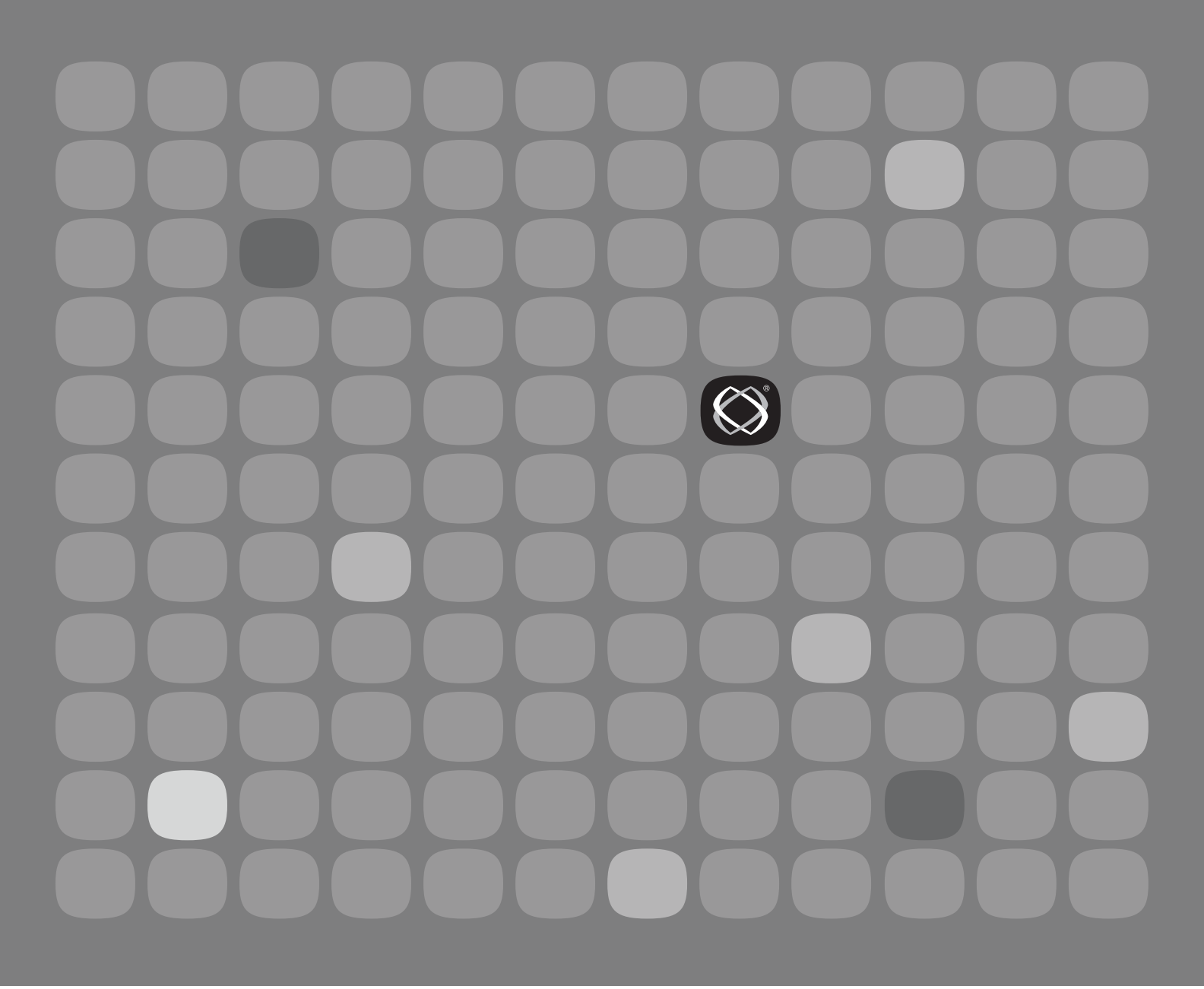

attachmate WRQ™

Reflection®

Reflection® X の評価

Reflection® X の評価

本ガイドでは、Reflection® X の主な機能を簡単に紹介します。

本ガイドの内容は以下のとおりです。

- ホストとの接続
  - 新規接続の確立と、設定事項の X クライアントファイルへの保存
  - 構成済みのクライアントテンプレートファイルを使用した、XDMCP ブロードキャストの開始
  - 複数の X サーバインスタンスの表示と管理
- 機能の評価
  - 複数 X スクリーン対応機能の使用
  - Secure Shell 鍵エージェントを使用した認証
  - ローカルマシン上にある実行ファイルの起動
  - IPID を使用した、VPN で割り当てられた IP アドレスの解決
  - 「RunRX」コマンドライン起動機能の使用
- 問題解決用ツール
- 安全な接続 : 概要
- Reflection 管理者用ツールキット
  - ツールキットを使用する前に

各項では、一般的な手順を取り上げ、ご自身でその機能を試すことができるようになっています。また、評価を進めながら、他の項の応用を兼ねた個別の練習もできるようになっています。

このバージョンの新機能に関する情報は、Reflection 製品に付随のオンラインヘルプで「新機能」を検索してください。

Reflection X の初めての起動

Reflection X を起動するには、以下の手順に従います。

- Windows の [スタート] メニューから、**[すべてのプログラム]** - **[Attachmate Reflection]** - **[Reflection X]** コマンドを選択します。

初めて Reflection X を起動すると、操作を開始できるオプションが入ったダイアログボックスが表示されます。既定では、このダイアログボックスは Reflection X 性能調整を実行するように設定されています。Reflection X 性能調整は、マシンでの X クライアントの描画速度を最適化します。このプロセスを実行することをお勧めしますが、約 2 分かかります (性能調整は、後で Reflection X マネージャの [ツール] メニューから実行することもできます)。

起動ダイアログボックスには、接続用の 3 つのオプション、すなわち XDMCP ブロードキャスト、クライアントウィザード、Reflection X マネージャの起動も含まれています。このチュートリアルでは、最後の項目を選択してください。

Reflection X マネージャに直接移動して、ローカルクライアントまたはリモートクライアントを起動します。

Reflection X マネージャから直接 XDMCP ブロードキャストとクライアントウィザードを使用する方法について説明します。

ホストとの接続

以下に、X クライントウィザード、テンプレートファイル、ユーザ独自の保存ファイルを使用して、X マネージャで接続をカスタム設定する方法を示します。詳細は、製品のオンラインヘルプを参照してください。

新規接続の確立と、設定事項の X クライアントファイルへの保存

ホストに接続する 1 つの方法として、Reflection X クライントウィザードを使用します。

やってみましょう

以下の手順で、ウィザードを使用して、任意のホストにクライアントファイル (.rxc) を作成および保存できます。

1. 以下のいずれかの方法を使用して、X　クライアントウィザードを起動します。
   - Reflection X マネージャで、**[ツール]** - **[クライアントウィザード]** コマンドを選択します。
   - Windows の [スタート] メニューから、**[すべてのプログラム]** - **[Attachmate Reflection]** - **[ウィザード]** - **[X クライアントウィザード]** コマンドを選択します。
2. [次へ] をクリックし、**[ホスト]** と **[種類]** に必要な値を入力します。[次へ] をクリックします。
3. **[起動方式]** を [TELNET] に設定します。
4. 必要に応じて、ユーザ名とパスワードを入力します。**[コマンドプロンプト]** の既定値を受け入れ、[次へ] をクリックします。

   注意：[ホストクライアントの確認] チェックボックスをクリアすると、セッション中に接続情報の確認が不要になります。
5. X クライアントアプリケーションの一覧から、**時計**や **X 端末**などのクライアントを選択します。[次へ] をクリックします。
6. この接続を識別できるような名前とファイル名を入力します。ショートカットを作成し、コンピュータ上でショートカットの場所を指定することもできます。[次へ] をクリックします。
6. **[クライアントの起動]** をクリックします。これにより、まだ実行されていない場合には Reflection X マネージャが自動的に起動します。
7. パスワードの入力を要求された場合は、パスワードを入力して [OK] をクリックします。X クライアントがデスクトップに表示されます。
8. X クライントウィザードに戻り、**[完了]** をクリックします。クライアントアプリケーションを閉じ、本製品の評価を続けます。

新しく作成したクライアントファイルを見るには、Reflection X マネージャを開いて、アプリケーションの左枠で **[クライアントファイル]** - **[クライアントの起動]** を展開します。既定のファイル名を受け入れると、「rxw0000」というファイルが表示されます。新規のファイルが作成されるごとに、rxw0001、rxw0002 のように数値が 1 ずつ増えていきます。カーソルをファイル名の上に置くと、入力した説明文が表示されます。クライアントファイルにもっとわかりやすい名前を付ける場合には、[クライアントの起動] 一覧内のファイルを右クリックして、[改名] を選択します。

以下のいずれかの方法を使用して、このクライアントファイルを使用して接続することができます。

- クライアントファイルアイコンをダブルクリックします。
- クライアントファイルアイコンを右クリックし、**[X クライアントに接続]** を選択します。
- クライアントファイルアイコンを選択し、メニューで **[アクション]** - **[X クライアントに接続]** コマンドを選択します。

構成済みのクライアントテンプレートファイルを使用した、XDMCP ブロードキャストの開始

X ディスプレイマネージャコントロールプロトコル (XDMCP) は、特定のホストマシン上で動作している X ディスプレイマネージャ (XDM) との通信に使用します。これは、ホストが X 環境の構成方法とどの X クライアントを実行するのかを制御するということを意味します。接続しているホストが XDMCP に対応している場合は、これが最も簡単な接続方法です。XDMCP は、トランスポートとして TCP/IP を使用している場合にだけ使用できます。

やってみましょう

以下に、Reflection X マネージャの XDMCP 構成済みクライアントテンプレートファイルを使用して、接続可能なホストに対して要求をブロードキャストする方法を紹介します。このファイルと、Reflection X で提供されているその他のテンプレートは、**[クライアントテンプレート]** にあります。**[クライアントテンプレート]** を右クリックすると、追加クライアント (および追加サーバ) を Web からダウンロードする手順に関する情報にアクセスできます。

Reflection X マネージャが起動していることを確認し、以下の手順に従います。

1. 左上枠で、[クライアントテンプレート] - **[XDMCP]** - **[xdmcpbrd]** をクリックします。**[XDMCP 接続の設定]** グループボックスに、詳細な構成を行うための接続情報が表示されます。
2. xdmcpbrd ファイルを右クリックしてポップアップメニューを表示し、**[X クライアントに接続]** をクリックします。

   X クライアントがまだ実行されていない場合は、[XDMCP ホストの選択] ダイアログボックスに接続可能なホストの一覧が表示されます。X クライアントがすでに実行されている場合は、[XDM セッションの開始] ダイアログボックスが表示されます。3 番目のラジオボタン選択して、新しい XDM セッションを新しい X サーバインスタンスで開始します。
3. ホストを選択し、[OK] をクリックします。
4. ユーザ名ならびにパスワードを入力します。

必要に応じて、[設定] メニューで、フォントやディスプレイなどの X マネージャの設定を変更できます。この設定をファイルに保存するには、**[ファイル]** - **[名前を付けて保存]** コマンドをクリックし、[名前を付けて保存] ダイアログボックスを表示します。ファイル名を入力し、[OK] をクリックします。新しいクライアントファイルは、**[クライアントファイル]** - **[XDMCP]** の下に表示されます。

複数の X サーバインスタンスの表示と管理

以下に、2 つの X サーバインスタンス (ディスプレイ)、および既定のインスタンス (「config」) を開始する方法を紹介します。初めに、構成済みテンプレートを使用して、Secure Shell を介した安全な接続を開きます。このテンプレートでは、Secure Shell による接続のみが許可されています。次に、既定の config サーバインスタンスの基本設定を使用して、自分の X サーバインスタンスを作成します。

やってみましょう

まず、実行中のすべてのクライアントを終了します。**[表示]** - **[X サーバ管理]** コマンドを使用して、X マネージャの下部に [X サーバ管理] グループボックスが表示されるようにします。次に、以下の手順に従います。

1. 左下枠で、**[X サーバテンプレート]** を展開します。**[SECURESHELL_only]** を選択し、ファイル名を右クリックしてポップアップメニューを表示します。
2. **[開始]** をクリックします。この X サーバインスタンスは、右下の **[X サーバ管理]** グループボックスに表示されます。接続名は、X マネージャのタイトルバーにディスプレイ番号「1」とともに表示されます。

   やってみましょう : このサーバインスタンスは、ユーザがログイン情報使ってログインしないと、SSH 接続を交渉できないようにします。これを確認するには、**[クライアントテンプレート]** - **[クライアントの起動]** を開き、任意のクライアントを選択して、**[X クライアント接続の設定]** グループボックスで接続方式として [REXEC] を選択します。[接続] をクリックして、エラーメッセージが表示されることを確認してください。SECURE SHELL が接続方式として選択されていないので、接続を確立できません。
3. **[X サーバ管理]** グループボックスで、[config] をクリックします。これにより、この X サーバインスタンスが「現在管理されているサーバインスタンス」になり、次に作成するサーバインスタンス用の基本設定として使用できます。

   注意 : 「config」サーバインスタンスは、X サーバインスタンスの基本設定であり、削除することはできません。これは、ユーザが独自の X サーバインスタンスを作成できるようにするものであり、Windows モード設定を除くすべての設定内容と属性が引き継がれます。
4. **[X サーバインスタンス]** を右クリックし、さらに [新規] をクリックします。新しい X サーバインスタンスに名前を付け、[Enter] を押します。
5. この新規インスタンスを右クリックし、表示されるポップアップメニューから [開始] をクリックします。このサーバインスタンスは **[X サーバ管理]** グループボックスに表示され、インスタンス名はタイトルバーにディスプレイ番号 (この場合は「2」) とともに表示されます。

今、config サーバインスタンスを含む 3 つの X サーバインスタンスを実行していますが、必要に応じてさらに多くのサーバインスタンスを開始することができます。

また、サーバインスタンスを切り替えることによって、それぞれを個々に構成することも可能です。これを行うには、**[X サーバ管理]** グループボックス内でサーバインスタンスを選択するか、**[アクション]** - **[X インスタンスの選択 / 開始]** コマンドをポイントし、管理対象のインスタンスを選択します。

機能の評価

複数 X スクリーン対応機能の使用

やってみましょう

Reflection の**複数 X スクリーン**機能は、作業で使用するクライアントアプリケーションを整理するための強力なツールです。これを使用すると、最高 9 スクリーンを 1 つのサーバインスタンスに割り当てることができます。各スクリーンサイズのカスタム設定、同一モニタへの出力、別のモニタへの出力などができます。

この機能を確認するには、X マネージャを開いて次の手順に従います。

1. **[設定]** - **[ウィンドウマネージャ]** をクリックします。**[ウィンドウモード]** で、**[X 端末風のデスクトップ]** を選択して、[OK] をクリックします。[Reflection X ルートウィンドウ] が表示されます。
2. X マネージャで、**[設定]** - **[X スクリーン]** をクリックします。**[X スクリーン数]** で、数字の「**3**」を入力します。1 ～ 9 まで入力できます。[OK] をクリックします。
3. 変更を適用するには、X サーバをリセットする必要があります。次に表示されるダイアログボックスで [OK] をクリックします。**[X サーバ管理]** で **[X スクリーン数]** が **3** になっていることを確認します。
4. [設定] ボタンをクリックして、[X スクリーンの設定] ダイアログボックスをもう一度開きます。
5. 各スクリーンのサイズを設定するには、**[X スクリーンの構成]** ボックスから目的のスクリーンを選択して、**[仮想サイズ]** を変更します。例えば、**X スクリーン 0** を **200 x 200** ピクセルに、**X スクリーン 1** を **400 x 400** ピクセルに、**X スクリーン 2** を **700 x 300** ピクセルに、それぞれ変更します。

   モニタが複数ある場合は、**[モニタ上の場所]** リストボックスを使用して、スクリーンの表示先を別のモニタに指定します。[OK] をクリックして変更を適用し、[X スクリーンの設定] ダイアログボックスを閉じます。
6. **[クライアントテンプレート]**、**[クライアントの起動]** の順に展開してクライアントテンプレートファイル (**unix** など) を選択し、クライアントアプリケーションを起動します。
7. 右の **[X クライアント接続の設定]** に、ホスト名とユーザ名を入力します。
8. **[コマンド]** テキストボックスで、コマンド文字列の display パラメータに数字「**0**」を追加して、次のようにします。

   ```
   -display %IP#0%
   ```

   [接続] をクリックします。
9. 表示されるダイアログボックスでパスワードを入力して [OK] をクリックします。クライアントアプリケーションのウィンドウが表示されます。
10. 同じまたは別のホストにあるあと 2 つのクライアントアプリケーションに対しても手順 6 ～ 9 を実行して、display パラメータにそれぞれ **1** および **2** を指定します。

    これで、3 つの異なるクライアントアプリケーションを実行する単一のサーバインスタンスができました。各クライアントアプリケーションは、表示先スクリーンもサイズも異なります。システムの構成によっては、スクリーンが別のモニタに表示されることもあります。

Secure Shell 鍵エージェントを使用した認証

やってみましょう

Reflection 鍵エージェントを使用すると、接続の認証に使用するローカルに格納されている秘密鍵を使用して、Secure Shell サーバに簡単にログインできます。鍵エージェントにより、ユーザ鍵の管理プロセスが簡素化され、別の Secure Shell サーバへのエージェント転送も実現されます。

この機能を確認するには、次の 3 つの主な手順を実行します。

- 鍵ペアの作成
- 公開鍵のサーバへのアップロード
- 鍵エージェントを使用した認証

鍵ペアの作成

Secure Shell で使用できるユーザ認証方式の 1 つは、「鍵ペア」とも呼ばれる公開鍵と秘密鍵に基づいています。以下の手順では両方の鍵が生成されますが、公開鍵をホストにアップロードする前に、次の手順を実行します。

1. [スタート] メニューから **[プログラム]** - **[Attachmate Reflection]** - **[ユーティリティ]** - **[鍵エージェント]** をクリックして、鍵エージェントを起動します。
2. 鍵エージェントの初回使用時には、パスフレーズを使用して初期設定することが要求されます。パスフレーズを入力して、[OK] をクリックします。

   鍵エージェントが初期設定済みの場合は、[ロック解除] ボタンをクリックして、パスフレーズを入力します。
3. [鍵エージェント] ダイアログボックスで、**[鍵の生成]** ボタンをクリックします。
4. [ユーザ鍵の生成] ダイアログボックスで、鍵の名前、種類、および長さを指定して、[OK] をクリックします。

公開鍵のサーバへのアップロード

以下の手順で、公開鍵をホストにアップロードします。これにより、そのホストを安全に認証できます。

1. [Reflection 鍵エージェント] ダイアログボックスで、作成した鍵を選択して、**[アップロード]** をクリックします。
2. [ホストへのアップロード] ダイアログボックスで、鍵のアップロード先ホスト名を入力します (そのホストで Secure Shell サーバが実行されている必要があります)。**[SSH 構成セクション]** は空欄にしたまま、[OK] をクリックします。
3. そのホストに対する有効なユーザ名を [Reflection Secure Shell] ダイアログボックスに入力します。[OK] をクリックします。
4. 初めてこのホストとの接続を確立する場合には、[ホスト鍵の信頼性] ダイアログボックスが表示されます。そのホストのシステム管理者に問い合わせて、ホスト鍵の有効性を確認できます。**[常時]** をクリックして、ホスト鍵を既知のホストの一覧に追加します。
5. このユーザのパスワードを入力して、[OK] をクリックします。
6. ホストへの安全な接続が確立されると、ダイアログボックスが開き、この鍵をアップロードするホスト上の場所に関する情報が表示されます。通常は、この設定を変更する必要はありません。
7. [公開鍵のアップロード] ダイアログボックスに、転送に関する情報が表示されます。[OK] をクリックして、ダイアログボックスを閉じます。
8. [Reflection 鍵エージェント] ダイアログボックスを閉じます。

鍵エージェントを使用した認証

以下の手順では、ホストにログインすると、認証 (パスワード) は鍵エージェントにより処理されます。

1. タスクバーで X マネージャのアイコンをクリックして起動します。
2. 左の **[クライアントの起動]** リストからホストの種類を選択します。
3. **[X クライアント接続の設定]** で、**[起動方式]** を **[SECURE SHELL]** に設定します。
4. **[ホスト名]** と **[ユーザ名]** に入力します。**[SSH 構成セクション]** は空欄のままにします。
5. **[詳細設定]** をクリックします。
6. [Reflection Secure Shell の設定] ダイアログボックスの **[一般]** タブで、**[ユーザ認証]** で **[公開鍵]** が選択されていることを確認します。
7. **[ユーザ鍵]** タブをクリックし、**[使用]** 列のボックスを選択して、作成した鍵を選択します。
8. [OK] をクリックして、[Reflection Secure Shell の設定] ダイアログボックスを閉じます。

9. X マネージャで、[接続] をクリックします。

目的のホストとの Secure Shell 接続が確立します。パスワードの入力は不要でしたね。パスワードは Secure Shell 鍵エージェントが処理しています。

ローカルマシン上にある実行ファイルの起動

やってみましょう

以下に、ローカル接続機能を使用して、Windows 実行ファイル (*.exe) を起動する手順を説明します。ローカルの実行ファイルを Reflection X から実行することは、単一のアプリケーションから複数のセッションを開始できる迅速な方法です。

以下の手順を使用して、Reflection X から X レジストリユーティリティ (英語版) を起動します。

1. タスクバーで Reflection X マネージャをクリックします (起動していない場合は、[スタート] メニューから Reflection X を起動します)。
2. **[クライアントファイル]** を拡張表示し **[ローカル接続]** をクリックします。**[ローカルクライアント接続の設定]** グループボックスに接続情報が表示されます。
3. **[参照]** をクリックして、[ローカル接続実行ファイルの参照] ダイアログボックスでファイル Regconv.exe を探します (このファイルは、Reflection プログラムフォルダにあります)。**[開く]** をクリックします。
4. **[接続]** をクリックして Reflection X レジストリユーティリティを起動します。

Reflection X レジストリユーティリティは、Windows レジストリの中から Reflection X に関連したものだけを表示します。このユーティリティに関する情報は、製品のオンラインヘルプを参照してください。

IPID を使用した、VPN で割り当てられた IP アドレスの解決

以下に、現在のサイトで仮想専用線 (VPN) を利用する場合に、Reflection X IPID サーバユーティリティを使用して、ホストと X マネージャの間の IP アドレスを解決する方法の概要を説明します。この手順にはホストでの IPID ソースコードの設定が含まれるため、この評価ガイドでは詳細に説明することはできませんが、この情報は VPN で割り当てられた IP アドレスを手作業で解決する場合に役立ちます。詳細についてはオンラインヘルプを参照してください。

背景 : VPN 接続での X クライアントの実行

ホスト接続に仮想専用線 (VPN) クライアントソフトウェアを使用する場合、X クライアントを検出して実行するためには、X マネージャの設定で IP アドレスを手作業で変更する必要があります。これは、VPN 接続ごとに、それぞれのコンピュータに異なる IP アドレスが割り当てられているからです。この IP アドレスは、そのコンピュータの TCP/IP 設定を基に Reflection X が設定した IP アドレスとは異なります。アドレスの相違は、以下の方法で解決できます。

- **[設定]** - **[ネットワーク]** コマンドをクリックして、**[リモート TCP/IP 接続を使用不可]** チェックボックスおよび **[ネットワークインタフェースの自動検出]** チェックボックスをクリアします。VPN で割り当てられた IP アドレスを **[IP アドレス]** ボックスに入力します。IP アドレスの値は、VPN ソフトウェアが割り当てます。VPN クライアントのアイコンを右クリックすると、この値を確認できます。詳細については、**http://support.wrq.com/techdocs/1580.html** や **http://support.wrq.com/techdocs/1632.html** で、技術ノート 1580 や 1632 (ともに英語版) を参照してください。
- Reflection X に含まれている IPID サーバを使用して IP アドレスを解決する方法については、次の項で説明します。

情報 : VPN で割り当てられた IP アドレスを IPID で解決

VPN クライアントソフトウェアで X マネージャが正しい IP アドレスを返さず、実行しようとしている X クライアントに IP アドレスを報告できない場合、「< ホスト名 > が見つかりません」や「接続の待ち時間が切れました」といったエラーメッセージが表示されます。ご使用のホストの初期設定を一部変更して、IPID サーバを実装することにより、VPN 接続するたびに IP アドレスを直接入力しなくても、これらの ID を解決することができます。これを実行する IPID サーバは、クライアントとデーモンで構成されています。デーモンは、ソースコードで提供され、常駐する UNIX ホスト上でコンパイルします。IP アドレスの解決は、Reflection X とデーモンの間の UDP データグラム通信によって行なわれます。

以下に、IPID サーバのセットアップ手順の概要を説明します (詳細については、製品のオンラインヘルプで「IPID、このユーティリティの概要」を検索するか、上記の技術ノートを参照してください)。

- まず、IPID 用のデーモンをダウンロードし、UNIX ホスト上でコンパイルします。デーモンを起動スクリプトに含めると、デーモンを手動で起動する必要がなくなります。
- 次に、**[ネットワークの設定]** パネル (**[設定]** - **[ネットワーク]** コマンド) で、**[リモート TCP/IP 接続を使用不可]** チェックボックスおよび **[ネットワークインタフェースの自動検出]** チェックボックスをクリアします。続いて、**[IPID ホストを使用]** を選択し、IPID サーバを実行するホストの IP アドレスを入力します。

設定後は、接続時に、割り当てられている IP アドレスが常駐する Windows レジストリを使用して、その IP アドレスが X マネージャとホストの間で自動的に解決されます。

「RunRX」コマンドライン起動機能の使用

情報 : コマンドラインからの Reflection X の起動

Reflection X マネージャには「RunRX」ユーティリティが含まれており、コマンドラインから X マネージャを起動できます。通常、このユーティリティは、ホスト、パスワード、起動方式、ならびにスクリプトをアプリケーションに渡し、カスタム仕様で起動するために使用します。

以下に、X マネージャの起動に使用するコマンドライン構文の例を示します。

```
RUNRX -m TELNET -h SYSTEM -u USER -p PASS -c /
etc/bin/MONITOR -nm
```

この構文により、X マネージャは、Telnet 接続を介して、ホスト「system」から起動画面なし (-nm) でクライアント「monitor」を起動します。ユーザは、「user」としてログインし、パスワードには「pass」を使用します。

ホスト、起動方式、ユーザ名、およびパスワードをコマンドライン上に直接記述せず、かわりにファイルに含めたい場合には、そのクライアントファイル (*.rxc) を参照することもできます。この接続の構文は以下のようになります。

RUNRX default1.rxc -c /etc/bin/MONITOR -nm

「RunRX」コマンドラインユーティリティのパラメータに関する詳しい情報は、製品のオンラインヘルプを参照してください。また、以下の Web サイトで技術ノート (英語版) を参照できます。

http://support.wrq.com/techdocs/1530.html

問題解決用ツール

Reflection X マネージャには、アプリケーションの問題を解決するためのいくつかのツールが組み込まれています。

[設定一覧] コマンド (**[設定]** - **[設定一覧]**) により、X マネージャの現在の状態を示すダイアログボックスを開いて、ユーザにすべての設定が表示されるようにしたり、出荷時の既定値から変更された設定のみ表示されるようにすることができます。

[フォント要求の記録] チェックボックス (**[設定]** - **[フォント]** の **[オプション]** グループボックス) を使用して、フォントの使用および代用状況を記録できます。このオプションにより X マネージャのログファイル (Logfile.txt) に書き込まれる情報を使用して、X マネージャでのフォントの問題を診断することができます。このログファイルには、ビデオカードの能力や OpenGL の互換性に関連するディスプレイの問題を書き込むこともできます。**[PFD をログファイルへ出力する]** ボタン (**[設定]** - **[サーバ]** - **[拡張機能]** - **[GLX]** - **[詳細設定]** - **[オプション]**) をクリックして、バージョン、ベンダ、表示された情報をファイルに書き込んで、分析に使用します。

X マネージャのトレースプログラム (**[ツール]** - **[クライアントトレース]**) は、X プロトコル情報を捕捉します。エンドユーザまたは弊社の技術サポートは、この情報を使用して診断を行うことができます。トレース情報は、X マネージャを初めて使用するユーザの教育にも利用できます。たとえば、Reflection X がインストールされている任意のマシン上でトレースを再生して、サーバとクライアント間の対話の動作や結果を確認することができます。

X プロトコル情報は、X マネージャのログファイルに標準的な ASCII ファイルで書き込まれるように指定できます。このファイルは、内容をそのまま理解できる形で表示することができます。または、あらゆる Reflection X インストールで再生可能なバイナリファイル Xscope.trc が既定で作成されるように指定できます。必要に応じて、トレース処理に、ファイルに読み込まれる情報を絞り込むことが可能なフィルタを適用することもできます。製品の問題を分析する際には、通常、trc ファイルが必要です。

安全な接続 : 概要

Reflection X マネージャは、以下の安全な接続に対応しています。

- **Secure Shell:** セキュリティ上問題のあるネットワークで、信頼するホストと使用マシンとの間に暗号化された安全な通信が必要な場合は、Secure Shell を使用するように X マネージャを構成できます。Secure Shell を使用するように Reflection を構成すると、マシンとリモートホストとの間のすべての接続が暗号化され、これらのマシン間で送信されるデータが保護されます。パスワードが、読み取りやすいテキスト形式でそのままネットワーク上に送信されることはありません。
- **Kerberos:** Reflection Kerberos マネージャは、X マネージャで使用できるオプションユーティリティです。このユーティリティを使用すると、プリンシパルプロファイルの作成または変更、レルムの追加または変更、チケットオプションの設定、Kerberos の設定のインポートとエクスポート、その他の Kerberos 管理作業の実行が可能です。
- **XDM Authorization-1:** これは、X マネージャで XDMCP を使用して行われる接続のセキュリティを向上させるオプションです。XDM 認証対応を構成することにより、XDM-AUTHORIZATION-1 を使用して XDMCP 接続を実行できます。この方式は MIT-MAGIC-COOKIE-1 方式に似ていますが、認証コードに DES (Data Encryption Standard) 暗号化を使用するのでより安全です。
- **グループポリシー:** Reflection 管理者用ツールキット (次ページ参照) には、非暗号化接続をユーザに許可しないポリシーが含まれています。グループポリシーエディタで、この「Allow Unencrypted Connections」ポリシーを使用不可にすることにより、Windows 2000 や Windows XP マシンからの非暗号化接続を防止できます。

管理ツール :

Reflection 管理者用ツールキット *

管理ツールをインストールするには、Reflection インストールプログラムを使用して、インストール可能な Reflection 製品の一覧から「Reflection 管理者用ツールキット」を選択します。

Reflection の管理ツールには、カスタム設定マネージャ、グループポリシー対応機能、および各 Reflection 製品用のプロファイラが含まれています。これらのツールを使用すると、システム管理者は、Reflection 製品をすばやく設定し配布することができます。

これらのツールを使用して、システム管理者は以下のことができます。

- ファイルまたは Web サーバに対して管理者用インストールを実行する
- ユーザ用の設定ファイルを作成する
- Reflection インストールを開き、カスタム設定を含むトランスフォームを作成する
- ユーザがインストールする機能セットを選択する (必要に応じて、機能を非表示にする)
- Reflection インストール、または独自の [アプリケーションの追加と削除] エントリを持つ別の「コンパニオン」データベースにファイルを追加する
- 機能およびコマンドへのユーザアクセスの制限など、Reflection 製品のプロファイルを設定する
- Microsoft グループポリシーエディタを使用して、個人またはユーザグループ別に Reflection の機能を制限する
- 製品ショートカットの場所、パラメータ、および説明を構成したり、カスタム設定された Reflection をインストールする単一のショートカットを作成する

Reflection 管理ツールの包括的な概要については、製品 CD に収録されている「Reflection System Administrator Guide」(英語版) を参照してください。

ツールキットを使用する前に

Reflection 管理ツールの使用を開始するには、まず各種 Reflection 製品と同様の方法で「Reflection 管理者用ツールキット」をインストールします。ツールキットは、必ず既定のフォルダにインストールするようにします。カスタム設定マネージャまたはプロファイラを起動するには、**[スタート]** をクリックして Reflection インストールを含むフォルダ (既定では **Attachmate Reflection**) を選択し、**[管理ツール]**、評価するツールの順にクリックします。

ヒント : カスタム設定マネージャを十分に評価するには、Reflection の管理者用インストールを使用可能にする必要があります。管理者用インストールは、カスタム設定マネージャの **[インストールの準備]** ダイアログボックスを使用して実行できます。

Reflection 製品の配布に関する詳細の参照先

これらのツールの詳細については、製品のオンラインヘルプを参照してください。Reflection の準備と配布についての包括的な概要と手順については、http://support.wrq.com/tutorials/deploy/ の「Deployment Guide」(英語版) を参照してください。

結び

ご使用の環境で Reflection を十分に評価していただけたでしょうか ? Reflection 製品の詳細については、弊社の Web サイト www.attachmatewrq.jp をご覧ください。

* 管理者用ツールキットは、評価版 CD または製品 CD にのみ収録されています。このツールキットは、Reflection からダウンロードした評価版の Reflection には含まれていません。無料の評価版 CD をご希望の方は、弊社までご連絡ください。

attachmateWRQ™

本社
1500 Dexter Avenue North
Seattle, Washington 98109
TEL 206 217 7500
800 872 2829
FAX 206 217 7515

日本支社
東京
TEL 03 5560 8970
FAX 03 5560 8975
日本語 Web サイト attachmatewrq.jp
日本語 E-mail j-info@attachmatewrq.com

その他の海外支店については、www.attachmatewrq.jp をご覧ください。

【販売代理店】
CYBERNET
サイバネットシステム株式会社
本　　社 〒112-0012 東京都文京区大塚2-15-6 ニッセイ音羽ビル
Tel:(03)-5978-5453 Fax:(03)-5978-2201
西日本支社 〒540-0028 大阪市中央区常盤町1-3-8 中央大通FNビル
Te:(06)-6940-3650 Fax:(06)-6940-3601

■ http://www.cybernet.co.jp/reflection/ ■ rinfo@cybernet.co.jp