# LogVillage 2.0

# 導入マニュアル

V2. 3J

# 株式会社 蒼 天

Copyright © 2003-2019 SO-TEN, Inc. All Rights Reserved.

# logVillage2.0 導入マニュアル

revision : MD-23-20190813

\*本書に記載の会社名および製品名は、各社の商標または登録商標です。
 \*本ソフトウェアを無断で複製することを禁止します。
 \*本書の一部または全部を無断転載することを禁止します。
 \*本書の内容に関しては、将来予告なしに変更する場合があります。

# 株式会社蒼天

http://www.so-ten.co.jp/ support@so-ten.co.jp

〒135-0032 東京都江東区福住 1-14-4 山崎ビル 1F TEL:03-5809-8406 FAX:03-5809-8495

# 目次

1.LogVillage の基本構成	5
1−1. 稼働環境	5
1-2.LogVillage の構成要素	8
1−3. 構成図	9
1-4. LogVillage の動作概要1	0
1-5. インストールプログラムの説明1	1
2. 本番運用までの手順	2
3. 導入前の準備と確認	3
3-1. LogVillageMGR⇔LogVillagePS 間通信方式についての確認	3
3-2. LogVillagePS→管理対象 PC への接続確認1	4
3-3. 管理対象 PC 情報の準備 1	6
4. LogVillageMGR のインストール 1	8
4-1.LogVillageMGR のインストール1	8
4-2.LogVillageMGR のライセンス登録2	23
5. LogVillagePS のインストール	26
5-1. インストールおよび運用環境について 2	26
5-2. LogVillagePS のインストール手順	32
5-3. LogVillagePS のセットアップ 3	35
6. LogVillage の初期設定	37
6−1. 初期設定項目と設定方法 3	37
6-2. LogVillagePS を複数台設置した場合の管理対象 PC との関係	8
6-3. ログ収集の仕組みと注意点 3	9
6-3-1. ログ収集スケジュール	39
6-3-2. ログ収集タイミング 4	0
7. 管理対象 PC の設定変更	1
7-1. 設定変更の方法	2
7-2. WorkGroup 環境での管理対象 PC 設定内容4	3
7-3. ActiveDirectory 環境での管理対象 PC 設定内容 6	51
7-3-1. グループポリシー設定変更項目6	52
7-3-2.LogVillageMGR に登録する管理対象 PC のユーザー設定項目8	33
7-3-2-1.Active Directory 上でDomain Admins 権限を持ったユーザーの作成と	
LogVillage への登録 8	\$4
7-3-2-2. Active Directory 上で OU の管理者権限を持ったユーザーの作成と LogVillag	;e
への登録9	12
8.LogVillageMGR 画面の基本操作 10	)4
8-1.LogVillageMGR 画面の表示方法10	)4
8-2. 画面概要	)5
8-3. システム設定画面	)6

9. 管理対象 PC 自動設定ツール 107
9-1.LogVillage 管理対象 PC 設定ツール 107
9-1-1. 対応 0S
9-1-2. 管理対象 PC での実行時の注意事項 107
9-1-3. 設定手順
9-2. 管理対象 PC を LogVillage マネージャに登録する110
10.LogVillage 運用のための情報 111
10-1. LogVillage マネージャ動作関連ログファイル111
10-1-1. ログ保存場所 111
10-1-2. ログ保存期間 111
10-2.LogVillage ポーリングサーバー動作関連ログファイル112
10-2-1. ログ保存場所 112
10-2-2. ログ保存期間
10-3. Apache2 動作関連ログファイル 113
10-3-1. ログ設定方法
10-3-2. ログ保存場所
10-3-3. ログ保存期間
11. SSL(暗号化)通信設定114
12. お問合せ
<< 補足資料 >>118

# 1. LogVillage の基本構成

LogVillageの基本構成について説明します。

# 1-1. 稼働環境

LogVillage の稼働環境について説明します。

■LogVillage マネージャ(以下:LogVillageMGRとする)

OS Windows Server 2016 Windows Server 2012 R2 Windows Server 2012 Windows Server 2008 R2 Windows Server 2008 Windows10 Pro, Education, Enterprise Windows8.1 Pro, Enterprise Windows 7 Professional, Windows 7 Enterprise, Windows 7 Ultimate

CPU Pentium4 2GHz 相当以上

メモリ 4GB 以上

ハードディスク

1GB 以上(LogVillage システム用領域) ※データ保管用として別途 HDD 容量が必要です。 ※ディスクのフォーマット形式は NTFS 限定です。

※他のアプリケーションと共存の場合、アプリケーション間の競合(干渉)が発生し、LogVillageMGRの動作が不安定 となる場合がありますので、LogVillageMGR専用の環境にインストールいただくことを推奨いたします。 ※インストール時にTCP80番ポートが開いている必要があります。

【ご注意事項】

LogVillage マネージャをインストールいただく PC サーバに、一定周期の OS 再起動処理の設定を 強く推奨いたします。 Windows Server OS: 30 日に1回

Windows Client OS: 1日に1回

■LogVillage ポーリングサーバー(以下:LogVillagePSとする)

OS Windows Server 2016 Windows Server 2012 R2 Windows Server 2012 Windows Server 2008 R2 Windows Server 2008 Windows10 Pro, Education, Enterprise Windows8.1 Pro, Enterprise Windows 7 Professional, Windows 7 Enterprise, Windows 7 Ultimate

CPU Pentium4 2GHz 以上

メモリ 2GB 以上

ハードディスク

100MB 以上(LogVillage システム用領域) ※ディスクのフォーマット形式は NTFS 限定です。

※LogVillagePS のインストールは「Workgroup」環境で行ってください。

- ・「ActiveDirectory」に参加している状態でLogVillagePSをインストールすると、正常動作しません。
- LogVillagePS をインストールしたサーバが「ActiveDirectory」環境で、管理対象 PC の環境が「WorkGroup」場
   合、ドメインコントローラ側でセキュリティレベルの変更が必要な事をご留意ください。(詳細は

「5. LogVillagePS のインストール」をご参照ください)

※Microsoft .NET Framework 3.5 または、Microsoft .NET Framework 3.5 sp1 がインストールされていることが 必要です。

※<u>ドメインコントローラとの共存は行えません。</u>

※他のアプリケーションと共存の場合、アプリケーション間の競合(干渉)が発生し、LogVillagePSの動作が不安定 となる場合がありますので、LogVillagePS専用の環境にインストールいただくことを推奨いたします。

0

【ご注意事項】

LogVillage PS をインストールいただく PC サーバに、一定周期の OS 再起動処理の設定を強く推奨 いたします。

再起動周期はOS 種別によって異なります。

Windows Server OS : 30 日に1回

Windows Client OS : 1日に1回

## ■管理対象PCのOS

OS Windows10 Pro, Education, Enterprise Windows8.1 Pro, Enterprise Windows 7 Home Premium, Windows 7 Professional, Windows 7 Ultimate, Enterprise Windows Server 2016 Windows Server 2012 R2 Windows Server 2012 Windows Server 2008 R2 Windows Server 2008 Mac OSX 10.3 以降 (※1)

※1. 別途 Mac OSX 対応ツール (オプション) が必要となります。

# 1-2.LogVillageの構成要素

LogVillage は以下により構成されます。

LogVillage マネージャ	・Web アプリケーション
: LogVillageMGR	—LogVillage 全体のシステム設定画面
	ーログ情報の検索・参照画面
	ー稼働状況のモニタリング画面
	・データベース
	ーログ情報の蓄積
	ーシステム設定情報の保存
LogVillage ポーリングサーバー	・ログ情報の収集(ポーリング)
: LogVillagePS	・アラート通知(メール、ポップアップ)
	・1つのLogVillageMGR に対して複数のLogVillagePS を
	設置可能
管理対象 PC 自動設定ツール	・管理対象 PC へ管理者権限を有するユーザーアカウン
	ト、パスワードを自動作成
	・管理対象 PC に対してログ収集を行うための設定を自動
	化
管理対象 PC	<ul> <li>LogVillage にてログ情報を収集される PC 端末(被管理)</li> </ul>
	PC)
	・プログラムのインストールは不要、但し、設定変更が
	必要

# 1-3. 構成図

構成図は下図の通りです。



# 1-4. LogVillage の動作概要

LogVillage の動作概要について説明します。

# ■管理対象 PC のデータが LogVillage データベースに格納されるまで

- ① LogVillagePS が管理対象 PC を監視し、情報などを取得します。
- ② LogVillagePS は、データを暗号化し LogVillageMGR の Spool フォルダへ送信します。
- LogVillageMGRは、Spoolフォルダに書き込まれたデータを復号化してLogVillageデータベースに書き込みます。

#### ■格納されたLogVillage データをブラウザで閲覧する

④ 管理コンソールよりブラウザを通してデータベースの内容を確認します。
 (この場合は、HTTP と HTTPS が使用可能です。)

#### ■LogVillagePS と管理対象 PC 間の通信について

以下のポートが解放されている必要があります。

- NetBIOS 用 139:TCP, 445:TCP, 137:UDP, 138:UDP
- DCOM 用 135:TCP

RPC 動的ポート (デフォルトでは 1024 から 65535 までの範囲の中で自動的に割り当てられます)

※LogVillagePS→ 管理対象 PC の方向のみ。

※LogVillagePSに固定 IP を付与できる環境である場合、「LogVillagePSの固定 IP」からのみ通 信許可、とすることにより、よりセキュアな設定とする事が可能です。



# 1-5. インストールプログラムの説明

LogVillage インストールプログラムについて説明します。

#### ■LogVillage マネージャ : LogVillageMGR

※通常のインストールフォルダ

C:\Program Files\SO-TEN\LogVillage

・Apache2 LogVillage で使用する WWW サーバープログラム野格納フォルダ

<ul> <li>MySQL</li> </ul>	- ログデータ蓄積用データベースの格納フォルダ
	※インストール時に他のインストール先を指定することも可能です。
	※管理対象 PC とログ収集スケジュール応じた容量を考慮してください。
	参考:1台1日5M(最大)
• Maneg	jer LogVillageMGR プログラムの格納フォルダ

- ・PHP Web アプリケーション PHP プログラムのフォルダ
- ・ZendOptimizer PHP 暗号化プログラムの格納フォルダ

## C:¥

- Spool
- LogVillagePS から LogVillageMGR ヘアップロードされた ログデータを一時的に格納するフォルダ

#### ■ポーリングサーバー: LogVillagePS

※通常のインストールフォルダ

C:¥Program Files¥SO-TEN¥LogVillage

PServer

LogVillagePS プログラムの格納フォルダ

# 2. 本番運用までの手順



# 3. 導入前の準備と確認

導入前の準備と、その確認方法について説明します。

# 3-1. LogVillageMGR⇔LogVillagePS 間通信方式についての確認

LogVillageMGR⇔LogVillagePS 間通信方式についての確認について説明します。

LogVillageMGR と LogVillagePS 間は WEBDAV 通信を行います。 LogVillageMGR⇔LogVillagePS 間で以下のポートが利用可能かを確認ください。

<ポート番号>

「80」番ポートを使用

## 3-2. LogVillagePS→管理対象 PC への接続確認

LogVillagePS が管理対象 PC の情報収集するために必要な接続の確認方法について説明します。

#### 1) 通信ポート一覧

LogVillagePS から管理対象 PC への接続には以下の通信ポートを使用します。

N	プロト	医后工机	LogVillagePS 側	落后十百	管理対象 PC 側
INO.	コル	迪信于校	ポート番号	迪信力问	ポート番号
1		NETBIOS セッションサービス	any	LogVillagePS→PC	139
2		NETBIOS セッションサービス	any	No.1 の return	139
3	тор	SMB サービス	any	LogVillagePS→PC	445
4	TOP	SMB サービス	any	No.3 の return	445
5		RPC ポート・マッパ	any	LogVillagePS→PC	135
6		RPC ポート・マッパ	any	No.5 の return	135
7		NetBIOS 名前サービス	any	LogVillagePS→PC	137
8	ססוו	NetBIOS 名前サービス	any	No.9 の return	137
9	UDP	NetBIOS データグラム・サービス	any	LogVillagePS→PC	138
10		NetBIOS データグラム・サービス	any	No.11の return	138

#### 2)必須条件

-NetBIOS over TCP/IP (NBT) での通信。

-LogVillagePS より管理対象 PC の名前解決。

ー管理対象 PC に対する LogVillagePS よりアクセスするための設定変更。

\*「7. 管理対象 PC の設定変更」を参照してください。

#### 3)アクセス可否の確認方法

LogVillagePS をインストールする PC の「コマンド プロンプト」より以下のコマンドを実行する ことにより LogVillagePS からのアクセスの可否を確認できます。

※必ず、管理対象 PC の設定変更を行ってから実行してください。

NET USE /USER:<\*A> ¥¥<\*B>¥IPC\$

\*A:管理対象PCの管理者権限を有するアカウント名

ActiveDirectory 環境の場合は、〈ドメイン名〉¥〈ユーザー名〉

- ex) so-ten. local¥logvillage
- \*B:管理対象 PC のコンピュータ名

OアクセスがOK の場合

C:¥>net use /User:< \*A> ¥¥<\*B>¥ipc\$ ¥¥<\*B>¥ipc\$ のパスワードまたはユーザー名が無効です。 '\*A'のパスワードを入力してください。'\*B'に接続します:

<\*A のパスワードを入力>

コマンドは正常に終了しました。

OFireWall 等の影響によるアクセス不可の場合

C:¥>net use /User:< \*A> ¥¥<\*B>¥ipc\$

システム エラー 53 が発生しました。 ネットワーク パスが見つかりません。

※上記のエラーが発生した場合は以下をご確認ください。

- ・管理対象PCの設定漏れ
- NetBIOS 接続の可否。(NetBIOS 接続が可能である必要があります)
- ・Windows 標準以外のファイアウォールが有効となっている場合、該当ファイアウォールの設 定変更が必要です。
- Oパスワード間違いまたは管理対象 PCの未設定の場合のアクセス不可の場合
- C:¥>net use /User:< \*A> ¥¥<\*B>¥ipc\$

システム エラー 1326 が発生しました。 ログオン失敗: ユーザー名を認識できないか、 またはパスワードが間違っています。

※上記のエラーが発生した場合は以下をご確認ください。

- ・管理対象 PC の設定漏れ。
- ・パスワード間違い

#### 4)接続確認ツール

LogVillagePSのインストール後はタスクトレイより接続確認用のツールが利用できます。 タスクトレイアイコンを右クリックし、「接続確認」を選択してください。 操作方法の詳細は別紙接続確認ツールマニュアルをご参照ください。

# 3-3. 管理対象 PC 情報の準備

管理対象 PC 情報の準備について説明します。

## 1)必要となる管理対象 PC 情報

LogVillage で管理するには、管理対象 PC に関する以下の情報を事前に準備しておく必要があります。

- ・コンピュータ名 (NetBIOS 名)
- ・管理者権限を有するアカウント名
- ・上記アカウントのパスワード

# 2) 登録用管理対象 PC 情報の準備

管理対象PCをLogVillageへ登録する方法は以下の3通りの何れかになります。

① 登録用 CSV ファイルを作成し「管理対象 PC の設定」画面より一括インポート登録を行いま す。

<CSV ファイル仕様>

前提条件	
文字コード	Shift-JIS
改行⊐ード	CRLF
レイアウト	・ファイルの1行目はヘッダ行とし項目名を入力する。
	・各項目は「,」で区切る。

ファイル項目			
項目名	文字種/形式	必須/任意	記述法など
アクセス名	半角英数記号	必須	コンピュータ名
			または IPアドレス
ユーザー名	半角英数記号	必須	ドメイン環境の場合、以下の通り
			となります。
			[ドケイン名]¥[ドメインユーザー名]
パスワード	半角英数記号	必須	
グループ名	半全角英数字記号	必須	グループ未作成の場合は"ALL"を
			入力
ポーリングサーバー名	半角英数記号	必須	
ID	入力不要		
OS 種別	半角数字	必須	1:Windows
			2:macOS
			3:Linux

※ポーリングサーバー名の不一致、アクセス名重複の場合はエラーとなります。

- ② 「管理対象 PC の設定」画面より1台ずつマニュアル登録を行います。
- ③ 「管理対象 PC 自動設定ツール」(オプション製品)により自動登録を行います。 ※WORKGROUP 環境のお客様にてご利用いただくツールとなります。

# 4. LogVillageMGR のインストール

LogVillageMGR のインストールについて説明します。

# 4-1. LogVillageMGR のインストール

Setup. exe を実行します。
 CD-ROM内 Installer フォルダ下の Manager フォルダを開きます。
 Setup. exe をダブルクリックします。



内容を確認し「次へ」をクリックします。

「次へ」	をク	リック	します。	
------	----	-----	------	--

LogVillag	ge 2.0	
Log Village 2.3	Log Villageマネージャのインストールを開始します。 このインストーラの実行にはお10分必要となります。 インストールを開始してもよいですか?	
	< 戻る(B) (XA (N))	キンセル

ソフトウェア使用許諾契約書を確認し、問題なければ「同意する」を選択し、 「次へ」をクリックします。

LogVillage2.3		
		<u> </u>
本ソフトウェア使用許諾契約書(以下 会社着天(以下、「弊社」という)との配 定義されるソフトウェア製品のための契	、「本契約」という)は、お客様と株式 肌に締結される、本契約を含む下記で 約書です。	•
<ul> <li>同意する(A)</li> <li>〇 同意しない(D)</li> </ul>		
allShield ————	< 戻る(B) 次へ	(N)> キャンセル

#### ③ 必要情報を入力します。

任意のアクセスアカウント、パスワードを入力し、「次へ」をクリックします。

<b>E</b> (

<u>アクセスアカウント、パスワードは「5-2.LogVillagePSのセットアップ」時で必要になりますの</u>で、大切に保管下さい。

<u>忘れると、LogVillagePSのセットアップが行えませんのでご注意下さい。</u>

④ Web サーバ(Apache)、Web アプリケーション(PHP) プログラム一式のインストール先を指定しま す。

LogVillageMGR プログラムのインストール先フォルダを変更しない場合は「次へ」をクリック します。

インストール先を変更する場合は、参照からインストール先フォルダを指定後、「次へ」を クリックします。

LogVillage2.3		24
Webサーバのインストール先		
Apache、PHPプログラム一式のインストール先	もを指定します。	
「インストール先のフォルダ―――		

LogVillage マネージャとポーリングサーバ間のファイル転送の際に使用する spool フォルダの 場所を指定します。この spool フォルダは最大で 2GB の容量となります。

spool のインストール先フォルダを変更しない場合は「次へ」をクリックします。

インストール先を変更する場合は、参照からインストール先フォルダを指定後、「次へ」をク リックします。

ログデータファイルの一時保存先	
LogVillageマネージャとボーリング† Spoolフォルダの場所を指定します Spoolフォルダは最大で2GBの容量	ナーバ間のファイル転送の際に使用する 量となります。
┌ インストール先のフォルダーーーーー	
ーインストール先のフォルダーーーー C¥spool	参照(R)
インストール先のフォルダ C.¥spool stallShield	参照(R)

データベース(MySQL)のインストール先を指定します。

変更しない場合は「次へ」をクリックします。

インストール先を変更する場合は、参照からインストール先フォルダを指定後、「次へ」をク リックします。

データベース(MySQL)のインストール先			
管理対象PCから収集したログ情報を蓄積す	オるデータベースのインストールダ	もを指定します。	
┌ インストール先のフォルダ			
「インストール先のフォルダ」 C:¥Program Files¥SO-TEN¥LogVillage			参照(R)
インストール先のフォルダー C¥Program Files¥SO-TEN¥LogVillage	¥MySQL		参照(R)
「インストール先のフォルダーー C:¥Program Files¥SO-TEN¥LogVillage #Shield	¥MySQL		参照(R)

LogVillage マネージャのインストール先を指定します。

変更しない場合は「次へ」をクリックします。

インストール先を変更する場合は、参照からインストール先フォルダを指定後、「次へ」をク リックします。

LogVillage2.3		
LogVillageマネージャのインストール先		
LogVillage マネージャのインストール先を指定します。		
「インストール先のフォルダ―――	 	
C:¥Program Files¥SO-TEN¥LogVillage¥Manager		参照(R)
InstallShield		

設定内容を確認し、問題なければ「次へ」をクリックします。

LogVillage2.3	NZA.
指定したインストール先は以下の通りです。	
現在のインストール先でよければ、[ン次へ (N) ] ボタンをクリックしインストールを開始して下さい。 変更する場合は[く戻る(B) ] ボタンをクリックして下さい。 現在のPBマー	
インストール先の確認	*
以下の場所にインストールします。 Webサーバのインストール先 [C:¥Program Files¥SO-TEN¥LogVillage] ログデータファイルの一時保存先 [C:¥spool] データベースのインストール先	
	F
Instalioniaid (N)>	キャンセル

LogVillage マネージャでは、マイクロソフト社製の "microsoft Visual C++ 2005 再配布可能 パッケージ"を利用しています。

そのため、以下のマイクロソフト ソフトウェアライセンス条項に同意いただく必要があります。

Microsoft Visual C++ 2005 使用許諾書を確認し「はい」をクリックします。

Microsoft Visual C++ 2005 SP1 再頒布可能パッケージ (x86)	_ 🗆 🗙
次の使用許諾契約をお読みください。PageDown キーを使ってスクロールし	てください。
マイクロソフト ソフトウェアライセンス条項 MICROSOFT VISUAL C++ 2005 RUNTIME LIBRARIES	-
本ソフトウェア ライセンス条項 (以下「本ライセンス条項」といいます) の条項 客様とMicrosoft Corporation ほたはお客様の居住地によってはその関連 の契約を構成します。以下の条項を注意してお読みべたさい。本ライセンス多 上記のソフトウェアおよびソフトウェアが記録された媒体(以下総称して「本ン ア」といいます) に適用されます。また、本ライセンス条項は、マイクロソフトの	は、お 会社)と 条項は、 ワトウェ
* 更新プログラム * 追加物 * インターネットベースのサービス * サポート サービス	T
使用許諾契約に同意されますか? [いいえ] を選ぶとインストールを中止しま ールするには、この契約に同意してください。	す。インスト
	いいえ(N)

- ⑤ インストールが開始されますので、数分間お待ち下さい。
- ⑥ インストールの完了を確認します。



# 4-2. LogVillageMGR のライセンス登録

LogVillageMGRのライセンス登録について説明します。

① LogVillgae 管理画面にログインします。

Internet Explorer を起動します。

以下のURLにアクセスするとLogVillage ログイン画面が表示されます。

http://<LogVillageMGR のコンピュータ名>/lv/login/

「ユーザー名」「パスワード」を入力し「ログイン」をクリックします。

LogVillage2.0		
ロダイン ユーザー名 	LogVillageのライセンスが未入力です。	

インストール直後のロ	グインユーザー名、パスワードは以下となります。
・ユ <b>ーザ</b> —名	so-ten
・パスワード	so-ten
※LogVillage ユーザー	-の設定後は以下の ID は無効となります。

※ご利用ブラウザについて

LogVillageMGRの対応ブラウザは InternetExplorer9 以降となります。

② 「ライセンス登録・更新」画面を開きます。

「システム設定」→「ライセンス登録・更新」をクリックします。

LogVillage2.0	v so-ten	
ダッシュボード	システム設定	
ログイン完了しました。	ライセンス登録・更新 初期期設定	•

# ③ ライセンスを更新します。

「ライセンス更新」をクリックします。

g village 2.0			so-ten
			システム設
ふ設定 〉 運用管理 〉 ライセンス登	緑・更新		
ライヤシフは掘			
お各棟番ち			
これの日外政	4	11七ノ人設定日時 相大型経動 会	
登録可能クライア、小PC	台	現在智慧教 台	
LogVillage リリースパージョン	V2.3.2.74	SULTERSY D	
マネージャのバージョン	V2.3.2.74		
データベースバージョン	V2.3.2.74		
ニメーショフ東新			
21620871			

「LogVillage2.0 ライセンスコード通知書」に記載されているライセンスコードを入力し、 「登録する」をクリックします。

LogVillage 2.0	 so-ten
⋬⋼⋟ᠴ⋇⋍⋷	システム設定
システム設定 > 運用管理 > ライセンス登録・更新 > ライセンス更新	
< <u> ライセンス情報</u>	
ライセンス更新	
ライセンス 三字ドン 単一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一	

#### ④ 登録完了を確認します。

ご購入いただいたライセンス情報が正しく表示されていることをご確認下さい。

gVillage 2.0			▼ so-ten
シュボード 資産管	理	<b>操作口</b> グ管理 移動管理	システム語
ふ設定 〉 運用管理 〉 ライセ	ンス登録・更新	Я	
ライセンス情報			
お客様番号	60.00		
ご利用期限	無期限	ライセンス設定日時 2016/12/20 02:37:22	
登録可能ボーリングサーバ	無制限	現在登録数0台	
登録可能クライアントPC	50 台	現在登錄数0台	
LogVillage リリースバージョン	V2.3.2.74		
マネージャのバージョン	V2.3.2.74		
データベースバージョン	V2.3.2.74		
利用可能機能			
稼動管理バッケージ			
資産管理オブション 操作管理オブション			
ノア1ル更新腹壁イフン	/=/		
ライセンス更新			

【ご注意ください】

Internet Explorer にて上記操作時に以下の画面が表示される時は、 LogVillageMGRの画面を信頼済みサイトに登録する必要があります。

① 「追加」をクリックします。



② 「追加」をクリックし、「閉じる」をクリックします。



http:// [LogVillageMGRのコンピュータ名] が表示されていることを確認してから追加してく ださい。

# 5. LogVillagePS のインストール

# 5-1. インストールおよび運用環境について

# 5-1-1. LogVillagePS インストール時の環境

LogVillagePS のインストールは「WorkGroup」環境で行ってください。

「ActiveDirectory」に参加している状態でLogVillagePSのインストールを行うと、正常動作が行えません。

サーバにPS をインストールする時の環境	動作
WorkGroup	0
ActiveDirectory	×

#### ※現在の環境を確認する方法

「マイコンピュータ」を右クリック「プロパティ」を選択しま す。

「システムのプロパティ」の「コンピュータ名」タブを開き、 「変更」ボタンを押下します。

「次のメンバ」が「ドメイン」の場合は「ActiveDirectory」に 参加しています。

「ワークグループ」の状態でインストールを実施します。

コンピュータ名の変更
このコンピュータの名前とメンバシップを変更できます。変更するとネットワーク リソースへのアクセスに影響する可能性があります。
コンピュータ名(Q): xxxxx
フル コンピュータ名: xxxxx.
□】 単義冊 ( <u>M</u> )…
がのメンバ 〇ドメイン <u>(2)</u> >
● ワークグループ(W): WORKGROUP
OK (*v)/7/L

#### 5-1-2. LogVillagePS のインストール環境

# (1) 管理対象 PC の「ファイルとプリンタ共有」がインストールされている事

使用中の「ローカルエリア接続」(または「ワイヤレスネットワーク接続」など)に 「Microsoft ネットワーク用クライアント」と「Microsoft ネットワーク用ファイルとプリン タ共有」、「インターネットプロトコル」がインストールされており、かつ、有効になって いる事が前提条件です。

🕹 ローカル エリア接続のプロパティ 🛛 ? 🔀
全般 詳細設定
接続方法
IIII VMware Accelerated AMD PCNet Adapto 構成( <u>C</u> )
この接続は次の項目を使用します(2):
☑ ■Microsoft ネットワーク用クライアント ☑ ■Microsoft ネットワーク用ファイルとプリンタ共有
✓ 県QoS パケット スケジューラ ✓ ラテインターネット プロトコル (TCP/TP)
インストール(M アンインストール(M) プロパティ(R) 説明
□ 接続時(ご通知論通ばにインバリケー々を表示する(W)
✓ 接続が限られているか利用不可能な場合に通知する(M)
OK キャンセル

「ローカルエリア接続」(または「ワイヤレスネットワーク接続」など)が無効になっている場合 は、ネットワーク接続ができない状態です。有効にしてください。



※「Microsoft ネットワーク用クライアント」と「Microsoft ネットワーク用ファイルとプリンタ 共有」の詳細に関しては、以下の URL をご参照ください。

ネットワークとダイヤルアップ接続を構成する http://technet.microsoft.com/ja-jp/library/cc758082(WS.10).aspx

#### (2)分散 COM 設定が有効となっている事

「コンポーネントサービス」を起動します。
 "Windows スタートメニュー"→「コントロールパネル」→「管理ツール」→「コンポーネント サービス」を起動します。
 ※「管理ツール」の表示のためには「コントロールパネル」で「小さいアイコン」または「大きいアイコン」の選択が必要です。

② 「マイコンピュータ」のプロパティを開きます。

「コンソール ルート」→「コンポーネント サービス」→「コンピュータ」→「マイ コ ンピュータ」を開きます。

「マイコンピュータ」を右クリックし「プロパティ」をクリックします。



「このコンピュータ上で分散 COM を有効にする」を変更します。
 「既定のプロパティ」タブを開きます。
 「このコンピュータ上で分散 COM を有効にする」にチェックが入っている事を確認し、

「OK」をクリックします。
マイ コンピュータ <u>のプロパティ</u>
全般 オプショノ 既定のプロパティ 既定のプロトコル MSDTC COM セキュリティ
マ このコンピュータ上で分散 COM を有効にする(E)
□ このコンピュータ上で COM インターネット サービスを有効にする(N)
- 既定の分散 COM 通信プロパティー
認識レベルは、パケットレベルのセキュリティを指定します。 歴史の認知にいていいい
接続 ▼
偽装レベルは、アプリケーションが呼び出し側を判別できるかどうかと、アプリケーション がクライアントの ID を使って動作できるかどうかを指定します。
既定の偽装レベルロ:
識別する
認証を使用し、既定の偽装レベルが匿名でない場合、参照の追跡にセキュリティを 提供することができます。 「 参照の追跡に追加のセキュリティを提供する(P)
OK 道用(A)

(3) 「ネットワークセキュリティ LAN Manager 認証レベル」の確認

◆LogVillagePS 運用時の注意点

管理対象 PC に比べ、LogVillagePS をインストールしたサーバのセキュリティレベルが低い 場合、設定変更が必要です。

**例えば、**管理対象 PC で最高レベルの「NTLMv2 応答のみを送信(LM と NTLM を拒否する)」を 選択し、LogVillagePS 側で「LM と NTLM 応答を送信する」(初期設定)を選択した場合、ロ グ収集が行えません。

「ネットワークセキュリティ LAN Manager 認証レベル」のセキュリティレベルを「NTLMv2 応答のみを送信(LM と NTLM を拒否する)」に設定することを推奨します。 但し、セキュリティレベルの変更に伴い、LogVillagePS をインストールしたサーバから他の NAS サーバ等に対するアクセスに影響が出る可能性があるのでご注意下さい。

- 「ローカルセキュリティポリシー」を起動します。
   "Windows スタートメニュー"→「コントロールパネル」→「管理ツール」→「ローカル セキュリティポリシー」を起動します。
- ② 「セキュリティオプション」を開きます。
   「セキュリティの設定」→「ローカルポリシー」→「セキュリティオプション」を開きます。
- 「ネットワークセキュリティ LAN Manager 認証レベル」を確認します。
   「LM と NTLM 応答を送信する」が最低レベルで、順にレベルが上がり「NTMLv2 応答のみ送 信¥LM と NTML を拒否する」が最高レベルです。

🦻 ローカル セキュリティ設定		×
ファイル(E) 操作( <u>A</u> ) 表示( <u>V</u>	) ヘルプ(王)	
$\leftarrow \rightarrow   \textcircled{1}   \times \textcircled{2}   \swarrow  $	et en	
🝺 セキュリティの設定	ポリシー △   セキュリティの設定	^
● ● ● アカウント ボリシー		
□	ネットリーク セキュリティ: LAN Manager 認証レベルのプロバティ 🛛 🔀	
🗉 🔛 ユーザー権利の割り当	ローカルセキュリティの設定	
	ニコー ネットワーク ヤキュリティ: LAN Manager 認証レベル	
■ ム崩キーのホリシー ■ ソフトウェア制限のポリシー		
🗄 👵 בישעב באר בישע די		
	1.4 に いてい 古物を送/テラス	
	LM Z NILM 応答を送信9の	
	LM と NTLM を送信する - ネゴシエーションの場合、NTLMv2 セッション セキュリティジ	
	NTLM 2 応答のみ送信する NTLM2 応答のみ送信する	
	NILMV2 応答のみ送信¥LM を拒否する NTLMv2 応答のみ送信¥LM と NTLM を拒否する	
	ugg ホットワーク アクビス 国治の SLD と治的の変換。 悪効 認識ネットワーク セキュリティ: LAN Manager 認証し、 LM と NTLM 応答を。	
	調ネットワーク セキュリティ・セキュア RPC を含むクラ 最小なし	
<                 >		~

(4) UAC (ユーザアカウント制御)機能を停止

インストール時は、UAC 機能を停止にしていただく必要があります。

・Windows7のUAC 停止手順

(他の Windows0S におきましては、画面構成等が異なる場合がありますが同様の設定をお願いいたします)

① 「ユーザー アカウント」を起動します。

"Windows スタートメニュー"→「コントロールパネル」→「ユーザー アカウント」を起動し ます。

※「ユーザー アカウント」の表示のためには「コントロールパネル」で「小さいアイコン」または「大きいアイコン」 の選択が必要です。

「ユーザー アカウント制御設定の変更」を変更します。
 「ユーザー アカウント制御設定の変更」をクリックします。



下図が表示された場合は、「はい」をクリックします。



スライダのつまみを一番下「通知しない」まで下げ、「OK」をクリックします。

🚱 ユーザー アカウント制御の設定		
コンピューターに対する ユーザー アカウント制 の防止に役立ちます。 ユ <u>ーザー アカウント</u> 制	5変更の通知を受け取るタイミングの選択 卸を使用すると、問題を起こす可能性があるプログラムからのコンピューターの変更 <u>明設定の詳細を表示</u>	^
常に通知する		
- [ -	以下の場合でも通知しない:	
	<ul> <li>プログラムがソフトウェアをインストールしようと する場合、またはコンピューターに変更を加えよう とする場合</li> </ul>	=
	<ul> <li>ユーザーが Windows 設定を変更する場合</li> </ul>	
	<ul> <li>         ・ 推奨されません。ユーザーアカウント制御でサポー トされない、Windows 7 用に保証されていないプ ログラムを使用する場合にのみ選択してください。     </li> </ul>	
通知しない		
		-
	・ ⑦OK キャンセル	

※OSにより、下図の場合があります。

その場合は「ユーザーアカウント制御(UAC)を使ってコンピュータの保護に役立てる」のチェックを外し、「OK」をクリックします。

ユーザー アカウント制御 (UAC) を有効にして、お使いのコンピュータをより安全にします。 ユーザー アカウント制御 (UAC) は、お使いのコンピュータに許可のない変更が行われるのを防ぐのに役立
ちます。お使いのコンピュータを保護するために、UAC を有効にしておくことをお勧めします。
OK キャンセル

下図が表示された場合は、「はい」をクリックします。

😚 ユーザー アカウント制御 🛛 💌
😯 次のプログラムにこのコンピューターへの変更を許可しますか?
<ul> <li>プログラム名: UserAccountControlSettings</li> <li>確認済みの発行元: Microsoft Windows</li> </ul>
<ul> <li>         ・ 詳細を表示する(D)         <ul> <li>             はい(Y)             しいいえ(N)         </li> </ul> </li> </ul>
<u>これらの通知を表示するタイミングを変更する</u>

アプリケーションを終了し、OS を再起動します。

# 5-2. LogVillagePS のインストール手順

LogVillagePSののインストール手順について説明します。

 Windows 管理者権限アカウントでログインし、Setup. exe を実行します。 CD-ROM内 Installer フォルダ下の PServer フォルダ開きます。 Setup. exe をダブルクリックします。



内容を確認し「次へ」をクリックします。
 「次へ」をクリックします。

LogVilla	age 2.0
LogVillage2.3	LogVillageポーリングサーバのインストールを開始します。 このインストーラの実行は数分で完了します。 インストールを開始してもよいですか?
	< 戻る(B) <b>次へ (N)&gt; キャンセル</b>

ソフトウェア使用許諾契約書を確認し、問題なければ「同意する」を選択し、 「次へ」をクリックします。

リフトウェア使用許諾契約書		
		-
ーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーー		
受社者夫(以下、「并社」というな 定義されるソフトウェア製品のための	Whatlammachta、本央前を含むて起じ D契約書です。	
<ul> <li>○ 同意する(A)</li> <li>○ 同意しない(D)</li> <li>IlShield</li> </ul>		ED店小(P)
ale	< 戻る(B) 次へ (	N)> キャンセル

LogVillagePSのインストール先フォルダを変更しない場合は「次へ」をクリックします。 インストール先を変更する場合は、参照からインストール先フォルダを指定後、「次へ」をク リックします。

ポーリングサーバのインストール先 LogVillage ポーリングサーバのインストール先を指定します。	- การโรม 年のาม ก	
ポーリングサーバのインストール先	LogVillage ポーリングサーバのインストール先を指定します。	
	ポーリングサーバのインストール先	

③ 「timeKeeper」機能のインストール有無を選択します。

④ 「インストール」を実行します。

Г

「インストール」をクリックします。

指定したインストール先は以下の	Di通りです。
現在のインストール先でよければ 変更する場合は[く戻る(B)]オ	([インストール]ボタンをクリックしインストールを開始して下さい。 ボタンをクリックして下さい。
現在の設定:	
インストール先の確認	
以下の場所にインストールします	ŧ.
LogVillage ポーリン [C:¥Program	がサーバのインストール先 n Files¥SO-TEN¥LogVillage¥PServer]
ज	L

LogVillage マネージャでは、マイクロソフト社製の "Microsoft Visual C++ 2005 再配布可能 パッケージ"を利用しています。

そのため、以下のマイクロソフト ソフトウェアライセンス条項に同意いただく必要があります。

Microsoft Visual C++ 2005 使用許諾書を確認し「はい」をクリックします。



- ※既にMicrosoft Visual C++ 2005 がインストールされている場合は、上記画面は表示 されません。
- ⑤ インストール完了までしばらく待ちます。
- ⑥ インストールの完了を確認します。
   「完了」をクリックするとインストール完了です。

InstallShield Wizard の完了		
セットアッフパは、コンピュータへの LogVillage ポーリングサーバ のインストールを完 了しました。		
< 戻る(B) <b>完了</b> キャンセル		

# 5-3. LogVillagePSのセットアップ

LogVillagePSのセットアップ手順について説明します。

 「LV\_TaskTray (PS)の起動」を起動します。
 "Windows スタートメニュー"→「すべてのプログラム」→「SO-TEN」→「LogVillage 2.0 ポ ーリングサーバー」→「LV\_TaskTray (PS)の起動」をクリックします。

— a

LogVillagePSの設定内容を入力します。

LV	ポーリングサーバ設定画	面 /		f
	ポーリングサーバ名	(マネージャで表示される名称)	<u>登録</u> キャンセル	
	┌マネージャ承認設定(初期	期設定時に使用)		
	マネージャサーバ名		(IP アドレスでも可)	
	アクセスアカント名		<u> </u>	
	バスワード		b c	
	(確認用)		d	
			e	

- a. 任意のLogVillagePS 名を決定します。
- b. LogVillageMGR をインストールした PC のコンピュータ名、もしくは IP アドレス名を入力 します。
- c. LogVillageMGR をインストールしたときに設定したアクセスアカウント名を入力します。
- \*1

d. LogVillageMGR をインストールしたときに設定したアクセスアカウント名のパスワードを 入力します。\*1

- e. 確認用でパスワードをもう一度入力します。
- f. 「登録」をクリックします。
   承認中を知らせるダイアログが表示されます。
   しばらくお待ちいただくと自動的に消えますので、ダイアログが消えた後、次に進んでください。
- \*1 c, d への入力内容は、「4-1. LogVillageMGR のインストール」の「③」で登録したアクセ スアカウント、パスワードとなります。
- 3 LogVillage 管理画面にログインします。
   Internet Explorer を起動します。
   以下の URL にアクセスすると LogVillage ログイン画面が表示されます。

http://<LogVillageMGRのコンピュータ名>/lv/login/

# ④ LogVillage PSの登録の確認を行います。

「システム設定」→「初期設定」→「ポーリングサーバ」をクリックします。

LogVillag	ge 2.0				▼ sa−ten
ダッシュボード	資産管理	操作ログ管理	移動管理		システム設定
ログイノ宗子しました。				ライセンス登録・更新	初期服役定
				$\mathcal{M} \mapsto \mathcal{O}(\mathcal{F})^{\mathcal{O}} \to \mathcal{O}$	
				管理対象PC	
				ログ収集スケジュール	

インストールしたLogVillagePSが「承認済み」として、リストに表示されていれば LogVillagePSのセットアップは完了です。

	4 9779 710 BRECKJ - 3X			
-] 初期設定				
▶ライセンス登録・更新	ポーリングサーバの接続許可、削除、ステーク	双変更を行います。		
*ボーリングサーバ	また、各ボーリングサーバの稼動状況も確認	できます。		
▶ 管理対象PC	0			
・ログ収集 スケジュール	設定内容の検索			
3 <u>共通設定</u>	10 115 (Par - 20)		weith white	
*ボーリングサーバ	ホーリングサーバ名		部分一致)	
*グループ	ステータス			
▶ 管理対象PC	检索			
▶トップ画面	LANC			
▶ WindowsUpdate情報	検索された設定内容			
▶ ウィルス対策ソフト定義ファイル				
トプロセス名辞書				
a second s	ポーリングサーバ名▼	バージョン▼	最終ログ取得日時▼	ステータス▼
*拡張項目名(資産管理)				
* 拡張項目名(変産管理) ヨ グループ単位設定	全てをチェック		Г	
▼拡張項目名(変産管理) ∃ <u>グループ単位設定</u> *LogVillageユーザー	全てをチェック PS1			承認違み
* 拡張項目名(変産管理) ヨ <b>グループ単位設定</b> * Log Villege ユーザー * ログ収集スケジュール	全てをチェック			承認済み
* 鉱築項目名 (変産管理) 日 <b>グループ単位設定</b> * LogVillage ユーザー * ログ収集スケジュール * 管理対象プロセス	全てをチェック			承認済み
* 鉱気項目名(変産管理) 3 <u>グループ単位設定</u> * Log Villege ユーザー * ログ収集スケジュール * 管理対象プロセス * 管理対象プロセス	全てをチェック 全てをチェック 全てをチェック			承認済み
* 鉱築項目名(浸産管理) ヨ <u>グルーブ単位設定</u> * LocVillage ユーザー * ログ収集スケジュール * 管理損象プロセス * 管理損象フィルダ	全てをチェック PS1 全てをチェック チェックしたポーリングサーバーの 登録校	消顺涂	[	承認済み
* 低気時目る(変更管理) コ <b>グループ単位設定</b> * Log Villetをユーザー - ログ収集スかジュール。 * 管理対象プロセス * 管理対象プロセス * 管理対象プロレズ * 管理対象プロレズ * 管理対象プロレズ	全てをチェック 上 全てをチェック チェックしたポーリングサーバーの 登録材 ポーリングサーバの登録考測除する前に、創除	消明除	属する管理対象PC水手動で	承認済み
* 虹奈 74日名 (交遣管理) コ <b>グルーブ単位設定</b> * LogVites ユーザー * 位が現象スケジュール * 管理対象プロセス * 管理対象プロレズ * 管理対象フィルダ * 管理対象フィルダ * 指定アブリケーション * 後石シックウェアライセンス	全てをチェック 全てをチェック チェックしたポーリングサーバーの 登録 ポーリングサーバの登録 を得 除する前に 創 開 他のポーリングサーバに割い 創 てるが、ポーリン	鋼「除 するボーリングサー」がに所得 グサーバを知っアンインスト	財な管理対象PCを手動で ールしてくたさい。	承認済み
* 紅菜 時日名 (変産管理) コ <b>グルーブ単位設定</b> * LogVitesユーザー * のグ収集スがジュール * 管理対象プロセス * 管理対象プロレス * 管理対象プロルズ * 管理対象プロルズ * 管理対象プロルズ * 指定アブリケーション * 後者"ンパウェアライセンス * 紅菜 項目データ登録(変産管理)	全てをチェック	調明除 するポーリングサーバニ所着 ダサーバを知こアンインスト	財る管理対象PCを手動で ールしてください。	承認済み
<ul> <li>* 拡張項目名(没量管理)</li> <li>ゴレーブ単位設定</li> <li>* LogVillesユーザー</li> <li>* ログ切集スグジュール</li> <li>* 管理対象プロセス</li> <li>* 管理対象プロセス</li> <li>* 管理対象プロレス</li> <li>* 管理対象プ</li></ul>	全てをチェック 全てをチェック チェックしたポーリングサーバーの 登録 ポーリングサーバの登録 参明除する前に、 朝除 他のポーリングサーバに割り当てるか、ポーリン	<b>御除</b> するポーリングサーバに所置 ダサーバを先にアンインスト	討ち管理対象PCを手動で ールしてください。	承認済み
* 鉱泉7月83(変産管理) 三 <b>グループ単位読定</b> * しなVileyをユーザー * ログ収集スかジュール * 管理持象プロセス * 管理持象ブルダ * 管理持象ブルダ * 管理持象ブルダ * 指変アブリケーション * 体積ヤンアトウエアライセンス * 鉱築項目デーク変語(変産管理) 三 <u>アラードポリシー酸定</u> + 指定ペルログ類生	全てをチェック PSI 全てをチェック チェックしたポーリングサーバーの 登録さ ポーリングサーバの登録を有限なする前に、 削除 他のポーリングサーバに割り当てるか、 ポーリン	<b>須川除</b> するボーリングサーバに所見 グサーバを知こアンインスト	する管理対象PCを手動で ールしてくださし。	承認済み

初期設定が全て完了するまで、サイドメニュー上部に「初期設定」メニューが表示されます。					
そのため、以下の設定項目が「初期設定」と「共通設定」または「グループ単位設定」に2重で表示されますので					
ご注意ください。					
・ライセンス登録・更新	・ポーリングサーバ	・管理対象 PC	・ログ収集スケジュール		
2重で表示される設定項目は、どちらをクリックいただいても問題ありません					
## 6. LogVillage の初期設定

LogVillageの初期設定について説明します。

# 6-1. 初期設定項目と設定方法

初期設定值日	設定方法		
初别改足項日	「システム設定」 画面	設定内容	
(手順1)ライセンスを登録す	「共通設定」	・LogVillageMGR のインストール直後:	
る	$\rightarrow$	LogVillage へのログイン後、「システム設	
	「ライセンス登録・更新」	定」メニューのみ表示されています。	
		・ライセンスコードを登録	
		ライセンスコードに応じたメニューが表示され	
		ます。	
(手順 2)LogVillagePS を登録	「共通設定」	・LogVillagePSの登録:	
する	$\rightarrow$	LogVillagePS 側よりを登録することで	
	「ポーリングサーバ」	"ステータス=承認済み"となり登録が完了	
(手順5)管理対象 PC を登録	「共通設定」	• 一括登録:	
する	$\rightarrow$	CSV ファイルより一括登録	
	「管理対象 PC」	・ 一台づつ登録 :	
		本画面より登録	
		• 自動登録 :	
		管理対象 PC 自動設定ツール(オプション)に	
		より自動登録	
(手順6)ログ収集のスケジュ	「グループ単位設定」	・グループ別に設定可能	
ールを設定する	$\rightarrow$	・ログの種類別に設定可能	
	「ログ収集スケジュール」		

### 【メモ】

初期設定が全て完了するまで、サイドメニュー上部に「初期設定」メニューが表示されます。

そのため、以下の設定項目が「初期設定」と「共通設定」または「グループ単位設定」に2重で表示されますので ご注意ください。

・ライセンス登録・更新 ・ポーリングサーバ ・管理対象 PC ・ログ収集スケジュール

2重で表示される設定項目は、どちらをクリックいただいても問題ありません。

## 6-2. LogVillagePS を複数台設置した場合の管理対象 PC との関係

LogVillagePS を複数台設置した場合の管理対象 PC との関係について説明します。

複数のLogVillagePS を設置した場合、各々の管理対象 PC が所属するLogVillagePS を指定してください。

※指定方法

「システム設定」→「管理対象 PC の設定」画面より、各々の管理対象 PC が所属する PS の指定を 行うことができます。

## 6-3. ログ収集の仕組みと注意点

ログ収集の仕組みと注意点について説明します。

## 6-3-1. ログ収集スケジュール

ログ収集スケジュールについて説明します。

LogVillage では、以下のログ収集の種類毎に独立した収集スケジュールを設定出来ます。

ログ収集の種類	関係するログ表示画面	
サービス	(稼働管理)	
	・サービス稼働時間	
インベントリ	(資産管理)	
	・PC 資産管理台帳→ハードウェア台帳	
ウィルス定義ファイル	(稼働管理)	
	セキュリティ対策更新状況	
	→ウィルス対策ソフト定義ファイルの更新状況	
インベントリ	(資産管理)	
	・PC 資産管理台帳→ハードウェア台帳	
アプリケーション	(稼働管理)	
	・アプリケーションインストール履歴	
	・セキュリティ対策更新状況	
	→WindowsUpdateの適用状況	
	(資産管理)	
	・PC 資産管理台帳→ソフトウェア台帳	
	・指定アプリケーションの表示	
外部記憶デバイス	(操作管理)	
	・デバイス接続履歴	
Web アクセス履歴	(操作管理)	
	・Web アクセス履歴	
パフォーマンス・プロセス	(稼働管理)	
	・パフォーマンスログ ・プロセス稼働時間	
イベントログ	(稼働管理)	
	・イベントログ	
	(操作管理)	
	・印刷履歴 ・ログオン・オフ履歴	
ファイル	(ファイル管理)	
	USB 接続の外部記憶デバイスの情報を自動収集する場合は、デバイス情	
	報をチェックしてください。	

※ご購入いただいた機能に限って設定可能です。

## 6-3-2. ログ収集タイミング

ログ収集タイミングについて説明します。

管理対象 PC が LogVillagePS からアクセス出来るネットワーク上に接続されていない間のログ情報 については以下の通りとなります。

- 1) 前回のネットワーク切断時点から再接続時まで遡ってログ情報が収集できる情報
  - ・アプリケーション情報
  - ・イベントログ情報
  - Web アクセス履歴情報
- 2) 接続毎に、最新情報を収集する情報
  - ・WMI 情報
  - ・ウィルス定義ファイル情報
- 3)前回のネットワーク切断時点から再接続時までのログ情報が収集できない情報 ※ログ収集時の情報のみ取得
  - ・外部記憶デバイス情報
  - ・パフォーマンス・プロセス情報
  - ・サービス情報
  - ・ファイル情報

### 7. 管理対象 PC の設定変更

管理対象 PC の設定変更について説明します。

#### 前提条件

・管理対象 PC がネットワークに参加している事

※「3-2. LogVillagePS→管理対象PCへのアクセス確認」を参照してください。

・管理対象 PC の「ファイルとプリンタ共有」がインストールされている事
 使用中の「ローカルエリア接続」(または「ワイヤレスネットワーク接続」など)に
 「Microsoft ネットワーク用ファイルとプリンタ共有」と「インターネットプロトコル」がインストールされており、かつ、有効になっている事が前提条件です。

🕹 ローカル エリア接続のフロパティ 🛛 🥐 🗙
全般 詳細設定
接続方法:
IIII VMware Accelerated AMD PCNet Adapti 構成( <u>C</u> )
この接続は次の項目を使用します(2):
✓ ■Microsoft ネットワーク用クライアント
✓ ■ Microsoft ネットワーク用ファイルとプリンタ共有
✓ ■ 005 バケット スケンユーラ ✓ 3=インターネット プロトコル (TCP/IP)
インストール(1)
<ul> <li>□ 接続時に通知領域にインジケータを表示する(W)</li> <li>☑ 接続が限られているか利用不可能な場合に通知する(M)</li> </ul>
 OK キャンセル

「ローカルエリア接続」(または「ワイヤレスネットワーク接続」など)が無効になっている場合 は、ネットワーク接続ができない状態です。有効にしてください。

名前 LAN またけご 速くいか。	種類	状態
▲ローカル エリア接続 ▲ローカル エリア接続 3 (1) ワイヤレスネットワーク接続	エクト LAN または LAN または 洗 LAN または	無効 無効 無効

※「Microsoft ネットワーク用クライアント」と「Microsoft ネットワーク用ファイルとプリンタ 共有」の詳細に関しては、以下の URL をご参照ください。

ネットワークとダイヤルアップ接続を構成する

http://technet.microsoft.com/ja-jp/library/cc758082(WS.10).aspx

## 7-1. 設定変更の方法

設定変更の方法について説明します。

1) ActiveDirectory 環境の場合

グループポリシー機能により設定変更が可能です。

※「7-4. ActiveDirectory 環境での管理対象 PC 設定内容」をご参照ください。

 WorkGroup 環境で管理対象 PC の管理者アカウント、パスワード情報を有する場合 管理対象 PC 自動設定ツール(オプション)にて自動設定が可能です。
 ※「9. 管理対象 PC 設定ツール(オプション)」をご参照ください。

3) WorkGroup 環境で管理対象 PC の管理者アカウント、パスワード情報を有しない場合 管理対象 PC 自動設定ツール(オプション)にて、管理者アカウント、パスワードの自動生成およ び自動設定が可能です。

※「9. 管理対象 PC 設定ツール(オプション)」をご参照ください。

4) その他

WorkGroup 環境での管理対象 PC に対するマニュアル操作での設定変更となります。 ※「7-3. WorkGroup 環境での管理対象 PC 設定内容」をご参照ください。

# 7-2. WorkGroup 環境での管理対象 PC 設定内容

WorkGroup 環境での管理対象 PC 設定内容について説明します。

手動で管理対象 PC の設定内容を変更する場合、以下の項目を変更します。

	1	リモートレジストリーサービス	
	目的	アプリケーション情報など、レジストリ情報を必要とするログの収集が可能となります。	
	設定内容 ・「サービス」の以下を「自動」「開始」に変更します。 「Remote Registry」		
	2	アカウント・ログオン・ログ	
	目的	ログオン・ログオフの履歴が残るように変更します。	
□ 設定内容 ・「ローカル セキュリティ ポリシー」の以下の「成功」を有効にします。		・「ローカル セキュリティ ポリシー」の以下の「成功」を有効にします。	
		「アカウントログオンイベントの監査」	
		「ロクオンイベントの監査」	
	3	ネットワークアクセス時のアカウント認証方法	
	目的	LogVillagePSからの通信に必要な設定で、ネットワークログオンの認証方法を変更します。	
日前 こう		・「ローカル セキュリティ ポリシー」の以下を「クラシック - ローカル ユーザーがローカル ユーザー	
		として認証する」に変更します。	
		「ネットワーク アクセス:ローカル アカウントの共有とセキュリティ モデル」	
	4	4 DCOM リモート起動のアクセス許可	
	目的	WI(ハードウェア台帳など)のWI情報を必要とするログの収集が可能となります。	
п	設定内容	・「コンポーネントサービス」の「起動とアクティブ化のアクセス許可」で以下の「許可」を有効にしま +	
_		9。	
		「リモートからのアクティブ化」	
		・「このコンピュータ上で分散 COM を有効にする」を有効にします。	
	5	ファイアウォール	
	目的	LogVillagePS からの通信に必要な設定で、ログ収集に必要な通信をブロックしないように変更します。	
	設定内容	・以下を無効にします。	
		「許可されたプログラムの一覧にあるプログラムも含め、すべての着信接続をブロックする」	
		・「例外」で以下を有効にします。	
		「Windows Management Instrumentation (WMI)」、「ファイルとプリンタの共有」	
	6	UAC 機能の停止	
	目的	LogVillagePSからの情報収集に必要な設定で、管理者への昇格を求めない状態に変更します。	
	設定内容	・「ユーザーアカウント制御の有効化または無効化」の以下のチェックを外します。	
		「ユーザーアカウント制御(UAC)を使ってコンピュータの保護に役立てる」	
		・または「ユーザー アカウント制御殿定の変更」を「通知しない」に変更します。	
		※UACを停止することなくご利用いただくことも可能です。	
		詳細は本項の設定ページをご参照ください。	

### 1) リモートレジストリーサービス

LogVillage では、レジストリより様々なデータを収集しています。このサービスが実行されてい ない場合 PC 利用状況やアプリケーション情報等のデータが収集されません。

① 「サービス」を起動します。

"Windows スタートメニュー"→「コントロールパネル」→「管理ツール」→「サービス」を起 動します。

※「管理ツール」の表示のためには「コントロールパネル」で「小さいアイコン」または「大きいアイコン」の選択が必要です。

② 「Remote Registry」を変更します。

「Remote Registry」をダブルクリックします。

タートアップの種類が「自動」以外の場合は、「自動」に変更します。 「OK」をクリックします。

ーカル コンピュ・	ーター) Remote Registry のプロパティ
≧般 ┃ログオン┃@	回復 依存関係
サービス名:	RemoteRegistry
表示名:	Remote Registry
[党8月:	リモートユーザーがこのコンピューターのレジスドリ設定を変更で
実行ファイルのパス C:¥Windows¥syst	: tem32¥svchost.exe -k regsvc
スタートアップの	自動
サービスの状態:	<u>ッナオクションの構成の詳細</u> を表示しより 開始
開始(S)	<b>停止(T)</b> 一時停止(P) 再開(R)
ここでサービスを開め	ー ーーーー
開始バラメーター(N	0:

### 2) アカウント・ログオン・ログ

LogVillage では、イベントログに書かれたログオン・ログオフ情報を元にログオン履歴を収集しています。この設定が行われていない場合、ログオン履歴が収集されません。

- 「ローカル セキュリティ ポリシー」を起動します。
   "Windows スタートメニュー"→「コントロールパネル」→「管理ツール」→「ローカル セキュリティ ポリシー」を起動します。
   ※「管理ツール」の表示のためには「コントロールパネル」で「小さいアイコン」または「大きいアイコン」の選択が必要です。
- ② 「監査ポリシー」を開きます。
   「セキュリティの設定」→「ローカル ポリシー」→「監査ポリシー」を開きます。
- ③ 「アカウントログオンイベントの監査」を変更します。
   「アカウントログオンイベントの監査」の「成功」にチェックを入れ、「OK」をクリックします。

アカウント ログオン イベントの監査のプロパティ	? ×
ローカル セキュリティの設定  説明	
アカウント ログオン イベントの監査	
次の場合に監査する: ▼ 成功(S) 「 失敗(F)	監査ポリシーを上書きするよう構成 <sup>ます。</sup> ベ <u>ントの監査</u> を参照してください。
ОК	

④ 「ログオンイベントの監査」を変更します。

「ログオンイベントの監査」の「成功」にチェックを入れ、「OK」をクリックします。

ログオン イベントの監査のプロパティ	? X
ローカルセキュリティの設定 説明	
ログオン イベントの監査	
次の場合に監査する	
▶ 成功(S) □ 失敗(F)	
この設定は、他のポリシーがカテゴリ レベルの監査ポリシーを上書きするよう構     されている場合は、強制されない場合があります。     詳細な情報については ログオン イベントの監査を参照してください。(Q921468	或))
OK	∃(A)

【ご注意ください】

上述の設定によりイベントログのセキュリティログにはLogVillagePSからのアクセスに対しても ログが残ります。

このため、ユーザーのアクセスログを保存するために、セキュリティログの最大サイズを変更してください。

※セキュリティログの「ログサイズ」変更方法

"Windows スタートメニュー"→「コントロールパネル」→「管理ツール」→「イベント ビュ ーア」を起動します。

※「管理ツール」の表示のためには「コントロールパネル」で「小さいアイコン」または「大きいアイコン」の選択が必要です。

「イベント ビューア」→「Windows ログ」→「セキュリティ」を右クリック「プロパティ」 を選択します。

「ログサイズ」の「最大ログ サイズ」を 「(任意の数値)KB」に変更し、「OK」をクリックします。(推奨値 163,840KB)

※セキュリティログがいっぱいになる状態が発生する場合には、この値をさらに大きいものに変更します。 ※「イベントログサイズが最大値に達したとき」は、お客様のポリシーに合わせて設定ください。

ログのプロパティ - セ	キュリティ (種類: 管理)	×
全般		
フル ネーム(F):	Security	
ログのパス(L):	%SystemRoot%#System32#Winevt#Logs#Security.evtx	
ログのサイズ:	20.00 MB(20,975,616 /ኁ፝イト)	
作成日時:	2011年12月9日 18:31:20	
更新日時:	2017年6月27日 13:03:13	
アクセス日時	2011年12月9日 18:31:20	
▶ ログを有効にする()	E)	
最大ログ サイズ (KB)	)(X): 163840 <u>↔</u>	
イベント ログ サイズか	「最大値に達したとき」	
○ 必要に応じて ○ ノベンホキト目	イベントを上書きする(最も古いイベントから)(W) 舞舎したい、空口がなアーカイゴオろ(A)	
C イベントを上書	きさいはい (ログセアーカイフラる (n) 書きしな() (ログは手動で消去)(N)	
		┙╽
<u>}</u>	OK キャンセル 適用(P)	

- 3) ネットワークアクセス時のアカウント認証方法
- 「ローカル セキュリティ ポリシー」を起動します。
   "Windows スタートメニュー"→「コントロールパネル」→「管理ツール」→「ローカル セキュリティ ポリシー」を起動します。
   ※管理ツール」の表示のためには「コントロールパネル」で「小さいアイコン」または「大きいアイコン」の選択が必要です。
- ② 「クラシック-ローカル ユーザーがローカル ユーザーとして認証する」を変更します。
   「セキュリティの設定」→「ローカルポリシー」→「セキュリティオプション」を開きます。

「ネットワーク アクセス:ローカル アカウントの共有とセキュリティ モデル」をダブルク リックします。

「クラシック - ローカル ユーザーがローカル ユーザーとして認証する」に変更し「OK」を クリックします。

ネットワーク	アクセス: ローカル アカウントの共有とセキュリティ モデルの <u>?</u> 🗙
ローカル セキ	Fュリティの設定  説明
1	ネットワーク アクセス: ローカル アカウントの共有とセキュリティ モデル
05990 -	ローカル ユーザーがローカル ユーザーとして認証する
	OK         キャンセル         適用(A)

#### 4) DCOM リモート起動のアクセス許可

WIIによるデータの収集のため、リモートからの起動許可が必要になります。 またLogVillage では、このWII情報を基本としているため、WII情報が収集されない場合、それ 以外のすべての情報を正しく収集することが出来ません。

通常この設定は行われていないため必ず設定変更が必要です。

 「コンポーネントサービス」を起動します。
 "Windows スタートメニュー"→「コントロールパネル」→「管理ツール」→「コンポーネント サービス」を起動します。
 ※「管理ツール」の表示のためには「コントロールパネル」で「小さいアイコン」または「大きいアイコン」の選択が必要で す。

② 「マイコンピュータ」のプロパティを開きます。

「コンソール ルート」→「コンポーネント サービス」→「コンピュータ」→「マイ コンピ ュータ」を開きます。

「マイコンピュータ」を右クリックし「プロパティ」をクリックします。

ションポーネントサービス		_ 🗆 ×
シファイル(F) 操作(A) 表示(V) ウィンドウ(W) ヘルプ(H)		_ <del>_</del> _ ×
◆ ◆   2 〒   ★ ◎ @   2 〒 11 11 11 11 11 11 11 11 11		
□コンソールルート	操作	
日 <sup>(1)</sup> コンポーネント サービス すべてのコンポーネントの更新(A)	コンピューター	<b></b>
	他の操作	×.
□ ○ ★ + · · · · · · · · · · · · · · · · · ·		
プロパティ(R)		
<u>د کار کار کار کار کار کار کار کار کار کار</u>		

③ 「起動とアクティブ化のアクセス許可」の「制限の編集」を変更します。
 「COM セキュリティ」タブを開き、「起動とアクティブ化のアクセス許可」の「制限の編集」をクリックします。

マイコンピューターのプロパティ ? ×
全般  オブション   既定のプロパティ   既定のプロトコル COM セキュリティー //ISDTC
アクセス許可 アプリケーションにアクセスできる既定のユーザーを変更できます。アプリケーションに 対するアクセス許可の制限を、そのアプリケーションで設定することもできます。 警告、アクセス許可を変更すると、アプリケーションの開始、接続、機能、 およびセキュリティで保護された実行に影響する可能性があります。
制限の編集(L) 既定値の編集(E)
起動とアクティブ化のアクセス許可 アプリケーションを起動したりオブジェクトをアクティブにしたりできる既定のユーザーを 変更できます。アプリケーションに対するアクセス許可の制限を、そのアプリケーショ ンで設定することもできます。
<del>制限の編集(0</del> 既定値の編集(D)
<u>プロパティの設定の詳細</u> を表示します。
OK キャンセル 適用(A)

LogVillage で使用するユーザーまたはグループをクリックします。

「起動許可」 にLogVillagePS からの接続に使用されるユーザーまたはグループ名が表示されない場合は、「追加」 を クリックし、アカウント名を入力し、「OK」 をクリックします。

「許可」列の「リモートからの起動」にチェックを入れます。

「許可」列の「リモートからのアクティブ化」にチェックを入れ、「OK」をクリックしま す。

Everyone LV87400732 (machapuchare¥LV87400732)						
Administrators (machapuchare¥/	Administrators)					
Service Cog Osers (machap	uchare¥Distributed	COM Users)				
	追加(D)	肖J『涂(R)				
dministrators のアクセス許可(P)	許可	拒否				
ローカルからの起動 リモートからの起動 ローカルからのアクティブ化 リモートからのアクティブ化	<b>SSS</b>					

④ 「このコンピュータ上で分散 COM を有効にする」を変更します。
 「既定のプロパティ」タブを開きます。
 「このコンピュータ上で分散 COM を有効にする」にチェックが入っている事を確認し、
 「OK」をクリックします。



設定完了後 OS の再起動が必要です。

#### 5) ファイアウォール

LogVillagePS から管理対象 PC への接続を許可する必要があります。 この設定が行われていない場合、情報を収集することが出来ません。 また、LogVillagePS 以外の PC からのアクセスを禁止できるよう「スコープの変更」を行うことを 推奨いたします。

#### 【ご注意ください】

Windows ファイアウォール機能以外のウイルス対策ソフト等のファイアウォール製品が有効となっ ている場合、当該ファイアウォール製品にて同様の設定変更が必要となります。

#### 【メモ】

Windows ファイアウォール機能を利用していない(無効)場合は、以下の設定は必要ありません。

Windows ファイアウォールの種類として「パブリック ネットワーク」と「ホーム ネットワークま たは社内 (プライベート) ネットワーク」があり、「パブリック ネットワーク」とは、空港、喫 茶店など、公共のネットワークを指しています。

LogVillage は社内環境にてご利用いただく事を想定しているため、「プライベート ネットワーク」でご利用いただく事を推奨いたします。

※「ホーム ネットワークまたは社内(プライベート)ネットワーク」と「パブリック」の設定については、後述の 「Windows7 のネットワーク設定とWindows ファイアウォールの関係」をご覧ください。

「Windows ファイアウォール」を起動します。
 "Windows スタートメニュー"→「コントロールパネル」→「Windows ファイアウォール」を起動します。

※ Windows ファイアウォール」の表示のためには「コントロールパネル」で「小さいアイコン」または「大きいアイコン」の選択が必要です。

 「許可されたプログラムの一覧にあるプログラムも含め、すべての着信接続をブロックする」 を確認します。

「Windows ファイアウォールの有効化または無効化」をクリックします。



接続中ネットワークの「許可されたプログラムの一覧にあるプログラムも含め、すべての着 信接続をブロックする」にチェックが無い事を確認し、「OK」をクリックします。



「Windows Management Instrumentation (WMI)」を変更します。
 「Windows ファイアウォールを介したプログラムまたは機能を許可する」をクリックします。



接続中ネットワークの「Windows Management Instrumentation (WMI)」にチェックを入れます。

				×
G ♥ ● Windows ファイアウォール ・ 許可されたプログラム	-	→ □>トロ-	ール パネルの	٩
Windows ファイアウォール経由の通信をプログラムに許す 許可されたプログラムおよびポートを追加、変更、または プログラムノニ海信を許可する金融性の詳細	可します 削除するには、[設定の変更] を	2クリックします	•	
デロされたプログラムおよび機能(A):		DALUGRA(N)		
名前	ホーム/社内 (プライベート)	パブリック 🔺	]	
□ BranchCache - コンテンツ取得 (HTTP を使用)				
□ BranchCache - ピア検出 (WSD を使用)				
□ BranchCache - ホスト型キャッシュ クライアン…			J	
□ BranchCache - ホスト型キャッシュ サーバー (				
□iSCSI サービス				
Media Center Extender				
□ Netlogon サービス				
□ Secure Socket トンネリング フロトコル				
			1	
	[ 詳細(L)	削除(M)	]	
	別のプログ	ラムの許可(R)		
	ОК	キャンセル		

④ 「ファイルとプリンターの共有」を変更します。
 接続中ネットワークの「ファイルとプリンターの共有」にチェックを入れ、全ての画面を「OK」で閉じます。

			- • ×
G ● Windows ファイアウォール ・ 許可されたプログラム		<ul> <li>✓</li> <li>✓</li></ul>	ルパネルの 🔎
Windows ファイアウォール経由の通信をプログラムに許 許可されたプログラムおよびポートを追加、変更、または	可します 削除するには、[設定の変更	町 をクリックします。	
プログラムに通信を許可する危険性の詳細		😚 設定の変更(N)	]
許可されたプログラムおよび機能(A):			
2 <u>m</u>	<u>ホーレ/注内(プライベー)</u>		
☑ファイルとプリンターの共有			
■ リモート アシスタンス			
ロリエート サービフ管理			
ロリモート ボリューム管理			
ロルーティングとリモート アクセス			
ロワイヤレス ポータブル デバイス			
□分散トランザクション コーディネーター			
	[] 詳細(L	_ <b>)</b> 削除(M)	
	別のプロ	コグラムの許可(R)	]
	ОК	キャンセル	]

6) UAC(ユーザアカウント制御)機能の停止

UAC 機能を停止するように変更します。

UAC 機能を停止せずにご利用になることも可能です。

その場合は、以下の「■UAC機能を停止せずに利用する方法」をご参照ください。

① 「ユーザー アカウント」を起動します。

"Windows スタートメニュー"→「コントロールパネル」→「ユーザー アカウント」を起動し ます。

※「ユーザー アカウント」の表示のためには「コントロールパネル」で「小さいアイコン」または「大きいアイコン」の選 択が必要です。

② 「ユーザー アカウント制御設定の変更」を変更します。





下図が表示された場合は、「はい」をクリックします。



スライダのつまみを一番下「通知しない」まで下げ、「OK」をクリックします。

😯 ユーザー アカウント制御の設定		- • •
コンピューターに対する ユーザー アカウント制 の防止に役立ちます。 ユーザー アカウント制	5変更の通知を受け取るタイミングの選択 抑を使用すると、問題を起こす可能性があるプログラムからのコンピューターの <u>朝設定の詳細を表示</u>	変更
常に通知する		
	以下の場合でも通知しない:	
	<ul> <li>プログラムがソフトウェアをインストールしようと する場合、またはコンピューターに変更を加えよう とする場合</li> </ul>	=
	<ul> <li>ユーザーが Windows 設定を変更する場合</li> </ul>	
	<ul> <li>         ・ 推奨されません。ユーザー アカウント制御でサポー トされない、Windows 7 用に保証されていないプ ログラムを使用する場合にのみ選択してください。     </li> </ul>	
通知しない		
	<b>*</b> *アンセ	

※以下のダイアログが表示される場合があります。

その場合は「ユーザーアカウント制御(UAC)を使ってコンピュータの保護に役立てる」のチェックを外し、「OK」をクリックします。

ユーザー アカウント制御 (UAC) を有効にして、お使いのコンピュータをより安全にします。 ユーザー アカウント制御 (UAC) は、お使いのコンピュータに許可のない変更が行われるのを防ぐのに役立 ちます。お使いのコンピュータを保護するために、UAC を有効にしておくことをお勧めします。
□ ユーザー アカウント制御 (UAC) を使ってコンピュータの保護に役立たせる
OK キャンセル

「はい」をクリックします。



#### ■UAC機能を停止せずに利用する方法

レジストリキーを編集し、リモートアクセスが行われた際にUAC機能を無効にする設定を行います。

レジストリはWindows の構成情報が格納されているデータベースです。 レジストリの編集内容に問題があると、システムが正常に動作しなくなる場合があります。 弊社ではレジストリの編集による如何なる問題に対しても補償いたしかねますので、 レジストリの編集はお客様の責任で行っていただくようお願いいたします。 なお、レジストリの編集前に必ずバックアップを作成することを推奨いたします。 バックアップの作成方法については、下記の<レジストリのバックアップ方法>をご参照 ください。

#### ① レジストリエディタを開く

[スタート] メニューから [検索] ボックスに「regedit.exe」と入力し、[Enter]を押します。 ※管理者のパスワードを要求するダイアログ ボックスが表示された場合はパスワードを入力 し[OK] をクリックしします。

確認を要求するダイアログ ボックスが表示された場合は [続行] をクリックします。

②以下の編集を行います。

しいごフトリの埋正	HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersi
レンストリの場所	on¥policies¥system
値の名前	LocalAccountTokenFilterPolicy
値のデータ	1

<レジストリのバックアップ方法>

- 1) レジストリエディタを開く ※手順は、上記①「レジストリエディタを開く」をご参照ください。
- 2) 左ペインより、以下のキーを右クリックし「エクスポート」を選択

 ${\sf HKEY\_LOCAL\_MACHINE} \\ {\sf SOFTWARE} \\ {\sf Microsoft} \\ {\sf Windows} \\ {\sf CurrentVersion} \\ {\sf Policies} \\ \\ {\sf System} \\$ 

3) 任意の名前を付けて保存

## 7-3. ActiveDirectory 環境での管理対象 PC 設定内容

ActiveDirectory 環境での管理対象 PC 設定内容について説明します。

グループポリシーを変更することにより、管理対象PCの設定を行います。 LogVillageを導入する環境により、参照先が異なりますのでご注意ください。

Directory 上に作成するユーザーの権限				
Domain Adr	nins			
参照先1.	7-3-1. グループポリシー設定変更項目			
参照先2.	7-3-2-1.Active Directory上でDomain Admins 権限を持ったユーザーの作成と LogVillage への登録			

Directory 上に作成するユーザーの権限					
00の管理:	OUの管理者権限				
参照先1.	7-3-1. グループポリシー設定変更項目				

参照先2. 7-3-2-2. Active Directory 上で OU の管理者権限を持ったユーザーの作成と LogVillage への登録

# 7-3-1. グループポリシー設定変更項目

グループポリシーで管理対象 PC の設定内容を変更する場合、以下の項目を変更します。

	1	リモートレジストリーサービス
	目的	アプリケーション情報など、レジストリ情報を必要とするログの収集が可能となります。
	設定内容	・「システムサービス」の以下を「自動」に定義します。
		「Remote Registry」
	2	アカウント・ログオン・ログ
_	目的	ログオン・ログオフの履歴が残るように変更します。
	設定内容	・「ローカルポリシー」の以下を「成功」に定義します。
		「アカウント ログオンイベントの監査」、「ログオンイベント の監査」
		・「セキュリティログの最大サイズ」を変更します。
	3	ネットワークアクセス時のアカウント認証方法
_	目的	LogVillagePSからの通信に必要な設定で、ネットワークログオンの認証方法を変更します。
Ш	設定内容	・「ローカルポリシー」の以下を「クラシックーローカルユーザーがローカルユーザーとして認証する」に
		定義します。
		「ネットワークアクセス:ローカルアカウントの共有とセキュリティモデル」
	4	DCOM リモート起動のアクセス許可
	<b>4</b> 目的	DCOM         リモート起動のアクセス許可           WII (ハードウェア台帳など)のWII 情報を必要とするログの収集が可能となります。
_	<b>4</b> 目的 設定内容	DCOM         リモート起動のアクセス許可           WII (ハードウェア台帳など)のWII 情報を必要とするログの収集が可能となります。           ・「ローカルポリシー」の「DCOM: セキュリティ記述子定義言語 (SDDL) 構文でのコンピュータ起動制限」
	<b>4</b> 目的 設定内容	DCOM         リモート起動のアクセス許可           WII (ハードウェア台帳など)のWII 情報を必要とするログの収集が可能となります。           ・「ローカルポリシー」の「DCOM: セキュリティ記述子定義言語(SDDL)構文でのコンピュータ起動制限」の以下を全ての項目で「許可」に定義します。
	<b>4</b> 目的 設定内容	DCOM         リモート起動のアクセス許可           WII (ハードウェア台帳など)のWII 情報を必要とするログの収集が可能となります。           ・「ローカルポリシー」の「DCOM: セキュリティ記述子定義言語 (SDDL) 構文でのコンピュータ起動制限」の以下を全ての項目で「許可」に定義します。 「Administrators」           「Administrators」
	<b>4</b> 目的 設定内容	DCOM         リモート起動のアクセス許可           WII (ハードウェア台帳など)のWII 情報を必要とするログの収集が可能となります。           ・「ローカルポリシー」の「DCOM: セキュリティ記述子定義言語 (SDDL) 構文でのコンピュータ起動制限」の以下を全ての項目で「許可」に定義します。 「Administrators」           ・「分散 COM 設定用*. adm ファイル」を配置し、「管理用テンプレート」に追加し、「有効」に定義します。
	4 目的 設定内容	DCOM         リモート起動のアクセス許可           WII (ハードウェア台帳など)のWII 情報を必要とするログの収集が可能となります。           ・「ローカルポリシー」の「DCOM: セキュリティ記述子定義言語 (SDDL) 構文でのコンピュータ起動制限」の以下を全ての項目で「許可」に定義します。 「Administrators」           ・「分散 COM 設定用*.adm ファイル」を配置し、「管理用テンプレート」に追加し、「有効」に定義します。           す。           ファイアウォール
	4 目的 設定内容 5	DCOM リモート起動のアクセス許可         WII (ハードウェア台帳など)のWII 情報を必要とするログの収集が可能となります。         ・「ローカルポリシー」の「DCOM: セキュリティ記述子定義言語 (SDDL) 構文でのコンピュータ起動制限」の以下を全ての項目で「許可」に定義します。         の以下を全ての項目で「許可」に定義します。         「Administrators」         ・「分散 COM 設定用*. adm ファイル」を配置し、「管理用テンプレート」に追加し、「有効」に定義します。         す。         ファイアウォール         」onVillangPS からの通信に必要な設定で、ログ収集に必要な通信をブロック」ないとうに変更します。
	4 目的 設定内容 5 目的 設定内容	DCOM リモート起動のアクセス許可         WII (ハードウェア台帳など)のWII 情報を必要とするログの収集が可能となります。         ・「ローカルポリシー」の「DOOM: セキュリティ記述子定義言語 (SDDL) 構文でのコンピュータ起動制限」の以下を全ての項目で「許可」に定義します。         「Administrators」         ・「分散 COM 設定用*. adm ファイル」を配置し、「管理用テンプレート」に追加し、「有効」に定義します。         す。         ファイアウォール         LogVillagePS からの通信に必要な設定で、ログ収集に必要な通信をブロックしないように変更します。         ・「ドメインプロファイル」の以下を有効に定義します
	4 目的 設定内容 5 目的 設定内容	DCOM リモート起動のアクセス許可         WII (ハードウェア台帳など)のWII 情報を必要とするログの収集が可能となります。         ・「ローカルポリシー」の「DOOM: セキュリティ記述子定義言語 (SDDL) 構文でのコンピュータ起動制限」の以下を全ての項目で「許可」に定義します。         「Administrators」         ・「分散 COM 設定用*. adm ファイル」を配置し、「管理用テンプレート」に追加し、「有効」に定義します。         ファイアウォール         LogVillagePS からの通信に必要な設定で、ログ収集に必要な通信をブロックしないように変更します。         ・「ドメインプロファイル」の以下を有効に定義します         「Windows ファイアウォール:リモート管理の例外を許可する」
	4 目的 設定内容 5 目的 設定内容	DCOM リモート起動のアクセス許可         WII (ハードウェア台帳など)のWII 情報を必要とするログの収集が可能となります。         ・「ローカルポリシー」の「DCOM: セキュリティ記述子定義言語 (SDDL) 構文でのコンピュータ起動制限」の以下を全ての項目で「許可」に定義します。         の以下を全ての項目で「許可」に定義します。         「Administrators」         ・「分散 COM 設定用*. adm ファイル」を配置し、「管理用テンプレート」に追加し、「有効」に定義します。         す。         ファイアウォール         LogVillagePS からの通信に必要な設定で、ログ収集に必要な通信をブロックしないように変更します。         ・「ドメインプロファイル」の以下を有効に定義します 「Windows ファイアウォール: リモート管理の例外を許可する」 「Windows ファイアウォール: ファイルとプリンタの共有の例外を許可する」
	4 目的 設定内容 5 目的 設定内容	DCOM リモート起動のアクセス許可WII (ハードウェア台帳など)のWII 情報を必要とするログの収集が可能となります。・「ローカルポリシー」の「DCOM: セキュリティ記述子定義言語 (SDDL) 構文でのコンピュータ起動制限」 の以下を全ての項目で「許可」に定義します。 「Administrators」・「分散 COM 設定用*. adm ファイル」を配置し、「管理用テンプレート」に追加し、「有効」に定義します。 す。ファイアウォールLogVillagePS からの通信に必要な設定で、ログ収集に必要な通信をブロックしないように変更します。・「ドメインプロファイル」の以下を有効に定義します 「Windows ファイアウォール: リモート管理の例外を許可する」 「Windows ファイアウォール: ファイルとプリンタの共有の例外を許可する」 「Windows ファイアウォール: ポートの例外を許可する」
	4 目的 設定内容 5 目的 設定内容	DCOM リモート起動のアクセス許可WII (ハードウェア台帳など)のWII 情報を必要とするログの収集が可能となります。・「ローカルポリシー」の「DOOM: セキュリティ記述子定義言語 (SDDL) 構文でのコンピュータ起動制限」 の以下を全ての項目で「許可」に定義します。 「Administrators」・「分散 COM 設定用*. adm ファイル」を配置し、「管理用テンプレート」に追加し、「有効」に定義します。ファイアウォールLogVillagePS からの通信に必要な設定で、ログ収集に必要な通信をブロックしないように変更します。・「ドメインプロファイル」の以下を有効に定義します 「Windows ファイアウォール: リモート管理の例外を許可する」 「Windows ファイアウォール: ポートの例外を許可する」 ・以下に「TCP135」を追加します。

※チェックリストとしてご利用ください。

## グループポリシー設定画面「グループ ポリシー管理エディタ」の表示方法

① 「グループポリシーの管理」を起動します。

"Windows スタートメニュー"→「管理ツール」→「グループポリシーの管理」を起動します。

## ② 設定を行うドメイン名または OU を展開します。

③ 変更するポリシーを右クリックし、「編集」をクリックします。

	屋 グルーナ ポリシーの管理				
	🛃 ファイル(F) 操作(A) 表示(V)	ウィンドウ(W) ヘルプ(H)		_ 8 ×	
	🗢 🔿 🖄 📆 🗔 🔀 🖬	3			
	<ul> <li>■ グループ ポリシーの管理</li> <li>□ ▲ フォレスト: 2008AD32Bit.local</li> <li>□ ▲ ドメイン</li> <li>□ ▲ 2008AD32Bit.local</li> </ul>	Default Domair スコープ  詳細   訳 リンク	n Policy 定  委任		
	■ Default Domain Pol ● ■ Domain Controllers ● ■ グループ ポリシー オブ ● ■ デ WMI フィルタ ● ■ スターター GPO	icy 編集(E) 強制(N) ジー → リンクの有効化(L) レポートの(保存(S) ま=○.0	): 2008AD32Bit.lo よび OU がこの GPO にリンクされていま 国本制 (、)	cal マ す(T): リンクの有効化 パス はい 2008AD32Bit.local	
	<ul> <li>国 ワイト</li> <li>説 グループ ポリシーのモデル作成</li> <li>ご グループ ポリシーの結果</li> </ul>	<ul> <li>えこから新しいウィンドウ(W)</li> <li>削除(D)</li> <li>名前の変更(M)</li> </ul>			
		最新の情報(こ更新(F)	★E+E - 次のグループ、ユーザーおよびコンピュー	タにのみ適用されます(S):	
		∧,1,7(H)			
屋グルーナ ポリシーの管理		I L MR Authenticated			
🔜 ファイル(F) 操作(A) 表示(V)	ウィンドウ(W) ヘルプ(H)		_8×		
				2018-201	
ダルーブ ポリシーの管理          ダルーブ ポリシーの管理          フォレスト: 2008AD32Bit.local              マンストン2008AD32Bit.local              マンストン2008AD32Bit.local              アンストン2008AD32Bit.local              アンストン2008AD32Bit.local              アンストン2008AD32Bit.local              アンストン2008AD32Bit.local             アンストン2008AD32Bit.local                 アンストン2008AD32Bit.local             アンストン2008AD32Bit.local             アンストン2008AD32Bit.local             アンストン2008AD32Bit.local             アンストン2008AD32Bit.local             アンストン2008AD32Bit.local             アンストン2008AD32Bit.local             アンストン2008AD32Bit.local             アンストン2008AD32Bit.local             アンストン2008AD32Bit.local             アンストン2008AD32Bit.local             アンストン2008AD32Bit.local             アントン2008AD32Bit.local             アントン2008AD32Bit.local             アントン2008AD32Bit.local             アントン2008AD32Bit.local             アントン2008AD32Bit.local             アントン2008AD32Bit.local	Iogvillage           2.3-7           1564           30100           S           Controller           3000	奏任   [2008AD32Bit.ik び OU がこの GPO (2リンクされていま [ 建和] (ヽ <b>理</b> のグループ、ユーザーおよびコンピュー s 『 削除(R) ィルタ(2リンクされています(W):	ical す(T): リンカの有効化 /パス (はい 2008AD32Bit.local. なにのみ適用されます(S): フロパティ(P)  「 間く(O)	左上図は、Defau Policy (全体) に です。 右下図は、OU名 に、GPO名「logvi	ılt Domain 設定する場合の例 「logvillage」 llage」を作成
GPO エディタを開きます。				設定する埋へ/	の何です
				し、設たりる場合の	פ ט ניפורת

1)リモートレジストリーサービス

「システムサービス」を開きます。
 設定を変更する「グループ ポリシー管理エディタ」を開きます。

「コンピュータの構成」→「ポリシー」→「Windows の設定」→「セキュリティの設定」→ 「システムサービス」の設定を開きます。

∬ グループ ポリシー管理エディタ				_ 🗆 ×
ファイル(F) 操作(A) 表示(V) ヘルプ(H)				
🗢 🔿 🔁 📷 🗟 🖬				
🖂 🛃 コンピュータの構成 📃	サービス名 -	スタートアップ	アクセス許可	
🗆 🚞 ポリシー 🦷	Remote Access Auto Conn	未定義	未定義	
🛛 🖃 🎽 ソフトウェアの設定	Remote Access Connectio	未定義	未定義	
🖂 🧮 Windows の設定	🔞 Remote Procedure Call (R	未定義	未定義	
📄 スクリプト (スタートアップ/シャットダウン)	Remote Procedure Call (R	未完美	<b>半定</b> 業	
🖂 📑 セキュリティの設定	🖲 Remote Registry	自動	未定義	
I I I アカウント ボリシー	Resultant Set of Folicy Fro	不定我	不足我	•
□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	Routing and Remote Access	未定義	未定義	
田 画 監査ボリシー	Secondary Logon	未定義	未定義	
田 副 ユーザー権利の割り当て	Secure Socket Tunneling P	未定義	未定義	
田 副 ゼキュリティ オノンヨン	Security Accounts Manager	未定義	未定義	
田 副 コペント ログ	Server	未定義	未定義	
	Shell Hardware Detection	未定義	未定義	
	SL UI Notification Service	未定義	未定義	
	Smart Card	未定義	未定義	•
	,			

② 「Remote Registry」を設定します。

サービス名「Remote Registry」をダブルクリックします。 「このポリシーの設定を定義する」にチェックを入れます。 「自動」にチェックを入れ、「OK」をクリックします。

Remote Registryのプロパティ	? ×
セキュリティ ポリシーの設定	
Remote Registry	
Cのポリシーの設定を定義する(D)     サードスのスタートアップ モードを選択してください:     A ちちせい)	
● 自動(U) ○ 手動(M)	
○ 無効(S)	
セキュリティの編集(E)	
OK キャンセル 適用(	A)

2) アカウント・ログオン・ログ

「監査ポリシー」を開きます。
 設定を変更する「グループ ポリシー管理エディタ」を開きます。
 「コンピュータの構成」→「ポリシー」→「Windows の設定」→「セキュリティの設定」→
 「ローカルポリシー」→「監査ポリシー」の設定を開きます。

』「グループ ポリシー管理エディタ			
ファイル(F) 操作(A) 表示(V) ヘルブ(H)			
🗢 🔿 🖄 📷 🗙 🗟  🖬			
🕞 👰 コンピュータの構成 📃	ポリシー ト	ポリシー設定	
🛛 🖂 ポリシー 👘	🔤 アカワント ロクオン イベントの監査	<i>[</i> /4,4/]	
🗉 🧮 ソフトウェアの設定		未定義	
🗆 🚞 Windows の設定	┃ 圓ೖ オブジェクト アクセスの監査	未定義	
スクリプト (スタートアップ/シャットダウン)	┃ 圓] システム イベントの監査	未定義	
□ □ □ セキュリティの設定	ディレクトリ サービスのアクセスの監査	未定義	
	「「「「プロセス追随の監査」	未完善	
	◎ ポリシーの変更の監査	未定義	
田町温道がリント	🏭 ログオン イベントの監査	成功	
国 国 ユーサー(単本)(の書)ワヨし 国 国 セキュリティオブション		未定義	
日 日 イベント ログ			
田 🔤 制限されたグループ 🚽			
	,		
	J		J

アカウント ログオンイベントの監査」を設定します。
 ポリシー名「アカウント ログオンイベントの監査」をダブルクリックします。

「これらのポリシーの設定を定義する」にチェックを入れます。

「成功」にチェックを入れ、「OK」をクリックします。

アカウント ログオン イベントの監査のブ	ロパティ		<u>? ×</u>
セキュリティ ポリシーの設定  説明			
アカウント ログオン イベント	∽の監査		
☑ これらのボリシーの設定を定義する 次の場合に監査する:	<u>(D)</u>		
✓ 成功(S) ○ 失敗(F)			
	ОК	キャンセル	適用( <u>A</u> )

「ログオンイベント の監査」を設定します。
 ポリシー名「ログオンイベント の監査」をダブルクリックします。
 「これらのポリシーの設定を定義する」にチェックを入れます。
 「成功」にチェックを入れ、「OK」をクリックします。

ログオン イベントの監査のプロパティ			<u>?×</u>
セキュリティ ポリシーの設定  説明			
ログオン イベントの監査			
<ul> <li>✓ これらのボリシーの設定を定義する 次の場合に監査する:</li> <li>✓ 成功(S)</li> <li>□ 失敗(E)</li> </ul>			
	ок	キャンセル	適用( <u>A</u> )

#### イベントログの修正

※手順③までの設定によりイベントログのセキュリティログにはLogVillagePS からのアクセスに 対してもログが残ります。

このため、ユーザーのアクセスログを保存するために、セキュリティログの最大サイズを変更して ください。

「イベントログ」を開きます。
 「コンピュータの構成」→「ポリシー」→「Windows の設定」→「セキュリティの設定」→
 「イベントログ」の設定を開きます。



②「セキュリティログの最大サイズ」を設定します。

ポリシー名「セキュリティログの最大サイズ」をダブルクリックします。

「このポリシーの設定を定義する」にチェックを入れます。

「(任意の数値)KB」に変更し、「OK」をクリックします。(推奨値 163,840KB)



※セキュリティログの最大サイズまでログが保存された場合の動作は、3種類あります。ポリシーに適した動作を選択してください。

・指定した日数を過ぎたら上書きする

ー定期間のログを必ず残すポリシーの場合は、この設定により指定した日数のセキュリティログが 必ず保存されます。

指定した日数を経過する前にセキュリティログが最大サイズになった場合、管理者権限を持ったユ ーザー以外では OS にログインできなくなります。

指定した日数以上 LogVillage にてセキュリティログを収集していない場合、上書により削除された期間のログが収集できません。

・必要に応じてイベントを上書きする

セキュリティログが最大サイズになった場合、古いログから削除されます。

ー定期間のログを必ず残すポリシーの場合は「指定した日数を過ぎたら上書きする」を選択する必 要があります。

LogVillage にてセキュリティログを収集していない場合、上書により削除された期間のログが収 集できません。

・イベントを上書きしない(手動でログを消去)

セキュリティログを手動で削除する必要があります。

各 PC 毎に手動でイベントログのメンテナンスを行うポリシーの場合のみ、選択してください。

ログが自動的に削除されても問題無い場合は、「必要に応じてイベントを上書きする」を選択して ください。

ログの削除を禁止している場合は、「イベントを上書きしない(手動でログを消去)」を選択して ください。 ※以下では、「指定した日数を過ぎたら上書きする」「7日間」の設定をご案内します。

「セキュリティログの保存日数」を設定します。
 「セキュリティログの保存日数」をダブルクリックします。
 「このポリシーの設定を定義する」にチェックを入れます。
 「(任意の数値)日」に変更し、「OK」をクリックします。



下図が表示されたら「OK」をクリックします。

提案された値の変更		? ×
セキュリティ ログの保存日数 の値が 7 日 (2	変更されたため、次の項目の設	定は提案された値に変更されます。
ポリシー	ポリシー設定	 - 提案された設定
しました ログの保存方法	未定義	指定した日数
•		<b>&gt;</b>
		OK キャンセル(C)

④ 「セキュリティログの保存方法」を設定します。

「セキュリティログの保存方法」をダブルクリックします。

「指定した日数を過ぎたら上書きする」にチェックが入っている事を確認し、「OK」をクリックします。



3) ネットワークアクセス時のアカウント認証方法

「セキュリティオプション」を開きます。

設定を変更する「グループ ポリシー管理エディタ」を開きます。 「コンピュータの構成」→「ポリシー」→「Windows の設定」→「セキュリティの設定」→ 「ローカルポリシー」→「セキュリティオプション」の設定を開きます。

∬ グルーナ ポリシー管理エディタ		
ファイル(F) 操作(A) 表示(V) ヘルプ(H)		
🗢 🔿   📶 🗟 📔 🖬		
🖂 🛃 コンピュータの構成 📃	ポリシー ^	ポリシー設定 ▲
🖂 🛄 ポリシー	🔤 ネットワーク アクセス: SAM アカウントの匿名の列挙を許可しない	未定義
田	📗 🔤 ネットワーク アクセス: ネットワーク認証のために資格情報または .NE	未定義
🖂 🚞 Windows の設定	🔢 🌆 ネットワーク アクセス: リモートからアクセスできるレジストリのパス	未定義
📄 スクリプト (スタートアップ/シャットダウン)	🔢 🔤 ネットワーク アクセス: リモートからアクセスできるレジストリのパスおよ	未定義
🖂 📑 セキュリティの設定		<b>十字</b> 業
🗉 🧱 アカウント ポリシー	■ 🔜 ネットワーク アクセス: ローカル アカウントの共有とセキュリティ モデル	クラシック - ローカル ユーザーがロー
🗆 🖬 ローカル ポリシー	100 ホパラークテンビス 医治モデンビスことの共有	木定義
■ ■ 監査ボリシー		未定義
□ ユーザー権利の割り当て		未定義
□    □    □    □    □    □    □	IIII ネットワーク ヤキョリティ: LAN Manager 認証レベル	未定義
	「「スットワーク ヤキョリティ・ヤキョア BPC を含むクライアント ベースの」	未定義
田 🛁 制成されたクルモノ	「「「ネットワーク ヤキョリティ・ヤキョア RPC を含むサーバー ベースの N	未定義
		*定義 1

「ネットワーク アクセス: ローカル アカウントの共有とセキュリティ モデル」を設定します。

「ネットワーク アクセス: ローカル アカウントの共有とセキュリティ モデル」をダブルク リックします。

「このポリシーの設定を定義する」にチェックを入れます。

「クラシックーローカルユーザがローカルユーザとして認証する」が選択されている事を確認し「OK」をクリックします。

ネットワーク アクセス: ローカル アカウン	ノトの共有とセキュ!	ノティ モデルのプロノ	(ታィ 🔹 🔉
セキュリティ ポリシーの設定  説明			
ネットワーク アクセス: ロー:	カル アカウントの共れ	肯とセキュリティ モデル	,
▼ このポリシーの設定を定義する(D) 「クラシック - ローカル ユーザーが	) iローカル ユーザーとi	して認証する	•
	OK	キャンセル	適用(A)

#### 4) DCOM リモート起動のアクセス許可

「セキュリティオプション」を開きます。
 設定を変更する「グループ ポリシー管理エディタ」を開きます。
 「コンピュータの構成」→「Windows の設定」→「セキュリティの設定」→「ローカルポリシー」→「セキュリティオプション」の設定を開きます。

』「グループ ポリシー管理エディタ		
ファイル(F) 操作(A) 表示(V) ヘルプ(H)		
🗢 🔿 🖄 📷 💥 🖼 😖 🛛 🖬		
	ポリシー	ポリシー設定 ▲
□ □ ハリシー	DCOM: セキュリティ記述子定義言語 (SDDL) 構文でのコンピュータ起動制限	O:BAG:BAD:(A;;CCDCLC
<ul> <li>○ Windows の設定</li> <li>スクリプト (スタートアップ/シャットダウン)</li> <li>○ セキュリティの設定</li> <li>○ アカウント ポリシー</li> <li>○ ローカル ポリシー</li> <li>○ 国 監査ポリシー</li> <li>○ 国 ビキュリティオプション</li> <li>○ セキュリティオプション</li> <li>○ セキュリティオプション</li> <li>○ マント ログ</li> <li>#IREされたグループ</li> </ul>	<ul> <li>Microsoft ネットワーク クライアンド・サード パーティ製の SMB サーバーへのパスワー</li> <li>Microsoft ネットワーク クライアンド・サーバーが同意すれば、通信にデジタル署名を</li> <li>Microsoft ネットワーク クライアンド、常に適信にデジタル署名を行う</li> <li>Microsoft ネットワーク サーバー: クライアンドが同意すれば、通信にデジタル署名を</li> <li>Microsoft ネットワーク サーバー: ウライアンドが同意すれば、通信にデジタル署名を</li> <li>Microsoft ネットワーク サーバー: ログオン時間の有効期間が切れるとクライアントを</li> <li>Microsoft ネットワーク サーバー: ログオン時間の有効期間が切れるとクライアントを</li> <li>Microsoft ネットワーク サーバー: ログオン時間の有効期間が切れるとクライアントを</li> <li>Microsoft ネットワーク サーバー: ボンは自信にデジタル署名を行う</li> <li>アカウント: Administrator アカウントの状態</li> <li>アカウント: Administrator アカウント名の変更</li> </ul>	未定義 未定定義 未定定義 未定定義 未未定定義 未 未定定義 + 未定定義 - -

② 「DCOM: セキュリティ記述子定義言語 (SDDL) 構文でのコンピュータ起動制限」を設定します。

ポリシー名「DCOM: セキュリティ記述子定義言語 (SDDL) 構文でのコンピュータ起動制限」 をダブルクリックします。

「このポリシーの設定を定義する」にチェックを入れます。

「セキュリティの編集」をクリックします。


「Administrators」をクリックし、「許可」に全てチェックが入っている事を確認後、「OK」をクリックします。



「OK」をクリックします。



③ 分散 COM 設定用の設定変更用ファイルを配置します。
 設定変更用ファイル(インストール媒体内 Tools フォルダ下の LV\_DCOM. adm)をドメインコントローラーサーバの x: ¥Windows¥inf ヘコピーします。
 ※x は 0S インストールドライブです。

LV\_DCOM. adm は以下の内容のテキストファイルです。

#### CLASS MACHINE

CATEGORY !!LogVillageDCOM

POLICY !!ChangeEnableDCOMPolicy KEYNAME "SOFTWARE¥Microsoft¥Ole" Valuename "EnableDCOM" VALUEON "Y" VALUEOFF "N" END POLICY

END CATEGORY

[strings] LogVillageDCOM="LogVillage 用 DCOM 設定" ChangeEnableDCOMPolicy="LogVillage 用 DCOM 設定"

④ 「LogVillage 用 DCOM 設定」を追加します。
 「コンピュータの構成」→「管理用テンプレート」を開きます。



「管理用テンプレート」を右クリック、「テンプレートの追加と削除」をクリックします。

■ グルーフ ポリシー管理エティタ		
ファイル(F) 操作(A) 表示(V) ヘルプ(H)		
🗢 🔿 🙍 📷 🗟 🖬 🝸		
<ul> <li>日 帰 コンピュータの構成</li> <li>日 一 ポリシー</li> </ul>	🔺 🧧 管理用テンプレート: ローカル :	コンピュータから取得したポリシー定義(ADMX)ファイルです。 ー
<ul> <li>□ □ □ ソフトウェアの設定</li> <li>□ □ □ Windows の設定</li> </ul>	項目を選択すると説明が表示されます。	設定
□ □ □ 管理用テンプレート: ローカル コンピ. I □ □ Windows コンポーネント	ーカから 即 テンプレートの追加と削除(A)	□コントロール パネル □コントコール パネル □システム
<ul> <li></li></ul>	フィルタオプション(0)	<ul> <li>ネットワーク</li> <li>ブリンタ</li> </ul>
	<u>すべてのタスク(K)</u> ・	○ 従来の管理用テンプレート (ADM) ● すべての設定
日	表示(∀) ▶	
● 🤮 基本設定	一覧のエクスポート(L)	
  管理用テンプレートの管理	ヘルプ(H)	

「追加」をクリックします。

テンプレートの追加と削除	×
現在のポリシー テンブレート(C):	
名前	サイズ 変更
UV_Printer	1KB 2008/09/12 15:20
追加(A) 賞/昭余(R)	閉じる(L)
	Mile and

「LV\_DCOM. adm」をクリック後、「開く」をクリックします。

🧾 ポリシー テンプレート			×
00 🕨 - 🗆 -	カル ディスク (C:) ・ Windows ・ int	f • • ▼ 🕢 検索	
🐚 整理 👻 📕 表示	🗧 🚽 📑 新しいフォルダ		0
お気に入りリンク	名前 ^	▼ 更新日時 2008/01/19/23:03 ファイルフォルダ	•  サイズ  •  ▲
📃 デスクトップ	ja-JP	2008/01/19 23:03 ファイル フォルダ	
■ コンピュータ	MSDTC NTDS	2008/01/19 20:30 ファイル フォルダ 2011/02/22 16:50 ファイル フォルダ	
<ul> <li>トキュメノト</li> <li>ドカチャ</li> </ul>	PERFLIB	2008/01/19 20:30 ファイル フォルダ	
	Psched	2008/01/19 20:41 ファイル フォルダ 2008/01/19 20:30 ファイル フォルダ	
→ 最近の変更	TAPISRV	2008/01/19 20:30 ファイル フォルダ	
▶ 検索	TermService	2008/01/19 20:30 ファイル フォルダ 2008/01/19 20:30 ファイル フォルダ	
····		2011/02/22 17:20 ファイル フォルダ	
	LV_DCOM.adm	2011/02/10 21:30 ADM ファイル 2008/09/12 15:20 ADM ファイル	1 KB 1 KB
	LV_PrinterWin7.adm	2011/01/13 19:50 ADM ファイル	1 KB 🚽
フォルダ	^ <u>.</u>		
	ファイル:名(N):	▼ ポリシー テンプレート	<b>•</b>
		開((0)	

FLV_DCOMJ	が一覧に表示された事	事を確認し、	「閉じる」	をクリック	します。
テンプレートの追加と削除		>	<		
現在のポリシー テンプレート(C)	):				
- Lan	サイズ	変更			
LV_DCOM	1KB	2011/02/10 21:30			
E LV_Frinter	1KB	2008/09/12 15:20			
1					
ietn(A) SUR	(2/0)	明((本(1)))			
19/0(A) Hyp.	汞(FV	ାମାତର(L)			

⑤「LogVillage 用 DCOM 設定」を有効に変更します。
 「管理用テンプレート」→「従来の管理テンプレート(ADM)」→「LogVillage 用 DCOM 設定」をクリックします。

びループ ポリシー管理エディタ
ファイノレ(F) 操作(A) 表示(V) ヘルプ(H)
• 🔿 🖄 🖬 📴 🖬 🝸
🖂 💼 税シー 🗾 🧧 LogVillage用DCOM設定
<ul> <li>              97トワコノの設定      </li> <li>             Windows の設定             管理用デンブレード・ローカル コンピュータから取         </li> <li>             Windows コンボーネント             ビ             ゴントロール パネル             ビ             ジンテム             ビ             マンボーネント             ビ             ジンテム             ビ             マンボーネント             ビ             ジンテム             ビ             マンボーネント             ビ             ジンテム             ビ             ジンテム             ビ             ジンテム             ビ             ジンテム             ビ             ジントロール パネル             ビ             ジンテム             ビ             ジンテム             ビ             ジンテム             ビ             ジンタ             ビ             ジンタ             ビ             ジンタ             ビ             ジー</li></ul>
LogVillage用DCOM設定     LogVillage用DCOM設定     マー     マー     マー     マー     ボス     ボス     振張     標準

「LogVillage 用 DCOM 設定」を右クリック「プロパティ」をクリックします。

夏ブルーブ ポリシー管理エディタ			
ファイル(F) 操作(A) 表示(V) ヘルブ(H)			
🗢 🔿 🙍 🖬 🖺 🗟 🖬 🝸			
	🧧 LogVillage用DCOM設定		
E = I = = = Windows の設定 □ = = 管理用テンプレート: □ーカル コンピュータから取	LogVillage用DCOM設定	- <u> 設定</u>	
■ ■ Windows コンポーネント ■ ■ コントロール パネル	<u>プロパティ</u> の表示		フィルタ有効(F) フィルタ オプション(O)…
<ul> <li>Эле и ний</li> <li>Эле и ний</li> <li>Эле и ний</li> </ul>	[		フィルタの再適用(E)
田 🎬 ネットワーク			すべてのタスク(K) 🕨 🕨
□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	注意: このレジストリ設定はポリシー キーに   格納されていないため、優先される設定で   キュレンナンわせす。スッチャーニッジの中す	[	プロパティ(R)
□ Log Village用DCOM設定 □ Log Village用プリンタ設定	のるこのなされます。そのためたこの設定を 実装するグループポリシーオブジェクトが削	1	ヘルプ(H)
🔄 📫 すべての設定 📃 💌	除された場合、この設定は残ります。	•	
	∖拡張√標準/		
1 個の設定			

「有効」	をクリック後、	LOKT	をクリック	します。

LogVillage用DCOM設定のプロ	パティ		? ×
設定  説明			
🔁 LogVillage用DCOM設定			
○ 未構成(C) ● 有効(E)			
]			
前の設定(P)	)次の設定(N)		
	ОК	キャンセル	適用(A)

#### 5) ファイアウォール

「ドメインプロファイル」を開きます。
 設定を変更する「グループ ポリシー管理エディタ」を開きます。

「コンピュータの構成」→「ポリシー」→「管理用テンプレート」→「ネットワーク」→ 「ネットワーク接続」→「Windows ファイアウォール」→「ドメインプロファイル」の設定 を開きます。



Windows ファイアウォール:着信ファイルとプリンタの共有の例外を許可する」を設定します。

設定名「Windows ファイアウォール:着信ファイルとプリンタの共有の例外を許可する」をダ ブルクリックします。

「有効」をクリックします。

「要請されない着信メッセージを許可する IP アドレス」に \* を入力し、「OK」をクリック します。

Windows ファイアウォール: 若信ファイルとプリンタの共有の例外を許可するのブロ... 💡 🗙

設定  説明   コメント			
📑 Windows ファイアウォール:	着信ファイルとプリンタの	)共有の例外を許可	142
C 土井式(C) ● 有効(E) ● 無効(D)			
要請されない着信メッセージを	許可する IP アドレス:		-
構文: どのネットワークからのメッセージ あるいは、数字または次のもの コンマで区切られた一覧を入力 1000:1 などの IP アドレス。 10230/24 などの JP アドレス。 10230/24 などの サブネット "localsubnet" という文字列 サポートされるパージョン:	も許可する場合は、"* の組み合わせを含む りしてください。 の説明。 りし	** と入力してくださ(	,\ <sub>0</sub>
Microsoft Windows XP Profe	essional SP2 以降		
前の設定(P)	次の設定(N)		
	ОК	キャンセル	適用(A)

※各管理対象 PC 上で、本設定をポーリングサーバーに対してのみ許可する場合は、\* をポーリングサーバーのアドレスに変更します。(スコープ設定)

③ 「Windows ファイアウォール:ローカルポートの例外を許可する」を設定します。
 設定名「Windows ファイアウォール:ローカルポートの例外を許可する」をダブルクリックします。

Windows ファイアウォール:ローカル ボートの例外を許可するのブロパティ	? ×
設定  説明   コメント	
🛅 Windows ファイアウォール・ローカル ポートの例外を許可する	
C 土穂(C) 有効(E) 一無次(D)	
サポートされるバージョン	
Microsoft Windows XP Professional SP2 以降	
前の設定(P) 次の設定(N)	
	(A)

「有効」をクリック後、「OK」をクリックします。

④ 「Windows ファイアウォール:着信ポートの例外を定義する」を設定します。
 設定名「Windows ファイアウォール:着信ポートの例外を定義する」をダブルクリックします。

「有効」をクリックし、「ポートの例外定義」の「表示」をクリックします。

Windows ファイアウォール: 若信ボートの例外を定義するのブロパティ	? ×
設定  説明   コメント	
🐨 Windows ファイアウォール: 著信ポートの例外を定義する	
● 有効(E)	
ホートの1例外の定義 表示 ポートを聞くかブロックするかほこにはす。	
構文:	
<port>:<transport>:<scope>:<status>:<name></name></status></scope></transport></port>	
<port>は、10 進数のボート番号です。</port>	
<transportとは、「icp」または「udp」のいすれかです。 /Serrenとは、"**"(オペアのネットローク)まそいけ</transportとは、「icp」または「udp」のいすれかです。 	
Nocuper は、* くられてのネットワークのあるには 数字または次のものの組み合わせを含む	
コンマで区切られた一覧です。	
10001 かどの TP つドレフ	
サホートされるハーション: Missess (A Mississes) (P. Professional, CPO, NPS	
Microsoft Windows XF Professional SF2 L/P≩	
OK キャンセル	適用(A)

「追加」をクリックします。

内容の表示	×
ポートの例外の定義	OK キャンセル
	追加(A)
	削//涂(R)

「追加する項目を入力してください」に「135:TCP:\*:enabled:DCOM\_TCP135」を入力し「OK」 をクリックします。

項目の追加	×
追加する項目を入力してください(E):	ок
135:TCP:*:enabled:DCOM_TCP135	キャンセル

※各管理対象 PC にて本設定をポーリングサーバーに対してのみ許可する場合、\*をポーリングサーバーのアドレスに変更して設定します。(スコープ設定)

# 「OK」を2回クリックし、画面を閉じます。

卒の表示		
ートの例外の定義		ОК
135:TCP:*:enabled:DCOM_TCP135		
		<b>追加(A)</b> 削除(R)
dows ファイアウォール: 著信ポートの例外を定義するのプロパティ 🏾 👔	×	
短  説明  コメント  デ Weatow フィノフウト ル またま トロバロス ちつぎます	1	
数定  説明   コメント  ○ Windows ファイアウォール: 著信ポートの例外を定義する ○ 未構成(C) ○ 有効(E) ○ 無効(D)		
<ul> <li></li></ul>		
<ul> <li></li></ul>		
対 印   ユメント       Windows ファイアウォール:着信ポートの例外を定義する      ・ 未構成(C)      ・ 有効(E)      ・ 有効(E)      ・ 無効(D)      ポートを聞くかブロックするが指定します。      構文:     ・ <port><transport><scope><status><name> <fort> は、10 道能のポート番号です。     <fort> は、10 近たのたりと含む        コンマで区切られた一覧です。          10001 ホンドの PD です。         100001 ホンドの PD です。         100000000000000000000000000000</fort></fort></fort></fort></fort></fort></fort></fort></name></status></scope></transport></port>		

⑤ 「Windows ファイアウォール:着信リモート管理の例外を許可する」を設定します。
 設定名「Windows ファイアウォール:着信リモート管理の例外を許可する」をダブルクリックします。

「有効」をクリックします。

「要請されない着信メッセージを許可するアドレス」に \* を入力し「OK」をクリックしま す。



※各管理対象 PC 上で、本設定をポーリングサーバーに対してのみ許可する場合は、\* をポーリングサーバーのアドレスに変更します。(スコープ設定)

以上で「7-4-1-2. グループポリシー設定変更項目 (Windows Server 2008 Active Directory 環 境)」の設定は完了です。

次は「7-4-2. LogVillageMGR に登録いただく各管理対象 PC のユーザー設定項目」を行います。

82

## 7-3-2. LogVillageMGR に登録する管理対象 PC のユーザー設定項目

LogVillageMGR に登録する管理対象 PC のユーザー設定項目について説明します。

Domain Admins 権限を持ったユーザーの作成を行います。

Domain Admins 権限を持ったユーザーを作成できない環境場合、OU レベルで管理者権限を持った ユーザーを作成する事も可能です。

Domain Admins 権限を持ったユーザーの作成方法は、以下を参照してください。
 7-4-2-1. Active Directory 上で Domain Admins 権限を持ったユーザーの作成と LogVillage への登録

・0U レベルで管理者権限を持ったユーザーの作成方法は、以下を参照してください。 7-4-2-2. Active Directory 上で0Uの管理者権限を持ったユーザーの作成とLogVillage への登録

7-3-2-1. Active Directory 上で Domain Admins 権限を持ったユーザーの作成と LogVillage への登録

Active Directory 上で Domain Admins 権限を持ったユーザーの作成と LogVillage への登録につい て説明します。

- ・ユーザー作成
- ・管理対象 PC に、グループ ポリシーを強制再適用する方法
- ・管理対象 PC 上で、設定反映を確認する方法
- ・LogVillage 管理対象 PCの設定に登録する時の注意点
- ・ユーザー作成
- 「Active Directory ユーザーとコンピュータ」起動します。
   "Windows スタートメニュー"→「管理ツール」→「Active Directory ユーザーとコンピュー ター」を起動します。
- ② 新規「ユーザー」を作成します。
   「Users」を選択し、空白部分で右クリック「新規作成」→「ユーザー」をクリックします。

Active Directory ユーザーとコンピューター						
ファイル(F) 操作(A) 表示(V) ヘルプ(H)						
🗢 🔿 🖄 📅 📋 🔯	(= ⇒) 2 💼 🗈 💿 0 💀 😰 🖬 😤 📚 🖆 🍸 2 🍇					
Active Directory ユーザーとコンピュ 日本語を加たクリ 日本語を加たクリ 日本語を加たクリ 日本語を加たクリ 日本語を加たクリ 日本語を加たクリ 日本語を加たります。 日本語を加たります。 日本語を加たりたき作成します。	28.00         3       Administrator         3       Administrator         3       Administrator         3       Administrator         34       Cert Publishe         48       Domain Admi         48       Domain Com	種類 ユーザー ゼキュリティ グル セキュリティ グル	説明 コンピューター/ドメインの管 このガルーブのメンバーは、ド このガルーブのメンバーはディ このガルーブのメンバーは、ド ドメインの首やてのワークステ ドメインのすべてのドメインコ ドメインのすべてのドメインコ ドメインの全ブスト ドメインの全ブスト ドメインの全ブスト ドメインの全ブスト ドメインの全ブスト マンクーブラメンバーは、I このガルーブのメンバーは、I このガルーブのサンバーは、ド スキーマの指定された管理者	<ul> <li>制御の委任(E) 検索(D</li> <li>新規(F成(N)</li> <li>すてのタスク(K)</li> <li>最新の情報に更</li> <li>一覧のエクスポー</li> <li>表示(V)</li> <li>アイコンの整列(D</li> <li>等間際高に整列(E プロパティ(R)</li> <li>ヘルプ(H)</li> </ul>	- コンピューター 連絡先 グループ InetOrgPerson msImaging-PSPs MSMQ キューエイリア フレナー コーザー	γλ

「姓」と「ユーザー ログオン名」に任意のユーザー名を入力し「次へ」をクリックします。 例: logvillage

新しいオブジェクト - ユーザー	× ×
🤱 作成先:	2008R2StaAD.local/Users
<b>女生(L)</b> :	logvillage
名(F):	1=2x71/0:
フル ネーム(A):	logvillage
ユーザー ログオン名(U):  logvillage	@2008R2StaAD.local
, ユーザー ログオン名(Wi	 ndows 2000 より前)(W):
2008R2STAAD¥	logvillage
	< 同ろ(日) (同ろ(日) (アス(N)) キャンパフル 1

「パスワード」と「パスワードの確認入力」に任意のパスワードを入力します。 「ユーザーは次回ログオン時にパスワード変更が必要」のチェックを外します。 「ユーザーはパスワードを変更できない」「パスワードを無制限にする」にチェックを入れ ます。

「次へ」をクリックします。

新しいオブジェクト - ユーザー	×
YF成先: 2008R2StaAD.local/Users	
パスワード(P): ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	
<ul> <li>□ ユーザーは次回□グオン#特にパスワード変更が必要(M)</li> <li>□ <u>ロ</u>ーザーはパスワードを変更できない(S)</li> <li>✓ パスワードを無邦限にする(W)</li> </ul>	
□ アカウントは無効(0)	
〈戻る(B) 次へ(N) > キャンセント	211

設定に間違いが無い事を確認後「完了」ボタンをクリックします。

新しいオブジェクト・	- ユーザー	×
1°F	成先: 2008R2StaAD.local/Users	3
[完了] をクリック	すると、次のオブジェクトが作成されます:	
フル ネーム: log ユーザー ログオ: ユーザーはパスワ パスワードを無罪	ivillage ン名: logvillage@2008R2StaAD.local フードを変更できない 期限にする	×
	< 戻る(B)	第7 キャンセル

③ 権限を付与します。

作成したユーザーを右クリックし「プロパティ」をクリックします。

例:logvillage

I Active Directory ユーザーとコンピューター						
ファイル(F) 操作(A) 表示(V) ヘルプ(H)						
← ⇒ 2 □ 4 □ × □	i 🖬 🗟 🖬	1 🕺 🗽 🛅	7 🗾 🍇			
Active Directory ユーザーとコンピュ	名前	種類	説明			
Instructure directation of 1 y = 20021     Instructure directation of 1 y = 2008R2StaADJocal     Instructure distaADJocal     Instructure directation	Administrator     Administrator     Administrator     Administrator     Allowed ROD     Cert Publishe     Domain Cont     Domain Admi     Domain Cont     Domain Con	12-47- 12-47- セキュリティグル セキュリティグル セキュリティグル セキュリティグル セキュリティグル セキュリティグル セキュリティグル セキュリティグル セキュリティグル 2-47- 2-47- セキュリティグル 2-57- セキュリティグル 2-57- セキュリティグル 2-57- セキュリティグル セキュリティグル	コンピューター/ドメインの管 このグルーブのメンバーは、ド このグルーブのメンバーは、ド このグルーブのメンバーは、ド ドメインの管理者 ドメインの管理者 ドメインの登げスト ドメインの全ゲスト ドメインの全エーザー エンターブライズの管理者 このグルーブのメンバーは、エ このグルーブのメンバーは、エ このグルーブのメンバーは、エ このグルーブのメンバーは、エ このグルーブのメンバーはドメ コンピューター/ドメインのの コピューター/ドメインのの コピューター/ドメインのの コピューター/ドメインのの マカフントを無効にする(S) パスワードのリセット(E) 移動(い) ホーム、ページを閉く(O) メールを送信(A) オペでのタスク(K) ・ すのでのタスク(K) ・ プロパティ(R)			

logvillageወታቢለታィ ? 🗙
ダイヤルイン 環境 セッション リモート制御 リモート デスクトップ サービスのプロファイル 個人用仮想デスクトップ COM+ フロザナ 全般  住所   アカウント   プロファイル  電話   所属されている組織   所属するグループ
所属するグループ(M): 名前 Active Directory ドメイン サービス フォルダー Domain Users 2008R2StaAD.local/Users
<u>注島力四(D)</u> 肖坦彦余(R)
プライマリ グループ: Domain Users
ブライマリグループの設定(S) Macintosh クライアントまたは POSIX 対応のアプリケ ーションがない場合は、プライマリグループを変更する 必要はありません。
のK またなれ、 活田(ム) へルゴ
OK         キャンセル         通用(A)         ヘルプ

「所属するグループ」タブを開き、「追加」をクリックします。

「選択するオブジェクト名を入力してください」に「domain admins」を入力し、「名前の確認」をクリックします。

グループ の選択	? 🗙
オブジェクトの種類の選択(S):   グループ または ビルトイン セキュリティ ブリンシパル 場所の指定(F):	オブジェクトの種類(0)
2008R2StaAD.local	場所(L)
選択するオブジェクト名を入力してください (例)(E):  domain admins	名前の確認(C)
	ОК <b>*</b> +>セル

「domain admins」に下線が表示された事を確認後、「OK」をクリックします。

ヴルーナ の選択			? ×
オブジェクトの種類の選択(S):  グループ または ビルトイン セキュリティ プリンシパル	_	オブジ	;ェクトの種類(0)
場所の指定(F): 2008R2StaAD.local	 _		場所(L)
違択するオブジェクト名を入力してください (例)(E): Domain Admins	_		品前の確認(C)
詳細設定(A)	ОК		

④ プライマリグループを変更します。

「Domain Admins」を選択し、「プライマリ グループの設定」をクリックします。

logvillageのプロパティ ? 🗙
ダイヤルイン 環境 セッション リモート制御 リ リモート デスクトップ サービスのプロファイル 個人用仮想デスクトップ COM+ フリガナ 全般 住所 アカウント プロファイル 電話 所属されている組織 所属するグループ
所属するグループ(M): - これが
ブライマリ グループの設定(S) Macintosh クライアントまたは POSIX 対応のアプリケ ーションがない場合は、プライマリ グループを変更する 必要はありません。
OK キャンセル 適用(A) ヘルプ

「プライマリ グループ」が「Domain Admins」に変更された事を確認後、「OK」をクリックし

ます。				
logvillageのプロパティ	? ×			
ダイヤルイン 環境 リ リモート デスクトップ サービスのプロファイル 個 全般 住所 アカウント プロファイル 電話	セッション リモート制御   人用仮想デスクトップ   COM+   フリガナ   舌   所属されている組織   所属するグループ			
所属するグループ(M):				
名前 Active Directory ドメイン	/サービス フォルダー			
Domain Admins 2008R2StaAD.local/Us Domain Users 2008R2StaAD.local/Us	ers			
ブライマリ グループ: Domain Admins				
ブライマリ グループの時定(S)、こううかな 必要はありま	い場合は、フライマリ グループを変更する せん。			
OK キャン	セル 適用(A) ヘルプ			

・管理対象 PC 上で、設定反映を確認する方法

① 「コンピュータの管理」を起動します。

"Windows スタートメニュー"→「コントロールパネル」→「管理ツール」→「コンピュータの 管理」を起動します。

「コンピュータの管理(ローカル)」→「ローカル ユーザーとグループ」→「グループ」を クリックします。



「Administrators」を開き確認します。
 「Administrators」をダブルクリックします。

所属するメンバ内に「<AD 名>判Omain Admins」が表示される事を確認してください。

Administratorsのプロパティ	? 🗙
全般	
Administrators	
説明(E): コンピュータ/ドメインに完全なアクセス権があります。	
所属するメンバ(M): AD¥Domain Admins AD¥so=ten admins Administrator So=ten	
<u>注首加(D)</u> 肖耶余(R)	
OK キャンセル 通	5月( <u>A</u> )

・管理対象 PC に、グループ ポリシーを強制再適用する方法
 管理対象 PC で以下の操作を実施します。
 コマンドプロンプトを起動します。
 <sup>"Windows スタートメニュー"→「ファイル名を指定して実行」に「cmd」と入力し「OK」をクリックします。
</sup>

「gpupdate /force」を入力し、実行します。

※gpupdate /force はグループポリシーを反映するコマンドです。

成功した場合は、下図のようなメッセージが表示されます。



ドメインコントローラへ接続できない場合は、下図のようなメッセージが表示されます。



#### ・LogVillage 管理対象 PC の設定に登録する時の注意点

登録時の「アカウント名」が通常と異なります。

例:以下の場合

ドメイン「AD. local」 管理対象 PC「host01」 AD. local のユーザー「logvillage」

## 「システム設定」→「管理対象 PC の設定」に登録する内容は、以下になります。

- ① コンピュータ名:host01
- ② アカウント名: AD. local¥logvillage
- ③ パスワード: (logvillage ユーザーに設定いただいたパスワード)

管理対象PCの影	定	
管理対象PCの登録	UZE	
コンビュータ名 アカウント名 パフロード	1	
バスワード (確認用)	3	

# 7-3-2-2. Active Directory 上で OU の管理者権限を持ったユーザーの作成と LogVillage への登録

OU 内にLogVillage 接続専用ユーザーを作成するために以下の作業を実施ください。

※「7-4-2-1. Active Directory 上で Domain Admins 権限を持ったユーザーの作成と LogVillage への登録」をご確認いただき、Domain Admins 権限を持ったユーザーを作成されている場合、この操作は不要です。

以下の項目があります。

- ・ユーザー作成
- ・管理対象 PC に、グループ ポリシーを強制再適用する方法
- ・管理対象 PC 上で、設定反映を確認する方法
- ・LogVillage 管理対象 PC の設定に登録する時の注意点

・ユーザー作成

- 「Active Directory ユーザーとコンピュータ」起動します。
   "Windows スタートメニュー"→「管理ツール」→「Active Directory ユーザーとコンピュー ター」を起動します。
- ② 新規「ユーザー」を作成します。
   該当 0U の上で右クリック「新規作成」→「ユーザー」をクリックします。
   例: 0U 名: logvillage



「姓」と「ユーザー ログオン名」に任意のユーザー名を入力し「次へ」をクリックします。 例: logvillage

新しいオブジェクト - ユーザー	× ×
🤱 作成先:	2008R2StaAD.local/Users
<b>女生(L)</b> :	logvillage
名(F):	1=2×71400
フル ネーム(A):	logvillage
ユーザー ログオン名(U):  logvillage	@2008R2StaAD.local
, ユーザー ログオン名(Wi	 ndows 2000 より前)(W):
2008R2STAAD¥	logvillage
	< 同ろ(日) (同ろ(日) (R)) (R

「パスワード」と「パスワードの確認入力」に任意のパスワードを入力します。 「ユーザーは次回ログオン時にパスワード変更が必要」のチェックを外します。 「ユーザーはパスワードを変更できない」「パスワードを無制限にする」にチェックを入れ ます。

「次へ」をクリックします。

新しいオブジェクト - ユーザー	×
Nep5先: 2008R2StaAD.local/Users	
パスワード(P): パスワードの確認入力(C): ●●●●●●●●●●	
<ul> <li>□ ユーザーは次回ログオン時にパスワード変更が必要(M)</li> <li>▽ <u>ローザーはパスワードを変更できない(S)</u></li> <li>▽ パスワードを無期限にする(W)</li> </ul>	
□ アカウントは無対(0)	
< 戻る(B) 次へ(N) > キャンセ	216

設定に間違いが無い事を確認後「完了」ボタンをクリックします。

新しいオブジェクト - ユーザー 🛛 🔀
ど 作成先: 2008R2StaAD Jocal/Users
「完了】をクリックすると、次のオブジェクトが作成されます:
フルネーム: logvillage ユーザー ログオン名: logvillage@2008R2StaAD.local ユーザー(よパスワードを変更できない) パスワードを無期限にする
〈戻る(B) デア キャンセル

③ セキュリティ グループを作成します。

該当00の上で右クリック「新規作成」→「グループ」をクリックします。



グループ名を入力します。 例:logvillage admins グループのスコープは「グローバル」選択します。 グループの種類は「セキュリティ」を選択します。 「OK」をクリックします。

<b>轻</b> 作成先:	2008R2StaAD.local/logvillage
ブループ名(A): logvillage admins	
ブループ名 (Windows 200 logvillage admins	0 より前)(W):
- グループのスコープ ○ ドメイン ローカル(0) ◎ グローバル(G) ○ エニハーワル(0)	グループの種類 ・ セキュリティ(S) ・ ロビボ(D)

④ 権限を付与します。

「Users」を開き、作成したユーザーを右クリック「プロパティ」をクリックします。 例: logvillage



Separation         ? ▼           ダイヤルイン         環境         セッション         リモート制御           リモート デスクトップ サービスのクロファイル         個人用仮想デスクトップ         cont         コリガナ           全般         住所         アカウント         プロファイル         電話         所属されている組織         所属するグループ
所属するグループ(M): 名前 Active Directory ドメイン サービス フォルダー Domain Users 2008R2StaAD.local/Users
<u> 達加(D)</u> ガライマリ グループ: Domain Users プライマリ グループ: Domain Users プライマリ グループの設定(S) Macintosh クライアントまたは POSIX 対応のアプリケ ーションがない場合は、プライマリ グループを変更する 必要はありません。
OK キャンセル 適用(A) ヘルブ

「所属するグループ」タブを開き、「追加」をクリックします。

「選択するオブジェクト名を入力してください」に「作成したセキュリティ グループ名 (例: logvillage admins)」を入力し、「名前の確認」をクリックします。

グループ の選択		? ×
オブジェクトの種類の選択(S):  グループ または ビルトイン セキュリティ プリンシパル		オブジェクトの種類(の)
場所の指定(F): 2008R2StaAD.local		場所(L)
選択オスナブジェクトタを入力してください (例)(E): logvillage admins		名前の確認(C)
	ОК	

「domain admins」に下線が表示された事を確認後、「OK」をクリックします。

グループ の選択	? >
オブジェクトの種類の)違択(S):   グループ または ビルトイン セキュリティ プリンシバル	オブジェクトの種類(O)
場所の指定(F): 2008R2StaAD.local	場所(L)
送けたすますが1-カトをまえ、力してください(例)(E): logvillage admins	名前の確認(C)
〕	)K キャンセル

(下線が追加されない場合、セキュリティグループの指定に問題があります。入力文字列の確認、およびセキュリティグループが正しく作成されているかを確認してください)

所属するグループに指定したセキュリティグループが追加されている事を確認し、「OK」を クリックします。

logvillageመታበለティ ? 🗙
ダイヤルイン 環境 セッション リモート制御 リモートデスクトップサービスのプロファイル 個人用仮想デスクトップ COM+ フリガナ 全般  住所  アカウント   プロファイル 電話   所属されている組織 所属するグループ
所属するグループ(M):
名前 Active Directory ドメイン サービス フォルダー
logvillage admins 2008R2StaAD.local/logvillage
<u> 注意力D(D)</u> 菁I厚余(R)
プライマリ グループ: Domain Users
OK キャンセル 適用(A) ヘルウ

⑤ グループポリシーを編集します。

"Windows スタートメニュー"→「管理ツール」→「グループポリシーの管理」を起動します。 設定を行う OU を展開します。

変更するポリシーを右クリックし、「編集」をクリックします。

例:0U名:logvillage

■グルーナ ポリシーの管理	
🔜 ファイル(F) 操作(A) 表示(V) ウィンドウ(W	) ヘルプ(H) <u></u>
🗢 🔿 🗾 📰 🗙 🖬 📘	
<ul> <li>◎ グループ ポリシーの管理</li> <li>○ フォレスト: 2008R2StaAD.local</li> <li>○ マオレスト: 2008R2StaAD.local</li> <li>○ Efault Domain Policy</li> <li>○ Domain Controllers</li> <li>○ Domain Control</li></ul>	Iogvillage       スコープ  詳細   設定   委任         リンウ       表示するリンクの場所(L):     2008R2StaAD.local       次のサイト、ドメイン、および OU がこの GPO (zリンクされています(T):       「登却   リンクの有効化   パス       (L)     (ハ (はい 2008R2StaAD.local/       (L)     (ハ (はい 2008R2StaAD.local/       (L)     (ハ (はい 2008R2StaAD.local/       (L)     シーク・(はい 2008R2StaAD.local/       (L)     シーク・(はい 2008R2StaAD.local/       (L)     シーク・(ない 2008R2StaAD.local/       (L)     シーク・(ない 2008R2StaAD.local/       (L)     シーク・(ない 2008R2StaAD.local/       (L)     シーク・(ない 2008R2StaAD.local/       (L)     (ハ (ない 2008R2StaAD.local/       (L)     シーク・(ない 2008R2StaAD.local/       (ない 2008R2StaAD.local/     ア       (ない 2008R2StaAD.local/     ア       (ロ)     ア       (ロ)     ア       (ロ)     ア       (ロ)     ア       (ロ)     ア<
GPO エディターを開きます。	

「コンピュータの構成」→「ポリシー」→「Windows の設定」→「セキュリティの設定」→ 「制限したグループ」を選択します。

「制限したグループ」の上で右クリックし、「グループの追加」を選択します。



「参照」をクリックします。

グループの追加		×
グループ(G): 		参照(B)
	OK	

作成したセキュリティグループ名を入力します。

例: logvillage admins

「名前の確認」をクリックし、入力文字列に下線が付与される事後、「OK」をクリックします。

グループ の選択			? ×
オブジェクトの種類の選択(S):  グループ または ビルトイン セキュリティ プリンシパル		オブジュ	:クトの種類(O)
場所の指定(F): 2008R2StaAD.local			場所(L)
) SERTEAT Logvillage admins		名詞	前の確認(C)
詳細設定(A)	OK		キャンセル

(下線が追加されない場合、セキュリティグループの指定に問題があります。入力文字列の 確認、およびセキュリティグループが正しく作成されているかを確認してください)

グループに「<AD 名>¥<作成したセキュリティグループ>」が表示されることを確認し、

「OK」をクリックします。

グループの追加		×
グループ(G): 2008R2STAAD¥logvillage admins		参照(B)
	ОК	キャンセル

## 「追加」をクリックします。

2008R2STAAD¥logvillage admins プロパティ	? ×
2008R2STAAD¥logvi のメンバーシップの構成	
このグループのメンバー(M):	
くこのグループにはメンバーを含めません>	追加(A)
	HUPTARV
このグループの所属(T): <このグループが既に属しているグループは変更しません>	追加(D)
	肖川F余(E)
OKキャンセル	適用(A)

「参照」をクリックします。

グループ メンバーシップ	×
グループ(G): 「	参照(B)
OK	

「Administrators」と入力します。

「名前の確認」を選択し、入力文字列に下線が付与される事を確認後、「OK」をクリックし

ます。

グループ の選択	? ×	(
オブジェクトの種類の選択(S):   グループ または ビルトイン セキュリティ プリンシパル	オブジェクトの種類(0)	
場所の指定(F): 2008R2StaAD.local		
選択オスナブジェクト名を入力してください (例)(E): Administrators	名前の確認(C)	]
	<u>ОК</u> ++>±и	

(下線が追加されない場合、セキュリティグループの指定に問題があります。入力文字列を 確認してください)

グループに「Administrators」が表示されることを確認し、「OK」クリックします。

グループ メンバーショ	プ		×
グループ(G): Administrators		参照(B)	
	ОК	キャンセル	

このグループの所属に「Administrators」が表示される事を確認し、「OK」クリックします。

2008R2STAAD¥logvil	lage admins プロ	パティ	? X
2008R2STAAD¥logvi (	Dメンバーシップの構成	\$ j	
このグループのメンバー(	M):		
くこのグループにはメント	(一を含めません)		追加(A)
			肖 『赤(Fl)
,	-		
このグループの所属(T):			(Rtw(p)
Hummistrators		L	
			肖耶余(E)
	ОК	キャンセル	適用(A)

制限されたグループに「<AD 名>¥<作成したセキュリティグループ>」が表示されることを 確認します

∬ グルーフ ポリシー管理エディター			
ファイル(F) 操作(A) 表示(V) ヘルプ(H)			
🗢 🔿 🙋 📅 🗟 🔽 🗊			
Igrillage [2008R2STA-AD.2008R2ST/▲	<u> 200-24- N</u>	バー   所属	するグループ
📃 🔄 コンピューターの構成 📃	2008R2STAAD¥logvillage admins	Adm	nistrators
🖂 🧰 ポリシー			
田 🎬 ソフトウェアの設定			
🖂 📔 Windows の設定			
🗉 🧰 名前解決ポリシー			
📄 スクリプト (スタートアップ/5			
🗆 🚡 セキュリティの設定			
🗉 📑 アカウント ポリシー			
🗉 🚎 ローカル ポリシー			
田 <u>i</u> <u>イベント ログ</u>			
田 强 制限されたグループ			
🗉 📑 システム サービス			
🗉 📑 LŸZŀIJ			
🗉 📴 ファイル システム			
田 🔝 ワイヤード (有線) ネ:			
田 🧰 セキュリティが強化され			
ニュー ネットワークリスト マネ			
🗉 🔤 ワイヤレス ネットワーク			
田 🔤 公開キーのボリシー			
田      ソフトウェアの制限のオ     マットレート			
田 二 ネットリーク アクセス(オ			
田 //フリケーション制御木			
∃ S IP セキュリティ ボリジュ ■ S T + PU22 のませんのす			
□ □ □ 管理用デンノレード □ □ □ □ □			

#### ・管理対象 PC 上で、設定反映を確認する方法

① 「コンピュータの管理」を起動します。

"Windows スタートメニュー"→「コントロールパネル」→「管理ツール」→「コンピュータの 管理」を起動します。

「コンピュータの管理(ローカル)」→「ローカル ユーザーとグループ」→「グループ」を クリックします。



「Administrators」を開き確認します。
 「Administrators」をダブルクリックします。

所属するメンバ内に「<AD 名>¥Domain Admins」が表示される事を確認してください。

Administratorsのプロパティ	? 🗙
全般	
Administrators	
説明(E): コンピュータ/ドメインに完全なアクセス権があります。	
所属するメンバ(M):	
AD¥Domain Admins AD¥so-ten admins Administrator So-ten	
<b>注加(D)</b> 肖耶念(R)	
<u> </u>	適用( <u>A</u> )

#### ・管理対象 PC に、グループ ポリシーを強制再適用する方法

管理対象 PC で以下の操作を実施します。

コマンドプロンプトを起動します。

"Windows スタートメニュー"→「ファイル名を指定して実行」に「cmd」と入力し「OK」をクリッ クします。

「gpupdate /force」を入力し、実行します。

※gpupdate /force はグループポリシーを反映するコマンドです。

成功した場合は、下図のようなメッセージが表示されます。



ドメインコントローラへ接続できない場合は、下図のようなメッセージが表示されます。



## ・LogVillage 管理対象 PC の設定に登録する時の注意点

登録時の「アカウント名」が通常と異なります。

例:以下の場合

ドメイン「AD. local」 管理対象 PC「host01」 AD. local のユーザー「logvillage」

# 「システム設定」→「管理対象 PC の設定」に登録する内容は、以下になります。

- ① コンピュータ名:host01
- ② アカウント名: AD. local¥logvillage
- ③ パスワード: (logvillage ユーザーに設定いただいたパスワード)

管理対象PCの設定					
管理対象PCの登録	NJZF				
コンビュータ名	1				
アカウント名	2				
バスワード	3				
バスワード (確認用)	3				

## 8. LogVillageMGR 画面の基本操作

LogVillageMGR 画面の基本操作について説明します。

## 8-1. LogVillageMGR 画面の表示方法

LogVillageMGR 画面の表示方法について説明します。

LogVillgae 管理画面にログインします。
 Internet Explorer を起動します。
 以下のURL にアクセスするとLogVillage ログイン画面が表示されます。

http://<LogVillageMGR のコンピュータ名>/lv/login/

インストール直後のログイン ID はユーザー設定を行うまでは以下の ID のみ有効となります。 また、ユーザー設定後は以下の ID は無効となりますので、新しく作成したユーザーの ID とパ スワードを忘れないようにご注意ください。

# 新しく設定したユーザーIDとパスワードを忘れた場合、LogVillageの再インストールが必要となります。ご注意ください。

・ユーザー名 so-ten

・パスワード so-ten

※ご利用ブラウザについて

LogVillageMGRの対応ブラウザは InternetExplorer9 以降となります。

#### 8-2. 画面概要

LogVillag	re 2.0					- so-ten
ダッシュボード	济庄管理	採作口グ管理	有動管理			システム設定
ロダイン完了しました。					3	
					U	

- ログ表示メインメニュー メインメニューの表示項目は、お買い上げいただいたライセンス、またはユーザー設定により異なります。
   参照したいメニューをクリックすると、ログ表示サブメニューが表示されます。
- ログインユーザー名
   現在のLogVillageへのログインユーザー名が表示されています。
   ログオフする場合は、ログインユーザ名をクリックし、[ログアウト]を選択します。
- ③ システム設定

クリック後、システム設定メニューが表示されます。 但し、ログインユーザーにシステム設定権限が付与されていない場合は表示されません。

※ブラウザの「戻る」ボタン

LogVillageMGR 画面ご利用にクリックすると画面がエラーとなる場合がありますのでご注意く ださい。

※LogVillageMGR 画面は複数画面を同時表示させることも可能です。

## 8-3. システム設定画面

LogVillage 2.0 2							so-ten		
ダッシュボード	資産管理	操作口步管理	移動管理			システム設定			
ログイン完てしました。						ボーリングサーバ	共通設定	•	
						グループ	グループ単位設定	•	
						管理対象PC	アラートポリシー設定	•	
						トップ画面	運用管理	•	
						WindowsUpdate情報			
						ウィルス対策ソフト定義ファイル			
						プロセス名辞書			
						拡張項目名(資産管理)			

- ① システム設定メニュー
  - ・メニュー項目をクリックすると設定画面が表示されます。
  - ・各設定項目で設定を行う機能、画面は運用マニュアルをご参照ください。
- ② ログ表示メインメニュー

クリックするとシステム設定画面が終了しログ表示サブメニューが表示されます。

【ご注意ください】

初期設定が全て完了するまで、サイドメニュー上部に「初期設定」メニューが表示されます。 そのため、以下の設定項目が「初期設定」と「共通設定」または「グループ単位設定」に2重表 示されますのでご注意ください。 ・ライセンス登録・更新

- ・ポーリングサーバ
- ・管理対象 PC
- ・ログ収集スケジュール
- 2重表示される設定項目は、どちらをクリックいただいても問題ありません。

## 9. 管理対象 PC 自動設定ツール

ワークグループ環境下の管理対象 PC の設定を行うツールです。

## 9-1. LogVillage 管理対象 PC 設定ツール

LogVillage 管理対象 PC 設定ツールについて説明します。

## 9-1-1. 対応 0S

Windows 7, 8, 10

# 9-1-2. 管理対象 PC での実行時の注意事項

- (1) 管理者権限を持ったユーザーでのログインが必要となります。
- (2) 自動的に PC 再起動が行われます。

(3) LogVillage が使用する管理者権限ユーザーアカウントおよびパスワードが管理対象 PC にランダムに自動生成されます。自動生成されるユーザーアカウント名は、"LV"+8 文字のランダム 数値(例:LV84558403 等)となります。

## 9-1-3. 設定手順

■LogVillageMGR での設定準備手順

ファイルを配置します。
 クライアント自動設定ツール¥pcsetupDLを、<LogVillageMGR プログラムインストール先>
 ¥ Apache2¥htdocs¥に貼り付けます。

※<LogVillageMGR プログラムインストール先>は、インストール先ディレクトリパスに読み 替えます。(32bit版OSにてデフォルトでインストールした場合 C:¥Program Files¥SO-TEN¥LogVillage となります。)

■管理対象 PC での設定手順

- 管理対象 PC にログインします。
   管理対象 PC に管理者権限を持ったユーザーでログインします。
- ② ダウンロードページにアクセスします。
   Internet Explorer を起動し、ダウンロードページを開きます。
   http://<マネージャのURL>/pcsetupDL/
- ③ 「ダウンロード」ボタンをクリックします。



④ ファイルを保存します。

「ディスクに保存する」にチェックが入っている事を確認後「OK」をクリックします。


- 保存したファイルを展開します。
   保存したファイル「setUPLVClient.zip」を展開します。
- ⑥ ファイルを実行します。
   「LVAutoSet\_WindowsVista-10. exe」をダブルクリック(実行)します。
- ⑦ 「設定開始」をクリックします。
   設定開始をダブルクリックし、「設定開始」をクリックします。

	自動設定で	を開始します。			
	OK	キャンセル			
LogV	illage クライアン	・ト設定ツール			
	LogVillageの設定を	行います。			
設定完了後、再起動を行いますので、 不要なアプリケーションは終了してください。					
	設定を開始しますか	1?			
	設定開始	中止			

⑧ 「OK」をクリックします。



OS を再起動します。

設定変更のためには再起動	が必要です。再起動な	をしますか?
	(‡い(Y)	いいえ(N)

⑪ 設定完了確認。

OS 再起動後、設定完了のウィンドウが表示された事を確認します。



# 9-2. 管理対象 PC を LogVillage マネージャに登録する

管理対象 PC を LogVillage マネージャに登録する方法を説明します。

# ① 「管理対象 PC」を開きます。

LogVillage 管理画面の「システム設定」→「管理対象 PC」をクリックします。

LogVíllage2.0						arlmin					
ダッシュボード	资源管理	操作口グ管理	存動管理	ネットワークスキャン	PC存储时間管理					システム設定	2
ロダイノ寮了しました。								ボーリングサーバ		共通設定	
								グループ		グループ単位設定	4
								E-E-119990		アラートポリシー設定	
								 1978B		運用管理	•
								WindowsUpdate情報			
								ウィルス対策ソフト定義	ファイル		
								プロセス名辞書			
								拉張項目名(資產管理)			
								ネットワークスキャン酸	Ē		
								ネットワークスキャンアラ	ラート設定		

② 設定を変更します。

自動設定ツールを実行した管理対象 PC は、ステータスが「登録待ち」となって自動登録されています。

「登録待ち」の管理対象 PC にチェックを入れます。

「グループ名」「所属するポーリングサーバー(PS)名」を選択し、ステータスを「稼動」

に変更後、「変更する」をクリックします。

このステータスに変更する事により、ログ収集が開始されます。

全てをチェック					-
SKYBLUE	logvillage	八丁堀	LV20M	手動	稼
	tatsu	八丁堀	LV20M	手動	稼
	LV69135142	八丁堀	LV20M	手動	稼
CE430EA3	LV29906409	八丁堀	LV20M	手動	稼
	LV15230752	八丁堀	LV20M	手動	稼
<ul> <li>CE430EA3</li> <li>OLIVE</li> <li>全てをチェック</li> <li>チェックした管理対象PC:</li> <li>管理対象PCの新規登録</li> </ul>	LV29906409 LV15230752 を 削除する	八丁堀 八丁堀 ]	LV20M	手動	

# 10. LogVillage 運用のための情報

LogVillage 運用のための情報について説明します。

#### 10-1. LogVillage マネージャ動作関連ログファイル

LogVillage マネージャ動作関連ログファイルについて説明します。

### 10-1-1. ログ保存場所

収集ログファイルのDBへの取り込み作業など、LogVillageマネージャの動作に関係するログファ イルは以下のフォルダに保存されます。

<LogVillage マネージャプログラムインストール先>¥Manager¥logs

※<LogVillage マネージャプログラムインストール先>は、インストール先ディレクトリパスに 読み替えます。(32bit版OSにてデフォルトでインストールした場合 C:¥Program Files¥SO-TEN¥LogVillage となります。)

ファイル名の例: LV-M-LOG20100130182054.txt

# 10-1-2. ログ保存期間

LogVillage マネージャのログファイルの保存期間は 30 日 となります。 30 日を経過したログファイルは自動削除されます。

#### 10-2. LogVillage ポーリングサーバー動作関連ログファイル

LogVillage ポーリングサーバー動作関連ログファイルについて説明します。

## 10-2-1. ログ保存場所

管理対象 PC への接続・情報収集など、LogVillage ポーリングサーバーの動作に関係するログファ イルは以下のフォルダに保存されます。

<LogVillage ポーリングサーバープログラムインストール先>¥PServer¥Logs

※<LogVillage ポーリングサーバープログラムインストール先>は、インストール先ディレクト リパスに読み替えます。(32bit版OSにてデフォルトでインストールした場合 C:¥Program Files¥S0-TEN¥LogVillage となります。)

ファイル名の例: LV-PS-L0G201001230182024.txt

# 10-2-2. ログ保存期間

LogVillage ポーリングサーバーのログファイルの保存期間は 30 日 となります。 30 日を経過したログファイルは自動削除されます。

#### 10-3. Apache2 動作関連ログファイル

Apache2 動作関連ログファイルについて説明します。 標準では Apache2 のエラーログのみが記録されます。

10-3-1. ログ設定方法

管理画面にアクセスした際のログや収集されたログファイルの転送ログなども 記録するためには次の設定を行ってください。

以下のフォルダを開き、「httpd. conf」ファイルを開きます。 <LogVillage マネージャプログラムインストール先>¥Apache2¥conf

※<LogVillage マネージャプログラムインストール先>は、インストール先ディレクトリパスに 読み替えます。(32bit版 0S にてインストール先ディレクトリを変更せずにインストールした場 合 C:¥ Program Files(x86)¥S0-TEN¥LogVillage です。)

次の文字列を検索し、先頭の「#」を削除して保存します。 「#CustomLog "logs/access.log" common」

"Windows スタートメニュー"→「コントロールパネル」→「管理ツール」→ 「サービス」から、サービス「Apache2」を再起動します。

# 10-3-2. ログ保存場所

Apache2 の動作に関係するログファイルは以下のフォルダに保存されます。

<LogVillage マネージャプログラムインストール先>¥Apache2¥Logs

ファイル名の例: access. log (アクセスログ), error. log (エラーログ)

#### 10-3-3. ログ保存期間

Apache2 のログファイルは無期限に保存されます。 Apache2 インストールディスクの残容量が少なくなる場合、定期メンテナンス作業時などに手動に てログファイルを移動、または削除してください。

### 11. SSL (暗号化) 通信設定

LogVillage マネージャとポーリングサーバ、LogVillage マネージャ管理画面を全て SSL 通信設定にて行うことができます。

本マニュアルでは、SSL 証明書は自己証明で設置する手順を記載していますので予めご了承ください。

①SSL 通信設定のための秘密鍵、公開鍵、自己証明書を作成

```
1)LogVillage マネージャのサーバにてコマンドプロンプトを起動
```

2) 以下のコマンドを入力

\_\_\_\_

- > cd C:¥ Program Files (x86)¥SO-TEN¥LogVillage¥Apache2¥bin ※上記は標準インストール場所で記載しています。
  - インストールフォルダを変更している場合は読み替えてください。

> openssl.exe genrsa -out .../conf/server.key 1024

※以下の入力が求められますが、入力行は「Common Name (eg, YOUR name)[]:の行のみです。

C:\Program Files\SO-TEN\LogVillage\Apache2\bin>openssl.exe req -new key .../conf/server.key -out .../conf/server.csr -config .../conf/openssl.cnf You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank. Country Name (2 letter code) [AU]: State or Province Name (full name) [Some-State]: Locality Name (eg, city) []: Organization Name (eg, company) [Internet Widgits Pty Ltd]: Organizational Unit Name (eg, section) []: Common Name (eg. YOUR name) []: (例: so-ten) Email Address []: Please enter the following 'extra' attributes to be sent with your certificate request A challenge password []:

```
An optional company name []:
```

> openssl.exe x509 -in ../conf/server.csr -out ../conf/server.crt -req signkey ../conf/server.key -days 365

②Apache (Web サーバ) 設定ファイルを編集

※編集前に必ずバックアップを行ってください。

(編集ファイルの場所) C:¥ Program Files (x86)¥SO-TEN¥LogVillage¥Apache2¥conf ※上記は標準インストール場所で記載しています。

インストールフォルダを変更している場合は読み替えてください。

(編集ファイル名) httpd. conf

(編集内容) #LoadModule ssl\_module modules/mod\_ssl.so

↓ ※"#" を削除 LoadModule ssl\_module modules/mod\_ssl.so

#Include conf/extra/httpd-ssl.conf ↓ ※"#" を削除 Include conf/extra/httpd-ssl.conf

③Apache (Web サーバ) 設定ファイルを編集

※編集前に必ずバックアップを行ってください。

(編集ファイルの場所) C:¥ Program Files (x86) ¥SO-TEN¥LogVillage¥Apache2¥conf¥extra ※上記は標準インストール場所で記載しています。

インストールフォルダを変更している場合は読み替えてください。

(編集ファイル名) httpd-ssl. conf

(編集内容) SSLSessionCache shmcb:C:/Program
Files/S0-TEN/LogVillage/Apache2/logs/ssl\_scache(512000)
↓ ※" #" を追加
#SSLSessionCache shmcb:C:/Program
Files/S0-TEN/LogVillage/Apache2/logs/ssl\_scache(512000)

④LogVillage マネージャの設定ファイルを SSL 通信対応に編集

(編集ファイルの場所) C:¥ Program Files (x86) ¥SO-TEN¥LogVillage¥Manager ※上記は標準インストール場所で記載しています。

インストールフォルダを変更している場合は読み替えてください。

(編集ファイル名) Config.ini

- (編集内容) GenAllSettingURL=http://localhost/lv/psauths/genAllSetting/ DeviceAlertURL=http://localhost/lv/psauths/genDeviceByPs/%d/ AppAlertURL=http://localhost/lv/psauths/genAppByPs/%d/ ↓ ※" http" を" https" に変更 GenAllSettingURL=https://localhost:443/lv/psauths/genAllSetting/ DeviceAlertURL=https://localhost:443/lv/psauths/genDeviceByPs/%d/
  - AppAlertURL=https://localhost:443/lv/psauths/genAppByPs/%d/

⑤LogVillage マネージャを再起動

再起動手順は本マニュアル末尾の「補足資料」をご参照ください。

⑥LogVillage ポーリングサーバの通信設定ファイルを SSL 通信対応に編集
 (編集ファイルの場所) C:¥ Program Files (x86)¥S0-TEN¥LogVillage¥PServer¥TaskTray
 ※上記は標準インストール場所で記載しています。

インストールフォルダを変更している場合は読み替えてください。

(編集ファイル名) Connect. ini

(編集内容) WebDavPort=80

↓ ※" 80" を" 443" に変更 WebDavPort=443

⑦LogVillage ポーリングサーバの設定ファイルを SSL 通信対応に編集

(編集ファイルの場所) C:¥ Program Files (x86)¥SO-TEN¥LogVillage¥PServer ※上記は標準インストール場所で記載しています。

インストールフォルダを変更している場合は読み替えてください。

(編集ファイル名) Config.ini

(編集内容) SSLIsOn=0

↓※" 0" を" 1" に変更

SSLIsOn=1

⑧LogVillage ポーリングサーバを再起動 再起動手順は本マニュアル末尾の「補足資料」をご参照ください。

⑨SSL 設定後の管理画面へのアクセス
 https://・・・・ としてアクセスください。

# 12. お問合せ

本製品に対するご意見、ご質問はメール、TEL、FAX にて下記までお問合せください。 お問合せの内容によっては、ご返答に多少お時間を頂戴する場合がありますので、予めご了承くだ さい。

〒104-0032 東京都江東区福住 1-14-4 山崎ビル 1F 株式会社蒼天 サポートセンター

e-mail	: <u>support@so-ten. co. jp</u>
TEL	: 03–5809–8406
FAX	: 03–5809–8495
受付·対応時間	:月~金曜日(祝祭日、年末年始休暇除く) 10:00~17:00

#### ■お客様情報

お客様番号

※「システム設定」→「ライセンスの登録・変更」画面に表示されます。
会社名(団体、学校名)、ご部署名
ご担当者名
メールアドレス
電話番号
FAX 番号
お問合せの内容(できるだけ詳しくお書きください)
■稼働環境
コンピュータメーカ名:
型番:
メモリ容量:
ハードディスク容量または種類:
OS バージョン:
サービスパック:

# << 補足資料 >>

LogVillage マネージャ、ポーリングサーバを強制終了、再起動は以下の手順にて行ってください。

■ LogVillage マネージャ

<終了手順>

- ① [コントロールパネル] → [サービス] から、下記のサービスを順に停止します。
  - 1) LV\_M\_MonitorSrv
  - 2) LV\_ManagerServer
  - 3) Apache2
  - 4) Embedded Database LOGVILLAGE2

#### <起動手順>

手動で終了した場合、以下の手順で起動を行ってください

OS を再起動した場合は自動起動されますので以下の手順は不要です。

- ① [コントロールパネル] → [サービス] から、下記のサービスを順に開始します。
  - 1) Apache2
  - 2) Embedded Database LOGVILLAGE2
  - 3) LV\_M\_MonitorSrv
- ②「LV\_M\_MonitorSrv」起動後、「LV\_ManagerServer」が開始される事を確認します。

#### ■ LogVillage ポーリングサーバ

#### <終了手順>

① [コントロールパネル] → [サービス] から、下記のサービスを停止します。

LV\_P\_MonitorSrv

- ② [タスクマネージャ] → [プロセス] から、下記のプロセスを順に選択し、「プロセスの終了」 をクリックします。
  - 1) LV\_TaskTray. exe
  - 2) LV\_PollingServer.exe

#### <起動手順>

- ① [コントロールパネル] [サービス] から、下記のサービスを起動します。 LV P MonitorSrv
- ② [タスクマネージャ]→[プロセス]にて、「LV\_PollingServer.exe」が表示(起動)される ことを確認します。
- ③ Windowss スタートメニューから、「LV\_TaskTray(PS)」を起動



# 株式会社 蒼天

〒135-0064 東京都江東区福住 1-14-4 山崎ビル 1F http://www.so-ten.co.jp/