WYSE TECHNOLOGY INC.

WDMセキュリティガイドライン

ホワイトペーパー

v1.0

2012/12/10

本文書は、Wyseクラウドクライアントおよびゼロクライアントを安全に管理するためのWyse Device Manager (WDM)の設定について詳しく説明します。また、安全な管理のためのWDMおよびWyse シンクライアント端末の設定に関する一般的なガイドラインと具体的な手順を説明します。

目次

1.	はじめに	2
2.	適用範囲	2
3.	参照資料	2
4.	WDMアーキテクチャ	3
5.	セキュリティガイドラインの概要	4
6.	詳細なセキュリティガイドライン	4
6.	1. セキュアモード (HTTPS) の有効化	4
6.	2. 非セキュアなコンポーネントおよびサービスの無効化	4
	6.2.1. FTP リポジトリの無効化	4
	6.2.2. HTTP リポジトリの無効化	5
	6.2.3. TFTP サーバー/サービス	5
6.	3. WDMのデフォルトパスワードおよびデフォルト設定の変更	5
	6.3.1. $SQL = - \beta - \sqrt{-\beta} - \beta $	5
	6.3.2. <i>ソフトウェアリポジトリ</i>	5
	6.3.3. 通信に使用されるポート	5
	6.3.4. ファイアウォール設定	6
	インストール時	6
	インストール後	6
6.	4. デフォルトの端末設定の変更	9
	6.4.1. Write-Filter	9
	6.4.2. リモートシャドウイング (VNC)	9
	6.4.3. BIOS およびユーザーのパスワード	
	6.4.4. ドメイン参加	
	6.4.5. PXEイメージング	
6.	5. Wyse端末での最新のファームウェアおよびソフトウェアの使用	
6	6. Active Directoryの統合および委任	
6	7. ネットワークの設定	
付録	A – 項目のチェックリスト	
付録	表B – IISでのセキュリティモード(HTTPS)の有効化	14

WDMセキュリティガイドライン

1. はじめに

本文書は、Wyseクラウドクライアントおよびゼロクライアントを安全に管理するためのWyse Device Manager (WDM)の設定について詳しく説明します。また、安全な管理のためのWDMおよびWyseシン クライアント端末の設定に関する一般的なガイドラインと具体的な手順を説明します。ご使用の端末が承認されたWDMサーバーによってのみ管理されるよう、本文書に記述された設定を有効にすることをお勧めします。

2. 適用範囲

本文書のガイドラインおよび推奨事項はWDMバージョン4.9向けのものですが、現在サポートされている WDMの旧バージョンにも適用できます。一部の設定手順は、WDMがインストールされている特定のオペ レーティングシステム (OS) に関連しています。本文書では、WDM 4.9をインストールするOSとして Windows Server 2008 R2を使用します。サポートされるその他すべてのOSにも同様の設定を適用できます。 本文書中の「端末」はクラウドクライアント(「シンクライアント」や「ゼロクライアント」とも呼ばれ る)を指します。また、「エージェント」はWDMエージェント(「HAgent」とも呼ばれる)を指します。

一般的な推奨事項:

- Wyseサポートサイトから入手可能な最新のWDMバージョン(適用可能なホットフィックスを含む)、OSおよびファームウェアのバージョンおよびHAagentを使用してください。
- WDMの導入前に本文書を最後までお読みください。デフォルト以外のパスワードの使用などの セキュリティ設定の中には、インストール前またはインストール時に設定した方が簡単なものが あります。また、ポートやパスワードにデフォルト以外の設定を選ぶ場合は、インストール時に [Custom]オプションを使用することをお勧めします。

3. 参照資料

0

本文書に加えて、次の資料を参照できます。

- 資料
 - WDM
 - WDM Installation Guide
 - WDM Administrators Guide
 - Wyse enhanced SUSE Linux INI Reference Guide
 - Wyse enhanced Ubuntu Linux INI Reference Guide
 - ThinOS INI Reference Guide
 - Windows Embedded Administrators Guide
- WDMのコモンクライテリア認証レポート
 - o <u>www.commoncriteriaportal.org/files/epfiles/Wyse CR.pdf</u>
 - o <u>www.commoncriteriaportal.org/files/epfiles/Wyse ST.pdf</u>
 - o <u>www.commoncriteriaportal.org/</u>

- Wyseソフトウェアのダウンロード
 - 。 <u>www.wyse.com</u>> [Support] > [Downloads] をクリックして製品を選択してください
 - o <u>https://appservices.wyse.com/pages/serviceandsupport/support/downloads.asp</u>

4. WDMアーキテクチャ

WDM Enterpriseは、主要コンポーネントを別々のサーバーにインストールすることで、パフォーマンス と拡張性の向上および帯域幅の最適化を図る分散アーキテクチャを提供しています。すべてのコンポーネ ントを単一のサーバーにインストールすることも可能です。WDM Workgroupでは、すべてのコンポー ネントが単一のサーバーにインストールされます。Workgroup機能とEnterprise機能の比較についての 詳細は、<u>http://www.wyse.com/products/software/management/WDM</u>を参照してください。



Wyse Cloud Clients

図 1: WDM Enterprise アーキテクチャ

5. セキュリティガイドラインの概要

ご使用のWyse端末を安全に管理するためのセキュリティガイドラインは以下の通りです。

- 1. セキュアモード (HTTPS) の有効化
- 2. 非セキュアなコンポーネントおよびサービスの無効化
- 3. WDMのデフォルトパスワードおよびデフォルト設定の変更
- 4. デフォルトの端末設定の変更
- 5. Wyse端末上での最新のファームウェアおよびソフトウェアの使用
- 6. Active Directoryの統合および委任の使用
- 7. ネットワークの設定

6. 詳細なセキュリティガイドライン

本セクションでは、WDMのセキュリティ機能と、前セクションに挙げた各項目の詳細な設定手順を説明 します。

6.1. セキュアモード (HTTPS) の有効化

WDMはシンクライアント端末管理にあたり、「非セキュア(HTTP)」と「セキュア(HTTPS)」とい う2つのプロトコルを使用できます。WDMのインストール時のデフォルトは非セキュアモード (HTTP)を使用するようになっていますが、インストール後にHTTPSを有効にすることも可能です。 本セクションでは、HTTPSを使用するためのWDM、IISおよびエージェントの設定手順を説明します。

セキュアモード(HTTPS)を設定するための手順

- 1. HTTPSを使用するようにIISを設定します 詳細な手順は「付録B-IISでのセキュアモード(HTTPS)の有効化」を参照してください。
- 2. WDMでHTTPSおよびCA認証を有効にします
 - a) [WyseDeviceManager] GUI を開きます
 - b) [Configuration Manager] > [Software Repositories]を選択し、リポジトリをダブルクリックします
 - c) [Secure (HTTPS)]を有効にします
 - d) [CA Validation]を有効にします
- 証明書を端末にインポートします ルート証明書/CA認証局のパブリック証明書を端末にインポートする方法については、「WDM Administrators Guide」を参照してください。WTOS、SUSE LinuxおよびUbuntu Linux OSを 搭載した端末については、INIファイルを通じて証明書をインポートする別の方法があります。

6.2. 非セキュアなコンポーネントおよびサービスの無効化

安全な管理環境を維持するには、次のサービスおよび機能を無効にする必要があります。

6.2.1. FTPリポジトリの無効化¹

a) [WyseDeviceManager] GUIを開きます

¹ PCoIP端末 (Pクラス) は、FTPを使ったファームウェアパッケージの配信のみをサポートしています。FTPリポジ トリを無効にすると、ファームウェアパッケージの配信によるアップデートができなくなります。

- b) [Configuration Manager] > [Software Repositories] を選択し、リポジトリをダブルクリック します
- c) [Transfer Type] ドロップダウンを[HTTP]に設定します

6.2.2. HTTPリポジトリの無効化

「付録B – IISでのセキュアモード(HTTPS)の有効化」の手順を実行してHTTPSを有効にして から、次の手順を実行してIISでHTTP通信を無効にします。

- a) [スタート]を ク リ ッ ク し 、 [プログラムとファイルの検索]テキストボックスに「inetmgr」 と入力して[インターネットインフォメーションサービス(IIS)マネージャー]を開きます
- b) [サイト] > [Rapport HTTP Server] > [Rapport HTTP Server] を選択し、右端のペインの[バインド...]をクリックして[サイトバインド]ページを開きます
- c) [サイトバインド]ページで、httpの行をクリックします
- d) [削除]および[閉じる]をクリックします

6.2.3. TFTPサーバー/サービス

WDMサーバーで以下を実行します。

- a) [スタート] > [すべてのプログラム] > [管理ツール] > [サービス]を押します
- b) [WDM TFTP]を見つけます
- c) ダブルクリックして[停止]を選択します
- d) [スタートアップの種類]を[無効]に設定します
- e) [OK]を押します

6.3. WDMのデフォルトパスワードおよびデフォルト設定の変更

WDMのインストール時、インストーラは、WDMで使用される多くのコンポーネントにデフォルトのパ スワードと設定を選択します。インストール後にデフォルト以外の値を設定できるものもありますが、イ ンストール時に設定しなければならないものもあります。

WDMインストーラで使用されるデフォルト設定は次の通りです。

6.3.1. SQLデータベースパスワード

WDMは、「sa」ユーザーの特権で「rapportdb」というSQL Serverインスタンスを使用します。 デフォルト以外のパスワードを指定する方法については、以下の「インストール時」セクション を参照してください。

6.3.2. ソフトウェアリポジトリ

WDM は、FTP、HTTPまたはHTTPSベースのソフトウェアリポジトリ(パスワード(WDMの マスターソフトウェアリポジトリと、1つ以上のリモートソフトウェアリポジトリ))の使用を サポートしています。デフォルト以外のパスワードを設定する方法については、以下の「インス トール時」および「インストール後」を参照してください。

6.3.3. 通信に使用されるポート

WDMは、WDMコンポーネントおよびHAgentとの通信にさまざまなポートを使用します。これ らのポートのリストは「Installation Guide」を参照してください。次のコンポーネントには、 標準以外(デフォルト以外)のポートを使用することをお勧めします。

- 。 WDM SQLデータベース: SQL Serverが使用するデフォルトのTCPポート1433
- WDM HTTPおよびHTTPSポート

6.3.4. ファイアウォール設定

WDMでは、WDMコンポーネントがインストールされたコンピュータのファイアウォール規則 から特定のポートを除外する必要があります。使用するサービスおよび機能のみを有効にしてく ださい(例外を追加してください)。

例えば、P20などのPCoIP端末がない場合は、ThreadX Manager Serviceが使用するTCPポート 9880および50,000の例外を追加する必要はありません。

本セクションの以降の部分では、WDMのインストール時またはインストール後にデフォルト設定を変更 するために使用できる具体的な手順を説明します。

インストール時

a. データベース設定

SQL Serverデータベースでデフォルト以外の設定をする場合は、インストール後よりも インストール時に行う方が簡単です。

SQL Serverパスワード

WDMインストーラは、ユーザー「sa」のために組み込みデータベース(インスタン ス名:RAPPORTDB)としてMicrosoft SQL Expressを含んでいます。インストー ルを[Typical]で実行すると、デフォルトパスワードが使用されます。[Custom]イン ストールでも、このパスワードを選択できます。また[Custom]インストールでは、 組み込みデータベースではなく、既存の(WDMの旧バージョンにインストールされ た)データベースや別のデータベース(SQL Serverのフルバージョンなど)を使用 できます。

SQL Server通信ポート

WDMは、SQL Serverデータベースとの通信に、デフォルトのTCPポート1433を使 用します。このポートは、[Custom]インストールを選択して設定できます。

b. ソフトウェアリポジトリパスワード

WDMエージェントは、[rapport]というユーザー名を使用して、WDMリポジトリに接続 します。[rapport]ユーザーのパスワードはデフォルト以外に変更することをお勧めしま す。[Typical]でインストールを実行するとデフォルトパスワードが使用されます。 [Custom]インストール時にもこのパスワードを選ぶことができます。

c. ファイアウォール設定

WDM 4.9以降、管理者がインストール時にPrerequisitesユーティリティを使用して、デフォルトのファイアウォールポートを設定できるようになりました。デフォルト以外の ポートを設定したい場合や、WDMの旧バージョンを使用している場合は、このユー ティリティのFirewall Settingsコンポーネントを実行せず、例外ファイアウォールを手 動で設定することをお勧めします。

インストール後

• 通信に使用するポート

WDMが使用するポートは、次のように設定できます。

• IIS

WDMは、端末との通信にインターネットインフォメーションサービス(IIS) のWebサーバーを使用します。WDMがインストールされたサーバーのIIS設定 で、次の変更を行う必要があります。

- WebサーバーHTTP(非セキュア)ポート:デフォルトのTCPポート80
- WebサーバーHTTPS (セキュア) ポート:デフォルトのTCPポート443

- 1. [スタート]をクリックし、[プログラムとファイルの検索]テキス トボックスに「inetmgr」と入力してIISマネージャーを開きま す
- [サイト] > [Rapport HTTP Server] > [Rapport HTTP Server]
 を選択し、右端のペインにある[バインド...]をクリックして[サ イトバインド]ページを開きます
- [サイトバインド]ページで、httpまたはhttpsの行をクリックします
- 4. [編集]をクリックして、[ポート]に新しい値を指定します
- 5. [OK]をクリックしてから、[閉じる]をクリックします
- 6. 設定を有効にするためにIISサーバーを再起動します
 - IISマネージャーの[Rapport HTTP Server]ページに移 動します
 - 右側パネルの[Webサイトの管理]で[再起動]をクリック します

注:変更後にWDMの [Preferences]ダイアログを開き、WDMで新 しい設定が反映されているかどうか確認してください。

- ソフトウェアリポジトリパスワード
 - 1. WDMがインストールされたWindowsサーバーで[コントロール パネル]を開 きます
 - 2. [ユーザーアカウント]に移動します
 - 3. ユーザー[rapport]のパスワードを変更します
 - 4. [WyseDeviceManager] GUIを開きます
 - 5. [Configuration Manager] > [Software Repositories] を選択します
 - 6. リポジトリをダブルクリックし、[HTTP]セクションの[Password]テキストボ ックスと[Verification]テキストボックスに、rapportユーザーの変更後の新し いパスワードを入力します
- SQL Server通信ポート

SQLポートを変更する(デフォルトの1433以外にする)には、次の手順を実行 します。

- データベースサーバー
 - [スタート]を押して、[Microsoft SQL Server] >[Configuration Tools]を選択します
 - 2. [SQL Server Configuration Manager]を開きます
 - 3. [SQL Server ネットワーク構成] > [RAPPORTDBのプロトコル] を選択します
 - 4. 右側ペインで[TCP/IP]をダブルクリックします
 - 5. [IP アドレス]タブで、データベースマシンに対応するIPアドレ スの[TCP ポート]値を設定します
 - 6. WDMマシンを再起動します
- 管理GUIおよびソフトウェアリポジトリを含むWDMコンポーネントを 実行するすべてのコンピュータ(分散インストールの場合)
 - 1. [レジストリーエディター]を開きます([スタート] > [プログラ ムとファイルの検索]フィールドに「regedit」と入力)
 - 2. [Software] > [Wow6432Node] > [Rapport] > [Database] /

- ードを選択します
- 3. [DBPort]の値をSQL Serverの設定と同じ値に設定します
- 4. [WyseDeviceManager] GUIを再起動します

WDM Preferences :

- [WyseDeviceManager] GUIを開きます
- [Configuration Manager] > [Preferences]を選択します
- [Service Preferences]をダブルクリックし、[Serv/Port Settings]を選択 します

6.4. デフォルトの端末設定の変更

シンクライアント端末上で端末設定を安全に管理するには、攻撃の脆弱性を軽減する設定も必要です 。本セクションでは、管理の必要があるさまざまな設定の概要を示します。設定方法の一部について は特に詳しく説明します。詳細(リモート送信可能なINI設定など)については、各プラットフォーム の管理者ガイドを参照してください。内容は以下の通りです。

1. Write-Filter

- 2. リモートシャドウイング (VNC)
- 3. BIOSおよびユーザーのパスワード
- 4. ドメイン参加
- 5. PXEイメージング

6.4.1. Write-Filter

WyseのWindows Embedded製品には「File Based Write Filter (FBWF)」という保護機構が組み込まれ ており、デフォルトで有効になっています。Write-Filterが有効になっている場合(システムトレイの緑 のボタンがオンの状態)、端末に対して行われた変更は再起動後は保持されず失われます。Write-Filter を有効または無効にできるのは管理者だけです。

Write-Filterを有効にしておくことをお勧めします。WDMは、Windows Embedded端末に対するアップ デートの実行時に、Write-Filterをリモートから自動的に有効/無効にします。

6.4.2. リモートシャドウイング (VNC)

Wyse端末(P20を除く)には、WDM管理者がユーザー端末の画面状態をWDM管理GUIから表示できる リモートシャドウイング用のVNCサーバーが組み込まれています。これにより、管理者およびデスク ユーザーは、端末ユーザーのいる場所やデスクまで出向くことなく、実際的な技術サポートを提供できる ようになります。

VCNクライアントはWDMサーバー上にあります。リモートシャドウ機能はVCNプロトコルを使用しま す。デフォルトでリモートシャドウセッションが確立されると、WDM管理者はセッションを開始するた めにパスワードを入力する必要があり、端末ユーザーに通知が行われます。端末ユーザーはリモートシャ ドウの要求を拒否することができます。リモートシャドウセッションが確立されると、ユーザーの承認後 あるいはタイムアウト後に、システムトレイのアイコンがアクティブセッションでの端末ユーザー情報を 提供します。 以下は、リモートシャドウをより安全にするためのオプションです。

- 端末からVNCクライアントを削除する(WESおよびLinux端末の場合)
- VNCクライアントを無効にし、デバッグ時のみ明示的に有効にする
- リモートシャドウイングのため、VNCが使用するデフォルトパスワードを変更する
- デフォルトのVNCクライアント(WDM内)およびVNCサーバー(端末上)を安全性の高いサードパーティ製バージョンに置き換えることで、暗号化とロギングを可能にする
- リモートシャドウの要求を受信した時点で、VNCサーバー(端末上)のデフォルト動作を設定する
- 既知のソースまたは承認されたソース(WDMサーバーなど)からの接続のみを受け入れるよう、VNCサーバー(端末上)を設定する

6.4.3. BIOSおよびユーザーのパスワード

Wyse端末は、ローカルユーザーおよびローカル管理者に対してパスワードを使用します。無許可ユー ザーが端末を使用したり、特権レベルを引き上げて悪用したりすることがないよう、これらの値を変更す る必要があります。

個々の端末上でこれらの設定を行うための手順については、プラットフォーム/OSに固有の管理者ガイ ドを参照してください。また、これらの設定を特定の1台の端末に対し設定し、Wyse USB Firmware Toolを使用してOSまたはファームウェアを吸い上げて(コピー/プルして)から、WDMを通じてすべての 端末に適用することもできます。

変更する必要がある設定およびパスワードを以下に示します。

1. BIOS設定

WTOS、Windows Embedded、またはWyse enhanced SUSE Linuxオペレーティングシステムを搭載した端末が該当します。これらのオペレーティングシステムを搭載した製品は、BIOS設定(ブートデバイス、ブートオーダー設定を含む)を保護するローカルBIOSパスワードを持っています。

レベル	Windows Embedded	Wyse enhanced SUSE Linux	Wyse enhanced Ubuntu Linux (ARMベースの T50)	WTOS (ARMベース のT10 ² を除く)
端末ごと (端末での直接 操作)	ブート時に[Del] キーを押してBIOS メニューを表示す る	ブート時に[Del] キーを押してBIOS メニューを表示す る	ブート時に電源ボ タンと[Del]キー ³ を 押す	ブート時に電源ボタ ンと[Del]キー ³ を押す
WDM経由	変更済みのOSと BIOS を、WDMを 通じて配信する	変更済みのOS、 BIOSおよびINI設定 を、WDMを通じて 配信する	変更済みのOS、 BIOSおよびINI設定 を、WDMを通じて 配信する	変更済みのOS、BIOS およびINI設定を、 WDMを通じて配信す る

表1:Wyse端末上のBIOSまたはブートメニューのオプション

² ARMベースのWTOSプラットフォーム (T10) には、ローカルブートまたはBIOSオプションがありません。すべての 関連する設定は、リモート配信されるINIファイルでのみ設定できます。

³ ブート時に2つのオプションがあります。電源ボタン+[P]キーを押すとブートオーダーを選択でき、電源ボタン+ [Del] キーを押すとBIOSメニューへ入るためのパスワード入力ダイアログが表示されます。

各プラットフォームにはプラットフォーム固有の設定があり、以下が制御可能です。

- BIOSパスワード
- ブート順序
- USBメモリからブート
- 2. ローカルユーザーおよび管理ユーザーのパスワード これは、WTOSおよびPCoIP端末(P20など)を含むすべてのWyse端末が該当します。

オペレーティングシステム/ プラットフォーム	ローカルユーザー	ローカル管理者
Windows Embedded	User	Administrator
Wyse enhanced SUSE Linux	Thinuser	Admin
Wyse enhanced Ubuntu	Thinuser guest	Admin
Linux WTOS	<なし>	Admin ⁴
PCoIP (P20)	<なし>	<admin パスワードを設定可能=""></admin>

表2:Wyse端末上のユーザーおよび管理者のアカウント

6.4.4. ドメイン参加

Windows Embedded端末は、会社のActive Directory (AD) ドメインに参加することもでき、端末ユ ーザーがADベースの認証情報を使用してログインするように構成できます。これによりセキュリティ の階層が追加され、通常のADベースのツールによるモニタリングが可能になります。

6.4.5. PXEイメージング

x86ベースのプラットフォーム上で実行されているWyse端末のイメージは、PXEプロトコルを使用して 吸い上げることができます。WDMには、PXEベースのイメージングを提供するためのTFTPサーバーが 組み込まれています。WDMは、PXE以外またはその他の方法によるOS/ファームウェアのアップデー ト(INIベース)をサポートしています。

PXEイメージングの必要がない場合は、端末からのPXE要求に応答するWDMサーバー上のTFTPサービスを無効にすることもお勧めします。端末上のBIOS設定のブートオーダーでPXEの優先度を低く設定するか、またはPXEサポートを無効にすることをお勧めします。これは通常、端末のキッティング時に変更する必要があります。

6.5. Wyse端末での最新のファームウェアおよびソフトウェアの使用

Wyse製品部門は、端末上で実行されるソフトウェアを定期的にアップデートします。これらのソフト ウェアアップデートは、Webサイトの[Support] > [Downloads]セクションで公開されています。アップ デートには、以下のカテゴリがあります。

- WDMエージェント (HAgent)
- OSまたはファームウェアのアップデート
- サードパーティコンポーネント (Citrix Receiver、VMware View Clientなど)のソフトウェア アップデート

⁴ WDMが配布するINI設定ファイルを通じて設定できます。

6.6. Active Directoryの統合および委任

WDM(およびそのコンポーネント)がインストールされているコンピュータへのアクセスについては、 通常のWindows認証情報を通じて管理することをお勧めします。WDM管理GUIへのアクセスは必要に応 じて提供し、WDMコンピュータへのアクセスを許可されたユーザーごとに、WDM管理GUIのための特 権を割り当てる必要があります。

WDMは、Active Directoryドメインにすでに参加しているコンピュータにインストールすることができ ます。追加の管理者については、WDM管理GUIのみをインストールしたコンピュータにアクセスを限定 する必要があります。

Active Directoryおよび委任の設定は、以下のように管理できます。

- [WyseDeviceManager] GUIを開きます
- [Configuration Manager] > [User Permissions] ノード(左側ペイン)を選択します
- 右クリックして[新規作成] > [User/Group]を選択します
- ローカルマシンのドメインまたはADドメインからユーザーを追加します
- 端末を管理するための以下のような特権を割り当てます
 - o 端末固有:リモートシャドウ、リアルタイム(再起動、シャットダウン)、削除
 - ・ パッケージ(OS/ファームウェア、ソフトウェア、設定)の作成、編集、登録および実装
 - o レポートの作成および表示
 - o ビューの作成、変更

6.7. ネットワークの設定

本セクションでは、WDMおよびWyse端末が使用しているネットワークが、コンピューティング環境全 般の共通セキュリティガイドラインに従っていることを確認するための一般的なガイドラインを説明しま す。

- DNSおよびDHCPサーバー Wyse端末は、DNSおよびDHCPベースのディスカバリ方式を使用して、WDMに自動チェック インによる登録を実行します。DNSおよびDHCPサーバーに権限のないユーザーがアクセスする ことによって端末が無許可で管理されないよう、これらのサーバーへのアクセスを制限すること をお勧めします。自動ディスカバリに必要なDNSおよびDHCPサーバー設定の詳細は「WDM Administrator's Guide」を参照してください。
- PXEトラフィック Wyse製品でのPXEプロトコルの使用についての詳細は「PXEイメージング」セクション(セク ション6.4)を参照してください。ネットワークにおけるPXEトラフィックを制限/ブロックす ることをお勧めします。
- パスワードポリシー 一般的なコンピュータシステムで堅牢なパスワードを設定するために利用されているパスワード の複雑性のガイドラインに従ってください。

付録A-項目のチェックリスト

本セクションでは、本文書で説明されている設定のリストを示します。

1.	はじめに	2
2.	適用範囲	2
3.	参照資料	2
4.	WDMアーキテクチャ	3
5.	セキュリティガイドラインの概要	4
6.	詳細なセキュリティガイドライン	4
6	.1. セキュアモード (HTTPS) の有効化	4
6	.2. 非セキュアなコンポーネントおよびサービスの無効化	4
	6.2.1. FTP リポジトリの無効化	4
	6.2.2. HTTP リポジトリの無効化	5
	6.2.3. TFTP サーバー/サービス	5
6	.3. WDMのデフォルトパスワードおよびデフォルト設定の変更	5
	6.3.1. SQLデータベースパスワード	5
	6.3.2. ソフトウェアリポジトリ	5
	6.3.3. 通信に使用されるポート	5
	6.3.4. ファイアウォール設定	6
	インストール時	6
	インストール後	6
6	.4. デフォルトの端末設定の変更	9
	6.4.1. Write-Filter	9
	6.4.2. リモートシャドウイング (VNC)	9
	6.4.3. BIOSおよびユーザーのパスワード	
	6.4.4 ドメイン参加	
	6.4.5. PXEイメージング	
6	5. Wyse端末での最新のファームウェアおよびソフトウェアの使用	
6	.6. Active Directoryの統合および委任	
6		
付金	■ 項目のチェックリスト	
付金	℞ – ⅡSでのセキュリティモード(HTTPS)の有効化	14

付録B-IISでのセキュリティモード(HTTPS)の有効化

HTTPSまたはルート証明書を使用したセキュアな通信の設定

SSLを使用したセキュアな通信の設定

IIS 6.0およびIIS 7 (および7.5) でSSLを有効にする方法は複数あります。IIS 6.0でSSLを設定するには、 以下のガイドラインを使用してください。

<u>Windows Server 2003上のIIS 6.0でのSSLの設定</u>

以下のガイドラインを使用してください。

- リンク<u>IIS 6.0 Resource Kit Tools</u>から**IIS 6.0 Resource Kit Tools**をダウンロードします。
 - 1. IIS 6.0 Resource Kit Toolsをインストールします。
 - 2. **コマンド プロンプト**に移動し、ディレクトリをバイナリ**selfssl.exe**の場所(「c:¥Program Files¥IIS Resources¥SelfSSL」など)に変更します。
 - 3. 以下のパラメータを指定して、selfsslユーティリティを実行します。
 - 4. selfssl /N:cn=certificate_name /S:site_id (例えば、selfssl /N:cn=MyComputer.Sample.com /S:1。サイトIDが1の場合、cnはコンピュータのFQDN名とIPアドレスを組み合わせたものになります)
 - 5. 次に、以下のようにしてSSLを設定します。
 - コマンドプロンプトに移動して、ディレクトリをadsutil.vbsファイルの場所(例えば 「c:¥Inetpub¥AdminScripts」)に変更します。
 - 以下のようにして、コマンドプロンプトからadsutil.vbsを実行します。
 - cscript.exe adsutil.vbs set /w3svc/site_id/SecureBindings ":443 (例えば、サイトIDが1の場合、cscript.exe adsutil.vbs set /w3svc/1/SecureBindings ":443)。

<u>Windows Server 2008 R2上のIIS 7でのSSLの設定</u>

以下のガイドラインを使用してください。

リンク<u>SelfSSL.exe</u>から**SelfSSL7**ユーティリティをダウンロードします。

- 1. 以下のパラメータを指定して、SelfSSL7.exeユーティリティを呼び出します。
- 2. SelfSSL7.exe /Q /N cn=Certificate_Name /I /S Web_Site_Name。例えば、SelfSSL7.exe /Q /N cn="TestCert.TestLab.com" /I /S "Default Web Site"

ルート証明書を使用したセキュアな通信の設定 Windows Server 2008 R2上のIIS 7へのルート証明書のインストール

以下のガイドラインを使用してください。

証明書をインストールするには、以下の2つの手順を実行する必要があります。

- **ドメインコントローラ**サーバーに証明書をインストールする
- **WDM**サーバーに証明書をインストールする

ドメインコントローラサーバーへの証明書のインストール:

以下のガイドラインを使用してください。

- 1. [サーバーマネージャー]を起動します。
- 2. ツリーペインで[役割]を選択し、[役割の追加]を選択します。
- 3. [役割の追加ウィザード]で、ツリーペインから[サーバーの役割]を選択します。
- 4. [サーバーの役割]ページで、[役割]リストから[Active Directory証明書サービス]を選択します。

Before You Begin Server Roles	Select one or more roles to install on this server.	Description
AD CS Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	Active Directory Certificate Services Active Directory Foedration Services Active Directory Federation Services Active Directory Rights Management Services Wendows Deployment Services Windows Server Update Services	Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

5. [次へ]->[次へ]をクリックします。次に、[役割サービス]リストで[認証機関]および[認証機関Web 登録]にチェックを入れます。

Add Roles Wizard		×
Select Role Serv	ices	
Before You Begin Server Roles AD CS Role Services CA Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	Select the role services to install for Active Directory Certificate Servi Certification Authority Online Responder Network Device Errollment Service Certificate Errollment Verb Service Certificate Errollment Policy Web Service	ces: Description: <u>Certification authority Web Enrollment</u> plivides a simple Web Interface that arequest set operior numericates, retrieve certificate revocation lists (CRLs), and enroll for smart card certificates.

6. IISがサーバーにインストールされていない場合は、[認証機関Web登録]にチェックを入れた後、 別ページで[役割の追加ウィザード]が表示されます。

	Warnel		
	Add role services and features required Enrollment?	I for Certification Authority Web	
	You cannot install Certification Authority Web Enrollment unle installed.	ss the required role services and features are also	
	Role Services:	Description:	
	 Web Server (IIS) Web Server Management Tools Remote Server Administration Tools Role Administration Tools 	<u>Web Server (IIS)</u> provides a reliable, manageable, and scalable Web application infrastructure.	
		Add Required Role Services Cancel	
(i) Why	are these role services and features required?		//

7. 上記ページで、[必要な役割サービスを追加]ボタンをクリックし、[次へ]をクリックして[セット アップの種類の指定]ページを開きます。

Add Roles Wizard	×
Specify Setup Ty	pe
Before You Begin Server Roles AD CS Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Web Server (IIS) Role Services Confirmation Progress Results	Certification Authorities can use data in Active Directory to simplify the issuance and management of certificates. Specify whether you want to set up an Enterprise or Standalone CA.
	More about the differences between enterprise and standalone setup
	< Previous Next > Instal Cancel

8. 上記ウィンドウで、必要に応じて[エンタープライズ]または[スタンドアロン]を選択し、[次へ]を クリックして[CA の種類の設定]ページを開きます。

Add Roles Wizard		×
Specify CA Type		
Before You Begin Server Roles AD CS Role Services Setup Type CA Type Private Key Cryptography CA Name Valdity Period Certificate Database Web Server (IIS) Role Services	A combination of root and subordinate CAs can be configured to create a hierarchical public key infrastructure (PKI). A root CA is a CA that issues its own self-signed certificate. A subordinate CA receives its certificate from another CA. Specify whether you want to set up a root or subordinate CA. © <u>Boot CA</u> Select this option if you are installing the first or only certification authority in a public key infrastructure. © <u>Subordinate CA</u> Select this option if your CA will obtain its CA certificate from another CA higher in a public key infrastructure.	
Confirmation Progress Results	More about public key infrastructure (PKI) < Previous	

9. [CA の種類の設定]ページで、必要に応じて[ルート CA]または[下位CA]を選択し、[次へ]をク リックして[秘密キーの設定]ページを開きます。



10. [秘密キーの設定]ページで、必要に応じて[新しい秘密キーを作成する]または[既存の秘密キーを 使用する]を選択し、[次へ]をクリックして[CAの暗号化を構成]ページを開きます。

Add Roles Wizard		×
Configure Crypto	graphy for CA	
Before You Begin Server Roles AD CS	To create a new private key, you must first select a <u>cryptographic service provider</u> , <u>hash algorithm</u> , and key length that are appropriate for the intended use of the certificates that you issue. Selecting a higher value for key length will result in stronger security, but increase the time needed to complete signing operations.	
Role Services Setup Type CA Type	Select a cryptographic service provider (CSP): Key character length: RSA#Microsoft Software Key Storage Provider I 1024	
Private Key Cryptography CA Name	Select the hash algorithm for signing certificates issued by this CA: SHA512 SHA512 SHA1 Uns	
Validity Period Certificate Database	Allow administrator interaction when the private law is accessed by the CA	
Web Server (IIS) Role Services Confirmation	The provide during the decorrection of the private key is accessed by the call	
Progress Results		
	More about cryptographic options for a CA	
	<previous next=""> Install Cancel</previous>	

11. [CAの暗号化を構成]ページで、必要に応じて[暗号化サービスプロバイダー(CSP)を選択] フィールドの 値を選択し、[キーの長さ]を指定し、[このCAから発行された証明書の署名に使 用するハッシュアルゴリズムを選択]フィールドの値を選択し、[CAが秘密キーにアクセスすると きに、管理者による操作を許可する]のチェックを選択または選択解除し、[次へ]ボタンをクリッ クして[CA名を構成]ページを開きます。

Add Roles Wizard	×
Configure CA Nar	ne
Before You Begin Server Roles AD CS	Type in a common name to identify this CA. This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.
Role Services	SurWDMLab-WIN-MHPTD0N5FCO-CA
Setup Type	Distinguished name suffix:
Private Key	DC=SurWUMLab,DC=com
Cryptography	
CA Name	Preview of distinguished name: CN=SurWDMIab-WIN-MHPTD0NSECO-CA_DC=SurWDMIab_DC=com
Validity Period	
Certificate Database	
Web Server (IIS)	
Role Services	
Confirmation	
Progress	
Results	
	More about configuring a CA name
	<previous next=""> Install Cancel</previous>

✓注:証明書の共通名は、WDMサーバーのコンピュータ名と一致している必要があります。

12. [CA名を構成]ページで[このCAの共通名]および[識別名のサフィックス]フィールドの値を指定し、[次へ]をクリックして[有効期間の設定]ページを開きます。

Add Roles Wizard Set Validity Peri	od
Before You Begin Server Roles AD CS Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Web Service (IIS) Role Services Confirmation Progress Results	A certificate will be issued to this CA to secure communications with other CAs and with clients requesting certificates. The validity period of a CA certificate can be based on a number of factors, including the intended purpose of the CA and security measures that you have taken to secure the CA. Select validity period for the certificate generated for this CA: Select validity period for the certificate generated for this CA: Select validity period for the certificate generated for this CA: Years CA expiration Date: 3/30/2017 11:20 AM Note that CA will issue certificates valid only until its expiration date.
	More about setting the certificate validity period
	< Previous Next > Install Cancel

13. [有効期間の設定]ページで、このCAから生成される証明書の有効期間を選択し、[次へ]をクリッ クして[証明書データベースを構成]ページを開きます。

Add Roles Wizard	
Configure Cert	ificate Database
Before You Begin Server Roles AD CS Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Web Service (TIS) Role Services Confirmation Progress	The certificate database records all certificates, issued certificates, and revoked or expired certificates. The database log can be used to monitor management activity for a CA. Qertificate database location: C::Windows/system32/CertLog @grtificate database log location: C::Windows/system32/CertLog C::Windows/system32/CertLog
Kesuis	< Previous Next > Instal Cancel

14. [証明書データベースを構成]ページで、[証明書データベースの場所]と[証明書データベースログの場所]を選択し、[次へ]をクリックして[Webサーバー(IIS)]の役割追加ページを開きます。

Add Roles Wizard Select Role Set	rvices	X
Before You Begin Server Roles AD CS Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Web Server (IIS) Role Services Confirmation Progress Results	Select the role services to install for Web Server (IIS): Role services: Web Server Common HTTP Features Static Content Default Document Directory Browsing HTTP Redirection WebDAV Publishing Application Development Application Development Application Development Server Side Includes Server Side	Description:
	< Previous	Vext > Install Cancel

- 15. デフォルト値を受け入れ、[次へ]>[インストール]をクリックします。
- 16. これで、Active Directory証明書サービス、Webサーバー(IIS)および認証機関Web登録がインストールされます。

erore rou begin	The following roles, role service	es, or features are being insta	iled:	
erver Roles	Active Directory Cert	ificate Services		
) CS	Web Server (IIS)			
Role Services	Remote Server Admi	nistration Tools		
Setup Type				
CA Type				
Private Key				
Cryptography				
CA Name				
Validity Period				
Certificate Database				
'eb Server (IIS)				
Role Services				
onfirmation				
ogress				
esults				

- 17. 証明書サービス(証明機関)をインストールしたら、ドメインコントローラの[インターネットイン フォメーションサービス(IIS)マネージャー]を起動します。
- 18. [サーバーマネージャー]のツリーペインで[役割]を展開し、[Webサーバー (IIS)]->[インター ネットインフォメーションサービス (IIS) マネージャー]をクリックして[インターネットイン フォメーション(IIS)マネージャー]ページを開きます。

ile <u>V</u> iew <u>H</u> elp					
Control of the second sec	WI Filter: ASP Directory Brossing HTTP Redirect	Authentication	Compression Compression Failed Recuest Tracing Rules ESAPT and CGI Restrictions Cotput Caching	Show Al Default Default Decument Handler Mappings Logging Request Filtering	ctions Open Feature Manage Server Restart Start Stop View Application Pools View Sites Help Online Help
	Certificates	Processes			

19. ツリーペインでサーバー名ノードを選択し、中央ペインで[サーバー証明書]アイコンをダブルク リックします。

Number Information Server	vices (IIS) Manager		
🚱 💽 📢 🕨 WIN-U6G	GFCJGQBT		🖸 🖂 🟠 I 🕐 🔹
Eile <u>V</u> iew <u>H</u> elp			
Connections	Server Certifica Use this feature to request and m with Web sites configured for SSL. Name	tes anage certificates that the Web server can use Issued To Issued By Issued To Issued By	Actions Import Create Certificate Request Complete Certificate Request Create Domain Certificate Create Self-Signed Certificate P Help Online Help
Ready			€ <u>=</u> .:

20. [サーバー証明書]ページの右側ペインで、[ドメイン証明書の作成...]をクリックして証明書の作成 を開始します。

Create Certificate		? ×
Distinguishe	d Name Properties	
Specify the required informa as official names and they c	ation for the certificate. State/province and City/locality must be specified annot contain abbreviations.	
Common name:	TestCertificate	
Organization:	Test	
Organizational <u>u</u> nit:	Business	
City/ <u>l</u> ocality	San Jose	
State/province:	CA	
Country/region:	US	
	Previous <u>N</u> ext Finish Canc	el

21. [証明書の作成]ページで必要な情報を入力し、[次へ]をクリックして[オンライン証明機関]ページ を開きます。

Create Certificate	<u>? ×</u>
Online Certification Authority	
Specify the certification authority within your domain that will sign the certificate. A friendly name is required and should be easy to remember.	5
speary Online Certification Authority:	
SurwDMLab-WIN-MHPTDUNSECO-CA (WIN-MHPTDUNSECO.SurWDMLab.com	.ct
Example: CertificateAuthorityName(ServerName	
TestCert.SurWDMLab.com	
Previous Next Einish	Cancel

- 22. [オンライン証明機関]ページで、[選択...]を選択して[オンライン証明機関の指定]を設定し、さら に[フレンドリ名]を指定して[終了]をクリックします。
- 23. これで、ドメインコントローラサーバーでの証明書のインストールが完了しました。次はWDM サーバーへの証明書のインストールに進みます。

WDMサーバーへの証明書のインストール:

以下のガイドラインを使用してください。

1. タスクバーで[スタート] > [管理ツール] > [インターネットインフォメーションサービス (IIS) マ ネージャー]をクリックし、[インターネットインフォメーションサービス(IIS)マネージャー]ペー ジを開きます。

🕒 🕥 📲 🕨 WIN-UGG	GFCJGQBT 🕨	D 🗠 🗠 🛛
Eile <u>V</u> iew <u>H</u> elp		Actions
Control of the second sec	WIN-UGGGFCJGQBT Home	Actions Open Feature Hanage Server Restart Start Stop View Application Pools View Sites Image: Help Online Help

2. ツリーペインでサーバー名ノードをクリックし、中央ペインで[サーバー証明書]アイコンをダブ ルクリックして[サーバー証明書]ページを開きます。

Internet Information Serv	vices (IIS) Manager			
🚱 💽 📢 🕨 WIN-U6G	GFCJGQBT		60	× 🕼 I 🕐 •
<u>File View H</u> elp				
Connections	Server Cel Use this feature to requer with Web sites configured Name	ttificates at and manage certificates that the Web server for SSL. Issued To	can use Issued B Issu	:Request tte Request <u>rtificate</u> d Certificate
Ready				· .:

3. [サーバー証明書]ページの右側ペインで[ドメイン証明書の作成...]をクリックし、証明書の作成を 開始します。

Create Certificate		? ×
Distinguishe	ed Name Properties	
Specify the required inform as official names and they o	ation for the certificate. State/province and City/locality must be specified cannot contain abbreviations.	
Common name:	TestCertificate	
Organization:	Test	
Organizational unit:	Business	
City/locality	San Jose	
State/province:	CA	
Country/region:	US	
	Previous <u>N</u> ext Finish Ca	ncel

4. [証明書の作成]ページで必要な情報を入力し、[次へ]をクリックして[オンライン証明機関]ページ を開きます。

Create Certificate	? ×
Online Certification Authority	
Specify the certification authority within your domain that will sign the certificate. A friendly name is required and should be easy to remember.	
Specify Online Certification Authority:	-
SurWDMLab-WIN-MHPTD0N5FCO-CA\WIN-MHPTD0N5FCO.SurWDMLab.com	
Example: CertificateAuthorityName\ServerName	
Friendly name:	
TestCert.SurWDMLab.com	
Previous Next Einish Cano	el

- 5. [オンライン証明機関]ページで、[選択...]をクリックして[オンライン証明機関の指定]を設定し、 さらに[フレンドリ名]を指定して[終了]をクリックします。
- 6. これで、WDMサーバーへの証明書のインストールが完了しました。
- 7. 証明書のインストール後に、サーバー名ノード > [サイト] > [Rapport HTTP Server]を選択し、 右端ペインの[サイトの編集]セクションの下にある[バインド...]をクリックして[サイトバインド] ダイアログを開きます。

💐 Internet Information Serv	ices (IIS) Manager	
G SJC-NBI	K-SDUBEY 🕨 Sites 🕨 Rapport HTTP Server 🕨	😰 🛛 🟠 🔞 •
<u>F</u> ile <u>V</u> iew <u>H</u> elp		
Connections	Rapport HTTP Server Home Filter	Actions Actions Edit Steplore Edit Ste Basic Settings View Applications View Virtual Directories Manage Web Site Restart Stop Browse Web Site Browse 80 (http) Advanced Settings Configure Failed Request Tracing Limits
	Filtering Authorin	Add FTP Publishing Help Online Help
<	🛅 Features View 💦 Content View	
Configuration: 'Rapport HTT	P Server' web.config	• <u></u>

8. [サイトバインド]ダイアログで[追加]をクリックし、[サイトバインドの追加]ダイアログを開きま す。

Add Site Binding				? 🗙
Iype: https ▼	IP address: All Unassigned		•	P <u>o</u> rt: 443
<u>SSL certificate:</u>				
Hotscielled		OK		Cancel

- 9. [サイトバインドの追加]ダイアログを開いたら、[種類]ドロップダウンからhttpsを選択し、[SSL 証明書]ドロップダウンから作成した証明書を選択し、[OK]ボタンをクリックします。
- 10. HTTPS通信のみを開始するには、以下のようにします。

サーバー名ノード> [サイト] > [Rapport HTTP Server] を選択し、[SSL設定]をダブルク リックします。

Internet Information Services (II	S) Hanager	-01
C C + WDV2K8R2X64EV	T + Sites + Rapport HTTP Server +	10 × 310
file yew tielp		
Connections 	SSL Settings	Actions By Apply By Cancel
Bir gi information Freis	P Rogare 52. C group C group C group C group P Rogare P Roduces New C Content Vew	e roj Ordentoj
Configuration: Secularity and antication that of	anfor - decates safe a Tassert KTP Sever">	61

11. [SSL設定]ページで[SSLが必要]チェックボックスを選択し、[適用]をクリックします。