JBAT

Secure Terminal

Win10版

ユーザーズ・ガイド

Version 1.0.1

一般的な注意

1. 本書の内容の一部または全部の無断転載・無断複写を禁止します。
2. 本書の内容は予告無しに変更することがあります。
3. 運用した結果の影響につきましては、本書の内容に関わらず、責任を負いかねますのでご了承ください。
4. 本書によって、工業所有権その他の権利の実施に対する保証、または実施権を許諾するものではありません。また、本書の掲載内容の使用により起因する工業所有権の諸問題については、当社は一切その責任を負うことはできません。
5. 製品内部の改造が行われた場合、当社は一切責任を負うことはできません。

商標について

本書中、以下は各社の商標または登録商標です。

Microsoft、Windows、Internet Explorer は、米国Microsoft Corporationの米国及びその他の国における登録商標または商標です。
Citrix、Citrix XenApp、Cirtix MetaFrame 、ICA、Citrix Presentation Server は Citrix Systems, Incの商標または登録商標です。
VMware、VMware Horizon、VMware Horizon Clientは米国VMware,Incの米国およびその他の地域における VMware 商標および登録商標です。
IBM は IBM Corporationの米国およびその他の国における商標です。

その他、本資料に記載の各名称は一般に各社の商標または登録商標です。

第 1.0.1 版 2021 年 7 月

このマニュアルは、製品の改良その他により適宣改訂されます。

はじめに

この度は、*SecureTerminal* Win10版をお買い上げ頂きましてありがとうございます。
本マニュアルは、*SecureTerminal* Win10版用のものです。当社から新たなマニュアルが提供されるまでは、本書が適用されます。
なお、本書内では *SecureTerminal* Win10版は以降、クライアント又は本製品と表記します。

本書が適用される機種は以下の通りです。

- *SecureTerminal* T8175 シリーズ
- *SecureTerminal* T8286 シリーズ
-

目　次

1章　概要

1.1　製品概要

SecureTerminal Win10 版は、Windows 10 IoT Enterprise 搭載のシンクライアント端末です。Microsoft RDP(Remote Desktop Protocol)、Microsoft Internet Explorer などの複数のクライアントソフトウェアが標準で組み込まれています。

このユーザーズ・ガイドでは、*SecureTerminal* Win10 版共通の使用方法について説明しています。

このマニュアルで説明している Windows 上での操作は、*SecureTerminal* で実装されている Windows 上のユニークな設定項目や機能についてのみとなります。

その他の Windows 上の操作は一般的な PC 上の Windows 10 と同様です。
これらの操作に関しましてはマイクロソフト社の資料や出版物を参照してください。

個々の製品におけるハードウェアの概要、各部名称などについては、各製品同梱のクイックスタートガイドを参照してください。また、このユーザーズ・ガイドでは、ホストエミュレーターを除くクライアントソフトウェアについて説明しています。
ホストエミュレーターに関しては、次の各ホストエミュレーターのユーザーズ・ガイドを参照してください。

1. TermPro をご使用の場合：「*SecureTerminal*：TermPro ユーザーズ・ガイド」
2. FALCON をご使用の場合：「*SecureTerminal*：FALCON for APTi ユーザーズ・ガイド」

これらのユーザーズ・ガイドは、当社ホームページからダウンロードできます。

1.2　ファイルシステム

DOM（Disc on Module :以下フラッシュディスクと記述）領域は、OS 領域として C:ドライブに割り当てられています。　また RAM 領域の一部は Z:ドライブに RAM ディスク(仮想ディスク)として割り当てられています。実メモリーを仮想ディスクとして割り当てているため、実際に利用可能な領域は、実際の実メモリーより少なくなります。

1.2.1 フラッシュディスク (C:)

フラッシュディスク(C:) には、オペレーティングシステム（Windows 10 IoT Enterprise）と標準で搭載されている各種アプリケーションが格納されています。フラッシュディスクは、管理者権限を持つアカウント以外がログインした場合には、通常書き込み保護されており、書き換えができません。管理者権限を持つアカウントでログインした場合は、Windows 10 で動作する一部のアプリケーションやデバイスドライバーなどをインストールすることが可能です。なお、出荷時での空き容量は機種によって異なりますのでご注意ください。
アプリケーションやドライバーの導入に際しては、「3.1　新規アプリケーションのインストール」を参照してください。

1.2.2　一時RAMディスク(Z:)

一時RAMディスク(Z:)は、RAMを仮想ディスクとして割り当てているため、クライアントの電源をOFFまたは、再起動すると消去されます。保存する必要のあるデータはこのドライブを使用しないで下さい。 フラッシュディスクに恒久的に保存する必要のない、各種アプリケーションの一時ファイルやインターネットの一時キャッシュなどに使用します。
詳しい設定方法は、「2.3.6　RAM ディスクのプロパティ」を参照してください。

1.2.3 ネットワークドライブ

ネットワークドライブを使用する場合は、Administrator または管理者特権を持つアカウントでログインする必要があります。

2章　起動と環境設定

本章ではアカウントのログオン方法および基本的な環境設定方法について説明しています。
ネットワークケーブルのプラグを LAN コネクタに接続すると、DHCP サーバーを使用して自動的に起動します。

2.1 ログオンアカウント

工場出荷時にはビルトイン・アカウントとして "Admin" と "User" の 2 種のログオン可能なアカウントが初期値で設定されています。 "Admin" にてログオンすると、すべての環境設定を行うことができます。
"User" でログオンすると、インストールされたソフトウェアを使用することはできますが、環境設定などの変更をすることはできません。
この "User" アカウントへの制限により、機能を損なう恐れのある OS への変更を防止し、ウィルスによる障害やソフトウェアの誤ったインストールを防ぎます。

2.2 ログオン

出荷値の状態では、以下のアカウントが既に設定されています。

初期アカウント	アカウント名	パスワード*	権限
Admin	***Admin***	***Admin***	管理者権限アカウント
User	***User***	***User***	制限ユーザーアカウント

* パスワードは大文字と小文字を区別します。

出荷時設定では "User" で自動ログオンが設定されていますので、環境設定を行う場合は、"User" をログオフしてから、"Admin" でログオンしなおしてください。
自動ログオンを取り消すには、『2.3.1 自動ログオンユーザー』を参照してください。
セキュリティー上、ご購入後は "Admin" のパスワードを変更してください。また、運用管理を容易にするために、同じグループの "Admin" のパスワードはなるべく同じ設定にしておくことを推奨します。

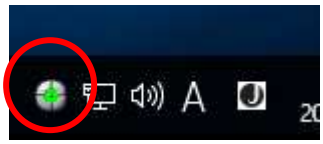
重要：
***SecureTerminal* XPE 版や *SecureTerminal* WES2009 版とはフラッシュディスクへの書込みの仕様が異なっています。設定変更を保存したい場合、必ずフラッシュディスクへの書込み（保存）が可能な状態（UWF フィルターの現在の状態が「無効」）であることを確認してから行ってください。**

2.3 WES 管理

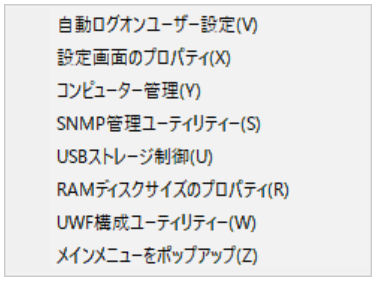
タスクトレイにある WES 管理アイコンにマウスポインタを合わせて、マウスの右クリックをすると、下記の管理メニューが表示されます。このアイコンは管理者権限を持つアカウントでログオンした場合にのみ表示されます。

① *SecureTerminal* の電源を立ち上げ、”Administrator” でログオンします。
もし事前に別ユーザー名でログオンしている場合には、必ずシステムを再起動させてからログオンしなおしてください。

② 画面右下のタスクトレイから WES 管理アイコン を右クリックします。



③ 下記の WES 管理のサブメニュー画面が表示されます。



また、上記のサブメニューの中から一番下の『メインメニューをポップアップ』を選ぶと下記の WES 管理メニューウィンドウが表示されますが、メニュー内容は同じです。

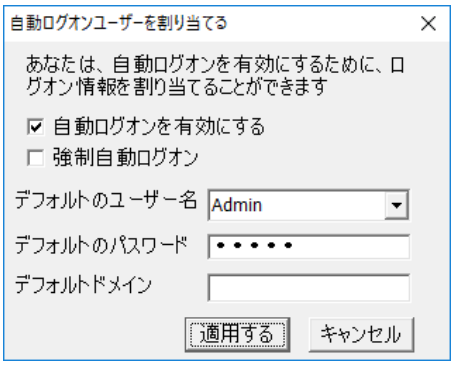
一部機能は設定を保存する必要があるため、フラッシュディスクへの書込み（保存）が可能な（現在のライトフィルタ=「無効」）状態のときのみ有効になりますのでご注意ください。

以下では、これらの各メニューを使用する場合の設定方法・手順について説明しています。

2.3.1　自動ログオンユーザー

自動ログオンや強制ログオンするアカウント（ユーザー）を選択します。
初期値は、 デフォルト・ユーザー名が "User"（制限ユーザーアカウント）の自動ログオンが設定されています。

重要：
***SecureTerminal* XPE 版や *SecureTerminal* WES2009 版とはフラッシュディスクへの書込みの仕様が異なっています。設定変更を保存したい場合、必ずフラッシュディスクへの書込み（保存）が可能な（現在のライトフィルタ=「無効」）状態であることを確認してから行ってください。**



『自動ログオン許可』 チェックボックス：
　自動ログオンを特定のユーザーアカウントに許可する場合に使用します。

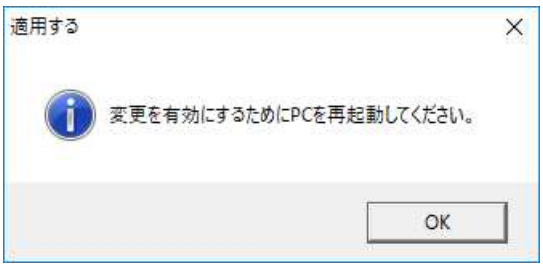
- チェックする：デフォルト・ユーザーで指定したアカウント（ユーザー）で自動ログオンします。
- チェックしない：起動時にログオン画面が表示され、アカウント名とパスワードを要求します。

『自動ログオン強制』 チェックボックス：
　デフォルト・ユーザーのアカウントで強制的にログオンさせたい場合に使用します。
　このチェックボックスは『自動ログオン許可』を設定したときのみ設定が可能です。

- チェックする：ユーザーがログオフ操作を行っても、デフォルト・ユーザーで指定したアカウント（ユーザー）で強制的に立ち上がります。
- チェックしない：ログオン強制はおこなわれず、自動ログオンだけが有効になります。

強制ログオンを解除したい場合は、ログオフ時にシフトキーを押しながら操作してください。ログオン画面が表示されます。

なお自動ログオンユーザーの設定を変更する場合には再起動が必要となるため、下記の画面が表示されますので、『OK』ボタンをクリックしてください。

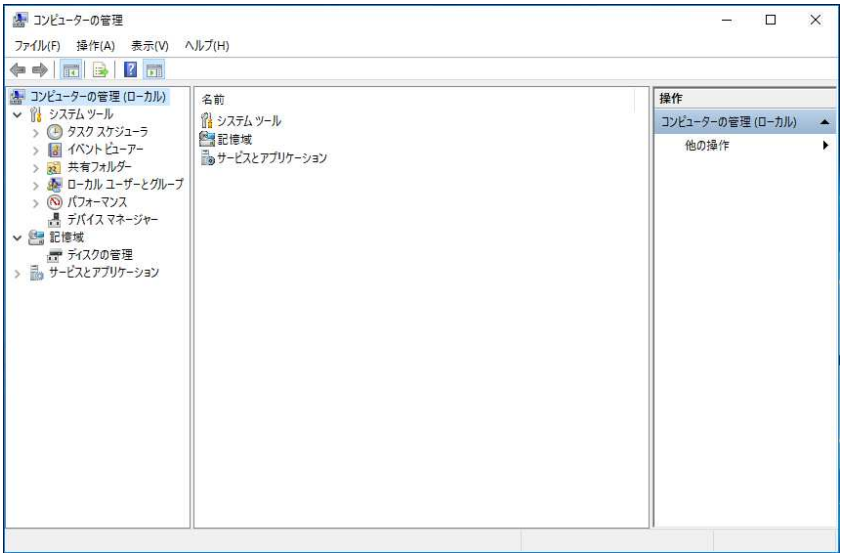


2.3.2　ディスプレイのカスタマイズ

Win10 版標準の『設定 – ディスプレイのカスタマイズ』画面が表示されます。
設定方法は一般の Windows 10 と同様です。

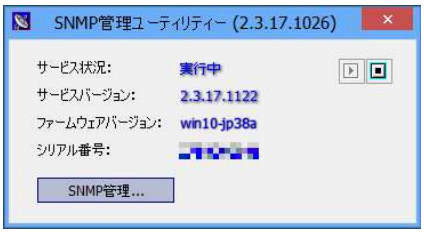
2.3.3　コンピューターの管理

Win10 版標準の『コンピューターの管理』ダイアログボックスが表示されます。
設定方法は一般の Windows 10 と同様です。



2.3.4　SNMP管理ユーティリティー

ファームウェアのバージョンやシアル番号を表示します。



『SNMP 管理...』ボタンをクリックすると、次の『SNMP 管理』ダイアログボックスが表示されます。

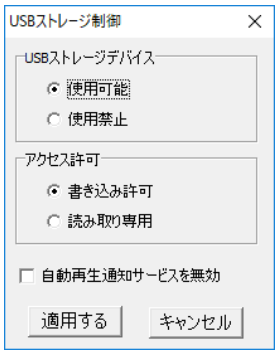
SNMP Administrator 管理ソフトウェア上で *SecureTerminal* の状況を表示させる場合、ここで設定した『Community』情報は、SNMP Administrator 管理ソフトウェア上で設定する『SNMP コミュニティ』と一致させておく必要があります。詳しくは SNMP Administrator 管理ソフトウェアのユーザーズ・ガイドを参照してください。
工場出荷時のデフォルトは『Public』が設定されています。

また、ここで設定した『端末』の『ロケーション』や『フィールド』情報（テキスト情報）は SNMP Administrator 管理ソフトウェア上で参照（表示）することができます。
設置場所や使用者情報などを入力しておくと、リモート管理時に参考になります。

2.3.5　USBストレージ制御

SecureTerminal に接続する USB ストレージデバイス（USB メモリー）のアクセス制御の設定を行います。
管理者権限を持つアカウントで設定/変更を行うことができます。
設定はすべてのアカウントに対して有効になります。

重要：
設定を保存する必要があるため、この設定はフラッシュディスクへの書込み（保存）が可能な（UWF フィルターの現在の状態が「無効」）状態の時にしか選択できません。



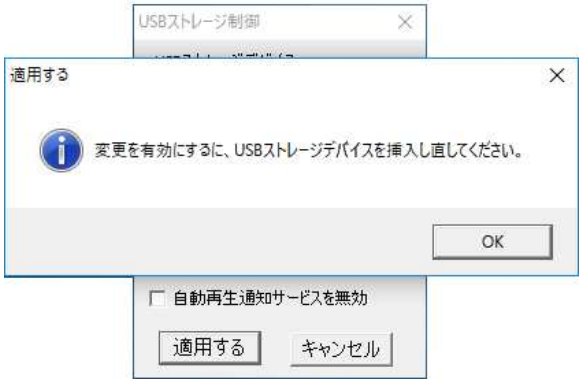
『デバイスの利用』
USB ストレージデバイスに対するアクセス制限の有効・無効を設定します。

- 『有効』：USB ストレージデバイスを使えるようにします。（工場出荷時）
- 『無効』：USB ストレージデバイスの利用を禁止します。

『アクセス許可』
アクセス許可の制限範囲を設定します。
このボックスは『USB ストレージデバイス』を『有効』設定したときのみ有効になります。

- 『読み書き許可』：データの読み取り、および書き込みの両方を許可します。（工場出荷時）
- 『読み取り専用』：データの読み取りのみ許可します。

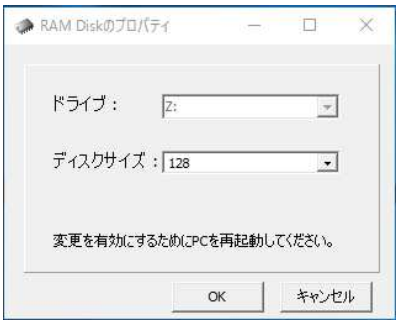
『オートプレイを無効にする』 チェックボックス：
接続した USB デバイスに対し、オートプレイの通知に対するオン・オフ設定をおこないます。



2.3.6　RAMディスクのプロパティ

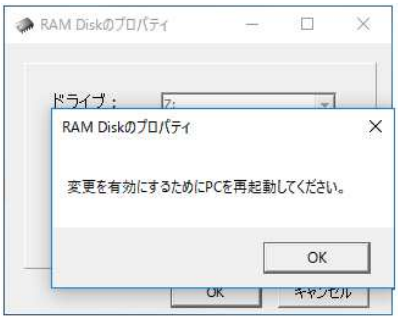
RAM ディスク（Z:ドライブ）の容量を変更します。工場出荷値は 128MB です。

重要：
設定を保存する必要があるため、この設定はフラッシュディスクへの書込み（保存）が可能な（UWF フィルターの現在の状態が「無効」）状態の時にしか選択できません。



ドライブ名は『Z:』(Z ドライブ) 固定で、変更できません。
設定できるディスクサイズは、4/ 8/ 16/ 24/ 32/ 48/ 64/ 96/ 128/ 256/ 512/ 1024 (MB)です。

RAM ディスクの設定を変更する場合には再起動が必要です。
下記の画面が表示されますので、『OK』ボタンをクリックしてください。



2.3.7　UWF構成ユーティリティー

SecureTerminal XPE 版、WES2009 版では、管理者権限を持つアカウントでログオンした時に、変更した内容がシャットダウン時にフラッシュディスクへ書き込まれる仕様になっていましたが、*SecureTerminal* Win10 版ではログオンしているアカウントに関係なく以下の状態のとき、シャットダウン時に書込み処理を行います。

- UWF 構成ユーティリティーで UWF フィルターの現在の状態が「無効」に設定されている状態のとき
- UWF 構成ユーティリティーのファイル除外設定で指定されているファイル・フォルダー
- UWF 構成ユーティリティーのレジストリ除外設定で指定されているレジストリ

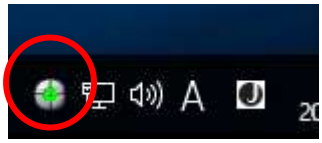
したがって、アプリケーションソフトの導入などフラッシュディスクへの書込み（保存）を行いたい場合は、事前に ”Admin” でログオンし、UWF フィルターを無効にしてから作業を行ってください。

重要：
この設定は管理者権限を持つアカウントでのみ行えます。
XPE 版、WES2009 版と異なり、フラッシュディスクへの書込みができる状態に設定した場合、ログオンするすべてのユーザーでディスクへの書込みができるようになります。

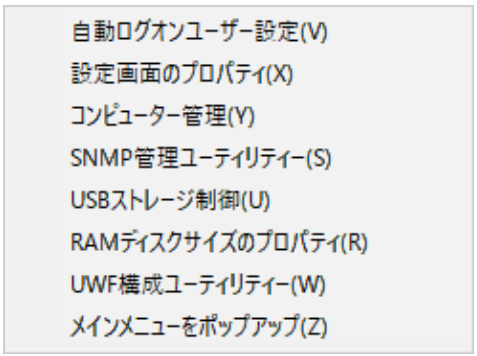
ディスクへの書込みができる状態で使用し続けることは、セキュリティーの観点からおすすめしません。
アプリケーションのインストールや設定変更を保存したら、すぐに UWF フィルターを有効にお使いください。

UWF フィルターを無効にしてフラッシュディスクへ書込めるようにするには、以下の手順で設定します。

① *SecureTerminal* の電源を立ち上げ、”Admin” でログオンします。
② タスクトレイから「WES 管理」アイコンを右クリックします。



③ 下記（左）の WES 管理のポップアップメニューから「UWF 構成ユーティリティー」を選択するか、「メインメニューの表示」を選んで「メインメニュー」を表示させ、「UWF 構成ユーティリティー」を選択します。



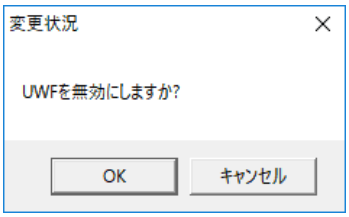
④ 下記の「統合書込みフィルター(UWF)構成ユーティリティー」の設定画面が表示されます。

『UWF フィルター』
次回起動時のフラッシュディスクへの書込みの有効・無効を設定します。

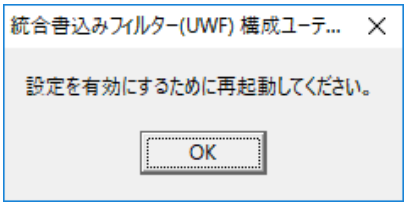
- 『有効』：フラッシュディスク保護状態です。シャットダウン時に書込みは行いません。
- 『無効』：シャットダウン時に変更を書込み保存します。

⑤ DOM への書込み（保存）ができるようにするためには、FBWF Status の現在の状態を「無効」にする必要がありますので、FBWF Status の「変更」ボタンをクリックします。

⑥ 下記の確認メッセージが表示されますので、「OK」ボタンをクリックしてください。



⑦ 下記のメッセージが表示されますので、「OK」ボタンをクリックして再起動してください。
OS 再起動後、DOM への書込み（保存）ができるようになります。



3章 アプリケーション

本章では新規にアプリケーションおよびデバイスドライバーをインストールする方法、および本製品に標準で組み込まれているアプリケーションについて説明しています。

3.1 新規アプリケーションのインストール

新しいアプリケーションやデバイスドライバーなどをインストールする場合は、"Admin"でログオンし、「統合書込みフィルター(UWF)構成ユーティリティー」でフラッシュディスクへ書込みができるように設定を変更してください。

注意：
フラッシュディスクの C ドライブへインストールすることは可能ですが、インストールプログラムやインストール時の一時ファイルなどがフラッシュディスク（C:）内に残ると、ディスク容量を圧迫する場合がありますので、ご注意ください。

少なくとも本ドライブ（C:）にはインストール後に、100MB 以上の空き容量を確保してください。

本製品に使用されている OS は、Windows 10 IoT Enterprise 版です。この OS は部分的に Windows 10 Enterprise と同等の機能を持っていますが、Windows 10 Enterprise の機能をフルサポートするものではありません。
そのため Windows 10 Enterprise 上では正常に動作するアプリケーション/デバイスドライバーでも、本製品上では正常に動作しない場合があります。アプリケーション/デバイスドライバーを追加導入する際には、十分な評価/テストを行ってからお使いください。

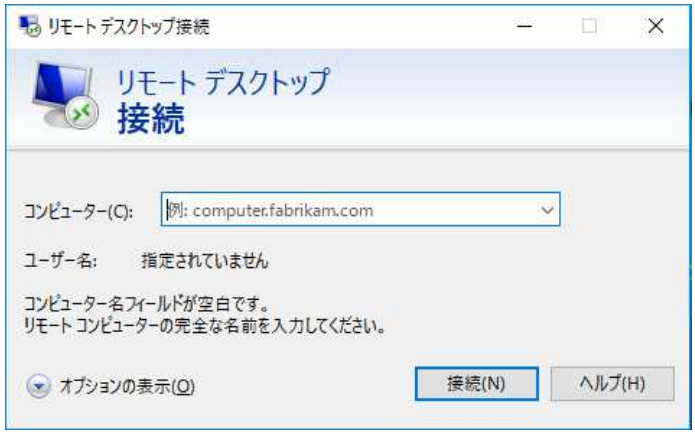
注意：
本製品には、設定を工場出荷値に初期化する機能はありません。デフォルトの設定を変更する前に、イメージのコピーを作成しておくことをおすすめします。
バックアップイメージの作成には、SNMP 管理ソフトウェアを使用します。

※ SNMP 管理ソフトウェアの入手に関しましては、弊社の担当営業までお問い合わせください。

3.2 RDPクライアント

RDP Client は、RDP(Microsoft Remote Desktop Protocol)プロトコルを使用して、他の Windows PC のデスクトップやターミナルサーバーへの接続を可能にするアプリケーションです。

プログラム起動画面



3.3 Citrix Receiver

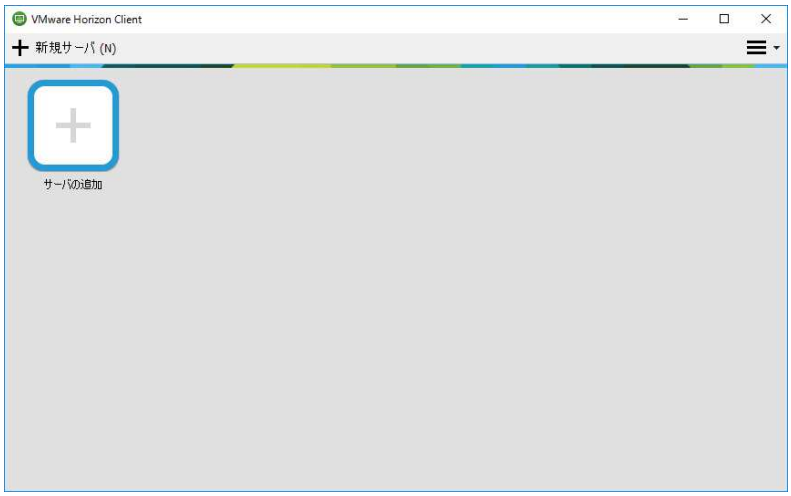
Citrix Receiver は、Citrix 社が提供するアプリケーションの仮想化サーバー、「Citrix XenApp」、または「XenDesktop」を利用するためのアプリケーションです。

プログラム起動画面

3.4 VMware Horizon Client

Vmware Horizon Client は、VMware 社が提供するアプリケーションの仮想化サーバー環境を利用するためのクライアントアプリケーションです。

プログラム起動画面



SecureTerminal ***Win10 版***

ユーザーズ・ガイド　*V 1.0.1*

JB アドバンスト･テクノロジー株式会社

SecureTerminal についてのお問い合わせは下記の窓口にご相談ください。

お客様相談センター

■電話相談窓口

受付時間　8:45-19:00

（日・祝日・12/30-1/4 を除く）

0120-28-3933

■FAX相談窓口

受付時間　24時間

0120-28-3977