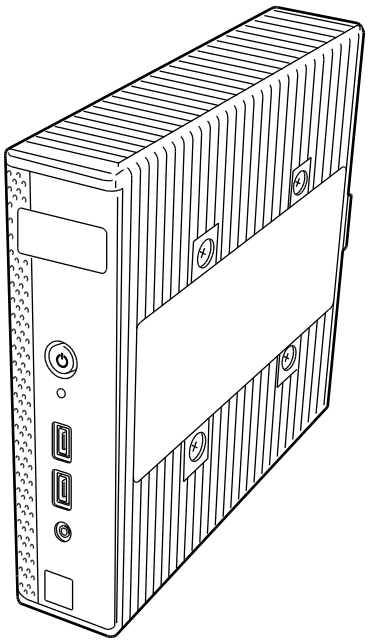
Express5800

NEC



Express5800シリーズ

US300d
ユーザーズガイド

2018年 6月　第8版

本製品のドキュメント

本製品のドキュメントは、次のように、冊子として添付されているもの(📖)と、Web 上で電子マニュアル(PDF)として開示されているものがあります。

📖 スタートアップガイド	本製品の開梱から運用までを順を追って説明しています。はじめにこのガイドをお読みください。

PDF ユーザーズガイド

使用上のご注意	本製品を安全に使うための情報について説明しています。**ご使用になる前に、必ずお読みください。**
1 章 US300d について	本製品を導入する際に知っておいていただきたいことについて説明しています。
2 章 基本事項の概要	シンクライアントの使用するための基本事項について説明しています。
3 章 便利なユーザー機能	ユーザー向けの機能の概要について説明します。
4 章 便利な管理者機能	管理者向けの機能の概要について説明します。
5 章 管理者ユーティリティーと設定に関する追加情報	管理者向けユーティリティーと設定に関する情報を紹介します。
6 章 システム管理	シンクライアント環境のメンテナンスに必要な日常作業の実行に役立つローカルおよびリモートシステム管理について説明します。
7 章 サーバー環境の設定	シンクライアントにネットワークおよびセッションサービスを提供するために必要なネットワークアーキテクチャーと企業サーバー環境について説明します。
8 章 ソフトウェア情報と注意・制限事項	本製品のソフトウェア情報と、運用における注意・制限事項について説明します。
9 章 運用・保守	日常の保守、トラブルシューティングについて説明しています。 「故障かな？」と思ったときは、装置の故障を疑う前に参照してください。
10 章 付録	

目　次

本書で使う表記

本文中の記号

本書では安全にかかわる注意記号のほかに 3 種類の記号を使用しています。これらの記号は、次のような意味があります。

	ハードウェアの取り扱い、ソフトウェアの操作などにおいて、守らなければならないことについて示しています。記載の手順に従わないときは、ハードウェアの故障、データの損失など、**重大な不具合が起きるおそれがあります。**
	ハードウェアの取り扱い、ソフトウェアの操作などにおいて、確認しておかなければならないことについて示しています。
	知っておくと役に立つ情報、便利なことについて示しています。

オペレーティングシステムの表記

本書では、Windows オペレーティングシステムを次のように表記します。

本書の表記	Windows OSの名称
Windows 8 ※1	Windows 8 Enterprise Edition
Windows 7	Windows 7 Enterprise 64-bit(x64) Edition Windows 7 Enterprise 32-bit(x86) Edition
Windows Vista	Windows Vista Business 64-bit(x64) Edition Windows Vista Business 32-bit(x86) Edition
Windows XP	Windows XP Professional x64 Edition Windows XP Professional
Windows 2012	Windows Server 2012 DataCenter Edition Windows Server 2012 Standard Edition
Windows 2008	Windows Server 2008 R2 Standard Edition Windows Server 2008 R2 Enterprise Edition Windows Server 2008 32bit Standard Edition Windows Server 2008 32bit Enterprise Edition Windows Server 2008 64bit Standard Edition Windows Server 2008 64bit Enterprise Edition
Windows 2003	Windows Server 2003 R2 Standard Edition Windows Server 2003 R2 Enterprise Edition Windows Server 2003 32bit Standard Edition Windows Server 2003 32bit Enterprise Edition Windows Server 2003 64bit Standard Edition Windows Server 2003 64bit Enterprise Edition

※1 本書では、特に記載がない限りWindows8は64ビット版を示します。

商　標

Microsoft、Windows、Windows Server、Windows Vista、MS-DOSは米国Microsoft Corporationの米国およびその他の国における登録商標または商標です。
Intel、インテル、XEON、インテルCore、Pentium、Celeron、インテルvProは米国Intel Corporationの登録商標または商標です。
ATI、ATI logo、FireProはAdvanced Micro Devices, Inc.の商標です。
Adaptecとそのロゴは米国Adaptec, Inc.の登録商標です。SCSI*Select*は米国Adaptec, Inc.の商標です。
LSI、LSIロゴのデザインは、米国LSI Corporationの登録商標または商標です。
Adobe、Adobeロゴ、Acrobatは、Adobe Systems Incorporated(アドビシステムズ社)の登録商標または商標です。
LinuxはLinus Torvaldsの米国およびその他の国における登録商標または商標です。
NVIDIA、NVIDIAロゴ、Quadroは、NVIDIA Corporation社の商標または登録商標です。
Wyse, Wyse Configuration Manager, Wyse USB Firmware Toolは、Wyse Technology Inc.の登録商標または商標です。

Symantec Norton Ghost
(c) 1999 Symantec Corporation. All Rights Reserved.

その他、記載の会社名および商品名は各社の商標または登録商標です。

重要なお知らせ

ネットワークを介して制御できる機器において、その制御用パスワードを初期値のまま運用しますと、悪意のある第三者による不正アクセスを許すリスクが発生します。不正アクセスにより機器が乗っ取られると、情報漏えいのみならず、可用性や完全性を阻害してシステムに被害を生じさせたり、ボットネットによるサイバー攻撃の足場に悪用されたりする可能性があります。

本製品の初期パスワードは、あくまでも保守運用における初期設定のために設けられています。**初期設定時に必ずパスワード変更を行ってください。**もし初期パスワードのまま運用して不正アクセスの被害が発生した場合、**弊社は一切の責任を負うことができません。**

なお、パスワード変更を行っても、強度の低いもの（桁数の少ないもの）や容易に考えられるもの（”123456789”, “abcdefg”, “password”, “Administrator” など）では不正アクセスの防止が困難です。**強度の強いパスワード（8文字以上で大文字/小文字/数字混在のもの**を推奨）に変更頂きますようお願い致します。

本書についての注意、補足

1. **本書の内容の一部または全部を無断転載することは禁じられています。**
2. **本書の内容に関しては将来予告なしに変更することがあります。**
3. **弊社の許可なく複製・改変などを行うことはできません。**
4. **本書は内容について万全を期して作成いたしましたが、万一ご不審な点や誤り、記載もれなどお気づきのことがありましたら、お買い求めの販売店にご連絡ください。**
5. **運用した結果の影響については、4 項にかかわらず責任を負いかねますのでご了承ください。**
6. **本書の説明で用いられているサンプル値は、すべて架空のものです。**

この説明書は、必要なときすぐに参照できるよう、お手元に置いておくようにしてください。

本書は作成日時点の情報をもとに作られており、画面イメージ、メッセージ、または手順などが**実際のものと異なるときがあります。**変更されているときは適宜読み替えてください。
また、ユーザーズガイドをはじめとするドキュメントは、以下の Web サイトから最新版をダウンロードできます。

http://www.nec.co.jp/

必要な情報を見つけるには

PDF 文書を開いた状態で、[検索]ウィンドウまたは[Find]ツールバーのいずれかを使用して、単語、語句、または単語の一部を検索できます。これらの機能の使用については、ご使用の PDF リーダーのヘルプを参照してください。

付属品の確認

梱包箱の中には、US300d 本体以外にいろいろな付属品が入っています。添付のスタートアップガイドを参照してすべてがそろっていることを確認し、それぞれ点検してください。万一足りないものや損傷しているものがある場合は、販売店に連絡してください。

第三者への譲渡について

本製品を第三者に譲渡(または売却)するときは、本書および添付の部品や説明書、ライセンス許諾書などのドキュメントも一緒にお渡しください。譲渡や売却の際には、必ず渡してください。

消耗品・本製品の廃棄について

本製品および電池の廃棄については各自治体の廃棄ルールに従ってください。詳しくは、各自治体へお問い合わせください。なお、本製品に添付の電源コードについても他の装置への転用を防ぐため、本体と一緒に廃棄してください。

本製品の輸送について

本製品およびオプションなどには、リチウム金属電池あるいはリチウムイオン電池を使用しています。
リチウム電池の輸送に関しては、航空・海上輸送規制が適用されますので、本製品およびオプションの航空機、船舶等での輸送については、お買い求めの販売店、または保守サービス会社へお問い合わせください。

各種権利、US300d が準拠する規制

各種権利

エンドユーザーライセンス契約 (Wyse Technology End User License Agreement("License"))

Wyse Technology 社のエンドユーザーライセンス契約のコピーはソフトウェアに含まれ、参照目的でのみ提供されます。購入日に http://www.wyse.com/license に掲載されているライセンスが、効力を持つライセンス契約です。ソフトウェアまたは製品をコピー、使用、またはインストールすることによって、ライセンス契約の条件に同意したものとみなします。

限定権利の説明

ユーザーは、本ソフトウェアが米国製であることを確認するものとします。また、ユーザーは、米国輸出管理規則をはじめとする本ソフトウェアに適用されるすべての適用可能な国際法および国内法ならびに米国およびその他の政府によって発行されるエンドユーザー、最終使用、および輸出先国に関する制限事項を遵守するものとします。本ソフトウェアの輸出については、http://www.microsoft.com/exporting を参照してください

準拠する規制

無線 LAN の使用および要件

無線 LAN オプションを備えたモデルには、無線送受信タイプのデバイス(RF モジュール)が含まれています。本製品の無線 LAN デバイスは、5GHz、2.4GHz 帯域で動作します(802.11a/b/g/n WLAN)。

一般的な目安として、本製品の近くで無線 LAN デバイスを使用する場合、無線 LAN デバイスと本製品の距離は 20cm 程度が一般的です(先端部含まず)。無線 LAN デバイスが起動し送受信中の場合は、本製品から 20cm 以上離して使用してください。

状況によっては、無線 LAN デバイスに関する制限事項が求められる場合があります。一般的な制限事項の例としては、以下のようなものがあります。

- 無線 LAN デバイスを使用した場合の処罰が不明な環境では、無線 LAN デバイスを使用または電源を入れる前に適切な機関に許可を求めてください。
- 無線 LAN デバイスの使用に関する制限は、国によって異なります。お使いのシステムには無線 LAN デバイスが装備されていますので、本システムを携帯して国境を越える移動を行う場合は、移動または旅行の前に、行先となる国における無線 LAN デバイスの使用に関する制限事項を現地の無線承認機関にご確認ください。
- 無線 LAN デバイスをユーザーが修理することはできません。無線 LAN デバイスはいかなる場合でも改造しないでください。無線 LAN デバイスを改造すると、使用許可は無効になります。修理が必要な場合は、メーカーにお問い合わせください。

AC アダプタ・電源コード

本製品に添付されている AC アダプタ(モデル NB-65B19)、電源コードを使用してください。

添付の AC アダプタ、電源コード以外のものは使用しないでください。
定格の合っていない AC アダプタ、電源コードを使用すると火災や誤動作、故障の原因となります。

⚠使用上のご注意(必ずお読みください)

本製品を安全に正しくご使用になるために必要な情報が記載されています。また、本文中の名称については本書の「1 章(2. 各部の名称と機能)」の項をご参照ください。

安全にかかわる表示について

本製品を安全にお使いいただくために、このユーザーズガイドの指示に従って操作してください。
本製品のどこが危険でどのような危険に遭うおそれがあるか、どうすれば危険を避けられるかなどについて説明しています。
ユーザーズガイドでは、危険の程度を表す言葉として、「警告」と「注意」という用語を使用しています。それぞれの用語は次のような意味を持つものとして定義されています。

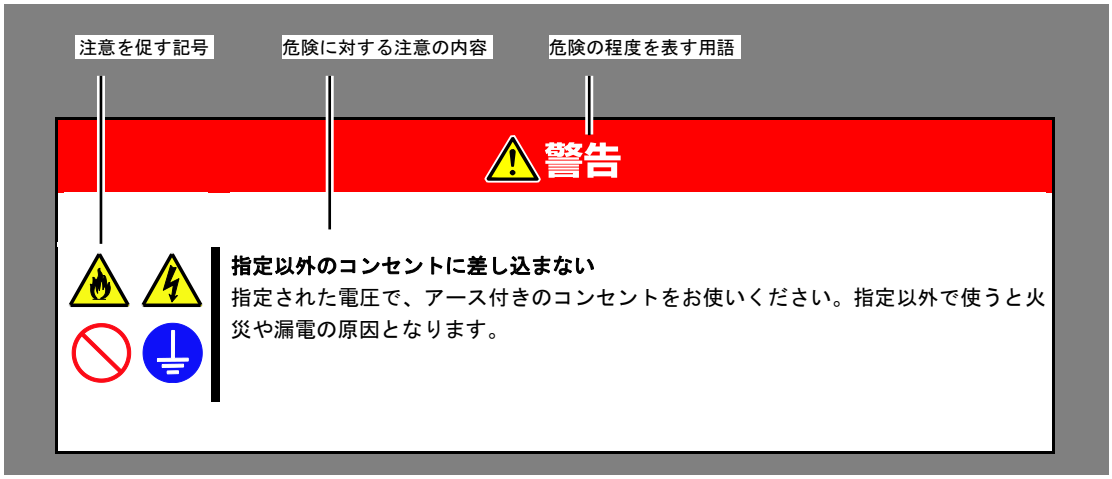
⚠警告 人が死亡する、または重傷を負うおそれがあることを示します。

⚠注意 火傷やけがなどを負うおそれや物的損害を負うおそれがあることを示します。

危険に対する注意・表示は次の 3 種類の記号を使って表しています。それぞれの記号は次のような意味を持つものとして定義されています。

△	**注意の喚起**	この記号は危険が発生するおそれがあることを表します。記号の中の絵表示は危険の内容を図案化したものです。	(例)  (感電注意)
⃠	**行為の禁止**	この記号は行為の禁止を表します。記号の中や近くの絵表示は、してはならない行為の内容を図案化したものです。	(例)  (分解禁止)
●	**行為の強制**	この記号は行為の強制を表します。記号の中の絵表示は、しなければならない行為の内容を図案化したものです。危険を避けるためにはこの行為が必要です。	(例)  (電源プラグを抜け)

(ユーザーズガイドでの表示例)



本書と警告ラベルで使用する記号とその内容

注意の喚起

	感電のおそれのあることを示します。		発煙または発火のおそれがあることを示します。
	爆発や破裂による傷害を負うおそれがあることを示します。		けがをするおそれがあることを示します。
	特定しない一般的な注意・警告を示します。		高温による傷害を負うおそれがあることを示します。

行為の禁止

	本製品を分解・修理・改造しないでください。感電や火災のおそれがあります。		水や液体がかかる場所で使用しないでください。水にぬらすと感電や発火のおそれがあります。
	指定された場所には触らないでください。感電や火傷などの傷害のおそれがあります。		火気に近づけないでください。発火するおそれがあります。
	ぬれた手で触らないでください。感電するおそれがあります。		特定しない一般的な禁止を示します。

行為の強制

	電源プラグをコンセントから抜いてください。火災や感電のおそれがあります。		特定しない一般的な使用者の行為を指示します。説明に従った操作をしてください。
	必ず接地してください。感電や火災のおそれがあります。		

安全上のご注意

本製品を安全にお使いいただくために、ここで説明する注意事項をよく読んでご理解し、安全にご活用ください。記号については、本書の「安全にかかわる表示について」の説明を参照してください。

全般的な注意事項

⚠警告

人命に関わる業務や高度な信頼性を必要とする業務には使用しない

本製品は、医療機器・原子力設備や機器、航空宇宙機器・輸送設備や機器など、人命に関わる設備や機器および高度な信頼性を必要とする設備や機器などへの組み込みやこれらの機器の制御などを目的とした使用は意図されておりません。これら設備や機器、制御システムなどに本製品を使用した結果、人身事故、財産損害などが生じても弊社はいかなる責任も負いかねます。

煙や異臭、異音がしたまま使用しない

万一、煙、異臭、異音などが生じたときは、ただちに電源をOFFにして電源プラグをコンセントから抜いてください。その後、お買い求めの販売店または保守サービス会社にご連絡ください。そのまま使用すると火災の原因となります。

針金や金属片を差し込まない

通気孔や光ディスクドライブのすきまから金属片や針金などの異物を差し込まないでください。感電の危険があります。

⚠注意

日本国外で使用しない

本製品は、日本国内用として製造・販売しています。日本国外では使用できません。本製品を日本国外で使用すると火災や感電の原因となります。

本機内に水や異物を入れない

本機内に水などの液体、ピンやクリップなどの異物を入れないでください。火災や感電、故障の原因となります。もし入ってしまったときは、ただちに電源をOFFにして、電源プラグをコンセントから抜いてください。分解しないで販売店または保守サービス会社にご連絡ください。

電源・電源コードに関する注意事項

⚠警告

ぬれた手で電源プラグを持たない
ぬれた手で電源プラグの抜き差しをしないでください。感電するおそれがあります。

アース線をガス管につながない
アース線は絶対にガス管につながないでください。ガス爆発の原因になります。

電源コードを接続したままアース線の取り付けや取り外しをしない
アース線の取り付け/取り外しは電源プラグをコンセントから抜いて行ってください。たとえ電源をOFFにしても電源プラグを接続したままアース線に触ると感電したり、ショートによる火災を起こしたりすることがあります。

⚠注意

指定以外のコンセントに差し込まない
指定された電圧で、アース付のコンセントをお使いください。指定以外で使うと火災や漏電の原因となります。また、延長コードが必要となるような場所には設置しないでください。本製品の電源仕様に合っていないコードに接続すると、コードが過熱して火災の原因となります。

たこ足配線にしない
コンセントに定格以上の電流が流れることによって、過熱して火災の原因となるおそれがあります。

中途半端に差し込まない
電源プラグは根元までしっかりと差し込んでください。中途半端に差し込むと接触不良のため発熱し、火災の原因となることがあります。また差し込み部にほこりがたまり、水滴などが付くと発熱し、火災の原因となるおそれがあります。

電源コードを持って引き抜かない
ケーブルを抜くときはコネクタ部分を持ってまっすぐに引き抜いてください。ケーブル部分を持って引っ張ったりコネクタ部分に無理な力を加えたりするとケーブル部分が破損し、火災や感電の原因となります。

⚠注意

指定以外の電源コードを使わない

本製品に添付されている電源コード以外のコードを使わないでください。電源コードに定格以上の電流が流れると、火災の原因となるおそれがあります。

また、電源コードの破損による感電や火災を防止するために次の注意をお守りください。

- コード部分を引っ張らない。
- 電源コードを折り曲げない。
- 電源コードをねじらない。
- 電源コードを踏まない。
- 電源コードをはさまない。
- 電源コードをステープラなどで固定しない。
- 電源コードを束ねたまま使わない。
- 電源コードに薬品類をかけない。
- 電源コードの上にものを載せない。
- 電源コードを改造・加工・修復しない。
- 損傷した電源コードを使わない。(損傷した電源コードはすぐ同じ規格の電源コードと取り替えてください。交換に関しては、お買い求めの販売店または保守サービス会社にご連絡ください。)

添付の電源コードを他の製品や用途に使用しない

添付の電源コードは本製品に接続し、使用することを目的として設計され、その安全性が確認されているものです。決して他の製品や用途に使用しないでください。火災や感電の原因となるおそれがあります。

設置・本機の移動・保管・接続に関する注意事項

⚠注意

指定以外の場所に設置・保管しない

本製品を次に示すような場所や本書で指定している場所以外に置かないでください。火災の原因となるおそれがあります。

- ほこりの多い場所。
- 給湯器のそばなど湿気の多い場所。
- 直射日光が当たる場所。
- 不安定な場所。

腐食性ガスの存在する環境で使用または保管しない

腐食性ガス(二酸化硫黄、硫化水素、二酸化窒素、塩素、アンモニア、オゾンなど)の存在する環境に設置し、使用しないでください。また、ほこりや空気中に腐食を促進する成分(塩化ナトリウムや硫黄など)や導電性の金属などが含まれている環境へも設置しないでください。本機内部のプリント板が腐食し、故障および発煙・発火の原因となるおそれがあります。もしご使用の環境で上記の疑いがあるときは、販売店または保守サービス会社にご相談ください。

電池に関する注意事項

⚠警告

電池は火の中に入れない
火の中に入れたり、加熱したりすると爆発したり、破裂したりするおそれがあります。

電池を分解、改造しない
分解、改造すると破裂したり、液もれするおそれがあります。弊社指定以外の電池は、品質、性能、安全性について保証の対象外となります。

⚠注意

電池はお子さま、特に乳幼児の手の届かない場所に保管する
電池内部には、有害物質を含んでいるため、誤って飲み込んだり、なめたりすると危険です。万一、飲み込んだ場合は、直ちに医師にご相談ください。

運用中の注意事項

⚠注意

雷がなったら触らない
雷が鳴りだしたら、ケーブル類も含めて本製品には触れないでください。また、機器の接続や取り外しも行わないでください。落雷による感電のおそれがあります。

ペットを近づけない
本製品にペットなどの生き物を近づけないでください。排泄物や体毛が本製品内部に入って火災や感電の原因となります。

通気開口部をふさがない
内部に熱がこもり、発煙、発火の原因となるおそれがあります。

ヘッドフォンを耳にあてたまま接続しない
ヘッドフォンを耳にあてたままヘッドフォン端子に接続しないでください。耳を痛めるおそれがあります。また、接続前にボリュームが大きくなっていないことを確認してください。

通気開口部に注意する
通気開口部とその周辺は、室温よりも高い温度となっております。長時間触れていると、低温やけどのおそれがありますので、肌の弱い方などは特にご注意ください。

無線機能仕様に関する注意事項

⚠注意

埋め込み型心臓ペースメーカー装着部から30cm以上離して使用する
埋め込み型心臓ペースメーカーを装着されている方は、本製品を心臓ペースメーカー装着部から30cm以上離して使用してください。電波により影響を受けるおそれがあります。

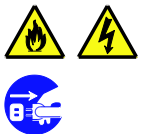
医療機関など本製品の使用を禁止した区域では本製品の電源または無線機能をOFFにする
医療機関などで本製品の使用を禁止した区域では、本製品の電源をOFFにするか、無線LANなどの無線機能をOFFにしてください。また、医療機関などで本製品の使用を認めた区域でも、近くで医療機器が使用されている場合には、本製品の電源をOFFにするか、無線LANなどの無線機能をOFFにしてください。医療機器に影響を与え、事故の原因になることがあります。詳しい内容については、各医療機関にお問い合わせください。

他の機器に電波障害を引き起こした場合は本製品の無線機能をOFFにする
本製品の無線機能を使用中に、他の機器に電波障害を引き起こした場合は、速やかに無線機能をOFFにするか、本製品の使用を中止してください。機器に影響を与え、誤動作による事故の原因になるおそれがあります。

運用中の注意事項

⚠注意

自分で分解・修理・改造はしない
絶対に分解したり、修理・改造を行ったりしないでください。本製品が正常に動作しなくなるばかりでなく、感電や火災の危険があります。



電源プラグを差し込んだまま取り扱わない
お手入れや装置に接続されているケーブルの取り付け/取り外しは、本製品の電源をOFFにして、電源プラグをコンセントから抜いて行ってください。たとえ電源をOFFにしても、電源コードを接続したまま本製品内の部品に触ると感電するおそれがあります。
また、電源プラグはときどき抜いて、乾いた布でほこりやゴミをよくふき取ってください。ほこりがたまったままで、水滴などが付くと発熱し、火災の原因となるおそれがあります。

取り扱い上のご注意

本製品を正しく動作させるため、次の注意事項をお守りください。これらの注意を無視した取り扱いをすると誤動作や故障の原因になります。

- 本製品の電源を一度 OFF にした後、再び ON にするときは 10 秒以上経過してからにしてください。無停電電源装置(UPS)に接続している場合も 10 秒以上経過してから ON になるようにスケジューリングの設定をしてください。
- 本製品を移動する前に電源を OFF にして、電源プラグをコンセントから抜いてください。
- 定期的に本製品を清掃してください。定期的な清掃はさまざまな故障を未然に防ぐ効果があります。
- 落雷等が原因で瞬間的に電圧が低下することがあります。この対策として無停電電源装置等を使用することをお勧めします。
- 本製品を正しく動作させるためにも室温を保てる場所に保管することをお勧めします。装置を保管する場合は、保管環境条件(温度：-20℃～60℃、湿度：20%～80%)を守って保管してください(ただし、結露しないこと)。
- 本製品のそばでは携帯電話や PHS、ポケットベルの電源を OFF にしておいてください。電波による誤動作の原因となります。
- インタフェースケーブルの取り扱いや接続について次の注意をお守りください。
  - 破損したケーブルコネクタを使用しない。
  - ケーブルを踏まない。
  - ケーブルの上にものを載せない。
  - ケーブルの接続がゆるんだまま使用しない。
  - 破損したケーブルを使用しない。
- 本製品は、寒い場所から暖かい場所に急に持ち込むと結露が発生し、そのまま使用すると誤作動や故障の原因となります。保管した大切なデータや資産を守るためにも、使用環境に十分になじませてからお使いください。
- オプションは本体に取り付けられるものであること、また接続できるものであることを確認してください。たとえ本体に取り付けや接続ができても正常に動作しないばかりか、本体が故障することがあります。
- オプションは弊社の純正品をお使いになることをお勧めします。他社製の製品が原因となって起きた故障や破損については保証期間中でも有償修理となります。

保守サービスについて
本製品の保守に関して専門的な知識を持つ保守員による定期的な診断・保守サービスを用意しています。
本製品をいつまでもよい状態でお使いになるためにも、保守サービス会社と定期保守サービスを契約されることをお勧めします。

健康を損なわないためのアドバイス

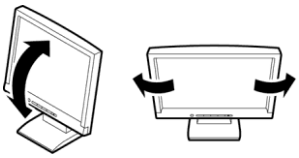
コンピュータ機器を長時間連続して使用すると、身体の各部に異常が起こることがあります。コンピュータを使用するときは、主に次の点に注意して身体に負担がかからないよう心掛けましょう。

よい作業姿勢で

コンピュータを使用するときの基本的な姿勢は、背筋を伸ばして椅子にすわり、キーボードを両手と床がほぼ平行になるような高さに置き、視線が目の高さよりもやや下向きに画面に注がれているという姿勢です。『よい作業姿勢』とはこの基本的な姿勢をとったとき、身体のどの部分にも余分な力が入っていない、つまり緊張している筋肉がもっとも少ない姿勢のことです。
『悪い作業姿勢』、たとえば背中を丸めたかっこうやディスプレイの画面に顔を近づけたままの状態で作業を行うと、疲労の原因や視力低下の原因となることがあります。

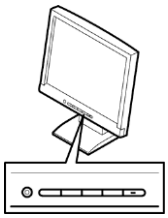
ディスプレイの角度を調節する

ディスプレイの多くは上下、左右の角度調節ができるようになっています。まぶしい光が画面に映り込むのを防いだり、表示内容を見やすくしたりするためにディスプレイの角度を調節することは、たいへん重要です。角度調節をせずに見づらい角度のまま作業を行うと『よい作業姿勢』を保てなくなりすぐに疲労してしまいます。ご使用の前にディスプレイを見やすいよう角度を調整してください。



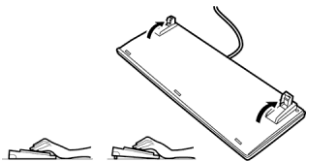
画面の明るさ・コントラストを調節する

ディスプレイは明るさ(ブライトネス)・コントラストを調節できる機能を持っています。年齢や個人差、まわりの明るさなどによって、画面の最適なブライトネス・コントラストは異なりますので、状況に応じて画面を見やすいように調節してください。画面が明るすぎたり、暗すぎたりすると目に悪影響をもたらします。



キーボードの角度を調節する

オプションのキーボードには、角度を変えることができるよう設計されているものもあります。入力しやすいようにキーボードの角度を変えることは、肩や腕、指への負担を軽減するのにたいへん有効です。



機器の清掃をする

機器をきれいに保つことは、美観の面からだけでなく、機能や安全上の観点からも大切です。特にディスプレイの画面は、ほこりなどで汚れると、表示内容が見にくくなりますので定期的に清掃する必要があります。

疲れたら休む

疲れを感じたら手を休め、軽い体操をするなど、気分転換をはかることをお勧めします。

NEC Express5800 シリーズ
US300d

1

US300d について

US300d を導入する際に知っておいていただきたいことについて説明します。

1. **はじめに**

   US300d について説明しています。

2. **各部の名称と機能**

   各部の名称と機能について説明しています。

3. **無線 LAN 機能**

   無線 LAN の機能、注意事項、設定について説明しています。

4. **設置と接続**

   US300d の設置と接続の方法について説明しています。

5. **システム BIOS のセットアップ**

   Basic Input Output System(BIOS)の設定方法について説明しています。

1. はじめに

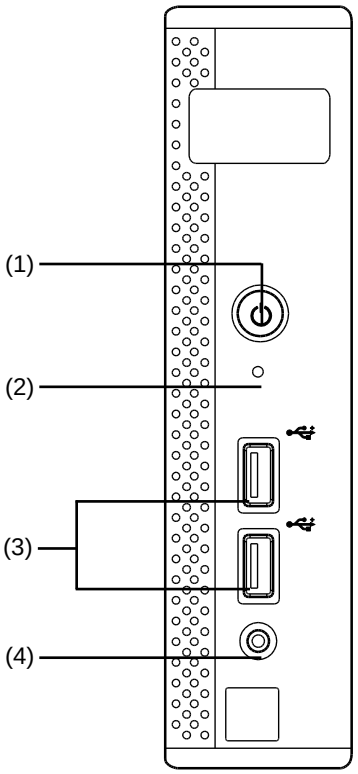
このたびは、NEC のシンクライアント製品をお買い求めいただき、まことにありがとうございます。
US300d は、仮想 PC 型、SBC 型シンクライアントシステムを構築するための卓上型シンクライアント端末です。
シンクライアント用途に適した専用 OS、ハードウェア構成によりセキュアな業務システムを提供します。

US300d の持つ機能を最大限に引き出すためにも、ご使用になる前に本書をよくお読みになり、取り扱いを十分にご理解ください。

2. 各部の名称

US300d の各部の名称とその機能について説明します。

2.1 装置前面



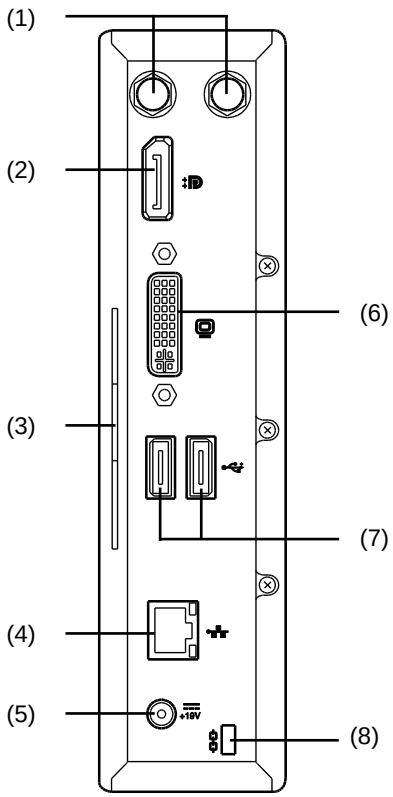
(1)　電源ボタン

(2)　ステータスランプ

(3)　USB2.0 ポート

(4)　コンポジットオーディオポート

2.2 装置背面



(1)　無線 LAN アンテナコネクタ
(無線 LAN モデルのみ)

(2)　ディスプレイポート

(3)　スライドタグ

(4)　LAN コネクタ

(5)　電源コネクタ

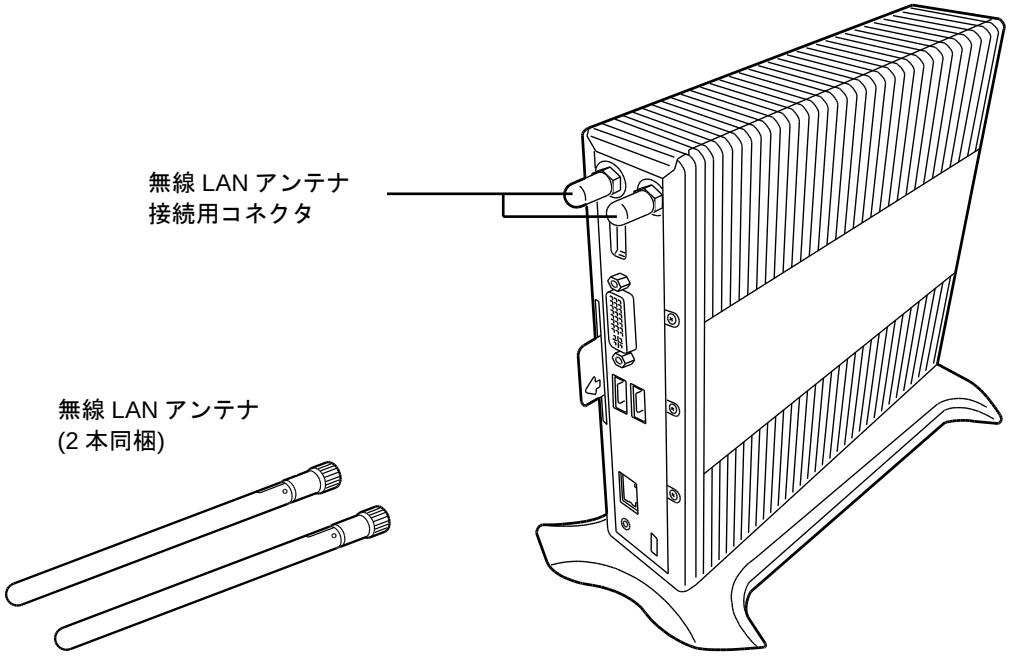
(6)　DVI-I ポート

(7)　USB2.0 ポート

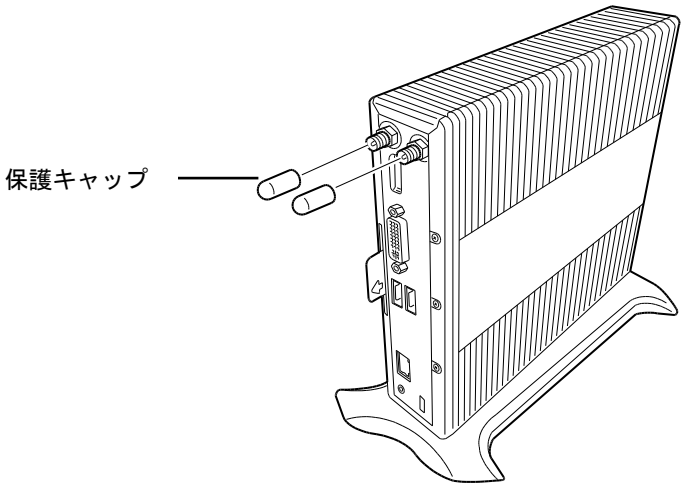
(8)　セキュリティスロット

2.2.1 無線 LAN アンテナ

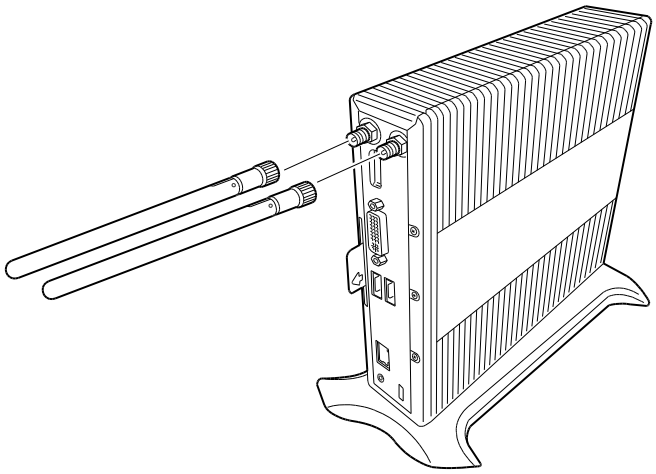
無線 LAN アンテナは、US300d に内蔵されている無線装置（RF モジュール）からの信号を送信し、受信します。



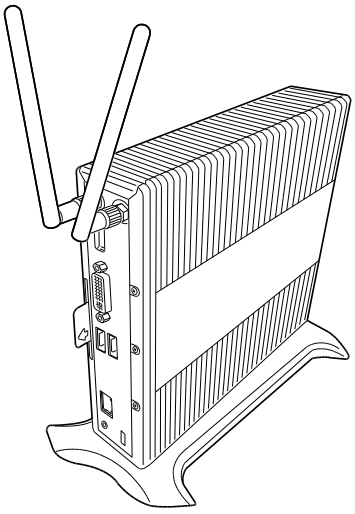
無線 LAN アンテナ接続用コネクタに取り付けられている保護キャップを取り外します。
取り外した保護キャップは、無くさないように保管してください。



同梱されている無線 LAN アンテナを、本体の無線 LAN アンテナポートにしっかりと取り付けてください。



良好な送受信が行えるように、アンテナの向きや角度を調整してください。



2.2.2 USB2.0 ポート

4 つの USB ポートは USB2.0 規格に対応した周辺機器(例えば、キーボード、マウス、HDD)を US300d に繋ぐことができます。

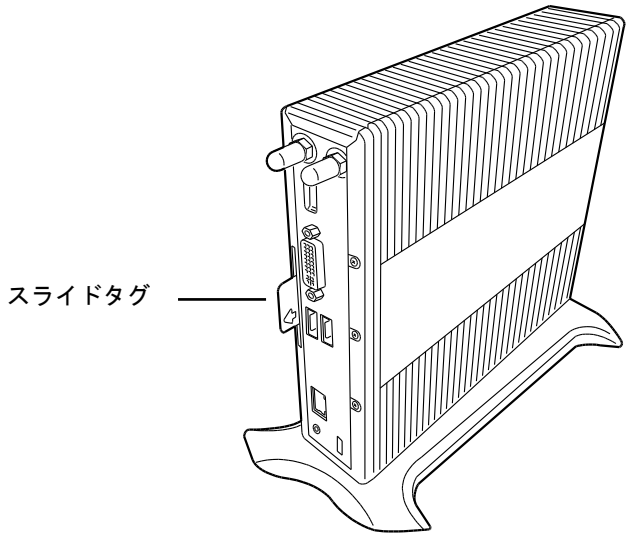
2.2.3 電源コネクタ

US300d に同梱された AC アダプタを使用してください。

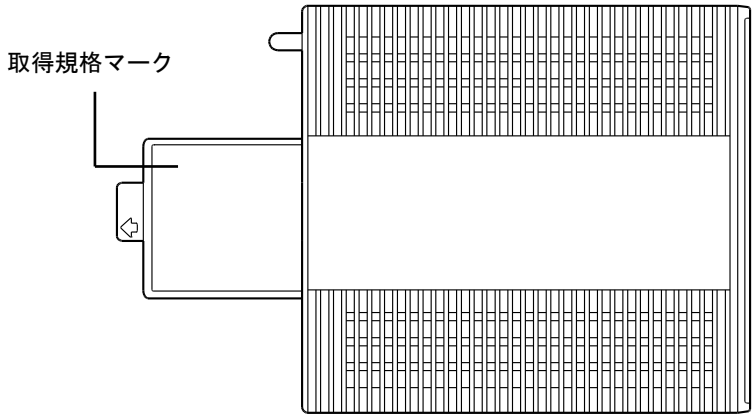
US300d に同梱された AC アダプタと電源コードだけを使用してください。他のアダプタや電源コードは同じように見えても、それらを使うとシステムを損傷させるおそれがあります。

2.2.4 スライドタグ

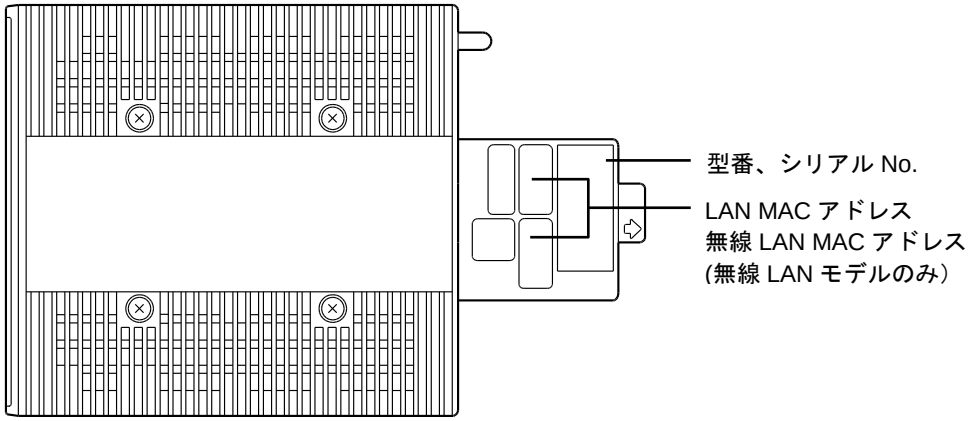
US300d の背面にスライドタグがついています。スライドタグには US300d の型番、シリアル No.、LAN MAC アドレス、取得規格マークなどのラベルが貼付けられています。



スライドタグ表面



スライドタグ裏面



重要

US300d を使用中はスライドタグを収納しておいてください。

3. 無線 LAN

無線 LAN によって、離れているコンピュータ同士でデータやプログラムなどを共有したり、メッセージを送受信することができます。

3.1 使用上の注意

US300d を正しく動作させるため、次の注意事項をお守りください。これらの注意を無視した取り扱いをすると誤動作や故障の原因になります。

- 通信速度・通信距離は、無線 LAN 対応機器や電波環境・障害物・設置環境などの周囲条件によって異なります。
- 電波の性質上、通信距離が離れるに従って通信速度は低下する傾向にあります。より快適にお使いいただくために、無線 LAN 対応機器同士は近い距離で使用することをおすすめします。
- 電子レンジを使用中に無線 LAN(IEEE802.11a/b/g/n)対応機器の通信速度、通信距離が低下する場合があります。無線 LAN(IEEE802.11a/b/g/n)対応機器と電子レンジは離して使用することをおすすめします。
- 無線 LAN(IEEE802.11a/b/g/n)対応機器と Bluetooth™ 対応機器を同時に使用された場合、それぞれの機器の通信速度や通信距離が低下する場合があります。
  無線 LAN(IEEE802.11a/b/g/n)対応機器と Bluetooth™ 対応機器はいずれかをオフにするか、離して使用することをおすすめします。
- ネットワークへの接続には、別売の無線 LAN アクセスポイント(以下アクセスポイント)などが必要です。
- 医療機関側が US300d の使用を禁止した区域では、US300d の電源を切るか無線 LAN 機能をオフにしてください。また、医療機関側が US300d の使用を認めた区域でも、近くで医療機器が使用されている場合には、US300d の電源を切るか無線 LAN 機能をオフにしてください。

3.2 無線 LAN 製品ご使用時におけるセキュリティに関するご注意

無線 LAN では、LAN ケーブルを使用するかわりに、電波を利用してパソコン等と無線アクセスポイント間での情報のやりとりを行うため、電波の届く範囲であれば自由に LAN 接続が可能であるという利点があります。

その反面、電波はある範囲内であれば障害物(壁等)を超えてすべての場所に届くため、セキュリティに関する設定を行っていない場合、以下のような問題が発生する可能性があります。

- 通信内容を盗み見られる
  悪意ある第三者が、電波を故意に傍受し、以下のような通信内容を盗み見られる可能性があります。
  - ID やパスワードまたはクレジットカード番号等の個人情報
  - メールの内容

- 不正に侵入される
  悪意ある第三者が、無断で個人や会社内のネットワークへアクセスし、以下のような行為をされてしまう可能性があります。
  - 個人情報や機密情報を取り出す(情報漏洩)
  - 特定の人物になりすまして通信し、不正な情報を流す(なりすまし)
  - 傍受した通信内容を書き換えて発信する(改ざん)
  - コンピュータウイルスなどの流しデータやシステムを破壊する(破壊)

本来、無線 LAN カードや無線アクセスポイントは、これらの問題に対応するためのセキュリティの仕組みを持っていますので、無線 LAN 製品のセキュリティに関する設定を行って製品を使用することで、その問題が発生する可能性は少なくなります。

セキュリティの設定を行わないで使用した場合の問題を十分理解した上で、お客様自身の判断と責任においてセキュリティに関する設定を行い、製品を使用することをおすすめします。

セキュリティの設定などについて、お客様ご自身で対処できない場合には、ファーストコンタクトセンターまでお問い合わせください。

セキュリティ対策を施さず、あるいは、無線 LAN の仕様上やむを得ない事情によりセキュリティの問題が発生してしまった場合、弊社はこれによって生じた損害に対する責任を負いかねます。

3.3 本機で設定できるセキュリティ

- 次のセキュリティについての設定をする場合、使用するアクセスポイントなどもこれらの設定に対応している必要があります。
- これらの設定は危険性をより低くするための手段であり、安全性を 100%保証するものではありません。

3.3.1 不正アクセスを防ぐ

- アクセスポイントと通信機器の両方に任意の SSID(ネットワーク名)を設定することで、同じ SSID を設定していない通信機器からの接続を回避できます。ただし、第三者に SSID を自動的に検出する機能を持った機器を使用されると、SSID を知られてしまいます。これを回避するには、アクセスポイント側で SSID を通知しないように、SSID の隠蔽の設定をする必要があります。
- 接続するパソコンなどの MAC アドレス(ネットワークカードが持っている固有の番号)をアクセスポイントに登録することで、登録した機器以外はアクセスポイントに接続できなくなります(MAC アドレスフィルタリング)。

3.3.2 盗聴(傍受)を防ぐ

Wi-Fi Alliance が提唱する WPA2/WPA(Wi-Fi Protected Access)機能を利用します。
IEEE802.1X/EAP(Extensible Authentication Protocol)規格によるユーザー認証、従来の WEP 機能に比べて大幅に暗号解読が困難とされる暗号方式 TKIP(Temporal Key Integrity Protocol)や AES(Advanced Encryption Standard)を使用することで、より高度なセキュリティ設定を行うことができます。

US300d の無線 LAN 機能は「WEP(Wired Equivalent Privacy)機能」にも対応しています。
WEP 機能には 64 ビット WEP 対応、128 ビット WEP 対応、152 ビット WEP 対応のものがあり、US300d の無線 LAN 機能は、すべてに対応しています。
ただし、暗号キーを設定していても、暗号キー自体を第三者に知られたり、暗号解読技術によって暗号を解読されたりする可能性があるため、本製品では WPA2/WPA による暗号化をおすすめします。

WPA2/WPA/WEP による暗号化を使用するためには、接続する相手の機器も同じセキュリティ機能に対応している必要があります。

3.4 無線 LAN の設定

本ガイドの「4 章 (13. 無線ローカルエリアネットワーク(LAN)の設定)」をご覧になり、設定を行ってください。

3.5 無線 LAN 機能でできること

US300d の無線 LAN 機能を使用することで、次のようなことができます。

3.5.1 無線 LAN 対応周辺機器(親機)との無線接続

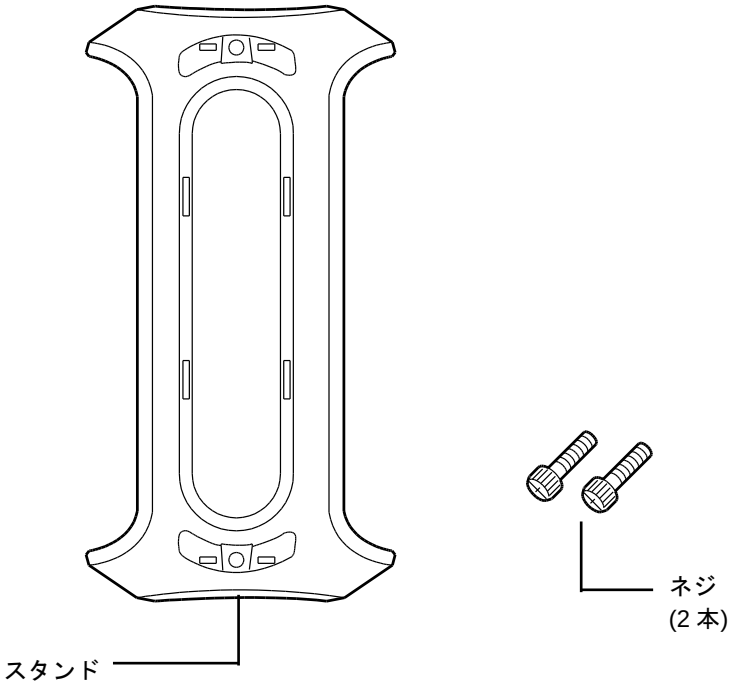
US300d と無線 LAN に対応した別売の周辺機器(親機)を使用すると、ケーブルで接続せずに LAN を利用することができます。例えば、無線 LAN に対応したルータやターミナルアダプタなどを利用してインターネットに接続することができます。

4. 設置と接続

US300d の設置と接続について説明します。

4.1 設置

US300d に添付されている、スタンドを使用して設置します。

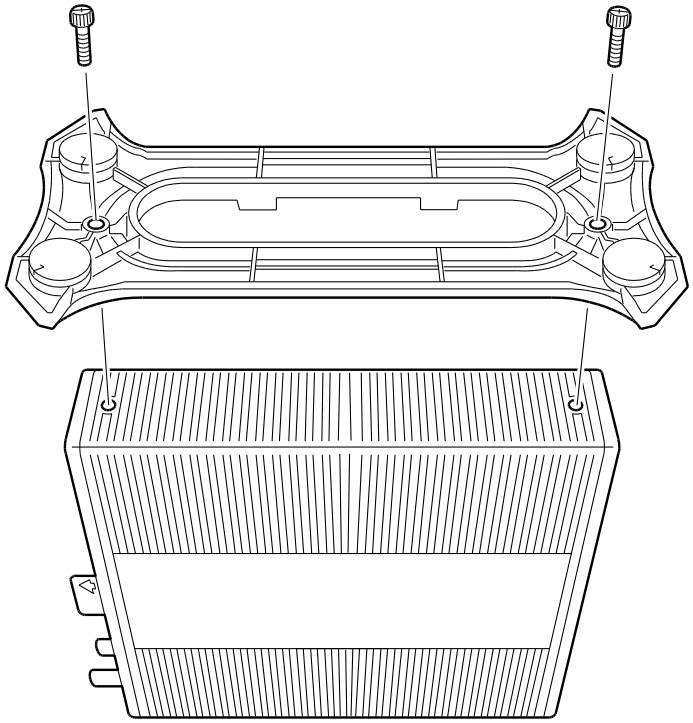


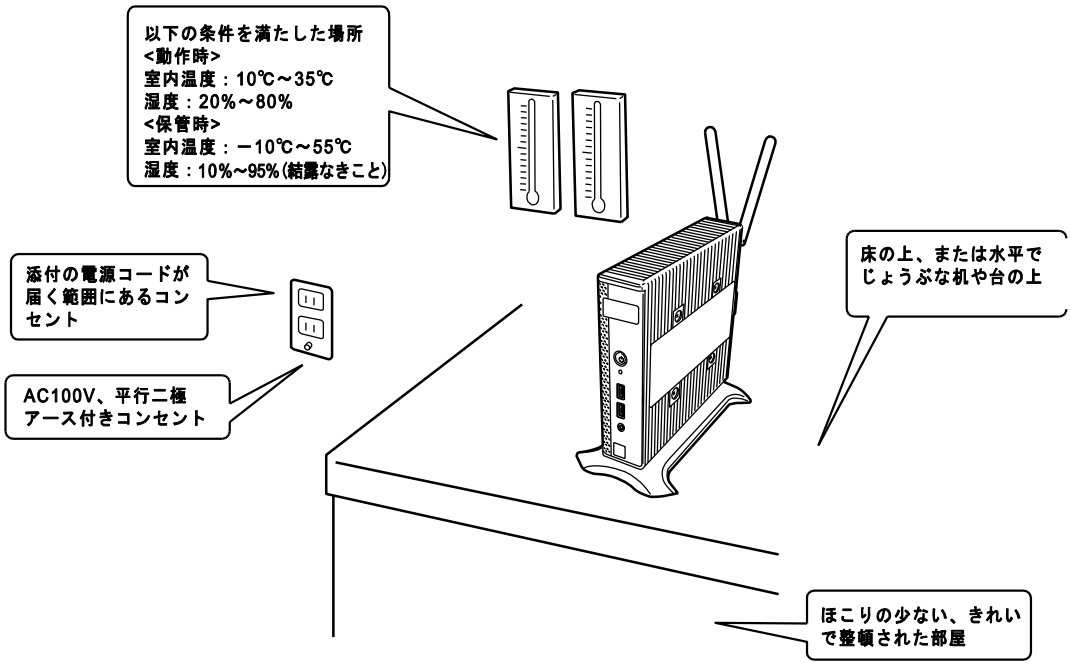
⚠注意

US300dを安全にお使いいただくために次の注意事項を必ずお守りください。指示を守らないと、火傷やけがなどを負うおそれや物的損害を負うおそれがあります。詳しくは、「使用上のご注意」をご覧ください。

- **指定以外の場所に設置しない**

US300d 底面のねじ穴とスタンドのねじ穴を合わせて、同梱のネジで取り付けます。





次に示す条件に当てはまるような場所には、US300d を設置しないでください。これらの場所に US300d を設置すると、誤動作の原因となります。

- 温度変化の激しい場所(暖房器、エアコン、冷蔵庫などの近く)。
- 強い振動の発生する場所。
- 腐食性ガスの発生する場所(大気中に硫黄の蒸気が発生する環境下など)、薬品類の近くや薬品類がかかるおそれのある場所。
- 帯電防止加工が施されていないじゅうたんを敷いた場所。
- 物の落下が考えられる場所。
- 電源コードまたはインタフェースケーブルを足で踏んだり、引っ掛けたりするおそれのある場所。
- 強い磁界を発生させるもの(テレビ、ラジオ、放送/通信用アンテナ、送電線、電磁クレーンなど)の近く(やむを得ない場合は、保守サービス会社に連絡してシールド工事などを行ってください)。
- 本体の電源コードを他の接地線(特に大電力を消費する装置など)と共用しているコンセントに接続しなければならない場所。
- 電源ノイズ(商用電源をリレーなどで ON/OFF する場合の接点スパークなど)を発生する装置の近くには設置しないでください。(電源ノイズを発生する装置の近くに設置するときは電源配線の分離やノイズフィルタの取り付けなどを保守サービス会社に連絡して行ってください。)

4.2 接続

US300d をネットワークに接続します。
ネットワークケーブルを接続してから添付の AC アダプタの電源コードを US300d に接続し、電源プラグをコンセントに接続します。

⚠警告

US300dを安全にお使いいただくために次の注意事項を必ずお守りください。指示を守らないと、人が死亡する、または重傷を負うおそれがあります。詳しくは「使用上のご注意」をご覧ください。

- **ぬれた手で電源プラグを持たない**

⚠注意

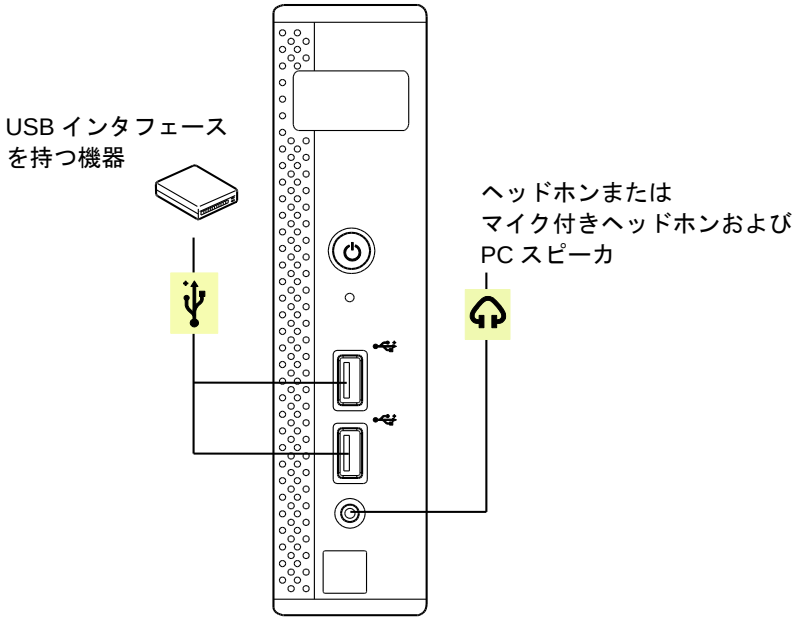
US300dを安全にお使いいただくために次の注意事項を必ずお守りください。指示を守らないと、火傷やけがなどを負うおそれや物的損害を負うおそれがあります。詳しくは、「使用上のご注意」をご覧ください。

- **指定以外のコンセントに差し込まない**
- **たこ足配線にしない**
- **中途半端に差し込まない**
- **指定以外の電源コードを使わない**
- **プラグを差し込んだままインタフェースケーブルの取り付けや取り外しをしない**
- **指定以外のインタフェースケーブルを使用しない**

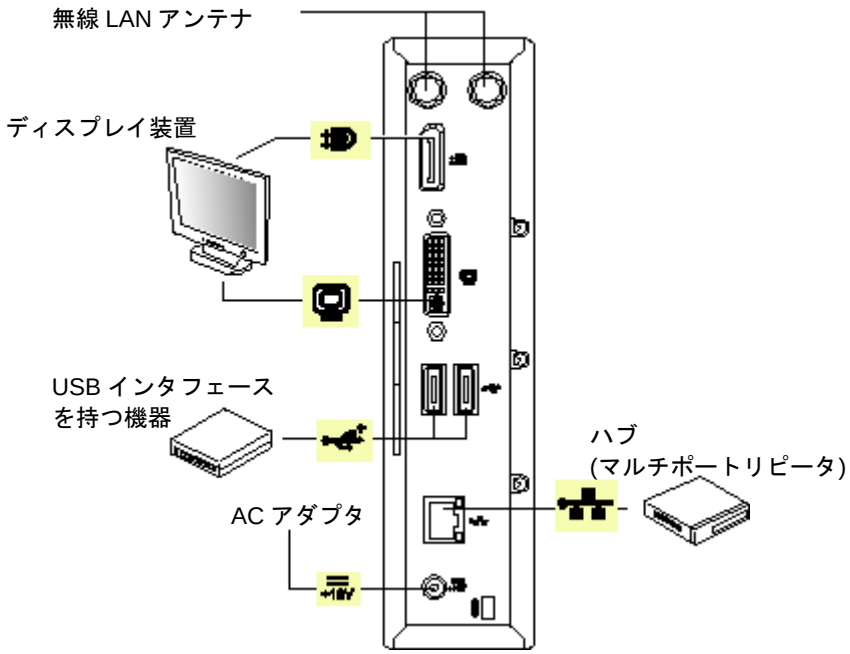
重要

- **US300d および接続する周辺機器の電源を OFF にしてから接続してください。ON の状態のまま接続すると誤動作や故障の原因となります。**
- **サードパーティの周辺機器およびインタフェースケーブルを接続する場合は、お買い求めの販売店でそれらの装置が US300d で使用できることをあらかじめ確認してください。サードパーティの装置の中には US300d で使用できないものがあります。サードパーティの周辺機器、または NEC が認定していない装置やインタフェースケーブルを使用したために起きた US300d の故障については、その責任を負いかねますのでご了承ください。**

装置前面



装置背面



チェック

VGA インタフェースで接続する場合は、US300d に添付している DVI-VGA 変換コネクタを使用してください。
モニタの構成に応じて、別売りのデュアルモニター用スプリッターケーブル[N8120-107]や DP-DVI 変換コネクタ[N8005-1004]を使用 してください。

5. システム BIOS のセットアップ

Basic Input Output System(BIOS)の設定方法について説明します。

本製品を導入したときやオプションの増設/取り外しをするときはここで説明する内容をよく理解して、正しく設定してください。

5.1 概要

SETUP はハードウェアに基本設定をするためのユーティリティーツールです。このユーティリティーは本体内のフラッシュメモリに標準でインストールされているため、専用のユーティリティーなどがなくても実行できます。

SETUP で設定される内容は、出荷時に最も標準で最適な状態に設定していますのでほとんどの場合において SETUP を使用する必要はありませんが、この後に説明するような場合など必要に応じて使用してください。

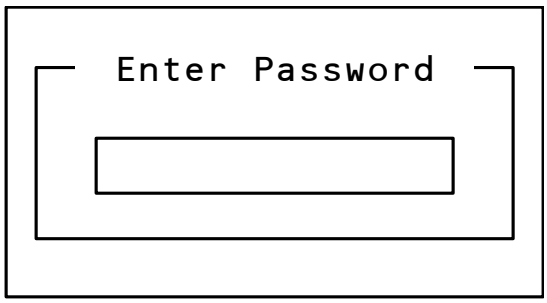
重要

- **SETUP の操作は、システム管理者(アドミニストレーター)が行ってください。**
- **SETUP では、パスワードを設定することができます。**
- **初期パスワードは "Fireport" (大文字・小文字区別)です。**
- **SETUP は、最新のバージョンがインストールされています。このため設定画面が本書で説明している内容と異なる場合があります。設定項目については、オンラインヘルプを参照するか、保守サービス会社に問い合わせてください。**
- **SETUP は Exit メニューまたは<Esc>、<F10>キーで必ず終了してください。SETUP を起動した状態でパワーオフ、リセットを行った場合には SETUP の設定が正しく更新されないことがあります。**

5.2 起動

本製品の電源を ON にして、画面表示がされるまでに<Del>キーを押し続けると、SETUP が起動して Main メニュー画面を表示します。

SETUP メニューを初めて起動するとき、もしくは、以前に SETUP を起動してパスワードの変更をしている場合は、パスワードを入力する画面が表示されます。パスワードを入力してください。
初めて起動するときのパスワードは“Fireport” (大文字・小文字区別)です。



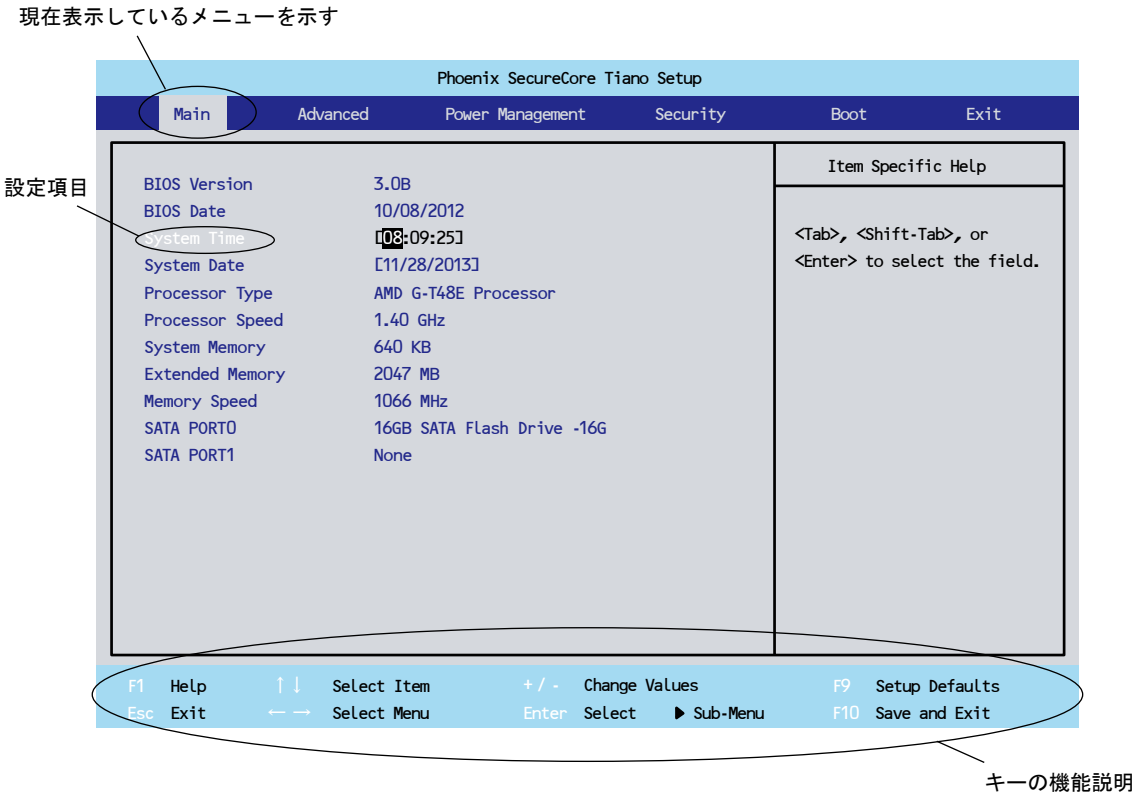
パスワードの入力は、３回まで行えます。３回とも誤ったパスワードを入力すると、本製品は動作を停止します（これより先の操作を行うことができません）。電源を OFF にしてください。パスワードを３回間違えても BIOS はロックされません。再度電源を ON にして SETUP の起動からやり直してください。

重要

BIOS 診断画面がエラーで停止した場合は、＜Del＞キーを押して一度 SETUP メニューを起動してください。
BIOS 診断画面がエラーで停止した場合は、＜F1＞キーを押さないでください。BIOS SETUP メニューの設定が初期値に戻ります。

5.3 キーと画面の説明

キーボード上の次のキーを使って SETUP を操作します(キーの機能については、画面下にも表示されています)。



カーソルキー(←、→)	Main, Advanced, Power Management, Security, Boot, Exit などのメニューを選択します。
カーソルキー(↑、↓)	画面に表示されている項目を選択します。文字の表示が反転している項目が現在選択されています。
<+>キー/<->キー	選択している項目の値(パラメーター)を変更します。サブメニューを選択している場合、このキーは無効です。
<+>キー	選択している項目の現在の設定値をひとつ次の設定値に変更します (増加)。
<->キー	選択している項目の現在の設定値をひとつ前の設定値に変更します (減少)。
<F1>キー	SETUP 画面内のキー操作のヘルプを表示します。
<F9>キー	すべての設定値にデフォルト値を書き込みます
<F10>キー	設定したパラメーターを保存して SETUP を終了します。
<Esc>キー	一つ前の画面に戻ります。押し続けると「Exit」メニューに進みます。
<Enter>	サブメニューの選択をします。

5.4 パラメーターと説明

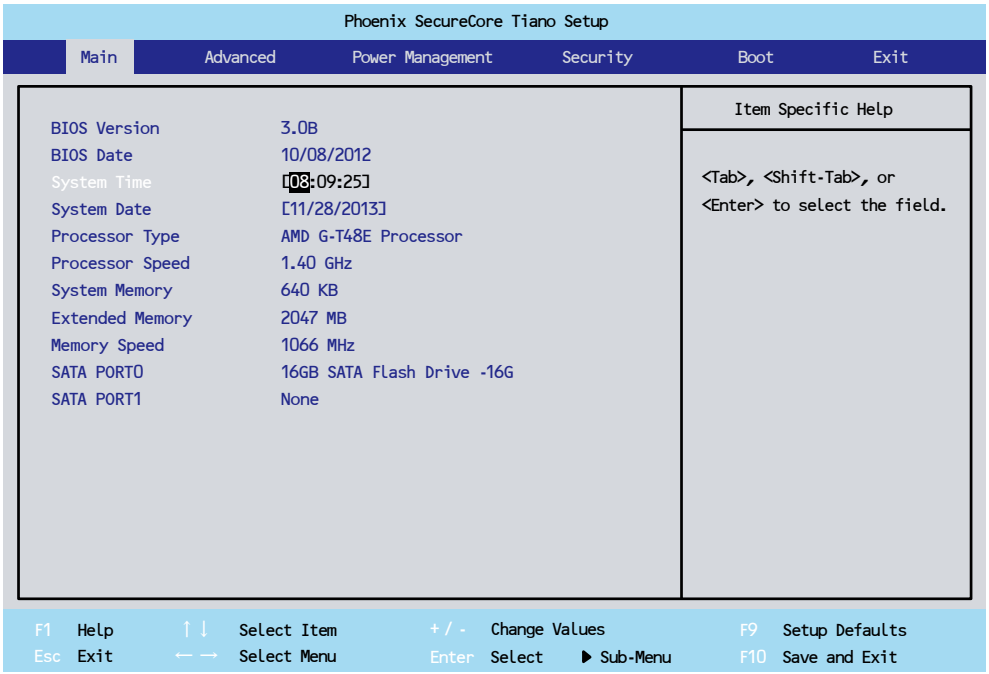
Setup には大きく分けて 6 種類のメニューがあります。

- Main メニュー
- Advanced メニュー
- Power Management メニュー
- Security メニュー
- Boot メニュー
- Exit メニュー

このメニューの中からサブメニューを選択することによって、さらに詳細な機能表示ができます。次に画面に表示されるメニュー別に設定できる機能やパラメーター、出荷時の設定を説明します。

5.4.1 Main

SETUP を起動すると、はじめに Main メニューが表示されます。



Main メニューの画面上で設定できる項目とその機能を示します。

項目については次の表を参照してください。

項　目	パラメーター	説　明
System Time	HH:MM:SS	時刻の設定をします。
System Date	MM/DD/YYYY	日付の設定をします。

重要

BIOS のパラメーターで時刻や日付の設定が正しく設定されていることを必ず確認してください。次の条件に当てはまる場合は、運用の前にシステム時計の確認・調整を行ってください。

- **装置の輸送後**
- **装置の保管後**

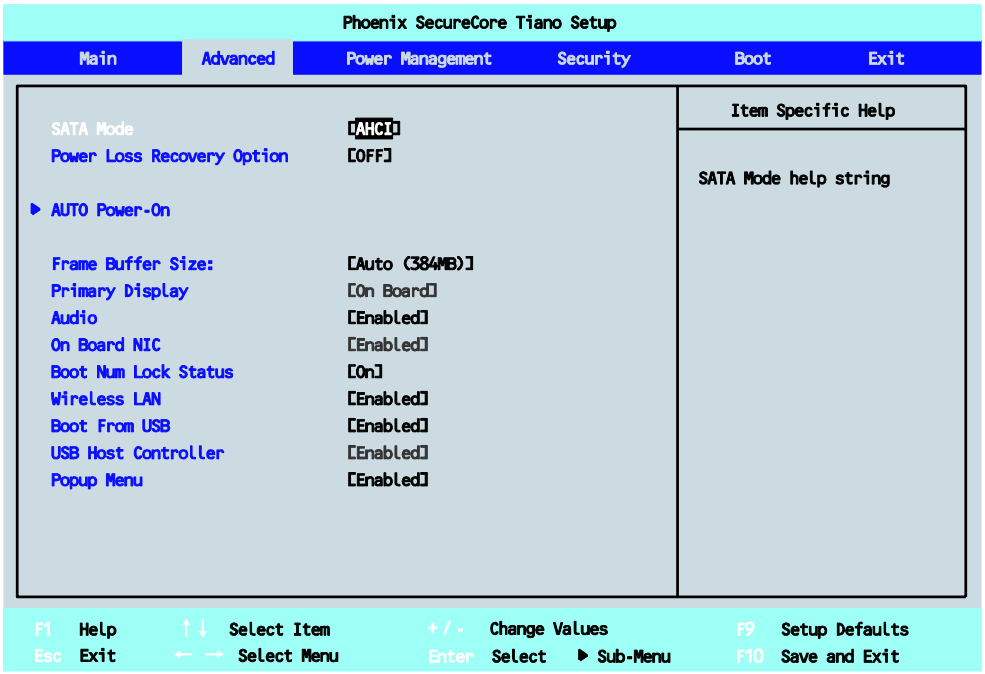
システム時計は、毎月 1 回程度の割合で確認してください。

システム時刻を調整しても時間の経過と共に著しい遅れや進みが生じる場合は、お買い求めの販売店、または保守サービス会社に保守を依頼してください。

5.4.2 Advanced

カーソルを「Advanced」の位置に移動させると、Advanced メニューが表示されます。

項目の前に「▶」が付いているメニューは、選択して「Enter」を押すと、サブメニューが表示されます。



Advanced メニューの画面上で設定できる項目とその機能を示します。

項目については次の表を参照してください。

項　目	パラメーター	説　明
SATA Mode	IDE [AHCI]	SATAモードを選択します。
Power Loss Recovery Option	Always On [Off] Last State	停電時の復旧オプションを指定します。
AUTO Power-On	—	自動パワーオンの設定を確認します。
Frame Buffer Size	Auto (384MB) 64MB 128MB 256MB 384MB 512MB 1GB	グラフィックのメモリサイズの設定をします。
Audio	Disabled [Enabled]	Audioの有効/無効を設定します。
Boot Num Lock Status	[On] Off	シンクライアント起動時の数字キーパッドの有効/無効を設定します。
Wireless LAN	Disabled [Enabled]	無線LANの有効/無効を設定します。
Boot From USB	Disabled [Enabled]	USBからのブートの有効/無効を設定します。
Popup menu	Disabled [Enabled]	設定変更しないでください。

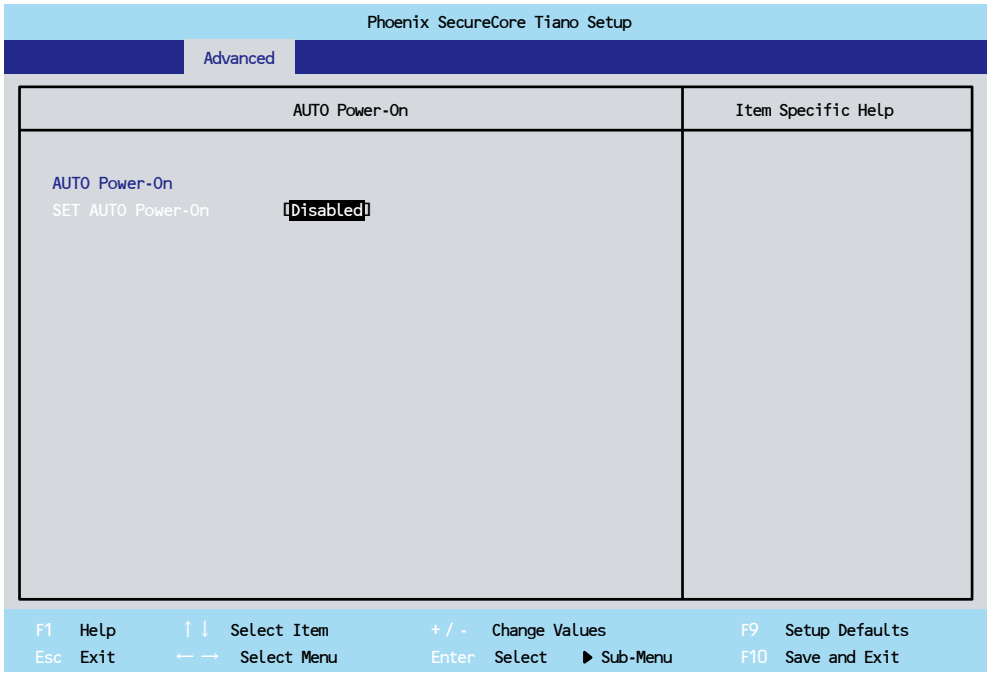
パラメーター欄の[　] は BIOS のデフォルト値です。

SATA Mode は必ず AHCI に設定してください。工場出荷時に AHCI に設定しています。

Exit – Load Setup Defaults を行うと IDE の設定に変わりますので必ず AHCI の設定に変更してください。

5.4.3 AUTO Power-On

Advanced メニューで「AUTO Power-On」を選択すると、自動パワーオンの設定を確認できます。



AUTO Power-On メニューの画面上で設定できる項目とその機能を示します。

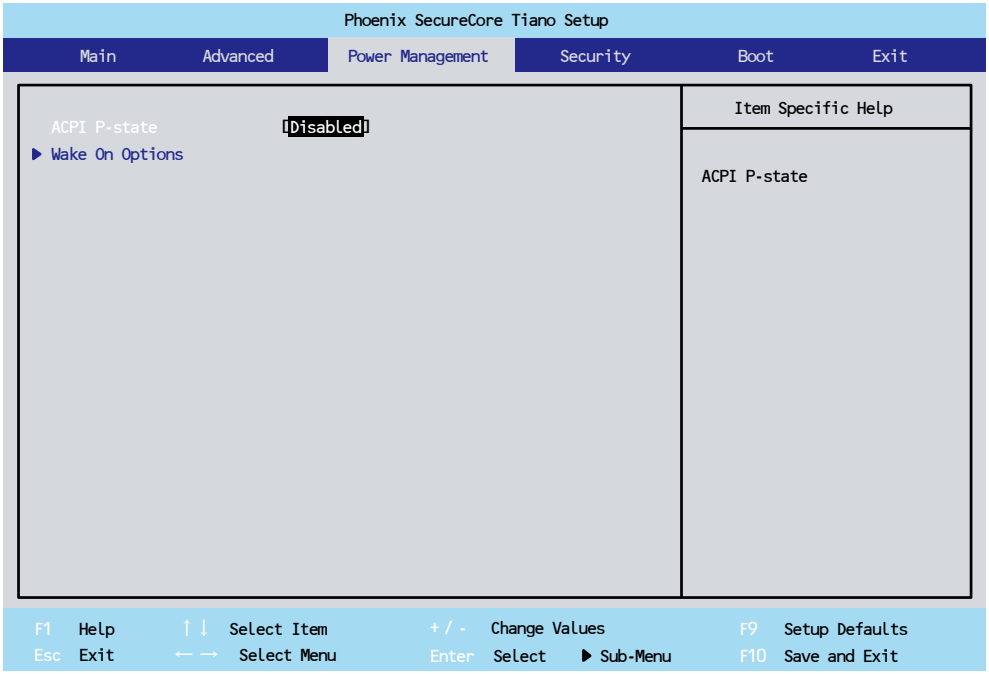
項目については次の表を参照してください。

項　目	パラメーター	説　明
SET AUTO Power-On	Enabled [Disabled]	自動パワーオンの有効/無効を設定します。

パラメーター欄の[　] は BIOS のデフォルト値です。

5.4.4 Power Management

カーソルを「Power Management」の位置に移動させると、Power Management メニューが表示されます。



Power Management メニューの画面上で設定できる項目とその機能を示します。

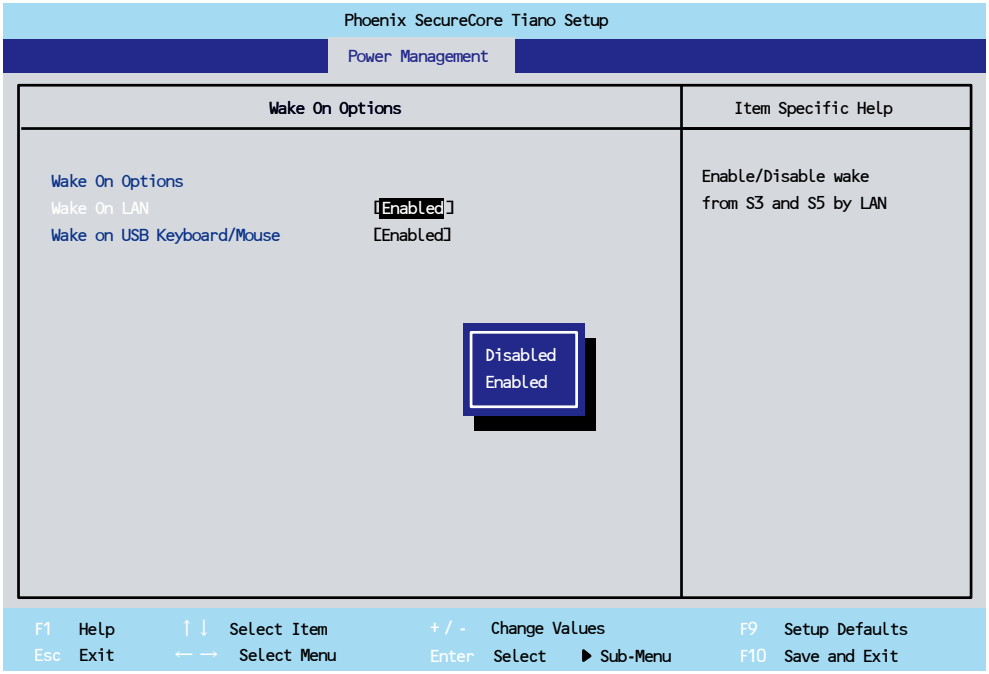
項目については次の表を参照してください。

項　目	パラメーター	説　明
ACPI P-state	[Disabled] Enabled	設定変更しないでください。
Wake On Options	ー	デバイスからの Wakeup設定を確認します。

パラメーター欄の[　] は BIOS のデフォルト値です。

5.4.5 Wake On Options

Power Management メニューで「Wake On Options」を選択すると、デバイスからの Wakeup 設定を確認できます。



Wake On Options メニューの画面上で設定できる項目とその機能を示します。

項目については次の表を参照してください。

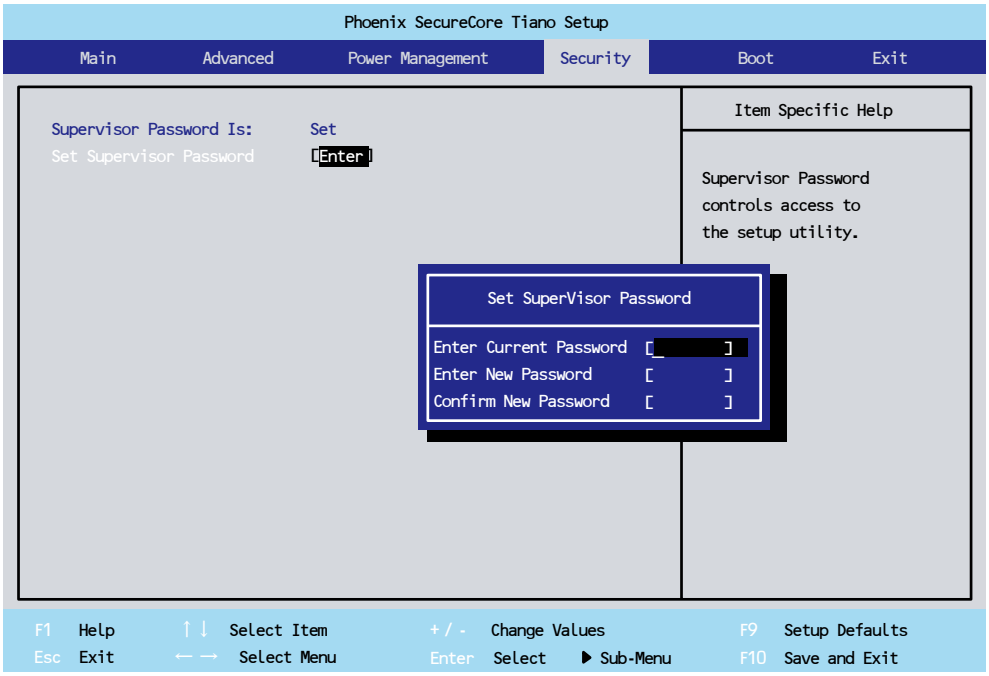
項　目	パラメーター	説　明
Wake On LAN	[Enabled] Disabled	設定変更しないでください。
Wake on USB Keyboard Mouse	[Enabled] Disabled	設定変更しないでください。

パラメーター欄の[　] は BIOS のデフォルト値です。

重要　**装置がスリープ状態の時に、キーボードやマウスを操作すると Wakeup します。**

5.4.6 Security

カーソルを「Security」の位置に移動させると、Security メニューが表示されます。



Security メニューの画面上で設定できる項目とその機能を示します。

項目については次の表を参照してください。

項　目	パラメーター	説　明
Supervisor Password is	Set	パスワードの設定状態を示します。
Set Supervisor Password		初期パスワードは “Fireport” です。 (大文字/小文字は区別します)

パラメーター欄の[　] は BIOS のデフォルト値です。

5.4.7 Boot

カーソルを「Boot」の位置に移動させると、Boot メニューが表示されます。

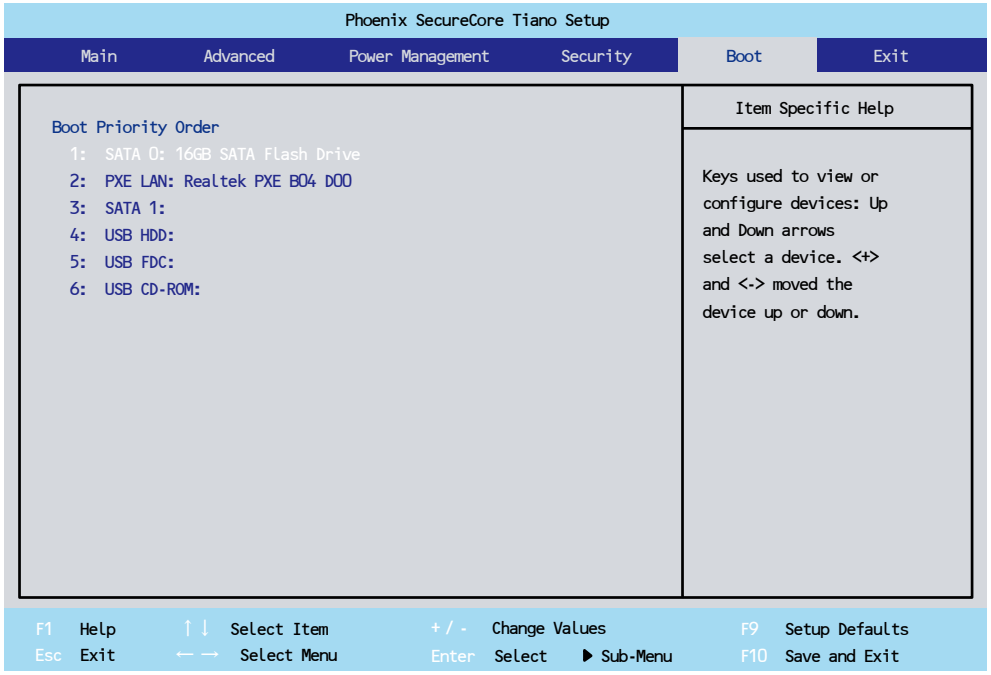
起動するデバイスを優先順に従ってリスト表示します。先頭デバイスからオペレーティングシステムを起動します。オペレーティングシステムが存在しないなど起動に失敗した場合は次のデバイスから起動します。

起動するデバイスを変更するには<↑><↓>キーを使用して変更したいデバイスにカーソルを合わせます。
<+>キーを押すとリストの上側に移動し、<->キーを押すとリストの下側に移動します。

出荷時の設定は、以下の優先順位に設定されています。

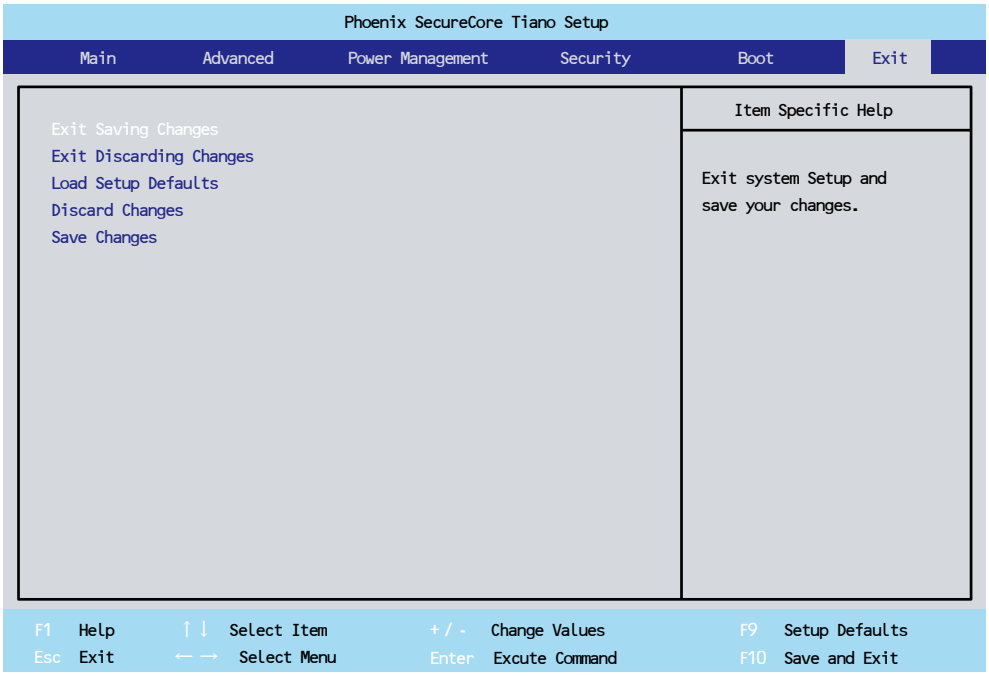
1. SATA フラッシュドライブ
2. オンボード LAN デバイス
3. SATA デバイス
4. USB HDD デバイス
5. USB FDC デバイス
6. USB CD-ROM デバイス

実際の画面には、以下のように表示されます。



5.4.8 Exit

カーソルを「Exit」の位置に移動させると、Exit メニューが表示されます。



このメニューの各オプションについて説明します。

設定項目	説　明
Exit Saving Changes	変更した内容を保存しBIOSセットアップメニューを終了します。(<F10>キーを押す終了方法と同じとなります。)
Exit Discarding Changes	設定値を保存せずに(現在設定した値を破棄して)、BIOSセットアップメニューを終了します。 ただし、Securityメニューで設定変更したPasswordは保存されます。
Load Setup Defaults	すべての設定値にデフォルト値を書き込みます。ここでの「デフォルト値」は、工場出荷時の値とは異なる場合があります。
Discard Changes	変更前の値に戻します。(BIOSセットアップメニューは継続されます。)
Save Changes	変更した値を保存します。(BIOSセットアップメニューは継続されます。)

重要

Load Setup Defaults を行うと Advance メニューの SATA Mode の設定が IDE に変更されます。IDE の設定のままだと US300d は起動しません。
必ず AHCI の設定に変更してください。

NEC Express5800 シリーズ
US300d

2 基本事項の概要

この章では、シンクライアントの使用するための基本事項について説明しています。

1. ログオン
2. ユーザーデスクトップについて
3. シンクライアントを設定する前に
4. プリンターの接続
5. モニターの接続
6. ログオフ

シンクライアントのリブート後も維持されるようにシンクライアント上で行った構成を保存するには、必ずシンクライアントを設定する前に File-Based Write Filter (FBWF)を無効にし、構成後に再び有効にしてください(「2 章(3. シンクライアントを設定する前に)」を参照してください)。

1. ログオン

シンクライアントにログオンした後の表示は、管理者設定によって異なります。ユーザーアカウント(5 章(10. 「ユーザーアカウント」ウィンドウによるユーザーとグループの管理)」を参照)を作成した後、管理者はユーザーアカウントに対し自動ログオンか(「4 章(12. Winlog による自動ログオンの有効化／無効化)」を参照)、ユーザー認証情報(ユーザー名、パスワード、ドメイン)に基づく手動ログオンかを設定できます。

セキュリティ上、すべてのシンクライアントで管理者のデフォルトパスワードを変更することをお勧めします(新たに設定した管理者パスワードを忘れると管理者としてログオンすることができなくなるので、ご注意ください)。管理者としてシンクライアントにログオンし、CTRL+ALT+DEL キー→「Windows のセキュリティ」ウィンドウ→「パスワードの変更」→「パスワードの変更」ダイアログボックスでパスワードを変更します。シンクライアントでパスワードを変更する前に必ず File Based Write Filter (FBWF)を無効にし、パスワード変更後に再度有効にしてください(「2 章(3.1 File-Based Write Filter (FBWF) ユーティリティーの使用方法)」を参照)。

1.1 自動ログオン

デフォルトでは、Administrators グループのメンバーとしてではなく Users グループのメンバーとしてシンクライアントのユーザーデスクトップに自動ログオンするよう設定されています。

ユーザーデスクトップへの自動ログオン後、デフォルトでは USB デバイスの自動再生は無効になっています。USB デバイスの自動再生を有効にするには、「デバイスとプリンター」ダイアログボックス(「スタート」→「コントロールパネル」→「デバイスとプリンター」)で対象となる USB デバイスを選択し、「自動再生」をクリックします。

別のユーザーまたは管理者としてログオンするには、以下の手順を実行してください。

1. SHIFT キーを押しながら「ログオフ」ボタン(「スタート」→「ログオフ」)を「ログオン」ウィンドウが表示されるまで押し、現在のデスクトップをログオフします。

2. 以下のガイドラインに従ってください(パスワードの大文字と小文字は区別されます)。
   - 管理者アカウントの場合、デフォルトのユーザー名は「administrator」で、パスワードは「Wyse#123」です。
   - ユーザーアカウントの場合、デフォルトのユーザー名は「user」で、パスワードは「Wyse#123」です。

管理者は Winlog を使用し、管理者として「Windows へログオン」ウィンドウから簡単にシンクライアントにログオンできるよう設定できます(「4 章(12. Winlog による自動ログオンの有効化／無効化)」を参照してください)。

1.2 手動ログオン

自動ログオンが有効でない場合は、シンクライアントの起動時に「Windows へログオン」ウィンドウが表示されます。
以下のガイドラインに従ってください(パスワードの大文字と小文字は区別されます)。

- 管理者アカウントの場合、デフォルトのユーザー名は「administrator」で、パスワードは「Wyse#123」です。
- ユーザーアカウントの場合、デフォルトのユーザー名は「user」で、パスワードは「Wyse#123」です。

2. ユーザーデスクトップについて

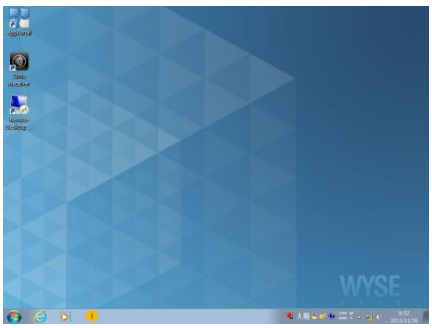
サーバーにログオンした後の表示は、管理者設定によって異なります。

標準的な Windows Embedded Standard 7 デスクトップの機能および「スタート」メニュー項目については、Microsoft 社のマニュアルを参照してください。
(http://support.microsoft.com のマイクロソフトサポートオンライン→Windows 7 サポートセンター)

ユーザーデスクトップ

一般的に、フルユーザータスクバー、デフォルト接続アイコンが表示されたデスクトップ、「スタート」メニュー(ユーザーメニューを開くには「スタート」ボタンをクリック)、およびユーザーシステムトレイのアイコンが表示されます。

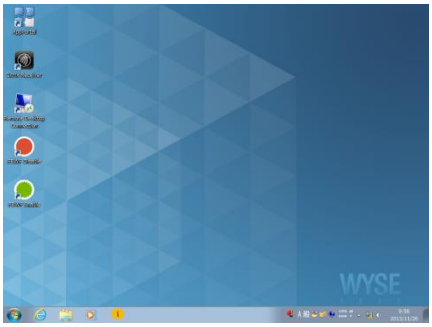
使用したいデスクトップ接続アイコンをクリックするか、「スタート」メニューの接続リンクを使用するだけで、接続の確立または切り替えができます。「3 章 便利なユーザー機能」も参照してください。



管理者デスクトップ

フル管理者タスクバー、デフォルト接続アイコンが表示されたデスクトップ、FBWF アイコン、右クリックで表示されるデスクトップポップアップメニュー、「スタート」メニュー(管理者メニューを開くには「スタート」ボタンをクリック)、および管理者システムトレイのアイコンが表示されます。

管理者コントロールパネル(「スタート」→「コントロールパネル」)には、標準的なコントロールパネルアイコンに加え、ユーザー環境設定とシステム管理の拡張リソースセットが含まれています。「4 章 便利な管理者機能」も参照してください。



3. シンクライアントを設定する前に

一部のユーティリティーのシンクライアント保護機能により、シンクライアントの設定はログオフおよび再起動後に失われます。フラッシュメモリへの誤った書き込みを防止し、不要な情報がローカルディスクに保存されないように消去するユーティリティーによって、ローカル設定およびプロファイル設定は削除されます。ユーティリティーによるシンクライアントの保護も重要ですが、管理者は、シンクライアントのログオフや再起動後も設定を維持したい場合があります。

シンクライアントを設定する前に、「2 章(3.1 File-Based Write Filter (FBWF)ユーティリティーの使用方法)」および「2 章(3.2 NetXClean ユーティリティーの使用方法)」を参照してください。

3.1 File-Based Write Filter (FBWF)ユーティリティーの使用方法

FBWF ユーティリティーは、フラッシュメモリへの誤った書き込みからシンクライアントを保護することにより、シンクライアントでのコンピューター処理にセキュアな環境を提供します。FBWF キャッシュのファイルをコミットしないと、変更した設定はシンクライアントの再起動時に失われます。シンクライアントの設定を変更し再起動後も設定を維持するようにできるのは、管理者のみです。

1. 管理者としてログオンします(「2 章(1. ログオン)」を参照してください)。

2. デスクトップの「FBWF Disable」アイコン(赤)をダブルクリックし、FBWF を無効にします。これにより、フィルターが無効になり、システムがリブートされます。

3. ユーザーデスクトップへの自動ログオンが有効な場合は、ユーザーデスクトップをログオフし、手順 1 と同様に管理者としてログオンします。

4. 本書の手順に従って、シンクライアントを設定します。

5. 設定完了後は、デスクトップの「FBWF Enable」アイコン(緑)をダブルクリックし、FBWF を有効にします。これにより、FBWF が有効になり、システムがリブートされます。これでシンクライアントの設定が保存され、リブート後も維持されます。

FBWF については、「5 章(3. File Based Write Filter (FBWF)の使用方法)」を参照してください。

3.2 NetXClean ユーティリティーの使用方法

NetXClean は、不要な情報をローカルディスクに格納しないようにするクリーンアップユーティリティーです。プリンターなどの特定のプロファイル設定を維持したい場合等、明示的に宣言したプロファイルを消去しないようにするには NetXClean の設定が必要になります。

NetXClean については、「5 章(4. NetXClean ユーティリティーについて)」を参照してください。

NetXClean の使用方法の詳細については、Wyse ナレッジベースソリューション#10621 (http://www.wyse.com/kb)を参照してください。

4. プリンターの接続

USB 接続でパラレルプリンターをシンクライアントに接続するには、USB プリンター変換ケーブルが必要です(本製品には添付されていません)。ご使用前に、プリンタードライバーのインストールガイドに従ってプリンタードライバーをインストールしてください。プリンターの接続については、「4 章(3. デバイスとプリンターの設定)」を参照してください。

5. モニターの接続

US300d は本体の DVI-I ポートやディスプレイポート、DVI-VGA 変換コネクタ、オプションのデュアルディスプレイ用スプリッターケーブル[N8120-107]、DP-DVI 変換コネクタ[N8005-1004]を使用してモニターに接続することができます。デュアルモニター表示の設定については、「4 章(4. デュアルモニター表示の設定)」を参照してください。

5.1 サポートされるモニタ構成

モニタ構成	DVI-Iポート	DisplayPort
シングル	DVI-D	-
	VGA(*1)	-
	DVI-I to DVI-D (*2)	-
	DVI-I to VGA (*2)	-
	-	DP
	-	DP-DVI変換コネクタ(*3)
デュアル	DVI-I to DVI-D / VGA (*2)	-
	DVI-D	DP
	VGA(*1)	DP
	DVI-I to DVI-D(*2)	DP
	DVI-I to VGA(*2)	DP
	DVI-D	DP-DVI変換コネクタ(*3)
	VGA(*1)	DP-DVI変換コネクタ(*3)
	DVI-I to DVI-D(*2)	DP-DVI変換コネクタ(*3)
	DVI-I to VGA(*2)	DP-DVI変換コネクタ(*3)

(*1) 標準添付品の DVI-VGA 変換コネクタを使った VGA 出力

(*2) デュアルディスプレイ用スプリッターケーブル[N8120-107]

(*3) DP-DVI 変換コネクタ[N8005-1004]

純正オプション以外のモニタについてはサポート対象外です。実運用環境への導入に関しては、運用環境に基づいた設定で十分な事前検証を行い、問題ないことを確認してから使用してください。

6. ログオフ

「ログオフ」メニュー(「スタート」→「ログオフ」)を使用して、シンクライアントをログオフ、再起動、スリープ、およびシャットダウンすることができます。「Windows のセキュリティ」ウィンドウ(CTRL+ALT+DEL キー)からシンクライアントをログオフすることもできます。

自動ログオンが有効な場合は、ログオフすると、シンクライアントが即座にデフォルトのユーザーデスクトップにログオンします。シンクライアントを終了するには、シャットダウンを使用してください。

NEC Express5800 シリーズ
US300d

3 便利なユーザー機能

この章では、「すべてのプログラム」メニュー(「スタート」→「すべてのプログラム」)にある以下のユーザー向けの機能の概要について説明します。

1. **Internet Explorerによるインターネット閲覧**
2. **Dell Wyseシンクライアント情報の表示**
3. **Citrix Receiver (Citrixサーバーへの接続)**
4. **Ericom社PowerTerm® Terminal Emulationとの接続の管理**
5. **リモートデスクトップ接続の確立**
6. **VMware View Clientによる仮想デスクトップへの接続**
7. **Quest vWorkspaceによる仮想デスクトップへの接続**

I. Internet Explorer によるインターネット閲覧

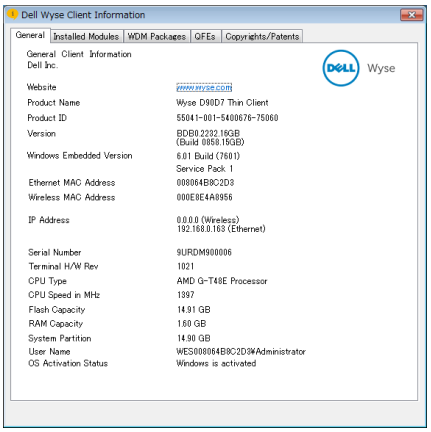
Microsoft Internet Explorer 10 を使用してインターネット閲覧が可能です。ブラウザーは、「スタート」→「すべてのプログラム」→「Internet Explorer」より起動します。ブラウザーには、出荷時に選択されているインターネットオプション設定があります。これはフラッシュメモリへの書き込みを制限し、使用可能フラッシュメモリ容量を使い果たさないようにするための設定なので、変更しないでください。ブラウザーリソースがさらに必要な場合は、ICA または RDP セッションを使用して別のブラウザーにアクセスできます。

ヒント

Internet Explorer の保護モードのステータスは、オフです。これは、ビルド内でユーザーアクセス制御(UAC)が無効になっているためです。ビルドに含まれる File Based Write Filter (FBWF)により、システムが保護されます(「File Based Write Filter (FBWF)の使用方法」を参照してください)。

2. Dell Wyse シンクライアント情報の表示

シンクライアントの情報を表示するには、「Dell Wyse Client Information」ダイアログボックスを使用します。「Dell Wyse Client Information」ダイアログボックスは「すべてのプログラム」→「Dell Wyse Client Information」で表示されます。ダイアログボックスに表示される情報は、ソフトウェアリリース版数によって異なります。たとえば、「General」タブをクリックすると、Web サイト、製品名、製品 ID、バージョン、Windows Embedded Standard バージョン、イーサネット MAC アドレス、ワイヤレス MAC アドレス、IP アドレス、シリアル番号、ターミナルハードウェアのリビジョン、CPU の種類、CPU 速度(MHz)、フラッシュメモリの容量、RAM の容量、システムパーティション、ユーザー名などの情報が表示されます。



以下のタブをクリックして、シンクライアント情報をさらに表示することもできます。

- **Installed Modules**
  シンクライアントにインストールされているアプリケーションのリストを表示します。

- **WDM Packages**
  シンクライアントに適用されている WDM パッケージのリストを表示します(「6 章(4. Wyse Device Manager ソフトウェアによるリモート管理)」を参照してください)。

- **QFEs**
  シンクライアントに適用されている Microsoft QFE (旧ホットフィックス)のリストを表示します。

- **Copyrights/Patents**
  Wyse の著作権および特許情報を表示します。

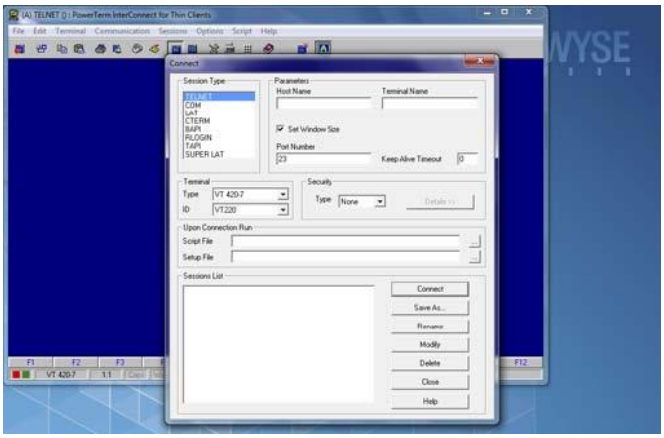
3. Citrix Receiver (Citrix サーバーへの接続)

Citrix Receiver を使用して、デスクトップからサーバー上で動作しているリモートアプリケーションに接続できます。Receiver を起動するには、「スタート」→「すべてのプログラム」→「Citrix Receiver」をクリックするか、デスクトップの「Citrix Receiver」アイコンをダブルクリックしてください。ICA クライアントアプリケーションのマニュアルは Citrix の Web サイトで入手できます(http://www.citrix.com)。

4. Ericom 社 PowerTerm® Terminal Emulation との接続の管理

接続を管理するには、PowerTerm Session Manager (「スタート」→「すべてのプログラム」→「Ericom-PowerTerm Terminal Emulation」→「PowerTerm Session Manager」)を使用します。

接続情報を設定するには、TELNET ウィンドウおよび「Connect」ダイアログボックス(「スタート」→「すべてのプログラム」→「Ericom-PowerTerm Terminal Emulation」→「PowerTerm Terminal Emulation」)を使用します。

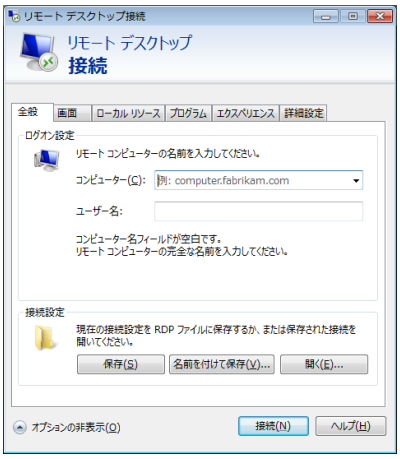


重要

Ericom 社 PowerTerm® Terminal Emulation はサポート対象外となります。実運用環境への導入に関しては、運用環境に基づいた設定で十分な事前検証を行い、システムインテグレーション上問題ないことを確認してから使用してください。

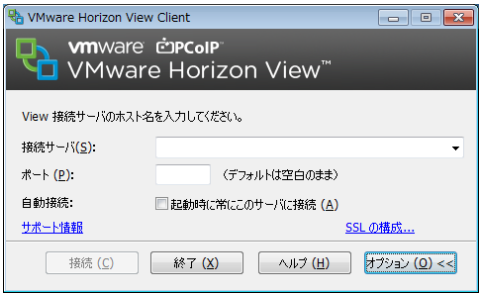
5. リモートデスクトップ接続の確立

リモートアプリケーションへ接続し管理するには、「リモートデスクトップ接続」ダイアログボックスを使用します(「スタート」→「すべてのプログラム」→「Remote Desktop Connection」→「Remote Desktop Connection」をクリック、またはデスクトップの「Remote Desktop Connection」アイコンをダブルクリック)。シングルモニター表示には標準バージョン(デフォルト)を使用します。1 つのセッションを 2 つのモニターに拡張するとき(デュアルモニター対応シンクライアントの場合)は、Span バージョンを使用できます。FBWF キャッシュがフルになりつつある場合は、「エクスペリエンス」タブでビットマップのキャッシュを無効にできます。リモートデスクトップ接続の使用方法については、Microsoft 社のマニュアルを参照してください (http://www.microsoft.com)。



6. VMware Horizon View Client による仮想デスクトップへの接続

「VMware Horizon View Client」ダイアログボックスを使用して、仮想デスクトップに接続するよう設定できます。「VMware Horizon View Client」ダイアログボックスは「スタート」→「すべてのプログラム」→「VMware」→「VMware Horizon View Client」により表示します。



6. 「接続サーバ」ドロップダウンリストで View Connection Server のホスト名または IP アドレスを入力、必要なオプションの設定をして、「接続」をクリックします。

7. 使用権限のあるユーザーの名前およびパスワードを入力し、「Login」をクリックします。

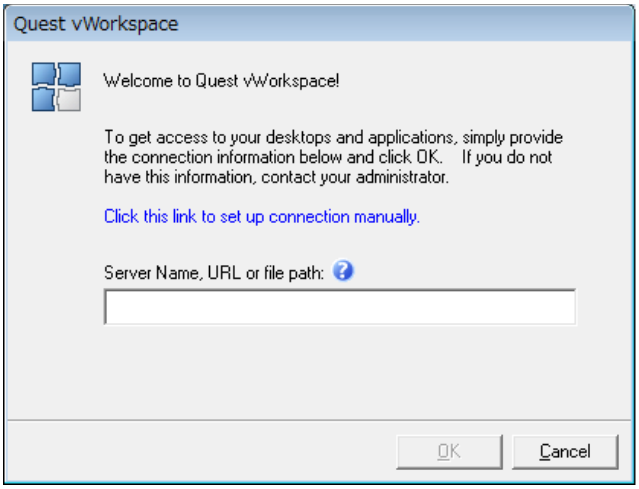
8. 表示されるリストからデスクトップを選択し、「接続」をクリックします。VMware Horizon View Client が指定されたデスクトップへの接続を試みます。接続後、クライアントウィンドウが表示されます。

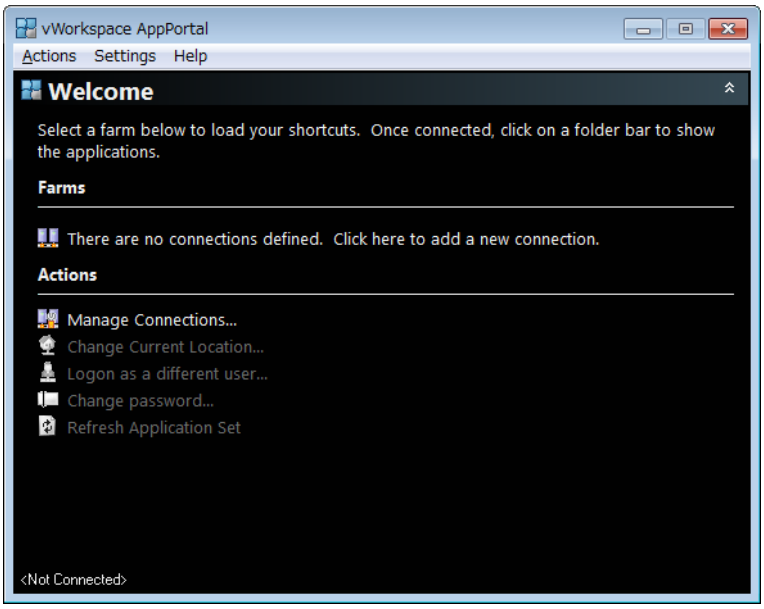
VMware Horizon View Client の使用方法については、VMware の Web サイトを参照してください (http://www.vmware.com)。

7. Quest vWorkspace による仮想デスクトップへの接続

「Quest vWorkspace」ダイアログボックスを使用して、仮想デスクトップに接続するよう設定できます。

「Quest vWorkspace」ダイアログボックスは「スタート」→「すべてのプログラム」→「Quest Software」→「vWorkspace Connector for Windows」→「AppPortal」(またはデスクトップの「AppPortal」アイコンをダブルクリック)により表示します。





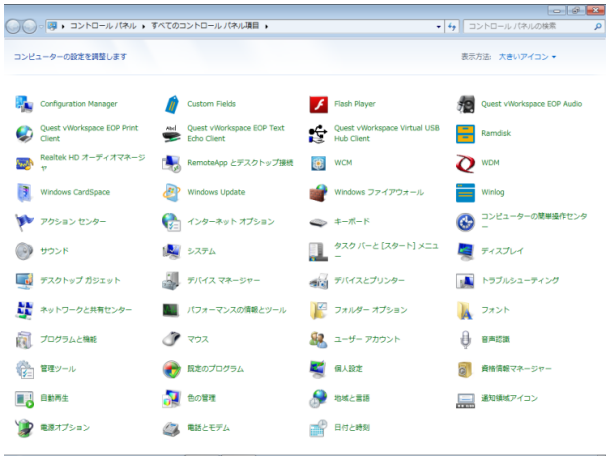
重要

Quest vWorkspace はサポート対象外となります。実運用環境への導入に関しては、運用環境に基づいた設定で十分な事前検証を行い、システムインテグレーション上問題ないことを確認してから使用してください。

NEC Express5800 シリーズ
US300d

4 便利な管理者機能

この章では、「コントロールパネル」メニュー(「スタート」→「コントロールパネル」)にある以下の管理者向けの機能の概要について説明します。



1. 管理ツールへのアクセスと管理ツールの使用
2. Custom Fieldsによる設定文字列の設定
3. デバイスとプリンターの設定
4. デュアルモニター表示の設定
5. RAMディスクサイズの設定
6. Realtek HD オーディオマネージャの使用方法
7. 地域と言語のオプションの選択
8. サウンドとオーディオデバイスの管理
9. ユーザーアカウントの管理
10. WCM Clientの使用方法
11. WDMプロパティの設定
12. Winlogによる自動ログオンの有効化／無効化
13. 無線ローカルエリアネットワーク(LAN)の設定
14. ワイヤレス接続の保存
15. Microsoft System Center Configuration Manager
16. Quest vWorkspace
17. 証明書の保存
18. USBストレージデバイスへのアクセス制御

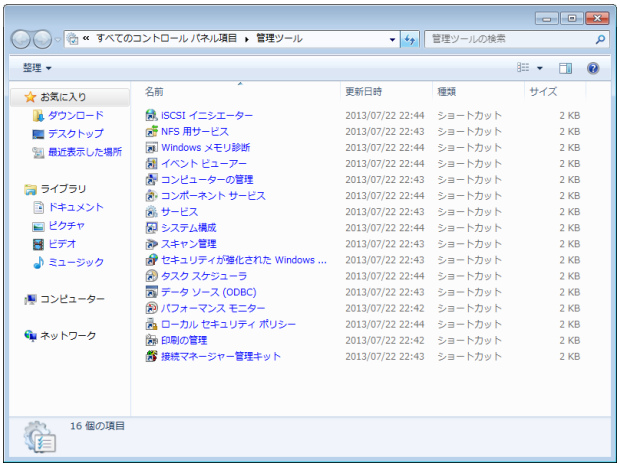
ヒント

デュアルモニターの表示設定など、一部の機能を設定する許可をユーザーに与えることはできますが、File Based Write Filter を使用してシンクライアントの設定を変更しリブート後も維持するよう設定できるのは、管理者のみです。

1. 管理ツールへのアクセスと管理ツールの使用

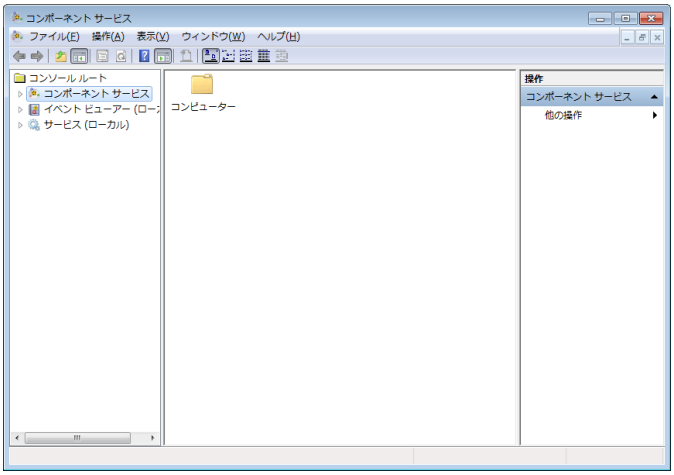
コントロールパネルの「管理ツール」アイコンをダブルクリックすると、「管理ツール」ウィンドウが表示されます。ここから以下の管理ツールにアクセスできます。

- 「コンポーネントサービスの設定」
- 「イベントの表示」
- 「サービスの管理」



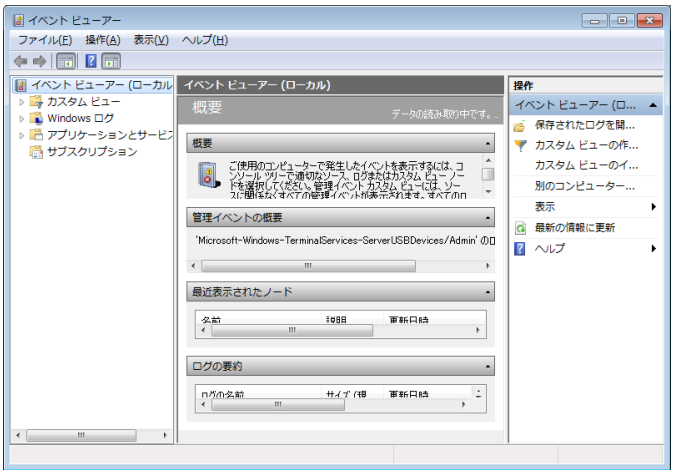
1.1 コンポーネントサービスの設定

「コンポーネントサービス」アイコンをダブルクリックすると、「コンポーネントサービス」ウィンドウが表示されます。コンソールでは、「コンポーネントサービス」、「イベントビューアー」、「ローカルサービス」の各項目を設定することができます。



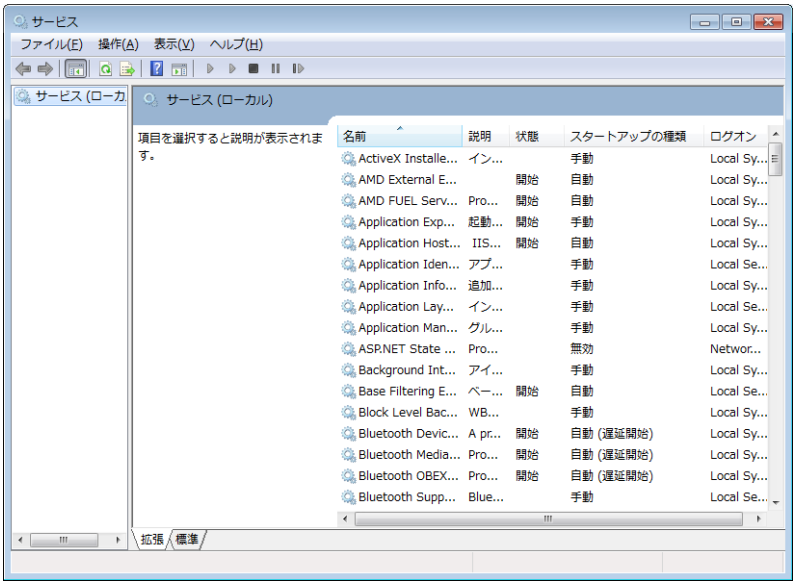
1.2 イベントの表示

「イベントビューアー」アイコンをダブルクリックすると、「イベントビューアー」ウィンドウが表示されます。このツールは、Windows や他のプログラムからの監視およびトラブルシューティングメッセージを表示します。



1.3 サービスの管理

「サービス」アイコンをダブルクリックすると、「サービス」ウィンドウが表示されます。このウィンドウには、シンクライアントにインストールされているサービスが一覧表示されます。TightVNC Server と Client Cleanup (NetXClean)は、シンクライアント管理者がタスクマネージャーにより停止、または再起動する必要がある場合があります。これらのサービスについては、「5 章(4. NetXClean ユーティリティーについて)」と「6 章(6.1 TightVNC サーバーのプロパティの設定)」を参照してください。



2. Custom Fields による設定文字列の設定

コントロールパネルの「Custom Fields」アイコンをダブルクリックすると、「Custom Fields」ダイアログボックスが表示されます。このダイアログボックスは、Wyse Device Manager (WDM)ソフトウェアが使用する設定文字列を入力するために使用します。文字列には、場所、ユーザー、管理者などの情報を設定することができます。

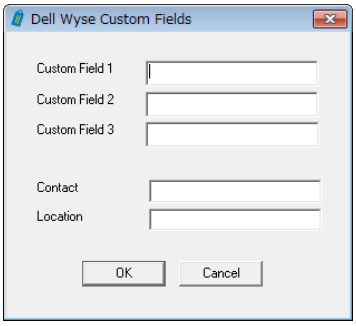
「OK」をクリックすると、ダイアログボックスで入力したカスタムフィールド情報が Windows レジストリに転送されます。これにより、Wyse Device Manager でこの情報を使用できるようになります。

重要

設定の変更を再起動後も保時するには、FBWF を無効にする必要があります。詳細な手順については「2 章(3.シンクライアントを設定する前に)」を参照してください。

WDM を使用したリモート管理およびシンクライアントソフトウェアのアップグレードについては、「6 章(4. Wyse Device Manager ソフトウェアによるリモート管理)」を参照してください。

カスタムフィールド情報の使用方法については、WDM のマニュアルを参照してください。



3. デバイスとプリンターの設定

デバイス(「4 章(3.1 デバイスの追加)」を参照)およびプリンター(「4 章(3.2 プリンターの追加)」を参照)を追加するには、「デバイスとプリンター」ウィンドウを使用します。

重要

設定の変更を再起動後も保時するには、FBWF を無効にする必要があります。詳細な手順については「2 章(3.シンクライアントを設定する前に)」を参照してください。また、デバイスまたはプリンターの設定を消去しないように NetXClean を設定してください。

3.1 デバイスの追加

デバイスをシンクライアントに追加するには、「デバイスの追加」ウィザードを実行します。

1. コントロールパネルで「デバイスとプリンター」アイコンをクリックし、「デバイスとプリンター」ウィンドウを開きます。

2. 「デバイスの追加」をクリックして「デバイスの追加」ウィザードを開きます。

3.2 プリンターの追加

プリンターをシンクライアントに追加するには、「プリンターの追加」ウィザードを実行します。

1. コントロールパネルで「デバイスとプリンター」アイコンをクリックし、「デバイスとプリンター」ウィンドウを開きます。

2. 「プリンターの追加」をクリックして「プリンターの追加」ウィザードを開きます。

   シンクライアントには、ローカル接続プリンターへのテキストのみの印刷をサポートするための汎用プリンタードライバーがインストールされています。ローカル接続プリンターにフルテキストおよび

グラフィックを出力するには、メーカーから提供されているドライバーを手順に従ってインストールします。

ICA または RDP アプリケーションからのネットワークプリンターへの出力は、サーバー上のプリンタードライバーを使用して実行できます。

サーバーのプリンタードライバーを使用して ICA または RDP セッションからローカル接続プリンターに出力すると、このプリンターでのフルテキストおよびグラフィック機能が利用可能になります。この操作を実行するには、「プリンターの追加」の手順に従って、プリンタードライバーをサーバーに、テキスト専用ドライバーをシンクライアントにインストールします。

3. プリンターをシンクライアントに接続します。

4. コントロールパネルで「デバイスとプリンター」アイコンをクリックし、「デバイスとプリンター」ウィンドウを開きます。

5. 「プリンターの追加」をクリックして「プリンターの追加」ウィザードを開き、「次へ」をクリックします。

6. 「ローカルプリンターを追加します」を選択します。

7. 「次のポートを使用」を選択し、リストからポートを選択し、「次へ」をクリックします。

8. プリンターのメーカーと機種を選択して「次へ」をクリックします。

9. プリンターの名前を入力して「次へ」をクリックします。

10. 「このプリンターを共有しない」を選択して「次へ」をクリックします。

11. テストページを印刷するかどうかを選択して「次へ」をクリックします。

12. 「完了」をクリックします。インストールが完了し、テストページ印刷オプションを選択した場合は、テストページが印刷されます。

4. デュアルモニター表示の設定

「画面の解像度」ウィンドウを使用して、デュアルモニターの設定を行うことができます。「画面の解像度」ウィンドウを表示するには、コントロールパネルの「ディスプレイ」アイコンをクリックし、「ディスプレイ表示の変更」リンクをクリックします(http://www.microsoft.com にある Microsoft 社のマニュアルを参照してください)。

なお、3 画面出力はできません。

重要

純正オプション以外のモニタについてはサポート対象外です。実運用環境への導入に関しては、運用環境に基づいた設定で十分な事前検証を行い、問題ないことを確認してから使用してください。

ヒント

本製品ではリモートデスクトップセッションでスパンモード表示するためのショートカットがスタートメニューに用意されています(「スタート」→「すべてのプログラム」→「Remote Desktop Connection」→「Span Remote Desktop Connection」)。スパンモードはモニタースパニングにより、1 つのリモートデスクトップセッションを複数のモニターにまたがって表示します。ただし、以下の要件を満たしている必要があります。

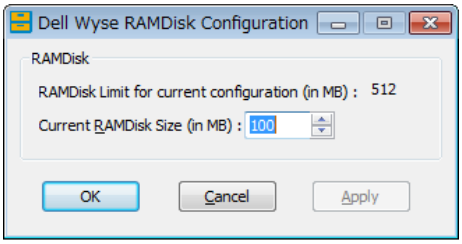
・リモートデスクトップ接続オプションの「画面」タブ→「リモートセッションですべてのモニターを使用する(U)」を無効にします。有効にした場合は、スパンモードではなくマルチモニター表示されます。
・すべてのモニターの解像度が同じであること。たとえば、2 台のモニタの解像度が両方とも 1024x768 である場合は連結表示できますが、1 台が 1024x768 でもう 1 台が 800x600 の場合は連結表示できません。
・すべてのモニタが水平 (横) に配置されていること。
・すべてのモニタの解像度の合計が 4096x2048 以下であること。

5. RAM ディスクサイズの設定

RAM ディスクは、一時的なデータ保存に使用される揮発性記憶空間です。「マイコンピュータ」ウィンドウでは、Z ドライブと表示されます。RAM ディスクは、管理者の判断により、他のデータの一時保存にも使用できます(「ファイルの保存とローカルドライブの使用方法」を参照してください)。
RAM ディスクには以下のものが保存されます。

- ブラウザーの Web ページのキャッシュ
- ブラウザーの履歴
- ブラウザーの Cookie
- ブラウザーのキャッシュ
- テンポラリインターネットファイル
- 印刷スプーリング
- ユーザーとシステムのテンポラリファイル

コントロールパネルの「Ramdisk」アイコンをダブルクリックすると、「Dell Wyse RAMDisk Configuration」ダイアログボックスが表示されます。このダイアログボックスを使用して、RAM ディスクのサイズを設定します。RAM ディスクのサイズを変更すると、システムを再起動して変更を有効にするように求められます。ただし、設定の変更を再起動後も保時するには、FBWF を無効にする必要があります。詳細な手順については「2 章(3.シンクライアントを設定する前に)」を参照してください。

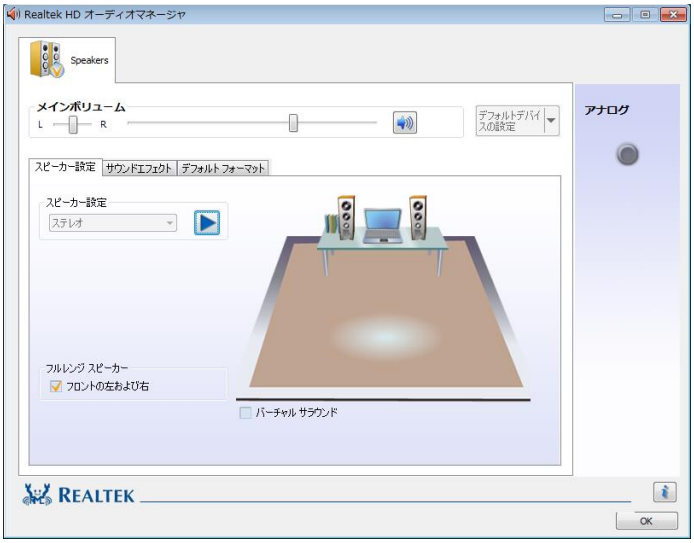


ヒント

デフォルトの RAM ディスクサイズは 100 MB、設定可能な最小 RAM ディスクサイズは 2 MB です。設定可能な最大 RAM ディスクサイズは、RAM が 512 MB を超えるシステムでは実際の RAM の約 10%です。
※「Dell Wyse RAMDisk Configuration」ツールのディスクサイズの設定上限は 512 MB ですが、RAM が 2 GB の本システムでは、RAM ディスクサイズは 200 MB(2 GB の約 10%)までを設定することを推奨します。

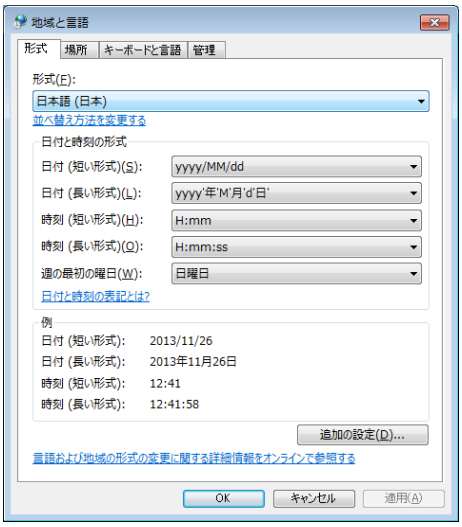
6. Realtek HD オーディオマネージャの使用方法

音声および音声デバイスを管理するには、「Realtek HD オーディオマネージャ」ダイアログボックス(「コントロールパネル」→「Realtek HD オーディオマネージャ」アイコン)を使用します。タスクバーのシステムトレイ内にある「音量」アイコンを使用して音量を調節することもできます。「音量」アイコンをクリックすると、マスター音量コントロールが開きます。電源付きスピーカーの使用をお勧めします。



7. 地域と言語のオプションの選択

コントロールパネルの「地域と言語のオプション」アイコンをダブルクリックすると、「地域と言語のオプション」ダイアログボックスが表示されます。このダイアログボックスを使用して、キーボードの言語を選択します。



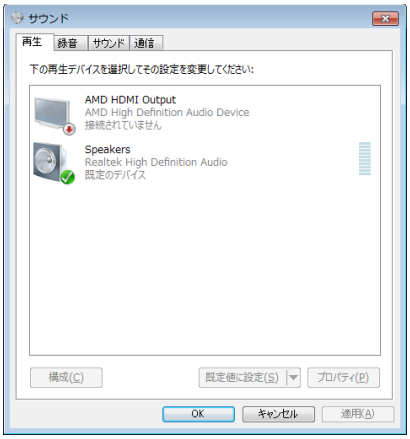
チェック

サポートされているキーボード言語は日本語と英語(米国)のみです。その他の言語は十分な事前検証を行い、システムインテグレーション上問題ないことを確認してから使用してください。

サードパーティ製ソフトウェア、Wyse アプリケーション、およびマイクロソフト社の名称は、インターフェース言語の変更後も英語で表示されます。シンクライアントに多言語ビルドが含まれており、別の言語に変更したい場合は、言語を変更した後に必ずシンクライアントを再起動してください。

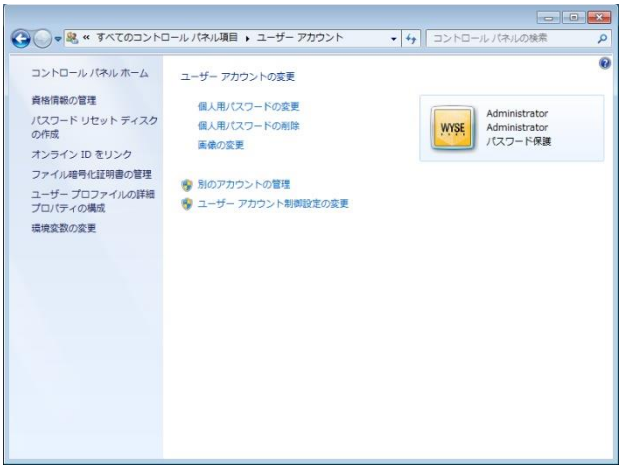
8. サウンドとオーディオデバイスの管理

コントロールパネルの「サウンド」アイコンをダブルクリックすると、「サウンド」ダイアログボックスが表示されます。このダイアログボックスを使用して、音声およびオーディオデバイスを管理します。タスクバーのシステムトレイ内にある「音量」アイコンを使用して音量を調節することもできます。「音量」アイコンをクリックすると、マスター音量コントロールが開きます。アクティブスピーカーを推奨します。



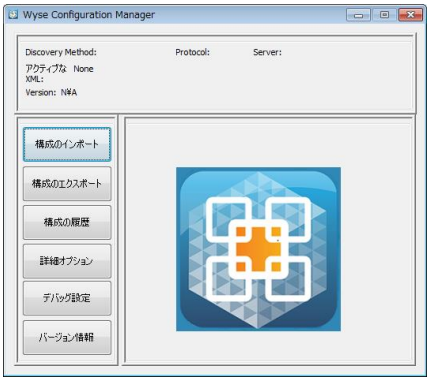
9. ユーザーアカウントの管理

コントロールパネルの「ユーザーアカウント」アイコンをダブルクリックすると、「ユーザーアカウント」ウィンドウが表示されます。このツールを使用して、ユーザーとグループを管理できます。ユーザーアカウントウィンドウについては、「5 章(10. 「ユーザーアカウント」ウィンドウによるユーザーとグループの管理)」を参照してください。



10. WCM Client の使用方法

WCM アプリケーションで作成した構成ファイルをシンクライアントに適用するには、WCM Client (「コントロールパネル」→「WCM」アイコン)を使用します。



Wyse Configuration Manager™ は、構成ファイルを作成してシンクライアントに適用する簡単なソリューションを提供しています。Wyse Configuration Manager については、
http://www.wyse.com/products/software/management を参照してください。

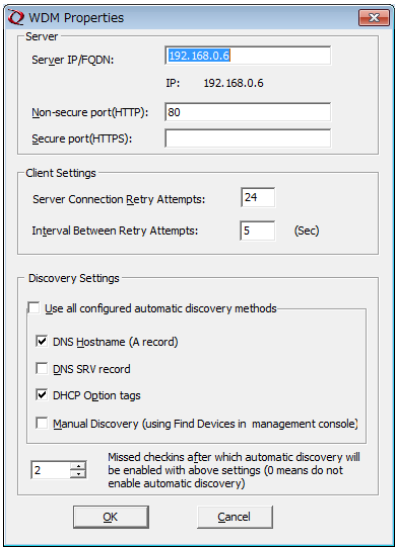
重要

Wyse Configuraion Manager™ はサポート対象外となります。実運用環境への導入に関しては、運用環境に基づいた設定で十分な事前検証を行い、システムインテグレーション上問題ないことを確認してから使用してください。
また、Wyse Configuration Manager™ はデフォルトの設定でサービスがスタートアップで自動起動します。使用されない場合は、FBWF を無効の状態で以下の設定を保存することで、無効にすることも可能です。FBWF については、「5 章 (3. File Based Write Filter (FBWF) の使用方法)」を参照してください。

1. **「コントロールパネル」→「管理ツール」→「サービス」を起動します。**
2. **「WCMservice」を選択し、右クリックメニューから「プロパティ」を開きます。**
3. **「全般」タブの「スタートアップの種類」を無効に設定し、「適用」ボタンをクリックします。**

11. WDM プロパティの設定

コントロールパネルの「WDM」アイコンをダブルクリックすると、「WDM Properties」ダイアログボックスが表示されます。このダイアログボックスを使用して、WDM の設定を行います。



1. 以下のようサーバーの設定を行います。
   - 「Server IP/FQDN」欄にＷＤＭサーバーの IP アドレスまたはホスト名を入力します。
   - 「Non secure port (HTTP)」欄に使用するポートの番号を入力します (デフォルトは 80)。
   - HTTPS を使用する場合は、「Secure Port (HTTPS)」欄に使用するポート番号を入力します (デフォルトは 443)。(任意))

2. 以下のようにクライアントの設定を行います。
   - 「Server Connection Retry Attempts」欄に、接続失敗後に WDM サーバーへの接続を試みる回数を入力します。
   - 「Interval Between Retry Attempts」欄に、接続失敗後に WDM サーバーへの接続を試みる間隔(秒単位)を入力します。

3. 以下のように WDM サーバーの検出方法の設定を行います。
   - 「Use all configured automatic discovery methods」を設定すると、「Discovery Settings」の全ての検出オプションが有効になります。
   - 「DNS Hostname (A record)」を有効にすると、DNS ホスト名を参照し、WDM サーバーを検出します。
   - 「DNS SRV record」を有効にすると、DNS SRV レコードを参照し、WDM サーバーを検出します。
   - 「DHCP Option tags」を有効にすると、DHCP オプションタグを参照し、ＷＤＭサーバーを検出します。

- 「Manual Discovery (using Find Devices in management console)」を有効にすると、WDM 管理コンソールから手動で検出できます。

WDM サーバー上の「Find Devices」の IP Range および Subnet による Discovery 機能はセキュリティ向上のため削除されました。現時点では WDM 上の「Find Devices」がサポートされていないため、「Manual Discovery」機能を有効にしても動作しません。

- 「Missed checkins after which aoutomatic discovery will be enabled with above settings (O means do not enable automatic discovery)」は自動検出オプション (Discovery Settings) が有効になるまでのチェックイン試行回数を設定します。

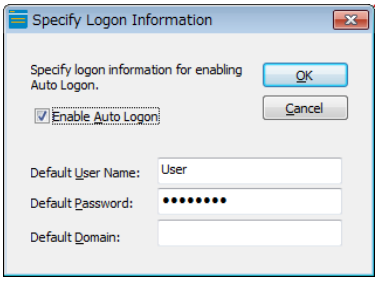
WDM ソフトウェアについては、「6 章 (4. Wyse Device Manager ソフトウェアによるリモート管理)」を参照してください。

12. Winlog による自動ログオンの有効化／無効化

シンクライアントのデフォルトでは、ユーザーデスクトップへの自動ログオンが有効になっています。コントロールパネルの「Winlog」アイコンをダブルクリックすると、「Winlog」ダイアログボックスが表示されます。このダイアログを使用して、自動ログオンを有効または無効にし、シンクライアントに自動ログオンするユーザー名、パスワード、およびドメインを変更します。

重要

設定の変更を再起動後も保時するには、FBWF を無効にする必要があります。詳細な手順については「2 章(3.シンクライアントを設定する前に)」を参照してください。



13. 無線ローカルエリアネットワーク(LAN)の設定

US300d 無線 LAN モデルでは、コントロールパネルの「ネットワークと共有センター」アイコンをクリックして、以下の操作を実行することができます。

ワイヤレスネットワークの管理(「ワイヤレスネットワークの管理」のリンクをクリック)。

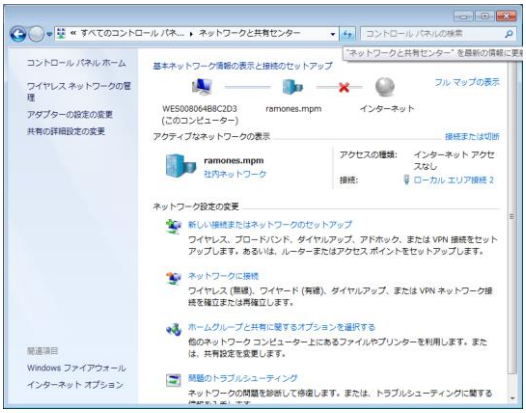
- **追加**
  「追加」をクリックしてウィザードを開き、ワイヤレスネットワークを追加します。既存のワイヤレスネットワークを編集するには、そのワイヤレスネットワークを右クリックして「プロパティ」を選択し、「ネットワークのプロパティ」ダイアログボックスを開きます。
- **アダプターのプロパティ**
  ワイヤレスアダプターの場合は、「アダプターのプロパティ」をクリックし、プロパティダイアログボックスを開きます。
- **プロファイルの種類**
  ユーザーごとのプロファイル作成機能を有効または無効にするには、「プロファイルの種類」をクリックし、ダイアログボックスを開きます。
- **ネットワークと共有センター**
  ネットワーク設定を行い、ネットワーク設定にアクセスできる「ネットワークと共有センター」ダイアログボックスに戻るには、「ネットワークと共有センター」をクリックします。

アダプターの設定の変更(「アダプターの設定の変更」リンクをクリックします。)

- ネットワーク接続の整理に使用できるオプションの一覧を開くには、「整理」をクリックします。
- 接続のステータス表示、接続、有効化、無効化、診断、名前の変更、および設定の変更に使用できるコマンドボタンの一覧を表示するには、任意の接続を選択します。

共有の詳細設定の変更(「共有の詳細設定の変更」リンクをクリックします。)

各ネットワークに使用するネットワークプロファイル設定を選択します。



リブート後も設定が維持されるように Regpersistence Tool でワイヤレス接続の設定を保存するには、「ワイヤレス接続の保存」を参照してください。

14. ワイヤレス接続の保存

Windows Embedded Standard 7 では、FBWF Enable モードでワイヤレスアクセス設定を保持するためには、レジストリフィルターを使用します。このユーティリティーを使用してワイヤレスアクセスを設定すると、リブートしても認証情報が維持されるので、シンクライアントを再起動する度に再認証する必要がなくなります。このユーティリティーは、ワークグループモード間およびドメイン間のワイヤレス接続用のサービスセット ID (SSID)を保存します。シンクライアントは、再起動時に目的の無線アクセスポイントに自動的に接続されます。

Windows Embedded Standard クライアントは、以下のネットワーク認証モードを使用してワイヤレスネットワークに接続できます。

- WEP を使用するオープンモードこの認証モードでは、シンクライアントがワイヤレスネットワークに接続している間にネットワークキーを入力する必要があります。シンクライアントは、リブート後、ワイヤレスネットワークに自動的に接続されます。
- WEP を使用する共有モード
- AES および TKIP を使用する WPA 認証
- AES および TKIP データ暗号化を使用する WPA-PSK
- AES および TKIP を使用する WPA2 認証
- AES および TKIP データ暗号化を使用する WPA2-PSK
- PEAP 認証プロセス

PEAP 認証プロセス中に生成されるセッション鍵は、ワイヤレスクライアントとワイヤレスアクセスポイント間で送受信されるデータを暗号化する WEP(Wired Equivalent Privacy)暗号鍵の鍵材料を提供します。

PEAP は、以下のワイヤレス認証方法のいずれとも使用できます(EAP-MD5 との使用はサポートされていません)。

- サーバーの認証に証明書を、ユーザーおよびクライアントコンピューターの認証に証明書またはスマートカードを使用する EAP-TLS
- サーバーの認証に証明書を、ユーザーの認証に認証情報を使用する EAP-MS-CHAP v2
- Microsoft 以外の EAP 認証方法

14.1 PEAP 高速再接続の使用

シンクライアントが 802.11 ワイヤレスネットワークに接続するときには、認証済みセッションの期間を限定するためにネットワーク管理者が有効期限の間隔を認証済みセッションに設定します。認証済みのシンクライアントがセッションを定期的に再認証して再開する必要がないように、高速再接続オプションを有効にすることができます。

各ワイヤレスアクセスポイントが同じ IAS (RADIUS)サーバーのクライアントとして設定されている場合のみ、PEAP による高速再接続が可能です。高速再接続は、ワイヤレスクライアントと RADIUS サーバーの両方で有効にする必要があります。

PEAP 高速再接続が有効になると、最初の PEAP 認証に成功した後、クライアントおよびサーバーは TLS セッション鍵をキャッシュに保存します。ユーザーが新しいワイヤレスアクセスポイントに関連付けられると、クライアントおよびサーバーは、キャッシュの有効期限が切れるまで、キャッシュに保存した鍵を使用して互いに再認証します。鍵はキャッシュに保存されるので、RADIUS サーバーは、クライアント接続が再接続であることをすばやく判断できます。このため、クライアントによる認証要求と RADIUS サーバーによる応答間の遅延を短縮できます。クライアントおよびサーバーに対するリソース要件も軽減されます。

セッション鍵をキャッシュに保存した RADIUS サーバーを使用しない場合は、完全な認証が必要で、認証情報または PIN が再度求められます。この状況になる可能性があるのは、以下のような場合です。

- 別の RADIUS サーバーのクライアントとして設定されている新しいワイヤレスアクセスポイントにユーザーを関連付ける場合
- ユーザーを関連付けるワイヤレスアクセスポイントは同じだが、ワイヤレスアクセスポイントが別の RADIUS サーバーに認証要求を転送する場合

どちらの状況でも、新しい RADIUS サーバーとの最初の認証に成功した後、クライアントは新しい TLS セッション鍵をキャッシュに保存します。クライアントは、複数の RADIUS サーバーの TLS セッション鍵をキャッシュに保存できます。

14.2 レジストリフィルターを使用したワイヤレス接続の設定

1. Administrator アカウントでログオンします。

2. FBWF を無効にします。

3. 自動再起動後、Administrator でログオンします。

4. 「コントロールパネル」→「フォルダーオプション」を起動します。

5. 「表示」タブの「隠しファイル、隠しフォルダー、および隠しドライブを表示する」をチェックし、「OK」ボタンをクリックします。

6. 下記フォルダーが存在するか確認します。存在しない場合は「Wlansvc」以下のフォルダーを新規に作成します。

   C:¥ProgramData¥Microsoft¥Wlansvc¥Profiles¥Interfaces

7. 「スタート」→「ファイル名を指定して実行」をクリックし、名前」テキストボックスに「regedit」と入力し、「OK」をクリックします。

8. HKLM¥System¥CurrentControlSet¥Services¥RegFilter¥Parameters¥MonitoredKeys の下に新しいキーを作成します。本手順では「4」のキーを作成します。もし、MonitoredKeys の下に「7」のキーを持っている場合は、新しいキー「8」を作成します(1 インクリメントした値を設定します)。

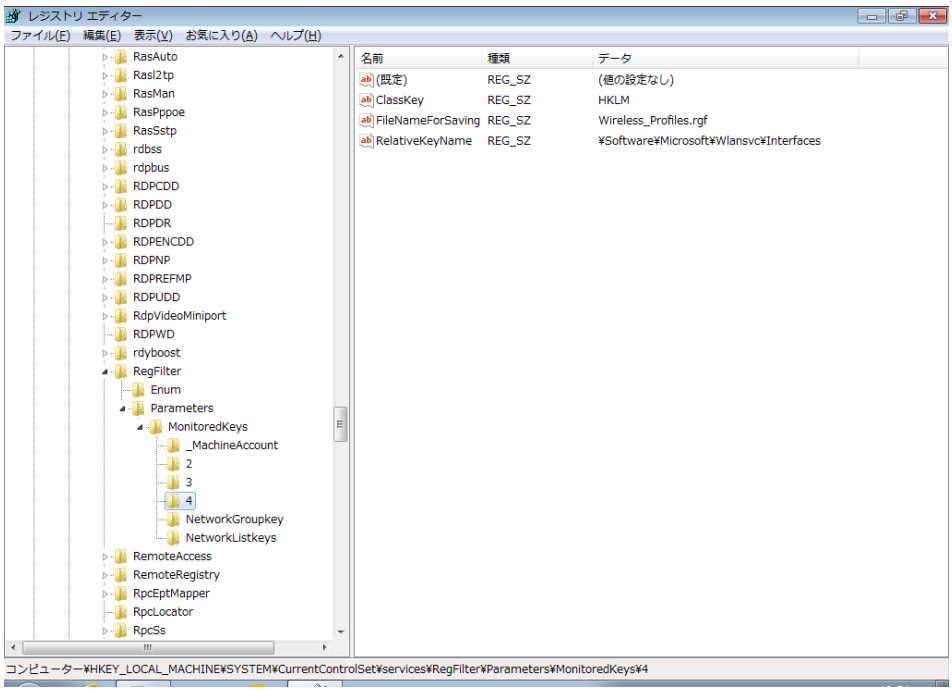
9. 前手順で作成したキーの下に下記キーを新しく作成します。

   HKLM¥System¥CurrentControlSet¥Services¥RegFilter¥Parameters¥MonitoredKeys¥4

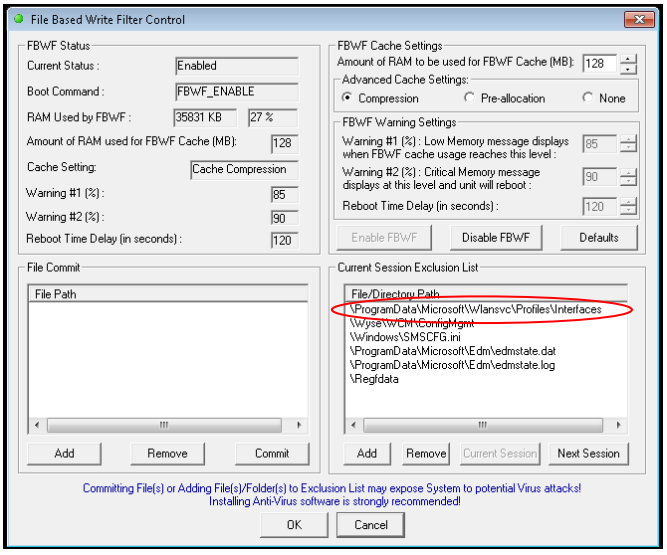
   種類 = REG-SZ
   キー名 = ClassKey
   値 = HKLM

   種類 = REG-SZ
   キー名 = FileNameForSaving
   値 = Wireless_Profiles.rgf

   種類 = REG-SZ
   キー名 = RelativeKeyName
   値 = ¥Software¥Microsoft¥Wlansvc¥Interfaces



10. FBWF を有効にします。
11. Administrator でログオンします。
12. システムトレイの FBWF アイコンを右クリックし、メニューから「Cofigure FBWF」をクリックします。
13. 「File Based Write Filter Control」ダイアログボックス「Current Session Exclusion List」の「Add」ボタンをクリックします。
14. ファイルまたはフォルダー参照ダイアログで、手順 6 で作成した C:¥ProgramData¥Microsoft¥Wlansvc¥Profiles¥Interfaces を選択し、「OK」ボタンをクリックします。



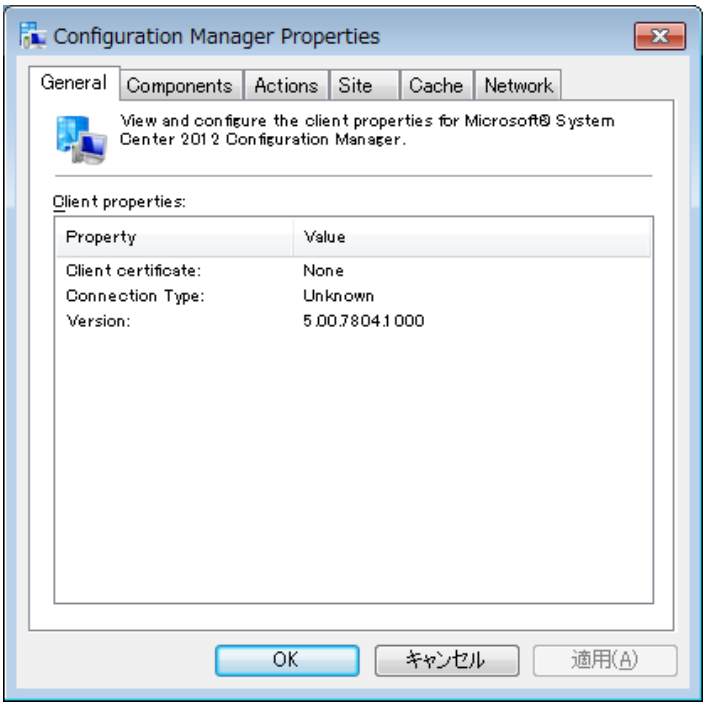
15. 再起動します。
16. User アカウントでログオンします。
17. ワイヤレスネットワークを設定し、接続を確立します。
18. 再起動します。

19. User アカウントでログオンします。
20. ワイヤレスネットワーク接続できることを確認します。

本設定によりワイヤレス接続設定は保持されますが、証明書は FBWF により再起動時に破棄されます。ワイヤレス接続で証明書認証を行う場合(EAP-PEAP、EAP-TLS)は注意が必要です。FBWF 有効時に再起動後も証明書を保持するには、「4 章(17. 証明書の保存)」を参照してください。

15. Microsoft System Center Configuration Manager

コントロールパネルの「Configuration Manager」アイコンをダブルクリックすると、「Configuration Manager Properties」ダイアログボックスが表示されます。このダイアログボックスを使用して、Configuration Manager の設定を行います。



重要

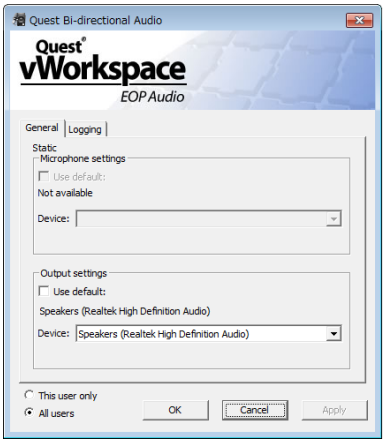
Configuration Manager はサポート対象外となります。実運用環境への導入に関しては、運用環境に基づいた設定で十分な事前検証を行い、システムインテグレーション上問題ないことを確認してから使用してください。

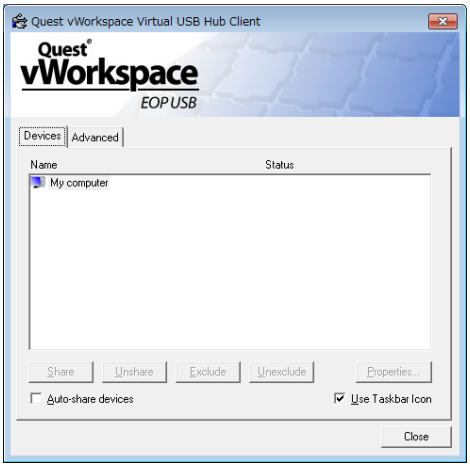
16. Quest vWorkspace

コントロールパネルから以下の Quest vWorkspace ソフトウェアを設定できます。

- Quest vWorkspace EOP Audio
- Quest vWorkspace EOP Print Client
- Quest vWorkspace EOP Text Echo Client
- Quest vWorkspace EOP USB Hub Client

各アイコンをダブルクリックすると、設定ダイアログボックスが表示されます。





重要

Quest vWorkspace はサポート対象外となります。実運用環境への導入に関しては、運用環境に基づいた設定で十分な事前検証を行い、システムインテグレーション上問題ないことを確認してから使用してください。

17. 証明書の保存

Windows Embedded Standard 7 では、FBWF(File Based Write Filter)によってフラッシュメモリへの誤った書き込みからシンクライアントを保護しています。シンクライアントがアクティブな状態である限りフラッシュへの書き込みは有効ですが、シンクライアントを再起動またはシャットダウンすると失われます。証明書の場合も、FBWF Enable モードでインストールした証明書は、シンクライアンを再起動またはシャットダウンすると失われます。無線 LAN 接続の資格認証に使用するユーザー証明書など、ユーザーが直接インストールした証明書を再起動後も使用したい場合は、FBWF Enable モードの状態で証明書を保持するようにシンクライアントを設定します。

ルート証明書は、ユーザーが直接インストール後も保持するようにカスタマイズすることはできません。必ず管理者が FBWF を無効にしてインストールする必要があります。詳細な手順については「2 章(3.シンクライアントを設定する前に)」を参照してください。

再起動後にユーザー証明書が破棄されないように FBWF の除外リストに追加する手順です。

1. Administrator アカウントでログオンします。

2. 「スタート」→「ファイル名を指定して実行」をクリックし、コマンドプロンプトを起動します。
   「名前」テキストボックスに「cmd」と入力し、「OK」をクリックします。

3. 以下の 3 つのユーザー固有のフォルダーを File Based Write Filter の除外リストに追加します。
   fbwfmgr /addexclusion c: ¥Users¥<ユーザー名>¥AppData¥Roaming¥Microsoft¥Crypto
   fbwfmgr /addexclusion c: ¥Users¥<ユーザー名>¥AppData¥Roaming¥Microsoft¥Protect
   fbwfmgr /addexclusion c: ¥Users¥<ユーザー名>¥AppData¥Roaming¥Microsoft¥SystemCertificates

4. 再起動します。再起動後に除外リストが有効になります。

既定の設定では Administrator および User アカウントは NetXClean.ini にプロファイルの削除対象外として登録されています。しかし、新規に追加したユーザーアカウントあるいはドメインユーザーアカウントの場合は、ユーザープロファイルは削除されます。ユーザープロファイルが削除されると、インストールした証明書もまた削除されるため、NetXClean.ini を使用してユーザープロファイルが削除されないように登録する必要があります。詳細な手順については「5 章(4. NetXClean ユーティリティーについて)」を参照してください。

18. USB ストレージデバイスへのアクセス制御

本製品では、USB ストレージデバイスへの読み取りと書き込みが行えるように設定されています。
USB ストレージデバイスへのアクセスを制御する場合は、下記を参照し、管理者が設定を行ってください。

1. Administrator アカウントでログオンします。

2. FBWF を無効にします。

3. 自動再起動後、Administrator でログオンします。

4. タスクバーを右クリックし、「タスクマネージャーの起動」をクリックします。

5. 「サービス」タブで「WPDBusEnum」の状態が「実行中」であることを確認します。状態が「停止」の場合は「WPDBusEnum」を右クリックし、「サービスの開始」をクリックし、状態が「実行中」となることを確認します。

- **後の手順で「リムーバブル記憶域へのアクセス」のポリシーを操作します。このポリシーを変更する際に「WPDBusEnum」サービスが停止していると、ポリシーが正しく適用されない場合があります。「WPDBusEnum」サービスは開始後 2 分程度で自動的に停止してしまうため、ポリシーを変更する前に必ずサービスの状態を確認してください。**

6. 「スタート」→「ファイル名を指定して実行」をクリックし、「名前」テキストボックスに「gpedit.msc」と入力し、「OK」をクリックします。

7. 「コンピューターの構成」→「管理用テンプレート」→「システム」→「リムーバブル記憶域へのアクセス」を選択します。

8. デバイスへのアクセスを禁止する（読み書き共に禁止する）場合は、設定を「有効」にします。
   - 読み取りアクセス権の拒否
   - 書き込みアクセスの拒否

   例) リムーバブルディスクへのアクセスを禁止する場合

設定	状態
リムーバブルディスク：読み取りアクセス権の拒否	有効
リムーバブルディスク：書き込みアクセスの拒否	有効

   読み取り専用とする（書き込みのみ禁止する）場合は、下記の設定を「有効」にします。
   - 書き込みアクセスの拒否

   例) リムーバブルディスクを書き込み禁止する場合

設定	状態
リムーバブルディスク：書き込みアクセスの拒否	有効

9. 「スタート」→「ファイル名を指定して実行」をクリックし、「名前」テキストボックスに「regedit」と入力し、「OK」をクリックします。

10. 以下の値を作成します。

キー	HKLM¥Software¥Policies¥Microsoft¥Windows¥RemovableStorageDevices
名前	ApplyPolicyOnUserLogoff
種類	REG_DWORD
値	0x00

- **このレジストリ値は、ポリシー設定後に光学ドライブがエクスプローラー等から見えなくなる問題を防ぐために設定しています。光学デバイスが見えなくなってしまった場合は、デバイスマネージャーから対象の光学ドライブを削除し、「ハードウェア変更のスキャン」を実行することで認識するようになります。**

11. 「スタート」→「ファイル名を指定して実行」をクリックし、「名前」テキストボックスに「gpupdate /force」と入力し、「OK」をクリックします。

12. 端末を再起動します。

13. Administrator アカウントでログオンします。

14. FBWF を有効にします。

- 読み込み書き込みを共に禁止した場合、デバイスは表示されますが、アクセスできません。
- Citrix 環境に USB メモリをデバイスマッピングさせた場合、フロッピーディスクドライブとして認識される場合があります。

- **USB ストレージデバイスを US300d に接続し、リモートデスクトップのデバイスマッピング機能を利用する場合、書き込み禁止の設定をしている場合でも USB ストレージデバイスに対してフォルダを作成できる場合があります。ファイルの作成はできません。**
- **Citrix 環境や VMWare View 環境へ接続する場合に USB リダイレクション機能を使用すると、仮想 PC 上で USB ストレージデバイスが使用可能となります。運用環境にあわせて、USB ストレージデバイスの使用を制限してください。設定方法は、各製品のガイドを参照してください。**

NEC Express5800 シリーズ
US300d

5 管理者ユーティリティーと設定に関する追加情報

この章では、管理者向けユーティリティーと設定に関する以下の情報を紹介します。

1. ユーティリティーの自動起動について
2. ログオフ、シャットダウン、および再起動の影響を受けるユーティリティー
3. File Based Write Filter (FBWF)の使用方法
4. NetXCleanユーティリティーについて
5. ファイルの保存とローカルドライブの使用方法
6. ネットワークドライブのマッピング
7. ドメインへの参加
8. WinPing診断ユーティリティーの使用方法
9. NetおよびTracertユーティリティーの使用方法
10. 「ユーザーアカウント」ウィンドウによるユーザーとグループの管理
11. シンクライアントのコンピューター名の変更

TightVNC ユーティリティーについては、「6 章(6. TightVNC を使用したシンクライアントのリモートシャドー)」を参照してください。

1. ユーティリティーの自動起動について

以下のユーティリティーは自動的に起動します。

- **File Based Write Filter**

  FBWF ユーティリティーは、システム起動時に自動的に起動されます。このユーティリティーは、フラッシュメモリへの誤った書き込みからシンクライアントを保護することにより、シンクライアントでのコンピューター処理にセキュアな環境を提供します。タスクバーのシステムトレイ内にある「File Based Writer Filter」アイコンの色によって、フィルターの有効(緑)／無効(赤)状態が示されます。FBWF については、「5 章(3. File Based Write Filter (FBWF)の使用方法)」を参照してください。

- **NetXClean**

  NetXClean ユーティリティーは、システム起動時に自動的に起動されます。NetXClean は、不要な情報をローカルディスクに格納しないようにするクリーンアップユーティリティーです。特定のプロファイル設定(プリンターなど)を維持したい場合は、必ず明示的に宣言したプロファイルを消去しないように NetXClean を設定してください。NetXClean については、「5 章(4. NetXClean ユーティリティーについて)」を参照してください。

- **VNC Server**

  Windows の VNC Server ユーティリティーは、シンクライアントに正常にログオンすると、自動的に起動されます。VNC は、管理およびサポート目的でシンクライアントデスクトップにリモートアクセスできるようにするユーティリティーです。VNC については、「6 章(6. TightVNC を使用したシンクライアントのリモートシャドー)」を参照してください。

2. ログオフ、シャットダウン、および再起動の影響を受けるユーティリティー

以下のユーティリティーは、シンクライアントのログオフ、再起動、シャットダウン時に影響を受けます。

- **File Based Write Filter キャッシュ**

  設定の変更を再起動後も保時するには、FBWF を無効にする必要があります。詳細な手順については「2 章(3.シンクライアントを設定する前に)」を参照してください。

  FBWF を無効にしないと、変更した設定はシンクライアントのシャットダウンまたは再起動時に失われます。FBWF キャッシュの内容は、単にログオフして同じまたは別のユーザーとして再度ログオンしただけでは失われません。

  FBWF を有効のまま FBWF キャッシュを書き込むには管理者による FBWF コマンドラインオプションの実行や、「File Based Write Filter Control」ダイアログボックスを使用する方法があります。詳細な手順については「5 章(3. File Based Write Filter (FBWF)の使用方法)」を参照してください。

  ユーザーは、FBWF の無効化および FBWF コマンドラインオプションの実行や、「File Based Write Filter Control」ダイアログボックスを使用できません。この操作は、ローカルおよびリモートの管理者機能です。

- **NetXClean ユーティリティー**

  NetXClean は、不要な情報をフラッシュメモリに格納しないようにするクリーンアップユーティリティーです。クリーンアップは、再起動、シャットダウン、またはユーザーによるログオフ時に自動的に実行されます。特定のプロファイル設定(プリンターなど)を維持したい場合は、必ず明示的に宣言したプロファイルを消去しないように NetXClean を設定してください。NetXClean については、「2 章(3. シンクライアントを設定する前に)」および「5 章(4. NetXClean ユーティリティーについて)」を参照してください。

- **電源管理**

  電源管理は、モニターへの映像信号を切り、指定したアイドル時間の経過後にモニターを節電モードにすることができます。設定は、「スタート」→「コントロール パネル」→「電源オプション」で行うことができます。

- **Wake-on-LAN**

  標準的な Windows Embedded Standard 機能により、接続する LAN 上のシンクライアント端末をすべて検出し、ボタンをワンクリックするだけで wake させることができます。この機能により、Wyse Device Manager ソフトウェアは、シャットダウンされた、またはスタンバイ状態のデバイスでイメージアップデートおよびリモート管理機能を実行できます。この機能を使用するには、シンクライアントに電源供給がされている必要があります。

● **シンクライアントの日付と時刻**

「日付と時刻」でインターネット時刻サーバーと同期すると、指定時間に自動的に、または手動でタイムサーバーにシンクライアントの日付時刻を同期させることができます。
シンクライアントの日付時刻を参照する必要があるアプリケーションもありますので、正確な時刻を維持するようにしてください。必要に応じて、「日付と時刻」ダイアログボックスで日付と時刻を変更してください。「日付と時刻」ダイアログボックスは、コントロールパネルの「日付と時刻」アイコンをダブルクリックするか、タスクバーのシステムトレイの「時刻」が表示されている箇所をクリックし、「日付と時刻の変更」リンクをクリックして開くことができます。ただし、User アカウントでログオンした場合、デフォルトの設定ではアクセス制限により「日付と時刻」のダイアログボックスから日付と時刻を変更できません。User アカウントで日付と時刻を変更するには、FBWF を無効にし、以下の手順を実施します。FBWF については、「5 章(3. File Based Write Filter (FBWF)の使用方法)」を参照してください。

1. Administrator でログオンします。

2. 「スタート」→「ファイル名を指定して実行」をクリックし、グループポリシーエディターを起動します。「名前」テキストボックスに「gpedit.msc」と入力し、「OK」をクリックします。

3. 「コンピューターの構成」→「Windows の設定」→「セキュリティの設定」→「ローカルポリシー」→「ユーザー権利の割り当て」→「システム時刻の変更」をダブルクリックします。

4. 「ローカルセキュリティの設定」タブの「ユーザーまたはグループの追加(U)...」ボタンをクリックします。

5. 「ユーザーまたはグループの選択」ダイアログボックスの選択するオブジェクト名の入力ボックスに「User」と入力し、「名前の確認(C)」ボタンをクリックします。

6. 「OK」ボタンをクリックし、User アカウントが追加されたことを確認します。

7. 「OK」をクリックします。

8. 再起動し、User アカウントで日付と時刻が変更できるとこと確認します。

3. File Based Write Filter (FBWF)の使用方法

FBWF は、フラッシュメモリへの誤った書き込みからシンクライアントを保護することにより、シンクライアントでのコンピューター処理にセキュアな環境を提供します(フラッシュメモリには、オペレーティングシステムおよび機能ソフトウェアコンポーネントが格納されています)。FBWF は過度のフラッシュ書き込み動作を防止するため、シンクライアントの寿命も長くなります。FBWF は、キャッシュを使用してすべてのフラッシュ書き込みを遮断し、入出力を要求したプロセスに正常終了メッセージを返すことで、フラッシュメモリへのリード／ライトアクセスが行われているように見せます。

遮断されキャッシュに保存されたフラッシュ書き込みは、シンクライアントがアクティブな状態である限り使用できますが、シンクライアントを再起動またはシャットダウンすると失われます。選択した変更を保存するには、WDM ソフトウェアを使用するかまたは手動で、「File Based WriteFilter Control」ダイアログボックス(管理者タスクバーのシステムトレイ内に表示されている FBWF アイコンをダブルクリック)の「Commit」を使用して、キャッシュ内の選択したファイルを必要に応じてフラッシュメモリに転送します。また、変更により影響を受けるファイルが不明な場合は、「File Based Write Filter Control」ダイアログボックスで FBWF をいったん無効にした後で変更を行い、変更後、FBWF を再度有効にすることもできます(「5 章(3.4 FBWF のコントロールの設定)」を参照してください)。FBWF は、コマンドライン(fbwfmgr)を使用するか、管理者システムトレイの「File Based Write Filter」アイコンをダブルクリックして、有効または無効にすることができます。FBWF は、指定したファイルをキャッシュからフラッシュメモリにコミット(書き込み)できます(コミットしたファイルに対してさらに変更を行った場合、変更を保存する必要があるときは、これらのファイルを再度コミットする必要があります)。また、FBWF はデスクトップの「FBWF を有効/FBWF を無効」アイコンを使用することによっても、有効または無効にすることができます。FBWF の状態(有効または無効)は、システムトレイの「File Based WriteFilter」アイコンによって表示されます(緑は FBWF が有効なことを示し、赤は FBWF が無効なことを示します)。

FBWF キャッシュに 80%以上データが入っている場合は、絶対にキャッシュの内容をコミット(書き込み)しないでください。、管理者はキャッシュの状態を定期的にチェックし、FBWF キャッシュに 80%以上データが入っている場合はシンクライアントを再起動する必要があります。

ターミナルサービスクライアントアクセスライセンス(TSCAL)は、FBWF の有効／無効にかかわらず常に保持されます。

FBWF の使用については、以下のセクションを参照してください。

- 「5 章(3.1 FBWF によるパスワードの変更)」
- 「5 章(3.2 FBWF コマンドラインオプションの実行)」
- 「5 章(3.3 デスクトップアイコンによる FBWF の有効化／無効化)」
- 「5 章(3.4 FBWF のコントロールの設定)」

3.1 FBWF によるパスワードの変更

Microsoft Windows ベースのコンピューターでは、セキュリティ上、ドメインコントローラーを使用してマシンアカウントパスワードを定期的に変更します。シンクライアントがこのようなドメインのメンバーの場合は、同じパスワード処理がシンクライアントに適用されます。FBWF が有効な場合、シンクライアントはドメインコントローラーでこのパスワードを正常に変更します。ただし、FBWF が有効なため、次回シンクライアント起動時、新しいパスワードは保持されません。このような場合は、以下の選択肢があります。

- DisablePasswordChange レジストリエントリーに「1」を設定し、シンクライアントでのマシンアカウントパスワードの変更を無効にする。
- 各オペレーティングシステム用の Microsoft 社のマニュアルを参照して、Windows ベースのサーバーでのマシンアカウントパスワードの変更を無効にする。例えば、Windows 2003 Server でのマシンアカウントパスワードの変更を無効にするには、各ワークステーションではなく、ドメイン内のすべてのドメインコントローラーで RefusePasswordChange レジストリエントリーに「1」を設定する。上記設定後も、シンクライアントは 30 日ごとにパスワードを変更しようとしますが、サーバーによって拒絶されます。

Windows 2003 Server のドメインコントローラーで RefusePasswordChange レジストリエントリーに「1」を設定すると、複製トラフィックは停止しますが、シンクライアントのトラフィックは停止しません。シンクライアントで DisablePasswordChange レジストリエントリーにも「1」を設定すると、シンクライアントのトラフィックと複製トラフィックがともに停止します。

3.1.1 シンクライアントでのマシンアカウントパスワード変更の無効化

1. 「スタート」→「ファイル名を指定して実行」をクリックし、レジストリエディターを起動します。「名前」テキストボックスに「regedit」と入力し、「OK」をクリックします。

2. 以下のレジストリサブキーの場所を探し、クリックします。
   HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥Netlogon¥Parameters

3. 右のペインで、DisablePasswordChange を右クリックします。

4. 「編集」メニューで「修正」をクリックします。

5. 「値のデータ」テキストボックスに「1」を入力し、「OK」をクリックします。

6. レジストリエディターを終了します。

3.1.2 Windows 2003 Server でのマシンアカウントパスワード変更の無効化

1. 「スタート」→「ファイル名を指定して実行」をクリックし、レジストリエディターを起動します。「名前」テキストボックスに「regedit」と入力し、「OK」をクリックします。

2. 以下のレジストリサブキーの場所を探し、クリックします。
   HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥Netlogon¥Parameters

3. 「編集」メニューで「新規」をポイントし、「DWORD 値」をクリックします。

4. レジストリエントリー名として RefusePasswordChange を入力し、「Enter」をクリックします。

5. 「編集」メニューで「修正」をクリックします。

6. 「値のデータ」テキストボックスに「1」を入力し、「OK」をクリックします。

7. レジストリエディターを終了します。

3.2 FBWF コマンドラインオプションの実行

FBWF の制御に使用できるコマンドラインは複数あります(コマンドラインの引数を組み合わせることはできません)。

重要　**これらのコマンドの不正使用を防止するためにファイルセキュリティを使用してください。**

FBWF のコマンドラインオプションについては、以下のガイドラインに従ってください(「スタート」→「ファイル名を指定して実行」をクリックして、「名前」テキストボックスに「command」と入力してコマンドプロンプトウィンドウを開き、コマンドを使用することもできます)。

ヒント　コマンドプロンプトウィンドウを開いて「fbwfmgr /」と入力すると、使用可能なコマンドがすべて表示されます。コマンドの情報が知りたい場合は、fbwfmgr /help <command>を実行してください。たとえば、/addvolume の情報が知りたい場合は、「fbwfmgr /help /addvolume」と入力します。

- **fbwfmgr**
  引数なし - カレントセッションおよび次のセッションの FBWF 設定を表示します。

- **fbwfmgr /enable**
  次回システムを起動後に FBWF を有効にします。FBWF が有効な場合、「File Based Write Filter」アイコンは緑です。

- **fbwfmgr /disable**

  次回システムを起動後に FBWF を無効にします。FBWF が無効な場合、「File Based Write Filter」アイコンは赤です。

- **fbwfmgr /commit C: <file_path>**

  ファイルに加えた変更を C ドライブにコミットします。ボリューム名と file_path の間にスペースが 1 つ入っていることに注意してください。ファイルパス(file_path)には¥で始まる絶対パスを入力します。たとえば、C:¥Program Files¥temp.txt をコミットする場合、コマンドは fbwfmgr /commit C: " ¥Program Files¥temp.txt”となります。

- **fbwfmgr /restore C: <file_path>**

  ファイルに加えた変更を破棄し、C ドライブから元の内容にファイルを復元します。ファイルパス(file_path)には¥で始まる絶対パスを入力します。削除されたファイルは回復されます。

- **fbwfmgr /addexclusion C: <file_or_dir_path>**

  ボリュームの除外リストにファイルまたはディレクトリを追加します。その結果、ファイルまたはディレクトリは FBWF による保護の対象から外れます。除外は、システム再起動後に有効になります。ファイルパスまたはディレクトリパス(file_or_dir_path)には、¥で始まる絶対パスを入力します。

- **fbwfmgr /removeexclusion C: <file_or_dir_path>**

  ボリュームの除外リストからファイルまたはディレクトリを削除します。その結果、ファイルまたはディレクトリは FBWF による保護の対象になります。除外の解除は、システム再起動後に有効になります。ファイルパスまたはディレクトリパス(file_or_dir_path)には、¥で始まる絶対パスを入力します。

- **fbwfmgr /overlaydetail**

  変更されたファイルおよびディレクトリのリストを、FBWF がファイルまたはディレクトリの変更データをキャッシュに保存するために使用するメモリのサイズとそれに対するオープンハンドルの数とともに表示します。

コミットの実行中に、別のコミットを実行しないでください。

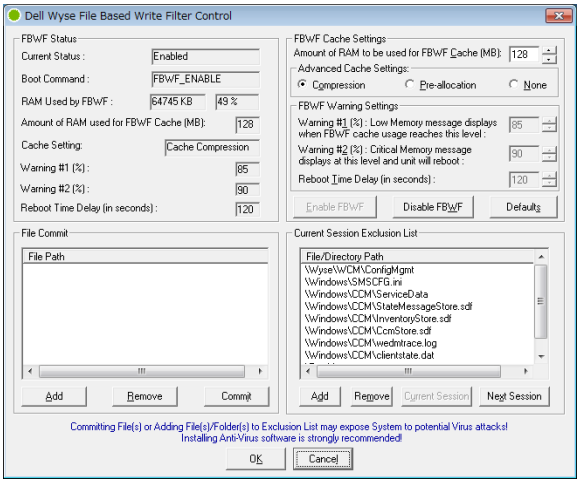
3.3 デスクトップアイコンによる FBWF の有効化／無効化

FBWF を有効または無効にするためのアイコンが管理者デスクトップにあります。

- 「FBWF を有効」アイコン(緑)ダブルクリックすると、FBWF が有効になります。このユーティリティーは、「5 章(3.2 FBWF コマンドラインオプションの実行)」で説明している fbwfmgr /enable コマンドラインオプションと同様の動作をします。ただし、このアイコンをダブルクリックすると、システムは自動で再起動され、FBWF が有効になります。FBWF が有効な場合、システムトレイの「File Based Write Filter」アイコンは緑です。
- 「FBWF を無効」アイコン(赤)ダブルクリックすると、FBWF が無効になります。このユーティリティーは、「5 章(3.2 FBWF コマンドラインオプションの実行)」で説明している fbwfmgr /disable コマンドラインオプションと同様の動作をします。ただし、このアイコンをダブルクリックすると、システムは自動で再起動され、FBWF が無効になります。FBWF は無効な状態を維持します。FBWF を有効にするには、「5 章(3.2 FBWF コマンドラインオプションの実行)」で説明しているように、「FBWF を有効」アイコンかコマンドラインを使用します。FBWF が無効な場合、システムトレイの「File Based Write Filter」アイコンは赤です。

3.4 FBWF のコントロールの設定

「File Based Write Filter Control」ダイアログボックスを使用して、現在の制御設定を表示・管理します。このダイアログボックスは、管理者タスクバーのシステムトレイ内に表示されている FBWF アイコンをダブルクリックして表示します。



以下のガイドラインに従ってください。

「FBWF Status」エリアには以下の項目があります。

- **Current Status**
  FBWF の現在の状態(有効または無効)を表示します。

- **Boot Command**
  Boot コマンドの現在の状態を表示します。(FBWF_ENABLE は、次のセッションでは FBWF が有効になることを意味します。FBWF_DISABLE は、次のセッションでは FBWF が無効になることを意味します)。

- **RAM used by FBWF**
  FBWF が現在使用している RAM のサイズを、キロバイト単位およびパーセンテージで表示します。「Current Status」が「Disabled」の場合、「RAM Used by FBWF」は常にゼロ(0)です。

- **Amount of RAM used for FBWF Cache**
  カレントセッションで FBWF キャッシュとして使用されている RAM のサイズを MB 単位で表示します。

- **Cache Setting**
  カレントセッションのキャッシュ設定を表示します。

- **Warning #1 (%)**
  カレントセッションのユーザーに、メモリ残量の減少を警告するメッセージを表示させる FBWF キャッシュのパーセント値を表示します。

- **Warning #2 (%)**
  ユーザーに、メモリ残量が限界まで枯渇していることを警告するメッセージを表示させる FBWF キャッシュのパーセント値と、同時に表示されるカレントセッションで自動リブートが行われるまでの秒数をカウントダウンするメッセージを表示します。

- **Reboot Time Delay (in seconds)**
  カレントセッションでキャッシュオーバーフロー発生により Warning #2 (%)のシステムリブートが実行されるまでの秒数を表示します。

「FBWF Cache Settings」エリアには以下の項目があります。

- **Amount of RAM to be used for FBWF Cache**
  次のセッションで FBWF キャッシュとして使用される RAM のサイズを MB 単位で表示します。この値は、16 MB～1024 MB の範囲である必要があります。この値が使用可能な RAM サイズの 35%を超えないようチェックします。

「Advanced Cache Settings」エリアには、キャッシュメモリの効率を高めるためのオプションがあります(「Compression」、「Pre-allocation」、「None」)。

「FBWF Warning Settings」エリアには以下の項目があります。

- **Warning #1 (%)**
  ユーザーにメモリ残量の減少を警告するメッセージを表示させる FBWF キャッシュのパーセント値を表示します(デフォルト値=85、最小値=50、最大値=90)。

- **Warning #2 (%)**
  ユーザーに、メモリ残量が限界まで枯渇していることを警告するメッセージを表示させる FBWF キャッシュのパーセント値と、同時に表示されるカレントセッションで自動リブートが行われるまでの秒数をカウントダウンするメッセージを表示します(デフォルト値=90、最小値=55、最大値=95)。

- **Reboot Time Delay (in seconds)**
  キャッシュオーバーフロー発生により Warning #2 (%)のシステムリブートが実行されるまでの秒数を表示します。

- **Enable FBWF**
  FBWF を有効にします。シンクライアントの再起動を求められます。シンクライアントを再起動後、変更が有効になります。システムを再起動して FBWF を有効にすると、システムトレイの「File Based Write Filter」アイコンは緑になります。

- **Disable FBWF**
  FBWF を無効にします。シンクライアントの再起動を求められます。シンクライアントを再起動後、変更が有効になります。システムを再起動して FBWF を無効にすると、システムトレイの「File Based Write Filter」アイコンは赤になります。

- **Defaults**
  「FBWF Cache Settings」エリア、「Advanced Cache Settings」エリア、および「FBWF Warning Settings」エリアをデフォルト値にリセットします。

「File Commit」エリアには以下の項目があります。

- **File Path**
  ファイルを追加、削除、および基本メディアにコミットします(ファイルをコミットしない場合は、リストからファイルパスを削除します)。シンクライアントは再起動されません。変更はただちにコミットされます。

「Current Session Exclusion List」エリアには以下の項目があります。

- **File/Directory Path**
  現在のセッション(現在のセッションでライトスルーされるファイルまたはディレクトリのリストが表示されます。タイトルは Current Session Exclusion List となります)または次のセッション(次のセッションでライトスルーされるファイルまたはディレクトリのリストを取り出します。タイトルは Next Session Exclusion List となります)で除外リストにファイルまたはディレクトリを追加するか、除外リストからファイルまたはディレクトリを削除できます。シンクライアントは自動で再起動されないため、管理者がシンクライアントを手動で再起動するまで変更は反映されません。

4. NetXClean ユーティリティーについて

NetXClean は、不要な情報がフラッシュメモリに保存されるのを防止します。NetXClean のクリーンアップは、サービスの起動またはユーザーによるログオフ時に自動的に実行されます。クリーンアップの実行はバックグラウンドで実行されるためユーザーからは見えず、またユーザーは何も入力する必要はありません。
NetXClean は、ガベージファイルの蓄積によりフラッシュメモリ内の容量が一杯になるのを防止します(たとえば、FBWF を無効な状態で運用を続けると、クリーンな状態に保つ必要があるフラッシュメモリ内のディレクトリにゴミが溜まります)。複数のユーザーがシンクライアントへのログオン権を持っている場合、ローカルに保存されるプロファイルや情報の一時キャッシュによってメモリ容量をすぐに使い果たす可能性があるので、NetXClean ユーティリティーは特に重要です。
NetXClean TweakUI 機能は以下の項目を消去します。

- 実行履歴
- 文書履歴
- ファイル検索履歴
- コンピューター検索履歴
- Internet Explorer 履歴
- 前回のユーザー
- 現在選択されている項目

NetXClean は、選択したディレクトリ、ファイル、およびプロファイルを消去します。また、設定ファイルに基づき、消去するディレクトリとファイル(および消去しないディレクトリとファイル)を判断します。消去する対象として別のディレクトリとファイルを選択するには、設定ファイルで該当ディレクトリとファイルを選択する必要があります。

NetXClean の消去する項目は、メーカーによって選択されているため、これらの変更はお勧めしません。もし変更が必要な場合は、必ず事前に十分な検証を行い問題がないことを確認してください。

設定ファイルでの選択にかかわらず、NetXClean は以下のディレクトリやその親ディレクトリを消去しません。

- Windows ディレクトリ
- Windows System サブディレクトリ
- サービスがインストールされているカレントディレクトリ

NetXClean は以下のプロファイルを消去しません。

- Administrator
- All Users
- Default User
- 前回ログオンしたユーザーのプロファイル

4.1 ユーザープロファイルの保存

NetXClean ユーティリティーはサービスの起動時、ユーザーによるログオフ時またはシャットダウン時に自動的に実行され、設定ファイル(NetXClean.ini)に基づいて、選択したディレクトリ、ファイル、およびプロファイルを消去します。既定の設定では Administrator および User アカウントは NetXClean.ini にユーザープロファイルの削除対象外として登録されていますが、新規に追加したユーザーアカウントあるいはドメインユーザーアカウントはユーザープロファイルが削除されます。ユーザープロファイルを削除対象外として登録するには以下の手順を実行する必要があります。

1. Administrator アカウントでログオンします。

2. FBWF を無効にします。

3. Administrator アカウントでログオンします。

4. C:¥Windows¥System32¥NetXClean.ini ファイルの「Profile」セクションにユーザー名を追加し、ファイルを保存します。
   [Profiles]
   P1=Administrator
   P2=User
   P3=<ユーザー名>

5. 再起動します。

6. Administrator アカウントでログオンします。

7. FBWF を有効にします。

5. ファイルの保存とローカルドライブの使用方法

管理者は、ローカルドライブとファイルの保存について以下の情報を把握する必要があります。

ファイルの保存

シンクライアントは、固定サイズのフラッシュメモリで、組み込みオペレーティングシステムを使用します。保持する必要があるファイルは、シンクライアントではなくサーバーに保存することをお勧めします。

重要

C ドライブに書き込みを行うフラッシュメモリ内アプリケーションの設定(特に、デフォルトでローカルシステムの C ドライブにキャッシュファイルを書き込むアプリケーション)には注意してください。ローカルドライブに書き込む必要がある場合は、Z ドライブを使用するようにアプリケーション設定を変更してください。「5 章(10.「ユーザーアカウント」ウィンドウによるユーザーとグループの管理)」で述べるデフォルト設定を使用すると、出荷時にインストールされているアプリケーションによる C ドライブへの書き込みを最小限に抑えることができます。

ドライブ Z

ドライブ Z は、シンクライアントのオンボード揮発性メモリ(Ms-ramdrive)です。保持する必要があるデータの保存には、このドライブは使用しないことをお勧めします。

RAM ディスクの設定については、「4 章(5. RAM ディスクサイズの設定)」を参照してください。

Z ドライブとローミングプロファイルの使用については、「5 章(7. ドメインへの参加)」を参照してください。

ドライブ C とフラッシュメモリ

ドライブ C は、オンボード不揮発性フラッシュメモリです。ドライブ C への書き込みは避けることをお勧めします。ドライブ C に書き込みを行うと、フラッシュメモリの空き容量が少なくなります。フラッシュメモリの空き容量が 3 MB を下回ると、シンクライアントの動作が不安定になります。

重要

フラッシュメモリは 3 MB 分の空き容量を残すことを強くお勧めします。フラッシュメモリの空き容量が 2 MB になると、シンクライアントのイメージが修復不可能な状態まで破壊され、正規のサービスセンターに連絡してシンクライアントの修理が必要になります。

FBWF が有効な場合は、フラッシュメモリを破壊から保護するために、FBWF キャッシュの容量が超えそうになった場合はエラーメッセージを表示します。このメッセージが表示されると、FBWF キャッシュのファイルをコミットすることはできず、キャッシュ内に残っているシンクライアント設定の変更は失われます。通常動作時に FBWF キャッシュに(FBWF が無効な場合はフラッシュメモリに直接)書き込まれる項目には、以下のようなものがあります。

- お気に入り
- 作成した接続
- 接続の削除と編集

フラッシュメモリをクリーンな状態に維持するにあたっての NetXClean の役割については、「5 章(4. NetXClean ユーティリティーについて)」を参照してください。

6. ネットワークドライブのマッピング

ユーザーと管理者は、ネットワークドライブをマッピングできます。ただし、シンクライアント再起動後もマッピングを保持するには、以下の手順を実行する必要があります。

- 「ログオン時に再接続する」チェックボックスを選択します。
- 設定の変更を再起動後も保時するには、FBWF を無効にする必要があります。詳細な手順については「2 章(3.シンクライアントを設定する前に)」を参照してください。

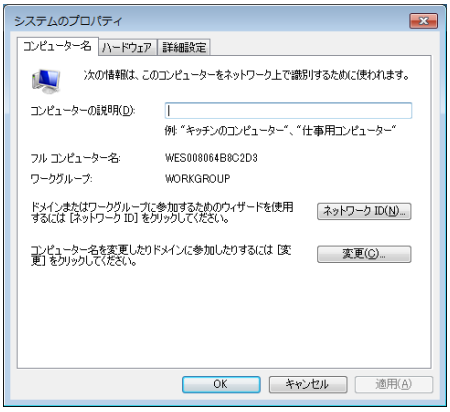
ユーザーマネージャユーティリティーを使用するか、または管理者が知っている別の方法によってリモートホームディレクトリを割り当てることもできます。

7. ドメインへの参加

シンクライアントをドメインに参加させるか、ローミングプロファイルを使用することにより、ドメインに参加することができます。

ドメインへの参加

管理者は、「コンピューター名の変更」ダイアログボックス(「スタート」→「コントロールパネル」→「システム」→「コンピューター名」タブ→「変更」)で、シンクライアントをドメインに参加させることができます。



重要

ログオン時にダウンロードされるプロファイルによってキャッシュやフラッシュメモリがオーバーフローする場合があるので、ドメインにシンクライアントを参加させるときは特に注意が必要です。

シンクライアントをドメインに参加させるときは、FBWF を無効にしてシンクライアントにドメイン情報を永続的に保存できるようにしてください。情報はドメイン参加後のブート時にシンクライアントに書き込まれるので、FBWF は次のブートまで無効のままにしてください。これは、Active Directory ドメインに参加するときに特に重要です。FBWF を無効または有効にする手順については、「2 章(3. シンクライアントを設定する前に)」を参照してください。

ドメイン変更を永続的にするには、以下の手順を実行します。

1. File Based Write Filter を無効にします。
2. ドメインに参加します。
3. シンクライアントをリブートします。
4. File Based Write Filter を有効にします。
5. シンクライアントをリブートします。

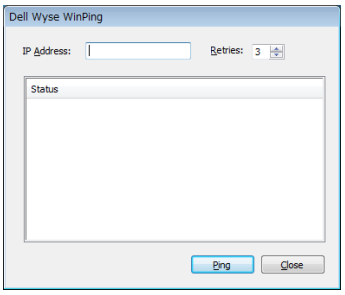
「FBWF を有効」アイコンを使用して FBWF を有効にすると、2 回目のリブートは自動的に実行されます。
デフォルトでは、シンクライアントの起動時またはユーザーのログオフ時に NetXClean ユーティリティーが、特に選択したシステム上のプロファイルを除くすべてのデータを消去します。NetXClean ユーティリティーで新しいプロファイルを消去しないようにする方法については、「5 章(4. NetXClean ユーティリティーについて)」を参照してください。

ローミングプロファイルの使用方法

C ドライブにローミングプロファイルを書き込むことにより、ドメインに参加できます。プロファイルのサイズを制限する必要があります。また、プロファイルは、シンクライアントの再起動時に失われます。
ローミングプロファイルを正常にダウンロードし正しく機能させるためには、ローミングプロファイル用に十分なフラッシュメモリ容量が必要です。ローミングプロファイル用の容量を確保するためにソフトウェアコンポーネントの削除が必要となる場合があります。

8. WinPing 診断ユーティリティーの使用方法

WinPing は、Windows PING (Packet Internet Groper)診断ユーティリティーを起動し、ping からの結果を表示するために使用します。「WinPing」ウィンドウを開くには、「スタート」→「ファイル名を指定して実行」をクリックして、「名前」テキストボックスに「WinPing」と入力し、「OK」をクリックします。



WinPing は、ネットワークホストにエコー要求を送信する診断ツールです。「ホスト」パラメーターには、有効な IP アドレスが入ります。ホストが動作可能な状態でネットワーク上に存在する場合は、エコー要求に応答します。デフォルトでは 3 回エコー要求を送信し、応答が検出されない場合は送信を停止します。WinPing は 1 秒に 1 回エコー要求を送信し、往復時間およびパケット損失の統計を計算し、完了時に短い要約を表示します。

WinPing は、以下の目的で使用します。

- ネットワークおよび各ホストの状態を判断する
- ハードウェアおよびソフトウェアの問題を追跡し、切り分ける
- ネットワークのテスト、評価、および管理を行う

重要

本機能はデフォルトの User アカウントでは「スタート」→「ファイル名を指定して実行」」を使用できないため、User アカウントからは起動できません。

9. Net および Tracert ユーティリティーの使用方法

Net および Tracert ユーティリティーは、IP ネットワーク上でのパケット経路決定などの管理用途に使用できます。これらのユーティリティーについては、http://www.microsoft.com を参照してください。

10.「ユーザーアカウント」ウィンドウによるユーザーとグループの管理

「ユーザーアカウント」ウィンドウを使用して、管理者は新しいユーザーアカウントを作成・管理することができます。また、新しいグループを作成し、詳細なユーザープロファイルのプロパティを設定することができます。「ユーザーアカウント」ウィンドウを開くには、「スタート」→「コントロールパネル」→「ユーザーアカウント」を選択します。デフォルトでは、新しいユーザーは Users グループのメンバーとなり、何も設定されていない状態です。管理者は、新しいユーザーの属性およびプロファイル設定を選択する必要があります。
以降に、以下の項目についてのガイドラインを示します。

- 新しいユーザーアカウントの作成
- ユーザーアカウントの編集
- ユーザープロファイルの設定

ヒント

「ユーザーアカウント」ウィンドウの使用については、ウィザードのヘルプアイコンかサンプルへのリンクをクリックしてください。たとえば、「ユーザーアカウント」ウィンドウのヘルプアイコンをクリックして「Windows ヘルプとサポート」ウィンドウを開くと、ユーザープロファイルやユーザーグループなどの項目を検索し、これらの項目の作成および管理の詳細な手順へのリンクを表示することができます。

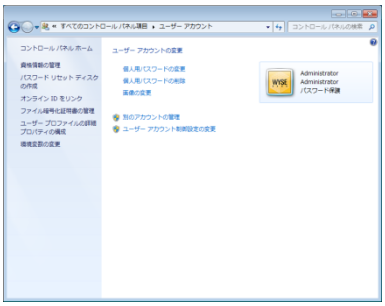
10.1　新しいユーザーアカウントの作成

VNC によってローカルまたはリモートで新しいユーザーアカウントを作成できるのは管理者のみです。
ローカルフラッシュメモリやディスク容量上の制約により、追加ユーザー数は最小限に抑えることをお勧めします。

重要

設定の変更を再起動後も保時するには、FBWF を無効にする必要があります。詳細な手順については「2 章(3.シンクライアントを設定する前に)」を参照してください。

1. 管理者としてログオンし、「ユーザーアカウント」ウィンドウを開きます(「スタート」→「コントロールパネル」→「ユーザーアカウント」)。



2. 「別のアカウントの管理」リンクをクリックし、「ユーザーアカウント」ウィンドウを開きます。

3. 「新しいアカウントの作成」リンクをクリックし、ウィザードを開きます。

4. 標準ユーザーと管理者の作成を完了すると、作成したユーザーが「ユーザーアカウント」ウィンドウに表示されます(「スタート」→「コントロールパネル」→「ユーザーアカウント」→「別のアカウントの管理」)。

10.2　ユーザーアカウントの編集

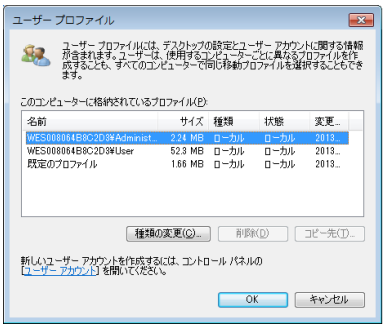
標準ユーザーや管理者アカウントのデフォルト設定を編集するには、「ユーザーアカウント」ウィンドウで、設定を変更したいアカウントをクリックし(「スタート」→「コントロールパネル」→「ユーザーアカウント」→「別のアカウントの管理」)、設定を変更します。

10.3　ユーザープロファイルの設定

シンクライアントに格納されている Default、Administrator、および User のプロファイルを設定するには、「ユーザープロファイル」ウィンドウを開き(「スタート」→「コントロールパネル」→「ユーザーアカウント」→「ユーザープロファイルの詳細プロパティの構成」)、ウィザードで提供する Microsoft 社のマニュアルに従って、「種類の変更」、「削除」、「コピー先」などのコマンドボタンを使用して設定します。.

重要

デフォルトでは、すべてのアプリケーション設定が C ドライブのキャッシュに保存されるように設定されています。FBWF キャッシュのオーバーフローを避けるために、RAM ディスク(Z ドライブ)へのキャッシュを(ユーザーおよび管理者アカウントでデフォルトに設定されているとおり)強くお勧めします。

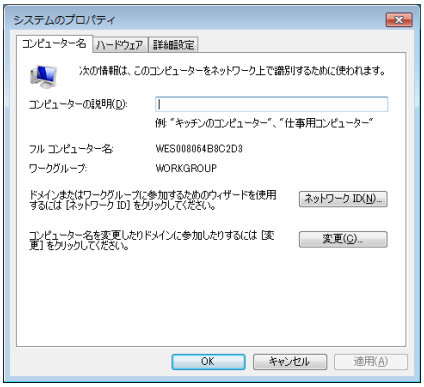


重要

フラッシュメモリのサイズが限られているため、新規ユーザーと既存のユーザーが使用できる他のアプリケーションでローカルファイルシステムへの書き込みを防ぐように設定することを強くお勧めします。同じ理由から、出荷時にインストールされているアプリケーションの設定を変更する場合は特にご注意ください。

11. シンクライアントのコンピューター名の変更

管理者は、「システムのプロパティ」ダイアログボックスの「コンピューター名」タブを使用して、シンクライアントのコンピューター名を変更することができます(「スタート」→「コントロールパネル」→「システム」→「システムの詳細設定」)。コンピューター名情報およびターミナルサービスクライアントアクセスライセンス(TSCAL)は、FBWF の有効／無効にかかわらず保持されます。このため、特定のコンピューターを識別する情報は維持され、シンクライアントのイメージをより簡単に管理できます。



NEC Express5800 シリーズ
US300d

6 システム管理

この章では、シンクライアント環境のメンテナンスに必要な日常作業の実行に役立つローカルおよびリモートシステム管理について説明します。

1. **デフォルト設定の復元**
2. **シンクライアントのBIOS設定へのアクセス**
3. **Wyse USB Firmware Toolによるデバイスイメージの作成**
4. **Wyse Device Managerソフトウェアによるリモート管理**
5. **周辺機器の設定と使用方法**
6. **TightVNCを使用したシンクライアントのリモートシャドー**

1. デフォルト設定の復元

以下の手順で、シンクライアントの各種デフォルト設定を復元できます。

- BIOS を使用して、BIOS セットアップユーティリティー内にあるすべての項目のデフォルト値を復元します(「6 章(2. シンクライアントの BIOS 設定へのアクセス)」を参照してください)。
- シンクライアントのイメージを再作成し、Wyse USB Firmware Tool または Wyse Device Manager を使用して工場出荷時のすべてのデフォルト設定を復元します(「6 章(3. Wyse USB Firmware Tool によるデバイスイメージの作成)」および「6 章(4. Wyse Device Manager ソフトウェアによるリモート管理)」を参照してください)。

イメージ再作成の準備

Windows Embedded Standard を実行するシンクライアントは、ファームウェアをアップグレードするときと同じプロセスでシンクライアントのイメージを再作成して工場出荷時のデフォルトに戻すことのみ可能です。イメージ再作成プロセスに必要なものは、以下のとおりです。

- **イメージ作成ソフトウェア**

  Windows Embedded Standard を実行するシンクライアントのイメージを再作成するために、二種類のイメージ作成ソフトウェア製品が提供されています。

  - Wyse® USB Firmware Tool™
    比較的小規模な環境にお勧めです(「6 章(3. Wyse USB Firmware Tool によるデバイスイメージの作成)」を参照してください)。
  - Wyse Device Manager™
    比較的大規模な環境にお勧めです(「6 章(4. Wyse Device Manager ソフトウェアによるリモート管理)」を参照してください)。

2. シンクライアントの BIOS 設定へのアクセス

クライアントを起動すると、短い時間 Wyse のロゴが表示されます。この期間に Del キーを押すと、シンクライアントの BIOS 画面に入って変更を行うことができます。パスワードの入力を求められた場合は、「Fireport」と入力してください。

US300d は工場出荷状態では SATA モードが「AHCI」に設定されております。しかし BIOS の「Load Setup Defaults」を使用してデフォルトに初期化すると、「IDE」に設定され、オペレーションシステムが起動できなくなります(OS の起動途中でブルースクリーンが表示されます)。以下の手順で、SATA モードを「AHCI」に設定してください。

1. **BIOS メニューの「Advanced」→「SATA Mode」を選択し、「Enter」キーを押します。**
2. **「AHCI」を選択し、「Enter」キーを押します。**
3. **BIOS メニューの「Exit」→「Exit Saving Changes」を選択し、「Enter」キーを押します。**
4. **「Yes」を選択し、「Enter」キーを押し、BIOS 設定の保存と再起動を行います。**

3. Wyse USB Firmware Tool によるデバイスイメージの作成

Wyse® USB Firmware Tool™ は、IT 部門やカスタマーサービス部門のスタッフが、サポートされているデバイスのイメージを簡単に作成するシンプルな USB イメージ作成ソリューションを提供します。
USB Firmware Tool は、下記 URL よりダウンロードできます。
http://www.nec.co.jp/products/thinclient/support/index.shtml

このツールの柔軟なウィンドウユーティリティーを使用して、以下の操作を簡単に実行できます。

- 端末からファームウェアイメージを取得し、他の対象端末にファームウェアイメージを送信するように USB メモリを設定します。
- コンピュータ上にあるファームウェアイメージを参照し、対象端末にファームウェアイメージを送信するように USB メモリを設定します。
- 異なる場所にいるユーザーが同時に使用できるように、ファームウェアイメージを既に構成済みの USB メモリを複製します

本製品のディスク容量は 16GB のため、USB Firmware Tool を使用してファームウェアイメージを取得するには、メモリ容量が 32GB の USB メモリが必要です。

4. Wyse Device Manager ソフトウェアによるリモート管理

Wyse Device Manager™ (WDM)サーバーは、シンクライアントにネットワーク管理サービス(リモートシャドー、リブート、シャットダウン、ブート、名前の変更、自動デバイスチェックインサポート、Wake-On-LAN、デバイスプロパティの変更などの機能による完全なユーザーデスクトップ制御)を提供します。WDM を使用すると、すべてのネットワークデバイスを使いやすい単一のコンソールで管理することができます。

WDM プロパティの設定については、「4 章(11. WDM プロパティの設定)」を参照してください。

WDM がアクセスできるローカルのカスタムフィールドについては、「4 章(2. Custom Fields による設定文字列の設定)」を参照してください。

また、Wyse Device Manager™ は、以下の Web サイトからウンロードできます。

http://www.nec.co.jp/products/thinclient/support/index.shtml

5. 周辺機器の設定と使用方法

本装置では周辺機器を接続して利用することができます。

なお、標準添付品、純正オプション以外の周辺機器についてはサポート対象外です。実運用環境への導入に関しては、運用環境に基づいた設定で十分な事前検証を行い、システムインテグレーション上問題ないことを確認してから使用してください。

6. TightVNC を使用したシンクライアントのリモートシャドー

TightVNC Server はシンクライアントにインストールされています。TightVNC Server を使用して、TightVNC Viewer がインストールされているリモートマシンからシンクライアントを操作および監視(リモートシャドー)できます。(TightVNC Viewer は事前にリモート操作／シャドーイングするマシンにインストールする必要があります。Wyse Device Manager ソフトウェアのコンポーネントには TightVNC Viewer が含まれており、WDM 管理コンソールからリモート操作できます。)
これにより、リモート管理者はシンクライアントの設置場所に行かずに、離れた場所からシンクライアントを設定またはリセットできます。VNC の主な目的はサポートとトラブルシューティングです。TightVNC Server は、シンクライアントの起動時にサービスとして自動的に起動されます。このサービスは、「サービス」ウィンドウ(「スタート」→「コントロールパネル」→「管理ツール」→「サービス」)から起動または停止することもできます。

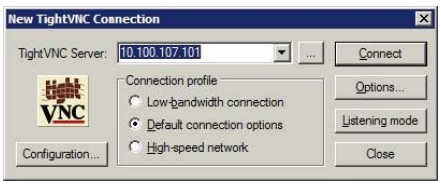
設定の変更を再起動後も保時するには、FBWF を無効にする必要があります。詳細な手順については「2 章(3.シンクライアントを設定する前に)」を参照してください。

TightVNC Viewer がインストールされているリモートマシンで管理者が TightVNC サーバーがインストールされているシンクライアントにアクセスするには、以下の条件を満たしている必要があります。

- 管理者が、シャドーイング、操作、および監視するシンクライアントの IP アドレス(または有効な DNS 名)を把握している(「3 章(2. Dell Wyse シンクライアント情報の表示)」を参照)。管理者が操作するシンクライアントの IP アドレスを見るには、管理者タスクバーのシステムトレイの「TightVNCServer」アイコンの上にマウスポインターを置きます。
- 管理者が、シャドーイング、操作、および監視するシンクライアントのプライマリパスワード(デフォルト：Wyse)を把握している(「6 章(6.1 TightVNC サーバーのプロパティの設定)」を参照)。

リモートマシンからシンクライアントをシャドーイングするには、以下の手順を実行します。

1. 「New Tight VNC Connection」ダイアログボックスを開きます(「スタート」→「すべてのプログラム」→「TightVNC」→「TightVNC Viewer」など)。



2. シャドーイング、操作、監視するシンクライアントの IP アドレスまたは有効な DNS 名を入力します(コマンドボタンでその他のオプションを設定することもできます)。

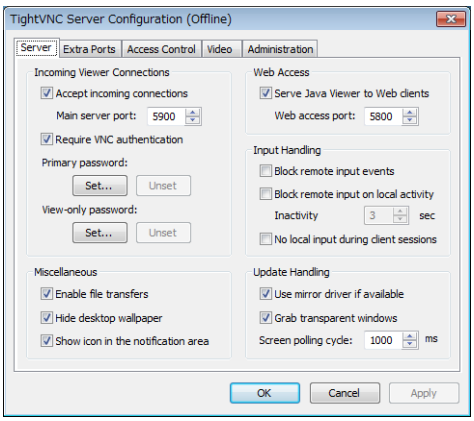
3. 「OK」をクリックし、「VNC Authentication」ダイアログボックスを開きます。

4. シャドーイングするシンクライアントのパスワード(シャドーイングするシンクライアントのプライマリパスワード。デフォルトパスワードは「Wyse」)を入力し、「OK」をクリックします。管理者向けに、リモートマシン上の別ウィンドウにシャドーイング、操作、監視するシンクライアントが表示されます。リモートマシンのマウスとキーボードで、ローカルでの操作時と同様にシンクライアントを操作します。

6.1 TightVNC サーバーのプロパティの設定

「TightVNC Server Configutation (Offline)」ダイアログボックスを開くには、「スタート」→「すべてのプログラム」→「TightVNC」→「TightVNC Server (Application Mode)」→「TightVNC Server-Offline Configuration」をクリックするか、または管理者タスクバーのシステムトレイ内の「TightVNC Server」アイコンをダブルクリックします。管理者は「サーバー」タブでプライマリパスワード(管理者がシンクライアントのシャドーを行う際に必要となるパスワード)を設定できます(デフォルトパスワードは「Wyse」)。

重要　**セキュリティ上、シンクライアントを受け取ったらただちにパスワードを変更することを強くお勧めします。**



パスワードの変更するには以下の手順を実施します。シンクライアントでパスワードを変更する前に必ず File Based Write Filter (FBWF)を無効にし、パスワード変更後に再度有効にしてください。詳細な手順については「2 章(3.シンクライアントを設定する前に)」を参照してください。

1. Administrator でログオンします。
2. タスクバーのシステムトレイにある「TightVNC」アイコンの右クリックメニューから「Configuration...」をクリックします。
3. 「TightVNC Control Authentication」ダイアログが表示され、Administrative password を入力します。デフォルトのパスワードは「Wyse」です。
4. 「TightVNC Server Configuration」ダイアログの「Administration」タブ→「Control Interface」→「Change...」ボタンをクリックします。
5. 「Change Password」ダイアログで、新しいパスワードと確認用パスワードを入力し、「OK」ボタンをクリックします。
6. 「TightVNC Server Configuration」ダイアログの「Server」タブ→「Incoming Viewer Connections」→「Primary password」→「Change...」ボタンをクリックします。
7. 「Change Password」ダイアログで、新しいパスワードと確認用パスワードを入力し、「OK」ボタンをクリックします。
8. 「TightVNC Server Configuration」ダイアログの「Server」タブ→「Incoming Viewer Connections」→「View-only password」→「Change...」ボタンをクリックします。
9. 「Change Password」ダイアログで、新しいパスワードと確認用パスワードを入力し、「OK」ボタンをクリックします。
10. 「TightVNC Server Configuration」ダイアログの「OK」ボタンをクリックします。

NEC Express5800 シリーズ
US300d

7 サーバー環境の設定

この章では、シンクライアントにネットワークおよびセッションサービスを提供するために必要なネットワークアーキテクチャーと企業サーバー環境について説明します。
本セクションでは以下の内容について説明します。

1. **ネットワークサービスの設定方法について**
2. **ダイナミックホストコンフィギュレーションプロトコル(DHCP)を使用する場合**
3. **ドメインネームシステム(DNS)を使用する場合**
4. **セッションサービスについて**
5. **ICAセッションサービスの設定**
6. **RDPセッションサービスの設定**
7. **VMware View Managerサービスの使用方法**

1. ネットワークサービスの設定方法について

シンクライアントが使用するネットワークサービスには、DHCP、DNS などがあります。ネットワークサービスの設定方法は、ご使用の環境で利用可能なものとそれをどのように設計・管理するかによって異なります。以下の項目で、ネットワークサービスの設定に役立つ重要な情報を紹介します。

- ダイナミックホストコンフィギュレーションプロトコル(DHCP)を使用する場合
- ドメインネームシステム(DNS)を使用する場合

2. ダイナミックホストコンフィギュレーションプロトコル(DHCP)を使用する場合

初期状態のシンクライアント(新しいシンクライアントまたはデフォルト設定にリセットされたシンクライアント)は IP アドレスおよびネットワーク設定を DHCP サーバーから取得するように設定されています。シンクライアントの設定およびアップグレードには、DHCP を使用することをお勧めします。これにより、複数のシンクライアントでこれらの設定を行う手間を軽減できます。DHCP サーバーを使用できない場合は、固定 IP アドレスを割り当てることができます。固定 IP アドレスは、デバイスごとにローカルに入力する必要があります。Wyse Device Manager (WDM)サーバーの IP アドレスも DHCP サーバーから取得できます(WDM については、「6 章(4. Wyse Device Manager ソフトウェアによるリモート管理)」を参照してください)。

シンクライアントでは、次の表に示す DHCP オプションを使用できます。DHCP サーバーの設定については、Microsoft 社の Web サイトのマニュアルを参照してください(http://www.microsoft.com)。

オプション	説明	備考
1	サブネットマスク	必須項目です。
3	ルーター	設定は任意ですが推奨されるオプションです。ただし、シンクライアントが別のサブネット上のサーバーと対話する必要がない限り、必要ありません
6	DNS サーバー	設定は任意ですが推奨されるオプションです。
12	ホスト名	設定は任意です。
15	ドメイン名	設定は任意ですが推奨されるオプションです。
43	ベンダークラス固有の情報	設定は任意です。
50	要求される IP	必須項目です。
51	リース時間	必須項目です。
52	オプションのオーバーロード	設定は任意です。
53	DHCP メッセージタイプ	必須項目です。
54	DHCP サーバーの IP アドレス	推奨オプションです。
55	パラメーター要求リスト	シンクライアントによって送信されます。
57	最大 DHCP メッセージサイズ	設定は任意です(常にシンクライアントによって送信されます)。
58	T1 (更新)時間	必須項目です。
59	T2 (リバインド)時間	必須項目です。
61	クライアント識別子	常に送信されます。
155	リモートサーバーの IP アドレスまたは名前	設定は任意です。
156	接続に使用するログオンユーザー名	設定は任意です。
157	接続に使用するドメイン名	設定は任意です。
158	接続に使用するログオンパスワード	設定は任意です。
159	接続用コマンドライン	設定は任意です。
160	接続用作業ディレクトリ	設定は任意です。
161	FTP サーバーリスト	設定は任意です。
162	FTP ファイルへのルートパス	設定は任意です。
163	SNMP トラップサーバーの IP アドレスリスト	設定は任意です。
164	SNMP 設定コミュニティー	設定は任意です。
165	RDP 起動公開アプリケーション	設定は任意です。
166	Ericom 社 PowerTerm® TEC モード	設定は任意です。
167	Ericom 社 PowerTerm® TEC ID	設定は任意です。
168	仮想ポートのサーバー名	設定は任意です。

3. ドメインネームシステム(DNS)を使用する場合

シンクライアントは、企業イントラネットで利用可能な DNS サーバー上で登録されている有効な DNS 名を受け付けます。シンクライアントは、ネットワーク上の DNS サーバーに名前を照会して IP アドレスを解決します。ほとんどの場合、DNS は必須ではありませんが、DNS を使用すると、IP アドレスではなく登録した DNS 名でホストにアクセスできます。Windows 2000 以降の Windows DNS サーバーはすべてダイナミック DNS (DDNS)を装備しており、サーバーはすべて DNS サーバーに動的に登録されます。DNS ドメインの DHCP エントリーおよびサーバー場所情報については、「7 章(2.ダイナミックホストコンフィギュレーションプロトコル(DHCP)の使用方法)」を参照してください。

4. セッションサービスについて

ICA および RDP セッションサービスを設定する前に、必ず以下のガイドラインを理解し、これに従ってください。

Windows Embedded Standard を実行するシンクライアントは、「7 章(7. VMware View Manager サービスの使用方法)」で説明しているような仮想デスクトップソリューションもサポートしています。

- **全体的なガイドライン**

  シンクライアントセッションサービスは、Citrix ICA および Microsoft RDP ソフトウェア製品のホストとして機能するサーバーによって提供されます。

- **ICA のガイドライン**

  Independent Computing Architecture (ICA)は、アプリケーションのロジックをユーザーインターフェースから切り離す 3 層から成るサーバーベースのコンピューティング技術です。ユーザーは、シンクライアントにインストールされている ICA クライアントソフトウェアにより表示されるアプリケーションの GUI を操作できます。一方、アプリケーションプロセスはすべてサーバー上で実行されます。ICA の設定については、「7 章(5. ICA セッションサービスの設定)」を参照してください。

ICA サーバーのライセンスは、Citrix Systems, Inc.から取得する必要があります。Citrix サーバーファームに同時にかかるシンクライアントの負荷に対応できるだけのクライアントライセンスを購入してください。すべてのライセンスが使用中のときに接続に失敗するのは、シンクライアントの故障によるものではありません。ICA クライアントソフトウェアは、シンクライアントにインストールされます。

- **RDP のガイドライン**

  Remote Desktop Protocol(RDP)は、シンクライアントが Windows Server 2003、Windows Server 2008 または Windows Server 2012 で動作するターミナルサービス (リモートデスクトップサービス) とネットワーク経由で通信するためのネットワークプロトコルです。RDP の設定については、「7 章(6. RDP セッションサービスの設定)」を参照してください。

5. ICA セッションサービスの設定

このセクションの情報を利用して ICA セッションサービスを設定する前に、必ず「セッションサービスについて」をお読みください。
ICA セッションサービスは、ターミナルサービス（リモートデスクトップサービス）と以下のいずれかがインストールされている状態で、Windows Server 2003、Windows Server 2008 または Windows Server 2012 を使用してネットワーク上で利用できます。

- Citrix XenApp
- Citrix XenDesktop

製品に添付されているガイドに従って上記の製品をインストールし、サーバー環境を共有するシンクライアントにセッションおよびアプリケーションを提供します。

ICA セッションサービスを Windows Server OS 上で使用する場合は、ネットワーク上のアクセス可能な場所にターミナルサービスクライアントアクセスライセンス(TSCAL)サーバーが常駐している必要があります。このサーバーは、デバイス単位で一時ライセンス(120 日間有効)を付与します。この一時ライセンスの有効期間(120 日間)が終了した後は、TSCAL を購入して TSCAL サーバーにインストールする必要があります(一時ライセンスまたは永久ライセンスなしで接続することはできません)。

6. RDP セッションサービスの設定

このセクションの情報を利用して RDP セッションサービスを設定する前に、必ず「セッションサービスについて」をお読みください。

RDP セッションサービスは、以下の端末にリモート接続するときに使用されます。
Windows 2003、Windows XP Professional、Windows Vista (サポート対象バージョンのみ)、Windows 7 (サポート対象バージョンのみ)、Windows 8 (サポート対象バージョンのみ) が動作するデスクトップ PC、または Windows Server 2003、Windows Server 2008、Windows Server 2012 が動作するサーバーRemote Desktop Protocol により、シンクライアントは Windows アプリケーションを Windows GUI 環境下で実行できます。ただし、実際にはこれらの Windows アプリケーションは接続しているコンピューター上で実行されています。

製品に添付されているガイドに従って上記の製品をインストールし、サーバー環境を共有するシンクライアントにセッションおよびアプリケーションを提供します。

Windows Server OS を使用する場合は、ネットワーク上のアクセス可能な場所にターミナルサービスクライアントアクセスライセンス(TSCAL)サーバーが常駐している必要があります。このサーバーは、デバイス単位で一時ライセンス(120 日間有効)を付与します。この一時ライセンスの有効期間(120 日間)が終了した後は、TSCAL を購入して TSCAL サーバーにインストールする必要があります(一時ライセンスまたは永久ライセンスなしで接続することはできません)。

7. VMware View Manager サービスの使用方法

VMware® View Manager は、システム管理者がデスクトップを設定し、ユーザーアクセスを制御するためのデスクトップ管理ソリューションです。クライアントソフトウェアを使用して、ユーザーは中央の仮想デスクトップ、バックエンドの物理システム、またはターミナルサーバーにセキュアに接続します。

View Manager のインストールおよび設定については、VMware の Web サイトを参照してください(http://www.vmware.com)。

View Manager は、以下の主要なコンポーネントで構成されています。

- **View Connection Server**
  クライアント接続のブローカーとして機能するソフトウェアサービスで、入って来たリモートデスクトップユーザー要求を認証し、仮想デスクトップ、物理デスクトップ、またはターミナルサーバーに適宜振り分けます。

- **View Agent**
  ゲスト仮想マシン、物理システム、またはターミナルサーバーにインストールされるソフトウェアサービスで、それらをすべて View Manager で管理できるようにします。RDP 接続の監視、仮想印刷、リモート USB のサポート、シングルサインオンなどの機能を提供します。

- **View Client**
  View Connection Server と通信する、ローカルでインストールするソフトウェアアプリケーションで、ユーザーが Microsoft リモートデスクトッププロトコル(RDP)を使用してデスクトップに接続できるようにします。

- **View Client with Offline Desktop (試行中)**
  ユーザーが仮想マシンをダウンロードしてローカルシステムで使用するためのオフラインデスクトップ機能をサポートするために拡張された View Client の 1 つのバージョンです。

- **View Portal**
  複数のオペレーティングシステムおよびブラウザーによってサポートされている View Client の Web 版です。

- **View Administrator**
  View Manager の管理者が View Connection Server を設定し、デスクトップを展開および管理し、ユーザー認証を制御し、システムイベントを開始および検査し、分析処理を行うための Web アプリケーションです。

- **View Composer**
  VirtualCenter サーバーにインストールされるソフトウェアサービスで、View Manager が、リンクされている複数のクローンデスクトップを中央の 1 つのベースイメージから迅速に展開できるようにします。

NEC Express5800 シリーズ
US300d

8

ソフトウェア情報と注意・制限事項

本製品のソフトウェア情報と、運用における注意・制限事項について説明します。

1. **本製品のソフトウェア情報**
   本製品のソフトウェア情報について説明します。

2. **注意・制限事項**
   本製品の運用における注意・制限事項について説明します。

1. ソフトウェア情報

本製品のソフトウェア情報を記載します。

1.1 ディスク構成

ディスクは 2 つのパーティションにより構成されます。

- BootAgent バージョン 2.8.0（ディスクの管理のドライブ文字の無い FAT32 で表示する 16 メガバイトの領域）
- OS パーティション

1.2 OS ビルド情報

項目	詳細
プラットフォーム	US300d
英語版OSビルドバージョン	BDB0.2231.16GB
日本語版OSビルドバージョン	BDB0.2232.16GB

1.3 BIOS 情報

項目	詳細
プラットフォーム	US300d
BIOSバージョン	3.0E

1.4 アプリケーション情報

アプリケーション名	製品バージョン
Adobe Flash Player ActiveX	11.8.800.94
Adobe Flash Player Plugin	11.8.800.94
AMD Catalyst Install Manager	8.0.915.0
Citrix HDX RealTime Media Engine	1.4
Citrix Receiver (Standard)	4.0.0.45893 (14.0.0.91)
Dell Wyse Client Information	3.0.0.22
File Based write filter manager	1.0.299.0
Intel® PROSet/Wireless Software for Bluetooth® Technology	3.1.1036.0352
Internet Explorer	10.0.9200.16635
Microsoft .NET Framework 4.5	4.5.50709
Microsoft Lync Vdi 2013	15.0.4420.1017
Microsoft Silverlight	5.1.20513.0
Microsoft System Center 2012 Configuration Manager	5.00.7804.1000
Microsoft Visual C++ 2005 Redistributable	8.0.61001
Microsoft Visual C++ 2008 Redistributable (x86)	9.0.30729.4148
Microsoft Visual C++ 2010 Redistributable (x86)	10.0.30319
Microsoft Visual C++ 2012 Redistributable (x86)	11.0.50727.1
Power Term InterConnect	10.1.0.0
Realtek High Definition Audio Driver	6.0.1.7004
Remote Desktop Client (RDP8.0)	6.2.9200.16398
TightVNC	2.6.4.0
VMware Horizon View Client	5.4.0.1219906
vWorkspace Connector for Windows	8.0.0.1186
WDM HAgent	6.1.1.3
Windows Media Player	12.0.7601.17514
Wyse Configuration Manager Agent	1.2.0.0

2. 注意・制限事項

本製品の使用時の注意・制限事項について説明します。

2.1 サポート対象外の機能およびソフトウェア

下記機能の使用についてはサポート対象外となります。実運用環境への導入に関しては、運用環境に基づいた設定で十分な事前検証を行い、システムインテグレーション上問題ないことを確認してから使用してください。

- Citrix HDX RealTime Media Engine
- Microsoft Lync Vdi 2013
- Microsoft System Center 2012 Configuration Manager
- Power Term InterConnect
- vWorkspace Connector for Windows
- Wyse Configuration Manager Agent

下記のソフトウェアの使用については記載しているバージョン以降をサポートします。導入に関しては必ず記載以降のバージョンを使用してください。前バージョンについてはサポート対象外となります。

- Wyse Device Manager 4.9.1 (Hotfix04091034412 適用)
- Wyse USB Firmware Tool v1.20.0.1

2.2 注意・制限事項

- 本製品に搭載されているソフトウェア、およびサポートページで公開されている関連ソフトウェアについて、ソフトウェア開発メーカーのサポート期間終了後は、不具合の修正対応ができなくなります。この場合、既知事例の確認といった限定的なサポートのみとなり、基本的には as-is(あるがまま)の状態で運用回避頂くことになります。このような事態を避けるためにシステム構築時、運用開始後は速やかに全ての運用ケースで十分な検証を行い問題がないことを確認してください。

- Windows OS を搭載したシンクライアント端末は、工場出荷状態で User アカウントに対して一部操作を制限する等の基本的なセキュリティ対策を実施していますが、セキュリティ面の問題がないことを保証するものではありません。お客様の運用環境やセキュリティ要件に合わせて、User アカウントに対する機能制限の追加や使用しないネットワークポートの閉塞といったカスタマイズを行い、問題ないことを事前確認の上、ご利用ください。

- シンクライアントシステムは他の IT システムと同様に、ネットワーク構成やポリシー設定、利用する周辺機器の仕様等の影響で動作しない、あるいは十分な性能が出ない可能性があります。また、機能によってはサードパーティ製のソフトウェアの導入が必要となります。本製品はあらゆる環境での動作は保証し

ておらず、ご利用にあたっては必ず運用される環境で事前に十分な検証を行い問題がないことを確認してください。

- 本製品は RDP セッションサービスで RDP8.0 を使用可能ですが、RDP8.0 を使用するには接続先仮想環境が RDP8.0 に対応している必要があります。対応していない場合は互換性がある RDP7.1 以前のバージョンの RDP が使用されます。RDP8.0 を使用した場合、「エクスペリエンス」タブの接続オプション「ビットマップキャッシュの保持」を有効（デフォルト有効）にすると、セッションからログオフ後に警告メッセージ「The System is running out of available memory.」が表示され、強制的に再起動する場合があります。これは、FBWF キャッシュの設定容量に対し、ローカルに保存されたキャッシュの容量が 90%を超えた場合に、FBWF のコントロールユーティリティーがシステムを保護するために自動で再起動するためです。

  RDP8.0 プロトコルは「ビットマップキャッシュの保持」が有効の場合、セッション内で使用した画像や動画のビットマップキャッシュをセッションログオフ後に端末上に保存し、次回アクセス時のパフォーマンスを改善します。しかし、本製品ではシステム保護のためにローカルフラッシュに対する書き込みは FBWF によりキャッシュに保存され、キャッシュ容量を超えてシステムに深刻な影響がでないように監視しています。RDP8.0 使用時にはキャッシュがオーバーフローすることが無いように接続オプションの「ビットマップキャッシュの保持」を無効にすることを強く推奨します。

  また、MS VDI(RDWeb アクセス)、あるいは VMware Horizon View Client 等のブローカーサーバー経由で RDP8.0 プロトコルを使用する場合は下記手順でビットマップキャッシュの保持を無効にできます。

  1. Administartor でログオンする。
  2. FBWF を無効にする。
  3. Administrator でログオンする。
  4. 「コントロールパネル」→「フォルダーオプション」→「表示」タブ→「隠しファイル、隠しフォルダー、及び隠しドライブを表示する」をチェックします。
  5. 「適用(A)」ボタンをクリックします。
  6. C:¥Users¥<ユーザー名>¥Documents¥Default.rdp ファイルを選択し、右クリックメニューの「プログラムから開く」をクリックします。

  既定の設定では Administrator および User アカウントは NetXClean.ini にプロファイルの削除対象外として登録されています。しかし、新規に追加したユーザーアカウントあるいはドメインユーザーアカウントの場合は､ユーザープロファイルは削除されます｡ユーザープロファイルが削除されると Default.rdp への変更も削除されるため、NetXClean.ini を使用してユーザープロファイルが削除されないように登録する必要があります。詳細な手順については「5 章(4. NetXClean ユーティリティーについて)」を参照してください。

  7. 「ほかのプログラム」→「メモ帳」をダブルクリックします。
  8. 下記の値を 1 から 0 へ変更し、ファイルを上書き保存します。
     bitmapcachepersisteenable:i=0
  9. ファイルを閉じて、FBWF を有効にします。

- 本製品では User アカウントでログオン時に、C ドライブに対してアクセスできないように制限されています。そのため、User アカウント上で各セッションサービス(ICA、RDP 等)を利用時に、「ローカルリソース」タブの接続オプション「ローカルデバイスとリソース」でローカルディスク(C:)を指定しても、セッション内で利用することはできません。

- RDP では Windows Media Player に対して、Widnows メディアリダイレクト機能をサポートしています。本機能はサーバー側の仮想デスクトップ上でマルチメディアコンテンツを再生すると、クライアントへエンコードした状態で送信し、デコード処理はクライアント側で行うため、ネットワーク帯域使用量の増加を防止できます。その結果負荷は軽減され、マルチメディア再生(VC-1、MPEG-1、H.264 など)がスムーズに処理されます。ただし、本機能は Windows Media Player に依存しており、Windows Media Player 以外のコンテンツでは動作しません(例えば FLASH、SilverLight、および QuickTime など)。

- RDP8.0 では RemoteFX Media Streaming 機能をサポートしていますが、システム要件として HYPER-V ホストサーバー上に別途 GPU が必要になり、仮想マシン上にも RemoteFX 3D ビデオアダプターが必要です。本機能はすべてのビデオフォーマットおよびビデオアプリケーションをサポートしており、FLASH、SilverLight、QuickTime および HTML5 などもクライアントへリダイレクトされ、スムーズに再生されます。RDP8.0 は、まず Windows メディアリダイレクトを有効にします。Windows メディアリダイレクトの条件が満たされない場合は自動的に RemoteFX Media Streaming 機能を使用するように切り替わります。

- Windows Media Player がサポートするコーデックについては Windows Media Player の「ヘルプ」-「バージョン情報」-「テクニカルサポート情報」をクリックすることで確認できます。

- 本製品は AMD Radeon™HD 6250 グラフィックスが搭載されており、Unified Video Decoder(UVD) 3 による VC-1、H.264、MPEG-2 のハードウェアデコーディングが可能です。Windows Media Player 12 には MPEG-2 のコーデックは標準で搭載されていませんが、本機能により US300d 上で MPEG-2 ファイルのローカル再生が可能です。しかし仮想マシン上では、コーデックが無いと再生できないため注意が必要です。

- ICA 接続で、Windows Media Player を使用して動画を再生すると、メモリ不足等が発生し動画が再生できなくなる場合があります。その場合は、US300d を再起動し、再接続してから動画を再生してください。

- Citrix HDX USB リダイレクション機能を使用すると、USB デバイスによっては端末側でブルースクリーンが発生する場合があります。使用する USB デバイスについては、事前に十分な検証を行い問題がないことを確認してから使用してください。

- Citrix XenDesktop 7 を使用して、Windows 8 の仮想 PC へ接続すると、デスクトップ上にマウスカーソルが表示されない場合があります。その場合は、一度デスクトップ上でマウスを右クリックしてください。

- 本製品に保存される Citrix サーバーへの設定情報は、デフォルトの設定では再起動すると破棄されます。

- Wyse Device Manager に含まれる TightVNC Viewer コンポーネントは本製品にインストールされている TightVNC Server の Attach Listening Viewer 機能には対応していません。

- Custom Fields に日本語等のマルチバイト文字(2 バイト文字)を設定すると、Wyse Device Manager 管理コンソール上で「Device Information」の表示が文字化けします。Custom Fields にはマルチバイト文字を使用しないでください。

- US300d の UAC(User Account Control)はデフォルトで無効に設定されております。Wyse Device Manager 等を使用したリモート管理に影響があるため、有効にしないでください。

- Internet Explorer の SmartScreen フィルター機能はデフォルトで無効に設定されております。通常は有効にする必要はありません。

- Windows エクスペリエンスインデックス機能で評価を実行すると、FBWF でシンクライアントを保護している都合上、ディスクパフォーマンスの測定でエラーになります。既定の動作ですので問題はありません。

- Wyse Device Manager 4.9.1 (Hotfix04091034412 適用)を使用して、US300d の OS クローンイメージ取得時に、OS のみ(CMOS と BIOS を除く)を選択すると、取得したクローンイメージの配信に失敗します。クローンイメージを取得する場合は、必ず OS イメージ取得オプションに「All」を選択してください。
  本事象は Wyse Device Manager 4.9.1 に HotFix 4 を適用することで修正されます。Wyse Device Manager 4.9.1 (HotFix 4) を適用した場合は、OS クローンイメージ取得時に、OS のみ(CMOS と BIOS を除く)を選択したクローンイメージの場合も正常に配信できます。

- [コントロールパネル] - [電源オプション] - [スリープ解除時のパスワード保護] - [パスワードを必要とする]が設定されている場合でも、スリープ解除時にパスワードを入力する画面には遷移されません。

- [コントロールパネル] - [マウス] - [ポインターオプション] - [文字の入力中にポインターを非表示にする]の設定を無効に設定しても文字の入力中にマウスポインターは表示されません。

- ICA 接続で全画面接続時に表示されるメッセージ(「ヒント: 全画面モードについて」)を表示した状態で放置した場合、接続後に ICA セッション内でキーボードやマウスなどの操作が効かなくなる場合があります。この場合は、セッションウィンドウをウィンドウモード(SHIFT＋F2 キー)に変更後、セッションウィンドウを[×]ボタンで閉じて再度 ICA セッションに接続してください。
  本事象を回避するには、「ヒント: 全画面モードについて」のダイアログを表示しないように設定してください。「ヒント: 全画面モードについて」のダイアログにて、「次回からこのダイアログボックスを表示しない」にチェックを入れることで、次回以降のログオンにおいては、「ヒント: 全画面モードについて」のダイアログは表示されなくなります。

- User 権限アカウントでは、Internet Explorer の[お気に入り]一覧にあるサイトの移動はできません。

NEC Express5800 シリーズ
US300d

9 運用・保守

本機の運用などにおいて、点検、保守、またはトラブルが起きたときの対処について説明します。

1. **クリーニング**
   本機を良い状態に保つため、クリーニングについて説明しています。

2. **トラブルシューティング**
   故障かな？と思ったときに参照してください。トラブルの原因とその対処方法について説明しています。

3. **移動と保管**
   移動、および保管方法について説明しています。

4. **ユーザーサポート**
   本製品に関するさまざまなサービスについて説明しています。サービスは、弊社、および弊社が認定した保守サービス会社が提供します。

1. クリーニング

本製品を良い状態に保つために定期的にクリーニングしてください。

警告

本製品を安全にお使いいただくために次の注意事項を必ずお守りください。指示を守らないと、人が死亡する、または重傷を負うおそれがあります。詳しくは「使用上のご注意」をご覧ください。

- **自分で分解・修理・改造はしない**

1.1 US300d・キーボードのクリーニング

本製品の外観の汚れは、柔らかい布でふき取ってください。汚れが落ちにくいときは、次のような方法できれいになります。

- **シンナー、ベンジンなどの揮発性の溶剤は使わないでください。材質のいたみや変色の原因になります。**
- **本製品、コンセント、ケーブル、本製品背面のコネクタ、本製品周辺は絶対に水などでぬらさないでください。**

11. 本製品の電源が OFF になっていることを確認する。
12. 本製品の電源コードをコンセントから抜く。
13. 電源コードの電源プラグ部分についているほこりを乾いた布でふき取る。
14. 中性洗剤をぬるま湯または水で薄めて柔らかい布を浸し、よく絞る。
15. 本製品の汚れた部分を手順 4 で用意した布で少し強めにこすって汚れを取る。
16. 真水でぬらしてよく絞った布でもう一度ふく。
17. 乾いた布でふく。

2. トラブルシューティング

本製品を使用中に故障と思われる現象が起きたら、まず本章を参考に現象を解析してください。

2.1 仮想 PC 接続時のトラブル

［?］**仮想PCに接続できない**

→ 仮想PCとUS300dの日付・時刻が設定されていない場合、仮想PCに接続できないことがあります。US300dを起動した直後は、日付・時刻が設定されていません。この場合、時刻サーバーを設定して、正しい日付・時刻を取得してください。

［?］**マウスポインタが見えにくい**

→ Windows Vista以降のOSの仮想PCに接続した場合、マウスポインタが黒く表示され、見にくい場合があります。この場合、仮想PC側の[コントロールパネル] - [マウス] - [ポインタ]タブ - [デザイン]からマウスポインタの設定を見えやすいものに変更してください。

［?］**デバイスマッピングさせたUSBストレージデバイス上の右クリックメニュー内に[新規作成]が表示されない**

→ 接続する仮想PCの環境によっては、デバイスマッピングさせたUSBストレージデバイス上の右クリックメニュー内に[新規作成]が表示されない場合があります。この場合、USBストレージデバイスとは別の場所でファイルまたはフォルダを作成し、USBストレージデバイスにコピーしてください。

［?］**ICAセッション接続直後に、ICAセッション内でキーボード操作/マウス操作ができない**

→ ICAセッション接続直後に、ICAセッション内でキーボード操作/マウス操作ができない場合があります。この場合、セッションウィンドウの[×]ボタンを押してICAセッションを切断し、再接続することで操作可能になる場合があります。

［?］**ICAセッション接続中にネットワーク切断などで切断されたセッションに対して再接続するとキーボード操作が効かない場合がある**

→ ICAセッション接続中にネットワーク切断などで切断されたセッションに対し、再接続するとキーボード操作が効かない場合があります。この場合、セッションウィンドウの[×]ボタンを押してICAセッションを切断し、再接続することで操作可能になる場合があります。

[?] ICAセッション上で、ショートカットキーの一部(Alt+Tab、Windowsキー組み合わせなど)が動作しない

→ ICAセッション上で、ショートカットキーの一部(Alt+Tab、Windowsキー組み合わせなど)が動作しない場合があります。この場合、US300dの[コントロールパネル] → [プログラムと機能]から "Microsoft Lync Vdi 2013" をアンインストールしてください。これにより、本事象が改善されます。

※ Microsoft Lync Vdi 2013 をアンインストールする場合、デフォルトのRAMディスクのサイズではアンインストールに失敗するため、事前に[コントロールパネル] → [Ramdisk]からRAMディスクの サイズを 200MBに増やしてください。
Microsoft Lync Vdi 2013 をアンインストール後は、RAMディスクのサイズを変更前のサイズに戻してください。[Ramdisk]については本書の「4章(5.RAMディスクサイズの設定)」を参照してください。

※ FBWFを無効に設定後に Microsoft Lync Vdi 2013 をアンインストールしてください。アンインストール後はFBWFを有効にしてください。
FBWFについては本書の「2章(3.1File-Based Write Filter (FBWF)ユーティリティーの使用方法)」を参照してください。

[?] RemoteFX USBデバイスリダイレクト機能が動作しない

→ RemoteFX USBデバイスリダイレクト機能を使用する場合は、[コントロールパネル] → [管理ツール] → [サービス]から VMware Horizon View USB サービスを停止して、[スタートアップの種類]を無効に設定してください。VMware Horizon View USB サービスを停止すると、RemoteFX USBデバイスリダイレクト機能は動作しますが、VMware Horizon View USBデバイスアクセス機能は動作しなくなります。

※ RemoteFX USBデバイスリダイレクト機能を動作させるには、次のポリシーが有効に設定されている必要があります。

[管理用テンプレート]
→ [Windows コンポーネント]
→ [リモートデスクトップサービス]
→ [リモートデスクトップ接続のクライアント]
→ [RemoteFX USB デバイスリダイレクト]
→ [サポートされている他の RemoteFX USB デバイスの、このコンピューターからの RDP リダイレクトを許可する]

※ US300d 再起動後も本設定を保持する場合は、FBWF を無効に設定後に本設定を実施してください。本設定完了後は FBWF を有効にしてください。
FBWF については本書の「2 章(3.1File-Based Write Filter (FBWF)ユーティリティーの使用方法)」を参照してください。

2.2 キーボードのトラブル

[?] Num Lock LEDの状態とキーボード動作の同期が取れていない

→ **Num Lock LEDの状態とキーボード動作の同期が取れない場合があります。**
(例：Num Lock LEDは点灯しているが、テンキーで数字が入力できない。)
この場合、仮想PC接続をログオフして、再度ログオンしてください。

[?] キーボードの抜き差しを行うと動作が不安定となる

→ **キーが押されたままでキーボードの抜き差しを行うと動作が不安定となる場合があります。**
キーボードの抜き差しを行う場合は、キーが押されていないことを確認してください。

2.3 プリンタのトラブル

［?］**US300dにプリンタを作成してRDP接続しても仮想PCにプリンタが作成されない**

→ プリンタドライバの日本語版モデル名と英語版モデル名が異なっている場合、US300dからのRDP接続ではプリンタが作成されません。US300dにプリンタを接続する場合、日本語版と英語版のプリンタドライバでモデル名が同じプリンタをご利用ください。

2.4 複数のシンクライアントを組み合わせて使用する場合のトラブル

［?］**PowerPoint や Web ページの画像や動画が表示されない**

→ 仮想PCへの接続をログオフせずに切断状態にして、別のシンクライアントから再接続する場合は、最初の接続と、次の接続の色深度を同じ設定としてください。例えば、最初にUS300dで接続する場合の、接続の色深度が16ビットの場合は、次に接続する別のシンクライアント(例えばUS100、またはWindows XPのRDPクライアント)の接続の色深度も16ビットとしてください。接続の色深度が一致していない場合、後の接続でPowerPointやWebページ等の画像が表示されない場合があります。色深度が違うシンクライアントから接続する可能性がある場合は、各クライアントでの作業を終える場合は、切断ではなく、仮想PCからログオフする運用としてください。特にUS100との共存環境では、US100のRDP接続の色設定に15ビットは使用しないでください。15ビットを使用した場合、動画が表示されない場合があります。

2.5 スリープ時のトラブル

［?］**スリープ時にマウス操作/キーボード操作を行っても復帰しない**

→ マウス/キーボードをUS300dから外した状態でスリープ状態に遷移した場合、その後にUS300dにマウス/キーボードを接続し、マウス操作/キーボード操作を行ってもUS300dはスリープから復帰しません。この場合、端末の電源ボタンを短押しすることでスリープから復帰させてください。

2.6 その他のトラブル

［?］**画面が動かない／動作が遅い等、装置の動作がおかしい**

→ ご使用の状況によっては動作が異常に見えることがあります。
しばらく待って、状態に改善が見られない場合は、再起動してください。
OSの操作ができない場合は、電源ボタンを押したままに（ 5秒以上）し、電源OFFの後、再度電源ボタンを押して起動してください。

3. 移動と保管

US300d を移動・保管するときは保守サービス会社に連絡してください。

⚠警告

US300dを安全にお使いいただくために次の注意事項を必ずお守りください。指示を守らないと、人が死亡する、または重傷を負うおそれがあります。詳しくは「使用上のご注意」をご覧ください。

- **自分で分解・修理・改造はしない**
- **リチウム電池を取り外さない**
- **プラグを差し込んだまま取り扱わない**

⚠注意

US300dを安全にお使いいただくために次の注意事項を必ずお守りください。指示を守らないと、火傷やけがなどを負うおそれや物的損害を負うおそれがあります。詳しくは、「使用上のご注意」をご覧ください。

- **落下注意**

重要

- **フロアのレイアウト変更など大掛かりな作業の場合はお買い上げの販売店または保守サービス会社に連絡してください。**
- **再度、運用する際、内蔵機器や本体を正しく動作させるためにも室温を保てる場所に保管することをお勧めします。**
  装置を保管する場合は、保管環境条件(温度 : -10～55℃、湿度 : 20～80%)を守って保管してください(ただし、結露しないこと)。

1. 本体の電源を OFF(POWER ランプ消灯)にする。
2. 本体に接続している電源コードをコンセントから抜く。
3. 本体に接続しているケーブルをすべて取り外す。
4. 本体に傷がついたり、衝撃や振動を受けたりしないようしっかりと梱包する。

重要

輸送後や保管後、装置を再び運用する場合は、運用の前にシステム時計の確認・調整をしてください。システム時計を調整しても時間の経過と共に著しい遅れや進みが生じる場合は、お買い求めの販売店、または保守サービス会社に保守を依頼してください。本装置、および、内蔵型のオプション機器は、寒い場所から暖かい場所に急に持ち込むと結露が発生し、そのまま使用すると誤動作や故障の原因となります。装置の移動後や保管後、再び運用する場合は、使用環境に十分なじませてからお使いください。

4. ユーザーサポート

アフターサービスをお受けになる前に、保証およびサービスの内容について確認してください。

4.1 保証について

本装置には『保証書』が添付されています。『保証書』は販売店で所定事項を記入してお渡ししますので、記載内容を確認のうえ、大切に保管してください。保証期間中に故障が発生した場合は、『保証書』の記載内容にもとづき無償修理いたします。詳しくは『保証書』およびこの後の「保守サービスについて」をご覧ください。
保証期間後の修理についてはお買い求めの販売店、最寄りの NEC または保守サービス会社に連絡してください。

- **弊社製以外(サードパーティ)の製品、または弊社が認定していない装置やインタフェースケーブルを使用したために起きた装置の故障については、その責任を負いかねますのでご了承ください。**
- **本体のスライドタグおよび側面の銘板に、製品の形式、SERIAL No. (号機番号)、定格、製造業者名、製造国が明記された銘板が貼ってあります。販売店にお問い合わせする際にこの内容をお伝えください。また銘板の号機番号と保証書の保証番号が一致していませんと、保証期間内に故障した場合でも、保証を受けられないことがありますのでご確認ください。万一違う場合は、販売店にご連絡ください。**

4.2 修理に出す前に

「故障かな？」と思ったら、以下の手順を行ってください。

1. 電源コードおよび他の装置と接続しているケーブルが正しく接続されていることを確認します。
2. 本章の「2. トラブルシューティング」を参照してください。該当する症状があれば記載されている処理を行ってください。
3. 本装置を操作するために必要となるソフトウェアが正しくインストールされていることを確認します。
4. 市販のウィルス検出プログラムなどでサーバーをチェックしてみてください。

以上の処理を行ってもなお異常があるときは、無理な操作をせず、お買い求めの販売店、最寄りの NEC または保守サービス会社にご連絡ください。その際にサーバーのランプの表示やディスプレイ装置のアラーム表示もご確認ください。故障時のランプやディスプレイによるアラーム表示は修理の際の有用な情報となることがあります。保守サービス会社の連絡先については、付録 C「保守サービス会社網一覧」をご覧ください。
なお、保証期間中の修理は必ず保証書を添えてお申し込みください。

重要

この装置は日本国内仕様のため、NEC の海外拠点で修理することはできません。ご了承ください。

4.3 修理に出す時は

修理に出される時は次のものを用意してください。

- □ 保証書
- □ ディスプレイ装置に表示されたメッセージのメモ
- □ 障害情報(障害情報は保守サービス会社から指示があったときのみ用意してください。)
- □ 本体・周辺機器の記録

4.4 補修用部品について

本装置の補修用部品の最低保有期間は、製造打ち切り後 5 年です。

4.5 保守サービスについて

保守サービスは NEC の保守サービス会社、および NEC が認定した保守サービス会社によってのみ実施されますので、純正部品の使用はもちろんのこと、技術力においてもご安心の上、ご都合に合わせてご利用いただけます。

なお、お客様が保守サービスをお受けになる際のご相談は、弊社営業担当または代理店で承っておりますのでご利用ください。保守サービスは、お客様に合わせて 2 種類ご用意しています。

保守サービスメニュー

契約保守サービス	お客様の障害コールにより優先的に技術者を派遣し、修理にあたります。この保守方式は、装置に応じた一定料金で保守サービスを実施させていただくもので、お客様との間に維持保守契約を結ばせていただきます。さまざまな保守サービスを用意しています。詳しくはこの後の説明をご覧ください。
未契約修理	お客様の障害コールにより、技術者を派遣し、修理にあたります。保守または修理料金はその都度精算する方式で、作業の内容によって異なります。

NEC では、お客様に合わせてさまざまな契約保守サービスをご用意しています。サービスの詳細については、「NEC コーポレートサイト(http://www.nec.co.jp/)」の「サポート情報」をご覧ください。

重要

- **サービスを受けるためには事前の契約が必要です。**
- **サービス料金は契約する日数/時間帯により異なります。**

4.6 情報サービスについて

本製品に関するご質問・ご相談は「ファーストコンタクトセンター」でお受けしています。
※　電話番号のかけまちがいが増えております。番号をよくお確かめの上、おかけください。

ファーストコンタクトセンター
TEL. 03-3455-5800(代表)
受付時間／9:00～12:00、13:00～17:00　月曜日～金曜日(祝祭日を除く)

お客様の装置本体を監視し、障害が発生した際に保守拠点からお客様に連絡する「エクスプレス通報サービス」の申し込みに関するご質問・ご相談は「エクスプレス受付センター」でお受けしています。
※　電話番号のかけまちがいが増えております。番号をよくお確かめの上、おかけください。

エクスプレス受付センター
TEL. 0120-22-3042
受付時間／9:00～17:00　月曜日～金曜日(祝祭日を除く)

インターネットでも情報を提供しています。

http://www.nec.co.jp/
NEC コーポレートサイト：製品情報、Q&A など最新 Express 情報満載！

http://club.express.nec.co.jp/
『Club Express』：『Club Express 会員』への登録をご案内しています。Express5800 シリーズをご利用になる上で役立つ情報サービスの詳細をご紹介しています。

http://www.fielding.co.jp/
NEC フィールディング(株)ホームページ：メンテナンス、ソリューション、用品、施設工事などの情報をご紹介しています。

NEC Express5800 シリーズ
US300d

10 付　録

付録 A　　無線 LAN 仕様一覧

無線 LAN の仕様について説明しています。

付録 B　　仕　様

本製品の仕様を記載しています。

付録 C　　保守サービス会社一覧

保守サービス会社の連絡先などを掲載しています。

付録 A　無線 LAN 仕様一覧

IEEE802.11a

項　目	規　格
準拠規格	IEEE802.11a
通信モード	54/48/36/24/18/12/9/6 (Mbps モード) *1
変調方式	OFDM 方式
無線チャンネル	36ch、40ch、44ch、48ch、52ch、56ch、60ch、64ch、100ch、104ch、108ch、112ch、116ch、120ch、124ch、128ch、132ch、136ch、140ch (パッシブスキャン) *2
周波数帯域	5GHz 帯域 (5.15～5.35GHz、5.47～5.725GHz) *3

*1：各規格による理論的な通信速度をもとにした通信モード表記であり、実効速度とは異なります。接続対象機器、電波環境、周囲の障害物、設置環境、使用状況、ご使用の OS、アプリケーション、ソフトウェアなどによっても通信速度、通信距離に影響する場合があります。

*2：パッシブスキャンのチャンネルは接続に時間がかかる場合があります。

*3：36ch、40ch、44ch、48ch、52ch、56ch、60ch、64ch を利用した無線 LAN の使用は、電波法令により屋内に限定されます。

IEEE802.11b/g

項　目	規　格
準拠規格	IEEE802.11b、IEEE802.11g
通信モード	IEEE802.11b モード：11/5.5/2/1 (Mbps モード) *1 IEEE802.11g モード：54/48/36/24/12/9/6 (Mbps モード) *1
無線チャンネル	1～11ch
周波数帯域	2.4GHz 帯域(2.4～2.462GHz)

*1：各規格による理論的な通信速度をもとにした通信モード表記であり、実効速度とは異なります。接続対象機器、電波環境、周囲の障害物、設置環境、使用状況、ご使用のＯＳ、アプリケーション、ソフトウェアなどによっても通信速度、通信距離に影響する場合があります。

IEEE802.11n

項　目	規　格
準拠規格	IEEE802.11n
通信モード （送信時）	20MHz 時：65/58.5/52/39/26/19.5/13/6.5 (Mbps モード) 20MHz、short GI 有効時：72.22/65/57.78/43.33/28.89/21.67/14.44/7.22 (Mbps モード) 40MHz 時：135/121.5/108/81/54/40.5/27/13.5 (Mbps モード) 40MHz、short GI 有効時：150/135/120/90/60/45/30/15 (Mbps モード) *2
通信モード （受信時）	20MHz 時：130/117/104/78/52/39/26/13 (Mbps モード) 20MHz、short GI 有効時：144.44/130/115.56/86.67/57.78/43.33/28.89/14.44 (Mbps モード) 40MHz 時：270/243/216/162/108/81/54/27 (Mbps モード) 40MHz、short GI 有効時：300/270/240/180/120/90/60/30 (Mbps モード) *2
変調方式	OFDM 方式、MIMO 方式
無線チャンネル	1～11ch (アクティブスキャン) 12ch、13ch (パッシブスキャン) *3 36ch、40ch、44ch、48ch、52ch、56ch、60ch、64ch、100ch、104ch、108ch、112ch、116ch、120ch、124ch、128ch、132ch、136ch、140ch (パッシブスキャン) *3 *4
周波数帯域	2.4GHz 帯域 (2.4～2.4835GHz) 5GHz 帯域 (5.15～5.35GHz、5.47～5.725GHz) *3

*1：「IEEE802.11n Draft2.0 準拠」の表記は、他の IEEE802.11n Draft 対応製品との接続性を保証するものではありません。

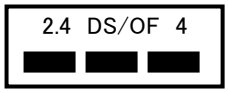
*2：各規格による理論的な通信速度をもとにした通信モード表記であり、実効速度とは異なります。接続対象機器、電波環境、周囲の障害物、設置環境、使用状況、ご使用の OS、アプリケーション、ソフトウェアなどによっても通信速度、通信距離に影響する場合があります。

*3：パッシブスキャンのチャンネルは接続に時間がかかる場合があります。

*4：36ch、40ch、44ch、48ch、52ch、56ch、60ch、64ch を利用した無線 LAN の使用は、電波法令により屋内に限定されます。

本製品は、技術基準適合証明を受けています。
IEEE802.11n(2.4GHz)、IEEE802.11b、IEEE802.11g 通信利用時は、2.4GHz 帯域の電波を使用しており、この周波数帯では、電子レンジ等の産業・科学・医療用機器のほか工場の製造ライン等で使用されている移動体識別用の構内無線局(免許を要する無線局)及び特定小電力無線局(免許を要しない無線局)並びにアマチュア無線局(免許を要する無線局)が運用されています。

IEEE802.11n(2.4GHz)、IEEE802.11b、IEEE802.11g 通信利用時は、2.4GHz 全帯域を使用する無線設備であり、移動体識別装置の帯域（2.427GHz～2.47075GHz）が回避可能です。変調方式として DS-SS 方式および、OFDM 方式を採用しており、与干渉距離は 40m です。



2.4　　：2.4GHz 帯を使用する無線機器を示す
DS/OF ：DS-SS 方式および OFDM 方式を示す
4　　：想定される干渉距離が 40m 以下であることを示す
■■■ ：全帯域を使用し、かつ移動体識別装置の帯域を回避可能であることを意味する

IEEE802.11a、IEEE802.11n(5GHz) 通信利用時は、5GHz 帯域（5.15GHz～5.35GHz、5.47GHz～5.725GHz）を使用しており、以下のチャンネルに対応しています。
W52：Ch36（5180MHz）,Ch40（5200MHz）,Ch44（5220MHz）,Ch48（5240MHz）
W53：Ch52（5260MHz）,Ch56（5280MHz）,Ch60（5300MHz）,Ch64（5320MHz）
W56：Ch100（5500MHz）,Ch104（5520MHz）,Ch108（5540MHz）,Ch112（5560MHz）,Ch116（5580MHz）,Ch120（5600MHz）,Ch124（5620MHz）,Ch128（5640MHz）,Ch132（5660MHz）,Ch136（5680MHz）,Ch140（5700MHz）
IEEE802.11a/n（W52、W53）無線 LAN の使用は、電波法令により屋内に限定されます。

1. この機器を使用する前に、近くで移動体識別用の構内無線局及び特定小電力無線局並びにアマチュア無線局が運用されていないことを確認して下さい。
2. 万一、この機器から移動体識別用の構内無線局に対して有害な電波干渉の事例が発生した場合には、速やかに使用周波数を変更するか又は電波の発射を停止した上、下記連絡先にご連絡頂き、混信回避のための処置等（例えば、パーティションの設置など）についてご相談して下さい。
3. その他、この機器から移動体識別用の特定小電力無線局あるいはアマチュア無線局に対して有害な電波干渉の事例が発生した場合など何かお困りのことが起きたときは、次の連絡先へお問い合わせ下さい。

連絡先:ファーストコンタクトセンター

TEL:03-3455-5800 （代表）
受付時間:9:00～12:00　13:00～17:00 月曜日～金曜日(祝日を除く)

※　番号をお間違えにならないようお確かめのうえご連絡ください。

付録 B　仕　様

項　目	仕　様
プロセッサ	AMD G シリーズ T48E 1.4 GHz デュアルコアプロセッサ （AMD Radeon™ HD 6250 グラフィックス搭載）
メモリ	16GB フラッシュ/2 GB DDR3 RAM
I/O 周辺機器サポート	DisplayPort x 1 （DisplayPort-DVI-I 変換コネクタ（オプション）を使用可能） DVI-I ポート x 1 （DVI-VGA（DB-15）アダプタ付属） 外部 USB 2.0 ポート x 4（前面 x 2、背面 x 2）
ネットワーク	10/100/1000Base-T ギガビットイーサネット（RJ45 コネクタ） 無線 LAN（シングル/デュアルバンド 802.11 a/b/g/n 内蔵ワイヤレス(無線 LAN モデルのみ)
ディスプレイ	VESA モニタサポート（Display Data Channel（DDC）による解像度およびリフレッシュレートの自動設定が可能） DisplayPort: 2,560 x 1,600（32 bpp の場合） DVI-I: 1,920 x 1,200（32 bpp の場合） デュアルディスプレイ: 1,920 x 1,200（32 bpp の場合）
オーディオ	コンポジットオーディオジャック: 1/8 インチミニ、16 ビットステレオ、 内蔵モノラルスピーカー
デバイスセキュリティ	デバイスセキュリティ Kensington セキュリティスロット標準搭載 (ケーブル別売）
物理的特性	高さ：170mm(6.7 インチ) 幅：40mm(1.6 インチ) 奥行：185mm(7.3 インチ) 重量：0.93 kg
電源	100V AC（各国共通、自動検出）、50/60 Hz、65 W、19 V DC ENERGY STAR 5.0 V 相外部/EuP 準拠電源アダプタ キーボード x 1、マウス x 1、モニタ x 1 が接続されている場合の平均消費電力: 9 ワット未満
温度範囲	動作時: 10～35 ℃ 保管時: -10～55 ℃
湿度	動作時 : 20～80 % 保管時 : 10～95 %（結露なきこと）
添付品	USB キーボード（日本語 109A キーボード） 光学式マウス（PS/2 インタフェースの場合は USB キーボード裏面に接続） AC アダプタ、電源コード、DVI-VGA 変換コネクタ、縦置き用スタンド、無線 LAN アンテナ（無線 LAN モデルのみ）
安全性認証	German EKI-ITB 2000、ISO 9241-3/-8 cULus 60950、TUV-GS、EN 60950 FCC Class B、CE、VCCI、C-Tick WEEE、RoHS 準拠

付録 C　保守サービス会社一覧

本製品、および関連製品のアフターサービスは、お買い上げの NEC 販売店、最寄りの NEC、または NEC フィールディング株式会社までお問い合わせください。
次の WEB サイトにも最新の情報が記載されています。

http://www.fielding.co.jp/

このほか、弊社販売店のサービス網がございます。お買い上げの販売店にお問い合わせください。

トラブル等についてのご連絡は、下記の電話番号へおかけください(電話番号のおかけ間違いにご注意ください)。なお、保守契約をされている装置のトラブルにつきましては、契約時にお知らせする契約専用電話(年中無休 24 時間受付)へおかけください。

【IT 機器の修理窓口】
修理受付センター(全国共通)　　0120-536-111 (フリーダイヤル)
携帯電話をご利用のお客様　　0570-064-211 (通話料お客さま負担)
(受付時間：月曜日から金曜日 AM9:00～PM6:00　土曜日、日曜日、祝祭日および当社規定の休日を除く)

US300d
ユーザーズガイド

2018 年　6 月　第 8 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）

<本装置の利用目的について>

本製品は、高速処理が可能であるため、高性能コンピュータの平和的利用に関する日本政府の指導対象になっております。

ご使用に際しましては、下記の点につきご注意いただけますよう、よろしくお願いいたします。

1. 本製品は不法侵入、盗難等の危険がない場所に設置してください。
2. パスワード等により適切なアクセス管理をお願いいたします。
3. 大量破壊兵器およびミサイルの開発、ならびに製造等に関わる不正なアクセスが行われるおそれがある場合には、事前に弊社相談窓口までご連絡ください。
4. 不正使用が発覚した場合には、速やかに弊社相談窓口までご連絡ください。

   弊社相談窓口　ファーストコンタクトセンター

   電話番号　03-3455-5800

この装置は、クラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをして下さい。　　VCCI－B

高調波適合品

高調波電流規格 JIS C 61000-3-2適合品

回線への接続について

本体を公衆回線や専用線に接続する場合は、本体に直接接続せず、技術基準に適合し認定されたボードまたはモデム等の通信端末機器を介して使用してください。

電源の瞬時電圧低下対策について

この装置は、落雷等による電源の瞬時電圧低下に対し不都合が生じることがあります。電源の瞬時電圧低下対策としては、交流無停電電源装置（UPS）等を使用されることをお勧めします。

レーザ安全基準について

この装置にオプションで接続される光学ドライブは、レーザに関する安全基準（JIS C-6802、IEC 60825-1）クラス1に適合しています。

日本国外でのご使用について

この装置は、日本国内での使用を前提としているため、海外各国での安全規格等の適用を受けておりません。したがって、この装置を輸出した場合に当該国での輸入通関および使用に対し罰金、事故による補償等の問題が発生することがあっても、弊社は直接・間接を問わず一切の責任を免除させていただきます。