

# Citrix Receiver for Linux 13.4について

Jan 23, 2017

Citrix Receiver for Linuxを使用すると、さまざまな種類のLinuxデバイスからデスクトップ、アプリケーション、およびデータにすばやく安全にアクセスできます。Citrix製品によるITインフラストラクチャ環境でReceiverを使用すると、作業を行うユーザーの機動性、便宜性、および柔軟性が向上します。

## Citrix Receiver for Linux 13.4

このリリースでは、以下の新しい機能および強化機能を提供し、以前報告されたさまざまな問題を解決し、操作性を向上させます。

- Desktop Viewer

Desktop Viewerによって、複数の仮想デスクトップとネイティブのデスクトップを同時に効果的に操作できます。Desktop Viewerソルバーの機能によって、モニターを横断したマルチモニターのサポートなど、ウィンドウモードと全画面モードのセッションの切り替えることができます。同じエンドポイントデバイス上で複数のXenDesktop接続を使うことにより、デスクトップセッションを切り替えて、複数のデスクトップで実行できます。すべてのデスクトップセッションを最小化し、Ctrl+Alt+Delキーボードシーケンスを送信し、接続を切断し、セッションをログオフするボタンが提供されるため、簡単にユーザーのセッションを管理できます。

- 相対マウスモードと絶対マウスモードのサポート
- 近接カードおよびシンクライアントOEMを統合するための資格情報を入力するSDK (CISDK)
- SecMaker CIDのサポート
- 選択的なH264のサポート

SoC SDKを使用している場合、H264最適化機能の更新が必要になる場合があります。

- 認証ダイアログの機能強化

Citrix Receiver for Linuxによって、認証ダイアログのタイトルを、HTTP応答ヘッダで名前X-Citrix-AM-Titleに変更できるようになりました。ユーザーは、ログオンする対象をより簡単に認識できます。

- FTUエクスペリエンスの強化 (特にSMS認証を使用している場合)

詳しくは、「[CTX205892](#)」を参照してください。

- デフォルトのスマートカードのサポートを強化

スマートカード認証を可能にするStoreFrontサーバーに接続した場合、\$ICAROOT/config/AuthManConfig.xml構成ファイルで「PKCS11module」に値が設定されていないと、Receiverが標準の場所でopensc-pkcs11.soドライバーを見つけて、それを使用します。これによって、AuthManConfig.xmlに変更を加える前に、リーダーやカードを挿入することを求めるメッセージが表示されることがあります。スマートカードを使用しない場合、「Log on with another method」リンクを選択します。

- セキュリティを継続的に向上させるために、Receiver for LinuxはTLS接続のOpenSSLのバージョン1.0.1を使用するようになりました。

## [このリリースで解決された問題について](#)

## このリリースの既知の問題について

- デフォルトでは、selfserviceおよびstorebrowseコマンドのプロキシサポートは提供されません。 StoreFrontサーバーでプロキシサーバーを使用するには、環境変数http\_proxyおよび/またはHTTPS\_PROXYを設定してからこれらのコマンドを使用してください。 環境変数は、次の形式で設定します：.[]

[#403729]

- デスクトップを最初に起動するとき、Citrix Receiver for LinuxはPIVスマートカードを認識しません。

[#491235]

- サーバーを再起動後すぐにCitrix Receiver for Linuxがサーバーを見つけられないと、不明確なエラーメッセージが表示されます。

[#553886]

- セッション画面の保持タイマーの有効期限が切れると、正しくないメッセージダイアログが表示されます。

[#556899]

- SSLv3プロトコルが有効なVDAに接続するとエラーメッセージ（「未知のエラー1000047」など）が表示されます。

[#558641]

- SSLv3プロトコルが有効なStoreFrontサーバーに接続すると全般ネットワークエラーが表示されます。

[#558653]

- storebrowseの-c SharedUserMode[=value]を使用してパラメーターSharedUserModeを変更するには、使用する値パラメーターの大文字と小文字を完全に一致させる必要があります。 storebrowseの値パラメーター、-c SharedUserMode[=value]を使用する場合、大文字と小文字はTrueまたはFalseと完全に一致している必要があります。無効な値パラメーターが使用されると、エラーメッセージは表示されません。 例：-c SharedUserMode=True

[#559402]

- SSLv3プロトコルのみを有効にしてターミナルサーバー（たとえば、RDS）に接続すると接続には予想通り失敗しますが、SSLピアハンドシェイクエラーによっては失敗しない可能性があります。

[#567407]

- 汎用USB Webカメラ入力が64ビットシステムで失敗します。

[#568556]

- storebrowse -dコマンドは、セルフサービスにより作成された以前にクリアされたキャッシュ済みのストア情報を削除しません。つまり、引き続いてストアに追加されると、セルフサービスUIが以前キャッシュされた状態から読み込みます。

[#569806]

- コネクションセンターはIPv6をサポートしません。

[#571743]

- 負の値を\$HOME/.ICAClient/All\_Regions.iniのTCPRecvBufferSizeなどの正数構成エントリとして指定すると、値は正の値としてWFICAに間違って渡されます。この問題を解決するには、\$ICAROOT/config/module.iniを使ってTCPRecvBufferSizeの負の値を設定します。

[#575474]

- GStreamerヘルパープロセスにより、GLIBスレッド問題に関連した警告が表示されます。

[#580753]

- ARMELブラウザプラグインは、このリリースでは機能しません。

[#588044]

- 64ビットのLinux Receiverから起動したWindows 7デスクトップ上のWindows Media Playerは、H264 gstreamerプラグインを使用しないと、ビデオやオーディオを再生できません。この問題が発生すると、サーバー側でレンダリングされたビデオが呼び出されます。

[#588298]

- '-span o'引数を使用してセッションウィンドウリダイレクトを上書きすると、Desktop Viewerツールバーを使用して、全画面モードのセッションをウィンドウモードに縮小することができません。

この問題を解決するには、'-span o'オプションを使用しないでください。代わりに、ウィンドウマネージャーで\_NET\_WM\_FULLSCREEN\_MONITORSサポートを使用するか、Desktop Viewerを無効にしてください。

[#634855]

- Desktop Viewerで「切り替え」ボタンの下の別のセッション名をクリックすると、セッションがポップアップしないことがあります。

[#648716]

- X1 UIからクラシックUIに切り替えると、Receiver for Linuxは応答なくなります。

セルフサービスUIがエラー「NoWebUI 0」を表示した場合、セルフサービス処理を再起動し、セルフサービスUIを通常に戻します。

[#652810]

- Flashリダイレクトがマルチモニタークライアントで誤った場所を使用します。

複数のモニターでクライアントがFlashリダイレクトを使用すると、Flashコンテンツが意図した以外のモニターや画面外に表示されます。これを回避するには、Flashリダイレクト機能を試行する前に、すべての使用可能なモニターでセッションが実行されていることを確認します。

[#653550]

- このリリースを更新すると、All\_Regions.iniファイルのオプションによって、エラーが発生することがあります。

[#654826]

- HDX Webカメラリダイレクトは、起動から45秒間無効になります。

これを回避するには、~/ICAclient/wfclient.iniファイル（または\$ICAROOT/config/module.iniファイル）の[wfclient]セクションに次のエントリを追加します。HDXRTMEWebCamLaunchDelayTime=0。

HDX Webカメラリダイレクトではなく、RTMEプラグインを使用する場合は、この値を変更しないでください。

[#655775]

# システム要件

Jan 23, 2017

このトピックでは、Citrix Receiver for Linuxのインストールに必要なシステムとユーザーの要件について説明します。

## Devices

- glibcxx 3.4.15以降、glibc 2.11.3以降、gtk 2.20.1以降、libcap1またはlibcap2、およびudevをサポートするLinuxカーネルのVersion 2.6.29以降。
- セルフサービスユーザーインターフェイス用
  - libwebkitまたはlibwebkitgtk 1.0
  - libxml2 2.7.8
  - libxerces-c 3.1
- ALSA (libasound2)、Speex、およびVorbisコーデックライブラリ。
- Receiverのインストールには20MBのディスク空き容量が必要です。インストールパッケージの内容を抽出するには、40MBのディスク空き容量が必要です。ディスクの空き容量を確認するには、ターミナルウィンドウで次のコマンドを実行します。  
df -k
- HDX MediaStream Flashリダイレクトを使用するSoC (system-on-a-chip) デバイスでは、1GB以上のRAMが必要です。
- 256色以上のビデオディスプレイ。
- TCP/IPネットワークシステム。

## H.264

x86デバイスの場合、1.6GHz以上のプロセッサで一般的な解像度（1280×1024ピクセルなど）の単一モニターセッションが良好に表示されます。HDX 3D Pro機能を使用する場合は、ネイティブのハードウェアアクセラレーションをサポートするグラフィックドライバと2GHz以上のプロセッサが必要です。

ARMデバイスで通常のH.264サポート機能およびHDX 3D Pro機能を使用する場合は、ハードウェアH.264デコーダーが必要です。より高速なプロセッサを使用することでパフォーマンスが向上します。

## HDX MediaStream Flashリダイレクト

HDX MediaStream Flashリダイレクトの要件については、[CTX134786](#)を参照してください。

最新機能およびセキュリティ上の修正を活用するには、新しいバージョンを展開する前に、最新のプラグインをテストすることをお勧めします。

## HDX RealTime Webカメラビデオ圧縮

HDX RealTime Webカメラビデオ圧縮の要件は以下のとおりです。

- Video4Linux互換Webカメラ
- ディストリビューションの"plugins-good"パッケージを含むGStreamer 0.10.25（または0.10.x以降）。

## HDX MediaStream Windows Mediaリダイレクト

HDX MediaStream Windows Mediaリダイレクトの要件は以下のとおりです。

- ディストリビューションの"plugins-good"パッケージを含むGStreamer 0.10.25（または0.10.x以降）。一般的に、バージョン0.10.15以降はHDX MediaStream Windowsメディアリダイレクトをサポートします。

注：または、<http://gststreamer.freedesktop.org>からGStreamerをダウンロードできます。特定のコーデックの使用には、その製造元からのライセンスが必要な場合があります。使用するコーデックのライセンス要件については、社内の法務部門に確認してください。

## Philips SpeechMike

Philips SpeechMikeデバイスをReceiverで使用する場合には、ユーザーデバイスに関連のドライバーをインストールする必要があります。必要な情報とソフトウェアのダウンロードについては、Philips社のWebサイトにアクセスしてください。

## スマートカードのサポート

Citrix Receiver for Linuxでスマートカードのサポートを構成するには、スマートカード認証を許可するよう構成されたStoreFrontサービスサイトが必要です。

### 注意

注：Web Interface構成（以前のProgram Neighborhoodエージェント）用のXenApp Servicesサイト、またはStoreFrontサーバーにより提供できる「従来のProgram Neighborhood エージェント」サイトでは、スマートカードはサポートされません。

Citrix Receiver for Linuxは、PCSC-Liteと互換性があるスマートカードリーダーおよび適切なLinuxプラットフォーム用のPKCS#11ドライバーがあるスマートカードをサポートします。デフォルトで、Receiver for Linuxは、標準の場所でopencsc-pkcs11.soを認識するようになりました。Receiver for Linuxが確実に標準以外の場所でopencsc-pkcs11.soを見つけるか、別のPKCS#11ドライバーを見つけるには、次の手順に従って構成ファイル内に場所を保存します。

1. 次の構成ファイルにアクセスします：`$ICAROOT/config/AuthManConfig.xml`
2. 行 `<key>PKCS11module</key>` に移動し、この行のすぐ後でドライバーの場所を `<value>` エレメントに追加します。  
注：ドライバーの場所のファイル名を入力すると、Receiverは\$ICAROOT/PKCS#11 ディレクトリ内のそのファイルに移動します。または、"/"から始まる絶対パスを使用できます。

スマートカードを取り出した場合のCitrix Receiver for Linuxの動作を構成するには、次の手順に従って構成ファイルでSmartCardRemovalActionを更新します。

1. 次の構成ファイルにアクセスします：`$ICAROOT/config/AuthManConfig.xml`
2. 行 `<key>SmartCardRemovalAction</key>` に移動し、この行のすぐ後で'noaction'または'forcelogoff'を`<value>` エレメントに追加します。

デフォルトの設定は'noaction'です。この場合、スマートカード上で削除を実行する時に、保存されている資格情報やスマートカードに関して生成されるトークンはクリアされません。'forcelogoff'を追加すると、スマートカードの削除時にすべて資格情報およびStoreFront内のトークンがクリアされます。

## Citrixサーバー

- XenAppの以下のバージョン：
  - XenApp 7.9
  - XenApp 7.8
  - XenApp 7.7
  - XenApp 7.6
  - XenApp 7.5
  - XenApp 6.5, Feature Pack 2, for Windows Server 2008 R2
  - XenApp 6.5, Feature Pack 1, for Windows Server 2008 R2

- XenApp 6.5 for Windows Server 2008 R2
- XenApp 6 for Windows Server 2008 R2
- XenApp 5 for Windows Server 2008
- XenDesktopの以下のバージョン :
  - XenDesktop 7.9
  - XenDesktop 7.8
  - XenDesktop 7.7
  - XenDesktop 7.6
  - XenDesktop 7.5
  - XenDesktop 7.1
  - XenDesktop 7.0
  - XenDesktop 5.6 Feature Pack 1
  - XenDesktop 5.6
  - XenDesktop 5.5
  - XenDesktop 5
- VDI-in-a-Box
  - VDI-in-a-Box 5.3
  - VDI-in-a-Box 5.2
- StoreFront Receiver for WebとWeb Interfaceとともに、NetScaler GatewayのプラグインがあってもなくてもCitrix Receiver for Linux 13.4のブラウザーベースのアクセスを実行できます。  
StoreFront :
  - StoreFront 3.x、2.6、2.5、および2.1  
StoreFrontストアへの直接アクセスを提供します。
  - Citrix Receiver for Webサイトが構成されたStoreFront  
StoreFrontストアへのWebブラウザーからのアクセスを提供します。この場合の制限事項については、[Receiver for Webサイト](#)の「重要な注意事項」を参照してください。

NetScaler VPNクライアントを使用する場合のWeb Interface :

- Web Interface 5.4.x for WindowsのWebサイト。  
デスクトップやアプリケーションへのWebブラウザーからのアクセスを提供します。
- XenApp ServicesサイトまたはXenDesktop Webサイトを構成したWeb Interface 5.x for Linux
- Citrix Receiverをユーザーに配布する方法 :
  - ユーザーによるreceiver.citrix.comからのダウンロードを有効にして、StoreFrontとともにメールまたはサービスアドレスの使用を構成します。
  - Citrix Receiver for Webサイト (StoreFrontと共に構成済み) からのインストールを提供します。
  - Citrix Web Interface 5.4からのReceiverのインストールを提供します。

Webブラウザー

- Mozilla Firefox 18.x以降
- Google Chrome 20または21 (StoreFrontが必要) 。  
注 : Google Chrome NPAPIサポートへの変更について詳しくは、Citrixのブログアール [Citrix Preparing for NPAPI being disabled by Google Chrome](#)」を参照してください。

## 接続性

Citrix Receiver for Linuxでは、以下の構成のいずれかを介して、HTTP、HTTPS、およびICA-over-TLS接続を確立できます。

- LAN接続の場合：
  - StoreFront ServicesサイトまたはCitrix Receiver for Webサイトを使用するStoreFront。
  - Web InterfaceサイトまたはXenApp Serviceサイトを使用するWeb Interface 5.4 for Windows。デバイスがドメインに属している場合と属していない場合について詳しくは、XenDesktop 7のドキュメントを参照してください。
- セキュリティ保護されたリモートまたはローカルの接続の場合：
  - Citrix NetScaler Gateway 11.1
  - Citrix NetScaler Gateway 11.0
  - Citrix NetScaler Gateway 10.5
  - Citrix NetScaler Gateway 10.1
  - Citrix Access Gateway Enterprise Edition 10
  - Citrix Access Gateway Enterprise Edition 9.x
  - Citrix Access Gateway VPXStoreFrontでサポートされるNetScaler GatewayおよびAccess Gatewayのバージョンについては、[StoreFrontのシステム要件](#)を参照してください。

注：このトピックに記載されているNetScaler Gatewayについての説明は、特に注記のない限りはAccess Gatewayにも該当します。

## セキュリティが保護された接続と証明書について

注：セキュリティ証明書については、「[セキュリティで保護された接続](#)」および「[セキュリティで保護された通信](#)」を参照してください。

### プライベート（自己署名）証明書

リモートゲートウェイにプライベート証明書がインストールされている場合は、組織の証明機関のルート証明書をユーザーデバイスにインストールしないと、Citrix ReceiverでCitrixリソースにアクセスできません。

注：接続時にリモートゲートウェイの証明書を検証できない場合（ローカルのキーストアにルート証明書が含まれていないため）、信頼されていない証明書のエラーメッセージが表示されます。ルート証明書をクライアントの証明書ストアにインストールする必要があります。

### ユーザーデバイスへのルート証明書のインストール

ユーザーデバイスへのルート証明書のインストール、およびWeb Interfaceでの証明書設定については、[Receiver通信のセキュリティ保護](#)を参照してください。

### ワイルドカード証明書

ワイルドカード証明書は、同一ドメイン内の任意のサーバーで個別のサーバー証明書の代わりに使用します。Citrix Receiver for Linuxはワイルドカード証明書をサポートしますが、組織のセキュリティポリシーに従って使用する必要があります。実際には、サブジェクトの別名（SAN）拡張内のサーバー名の一覧に含まれている証明書などのワイルドカード証明書に代わるものを考慮が必要なことがあります。こういった証明書は、私的証明機関および公的証明機関の両方が発行できます。

### 中間証明書とNetScaler Gateway

証明書チェーンに中間証明書が含まれる場合は、中間証明書をNetScaler Gatewayのサーバー証明書に追加する必要があります。詳しくは、「[中間証明書の構成](#)」を参照してください。

## ユーザー側の要件

Citrix Receiver for Linuxをインストールするためにスーパーユーザー（root）としてログオンする必要はありません。ただし、USBサポートを有効にするには、スーパーユーザーとしてReceiverをインストールおよび構成してください。スーパーユーザー以外のユーザーとしてReceiverをインストールした場合でも、サポートされているWebブラウザでStoreFrontを使用したりReceiverのネイティブインターフェイスを使用したりして公開リソースにアクセスできます。

## システム要件を満たしているかどうかのチェック

Citrixは、Receiverインストールパッケージの一部としてhdxcheck.shスクリプトを提供します。このスクリプトはReceiver for Linuxのすべての機能を実行できるようにするため、デバイスがすべてのシステム要件を満たしているかどうかをチェックします。このスクリプトは、インストールパッケージのUtilitiesディレクトリにあります。

### hdxcheck.shスクリプトを実行するには

1. ターミナルウィンドウを開きます。
2. 公開キー基盤（PKI）の各証明書に同じパスワードを使用する場合は「`cd $ICAROOT/util`」と入力してEnterキーを押し、インストールパッケージのUtilitiesディレクトリに移動します。
3. 公開キー基盤（PKI）の各証明書に同じパスワードを使用する場合は「`./hdxcheck.sh`」と入力してスクリプトを実行します。

# インストールとセットアップ

Jan 23, 2017

Citrix Receiver for Linuxのインストールは、以下のパッケージを使用して行います。これらのパッケージは、[Citrix Webサイト](#)のダウンロード用ページからダウンロードできます。

パッケージ名	内容
<b>Debianパッケージ (Ubuntu、Debian、Linux Mintなど)</b>	
icaclient_13.4.0.10109380_amd64.deb	セルフサービスサポート、64ビットx86_64
icaclient_13.4.0.10109380_i386.deb	セルフサービスサポート、32ビットx86
icaclient_13.4.0.10109380_armhf.deb	セルフサービスサポート、ARM HF
icaclient_13.4.0.10109380_armel.deb	セルフサービスサポート、ARM EL
icaclientWeb_13.4.0.10109380_amd64.deb	Web Receiverのみ、64ビットx86_64
icaclientWeb_13.4.0.10109380_i386.deb	Web Receiverのみ、32ビットx86
icaclientWeb_13.4.0.10109380_armhf.deb	Web Receiverのみ、ARM HF
icaclientWeb_13.4.0.10109380_armel.deb	Web Receiverのみ、ARM EL
ctxusb_2.7.10109380_amd64.deb	USBパッケージ、64ビットx86_64
ctxusb_2.7.10109380_i386.deb	USBパッケージ、32ビットx86
ctxusb_2.7.10109380_armhf.deb	USBパッケージ、ARM HF
ctxusb_2.7.10109380_armel.deb	USBパッケージ、ARM EL
<b>Redhatパッケージ (Redhat、SUSE、Fedoraなど)</b>	
ICAClient-rhel-13.4.0.10109380-0.x86_64.rpm	セルフサービスサポート、RedHat (Linux VDAを含む) ベース、64ビットx86_64

ICAClient-rhel-13.4.0.10109380-0.i386.rpm	セルフサービスサポート、RedHatベース、32ビットx86
ICAClientWeb-rhel-13.4.0.10109380-0.x86_64.rpm	Web Receiverのみ、RedHatベース、64ビットx86_64
ICAClientWeb-rhel-13.4.0.10109380-0.i386.rpm	Web Receiverのみ、RedHatベース、32ビットx86
ICAClient-suse-13.4.0.10109380-0.x86_64.rpm	セルフサービスサポート、SUSEベース、64ビットx86_64
ICAClient-suse-13.4.0.10109380-0.i386.rpm	セルフサービスサポート、SUSEベース、32ビットx86
ICAClient-suse11sp3-13.4.0.10109380-0.x86_64.rpm	セルフサービスサポート、SUSE 11 sp3 (Linux VDAを含む) ベース、64ビットx86_64
ICAClient-suse11sp3-13.4.0.10109380-0.i386.rpm	セルフサービスサポート、SUSE 11 sp3ベース、32ビットx86
ICAClientWeb-suse-13.4.0.10109380-0.x86_64.rpm	Web Receiverのみ、SUSEベース、64ビットx86_64
ICAClientWeb-suse-13.4.0.10109380-0.i386.rpm	Web Receiverのみ、SUSEベース、32ビットx86
ctxusb-2.7.10109380-1.x86_64.rpm	USBパッケージ、64ビットx86_64
ctxusb-2.7.10109380-1.i386.rpm	USBパッケージ、32ビットx86
<b>Tarball (任意のディストリビューション用のスクリプトインストーラ)</b>	
linuxx64-13.4.0.10109380.tar.gz	64ビットIntel
linuxx86-13.4.0.10109380.tar.gz	32ビットIntel
linuxarmhf-13.4.0.10109380.tar.gz	ARM EL
linuxarm-13.4.0.10109380.tar.gz	ARM HF

Web Receiverをサポートするパッケージとセルフサービスをサポートするパッケージの違いは、後者にはWeb Receiverに必要なコンポーネントに加えてセルフサービスに必要なコンポーネントが含まれている点です。セルフサービスに必要なコンポーネントは、Web Receiverに必要なコンポーネントのスーパーセットですが、インストールされるファイルは同一です。

Web Receiverのサポートのみが必要である場合、または使用するディストリビューションにセルフサービスをサポートするために必要なパッケージが存在しない場合は、Web Receiverのみのパッケージをインストールします。

## 注意

可能な場合は、DebianパッケージまたはRPMパッケージを使用してCitrix Receiverをインストールしてください。これらのファイルは、必要なすべてのパッケージが自動的にインストールされるため、一般的には取り扱いがより簡単です。特定のディレクトリにCitrix Receiverをインストールする場合は、Tarballパッケージを使用します。

DebianパッケージからCitrix Receiver for Linuxをインストールするには

Ubuntu上にReceiverをDebianパッケージでインストールする場合は、Ubuntuソフトウェアセンターでパッケージを開くと便利です。

以下の手順で、***packagename***に実際のインストールパッケージの名前を指定します。

このプロシージャではコマンドラインとUbuntu/Debian/Mint用のネイティブパッケージマネージャーを使用します。また、ファイルブラウザでダウンロードした.debパッケージをダブルクリックしてパッケージをインストールすることもできます。通常、これによりパッケージマネージャーが起動して、必要なソフトウェアが自動的にダウンロードされます。パッケージマネージャーを使用できない場合は、同様の機能を持つコマンドラインツール、**gdebi**を使用することをお勧めします。

コマンドラインを使ってパッケージをインストールするには

1. スーパーユーザー (root) としてログオンします。
2. ターミナルウィンドウを開きます。
3. 「**gdebi packagename.deb**」と入力して、次の3つのパッケージのインストールを実行します。次に例を示します。
  - gdebi icaclient\_13.4.0.10109380\_amd64.deb
  - gdebi icaclientWeb\_13.4.0.10109380\_amd64.deb
  - gdebi ctxusb\_2.7.10109380\_amd64.deb

注：上記の例でdpkgを使用するには、「gdebi」を「dpkg -i」に変更します。

icaclientパッケージまたはicaclientWebパッケージをインストールする必要があります。必要に応じて、ctxusbパッケージで汎用USBリダイレクトをサポートします。

4. dkpgを使用する場合、「**sudo apt-get -f install**」と入力して、必要な依存ソフトウェアをインストールします。
5. エンドユーザーライセンス契約に同意します。

RPMパッケージからCitrix Receiver for Linuxをインストールするには

Citrix ReceiverをSUSEのRPMパッケージからインストールしている場合は、rpmユーティリティではなく、YaSTまたはZyppユーティリティを使用します。rpmユーティリティは必要な従属ソフトウェアを一切ダウンロードまたはインストールしません。rpmパッケージのみをインストールします。必要な従属ソフトウェアが見つからない場合、エラーが発生します。

注：RPMパッケージを使ったインストールの例を見るには、Citrix Blogの記事「[Installing Citrix Receiver for Linux 13.2.1 on SUSE Linux Enterprise Desktop](#)」を参照してください。

以下の手順で、**packagename**に実際のインストールパッケージの名前を指定します。

注：Red Hatベースのディストリビューション（RHEL、CentOS、Fedora、ほか）でインストール“... requires libwebkitgtk-1.0.so.0”ということを示すエラーが表示される場合、見つからないパッケージを提供できるEPELレポジトリ（詳細は、<https://fedoraproject.org/wiki/EPEL>で参照できます）を追加する、パッケージのWebバリエーションに切り替える必要があります。

Red HatでEPELレポジトリをセットアップするには

1. ここから適切なソースRPMパッケージをダウンロードします：

[https://fedoraproject.org/wiki/EPEL#How\\_can\\_I\\_use\\_these\\_extra\\_packages.3](https://fedoraproject.org/wiki/EPEL#How_can_I_use_these_extra_packages.3)

2. Red Hat Enterprise 7.xの例：

**yum localinstall epel-release-latest-7 .noarch.rpm**

ヒント：RPM Package Managerでは、必要なソフトウェアが自動的にダウンロードされません。必要なソフトウェアをダウンロードしてインストールするには、コマンドラインで**zypper install <file name>**（OpenSUSE）または**yum localinstall <filename>**（Fedora/Red Hat）を使用することをお勧めします。

EPELレポジトリをセットアップ後、RPMパッケージからReceiverをインストールします

1. スーパーユーザー（root）としてログオンします。

2. 「zypper in packagename.rpm」と入力して、次の3つのパッケージのインストールを実行します。

注：icaclientパッケージまたはicaclientWebパッケージをインストールする必要があります。必要に応じて、ctxusbパッケージで汎用USBリダイレクトをサポートします。

3. ターミナルウィンドウを開きます。

SUSEインストールの場合：

```
zypper in ICAClient-suse-13.4.0.10109380-0.x86_64.rpm
```

```
zypper in ICAClient-suse-13.4.0.10109380-0.i386.rpm
```

```
zypper in ctxusb-2.7.10109380-1.x86_64.rpm
```

Red Hatインストールの場合：

```
yum localinstall ICAClient-rhel-13.4.0.10109380-0.i386.rpm
```

```
yum localinstall ICAClientWeb-rhel-13.4.0.10109380-0.i386.rpm
```

```
yum localhost ctxusb-2.7.10109380-1.i386.rpm
```

4. エンドユーザーライセンス契約に同意します。

**Tarball**パッケージから**Citrix Receiver for Linux**をインストールするには

注：Tarballパッケージは依存関係のチェックまたは依存関係のインストールを実行しません。すべてのシステムの依存関係は、別個に解決される必要があります。

1. ターミナルウィンドウを開きます。

2. .tar.gzファイルを展開して、その内容を一時ディレクトリに保存します。たとえば次のように入力します。 `tar xvfz packagename.tar.gz`
3. 「**./setupwfc**」と入力してEnterキーを押し、セットアッププログラムを実行します。
4. デフォルトの1 (Receiverのインストール) を選択してEnterを押します。
5. 必要なインストールディレクトリのパスおよび名前を入力してEnterキーを押します。インストールディレクトリを指定せずにEnterキーを押すと、デフォルトの場所にReceiverがインストールされます。

スーパーユーザー (root) のデフォルトのインストールディレクトリは、`/opt/Citrix/ICAClient`です。

非スーパーユーザーのデフォルトのインストールディレクトリは、`$HOME/ICAClient/platform`です。platformは、システムにより生成されるオペレーティングシステムIDです。例：`$HOME/ICAClient/linuxx86` for the Linux/x86 platform

注：デフォルトのインストール先以外のディレクトリにインストールする場合は、`$HOME/.profile`または`$HOME/.bash_profile`の`$ICAROOT`にそのディレクトリを設定します。

6. インストールを続行するには、「y」を入力し、Enterキーを押します。
7. Receiverをデスクトップ環境に統合するかどうかを選択できます。これにより、Citrix Receiverを起動するためのメニューオプションがデスクトップ環境に作成されます。「y」と入力すると、デスクトップ統合が有効になります。

注：Receiverをデフォルトのインストール先以外のディレクトリにインストールする場合は、デスクトップ統合が正しく機能するように、`$HOME/.profile`または`$HOME/.bash_profile`の`$ICAROOT`にインストール先ディレクトリを設定してください。

8. GStreamerがインストール済みの場合は、GStreamerをReceiverに統合してHDX Mediastreamマルチメディアアクセラレーションをサポートするかどうかを選択できます。Receiverを統合する場合は、「y」と入力します。

注：一部のプラットフォームにおいては、tar形式の配布からクライアントをインストールすると、KDEおよびGNOMEへの統合を求めるプロンプトが表示された後でシステムがハングすることがあります。この問題は、`gststreamer-0.10`を初めて初期化する場合に発生します。この問題が発生した場合、(ctrl+cを用いて)インストール処理を中断して、コマンド**gst-inspect-0.10 --gst-disable-registry-fork --version**を実行します。このコマンドを実行後、システムがハングすることなくtar形式のセットアップを再実行できるようになります。

9. スーパーユーザー (root) としてログオンしている場合、XenDesktopおよびXenApp公開VDIアプリケーションのUSBサポートのインストールを選択できます。「y」と入力すると、USBサポートがインストールされます。

注：スーパーユーザー (root) としてログオンしていない場合、「USB support cannot be installed by non-root users. (root以外のユーザーはUSBサポートをインストールできません)」という警告が表示されます。この機能を使用する場合は、スーパーユーザーとしてインストーラーを実行してください。

10. インストールが完了すると、メインのインストールメニューに戻ります。セットアッププログラムを終了するには、「3」を入力してEnterキーを押します。

# Citrix Receiver for Linuxのインストールのカスタマイズ

Jan 23, 2017

Citrix Receiverパッケージのコンテンツを変更しファイルを再パッケージして、インストール前にReceiver構成をカスタマイズできます。この変更パッケージを使用してインストールするすべてのバージョンにこの変更が含まれます。

## 注意

インストールの例を見るには、Citrix Blogの記事「[Installing Citrix Receiver for Linux 13.2.1 on SUSE Linux Enterprise Desktop](#)」を参照してください。

Citrix Receiver for Linuxのインストールをカスタマイズするには

1. Citrix Receiverパッケージファイルを空のディレクトリに展開します。パッケージファイルの名前は、platform.major.minor.release.build.tar.gz (Linux/x86プラットフォームならlinuxx86.13.2.0.nnnnnn.tar.gzなど) です。
2. Receiverパッケージに必要な変更を加えます。たとえば、標準のReceiverのインストールには含まれていない発行機関からの証明書を使用する場合は、新しいTLSルート証明書をパッケージに追加します。新しいTLSルート証明書をパッケージに追加する方法については、Citrix製品ドキュメントサイトの「  
—ユーザーデバイスへのルート証明書のインストール  
」を参照してください。 Receiverに付属の証明書については、Citrix製品ドキュメントサイトの「  
—SSLおよびTLSの構成と有効化  
」を参照してください。
3. PkgIDファイルを開きます。
4. パッケージを変更したことを示すために次の行を追加します :MODIFIED=traceinfo ここでtraceinfoは、パッケージの変更者と変更日時を示します。この情報の形式は、任意のものにできます。
5. ファイルを保存して閉じます。
6. パッケージファイルの一覧platform/platform.psf (たとえばLinux/x86プラットフォームの場合ならlinuxx86/linuxx86.psf) を開きます。
7. パッケージファイルの一覧を更新して、パッケージに対する変更を適用します。このファイルを更新しない場合、新しいパッケージのインストール時にエラーが起こることがあります。変更には、修正したファイルのサイズの更新、またはパッケージに追加したファイルに対する新しい行の追加などを含めることができます。パッケージファイルの一覧に含まれている列には次のようなものがあります。
  - File type
  - 相対パス
  - サブパッケージ (corから編集不可)
  - 権限
  - 所有者
  - グループ
  - サイズ
8. ファイルを保存して閉じます。
9. vm-create-from-templateコマンドを使用します。tarを使ってReceiverパッケージファイルを再生成します。例 :tar czf ../newpackage.tar.gz \* ここで<newpackage>は、新しいReceiverパッケージファイルの名前です。

# Citrix Receiver for Linuxの起動

Jan 23, 2017

Citrix Receiverは、ターミナルプロンプト、またはサポートされているデスクトップ環境を使って起動できます。

Citrix Receiverをデフォルトのインストールディレクトリにインストールしなかった場合は、環境変数ICAROOTに実際のインストール先ディレクトリを指定しておく必要があります。

## ヒント

以下の手順は、Webパッケージによるインストールや、tar形式を使用したにもかかわらずセルフサービス要件が満たされなかった場合は適用されません。

コマンドウィンドウでCitrix Receiverを起動するには

コマンドウィンドウで、`/opt/Citrix/ICAClient/selfservice` と入力して、Enterを押します（ここで、`/opt/Citrix/ICAClient`はCitrix Receiverをインストールしたディレクトリです）。

LinuxデスクトップからCitrix Receiverを起動するには

ファイルマネージャーを使ってLinuxデスクトップ環境からCitrix Receiverを起動できます。

一部のデスクトップでは、メニューからCitrix Receiverを起動することもできます。Linuxのディストリビューションにより、Receiverを起動するためのメニューの位置が異なる場合があります。

# Citrix Receiver for LinuxをICA-to-Xプロキシとして使用する

Jan 23, 2017

Citrix Receiverを実行しているワークステーションをサーバーとして使用し、出力を別のX11対応デバイスに転送できます。Citrix Receiverを使用できないX端末またはUNIXワークステーションにMicrosoft Windows用アプリケーションを配信する場合などに、この方法を使います。

## 注意

Citrix Receiverソフトウェアは多くのXデバイスで使用できるので、このデバイスへのソフトウェアのインストールはこの方法を使用することをお勧めします。Citrix ReceiverをICA-to-Xプロキシとして実行することを、サーバー側ICAとも呼びます。

この方法では、実行するCitrix ReceiverをICAからX11へのコンバーターとして使うことで、X11の出力をローカルのLinuxデスクトップ画面に転送します。また、その出力をさらに別のX11コンピューターの画面に転送できます。つまり、1つのシステムで複数のCitrix Receiverのコピーを同時に実行し、それぞれの出力を別の異なるデバイスに送信できます。

この図は、Citrix Receiver for LinuxがICA-to-Xプロキシとして動作するシステムを示しています。



この方法を使うようにシステムを設定するには、LinuxサーバーをICAからX11へのプロキシサーバーとして機能させる必要があります。

- X端末が既にある場合は、XアプリケーションをX端末に供給するLinuxサーバーでCitrix Receiverを実行できます。
- Citrix Receiverを使用できないUNIXワークステーションにアプリケーションを配布する場合は、プロキシサーバーとして機能するサーバーが1台必要です。たとえば、Linuxを実行しているPCをプロキシサーバーとして使用できます。

## サポートされる機能

アプリケーションは、ICAプロトコルの機能を使用して、X11の最終デバイスに提供されます。デフォルトで、プロキシサーバー上のドライブにアクセスするには、ドライブマッピング機能を使う方法しかありません。（通常はローカルドライブがい）X端末を使用している場合は、これは問題ありません。ほかのUNIXワークステーションにアプリケーションを配布する場合は、次のいずれか実行できます。

- ローカルのUNIXワークステーションをNFSを使ってプロキシサーバーにマウントし、プロキシサーバー上のNFSマウントポイントをクライアントドライブとしてマップしてアクセスする。
- SAMBAなどのNFSからSMBへのプロキシサーバー、またはMicrosoft Services for UNIXなどのサーバー上のNFSクライアントを使用する。

次の機能は、最終デバイスに提供されません。

- プロキシとして機能するサーバーがオーディオをサポートしている場合でも、X11デバイスではオーディオを使用できません。

- クライアントプリンターは、X11デバイスでは使用できません。LPD印刷機能を使ってサーバーからUNIXプリンターに手動でアクセスするか、ネットワークプリンターを使用する必要があります。

X端末またはUNIXワークステーションからCitrix Receiverをサーバー側ICAとして起動するには

1. sshまたはtelnetを使って、プロキシとして動作しているデバイスに接続します。
2. プロキシデバイスのシェルで、**DISPLAY**環境変数をローカルデバイスに設定します。たとえば、Cシェルでは、次のように入力します。

```
setenv DISPLAY <local:0>
```

注：コマンドssh -X を使ってプロキシとして動作するデバイスに接続する場合は、**DISPLAY**環境変数を設定する必要はありません。

3. ローカルデバイスのコマンドプロンプトで、次のように入力します。xhost <proxy server name>
4. Receiverをデフォルトのインストールディレクトリにインストールしない場合は、環境変数ICAROOTに実際のインストール先ディレクトリを指定しておく必要があります。
5. Citrix Receiverがインストールされているディレクトリを探します。コマンドプロンプトで、「selfservice &

# Citrix Receiver for Linuxをアンインストールするには

Jan 23, 2017

以下の手順は、Tarballパッケージでテストされています。RPMおよびDebianパッケージの場合は、オペレーティングシステム側の標準的なツールを使用してアンインストールしてください。

環境変数ICAROOTはクライアントのインストールディレクトリに設定する必要があります。非スーパーユーザーのデフォルトのインストールディレクトリは、\$HOME/ICAClient/platformです。ここで、platform変数はシステムにより生成されるオペレーティングシステムIDです。例：Linux/x86プラットフォームの場合、\$HOME/ICAClient/linuxx86。権限を持つユーザーのインストールは、デフォルトが/opt/Citrix/ICAClientです。

1. セットアッププログラムを実行するには、「\$ICAROOT/setupwfc Enterキーを押します。
2. Citrix Receiver for Linuxをアンインストールするには、「2 Enterキーを押します。

## 注意

Citrix Receiver for Linuxをアンインストールするには、インストール時と同じユーザーアカウントでシステムにログオンする必要があります。

# 接続

Jan 23, 2017

Citrix Receiverにより、仮想デスクトップやアプリケーションへの安全なセルフサービスアクセスと、Windows、Web、およびSaaS (Software as a Service) アプリケーションへのオンデマンドアクセスが提供されます。ユーザーのアクセスは、Citrix StoreFrontや従来のWeb InterfaceのWebページにより管理されます。

Citrix Receiverのユーザーインターフェイスを使用してリソースに接続するには

Citrix Receiverのホームページには、ユーザーのアカウント設定（つまり接続先のサーバー）とCitrix XenDesktopまたはCitrix XenAppの管理者による構成に基づいて、そのユーザーに提供されている仮想デスクトップやアプリケーションが表示されます。ユーザーは、[環境設定] ダイアログボックスの[アカウント] ページにStoreFrontサーバーのURLや自分のメールアドレス（メールアドレスによるアカウント検出が有効な場合）を入力してアカウントの構成を行います。

## ヒント

StoreFrontサーバーの複数のストアに同じ名前が使用されている場合、[アカウント] ページはそれらのストアを同一のものとして表示します。このような混乱を避けるため、管理者はストアを構成するときに一意のストア名を使用する必要があります。Program Neighborhoodエージェントの場合、ストアURLが表示され、ストアを確実に識別します。

ユーザーがストアに接続すると、Citrix Receiverのホームページで特定のデスクトップやアプリケーションを検索したり、「+」（プラス記号）をクリックしてそれらの一覧を参照したりできます。デスクトップやアプリケーションのアイコンをクリックすると、その項目がホームページにコピーされます。コピーされた項目をクリックすると、その項目が起動します。このときに、接続が作成されます。

## 接続設定の構成

Citrix Receiverと、XenAppおよびXenDesktopサーバー間の接続に対する数々のデフォルトの設定を構成できます。また必要に応じて、個々の接続に対する設定を変更することもできます。

このセクションの以降のトピックでは、Citrix Receiverのユーザーが実行する一般的な操作の手順について説明します。管理者とユーザーの作業と責任範囲は重複することがありますが、ここでは一般的にユーザーが行う操作について「ユーザー」という用語を使用して区別します。

- [コマンドラインまたはWebブラウザからリソースに接続する](#)
- [リソース接続のトラブルシューティング](#)
- [構成ファイルを使ったReceiverのカスタマイズ](#)

# コマンドラインまたはWebブラウザからリソースに接続する

Jan 23, 2017

Receiverのホームページでデスクトップやアプリケーションのアイコンをクリックすると、サーバーへの接続が作成されます。また、コマンドラインやWebブラウザから接続を開くこともできます。

コマンドラインでProgram NeighborhoodまたはStoreFrontサーバーへの接続を作成するには

まず、サーバー上でストアが使用可能であることを確認します。必要に応じて、次のコマンドを実行してストアを追加します。

```
./util/storebrowse --addstore <store URL>
```

1. 接続するデスクトップまたはアプリケーションの固有のIDを取得します。このIDは、以下のコマンドによる出力の最初の引用文字列です。

- サーバー上のすべてのデスクトップおよびアプリケーションの一覧を取得するには、次のコマンドを実行します。

```
./util/storebrowse -E <store URL>
```

- サブスクリプト済みのデスクトップおよびアプリケーションの一覧を取得するには、次のコマンドを実行します。

```
./util/storebrowse -S <store URL>
```

2. 次のコマンドを実行して、デスクトップまたはアプリケーションを起動します。

```
./util/storebrowse -L <desktop or application ID> <store URL>
```

サーバーに接続できない場合は、管理者がサーバーの場所またはSOCKSプロキシの詳細を変更する必要がある場合があります。詳しくは、「[プロキシサーバー経由の接続](#)」を参照してください。

Webブラウザで接続を作成するには

通常、Mozilla、Netscape、またはChromeを構成する場合、インストール時に自動的に接続が構成されます。

Firefox、Mozilla、またはChrome用に.mailcapおよびMIMEファイルを手動で設定する必要がある場合は、次の手順に従ってファイルを変更して、ICAファイル（拡張子.ica）によりReceiverの実行可能ファイル（wfica）が起動するようにします。ほかのブラウザを使用するには、必要に合わせてブラウザ構成を変更する必要があります。

1. .mailcapファイルを変更する場合は、\$HOME内で、.mailcapファイルを作成または変更して次の行を追加します。

```
application/x-ica; /opt/Citrix/ICAclient/wfica.sh %s; x-mozilla-flags=plugin:Citrix ICA
```

2. MIMEファイルを変更する場合は、\$HOME内で、.mime.typesファイルを作成または変更して次の行を追加します。

```
application/x-ica ica
```

ここで、icaの前にあるx-は、そのicaがInternet Assigned Numbers Authority (IANA) 公認のMIMEタイプでないことを意味します。

# リソース接続のトラブルシューティング

Jan 23, 2017

ユーザーがアクティブな接続を管理するには、接続センターを使用します。セッションの動作が遅い、または接続に問題がある場合、ユーザーや管理者は接続センターを使用してトラブルシューティングを行います。ユーザーは、接続センターで以下の操作を行います。

- アプリケーションを終了する。
- セッションからログオフする。これによりセッションが終了し、実行中のアプリケーションが終了します。
- セッションから切断する。これにより、アプリケーションを実行したまま（切断時にアプリケーションを閉じるようにサーバーを構成していない場合）、選択した接続のサーバー接続が切断されます。
- 接続の転送統計値を参照する。

接続を管理するには

1. Receiverメニューで [接続センター] を選択します。  
接続先のサーバーと、各サーバー上でアクティブなセッションが表示されます。
2. 次のいずれかを行います。
  - サーバーを選択して、切断またはログオフしたり、プロパティを表示したりします。
  - アプリケーションを選択して、ウィンドウを閉じます。

# 構成ファイルを使ったカスタマイズ

Jan 23, 2017

## 構成ファイルについて

Receiverの構成ファイルを編集すると、高度な設定や一般的ではない設定を変更できます。これらの構成ファイルは、wficaの起動時に毎回読み取られます。変更する内容により、異なる構成ファイルを編集できます。

セッション共有が有効な場合は、更新した構成ファイルに基づくセッションが作成される代わりに既存のセッションが使用されることがあります。この場合、更新した構成ファイルの設定はセッションに反映されません。

### すべてのCitrix Receiverユーザーに変更を適用する

Citrix Receiverのすべてのユーザーに変更を適用する場合は、\$ICAROOT/configディレクトリ内のmodule.ini構成ファイルを編集します。

#### 注意

module.iniの値をほかの構成ファイルで上書きする場合を除き、module.iniの構成値のエントリをAll\_Regions.iniに追加する必要はありません。All\_Regions.iniのエントリでデフォルト値を設定すると、その設定に対するmodule.iniの値は使用されません。

### 新しいCitrix Receiverユーザーに変更を適用する

\$HOME/.ICAClient/wfclient.iniファイルが存在しない場合、wficaが\$ICAROOT/config/wfclient.テンプレートをコピーして作成します。このテンプレートファイルに変更を加えると、以降のすべての新しいCitrix Receiverユーザーに適用されます。

### 特定のユーザーのすべてのコネクションに変更を適用する

特定のユーザーのすべてのコネクションに変更を適用する場合は、そのユーザーの\$HOME/.ICAClientディレクトリ内のwfclient.iniファイルを編集します。この構成ファイルによる設定は、そのユーザーの新しいコネクションに適用されます。

### 構成ファイルエントリを検証する

wfclient.iniのエントリの値を制限するには、設定可能な値またはその範囲をAll\_Regions.iniで指定できます。詳しくは、\$ICAROOT/configディレクトリ内のAll\_Regions.iniファイルを参照してください。

#### 注意

module.iniとwfclient.iniで同一エントリに対する値を設定すると、wfclient.iniの値が優先されます。

### 構成ファイルのパラメーターについて

各構成ファイルのパラメーターは、セクションでグループ化されています。各セクションの冒頭には、角かっこで囲まれたセクション名（クライアント側ドライブのマッピングに関するパラメーターの[ClientDrive]など）が記述されています。

特に注記がある場合を除き、記述されていないパラメーターには自動的にデフォルト値が適用されます。パラメーターに値が設定されていない場合も、自動的にデフォルト値が適用されます。たとえば、「InitialProgram=」の後に値が記述されていない場合、デフォルトの設定である「ログオン後にプログラムを実行しない」が適用されます。

## 優先順位

All\_Regions.iniにより、ほかの構成ファイルに設定可能なパラメーターが指定されます。設定可能な値の範囲を指定したり、特定の値を指定したりできます。すべてのReceiverユーザーに適用される設定を変更するには、module.iniを編集します。

通常、構成ファイルは以下の順序でチェックされます。

1. All\_Regions.ini。この構成ファイルの値は、以下のファイルの値よりも優先されます。
  - コネクションのICAファイル
  - wfclient.ini
2. module.ini。この構成ファイルの値は、All\_Regions.ini、コネクションのICAファイル、またはwfclient.iniで設定されておらず、All\_Regions.iniで制限されていない場合に適用されます。

いずれの構成ファイルでも設定されていない場合は、Receiverのデフォルト設定が適用されます。

## 注意

上記の優先順位には例外があります。たとえば、セキュリティ上の理由から、サーバーの設定が適用されないように、一部の値がwfclient.iniから読み取られる場合があります。

# Web Interfaceを使用したCitrix XenApp（以前のProgram Neighborhoodエージェント）接続の構成

Jan 23, 2017

このトピックは、Web Interface上のXenApp ServicesまたはStoreFront上の「旧来のProgram Neighborhood Agent」を使用した展開にのみ適用されます。

selfservice、storebrowse、およびpnabrowseなどのオプションにより、XenApp Servicesサイトを実行するサーバーを介して公開リソース（公開アプリケーションやサーバーデスクトップ）に接続できます。これらのプログラムは接続を直接起動したり、ユーザーが公開リソースにアクセスできるメニューアイテムを作成するために使用したりできます。またpnabrowseは、この目的のためにデスクトップアイテムを作成することもできます。

ネットワーク上でCitrix XenAppを実行しているすべてのユーザーに対してカスタマイズ可能なオプションは、構成ファイルのconfig.xmlで定義されます。このファイルは、Web Interfaceサーバー上に格納されています。ユーザーがこれらのプログラムのいずれかを起動すると、このサーバーから構成データが読み取られます。その後、設定およびユーザーインターフェイスをconfig.xmlファイルで指定された間隔で定期的に更新します。

## Important

config.xmlの設定は、XenApp Servicesサイトで定義されたすべての接続に適用されます。

## コンテンツの公開

XenApp Servicesサイトも、アプリケーションやデスクトップではなくファイルを公開します。この処理は、コンテンツの公開と称され、pnabrowseにより公開ファイルを開くことができます。

Receiverにより認識されるファイルのタイプには制限があります。システム上で公開コンテンツのファイルタイプが認識され、ユーザーがReceiverを使用してそのコンテンツを表示するためには、そのファイルタイプに関連付けられたアプリケーションが公開されている必要があります。たとえば、公開されたAdobe PDFファイルをReceiverで表示するには、Adobe PDFビューアーなどのアプリケーションが公開されている必要があります。適切なアプリケーションが公開されていない場合、ユーザーは公開コンテンツを表示できません。

# 最適化

Jan 23, 2017

環境を最適化することで、Citrix Receiverのパフォーマンスおよびユーザーエクスペリエンスを向上させることができます。次のことを実行することで、パフォーマンスを向上させて最適化できます。

- ユーザーデバイスのマッピング
- USBサポートの構成
- 狭帯域幅接続でのパフォーマンスの向上
- マルチメディアパフォーマンスの向上
- 画面タイルのパフォーマンスの最適化

## ユーザーデバイスのマッピング

Citrix Receiverは、XenAppおよびXenDesktopサーバーへの接続に対してクライアントデバイスのマッピングをサポートします。クライアントデバイスのマッピングによって、サーバー上で実行しているリモートアプリケーションから、ローカルのユーザーデバイスに接続しているデバイスにアクセスできるようになります。ユーザーデバイスのユーザーには、アプリケーションやシステムなどのリソースがローカルで実行されているように表示されます。クライアントデバイスのマッピングを行う前に、サーバーでこの機能をサポートしていることを確認してください。

注：SELinux (Security-Enhanced Linux) のセキュリティモジュールにより、XenAppおよびXenDesktopのクライアント側ドライブのマッピング機能とUSBリダイレクト機能が正しく動作しなくなることがあります。これらの機能を使用する場合は、サーバー上でこれらの機能を構成する前にSELinuxを無効にしてください。

## クライアント側ドライブのマッピング

クライアント側ドライブのマッピング機能により、XenAppまたはXenDesktopサーバーのドライブ文字をローカルユーザーデバイスにあるディレクトリにリダイレクトできます。たとえば、Citrixユーザーセッション内で表示されるHドライブにアクセスしたときに、ローカルユーザーデバイスの特定のディレクトリにリダイレクトされるように設定できます。

クライアントドライブマッピングにより、CD-ROM、DVD、またはUSBメモリスティックなど、セッションにおいてユーザーが使用できるローカルユーザーデバイスにマウントされた任意のディレクトリに、ローカルユーザーがアクセスする権限を授けられます。サーバーでクライアント側ドライブのマッピングが許可されている場合、ユーザーはセッション内で各自のローカルファイルを読み込んで、再びローカルドライブに保存したり、サーバーのドライブに保存したりできます。

2種類のドライブマッピングを実行できます。

- 静的なクライアントドライブマッピングでは、ログオン時にユーザーデバイスの任意のファイルシステムがサーバー上の特定のドライブ文字にマップされるように設定できます。たとえば、CD-ROM、DVD、またはUSBメモリスティックなどのハードウェアデバイスのマウントポイントだけでなく、ユーザーのホームディレクトリや/tmpディレクトリのすべてまたは一部分をマップできます。
- 動的なクライアントドライブマッピングでは、CD-ROMドライブ、DVDドライブ、USBメモリスティックなどのハードウェアデバイスがマウントされるユーザーデバイス上のディレクトリが監視され、セッション内で追加した新しいデバイスが、サーバーで使用可能な最初のドライブ文字に自動的にマップされます。

クライアント側デバイスのマッピングを無効にしない限り、Citrix ReceiverがXenAppやXenDesktopに再接続したときに、マッピングが再確立されます。ポリシーを使用すると、クライアント側デバイスのマッピングを詳細に制御できます。詳しくは、[XenApp](#)および[XenDesktop](#)のドキュメントを参照してください。

ユーザーがドライブマッピングを設定するときは、[環境設定] ダイアログボックスを使用します。詳しくは、[「環境設定」](#)を参照してください。

注：デフォルトでは、静的なクライアントドライブマッピングを有効にすると自動的に動的なクライアントドライブマッピングも有効になります。静的なクライアントドライブマッピングを有効にして動的なクライアントドライブマッピングを無効するには、wfclient.iniでDynamicCDMにFalseを設定します。

## クライアントプリンターマッピング

Citrix Receiverは、ネットワークプリンターおよびユーザーデバイスにローカルで接続されているプリンターへの出力をサポートします。デフォルトでは、ポリシーを作成して変更しない限り、XenAppにより次のことを実行できます。

- ユーザーデバイスからアクセス可能なすべてのプリントデバイスに出力する
- プリンターを追加する

ただし、これらの設定はすべての環境に対して最適な設定とはならない可能性があります。たとえば、ユーザーデバイスからアクセスできるすべてのプリンターへの出力が可能なデフォルトの設定は、最も管理しやすい設定ですが、一部の環境ではログオン時間に時間がかかる要因となる可能性があります。このような状況では、ユーザーデバイス上で構成されたプリンターの一覧に制限するようにします。

また、組織のセキュリティポリシーによっては、ローカルプリンターポートのマッピングを禁止しなければならない場合があります。これを行うには、サーバーのICAポリシーで [クライアントCOMポートを自動接続する] 設定で [無効] を選択します。

ユーザーデバイス上で構成されたプリンターの一覧を制限するには

1. 次のいずれかの場所にある構成ファイル (wfclient.ini) を開きます。
  - %HOME%/ICAClient (1人のユーザーに対するプリンターを制限する場合)
  - %SICAROOT%/configディレクトリ (すべてのユーザーのプリンターを制限する場合。すべてのユーザーとは、構成ファイルの変更後にselfserviceプログラムを初めて使用するすべてのReceiverユーザーを指します)
2. [WFClient] セクションに、次のパラメーターを入力します。

```
ClientPrinterList=<printer1>:<printer2>:<printer3>
```

ここで<printer1>、<printer2>などは、選択したプリンターの名前です。各プリンターをコロン (:) で区切って指定します。

3. ファイルを保存して閉じます。

## XenApp for Windowsでのクライアントプリンターマッピング

Citrix Receiver for LinuxはCitrix PSユニバーサルプリンタードライバーをサポートします。そのためほとんどの場合、ネットワークプリンターまたはユーザーデバイスにローカルで接続されているプリンターへの出力をユーザーがローカルで構成する必要はありません。ただし、ユーザーデバイスのプリントソフトウェアがユニバーサルプリンタードライバーをサポートしていない場合などは、XenApp for Windows上でクライアントプリンターを手動でマップする必要があります。

サーバーにローカルプリンターをマップするには

1. Citrix Receiverでサーバーへのセッションを開始して起動し、XenAppサーバーにログオンします。
2. [スタート] ボタンをクリックし、[設定] > [プリンター] の順に選択します。
3. [ファイル] メニューから [プリンターの追加] を選択します。

プリンターの追加ウィザードが開きます。

4. ウィザードを使って、クライアントネットワークやクライアントドメインからネットワークプリンターを追加します。ほとんどの場合、ネイティブのリモートデスクトップサービスで作成される「セッション3の<クライアント名>からのHP LaserJet 4」などの標準のプリンター名となります。

プリンターの追加について詳しくは、Windowsオペレーティングシステムのドキュメントを参照してください。

## XenApp for UNIXでのクライアントプリンターマッピング

UNIX環境では、Citrix Receiverにより定義されたプリンタードライバは無視されます。ユーザーデバイスのプリントシステムは、アプリケーションにより生成された出力形式を制御する必要があります。

ユーザーがCitrix XenApp for UNIX（日本語版はリリースされていません）からクライアントプリンターに出力できるようにするには、事前に管理者が印刷機能を有効にしておく必要があります。詳しくは、XenAppおよびXenDesktopドキュメントの「[XenApp for UNIX](#)」を参照してください。

## クライアントオーディオマッピング

クライアントオーディオマッピングにより、XenAppサーバー上で実行しているアプリケーションのサウンドを、ユーザーデバイスにインストールされているサウンドデバイスで再生できます。管理者はサーバーで接続ごとに音質レベルを設定できますが、ユーザーもユーザーデバイスで音質レベルを設定できます。ユーザーデバイスとサーバーの音質レベルの設定が異なる場合は、低い方の音質レベルが使用されます。

クライアントオーディオマッピングを使用すると、サーバーとネットワークに大きな負荷がかかります。音質を高くすると、オーディオデータの伝送により多くの帯域幅が必要になります。また高音質にするとサーバーのCPUもより多く使用します。

クライアントオーディオマッピングは、ポリシーを使用して構成します。詳しくは、[XenApp](#)および[XenDesktop](#)のドキュメントを参照してください。

注：クライアントオーディオマッピングは、Citrix XenApp for UNIX（日本語版未発表）に接続する場合はサポートされません。

### 非デフォルトのオーディオデバイスを設定するには

デフォルトのオーディオデバイスは、一般的にはシステムに対して構成されているデフォルトのALSAデバイスです。次の方法を使って、別のデバイスを指定します。

1. 変更を適用するユーザーの構成ファイルを選択して開きます。ほかのユーザーに適用される特定の設定ファイルを更新する方法については、「[設定ファイルを使ったReceiverのカスタマイズ](#)」を参照してください。
2. 次のオプションを追加して、必要に応じてセクションを作成します。

```
[ClientAudio]
```

```
AudioDevice = <device>
```

ここで<device>情報は、オペレーティングシステム上のALSA構成ファイルにあります。

注：この情報の場所は、すべてのLinuxオペレーティングシステムでの標準ではありません。この情報の場所について詳しくは、オペレーティングシステムドキュメントを参照してください。

### USBサポートの構成

USBサポート機能により、ユーザーが仮想デスクトップ上で作業しているときにさまざまな種類のUSBデバイスを使用できるようになります。ユーザーがコンピューターにUSBデバイスを接続すると、仮想デスクトップ内でそのデバイス进行操作できるようになります。この機能では、フラッシュドライブ、スマートフォン、PDA、プリンター、スキャナー、MP3プレーヤー、セキュリティデバイス、およびタブレットなどのUSBデバイスがサポートされます。

USBリダイレクトは、XenApp 7.6（以降）またはXenDesktopを必要とします。XenAppは、マストストレージデバイスのUSBリダイレクトをサポートせず、オーディオデバイスをサポートするには特殊な構成が必要です。詳しくは、XenApp 7.6のド

キュメントを参照してください。

ほとんどの場合で標準のオーディオまたはWebカメラのリダイレクトの方がより適しているとはいえ、Webカメラ、マイク、スピーカー、およびヘッドセットなどUSBデバイスのアイソクロナス機能は、一般的な高速LAN環境でサポートされます。

XenDesktopセッションでは次の種類のデバイスは直接サポートされるため、USBサポート機能は使用されません。

- キーボード
- マウス
- スマートカード
- ヘッドセット
- Webカメラ

注：特殊用途のUSBデバイス（Bloombergキーボードや3Dマウスなど）では、USBサポート機能が使用されるように構成できます。そのほかの特殊用途のUSBデバイスのポリシー規則の構成については、[CTX120292](#)を参照してください。

デフォルトでは、特定の種類のUSBデバイスがXenDesktopセッションで動作しないように設定されています。たとえば、内部USBでシステムボードに装着されたネットワークインターフェイスカードは、リモートで動作する仮想デスクトップでの使用には適しません。次の種類のUSBデバイスは、XenDesktopセッションでの使用をデフォルトでサポートしていません。

- Bluetoothドングル
- 統合ネットワークインターフェイスカード
- USBハブ

リモート操作可能なUSBデバイスのデフォルトの一覧を更新するには、\$ICAROOT/にあるusb.confファイルを変更します。詳しくは、「[リモートで実行できるUSBデバイスの一覧の更新](#)」を参照してください。

エンドポイント側のUSBデバイスを仮想デスクトップ内で使用できるようにするには、USBポリシー規則を有効にする必要があります。詳しくは、[XenDesktop](#)のドキュメントを参照してください。

## USBサポートのしくみ

ユーザーがエンドポイントにUSBデバイスを接続すると、USBポリシーが照合され、許可されているデバイスであることが認識されると、仮想デスクトップ上で使用可能になります。USBポリシーで拒否されるデバイスは、ローカルのデスクトップでのみ使用可能になります。

デスクトップアプライアンスモードを介してアクセスするデスクトップでは、ユーザーがUSBデバイスを接続すると自動的に仮想デスクトップで使用可能になります。USBドライブの制御と表示は、仮想デスクトップにより処理されます。

デスクトップアプライアンスモードが使用中でない限り、ユーザーがリダイレクトを実行するためユーザーデバイスに接続する時、セッションウィンドウにフォーカスがある必要があります。

## マストストレージデバイス

USBマストストレージデバイスがローカルデスクトップに接続されたままユーザーが仮想デスクトップを切断した場合、その仮想デスクトップに再接続してもマストストレージデバイスは接続されません。マストストレージデバイスが仮想デスクトップに接続されるようにするには、仮想デスクトップへの再接続後にマストストレージデバイスをいったん取り外してから再度接続する必要があります。

注：USBマストストレージデバイスのリモートサポートを拒否するように構成されているLinuxワークステーションにマストストレージデバイスを接続する場合、Receiverソフトウェアによりデバイスが受け入れられず、別のLinuxファイルブラウザーが得られます。そのためユーザーデバイス上では、事前にリムーバブルストレージの [メディアが挿入されたら参照する] 設定を無

効にしておくことをお勧めします。たとえばDebianベースのデバイスでは、Debianメニューバーで [システム] > [設定] > [リムーバブルデバイスとメディア] の順に選択し、[ストレージ] タブの [リムーバブルストレージ] で [メディアが挿入されたら参照する] チェックボックスをオフにします。

注: [クライアントUSBデバイスリダイレクト]サーバーポリシーを有効にすると、クライアントドライブマッピングが有効な場合でもマストレージデバイスは常にUSBデバイスとして送信されます。

## Webカメラ

デフォルトでは、HDX RealTime Webカメラビデオ圧縮機能によりWebカメラのパフォーマンスが最適化されます。ただし一部の環境では、ユーザーがUSBサポート機能を使ってWebカメラを接続しなければならない場合があります。この場合、管理者がHDX RealTime Webカメラビデオ圧縮を無効にする必要があります。詳しくは、「[HDX RealTime Webカメラビデオ圧縮の構成](#)」を参照してください。

## デフォルトで許可されるUSBクラス

次のUSBデバイスのクラスは、デフォルトのUSBポリシー規則により許可されます。

### オーディオ (クラス01)

マイク、スピーカー、ヘッドセット、およびMIDIコントローラーがあります。

### 物理的インターフェイス (クラス05)

このデバイスはHIDに似ていますが、一般的にはリアルタイムの入力またはフィードバックを提供し、フォースフィードバックジョイスティック、モーションプラットフォーム、およびフォースフィードバックエクソスケルトンなどがあります。

### 静止画 (クラス06)

このクラスのデバイスとして、デジタルカメラおよびスキャナーがあります。ほとんどのデジタルカメラは、画像転送プロトコル (PTP) またはメディア転送プロトコル (MTP) を使ってコンピューターやほかの周辺機器にイメージを転送する静止画クラスをサポートします。また、デジタルカメラはマストレージデバイスとして機能する場合もあり、カメラ自体のメニューを使っていずれかのクラスを使用するように構成できます。

カメラがマストレージデバイスとして機能する場合はクライアントドライブマッピングが使用され、USBサポートは必要ありません。

### プリンター (クラス07)

一部のプリンターではベンダー固有のプロトコル (クラスff) が使用されますが、一般的にはこのクラスにほとんどのプリンターが含まれます。マルチ機能プリンターの場合は、USBハブが内蔵されていたり、混合デバイスであったりする場合があります。いずれの場合も、印刷機能では一般的にプリンタークラスが使用され、スキャナーやFAX機能では静止画などの別のクラスが使用されます。

プリンターは通常、USBサポートなしで適切に動作します。

### マストレージデバイス (クラス08)

最も一般的なマストレージデバイス (大容量記憶装置) として、USBフラッシュドライブがあります。そのほかには、USB接続のハードドライブ、CD/DVDドライブ、およびSD/MMCカードリーダーがあります。マストレージインターフェイスを示す、メディアプレーヤー、デジタルカメラ、および携帯電話など、内部ストレージを持つさまざまな種類のデバイスがあります。既知のサブクラスには次のものが含まれます。

- 01 制限付きフラッシュデバイス

- 02 一般的なCD/DVDデバイス (ATAPI/MMC-2)
- 03 一般的なテープデバイス (QIC-157)
- 04 一般的なフロッピーディスクドライブ (UFI)
- 05 一般的なフロッピーディスクドライブ (SFF-8070i)
- 06 ほとんどのマストレージデバイスはこのSCSIのバリエーションを使用します

マストレージデバイスには、クライアントドライブマッピングを介して頻繁にアクセスすることができ、USBサポートは必要ありません。

**重要：** ウィルスプログラムの中には、あらゆる種類のマストレージデバイスを媒体にして活発に増殖するものがあります。クライアントドライブマッピングまたはUSBサポートのいずれかを介してマストレージデバイスの使用を許可する必要があるかどうか、注意深く考慮してください。このリスクを減らすため、クライアントドライブマッピングによりファイルが実行されるのを防ぐようにサーバーが構成されている可能性があります。

#### コンテンツセキュリティ (クラス0d)

通常、ライセンスまたはデジタル権利の管理のためのコンテンツ保護を実行します。このクラスのデバイスとして、donglesがあります。

#### パーソナルヘルスケア (クラス0f)

このデバイスには、血圧センサー、心拍数モニター、万歩計、薬剤モニター、肺活量計などの個人用健康器具があります。

#### アプリケーションおよびベンダー固有 (クラスfeおよびff)

多くのデバイスがベンダー独自のプロトコルまたはUSBコンソーシアムで標準化されていないプロトコルを使用しており、これらは通常はベンダー固有 (クラスff) として分類されます。

## デフォルトで拒否されるUSBデバイスのクラス

次のUSBデバイスのクラスは、デフォルトのUSBポリシー規則により拒否されます。

#### 通信およびCDCコントロール (クラス02および0a)

モデム、ISDNアダプター、ネットワークアダプター、一部の電話およびFAX機器があります。

仮想デスクトップ自体への接続にこれらのデバイスのいずれかが使用される場合があるため、デフォルトのUSBポリシーではこれらのデバイスのリモートでの実行は許可されていません。

#### ヒューマンインターフェイスデバイス (クラス03)

さまざまな種類の入出力デバイスを含みます。一般的なヒューマンインターフェイスデバイス (HID) として、キーボード、マウス、ポインティングデバイス、グラフィックタブレット、センサー、およびゲームのコントローラー、ボタン、およびコントロール機能などがあります。

Subclass 01は起動インターフェイスクラスと呼ばれ、キーボードおよびマウスで使用されます。

デフォルトのUSBポリシーはUSBキーボード (クラス03、サブクラス01、プロトコル1) またはUSBマウス (クラス03、サブクラス01、プロトコル2) を許可しません。これは、ほとんどのキーボードおよびマウスはUSBサポートなしでも適切に処理され、一般に仮想デスクトップ内だけでなくローカルでも使用されるためです。

#### USBハブ (クラス09)

USBハブにより、追加のデバイスをローカルコンピューターに接続できます。これらのデバイスにリモートでアクセスする

要はありません。

### スマートカード (クラス0b)

スマートカードリーダーには、非接触式および接触式のスマートカードリーダーがあり、また埋め込みスマートカード同等チップがあるUSBトークンもあります。

スマートカードリーダーは、スマートカードサポート機能によりアクセスできるため、USBサポートは必要ありません。

### ビデオ (クラス0e)

このクラスのデバイスとして、ビデオ、Webカメラ、デジタルカムコーダー、アナログビデオ変換機、一部のテレビチューナー、およびビデオストリーミングをサポートする一部のデジタルカメラなど、ビデオ関連の機器があります。

デフォルトでは、HDX RealTime Webカメラビデオ圧縮機能によりWebカメラのパフォーマンスが最適化されます。

### ワイヤレスコントローラー (クラスe0)

このクラスのデバイスとして、ウルトラワイドバンドコントローラーやBluetoothなど、さまざまなワイヤレスコントローラーがあります。

これらのデバイスの中には、重要なネットワークアクセスを提供していたり、Bluetoothキーボードやマウスなどの基幹周辺装置を接続していたりするものがあります。

デフォルトのUSBポリシーはこれらのデバイスを許可していません。ただし、USBサポートを使ったアクセスに適したデバイスもあります。

## リモート操作で使用できるUSBデバイスの一覧の変更

ユーザーデバイスの\$ICAROOT/にあるusb.confファイルに含まれるデフォルト規則の一覧を変更して、デスクトップへリモートで実行できるUSBデバイスの範囲を更新できます。

新しいポリシー規則を追加して一覧を更新し、デフォルト範囲に含まれないUSBデバイスを許可または拒否します。この方法により管理者により作成された規則は、どのデバイスがサーバーに提供されるかを制御します。次にサーバー上で規則が、どのデバイスが受け付けられるかを制御します。

デバイスのリモートでの実行を許可しないためのデフォルトポリシー構成は次のとおりです。

```
DENY: class=09 # Hub devices
```

```
DENY: class=03 subclass=01 # HID Boot device (keyboards and mice)
```

```
DENY: class=0b # Smartcard
```

```
DENY: class=e0 # Wireless Controllers
```

```
DENY: class=02 # Communications and CDC Control
```

```
DENY: class=03 # UVC (webcam)
```

```
DENY: class=0a # CDC Data
```

```
ALLOW: # Ultimate fallback: allow everything else
```

## USBポリシー規則の作成

ヒント：新しいポリシー規則を作成する場合、USB Webサイト (<http://www.usb.org/>) でUSBクラスコードを参照してください。

ユーザーデバイス上のusb.confファイルで指定するポリシー規則は、{ALLOW:|DENY:}に次のタグの値をベースとした式セットが付いた形式にします。

タグ	説明
VID	デバイス記述子のベンダーID
REL	デバイス記述子のリリースID
PID	デバイス記述子の製品ID
Class	デバイス記述子またはインターフェイス記述子のクラス
SubClass	デバイス記述子またはインターフェイス記述子のサブクラス
Prot	デバイス記述子またはインターフェイス記述子のプロトコル

新しいポリシー規則を作成する場合、以下の点に注意してください。

- 大文字と小文字は区別されません。
- 規則の最後に、"#"で始まる任意のコメントを追加できます。区切り文字は不要で、コメントは無視されます。
- 空白行およびコメントのみの行は無視されます。
- 区切りとして使用されるスペースは無視されますが、番号または識別子の間にスペースを入れることはできません。たとえば、Deny: Class=08 SubClass=05は有効な規則ですが、Deny: Class=0 8 Sub Class=05は無効です。
- タグは合致を意味する演算子の"="を使用する必要があります。たとえば、VID=1230とします。

## 例

次の例は、ユーザーデバイス上のusb.confファイルのセクションを示しています。これらの規則を実装するには、サーバーに同じ規則のセットがある必要があります。

```
ALLOW: VID=1230 PID=0007 # ANOther Industries, ANOther Flash Drive
```

```
DENY: Class=08 SubClass=05 # Mass Storage Devices
```

```
Class=0D # All Security Devices
```

## スタートアップモードの構成

デスクトップアプライアンスモードを使って、仮想デスクトップを開始したときに既に接続されているクライアント側のUSBデバイスを有効にしたり無効にしたりできます。これを行うには、各ユーザーデバイスで\$ICAROOT/config/module.iniファイルを開き、DesktopApplianceMode = Boolean を以下のように設定します。

TRUE	開始時に接続されているUSBデバイスが使用可能になります。サーバー（レジストリエントリ）またはユーザーデバイス（ポリシールール構成ファイル）のUSBポリシーでデバイスが禁止されていない場合のみ。
------	---

FALSE	USBデバイスは使用可能になりません。
-------	---------------------

## 狭帯域幅接続でのパフォーマンスの向上

サーバー上ではXenAppまたはXenDesktop、ユーザーデバイスではReceiverのそれぞれ最新バージョンを使用することを推奨します。

帯域幅の狭い接続を使用する場合は、Receiverの構成や使い方を変えてパフォーマンスを向上させることができます。

- **Receiverの接続構成** - Receiverの接続構成を変更することで、ICAで消費される帯域幅を減らしてパフォーマンスを改善できます。
- **Receiverの使用方法** - Receiverの使用方法を変更することで、高いパフォーマンスが求められる接続での消費帯域幅を抑えることができます。
- **UDPオーディオの有効化** - この機能を有効にすると、ネットワークトラフィック負荷の高いVoIP (Voice over IP) 接続での遅延レベルが安定します。
- **最新バージョンのXenAppおよびReceiver for Linuxの使用** - Citrix製品では、パフォーマンスを向上して機能を拡張するためのバージョンアップが常に行われています。また、多くのパフォーマンス機能を使用するには、最新のReceiverおよびサーバーソフトウェアが必要である場合もあります。

## 接続の構成

デバイスのプロセッサの処理能力や接続に使用する帯域幅が限られている場合は、使用する機能とパフォーマンスのバランスを考慮する必要があります。ユーザーおよび管理者は、パフォーマンスを低下させずに多くの機能を利用できるように、構成を変更することができます。サーバーまたはユーザーデバイスで次の変更を行うと、接続に必要な帯域幅を減らしてパフォーマンスを向上させることができます。

- **SpeedScreenの有効化** - SpeedScreenを有効にすると、遅延時間の長いネットワーク接続でも、ユーザーの入力やマウスのクリックに対する反応時間が短くなります。この構成は、サーバー上でSpeedScreen管理ツールを使用して行います。Receiverにおいてデフォルトでは、これはキーボード操作に対しては無効になっており、遅延時間の長いネットワーク接続におけるマウス操作に対してのみ有効です。詳しくは、『  
— Citrix Receiver for Linux OEM's Reference Guide  
』を参照してください。
- **データ圧縮の有効化** - データを圧縮すると、接続を介して転送されるデータ量が減少します。これにはデータの圧縮と展開を行うためのプロセッサリソースが必要になりますが、低帯域幅接続でのパフォーマンスを向上させることができます。この機能を有効にするには、Citrixポリシーの [音質] および [イメージ圧縮] 設定を使用します。
- **ウィンドウサイズの縮小** - ウィンドウサイズを必要最小限に抑えます。XenApp Servicesサイトで、[セッションオプション] を設定します。
- **表示色数の変更** - 表示色数を256色に変更します。XenApp Servicesサイトで、[セッションオプション] を設定します。
- **音質の変更** - サウンドのサポート機能を使用する場合は、Citrixポリシーの [音質] 設定で音質を下げます。

## UDPオーディオの有効化

UDPオーディオ機能を有効にすると、インターネット接続を介した通話品質が向上します。この機能では、TCP (Transmission Control Protocol) の代わりにUDP (User Datagram Protocol) が使用されます。

以下の点に注意してください。

- 暗号化されたセッション (TLSまたはSecureICAを使用するセッション) では、UDPオーディオを使用できません。このようなセッションでは、TCP上でオーディオデータが転送されます。
- ICAチャンネルの優先度により、UDPオーディオの動作が異なります。

1. module.iniファイルのClientAudioセクションで、以下のオプションを設定します。
  - EnableUDPAudioにTrueを指定します。デフォルトではFalseが設定されており、UDPオーディオが無効になります。
  - UDPAudioPortLowおよびUDPAudioPortHighに、UDPオーディオで使用されるポート番号の最小値および最大値を指定します。デフォルトでは、ポート16500~16509が使用されます。
2. 中レベルの音質が適用されるように、クライアント側およびサーバー側のオーディオ設定を以下のように構成します。

		クライアント側の音質レベル		
		高	中	低
サーバー側の音質レベル	高	高	中	低
	中	中	中	低
	低	低	低	低

UDPオーディオを有効にしても、中レベルの音質が適用されない場合はTCPが使用されます。

## Receiverの使用方法の変更

ICA技術は高度に最適化されているため、通常、処理能力の高いCPUを搭載したクライアントデバイスや広い帯域幅を必要としません。ただし、接続の帯域幅が非常に狭い接続では、適切なパフォーマンスを得るために、次のことを考慮してください。

- クライアント側ドライブ上のサイズの大きいファイルにはアクセスしない。クライアントドライブマッピングを使ってファイルにアクセスすると、サーバーとの接続でそのファイルのデータが転送されることになります。遅い接続では、大きなファイルを転送するのに時間がかかることがあります。
- クライアント側のローカルプリンターで大きな文書を印刷しない。クライアント側のローカルプリンターで文書を印刷すると、サーバーとの接続でそのファイルのデータが転送されることになります。遅い接続では、大きなファイルを転送するのに時間がかかることがあります。
- マルチメディアコンテンツを再生しない。マルチメディアファイルを再生するには、広い帯域幅が必要です。そのため、パフォーマンスが低下する可能性があります。

### マルチメディアパフォーマンスの向上

Receiverには、メディアリッチな今日のユーザー環境に高品位なユーザーエクスペリエンスを提供する幅広い技術セットが含まれています。以下の機能により、ホストされるアプリケーションやデスクトップでのユーザーエクスペリエンスが向上します。

- HDX MediaStream Windows Mediaリダイレクト
- HDX MediaStream Flashリダイレクト
- HDX RealTime Webカメラビデオ圧縮
- H.264サポート

### HDX MediaStream Windows Mediaリダイレクトの構成

HDX MediaStream Windows Mediaリダイレクトを実行すると、Linuxユーザーデバイスでアクセスする仮想Windowsデスクトップでマルチメディア再生時の帯域幅が軽減されます。HDX MediaStream Windows Mediaリダイレクトは、サーバーではなくユーザーデバイスでメディアランタイムファイルを再生し、マルチメディアファイルの再生に必要な帯域幅を減少させ

メカニズムです。

HDX MediaStream Windows Mediaリダイレクトは、仮想Windowsデスクトップで実行中のWindows Media Playerおよび互換プレーヤーのパフォーマンスを向上させます。次の形式を含む、さまざまなファイル形式をサポートしています。

- Advanced Systems Format (ASF)
- Motion Picture Experts Group (MPEG)
- Audio-Video Interleaved (AVI)
- MPEG Audio Layer-3 (MP3)
- WAVサウンドファイル

Receiverには、Windows用のメディア形式であるGUIDをGStreamer用のMIMEタイプに変換するためのテキストベースの変換テーブルであるMediaStreamingConfig.tblが含まれています。この変換テーブルは、以下の目的で編集できます。

- 不明またはサポートされないメディアフィルター/ファイル形式を変換テーブルに追加する。
- 問題が生じるGUIDをブラックリストに追加して、強制的にサーバー側でレンダリングされるようにする。
- GStreamerパラメーターの変更により問題のある形式をトラブルシューティングできるようにするため、追加のパラメーターを既存のMIME文字列に追加する。
- ユーザーデバイス上のGStreamerによりサポートされているメディアファイルの種類に応じて、カスタムの構成を管理および展開する。

クライアント側でのコンテンツ取得機能を使用すると、http://、mms://、およびrtsp://形式のURLからのストリーム配信メディアを、Citrixサーバーを介さずにユーザーデバイスで直接取得できます。サーバーは、ユーザーデバイスをメディアに接続して、再生、一時停止、停止、音量、シークなどの制御コマンドを送信するだけで、メディアデータの処理は行いません。この機能を使用するには、ユーザーデバイス上に高度なマルチメディアGStreamerライブラリをインストールする必要があります。

## Windows Mediaリダイレクトを実装するには

1. オープンソースのマルチメディアフレームワークであるGStreamer 0.10を各ユーザーデバイス上にインストールします。通常、Receiverよりも前にGStreamerをインストールします。  
ほとんどのLinuxディストリビューションにはGStreamerが含まれています。または、<http://gstreamer.freedesktop.org>からGStreamerをダウンロードできます。
2. クライアント側でのコンテンツ取得機能を有効にするには、再生するメディアのファイルタイプに対応するGStreamerのプロトコルソースプラグインをインストールします。このプラグインのインストールおよび動作を確認するには、gst-launchユーティリティを使用します。このプラグインが正しくインストールされている場合、gst-launchでURLのマルチメディアを再生できます。たとえば、次のコマンドを実行します。gst-launch-0.10 playbin2 uri=http://example-source/file.wmv ビデオが正しく再生されるかチェックします。
3. Receiverをインストールするときに、GStreamerオプションを選択します。

クライアント側でのコンテンツ取得機能を使用する場合は、次のことに注意してください。

- この機能は、デフォルトで有効になります。無効にするには、All-Regions.iniファイルのMultimediaセクションにあるSpeedScreenMMACSFEnabledオプションを使用します。ここでFalseを指定すると、Windows Mediaリダイレクト機能が使用されます。
- デフォルトでは、すべてのMediaStream機能でGStreamerのplaybin2プロトコルが使用されます。従来のplaybinプロトコルが使用されるようにするには、All-Regions.iniファイルのMultimediaセクションにあるSpeedScreenMMAEnablePlaybinオプションを使用します。ただし、クライアント側でのコンテンツ取得機能では常にplaybin2プロトコルが使用されます。
- Receiverでは、.asxや.nscなどのストリーム構成情報ファイルや再生リストファイルを認識できません。可能な場合は、これらのファイルを参照しない標準的なURLをユーザーが指定する必要があります。URLが有効かどうかは、gst-launchを使用して確認できます。

## HDX MediaStream Flashリダイレクトの構成

HDX MediaStream Flashリダイレクトにより、Adobe Flashコンテンツがユーザーデバイス上でローカルに再生され、帯域幅要件を増やすことなく高品位な音声やビデオの再生機能が提供されます。

1. この機能に必要な要件をユーザーデバイスが満たしていることを確認します。詳しくは、[必要なシステム](#)を参照してください。
2. wfclient.iniの[WFClient]セクション（特定ユーザーのすべての接続に適用する場合）またはAll\_Regions.iniの[Client Engine\Application Launching]セクション（環境内のすべてのユーザーに適用する場合）に、以下のパラメーターを追加します。

- **HDXFlashUseFlashRemoting=Ask | Never | Always**

ユーザーデバイス上でHDX MediaStream for Flashを有効にします。デフォルトでは、**Never**に設定されています。これにより、FlashコンテンツのWebページに接続したときに、そのコンテンツを最適化するかどうかを確認するダイアログボックスが開きます。

- **HDXFlashEnableServerSideContent Fetching=Disabled | Enabled**

サーバー側でのコンテンツ取得機能を有効または無効にします。デフォルトでは、**Disabled**に設定されています。

- **HDXFlashUseServerHttpCookie=Disabled | Enabled**

HTTP Cookieのリダイレクトを有効または無効にします。デフォルトでは、**Disabled**に設定されています。

- **HDXFlashEnableClientSideCaching=Disabled | Enabled**

Receiverにより取得されたWebコンテンツのクライアント側キャッシュを有効または無効にします。デフォルトでは、**Enabled**に設定されています。

- **HDXFlashClient CacheSize= [25-250]**

クライアント側でのキャッシュのサイズを、MB単位で定義します。この値は、25~250MBの間で定義できます。サイズが制限値に到達すると、キャッシュ内の既存のコンテンツが削除され、新しいコンテンツが保存されます。デフォルトでは、**100**に設定されています。

- **HDXFlashServerSideContent CacheType=Persistent | Temporary | NoCaching**

サーバー側でのコンテンツ取得機能により取得されたコンテンツのキャッシュの種類を定義します。デフォルトでは、**Persistent**に設定されています。

注：このパラメーターは、**HDXFlashEnableServerSideContent Fetching**を**Enabled**に設定した場合にのみ必要です。

3. Flashリダイレクトはデフォルトで無効になっています。/config/module.iniファイルで、FlashV2=OffをFlashV2=Onに変更して、この機能を有効にします。

## HDX RealTime Webカメラビデオ圧縮の構成

HDX RealTime機能のWebカメラビデオ圧縮オプションを使用すると、ビデオ会議で消費される帯域幅を効率化できます。これにより、GoToMeeting HD Faces、Skype for businessなどのアプリケーションを使用するときに最適なパフォーマンスが提供されます。

1. この機能に必要な要件をユーザーデバイスが満たしていることを確認します。
2. マルチメディア仮想チャンネルを有効にする必要があります。これを実行するには、SICAROOT/configディレクトリにあるmodule.ini構成ファイルを開き、[ICA3.0]セクションのMultiMediaを"On"に設定します。
3. オーディオ入力を有効にするには、[環境設定] ダイアログボックスの[マイクとWebカメラ] ページで、[マイクとWebカメラを使用する] をクリックします。

## HDX RealTime Webカメラビデオ圧縮の無効化

デフォルトでは、HDX RealTime Webカメラビデオ圧縮機能によりWebカメラのパフォーマンスが最適化されます。ただし一部の環境では、ユーザーがUSBサポート機能を使ってWebカメラを接続しなければならない場合があります。これを実行するには、次の手順を実行する必要があります：

- HDX RealTime Webカメラビデオ圧縮を無効にする
- WebカメラのUSBサポートを有効にする

1. 次のパラメーターを適切なINIファイルの[WFClient]セクションに追加する：

```
HDXWebCamEnabled=Off
```

詳しくは、「[構成ファイルを使ったReceiverのカスタマイズ](#)」を参照してください。

2. usb.confファイルを開きます。通常このファイルは、\$ICAROOT/usb.confにあります。

3. 次の行を削除するか、コメントアウトします。

```
DENY: class=0e # UVC (default via HDX RealTime Webcam Video Compression)
```

4. ファイルを保存して閉じます。

## H.264サポートの構成

Receiverでは、XenDesktop 7で配信されるHDX 3D Proグラフィックを含むH.264グラフィックがサポートされます。この機能では、デフォルトで有効になっている深圧縮コーデックが使用されます。これにより、専門的なグラフィック処理アプリケーションをWANネットワークを介して使用する場合でも、既存のJPEGフォーマットよりも高いパフォーマンスが提供されます。

この機能を無効にする（つまりグラフィックをJPEGコーデックで処理する）には、このトピックの手順に従ってください。深圧縮コーデックを有効にしたまま、テキストトラッキングを無効にすることもできます。グラフィックに含まれるテキストが多くないまたは重要でない場合は、テキストトラッキングを無効にすることにより、複雑なグラフィック処理時のCPU負荷を軽減できます。

**重要：**この機能を構成する場合は、XenDesktopのポリシーの[表示品質]設定で無損失品質を指定しないでください。無損失品質を指定するとサーバー側のH.264エンコーディングが無効になり、Receiverでこの機能が動作しなくなります。

**深圧縮コーデックのサポートを無効にするには：**

wfclient.iniで、H264EnabledにFalseを設定します。これにより、テキストトラッキングも無効になります。

**テキストトラッキングのみを無効にするには**

深圧縮コーデックのサポートを有効にしたまま、wfclient.iniでtextTrackingEnabledにFalseを設定します。

## 画面タイルのパフォーマンスの最適化

Direct-to-Screenビットマップデコード、バッチタイルデコード、およびXSyncの待機機能を使用すると、JPEGエンコードの画面タイルの処理パフォーマンスを最適化できます。

1. JPEGライブラリがこれらの機能をサポートすることを確認します。
2. wfclient.iniの[Thinwire3.0]セクションで、DirectDecodeおよびBatchDecodeにTrueを指定します。

注：バッチタイルデコード機能を有効にすると、XSyncの待機機能が自動的に有効になります。

# 操作性の向上

Jan 23, 2017

Receiverには、ユーザーエクスペリエンスを向上させるための以下の機能が用意されています。

- [基本設定の設定](#)
- [ClearTypeフォントスムージングの構成](#)
- [ユーザーフォルダーのリダイレクトの構成](#)
- [サーバーからクライアントへのコンテンツリダイレクトのセットアップ](#)
- [キーボードの制御](#)
- [xcaptureの使用](#)
- [ユーザーの自動再接続](#)
- [セッション画面の保持](#)
- [相対マウス](#)

## 基本設定の設定

各種設定を行うには、Citrix Receiverメニューの [環境設定] を選択します。ここでは、デスクトップの表示モード、セッションの自動再接続、およびローカルのファイルやデバイスへのアクセスについて設定します。

## アカウントを管理するには

デスクトップやアプリケーションにアクセスするには、XenDesktopまたはXenAppのアカウントが必要です。ヘルプデスク担当者により、Citrix Receiver上でアカウントを追加したり、既存のアカウントのNetScaler GatewayまたはAccess Gatewayサーバーの指定を変更したりすることが指示される場合があります。また、Citrix Receiverからアカウントを削除することもできます。

1. [環境設定] ダイアログボックスの [アカウント] ページで、次のいずれかを実行します。
  - アカウントを追加するには、[追加] をクリックします。ヘルプデスク担当者により、新しいアカウントを作成するためのプロビジョニングファイルが提供される場合もあります。
  - アカウントで接続するストアの詳細（デフォルトのゲートウェイなど）を変更するには、[編集] をクリックします。
  - アカウントを一覧から削除するには、[削除] をクリックします。
2. 画面の指示に従って操作します。サーバーへの認証情報が必要な場合があります。

## デスクトップの表示モードを変更するには

この機能は、Citrix XenApp for UNIXのセッションでは使用できません。

デスクトップを全画面で表示（全画面モード。デフォルト）したり、ウィンドウ内に表示（ウィンドウモード）したりできます。

- [環境設定] ダイアログボックスの [全般] ページを開き、[デスクトップの表示] オプションを使用して表示モードを選択します。

Receiver for Linuxの新しい **[You can enable Desktop Viewer]** ツールバー機能で、ここで述べた構成で指定された元の設定からリモートセッションのウィンドウ構成を動的に変更できるようになりました。

## Desktop Viewer

企業組織にはそれぞれ異なるニーズがあります。ユーザーが仮想デスクトップにアクセスする方法の要件は、ユーザーに

よって、そして企業ニーズが展開するにつれて変化する可能性があります。ユーザーが仮想デスクトップに接続したり接続を構成したりするときの手順は、管理者によるReceiver for Linuxセットアップ方法によって異なります。

ユーザーが仮想デスクトップを操作する必要がある場合は、Desktop Viewerを使用します。ユーザーの仮想デスクトップは公開仮想デスクトップにすることができ、または共有デスクトップや専用デスクトップにもすることができます。このアクセスシナリオでは、Desktop Viewerツールバー機能により、モニターを横断したマルチモニターサポートなど、ウィンドウモードと全画面モードのセッションの切り替えることができます。ユーザーは、同じユーザーデバイス上で複数のXenDesktopコネクションを確立して、デスクトップセッションを切り替え、複数のデスクトップを使用できます。すべてのデスクトップセッションを最小化し、Ctrl+Alt+Delシーケンスを送信し、接続を切断し、セッションをログオフするボタンが提供されるため、簡単にユーザーのセッションを管理できます。

Desktop Viewerのユーザー補助機能として、Ctrl+ Alt + Breakキーを押すと、ポップアップウィンドウでDesktop Viewerツールバーが開きます。

Desktop Viewerを有効/無効にしたり、ユーザー補助機能のキーシーケンスを変更するための詳細設定の入力については、Linux OEMガイドを参照してください。

## セッションへの自動再接続を有効にするには

Citrix Receiverには、ネットワークインフラストラクチャの問題があるなどの理由で切断されたデスクトップやアプリケーションのセッションに、自動的に再接続するための機能が用意されています。

- [環境設定] ダイアログボックスの [全般] ページを開き、[アプリやデスクトップへの再接続] でオプションを選択します。

## ローカルファイルへのアクセスを制御するには

仮想デスクトップやアプリケーションからローカルコンピューター上のファイルにアクセスする場合は、そのアクセス方法を制御することができます。

1. [環境設定] ダイアログボックスの [ファイルアクセス] ページを開き、マップするドライブを選択してから適切なオプションを選択します。
  - 読み取り/書き込み：デスクトップやアプリケーションでのローカルファイルの読み取りおよび書き込みを許可します。
  - 読み取りのみ：デスクトップやアプリケーションでのローカルファイルの読み取りのみを許可し、書き込みを禁止します。
  - アクセスなし：デスクトップやアプリケーションでのローカルファイルへのアクセスを禁止します。
  - 毎回確認する：デスクトップやアプリケーションでのローカルファイルにアクセスするときに、毎回確認メッセージを表示します。
2. ローカルファイルへのアクセスを許可するオプションを選択すると、ユーザーデバイス上の場所を参照するときの時間を節約できます。[追加] をクリックして場所を指定し、それに割り当てるドライブ文字を選択します。

## マイクまたはWebカメラをセットアップするには

仮想デスクトップやアプリケーションからローカルコンピューター上のマイクやWebカメラにアクセスする場合は、そのアクセス方法を制御できます。

[環境設定] ダイアログボックスの [マイクとWebカメラ] ページでは、次のオプションを選択できます。

- マイクとWebカメラを使用する：デスクトップやアプリケーションでのマイクやWebカメラの使用を許可します。
- マイクとWebカメラを使用しない：デスクトップやアプリケーションでのマイクやWebカメラの使用を禁止します。

## Flash Playerをセットアップするには

Flashコンテンツの表示方法を選択できます。通常、これらのコンテンツにはビデオ、アニメーション、およびアプリケーションが含まれ、Flash Playerを使って表示します。

[環境設定] ダイアログボックスの [Flash] ページでは、次のオプションを選択できます。

- コンテンツを最適化する：コンテンツの再生品質を向上させます。ただし、セキュリティが低下する可能性があります。
- 最適化しない：セキュリティを犠牲にすることなく、標準的な再生品質が提供されます。
- 毎回確認する：Flashコンテンツを表示するときに、毎回確認メッセージを表示します。

### ClearTypeフォントスムージングの構成

ClearTypeフォントスムージング（サブピクセルのフォントレンダリング）は、従来のフォントスムージングやアンチエイリアスに比べて表示フォントの質を向上させます。この機能を有効/無効にしたりスムージングの種類を指定したりするには、適切な構成ファイルの[WFClient]セクションで次の設定を編集します。

FontSmoothingType = <number>

<number>に以下のいずれかの値を設定します。

値	動作
0	デバイス側の設定が適用されます。デバイス側の設定は、FontSmoothingTypePrefで定義します。
1	スムージング処理なし
2	標準のスムージング
3	ClearType（水平サブピクセル）スムージング

標準スムージングまたはClearTypeスムージングを使用すると、Receiverで消費される帯域幅が増加することがあります。

重要：サーバー側の設定は、ICAファイルのFontSmoothingTypeで定義できます。この設定は、[WFClient]の設定よりも優先されます。FontSmoothingTypeが0の場合、[WFClient]の次の設定によりローカルの動作が決定されます。

FontSmoothingTypePref = <number>

<number>に以下のいずれかの値を設定します。

値	動作
0	スムージング処理なし
1	
2	標準のスムージング
3	ClearType（水平サブピクセル）スムージング（デフォルト）

### ユーザーフォルダーのリダイレクトの構成

この機能では、ユーザーごとに個別に設定される以下の2つのユーザーフォルダー（特殊フォルダー）が対象になります。

- ユーザーのデスクトップフォルダー
- ユーザーのドキュメントフォルダー（Windows XPではマイドキュメント）

ユーザーフォルダーのリダイレクト機能では、ユーザーデバイス上の特定の場所をユーザーフォルダーとして指定できます。これにより、サーバーの種類やファーム構成が異なってもこれらのフォルダーに一貫してアクセスできるようになります。たとえば、異なるサーバーファームのサーバーにログオンする必要があるモバイルユーザーには便利な機能です。常に同じサーバーファーム内のサーバーにログオンする静的な社内ワークステーションの場合、この機能はあまり必要ではありません。

## ユーザーフォルダーのリダイレクトを構成するには

2つの処理が必要です。まず、module.iniにエントリを作成してユーザーフォルダーのリダイレクトを設定します。次に、以下のように[WFClient]セクションにフォルダーの場所を指定します。

1. 次の文字列をmodule.ini（\$ICAROOT/config/module.iniなど）に追加します。  
[ClientDrive]

```
SFRAllowed = True
```

2. 次の文字列を[WFClient]セクション（\$HOME/.ICAClient/wfclient.iniなど）に追加します。  
DocumentsFolder = <documents>

```
DesktopFolder = <desktop>
```

ここで、documents やdesktop は、それぞれユーザーのDocumentsフォルダーおよびDesktopフォルダーとして使用するディレクトリのUNIXファイル名（フルパス）です。次に例を示します。

```
DesktopFolder = $HOME/.ICAClient/desktop
```

- \$HOMEなどの環境変数として、パスで任意のコンポーネントを指定できます。
- 両方のパラメーターの値を指定する必要があります。
- 指定するディレクトリは、クライアントデバイスマッピングを介して使用できる必要があります。このため、このディレクトリはマップされたクライアントデバイスのサブツリーにある必要があります。
- ドライブ文字として、Cまたはそれ以降を使用する必要があります。

## サーバーからクライアントへのコンテンツリダイレクトのセットアップ

公開アプリケーションで使用しているファイル内に埋め込まれている特定のURLを、ローカルのアプリケーションで開くように指定できます。たとえば、セッションで実行するMicrosoft OutlookでWebページへのリンクをクリックすると、そのWebページがユーザーデバイス上のWebブラウザで開きます。管理者は、この機能を使ってサーバーのリソースをより効率よく配分し、ユーザー側のパフォーマンスを向上させることができます。

次の種類のURLをクライアントにリダイレクトできます。

- HTTP（Hypertext Transfer Protocol）
- HTTPS（Secure Hypertext Transfer Protocol）
- RTSP（Real Player）
- RTSPU（Real Player）
- PNM（従来のReal Players）

Citrix Receiverに適切なアプリケーションがない場合、またはコンテンツに直接アクセスできない場合は、URLがサーバー上のアプリケーションで開きます。

サーバーからクライアントへのコンテンツリダイレクト機能は、サーバー側で構成します。Citrix Receiverでは、RealPlayerとWebブラウザ（Firefox、Mozilla、またはNetscapeの内の最低1つ）がUNIXパスに指定されている場合は、この機能がデフォルトで有効になります。

## 注意

RealPlayer for Linuxについて詳しくは、<http://www.real.com/resources/unix/>を参照してください。

## RealPlayerとWebブラウザがパスにない場合に、サーバーからクライアントへのコンテンツリダイレクト機能を有効にするには

1. 構成ファイルwfclient.iniを開きます。
2. [Browser]セクションで、次の設定を変更します。

Path=path

Command=command

ここで<path>は、Webブラウザの実行ファイルのディレクトリです。また、<command>はリダイレクトされるURLを処理する実行ファイルの名前で、サーバーから送信されるURLに追加されます。次に例を示します。

```
SICAROOT/nslaunch netscape,firefox,mozilla
```

このコマンドにより、以下が実行されます。

- 既存のWebブラウザウィンドウにURLを渡すnslaunchユーティリティが起動します。
- リストで指定された各Webブラウザを順番に試行して、コンテンツを表示します。

3. [Player]セクションで、次の設定を変更します。

Path=path

Command=command

ここで<path>は、RealPlayerの実行ファイルのディレクトリです。また、<command>はリダイレクトされるマルチメディアURLを処理する実行ファイルの名前で、サーバーから送信されるURLに追加されます。

4. ファイルを保存して閉じます。

## 注意

どちらのPath設定においても、WebブラウザおよびRealPlay実行ファイルがあるディレクトリだけを指定する必要があります。実行ファイルのフルパスは必要ありません。たとえば、[Browser]セクションではPathの値は/usr/X11R6/bin/netscapeではなく、/usr/X11R6/binとなります。また、複数のディレクトリ名をコロンで区切って指定できます。この値を指定しない場合、SPAT Hが使用されます。

## Receiverで、サーバーからクライアントへのコンテンツリダイレクト機能を無効

## にするには

1. 構成ファイルmodule.iniを開きます。
2. CREnabledの設定をOffに変更します。
3. ファイルを保存して閉じます。

### キーボードの制御

Ctrl+Alt+Delキーを送信するためのキーを設定するには：

1. Ctrl+Alt+Delキー操作を送信するために使用するキーの組み合わせを決定します。
2. 適切な構成ファイルを開き、[WFClient]セクションのUseCtrlAltEndで、以下の値を設定します。
  - Trueを指定すると、Ctrl+Alt+Endキーを押すことでリモートのデスクトップにCtrl+Alt+Delキー操作が送信されます。
  - False (デフォルト) を指定すると、Ctrl+Alt+Enterキーを押すことでリモートのデスクトップにCtrl+Alt+Delキー操作が送信されます。

### xcaptureの使用

Citrix Receiverのパッケージには、サーバーのクリップボードと、Xデスクトップ上のICCCMに準拠していないX Windowアプリケーション間で画像をコピーおよび貼り付けできる、xcaptureユーティリティが付属しています。xcaptureを使って、次の操作を実行できます。

- ダイアログボックスや画面領域をキャプチャし、コネクションウィンドウ内で実行中のアプリケーションと、ユーザーデバイスデスクトップ (ICCCMに準拠していないX Windowアプリケーションを含む) 間でコピーする。
- コネクションウィンドウと、グラフィックを編集するX Windowアプリケーションであるxmagまたはxv間で、画像をコピーする。

## コマンドラインからxcaptureを起動するには

コマンドプロンプトで、「/opt/Citrix/ICAClient/util/xcapture」と入力して、Enterを押します（ここで、/opt/Citrix/ICAClientはReceiverをインストールしたディレクトリです）。

## ユーザーデバイスデスクトップからコピーするには

1. [xcapture] ダイアログボックスで、[画面から] をクリックします。カーソルが十字型に変わります。
2. 次のいずれかを選択します。
  - ウィンドウの選択。コピーするウィンドウの上にカーソルを移動し、マウスの中央ボタンをクリックします。
  - 領域の選択。マウスの左ボタンを押したままカーソルをドラッグして、コピーする領域を選択します。
  - 選択の取り消し。マウスの右ボタンをクリックします。ドラッグしているときに中央ボタンまたは左ボタンを押したままマウスの右ボタンをクリックすると、選択が解除されます。
3. [xcapture] ダイアログボックスで、[ICAへ] をクリックします。ボタンの色が変わり、情報を処理していることが示されます。
4. 転送が完了したら、コネクションウィンドウから起動したアプリケーションで適切なコマンドを使用して、情報を貼り付けます。

## xvから、ICAセッション内のアプリケーションにコピーするには

1. xvで情報をコピーします。
2. [xcapture] ダイアログボックスで、[xvから]、[ICAへ] の順にクリックします。ボタンの色が変わり、情報を処理していることが示されます。

3. 転送が完了したら、コネクションウィンドウから起動したアプリケーションで適切なコマンドを使用して、情報を貼り付けます。

## ICAセッション内のアプリケーションからxvにコピーするには

1. ICAセッション内のアプリケーションで、情報をコピーします。
2. [xcapture] ダイアログボックスで、[ICAから]、[xvへ]の順にクリックします。ボタンの色が変わり、情報を処理していることが示されます。
3. 転送が完了したら、コピーした情報をxv内に貼り付けます。

### ユーザーの自動再接続

このトピックでは、HDX Broadcastのクライアント自動再接続機能について説明します。この機能は、HDX Broadcastセッション画面の保持機能と組み合わせて使用することをお勧めします。

ネットワークの状態が不安定であったり、待ち時間が非常に変わりやすかったりする場合、また、無線デバイスの伝送距離に制限がある場合に、セッションが切断されてしまうことがあります。HDX Broadcastのクライアント自動再接続機能では、ネットワークの問題などによって切断されたセッションをCitrix Receiverが検出すると、そのセッションに自動的に再接続します。

この機能がサーバーで有効になっていると、ユーザーは作業を続けるために手動で再接続する必要がありません。Citrix Receiverは、セッションへの接続に成功するかユーザーがキャンセルするまで設定した回数再接続を試行します。サーバー側でユーザー認証を要求する設定になっている場合、再接続時にユーザーの資格情報を入力するためのダイアログボックスが開きます。ユーザーがセッションからログオフしないでアプリケーションを終了してセッションを切断した場合、自動再接続は行われません。自動再接続は、ユーザーによる切断以外の理由で切断されたセッションに対してのみ行われます。

デフォルトでは、Citrix Receiverは30秒間待機してから切断したセッションに再接続を実行し、またこれを3回試行します。

AccessGatewayを介して接続すると、ACRは使用できません。ネットワークの障害から保護するため、AccessGateway上で構成するだけでなく、サーバーとクライアントの両方でもセッション画面の保持を有効にしておきます。

HDX Broadcastのクライアント自動再接続の構成手順については、XenAppおよびXenDesktopのドキュメントを参照してください。

### セッション画面の保持

このトピックは、デフォルトで有効になっているHDX Broadcastセッション画面の保持機能について説明します。

HDX Broadcastセッション画面の保持を有効にすると、公開アプリケーションへの接続が中断しても、ユーザーのセッション画面には作業中の画面が保持され、表示されたままになります。たとえば、ワイヤレス接続でのセッション中にトンネルや障害物などの影響で接続に障害が生じた場合、ユーザーデバイス上の画面表示が停止します。トンネルから出るなどして再接続されると、ユーザーはそのまま作業を続行できます。接続が切断している間、ユーザーのデータのすべて、キー入力、およびその他の操作は記憶され、アプリケーションは応答しないまま表示されます。接続が再度確立されると、これらすべての操作がアプリケーション内に反映されます。

クライアント自動再接続とセッション画面の保持が構成されている時、接続の問題がある場合にはセッションの画面保持が優先して実行されます。セッション画面の保持は既存のセッションへの接続を再度確立しようとします。接続の問題を検出するには最大で25秒かかることがあり、次に再接続するための構成可能な期間（デフォルトは180秒）を指定します。セッション画面の保持が再接続に失敗すると、クライアント自動再接続が再接続を試みます。

HDX Broadcastセッション画面の保持を有効にすると、セッションの通信に使用されるデフォルトのポートは、1494から2598に変更されます。

Citrix Receiverのユーザーには、サーバー側の設定が自動的に適用されます。詳しくは、XenAppおよびXenDesktopのドキュメントを参照してください。

## Important

HDX Broadcastセッション画面の保持では、サーバー上で（ポリシー設定を使って）Common Gateway Protocolを有効にする必要があります。Common Gateway Protocolを無効にすると、HDX Broadcastセッション画面の保持も無効になります。

## 相対マウス

相対マウスのサポートでは、マウスの絶対位置ではなく相対位置を読み取るオプションを提供します。この機能は、マウスが絶対位置ではなく相対位置の入力を必要とするアプリケーションに必要です。

## 注意

この機能は、XenAppまたはXenDesktop 7.8以降を実行しているセッションでのみ使用できます。デフォルトでは、無効になっています。

この機能を有効にするには、以下の手順に従います。

ファイル\$HOME/.ICAClient/wfclient.iniの[WFClient]セクションにエントリRelativeMouse=1を追加します。

これによって、機能が有効になります。有効にするまでは、無効になっています。

## ヒント

相対マウス機能を有効にする方法について詳しくは、セクション「[Alternative Relative Mouse values](#)」を参照してください。

この機能を有効にするには、以下の手順に従います。

「Ctrl/F12」と入力します。

機能が有効になった後、再度「Ctrl/F12」と入力し、クライアントでサーバーポインターの位置を同期します（サーバーおよびクライアントのポインター位置は、相対マウスを使用する場合には同期しません）。

この機能を無効にするには、以下の手順に従います。

「Ctrl-Shift/F12」と入力します。

この機能は、セッションウィンドウからフォーカスが失われた場合もオフになります。

## 相対マウスのその他の値

別の方法として、相対マウスで次の値も使用できます。

- RelativeMouse=2。機能を有効にし、セッションウィンドウがフォーカスを取り戻すとアクティブになります。
- RelativeMouse=3。機能を有効にし、アクティブにし、常時アクティブ状態に維持します。

キーボードコマンドを変更するには、以下のような設定を設定を追加します。

- `RelativemouseOnChar=F11`
- `RelativeMouseOnShift=Shift`
- `RelativemouseOffChar=F11`
- `RelativeMouseOffShift=Shift`

**RelativemouseOnChar**および**RelativemouseOff Char**でサポートされる値は、Citrix Receiverインストールツリーの `config/module.ini` ファイルの [Hotkey Keys] に一覧があります。**RelativeMouseOnShift**および**RelativeMouseOffShift**の値は、使用される識別子キーを設定し、[Hotkey Shift States] 見出しの下に一覧があります。

# セキュア

Jan 23, 2017

ここでは次のことについて説明します。

- [プロキシサーバー経由の接続](#)
- [Secure GatewayまたはCitrix SSL Relayの使用](#)
- [NetScaler Gateway経由の接続](#)

サーバーファームとCitrix Receiver間の通信を保護するには、以下の一連のセキュリティ技術を使用します。

- SOCKSプロキシサーバーまたはSecureプロキシサーバー（セキュリティプロキシサーバー、HTTPSプロキシサーバーまたはTLSトンネリングプロキシサーバーとも呼ばれます）。プロキシサーバーでネットワークから外部へのアクセスや外部からネットワークへのアクセスを制限して、Receiverとサーバー間の接続を制御できます。Receiverは、SOCKSプロトコルとSecureプロキシプロトコルをサポートしています。
- Secure GatewayまたはTransport Layer Security (TLS) プロトコルによるSSL Relayソリューション。TLS Version 1.0から1.2がサポートされます。
- ファイアウォール。ネットワークファイアウォールは、送信先アドレスとポート番号に基づいてパケットを通過させたりブロックしたりできます。サーバーの内部IPアドレスを外部インターネットアドレスにマップするネットワークファイアウォール（つまりNAT（Network Address Translation：ネットワークアドレス変換））を介してReceiverを使用する場合は、外部アドレスを構成します。

## プロキシサーバー経由の接続

プロキシサーバーは、ネットワーク内部から外部への、および外部から内部へのアクセスを制限して、Citrix ReceiverとCitrix XenAppやCitrix XenDesktopとの間の接続を制御するために使います。Citrix Receiverは、SOCKSプロトコル、Secure GatewayおよびCitrix SSL Relay、Secureプロキシプロトコル、およびWindows NTチャレンジ/レスポンス（NTLM）認証をサポートしています。

サポートされているプロキシの種類の一覧は、Trusted\_Regions.iniとUntrusted\_Regions.iniの内容によってAuto、None、およびWpadの種類に制限されます。SOCKS、Secure、またはScriptといった種類を使用する必要がある場合は、それらのファイルを編集して、許可された一覧へ追加の種類を追加します。

## 注意

確実に安全な接続を実行するには、TLSを有効にします。

## セキュアプロキシサーバー経由の接続

Secureプロキシプロトコルを使用する接続を構成して、Windows NTチャレンジ/レスポンス（NTLM）認証のサポートを有効にできます。このプロトコルを使用できる場合は、追加構成なしで実行時にこれが検出され使用されます。

## Important

NTLMをサポートするには、ユーザーデバイスにOpenSSLライブラリのlibcrypto.soをインストールする必要があります。このライブラリは、多くの場合Linuxディストリビューションに含まれていますが、新しいウィンドウが必要な場合、<http://www.openssl.org>からダウンロードすることもできます。

## Secure GatewayまたはCitrix SSL Relayの使用

ReceiverをSecure GatewayまたはCitrix SSL (Secure Sockets Layer) Relayと共に使うことができます。ReceiverはTLSプロトコルをサポートします。TLS (Transport Layer Security) は、標準化されたSSLプロトコルの最新版です。IETF (Internet Engineering TaskForce) が、SSLの公開標準規格の開発をNetscape Communications社から引き継いだときに、SSLという名前をTLSに変更しました。TLSは、サーバーの認証、データの暗号化、メッセージの整合性の確認を行って、データ通信を保護します。米国政府など、データ通信を保護するためにTLSの使用を必須としている組織もあります。このような組織では、さらにFIPS 140 (Federal Information Processing Standard) などのテスト済み暗号化基準の使用を義務付けられる場合があります。FIPS 140は、暗号化の情報処理規格です。

## Secure Gatewayを経由する接続

Secure Gatewayを通常モードまたはリレーモードのどちらかで使用して、Citrix Receiverとサーバーの間に保護された通信チャンネルを提供できます。Secure Gatewayを通常モードで使用し、ユーザーがWeb Interface経由で接続する場合は、Citrix Receiver側での構成は不要です。

Citrix ReceiverがSecure Gatewayサーバーと通信するときは、リモートのWeb Interfaceサーバーで構成されている設定が使用されます。Citrix Receiverをサポートするプロキシサーバー設定の構成については、[Web Interface](#)のドキュメントを参照してください。

Secure Gateway Proxyがセキュリティで保護されたネットワーク内のサーバーにインストールされている場合は、Secure Gateway Proxyをリレーモードで使用できます。詳しくは、[XenApp \(Secure Gateway\)](#) のドキュメントを参照してください。

ただし、リレーモードで使用する場合、Secure Gatewayサーバーはプロキシサーバーとして機能するため、Citrix Receiverで次の項目を構成する必要があります。

- Secure Gatewayサーバーの完全修飾ドメイン名。
- Secure Gatewayサーバーのポート番号。Secure Gateway, Version 2.xでは、リレーモードはサポートされていません。

完全修飾ドメイン名には、以下の3つの要素を順に指定する必要があります。

- Host name
- サブドメイン名
- 最上位ドメイン名

たとえば、my\_computer.my\_company.comは完全修飾ドメイン名です。ホスト名 (my\_computer) 、サブドメイン名 (my\_company) 、最上位ドメイン名 (com) が順に指定されています。一般的には、サブドメイン名と最上位ドメイン名の組み合わせ (my\_company.com) をドメイン名といいます。

## Citrix SSL Relayを使用する接続

デフォルトではCitrix SSL Relayのリスナーポートとして、TLSで保護された通信の標準ポートであるXenAppサーバーのTCPポート443が使用されます。SSL Relayは、SSL/TLS接続要求を受信すると、その要求を解読してからサーバーに転送します。

443以外のリスナーポートを構成する場合、Citrix Receiverに対して非標準のリスナーポート番号を指定する必要があります。

Citrix SSL Relayを使用すると、次の通信のセキュリティを保護できます。

- TLSが有効なユーザーデバイスとサーバー間の通信。

- Web InterfaceによるXenAppサーバーとWebサーバー間の通信。

SSL Relayによるセキュリティ機能については、[XenApp](#)のドキュメントを参照してください。 TLS暗号化を使用するためのWeb Interfaceの構成については、[Web Interface](#)のドキュメントを参照してください。

## TLSの構成および有効化

[WFClient]セクションに次の構成オプションを追加することでネゴシエートできるTLSプロトコルのバージョンを制御できます。

- MinimumTLS=1.0
- MaximumTLS=1.2

これらはデフォルト値で、コードで設定されています。 必要に応じてこれを変更します。

注：これらの値は、プログラムの開始時に必ず読み取られます。 selfserviceまたはstorebrowseを開始した後でこれらの値を変更する場合、「**killall AuthManagerDaemon ServiceRecord selfservice storebrowse**」と入力する必要があります

注：このバージョンのCitrix Receiver for LinuxではSSLv3プロトコルの使用を無効にしています。

Citrix Receiver とXenApp/XenDesktop間をTLSを使用してTCP接続する場合、Citrix Receiver for Linuxは次の暗号の組み合わせとともにTLS接続のためのTLS 1.0、1.1、および1.2をサポートします。

- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_RSA\_WITH\_RC4\_128\_SHA
- TLS\_RSA\_WITH\_RC4\_128\_MD5
- TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA

Citrix Receiver とXenApp/XenDesktop間をTLSを使用してUDP接続する場合、Citrix Receiver for Linuxは次の暗号の組み合わせとともにDTLS 1.0をサポートします。

- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA

## ユーザーデバイスへのルート証明書のインストール

TLSを使うには、サーバー証明書の証明機関の署名を確認するためのルート証明書がユーザーデバイスにインストールされている必要があります。 Citrix Receiverでは、デフォルトで以下の証明書がサポートされます。

証明書	証明機関
Class4PCA_G2_v2.pem	VeriSign Trust Network
Class3PCA_G2_v2.pem	VeriSign Trust Network
BTCTRoot.pem	Baltimore Cyber Trust Root
GTECTGlobalRoot.pem	GTE Cyber Trust Global Root
Pcs3ss_v4.pem	Class 3 Public Primary Certification Authority

GeoTrust_Global_CA.pem	GeoTrust
DigiCertGlobalRootCA.pem	DigiCert Global Root CA

これらの証明書を使用する場合は、ルート証明書をユーザーデバイスにインストールする必要はありません。ただし、上記の証明機関以外の証明書を使用する場合は、該当する証明機関からルート証明書を取得して、各ユーザーデバイスにインストールする必要があります。

**重要：** Citrix Receiverでサポートされる証明書のキーの長さは、4096ビットまでです。証明機関のルート証明書と中間証明書、およびお使いのサーバーの証明書は4096ビット長以下である必要があります。

**注：** Receiver for Linux 13.0は、ローカルデバイスのc\_rehashを使用します。バージョン13.1以降は、以降で説明しているようにctx\_rehashツールを使用します。

### ルート証明書の使用

証明機関により発行され、ユーザーデバイスに信頼されていないサーバー証明書を認証するには、StoreFrontストアを追加する前に以下の手順を行ってください。

1. PEM形式のルート証明書を入手します。  
ヒント：PEM形式の証明書が見つからない場合は、opensslユーティリティを使用してCRT形式の証明書をPEMファイルに変換できます。
2. パッケージをインストールしたユーザー（通常はルート）が、以下の手順を実行します。
  1. ルート証明書を\$ICAROOT/keystore/cacertsにコピーします。
  2. 次のコマンドを実行します。  
\$ICAROOT/util/ctx\_rehash

### 中間証明書の使用

お使いのStoreFrontサーバーが使用している証明書と一致する中間証明書を提供できない場合、または中間証明書をインストールしてスマートカードユーザーをサポートする必要がある場合、StoreFrontストアを追加する前に次の手順を実行します。

1. PEM形式の中間証明書を別途入手します。  
ヒント：PEM形式の証明書が見つからない場合は、opensslユーティリティを使用してCRT形式の証明書をPEMファイルに変換できます。
2. パッケージをインストールしたユーザー（通常はルート）が、以下の手順を実行します。
  1. ファイルを\$ICAROOT/keystore/intcertsにコピーします。
  2. パッケージをインストールしたユーザーとして次のコマンドを実行します。  
\$ICAROOT/util/ctx\_rehash

## スマートカードサポートの有効化

Citrix Receiver for Linuxは、さまざまな種類のスマートカードリーダーをサポートしています。サーバーとReceiverの両方でスマートカードのサポートを有効にすると、以下の機能が有効になります。

- スマートカードによるログオン認証。スマートカードを使って、Citrix XenAppサーバーにログオンするユーザーを認証します。
- スマートカード対応アプリケーションのサポート。スマートカード対応の公開アプリケーションを使って、ローカルのス

マートカードリーダーにアクセスできます。

スマートカードのデータは機密性の高い情報であるため、TLSなどの信頼された証明機関から認証されたセキュリティアーキテクチャを経由して転送する必要があります。

次に、スマートカードサポートを使用するための条件を示します。

- スマートカードリーダーと公開アプリケーションが、業界標準のPC/SC規格に準拠している必要があります。
- 使用するスマートカードに適切なドライバーをインストールする必要があります。
- PC/SC Liteパッケージをインストールする必要があります。
- ミドルウェアがPC/SCを使ってスマートカードにアクセスするためのpcscdデーモンをインストールして実行する必要があります。
- 64ビットシステムには、64ビットと32ビットの両バージョンの"libpcsc-lite1"パッケージがある必要があります。

**重要：** SunRayサーバーソフトウェアVersion 2.0以降でSunRayターミナルを使用している場合は、PC/SCバイパスパッケージをインストールする必要があります。このパッケージは、SunのWebサイト ([www.sun.com](http://www.sun.com)) からダウンロードできます。サーバー上でのスマートカードサポートの構成について詳しくは、[XenDesktop](#)および[XenApp](#)のドキュメントを参照してください。

### NetScaler Gateway経由の接続

Citrix NetScaler Gateway (旧称「Access Gateway」) を使用すると、StoreFrontストアへの接続を保護して、デスクトップやアプリケーションへのユーザーアクセスを詳細に管理できます。

### NetScaler Gateway経由でデスクトップやアプリケーションに接続するには

1. 管理者により提供されたNetScaler GatewayのURLを指定します。これを行うには、以下のいずれかの手順に従います。
  - セルフサービスユーザーインターフェイスの初回使用時に、[アカウントの追加] ダイアログボックスでURLを入力します。
  - セルフサービスユーザーインターフェイスの初回使用時以降は、[環境設定] > [アカウント] > [追加] の順に選択します。
  - storebrowseコマンドで接続する場合は、コマンドラインにURLを入力します。URLにより、ゲートウェイと、必要に応じて特定のストアが指定されます。
  - Receiverで検出された最初のストアに接続されるようにするには、URLを <https://gateway.company.com> の形式で使用します。
  - 特定のストアに接続する場合は、URLを <https://gateway.company.com?<storename>> の形式で使用します。この動的URLは、非標準の形式です。そのため、= (等号記号) をURLに含めないでください。storebrowseコマンドで特定のストアに接続する場合は、URLを引用符で囲んで指定します。
2. 資格情報の入力を確認するメッセージが表示されたら、ユーザー名、パスワード、およびセキュリティトークンを入力します。手順について詳しくは、NetScaler Gatewayのドキュメントを参照してください。認証処理が完了すると、デスクトップまたはアプリケーションが表示されます。

# トラブルシューティング

Jan 23, 2017

ここでは、管理者によるCitrix Receiver for Linuxのトラブルシューティングに役立つ情報について説明します。

- [接続の問題](#)
- [表示の問題](#)
- [ブラウザの問題](#)
- [その他の問題](#)
- [コネクション構成エラー](#)
- [wfclient.ini構成エラー](#)
- [PACファイルエラー](#)
- [その他のエラー](#)
- [Citrixテクニカルサポートへの診断情報の送付](#)

## 接続の問題

以下の接続関連の問題が確認されています。

## Windows Media Playerが特定のフォーマットのファイルを再生できない

要求されたフォーマットを処理するためのGStreamerプラグインがCitrix Receiverにないことがあります。この場合は通常、サーバーに別のフォーマットが要求されます。まれに、適正プラグインの初期チェックにおいて必要なプラグインが存在すると間違っして示されることがあります。これは検出される必要があり、ファイルの再生中Windows Media Playerで問題が起こったことを示すエラーダイアログがサーバーに表示されます。Citrix Receiverにより件の形式は拒否されるため、セッション内でファイルの再生を再試行すると通常は正常に機能し、その結果、サーバーがほかのフォーマットを要求するか、あるいはメディアそのものをレンダリングします。

まれに、進行状況インジケータがWindows Media Playerで正常に動作しているにもかかわらず、適正なプラグインがないという事実が検出されずにファイルが正常に再生されないことがあります。

以降のセッションで、このエラーダイアログや再生の失敗を避けるには：

1. たとえば、構成オプション"SpeedScreenMMAVerbose=On"を\$Home/.ICAClient/wfclient.iniの[WFClient]セクションに一時的に追加します。
2. ターミナルから開始されたセルフサービスのWFICAを再開します。
3. このエラーを生成するビデオを再生します。
4. 見つかないプラグイントレースに関連付けられたMIMEの種類、またはサポートされているはずだけでも再生されないMIMEの種類 ("video/x-h264.."など) を (トレースアウトプットなどに) メモします。
5. メモしたMIMEの種類がある行で、\$ICAROOT/config/MediaStreamingConfig.tblを編集し、'!'とそのMIMEの種類の間 '?'を挿入します。これによりフォーマットが無効となります。
6. このエラー状態の原因となるその他のメディアフォーマットに対して、(上記の) 手順2~5を繰り返します。
7. GStreamerプラグインのほかのセットがあるその他のマシンに、この変更したMediaStreamingConfig.tblを配信します。

注：または、MIMEの種類を識別した後、それをデコードするためにGStreamerプラグインをインストールすることができます。

## 公開リソースまたはデスクトップセッションに接続できない

Windowsサーバーへの接続を確立しているときに、ダイアログボックスに「サーバーxxxに接続しています」というメッセー

ジが表示された後に、接続画面が何も開かない場合は、サーバーのクライアントアクセスライセンス (CAL) の構成を確認する必要があります。ライセンスについて詳しくは、[製品ライセンスの有効化](#)を参照してください。

## セッションに再接続できない場合がある

Receiverからの要求よりも多いウィンドウの色数でセッションを再接続しようとする、接続に失敗する場合があります。これは、サーバーのメモリ不足が原因です。再接続に失敗した場合、Receiverはセッションで元の色数を使おうとします。再接続した場合は、サーバーは新しいセッションを要求した色数で開始しようとし、元のセッションは切断されたままになります。ただし、サーバーのメモリが依然不足している場合は2つ目のセッションも失敗する可能性があります。

## サーバー名を省略せずに指定してもサーバーに接続できない

ネットワークでDNS (ドメインネームシステム) を構成すると、接続するサーバー名を解決できるようになります。構成されたDNSがない場合は、サーバー名をIPアドレスに解決することができません。または、接続先サーバーの名前の代わりにIPアドレスを指定することもできます。ただし、TLS接続では、IPアドレスではなく完全修飾ドメイン名の指定が必要です。

## 接続時に「プロキシを検出できません。」というエラーメッセージが表示される

コネクションで自動プロキシ検出を使用するように構成されていて、接続時に「プロキシを検出できません。JavaScript エラーです。」というエラーメッセージが表示される場合は、\$ICAROOT/util内にwpad.datファイルをコピーします。次のコマンドを実行します。ここで、hostnameは接続するサーバーのホスト名です。

```
cat wpad.dat | ./pacexec pac.js FindProxyForURL http://hostname hostname 2>&1 | grep "undeclared variable"
```

コマンドを実行しても出力がない場合は、サーバーのwpad.datファイルに調査が必要な深刻な問題があります。ただし、「assignment to undeclared variable ...」のような出力がある場合は問題を解決できます。pac.jsを開き、出力内に表示されている各変数について、ファイルの最初に次の形式の行を追加します。ここで、「...」は変数名です。

```
var ...;
```

## セッションの開始に時間がかかる

マウスを動かすまでセッションが開始されないことがあります。Linuxカーネルでの乱数生成に問題があると、この問題が発生します。この問題を回避するには、run an entropy-generating daemon such as rngd (ハードウェアベース) または haveged (Magic Software) などのエントロピー生成デーモンを実行してください。

## シリアルポート設定を構成する

単一のシリアルポートを構成するには、\$ICAROOT/config/module.ini構成ファイルに次のエントリを追加します。

```
LastComPortNum=1 ComPort1=<device>
```

複数のシリアルポートを構成するには、\$ICAROOT/config/module.ini構成ファイルに次のエントリを追加します。

```
LastComPortNum=2 ComPort1=<device1> ComPort2=<device2>
```

## 接続エラー

「接続エラー：認証サービスとの通信中にプロトコルエラーが発生しました」というエラーダイアログボックスが開きます。以下のような多くの問題がこのエラー条件を引き起こします。

- ローカルコンピューターとリモートコンピューターが共通のTLSプロトコルをネゴシエートできないとき。
- リモートコンピューターが不適切にクライアント証明書を要求するとき。IISはCitrix/Authentication/Certificateの証明書

のみを許可または要求する必要があります。

- ほかの問題。

## 表示の問題

### スクリーンティアリングが起きるのはなぜですか？

スクリーンティアリングは、横ブロックに画面上で複数の異なるフレームが同時に積み重なって表示されるときに発生します。画面上のコンテンツを迅速に大幅に変更するとよく見られる現象です。データはティアリングを避ける方法でVDAでキャプチャされ、ティアリングを起こさない方法でクライアントに渡されますが、X11 (Linux/Unixグラフィックスサブシステム) によって、ティアリングを防ぐ方法で画面に描画する一貫した方法が提供されません。

スクリーンティアリングを防ぐには、アプリケーションの描画と画面の描画を同期化する標準的なアプローチをお勧めします。つまり、vsvncによる次のフレームの描画開始を待機します。Linuxを使用する場合、クライアントに搭載されているグラフィックスハードウェアおよび使用するウィンドウマネージャーに応じて、多くの選択肢があります。これらの選択肢は2つのソリューションに分けられます。

- X11 GPU設定
- コンポジションマネージャーを使用する

#### X11 GPU構成

Intel HDグラフィックスについては、以下の内容でxorg.conf.dに**20-intel.conf**というファイルを作成します。

```
Section "Device"
    Identifier "Intel Graphics"
    Driver "intel"
    Option "AccelMethod" "sna"
    Option "TearFree" "true"
EndSection
```

Nvidiaグラフィックスについては、お使いの構成に対応する"MetaModes"オプションを含む、xorg.conf.dフォルダーでファイルを見つけます。コンマ区切りの使用されるMetaModeごとに、以下を追加します。

```
{ForceFullCompositionPipeline = On}
```

次に例を示します。

```
Option "MetaModes" "DFP-0: 1920x1200 +0+0 {ForceFullCompositionPipeline = On}"
```

注：異なるLinuxディストリビューションはxorg.conf.dに対して異なるパスを使用します。たとえば、/etc/X11/xorg.conf.d、または、/user/share/X11/xorg.conf.d。

#### コンポジションマネージャー

以下を使用します。

- Compiz (Ubuntu Unityに組み込み)。ComprizConfig Settings Managerをインストールする必要があります。

"ComprizConfig Settings Manager"を実行

"General->Composition"で"Undirect Fullscreen Windows"をチェック解除

注：ComprizConfig Settings Managerは注意して使用してください。誤って値を変更するとシステムが起動しなくなる可能性があります。

- Compton (アドオンユーティリティ)。詳しくは、Comptonのmanページ/ドキュメントを参照してください。たとえば、次のコマンドを実行します。

```
compton --vsync opengl --vsync -aggressive
```

### キーボードの使用時に不正なキーストロークが表示される

英語以外のキーボードを使用している場合、画面表示がキーボード入力と一致しないことがあります。この場合、使用しているキーボードの種類とレイアウトを指定する必要があります。キーボードの指定については、「[キーボードの構成](#)」を参照してください。

## シームレスウィンドウの移動時に過度に再描画される

ウィンドウマネージャーの種類によっては、ウィンドウを移動すると新しいウィンドウ位置が常にサーバーにレポートされるため、再描画が過度に発生することがあります。ウィンドウを移動したときにウィンドウ枠のみを描画するモードに切り替えると、この問題は解決します。

## アイコンの互換性

Receiverは、ほとんどのウィンドウマネージャーと連携するウィンドウアイコンを作成しますが、ICCCM (Inter-Client Communication Convention Manual : クライアント間通信規約マニュアル) に準拠していません。

### ICCCMに完全に準拠するには

1. 構成ファイルwfclient.iniを開きます。
2. [WFClient]セクションで次のように行を編集します。 UseIconWindow=True
3. ファイルを保存して閉じます。

## カーソルの表示に問題がある

カーソルの色が背景色と同じまたは似ている場合には、見分けるのが難しくなることがあります。この問題は、カーソルを黒または白にすることで解決できます。

### カーソルの色を変更するには

1. 構成ファイルwfclient.iniを開きます。
2. 次のいずれかの行を[WFClient]セクションに追加します。  
CursorStipple=ffff,ffff (カーソルを黒で表示)  
  
CursorStipple=0,0 (カーソルを白で表示)
3. ファイルを保存して閉じます。

## 画面上で色がちらつく

コネクションウィンドウの内/外にマウスを移動させると、フォーカスのないウィンドウの色がちらつくことがあります。これは、PseudoColor表示でX Windows Systemを使用する場合の制限事項として知られています。可能な場合、問題のあるコネクションではより色数の多いウィンドウを使用してください。

## True Color表示による色の高速変更

サーバーに接続するとき、ウィンドウの色数として256色を選択できます。256色を選択する場合は、ビデオカードがパレットをサポートしていて、アプリケーションでパレットの色を高速変更し、アニメーション表示が可能であることが前提になります。

True Color表示では、パレットを高速変更してアニメーションを生成する機能はエミュレートできません。ソフトウェアでのこの機能のエミュレーションは相対的に時間がかかり、多くのネットワークトラフィックが費やされます。この問題を解決

するために、Receiverは高速パレット変更をバッファーに格納し、数秒ごとに実際のパレットを更新するように設定されています。

## 日本語を使用する場合の問題

Receiverでは、日本語文字にEUC-JPまたはUTF-8文字エンコードが使用されます。一方、サーバー側ではShift-JIS文字エンコードが使用されます。Receiverでは、これらの文字セット間でのエンコーディングが実行されません。このため、ファイルに日本語の名前を使用し、クライアントドライブマッピングを使用してローカルコンピューターにそのファイルを保存する場合、ローカルコンピューターではその日本語ファイル名が正しく表示されません。逆に、ローカルで日本語名のファイルを作成し、クライアントドライブマッピングを使用してサーバーに保存した場合、サーバー上でこのファイル名を正しく表示できません。この問題は、拡張パラメーターパス機能で 사용되는パラメーターの日本語でも発生します。

## セッションを複数のモニターに表示する

全画面モードのセッションは、すべてのモニターの表示領域全体に表示されます。また、コマンドラインオプションとして-spanを使用することもできます。これにより全画面セッションを複数モニターにまたがって表示できます。

Desktop Viewerツールバーの機能によって、モニターを横断したマルチモニターサポートなど、ウィンドウモードと全画面モードのセッションの切り替えることができます。詳しくは、「[操作性の向上](#)」を参照してください。

**重要：**-spanは、シームレスセッションや標準のウィンドウセッション、またそれらが混在するセッションには適用されません。

-spanオプションは、以下のように指定します。

```
-span [h][o][a] [<mon1>[,<mon2>[,<mon3>,<mon4>]]]
```

ここで **h** を指定すると、モニターの一覧が `stdout` に出力されます。また、この値のみを指定した場合、モニター一覧の出力に `wfica` が終了します。

ここで **o** を指定すると、セッションウィンドウのリダイレクト属性が `override-redirect` になります。

**注意：**この値の使用は推奨されません。これは、非協調性のウィンドウマネージャーで使用するための最後の手段です。セッションウィンドウはウィンドウマネージャーで非表示となり、アイコンもなく、再スタックできません。セッションを終了することによってのみウィンドウを削除できます。

ここで **a** を指定すると、すべてのモニターを使用してセッションが表示されます。

-spanオプションの残りの値は、使用するモニターの番号として処理されます。特定のモニターを使用する場合は単一の値 (`<mon1>`) を指定します。また、表示領域の左上と右下のモニターを指定 (`<mon1>,<mon2>`) したり、上端、下端、左端、および右端のモニターを指定 (`<mon1>,<mon2>,<mon3>,<mon4>`) したりできます。

ここで **o** を指定しない場合、`wfica` コマンドでは、`_NET_FULLSCREEN_MONITORS` メッセージによりウィンドウマネージャーから適切なウィンドウレイアウトが取得されます (サポートされる場合)。それ以外の場合は、サイズおよび位置に関するヒントを使用して必要なレイアウトを要求します。

ウィンドウマネージャーがこのクライアントメッセージをサポートするかどうかを確認するには、次のコマンドを実行します。

```
xprop -root | grep _NET_WM_FULLSCREEN_MONITORS
```

出力がない場合、サポートされません。サポートされないウィンドウマネージャーでは、ウィンドウリダイレクトの上書き (`override-redirect`) が必要な場合があります。 `override-redirect` ウィンドウをセットアップするには、-span o を使用します。

コマンドラインからセッションを複数のモニターにまたがって実行するには

1. コマンドプロンプトで、次のコマンドを実行します。

```
/opt/Citrix/ICAClient/wfica -span h
```

ユーザーデバイスに現在接続しているモニターの番号の一覧がstdoutに出力され、wficaが終了します。

2. これらのモニターの番号をメモしておきます。
3. コマンドプロンプトで、次のコマンドを実行します。

```
/opt/Citrix/ICAClient/wfica -span [w[x,y,z]]
```

ここでw、x、y、およびzは、手順1でメモしたモニターの番号です。特定のモニターを使用する場合は単一の値 (w) を指定します。また、表示領域の左上と右下のモニターを指定 (w,x) したり、上端、下端、左端、および右端のモニターを指定 (w,x,y,z) したりできます。

**重要** : selfserviceを起動したりWebブラウザでWeb interfaceに接続したりする前に、WFICA\_OPTS変数を定義しておく必要があります。これを行うには、プロファイルファイル (通常は、\$HOME/.bash\_profileまたは\$HOME/.profile) を編集して、WFICA\_OPTS変数を定義する行を追加します。次に例を示します。

```
export WFICA_OPTS="-span a"
```

この変更は、XenAppおよびXenDesktopセッションの両方に適用されます。

selfserviceまたはstorebrowseをすでに開始している場合は、新しい環境変数を適用するために開始したプロセスを削除する必要があります。次のコマンドで削除します :

```
killall AuthManagerDaemon ServiceRecord storebrowse
```

## 全画面セッションからローカルアプリケーションまたはほかのセッションに切り替えることができない

この問題は、クライアント側のシステムUIが非表示になっていて、キーボード透過機能が通常のキーボードコマンド (Alt+Tabなど) を無効にし、代わりにサーバーにコマンドを送るために発生します。

この問題を回避するには、フォーカスがセッションウィンドウに移るまでCtrl+F2キーを押してキーボード透過機能を一時的にオフにします。代替の回避策としてTransparentKeyPassthroughをいいえに\$ICAROOT/config/module.iniで設定します。これによりキーボード透過機能は無効になりますが、All\_regions.iniファイルにこの設定を追加してICAファイルを上書きする必要があります。

### ブラウザの問題

## Windowsセッション内のリンクをクリックすると、コンテンツがクライアントコンピュータのWebブラウザで表示される

サーバーからクライアントへのコンテンツリダイレクトは、wfclient.iniで有効になっています。このため、ローカルのアプリケーションが実行されます。サーバーからクライアントへのコンテンツリダイレクト機能を無効にするは、「[サーバーからクライアントへのコンテンツリダイレクトのセットアップ](#)」を参照してください。

## 公開リソースにアクセスするとき、Webブラウザにファイルの保存ダイアログボックスが表示される

FirefoxやChrome以外のWebブラウザでは、公開リソースに接続するための設定が必要な場合があります。Web Interfaceを介して接続する場合、リソースの一覧が表示されたWeb Interfaceのページにアクセスできる場合があります。公開されているリソースの一覧からアイコンをクリックしてリソースにアクセスしようとする、ICAファイルの保存を確認するメッ

ページが表示されることがあります。

## Mozilla、Firefox、Netscape以外の Webブラウザを構成するには

Webブラウザにより詳細は異なりますが、WebブラウザのMIMEタイプをセットアップして、MIMEタイプapplication/x-icaまたはICAファイルが\$ICAROOT/wficaにより実行されるように設定します。

### インストーラーでサポートされないWebブラウザ

特定のWebブラウザで問題が生じる場合、setupwfcを実行する前に環境変数BROWSERを設定して必要なWebブラウザのローカルパスや名前を指定してください。

### Firefoxでデスクトップまたはアプリケーションを起動しても何も実行されない

ICAプラグインを有効にしてください。

### FirefoxでICAプラグインが有効になっているがデスクトップおよびアプリケーションセッションが開始されない

ICAプラグインを無効にしてください。

#### その他の問題

そのほか、以下の問題が確認されています。

## サーバーがReceiverにセッションを閉じる指示をしたかどうかを確認する

wficaプログラムを使って、セッションを中断するコマンドをサーバーからいつ受信したのか、ログを記録できます。

Syslogシステムを介してこの情報を記録するには、値を6に設定した*SyslogThreshold*を構成ファイルの[WFClient]セクションに追加します。これにより、LOG\_INFO以上の優先度のメッセージのログが記録されます。*SyslogThreshold*のデフォルト値は4 (LOG\_WARNING) です。

同様に、wficaが情報を標準のエラーに送信するようにするには、値を6に設定した*PrintLogThreshold*を[WFClient]セクションに追加します。*PrintLogThreshold*のデフォルト値は0 (LOG\_EMERG) です。

Syslogシステムの構成手順については、オペレーティングシステムのドキュメントを参照してください。

## 構成ファイルの設定が適用されない

設定を適用するには、wfclient.iniの各エントリに対応するエントリがAll\_Regions.ini内に存在する必要があります。これに加えて、wfclient.iniの[Thinwire3.0]、[ClientDrive]、および[TCP/IP]セクションについて、実行する設定に対してcanonicalization.ini内に対応するエントリが必要です。詳しくは、\$ICAROOT/configディレクトリ内のAll\_Regions.iniおよびcanonicalization.iniファイルを参照してください。

## シリアルポートにアクセスする公開アプリケーションの実行に問題がある

公開アプリケーションがシリアルポートにアクセスする必要がある場合、ポートがほかのアプリケーションによりロックされていると元のアプリケーションを実行できません (エラーメッセージの表示または非表示はアプリケーションにより異なる)。このような環境では、シリアルポートを一時的にロックしたり、シリアルポートをロックしたまま解除せずに終了したりしているアプリケーションがないかをチェックします。

この問題を解決するには、シリアルポートをブロックしているアプリケーションを終了します。UUCPスタイルのロックの場合は、アプリケーションの終了後にロックファイルが残る可能性があります。このロックファイルの場所は、使用しているオペレーティングシステムにより異なります。

## Receiverを起動できない

Receiverを起動できず、「Application default file could not be found or is out of date」というメッセージが表示される場合は、環境変数ICAROOTが適切に定義されていません。デフォルト以外の場所にReceiverをインストールした場合は、環境変数ICAROOTを定義する必要があります。この問題を解決するには、次のいずれかを実行してください。

- ICAROOTをインストールディレクトリとして定義する。

ICAROOT環境変数が正しく定義されているかどうかをチェックするには、Receiverをターミナルセッションから起動します。エラーメッセージが表示される場合は、ICAROOT環境変数が正しく定義されていません。

- Receiverをデフォルトの場所に再インストールする。Receiverのインストールについて詳しくは、[Receiver for Linuxのダウンロードとインストール](#)を参照してください。

以前デフォルトの場所にReceiverをインストールしていた場合は、再インストールする前に/opt/Citrix/ICAClientまたは\$HOME/ICAClient/platformディレクトリを削除する必要があります。

## キーボードショートカットが正しく機能しない

ウィンドウマネージャーで同じキーボードショートカットが定義されている場合、セッションでのキーボードショートカットが正しく機能しない場合があります。たとえば、KDEウィンドウマネージャーでデスクトップ13~16に切り替えるためのキーの組み合わせである、Ctrl+Shift+F1~F4キーがこれに該当します。この問題を解決するには、以下の方法を使用します。

- ローカルのキーの組み合わせをサーバー側のキーの組み合わせにマップするトランスレートモードを使用します。たとえば、デフォルトのトランスレートモードでは、Ctrl+Shift+F1がサーバー側のAlt+F1にマップされています。これを変更してほかのローカルキーの組み合わせを使用するには、\$HOME/.ICAClient/wfclient.iniの[WFClient]セクションを編集します。たとえば、次の変更によりローカルのAlt+Ctrl+F1がサーバー側のAlt+F1にマップされます。
  - Hotkey1Shift=Ctrl+Shift を Hotkey1Shift=Alt+Ctrlに変更します。
- キーの組み合わせをすべてサーバー側に直接送信するダイレクトモードを使用します。この場合、キーの組み合わせはローカルでは処理されません。ダイレクトモードを構成するには、\$HOME/.ICAClient/wfclient.iniの[WFClient]セクションで、TransparentKeyPassthrough を Remoteに設定します。
- ウィンドウマネージャー側のキーボードショートカットを再構成して競合を解消します。

## リモートのクローアチア語キーボードを有効にする

クローアチア語キーボードレイアウトでリモートの仮想デスクトップにASCII文字が正しく送信されるようにするには、以下の手順に従います。

1. 適切な構成ファイルを開き、[WFClient]セクションのUseEUKSforASCIIでTrueを指定します。
2. UseEUKSで2を指定します。

## Citrix SSLSDKまたはOpenSSLのバージョン番号を確認する

実行中のCitrix SSLSDKまたはOpenSSLのバージョン番号を確認するには、次のコマンドを使用できます。

```
strings libctxssl.so | grep "Citrix SSLSDK"
```

また、AuthManagerDaemonまたはPrimaryAuthManager上でもこのコマンドを実行できます。

## クライアントで日本語キーボードを使用する

日本語キーボードの使用を構成するには、wfclient.ini構成ファイルで次のエントリを更新します。  
KeyboardLayout=Japanese (JIS)

## クライアントでABNT2キーボードを使用する

ABNT2キーボードの使用を構成するには、wfclient.ini構成ファイルで次のエントリを更新します。  
KeyboardLayout=Brazilian (ABNT2)

## ローカルキーボードの一部のキーが正常に機能しない

SICAROOT/config/module.iniの一覧で最適のサーバーレイアウトを選択します。

### コネクション構成エラー

このエラーは、コネクションエントリが適切に構成されていない場合に発生します。

**E\_MISSING\_INI\_SECTION** - 構成ファイルを検証してください："..." 構成ファイルでセクション"...が見つかりません。

構成ファイルが直接編集されたか、壊れています。

**E\_MISSING\_INI\_ENTRY** - 構成ファイルを検証してください："..." セクション"...にはエントリ"...が含まれている必要があります。

構成ファイルが直接編集されたか、壊れています。

**E\_INI\_VENDOR\_RANGE** - 構成ファイルを検証してください："..." 構成ファイルのXサーバーベンダーの範囲"...が無効です。

構成ファイル内のXサーバーのベンダー情報が壊れています。Citrixに連絡してください。

### wfclient.ini構成エラー

これらのエラーは、wfclient.iniの構成が正しくない場合に発生します。

**E\_CANNOT\_WRITE\_FILE** - ファイルを書き込めません："..."

コネクションデータベースに保存するときに、空きディスク容量が不足するなどのエラーが発生しました。

**E\_CANNOT\_CREATE\_FILE** - ファイルを作成できません："..."

新しいコネクションデータベースの作成時にエラーが発生しました。

**E\_PNAGENT\_FILE\_UNREADABLE** - Citrix XenApp ファイル"...を読み取れません：そのようなファイルまたはディレクトリはありません。

— または —

**Citrix XenApp ファイル"...を読み取れません：アクセスは拒否されました。**

デスクトップアイテムまたはメニューからリソースにアクセスしようとしていますが、そのリソースのXenAppファイルを使用できません。 [ビュー] メニューの [アプリケーションの更新] を選択して公開リソースの一覧を更新し、もう一度リソースにアクセスしてみてください。問題が解決されない場合は、デスクトップアイコンまたはメニューのプロパティ、およびアイコンまたはメニューが参照しているXenAppファイルのプロパティを確認します。

## PACファイルエラー

プロキシ自動検出スクリプトファイル (PACファイル) を使用してプロキシ構成を指定する場合、以下のエラーが発生することがあります。

**プロキシを検出できません。不正な自動構成URLです。**

ブラウザーで指定したアドレスのURLのタイプが無効です。有効なタイプは「http://」および「https://」で、ほかのタイプはサポートされていません。アドレスを有効なURLタイプに変更してもう一度試してください。

**プロキシを検出できません。PACスクリプトHTTPダウンロードに失敗しました。接続できません。**

入力した名前またはアドレスが間違っていないかチェックします。間違いがある場合は、それを修正してもう一度入力します。間違いがない場合は、サーバーがダウンしています。しばらくしてから、もう一度試してください。

**プロキシを検出できません。PACスクリプトHTTPダウンロードに失敗しました。パスが見つかりません。**

必要なPACファイルがサーバーにありません。サーバー上でこれを変更するか、ブラウザーを再構成してください。

**プロキシを検出できません。PACスクリプトHTTPダウンロードに失敗しました。**

PACファイルのダウンロード中に接続が切断しました。再接続してもう一度実行します。

**プロキシを検出できません。自動構成スクリプトが無効です。**

PACファイルが空です。サーバー上でこれを変更するか、ブラウザーを再構成してください。

**プロキシを検出できません。JavaScriptサポートしていません。**

PAC実行ファイルまたはpac.jsテキストファイルがありません。Receiverを再起動します。

**プロキシを検出できません。JavaScriptエラーです。**

PACファイルに含まれているJavaScriptが無効です。サーバーでPACファイルを修正してください。 [接続の問題](#) も参照してください。

**プロキシを検出できません。プロキシ自動構成スクリプトから不正な結果が返されました。**

サーバーから不正な形式の応答を受信しました。サーバー上でこれを変更するか、ブラウザーを再構成してください。

## その他のエラー

ここでは、Receiverの使用中に発生する可能性がある一般的なエラーを示します。

**An error occurred. The error code is 11 (E\_MISSING\_INI\_SECTION). Please refer to the documentation. Exiting.**

Receiverをコマンドラインから実行するときにこのメッセージが表示される場合は、通常コマンドラインに指定した名前がappsrv.iniにないことを意味します。

**E\_BAD\_OPTION - オプション"..."は無効です。**

オプション"..."の引数が指定されていません。

**E\_BAD\_ARG - オプション"..."に無効な引数があります : "..."**

オプション"..."に無効な引数が指定されています。

**E\_INI\_KEY\_SYNTAX** - 構成ファイル"...のキー"...が無効です。

構成ファイル内のXサーバーのベンダー情報が壊れています。新しい構成ファイルを作成してください。

**E\_INI\_VALUE\_SYNTAX** - 構成ファイル"...の値"...が無効です。

構成ファイル内のXサーバーのベンダー情報が壊れています。新しい構成ファイルを作成してください。

**E\_SERVER\_NAMELOOKUP\_FAILURE** - サーバー"...に接続できません。

サーバー名を解決できません。

1つ以上のファイルに書き込めません : "... ディスクの空き容量の問題または権限の問題を解決して、もう一度実行してください。

ディスクの空き容量または権限をチェックします。問題が見つかった場合は、これを修正し、エラーのあった操作をもう一度試してください。

サーバー接続がなくなりました。再接続してもう一度実行します。これらのファイルにはデータがない可能性があります : "..."

再接続し、エラーのあった操作をもう一度試してください。

#### Citrixテクニカルサポートへの診断情報の送付

Receiverの実行時に問題が発生した場合、Citrixテクニカルサポートに診断情報の提出を求められる場合があります。この情報は、Citrixテクニカルサポートで問題を調査して修正する目的で使用されます。

Receiverに関する診断情報を取得するには

1. インストールディレクトリに、「util/lurdump」と入力します。セッションが開かれていて、可能なら問題が発生している間にこれを事項することをお勧めします。  
Receiverのバージョン、構成ファイルの内容、およびさまざまなシステム変数値などの詳細な診断情報を含むファイルが作成されます。
2. テクニカルサポートにこのファイルを送信する前に、ファイルに機密情報が含まれていないことを確認してください。

# コマンドラインパラメーター

Jan 23, 2017

次の表は、Citrix Receiver for Linuxで使用できるコマンドラインパラメーターの一覧です。

## 注意

wficaまたはstorebrowseコマンドに-?、-help、または-hオプションを指定して実行すると、パラメーターの一覧が出力されます。

## wfica

接続ファイルを使用するには、wficaの後にそのファイルの名前を入力します。次のオプションは指定しません。

ユーザー	公開キー基盤 (PKI) の各証明書に同じパスワードを使用する場合は「
使用するカスタム接続を接続ファイルから選択する。 注：セルフサービスユーザーインターフェイスを使用する場合、この方法でカスタム接続をセットアップすることはできません。	-desc description
起動に使用するデスクトップファイルを指定する。	-desktop filename
接続ファイルを指定する。	-file connection filename
代替プロトコルファイルを設定する。別のmodule.iniを使うことができます。	-protocolfile filename
代替クライアント構成ファイルを設定する。別のwfclient.iniを使うことができます。	-clientfile filename
Citrix Receiver名として、<name>で指定した名前を表示する。デフォルトではデバイス名がReceiver名として表示されます。ただしSunrayデバイスを使用している場合は、デフォルト名はデバイスのMACアドレスから取得されます。これは、.ICAClient/wfclient.iniのClientNameエントリにより上書きされますが、このエントリも-clientname <name>コマンドで上書きできます。	-clientname name
この表のパラメーター一覧を表示する。	-help
バージョン情報を表示する。	-version

<p>ユーザー エラーコードおよび文字列を表示する。</p> <p>Receiverインストールファイルの場所を設定する。これは、ICAROOT環境変数を設定することと同じです。</p>	<p>公開キー基盤 (PKI) の各証明書に同じパス ワードを使用する場合は「</p>
<p>コネクションダイアログボックスが表示されないようにする。</p>	-quiet
<p>キーロギングを有効にする。</p>	-keylog
<p>セッションのジオメトリを設定する。</p>	-geometry WxH+X+Y
<p>ウィンドウの色数を設定する。</p>	-depth <4   8   16   24   auto>
<p>マルチモニターの表示を設定する。</p>	-span [h][o][a   <mon1>[, <mon2>[, <mon3>[, <mon4>]]]
<p>クライアントデバイスのカラーマップを使用する。</p>	-private
<p>共有カラーマップを使用する。</p>	-shared
<p>公開アプリケーションに渡す文字列を指定する。</p>	-param string
<p>公開アプリケーションからクライアントドライブマッピングを使ってアクセスするUNIXパスを指定する。</p>	-fileparam unixpath
<p>ユーザー名を指定する。</p>	-username username
<p>偽装パスワードを指定する。</p>	-password password
<p>クリアテキストのパスワードを指定する。</p>	-clearpassword " <clear password>"
<p>ドメインを指定する。</p>	-domain domain
<p>初期プログラムを指定する。</p>	-program program

<p>ユーザー</p> <p>使用する初期プログラムのディレクトリを指定する。</p> <p>サウンドをオンにする。</p>	<p>公開キー基盤 (PKI) の各証明書に同じパスワードを使用する場合は「</p>
<p>サウンドをオフにする。</p>	<p>-nosound</p>
<p>ドライブマッピングの上書きを設定する。AS=&lt;path&gt;形式で指定します。ここで&lt;path&gt;は、環境変数が含まれている場所です (AS=\$HOME/tmpなど)。ドライブごとに、このパラメーターを指定してください。上書き設定が正しく適用されるようにするには、上書きする既存のマッピングが存在する必要があります。</p>	<p>-drivemap string</p>

ヒント：すべての wfica コマンドのオプションは環境変数 WFICA\_OPTS でも使用できます。これにより、Receiver のネイティブ UI や Citrix StoreFront でもこれらのオプションを使用できます。

### storebrowse

次の表は、storebrowse コマンドのオプションの一覧です。

オプション	説明	注
-L、--launch	接続先の公開リソースの名前を指定します。これにより、公開リソースへの接続が起動します。セッションは接続されたまま、コマンドが終了します。	
-E、--enumerate	使用可能なリソースが列挙されます。	デフォルトでは、リソース名、表示名、およびそのリソースを格納するフォルダー名が表示されます。ほかの情報を表示するには、--details オプションを使用します。
-S、--subscribed	サブスクリプションするリソースを一覧表示します。	デフォルトでは、リソース名、表示名、およびそのリソースを格納するフォルダー名が表示されます。ほかの情報を表示するには、--details オプションを使用します。
-M、--details 次の -E または -S オプションを使用します。	列挙する公開アプリケーションの属性を指定できます。引数として、列挙する属性の値の合計値を指定します。属性の値は、Publisher (0x1)、VideoType (0x2)、SoundType (0x4)、AppInStartMenu (0x8)、AppOnDesktop (0x10)、AppIsDesktop (0x20)、AppIsDisabled (0x40)、WindowType (0x80)、WindowScale (0x100)、DisplayName (0x200)、および	これらの情報の一部は、storebrowse では使用できません。この場合、0 が出力されます。これらの属性値は、16進数または10進数で指定できます (0x200 または 512 など)。

オプション	説明	注
	<p>AppIsMandatory (0x10000) です。 -S、-s、および-uオプションでは、 CreateShortcuts (0x100000) を指定して、サブスクライブしたアプリケーションのメニュー項目を作成できます。-Sオプションでは、RemoveShortcuts (0x200000) を指定して、すべてのメニュー項目を削除できます。</p>	
-v、--version	storebrowseのバージョン番号が標準出力に出力されます。	
-h、-?、--help	storebrowseの使用方法が表示されます。	この表を簡潔にした内容が表示されます。
-U、--username	ユーザーのユーザー名を指定します。	StoreFrontで使用する場合、サイトがHTTP基本認証をサポートするよう構成する必要があります。構成しない場合、これらのオプションは無視されます。
-P、--password	ユーザーのパスワードを指定します。	
-D、--domain	ユーザーのドメインを指定します。	
-r、--icaroot	Receiver for Linuxのインストール先のルートディレクトリを指定します。	ディレクトリを指定しない場合は、実行時に値が特定されます。
-i、--icons 次の-E、または-S オプションを使用します。	<p>デスクトップまたはアプリケーションのアイコンをPNG形式で取得します。アイコンのサイズや解像度は、best または size 実行する。</p> <p>コマンド best を使用すると、サーバー上で使用可能な最適なサイズのアイコンが取得されます。取得した後で任意のサイズに変更することができます。デバイスが best は、ストレージや帯域幅について最も効率的であり、スクリプト化も簡単です。</p> <p>コマンド size を使用すると、指定のサイズや解像度のアイコンがフェッチされます。</p> <p>いずれの引数でも、-Eまたは-Sオプションで返されるリソースごとにアイコンファイルが作成されます。</p>	<p>デバイスがbestで取得されるアイコンファイルの名前は、&lt;resource name&gt;.pngです。</p> <p>デバイスがsizeは「WxB」形式で指定します。ここで「W」はアイコンの幅（すべてのアイコンは正方形なので幅のみを指定します）で、「B」は色の解像度（1ピクセルあたりのビット数）です。「W」は必須ですが、「B」は省略できます。「B」を省略すると、そのサイズで使用可能なすべての解像度のアイコンが取得されます。作成されるアイコンファイルの名前は、&lt;resource name&gt;_WxWxB.pngです。</p>
-u、--unsubscribe	指定したストアのリソースのサブスクリプションを解除します。	
-s、--subscribe	指定したストアのリソースをサブスクライブします。	異なるReceiverを使用する場合は、Program Neighborhood Agentサーバーのサブスクリプションは失われます。

オプション	説明	注
-W[r R], --reconnect [r R]	アクティブセッションおよび切断セッションに再接続されます。	Rを指定すると、すべての切断セッションに再接続されます。Rを指定すると、すべてのアクティブセッションおよび切断セッションに再接続されます。
-WD, --disconnect	すべてのセッションが切断されます。	指定したストアのセッションにのみ適用されます。
-WT, --logoff	すべてのセッションからログオフされます。	指定したストアのセッションにのみ適用されます。
-l, --liststores	storebrowseで接続可能なStoreFrontストアの一覧を表示します。これらは、ServiceRecordプロキシで登録されたストアです。また、Program Neighborhoodサイトの一覧も表示されます。	
-a, --addstore	新しいストアをService Recordデーモンに登録します。ゲートウェイやビーコンの情報も登録されます。	ストアの完全なURLを返します。失敗するとエラーが表示されます。
-g, --storegateway	Service Recordデーモンに登録済みのストアのデフォルトのゲートウェイを設定します。	以下の構文で使用します。 ./util/storebrowse --storegateway "<unique gateway name>" '<store URL>'  重要：ストアのゲートウェイの一覧で、同じゲートウェイ名を使用することはできません。
-d, --deletestore	ストアのService Recordデーモンへの登録を解除します。	
-c, --configselfservice	セルフサービスユーザーインターフェイスの設定を取得および設定します。この設定は、StoreCache.ctxに格納されます。引数は、<entry[=value]>を指定します。「entry」のみを指定すると、現在の設定値が出力されます。「value」を指定すると、その値がセルフサービスユーザーインターフェイスに設定されます。	例：storebrowse --configselfservice SharedUserMode=True  重要：「entry」および「value」では大文字と小文字が区別されます。StoreCache.ctxに格納されている設定と大文字/小文字が異なる場合、そのコマンドは失敗します。
-C, --addCR	Citrix Receiver (CR) ファイルを読み取って、各ストアの追加を確認するメッセージを表示します。	-aオプションと同じ出力が得られますが、複数のストアが含まれる場合があります（各行に1つのストア）。
-K, --killdaemon	storebrowseデーモンプロセスを強制終了します。	すべての資格情報およびトークンがリフレッシュされます。

## pnabrowse

重要：pnabrowseは廃止予定のユーティリティですが、これを使用してWeb InterfaceのProgram Neighborhoodエージェントサイトからサーバーや公開リソースの一覧を照会して、これらに接続することができます。pnabrowseのStoreFrontスト

アでの使用はお勧めしません。代わりに、storebrowseを使用してください。storebrowseは、サイトおよびストアから資格情報を要求できます。-U、-P、および-Dオプションは、Program Neighborhoodエージェントサイトでのみ動作します。必要に応じて、接続先サーバーを指定する引数を指定できます。以下のいずれかの方法でサーバーを指定します。

- -Sおよび-Aオプションでは、XenAppサーバーの名前を指定します。
- -Eおよび-Lオプションでは、Web InterfaceサーバーのURLを指定します。

pnabrowseユーティリティは、処理の成功または失敗を示す終了値を返します。XenAppで以下のオプションを使用できません。

オプション	説明
-S	サーバーの一覧を各行に1つずつ出力します。
-A	公開アプリケーションの一覧を各行に1つずつ出力します。
-m	-Aオプションと一緒に指定して、公開アプリケーションに関するより詳細な情報 (Publisher、Video Type、Sound Type、AppInStartMenu、AppOnDesktop、ApplsDesktop、ApplsDisabled、Window Type、WindowScale、およびDisplay Name。) を出力します。
-M	-Aオプションと一緒に指定して、公開アプリケーションに関する特定の情報を出力します。引数として、列挙する属性の値の合計値 (1-1023) を指定します。属性の値は、Publisher (1)、VideoType (2)、SoundType (4)、AppInStartMenu (8)、AppOnDesktop (16)、ApplsDesktop (32)、ApplsDisabled (64)、WindowType (128)、WindowScale (256)、およびDisplayName(512)です。
-c	-Aオプションに追加して、クライアントエンジンで公開アプリケーションに接続するための (最低限の) 情報 (アプリケーション名、ブラウズサーバー、ウィンドウ解像度、色数、オーディオ、および暗号化設定など) を指定するファイルを作成します。作成されるファイルには、/tmp/<xxx>_1.ica、/tmp/<xxx>_2.icaなどの名前が設定されます (<xxx>はpnabrowseプロセスの10進数の識別子)。
-d	-Lと一緒に使用されて、XDGデスクトップファイルを指定します。
-e	エラー数を表示します。
-i	-Aオプションでの出力に、公開アプリケーションのアイコンイメージファイルのパスを追加します。指定するサイズ (WxB) オプションにより、XPMまたはPNGファイルのパスが返されます。 <ul style="list-style-type: none"> <li>• 「-i」を指定すると、XPM形式で1ピクセルあたり4ビットの16x16アイコンが返されます。</li> <li>• 「-iWxB」を指定すると、PNG形式で1ピクセルあたりBビットのWxWアイコンが返されます。</li> </ul>
-f	-Aオプションでの出力に、公開アプリケーションのXenAppでのフォルダー名を追加します。
-u	プロキシサーバーに対するユーザー名を指定します。

オプション	説明 キシサーバーに対するパスワードを指定します。
次のオプションは、Citrix XenApp (Program Neighborhoodエージェント) サービス機能を提供し、XenAppおよびXenDesktop機能の両方で使用できます。	
オプション	説明
-D	Web InterfaceサーバーまたはCitrix XenApp (Program Neighborhoodエージェント) Serviceのサーバーでユーザーを認証するためのドメインを指定します。
-E	<p>Citrix XenAppに照会して、すべての公開リソースを列挙します。</p> <p>-Eおよび-Lの両方を指定した場合は、最後のオプションが適用されます。ユーティリティは終了し、接続は開いたままになります。</p> <p>各リソースについて、以下の情報が標準出力に出力されます。各項目は一重引用符で囲まれ、タブ文字で区切られます。</p> <p>Name : アプリケーションの表示名。Access管理コンソールのアプリケーションのプロパティダイアログボックスに表示されます。</p> <p>Folder : アプリケーションのProgram Neighborhoodフォルダー名。Access管理コンソールのアプリケーションのプロパティダイアログボックスに表示されます。</p> <p>Type : アプリケーション (Application) またはコンテンツ (Content) 。</p> <p>Icon : XPM形式のアイコンファイルのフルパス。</p>
-L	接続先の公開リソースの名前を指定します。これによりCitrix XenAppが照会され、公開リソースへの接続が起動します。-Eおよび-Lの両方を指定した場合は、最後のオプションが適用されます。ユーティリティは終了し、接続は開いたままになります。
-N	新しいパスワードを指定します。このオプションは、既存の資格情報と一緒に指定する必要があります。また、既存のパスワードの有効期限が切れた場合 (終了コード238 : E_PASSWORD_EXPIREDで示されます) のみ有効です。
-P	Web InterfaceサーバーまたはCitrix XenApp (Program Neighborhoodエージェント) Serviceのサーバーでユーザーを認証するためのパスワードを指定します。
-U	Web InterfaceサーバーまたはCitrix XenApp (Program Neighborhoodエージェント) Serviceのサーバーでユーザーを認証するためのユーザー名を指定します。
-WD	そのユーザーのすべてのアクティブセッションを切断します。

オプション	説明 そのユーザーのすべてのセッションを終了します。
-Wr	そのユーザーのすべての切断セッションを再接続します。
-WR	そのユーザーのすべてのセッション（アクティブセッションおよび切断セッション）を再接続します。
-k	ユーザー名、パスワード、およびドメインの代わりに、既存のKerberosチケットを使用して認証します。クライアント側およびサーバー側で構成が必要です。詳しくは、「 — <i>Using Kerberos with Citrix Receiver for Linux Guide</i> 」を参照してください。このドキュメントは、Citrixより秘密保持契約の下で提供されます。

以下の共通オプションも使用できます。

オプション	説明
-q	サイレントモード。エラーメッセージを出力しません。
-r	-Eまたは-Aオプションでの出力に、公開アプリケーションの生アイコンデータを追加します。
-V	バージョンの詳細を表示します。
-h	各オプションの使用方法を表示します。
-?	各オプションの使用方法を表示します。