BigFix Remote Control オンデマンド・ターゲット・ガイド

目次

第 1 章. BigFix Remote Control オンデマンド・ターゲット・ガイドの概要

ターゲット・ソフトウェアがインストールされていないターゲットとのリモート・コントロール・セッションをインターネット経由で開始するには、Remote Control を使用します。

Remote Control には、Remote Control サーバーでセッションを認証および管理できるようにするためのターゲット・ソフトウェアを一時的にインストールする目的で使用できる機能が用意されています。 また、場所に関係なく、Lite Web Portal を使用してインターネットまたはイントラネットからオンデマンド・ターゲットを管理することもできます。

これらのリモート・コントロール・セッションは、ブローカー・コンポーネントを使用して接続を確立することによって、開始されます。Remote Control は、ターゲット・ソフトウェアをインストールする前にターゲット・ユーザーが必須情報を入力するためにアクセスできるデフォルトの Web ページを提供しています。この Web ページは、インターネットで公開する必要があります。この Web ページは、Remote Control サーバー・コンポーネントがインストールされている場合に使用できます。ただし、セキュリティー上の理由から、サーバーがインターネット上で見える状態にしないでください。したがって、インターネットに接続された HTTP またはアプリケーション・サーバーで Web ページをホストしたり、リバース・プロキシーを利用して Web ページを公開したりすることはできます。ブローカーをリバース・プロキシーとしてセットアップできます。リバース・プロキシーを使用すると、インターネット上のサーバーに対するフルアクセスがなくても、Web ページにアクセスできます。リバース・プロキシーの使用の詳細については、インターネット・ユーザーのオンデマンド・ターゲット・ポータルへのアクセスを参照してください。Web ページをカスタマイズするには、ページに入力フィールドを追加します。Web ページを独自の会社 Web サイトに組み込むこともできます。

ターゲット・ソフトウェアがインストールされ、サーバーで接続情報が認証されると、リモート・コントロール・セッションが開始されます。ただし、コントローラー・ユーザーがターゲットにアクセスするための十分なアクセス権限を持っていない場合は、リモート・コントロール・セッションが拒否されます。オンデマンド・ターゲットからの接続では、ブローカーに到達するために HTTP プロキシー・サーバーを使用できます。プロキシー・サーバーが存在する場合は、プロキシー設定が、Internet Explorer のプロキシー設定または Firefox のプロキシー設定から自動的に取得されます。プロキシー・サーバーに認証が必要な場合、セッション開始前に、ターゲット・ユーザーはプロキシー資格情報を入力するように求められます。リモート・コントロール・セッション中に使用可能な機能は、サーバー・ポリシーによって決まります。ターゲット・ソフトウェアは、セッション終了時にターゲット・コンピューターから削除されます。リモート・コントロール・セッション中に使用可能な機能について詳しくは、「*BigFix® Remote Control* インストール・ガイド」を参照してください。

注: オンデマンド・ターゲットとのセッションはサーバーで管理されますが、ターゲットは未登録として分類されます。ターゲットの詳細はサーバーに保存されず、ターゲット・ソフトウェアはセッション終了時に削除されます。セッションに使用されるポリシーは、コントローラー・ユーザーの ID にのみ基づきます。

ランディング・ページの URL の構成

Remote Control は、ターゲット・ユーザーがターゲット・ソフトウェアを一時的にインストールするためにアクセスできるデフォルトの Web ページを提供しています。この Web ページの URL は `http://trcserver/trc/`

`ondemand/index.jsp` です。変数 *trcserver* は、ご使用の Remote Control サーバーのホスト名または IP アドレスです。デフォルトの Web ページは、Remote Control サーバーがインストール済みの場合に提供されます。ターゲット・ユーザーがアクセスできる URL を提供するようにサーバー・プロパティーを構成することもできます。定義された URL は、コントローラー・ユーザーがブローカー・リモート・コントロール・セッションを開始したときにコントローラー・ユーザーに表示されます。

URL の定義に使用するプロパティーは **ondemand.url** で、これは `ondemand.properties` ファイルに含まれています。このプロパティーを構成するには、以下の手順を実行します。

注: プロパティー・ファイルを手動で編集することもできます。手動で編集した後は、必ず**「アドミニストレーター」 > 「アプリケーションをリセット」**をクリックしてください。

1. 有効な管理者 ID およびパスワードでサーバー UI にログオンします。
2. **「アドミニストレーター」 > 「プロパティー・ファイルを編集」**をクリックします。
3. **ondemand.properties** を選択します。
4. **ondemand.url** プロパティーを適切な値に設定します。

   プロパティーをブランクのままにする

   コントローラー・ユーザーに対して URL を表示しないようにするには、プロパティーの値を入力しないでください。

   Web ページを表示する

   ondemand.url プロパティーは、デフォルトで `https://localhost/trc/ondemand/index.jsp?conncode=%c` に設定されます。`localhost` をリモート・コントロール・サーバーのアドレスに置き換えます。リバース・プロキシーを使用するには、`localhost/trc/ondemand` を、リバース・プロキシーとして構成されているブローカーの完全修飾パブリック・ドメイン名に置き換えます。例えば、`https://broker.example.com/index.jsp?conncode=%c` です。リバース・プロキシーの構成について詳しくは、インターネット・ユーザーのオンデマンド・ターゲット・ポータルへのアクセスを参照してください。localhost を置き換えない場合、`trc_broker.properties` ファイルの **ServerURL** プロパティーに定義されている値が、コントローラーに表示される URL の作成に使用されます。%c 変数は、URL がコントローラー・ウィンドウに表示されるときにセッション接続コードに置き換えられます。デフォルト・ページでは、セッション接続コードの入力が必要です。

   このプロパティーを、カスタマイズした独自の Web ページの URL に設定することもできます。

表 1. コントローラー・ユーザーに対する URL の表示方法。

ondemand.url=	ServerURL=	URL の表示方法
`http://localhost/trc/ondemand/index.jsp`	`https://rcserver.com/trc`	`https://rcserver.com/trc/ondemand/index.jsp`

ondemand.url=	ServerURL=	URL の表示方法
`https://mypage.com/trc/ondemand/index.jsp?conncode=%c`	`https://mycompany.com/trc`	`https://mypage.com/trc/ondemand/index.jsp?conncode=1234567` 接続コードが 1234567 の場合
`https://broker.example.com/index.jsp?conncode=%c`	`https://rcserver.com/trc`	`https://broker.example.com/index.jsp?conncode=1234567` 接続コードが 1234567 の場合

注: この例では、次の 3 つのホスト名があります。

- ***rcserver.com*** は、サーバーがブローカーから直接アクセスできる場合に使用される Remote Control サーバーのホスト名です。
- ***mycompany.com*** は、HTTP プロキシー経由で Remote Control サーバーにアクセスするために使用されるプロキシー・ホスト名です。
- ***broker.example.com*** は、Remote Control ブローカーのパブリック DNS です。
- ***mypage.com*** は、HTTP プロキシー経由で Remote Control ブローカーにアクセスするために仮想ホスト名として使用されるパブリック DNS です。

上記の 4 つのすべての組み合わせが表に示されているわけではありません。

5. **「送信」**をクリックします。
6. **「アドミニストレーター」 > 「アプリケーションをリセット」**をクリックします。

定義された URL は、ユーザーがブローカー・リモート・コントロール・セッションを開始したときに**「接続コード」**ウィンドウに表示されます。

カスタム入力フィールドの構成

ターゲット・ソフトウェアのダウンロードおよび一時インストールのプロセス中に使用されるデフォルトの Web ページに、入力フィールドを追加できます。

Remote Control には、必須の接続コード・フィールドを持つデフォルト Web ページが提供されています。サーバー・プロパティーを編集して、この Web ページに入力フィールドを追加することができます。ただし、ページの設計や動作を変更すると、サーバーのアップグレードがあった場合にカスタマイズは自動的に維持されません。

カスタム・フィールドを作成するには、以下の手順を実行します。

1. 有効な管理者 ID およびパスワードでサーバー UI にログオンします。
2. **「アドミニストレーター」 > 「プロパティー・ファイルを編集」**をクリックします。
3. **ondemand.properties** を選択します。
4. カスタム・フィールドの値を入力します。

ondemand.custom.field.x.label

フィールドの表示名を入力します。ラベルに対して入力されたテキストは、デフォルトの Web ページに表示されます。

ondemand.custom.field.x.required

このフィールドが必須フィールドかどうかを判別する値を設定します。

True

ターゲット・ユーザーはこの入力フィールドに情報を入力する必要があります。

注: 値を true に設定した場合、ラベル・フィールドの値も定義する必要があり、そうしない場合、このフィールドは表示されません。

False

ターゲット・ユーザーはこの入力フィールドにオプションで情報を入力することができます。

このフィールド定義について詳しくは、オンデマンド・プロパティー・ファイルを参照してください。

5. 「**送信**」をクリックします。
6. **「アドミニストレーター」 > 「アプリケーションをリセット」**をクリックします。

ターゲット・ソフトウェアのダウンロードおよび一時インストールのプロセスを開始するために使用される Web ページに、カスタム・フィールドが表示されます。新しいプロパティーを追加するには、プロパティー・ファイルを手動で編集する必要があります。手動で編集した後、**「アドミニストレーター」 > 「アプリケーションをリセット」**をクリックする必要があります。新しいプロパティー値について詳しくは、オンデマンド・プロパティー・ファイルを参照してください。

カスタム・ランディング・ページの作成

ターゲット・ソフトウェアをダウンロードおよび一時インストールするプロセスを開始するために使用する Web ページをカスタマイズできます。Web ページは、ユーザーの企業 Web サイトに統合できます。

オンデマンド・ターゲットとのリモート・コントロール・セッションには、リモート・コントロール・サーバーの特定のリソースが、インターネット経由でユーザーに使用可能になることが必要です。ただし、リモート・コントロール・サーバーがインターネットから直接使用可能になることは好ましくありません。

したがって、必要なリソースの数が少ないことから、以下に示すいくつかの方法を使用して、オンデマンド・ターゲット機能を使用可能にすることができます。

- 環境内の少なくとも 1 つのブローカーをリバース・プロキシーとして構成します。この構成によって、インターネット・ユーザーは、リモート・コントロール・サーバーの限定されたリソース・セットにアクセスすることが許可されます。このリソースは、インターネット経由のオンデマンド・ターゲット接続をサポート

するためのみに必要とされるものです。リバース・プロキシーの構成について詳しくは、インターネット・ユーザーのオンデマンド・ターゲット・ポータルへのアクセスを参照してください。
- オンデマンド・ターゲットとのリモート・コントロール・セッションを実行するポータルとして使用する別個の Web サイトを有効にします。

両方のケースで、`ondemand.properties` ファイルの **ondemand.url** プロパティーの値を編集する必要があります。オンデマンド・ターゲット・アプリケーションへのアクセスを提供する外部サービスを参照する URL を設定します。静的 Web サイトまたは動的 Web サイトを使用可能に設定できます。**ondemand.url** プロパティーの編集について詳しくは、ランディング・ページの URL の構成を参照してください。

Lite Web Portal を使用して Remote Control セッションを起動し、カスタム・ランディング・ページを構成する場合は、`ondemand.properties` ファイル内の **liteweb.portal.url** プロパティーの値を編集する必要があります。Lite Web Portal プロパティーの設定の詳細については、Lite Web Portal の設定 を参照してください。

静的カスタム Web ポータルの構成

静的 Web ポータルを構成することにより、 オンデマンド・ターゲットの機能を自社の Web サイトに統合することができます。この種の統合を行うには、 一連のリソースをリモート・コントロール・サーバーのデフォルト・ポータルから 外部にある自社の Web サイトにコピーする必要があります。この Web サイトを、 オンデマンド・セッションを実行する静的ポータルとして使用します。

静的という用語は、Web サーバー・システムでファイル自体が編集されない限り、Web サーバーによって提供されるコンテンツが変化しないことを指します。

ご使用の Web サイトにコピーする必要があるリソース群は、 プラグインおよびオンデマンド・ターゲット・アプリケーションのファイルです。これらのファイルをご使用の Web サイトにコピーすると、 オンデマンド・セッションの開始に必要なすべてのファイルをそこからダウンロードできます。

この方法の欠点は、 静的ポータルと内部リモート・コントロール・サーバーの間で通信が行われないことです。そのため、カスタム・データを提供したり、リモート・コントロール・セッションの開始前に接続コードを検証したりすることはできません。構成も静的であるため、 オンデマンド・ターゲットの開始後に接続コードを提供する必要があります。

静的ポータルを構成するための前提条件は、インターネット経由でコンテンツを提供する Web サーバーがあることです。コンテンツの追加や編集を行えるように、Web サーバーに対する許可が必要です。 また、Web テクノロジーの知識も必要です。

静的ポータルを構成するには、以下の手順を実行します。

1. リモート・コントロール・サーバー上の以下のディレクトリーに移動します。
   RC_SERVER_INSTALL_DIR`\wlp\usr\servers\trcserver\apps\TRCAPP.ear\trc.war\ondemand`

   各表記の意味は次のとおりです。*RCSERVER_INSTALL_DIR* は、Remote Control サーバーのインストール・ディレクトリーです。
2. 10.x.x.*<version>* ディレクトリーを、 ご使用の Web サイトの `\ondemand` ディレクトリーにコピーします。ディレクトリーには、`ODTJPlugin.jar`、`ODTIEPlugin.cab`、`odtffplugin.xpi`、および

`TRCPlayer.jar` の各ファイルが入っています。ディレクトリーの 1 つには、`lnx32` および `win32` の各ディレクトリーが入っています。これらのディレクトリーの内容もコピーする必要があります。

3. 構成ファイルを作成します。
   構成ファイルには、使用可能なブローカーの詳細情報を格納する必要があります。ブローカーのホスト名をセミコロン区切りのリストで指定します。ここには、ブローカーによって提示された証明書が信頼できるかどうかを検証するために使用できる証明書のリストも格納します。このファイルに拡張子 `.properties` を付けて保存します。
   例えば、`config.properties` に以下の項目を格納します。

```
BrokerList=rcbroker.example.org:8881
-----BEGIN CERTIFICATE-----
Base64 encoded certificate data
-----END CERTIFICATE-----
```

   各部の意味は以下のとおりです。*Base64 encoded certificate data* は、特定の証明書の証明書データです。証明書データは Remote Control サーバーから コピーすることができます。追加する各証明書には BEGIN CERTIFICATE セクションおよび END CERTIFICATE セクションが必要です。
   a. **「アドミニストレーター」 > 「すべての信頼証明書 (All Trusted Certificates)」**を選択します。
   b. 証明書を選択します。
   c. **「証明書の編集」**を選択します。
   d. 証明書のテキストを構成ファイルにコピーします。
4. オンデマンド・ターゲットの開始に使用できるインストール方式ごとに HTML ページを作成します。

ActiveX コントロール

ActiveX コントロールによるインストール・メカニズムを提供するために使用する HTML ページには、アプレットを開始するための JavaScript™ コードの短いセグメントを入れる必要があります。それには、ActiveX コントロールをインポートするための **<object>** タグも含まれます。以下の例では、`config.properties` という構成ファイルと `rcweb.example.org` という Web サーバーを使用しています。パスおよびファイル名は、 ご使用の環境に合わせて変更する必要があります。**<head>** タグの中には、 以下の要素を追加して必要な JavaScript™ コードを入れる必要があります。

```
<script  type="text/javascript">
 function autoLaunch() {
var ctl = document.getElementById('OnDemandCtl');
 ctl.LaunchOnDemand("",
 "http://rcweb.example.org/ondemand/config.properties");
 }</script>
```

ページの **<body>** 要素には、以下の要素を入れる必要があります。

```
<div style="height:200px">
<object id="OnDemandCtl"
classid="CLSID:E8A8645D-629A-4E27-B66C-67AE140C76A4"
```

```
codebase="ondemand/VERSION_NUMBER_1/ODTIEPlugin.cab#VERSION_NUMBER_1" >
</object>
</div>
```

VERSION_NUMBER_1 は、 ステップ 2 で `ODTIEPlugin.cab` ファイルをコピーした宛先フォルダーのバージョン番号で置き換えてください。例えば、codebase="9.1.0.0020/ODTIEPlugin.cab#9.1.0.0020" とします。

ターゲット・ユーザーが Internet Explorer を使用しており、ActiveX がサポートされていて有効化されている場合は、HTML ページにアクセスすると、 オンデマンド・ターゲット・アプリケーションが自動的にダウンロードされて開始されます。

Firefox プラグイン

注: Mozilla はレガシー・アドオンのサポートを終了したため、Firefox プラグインのインストールは、Firefox バージョン 57 以上では正常に完了しません。このインストール方法のサポートは、バージョン 9.1.4. IF0003 (ビルド番号 0309) 以降のリモート・コントロールでは推奨されません。

Firefox プラグインによるインストール・メカニズムを提供するために使用する HTML ページには、 以下のコンテンツを入れる必要があります。サーバーは、`.xpi` ファイルを MIME タイプ「application/x-xpinstall」に関連付けるように構成する必要があります。MIME タイプの構成方法は、 使用する Web サーバーによって異なります。以下の例では、`config.properties` という構成ファイルと `rcweb.example.org` という Web サーバーを使用しています。パスおよびファイル名は、 ご使用の環境に合わせて変更する必要があります。`ondemand.js` ファイルおよび `ondemandff.js` ファイルを Remote Control サーバーの `ondemand` ディレクトリーからご使用の Web サイトの `ondemand` ディレクトリーにコピーします。**<head>** タグの中には、 以下の要素を追加して必要な JavaScript™ コードを入れる必要があります。

```
<script  type="text/javascript" src="ondemand/ondemandff.js"></script>
<script type="text/javascript">
  function checkForPlugin() {
 ondemandFFPlugin.checkPlugin();
}
</script>
```

ページの **<body>** タグには、以下の内容 "setTimeout(checkForPlugin, 2000);" を指定した **onload** 属性を含める必要があります。

例えば、以下のようにします。

```
<body onload="setTimeout(checkForPlugin, 2000);">
```

<body> タグには、以下の要素も含める必要があります。

```
<form name="downloadPluginWin32" id="downloadPluginWin32"
action="ondemand/VERSION_NUMBER_1/win32/odtffplugin.xpi" method="get"
onSubmit="return true;"></form>
<form  name="downloadPluginLnx32" id="downloadPluginLnx32"
action="ondemand/VERSION_NUMBER_1/lnx32/odtffplugin.xpi"
 method="get"  onSubmit="return true;"></form>

<object id="odl-params">
   <param name="config_url"
value="http://rcweb.example.org/ondemand/config.properties"/>
</object>

<object id="odl-plugin-handle">
<param name="odt-plugin-version" value="VERSION_NUMBER_1">
</object>
```

VERSION_NUMBER_1 は、ステップ 2 で `odtffplugin.xpi` ファイルをコピーした宛先フォルダーのバージョン番号で置き換えてください。例えば、action="9.1.0.0020/odtffplugin.xpi とします。

ターゲット・ユーザーが Firefox ブラウザーを使用しているときに Firefox プラグインおよび JavaScript™ が有効になっている場合は、HTML ページにアクセスすると、オンデマンド・ターゲット・アプリケーションが自動的にダウンロードされて開始されます。

Java™ アプレット

アプレットによるインストール・メカニズムを提供するために使用する HTML ページでは、 ページの **<body>** 要素に以下のコンテンツを入れる必要があります。以下の例では、`config.properties` という構成ファイルと `rcweb.example.org` という Web サーバーを使用しています。パスおよびファイル名は、 ご使用の環境に合わせて変更する必要があります。

```
<applet archive="VERSION_NUMBER_1/ODTJPlugin.jar"
code="com.bigfix.remotecontrol.odt.plugin.app.ODTJPluginApplet">
  <param name="codebase_lookup" value="false" />
  <param name="config_url"
value="http://rcweb.example.org/ondemand/config.properties"/>
</applet>
```

VERSION_NUMBER_1 は、 ステップ 2 で `ODTJPlugin.jar` ファイルをコピーした宛先フォルダーのバージョン番号で置き換えてください。ターゲット・ユーザーのコンピューターで Java™ が有効になっている場合は、HTML ページにアクセスすると、 オンデマンド・ターゲット・アプリケーションが自動的にダウンロードされて開始されます。

Java™Web Start

Java™ Web Start によるインストール・メカニズムの場合は HTML ページが不要です。JNLP ファイルが作成されていることが必要です。JNLP ファイルには、 別の HTML ページから直接リンクすることができます。ページにアクセスすると、 オンデマンド・ターゲット・アプリケーション用の Java™ Web Start 配信プラグインがアクティブになり、 自動的にアプリケーションがダウンロードされて開始されます。

JNLP ファイルを作成するには、 以下のサンプル・コンテンツを使用してください。以下の例では、`config.properties` という構成ファイルと `rcweb.example.org` という Web サーバーを使用しています。パスおよびファイル名は、 ご使用の環境に合わせて変更する必要があります。タイトルの 10.x.x を適切なターゲット・バージョンに変更します。

```
<?xml version="1.0" encoding="utf-8"?>
<jnlp spec="1.0+"
 codebase="http://rcweb.example.org/ondemand/VERSION_NUMBER_1/">
<information>
 <title>Remote Control Launcher for
 On Demand target 10.x.x</title>
 <vendor>HCL</vendor>
</information>
<security><all-permissions/></security>
<resources>
 <j2se version="1.4+"/>
 <jar href="ODTJPlugin.jar"/>
</resources>
<application-desc>
<argument>--config_url</argument>
<argument>http://rcweb.example.org/ondemand/config.properties</argument>
</application-desc>
</jnlp>
```

VERSION_NUMBER_1 は、ステップ 2 で `ODTJPlugin.jar` ファイルをコピーした宛先フォルダーのバージョン番号で置き換えてください。

注: JNLP ファイルの URL を フォールバック URL としてカスタム HTML ページに追加することができます。ターゲット・ユーザーは、 別のインストール方法を選択したときにオンデマンド・ターゲットの開始に失敗した場合に、 このリンクをクリックすることができます。Java™ Web Start のインストール方法を使用してターゲットがダウンロードされ、開始されます。

5. **オプション:** ターゲット・ユーザーが Remote Control プレイヤーを開始するためにアクセスできる HTML ページを作成します。

プレイヤーを使用すると、 保存してあるオンデマンド・セッションの記録を再生することができます。プレイヤーを開始するには、 ページに以下の要素を入れる必要があります。次の例では、`rcweb.example.org` という Web サーバーを使用しています。パスは、ご使用の環境に合わせて変更する必要があります。

```
<applet id="player" width="100" height="100" align="middle"
archive="VERSION_NUMBER_1/TRCPlayer.jar"
 code="com.bigfix.remotecontrol.ayudame.playerui.RecorderApplet">
<param name="codebase_lookup" value="false">
</applet>
```

VERSION_NUMBER_1 は、 ステップ 2 で `TRCPlayer.jar` ファイルをコピーした宛先フォルダーのバージョン番号で置き換えてください。
例えば、`http://rcweb.example.org/ondemand/9.1.0.0020/TRCPlayer.jar` です。

動的カスタム Web ポータルの構成

動的 Web ポータルを構成することによって、オンデマンド・ターゲット機能をユーザー独自の Web サイトに統合することができます。このタイプの統合によって、ユーザーの Web サイトが、サービス URL のセットを介して Remote Control サーバーと通信できるようになります。

この URL は以下のために使用できます。

- カスタム・セッション・データを Remote Control サーバーに送信し、サーバーに保存できるようにします。
- 接続コードを検証し、オンデマンド・ターゲット・アプリケーションおよびデリバリー・プラグインをダウンロードする前にコードの検査が終わっているようにします。
- ブローカーの環境構成を動的に取得することで、プロパティー・ファイルを手動で編集する必要をなくします。例えば、ブローカーのセットが変更された場合や、新しい信頼証明書が追加された場合です。

オンデマンド・ターゲット機能では、動的 Web がセットアップされていることが必要です。これは、ご使用の Web サーバーと内部の Remote Control サーバーとの相互作用を、ユーザーの Web サイト内にプログラムで設定する必要があるためです。したがって、ご使用の環境で使用されている特定の動的 Web テクノロジーに関する十分な実用的知識が必要です。

動的 Web サイトを実装する際、様々なテクノロジーを使用することができます。選択された基本テクノロジーによって必要な手順が異なるため、必要とされる機能を実現する方法を詳細に説明することはできません。

動的ポータルを構成するには、以下の手順を実行します。

1. リモート・コントロール・サーバー上の以下のディレクトリーに移動します。
   RC_SERVER_INSTALL_DIR\wlp\usr\servers\trcserver\apps\TRCAPP.ear\trc.war\ondemand

   各表記の意味は次のとおりです。*RCSERVER_INSTALL_DIR* は、Remote Control サーバーのインストール・ディレクトリーです。`ondemand` ディレクトリーには 10.x.x バージョン番号ディレクトリーが含まれています。

2. 最新のバージョン番号ディレクトリーから、各自の Web サイトのバージョン番号ディレクトリーに、以下のファイルおよびディレクトリーをコピーします。

   ファイル

   `ODTJPlugin.jar`、`ODTIEPlugin.cab`、`odtffplugin.xpi`、および `TRCPlayer.jar`。

   ディレクトリー

   lnx32、lnx64、および win32。

   これらのディレクトリーの内容も、ご使用の Web サイトにコピーする必要があります。

3. ターゲット・ユーザーがカスタム・データおよび接続コードを入力するためのページを作成します。このページは、ご使用の Web サーバーによって生成できます。`trc/broker/OnDemandCustomDataConfig` サービス URL を使用して、Remote Control サーバーに構成されている現在のカスタム・データ・フィールドのセットを取得できます。

   表 2. `/trc/broker/OnDemandCustomDataConfig` URL

   `/trc/broker/OnDemandCustomDataConfig` URL のパラメーターおよび出力の説明。

URL	**`/trc/broker/OnDemandCustomDataConfig`**
HTTP メソッド	GET
パラメーター	N/A

出力	HTTP 200 OK (以下のペイロードを持つ):
	`<response>`
	`<remotecontrol>`
	`<field name="Field1" label="Label for Field 1"`
	`required="true or false"/>`
	`<field name="Field2" label="Label for Field 2"`
	`required="true or false"/>`
	`....`
	`</remotecontrol></response>`
	
	返される **<field>** エレメントの数は、サーバー上の `ondemand.properties` ファイルの構成によって異なります。
	
	name 属性は、サーバーに返信されるときにフィールドに対して期待されるパラメーター名を指定します。
	
	label 属性は、Accept-Language ヘッダーを使用することによって HTTP 要求内で要求されたロケールの表示値を指定します。

URL	`/trc/broker/OnDemandCustomDataConfig`

required 属性の値は true または false です。この属性は、Remote Control サーバーに送信されたときにこのフィールドに値が必須かどうかを指定します。

ページが動的ポータルに送信されると、URL `broker/OnDemandSessionData` を使用して、データを Remote Control サーバーに送信できます。**OnDemandSessionData** URL は、接続コードと、提供されたカスタム・データ・フィールドを検証します。

注: ターゲット・ユーザーのブラウザーは Remote Control サーバーに直接アクセスできませんが、動的ポータルにのみアクセスできるため、データを送信する必要があります。

表 3. `/trc/broker/OnDemandSessionData` URL

`/trc/broker/OnDemandSessionData` URL のパラメーターおよび出力の説明。

URL	`/trc/broker/OnDemandSessionData`
HTTP メソッド	POST
パラメーター	conn_code
出力	`HTTP 200 OK` - データが正しい場合 ペイロードなし `HTTP 404` - 接続コードが不明 ペイロードなし `HTTP 400` - 必要なセッション情報が空白であるか、提供されていません。 ペイロードなし `HTTP 408` - 必要なセッションがタイムアウトになりました ペイロードなし

データの送信に成功した場合、動的ポータルは、インストール・プラグインがアクティブ化されているページにターゲット・ユーザーをリダイレクトします。

4. **起動**ページを作成します。
   ページを生成するためのコンテンツについては、ステップ 4 を参照してください。 `trc/broker/OnDemandSessionConfig` URL を使用することによって、Web サーバーから**起動**ページを生成できます。OnDemandSessionConfig URL は、プラグインによって使用される構成を返します。要求をサーバーに転送して構成データを返す、単純なページが生成される必要があります。**config_url** パラメーターの値をページの URL に設定します。プラグインは次に、**config_url** パラメーターに定義された URL を使用して、Remote Control サーバーから構成を取得します。

表 4. `/trc/broker/OnDemandSessionConfig` URL

`/trc/broker/OnDemandSessionConfig` URL のパラメーターおよび出力の説明。

URL	`/trc/broker/OnDemandSessionConfig`
HTTP メソッド	GET
パラメーター	conn_code
出力	HTTP 200 OK - 接続コードが有効の場合

```
ConnectionCode=12345
BrokerList=rcbroker.example.org:8881
-----BEGIN CERTIFICATE-----
Base64 encoded certificate data
-----END CERTIFICATE-----
```

各表記の意味は次のとおりです。*Base64 encoded certificate data* は、特定の証明書の証明書データです。

HTTP 404 - 接続コードが不明

ペイロードなし

.

インターネット・ユーザーのオンデマンド・ターゲット・ポータルへのアクセス

イントラネット内の Remote Control サーバー上にあるオンデマンド・ポータルへのアクセスをインターネット・ユーザーに提供するように、DMZ のリバース・プロキシーを構成できます。リバース・プロキシーはオンデマンド・ポータルへのアクセスのみを許可し、Remote Control サーバーの他のセクションへのアクセスを許可してはなりません。

Remote Control は、展開および構成を容易にする統合リバース・プロキシーを提供します。Remote Control ブローカー・コンポーネントには、制限付きのプロキシー機能があります。統合リバース・プロキシーでは、Remote Control コンポーネントのみを使用してブローカー環境を展開できます。サード・パーティー・コンポーネントは必要ありません。リバース・プロキシーは、HTTP と HTTPS の両方をサポートし、HTTP と HTTPS の組み合わせもサポートします。例えば、HTTP プロトコルを使用してブローカー URL を構成し、HTTPS を使用してブローカー・プロパティー・ファイル内のサーバー URL を構成できます。ターゲット・ユーザーは、ブローカーのホスト名を含む HTTP オンデマンド URL を入力します。リバース・プロキシーはこの要求を受け入れ、定義済みの HTTPS サーバー URL を使用して、サーバーからオンデマンド・ポータル・ページを取得します。プロキシーは、オンデマンド・ポータルにアクセスする目的でのみ使用でき、汎用リバース・プロキシーとして構成することはできません。プロキシーは、スケーラビリティーに対応するように設計されていません。非常に高い使用率が見込まれる展開の場合は、既

製のリバース HTTP プロキシーを使用できます。また、独自のインターネット Web サイトでカスタム・オンデマンド・ポータルをホストすることもできます。

リバース・プロキシーの制限:

- ブローカーは HTTP 1.0 および 1.1 のみをサポートします。他のバージョンの HTTP 要求では、「HTTP 505 サポートされていないバージョン」エラーになります。
- リバース・プロキシーを汎用リバース・プロキシー・サーバーとして使用することはできません。
- リバース・プロキシーを使用して、Remote Control サーバーのその他の部分をインターネットに公開することはできません。例えば、ターゲットによる登録またはユーザーによるログインを許可するようにリバース・プロキシーを構成することはできません。

HTTP および HTTPS 接続を listen するための ブローカーの構成

HTTP および HTTPS 接続を受け入れるようにブローカーを構成するには、ブローカーの構成ファイルに接続を追加します。

`trc_broker.properties` ファイルを編集して、ブローカーのプロキシー機能を有効にするために必要な接続タイプおよびパラメーターを構成します。

Windows™ コンピューターの場合、このファイルはブローカーの作業ディレクトリーの `\Broker` ディレクトリーにあります。

Windows™ システムを使用している場合、ファイルは `\ProgramData\BigFix\Remote Control\Broker\` にあります。Linux™ システムの場合、このファイルは `/etc` ディレクトリーにあります。ブローカー構成について詳しくは、「*BigFix® Remote Control* 管理者ガイド」を参照してください。

接続を構成するには、以下の手順を実行します。

- HTTP 接続を受け入れるようにブローカーを構成するには、以下の手順を実行します。

  1. 接続タイプ **InboundHTTP** を使用して、構成ファイルに接続を追加します。

     prefix.ConnectionType

     接続のタイプを定義します。*InboundHTTP* または *InboundHTTP6* に設定する必要があります。

     InboundHTTP

     IPv4 アドレスを使用する HTTP 接続を listen します。

     InboundHTTP6

     IPv6 アドレスを使用する HTTP 接続を listen します。

  2. オプションのキーワードを設定します。接続では **PortToListen** を除いてデフォルト構成から値を継承します。

     prefix.PortToListen

listen に使用する TCP ポート。デフォルトは 80 です。

prefix.BindTo

指定されたアドレスのみで着信接続を受け入れます。デフォルトは、デフォルト構成から継承された **DefaultBindTo** の値です。

prefix.RetryDelay

listen ポートを開く試行の間隔。デフォルトは、デフォルト構成から継承された **DefaultRetryDelay** の値です。

- HTTPS 接続を受け入れるようにブローカーを構成するには、以下の手順を実行します。

1. 接続タイプ **InboundHTTPS** を使用して、構成ファイルに接続を追加します。

   prefix.ConnectionType

   接続のタイプを定義します。*InboundHTTPS* または *InboundHTTPS6* に設定する必要があります。

   InboundHTTPS

   IPv4 アドレスを使用する HTTPS 接続を listen します。

   InboundHTTPS6

   IPv6 アドレスを使用する HTTPS 接続を listen します。

2. オプションのキーワードを設定します。接続では **PortToListen** を除いてデフォルト構成から値を継承します。

   prefix.PortToListen

   listen に使用する TCP ポート。デフォルトは 443 です。

   prefix.BindTo

   指定されたアドレスのみで着信接続を受け入れます。デフォルトは、デフォルト構成から継承された **DefaultBindTo** または **DefaultBindTo6** の値です。

   prefix.RetryDelay

   listen ポートを開く試行の間隔。デフォルトは、デフォルト構成から継承された **DefaultRetryDelay** の値です。

   prefix.TLSCertificateFile

   ブローカーの証明書のファイル名およびパス。デフォルトは、デフォルト構成から継承された **DefaultTLSCertificateFile** の値です。

   prefix.TLSCertificatePassphrase

   ブローカーの証明書のパスフレーズ。デフォルトは、デフォルト構成から継承された **DefaultTLSCertificatePassphrase** の値です。

prefix.HTTPSCipherList

ネットワーク接続の保護に使用できる暗号スイートのリスト。デフォルトは、デフォルト構成から継承された **DefaultHTTPSCipherList** の値です。

注: デフォルトのブローカー構成パラメーターについて詳しくは、「*BigFix® Remote Control* 管理者ガイド」を参照してください。

リバース・プロキシーとブローカーの間でのポートの共有

ブローカーがリバース・プロキシーとともに構成されている場合は、 リバース・プロキシーとブローカーの両方にポート 443 を使用することができます。

ブローカーはポート 443 で構成することをお勧めします。理由は、 クライアントが HTTP プロキシーまたは制限のあるファイアウォール・ポリシーを持つネットワークから接続する場合に、 いくつかのポートを除いて発信接続がブロックされてしまう可能性があるためです。ポート 443 への接続は 可能ですが、SSL/TLS プロトコルを確実に使用するための検査が行われる可能性があります。ブローカーがポート 443 を共有するように構成することができます。

エンドポイント、他のブローカー、および HTTPS 要求からの接続を受け入れるポートを構成するには、 ポート 443 で **Inbound** 接続または **Inbound6** 接続を構成し、**InboundHTTPS** 接続または **InboundHTTPS6** 接続を構成します。

例えば、以下のようにします。

1.ConnectionType = Inbound

1.PortToListen = 443

2.ConnectionType = InboundHTTPS

ブローカーは、同じポート **PortToListen** およびインターフェース **BindTo** を使用する 2 つの接続が構成に存在することを検出すると、自動的にそれら 2 つの接続をマージします。

例外として、**InboundHTTP** 接続または **InboundHTTP6** 接続を別の種類のインバウンド接続とマージすることはできません。この制限が設けられている理由は、ブローカーが暗号化なしの接続と暗号化ありの接続を同じポートでサポートしないためです。**InboundHTTP** 接続または **InboundHTTP6** 接続が別の種類のインバウンド接続と同じポートおよびインターフェースで構成されている場合、ブローカーはログにエラーを書き込みます。また、内部で **InboundHTTP** 接続または **InboundHTTP6** 接続を無効にします。

接続のパラメーターは以下の方法でマージされます。

表 5. マージされた接続のパラメーター値

パラメーター	実行される処理
prefix.RetryDelay prefix.TLSCertificateFile prefix.TLSCertificatePassphrase	このパラメーターは、 ロードされた最初の接続から取得されます。以降の接続から得たパラメーターは無視されます。パラメーターが矛盾する場合は、 そのつど警告がログに書き込まれます。
prefix.TLSCipherList	**HTTPSCipherList** は **TLSCipherList** をオーバーライドします。パラメーターが矛盾する場合は、警告がログに書き込まれます。

リバース・プロキシーを使用するためのランディング・ページ URL の設定

ブローカーでリバース・プロキシーを構成すると、 異なった方法でランディング・ページの URL が構成されます。URL には、 サーバーのホスト名および IP アドレスではなく、 ブローカーのホスト名または IP アドレスが含まれていなければなりません。

URL を定義するプロパティーは **ondemand.url** であり、`ondemand.properties` ファイルに含まれています。このプロパティーを構成するには、以下の手順を実行します。

注: プロパティー・ファイルを手動で編集することもできます。手動で編集した後は、必ず**「アドミニストレーター」 > 「アプリケーションをリセット」**をクリックしてください。

1. 有効な管理者 ID およびパスワードでサーバー UI にログオンします。
2. **「アドミニストレーター」 > 「プロパティー・ファイルを編集」**をクリックします。
3. **ondemand.properties** を選択します。
4. **ondemand.url** プロパティーを適切な値に設定します。
   このアドレスには、**inboundHTTP** 接続または **inboundHTTPS** 接続で構成されたブローカーのホスト名または IP アドレスを含める必要があります。例えば、 `https://broker.example.com/index.jsp?conncode=%c`
5. 「**送信**」をクリックします。
6. **「アドミニストレーター」 > 「アプリケーションをリセット」**をクリックします。

定義された URL をターゲット・ユーザーがブラウザーに入力すると、 要求がプロキシーに送信されてサーバーに渡されます。この処理中に、 リバース・プロキシーはこの URL を関連したサーバー URL に書き換え、 ページをサーバーから取得できるようにします。

注: HTTPS の代わりに HTTP を使用するには、以下のようにします。

- ブローカー構成を `InboundHTTPS` ではなく、`InboundHTTP` に設定します。
- **ondemand.url** にプレフィックスとして `https` ではなく `http` を付けます。

未登録ターゲットに対するセッション許可の設定

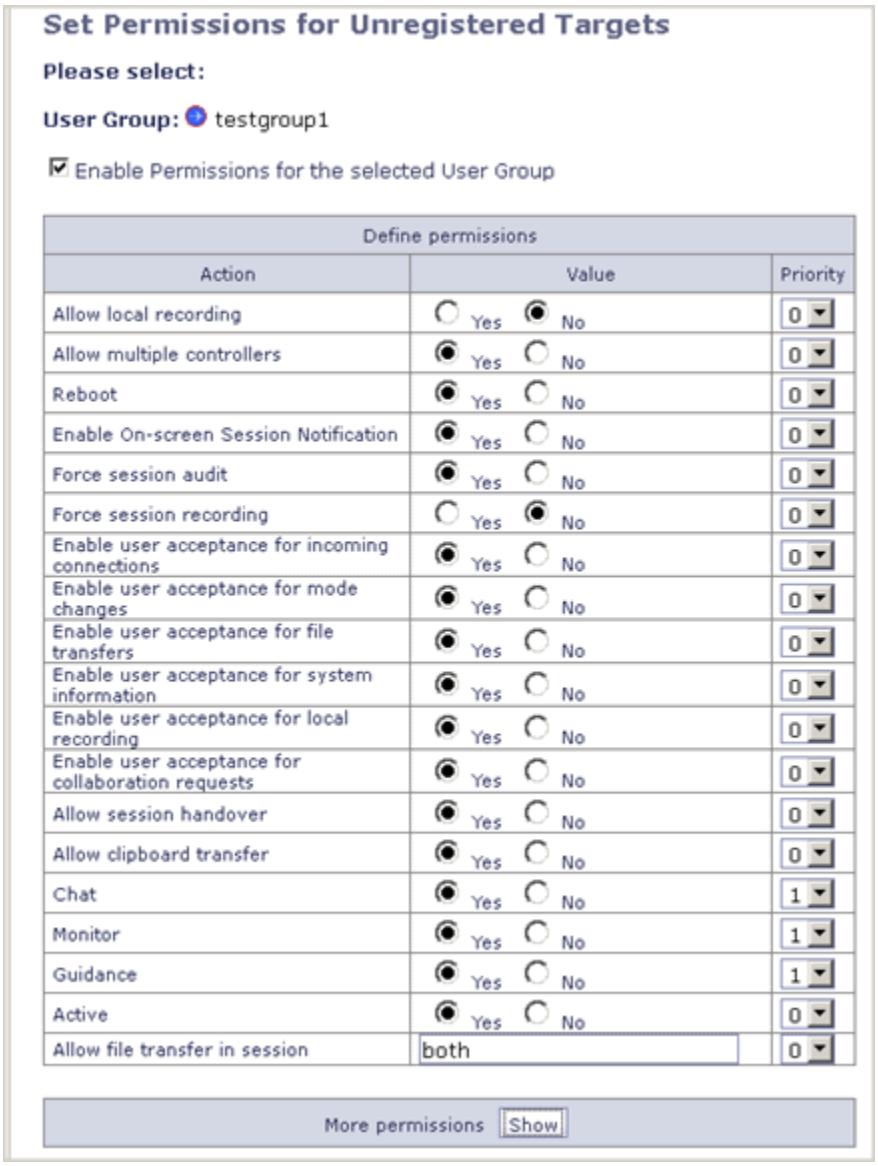
ブローカー・セッションに参加するターゲットは、 サーバーからセッション・ポリシーを受信します。これらのポリシーは、 セッション内のユーザーおよびターゲットが関連付けられているユーザーおよびターゲット・グループ許可リンクから 解決されます。オンデマンド・ターゲットは ブローカーのリモート・コントロール・セッションに参加します。しかし、サーバーには登録されず、 通常のターゲット・グループには属しません。ターゲット・ソフトウェアをインストールして、正しいブローカー設定で構成し、ターゲット・プロパティー **Managed** を「いいえ」に設定したコンピューターを未登録ターゲットにすることもできます。未登録ターゲットに対するセッション許可を定義するには、**「未登録ターゲットに対する許可の設定」**機能を使用します。

未登録ターゲットの場合、 コンピューターの ID は Remote Control サーバーに格納されません。そのため、 ユーザーがリモート・コントロール・セッションを開始できるかどうかの判別や 適用されるポリシーの判別にターゲットの ID を使用することはできません。

未登録ターゲットとのセッションに対するポリシーを設定するには、 コントローラー・ユーザーが属するユーザー・グループを選択します。このグループを使用すると、 管理対象セッションの場合と同じ方法でポリシーが解決されます。コントローラー・ユーザーが属するユーザー・グループに定義されたポリシーは、 未登録ターゲット・セッションに対して選択されたポリシーと結合されます。

未登録ターゲットとのリモート・コントロール・セッションに対するポリシーを定義するには、 以下の手順を実行します。

1. 有効な管理者 ID およびパスワードで Remote Control サーバーにログオンします。
2. レポートを実行してユーザー・グループを表示します。
   検索機能を使用することもできます。
3. ユーザー・グループを選択します。
4. **「未登録ターゲットに対する許可の設定」**を選択します。
   「未登録ターゲットに対する許可の設定」パネルが表示されます。



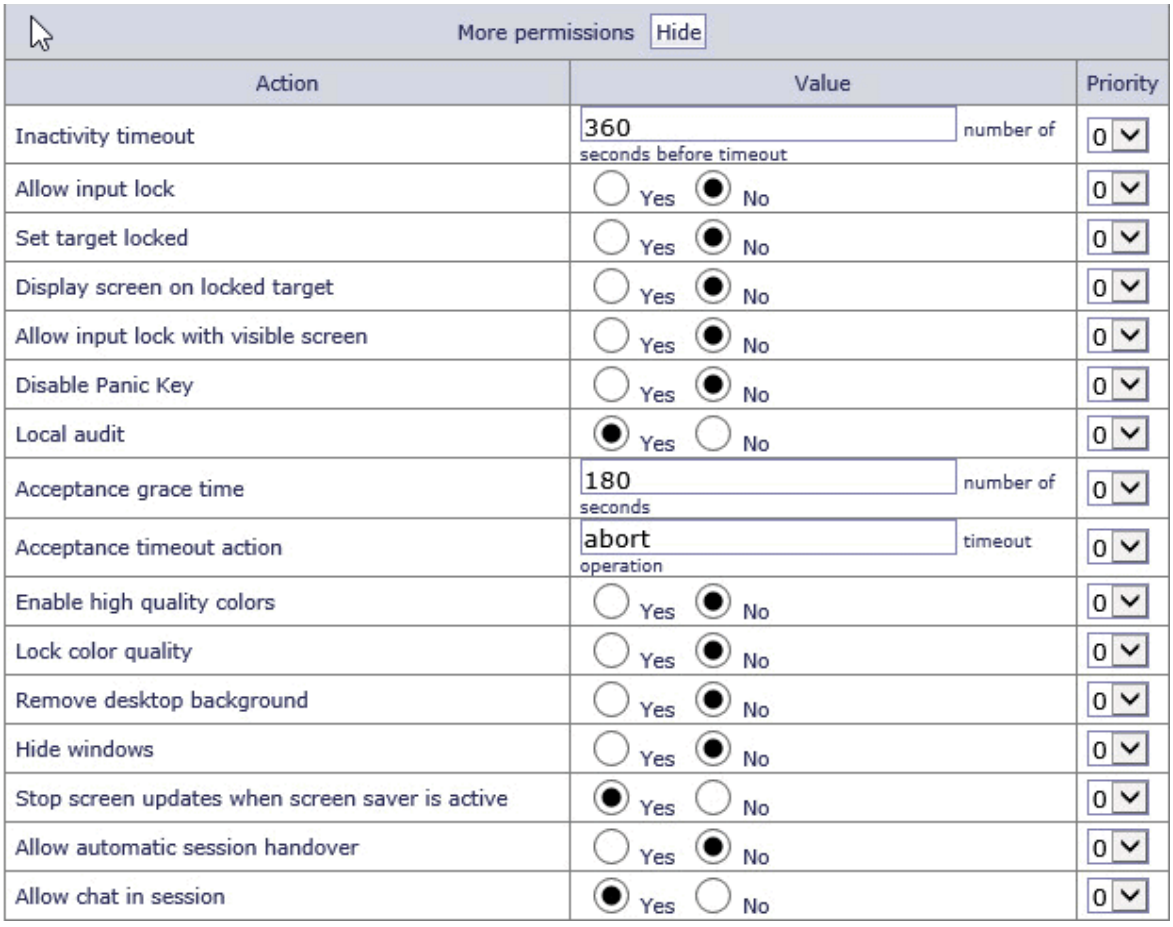
5. 必要に応じて、アイコンをクリックして別のユーザー・グループを選択します。
6. ポリシーを有効にするために、**「選択されたユーザー・グループについて許可を有効にする」**をクリックします。

注: 「選択されたユーザー・グループについて許可を有効にする」をクリアして**「送信」**をクリックした場合、 そのユーザー・グループおよび未登録ターゲットにポリシーは設定されません。

7. ポリシーの値を設定するか、選択されているデフォルト値を保持します。
   ポリシーの優先度の値を設定することもできます。コントローラー・ユーザーが複数のユーザー・グループのメンバーである場合は、 オーバーライド対象のポリシーに高い優先度を選択してください。
   例えば、 コントローラー・ユーザーが group1 および group2 のメンバーであるとします。group2 は、「チャット」が「いいえ」と定義された一連の未登録ターゲット・ポリシーにリンクされています。group1

は「チャット」が「はい」であり、 優先度は 0 です。ユーザーが両方のグループに属するため、 サーバーは「チャット」の値に対して競合する 2 つの値を取得することになり、 「いいえ」の値が適用されます。そのため、group2 の値「いいえ」をオーバーライドして、セッションで「チャット」が「はい」に設定されるようにするには、group1 に対して優先度を 1 として「チャット」を「はい」に設定します。ポリシーについて詳しくは、未登録ターゲットのセッション・ポリシーを参照してください。

8. **「その他の許可」**セクションの**「表示」**をクリックして、追加のポリシーの値を設定します。



9. 必要に応じて許可のスケジュールを設定します。
10. ポリシーをただちに有効にするには、**「送信」**をクリックします。選択したポリシーをいつ有効にするかを定義するには、スケジュールを作成します。スケジュールを作成するには、ステップ 11 に進んでください。
11. **「繰り返しスケジュール」**リストからオプションを選択し、**「送信」**をクリックします。

1 回のみ

ポリシーは、開始日時から終了日時までに限って有効になります。

a. 開始日を `yyyy-mm-dd` の形式で入力するか、カレンダー・アイコンを選択して日付を選択します。
b. 「開始時刻」に `hh:mm:ss` の形式で入力します。
c. 終了日を `yyyy-mm-dd` の形式で入力するか、カレンダー・アイコンを選択して日付を選択します。
d. 「終了時刻」に `hh:mm:ss` の形式で入力します。

毎日

ポリシーは、開始日から終了日までの毎日、選択した開始時刻から終了時刻まで有効になります。

a. 開始日を `yyyy-mm-dd` の形式で入力するか、カレンダー・アイコンを選択して日付を選択します。
b. 終了日を `yyyy-mm-dd` の形式で入力するか、カレンダー・アイコンを選択して日付を選択します。
c. 「開始時刻」に `hh:mm:ss` の形式で入力します。
d. 「終了時刻」に `hh:mm:ss` の形式で入力します。

週次

ポリシーは、開始日から終了日まで毎週、選択した日に、選択した開始時刻から終了時刻まで有効になります。

a. 開始日を `yyyy-mm-dd` の形式で入力するか、カレンダー・アイコンを選択して日付を選択します。
b. 「開始時刻」に `hh:mm:ss` の形式で入力します。
c. 終了日を `yyyy-mm-dd` の形式で入力するか、カレンダー・アイコンを選択して日付を選択します。
d. 「終了時刻」に `hh:mm:ss` の形式で入力します。
e. 日付を選択します。

12. **「送信」**をクリックします。

未登録ターゲットのセッション・ポリシー

未登録ターゲットに使用できるセッション・ポリシーのセットは、2 つのセクションに分けられます。コア・ポリシーは、セッション中のリモート・サポート・アクションに対応します。拡張ポリシーは、セッション中のセッション管理アクションに対応します。コア・ポリシーは常時、**「未登録ターゲットに対する許可の設定」**画面に表示されています。拡張ポリシーの値を設定するには、**「その他の許可」**セクションの**「表示」**をクリックします。

コア・ポリシー

セッション・ポリシーの設定の詳細については、未登録ターゲットに対するセッション許可の設定を参照してください。

ポリシー・リストの定義

セキュリティー・ポリシー

再起動

再起動要求をターゲット・コンピューターに送信して、リモート側でリブートできるようにします。セッション開始パネルでセッション・モード・オプションとして「リブート」を使用可能にするかどうかを決定します。

「はい」に設定

セッション開始パネルにオプションとして「リブート」が表示されます。

「いいえ」に設定

セッション開始パネルにオプションとして「リブート」が表示されません。

複数のコントローラーを許可

コラボレーションを有効にして、複数のコントローラーがセッションに参加できるようにします。コントローラー・ウィンドウでコラボレーション・オプションを使用可能にするかどうかを決定します。参加者が複数存在するコラボレーション・セッションについて詳しくは、「*BigFix® Remote Control* コントローラー・ユーザーズ・ガイド」を参照してください。

「はい」に設定

コントローラー・ウィンドウで、コラボレーション・アイコンが使用できます。

「いいえ」に設定

コントローラー・ウィンドウでコラボレーション・アイコンが使用可能になりません。

「ローカル記録機能の許可」

制御しているシステムでセッションのローカル記録を作成して保存できるようにします。コントローラー・ウィンドウで記録アイコンを使用可能にするかどうかを決定します。セッションの記録について詳しくは、「*BigFix® Remote Control* コントローラー・ユーザーズ・ガイド」を参照してください。

「はい」に設定

コントローラー・ウィンドウで記録アイコンが使用可能になります。

「いいえ」に設定

コントローラー・ウィンドウで記録アイコンが使用可能になりません。

表示中のセッションの通知を使用可能にする

リモート・コントロール・セッションが進行中であることを示す半透明のオーバーレイをターゲット・コンピューターに表示するかどうかを決定します。これは、プライバシーが懸念される場合に使用する必要があります。これによってターゲット・ユーザーは、第三者がリモート側で自分のコンピューターを表示または制御しているときに明確に通知されるようになります。

「はい」に設定

ターゲット画面に半透明のオーバーレイが、**Remote Control**「」というテキストとともに表示されます。また、進行中のリモート・コントロール・セッションのタイプも表示されます。このオーバーレイはキーボードまたはマウスのアクションを妨害するものではないため、ユーザーは画面の操作を続行できます。

「いいえ」に設定

ターゲット・コンピューターにオーバーレイは表示されません。

注: このポリシーは、Windows™ オペレーティング・システムがインストールされているターゲットでのみサポートされます。

一定時間操作がなかったことによるタイムアウト

セッション・アクティビティーがない場合に、接続の終了まで待機する秒数。タイマーを無効にして、セッションが自動的に終了しないようにするには、この値を 0 に設定します。最小タイムアウト値は 60 秒です。1 から 59 までの値を設定した場合、セッションは 60 秒間アクティビティーがないとタイムアウトになります。

注: 非アクティブ・タイムアウトの値は、「アクティブ」セッション・モードにのみ適用されます。他のセッション・モードの使用時には、セッションは自動的に終了しません。

デフォルト値は 0 です。

監査ポリシー

セッション記録を強制

すべてのセッションが記録され、セッションの記録がサーバーにアップロードされて保存されます。

「はい」に設定

セッションの記録は、セッション終了時にサーバーに保存されます。セッション詳細パネルで、記録を再生するためのリンクを使用することもできます。

「いいえ」に設定

記録は保管されないため、セッション詳細パネルのリンクも使用できません。

セッション監査を強制

監査可能イベントのログが自動的にサーバーに保管されます。セッション詳細パネルにこれらのイベントを表示するかどうかを決定します。

「はい」に設定

セッション中に発生したコントローラー・イベントおよびターゲット・イベントが、セッション詳細パネルに表示されます。

「いいえ」に設定

コントローラー・イベントおよびターゲット・イベントは、セッション詳細パネルに表示されません。

コントロール・ポリシー

システム情報におけるユーザーの受け入れを使用可能にする

コントローラー・ユーザーがターゲット・システム情報の表示を選択したときに、ターゲット・コンピューターでユーザー確認ウィンドウを表示するために、このポリシーを使用します。

「はい」に設定

コントローラー・ユーザーがコントローラー・ウィンドウのシステム情報アイコンをクリックすると、ユーザー確認ウィンドウが表示されます。ターゲット・ユーザーは、ターゲット・システム情報の表示要求を受け入れるか、拒否する必要があります。ターゲット・ユーザーが「受け入れ」をクリックすると、コントローラー・システムでターゲット・システム情報が別のウィンドウに表示されます。「拒否」をクリックすると、コントローラーにメッセージが表示され、システム情報は表示されません。

「いいえ」に設定

コントローラー・ユーザーがシステム情報アイコンをクリックすると、ターゲット・システム情報が自動的に表示されます。

ファイル転送におけるユーザーの受け入れを使用可能にする

コントローラー・ユーザーがターゲットからコントローラー・システムへのファイル転送を選択したときに、ターゲット・コンピューターでユーザー確認ウィンドウを表示するために使用します。

「はい」に設定

確認ウィンドウは以下の 2 とおりの場合に表示されます。ターゲット・ユーザーは、ファイル転送を受け入れるか、拒否する必要があります。

- コントローラー・ユーザーがコントローラー・ウィンドウのファイルの転送メニューから**「ファイルをプル」**を選択した場合。

  注: ターゲット・ユーザーは、要求を受け入れた後、転送するファイルを選択する必要があります。

- コントローラー・ユーザーがターゲット・ウィンドウの**「アクション」**メニューから**「コントローラーへファイルを送信」**を選択した場合。

「いいえ」に設定

要求された場合、確認ウィンドウは表示されず、ファイルは自動的にターゲットからコントローラー・システムに転送されます。

モード変更におけるユーザーの受け入れを使用可能にする

コントローラー・ユーザーがセッション・モード・リストから別のセッション・モードを選択したときに、ターゲット・コンピューターでユーザー確認ウィンドウを表示するために使用します。

「はい」に設定

セッション・モードの変更が要求されるたびにユーザー確認ウィンドウが表示され、ターゲット・ユーザーは要求を受け入れるか、拒否する必要があります。

「いいえ」に設定

ユーザー確認ウィンドウは表示されず、セッション・モードは自動的に変更されます。

着信接続におけるユーザーの受け入れを使用可能にする

リモート・コントロール・セッションが要求されたときに、ターゲット・コンピューターでユーザー確認ウィンドウを表示するために、このポリシーを使用します。ターゲット・ユーザーは、セッションを受け入れるか、拒否する必要があります。

注: このポリシーは、**「受け入れ猶予時間」**および**「受け入れタイムアウト時のアクション」**とともに機能します。

「はい」に設定

確認ウィンドウが表示されます。ターゲット・ユーザーは、**「受け入れ猶予時間」**に定義された秒数内にセッションを受け入れるか、拒否する必要があります。

注:

1. ターゲット・ユーザーは、**確認**ウィンドウで別のセッション・モードを選択することもできます。
2. ターゲット・ユーザーが実行中のアプリケーションを非表示にするには、確認ウィンドウで「アプリケーションの非表示 (Hide applications)」オプションを選択します。アプリケーションの非表示について詳しくは、「*BigFix® Remote Control* コントローラー・ユーザーズ・ガイド」を参照してください。
3. 「はい」に設定する場合は、セッションの受け入れまたは拒否を行うための時間をターゲット・ユーザーに与えるために、「受け入れ猶予時間」を 0 より大きい値にする必要があります。

受け入れる

セッションが開始されます。

拒否

セッションは開始されず、メッセージが表示されます。

「いいえ」に設定

セッションが自動的に確立され、ターゲットに**確認**ウィンドウは表示されません。

クリップボードの転送の許可 (Allow clipboard transfer)

コントローラー・セッション・ウィンドウで**クリップボード転送**アイコンを使用可能にするかどうかを決定します。

「はい」に設定

コントローラー・ウィンドウでクリップボード転送アイコンが使用可能になります。このアイコンを使用すると、コントローラーとターゲット間でクリップボードの内容を転送できます。

「いいえ」に設定

コントローラー・ウィンドウでクリップボード転送アイコンは使用可能になりません。

セッション・ハンドオーバーの許可 (Allow session handover)

コラボレーション・セッションのマスター・コントローラーでこの機能を使用すると、セッションの制御を新しいコントローラーにハンドオーバーできます。コラボレーション制御パネルで**「ハンドオーバー」**オプションを使用可能にするかどうかを決定します。ハンドオーバー機能について詳しくは、「*BigFix® Remote Control* コントローラー・ユーザーズ・ガイド」を参照してください。

「はい」に設定

コラボレーション制御パネルに**「ハンドオーバー」**オプションが表示されます。

「いいえ」に設定

コラボレーション制御パネルに**「ハンドオーバー」**オプションは表示されません。

コラボレーション要求に対するユーザー確認を有効にする (Enable user acceptance for collaboration requests)

別のコントローラーがコラボレーション・セッションに参加しようとしたときに、ターゲット・コンピューターでユーザー確認ウィンドウを表示するために、このポリシーを使用します。コラボレーション・セッションへの参加について詳しくは、「*BigFix® Remote Control* コントローラー・ユーザーズ・ガイド」を参照してください。

「はい」に設定

マスター・コントローラーがコラボレーション・セッションの共有を受け入れた後、ターゲット・コンピューターにユーザー確認ウィンドウが表示されます。別のコントローラーがセッションに参加できるかどうかは、ターゲット・ユーザーの応答によって決まります。

受け入れる

別のコントローラーが新たにコラボレーション・セッションに参加します。

拒否

ターゲットがセッションを拒否したことを通知するメッセージが別のコントローラーに表示され、別のコントローラーはコラボレーション・セッションに参加しません。

ターゲット・ユーザーが**「受け入れ猶予時間」**に定義された時間内にユーザー確認に応答しなかった場合は、ターゲットがセッションを拒否したことを通知するメッセージが別のコントローラーに表示され、別のコントローラーはコラボレーション・セッションに参加しません。

「いいえ」に設定

マスター・コントローラーがコラボレーション・セッションの共有を受け入れた後、ターゲット・コンピューターにユーザー確認ウィンドウは表示されません。別のコントローラーはセッションに自動的に参加します。

ローカル記録でユーザー確認を有効にする (Enable user acceptance for local recording)

コントローラー・ユーザーがコントローラー・ウィンドウで記録アイコンをクリックしたときに、ユーザー確認ウィンドウを表示するために、この機能を使用します。ターゲット・ユーザーは、リモート・コントロール・セッションのローカル記録の作成要求を受け入れるか、拒否する必要があります。

「はい」に設定

コントローラー・ユーザーがコントローラー・ウィンドウの記録アイコンをクリックすると、メッセージ・ウィンドウが表示されます。ターゲット・ユーザーが**「同意する」**をクリックした場合は、コントローラー・ユーザーが記録の保存場所を選択できます。ターゲット・ユーザーが**「拒否」**をクリックした場合は、コントローラー・ユーザーに拒否のメッセージが表示されます。

ターゲット・ユーザーが要求を受け入れた後、コントローラー・ユーザーが同一セッション内でローカル記録を停止してから再開した場合、確認ウィンドウは再表示されません。

「いいえ」に設定

コントローラー・ユーザーがコントローラー・ウィンドウで記録アイコンをクリックした場合は、コントローラー・ユーザーが記録の保存場所を選択できます。メッセージ・ウィンドウは表示されません。

構成ポリシー

アクティブ

ターゲット・コンピューターがアクティブ・セッションに参加できるかどうか、およびセッション開始パネルでセッション・モードとして「アクティブ」を使用可能にするかどうかを決定します。「アクティブ」セッション・モードについて詳しくは、「*BigFix® Remote Control* コントローラー・ユーザーズ・ガイド」を参照してください。

「はい」に設定

セッション開始パネルでセッション・モードとして「アクティブ」が選択可能になります。

「いいえ」に設定

セッション開始パネルでセッション・モードとして「アクティブ」が選択可能になりません。

ガイダンス

ターゲット・コンピューターがガイダンス・セッションに参加できるかどうか、およびセッション開始パネルでセッション・モードとして「ガイダンス」を使用可能にするかどうかを決定します。「ガイダンス」セッション・モードについて詳しくは、「*BigFix® Remote Control* コントローラー・ユーザーズ・ガイド」を参照してください。

「はい」に設定

セッション開始パネルでセッション・モードとして「ガイダンス」が選択可能になります。

「いいえ」に設定

セッション開始パネルでセッション・モードとして「ガイダンス」が選択可能になりません。

モニター

ターゲット・コンピューターがモニター・セッションに参加できるかどうか、およびセッション開始パネルでセッション・モードとして「モニター」を使用可能にするかどうかを決定します。「モニター」セッション・モードについて詳しくは、「*BigFix® Remote Control* コントローラー・ユーザーズ・ガイド」を参照してください。

「はい」に設定

セッション開始パネルでセッション・モードとして**「モニター」**オプションが使用可能になります。

「いいえ」に設定

セッション開始パネルでセッション・モードとして**「モニター」**オプションが使用可能になりません。

チャット

ターゲット・コンピューターがチャット専用セッションに参加できるかどうか、およびセッション開始パネルでセッション・モードとして「チャット」を使用可能にするかどうかを決定します。「チャット」セッション・モードについて詳しくは、「*BigFix® Remote Control* コントローラー・ユーザーズ・ガイド」を参照してください。

「はい」に設定

セッション開始パネルでセッション・モードとして「チャット」が選択可能になります。

「いいえ」に設定

セッション開始パネルでセッション・モードとして「チャット」が選択可能になりません。

セッション中のファイル転送を許可

「アクティブ」セッション中のファイル転送を制御します。この値によって、**コントローラー**・ウィンドウに表示される**「ファイル転送」**メニューの**「ファイルの送信」**オプションおよび**「ファイルをプル」**オプションが使用可能になるかどうかが決まります。ファイルの転送について詳しくは、「*BigFix® Remote Control* コントローラー・ユーザーズ・ガイド」を参照してください。

「なし」に設定

「ファイルの送信」オプションおよび**「ファイルをプル」**オプションは使用可能になりません。ファイルを転送することはできません。

「両方」に設定

「ファイルの送信」オプションおよび**「ファイルをプル」**オプションが選択可能になります。ターゲットへのファイル転送、およびターゲットからのファイル転送が可能です。これがデフォルト値です。

「プル」に設定

「ファイルをプル」オプションのみが可能です。ターゲットからのファイル転送が可能です。

「送信」に設定

「ファイルの送信」オプションのみが可能です。ターゲットへのファイル転送が可能です。

拡張ポリシー

ポリシー・リストの定義

セキュリティー・ポリシー

ターゲットのロックを設定

すべてのセッションのローカル入力および表示をロックするかどうかを決定します。ターゲット・ユーザーは、リモート・コントロール・セッション中にターゲットでマウスまたはキーボードを使用できません。

「はい」に設定

セッションが開始されるとターゲット画面がブランクになるため、ターゲット・ユーザーはセッション中は画面を操作できなくなります。その場合でも、コントローラー・ウィンドウでは、ターゲット・デスクトップがコントローラー・ユーザーに表示されます。

「いいえ」に設定

セッションが開始されると、ターゲット画面はブランクにならず、ターゲット・ユーザーは画面を操作することができます。

「入力ロックの許可」

リモート・コントロール・セッション中にコントローラー・ユーザーがターゲットのローカル入力および表示をロックできるかどうかを決定します。コントローラー・ウィンドウに「プライバシーを使用可能にする」オプションを表示するかどうかを決定します。

「はい」に設定

「プライバシーの有効化」オプションは、コントローラー・ウィンドウの**「ターゲット内のアクションを実行」**メニューで選択できます。コントローラー・ウィンドウ機能について詳しくは、「*BigFix® Remote Control* コントローラー・ユーザーズ・ガイド」を参照してください。

「いいえ」に設定

「プライバシーの有効化」オプションは、コントローラー・ウィンドウの**「ターゲット内のアクションを実行」**メニューで選択できません。

画面を表示可能にして入力ロックを許可 (Allow input lock with visible screen)

このプロパティーは、**「入力ロックを許可」**とともに機能することも、また、単独で機能することもできます。リモート・コントロール・セッション中にターゲット・ユーザーのマウスおよびキーボードをロックするには、**「表示される画面で入力ロックを許可」**を使用します。

「はい」に設定

コントローラー・ウィンドウで**「ターゲット内のアクションを実行」**メニューの**「ターゲットの入力をロック」**メニュー項目が有効になります。**「ターゲットの入力をロック」**を選択すると、リモート・コントロール・セッション中にターゲット・ユーザーのマウスおよびキーボードがロックされます。ターゲット・ユーザーに対してはターゲット画面が引き続き表示されます。

「いいえ」に設定

コントローラー・ウィンドウの**「ターゲット内のアクションを実行」**メニューで「ターゲットの入力をロック」メニュー項目は有効になりません。

注: セッション中に**「プライバシーの有効化」**が選択された場合は、リモート・ユーザー入力が自動的にロックされます。入力をロックせずにプライバシーを使用可能にすることはできません。

ロックされたターゲットでの画面の表示 (Display screen on locked target)

「ターゲットのロックを設定」とともに機能します。これを使用すると、セッション開始時にプライバシー・モードを有効にすることができます。**「ロックされたターゲットでの画面の表示」**を使用すると、プライバシー・モードが有効になっているときに、ターゲット・ユーザーがリモート・コントロール・セッション中に画面を表示できるかどうかを決定できます。

「はい」に設定

プライバシー・モードの場合、セッション中にターゲット・ユーザーに対してターゲット画面が表示されますが、マウスとキーボードの制御はロックされます。

「いいえ」に設定

セッション中に、ターゲット・ユーザーに対してターゲット画面は表示されず、プライバシー・ビットマップが表示されます。ターゲット・ユーザーのマウスおよびキーボードの入力も無効になります。

注: 「ロックされたターゲットでの画面の表示」を有効にするには、**「ターゲットのロックを設定」**を「はい」に設定する必要があります。

パニック・キーの無効化

ターゲット・ユーザーが PAUSE/BREAK キーを使用してリモート・コントロール・セッションを自動的に終了できるようにするかどうかを決定します。

「はい」に設定

ターゲット・ユーザーは Pause Break キーを使用してリモート・コントロール・セッションを自動終了できません。

「いいえ」に設定

ターゲット・ユーザーは、PAUSE/BREAK キーを使用してリモート・コントロール・セッションを自動的に終了できます。

監査ポリシー

ローカル監査

リモート・コントロール・セッション中に発生した監査可能イベントのログを作成するために使用します。`trcaudit_date_time.log` ファイルが作成されます。*date_time* はセッションが発生した日時です。例えば、`trcaudit_20130805_132527.log` です。

「はい」に設定

コントローラーおよびターゲット・コンピューターで監査ログが作成され、現在ログオンしているユーザーのホーム・ディレクトリーに保管されます。

「いいえ」に設定

ログは作成されず、コントローラーまたはターゲット・コンピューターにも保管されません。

コントロール・ポリシー

高品質カラーを使用可能にする

セッションの開始時に、コントローラー・ウィンドウでターゲット・デスクトップを高品質カラーで表示するかどうかを決定します。**「カラー品質のロック」**とともに使用します。

「はい」に設定

セッション開始時にトゥルー・カラーの 24 ビット・モードでターゲット・デスクトップが表示されます。部分的な画面更新も有効になります。

「いいえ」に設定

セッション開始時に 8 ビット・カラー・モードでターゲット・デスクトップが表示されます。部分的な画面更新も有効になります。この値はデフォルト値です。

スクリーン・セーバーがアクティブな場合に画面更新を停止する (Stop screen updates when screen saver is active)

スクリーン・セーバーがアクティブであることが検出されたときに、ターゲットによる画面更新の送信を停止します。

「はい」に設定

ターゲット・システムでスクリーン・セーバーがアクティブであるときに、ターゲットによる画面更新の送信が停止されます。コントローラーには、シミュレートされたスクリーン・セーバーが表示されて、スクリーン・セーバーがリモート・ディスプレイでアクティブになっていることがコントローラー・ユーザーに示されます。コントローラー・ユーザーは、通常の方法 (キーを押す、またはマウスを移動する) でスクリーン・セーバーを閉じることができます。

「いいえ」に設定

シミュレートされたスクリーン・セーバーはセッション・ウィンドウに表示されません。ターゲット画面が通常どおり表示され、ターゲットは引き続き画面更新を送信します。

ウィンドウの非表示

「着信接続におけるユーザーの受け入れを使用可能にする」も「はい」に設定されているときに、ユーザー確認ウィンドウに**「ウィンドウの非表示」**チェック・ボックスを表示するかどうかを決定します。

「はい」に設定

ユーザー確認ウィンドウに**「ウィンドウの非表示」**チェック・ボックスが表示されます。

「いいえ」に設定

ユーザー確認ウィンドウに**「ウィンドウの非表示」**チェック・ボックスは表示されません。

デスクトップ・バックグラウンドの除去

リモート・コントロール・セッション中にターゲットのデスクトップ・バックグラウンド・イメージをビューから除去するために、このポリシーを使用します。

「はい」に設定

リモート・コントロール・セッション中に、ターゲットのデスクトップ・バックグラウンド・イメージは表示されません。

「いいえ」に設定

リモート・コントロール・セッション中、ターゲットのデスクトップ背景画像は表示されます。

カラー品質のロック

リモート・コントロール・セッション開始時のカラー品質を、セッション中に変更できるかどうかを判別します。**「高品質カラーを使用可能にする」**とともに使用します。

「はい」に設定

リモート・コントロール・セッションに対して選択された初期カラー品質はロックされ、セッション中に変更することはできません。コントローラー・ウィンドウで、**「パフォーマンス設定」**アイコンが使用不可になります。コントローラー・ユーザーは、ネットワークが低速の場合にセッションのパフォーマンスを向上させるために設定を変更することができません。

「いいえ」に設定

セッション中にカラー品質を変更することができます。コントローラー・ウィンドウで、**「パフォーマンス設定」**アイコンが使用可能になります。

受け入れタイムアウト時のアクション

ユーザー確認ウィンドウがタイムアウトになる場合に実行されるアクションです。ターゲット・ユーザーは、**「受け入れ猶予時間」**に定義された秒数内に「受け入れ」または「拒否」をクリックしませんでした。

中止

セッションは確立されません。デフォルトは「打ち切り (Abort)」です。

続行

セッションが確立されます。

受け入れ猶予時間

セッションが開始されるまで、またはタイムアウトになるまでに、ターゲット・ユーザーの応答を待機する秒数を設定します。**「着信接続におけるユーザーの受け入れを使用可能にする」**とともに使用します。

注: 「着信接続におけるユーザーの受け入れを使用可能にする」ポリシーが「はい」に設定されている場合は、応答する時間をターゲット・ユーザーに与えるために、**「受け入れ猶予時間」**を 0 より大きい値に設定する必要があります。

構成ポリシー

自動セッション・ハンドオーバーを許可

マスター・コントローラーとブローカーの接続が切れたときに、コラボレーション・セッションを自動的に別の参加者にハンドオーバーするかどうかを決定します。このポリシーは、ブローカーを使用して開始したコラボレーション・セッションにのみ適用されます。セッション回復力について詳しくは、「*BigFix® Remote Control* コントローラー・ユーザーズ・ガイド」を参照してください。

「はい」に設定

マスター・コントローラーが 3 分以内にブローカーに再接続しない場合、セッション制御は自動的に別の参加者に渡されます。ただし、ユーザーの受け入れが有効になっている場合、ターゲット・ユーザーは新しいマスター・コントローラーを受け入れるか、拒否する必要があります。

「いいえ」に設定

マスター・コントローラーが 10 分以内にブローカーに再接続しない場合、セッションは終了します。この値はデフォルト値です。

セッション中のチャットを許可

リモート・コントロール・セッション中にチャット機能を使用可能にするかどうか、およびコントローラー・ウィンドウでチャット・アイコンを使用可能にするかどうかを決定します。チャット機能について詳しくは、「*BigFix® Remote Control* コントローラー・ユーザーズ・ガイド」を参照してください。

「はい」に設定

コントローラー・ウィンドウでチャット・アイコンを選択できます。

「いいえ」に設定

コントローラー・ウィンドウでチャット・アイコンが無効になります。

ポリシー・リストの値

表 6. 有効なポリシー値とデフォルト・ポリシー値

ポリシー	有効な値	デフォルト値
再起動	yes | no	yes
複数のコントローラーを許可	yes | no	yes
「ローカル記録機能の許可」	yes | no	no
ターゲットのロックを設定	yes | no	no
「入力ロックの許可」	yes | no	no
画面上のセッション通知の有効化	yes | no	yes
画面を表示可能にして入力ロックを許可 (Allow input lock with visible screen)	yes | no	no
ロックされたターゲットでの画面の表示 (Display screen on locked target)	yes | no	no
一定時間操作がなかったことによるタイムアウト	秒数	360
セッション記録を強制	yes | no	no
ローカル監査	yes | no	yes
セッション監査を強制	はい | いいえ (サーバーでのライブ監査)	yes
パニック・キーを使用不可にする	yes | no	no
高品質カラーを使用可能にする	yes | no	no
システム情報におけるユーザーの受け入れを使用可能にする	yes | no	yes
ファイル転送におけるユーザーの受け入れを使用可能にする	yes | no	yes
モード変更におけるユーザーの受け入れを使用可能にする	yes | no	yes
着信接続におけるユーザーの受け入れを使用可能にする	yes | no	yes
クリップボードの転送の許可 (Allow clipboard transfer)	yes | no	yes
セッション・ハンドオーバーの許可 (Allow session handover)	yes | no	yes
コラボレーション要求に対するユーザー確認を有効にする (Enable user acceptance for collaboration requests)	yes | no	yes

表 6. 有効なポリシー値とデフォルト・ポリシー値 (続く)

ポリシー	有効な値	デフォルト値
スクリーン・セーバーがアクティブな場合に画面更新を停止する (Stop screen updates when screen saver is active)	yes | no	yes
ローカル記録でユーザー確認を有効にする (Enable user acceptance for local recording)	yes | no	yes
ウィンドウの非表示	yes | no	no
デスクトップ・バックグラウンドの除去	yes | no	no
カラー品質のロック	yes | no	no
受け入れタイムアウト時のアクション	中止 (abort) | 続行 (proceed)	abort
受け入れ猶予時間	秒数	180
セッション中のチャットを許可	yes | no	yes
自動セッション・ハンドオーバーを許可	yes | no	no
アクティブ	yes | no	yes
ガイダンス	yes | no	yes
モニター	yes | no	yes
チャット	yes | no	yes
セッション中のファイル転送を許可	なし | 転送 (pull) | 送信 | 両方	both

ブローカーの一時記録ディレクトリーの定義

ブローカー・プロパティーを構成することによって、セッション記録が一時的に保管されるディレクトリーをブローカー上に定義できます。

ブローカーを使用するリモート・コントロール・セッションでは、**「セッション記録を強制」** ポリシーが有効にされている場合、セッションはブローカーによって記録されます。記録が行われている間、データはブローカー上に一時的に保管され、その後、セッションの最後にサーバーにアップロードされます。ブローカー構成ファイルにプロパティーを追加することによって、記録を保管するディレクトリーを定義できます。記録ディレクトリーを定義するには、以下の手順を実行します。

1. `trc_broker.properties` ファイルを編集します。
   Windows™ オペレーティング・システムの場合、このプロパティー・ファイルはブローカーの作業ディレクトリーの `\Broker` ディレクトリーにあります。

Windows™ システムの場合、ファイルは `\ProgramData\BigFix\Remote Control\Broker\` にあります。

Linux™ オペレーティング・システムの場合、ファイルは `/etc` ディレクトリーにあります。

2. 以下のプロパティーを追加します。

RecordingDir

このプロパティーを使用して、**「セッション記録を強制」**が「はい」に設定されている場合に、セッション記録が一時的に保管されるブローカー上のディレクトリーを定義します。

例えば、`RecordingDir=c:\\tmp` です。パス内で円記号 () を使用している場合、2 つの円記号を入力する必要があります。

相対ディレクトリーを指定することもできます。例えば、`RecordingDir=tmp` です。記録は、ブローカーの作業ディレクトリーの tmp ディレクトリーに一時的に保管されます。

プロパティー・ファイルに `RecordingDir` を追加しない場合、記録はブローカーの作業ディレクトリーに一時的に保管されます。

オンデマンド・ターゲットのインストール方式

オンデマンド・ターゲットのインストール方式は、`ondemand.properties` ファイルのプロパティー、およびターゲット・ユーザーが使用するブラウザー、によって決まります。

ターゲット・ユーザーがランディング・ページで接続コードを入力し、**「同意する」**をクリックすると、オンデマンド・ターゲットのインストール・プロセスが自動的に開始されます。使用されるインストール方式は、まず `ondemand.properties` ファイルのプロパティーで決まり、その次にターゲット・ユーザーが使用しているブラウザーで決まります。

以下のプロパティーは、`ondemand.properties` ファイルで使用できます。これらのプロパティーを構成して、オンデマンド・ターゲットで使用するインストール方式を決めることができます。

ondemand.enable.plugins

このプロパティーは、プラグイン・インストール方式を使用可能または使用不可にするのに使用します。

ondemand.enable.jnlp

このプロパティーは、Java™ Web Start インストール方式を使用可能または使用不可にするのに使用します。

ondemand.enable.executable

このプロパティーは、実行可能ファイル・インストール方式を使用可能または使用不可にするのに使用します。

プロパティーについて詳しくは、オンデマンド・プロパティー・ファイルを参照してください。

デフォルトでは、すべてプロパティーが無効にされています。そのため、使用されるインストール方式はターゲット・ユーザーが使用しているブラウザーによって決まります。ターゲット・ユーザーが Internet Explorer を使用している場合は、ActiveX 方式が使用されます。Firefox ブラウザーを使用している場合は、Firefox プラグイン方式が使用されます。Internet Explorer と Firefox 以外のブラウザーを使用している場合は、Java™ アプレット方式が使用され、ブラウザーの Java™ プラグインが検出されます。例えば、Chrome ブラウザーを使用している場合は Java™ アプレット方式が使用され、ブラウザーの Java™ プラグインが検出されます。

注: 実行可能ファイルによるインストール方式は、MacOS デバイスでオンデマンド・ターゲットを使用している場合に使用できる唯一の方式です。

どの場合においても、起動ページが表示され、特定の指示が示されます。

オンデマンド・ターゲットの開始に失敗した場合は、ターゲット・ユーザーがその他のインストール方式を使用できるようにフェイルオーバー・リンクが提供されます。Java™ Web Start 方式か実行可能ファイルを使用できます。プロパティーを構成するときのインストール方式の決定について詳しくは、オンデマンド・ターゲットで使用するインストール方式の決定を参照してください。

注: ターゲット・コンピューターで JavaScript™ が有効になっていない場合は、ユーザーが**「同意する」**をクリックした後、起動ページが表示されます。ターゲット・ユーザーはコンピューターで JavaScript™ を有効にして、起動ページで**「開始」**をクリックする必要があります。

ActiveX コントロールの使用による オンデマンド・ターゲットのダウンロード

ターゲット・ユーザーが Internet Explorer を使用していて、ActiveX が有効になっている場合、オンデマンド・ターゲットは、ActiveX コントロールを使用して自動的にインストールされて開始されます。

ターゲット・ユーザーがランディング・ページで**「同意します」**をクリックすると、起動ページが表示されます。

ターゲット・ユーザーは、ページに表示される指示に従う必要があります。ユーザーはブラウザーの指示に従い、**「インストール」**をクリックしてプラグインをインストールする必要があります。ユーザー・アカウント制御のプロンプトが表示されたら、**「はい」**をクリックする必要があります。オンデマンド・ターゲット実行可能ファイルとその構成がダウンロードされてインストールされます。すべてのインストール・エラーはログ・ファイルに書き込まれます。エラーについて詳しくは、ActiveX 方式のインストールを使用するときのエラーを参照してください。セッションが開始する前に、セッションを受け入れるか拒否するかを尋ねるプロンプトがターゲット・ユーザーに出されることがあります。

ActiveX コントロールがロードされるとき、様々なアイコンが表示されることがあります。これらのアイコンは、コントロールのインストールの状況、およびオンデマンド・ターゲットのロードの状況を示します。アイコンについて詳しくは、オンデマンド・ターゲットのインストールおよびロードの状況アイコンを参照してください。

オンデマンド・ターゲットの開始に失敗した場合は、別のインストール方式を使用することができます。使用可能なインストール方式へのリンクが表示されます。リンクの数は、有効にしているプロパティーによって異なります。どのリンクが表示されるかについて詳しくは、オンデマンド・ターゲットで使用するインストール方式の決定を参照してください。

Firefox プラグインを使用した オンデマンド・ターゲットのダウンロード

ターゲット・ユーザーが Firefox を使用しているときに、Firefox プラグインおよび Java™ スクリプトが有効な場合、オンデマンド・ターゲットが自動的にインストールされ、開始されます。

注: Mozilla はレガシー・アドオンのサポートを終了したため、Firefox プラグインのインストールは、Firefox バージョン 57 以上では正常に完了しません。このインストール方法のサポートは、バージョン 9.1.4. IF0003 (ビルド番号 0309) 以降の Remote Control では推奨されません。。

ターゲット・ユーザーがランディング・ページで**「同意します」**をクリックすると、起動ページが表示されます。

ターゲット・ユーザーは、ページに表示される指示に従う必要があります。プラグインが既にインストールされており、アップグレードする必要がない場合は、オンデマンド・ターゲット実行可能ファイルがその構成とともにダウンロードされ、インストールされます。プラグインがまだインストールされていない場合、またはプラグインをアップグレードする必要がある場合は、ターゲット・ユーザーが**「許可」**をクリックしてファイルをダウンロードする必要があります。ファイルがダウンロードされたら、ターゲット・ユーザーが**「今すぐインストール」**をクリックして、ターゲットをインストールする必要があります。ユーザー・アカウント制御のプロンプトが表示されたら、**「はい」**をクリックする必要があります。

プラグインがロードされるときに、さまざまなアイコンが表示されることがあります。これらのアイコンは、プラグインのインストールの状況、およびオンデマンド・ターゲットのロードの状況を示します。アイコンについて詳しくは、オンデマンド・ターゲットのインストールおよびロードの状況アイコンを参照してください。

オンデマンド・ターゲットの開始に失敗した場合は、別のインストール方式を使用することができます。使用可能なインストール方式へのリンクが表示されます。リンクの数は、有効にしているプロパティーによって異なります。どのリンクが表示されるかについて詳しくは、オンデマンド・ターゲットで使用するインストール方式の決定を参照してください。

注: Firefox プラグインを確実に稼働させるには、Firefox Extended Support Release バージョン 24.0 以降を使用している必要があります。Firefox プラグインがインストールされているが無効になっている場合、ターゲット・ユーザーはプラグインをインストールするように求められます。プラグインは無効になっているため、開始されません。続行するには、ターゲット・ユーザーが**「オンデマンド・ターゲットの開始が失敗した場合、ヘルプ・デスクの担当者から指示されたときにここをクリックしてください」**をクリックする必要があります。

Java™ アプレットを使用したオンデマンド・ターゲットのダウンロード

オンデマンド・ターゲットは、Java アプレットを使用して、自動的にインストールおよび開始することもできます。このオプションはブラウザー依存ではないため、さまざまなブラウザーで使用できます。

ターゲット・ユーザーがランディング・ページで**「同意します」**をクリックすると、Java™ アプレットの起動ページが表示されます。

ターゲット・ユーザーは、ページに表示される指示に従う必要があります。アプリケーションを実行するためのプロンプトが表示されたら、ターゲット・ユーザーは**「実行」**をクリックして、インストール・プロセスを開始する必要があります。**ユーザー・アカウント制御**のプロンプトが表示されたら、**「はい」**をクリックする必要があります。セッションの**「着信接続におけるユーザーの受け入れを使用可能にする」**ポリシーが有効になっている場合、ターゲット・ユーザーは、セッションを受け入れるか拒否するように求められます。ターゲット・ユーザーが**「拒否」**を選択した場合、または時間内に受け入れなかった場合は、セッションが開始されません。ターゲット・ユーザーが**「同意する」**を選択すると、セッションが開始されます。インストール中に発生したエラーはすべて、ログ・ファイルに書き込まれます。エラーについて詳しくは、Java アプレット方式のインストールを使用するときのエラーを参照してください。

Java アプレットがロードされると、さまざまなアイコンが表示される可能性があります。これらのアイコンは、コントロールのインストールの状況、およびオンデマンド・ターゲットのロードの状況を示します。アイコンについて詳しくは、オンデマンド・ターゲットのインストールおよびロードの状況アイコンを参照してください。

オンデマンド・ターゲットの開始に失敗した場合は、別のインストール方式を使用することができます。使用可能なインストール方式へのリンクが表示されます。リンクの数は、有効にしているプロパティーによって異なります。どのリンクが表示されるかについて詳しくは、オンデマンド・ターゲットで使用するインストール方式の決定を参照してください。

注: Java™ アプレットは、Java™ バージョン 1.5 で作成されています。そのため、Java™ アプレットを正しく実行させるには、ターゲット・ユーザーがブラウザーにバージョン 1.5 以降の Java™ プラグインをインストールしておく必要があります。

実行可能ファイルを使用した オンデマンド・ターゲットのダウンロード

ondemand.enable.executable プロパティーが有効な場合、実行可能ファイルを使用することでオンデマンド・ターゲットを自動的にインストールして開始できます。

インストール方式の決定方法については、オンデマンド・ターゲットで使用するインストール方式の決定を参照してください。実行可能ファイル・インストール方式には、ターゲット・システムにプラグインをインストールする必要がないことに加え、ターゲット・マシン上にインストールされている Java™ に依存しないという利点があります。

ターゲット・ユーザーがランディング・ページで**「同意します」**をクリックすると、起動ページが表示されます。

ターゲット・ユーザーは、ページに表示される指示に従う必要があります。プロンプトが出されたらファイルをダウンロードして保存し、ご使用のオペレーティング・システムに該当する手順を実行します。

Windows™ システム

ダウンロードが完了したら、ファイルを実行します。**ユーザー・アカウント制御**のプロンプトが表示されたら、**「はい」**をクリックします。

Linux™ システム

ダウンロードしたファイルのアクセス権を変更します。ダウンロード・ディレクトリー内の端末ウィンドウに「chmod a+x BigFixRC*」と入力します。ファイルを実行する。

mac OS システム

Remote Control サーバーで、**ondemand.macos.package** プロパティーの値を確認します。

それを確認するには以下を実行します。

1. Remote Control サーバーの UI で、**「アドミニストレーター」 > 「プロパティー・ファイルを編集」**をクリックします。
2. ドロップダウン・メニューから「`ondemand.properties`」を選択します。
3. **ondemand.macos.package** プロパティーの値を確認します。
   - `.pkg` (新規インストールのデフォルト値) を選択した場合は、macOS ターゲットとのセッションの開始 に示す指示に従います。
   - `.zip` を選択した場合は、オンデマンド・ターゲット・アプリケーションを `.zip` ファイルから抽出し、抽出されたアプリケーション・ファイルをダブルクリックします。

     注: これは、macOS Catalina 以降では動作しません。詳しくは、『macOS でオンデマンド・ターゲットを起動するとエラーが発生する』を参照してください。

   で指定したストリングを置換する場合は、このボタンをクリックします。

注: 実行可能ファイルをダウンロードまたは解凍した後にファイル名を変更することはできません。

セッションが開始する前に、セッションを受け入れるか拒否するかを尋ねるプロンプトがターゲット・ユーザーに出されることがあります。

オンデマンド・ターゲットの開始に失敗し、フェイルオーバー・リンクが提供された場合は、**「オンデマンド・ターゲットの開始が失敗した場合、ヘルプ・デスクの担当者から指示されたときにここをクリックしてください。(Java Web Start)」**をクリックします。Java™ Web Start のインストール方式を使用してターゲットがインストールされます。

Java™ Web Start を使用したダウンロード

ターゲット・ユーザーが Internet Explorer を使用しており、ActiveX が無効になっている場合、Java™ Web Start を使用して、オンデマンド・ターゲットが自動的にインストールされ、開始されます。ActiveX、Firefox、または Java™ アプレットのインストール方式が失敗した場合も、ターゲット・ユーザーは Java™ Web Start のインストール方式を選択できます。

ターゲット・ユーザーがランディング・ページで**「同意します」**をクリックすると、Java™ Web Start の起動ページが表示されます。

ターゲット・ユーザーは、ページに表示される指示に従う必要があります。インストール・プロセスが開始されない場合は、ターゲット・ユーザーが起動ページで**「開始」**をクリックすることもできます。アプリケーションを実行するためのプロンプトが表示されたら、ターゲット・ユーザーは**「実行」**をクリックして、インストール・プロセスを開始する必要があります。**ユーザー・アカウント制御**のプロンプトが表示されたら、**「はい」**をクリックする必要があります。

注: ターゲット・コンピューターに Java™ がインストールされていない場合、ユーザーはオプションで JNLP ファイルをダウンロードして保存できます。ただし、システムではそのファイルを実行できません。

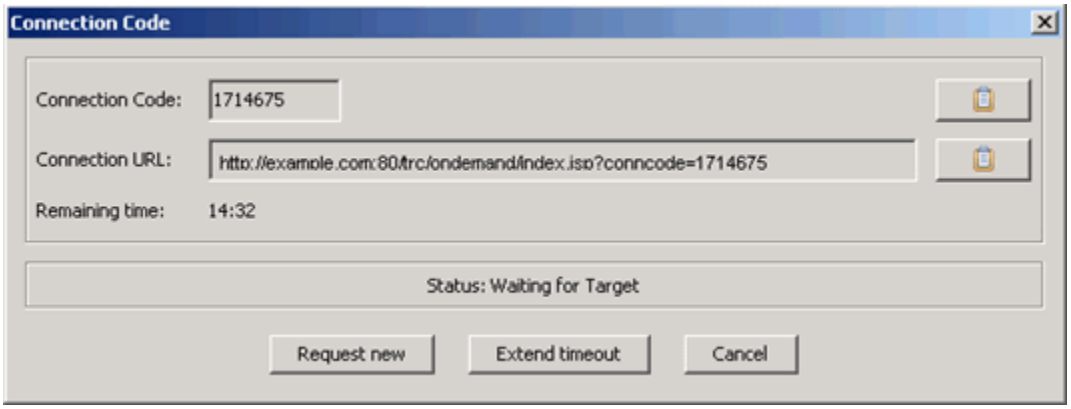
セッションの**「着信接続におけるユーザーの受け入れを使用可能にする」**ポリシーが有効になっている場合、ターゲット・ユーザーは、セッションを受け入れるか拒否するように求められます。ターゲット・ユーザーが**「拒否」**を選択した場合、または時間内に受け入れなかった場合は、セッションが開始されません。ターゲット・ユーザーが**「同意する」**を選択すると、セッションが開始されます。インストール中にエラーが発生すると、それらはすべて表示され、セッションが開始されません。さらにエラーは、ログ・ファイルに書き込まれます。

オンデマンド・ターゲットとのセッションの開始

ターゲット・ソフトウェアがまだインストールされていないターゲットとの リモート・コントロール・セッションをインターネット経由で開始することができます。

Remote Control には、 ターゲット・ユーザーがターゲット・ソフトウェアを一時的にインストールするために アクセスできる Web ページの URL の取得に使用できる機能が備わっています。ブローカー・セッションを開始すると、接続コードおよび URL が表示されます。ターゲット・ユーザーがインストール・プロセスを進めるには、 この URL をブラウザーに入力する必要があります。この処理中は、 必ず画面上の説明に従ってください。

1. 有効な ID およびパスワードで Remote Control サーバーにログオンします。
2. **「対象」 > 「ブローカー・セッションの開始」**をクリックします。
   「接続コード」ウィンドウが表示されます。



接続コード

接続コードは、サーバーがセッションを認証するために使用します。クリップボード・アイコンを使用して接続コードをクリップボードにコピーしてください。

接続 URL

この URL は、ターゲット・ソフトウェアのダウンロードおよびインストールのために ターゲット・ユーザーがアクセスできる Web ページを提供します。クリップボード・アイコンを使用して URL をクリップボードにコピーしてください。

新規を要求

新しい接続コードを要求する場合は、**「新規を要求」**をクリックします。

タイムアウトを延長

セッション接続を行うことができる時間を延長するには、**「タイムアウトを延長」**をクリックします。

キャンセル\n

「キャンセル」をクリックすると、「接続コード」ウィンドウが閉じられます。ターゲット・ソフトウェアはインストールされず、ターゲットへの接続も行われません。

3. 接続コードおよび URL を、ターゲット・コンピューターのユーザーに提供する必要があります。
   この URL をブラウザーに入力して画面上の説明に従うようにターゲット・ユーザーに依頼してください。

ターゲット・ユーザーが必要な情報を入力すると、ターゲット・ソフトウェアのインストール・プロセスが開始されます。必要な許可をコントローラー・ユーザーが持っており、セッションがサーバーによって認証されている場合は、リモート・コントロール・セッションが開始します。セッションのユーザー確認が有効になっている場合、ターゲット・ユーザーはセッションを受け入れるか拒否する必要があります。

ターゲット・ユーザーが管理者権限を持っている場合、オンデマンド・ターゲット・バイナリーが実行されるときに UAC プロンプトが表示されます。ターゲット・ユーザーに管理者権限がない場合、UAC プロンプトは表示されません。この場合、バイナリーを実行するために特別な権限は必要ありません。

注: ターゲット・ユーザーがセッションを拒否すると、オンデマンド・ターゲットに関連付けられたすべてのファイルおよびディレクトリーが削除されます。

macOS ターゲットとのセッションの開始

macOS ターゲットでオンデマンド・ターゲット・セッションを開始する方法について説明します。

Remote Control サーバーで、`ondemand.properties` ファイル内のプロパティー **ondemand.macos.package** が `.pkg` に設定されていることを確認します。それを確認するには以下を実行します。

1. Remote Control サーバーの UI で、**「アドミニストレーター」 > 「プロパティー・ファイルを編集」**をクリックします。
2. ドロップダウン・メニューから、`ondemand.properties` を選択して **ondemand.macos.package** プロパティーの値を確認します。

ondemand.macos.package を `.pkg` に設定すると、ダウンロードしたファイルのアクセス権を手動で変更することなく、macOS ターゲットでセッションを開始できます。プロパティーを設定した後、macOS ターゲットでセッションを開始するには、次の手順を実行します。

1. ブローカー・セッションを開始します。手順については、「macOS ターゲットとのセッションの開始」を参照してください。
2. セッションを開始する macOS ターゲットでブラウザーを開きます。

3. コントローラーに表示されている接続 URL を開き、そのページに表示される指示に従います。`.pkg` ファイルが自動的にダウンロードされます。
4. `.pkg` ファイルが正常にダウンロードされたら、ファイルをダブルクリックして起動します。
5. インストーラーの説明に従って、インストールを完了します。
6. **「閉じる」**をクリックして、インストーラーを閉じます。
   注: 「インストール場所の変更...」を選択する管理者権限がない場合は、エラー・メッセージ「この場所に `Remote Control` オンデマンド・ターゲットをインストールできません...」と表示される場合があります。ただし、これは macOS インストーラー・アプリケーションのバグのようですので、このメッセージを無視しても問題ありません)。

- インストールが完了すると、オンデマンド・ターゲット・アプリケーションが起動し、ブローカー・セッションに自動的に接続します。
- インストール中に **「自分のみインストール」**を選択した場合は、オンデマンド・ターゲット・アプリケーションがフォルダー `/Library/Caches/RCODT or $HOME/Library/Caches/RCODT` にインストールされます。
- インストールが成功すると、`.pkg` ファイルは自動的に削除されます。
- ブローカー・セッションが終了すると、アプリケーションは自動的に削除されます。したがって、セッションが終了した後は、アプリケーションの追跡は残されません。

注: オンデマンド・ターゲットが正しく機能するには、「アクセシビリティー」と「画面収録」の許可が必要です。これらの許可を設定する手順については、「Remote Control ターゲット・バージョン V10 IF0001 以降で必要な macOS 権限を有効にする」を参照してください。

オンデマンド・ターゲットとのセッション中の制限

オンデマンド・ターゲットとのリモート・コントロール・セッション中には、 いくつかの制限が適用される場合があります。

セッション中の制限

オンデマンド・ターゲットはアプリケーションとして実行されます。そのため、 実行中には、リモート・コントロール・セッション中に、 ターゲット・コンピューターでのユーザー権限に応じて以下の制限が適用される場合があります。

表 7. オンデマンド・ターゲットとのリモート・コントロール・セッション中の制限

	制限	Windows™ Server 2008 R2	Windows™ 7	Windows™ Server 2012	Windows™ Server 2016	Windows™ Server 2019	Windows™ 10	Linux™	macOS
1	ロック画面	すべてのユーザー	すべてのユーザー	すべてのユーザー	すべてのユーザー	すべてのユーザー	すべてのユーザー	いいえ	いいえ
2	セキュリティーで保	すべてのユーザー	すべてのユーザー	すべてのユーザー	すべてのユーザー	すべてのユーザー	すべてのユーザー	N/A	N/A

表 7. オンデマンド・ターゲットとのリモート・コントロール・セッション中の制限 (続く)

	制限	Windows™ Server 2008 R2	Windows™ 7	Windows™ Server 2012	Windows™ Server 2016	Windows™ Server 2019	Windows™ 10	Linux™	macOS
	護されたデスクトップでの UAC プロンプト								
3	高整合性レベルのコントロール Windows™	標準ユーザー	標準ユーザー	標準ユーザー	標準ユーザー	標準ユーザー	標準ユーザー	N/A	N/A
4	Modern UI	N/A	N/A	標準ユーザー	標準ユーザー	標準ユーザー	標準ユーザー	N/A	N/A
5	ユーザーの簡易切り替え	すべてのユーザー	すべてのユーザー	N/A	N/A	N/A	N/A	すべてのユーザー	すべてのユーザー
6	挿入 Ctrl+Alt+Del	標準ユーザー	標準ユーザー	標準ユーザー	標準ユーザー	標準ユーザー	標準ユーザー	いいえ	N/A
7	全画面テキスト・モード	すべてのユーザー	すべてのユーザー	N/A	N/A	N/A	N/A	すべてのユーザー	N/A
8	ログアウト中	すべてのユーザー	すべてのユーザー	すべてのユーザー	すべてのユーザー	すべてのユーザー	すべてのユーザー	すべてのユーザー	すべてのユーザー

表 7: オンデマンド・ターゲットとのリモート・コントロール・セッション中の制限 で使用している値の説明を以下の表に示します。

値	説明\n
すべてのユーザー	この制限は、標準ユーザーと管理者ユーザーの両方に影響します。
標準ユーザー	この制限は標準ユーザーのみに影響します。
N/A	この制限は当該オペレーティング・システムに適用されません。例えば、 オペレーティング・システムにユーザー・アカウント制御 (UAC) が備わっていない場合が挙げられます。

値	説明\n
いいえ	当該オペレーティング・システムの制限ではありません。

1. ロック画面

   リモート・コントロール・セッション中にターゲット・システムがロックされている場合は、 以下のメッセージがコントローラーに表示されます。 「お待ちください... エンド・ユーザーによるセキュアなデスクトップ・アクション (UAC プロンプト、ユーザーの簡易切り替え、画面のロック) が完了するまで、画面キャプチャーはターゲット・オペレーティング・システムによって一時的に中断されます。このアクションが完了すると、画面キャプチャーが再開されます。」 ターゲット上のロック画面は、 リモート・コントロール・セッションのウィンドウに表示されません。コントローラー・ユーザーは入力コントロールを使用することもできません。

2. セキュリティーで保護されたデスクトップでの UAC プロンプト

   UAC プロンプトがターゲット・システムに表示されていても、 コントローラー側ではリモート・コントロール・セッション・ウィンドウに表示されません。代わりに、以下のメッセージが表示されます。 「お待ちください... エンド・ユーザーによるセキュアなデスクトップ・アクション (UAC プロンプト、ユーザーの簡易切り替え、画面のロック) が完了するまで、画面キャプチャーはターゲット・オペレーティング・システムによって一時的に中断されます。このアクションが完了すると、画面キャプチャーが再開されます。」 このオペレーティング・システムにはユーザー・アカウント制御が備わっていないため、 この制限は Linux™ には影響しません。

   注: この制限を回避するには、UAC レベルを 「アプリがコンピューターに変更を加えようとした場合にのみ通知する (デスクトップを暗くしない)」 に設定します。この場合、UAC プロンプト・ウィンドウはセキュリティーで保護されたデスクトップに表示されず、オンデマンド・ターゲットはそれをキャプチャーできます。

3. 高整合性レベルのコントロール Windows™

   高整合性レベルにより、一部のウィンドウを開くには特権アクセスが必要です。これらのウィンドウのいずれかにフォーカスがある場合、コントローラーは、ターゲット・システムの該当するウィンドウにマウス入力やキーボード入力を送信できません。例: 特定のコントロール・パネル、regedit、または管理者のコマンド・プロンプトのウィンドウ。アクションは引き続きコントローラーから表示できるが、コントローラーからウィンドウと対話する方法がない場合、ユーザーはターゲット・マシンでアクションを実行できます。

4. Modern UI

   Modern UI (旧称メトロ) が表示されているときは、 ターゲットがユーザー・インターフェースを表示の上に表示することができません。この問題は、スタート画面および Modern UI スタイルのアプリケーションに影響します。この問題によって最も大きな影響を受けるターゲット上の UI 機能は以下のとおりです。
   - ユーザー確認プロンプト
   - 画面上のセッション通知の有効化 (OSSN)
   - ガイダンスのアクション
   - 強調表示および描画

Modern UI ではタスクバーも表示されません。そのため、 ターゲットの通知アイコンは表示されず、アクセスすることもできません。 ユーザーは、セッションがアクティブかどうかを知ることができません。Modern UI が最初に導入されたバージョンは Windows™ 8 および Windows™ 2012 オペレーティング・システムであるため、 この制限はこれらのオペレーティング・システムのみに影響します。

5. ユーザーの簡易切り替え

   別のターゲット・ユーザー・アカウントに切り替えるときに、 以下のメッセージがコントローラーに表示されます。「お待ちください... エンド・ユーザーによるセキュアなデスクトップ・アクション（UAC プロンプト、ユーザーの簡易切り替え、画面のロック）が完了するまで、画面キャプチャーはターゲット・オペレーティング・システムによって一時的に中断されます。このアクションが完了すると、画面キャプチャーが再開されます。」

6. Ctrl+Alt+Del の送信

   Windows™ Vista 以降の管理者権限を持つユーザー以外のユーザーは、 リモート・コントロール・セッション中に **Ctrl+Alt+Del** を送信することができません。この制限の回避策について詳しくは、Ctrl + Alt + Del の回避策を参照してください。

7. 全画面テキスト・モード

   ユーザーがテキスト・モード・アプリケーションを全画面に切り替えるときに、 以下のメッセージがコントローラーに表示されます。「お待ちください... エンド・ユーザーによるセキュアなデスクトップ・アクション（UAC プロンプト、ユーザーの簡易切り替え、画面のロック）が完了するまで、画面キャプチャーはターゲット・オペレーティング・システムによって一時的に中断されます。このアクションが完了すると、画面キャプチャーが再開されます。」 全画面テキストはセッションのウィンドウに表示されません。

8. ログアウト中

   ユーザーがログアウトすると、 そのユーザーのセッションで実行されているすべてのアプリケーションが強制終了されます。オンデマンド・ターゲットはアプリケーションとして実行されるため、 同様に強制終了されます。

リモート・コントロール・セッション中にファイルを転送する場合は、 以下の制限に注意する必要があります。

注: 書き込みのために管理者権限が必要なターゲットのディレクトリー (Program Files ディレクトリーなど) にファイルを転送することはできません。ユーザーのプロファイル・ディレクトリーまたは temp ディレクトリーにファイルを転送した後、ローカル環境のツール (Windows™ エクスプローラーや cmd.exe などのツール) を使用して、そのファイルを所定の場所に移動することはできます。ただし、 この処理中に UAC プロンプトが出される場合がありますが、 セキュリティーで保護されたデスクトップでの UAC プロンプトの制限のため、 そのプロンプトは表示されず、操作することもできません。ターゲットからコントローラーに転送する場合にも 同じ制限が適用されます。

Ctrl + Alt + Del の回避策

「Ctrl-Alt-Del」をクリックすると、 セキュリティーで保護されたデスクトップに 「Windows™ のセキュリティー」ダイアログが表示されます。オンデマンド・ターゲットは セキュリティーで保護されたデスクトップをキャプチャーできないため、このダイアログが表示されると、 オンデマンド・リモート・コントロール・セッションは一時停止します。例外は、 「ようこそ」画面が使用可能な Windows™ XP で代わりにタスク・マネージャーが開始されている場合です。

「Windows™ のセキュリティー」ダイアログには 5 つのオプションがあります。ただし、 コントローラー・ユーザーは他の方法でオプションを選択することができます。

「ワークステーションのロック」

コントローラー・ウィンドウで **「アクション」 > 「ワークステーションをロック」**を選択します。

「ログオフ」および「シャットダウン」

これらのオプションは、Windows™ オペレーティング・システムの**「スタート」**メニューから選択することができます。

パスワードを変更します

コントロール・パネルのパスワード変更オプションにアクセスできます。

「タスク マネージャ」

コントローラー・ウィンドウで **「アクション」 > 「タスク・マネージャー (Task Manager)」**を選択します。Windows™ タスクバーを右クリックすることもできます。

オンデマンド・ターゲットでのセッション記録の保存

オンデマンド・ターゲットのユーザーは、リモート・コントロール・セッションの記録をユーザーのコンピューターに保存できます。セッションを受け入れたときに記録を保存するか、またはセッション中に記録を開始して保存するかを選択できます。

記録は、`OnDemandRecordings` ディレクトリー内にあるターゲット・ユーザーのホーム・ディレクトリーに保存されます。ファイル名の形式は次のとおりです。

`trcrecording_`*`YYYYMMDD_HHMMSS`*`.trc`。ここで、 *YYYYMMDD_HHMMSS* は、ファイルが保存された時刻のタイム・スタンプです。

記録ファイルは、セッション終了時に削除されません。

記録の保存方法を以下から選択してください。

- セッション受け入れウィンドウで、**「ローカル記録を保持」**を選択します。
  セッションに対して**「着信接続におけるユーザーの受け入れを使用可能にする」**ポリシーが設定されている場合は、**「ローカル記録を保持」**オプションが使用可能になります。セッション開始時に記録が開始されます。**「アクション」 > 「ローカル記録の停止」**を選択すると、そのセッション中の任意の時点で記録を停止できます。
- **「アクション」 > 「ローカル記録の開始」**を選択して、セッション中に記録を開始します。

その時点以降のセッション・アクティビティーが記録され、ターゲット・コンピューターに保存されます。

「アクション」 > 「ローカル記録の停止」を選択して、記録を停止します。

セッション中に**「ローカル記録の開始」**をクリックするたびに、新しい記録ファイルがコンピューターに保存されます。

セッション記録を保存したら、ヘルプ・デスクの担当者から URL を取得して、記録を再生できます。URL の形式は以下のとおりです。

Remote Control サーバーに直接アクセスできる場合、URL は `http(s)://server_name:port/trc/ondemand/player.jsp` (*server_name:port* はサーバーの IP アドレスおよびポート) です。

インターネットからページにアクセスする場合、URL は `http(s)://broker_name:port/player.jsp` (*broker_name:port* はリバース・プロキシーの IP アドレスおよびポート) です。

記録を再生するには、以下の手順を実行してください。

1. URL をブラウザーに入力します。セッション記録プレイヤーが自動的に開始されます。
2. プレイヤーが開始されない場合は、**「実行」**をクリックします。
3. 記録ファイルを参照して、**「OK」**をクリックします。記録ファイルは、ホーム・ディレクトリー内の `OnDemandRecordings` ディレクトリーに保存されています。

ブローカー・コラボレーション・セッションのハンドオーバー

ブローカーを使用するコラボレーション・セッションのマスター・コントローラーは、セッションの完全な制御を別の承認者に渡すことができます。

コラボレーション・セッション中に**「ハンドオーバー」**機能を使用して、セッションの完全な制御をセッション内の他のいずれかの承認者に渡します。その承認者がマスター・コントローラーになり、セッションを終了せずにそのままに維持することができます。この機能が使用できるかどうかは、サーバー・ポリシーの**「セッション・ハンドオーバーを許可」**の値によって決まります。

「はい」に設定

コラボレーション制御パネルに**「ハンドオーバー」**ボタンが表示されます。

「いいえ」に設定

コラボレーション制御パネルに**「ハンドオーバー」**ボタンは表示されません。

コラボレーション・セッションのコントロールを新しいマスター・コントローラーに渡すには、以下の手順を実行します。

1. コラボレーション制御パネルの承認者リストで目的のコントローラーを選択します。
2. **「ハンドオーバー」**をクリックします。
   ハンドオーバー要求の結果は、**「コラボレーション要求に対するユーザー確認を有効にする」**サーバー・ポリシーに設定された値によって決まります。

セッションでこのポリシーが「はい」に設定されている場合、ターゲット・ユーザーは、制御のハンドオーバー要求を受け入れるかまたは拒否するかを尋ねられます。ターゲット・ユーザーが要求を受け入れると、選択されたコントローラーにセッションの完全な制御が渡されます。ターゲット・ユーザーが拒否した場合、または時間内に応答しなかった場合は、拒否のメッセージが、要求者の画面と選択されたコントローラーの画面に表示されます。要求者がセッションのマスター・コントローラーのままとなります。**「OK」**をクリックします。

注: ターゲット・ユーザーが時間内に応答せず、**「受け入れタイムアウト時のアクション」**サーバー・ポリシーが PROCEED に設定されている場合、制御は新しいマスター・コントローラーに渡されます。

「コラボレーション要求に対するユーザー確認を有効にする」が「いいえ」に設定されている場合、ターゲット・ユーザーによるユーザー確認は必要なく、セッションの完全な制御が新しいマスター・コントローラーに渡されます。

セッションが新しいマスター・コントローラーにハンドオーバーされた場合、コラボレーション制御パネルが新しいマスター・コントローラーのシステム上に開きます。コラボレーション制御パネルに承認者のリストが表示されます。元のマスター・コントローラーはセッションの入力を制御できなくなります。新しいマスター・コントローラーの IP アドレスが、元のマスター・コントローラーのセッション・ウィンドウのウィンドウ・タイトルに表示されます。

新しいマスター・コントローラーのセッション・ウィンドウのウィンドウ・タイトルに、ターゲットの IP アドレスが表示されます。

注: セッションのポリシーは、セッションが開始されたときのままになります。コントローラー・ユーザーが変更されても、ポリシーは変更されません。セッションに設定された初期ポリシーは、どのユーザーがマスター・コントローラーになるかに関係なく、コラボレーション・セッション全体を通して有効になります。

セッションの終了

Remote Control オンデマンド・ターゲットとのセッションを終了すると、関連したすべてのファイルおよびディレクトリーが削除されます。

オンデマンド・ターゲットとのリモート・コントロール・セッションを以下の方法で終了できます。

- タスクバーの**「接続」**アイコン  をクリックする。
- コントローラー・ウィンドウの右上にある**「X」**をクリックする。

「はい」をクリックするとセッションが終了します。

セッションが終了し、オンデマンド・ターゲットに関連付けられたファイルおよびディレクトリーが削除されます。オンデマンド・ターゲットのバイナリー・ファイル、構成ファイル、およびインストール・ディレクトリーが、そ

のすべての内容とともに削除されます。オンデマンド・ターゲットのトレース・ファイルも、ターゲットに保存するように選択しない限り、削除されます。ログ・ファイルの保存について詳しくは、セッション・ログ・ファイルの保存を参照してください。

ターゲット・ユーザーは、キーボードの **Pause** を押すか、接続アイコンをクリックして、セッションを終了することができます。ターゲット・ユーザーがセッションをクローズすると、セッションは即時に終了します。

注: ネットワーク障害などのユーザー以外のイベントによってセッションが中断された場合、トレース・ファイルは削除されません。トレース・ファイルをデバッグ目的で使用してください。

切断時のコラボレーション・セッションの終了

コラボレーションが開始されたセッションを終了するときに、セッションを維持するか、セッションを切断するかを選択できます。

リモート・コントロール・セッションを以下の方法で終了できます。

- タスクバーの**「接続」**アイコンをクリックする。 
- コントローラー・ウィンドウの右上にある**「X」**をクリックする。

セッション内でコラボレーションが開始されていると、セッションのマスター・コントローラーに、コラボレーションが進行中であるという警告が出されます。以下のメッセージが表示されます。 コラボレーション・セッションが進行中です。切断すると、セッションが終了します。セッションを開いたままにしますか?

切断してセッションを終了するか、マスター・コントローラーとしてセッションを維持するかのいずれかを選択することができます。

キャンセル\n

「キャンセル」をクリックすると、コラボレーション・セッションが続行し、マスター・コントローラーの状態が維持されます。

セッションの切断

「セッションの切断」をクリックすると、コラボレーション・セッションが終了し、すべての参加者が切断されます。

セッション・ログ・ファイルの保存

Remote Control オンデマンド・ターゲットとのセッション中に作成されたトレース・ログ・ファイルを保存できます。

オンデマンド・ターゲットのインストール時に作成されたログ・ファイルは、デバッグ目的で使用できます。ログ・ファイルは、オンデマンド・ターゲットとのリモート・コントロール・セッションの終了時に削除されます。ターゲットにファイルを保存するには、**「セッション・ログを保持」**機能を使用します。

コントローラー・ウィンドウで、**「ターゲット内のアクションを実行」 > 「セッション・ログを保持」**をクリックして、ログ・ファイルを保存します。

ログ・ファイルは、ターゲット・コンピューターにあるユーザーのホーム・ディレクトリーに保存されます。ファイルは次の形式で保存されます。

`trc_odt_trace_yyyymmdd_hhmmss.log`

例えば、 `trc_odt_trace_20130530_095900.log`

セッションが終了する前に、セッション・ログを保存するように選択した場合は、**「ターゲット内のアクションを実行」 > 「セッション・ログを削除」**を選択して、ログを削除できます。

注: セッション中にターゲット・ユーザーが切り替えられた場合、ログ・ファイルは、セッションを開始したターゲット・ユーザーのホーム・ディレクトリーに保存されます。

の未登録ターゲットのセッション履歴

オンデマンド・ターゲットとのリモート・コントロール・セッションに参加したら、セッション履歴を表示できます。未登録ターゲットが使用されたセッションは、**「すべてのセッション履歴」**レポートおよび**「ユーザーのセッション履歴」**レポートに、登録済みターゲットのセッションとともにリストされます。未登録ターゲットのみが使用されたセッションのリストを表示することもできます。

未登録ターゲットのセッション履歴の表示

以前のセッションのリストを表示するには、 **「すべてのセッション履歴」**または **「ユーザーのセッション履歴」**のレポートを表示します。これらのレポートには、 登録済みおよび未登録のターゲットのセッションが表示されます。レポートの**「登録済みターゲット」**列は、 セッションのターゲットが Remote Control サーバーに登録されていたかどうかを示します。未登録ターゲットに限ったセッションのリストを表示するには、 **「すべての未登録ターゲットのセッション」**レポートを使用します。

「すべての未登録ターゲットのセッション」レポートを表示するには、以下の手順を実行します。

1. 有効な管理者 ID およびパスワードで Remote Control サーバーにログオンします。
2. **「セッション」 > 「すべての未登録ターゲットのセッション」**を選択します。
   「未登録ターゲットのセッション履歴」パネルが表示されます。

   注: カスタム・データの列見出しは、 フィールドに対して `ondemand.properties` ファイルで定義されている現在のラベル名を反映しています。列のデータは、すべて同じ形式であるとは限りません。

例えば、**ondemand.custom.field.0.label= Name** であったものを **ondemand.custom.field.0.label= Email** に変更した場合は、「Email」という見出しが付いた列に名前と E メール・アドレスが表示される場合があります。`ondemand.properties` ファイルについて詳しくは、オンデマンド・プロパティー・ファイルを参照してください。

セッションの詳細の表示

「セッション詳細」機能を使用すると、 未登録ターゲットとのリモート・コントロール・セッションに関する詳細が表示されます。**「未登録ターゲットのセッション履歴」**レポートからセッションを選択することができます。セッションの詳細が表示されます。

特定のセッションのセッション詳細を表示するには、 以下の手順を実行します。

1. **「セッション」 > 「すべての未登録ターゲットのセッション」**をクリックします。
2. リストからセッションを選択します。
3. 左側のアクション・リストから**「セッション詳細」**を選択します。

「Remote Control セッション情報」パネルが表示されます。オンデマンド・ターゲット・セッションの間は、 オンデマンド・ポータル・ページでデータが入力されたカスタム・データ・フィールドが **「セッション詳細」**セクションに表示されます。コントローラー・ユーザーの ユーザー ID も表示されます。セッションのポリシーが表示されるほか、 コントローラー監査イベントまたはターゲット監査イベントがあれば、 設定されたポリシーに応じて表示されます。セッションの **「セッション監査を強制」**ポリシーが「はい」に設定されている場合は、 保存されている監査項目が表示されます。**「セッション記録を強制」**ポリシーが「はい」に設定されている場合は、 セッションの記録を再生するためのリンクも表示されます。**「このセッションの記録を再生します」**をクリックすると、 **「セッションのレコード・プレイヤー」**ウィンドウが開き、記録が再生されます。

データベース表の定義

オンデマンド・ターゲットとのリモート・コントロール・セッションのデータを保持するデータベース表についての説明および定義を示します。SESSIONS_DATA 表は、ターゲット・ユーザーによって使用されるデフォルトの Web ページから送信されるデータを保持します。SESSIONS 表は、セッション・データを保持します。

表 8. SESSION_DATA 表

表名	列名	型名	LENGTH	NULL
SESSION_DATA	SESSIONKEY	INTEGER	4	いいえ
	CUSTOM0	VARCHAR	128	はい
	CUSTOM1	VARCHAR	128	はい
	CUSTOM2	VARCHAR	128	はい
	CUSTOM3	VARCHAR	128	はい
	CUSTOM4	VARCHAR	128	はい

表 8. SESSION_DATA 表 (続く)

表名	列名	型名	LENGTH	NULL
	CUSTOM5	VARCHAR	128	はい
	CUSTOM6	VARCHAR	128	はい
	CUSTOM7	VARCHAR	128	はい
	CUSTOM8	VARCHAR	128	はい
	CUSTOM9	VARCHAR	128	はい

表 9. SESSIONS 表

表名	列名	型名	LENGTH	NULL
SESSIONS	SESSIONKEY	INTEGER	4	いいえ
	USERKEY	INTEGER	4	いいえ
	HWKEY	INTEGER	4	いいえ
	REGISTERED_TARGET	CHAR	1	いいえ
	REQUEST_TIME	TIMESTAMP	10	はい
	START_TIME	TIMESTAMP	10	はい
	END_TIME	TIMESTAMP	10	はい
	DESCRIPTION	VARCHAR	512	はい
	KNOWNUSERNAME	VARCHAR	128	はい
	KNOWNCOMPUTERNAME	VARCHAR	255	はい
	SESSION_TOKEN	VARCHAR	256	はい

オンデマンド・プロパティー・ファイル

オンデマンド・ターゲットとのリモート・コントロール・セッションのプロパティーを作成および構成するには、`ondemand.properties` ファイルを編集します。

オンデマンド・ターゲットとのリモート・コントロール・セッション中に使用されるプロパティーを構成するには、`ondemand.properties` ファイルを使用します。

- このファイルをサーバー UI から編集するには、**「アドミニストレーター」 > 「プロパティー・ファイルを編集」**をクリックします。
- このファイルは、手動で編集することもできます。このファイルは以下のディレクトリーにあります。

  Windows™ オペレーティング・システム:

[installdir]\wlp\usr\servers\trcserver\apps\TRCAPP.ear\trc.war\WEB-INF\classes *[installdir]* は、Remote Control サーバーのインストール・ディレクトリーです。例えば、`C:\Program Files (x86)\BigFix\TRC\server\wlp\usr\servers\trcserver\apps\TRCAPP.ear\trc.war\WEB-INF\classes`

Linux™ オペレーティング・システム:

[installdir]/wlp/usr/servers/trcserver/apps/TRCAPP.ear/trc.war/WEB-INF/classes *[installdir]* は、Remote Control サーバーのインストール・ディレクトリーです。例えば、`/opt/Bigfix/server/wlp/usr/servers/trcserver/apps/TRCAPP.ear/trc.war/WEB-INF/classes`

- ファイルを編集したら、**「アドミニストレーター」 > 「アプリケーションをリセット」**をクリックする必要があります。

ランディング・ページ URL をカスタマイズするプロパティー

ondemand.url プロパティーは、デフォルトで `https://localhost/trc/ondemand/index.jsp?conncode=%c` に設定されます。`localhost` をリモート・コントロール・サーバーのアドレスに置き換えます。リバース・プロキシーを使用するには、`localhost/trc/ondemand` を、リバース・プロキシーとして構成されているブローカーの完全修飾パブリック・ドメイン名に置き換えます。例えば、`https://broker.example.com/index.jsp?conncode=%c` です。リバース・プロキシーの構成について詳しくは、インターネット・ユーザーのオンデマンド・ターゲット・ポータルへのアクセスを参照してください。localhost を置き換えない場合、`trc_broker.properties` ファイルの **ServerURL** プロパティーに定義されている値が、コントローラーに表示される URL の作成に使用されます。%c 変数は、URL がコントローラー・ウィンドウに表示されるときにセッション接続コードに置き換えられます。デフォルト・ページでは、セッション接続コードの入力が必要です。

このプロパティーを、カスタマイズした独自の Web ページの URL に設定することもできます。

表 10. コントローラー・ユーザーに対する URL の表示方法。

ondemand.url=	ServerURL=	URL の表示方法
`http://localhost/trc/ondemand/index.jsp`	`https://rcserver.com/trc`	`https://rcserver.com/trc/ondemand/index.jsp`
`https://mypage.com/trc/ondemand/index.jsp?conncode=%c`	`https://mycompany.com/trc`	`https://mypage.com/trc/ondemand/index.jsp?conncode=1234567` 接続コードが 1234567 の場合
`https://broker.example.com/index.jsp?conncode=%c`	`https://rcserver.com/trc`	`https://broker.example.com/index.jsp?conncode=1234567` 接続コードが 1234567 の場合

注: この例では、次の 3 つのホスト名があります。

- ***rcserver.com*** は、サーバーがブローカーから直接アクセスできる場合に使用される Remote Control サーバーのホスト名です。
- ***mycompany.com*** は、HTTP プロキシー経由で Remote Control サーバーにアクセスするために使用されるプロキシー・ホスト名です。
- ***broker.example.com*** は、Remote Control ブローカーのパブリック DNS です。
- ***mypage.com*** は、HTTP プロキシー経由で Remote Control ブローカーにアクセスするために仮想ホスト名として使用されるパブリック DNS です。

上記の 4 つのすべての組み合わせが表に示されているわけではありません。

```
ondemand.url=
```

変更可能フィールド	**ondemand.url**
フィールドの説明	ターゲット・ソフトウェアをダウンロードして一時的にインストールするためのプロセスを開始する目的でターゲット・ユーザーがアクセスできるページの URL。
有効な値	ユーザー定義の URL。例えば、`https://broker.example.com/index.jsp?conncode=%c`
値の定義	デフォルト値は `https://localhost/trc/ondemand/index.jsp?conncode=%c` です。

オンデマンド・ターゲットのダウンロード方法および開始方法を決定するプロパティー

```
ondemand.enable.plugins=
```

変更可能フィールド	**ondemand.enable.plugins**
フィールドの説明	オンデマンド・ターゲットのダウンロードおよび開始に、プラグイン (Firefox プラグイン、Internet Explorer Active X、または Java™ アプレット) 方式を使用するかどうかを決定します。オンデマンド・ターゲットを開始するために使用される方式について詳しくは、オンデマンド・ターゲットのインストール方式を参照してください。
有効な値	*true* または *false*
値の定義	***true*** 使用しているブラウザーに応じて、オンデマンド・ターゲットのダウンロードおよび開始にプラグイン (Firefox プラグイン、Internet Explorer Active X、または Java™ アプレット) 方式が使用されます。 ***false***

	オンデマンド・ターゲットのダウンロードおよび開始にプラグイン (Firefox プラグイン、Internet Explorer Active X、または Java™ アプレット) 方式は使用されません。

```
ondemand.enable.executable=
```

変更可能フィールド	**ondemand.enable.executable**
フィールドの説明	オンデマンド・ターゲットのダウンロードおよび開始に、スタンドアロン実行可能ファイルを使用するかどうかを決定します。さらに、オンデマンド・ターゲットの開始に失敗した場合に、実行可能ファイル方式を使用するためのフェイルオーバー・リンクを提供するかどうも決定します。このフェイルオーバー・リンクは、プラグイン (Firefox プラグイン、Internet Explorer Active X、または Java™ アプレット) 方式を使用している場合に提供されます。オンデマンド・ターゲットを開始するために使用される方式について詳しくは、オンデマンド・ターゲットのインストール方式を参照してください。
有効な値	*true* または *false*
値の定義	***true*** **ondemand.enable.plugins** プロパティーが *false* に設定されている場合、オンデマンド・ターゲットのダウンロードおよび開始に実行可能ファイルが使用されます。 **ondemand.enable.plugins** プロパティーが *true* に設定されており、かつプラグインが検出されないか Java™ プラグインがインストールされていない、または使用可能になっていない場合、実行可能ファイル方式が使用されます。 プラグイン方式または Java アプレット方式を使用した場合にオンデマンド・ターゲットの開始が失敗した場合、実行可能ファイル方式を使用するためのフェイルオーバー・リンクが提供されます。 ***false*** オンデマンド・ターゲットのダウンロードおよび開始に実行可能ファイルは使用されません。プラグイン方式または Java アプレット方式を使用した場合にオンデマンド・ターゲットの開始が失敗した場合、実行可能ファイル方式を使用するためのフェイルオーバー・リンクは提供されません。

```
ondemand.enable.jnlp=
```

変更可能フィールド	**ondemand.enable.jnlp**

フィールドの説明	オンデマンド・ターゲットをダウンロードおよび開始するためのオプションとして Java Web Start 方式を提供するかどうかを決定します。さらに、プラグイン方式、Java アプレット方式、または実行可能ファイル方式を使用してオンデマンド・ターゲットの開始に失敗した場合に、Java Web Start 方式を使用するためのフェイルオーバー・リンクを提供するかどうかも決定します。オンデマンド・ターゲットを開始するために使用される方式について詳しくは、オンデマンド・ターゲットのインストール方式を参照してください。
有効な値	*true* または *false*
値の定義	***true*** **ondemand.enable.plugins** および **ondemand.enable.executable** が *false* に設定されている場合、オンデマンド・ターゲットのダウンロードおよび開始に Java Web Start 方式が使用されます。 **ondemand.enable.plugins** または **ondemand.enable.executable** が *true* に設定されている場合、プラグイン方式、Java アプレット方式、または実行可能ファイル方式を使用してオンデマンド・ターゲットの開始に失敗した場合に、Java Web Start 方式を使用するためのフェイルオーバー・リンクが提供されます。 ***false*** オンデマンド・ターゲットの開始に失敗した場合に、Java Web Start 方式を使用するためのフェイルオーバー・リンクは提供されません。

構成されている URL からアクセスされる Web ページにカスタム・フィールドを追加するためのプロパティー

ondemand.url プロパティーに定義されている URL からアクセスされる Web ページにカスタム・フィールドを追加するには、以下のプロパティーを使用します。デフォルトでは 4 個のカスタム・フィールドを使用できます。カスタム・フィールドをさらに追加するには、`ondemand.properties` ファイルを手動で編集します。

注: ファイルを手動で編集したら、画面に新しいツールを表示させるため、サーバー・サービスを再始動してください。

```
ondemand.custom.field.x.label=
```

変更可能フィールド	**ondemand.custom.field.x.label**
フィールドの説明	オンデマンド・ターゲットとのセッションを開始するために使用されるデフォルトの Web ページで追加の入力フィールドに使用する表示名。x は 1 から 9 です。 このプロパティーの値を設定していない場合、フィールドは表示されません。例えば、次の構成例では、カスタムの **Name** フィールドが定義されます

	が、**ondemand.custom.field.1.label** が定義されていないため、インデックス 1 の定義は破棄されます。 ondemand.custom.field.0.label=Name ondemand.custom.field.1.required=true ondemand.custom.field.1.label.fr=Numéro de téléphone
有効な値	ユーザー定義。例えば、以下のようにします。 `ondemand.custom.field.1.label=Name` Web ページ・メニューに Name というテキストが表示されます。
値の定義	

```
ondemand.custom.field.x.required=
```

変更可能フィールド	**ondemand.custom.field.x.required=**
フィールドの説明	カスタム・フィールドが必須フィールドであるかどうかを決定します。
有効な値	True、False。
値の定義	**True** ターゲット・ユーザーは、フィールドにデータを入力する必要があります。 **False** ターゲット・ユーザーは、任意でフィールドにデータを入力できます。

```
ondemand.custom.field.x.label.locale=
```

変更可能フィールド	**ondemand.custom.field.x.label.locale**
フィールドの説明	カスタム・フィールドのラベル名の翻訳。x は 1 から 9 です。
有効な値	ユーザー定義。例えば、以下のようにします。 `ondemand.custom.field.1.label.fr=Numéro de téléphone`
値の定義	ブラウザーのロケールの翻訳が指定されていない場合は、**ondemand.custom.field.x.label** プロパティーの値が表示されます。

Lite Web Portal を構成するプロパティー

```
liteweb.portal.enable=
```

変更可能フィールド	**liteweb.portal.enable**

フィールドの説明	これにより、「Lite Web Portal」機能が有効になります。「Lite Web Portal」に関連する OnDemand チャネルを介したすべてのアクセスを受け入れるか拒否するかを決定します。
有効な値	True、False。
値の定義	**True** 「Lite Web Portal」に関連する OnDemand チャネルを介したすべてのアクセスが受け付けられます。 **False** 「Lite Web Portal」に関連する OnDemand チャネルを介したすべてのアクセスが拒否され、無視されます。デフォルトは False です。

```
liteweb.portal.autodetect.url=
```

変更可能フィールド	**liteweb.portal.autodetect.url**
フィールドの説明	「Lite Web Portal」は、要求を発信したブローカーを動的に解決することによって応答を作成します。
有効な値	True、False。
値の定義	**True** ポータルを企業ネットワーク内と外部の両方から使用する場合は、True に設定します。デフォルトは True です。 **False** false に設定すると、応答の作成に liteweb.portal.url が使用されます。

```
liteweb.portal.url=
```

変更可能フィールド	**liteweb.portal.url**
フィールドの説明	https://hostname:port の形式のリバース・プロキシー・ブローカーの URL。
有効な値	https://hostname:port の形式のユーザー定義 URL。
値の定義	**liteweb.portal.autodetect.url** が False に設定されている場合にのみ使用されます。

オンデマンド・ターゲットで使用するインストール方式の決定

オンデマンド・インストール方式のプロパティー構成によって、どのインストール方式をオンデマンド・ターゲットで使用するかが決まります。

ondemand.enable.plugins プロパティー、**ondemand.enable.executable** プロパティー、および **ondemand.enable.jnlp** プロパティーを構成するときは、以下の情報を使用してオンデマンド・ターゲットで使用するインストール方式の決定に役立ててください。

注: 実行可能ファイルによるインストール方式は、MacOS デバイスでオンデマンド・ターゲットを使用している場合に使用できる唯一の方式です。

注: Mozilla はレガシー・アドオンのサポートを終了したため、Firefox プラグインのインストールは、Firefox バージョン 57 以上では正常に完了しません。このインストール方法のサポートは、バージョン 9.1.4. IF0003 (ビルド番号 0309) 以降の Remote Control では推奨されません。。

表 11. プロパティー値によるオンデマンド・ターゲットのインストール方式の決定

ondemand. enable. plugins	ondemand. enable. executable	ondemand. enable. jnlp	使用されるインストール方式	提供されるフェイルオーバー・リンク
はい	はい	はい	ターゲット・ユーザーが使用するブラウザーに応じて、プラグイン方式 (Firefox プラグイン、Internet Explorer ActiveX、または Java™ アプレット) が使用されます。ただし、プラグインが検出されないか、Java™ プラグインがインストールされていないか、有効にされていない場合は、実行可能ファイル方式が使用されます。	起動ページは、オンデマンド・ターゲットの開始に失敗した場合に使用できるフェイルオーバー・リンクを 2つ提供します。Java™ Web Start 方式を使用するフェイルオーバー・リンクと、実行可能ファイル方式を使用するフェイルオーバー・リンクです。
はい	はい	いいえ	ターゲット・ユーザーが使用するブラウザーに応じて、プラグイン方式 (Firefox プラグイン、Internet Explorer ActiveX、または Java™ アプレット) が使用されます。ただし、プラグインが検出されないか、Java™ プラグインがインストールされていないか、有効にされていない場合は、実行可能ファイル方式が使用されます。	起動ページは、オンデマンド・ターゲットの開始に失敗した場合に使用できるフェイルオーバー・リンクを 1 つ提供します。このフェイルオーバー・リンクは、実行可能ファイル方式のみを使用します。
はい	いいえ	はい	ターゲット・ユーザーが使用するブラウザーに応じて、	起動ページは、オンデマンド・ターゲットの開始に失敗した場

表 11. プロパティー値によるオンデマンド・ターゲットのインストール方式の決定 (続く)

ondemand. enable. plugins	ondemand. enable. executable	ondemand. enable. jnlp	使用されるインストール方式	提供されるフェイルオーバー・リンク
			プラグイン方式 (Firefox プラグイン、Internet Explorer ActiveX、または Java™ アプレット) が使用されます。	合に使用できるフェイルオーバー・リンクを 1 つ提供します。このフェイルオーバー・リンクは、Java™ Web Start 方式のみを使用します。
はい	いいえ	いいえ	ターゲット・ユーザーが使用するブラウザーに応じて、プラグイン方式 (Firefox プラグイン、Internet Explorer ActiveX、または Java™ アプレット) が使用されます。	起動ページにフェイルオーバー・リンクの提供はありません。
いいえ	いいえ	いいえ	使用可能なインストール方式がありません。ページにメッセージ「オンデマンド・ターゲットを実行できません: サーバー上にインストール方式が構成されていません (Unable to run the on-demand target: No installation methods are configured on the server)」が表示されます。	適用外
いいえ	いいえ	はい	Java™ Web Start 方式が使用されます。	適用外
いいえ	はい	いいえ	オンデマンド・ターゲットの実行可能ファイルが使用されます。	起動ページにフェイルオーバー・リンクの提供はありません。
いいえ	はい	はい	オンデマンド・ターゲットの実行可能ファイルが使用されます。	起動ページは、オンデマンド・ターゲットの開始に失敗した場合に使用できるフェイルオーバー・リンクを 1 つ提供します。このリンクは、Java™ Web Start 方式のみを使用します。

.

Lite Web Portal

Lite Web Portal では、コントローラーとターゲットがインターネット上にある場合でも、VPN を使用せずにオンデマンド・ターゲットで Remote Control セッションを開始できます。

Lite Web ポータルでは、VPN 経由で企業ネットワークに接続しなくても、オンデマンド・ターゲット・セッションを開始できます。これは、テレワーク・シナリオでの VPN 過負荷の課題に対処します。これにより、ターゲットとコントローラー・マシンが企業ネットワーク内にある場合だけでなく、企業ネットワークの外部にある場合にもターゲットを管理できます。Lite Web Portal を使用すると、標準のブローカー・セッションと同様にオンデマンド・ターゲットをシームレスに管理できます。

この機能はデフォルトでは構成されていません。Remote Control 管理者として、Lite Web Portal を介して接続を確立するには、関連する設定を構成する必要があります。構成設定方法について詳しくは、Lite Web Portal の設定 を参照してください。Lite Web Portal の設定を有効にすると、Lite Web Portal を使用してオンデマンド・ターゲットとのセッションを確立できます。セッションの開始方法については、Lite Web Portal を使用したセッションの開始 を参照してください。セッションが確立されると、コントローラーからサーバーへの他の HTTPS コールもリバース・プロキシー・トンネルを通過します。

HTTP のみ: HTTPS リバース・プロキシー (InboudHTTPS 接続の種類) をポータルに使用することをお勧めします。これにより、HTTPS チャネルの確立が保証されます。

ブローカーの証明書: 追加のブローカーの証明書は必要ありません。Lite Web Portal は、既存のブローカーの証明書を使用できます。

ポリシー: 標準のブローカー・セッションで使用されているのと同じポリシーは、セッションが Lite Web Portal を介して開始されるときにも有効になります。詳しくは、『未登録ターゲットのセッション・ポリシー』を参照してください。

トラブルシューティングと監視については、「Lite Web Portal アクティビティーのモニタリング」を参照してください。

制限:

- リバース・プロキシーの制限は、Lite Web Portal にも適用されます。
- Lite Web Portal は現在 SSO をサポートしていません。SSO 操作しているユーザーは LDAP を構成している場合があり、資格情報の検証は LDAP を介して行われる場合があります。そうでない場合は、ローカルのリモート・コントロール・データベースでユーザー・レベルでパスワードを定義する必要があります。
- Lite Web Portal では、コントローラーからの登録のアップロードはサポートされていません。セッション登録を保存するには、ターゲットに登録するポリシーを設定し、そこから記録をアップロードします。

Lite Web Portal の設定

オンデマンド・ターゲット・セッションを開始するように Lite Web Portal を構成する方法について説明します。

Lite Web Portal を構成するには、以下の手順を実行します。

1. 有効な管理者 ID およびパスワードでサーバー UI にログオンします。
2. **「アドミニストレーター」 > 「プロパティー・ファイルを編集」** をクリックし、ドロップダウン・メニューから **「ondemand.properties」** を選択します。
3. **「Lite Web Portal の選択を有効にして構成する」**セクションまでスクロール・ダウンします。
4. カスタム・フィールドの値を入力します。

   Liteweb.portal.enable

   Lite Web Portal を有効にするには、`True` に設定します。

   Liteweb.portal.autodetect.url

   True に設定します。これにより、ブローカーがプロキシーとして機能する残りのアクションが解決されます。

   Liteweb.portal.url

   liteweb.portal.autodetect.url が True に設定されている場合は無視します。false の場合は、ブローカー・マシンのホスト名とポートを構成します。

5. 「**送信**」をクリックします。
6. **「アドミニストレーター」 > 「アプリケーションをリセット」**をクリックします。

このフィールド定義について詳しくは、Lite Web Portal を構成するプロパティーを参照してください。

注: Remote Control ブローカーの代わりにサード・パーティーのリバース・プロキシーを使用している場合は、Lite Web Portal が正しく動作するように、`https://<proxy>:<port>/<page>` から来るすべての要求が `https://<rcserver>:<port>/trc/ondemand/<page>` に転送されていることを確認します。

Lite Web Portal を使用したセッションの開始

Lite Web Portal を使用してオンデマンド・ターゲット・セッションを開始する方法について説明します。

- Light Web Portal のプロパティーが構成されていることを確認します。構成方法については、「Lite Web Portal の設定」を参照してください。
- リバース・プロキシーが正しく構成されていることを確認します。

注: サード・パーティーのリバース・プロキシーを使用していて、「ブローカー・セッションの開始」または「ブローカー・セッションに参加」をクリックした後にエラーが発生した場合は、次の操作を行います。

- URL **https://<hostname>:<port>/lwlogin** (「hostname」はリバース・プロキシー・サーバー) を使用して Lite Web Portal にアクセスしていることを確認してください。
- 正しい URL を使用して Lite Web Portal にアクセスしていてもエラーが発生する場合は、プロキシーが正しく構成されていることを確認してください。**https://<hostname>:<port>/lwlogin** へのすべての要求は、プロキシー・サーバーによっては **https://<hostname>:<port>/**

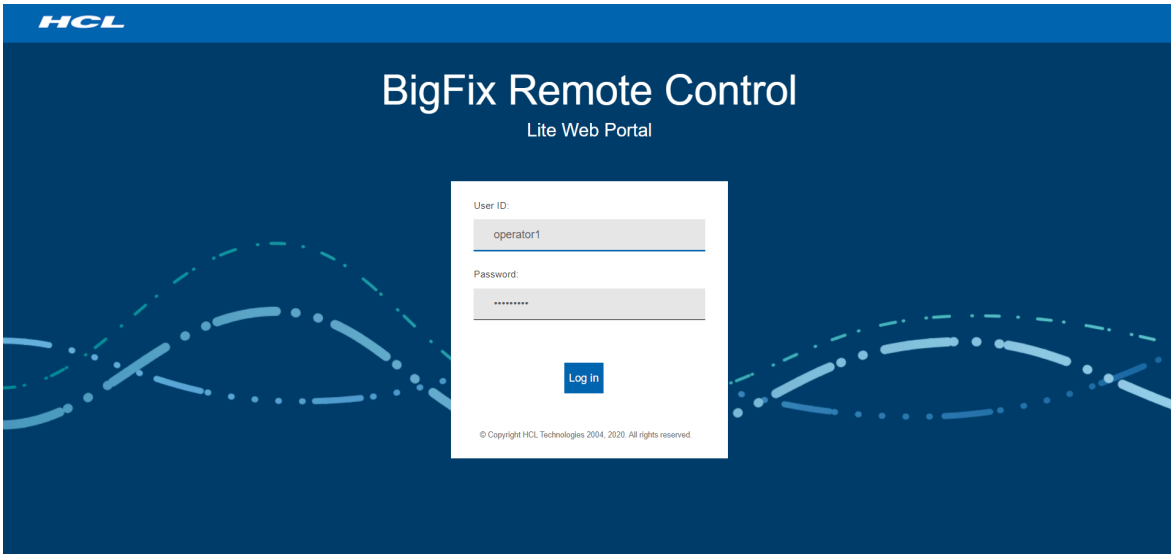
trc/ondemand/<page> または **https://<rcserver>:<port>/trc/ondemand/<page>** (ここでは <rcserver> は Remote Control サーバーのホスト名) に転送する必要があることに注意してください。

- セッションを確立するシステムに Remote Control コントローラーがインストールされていることを確認します。

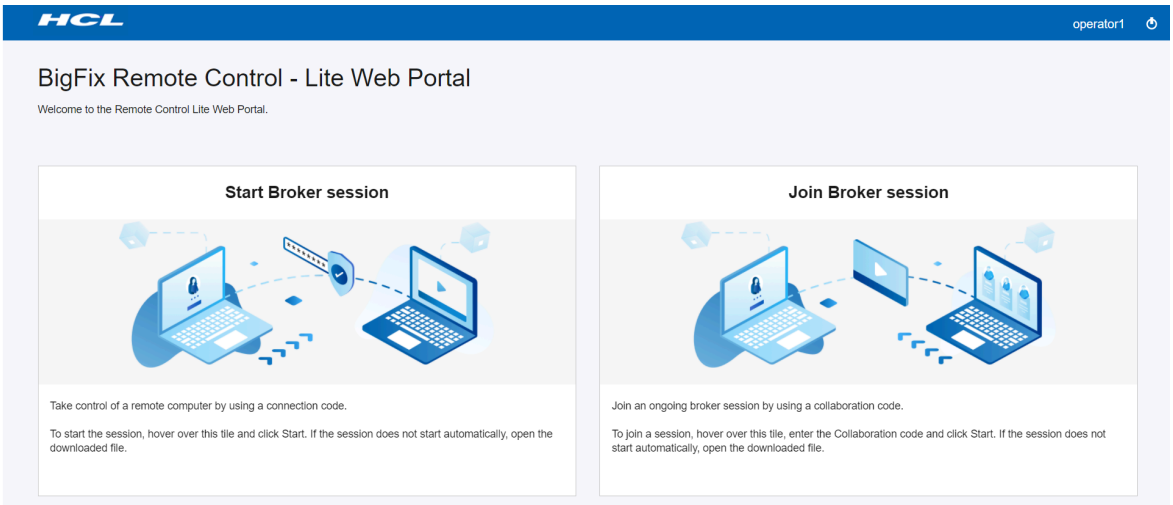
注: パフォーマンスとセキュリティー上の理由から、インターネット経由で実行時に `trc_console.jar` をダウンロードすることはお勧めできません。そのため、プリインストールされたコントローラーを使用して、Lite Web Portal を介してリモート・セッションを開始します。

ターゲットとコントローラーがインターネット上にある場合でも、VPN を使用せずにオンデマンド・ターゲット・セッションを開始します。

1. Remote Control サーバー URL (Light Web Portal のプロパティーで https://hostname:port/lwlogin の形式で構成します) を開きます。ログイン画面が次のように表示されます。



2. 有効な ID とパスワードを使用してログインします。正常にログインすると、次のように、Lite Web Portal ページが表示されます。



3. **「ブローカー・セッションの開始」**をクリックし、**「開始」**をクリックします。`*.trcjws` ファイルが自動的にダウンロードされます。
4. ダウンロードしたファイルをクリックします。Remote Control コントローラーが開き、生成された接続コードと URL が表示されます。
5. 接続コードまたは URL をターゲット・コンピューター・ユーザーと共有します。この URL をブラウザーに入力して画面上の説明に従うようにターゲット・ユーザーに依頼してください。

ターゲット・ユーザーが必要な情報を入力すると、 ターゲット・ソフトウェアのインストール・プロセスが開始されます。必要な許可をコントローラー・ユーザーが持っており、 セッションがサーバーによって認証されている場合は、 リモート・コントロール・セッションが開始します。セッションのユーザー確認が有効になっている場合、ターゲット・ユーザーはセッションを受け入れるか拒否する必要があります。

ターゲット・ユーザーが管理者権限を持っている場合、オンデマンド・ターゲット・バイナリーが実行されるときに UAC プロンプトが表示されます。ターゲット・ユーザーに管理者権限がない場合、UAC プロンプトは表示されません。この場合、バイナリーを実行するために特別な権限は必要ありません。

注: ターゲット・ユーザーがセッションを拒否すると、 オンデマンド・ターゲットに関連付けられたすべてのファイルおよびディレクトリーが削除されます。

関連情報

オンデマンド・ターゲットとのセッションの開始

Lite Web Portal アクティビティーのモニタリング

Lite Web Portal アクティビティはー、Remote Control サーバーのログ・ファイルに記録されます。

ログ・メッセージの形式は次のとおりです。

```
[LEVEL] LiteWebPortal - Message
```

各部の意味は以下のとおりです。

- `LEVEL` はメッセージの関連度です。可能な値は、DEBUG、INFO、WARNING および ERROR です。
- `LiteWebPortal` は、Lite Web Portal アクティビティーを識別するメッセージ・プレフィックスです。
- `Message` は、ポータルのアクティビティーを示すメッセージです。

通常とは異なる Lite Web Portal のアクティビティーを登録する場合は、HCL サポートにお問い合わせください。

トラブルシューティング

オンデマンド・ターゲットのインストール時には、 ターゲット・ユーザーのホーム・ディレクトリーにログ・ファイルが作成されます。このファイルをデバッグのために使用して、 ターゲットのインストール中やリモート・コントロール・セッション中に発生したエラーについて調査することができます。

ログ・ファイルは以下の命名形式で作成されます。

`trc_odt_trace_yyyymmdd_hhmmss.log`

例えば、`trc_odt_trace_20130509_143252.log` です。

Java™ アプレット方式のインストールを使用するときのエラー

Java™ アプレット方式を使用してオンデマンド・ターゲットをインストールするとき、以下のエラーが報告されることがあります。エラーは状況ウィンドウに表示され、ログ・ファイルにも書き込まれます。状況ウィンドウは、ターゲット・ユーザーによって閉じられるまで表示されます。Java™ アプレット・インストールについて詳しくは、Java アプレットを使用したオンデマンド・ターゲットのダウンロードを参照してください。

正しくない URL:{0}

誤った形式の URL がターゲット・ユーザーによって入力された場合。例えば、次のような URL は無効です。http://example.com/#123456

{0} の正しくないサーバー応答: 応答コード {1}

無効な URL が提供された場合。例えば、「`http://example.com/index.jsp?conncode=0000000` の正しくないサーバー応答: 応答コード: `404`」と表示されます。

ホスト・アーキテクチャーを判別できません

Java™ アプレットは、ターゲット・コンピューターのアーキテクチャーが 32 ビットか 64 ビットかを判別できません。

{0} -c={1} -l={2} の実行でエラーが発生しました。

Java™ アプレットがオンデマンド・ランチャーの開始に失敗した場合。例えば、「`/tmp/trc_odt-abc-123.exe -c=http://configurl -l=C:Userstgtusertrc_odt_trace_20130510_131023.log` の実行中にエラーが発生しました (Error running /tmp/trc_odt-abc-123.exe -c=http://configurl -l=C:Userstgtusertrc_odt_trace_20130510_131023.log)」と表示されます。

{0} からのダウンロード中に IO エラーが発生しました

ODL または構成パッケージをサーバーからダウンロードするときに読み取りまたは書き込みエラーが発生した場合。例えば、「`http://configurl` からのダウンロード中に `IO` エラーが発生しました」と表示されます。

ログ・ファイルを書き込み用に開けません

Java™ アプレットがデバッグ・ログ・ファイルを作成できない場合。

注: Java™ アプレットは、Java™ バージョン 1.5 で作成されています。そのため、Java™ アプレットを正しく実行させるには、ターゲット・ユーザーがブラウザーにバージョン 1.5 以降の Java™ プラグインをインストールしておく必要があります。

ActiveX 方式のインストールを使用するときのエラー

ActiveX 方式を使用してオンデマンド・ターゲットをインストールするとき、以下のエラーが報告されることがあります。エラーはログ・ファイルに書き込まれます。ActiveX インストール方式について詳しくは、ActiveX コントロールの使用による オンデマンド・ターゲットのダウンロードを参照してください。

オンデマンド・ターゲット・アプリケーション・ファイルのダウンロードに失敗しました

オンデマンド・ターゲットのインストールに必要なファイルのダウンロードに失敗しました。

オンデマンド・ターゲット構成ファイルのダウンロードに失敗しました

オンデマンド・ターゲットの構成に必要なファイルのダウンロードに失敗しました。

オンデマンド・ターゲットのインストールおよびロードの状況アイコン

状況アイコンは、オンデマンド・ターゲットのインストール中およびロード中に表示され、 成功したか失敗したかを示します。

プラグインのダウンロード中およびインストール中に表示されるアイコン。オンデマンド・ターゲットのロード中にも表示されます。

プラグインが正常にインストールされ、オンデマンド・ターゲットがロードされたときに表示されるアイコン。

プラグインのインストールに失敗したかオンデマンド・ターゲットのロードに失敗したときに表示されるアイコン。エラーは、 ユーザーのホーム・ディレクトリーのログ・ファイルに書き込まれます。

macOS でオンデマンド・ターゲットを起動するとエラーが発生する

オンデマンド・ターゲット・パッケージをダウンロードした後、アプリケーションを起動しようとすると、「アプリケーション "BigFixRC-xxx" を開けません」というエラーが表示されることがあります。

これは、プログラムがインターネットからダウンロードされると (サイトが信頼されているかどうかに関係なく)、ブラウザーや Archive Manager などの他のアプリケーションが、アプリケーションに信頼できないというフラグを立て、特定のファイル属性を設定することによってファイルを検疫できるためです。これにより、アプリケーションが起動されなくなります。

この問題を解決するには、サーバーを 10.0.0-0029 以降のバージョンにアップグレードするか、オンデマンド・ターゲットを使用するたびに以下のステップを実行します。

1. `BigFixRC.zip` を「ダウンロード」フォルダーに保存します。
2. 「`.zip`」ファイルをダブルクリックして、`.app` を抽出します。

   注: Safari を使用している場合、.app は自動的に抽出されます。

3. 端末アプリケーションを開き、以下を実行します
   a. `xattr -dr com.apple.quarantine $HOME/Downloads/BigFixRC_-_xxx.app`
   b. `chmod -R u+x $HOME/Downloads/BigFixRC_-_xxx.app`

      注: コマンドの `xxx` は、ファイル名で報告された文字列に置き換える必要があります。

4. 「`.app`」をダブルクリックするか、端末で `open $HOME/Downloads/BigFixRC_-_xxx.app` を実行します。

オンデマンド・ターゲットが起動されます。

よくある質問

オンデマンド・ターゲットの定義を教えてください。

オンデマンド・ターゲットとは、インターネット上にあるシステムでリモート・コントロール・セッションを開始できるように一時的にインストールされるターゲットのことです。セッションは Remote Control サーバーで設定されたポリシーに従って管理され、ターゲット・ソフトウェアはセッション終了時に削除されます。

未登録ターゲットの定義を教えてください。

未登録ターゲットとは、その詳細を Remote Control サーバーにアップロードしないターゲットのことです。未登録ターゲットには 2 つのタイプがあります。

- オンデマンド・ターゲット。
- ターゲット・ソフトウェアがインストールされており、**Managed** プロパティーが「いいえ」に設定されており、**BrokerList** プロパティーがブローカーのリストで構成されているシステム。

所有する独自の Web サイトで、オンデマンド・ターゲット・ポータルへのアクセスを提供する方法を教えてください。

静的ポータルまたは動的ポータルを作成することで、Web ページを独自のサイトに組み込むことができます。カスタム・ポータルの作成の詳細については、カスタム・ランディング・ページの作成を参照してください。

リモート・コントロール・セッション中に、画面にメッセージが表示されてフリーズし、セッションが一時停止する理由を教えてください。

代わりに、 以下のメッセージが表示されます。 「 お待ちください... エンド・ユーザーによるセキュアなデスクトップ・アクション（UAC プロンプト、ユーザーの簡易切り替え、画面のロック）が完了するまで、画面キャプチャーはターゲット・オペレーティング・システムによって一時的に中断されます。このアクションが完了すると、画面キャプチャーが再開されます」というメッセージは、以下の理由により表示されることがあります。

ターゲット・システムに Windows™ がインストールされている場合

- ターゲット・システムにユーザー・アクセス制御のプロンプトが表示されている。
- ターゲット・システムで**「ユーザーの簡易切り替え」**が有効になっており、別のユーザーがログオンした。
- ターゲット画面がロックされており、ターゲット・ユーザーがロックを解除しなければならない。

ターゲット・システムに Linux™ がインストールされている場合

- ターゲット・システムで**「ユーザーの簡易切り替え」**が有効になっており、別のユーザーがログオンした。

リモート・コントロール・セッションは、ターゲット・ユーザーが関連アクションを完了し、セッションが開始された元のターゲット・デスクトップが再表示された後で、続行されます。例えば、別のユーザーに切り替えた場合、セッションを続行するには、元のターゲット・ユーザーのデスクトップに再び切り替える必要があります。

自分のコンピューターに保存したオンデマンド・セッションの記録を再生する方法を教えてください。

ヘルプ・デスクの担当者から Web ページの URL を取得する必要があります。Web ページにアクセスすると、Remote Control プレイヤーがダウンロードされ、開始されます。このプレイヤーを使用して、記録ファイルを再生します。記録の保存および再生の詳細については、オンデマンド・ターゲットでのセッション記録の保存を参照してください。

ターゲットとコントローラの両方がインターネット上にある VPN を使用せずにオンデマンド・セッションを開始するにはどうすればよいですか?

この場合、オンデマンド・セッションを開始するように Lite Web Portal を構成する必要があります。詳しくは、『Lite Web Portal の設定』を参照してください。

索引

ほ