このリリースについて

Jun 22, 2016

Citrix Receiver for Macを使用して、ユーザーはXenAppサーバーやXenDesktopサーバーで公開されているリソースにアクセスできます。管理者はReceiverをユーザーに簡単に配布でき、ユーザーはシンプルな操作でアプリケーションや仮想デスクトップにすばやく安全にアクセスできます。

最新のリリースをCitrix Receiver for Macのダウンロードページからダウンロードできます。

バージョン12.1の新機能

NetScaler Gatewayに対するスマートカード認証

この機能により、スマートカード認証を使ってNetScaler Gatewayを経由したCitrix Receiverによるアプリケーションやデスクトップへのアクセスが有効になります。この機能について詳しくは、「スマートカード認証用の要件」を参照してください。

分割画面に対するElキャプションのサポート

Citrix Receiver for Mac（12.0）の以前のリリースでは、OS X El Capitanのサポートが導入されました。このリリースでは、El Capitanの分割画面機能をフルサポートしています。

クライアントの自動再接続とセッション画面の保持の改善

この改善により、CloudBridgeとNetScaler Gatewayの相互運用性がより向上しています。セッションは、接続パスには関係なく、クライアントの自動再接続とセッション画面の保持を使って再接続できます。このリリースに特定の拡張は以下の通りです。

機能強化された接続メッセージによりユーザーに接続状況が示され、またいつ接続が失われ、何するのかが通知されます。

カウントダウンタイマー（分/秒単位）により、セッションがタイムアウトするまでの時間が示されるようになりました。セッションは、カウントダウンタイマーの有効期限が切れると中断されます。デフォルトでは、タイムアウト値は2分に設定されています。デフォルト値は、**TransportReconnectMaxRetrySeconds** ICAファイル設定で変更できます。

> ### 注意
>
> この機能により、XenAppおよびXenDesktopの追加のセッション管理設定である**TransportReconnectRetryMaxTimeSeconds**がサポートされます。
>
> **TransportReconnectDelay**および**TransportReconnectRetries**は今後使用されません。詳しくは、「セッション管理」を参照してください。

バージョン12.0の新機能

StoreFront 3.0の中央集中型のカスタマイズおよびブランド化機能と組み合わせて使用すると、このReceiver for Macのユーザーは、StoreFrontから提供される集中管理されたアプリケーションやデスクトップを使用できるようになります。これは、WindowsデスクトップのReceiverやHTML5およびChrome Web ReceiverがStoreFront 3.0に割り当てられた場合と同じ環境が提供されるということです。

OS X El Capitan（10.11）のサポート。

セッションcookieのサポート：StoreFront 3.0に必要な新しいWeb APIを使用する、また負荷分散をサポートするために、Citrix Receiver for Mac 12.0はWebセッションcookieをサポートします。

タイムゾーンの強化：Citrix Receiver for Mac 12.0をXenAppタイムゾーンのリダイレクトと共に使用すると、ローカルのタイムゾーンがより正確に検出されます。詳しくは、「タイムゾーン制御のポリシー設定」を参照してください。

Citrix Receiver for Mac 12で解決された問題

Mar 10, 2016

Citrix Receiver for Mac 12で解決された問題

このリリースではスマートカード統合に関する多くの問題が解決されています。 一部の問題については未解決で、引き続き調査が実行されます。

このリリースで解決されたそのほかの問題：

- 日本語環境で、資格情報を入力するダイアログボックスに正しくないメッセージ「デモアカウントにログオンしてください」が表示されました。 正しくは「仮想デスクトップにログオンしてください」でした。[#LC2682]
- Receiverの複数のディスクイメージを同時にマウントすると、間違ったインストーラーが起動することがありました。 [#551605]
- CIDR表記のOS Xプロキシバイパスエントリが無視されました。 [#564250]
- OS Xバイパス一覧の最初の250文字のみが使用されました。 [#567089]
- 内部ビーコンの誤検知チェックが特定のISPで失敗することがありました。これらのISPはBarefruitのDNSエラーリダイレクトソフトウェアをインストールしていました。 [#572456]

Citrix Receiver for Mac 12.1で解決された問題

- OS Xに組み込まれているVPNサポートを使用している場合、VPNがアクティブな間にCitrix Receiverが構成済みのアカウントに接続できなかったことがある問題が解決されました。
- セッションが分割ビューになった場合にセッションの表示が乱れるOS X El Capitanの問題が解決しました。 [582397]
- F5プロキシを使って外部接続しようとするとビーコンの検出に失敗する問題が解決されました。 [582885]
- システム環境設定で構成されたキーボードショートカットがセッションに適用されなかった問題が解決されました。 [583033]
- ビューアーがクラッシュする原因であった、Citrix Receiver for Mac 11.9.15および12の「+」キーボード記号の問題が解決されました。 [586179] [577922]
- あるアプリケーションを起動後に、Citrix Receiverにより別のアプリケーションに対する認証を求められる問題が解決されました。 [592460]
- キーボードの組み合わせCtrl + Qキーが正しく渡されなかったデスクトップセッションの問題が解決されました。 [600601

Citrix Receiver for Mac 12.1.100で解決された問題

- 名前が「@」で始まるアプリケーションまたはデスクトップを起動するとセッションがクラッシュする問題が解決しました。 [LC4296]
- NetScaler Gatewayに対するIPV6接続が失敗する問題が解決しました。 [LC4512]
- Cisco ASA 9.32 SSL VPNを介して接続するとReceiver for Macセッションが失敗する問題が解決しました。 [LC3887]
- セッションが切断すると「リモートSSLピアが bad MACアラートを送信しました。」というエラーメッセージが表示される問題が解決しました。[LC4367]
- 単一の日本語または簡体中国語を入力しようとするとセッションデスクトップには文字が表示されない問題が解決しました。 [603635]

Citrix Receiver for Mac 12の既知の問題

Jul 07, 2016

Citrix Receiver for Mac 12の既知の問題

このリリースでは、以下の既知の問題が確認されています。

- OS X El Capitan（10.11）では、仮想デスクトップとアプリは通常スプリットビューでは表示されません。 [#582397]
- スマートカード認証を使用すると、XenDesktopセッションを開始できません。 [#550781]
- PIVスマートカードを使用する場合、ReceiverはXenDesktop 5.6セッションに再接続できません。 [#550986]
- セッションからの切断時に公開コマンドプロンプトが最小化されていると、再接続時にコマンドプロンプトが再表示されない可能性があります。 [#411702]
- 複数の証明書がインストールされていて一部の証明書が失効していると、SSL SDKで、証明書チェーンを失効済みと誤ったフラグが設定される可能性があります。 キーチェーンアクセスから失効証明書を削除すると、この問題は解決されます。 [#511574]
- 更新の前にユーザーがアプリをサブスクライブすると、Receiverで表示されるアプリケーション名はBrokerおよびStoreFrontで更新が反映されません。 この問題が発生する場合、ユーザーはアプリを削除してから再度サブスクライブできます。 [#515097]
- Windowsのログオンメッセージの表示中にデスクトップウィンドウのサイズを変更すると、セッションが応答しなくなる可能性があります。 [#525833]
- OS X Mountain Lion（10.8）を使用していて、Receiver 11.9または11.9.15からReceiver 12.0にアップグレードしている場合、Receiverの起動時に新しいバージョンと古いバージョンの両方のReceiverが開く可能性があります。 [#552496]
- Mac OS X向けのGoogle Chromeブラウザーでダウンロードバーの.icaファイルをダブルクリックすると、複数の.icaファイルが起動し、エラーメッセージが表示される可能性があります。 [#564961]
- Web InterfaceのPNAアカウントへのログオン時に、ユーザーが失効したパスワードを変更できない可能性があります。 [#568394]
  ビデオ通話セッション中に全画面モードにすると、XenDesktopツールバーのボタン下側が欠ける可能性があります。 [#570480]
- Mac OS X Mountain Lion（10.8）が動作するコンピューターのユーザーには、Receiverのユーザーインターフェイス上でログオンという文字列とダウンアイコンが重なって表示されることがあります。 この場合、ダウンアイコンをクリックする代わりに［ログオン］またはユーザー名の文字列アイコンをクリックできます。 [#504302]
- DirectXまたはOpenGLアプリケーションを実行中にフルスクリーンに変更すると、カーソルが非表示となります。 [#510745]
- サーバーの言語が繁体字中国語に設定されると、セッション内で"["または"]"を入力できなくなります。 [#511877]
- 状態の変更がユーザーのアイドル状態に起因する場合、カーソルを移動してもLyncの状態は［退席中］から［連絡可能］に変更されません。 この場合、ユーザーは手動で［連絡可能］に状態を変更する必要があります。 [#512074]
- マルチモニター構成では、表示が再構成されるとシームレスアプリがプライマリ表示に移動することがあります。 [#506532]
- HDXアプリが黒色表示となることがあります。 この問題が発生したら、アプリケーションをドラッグし、［閉じる］ボタンがあるべき場所をクリックしてクリックしてそれを閉じます。 [#426991]
- OS X Yosemite（10.10）では、SafariのアップグレードバージョンによりポップアップウィンドウとしてReceiverがブロックされることがあります。 アプリやデスクトップを開くためのポップアップウィンドウを有効にすると、問題が解決します。

Citrix Receiver for Mac 12.1の既知の問題

このリリースでは、以下の既知の問題が確認されています。

- Windowsのログオンメッセージの表示中にデスクトップウィンドウのサイズを変更すると、セッションが応答しなくなります。
  [525833]
- Chromeから仮想デスクトップを起動すると、エラーメッセージが表示されることがあります。
  [564961]
- ビューアーは正しいキーボードレイアウトをサーバーに送らず、キーボードマッピングの問題が発生します。
  [581829]
- OS X 10.11（El Capitan）マシンへのセッションでスムースローミングを実行すると、セッションが再接続に成功しないことがあります。 最初に再接続に失敗したら、［アプリの更新］メニューコマンドを使って、セッションに再度再接続します。
  [601542]

Receiver for Mac 12.0のシステム要件

Oct 31, 2016

Citrix Receiver for Mac 12.0でサポートされるオペレーティングシステム

- OS X El Capitan（10.11）
- OS X Yosemite（10.10）
- OS X Mavericks（10.9）
- OS X Mountain Lion（10.8）

Mountain Lionよりも前のOS Xのリリースはサポートされません。

Citrix Receiver for Mac OS X Lion（10.7）以前のバージョンが必要な場合は、「Citrix Receiver for Mac 11.9.x」を参照してください。

ハードウェア要件

- 110MB以上の空きディスク領域
- サーバーに接続するためのネットワークまたはインターネット接続

サポートされるサーバー

- XenAppの以下のバージョン：
  - Citrix XenApp 7.6 for Windows Server 2012 R2
  - Citrix XenApp 7.5 for Windows Server 2012 R2
  - Citrix XenApp 6.5 for Windows Server 2008 R2
- XenDesktopの以下のバージョン：
  - XenDesktop 7.6
  - XenDesktop 7.5
  - XenDesktop 7.1
  - XenDesktop 7
- Citrix VDI-in-a-Box 5.4、および5.3
- StoreFront：
  - StoreFront 3.0
  - StoreFront 2.6
  - StoreFront 2.5
  - StoreFront 2.1
- Web Interface：
  - アプリケーションに（Webブラウザーからではなく）Receiverでアクセスする場合は、Web Interface 5.4 for WindowとXenApp Servicesサイト（Program Neighborhoodエージェントサービスサイト）。
- Receiverの展開：
  - Citrix Receiver for Web 2.1、2.5、および2.6
  - Citrix Web Interface 5.4

サポートされるWebブラウザー

- Safari 6.0以降
- Mozilla Firefox 22.x以降
- Google Chrome 28.x以降

Connectivity

OS X El CapitanでユーザーがCitrix Receiver for Mac 12を実行していて、また接続に問題がある場合、NetScaler Gateway Pluginのアップグレードが必要な場合があります。詳しくは、Citrixダウンロードページのアーティクル「NetScaler Gateway Plug-in v3.1.4 for Mac OS X (El Capitan Support)」を参照してください。

Citrix Receiver for MacでXenAppまたはXenDesktopにアクセスする場合、以下のいずれかの構成でのHTTP、HTTPS、およびICA-over-TLS接続がサポートされます。

LAN接続の場合：

- StoreFront ServicesサイトまたはReceiver for Webサイトを使用するStoreFront。
- Web Interface 5.4 for WindowsとXenApp Servicesサイト。

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 11.0（含むVPX）
- Citrix NetScaler Gateway 10.5（含むVPX）
- Citrix NetScaler Gateway 10.1（含むVPX）
- Citrix Access Gateway Enterprise Edition 10.x（含むVPX）
- Citrix Access Gateway Enterprise Edition 9.x（含むVPX）
- Citrix Access Gateway VPX
- Citrix Secure Gateway 3.x（Web Interfaceを使用する環境でのみ）

StoreFrontとAccess GatewayまたはNetScaler Gatewayの展開については、Access GatewayまたはNetScaler GatewayとStoreFrontのドキュメントを参照してください。

認証

StoreFrontへの接続では、Receiverで以下の認証方法がサポートされます。

	ブラウザーを使った Receiver for Web	StoreFront Servicesサイト（ネイティブ）	StoreFront XenApp Servicesサイト（ネイティブ）	NetScalerから Receiver for Web（ブラウザー）	NetScalerから StoreFront Servicesサイト（ネイティブ）
匿名	はい	はい			
ドメイン	はい	はい		はい *	はい *
ドメインパススルー					
セキュリティトークン				はい *	はい *
2要素（セキュリティトークンがあるドメイン）*				はい *	はい *
SMS				はい *	はい *

スマートカード** ユーザー証明書	ブラウザーを使った**Receiver for Web**	はい **StoreFront Servicesサイト（ネイティブ）**	はい **StoreFront XenApp Servicesサイト（ネイティブ）**	はい* **NetScalerからReceiver for Web（ブラウザー）** はい（NetScaler Gateway Plugin）	はい* **NetScalerからStoreFront Servicesサイト（ネイティブ）** はい（NetScaler Gateway Plugin）

*Receiver for WebサイトおよびNetScaler Gatewayを含む展開に対してのみ使用できます（デバイスへの関連プラグインのインストールは関係なし）。

**OS X 10.10でスマートカードを使用するには、OS X 10.10.2以上をインストールする必要があります。

Web Interface 5.4への接続では、Receiverで以下の認証方法がサポートされます。
注：（Web Interfaceでは、指定ユーザーによる認証がドメイン+セキュリティトークン認証に相当します）。

	Web Interface（ブラウザー）	**Web Interface XenApp Servicesサイト**	**NetScalerからWeb Interface（ブラウザー）**	**NetScalerからWeb Interface XenApp Servicesサイト**
匿名	はい			
ドメイン	はい	はい	はい	はい
ドメインパススルー				
セキュリティトークン			はい*	はい
2要素（セキュリティトークンがあるドメイン）*			はい*	はい
SMS			はい*	はい
スマートカード**	はい	はい	はい	はい
ユーザー証明書			はい（NetScaler Gateway Pluginが必要）	はい（NetScaler Gateway Pluginが必要）

* NetScaler Gatewayを展開する環境でのみ使用できます（デバイスへの関連プラグインのインストールは関係なし）。

**Appleのスマートカードのサポートに対する変更により、スマートカードはOS X 10.10によりサポートされていません。

認証については、Citrix製品ドキュメントのAccess GatewayまたはNetScaler GatewayとStoreFrontのドキュメントを参照してください。 Web Interfaceでサポートされるそのほかの認証方法については、Citrix製品ドキュメントのWeb Interfaceのドキュメントで「Web Interfaceの認証方法の構成」を参照してください。

スマートカード認証用の要件

Nov 13, 2015

Receiver for Macは次の構成においてスマートカード認証をサポートします。

- StoreFront 2.xおよびXenDesktop 5.6以上またはXenApp 6.5以上があるReceiver for Webに対するスマートカード認証
- Microsoft OutlookやMicrosoft Officeなどのスマートカード対応アプリケーションでは、仮想デスクトップやアプリケーションセッションでドキュメントにデジタル署名を追加したりファイルを暗号化したりできます。
- 複数の証明書 - Receiver for Macは単一のスマートカードまたは複数のスマートカードでの複数の証明書の使用をサポートします。ユーザーがスマートカードをリーダーに挿入すると、ユーザーデバイス上で実行する、Receiverを含むすべてのアプリケーションで複数の証明書を使用できるようになります。
- ダブルホップセッション - ダブルホップセッションでは、Receiverとユーザーの仮想デスクトップとの間に追加の接続が確立されます。

  ダブルホップセッションをサポートする展開方法については、XenAppおよびXenDesktopのドキュメントを参照してください。詳しくは、「スマートカード展開」を参照してください。

NetScalerに対するスマートカード認証について

スマートカードを使って接続を認証する場合、スマートカードに複数の使用可能な証明書が入っていると、証明書を選択するようCitrix Receiverがプロンプトを表示します。証明書を選択したら、スマートカードのパスワードを入力するようにCitrix Receiverからプロンプトが表示され、認証が実行されてセッションが開始します。

スマートカードにある証明書のうち適切なものが一つだけの場合は、Citrix Receiverはその証明書を使用して選択を求めるプロンプトは表示されません。ただし、接続を認証してセッションを開始するために、スマートカードに割り当てられたパスワードを入力する必要はあります。

スマートカード認証用のPKCS#11モジュールの指定

Citrix Receiverの［基本設定］ウィンドウの詳細構成オプションを使って、認証目的用にPKCS#11モジュールを指定できます。

1. Citrix Receiverで**［基本設定］**を選択します。
2. ［基本設定］ウィンドウで**［詳細］**をクリックします。
3. PKCS#11フィールドで適切なモジュールを選択します。一覧に必要なモジュールがない場合は、**［その他］**をクリックしてPKCS#11モジュールの場所を参照します。
4. 適切なモジュールを選択したら、**［追加］**をクリックします。

サポートされるリーダー、ミドルウェア、およびスマートカードプロファイル

Receiver for Macは多くのMac OS X互換スマートカードリーダーおよび暗号化ミドルウェアをサポートします。Citrixは次の操作について検証済みです。

サポートされるスマートカードリーダー：

- 一般的なUSB接続スマートカードリーダー

サポートされるミドルウェア：

- Clariify
- Activeidentityクライアントのバージョン

- Charismathicsクライアントのバージョン

サポートされているスマートカード：

- PIVカード
- Common Access Card（CAC）

ユーザーデバイスを構成するため、ベンダーのMac OS X互換スマートカードリーダーおよび暗号化ミドルウェアにより提供された指示に従います。

制限事項

- 証明書は、ユーザーデバイス上ではなくスマートカード上に格納されている必要があります。
- Receiver for Macでは、ユーザーの選択した証明書が保存されません。
- Receiver for Macでは、ユーザーのスマートカードPINが格納または保存されません。PINの取得はオペレーティングシステムにより処理され、独自のキャッシングメカニズムがある場合があります。
- Receiver for Macでは、スマートカードが挿入されたときに自動的には切断セッションに再接続されません。
- スマートカード認証でVPNトンネルを使用するには、ユーザーがNetScaler Gateway Plug-inをインストールしてWebページ経由でログオンする必要があります。この場合、各手順でスマートカードとPINによる認証が必要になります。スマートカードユーザーは、NetScaler Gateway Plug-inを使用したStoreFrontへのパススルー認証を使用できません。

詳しい情報の参照先

以下の情報も参照してください。

- Configuring Citrix XenDesktop 7.6 andNetScaler Gateway 10.5 with PIV SmartCard Authentication（PDF）
- Smart Card Support with Citrix Receiver for Mac 11.9.15 on OS X 10.10.2

Receiver for Macのインストール、セットアップ、アップグレード、展開、または削除

Oct 31, 2016

Receiver for Macのこのリリースは単一のインストールパッケージCitrixReceiver.dmgで提供されており、NetScaler Gateway、Access Gateway、およびSecure Gatewayを使用したリモートアクセスをサポートしています。

ここでは次のことについて説明します。

- Receiver for Macの手動インストール
- Receiver for Mac 12.0へのアップグレード
- Receiver for Macの展開と構成について
- Receiver for WebサイトからのReceiverの配布
- Web Interfaceのログオン画面からのReceiverの展開
- Receiver for Macのアンインストール

インストール

Receiverは、次の方法でインストールできます。

- ユーザーによるCitrix.comからのインストール
  - Receiverを初めて使用するユーザーがReceiverのインストールファイルをCitrix.comなどのダウンロードサイトから入手した場合は、サーバーURLの代わりにメールアドレスを入力してアカウントをセットアップできます。これにより、メールアドレスに関連付けられたNetScaler GatewayやStoreFrontサーバーが識別され、ログオン用のメッセージが表示されてインストールを続行します。この機能は、メールベースのアカウント検出と呼ばれます。
    注：初めて使用するユーザーとは、デバイスにReceiverをインストールしていないユーザーを指します。
  - Citrix.com以外の場所（Receiver for Webサイトなど）からReceiverをダウンロードした場合は、メールアドレスによるアカウントセットアップを使用できません。
  - Receiverの構成が必要な環境では、ほかの方法でReceiverをユーザーに配布してください。
- Receiver for WebサイトまたはWeb Interfaceからの自動インストール
  - Receiverを初めて使用するユーザーがアカウントをセットアップするには、サーバーのURLを入力するかプロビジョニングファイルをダウンロードします。
- ESD（Electronic Software Delivery：電子ソフトウェア配信）ツールによるインストール
  - Receiverを初めて使用するユーザーがアカウントをセットアップするには、サーバーのURLを入力する必要があります。

Receiver for Macの手動インストール

ユーザーは、管理者が用意したWeb Interfaceやネットワーク共有を使用したり、Citrix社のWebサイト（http://www.citrix.com）からCitrixReceiver.dmgを直接ダウンロードしたりして、Receiverをインストールできます。

Receiver for Macをインストールするには

1. Citrix社のWebサイトから、適切なバージョンのReceiverのDMGファイルをダウンロードして開きます。
2. ［はじめに］ページで［続ける］をクリックします。
3. ［使用許諾契約］ページで［続ける］をクリックします。
4. 使用許諾契約の内容を確認して、［同意する］をクリックします。
5. ［インストールの種類］ページで、［インストール］をクリックします。
6. ローカルデバイスに管理者のユーザー名とパスワードを入力します。

Receiver for Mac 12.0へのアップグレード

Online Plug-in for Mac Version 10.xおよび11.xからのアップグレードがサポートされています。また、Receiver for Mac 11.3、11.4、11.5、11.6、11.7.x、11.8.x、および11.9.xからアップグレードすることもできます。

ShareFileとの統合機能は、バージョン11.8から削除されています。Receiver for MacとShareFileを統合した場合は、アップグレード時にShareFileアプリケーションのダウンロードを確認するメッセージが表示されます。このアプリケーションを使用して、引き続きリモートデータにアクセスできます。

Receiver for Macの展開と構成について

StoreFront環境：

- Citrix製品ドキュメントを参照して、NetScaler GatewayおよびStoreFront 2.xを構成してください。 StoreFrontにより作成されたプロビジョニングファイルをメールに添付して、アップグレード方法およびReceiverのインストール後にプロビジョニングファイルを開く方法をユーザーに通知します。
- プロビジョニングファイルを使用する代わりに、どちらかのNetScaler GatewayのURLを入力するようユーザーに指示します。 StoreFrontのドキュメントで説明されているメールアドレスによるアカウント検出を構成済みの場合は、自分のメールアドレスを入力するようにユーザーに指示します。
- また、Receiver for Webサイトを構成する方法もあります。詳しくは、StoreFrontのドキュメントを参照してください。Receiverのアップグレード方法、Receiver for Webサイトへのアクセス方法、Receiver for Webサイトからのプロビジョニングファイルのダウンロード方法（ユーザー名をクリックしてから［アクティブ化］をクリック）をユーザーに通知します。

Web Interfaceで展開する場合：

- Web InterfaceサイトをReceiver for Mac 11.9でアップグレードして、ユーザーにReceiverのアップグレード方法を通知します。 たとえば、ユーザーの［メッセージ］画面に、Receiverのアップグレードを確認するメッセージを表示できます。

Receiver for WebサイトからのReceiverの配布

ReceiverをReceiver for Webサイトからユーザーに配布すると、Webブラウザーからアプリケーションにアクセスするユーザーに確実にReceiverをインストールさせることができます。Receiver for Webサイトを使用すると、ユーザーはWebページを経由してStoreFrontストアにアクセスできます。Receiver for Webサイトで適切なバージョンのReceiverがインストールされていないことが検出されると、Receiverをダウンロードしてインストールするためのページが表示されます。詳しくは、StoreFrontのドキュメントを参照してください。

Web Interfaceのログオン画面からのReceiverの展開

Web Interfaceのログオン画面でReceiverをユーザーに配布すると、ユーザーがWeb Interfaceを使用する前に確実にReceiverをインストールさせることができます。Web Interfaceでは、Citrixクライアントソフトウェアを検出して必要に応じてインストールするための機能が提供されます。この機能により、ユーザーは自分の環境に適したソフトウェアをインストールできます。

管理者は、ユーザーがXenApp Webサイトにアクセスしたときに自動的にクライアント検出および展開処理が実行されるように構成できます。Web Interfaceで適切なバージョンのReceiverがインストールされていないことが検出されると、Receiverをダウンロードしてインストールするためのページが表示されます。

管理者は、ユーザーの［メッセージ］画面にインストール用の説明文およびリンクを表示することもできます。ユーザーがこのリンクをクリックすると、クライアント検出および展開処理が開始されます。また、この説明文を使用して、Citrixクライアントソフトウェアを最新バージョンにアップグレードするためのページにアクセスさせることもできます。

この機能を使用するには、Web Interfaceサーバー上にReceiverのインストールファイルを配置しておく必要があります。Web Interfaceのデフォルトでは、XenAppまたはXenDesktopのインストールメディアで提供されている名前でReceiverのイ

ンストールファイルが検索されます。ReceiverをCitrix社のWebサイトからダウンロードした場合、または以前のバージョンの Receiverを配布する場合は、XenApp Webサイトの構成ファイルのClientIcaMacパラメーターに適切なファイル名が指定されていることを確認してください。

詳しくは、Web Interfaceのドキュメントを参照してください。

Receiver for Macのアンインストール

Receiverをアンインストールするには、CitrixReceiver.dmgを開き、［Uninstall Citrix Receiver］をダブルクリックして、画面に表示される指示に従って操作します。

Receiver for Macの構成

Nov 13, 2015

ホストされているアプリケーションやデスクトップにユーザーがアクセスできるようにするには、Receiverソフトウェアをインストールした後で、以下の構成を行う必要があります。

- アプリケーション配信の構成 - XenApp環境を正しく構成します。オプションについて理解し、ユーザーに対しわかりやすいアプリケーションについての説明を提供します。
- セルフサービスモードの構成- セルフサービスモードを構成します。これにより、ユーザーがReceiverのユーザーインターフェイスからアプリケーションをサブスクライブできます。
- StoreFrontの構成 - このストアにより、XenDesktopサイトおよびXenAppファームからデスクトップとアプリケーションが列挙および集約され、これらのリソースをユーザーが使用できるようになります。
- ユーザーへのアカウント情報の提供- ユーザーがアカウントをセットアップするための情報を提供します。ユーザーは、このアカウントを使用してアプリケーションやデスクトップにアクセスします。環境によっては、ユーザーが手作業でアカウントをセットアップする必要があります。
- 外部から接続するユーザー（遠隔地からまたはインターネット経由で接続するユーザーなど）にアクセスを提供するには、NetScaler Gatewayを使用した認証を構成します。詳しくは、「Netscaler Gateway」を参照してください。

アプリケーション配信の構成

XenDesktopまたはXenAppでアプリケーションをユーザーに配信するときは、ストアのアプリケーションにアクセスするユーザーのエクスペリエンスを向上させるために、次のオプションについて検討します。

Webアクセスモード

いずれの構成を実行することなく、Receiver for Macではアプリケーションやデスクトップに対するブラウザーベースのアクセスであるWebアクセスを実行できます。Receiver for WebまたはWeb InterfaceサイトをWebブラウザーで開き、使用するアプリケーションを選択して実行するだけです。Webアクセスモードでは、ユーザーのデバイスのアプリケーションフォルダーにアプリケーションのショートカットが置かれます。

セルフサービスモード

StoreFrontアカウントをReceiverに追加したり、StoreFrontサイトをポイントするようにReceiverを構成したりして、セルフサービスモードを構成できます。これにより、ユーザーはReceiverを介してアプリケーションをサブスクライブできます。この拡張ユーザーエクスペリエンスはモバイルアプリケーションストアのものと同様です。セルフサービスモードでは、必要に応じて必須設定、自動プロビジョニング設定、お勧めのアプリケーションキーワード設定を構成できます。いずれかのユーザーがアプリケーションを選択すると、そのアプリケーションに対するショートカットがユーザーデバイスのアプリケーションフォルダーに置かれます。

StoreFront 3.0サイトにアクセスすると、Receiver Tech Previewユーザーエクスペリエンスを実行できます。Receiver Tech Previewユーザーエクスペリエンスについて詳しくは、「ReceiverおよびStoreFront 3.0 Technology Preview」を参照してください。

XenAppファームでアプリケーションを公開する場合、StoreFrontストアを介したアプリケーションへのユーザーアクセスの利便性を高めるため、公開アプリケーションについてわかりやすい説明を付加してください。この説明は、Citrix Receiverを介してユーザーに表示できます。

セルフサービスモードの構成

以前にも説明したように、StoreFrontアカウントをReceiverに追加したり、StoreFrontサイトをポイントするようにReceiverを構成したりして、セルフサービスモードを構成できます。これにより、ユーザーはReceiverのユーザーインターフェイスを

介してアプリケーションをサブスクライブできます。この拡張ユーザーエクスペリエンスはモバイルアプリケーションスト
のものと同様です。

セルフサービス モードでは、必要に応じて必須設定、自動プロビジョニング設定、お勧めのアプリケーションキーワード設定を構成できます。

- アプリケーションがストアのユーザー全員に自動的にサブスクライブされるようにするには、説明にKEYWORDS:Autoという文字列をXenAppでアプリケーションを公開するときに、説明として追加します。ユーザーがストアにログオンすると、そのアプリケーションを手動でサブスクライブしなくても自動的にプロビジョニングされます。
- アプリケーションの説明にという文字列を追加すると、そのアプリケーションがCitrix Receiverの[おすすめ] 一覧に表示され、ユーザーがそのアプリケーションを見つけやすくなります。

詳しくは、StoreFrontのドキュメントを参照してください。

XenApp展開環境のWeb Interfaceで、XenApp Servicesサイトを作成します。サイト名およびその作成方法は、インストールしているWeb Interfaceのバージョンにより異なります。詳しくは、Web Interfaceのドキュメントを参照してください。

StoreFrontの構成

StoreFrontで作成するストアは、Citrix Receiverのリソース配信インフラストラクチャと認証を提供するサービスにより構成されます。このストアにより、XenDesktopサイトおよびXenAppファームからデスクトップとアプリケーションが列挙および集約され、これらのリソースをユーザーが使用できるようになります。

1. StoreFrontをインストールして構成します。詳しくは、StoreFrontのドキュメントを参照してください。

   注：独自のReceiverダウンロードサイトを作成する管理者用に、テンプレートが提供されています。
2. XenAppやXenDesktopのアプリケーションと同様の手順で、CloudGateway用にストアを構成します。ユーザーのReceiver側で特別な設定を行う必要はありません。詳しくは、StoreFrontのドキュメントの「
   — ストアの構成
   」を参照してください。

ユーザーへのアカウント情報の提供

管理者は、ユーザーにアカウントの情報を提供します。ユーザーは、この情報を使用してアプリケーションやデスクトップにアクセスします。次の方法でユーザーに情報を提供できます。

- メールアドレスによるアカウント検出を構成する
- ユーザーにプロビジョニングファイルを提供する
- ユーザーにセットアップ用のURLを提供する
- アカウント情報をユーザーに手入力させる

メールアドレスによるアカウント検出を構成する

管理者は、メールアドレスによるReceiverアカウントの検出機能を構成できます。この機能を有効にした場合、ユーザーはReceiverの初期設定時にサーバーのURLの代わりに自分のメールアドレスを入力できます。DNS（Domain Name System）サービス（SRV）レコードにより、そのメールアドレスに関連付けられているNetScaler Gateway、Access Gateway、またはStoreFrontサーバーが自動的に検出され、ホストされているアプリケーションやデスクトップにアクセスするためのログオンを求めるメッセージが表示されます。

メールアドレスによるReceiverアカウントの検出機能が正しく動作するようにDNSサーバーを構成する方法については、StoreFrontドキュメントの「
— メールアドレスによるアカウント検出を構成する
」を参照してください。.

メールアドレスによるReceiverアカウントの検出機能が正しく動作するようにNetScaler GatewayやAccess Gatewayを構成する方法については、NetScaler GatewayまたはAccess Gatewayドキュメントの「
— Connecting to StoreFront by Using Email-Based Discovery
」を参照してください。

ユーザーにプロビジョニングファイルを提供する

管理者は、StoreFrontを使用して、接続の詳細情報を定義したプロビジョニングファイルを作成できます。作成したプロビジョニングファイルをユーザーに提供して、Receiverを自動的に構成できるようにします。Receiverをインストールした後で、提供されたファイルをユーザーが開くとReceiverが自動的に構成されます。Receiver for Webサイトを構成する場合は、そのサイトからユーザーにReceiverのプロビジョニングファイルを提供することもできます。

詳しくは、StoreFrontのドキュメントを参照してください。

ユーザーにセットアップ用のURLを提供する

管理者は、Citrix Receiver for Mac Setup URL Generatorを使用して、必要なアカウント情報を含んでいるURLを生成できます。Receiveをインストールした後で、管理者から提供されたURLをユーザーがクリックしてアカウントを構成し、リソースにアクセスできます。Setup URL Generatorユーティリティで生成したURLは、すべてのユーザーにメールで送信したりWebサイトに掲載したりできます。

アカウント情報をユーザーに手入力させる

ユーザーにアカウント情報を入力させる場合は、以下の情報を提供する必要があります。

- XenApp ServicesサイトやStoreFrontストアのURL。例：https://servername.example.com
- NetScaler GatewayまたはAccess Gatewayを使用する環境では、そのアドレスと製品エディション、および使用する認証方法
  NetScaler GatewayまたはAccess Gatewayの構成について詳しくは、「NetScaler Gateway」または「Access Gateway」のドキュメントを参照してください。

ユーザーが新しいアカウントの詳細を入力すると、Receiverにより接続が検証されます。検証に成功すると、そのアカウントにログオンするための画面が開きます。

Receiver for Mac環境の最適化

Nov 13, 2015

Receiverのパフォーマンスを最大限に引き出すには、以下の方法で環境を最適化します。

- ユーザーの自動再接続
- HDX Broadcastセッション画面の保持機能の提供
- ローミングユーザーのセッションの維持
- クライアント側デバイスのマッピング

ユーザーの再接続

ユーザーの自動再接続

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Receiverが検出して、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。再接続は、接続に成功するかユーザーがキャンセルするまで繰り返し試行されます。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。

管理者は、サーバーのポリシーを使用してHDX Broadcastのクライアント自動再接続機能を構成します。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。

デスクトップの再起動

仮想デスクトップで起動しない、接続に時間がかかる、または破損したなどの問題が生じた場合、ユーザーはそのデスクトップを再起動できます。管理者は、XenDesktopでこの機能を構成する必要があります。

ユーザーがサブスクライブしたデスクトップやユーザーの［アプリ］ページには、状況依存型のメニュー項目[再起動］が表示されます。デスクトップの再起動が無効に設定されている場合、このメニュー項目は使用できません。ユーザーが［再起動］を選択すると、Receiverがそのデスクトップをシャットダウンしてから起動します。

重要：デスクトップの再起動により、未保存のデータが失われる場合があることをユーザーに説明してください。

HDX Broadcastセッション画面の保持機能の提供

HDX Broadcastセッション画面の保持機能を有効にすると、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。セッション画面の保持を有効にしておくと、このような接続の中断時にセッション画面が表示されたままになり、接続が回復するまで維持されるようになります。

セッションに接続できないときに、ユーザーに警告ダイアログボックスが表示されるように構成できます。

管理者は、サーバーのポリシーを使用してHDX Broadcastセッション画面の保持機能を設定します。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。

Receiverのユーザーは、サーバー側のHDX Broadcastセッション画面の保持設定を変更できません。

重要：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。

ローミングユーザーのセッションの維持

ワークスペースコントロール機能を有効にすると、ユーザーがセッションの途中でデバイスを切り替えても、新しいデバイス上でそのデスクトップやアプリケーションでの作業を継続できます。これにより、たとえば病院で臨床医がほかのワークステーションに移動しても、移動先のデバイスでデスクトップやアプリケーションを起動し直す必要がなくなります。

ポリシーおよびクライアント側ドライブのマッピングの構成は、ユーザーがほかのデバイスに移動したときに、そのデバイスに適したものに自動的に切り替わります。ポリシーおよびマッピングの構成は、ユーザーがログオンするデバイスに応じて動的に適用されます。たとえば、医療従事者が緊急治療室のユーザーデバイスからログオフして、レントゲン室で別のワークステーションにログオンした場合、そのワークステーションでのセッション用に設定されたポリシー、プリンターマッピング、およびクライアント側ドライブマッピングが自動的に適用されます。

ワークスペースコントロール設定を構成するには

1. Receiverウィンドウで下向き矢印のアイコンをクリックして、［環境設定］を選択します。
2. ［一般設定］タブをクリックします。
3. 次のいずれかのオプションを選択します。
   - Receiverへのログオン時にアプリケーションに再接続する: ユーザーがReceiverを起動してログオンしたときに、切断セッションに再接続されます。
   - アプリケーションの起動時または更新時に再接続する: ユーザーがReceiverを起動したとき、およびCitrix Receiverのメニューで［アプリケーション一覧の更新］を選択したときに、切断セッションに再接続されます。

クライアント側デバイスのマッピング

Receiverでは、ローカルのドライブやデバイスがセッション内で自動的にマップされます。これにより、セッション内でクライアント側のドライブやデバイスにアクセスできるようになります。クライアント側デバイスのマッピング機能をサーバーで有効にすると、サーバー上で動作するリモートのアプリケーションやデスクトップで、ユーザーデバイスに接続されているローカルのデバイスを使用できるようになります。マシンの追加方法

- ローカルのドライブ、COMポート、およびプリンターにアクセスする。
- セッション内で、サーバー上のシステムサウンドやオーディオファイルを再生する。

クライアント側オーディオのマッピングおよびクライアント側プリンターのマッピングでは、ユーザーデバイス側での設定が不要です。

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を有効にすると、セッション内でユーザーデバイス上のローカルドライブ（CD-ROMドライブ、DVDドライブ、USBメモリスティックなど）にアクセスできるようになります。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。

Receiver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を監視して、セッション内で追加された新しいディレクトリを、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します。

ユーザーは、Receiverの［環境設定］を使用して、マップされたドライブに対する読み取りと書き込みアクセスを制御できます。

マップされたドライブの読み取りと書き込みアクセスを制御するには

1. Receiverのホームページで下向き矢印のアイコンをクリックし、［環境設定］を選択します。
2. ［デバイス］をクリックします。
3. 以下のいずれかのアクセスレベルを選択します。
   - 読み出し/書き込み
   - 読み取り専用
   - アクセスしない
   - 毎回確認する
4. 変更内容を適用するには、既存のセッションからログオフして、再接続します。

クライアント側COMポートのマッピング

クライアント側COMポートのマッピングを有効にすると、セッション内でローカルマシンのCOMポート上のデバイスにアクセスできるようになります。これらのマッピングはいずれかのほかのネットワークマッピング［毎回確認する］のように使用できます。

Macintoshのシリアルポートでは、Windowsアプリケーションで使用される一部の制御信号線が提供されません。具体的には、DSR（Data Set Ready）、DCD（Device Carrier Detect）、RI（Ring Indicator）、およびRTS（Request To Send）線がありません。これらの信号によりハードウェアハンドシェイクやフロー制御を行うWindowsアプリケーションでは、Macintoshのシリアルポートを使用できない場合があります。Macintoshのシリアル通信では、CTS（Clear To Send）とDTR（Data Terminal Ready）により入力および出力のハードウェアハンドシェイクが行われます。

クライアント側COMポートをマップするには

1. Receiverのホームページで下向き矢印のアイコンをクリックし、［環境設定］を選択します。
2. ［デバイス］をクリックします。
3. ［マップされたCOMポート］の一覧から、マップするCOMポートを選択します。これはセッション内で表示される仮想COMポートであり、ローカルマシン上の物理ポートではありません。
4. ［デバイス］列のポップアップメニューから、その仮想COMポートに割り当てるデバイスを選択します。
5. Receiverを起動して、サーバーにログオンします。
6. コマンドプロンプトを開きます。コマンドプロンプトで、次のコマンドを実行します。
   net use com: \\client\com:

   ここで、にサーバー側のCOMポート番号（ポート1～9）を指定し、にクライアント側のCOMポート番号（ポート1～4）を指定します。

7. 正しくマッピングされていることを確認するには、コマンドプロンプトでnet useを実行します。これにより、マップされたドライブ、LPTポート、およびCOMポートの一覧が表示されます。

Receiver for Macでのユーザーエクスペリエンスの向上

Nov 13, 2015

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。

- ClearTypeフォントスムージング
- クライアント側のマイク入力
- Windows特殊キー
- Windowsのショートカットやキーの組み合わせ
- IME（Input Method Editor）とインターナショナルキーボードレイアウトの使用
- 複数モニターの使用
- デスクトップツールバーの使用

ClearTypeフォントスムージング

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。

サーバー側でClearTypeフォントスムージングを有効にしても、ユーザーデバイスで強制的にClearTypeフォントスムージングが使用されるわけではありません。管理者がサーバー側でClearTypeフォントスムージングのサポートを有効にすると、ユーザーデバイス側でこの機能が有効な場合のみフォントスムージングが使用されます。

Receiverはユーザーデバイスのフォントスムージング設定を自動的に検出し、それをサーバーに送信します。セッションはこの設定を使って接続されます。セッションが切断または終了すると、サーバー側の設定が元に戻ります。

クライアント側のマイク入力

Receiverは、クライアント側の複数のマイク入力をサポートします。ユーザーは、ローカルのマイクを使用して以下の操作を実行できます。

- ソフトフォンでの通話やWeb会議などのリアルタイムのアクティビティ。
- ホストされている録音アプリケーション（ディクテーションプログラムなど）の使用。
- 録画と録音。

Receiverでは、デジタルディクテーションがサポートされます。サーバー上でのこの機能を構成する方法について詳しくは、XenAppおよびXenDesktopのドキュメントを参照してください。

ユーザーは、ユーザーデバイスに接続されたマイクをセッションで使用するかどうかを、Receiverの［環境設定］の［マイクとWebカメラ］タブで設定できます。

- マイクおよびWebカメラを使用する
- マイクおよびWebカメラを使用しない
- 毎回確認する

［毎回確認する］を選択すると、ホストされているアプリケーションやデスクトップに接続するたびに、そのセッションでマイクを使用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。

Windows特殊キー

Receiverには、MacキーボードでWindowsアプリケーションのファンクションキーなどの特殊キーを簡単に使用するための追加オプションが用意されています。［キーボード］タブでは、必要に応じて以下のオプションを選択できます。

- Ctrlキー用のショートカット：セッション内で、Ctrlキーと文字キーの組み合わせとして使用するMacキーボードの組み合わせを指定します。ここで［⌘（command）または⌃（control）］を選択すると、使い慣れたcommand+文字キーのMac

ショートカットをWindowsのCtrl+文字キーとして使用できます。［^（control）］を選択すると、control+文字キーをCtrl+文字キーとして使用できます。

- Altキー用のショートカット：セッション内で、Altキーとして使用するMacキーボードのキーを指定します。ここで［⌘⌥（command+option）］を選択すると、Macキーボードのcommand+option+文字キーを、WindowsのAlt+文字キーの組み合わせとして使用できます。［⌘（command）］を選択すると、commandキーをAltキーとして使用できます。
- ［Windowsロゴキーとして右側の⌘（command）を使用する］を選択すると、Macキーボードの右側にあるcommandキーをWindowsロゴキーとして使用できます。このオプションが無効な場合、右側のcommandキーは左側のcommandキーと同じように動作します。この場合、Windowsロゴキーを使用するには、［キーボード］メニューを使用します（［キーボード］>［Windowsショートカットを送信］>［スタート］）。
- ［特殊キーをそのまま送信する］チェックボックスをオンにすると、特殊キーの変換が無効になり、Macキーボードの操作がそのままセッションに送信されます。たとえば、optionキーとテンキーの1キーを一緒に押すと、セッションではF1キーに変換されます。ここで［特殊キーをそのまま送信する］チェックボックスをオンにすると、セッションでは1キーとして処理されます。このチェックボックスはデフォルトでオフになっており、option+1キーはF1キーに変換されます。

ファンクションキーやそのほかの特殊キーをセッション内で使用するときに、［キーボード］メニューを使用することもできます。

テンキーが付属しているキーボードでは、さらに以下のキー操作を使用できます。

PCキー	**Macキー操作**
挿入	テンキーの0キー0。Macキーボードのnum lockはオフである必要があります（オン/オフを切り替えるにはclearキーを使用します） option+help
Del	テンキーの小数点キー。Macキーボードのnum lockはオフである必要があります（オン/オフを切り替えるにはclearキーを使用します） Clear
F1～F9	option+1～9（テンキー）
F10	option+0（テンキー）
F11	option+テンキーの負符号（-）キー
F12	option+テンキーの正符号（+）キー

Windowsのショートカットやキーの組み合わせ

Macキーボードからのキーの組み合わせ（著作権記号「©」を入力するoption+Gキーなど）は、リモートセッションでも正しく処理されます。ただし、一部のキー操作は、リモートのアプリケーションやデスクトップで処理されず、Macオペレーティングシステム側で処理されます。この場合、そのキー操作によりMacオペレーティングシステムの機能がトリガーされます。

また、セッションでInsなど一部のキーを使用しようと思っても、通常のMacキーボードにこれらのキーはありません。Windows 8では、チャームやアプリコマンドを表示したり、アプリのスナップや切り替えを行ったりするための専用のショートカットがあります。本来、これらのショートカットはMacキーボードでは使用できませんが、［キーボード］メニューを使ってリモートのデスクトップやアプリケーションに送信できます。

キーボードやキー操作の構成は、デバイスにより大きく異なることがあります。このため、Receiverには、セッション内のアプリケーションやデスクトップにキー操作を正しく転送するためのオプションが用意されています。これらのオプションについては、下の表を参照してください。Receiverでのデフォルトの動作についても説明します。Receiverやそのほかの設定でデフォルトの動作を変更すると、リモートのデスクトップやアプリケーションに異なるキー操作が送信される場合があります。

重要：新しいMacキーボードでは、下の表に示す一部のキーの組み合わせを使用できない場合があります。この場合、これらのキー操作をセッションで使用するには、［キーボード］メニューを使用します。
下の表について、以下の点に注意してください。

- Macキーボードの特殊キーは小文字で示します（ファンクションキーを除くcontrol、command、optionなど）。また、英字キーは大文字で表記されていますが、Shiftキーを同時に押すという意味ではありません。
- キー名の間のプラス記号（+）は、それらのキーを同時に押すことを示します（control+Cなど）。
- 文字キーは、英数字および句読点のキーを指します。特殊キーは単独では文字を入力しない修飾キーや制御キーを指し、Ctrl（control）、Alt、Shift（shift）、command、option、方向キー、およびファンクションキーが含まれます。
- 使用するメニューは、そのセッションのCitrix Viewerメニューを指します。
- ユーザーデバイスの構成によっては、一部のキーの組み合わせが意図したとおりに機能しない場合があります。この場合、その代替操作を示します。
- fnキーはMacキーボードの修飾キーのうちの1つで、F1～F12キーはPCまたはMacキーボードの各ファンクションキーに相当します。

Windowsキー	**Macキー操作**
Alt+文字キー	command+option+文字キー（たとえば、セッションでＡｌｔ+Cキー操作を使用するには、command+option+Cを押します）
Alt+特殊キー	option+特殊キー（option+tabなど） command+option+特殊キー（command+option+tabなど）
Ctrl+文字キー	command+文字キー（command+Cなど） control+文字キー（control+Cなど）
Ctrl+特殊キー	control+特殊キー（control+F4など） command+特殊キー（command+F4など）
Ctrl/Alt/Shift/Windowsロゴ+ファンクションキー	［キーボード］メニューの［ファンクションキーを送信］>（control/option/shift/commandを押しながら）［F1～F12］
Ctrl+Alt	control-option-command

Windowsキー Ctrl+Alt+Delete	**Macキー操作** control+option+Forward Delete control+option+fn+delete（MacBookキーボード） ［キーボード］メニューの［Ctrl+Alt+Delを送信］
削除	削除 ［キーボード］メニューの［キーを送信］>［Del］ fn+backspace（一部のUSキーボードではfn+delete）
end	end fn+右方向キー
Esc	esc ［キーボード］メニューの［キーを送信］>［Esc］
F1～F12	F1～F12 ［キーボード］メニューの［ファンクションキーを送信］>［F1～F12］
ホーム	ホーム fn+左方向キー
Ins	［キーボード］メニューの［キーを送信］>［Ins］
NumLock	Clear
page down	page down fn+下方向キー
page up	page up fn+上方向キー
Space	［キーボード］メニューの［キーを送信］>［スペース］
ページ	［キーボード］メニューの［キーを送信］>［Tab］

Windowsキー	相当するCommandキー（Receiverのデフォルトのキーボード設定）
	［キーボード］メニューの［Windowsショートカットを送信］>［スタート］
チャームを表示するキー	［キーボード］メニューの［Windowsショートカットを送信］>［チャーム］
アプリケコマンドを表示するキー	［キーボード］メニューの［Windowsショートカットを送信］>［アプリコマンド］
アプリをスナップするキー	［キーボード］メニューの［Windowsショートカットを送信］>［スナップ］
アプリを切り替えるキー	［キーボード］メニューの［Windowsショートカットを送信］>［アプリの切り替え］

IME（Input Method Editor）とインターナショナルキーボードレイアウトの使用

Receiverでは、ユーザーデバイス（クライアント）側またはサーバー側のIME（Input Method Editor）を使用できます。

クライアント側IMEが有効な場合、ユーザーが入力する文字列は、別ウィンドウではなく入力ポイントに直接入力されます。

また、Receiverで使用するキーボードレイアウトを選択することもできます。

クライアント側のIMEを有効にするには

1. ［Citrix Viewer］メニューバーで、［キーボード］、［インターナショナル］、［クライアントIMEを使用］の順に選択します。
2. サーバー側のIMEが直接入力モードまたは半角英数モードになっていることを確認します。
3. Mac側のIME（入力プログラム）を使用して文字列を入力します。

IME入力時の確定前文字列の挿入ポイント（`）を表示するには

- ［Citrix Viewer］メニューバーで、［キーボード］、［インターナショナル］、［変換中マークを使用］の順に選択します。

サーバー側のIMEを使用するには

- クライアント側のIMEが半角英数モードになっていることを確認します。

サーバー側IMEの入力モードキーの割り当て

Receiverでは、サーバー側のWindows IMEで入力モードを切り替えるときに使用するキーが、特定のMacキーボードに割り当てられます。次の表は、サーバー側のシステムローケルの設定と、Macキーボードのoptionキーに割り当てられるWindows IMEの入力モードキーを示しています。

サーバー側システムロケール	サーバー側IMEの入力モードキー
日本語	漢字キー（日本語キーボードのAlt + 半角/全角）

韓国語ー側システムロケール	右Altキー側(韓国語キーボードの)ハングル/英語切り替え)

インターナショナルキーボードレイアウトを使用するには

- クライアント側およびサーバー側で、サーバー側のデフォルトの入力言語と同じキーボードレイアウトが設定されていることを確認してください。

複数モニターの使用

Receiver for Macのメニューオプションである **[フルスクリーンのすべてのディスプレイを使用する]** を使って、複数のモニターを使ったフルスクリーンモードを実行できます。

既知の制限事項

単一モニターのフルスクリーンまたはすべてのモニターを使ったフルスクリーンモードのみがサポートされています。これ
メニューアイテムを使って構成できます。

デスクトップツールバーの使用

ウィンドウモードおよびフルスクリーンモードのどちらでもデスクトップツーバーにアクセスできるようになりました。以
は、フルスクリーンモードでのみデスクトップツールバーが表示されていました。ツールバーには次のような変更が追加さ
ています。

- ツールバーから **[ホーム]** ボタンが削除されました。この機能は、次のコマンドを使って実行できます。
  - Cmd+Tabを押して、前のアクティブなアプリケーションに切り替えます。
  - Ctrl+左矢印を押して、前のスペースに切り替えます。
  - 内蔵のトラックパッドを使って、またはMagic Mouseのジェスチャーにより別のスペースに切り替えます。
  - フルスクリーンモード時に画面の端にカーソルを動かすと、アクティブにするアプリケーションを選択できるドックが表示されます。
- ツールバーから **[ウィンドウ]** ボタンが削除されました。フルスクリーンモードからウィンドウモードには次の方法により切り替えることができます。
  - OS X 10.10の場合、ドロップダウンメニューバーで緑色のウィンドウボタンをクリックします。  または 
  - OS X 10.7、10.8、および10.9の場合、ドロップダウンメニューバーで青色のメニューボタンをクリックします。 
  - OS Xのすべてのバージョンで、ドロップダウンメニューの **[表示]** メニューから **[フルスクリーンを解除]** を選択します。
- ツールバードラッグの動作が更新され、複数モニターを使ったフルスクリーンのウィンドウ間でのドラッグがサポートされています。

Receiver通信のセキュリティ保護

Mar 10, 2016

ここでは次のことについて説明します。

サーバーファームと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。

- Citrix NetScaler GatewayまたはCitrix Access Gateway。 これらのゲートウェイ製品とStoreFrontの構成について詳しくは、StoreFrontのドキュメントを参照してください。
  注：StoreFrontサーバーとユーザーデバイス間の通信を保護するには、NetScaler Gatewayを使用することをお勧めします。
- 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、Citrix Receiverとサーバー間の接続を制御できます。 Citrix 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 Secure GatewayをWeb Interfaceと一緒に使うと、社内ネットワーク上のサーバーにインターネットを介して接続できる、暗号化された安全な単一のアクセスポイントをユーザーに提供できます。
- Transport Layer Security（TLS）プロトコルによるSSL Relayソリューション
- 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。

証明書について

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警告が表示されます。 ユーザーが警告に対してそのまま続行することを選択した場合、アプリケーションの一覧が表示されますが、アプリケーションの起動に失敗します。

Receiver for Macデバイスへのルート証明書のインポート

証明書の発行者のルート証明書を取得して、デバイスに設定されているアカウントに電子メールで送信します。 添付ファイルをクリックすると、ルート証明書をインポートするかどうかを確認するメッセージが表示されます。

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。 Receiver for Macでは、ワイルドカード証明書がサポートされています。

中間証明書とAccess Gatewayまたは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Access GatewayまたはNetScaler Gatewayのサーバー証明書にマップする必要があります。 方法については、NetScaler Gatewayのドキュメントを参照してください。 Access Gatewayを使用する場合は、使用するAccess Gatewayのエディションに関するKnowledge Baseアーティクルを参照してください。

CTX114146：How to Install an Intermediate Certificate on Access Gateway Enterprise Edition

NetScaler GatewayまたはAccess Gateway Enterprise Editionによる接続

リモートのユーザーがNetScaler GatewayやAccess Gatewayを介してCloudGateway環境に接続できるようにするには、CloudGatewayのコンポーネントであるStoreFrontと通信するようにNetScaler GatewayまたはAccess Gatewayを構成します。 このアクセスを有効にする方法は、CloudGatewayのエディションによって異なります。

ネットワークCloudGateway Expressを展開する場合、NetScaler GatewayまたはAccess GatewayとStoreFrontを統合することでNetScaler GatewayまたはAccess Gatewayを経由して内部ユーザーやリモートユーザーがStoreFrontに接続できます。 ユーザーは、StoreFrontに接続してXenAppの公開アプリケーションやXenDesktopの仮想デスクトップにアクセスします。 ユーザーは、Citrix Receiverを使用して接続を行います。

NetScaler Gatewayでの構成について詳しくは、「Configuring NetScaler Gateway Settings with the Remote Access Wizard」を参照してください。 Access Gatewayでの構成について詳しくは、「Integrating Access Gateway with CloudGateway」を参照してください。

リモートのユーザーがAccess Gatewayを介してWeb Interface環境に接続できるようにするには、Web Interfaceと通信するようにAccess Gatewayを構成します。詳しくは、「Configuring Access Gateway Enterprise Edition to Communicate with the Web Interface」の各トピックを参照してください。

Secure Gatewayを経由する接続

このトピックの内容は、Web Interface環境にのみ適用されます。

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、Receiverとサーバーの間に保護された通信チャ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、Receiver側での構成は不要です。

ReceiverがSecure Gatewayサーバーに接続するときは、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。 Receiverに対するプロキシサーバー設定の構成について詳しくは、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。 リレーモードについて詳しくは、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、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.example.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（example）、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（example.com）をドメイン名といいます。

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するために使います。 Receiverは、SOCKSプロトコルとSecureプロキシプロトコルの両方をサポートしています。

ReceiverでXenAppサーバーまたはXenDesktopサーバーと通信する場合、Web Interfaceサーバー上でリモートで構成されているプロキシサーバー設定が使用されます。 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。

ReceiverでWebサーバーと通信する場合は、ユーザーデバイス上のデフォルトのWebブラウザーで構成されているプロキシサーバー設定が使用されます。 各ユーザーデバイス上のデフォルトのWebブラウザーで、プロキシサーバー設定を構成する必要があります。

ファイアウォールを介した接続

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。 ファイアウォールが使用されている環境では、ReceiverとWebサーバーおよびCitrix製品のサーバーとの通信がファイアウォールでブロックされないように設定する必要があります。 このためには、ユーザーデバイスとWebサーバー間のHTTPトラフィック（一般に標準HTTPポート80、またはセキュアなWebサーバーを使用している場合はポート443での通信）がファイアウォールを通過できるように設定します。 また、ReceiverとCitrix製品サーバー間の通信では、ポート1494とポート2598の受信ICAトラフィックがファイアウォールを通過できるように設定します。

ファイヤウォールによるネットワークアドレス変換（NAT：Network Address Translation）を使用している場合は、Web Interfaceを使って内部アドレスから外部アドレスおよびポートへのマッピングを定義できます。 たとえば、XenAppサーバーやXenDesktopサーバーに代替アドレスが設定されていない場合は、Web InterfaceからReceiverに代替アドレスが提供されるように設定できます。 これにより、Receiverでのサーバー接続で、外部アドレスおよびポート番号が使用されるようになります。 詳しくは、Web Interfaceのドキュメントを参照してください。

Secure Sockets Layer（SSL）Relayによる接続

Receiver for Mac 12.0をSecure Sockets Layer（SSL）Relayサービスと統合できます。これにより、Citrix ReceiverおよびXenApp/XenDesktop間のTLS接続のためTLS 1.0、1.1、および1.2と次の暗号をサポートします。

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- 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

Transport Layer Security（TLS）は、SSLプロトコルの最新の標準化バージョンです。 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。

Citrix SSL RelayによるセキュアなTLS通信では、デフォルトでサーバーのTCPポート443が使用されます。 Citrix SSL Relayは、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。ユーザーがTLS+HTTPSブラウズを選択した場合は、Citrix XML Serviceに転送します。

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機能が有効になっているReceiverとサーバー間の通信。
- サーバーファームのXenAppサーバーと、Web InterfaceのWebサーバーとの間の通信。

SSL Relayを構成して通信を保護したり、Web InterfaceサーバーでのTLS暗号化を構成したりする方法について詳しくは、XenAppおよびWeb Interfaceのドキュメントを参照してください。

> **注意**
>
> Citrix Receiver for Macは、プラットフォーム(OS X)の暗号化機能をReceiverとStorefrontの接続に使用します。

ReceiverのTLSの構成と有効化

TLSのセットアップは、以下の2つの手順で行います。

1. XenAppサーバー、XenDesktopサーバー、およびWeb Interfaceサーバー上でSSL Relayをセットアップし、必要なサーバー証明書を入手してインストールします。 詳しくは、XenAppおよびWeb Interfaceのドキュメントを参照してください。
2. ユーザーデバイス上で、ルート証明書をインストールします。

ユーザーデバイスへのルート証明書のインストール

TLS機能が有効になっているReceiverとサーバーファーム間の通信をTLSで保護するには、サーバー証明書の証明機関の署名を認証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。

Mac OS Xには約100の商用ルート証明書が付属していますが、ほかの証明書を使用する場合は、証明機関から証明書を入手して、それを各ユーザーデバイスにインストールします。

企業の方針によっては、ルート証明書のインストールはエンドユーザーではなく管理者が行う場合があります。 ルート証明書を簡単および確実にインストールするには、Mac OS Xのキーチェーンにその証明書を追加します。

ルート証明書をキーチェーンに追加するには

1. 証明書を含んでいるファイルをダブルクリックします。 これにより、キーチェーンアクセスが起動します。
2. ［証明書の追加］ダイアログボックスで、［キーチェーン］ポップアップメニューから以下のいずれかのオプションを選択します。
   - ログイン：現在のログインユーザーにのみ証明書が適用されます。

- システム：そのデバイスにログインするすべてのユーザーに証明書が適用されます。

3. ［OK］をクリックします。
4. ［認証］ダイアログボックスにパスワードを入力し、［OK］をクリックします。

ルート証明書がインストールされ、SSLが有効なすべてのアプリケーションで使用可能になります。

SSLポリシーについて

ここでは、Citrix Receiver for Mac Version 12.0でSSL経由のICAセッションのセキュリティポリシーを構成するための情報について説明します。 ICA接続に使用される一部のSSL設定をCitrix Receiverで構成できます。 これらの設定はユーザーインターフェイスに表示されません。変更するにはReceiverが動作するデバイス上でコマンドを実行する必要があります。

> ### 注意
>
> デバイスがOS Xサーバーなどのモバイルデバイス管理ソリューションで制御されている場合は、SSLポリシーはほかの方法でも管理できます。

SSLポリシーには以下の設定が含まれます。

SecurityComplianceMode。 ポリシーのセキュリティコンプライアンスモードを設定します。 SecurityComplianceModeを構成しない場合は、デフォルト値としてFIPSが使用されます。 この設定に適用できる値は以下のとおりです。

- **None**。 コンプライアンスモードは適用されません。
- **FIPS**。 FIPS暗号モジュールが使用されます。
- **SP800-52**。 NIST SP800-52r1コンプライアンスが適用されます。

SecurityComplianceModeをSP800-52に設定する： コピー

```
defaults write com.citrix.receiver.nomas SecurityComplianceMode SP800-52
```

SecurityAllowedTLSVersions。 この設定により、プロトコルネゴシエーション中に受け入れられるべきTLSプロトコルのバージョンが指定されます。 この情報は配列として表され、指定可能な値のどの組み合わせもサポートされます。 この設定を構成しない場合は、TLS10、TLS11、TLS12がデフォルト値として使用されます。 この設定に適用できる値は以下のとおりです。

- **TLS10**。 TLS 1.0プロトコルを許可することを指定します。
- **TLS11**。 TLS 1.1プロトコルを許可することを指定します。
- **TLS12**。 TLS 1.2プロトコルを許可することを指定します。

SecurityAllowedTLSVersionsをTLS 1.1およびTLS 1.2に設定する： コピー

```
defaults write com.citrix.receiver.nomas SecurityAllowedTLSVersions -array TLS11 TLS12
```

SSLCertificateRevocationCheckPolicy。 この機能により、Citrixサーバーの暗号化認証機能が強化され、クライアントとサーバーの間のSSL/TLS接続の全体的なセキュリティが向上します。 この設定により、OS Xクライアントでssl経由のリモートセッションを開くときに、所与の信頼されたルート証明機関を扱う方法を制御します。

この設定を有効にすると、サーバー証明書が失効していないかどうかがクライアントによりチェックされます。 証明書失効一覧のチェックには複数のレベルがあります。 たとえば、ローカルの証明書失効一覧だけがチェックされるようにクライアントを構成したり、ローカルおよびネットワーク上の証明書失効一覧がチェックされるように構成したりできます。 さらに、すべての証明書失効一覧で証明書の有効性が検証されたときのみユーザーがログオンできるように、証明書チェックを構成できます。

証明書失効一覧（CRL）チェックは、一部の証明書発行元によりサポートされる高度な機能です。 これにより、証明書の秘密キーの暗号化が危うくなったり、単にDNS名に予期しない変更があったりした場合に、管理者はセキュリティ証明書を失効させる、つまり失効日より前に無効にすることができます。

この設定に適用できる値は以下のとおりです。

- **NoCheck**。 証明書失効一覧をチェックしません。
- **CheckWithNoNetworkAccess**。 証明書失効一覧がチェックされます。 ローカルの証明書失効一覧のストアのみが使用されます。 すべての配布ポイントが無視されます。 証明書失効一覧の検索は、対象のSSL Relay/Secure Gatewayサーバーによって提示されるサーバー証明書の検証において重大な意味を持ちません。
- **FullAccessCheck**。 証明書失効一覧がチェックされます。 ローカルの証明書失効一覧のストアおよびすべての配布ポイントが使用されます。 証明書失効一覧の検索は、対象のSSL Relay/Secure Gatewayサーバーによって提示されるサーバー証明書の検証において重大な意味を持ちません。
- **FullAccessCheckAndCRLRequired**。 証明書失効一覧がチェックされますがルートCAは除外されます。 ローカルの証明書失効一覧のストアおよびすべての配布ポイントが使用されます。 すべての必要な証明書失効一覧の検索が検証において重大な意味を持ちます。
- **FullAccessCheckAndCRLRequiredAll**。 ルートCAを含め、証明書失効一覧がチェックされます。 ローカルの証明書失効一覧のストアおよびすべての配布ポイントが使用されます。 すべての必要な証明書失効一覧の検索が検証において重大な意味を持ちます。

> ### 注意
>
> SSLCertificateRevocationCheckPolicyを設定しない場合は、デフォルト値としてFullAccessCheckが使用されます。

SSLCertificateRevocationCheckPolicyをFullAccessCheckAndCRLRequredに設定する： コピー

```
defaults write com.citrix.receiver.nomas SSLCertificateRevocationCheckPolicy FullAccessCheckAndCRLRequired
```

SSLポリシーの構成

管理対象外のコンピューターでSSL設定を行使するには、Terminal.appで**defaults**コマンドを実行します。

defaultsはコマンドラインアプリケーションで、OS Xの環境設定plistファイルにアプリ設定を追加、編集、および削除するために使用できます。

設定を変更するには

1. ［アプリケーション］、［ユーティリティ］、［ターミナル］の順に選択します。
2. ターミナルで以下のコマンドを実行します。

   defaults write com.citrix.receiver.nomas

各オプションの意味は次のとおりです。

：前述のように設定の名前です。

：設定の種類を指定するスイッチで、-stringまたは-arrayのどちらかです。 設定の種類が文字列である場合はこれを省略できます。

：設定の値です。 値が配列で複数の値を設定する場合は、値をスペースで区切る必要があります。

次に例を示します。 コピー

```
defaults write com.citrix.receiver.nomas SecurityAllowedTLSVersions -array TLS11 TLS12
```

デフォルト構成へのリセット

設定をデフォルトに戻すには

1. ［アプリケーション］、［ユーティリティ］、［ターミナル］の順に選択します。
2. ターミナルで以下のコマンドを実行します。

   defaults delete com.citrix.receiver.nomas

各オプションの意味は次のとおりです。

：前述のように設定の名前です。

次に例を示します。 コピー

```
defaults delete com.citrix.receiver.nomas SecurityAllowedTLSVersions
```