MS81: WebSphere® MQ internet pass-thru バージョン 1.2

SC88-9258-00
(英文原典：SC34-6100-00)

お願い

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

本書は、MS81: WebSphere MQ internet pass-thru のバージョン 1.2 (プログラム番号 5639-L92)、および新しい版で明記されてされていない限り、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。

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)

原　典： SC34-6100-00
MS81: WebSphere® MQ internet pass-thru
Version 1.2

発　行： 日本アイ・ビー・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 2002.4

この文書では、平成明朝体™W3、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™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

目次

図 v

特記事項 vii
商標 vii

まえがき ix
internet pass-thru とは ? ix
対象読者 ix
本書を理解する上での必要な知識 ix
前提条件 x
アクセシビリティー情報 x

参照文献 xiii

変更の要約 xv

第 1 章 WebSphere MQ internet pass-thru の紹介 1

第 2 章 internet pass-thru の機能 . . . 7
internet pass-thru の機能の概要 7
HTTP サポート 8
SOCKS サポート 9
SSL サポート 9
SSL ハンドシェーク 10
MQIPT および SSL 12
トラストの設定 12
SSL のテスト 13
SSL エラー・メッセージ 13
Quality of Service (QoS) 14
サーブレット 15
KeyMan 16
サポートされるトークンのタイプ 16
サポートされている標準データ形式 17
KeyMan FAQ 18
Network Dispatcher サポート 20
クラスター化 21
サポートされるチャネル構成 23
Java Security Manager 24
正常終了と失敗条件 26
メッセージの安全性 26
接続ログ 26
その他のセキュリティー上の考慮事項 27

第 3 章 先行バージョンからのアップグレード 29
新規構成オプション 29

第 4 章 Windows での internet pass-thru のインストール 31
ファイルのダウンロードとインストール 32
internet pass-thru のセットアップ 32
コマンド行からの internet pass-thru の開始 32
コマンド行からの Administration Client の開始 . . 33
Windows サービス制御プログラムの使用 34
Windows サービスとしての internet pass-thru のアンインストール 34
internet pass-thru のアンインストール 34

第 5 章 Sun Solaris での internet pass-thru のインストール 35
ファイルのダウンロードとインストール 35
internet pass-thru のセットアップ 36
コマンド行からの internet pass-thru の開始 36
internet pass-thru の自動開始 37
コマンド行からの Administration Client の開始 . . 37
internet pass-thru のアンインストール 38

第 6 章 AIX での internet pass-thru のインストール 39
ファイルのダウンロードとインストール 39
internet pass-thru のセットアップ 40
コマンド行からの internet pass-thru の開始 40
internet pass-thru の自動開始 41
コマンド行からの Administration Client の開始 . . 41
internet pass-thru のアンインストール 42

第 7 章 HP-UX での internet pass-thru のインストール 43
ファイルのダウンロードとインストール 43
internet pass-thru のセットアップ 44
コマンド行からの internet pass-thru の開始 44
internet pass-thru の自動開始 45
コマンド行からの Administration Client の開始 . . 45
internet pass-thru のアンインストール 46

第 8 章 Linux での internet pass-thru のインストール 47
ファイルのダウンロードとインストール 47
internet pass-thru のセットアップ 48
コマンド行からの internet pass-thru の開始 48
internet pass-thru の自動開始 49
コマンド行からの Administration Client の開始 . . 49
internet pass-thru のアンインストール 50

第 9 章 internet pass-thru の管理と構成 51
internet pass-thru Administration Client の使用 . . . 51
Administration Client の開始 51
MQIPT の管理 52

プロパティーの継承 53
ファイル・メニュー・オプション 53
MQIPT メニュー・オプション 54
ヘルプ・メニュー・オプション 55
internet pass-thru 行モード・コマンド 56
行モード・コマンドによる internet pass-thru の管理 56
構成参照情報 57
プロパティーの要約 58
グローバル・セクション参照情報 60
経路セクション参照情報 61

第 10 章 internet pass-thru の使用開始 71

前提事項 71
構成の例 72
インストール検証テスト 72
SSL サーバー認証 74
SSL クライアント認証 77
HTTP プロキシー構成 79
構成アクセス制御 82
Quality of Service (QoS) の構成 85
SOCKS プロキシーの構成 88
SOCKS クライアントの構成 90
SSL プロキシーの構成 91
SSL テスト証明書の作成 95
MQIPT サーブレットの構成 96
MQIPT クラスター化サポートの構成 98
鍵リング・ファイルの作成 102

第 11 章 internet pass-thru の維持 105

保守 105
問題判別 105
internet pass-thru の自動的開始 107
エンドツーエンド接続の検査 107
エラーのトレース 107
問題の報告 108
パフォーマンス・チューニング 108
スレッド・プール管理 108
接続スレッド 108
アイドル・タイムアウト 108

第 12 章 メッセージ 111

索引 127

図

1. チャネル・コンセントレーターとしての MQIPT の例 2
2. 「非武装地帯」を持つ MQIPT の例 2
3. MQIPT および HTTP トンネル操作の例 . . . 3
4. MQIPT と SSL の例 3
5. 可能な MQIPT 構成を示す WebSphere MQ トポロジー 5
6. MQIPT での Network Dispatcher の使用 20
7. MQIPT クラスター化のサポート 23
8. MQIPT への初回アクセス時のウィンドウ 52
9. 経路の追加 55
10. IVT ネットワーク・ダイアグラム 72
11. IVT 構成 73
12. SSL サーバー・ネットワーク・ダイアグラム 74
13. SSL サーバー認証 75
14. SSL クライアント・ネットワーク・ダイアグラム 77
15. SSL クライアント認証 78
16. HTTP プロキシー・ネットワーク・ダイアグラム 80
17. HTTP プロキシー構成 81
18. アクセス制御ネットワーク・ダイアグラム 83
19. アクセス制御構成 83
20. QoS ネットワーク・ダイアグラム 85
21. QoS 構成 86
22. SOCKS プロキシー・ネットワーク・ダイアグラム 88
23. SOCKS プロキシー構成 89
24. SOCKS クライアント・ネットワーク・ダイアグラム 90
25. SOCKS クライアント構成 90
26. SSL プロキシー・ネットワーク・ダイアグラム 92
27. SSL プロキシー構成 93
28. サーブレット・ネットワーク・ダイアグラム 96
29. サーブレット構成 97
30. クラスター化ネットワーク・ダイアグラム 99
31. クラスター化構成 100
32. 問題判別フローチャート 106

特記事項

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で提供し、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ます。

本書に記載の製品、プログラム、またはサービス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、プログラム、またはサービスについては、日本アイ・ビー・エム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。 IBM 製品、プログラムまたはサービスに代えて、IBM の知的所有権を侵害することのない機能的に同等のプログラムまたは製品を使用することができます。ただし、IBM によって明示的に指定されたものを除き、他社の製品と組み合わせた場合の操作の評価と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。使用許諾については、下記の宛先に書面にてご照会ください。

〒106-0032 東京都港区六本木 3 丁目 2-31
IBM World Trade Asia Corporation
Intellectual Property Law & Licensing

本書に含まれる情報は、IBM の正式なテストを受けておらず、現存するままの状態で配布されます。この情報の利用またはこうした手法の導入は、お客様の責任であるとともに、これを評価しお客様の稼働環境への統合するお客様の能力に依存します。個々の項目は、特定の状況における正確性について IBM によって検討されていますが、全く同一または同様な結果が得られる保証はありません。お客様自身の環境にこれらの手法を適用しようとする場合は、お客様自身のリスクにおいて行っていただきます。

商標

以下は、IBM Corporation の商標です。

AIX	FFST	First Failure Support Technology
IBM	IBMLink	MQSeries
SupportPac	WebSphere	

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などはそれぞれ各社の商標または登録商標です。

まえがき

internet pass-thru とは ?

WebSphere MQ internet pass-thru は、以前は MQSeries internet pass-thru と呼ばれていました。本書では、MQSeries を WebSphere MQ と呼ぶことにします。ただし、すべての MQSeries のマニュアルが直ちに名前を WebSphere MQ に変更するわけではなく、しばらくは、MQSeries と WebSphere MQ の両方を使用することになります。

IBM® WebSphere MQ internet pass-thru は、以下の特徴を備えています。

- WebSphere MQ 基本製品を拡張したもので、インターネットを介したリモート・サイト間でのメッセージング・ソリューションをインプリメントする場合に使用できます。
- WebSphere MQ チャネル・プロトコルを HTTP の中に組み込んだり、プロキシーとして機能させたりすることにより、このプロトコルがファイアウォールに出入りする通路をより簡単、かつより管理可能なものにします。
- WebSphere MQ メッセージ・フローの送受信が可能なスタンドアロン・サービスとして働きます。それを実行するシステムは、WebSphere MQ キュー・マネージャーをホスト処理する必要がありません。
- WebSphere MQ を使用して企業間トランザクションを提供する手助けをします。
- 既存の未変更 WebSphere MQ アプリケーションをファイアウォールで使用できるようにします。
- 複数のキュー・マネージャーにアクセスする場合の単一制御点を備えています。
- すべてのデータの暗号化を可能にします。

本書では便宜上、WebSphere MQ internet pass-thru をしばしば “MQIPT” と呼んでいます。

対象読者

本書は、システム設計者、WebSphere MQ 技術管理者、ファイアウォールおよびネットワーク管理者向けに作成されています。

本書を理解する上での必要な知識

以下のことを十分に理解しておく必要があります。

- WebSphere MQ キュー・マネージャーとメッセージ・チャネルの管理 (「*MQSeries System Administration*」および「*MQSeries 相互通信*」に説明があります)。
- ファイアウォールのインプリメント方法
- インターネット・プロトコルの経路 (ルート) 指定 / ネットワーキング
- ロード・バランシングおよび拡張可用性のための IBM Network Dispatcher
- IBM WebSphere Application Server

前提条件

当リリースの internet pass-thru は、以下のオペレーティング・システムで稼働します。

- Windows NT® V4.0 (Service Pack 6 を適用したもの)
- Windows 2000
- Windows XP
- Sun Solaris
- AIX®
- HP-UX 11
- Linux

注: AIX と HP-UX は、これらのプラットフォームで Java 1.4 がリリースされたときに使用可能になります。

JDK は、1.4.0 以上のレベルまたはそれ以降の互換性のあるリリースでなければなりません。

サポートされる唯一のネットワーク・プロトコルは TCP/IP です。

Administration Client ヘルプには Netscape ブラウザーが必要です。

アクセシビリティー情報

Administration Client GUI は、アクセシビリティーを考慮に入れて作成されています。キーボード相当機能を使用すれば、マウスを使用しなくても、提供されるすべての機能を簡単に実行できます。タブやシフト・タブ、Ctrl タブ、カーソル・キーなどを標準方法で使用して、画面をナビゲートすることができます。ボタンを押す操作に代わるものとして、まずボタンを選択し、次に Enter キーを押します。

メニュー・オプションを表示するには、タブとカーソル・キーを併用するか、またはアクセラレーター・キーを使用します。アクセラレーター・キーはすべてのオプションで使用できます。たとえば、GUI をクローズする場合は、まず alt-f を選択し、次に alt-q (File->Quit) を選択します。メニュー項目を表示したならば、Enter キーを使ってそれをアクティブにすることができます。

ツリーをナビゲートする場合は、カーソル・キーを使用します。特に、右カーソル・キーと左カーソル・キーを使って MQIPT ノードをオープンしたりクローズしたりできるため、経路の表示や非表示が可能になります。

選択したチェック・ボックスの状態を変更するには、スペース・キーを使用します。編集用のフィールドを選択するには、Enter キーを使用します。

ルック・アンド・フィール

理想的には、GUI はこの環境のルック・アンド・フィールを持っていなければなりません。これは必ずしも常に可能ではないので、構成ファイルを提供して GUI のルック・アンド・フィールをユーザーのニーズに合わせることができます。この構成ファイルは ″custom.properties″ と呼ばれていて、`bin` サブディレクトリーに入れておかなければなりません。

この構成ファイルを使用して以下の構成を行います。

- 前景色 - テキストのカラー
- 背景色
- テキストのフォント
- テキストのスタイル - プレーン、太字、イタリック、または太字イタリック

″customSample.properties″ 構成ファイルが提供されており、この構成ファイルにはその変更方法示すコメントが含まれています。このファイルを `bin/custom.properties` にコピーして、必要な変更を加えることをお勧めします。

参照文献

本書は、インストール製品の一部として PDF と HTML で提供されます。本書は、表 1 に示されているディレクトリーにインストールされています。「Administration Client」を使用する前に、<lang>/html サブディレクトリーに入っているファイルを UNZIP する必要があります。

- PDF

  doc¥<lang>¥pdf¥<filename>.pdf

- HTML (自己解凍 ZIP ファイルに入っています)

  doc¥<lang>¥html¥<filename>.zip

本書は、以下の言語で作成されています。言語とその対応ファイル名については、以下の表を参照してください。

表 1. 言語とファイル名の要約

言語	ロケール	PDF ファイル名	HTML ファイル名
中国語 (簡体字)	zn_CN	amqyzb00.pdf	amqyzb00.zip
ドイツ語	de_DE	amqygb00.pdf	amqygb00.zip
日本語	ja_JP	amqyjb00.pdf	amqyjb00.zip
韓国語	ko_KR	amqykb00.pdf	amqykb00.zip
ポルトガル・ブラジル語	pt_BR	amqybb00.pdf	amqybb00.zip
スペイン語	es_ES	amqysb00.pdf	amqysb00.zip
米国英語	en_US	amqyab00.pdf	amqyab00.zip

以下の資料も有用です。

- *MQSeries 相互通信*、SC88-7775
- *MQSeries システム管理の手引き*、SC88-7776
- *MQSeries クライアント*、GC88-7495
- *MQSeries キュー・マネージャー・クラスター*、SD88-7165

これらの資料は、WebSphere MQ チャネルとその属性の定義に関する情報、特に CONNAME の定義に関する情報を提供します。

WebSphere MQ 資料は、以下の URL から入手できます。

http://www.ibm.com/software/ts/mqseries/library/

変更の要約

このバージョンの WebSphere MQ internet pass-thru には、以下の拡張機能が含まれています。

- 構成の例
- 改良された SSL トレース
- Java Security Manager
- SSL 証明書と鍵リング・ファイルを管理するための KeyMan ユーティリティー
- Linux サポート (Quality of Service for WebSphere MQ メッセージを含む)
- Windows プラットフォームで使用できる NLS インストール・イメージ
- 大文字小文字を区別しないプロパティー名
- サーブレット・バージョン
- Socks クライアントおよびサーバー・サポート
- SSL プロキシー・モード
- Administration Client 用のトラフィック・ライト状況
- WebSphere MQ クラスター・サポート

第 1 章 WebSphere MQ internet pass-thru の紹介

WebSphere MQ internet pass-thru は、WebSphere MQ の基本製品を拡張したものです。 MQIPT は、2 つの WebSphere MQ キュー・マネージャー間、あるいは WebSphere MQ クライアントと WebSphere MQ キュー・マネージャー間で WebSphere MQ メッセージ・フローの送受信を行うことができる、スタンドアロンのサービスとして稼働します。 MQIPT は、クライアントとサーバーが同じ物理ネットワーク上にいない場合でもこの接続を可能にしています。

2 つの WebSphere MQ キュー・マネージャー間、または WebSphere MQ クライアントと WebSphere MQ キュー・マネージャー間の通信パスに 1 つまたは複数の MQIPT を設定することができます。 MQIPT を使用すれば、2 つの WebSphere MQ システムは、両者間に TCP/IP 直接接続を設けなくてもメッセージ交換を行えるようになります。この方法は、ファイアウォール構成により 2 つのシステム間の TCP/IP 直接接続が禁止されている場合に有効です。

MQIPT は、1 つまたは複数の TCP/IP ポートで着信接続を listen します。そこでは、通常の WebSphere MQ メッセージや、HTTP の中に組み込まれた WebSphere MQ メッセージ、 SSL (Secure Sockets Layer) で暗号化された WebSphere MQ メッセージを送信することができます。このサービスは、複数の同時接続を処理することができます。

最初の TCP/IP 接続要求を行う WebSphere MQ チャネルは「呼び出し元」と呼ばれ、呼び出し元の接続先チャネルは「レスポンダー」、呼び出し元の最終接続先であるキュー・マネージャーは「宛先キュー・マネージャー」と呼ばれます。

MQIPT の使用法としては、次のことが考えられます。

- MQIPT をチャネル・コンセントレーターとして使用することができる。これにより、いくつかの個別のホストに接続されたチャネルが、ファイアウォールからは、それらがすべて MQIPT ホストに接続されているように見えます。このため、ファイアウォール・フィルター規則の定義と管理が容易になります。

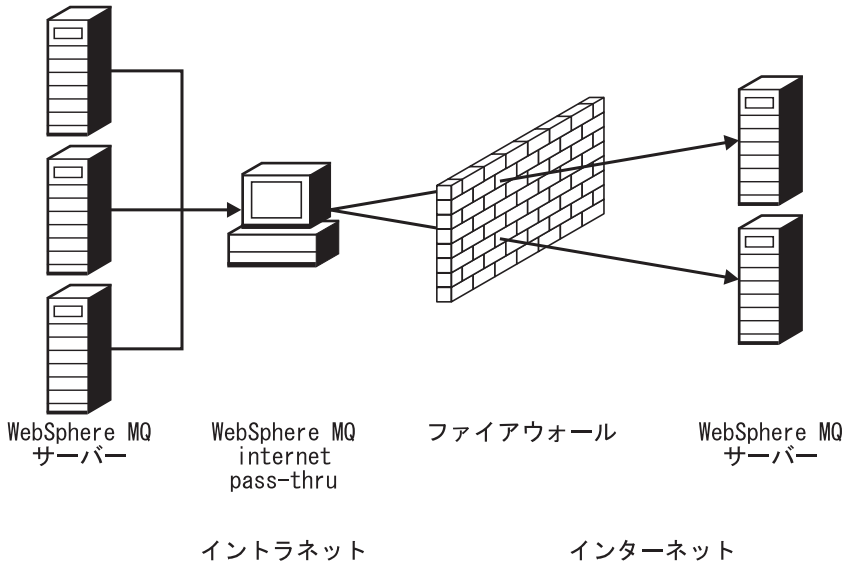

図 1. チャネル・コンセントレーターとしての MQIPT の例

- MQIPT をファイアウォールの「非武装地帯 (DMZ)」 (認識されたトラステッド・インターネット・プロトコル (IP) アドレスを持つマシン上の) に入れた場合は、MQIPT を使って、WebSphere MQ 着信チャネル接続を listen し、次にそれをトラステッド・イントラネットに転送することができます。内部ファイアウォールは、このトラステッド・マシンがインバウンド接続を行えるようにしなければなりません。この構成の場合、MQIPT は、外部からのアクセス要求からは、トラステッド・イントラネット内にある各マシンの本当の IP アドレスが見えないようにしています。このため、MQIPT は単一アクセス・ポイントを提供しています。

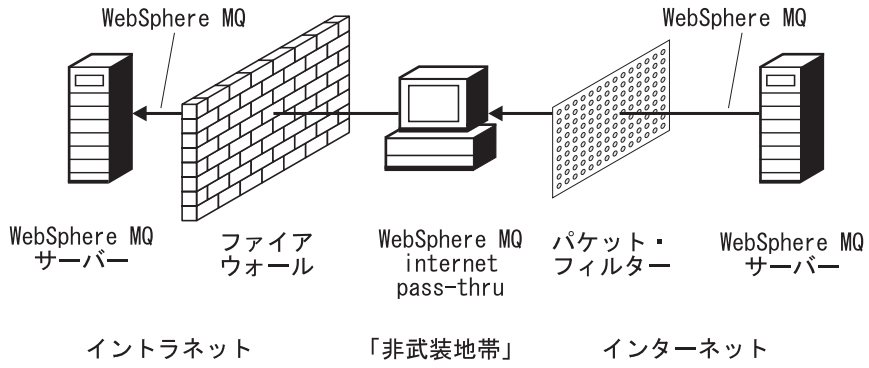

図 2. 「非武装地帯」を持つ MQIPT の例

- 2 つの MQIPT をインライン配置した場合、両者は HTTP または SSL を使用して相互に通信することができます。 HTTP トンネル・フィーチャーを使用すれば、既存の HTTP プロキシーを利用することにより、要求をファイアウォール経由で送信することができます。最初の MQIPT は WebSphere MQ プロトコルを HTTP に挿入し、2 番目の MQIPT は、 WebSphere MQ プロトコルをその HTTP ラッパーから取り出して、それを宛先キュー・マネージャーに転送します。

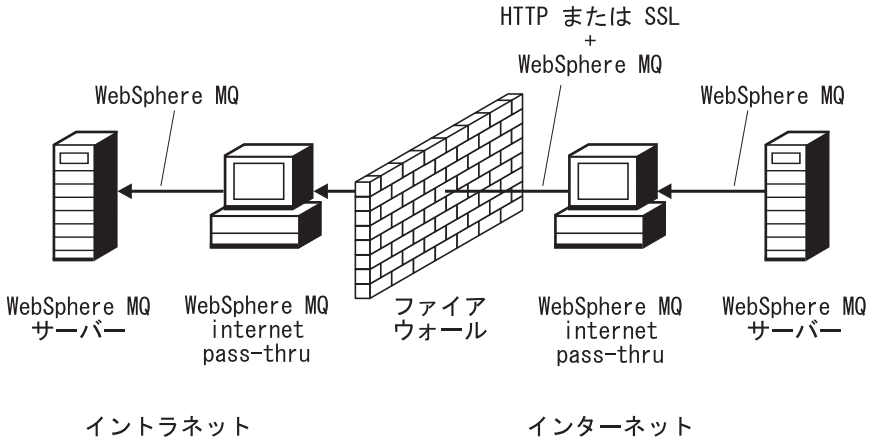

図 3. MQIPT および HTTP トンネル操作の例

- 同様に、要求は、暗号化してからファイアウォール経由で送信することができます。最初の MQIPT はデータを暗号化し、2 番目の MQIPT は、SSL を使用してそれを暗号化解除してから宛先キュー・マネージャーに送信します。

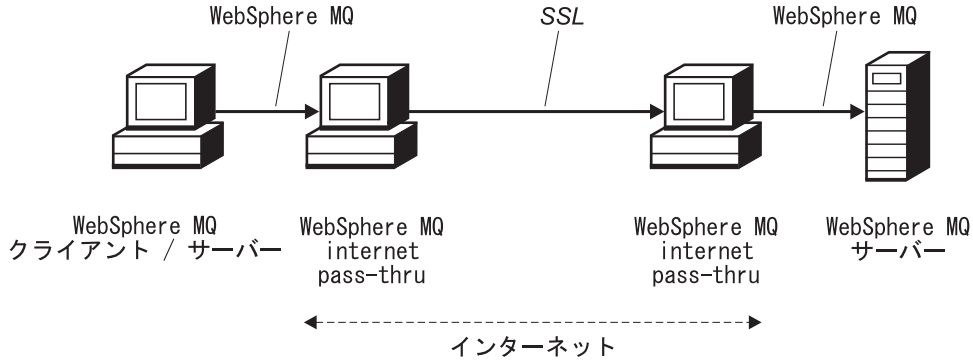

図 4. MQIPT と SSL の例

MQIPT は、データをソースから宛先へ送信する場合、それをメモリーに入れておきます。データがディスクに保管されることはありません (ただし、オペレーティング・システムによってディスクにページングされるメモリーを除きます)。 MQIPT が明示的にディスクにアクセスするのは、構成ファイルを読み取るときと、ログおよびトレース・レコードを書き込むときだけです。

全範囲の WebSphere MQ チャネル・タイプを 1 つまたは複数の MQIPT で使用することができます。通信パスに MQIPT が存在していても、接続された WebSphere MQ コンポーネントの機能特性には影響はありませんが、メッセージ転送のパフォーマンスには多少の影響がある可能性があります。

MQIPT は、WebSphere MQ Publish/Subscribe または WebSphere MQ Integrator メッセージ・ブローカーと一緒に使用できます。

5 ページの図 5 は、WebSphere MQ トポロジーの MQIPT で可能なすべての構成を示しています。この図では、「アウトバウンド接続」側のファイアウォールを超えたところにある HTTP プロキシー、SOCKS プロキシー、および MQIPT マシンがインターネット上で結合される可能性があることを示しています。たとえば、ある

MQIPT マシンは、 1 つまたは複数の SOCKS または HTTP プロキシー・マシン、さらには複数の MQIPT マシンと通信してからその宛先に到達することができます。

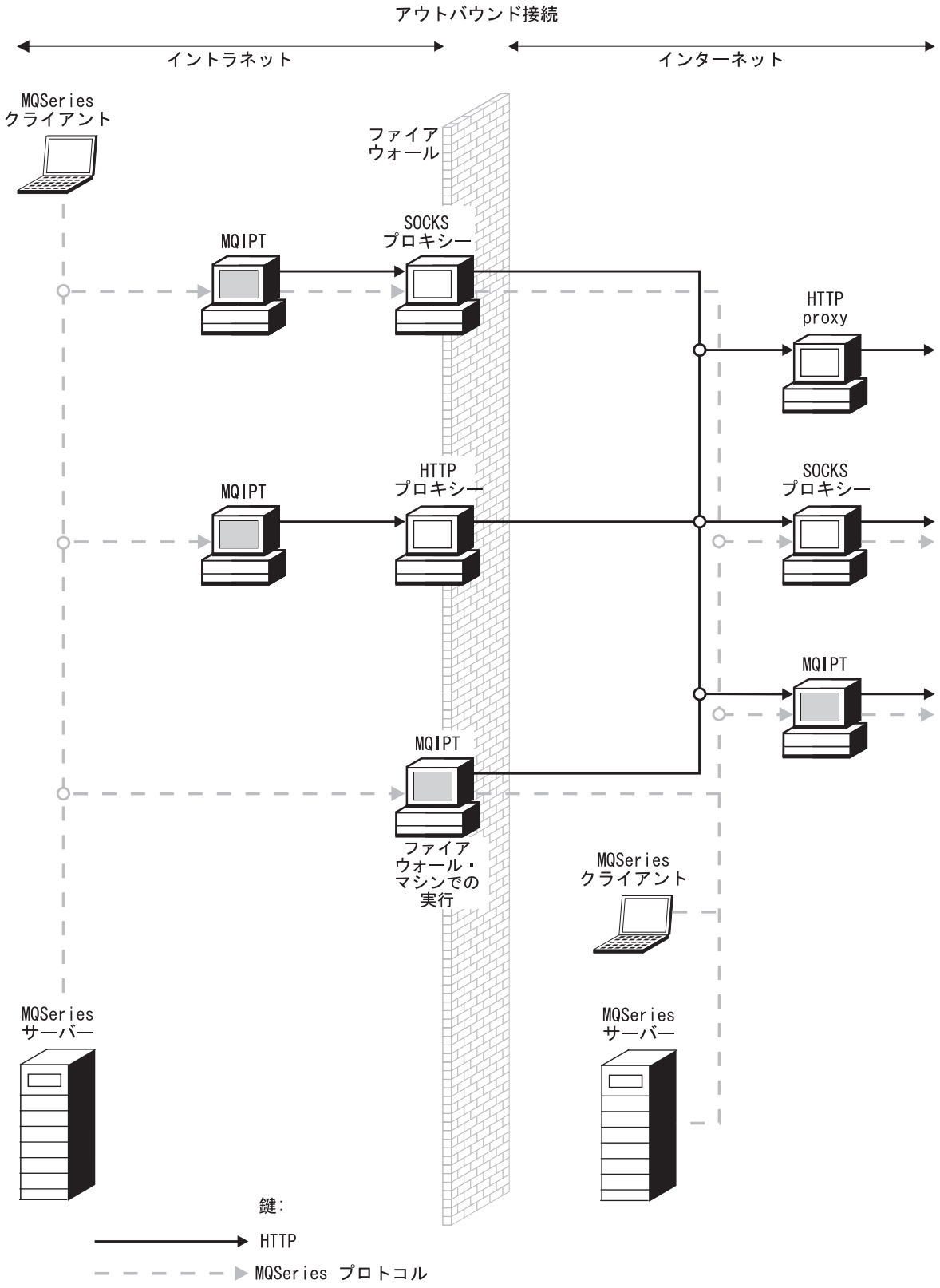

図 5. 可能な MQIPT 構成を示す WebSphere MQ トポロジー (1/2)

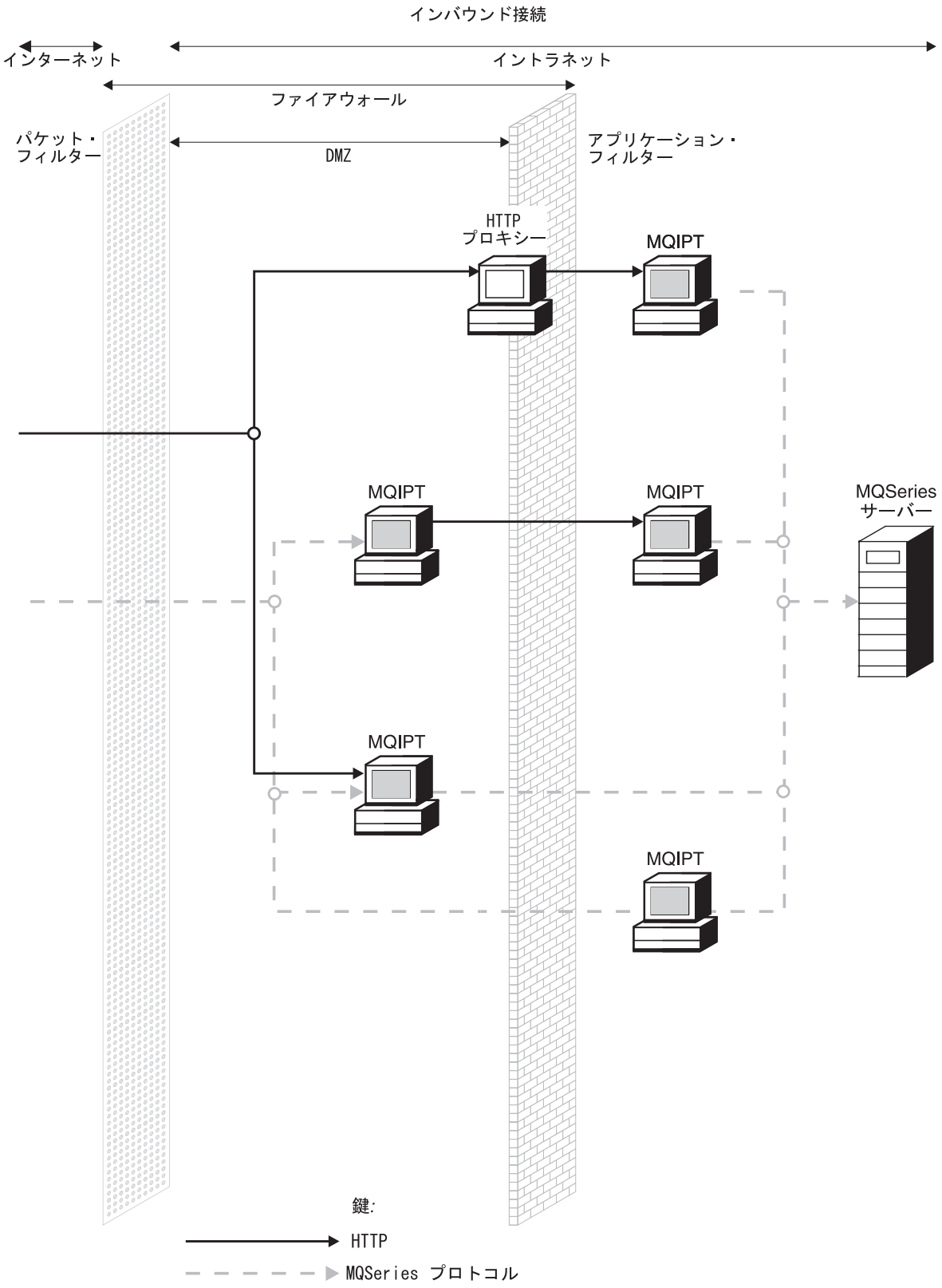

図 5. 可能な MQIPT 構成を示す WebSphere MQ トポロジー (2/2)

第 2 章 internet pass-thru の機能

この章では、internet pass-thru の機能の概要を述べ、その後で以下の項目についてより詳しく説明します。

- 8 ページの『HTTP サポート』
- 9 ページの『SOCKS サポート』
- 9 ページの『SSL サポート』
- 14 ページの『Quality of Service (QoS)』
- 16 ページの『KeyMan』
- 20 ページの『Network Dispatcher サポート』
- 21 ページの『クラスター化』
- 23 ページの『サポートされるチャネル構成』
- 24 ページの『Java Security Manager』
- 26 ページの『正常終了と失敗条件』
- 26 ページの『メッセージの安全性』
- 26 ページの『接続ログ』
- 27 ページの『その他のセキュリティー上の考慮事項』

internet pass-thru の機能の概要

最も単純な構成の MQIPT は、WebSphere MQ プロトコル転送プログラムとして機能します。 MQIPT は、TCP/IP ポートで listen し、WebSphere MQ チャネルからの接続要求を受け入れます。正しい形式の要求を受信した場合、MQIPT は、さらに自分自身と宛先 WebSphere MQ キュー・マネージャー間の TCP/IP 接続を確立します。次に MQIPT は、着信接続から受信したすべてのプロトコル・パケットを宛先キュー・マネージャーに渡し、宛先キュー・マネージャーから受信したプロトコル・パケットを元の着信接続に戻します。

WebSphere MQ プロトコルへ (クライアント / サーバーまたはキュー・マネージャーからキュー・マネージャーへ) の変更は行われません。それは、どちらの側も中間の存在を直接認識していないからです。したがって、新しいバージョンの WebSphere MQ クライアント・コードやサーバー・コードは必要ありません。

MQIPT を使用するためには、宛先キュー・マネージャーのホスト名とポートではなく、MQIPT のホスト名とポートを使用するように呼び出し元チャネルを構成する必要があります。これは WebSphere MQ チャネルの CONNAME プロパティーで定義されます。 MQIPT はチャネル名を調べません。チャネル名は単に宛先キュー・マネージャーに渡されるだけです。クライアント / サーバー・チャネルのユーザー ID やパスワードなどの他の構成フィールドも、同様に、宛先キュー・マネージャーに渡されます。

MQIPT を使用して、1 つまたは複数の宛先キュー・マネージャーへのアクセス権を許可することができます。この機能を働かせるためには、どのキュー・マネージャ

ーに接続するかを MQIPT に指示するメカニズムが用意されていなければなりません。このため、MQIPT は、着信 TCP/IP ポート番号を使用して接続先のキュー・マネージャーを判別します。この操作については、次のパラグラフで説明します。

複数の宛先キュー・マネージャーにアクセスできるようにするには、複数の TCP/IP ポートで listen するように MQIPT を構成します。 listen する各ポートは、MQIPT「経路」を介して宛先キュー・マネージャーにマップされます。 MQIPT 管理者は、最高 100 経路まで定義することができます。これらの経路は、listen する TCP/IP ポートを宛先キュー・マネージャーのホスト名とポートに関連付けます。つまり、宛先キュー・マネージャーのホスト名 (IP アドレス) は発信元のチャネルには決して見えません。各経路は、自分が listen するポートと宛先の間に存在する複数の接続を処理することができます。この場合、これらの接続はそれぞれ独立に機能します。

HTTP サポート

オプションとして、転送するデータ・パケットを HTTP 要求としてエンコードするように MQIPT を構成することができます。 MQIPT は、チャンク操作を伴う HTTP トンネル操作も、チャンク操作を伴わない HTTP トンネル操作もサポートします。

今日の WebSphere MQ チャネルは HTTP 要求を受け入れないため、HTTP 要求を受信してそれを通常の WebSphere MQ プロトコル・パケットに変換するために、2 番目の MQIPT が必要になります。 2 番目の MQIPT は、HTTP ヘッダーを取り去り、着信パケットを元の標準 WebSphere MQ プロトコル・パケットに変換してから、それを宛先キュー・マネージャーに渡します。

チャンク操作を伴わない HTTP トンネル操作を使用する場合は、HTTP 応答が各 HTTP 要求ごとに最初の MQIPT に戻されます。この応答は、宛先キュー・マネージャーからの応答であったりダミーの確認通知であったりします。どちらかの WebSphere MQ システムが一連の WebSphere MQプロトコル・パケットを送信しなければならない場合 (大きなメッセージを転送するときに発生する) は、いくつかの HTTP 要求 / 応答のペアを使用してデータを転送します。これを行うために、MQIPT は追加の要求または応答のフローを挿入します。

チャンク操作を伴う HTTP トンネル操作を使用する場合は、最初のパケットだけを HTTP ヘッダーでラップします。中間のパケットと最後のパケットにはチャンク・ヘッダーがありません。このため、2 番目の MQIPT からのダミーの確認通知を待機する必要がないため、チャンク操作を伴わない HTTP トンネル操作の場合のパフォーマンスよりも多少高いパフォーマンスが得られます。

HTTP を 2 つの MQIPT 間で使用する場合は、HTTP 要求や応答が流れる TCP/IP 接続はパーシスタントになり、メッセージ・チャネルの存続時間中、オープン状態になっています。 MQIPT は、要求 / 応答ペア間の TCP/IP 接続をクローズしないでください。

2 つの MQIPT が HTTP を介して通信している場合、HTTP 要求が長い時間、処理未のままになっていることがあります。たとえば、要求発行者 / サーバー・チャネルにおいて、サーバー・サイドが、新規のメッセージが伝送キューに到着するのを待機している場合です。 WebSphere MQ チャネル・プロトコルは「ハートビート」

メカニズムを備えています。この場合は、待機している側が定期的にハートビート・メッセージを相手側に送信する必要があり (デフォルトのハートビート間隔は 5 分)、MQIPT はこのハートビートを HTTP 応答として使用します。一部のファイアウォールでタイムアウトの問題が発生するのを避けようとして、このチャネル・ハートビートを使用不可にしたり、それを過度に高い値に設定したりしないでください。

HTTP プロキシーによっては、パーシスタント接続を制御するための独自のプロパティー (たとえば、1 つのパーシスタント接続で発行可能な要求の数) を備えているものがあります。 HTTP プロキシーは HTTP 1.1 プロトコルもサポートする必要があります。 IBM WebSphere Caching Proxy を使用するときは、以下のプロパティーをリセットする必要があります。

- 高い値 (たとえば、5000) に設定された MaxPersistenceRequest
- 高い値 (たとえば、12 時間) に設定された PersistentTimeout
- オン に設定された ProxyPersistence

SOCKS サポート

ファイアウォールを介したアウトバウンド接続を作成する場合は、アプリケーションを SOCKS 対応にしておくことによって、すべての接続が SOCKS プロキシーを介して行われ、それによりファイアウォールを介した終了制御点が使用可能になるようにすることができます。

旧リリースの MQIPT では、Java システム・プロパティー `SocksProxyHost` および `SocksProxyPort` を設定することによって SOCKS のサポートを行っていました。しかしこの方法では、MQIPT によって行われたすべての接続が影響を受けるため、すべての経路が同じ SOCKS プロキシーを使用することを余儀なくされました。今回のリリースの MQIPT では、SOCKS V5 のサポートがインプリメントされていますが、これは IPV4 形式アドレスのサポートが使用され、かつユーザー認証はない場合に限られます。

各経路が別々の SOCKS プロキシーと通信できるように構成するには、`SocksClient`、`SocksProxy`、および `SocksProxyPort` プロパティーを使用します。

`SocksServer` プロパティーを使用すれば、各経路を SOCKS サーバー (プロキシー) として機能させることもできます。こうすることによって、SOCKS 化された WebSphere MQ アプリケーションは MQIPT 経由でその宛先に接続できるようになります。このフィーチャーを使用する場合は、宛先と宛先ポートが SOCKS ハンドシェーク中に取得されるため、経路に関して定義された `Destination` および `DestinationPort` プロパティーは無視されます。これは WebSphere MQ クラスター化をサポートするための重要なフィーチャーです。 MQIPT を WebSphere MQ クラスター化で使用する場合の詳細については、21 ページの『クラスター化』を参照してください。

SSL サポート

SSL プロトコルは、不安定な通信チャネルに関する接続セキュリティーを提供し、以下の保証を行います。

通信プライバシー
クライアントとサーバー間で交換するデータを暗号化することにより、接続を私用にする (たとえば、当事者しかデータを理解できないようにする) ことができます。こうすれば、クレジット・カード番号などの私用情報を安全に転送できるようになります。

通信の保全性
接続は信頼できます。メッセージの移送には、安全なハッシュ機能に基づいたメッセージ保全性チェックが伴います。

認証 クライアントはサーバーを認証でき、認証されたサーバーはクライアントを認証することができます。つまり、情報は、意図された当事者間でのみ交換されることが保証されます。認証メカニズムは、ディジタル証明書 (X.509v3 証明書) の交換に基づいています。

SSL プロトコルは、通信者の認証にさまざまなディジタル署名アルゴリズムを使用することができます。 SSL で使用する暗号化、データ機密性のための暗号化、およびメッセージ保全性のためのセキュア・ハッシュは、クライアントとサーバー間で秘密鍵を共用することを前提にしています。 SSL は、秘密鍵の共用を可能にするさまざまな鍵交換メカニズムを備えています。 SSL は、暗号化やハッシュのための各種のアルゴリズムを使用することができます。各種の暗号アルゴリズムがサポートされており、ユーザーは、SSL 暗号スイートを使用してそれらの暗号アルゴリズムを指定します。以下の暗号スイートがサポートされています。

SSL_RSA_EXPORT_WITH_RC4_40_MD5
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5#
SSL_RSA_WITH_3DES_EDE_CBC_SHA
SSL_RSA_WITH_NULL_MD5
SSL_RSA_WITH_NULL_SHA
SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
SSL_DHE_DSS_WITH_3DES__EDE_CBC_SHA
SSL_DHE_RSA_WITH_3DES__EDE_CBC_SHA
SSL_DH_anon_WITH_RC4_40_MD5
SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA
SSL_RSA_WITH_RC4_128_MD5
SSL_RSA_WITH_RC4_128_SHA
SSL_RSA_WITH_DES_CBC_SHA
SSL_DHE_RSA_WITH_DES_CBC_SHA
SSL_DHE_DSS_WITH_DES_CBC_SHA
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA
SSL_DH_anon_WITH_RC4_128_MD5
SSL_DH_anon_WITH_DES_CBC_SHA

SSL ハンドシェーク

SSL ハンドシェーク・プロセスは、SSL クライアントとサーバー間で初期接続要求が出されたときに行われ、そのときには、暗号スイートの認証とネゴシエーションが実行されます。

上記の SSL 暗号スイートは、匿名暗号スイートを除き、すべてサーバー認証が必要であり、クライアント認証が可能になっています。したがって、クライアント認証を要求するようにサーバーを構成することができます。 SSL における通信ピア認証は、公開鍵暗号と X.509v3 ディジタル証明書に基づいて行われます。 SSL プロトコルでの認証を必要とするサイトには、秘密鍵とディジタル証明書 (対応する公開鍵が含まれている) が必要になるほか、そのサイトのアイデンティティー、証明書の有効期間などに関する情報も必要になります。証明書は認証局によって署名されており、このような権限の付いた証明書は署名者証明書と呼ばれます。 1 つまたは複数の署名者証明書が付随している証明書は証明書チェーンを形成します。証明書チェーンの特徴として、最初の証明書 (サイト証明書) から始めて、チェーン内の各証明書の署名を検査するために、その次の署名者証明書に含まれている公開鍵を使用できるという点が挙げられます。

サーバー認証が必要な安全な接続を確立する場合、サーバーは、自分のアイデンティティーを証明するための証明書チェーンをクライアントに送ります。 SSL クライアントは、サーバーを認証できる (たとえば、サーバーのサイト証明書の署名が正しいことを証明できる) 場合にのみ、サーバーへの接続の確立を続行します。その署名が正しいことを証明するためには、SSL クライアントが、サーバー・サイトそのもの、またはサーバーから提供された証明書チェーンの中の少なくとも 1 人の署名者を信用する必要があります。信用できるサイトや署名者の証明書は、この検証を行うためにクライアント・サイドで保持しておく必要があります。

SSL クライアントは、サイト証明書から始めて、サーバーの証明書チェーンを調べます。サイト証明書が信用できるサイトまたは署名者証明書のリポジトリーに入っている場合、または証明書チェーン内の署名者証明書を信用できる署名者証明書のリポジトリーに基づいて検証できる場合は、サイト証明書の署名が有効であると見なします。後者の場合、SSL クライアントは、信用できる署名者証明書から始めてサーバーのサイト証明書に至るまで、証明書チェーンが本当に正しく署名されているかどうか調べます。このプロセスに係る含まれ証明書は、すべて形式の正確さと日付の妥当性の点からも調べられます。これらのどの 1 つの検査にでもパスしないと、サーバーへの接続は拒否されます。サーバー証明書の検査が済めば、クライアントは、その証明書に組み込まれた公開鍵を次の SSL プロトコル・ステップで使用します。 SSL 接続を確立できるのは、サーバーが実際に、対応する秘密鍵を所有している場合のみです。

クライアント認証もこれと同じ手順を踏みます。つまり、SSL サーバーがクライアント認証を必要とする場合、クライアントは、証明書チェーンのアイデンティティーを証明するためにそれをサーバーに送り、サーバーは、信用できるサイトと署名者証明書のリポジトリーに基づいてそのチェーンを検証します。クライアント証明書の検証が済めば、サーバーは、その証明書に組み込まれた公開鍵を次の SSL プロトコル・ステップで使用します。 SSL 接続を確立できるのは、クライアントが実際に、対応する秘密鍵を所有している場合のみです。

SSL プロトコルそれ自体は、極めて高度な通信セキュリティーを備えています。しかし、このプロトコルは、アプリケーションから提供された情報に基づいて作動します。その情報ベースも安全に維持されている場合にのみ、安全な通信という全体的なゴールを達成できます。たとえば、信用できるサイトおよび署名者証明書のリポジトリーが危険にさらされることになれば、非常に安全性の低い通信相手との確実な接続を確立することになる可能性があります。

MQIPT および SSL

SSL V3.0 は、Public Key Cryptography Standards (PKCS) #12 トークンを使用してインプリメントされています。このトークンは、 X509.V3 証明書が含まれた鍵リング・ファイル (.p12 または .pfx のファイル・タイプを持つ) に保管されています。

MQIPT は、接続がどちらの側から始まるかに従って、SSL クライアントとして機能できるか、SSL サーバーとして機能できるかが決まります。クライアントは接続を開始し、サーバーは接続要求を受け入れます。 1 つの MQIPT 経路がクライアントとサーバーの両方として機能することは可能ですが、その場合は、パフォーマンス上の理由から、SSL Proxy Mode フィーチャーを使用することをお勧めします。各 MQIPT 経路は、それぞれ独自の SSL プロパティー・セットを持つように独立して構成することができます。詳細については、 61 ページの『経路セクション参照情報』を参照してください。

トラストの設定

鍵リング・ファイルには、署名者証明書または署名者証明書のチェーンが組み込まれている個人用証明書が入っています。接続を行なうときに認証を使用可能にするには、証明書にトラストの設定が必要です。トラストのレベルには、次の 2 つがあります。

ピアとしてのトラスト
この証明書だけが信用でき、この証明書によって署名された証明書はどれも信用できないことを意味します。

認証局 (CA) としてのトラスト
この証明書によって署名された証明書はすべて信用できることを意味します。

SSLServerKeyRing プロパティーによって識別された、SSL サーバー・サイドの鍵リング・ファイルには、その個人用証明書が入っていなければなりません。SSLServerCAKeyRing プロパティーによって識別された 2 番目の鍵リング・ファイルには、信用できるすべての証明書 (CA またはピア) が入っていなければなりません。 SSLClientKeyRing プロパティーによって識別された鍵リング・ファイルには、その個人用証明書が入っていなければなりません。 SSLClientCAKeyRing プロパティーによって識別された 2 番目の鍵リング・ファイルには、信用できるすべての証明書 (CA またはピア) が入っていなければなりません。鍵リング・ファイルには、CRL (Certification Revocation List) のリストも入れることができます。

MQIPT で提供されるサンプル鍵リング・ファイル (sslSample.pfx) に入っている証明書に類似した自己署名証明書も使用できます。

KeyMan ユーティリティー (ssl サブディレクトリーに入っている) を使用して自己署名証明書を作成し、証明書と鍵リング・ファイルを管理することができます。詳細については、 16 ページの『KeyMan』を参照してください。

すべての鍵リング・ファイルとパスワード・ファイルを保護するために、オペレーティング・システムのセキュリティー・フィーチャーを使用してそれらへの無許可アクセスを防止する必要があります。

SSL のテスト

71 ページの『第 10 章 internet pass-thru の使用開始』では、SSL 接続のテストに使用できるタスクについて説明しています。

証明書や証明書管理テクノロジーが、以下に示すような多くのベンダーから提供されています。

- RSA Security (www.rsasecurity.com)
- Entrust Technologies (www.entrust.com)
- Verisign (www.verisign.com)

SSL エラー・メッセージ

いずれかの SSL メソッド呼び出しで無効なパラメーター値が使用された場合や、間違ったデータが SSL プロトコルに提供された場合は、以下のようなエラー・コードが SSLRuntimeException に表示されることがあります。

表 2. SSLRuntimeException エラー・メッセージ

ID	説明
1	メソッドの使用法が間違っている、あるいは 1 つまたは複数の入力パラメーターが範囲外である
2	提供されたデータを処理できない
3	提供されたデータの署名を検証できない
10	署名者証明書のサブジェクト名が、その証明書の発行者名と一致しない
11	証明書のタイプがサポートされていない
12	有効期間前の証明書が使用されている
13	証明書の有効期限が切れている
14	証明書の署名を検証できない
15	証明書を使用できない
20	クライアントによって提示されたすべての暗号スイートがサーバーでサポートされていない
21	クライアントによって提示された圧縮方法がサーバーでサポートされていない
22	証明書が使用可能でない
23	アルゴリズムまたは形式のタイプがサポートされていない
24	古くなった情報が拒否された
25	証明書が失効した
26	CRL のセットが不完全である (一部のデルタ CRL が欠落している)
27	証明する名前がすでに存在している
28	証明される公開鍵がすでに存在している
29	一部のシリアル番号または鍵 (証明書、CRL) が間違っている

SSL ハンドシェーク・プロトコルの例外が終了すると、SSLException が throw されます。

表 3. SSLException エラー・メッセージ

ID	説明

表 3. *SSLException* エラー・メッセージ *(続き)*

3	SSLContext に定義された接続時間がタイムアウトになったが、ピアからの応答がない
4	SSL ハンドシェーク時に接続がピアによって打ち切られたが、エラー表示が出ない
10	予期しないメッセージを受け取った
20	無効なレコード MAC を含むメッセージを受け取った
30	解凍に失敗した
40	ハンドシェークに失敗した
41	ピアから証明書が送信されない
42	無効な証明書を受け取った
43	サポートされていない証明書を受け取った
44	失効した証明書を受け取った
45	有効期限が切れた証明書を受け取った
46	不明な証明書を受け取った
47	正しくないパラメーターを検出した

Quality of Service (QoS)

IBM WebSphere Edge Server は、Linux プラットフォームで Transactional Quality of Service プラグインを介して帯域幅管理ソリューションを提供します。Transactional Quality of Service (TQoS) とは、ネットワーク・ユーザーに提供される、スループットや遅延などのエレメントで表される全体的なサービスを指します。属性を設定することにより、接続を介して送信されるすべての出力データに QoS を関連付けることができます。これによりポリシー管理者は、特定のサーバーに関連するトラフィックを識別する規則や、このトラフィックに対する固有な DiffServ 制御機能を持つポリシー・アクションを定義することができます。たとえば、インストール先では、クライアント・ブラウズをサポートするサーバー・トラフィックに関連した発信トラフィックではなく、特定量の商品の販売をサポートするサーバー・トラフィックに関連した発信トラフィックを優遇するように指定するポリシーを定義することができます。 MQIPT では、Policy Agent (pagent) をインストールし、それを実行して、Quality of Service (QoS) をインプリメントするだけで済みます。

TQoS ポリシーは、ポリシー構成ファイル (`pagent.conf`) に定義されるか、または LDAP サーバーを使用して定義されます。 TQoS pagent は、ポリシー構成ファイルにアクセスするか、LDAP サーバーを使用するか、あるいはその両方を行って、TQoS ポリシー・エントリーを検索することができます。「*IBM Edge Server Administration Guide*」では、pagent について詳しく説明しています。この資料は、次の URL にあります。

`http://www-3.ibm.com/software/webservers/edgeserver/library.html`

このサイトから HTML をオンラインで表示することも、PDF バージョンをダウンロードすることもできます。この場合、どちらの形式を使っても、TQoS の検索を行えます。

TQoS を持つ WES をどこへダウンロードするかについての詳細が、MQIPT Readme.txt に記載されています。

MQIPT は、libmqiptqos.so というダミー・ライブラリー (lib サブディレクトリーに入っている) が付いて出荷されます。 TQoS のインストールが済んだならば、bin サブディレクトリーの mqipt スクリプトを編集し、WES lib サブディレクトリーを指すように LD_LIBRARY_PATH 環境変数を変更する必要があります。

MQIPT では、pagent をインストールし、それを実行して、Quality of Service (QoS) をインプリメントするだけで済みます。 MQIPT を使用すれば、それぞれの方向に流れるデータ用の経路にアプリケーション優先順位を設定できるため、その経路を使用するすべてのチャネルがこの影響を受けることになります。この優先順位は、MQIPT プロパティー QosToCaller および QosToDest を使用して定義され (詳細については、61 ページの『経路セクション参照情報』を参照)、ここで使用する値は pagent.conf 制御ファイルの ApplicationPriority ポリシー定義と一致しなければなりません。一致するポリシーを pagent が見つけられない場合は、このデータには優先順位が割り当てられません。ポリシーに対する変更は、pagent が再始動されるまで MQIPT に反映されません。ポリシー定義の詳細については、85 ページの『Quality of Service (QoS) の構成』を参照してください。

サーブレット

Application Server に配置できる MQIPT のサーブレット・バージョン (MQIPTServlet と呼ばれる) が使用可能になりました。このバージョンは、「通常の」 MQIPT と同じような機能を持っていますが、1 つの経路しか持っていないような作動をします。 WebSphere MQ チャネルを開始するための着信接続要求は、MQIPTServlet のインスタンスによって処理され、それぞれのインスタンスは、宛先キュー・マネージャーとのパーシスタント接続を維持しています。後続のデータ・フローは、最初の接続要求時に作成されたセッション ID を使って、同じチャネルで維持されます。

MQIPTServlet.war という Web アプリケーション・アーカイブ・ファイルは、Web サブディレクトリーに入っています。この war は、Application Server にインポートする必要があります。

MQIPTServlet を構成するには、web.xml ファイル (Application Server の WEB-INF サブディレクトリーに入っている) にプロパティーを設定します。 MQIPTServlet では、既存の MQIPT プロパティーのサブセットのみが適用できます。以下のプロパティーは MQIPTServlet で使用できます。

- ClientAccess
- ConnectionLog
- MaxLogfileSize
- QMgrAccess
- Trace

接続ログやトレース・ファイルは、LogDir という新規のプロパティーで定義されているディレクトリーに書き込まれます。 MQIPTServlet を開始する前に、このプロパティーを定義することをお勧めします。

MQIPTServlet で使用するリソースの量を制御するために、Application Server 内のアクティブ・セッションの最大数またはサーブレットのインスタンスの数を設定することができます。

MQIPTServlet は、IBM WebSphere Application Server 4.0、Tomcat 3.3、および Tomcat 4.0 を使用してテスト済みです。

構成の例については、 96 ページの『MQIPT サーブレットの構成』を参照してください。

KeyMan

KeyMan というスタンドアロン・ユーティリティーが MQIPT と同梱で出荷されるようになったので、SSL 証明書と鍵リング・ファイルの管理が可能になりました。KeyMan の ZIP は ssl サブディレクトリーに入っています。 KeyMan をインストールするには、このファイルを一時ディレクトリーに UNZIP して、README.txt ファイルに入っている指示を実行します。 KeyMan には多くのフィーチャーが含まれていますが、このセクションでは、テスト証明書の作成と、PKCS#12 トークンが入っている鍵リング・ファイルの管理についてだけ説明します。

KeyMan は、公開鍵インフラストラクチャー (Public Key Infrastructure - PKI) のクライアント・サイドの管理ツールです。 KeyMan は、鍵、証明書、証明書取り消しリスト (CRL)、およびこれらの各アイテムの保管や検索を行うためのそれぞれのリポジトリーを管理します。証明書の全ライフ・サイクルおよびがユーザー証明書のプロセスがサポートされます。

KeyMan は、鍵、証明書、および取り消しリストの集合が入ったリポジトリーを管理します。リポジトリーはトークンと呼ばれます。トークンは、特定のアプリケーション (たとえば、MQIPT) のトラスト設定からなります。通常、トークンには、ユーザーを他のサイトに認証するための秘密鍵とそれに関連する証明書チェーンが含まれています。さらに、トークンは、信用できる通信相手と認証局 (CA) の証明書も保持しています。

サポートされるトークンのタイプ

KeyMan は、異なるタイプのいくつかのトークンをサポートします。トークンとは、鍵、証明書、CRL、およびトラスト設定を保持するリポジトリーを指します。トークンによっては、これらのアイテム・タイプのサブセットしか保管しないものもあります。

PKCS#7 トークン

証明書のセット、および関連する CRL (オプショナル) が入っています。鍵をこのタイプのリポジトリーに保管することはできません。このリポジトリーは認証を必要としません。証明書と CRL は署名によって保護されます。ただし、相手側は特定の PKCS#7 トークンに保管されたアイテムのセットを変更することができます。このタイプのトークンは、予定されたアイテム・セットを何らかのコンテキストで定義するときに使用します。

PKCS#12 トークン

秘密鍵、証明書、および関連する CRL が入っています。これらの内容はユ

ーザー・パスワードによって保護されます。一般公開アイテム (証明書、CRL) と私用アイテム (鍵) は、それぞれ異なる強度のアルゴリズムで保護されています。

PKCS#11 (CryptoKi) リポジトリー

PKCS#11 は、暗号トークンとのインターフェースを定義します。これらのトークンは、鍵と証明書を保管することができます。 CRL の保管はサポートされません。トークンへのアクセスは、個人識別番号 (PIN) によって保護されています。ユーザーは、KeyMan がトークンにアクセスするために使用するトークン特有の PKCS#11 DLL を指定する必要があります。

KeyMan は、PKCS#11 番号 2.01 および 2.10 DLL をサポートします。

PKCS#7 と PKCS#12 はソフト・トークンであり、異なるメディア (たとえば、ファイル、URI、クリップボードなど) から検索することができます。

KeyMan は、不明な形式を持つデータから PKCS#7 トークンを構成できる特殊な機能を備えています。 KeyMan は、このデータをスキャンして X.509 証明書と CRL を見つけ出し、検出された証明書と CRL から PKCS#7 トークンを構成します。証明書や CRL が入った E メールを受け取った場合は、KeyMan の E メール・フォルダーを開くことができるので、KeyMan は X.509 アイテムの抜き出しを試みます。もちろん、これらのデータを元の形式で保管し直すことはできません。抜き出したデータは、PKCS#7 形式を使用してファイルに保管することができます。

サポートされている標準データ形式

KeyMan は、いくつかの標準データ形式をサポートします。それらの意味と使用法について説明します。

PKCS#7

このデータ形式は、証明書と CRL の集合です。 PKCS#7 に記述されている証明書と CRL のセットは保護されません。ただし、個々の証明書と CRL は署名によって保護されます。 PKCS#7 は、予定された証明書と CRL のセットを何らかのコンテキストで定義するたびに使用されます。 Windows システムでは、PKCS#7 ファイルの標準のファイル・サフィックスは .p7r および .p7b です。

PKCS#10

PKCS#10 は認証要求メッセージを定義します。 PKCS#10 には、公開鍵と要求発行者の X.500 名に関する情報が含まれています。このメッセージは、対応する秘密鍵で署名されています。 PKCS#10 メッセージは、2 進数形式と ASCII 対応形式で生成できます。このメッセージは、認証局 (CA) へ送信する必要があります。

PKCS#12

PKCS#12 は、秘密鍵や関連する証明書のインポートとエクスポートを行うために、ブラウザーや Web サーバーによって使用されます。 KeyMan は、これらの PKCS#12 ファイルの読み取り / 書き込みを行うことができます。これらのプログラムは、PKCS#12 の非常に限られたプロファイルしか理解しませんが、KeyMan はもっと一般的な PKCS#12 ファイルを生成することができます。 KeyMan は、秘密鍵、証明書、CRL、および対応するトラスト設定を PKCS#12 ファイルに保管することができます。 PKCS#12

ファイルはパスフレーズ (パスワード) によって保護されます。通常、PKCS#12 トークンには、特定のアプリケーションのためのトラスト・ポリシーが入っています。 IBM BlueZ SSLite の場合、鍵と関連証明書チェーンはクライアント / サーバー認証に使用されます。他の証明書は、該当するトラスト設定に応じて、信用できる CA または信用できるサーバーの役目を果たします。 Windows システムでは、PKCS#12 ファイルの標準のファイル・サフィックスは .p12 および .pfx です。

SPKAC

SignedPublicKeyAndChallenge (SPKAC) は、CA から証明書を要求するためのデータ形式です。この特定の形式は、HTML タグ <keygen> を使用するたびに Netscape によって生成されます。この形式には、署名された公開鍵と質問が入っています。 KeyMan は、このデータ形式を 2 進数形式と Base64 形式で生成することができます。

X.509 V3 証明書

KeyMan は、X.509 V3 証明書を 2 進数形式で読み取ったり、ASCII 防御形式でラップしたりできます。これらのファイルはオープンでき、また KeyMan にインポートすることもできます。また、トークンの個々の証明書をこれらの 2 つの形式で書き込むこともできます (「**Certificate Details (証明書の詳細情報)」-> 「Save Icon (保管アイコン)**」)。 Windows システムでは、X.509 証明書ファイルの標準のファイル・サフィックスは .crt、.cer、および .der です。

X.509 V2 証明書取り消しリスト (CRL)

KeyMan は、X.509 V2 CRL を 2 進数形式で読み取るか、または、ASCII 防御形式でラップすることができます。単一の CRL をオープンすることはできません。 KeyMan は、前から関連する CA 証明書が入っているトークンにだけ CRL をインポートすることができます。単一の CRL を 2 進数形式または ASCII 防御形式で書き込むことができます (「**Certificate details (証明書の詳細情報)」-> 「CRLs details (CRL の詳細情報)」 -> 「Save Icon (保管アイコン)**」)。 Windows システムでは、X.509 CRL ファイルの標準のファイル・サフィックスは .crl です。

KeyMan FAQ

暗号や関連用語に関する一般的な質問については、RSA Laboratories およびその ″Frequently Asked Questions (FAQ) About Today's Cryptography″ を参照してください。以下の FAQ では、KeyMan に関連する質問について説明します。

Netscape や Internet Explorer で生成した PKCS#12 ファイルを KeyMan で読み取ることができますか ?

Netscape ブラウザーや Internet Explorer で生成した PKCS#12 ファイルの内容を保護するパスワードを知っていれば、これらのファイルを KeyMan で読み取ることができます。

Netscape や Internet Explorer で読み取ることができる PKCS#12 ファイルを KeyMan で作成できますか ?

PKCS#12 標準では、自由にアルゴリズムを選択したり、コンテンツを調整したりできます。これらのブラウザーは、可能なすべてのオプションのうち、非常に限られたプロファイルしか受け入れません。 KeyMan は、Netscape や Internet Explorer が読み取ることができる PKCS#12 ファイル

を生成することができます。 KeyMan を使用すれば PKCS#12 についてより多くのことが行えるので、これらのブラウザーが理解できないようなファイルを作成することも可能です。各ブラウザーに共通なプロファイルの場合、公開 / 私用暗号化 (「**Menu Options (メニュー・オプション)**」 **->「PKCS#12 Settings (PKCS#12 の設定)**」を参照) は、それぞれ ″RC2 (40 ビット)″/″DES (168 ビット)″ になっていなければなりません。ちょうど 1 つの私用証明書が PKCS#12 トークンに入っていなければなりません。

私用証明書とはどんなものですか ?

KeyMan は、一致した鍵と証明書を検出すると、この 2 つのアイテムを私用証明書に組み入れます。つまり、どの私用証明書についても、それに対応する秘密鍵も所有することになります。証明書をトークンにインポートすると、KeyMan は、一致する秘密鍵がないか調べ、自動的にその鍵とインポートした証明書を私用証明書に組み入れます。この場合は、KeyMan からダイアログで通知されます。

CA とは何ですか、またピア証明書とは ?

トークンに入っている証明書はトラストを確立します。これらの証明書は、ユーザーが誰を信用しているかを定義しています。トラストの意味や、証明書の正確な評価は、そのトークンを使用するアプリケーションによって異なります。 KeyMan の場合は、証明書について 2 つのタイプのトラスト、すなわち CA とピアをセットアップすることができます。証明書を CA として信用する場合は、この CA によって直接または間接的に署名されたすべての証明書を暗黙に信用することになります。トラスト・レベルを「ピア」に設定すると、この証明書しか信用しないことになります。トラストは、「ピア」証明書によって署名された証明書までは拡張されません。

私用証明書でもなく、CA でもなく、ピア証明書でもないこれらの証明書は、何ですか ?

KeyMan は、各私用証明書ごとに、ルート証明書に至るまでの全チェーンを保管しようとします。これらの証明書はトラストを必要としないため、CA またはピアの証明書の中には出てきません。鍵リング「All Certificate Items (すべての証明書アイテム)」を選択した場合は、これらの証明書を見つけることができます。信用できない証明書にはアイコンがありません。

トークンとは ?

トークンとは、鍵、証明書、および CRL の集まりです。トークンは、何らかのメディア (たとえば、ファイル、URL、ハードウェアの一部など) に保管されます。トークンには、いろいろなタイプといろいろな機能があります。たとえば、ソフトウェア・トークン、ハードウェア・トークン、無保護トークン、パスワードや PIN によって保護されているトークンなど。

鍵リングとは ?

トークンは鍵リングのセットからなっています。特定の鍵リングは、特定のアイテム・セット (たとえば、同一トラスト・レベルの証明書、ユーザーが所有する秘密鍵の証明書、一致する証明書のない鍵など) を識別します。

Network Dispatcher サポート

MQIPT を IBM Network Dispatcher と一緒に使用すれば、カスタム・アドバイザーを使用できるので、多くのサーバーの可用性とロード・バランシングを拡張することができます。このセクションでは、読者が Network Dispatcher とカスタム・アドバイザーについて詳しい知識を持っていることを前提に説明しています。

MQIPT では、2 つのカスタム・アドバイザーが提供されます。これらのカスタム・アドバイザーは、lib サブディレクトリーに入っています。カスタム・アドバイザーをインストールする場合は、「*Network Dispatcher User's Guide*」(GD88-7807) に示されている指示を実行してください。 図 6 は、Network Dispatcher を使用して、MQIPT のポート・アドレス 1414 をモニターする場合の例を示しています。各 MQIPT が同じ構成ファイルを持っていなければならない点に注意してください。

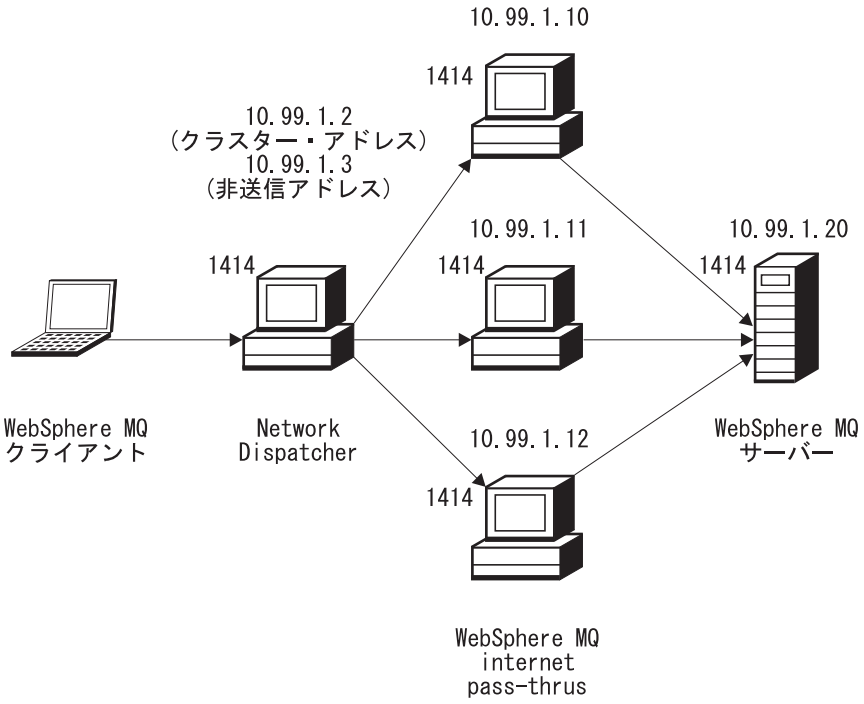

図 6. MQIPT での Network Dispatcher の使用

ポート 1414 およびロード・バランシングされたサーバー・マシンを定義するためのディスパッチャー・コンポーネントの構成方法については、「*Network Dispatcher User's Guide*」を参照してください。 Administration Client のメニュー・オプション、または "ndcontrol" ライン・モード・コマンドのいずれかを使用できます。たとえば、以下のとおりです。

```
ndcontrol port add 10.99.1.2 : 1414
ndcontrol server add 10.99.1.2 : 1414 : 10.99.1.10
ndcontrol server add 10.99.1.2 : 1414 : 10.99.1.11
ndcontrol server add 10.99.1.2 : 1414 : 10.99.1.12
```

MQIPT 構成ファイルの経路定義は、以下のようになります。

```
[route]
ListenerPort=1414
Destination=10.99.1.20
DestinationPort=1414
NDAdvisor=true
```

カスタム・アドバイザーの開始 (および停止) は、コマンド行からしか行えません。たとえば、以下のとおりです。

```
ndcontrol advisor start mqipt_normal 1414
```

このコマンドは、MQIPT アドバイザーを「通常」モードで開始します。このモードの場合、ベース・アドバイザーは独自のタイミングを実行して、各 MQIPT の重み付け係数を計算します。 MQIPT アドバイザーを「置換」モードで使用するには、次の行を MQIPT 経路定義に追加します。

```
NDAdvisorReplaceMode=true
```

また、mqipt_normal カスタム・アドバイザーではなく、mqipt_replace カスタム・アドバイザーも開始する必要があります。たとえば、以下のとおりです。

```
ndcontrol advisor start mqipt_replace 1414
```

アドバイザーを使用して SSL リスナー・ポートをモニターする場合 (つまり、mqipt.conf 構成ファイルにSSLServer=true が指定されている場合) は、「トリガー」ファイルを Network Dispatcher の作業ディレクトリーに入れる必要があります。この「トリガー」ファイルには、モニターする経路に関連する特定の名前が付いています。たとえば、経路 1414 が SSLServer=true となっている場合は、mqipt1414.ssl というファイルを c:¥winnt¥system32 ディレクトリー (Windows NT 上) に入れなければなりません。詳細については、mqipt1414Sample.ssl ファイルを参照してください。

クラスター化

WebSphere MQ クラスターを MQIPT で使用することができます。そのためには、インターネットを拡張するクラスターに各キュー・マネージャーを SOCKS 化し、MQIPT を SOCKS プロキシーとして機能させます。キュー・マネージャーをクラスターに構成するには非常に多くの方法があるため、以下の説明は、「*MQSeries* キュー・マネージャー・クラスター」(SD88-7165) の第 1 部、第 3 章に示されているタスクに基づいて行っています。次の図は、タスク 2『クラスターへの新規 Queue Manager の追加』で定義されている図を拡張したものです。 NEWYORK と CHICAGO は、HOME というクラスターに入っていて、この両者はフル・リポジトリーを保持しています。 NEWYORK、LONDON、および PARIS は、INVENTORY という別のクラスターに入っています。 CHICAGO は、MQIPT を必要としないクラスターに入っているので、SOCKS 化する必要がないことに注意してください。

INVENTORY クラスター内の各キュー・マネージャーは、MQIPT では事実上「非表示」になっています。キュー・マネージャーはすでに SOCKS 化されているため、クラスター送信側チャネルを開始すると、SOCKS プロキシーとして機能する MQIPT を使用して、要求がその宛先に送信されます。通常は、クラスター受信側チャネル上の CONNAME を使用してローカル・キュー・マネージャーを識別しますが、MQIPT と一緒に使用する場合、CONNAME は、ローカル MQIPT とその着信

リスナー・ポートを識別する必要があります。次の図では、すべての着信リスナー・ポート・アドレスが 1414 であり、発信リスナー・ポート・アドレスが 1415 です。

SOCKS 化されたキュー・マネージャーを実行するには 2 つの方法があります。 1 つの方法は、キュー・マネージャーが稼働するマシン全体の SOCKS 化です。もう 1 つの方法は、キュー・マネージャーだけの SOCKS 化です。いずれの方法の場合も、MQIPT を SOCKS プロキシーとして使用してリモート接続だけを行うように SOCKS クライアントを構成し、ユーザー認証を使用不可にする必要があります。 SOCKS サポートを可能にする多数の製品が販売されています。 SOCKS V5 プロトコルをサポートする製品を選択する必要があります。 MQIPT における SOCKS サポートの詳細については、9 ページの『SOCKS サポート』を参照してください。

クラスター・ネットワークの構成方法の例については、98 ページの『MQIPT クラスター化サポートの構成』を参照してください。

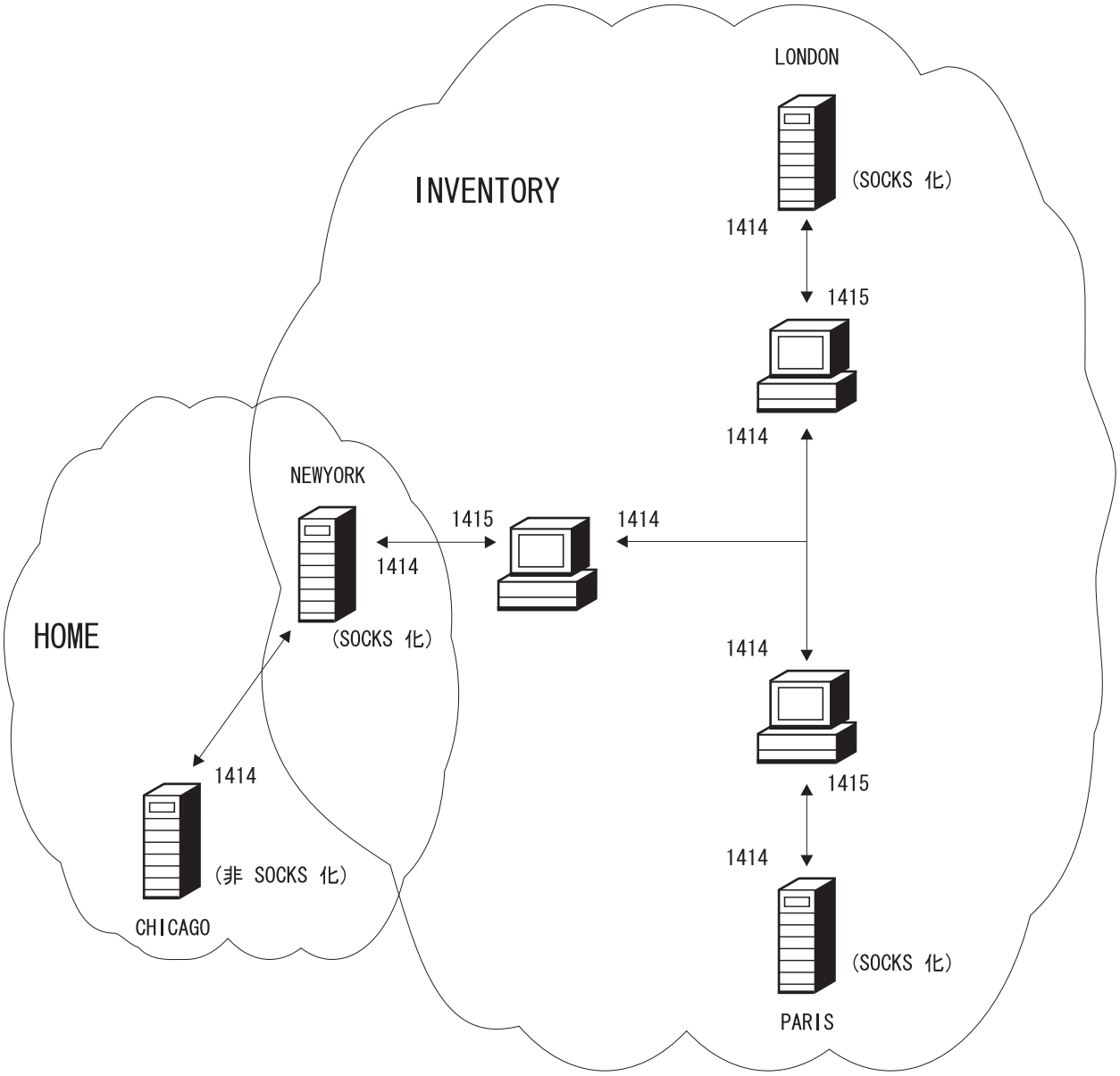

図 7. MQIPT クラスター化のサポート

サポートされるチャネル構成

すべての WebSphere MQ チャネル・タイプがサポートされますが、構成は TCP/IP 接続に限定されます。 WebSphere MQ クライアントやキュー・マネージャーからは、MQIPT は宛先キュー・マネージャーのように見えます。チャネル構成に宛先ホストとポート番号が必要な場合は、MQIPT ホスト名とリスナー・ポート番号が指定されます。

クライアント / サーバー・チャネル

MQIPT は、着信クライアント接続要求を listen してから、それらを転送します (この場合、HTTP トンネル操作または SSL を使用して転送するか、標準の WebSphere MQ プロトコル・パケットとして転送するかのいずれかの方法をと

ります)。 MQIPT が HTTP トンネル操作か SSL を使用する場合は、2 番目の MQIPT との接続を使用して転送します。 HTTP トンネル操作を使用しない場合は、宛先キュー・マネージャーと見なすマシン (ただしこの場合、結局、もう 1 つの MQIPT ということになることもある) との接続を使用して転送します。宛先キュー・マネージャーがクライアント接続を受け入れると、クライアントとサーバー間でパケットがリレーされます。

クラスター送信側 / 受信側チャネル
クラスター送信側チャネルから着信要求を受け取った場合、MQIPT は、キュー・マネージャーが SOCKS 化されていて、真の宛先アドレスは、SOCKS ハンドシェーク・プロセス時に取得されると想定します。 MQIPT は、クライアント接続チャネルの場合とまったく同じ方法で、その要求を次の MQIPT または宛先キュー・マネージャーに転送します。この操作には、自動定義されたクラスター送信側チャネルも使用されます。

送信側 / 受信側
MQIPT は、送信側チャネルから着信要求を受け取った場合、クライアント接続チャネルの場合とまったく同じ方法で、その要求を次の MQIPT または宛先キュー・マネージャーに転送します。宛先キュー・マネージャーは、その着信要求を検証し、該当する場合は、受信側チャネルを開始します。送信側チャネルと受信側チャネル間のすべての通信 (セキュリティー・フローを含む) がリレーされます。

要求発行者 / 送信側
この組み合わせは、上記のタイプと同じ方法で処理されます。接続要求の検証は、宛先キュー・マネージャーのサーバー・チャネルによって行われます。

要求発行者 / 送信側
2 つのキュー・マネージャーを相互に直接接続することは許可されていない場合で、どちらも MQIPT に接続することができ、かつそれからの接続を受け入れることができる場合は、「コールバック」構成が役に立つことがあります。

送信側 / 要求発行者および送信側 / 受信側
これらは、送信側 / 受信側構成と同じような方法で MQIPT によって処理されます。

Java Security Manager

Java Security Manager のサポートは、当初、ソケット接続制御を管理するために、SSL プロキシー・モード・フィーチャーで使用することを目的にインプリメントされましたが、このサポートを他の任意の MQIPT フィーチャーと一緒に使用して別のレベルのセキュリティーを提供することもできます。

MQIPT は、`java.lang.SecurityManager` クラスに定義されたデフォルトの Java Security Manager を使用します。 MQIPT の Java Security Manager フィーチャーは、`SecurityManager` グローバル・プロパティーを使用して使用可能にしたり、使用不可にしたりできます。詳細については、60 ページの『グローバル・セクション参照情報』を参照してください。

Java Security Manager は 2 つのデフォルト・ポリシー・ファイルを使用します。グローバル・システム `$JREHOME/lib/security/java.policy` (ここで、`$JREHOME` は、ユーザーの Java ランタイム環境が入っているディレクトリー) は、ホスト上の仮想

計算機のすべてのインスタンスによって使用されます。 .java.policy という 2 番目のユーザー固有なポリシー・ファイルは、ユーザーのホーム・ディレクトリーに存在することができます。もう 1 つの MQIPT ポリシー・ファイルも使用できます。詳細については、 60 ページの『グローバル・セクション参照情報』を参照してください。もう 1 つのポリシー・ファイルを使用する場合は、policy.allowSystemProperty プロパティーがグローバル・システム・ポリシー・ファイル (java.security) で true に設定されていることを確認します。

ポリシー・ファイルの構文は非常に複雑です。それをテキスト・エディターで変更することは可能ですが、 Java から提供される policytool ユーティリティーを使用して変更することをお勧めします。 policytool ユーティリティーは、$JREHOME/bin ディレクトリーに入っていて、Java 資料に詳しく説明されています。

MQIPT ではサンプル・ポリシー・ファイル (mqiptSample.policy) が提供されていて、MQIPT を実行するにはどの許可を設定する必要があるかが分かるようになっています。誰が MQIPT に接続できるか、MQIPT は誰に接続できるかを制御するためのユーザー独自の特定要件を満たすために、追加 / 変更 / 削除が必要になるのは、java.net.SocketPermission エントリーのみです。このサンプル・ファイルでは、MQIPT がデフォルトのホーム・ディレクトリー、たとえば、c:¥Program Files¥IBM¥Websphere MQ internet pass-thru¥ にインストール済みであることを前提にしています。 MQIPT が別のロケーションにインストールされている場合は、そのことを codeBase および java.io.FilePermission 定義に反映する必要があります。

許可は通常、3 つの属性を使用して定義され、ソケット接続を制御するための値は、以下のとおりです。

クラス許可

java.net.SocketPermission

制御対象の名前

これは hostname:port 形式で構成されています。この場合、この名前の各コンポーネントは、ワイルドカードで指定することができます。ホスト名は、ドメイン・ネームであっても、IP アドレスであっても構いません。ホスト名の左端位置には、アスタリスクを指定することができます。たとえば、harry.company1.com は、以下のいずれかと一致します。

- harry
- harry.company1.com
- *.company1.com
- *
- 123.456.789 (harry.company1.com の IP アドレスであることが前提)

名前のポート・コンポーネントは、単一のポート・アドレスまたはポート・アドレスの範囲で指定できます。たとえば、以下のとおりです。

- 1414 (ポート 1414 のみ)
- 1414- (すべてのポート・アドレスが 1414 以上)
- -1414 (すべてのポート・アドレスが 1414 以下)
- 1-1414 (すべてのポート・アドレスが 1 〜 1414)

許可されたアクション

`java.net.SocketPermission` で使用されるアクションは、以下のとおりです。

- 受け入れ。指定された宛先からの接続を受け入れられるようにする
- 接続。指定された宛先に接続できるようにする
- listen。指定されたポート (複数の場合もある) で接続要求を listen できるようにする
- 解決。DNS ネーム・サービスを使用してドメイン・ネームを IP アドレスに解決できるようにする

Java Security Manager の制御は、`java.security.manager` および `java.security.policy` Java システム・プロパティーを使用して行うことも可能ですが、MQIPT の制御には、SecurityManager および SecurityManagerPolicy プロパティーを使用することをお勧めします。

正常終了と失敗条件

WebSphere MQ チャネルのクローズ (正常または異常) を検出すると、MQIPT は、そのチャネル・クローズを伝搬します。管理者が MQIPT への経路をクローズすると、その経路を通るすべてのチャネルがクローズされます。

MQIPT は、オプションのアイドル・タイムアウト機能を備えています。チャネルがタイムアウトを超過して一定の時間アイドル状態になっていることを検出すると、MQIPT は、この 2 つの接続の即時シャットダウンを行います。

チャネルの両端にある 2 つの WebSphere MQ システムは、これらの異常終了状態をネットワーク障害、または相手側によるチャネルの終了のいずれかと見なします。次に、これらのチャネルは、MQIPT を使用していない場合とまったく同じように、再始動してリカバリーすることができます (障害がプロトコル未確定期間中に発生した場合)。

メッセージの安全性

高速の非持続 WebSphere MQ メッセージを使用するときに、MQIPT 経路が失敗するか、または WebSphere MQ の転送中に MQIPT を再始動すると、メッセージが消失することがあります。この経路を再始動する前に、MQIPT を使用しているすべての WebSphere MQ チャネルが非アクティブ状態になっていることを確認してください。

WebSphere MQ メッセージとチャネルの詳細については、「*MQSeries 相互通信*」(SC88-7775) を参照してください。

接続ログ

MQIPT は、すべての成功および失敗接続試行のリストを収めた接続ログ機能を提供します。この機能の制御は、 `ConnectionLog` および `MaxLogFileSize` プロパティーを使用して行います。詳細については、60 ページの『グローバル・セクション参照情報』を参照してください。

MQIPT を開始するたびに、新規の接続ログが作成され、識別のために、ファイル名に現在のタイム・スタンプが入れられます。たとえば、以下のとおりです。

```
mqiptYYYYMMDDHHmmSS.log
```

ここで、

- YYYY は年
- MM は月
- DD は日
- HH は時間
- mm は分
- SS は秒

監査の目的で、これらのログ・ファイルは消去されません。これらのファイルの管理や、これらが不要になったときの削除は、MQIPT 管理者が行います。

その他のセキュリティー上の考慮事項

SSL を使用しないことに決定した場合は、MQIPT からチャネル・セキュリティー・フローが提供されるので、WebSphere MQ チャネル出口ルーチンを使用して、チャネル全体にわたり端から端までセキュリティーを提供することができます。

MQIPT は、このほかにも、設計者が安全なソリューションを作成する際に役立ついくつかの機能を提供します。それは、以下のとおりです。

- 内部ネットワーク内の多くのクライアントが発信接続を試行している場合は、これらのクライアントはすべて、ファイアウォールの内部にある MQIPT を通過することができます。このため、ファイアウォール管理者は、MQIPT マシンだけへの外部アクセス権を付与する必要があります。
- MQIPT は、自分が SOCKS プロキシーとして機能していない限り、構成ファイルに明示的に構成されているキュー・マネージャーにのみ接続することができます。
- MQIPT は、自分が送受信するメッセージが有効であり、WebSphere MQ プロトコルに準拠しているか調べます。こうすることによって、MQIPT が、WebSphere MQ プロトコルの外側のセキュリティー・アタックに使用されるのを防止することができます。 MQIPT が SSL プロキシーとして機能している場合に、すべての WebSphere MQ データとプロトコルが暗号化されていれば、MQIPT は初期 SSL ハンドシェークしか保証できません。このような場合は、Java Security Manager を使用することをお勧めします。 24 ページの『Java Security Manager』を参照してください。
- これによって、チャネル出口ルーチンで、独自のエンドツーエンド・セキュリティー・プロトコルを実行することができます。
- MQIPT を使用すれば、MaxConnectionThreads プロパティーを設定して、着信要求の総数を制限することができます。こうすれば、攻撃を受けやすい内部キュー・マネージャーをサービス妨害アタックから保護するのに役立ちます。

MQIPT の mqipt.conf 構成ファイルは内部ホストへのアクセスを制御するので、このファイルを保護する必要があります。また、コマンド・ポート (それが使用可能

になっている場合) への無許可アクセスを防止する必要があります。そのようなアクセスにより、外部から MQIPT をシャットダウンすることができるからです。

第 3 章 先行バージョンからのアップグレード

MQIPT をバージョン 1.1 からバージョン 1.2 へアップグレードするには、以下のステップを実行します。

1. mqipt.conf 構成ファイルのコピーをとり、それを MQIPT ホーム・ディレクトリー以外のロケーションに保管します。
2. 次のコマンドを実行して、MQIPT を停止します。

   ```
   mqiptAdmin -stop
   ```

3. MQIPT がサービスとしてインストールされている場合は、それを除去してから MQIPT をアンインストールしなければなりません。

   ```
   mqiptService -remove
   ```

4. MQIPT のアンインストール・プログラムを実行します。
5. MQIPT V1.2 のインストールが済んだならば、保管済み構成ファイルを MQIPT ホーム・ディレクトリーにコピーします。新規の mqiptSample.conf ファイルには、使用可能な新規のプロパティーが示されています。
6. MQIPT Administration GUI を使用して、MQIPT に対する変更を管理します。V1.1 の構成ファイルはこの GUI と互換性があります。

新規構成オプション

以下のプロパティーは、バージョン 1.2 で初めて取り入れられたものです。

LogDir
QoS
QosToDest
QosToCaller
SecurityManager
SecurityManagerPolicy
ServletClient
SocksClient
SocksServer
SocksProxyHost
SocksProxyPort
SSLProxyMode
UriName

これらのすべてのプロパティーに関する参照情報については、 57 ページの『構成参照情報』を参照してください。

第 4 章 Windows での internet pass-thru のインストール

この章では、Windows NT、Windows 2000、または Windows XP システムで MQIPT をインストールする方法について説明します。

- 『ファイルのダウンロードとインストール』
- 32 ページの『internet pass-thru のセットアップ』
- 32 ページの『コマンド行からの internet pass-thru の開始』
- 33 ページの『コマンド行からの Administration Client の開始』
- 34 ページの『Windows サービス制御プログラムの使用』
- 34 ページの『Windows サービスとしての internet pass-thru のアンインストール』
- 34 ページの『internet pass-thru のアンインストール』

ファイルのダウンロードとインストール

MQIPT は、以下の URL の WebSphere MQ SupportPac Web ページからダウンロードします。

`http://www.ibm.com/software/ts/mqseries/downloads`

ダウンロードの指示を実行してください。

コマンド・プロンプトをオープンし、`ms81_nt.zip` を一時ディレクトリーに解凍します。 `setup.exe` を実行し、オンライン指示に従います。

MQIPT は、管理者権限を持つユーザーがインストールしなければなりません。

MQIPT には、以下の表に示されているファイルと、その次の表に示されている Administration Client GUI 用のファイル (別個にインストール可能なフィーチャーとして出荷される) が含まれています。

ファイル	目的
Readme.txt	資料に記載されていない最新情報
mqiptSample.conf	サンプル構成ファイル
ssl¥sslSample.pfx	テスト鍵リング・ファイル
ssl¥sslSample.pwd	テスト鍵リング・ファイル用のパスワード・ファイル
ssl¥sslCAdefault.pfx	サンプル認証局 (CA) 鍵リング・ファイル
ssl¥sslCAdefault.pwd	サンプル認証局 (CA) 鍵リング・ファイル用のパスワード・ファイル
ssl¥KeyMan.zip	KeyMan ユーティリティー
lib¥MQipt.jar	ランタイム、クラス、およびプロパティー・ファイルが入っている
lib¥ADV_mqipt_normal. class	「通常」モード用 Network Dispatcher アドバイザー
lib¥ADV_mqipt_replace. class	「置換」モード用 Network Dispatcher アドバイザー

ファイル	目的
lib¥mqipt1414Sample.ssl	Network Dispatcher アドバイザー用のサンプル・トリガー・ファイル
bin¥mqipt.bat	コマンド行から MQIPT を実行するためのショートカット
bin¥mqiptAdmin.bat	MQIPT を停止し、ファイル情報をリフレッシュするためのショートカット
bin¥mqiptservice.exe	MQIPT を Windows Service Control Manager に追加したり、除去したりするためのもの
bin¥mqiptVersion.bat	MQIPT のバージョン番号の表示
web¥MQIPTServlet.war	サーブレット・バージョン用の Web アーカイブ・ファイル
doc¥<lang>¥pdf¥<filename>.pdf	PDF 形式の「*internet pass-thru*」マニュアル。ソフトコピー文書の詳細については、 xiii ページの『参照文献』を参照。
doc¥<lang>¥html¥<filename>.zip	HTML 形式の「*internet pass-thru*」マニュアルのマスター・ファイル。ソフトコピー文書の詳細については、 xiii ページの『参照文献』を参照。

Administration Client GUI フィーチャーに関連するファイルは、以下のとおりです。

ファイル	目的
lib¥guiadmin.jar	ランタイム、クラス、およびプロパティー・ファイルが入っている
bin¥mqiptGui.bat	コマンド行から Administration Client を実行するためのショートカット
bin¥customSample. properties	Administration Client の外観およびアクセシビリティーをカスタマイズするためのサンプル・ファイル

インストーラーは、`MQipt.jar` および `guiadmin.jar` ファイルのロケーションでシステム CLASSPATH 環境変数を更新します。

internet pass-thru のセットアップ

MQIPT を初めて開始する場合は、その前に、`mqiptSample.conf` サンプル構成ファイルを `mqipt.conf` にコピーしてください。構成と管理については、 51 ページの『第 9 章 internet pass-thru の管理と構成』を参照してください。

コマンド行からの internet pass-thru の開始

コマンド・プロンプトをオープンし、ディレクトリーを `bin` ディレクトリーに変えて、`mqipt` を実行します。たとえば、以下のとおりです。

```
c:
cd ¥mqipt¥bin
mqipt ..
```

Windows の「Start (スタート)」->「Programs (プログラム)」メニューからも MQIPT を開始できます。

オプションを指定しないで mqipt スクリプトを実行すると、 “.” のデフォルト・ロケーションが構成ファイルに使用されます (mqipt.conf)。異なるロケーションを指定するには、次のようにします。

```
mqipt <directory name>
```

MQIPT の状況を示すメッセージがコンソールに表示されます。エラーが起こった場合は、 105 ページの『問題判別』を参照してください。以下のメッセージは、MQIPT が正常に開始された場合の例です。

```
5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
MQCPI004 Reading configuration information from c:¥mqipt¥mqipt.conf
MQCPI008 Listening for control commands on port 1881
MQCPI011 The path c:¥mqipt¥logs will be used to store the log files
MQCPI006 Route 1418 has started and will forward messages to :
MQCPI034 ....mqserver.company4.com(1414)
MQCPI035 ....using MQ protocols
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....mqipt.company2.com(1415)
MQCPI035 ....using MQ protocols
MQCPI036 ....SSL Client side enabled with properties :
MQCPI031 ......cipher suites <null>
MQCPI032 ......keyring file c:¥mqipt¥KeyMan.pfx
MQCPI038 ......distinguished name(s) CN=*Doe O=IBM OU=* L=* ST=* C=*
```

MQIPT を初めて呼び出すときは、以下の mqipt ホーム・ディレクトリーのサブディレクトリーが自動的に作成されます。

- 接続ログが保管されている ″logs″ ディレクトリー
- 任意の First Failure Support Technology™(FFST™) とトレース・レコードが書き込まれる ″errors″ ディレクトリー

コマンド行からの Administration Client の開始

コマンド・プロンプトをオープンし、ディレクトリーを bin ディレクトリーに変えて、mqiptGui を実行します。たとえば、以下のとおりです。

```
c:
cd ¥mqipt¥bin
mqiptGui
```

SOCKS プロキシーを使用して、Administration Client がファイアウォール経由で外部の MQIPT に接続できるようにするには、以下のように、ホスト名またはアドレス、およびポート番号を指定します。

```
mqiptGui <socksHostName <socksPort>>
```

デフォルトの socksPort は 1080 です。

Administration Client の状況が、Administration Client のメイン・ウィンドウにメッセージで示されます。

Windows サービス制御プログラムの使用

別個のサービス制御プログラム (mqiptservice.exe) が提供されるので、MQIPT を Windows サービスとして管理したり開始したりできるようになります。

mqiptservice.exe は、以下のようなコマンド行引き数をとります。

mqiptservice -install *path*
サービスを Windows サービス・パネル上に手動サービスとして表示するように、そのサービスをインストールして登録します。サービス・パネルへ進み、設定を “automatic” に変更して、システム開始時に MQIPT が自動的に開始されるようにします。このサービスをインストールしたならば、Windows をリブートする必要があります。パス・パラメーター (指定が必要) は、mqipt.conf 構成ファイルが入っているディレクトリーへの完全修飾パスです。このパス名にブランクが含まれている場合は、その名前を引用符で囲んでください。

mqiptservice -remove
サービスを除去して、サービス・パネルに表示されないようにします。

mqiptservice ?
有効な引き数をリストする米国英語のヘルプ・メッセージを表示します。

同一コマンドに「インストール」と「除去」の両方を指定すると、エラーになります。

Windows は、引き数のない mqiptservice プログラムを内部で呼び出します。ユーザーが引き数のないコマンド行からそれを呼び出すと、プログラムがタイムアウトになり、エラーが戻されます。

MQIPT サービスを開始すると、アクティブなすべての MQIPT 経路が始動します。それを停止すると、すべての経路が即時シャットダウンされます。

注: システムの PATH 環境変数には、JNI ランタイム・ライブラリーのロケーションが入っていなければなりません。 jvm.dll ファイルは、JDK の classics サブディレクトリーに入っています。

Windows サービスとしての internet pass-thru のアンインストール

サービスとしての MQIPT をアンインストールするには、まず、Windows サービス・パネルからそれを停止します。次に、コマンド・プロンプトをオープンして、MQIPT の bin サブディレクトリーへ進み、以下のように入力します。

```
mqiptservice -remove
```

internet pass-thru のアンインストール

システムから MQIPT をアンインストールする前に、上記のようにして、Windows サービスとしてのそれを除去します。次に、Windows の「Start (スタート)」メニューからアンインストール・プロセスを実行します。

第 5 章 Sun Solaris での internet pass-thru のインストール

この章では、Sun Solaris システムで MQIPT をインストールする方法について説明します。

- 『ファイルのダウンロードとインストール』
- 36 ページの『internet pass-thru のセットアップ』
- 36 ページの『コマンド行からの internet pass-thru の開始』
- 37 ページの『internet pass-thru の自動開始』
- 37 ページの『コマンド行からの Administration Client の開始』
- 38 ページの『internet pass-thru のアンインストール』

ファイルのダウンロードとインストール

MQIPT は、以下の URL の WebSphere MQ SupportPac Web ページからダウンロードします。

```
http://www.ibm.com/software/ts/mqseries/downloads
```

ダウンロードの指示を実行してください。

ルート としてログインし、ms81_sol.tar.Z を解凍して一時ディレクトリーに入れます。次の例のように、pkgadd コマンドを実行します。

```
login root
cd /tmp
uncompress -fv ms81_sol.tar.Z
tar xvf ms81_sol.tar
pkgadd -d . mqipt
```

この例では、ms81_sol.tar.Z が /tmp ディレクトリーに入っていることを前提にしています。

MQIPT には、以下の表に示されているファイル (Administration Client GUI のファイルを含む) が入っています。

ファイル	目的
Readme.txt	資料に記載されていない最新情報
mqiptSample.conf	サンプル構成ファイル
ssl/sslSample.pfx	テスト鍵リング・ファイル
ssl/sslSample.pwd	テスト鍵リング・ファイル用のパスワード・ファイル
ssl/sslCAdefault.pfx	サンプル認証局 (CA) 鍵リング・ファイル
ssl/sslCAdefault.pwd	サンプル認証局 (CA) 鍵リング・ファイル用のパスワード・ファイル
ssl/KeyMan.zip	KeyMan ユーティリティー
lib/MQipt.jar	ランタイム、クラス、およびプロパティー・ファイルが入っている
lib/ADV_mqipt_normal. class	「通常」モード用 Network Dispatcher アドバイザー

ファイル	目的
lib/ADV_mqipt_replace. class	「置換」モード用 Network Dispatcher アドバイザー
lib/mqipt1414Sample.ssl	Network Dispatcher アドバイザー用のサンプル・トリガー・ファイル
bin/mqipt	コマンド行から MQIPT を実行するためのショートカット
bin/mqiptAdmin	MQIPT を停止し、ファイル情報をリフレッシュするためのショートカット
bin/mqiptVersion	MQIPT のバージョン番号の表示
bin/mqiptService	システム始動時に MQIPT が自動的に開始されるようにするための MQIPT のインストール
bin/mqiptEnv	mqipt.jar ファイルのロケーションを定義し、他のスクリプトでのみ使用する。
web/MQIPTServlet.war	サーブレット・バージョン用の Web アーカイブ・ファイル
doc/<lang>/pdf/ <filename>.pdf	PDF 形式の「*internet pass-thru*」マニュアル。ソフトコピー文書の詳細については、 xiii ページの『参照文献』を参照。
doc/<lang>/html/ <filename>.zip	HTML 形式の「*internet pass-thru*」マニュアルのマスター・ファイル。ソフトコピー文書の詳細については、 xiii ページの『参照文献』を参照。
lib/mqiptGui.jar	Administration Client GUI 用のランタイム、クラス、およびプロパティー・ファイルが入っている
bin/mqiptGui	コマンド行から Administration Client GUI を実行するためのショートカット
bin/customSample. properties	Administration Client の外観およびアクセシビリティーをカスタマイズするためのサンプル・ファイル

internet pass-thru のセットアップ

MQIPT を初めて開始する場合は、その前に、mqiptSample.conf サンプル構成ファイルを mqipt.conf にコピーしてください。構成と管理については、 51 ページの『第 9 章 internet pass-thru の管理と構成』を参照してください。

コマンド行からの internet pass-thru の開始

ルート としてログインし、ディレクトリーを bin ディレクトリーに変えます。たとえば、以下のとおりです。

```
cd /opt/mqipt/bin
mqipt ..
```

オプションを指定しないで mqipt スクリプトを実行すると、“.” のデフォルト・ロケーションが構成ファイル (mqipt.conf) に使用されます。異なるロケーションを指定するには、次のようにします。

```
mqipt <directory name>
```

MQIPT の状況を示すメッセージがコンソールに表示されます。エラーが起こった場合は、 105 ページの『問題判別』を参照してください。以下のメッセージは、MQIPT が正常に開始された場合の例です。

```
5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
MQCPI004 Reading configuration information from /opt/mqipt/mqipt.conf
MQCPI008 Listening for control commands on port 1881
MQCPI011 The path /opt/mqipt/logs will be used to store the log files
MQCPI006 Route 1418 has started and will forward messages to :
MQCPI034 ....mqserver.company4.com(1414)
MQCPI035 ....using MQ protocols
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....mqipt.company2.com(1415)
MQCPI035 ....using MQ protocols
MQCPI036 ....SSL Client side enabled with properties :
MQCPI031 ......cipher suites <null>
MQCPI032 ......keyring file /opt/mqipt/KeyMan.pfx
MQCPI038 ......distinguished name(s) CN=*Doe O=IBM OU=* L=* ST=* C=*
```

MQIPT を初めて呼び出すときは、mqipt ホーム・ディレクトリーの以下のサブディレクトリーが自動的に作成されます。

- 接続ログが保管されている ″logs″ ディレクトリー
- 任意の First Failure Support Technology (FFST) とトレース・レコードが書き込まれる ″errors″ ディレクトリー

internet pass-thru の自動開始

システム開始時に MQIPT が自動的に開始されるようにするには、mqiptService スクリプトを実行します。たとえば、以下のとおりです。

```
cd /opt/mqipt/bin
mqiptService -install
```

MQIPT が自動的に開始されないようにするには、次のようにします。

```
cd /opt/mqipt/bin
mqiptService -remove
```

コマンド行からの Administration Client の開始

コマンド・プロンプトをオープンし、ディレクトリーを bin ディレクトリーに変えて、mqiptGui を実行します。たとえば、以下のとおりです。

```
cd /opt/mqipt/bin
mqiptGui
```

Administration Client がファイアウォール経由で外部の MQIPT に接続できるようにするには、以下のように、ホスト名またはアドレス、およびポート番号を指定します。

```
mqiptGui <socksHostName <socksPort>>
```

デフォルトの socksPort は 1080 です。

Administration Client の状況が、Administration Client のメイン・ウィンドウにメッセージで示されます。

internet pass-thru のアンインストール

37 ページの『internet pass-thru の自動開始』に説明されているように、MQIPT をシステムからアンインストールする前に、それが自動的に開始されないようにしてください。 ルート としてログインし、次のように pkgrm コマンドを実行します。

```
pkgrm mqipt
```

第 6 章 AIX での internet pass-thru のインストール

この章では、AIX システムで MQIPT をインストールする方法について説明します。

- 『ファイルのダウンロードとインストール』
- 40 ページの『internet pass-thru のセットアップ』
- 40 ページの『コマンド行からの internet pass-thru の開始』
- 41 ページの『internet pass-thru の自動開始』
- 41 ページの『コマンド行からの Administration Client の開始』
- 42 ページの『internet pass-thru のアンインストール』

ファイルのダウンロードとインストール

MQIPT は、次の URL の WebSphere MQ SupportPac Web ページからダウンロードします。

```
http://www.ibm.com/software/ts/mqseries/downloads
```

ダウンロードの指示を実行してください。

ルート としてログインし、ms81_aix.tar.Z を解凍して一時ディレクトリーに入れます。次の例のように、installp コマンドを実行します。

```
cd /tmp
uncompress -fv ms81_aix.tar.Z
tar xvf ms81_aix.tar
installp -d . -a mqipt-RT
```

この例では、ms81_aix.tar.Z が /tmp ディレクトリーに入っていることを前提にしています。

MQIPT には、以下の表に示されているファイル (Administration Client GUI のファイルを含む) が入っています。

ファイル	目的
Readme.txt	資料に記載されていない最新情報
mqiptSample.conf	サンプル構成ファイル
ssl/sslSample.pfx	テスト鍵リング・ファイル
ssl/sslSample.pwd	テスト鍵リング・ファイル用のパスワード・ファイル
ssl/sslCAdefault.pfx	サンプル認証局 (CA) 鍵リング・ファイル
ssl/sslCAdefault.pwd	サンプル認証局 (CA) 鍵リング・ファイル用のパスワード・ファイル
ssl/KeyMan.zip	KeyMan ユーティリティー
lib/MQipt.jar	ランタイム、クラス、およびプロパティー・ファイルが入っている
lib/ADV_mqipt_normal. class	「通常」モード用 Network Dispatcher アドバイザー

ファイル	目的
lib/ADV_mqipt_replace. class	「置換」モード用 Network Dispatcher アドバイザー
lib/mqipt1414Sample.ssl	Network Dispatcher アドバイザー用のサンプル・トリガー・ファイル
bin/mqipt	コマンド行から MQIPT を実行するためのショートカット
bin/mqiptAdmin	MQIPT を停止し、ファイル情報をリフレッシュするためのショートカット
bin/mqiptVersion	MQIPT のバージョン番号の表示
bin/mqiptService	システム始動時に MQIPT が自動的に開始されるようにするための MQIPT のインストール
bin/mqiptEnv	mqipt.jar ファイルのロケーションを定義し、他のスクリプトでのみ使用する。
web/MQIPTServlet.war	サーブレット・バージョン用の Web アーカイブ・ファイル
doc/<lang>/pdf/ <filename>.pdf	PDF 形式の *internet pass-thru*。ソフトコピー文書の詳細については、 xiii ページの『参照文献』を参照。
doc/<lang>/html/ <filename>.zip	HTML 形式の「*internet pass-thru*」マニュアルのマスター・ファイル。ソフトコピー文書の詳細については、 xiii ページの『参照文献』を参照。
lib/mqiptGui.jar	ランタイム、クラス、およびプロパティー・ファイルが入っている
bin/mqiptGui	コマンド行から Administration Client を実行するためのショートカット
bin/customSample. properties	Administration Client の外観およびアクセシビリティーをカスタマイズするためのサンプル・ファイル

internet pass-thru のセットアップ

MQIPT を初めて開始する場合は、その前に、mqiptSample.conf サンプル構成ファイルを mqipt.conf にコピーしてください。構成と管理については、 51 ページの『第 9 章 internet pass-thru の管理と構成』を参照してください。

コマンド行からの internet pass-thru の開始

ルート としてログインし、ディレクトリーを bin ディレクトリーに変えます。たとえば、以下のとおりです。

```
cd /usr/opt/mqipt/bin
mqipt ..
```

オプションを指定しないで mqipt スクリプトを実行すると、“.” のデフォルト・ロケーションが構成ファイル (mqipt.conf) に使用されます。異なるロケーションを指定するには、次のようにします。

```
mqipt <directory name>
```

MQIPT の状況を示すメッセージがコンソールに表示されます。エラーが起こった場合は、 105 ページの『問題判別』を参照してください。以下のメッセージは、MQIPT が正常に開始された場合の例です。

```
5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
MQCPI004 Reading configuration information from /usr/opt/mqipt/mqipt.conf
MQCPI008 Listening for control commands on port 1881
MQCPI011 The path /usr/opt/mqipt/logs will be used to store the log files
MQCPI006 Route 1418 has started and will forward messages to :
MQCPI034 ....mqserver.company4.com(1414)
MQCPI035 ....using MQ protocols
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....mqipt.company2.com(1415)
MQCPI035 ....using MQ protocols
MQCPI036 ....SSL Client side enabled with properties :
MQCPI031 ......cipher suites <null>
MQCPI032 ......keyring file /usr/opt/mqipt/KeyMan.pfx
MQCPI038 ......distinguished name(s) CN=*Doe O=IBM OU=* L=* ST=* C=*
```

MQIPT を初めて呼び出すときは、mqipt ホーム・ディレクトリーの以下のサブディレクトリーが自動的に作成されます。

- 接続ログが保管されている ″logs″ ディレクトリー
- 任意の First Failure Support Technology (FFST) とトレース・レコードが書き込まれる ″errors″ ディレクトリー

internet pass-thru の自動開始

システム開始時に MQIPT が自動的に開始されるようにするには、mqiptService スクリプトを実行してエントリーを inittab に追加します。たとえば、以下のとおりです。

```
cd /usr/opt/mqipt/bin
../mqiptService -install
```

MQIPT が自動的に開始されないようにして、そのエントリーを inittab から除去するには、次のようにします。

```
cd /usr/opt/mqipt/bin
../mqiptService -remove
```

コマンド行からの Administration Client の開始

コマンド・プロンプトをオープンし、ディレクトリーを bin ディレクトリーに変えて、mqiptGui を実行します。たとえば、以下のとおりです。

```
cd /usr/opt/mqipt/bin
../mqiptGui
```

Administration Client がファイアウォール経由で外部の MQIPT に接続できるようにするには、以下のように、ホスト名またはアドレス、およびポート番号を指定します。

```
mqiptGui <socksHostName <socksPort>>
```

デフォルトの socksPort は 1080 です。

Administration Client の状況が、Administration Client のメイン・ウィンドウにメッセージで示されます。

internet pass-thru のアンインストール

41 ページの『internet pass-thru の自動開始』に説明されているように、MQIPT をシステムからアンインストールする前に、それが自動的に開始されないようにしてください。 ルート としてログインし、次のように `installp` コマンドを実行します。

```
installp -u mqipt-RT
```

第 7 章 HP-UX での internet pass-thru のインストール

この章では、HP-UX システムで MQIPT をインストールする方法について説明します。

- 『ファイルのダウンロードとインストール』
- 44 ページの『internet pass-thru のセットアップ』
- 44 ページの『コマンド行からの internet pass-thru の開始』
- 45 ページの『internet pass-thru の自動開始』
- 45 ページの『コマンド行からの Administration Client の開始』
- 46 ページの『internet pass-thru のアンインストール』

ファイルのダウンロードとインストール

MQIPT は、以下の URL の WebSphere MQ SupportPac Web ページからダウンロードします。

```
http://www.ibm.com/software/ts/mqseries/downloads
```

ダウンロードの指示を実行してください。

ルート としてログインし、ms81_hp11.tar.Z を解凍して一時ディレクトリーに入れます。次の例のように、swinstall コマンドを実行します。

```
login root
cd /tmp
uncompress -fv ms81_hp11.tar.Z
tar xvf ms81_hp11.tar
swinstall -s /tmp MQIPT.MQIPT-RT
```

この例では、ms81_hp11.tar.Z が /tmp ディレクトリーに入っていることを前提にしています。

MQIPT には、以下の表に示されているファイル (Administration Client GUI のファイルを含む) が入っています。

ファイル	目的
Readme.txt	資料に記載されていない最新情報
mqiptSample.conf	サンプル構成ファイル
ssl/sslSample.pfx	テスト鍵リング・ファイル
ssl/sslSample.pwd	テスト鍵リング・ファイル用のパスワード・ファイル
ssl/sslCAdefault.pfx	サンプル認証局 (CA) 鍵リング・ファイル
ssl/sslCAdefault.pwd	サンプル認証局 (CA) 鍵リング・ファイル用のパスワード・ファイル
ssl/KeyMan.zip	KeyMan ユーティリティー
lib/MQipt.jar	ランタイム、クラス、およびプロパティー・ファイルが入っている
lib/ADV_mqipt_normal. class	「通常」モード用 Network Dispatcher アドバイザー

ファイル	目的
lib/ADV_mqipt_replace. class	「置換」モード用 Network Dispatcher アドバイザー
lib/mqipt1414Sample.ssl	Network Dispatcher アドバイザー用のサンプル・トリガー・ファイル
bin/mqipt	コマンド行から MQIPT を実行するためのショートカット
bin/mqiptAdmin	MQIPT を停止し、ファイル情報を最新表示するためのショートカット
bin/mqiptVersion	MQIPT のバージョン番号の表示
bin/mqiptService	システム始動時に MQIPT が自動的に開始されるようにするための MQIPT のインストール
bin/mqiptEnv	mqipt.jar ファイルのロケーションを定義し、他のスクリプトでのみ使用する。
bin/mqiptFork	システム始動時に MQIPT の立ち上げに使用
web/MQIPTServlet.war	サーブレット・バージョン用の Web アーカイブ・ファイル
doc/<lang>/pdf/ <filename>.pdf	PDF 形式の「*internet pass-thru*」マニュアル。ソフトコピー文書の詳細については、 xiii ページの『参照文献』を参照。
doc/<lang>/html/ <filename>.zip	HTML 形式の「*internet pass-thru*」マニュアルのマスター・ファイル。ソフトコピー文書の詳細については、 xiii ページの『参照文献』を参照。
lib/mqiptGui.jar	Administration Client GUI 用のランタイム、クラス、およびプロパティー・ファイルが入っている
bin/mqiptGui	コマンド行から Administration Client GUI を実行するためのショートカット
bin/customSample. properties	Administration Client の外観およびアクセシビリティーをカスタマイズするためのサンプル・ファイル

internet pass-thru のセットアップ

MQIPT を初めて開始する場合は、その前に、mqiptSample.conf サンプル構成ファイルを mqipt.conf にコピーしてください。構成と管理については、 51 ページの『第 9 章 internet pass-thru の管理と構成』を参照してください。

コマンド行からの internet pass-thru の開始

ルート としてログインし、ディレクトリーを bin ディレクトリーに変えます。たとえば、以下のとおりです。

```
cd /opt/mqipt/bin
mqipt ..
```

オプションを指定しないで mqipt スクリプトを実行すると、“.” のデフォルト・ロケーションが構成ファイルに使用されます (mqipt.conf)。異なるロケーションを指定するには、次のようにします。

```
mqipt <directory name>
```

MQIPT の状況を示すメッセージがコンソールに表示されます。エラーが起こった場合は、 105 ページの『問題判別』を参照してください。以下のメッセージは、MQIPT が正常に開始された場合の例です。

```
5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
MQCPI004 Reading configuration information from /opt/mqipt/mqipt.conf
MQCPI008 Listening for control commands on port 1881
MQCPI011 The path /opt/mqipt/logs will be used to store the log files
MQCPI006 Route 1418 has started and will forward messages to :
MQCPI034 ....mqserver.company4.com(1414)
MQCPI035 ....using MQ protocols
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....mqipt.company2.com(1415)
MQCPI035 ....using MQ protocols
MQCPI036 ....SSL Client side enabled with properties :
MQCPI031 ......cipher suites <null>
MQCPI032 ......keyring file /opt/mqipt/KeyMan.pfx
MQCPI038 ......distinguished name(s) CN=*Doe O=IBM OU=* L=* ST=* C=*
```

MQIPT を初めて呼び出すときは、mqipt ホーム・ディレクトリーの以下のサブディレクトリーが自動的に作成されます。

- 接続ログが保管されている ″logs″ ディレクトリー
- 任意の First Failure Support Technology (FFST) とトレース・レコードが書き込まれる ″errors″ ディレクトリー

internet pass-thru の自動開始

システム開始時に MQIPT が自動的に開始されるようにするには、mqiptService スクリプトを実行します。たとえば、以下のとおりです。

```
cd /opt/mqipt/bin
mqiptService -install
```

ここでは、JDK 1.4 がすでに /opt/java1.4 というディレクトリーにインストール済みであることを前提にしています。インストール済みでない場合は、mqipt.ske ファイルを編集して、JDK のロケーションを指すように PATH 変数を変更してください。 mqiptService -install コマンドを実行する前に、この変更を適用する必要があります。

MQIPT をサービスとして開始すると、console.log ログ・ファイルが logs サブディレクトリーに書き込まれます。このサブディレクトリーは、MQIPT を初めて実行するときに作成されるため、MQIPT をサービスとして実行する前に、少なくとも 1 回はそれを実行しておく必要があります。

MQIPT が自動的に開始されないようにするには、次のようにします。

```
cd /opt/mqipt/bin
mqiptService -remove
```

コマンド行からの Administration Client の開始

コマンド・プロンプトをオープンし、ディレクトリーを bin ディレクトリーに変えて、mqiptGui を実行します。たとえば、以下のとおりです。

```
cd /opt/mqipt/bin
mqiptGui
```

Administration Client がファイアウォール経由で外部の MQIPT に接続できるようにするには、以下のように、ホスト名またはアドレス、およびポート番号を指定します。

```
mqiptGui <socksHostName <socksPort>>
```

デフォルトの socksPort は 1080 です。

Administration Client の状況が、Administration Client のメイン・ウィンドウにメッセージで示されます。

internet pass-thru のアンインストール

45 ページの『internet pass-thru の自動開始』に説明されているように、MQIPT をシステムからアンインストールする前に、それが自動的に開始されないようにしてください。 ルート としてログインし、次のように swremove コマンドを実行します。

```
swremove MQIPT
```

第 8 章 Linux での internet pass-thru のインストール

この章では、Linux システムで MQIPT をインストールする方法について説明します。

- 『ファイルのダウンロードとインストール』
- 48 ページの『internet pass-thru のセットアップ』
- 48 ページの『コマンド行からの internet pass-thru の開始』
- 49 ページの『internet pass-thru の自動開始』
- 49 ページの『コマンド行からの Administration Client の開始』
- 50 ページの『internet pass-thru のアンインストール』

ファイルのダウンロードとインストール

MQIPT は、以下の URL の WebSphere MQ SupportPac Web ページからダウンロードします。

```
http://www.ibm.com/software/ts/mqseries/downloads
```

ダウンロードの指示を実行してください。

ルート としてログインし、ms81_linux.tar.gz を解凍して一時ディレクトリーに入れます。次の例のように、rpm コマンドを実行します。

```
login root
cd /tmp
gunzip -fv ms81_linux.tar.gz
tar xvf mq81_linux.tar
cd i386
rpm -i WebSphereMQ-IPT-1.2.0-0.i386.rpm
```

この例では、ms81_linux.tar.gz が /tmp ディレクトリーに入っていることを前提にしています。

MQIPT には、以下の表に示されているファイル (Administration Client GUI のファイルを含む) が入っています。

ファイル	目的
Readme.txt	資料に記載されていない最新情報
mqiptSample.conf	サンプル構成ファイル
ssl/sslSample.pfx	テスト鍵リング・ファイル
ssl/sslSample.pwd	テスト鍵リング・ファイル用のパスワード・ファイル
ssl/sslCAdefault.pfx	サンプル認証局 (CA) 鍵リング・ファイル
ssl/sslCAdefault.pwd	サンプル認証局 (CA) 鍵リング・ファイル用のパスワード・ファイル
ssl/KeyMan.zip	KeyMan ユーティリティー
lib/MQipt.jar	ランタイム、クラス、およびプロパティー・ファイルが入っている

ファイル	目的
lib/ADV_mqipt_normal. class	「通常」モード用 Network Dispatcher アドバイザー
lib/ADV_mqipt_replace. class	「置換」モード用 Network Dispatcher アドバイザー
lib/mqipt1414Sample.ssl	Network Dispatcher アドバイザー用のサンプル・トリガー・ファイル
lib/libiptqos.so	Quality of Service サポート用のランタイム・ライブラリー
bin/mqipt	コマンド行から MQIPT を実行するためのショートカット
bin/mqiptAdmin	MQIPT を停止し、ファイル情報をリフレッシュするためのショートカット
bin/mqiptVersion	MQIPT のバージョン番号の表示
bin/mqiptService	システム始動時に MQIPT が自動的に開始されるようにするための MQIPT のインストール
bin/mqiptEnv	mqipt.jar ファイルのロケーションを定義し、他のスクリプトでのみ使用する。
web/MQIPTServlet.war	サーブレット・バージョン用の Web アーカイブ・ファイル
doc/<land>/pdf/ <filename>.pdf	PDF 形式の「*internet pass-thru*」マニュアル。ソフトコピー文書の詳細については、 xiii ページの『参照文献』を参照。
doc/<lang>/html/ <filename>.zip	HTML 形式の「*internet pass-thru*」マニュアルのマスター・ファイル。ソフトコピー文書の詳細については、 xiii ページの『参照文献』を参照。
lib/mqiptGui.jar	Administration Client GUI 用のランタイム、クラス、およびプロパティー・ファイルが入っている
bin/mqiptGui	コマンド行から Administration Client GUI を実行するためのショートカット
bin/customSample. properties	Administration Client の外観およびアクセシビリティーをカスタマイズするためのサンプル・ファイル

internet pass-thru のセットアップ

MQIPT を初めて開始する場合は、その前に、mqiptSample.conf サンプル構成ファイルを mqipt.conf にコピーしてください。構成と管理については、 51 ページの『第 9 章 internet pass-thru の管理と構成』を参照してください。

コマンド行からの internet pass-thru の開始

ルート としてログインし、ディレクトリーを bin ディレクトリーに変えます。たとえば、以下のとおりです。

```
cd /opt/mqipt/bin
mqipt ..
```

オプションを指定しないで mqipt スクリプトを実行すると、“.” のデフォルト・ロケーションが構成ファイル (mqipt.conf) に使用されます。異なるロケーションを指定するには、次のようにします。

```
mqipt <directory name>
```

MQIPT の状況を示すメッセージがコンソールに表示されます。エラーが起こった場合は、 105 ページの『問題判別』を参照してください。以下のメッセージは、MQIPT が正常に開始された場合の例です。

```
5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
MQCPI004 Reading configuration information from /opt/mqipt/mqipt.conf
MQCPI008 Listening for control commands on port 1881
MQCPI011 The path /opt/mqipt/logs will be used to store the log files
MQCPI006 Route 1418 has started and will forward messages to :
MQCPI034 ....mqserver.company4.com(1414)
MQCPI035 ....using MQ protocols
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....mqipt.company2.com(1415)
MQCPI035 ....using MQ protocols
MQCPI036 ....SSL Client side enabled with properties :
MQCPI031 ......cipher suites <null>
MQCPI032 ......keyring file /opt/mqipt/KeyMan.pfx
MQCPI038 ......distinguished name(s) CN=*Doe O=IBM OU=* L=* ST=* C=*
```

MQIPT を初めて呼び出すときは、mqipt ホーム・ディレクトリーの以下のサブディレクトリーが自動的に作成されます。

- 接続ログが保管されている ″logs″ ディレクトリー
- 任意の First Failure Support Technology (FFST) とトレース・レコードが書き込まれる ″errors″ ディレクトリー

internet pass-thru の自動開始

システム開始時に MQIPT が自動的に開始されるようにするには、mqiptService スクリプトを実行します。たとえば、以下のとおりです。

```
cd /opt/mqipt/bin
mqiptService -install
```

MQIPT をサービスとして開始すると、console.log ファイルが logs サブディレクトリーに書き込まれます。このサブディレクトリーは、MQIPT を初めて実行するときに作成されるので、MQIPT をサービスとして実行する前に、少なくとも 1 回はそれを実行しておく必要があります。

MQIPT が自動的に開始されないようにするには、次のようにします。

```
cd /opt/mqipt/bin
mqiptService -remove
```

コマンド行からの Administration Client の開始

コマンド・プロンプトをオープンし、ディレクトリーを bin ディレクトリーに変えて、mqiptGui を実行します。たとえば、以下のとおりです。

```
cd /opt/mqipt/bin
mqiptGui
```

Administration Client がファイアウォール経由で外部の MQIPT に接続できるようにするには、以下のように、ホスト名またはアドレス、およびポート番号を指定します。

```
mqiptGui <socksHostName <socksPort>>
```

デフォルトの socksPort は 1080 です。

Administration Client の状況が、Administration Client のメイン・ウィンドウにメッセージで示されます。

internet pass-thru のアンインストール

49 ページの『internet pass-thru の自動開始』に説明されているように、MQIPT をシステムからアンインストールする前に、それが自動的に開始されないようにしてください。 ルート としてログインし、次のように swremove コマンドを実行します。

```
rpm -e WebSphereMQ-IPT-1.2.0-0
```

第 9 章 internet pass-thru の管理と構成

MQIPT の構成を行うには、mqipt.conf 構成ファイルに変更を加えます。この変更を行うには、Administration Client を使用する (この方法を推奨) か、または選択したエディターを使用します。この章では、関連する参照情報を使用して、これらの 2 つの手法について説明します。

- 『internet pass-thru Administration Client の使用』
- 56 ページの『internet pass-thru 行モード・コマンド』
- 57 ページの『構成参照情報』

internet pass-thru Administration Client の使用

Administration Client を使用して、1 つまたは複数の MQIPT を構成したり更新したりできます。 Application Client は、MQIPT のグローバル・プロパティーと経路固有のプロパティーを表示します。

Administration Client のローカル側に保管される唯一のデータは MQIPT のリストであり、このリストは client.conf というファイルに入っています。グローバル・プロパティーと経路プロパティーは、常に、MQIPT から取り出されてから、Administration Client に表示されます。

Administration Client の開始

Administration Client を開始する場合は、MQIPT の bin サブディレクトリーに入っている mqiptGui スクリプトを使用します。 Administration Client の開始に関する説明については、各プラットフォームのインストールの章を参照してください。

Administration Client の初回の開始時には、ダイアログ・ボックスが表示されて、ユーザーは MQIPT との接続情報の入力を求められます。必要な情報は、以下のとおりです。

「MQIPT Name (MQIPT の名前)」
この MQIPT の説明に使用する名前。この情報は必須ではありませんが、入力をお勧めします。

「Network Address (ネットワーク・アドレス)」
MQIPT が常駐するシステムのアドレス。ネーム・サーバーによって認識された名前、小数点付き 10 進数アドレス、またはローカル・ホスト (MQIPT がクライアントと同じマシンにある場合) のいずれか。

「Command Port (コマンド・ポート)」
MQIPT がコマンドを listen するポートの番号。

「Timeout (タイムアウト)」
Administration Client が MQIPT との接続を待機する時間 (秒数)。できるだけこの値を小さくして、ウィンドウの最新表示時間を減らします。

「Access Password (アクセス・パスワード)」
MQIPT と通信するとき使用するパスワード。このフィールドは、パスワード検

査が有効になっている場合にのみ入力します。 (AccessPW が MQIPT 構成ファイルに提供されていて、かつヌル・ストリング以外の値である場合に、パスワード検査が有効です。)

「Save Password (パスワードの保管)」
このチェック・ボックスがブランクのままであれば、パスワードは、このセッションの期間中、または MQIPT を除去するまで記憶されています。このチェック・ボックスを選択すると、パスワードは、将来のセッションのために保管されます。

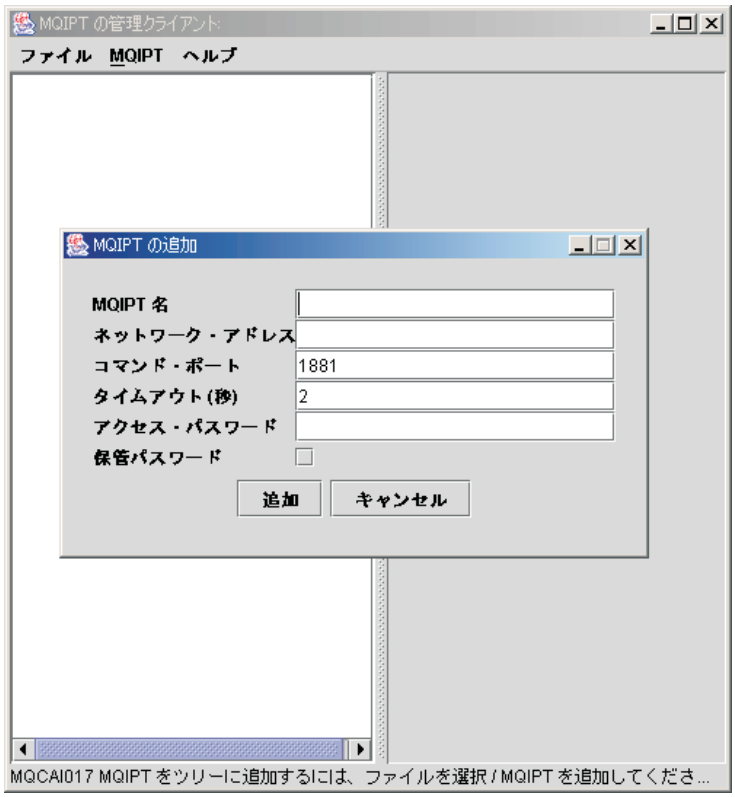

図 8. MQIPT への初回アクセス時のウィンドウ

MQIPT の管理

MQIPT の更新は一度に 1 つしか行えないため、リストから別の MQIPT を選択した場合は、未処理の変更をすべて適用してから次の作業へ進まなければなりません。いずれかのプロパティーに変更を加えても、「Apply (適用)」メニュー・オプションを使用するまでは MQIPT は影響を受けません。

リストから MQIPT を選択すると、グローバル・プロパティーと経路プロパティーが MQIPT から取り出されます。 MQIPT が稼働していない場合や、誤りの CommandPort が指定された場合は、エラー・メッセージが出ます。ホスト名や CommandPort の変更は、「Connection (接続)」メニュー・オプションから行えます。

リストの MQIPT をダブルクリックすると、経路のリストが表示されます。経路を選択すると、そのプロパティーが表示されます。プロパティーは、ユーザーの要件に合わせて調整できます。

MQSeries internet pass-thru バージョン 1.0 の構成ファイル (mqipt.conf) を使用する場合は、経路名が表示されません。経路名を追加するには、「Name (名前)」フィールドを更新します。

変更を適用すると、構成ファイルは、タイム・スタンプを記録されて MQIPT へ戻され、変更内容が即時に有効になります。既存のコメント行はすべて消失します。

経路を追加するには、「Add Route (経路の追加)」メニュー・オプションを使用します。この新規経路では、グローバル・プロパティーによって定義されたデフォルトのプロパティー・セットが表示されます。

プロパティーの継承

Administration Client で MQIPT や経路のプロパティーを設定する方法には、以下のような階層があります。

1. どのプロパティーにもデフォルト値があり、プロパティーが構成ファイルに記述されていない場合や、Administration Client のユーザー処置によって明確に設定されていない場合は、このデフォルト値が使用されます。
2. MQIPT 全体に対して設定されたグローバル・プロパティーは、その適用を禁止する特定の経路情報がない限り、各 MQIPT のすべての経路で使用されます。つまり、構成ファイルの場合、追加のプロパティーが経路スタンザに設定されない限り、グローバル・スタンザに設定されたプロパティーがすべての経路に伝搬されます。 Administration Client ユーザーによって MQIPT に設定されたプロパティーは、経路に対して別途プロパティーが設定されない限り、すべての経路に伝搬されます。
3. ある経路に対して設定されたすべての値は、デフォルト値やグローバル設定値とは関係なく、その経路用として維持されます。

ファイル・メニュー・オプション

「File (ファイル)」メニューを選択すると、ツリー管理に関連するオプションのほとんどが表示されます。

「Add MQIPT (MQIPT の追加)」
クライアントを初めて使用するときに表示されるダイアログと同じダイアログが表示されます (51 ページの『Administration Client の開始』を参照)。

「Remove MQIPT (MQIPT の除去)」
現在強調表示されている MQIPT を Administration Client のツリーだけから除去します。この除去によって MQIPT の実行が影響を受けることはありません。

「Save Configuration (構成の保管)」
ツリーの MQIPT ノードを Administration Client の構成ファイルに保管して、それを次回に開始するときにこれらのノードを読み取れるようにします。
MQIPT ノードのみが保管されます。グローバル・プロパティーと経路プロパティーは、常に、MQIPT から取り出されます。

「Quit (終了)」

Administration Client の実行を停止します。ただし、Administration Client は、まず、ツリーまたは現行 MQIPT が変更されたかどうかを調べます。このうちのいずれか、または両方が変更された場合は、1 つまたは複数のダイアログが表示され、クライアントの保管、または MQIPT への変更の適用、あるいはその両方を行いたいかどうかを尋ねられます。

MQIPT メニュー・オプション

「Connection (接続)」

MQIPT のアクセス・パラメーターを変更します。変更結果はツリー・ビューに示されます。ツリー・ビューでは、 51 ページの『Administration Client の開始』に示されているようなウィンドウが表示されます。

「Password (パスワード)」

リモート MQIPT のパスワード・プロパティーを変更します。このアクションによりパスワード・ダイアログが表示され、ユーザーは、以下の入力を行うよう求められます。

- 「**Current Password (現行パスワード)**」: 不正使用のチェックのために、現行パスワードを示す必要があります。それを示さないとその変更を行えません。現在有効なパスワードがない場合は、このフィールドをブランクにされます。
- 「**New Password (新規パスワード)**」: 新規パスワードを入力します。この MQIPT でパスワードの使用を止めたい場合は、ブランクにしておきます。
- 「**New Password Again (再度新規パスワード)**」: 「New Password (新規パスワード)」フィールドへの入力ミスを防ぐために、同じ情報を再度入力するよう要求されます。
- 「**Save Password (パスワードの保管)**」: この MQIPT の他のアクセス・プロパティーと一緒に、新規パスワードをローカル側に保管するかどうかを決定するために使用されます。

「Add Route (経路の追加)」

選択した MQIPT に経路を追加します。詳細については、 55 ページの図 9を参照してください。各経路は、MQIPT 用の固有な ListenerPort を持っていなければなりません。

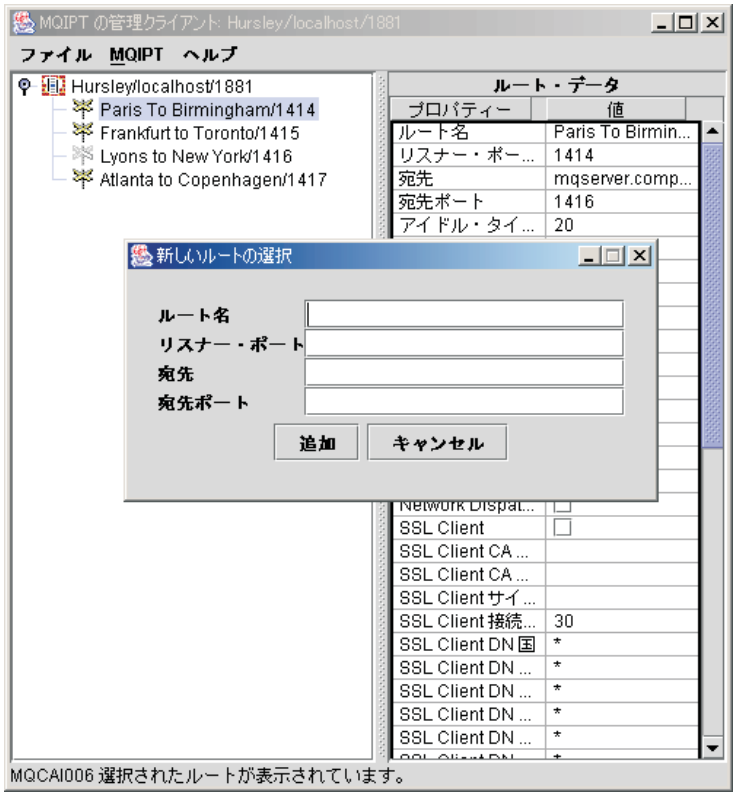

図 9. 経路の追加

「Delete Route (経路の削除)」
選択された経路を MQIPT から削除します。この削除は、「Apply (適用)」メニュー・オプションが使用されるまで、MQIPT に影響を与えません。

「Apply (適用)」
MQIPT の構成に対して行った変更に間違いがなければ、このオプションで新規の構成ファイルが MQIPT に送られ、MQIPT はそれを保管します。新規設定は直ちに有効になります。

「Refresh (リフレッシュ)」
選択された MQIPT から構成ファイルを読み取り、リフレッシュを行います。

「Stop (停止)」
STOP コマンドを MQIPT に送って、実行を停止するよう指示します。このコマンドが実行されたならば、MQIPT との連絡が切断されます。グローバル・プロパティーである RemoteShutdown がオンにされない限り、このコマンドは無視されます。

経路情報は、MQIPT グローバル情報と同じ方法で更新できます。経路のプロパティーを変更した場合は、その変更が有効になる前にそれを適用する必要があります。これを行うには、「MQIPT/Apply (MQIPT/ 適用)」メニュー・オプションを選択するか、または構成の保管を要求されたときに「はい」と答えます。

ヘルプ・メニュー・オプション

ヘルプ
Netscape を使用して、Administration Client の使用方法に関する情報を表示し、

左方のペインから、「Administering and configuring internet pass-thru (internet pass-thru の管理と保管)」を選択します。 Administration Client を使用する前に、<lang>/html サブディレクトリーに入っているファイルを圧縮解除する必要があります。

製品情報

Administration Client のバージョンに関する情報が入っているウィンドウを表示します。

internet pass-thru 行モード・コマンド

Administration Client を使用しない場合は、行モード・コマンドを使用して internet pass-thru の管理と構成を行うことができます。

行モード・コマンドによる internet pass-thru の管理

選択したエディターを使用して、自分の要件を満たすように mqipt.conf 構成ファイルを変更します。変更できるプロパティーのリストについては、57 ページの『構成参照情報』を参照してください。

mqipt.conf のグローバル・セクションに CommandPort の値が指定されている場合は、MQIPT はこのポートで以下の ASCII 管理コマンドを listen します。

```
mqiptAdmin -refresh {hostname {port} }      sends the refresh command
mqiptAdmin -stop    {hostname {port} }      sends the stop command
```

mqiptAdmin スクリプトは bin サブディレクトリーに入っています。

入っていなければ、デフォルトで、ホスト名が localhost になり、ポートが 1881 になります。

STOP

MQIPT は、すべての接続をクローズし、着信接続の listen を停止してから終了します。 Administration Client の「MQIPT/Stop (MQIPT/停止)」メニュー・オプションを使用した場合も同じ結果が得られます。 mqipt.conf ファイルに RemoteShutDown=true を指定していない限り、このコマンドは無視されます。

REFRESH

MQIPT は mqipt.conf を再読み取りします。 MQIPT は以下の処理を行います。

- 現在アクティブなすべての経路に非アクティブのマークが付いている (または、それらの経路がすべて欠落している) のを検出した場合、MQIPT は、それらの経路をクローズし、これらの経路での着信接続の listen を停止します。
- 現在実行していないいずれかの経路が構成ファイルでアクティブのマークが付いているのを検出した場合、MQIPT はそれらの経路を始動します。
- 現在実行中の経路の構成パラメーターが変更されているのを検出した場合、MQIPT は、変更値をそれらの経路に適用します。可能であれば (たとえば、トレースの設定値が変更された場合)、MQIPT は、稼働している接続を中断することなくこの操作を実行します。パラメーターの変更 (たとえば、宛先の

変更) によっては、MQIPT がすべての接続をクローズしないと、変更内容を有効にしたり、経路を再始動したりできないものがあります。

Administration Client が MQIPT の設定値を一切変更していなければ、Administration Client の「MQIPT/Apply (MQIPT/ 適用)」メニュー・オプションを使用した場合も同じ結果が得られます。

Windows では、これらの管理機能は「Start (スタート)」->「Programs (プログラム)」メニューからも使用できます。

構成参照情報

いくつかの簡単な構成をセットアップする方法については、71 ページの『第 10 章 internet pass-thru の使用開始』を参照してください。サンプル構成については、MQIPT のホーム・ディレクトリーに入っている mqiptSample.conf ファイルを参照してください。

mqipt.conf ファイルはセクションのセットからなっています。 1 つのグローバル・セクションが設けられているほか、MQIPT を介して定義されている各経路ごとに 1 つずつセクションがあります。この簡単な構成では経路が 1 つしかないため、ファイルには 2 つのセクション、すなわち 1 つのグローバル・セクションと 1 つの経路セクションがあります。

それぞれのセクションには、名前 / 値のプロパティー・ペアが含まれています。プロパティーには、グローバル・セクションにしか現れないもの、経路セクションにしか現れないもの、また、経路セクションとグローバル・セクションの両方に現れるものがあります。あるプロパティーが経路セクションとグローバル・セクションの両方に現れる場合は、経路セクションのプロパティー値がグローバル・セクションの値をオーバーライドしますが、そのオーバーライドは当該経路についてだけ行われます。このようにして、グローバル・セクションを使用してデフォルト値を設定することにより、それらのデフォルト値を、個々の経路セクションで設定されていないプロパティーに使用することができます。

グローバル・セクションは、[global] の文字が入っている行で始まり、最初の経路セクションが始まるところで終了します。グローバル・セクションは、ファイル内のすべての経路セクションの先頭になければなりません。各経路セクションは、[route] の文字が入っている行で始まり、次の経路セクションが始まるところ、または構成ファイルの末尾に達したところで終了します。

認識されないすべてのキーワード名 (つまり、本書で定義された名前に含まれていない名前のすべての名前 / 値のペア) は無視されます。経路セクションに現れる名前 / 値のペアが認識済みの名前を持っているが、無効な値を持っている場合 (たとえば、MinConnectionThreads=x または HTTP=unsure)、その経路は使用不可になります (つまり、着信接続を一切 listen しません)。グローバル・セクションに現れる名前 / 値のペアが認識済みの名前を持っているが、無効な値を持っている場合は、すべての経路が使用不可になり、MQIPT は開始されません。プロパティーが true と false の値をとるものとしてリストされている場合は、大文字と小文字が混在する任意の文字を使用できます。

プロパティーの要約

表 4 は、以下のものを示しています。

- すべてのプロパティー
- そのプロパティーがグローバル・セクション、経路セクション、あるいはその両方のいずれに適用されるか
- デフォルト値

あるプロパティーがグローバル・セクションにも経路セクションにも含まれていない場合は、表に示されているデフォルト値が使用されます。

表 4. 構成プロパティーの要約

プロパティーの名前	グローバル	経路	デフォルト
AccessPW	はい		<null>
Active	はい	はい	true
ClientAccess	はい	はい	false
CommandPort	はい		<null>[1]
ConnectionLog	はい		true
Destination		はい	<null>
DestinationPort		はい	1414
HTTP[6,7]	はい	はい	false
HTTPChunking[1]	はい	はい	false
HTTPProxy[1]	はい	はい	<null>
HTTPProxyPort[1]	はい	はい	8080
IdleTimeout	はい	はい	0
ListenerPort		はい	<null>
LogDir (MQIPTServlet の場合にのみ有効)			<null>
MaxConnectionThreads	はい	はい	100
MaxLogFileSize	はい		50
MinConnectionThreads	はい	はい	5
Name		はい	<null>
NDAdvisor	はい	はい	false
NDAdvisorReplaceMode[4]	はい	はい	false
QMgrAccess	はい	はい	true
QoS (Linux でのみ使用可)	はい	はい	false
QosToCaller[9]	はい	はい	1
QosToDest[9]	はい	はい	1
RemoteShutdown	はい		false
SecurityManager	はい		false
SecurityManagerPolicy	はい		<null>
ServletClient[1]	はい	はい	false
SocksClient	はい	はい	false
SocksProxyHost[8]	はい	はい	<null>

表 4. 構成プロパティーの要約 (続き)

プロパティーの名前	グローバル	経路	デフォルト
SocksProxyPort[8]	はい	はい	1080
SocksServer[7]	はい	はい	false
SSLClient	はい	はい	false
SSLClientCipherSuites[2]	はい	はい	<null>
SSLClientConnectTimeout[2]	はい	はい	30
SSLClientDN_C[2]	はい	はい	*[5]
SSLClientDN_CN[2]	はい	はい	*[5]
SSLClientDN_L[2]	はい	はい	*[5]
SSLClientDN_O[2]	はい	はい	*[5]
SSLClientDN_OU[2]	はい	はい	*[5]
SSLClientDN_ST[2]	はい	はい	*[5]
SSLClientKeyRing[2]	はい	はい	<null>
SSLClientKeyRingPW[2]	はい	はい	<null>
SSLProxyMode	はい	はい	false
SSLServer[6]	はい	はい	false
SSLServerAskClientAuth[3]	はい	はい	false
SSLServerCipherSuites[3]	はい	はい	<null>
SSLServerDN_C[3]	はい	はい	*[5]
SSLServerDN_CN[3]	はい	はい	*[5]
SSLServerDN_L[3]	はい	はい	*[5]
SSLServerDN_O[3]	はい	はい	*[5]
SSLServerDN_OU[3]	はい	はい	*[5]
SSLServerDN_ST[3]	はい	はい	*[5]
SSLServerKeyRing[3]	はい	はい	<null>
SSLServerKeyRingPW[3]	はい	はい	<null>
Trace	はい	はい	0
UriName (デフォルト設定の詳細については、69 ページを参照。)[1]	はい	はい	

注:

1. これらのプロパティーを有効にするには、HTTP を true に設定します。
2. これらのプロパティーを有効にするには、SSLClient を true に設定します。
3. これらのプロパティーを有効にするには、SSLServer を true に設定します。
4. これらのプロパティーを有効にするには、NDAdvisor を true に設定します。
5. ″*″ 記号はワイルドカードを表します。
6. HTTP と SSLServer を一緒に使用することはできません。 HTTP プロパティーは、正方向接続の定義にのみ使用されます。 ListenerPort への着信データは自動的に検出されるため、SSLServer を設定するとランタイム例外が発生します。

7. HTTP と SocksServer を一緒に使用することはできません。 HTTP プロパティーは、正方向接続の定義にのみ使用されます。 ListenerPort への着信データは自動的に検出されるため、SocksServer を設定するとランタイム例外が発生します。
8. これらのプロパティーを有効にするには、SocksClient を true に設定します。
9. これらのプロパティーを有効にするには、QoS を true に設定します。

グローバル・セクション参照情報

グローバル・セクションには、ListenerPort、Destination、DestinationPort、および Name のほかに、以下のプロパティーと、61 ページの『経路セクション参照情報』に示されているプロパティーを入れることができます。

AccessPW

Administration Controller がコマンドを MQIPT に送信するときに使用するパスワード。このプロパティーがない場合やブランクに設定されている場合は、検査は行われません。

CommandPort

MQIPT が `mqiptAdmin` ユーティリティーまたは Administration Client からの構成コマンドを listen する TCP/IP ポート。 Administration Client からのコマンド・ポートは、他のすべてのプロパティーと同じ方法で変更できます。ただし、接続プロパティーは変更しないでください。新規のセットアップを MQIPT に適用すると、Administration Client が自動的に接続プロパティーを変更します。

`CommandPort` プロパティーがない場合は、MQIPT は構成コマンドを listen しません。コマンド・ポートで listen したい場合は、1881 を使用することをお勧めします。 Administration Client は CommandPort に対するデフォルト値を持っていませんが、行モード・コマンドを使用する場合、1881 がデフォルト値になります。

ConnectionLog

`true` または `false` のいずれか。 true であれば、MQIPT はすべての接続試行 (成功またはそれ以外) を `logs` サブディレクトリーにログ記録し、切断イベントを `mqiptYYYYMMDDHHmmSS.log` ファイルにログ記録します。デフォルト値は true です。このプロパティーが `true` から `false` に変更されると、MQIPT は既存の接続ログをクローズして新規の接続ログを作成します。プロパティーが `true` にリセットされたとき、新規の接続ログが使用されます。

MaxLogFileSize

`mqipt.log` 接続ログ・ファイルの最大サイズ (KB で指定)。 `mqipt.log` ファイル・サイズがこの最大値を超えると、バックアップ・コピー `mqipt.back` が作成され、新規ファイルが開始されます。保管できるバックアップ・ファイルは 1 つだけです。したがって、メイン・ログ・ファイルがいっぱいになると、それ以前のバックアップはすべて消去されます。デフォルト値は 50 で、最小許可値は 5 です。

RemoteShutDown

`true` または `false` のいずれか。 true の場合 (およびコマンド・ポートがある場合) は、コマンド・ポートで STOP コマンドを受け取るたびに MQIPT がシャットダウンします。デフォルト値は false です。

SecurityManager

MQIPT のこのインスタンスに対して Java Security Manager を使用可能にするには、このプロパティーを true に設定します。このプロパティーは、正しい許可が付与されることを前提にしています。詳細については、 24 ページの『Java Security Manager』を参照してください。このプロパティーのデフォルト値は false です。

SecurityManagerPolicy

ポリシー・ファイルの完全修飾名。このプロパティーが設定されていないと、デフォルトのシステムとユーザー・ポリシー・ファイルが使用されます。 Java Security Manager がすでに使用可能になっていると、このプロパティーは、変更しても、その変更は、Java Security Manager を使用不可にし、再度使用可能にするまで有効になりません。

経路セクション参照情報

経路セクションには、以下のプロパティーが含まれている場合があります。

Active

この経路は、Active の値が `true` に設定されている場合にのみ着信接続を受け入れます。つまり、`Active=false` と設定すれば、経路セクションを構成ファイルから削除しなくても、宛先へのアクセスを一時的にシャットオフすることができます。このプロパティーを `false` に変更すると、経路は、REFRESH コマンドを出したときに停止します。この経路へのすべての接続は終了します。

ClientAccess

この経路は、ClientAccess の値が `true` に設定されている場合にのみ着信クライアント・チャネル接続を可能にします。クライアント要求のみ、キュー・マネージャー要求のみ、または両方のタイプの要求を受け入れるように、MQIPT を構成することができる点に注意してください。このプロパティーは、QMgrAccess プロパティーと一緒に使用してください。このプロパティーを `false` に変更すると、経路は停止され、REFRESH コマンドを出したときに再始動されます。この経路へのすべての接続は終了します。

Destination

この経路の接続先キュー・マネージャー (または後続の MQIPT) のホスト名 (またはドット 10 進 IP アドレス)。各経路セクションには、明示的な Destination 値が含まれて**いなければなりません**。同一 Destination を指す複数の経路セクションを持つことができます。ある経路がこのプロパティーの変更によって影響を受けた場合は、経路は停止され、REFRESH コマンドを出したときに再始動されます。この経路へのすべての接続は終了します。

DestinationPort

この経路の接続先 Destination ホスト上のポート。複数の経路が Destination と DestinationPort の同一の組み合わせを指すことは有効です。各経路セクションには、明示的な DestinationPort 値が含まれて**いなければなりません**。ある経路がこのプロパティーの変更によって影響を受けた場合は、経路は停止され、REFRESH コマンドを出したときに再始動されます。この経路へのすべての接続は終了します。

HTTP

アウトバウンド HTTP トンネル操作要求を行う (つまり、HTTP を介して別の MQIPT と通信する) 経路の場合に、これを `true` に設定します。 WebSphere

MQ キュー・マネージャーへ向かう経路の場合に false に設定します。このプロパティーを false に変更すると、経路は停止され、REFRESH コマンドを出したときに再始動されます。この経路へのすべての接続は終了します。 HTTP チャンク操作を使用するには、このプロパティーを true に設定します。このプロパティーは、以下のプロパティーと一緒に使用できます。

- QoS
- SocksClient
- SSLClient
- SSLProxyMode

HTTPChunking
チャンク操作と一緒に HTTP トンネル操作を使用してアウトバウンド要求を行う経路について、これを true に設定します。 HTTP プロパティーも true に設定する必要があります。 HTTP チャンク操作を使用しないときは false に設定します。このプロパティーを false に変更すると、経路は停止され、REFRESH コマンドを出したときに再始動されます。この経路へのすべての接続は終了します。

HTTPProxy
この経路のすべての接続が使用する HTTP プロキシーのホスト名 (またはドット 10 進 IP アドレス)。このプロパティーを変更すると、経路は停止され、REFRESH コマンドを出したときに再始動されます。この経路へのすべての接続は終了します。

HTTPProxyPort
HTTP プロキシーで使用するポート・アドレス。デフォルト値は 8080 です。このプロパティーを変更すると、経路は停止され、REFRESH コマンドを出したときに再始動されます。この経路へのすべての接続は終了します。

IdleTimeout
アイドル接続をクローズする時刻 (分)。キュー・マネージャー間チャネルは DISCINT プロパティーも持つことに注意してください。 IdleTimeout パラメーターを設定した場合は、DISCINT をメモにとっておきます。 0 の値はアイドル・タイムアウトがないことを示します。このプロパティーの変更結果が有効になるのは、経路を再始動したときだけです。

ListenerPort
この経路が着信要求を listen するポート番号。各経路セクションには、明示的な ListenerPort 値が含まれて**いなければなりません**。さらに、各セクションに設定された ListenerPort 値は異なっていなければなりません。選択されたポートが、同一ホストで稼働している他の任意の TCP/IP リスナーによってすでに使用されていれば、有効な任意のポート番号を使用することができます (ポート 80 および 443 を含む)。

LogDir
このプロパティーを使用して、ログおよびトレース・ファイルのディレクトリー名を定義します。このプロパティーに対する変更は、MQIPTServlet が停止されて再始動されるまで、有効になりません。デフォルト値は <null> です。このプロパティーは MQIPTServlet に対してのみ有効です

MaxConnectionThreads
この経路が処理できる接続スレッドの最大数、つまり、同時接続の最大数。この

限度に達すると、MaxConnectionThreads 値は、すべてのスレッドが使用中になっている場合にキューに入れられる接続の数を示します。その数を超えると、後続の接続要求は拒否されます。最小許可値は、1 または MinConnectionThreads の値のいずれか大きいほうです。このプロパティーを変更したために経路が影響を受ける場合は、REFRESH コマンドを出すときにこの新規値が使用されます。すべての接続がこの新規値を即時に使用します。経路は終了します。

MinConnectionThreads
接続スレッド (この経路の着信接続を処理するスレッド) の最小数。この数は、経路を開始するときに割り振られるスレッドの数であり、割り振られたスレッドの総数は、経路がアクティブになっている間、この値より小さくなることはありません。最小許可値は 0 であり、この値は MaxConnectionThreads に対して指定した値よりも小さくなければなりません。このプロパティーの変更結果が有効になるのは、経路を再始動したときのみです。

Name
経路を識別するためのオプショナル名。この名前は、コンソール・メッセージとトレース情報に現れます。このプロパティーの変更結果が有効になるのは、経路を再始動したときのみです。

NDAdvisor
経路がカスタム・アドバイザーからの要求に応答できるようにするには、Network Dispatcher によって管理される経路についてこのプロパティーを true に設定します。このプロパティーを false に変更すると、経路は、REFRESH コマンドを出したときに停止されます。この経路へのすべての接続は終了します。 NDAdvisorReplaceMode プロパティーを使用するには、このプロパティーを true に設定します。

NDAdvisorReplaceMode
Network Dispatcher カスタム・アドバイザーの「置換」モードを使用するには、このプロパティーを true に設定します。この経路の ListenerPort アドレスに対して mqipt_replace カスタム・アドバイザーを開始しておかなければなりません。「通常」モードを使用するには、このプロパティーを false に設定します。このプロパティーを使用するには、NDAdvisor プロパティーを true に設定します。

QMgrAccess
この経路で着信キュー・マネージャーのチャネル接続 (たとえば、送信側チャネル) を使用できるのは、QMgrAccess の値が true 値に設定されている場合だけです。このプロパティーを false に変更すると、経路は、REFRESH コマンドを出したときに停止されます。この経路へのすべての接続は終了します。

QoS
この経路上のすべての接続に対して Quality of Service を使用できるようにするには、このプロパティーを true に設定します。このプロパティーは Linux でのみ使用可能にできます。このプロパティーを変更すると、経路は停止され、REFRESH コマンドを出したときに再始動されます。この経路へのすべての接続は終了します。このプロパティーは、以下のプロパティーと一緒に使用できます。

- HTTP
- SSLClient

- SSLProxyMode
- SSLServer

QosToCaller
このプロパティーは、MQIPT マシンから接続イニシエーターへのすべてのトラフィックについて優先順位を設定します。このプロパティーの設定値 1 は低優先順位、2 は中間優先順位、3 は高優先順位を表します (デフォルトは 1 です)。このプロパティーを変更 (および QoS を true に設定) すると、経路は停止され、REFRESH コマンドを出したときに再始動されます。この経路へのすべての接続は終了します。

QosToDest
このプロパティーは、MQIPT マシンから接続宛先 (Destination プロパティーで定義) へのすべてのトラフィックについて優先順位を設定します。このプロパティーの設定値 1 は低優先順位、2 は中間優先順位、3 は高優先順位を表します (デフォルトは 1 です)。このプロパティーを変更 (および QoS を true に設定) すると、経路は停止され、REFRESH コマンドを出したときに再始動されます。この経路へのすべての接続は終了します。

ServletClient
MQIPT サーブレットに接続するときにこのプロパティーを true に設定します。 HTTP プロパティーも true に設定する必要があります。このプロパティーを変更 (および HTTP を true に設定) すると、経路は停止され、REFRESH コマンドを出したときに再始動されます。

SocksClient
経路を Socks クライアントとして機能させ、Socks プロキシーを介するすべての接続を SocksProxyHost および SocksProxyPort プロパティーを使用して定義させるようにするには、このプロパティーを true に設定します。このプロパティーを変更すると、経路は停止され、REFRESH コマンドを出したときに再始動されます。この経路へのすべての接続は終了します。このプロパティーは、以下のプロパティーと一緒に使用できます。

- HTTP
- SocksServer
- SSLClient
- SSLProxyMode

SocksProxyHost
この経路のすべての接続が使用する Socks プロキシーのホスト名 (またはドット 10 進 IP アドレス)。このプロパティーを変更 (および SocksClient を true に設定) すると、経路は停止され、REFRESH コマンドを出したときに再始動されます。この経路へのすべての接続は終了します。

SocksProxyPort
Socks プロキシーで使用するポート・アドレス。デフォルト値は 1080 です。このプロパティーを変更 (および SocksClient を true に設定) すると、経路は停止され、REFRESH コマンドを出したときに再始動されます。この経路へのすべての接続は終了します。

SocksServer
経路を Socks クライアントとして機能させ、Socks クライアント接続を受け入

れるようにするには、このプロパティーを true に設定します。このプロパティーを変更すると、経路は停止され、REFRESH コマンドを出したときに再始動されます。この経路へのすべての接続は終了します。このプロパティーは、以下のプロパティーと一緒に使用できます。

- SocksClient
- SSLProxyMode
- SSLServer

SSLClient
経路を SSL クライアントとして機能させ、発信 SSL 接続を行わせるようにするには、このプロパティーを true に設定します。 true に設定することは、宛先が、SSL サーバーとして機能する別の MQIPT であることを意味します。このプロパティーを変更すると、経路は停止され、REFRESH コマンドを出したときに再始動されます。この経路へのすべての接続は終了します。このプロパティーは、以下のプロパティーと一緒に使用できます。

- HTTP
- QoS
- SSLProxyMode

SSLClientCipherSuites
SSL クライアント・サイドで使用する SSL 暗号スイートの名前。この名前として可能なのは、サポートされている 1 つまたは複数の暗号スイートです。この名前をブランクにしておくと、SSL クライアントは SSLClientKeyRing からとった、サポートされている暗号スイートを使用します。このプロパティーを変更すると、経路は停止され、REFRESH コマンドを出したときに再始動されます。この経路へのすべての接続は終了します。

SSLClientConnectTimeout
このプロパティーを、SSL クライアントが SSL 接続の受け入れを待機する秒数に設定します。このプロパティーを変更したために経路が影響を受ける場合は、REFRESH コマンドを出すときにこの新規値を使用します。経路は終了します。

SSLClientDN_C
この国名の SSL サーバーから受け取った証明書を受け入れるには、このプロパティーを使用します。この名前の先頭または末尾にアスタリスク (*) を付けて、その有効範囲を拡張することができます。このプロパティーを指定しないと、「すべての会社名」になります。このプロパティーを変更すると、経路は停止され、REFRESH コマンドを出したときに再始動されます。この経路へのすべての接続は終了します。

SSLClientDN_CN
この共有名の SSL サーバーから受け取った証明書を受け入れるには、このプロパティーを使用します。この名前の先頭または末尾にアスタリスク (*) を付けて、その有効範囲を拡張することができます。このプロパティーを指定しないと、「すべての共有名」を暗黙指定したことになります。このプロパティーを変更すると、経路は停止され、REFRESH コマンドを出したときに再始動されます。この経路へのすべての接続は終了します。

SSLClientDN_L
このロケーションの SSL サーバーから受け取った証明書を受け入れるには、このプロパティーを使用します。この名前の先頭または末尾にアスタリスク (*)

を付けて、その有効範囲を拡張することができます。このプロパティーを指定しないと、「すべてのロケーション」を暗黙指定したことになります。このプロパティーを変更すると、経路は停止され、REFRESH コマンドを出したときに再始動されます。この経路へのすべての接続は終了します。

SSLClientDN_O
この組織の SSL サーバーから受け取った証明書を受け入れるには、このプロパティーを使用します。この名前の先頭または末尾にアスタリスク (*) を付けて、その有効範囲を拡張することができます。このプロパティーを指定しないと、「すべての組織」になります。このプロパティーを変更すると、経路は停止され、REFRESH コマンドを出したときに再始動されます。この経路へのすべての接続は終了します。

SSLClientDN_OU
この部門の SSL サーバーから受け取った証明書を受け入れるには、このプロパティーを使用します。この名前の先頭または末尾にアスタリスク (*) を付けて、その有効範囲を拡張することができます。このプロパティーを指定しないと、「すべての部門」を暗黙指定したことになります。このプロパティーを変更すると、経路は停止され、REFRESH コマンドを出したときに再始動されます。この経路へのすべての接続は終了します。

SSLClientDN_ST
この都道府県の SSL サーバーから受け取った証明書を受け入れるには、このプロパティーを使用します。この名前の先頭または末尾にアスタリスク (*) を付けて、その有効範囲を拡張することができます。このプロパティーを指定しないと、「すべての都道府県」になります。このプロパティーを変更すると、経路は停止され、REFRESH コマンドを出したときに再始動されます。この経路へのすべての接続は終了します。

SSLClientKeyRing
クライアント証明書が入っている鍵リング・ファイルの完全修飾名。 **Windows プラットフォーム**では、ファイル分離文字として二重円記号 (¥¥) を使用する必要があります。 SSLClient を `true` に設定する場合は、SSLClientKeyRing を指定する必要があります。このプロパティーを変更すると、経路は停止され、REFRESH コマンドを出したときに再始動されます。この経路へのすべての接続は終了します。

SSLClientKeyRingPW
クライアント鍵リングをオープンするためのパスワードが入っている完全修飾ファイル名。 **Windows プラットフォーム**では、ファイル分離文字として二重円記号 (¥¥) を使用する必要があります。 SSLClient を `true` に設定する場合は、SSLClientKeyRingPW を指定する必要があります。このプロパティーを変更すると、経路は停止され、REFRESH コマンドを出したときに再始動されます。この経路へのすべての接続は終了します。

SSLProxyMode
経路が SSL クライアント接続要求のみを受け入れ、要求を直接宛先へトンネル化できるようにするには、このプロパティーを `true` に設定します。このプロパティーを変更すると、経路は停止され、REFRESH コマンドを出したときに再始動されます。この経路へのすべての接続は終了します。このプロパティーは、以下のプロパティーと一緒に使用できます。

- HTTP

- QoS
- SocksClient
- SSLClient
- SSLServer

SSLServer
経路を SSL サーバーとして機能させ、着信 SSL 接続を受け入れるようにするには、このプロパティーを true に設定します。 true に設定することは、呼び出し側が、SSL クライアントとして機能する別の MQIPT であることを意味します。このプロパティーを変更すると、経路は停止され、REFRESH コマンドを出したときに再始動されます。この経路へのすべての接続は終了します。このプロパティーは、以下のプロパティーと一緒に使用できます。

- QoS
- SocksServer
- SSLProxyMode

SSLServerAskClientAuth
SSL サーバーによる SSL クライアント認証を要求するには、このプロパティーを使用します。 SSL クライアントは、SSL サーバーに送信する独自の証明書を持っていなければなりません。この証明書は鍵リング・ファイルから取り出されます。このプロパティーを変更すると、経路は停止され、REFRESH コマンドを出したときに再始動されます。この経路へのすべての接続は終了します。

SSLServerCipherSuites
SSL サーバー・サイドで使用する SSL 暗号スイートの名前。この名前として可能なのは、サポートされている 1 つまたは複数の暗号スイートです。この名前をブランクにしておくと、SSL サーバーは SSLServerKeyRing からとった、サポートされている暗号スイートを使用します。このプロパティーを変更すると、経路は停止され、REFRESH コマンドを出したときに再始動されます。この経路へのすべての接続は終了します。

SSLServerDN_C
この国名の SSL クライアントから受け取った証明書を受け入れるには、このプロパティーを使用します。この名前の先頭または末尾にアスタリスク (*) を付けて、その有効範囲を拡張することができます。このプロパティーを指定しないと、「すべての会社名」を暗黙指定したことになります。このプロパティーを変更すると、経路は停止され、REFRESH コマンドを出したときに再始動されます。この経路へのすべての接続は終了します。

SSLServerDN_CN
この共有名の SSL クライアントから受け取った証明書を受け入れるには、このプロパティーを使用します。この名前の先頭または末尾にアスタリスク (*) を付けて、その有効範囲を拡張することができます。このプロパティーを指定しないと、「すべての共有名」を暗黙指定したことになります。このプロパティーを変更すると、経路は停止され、REFRESH コマンドを出したときに再始動されます。この経路へのすべての接続は終了します。

SSLServerDN_L
このロケーションの SSL クライアントから受け取った証明書を受け入れるには、このプロパティーを使用します。この名前の先頭または末尾にアスタリスク (*) を付けて、その有効範囲を拡張することができます。このプロパティーを指

定しないと、「すべてのロケーション」を暗黙指定したことになります。このプロパティーを変更すると、経路は停止され、REFRESH コマンドを出したときに再始動されます。この経路へのすべての接続は終了します。

SSLServerDN_O
この組織の SSL クライアントから受け取った証明書を受け入れるには、このプロパティーを使用します。この名前の先頭または末尾にアスタリスク (*) を付けて、その有効範囲を拡張することができます。このプロパティーを指定しないと、「すべての組織」を暗黙指定したことになります。このプロパティーを変更すると、経路は停止され、REFRESH コマンドを出したときに再始動されます。この経路へのすべての接続は終了します。

SSLServerDN_OU
この部門の SSL クライアントから受け取った証明書を受け入れるには、このプロパティーを使用します。この名前の先頭または末尾にアスタリスク (*) を付けて、その有効範囲を拡張することができます。このプロパティーを指定しないと、「すべての部門」を暗黙指定したことになります。このプロパティーを変更すると、経路は停止され、REFRESH コマンドを出したときに再始動されます。この経路へのすべての接続は終了します。

SSLServerDN_ST
この都道府県の SSL クライアントから受け取った証明書を受け入れるには、このプロパティーを使用します。この名前の先頭または末尾にアスタリスク (*) を付けて、その有効範囲を拡張することができます。このプロパティーを指定しないと、「すべての都道府県」を暗黙指定したことになります。このプロパティーを変更すると、経路は停止され、REFRESH コマンドを出したときに再始動されます。この経路へのすべての接続は終了します。

SSLServerKeyRing
サーバー証明書が入っている鍵リング・ファイルの完全修飾名。 **Windows プラットフォーム**では、ファイル分離文字として二重円記号 (¥¥) を使用する必要があります。 SSLServer を `true` にする場合は、SSLServerKeyRing を指定する必要があります。このプロパティーを変更すると、経路は停止され、REFRESH コマンドを出したときに再始動されます。この経路へのすべての接続は終了します。

SSLServerKeyRingPW
サーバー鍵リングをオープンするためのパスワードが入っている完全修飾ファイル名。 **Windows プラットフォーム**では、ファイル分離文字として二重円記号 (¥¥) を使用する必要があります。 SSLServer を `true` にする場合は、SSLServerKeyRingPW を指定する必要があります。このプロパティーを変更すると、経路は停止され、REFRESH コマンドを出したときに再始動されます。この経路へのすべての接続は終了します。

Trace
必要なトレースのレベルは、0 ～ 5 の範囲の整数で指定できます。 0 の値はトレースを行わないことを意味し、 5 は全トレースを要求します。

このプロパティーを変更したために経路が影響を受ける場合は、REFRESH コマンドを出すときにこの新規値を使用します。すべての接続がこの新規値を即時にとり上げます。経路は終了します。

UriName

このプロパティーを使用すれば、HTTP プロキシーや MQIPT サーブレットを使用するときに、リソースの Uniform Resource Identifier の名前を変更することができます。ただし、ほとんどの構成の場合、デフォルト値が使用されます。HTTP プロキシーの場合のデフォルトは、次のようになっています。

```
HTTP://<destination>:<destination_port>/mqipt
```

MQIPT サーブレットの場合のデフォルトは、次のようになっています。

```
HTTP://<destination>:<destination_port>/MQIPTServlet
```

このプロパティーを変更 (および、HTTP または ServletClient を `True` に設定) すると、経路は停止され、REFRESH コマンドを出したときに再始動されます。

第 10 章 internet pass-thru の使用開始

この章では、MQIPT の使用を開始するのに役立つ情報を提供します。ここでは、本製品を正しくインストールするためのいくつかの簡単な構成をセットアップします。

この章には、以下のようなセクションが設けられています。

- 『前提事項』
- 72 ページの『構成の例』
- 72 ページの『インストール検証テスト』
- 74 ページの『SSL サーバー認証』
- 77 ページの『SSL クライアント認証』
- 79 ページの『HTTP プロキシー構成』
- 82 ページの『構成アクセス制御』
- 85 ページの『Quality of Service (QoS) の構成』
- 88 ページの『SOCKS プロキシーの構成』
- 90 ページの『SOCKS クライアントの構成』
- 91 ページの『SSL プロキシーの構成』
- 95 ページの『SSL テスト証明書の作成』
- 96 ページの『MQIPT サーブレットの構成』
- 98 ページの『MQIPT クラスター化サポートの構成』
- 102 ページの『鍵リング・ファイルの作成』

前提事項

各例について、以下のような前提事項を想定しています。

- Windows NT を使用する (ただし、各例は、サポートされている任意のプラットフォームで稼働する)
- ユーザーは、キュー・マネージャー、キュー、および WebSphere MQ 上のチャネルについて詳しい知識を持っている
- WebSphere MQ クライアントおよびサーバーがインストール済みである
- MQIPT が `C:¥mqipt` (Windows の場合) ディレクトリーにインストール済みである
- クライアント、サーバー、および各 MQIPT が別々のマシンにインストール済みである
- ユーザーが、`amqsputc` コマンドを使用してメッセージをキューに入れる操作に慣れている
- ユーザーが、`amqsgetc` コマンドを使用してメッセージをキューから取り出す操作に慣れている

WebSphere MQ サーバーでは、以下の作業が完了しています。

- MQIPT.QM1 というキュー・マネージャーの定義
- MQIPT.CONN.CHANNEL というサーバー接続チャネルの定義
- MQIPT.LOCAL.QUEUE というローカル・キューの定義
- ポート 1414 での MQIPT.QM1 に対する TCP/IP の開始

同一マシン上の 1 つのポート・アドレスでは、1 つのアプリケーションしか listen できません。ポート 1414 が使用中であれば、空きポート・アドレスを選択し、例の中の 1414 と置き換えます。

これを済ませておけば、amqsputc コマンドを使用してメッセージをキュー・マネージャーのローカル・キューに入れ、 amqsgetc コマンドを使用してそれを取り出すことにより、WebSphere MQ クライアントからキュー・マネージャーへの経路をテストすることができます。

構成の例

以下の例は、ダイアグラムとステップバイステップの指示で表されています。各ダイアグラムの右側にあるチェック・ボックスを使用して、例の進行状況を追跡することができます。一部の例では、mqipt.conf ファイルの編集が必要になります。このファイルは、MQIPT ホーム・ディレクトリーに収められています。

開始する前に、以下の作業を完了していることを確認してください。

- mqiptSample.conf を mqipt.conf にコピーする
- mqipt.conf を編集し、すべての経路を削除する
- ClientAccess のエントリーを True に変更する
- Destination を mqserver.company2.com からキュー・マネージャーの宛先へ変更する
- DestinationPort アドレスをキュー・マネージャーで使用するアドレスへ変更する
- 71 ページの『前提事項』を読む

インストール検証テスト

これは、MQIPT が正しくインストールされたことを確認するための簡単な構成です。

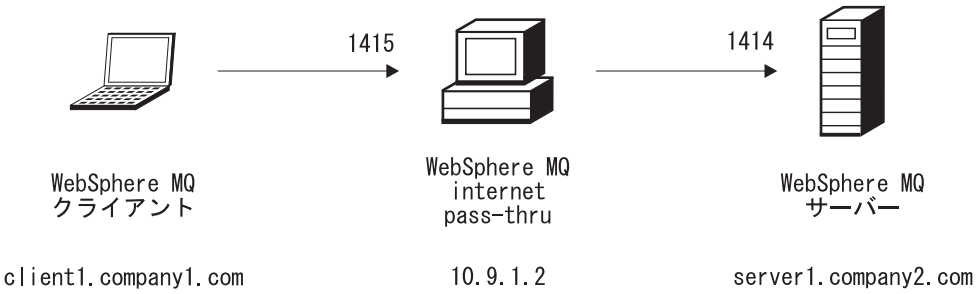

図 10. IVT ネットワーク・ダイアグラム

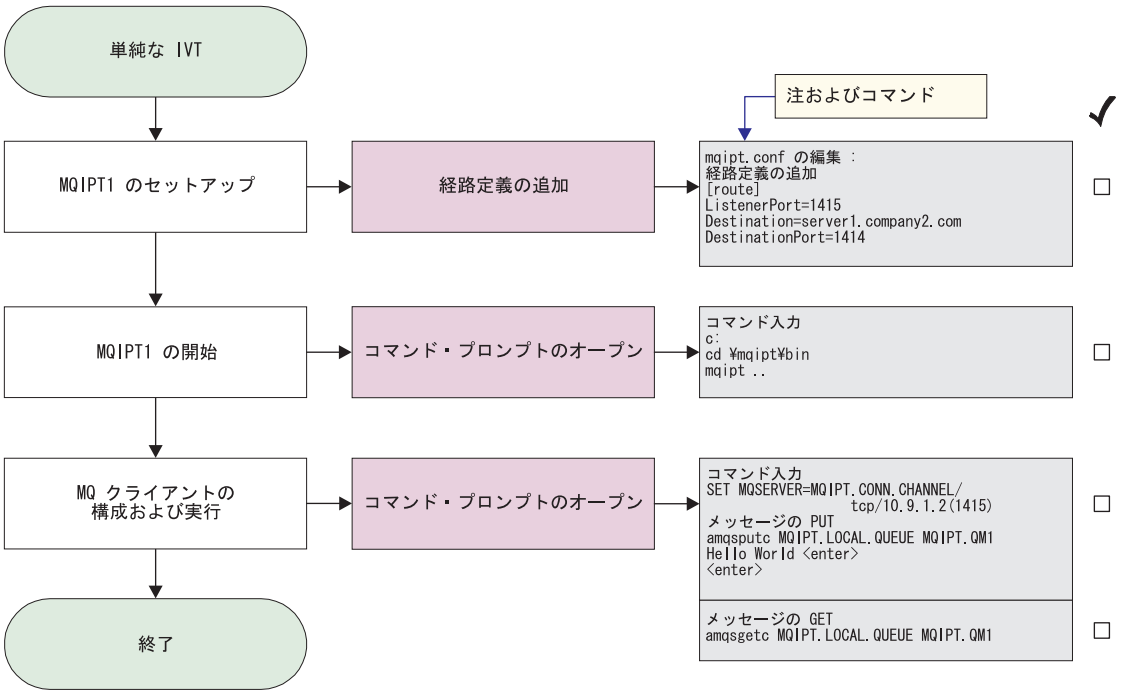

図 11. IVT 構成

開始する前に、以下の作業を行います。

1. MQIPT1 をセットアップします

   mqipt.conf を編集し、経路定義を追加します。

   ```
   [route]
   ListenerPort=1415
   Destination=server1.company2.com
   DestinationPort=1414
   ```

2. MQIPT1 を開始します

   コマンド・プロンプトをオープンし、次のように入力します。

   ```
   c:
   cd ¥mqipt¥bin
   mqipt ..
   ```

   以下のメッセージが正常終了を示します。

   ```
   5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
   MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
   MQCPI004 Reading configuration information from C:¥mqipt¥mqipt.conf
   MQCPI011 The path C:¥mqipt¥logs will be used to store the log files
   MQCPI006 Route 1415 has started and will forward messages to :
   MQCPI034 ....server1.company2.com(1414)
   MQCPI035 ....using MQ protocols
   ```

3. WebSphere MQ クライアント・マシンのコマンド・プロンプトに対して、次のように入力します。

   ```
   SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/10.9.1.2(1415)
   ```

4. 以下のコマンドを使用してメッセージを入力します。

   ```
   amqsputc MQIPT.LOCAL.QUEUE MQIPT1.QM1
   Hello world <enter>
    <enter>
   ```

5. 以下のコマンドを使用してメッセージを入手します。

```
amqsgetc MQIPT.LOCAL.QUEUE MQIPT1.QM1
```

「Hello world (ようこそ)」が表示されます。

SSL サーバー認証

この例では、2 つの MQIPT を介して WebSphere MQ クライアントと WebSphere MQ サーバーを接続することにより、サンプル・テスト証明書 (sslsample.pfx 鍵リング・ファイル) を使用して SSL 接続をテストします。 SSL ハンドシェーク時に、サーバーはそのテスト証明書をクライアントに送信します。クライアントは、その証明書 (trust-as-peer フラグが付いている) のコピーを使用してサーバーを認証します。デフォルトの暗号スイート SSL_RSA_WITH_RC4_128_MD5 が使用されます (72 ページの『インストール検証テスト』から作成された mqipt.conf に基づく)。この例で使用するためのテスト証明書を作成する方法の詳細については、95 ページの『SSL テスト証明書の作成』を参照してください。

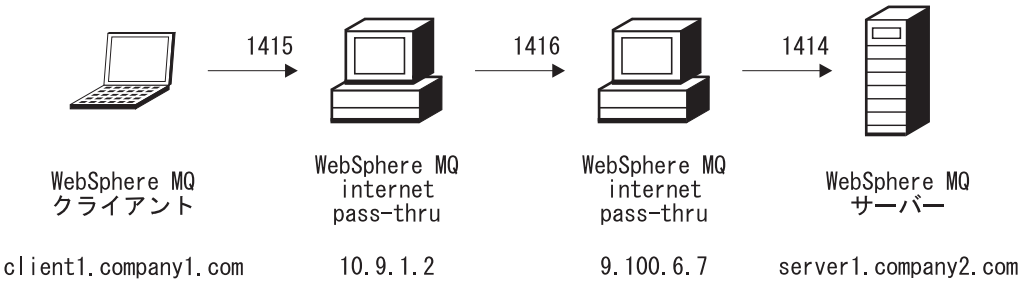

図 12. SSL サーバー・ネットワーク・ダイアグラム

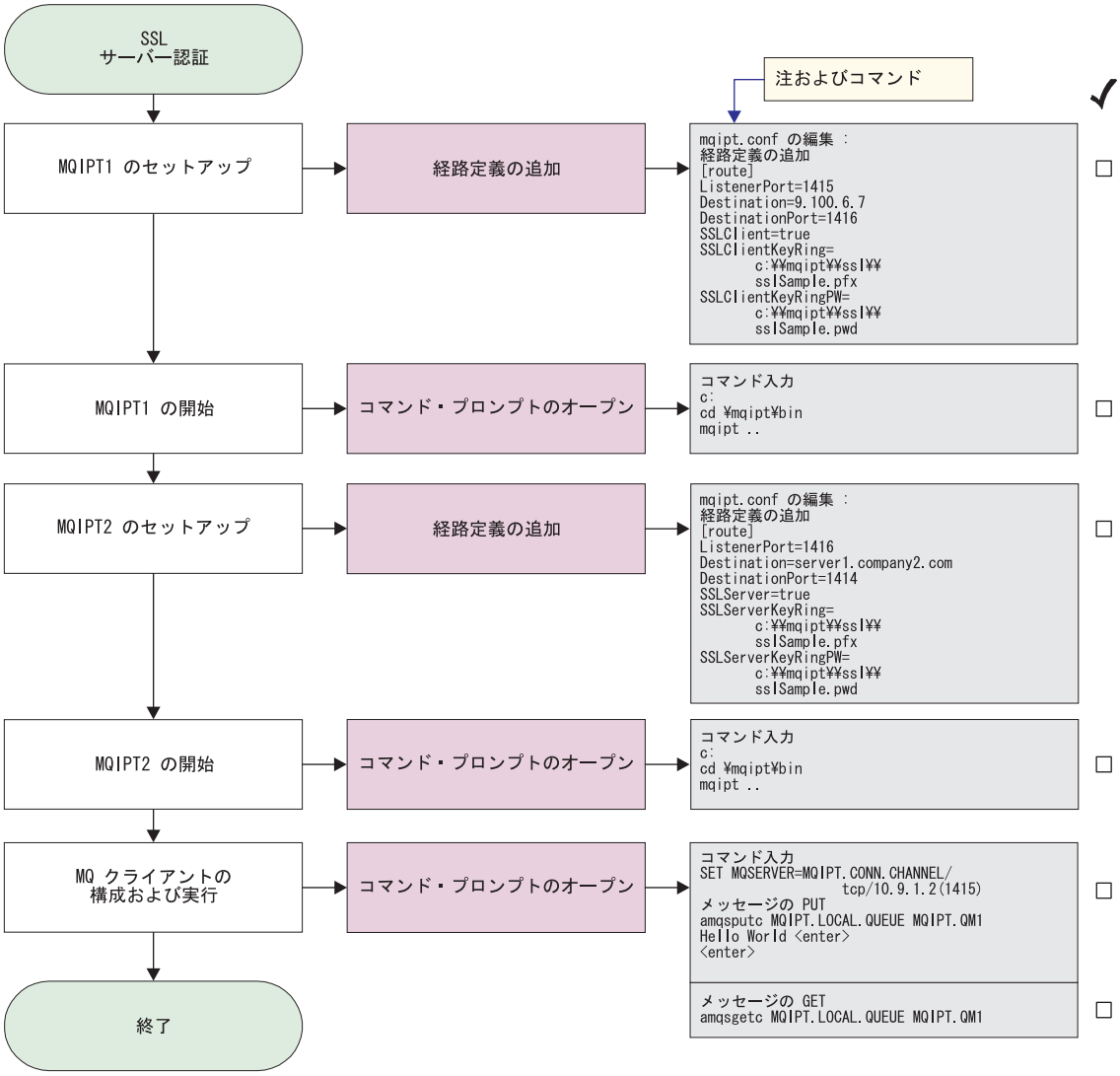

図 13. SSL サーバー認証

1. MQIPT1 をセットアップします

   mqipt.conf を編集し、経路定義を追加します。

   ```
   [route]
   ListenerPort=1415
   Destination=9.100.6.7
   DestinationPort=1416
   SSLClient=true
   SSLClientKeyRing=C:¥¥mqipt¥¥sslSample.pfx
   SSLClientKeyRingPW=C:¥¥mqipt¥¥sslSample.pwd
   ```

2. MQIPT1 を開始します

   コマンド・プロンプトをオープンし、次のように入力します。

   ```
   c:
   cd ¥mqipt¥bin
   mqipt ..
   ```

   以下のメッセージが正常終了を示します。

```
5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
MQCPI011 The path c:¥mqipt¥logs will be used to store the log files
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....9.100.6.7(1416)
MQCPI035 ....using MQ protocols
MQCPI036 ....SSL Client side enabled with properties :
MQCPI031 ......cipher suites <null>
MQCPI032 ......keyring file c:¥mqipt¥sslSample.pfx
MQCPI047 ......CA keyring file <null>
MQCPI038 ......distinguished name(s) CN=* O=* OU=* L=* ST=* C=*
```

3. MQIPT2 をセットアップします

   mqipt.conf を編集し、経路定義を追加します。

   ```
   [route]
   ListenerPort=1416
   Destination=Server1.company2.com
   DestinationPort=1414
   SSLClient=true
   SSLServerKeyRing=C:¥¥mqipt¥¥sslSample.pfx
   SSLServerKeyRingPW=C:¥¥mqipt¥¥sslSample.pwd
   ```

4. MQIPT2 を開始します

   コマンド・プロンプトをオープンし、次のように入力します。

   ```
   c:
   cd ¥mqipt¥bin
   mqipt
   ```

   以下のメッセージが正常終了を示します。

   ```
   5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
   MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
   MQCPI011 The path c:¥mqipt¥logs will be used to store the log files
   MQCPI006 Route 14196 has started and will forward messages to :
   MQCPI034 ....server1.company2.com(1414)
   MQCPI035 ....using MQ protocols
   MQCPI037 ....SSL Server side enabled with properties :
   MQCPI031 ......cipher suites <null>
   MQCPI032 ......keyring file c:¥mqipt¥sslSample.pfx
   MQCPI047 ......CA keyring file <null>
   MQCPI038 ......distinguished name(s) CN=* O=* OU=* L=* ST=* C=*
   MQCPI033 ......client authentication set to false
   ```

5. WebSphere MQ クライアント・マシンのコマンド・プロンプトに対して、次のように入力します。

   ```
   SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/10.9.1.2(1415)
   ```

6. 以下のコマンドを使用してメッセージを入力します。

   ```
   amqsputc MQIPT.LOCAL.QUEUE MQIPT1.QM1
   Hello world <enter>
    <enter>
   ```

7. 以下のコマンドを使用してメッセージを入手します。

   ```
   amqsgetc MQIPT.LOCAL.QUEUE MQIPT1.QM1
   ```

「Hello world (ようこそ)」が表示されます。

SSL クライアント認証

この例では、サンプル・テスト証明書を使用して SSL 接続をテストします。このテストではサーバーとクライアントの認証を行います。 SSL ハンドシェーク時に、サーバーはそのテスト証明書をクライアントに送信します。クライアントは、その証明書 (trust-as-peer フラグが付いている) のコピーを使用してサーバーを認証します。次に、クライアントはそのテスト証明書をサーバーに送信します。サーバーは、その証明書 (trust-as-peer フラグが付いている) のコピーを使用してクライアントを認証します。デフォルトの暗号スイート SSL_RSA_WITH_RC4_128_MD5 が使用されます (72 ページの『インストール検証テスト』から作成された mqipt.conf に基づく)。

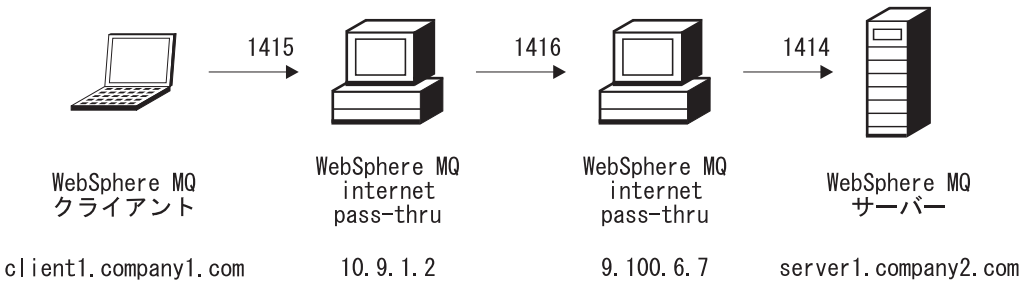

図 14. SSL クライアント・ネットワーク・ダイアグラム

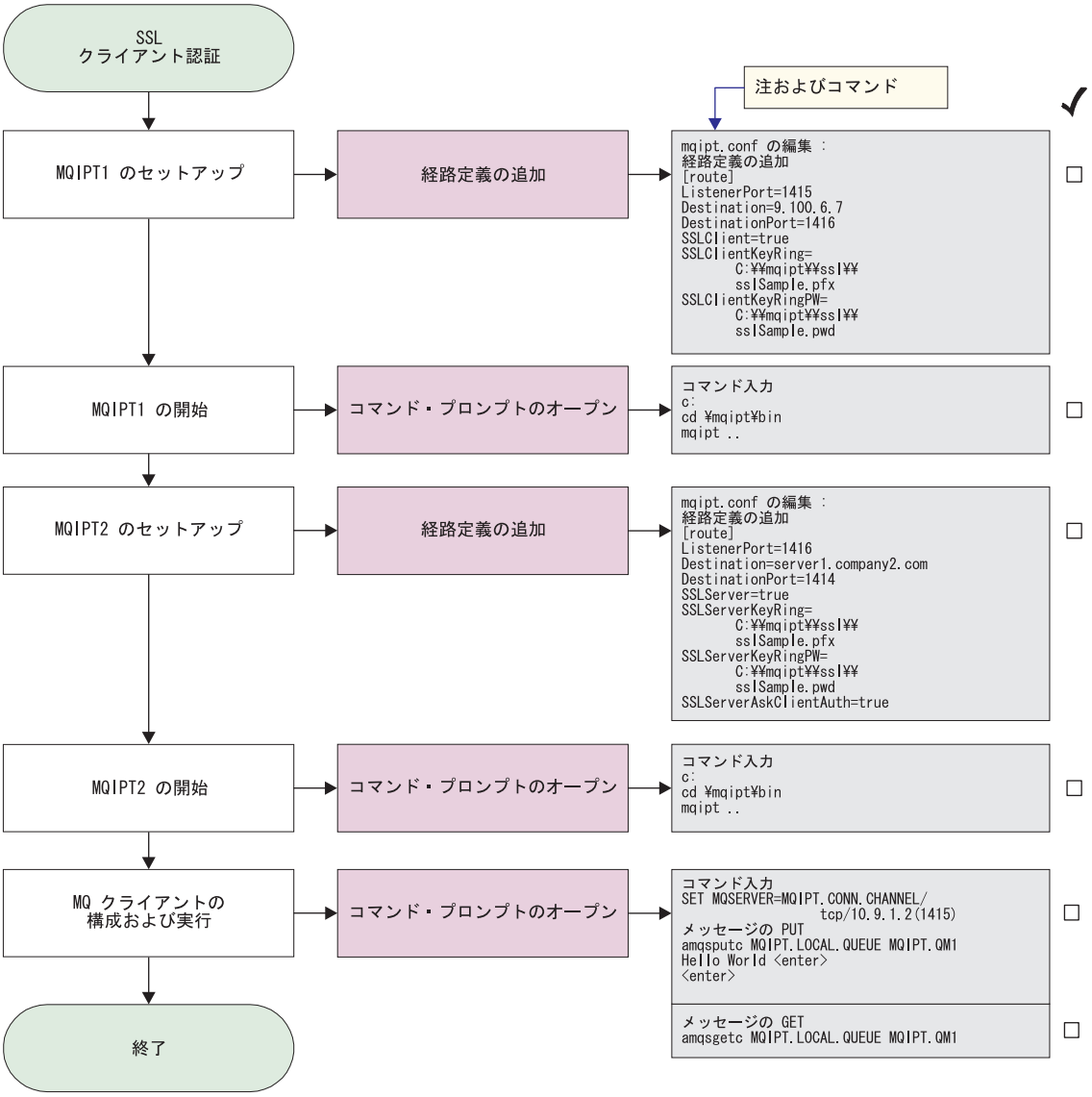

図 15. SSL クライアント認証

1. MQIPT1 をセットアップします

   mqipt.conf を編集し、経路定義を追加します。

   ```
   [route]
   ListenerPort=1415
   Destination=9.100.6.7
   DestinationPort=1416
   SSLClient=true
   SSLClientKeyRing=C:¥¥mqipt¥¥sslSample.pfx
   SSLClientKeyRingPW=C:¥¥mqipt¥¥sslSample.pwd
   ```

2. MQIPT1 を開始します

   コマンド・プロンプトをオープンし、次のように入力します。

   ```
   c:
   cd ¥mqipt¥bin
   mqipt ..
   ```

   以下のメッセージが正常終了を示します。

```
5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
MQCPI011 The path c:¥mqipt¥logs will be used to store the log files
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....9.100.6.7(1416)
MQCPI035 ....using MQ protocols
MQCPI036 ....SSL Client side enabled with properties :
MQCPI031 ......cipher suites <null>
MQCPI032 ......keyring file c:¥mqipt¥sslSample.pfx
MQCPI047 ......CA keyring file <null>
MQCPI038 ......distinguished name(s) CN=* O=* OU=* L=* ST=* C=*
```

3. MQIPT2 をセットアップします

   mqipt.conf を編集し、経路定義を追加します。

   ```
   [route]
   ListenerPort=1416
   Destination=Server1.company2.com
   DestinationPort=1414
   SSLClient=true
   SSLServerKeyRing=C:¥¥mqipt¥¥sslSample.pfx
   SSLServerKeyRingPW=C:¥¥mqipt¥¥sslSample.pwd
   ```

4. MQIPT2 を開始します

   コマンド・プロンプトをオープンし、次のように入力します。

   ```
   c:
   cd ¥mqipt¥bin
   mqipt
   ```

   以下のメッセージが正常終了を示します。

   ```
   5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
   MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
   MQCPI011 The path c:¥mqipt¥logs will be used to store the log files
   MQCPI006 Route 1416 has started and will forward messages to :
   MQCPI034 ....server1.company2.com(1414)
   MQCPI035 ....using MQ protocols
   MQCPI037 ....SSL Server side enabled with properties :
   MQCPI031 ......cipher suites <null>
   MQCPI032 ......keyring file c:¥mqipt¥sslSample.pfx
   MQCPI047 ......CA keyring file <null>
   MQCPI038 ......distinguished name(s) CN=* O=* OU=* L=* ST=* C=*
   MQCPI033 ......client authentication set to true
   ```

5. WebSphere MQ クライアント・マシンのコマンド・プロンプトに対して、次のように入力します。

   ```
   SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/10.9.1.2(1415)
   ```

6. 以下のコマンドを使用してメッセージを入力します。

   ```
   amqsputc MQIPT.LOCAL.QUEUE MQIPT1.QM1
   Hello world <enter>
    <enter>
   ```

7. 以下のコマンドを使用してメッセージを入手します。

   ```
   amqsgetc MQIPT.LOCAL.QUEUE MQIPT1.QM1
   ```

「Hello world (ようこそ)」が表示されます。

HTTP プロキシー構成

この例では、HTTP プロキシー (IBM Caching Proxy) を使用して接続をテストします。 CP はレベル 3.6 以上でなければなりません。また、以下の点についてもチェックが必要です。

- ProxyPersistance は オン でなければなりません。これによってパーシスタント接続が可能になります。
- MaxPersistRequest は 5000 でなければなりません。この数値は、接続を切断する前に単一接続で行える要求の数です。
- PersistTimeout は 12hrs でなければなりません。これは接続が存在できる時間です。

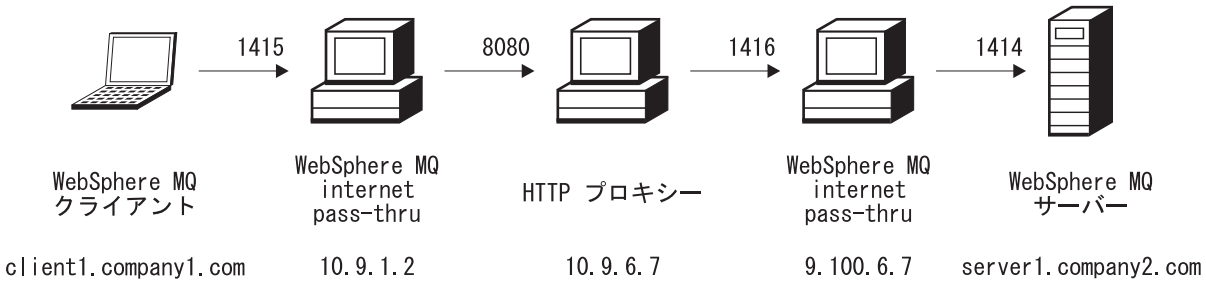

図 16. HTTP プロキシー・ネットワーク・ダイアグラム

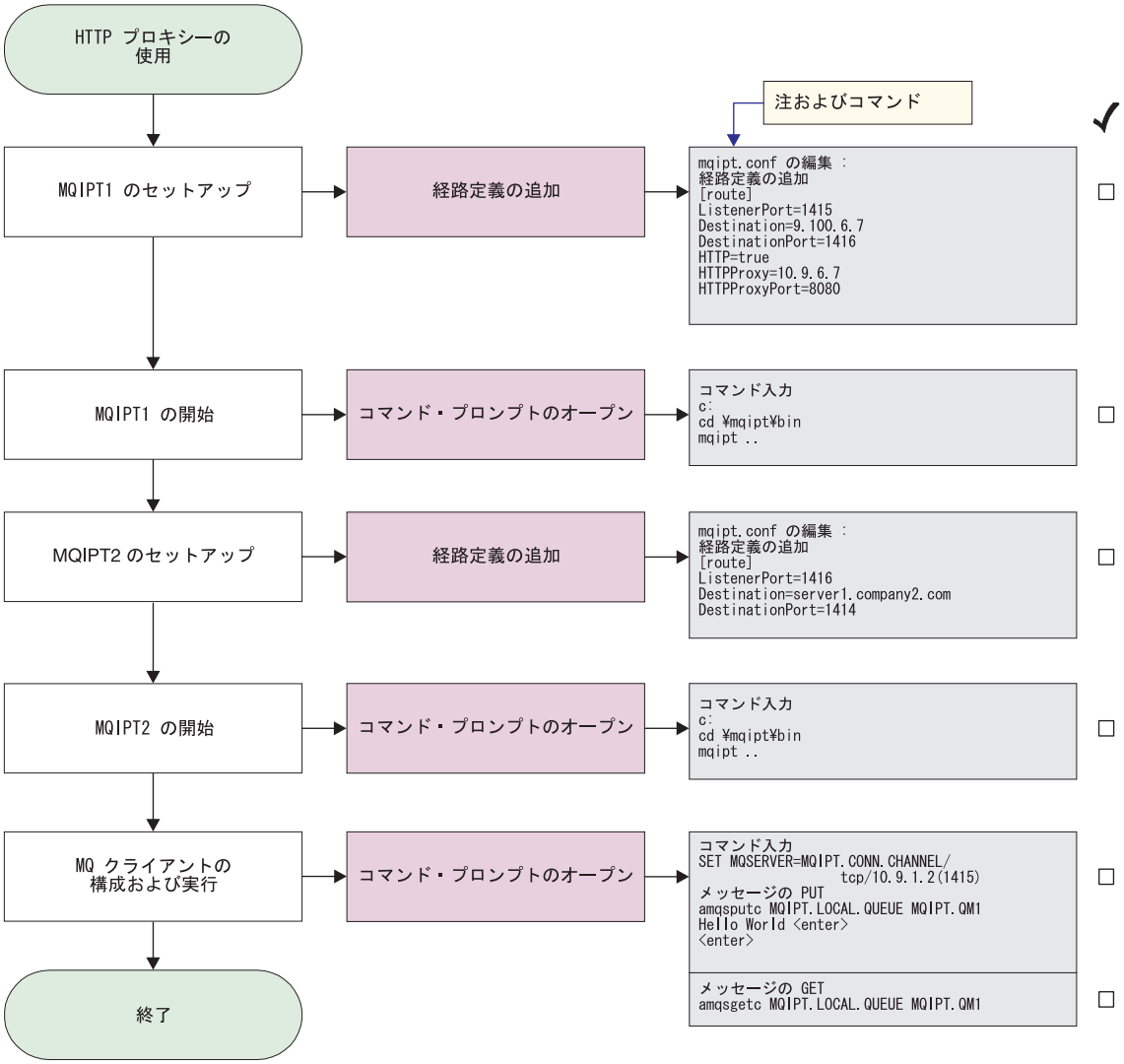

図 17. HTTP プロキシー構成

1. MQIPT1 をセットアップします

   mqipt.conf を編集し、経路定義を追加します。

   ```
   [route]
   ListenerPort=1415
   Destination=9.100.6.7
   DestinationPort=1416
   HTTP=true
   HTTPProxy=true
   HTTPProxyPort=8080
   ```

2. MQIPT1 を開始します

   コマンド・プロンプトをオープンし、次のように入力します。

   ```
   c:
   cd ¥mqipt¥bin
   mqipt ..
   ```

   以下のメッセージが正常終了を示します。

   ```
   5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
   MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
   MQCPI004 Reading configuration information from C:¥mqipt¥mqipt.conf
   ```

```
MQCPI011 The path C:¥mqipt¥logs will be used to store the log files
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....9.100.6.7(1416)
MQCPI035 ....using HTTP
MQCPI024 ....and HTTP proxy at 10.9.6.7(1080)
```

3. MQIPT2 をセットアップします

   mqipt.conf を編集し、経路定義を追加します。

   ```
   [route]
   ListenerPort=1416
   Destination=Server1.company2.com
   DestinationPort=1414
   ```

4. MQIPT2 を開始します

   コマンド・プロンプトをオープンし、次のように入力します。

   ```
   c:
   cd ¥mqipt¥bin
   mqipt
   ```

   以下のメッセージが正常終了を示します。

   ```
   5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
   MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
   MQCPI004 Reading configuration information from C:¥mqipt¥mqipt.conf
   MQCPI011 The path C:¥mqipt¥logs will be used to store the log files
   MQCPI006 Route 1416 has started and will forward messages to :
   MQCPI034 ....server1.company2.com(1414)
   MQCPI035 ....using MQ protocols
   ```

5. WebSphere MQ クライアント・マシンのコマンド・プロンプトに対して、次のように入力します。

   ```
   SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/10.9.1.2(1415)
   ```

6. 以下のコマンドを使用してメッセージを入力します。

   ```
   amqsputc MQIPT.LOCAL.QUEUE MQIPT1.QM1
   Hello world <enter>
    <enter>
   ```

7. 以下のコマンドを使用してメッセージを入手します。

   ```
   amqsgetc MQIPT.LOCAL.QUEUE MQIPT1.QM1
   ```

「Hello world (ようこそ)」が表示されます。

構成アクセス制御

この例では、セキュリティー検査を MQIPT リスナー・ポートに追加することによって、特定のクライアントからの接続だけを受け入れるように MQIPT をセットアップします。ここでは、 Java Security Manager を使用します。

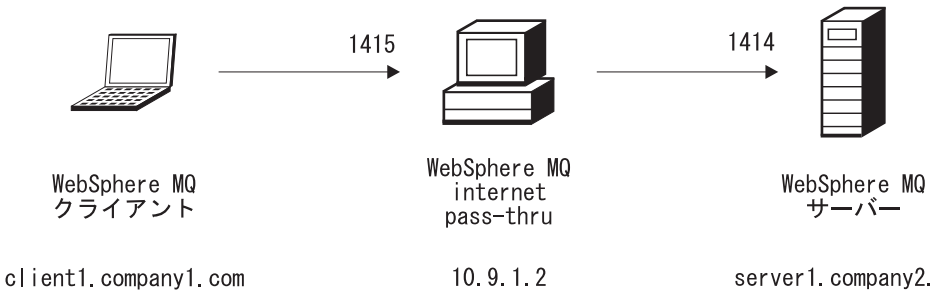

図 18. アクセス制御ネットワーク・ダイアグラム

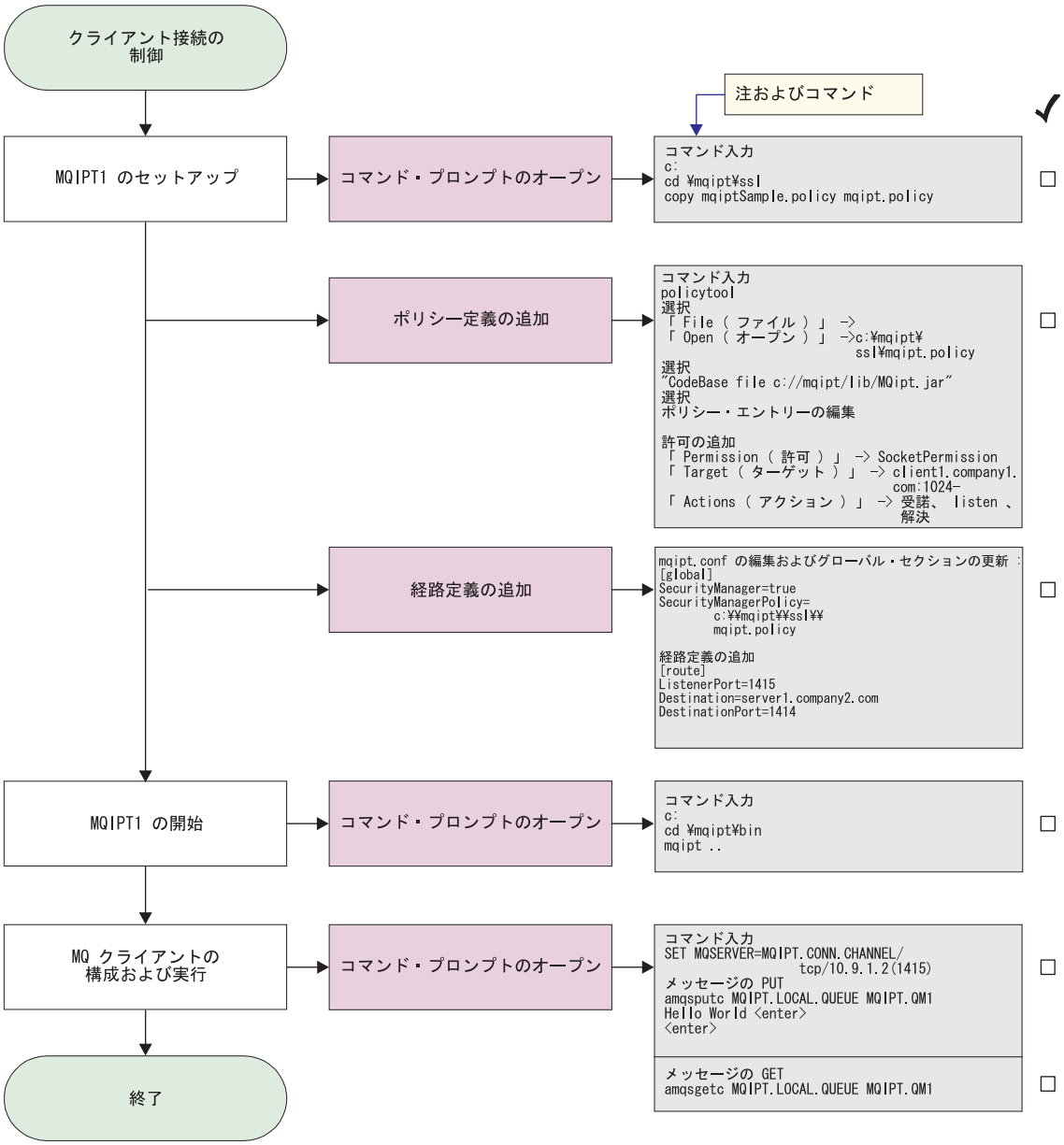

図 19. アクセス制御構成

1. MQIPT1 をセットアップします

a. コマンド・プロンプトをオープンし、次のように入力します。

```
c:
cd ¥mqipt¥ssl
copy c:¥mqipt¥ssl¥mqiptSample.policy to mqipt.policy
```

b. 以下のコマンドを使用してポリシー定義を追加します。

```
policytool
```

1) 「File (ファイル)」->「Open (オープン)」->「c:¥mqipt¥ssl¥mqipt.policy」と選択します。

2) 以下のコマンドを選択します。

```
file://C:/Program Files/IBM/WebSphere MQ internet pass-thru/lib/MQipt.jar
```

3) CodeBase を、

```
file://C:/Program Files/IBM/WebSphere MQ internet pass-thru/lib/MQipt.jar
```

から、次のように変更します。

```
file://C:/mqipt/lib/MQipt.jar
```

4) すべての許可を、

```
C:¥¥Program Files¥¥IBM¥¥WebSphere MQ internet pass-thru
```

から、次のように変更します。

```
C:¥¥mqipt
```

5) SocketPermission を追加します。

```
Permission=SocketPermission
Target=client1.company1.com:1024-
Acitons=accept, listen, resolve
```

c. mqipt.conf を編集し、

1) 2 つのプロパティーを次のグローバル・セクションに追加します。

```
[global]
SecurityManager=true
SecurityManagerPolicy=c:¥¥mqipt¥¥ssl¥¥mqipt.policy
```

2) 経路定義は、以下のとおりです。

```
[route]
ListenerPort=1415
Destination=server1.company2.com
DestinationPort=1414
```

2. MQIPT1 を開始します

コマンド・プロンプトをオープンし、次のように入力します。

```
c:
cd ¥mqipt¥bin
mqipt ..
```

以下のメッセージが正常終了を示します。

```
5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
MQCPI004 Reading configuration information from C:¥mqipt¥mqipt.conf
MQCPI055 Setting the java.security.policy to c:¥mqipt¥mqipt.policy
MQCPI053 Starting the Java Security Manager
MQCPI011 The path C:¥mqipt¥logs will be used to store the log files
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....using MQ protocols
```

3. WebSphere MQ クライアント・マシンのコマンド・プロンプトに対して、次のように入力します。

   ```
   SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/10.9.1.2(1415)
   ```

4. 以下のコマンドを使用してメッセージを入力します。

   ```
   amqsputc MQIPT.LOCAL.QUEUE MQIPT1.QM1
   Hello world <enter>
    <enter>
   ```

5. 以下のコマンドを使用してメッセージを入手します。

   ```
   amqsgetc MQIPT.LOCAL.QUEUE MQIPT1.QM1
   ```

「Hello world (ようこそ)」が表示されます。

Quality of Service (QoS) の構成

この例では、TQoS が MQIPT と同じマシンにインストールされていることを前提にしています。

この例では、Quality of Service (QoS) を MQIPT 経路上のすべてのチャネルに適用します。これは、MQIPT を Linux プラットフォームで実行するときにのみインプリメントできます。このサンプルは、MQIPT から WebSphere MQ クライアントに送信されたすべてのデータに関して「平均」の優先順位を設定し、WebSphere MQ サーバーに送信されたすべてのデーに関して「良好」の優先順位を設定します。下記のサンプル pagent ポリシーを使用すれば、以下の優先順位を `QosToCaller` と `QosToDest` に適用することができます。

- 1 - 平均
- 2 - 良好
- 3 - 非常に良好

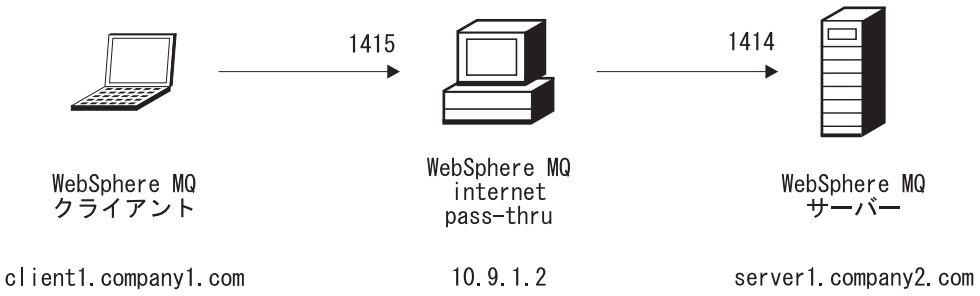

図 20. QoS ネットワーク・ダイアグラム

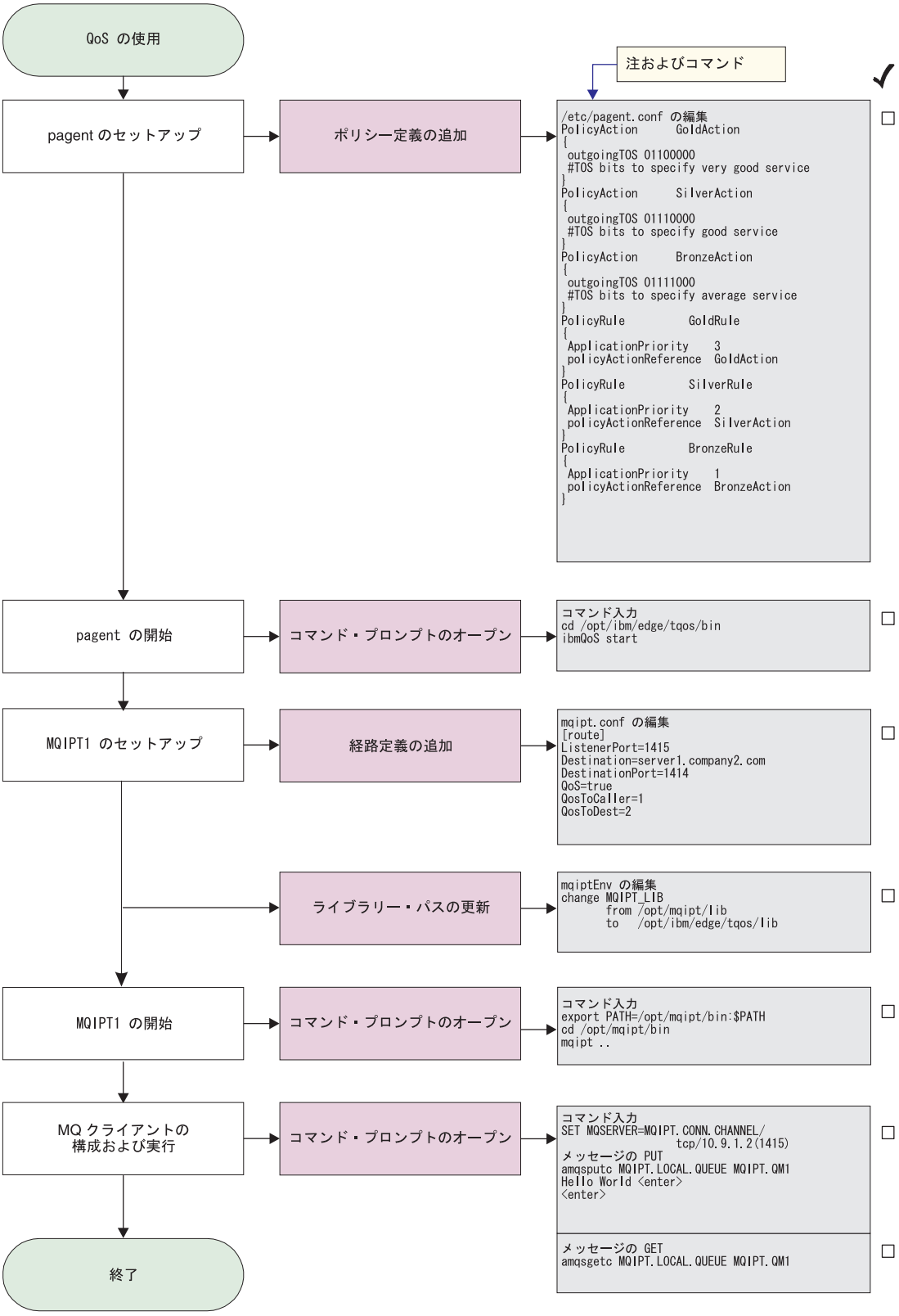

図 21. QoS 構成

1. pagent のセットアップ

   `/etc/pagent.conf` を編集し、以下のコマンドを追加します。

```
PolicyAction      GoldAction
{
 outgoingTOS 01100000
 #TOS bits to specify very good service
}
PolicyAction      SilverAction
{
 outgoingTOS 01110000
 #TOS bits to specify good service
}
PolicyAction      BronzeAction
{
 outgoingTOS 01111000
 #TOS bits to specify average service
}
PolicyRule          GoldRule
{
 ApplicationPriority    3
 policyActionReference  GoldAction
}
PolicyRule          SilverRule
{
 ApplicationPriority    2
 policyActionReference  SilverAction
}
PolicyRule          BronzeRule
{
 ApplicationPriority    1
 policyActionReference  BronzeAction
}
```

2. pagent を開始します

   コマンド・プロンプトをオープンし、次のように入力します。

   ```
   cd /opt/ibm/edge/tqos/bin
   ibmQoS start
   ```

3. MQIPT1 をセットアップします

   mqipt.conf を編集し、経路定義を追加します。

   ```
   [route]
   ListenerPort=1415
   Destination=server1.company2.com
   DestinationPort=1414
   QoS=true
   QosToCaller=1
   QosToDest=2
   ```

4. ライブラリー・パスを更新します。

   mqiptEnv (/opt/mqipt/bin に入っている) を編集し、MQIPT_LIB を、

   ```
   /opt/mqipt/lib
   ```

   から、次のように変更します。

   ```
   /opt/ibm/edge/tqos/lib
   ```

5. MQIPT1 を開始します

   コマンド・プロンプトをオープンし、次のように入力します。

   ```
   export PATH=/opt/mqipt/bin:$PATH
   cd /opt/mqipt/bin
   mqipt ..
   ```

   以下のメッセージが正常終了を示します。

```
5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
MQCPI001 Websphere MQ internet pass-thru Version 1.2 starting
MQCPI004 Reading configuration information from /opt/mqipt/mqipt.conf
MQCPI011 The path /opt/mqipt/logs will be used to store the log files
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....using MQ protocols
MQCPI049 ....QoS priority to dest = 2, to caller = 1
```

6. WebSphere MQ クライアント・マシンのコマンド・プロンプトに対して、次のように入力します。

```
SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/10.9.1.2(1415)
```

7. 以下のコマンドを使用してメッセージを入力します。

```
amqsputc MQIPT.LOCAL.QUEUE MQIPT1.QM1
Hello world <enter>
 <enter>
```

8. 以下のコマンドを使用してメッセージを入手します。

```
amqsgetc MQIPT.LOCAL.QUEUE MQIPT1.QM1
```

「Hello world (ようこそ)」が表示されます。

SOCKS プロキシーの構成

この例では、MQIPT を SOCKS プロキシーとして機能させることができます。このサンプルを実行する前に、WebSphere MQ クライアントを SOCKS 化しておかなければなりません。また SOCKS 構成が SOCKS プロキシーとしての MQIPT を指していなければなりません。 MQIPT Destination および DestinationPort プロパティーの定義は何でも構いません。それは、SOCKS ハンドシェーク・プロセス時に真の宛先を WebSphere MQ クライアントから入手するからです。

開始する前に、マシン全体または WebSphere MQ クライアント・アプリケーション (amqsputc/amqsgetc) のいずれかを SOCKS 化する必要があります。また、SOCKS クライアントも以下のように構成する必要があります。

- SOCKS プロキシーとしての MQIPT を指す
- SOCKS V5 サポートを使用可能にする
- ユーザー認証を使用不可にする
- MQIPT ネットワーク・アドレスだけと接続する

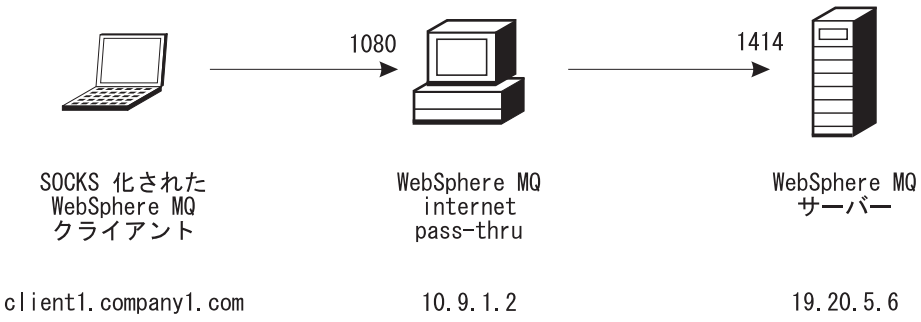

図 22. SOCKS プロキシー・ネットワーク・ダイアグラム

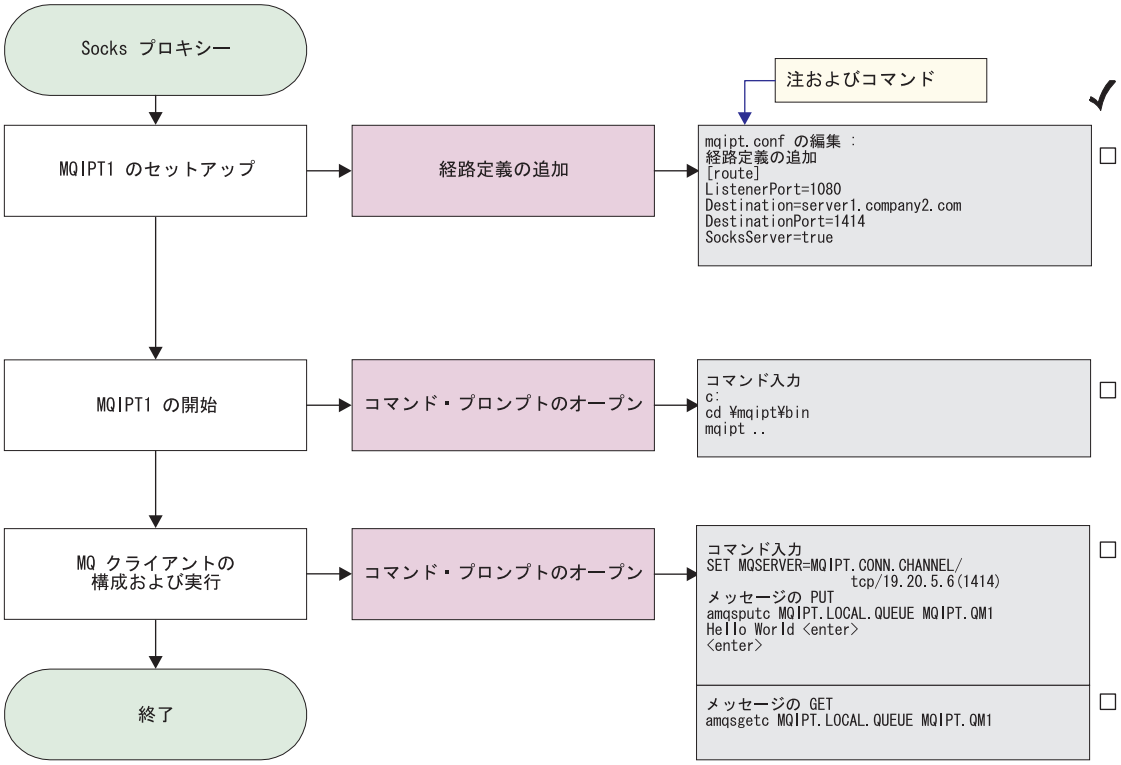

図 23. SOCKS プロキシー構成

1. MQIPT1 をセットアップします

   mqipt.conf を編集し、経路定義を追加します。

   ```
   [route]
   ListenerPort=1080
   Destination=server1.company2.com
   DestinationPort=1414
   SocksServer=true
   ```

2. MQIPT1 を開始します

   コマンド・プロンプトをオープンし、次のように入力します。

   ```
   c:
   cd ¥mqipt¥bin
   mqipt ..
   ```

   以下のメッセージが正常終了を示します。

   ```
   5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
   MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
   MQCPI004 Reading configuration information from C:¥mqipt¥mqipt.conf
   MQCPI011 The path C:¥mqipt¥logs will be used to store the log files
   MQCPI006 Route 1080 has started and will forward messages to :
   MQCPI034 ....server1.company2.com(1414)
   MQCPI035 ....using MQ protocols
   MQCPI052 ....Socks server side enabled
   ```

3. WebSphere MQ クライアント・マシンのコマンド・プロンプトに対して、次のように入力します。

   ```
   SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/19.20.5.6(1414)
   ```

4. 以下のコマンドを使用してメッセージを入力します。

```
amqsputc MQIPT.LOCAL.QUEUE MQIPT1.QM1
Hello world <enter>
 <enter>
```

5. 以下のコマンドを使用してメッセージを入手します。

```
amqsgetc MQIPT.LOCAL.QUEUE MQIPT1.QM1
```

「Hello world (ようこそ)」が表示されます。

SOCKS クライアントの構成

この例では、既存の SOCKS プロキシーを使用して、MQIPT をあたかも SOCKS 化されているかのように機能させます。この方法は 88 ページの『SOCKS プロキシーの構成』の場合と似ていますが、MQIPT が、WebSphere MQ クライアントではなく、SOCKS 化された接続を行う点が異なります。

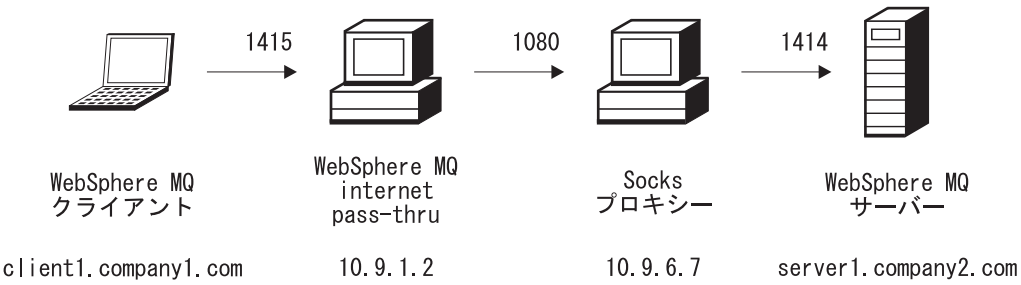

図 24. SOCKS クライアント・ネットワーク・ダイアグラム

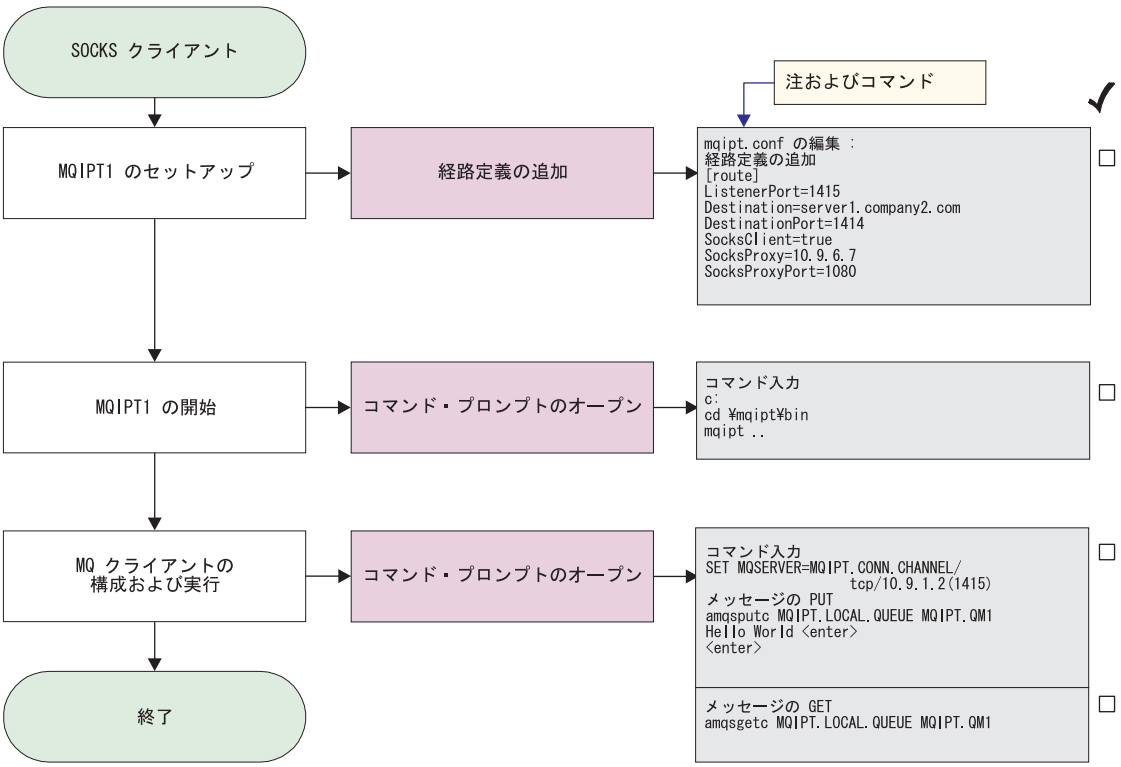

図 25. SOCKS クライアント構成

1. MQIPT1 をセットアップします

   mqipt.conf を編集し、経路定義を追加します。

   ```
   [route]
   ListenerPort=1415
   Destination=server1.company2.com
   DestinationPort=1414
   SocksClient=true
   SocksProxy=10.9.6.7
   SocksProxyPort=1080
   ```

2. MQIPT1 を開始します

   コマンド・プロンプトをオープンし、次のように入力します。

   ```
   c:
   cd ¥mqipt¥bin
   mqipt ..
   ```

   以下のメッセージが正常終了を示します。

   ```
   5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
   MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
   MQCPI004 Reading configuration information from C:¥mqipt¥mqipt.conf
   MQCPI022 Password checking has been disabled on the command port
   MQCPI011 The path C:¥mqipt¥logs will be used to store the log files
   MQCPI006 Route 1415 has started and will forward messages to :
   MQCPI034 ....server1.company2.com(1414)
   MQCPI035 ....using MQ protocols
   MQCPI039 ....and Socks proxy at 10.9.6.7(1080)
   ```

3. WebSphere MQ クライアント・マシンのコマンド・プロンプトに対して、次のように入力します。

   ```
   SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/10.9.1.2(1415)
   ```

4. 以下のコマンドを使用してメッセージを入力します。

   ```
   amqsputc MQIPT.LOCAL.QUEUE MQIPT1.QM1
   Hello world <enter>
    <enter>
   ```

5. 以下のコマンドを使用してメッセージを入手します。

   ```
   amqsgetc MQIPT.LOCAL.QUEUE MQIPT1.QM1
   ```

「Hello world (ようこそ)」が表示されます。

SSL プロキシーの構成

この例では、MQIPT を SSL プロキシー・モードで実行し、MQIPT が SSL クライアントからの SSL 接続要求を受け入れて、それを SSL サーバーへトンネル操作で送信できるようにします。

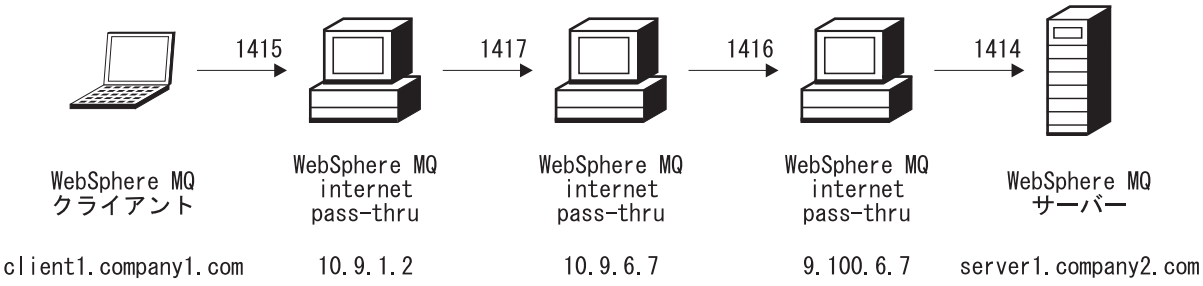

図 26. SSL プロキシー・ネットワーク・ダイアグラム

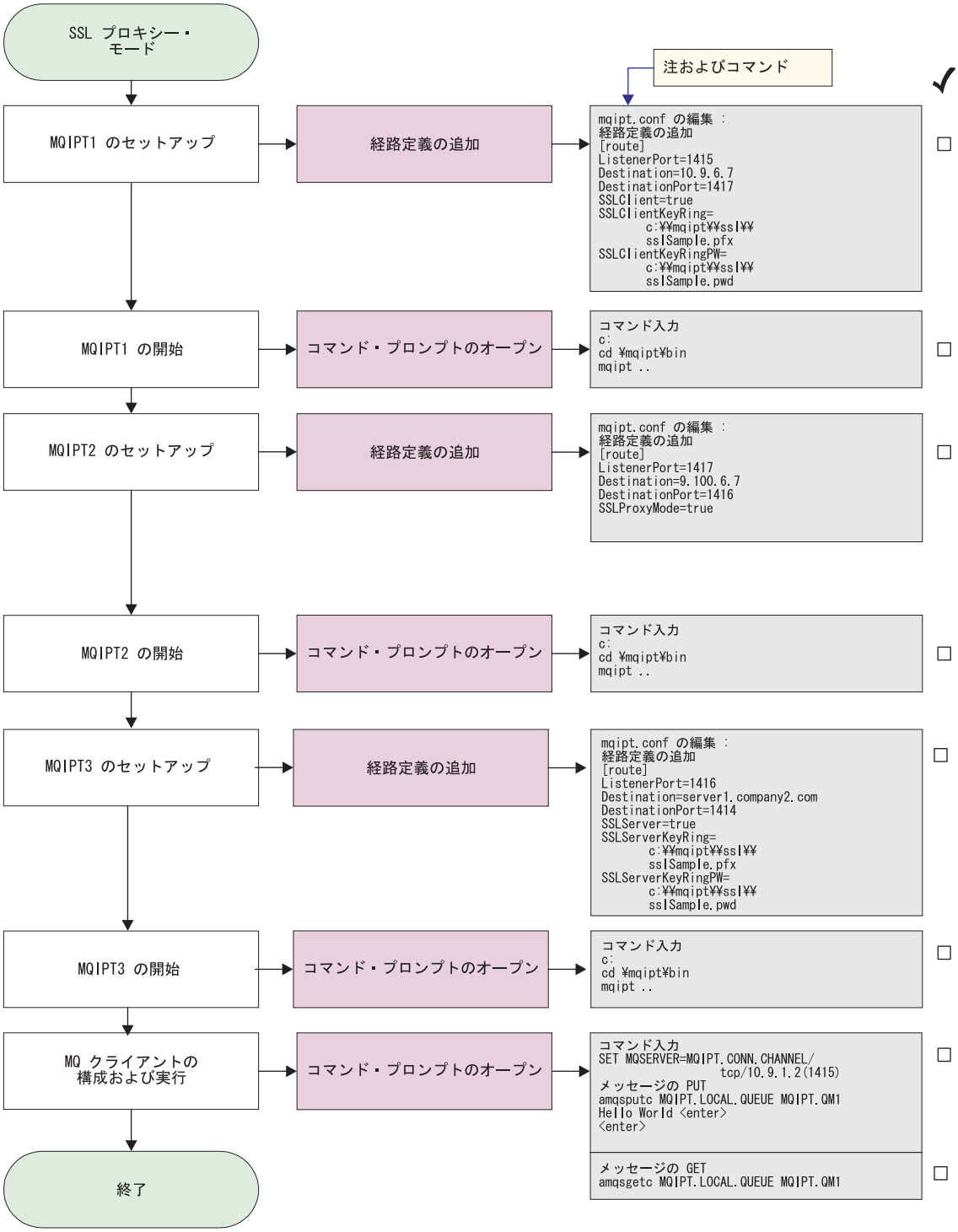

図 27. SSL プロキシー構成

1. MQIPT1 をセットアップします

   `mqipt.conf` を編集し、経路定義を追加します。

   ```
   [route]
   ListenerPort=1415
   Destination=10.9.6.7
   DestinationPort=1417
   ```

```
SSLClient=true
SSLClientKeyRing=c:¥¥mqipt¥¥ssl¥¥sslSample.pfx
SSLClientKeyRingPW=c:¥¥mqipt¥¥ssl¥¥sslSample.pwd
```

2. MQIPT1 を開始します

   コマンド・プロンプトをオープンし、次のように入力します。

   ```
   c:
   cd ¥mqipt¥bin
   mqipt ..
   ```

   以下のメッセージが正常終了を示します。

   ```
   5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
   MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
   MQCPI004 Reading configuration information from C:¥mqipt¥mqipt.conf
   MQCPI011 The path C:¥mqipt¥logs will be used to store the log files
   MQCPI006 Route 1415 has started and will forward messages to :
   MQCPI034 ....10.9.6.7(1417)
   MQCPI035 ....using MQ protocols
   MQCPI036 ....SSL Client side enabled with properties :
   MQCPI031 ......cipher suites <null>
   MQCPI032 ......keyring file c:¥mqipt¥ssl¥sslSample.pfx
   MQCPI047 ......CA keyring file <null>
   MQCPI038 ......distinguished name(s) CN=* O=* OU=* L=* ST=* C=*
   ```

3. MQIPT2 をセットアップします

   mqipt.conf を編集し、経路定義を追加します。

   ```
   [route]
   ListenerPort=1417
   Destination=9.100.6.7
   DestinationPort=1416
   SSLProxyMode=true
   ```

4. MQIPT2 を開始します

   コマンド・プロンプトをオープンし、次のように入力します。

   ```
   c:
   cd ¥mqipt¥bin
   mqipt
   ```

   以下のメッセージが正常終了を示します。

   ```
   5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
   MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
   MQCPI004 Reading configuration information from C:¥mqipt¥mqipt.conf
   MQCPI011 The path C:¥mqipt¥logs will be used to store the log files
   MQCPI006 Route 1417 has started and will forward messages to :
   MQCPI034 ....9.100.6.7(1416)
   MQCPI035 ....using SSLProxyMode
   ```

5. MQIPT3 をセットアップします

   mqipt.conf を編集し、経路定義を追加します。

   ```
   [route]
   ListenerPort=1416
   Destination=server1.company2.com
   DestinationPort=1414
   SSLServer=true
   SSLServerKeyRing=c:¥¥mqipt¥¥ssl¥¥sslSample.pfx
   SSLServerKeyRingPW=c:¥¥mqipt¥¥ssl¥¥sslSample.pwd
   ```

6. MQIPT3 を開始します

   コマンド・プロンプトをオープンし、次のように入力します。

```
c:
cd ¥mqipt¥bin
mqipt
```

以下のメッセージが正常終了を示します。

```
5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
MQCPI004 Reading configuration information from C:¥mqipt¥mqipt.conf
MQCPI011 The path C:¥mqipt¥logs will be used to store the log files
MQCPI006 Route 1416 has started and will forward messages to :
MQCPI034 ....server1.company2.com(1414)
MQCPI035 ....using MQ protocols
MQCPI037 ....SSL Server side enabled with properties :
MQCPI031 ......cipher suites <null>
MQCPI032 ......keyring file c:¥mqipt¥ssl¥sslSample.pfx
MQCPI047 ......CA keyring file <null>
MQCPI038 ......distinguished name(s) CN=* O=* OU=* L=* ST=* C=*
MQCPI033 ......client authentication set to false
```

7. WebSphere MQ クライアント・マシンのコマンド・プロンプトに対して、次のように入力します。

```
SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/10.9.1.2(1415)
```

8. 以下のコマンドを使用してメッセージを入力します。

```
amqsputc MQIPT.LOCAL.QUEUE MQIPT1.QM1
Hello world <enter>
 <enter>
```

9. 以下のコマンドを使用してメッセージを入手します。

```
amqsgetc MQIPT.LOCAL.QUEUE MQIPT1.QM1
```

「Hello world (ようこそ)」が表示されます。

SSL テスト証明書の作成

この例では、MQIPT 経路のテストに使用できる自己署名証明書を作成する方法を示します。この証明書では、trust-as-peer フラグをオンにします。

1. KeyMan を開始します
2. 「Create new... (新規作成...)」を選択します
3. 「PKCS#12 Token (PKCS#12 トークン)」を選択します
4. 「Action (アクション)」->「Generate Key (鍵を生成)」と選択します
   新規の鍵ペアが ″RSA / 1024-bit″ リストに表示されます
5. 新規の鍵ペアを選択します
6. 「Action (アクション)」->「Create Certificate (証明書を作成)」と選択します
7. 「Self-signed Certificate (自己署名証明書)」を選択します
8. 証明書の詳細情報を入力します
   ダイアログが表示され、「私用証明書が鍵と結合され、ラベルの入力はオプショナルである」ことが示されます。
9. 新規の証明書を選択します
10. 証明書の詳細情報を表示します
11. 証明書プロパティーを変更します
12. trust-as-peer フラグをオンにします

13. ダイアログをクローズし、「File (ファイル)」->「Save (保管)」と選択します
14. パスワードを入力します (たとえば、myPassWord)
15. 新規の鍵リング・ファイルのファイル名を入力します (たとえば、c:¥mqipt¥ssl¥testRoute1414.pfx)

    「File format as PKCS#12 / PFX (PKCS#12 / PFX としてのファイル形式)」を保持し、「Wrap key ring into a Java class (鍵リングを Java クラスにラップする)」に**チェックマークを付けないでください**
16. 上記操作で使用したパスワード (myPassWord) が入っているテキスト・ファイルを作成します。

    たとえば、c:¥mqipt¥ssl¥testRoute1414.pwd

これで、この鍵リング・ファイルを 74 ページの『SSL サーバー認証』例で使用できるようになりました。

MQIPT サーブレットの構成

このサンプルでは Tomcat Application Server を使用するので、それが c:¥jakarta-tomcat-4.0.1 ディレクトリーにインストール済みであることが前提です。

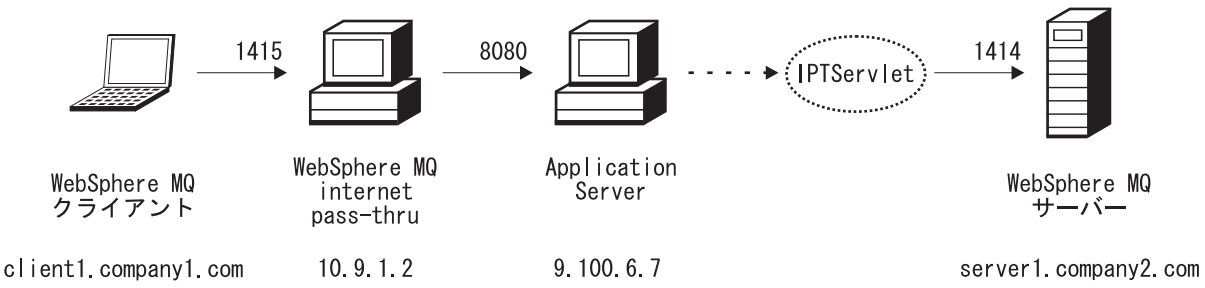

図 28. サーブレット・ネットワーク・ダイアグラム

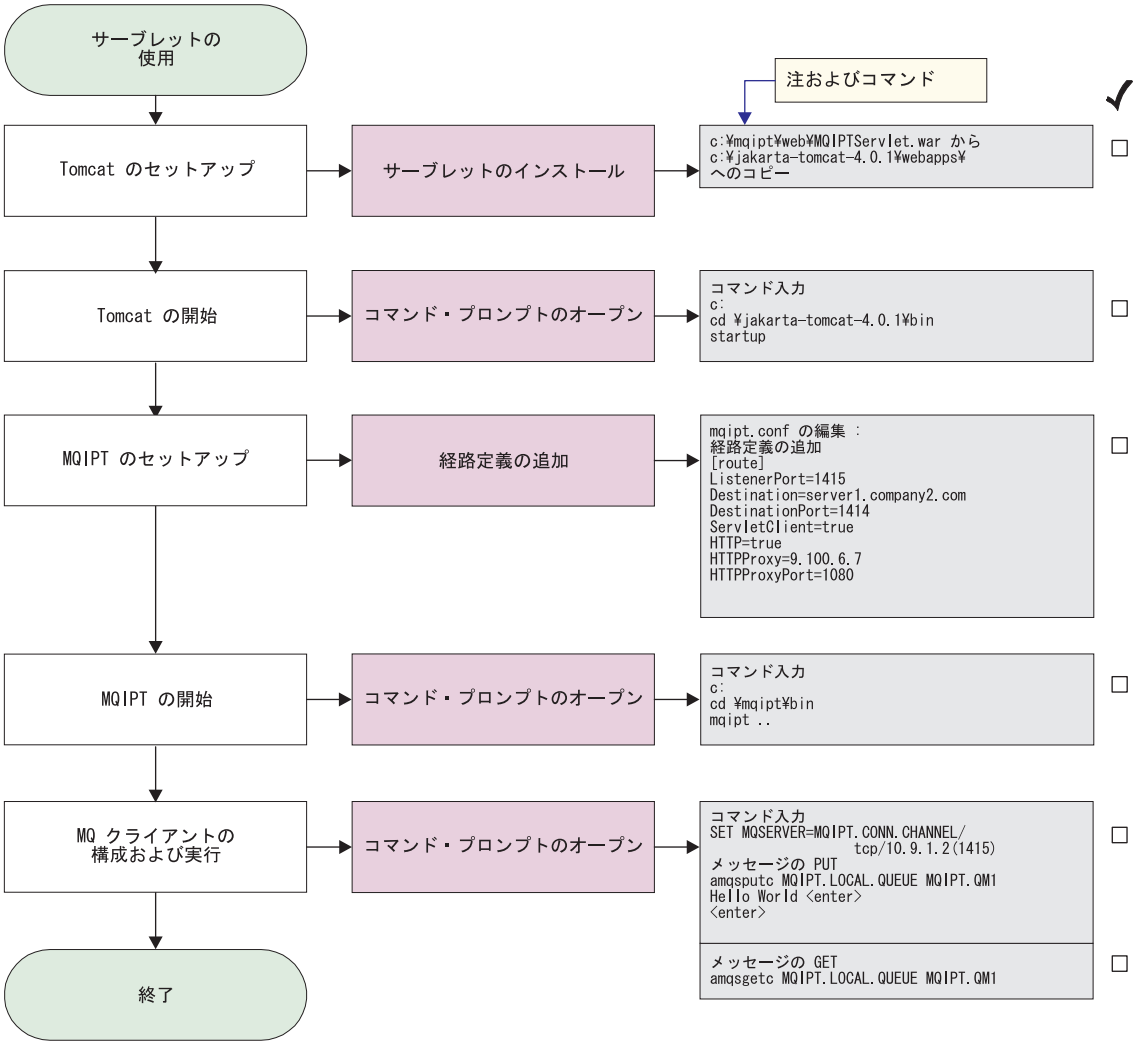

図 29. サーブレット構成

1. Tomcat をセットアップします

   次のコマンドを、

   ```
   c:¥mqipt¥web¥MQIPTServlet.war
   ```

   次のコマンドへコピーします。

   ```
   c:¥jakarta-tomcat-4.0.1¥webapps
   ```

2. Tomcat を開始します

   コマンド・プロンプトをオープンし、次のように入力します。

   ```
   c:
   cd ¥jakarta-tomcat-4.0.1¥bin
   startup
   ```

3. MQIPT1 をセットアップします

   mqipt.conf を編集し、経路定義を追加します。

   ```
   [route]
   ListenerPort=1415
   Destination=server1.company2.com
   DestinationPort=1414
   ```

```
ServletClient=true
HTTP=true
HTTPProxy=9.100.6.7
HTTPProxyPort=8080
```

4. MQIPT1 を開始します

   コマンド・プロンプトをオープンし、次のように入力します。

   ```
   c:
   cd ¥mqipt¥bin
   mqipt ..
   ```

   以下のメッセージが正常終了を示します。

   ```
   5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
   MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
   MQCPI004 Reading configuration information from C:¥mqipt¥mqipt.conf
   MQCPI011 The path C:¥mqipt¥logs will be used to store the log files
   MQCPI006 Route 1415 has started and will forward messages to :
   MQCPI034 ....server1.company2.com(1414)
   MQCPI035 ....using HTTP
   MQCPI024 ....and HTTP proxy at 9.100.6.7(8080)
   MQCPI059 ....servlet client enabled
   ```

5. WebSphere MQ クライアント・マシンのコマンド・プロンプトに対して、次のように入力します。

   ```
   SET MQSERVER=MQIPT.CONN.CHANNEL/tcp/10.9.1.2(1415)
   ```

6. 以下のコマンドを使用してメッセージを入力します。

   ```
   amqsputc MQIPT.LOCAL.QUEUE MQIPT1.QM1
   Hello world <enter>
    <enter>
   ```

7. 以下のコマンドを使用してメッセージを入手します。

   ```
   amqsgetc MQIPT.LOCAL.QUEUE MQIPT1.QM1
   ```

「Hello world (ようこそ)」が表示されます。

MQIPT クラスター化サポートの構成

この例では、 71 ページの『前提事項』に加え、以下の作業も完了している必要があります。

WebSphere MQ サーバー LONDON については、

- LONDON というキュー・マネージャーの定義
- MQIPT.CONN.CHANNEL というサーバー接続チャネルの定義
- ポート 1414 での LONDON に対する TCP/IP の開始
- キュー・マネージャーの SOCKS 化

WebSphere MQ サーバー NEWYORK については、

- NEWYORK というキュー・マネージャーの定義
- MQIPT.CONN.CHANNEL というサーバー接続チャネルの定義
- ポート 1414 での NEWYORK に対する TCP/IP リスナーの開始
- キュー・マネージャーの SOCKS 化

キュー・マネージャーを SOCKS 化するには、マシン全体を SOCKS 化するか、または WebSphere MQ サーバー・アプリケーションだけを SOCKS 化します。以下の操作を行うように、SOCKS クライアントを構成します。

- SOCKS プロキシーとしての MQIPT を指す
- SOCKS V5 サポートを使用可能にする
- ユーザー認証を使用不可にする
- MQIPT だけとのリモート接続を行う

同一マシン上の 1 つのポート・アドレスでは、1 つのアプリケーションしか listen できません。ポート 1414 が使用中であれば、空きポート・アドレスを選択し、例の中の 1414 と置き換えます。これを済ませておけば、メッセージを LONDON のローカル・キューに入れ、それを NEWYORK から取り出すことで、キュー・マネージャー間の経路をテストすることができます。

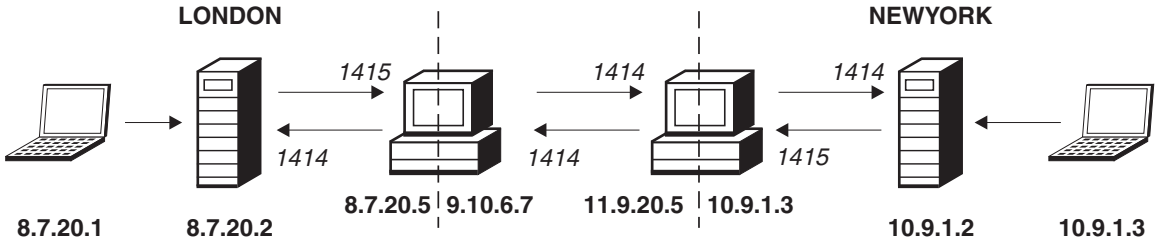

図 30. クラスター化ネットワーク・ダイアグラム

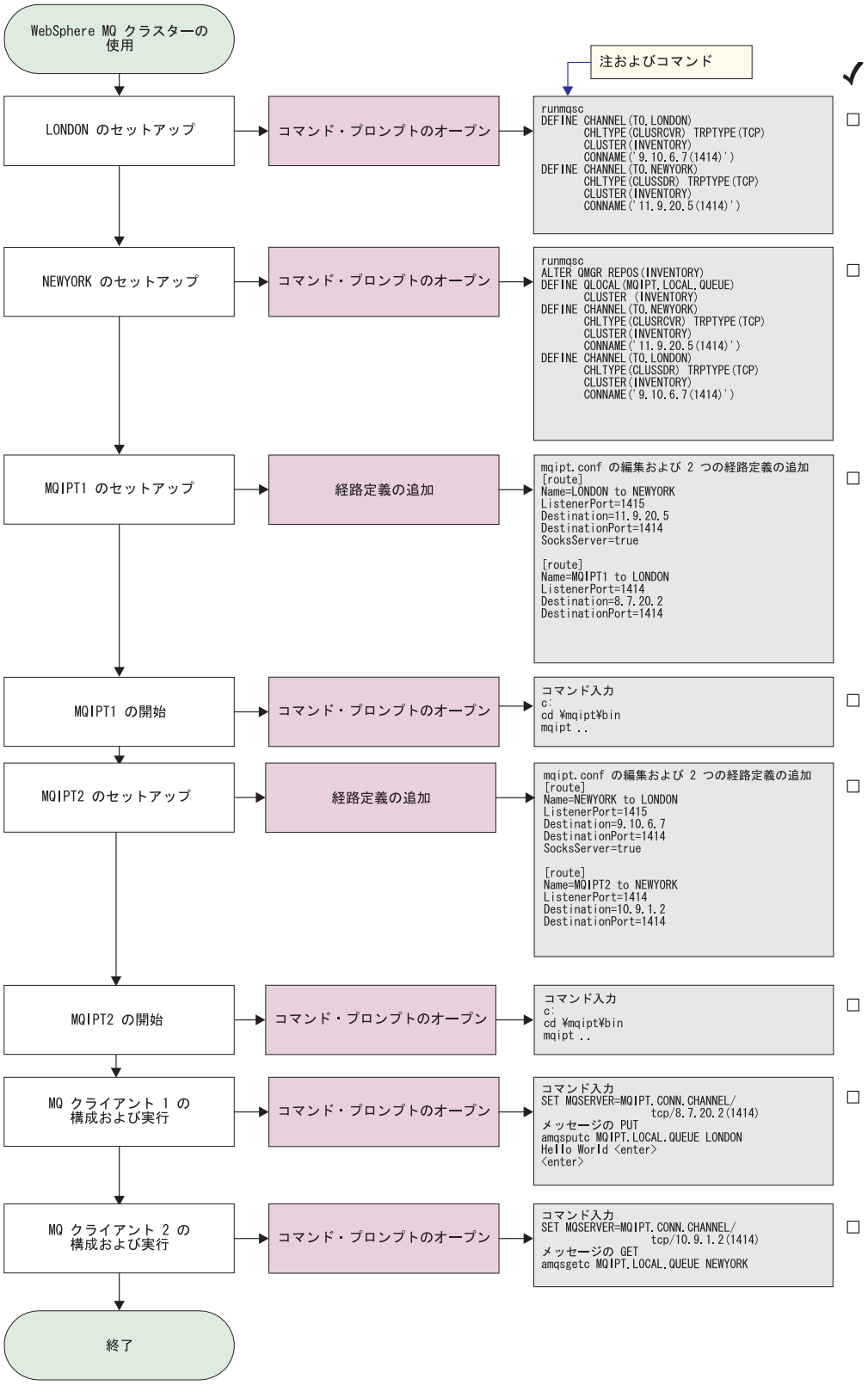

図 31. クラスター化構成

1. LONDON をセットアップします
   コマンド・プロンプトをオープンし、次のように入力します。

```
runmqsc
DEFINE CHANNEL(TO.LONDON) +
       CHLTYPE(CLUSRCVR) TRPTYPE(TCP) +
       CLUSTER(INVENTORY) +
       CONNAME('9.10.6.7(1414)')
DEFINE CHANNEL(TO.NEWYORK) +
       CHLTYPE(CLUSSDR) TRPTYPE(TCP) +
       CLUSTER(INVENTORY) +
       CONNAME('11.9.20.5(1414)')
```

2. NEWYORK をセットアップします

   コマンド・プロンプトをオープンし、次のように入力します。

```
runmqsc
ALTER QMGR REPOS(INVENTORY)
DEFINE QLOCAL(MQIPT.LOCAL.QUEUE) +
       CLUSTER(INVENTORY)
DEFINE CHANNEL(TO.NEWYORK) +
       CHLTYPE(CLUSRCVR) TRPTYPE(TCP) +
       CLUSTER(INVENTORY) +
       CONNAME('11.9.20.5(1414)')
DEFINE CHANNEL(TO.LONDON) +
       CHLTYPE(CLUSSDR) TRPTYPE(TCP) +
       CLUSTER(INVENTORY) +
       CONNAME('9.10.6.7(1414)')
```

3. MQIPT1 をセットアップします

   mqipt.conf を編集し、2 つの経路定義を追加します。

```
[route]
Name=LONDON to NEWYORK
ListenerPort=1415
Destination=11.9.20.5
DestinationPort=1414
SocksServer=true
```

```
[route]
Name=MQIPT1 to LONDON
ListenerPort=1414
Destination=8.7.20.2
DestinationPort=1414
```

4. MQIPT1 を開始します

   コマンド・プロンプトをオープンし、次のように入力します。

```
c:
cd ¥mqipt¥bin
mqipt ..
```

   以下のメッセージが正常終了を示します。

```
5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
MQCPI004 Reading configuration information from C:¥mqipt¥mqipt.conf
MQCPI011 The path C:¥mqipt¥logs will be used to store the log files
MQCPI006 Route 1415 has started and will forward messages to :
MQCPI034 ....11.9.20.5(1414)
MQCPI035 ....using MQ protocols
MQCPI052 ....Socks server side enabled
MQCPI006 Route 1414 has started and will forward messages to :
MQCPI034 ....8.7.20.2(1414)
MQCPI035 ....using MQ protocols
```

5. MQIPT2 をセットアップします

   mqipt.conf を編集し、2 つの経路定義を追加します。

```
[route]
Name=NEWYORK to LONDON
ListenerPort=1415
Destination=9.10.6.7
DestinationPort=1414
SocksServer=true
[route]
Name=MQIPT2 to NEWYORK
ListenerPort=1414
Destination=10.9.1.2
DestinationPort=1414
```

6. MQIPT2 を開始します

   コマンド・プロンプトをオープンし、次のように入力します。

   ```
   c:
   cd ¥mqipt¥bin
   mqipt ..
   ```

   以下のメッセージが正常終了を示します。

   ```
   5639-L92 (C) Copyright IBM Corp. 2000-2002 All Rights Reserved
   MQCPI001 WebSphere MQ internet pass-thru Version 1.2 starting
   MQCPI004 Reading configuration information from C:¥mqipt¥mqipt.conf
   MQCPI011 The path C:¥mqipt¥logs will be used to store the log files
   MQCPI006 Route 1415 has started and will forward messages to :
   MQCPI034 ....9.10.6.7(1414)
   MQCPI035 ....using MQ protocols
   MQCPI052 ....Socks server side enabled
   MQCPI006 Route 1414 has started and will forward messages to :
   MQCPI034 ....10.9.1.2(1414)
   MQCPI035 ....using MQ protocols
   ```

7. 最初の WebSphere MQ クライアント・マシン (8. 7. 20. 1) のコマンド・プロンプトに対して、次のように入力します。

   ```
   SET MQSERVER=MQIPT.CONN.CHANNEL/TCP/8.7.20.2(1414)
   ```

8. 以下のコマンドを使用してメッセージを入力します。

   ```
   amqsputc MQIPT.LOCAL.QUEUE LONDON
   Hello world <enter>
    <enter>
   ```

9. 2 番目の WebSphere MQ クライアント・マシン (10. 9. 1. 3) のコマンド・プロンプトに対して、次のように入力します。

   ```
   SET MQSERVER=MQIPT.CONN.CHANNEL/TCP/10.9.1.2(1414)
   ```

10. 2 番目の WebSphere MQ クライアント・マシンで、次のコマンドを使用してこのメッセージを入手します。

    ```
    amqsgetc MQIPT.LOCAL.QUEUE NEWYORK
    ```

「Hello world (ようこそ)」が表示されます。

鍵リング・ファイルの作成

このサンプルでは、ユーザーが Keyman を使用してトラステッド CA から新規の証明書を要求し、ユーザーの個人用証明書がファイル (たとえば、server.cer) でユーザーに戻されたことを前提にしています。サーバー認証を行うにはこれで十分です。クライアント認証が必要な場合は、2 番目の証明書 (たとえば、client.cer) を要求し、以下のステップを 2 回実行して 2 つの鍵リング・ファイルを作成する必要があります。

1. KeyMan を開始します

2. 「Create new... (新規作成...)」を選択します
3. 「PKCS#12 Token (PKCS#12 トークン)」を選択します
4. 「Action (アクション)」->「Generate Key (鍵を生成)」と選択します
   新規の鍵ペアが ″RSA / 1024-bit″ リストに表示されます
5. 新規の鍵ペアを選択します
6. 「Action (アクション)」->「Request Certificate (証明書を要求)」と選択します
   オンライン指示に従います
7. 「File (ファイル)」->「Save (保管)」と選択します
8. パスワードを入力します
9. 新規の鍵リング・ファイルのファイル名を入力します
   たとえば、c:¥mqipt¥ssl¥myServer.pfx
10. 「File format as PKCS#12 / PFX (PKCS#12 / PFX としてのファイル形式)」を保持し、「Wrap key ring into a Java class (鍵リングを Java クラスにラップする)」に**チェックマークを付けないでください**
11. 「File (ファイル)」->「Exit (終了)」と選択します
12. 上記操作で使用したパスワード (myPassWord) が入っているテキスト・ファイルを作成します。
    たとえば、c:¥mqipt¥ssl¥myServer.pwd

証明書を戻してもらう場合は、元の鍵リング・ファイル (myServer.pfx) をオープンします。次に、以下の操作を行います。

1. KeyMan を開始します
2. 「Open existing... (既存のファイルのオープン...)」を選択します
3. 「Local resource (ローカル・リソース)」を選択します
4. 「Open a file... (ファイルのオープン...)」を選択します
5. 個人用証明書ファイルの名前を入力します
   たとえば、c:¥mqipt¥ssl¥myServer.pfx
6. パスワードを入力します
7. 「File (ファイル)」->「Import (インポート)」と選択します
8. 「Local resource (ローカル・リソース)」を選択します
9. 「Open a file... (ファイルのオープン...)」を選択します
10. server.cer を入力します
    ダイアログが表示され、「私用証明書が秘密鍵と結合される」ことが示されます。
11. 「File (ファイル)」->「Save (保管)」と選択します
12. 「File (ファイル)」->「Exit (終了)」と選択します

上記ステップを繰り返し、client.cer ファイルから myClient.pfx を 作成します。 KeyMan を使用してサンプル CA 鍵リング・ファイル sslCAdefault.pfx の内容を調べ、自分の個人用証明書がリスト内のいずれかの CA によって署名されているかどうか確認します。署名されていれば、そのサンプル CA 鍵リング・ファイルを使用できます。そうでなければ、自分の個人用証明書を署名した CA 証明書が含まれている鍵リング・ファイルを作成する必要があります。このファイルは、個

人用証明書と一緒に戻されていることがあります。戻されていなければ、自分の個人用証明書を提供した CA に CA 証明書を要求し、それを sslCAdefault.pfx にインポートする必要があります。 CA 鍵リング・ファイルは、クライアント・サイドで使用することも、サーバー・サイドで使用することもできます。これらの新規鍵リング・ファイルをサーバー認証に使用する際は、 74 ページの『SSL サーバー認証』の例を参照して、以下の経路プロパティーを設定してください。

```
SSLClientCAKeyRing=c:¥¥mqipt¥¥ssl¥¥sslCAdefault.pfx
SSLClientCAKeyRingPW=c:¥¥mqipt¥¥ssl¥¥sslCAdefault.pwd
SSLServerKeyRing=c:¥¥mqipt¥¥ssl¥¥myServer.pfx
SSLServerKeyRingPW=c:¥¥mqipt¥¥ssl¥¥myServer.pwd
SSLServerCAKeyRing=c:¥¥mqipt¥¥ssl¥¥sslCAdefault.pfx
SSLServerCAKeyRingPW=c:¥¥mqipt¥¥ssl¥¥sslCAdefault.pwd
```

これらの新規鍵リング・ファイルをクライアントおよびサーバー認証に使用する際は、 77 ページの『SSL クライアント認証』の例を参照して、以下の経路プロパティーを設定してください。

```
SSLClientKeyRing=c:¥¥mqipt¥¥ssl¥¥myClient.pfx
SSLClientKeyRingPW=c:¥¥mqipt¥¥ssl¥¥myClient.pwd
SSLClientCAKeyRing=c:¥¥mqipt¥¥ssl¥¥sslCAdefault.pfx
SSLClientCAKeyRingPW=c:¥¥mqipt¥¥ssl¥¥sslCAdefault.pwd
SSLServerKeyRing=c:¥¥mqipt¥¥ssl¥¥myServer.pfx
SSLServerKeyRingPW=c:¥¥mqipt¥¥ssl¥¥myServer.pwd
SSLServerCAKeyRing=c:¥¥mqipt¥¥ssl¥¥sslCAdefault.pfx
SSLServerCAKeyRingPW=c:¥¥mqipt¥¥ssl¥¥sslCAdefault.pwd
```

第 11 章 internet pass-thru の維持

この章では、internet pass-thru の稼働を維持する方法について説明します。この章には、以下のセクションがあります。

- 『保守』
- 『問題判別』
- 108 ページの『パフォーマンス・チューニング』

保守

通常のバックアップ手順の一環として、以下のファイルを定期的にバックアップする必要があります。

- mqipt.conf 構成ファイル
- 以下のプロパティーで定義された mqipt.conf 内の SSL 鍵リング・ファイル。
  - SSLClientKeyRing
  - SSLClientCAKeyRing
  - SSLServerKeyRing
  - SSLServerCAKeyRing
- 以下のプロパティーで定義された mqipt.conf 内の SSL 鍵リング・パスワード・ファイル。
  - SSLClientKeyRingPW
  - SSLClientCAKeyRingPW
  - SSLServerKeyRingPW
  - SSLServerCAKeyRingPW
- Administration Client 構成ファイル (client.conf)。このファイルには、Administration Client に認識されているすべての MQIPT に関する接続情報が収められています。

問題判別

問題が発生したかどうかを最初に調べる場合、以下のようないくつかの共通な落とし穴があります。

- MQIPT システムがインストールされたばかりで、まだリブートされていない。
- キュー・マネージャーに直接接続された経路で HTTP が true に設定されている。
- キュー・マネージャーに直接接続された経路で SSLClient が true に設定されている。
- CLASSPATH が正しく設定されていない。
- PATH が正しく設定されていない。
- 鍵リング・ファイル用に保管されたパスワードに大文字小文字の区別がある。

次のステップでは、図 32に示されているフローチャートに従います。数字は、下に示されている注の番号を指しています。

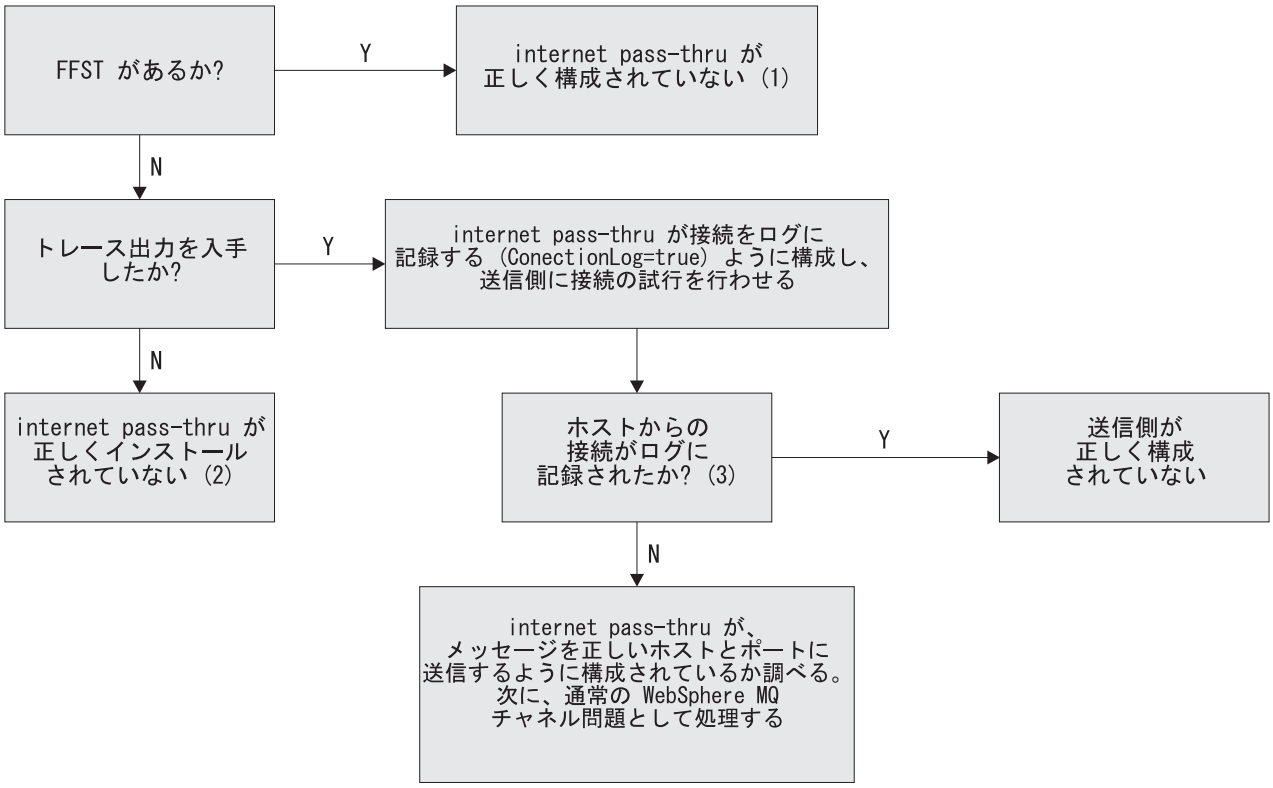

図 32. 問題判別フローチャート

注:

1. FFST レポートが (errors サブディレクトリーに) 見つかったならば、MQIPT が正しくインストールされていることが分かります。構成に問題があるかもしれません。

   各 FFST は、MQIPT、つまり経路の始動プロセスを終了させる問題を報告します。各 FFST の原因になった問題を修正してください。次に、古い FFST を削除するか、または MQIPT をリフレッシュしてください。
2. MQIPT が正しくインストールされていない場合は、すべてのファイルが正しい位置に配置され、CLASSPATH が更新されていることを確認します。これが正しいかどうかを調べるには、MQIPT を手動で開始してみてください。
3. 手動で MQIPT を開始します。

   コマンド・プロンプトをオープンします。 bin サブディレクトリーへ進み、次のように入力します。

   ```
   mqipt xxx
   ```

   ここで、*xxx* は MQIPT ホーム・ディレクトリーです。この場合は、それは "**..**" です。

   これにより、MQIPT が開始し、構成を見つけるためにホーム・ディレクトリーを探します。エラー・メッセージや FFST がないか、errors サブディレクトリーを探します。

エラー・メッセージがないか、MQIPT のテキスト出力を調べ、エラーを訂正します。 FFST を調べ、エラーがあればそれを訂正します。構成ファイルのグローバル・セクションに問題があれば、MQIPT は開始しません。構成ファイルの経路セクションに問題があれば、経路は開始しません。

internet pass-thru の自動的開始

MQIPT を Windows NT Service としてインストールする場合、その開始が自動的に行われるように変更すると、MQIPT はシステムの始動時に自動的に開始されます。インストールが正しく行われたことを確認するには、MQIPT を Windows NT Service としてインストールする前に必ず MQIPT を 1 回手動で開始してください。詳細については、34 ページの『Windows サービス制御プログラムの使用』を参照してください。

エラー・メッセージ “Unable to locate DLL...” が出た場合は、間違った `mqiptService` プログラムを使用しているか、またはシステムの PATH 環境変数が正しく構成されていません。 PATH には、JNI ランタイム・ライブラリーのロケーションが入っていなければなりません。このファイル (`jvm.dll`) は、JDK のクライアント・サブディレクトリーに入っています。

エンドツーエンド接続の検査

MQIPT が正しくインストールされたならば、次にとるステップは、経路が正しくセットアップされているかどうかの検査です。

`mqipt.conf` 構成ファイルでは、`ConnectionLog` プロパティーを true に設定します。 MQIPT を開始またはリフレッシュして接続を試みます。ホーム・ディレクトリーの下のログ・ディレクトリーに接続ログが作成されます。接続ログが作成されない場合は、MQIPT が正しくインストールされていないことがわかります。接続の試行が記録されない場合は、送信側が正しくセットアップされていません。接続の試行が記録されていれば、MQIPT がメッセージを正しいアドレスに転送しているかどうか調べてください。

エラーのトレース

MQIPT は、詳細な実行トレース機能を提供します。この機能は、トレース属性によって制御されます。経路はそれぞれ独立にトレースできます。トレース・ファイルは *xxx*¥errors ディレクトリーに書き込まれます (ここで、*xxx* は `mqipt.conf` が入っているディレクトリーです)。作成された各トレース・ファイルには、次のような形式の名前が付けられています。

`iptroute`*`nnnnn`*`.trc`

ここで、*nnnnn* は、経路が listen するポートの番号です。特定の経路に直接関連していないスレッド (たとえば、コマンド入力を処理するスレッド) からのトレース出力は、`iptmain.trc` という別個のファイルに書き込まれます。

予期しない致命的エラーは、FFST レコードとしてエラー・ログ・ファイルに書き込まれ、*xxx*¥errors ディレクトリーに保持されます (ここで、*xxx* は、`mqipt.conf` が入っているディレクトリーです)。 FFST ファイルの形式は次のようになっています。

`ipt`*`xxx`*`.FFST`

ここで、*xxx* は、FFST が生成された順序です (1 が最も古いものです)。長時間実行システムでは、システムで生成可能な最大数に達することがあります。この場合は、生成されたすべての FFST が mqipt0.FFST ファイルに書き込まれます。mqipt0.FFST ファイルが作成された場合は、都合のつき次第、MQIPT を停止して再始動し、古いファイルを削除する必要があります。

問題の報告

問題を IBM サービス・センターに報告する必要がある場合は、以下の情報を提供していただくと、問題の解決が速まることがあります。

- 使用している簡単なネットワーク・ダイアグラム (IP アドレスを含む) を提供する。
- 複数の MQIPT を使用している場合は、各 MQIPT マシンのシステム・クロックを同期化する。こうしておけば、各 MQIPT のトレース・エントリーを突き合わせる際に役立ちます。
- 古いトレース・ファイルを削除する。
- クライアントを実行して問題を作成する。こうすれば、トレース・ファイルには、問題のインスタンスが 1 つしか入りません。
- すべての MQIPT .trc および .log ファイルのコピーを送信する。

パフォーマンス・チューニング

ここでは、システムをチューニングする場合のいくつかのヒントを示します。

スレッド・プール管理

各経路の相対パフォーマンスは、スレッド・プールとアイドル・タイムアウト仕様を組み合わせて使用してチューニングすることができます。

接続スレッド

各 MQIPT 経路には、着信通信要求を処理している、並行して実行しているスレッドの作業プールが割り当てられています。初期化時に、スレッドのプールが作成され (そのサイズは、経路の MinConnectionThreads 属性に指定されている)、1 つのスレッドが、最初の着信要求を処理するように指名されます。この要求が到着すると、そのスレッドはこの要求の処理を即時に開始し、その次のスレッドが、次の着信要求を処理するように割り当てられます。すべてのスレッドが作業を割り当てられていると、新規のスレッドが作成されて作業プールに追加され、作業が割り当てられます。このようにして、プールは MaxConnectionThreads に達するまで増大します。作業スレッドの数が MaxConnectionThreads に達すると、次の着信要求は、1 つのスレッドが解放されて作業プールに戻されるまで待ちます。これが経路の最大作業容量であり、この限度を超えると、追加の要求は受け入れられません。会話が終了するか、または指定されたタイムアウト期間を過ぎると、スレッドはプールに戻されます。

アイドル・タイムアウト

デフォルトでは、非アクティブ状態になっていることが理由で作業スレッドが終了させられることはありません。あるスレッドをある会話に割り当てると、そのスレッドは、その会話が正常終了するか、経路が非活動になるか、または MQIPT がシ

ャットダウンするまでその会話に割り当てられたままになっています。オプションで、アイドル・タイムアウト間隔を指定できるため、指定された期間 (分単位) 非アクティブ状態になっているすべてのスレッドが終了します。モニター・スレッドは、スレッド・アイドル時間について定期的な検査を行い、しきい値を超えたスレッドを終了させます。スレッドは、作業プールに戻されてリサイクルされます。

第 12 章 メッセージ

MQIPT をコマンド行から実行すると、MQIPT は、少数の通知メッセージとエラー・メッセージをコンソール上に表示します (米国英語でのみ)。

以下の点に注意してください。

- MQCAxxxx メッセージは Administration Client メッセージです。
- MQCPxxxx メッセージは MQIPT メッセージです。
- MQCxIxxx メッセージは通知メッセージです。
- MQCxExxx メッセージはエラー・メッセージです。

MQCAE001 Unknown host: {0}

説明: MQIPT ホストが見つかりません。

ユーザーの処置: MQIPT の所在を示すホスト名が正しく指定されているか調べてください。

MQCAE002 The following error was reported by the system: {0}

説明: エラーが起こりました。システム・コマンドの実行中に、エラーが報告されました。

MQCAE005 No valid destination address has been defined

説明: 経路の追加操作で、宛先フィールドがブランクのまま残されました。

ユーザーの処置: 有効な宛先アドレスを入力してください。

MQCAE006 No valid destination port has been defined

説明: 経路の追加操作で、宛先ポート・アドレス・フィールドがブランクのまま残されました。

ユーザーの処置: 有効な宛先ポート・アドレスを入力してください。

MQCAE007 No valid listener port has been defined

説明: 経路の追加操作で、リスナー・ポート・アドレス・フィールドがブランクのまま残されました。

ユーザーの処置: 有効なリスナー・ポート・アドレス (1 ～ 65535) を入力してください。

MQCAE008 No valid network address has been defined

説明: MQIPT の追加操作で、ネットワーク・アドレス・フィールドがブランクのまま残されました。

ユーザーの処置: 有効なネットワーク・アドレスを入力してください。

MQCAE009 No valid command port has been defined

説明: MQIPT の追加操作で、無効なコマンド・ポート・アドレスが使用されました。

ユーザーの処置: 有効なコマンド・ポート・アドレス (1 ～ 65535) を入力してください。

MQCAE010 Could not show online help

説明: オンライン・ヘルプのファイルはありますが、表示できません。

ユーザーの処置: Acrobat Reader がシステム PATH に入っているか確認してください。

MQCAE011 Could not parse parameter

説明: 内部エラーが発生して、テーブルに入っていないパラメーターを更新しようとしました。

ユーザーの処置: この状態が継続する場合は、IBM 技術支援に連絡してください。

MQCAE012 Could not find file for online help

説明: ″guiadmin.pdf″ ファイルが見つかりません。

ユーザーの処置: このファイルが doc サブディレクトリーでアクセス可能であることを確認してください。

MQCAE013 Interrupted while trying to show online help

説明: オンライン・ヘルプを表示しているときにシステム・エラーが起こりました。

ユーザーの処置: もう 1 度操作を行ってください。この状態が継続する場合は、IBM 技術支援に連絡してください。

MQCAE015 The password you have just entered has not been recognized

説明: MQIPT は有効なパスワードを期待しています。最後に使用したパスワードが間違っています。パスワードは、構成ファイルに定義したものと一致していなければなりません。

ユーザーの処置: 「**MQIPT**」->「**Connection (接続)**」パネルを使用してそのパスワードを変更し、もう 1 度最後のコマンドを実行してみてください。

MQCAE016 Node mismatch

説明: ツリーで選択したノードとメモリー内のデータ間に内部矛盾があります。

ユーザーの処置: Administration Client をクローズして、もう 1 度コマンドを実行してみてください。この状態が継続する場合は、IBM 技術支援に連絡してください。

MQCAE017 Could not create NLS text for message {0}

説明: 定義されたメッセージ番号に該当する NLS テキストが見つかりません。

ユーザーの処置: ″guiadmin.properties″ ファイルが破壊されたため、指定されたメッセージ番号が見つからないのかもしれません。以下の検査を行ってください。

- 該当する新規メッセージが README ファイルに入っているか
- ″guideadmin.jar″ ファイルがシステム CLASSPATH に入っているか
- ″guideadmin.properties″ ファイルが ″guideadmin.jar″ ファイルに入っているか
- メッセージ番号が ″guideadmin.properties″ ファイルに入っているか

MQCAE018 Could not create NLS text for message MQCAE017

説明: メッセージ番号 {0} がシステム・プロパティー・リストに入っていません。

ユーザーの処置: ″guideadmin.properties″ ファイルが破壊されている可能性があります。以下の検査を行ってください。

- ″guideadmin.jar″ ファイルがシステム CLASSPATH に入っているか
- ″guideadmin.properties″ ファイルが ″guideadmin.jar″ ファイルに入っているか
- メッセージ番号が ″guideadmin.properties″ ファイルに入っているか

MQCAE019 You have failed to repeat your proposed new password

説明: パスワードの変更時に、検証用の 2 回の入力が行われませんでした。

ユーザーの処置: 新規パスワードを該当フィールドにもう 1 度入力してください。

MQCAE020 Failed to change MQIPT access parameters

説明: MQIPT アクセス・パラメーターの変更時に、内部エラーが検出されました。

ユーザーの処置: Administration Client をクローズして、もう 1 度コマンドを実行してみてください。この状態が継続する場合は、IBM 技術支援に連絡してください。

MQCAE021 Internal failure to identify MQIPT

説明: 構成ファイルを MQIPT に保管中に、内部エラーが検出されました。

ユーザーの処置: Administration Client をクローズして、もう 1 度コマンドを実行してみてください。この状態が継続する場合は、IBM 技術支援に連絡してください。

MQCAE022 Internal failure to save MQIPT configuration

説明: 構成ファイルを MQIPT に保管中に、内部エラーが検出されました。

ユーザーの処置: Administration Client をクローズして、もう 1 度コマンドを実行してみてください。この

状態が継続する場合は、IBM 技術支援に連絡してください。

MQCAE023 MQIPT {0} did not recognize your password.

説明: MQIPT は有効なパスワードを期待しています。最後に使用したパスワードが間違っています。パスワードは、構成ファイルに定義したものと一致していなければなりません。

ユーザーの処置: 「**MQIPT**」->「**Connection (接続)**」メニューを使用してそのパスワードを変更し、もう 1 度コマンドを実行してみてください。

MQCAE024 MQIPT {0} has not recognized the command.

説明: Administration Client が MQIPT に送信したコマンドが認識されません。

ユーザーの処置: Administration Client が使用したコードのバージョンが MQIPT と同じであるか調べてください。

MQCAE025 MQIPT {0} has failed to send configuration file.

説明: MQIPT が構成ファイルを送信しようとして失敗しました。

ユーザーの処置: Administration Client をクローズして、もう 1 度コマンドを実行してみてください。それでもうまくいかない場合は、MQIPT をいったん停止した後、再始動してください。

MQCAE026 Remote shutdown is disabled on MQIPT {0}.

説明: リモート・シャットダウンが構成ファイルで使用可能になっていないため、MQIPT をリモート側でシャットダウンしようとして失敗しました。

ユーザーの処置: MQIPT のリモート・シャットダウンを使用可能にするには、構成ファイルを編集し、RemoteShutDown プロパティーを true に設定します。

MQCAE027 Look and feel {0} is not supported.

説明: 使用しているプラットフォーム用の推奨ルック・アンド・フィールは使用できません。

ユーザーの処置: システム・デフォルトのルック・アンド・フィールで処理が続行されます。

MQCAE028 Look and feel class {0} cannot be found.

説明: 使用しているプラットフォーム用の推奨ルック・アンド・フィールは使用できません。

ユーザーの処置: システム・デフォルトのルック・アンド・フィールで処理が続行されます。

MQCAE029 Minimum Connection Threads must be non-negative and no bigger than Maximum Connection Threads

説明: 最小接続スレッド値は、最大接続スレッド値以下でなければなりません。

ユーザーの処置: 値を適宜変更してください。

MQCAE030 Maximum Connection Threads must be greater than zero and at least as big as Minimum Connection Threads

説明: 最大接続スレッド値は、最小接続スレッド値より大きくなければなりません。

ユーザーの処置: 値を適宜変更してください。

MQCAE031 Port numbers must be in the range 0 to 65535

説明: 仕様に合致しない値を設定しようとしています。

ユーザーの処置: 値を適宜変更してください。

MQCAE032 Trace must be in the range 0 to 5

説明: 仕様に合致しない値を設定しようとしています。

ユーザーの処置: 値を適宜変更してください。

MQCAE033 Max Log file size must be in the range 5 to 50

説明: 仕様に合致しない値を設定しようとしています。

ユーザーの処置: 値を適宜変更してください。

MQCAE049 No route has been selected on any MQIPT

説明: 削除する経路をまず選択しないで、その経路を削除しようとしました。

ユーザーの処置: 経路を選択してから、もう 1 度コマンドを実行してみてください。

MQCAE050 Could not connect to MQIPT {0}

説明: Administration Client が、指定された MQIPT に接続できません。

ユーザーの処置: この原因としては、以下のことが考えられます。

- MQIPT が稼働していない。
- MQIPT が自分のコマンド・ポートで listen していない。
- 1 つの Administration Client しか MQIPT CommandPort を使用していない。
- 要求がタイムアウトになった。

MQCAE051 Could not read reply from MQIPT {0}

説明: MQIPT から応答が送られてきましたが、それが所定のプロトコルに準拠していません。

ユーザーの処置: Administration Client が使用したコードのバージョンが MQIPT と同じであるか調べてください。

MQCAE052 Configuration has not been saved

説明: MQIPT から有効な応答が送られてきましたが、後続の構成ファイルへの保管に失敗しました。

ユーザーの処置: MQIPT が構成ファイルへの書き込みアクセス権限を持っているか調べてください。

MQCAE053 MQIPT has not confirmed saving of configuration

説明: 構成ファイルが MQIPT へ送信されましたが、MQIPT はその確認に失敗しました。

ユーザーの処置: この原因としては、以下のことが考えられます。

- MQIPT が稼働していない。
- MQIPT が自分のコマンド・ポートで listen していない。
- 1 つの Administration Client しか MQIPT CommandPort を使用していない。
- 要求がタイムアウトになった。

MQCAE054 MQIPT data has not been refreshed

説明: MQIPT に連絡しましたが、Administration Client は構成ファイルを読み取ることができませんでした。

ユーザーの処置: この原因としては、以下のことが考えられます。

1. MQIPT が失敗した。
2. 要求がタイムアウトになった。

MQCAE055 No MQIPT or route on an MQIPT has been selected

説明: MQIPT または経路が選択されていないため、ユーザーが選択したメニュー・オプションを実行できません。

ユーザーの処置: 適切な MQIPT または経路を選択して、もう 1 度実行してみてください。

MQCAE056 Duplicate listener port has been rejected

説明: 指定されたリスナー・ポートが別の経路で使用されているため、そのポートが拒否されました。

ユーザーの処置: 別のリスナー・ポートを選択して、もう 1 度実行してみてください。

MQCAI002 The MQIPT has been removed from display

説明: ツリーから選択したノードの MQIPT が、クライアントのメモリーから除去されました。

MQCAI003 New route added to the display

説明: 今指定した新規経路が現行の MQIPT に追加されました。

MQCAI004 Route has been removed from the display

説明: ツリーから選択した経路がクライアントのメモリーから除去されました。

MQCAI005 Selected MQIPT is being displayed

説明: ツリーから選択した MQIPT のグローバル・パラメーターがテーブルに示されています。

MQCAI006 Selected route is being displayed

説明: ツリーから選択した経路のパラメーターがテーブルに示されています。

MQCAI007 Client configuration has been saved

説明: ツリー上のすべての MQIPT に関するアクセス・パラメーターが保管されました。

MQCAI008 Display of online help succeeded

説明: オンライン・ヘルプが要求どおりに表示されました。

MQCAI009 Table has been updated

説明: テーブルに入力された値を使用して、メモリー内のモデルが更新されました。

MQCAI010 No MQIPT or route has been selected.

説明: アクションをとるための情報が不十分なため、アクションがとられませんでした。

MQCAI011 User Action has been cancelled

説明: 開始済みのポップアップ・ウィンドウ関連のアクションがキャンセルされました。

MQCAI014 Configuration has been saved on MQIPT

説明: 現在ツリー上で選択されている MQIPT に新規の構成ファイルが保管され、それを使用して MQIPT が再始動されました。

MQCAI015 Online help has terminated

説明: オンライン・ヘルプが要求どおりに表示され、その後で終了しました。

MQCAI017 Select File/Add MQIPT to add an MQIPT to the tree

説明: このメッセージは、ツリー上に MQIPT がないときに表示され、その追加方法を知らせます。

MQCAI018 New MQIPT added to display

説明: 指示どおり、新規の MQIPT がツリーに追加されました。

MQCAI019 MQIPT access parameters have been changed

説明: 現在ツリー上で選択されている MQIPT のアクセス・パラメーターが変更されました。

MQCAI021 Select an MQIPT or route on the tree to display its contents

説明: このメッセージは、情報がテーブルに表示されていないときに表示され、その表示方法を知らせます。

MQCAI022 The command port has changed

説明: 変更を指示された MQIPT のコマンド・ポートが今変更されました。

MQCAI023 The password has changed

説明: 今後、変更された MQIPT と通信する場合は、この新規パスワードが使用されます。

MQCAI025 MQIPT {0} has been refreshed.

説明: MQIPT に関して保持されている情報が、その構成ファイルの読み取りで更新されました。

MQCAI026 MQIPT {0} has received shutdown request.

説明: MQIPT がシャットダウン要求の受信を確認して、今シャットダウンするところです。

MQCAI027 Client configuration has been refreshed

説明: Administration Client に表示されている情報が、ローカル "client.conf" ファイルからリフレッシュされました。

MQCAI028 MQIPT {0} is active

説明: MQIPT が PING 要求に正常に応答しました。

MQCAI029 MQIPT {0} is not active

説明: MQIPT が、指定時間内に PING 要求に応答しませんでした。

ユーザーの処置: この原因としては、以下のことが考えられます。

- MQIPT が稼働していない。
- MQIPT が自分のコマンド・ポートで listen していない。
- 要求がタイムアウトになった。このタイムアウト時間は、MQIPT に関する接続情報のタイムアウト・プロパティーを変更することによって増やすことができます。

MQCAI030 Route {0} is active

説明: MQIPT が PING 要求に正常に応答しました。

MQCAI031 Route {0} is not active

説明: MQIPT 経路が、指定時間内に PING 要求に応答しませんでした。

ユーザーの処置: この原因としては、以下のことが考えられます。

- MQIPT が稼働していない。
- MQIPT が自分のコマンド・ポートで listen していない。
- 要求がタイムアウトになった。このタイムアウト時間は、MQIPT に関する接続情報のタイムアウト・プロパティーを変更することによって増やすことができます。

MQCAI100 This script is used to start the Administration Client for {0}. Specifying a SOCKS proxy will allow the Administrator Client to talk to an MQIPT through a firewall.

説明: mqiptGui スクリプトに関するオンライン・ヘルプ情報。

MQCAI101 Format of command is:

説明: mqiptGui スクリプトに関するオンライン・ヘルプ情報。

MQCAI102 mqiptGui {socks_host{socks_port}}

説明: mqiptGui スクリプトに関するオンライン・ヘルプ情報。

MQCAI103 socks_host-host name of SOCKS proxy (optional)

説明: mqiptGui スクリプトに関するオンライン・ヘルプ情報。

MQCAI104 socks_port-SOCKS proxy port address (optional-default 1080)

説明: mqiptGui スクリプトに関するオンライン・ヘルプ情報。

MQCPE000 Could not locate message data when handling message {0}

説明: メッセージ番号 {0} がシステム・プロパティー・リストに入っていません。

ユーザーの処置: ″mqipt.properties″ ファイルが破壊されたため、指定されたメッセージ番号が見つかりません。以下の検査を行ってください。

- ″MQipt.jar″ ファイルがシステム CLASSPATH に入っているか
- ″mqipt.properties″ ファイルが ″MQipt.jar″ ファイルに入っているか
- メッセージ番号が ″mqipt.properties″ ファイルに入っているか

MQCPE001 Directory does not exist or is not a directory

説明: 初期化時に、必要なディレクトリーが見つかりませんでした。このメッセージは、MQIPT 構成ファイル mqipt.conf、または デフォルト・ディレクトリーの MQIPT コマンド行始動オプションのいずれかに指定されたディレクトリーを指しています。

ユーザーの処置: 正しいディレクトリーを指定して、もう 1 度コマンドを実行してみてください。

MQCPE004 Route startup failed on port {0}

説明: 指定された ListenerPort 番号の経路を開始できません。

ユーザーの処置: 経路始動時に入出力エラーが起こりました。この問題の詳細については、他の隣接エラー・メッセージやログ・レコードを調べてください。

MQCPE005 The configuration file {0} could not be found

説明: 指定されたディレクトリーに MQIPT 構成ファイル ″mqipt.conf″ が入っていません。

ユーザーの処置: 正しいディレクトリーを指定して、もう 1 度コマンドを実行してみてください。

MQCPE006 The number of routes has exceeded {0}. MQIPT will start but this configuration is unsupported.

説明: ユーザーの構成が、MQIPT の 1 つのインスタンスに関してサポートされる経路の最大数を超えました。操作は停止されませんが、結果としてシステムが不安定になったり、過負荷になったりすることがありま

す。示された経路の最大数を超える構成はサポートされません。

ユーザーの処置: インスタンス当たりの経路数が少ない MQIPT の別のインスタンスを開始することを考えてください。

MQCPE007 Route not restarted on listener port {0}

説明: REFRESH 操作で、指定された ListenerPort で作動する経路が新規構成で再始動されませんでした。

ユーザーの処置: この問題の詳細については、他の隣接エラー・メッセージを調べてください。

MQCPE008 Duplicate route defined for listener port {0}

説明: 同じ ListenerPort 値を持つ複数の経路が定義されています。

ユーザーの処置: 重複した経路を構成ファイルから除去し、もう 1 度コマンドを実行してみてください。

MQCPE009 LogPath parameter {0} is not valid.

説明: テキストに示されているログ・パスが存在しないか、または所定の時点にアクセス可能でありません。

ユーザーの処置: ディレクトリーが存在し、それが MQIPT からアクセス可能であるか調べてください。

MQCPE010 Listener or command port number {0} is not valid

説明: コマンド・ポートまたはリスナー・ポート・パラメーターついて提供されたポート番号が無効です。

ユーザーの処置: 使用可能な有効なポート番号を指定してください。ネットワークでのポート番号の使用の指針については、ネットワーク管理者にお尋ねください。

MQCPE011 The trace level {0} is outside the valid range 0 - 5

説明: 指定されたトレース・オプションが要求されましたが、それが 0 ～ 5 の有効範囲に入っていません。

ユーザーの処置: 0 ～ 5 のトレース値を指定してください。

MQCPE012 The value {0} is not valid for the attribute {1}

説明: 無効なプロパティー値が指定されています。

ユーザーの処置: 各制御パラメーターに関する有効値の詳細については、本書の該当個所を参照してください。

MQCPE013 ListenerPort property was not found in route {0}

説明: MQIPT が、ListenerPort プロパティーを含んでいない経路を構成ファイルに検出しました。
ListenerPort プロパティーは、各経路に関する基本的な固有 ID であるため、必須です。

ユーザーの処置: 所定の各経路に対して有効な ListenerPort を指定してください。

MQCPE014 ListenerPort property value {0} is not valid

説明: 経路の ListenerPort プロパティーに対して無効なポート・アドレスが指定されています。

ユーザーの処置: ポート・アドレスは 1024 ～ 65535 の範囲でなければなりません。構成ファイル内の各 ListenerPort を調べてください。

MQCPE015 No text was found for message number {0}

説明: 内部エラーが検出されましたが、そのエラーについての説明は用意されていません。

ユーザーの処置: ″mqipt.properties″ ファイルが破壊されたため、指定されたメッセージ番号が見つかりません。以下の検査を行ってください。

- 該当する新規メッセージが README ファイルに入っているか
- ″MQipt.jar″ ファイルがシステム CLASSPATH に入っているか
- ″mqipt.properties″ ファイルが ″MQipt.jar″ ファイルに入っているか
- メッセージ番号が ″mqipt.properties″ ファイルに入っているか

MQCPE016 The maximum number of connection threads is {0} but this is less than the minimum number of connection threads, which is {1}

説明: ユーザーの構成で接続スレッドの最小数が指定されていますが、それが接続スレッドの最大数を超えた値になっています。

ユーザーの処置: 考えられる原因は、単一経路でのエラー、プロパティー・プロパティーと経路プロパティーの間の矛盾、または経路プロパティーによるシステム・デフォルト値のオーバーライドなどです。有効な値と適用

可能なデフォルト値の詳細については、本書の該当する章を参照してください。

MQCPE017 The exception {0} was thrown, causing MQIPT to shut down

説明: MQIPT が異常終了してシャットダウンしました。この状態の発生原因としては、システムの環境条件または制約 (たとえば、メモリー・オーバーフロー) が考えられます。

ユーザーの処置: この状態が継続する場合は、IBM 技術支援に連絡してください。

MQCPE018 The ListenerPort property is blank - the route will not start

説明: 経路で ListenerPort 番号が欠落しています。

ユーザーの処置: 構成ファイルを編集し、有効な ListenerPort を追加してください。

MQCPE019 The stanza {0} was not found before the following: {1}

説明: 構成ファイルでシーケンス・エラーが起こりました。

ユーザーの処置: 構成ファイルを編集し、すべての [route] エントリーが [global] エントリーの後に来ていることを確認してください。

MQCPE020 The new value for MaxConnectionThreads is {0}. This must be greater than the current value {1}

説明: 経路を開始した後は、MaxConnectionThread プロパティーを増やすことだけができます。

ユーザーの処置: 構成ファイルを編集し、MaxConnectionThread プロパティーを変更してください。

MQCPE021 The property Destination was not supplied for route {0}

説明: Destination プロパティーは経路内に必須ですが、指定された経路で欠落しています。

ユーザーの処置: 構成ファイルを編集し、所定の経路について Destination プロパティーを追加してください。

MQCPE022 The CommandPort value {0} is outside the valid range 1 - 65535.

説明: CommandPort プロパティーが 1 ～ 65535 の範囲外です。

ユーザーの処置: 構成ファイルを編集し、CommandPort プロパティーを有効なポート・アドレスに変更してください。

MQCPE023 Request for shutdown from Administration Client {0} is ignored because it is disabled.

説明: リモート・シャットダウンが構成ファイルで使用可能になっていないため、MQIPT をリモート側でシャットダウンしようとして失敗しました。

ユーザーの処置: MQIPT のリモート・シャットダウンを使用可能にするには、構成ファイルを編集し、RemoteShutDown プロパティーを true に設定します。

MQCPE024 The command received by the MQIPT controller has not been recognized.

説明: MQIPT が、認識できないコマンドをコマンド・ポートから受け取りました。

ユーザーの処置: ″mqipt.log″ ファイルにそのコマンドのアイデンティティーが含まれているか調べてください。

MQCPE025 Failed to connect to server on host {0}, port {1}.

説明: 行モード (非 GUI) Administration Client が MQIPT との通信に失敗しました。

ユーザーの処置: CommandPort プロパティーが構成ファイルに {1} として指定されており、MQIPT が {0} で稼働していることを確認してください。

MQCPE026 No reply received from server on host {0}, port {1}.

説明: 行モード (非 GUI) Administration Client が MQIPT との通信に失敗しましたが、まだ応答を受け取っていません。

ユーザーの処置: これは、要求がタイムアウトになったか、または MQIPT に問題があることを示しています。

MQCPE027 Reply from MQIPT not recognized.

説明: 行モード (非 GUI) Administration Client が、認識できない応答を MQIPT から受け取りました。

ユーザーの処置: mqiptAdmin スクリプトが MQIPT と同じバージョンの ″MQipt.jar″ ファイルを使用しているか調べてください。

MQCPE028 Invalid stanza detected: {0}

説明: 示されている未認識のスタンザが構成ファイルで見つかりました。

ユーザーの処置: 構成ファイルでは、[global] スタンザと [route] スタンザのみが有効です。

MQCPE029 Was not able to flush log output.

説明: 通信バッファーがフラッシュされたため、一部のメッセージがログに書き込まれなかった可能性があります。

ユーザーの処置: MQIPT ホーム・ディレクトリーのディスクがいっぱいになっていないか、MQIPT がまだログ・サブディレクトリーへのアクセス権を持っているか調べてください。

MQCPE030 {0} not found in CLASSPATH.

説明: 指定された JAR ファイルがシステム環境 CLASSPATH 変数に入っていません。

ユーザーの処置: 指定されたファイルをシステム CLASSPATH に追加してください。

MQCPE031 {0} class not found.

説明: このメッセージは、MQIPT のバージョン番号を表示するときに生成されます。指定されたクラスが MQIPT JAR ファイルに入っていないか、またはシステム環境 CLASSPATH 変数が破壊されています。

ユーザーの処置: 指定されたクラス・ファイルが ″MQipt.jar″ ファイルに入っているか、また ″MQipt.jar″ ファイルがシステム CLASSPATH に入っているか調べてください。

MQCPE033 Failed to send configuration file to Administration Client at {0}

説明: 構成ファイルを Administration Client に送信しているときにエラーが起こりました。

ユーザーの処置: 構成ファイルが MQIPT ホーム・ディレクトリーに入っているか、また別のプロセスで共用されていないか調べてください。

MQCPE034 Administration Client at {0} did not supply the correct password.

説明: 構成ファイルの AccessPW プロパティーが、Administration Client によって提供されたものと一致しません。

ユーザーの処置: 構成ファイルの AccessPW プロパティーを変更するか、または Administration Client に保管されているパスワードを変更してください。

MQCPE035 Failed to start command listener on port {0}

説明: 指定されたポート・アドレスのコマンド・リスナーを開始するときに入出力エラーが起こりました。

ユーザーの処置: 構成ファイルの CommandPort プロパティーで使用されたポート・アドレスを調べてください。

MQCPE038 MQIPT has not started as expected

説明: このメッセージは、MQIPT をシステム・サービスとして開始する mqipt fork プロセスによって生成されます。

ユーザーの処置: 詳細については、エラー・ログを調べてください。 MQIPT が稼働しているかどうかを調べる前に、IPTFork で使用するスリープ時間を増やしてみることができます。 mqiptFork スクリプトを編集し、IPTFork に渡したパラメーター値を大きくしてください。

MQCPE039 I/O error occurred running mqipt script

説明: fork プロセスから MQIPT を立ち上げるときにエラーが起こりました。

ユーザーの処置: システム PATH 環境変数に JDK のロケーションが入っている、また mqipt スクリプトが実行権限を持っているか調べてください。

MQCPE040 Interruption occurred running mqipt script

説明: fork プロセスから MQIPT を立ち上げた後にエラーが起こりました。

ユーザーの処置: 詳細については、エラー・ログを調べてください。この状態が継続する場合は、IBM 技術支援に連絡してください。

MQCPE041 Unsupported level of Java - {0}

説明: MQIPT が、指定されたレベルの Java を使用して開始されました。

ユーザーの処置: 詳細については、本書の該当個所に示されている前提条件を調べてください。

MQCPE042 There is a conflict with the following properties on route {0}:

説明: 一部のプロパティーは、他のプロパティーと一緒に使用できません。このメッセージは、対立するプロパティーのリストの前に表示されます。

ユーザーの処置: 以下のエラー・メッセージを調べて、適切なアクションをとってください。

MQCPE043 ....{0} and {1}

説明: これらのプロパティーは、同じ経路上で同時に設定することはできません。

ユーザーの処置: 構成ファイルを編集し、所定の経路上の指定されたプロパティーの 1 つを使用不可にしてください。

MQCPE044 {0} is only valid on the {1} operating system

説明: MQIPT の一部のフィーチャーは特定のプラットフォームでのみ有効です。

ユーザーの処置: 構成ファイルを編集し、指定されたプロパティーを使用不可にしてください。

MQCPE045 ....HTTP proxy name is missing

説明: HTTP プロパティーが true に設定されている場合は、HTTPProxy プロパティーを設定する必要があります。

ユーザーの処置: 構成ファイルを編集し、所定の経路について HTTPProxy を定義してください。

MQCPE046 {0} is not allowed as Pagent has failed to initialize

説明: Pagent は、MQIPT の Quality of Service を提供するアプリケーションです。 MQIPT が始動時にこのアプリケーションの初期化に失敗し、所定の経路について QoS プロパティーが true に設定されました。

ユーザーの処置: 構成ファイルを編集し、所定の経路について QoS を使用不可にしてください。

MQCPE047 Pagent has failed to initialize

説明: Pagent は、MQIPT の Quality of Service を提供するアプリケーションです。 MQIPT は始動時にこのアプリケーションの初期化に失敗しました。

ユーザーの処置: Pagent を使用していなければ、このエラー・メッセージを無視することができますが、QoS プロパティーを false に設定する必要があります。

MQCPE048 Route startup failed on port {0}, exception was : {1}

説明: 指定された ListenerPort 番号の経路を開始できません。

ユーザーの処置: この問題の詳細については、他の隣接エラー・メッセージやログ・レコードを調べてください。

MQCPE049 Error starting or stopping the Java Security Manager {0}

説明: Java Security Manager を開始または停止しようとしているときに、例外が throw されました。

ユーザーの処置: Java Security Manager はすでに使用可能になっていますが、ランタイム許可がまだ使用可能になっていません。 setSecurityManager の RuntimePermission をローカル・ポリシー・ファイルに追加してください。変更結果を有効にするには、MQIPT を再始動する必要があります。

MQCPE050 Security exception on port {0} from the Administration Client

説明: Administration Client からの接続を受け入れているときに、セキュリティー例外が throw されました。

ユーザーの処置: Java Security Manager はすでに使用可能になっていますが、エラー・メッセージに示されているホストについては許可が付与されていません。このホストを MQIPT に接続できるようにするには、CommandPort のポート・アドレスでの接続を受け入れ / 解決するための SocketPermission を追加してください。変更結果を有効にするには、Java Security Manager を再始動する必要があります。

MQCPE051 Security exception accepting a connection on route {0}

説明: 指定された経路への接続を受け入れているときに、セキュリティー例外が throw されました。

ユーザーの処置: Java Security Manager はすでに使用可能になっていますが、エラー・メッセージに示されて

いるホストについては許可が付与されていません。ホストをこの経路に接続できるようにするには、ListenerPort への接続を受け入れ / 解決するための SocketPermission を追加してください。変更結果を有効にするには、Java Security Manager を再始動する必要があります。

MQCPE052 Connection request on route {0} failed : {1}

説明: このメッセージは、接続要求のセキュリティー例外を記録する接続ログに出されます。

ユーザーの処置: Java Security Manager はすでに使用可能になっていますが、エラー・メッセージに示されているホストについては許可が付与されていません。ホストをこの経路に接続できるようにするには、ListenerPort への接続を受け入れ / 解決するための SocketPermission を追加してください。変更結果を有効にするには、Java Security Manager を再始動する必要があります。

MQCPE053 Security exception making a connection to {0}({1})

説明: 指定された経路への接続を作成しているときに、セキュリティー例外が throw されました。

ユーザーの処置: Java Security Manager はすでに使用可能になっていますが、エラー・メッセージに示されているホストについては許可が付与されていません。ホストをこの経路に接続できるようにするには、ListenerPort への接続を受け入れ / 解決するための SocketPermission を追加してください。変更結果を有効にするには、Java Security Manager を再始動する必要があります。

MQCPE054 Connection request to {0}({1}) failed : {2}

説明: このメッセージは、ターゲット・ホストに対する接続要求のセキュリティー例外を記録する接続ログに出されます。

ユーザーの処置: Java Security Manager はすでに使用可能になっていますが、エラー・メッセージに示されているホストについては許可が付与されていません。ホストをこの経路に接続できるようにするには、ListenerPort への接続を受け入れ / 解決するための SocketPermission を追加してください。変更結果を有効にするには、Java Security Manager を再始動する必要があります。

MQCPE055 ....Socks proxy name is missing

説明: SocksClient プロパティーが true に設定されている場合は、SocksProxy プロパティーを設定する必要があります。

ユーザーの処置: 構成ファイルを編集し、所定の経路について SocksProxy を定義してください。

MQCPE056 Conflict with route properties

説明: 一部のプロパティーは、他のプロパティーと一緒に使用できません。

ユーザーの処置: このエラーの詳細についてコンソール・メッセージを調べ、適切なアクションをとってください。

MQCPE057 Connection from {0} to host {1} closed - the SSL protocol ({2})was not recognized

説明: この経路が SSL プロキシー・モードになり、初期データ・フローが認識されません。

ユーザーの処置: この経路に対して SSL 接続のみが行われていることを確認してください。

MQCPI001 {0} starting

説明: この MQIPT インスタンスが実行を開始しています。この後も、引き続き初期化メッセージが出されます。

MQCPI002 {0} shutting down

説明: MQIPT がシャットダウンしようとしています。このシャットダウンは、STOP コマンドが出された結果起こることもあれば、構成エラーのために正常な始動や REFRESH アクションが行われない場合に自動的に起こることもあります。

MQCPI003 {0} shutdown complete

説明: シャットダウン・プロセスが完了しました。これで、すべての MQIPT プロセスが終了しました。

MQCPI004 Reading configuration information from {0}

説明: MQIPT 構成ファイル mqipt.conf が、このメッセージに示されているディレクトリーから読み込まれています。

MQCPI005 Listener port specified as not active - {0} -> {1}({2})

説明: このメッセージで参照されている経路が非アクティブとしてマークされています。この経路では、どの通信要求も受け入れられません。

MQCPI006 Route {0} has started and will forward messages to:

説明: このメッセージに示されているリスナー・ポートで経路が開始されました。このメッセージの後には、この経路に関連するすべてのプロパティーをリストした他のメッセージが続きます。

MQCPI007 Route stopped on port {0}

説明: 指定された ListenerPort で作動する経路がシャットダウンしようとしています。このアクションは、通常、REFRESH コマンドを MQIPT に出し、経路構成が変更されたときにとられます。

MQCPI008 Listening for control commands on port {0}

説明: この MQIPT インスタンスは、指定されたポートで制御コマンドを listen しています。

MQCPI009 Control command received: {0}

説明: このメッセージは、制御コマンドがコマンド・ポートで受け取られたことを示しています。該当する場合は、詳細情報がこのメッセージに組み込まれます。

MQCPI010 Stopping command port on {0}

説明: REFRESH 操作の場合、コマンド・ポートは新規構成では使用されなくなりました。指定されたポートでは、コマンドは受け取られなくなりました。

MQCPI011 The path {0} will be used to store the log files

説明: 現行構成では、ロギング出力はこのメッセージに示されているロケーションに送られます。

ユーザーの処置: 構成に修正を加えた場合や REFRESH 操作を要求した場合は、これが変わることがあります。

MQCPI012 Changing the value of MinConnectionThreads has no effect after the route is started

説明: 経路の始動時に接続スレッドの最少値が割り当てられますが、この値は MQIPT を再始動するまで変更できません。

MQCPI013 Connection from {0} to host {1} closed

説明: このメッセージは、接続アクティビティーを記録する接続ログに出されます。

MQCPI014 Connection from {0} to host {1} closed - the protocol was not recognized

説明: このメッセージは、接続アクティビティーを記録する接続ログに出されます。

MQCPI015 Connection from a client on {0} to host {1} was rejected because client access has been disabled on this route

説明: このメッセージは、接続アクティビティーを記録する接続ログに出されます。

MQCPI016 Connection from a queue manager on {0} to host {1} was rejected because queue manager access has been disabled on this route

説明: このメッセージは、接続アクティビティーを記録する接続ログに出されます。

MQCPI017 A queue manager on {0} was connected to host {1}

説明: このメッセージは、接続アクティビティーを記録する接続ログに出されます。

MQCPI018 A client on {0} was connected to host {1}

説明: このメッセージは、接続アクティビティーを記録する接続ログに出されます。

MQCPI019 {0} routes have been created - this exceeds the maximum number of supported routes, which is {1}

説明: サポートされている経路の最大数を超えました。

ユーザーの処置: MQIPT は引き続き作動しますが、2 番目の MQIPT インスタンスを作成し、両者間で経路を分割することをお勧めします。

MQCPI020 The configuration file has been sent to the Administration Client.

説明: Administration Client からの要求の結果、構成ファイルが送信されました。

MQCPI021 Password checking has been enabled on the command port.

説明: このメッセージは、コマンド・ポートにアクセスするにはパスワードが必要であることを示しています。

MQCPI022 Password checking has been disabled on the command port.

説明: このメッセージは、コマンド・ポートにアクセスするのにパスワードが必要でないことを示しています。

MQCPI024 ....using HTTP proxy {0}({1})

説明: このメッセージは、この経路の発信接続がこの HTTP プロキシーを使用して行われることを示しています。

MQCPI025 The refresh requested by Administration Client {0} has finished.

説明: REFRESH コマンドを受け取った結果、MQIPT はその構成ファイルを再読み取りし、再始動しました。

MQCPI026 Administration Client {0} has requested shutdown.

説明: STOP コマンドを受け取った結果、MQIPT はシャットダウンします。

MQCPI027 {0} sent to {1} on port {2}

説明: このメッセージは、行モード (非 GUI) Administration Client から指定 MQIPT へ送信されたコマンドをシステム・コンソールに表示します。

MQCPI031 ......cipher suites {0}

説明: このメッセージは、この経路に使用されている暗号スイートをリストします。

MQCPI032 ......key ring file {0}

説明: このメッセージは、この経路の鍵リングのファイル名を示しています。

MQCPI033 ......client authentication set to {0}

説明: このメッセージは、SSL サーバーがこの経路のクライアント認証を要求しているかどうかを定義します。

MQCPI034 ....{0}({1})

説明: このメッセージは、この経路の宛先と宛先ポート・アドレスを示しています。

MQCPI035 ....using {0}

説明: このメッセージは、使用されているプロトコルを宛先に示します。それは MQSeries プロトコル、HTTP トンネル操作、または HTTP チャンク操作のいずれかです。

MQCPI036 ....SSL Client side enabled with properties :

説明: このメッセージは、この経路が SSL を使用して宛先ホストにデータを送信することを示します。

MQCPI037 ....SSL Server side enabled with properties :

説明: このメッセージは、この経路が SSL を使用して送信元のホストからデータを受け取ることを示します。

MQCPI038 ......distinguished name(s) {0}

説明: このメッセージは、証明書の認証を制御するために使用する Distinguish Name (公開鍵持ち主情報) をリストします。

MQCPI039 ....via Socks proxy {0}({1})

説明: このメッセージは、この経路の発信接続がこの Socks プロキシー (MQIPT をコマンド行から開始するときに定義される) を使用して行われることを示しています。

MQCPI040 Command port has been accessed by Administration Client {0}

説明: このメッセージは、システム・コンソールと MQIPT ログ・ファイル (ロギングが使用可能になっている場合) に書き込まれます。 MQIPT が Administration Client からの接続を受け取りました。

MQCPI041 ....will reply to Network Dispatcher advisor requests in {0} mode

説明: このメッセージは、経路の開始時にシステム・コンソールに書き込まれます。 MQIPT が Network Dispatcher アドバイザーに応答するために使用するモードを示すために使用されます。有効なオプションは、「通常」と「置換」です。

MQCPI042 Maximum connections reached on route {0} - further requests will be blocked

説明: このメッセージは、所定の経路に関する接続の最大数に達したときにシステム・コンソールに書き出されます。それ以降の要求は、接続が解放されるか、または MaxConnectionThreads 値を増やすまでブロックされます。

MQCPI043 Connections on route {0} now unblocked

説明: このメッセージは、所定の経路が接続要求についてブロックを解かれたときにシステム・コンソールに書き出されます。

MQCPI044 MQIPT has been launched from system startup

説明: MQIPT がシステム・サービスとして開始されました。

MQCPI045 Launching MQIPT from system startup

説明: MQIPT がシステム・サービスとして開始されるところです。

MQCPI046 Sleeping for {0} seconds while MQIPT is launched from system startup

説明: fork プロセスは、MQIPT がシステム・サービスとして正常に開始されたかどうか確認する前に、この時間だけスリープします。

MQCPI047 .....CA keyring file {0}

説明: このメッセージは、この経路の CA 鍵リングのファイル名を示しています。

MQCPI048 The ping by Administration Client {0} has finished

説明: IPTController から Administration Client への応答メッセージ。

MQCPI049 ....QoS priority to dest = {0}, to caller = {1}

説明: このメッセージは、この経路における両方向のトラフィックの優先順位を示しています。

MQCPI050 Adding entry to inittab to automatically start MQIPT at system startup

説明: ユーザーが mqiptService スクリプトを実行して MQIPT をシステム・サービスとして開始しました。

MQCPI051 Removing entry from inittab that automatically starts MQIPT at system startup

説明: ユーザーが mqiptService スクリプトを実行して、システム・サービスとしての MQIPT の開始を中止しました。

MQCPI052 ....Socks server side enabled

説明: この経路は SOCKS サーバー (プロキシー) として機能し、SOCKS 化されたアプリケーションからの接続を受け入れます。

MQCPI053 Starting the Java Security Manager

説明: SecurityManager プロパティーが true に設定されているため、デフォルトの Java Security Manager が開始されます。

MQCPI054 Stopping the Java Security Manager

説明: SecurityManager プロパティーが false に設定されているため、デフォルトの Java Security Manager が停止されます。

MQCPI055 Setting the java.security.policy to {0}

説明: デフォルトの Java Security Manager が開始されるところです。提供されたポリシー・ファイルを使用します。

MQCPI056 The Java Security Manager must be restarted to use a new policy file

説明: SecurityManagerPolicy プロパティーが変更されましたが、Java Security Manager を再始動するまで有効になりません。

ユーザーの処置: SecurityManager プロパティーを false に変更し、REFRESH コマンドを出して、Java Security Manager を停止してください。次に、SecurityManager を true に戻し、再度 REFRESH コマンドを出して、Java Security Manager を新規ポリシー・ファイルで開始してください。

MQCPI057 ....trace level {0} enabled

説明: このメッセージは、経路の開始時にシステム・コンソールに書き出されます。この経路で使用可能なトレースのレベルを表示するために使用されます。

MQCPI058 ....and a URI name of {0}

説明: このメッセージは、経路の開始時にシステム・コンソールに書き出されます。この経路の Uniform Resource Identifier 名を表示するために使用されます。

MQCPI059 ....servlet client enabled

説明: このメッセージは、経路の開始時にシステム・コンソールに書き出されます。この経路は MQIPT サーブレットに接続します。

MQCPI060 Installing files to automatically start MQIPT at system startup

説明: ユーザーが mqiptService スクリプトを実行して MQIPT をシステム・サービスとして開始しました。

MQCPI061 Removing files that automatically starts MQIPT at system startup

説明: ユーザーが mqiptService スクリプトを実行して、システム・サービスとしての MQIPT の開始を中止しました。

MQCPI064 ....no SSL authentication on this route

説明: このメッセージは、経路を開始したときにシステム・コンソールに書き出され、また、匿名暗号スイートが指定されているため、この経路に対して SSL 認証が使用されていないことを示します。

MQCPI065 ....in SSL proxy mode

説明: このメッセージは、経路を開始したときにシステム・コンソールに書き出され、また、この経路が SSL プロキシー・モードで作動していることを示します。

MQCPI100 This script is used to start {0}

説明: mqipt スクリプトからのオンライン・ヘルプ・メッセージ。

MQCPI101 Format of command is :

説明: mqipt スクリプトからのオンライン・ヘルプ・メッセージ。

MQCPI102 mqipt {dir_name}

説明: mqipt スクリプトからのオンライン・ヘルプ・メッセージ。

MQCPI103 dir_name - directory containing mqipt.conf

説明: mqipt スクリプトからのオンライン・ヘルプ・メッセージ。

MQCPI106 This script is used to display the current version number of {0}

説明: mqiptVersion スクリプトからのオンライン・ヘルプ・メッセージ。

MQCPI107 mqiptVersion {-v}

説明: mqiptVersion スクリプトからのオンライン・ヘルプ・メッセージ。

MQCPI108 where -v will also display the build timestamp

説明: mqiptVersion スクリプトからのオンライン・ヘルプ・メッセージ。

MQCPI109 This script is used to start {0}, from system startup, in another JVM and is only used in mqipt.ske. Use the mqipt script to start MQIPT from the command line.

説明: mqiptFork スクリプトからのオンライン・ヘルプ・メッセージ。

MQCPI110 This class is used to display a simple NLS message on the console

説明: IPTMessages クラスからのオンライン・ヘルプ・メッセージ。

MQCPI111 java com.ibm.mq.ipt.IPTMessages (message_id1) {message_id2} {message_id...}

説明: IPTMessages クラスからのオンライン・ヘルプ・メッセージ。

MQCPI112 where message_id matches a key in the file mqipt.properties

説明: IPTMessages クラスからのオンライン・ヘルプ・メッセージ。

MQCPI113 This script is used to manage MQIPT as a system service

説明: mqiptService スクリプトからのオンライン・ヘルプ・メッセージ。

MQCPI114 mqiptService (-install | -remove)

説明: mqiptService スクリプトからのオンライン・ヘルプ・メッセージ。

MQCPI115 -install will install files to start MQIPT automatically at system startup

説明: mqiptService スクリプトからのオンライン・ヘルプ・メッセージ。

MQCPI116 -remove will remove files that start MQIPT automatically at system startup

説明: mqiptService スクリプトからのオンライン・ヘルプ・メッセージ。

索引

日本語, 数字, 英字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

[ア行]

アイドル・タイムアウト
  パフォーマンス・チューニング 108
アクセシビリティー情報 x
宛先キュー・マネージャー、アクセス 7
暗号アルゴリズム 10
暗号化 3
暗号スイート 10
エラーのトレース 107
エンドツーエンド接続
  問題 107

[カ行]

鍵ファイルのバックアップ 105
共通問題 105
行モード・コマンド 56
行モード・コマンドによる MQIPT の管理 56
クライアント / サーバー・チャネル 23
クラスター送信側 / 受信側チャネル 24
構成
  行モード・コマンドの使用 56
  参照情報 57
  デフォルト構成ファイル 57
  ファイル保護 28
  プロパティー参照情報 60
  プロパティーの要約 58
  Administration Client の使用 51
構成の例 1, 72
  インストール検証テスト 72
  鍵リング・ファイルの作成 102
  構成アクセス制御 82
  HTTP プロキシー構成 79
  MQIPT クラスター化サポートの構成 98
  MQIPT サーブレットの構成 96
  Quality of Service (QoS) の構成 85
  SOCKS クライアントの構成 90
  SOCKS プロキシーの構成 88
  SSL クライアント認証 77
  SSL サーバー認証 74
  SSL テスト証明書の作成 95
  SSL プロキシーの構成 91
コマンド行からの MQIPT の開始
  AIX で 40
  HP-UX での 44
  Linux での 48
  Sun Solaris での 36
  Windows での 32

[サ行]

サービス制御プログラム、Windows 34
サービス妨害アタック 27
サーブレット 15
参考文献 xiii
実行トレース機能 107
失敗条件 26
終了 26
紹介 1
障害検出 105
スレッド・プール管理 108
正常終了 26
接続スレッド
  パフォーマンス・チューニング 108
接続ログ 26
先行 MQIPT からのアップグレード 29
前提事項 71
前提条件 x
送信側 / 受信側チャネル 24
送信側 / 要求発行者チャネル 24

[タ行]

チャネル構成 23
チャネル・コンセントレーターとしての MQIPT 1
チャンク操作、HTTP 8
テクノロジー関連の証明書 13
トラストの設定 12
トンネル操作、HTTP 8

[ハ行]

ハートビート・メカニズム 9
パフォーマンス・チューニング 108
ハンドシェーク 10
非武装地帯、MQIPT 2
プロトコル転送プログラム、MQIPT 7
プロパティー
  新規 29
  要約 58
プロパティーの継承 53
変更の要約 xv
保守 105

[マ行]

メッセージ 111
問題の報告 108
問題判別 105

[ヤ行]

要求発行者 / 送信側チャネル 24

A

AccessPW プロパティー 60
Active 構成プロパティー 61
Administration Client 51
  開始 51
  接続情報 51
  ファイル・メニュー・オプション 53
  プロパティーの継承 53
  ヘルプ情報 55
  AIX での開始 41
  HP-UX での開始 45
  Linux での開始 49
  MQIPT の管理 52
  MQIPT メニュー・オプション 54
  Sun Solaris での開始 37
  Windows での開始 33
AIX
  コマンド行からの Administration Client の開始 41
  コマンド行からの MQIPT の開始 40
  MQIPT のアンインストール 42
  MQIPT のインストール 39
  MQIPT の自動開始 41
  MQIPT のセットアップ 40
  MQIPT ファイルのインストール 39
  MQIPT ファイルのダウンロード 39

C

ClientAccess 構成プロパティー 61
CommandPort 構成プロパティー 60
ConnectionLog 構成プロパティー 60

D

Destination 構成プロパティー 61
DestinationPort 構成プロパティー 61

F

FFST レポート 106

H

HP-UX
  コマンド行からの Administration Client の開始 45
  コマンド行からの MQIPT の開始 44
  MQIPT のアンインストール 46
  MQIPT のインストール 43
  MQIPT の自動開始 45
  MQIPT のセットアップ 44
  MQIPT ファイルのインストール 43
  MQIPT ファイルのダウンロード 43
HTTP 構成プロパティー 61
HTTP サポート 8
HTTP トンネル操作、HTTP 2
HTTPChunking 構成プロパティー 62
HTTPProxy 構成プロパティー 62
HTTPProxyPort 構成プロパティー 62

I

IdleTimeout 構成プロパティー 62

J

Java Security Manager 24

K

KeyMan 16
  サポートされている標準データ形式 17
  サポートされるトークンのタイプ 16
  FAQ 18

L

Linux
  コマンド行からの Administration Client の開始 49
  コマンド行からの MQIPT の開始 48
  MQIPT のアンインストール 50
  MQIPT のインストール 47
  MQIPT の自動開始 49
  MQIPT のセットアップ 48
Linux *(続き)*
  MQIPT ファイルのダウンロード 47
linux
  MQIPT ファイルのインストール 47
ListenerPort 構成プロパティー 62
LogDir 構成プロパティー 62

M

MaxConnectionThreads 構成プロパティー 62
MaxLogFileSize 構成プロパティー 60
MinConnectionThreads 構成プロパティー 63
MQIPT および SSL 12
MQIPT のアンインストール
  AIX で 42
  HP-UX での 46
  Linux での 50
  Sun Solaris での 38
  Windows での 34
MQIPT の概要 7
MQIPT の管理 51
MQIPT の自動開始
  AIX で 41
  HP-UX での 45
  Linux での 49
  Sun Solaris での 37
MQIPT の自動的開始
  問題 107
MQIPT の使用開始 71
MQIPT の使用法 1
MQIPT のセットアップ
  AIX で 40
  HP-UX での 44
  Linux での 48
  Sun Solaris での 36
  Windows での 32
MQIPT のトポロジー 3
MQIPT ファイルのインストール
  AIX での 39
  HP-UX での 43
  Linux での 47
  Sun Solaris での 35
  Windows での 31
MQIPT ファイルのダウンロード
  AIX での 39
  HP-UX での 43
  Linux での 47
  Sun Solaris での 35
  Windows での 31

N

Name 構成プロパティー 63
NDAdvisor プロパティー 63
NDAdvisorReplaceMode プロパティー 63
Network Dispatcher 20

P

PKCS#10 17
PKCS#11 (CryptoKi) リポジトリー 17
PKCS#12 17
PKCS#12 トークン 16
PKCS#7 17
PKCS#7 トークン 16

Q

QMgrAccess 構成プロパティー 63
QoS 14
QoS 構成プロパティー 63
QoToCaller 構成プロパティー 64
QoToDest 構成プロパティー 64

R

REFRESH 行モード・コマンド 56
RemoteShutDown 構成プロパティー 60

S

SecurityManager 構成プロパティー 61
SecurityManagerPolicy 構成プロパティー 61
ServletClient 構成プロパティー 64
SOCKS サポート 9
SocksClient 構成プロパティー 64
SocksProxyHost 構成プロパティー 64
SocksProxyPort 構成プロパティー 64
SocksServer 構成プロパティー 64
SPKAC 18
SSL サポート 9
  エラー・メッセージ 13
  テスト 13
  トラストの設定 12
  ハンドシェーク 10
  例 3
  MQIPT および SSL 12
SSLClient 構成プロパティー 65
SSLClientCipherSuites 構成プロパティー 65
SSLClientConnectTimeout プロパティー 65
SSLClientDN_C 構成プロパティー 65
SSLClientDN_CN 構成プロパティー 65

SSLClientDN_L 構成プロパティー 65
SSLClientDN_O 構成プロパティー 66
SSLClientDN_OU 構成プロパティー 66
SSLClientDN_ST 構成プロパティー 66
SSLClientKeyRing 構成プロパティー 66
SSLClientKeyRingPW 構成プロパティー 66
SSLProxyMode 構成プロパティー 66
SSLServer 構成プロパティー 67
SSLServerAskClientAuth 構成プロパティー 67
SSLServerCipherSuites 構成プロパティー 67
SSLServerDN_C 構成プロパティー 67
SSLServerDN_CN 構成プロパティー 67
SSLServerDN_L 構成プロパティー 67
SSLServerDN_O 構成プロパティー 68
SSLServerDN_OU 構成プロパティー 68
SSLServerDN_ST 構成プロパティー 68
SSLServerKeyRing 構成プロパティー 68
SSLServerKeyRingPW 構成プロパティー 68
STOP 行モード・コマンド 56
Sun Solaris
  コマンド行からの Administration Client の開始 37
  コマンド行からの MQIPT の開始 36
  MQIPT のアンインストール 38
  MQIPT のインストール 35
  MQIPT の自動開始 37
  MQIPT のセットアップ 36
  MQIPT ファイルのインストール 35
  MQIPT ファイルのダウンロード 35
SupportPac Web ページ・アドレス 31

T

TCP/IP および MQIPT 7
Trace 構成プロパティー 68

U

UriName 構成プロパティー 69

W

Windows
  コマンド行からの Administration Client の開始 33
  コマンド行からの MQIPT の開始 32
  サービス制御プログラム 34
  サービスとしての MQIPT のアンインストール 34
  MQIPT のアンインストール 34
  MQIPT のインストール 31
  MQIPT のセットアップ 32
  MQIPT ファイルのインストール 31
  MQIPT ファイルのダウンロード 31

X

X.509 V2 証明書取り消しリスト (CRL) 18
X.509 V3 証明書 18