



シンクライアント端末

Windows 10 接続 利用時の注意/制限事項

目次

1.	はじめに.....	3
2.	改訂履歴.....	4
3.	サポート対象機種.....	5
4.	評価におけるシステム構成.....	6
5.	USB 機器の利用における注意/制限事項.....	8
6.	US100d.....	9
6.1	US100d 注意/制限事項.....	9
7.	US300d.....	11
7.1	モジュールのアップグレード.....	11
7.2	Citrix Receiver と StoreFront 間のトランスポート.....	11
7.3	US300d の USB 機器利用における注意/制限事項.....	12
7.4	US300d 注意/制限事項.....	12
8.	US310e.....	14
8.1	モジュールのアップグレード.....	14
8.2	Citrix Receiver と StoreFront 間のトランスポート.....	14
8.3	ACS (Atrust Client Setup)の注意/制限事項.....	15
8.4	US310e の USB 機器利用における注意/制限事項.....	15
8.5	US310e 注意/制限事項.....	15

1. はじめに

本書はシンクライアント端末の管理者向けに記載された「シンクライアント端末 Windows 10 利用時の注意/制限事項」です。

本書に掲載されている情報は特定の条件において得られたものであり、記載以外の 注意/制限事項がないことを保証するものではありません。

2. 改訂履歴

改訂履歴

改版	改訂年月日	改訂内容
1.0	2016/04/08	新規作成
1.1	2016/06/13	US310e 用 Citrix Receiver のアップグレードに伴う記載内容の更新

3. サポート対象機種

本書は下記のシンクライアントをサポート対象として記載しています。

- US100d
- US300d
- US310e

4. 評価におけるシステム構成

本書は次のシステム構成で弊社が実施した評価結果に基づいて記載しています。

※ 下記に記載されているコンポーネントおよびシステム環境以外については未評価です。

シンクライアント

- US100d (WTOS 8.1_027) 英語版/日本語版
- US300d (BDB0.2231.15GB/BDB0.2231.16GB) 英語版/日本語版
 - リモートデスクトップ接続 6.3.9600 リモートデスクトッププロトコル 8.1 サポート ※1
 - Citrix Receiver 14.4.0.8014 ※1
 - VMware Horizon Client 3.5.2.30397 ※1
 - Internet Explorer 11.0.9600.18204 ※1
- US310e (1.20-INTL) 英語版/日本語版
 - リモートデスクトップ接続 6.2.9200 リモートデスクトッププロトコル 8.0 サポート
 - Citrix Receiver 14.4.1000.16 ※2
 - VMware Horizon Client 3.5.2.30397 ※2
 - Internet Explorer 10.0.9200.16384

※1. Wyse Device Manager (WDM) を利用してパッケージモジュールを配信

※2. Atrust Device Manager (ADM) を利用してパッケージモジュールを配信

仮想デスクトップ

RDP

- Windows 10 Enterprise 32bit 10.0.10240 ビルド 10240
10.0.10586 ビルド 10586

ICA

- Citrix XenDesktop 7.6
 - Citrix Studio 7.6.3.5029 ※1
 - Citrix Broker Service 7.6.3.5024 ※1
 - Citrix ConfigMgr WOL 7.6.3.5014 ※1
 - Citrix Host Service 7.6.3.5021 ※1
 - Citrix Machine Creation Service 7.6.3.5020 ※1
 - Citrix Monitor Service 7.6.3.5014 ※1
 - Citrix Monitor Service PowerShell snap-in 7.6.2.5014 ※1
 - Citrix グループポリシー管理 2.5.0.0 ※2
 - Citrix Director 7.6.300.2 ※2

- Citrix WMI Proxy Plugin 7.6.300.02 ※2
- Citrix XenDesktop PowerShell Module 7.6.2.5029 ※2
- Citrix StoreFront 3.0.1 ※2
- Citrix Desktop OS Virtual Desktop Agent x86 7.6.300.7020 ※2
- DesktopVDACoreWX86_7_6_305 ※3
- Citrix Licensing 11.12.1 Build 14100 ※4

※1. HotFix Pack 3

※2. Feature Pack 3

※3. DesktopVDACoreWX86_7_6_305.msp

※4. Feature Pack 1

PCoIP

- VMware Horizon 6.2.2
 - VMware Horizon 6 Connection Server 6.2.2.3508079
 - VMware Horizon 6 HTML Access 3.5.3.3508077
 - VMware Horizon View Agent 6.2.2.3526061

5. USB 機器の利用における注意/制限事項

USB デバイスは各製造ベンダーで異なるアーキテクチャを持っており、それらデバイスの利用はアプリケーション、ホストシステム、ネットワーク、ポリシー等に依存します。特定のデバイスに対して基本的な動作確認を行っておりますが、それらすべての詳細な組み合わせ(システムインテグレーション)の動作を保証するものではありません。USB デバイスを利用する場合は、システムインテグレーションとして必ず導入環境を想定した事前の詳細な検証、ベンチマークテストなどを実施し、システム導入にあつた PoC(Proof of Concept)策定の上ご利用ください。システム環境上、各種設定やシステム環境の組み合わせ上発生する事象の場合、システムインテグレーションとして、設定回避や運用回避などでシステム環境に合った利用を行う必要があります。ご使用になる場合は、必ず事前に運用環境に基づいた設定で十分な事前検証を行い、問題がないことを確認してご使用ください。

6. US100d

6.1 US100d 注意/制限事項

US100d から Windows 10 に接続した場合、以下の注意/制限事項があります。

- 1 US100d (WTOS Ver 8.1_027 以前)では TLS 1.1 および TLS 1.2 に未対応です。US100d は次期ファームウェアアップデートで TLS 1.1 および TLS 1.2 に対応予定です。
- 2 VMware Horizon 6.2 以降から、デスクトップゲスト OS として Windows 10 がサポートされていますが、VMware Horizon 6.2.1 以降はセキュリティ強化として SSL 3.0 がサポートされなくなり、デフォルトで、TLS 1.1 および TLS 1.2 が有効となっているため、US100d (WTOS Ver 8.1_027 以前)では接続することができません。
- 3 Citrix XenDesktop/XenApp で TLS 1.1 および TLS 1.2 が有効となっている環境に US100d (WTOS Ver 8.1_027 以前)では接続することができません。
- 4 VMware Connection Server で[ユーザーによるマシンのリセットを許可]の設定を有効に設定し、US100d からリセット操作を実行してもデスクトップゲスト OS はリセットされません。
- 5 Windows 10 の「スタートメニュー」→「シャットダウンまたはサインアウト」メニュー表示が不正になる場合があります。
- 6 ネットワークレベル認証以外からの接続も許可するように設定されている Windows 10 に対して、US100d からネットワークレベル認証を無効に設定した状態で接続すると接続に失敗します。US100d の設定でネットワークレベル認証を有効にして接続してください。
- 7 Citrix XenDesktop 環境で UDP でのオーディオリアルタイムトランスポート機能を有効に設定しても、Windows 10 に接続した場合は正常に動作しません。
- 8 Citrix XenDesktop 環境で仮想デスクトップ(VDA)を TLS 1.2 で暗号化する構成で構築している場合、US100d で仮想デスクトップに接続すると次のメッセージが表示され接続に失敗します。
[メッセージ内容]
"選択した Citrix SSL サーバーは、接続を受け入れていません。"
- 9 ICA セッションで Microsoft Edge の動作が遅い場合があります。この場合、Internet Explorer など別のブラウザをご利用ください。

- 10 Windows 10 のスタートメニューおよびすべてのアプリの画面表示に時間が掛かる場合があります。

7. US300d

7.1 モジュールのアップグレード

工場出荷状態の US300d にデフォルトインストールされているモジュールは次の通りです。

- Citrix Receiver 14.0.0.91
- VMware Horizon View Client 5.4.0.1219906
- リモートデスクトップ接続 (mstsc.exe) 6.2.9200.16398
- Internet Explorer 10.0.9200.16635

Windows 10 に接続するにあたり、モジュールを次のバージョンにアップグレードしてください。

- Citrix Receiver 14.4.0.8014
- VMware Horizon Client 3.5.2.30397
- リモートデスクトップ接続 (mstsc.exe) 6.3.9600
- Internet Explorer 11.0.9600.18204

※ 必要なモジュールのみをアップグレードする形でも問題ありません。

例：RDP 接続を利用している場合は Citrix Receiver、VMware Horizon Client のアップグレードは不要です。接続にブラウザを利用している場合は Internet Explorer も合わせてアップグレードしてください。

US300d のモジュールのアップグレードには WDM(Wyse Device Manager)の使用を推奨します。各モジュールの WDM 配信用パッケージは NEC サポートサイトにて公開予定です。

NEC サポートサイト： <http://jpn.nec.com/thinclient/support/index.html>

7.2 Citrix Receiver と StoreFront 間のトランスポート

Citrix Receiver 4.0 以降は SelfService Plugin を使用する(Store Service サイトに接続する場合、HTTPS(セキュア)プロトコルの使用が既定となっております。StoreFront 間の接続に HTTP プロトコルを使用する場合、アカウントの追加の「追加」ボタンクリック時に “HTTPS で始まる安全なサーバーアドレスを入力してください。” とメッセージが表示されサーバーアドレスを入力することができません。弊社では HTTPS(セキュア)プロトコルの使用を推奨しておりますが、以下の手順で HTTP プロトコルの使用を許可することができます。

1. FBWF を無効にします。
2. Administrator アカウントでログオンします。

3. 「ファイル名を指定して実行」ダイアログを起動して、「regedit」と入力し、レジストリエディターを起動します。
4. 下記レジストリを編集および登録します。
[HKEY_LOCAL_MACHINE¥Software¥Citrix¥Dazzle]
AllowAddStore="A"
[HKEY_LOCAL_MACHINE¥Software¥Citrix¥AuthManager]
ConnectionSecurityMode="Any" (REG_SZ) ← 本レジストリ値は手動で追加登録します。
5. FBWF を有効にします。

7.3 US300d の USB 機器利用における注意/制限事項

US300d は FBWF によりシャットダウン/再起動後すべての変更が破棄されます。そのため USB デバイスドライバのインストールも破棄され、起動時に毎回 USB デバイスドライバのインストールウィザードが起動します。USB デバイスドライバのインストール状態を US300d のシャットダウン/再起動後も保持させる場合は FBWF を無効に設定して使用ポートごとに USB デバイスドライバをインストールしてください。

7.4 US300d 注意/制限事項

US300d から Windows 10 に接続した場合、以下の注意/制限事項があります。

- 1 VMware Horizon 6.2 以降から、デスクトップゲスト OS として Windows 10 がサポートされていますが、VMware Horizon 6.2.1 以降はセキュリティ強化として SSL 3.0 がサポートされなくなり、デフォルトで、TLS 1.1 および TLS 1.2 が有効となっています。US300d は TLS 1.1 および TLS 1.2 の使用がデフォルトでは有効になっていないため手動で有効に設定する必要があります。有効に設定するには US300d の「スタートメニュー」→「コントロールパネル」→「インターネットオプション」→「詳細設定」タブ →「設定」→「セキュリティ」で、「TLS 1.1 の使用」および「TLS 1.2 の使用」にチェックを入れてください。本設定は US300d の FBWF を無効にして実施し、実施後は FBWF を再度有効にしてください。FBWF が有効の状態では実施されると US300d をシャットダウン、または再起動すると設定した内容が破棄されます。
- 2 VMware Connection Server で[ユーザーによるマシンのリセットを許可]の設定を有効に設定し、US300d からリセット操作を実行してもデスクトップゲスト OS はリセットされません。
- 3 Windows 10 の「スタートメニュー」→「シャットダウンまたはサインアウト」メニュー表示が不正になる場合があります。
- 4 Citrix で仮想デスクトップ(VDA)を TLS 1.2 で暗号化する構成で構築し[セッション画面の保持]が有効に設定されている場合、ICA セッションが切断されるとセッションに自動再接続される動作になりますが、自動再接続時に仮想デスクトップでブルースクリーンが発生するため自動再接続に失敗します。

- 5 ICA セッションで Microsoft Edge の動作が遅い場合があります。この場合、Internet Explorer など別のブラウザをご利用ください。
- 6 ICA セッションで Flash リダイレクションが動作しません。
- 7 ICA セッションで デスクトップコンポジションリダイレクトが動作しません。
- 8 Windows 10 のスタートメニューおよびすべてのアプリの画面表示に時間が掛かる場合があります。
- 9 Citrix Receiver から StoreFront の統合エクスペリエンスに接続後の UI 操作時に、スクリプトエラーが発生する場合があります。

8. US310e

8.1 モジュールのアップグレード

工場出荷状態の US310e にデフォルトインストールされているモジュールは次の通りです。

- Citrix Receiver 14.2.0.10
- VMware Horizon View Client 3.2.0.24246
- リモートデスクトップ接続 (mstsc.exe) 6.2.9200.16384
- Internet Explorer 10.0.9200.16384

Windows 10 に接続するにあたり、モジュールを次のバージョンにアップグレードしてください。

- Citrix Receiver 14.4.1000.16
- VMware Horizon Client 3.5.2.30397

※ 必要なモジュールのみをアップグレードする形でも問題ありません。

例：RDP 接続を利用している場合は 本アップグレードは不要です。

US310e のモジュールのアップグレードには ADM(Atrust Device Manager)の使用を推奨します。各モジュールの ADM 配信用パッケージは NEC サポートサイトにて公開予定です。

NEC サポートサイト： <http://jpn.nec.com/thinclient/support/index.html>

※ US310e Citrix 配信パッケージは下記 2 種類の ADM 配信用パッケージを公開予定です。

- SSON 機能有り："/includeSSON" オプション有りで Citrix Receiver 14.4.1000.16 をインストールする。
- SSON 機能無し："/includeSSON" オプション無しで Citrix Receiver 14.4.1000.16 をインストールする。

※ NEC サポートサイトで公開予定の Citrix Receiver 14.4.1000.16/VMware Horizon Client 3.5.2.30397 の ADM 配信用パッケージは FW 1.10-INTL へは適用できません。初めに US310e のファームウェアを FW 1.20-INTL へバージョンアップした後、Citrix Receiver 14.4.1000.16/VMware Horizon Client 3.5.2.30397 の ADM 配信用パッケージを適用してください。

8.2 Citrix Receiver と StoreFront 間のトランスポート

Citrix Receiver 4.0 以降は SelfService Plugin を使用する(Store Service サイトに接続する場合、HTTPS(セキュア)プロトコルの使用が既定となっております。StoreFront 間に HTTP プロトコルを使用する場合、「アカウントの追加」時に "HTTPS で始まる安全なサーバーアドレスを入力してください。" とメッセージが表示され入力できません。弊社では HTTPS(セキュア)プロトコルの使用を推奨しますが、以下の手順で HTTP プロトコルの使用を許可することができます。

す。

1. UWF を無効にします。
2. Administrator アカウントでログオンします。
3. 「ファイル名を指定して実行」ダイアログを起動して、「regedit」と入力し、レジストリエディターを起動します。
4. 下記レジストリを編集および登録します。

```
[HKEY_LOCAL_MACHINE¥Software¥Wow6432Node¥Citrix¥Dazzle]
```

```
AllowAddStore="A"
```

```
[HKEY_LOCAL_MACHINE¥Software¥Wow6432Node¥Citrix¥AuthManager]
```

```
ConnectionSecurityMode="Any" (REG_SZ) ← 本レジストリ値は手動で追加登録します。
```

5. UWF を有効にします。

8.3 ACS (Atrust Client Setup)の注意/制限事項

US310e から XenApp/XenDesktop の仮想化リソースへ接続する方法には、Citrix Receiver 既定のインターフェース (SelfService Plugin、ウェブブラウザ)を使用する方法と、ACS(Atrust Client Setup)を使用する方法があります。ACS(Atrust Client Setup)を使用する場合は、以下の点に注意してください。

- ACS の ICA 接続ショートカットは XenApp/XenDesktop 7.6 以降のセッションへの接続に非対応です。XenApp/XenDesktop 7.6 以降のセッションに接続する場合は Citrix Receiver を使用してください。

8.4 US310e の USB 機器利用における注意/制限事項

US310e は UWF によりシャットダウン/再起動後すべての変更が破棄されます。そのため USB デバイスドライバーのインストールも破棄され、起動時に毎回 USB デバイスドライバーのインストールウィザードが起動します。USB デバイスドライバーのインストール状態を US310e のシャットダウン/再起動後も保持させる場合は UWF を無効に設定して使用ポートごとに USB デバイスドライバーをインストールしてください。

8.5 US310e 注意/制限事項

US310e から Windows 10 に接続した場合、以下の注意/制限事項があります。

1. VMware Connection Server で[ユーザーによるマシンのリセットを許可]の設定を有効に設定し、US310e からリセット操作を実行してもデスクトップゲスト OS はリセットされません。
2. Windows 10 の「スタートメニュー」→「シャットダウンまたはサインアウト」メニュー表示が不正になる場合があります。

- 3 Citrix で仮想デスクトップ(VDA)を TLS 1.2 で暗号化する構成で構築し[セッション画面の保持]が有効に設定されている場合、ICA セッションが切断されるとセッションに自動再接続される動作になりますが、自動再接続時に仮想デスクトップでブルースクリーンが発生するため自動再接続に失敗します。
- 4 ICA セッションで Microsoft Edge の動作が遅い場合があります。この場合、Internet Explorer など別のブラウザをご利用ください。
- 5 ICA セッションで Flash リダイレクションが動作しません。
- 6 ICA セッションで デスクトップコンポジションリダイレクトが動作しません。
- 7 Windows 10 のスタートメニューおよびすべてのアプリの画面表示に時間が掛かる場合があります。

シンクライアント端末
Windows 10 接続 利用時の注意/制限事項

2016 年 6 月 第 1.1 版

日 本 電 気 株 式 会 社
東京都港区芝五丁目 7 番 1 号
TEL (03) 3454-1111 (大代表)

© NEC Corporation 2016

日本電気株式会社の許可なく複製・改変などを行うことはできません。