iSeries

ファイアウォール環境に対するマネージメント・セントラル接続の構成

iSeries

ファイアウォール環境に対するマネージメント・セントラル接続の構成

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

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

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

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

(URL は、変更になる場合があります)

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

原　典： iSeries
Configuring Management Central Connections for Firewall Environments
Experience Report

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 2005.8

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

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

© Copyright International Business Machines Corporation 2005. All rights reserved.

© Copyright IBM Japan 2005

目次

© Copyright IBM Corp. 2005

ファイアウォール環境に対するマネージメント・セントラル接続の構成

この報告書では、マネージメント・セントラル接続と、マネージメント・セントラルを V5R3 のさまざまなファイアウォール環境内で使用可能にするうえで必要な構成について、詳しく説明します。分散管理アプリケーションであるマネージメント・セントラルは、多数の着信および発信 TCP/IP ソケット接続を必要とします。これに対して、ファイアウォールでは、着信および発信接続を制限/変更することを前提としています。ファイアウォール環境でのマネージメント・セントラルの構成を支援するために、この報告書では、マネージメント・セントラル接続の性質と方向、および、マネージメント・セントラル接続の一部を制限または使用不可とする、特定のタイプのファイアウォールにおける制約について説明します。静的ネットワーク・アドレス変換 (NAT) と動的 NAT の両方について記載します。 3 つの基本的なファイアウォール環境について、マネージメント・セントラルをそれぞれの環境で正しく動作させるために必要な構成と共に説明します。これらの基本的な環境および関連する構成は、より複雑なファイアウォール環境でマネージメント・セントラルを使用可能にするためのガイドとして使用されることを意図しています。

用語
この報告書で使用される重要な用語を定義します。

マネージメント・セントラル接続
グラフィカル・クライアントとマネージメント・セントラル・サーバーとの間で確立されるさまざまな接続について説明します。それぞれの接続を使用するアプリケーションごとに、アプリケーションをグループ化します。

マネージメント・セントラル・ファイアウォールのクイック・リファレンス
簡単なケースで、マネージメント・セントラルを機能させるために、ファイアウォールで開ける必要のあるポートがリストされた表です (ネットワーク・アドレス変換が使用されている場合は無効)。

ネットワーク・アドレス変換によるマネージメント・セントラルの制限
静的および動的ネットワーク・アドレス変換について、およびこれらのアドレス変換のタイプがマネージメント・セントラルに及ぼす影響について説明します。

シナリオ 1 - ファイアウォールによって保護されたグラフィカル・クライアント
グラフィカル・クライアントがファイアウォールによってネットワークの他の部分から保護されている場合に、マネージメント・セントラルを使用可能にするために必要な構成について、詳しく説明します。

シナリオ 2 - ファイアウォールによって保護されたセントラル・システム
セントラル・システムおよびエンドポイント・システム・サーバーが、共通のファイアウォールによってグラフィカル・クライアントとネットワークの他の部分から、保護されている場合に、マネージメント・セントラルを使用可能にするために必要な構成について、詳しく説明します。

シナリオ 3 - ファイアウォールによって保護されたエンドポイント・システム
エンドポイント・システム・サーバーが、共通のファイアウォールによって、セントラル・システム、ソース・システム、およびネットワークの他の部分から保護されている場合に、マネージメント・セントラルを使用可能にするために必要な構成について、詳しく説明します。

© Copyright IBM Corp. 2005

第 1 章 用語

主要な用語を明確に定義しておくことが重要です。マネージメント・セントラルおよびファイアウォールに関連する用語の中にはあいまいなものもあるので、始めにそれらを明確に定義することが必要となります。本書で使用されているこれらの用語は、特に記述されていない限り、この定義で示されたとおりの内容を指しています。

セントラル・システム (CS) (Central System (CS))
他の iSeries システムを管理するために使用される iSeries(TM) システム。マネージメント・セントラル (MC) のセントラル・システムは、マネージメント・セントラル (MC) のエンドポイント・システムに要求を送信して応答を受信し、タスクやモニター・サービスを実行する。システム、インベントリー、タスク、およびモニターの定義を含むマネージメント・セントラル・データは、セントラル・システム iSeries に保管される。それぞれの iSeries システムは、MC セントラル・システムとしての管理を行えるほか、MC エンドポイント・システムとして管理される側となることもできる。

動的ネットワーク・アドレス変換 (動的 NAT) (Dynamic Network Address Translation (Dynamic NAT))
ローカル IP アドレスを、グローバル IP アドレスのプールの中で最初に使用可能なものにマッピングすること。ほとんどのファイアウォールにはこのオプションがあり、ユーザーが各接続ごとに動的 NAT、静的 NAT を指定したり、NAT を使用しないように指定したりすることができる。ポート・アドレス変換 (PAT)、単一アドレス NAT、ポート・レベル多重化 NAT、および多重定義とも呼ばれる。本書では、これらのタイプはすべて、単に動的 NAT と表記している。

エンドポイント・システム (EP) (Endpoint System (EP))
iSeries セントラル・システムによって管理される iSeries システム。マネージメント・セントラル (MC) のセントラル・システムは、マネージメント・セントラル (MC) のエンドポイント・システムに要求を送信して応答を受信し、タスクやモニター・サービスを実行する。それぞれの iSeries システムは、MC セントラル・システムとしての管理を行えるほか、MC エンドポイント・システムとして管理される側となることもできる。

iSeries ホスト・サーバー (iSeries Host Server)
iSeries 上で稼働し、iSeries ナビゲーター・クライアントからの要求を受信して処理するサーバー。これらのホスト・サーバーにはさまざまな目的があり、iSeries ナビゲーターが持つ単一システムの機能の多くを提供する (これには、「ユーザー接続」コンテナーの下にあるシステムに提供されるほとんどの機能が含まれる)。

マネージメント・セントラル (MC) (Management Central (MC))
マネージメント・セントラルは、3 層の分散アーキテクチャーで構成され、 iSeries システム管理アプリケーションのセットをホストする。マネージメント・セントラルには、iSeries ナビゲーター・グラフィカル・クライアント (V5R1 ではオペレーション・ナビゲーター)、iSeries MC セントラル・システム・サーバー、および iSeries MC エンドポイント・システム・サーバー内にインプリメントされる、C++ および Java(TM) ベース・クラスのインフラストラクチャーが含まれる。

マネージメント・セントラル・アプリケーション (Management Central Application)
マネージメント・セントラル・インフラストラクチャーを使用する関連機能のセット。例えば、マネージメント・セントラル・アプリケーションである「システム・モニター」は、グラフ表示、しきい値、および自動化プリミティブを使用して、iSeries のシステム・レベルのパフォーマンス・メ

© Copyright IBM Corp. 2005

トリックを分散モニターすることができる。マネージメント・セントラル・アプリケーションの「リモート・コマンド」は、永続的な iSeries のコマンド定義、分散コマンド実行、およびトラッキングを提供する。

マネージメント・セントラル C++ インフラストラクチャー (Management Central C++ infrastructure)
C++ クラス・ライブラリーとしてインプリメントされた MC の分散アーキテクチャー。このライブラリーでは、通信、パーシスタンス、分散、同期および非同期の処理など、豊富なアプリケーション・ビルド・ブロックのセットを使用できる。 MC C++ インフラストラクチャーは、iSeries ナビゲーターのグラフィカル・クライアント (V5R1 ではオペレーション・ナビゲーター)、iSeries MC セントラル・システム・サーバー、および iSeries MC エンドポイント・システム・サーバー内で使用できる。

マネージメント・セントラル Java インフラストラクチャー (Management Central Java Infrastructure)
Java クラス・ライブラリーとしてインプリメントされた MC の分散アーキテクチャー。このライブラリーでは、通信、パーシスタンス、分散、同期および非同期の処理など、豊富なアプリケーション・ビルド・ブロックのセットを使用できる。 MC Java インフラストラクチャーは、iSeries ナビゲーターのグラフィカル・クライアント (V5R1 ではオペレーション・ナビゲーター)、 iSeries MC セントラル・システム・サーバー、および iSeries MC エンドポイント・システム・サーバーで使用できる。

ソース・システム (または、モデル・システム) (Source System (Model System))
マネージメント・セントラルのアプリケーション・データのソースまたはモデルとして使用される iSeries システム。例えば「ソフトウェアの配布」では、すべてのターゲット・システムがどのソース・システムからパッケージ配布項目を取得するかが選択される。「修正を比較して更新」は、すべてのターゲット・システムの比較対象とする (および更新元となる) モデル・システムを選択する。

静的ネットワーク・アドレス変換 (静的 NAT) (Static Network Address Translation (Static NAT))
1 つの内部 IP アドレスを、特定 (かつ不変) の外部 IP アドレスにマッピングすること。1 対 1 の静的マッピング。ほとんどのファイアウォールにはこのオプションがあり、ユーザーが各接続ごとに動的 NAT、静的 NAT を指定したり、NAT を使用しないように指定したりすることができる。

ターゲット・システム (Target Systems)
マネージメント・セントラル・アプリケーションのデータまたはアクションの、宛先または受信側となる iSeries システム。例えば、「修正を比較して更新」(または同様の他のタスク) のターゲットとして使用される、1 つ以上のシステムのことを指す。これらのシステムはソース・システム (またはモデル・システム) と比較され、必要に応じて更新される。

第 2 章 マネージメント・セントラル接続

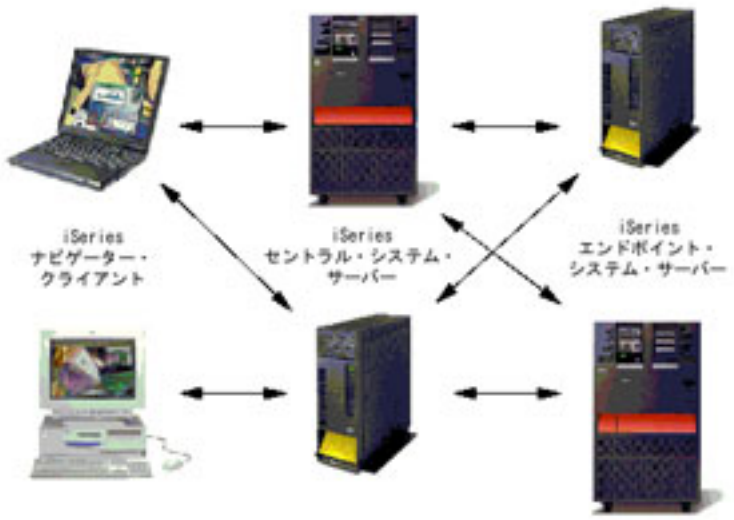

図 1. マネージメント・セントラル接続の概要

以下のセクションでは、インフラストラクチャー、アプリケーション、セキュア・ソケット、および接続構成など、マネージメント・セントラル接続の概要について説明します。

マネージメント・セントラルは、3 層のアーキテクチャーで構成されており、複数システムの管理を、セントラル・システムの iSeries を介して、iSeries(TM) ナビゲーターのグラフィカル・クライアント (V5R1 ではオペレーション・ナビゲーター) から実行できるようにします。マネージメント・セントラルのアーキテクチャーは、類似した別個の 2 つの分散インフラストラクチャーから成り、その 1 つは C++ で、もう 1 つは Java(TM) でインプリメントされています。 V5R3 より、C++ インフラストラクチャーは段階的に廃止され、Java インフラストラクチャーに置き換えられます。グラフィカル・クライアント上では、 C++ と Java インフラストラクチャーの双方が、iSeries ナビゲーターのプロセス内で使用されます。 iSeries サーバー上では、マネージメント・セントラルの C++ および Java インフラストラクチャーは、2 つの別個の長期実行デーモン・ジョブ内 (C++ は QYPSSRV、Java は QYPSJSVR) で別個に作動します。V5R3 からは、 QYPSJSVR ジョブのみが存在し、このジョブが、V5R2 以前は QYPSSRV ジョブがサポートしていた機能もサポートしています。マネージメント・セントラルの C++ および Java インフラストラクチャーのインプリメンテーションによって確立される TCP/IP 接続の特性と制限は、固有のものです。したがって、それぞれのインフラストラクチャーによって使用可能となるマネージメント・セントラル・アプリケーションには、それらと同じ特性と制限が適用されます。

V5R2 以前のリリースでは、マネージメント・セントラルが 2 つのインフラストラクチャーとサーバーを使用するため、個々のシステムにあるそれぞれの MC アプリケーションでどのポートが使用されているのかを判別することが難しい場合もありますが、 V5R3 では、V5R3 の Java サーバーのみに切り替えられました。以下のセクションでは、それぞれの MC アプリケーションで使用されるポートについて詳しく説明します。ただし、使用する MC アプリケーションの数が極めて少ない場合や、 1 つか 2 つ使用されな

© Copyright IBM Corp. 2005

いポートがあってもすべての MC ポートを開けてしまって問題ない場合には、このセクションは参考程度に目を通すだけでも差し支えありません。使用されるポート、および設定が必要と思われるその他のプロパティーについてのみ注目すればよく、実際にポートやプロパティーを使用するアプリケーションについては、留意する必要はありません。

C++ インフラストラクチャー

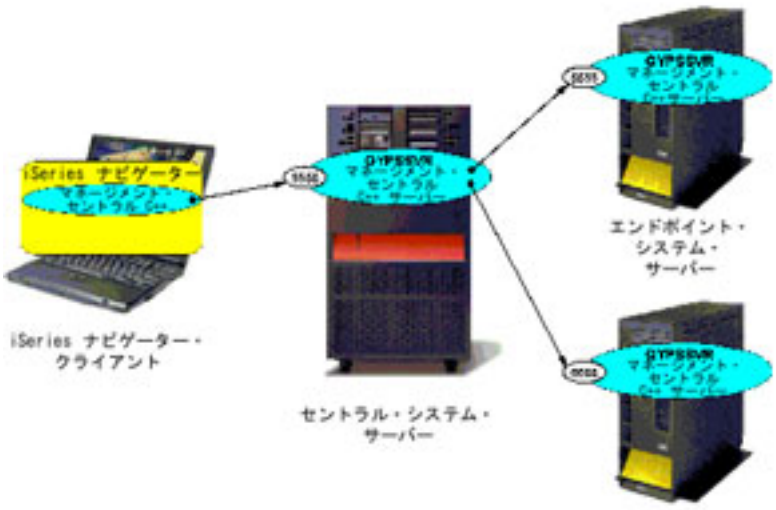

図 2. マネージメント・セントラルの C++ インフラストラクチャー接続

上の図は、初期の V4R3 マネージメント・セントラル製品で導入された C++ インフラストラクチャーで確立される接続とポートを表しています。C++ インフラストラクチャーのインプリメンテーションは、各グラフィカル・クライアントからセントラル・システム・サーバー (QYPSSRV) へ、および、セントラル・システム・サーバーから各エンドポイント・システム・サーバー (QYPSSRV) への、2 地点間の TCP/IP ソケットを作成します。すべての 2 システム間のシングル・ソケット接続で、パケットが双方向に送受信されます。C++ サーバーへの着信接続用のポート番号は、デフォルトで 5555 に設定されていますが、各 iSeries サーバー上で「サービス・テーブル項目 (Service Table Entries)」によって構成可能です (『接続構成』を参照)。C++ インフラストラクチャーは、iSeries サーバーからグラフィカル・クライアントへの接続の確立を試行することはありません。

V5R3 では、C++ サーバー (QYPSSRV) は存在しないので、QYPSJSVR ジョブが、QYPSSRV で行われていた処理を引き継いでいます。そのため V5R3 では、QUAFFS がポート 5555 で (通常の 5544 に加えて) 着信接続を listen しています。 V5R1 および V5R2 システム上で稼働する C++ サーバーは、ポート 5555 を使用して、V5R3 システム上の Java サーバー (QYPSJSVR) に接続します。上の図では、各 iSeries 上の C++ サーバーを示していますが、V5R3 ではこれらのサーバーは QYPSJSVR に置き換えられ、QYPSJSVR がポート 5555 を listen しています。

V5R2 以降では、C++ マネージメント・セントラル・インフラストラクチャーで、以下のアプリケーションを使用できます。

- システム・モニター
- グラフ・ヒストリー
- 収集サービス
- インベントリー
- ユーザーおよびグループ (ユーザー送信を除く)
- コマンドの実行
- プロダクトのインストール
- 修正 (修正の送信を除く)

V5R3 システムでは、これらのアプリケーションは、マネージメント・セントラル Java インフラストラクチャーを使用して実行されます (後のセクションで説明します)。そのため、これらのアプリケーションは、V5R3 システム間で稼働している場合は Java インフラストラクチャーのポートを使用して通信し、V5R2 システム間 (または V5R2 システムと V5R3 システムとの間) で稼働している場合は、CA++ インフラストラクチャーのポートを使用します。

CA++ 拡張

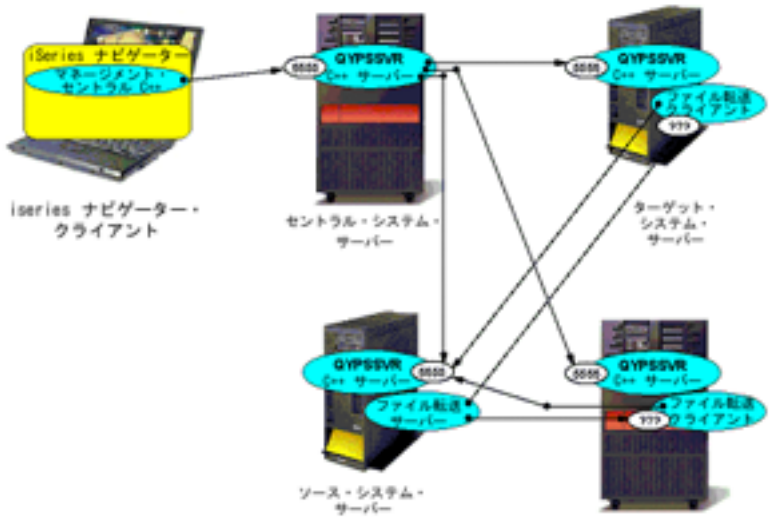

図 3. マネージメント・セントラル CA++ 拡張の接続

iSeries サーバーの CA++ インフラストラクチャーは、ソース iSeries サーバーと複数のターゲット iSeries サーバーとの間に、ファイル転送機能 (BDT - 大量データ転送プログラム) を提供します。このファイル転送機能は、各ターゲット・サーバーでは転送クライアント・ジョブとして、ソース・サーバーでは転送サーバー・ジョブとして、インプリメントされます。上の図は、 VA マネージメント・セントラル製品で導入されたファイル転送機能によってポートと接続が確立された、CA++ インフラストラクチャーのポートおよび接続の拡張を表しています。グラフィカル・クライアントとセントラル・システム・サーバーとの間の接続、およびセントラル・システム・サーバーと各エンドポイント・システム・サーバーとの間の接続に加

えて、短波での 2 地点間 TCP/IP ソケット接続が、各ターゲット・システム上のファイル転送クライアントとソース・システム・サーバー (QUIPS) との間に確立されています。ファイル転送クライアントは、自身のコールバック IP アドレスおよびポート番号を判別し、この一時的なソケット接続を使用してファイル転送サーバーへ伝達します。ファイル転送クライアントは、getHostName 呼び出しおよび getHostByName 呼び出しを使用して、自身のコールバック IP アドレスを判別します。

ターゲット・システムのホスト名は、各 iSeries サーバーで QYPS_HOSTNAME プロパティーによって構成可能です (『接続構成』を参照)。続いて、TCP/IP ソケットのコールバック接続が、ソース・システム上の関連するファイル転送サーバーから、各ターゲット・システム上のファイル転送クライアントに対して確立されます。 C++ インフラストラクチャーの場合と同様に、ソース・システム・サーバー (QYPSSRV) の着信接続用のポート番号は、デフォルトで 5555 となっています。ファイル転送コールバック接続のポート番号は、デフォルトで 1024 より大きい値に設定され、ターゲット・システムで無作為に選ばれます。
V5R2 以降のシステムでは、ファイル転送コールバック接続用のポート番号の範囲は、マネージメント・セントラル構成プロパティーを使用して各サーバー上で構成することができます (『接続構成』を参照)。

V5R2 以降では、C++ インフラストラクチャーによって使用可能な以下のマネージメント・セントラル・アプリケーションでも、 C++ ファイル転送機能を利用します。

- パッケージの配布
- プロダクトの送信
- ユーザー送信
- 修正の送信

C++ インフラストラクチャーのセクションで前述したように、V5R3 では Java サーバーが C++ サーバーの機能を引き継いでおり、QYPSSRV ジョブは存在しません。そのため、V5R3 システムでは、上記のアプリケーションは、マネージメント・セントラル Java インフラストラクチャーおよびマネージメント・セントラル Java 拡張 (後述のセクションで説明) を使用して実行されます。つまり、これらのアプリケーションは、V5R3 システム間で稼働する場合には Java インフラストラクチャーと Java 拡張ポートを使用して通信し、V5R2 システム間 (または V5R2 システムと V5R3 システムとの間) で稼働する場合は C++ インフラストラクチャーと C++ 拡張ポートを使用します。

Java インフラストラクチャー

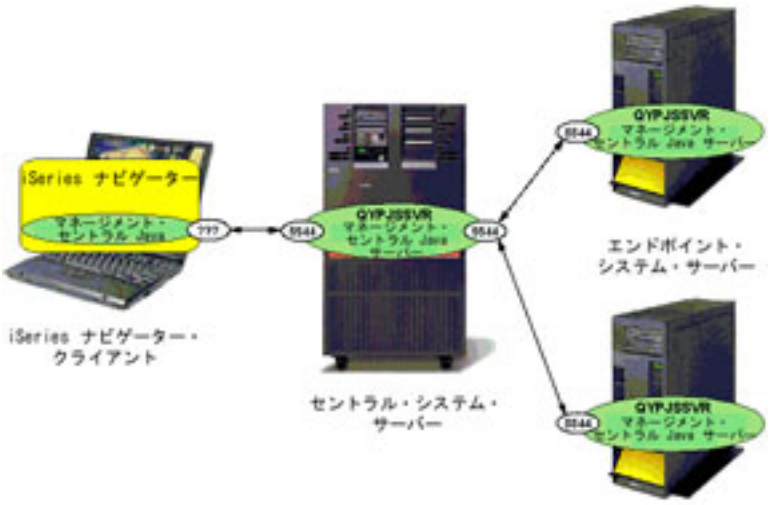

図 4. マネージメント・セントラルの Java インフラストラクチャー接続

上の図は、V5R1 マネージメント・セントラル製品で導入された Java インフラストラクチャーによって確立された接続およびポートを表しています。 Java インフラストラクチャーは、Java リモート・メソッド呼び出し (RMI) テクノロジーを利用して、グラフィカル・クライアントと iSeries サーバー (QYPSJSVR) との間の接続を確立します。RMI は、システム間で TCP/IP ソケット接続を確立して維持し、RMI でマーシャルされたデータをやり取りします。 Java インフラストラクチャーによって高頻度で利用される RMI 機能 (リモート・オブジェクト/参照) の副次作用として、各システム間で双方向の TCP/IP ソケットを確立することが必要となります。 RMI は、コールバック・ホスト名とポート番号を含む各リモート参照ごとに、マーシャルされたデータを生成します。この (ホスト名とポート番号を含む) マーシャルされたデータは、 RMI プロトコル内にあり、動的な変換では使用できません。各システムは、getHostName 呼び出しを使用して、自身のホスト名を判別します。ホスト名は、QYPS_HOSTNAME プロパティーを使用して、各 iSeries ナビゲーターのグラフィカル・クライアントおよび各 iSeries サーバーで構成可能です (『接続構成』を参照)。

マーシャルされたデータ内のホスト名およびポート番号は、このシステムへ戻る通信を行うために、別のシステムによって使用されます。Java サーバー (QYPSJSVR) の着信接続用のポート番号はデフォルトでは 5544 であり、各 iSeries サーバーで「サービス・テーブル項目 (Service Table Entries)」を使用して構成可能です (『接続構成』を参照)。グラフィカル・クライアントの着信 Java インフラストラクチャー接続用のポート番号は、デフォルトでは、クライアント・システムで無作為に選ばれます。これは、各クライアントでプロパティー・ファイルを使用して構成可能です (『接続構成』を参照)。マーシャルされたデータ内のホスト名 (実際のホスト名または IP アドレスのいずれか) は、他のシステムがこのシステムと通信するために使用するアドレスを表しています。デフォルトでは、このホスト名は、そのホストが自身の IP アドレスとして認識している値に設定されます。これは、各 iSeries サーバーおよびグラフィカル・クライアントで QYPS_HOSTNAME プロパティーを使用して構成可能です (『接続構成』を参照)。

Java インフラストラクチャーは、V5R1 マネージメント・セントラル製品で導入されました。V5R3 では以下のアプリケーションを使用できます。

- システム値の比較および更新
- 日付および時間の同期化
- 機能の同期化
- ジョブ・モニター
- メッセージ・モニター
- ファイル・モニター
- B2B モニター
- BRMS タスク
- スケジュール済み LPAR リソースの移動

以下のアプリケーションは、V5R3 システムでは Java インフラストラクチャーを使用しますが、V5R2 以前のシステムでは C++ インフラストラクチャーを使用します (詳しくは、『C++ インフラストラクチャー』のセクションを参照)。

- システム・モニター
- グラフ・ヒストリー
- 収集サービス
- インベントリー
- ユーザーおよびグループ (ユーザー送信を除く)
- コマンドの実行
- プロダクトのインストール
- 修正 (修正の送信を除く)

以下の図 4a で示すとおり、「日付および時間の同期化」アプリケーションは、上の図 4 では示されていない追加の接続を確立します。「日付および時間の同期化」では、すべてのターゲット・システムの Java サーバーが、モデル・システムの Java サーバーに接続し、今度はそのモデル・システムが各ターゲット・システムの Java サーバーへと接続します。

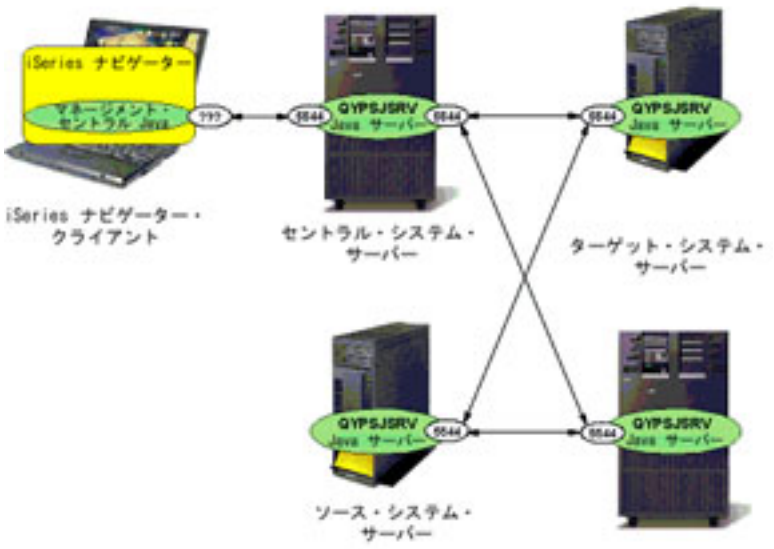

図 4a. マネージメント・セントラルの日付および時間の同期化の接続

また、「機能の同期化」アプリケーションは、モデル・システムを別のエンドポイントと同様に扱います。つまり、CS の Java サーバーはモデル・システムの Java サーバーに接続し、モデル・システムの Java サーバーは CS の Java サーバーに接続します。

Java 拡張

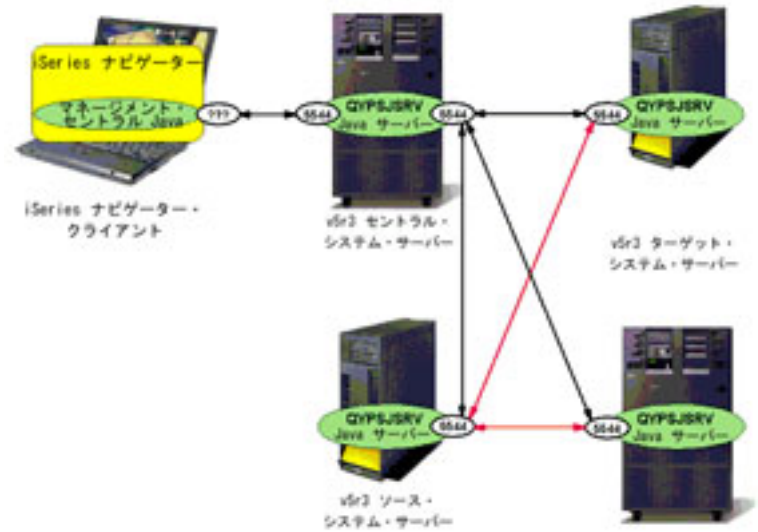

図 5. マネージメント・セントラルの Java 拡張用の接続 (赤が BDT 接続)

V5R3 では、Java インフラストラクチャーに、ソース iSeries サーバーと複数のターゲット iSeries サーバーとの間でのファイル転送機能 (BDT - 大量データ転送プログラム) が追加されました。この BDT 機能は、C++ の BDT 機能 (前述の 『CA++ 拡張』のセクションを参照) と同じ機能を提供しますが、インプリメントの方法は異なります。 Java ファイル転送機能では、ファイル転送を実行するために Java インフラストラクチャーのポートを使用しますが、この機能は V5R3 で導入されたものであるため、これが可能となるのは、V5R3 以降のソース・システムと V5R3 以降のターゲット・システムとの間のみです。ソース・システムまたはターゲット・システムの一方 (または両方) が V5R2 以前のモデルである場合、それらのシステム間でのファイル転送には、C++ ファイル転送機能とそれに関連するポートが使用されます。

上の図 5 は、V5R3 ソース・システムと V5R3 ターゲット・システムとの間の Java BDT で使用される接続を表しています。V5R3 ソース・システムと V5R3 ターゲット・システムを使用する場合、大量データ転送プログラムでは、ポート 5544 で開始された接続を使用するという点に注意してください。つまり、前述の『C++ 拡張』のセクションで述べたポート番号の範囲は使用されません。ただし、ソースまたはターゲットのいずれかが V5R3 より前のリリースである場合には、C++ 拡張ポートが使用されることから、この範囲内のポートが使用されます。

V5R3 では、以下のマネージメント・セントラル・アプリケーションが Java インフラストラクチャーを使用し、また、Java ファイル転送機能も利用します。

- パッケージの配布
- プロダクトの送信
- ユーザー送信
- 修正の送信

V5R3 以降のシステムのみを使用している場合、これらのアプリケーションでは Java ファイル転送機能を使用する点に注意してください。V5R2 以前のシステムが 1 つ以上含まれている場合の通信では、引き続き C++ ファイル転送機能を使用します (詳しくは『C++ 拡張』のセクションを参照)。

ホスト・サーバー

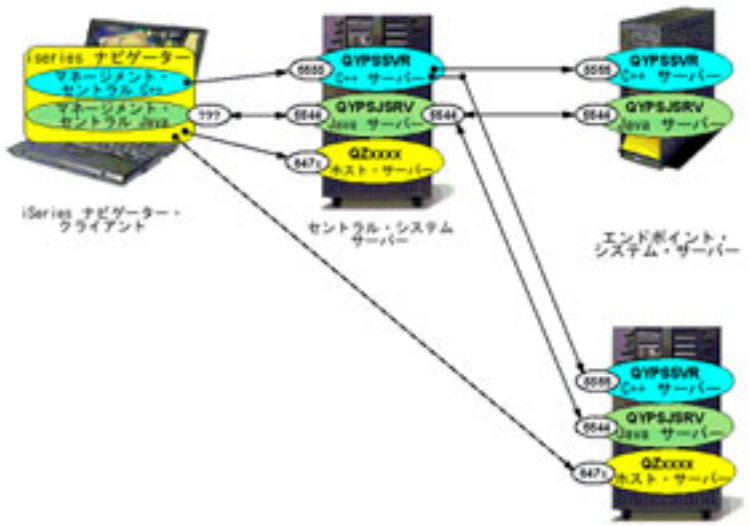

図 6. マネージメント・セントラルが使用するホスト・サーバーに対する接続

iSeries ナビゲーターのグラフィカル・クライアント内では、マネージメント・セントラル分散アプリケーションと、単一システムの iSeries ナビゲーター機能が混在しています。これらの単一システムのナビゲーター機能は、iSeries ホスト・サーバーのセットに対して、2 地点間 TCP/IP ソケット接続を確立します。これらの iSeries ホスト・サーバーへの 2 地点間ソケット接続は、各 iSeries ナビゲーター・クライアント内にある複数のアプリケーションで共有されます。マネージメント・セントラル・アプリケーションのインプリメンテーションの一部は、グラフィカル・クライアントにあるこれらの共有ホスト・サーバー接続を利用して、セントラル・システムと対話します。同様に、一部のマネージメント・セントラル・アプリケーションが、これらの接続を利用してエンドポイント・システムと直接対話します。例えば、「システム値の比較および更新」は、iSeries ナビゲーターのグラフィカル・クライアントから直接モデル・システムに接続し、モデル・システムからシステム値を取得します。以下の URL のページ http://publib.boulder.ibm.com/iseries/V5R3/ic2962/index.htm?info/rzaii/rzaiihstsvrbyfnctn.htm および http://publib.boulder.ibm.com/iseries/V5R3/ic2962/index.htm?info/rzaii/rzaiicahstsvr.htm では、iSeries ホスト・サーバーと、それらがクライアント・アプリケーションに提供する機能について詳しく説明しています。各 iSeries ホスト・サーバーで使用されるポート番号のリストを入手するには、http://www-1.ibm.com/servers/eserver/iseries/access/caiixe1.htm にアクセスし、APAR II12227 を選択してください。iSeries ホスト・サーバーが使用するポート番号は、通常、マネージメント・セントラルによって使用されるものであり、非 SSL 接続では 8470 から 8476、SSL 接続では 9470 から 9476 の範囲です。

セキュア・ソケット・レイヤー

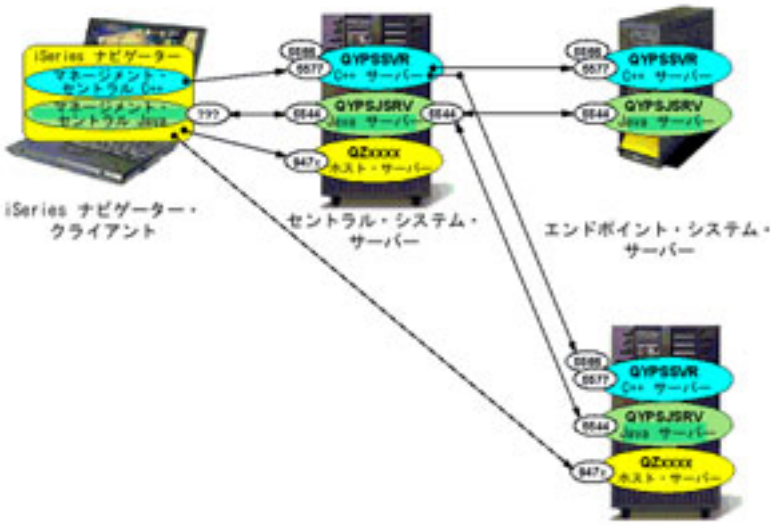

図 7. マネージメント・セントラル SSL 接続

グラフィカル・クライアント、セントラル・システム、およびエンドポイント・システムのすべてが、同じローカル・エリア・ネットワーク内にない場合 (例えば、自宅からオペレーション・ナビゲーターを使用して、仕事場の iSeries システムを管理している場合など)、ユーザーのシステム間で送受信されるマネージメント・セントラル要求は、ユーザーの制御できないネットワークを介して転送されます。このデータは傍受される可能性があります。このデータを保護するには SSL (セキュア・ソケット・レイヤー) の使用が最適です。マネージメント・セントラルでは、SSL 接続を利用して、データ暗号化と証明書検証によるセキュリティー向上を実現できます。iSeries サーバーと iSeries ナビゲーター・クライアントのセット全体にわたって SSL を構成し、マネージメント・セントラルで SSL を使用するという作業は、非常に大変な作業となります。

次に示す IBM Information Center のページ (URL: http://publib.boulder.ibm.com/iseries/V5R3/ic2962/index.htm?info/rzain/rzainoverview.htm) では、 iSeries ナビゲーターとマネージメント・セントラル用の SSL 構成について詳しく説明しています (「SSL 使用可能化計画 (Plan for SSL enablement)」を選択してから、「SSL によるアプリケーションの保護 (Secure applications with SSL)」->「マネージメント・セントラル (Management Central)」の順にリンクを選択してください)。マネージメント・セントラルを SSL 用に構成し、SSL を使用可能にすると、C++ インフラストラクチャー内でのサーバー認証はポート番号 5566 を使用し、C++ インフラストラクチャー内でのクライアント/サーバー認証はポート番号 5577 を使用します。

SSL を使用可能にした場合のマネージメント・セントラル接続とポート番号に対する影響は、前出の C++ インフラストラクチャー接続の図において、ポート番号 5555 が、選択された認証に応じて 5566 および/または 5577 に置き換わる、という点のみです。Java インフラストラクチャーは、SSL の使用可能化や、選択された認証に関係なく、引き続きポート番号 5544 を使用します。これらの各ポート番号は、マネージメント・セントラルの構成プロパティーによって構成可能です (『接続構成』を参照)。

マネージメント・セントラル・アプリケーションによって通常利用される iSeries ホスト・サーバーが SSL 用に構成されている場合、それらのホスト・サーバーによって使用されるポート番号は、9470 から 9476 の範囲です。

接続構成

各サーバーおよび各 iSeries ナビゲーター・クライアントの、マネージメント・セントラル接続特性の一部は、構成可能となっています。以下に、マネージメント・セントラル接続特性、構成メカニズム、およびデフォルトの値/振る舞いを記したリストを示します。

「サービス・テーブル項目 (Service Table Entries)」によるサーバー構成 (すべてのリリース) - WRKSRVTBLE

接続特性	*構成メカニズム*	*デフォルト値*
Java サーバー・ポート	サービス “as-mgtctrlj” - プロトコル “tcp”	5544
C++ サーバー非 SSL ポート (V5R3 では Java サーバーが使用)	サービス “as-mgtctrl” - プロトコル “tcp”	5555
C++ SSL サーバー検証ポート (V5R3 では Java サーバーが使用)	サービス “as-mgtctrl-ss” - プロトコル “tcp”	5566
C++ SSL Clt/Svr 検証ポート (V5R3 では Java サーバーが使用)	サービス “as-mgtctrl-cs” - プロトコル “tcp”	5577

システム・レベル環境変数によるサーバー構成 (V5R2 のみ) - WRKENVVAR LEVEL(*SYS)

接続特性	*構成メカニズム*	*デフォルト値*
ファイル転送ポートの範囲	変数 “QYPS_MINIMUM_PORT”	1024
ファイル転送ポートの範囲	変数 “QYPS_MAXIMUM_PORT”	32768

ファイル「/QIBM/UserData/OS400/MGTC/config/McConfig.properties」でのサーバー構成 (V5R1 および V5R2 のみ)

接続特性	*構成メカニズム*	*デフォルト値*
Java サーバー・ホスト名	プロパティー ″QYPS_HOSTNAME=xxxx″	IP アドレス/ホスト名

ファイル「/QIBM/UserData/OS400/MGTC/config/McEPConfig.properties」でのサーバー構成 (V5R3 のみ)

接続特性	*構成メカニズム*	*デフォルト値*
ファイル転送ポートの範囲	プロパティー ″QYPS_MINIMUM_PORT″	1024
ファイル転送ポートの範囲	プロパティー “QYPS_MAXIMUM_PORT”	32768
Java サーバー・ホスト名	プロパティー ″QYPS_HOSTNAME=xxxx	IP アドレス/ホスト名

ファイル「C:¥MgmtCtrl.properties」でのクライアント構成 (すべてのリリース)

接続特性	*構成メカニズム*	*デフォルト値*

Java クライアント・ホスト名	プロパティー ″;QYPS_HOSTNAME=xxxx″	IP アドレス/ホスト名
Java クライアント・ポート	プロパティー ″QYPSJ_LOCAL_PORT=xxxx″	ランダム

注: iSeries ホスト・サーバーで使用されるポート番号は、関連する「サービス・テーブル項目 (Service Table Entries)」によって、各 iSeries サーバーで構成することもできます。

第 3 章 マネージメント・セントラル・ファイアウォールのクイック・リファレンス

以下のセクションは、マネージメント・セントラルを、ファイアウォールを介して機能するようにセットアップするためのクイック・リファレンスです。この表は、マネージメント・セントラルと、使用するネットワーク構成が以下の方法でセットアップされている場合にのみ有効です。

- 関係するファイアウォールが、ネットワークアドレス変換を使用しない。
- 使用するグラフィカル・クライアントの MgmtCtrl.properties ファイルで、 QYPSJ_LOCAL_PORT=5544 と設定されている。5544 が使用されるようにこのプロパティーを設定するには、使用する PC で C:¥ に MgmtCtrl.properties というテキスト・ファイルを作成 (まだ存在しない場合) して、 QYPSJ_LOCAL_PORT=5544 という行を追加してください。
- 使用するすべての iSeries(TM) システムで、サービス・テーブル項目 as-mgtctrl が 5555 に設定され (SSL がオンの場合、as-mgtctrl-ss は 5566、as-mgtctrl-cs は 5577)、as-mgtctrlj が 5544 に設定されている。これらはデフォルトの設定値であり、変更されているかどうかをチェックするには、WRKSRVTBLE を使用します。

注: SSL が使用可能となっている場合は、括弧内のポートも開かれている必要があります。

アプリケーションのタイプ	アプリケーション	グラフィカル・クライアントのファイアウォールで開くポート	セントラル・システムのファイアウォールで開くポート	ソース・システムが使用されている場合に、ソース・システムのファイアウォールで開くポート	エンドポイント・システムのファイアウォールで開くポート
Java(TM) インフラストラクチャー	- ジョブ・モニター - メッセージ・モニター - ファイル・モニター - B2B モニター - BRMS タスク - 機能の同期化 (ソース・システムを使用)	5544	5544 5555 (5566、5577) 8470 から 8476*	5544	5544
	- スケジュール済み LPAR リソースの移動	5544	5544 5555 (5566、5577) 8470 から 8476*	N/A	5544**
	- 日付および時間の同期化	5544	5544 5555 (5566、5577) 8470 から 8476*	5544	5544
	- システム値の比較および更新	5544	5544 5555 (5566、5577) 8470 から 8476*	8470 から 8476*	5544

© Copyright IBM Corp. 2005

C++ インフラストラクチャー (V5R3 では Java インフラストラクチャー)	- システム・モニター - グラフ・ヒストリー - 収集サービス - インベントリー - ユーザーおよびグループ (ユーザー送信を除く) - コマンドの実行 - プロダクトのインストール - 修正 (修正のインストールを除く)	N/A	5544 5555 (5566、5577) 8470 から 8476*	N/A	5544 - V5R3 システムのみ 5555 (5566、5577)
C++ 拡張 (V5R3 では Java 拡張)	- パッケージの配布 - プロダクトの送信 - ユーザー送信 - 修正の送信	N/A	5544 5555 (5566、5577) 8470 から 8476*	5544 - V5R3 システムのみ 5555 (5566、5577)	5544 - V5R3 システムのみ 5555、(5566、5577)、ファイル転送クライアント用のポート範囲 ***

* 8470 から 8476 は、ホスト・サーバーが使用するポートの範囲です。各マネージメント・セントラル・アプリケーションは、これらのポートの別個のサブセットを使用します。マネージメント・セントラルで SSL が使用されている場合は、この代わりに 9470 から 9476 が開かれている必要があります。

**「スケジュール済み LPAR リソースの移動」では、1 次区画が唯一のエンドポイント・システムです。

*** QYPS_MINIMUM_PORT および QYPS_MAXIMUM_PORT の指定:

- V5R2 ターゲット・システムでは、システム・レベル環境変数 QYPS_MINIMUM_PORT および QYPS_MAXIMUM_PORT が、ファイル転送クライアントによって使用されるポートの範囲に設定されるように、各ターゲット・システムで指定することができます。
- V5R3 ターゲット・システムでは、QYPS_MINIMUM_PORT および QYPS_MAXIMUM_PORT を、/QIBM/UserData/OS400/MGTC/config/McEPConfig.properties ファイルで指定することができます。
- V5R1 ターゲット・システムでは、この範囲は 1024 から 32,768 であり、変更できません。

詳しくは、『マネージメント・セントラル接続』を参照してください。

第 4 章 ネットワーク・アドレス変換によるマネージメント・セントラルの制限

ファイアウォールは、本質的に、特定のシステムまたはシステムのセットに対して確立できる接続のタイプを制限します。分散アプリケーションを使用するために、ファイアウォールの構成変更、またはアプリケーションの構成変更、あるいはその両方が必要となる場合があります。分散アプリケーションを使用できるようにするための構成変更が存在せず、ファイアウォールを使用不可とするか完全に除去する以外には方法がない場合もあります。このセクションでは、ネットワーク・アドレス変換を使用するファイアウォールと、マネージメント・セントラルなどの分散アプリケーションにおいて、ファイアウォールが原因となって生じる制限について説明します。

ネットワーク・アドレス変換 (NAT)

ファイアウォールの多くは、ネットワーク・アドレス変換 (NAT) を使用するように構成できます。これを行うには、保護されたシステムが送受信する要求の一部またはすべてを、発信元または宛先の IP アドレスを変更することによって変更する規則を、管理者が設定します。ネットワーク・アドレス変換には数多くのタイプがありますが、動的 NAT と静的 NAT という 2 つのカテゴリーに大別することができます。例外はありますが、通常、マネージメント・セントラルのほとんどは、静的 NAT と連動するように構成することができます。動的 NAT と連動するように構成することはできません。

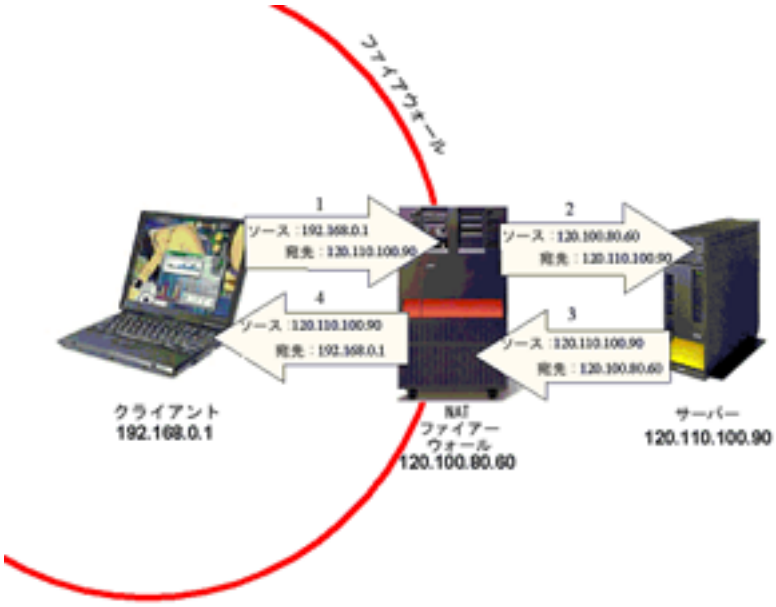

図 8. ネットワーク・アドレス変換

NAT が使用されるケースを上記の図に示します。ファイアウォール内のシステムが、ファイアウォール外のシステムとの接続を開始すると (上図のステップ 1)、ファイアウォールはその要求を受け取り、パケットのソース IP アドレス (パケットの発信元の IP アドレス) を、ファイアウォールの外部 IP アドレスと置き換えます (2)。このように、この要求に関連したすべての応答は、ファイアウォールに送信されます。その同じ接続に応答が返ってくると (3)、その応答はファイアウォールに到達します (これは、ファイアウ

© Copyright IBM Corp. 2005

ォールが、発信要求で、ソース IP アドレスをファイアウォールの外部アドレスに置き換えたためです)。ファイアウォールはこの応答を受け取り、通過を許可すべき応答かどうかを検証し、宛先の IP アドレスを変更して、適切な内部システムに転送します (4) 。

前述のように、内部システムによって接続が開始されれば、ファイアウォールの外部にあるシステムは、その接続を使用して内部システムと通信できます。これは、静的 NAT、動的 NAT の両方に当てはまります。静的 NAT と動的 NAT の違いは、静的 NAT では、外部システムがファイアウォール内部にあるシステムとの接続を開始できるのに対し、動的 NAT ではこれができないという点です。

静的 NAT

静的 NAT では、内部 IP アドレスを外部 IP アドレスにマップするテーブルがあります。ファイアウォール内部にある、内部 IP アドレス 192.168.0.1 のシステムから要求が送信されている場合、ファイアウォールは、テーブル内でその内部アドレスを探索して、どの外部アドレスに変換すべきかを調べます。次に、その外部 IP アドレスに応答が返ってくると、ファイアウォールは再度そのテーブルを使って、その外部 IP アドレスに関連付けられている内部システムを調べます。このテーブルは、静的と言えます (内部システムの外部 IP アドレスが、常に同じとなります)。つまり、内部システムの外部 IP アドレスを知っていれば、ファイアウォール外部のシステムは、その内部システムへの接続を開始できることになります。

動的 NAT

動的 NAT では、ファイアウォールは、発信要求に与える外部 IP アドレスを動的に決定します。すべての要求に同じ外部 IP アドレスが使用される可能性も、また、外部 IP アドレスのプール内にある使用可能なアドレスが各要求で順次使用される可能性もあります。静的なテーブルは使用されないため、ある時点では、内部システムの外部アドレスが 120.110.100.95 であり、次回には外部アドレスが 120.110.90.85 となる、という可能性があります。ファイアウォールが内部 IP アドレスを外部アドレスに変換するたびに、ファイアウォールはそれを記録しておくので、同じ接続に応答が返された場合には、ファイアウォールはその応答を適切な内部 IP アドレスへ送ることができます。

この方法で外部 IP アドレスを配布すると、ファイアウォール外部のシステムは、どの外部 IP アドレスを使用するか決められないため、内部システムへの接続を開始することはできません。ファイアウォール外部のシステムがファイアウォール内部のシステムと対話するには、ファイアウォール内部のシステムによって開始された要求に対して応答することが唯一の方法となります。

マネージメント・セントラルの制限

外部システムがファイアウォール内部のシステムへの接続を開始する必要がある分散アプリケーション (マネージメント・セントラル・アプリケーションを含む) はいずれも、動的 NAT とは連動しません。特定の動的 NAT の設定でのマネージメント・セントラルの使用については、前出の『マネージメント・セントラル接続』のセクションを参照し、どのマネージメント・セントラル・アプリケーションでどの接続を使用するかを確認してください (PC から CS、CS から PC、CS から EP、 EP から CS など)。その情報を、動的 NAT を使用しているシステムおよび接続に関する情報と共に使用して、稼働するアプリケーション、および稼働しないアプリケーションを判別してください。

外部システムからファイアウォール内部のシステムへの接続を確立する必要のある分散アプリケーション (マネージメント・セントラル・アプリケーションを含む) は、静的 NAT と連動します。ただし、ファイアウォール内部のシステムとの接続を確立しようとする外部システムが、その内部システムの外部 IP アド

レスを使用するように、特別にこれらのアプリケーションを構成することが必要となる場合がよくあります。マネージメント・セントラルにおいて、システム (iSeries(TM) または PC) が静的 NAT を使用するファイアウォール内部にある場合は、そのシステムの QYPS_HOSTNAME プロパティーを外部 IP アドレスに設定する必要があります。また、そのシステムが、ファイアウォール内部のシステムと外部のシステム両方と接続している場合には、内部システムに対してはその内部 IP アドレスに、外部システムに対してはその外部 IP アドレスに解決するホスト名を、そのシステムの QYPS_HOSTNAME に設定する必要があります。『マネージメント・セントラル接続』のセクションでは、この QYPS_HOSTNAME プロパティーの設定方法について説明しています (このプロパティーの設定は、システムのリリース時期によって異なります)。

第 5 章 ファイアウォールによって保護されたグラフィカル・クライアント

インターネットへの直接接続にも使用される、マネージメント・セントラルのグラフィカル・クライアントは、ファイアウォールによって保護されていることがよくあります。ソフトウェアおよび/またはハードウェアのファイアウォールは、高速のインターネット接続と共に、家庭でも一般的になりつつあります。特別な構成を行わないと、この簡単なファイアウォール環境によって、マネージメント・セントラルの機能が制限される場合があります。

目的

グラフィカル・クライアントがファイアウォールによって保護されている一般的なファイアウォール環境において、必要となるマネージメント・セントラル構成を詳しく説明します。

詳細

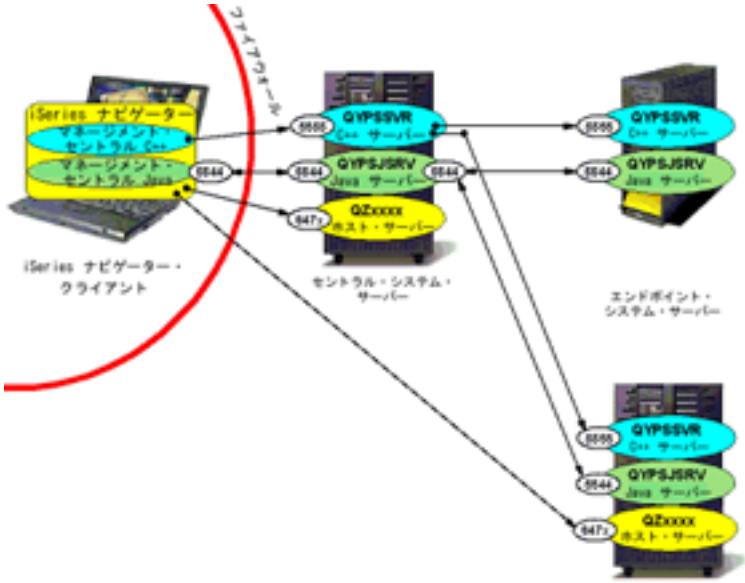

図 9. ファイアウォールによって保護されたグラフィカル・クライアント

上の図で注目すべきいくつかの重要点は、次のとおりです。

- セントラル・システムからエンドポイント・システムへの通信は、すべてファイアウォールの外にあるため、影響を受けません。セントラル・システムとエンドポイントとの間に追加のファイアウォールが存在する場合は、シナリオ 3 を参照するか、そのような接続の構成に関する情報を『マネージメント・セントラル接続』のセクションで参照してください。
- この図では、C++ サーバーが表示されていますが、V5R3 システムでは C++ サーバーは存在せず、その代わりに Java サーバーがポート 5555 を listen しています。

© Copyright IBM Corp. 2005

- グラフィカル・クライアントから、iSeries (TM) セントラル・システムのマネージメント・セントラル C++ サーバー (V5R3 では Java サーバー) へのポート 5555 での接続、および Java (TM) サーバーへのポート 5544 での接続は、ポート 5544 および 5555 に関する追加の構成を行わなくても、ファイアウォールを介して接続できます。
- iSeries セントラル・システムのホスト・サーバーへのグラフィカル・クライアント接続は、追加の構成を行わなくても、ファイアウォールを介して接続できます。
- デフォルトでは、セントラル・システムの Java サーバーからグラフィカル・クライアントへの接続用のポートは、無作為に選ばれます。このシナリオでは、マネージメント・セントラルの PC のプロパティー・ファイルで単一のポートを設定して (『接続構成』を参照)、CS からグラフィカル・クライアントへ戻る接続に使用されるポートが無作為に選ばれないようにする必要があります (図では 5544 が使用されていますが、別のポートを使用することもできます)。これについての詳細は、以下の説明を参照してください。
- SSL が使用されている場合には、この文書全体で、ポート 5555 と記されている箇所にポート 5566 と 5577 を含める必要があります。

マネージメント・セントラルを構成するステップは、NAT を使用するためにファイアウォールがどのように構成されているかによって、多少の違いがあります。

Warning: Temporary Level 2 Header

NAT を使用していないファイアウォール

- 前出の 4 番目の項目、および上の図で示されているように、セントラル・システムからグラフィカル・クライアントへの接続に使用するポートに、特定のポートを設定してください (詳しくは、『マネージメント・セントラル接続』のセクションを参照)。
- ファイアウォールを構成してその特定のポートを開き、セントラル・システムからのトラフィックがグラフィカル・クライアントへ到達できるようにしてください。

静的 NAT を使用するファイアウォール

- NAT を使用していないファイアウォールに関する、上記の説明に従ってください。
- グラフィカル・クライアントで QYPS_HOSTNAME プロパティー (『マネージメント・セントラル接続』のセクションを参照) に、このグラフィカル・クライアントの外部 IP アドレス (このグラフィカル・クライアントに接続するために、ファイアウォール外部のシステムが使用する IP アドレス) を設定してください。

動的 NAT を使用するファイアウォール

グラフィカル・クライアントを保護しているファイアウォールが動的 NAT を使用している場合、セントラル・システムは、グラフィカル・クライアントに戻る接続を確立することはできません。このため、Java インフラストラクチャーを使用するすべての MC アプリケーションは作動しません。Java インフラストラクチャーを使用しないアプリケーション (V5R2 では C++ アプリケーションであったが、 V5R3 で Java アプリケーションに変換されたアプリケーションを含む) は、構成を行わなくても正常に動作します (これは、PC に戻る接続を行うのは Java インフラストラクチャーのみであるためです)。

第 6 章 ファイアウォールによって保護されたセントラル・システム

もう 1 つの一般的なファイアウォール環境として、企業の内部ネットワークをインターネット・トラフィックから保護する、ソフトウェアおよび/またはハードウェアのファイアウォールがあります。 MC セントラル・システムに接続しようとするグラフィカル・クライアントがファイアウォール外部に位置している場合、マネージメント・セントラルの機能をすべて使用できるようにするには、構成を多少行う必要があります。

目的

iSeries (TM) のセントラル・システムおよびエンドポイント・システム・サーバーがファイアウォールによって保護されており、かつグラフィカル・クライアントがファイアウォールの外部に存在する、という一般的なファイアウォール環境において必要となるマネージメント・セントラル構成を詳しく説明します。

詳細

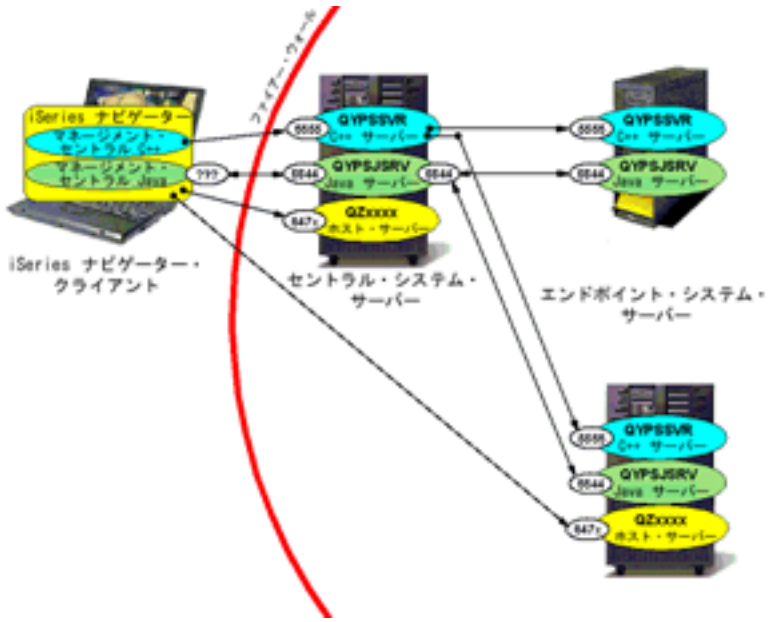

図 10. ファイアウォールによって保護された iSeries システム (CS および EP)

上の図で注目すべきいくつかの重要点は、次のとおりです。

- セントラル・システムからエンドポイント・システムへの通信は、これらがすべてファイアウォール内部にあるため、影響を受けません。セントラル・システムとエンドポイントとの間に追加のファイアウォールが存在する場合は、シナリオ 3 を参照するか、そのような接続の構成に関する情報を『マネージメント・セントラル接続』のセクションで参照してください。
- この図では、C++ サーバーが表示されていますが、V5R3 システムでは C++ サーバーは存在せず、その代わりに Java サーバーがポート 5555 を listen しています。

© Copyright IBM Corp. 2005

- グラフィカル・クライアントは、iSeries セントラル・システムにおいて、ポート 5555 でマネージメント・セントラルの C++ サーバー (V5R3 では Java サーバー) に、またポート 5544 で Java (TM) サーバーに、接続する必要があります。
- グラフィカル・クライアントは、セントラル・システム上のホスト・サーバー、また場合によっては他のシステム上にあるホスト・サーバーに接続する必要があります (例えば、グラフィカル・クライアントは、「システム値の比較および更新」アプリケーションを実行する場合、ホスト・サーバーを使用してモデル・システムに直接接続します)。
- SSL が使用されている場合には、この文書全体で、ポート 5555 と記されている箇所にポート 5566 と 5577 を含める必要があります。

マネージメント・セントラルを構成するステップは、NAT を使用するためにファイアウォールがどのように構成されているかによって、多少の違いがあります。

NAT を使用していないファイアウォール

- ファイアウォールのポート 5544 および 5555 を開き、グラフィカル・クライアントが、マネージメント・セントラルのセントラル・システムに接続できるようにしてください。
- 使用されているマネージメント・セントラル機能で必要なホスト・サーバーのポートを、ファイアウォールで開いてください。ファイアウォールを介して処理を行うホスト・サーバーのセットアップに関する一般的な追加情報は、 http://www-1.ibm.com/servers/eserver/iseries/access/cafirewl.htm を参照してください。

静的 NAT を使用するファイアウォール

- NAT を使用していないファイアウォールに関する、上記の説明に従ってください。
- iSeries ナビゲーターで、セントラル・システムが CS の外部 IP アドレスに接続するよう設定してください (「ユーザー接続」の下にあるセントラル・システムが外部 IP アドレスを使用するようにします)。
- 『マネージメント・セントラル接続』のセクションの説明に従って、セントラル・システムで QYPS_HOSTNAME を設定してください。これには、以下の 2 つの方法があります。
  1. セントラル・システムの QYPS_HOSTNAME を、セントラル・システムの外部 IP アドレスに設定する。この場合、すべての MC システム (エンドポイント・システムを含む。これはファイアウォール内にある可能性があります) が、外部 IP アドレスを使用してセントラル・システムに接続するということになります。
  2. QYPS_HOSTNAME の値に、外部システム (例えばグラフィカル・クライアント) の場合はセントラル・システムの外部 IP アドレスに解決し、内部システムの場合はセントラル・システムの内部 IP アドレスに解決する、という特定のホスト名を設定する。

動的 NAT を使用するファイアウォール

セントラル・システムを保護しているファイアウォールが動的 NAT を使用している場合、グラフィカル・クライアントは、これに接続することができません。つまり、ファイアウォール外部のシステムはいずれも、セントラル・システムへの接続を開始して分散アプリケーションを使用することはできません。

第 7 章 ファイアウォールによって保護されたエンドポイント・システム

特定の状況では、1 つの物理的な位置でセントラル・システムを使用して、別の場所にあるエンドポイント・システムのセットを管理する、という方法が適している場合があります。このケースでは、それらのエンドポイント・システムがファイアウォールで保護されていることが多く、そうした状況下では問題が多少発生する可能性があります。このシナリオでは、発生する可能性のある問題とその修正方法を説明します。

目的

エンドポイント・システムがファイアウォールによって保護されており、かつグラフィカル・クライアントとセントラル・システムの両方がファイアウォールの外部に存在する、というファイアウォール環境において必要となるマネージメント・セントラル構成を説明します。

詳細

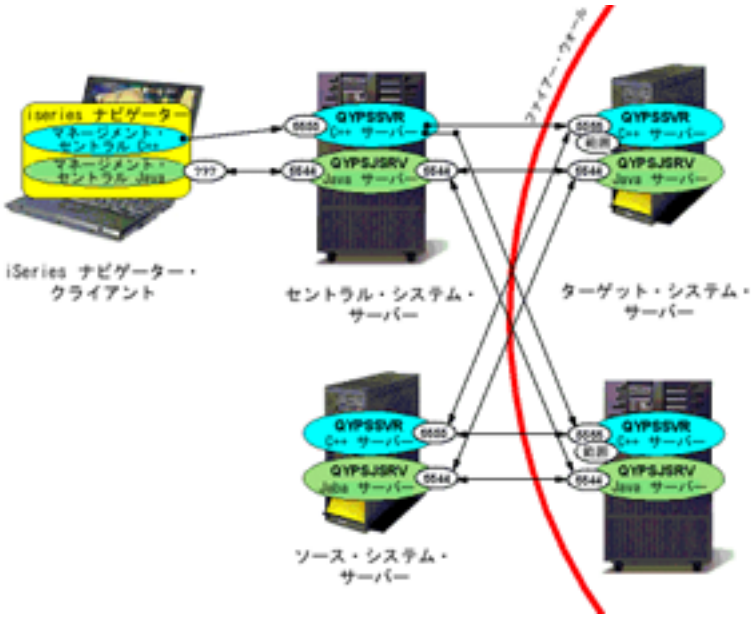

図 11. ファイアウォールによって保護されたエンドポイント・システム

この図は、エンドポイント・システムを保護しているファイアウォールを介して確立する必要のある接続を表しています。上の図で注目すべきいくつかの重要点は、次のとおりです。

- この図では、グラフィカル・クライアントからセントラル・システムへの接続がファイアウォール経由ではないことを前提としています。これに該当しない場合は、シナリオ 1 およびシナリオ 2 を参照するか、『マネージメント・セントラル接続』のセクションで、その場合の構成方法を参照してください。
- この図では、C++ サーバーが表示されていますが、V5R3 システムでは C++ サーバーは存在せず、その代わりに Java サーバーがポート 5555 を listen しています。

© Copyright IBM Corp. 2005

- この図には、グラフィカル・クライアントからセントラル・システム、またはグラフィカル・クライアントからエンドポイント・システムへのホスト・サーバー接続は含まれていません。ファイアウォールがこれらの接続を許可するようセットアップされていることが重要です。これらの接続を許可するために必要な作業については、シナリオ 2 を参照してください。
- この図では、ソース・システムはファイアウォールの外部にあります (ソース・システムは、ファイアウォール外部の CS または別のシステムである可能性があります)。ソース・システムがファイアウォール内部にある場合は、ソース・システムの通信するエンドポイント・システムもファイアウォール内部にあることから、ソース・システムの接続に関する問題は発生しないため、後述する構成の中には不要となるものもあります。
- CS は、5544 および 5555 の 2 つのポートで EP と通信します。
- SSL が使用されている場合には、この文書全体で、ポート 5555 と記されている箇所にポート 5566 と 5577 を含める必要があります。
- この図では、アプリケーションが BDT (C++ 拡張) を使用する場合、各ターゲット・システム (エンドポイント・システム) が listen するポートを無作為に選択し、ソース/モデル・システムの BDT サーバーはそのポートでエンドポイント・システムに接続してデータ転送を行う、という点に注意してください。
- V5R2 および V5R3 エンドポイント・システムでは、『マネージメント・セントラル接続』のセクションで述べた QYPS_MINIMUM_PORT プロパティーおよび QYPS_MAXIMUM_PORT プロパティーを使用して、この BDT ポート用のポート範囲を指定することができます。実行される各タスクは、開始時にそれぞれ個別の BDT ポートを必要とするため、BDT を使用するマネージメント・セントラル・アプリケーション 7 つをすべて同じターゲット・システムに対して同時に開始できるようにするには、ポート範囲に、少なくとも 7 つのポートがなければなりません。

マネージメント・セントラルを構成するステップは、NAT を使用するためにファイアウォールがどのように構成されているかによって、多少の違いがあります。

NAT を使用していないファイアウォール

ファイアウォールがネットワーク・アドレス変換 (NAT) を使用しない場合、構成は極めて単純なものとなります。

- ファイアウォールのポート 5544 および 5555 を開き、セントラル・システムおよびソース・システムが、エンドポイント・システムに接続できるようにします。
- ホスト・サーバー接続の許可に関する情報は、シナリオ 2 を参照してください。
- 同時に開始される各 BDT アプリケーションにそれぞれ 1 つのポートを割り振れるよう、十分なポートの範囲を各ターゲット・システムで指定してください。
- ファイアウォールでこの範囲のポートを開き、ソース/モデル・システムが、ターゲット・システムにデータを送信できるようにしてください。

静的 NAT を使用するファイアウォール

- NAT を使用していないファイアウォールに関する、上記の説明に従ってください。
- 必ず、ファイアウォール内部のマネージメント・セントラルにある各エンドポイント・システムが、セントラル・システムにあるエンドポイント・システムのリストに指定されている外部 IP アドレスを使用するようにしてください (これは、セントラル・システムが、どのエンドポイント・システムの内部 IP

アドレスに対しても接続できないためです)。または、検索頻度が常時に設定されている場合、必ず、セントラル・システムで、エンドポイント・システム名が、それらエンドポイント・システムの持つ外部 IP アドレスに解決されるようにしてください。

- 『マネージメント・セントラル接続』のセクションの説明に従って、各エンドポイント・システムで QYPS_HOSTNAME を設定してください。これを設定するには、以下のいずれかの方法を使用します。
  1. QYPS_HOSTNAME を、そのシステムの外部 IP アドレスに設定する。この場合、すべての MC システム (ファイアウォール内部にあるモデル・システムを含む) は、外部 IP アドレスを使用してセントラル・システムに接続することになります。
  2. QYPS_HOSTNAME の値に、外部システム (例えば CS) の場合はエンドポイント・システムの外部 IP アドレスに解決し、内部システムの場合はそのシステムの内部 IP アドレスに解決する、という特定のホスト名を設定する。

     注: QYPS_HOSTNAME を、(IP アドレスではなく) ホスト名に設定すると、Java (TM) インフラストラクチャーおよび拡張では正しく機能します。その場合、この QYPS_HOSTNAME 値は他のシステムに渡されて解決されます。ただし、QYPS_HOSTNAME に、IP アドレスではなくホスト名を設定しても、C++ 拡張 (大量データ転送) には影響しません。QYPS_HOSTNAME が、IP アドレスではなくホスト名に設定されている場合、各エンドポイント・システムの大量データ転送クライアントは、単にホスト名をリモート・システムに渡してリモート・システムで解決させる代わりに、最初にそのエンドポイント・システムにある DNS またはホスト・テーブルを使用して、この QYPS_HOSTNAME を IP アドレスに解決し、次にこの IP アドレスを渡します。結局、C++ インフラストラクチャーではこの QYPS_HOSTNAME 値を全く使用しないため、C++ インフラストラクチャーでの考慮事項は存在しません。

動的 NAT を使用するファイアウォール

エンドポイント・システムを保護しているファイアウォールが動的 NAT を使用している場合、セントラル・システムは、これらに接続することはできません。つまり、ファイアウォール外部のシステムはいずれも、エンドポイント・システムに対して接続を開始して、分散アプリケーションを使用することはできません。

Printed in Japan

日本アイ・ビー・エム株式会社
〒106-8711　東京都港区六本木3-2-12