

Lite

**導入マニュアル**

V2.5J

株式会社ワッセイ・ソフトウェア・テクノロジー

**logVillage2.0 Lite 　導入マニュアル**

revision　：　MDL-25-20220830

最終更新日：2022年8月30日

\*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。

**株式会社ワッセイ・ソフトウェア・テクノロジー**

〒540-0035

大阪市中央区釣鐘町1丁目3-4 ダイクウビル2F

TEL: 06-6944-8901　FAX: 06-6944-8885

http://www.wasay.co.jp

**目次**

[1.LogVillageの基本構成 5](#_Toc36368929)

[1-1.稼働環境 5](#_Toc36368930)

[1-2.LogVillageの構成要素 8](#_Toc36368931)

[1-3.構成イメージ図 9](#_Toc36368932)

[1-4.LogVillageの動作概要 10](#_Toc36368933)

[1-5.インストールプログラムの説明 11](#_Toc36368934)

[2.本番運用までの手順 12](#_Toc36368935)

[3.導入前の準備と確認 13](#_Toc36368936)

[3-1. LogVillageMGR⇔LogVillagePS間通信方式についての確認 13](#_Toc36368937)

[3-2. LogVillagePS→管理対象PCへの接続確認 14](#_Toc36368938)

[3-3.管理対象PC情報の準備 16](#_Toc36368939)

[4.LogVillageMGRのインストール 17](#_Toc36368940)

[4-1.LogVillageMGRのインストール 17](#_Toc36368941)

[4-2.LogVillageMGRのライセンス登録 22](#_Toc36368942)

[5.LogVillagePSのインストール 25](#_Toc36368943)

[5-1.インストールおよび運用環境について 25](#_Toc36368944)

[5-2.LogVillagePSのインストール手順 31](#_Toc36368945)

[5-3.LogVillagePSのセットアップ 34](#_Toc36368946)

[6.LogVillage PCエージェントのインストール 36](#_Toc36368947)

[6-1.PCエージェントの稼働環境 36](#_Toc36368948)

[6-2.PCエージェントのインストール前準備 36](#_Toc36368949)

[6-3.PCエージェントのインストール 36](#_Toc36368950)

[6-4.インストール確認 38](#_Toc36368951)

[6-5.PCエージェントの起動間隔設定 38](#_Toc36368952)

[6-6.PCエージェントのアンインストール 38](#_Toc36368953)

[7.Phantosysログ取得エージェントのインストール 39](#_Toc36368954)

[7-1.Phantosysログ・サーバエージェントのインストール 39](#_Toc36368955)

[7-2.Phantosysログ・クライアントエージェントのインストール 42](#_Toc36368956)

[7-3.Phantosysログ取得エージェントのアンインストール 42](#_Toc36368957)

[8.LogVillageの初期設定 43](#_Toc36368958)

[8-1.初期設定項目と設定方法 43](#_Toc36368959)

[8-2. LogVillagePSを複数台設置した場合の管理対象PCとの関係 44](#_Toc36368960)

[8-3.ログ収集の仕組みと注意点 45](#_Toc36368961)

[8-3-1.ログ収集スケジュール 45](#_Toc36368962)

[8-3-2.ログ収集タイミング 46](#_Toc36368963)

[9.管理対象PCの設定変更 47](#_Toc36368964)

[9-1.設定変更の方法 48](#_Toc36368965)

[9-2.WorkGroup環境での管理対象PC設定内容 49](#_Toc36368966)

[9-3.ActiveDirectory環境での管理対象PC設定内容 67](#_Toc36368967)

[9-3-1.グループポリシー設定変更項目 68](#_Toc36368968)

[9-3-2.LogVillageMGRに登録する管理対象PCのユーザー設定項目 89](#_Toc36368969)

[9-3-2-1.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 91](#_Toc36368970)

[9-3-2-2.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 99](#_Toc36368971)

[10.LogVillageMGR画面の基本操作 111](#_Toc36368972)

[10-1.LogVillageMGR画面の表示方法 111](#_Toc36368973)

[10-2.画面概要 112](#_Toc36368974)

[10-3.システム設定画面 113](#_Toc36368975)

[11.管理対象PC自動設定ツール 114](#_Toc36368976)

[11-1.LogVillage 管理対象PC設定ツール 114](#_Toc36368977)

[11-1-1.対応OS 114](#_Toc36368978)

[11-1-2.管理対象PCでの実行時の注意事項 114](#_Toc36368979)

[11-1-3.設定手順 115](#_Toc36368980)

[11-2.管理対象PCをLogVillageマネージャに登録する 117](#_Toc36368981)

[12.LogVillage運用のための情報 118](#_Toc36368982)

[12-1. LogVillage マネージャ動作関連ログファイル 118](#_Toc36368983)

[12-1-1.ログ保存場所 118](#_Toc36368984)

[12-1-2.ログ保存期間 118](#_Toc36368985)

[12-2.LogVillage ポーリングサーバー動作関連ログファイル 119](#_Toc36368986)

[12-2-1.ログ保存場所 119](#_Toc36368987)

[12-2-2.ログ保存期間 119](#_Toc36368988)

[12-3. Apache2動作関連ログファイル 120](#_Toc36368989)

[12-3-1.ログ設定方法 120](#_Toc36368990)

[12-3-2.ログ保存場所 120](#_Toc36368991)

[12-3-3.ログ保存期間 120](#_Toc36368992)

[13.SSL（暗号化）通信設定 121](#_Toc36368993)

[14.お問合せ 124](#_Toc36368994)

[＜＜　　　補足資料　　　＞＞ 125](#_Toc36368995)

[「8-3-1.ログ収集スケジュール」にPC利用ログを追記 129](#_Toc36368996)

# 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 2022

Windows Server 2019

Windows Server 2016

Windows Server 2012 R2

Windows Server 2012

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

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

OS Windows Server 2022

Windows Server 2019

Windows Server 2016

Windows Server 2012 R2

Windows Server 2012

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。

※ドメインコントローラとの共存は行えません。

※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。

。

【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

■管理対象PCのOS

OS Windows11 Pro, Education, Enterprise

Windows10 Pro, Education, Enterprise

Windows8.1 Pro, Enterprise

Windows Server 2022

Windows Server 2019

Windows Server 2016

Windows Server 2012 R2

Windows Server 2012

macOS 10.3以降（※1）

Linux（対応ディストリビューション、バージョンは別途お問合せください）（※2）

※1. 別途macOS対応オプションが必要となります。

※1. 別途Linux対応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  　： LogVillageMGR | ・Webアプリケーション  　－LogVillage全体のシステム設定画面  　－ログ情報の検索・参照画面  　－稼働状況のモニタリング画面  ・データベース  　－ログ情報の蓄積  　－システム設定情報の保存 |
| LogVillageポーリングサーバー  ：LogVillagePS | ・ログ情報の収集（ポーリング）  ・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 |
| LogVillage PCエージェント | ・管理対象PCのログオン・オフ取得 |
| Phantosysログ取得サーバエージェント | ・Phantosysブートサーバのログ取得 |
| Phantosysログ取得クライアントエージェント | ・PhantosysクライアントのPhantosys関連ログ取得 |
| 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 | ・LogVillageにてログ情報を収集されるPC端末（被管理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.構成イメージ図

LogVillage構成要素の関係イメージ図は下図の通りです。

LogVillageマネージャ

http or https

Phantosysブートサーバ

Phantosys冗長サーバ

管理画面

データベース

管理PC

Webアクセス

TCP 4003

Phantosysログ取得

クライアントエージェント

LogVillage

PCエージェント

ログオン・オフ情報

Phantosys

サーバログ情報

Phantosys

サーバログ取得

TCP 80 or 443

LogVillageポーリングサーバ

Phantosysログ取得

サーバエージェント

イベントログ、Web閲覧ログ取得

TCP 135/139/

445

UDP 137/138

Phantosys

クライアントログ情報

管理対象PC群

## 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。
3. 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

1. 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。

**logVillageマネージャ：Mgr**

データ

ベース

Apache

Mgr:Spool Dir

logVillage：PS

logVillage：PS

logVillage：PS

②

③

①

Mgr:サービス

PHP

管理対象PC

http

https

http

④

・DCOM用 135:TCP

・NetBIOS用 139:TCP　445:TCP　137:UDP　138:UDP

・未使用の20ポート（ハイポート）

管理コンソール

## 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

・MySQL 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）

・Maneger 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へ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

導入前の準備と確認

（導入マニュアル：3.導入前の準備と確認）

LogVillageマネージャのインストール

（導入マニュアル：4.LogVillageMGRのインストール）

LogVillageポーリングサーバーのインストール

（導入マニュアル：5.LogVillagePSのインストール）

LogVillageの基本設定

（導入マニュアル：6.LogVillageの基本設定）

管理対象PCの設定変更

（導入マニュアル：7.管理対象PCの設定変更）

ユーザー様の運用に合わせて設定を変更します。

「運用マニュアル」をご確認ください。

# 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。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No. | プロト コル | 通信手段 | LogVillagePS側 ポート番号 | 通信方向 | 管理対象PC側 ポート番号 |
| 1 | TCP | 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 | SMBサービス | any | LogVillagePS→PC | 445 |
| 4 | 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 | UDP | NetBIOS名前サービス | any | LogVillagePS→PC | 137 |
| 8 | NetBIOS名前サービス | any | No.9のreturn | 137 |
| 9 | 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。

－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

〇アクセスが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。

○FireWall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。

○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ファイルの例　　　＞＞

■WORKGROUP環境の場合

コンピュータ名,ユーザー名,パスワード,グループ名,ポーリングサーバー名,

PC-NAME1,user1,passwd1,ALL,ps1,

PC-NAME2,user2,passwd2,ALL,ps1,

PC-NAME3,user3,passwd3,ALL,ps1,

PC-NAME4,user4,passwd4,ALL,ps1,

■ActiveDirectory環境の場合

コンピュータ名,ユーザー名,パスワード,グループ名,ポーリングサーバー名

PC-NAME1,user.local\logvillage,passwd1,ALL,ps1,

PC-NAME2,user.local\logvillage,passwd1,ALL,ps1,

PC-NAME3,user.local\logvillage,passwd1,ALL,ps1,

PC-NAME4,user.local\logvillage,passwd1,ALL,ps1,

1. 「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。
2. 「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

1. 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。



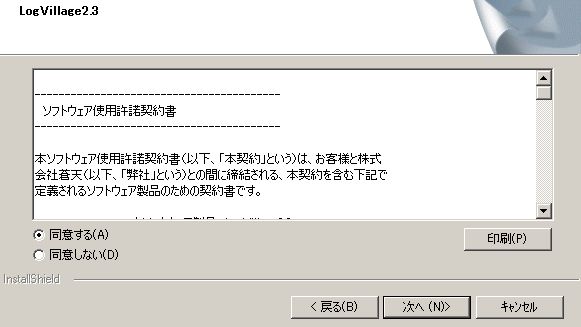
1. 内容を確認し「次へ」をクリックします。

「次へ」をクリックします。



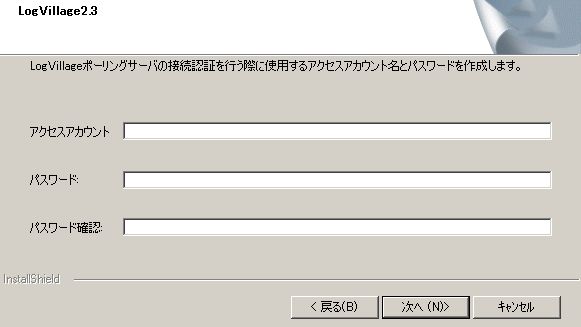
ソフトウェア使用許諾契約書を確認し、問題なければ「同意する」を選択し、

「次へ」をクリックします。



1. 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。



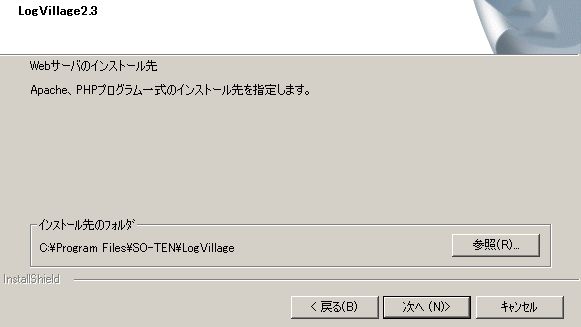
**アクセスアカウント、パスワードは「5-2.LogVillagePSのセットアップ」時で必要になりますので、大切に保管下さい。**

**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。**

1. 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。

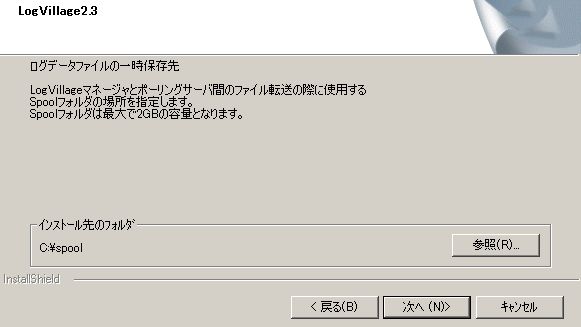
インストール先を変更する場合は、参照からインストール先フォルダを指定後、「次へ」をクリックします。



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。

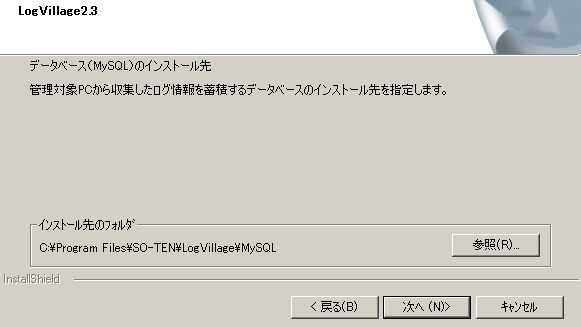
インストール先を変更する場合は、参照からインストール先フォルダを指定後、「次へ」をクリックします。



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。

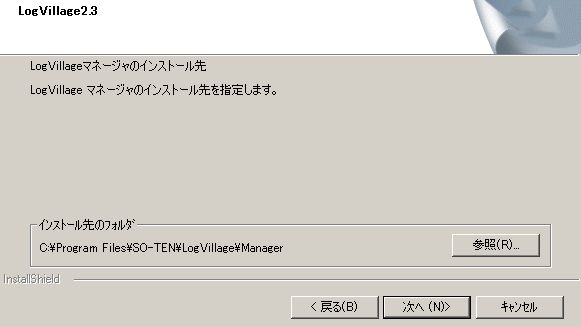
インストール先を変更する場合は、参照からインストール先フォルダを指定後、「次へ」をクリックします。



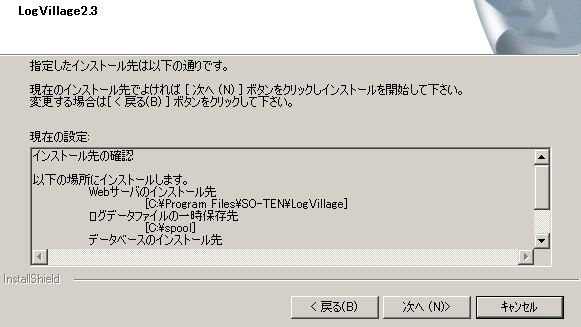
LogVillageマネージャのインストール先を指定します。

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。



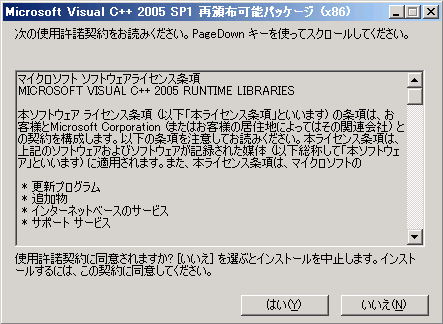
設定内容を確認し、問題なければ「次へ」をクリックします。



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。

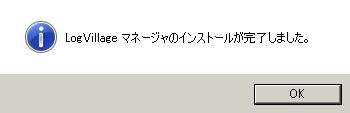
そのため、以下のマイクロソフト ソフトウェアライセンス条項に同意いただく必要があります。

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



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

「OK」をクリックするとインストール完了です。



## 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。

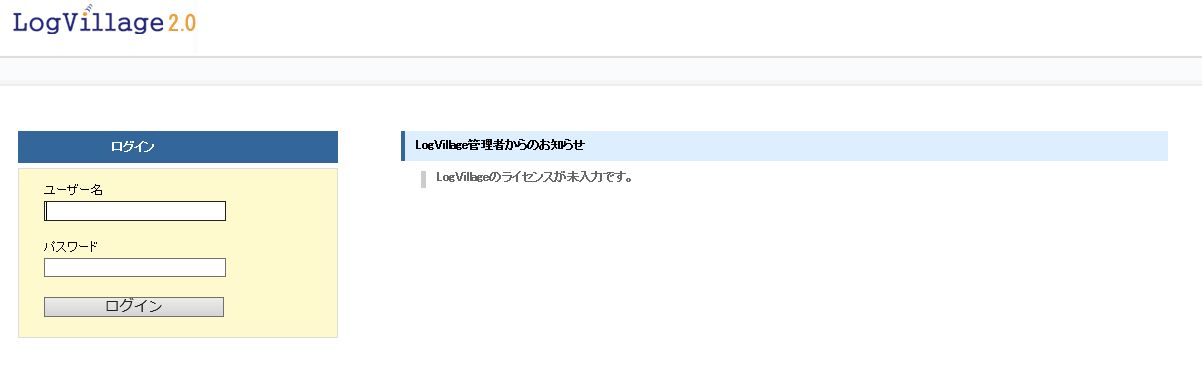
1. LogVillgae管理画面にログインします。

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。



**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。**

**・ユーザー名 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。**

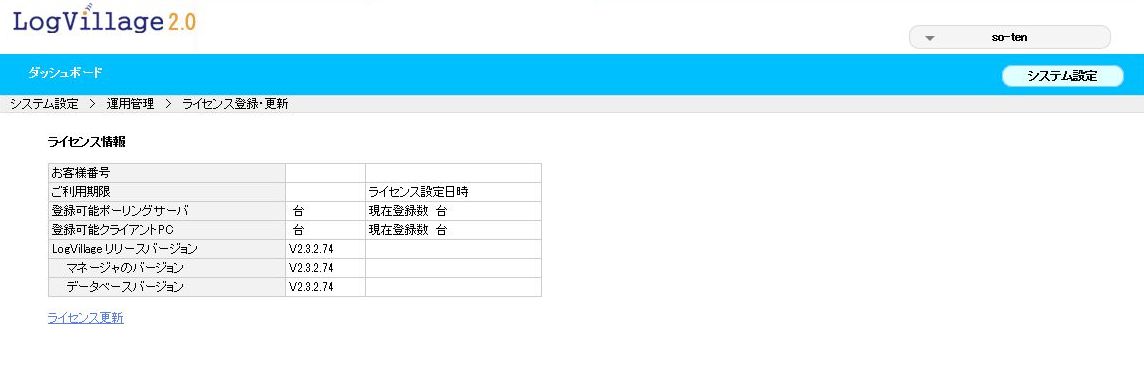
1. 「ライセンス登録・更新」画面を開きます。

「システム設定」→「ライセンス登録・更新」をクリックします。



1. 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。



「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。



1. 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。

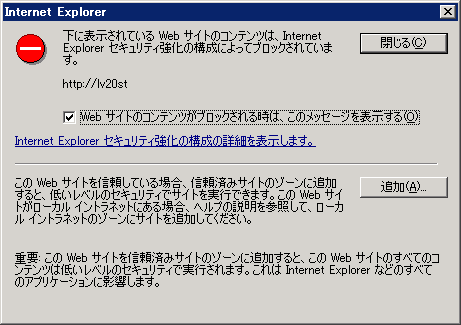


【ご注意ください】

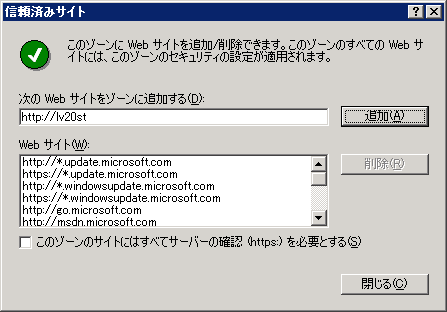
Internet Explorerにて上記操作時に以下の画面が表示される時は、

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。



1. 「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

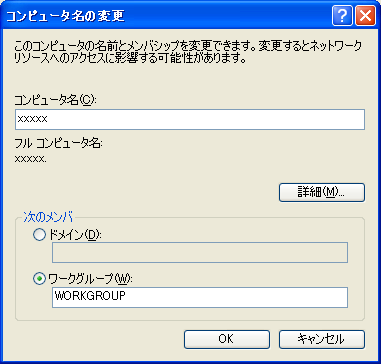
## 5-1.インストールおよび運用環境について

**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 | ○ |
| 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。

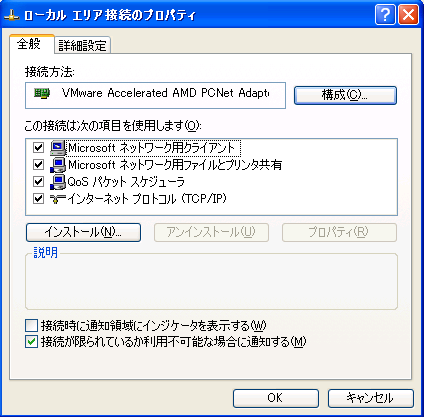
「次のメンバ」が「ドメイン」の場合は「ActiveDirectory」に　　　参加しています。

「ワークグループ」の状態でインストールを実施します。

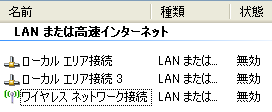
**5-1-2.LogVillagePSのインストール環境**

**(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」（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

1. 「コンポーネントサービス」を起動します。

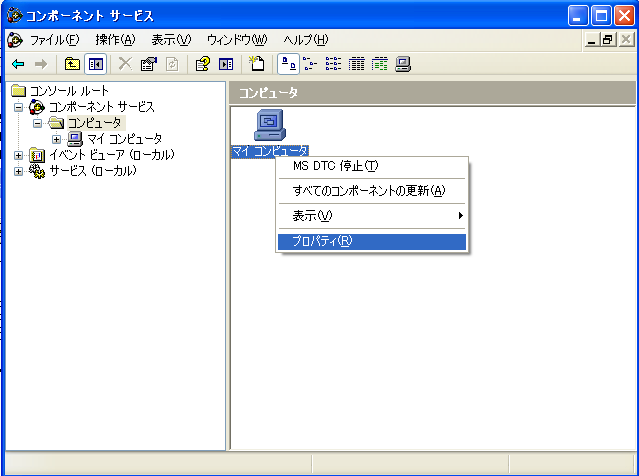
"Windowsスタートメニュー"→「コントロールパネル」→「管理ツール」→「コンポーネント サービス」を起動します。

※「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。

1. 「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。

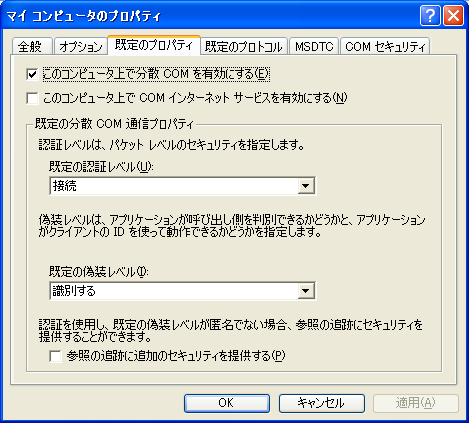
「マイコンピュータ」を右クリックし「プロパティ」をクリックします。



1. 「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。



**(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。**

1. 「ローカルセキュリティポリシー」を起動します。

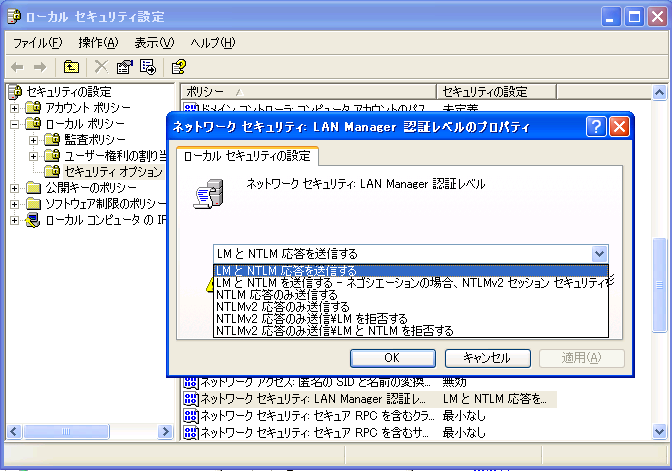
"Windowsスタートメニュー"→「コントロールパネル」→「管理ツール」→「コンポーネント サービス」を起動します。

1. 「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」→「監査ポリシー」を開きます。

1. 「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。

****

**(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WindowsOS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。

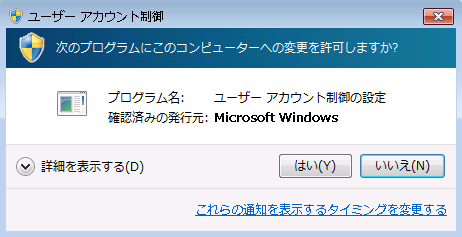
※「ユーザー アカウント」の表示のためには「コントロールパネル」で「小さいアイコン」または「大きいアイコン」の選択が必要です。

1. 「ユーザー アカウント制御設定の変更」を変更します。

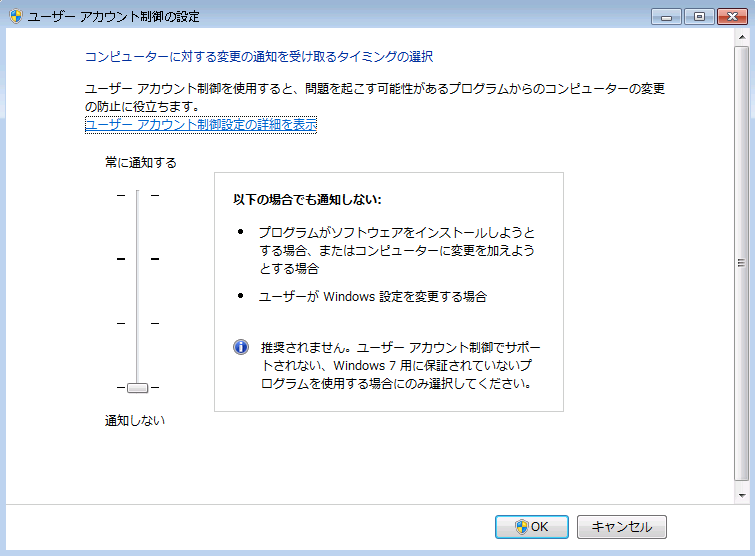
「ユーザー アカウント制御設定の変更」をクリックします。



下図が表示された場合は、「はい」をクリックします。

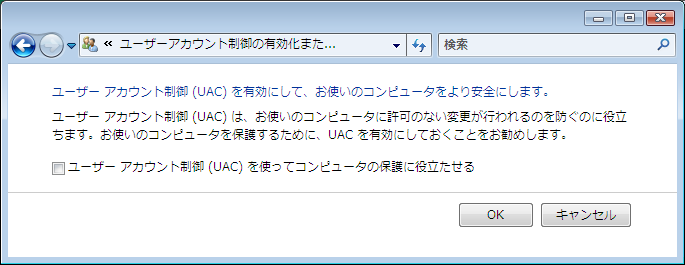


スライダのつまみを一番下「通知しない」まで下げ、「OK」をクリックします。

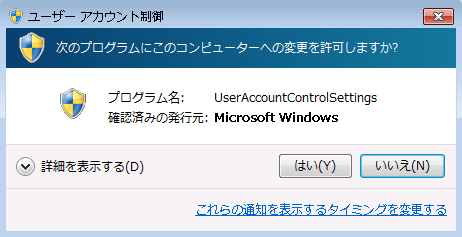


※OSにより、下図の場合があります。

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。



下図が表示された場合は、「はい」をクリックします。



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。

1. 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。



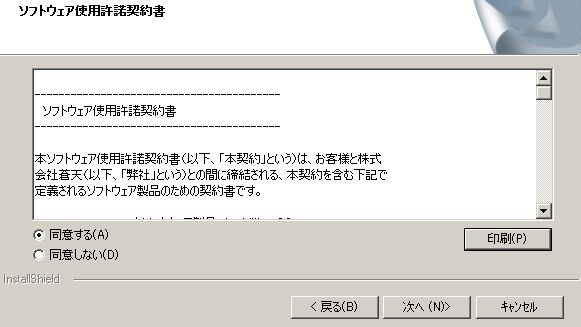
1. 内容を確認し「次へ」をクリックします。

「次へ」をクリックします。



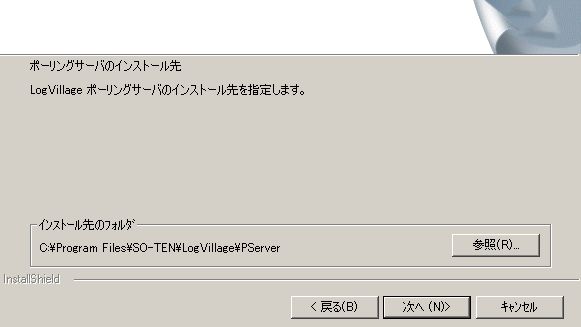
1. ソフトウェア使用許諾契約書を確認し、問題なければ「同意する」を選択し、

「次へ」をクリックします。



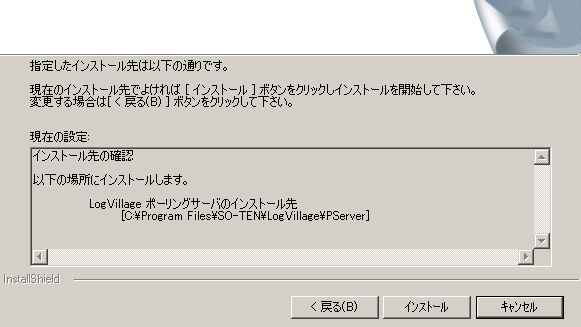
1. LogVillagePSのインストール先フォルダを変更しない場合は「次へ」をクリックします。

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。



1. 「インストール」を実行します。

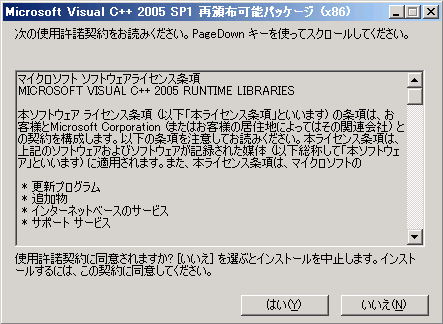
「インストール」をクリックします。



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。

1. インストール完了までしばらく待ちます。
2. 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。



## 5-3.LogVillagePSのセットアップ

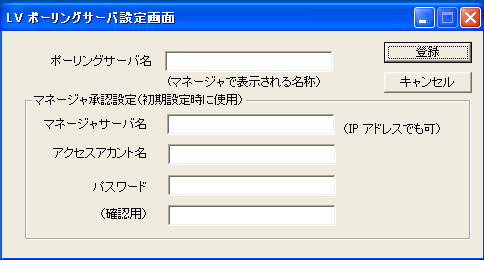
LogVillagePSのセットアップ手順について説明します。

1. 「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。

1. LogVillagePSの設定内容を入力します。

a



e

f

d

c

b

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。

1. 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。

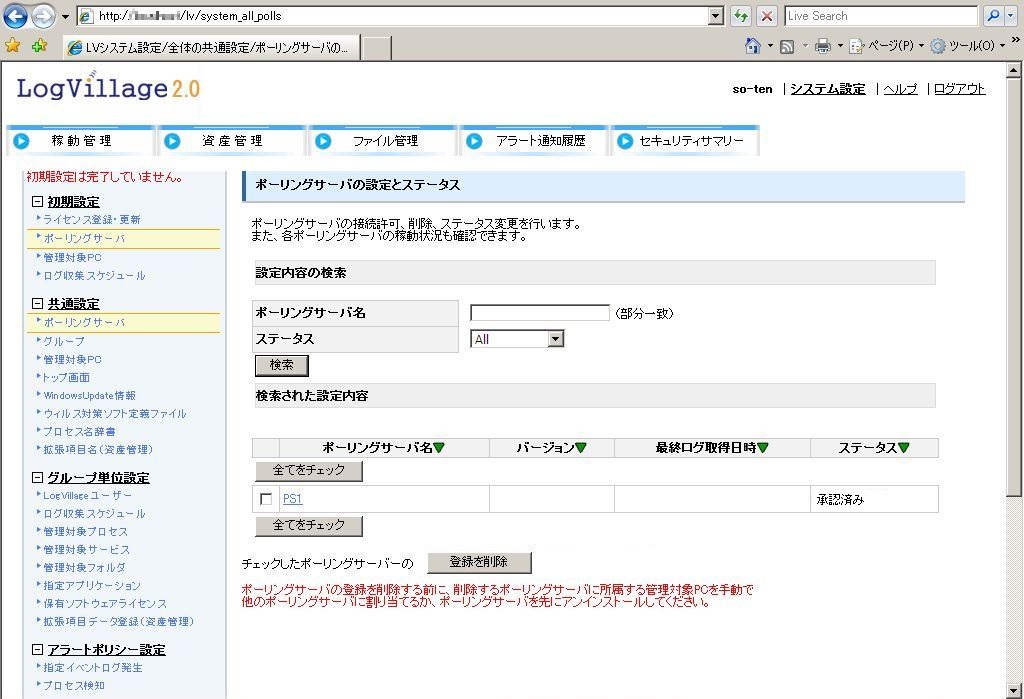
http://<LogVillageMGRのコンピュータ名>/lv/login/

1. 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。



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。



【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.LogVillage PCエージェントのインストール

　PCエージェントは、管理対象PCにインストールするPCログオン・オフ情報を取得する管理ソフトウェアであり、取得したログオン・オフ情報はLogVillageマネージャにアップロードされます。

　PCエージェントは、「Windosタスクスケジューラ」により自動実行され、「Windowsタスクスケジューラ」への登録はインストール時に自動で行われます。

## 6-1.PCエージェントの稼働環境

OS 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

500MB以上（LogVillagePCエージェントシステム用領域

## 6-2.PCエージェントのインストール前準備

　インストールの実行前に構成ファイルにLogVillageマネージャ情報を設定します。

1. 構成ファイルを開く

「ログオンオフ履歴用エージェント」フォルダ内のconfig.iniファイルをメモ帳等のテキストエディタで開きまｓ。

1. 構成ファイルを編集

（3行目）Server=[管理サーバのIPアドレス]

　SSL通信設定の場合、以下も編集します。

（4行目）Port=443

（5行目）SSL=1

***※構成ファイル（config.ini）は、必ずsetup.exe、Setup\_Lite.msiと同じ場所に保管してください。***

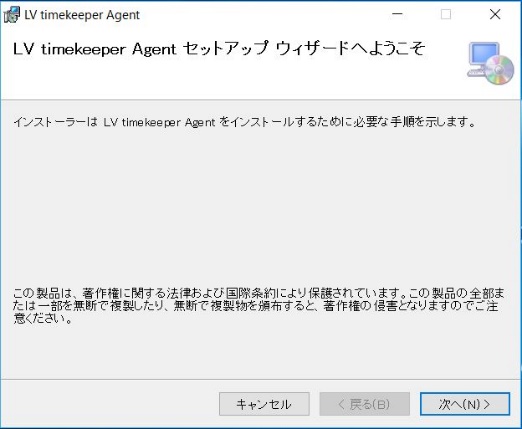
## 6-3.PCエージェントのインストール

1. ログオンオフ履歴用エージェント フォルダ内の「setup.exe」を起動

「この不明な発行元からのアプリがデバイスに変更を加えることを許可しますか？」と表示された場合は[はい]をクリックします。

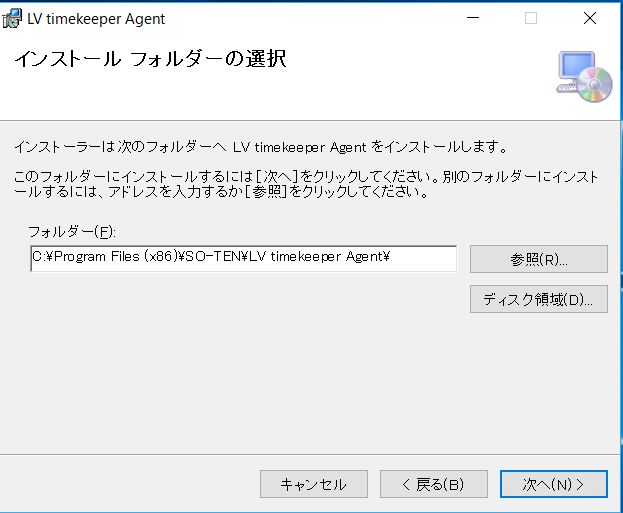
1. インストール開始

[次へ]をクリック



1. インストール フォルダの選択

エージェントプログラムのインストール先を変更する場合は[参照]をクリックしインストール場所を指定し［次へ］をクリック

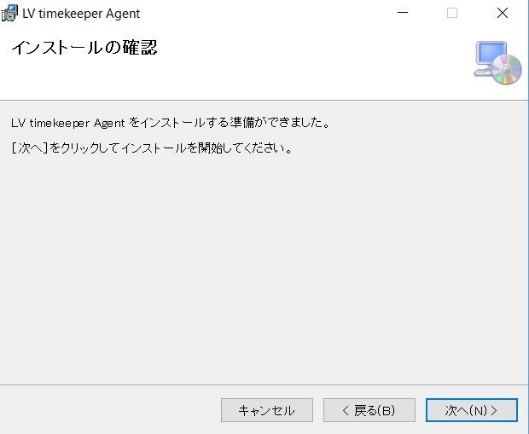


　　　※デフォルトのインストール場所は以下となります。

C:\Program Files (x86)\SO-TEN\LV timekeeper Agent

1. インストールの確認

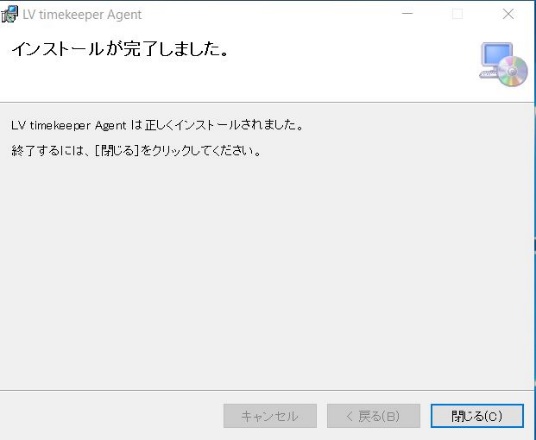
[次へ]をクリックし、インストールを開始します。



*※インストール開始後、「この不明な発行元からのアプリがデバイスに変更を加えることを許可しますか？」と表示された場合は[はい]をクリックします。*

1. インストール完了

[閉じる]をクリックし、インストールを終了します。



## 6-4.インストール確認

　タスクスケジューラにPCエージェントが登録されていればインストールに問題がありません。

1. タスクスケジューラを開く

コントロールパネル→管理ツール→タスクスケジューラ

1. 登録タスクを開く

左ペインより、[タスクスケジューラ ライブラリ]をクリック

1. 登録タスクを確認

中ペインに、以下のタスクが表示されていることを確認します。

・LV\_timeKeeper\_agent

・LV\_timeKeeper\_schedule

## 6-5.PCエージェントの起動間隔設定

　LogVillage管理画面の以下の設定間隔にて起動しログオン・オフ情報を取得します。

　（画面）　　：システム設定→グループ単位設定→ログ収集スケジュール

　（設定項目）：ALLグループの“PC利用ログ”項目に設定した分数

## 6-6.PCエージェントのアンインストール

　アンインストールを行う場合、以下の手順で行います。

　アンインストールを行うと、タスクスケジューラ設定も同時に削除されます。

1. プログラムと機能を開く

コントロールパネル→プログラムと機能

1. アンインストールを実行

「LV timeKeeper Agent」を右クリックし[アンインストール」を選択

*※インストールフォルダ「LogVillageAgent」はアンインストール後もログファイル、設定ファイルなどが残ります。*

*完全に削除するには、手動で同フォルダの削除を行ってください。*

# 7.Phantosysログ取得エージェントのインストール

Phantosysログを取得する場合にインストールを行ってください。

## 7-1.Phantosysログ・サーバエージェントのインストール

LogVillageポーリングサーバがインストールされているサーバへインストールを行います。

Phantosysログ・サーバエージェントはブートサーバ（冗長ブートサーバ）の**TCP 4003番ポートにて通信**を行います。

1. インストール

Phantosysログ用エージェント フォルダ→「Setup\_server」フォルダ内の

setup.exe を実行し、サーバ用エージェントをインストールします。

（デフォルトインストール先）

　C:\Program Files (x86)\SO-TEN\LogVillage\PhantosysLvServer

*※インストールウィザードにて変更可能です。*

1. 設定ファイル（config.ini）を編集

　1)サーバ用エージェントインストールフォルダ内の「config.ini」を開きます。

　2)以下を編集します。

[Config]

　　Server=　 *※ LogVillageマネージャのIPアドレス (例)192.168.50.100]*

Port=80 　 *※ SSL通信設定の場合は「443」*

SSL=0　 *※ SSL通信設定の場合は「1」*

Username=　*※ LogVillageマネージャインストール時に設定したアクセスアカウント名*

Password=　*※ 同上パスワード*

msInterval=2500　*※ 本設定は変更しません*

*ブートサーバ上のホストのステータ変更のチェック間隔[ms]*

Periodic=180　*※ ブートサーバ上の全ホストの最新ステータスのチェック間隔[s]*

*推奨値：180*

LinuxPeriodic=0　*※ ブートサーバ上の全Linuxホストの最新ステータスのチェック間隔[s]*

*Linuxホストがない場合：0、Linuxホストがある場合：30（推奨値）*

StatusPeriodic=30　*※ ブートサーバの全Windowsホストの最新ステータスのチェック間隔[s]*

*Windowsホストがない場合：0、Windowsホストがある場合：30（推奨値）*

List=1　*※ 本設定は変更しません*

UseWMI=1　*※ 本設定は変更しません*

UseSSH=0　*※ Linuxホストのログインアカウント名取得の設定*

*取得しない：0、取得する：1*

DualBoot=0　*※ ホストのWindowsOSのデュアルブートの有無の設定*

*デュアルブートなし：0、デュアルブートあり：1*

OSCheck=1　*※ 本設定は変更しません*

StatusLog=0　*※ 本設定は変更しません*

XML=0　*※ 本設定は変更しません*

Crypt=0　 *※ 取得データの暗号化設定（暗号化の場合、ウイルス対策ソフトの影響を受ける場合があります。）*

*0:暗号化なし、1:暗号化*

Debug=0　*※ 本設定は変更しません*

DebugLog=0　*※ 本設定は変更しません*

LogSize=150　*※ 動作ログファイルの最大サイズ(KB)*

LogCount=30　*※ 動作ログファイルのローテート最大ファイル数*

[FileShare]

Path=\\[MGRコンピュータ名]\decryptdata　*※ PIS連携時のみ設定*

*（PIS連携用ホストステータスファイルをファイル共有でMGRへ配置する場合のspoolの場所の設定）*

1. 設定ファイル（phantosys.ini）を編集

　1)サーバ用エージェントインストールフォルダ内の「phantosys.ini」を開きます。

　2)以下のPhantosysブートサーバ情報を編集します。

冗長ブートサーバの情報は、[Phantosys\_1]以下に記述します。

[Phantosys]

Display=　　*※ ブートサーバのコンピュータ名*

Server=　　 *※ ブートサーバのIPアドレス*

Port=4003　 *※ Phantosysへのアクセスポートが変更されている場合のみ変更*

Username=　 *※ Phantosysのアクセスユーザー名*

Password=　 *※ Phantosysのアクセスパスワード*

[Config]

Count=1　*※ 冗長ブートサーバの台数を記述します。*

[Phantosys\_1]　*※ 設定内容は[Phantosys]セクションとDisplay、Server以外は同じ*

Display=

Server=

Port=4003

Username=

Password=

*※2台目以降の冗長サーバは、[Phantosys\_2]、[Phantosys\_3]として記述します。*

1. Phantosys dllファイルをコピー

Phantosysシステムのファイル「PSA.dll」をサーバ用エージェントインストールフォルダにコピーします。

*※Phantosysシステムのファイル名が「PSA10.dll」等の場合、必ず「PSA.dll」にリネイムを行ってください。*

1. PCリストを作成

管理対象となるブートサーバに登録されているコンピュータ名のリストを以下のファイル仕様にて作成し、サーバ用エージェントインストールフォルダの保管します。

|  |  |
| --- | --- |
| 前提条件 | |
| ファイル名 | list.csv |
| ファイル配置場所 | server.exeと同じ場所  ※デフォルトの場所  C:\Program Files (x86)\SO-TEN\LogVillage\PhantosysLvServer |
| 文字コード | Shift-JIS |
| 改行コード | CRLF |
| レイアウト | ヘッダ行なし。（1行目からデータを記述） |

|  |  |  |  |
| --- | --- | --- | --- |
| 項目名 | 文字種/形式 | 必須/任意 | 記述法など |
| コンピュータ名 | 半角英数記号 | 必須 | PC-001  ※Phantosysに登録されているコンピュータ名 |

1. サービスを開始

コントロールパネル→管理ツール→サービスにて、「PhantosysLvServer」を開始します。

## 7-2.Phantosysログ・クライアントエージェントのインストール

PhantosysのWindowsクライアントPCへインストールを行います。

1. インストール

Phantosysログ用エージェント フォルダ→「Setup\_client」フォルダ内の

setup.exe を実行し、クライアント用エージェントをインストールします。

（デフォルトインストール先）

　C:\Program Files (x86)\LogVillage\PhantosysLvClient

*※インストールウィザードにて変更可能です。*

1. 設定ファイル（config.ini）を編集

　1)クライアント用エージェントインストールフォルダ内の「config.ini」を開きます。

　2)以下を編集します。

[Config]

　　Server=　 *※ LogVillageマネージャのIPアドレス (例)192.168.50.100*

Port=80 *※ SSL通信設定の場合は「443」*

SSL=0　 *※ SSL通信設定の場合は「1」*

Username= *※ LogVillageマネージャインストール時に設定したアクセスアカウント名*

Password= *※同上パスワード*

1. Phantosysファイルをコピー

Phantosysシステムのファイル「PCA.dll」をクライアント用エージェントインストールフォルダにコピーします。

1. サービスを開始

コントロールパネル→管理ツール→サービスにて、「PhantosysLvClient」を開始します。

## 7-3.Phantosysログ取得エージェントのアンインストール

1. サーバエージェントのアンインストール
2. ポーリングサーバのコントロールパネル→プログラムと機能を開く
3. 「PhantosysLvServer」を右クリックし“アンインストール“を選択
4. クライアントエージェントのアンインストール
5. クライアントPCのコントロールパネル→プログラムと機能を開く

2)「PhantosysLvClient」を右クリックし“アンインストール“を選択

# 8.LogVillageの初期設定

LogVillageの初期設定について説明します。

## 8-1.初期設定項目と設定方法

|  |  |  |
| --- | --- | --- |
| **初期設定項目** | **設定方法** | |
| **「システム設定」画面** | **設定内容** |
| （手順1）ライセンスを登録する | 「共通設定」  →  「ライセンス登録・更新」 | ・LogVillageMGRのインストール直後：  　LogVillageへのログイン後、「システム設定」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を登録する | 「共通設定」  →  「ポーリングサーバ」 | ・LogVillagePSの登録：  　LogVillagePS側よりを登録することで  “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を登録する | 「共通設定」  →  「管理対象PC」 | ・一括登録：  　CSVファイルより一括登録  ・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ールを設定する | 「グループ単位設定」  →  「ログ収集スケジュール」 | ・グループ別に設定可能  ・ログの種類別に設定可能 |

【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。

## 8-2. 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。

## 8-3.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。

### 8-3-1.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 |
| PC利用ログ | ・ログオン・オフ履歴  LogVillagePCエージェントからのログ情報アップロードの間隔。 |

※ご購入いただいた機能に限って設定可能です。

### 8-3-2.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

# 9.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。

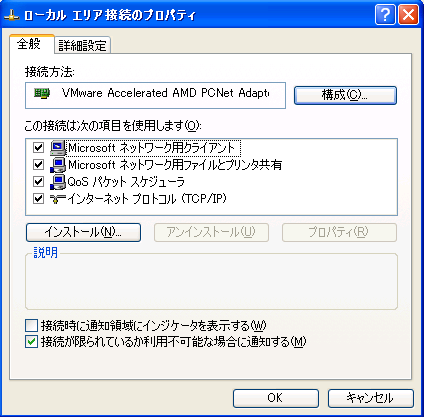
**前提条件**

・管理対象PCがネットワークに参加している事

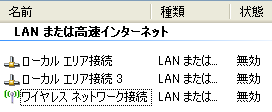
※「3-2. LogVillagePS→管理対象PCへのアクセス確認」を参照してください。

・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」（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

## 9-1.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。

2）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。

## 9-2.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。  「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」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。 |
| 設定内容 | ・「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** | **DCOM リモート起動のアクセス許可** |
| 目的 | WMI（ハードウェア台帳など）のWMI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 | ・「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」を有効にします。  「リモートからの起動」  「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 アカウント制御設定の変更」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。

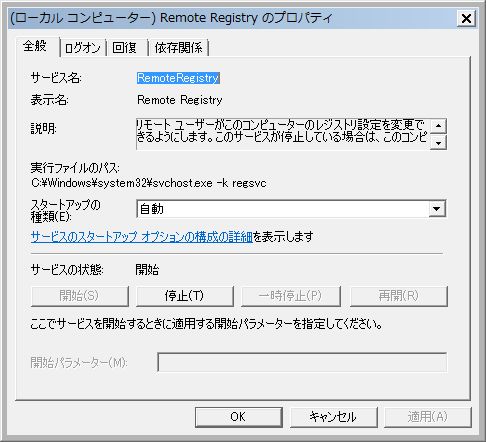
※「管理ツール」の表示のためには「コントロールパネル」で「小さいアイコン」または「大きいアイコン」の選択が必要です。

1. 「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。



**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。

1. 「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。

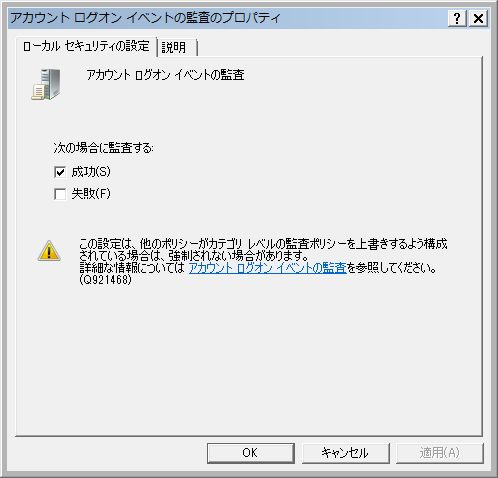
※「管理ツール」の表示のためには「コントロールパネル」で「小さいアイコン」または「大きいアイコン」の選択が必要です。

1. 「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。

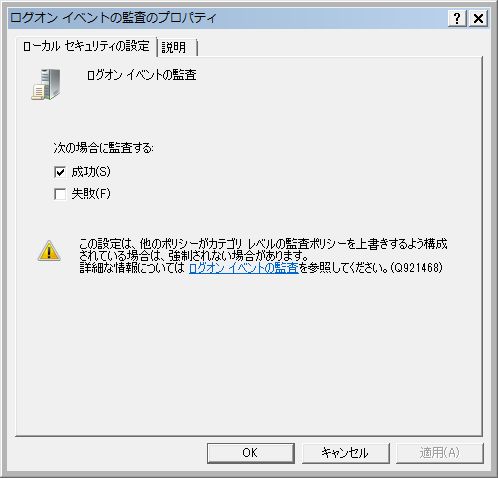
1. 「アカウントログオンイベントの監査」を変更します。

「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。



1. 「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。



【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。

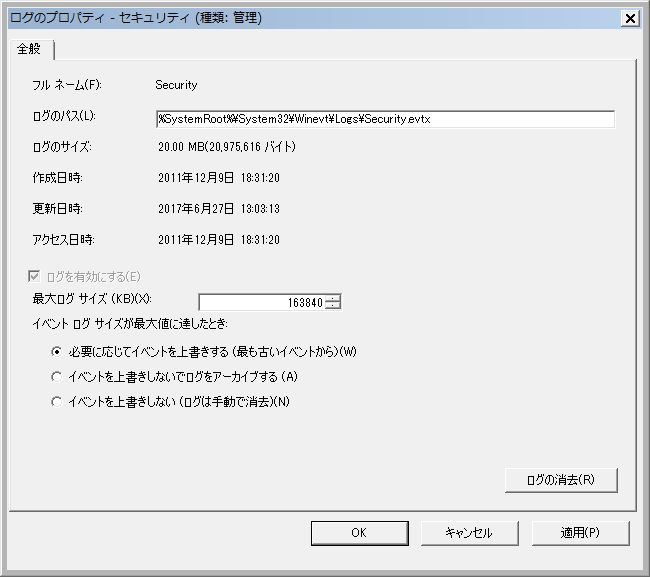
※「管理ツール」の表示のためには「コントロールパネル」で「小さいアイコン」または「大きいアイコン」の選択が必要です。

「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。



**3）ネットワークアクセス時のアカウント認証方法**

1. 「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。

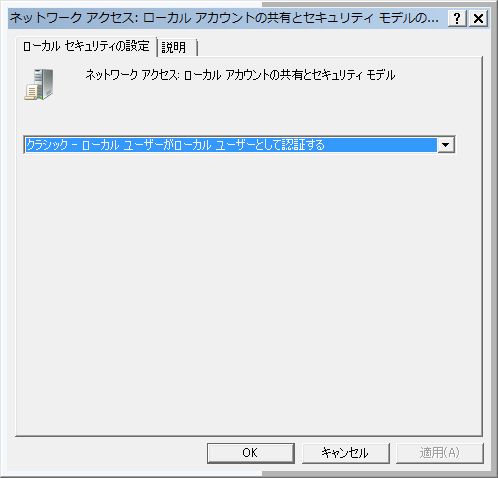
※管理ツール」の表示のためには「コントロールパネル」で「小さいアイコン」または「大きいアイコン」の選択が必要です。

1. 「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。



**4）DCOM リモート起動のアクセス許可**

WMI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WMI情報を基本としているため、WMI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。**

1. 「コンポーネントサービス」を起動します。

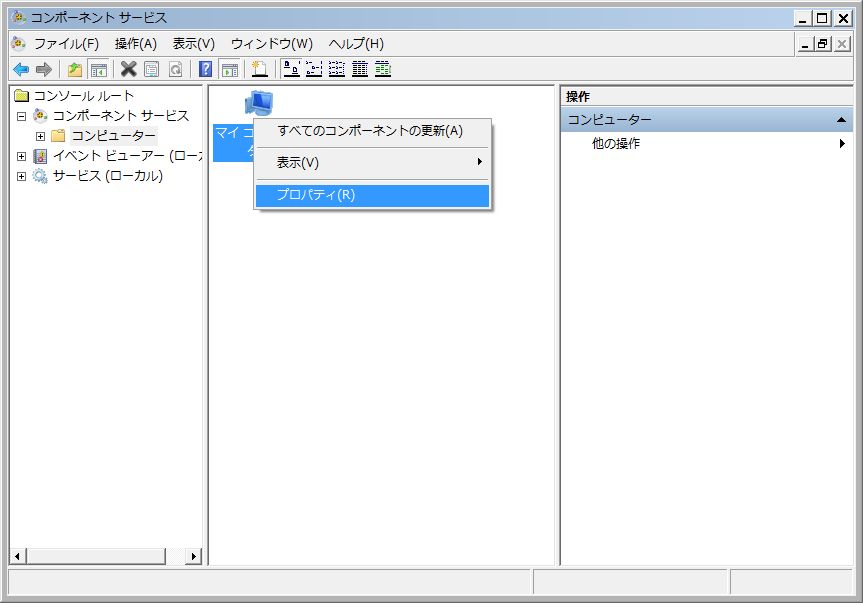
"Windowsスタートメニュー"→「コントロールパネル」→「管理ツール」→「コンポーネント サービス」を起動します。

※「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。

1. 「マイコンピュータ」のプロパティを開きます。

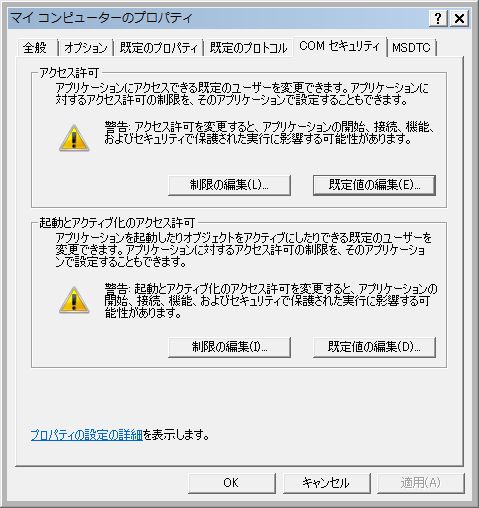
「コンソール ルート」→「コンポーネント サービス」→「コンピュータ」→「マイ コンピュータ」を開きます。

「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。



1. 「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。

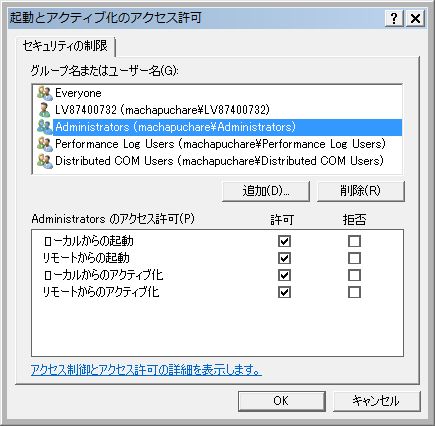


LogVillageで使用するユーザーまたはグループをクリックします。

「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。

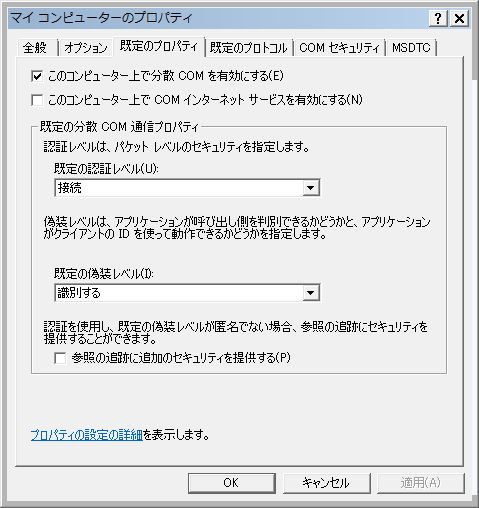
「許可」列の「リモートからのアクティブ化」にチェックを入れ、「OK」をクリックします。



1. 「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。

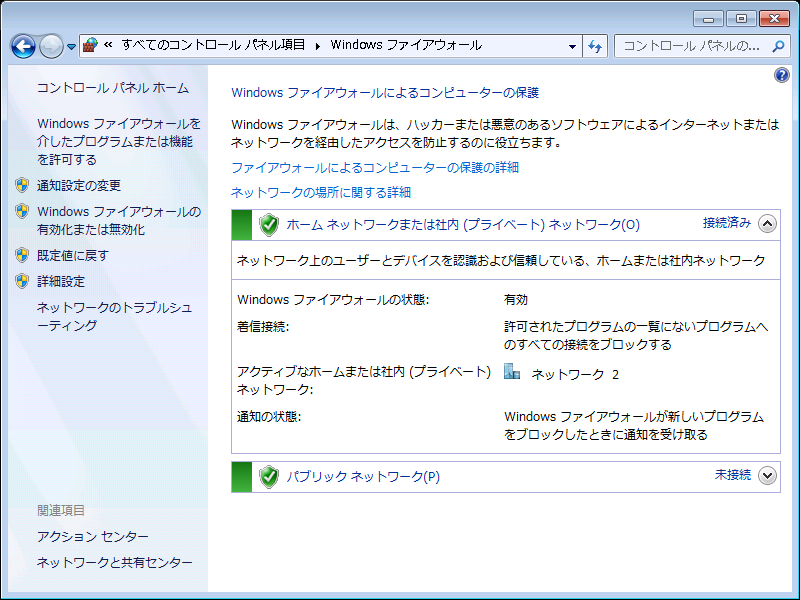
1. 「Windowsファイアウォール」を起動します。

"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。

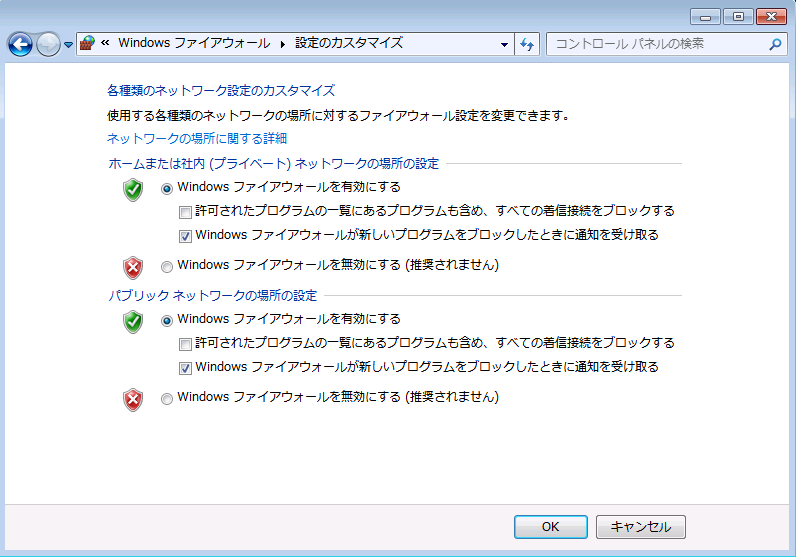
※「Windowsファイアウォール」の表示のためには「コントロールパネル」で「小さいアイコン」または「大きいアイコン」の選択が必要です。

1. 「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。

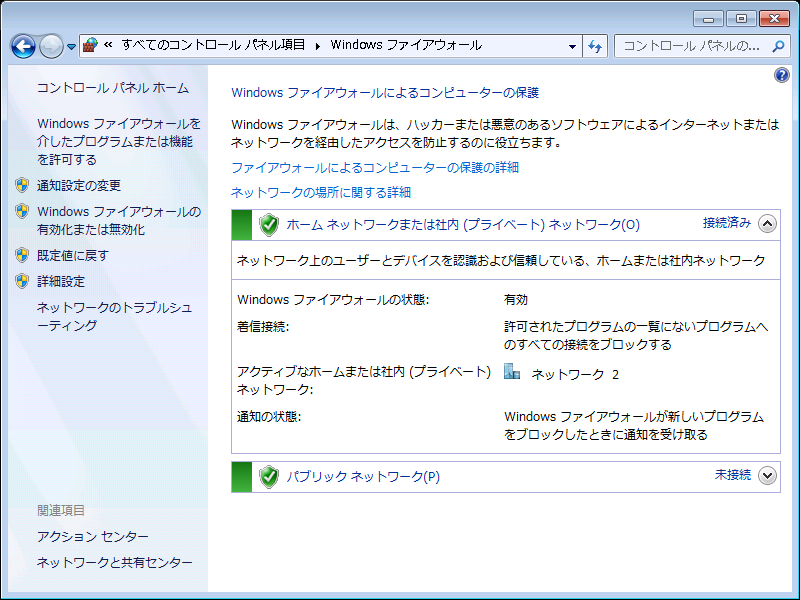


接続中ネットワークの「許可されたプログラムの一覧にあるプログラムも含め、すべての着信接続をブロックする」にチェックが無い事を確認し、「OK」をクリックします。

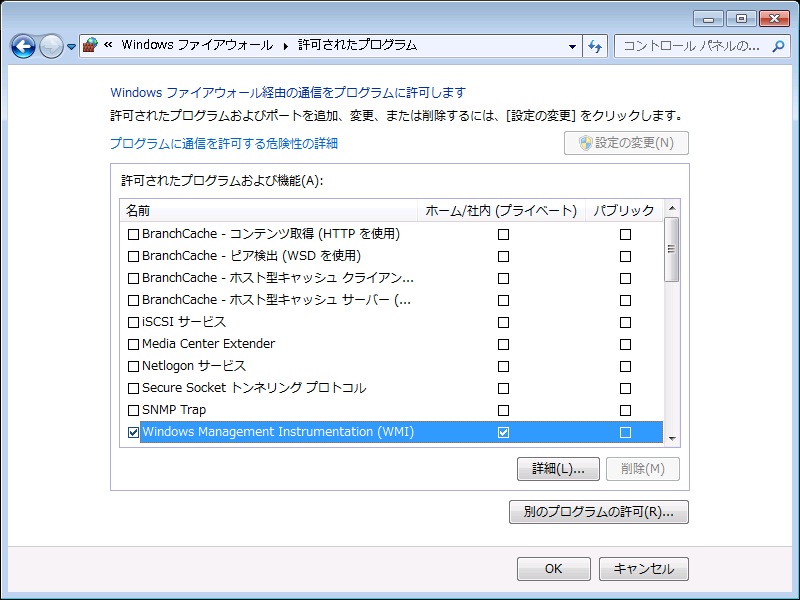


1. 「Windows Management Instrumentation (WMI)」を変更します。

「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。

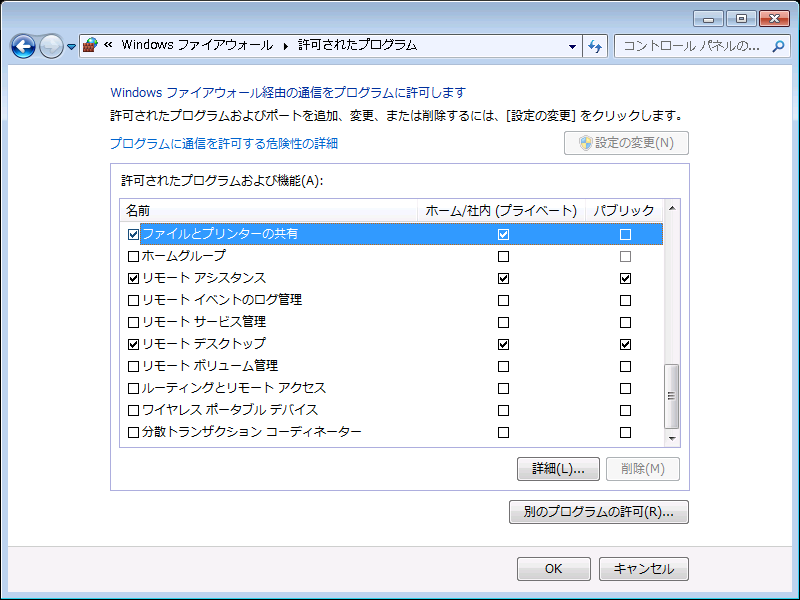


接続中ネットワークの「Windows Management Instrumentation (WMI)」にチェックを入れます。



1. 「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。

　　　**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。

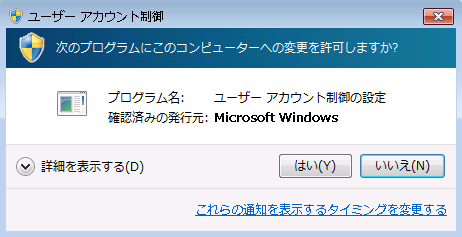
※「ユーザー アカウント」の表示のためには「コントロールパネル」で「小さいアイコン」または「大きいアイコン」の選択が必要です。

1. 「ユーザー アカウント制御設定の変更」を変更します。

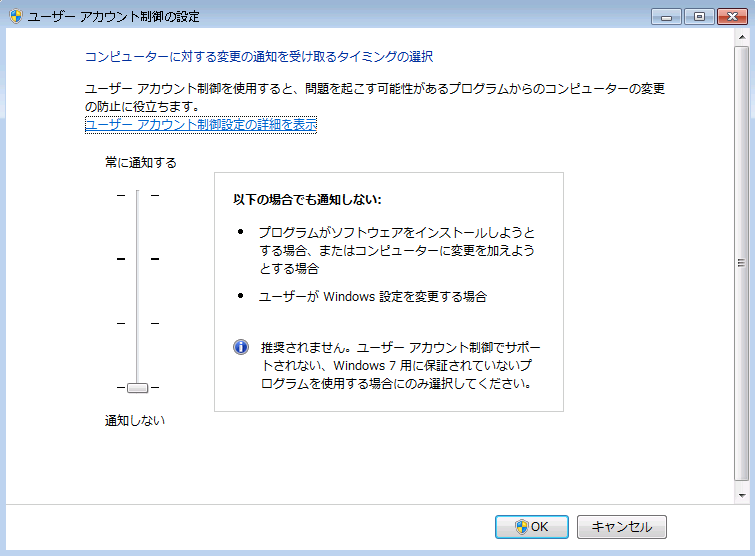
「ユーザー アカウント制御設定の変更」をクリックします。



下図が表示された場合は、「はい」をクリックします。

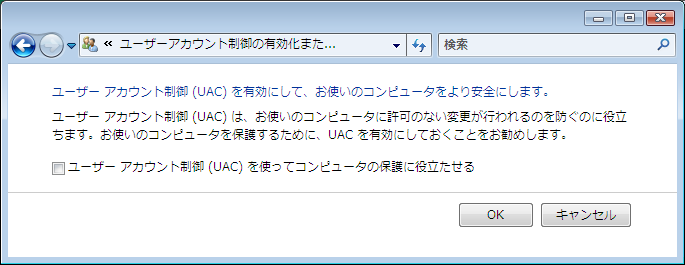


スライダのつまみを一番下「通知しない」まで下げ、「OK」をクリックします。

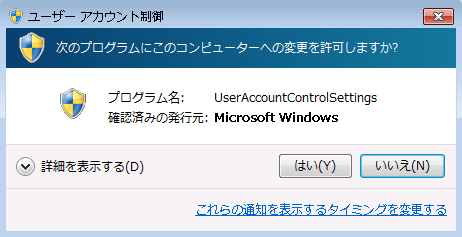


※以下のダイアログが表示される場合があります。

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。



「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。

|  |  |
| --- | --- |
| レジストリの場所 | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\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

　HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system

3) 任意の名前を付けて保存

## 9-3.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 Admins |

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** |
| 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

### 9-3-1.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。 |
| 設定内容 | ・「ローカルポリシー」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** |
| 目的 | WMI（ハードウェア台帳など）のWMI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 | ・「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。 |
| **□** | **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 | ・「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」  ・以下に「TCP135」を追加します。  「Windows ファイアウォール:ポートの例外を定義する」 |

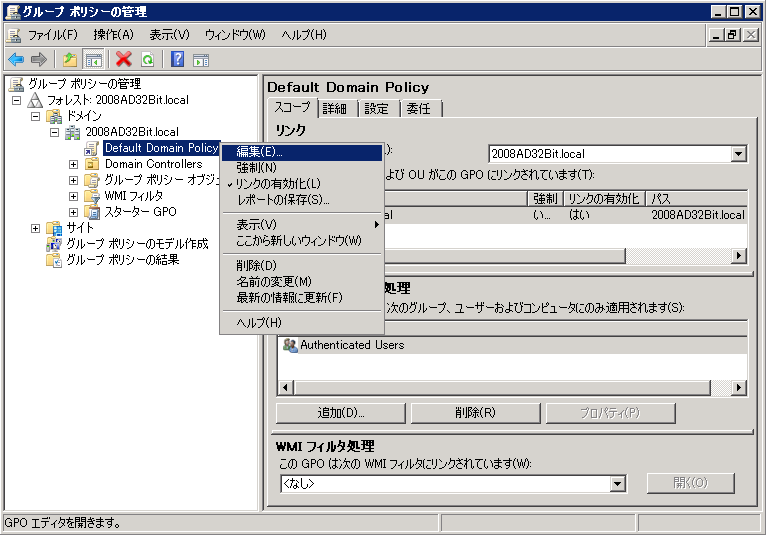
※チェックリストとしてご利用ください。

**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**

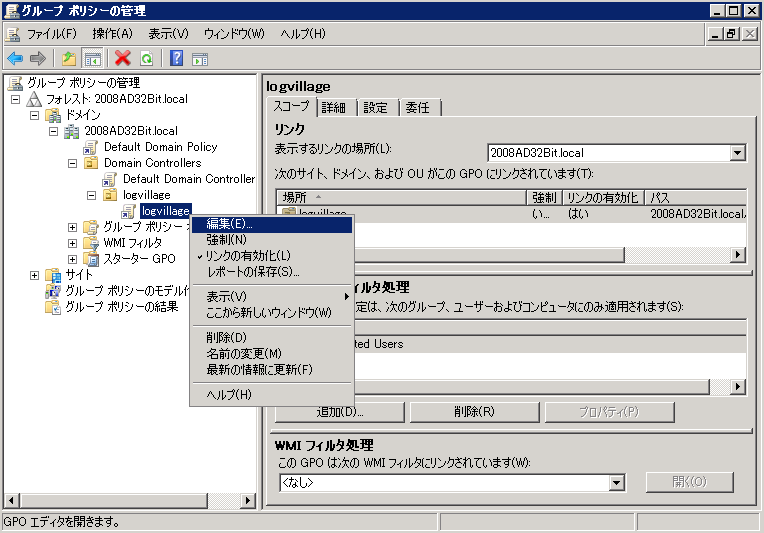
1. 「グループポリシーの管理」を起動します。

"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。

1. 設定を行うドメイン名またはOUを展開します。
2. 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。



③



左上図は、Default Domain Policy（全体）に設定する場合の例です。

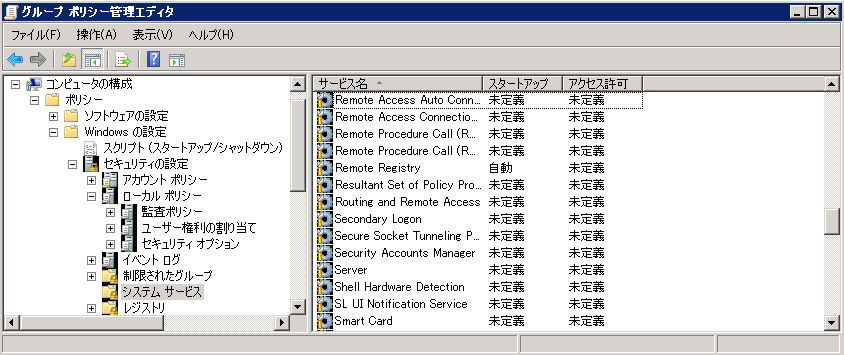
右下図は、OU名「logvillage」に、GPO名「logvillage」を作成し、設定する場合の例です。

1）リモートレジストリーサービス

1. 「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。



1. 「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。

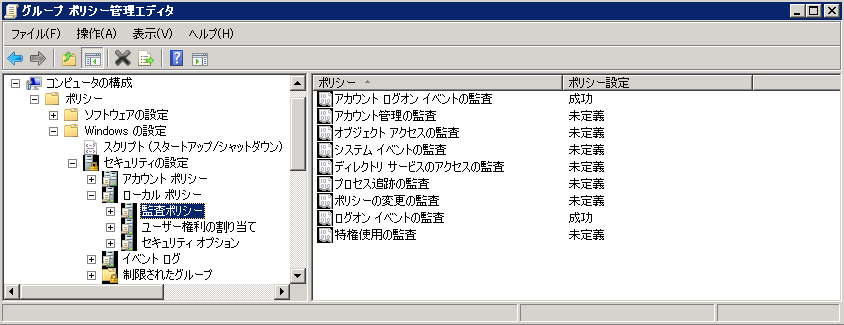


**2）アカウント・ログオン・ログ**

1. 「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。

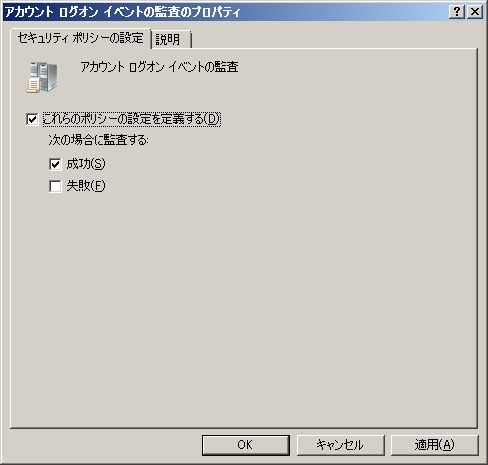


1. 「アカウント ログオンイベントの監査」を設定します。

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。

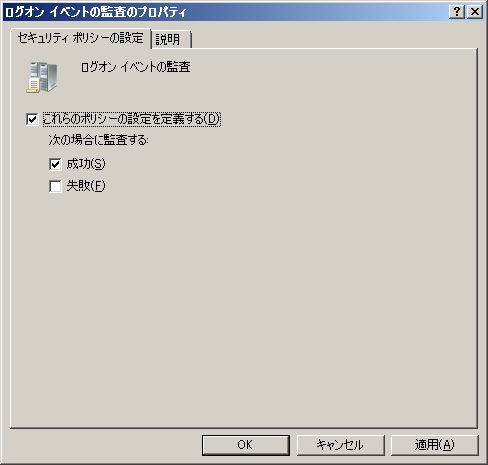


1. 「ログオンイベント の監査」を設定します。

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。



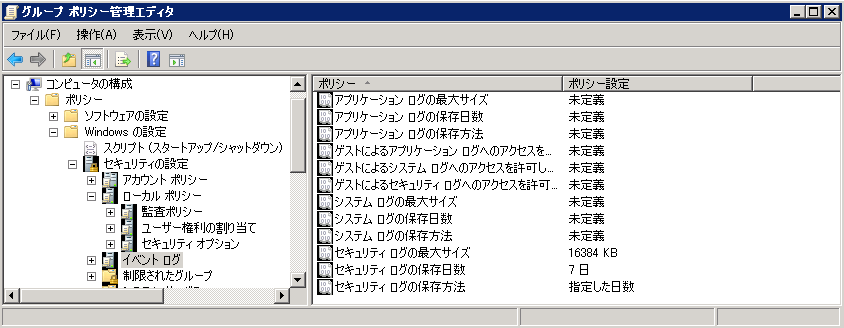
**イベントログの修正**

※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。

1. 「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。

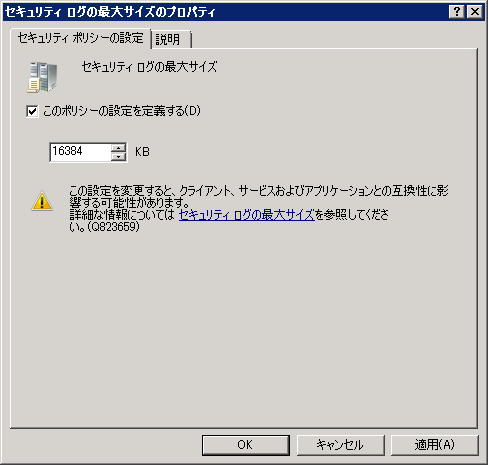


1. 「セキュリティログの最大サイズ」を設定します。

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

一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。

一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。

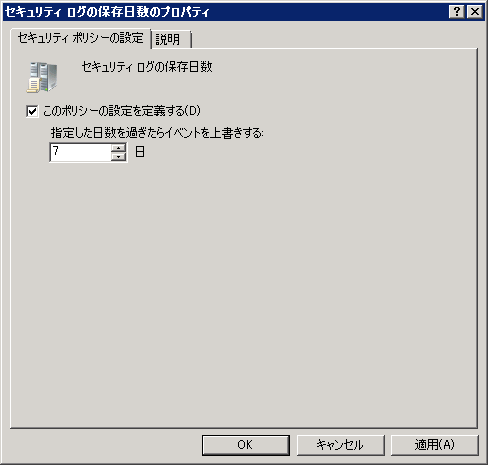
※以下では、「指定した日数を過ぎたら上書きする」「7日間」の設定をご案内します。

1. 「セキュリティログの保存日数」を設定します。

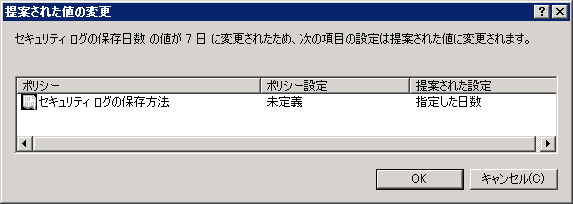
「セキュリティログの保存日数」をダブルクリックします。

「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。



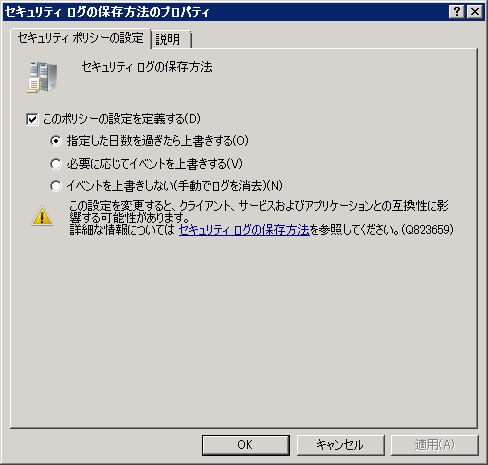
下図が表示されたら「OK」をクリックします。



1. 「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。

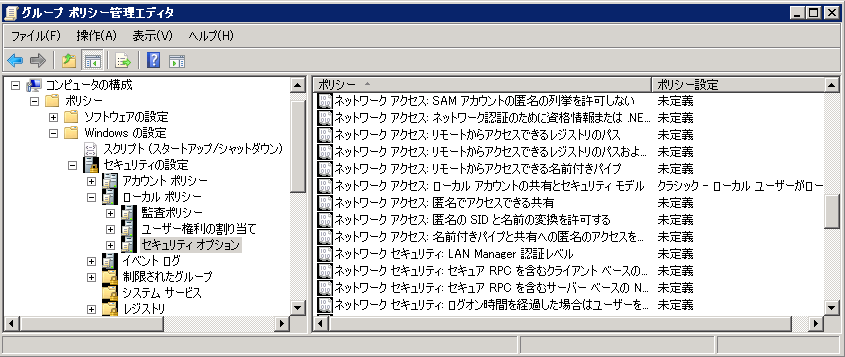


**3）ネットワークアクセス時のアカウント認証方法**

1. 「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。

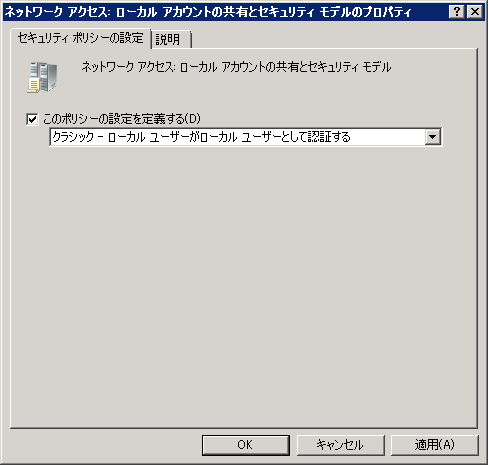


1. 「ネットワーク アクセス: ローカル アカウントの共有とセキュリティ モデル」を設定します。

「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－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。

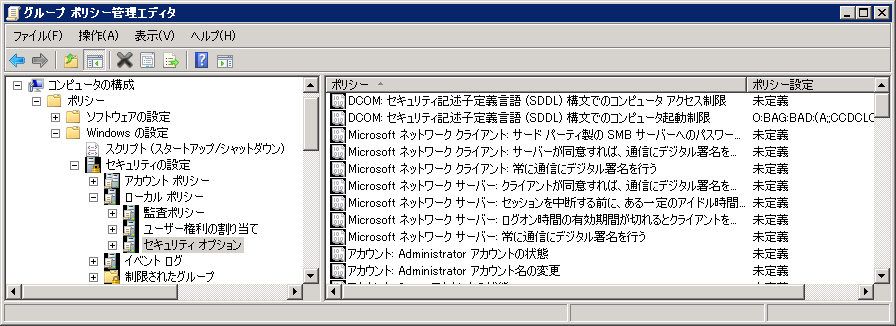


**4）DCOM リモート起動のアクセス許可**

1. 「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。

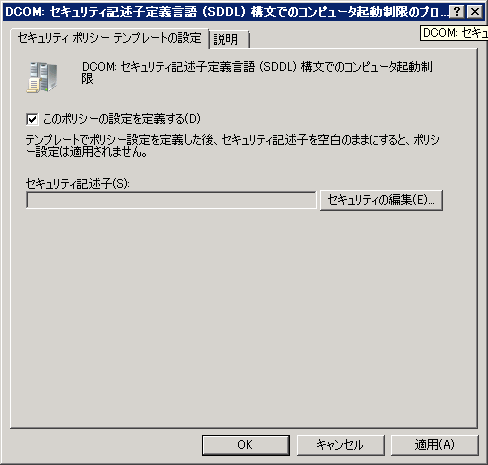


1. 「DCOM: セキュリティ記述子定義言語 (SDDL) 構文でのコンピュータ起動制限」を設定します。

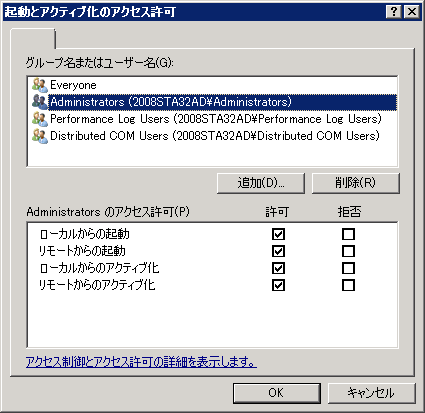
ポリシー名「DCOM: セキュリティ記述子定義言語 (SDDL) 構文でのコンピュータ起動制限」をダブルクリックします。

「このポリシーの設定を定義する」にチェックを入れます。

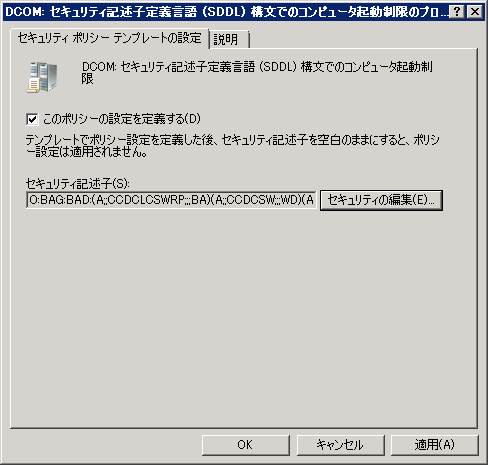
「セキュリティの編集」をクリックします。



「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。



1. 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へコピーします。

※xはOS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

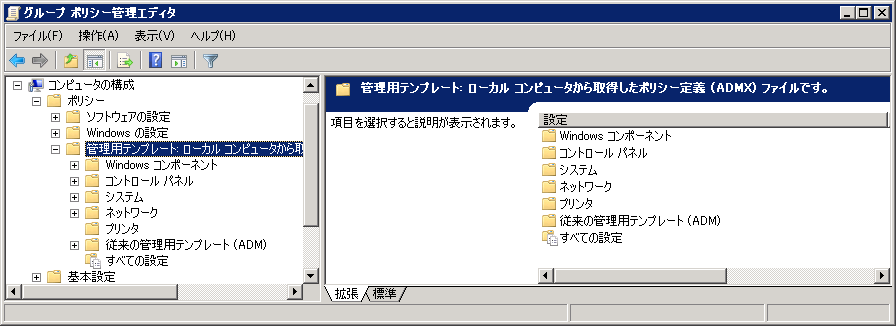
[strings]

LogVillageDCOM="LogVillage用DCOM設定"

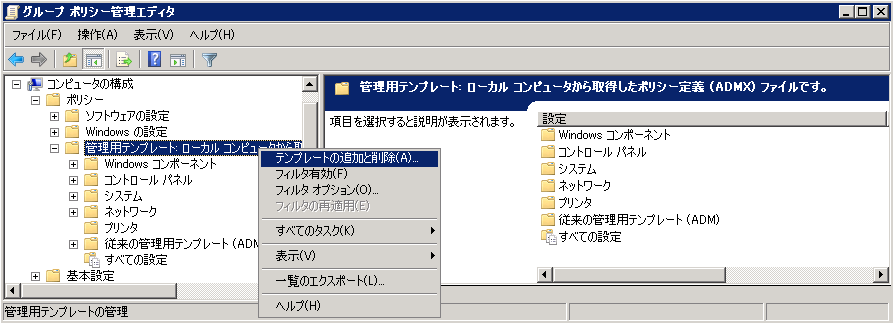
ChangeEnableDCOMPolicy="LogVillage用DCOM設定"

1. 「LogVillage用DCOM設定」を追加します。

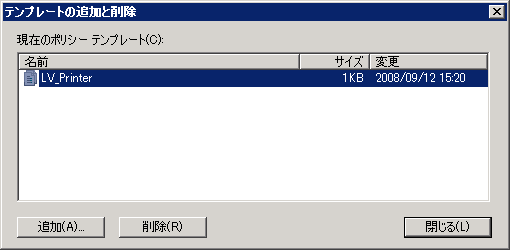
「コンピュータの構成」→「管理用テンプレート」を開きます。



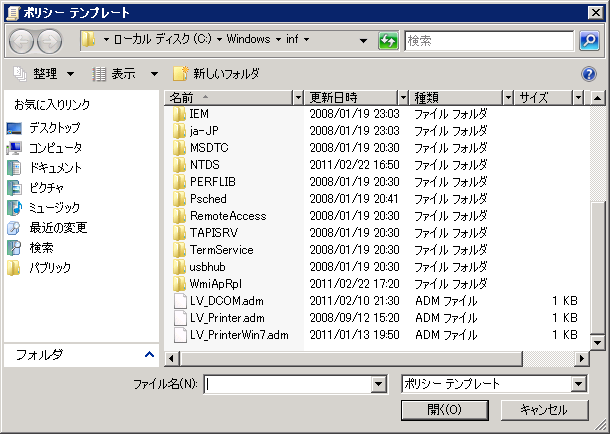
「管理用テンプレート」を右クリック、「テンプレートの追加と削除」をクリックします。



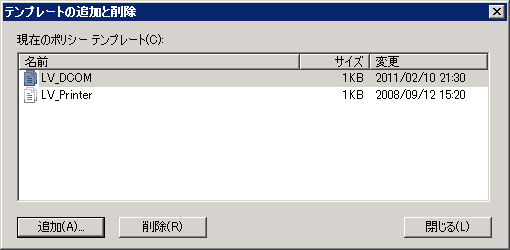
「追加」をクリックします。



「LV\_DCOM.adm」をクリック後、「開く」をクリックします。

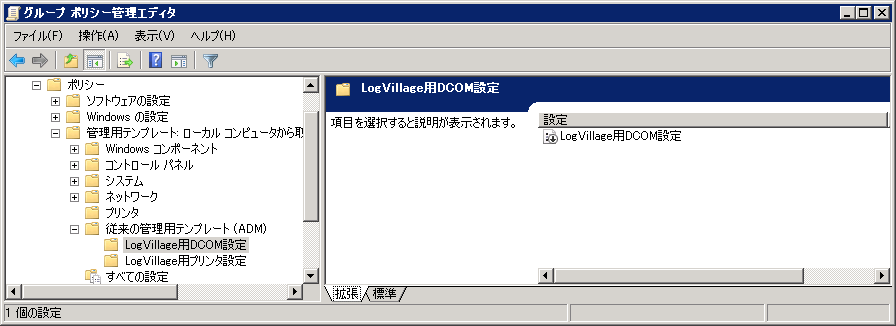


「LV\_DCOM」が一覧に表示された事を確認し、「閉じる」をクリックします。

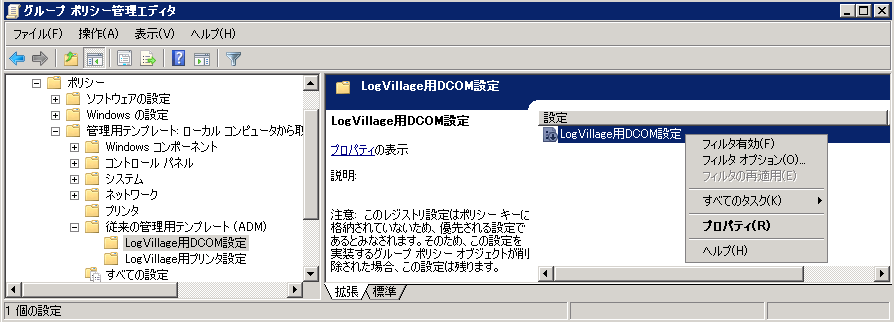


1. 「LogVillage用DCOM設定」を有効に変更します。

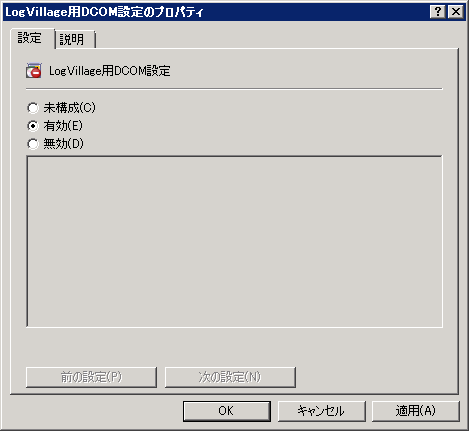
「管理用テンプレート」→「従来の管理テンプレート（ADM）」→「LogVillage用DCOM設定」をクリックします。



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



「有効」をクリック後、「OK」をクリックします。

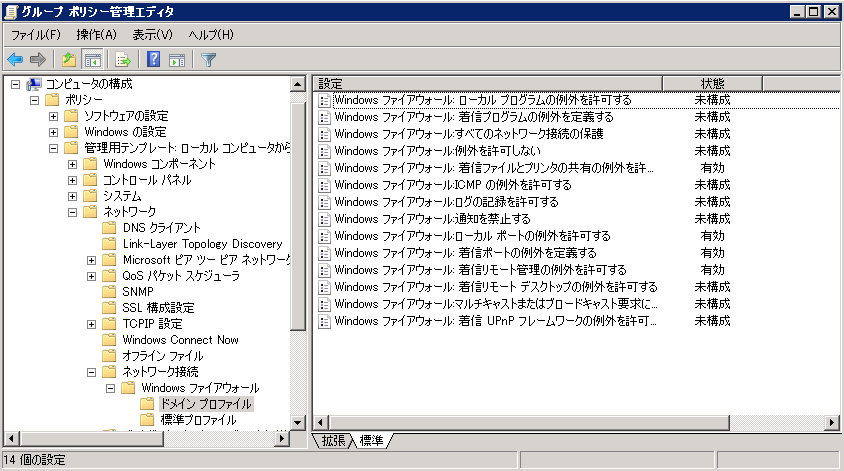


**5）ファイアウォール**

1. 「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。

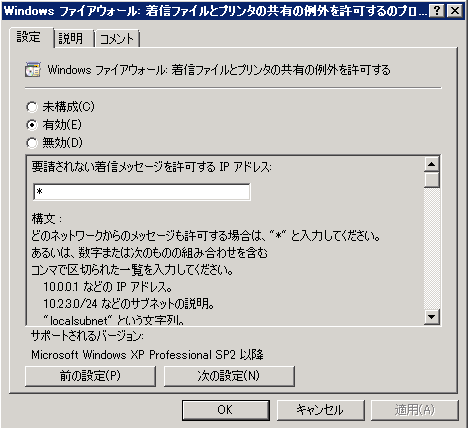


1. 「Windowsファイアウォール：着信ファイルとプリンタの共有の例外を許可する」を設定します。

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。

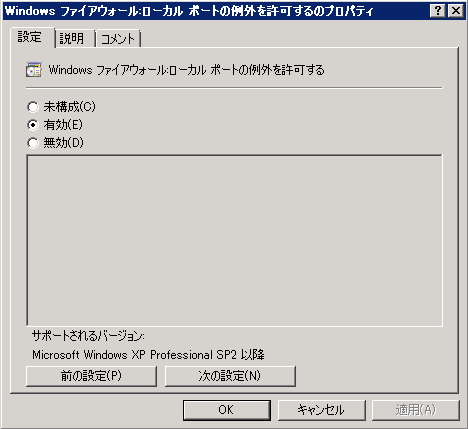
****

※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）

1. 「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。

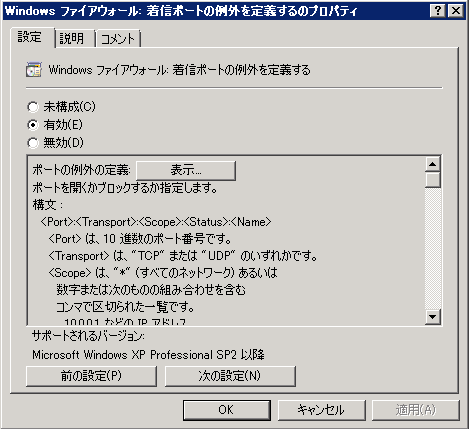
「有効」をクリック後、「OK」をクリックします。



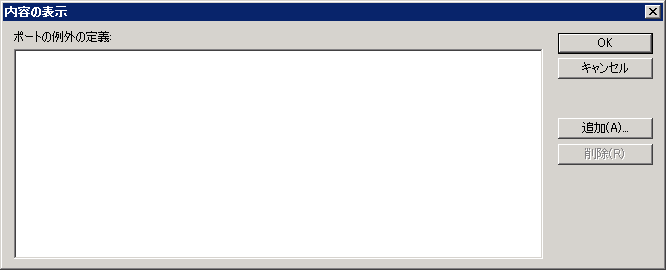
1. 「Windowsファイアウォール：着信ポートの例外を定義する」を設定します。

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。

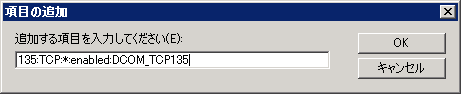
「有効」をクリックし、「ポートの例外定義」の「表示」をクリックします。



「追加」をクリックします。

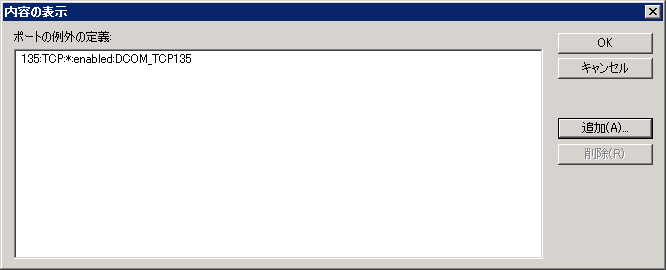


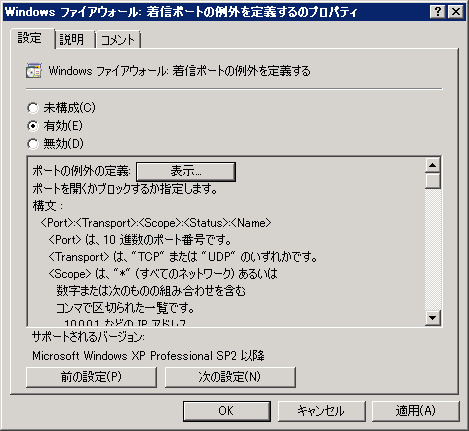
「追加する項目を入力してください」に「135:TCP:\*:enabled:DCOM\_TCP135」を入力し「OK」をクリックします。



※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。



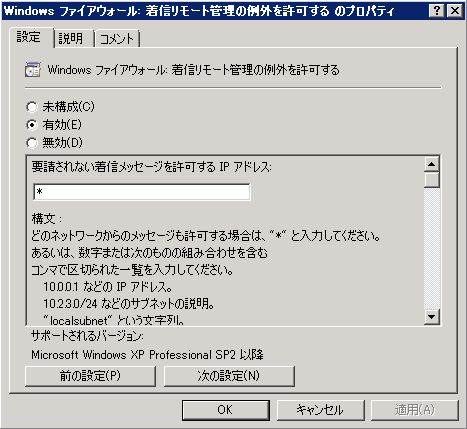


1. 「Windowsファイアウォール：着信リモート管理の例外を許可する」を設定します。

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。

### 9-3-2.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

・OU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OUの管理者権限を持ったユーザーの作成とLogVillageへの登録

#### 9-3-2-1.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

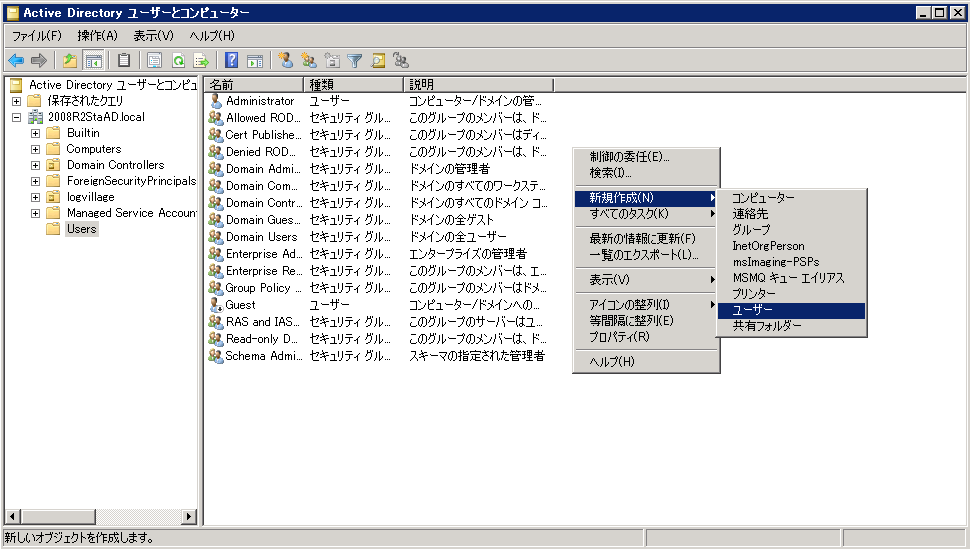
**・ユーザー作成**

1. 「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。

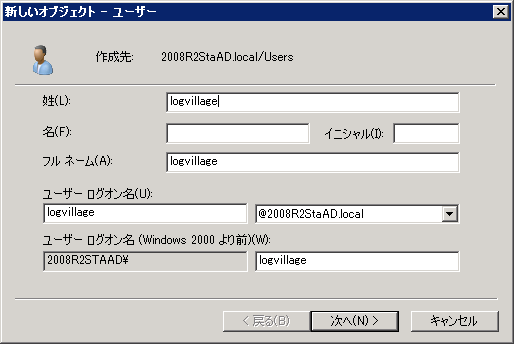
1. 新規「ユーザー」を作成します。

「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。



「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

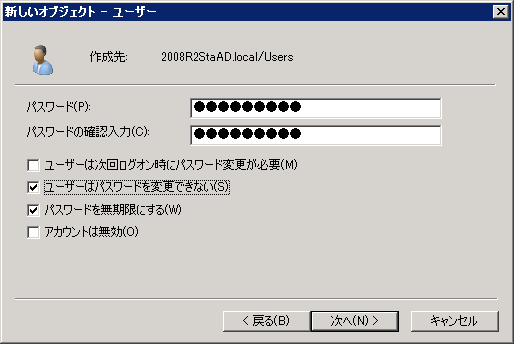


「パスワード」と「パスワードの確認入力」に任意のパスワードを入力します。

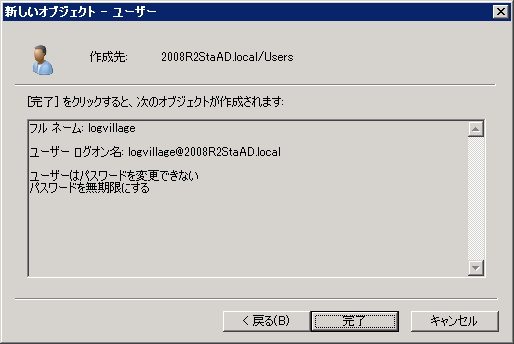
「ユーザーは次回ログオン時にパスワード変更が必要」のチェックを外します。

「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。



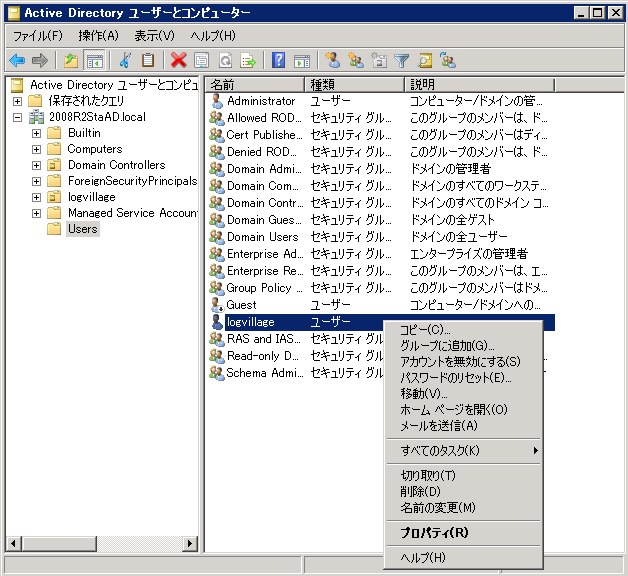
設定に間違いが無い事を確認後「完了」ボタンをクリックします。



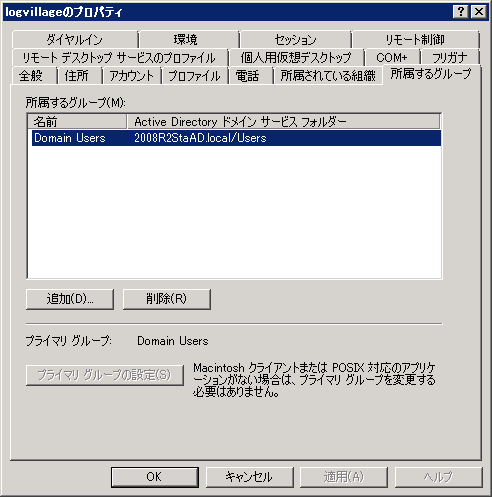
1. 権限を付与します。

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。

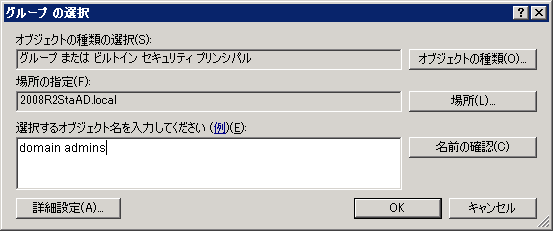
　例：logvillage



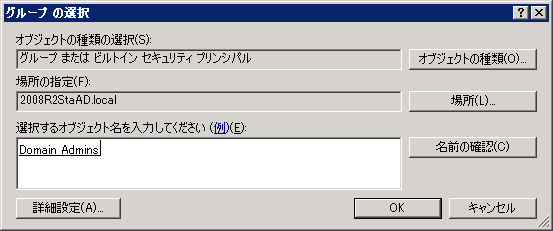
「所属するグループ」タブを開き、「追加」をクリックします。



「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。

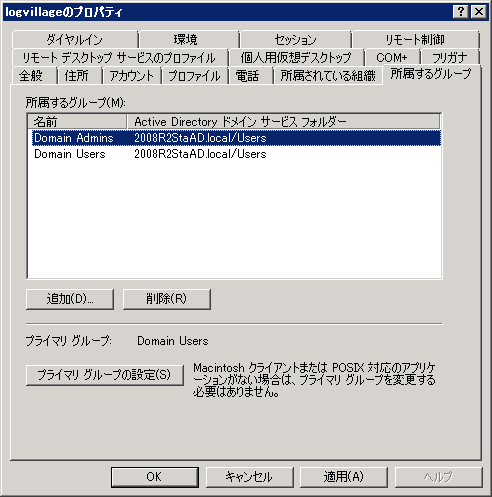


「domain admins」に下線が表示された事を確認後、「OK」をクリックします。

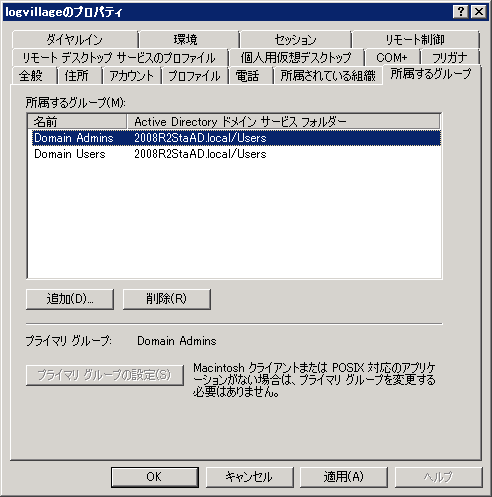


1. プライマリグループを変更します。

「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。



「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。

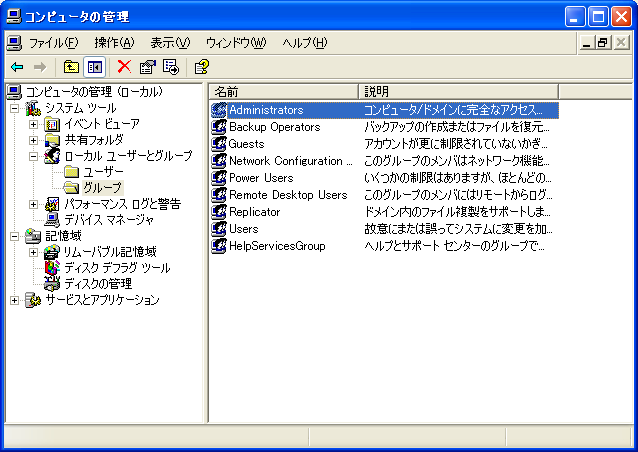


**・管理対象PC上で、設定反映を確認する方法**

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。

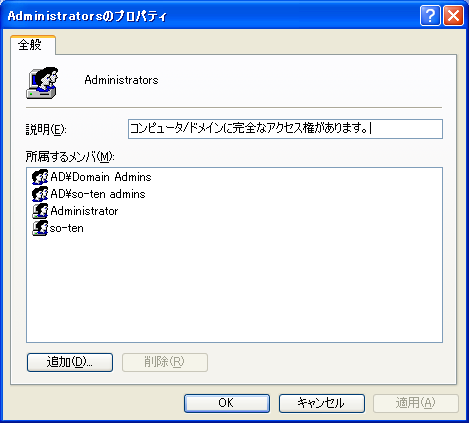
「コンピュータの管理（ローカル）」→「ローカル ユーザーとグループ」→「グループ」をクリックします。



1. 「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。



**・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。

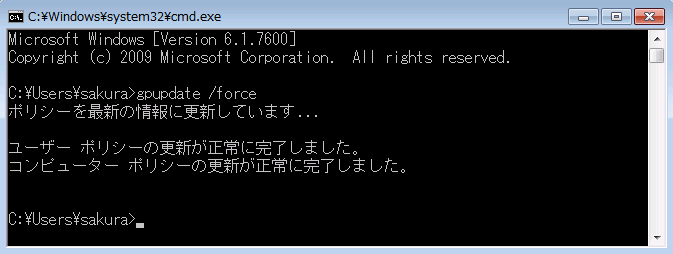
コマンドプロンプトを起動します。

"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。

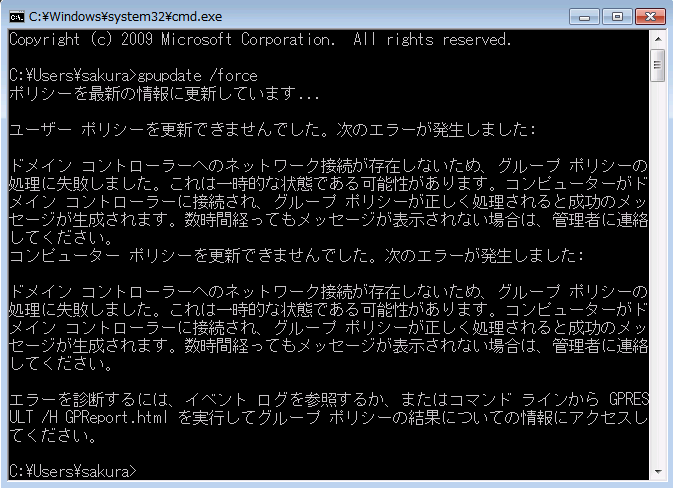
「gpupdate /force」を入力し、実行します。

※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」

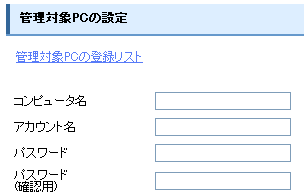
AD.localのユーザー「logvillage」

「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）



①

②

③

③

#### 9-3-2-2.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**

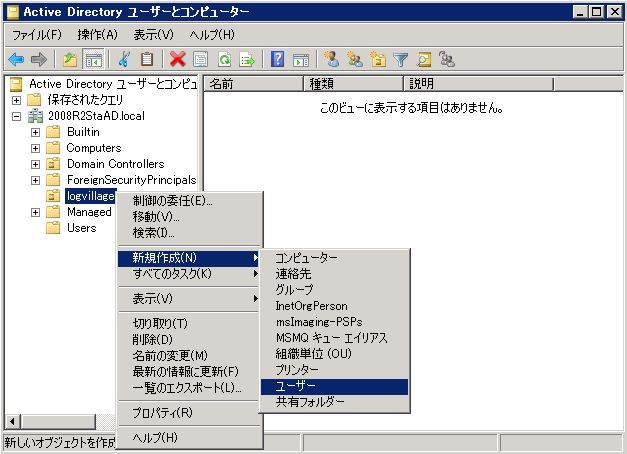
1. 「Active Directory ユーザーとコンピュータ」起動します。

"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。

1. 新規「ユーザー」を作成します。

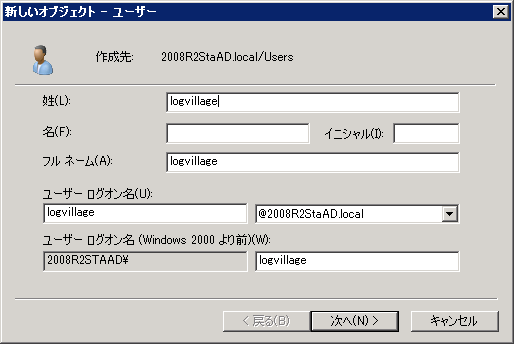
該当OUの上で右クリック「新規作成」→「ユーザー」をクリックします。

　例：OU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

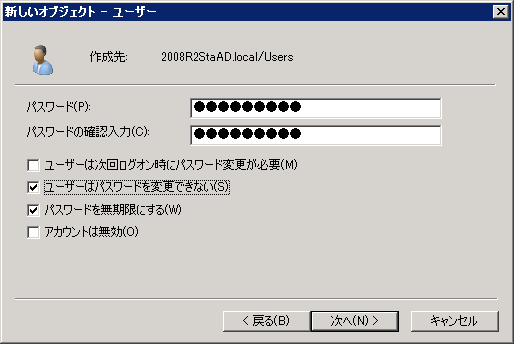


「パスワード」と「パスワードの確認入力」に任意のパスワードを入力します。

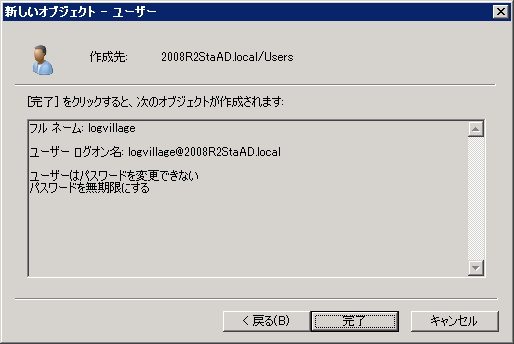
「ユーザーは次回ログオン時にパスワード変更が必要」のチェックを外します。

「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。

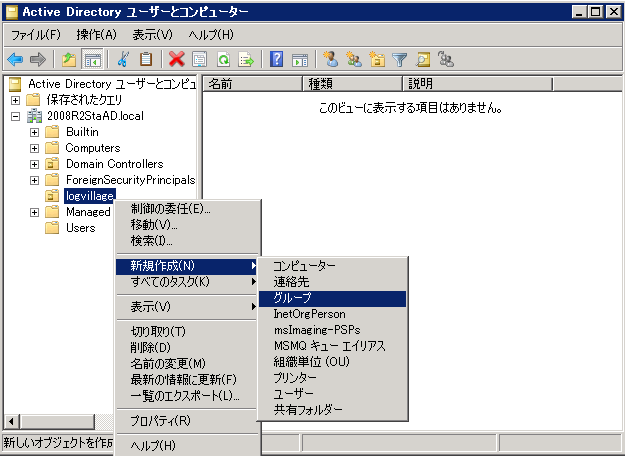


設定に間違いが無い事を確認後「完了」ボタンをクリックします。



1. セキュリティ グループを作成します。

該当OUの上で右クリック「新規作成」→「グループ」をクリックします。



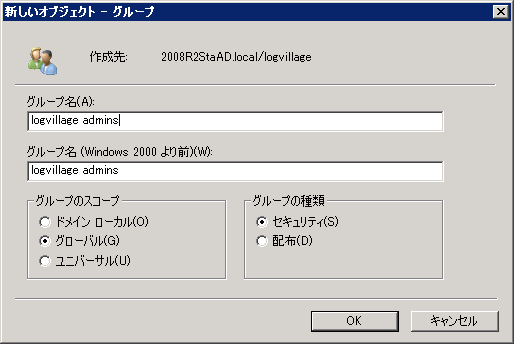
グループ名を入力します。

　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。

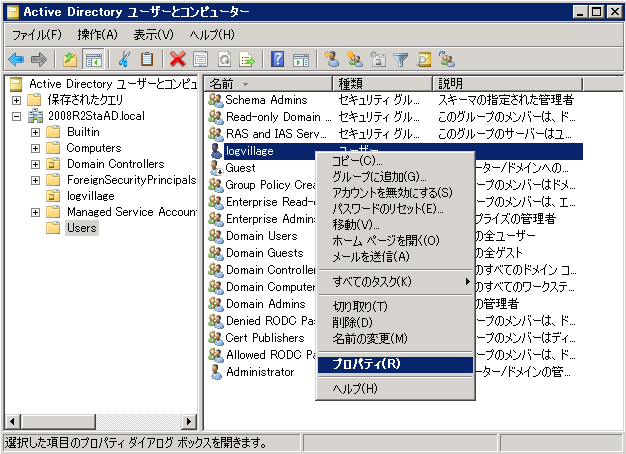
「OK」をクリックします。



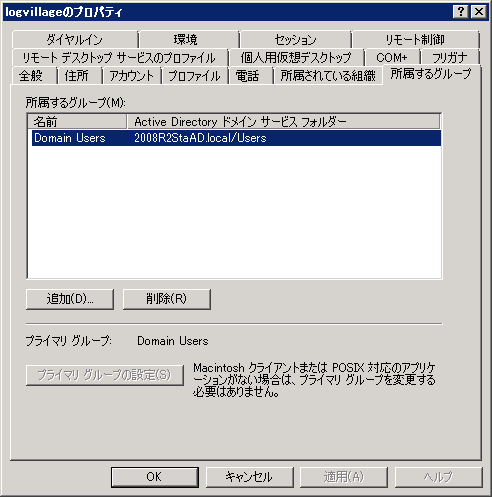
1. 権限を付与します。

「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。

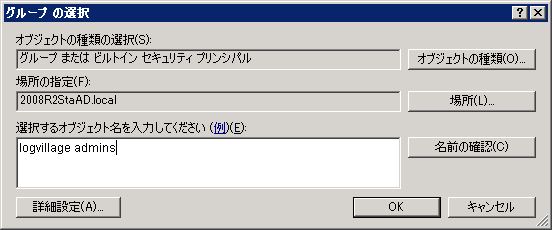
　例：logvillage



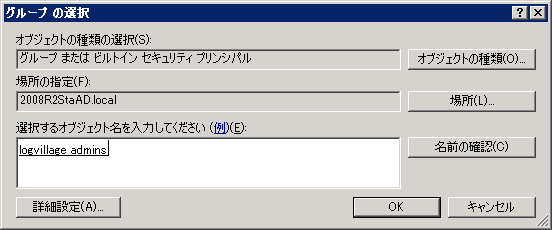
「所属するグループ」タブを開き、「追加」をクリックします。



「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。

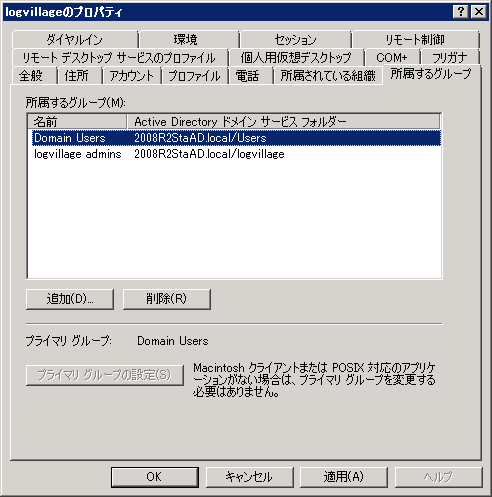


「domain admins」に下線が表示された事を確認後、「OK」をクリックします。



（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。



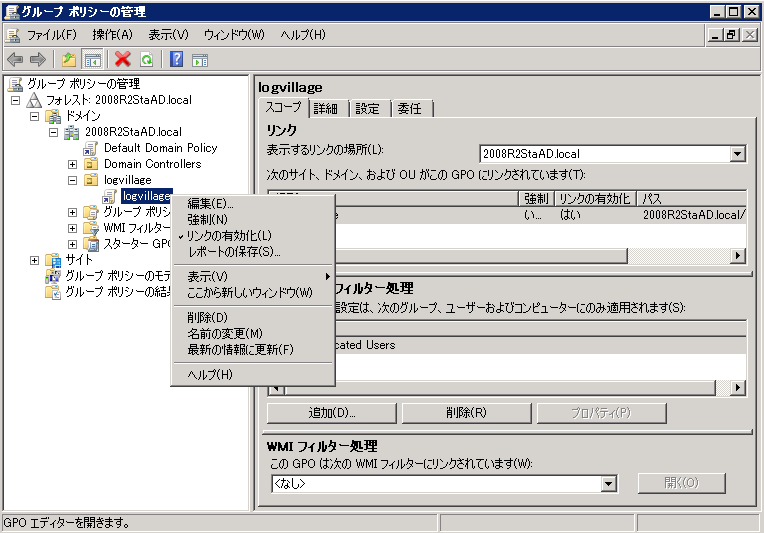
1. グループポリシーを編集します。

"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。

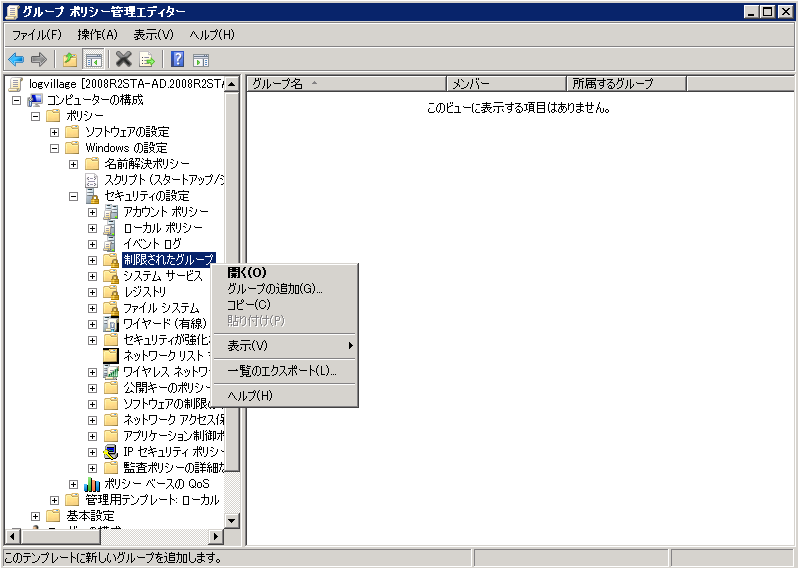
変更するポリシーを右クリックし、「編集」をクリックします。

　例：OU名：logvillage

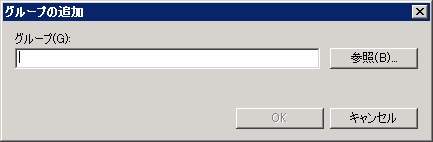


「コンピュータの構成」→「ポリシー」→「Windowsの設定」→「セキュリティの設定」→「制限したグループ」を選択します。

「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。



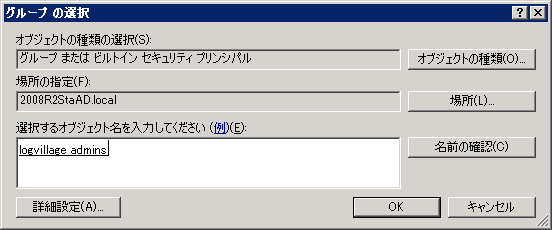
「参照」をクリックします。



作成したセキュリティグループ名を入力します。

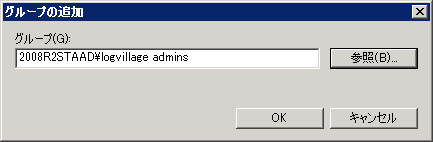
　例：logvillage admins

「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。

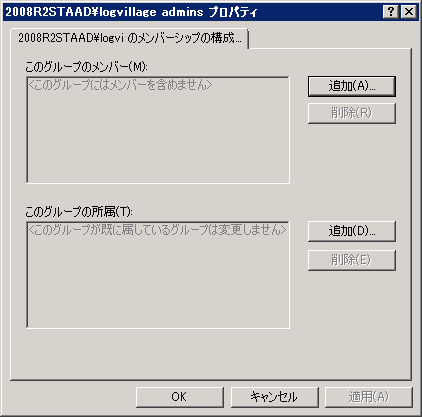


（下線が追加されない場合、セキュリティグループの指定に問題があります。入力文字列の確認、およびセキュリティグループが正しく作成されているかを確認してください）

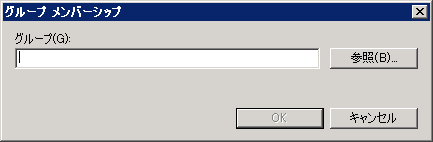
グループに「＜AD名＞\＜作成したセキュリティグループ＞」が表示されることを確認し、「OK」をクリックします。



「追加」をクリックします。

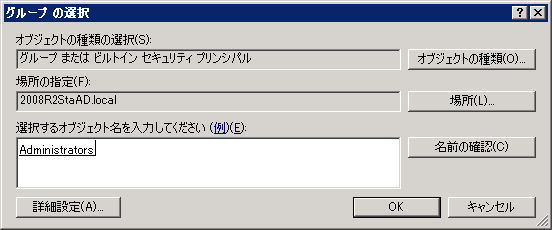


「参照」をクリックします。



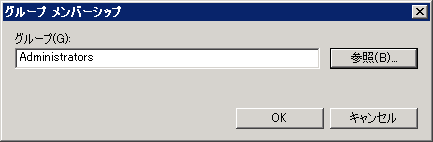
「Administrators」と入力します。

「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。

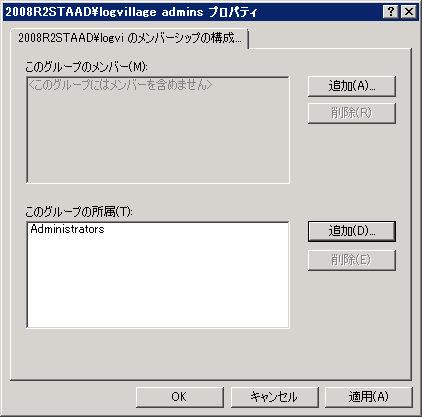


（下線が追加されない場合、セキュリティグループの指定に問題があります。入力文字列を確認してください）

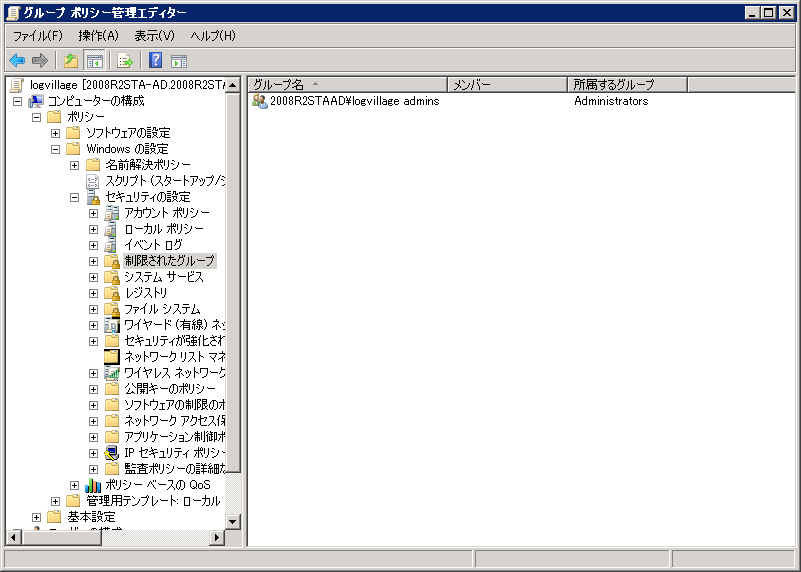
グループに「Administrators」が表示されることを確認し、「OK」クリックします。



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。



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

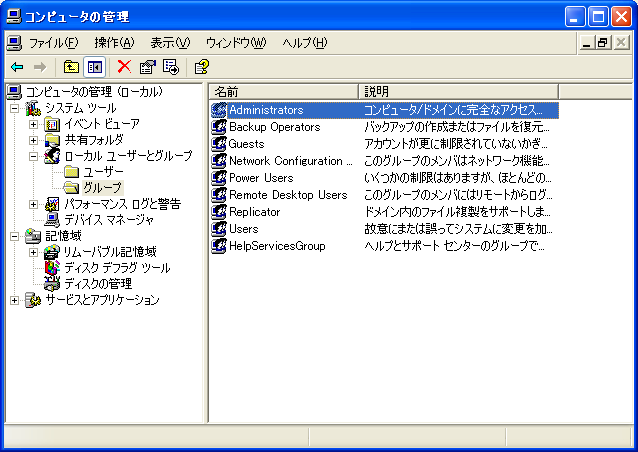


**・管理対象PC上で、設定反映を確認する方法**

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。

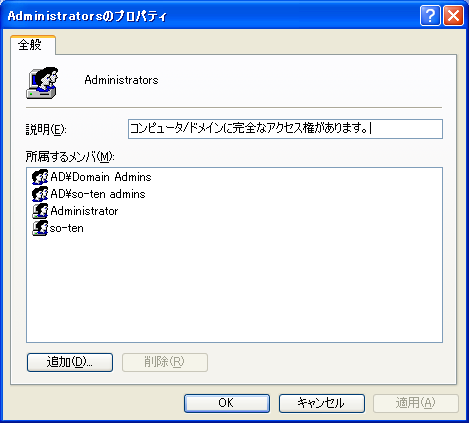
「コンピュータの管理（ローカル）」→「ローカル ユーザーとグループ」→「グループ」をクリックします。



1. 「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。



**・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。

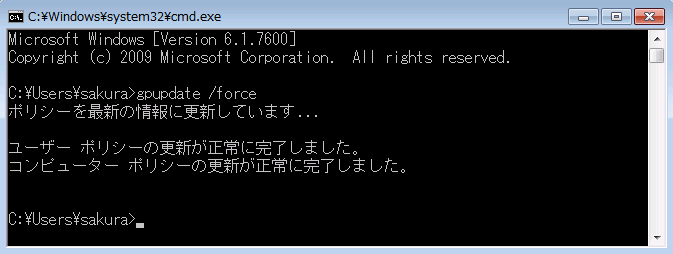
コマンドプロンプトを起動します。

"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。

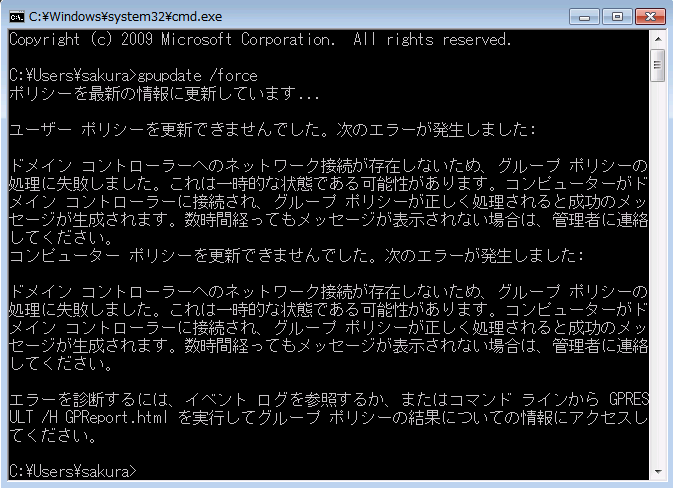
「gpupdate /force」を入力し、実行します。

※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」

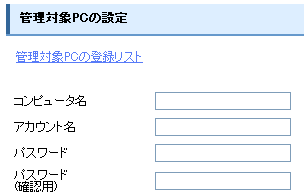
AD.localのユーザー「logvillage」

「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）



①

②

③

③

# 10.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。

## 10-1.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。

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/

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

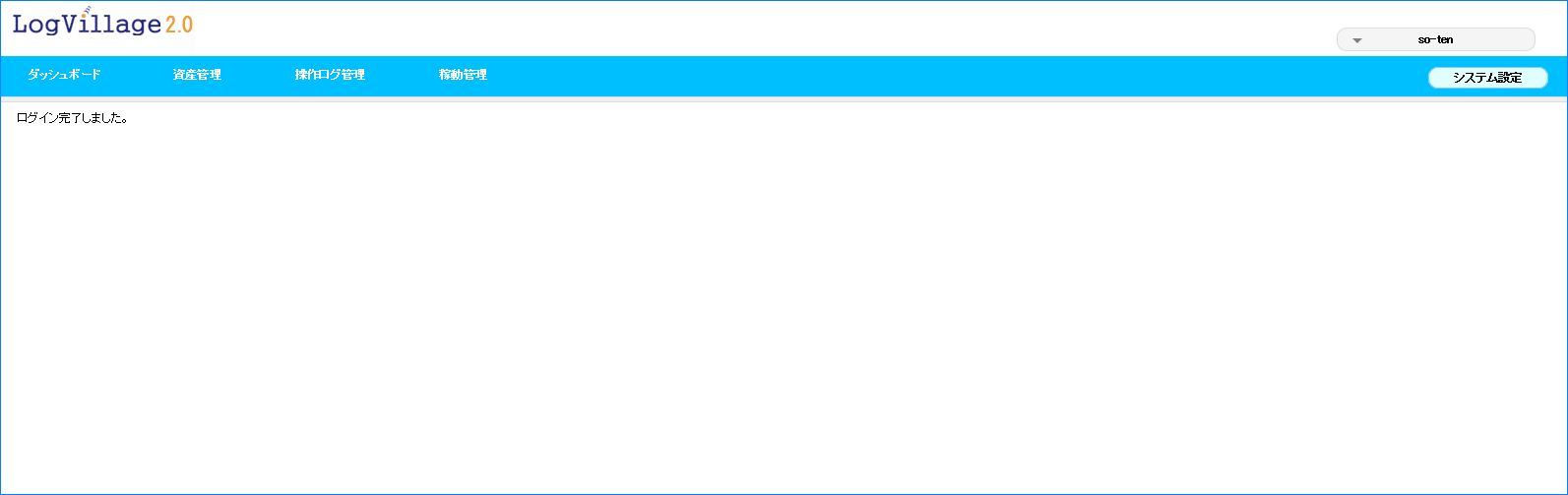
**※ご利用ブラウザについて**

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

## 10-2.画面概要

LogVillageMGRへログインを行うと下の画面が表示されます。

②



③

①

1. 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。

1. 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。

1. 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。

## 10-3.システム設定画面



②

①

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。

1. 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。

# 11.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。

## 11-1.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。

### 11-1-1.対応OS

Windows 7,8,10

### 11-1-2.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。

### 11-1-3.設定手順

■LogVillageMGRでの設定準備手順

1. 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

1. 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。

1. 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。

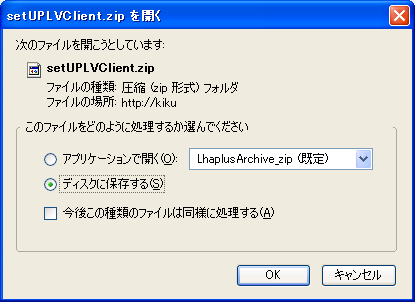
http://<マネージャのURL>/pcsetupDL/

1. 「ダウンロード」ボタンをクリックします。



1. 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。



1. 保存したファイルを展開します。

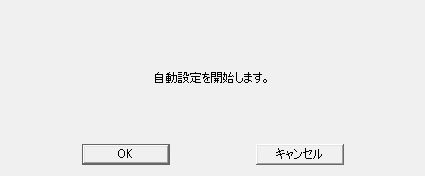
保存したファイル「setUPLVClient.zip」を展開します。

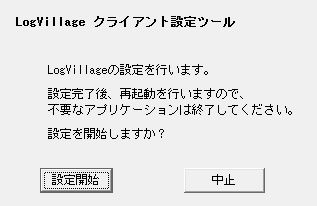
1. ファイルを実行します。

「LVAutoSet\_WindowsVista-10.exe」をダブルクリック（実行）します。

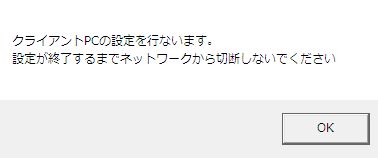
1. 「設定開始」をクリックします。

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。

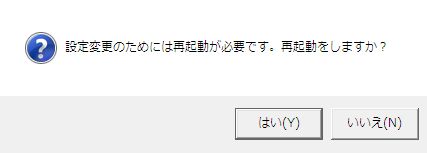




1. 「OK」をクリックします。

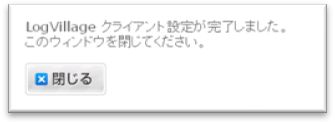


1. OSを再起動します。



1. 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。

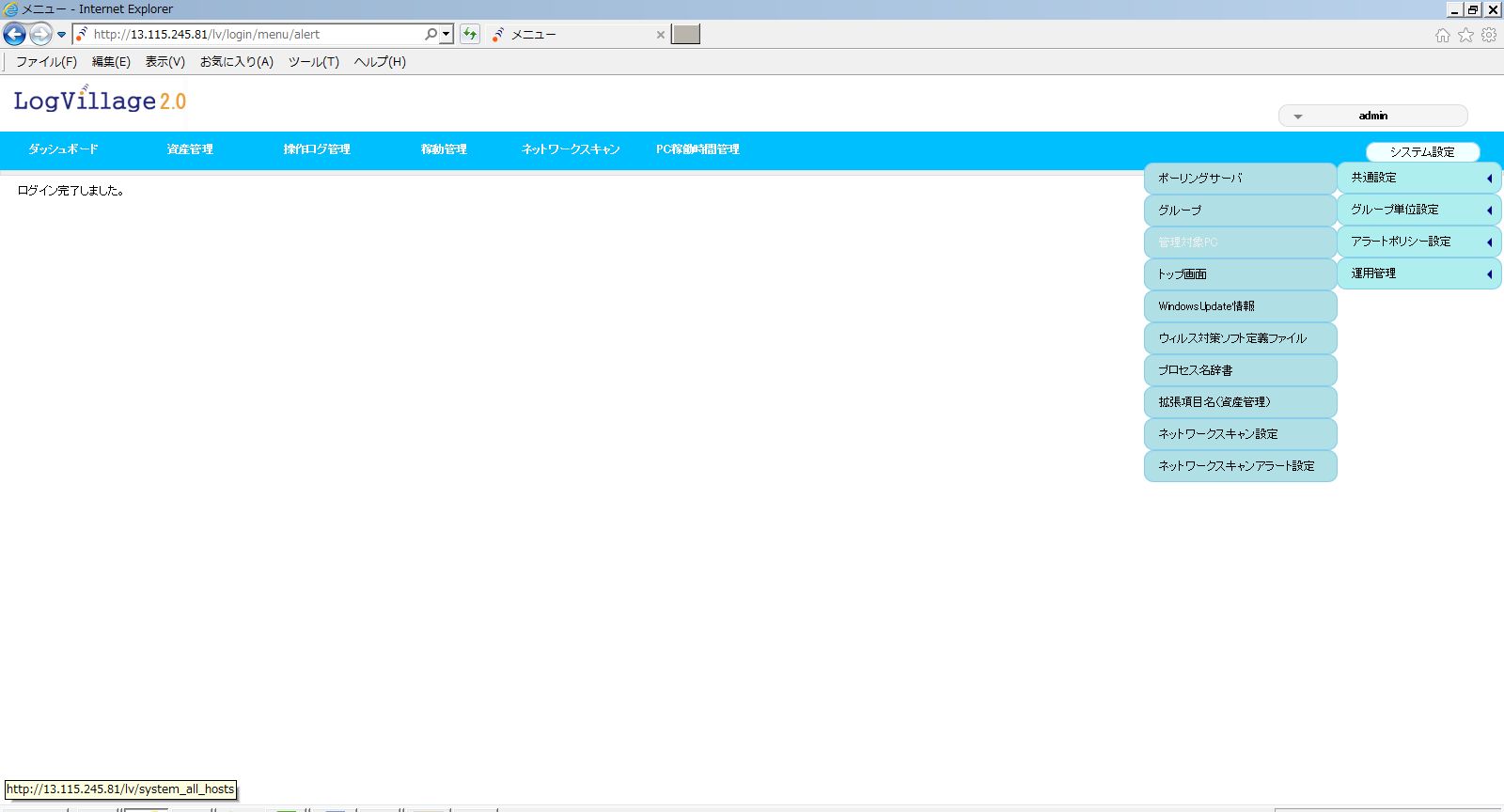


## 11-2.管理対象PCをLogVillageマネージャに登録する

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。



1. 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。



# 12.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。

## 12-1. 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。

### 12-1-1.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

### 12-1-2.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。

## 12-2.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。

### 12-2-1.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\SO-TEN\LogVillage となります。）

ファイル名の例：　LV-PS-LOG201001230182024.txt

### 12-2-2.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。

## 12-3. 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。

### 12-3-1.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OS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\SO-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。

### 12-3-2.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)

### 12-3-3.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。

## 12-4. LogVillage PCエージェントの動作関連ログファイル

LogVillage PCエージェントの動作関連ログファイルについて説明します。

### 12-4-1.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 PCエージェントのインストール先＞\log

※＜LogVillage PCエージェントのインストール先＞は、インストール先ディレクトリパスに読み替えます。

### 12-4-2.ログ保存期間

LogVillage PCエージェント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。

但し、ホスト（PC）が復元モードの場合は起動ごとに前回起動のログが削除されます。

# 13.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\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 2048

　　> openssl.exe req -new -key ../conf/server.key -out ../conf/server.csr -config ../conf/openssl.cnf

*※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

　　　※上記コマンドで発行される自己証明書の有効期間は「1年（365日）」となります。

　　　　有効期間を延長する場合はコマンド末尾の「-days 365」を「-days 1825」等に変更

を行ってください。

　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\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\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/SO-TEN/LogVillage/Apache2/logs/ssl\_scache(512000)

↓　*※”#”を追加*

#SSLSessionCache shmcb:C:/Program

Files/SO-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\\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\\\SO-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\\\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。

# 14.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。

〒540-0035 大阪市中央区釣鐘町1丁目3-4 ダイクウビル2F

株式会社ワッセイ・ソフトウェア・テクノロジー

e-mail ：

TEL ：06-6944-8901

FAX ：06-6944-8885

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

改訂履歴

|  |  |  |
| --- | --- | --- |
| Revision | 発行日 | 改訂履歴 |
| MD-20-20081113 | 2008年11月13日 | 7-4.ActiveDirectory環境での管理対象PC設定内容  7-4-1グループポリシー設定変更項目  ７）.プリンターログ設定  を変更。 |
| MD-20-20081113 | 2008年11月13日 | 1.LogVillageの基本構成  1-1.稼働環境　■ポーリングサーバーにsp1の記述を追加しました。  ※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。 |
| MD-20-20081017 | 2008年10月17日 | 7-3.WorkGroup環境での管理対象PC設定内容  各OSについての記述を追加。 |
|  |  | 1）.Active　Directory上でのユーザー作成とLogVillageへの登録（項目タイトルの変更） |
| MD-20-20081002 | 2008年10月2日 | 7-4-2. 1） アカウント名の例をlv20\logvillage からAD.local\logvillageに変更 |
| MD-20-20090306 | 2009年3月6日 | 7-4-2.1）画面付きの情報に変更 |
| MD-20-20090420 | 2009年4月20日 | 補足資料4,8,9　PSプロセス化に伴い終了方法を修正。 |
| MD-20-20091125 | 2009年11月25日 | 1-1.OSの定期的な再起動を追加  4.インストール画面キャプチャ変更  5.インストール画面キャプチャ変更  7-1.グループポリシー削除  7-4-1.リモート管理の例外を許可する。を変更  7-4-2.OU用ユーザー作成方法追加  補足資料にMgrとPSの再起動方法を追加 |
| MD-20-20100129 | 2010年1月29日 | 10.LogVillage運用のための情報を追加 |
| MD-20-20100301 | 2010年3月1日 | 7.管理対象PCの設定変更にWindows7を追加 |
| MD-20-20100408 | 2010年4月8日 | 7.管理対象PCの設定変更を追加・修正  4）ファイアウォールを変更 |
| MD-20-20101122 | 2010年11月22日 | Windows7, Windows Server 2008 対応のため、以下を修正。  1-1.稼働環境  7.管理対象PCの設定変更  9.管理対象PCの設定ツール（オプション） |
|  |  | Mac版PSを導入する場合spoolをCにするよう記載  4-1.LogVillageMGRのインストール |
| MD-20-20101227 | 2010年12月27日 | upgrade.exeファイル名間違いを修正  4-3.LogVillageデータベースのライセンス登録  7-3.WorkGroup環境での管理対象PC設定内容  2）プリンターログ　に、Windows7を追加  ※Win7,2008R2の印刷履歴対象外の記述を削除。  Win7の印刷履歴未対応の部分を削除 |
| MD-20-20110311 | 2011年03月11日 | グループ文書に変更  　全体的な体裁や文言の統一など、全面修正  4-3.LogVillageデータベースのライセンス登録  　DB5.1ライセンス登録方法を追加  7.管理対象PCの設定変更  7-3.WorkGroup環境での管理対象PC設定内容  　分散COMの確認方法を追加  7-4.ActiveDirectory環境での管理対象PC設定内容  　Windows7用ADの印刷設定を追加  　DCOM設定方法を追加  ＜＜　　　補足資料　　　＞＞  Mgr再起動方法にタスクトレイを先に終了するよう変更 |
| MD-23-20120220 | 2012年2月20日 | DBがMySQLに変更となったことに伴う変更  管理画面デザイン変更に伴う変更 |
| 会社所在地、連絡先を変更  7-4.ActiveDirectory環境での管理対象PC設定内容  　Windows7用ADの印刷設定を変更  9-1.LogVillage 管理対象PC設定ツール（ダウンロード版）にWindows7を追記 |
| MD-23-20120220 | 2012年3月27日 | 7-4-1-2. 2)プリンターログ設定  ②設定変更用ファイルを配置します。（Windows7以降）を削除 |
| MD-23-20120417 | 2012年4月17日 | 7-4-1-1. 2)プリンターログ設定  Windows7以降の設定を全て削除 |
| MD-23-20120417 | 2012年4月17日 | 7-4-1-1. 5）DCOM リモート起動のアクセス許可  ⑤がサンプル画像違いのため削除 |
| MD-23-20120417 | 2012年4月17日 | 7-4-1-2. 2)プリンターログ設定  Windows7以降の設定を全て削除 |
| MD-23-20120426 | 2012年4月26日 | P17 誤字修正 |
| MD-23-20120426 | 2012年4月26日 | P27 誤字修正 |
| MD-23-20120426 | 2012年4月26日 | P105 脱字修正 |
| MD-23-20120807 | 2012年8月7日 | 10-3-1　Apacheログの設定方法を追加  5-2、6-1　PSの登録方法を変更  5　PSの設定を追加(MSネットワーク、DCOM、LM認証)  3-2　接続確認ツールを追加 |
| MD-23-20120918 | 2012年9月18日 | 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  を追加 |
| MD-23-20150907 | 2015年9月7日 | 5.LogVillagePSのインストール  5-1-2.LogVillagePSのインストール環境 (4)を  追加 |
|  |  | 5.LogVillagePSのインストール  　5-2.LogVillagePSのインストール手順　①  を修正 |
| MD-23-20161220 |  | 新UIイメージに変更 |
| MD-23-20170629 | 2017年6月29日 | Windows2K、XP、Vista、2003を削除 |
| MD-23-20171123 | 2017年11月23日 | 5.LogVillagePSのインストール  5-2.LogVillagePSのインストール手順  ③「timeKeeper」機能のインストール有無を選択を追加。 |
| MD-23-20171215 | 2017年12月15日 | 11.SSL（暗号化）通信設定を追加 |
|  |  | ＜補足資料＞LogVillageの再起動手順を変更 |
| MD-25-20190228 | 2019年2月28日 | 「1-3.構成イメージ図を」修正 |
|  |  | 「5.LogVillagePSのインストール」  タイムキーパー選択の項目を削除 |
|  |  | 「6.PCエージェントのインストール」を追記 |
|  |  | 「7.Phantosysログ取得エージェントのインストール」を追記 |
|  |  | 複数のページ崩れを修正 |
|  |  | 「8-3-1.ログ収集スケジュール」にPC利用ログを追記 同、“ファイル“を削除 |
| MD-25-20190410 | 2019年4月10日 | 「7-1.Phantosysログ・サーバエージェントのインストール」に  “⑤ PCリストを作成”を追記 |
| MD-25-20200302 | 2020年3月2日 | 「13.SSL（暗号化）通信設定」  自己証明書の有効期間についての注釈を追記 |
| MD-25-20200330 | 2020年3月30日 | 7-1.Phantosysログ・サーバエージェントのインストール  「②設定ファイル（config.ini）を編集」に追記 |
| MD-25-20200903 | 2020年9月3日 | 7-1.Phantosysログ・サーバエージェントのインストール  「②設定ファイル（config.ini）を編集」に追記 |
| MD-25-20210112 | 2021年1月12日 | 「1-1.稼働環境」更新 |
| 「12-4. LogVillage PCエージェントの動作関連ログファイル」を追記 |
| MD-25-20220817 | 2022年8月17日 | 「1-1.稼働環境」対応OSを更新 |
| MD-25-20220830 | 2022年8月30日 | 「6-4.インストール確認」修正 |