

<u>Dell シンクライアント検証機 Quick Start Guide Wyse ThinOS 機編</u>

本ドキュメントでは、Dellより貸出させていただいた、シンクライアント機(Wyse ThinOS モデル)をご利用いただくための基本的な概念と操作方法について説明しています。

概要

Dell Wyse Thin OS(以下 WTOS)シンクライアントは、ICA/RDP/PCoIP 画面転送プロトコルに特 化した専用端末です。

WTOS は、Citrix/Microsoft/VMWare 仮想デスクトップソリューションに最適なシンクライアントとして 利用することができます。

本スタートアップガイドでは、WTOS シンクライアントを導入するにあたり、初期設定/テスト/デモ等を短時間で構成するためのマニュアルです。注

注意: 実際の運用にあっては、本説明のノウハウを元に、最適な設定を実施する必要があります。本説 明は、初回利用時や効果的なデモ/テスト環境を短時間で構成するために用いることができます。実運 用に向けた高度な設定や詳細仕様に関しては、「Dell Wyse ThinOS Administrator's Guide 」や「Dell Wyse ThinOS INI Reference Guide」をご参照ください。

テスト環境の構成例

WTOS シンクライアントの企業導入は、FTP サーバを用いた集中管理が効果的です。これは、シンクラ イアントのローカル設定をまったく行う必要がないため、数千台~数万台以上の管理が容易に集中管理 することができます。ただし、テスト/デモ環境において、FTP サーバを用意できない場合でも、ローカルの 必要な設定を実施することで、効果的なテスト/デモを実施することができます。 本説明では、下記の設定方法に関して解説します。

- 1. WTOS シンクライアントのローカル設定を用いた構成概要
- 2. Wyse Thin OS ネットワーク設定
- 3. WTOS 上のタイムゾーンと時刻サーバの設定
- 4. コネクションブローカーへの接続
 - 4-1. Citrix XenDesktop/XenAppの場合
 - 4-2. VMware Horizon View の場合
 - 4-3. Microsoft Remote Desktop Service の場合
- 5. 端末の初期化



1. WTOS シンクライアントのローカル設定を用いた構成概要

図 1 に示すように、WTOS シンクライアントから、Citrix/Microsoft/VMWare 仮想デスクトップソリュ ーション上のデスクトップ(アプリケーション)へ接続するための環境を構築します。ネットワーク環境上に DCHP サーバ等が存在しない場合、WTOS シンクライアント端末のローカル設定を実施する必要があり ます。ここでは、初回利用時の IP アドレス設定や コネクションブローカー(コネクションサーバ)設定を 解説します。



図1仮想デスクトップインフラストラクチャ(VDI)環境への接続イメージ

ハードウェア設定

WTOS シンクライアントの準備(電源、ネットワーク接続)を行い、物理的に Citrix/Microsoft/VMWare のコネクションブローカーとのネットワーク接続が可能な構成を構築します。

- 電源アダプタ/電源ケーブル接続
- イーサーネット接続
- USB キーボード/マウス接続

ソフトウェア設定(WTOS 上)

2. Wyse Thin OS ネットワーク設定

イーサーネットによりネットワーク接続した WTOS を初回起動すると、DHCP/BOOTP による自動 IP ア ドレス取得の仕組み(デフォルト設定)により、IP アドレスの取得を試みます。DHCP サーバによる IP ア ドレス割り当てを実施していない環境においては、図 2 に示すところで止まり、DHCP の IP アドレス取得 プロセスのタイムアウトメッセージ(DHCP が失敗しました、"ネットワーク設定"を確認してください)が WTOS のイベントログ上に記録されます。注

注意:DHCP クライアントによる IP アドレスの取得を試みるため、DHCP サーバが存在しない場合、



IP アドレス取 得処理がタイムアウトするまでに、数十秒かかります。このため、次に示すネットワーク構成 を実施します。

システム情報(S)
全般(g) 著作権(c) イベントログ(E) 統計(S) 有線(E) 無線(W)
06:00:39 ENET: set default gateway 10.1.120.254 06:00:39 AUDID: 鉄音デバイスを変更: HD Audio 06:00:39 AUDID: 舞生デバイスを変更: HD Audio 06:00:39 ENET: set default gateway 10.1.120.254 06:00:40 VUSB: ローカル認識: デバイス(0x148f,0x372,0xff,0xff,0xff) 06:00:41 VUSB: ローカル認識: デバイス(0x0461,0x4016,0x03,0x01,0x02) 06:00:41 USB: 新しい 1.5Mbps device "usbhid" をポート 12 で検出しました 06:00:42 VUSB: 新しい 1.5Mbps device "usbhid" をポート 7 で検出しました 06:00:42 USB: 新しい 1.5Mbps device "usbhid" をポート 7 で検出しました
ネットワーク設定 × × × × ・ ベットワーク設定
□ 三素板(g) □ オノション(1) 有称(c) 三森(W) ノロキン(2)
 O ENET - 有線接続
O WLAN - ワイヤレス接続
レビス 固定のネームサーバを使用
DNS サーバ(2):
WINS サーバ(W):
TCP Timeout: 1 × 30 秒

図 2 DHCP による IP アドレスの取得ログ (イベントログ)

WTOS のデスクトップより、ローカルで静的 IP アドレスを設定します(デフォルト: 「DHCP/BOOTP によりアドレスを割り当てる(H)」)。WTOS デスクトップより、[デスクトップ]→[システム情報(S)]→[ネットワーク設定(N)]を選択します(図 3 参照)。

補足:図 2 に示す DHCP クライアントによる IP アドレス取得のタイムアウトを待つことで、「ネットワーク設定」ダイアログ(図 2 の下の画面)が出力されます。この場合、タイムアウトまで数十秒待つ必要があるため、ここでは、WTOS のネットワーク設定を選択し、静的 IP アドレスを設定します。



図 3 WTOS のネットワーク設定

「ネットワーク設定」ダイアログの「全般(G)」-「有線(E)」タブの「プロパティ」において、「静的 IP アドレスを 指定する(A)」を選択します。WTOS のローカル IP アドレス、サブネットマスク、デフォルトゲートウェイをそ れぞれ、環境に合わせて設定し、[OK]ボタンをクリックします(図 4 参照)。



補足: ネットワーク環境上で名前解決が必要な環境の場合、「ネットワーク設定」ダイアログの「全般 (G)」タブにある、「DNS ドメイン(D)」、「DNS サーバ(V)」もしくは、「WINS サーバ(W)」上で必要 な名前解決サーバの IP アドレスを設定します。(図 5 参照)

■ ネットワーク設定 ×
全般(<u>G</u>) オプション(<u>I</u>) 有線(E) 無線(<u>W</u>) プロキシ(P)
イーサネット速度(<u>T</u>): 自動検出 ラ ▽ IP∨4 アドレス指定:静的IP
プロパティ(P) 「IPv6- IPv6- ネットワーク設定 ×
7
■ IEEE80 DHCP / BOOTP による自動取得(出) ● 静的 IP アドレスを指定(A)
IP アドレス(1): 10.1.120.101 ネットマスク(U): 255.255.255.0 ゲートウェイ(W): 10.1.120.254

図 4 WTOS ローカルネットワーク設定



フォルトゲートウェイを設定するインターフェース ● ENET - 有線接続 ● WLAN - ワイヤレス接続 7 固定のネームサーバを使用 DNS ドメイン(D): DNS サーバ(V):	殿(<u>G) オプション(T</u>) 有線(Ĕ) 無線(₩)	プロキシ(<u>P</u>)
 ○ ENET - 有線接続 ○ WLAN - ワイヤレス接続 7 固定のネームサーバを使用 DNS ドメイン(Q): DNS サーバ(V): 	デフォルトゲートウェイ	を設定するインターフェー	z
 O WLAN - ワイヤレス接続 7 固定のネームサーバを使用 DNS ドメイン(Q): DNS サーバ(V): 	O ENET - 有線	接続	
7 固定のネームサーバを使用 DNS ドメイン(D):	O WLAN - ワイ	ヤレス接続	
/ 固定のネームサーハを使用 DNS ドメイン(D): 「 DNS サーバ(V):		5.准四	
	✓ 固定のネームサーハネ DNP ドメイン/D)・	2 使用	
DNS サーバ(V):			
	DNS サーバ(<u>V</u>):		
WINS サーバ(<u>W</u>):			

図 5 名前解決サーバの設定

3. WTOS 上のタイムゾーンと時刻サーバの設定

仮想デスクトップソリューションのコネクションサーバと接続するための WTOS 上でタイムゾーンとタイムサー バを設定します。WTOS デスクトップより、[デスクトップ]→[システム情報(S)]→[システム設定(S)]を選 択します(図 6 参照)。



図 6 WTOS のシステム設定

図7のように「時間/日付(D)」タブにある「タイムゾーン」と時刻サーバを設定します。

◎ プロパティ(F)	×
全般(G) 時間/日付(D) カスタム	青報(世)
● タイムゾーン: (GMT+09:00) 大阪、	札幌、東京
□ 夏時間を有効にする(Y)	
開始(<u>R</u>): ┃月 ▼ 第	1週 🚽 月曜日 🚽
終了(E): 1月 👤 第	
時刻表示形式(I): 24-hour fi	ormat 🗧
日付表示形式(E): yyyy/mm/d	t t
時刻サーバ(<u>I</u>): 10.1.120 .1	1
Bł	†と時刻の変更(<u>H</u>)
<u>O</u> K	Cance 1

図 7 WTOS 上のタイムゾーンと時刻サーバ設定

4.コネクションブローカーへの接続

WTOS を起動後(ネットワーク設定完了後)、WTOS ローカルデスクトップ上には、図 5 に 示すよう に、「Default ICA」アイコンと「Default RDP」アイコンが表示されます。また、タスクマネー ジャ上に「接続マネージャ」が最小化されています。

このステップガイドでは「リモート接続設定」を変更し、Citrix/Microsoft/VMWareのコネクションブローカーへの接続設定を構成していきます。(図 8 参照)





図 8 コネクションブローカー設定

4-1.Citrix XenDesktop/XenAppの場合

XenDesktop/XenAppへの接続設定を実施するため、図8のように「リモート接続設定(R)」を選択し、リモート接続設定のダイアログを立ち上げます。

XenDesktop/XenApp への接続するため、StoreFront を利用している場合は図 9 のように「プローカー選択(T)」メニューの下にある「StoreFront UI の有効化(E)」を選択してください。

回 リモート接続設定(R)	×
ブローカー(<u>B</u>) 表示設定(<u>V</u>) ー	·般設定(G) 認証設定(H)
プローカー選択(<u>I</u>):	Citrix Xen ▼ StoreFront UIの有効化(E)
プローカーサーバ(<u>S</u>): 自動接続リスト(<u>A</u>): □ ログイン時に自動再 ● 非アクティブなも	10.1.120.71 接続を有効にする(L) マッションのみに接続
 ○アクティブ・非フ ボタンメニューから ●非アクティブな+ ○アクティブ・非フ 	?クティブなセッションに接続 自動再接続を有効にする(U) 2ッションのみに接続 アクティブなセッションに接続
アカウントセルフサービス(E	Ð:
デフォルトICA環境選択:	XenApp(<u>P</u>) XenDesktop(<u>D</u>)
D K	Cance 1

図 9 XenDesktop/XenAppへの接続設定

- プローカー選択: Citrix Xen を選択する

- StoreFront UI の有効化: チェックあり

- **ブローカーサーバ**: Store Front の IP アドレスもしくは FQDN 名を入力する 補足: Store Front の XenApp Services Support もしくは Web Interface を利用する場合は 以下のように設定します。 (図 10)



- **プローカー選択:** Citrix Xen を選択する

- StoreFront UI の有効化: チェックなし

- **ブローカーサーバ:** Store Front XenApp Services Support もしくは Web Interface の XenApp Services のフルパス (図 11 参照)を入力する。

■ リモート接続設定(R)	×
ブローカー(<u>B</u>) 表示設定(<u>V</u>) 一般設定(<u>G</u>) 認証設定(<u>H</u>)	
プローカー選択(I): Citrix Xen ▼ □ StoreFront UIの有効化(E) ◆	
プローカーサーバ(<u>S</u>): 0.71/Citrix/Store/PNAgent.xml 自動接続リスト(<u>A</u>):	-
 □ ログイン時に自動再接続を有効にする(L) ○ 非アクティブなセッションのみに接続 ○ アクティブ・非アクティブなセッションに接続 	
 □ ボタンメニューから自動再接続を有効にする(U) ● 非アクティブなセッションのみに接続 ● アクティブ・非アクティブなセッションに接続 	
アカウントセルフサービス(<u>R</u>):	
デフォルトICA環境選択: XenApp(P) XenDesktop(D)	
OK Cancel	



Configure XenApp Services Support	Manage NetScaler Gat Manage Beacons
Allows users with the Citrix Online Plug-in or with devices that require XenApp	Set Default Website
Services URLs to access this store.	View
	🖪 Refresh
Enable XenApp Services support	P Help
XenApp Services URL: http://xd7-ddc01.tkolab.local/Citrix/Store/PNAgent/config.xml	Store Service
Default store The Citrix Online Plug-in enables you to specify a default store for users.	Manage Delivery Contr Configure Unified Expe Manage Authenticatio
Default store: None	Manage Receiver for Configure Remote Acc
OK Cancel	Configure XenApp Ser
	Configure Store Settings



図 11 Store FrontのXenApp Services Supportの設定

上記の設定完了後「OK」ボタンを選択することで、WTOS が再起動されます。 WTOS 再起動後には以下のように Citrix XenDesktop/XenApp 環境へ接続するためのサインオン ダイアログが表示されますので、有効なサインオン情報を入力します。(図 12 参照)



図 12 Citrix XenDesktop/XenApp サインオンダイアログ

補足: WTOS から Citrix XenDesktop へ初期ログインユーザの場合は左側のツールバーの「Apps」ア イコンからアクセス可能はアプリケーションを選択し、ローカル画面に表示させる必要がございます。(図13)



図 13 WTOS の Citrix XenDesktop/XenApp アプリケーションアイコン





4-2VMware Horizon View の場合

VMware Horizon View への接続設定を実施するため、図 8 のように「リモート接続設定(R)」を選択し、リモート接続設定のダイアログを立ち上げます。

VMware Horizon View への接続するためには図 14 のように設定を行います。

	一般設定(<u>G)</u> 認証設定(<u>H</u>)
ブローカー選択(<u>I</u>):	VMwareView 👤
プローカーサーバ(<u>S</u>):	https://10.1.120.12
自動接続リスト(<u>A</u>):	
セキュリティモード	
○ 警告(ℝ) (信頼されてい	ないサーバに接続する前に警告する)
○ 完全(E) (信頼されてい	いないサーバに接続しない)
○ 無効(W) (サーバID証明)	書を検証しない) 🔫 💻
	・ュリティポリシを使用)
○ 既定(D) (システムセキ	
○ 既定(D) (システムセキ 接続プロトコル(P):	「デフォルト プロトコルのみ 📃 🖣
○ 既定(<u>D</u>) (システムセキ 接続プロトコル(<u>P</u>):	「デフォルト プロトコルのみ 📃 🖣

図 14 Horizon View の接続設定

- **プローカー選択:** VMware View を選択する
- ブローカーサーバ: 接続サーバの IP アドレスもしくは FQDN 名を入力する
- セキュリティモード: 無効(W) (サーバ ID 証明書を検証しない)を選択する注
- 接続プロトコル:デフォルトプロトコルのみを選択する。

注:初回利用時や効果的なデモ/テスト環境を短時間で構成するためにセキュリティモードを「無効」に設定しております。実際の運用にあっては、ご利用の環境に適した設定を行うようにお願いします。 上記の設定完了後「OK」ボタンを選択することで、WTOS が再起動されます。

WTOS 再起動後には以下のように VMware Horizon View 環境へ接続するためのサインオンダイア ログが表示されますので、有効なサインオン情報を入力します。(図 15 参照)



vm ware Horiz	zon
サーバー名: 🔓	https://vcs01.dw.local
ユーザ名(U):	user01
パスワード(E):	********
ドメイン(<u>D</u>):	DW.local 👤

図 15 VMware Horizon View サインオンダイアログ

補足: デスクトッププールのプロトコル設定により表示されるデスクトッププールアイコンが異なります。(図 13)



図 16 VMware Horizon View デスクトッププールアイコン



4-3.Microsoft Remote Desktop Service の場合

Microsoft Remote Desktop Service への接続設定を実施するため、図8のように「リモート接続設定(R)」を選択し、リモート接続設定のダイアログを立ち上げます。

Microsoft Remote Desktop Service への接続するためには図 17 のように設定を行います。

回 リモート接続設定(R)	×
ブローカー(<u>B</u>) 表示設定(<u>V</u>) 一	般設定(<u>G</u>) 認証設定(<u>H</u>)
プローカー選択(<u>I</u>):	Microsoft 📃 🗲
ブローカーサーバ(<u>S</u>): 自動接続リスト(<u>A</u>):	10.1.120.31
O K	Cance 1

図 17 Microsoft Remote Desktop Service の接続設定

- **プローカー選択:** Microsoft を選択する

- **ブローカーサーバ:RD** 接続ブローカーサーバの IP アドレスもしくは FQDN 名を入力する 上記の設定完了後「OK」ボタンを選択することで、WTOS が再起動されます。

WTOS 再起動後には以下のように Microsoft Remote Desktop Service 環境へ接続するための サインオンダイアログが表示されますので、有効なサインオン情報を入力します。注(図 18 参照) 注:WTOS の仕様上 RDS 環境へ接続するためには証明書登録が必須となっております。証明書登 録するための詳細情報につきましては捕捉の「Microsoft Remote Desktop Service 接続するため の証明書登録について」をご参照ください。



ユーザ名(山):	user01	
パスワード(Ⴒ):	*****	
ドメイン(<u>D</u>):	DW.local	Ŧ

図 18 Microsoft サインオンダイアログ

以下の WTOS 画面は Microsoft Remote Desktop Service のセッションホストの Remote App としてワードパッドを実行した画面となります。(図 19 参照)



図 19 WTOS の Microsoft Remote Desktop Service のアプリケーション



補足: Microsoft Remote Desktop Service 接続するための証明書登録について

こちらの設定では初回利用時や効果的なデモ/テスト環境を短時間で構成するために RDS 環境の RD Web のデフォルト証明書をエクスポートし設定を行っております。実際の運用にあっては、最適な設定を 行うようにお願いします。(図 20 参照)

型で Web サイトの認証	
DW-AD01-CA で、このサイトを次のように認証しました:	sources
rds01.dw.local このサーバーへの接続は暗号化されていま す。	クトップ接続
このサイトを信頼するべきですか?	

図 20 Microsoft RD Webの証明書

一般の Fat PC からウェブブラウザーを利用し、RD Web の証明書をエクスポートします。エクスポートした 証明書の拡張子を.cer(デフォルト)から.crt に変更し、 Fat32 形式の USB に保存します。 エクスポートした RD Web の証明書を登録するため、証明書を保存した USB を WTOS 端末の USB ポートに差し込み、図 21 のように「システム診断(B)」を選択し「証明書」タブに移動します。 「ソース(F)」項目から USB メモリを選択し「登録(M)」ボタンをクリックすることで、上記で保存した 証明書ファイルの登録が可能です。(図 21 参照)

	・システムツール(Y) ×
	デバイス参照(<u>V</u>) 証明書(<u>A</u>) パッケージ(<u>P</u>) Global INI(<u>I</u>) User INI(<u>U</u>)
	ソース(E): USBメモリ
 	BTCTRoot.crt Class3PCA.G2_v2.crt Entrust.G2.crt gd-class2-root.crt GTCTGlobalRoot.crt Pc32s_v4.crt DV RootCA.crt TVB gdvCa
 ● システムツール(Y) ■ システム診断(B) 	証明書参照(⊻)
 ∑プリケーション(A): →	QK QK

図 21WTOS の証明書登録画面



5.端末の初期化

WTOS のすべての設定をリセットして、工場出荷状態に戻す手順ついて説明します。 WTOS のデスクトップ画面上を左クリックして、「シャットダウン」をクリックすることで、図 22 のように WTOS のシャットダウンダイアログが表示されます。



図 22WTOS のシャットダウン画面

「システムを出荷状態にリセット」のチェックボックスをオンにした後、「システムのシャットダウン」を選択します。

以上