System i

ネットワーキング
E-mail

バージョン 6 リリース 1

System i

ネットワーキング
E-mail

バージョン 6 リリース 1

ご注意

本書および本書で紹介する製品をご使用になる前に、 63 ページの『特記事項』に記載されている情報をお読みください。

本書は、IBM i5/OS (プロダクト番号 5761-SS1) バージョン 6、リリース 1、モディフィケーション 0 に適用されます。また、改訂版で特に断りがない限り、それ以降のすべてのリリースおよびモディフィケーションに適用されます。 このバージョンは、すべての RISC モデルで稼働するとは限りません。また CISC モデルでは稼働しません。

IBM 発行のマニュアルに関する情報のページ

`http://www.ibm.com/jp/manuals/`

こちらから、日本語版および英語版のオンライン・ライブラリーをご利用いただけます。また、マニュアルに関するご意見やご感想を、上記ページよりお送りください。今後の参考にさせていただきます。

(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： System i
Networking
E-mail
Version 6 Release 1

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 2008.2

目次

電子メール

この情報を利用して、ご使用のシステムでの電子メールの計画、構成、使用、管理、およびトラブルシューティングを行ってください。

この情報は、すでに i5/OS® オペレーティング・システムで作業した経験があり、TCP/IP、Simple Mail Transfer Protocol (SMTP)、および電子メールの概念について基本的な知識のある方を対象にしています。

V6R1 の新機能

電子メールのトピック・コレクションの新しい情報または大幅に改訂された情報は、次のとおりです。

SMTP S/MIME サポート

secure/Multipurpose Internet Mail Extensions (S/MIME) プロトコルは、Simple Mail Transfer Protocol (SMTP) 配信で複数のトランザクションがある場合に、電子メールの送信側を検査するために使用できます。このプロトコルを使用すると、電子メール文書の署名や、暗号化を行うことができます。新しい API である QtmsCreateSendEmail は、S/MIME サポートを提供します。

S/MIME の定義および、この新規 API を使用する際の構成ステップを紹介するシナリオについては、次のトピックを参照してください。

- 2 ページの『電子メールの概念』
- 8 ページの『シナリオ: S/MIME を使用するための QtmsCreateSendEmail API の構成』

SMTP 認証および SSL/TLS サポート

SMTP 認証を使用して、電子メールの発信元を追跡できるようになりました。また、i5/OS SMTP サーバーは、Secure Sockets Layer (SSL) または Transport Layer Security (TLS) のいずれかによって保護されるセッションをサポートします。

- 12 ページの『Simple Mail Transfer Protocol へのアクセスの制御』
- 30 ページの『電子メール送信者のトラッキング』

POP SSL/TLS サポート

i5/OS Post Office Protocol (POP) サーバーが、SSL/TLS セッションをサポートするようになりました。このサーバーで、ユーザー ID とパスワードを暗号化できます。

- 35 ページの『Post Office Protocol 電子メール・クライアントのセットアップ』

新機能または変更情報の確認方法

本書では、技術変更のあった箇所を見つけやすくするために、次の方法を採用しています。

- 新情報または変更情報の開始箇所に付ける » イメージ。
- 新情報または変更情報の終了箇所に付ける « イメージ。

PDF ファイルでは、新情報および変更情報の左マージンにリビジョン・バー (|) が付けられている場合があります。

| このリリースの新機能および変更情報に関するその他の情報については、『注記 (英語)』を参照してください。

「電子メール」の PDF ファイル

この情報の PDF ファイルを表示および印刷することができます。

この文書の PDF 版を表示またはダウンロードするには、「電子メール」を選択します。

PDF ファイルの保存

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

1. ご使用のブラウザーで PDF リンクを右クリックします。
2. ローカルに PDF を保存するオプションをクリックする。
3. PDF を保存したいディレクトリーに進む。
4. 「**保存**」をクリックする。

Adobe Reader のダウンロード

PDF を表示または印刷するには、システムに Adobe® Reader がシステムにインストールされている必要があります。 Adobe Reader は、Adobe の Web サイト (www.adobe.com/products/acrobat/readstep.html) から無償でダウンロードすることができます。

関連資料

60 ページの『電子メールの関連情報』

製品マニュアル、IBM® Redbooks® 資料、Web サイト、およびその他の Information Center のトピック・コレクションには、電子メール・トピック・コレクションに関連した情報が含まれています。PDF ファイルは、すべて表示または印刷できます。

電子メールの概念

電子メール (E-mail) は、必要不可欠なビジネス・ツールとなっています。i5/OS オペレーティング・システムでは、Simple Mail Transfer Protocol (SMTP) や Post Office Protocol (POP) などのプロトコルを使用し、電子メールがネットワーク上で円滑かつ効率的に行き来するようにします。

配信方式

次の追加の電子メールの概念では、その他の電子メールの配信方式について説明します。

- Multipurpose Internet Mail Extensions (MIME)

  MIME は、互いに異なるファイル・フォーマットを編成するための標準化された方式です。 SMTP は、行の最大長 1000 文字の 7 ビット ASCII テキストに限定されます。MIME は、リッチ・テキスト、イメージ、およびオーディオ・ファイルまたはビデオ・ファイルなどのより拡張されたファイル・タイプをサポートするために開発されました。MIME は、SMTP でメッセージを送信する前に、ヘッダーを使ってメッセージ内にあるさまざまなファイル・タイプを識別し、バイナリー形式データのファイルが単純な SMTP データに見えるようにエンコードします。次にメール・クライアントはこのメッセージを受信し、ファイルを読み取るために MIME ヘッダーを解釈することにより正しいファイル・タイプへとデコードします。

| - S/MIME

Secure/MIME は MIME プロトコルの機密保護機能のあるバージョンです。このプロトコルを使用すると、相手が異なるメール・プログラムを使用している場合にも、暗号化された電子署名付きのメール・メッセージを送信できます。

- AnyMail/400 フレームワーク

  SMTP から着信する、ローカル・ユーザー (このシステムにメール・アカウントを持つユーザー) 宛てのメールは、AnyMail/400 フレームワークによって処理されます。 メール・サーバー・フレームワークは、電子メールの配布を可能にするメール配布構造です。 特定のメール・タイプを処理する場合、メール・サーバー・フレームワークは出口プログラムまたはスナップインを呼び出します。

- ネットワーク体系配布サービス (SNADS)

  SNADS は、システムによるネットワーク (単数) 内での電子メールの受信、経路指定、および送信について定めた一連のルール群を定義した、IBM の非同期配布サービスです。 このトピック内では、SNADS とは、**優先アドレス**が**ユーザー ID/アドレス**にセットされているユーザーのプロファイルのことをいいます。 優先アドレスはメール・サーバー・フレームワークに、システム配布ディレクトリーの中のどのフィールドをアドレスとして使用すべきかを伝えます。

  関連概念

  35 ページの『電子メールの送受信』
  ご使用のシステムはメール・サーバーで、ここに電子メール・ユーザー (SNADS、POP、または Lotus® ユーザー) が登録されています。電子メール・ユーザーは、POP クライアントまたは SNADS クライアントのいずれかを使用して電子メールの送信、受信および読み取りを行うことができます。

  関連タスク

  14 ページの『システム・ネットワーク体系配布サービス待ち行列の保留』
  SMTP アプリケーションが電子メールの配布に使用する、システム・ネットワーク体系配布サービス (SNADS) 配布待ち行列を保留することができます。 そうすることで、電子メールの配布を制限する、追加の保護を提供します。

i5/OS での Simple Mail Transfer Protocol

Simple Mail Transfer Protocol (SMTP) は、オペレーティング・システムで電子メールを送受信できるようにするためのプロトコルです。

SMTP は、本質的には、1 つのメール・サーバーから別のメール・サーバーへと、メールの終端間送達を実行します。 SMTP 送信側 (クライアント) と宛先 SMTP 受信側 (サーバー) は、直接接続されます。SMTP クライアントは、SMTP 受信側 (サーバー) への送信とコピーが正常に実行されるまで、メールを送信側で保持しておきます。

このオペレーティング・システム上の SMTP は、メモ、メッセージ、および ASCII テキスト文書の配布をサポートします。 SMTP では、Multipurpose Internet Mail Extensions (MIME) プロトコルを使用することにより、プレーン・テキスト以外の形式もサポートできます。 MIME は、メール・メッセージの内容を記述したヘッダーを付けてメールを受信側クライアントに送信するための、インターネット標準です。 これらのメッセージには、ビデオ、音声、またはバイナリーの部分を含めることができます。

SMTP 電子メール配布について

電子メールを宛先に確実に届けるためには、SMTP は、電子メールを正しいホストと、そのホスト上にあるユーザー ID に配布できなければなりません。 メールが bobsmith@mycompany.com に送信されるとします。

まず、SMTP は、電子メールの宛先 (bobsmith) がローカル・サーバーのユーザーかどうかを検査します。ローカル・システムのユーザーでないと判断した場合、SMTP はこの電子メールを次のホスティング・サーバーに転送します。 次のホストが最終ホストであるかどうかは分かりません。 SMTP は、SMTP プロトコルで見つかったアドレス情報からホスト名を判別します。

それから SMTP は、ドメイン・ネーム・システム (DNS) サーバーまたはローカル・ホスト・テーブルのいずれかを使用して、そのホストのアドレスを解決します。ホスト名は、電子メール・アカウントの一部として使用するものです (ここでは、mycompany.com)。IP アドレスは、SMTP がメールの送信先となる正しいメール・サーバーを検出するのに使用するものです (ここでは、192.1.1.10)。

1. SMTP サーバーがローカル・ホスト・テーブルでホスト名アドレスを検索するときは、IPv6 アドレスは無視されます。
2. 構成済みのいずれかの DNS サーバーに IPv6 アドレスがある場合は、構成済みのすべての DNS サーバーが、構成済みサーバーが権限を持っていない電子メール・ドメイン解決のための再帰をサポートする必要があります。

以下のトピックでは、DNS を SMTP と関連付けて説明しています。

- DNS ドメインのセットアップ
- メールおよびメール交換 (MX) レコード

着信電子メールの場合、SMTP サーバーはまずその宛先ホスト名をインターネット・プロトコル (IP) アドレスに変換します。 別名割り当て機能のために、サーバーが複数のホスト名を持つことがありえます。 したがって、SMTP サーバーはソケット・インターフェースを使用して、その IP アドレスがローカル・ホストのインターフェースによって使用されているものの 1 つであるかどうかを判別します。

関連概念

DNS

メールおよびメール・エクスチェンジャー・レコード

関連タスク

DNS ドメインのセットアップ

16 ページの『電子メールの構成』
ご使用のシステムで電子メールをセットアップするには、TCP/IP を構成し、Simple Mail Transfer Protocol (SMTP) および Post Office Protocol (POP) サーバーをセットアップし、電子メール・サーバーを開始する必要があります。

i5/OS での Post Office Protocol

Post Office Protocol (POP) サーバーは、i5/OS における Post Office Protocol バージョン 3 メール・インターフェースのインプリメンテーションです。

POP サーバーは、クライアントがメールを取り出せる電子メールボックスを、このオペレーティング・システム上に提供します。Netscape Mail、Outlook Express、または Eudora など、POP3 プロトコルをサポートするメール・クライアントであれば、このサーバーを使用することができます。クライアントは、Windows®、Linux®、AIX®、または Macintosh など任意のプラットフォームで実行できます。

POP サーバーは、メール・クライアントがメールを取り出すまでの間、メールの一時的な保持区域として機能します。メール・クライアントは、サーバーに接続すると、そのメールボックスの内容を照会して、取り出せるメールがないか調べます。メールがある場合、メール・メッセージを 1 度に 1 つずつ取り出します。メッセージが 1 つ取り出された後、クライアントはサーバーに対し、クライアント・セッションが完了するときにそのメッセージに削除マークを付けるよう指示します。 クライアントは、メールボックス内

のメッセージをすべて取り出されると、コマンドを発行し、サーバーに対して、削除マークの付いたメッセージをすべて削除し、クライアントを切断するように指示します。

POP メール・クライアントは、*verbs* を使って POP サーバーと通信します。このオペレーティング・システムで POP サーバーによってサポートされる verb については、『Post Office Protocol』トピックに記載されています。

関連タスク

16 ページの『System i ナビゲーターを使用した電子メール・サーバーへのアクセス』
System i™ ナビゲーターを使用して、Simple Mail Transfer Protocol (SMTP) および Post Office Protocol (POP) 電子メール・サーバーを構成および管理することができます。

17 ページの『電子メールのための Simple Mail Transfer Protocol サーバーおよび Post Office Protocol サーバーの構成』
電子メールを使用するには、ご使用のシステム上で Simple Mail Transfer Protocol (SMTP) サーバーおよび Post Office Protocol (POP) サーバーを構成する必要があります。

関連資料

55 ページの『Post Office Protocol』
Post Office Protocol (POP) バージョン 3 のメール・インターフェースは、Request for Comments (RFC) 1939 (POP3)、RFC 2449 (POP3 拡張機能メカニズム)、および RFC 2595 (IMAP、POP3、および ACAP との TLS の使用) で定義されています。RFC は、進化していくインターネット標準を定義するために使用されるメカニズムです。

関連情報

RFC Index

シナリオ: 電子メール

次のシナリオでは、ローカル・ユーザー同士の電子メールに対する処理動作、および S/MIME を使用する場合の QtmsCreateSendEmail API の構成方法を例示します。

シナリオ: ローカルでの電子メールの送受信

このシナリオでは、ローカル・ユーザー間で電子メールがどのように処理されるかを例示します。

状態

人事部長の Jane Smith は、法務部門の Sam Jones にメッセージを送信する必要があります。二人とも MyCompany 社の本社で働いています。このプロセスに従うことにより、システムで電子メールがどのように処理されるかを知ることができます。

この例の目的は次のとおりです。

- 電子メール・クライアントと電子メール・サーバーが互いにどのように関係するか、およびメッセージがどう処理されるかを示す。
- SMTP サーバーを使用してメールを送信する。
- メールを POP ユーザーに送達する。

詳細

Jane は Netscape メール・クライアントを使用しています。メッセージを書き、SamJones@mycompany.com に送信します。次の図では、ネットワーク内のメール・メッセージの進路を示します。

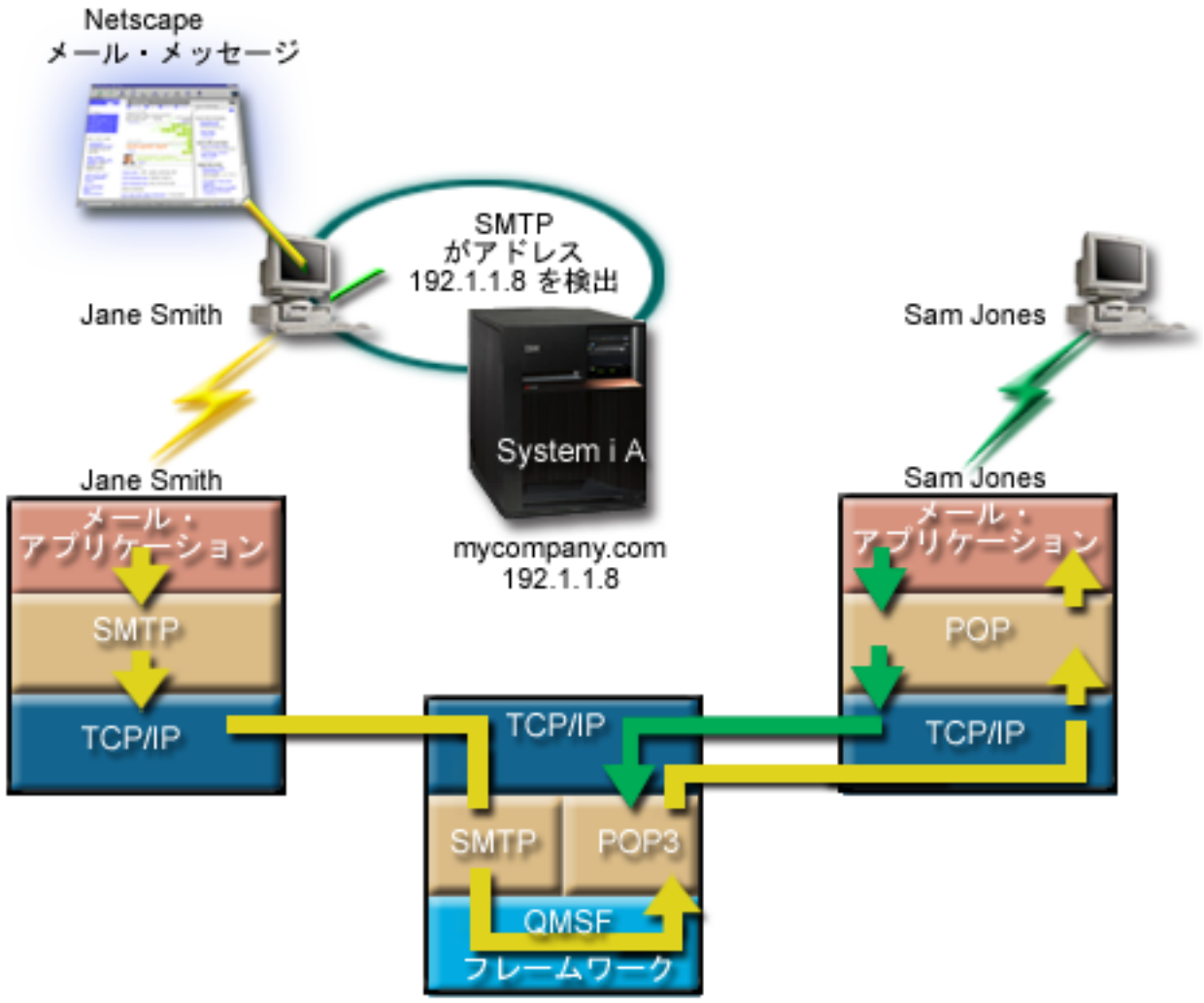

図 1. ネットワーク構成の例

次のテキストは、メール・メッセージのネットワーク内の進路の各フェーズを説明しています。

フェーズ 1: SMTP クライアントから SMTP サーバーまで

Jane の PC 上の SMTP クライアントは、発信サーバーおよび ID として入力された構成データを使用します。ID フィールドは「**送信元** 」アドレスに使用されます。発信サーバーとは、PC SMTP クライアントがコンタクトするホストのことです。このアドレスはドメインとして入力されるため、SMTP クライアントはドメイン・ネーム・システム (DNS) を照会して SMTP サーバーの IP アドレスを入手し、それが 192.1.1.8 であることが分かります。

SMTP クライアントは、これで SMTP ポート (192.1.1.8 のポート 25) 上の SMTP サーバーにコンタクトします。 クライアントとサーバー間で使用されるダイアログは、SMTP プロトコルです。SMTP サーバー

はメールの送達を受け入れ、メッセージはクライアントからサーバーへと TCP/IP を使用して伝送されます。

フェーズ 2: SMTP サーバーはメッセージを POP サーバーに送達する

SMTP サーバーは、宛先がローカルであるかどうかを知るために宛先のドメインを検査します。宛先がローカルであるため、メールは Integrated File System ファイルへ書き込まれ、QMSF フレームワーク作成メッセージのアプリケーション・プログラミング・インターフェース (API) が使用されてメッセージ情報が QMSF 待ち行列に入れられます。QMSF フレームワークは、特定のメール・タイプを処理するために出口プログラムまたはスナップインを呼び出して、電子メールの配布が行えるようにします。メッセージ情報は Sam のアドレスを SMTP 形式で示しているため、フレームワークは SMTP アドレス解決出口プログラムを呼び出します。このプログラムは、メッセージがローカルであることを再度検査し、メッセージがローカルであるため、システム配布ディレクトリー (WRKDIRE を介して入力されたデータ) を使用して宛先の SMTP アドレスを検索します。Sam のアドレスを発見し、メールのサービス・レベルがシステム・メッセージ保管であることをこのユーザーのディレクトリー項目で検出し、したがって、それを POP アカウントとして認識します。 その後 SMTP アドレス解決は、Sam のプロファイル情報をメッセージ情報に追加し、その情報を POP ローカル送達としてマークします。それから QMSF フレームワークは、POP ローカル送達出口プログラムを呼び出し、この出口プログラムがプロファイル情報および Integrated File System ファイルを検索して、メールを Sam のメールボックスに送達します。

フェーズ 3: POP クライアントが Sam Jones 宛てのメッセージを POP サーバーから取り出す

Sam は自分のメールボックスにある電子メールをチェックするために、メール・クライアント (Netscape) を使用することにします。Sam の PC 上の POP クライアントは、mycompany.com にある POP サーバーで、ユーザー名 SamJones とパスワード (******) を使用するよう構成されています。ドメイン名は、IP アドレスへと再度変換されます (DNS を使用して)。POP クライアントは POP サーバーに、POP ポートおよび POP3 プロトコルを使用してコンタクトします。オペレーティング・システム上の POP サーバーは、メールボックスのユーザー名とパスワードが i5/OS ユーザーのプロファイルとパスワードと一致しているかどうか検査します。妥当性検査が行われた後、そのプロファイル名は Sam のメールボックスを検索するために使用されます。POP クライアントはメッセージをロードし、POP サーバーに対してこのメールを POP メールボックスから削除する要求を送信します。これでメッセージは Netscape に表示され、Sam は読むことができます。

関連概念

11 ページの『電子メールの計画』
電子メールをセットアップする前に、ご使用のシステムで電子メールをどのように使用するか、 基本的な計画を立てておく必要があります。

関連資料

53 ページの『Simple Mail Transfer Protocol』
Simple Mail Transfer Protocol (SMTP) は、電子メールの送受信に使用される TCP/IP プロトコルです。通常は POP3 または Internet Message Access Protocol とともに、サーバー・メールボックスへのメッセージの保管、およびユーザーへのメッセージのサーバーからの定期的なダウンロードに使用されます。

55 ページの『Post Office Protocol』
Post Office Protocol (POP) バージョン 3 のメール・インターフェースは、Request for Comments (RFC) 1939 (POP3)、RFC 2449 (POP3 拡張機能メカニズム)、および RFC 2595 (IMAP、POP3、および ACAP との TLS の使用) で定義されています。RFC は、進化していくインターネット標準を定義するために使用されるメカニズムです。

シナリオ: S/MIME を使用するための QtmsCreateSendEmail API の構成

このシナリオでは、secure/MIME (S/MIME) を使用するように QtmsCreateSendEmail API を構成する方法を例示します。

状態

ユーザー ID jsmith を持つユーザー John Smith が、S/MIME を使用するように QtmsCreateSendEmail API を構成しようとしています。S/MIME は、プログラム経由で電子メールを送信する手段として QtmmSendMail API よりも安全です。

詳細

署名付きの暗号化された電子メールを送信するために、John は、i5/OS V6R1 が稼動している彼のシステムに次のオプションをインストールしておく必要があります。

- i5/OS PASE (5761-SS1 オプション 33)
- デジタル証明書マネージャー (5761-SS1 オプション 34)
- OpenSSL (5733-SC1 オプション 1)

ユーザー証明書ストアの作成

S/MIME を使用するには、ユーザー証明書ストアと呼ばれる、ユーザー証明書のリポジトリーが必要となります。オペレーティング・システムでは、ユーザーの証明書には命名規則 *userid*.usrcrt が使用されます。証明書は、/qibm/userdata/icss/cert/download/client ディレクトリーにあります。

John は、メール・メッセージの作成および送信ジョブに使用する自分のユーザー・プロファイルに対して、ユーザー証明書ストアをセットアップする必要があります。ユーザー証明書ストアの管理には、デジタル証明書マネージャー (DCM) を使用できます。

ユーザー証明書ストアを作成するには、次のステップを実行してください。

1. 次のようにユーザー・プロファイルの名前を使用して、サブディレクトリーを作成します。

   ```
   cd /qibm/userdata/icss/cert/download/client
   mkdir jsmith
   ```

2. Web ブラウザーを使用して、ご使用のシステムの「System i タスク (System i Tasks)」ページ http://*your_system_name*: 2001 に移動します。
3. 「System i タスク (System i Tasks)」ページの製品リストから「**デジタル証明書マネージャー**」を選択して、DCM ユーザー・インターフェースにアクセスします。左側ペインで、「**新規の証明書ストアの作成**」をクリックします。
4. 「新規の証明書ストアの作成」ページで、「**その他のシステム証明書ストア (Other System Certificate Store)**」を選択し、「**続行**」をクリックします。
5. 新規証明書ストアでの証明書の作成」ページで、「**証明書ストアに証明書を作成しません** 」を選択します。
6. 「証明書ストア名およびパスワード」ページで、証明書ストアのパス名とパスワードを設定します。ご使用のユーザー ID を含む証明書ストアのパスを設定します。例えば、John の場合は、ストア・パスを /qibm/userdata/icss/cert/download/client/jsmith/jsmith.kdb と設定します。

送信側のユーザー証明書の System i へのエクスポート

John の Web ブラウザーは、Internet Explorer (IE) 6 です。送信側のユーザー証明書は、認証局 (CA) から取得され、IE 6 にインストールされています。

送信側のユーザー証明書を System i プラットフォームにエクスポートするために、John は次の手順に従います。

1. IE のウィンドウで、「**ツール**」 → 「**インターネット オプション**」を選択します。
2. 「**コンテンツ**」タブで、「**証明書**」をクリックします。
3. 「**個人**」タブで、送信側の証明書を選択し、「**エクスポート**」をクリックします。
4. 「証明書のエクスポート ウィザード」ページで、「**次へ**」をクリックします。
5. 「秘密キーのエクスポート」ページで、「**はい、秘密キーをエクスポートします**」を選択し、「**次へ**」をクリックします。
6. 「エクスポート ファイルの形式」ページで、「**Personal Information Exchange - PKCS #12 (.PFX)**」の下の「**強力な保護を有効にする (IE 5.0、NT 4.0 SP4 またはそれ以上が必要)**」を選択します。
7. 「パスワード」ページで、証明書のパスワードを入力します。
8. 「エクスポートするファイル」ページで、エクスポートするファイルの名前 (例: C:¥temp¥jsmithcert.pfx) を指定し、「**次へ**」をクリックします。
9. 「証明書のエクスポート ウィザードの完了」ページで、「**完了**」をクリックします。
10. FTP を使用して、送信側のユーザー証明書 jsmithcert.pfx を、System i プラットフォームに ASCII モードで送信します。この例では、このファイルは、System i Integrated File System のディレクトリー /home/jsmith に送信されるものとします。この証明書のインポートについて詳しくは、 10 ページの『送信側証明書の System i へのインポート』を参照してください。

宛先のユーザー証明書の System i へのエクスポート

John の場合、宛先の証明書を System i プラットフォームにエクスポートするために、次のステップを実行します。

1. IE のウィンドウで、「**ツール**」 → 「**インターネット オプション**」を選択します。
2. 「インターネット オプション」で「**コンテンツ**」タブをクリックし、「**証明書**」をクリックします。
3. 「インターネット オプション」ページの「**個人**」タブで、証明書を選択し、「**エクスポート**」をクリックします。

   複数の証明書が存在する場合は、すべての証明書に対し、ステップ 3 から 7 を繰り返す必要があります。
4. 「証明書のエクスポート ウィザード」ページで、「**次へ**」をクリックします。
5. 「エクスポート ファイルの形式」ページで、「**DER encoded binary X.509 (.CER)**」を選択します。
6. 「エクスポートするファイル」ページで、エクスポートするファイルの名前 (例: C:¥temp¥receiveruser.cer) を指定し、「**次へ**」をクリックします。
7. 「証明書のエクスポート ウィザードの完了」ページで、「**完了**」をクリックします。
8. FTP を使用して、宛先のユーザー証明書 receiver.cet を、System i プラットフォームに ASCII モードで送信します。この例では、このファイルは、System i Integrated File System のディレクトリー /home/jsmith に送信されるものとします。宛先証明書のインポート方法については、 10 ページの『宛先の証明書の System i へのインポート』を参照してください。
9. S/MIME で使用する宛先ごとに、上記すべてのステップを繰り返してください。

送信側証明書の System i へのインポート

次に、John は、DCM を使用して、ユーザー証明書と秘密鍵をユーザー証明書ストアにインポートする必要があります。インポートされる証明書のパスワードは、鍵ストアのパスワードと同じでなければなりません。また、John は電子メールの送信先となるユーザーの証明書をすべてインポートする必要があります。

1. Web ブラウザーを使用して、ご使用のシステムの「System i タスク (System i Tasks)」ページ http://*your_system_name*: 2001 に移動します。
2. 「System i タスク (System i Tasks)」ページの製品リストから「**デジタル証明書マネージャー**」を選択して、DCM ユーザー・インターフェースにアクセスします。
3. 「証明書ストアの選択」ページで、「**その他のシステム証明書ストア (Other System Certificate Store)**」を選択し、「**続行**」をクリックします。
4. 「証明書ストア名およびパスワード」ページで、証明書ストアのパスとファイル名、およびパスワードを入力し、「**続行**」をクリックします。John の場合、ファイル名は /qibm/userdata/icss/cert/download/client/jsmith/jsmith.kdb になります。
5. 「**証明書の管理**」 → 「**証明書のインポート**」を展開します。「**サーバーまたはクライアント**」を選択して、送信側の証明書をインポートします。「**続行**」をクリックします。
6. 「サーバーまたはクライアント証明書のインポート (Import Server or Client Certificate)」ページで、送信側の証明書の Integrated File System ディレクトリーおよびファイル名を入力し、「**続行**」をクリックします。 9 ページの『送信側のユーザー証明書の System i へのエクスポート』 では、Integrated File System ディレクトリーおよびファイルは、/home/jsmith/ jsmithcert.pfx です。
7. 証明書ラベル、つまり、送信側の電子メール・アドレスを小文字で指定します。「**続行**」をクリックします。
8. 「**OK**」をクリックします。

宛先の証明書の System i へのインポート

宛先の証明書を System i プラットフォームにインポートするには、次のステップに従ってください。

1. Web ブラウザーを使用して、ご使用のシステムの「System i タスク (System i Tasks)」ページ http://*your_system_name*: 2001 に移動します。
2. 「System i タスク (System i Tasks)」ページの製品リストから「**デジタル証明書マネージャー**」を選択して、DCM ユーザー・インターフェースにアクセスします。
3. 「証明書ストアの選択」ページで、「**その他のシステム証明書ストア (Other System Certificate Store)**」を選択し、「**続行**」をクリックします。
4. 「証明書ストア名およびパスワード」ページで、証明書ストアのパスとファイル名、およびパスワードを入力し、「**続行**」をクリックします。John の場合、ファイル名は /qibm/userdata/icss/cert/download/client/jsmith/jsmith.kdb になります。
5. 「**証明書の管理**」 → 「**証明書のインポート**」を展開します。「**認証局 (CA)**」を選択し、宛先の証明書をインポートします。「**続行**」をクリックします。
6. 「認証局 (CA) 証明書のインポート」ページで、宛先の証明書の Integrated File System ディレクトリーおよびファイル名を入力し、「**続行**」をクリックします。 9 ページの『宛先のユーザー証明書の System i へのエクスポート』 では、宛先の Integrated File System ディレクトリーおよびファイルは、/home/jsmith/receiveruser.cer です。
7. CA 証明書ラベル、つまり、宛先の電子メール・アドレスを小文字で指定します。「**続行**」をクリックします。
8. 送信側が使用する必要のある宛先の証明書ごとに、上記のすべてのステップを繰り返してください。

| **関連概念**
| デジタル証明書マネージャー
| **関連資料**
| API または MIME メールの作成および送信 (QtmsCreateSendEmail) API

電子メールの計画

電子メールをセットアップする前に、ご使用のシステムで電子メールをどのように使用するか、基本的な計画を立てておく必要があります。

電子メールのセットアップを開始する前に、以下の質問に答えてください。

1. 自分の電子メール・アドレスはどのようになるか ?
2. ドメイン・ネーム・サーバー (DNS) の IP アドレスは ?
3. ファイアウォールはあるか ? 答えが「はい」の場合、IP アドレスは ?
4. メール・プロキシー、メール・ルーター、またはメール中継はあるか ? 答えが「はい」の場合、IP アドレスは ?
5. Domino® データベースを使用しようとしているか ?
6. メール受信に i5/OS POP サーバーを使用しようとしているか ?

電子メールの動作についての基本情報を 電子メールのシナリオで参照することができます。

Domino サーバーおよび i5/OS SMTP サーバーを使用する場合は、『同一システム上で Domino と SMTP サーバーをホストする』トピックを参照してください。 Domino の詳細については、『Domino』トピック、または Lotus Domino for i5/OS の Web サイトを参照してください。

SMTP サーバーまたは POP サーバーを使用する予定がない場合は、ユーザーが知らずにこれらを使用することがないよう使用不可にしてください。

関連概念

5 ページの『シナリオ: ローカルでの電子メールの送受信』
このシナリオでは、ローカル・ユーザー間で電子メールがどのように処理されるかを例示します。

Domino

関連タスク

16 ページの『電子メールの構成』
ご使用のシステムで電子メールをセットアップするには、TCP/IP を構成し、Simple Mail Transfer Protocol (SMTP) および Post Office Protocol (POP) サーバーをセットアップし、電子メール・サーバーを開始する必要があります。

44 ページの『同一システム上で Domino と SMTP サーバーをホストする』
Domino と Simple Mail Transfer Protocol (SMTP) が同一システム上で稼動している場合は、それぞれを特定の IP アドレスにバインドするように構成することをお勧めします。

関連情報

Lotus Domino for i5/OS

電子メールへのアクセスの制御

電子メールを通じて誰がシステムにアクセスするかを制御して、悪意のある攻撃からデータを保護する必要があります。

このセクションでは、電子メール・サーバーをフラッディングやスパミングから守るためのヒントを紹介します。

関連概念

独立ディスク・プールの使用

55 ページの『電子メールの問題判別』
簡単な手順で、電子メールの問題の原因を判別することができます。

関連タスク

31 ページの『メッセージ中継の制限』
電子メール・サーバーがスパミングまたはバルク・メールの大量送信に使用されるのを防ぐために、中継制限機能を使用します。 この機能で、メッセージ中継の目的でご使用のシステムを使用できるユーザーを指定できます。 ただし、メッセージの中継を制限する場合は、電子メールを認証することはできません。

34 ページの『接続制限』
システムの安全を確保するには、電子メール・サーバーを悪用する可能性のあるユーザーからの接続を防ぐ必要があります。

関連情報

AS/400 インターネット・セキュリティー: インターネットの HARM から AS/400 を保護する (AS/400 Internet Security: Protecting Your AS/400 from HARM in the Internet)

Simple Mail Transfer Protocol へのアクセスの制御

システムへの悪意のある攻撃または非送信請求メール (スパム) を防ぐには、Simple Mail Transfer Protocol (SMTP) へのアクセスを制御する必要があります。

SMTP クライアントからご使用のシステムへのアクセスを許可する場合は、次のタスクを実行して、システムをアタックから保護する必要があります。

- 可能であれば、システム配布ディレクトリーの *ANY *ANY 項目の使用は避ける。システムに *ANY *ANY 項目がなければ、何者かが SMTP を使用してユーザーのシステムまたはネットワークに過負荷を発生させることが、より難しくなります。ご使用のシステムを介して別のシステムへと転送されている迷惑メールで補助記憶域がいっぱいになったときに、ご使用のシステムまたはネットワークに過負荷が発生します。
- 補助記憶域プール (ASP) に適切なしきい値を設定して、望ましくないオブジェクトによりシステムに過負荷が発生するのを回避する。システム・サービス・ツール (SST) か専用保守ツール (DST) かどちらかを使用して、ASP のしきい値を表示したり設定することができます。
- 事前開始ジョブ項目の変更 (CHGPJE) コマンドを使用することにより作成される事前開始ジョブの最大数を調整する。これは、サービス妨害アタックの際に作成されるジョブの数を制限することになります。 デフォルトは、しきい値の最大である 256 です。
- リレーおよび接続を制約することによって、ご使用の接続を外部者が使用して非送信請求電子メール (スパム) を送信することを防ぎます。
- i5/OS V6R1 が稼動しているシステム上では、電子メールの送信で認証を必須にすることにより、スパムを回避できます。リモート・サーバーに認証が必要な場合は、ローカル・サーバーで認証をセットアップできます。

関連資料

SMTP 属性の変更 (CHGSMTPA)

Post Office Protocol へのアクセスの制御

システムの安全を確保するには、Post Office Protocol (POP) へのアクセスを制御する必要があります。

ユーザー ID やパスワードなどの POP データ・ストリームを保護するために、POP サーバーで暗号化を使用するかどうかを指定できます。Secure Sockets Layer (SSL) または Transport Layer Security (TLS) により、暗号化が提供されます。セキュア POP セッションがサポートされるかどうかを指定するには、POP サーバー属性の変更 (CHGPOPA) CL コマンドで ALWSSL パラメーターを設定します。

ご使用のシステムを POP クライアントにアクセスさせたい場合は、下記のセキュリティー上の考慮事項に注意します。

- POP メール・サーバーは、自分のメールボックスにアクセスしようとするクライアントに認証を提供します。 クライアントは、ユーザー ID とパスワードをサーバーに送信します。

  POP メール・サーバーは、送信されたユーザー ID とパスワードを、そのユーザーの i5/OS ユーザー・プロファイルとパスワードと照合して検証します。 POP クライアント上でユーザー ID とパスワードが保管される方法についてはユーザーは制御しないので、権限が制限された特別なユーザー・プロファイルをシステム上に作成したほうがよい場合もあります。 いかなる者もこのユーザー・プロファイルを対話式セッションで使用できないようにするために、そのユーザー・プロファイルに以下の値を設定することができます。
  初期メニュー (INLMNU) を *SIGNOFF に設定する
  初期プログラム (INLPGM) を *NONE に設定する
  機能制限 (LMTCPB) を *YES に設定する
- 悪意のある侵入者が望ましくないオブジェクトでシステムに負荷を発生させることを防ぐために、必ずユーザーの補助記憶域プール (ASP) に適切なしきい値を設定する。ASP 記憶域しきい値により、オペレーティング・システムに十分なワークスペースがないことによるシステムの停止を防ぐことができます。 システム・サービス・ツール (SST) か専用保守ツール (DST) かどちらかを使用して、ASP のしきい値を表示したり設定することができます。
- ASP しきい値を使って、システムがフラッディングされないようにすることが必要である一方で、メールを正しく保管し送達するために適切なスペースをシステムが保有していることも必ず確認する必要もあります。 システムに一時メール用の適切な記憶域がないためにメール・サーバーがメールを送達できない場合、これはユーザーの保全性にかかわる問題です。 システム記憶域の使用率が高い場合、メールは実行を停止します。

  通常は、ストレージ・スペースは重要な問題ではありません。 クライアントがメールを受信すると、メール・サーバーはそのメールをシステムから削除します。

関連概念

55 ページの『電子メールの問題判別』
簡単な手順で、電子メールの問題の原因を判別することができます。

電子メールへのアクセスの防止

システムの使用方法によっては、ユーザーが SMTP サーバーおよび POP サーバーを通じて電子メールにアクセスしないようにする場合があります。電子メールへのアクセスをすべて不可にするか、場合によってアクセスを許可することができます。

Simple Mail Transfer Protocol アクセスの防止

いかなる者にも、ご使用のシステムとの間でのメール配布のやりとりに Simple Mail Transfer Protocol (SMTP) を使用させたくない場合は、SMTP サーバーを稼働できなくする必要があります。

SMTP は、デフォルトでは、TCP/IP が開始されると自動的に開始するように構成されます。SMTP をまったく使用しない予定である場合は、システム上で SMTP を構成すべきではありません (あるいはいかなる他者にも SMTP を構成させるべきではありません)。

TCP/IP の開始時に Simple Mail Transfer Protocol を開始させない:

たまには Simple Mail Transfer Protocol (SMTP) を使う必要もあるものの、SMTP サーバーへのユーザー・アクセス数を制限したい場合。

TCP/IP を開始する時に SMTP サーバーが自動的に開始しないようにするには、次のステップに従ってください。

1. System i ナビゲーターで、「**ユーザーのシステム**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」と展開します。
2. 「**SMTP**」を右ボタンでクリックし、「**プロパティー**」を選択します。
3. 「**TCP/IP の開始時に開始**」を選択解除します。

Simple Mail Transfer Protocol ポートへのアクセスの防止:

未知のアプリケーションから Simple Mail Transfer Protocol (SMTP) サーバーを保護するために、SMTP ポートへのアクセスを防止することができます。

SMTP へのアクセスを開始させないようにし、何者かがユーザー・アプリケーション (ソケット・アプリケーションなど) をシステムが通常 SMTP 用として使用するポートに関連付けないようにするために、以下のステップを実行します。

1. System i ナビゲーターで、「**ユーザーのシステム**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」と展開します。
2. 「**TCP/IP 構成**」を右クリックして「**プロパティー**」を選択します。
3. 「TCP/IP 構成プロパティー」ウィンドウで「**ポート制限**」タブをクリックします。
4. 「ポート制限」ページで「**追加**」をクリックします。
5. 「ポート制限の追加」ページで、以下の設定を指定します。
   - 「**ユーザー名**」: システム上で保護するユーザー・プロファイル名を指定します。 (保護されるユーザー・プロファイルとは、権限を与えられたプログラムを所有しておらず、他のユーザーに知られているパスワードを持たないユーザー・プロファイルのことです。) ポートを特定のユーザーに制限することにより、自動的に他のすべてのユーザーを除外することができます。
   - 「**開始ポート**」: 25
   - 「**終了ポート**」: 25
   - 「**プロトコル**」: TCP
6. 「**OK**」をクリックして、制限を追加します。
7. 「**ポート制限**」ページで「**追加**」をクリックし、UDP についても同じ手順を繰り返します。
8. 「**OK**」をクリックしてポート制限を保管し、「**TCP/IP 構成プロパティー**」 ウィンドウをクローズします。 ポート制限は、次回 TCP/IP を開始した時点で有効になります。ポート制限を設定した時点で TCP/IP がアクティブである場合は、TCP/IP を終了させてもう一度開始する必要があります。

システム・ネットワーク体系配布サービス待ち行列の保留:

SMTP アプリケーションが電子メールの配布に使用する、システム・ネットワーク体系配布サービス (SNADS) 配布待ち行列を保留することができます。そうすることで、電子メールの配布を制限する、追加の保護を提供します。

配布待ち行列を保留するには、文字ベースのインターフェースに以下のコマンドを入力します。

```
HLDDSTQ  DSTQ(QSMTPQ)PTY(*NORMAL)
HLDDSTQ  DSTQ(QSMTPQ)PTY(*HIGH)
```

関連概念

2 ページの『電子メールの概念』
電子メール (E-mail) は、必要不可欠なビジネス・ツールとなっています。i5/OS オペレーティング・システムでは、Simple Mail Transfer Protocol (SMTP) や Post Office Protocol (POP) などのプロトコルを使用し、電子メールがネットワーク上で円滑かつ効率的に行き来するようにします。

Post Office Protocol アクセスの防止

いかなる者にも Post Office Protocol (POP) を使用してシステムへアクセスさせたくない場合、POP サーバーを稼働できなくする必要があります。

POP をまったく使用しない予定である場合は、システム上で SMTP を構成すべきではありません (あるいはいかなる他者にも SMTP を構成させるべきではありません)。

TCP/IP の開始時に Post Office Protocol を開始させない:

時折 Post Office Protocol (POP) を使う必要があるが、ユーザーの POP サーバーへのアクセス回数を制限したい場合。

POP サーバーは、デフォルトでは、TCP/IP が開始されると自動的に開始するように構成されます。TCP/IP を開始する時に POP サーバーが自動的に開始しないようにするには、次のステップに従ってください。

1. System i ナビゲーターで、「**ユーザーのシステム**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」と展開します。
2. 「**POP**」を右ボタンでクリックし、「**プロパティー**」を選択します。
3. 「**TCP/IP の開始時に開始**」を選択解除します。

Post Office Protocol ポートへのアクセスの防止:

未知のアプリケーションから Post Office Protocol (POP) サーバーを保護するために、POP ポートへのアクセスを防止することができます。

POP サーバーを開始させないようにし、何者かがユーザー・アプリケーション (ソケット・アプリケーションなど) をシステムが通常 POP 用として使用するポートに関連付けないようにするために、以下のステップを実行します。

1. System i ナビゲーターでシステムに接続し、「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」の順に展開します。
2. 「**TCP/IP 構成**」を右クリックして「**プロパティー**」を選択します。
3. 「TCP/IP 構成プロパティー」ウィンドウで「**ポート制限**」タブをクリックします。
4. 「ポート制限」ページで「**追加**」をクリックします。
5. 「ポート制限の追加」ページで、以下の設定を指定します。

- 「**ユーザー名**」: システム上で保護するユーザー・プロファイル名を指定します。 (保護されるユーザー・プロファイルとは、権限を与えられたプログラムを所有しておらず、他のユーザーに知られているパスワードを持たないユーザー・プロファイルのことです。) ポートを特定のユーザーに制限することにより、自動的に他のすべてのユーザーを除外することができます。
- 「**開始ポート**」: 110 995
- 「**終了ポート**」: 110 995
- 「**プロトコル**」: TCP

6. 「**OK**」をクリックして、制限を追加します。
7. 「ポート制限」ページで「**追加**」をクリックし、UDP についても同じ手順を繰り返します。
8. 「**OK**」をクリックしてポート制限を保管し、「TCP/IP 構成プロパティー」 ウィンドウをクローズします。

ポート制限は、次回 TCP/IP を開始した時点で有効になります。ポート制限を設定した時点で TCP/IP がアクティブである場合は、TCP/IP を終了させてもう一度開始する必要があります。

電子メールの構成

ご使用のシステムで電子メールをセットアップするには、TCP/IP を構成し、Simple Mail Transfer Protocol (SMTP) および Post Office Protocol (POP) サーバーをセットアップし、電子メール・サーバーを開始する必要があります。

関連概念

3 ページの『i5/OS での Simple Mail Transfer Protocol』
Simple Mail Transfer Protocol (SMTP) は、オペレーティング・システムで電子メールを送受信できるようにするためのプロトコルです。

11 ページの『電子メールの計画』
電子メールをセットアップする前に、ご使用のシステムで電子メールをどのように使用するか、 基本的な計画を立てておく必要があります。

System i ナビゲーターを使用した電子メール・サーバーへのアクセス

System i ナビゲーターを使用して、Simple Mail Transfer Protocol (SMTP) および Post Office Protocol (POP) 電子メール・サーバーを構成および管理することができます。

System i ナビゲーターで POP または SMTP にアクセスするには、次のステップに従います。

1. 「**クライアント・アクセス Windows エクスプレス版**」フォルダーをダブルクリックします。
2. **System i ナビゲーター**をダブルクリックします。初めて System i ナビゲーターを使用する場合は、「**新規接続**」アイコンをクリックして、ご使用のシステムとの接続を確立します。
3. System i ナビゲーターで、「**ユーザーのシステム**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」と展開します。
4. 「**SMTP**」をダブルクリックして「SMTP プロパティー」ダイアログを開くか、あるいは「**POP**」をダブルクリックして「POP プロパティー」ダイアログを開きます。

関連概念

4 ページの『i5/OS での Post Office Protocol』
Post Office Protocol (POP) サーバーは、i5/OS における Post Office Protocol バージョン 3 メール・インターフェースのインプリメンテーションです。

電子メールのための TCP/IP の構成

ご使用のシステム上で電子メールを構成するには、事前に TCP/IP をセットアップする必要があります。

ご使用のシステムでの電子メールの設定が初めての場合には、以下のステップを実行してください。 ご使用のシステム上で既に TCP/IP が構成されている場合は、電子メール用の Simple Mail Transfer Protocol (SMTP) および Post Office Protocol (POP) サーバーの構成に直接進んでください。

1. System i ナビゲーターで、「**ユーザーのシステム**」 → 「**ネットワーク**」 → 「**TCP/IP 構成**」の順に展開します。
2. 「**インターフェース**」を右ボタンでクリックして、「**新規インターフェース**」、および新しいインターフェースが提示するネットワークのタイプを選択します。ウィザードの指示に従って、新規 TCP/IP インターフェースを作成します。このウィザードは、次の情報を提供するよう要求してきます。
   - 接続のタイプ
   - ハードウェア・リソース
   - 回線記述
   - IP アドレス
   - ホスト名
   - ドメイン名

     ウィザードで使用するホスト名およびドメイン名は、完全修飾ドメイン名を構成します。 SMTP では、他の SMTP ホストと通信するために、完全修飾ドメイン名が必要です。

     例えば、ローカル・ホスト名が ASHOST で、ローカル・ドメイン名が DOMAIN.COMPANY.COM の場合には、完全修飾ドメイン名は ASHOST.DOMAIN.COMPANY.COM となります。
   - 開始するサーバー
3. ウィザードでの作業が終わったら、「**TCP/IP**」を右ボタンでクリックしてから、「**プロパティー**」を選択します。「TCP/IP プロパティー」ダイアログが表示されます。
4. 「**ホスト・テーブル**」タブをクリックします。
5. 「**追加**」をクリックします。 「TCP/IP ホスト・テーブル項目」ダイアログが表示されます。
6. 「新しいインターフェース」ウィザードで使用した IP アドレスおよびホスト名を入力します。
7. 「**OK**」をクリックして、「TCP/IP ホスト・テーブル項目」ダイアログを閉じます。
8. 「**OK**」をクリックして、「TCP/IP プロパティー」ダイアログを閉じます。

関連概念

55 ページの『電子メールの問題判別』
簡単な手順で、電子メールの問題の原因を判別することができます。

関連タスク

『電子メールのための Simple Mail Transfer Protocol サーバーおよび Post Office Protocol サーバーの構成』
電子メールを使用するには、ご使用のシステム上で Simple Mail Transfer Protocol (SMTP) サーバーおよび Post Office Protocol (POP) サーバーを構成する必要があります。

電子メールのための Simple Mail Transfer Protocol サーバーおよび Post Office Protocol サーバーの構成

電子メールを使用するには、ご使用のシステム上で Simple Mail Transfer Protocol (SMTP) サーバーおよび Post Office Protocol (POP) サーバーを構成する必要があります。

注: SMTP サーバーと POP サーバーは、両方とも正しく構成する必要があります。

関連概念

4 ページの『i5/OS での Post Office Protocol』
Post Office Protocol (POP) サーバーは、i5/OS における Post Office Protocol バージョン 3 メール・インターフェースのインプリメンテーションです。

関連タスク

17 ページの『電子メールのための TCP/IP の構成』
ご使用のシステム上で電子メールを構成するには、事前に TCP/IP をセットアップする必要があります。

Simple Mail Transfer Protocol サーバーの構成

TCP/IP を構成した時点で、システムは自動的に SMTP を構成しています。 ただし、電子メールが SMTP サーバーで正しく処理されることを確実にするため、いくつかの SMTP プロパティーを変更する必要があります。

SMTP プロパティーを変更するには、次のステップを実行してください。

1. System i ナビゲーターで、「**ユーザーのシステム**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」と展開します。
2. 「**SMTP**」をダブルクリックします。
3. 次の表にリストされているタブをクリックして、「次に、以下のアクションを実行します」列に示されているフィールド値を設定します。

このタブをクリックします。	次に、以下のアクションを実行します。
一般	「**TCP/IP の開始時に開始**」を選択します。[1]
一般	「**メッセージ分割サイズ**」フィールドで、「**無限大**」を選択します。
一般	メール・ルーターがある場合には、mailrouter.company.com などのメール・ルーターの名前を入力します。メール・ルーター名は、電子メールがローカル・メールでない場合に SMTP がこのメールを経路指定する先のシステム名です。 詳しくは、System i ナビゲーターのヘルプを参照してください。
一般	ファイアウォール設定がある場合には、「**ファイアウォールを介したルーターへの発信メールの転送**」を選択します。
一般	Domino サーバーで電子メールを交換する際には、「**パーセント記号をルーティング文字として解釈**」フィールドをクリアします。
一般	すべての非ローカル電子メールを別の SMTP サーバーに転送する場合は、「**転送先のメール・ハブ・ドメイン (Forwarding mailhub domain)**」フィールドに完全修飾メール・エクスチェンジャー・ドメイン名を指定します。
一般	SMTP サーバーで bare LF または CRLF (復帰改行) をサポートする場合は、「**bare LF を許可 (Allow bare line feed)**」を選択します。SMTP サーバーで CRLF のみをサポートする場合は、「**bare LF を許可 (Allow bare line feed)**」チェック・ボックスのチェックを外します。
自動登録	電子メールの送信に SNDDST コマンド、電子メールの受信に RCVDST コマンドを使用し、インターネット・アドレッシングの代わりに SNADS アドレッシングを使用する場合は、「**システム配布ディレクトリーにリモート・ユーザーを自動的に追加**」チェック・ボックスを選択します。

このタブをクリックします。	次に、以下のアクションを実行します。
自動登録	電子メールの送信に SNDDST コマンド、電子メールの受信に RCVDST コマンドを使用する場合は、「**ユーザーの追加先**」フィールドで「**システム別名テーブル**」をクリックします。
[1] この変更は、次回 SMTP サーバーが開始されたときに有効になります。	

4. 「**OK**」をクリックして、変更を受け入れます。

関連タスク

29 ページの『ローカルおよび中継のための電子メールの認証』
電子メールの送信において認証を必須とすることにより、ご使用のサーバーでスパムを防ぐことが可能になりました。メッセージの中継を制限する場合は、認証を必須にすることはできません。ご使用のサーバーに対して認証をセットアップすることをお勧めします。

受信側システム上で SMTP サーバーとクライアント間で SSL を使用可能にする:

受信側システム上で SMTP サーバーとクライアント間で SSL を使用可能にするには、次のステップを実行してください。サーバー証明書が、SMTP サーバー上に既に作成済みであることを前提としています。

このタスクを実行するにあたって、受信側システムに接続していることを確認してください。

DCM の開始および構成

1. Web ブラウザーで、http://*your_system*: 2001/ から SMTP サーバーに接続します。
2. 「i5/OS タスク (i5/OS タスク)」ページで、「**デジタル証明書マネージャー**」を選択し、「**証明書ストアの選択**」をクリックします。
3. 「証明書ストアの選択」ページで、「***SYSTEM**」を選択し、「**続行**」をクリックします。
4. 「証明書ストア名およびパスワード」ページで、証明書ストアのパスワードを入力します。
5. 「**アプリケーションの管理**」 → 「**証明書割り当ての更新**」を展開し、「**サーバー**」を選択します。
6. 「**i5/OS TCP/IP SMTP サーバー**」を選択し、必要に応じて「**証明書割り当ての更新**」をクリックします。

SMTP サーバーの構成

SSL サポートを使用可能にするには、SMTP 属性の変更 (CHGSMTPA) コマンドを使用し、ALWAUTH パラメーターを *LCLRLY または *RELAY のいずれかに設定します。

- パラメーターを *RELAY に設定した場合は、もう一方の SMTP サーバーから送信される電子メールのみが SSL の使用をサポートします。
- パラメーターを *LCLRLY に設定した場合は、MSF メッセージの検査 (VFYMSFMSG) およびユーザーからの確認 (VFYFROMUSR) パラメーターも有効になります。また、デフォルト値が指定されていると、ある種の電子メールがリジェクトされます。リジェクト・サポートを使用可能にするか決定してください。

SMTP クライアントの構成

System i SMTP 受信側サーバーにログオンできるように System i SMTP クライアントを構成する必要があります。次のようにして、SMTP リスト項目の追加 (ADDSMTPLE) CL コマンドを使用して、ホスト認証リストに項目を追加します。

```
ADDSMTPLE TYPE(*HOSTAUTH) HOSTNAME(yoursystem.realm.com) USERNAME(receiver) PASSWORD(xxxx)
```

ホスト名は大文字で保管されており、電子メール・アドレスと一致する必要があります。電子メールが myemail@yoursystem の場合には、次の項目を追加する必要があります。

```
ADDSMTPLE TYPE(*HOSTAUTH) HOSTNAME(YOURSYSTEM) USERNAME(receiver) PASSWORD(xxxx)
```

送信側システム上で SMTP サーバーとクライアント間で SSL を使用可能にする:

このタスクを実行するには、送信側システムに接続している必要があります。

1. Web ブラウザーで、http://*your_system*: 2001/ から SMTP サーバーに接続します。
2. 「i5/OS タスク (i5/OS タスク)」ページで、「**デジタル証明書マネージャー**」を選択し、「**証明書ストアの選択**」をクリックします。
3. 「証明書ストアの選択」ページで、「***SYSTEM**」を選択し、「**続行**」をクリックします。
4. 「証明書ストア名およびパスワード」ページで、証明書ストアのパスワードを入力し、「**続行**」をクリックします。 ユーザー証明書がない場合、またはユーザー証明書を作成したい場合は、ステップ 5 から 8 を実行してください。それ以外の場合は、ステップ 9 にスキップしてください。
5. 「証明書の作成」ページで、「**ユーザー証明書**」を選択し、「**続行**」をクリックします。
6. 「ユーザー証明書の作成」ページで、証明書情報の必須フィールドを指定し、「**続行**」をクリックします。
7. 「潜在的なスクリプト違反 (Potential Scripting Violation)」ウィンドウで、「**はい**」をクリックします。
8. 「ユーザー証明書の作成」ページで、「**OK**」をクリックします。システムは、クライアントのユーザー証明書を使用します。
9. 「**アプリケーションの管理**」 → 「**証明書割り当ての更新**」を展開し、「**サーバーまたはクライアントの証明書**」を選択します。
10. 「証明書割り当ての更新」ページで、「**クライアント**」を選択し、「**続行**」を選択します。
11. 「**i5/OS TCP/IP クライアント**」を選択し、「**証明書割り当ての更新**」ボタンをクリックします。

受信側の認証局 (CA) の送信側システムへのインストール:

受信側のデジタル証明書が、送信側システムに認識されていない認証局 (CA) によって発行される場合は、送信側システムに認証局 (CA) のデジタル証明書をインストールしてください。

ローカル CA 証明書のエクスポート、およびローカル CA 証明書の送信側システムへの送信

認証局 (CA) がローカルにあると仮定します。ただし、この手順に従って、送信側システムに認識されていない任意の CA 証明書をエクスポートできます。

ローカル CA 証明書をエクスポートするには、次の手順に従ってください。

1. 「**証明書ストアの選択**」をクリックして、「**ローカル認証局 (CA)**」を選択します。「**続行**」をクリックします。
2. 「証明書ストア名およびパスワード」ページで、パスワードを入力します。
3. 「**ローカル CA の管理**」 → 「**エクスポート**」を展開し、「**ファイル**」**-** 「**ファイルへのエクスポート**」を選択します。「**続行**」をクリックします。
4. 「証明書のエクスポート」ページで、CA 証明書を保管するディレクトリーおよびファイル名ロケーションを入力します。ディレクトリーが存在しない場合は、mkdir コマンドを使用して作成します。
5. 「証明書のエクスポートが正常に終了しました」ページで、「**OK**」をクリックします。

| 6. FTP を ASCII モードで使用して、受信側システムから送信側システムに CA 証明書を送信します。

| **CA 証明書の送信側システムへのインストール**

| 1. 「証明書ストアの選択」ページで、「***SYSTEM**」を選択し、「**続行**」をクリックします。
| 2. 「証明書ストア名およびパスワード」ページで、パスワードを入力し、「**続行**」をクリックします。
| 3. 「**証明書の管理**」 → 「**証明書のインポート**」を展開し、「**認証局 (CA)**」を選択してから「**続行**」をクリックします。
| 4. 「認証局 (CA) 証明書のインポート」ページで、受信側 CA 証明書を保管したディレクトリーを入力します。「**続行**」をクリックします。
| 5. 証明書ラベルを証明書に割り当て、「**続行**」をクリックします。メッセージ「**証明書がインポートされました**」が表示されます。
| 6. 「**OK**」をクリックします。

Post Office Protocol サーバーの構成

POP クライアントにメールを送信するには、まず Post Office Protocol (POP) サーバーを構成する必要があります。

POP クライアントから要求されると、POP サーバーは、ユーザーのメールボックスから POP クライアントに電子メールを送信します。電子メールを使えるようシステムを完全に準備するには、POP サーバーの構成が必要です。

Netscape Mail または Eudora Pro などのメール・プログラム用に POP サーバーを構成する場合は、以下のステップを実行してください。

1. System i ナビゲーターで、「**ユーザーのシステム**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」と展開します。
2. 「**POP**」をダブルクリックします。
3. 次の表を参照してフィールド値を設定します。

このタブをクリックします。	次に、以下のアクションを実行します。
一般	「**TCP/IP の開始時に開始**」を選択します。
一般	TLS/SSL および非セキュア POP の両セッションを許可する場合は、「**サーバーと一緒に開始するソケット層サポート (Socket layer support to be started with server)**」で「**セキュアおよび非セキュアの両方 (Both secure and nonsecure)**」を選択します。
構成	「**メッセージ分割サイズ**」フィールドで、「**無限大**」を選択します。
構成	POP クライアントがダイヤルアップ回線を通してログオンし、サイズの大きなメールを受信する場合は、「**非活動タイムアウト値 (Inactivity timeout value)**」を大きくします。
マッピング	「**サポートされない CCSID が示されたときにのみ使用**」を選択します。

4. 「**OK**」をクリックして、変更を受け入れます。

| **証明書の Post Office Protocol サーバーへの関連付け:**

| ローカル認証局 (CA) の作成中に、証明書を Post Office Protocol (POP) サーバー・アプリケーションに割
| り当てるタスクを実行しなかった場合、または公開 CA から証明書を要求するようにシステムを構成した
| 場合は、このタスクを実行します。

| 1. IBM ディジタル証明書マネージャーの開始。証明書を取得または作成する必要がある場合、あるいは
| 証明書システムをセットアップまたは変更する必要がある場合は、この時点で行います。 証明書シス
| テムのセットアップに関する情報は、『DCM の構成』を参照してください。
| 2. 「**証明書ストアの選択**」をクリックします。
| 3. 「***SYSTEM**」を選択します。「**続行**」をクリックします。
| 4. *SYSTEM 証明書ストア用の適切なパスワードを入力します。「**続行**」をクリックします。
| 5. 左のナビゲーション・メニューが再ロードされたら、「**アプリケーションの管理**」を展開します。
| 6. 「**証明書割り当ての更新**」をクリックします。
| 7. 「**サーバー・アプリケーション (Server application)**」を選択します。「**続行**」をクリックします。
| 8. 「**i5/OS TCP/IP POP サーバー**」を選択します。
| 9. 「**証明書割り当ての更新**」をクリックして、証明書をこの POP サーバーに割り当てます。
| 10. リストからサーバーに割り当てる証明書を選択します。
| 11. 「**新規証明書の割り当て**」をクリックします。
| 12. POP サーバーの証明書のセットアップが終了したら、「**完了**」をクリックします。

電子メール・ユーザーの登録

電子メール・ユーザーを登録するには、ユーザー・プロファイルを作成する必要があります。

ユーザー・プロファイルによって、i5/OS オペレーティング・システムは電子メールの宛先または送信側を判別します。 電子メール・システムに含める必要のあるユーザーすべてについて、システムにユーザー・プロファイルを作成する必要があります。

各ユーザーについてユーザー・プロファイルを作成すると、自動的にシステム配布ディレクトリーにそのユーザーが登録されます。システム配布ディレクトリーは、Simple Mail Transfer Protocol (SMTP) がローカル電子メールの送信先を判別するために使用するものです。

Systems Network Architecture Distribution Services (SNADS) および Post Office Protocol (POP) の電子メール・ユーザーのためにユーザー・プロファイルを作成するには、以下の手順に従ってください。

1. System i ナビゲーターで、「**ユーザーのシステム**」 → 「**ユーザーおよびグループ**」と展開します。
2. 「**すべてのユーザー**」を右ボタンでクリックしてから、「**新規ユーザー**」を選択します。
3. ユーザーのユーザー名およびパスワードを入力します。

   注: このパスワードは、POP ユーザーによって自分の POP メールボックスにアクセスするために使用されます。
4. 「**機能**」ボタンをクリックします。
5. 「**特権**」タブをクリックします。「特権クラス」が「**ユーザー**」であることを確認します。
6. 「**OK**」をクリックします。
7. 「**個人**」ボタンをクリックします。
8. 「**メール**」タブをクリックします。
9. 「**メール・サービス・レベル**」を選択します。
   - ユーザーが SNADS ユーザーの場合には、「**ユーザー索引**」を選択します。

| • ユーザーが POP3 メール・ユーザーの場合には、「**システム・メールボックス**」を選択します。

10. 「**優先アドレス・タイプ**」を選択します。
    - ユーザーが SNADS ユーザーの場合には、「**ユーザー ID およびアドレス**」を選択します。
| • ユーザーが POP3 メール・ユーザーの場合には、「**SMTP 名**」を選択します。
11. 必要なドメイン名が SMTP 電子メール・ドメインに表示されていることを確認します。 通常はデフォルト名で正しいのですが、複数のローカル・ドメインがある場合にはデフォルト名を変更しなければならない場合があります。
12. 「**OK**」をクリックします。SNADS ユーザーを登録している場合、これで登録は完了です。 電子メールを取り出すためだけに i5/OS POP サーバーを使用する POP ユーザーを登録している場合には、次のステップに進みます。
13. 「**ジョブ**」ボタンをクリックします。
14. 「**セッション開始**」タブをクリックします。
15. 「**初期メニュー**」フィールドで、「**サイン・オフ**」を選択します。上記のように設定すると、ユーザーは、システムにサインオンしようとしても、電子メールの取得またはパスワード変更以外は、自動的にサインオフされます。
16. 「**OK**」をクリックします。
17. 「**OK**」をクリックします。
18. 上記の手順を繰り返し、すべての電子メール・ユーザーのユーザー・プロファイルを用意します。

関連概念

35 ページの『電子メールの送受信』
ご使用のシステムはメール・サーバーで、ここに電子メール・ユーザー (SNADS、POP、または Lotus ユーザー) が登録されています。電子メール・ユーザーは、POP クライアントまたは SNADS クライアントのいずれかを使用して電子メールの送信、受信および読み取りを行うことができます。

関連タスク

38 ページの『システム・ネットワーク体系 (SNA) 配布サービスを使用した電子メールの送信』
システム・ネットワーク体系 (SNA) 配布サービス (SNADS) クライアント・プログラムを使用して、ご使用のシステムから電子メールを送信できます。電子メールの送信者は、 ローカルな SNADS ユーザーでなければなりません。

電子メール・サーバーの開始および停止

必要なサーバーを開始して、すべてが正しく作動していることと、変更した構成が有効になっていることを確認します。そのために、サーバーの再始動が必要な場合もあります。サーバーを停止してから、サーバーの開始のステップを再度実行することによって、サーバーを再始動できます。

関連タスク

42 ページの『電子メール・サーバーの検査』
電子メール関連の最も一般的な問題の 1 つに、 適切なサーバーが開始しないという問題があります。電子メール・サーバーを使用する前に、その電子メール・サーバーの状況を検査し、それらがすべて稼働中であることを確認する必要があります。

電子メール・サーバーの開始

サーバーを開始し、ご使用のシステムを電子メール・ユーザーが登録された電子メール・サーバーにすることができます。

サーバーを開始するには、以下の手順に従ってください。

1. System i ナビゲーターで、**「ユーザーのシステム」 → 「ネットワーク」**と展開します。
2. 「**TCP/IP 構成**」を右クリックして「**プロパティー**」を選択します。「TCP/IP 構成プロパティー」ダイアログが開きます。
   - TCP/IP 状況が Started の場合には、「**OK**」をクリックして、次のステップに進みます。
   - そうでない場合には、「**キャンセル**」をクリックして、「TCP/IP 構成プロパティー」ダイアログをクローズします。それから「**TCP/IP 構成**」を右ボタンでクリックし、「**開始**」を選択します。完了したら、「**OK**」をクリックします。
3. **「サーバー」 → 「TCP/IP」**の順に展開します。SMTP および POP サーバーが開始されていない場合には、次の手順で始動します。
   a. 「**SMTP**」を右ボタンでクリックし、「**開始**」を選択します。
   b. 「**POP**」を右ボタンでクリックし、「**開始**」を選択します。
4. 文字ベース・インターフェースを開き、STRMSF と入力してメール・サーバー・フレームワークを開始します。
5. SNADS を使用している場合は、STRSBS QSNADS と入力して QSNADS サブシステムを開始します。

サーバーが開始しました。現在、ご使用のシステムは電子メール・ユーザーが登録された電子メール・サーバーを実行しています。

電子メール・サーバーの停止

System i ナビゲーターを使用して、電子メール・サーバーを停止できます。

サーバーを停止するには、以下の手順に従ってください。

1. System i ナビゲーターで、**「ユーザーのシステム」 → 「ネットワーク」 → 「サーバー」 → 「TCP/IP」**と展開します。SMTP および POP サーバーが開始されている場合には、次の手順で停止します。
   a. 「**SMTP**」を右ボタンでクリックし、「**停止**」を選択します。
   b. 「**POP**」を右ボタンでクリックし、「**停止**」を選択します。
2. 文字ベースのインターフェースをオープンし、ENDMSF と入力してメール・サーバー・フレームワークを終了します。
3. SNADS を使用している場合は、ENDSBS QSNADS と入力して QSNADS サブシステムを終了します。

ダイヤルアップ・メール接続プロファイルの構成

AT&T Global Network のサポートがない場合は、まずメール接続プロファイルを構成する必要があります。

ダイヤルアップ接続プロファイルを手作業で作成するには、以下のステップを実行してください。

注: AT&T Global Network サポートをお持ちの場合は、ISP ダイヤルアップ接続ウィザードの構成にスキップできます。

1. System i ナビゲーターで、**「ユーザーのシステム」 → 「ネットワーク」 → 「リモート・アクセス・サービス」**の順に展開します。
2. 「**レシーバー接続プロファイル**」を右マウス・ボタン・クリックし、「**新規プロファイル**」を選択します。
3. 「**プロトコル・タイプ**」に「**PPP**」を選択します。
4. 「**接続タイプ**」に「**交換回線**」を選択します。

5. 「**TCP/IP 構成**」を展開して、「**接続**」を選択します。
6. 「**サーバー**」 → 「**TCP/IP**」の順に展開します。
7. 「**SMTP**」を右ボタンでクリックし、「**プロパティー**」を選択します。
8. 「**スケジューラー**」タブをクリックします。「**SMTP の開始時にスケジューラーを開始 (Start scheduler when SMTP is started)**」チェック・ボックスを選択し、作成した接続プロファイルを指定します。
9. 「ETRN」ページをクリックし、「**ETRN をサポート (ダイヤルアップ・メール検索) (Support ETRN (Dial-up mail retrieval))**」チェック・ボックスを選択します。 「**追加**」をクリックし、ISP の発信サーバーのアドレスのドメイン名を指定します。
10. ファイアウォールを使用可能にし、インターネット・サービス・プロバイダー (ISP) の発信メール・サーバーを指定します。
11. ウィザードをさらに実行し、新しい ISP のダイヤルアップ接続をセットアップします。

関連タスク

『ISP ダイヤルアップ接続ウィザードの構成』
Simple Mail Transfer Protocol (SMTP) スケジューラー機能を使用して、多数の電子メールをインターネット・サービス・プロバイダーを通じて送信するには、まずダイヤルアップ接続プロファイルを構成する必要があります。

ISP ダイヤルアップ接続ウィザードの構成

Simple Mail Transfer Protocol (SMTP) スケジューラー機能を使用して、多数の電子メールをインターネット・サービス・プロバイダーを通じて送信するには、まずダイヤルアップ接続プロファイルを構成する必要があります。

インターネット・サービス・プロバイダー (ISP) ダイヤルアップ接続ウィザードを使用して、ISP ダイヤルアップ接続プロファイルを構成することが可能です。

前提条件:

AT&T Global Network サポートがない場合は、ダイヤルアップ・メール接続プロファイルの構成を参照して、予備的なステップを実行してください。 接続ウィザードが、メール・サーバー (SMTP および POP) の IP アドレス、割り当てられたドメイン名、アカウント名、およびパスワードを表示します。

ウィザードを実行し、SMTP スケジューラーを構成するには、以下のステップを実行してください。

1. System i ナビゲーターで、「**ユーザーのシステム**」 → 「**ネットワーク**」 → 「**リモート・アクセス・サービス**」の順に展開します。
2. 「**発信元接続プロファイル**」で右ボタンをクリックし、「**新規 AT&T Global Network ダイヤル接続 (New AT Global Network Dial Connection)**」を選択します。
3. 「ウェルカム」パネルで、「**次へ**」をクリックして起動します。
4. 「**アプリケーション・タイプ (Application Type)**」パネルで、「**メール交換アプリケーション**」を選択してから、「**次へ**」をクリックします。
5. 続けてウィザードを実行し、新しい AT&T Global Network ダイヤル接続をセットアップします。

ダイヤルアップ接続の構成が済んだら、バッチ ISP 電子メール・ジョブのスケジュールを行う準備ができたことになります。

関連タスク

24 ページの『ダイヤルアップ・メール接続プロファイルの構成』
AT&T Global Network のサポートがない場合は、まずメール接続プロファイルを構成する必要があります。

『バッチ ISP 電子メール・ジョブのスケジュール』
接続の確立に必要な時間を制限するために、一定の間隔でインターネット・サービス・プロバイダー (ISP) に接続するメール・ダイヤルアップ・ジョブをスケジュールすることができます。ご使用のシステムが ISP に接続して会社の電子メールを送信する時間間隔を設定するには、SMTP スケジューラーを使用します。

バッチ ISP 電子メール・ジョブのスケジュール

接続の確立に必要な時間を制限するために、一定の間隔でインターネット・サービス・プロバイダー (ISP) に接続するメール・ダイヤルアップ・ジョブをスケジュールすることができます。ご使用のシステムが ISP に接続して会社の電子メールを送信する時間間隔を設定するには、SMTP スケジューラーを使用します。

前提条件:

ISP ダイヤルアップ接続ウィザードを使用して接続を構成します。

ISP に電子メールを送信するよう SMTP スケジューラーを設定するには、以下のステップに従ってください。

1. System i ナビゲーターで、「**ユーザーのシステム**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」と展開します。
2. 「**SMTP**」をダブルクリックします。
3. 「**スケジューラー**」タブをクリックします。
4. 「**SMTP の開始時にスケジューラーを開始 (Start scheduler when SMTP is started)**」チェック・ボックスを選択します。
5. AT&T Global Network ダイヤラー・ウィザードで構成した「**2 地点間接続プロファイル**」か、手作業で構成した 「**2 地点間接続プロファイル**」を選択します。
6. 「**メール転送間隔**」では、SMTP が待ち行列に入っている電子メールを転送する間隔を分単位で設定します。
7. ご使用の ISP が AT&T Global Network でなければ、「**リモート・サーバー接続時に ETRN を発行 (Issue ETRN when connecting to remote server)**」チェック・ボックスを選択します。
8. ISP のネットワーク上の着信メール・サーバーの「サーバー IP アドレス」を入力し、この SMTP サーバーが ETRN を発行する「登録 ISP host.domain (Registered ISP host.domain)」を入力します。
9. 「**OK**」をクリックします。

関連タスク

25 ページの『ISP ダイヤルアップ接続ウィザードの構成』
Simple Mail Transfer Protocol (SMTP) スケジューラー機能を使用して、多数の電子メールをインターネット・サービス・プロバイダーを通じて送信するには、まずダイヤルアップ接続プロファイルを構成する必要があります。

27 ページの『ダイヤルアップでメールを取得するための、SMTP サーバーの構成』
Simple Mail Transfer Protocol (SMTP) サーバーを使用して、リモート・ダイヤルアップ事業所のためにメールを受信することができます。

ダイヤルアップでメールを取得するための、SMTP サーバーの構成

Simple Mail Transfer Protocol (SMTP) サーバーを使用して、リモート・ダイヤルアップ事業所のためにメールを受信することができます。

システムには固定 IP アドレスが必要であり、DNS に登録されていなければなりません。 このシステムを指す DNS には、リモート・ダイヤルアップ・サーバーがメールを検索する host.domain ごとに MX 項目も必要となります。システムは、自分のローカル・ホスト・テーブルに、これらの host.domain の別名を持つ必要もあります。 リモート・ダイヤルアップ・サーバーが i5/OS オペレーティング・システムの場合、それらはバッチ ISP 電子メール・ジョブをスケジュールするように、構成しなければなりません。

リモート・ダイヤルアップ・メール・サーバーから電子メール要求を受信するには、以下のステップを実行してください。

1. System i ナビゲーターで、「**ユーザーのシステム**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」と展開します。
2. 「**SMTP**」をダブルクリックします。
3. 「**ETRN**」タブをクリックします。
4. 「**ETRN をサポート (ダイヤルアップ・メール検索) (Support ETRN (Dial-up mail retrieval))**」チェック・ボックスを選択します。
5. 「**追加**」をクリックして、ISP のホストおよびドメイン名を指定します。複数のメール・サーバーがメールの要求を行う場合は、これを複数回行います。
6. 「**OK**」をクリックします。

関連タスク

26 ページの『バッチ ISP 電子メール・ジョブのスケジュール』
接続の確立に必要な時間を制限するために、一定の間隔でインターネット・サービス・プロバイダー (ISP) に接続するメール・ダイヤルアップ・ジョブをスケジュールすることができます。ご使用のシステムが ISP に接続して会社の電子メールを送信する時間間隔を設定するには、SMTP スケジューラーを使用します。

複数ドメインのサポート

インターネット・サービス・プロバイダー (ISP) 機能をホストするために、Simple Mail Transfer Protocol (SMTP) サーバーを、複数のドメインをサポートするように構成することができます。

SMTP サーバーが ISP 機能をホスティングするためには、SMTP が複数のドメインで機能する必要があります。SMTP クライアントは、この構成情報を使用して、電子メールの送信時にどのインターフェースにバインドするか、どのメールをローカルとして処理 (つまりクライアント自身で解決し、送信する) するか、どのメールを構成済みのファイアウォール・メール・デーモンに転送するかを認識します。

1. System i ナビゲーターで、「**ユーザーのシステム**」 → 「**TCP/IP**」 → 「**ネットワーク**」の順に展開します。
2. 「**SMTP**」を右ボタンでクリックし、「**プロパティー**」を選択します。
3. 「**複数ドメイン**」タブをクリックします。
4. 「**追加**」をクリックし、サポートしたいドメインとインターフェースを指定します。
5. 「**OK**」をクリックします。

関連概念

29 ページの『電子メール・ルーターの前提条件』
このトピックでは、電子メール・ルーターを構成する前に行う必要があることについて説明します。

電子メールの保護

電子メールを保護するためには、ファイアウォールの使用、中継および接続の制限、ウィルス対策のフィルターが有効です。

Simple Mail Transfer Protocol (SMTP) サーバーにおいて、機密保護機能のある環境を促進するのは重要なことです。 SMTP サーバーとユーザーを、内部および外部の障害から保護しなければなりません。

関連概念

| 2 ページの『電子メールの概念』
| 電子メール (E-mail) は、必要不可欠なビジネス・ツールとなっています。i5/OS オペレーティング・システムでは、Simple Mail Transfer Protocol (SMTP) や Post Office Protocol (POP) などのプロトコルを
| 使用し、電子メールがネットワーク上で円滑かつ効率的に行き来するようにします。

関連資料

| Create and Send MIME E-mail (QtmsCreateSendEmail) API

関連情報

| 電子メール・セキュリティー

ルーターまたはファイアウォールを介した電子メールの送信

電子メール・ルーターは、Simple Message Transfer Protocol (SMTP) が宛先の正確な IP アドレスを見つけられない場合にメールを送達する中間システムです。

電子メール・ルーターは、電子メールを IP アドレスまたは他のルーターに経路指定します。 ローカルのサーバーが電子メールをシステムに配布できなかった場合には、その発信電子メールを代替システムに経路指定します。ファイアウォールがある場合には、このファイアウォールをルーターとして使用できます。

以下の手順に従ってルーターを構成する前に、 29 ページの『電子メール・ルーターの前提条件』 を参照してください。

ルーターを設定するには、以下の手順に従ってください。

1. System i ナビゲーターで、「**ユーザーのシステム**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」と展開します。
2. 「**SMTP**」をダブルクリックします。
3. 「**一般**」タブをクリックします。
4. 「メール・ルーター」名を入力します。

ファイアウォールを介して電子メールを経路指定するには、以下の手順に従ってください。

1. System i ナビゲーターで、「**ユーザーのシステム**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」と展開します。
2. 「**SMTP**」をダブルクリックします。
3. 「**一般**」タブをクリックします。
4. 「**メール・ルーター**」フィールドに、`FWAS400.company.com` などのファイアウォールの名前を入力します。
5. 「**ファイアウォールを介したルーターへの発信メールの転送**」を選択します。

電子メール・ルーターの前提条件

このトピックでは、電子メール・ルーターを構成する前に行う必要があることについて説明します。

電子メール・ルーターを構成する前に、以下の特徴について考慮してください。

- 中間サーバーは、i5/OS オペレーティング・システムである必要はありません。 メール・ルーターに必要なのは、電子メールを経路指定しなければならないすべてのホスト・サーバーを含むホスト・テーブルのみです。 i5/OS オペレーティング・システムがメール・ルーターである場合には、特別なシステム・レベルは必要ありません。
- ソース・サーバーとターゲット・サーバーとの間の経路指定のために設定できる中間システムは 1 つのみです。 メール・ルーターをネストすることはできません。
- Simple Mail Transfer Protocol (SMTP) は開始時に、ローカル・ホスト・テーブル (LHT) またはドメイン・ネーム・システム (DNS) サーバーのどちらかから、メール・ルーターの IP アドレスを取得可能でなければなりません。 SMTP がメール・ルーターの IP アドレスを取得できない場合、SMTP はルーターを使用しないで実行します。
- SMTP クライアント・ファイアウォール・サポートはメール・ルーターを使用して、ローカル (保護) ドメイン外のホストに宛てられた電子メールを転送します。電子メールを配布するために、メール・ルーターは、電子メールをファイアウォールを介して転送する権限を持つサーバーでなければなりません。また、SMTP ファイアウォール・サポートを有効にすると、ドメインが i5/OS オペレーティング・システム上にない宛先へのメールはルーターを通過することになります。 i5/OS V5R1 およびそれ以降は、複数のローカル・ドメインをサポートしています。ファイアウォールを介してメールを送信しないドメインを複数、構成することができます。

関連タスク

27 ページの『複数ドメインのサポート』
インターネット・サービス・プロバイダー (ISP) 機能をホストするために、Simple Mail Transfer Protocol (SMTP) サーバーを、複数のドメインをサポートするように構成することができます。

ローカルおよび中継のための電子メールの認証

電子メールの送信において認証を必須とすることにより、ご使用のサーバーでスパムを防ぐことが可能になりました。メッセージの中継を制限する場合は、認証を必須にすることはできません。ご使用のサーバーに対して認証をセットアップすることをお勧めします。

ご使用のサーバーで認証を有効にするには、次のステップを実行してください。

1. System i ナビゲーターで、「**ユーザーのシステム**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」と展開します。
2. 「**SMTP**」をダブルクリックします。
3. 「**認証**」タブをクリックして、「次に、以下のアクションを実行します」列に示されているフィールド値を設定します。

このタブをクリックします。	次に、以下のアクションを実行します。
認証	サーバーで TLS/SSL を使用して、メッセージを中継する場合にローカルで TLS/SSL を認証する場合は、「**TLS/SSL を必須とし、メッセージを中継する場合にローカルでそれを認証する (Require TLS/SSL and authenticate it locally and when using the relay)**」を選択します。

このタブをクリックします。	次に、以下のアクションを実行します。
認証	サーバーで TLS/SSL を使用し、中継機能を使用する場合にのみそれを認証する場合は、「**TLS/SSL を必須とし、中継のみを認証 (Require TLS/SSL and authenticate only the relay)**」を選択します。
認証	SMTP へのログオンが許可されているリストにあるユーザーのみを許可する場合は、「**ローカル配信で ID を検査 (Verify IDs on local delivery)**」を選択します。
認証	SMTP サーバーで、メール・サーバー・フレームワーク (MSF) のスナップイン機能を使用して照合されない電子メールをリジェクトできるようにするには、「**メッセージ発信元の検査 (Verify message originator)**」を選択します。
認証	SMTP サーバーで、送信側の電子メール・アドレスがシステム配布ディレクトリーにあるかどうか、およびそのアドレスが一致するかどうかを検査するには、「**ユーザー**」または「**受け入れリストにないユーザー (Users not on the accept list)**」を選択します。電子メール・アドレスが一致しない場合、そのユーザーはリジェクトされます。

4. 「**OK**」をクリックして、変更を受け入れます。

関連タスク

31 ページの『メッセージ中継の制限』
電子メール・サーバーがスパミングまたはバルク・メールの大量送信に使用されるのを防ぐために、中継制限機能を使用します。 この機能で、メッセージ中継の目的でご使用のシステムを使用できるユーザーを指定できます。 ただし、メッセージの中継を制限する場合は、電子メールを認証することはできません。

18 ページの『Simple Mail Transfer Protocol サーバーの構成』
TCP/IP を構成した時点で、システムは自動的に SMTP を構成しています。 ただし、電子メールが SMTP サーバーで正しく処理されることを確実にするため、 いくつかの SMTP プロパティーを変更する必要があります。

電子メール送信者のトラッキング

現在、SMTP サーバーでは、認証されていない電子メール送信者をリジェクトするよう設定できるようになりました。加えて、SMTP メール・サーバー・フレームワーク (MSF) のスナップイン機能で、照合されていない電子メールをリジェクトするよう設定できるようになりました。

照合されない送信者または電子メールをリジェクトするにはトランザクションの暗号化、つまり、TLS/SSL プロトコルを使用可能にする必要があります。

照合されない電子メール送信者のリジェクト

照合されない電子メール送信者をリジェクトするには、次の手順に従ってください。

1. System i ナビゲーターで、「**ユーザーのシステム**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」の順に展開します。
2. 「**SMTP**」を右ボタンでクリックし、「**プロパティー**」を選択します。
3. 「**認証**」タブをクリックします。
4. すべての電子メール送信者を確認するには、「**ユーザーからのメールを検査 (Verify mail from user)**」フィールドで、「**すべて**」を選択します。受け入れリストにないユーザーのみを検査する場合は、「**受け入れリストにないユーザー (Users not on the accept list)**」を選択します。
5. 「**OK**」をクリックします。

SMTP サーバーが、送信者がシステム配布ディレクトリーにあるか、および電子メール・アドレスがディレクトリー内のアドレスと一致するかを検査します。不一致があれば、そのユーザーはリジェクトされます。

照合されない電子メールのリジェクト

照合されない電子メールをリジェクトするには、次の手順に従ってください。

1. System i ナビゲーターで、「**ユーザーのシステム**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」の順に展開します。
2. 「**SMTP**」を右ボタンでクリックし、「**プロパティー**」を選択します。
3. 「**認証**」タブをクリックします。
4. 「**認証を許可 (Allow authentication)**」フィールドで、「**TLS/SSL を必須とし、メッセージを中継する場合にローカルでそれを認証する (Require TLS/SSL and authenticate it locally and when using the relay)**」を選択します。
5. 「**MSF メッセージ発信元の検査 (Verify MSF message originator)**」を選択します。
6. 「**OK**」をクリックします。

電子メールが認証済みソースからのものでない場合は、QzmfCrtMailMsg() API を発行したユーザーが、MSF メッセージの発信元である必要があります。それ以外の場合、SMTP スナップイン機能は電子メールをリジェクトします。

メッセージ中継の制限

電子メール・サーバーがスパミングまたはバルク・メールの大量送信に使用されるのを防ぐために、中継制限機能を使用します。この機能で、メッセージ中継の目的でご使用のシステムを使用できるユーザーを指定できます。ただし、メッセージの中継を制限する場合は、電子メールを認証することはできません。

中継の許可については、6 種類のオプションがあります。

- 「すべての中継メッセージを許可する (Allow all relay messages)」
- 「すべての中継メッセージをブロックする (Block all relay messages)」
- 「近隣ドメイン・リストにある宛先の中継メッセージだけ受け入れる (Accept relay messages for only the near domains list)」
- 「アドレス中継リストからの中継メッセージだけ受け入れる (Accept relay messages from only the address relay list)」
- 「近隣ドメイン・リストとアドレス中継リストの両方からの中継メッセージを受け入れる (Accept relay messages using both the near domains and address relay lists)」
- 「指定された期間 POP クライアントからの中継メッセージを受け入れる (Accept relay messages from POP clients for a specified period of time)」

現状では、「**TLS/SSL も認証も行わない (TLS/SSL and no authentication will be done)**」オプションを選択した場合のみ、中継を制限できます。System i ナビゲーターでは、SMTP プロパティーを指定したときに、このオプションが「認証」ページに表示されます。

インターネットに電子メールを送信できるユーザーを指定するには、以下のステップを実行してください。

1. System i ナビゲーターで、「**ユーザーのシステム**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」と展開します。
2. 「**SMTP**」を右ボタンでクリックし、「**プロパティー**」を選択します。

3. 「**リレーの制限 (Relay Restrictions)**」タブをクリックします。
4. ここに表示されるオプションの中から、適切なリレーの制限を選択します。

   注: 「**近隣ドメイン・リストにある宛先のリレー・メッセージだけ受け入れる (Accept relay messages for only recipients in the near domains list)**」または「**近隣ドメイン・リストとアドレス・リレー・リストの両方からのリレー・メッセージを受け入れる (Accept relay messages using both the near domains and address relay lists)**」を選択する場合は、次に「**一般**」タブをクリックして、中継の受け入れ先の近隣ドメインをリストします。
5. 「**OK**」をクリックします。

関連概念

11 ページの『電子メールへのアクセスの制御』
電子メールを通じて誰がシステムにアクセスするかを制御して、悪意のある攻撃からデータを保護する必要があります。

関連タスク

29 ページの『ローカルおよび中継のための電子メールの認証』
電子メールの送信において認証を必須とすることにより、ご使用のサーバーでスパムを防ぐことが可能になりました。メッセージの中継を制限する場合は、認証を必須にすることはできません。ご使用のサーバーに対して認証をセットアップすることをお勧めします。

関連資料

SMTP 属性の変更 (CHGSMTPA)

Post Office Protocol クライアントからの中継メッセージを受け入れる

中継制限のオプションの 1 つによって、 Post Office Protocol (POP) クライアントが POP サーバーにログオンした後、指定の期間だけ Simple Mail Transfer Protocol (SMTP) を使用してメッセージを中継できるようになります。

この機能を一般に POP before SMTP と呼びます。これは特に動的 IP アドレスを使用するモバイル端末で仕事をする人にとって便利な機能です。動的 IP アドレスをセキュリティー検査する際、固定 IP アドレスを使用する検査機能は有効でないためです。モバイル端末で仕事をする人が POP サーバーへの認証を一度行えば、指定の期間 (15 から 65535 分) に渡って再度認証を行うことなく電子メールを送信できるようにすることができます。

例えば、リモート・ユーザーが POP サーバーにログオンした後、 4 時間 (240 分) に渡って SMTP サーバーを使用したメッセージの中継を実行できるようにシステムを構成することなどができます。 今回は、モバイル端末で仕事をする人が POP サーバーにログオンして自分の電子メールを受信する例を考えてみます。まず、POP サーバーがこのユーザーの IP アドレスとタイム・スタンプを待ち行列に記録します。 1 時間後、同じユーザーが電子メール・メッセージを送信するとします。ユーザーが SMTP を使用して電子メール・メッセージを送信すると、 SMTP サーバーは待ち行列を検査して、そのユーザーが設定された期間内に POP サーバーにアクセスして電子メールを受信しているかどうかを検査します。ユーザーの確認が取れた場合、SMTP サーバーは電子メール・メッセージを SMTP クライアントに中継し、電子メールの受信側に配信します。

注: 電子メール・サーバーにアクセス可能なユーザーをより細かく制御したい場合には、中継制限機能と接続制限機能を組み合わせて使用することができます。例えば、特定のユーザー・グループに対して電子メール・サーバーへの接続を制限しながら、そのグループ内の特定の POP クライアントに対しては SMTP サーバーを使用した電子メール・メッセージの送信を許可するようにしたい場合などがあります。

POP クライアントが指定の期間だけメッセージを中継できるようにするには、以下のステップを実行します。

1. System i ナビゲーターで、「**ユーザーのシステム**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」と展開します。
2. 「**SMTP**」を右ボタンでクリックし、「**プロパティー**」を選択します。
3. 「**リレーの制限 (Relay Restrictions)**」タブをクリックします。
4. 「**メッセージ中継の許可 (Allow relay messages)**」で「**指定**」を選択します。
5. 「**POP クライアントから指定期間 (15 から 65535) だけ (From the POP client for the following duration (15 - 65535))**」を選択して時間値を入力し、クライアントに SMTP サーバーを使用したメールの送信を許可する分数を指定します。
6. 「**OK**」をクリックします。

中継制限機能と接続制限機能の併用

i5/OS オペレーティング・システムでは、中継制限機能と接続制限機能を併用することで、だれが電子メール・サーバーにアクセスできるのかを慎重に制御することができます。

特定のユーザー・グループに対して電子メール・サーバーへの接続を制限しながら、そのグループ内の特定の Post Office Protocol (POP) クライアントに対しては SMTP サーバーを使用した電子メール・メッセージの送信を許可するようにすることができます。

例えば、ある特定範囲の IP アドレス内にいるユーザーが日常的にスパム電子メールを送信していることが分かっているとします。その場合、その範囲内にあるアドレスからの電子メール・サーバーへの接続を制限する必要が出てきます。しかし、その IP アドレスの範囲内の一部に関しては i5/OS のトラステッド・ユーザーであることが分かっているため、それらの i5/OS ユーザー・プロファイルを持つユーザーについては、 POP サーバーへのログオン後、指定の期間だけメッセージの中継を許可する必要があります。

幸い、接続制限機能を使用して特定範囲の IP アドレスの接続を制限しながら、中継制限機能を使用して、その制限範囲内の特定のトラステッド・ユーザー (POP クライアント) には Simple Mail Transfer Protocol (SMTP) サーバーを使用した電子メールの送信を許可するようにすることができます。 i5/OS オペレーティング・システムは、まずシステムが POP クライアントに対して指定の期間だけメッセージの中継を許可するように構成されているかどうかを検査します。 次に、接続の制限があるかどうかを検査します。 i5/OS のこの機能により、だれが SMTP サーバーを使用してメッセージを中継できるのか、そしてだれが電子メール・サーバーに接続することができるのかを細かく制御することができます。

| 接続制限機能と中継制限機能を併用する場合は、SMTP 属性の変更 (CHGSMTPA) CL コマンドで
| OVRRJTNNL(*YES) (拒否接続リストの指定変更) を指定する必要があります。このパラメーターを使用す
| ると、POP サーバー認証機能が接続制限構成を指定変更できるようになります。後日、被制限グループ内
| の POP クライアントに電子メール・サーバーの使用を許可する中継制限を取り消す必要が出てくる場合が
| あります。その場合は、CHGSMTPA コマンドで OVRRJTNNL(*NO) を指定する必要があります。

関連タスク

34 ページの『接続制限』
システムの安全を確保するには、電子メール・サーバーを悪用する可能性のあるユーザーからの接続を防ぐ必要があります。

関連資料

| SMTP 属性の変更 (CHGSMTPA)

接続制限

システムの安全を確保するには、電子メール・サーバーを悪用する可能性のあるユーザーからの接続を防ぐ必要があります。

好ましくないユーザーがシステムに接続して、不正なメールを送信することがあるかもしれません。 こうした不正な電子メールは、処理装置のサイクルおよびスペースを大いに占有します。また、こちら側のシステムが不正なメールの他のシステムへの受け渡しを許可している場合でも、こちら側のシステムから送られるメールの受け取りを別のサーバーが拒否することもあります。

好ましくない既知のユーザーの IP アドレスを指定することもできますし、Realtime Blackhole List (RBL) サーバーを持つホストに接続することもできます。これらの Realtime Blackhole List は、不正なメールを送信している既知の IP アドレスのリストを提供しています。

既知の IP アドレスを指定する、あるいは Realtime Blackhole List を持つホストを指定するには、以下の手順に従ってください。

1. System i ナビゲーターで、「**ユーザーのシステム**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」と展開します。
2. 「**SMTP**」を右ボタンでクリックし、「**プロパティー**」を選択します。
3. 「接続の制限 (Connection Restrictions)」ページをクリックします。
4. 「**追加**」をクリックし、使用したい Realtime Blackhole List を持つサーバーのホスト名を追加します。
5. 「**追加**」をクリックし、接続試行を制限する特定の IP アドレスを追加します。
6. 「**OK**」をクリックします。

関連概念

11 ページの『電子メールへのアクセスの制御』
電子メールを通じて誰がシステムにアクセスするかを制御して、悪意のある攻撃からデータを保護する必要があります。

関連タスク

33 ページの『中継制限機能と接続制限機能の併用』
i5/OS オペレーティング・システムでは、中継制限機能と接続制限機能を併用することで、 だれが電子メール・サーバーにアクセスできるのかを慎重に制御することができます。

ウィルスの拡散を防ぐための電子メールのフィルター操作

電子サーバーに侵入する恐れのあるウィルスが拡散するのを防ぐために、着信電子メールに特定の件名、タイプ、ファイル名、および発信元アドレスが含まれていないかどうかを調べるフィルターを作成できます。こうして、電子メールを検疫または廃棄することができます。

ウィルス対策のフィルターを掛けると、疑わしい電子メールは、管理者によって設定されたパラメーターに基づいて自動的に隔離または廃棄されます。電子メールは、以下の基準のうちどれでも、あるいはすべてによって、フィルターに掛けることができます。

1. **アドレス** - 個別またはドメイン
2. **件名** - ILOVEYOU
3. **添付ファイル名** - lovebug.vbs あるいは *.vbs
4. **MIME タイプ** - image/* あるいは image/jpg

値にはワイルドカード文字を含めることができます。1 つのワイルドカード文字が 1 つのアスタリスク (*) で、これによって 1 つまたは複数の任意の文字がワイルドカードのその位置に存在する可能性がある

ことを示します。例えば、*.vbs を使って、拡張子 .vbs を持つファイル名をチェックすることができます。*@us.ibm.com という発信元は、米国内の IBM からのすべてのメールをフィルターに掛け、image/* のフィルターは、すべてのサブタイプのなかでタイプがイメージであるものをフィルターに掛けます。

フィルターを作成するには、以下の手順に従ってください。

1. System i ナビゲーターで、「**ユーザーのシステム**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」と展開します。
2. 「**SMTP**」を右ボタンでクリックし、「**プロパティー**」を選択します。
3. 「フィルター」ページを選択します。
4. 「**メッセージの保持 (Keep message)**」または「**メッセージの廃棄 (Discard message)**」を選択します。「**メッセージの保持 (Keep message)**」を選択すると、メッセージのコピーは保管されるものの、これが宛先に送信されることはありません。
5. 「**追加**」をクリックし、ウィルスが含まれているかもしれないメッセージを識別する基準を指定します。この基準に合致するメッセージは、宛先に送信されません。
6. 「**OK**」をクリックして、変更を保管します。

上記のツールに加え、補足的なアンチウィルス・ソリューションをインプリメントする必要があります。

電子メールの送受信

ご使用のシステムはメール・サーバーで、ここに電子メール・ユーザー (SNADS、POP、または Lotus ユーザー) が登録されています。電子メール・ユーザーは、POP クライアントまたは SNADS クライアントのいずれかを使用して電子メールの送信、受信および読み取りを行うことができます。

| ユーザーは、MIME メールの送信 (QtmmSendMail) API または MIME メールの作成および送信
| (QtmsCreateSendEmail) API を使用して、i5/OS プログラムから電子メールを送信できます。
| QtmsCreateSendEmail API を使用すると、ユーザーは secure/MIME を使用して MIME 文書に署名し、それを暗号化できます。secure/MIME とは、MIME プロトコルの機密保護機能があるバージョンです。プログラム経由で電子メールを送信する手段として推奨されているのは、QtmsCreateSendEmail API です。

| 加えて、ユーザーは、次の異なる方法で電子メールを送受信できるようになります。

関連概念

2 ページの『電子メールの概念』
電子メール (E-mail) は、必要不可欠なビジネス・ツールとなっています。i5/OS オペレーティング・システムでは、Simple Mail Transfer Protocol (SMTP) や Post Office Protocol (POP) などのプロトコルを使用し、電子メールがネットワーク上で円滑かつ効率的に行き来するようにします。

関連タスク

22 ページの『電子メール・ユーザーの登録』
電子メール・ユーザーを登録するには、 ユーザー・プロファイルを作成する必要があります。

関連資料

API または MIME メールの作成および送信 (QtmsCreateSendEmail) API

MIME メール送信 (QtmmSendMail) API

Post Office Protocol 電子メール・クライアントのセットアップ

Post Office Protocol (POP) サーバーを使用して電子メールを受信および保管する場合は、まず電子メール・クライアントをセットアップする必要があります。

ご使用のシステムでは、電子メールのストア・アンド・フォワードに POP サーバーを使用しています。電子メール・クライアントは POP サーバーと協働して、クライアント側のユーザーのために電子メールの受信と保管を行います。POP をサポートする電子メール・クライアントは、Eudora、Outlook Express、および Lotus Notes® など多数あります。クライアントを構成するための手順は、各クライアントのインターフェースに応じて異なります。 ただし、指定する必要のある情報は同じです。 ここでは、Outlook Express を例として取り上げます。

1. POP 電子メール・クライアント・プログラム情報を収集します。
   - ユーザー ID および完全修飾ドメイン名 (ホスト名とドメイン名)。 これは、ユーザーのメール受信用の電子メール・アドレスであり、通常は、userID@hostname.domainname の形式で指定します。

     注: クライアントの中には、ホスト・アドレスを何度も入力しなければならないものもあります。メール受信用の POP サーバーのホストの指定、メール送信用の SMTP のホストの指定、および宛先に対する電子メール送信者の確認などで入力が必要になります。
   - POP ユーザーまたはアカウント名。これは、i5/OS ユーザー・プロファイル名と同じです。
   - ユーザー・パスワード。このパスワードは、i5/OS ユーザー・プロファイル・パスワードと同じでなければなりません。
2. ユーザーおよびユーザーの設定を確認します。例えば、Outlook Express では、「**ツール**」 → 「**アカウント**」をクリックし、「**メール**」タブで、ユーザーおよびユーザー設定の情報を確認します。
   - ユーザー名。これは、i5/OS ユーザー・プロファイル名です。
   - ユーザーの電子メールのアドレス。これはユーザー ID と完全修飾ドメイン名です。
   - 応答先アドレス。これは、ネットワーク管理者が指定するユーザーの電子メール・アドレスと同じにすることができますが、i5/OS ユーザー・プロファイルがシステムに存在している必要があります。
3. 発信メール (SMTP) サーバーを確認します。電子メール・クライアントで SMTP サーバーを識別する必要があります。なぜなら、SMTP サーバーは、クライアントのユーザーにメール送信を許可するサーバーだからです。例えば、Outlook Express では、「**ツール**」 → 「**アカウント**」をクリックし、電子メールのアカウントを選択して「**プロパティ**」をクリックします。「**サーバー**」タブをクリックして、SMTP サーバーを確認します。
   - POP ユーザーまたはアカウント名。これは、ユーザーの電子メール・アドレスのユーザー ID です。また、i5/OS ユーザー・プロファイル名でもあります。
   - 発信メール (SMTP) サーバー。これは、システム・ホスト名です。
4. 着信メール (POP) サーバーを確認します。例えば、Outlook Express では、「**ツール**」 → 「**アカウント**」をクリックし、電子メールのアカウントを選択して「**プロパティ**」をクリックします。「**サーバー**」タブをクリックして、POP サーバーを確認します。
   - 着信メール・サーバー。これは、システム・ホスト名です。
5. TLS/SSL を使用するようにクライアント・プログラムを構成します。例えば、Outlook Express では、次の手順に従って構成してください。
   a. 「**ツール**」 → 「**アカウント**」をクリックし、電子メール・アカウントを選択します。
   b. 「**プロパティ**」をクリックし、「**サーバー**」タブをクリックします。
   c. 「**このサーバーは認証が必要**」を選択し、「**設定**」をクリックします。
   d. 「**受信メールサーバーと同じ設定を使用する**」を選択し、「**OK**」をクリックします。
   e. 「**詳細設定**」タブをクリックし、受信 (POP) メール・サーバーと送信 (SMTP) メール・サーバーの両方で「**このサーバーはセキュリティで保護された接続 (SSL) が必要**」を選択します。「**OK**」をクリックします。
   f. 「**適用**」、次に「**OK**」をクリックして、「プロパティ」ウィンドウを閉じます。

JavaMail

JavaMail を使用して、電子メールのクライアント・アプリケーションを開発できます。

JavaMail API は、Java™ テクノロジーを基にした電子メール・クライアント・アプリケーションを作成するのに使用できる、プラットフォームからもプロトコルからも独立したフレームワークを提供します。JavaMail API を使用すると、マルチメディア・メール・メッセージの送信、および Internet Mail Access Protocol (IMAP) のインプリメンテーション (フォルダー、認証、および添付ファイルの処理をサポート) を使用可能にできるメール・クライアントを作成することが可能です。

SMTP は文字データしかサポートしないため、定形式テキスト、ファイル添付 (テキストおよびバイナリー)、およびマルチメディア・コンテンツなどの複雑なデータを表現するには MIME を使用します。MIME メールの送信 (QtmmSendMail) API を使用する場合は、ユーザーのアプリケーションで、データを適切なコンテンツに変換するようにしなければなりません。JavaMail インプリメンテーションは、統合 MIME 処理機能を提供します。

JavaMail コンポーネントは、IBM Developer Kit for Java の一部として組み込まれています。

関連概念

JavaMail

スプール・ファイルの PDF ファイルとしての送信

スプール・ファイルを Adobe PDF に送信し、その文書を電子メールで配布することができます。

IBM Infoprint® Server for iSeries™ ライセンス・プログラム (5722-IP1) を使用して、任意の i5/OS 出力から AdobePDF ファイルを生成できます。この生成された PDF ファイルを、電子メールの添付ファイルとして送信することができます。1 つのアドレスに対して単一のスプール・ファイルを送信できます。1 つのスプール・ファイルをいくつかの PDF に分割して、それぞれを別のアドレスに送ることもできます。この方式を使えば、顧客宛ての送り状をそれぞれ異なる PDF ファイルに送信し、該当する送り状をそれぞれの顧客の電子メール・アドレスに送信することが可能です。この出力方式を使用するには、IBM Infoprint Server for iSeries ライセンス・プログラムが必要です。

関連情報


InfoPrint Server User's Guide PDF


IBM eServer iSeries Printing Redbooks VI -- The Output of e-business

アドレスとして Lightweight Directory Access Protocol を使用する

Lightweight Directory Access Protocol (LDAP) を使用して、システム配布ディレクトリーを基にした共通アドレス帳を提供することができます。

| IBM Tivoli® Directory Server for i5/OS (IBM の LDAP の実装) を使用して、以前 MAPI によって提供さ
| れた機能を置き換えることができます。LDAP を使用すれば、すべてのユーザーがクライアント・アプリ
| ケーションから使用できる単一のアドレス帳を提供することができます。

LDAP を使用するには、次のタスクを実行してください。

1. Directory Server を開始します。
2. Directory Server に情報を公開します。

3. メール・クライアントを、LDAP を使用するように構成する。このタスクを完了するステップは、メール・クライアント (例えば、Netscape または Eudora) によって異なります。メール・クライアントのプロパティーを編集して、メール・アドレッシングに使用するディレクトリー・サーバー (Directory Server) として LDAP サーバーを指定します。

関連タスク

ディレクトリー・サーバーの開始

ディレクトリー・サーバーに情報を公開する

関連資料

IBM Tivoli Directory Server for i5/OS (LDAP)

システム・ネットワーク体系 (SNA) 配布サービスを使用した電子メールの送信

システム・ネットワーク体系 (SNA) 配布サービス (SNADS) クライアント・プログラムを使用して、ご使用のシステムから電子メールを送信できます。電子メールの送信者は、ローカルな SNADS ユーザーでなければなりません。

前提条件

ローカル SNADS ユーザーは、ローカル・システム配布ディレクトリー項目に登録される必要があるため、ユーザー・プロファイルが必要になります。ローカル SNADS 電子メール・ユーザーを登録するには、『電子メール・ユーザーの登録』を参照してください。

電子メールを送信するには、次の手順に従ってください。

1. i5/OS 文字ベース・インターフェースで、SNDDST (配布の送信コマンド) と入力し、Enter (キー) を押します。
2. F10 を押して、すべてのパラメーターを表示させます。
3. 最初のプロンプトの「*送信する情報*」に *LMSG と入力して、実行キーを押します。
4. 受信者のユーザー ID サーバー・アドレス、または IP アドレスを入力します。
5. 「*記述*」プロンプトにメッセージの説明を入力します。
6. Page Down キーを押して、「*長いメッセージ*」プロンプトに電子メールを入力します。
7. 実行キーを押して、電子メールを送信します。

注: 配布の送信 (SNDDST) コマンドを使用してメールを送信する場合には、IP アドレスも使用することができます。

関連タスク

22 ページの『電子メール・ユーザーの登録』
電子メール・ユーザーを登録するには、 ユーザー・プロファイルを作成する必要があります。

41 ページの『システム・ネットワーク体系 (SNA) 配布サービスを使用した電子メールの受信』
システム・ネットワーク体系 (SNA) 配布サービス (SNADS) クライアント・プログラムを使用して、ご使用のシステムで電子メールを受信できます。電子メールの受信側は、 ローカルな SNADS ユーザーでなければなりません。

宛先を区別するためのヘッダーのセットアップ

配布属性の変更 (CHGDSTA) コマンドを使うと、メール配布のメッセージ・サービス属性 (X.400 サポート) の内容を変更できます。

宛先の保持 (KEEPRCP) パラメーターを使うと、どの宛先情報を保管あるいは送信するかを、各メール配布ごとに指定することができます。 このパラメーターの設定は、SNDDST のメモに対して、どのように MIME ヘッダーが作成されるかに影響します。

CC タグと BCC タグが MIME ヘッダー (およびクライアントの画面) に現れるようにするには、KEEPRCP パラメーターを *ALL に設定する必要があります。 BCC 宛先は、このパラメーターの設定に関係なく、表示されません。それが BCC 宛先の目的です。 TO 宛先と CC 宛先は、SNDDST のメモのテキストに現れます。

Multipurpose Internet Mail Extension コンテンツ・タイプ

標準インターネット・テキスト注記は、汎用ヘッダーとテキスト本文とで成り立っています。 しかし、Multipurpose Internet Mail Extension (MIME) 注記は、複数パーツから成り立っている場合があり、これによりテキストにマルチメディア添付ファイルを含めることができます。

汎用ヘッダーにコンテンツ・タイプとして `Multipart/Mixed` が含まれていたら、1 つ以上の添付ファイルが続いています。各添付ファイルには、先頭と末尾の境界があります。 境界の ID は、Content-Type ヘッダー・タグに続く *boundary*= パラメーターで設定されます。 複数パーツ MIME 注記の例を図 1 に示します。 この例では、各パーツにコンテンツ・タイプがあり、各テキスト・コンテンツ・タイプには、オプションで文字セット (charset) を定義できます。

```
     From
@SYSNAM6.CITY.COMPANY.COM:popct08@SYSNAM6.city.company.com Wed
Jan 10
11:33:18 1996 Return-Path:
<@SYSNAM6.CITY.COMPANY.COM:popct08@SYSNAM6.city.company.com> Received: from
SYSNAM6.city.company.com by
fakeps2.city.company.com (COMPANY
          OS/2 SENDMAIL VERSION 1.3.2)/1.0) id AA0329; Wed, 10
Jan 96 11:33:18 -0500 Date: Wed, 10
Jan 96
11:33:18 -0500 Message-Id: <9601101633.AA0329@fakeps2.city.company.com> Received:
  from endmail9 by SYSNAM6.CITY.COMPANY. (IBM i5/OS SMTP V03R02M00) with TCP;
Wed, 10
Jan 1996 10:23:42
+0000. X-Sender: popct08@SYSNAM6.city.ibm.com (Unverified) X-Mailer: Windows
Eudora Pro
Version 2.1.2
Mime-Version:1.0Content-Type:multipart/mixed;boundary="=====================_821301929==
 _"
To: fake@fakeps2.city.company.com From:
endmail9 <popct08@SYSNAM6.city.company.com> Subject:
eudora attachments
X-Attachments:C:¥EUDORA¥ARGYLE.BMP;--=====================_821301929==_
Content-Type: text/plain; charset=

 "us-ascii" An example of using Eudora to send a text
andbitmap.--=====================_821301929==_
Content-Type: application/octet-stream; name="ARGYLE.BMP";
x-mac-type="424D5070"; x-mac-creator="4A565752"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=


"ARGYLE.BMP"
Qk12AgAAAAAAAHYAAAAoAAAAIAAAACAAAAABAAQAAAAAAAACAAAAAAAAAAAAAAAAAAAQAAAAAAAA
AAAAgAAAgAAAAICAAIAAAACAAIAAgIAAAICAgADAwMAAAAD/AAD/AAAA//8A/wAAAP8A/wD//wAA
////AE1ERERERERERZERERERERE1E1ERERERERsZERERERETURE1EREREGxsZERERERNRERE1ERE
REbGxsZERERE1ERERE1ERERsbGxsZERETURERERE1ERGxsbGxsZERNRERERERE1EbGxsbGxsZE1E
RERERERE1sbGxsbGxsbURERERERERG1sbGxsbGxtZERERERERbG1sbGxsbG1sZERERERERsbG1s
bGxsbWxsZERERERGxsbG1sbGxtbGxsZERERbGxsbG1sbG1sbGxsZERERsbGxsbG1sbWxsbGxsZE
RGxsbGxsbG1tbGxsbGxsZEbGxsbGxsbG1sbGxsbGxsZEbGxsbGxsbW1sbGxsbGxkREbGxsbGxtbG
1sbGxsbGREREbGxsbG1sbG1sbGxsZEREREbGxsbWxsbG1sbGxkREREREbGxtbGxsbG1sbGREREREE
REbG1sbGxsbG1sZERERERERERbWxsbGxsbG1kRERERERERNbGxsbGxsbG1ERERERERE1EbGxsbGxs
ZE1ERERERETUREbGxsbGxkRE1ERERERNREREbGxsbGRERE1ERERE1EREREbGxsZERERE1ERETURE
REREbGxkRERERE1ERNREREREREbGREREREREE1E1ERERERERERZERERERERE3UREREREREREREREREREREREREREREREE--=====================_821301929==_--
```

図 2. 複数パーツ MIME 注記の例

SNDDST コマンドの IP アドレスのサポート

「*Internet Recipient*」プロンプトにインターネット電子メール・アドレスを入力すると、SNDDST コマンドで電子メールをインターネットに送信できます。

ご使用のネットワークで、SNA 配布サービス (SNADS) およびオフィス・アプリケーションを使用して電子メールのやりとりをしている場合は、ユーザーが配信の送信 (SNDDST) コマンドを使用して IP アドレスを使用できるように、電子メール・システムを構成する必要があります。

次の手順に従って、メール・システムを構成します。

1. i5/OS 文字ベース・インターフェースに次のように入力します。ADDDIRE USRID(INTERNET GATEWAY) USRD('Allow SNDDST to send INTERNET Mail') SYSNAME(INTERNET) MSFSRVLVL(*USRIDX) PREFADR(NETUSRID *IBM ATCONTXT)
2. CHGDSTA SMTPRTE(INTERNET GATEWAY) と入力し、実行キーを押します。

これで、SNADS ユーザーは、「*Internet Recipient*」プロンプトにインターネット電子メール・アドレスを入力することにより、SNDDST コマンドで電子メールをインターネットに送信できるようになりました。

関連情報

AS/400 Electronic-Mail Capabilities Redbook

ファイルの添付

SNDDST に示したコマンドを使用して電子メールを送信する場合、電子メールと共にファイルまたは文書を送信することもできます。

配布の送信 (SNDDST) コマンドを使用して、添付ファイルまたは文書と一緒に電子メールを送信できます。SNDDST で一度に送信できる文書またはファイルは 1 つだけです。複数の添付ファイルを送信したい場合は、MIME メール送信 (QtmmSendMail) API を使用して MIME メールを送信してください。

電子メールに文書を添付して送信するには、文字ベースのインターフェースに次のように入力します。

```
SNDDST TYPE(*DOC) DSTD(your description) TOUSRID(anyuser) DOC(yourdoc) FLR(yourfolder)
```

電子メールにファイルを添付して送信するには、文字ベースのインターフェースに次のように入力します。

```
SNDDST TYPE(*FILE) DSTD(description) TOUSRID(any user)
MSG(message optional) DOCFILE(youlib/yourfile) DOCMBR(yourmbr)
```

エラー・メッセージを受け取る場合は、配布の送信 (SNDDST) コマンドと互換性のない形式のファイルまたは文書を送信しようとしている可能性があります。i5/OS CL CPY コマンドを使用すると、ファイルを SNDDST コマンド互換のファイルまたは文書に変換できます。

SNDDST を使って送信する場合のファイル・タイプの変換

スプール・ファイルが既に作成されており、物理ファイルとフォルダーが既に存在しているとすると、ファイルを送信で必要とされる形式に変換する必要があります。

1. スプール・ファイルをデータベース物理ファイルに移動する。

   ```
   CPYSPLF  FILE(splfile)  TOFILE(dbfile)  JOB(job3/job2/job1) SPLNBR(splnbr) TOMBR(mbr)
   ```

2. 物理データベース・ファイルをフォルダーに移動する。

   ```
   CPYTOPCD  FROMFILE(lib/dbfile)  TOFLR(folder) FROMMBR(mbr)  REPLACE(*YES)
   ```

3. 文書を送信する。

   ```
   SNDDST  TYPE(*DOC)  TOUSRID(user address) DSTD(MAIL) DOC(mbr)  FLR(folder)
   ```

   関連資料

   MIME メール送信 (QtmmSendMail) API

システム・ネットワーク体系 (SNA) 配布サービスを使用した電子メールの受信

システム・ネットワーク体系 (SNA) 配布サービス (SNADS) クライアント・プログラムを使用して、ご使用のシステムで電子メールを受信できます。電子メールの受信側は、ローカルな SNADS ユーザーでなければなりません。

電子メールを受信するには、次の手順に従ってください。

1. 文字ベースのインターフェースに、QRYDST (配布の照会コマンド) と入力して F4 を押します。配布のリストが表示されます。
2. F10 を押して、追加のパラメーターを表示します。
3. 「**出力を受け取るファイル**」フィールドに、覚えやすいファイルおよびライブラリー名を入力し、実行キーを押します。システムはこれらの物理ファイルを作成します。

4. WRKF (ファイルの処理コマンド) と入力し、実行キーを押します。「ファイル処理」画面が表示されます。
5. ステップ 3 で指定したファイル名およびライブラリーを入力し、F4 を押します。
6. 画面に、すべての配布 (電子メール) がリストされます。表示したい配布の隣に 5 と入力し、実行キーを押します。
7. 「物理ファイル・メンバーの表示 (Display Physical File Member (DSPPFM))」表示画面で実行キーを押します。
8. 次の表示画面に、メールごとに、数字から成る長ストリングがあります。 7 番目から 26 番目の文字をコピーします。
9. F3 を 2 回押して終了します。
10. RCVDST (配布の受信コマンド) と入力し、実行キーを押します。
11. 「**配布識別コード**」フィールドに、コピーした 7 番目から 26 番目の文字を貼り付けます。
12. 「**出力を受け取るファイル**」フィールドに、新しいファイル名と、先に使用したのと同じライブラリー名を入力し、実行キーを押します。
13. 「DSPPFM」(物理ファイル・メンバーの表示 (Display Physical File Member)) と入力して、今作成したファイルを表示します。
14. F20 (Shift + F8) を押して左にスクロールさせ、メッセージを読みます。

関連タスク

38 ページの『システム・ネットワーク体系 (SNA) 配布サービスを使用した電子メールの送信』
システム・ネットワーク体系 (SNA) 配布サービス (SNADS) クライアント・プログラムを使用して、ご使用のシステムから電子メールを送信できます。電子メールの送信者は、 ローカルな SNADS ユーザーでなければなりません。

電子メールの管理

熟練したユーザーまたは管理者が、電子メール・サーバー、ユーザー、およびメッセージを管理し、ご使用のネットワーク内で電子メールが確実に配布されるようにすることができます。

電子メール・サーバーの検査

電子メール関連の最も一般的な問題の 1 つに、適切なサーバーが開始しないという問題があります。電子メール・サーバーを使用する前に、その電子メール・サーバーの状況を検査し、それらがすべて稼働中であることを確認する必要があります。

サーバーの状況を確認するには、次の手順を実行してください。

1. System i ナビゲーターで、**「ユーザーのシステム」** → **「実行管理機能」** → **「サーバー・ジョブ」**の順に展開します。
2. SMTP サーバーが活動状態であることを検査します。「活動状態サーバー・ジョブ (Active Server Jobs)」リストの「ジョブ名」列で **Qtsmtp** ジョブを探します。
3. **Qtsmtp** ジョブがリストされていない場合は、SMTP サーバーを開始を行います。
4. メール・サーバー・フレームワーク・サーバーが活動状態であることを検査します。「活動状態サーバー・ジョブ (Active Server Jobs)」リストの「ジョブ名」列で **Qmsf** ジョブを探します。
5. Qmsf ジョブがリストされていない場合は、文字ベースのインターフェースで、STRMSF (メール・サーバー・フレームワークの開始コマンド) と入力します。

6. POP サーバーが活動状態であることを検査します。「活動状態サーバー・ジョブ (Active Server Jobs)」リストの「ジョブ名」列で **Qtpop** ジョブを探します。
7. **Qtpop** ジョブがリストされていない場合は、POP サーバーを開始を行います。
8. SNADS サーバーが活動状態であることを検査します。「活動状態サーバー・ジョブ (Active Server Jobs)」リストの「ジョブ名」列で **Qsnads** ジョブを探します。
9. QSNADS ジョブがリストされていない場合は、SNADS を開始します。文字ベース・インターフェースで、`STRSBS QSNADS` と入力します。

電子メールを稼動させるには、すべての電子メール・サーバーが始動されている必要があります。

関連概念

23 ページの『電子メール・サーバーの開始および停止』
必要なサーバーを開始して、すべてが正しく作動していることと、 変更した構成が有効になっていることを確認します。そのために、サーバーの再始動が必要な場合もあります。 サーバーを停止してから、サーバーの開始のステップを再度実行することによって、サーバーを再始動できます。

55 ページの『電子メールの問題判別』
簡単な手順で、電子メールの問題の原因を判別することができます。

Post Office Protocol 電子メール・ユーザーの除去

System i ナビゲーターを使用して、Post Office Protocol (POP) 電子メール・ユーザーを除去できます。

オペレーティング・システムから電子メール・ユーザーを除去するには、システム配布ディレクトリー項目を削除しなければなりません。

1. 文字ベース・インターフェースで、WRKDIRE (ディレクトリー項目の処理コマンド) と入力します。
2. 削除したいユーザーの「*Opt*」フィールドまで、タブ・キーを使って移動します。
3. 4 (削除) とタイプし、実行キーを押します。実行キーをもう 1 回押して、確認します。これで、電子メールがそのユーザーの POP メールボックスに送達されなくなります。
4. このユーザーとして、POP メール・クライアント・プログラムにサインオンします。すべての電子メールを受信および削除します。

大きなサイズの電子メール・メッセージの分割の防止

大きなサイズの電子メール・メッセージがより小さく紛らわしい断片に分割して送信されるのを防ぐことが必要な場合があります。

Simple Mail Transfer Protocol (SMTP) は、大きなサイズのメッセージを小さく分割して構成することができます。ただし、多くのメール・クライアントはこれらの部分を再組み立てすることができないために、メッセージが読めないという結果になります。大きいサイズのメッセージがいくつかの部分に分断されていて、メッセージの宛先がそのメッセージを読めないということがわかった場合には、SMTP の分割機能を使用不可にすることもできます。

SMTP 電子メールを分割しないようにするには、次の手順に従ってください。

1. System i ナビゲーターで、**「ユーザーのシステム」** → **「ネットワーク」** → **「サーバー」** → **「TCP/IP」**と展開します。
2. **「POP」**をダブルクリックします。「POP プロパティー」ダイアログが表示されます。
3. **「構成」**タブをクリックします。
4. **「メッセージ分割サイズ」**フィールドで、**「無限大」**を選択します。

注: 電子メール・メッセージの分割をオフにすると、大きなサイズのメッセージを処理できないネットワークに大きなサイズの電子メールを送信した場合に、問題が発生する可能性があります。

関連概念

55 ページの『電子メールのトラブルシューティング』
この情報は、起こりうる電子メール関連の問題の解決に役立つことを目的としています。

電子メールの配信状況を受け取る

ユーザーが発信メールの送信状況に関するメッセージを受け取ることを希望している場合、Delivery Status Notification 機能を使用可能にする必要があります。

Delivery Status Notification を使用すると、電子メール・クライアントは、電子メールの送信、中継、または失敗時に状況メッセージを受け取ることができます。電子メール・クライアントがこの要求を行えるようにするには、Delivery Status Notification を使用可能にする必要があります。

この作業で可能になるのは、ユーザーに対して Delivery Status Notification を使用可能にすることのみです。ユーザーが Delivery Status Notification 機能を有効にするには、ユーザー各自が使用しているメール・クライアントでパラメーターを設定する必要があります。パラメーターは、メール・クライアントごとに異なります。

Delivery Status Notification を使用可能にするには、次のステップを実行してください。

1. System i ナビゲーターで、「**ユーザーのシステム**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」と展開します。
2. 「**SMTP**」を右ボタンでクリックし、「**プロパティー**」を選択します。
3. 「追加パラメーター」ページをクリックします。
4. 「**Delivery Status Notification (DSN) のサポート (Support Delivery Status Notification (DSN))**」チェック・ボックスを選択し、「DSN 通知責任者のアドレス (DSN notification Responsible Person address)」を指定します。
5. 「**OK**」をクリックします。

Delivery Status Notification を使用するとリソースが消費され、電子メールの受信側の最大数に影響を及ぼす可能性があります。

同一システム上で Domino と SMTP サーバーをホストする

Domino と Simple Mail Transfer Protocol (SMTP) が同一システム上で稼動している場合は、それぞれを特定の IP アドレスにバインドするように構成することをお勧めします。

同一システム上で Domino と SMTP サーバーをホスティングする時は、各サーバーをそれぞれ 1 つの IP アドレスにバインドする必要があります。 そうすれば、電子メールは適切な IP アドレスを使用して Domino あるいは SMTP のユーザーに送信され、Domino または SMTP が 1 つのポートを共用しているにもかかわらず、電子メールは意図するシステムによってのみ処理されます。

SMTP サーバーに特定の IP アドレスを使用させるには、次の手順に従ってください。

1. System i ナビゲーターで、「**ユーザーのシステム**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」と展開します。
2. 「**SMTP**」を右ボタンでクリックし、「**プロパティー**」を選択します。
3. 「**バインディング**」タブをクリックします。

4. すべてのインターフェースをポート 25 にバインドする場合は、「**すべてのインターフェースを使用 (Use all interfaces)**」ラジオ・ボタンを選択します。
5. バインドするクライアントおよびサーバーのバインド・インターフェースを指定する場合は、「**インターフェースを選択 (Select an interface)**」ラジオ・ボタンを選択します。

   注: システムまたはファイアウォールのいずれかでネットワーク・アドレス変換 (NAT) を使用する場合には、i5/OS SMTP クライアントに 1 つの特定の IP アドレスを使用させる必要があります。
6. 「**OK**」をクリックします。

これで、SMTP は、この IP アドレス宛てのメールのみを受信します。 Domain Name System (DNS) サーバー、ローカル・ホスト・テーブル、およびシステム配布ディレクトリーに、この強制された IP アドレスがあることを確認します。

Domino SMTP を特定の TCP/IP アドレスにバインドする方法については、LotusDomino Reference ライブラリー (英語) を参照してください。

関連概念

11 ページの『電子メールの計画』
電子メールをセットアップする前に、ご使用のシステムで電子メールをどのように使用するか、 基本的な計画を立てておく必要があります。

IP フィルター操作とネットワーク・アドレス変換

同一システム上で Domino LDAP と Directory Server をホストする

Domino LDAP と IBM Tivoli Directory Server for i5/OS (Directory Server) が同じシステム上で稼動している場合は、それぞれを特定の IP アドレスにバインドするように構成することをお勧めします。

Domino LDAP と Directory Server を同じシステム上でホスティングする場合は、各サーバーごとに異なるポート番号を設定することも、各サーバーを 1 つの IP アドレスにバインドすることもできます。ポート番号を変更するとクライアントを混乱させる可能性があるので、各サーバーごとに特定の IP アドレスを指定することが最良のソリューションです。Domino および Simple Mail Transfer Protocol (SMTP) はそれぞれ該当する LDAP サーバーを、電子メール・アドレッシングのために使用します。

ディレクトリー・サーバーに特定の IP アドレスを使用させるには、次の手順に従ってください。

1. System i ナビゲーターで、「**ユーザーのシステム**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」の順に選択します。
2. 「**ディレクトリー**」を右ボタンでクリックし、「**プロパティー**」を選択します。
3. 「**ネットワーク**」タブをクリックします。
4. 「**IP アドレス**」をクリックします。
5. 「**選択された IP アドレスの使用 (Use selected IP addresses)**」を選択し、バインドしたいインターフェースをリストから指定します。
6. 「**OK**」をクリックして、「ディレクトリー - IP アドレス」ページを閉じます。
7. 「**OK**」をクリックして、「ディレクトリー・プロパティー (Directory Properties)」ページを閉じます。
8. オプション: Domino LDAP を使用している場合、Domino LDAP を特定の TCP/IP アドレスにバインドする方法についての説明は、Lotus Domino Reference ライブラリーを参照してください。
9. 電子メール用のサーバーの開始

関連情報

Lotus Domino 参照ライブラリー (英語)

Simple Mail Transfer Protocol サーバーのパフォーマンス管理

マルチプロセッシングを使用する、負荷の大きい Simple Mail Transfer Protocol (SMTP) サーバーを管理するためのヒントです。

ご使用の SMTP サーバーは、それぞれの電子メール要求ごとの事前開始ジョブの追加と終了にすべての能力を使用していることが原因で、負荷が大きくなっている可能性があります。

事前開始ジョブの数がシステムのパフォーマンスに影響を与えていることが分かった場合には、このしきい値を低く設定できます。 ジョブの数を増やしたい場合には、事前開始ジョブの数を多くします。

事前開始ジョブを使用すると、すべての電子メール要求はそれ自体のジョブとして実行します。この方法により、各ジョブはそれ自体のクライアントまたはサーバー・プログラムの必要と要求にだけ集中できるようになります。 各ジョブはタイムアウト呼び出しの時間を長く設定して、大量の不正な電子メールを受信しないようにホスト名を通知できるようにすることができます。

負荷の大きい SMTP サーバーを管理するには、以下の値を変更することができます。

- 初期化の際に開始するジョブ数
- ジョブの限界値
- システムが限界値に到達したときに追加するジョブ数
- 同時に実行可能なジョブ数の最大値
- ジョブ用のサブシステムの選択

負荷の大きいシステムを管理するには、SMTP サーバーおよび SMTP クライアントの値を変更する必要があります。

SMTP サーバーは、デーモンおよび事前開始ジョブ、すなわち QTSMTPSRVD と QTMSMTPSRVP を処理します。 SMTP クライアントは、デーモンおよび事前開始ジョブ、すなわち QTSMTPCLTD と QTSMTPCLTP を処理します。

SMTP サーバーで値を変更するには、次のステップに従います。

1. 文字ベース・インターフェースで、CHGPJE (ジョブ項目変更コマンド) と入力します。
2. プロンプトに以下の値を入力し、実行キーを押します。

プロンプト	値
サブシステム	QSYSWRK
ライブラリー	QSYS
プログラム	QTMSSRCP
ライブラリー	QTCP
ジョブの開始	*SAME
ジョブ数の初期値	4
しきい値	2
追加するジョブ数	2
ジョブ数の最大値	20

上記の値は、システムが 4 つの事前開始ジョブを開始すること、使用可能なジョブが 2 を下回ると 2 つを追加して開始すること、および最大で 20 個の事前開始ジョブを許可することを保証するものです。

Simple Mail Transfer Protocol サーバーの値の変更

この手順を使用して、Simple Mail Transfer Protocol (SMTP) サーバーの値を変更してください。

1. 文字ベース・インターフェースで、CHGPJE (ジョブ項目変更コマンド) と入力します。
2. プロンプトに以下の値を入力し、実行キーを押します。

プロンプト	値
サブシステム	QSYSWRK
ライブラリー	QSYS
プログラム	QTMSSRCP
ライブラリー	QTCP
ジョブの開始	*SAME
ジョブ数の初期値	4
しきい値	2
追加するジョブ数	2
ジョブ数の最大値	20

上記の値は、システムが 4 つの事前開始ジョブを開始すること、使用可能なジョブが 2 を下回ると 2 つを追加して開始すること、および最大で 20 個の事前開始ジョブを許可することを保証するものです。

Simple Mail Transfer Protocol クライアントの値の変更

この手順を使用して、Simple Mail Transfer Protocol (SMTP) クライアントの値を変更してください。

1. 文字ベース・インターフェースで、CHGPIE (ジョブ項目変更コマンド) と入力します。
2. プロンプトの後に以下の値を入力し、実行キーを押します。

プロンプト	値
サブシステム	QSYSWRK
ライブラリー	QSYS
プログラム	QTMSCLCP
ライブラリー	QTCP
ジョブの開始	*SAME
ジョブ数の初期値	4
しきい値	2
追加するジョブ数	2
ジョブ数の最大値	20

上記の値は、SMTP クライアントが 4 つの事前開始ジョブを開始すること、使用可能なジョブが 2 を下回ると 2 つを追加して開始すること、および最大で 20 個の事前開始ジョブを許可することを保証するものです。

Simple Mail Transfer Protocol サーバー・ジョブ用新規サブシステムの選択

この手順を使用して、Simple Mail Transfer Protocol (SMTP) サーバー・ジョブ用の新規サブシステムを選択してください。

1. SMTP サーバーに別個のサブシステムを指定できます。 これにより、リソースを共用する必要性がなくなるので、パフォーマンスが向上するはずです。
2. 別個のサブシステムを指定するには、以下の手順を実行します。
   a. System i ナビゲーターで、「**ユーザーのシステム**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」と展開します。
   b. 「**SMTP**」を右ボタンでクリックし、「**プロパティー**」を選択します。
   c. 「**追加パラメーター**」タブをクリックします。
   d. 「**サブシステム記述**」ラジオ・ボタンを選択します。
   e. 新しいサブシステムの名前を入力し、サブシステム記述とジョブ待ち行列を作成するライブラリーを入力します。

プログラムは、指定されたサブシステムが存在しないかどうか検査します。存在しなければ、プログラムはそのサブシステムを、経路指定テーブル、自動開始ジョブ項目、事前開始ジョブ項目、およびジョブ記述と一緒に作成します。サブシステムは既存のものでなくても、サブシステム記述とジョブ待ち行列のためのライブラリーは既存のものでなければなりません。 サーバーの始動ジョブが処理されると、新しく作成されたサブシステムのパラメーターが指定され、そのサブシステムのバッチ始動用のサーバー・ジョブが発行されます。

電子メール参照情報

ここには、メール・サーバー・ジャーナル項目、Simple Mail Transfer Protocol (SMTP) コマンド、および Post Office Protocol (POP) の verb およびパラメーターについての参照情報が記載されています。

メール・サーバー・ジャーナル項目

ジャーナル項目で使用されるコードとメッセージを理解するために、この情報を使用してください。

以下の表では、構成要素ジャーナル項目を読むための、より詳細な情報を提供します。

- 『ジャーナル項目における省略語』
- 49 ページの『SMTP クライアントに関するログ項目』
- 50 ページの『SMTP サーバーに関するログ項目』
- 51 ページの『ブリッジ・サーバーに関するログ項目』
- 52 ページの『Message Switching Facility (MSF) の存在と関数の作成』

ジャーナル項目における省略語

省略語	定義
LIN	ローカル受信。ローカル配信でメモを受信しました。後続の IP アドレスは、メモの送信元のホストです。
RIN	中継受信。別の SMTP デーモンに中継するためにメモを受信しました。送信元の IP アドレスが後に続きます。
R	宛先
O	発信元

省略語	定義
U	配布不能な宛先
QTMSINQ	SMTP の入力待ち行列
QTMSOUTQ	SMTP の出力待ち行列
QTMSBSSQ	システム記憶域のしきい値を超えたときに、メッセージが置かれる保留待ち行列。
QTMSRTQ1	1 次レベルの再試行待ち行列
QTMSRTQ2	2 次レベルの再試行待ち行列
RRSL	解決した宛先

各ジャーナル項目には、2 文字のサブタイプまたはコードが先行します。 サブタイプまたはコードの先頭文字は、項目のファンクション識別コードです。 サブタイプまたはコード の 2 番目の文字は、このジャーナル項目が記録しているアクションです。 ファンクション識別コードは、次の表で示す通りです。

ファンクション識別コード	説明
7	ブリッジ・サーバー項目
8	SMTP クライアント
9	SMTP サーバー
A	MSF 非送達
B	MSF ローカル送達
C	MSF メッセージ転送
D	POP 作成メッセージ
E	メール API 送信
F	Domino MTA
G	スナップインのトンネル
H	SNADS (交換プログラム)
I	MIME 構文解析プログラム (ローカル送達スナップイン)
L	FAX (ローカル送達)
M	SNADS
O	フィルター掛け
P	アドレス解決用の MSF SMTP 出口

ここに記述されているジャーナル項目はすべてログ項目 (LG) タイプです。

SMTP クライアントに関するログ項目

タイプ	アクション	サブタイプまたはコード	コメント
LG	処理用にコンテナーを待ち行列から解除	8B	フローター・タグが設定された直後に、メールの待ち行列解除をログに記録
LG	メール配信の成功	88 82	正常に送信されたメールをログに記録。各宛先をログに記録。

タイプ	アクション	サブタイプまたはコード	コメント
LG	配信不能メール	83	配信されなかったメールをログに記録
LG	1 次レベルのタイムアウト	8C	1 次レベルの再試行待ち行列に追加された際をログに記録
LG	2 次レベルのタイムアウト	8D	2 次レベルの再試行待ち行列に追加された際をログに記録
LG	メールは再試行可能	8E 8F	再試行メールがいつ QTMSOUTQ に戻されたかをログに記録
LG	COD が発信元に戻される	87	配信確認 (COD) が BRSR 待ち行列にエンキューされた際をログに記録。
LG	処理不能、リソースの負荷が高い	86	接続のメトリックがいっぱいのために、メールがいつ QTMSOUTQ に書き戻されたかをログに記録
LG	宛先レコードを検査	86	宛先の状況が変化した (つまり、MS レコードが解決され、メッセージを配信する準備ができた) ために、メールがいつ QTMSOUTQ に書き戻されたかをログに記録
LG	配信不能	87	配信不可の通知を 2 箇所から受信したことを理由に、メールが QTMSINQ に転送されたことをログに記録
LG	MX 照会	8K	照会バッファーに伴って障害が起こった場合、res_send 障害と、理由を示す errno をログに記録

SMTP サーバーに関するログ項目

タイプ	アクション	サブタイプまたはコード	コメント
LG	メール受信	94 91 92 9T 99	終了シーケンス CRLF <.> CRLF (ローカル) の受信直後に、メールの受信をログに記録。 発信元および宛先をログに記録。メッセージ・サイズ *nnnnn* (*nnnnn* はバイト数)。 MSGID

タイプ	アクション	サブタイプまたはコード	コメント
LG	中継されたメールの受信	95 91 92	終了シーケンス CRLF <.> CRLF (リレー) の受信直後に、MAIL をログに記録。発信元および宛先をログに記録。
LG	メールをブリッジ・サーバーに渡す	97	QTMSINQ (着信メール) への MAIL の項目をログに記録
LG	メールをリモート送達用のクライアントに渡す	96	QTMSOUTQ (中継されたメール) への MAIL の項目をログに記録
LG	CONNECTION REFUSED 1.2.3.4....	9S	制限された接続設定値に基づいて拒否された接続をログに記録。1.2.3.4 は拒否された IP アドレス。
LG	RELAY REFUSED 1.2.3.4....	9V	制限された中継設定値に基づいて拒否された中継をログに記録。 1.2.3.4 は拒否された IP アドレス。
LG	SMTP サーバーによってリジェクトされた	9W	メッセージは SMTP サーバーによってリジェクトされた。

ブリッジ・サーバーに関するログ項目

タイプ	アクション	サブタイプまたはコード	コメント
LG	IN 待ち行列のメールを送る	7A	QTMSINQ からデキューされているメールをログに記録
LG	メールを SNADS に渡す	7O	QSNADS への正常な転送を記録
LG	スペース使用量を理由に、コンテナーを BUSY 待ち行列に入れる	7L	しきい値オーバーフローのためにメールが QTMSBSSQ にエンキューされた場合に記録。
LG	BUSY 待ち行列のメールを送る	7M	QTMSBSSQ からのメールのデキューを記録。スペースは再利用され、メールは処理できる状態にある。
LG	MSF へのメッセージを渡す	7H 71 72	メッセージがフレームワークに挿入される時に記録
LG	COD メッセージの作成	7R 7G	COD メッセージがフレームワークに挿入される時に記録。 新規 COD メッセージが作成中であるため、MSF MSGID をログに記録

タイプ	アクション	サブタイプまたはコード	コメント
LG	メールのこの部分を受信側に送達できない	7P 7G	配信不能通知を作成していたことをログに記録。新規配信不能メッセージ通知の MSGID をログに記録。

Message Switching Facility (MSF) の存在と関数の作成

タイプ	アクション	サブタイプまたはコード	コメント
LG	非送達メッセージの作成	AP A1 A2	MSF に挿入される送達不能メッセージを記録。
LG	メールは POP メール・ボックスに送達される	B8 B2	ローカルの POP メールボックスへのメッセージの送達を記録。IP アドレスは POP メールボックス・ディレクトリーになる。受信側もリストされる。
LG	COD メッセージを MSF に送信する	BR B1 B2	COD メッセージの MSF への追加を記録
LG	可用性の検査	CN	MSF 出口を転送する SMTP メッセージ。SMTP が開始されていなかったために QMSF 待ち行列に書き戻された MSGID を記録。
LG	メールのエンキュー	C6 C1 C2	QTMSOUTQ に書き込まれているメールをログに記録する
LG	Sendmail API の使用	EH E1 E2 ET	SendMail API によるメッセージの作成を記録。メッセージ・サイズ *nnnnn*。ここで、*nnnnn* はメッセージのサイズ (すべての添付)。
LG	メールは、SNADS ブリッジされたリモート・システムを宛先にしている	G8 G2	メッセージがトンネルされた時に記録。受信側に送信されたシステムを含む。
LG	SNADS ブリッジを介してトンネルされたメールが受信される。	GQ G2	ローカル送達受信側用にトンネルされたメッセージの受信を記録
LG	アドレス解決 SNADS から/アドレス解決 SNADS に、スイッチする	H1	SNADS がメッセージを MSF にスイッチ
LG	構文解析された MIME 注釈をフレームワークに再度追加	IH I1 I2 IG	構文解析された MIME メッセージが MSF に再度追加される時にログに記録

タイプ	アクション	サブタイプまたはコード	コメント
LG	フィルターのためにリジェクトされた	OW	メッセージはリジェクトされた。そのメッセージが廃棄されたか、注意が払われたままであるかを示す。メッセージが再度書き出され送達される場合は、注意が払われている。
LG	SMTP アドレス解決 MSF 出口プログラムによって入力される	P2	メッセージは次のようにタグされています。 • **POP LclDel:** 送達するために、POP ローカル・デリバリー出口プログラムにタグされている。 • **SMTP MsgFwd:** 送信するために SMTP に転送されるようタグされている。 • **SMTP NonDel:** 非送達通知としてマークされている。 • **Parse:** 構文解析プログラム・コードに送信される。 • **PutBk:** なんらかの別の出口を処理するフレームワークに書き戻す (例、Domino または SNADS)。 • **chg to SNADS:** アドレス・タイプを SNADS に変更する。

関連タスク

57 ページの『構成要素ジャーナルの検査』
特定の電子メールの問題の解決方法を判別するために、エラーを記録した実行記録を確認することができます。

Simple Mail Transfer Protocol

Simple Mail Transfer Protocol (SMTP) は、電子メールの送受信に使用される TCP/IP プロトコルです。通常は POP3 または Internet Message Access Protocol とともに、サーバー・メールボックスへのメッセージの保管、およびユーザーへのメッセージのサーバーからの定期的なダウンロードに使用されます。

SMTP コマンド

以下の表に、SMTP コマンド、コマンド機能、および i5/OS SMTP サーバーがそのコマンドをサポートしているかどうかを記述します。

SMTP コマンド	機能	System i はサポートされます
AUTH (許可)	SMTP サーバーに対する認証メカニズムを指定する。 PLAIN と LOGIN の両方がサポートされる。	あり
DATA (Data)	コマンドに続く行を送信側からの電子メールと見なす。	あり
EHLO (Extension Hello)	SMTP 拡張機能を使用可能にする。	あり
EXPN (Expand)	メーリング・リストが識別されたことを確認するように受信側に要求する。	なし
HELO (Hello)	SMTP 送信側を SMTP 受信側に識別させる。	あり
HELP (Help)	受信側が発信元に支援情報を送信するように要求する。	あり
MAIL (Mail)	1 つ以上の宛先に電子メールを配布する電子メール・トランザクションを開始する。	あり
NOOP (Noop)	受信側に有効な応答を送信する (しかし他の処置は指定しない) ように要求する。	あり
QUIT (Quit)	受信側に有効な応答を送信して、伝送チャネルをクローズするように要求する。	あり
RCPT (Recipient)	電子メールの個別の宛先を識別する。	あり
RSET (Reset)	現在の電子メール・トランザクションを終了する。	あり
SAML (Send and mail)	ユーザーが活動状態にない場合、電子メールを 1 つ以上のワークステーションおよび宛先に配布する。	なし
SEND (Send)	電子メールを 1 つ以上のワークステーションに配布する。	なし
SOML (Send or mail)	ユーザーが活動状態にない場合、電子メールを 1 つ以上のワークステーションまたは宛先に配布する。	なし
STARTTLS (Start Transport Layer Security)	SMTP クライアントとの Secure Sockets Layer (SSL) または TLS 折衝を開始して、SSL または TLS セッションを確立するよう SMTP サーバーに要求する。	あり
TURN (Turn)	受信側が有効な応答を送信して SMTP 送信側となるように要求するか、または受信側が拒否の応答を送信して SMTP 受信側のままでいるかを要求する。	なし
VRFY (Verify)	ユーザーが識別されたことを確認するように受信側に要求する。	あり

関連概念

5 ページの『シナリオ: ローカルでの電子メールの送受信』
このシナリオでは、ローカル・ユーザー間で電子メールがどのように処理されるかを例示します。

Post Office Protocol

Post Office Protocol (POP) バージョン 3 のメール・インターフェースは、Request for Comments (RFC) 1939 (POP3)、RFC 2449 (POP3 拡張機能メカニズム)、および RFC 2595 (IMAP、POP3、および ACAP との TLS の使用) で定義されています。RFC は、進化していくインターネット標準を定義するために使用されるメカニズムです。

クライアント・ソフトウェアは、*verbs* と呼ばれるコマンドを使って POP サーバーと通信します。 i5/OS POP サーバーは以下の verb をサポートしています。

verb とパラメーター	説明
USER <id>	ユーザー ID を渡す
PASS <password>	パスワード
STAT	メールボックスを照会する
LIST <opt msg #>	メッセージの統計を照会する
RETR <msg #>	メッセージを検索する
DELE <msg #>	メッセージを削除する
RSET	メッセージ削除状況をリセットする
TOP <msg #> <lines>	メッセージのヘッダーとデータを検索する
UIDL <opt msg #>	メッセージ固有の ID リストを入手する
NOOP	ノーオペレーション
QUIT	クライアント・セッションを終了する
CAPA	機能をリストする
STLS	Transport Layer Security (TLS) を開始する

関連概念

5 ページの『シナリオ: ローカルでの電子メールの送受信』
このシナリオでは、ローカル・ユーザー間で電子メールがどのように処理されるかを例示します。

4 ページの『i5/OS での Post Office Protocol』
Post Office Protocol (POP) サーバーは、i5/OS における Post Office Protocol バージョン 3 メール・インターフェースのインプリメンテーションです。

電子メールのトラブルシューティング

この情報は、起こりうる電子メール関連の問題の解決に役立つことを目的としています。

関連タスク

43 ページの『大きなサイズの電子メール・メッセージの分割の防止』
大きなサイズの電子メール・メッセージがより小さく紛らわしい断片に分割して送信されるのを防ぐことが必要な場合があります。

電子メールの問題判別

簡単な手順で、電子メールの問題の原因を判別することができます。

Simple Mail Transfer Protocol (SMTP) の問題について考えられる原因を識別するには、次のステップに従います。

1. TCP/IP が電子メール用に構成されているかを検査します。
   a. 必須の PTF がすべてインストール済みであることを確認します。
   b. 電子メール・サーバーの検査を行ない、必要なサーバーが開始されていて稼働していることを確認します。
2. ローカル・ドメイン名を確認します。
   a. System i ナビゲーターで、**「ユーザーのシステム」** → **「ネットワーク」**と展開します。
   b. 「**TCP/IP 構成**」を右クリックして「**プロパティー**」を選択します。
   c. 「**ホスト・ドメイン情報**」タブをクリックして、ローカル・ドメイン名を確認します。
3. SMTP 再試行値を小さい値に設定します。
   a. System i ナビゲーターで、**「ユーザーのシステム」** → **「ネットワーク」** → **「サーバー」** → **「TCP/IP」**と展開します。
   b. 「**SMTP**」をダブルクリックします。
   c. 「**アウトバウンド・メール再試行回数**」タブをクリックします。
4. 受信者のユーザー ID およびアドレスがシステム配布ディレクトリーにあることを確認します。
   a. System i ナビゲーターで、**「ユーザーのシステム」** → **「ネットワーク」** → **「ユーザーおよびグループ」** → **「すべてのユーザー」**の順に展開します。
   b. ユーザー ID の「**プロファイル**」を右ボタンでクリックし、「**プロパティー**」を選択します。
   c. 「**個人**」をクリックし、「**メール**」タブを表示して、アドレスを検査します。
5. 電子メールが宛先アドレスに到達するのにホスト・テーブル項目が必要かどうかを確認します。
   a. 文字ベース・インターフェースで、CHGTCPHTE (TCP/IP ホスト・テーブル項目の変更コマンド) と入力し、電子メール・サーバーの IP アドレスを入力します。
   b. ホスト・テーブル項目が表示されない場合には、その IP アドレスのホスト名を入力します。
6. 記憶域のしきい値を超過していないことを確認します。
   a. System i ナビゲーターで、**「ユーザーのシステム」** → **「構成およびサービス」** → **「ハードウェア」** → **「ディスク装置」** → **「ディスク・プール」**の順に展開します。
   b. 表示したいソース・ディスク・プールを右マウス・ボタン・クリックし、「**プロパティー**」を選択します。
   c. 「**容量**」タブを選択します。

   システムの使用量がしきい値より大きい場合、メールの作動が停止する可能性があります。
7. 電子メール分割が使用不可のになっているか検査します。
   a. System i ナビゲーターで、**「ユーザーのシステム」** → **「ネットワーク」** → **「サーバー」** → **「TCP/IP」**と展開します。
   b. 「**POP**」をダブルクリックします。「POP プロパティー」ダイアログが表示されます。
   c. 「**構成**」タブをクリックします。
   d. 「**メッセージ分割サイズ**」フィールドで、「**無限大**」が選択されているか検査します。
8. TCP/IP アプリケーションの追跡コマンドを実行します。文字ベース・インターフェースで、TRCTCPAPP と入力します。
9. 問題を突き止めるために、構成要素ジャーナルの検査をします。

関連概念

11 ページの『電子メールへのアクセスの制御』
電子メールを通じて誰がシステムにアクセスするかを制御して、悪意のある攻撃からデータを保護する必要があります。

独立ディスク・プールの使用

13 ページの『Post Office Protocol へのアクセスの制御』
システムの安全を確保するには、Post Office Protocol (POP) へのアクセスを制御する必要があります。

59 ページの『QtmmSendMail API の問題の解決』
このトラブルシューティング・プロセスを使用して、MIME メールの送信 (QtmmSendMail) API に発生した問題を解決できます。

関連タスク

42 ページの『電子メール・サーバーの検査』
電子メール関連の最も一般的な問題の 1 つに、 適切なサーバーが開始しないという問題があります。電子メール・サーバーを使用する前に、その電子メール・サーバーの状況を検査し、それらがすべて稼働中であることを確認する必要があります。

17 ページの『電子メールのための TCP/IP の構成』
ご使用のシステム上で電子メールを構成するには、事前に TCP/IP をセットアップする必要があります。

60 ページの『メール・サーバー・フレームワーク・ジョブの検査』
QtmmSendMail API のエラーの考えられる原因を判別するには、QSYSWRK システムでメール・サーバー・フレームワーク・ジョブを検査する必要があります。

『構成要素ジャーナルの検査』
特定の電子メールの問題の解決方法を判別するために、エラーを記録した実行記録を確認することができます。

58 ページの『配布不能電子メールの追跡』
汎用ユーザー ID を使用して、 配布不能な電子メールの問題を追跡することができます。 この方法は、電子メールの配布および構成の両方の問題に役立てることができます。

関連情報

IBM System i のサポート (英語)

構成要素ジャーナルの検査

特定の電子メールの問題の解決方法を判別するために、エラーを記録した実行記録を確認することができます。

オペレーティング・システムでは、電子メール・サーバーがメールを送信しない理由を判別できるよう、さまざまな待ち行列、プログラム、およびジャーナル処理文書を使用します。 ジャーナル処理機能を実行することにより、電子メール・システムの問題を判断しやすくなる場合があります。 ジャーナル処理は処理装置のサイクルを使用するため、ジャーナル処理を停止した方がマシンのパフォーマンスは良くなります。

ジャーナル処理機能により、以下の項目が記載されます。

- 推移 -- プログラムから待ち行列、待ち行列からプログラム。
- イベント -- サーバー経由でのメールの到着、クライアント経由でのメールの転送、再試行待ち行列またはリソース使用中待ち行列へのメールの保管。
- トラッキングおよび測定データ -- 822 メッセージ ID、MSF メッセージ ID、メッセージのサイズ、発信元、宛先。

ジャーナル・レコードはジャーナル・レシーバーに保管されます。これらのレシーバーはユーザー管理です。ジャーナルがいっぱいになった時は、ジャーナル変更 (CHGJRN) コマンドを出して新しいジャーナル・レシーバーに変更します。新しい SMTP ジャーナル処理機能は、QZMF ジャーナルを使用します。

ジャーナル処理をオンにし、ジャーナルの内容を表示するには、次のステップに従ってください。

1. System i ナビゲーターで、「**ユーザーのシステム**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」と展開します。
2. 「**SMTP**」をダブルクリックします。
3. 「**一般**」タブをクリックします。
4. 「**ジャーナル項目を使用可能にする**」チェック・ボックスを選択します。
5. エミュレーション・セッションを開きます。
6. SMTP ジャーナル項目を表示できる形式に変換するには、文字ベース・インターフェースで、次のように入力します。 `DSPJRN JRN(QZMF) OUTPUT(*OUTFILE) OUTFILE(jrnlib/zmfstuff) OUTMBR(MAR2) ENTDTALEN(512)` ここで *jrnlib* はライブラリーの名前で、*zmfstuff* は物理ファイルの名前です。
7. SMTP ジャーナル項目を表示するには、コマンド行に `DSPPFM FILE(jrnlib/zmfstuff) MBR(MAR2)` と入力します。
8. F20 (Shift + F8) を押して、ジャーナル固有の情報を表示させます。

関連概念

55 ページの『電子メールの問題判別』
簡単な手順で、電子メールの問題の原因を判別することができます。

関連資料

48 ページの『メール・サーバー・ジャーナル項目』
ジャーナル項目で使用されるコードとメッセージを理解するために、この情報を使用してください。

配布不能電子メールの追跡

汎用ユーザー ID を使用して、配布不能な電子メールの問題を追跡することができます。 この方法は、電子メールの配布および構成の両方の問題に役立てることができます。

1. 通知を受け取るためにユーザー ID を選択または作成します。文字ベース・インターフェースで、`CRTUSRPRF` (ユーザー・プロファイルの作成コマンド) と入力し、実行キーを押します。
2. `WRKDIRE` (ディレクトリー項目の処理コマンド) と入力し、実行キーを押します。
3. 1 をタイプし、システム配布ディレクトリーにユーザーを追加します。
4. Mail Store 値が 2 で Preferred Address 値が 3 であることを確認します。
5. F19 (SMTP のための名前の追加) を押します。
6. `NONDELIVERY@localhost.domain` を、任意の POP ユーザーに対する SMTP アドレスとして入力します。

このユーザーは、配布不能の電子メールのコピーを受信します。

注: 入力するユーザー ID は、配布不能の通知を効果的にモニターできるようにするために、実際の ID にしなければなりません。送信側は、配布不能の通知のコピーを、電子メールを受信しなかった宛先のリストと共に受け取ります。

関連概念

55 ページの『電子メールの問題判別』
簡単な手順で、電子メールの問題の原因を判別することができます。

QtmmSendMail API の問題の解決

このトラブルシューティング・プロセスを使用して、MIME メールの送信 (QtmmSendMail) API に発生した問題を解決できます。

QtmmSendMail API とともに戻されるエラーを検出する場合があります。 API によって戻されるエラー・メッセージの説明については、『QtmmSendMail API』を参照してください。

関連概念

55 ページの『電子メールの問題判別』
簡単な手順で、電子メールの問題の原因を判別することができます。

関連資料

MIME メール送信 (QtmmSendMail) API

API 呼び出しの検査

QtmmSendMail アプリケーション・プログラミング・インターフェース (API) のエラーからリカバリーするには、ワークステーション画面で、API からエラー・メッセージを受け取っていることを確認する必要があります。

エラーを戻すようにコーディングしている場合、プログラムはエラーをプログラムに戻します。ただし、次の例に示されているようにこの値を 0 に設定すると、エラーはご使用のワークステーションの画面に表示されます。

C の例

```
Qus_EC_t         Snd_Error_Code;
Snd_Error_Code.Bytes_Provided=0;
```

RPG の例

```
DAPIError     DS
D APIBytes          1     4B 0
D CPFId             9    15
C              Eval    APIBytes   = 0
```

Multipurpose Internet Mail Extension ファイルの検査

Multipurpose Internet Mail Extension (MIME) ファイルに問題があり、QtmmSendMail API がエラーを戻す原因となっている可能性があります。MIME ファイルを検査し、こうした問題が修正済みであることを確認する必要があります。

1. MIME ファイルの位置を検査します。 MIME ファイルは ROOT システムになければなりません。名前は「/」で始めなければならず (例: /myfile.txt)、ファイル名には、パス /mydirectory/myfile.mime が含まれていなければなりません。
2. 権限レベルを検査します。 QMSF および QTCP プロファイルには、MIME ファイルを読み取り削除する権限がなければなりません。
   a. 文字ベース・インターフェースで、WRKLNK (オブジェクト・リンクの処理コマンド) と入力します。
   b. 9 (表示) をタイプして、QMST および QTCP 権限を処理します。「権限の処理」画面が表示されます。
3. MIME ファイルのヘッダーと本文との間に、ヘッダーの終わり (CRLFCRLF) ステートメントがあることを確認します。
4. MIME ファイルが MIME Request For Comments (RFC) に準拠していることを確認します。

注: ヘッダーの終わりステートメントについて詳しくは、RFC2822 (http://rfc.net/rfc2822.html) のセクション 2.1 (英語) を参照してください。

メール・サーバー・フレームワーク・ジョブの検査

QtmmSendMail API のエラーの考えられる原因を判別するには、QSYSWRK システムでメール・サーバー・フレームワーク・ジョブを検査する必要があります。

1. MSF がメッセージの処理を停止したら、エラー・メッセージがないか MSF ジョブを検査します。
2. フレームワーク・ジョブが完了したら、MIME ファイルは削除されているはずです。これは、フレームワークが MIME ファイルを処理したことを示します。問題の原因は API ではなく、SMTP にあります。

関連概念

55 ページの『電子メールの問題判別』
簡単な手順で、電子メールの問題の原因を判別することができます。

電子メールの関連情報

製品マニュアル、IBM Redbooks 資料、Web サイト、およびその他の Information Center のトピック・コレクションには、電子メール・トピック・コレクションに関連した情報が含まれています。PDF ファイルは、すべて表示または印刷できます。

マニュアル

AnyMail/400 Mail Server Framework Support (約 622 KB)

i5/OS メール・サーバーを駆動するフレームワークについて説明します。

IBM Redbooks

- AS/400® Electronic-Mail Capabilities

  電子メールおよび SMTP の詳細情報については、この IBM Redbooks 資料を参照してください。

- AS/400 Internet Security: Protecting Your AS/400 from HARM in the Internet (約 2160 KB)

  この Redbooks 資料には、ご使用のシステムが過負荷を発生させるアタックの被害に遭った場合に、i5/OS オペレーティング・システムをクリーンアップするステップを含む、セキュリティー情報が記載されています。

Web サイト

- IBM System i のサポート (英語)

  ご使用のワークステーションを Internet PTF ページへのゲートウェイとして使用することにより、ご使用の i5/OS オペレーティング・システムに現行の PDF をダウンロードしたり、Technical Information および Databases カテゴリーから i5/OS ソリューションを表示したりすることができます。

- RFC 索引 (英語)

| 電子メール・プロトコルは RFC (Request for Comments) で定義されます。RFC は、進化していくインターネット標準を定義するために使用される手段です。 SMTP の追加情報については、RFC 1939 (POP3)、RFC 2449 (POP3 拡張機能のメカニズム)、および RFC 2595 (IMAP、POP3、および ACAP との TLS の使用) を参照してください。

- Lotus Domino for i5/OS (英語)

  この Web ページでは、Lotus Domino for i5/OS およびこのライセンス・プログラムが提供するソリューションが紹介されています。

- Lotus Domino 参照ライブラリー (英語)

  Domino については、ホワイト・ペーパー、ブック、プレゼンテーションなどを参照してください。

- Lotus 文書 (英語)

  『Lotus 文書』ページには、製品資料、ホワイト・ペーパー、Redbooks 資料などのリソースへのリンクが掲載されています。

その他の情報

System i とインターネット・セキュリティー

System i のネットワークを保護するには、この Information Center のトピックを参照してください。

関連資料

2 ページの『「電子メール」の PDF ファイル』
この情報の PDF ファイルを表示および印刷することができます。

付録. 特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒106-8711
東京都港区六本木 3-2-12
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

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。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、IBM 機械コードのご使用条件、またはそれと同等の条項に基づいて、 IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。 IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があり、単に目標を示しているものです。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。

それぞれの複製物、サンプル・プログラムのいかなる部分、またはすべての派生的創作物にも、次のように、著作権表示を入れていただく必要があります。

© (お客様の会社名) (西暦年). このコードの一部は、IBM Corp. のサンプル・プログラムから取られています。 © Copyright IBM Corp. _年を入れる_. All rights reserved.

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

プログラミング・インターフェース情報

本書には、プログラムを作成するユーザーが IBM i5/OS のサービスを使用するためのプログラミング・インターフェースが記述されています。

商標

以下は、International Business Machines Corporation の米国およびその他の国における商標です。

AIX
AS/400
eServer
i5/OS
IBM
IBM (ロゴ)
Infoprint
iSeries
Lotus
Lotus Domino
Lotus Notes
Redbooks
System i
The Output of e-business
Tivoli

Adobe、Adobe ロゴ、PostScript、PostScript ロゴは、Adobe Systems Incorporated の米国およびその他の国における登録商標または商標です。

Linux は、Linus Torvalds の米国およびその他の国における商標です。

Microsoft、Windows、Windows NT および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

Java およびすべての Java 関連の商標およびロゴは、Sun Microsystems, Inc. の米国およびその他の国における商標または登録商標です。

他の会社名、製品名およびサービス名等はそれぞれ各社の商標です。

使用条件

これらの資料は、以下の条件に同意していただける場合に限りご使用いただけます。

個人使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、非商業的な個人による使用目的に限り複製することができます。ただし、IBM の明示的な承諾をえずに、これらの資料またはその一部について、二次的著作物を作成したり、配布 (頒布、送信を含む) または表示 (上映を含む) することはできません。

商業的使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、お客様の企業内に限り、複製、配布、および表示することができます。 ただし、IBM の明示的な承諾をえずにこれらの資料の二次的著作物を作成したり、お客様の企業外で資料またはその一部を複製、配布、または表示することはできません。

ここで明示的に許可されているもの以外に、資料や資料内に含まれる情報、データ、ソフトウェア、またはその他の知的所有権に対するいかなる許可、ライセンス、または権利を明示的にも黙示的にも付与するものではありません。

資料の使用が IBM の利益を損なうと判断された場合や、上記の条件が適切に守られていないと判断された場合、IBM はいつでも自らの判断により、ここで与えた許可を撤回できるものとさせていただきます。

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入関連法規を含む、すべての関連法規を遵守するものとします。

IBM は、これらの資料の内容についていかなる保証もしません。これらの資料は、特定物として現存するままの状態で提供され、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されます。

Printed in Japan

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