別の登録済みユーザー・プロファイルを使用してください。

サーバー・メッセージ待ち行列の判読不能メッセージ

メッセージ待ち行列コード化文字セット ID (CCSID) が *HEX (65535) に設定されている場合には、Windows イベント・ログ・メッセージは正しく表示されません。サーバー・メッセージ待ち行列に判読不能メッセージ (NWSO の MSGQ パラメーターで識別される) があった場合には、以下のアクションを実行してください。

1. i5/OS コンソールでコマンド CHGMSGQ を入力して、サーバー・メッセージ待ち行列 CCSID を *HEX (65535) 以外のもの、たとえば *MSG に変更します。

たとえば、ライブラリー MYLIB でメッセージ待ち行列名が MYSVRQ の場合には、i5/OS 上で以下のコマンドを使用して、メッセージ待ち行列 CCSID を変更します。CHGMSGQ MSGQ(MYLIB/MYSVRQ) CCSID(*MSG)

2. 問題が続く場合には、 [@server IBM iSeries サポート Web ページ \(英語\)](#)  の技術情報データベースをチェックしてください。それでも解決しない場合には、テクニカル・サポート・プロバイダーに連絡してください。

Windows システム・メモリー・ダンプを取る際の問題

システム・ドライブで十分なスペースがある場合には、統合 Windows サーバーは自動的に構成され、STOP エラーまたはブルー・スクリーンが表示される場合には、システム・メモリー・ダンプを収集することができます。システム・メモリー・ダンプが収集されない場合には、以下のことを行ってください。



1. 「スタート」、「プログラム」、「管理ツール」を選択します。
2. 「コンピュータの管理」をクリックします。
3. 「操作」メニューの中で、「プロパティ」をクリックします。

4. 「詳細」タブを選択します。
5. 「起動/回復」ボタンをクリックします。
6. 「デバッグ情報を次へ書き込む:」ボックスをチェックします。ブルー・スクリーンが表示される場合に作成される memory.dmp ファイルへのデフォルト・パスは %SystemRoot% であり、これは Windows 2000 Server では C:\WINNT、Windows Server 2003 では C:\WINDOWS です。

システム・メモリー・ダンプの取得を妨げる他の問題として、以下のものが含まれます。

- 指定されているページング・ファイルのサイズが十分ではありません。ページング・ファイルのサイズは、すべての物理 RAM に 12 MB を加えた量を保持できるだけの大きさになければなりません。ご使用のマシンで物理 RAM の量を確認するには、以下のことを実行してください。
 1. 「スタート」、「設定」、「コントロール パネル」の順に選択します。
 2. 「システム」をダブルクリックします。「一般」ページの「コンピュータ」にリストされている値は、ご使用のシステムにある物理 RAM の量を示しています。

ページング・ファイルのサイズを確認または変更するには、以下のことを実行してください。

1. 「詳細」タブを選択し、「仮想メモリ」セクションの「パフォーマンス オプション」ボタンをクリックします。ウィンドウの「仮想メモリ」部分には、現在のページング・ファイル・サイズが示されています。
 2. ページング・ファイルのサイズを変更する必要がある場合、「変更」ボタンをクリックします。
- ページング・ファイルは、システム・ドライブ上にはありません。ページング・ファイルがシステム・ドライブにないと、システム・メモリー・ダンプは収集されません。システム・ドライブは C: ドライブです。これを確認または変更するには、以下のことを実行してください。
 1. 「詳細」タブを選択し、「仮想メモリ」セクションの「パフォーマンス オプション」ボタンをクリックします。
 - memory.dmp ファイルのパスとして指定したドライブでは、スペースが十分に使用できません。memory.dmp ファイルのデフォルト・パスはシステム・ドライブですが、これを他のドライブに変更することができます。システム・ドライブまたは変更した場合にはそのドライブに、十分なフリー・スペースがあることを確認してください。必要なフリー・スペースは、物理 RAM に 12 MB を足したサイズです。
 - 問題が続く場合には、 IBM iSeries サポート Web ページ (英語)  の技術情報データベースをチェックしてください。それでも解決しない場合には、テクニカル・サポート・プロバイダーに連絡してください。

統合 Windows サーバーの再インストール

統合 Windows サーバーが損傷を受けている場合、それを再インストールすることによって、インストールしてあるアプリケーションおよびユーザー・データを保護できます。NT ロードャー (NTLDR) の「ブート」メニューを使って、ログオンするか、DOS で始動することは可能です。(ただし、ブート・ドライブが FAT としてフォーマットされたままでなければなりません。) その後、Windows サーバーを再インストールすることができます。これによってシステムは、元々インストールされていた Windows サーバーのベース・レベル・コードに戻ります。次に、インストールした何らかの Microsoft サービス・パックを再適用する必要があります。最新の IBM iSeries 統合サーバー・サポートのサービス・パックを再インストールする必要もあります。

Windows サーバーを再インストールするには、以下のようにします。

1. 統合サーバーを停止します。163 ページの『統合サーバーの開始と停止』を参照してください。

2. ブート・メニューで、PC-DOS または Windows サーバー (機能しているもの) のブートを選択します。
3. Windows サーバーを選択した場合には、MS-DOS ウィンドウをオープンします。
- 4.

- Windows 2000 の場合、`winnt /s:D:\i386 /u:D:\unattend.txt` と入力します。
- Windows Server 2003 の場合、`winnt /b /t:C: /s:D:\i386 /u:D:\unattend.txt` と入力します。

5. DOS ウィンドウで、次のように入力します。

```
D:
cd \i386
winnt /s:D:\i386 /u:D:\unattend.txt
```

6. Enter キーを押します。

注: ネットワーク・ドライブが損傷を受けて、統合 Windows サーバーにログオンすることも、DOS から始動することもできない場合があります。この場合、使用可能なバックアップから、事前定義およびユーザー定義された記憶域をすべて復元します。211 ページの『統合 Windows サーバー用事前定義ディスク・ドライブのバックアップ』および212 ページの『統合 Windows サーバー用ユーザー定義ディスク・ドライブのバックアップ』を参照してください。

また、Windows 2000 Server および Windows Server 2003 には、Windows Recovery Console があります。これは、システムへのアクセスを限定して、さまざまな管理作業を実行したり、システムを修理したりするためのコマンド行コンソールです。詳細は、Windows 2000 Server または Windows Server 2003 の資料を参照してください。

さらに、100 ページの『i5/OS コンソールからのインストールの開始』の手順に従って、最初から再インストールする必要もあります。

統合 Windows サーバーのサービス・データの収集

サポート担当者へサービス・データを渡す必要がある場合、まず、i5/OS ログ (230 ページの『メッセージ・ログとジョブ・ログのチェック』を参照) および Windows イベント・ログを調べます。また、i5/OS で Windows イベント・ログのコピーも作成し (167 ページの『メッセージ・ログ』を参照)、リモート・トラブルシューティングの Windows サーバー・ダンプを作成することもできます。これらのトピックは、詳細な診断情報を集めるためのダンプを作成する際に役立ちます。

1. 『i5/OS での統合 Windows サーバーのメモリー・ダンプの作成』。
2. このダンプからまずどの構成ファイルおよびログ・ファイルを参照するべきかを知るには、271 ページの『i5/OS でのネットワーク・サーバー記述 (NWSD) ダンプ・ツールの使用』を参照してください。

i5/OS での統合 Windows サーバーのメモリー・ダンプの作成

統合サーバーで生じる問題の解決に役立てるために、i5/OS 上で Windows メモリー・ダンプ・ファイルを作成することができます。iSeries Windows サーバーをインストールすると、デフォルトでダンプはシステム・ドライブに入ります。

- %SystemRoot%\Memory.Dmp (Windows Server 2003 の場合)。
- %SystemRoot%\Memory.Dmp (Windows 2000 Server の場合)。

注: Windows で全メモリー・ダンプの作成を正常に完了するには、ページ・ファイルは、システム・ドライブ上に置かれていて、しかも少なくともメモリー・サイズに 12 メガバイトを加えたサイズに等しくなければなりません。メモリー内容は、ダンプ中にページ・ファイルに書き込まれます。これは、メモリー・ダンプ・プロセスの最初のステップです。2 番目のステップでは、ページ・ファイルのデータが実際のダンプ・ファイルに書き込まれます。このステップは、ダンプ後のシステ

ムのブート時に行われます。メモリー・ダンプ・ファイル (デフォルトでは memory.dmp) を収容するドライブには、インストール済みメモリーと同じ大きさのフリー・スペースがなければなりません。

システム・ドライブにファイルをページングするためのスペースが十分にある場合には、デフォルトでメモリー・ダンプが使用可能になります。メモリー・ダンプ・サポートが使用可能になっていることを検査したり、memory.dmp ファイルを異なるドライブに書き込んだりするには、次のステップを行います。

1. 「スタート」、「設定」、「コントロール パネル」の順に選択します。
2. 「システム」アプリケーションをオープンします。
 - 「詳細」タブ、「起動/回復」ボタンの順にクリックします。
3. 「デバッグ情報を次へ書き込む」チェック・ボックスをクリックします。
4. 必要なら、ダンプ・ファイルの位置を変更します。
5. カーネル停止エラーが起きるたびにシステムがファイルを上書きするようにしたい場合には、「既存のファイルに上書きする」チェック・ボックスをクリックしてオンにします。
6. ページ・ファイルのサイズと、システム・ドライブで使用可能なフリー・スペースの大きさに基づき、適切なタイプのメモリー・ダンプを選択します (小規模メモリー・ダンプ、カーネル・メモリー・ダンプ、完全メモリー・ダンプ)。
7. 「OK」をクリックします。

i5/OS でのネットワーク・サーバー記述 (NWS D) ダンプ・ツールの使用

ネットワーク・サーバー記述 (NWS D) のダンプ・ツール (QFPDMPLS) を使用して、ご使用の統合 Windows サーバーで使用される、それぞれの構成ファイルおよびログ・ファイルをダンプできます。これを実行するには、*ALLOBJ 特殊権限が必要です。

それには、次のステップを行います。

1. NWS D をオフに変更します (163 ページの『統合サーバーの開始と停止』を参照)。
2. i5/OS コマンド行に、次のように入力します。

```
CALL QFPDMPLS PARM(nwsdname)
```

nwsdname はネットワーク・サーバー記述名です。

プログラムは、複数のメンバーを使用してデータベース・ファイル QGPL/QFPNWS DMP を作成します。それぞれのデータベース・ファイル・メンバー名は、NWS D 名とそれに続く 2 桁の数字 (01 以上 99 以下) で構成されます。たとえば、MYSERVER という名前の NWS D の場合には、最初のメンバー名は MYSERVER01 です。

3. メンバーを表示して、サーバー記述に関連する異なるファイルの内容を調べてください。問題を引き起こしているインストール・ステップに応じて、問題の分析には異なるファイルが重要になります。
4. 以下の表を参照して、特定のインストール・ステップでのそれぞれのファイルの重要性に注意してください。ファイルに 1 とマークされている場合には、問題分析においてそれを最初に参照し、2 は 2 番目に、3 は最後に参照します。マークされていないファイルはインストールに関係していませんが、別の場合に関係してくることもあります。メンバーによっては、インストール後の段階で作成されるものもあります。

注: ドライブを NTFS に変換する場合は、QFPDMPLS を使用してシステム・ドライブでファイルを検索することはできません。

あるサーバーでは、以下にリストされているすべてのファイルを見つけれないかもしれません。特定のファイルが見つからない場合には、そのファイルは QFPDMPLS API により検索されず、対応するデータベース・メンバーは作成されません。

NWSD 構成ファイルおよびログ・ファイル

メンバー名	データタイプ	ファイル名	Windows ディレクトリー	インストール	インストール後
nwsdname01	Txt	CONFIG.SYS	C:¥	3	3
nwsdname02	Txt	AUTOEXEC.BAT	C:¥	2	2
nwsdname03	Txt	BOOT.INI	C:¥		
nwsdname04	Txt	HOSTS	C:¥ または D:¥		3
nwsdname05	Txt	QVNI.CFG	C:¥ または D:¥		
nwsdname06	Txt	QVNACFG.TXT	C:¥ または D:¥		
nwsdname07	Txt	QVNADAEM.LOG	C:¥ または D:¥		
nwsdname08	Txt	DUMPFIL.E01	C:¥		
nwsdname09	Bin	DUMPFIL.E01	C:¥		
nwsdname10	Txt	DUMPFIL.E02	C:¥		
nwsdname11	Bin	DUMPFIL.E02	C:¥		
nwsdname12	Txt	UNATTEND.TXT	D:¥	1	
nwsdname13	Txt	INSWNTSV.LNG	D:¥	2	
nwsdname14	Txt	INSWNTSV.VER	D:¥	2	
nwsdname15	Txt	QVNADAEM.LOG	D:¥		
nwsdname16	Txt	QVNARCMD.LOG	D:¥		
nwsdname17	Txt	QVNDT400.LOG	D:¥		
nwsdname18	Txt	QVNDVSTP.LOG	D:¥		
nwsdname19	Txt	QVNDVSCD.LOG	D:¥		
nwsdname20	Txt	QVNDVSDD.LOG	D:¥		
nwsdname21	Txt	EVENTSYS.TXT	D:¥		
nwsdname22	Txt	EVENTSEC.TXT	D:¥		
nwsdname23	Txt	EVENTAPP.TXT	D:¥		
nwsdname24	Txt	PERFDATA.TSV	D:¥		
nwsdname25	Txt	REGSERV.TXT	D:¥		
nwsdname26	Txt	REGIBM.TXT	D:¥		
nwsdname27	Txt	REGIBMCO.TXT	D:¥		
nwsdname28	Txt	DUMPFIL.D01	D:¥		
nwsdname29	Bin	DUMPFIL.D01	D:¥		
nwsdname30	Txt	DUMPFIL.D02	D:¥		
nwsdname31	Bin	DUMPFIL.D02	D:¥		
nwsdname32	Txt	HOSTS	%SystemRoot%\¥SYSTEM32¥DRIVERS¥ETC		3
nwsdname33	Txt	LMHOSTS	%SystemRoot%\¥SYSTEM32¥DRIVERS¥ETC		3
nwsdname34	Bin	MEMORY.DMP	C:¥WINNT		
nwsdname35	Txt	VRMFLOG.TXT	E:¥PROGRA~1¥IBM¥AS400NT¥SERVICE¥VRM		
nwsdname36	Txt	PTFLOG.TXT	E:¥PROGRA~1¥IBM¥AS400NT¥SERVICE¥PTF		
nwsdname37	Txt	PTFUNIN.TXT	E:¥PROGRA~1¥IBM¥AS400NT¥SERVICE¥PTF		
nwsdname38	Txt	A4EXCEPT.LOG	D:¥		
nwsdname39	Txt	DUMPFIL.E01	E:¥		
nwsdname40	Bin	DUMPFIL.E01	E:¥		
nwsdname41	Txt	DUMPFIL.E02	E:¥		
nwsdname42	Bin	DUMPFIL.E02	E:¥		
nwsdname43	Txt	CMDLINES.TXT	D:¥I386¥\$OEM\$	2	
nwsdname44	Txt	QVNABKUP.LOG	D:¥AS400NT		
nwsdname45	Txt	QVNADAEM.LOG	D:¥AS400NT		

メンバー名	データ タイプ	ファイル名	Windows ディレクトリー	インストール	インストール 後
nwsdname46	Txt	QCONVGRP.LOG	D:\AS400NT		
nwsdname47	Txt	SETUPACT.LOG	C:\WINNT	1	
nwsdname48	Txt	SETUPAPI.LOG	C:\WINNT	1	
nwsdname49	Txt	SETUPERR.LOG	C:\WINNT	1	
nwsdname50	Txt	SETUPLOG.TXT	C:\WINNT	1	
nwsdname51	Txt	VRMFLOG.TXT	D:\AS400NT		
nwsdname52	Txt	PTFLOG.TXT	D:\AS400NT		
nwsdname53	Txt	PTFUNIN.TXT	D:\AS400NT		
nwsdname54	Txt	VRMLOG.TXT	%SystemRoot%\AS400WSV\SERVICE\VRM		
nwsdname55	Txt	PTFLOG.TXT	%SystemRoot%\AS400WSV\SERVICE\SERVPACK		
nwsdname56	Txt	PTFUNIN.TXT	%SystemRoot%\AS400WSV\SERVICE\SERVPACK		
nwsdname57	Txt	QVNDVEU.LOG	D:\AS400NT		
nwsdname58	Txt	SERVICE.LOG	D:\AS400NT		
nwsdname59	Txt	LVDELOEM.LOG	D:\AS400NT		
nwsdname60	Txt	INVOKINF.LOG	D:\AS400NT		
nwsdname61	Txt	LVMMASTER.LOG	D:\AS400NT		
nwsdname62	Txt	QITDINST.LOG	D:\AS400NT		
nwsdname63	Txt	QVNDVIMR.LOG	D:\AS400NT		
nwsdname64	Txt	QVNDVIMC.LOG	D:\AS400NT		
nwsdname65	Txt	QVNDSDMR.LOG	D:\AS400NT		
nwsdname66	Txt	QVNDSDMC.LOG	D:\AS400NT		
nwsdname67	Txt	QVNILMGR.LOG	D:\AS400NT		

第 15 章 ネットワーク・サーバー記述構成ファイル

独自の構成ファイルを作成すれば、統合 Windows サーバーをカスタマイズすることができます。たとえば、画面の解像度を変更したり、IPX プロトコルのインストールを抑制したりできます。これを行うには、以下のステップを実行してください。

1. NWSD 構成ファイルを作成します。 73 ページの『ネットワーク・サーバー記述』を参照してください。
2. サーバーをインストールしたり、ネットワーク・サーバー記述を作成または変更したりする際に、構成ファイル・パラメーターを使用してこのファイルを指定します。

ネットワーク・サーバーを始動するたびに、i5/OS は、構成ファイルを使用して、指定された統合サーバー・ファイルをサーバーの C、または D ドライブで変更します。

Windows サーバー導入 (INSWNTSVR) コマンドが統合サーバーを活動化すると、Windows 不在インストール・セットアップ・スクリプト・ファイル (UNATTEND.TXT) が生成されます。INSWNTSVR コマンドで構成ファイルを指定すると、このファイルをインストール時に使用して UNATTEND.TXT ファイルを変更できます。

重要: 構成ファイルを変更する際には、十分に注意してください。たとえば、UNATTEND.TXT からデバイス・ドライバーを除去したり、OEM セクションや TCP をインストールするセクションを変更したりしないでください。そうでないと、変更が原因でサーバーが正常に始動しなくなる可能性があります。インストール済みのサーバーを変更するための構成ファイルを作成している場合には、変更するファイルのバックアップ・コピーを最初に作成してください。

- システム・ドライブの形式を知るには、ネットワーク・サーバー記憶域の処理 (WRKNWSSTG) コマンドを使用することができます。
- 構成ファイルを作成する前に、『NWSD 構成ファイル形式』をお読みください。このセクションでは、それぞれの項目タイプの使用方法を説明します。
- また、287 ページの『キーワード値に対する置換変数の使用』のトピックで、使用できる変数や、リストを作成する方法について調べてください。
- また、277 ページの『例: NWSD 構成ファイル』も参照してください。
- これで、276 ページの『NWSD 構成ファイルの作成』の手順を実行する用意ができました。

構成ファイルを作成した後でサーバーを始動するのに問題が発生する場合には、242 ページの『NWSD 構成ファイルのエラー』を参照してください。

NWSD 構成ファイル形式

NWSD 構成ファイルは、それぞれ機能が異なる複数の項目タイプのオカレンスで構成されています。項目タイプは以下のとおりです。

277 ページの『CLEARCONFIG 項目タイプによる既存の統合サーバー・ファイルからの行の削除』
統合サーバー・ファイルからすべての行を除去するには、この項目タイプを使用します。

278 ページの『ADDCONFIG 項目タイプによる統合サーバー・ファイルの変更』
統合サーバー・ファイルで行を追加、置換、または除去するには、この項目タイプを使用します。

283 ページの『UPDATECONFIG 項目タイプによる統合 Windows サーバー・ファイルの変更』

統合サーバー・ファイルで行内のストリングを追加または除去するには、この項目タイプを使用します。

284 ページの『SETDEFAULTS 項目タイプによる構成デフォルトの設定』

特定のキーワードのデフォルト値を設定するには、この項目タイプを使用します。 i5/OS uses the defaults only when processing ADDCONFIG and UPDATECONFIG entries in the current file member.

項目タイプのオカレンスのことを項目といいます。それぞれの項目には一連のキーワードがあり、等号 (=) とそれらのキーワードの値が後に続きます。

形式のガイドライン

- ソース物理ファイル・レコード長は、92 バイトでなければなりません。
- 1 行には、1 つの項目しか入れられません。ただし、1 つの項目を複数の行にすることができます。
- 項目タイプと等号の間、等号の前後、およびコンマの後にはブランク・スペースを入れることができます。
- 項目の間およびキーワードの間にはブランク行を入れることができます。

キーワード

- 入力キーワードは、任意の順序で入力できます。
- 項目内の最後のキーワード以外のすべてのキーワード値の後には、コンマを使用します。
- キーワード値にコンマ、ブランク・スペース、アスタリスク、等号、または単一引用符が入っている場合は、そのキーワード値を単一引用符で囲んでください。
- 単一引用符の入ったキーワード値を使用する場合には、値の中の引用符であることを示すために引用符を 2 つ使用してください。
- キーワード値ストリングは、最大で 1024 文字にすることができます。
- キーワード値は、複数の行にまたがって入力できますが、その場合は単一引用符で囲まなければなりません。値には、各行の先頭および末尾ブランクも含まれます。

注記

- 注記はアスタリスク (*) で始まります。
- 注記は、単独の行にすることも、注記でない他のテキストと合わせて行にすることもできます。

NWSD 構成ファイルの作成

構成ファイルを作成する前に、275 ページの『NWSD 構成ファイル形式』および 287 ページの『キーワード値に対する置換変数の使用』のトピックをお読みください。また、277 ページの『例: NWSD 構成ファイル』も参照してください。

NWSD 構成ファイルを作成するには、以下のようにします。

1. ソース物理ファイルを作成します。
 - a. i5/OS コマンド行で、CRTSRCPF と入力し F4 を押します。
 - b. ファイルの名前、説明テキスト、およびメンバー名を入力して Enter キーを押し、ファイルを作成します。

2. 使用可能なエディターを使用して、構文的に正しい項目を NWSD に適合するファイルに追加します。275 ページの『NWSD 構成ファイル形式』を参照してください。たとえば、PDM によるメンバーの処理 (WRKMBRPDM) コマンドを使用できます。
 - a. i5/OS コマンド行で、WRKMBRPDM file(*yourfilename*) mbr(*mbrname*) と入力し、Enter キーを押します。
 - b. 編集するファイルの横に 2 と入力します。

例: NWSD 構成ファイル

この構成ファイル例は以下の作業を行います。

- デフォルト・ファイル・パスを設定する
- 時間帯を削除し、構成変数によって追加し直す
- 表示構成行が UserData セクションの前に追加されるようにデフォルト検索値を設定する
- 表示を構成する行を追加する

```

+-----+
| ***** Beginning of data ***** |
| ***** |
| * Update D:¥UNATTEND.TXT |
| ***** |
| * |
| ===== |
| * Set default directory and file name values. |
| ===== |
| SETDEFAULTS TARGETDIR = 'D:¥', TARGETFILE = 'UNATTEND.TXT' |
| * |
| ===== |
| * Delete and use a substitution variable to re-add TimeZone line. |
| ===== |
| ADDCONFIG VAR      = 'TimeZone', ADDWHEN = 'NEVER', DELETEWHEN = 'ALWAYS' |
| ADDCONFIG ADDSTR   = 'TimeZone="%TIMEZONE%"', |
| FILESEARCHSTR     = '%FPA_L_BRACKET%GuiUnattended%FPA_R_BRACKET%' |
| * |
| * Add lines to configure the display. |
| ===== |
| * Set default search values to add new statements to the file |
| * before the UserData section header line. |
| SETDEFAULTS FILESEARCHSTR = '%FPA_L_BRACKET%UserData%FPA_R_BRACKET%', |
| FILESEARCHPOS = 'BEFORE' |
| * |
| * Add the display statements to the file. |
| ADDCONFIG ADDSTR = '%FPA_L_BRACKET%Display%FPA_R_BRACKET%', |
| UNIQUE = 'YES' |
| ADDCONFIG ADDSTR = 'ConfigureAtLogon = 0', UNIQUE = 'YES' |
| ADDCONFIG ADDSTR = 'BitsPerPel = 16', UNIQUE = 'YES' |
| ADDCONFIG ADDSTR = 'XResolution = 640', UNIQUE = 'YES' |
| ADDCONFIG ADDSTR = 'YResolution = 480', UNIQUE = 'YES' |
| ADDCONFIG ADDSTR = 'VRefresh = 60', UNIQUE = 'YES' |
| ADDCONFIG ADDSTR = 'AutoConfirm = 1', UNIQUE = 'YES' |
| * |
+-----+

```

CLEARCONFIG 項目タイプによる既存の統合サーバー・ファイルからの行の削除

CLEARCONFIG 項目タイプを使用すると、既存の統合サーバー・ファイルからすべての行を除去できます。

重要: 統合サーバー・ファイルからすべての行を除去すると、ネットワーク・サーバーをオンに変更できなくなる可能性があります。問題がある場合、242 ページの『NWS D 構成ファイルのエラー』を参照してください。

統合サーバー・ファイルをクリアするには、以下のような CLEARCONFIG 項目タイプの入った NWS D 構成ファイルを作成します。

```
CLEARCONFIG
LINECOMMENT = '<"REM "|<comment_string>>', (オプション)
TARGETDIR   = '<BOOT|path>', (オプション)
TARGETFILE  = '<file_name>' (必須)
```

CLEARCONFIG キーワードの詳細については、以下のキーワード・リンクを使用してください。275 ページの『NWS D 構成ファイル形式』または『ADDCONFIG 項目タイプによる統合サーバー・ファイルの変更』に戻ることができます。

- 281 ページの『LINECOMMENT キーワード』
- 『TARGETDIR キーワード』
- 『TARGETFILE キーワード』

TARGETDIR キーワード

TARGETDIR では、クリアする統合サーバー・ファイルのパスを指定します。

注: ファイルを変更する際、i5/OS はそのファイルの最初のディレクトリーしか使用しません。他の項目によって異なるターゲット・ディレクトリーが指定されていても無視されます。

TARGETFILE キーワード

TARGETFILE では、クリアする統合サーバー・ファイルを指定します。

ADDCONFIG 項目タイプによる統合サーバー・ファイルの変更

ADDCONFIG 項目タイプを使用すると、統合 Windows サーバー・ファイルを以下のように変更できます。

- ファイルの先頭または末尾に行を追加する。
- 特定のストリングを備えた行の前または後に新しい行を追加する。
- ファイル内の行を削除する。
- ファイル内の行の最初、最後、またはすべてのオカレンスを置換する。
- ファイルを変更するディレクトリーを指定する。

統合サーバー・ファイルを変更するには、以下のような ADDCONFIG 項目タイプの入った NWS D 構成ファイルを作成します。

```
ADDCONFIG
VAR           = '<variable_name>', (条件付きで必須)
ADDSTR       = '<line to process>', (オプション)
ADDWHEN      = '<ALWAYS|NEVER|<expression>>', (オプション)
DELETEWHEN  = '<NEVER|ALWAYS|<expression>>', (オプション)
LINECOMMENT  = '<"REM "|<comment_string>>', (オプション)
LOCATION      = '<END|BEGIN>', (オプション)
FILESEARCHPOS = '<AFTER|BEFORE>', (オプション)
FILESEARCHSTR = '<search_string>', (条件付きで必須)
FILESEARCHSTROCC = '<LAST|FIRST>', (オプション)
REPLACEOCC  = '<LAST|FIRST|ALL>', (オプション)
```



```
TARGETDIR    = '<BOOT|path>',          (オプション)
TARGETFILE   = '<CONFIG.SYS|<file_name>>', (オプション)
UNIQUE       = '<NO|YES>'            (オプション)
```

ADDCONFIG キーワードの詳細については、以下のキーワード・リンクを使用してください。 275 ページの『NWSO 構成ファイル形式』または 283 ページの『UPDATECONFIG 項目タイプによる統合 Windows サーバー・ファイルの変更』に戻ることができます。

- 『VAR キーワード』
- 『ADDSTR キーワード』
- 『ADDWHEN キーワード』
- 280 ページの『DELETEWHEN キーワード』
- 281 ページの『LINECOMMENT キーワード』
- 281 ページの『LOCATION キーワード』
- 281 ページの『FILESEARCHPOS キーワード (ADDCONFIG 項目タイプ)』
- 281 ページの『FILESEARCHSTR キーワード』
- 282 ページの『FILESEARCHSTROCC キーワード』
- 282 ページの『REPLACEOCC キーワード』
- 282 ページの『TARGETDIR キーワード』
- 282 ページの『TARGETFILE キーワード』
- 283 ページの『UNIQUE キーワード』

VAR キーワード

VAR は、ファイルに追加したりファイルから削除したりする行を識別する値を、等号の左側に指定します。たとえば、以下のようにします。

```
ADDCONFIG
  VAR = 'FILES'
```

i5/OS では、REPLACEOCC を指定しない場合は、このキーワードが必要です。

ADDSTR キーワード

ADDSTR では、統合 Windows サーバー・ファイルに追加するストリングを指定します。たとえば、以下のようにします。

```
ADDCONFIG
  VAR = 'FILES'
  ADDSTR = '60'
```

ADDWHEN キーワード

ADDWHEN では、処理のどの時点で i5/OS が新しい行またはストリングを統合 Windows サーバー・ファイルに追加するかを指定します。

以下の値を指定できます。

- ALWAYS。i5/OS が構成ファイルを処理するごとに行またはストリングが追加されます。(メンバーの SETDEFAULTS 項目を使用して他のデフォルト値を定義していない限り、ALWAYS がデフォルトになります。)
- NEVER。i5/OS が行またはストリングを追加することはありません。

- 指定された条件が真の場合に i5/OS が行またはストリングを追加するように指示する式。式は演算子で構成されるものであり (『ADDWHEN および DELETEWHEN 式演算子』を参照)、 TRUE または FALSE のいずれかでなければなりません。

注: i5/OS が式 (たとえば、アスタリスク (*) の付いているもの) を数学演算と解釈しないようにするには、その式を引用符で囲んでください。たとえば、NWSD タイプが *WINDOWSNT の場合に行を追加するには、以下のようにします。

```
ADDWHEN = '(%FPANWSDTYPE%=="*WINDOWSNT")'
```

ADDWHEN および DELETEWHEN 式演算子

式では以下の演算子を使用できます。

演算子	説明
==	2 つのオペランドが等価の場合は TRUE、そうでない場合は FALSE を返します。
!=	2 つのオペランドが等価の場合は FALSE、そうでない場合は TRUE を返します。
>	左のオペランドが右のオペランドより大きい場合は TRUE、そうでない場合は FALSE を返します。オペランドがストリングの場合には、ASCII 値が比較されます。
<	左のオペランドが右のオペランドより小さい場合は TRUE、そうでない場合は FALSE を返します。オペランドがストリングの場合には、ASCII 値が比較されます。
>=	左のオペランドが右のオペランドより大きいか等しい場合は TRUE、そうでない場合は FALSE を返します。オペランドがストリングの場合には、ASCII 値が比較されます。
<=	左のオペランドが右のオペランドより小さいか等しい場合は TRUE、そうでない場合は FALSE を返します。オペランドがストリングの場合には、ASCII 値が比較されます。
&&	論理 AND。両方の値が 0 以外の場合に、TRUE を返します。オペランドは整数でなければなりません。
	論理 OR。いずれかのオペランドに 0 以外の値がある場合に、TRUE を返します。オペランドは整数でなければなりません。
+	オペランドが両方整数の場合には、結果はその整数の合計になります。オペランドが両方ストリングの場合には、結果はそのストリングの連結になります。
-	整数を減算します。
*	整数を乗算します。
/	整数を除算します。
()	評価の順序は括弧によって規定されます。
!	論理 NOT。単一オペランドの値が 0 の場合には TRUE、0 でない場合には FALSE を返します。
ALWAYS	常に TRUE を返します。
NEVER	常に FALSE を返します。

DELETEWHEN キーワード

処理のどの時点で i5/OS が行またはストリングをファイルから削除するかを指定するには、DELETEWHEN を使用します。以下の値を指定できます。

- ALWAYS。i5/OS が構成ファイルを処理するごとに行またはストリングが削除されます。
- NEVER。i5/OS が行またはストリングを削除することはありません。(メンバーの SETDEFAULTS 項目を使用して他のデフォルト値を定義していない限り、NEVER がデフォルトになります。)

- 指定された条件が真の場合に i5/OS が行またはストリングを削除するように指示する式。式は演算子で構成されるものであり (280 ページの『ADDWHEN および DELETEWHEN 式演算子』を参照)、 TRUE または FALSE のいずれかでなければなりません。

注: i5/OS が式 (たとえば、アスタリスク (*) の付いているもの) を数学演算と解釈しないようにするには、その式を引用符で囲んでください。たとえば、NWSD タイプが *WINDOWSNT の場合に行を削除するには、以下のようにします。

```
DELETEWHEN = '(%FPANWSdtype%=="*WINDOWSNT")'
```

LINECOMMENT キーワード

LINECOMMENT は、ファイル内の注記を識別する接頭部ストリングを指定します。REM を使って LINECOMMENT が注記であることを表すようにするには、デフォルト値を使用します。別の値を指定することもできます。たとえば、セミコロンで注記を識別するには、そのファイルを参照する**最初の項目**に LINECOMMENT = ';' と指定します。(i5/OS は、他の項目にある LINECOMMENT キーワードを無視します。)

LOCATION キーワード

LOCATION は、ファイルで新しい行を追加する位置を指定します。デフォルト値 END が指定されている場合、i5/OS はファイルの末尾に行を追加します。i5/OS で、ファイルの先頭に行が追加されるようにするには、BEGIN を指定します。

LINESEARCHPOS キーワード

ADDSTR キーワード値で指定するストリングを LINESEARCHSTR キーワードで指定した文字列の後 (AFTER、デフォルト) に追加するか前に追加するかを指定するには、LINESEARCHPOS を使用します。

LINESEARCHSTR キーワード

行内で検索するストリングを指定します。

注: 等号の右側のみ LINESEARCHSTR の検索に使用されます。

LINELOCATION キーワード

ADDSTR キーワード値で指定するストリングを行のどこに追加するかを指定するには、LINELOCATION を使用します。

デフォルト値 END を使用すると、i5/OS は行の末尾にストリングを追加します。逆に、BEGIN を指定すると、i5/OS は行の先頭にストリングを追加します。

FILESEARCHPOS キーワード (ADDCONFIG 項目タイプ)

ファイル検索文字列を基準にしたどの位置に行を追加するかを指定します。以下の値を指定できます。

- AFTER。i5/OS はファイル検索文字列の入った行の後に行を追加します。(メンバーの SETDEFAULTS 項目を使用して他のデフォルト値を定義していない限り、AFTER がデフォルトになります。)
- BEFORE。i5/OS は検索文字列の入った行の前に行を追加します。

FILESEARCHSTR キーワード

置換する行を指定するには、REPLACEOCC キーワードとともに FILESEARCHSTR を使用します。行全体を値として指定しなければなりません。

新しい行を追加する際には、FILESEARCHSTR は検出する行のどの部分でも構いません。

メンバーの SETDEFAULTS 項目を使用してデフォルト値を定義していない限り、デフォルト値はありません。

FILESEARCHSTROCC キーワード

ファイルで何度も現れるストリングについて、新しい行の位置指定に使用するオカレンスを指定します。

デフォルト値 LAST は、検索文字列の最後のオカレンスを指定します。i5/OS で、検索ストリングの最初のオカレンスが使用されるようにするには、FIRST を指定します。

REPLACEOCC キーワード

置換する行のオカレンスを指定します。

- LAST を使用すると、i5/OS は FILESEARCHSTR の最後のオカレンスを置換します。
- ALL を使用すると、i5/OS は FILESEARCHSTR のすべてのオカレンスを置換します。
- FIRST を使用すると、i5/OS は FILESEARCHSTR の最初のオカレンスを置換します。

置換するすべての行を指定するには、FILESEARCHSTR を使用します。

i5/OS は、FILESEARCHSTR に適合する行を削除し、ファイルのこの位置に指定された VAR および ADDSTR を追加します。

注: REPLACEOCC は、LOCATION および FILESEARCHPOS よりも優先されます。REPLACEOCC キーワードで使用される FILESEARCHSTR 値が検出されない場合、i5/OS は LOCATION キーワードの値に基づいて新しい行を追加しますが、行の置換は実行しません。

TARGETDIR キーワード

TARGETDIR では、変更する統合サーバー・ファイルのパスを指定します。

最初に SETDEFAULTS 項目を使用してデフォルトを変更しない限り、UNATTEND.TXT または独自の統合サーバー・ファイルのパスを指定する必要があります。(このキーワードのデフォルトは BOOT です。この値の場合、i5/OS は C ドライブのルート・ディレクトリーにあるファイルを変更します。)

注:

1. NWSD 構成ファイルがサポートされているのは、FAT としてフォーマットされている事前定義ディスク・ドライブのみです。NTFS に変換されている記憶域には構成ファイルではアクセスできません。179 ページの『統合 Windows サーバーの事前定義ディスク・ドライブ』を参照してください。
2. ファイルを変更する際、i5/OS はそのファイルの最初のディレクトリーしか使用しません。他の項目によって異なるターゲット・ディレクトリーが指定されていても無視されます。

TARGETFILE キーワード

TARGETFILE では、変更する統合サーバー・ファイルを指定します。UNATTEND.TXT の値を指定すると、i5/OS は、統合サーバー不在インストール・セットアップ・スクリプト・ファイルを変更します。

最初に SETDEFAULTS 項目を使用してデフォルトを変更しない限り、UNATTEND.TXT または独自の統合サーバー・ファイルを指定する必要があります。(このキーワードのデフォルトは CONFIG.SYS です。)

UNIQUE キーワード

ファイルで 1 行につき 1 つのオカレンスしか存在できないようにする場合は、YES を指定します。

デフォルト値 NO では、複数のオカレンスが存在することができます。

VAROCC キーワード

使用する変数のオカレンスを指定するには、VAROCC を使用します。

変数の最後のオカレンスを変更する場合は、デフォルト値を使用できます。そうでない場合には、FIRST を指定して、変数の最初のオカレンスを変更します。

VARVALUE キーワード

指定する変数がこの値になっている行だけを変更するには、VARVALUE を使用します。

変更したい式の右側にあるストリングの全体または一部を指定できます。

UPDATECONFIG 項目タイプによる統合 Windows サーバー・ファイルの変更

UPDATECONFIG 項目タイプを使用すると、統合サーバー・ファイルを以下のように変更できます。

- ファイルで行にストリングを追加する。
- 指定されたストリングの前または後に新しいストリングを追加する。
- ファイルの行からストリングを削除する。
- ファイルを変更するパスを指定する。

統合サーバー・ファイルを変更するには、以下のような UPDATECONFIG 項目タイプの入った NWSD 構成ファイルを作成します。

```
UPDATECONFIG
VAR                = '<variable_name>',          (必須)
ADDSTR             = '<line to process>',        (必須)
ADDWHEN            = '<ALWAYS|NEVER|<expression>>', (オプション)
DELETEWHEN        = '<NEVER|ALWAYS|<expression>>', (オプション)
LINECOMMENT       = '<"REM "|<comment_string>>', (オプション)
LINELOCATION        = '<END|BEGIN>',              (オプション)
LINESEARCHPOS     = '<AFTER|BEFORE>',            (オプション)
LINESEARCHSTR     = '<string within a line>',    (オプション)
FILESEARCHPOS     = '<AFTER|BEFORE>',            (オプション)
FILESEARCHSTR     = '<search string>',           (オプション)
FILESEARCHSTROCC = '<LAST|FIRST>',              (オプション)
TARGETDIR         = '<BOOT|<path>>',             (オプション)
TARGETFILE        = '<CONFIG.SYS|<file_name>>', (オプション)
VAROCC            = '<LAST|FIRST>',             (オプション)
VARVALUE          = '<variable value>'          (オプション)
```

UPDATECONFIG キーワードの詳細については、以下のキーワード・リンクを使用してください。 275 ページの『NWSD 構成ファイル形式』または 284 ページの『SETDEFAULTS 項目タイプによる構成デフォルトの設定』に戻ることもできます。

- 279 ページの『VAR キーワード』
- 279 ページの『ADDSTR キーワード』
- 279 ページの『ADDWHEN キーワード』
- 280 ページの『DELETEWHEN キーワード』

- 281 ページの『LINECOMMENT キーワード』
- 281 ページの『LINELOCATION キーワード』
- 281 ページの『LINESEARCHPOS キーワード』
- 281 ページの『LINESEARCHSTR キーワード』
- 『FILESEARCHPOS キーワード (UPDATECONFIG 項目タイプ)』
- 『FILESEARCHSTR キーワード (UPDATECONFIG 項目タイプ)』
- 『FILESEARCHSTROCC キーワード (UPDATECONFIG 項目タイプ)』
- 282 ページの『TARGETDIR キーワード』
- 282 ページの『TARGETFILE キーワード』
- 283 ページの『VAROCC キーワード』
- 283 ページの『VARVALUE キーワード』

FILESEARCHPOS キーワード (UPDATECONFIG 項目タイプ)

検索文字列の入った行を基準として i5/OS に検出させる変数のオカレンスを指定するには、FILESEARCHPOS を使用します。以下の値を使用できます。

- AFTER。i5/OS は、検索文字列の入っている行の後における変数の最初のオカレンスを検出します。(メンバーの SETDEFAULTS 項目を使用して他のデフォルト値を定義していない限り、AFTER がデフォルトになります。)
- BEFORE。i5/OS は、検索文字列の入っている行の前における変数の最初のオカレンスを検出します。

注: 検索文字列が検出されない場合、i5/OS は VAROCC キーワードから変更する行を判別します。

FILESEARCHSTR キーワード (UPDATECONFIG 項目タイプ)

置換する変数のオカレンスを i5/OS が見つけるのに使用する検索変数を指定するには、FILESEARCHSTR を使用します。

メンバーの SETDEFAULTS 項目を使用してデフォルト値を定義していない限り、デフォルト値はありません。

FILESEARCHSTROCC キーワード (UPDATECONFIG 項目タイプ)

ファイルで何度も現れるストリングについて、変更する行の検出に使用するオカレンスを指定するには、FILESEARCHSTROCC を使用します。

デフォルト値 LAST を使用すると、i5/OS は検索文字列の最後のオカレンスを使用します。i5/OS が検索文字列の最初のオカレンスを使用するには、FIRST を指定します。

SETDEFAULTS 項目タイプによる構成デフォルトの設定

ADDCONFIG および UPDATECONFIG 項目タイプの特定のキーワードのデフォルト値を設定するには、SETDEFAULTS を使用します。以下の作業を行うデフォルトを設定できます。

- 行を追加および削除する。
- 行を検索する。
- 変更するファイル名およびパスを識別する。

デフォルトを設定するには、以下のような SETDEFAULTS 項目タイプを備えた NWS D 構成ファイルを作成します。

```
SETDEFAULTS
ADDWHEN      = '<ALWAYS|NEVER|<expression>>', (オプション)
DELETEWHEN  = '<NEVER|ALWAYS|<expression>>', (オプション)
FILESEARCHPOS = '<AFTER|BEFORE>', (オプション)
FILESEARCHSTR = '<search_string>', (オプション)
TARGETDIR    = '<path>', (オプション)
TARGETFILE   = '<file_name>' (オプション)
```

SETDEFAULTS キーワードの詳細については、以下のキーワード・リンクを使用してください。

- 『ADDWHEN』
- 『DELETEWHEN』
- 286 ページの『FILESEARCHPOS キーワード (SETDEFAULTS 項目タイプ)』
- 286 ページの『FILESEARCHSTR キーワード (SETDEFAULTS 項目タイプ)』
- 286 ページの『TARGETDIR』
- 286 ページの『TARGETFILE』

ADDWHEN

ADDCONFIG および UPDATECONFIG 項目タイプの ADDWHEN キーワードのデフォルト値を設定するには、SETDEFAULTS 項目タイプとともに ADDWHEN を使用します。

処理のどの時点で i5/OS が新しい行またはストリングをファイルに追加するかを示すデフォルトを指定できます。以下の値を指定できます。

- ALWAYS。i5/OS が構成ファイルを処理するごとに行またはストリングが追加されます。(他のデフォルトを定義していない限り、ALWAYS がデフォルトになります。)
- NEVER。i5/OS が行またはストリングを追加することはありません。
- 指定された条件が真の場合に i5/OS が行またはストリングを追加するように指示する式。式はオペランドで構成されるものであり (280 ページの『ADDWHEN および DELETEWHEN 式演算子』を参照)、TRUE または FALSE のいずれかでなければなりません。

注: i5/OS が式 (たとえば、アスタリスク (*) の付いているもの) を数学演算と解釈しないようにするには、その式を引用符で囲んでください。たとえば、NWS D タイプが *WINDOWSNT の場合に行を追加するには、以下のようにします。

```
ADDWHEN = '(%FPANWSDTYPE%=="*WINDOWSNT")'
```

DELETEWHEN

ADDCONFIG および UPDATECONFIG 項目タイプの DELETEWHEN キーワードのデフォルト値を設定するには、SETDEFAULTS 項目タイプとともに DELETEWHEN を使用します。

処理のどの時点で i5/OS が行またはストリングをファイルから削除するかを指定します。

以下の値を指定できます。

- ALWAYS。i5/OS が構成ファイルを処理するごとに行またはストリングが削除されます。
- NEVER。i5/OS が行またはストリングを削除することはありません。(他のデフォルトを定義していない限り、NEVER がデフォルトになります。)

- 指定された条件が真の場合に i5/OS が行またはストリングを削除するように指示する式。式はオペランドで構成されるものであり (280 ページの『ADDWHEN および DELETEWHEN 式演算子』を参照)、TRUE または FALSE のいずれかでなければなりません。

注: i5/OS が式 (たとえば、アスタリスク (*) の付いているもの) を数学演算と解釈しないようにするには、その式を引用符で囲んでください。たとえば、NWSD タイプが *WINDOWSNT の場合に行を削除するには、以下のようにします。

```
DELETEWHEN = '(%FPANWSdtype%=="*WINDOWSNT")'
```

FILESEARCHPOS キーワード (SETDEFAULTS 項目タイプ)

ADDCONFIG および UPDATECONFIG 項目タイプの FILESEARCHPOS キーワードのデフォルト値を設定するには、SETDEFAULTS 項目タイプとともに FILESEARCHPOS を使用します。

ファイル検索文字列を基準にしたどの位置に行を追加するかを指定します。以下の値を指定できます。

- AFTER。ファイル検索文字列の入った行の後に行が追加されます。(他のデフォルトを定義していない限り、AFTER がデフォルトになります。)
- BEFORE。i5/OS は検索文字列の入った行の前に行を追加します。

FILESEARCHSTR キーワード (SETDEFAULTS 項目タイプ)

ADDCONFIG および UPDATECONFIG 項目タイプの FILESEARCHSTR キーワードのデフォルト値を設定するには、SETDEFAULTS 項目タイプとともに FILESEARCHSTR を使用します。

FILESEARCHSTR 値は、検出する行のどの部分でも構いません。

TARGETDIR

ADDCONFIG および UPDATECONFIG 項目タイプの TARGETDIR キーワードのデフォルト値を設定するには、SETDEFAULTS 項目タイプとともに TARGETDIR を使用します。

パスは、処理するファイルが置かれているディレクトリーを指定します。

たとえば、デフォルト TARGETDIR 値をドライブ D 上のファイルに設定するには、次のようにします。

```
SETDEFAULTS TARGETDIR = 'D:¥'
```

TARGETFILE

ADDCONFIG および UPDATECONFIG 項目タイプの TARGETFILE キーワードのデフォルト値を設定するには、SETDEFAULTS 項目タイプとともに TARGETFILE を使用します。

名前は、処理するファイルを指定します。

たとえば、デフォルト TARGETFILE 値をドライブ D 上のファイル UNATTEND.TXT に設定するには、次のようにします。

```
SETDEFAULTS  
TARGETDIR = 'D:¥',  
TARGETFILE = 'UNATTEND.TXT'
```


キーワード値に対する置換変数の使用

キーワード値に置換変数を使用することができます。NWSD 構成ファイルは、変数に正しい値を置換します。これらの置換変数は、NWSD、または NWSD で検出されるハードウェアに格納されている値を使用して構成されています。

i5/OS には、以下の変数があります。

置換変数	説明
%FPAIPADDRPP%	TCP/IP アドレス (NWSD ポート *VRTETHPTP) *
%FPAIPADDR01%	TCP/IP アドレス (NWSD ポート 1) *
%FPAIPADDR02%	TCP/IP アドレス (NWSD ポート 2) *
%FPAIPADDR03%	TCP/IP アドレス (NWSD ポート 3) *
%FPASUBNETPP%	TCP/IP サブネット・アドレス (NWSD ポート *VRTETHPTP) *
%FPASUBNET01%	TCP/IP サブネット・アドレス (NWSD ポート 1) *
%FPASUBNET02%	TCP/IP サブネット・アドレス (NWSD ポート 2) *
%FPASUBNET03%	TCP/IP サブネット・アドレス (NWSD ポート 3) *
%FPATCPHOSTNAME%	TCP/IP ホスト名
%FPATCPDOMAIN%	TCP/IP ドメイン名
%FPATCPDNSS%	コンマで区切られた複数の TCP/IP DNS
%FPATCPDNS01%	TCP/IP ドメイン名サーバー 1
%FPATCPDNS02%	TCP/IP ドメイン名サーバー 2
%FPATCPDNS03%	TCP/IP ドメイン名サーバー 3
%FPANWSDTYPE%	オンに変更しようとしている NWSD のタイプ
%FPANWSDNAME%	オンに変更しようとしている NWSD の名前
%FPACARDTYPE%	オンに変更しようとしている NWSD のリソース・タイプ (たとえば、2890、2892、4812、2689、iSCSI)
%FPAINSMEM%	検出されたインストール済みのメモリー量
%FPAUSEMEM%	検出された使用可能なメモリー量
%FPACODEPAGE%	EBCDIC からの変換に使われる ASCII コード・ページ
%FPALANGVERS%	NWSD で使われる i5/OS 言語バージョン
%FPASYSDRIVE%	システム・ドライブで使われるドライブ名 (V4R4 以前でサーバーがインストールされていれば C、E)
%FPA_CARET%	脱字記号 (^)
%FPA_L_BRACKET%	左ブラケット記号 (l)
%FPA_R_BRACKET%	右ブラケット記号 (r)
%FPA_PERCENT%	パーセント記号 (%)。注: パーセント機能は置換変数の区切り文字として使用されるため、置換変数区切り文字でないパーセント記号をストリングに挿入する場合には、この置換変数を使用しなければなりません。
%FPABOOTDRIVE%	統合 xSeries サーバーでは常にドライブ E
%FPACFGFILE%	処理中の NWSD 構成ファイルの名前
%FPACFGLIB%	処理中の NWSD 構成ファイルを収容したライブラリーの名前
%FPACFGMBR%	処理中の NWSD 構成ファイルのメンバーの名前
* 値は NWSD から検索されます。	

QUSRSYS 内にファイルを作成し、NWSD の名前に接尾部 'VA' を付けた名前を付けて、追加の置換変数を構成することができます。このファイルは、最小レコード長 16、最大レコード長 271 のソース物理ファイルとして作成する必要があります。

たとえば、i5/OS コマンド行で次のように入力します。

```
CRTSRCPF FILE(QUSRSYS/nwsdnameVA) RCDLEN(271)
  MBR(nwsdname) MAXMBRS(1)
  TEXT('Configuration file variables')
```

メンバー 'nwsdname' のデータは、以下のように形式化された固定列に入ります。

- 桁 1 から 15 まではブランクが埋め込まれた変数名
- 桁 16 以降は値

たとえば、以下のようにします。



```
Columns:
12345678901234567890123456789012345678901234567890...
myaddr          9.5.9.1
```

ここで、%myaddr% は使用できる置換変数のリストに追加されており、その値は "9.5.9.1" です。

第 16 章 関連情報

下記のリストは、iSeries マニュアルおよび IBM レッドブック (PDF 形式)、Web サイト、および iSeries の Windows 環境トピックに関連した Information Center トピックです。PDF は表示および印刷できません。

マニュアル

- 「iSeries Performance Capabilities Reference 」
- 「バックアップおよび回復の手引き 」
- ハードウェア・インストールの指示。トピック『Install iSeries features』を参照。

レッドブック (www.redbooks.ibm.com)

「Microsoft Windows Server 2003 Integration with iSeries」 (SG24-6959) 

| 「IBM xSeries and BladeCenter Server Management」 (SG24-6495) 

Web サイト

- | • 最新の製品とサービスの情報: IBM iSeries Integrated xSeries solutions 
| (www.ibm.com/servers/eserver/series/integratedxseries)
- iSeries Performance Management 
(www.ibm.com/eserver/series/perfmgmt)
- IXA install read me first 
(www.ibm.com/servers/eserver/series/integratedxseries/ixareadme)
- | • iSCSI install read me first 
| (www.ibm.com/servers/eserver/series/integratedxseries/iscsireadme)
- IXS install read me first 
(www.ibm.com/servers/eserver/series/integratedxseries/ixsreadme)
- | • Troubleshooting 
| (www.ibm.com/servers/eserver/series/integratedxseries/troubleshooting.html).

付録. 特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

- | 〒106-0032
- | 東京都港区六本木 3-2-31
- | IBM World Trade Asia Corporation
- | Licensing

以下の保証は、国または地域の法律に沿わない場合は、適用されません。IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態を提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとしします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

- | 本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム
- | 契約の契約条項、IBM プログラムのご使用条件、IBM 機械コードのご使用条件、またはそれと同等の条項
- | に基づいて、IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性があります。その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があります、単に目標を示しているものです。

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

商標

以下は、IBM Corporation の商標です。

AIX
AS/400
BladeCenter
DB2
IBM
iSeries
Netfinity
NetServer
OS/400
i5/OS
PAL
Redbooks
ServerGuide
Virtualization Engine
xSeries

Pentium は、Intel Corporation の米国およびその他の国における商標です。

- | Linux は、Linus Torvalds の米国およびその他の国における商標です。

Microsoft、Windows、Windows NT および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

他の会社名、製品名およびサービス名等はそれぞれ各社の商標です。

使用条件

これらの資料は、以下の条件に同意していただける場合に限りご使用いただけます。

個人使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、非商業的な個人による使用目的に限り複製することができます。ただし、IBM の明示的な承諾をえずに、これらの資料またはその一部について、二次的著作物を作成したり、配布 (頒布、送信を含む) または表示 (上映を含む) することはできません。

商業的使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、お客様の企業内に限り、複製、配布、および表示することができます。ただし、IBM の明示的な承諾をえずにこれらの資料の二次的著作物を作成したり、お客様の企業外で資料またはその一部を複製、配布、または表示することはできません。

ここで明示的に許可されているもの以外に、資料や資料内に含まれる情報、データ、ソフトウェア、またはその他の知的所有権に対するいかなる許可、ライセンス、または権利を明示的にも黙示的にも付与するものではありません。

資料の使用が IBM の利益を損なうと判断された場合や、上記の条件が適切に守られていないと判断された場合、IBM はいつでも自らの判断により、ここで与えた許可を撤回できるものとさせていただきます。

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入関連法規を含む、すべての関連法規を遵守するものとします。

IBM は、これらの資料の内容についていかなる保証もしません。これらの資料は、特定物として現存するままの状態を提供され、第三者の権利の不侵害の保証、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されます。



Printed in Japan