LogVillage2.0

# 導入マニュアル

V2.3J

株式会社 蒼 天

# logVillage2.0　導入マニュアル

revision　:　MD-23-20170629

---



---

**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

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。
※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
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。

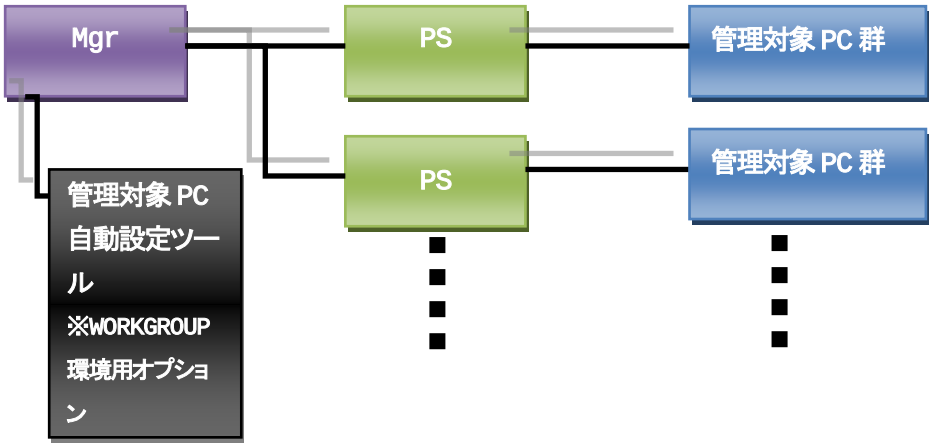
## 1-2. LogVillage の構成要素

LogVillage は以下により構成されます。

| | |
|---|---|
| LogVillage マネージャ<br>：LogVillageMGR | ・Web アプリケーション<br>ーLogVillage 全体のシステム設定画面<br>ーログ情報の検索・参照画面<br>ー稼働状況のモニタリング画面<br>・データベース<br>ーログ情報の蓄積<br>ーシステム設定情報の保存 |
| LogVillage ポーリングサーバー<br>：LogVillagePS | ・ログ情報の収集（ポーリング）<br>・アラート通知（メール、ポップアップ）<br>・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<br>・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）<br>・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。

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**

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。

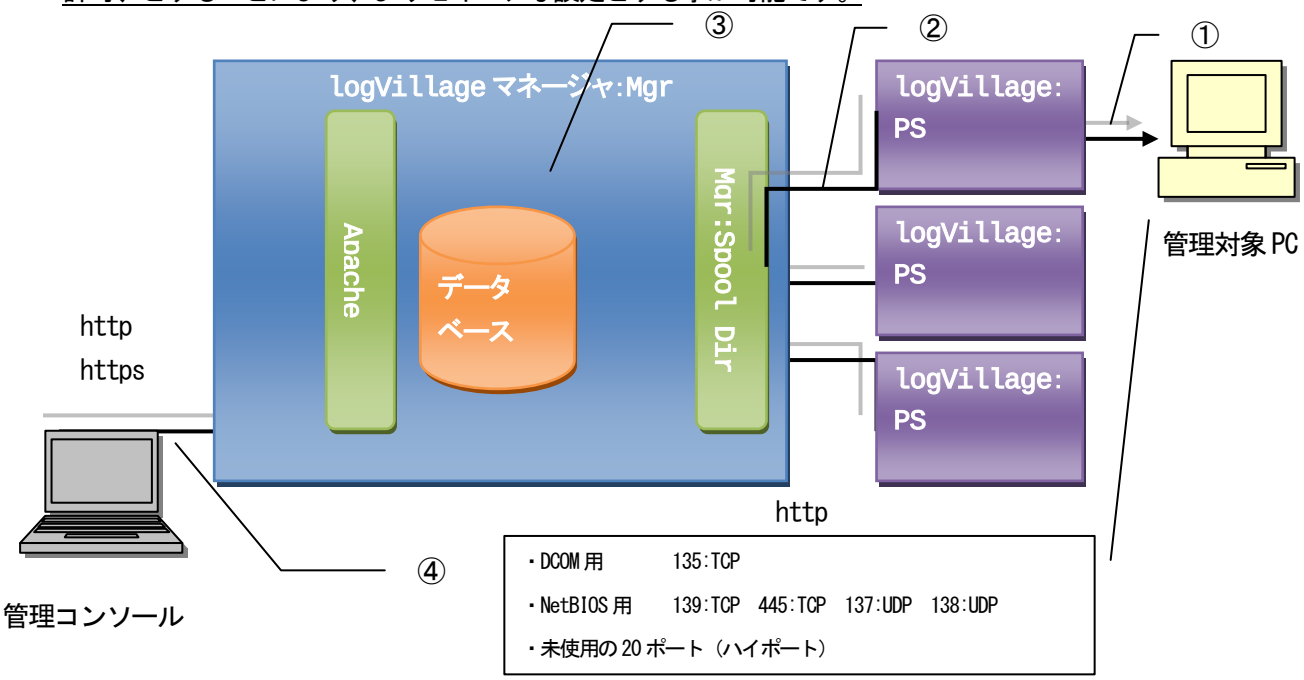
・NetBIOS 用　　139:TCP, 445:TCP, 137:UDP, 138:UDP

・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
- ・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

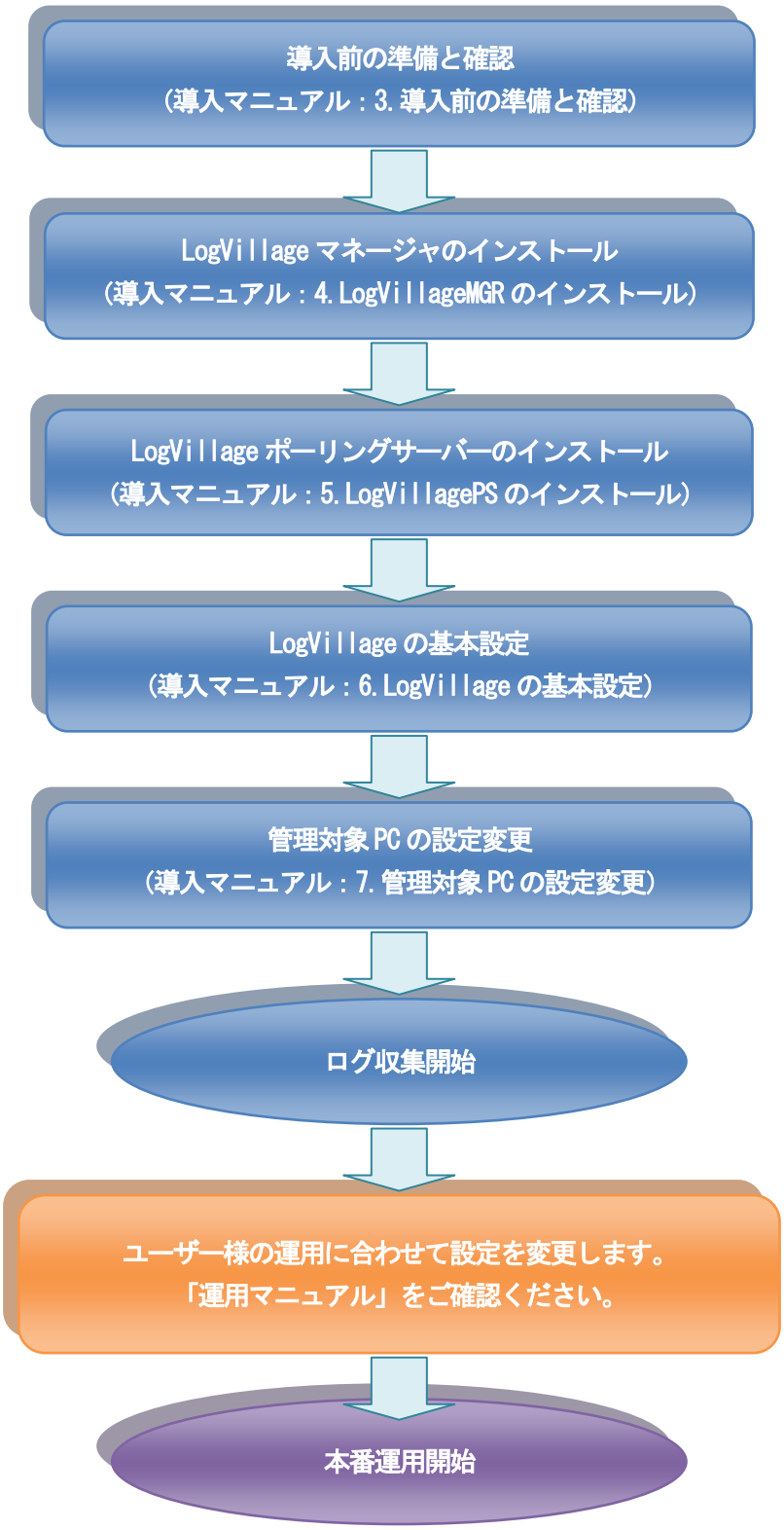
**■ポーリングサーバー：LogVillagePS**

※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）
ログ収集開始
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。
本番運用開始

## 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

○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。 |

〇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。<br>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。

〇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。<br>ログオン失敗: ユーザー名を認識できないか、<br>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のをご確認ください。

・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,
```

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

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。

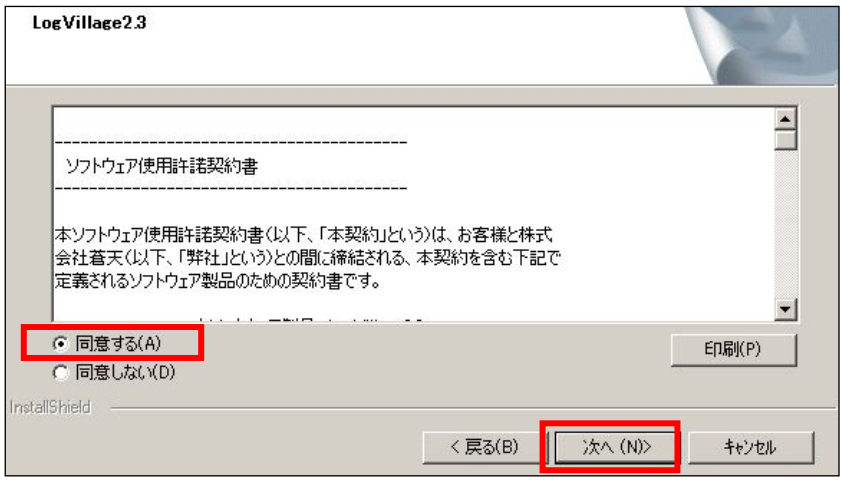
Setup.exe をダブルクリックします。


② 内容を確認し「次へ」をクリックします。

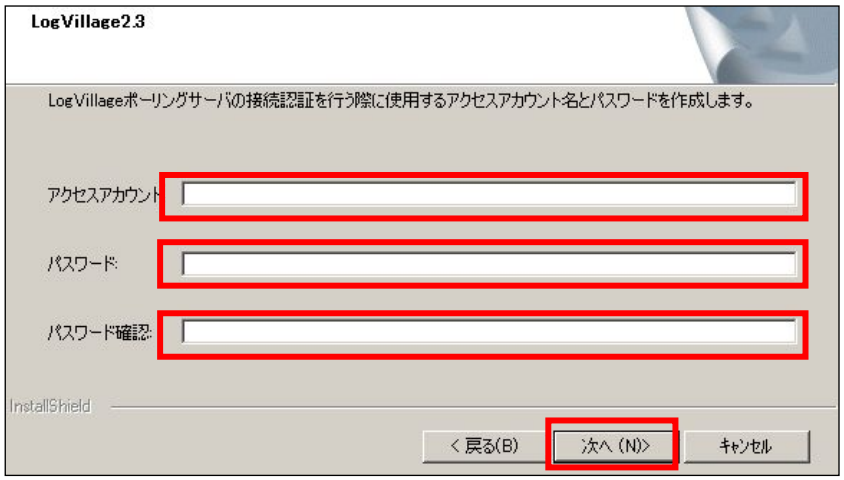
「次へ」をクリックします。


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。

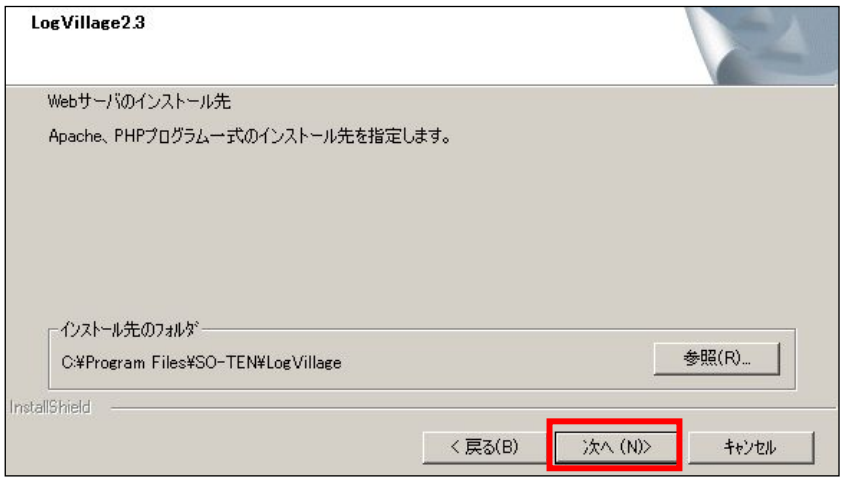


③ 必要情報を入力します。
任意のアクセスアカウント、パスワードを入力し、「次へ」をクリックします。

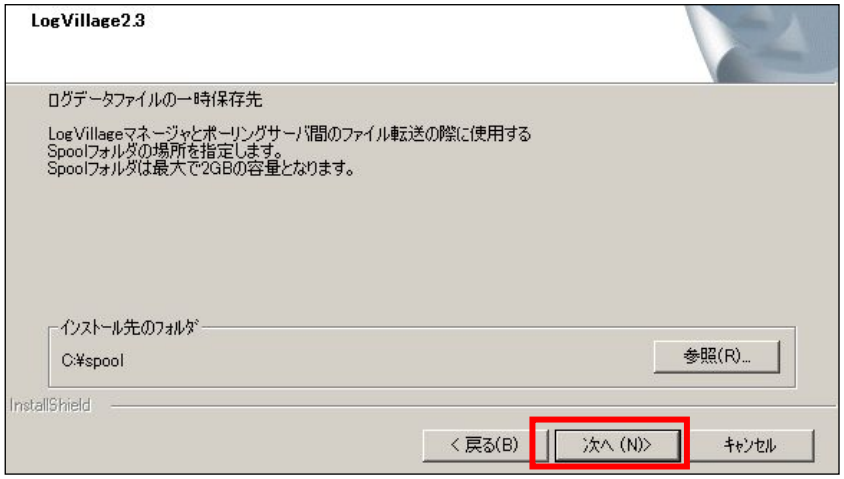



**アクセスアカウント、パスワードは「5-2. LogVillagePS のセットアップ」時で必要になりますので、大切に保管下さい。**
**忘れると、LogVillagePS のセットアップが行えませんのでご注意下さい。**

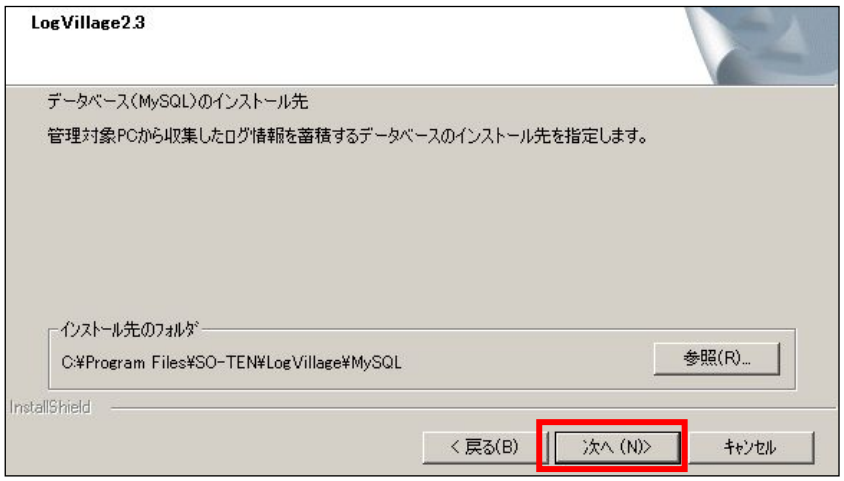
④ Web サーバ(Apache)、Web アプリケーション(PHP)プログラム一式のインストール先を指定します。
LogVillageMGR プログラムのインストール先フォルダを変更しない場合は「次へ」をクリックします。
インストール先を変更する場合は、参照からインストール先フォルダを指定後、「次へ」をクリックします。



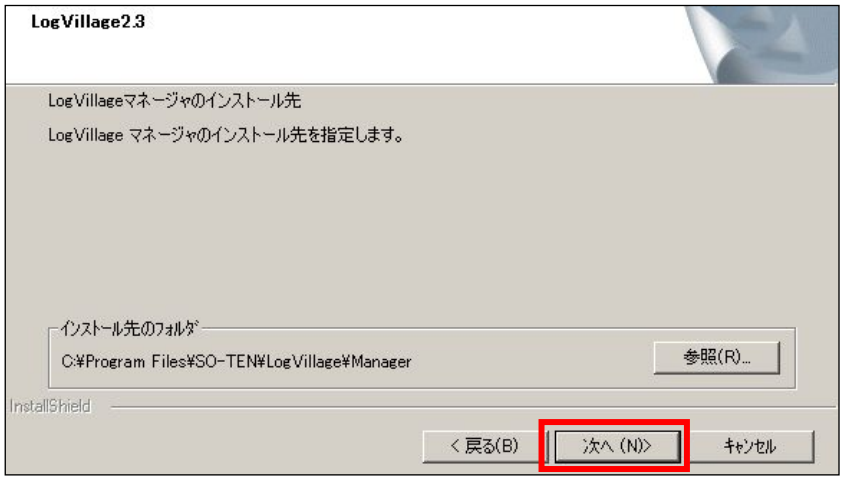
LogVillage マネージャとポーリングサーバ間のファイル転送の際に使用する spool フォルダの場所を指定します。この spool フォルダは最大で 2GB の容量となるます。
spool のインストール先フォルダを変更しない場合は「次へ」をクリックします。
インストール先を変更する場合は、参照からインストール先フォルダを指定後、「次へ」をクリックします。
※管理対象 PC に MacOSX が含まれる場合、デフォルト「C:¥spool」のまま変更しないでください。



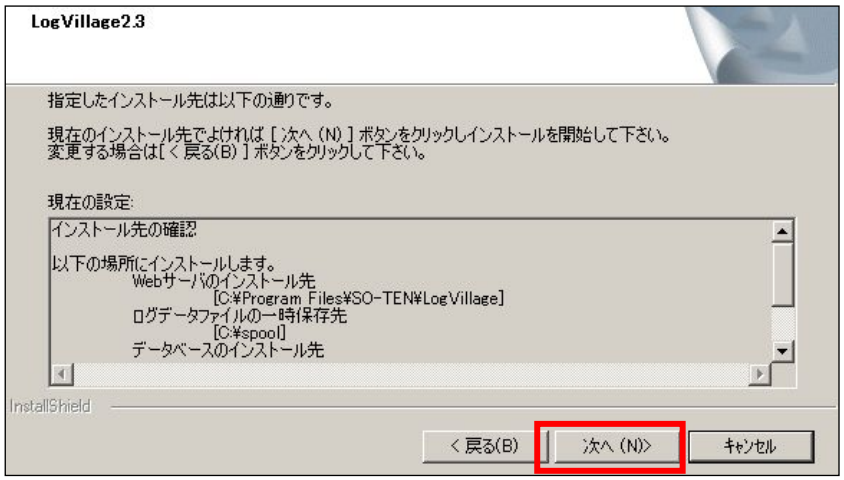

データベース（MySQL）のインストール先を指定します。
変更しない場合は「次へ」をクリックします。
インストール先を変更する場合は、参照からインストール先フォルダを指定後、「次へ」をクリックします。



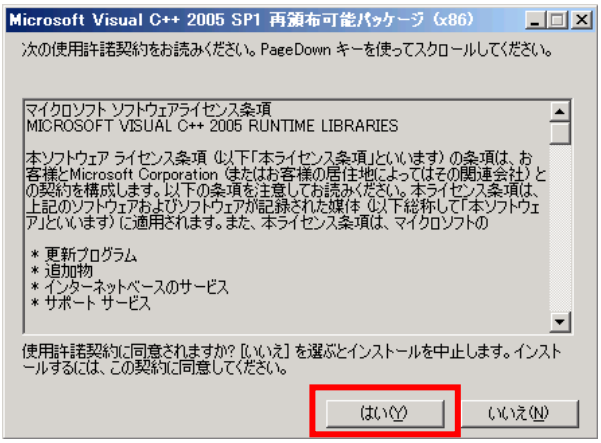
LogVillage マネージャのインストール先を指定します。
変更しない場合は「次へ」をクリックします。
インストール先を変更する場合は、参照からインストール先フォルダを指定後、「次へ」をクリックします。




設定内容を確認し、問題なければ「次へ」をクリックします。

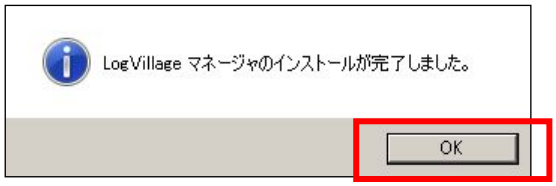



LogVillage マネージャでは、マイクロソフト社製の“microsoft Visual C++ 2005 再配布可能パッケージ”を 利用しています。
そのため、以下のマイクロソフト ソフトウェアライセンス条項に同意いただく必要があります。
Microsoft Visual C++ 2005 使用許諾書を確認し「はい」をクリックします。




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。
「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。

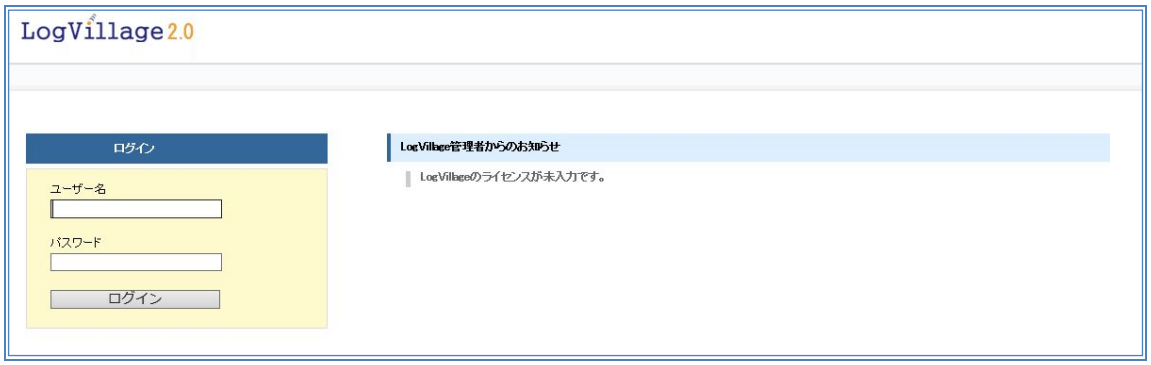
① LogVillgae 管理画面にログインします。

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**

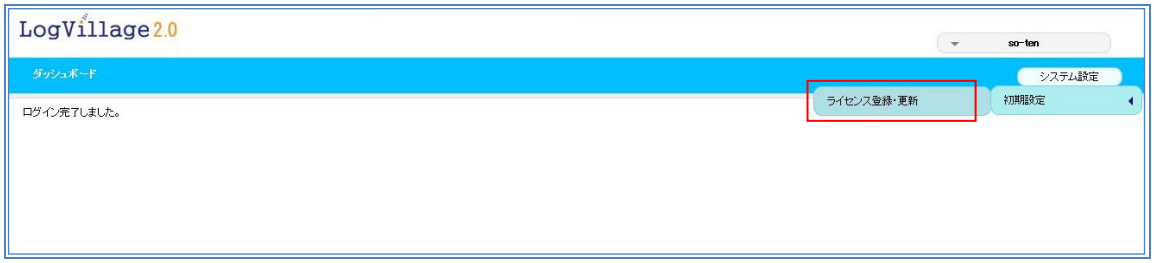
**・パスワード　　so-ten**

※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**

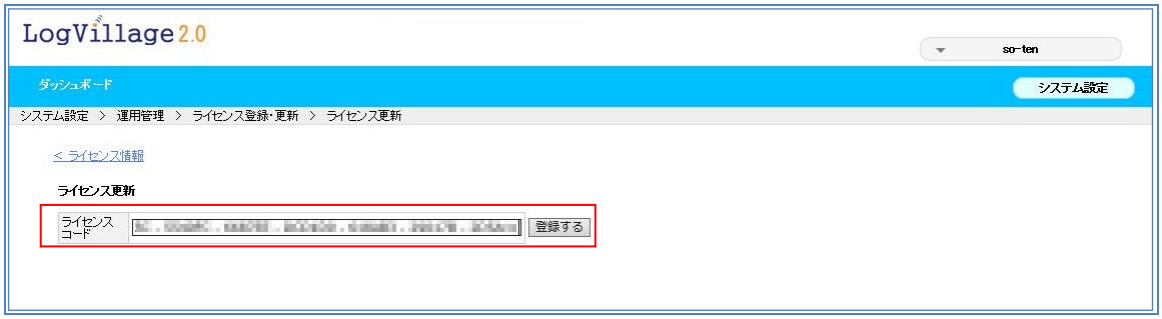
**LogVillageMGR の対応ブラウザは InternetExplorer9 以降となります。**

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。




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。


「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。



④ 登録完了を確認します。

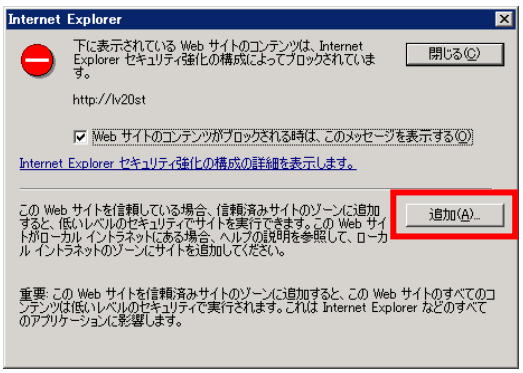
ご購入いただいたライセンス情報が正しく表示されていることをご確認下さい。


【ご注意ください】

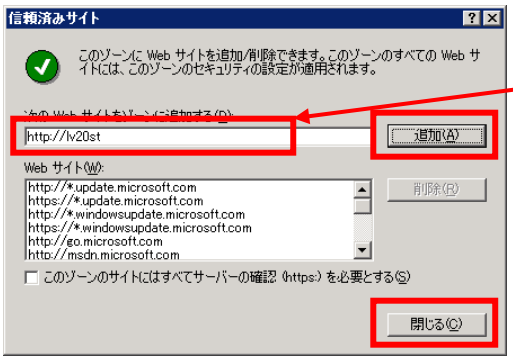
Internet Explorer にて上記操作時に以下の画面が表示される時は、

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。

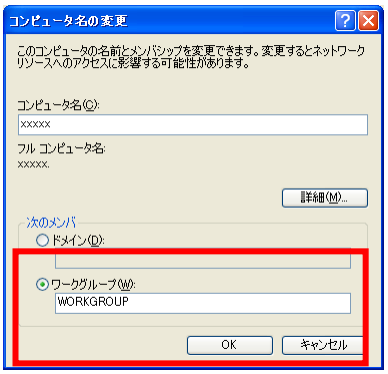
「ActiveDirectory」に参加している状態で LogVillagePS のインストールを行うと、正常動作が行えません。

| サーバに PS をインストールする時の環境 | 動作 |
|---|---|
| WorkGroup | ○ |
| 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。



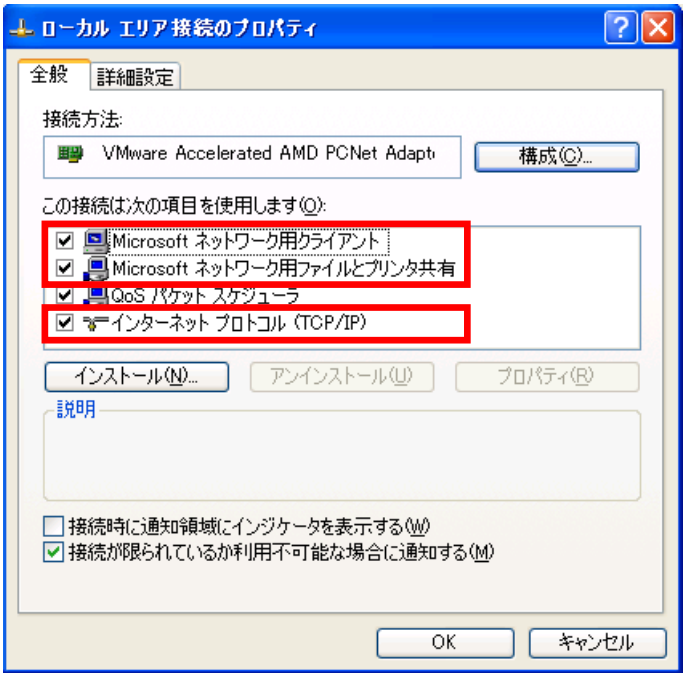

「次のメンバ」が「ドメイン」の場合は「ActiveDirectory」に参加しています。

「ワークグループ」の状態でインストールを実施します。

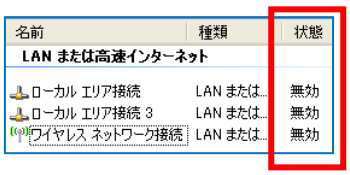
### 5-1-2. LogVillagePS のインストール環境

(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

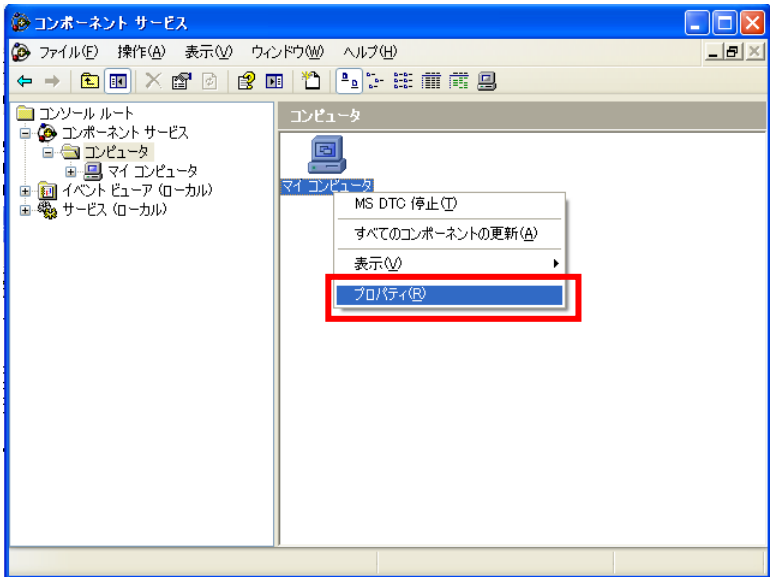
**(2)分散 COM 設定が有効となっている事**

① 「コンポーネントサービス」を起動します。

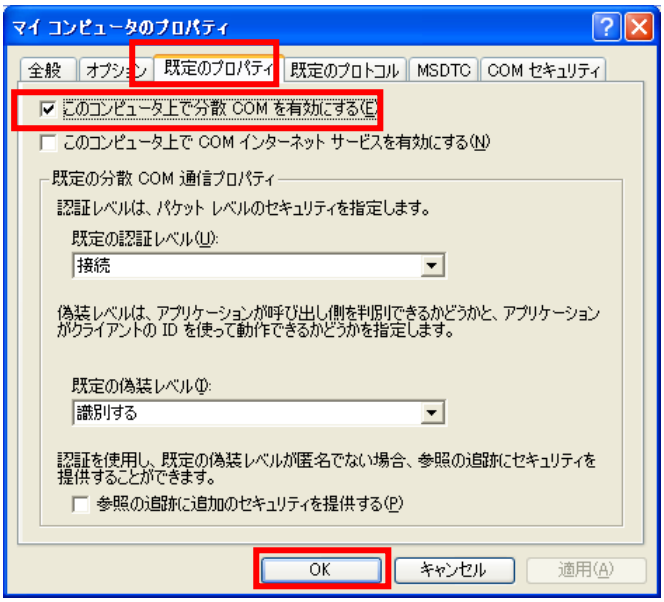
"Windows スタートメニュー"→「コントロールパネル」→「管理ツール」→「コンポーネント サービス」を起動します。

※「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。

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。




③ 「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。




## ⑶ 「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。

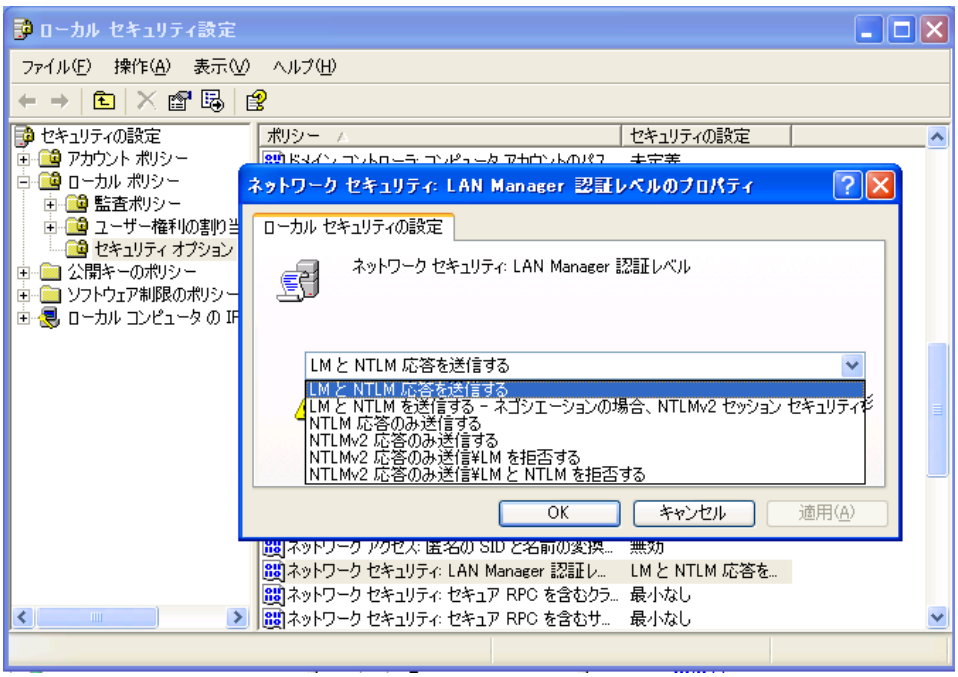
**「ネットワークセキュリティ LAN Manager 認証レベル」のセキュリティレベルを**「NTLMv2 応答のみを送信（LM と NTLM を拒否する）」に設定**することを推奨します。**

**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。

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」→「監査ポリシー」を開きます。

③ 「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）

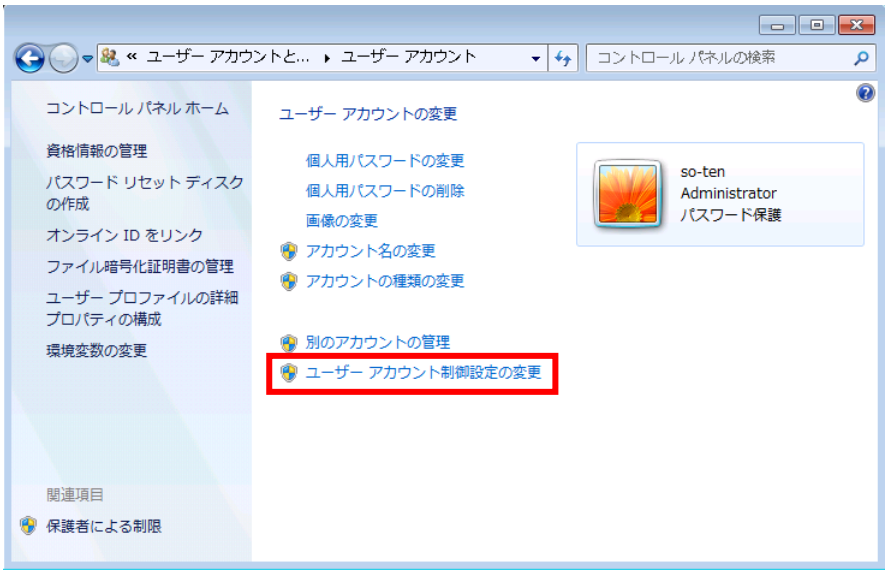
① 「ユーザー アカウント」を起動します。

"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。

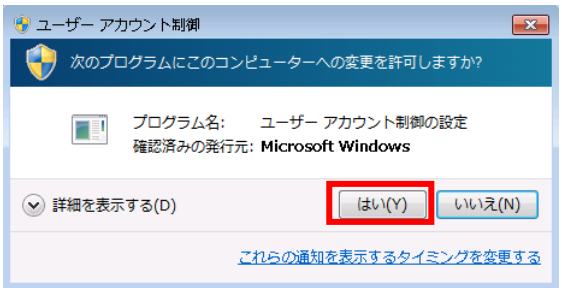
※「ユーザー アカウント」の表示のためには「コントロールパネル」で「小さいアイコン」または「大きいアイコン」の選択が必要です。

② 「ユーザー アカウント制御設定の変更」を変更します。

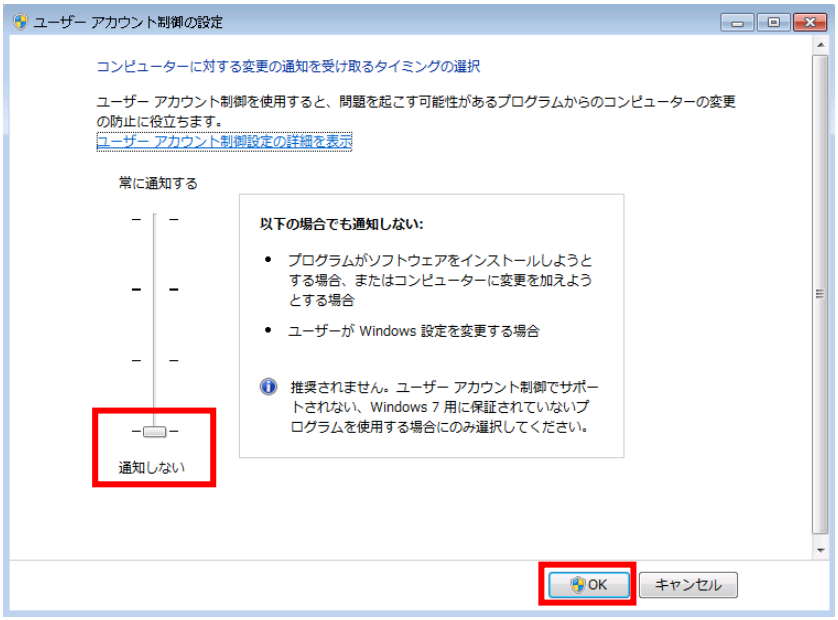
「ユーザー アカウント制御設定の変更」をクリックします。



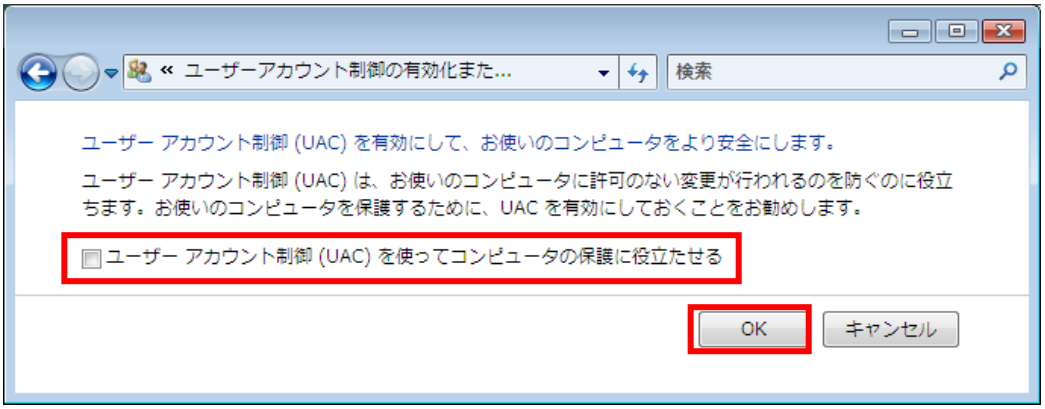

下図が表示された場合は、「はい」をクリックします。




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。

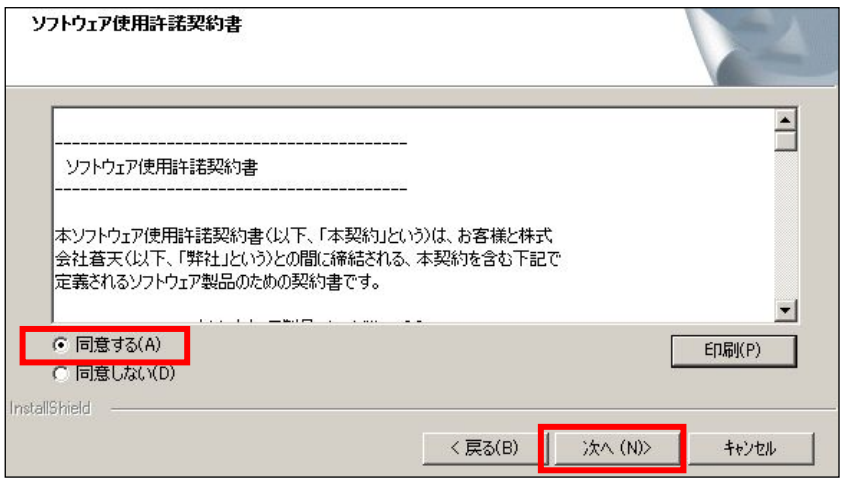
## 5-2. LogVillagePS のインストール手順

LogVillagePS ののインストール手順について説明します。

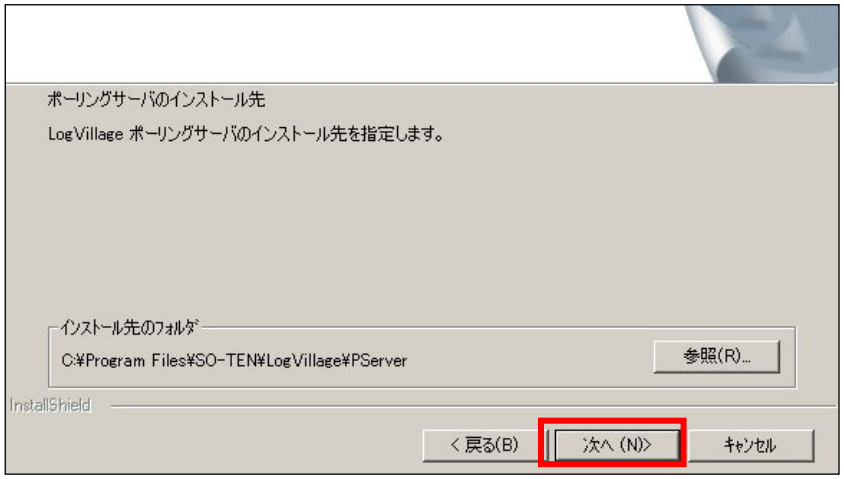
① Windows 管理者権限アカウントでログインし、Setup.exe を実行します。
CD-ROM 内 Installer フォルダ下の PServer フォルダ開きます。
Setup.exe をダブルクリックします。


② 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。

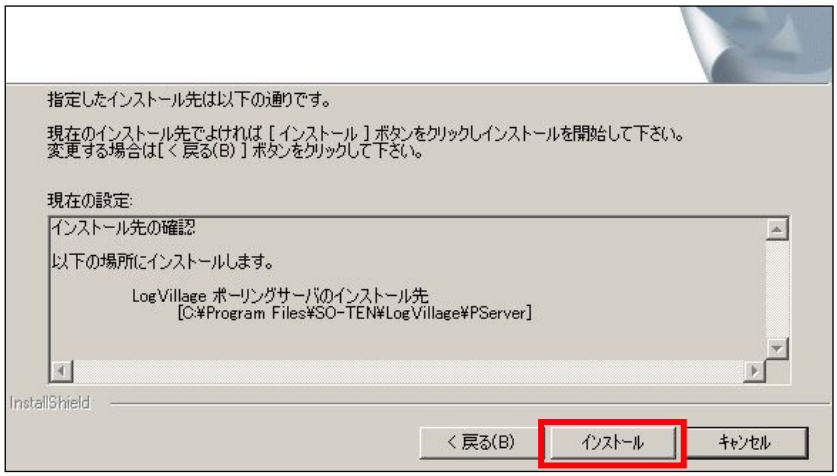

ソフトウェア使用許諾契約書を確認し、問題なければ「同意する」を選択し、
「次へ」をクリックします。



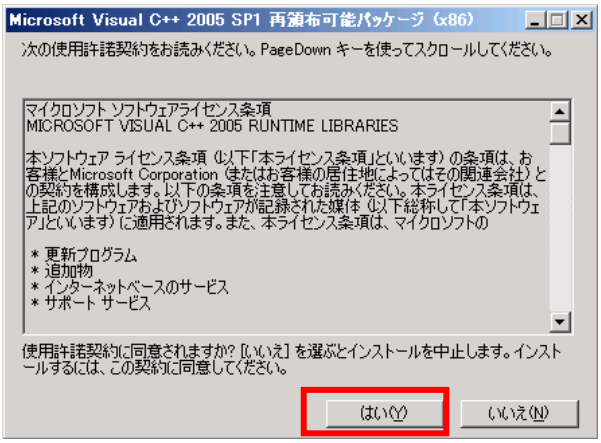
LogVillagePS のインストール先フォルダを変更しない場合は「次へ」をクリックします。
インストール先を変更する場合は、参照からインストール先フォルダを指定後、「次へ」をクリックします。




③ 「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。



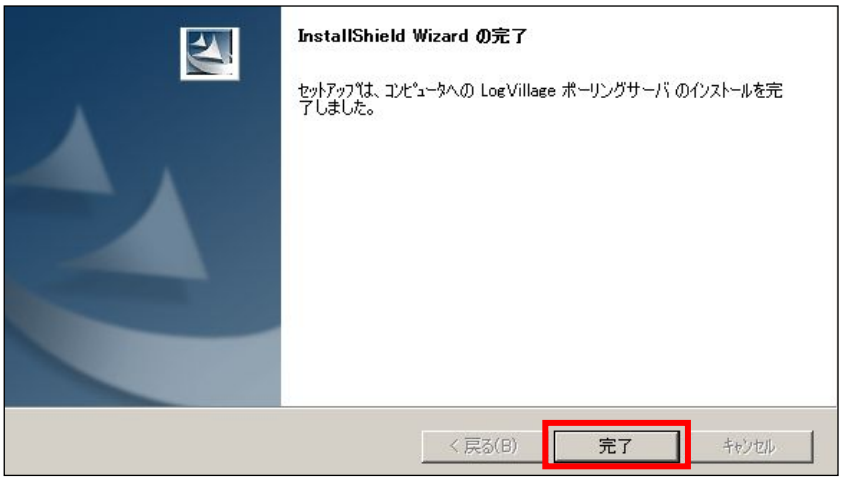
LogVillage マネージャでは、マイクロソフト社製の“Microsoft Visual C++ 2005 再配布可能パッケージ”を 利用しています。
そのため、以下のマイクロソフト ソフトウェアライセンス条項に同意いただく必要があります。
Microsoft Visual C++ 2005 使用許諾書を確認し「はい」をクリックします。




※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。

④ インストール完了まで、しばらく待ちます。

⑤ 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。

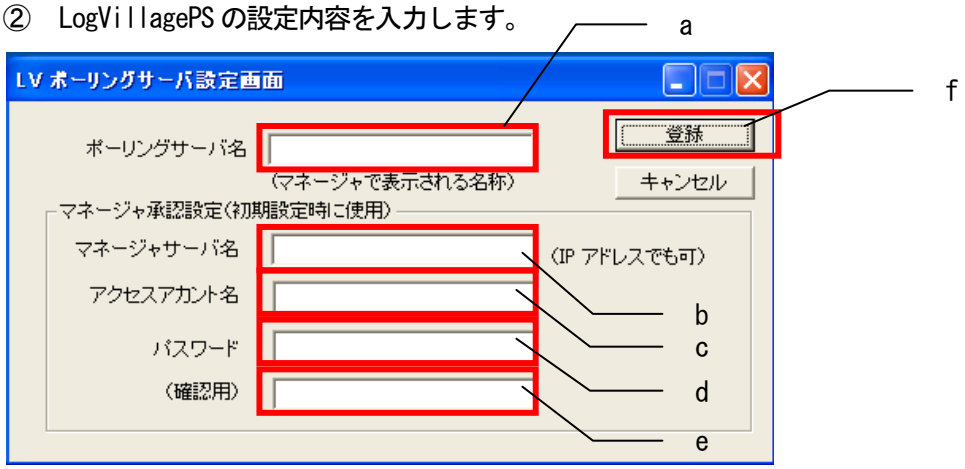


## 5-3. LogVillagePS のセットアップ

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。

② LogVillagePS の設定内容を入力します。




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。

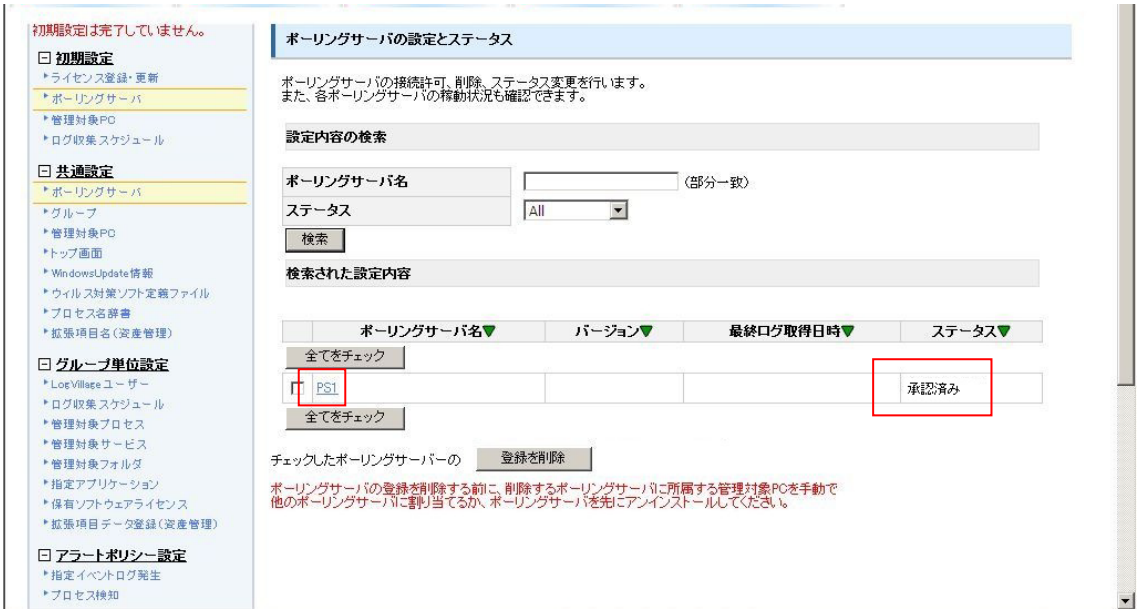
③ LogVillage 管理画面にログインします。
Internet Explorer を起動します。
以下の URL にアクセスすると LogVillage ログイン画面が表示されます。

| 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。


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」<br>→<br>「ライセンス登録・更新」 | ・LogVillageMGR のインストール直後：<br>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。<br>・ライセンスコードを登録<br>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」<br>→<br>「ポーリングサーバ」 | ・LogVillagePS の登録：<br>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」<br>→<br>「管理対象 PC」 | ・一括登録：<br>CSV ファイルより一括登録<br>・一台づつ登録：<br>本画面より登録<br>・自動登録：<br>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」<br>→<br>「ログ収集スケジュール」 | ・グループ別に設定可能<br>・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。

## 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）<br>・サービス稼働時間 |
| インベントリ | （資産管理）<br>・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）<br>セキュリティ対策更新状況<br>→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）<br>・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）<br>・アプリケーションインストール履歴<br>・セキュリティ対策更新状況<br>→WindowsUpdate の適用状況<br>（資産管理）<br>・PC 資産管理台帳→ソフトウェア台帳<br>・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）<br>・デバイス接続履歴 |
| Web アクセス履歴 | （操作管理）<br>・Web アクセス履歴 |
| パフォーマンス・プロセス | （稼働管理）<br>・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）<br>・イベントログ<br>（操作管理）<br>・印刷履歴　・ログオン・オフ履歴 |
| ファイル | （ファイル管理）<br>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。

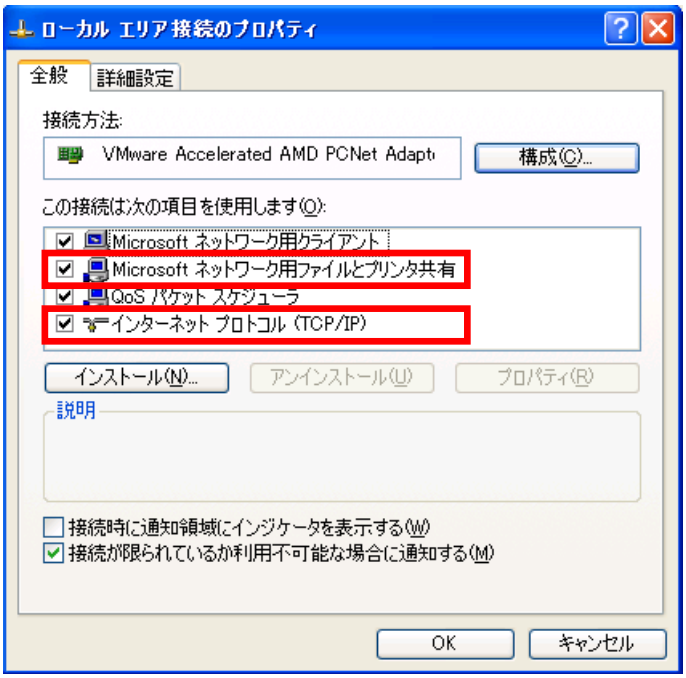
**前提条件**

・管理対象 PC がネットワークに参加している事

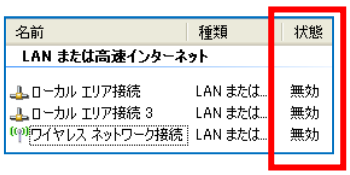
※「3-2. LogVillagePS→管理対象 PC へのアクセス確認」を参照してください。

・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」（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

## 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。

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。

## 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。<br>「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。<br>「アカウントログオンイベントの監査」<br>「ログオンイベントの監査」<br>・「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。<br>「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。<br>「リモートからの起動」<br>「リモートからのアクティブ化」<br>・「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。<br>「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」<br>・「例外」で以下を有効にします。<br>「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。<br>「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」<br>・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。<br>※UAC を停止することなくご利用いただくことも可能です。<br>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。

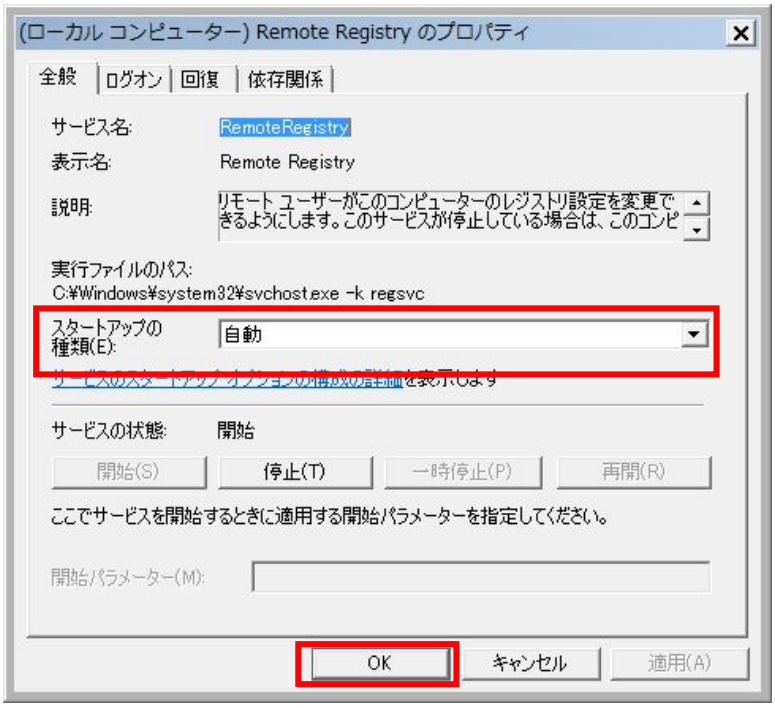
※「管理ツール」の表示のためには「コントロールパネル」で「小さいアイコン」または「大きいアイコン」の選択が必要です。

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。



### 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。

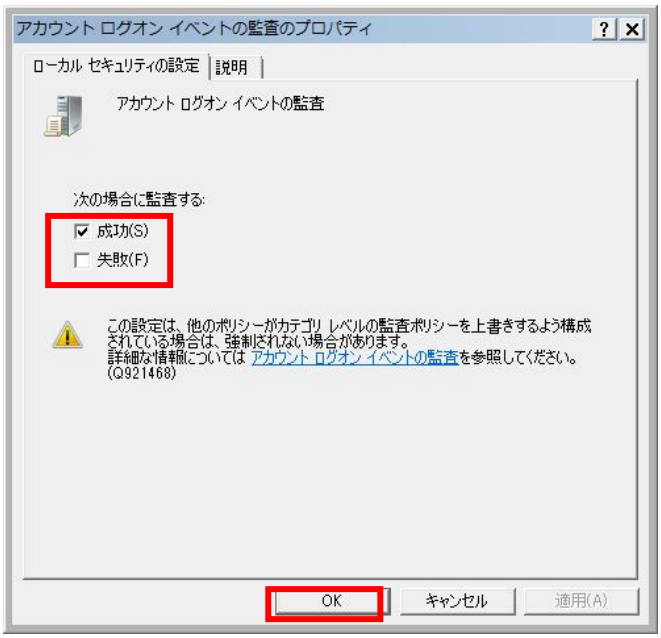
※「管理ツール」の表示のためには「コントロールパネル」で「小さいアイコン」または「大きいアイコン」の選択が必要です。

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。

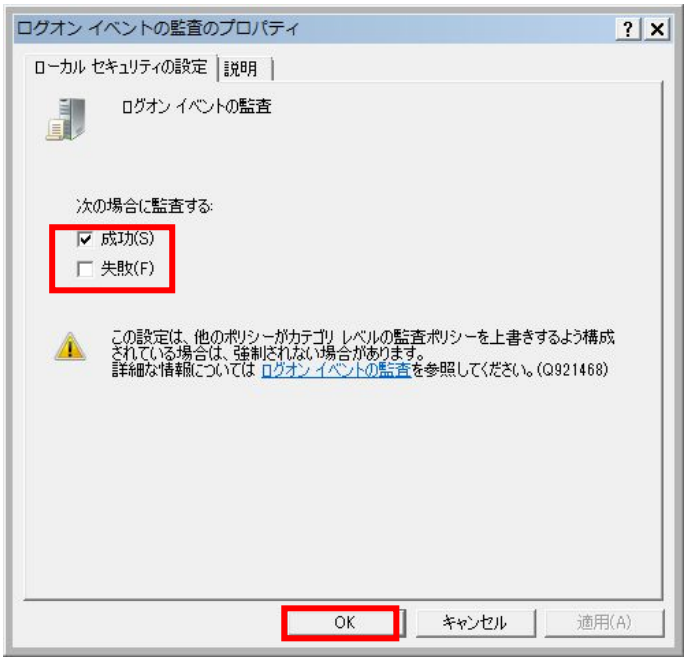
③ 「アカウントログオンイベントの監査」を変更します。

「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。



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。



【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。

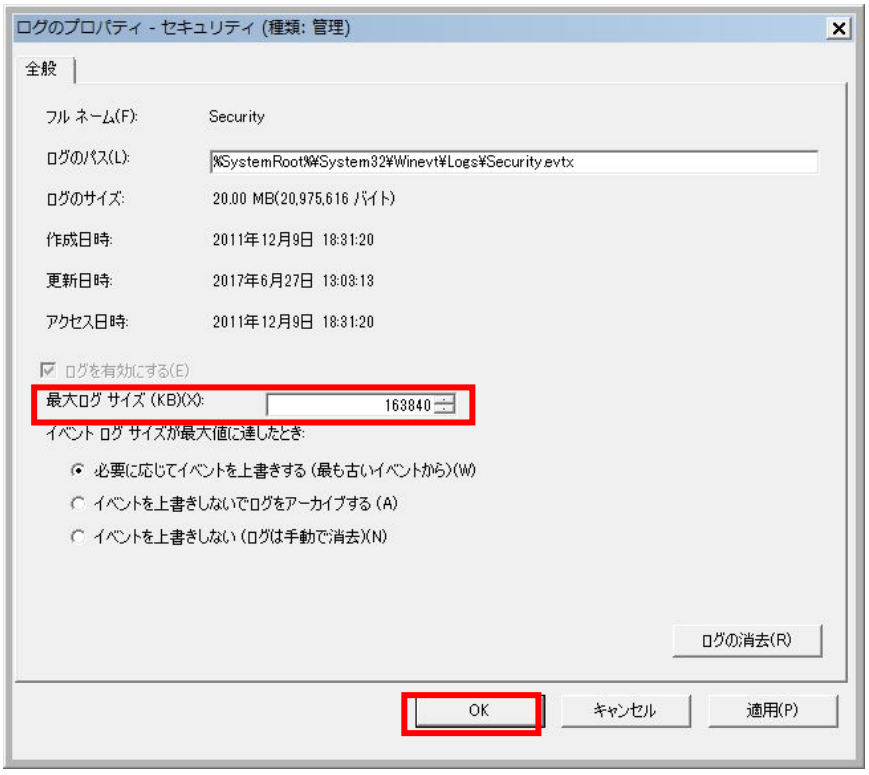
※「管理ツール」の表示のためには「コントロールパネル」で「小さいアイコン」または「大きいアイコン」の選択が必要です。

「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。

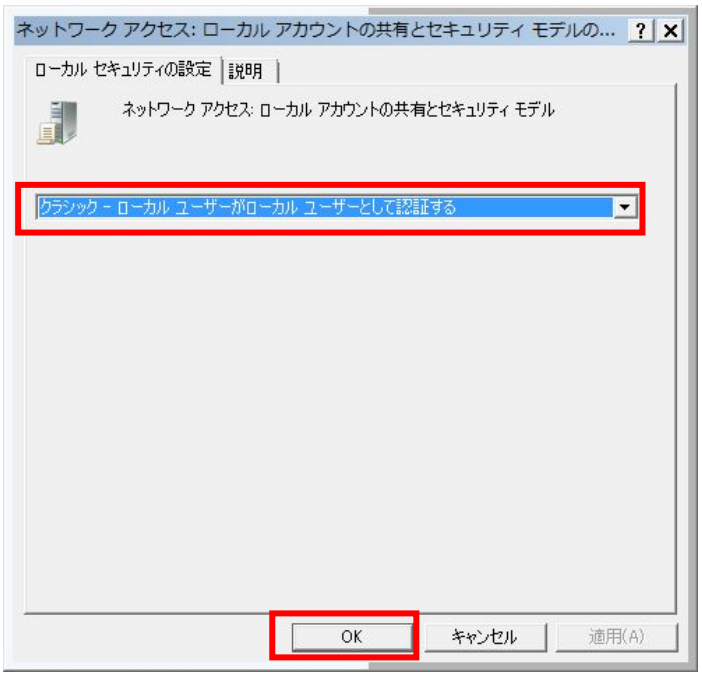
※管理ツール」の表示のためには「コントロールパネル」で「小さいアイコン」または「大きいアイコン」の選択が必要です。

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。

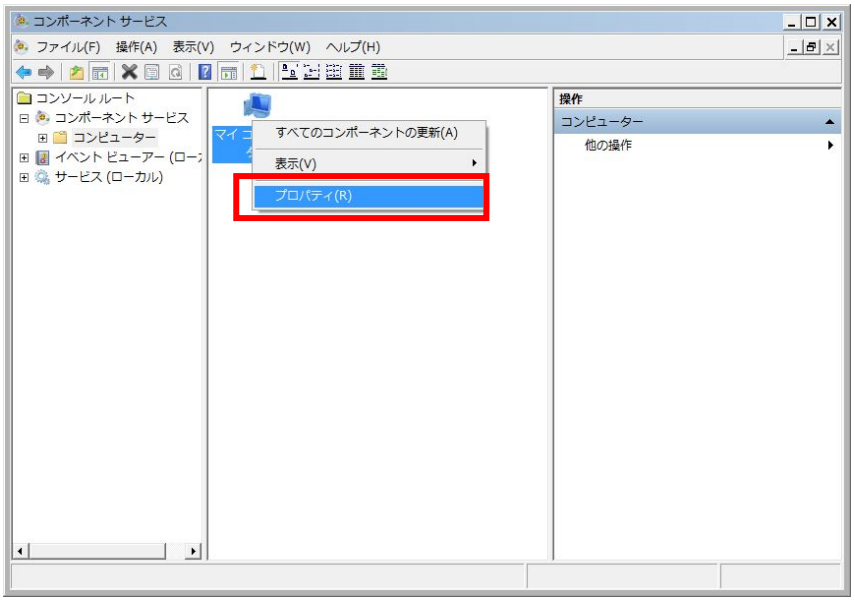


### 4) DCOM リモート起動のアクセス許可

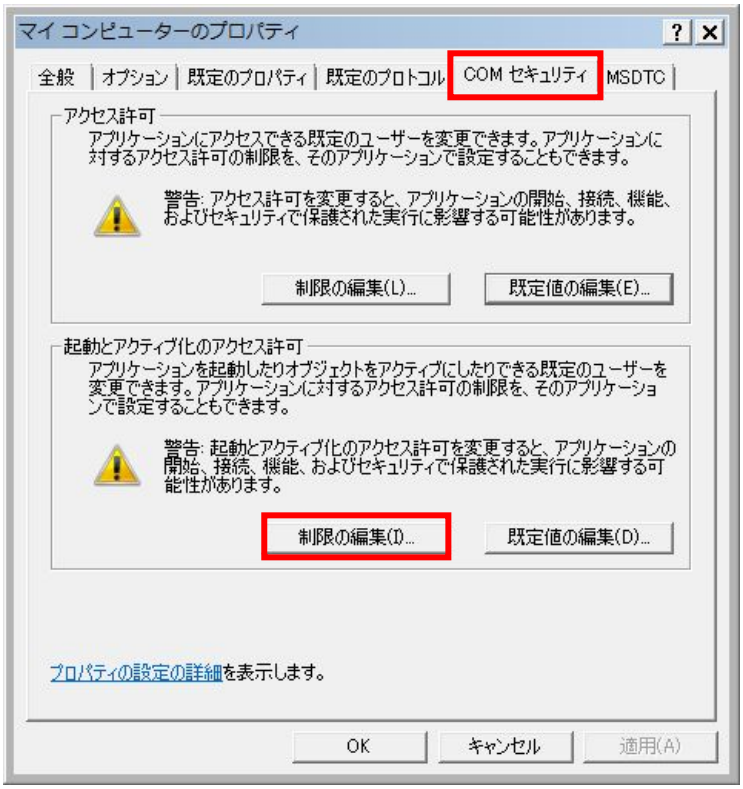
WMI によるデータの収集のため、リモートからの起動許可が必要になります。
またLogVillage では、この WMI 情報を基本としているため、WMI 情報が収集されない場合、それ以外のすべての情報を正しく収集することが出来ません。
**通常この設定は行われていないため必ず設定変更が必要です。**

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。

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。



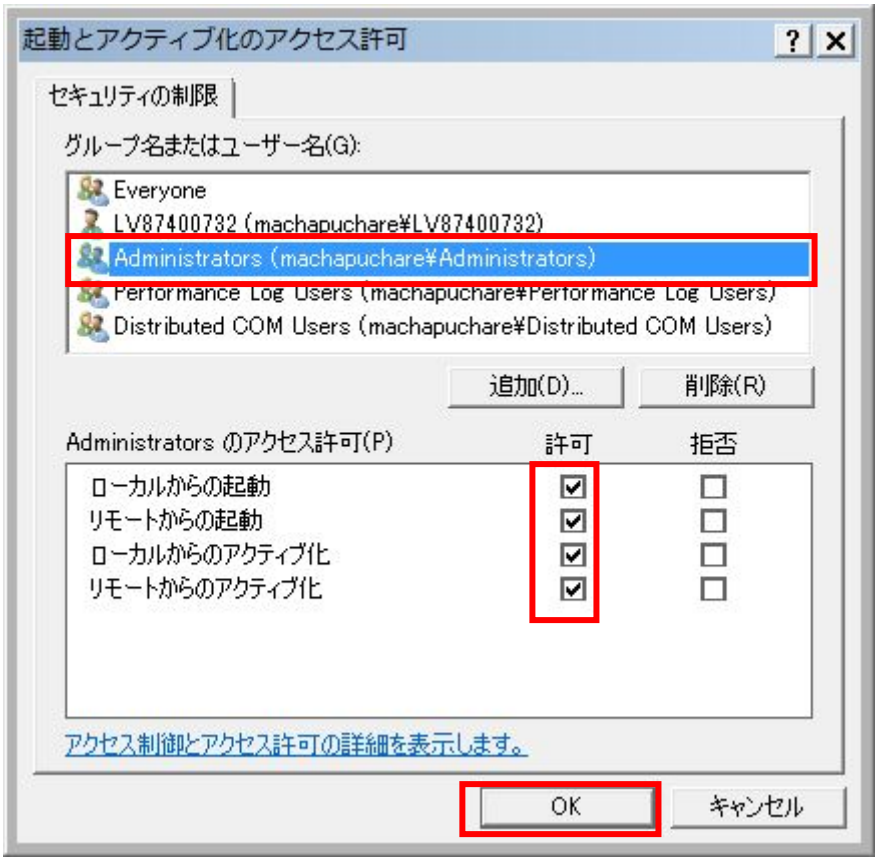
③　「起動とアクティブ化のアクセス許可」の「制限の編集」を変更します。
「COM セキュリティ」タブを開き、「起動とアクティブ化のアクセス許可」の「制限の編集」をクリックします。



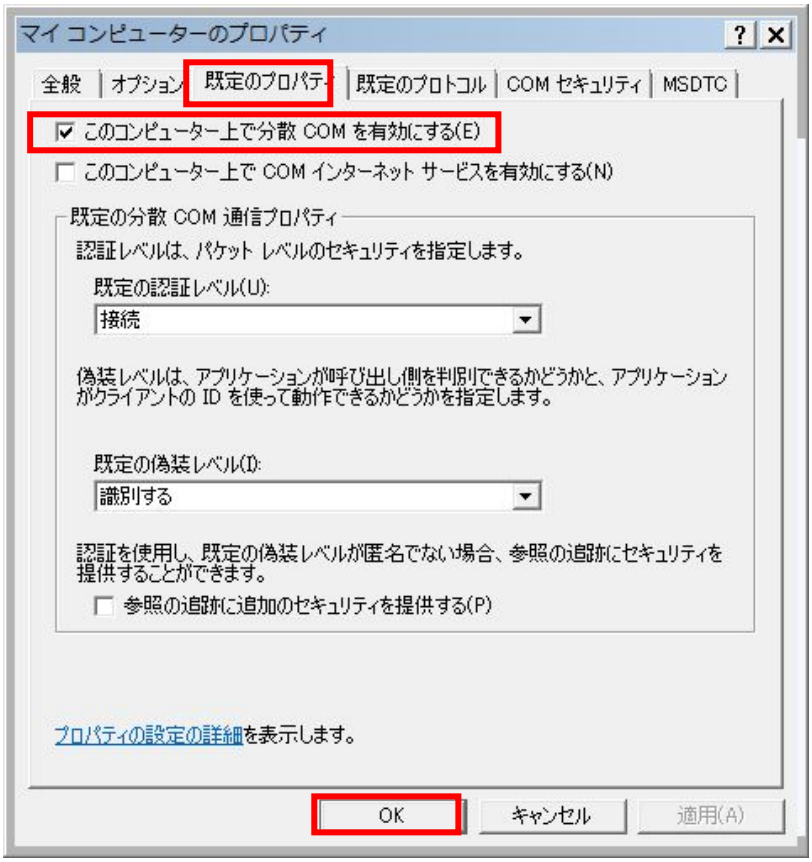
LogVillage で使用するユーザーまたはグループをクリックします。

「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。



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。

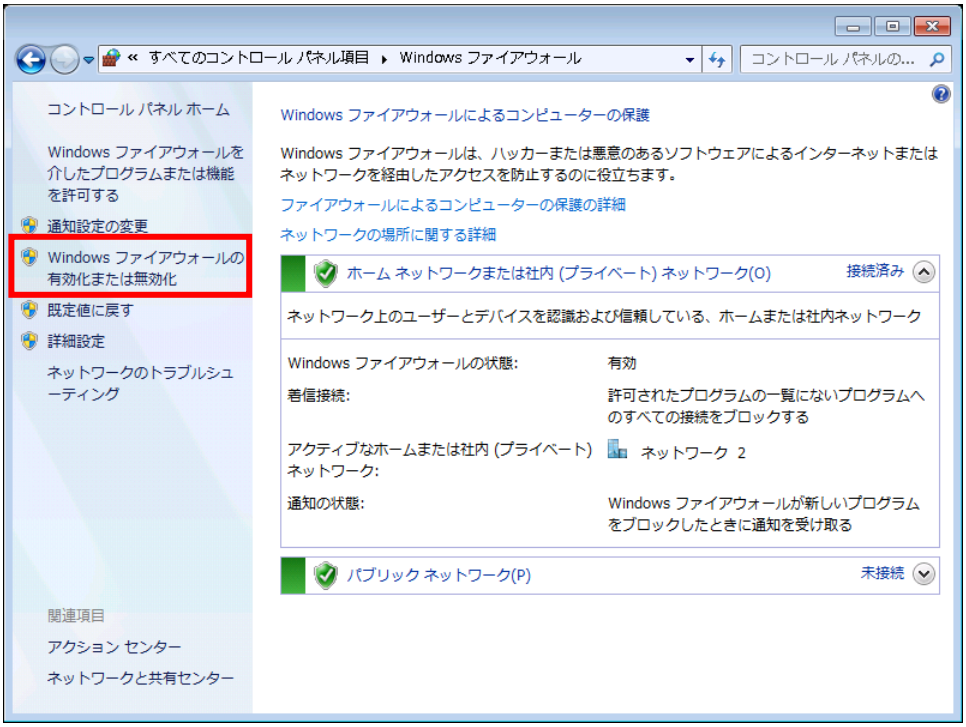
Windows ファイアウォールの種類として「パブリック ネットワーク」と「ホーム ネットワークまたは社内（プライベート）ネットワーク」があり、「パブリック ネットワーク」とは、空港、喫茶店など、公共のネットワークを指しています。
LogVillage は社内環境にてご利用いただく事を想定しているため、「プライベート ネットワーク」でご利用いただく事を推奨いたします。

※「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。

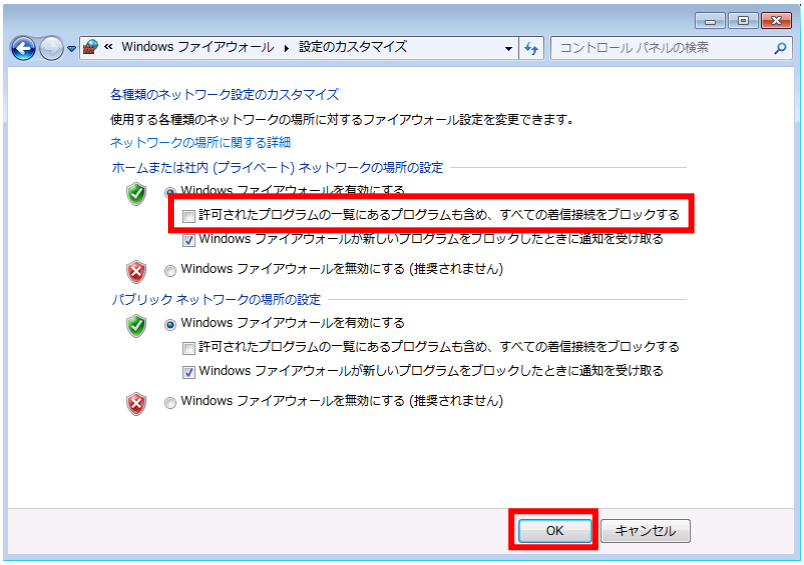
① 「Windows ファイアウォール」を起動します。
"Windows スタートメニュー"→「コントロールパネル」→「Windows ファイアウォール」を起動します。

※「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。

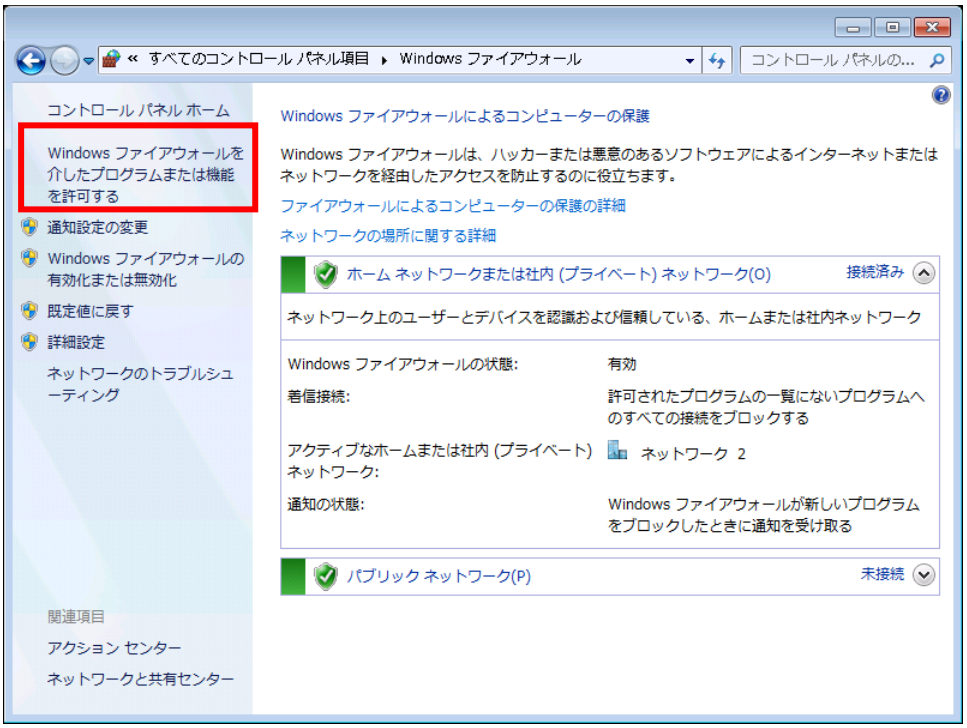
② 「許可されたプログラムの一覧にあるプログラムも含め、すべての着信接続をブロックする」を確認します。
「Windows ファイアウォールの有効化または無効化」をクリックします。


« すべてのコントロール パネル項目 ▸ Windows ファイアウォール
コントロール パネルの...
コントロール パネル ホーム
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
通知設定の変更
Windows ファイアウォールの有効化または無効化
既定値に戻す
詳細設定
ネットワークのトラブルシューティング
関連項目
アクション センター
ネットワークと共有センター
Windows ファイアウォールによるコンピューターの保護
Windows ファイアウォールは、ハッカーまたは悪意のあるソフトウェアによるインターネットまたはネットワークを経由したアクセスを防止するのに役立ちます。
ファイアウォールによるコンピューターの保護の詳細
ネットワークの場所に関する詳細
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(O)
接続済み
ネットワーク上のユーザーとデバイスを認識および信頼している、ホームまたは社内ネットワーク
Windows ファイアウォールの状態:
有効
着信接続:
許可されたプログラムの一覧にないプログラムへのすべての接続をブロックする
アクティブなホームまたは社内 (プライベート) ネットワーク:
ネットワーク 2
通知の状態:
Windows ファイアウォールが新しいプログラムをブロックしたときに通知を受け取る
パブリック ネットワーク(P)
未接続

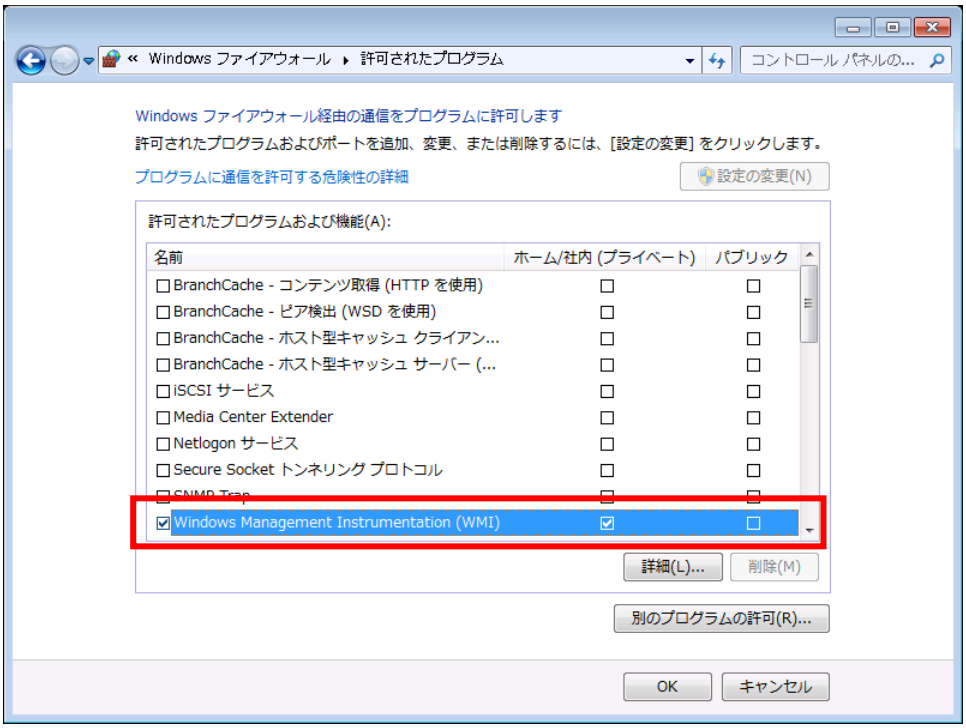
接続中ネットワークの「許可されたプログラムの一覧にあるプログラムも含め、すべての着信接続をブロックする」にチェックが無い事を確認し、「OK」をクリックします。



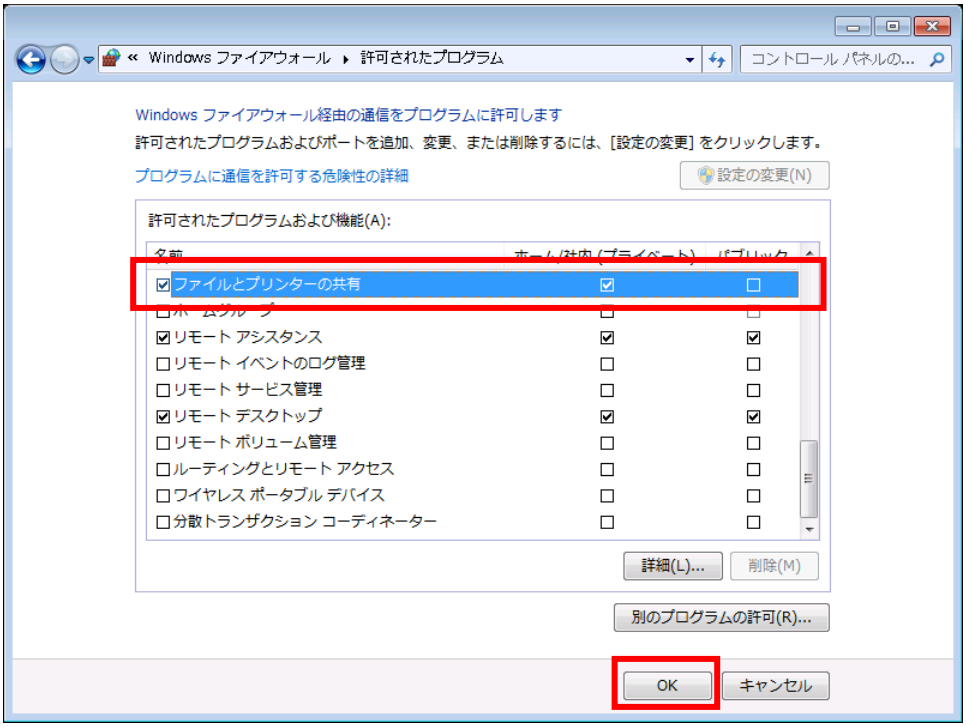

③　「Windows Management Instrumentation (WMI)」を変更します。
「Windows ファイアウォールを介したプログラムまたは機能を許可する」をクリックします。



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



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。



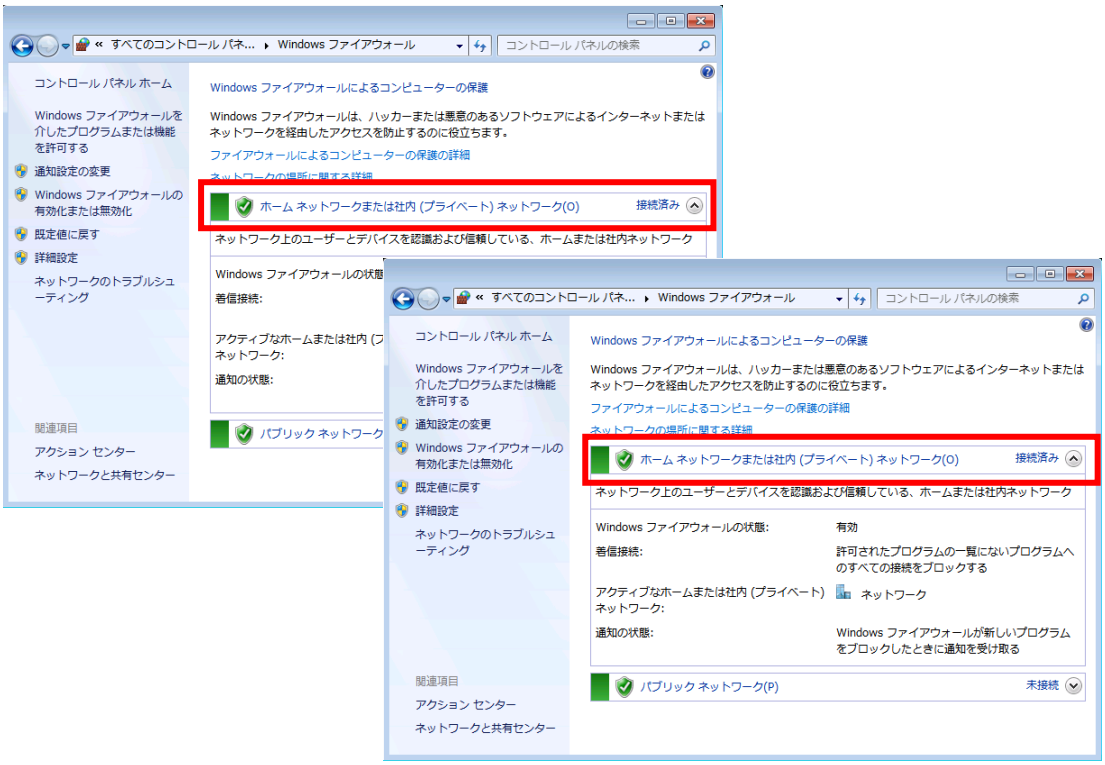
・Windows7 のネットワーク設定と Windows ファイアウォールの関係

LogVillagePS と管理対象 PC が別セグメントで「ネットワークと共有センター」のアクティブなネットワークが「ホーム／社内 ネットワーク」の場合、Windows ファイアウォールの「ホーム／社内」に LogVillage 用の設定を行っても、情報が収集できません。この場合「パブリック」をご利用ください。

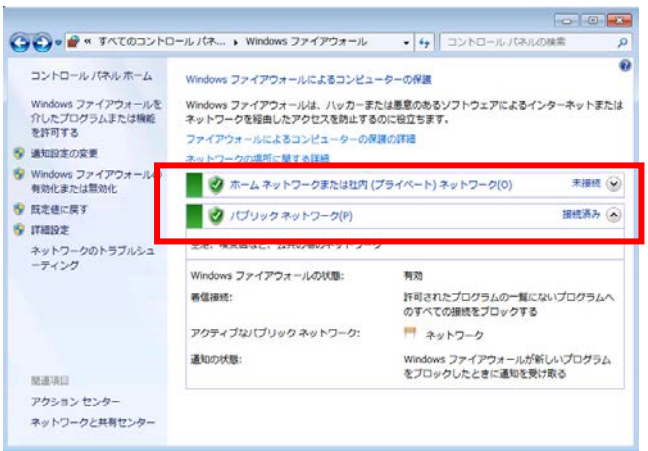
・ネットワークの場所を確認する方法

・Windows ファイアウォールが下図の場合は「ホーム/社内（プライベート）」です。

※LogVillagePS と管理対象 PC が別セグメントの場合、この環境ではログが収集できません。




・Windows ファイアウォールが下図の場合「パブリック」です。



**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。**

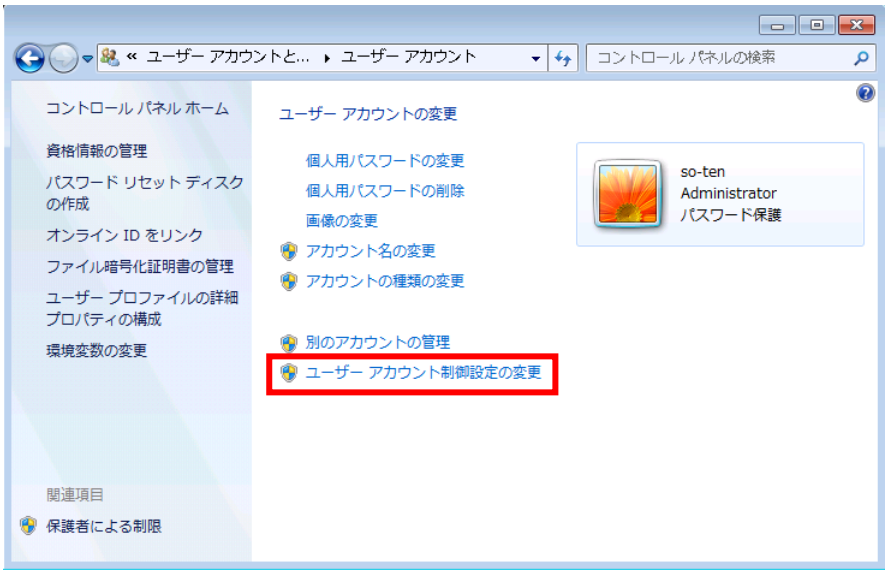
① 「ユーザー アカウント」を起動します。

"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。

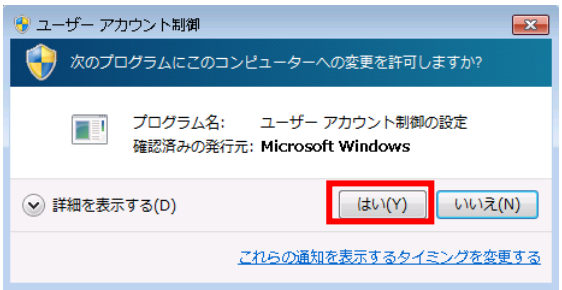
※「ユーザー アカウント」の表示のためには「コントロールパネル」で「小さいアイコン」または「大きいアイコン」の選択が必要です。

② 「ユーザー アカウント制御設定の変更」を変更します。

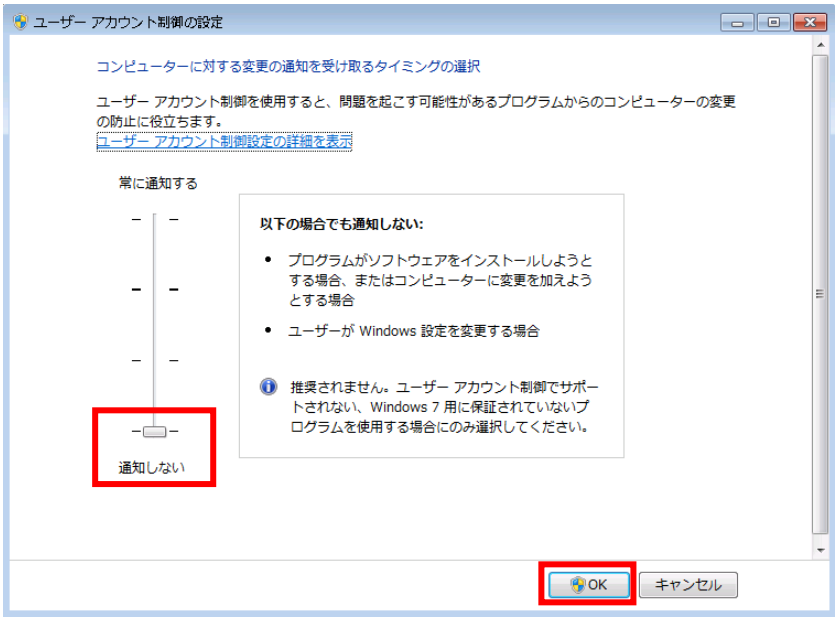
「ユーザー アカウント制御設定の変更」をクリックします。



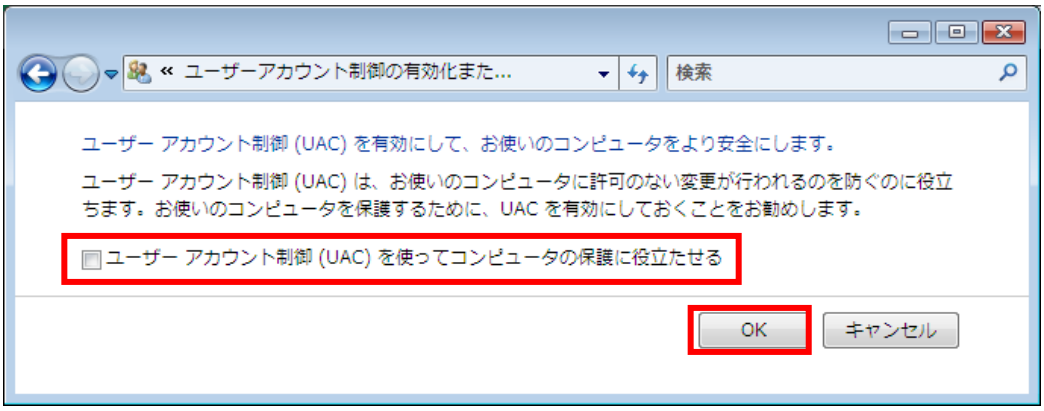

下図が表示された場合は、「はい」をクリックします。



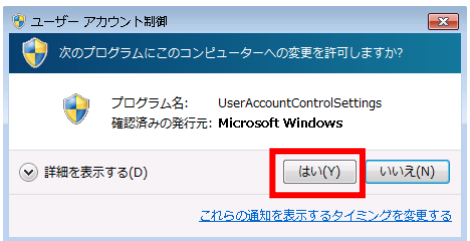
スライダのつまみを一番下「通知しない」まで下げ、「OK」をクリックします。




※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

## 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 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

## 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。<br>「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。<br>「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」<br>・「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。<br>「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。<br>「Administrators」<br>・「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<br>「Windows ファイアウォール:リモート管理の例外を許可する」<br>「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」<br>「Windows ファイアウォール: ポートの例外を許可する」<br>・以下に「TCP135」を追加します。<br>「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。

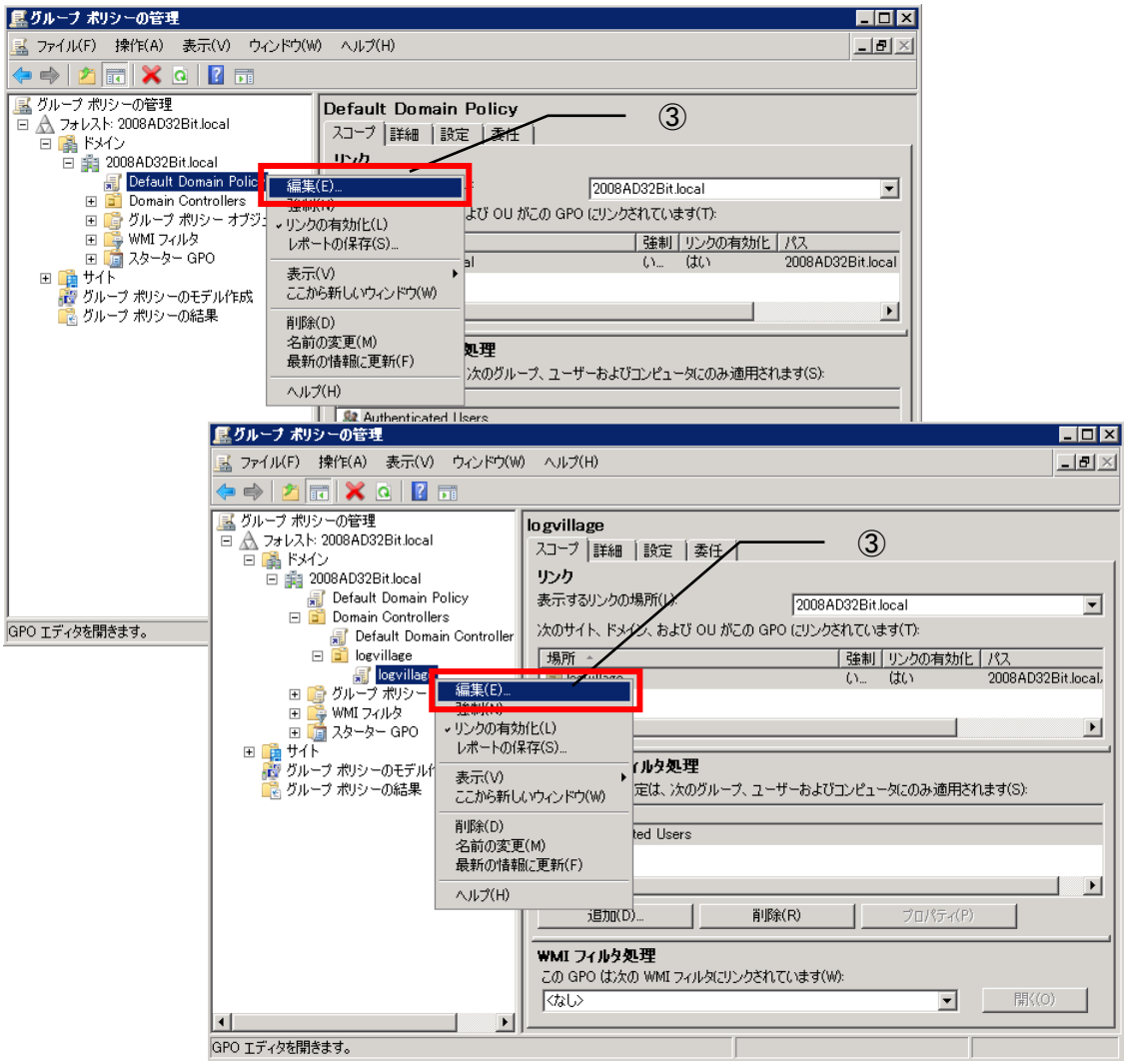
**グループポリシー設定画面「グループ ポリシー管理エディタ」の表示方法**

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。

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。



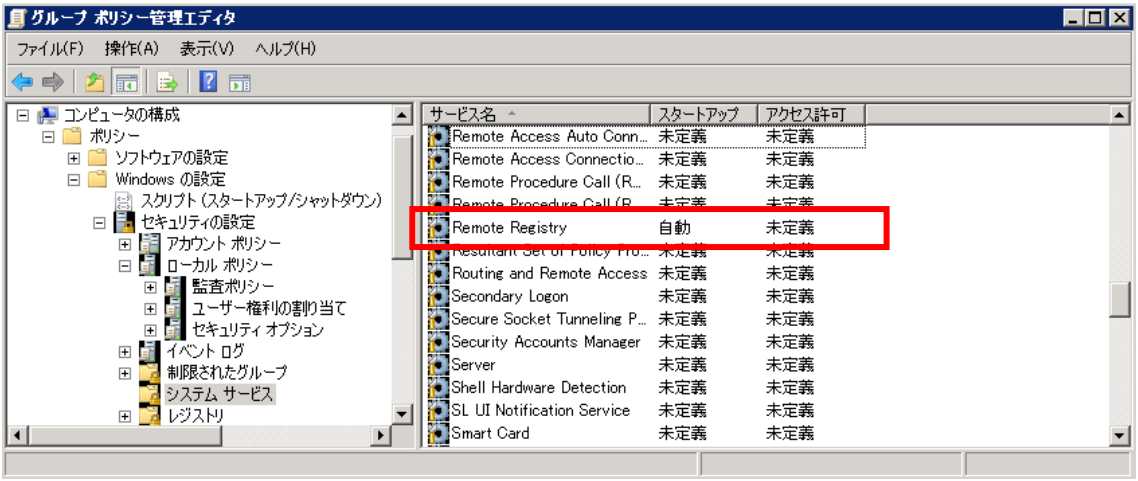

左上図は、Default Domain Policy（全体）に設定する場合の例です。

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。

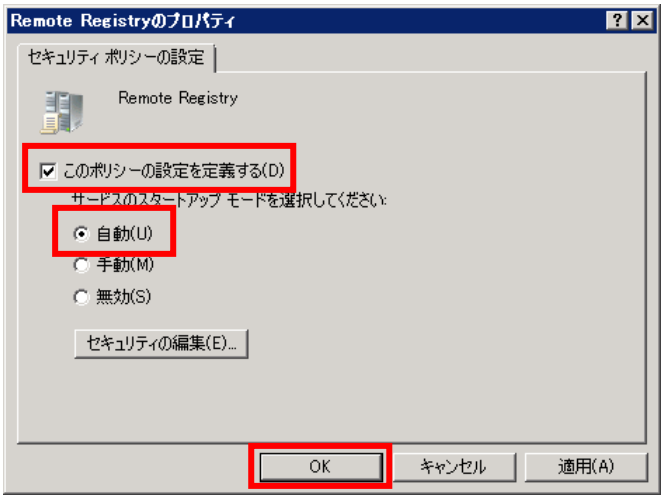
**1)リモートレジストリーサービス**

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。




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。

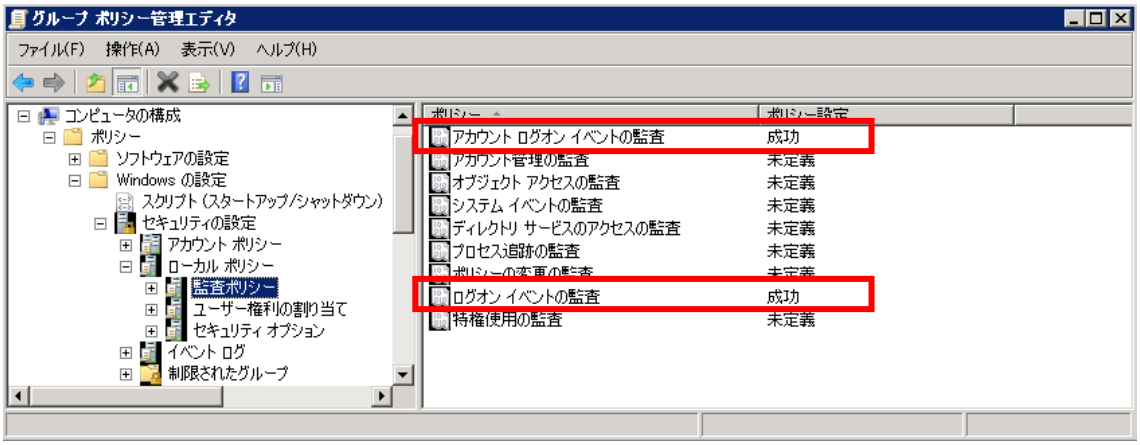


### 2) アカウント・ログオン・ログ

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。

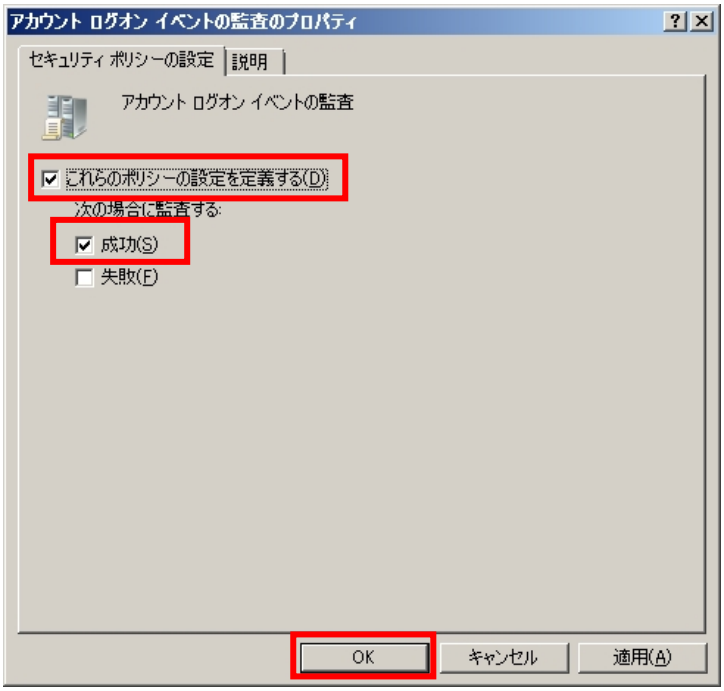



② 「アカウント ログオンイベントの監査」を設定します。

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。

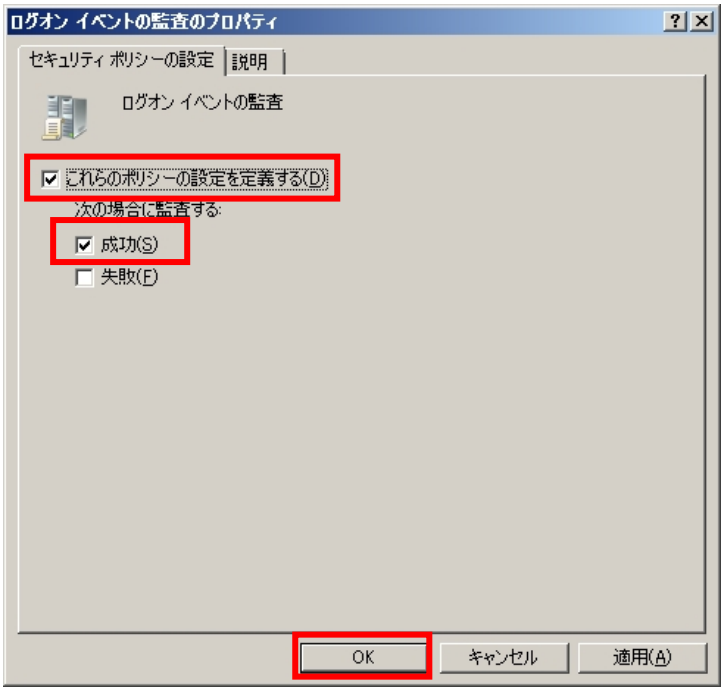


③　「ログオンイベント の監査」を設定します。

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。



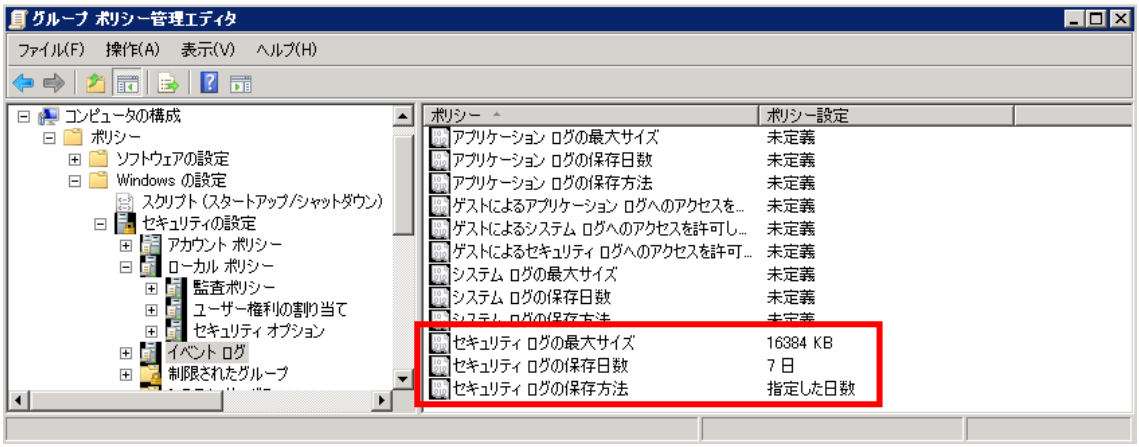
**イベントログの修正**

※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。

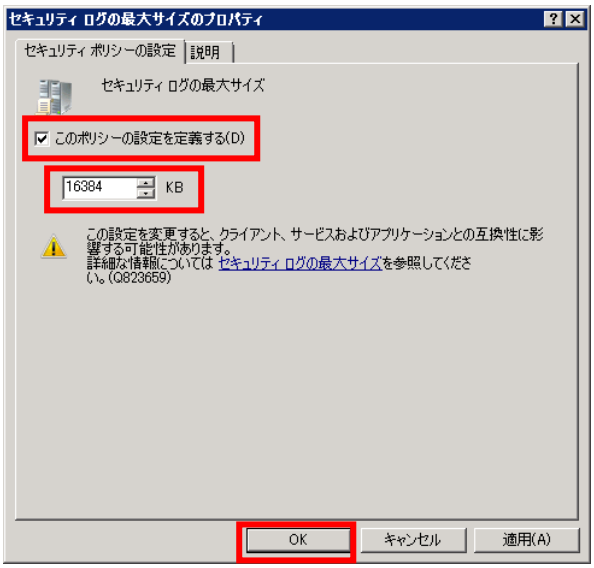



② 「セキュリティログの最大サイズ」を設定します。

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
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。

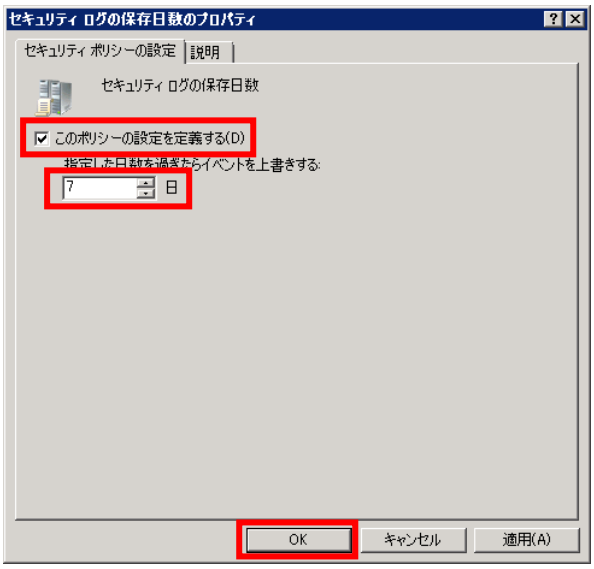
・必要に応じてイベントを上書きする
セキュリティログが最大サイズになった場合、古いログから削除されます。
一定期間のログを必ず残すポリシーの場合は「指定した日数を過ぎたら上書きする」を選択する必要があります。
LogVillage にてセキュリティログを収集していない場合、上書により削除された期間のログが収集できません。

・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。

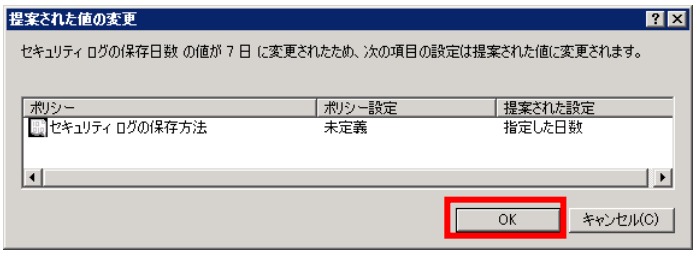
ログが自動的に削除されても問題無い場合は、「必要に応じてイベントを上書きする」を選択してください。
ログの削除を禁止している場合は、「イベントを上書きしない（手動でログを消去）」を選択してください。

※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。

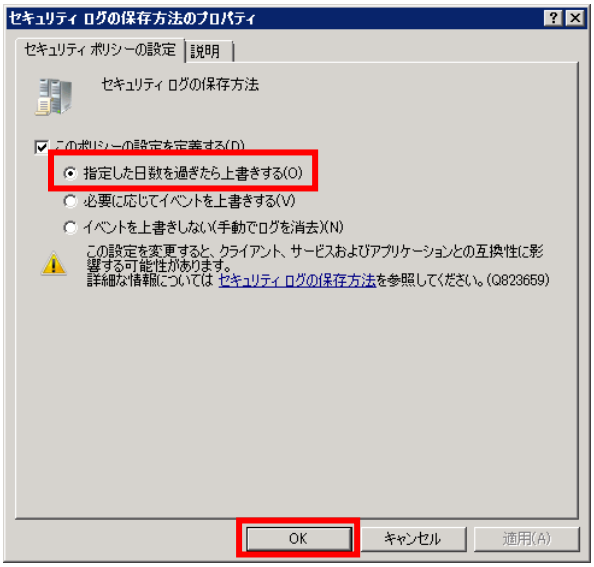
③　「セキュリティログの保存日数」を設定します。
「セキュリティログの保存日数」をダブルクリックします。
「このポリシーの設定を定義する」にチェックを入れます。
「（任意の数値）日」に変更し、「OK」をクリックします。




下図が表示されたら「OK」をクリックします。

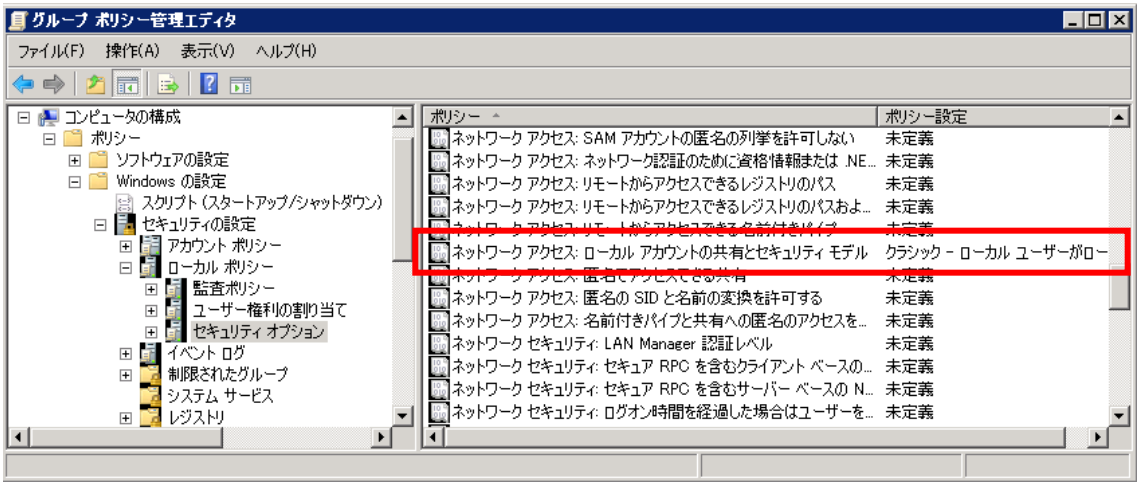


④　「セキュリティログの保存方法」を設定します。
「セキュリティログの保存方法」をダブルクリックします。
「指定した日数を過ぎたら上書きする」にチェックが入っている事を確認し、「OK」をクリックします。

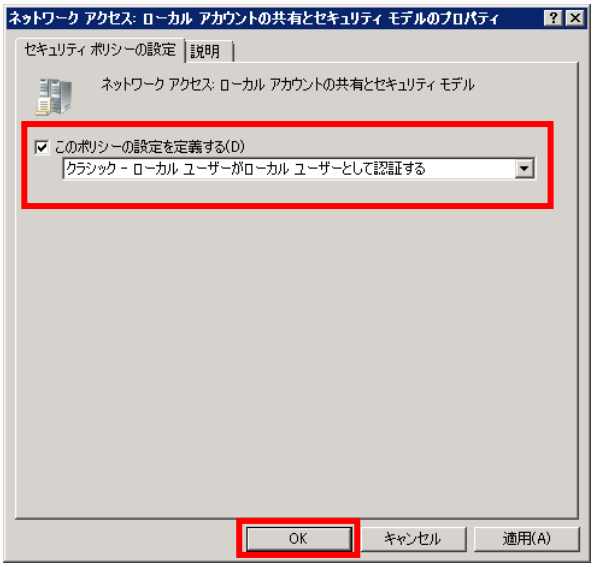


### 3）ネットワークアクセス時のアカウント認証方法

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。

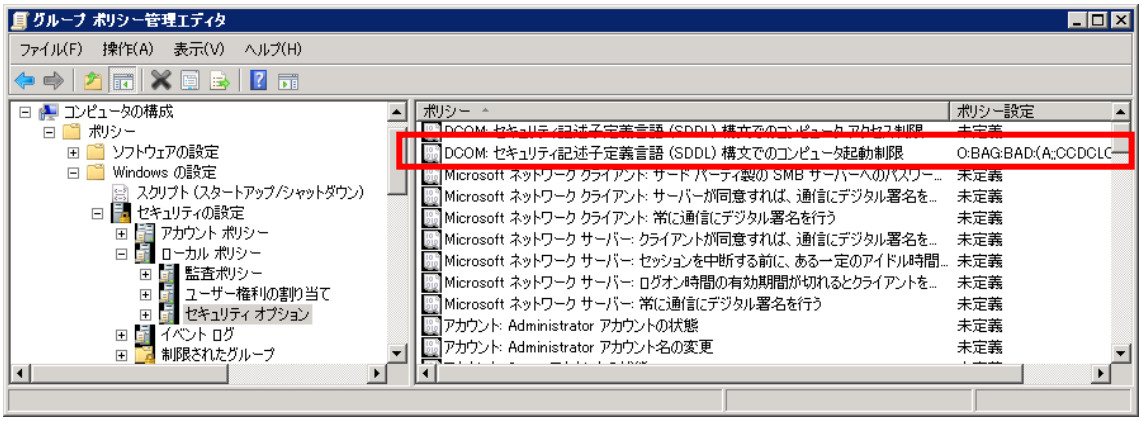



② 「ネットワーク アクセス: ローカル アカウントの共有とセキュリティ モデル」を設定します。
「ネットワーク アクセス: ローカル アカウントの共有とセキュリティ モデル」をダブルクリックします。
「このポリシーの設定を定義する」にチェックを入れます。
「クラシック－ローカルユーザがローカルユーザとして認証する」が選択されている事を確認し「OK」をクリックします。

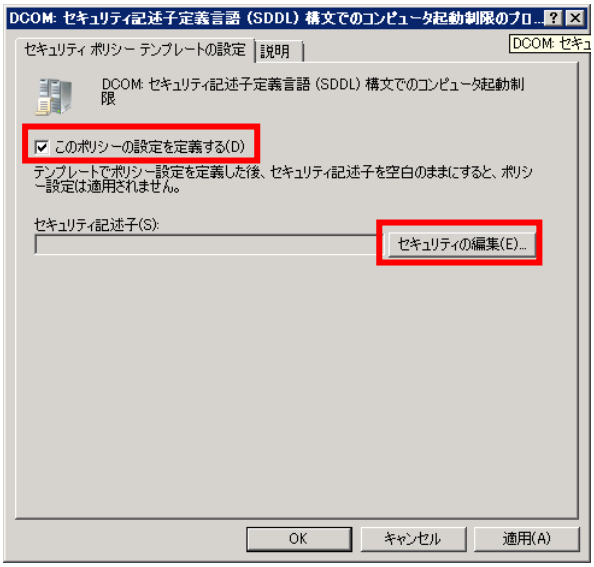


### 4) DCOM リモート起動のアクセス許可

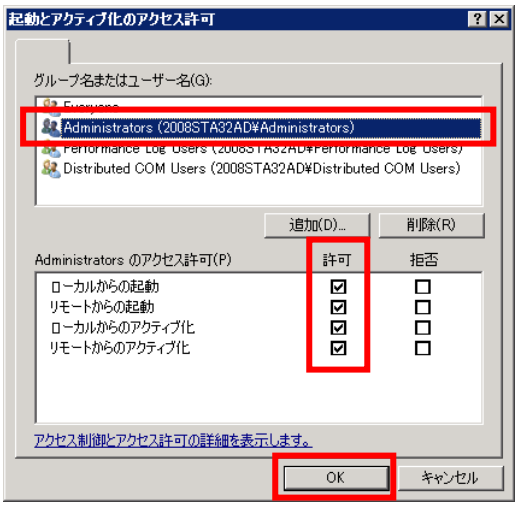
① 「セキュリティオプション」を開きます。
設定を変更する「グループ ポリシー管理エディタ」を開きます。
「コンピュータの構成」→「Windows の設定」→「セキュリティの設定」→「ローカルポリシー」→「セキュリティオプション」の設定を開きます。



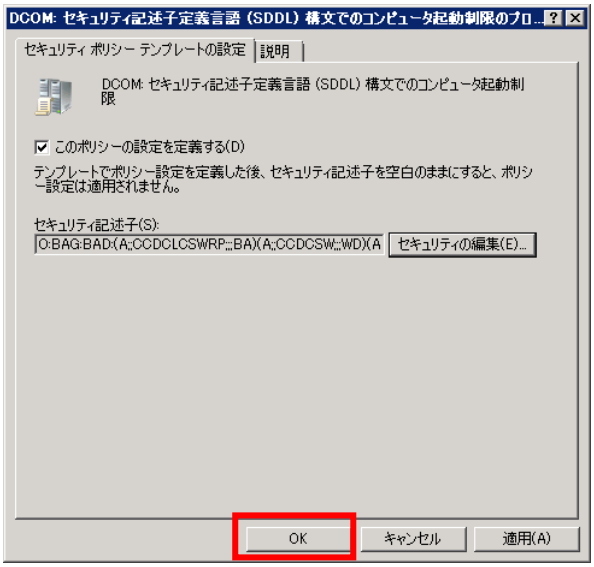

② 「DCOM: セキュリティ記述子定義言語 (SDDL) 構文でのコンピュータ起動制限」を設定します。
ポリシー名「DCOM: セキュリティ記述子定義言語 (SDDL) 構文でのコンピュータ起動制限」をダブルクリックします。
「このポリシーの設定を定義する」にチェックを入れます。
「セキュリティの編集」をクリックします。



「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。

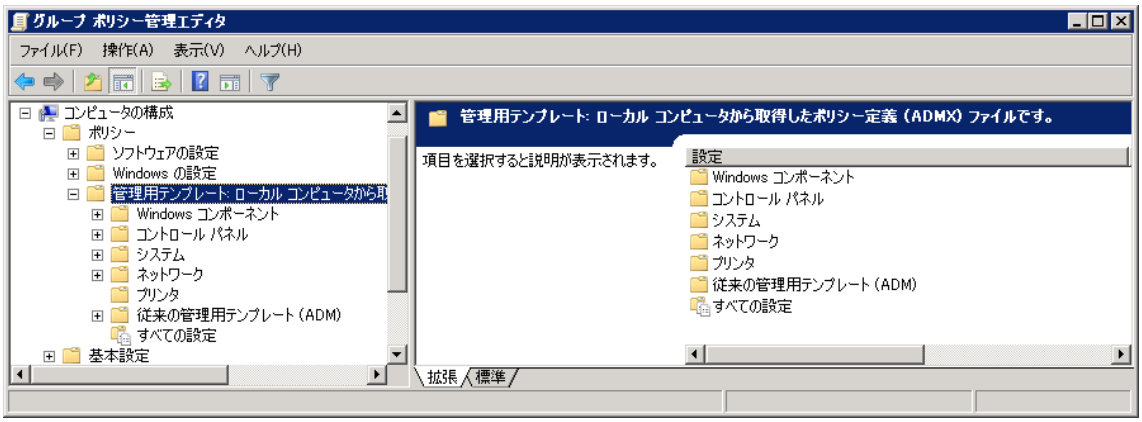


③ 分散 COM 設定用の設定変更用ファイルを配置します。
設定変更用ファイル（インストール媒体内 Tools フォルダ下の LV_DCOM.adm）をドメインコントローラーサーバの x:¥Windows¥inf へコピーします。
※x は OS インストールドライブです。

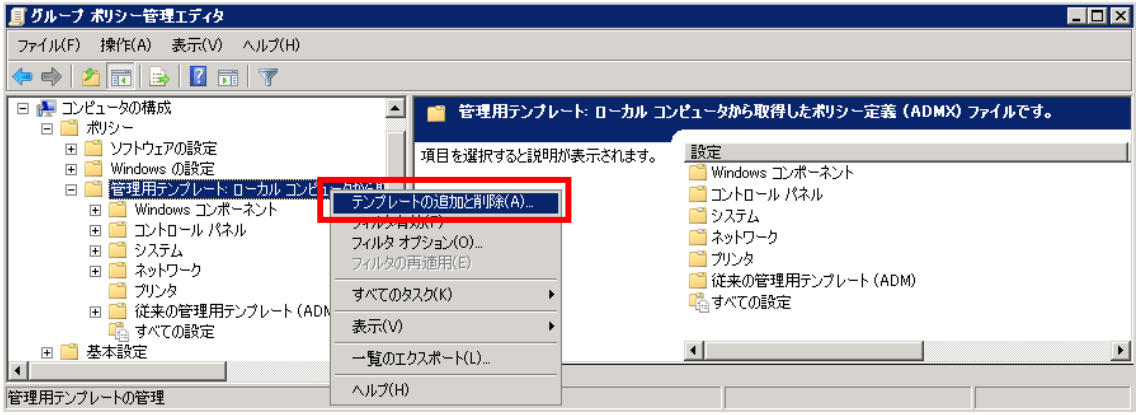
LV_DCOM.adm は以下の内容のテキストファイルです。

```
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"
```

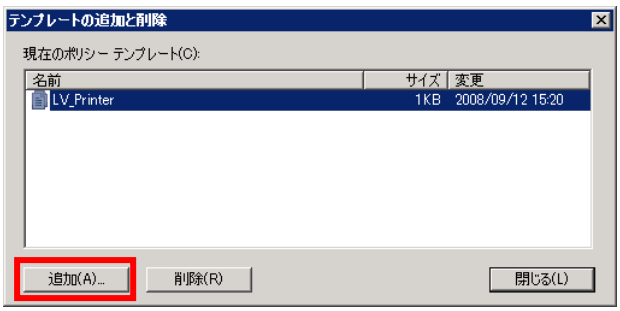
④ 「LogVillage 用 DCOM 設定」を追加します。
「コンピュータの構成」→「管理用テンプレート」を開きます。



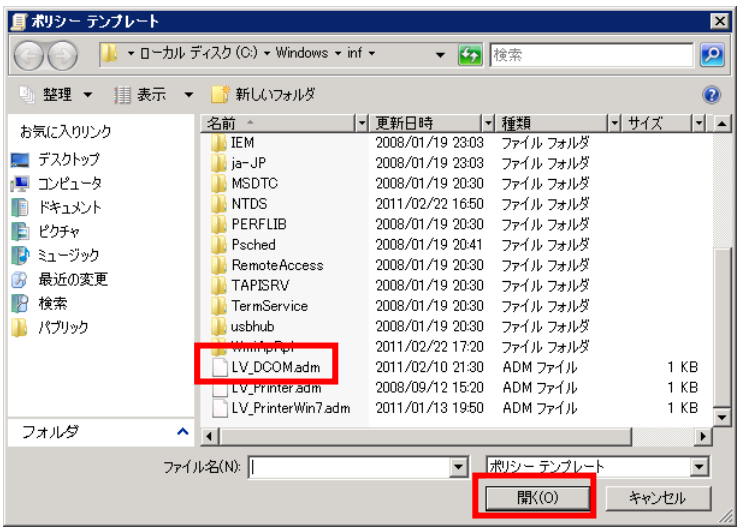
「管理用テンプレート」を右クリック、「テンプレートの追加と削除」をクリックします。



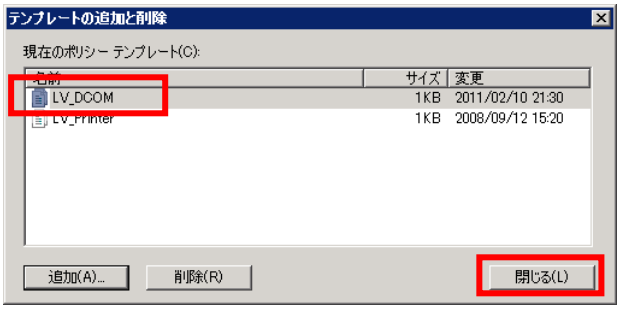

「追加」をクリックします。



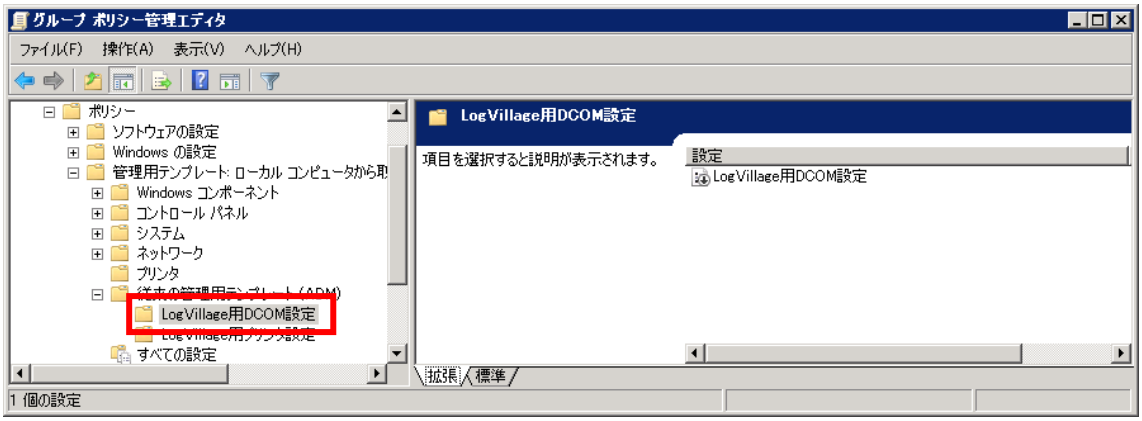

「LV_DCOM.adm」をクリック後、「開く」をクリックします。



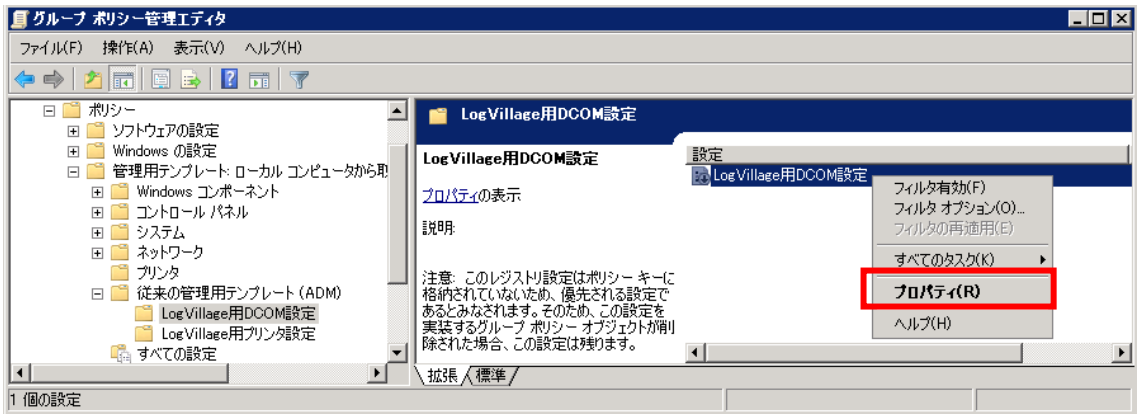
「LV_DCOM」が一覧に表示された事を確認し、「閉じる」をクリックします。



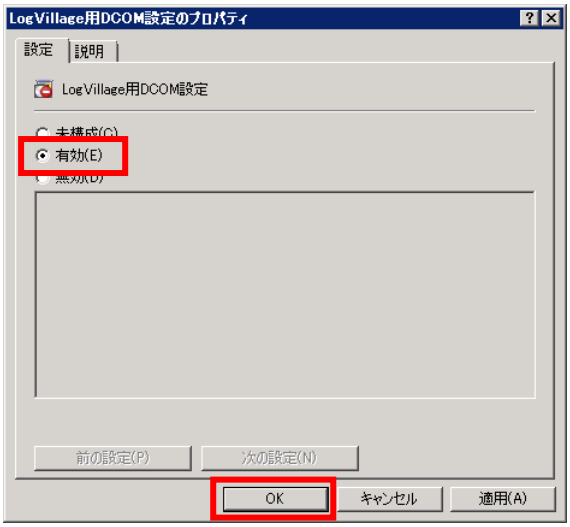

⑤　「LogVillage 用 DCOM 設定」を有効に変更します。
「管理用テンプレート」→「従来の管理テンプレート（ADM）」→「LogVillage 用 DCOM 設定」をクリックします。




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



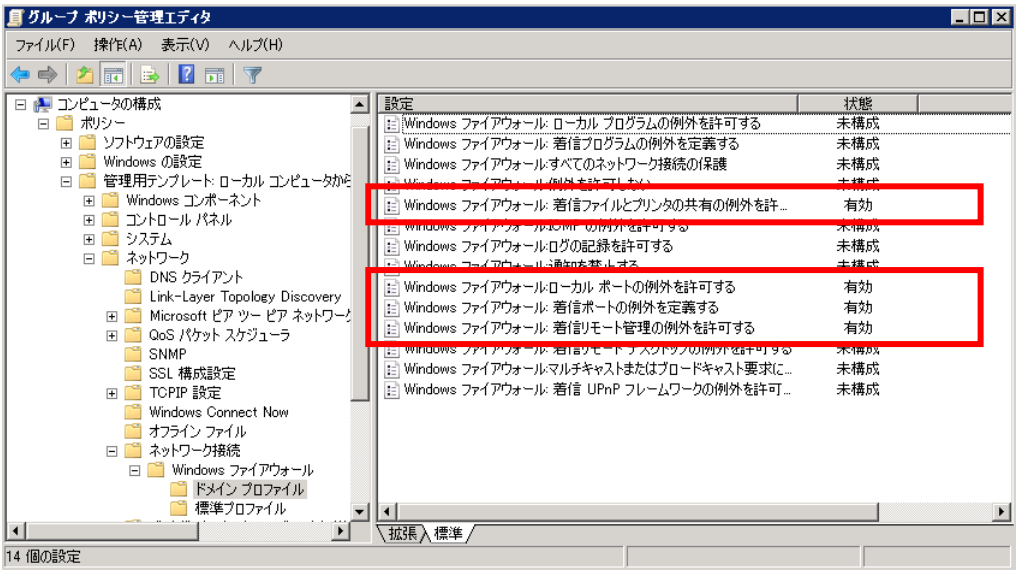
「有効」をクリック後、「OK」をクリックします。



## 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。

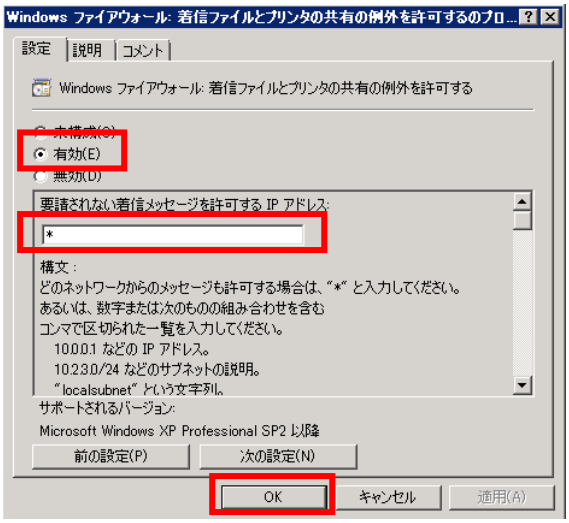


② 「Windows ファイアウォール：着信ファイルとプリンタの共有の例外を許可する」を設定します。

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。

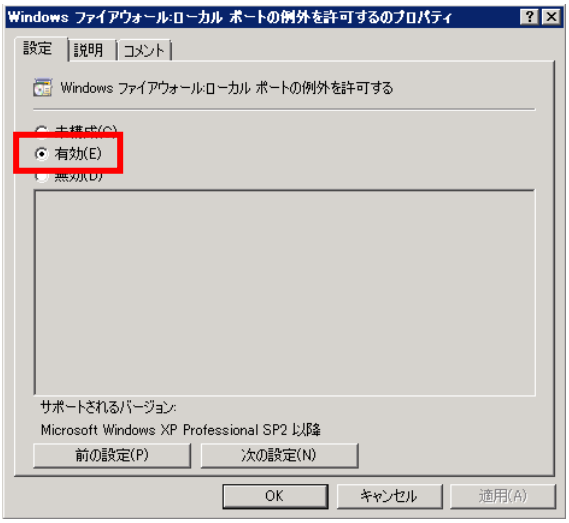



※各管理対象 PC 上で、本設定をポーリングサーバーに対してのみ許可する場合は、＊ をポーリングサーバーのアドレスに変更します。（スコープ設定）

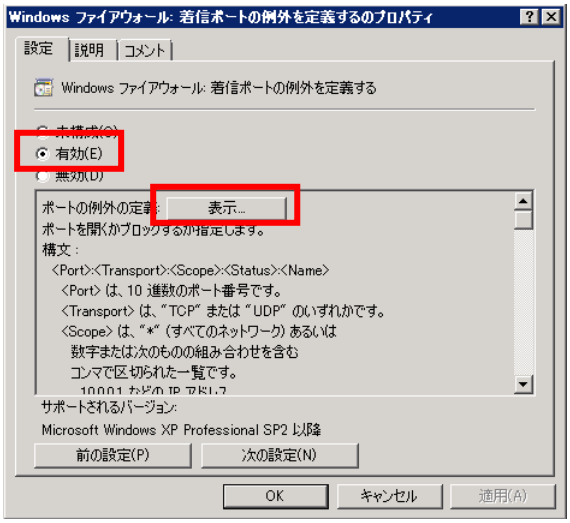
③ 「Windows ファイアウォール：ローカルポートの例外を許可する」を設定します。

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。

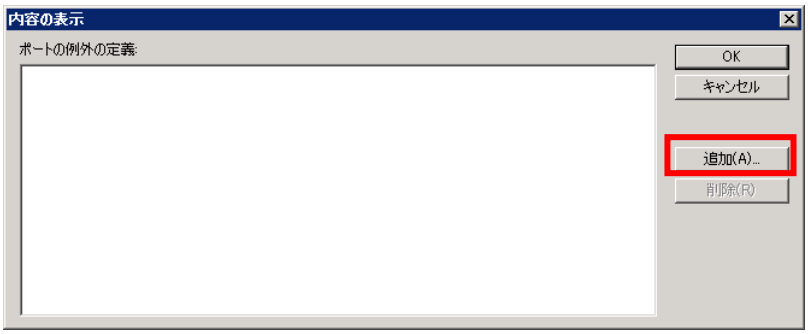
「有効」をクリック後、「OK」をクリックします。



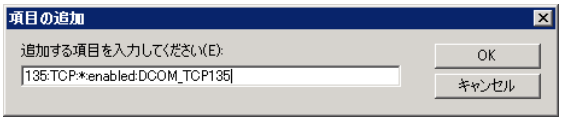
④　「Windows ファイアウォール：着信ポートの例外を定義する」を設定します。
設定名「Windows ファイアウォール：着信ポートの例外を定義する」をダブルクリックします。
「有効」をクリックし、「ポートの例外定義」の「表示」をクリックします。




「追加」をクリックします。

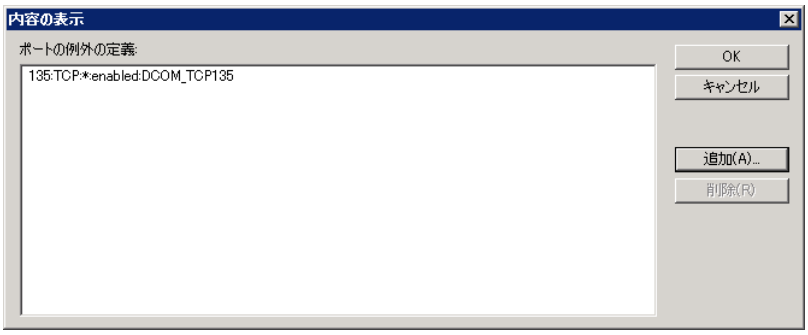


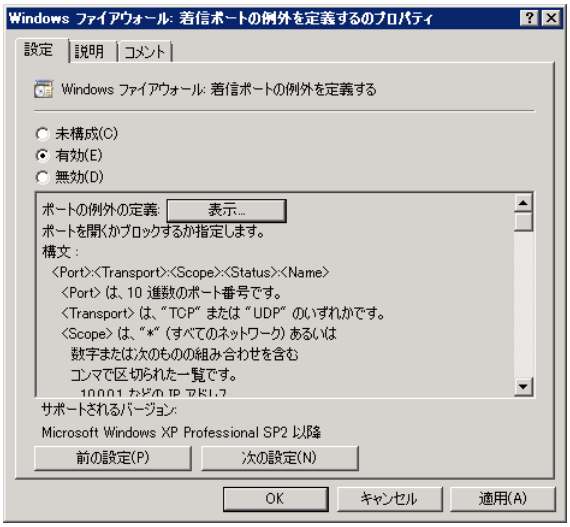

「追加する項目を入力してください」に「135:TCP:*:enabled:DCOM_TCP135」を入力し「OK」をクリックします。




※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。



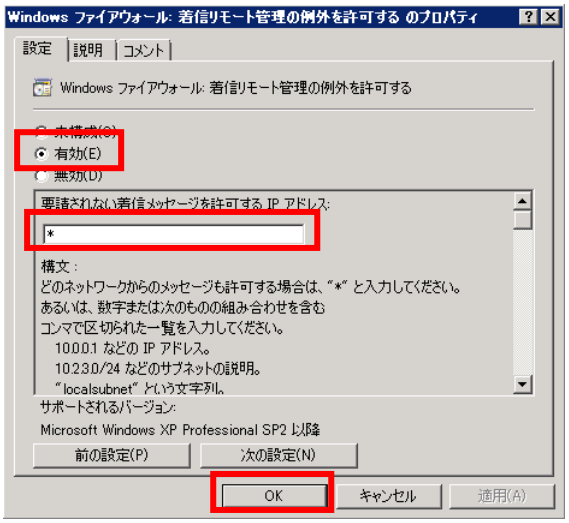



⑤　「Windows ファイアウォール：着信リモート管理の例外を許可する」を設定します。

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。

## 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

・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

## 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

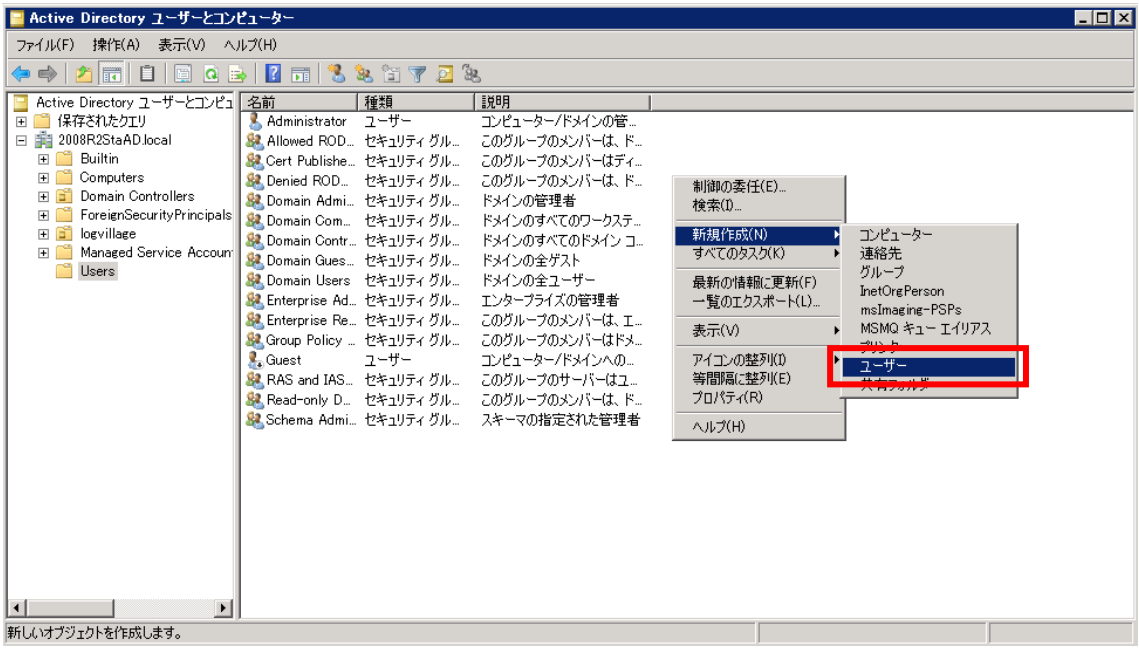
Active Directory 上で Domain Admins 権限を持ったユーザーの作成と LogVillage への登録について説明します。

・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

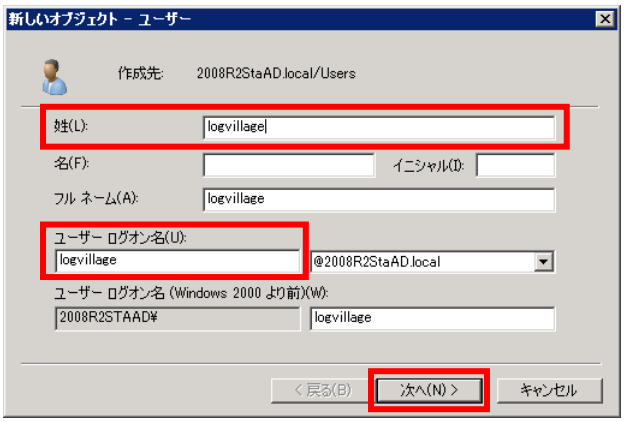
**・ユーザー作成**

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。

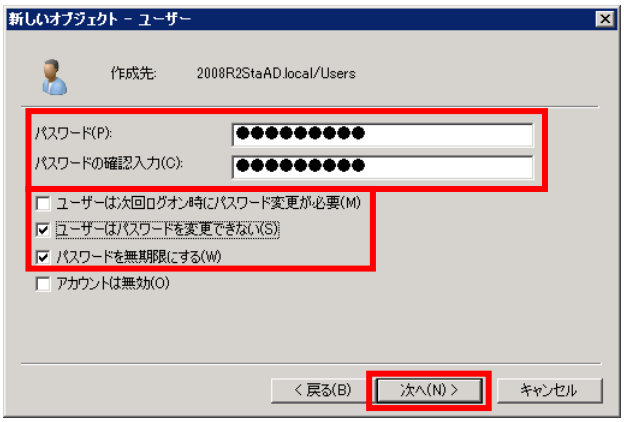
② 新規「ユーザー」を作成します。
「Users」を選択し、空白部分で右クリック「新規作成」→「ユーザー」をクリックします。



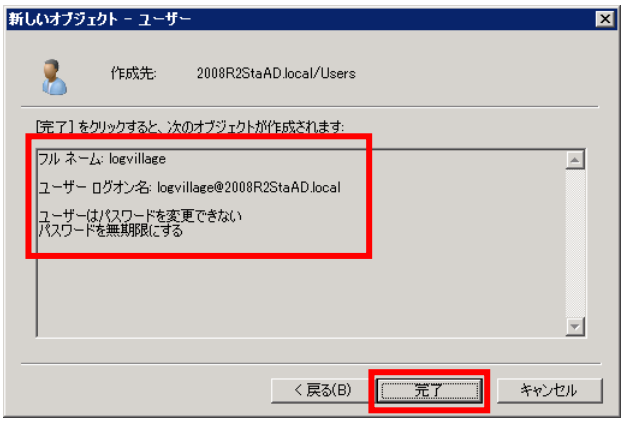
「姓」と「ユーザー ログオン名」に任意のユーザー名を入力し「次へ」をクリックします。
例：logvillage




「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。



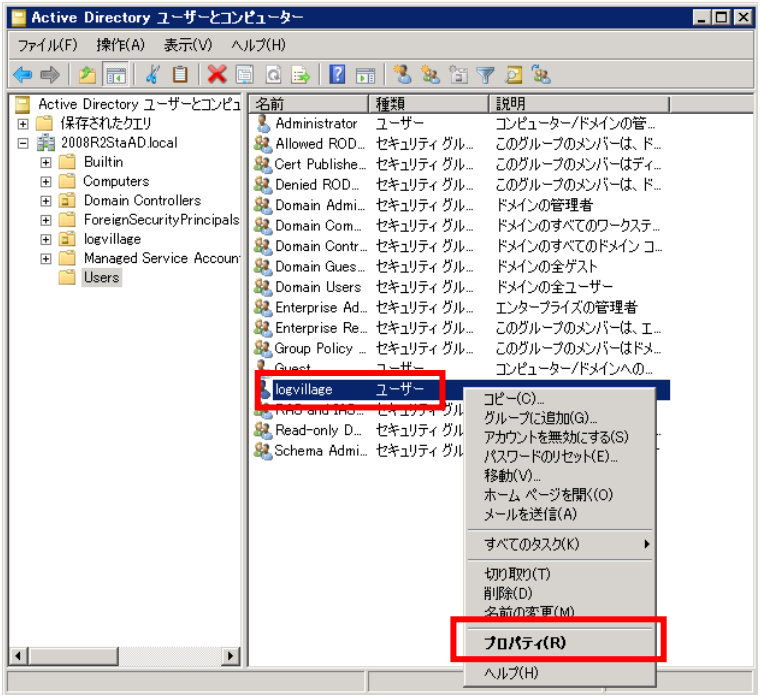
設定に間違いが無い事を確認後「完了」ボタンをクリックします。



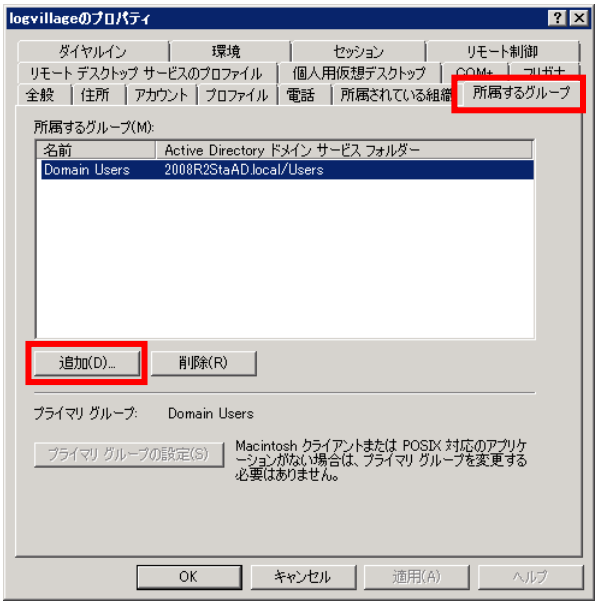

③ 権限を付与します。

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。

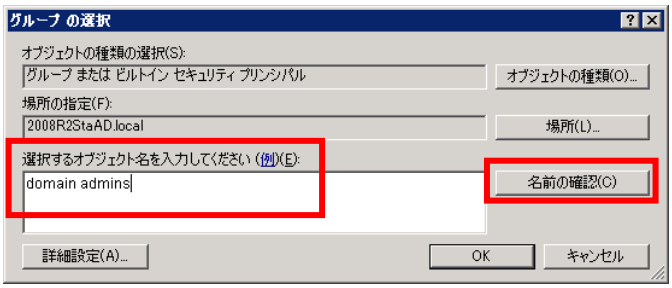
例：logvillage



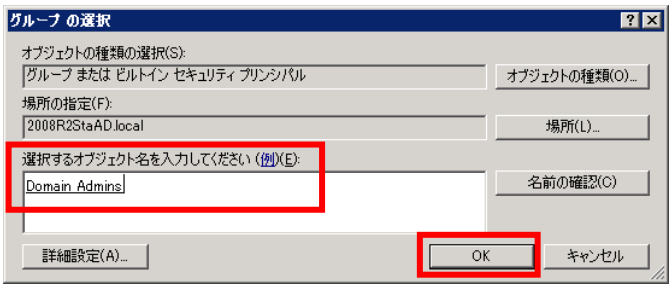
「所属するグループ」タブを開き、「追加」をクリックします。




「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。

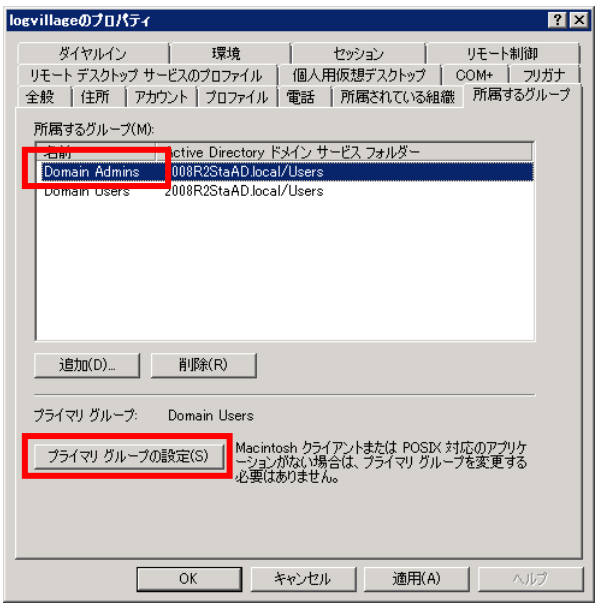



「domain admins」に下線が表示された事を確認後、「OK」をクリックします。

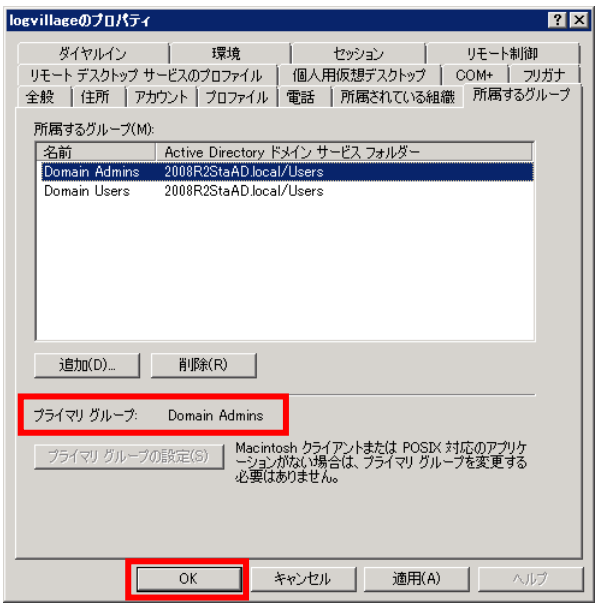


④ プライマリグループを変更します。

「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。




「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。

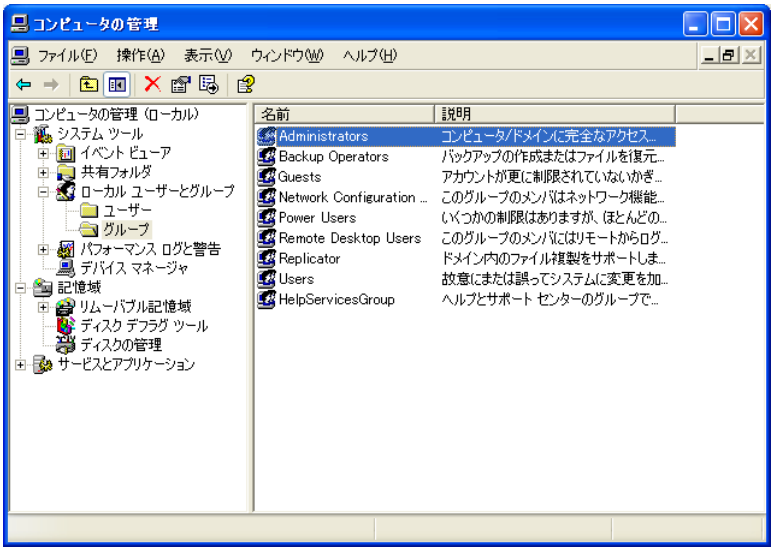


**・管理対象 PC 上で、設定反映を確認する方法**

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。

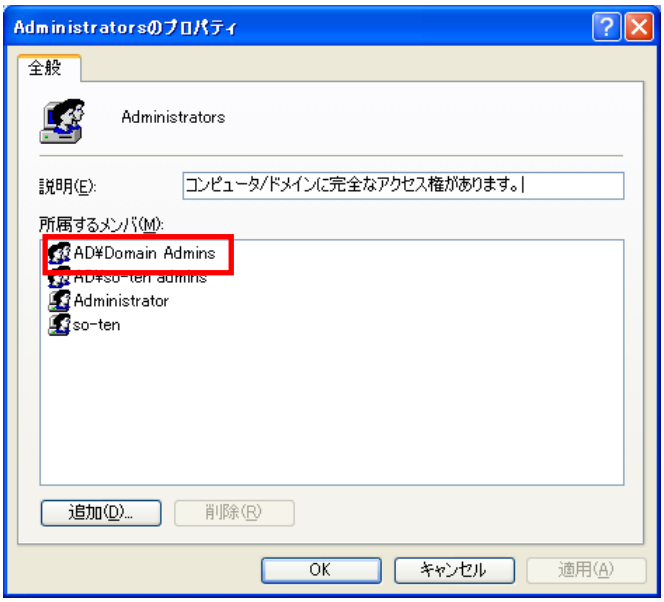
「コンピュータの管理（ローカル）」→「ローカル ユーザーとグループ」→「グループ」をクリックします。




② 「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。

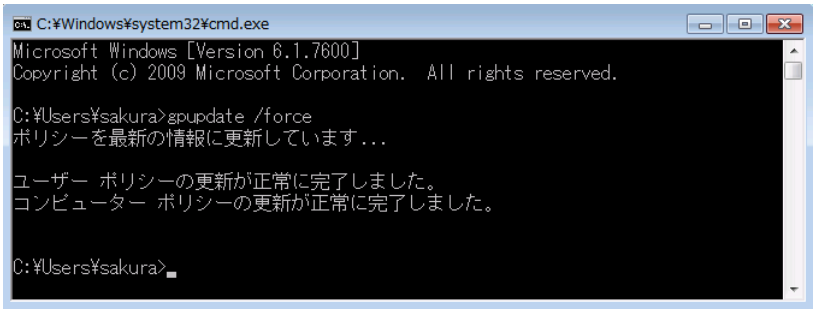
コマンドプロンプトを起動します。

"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。

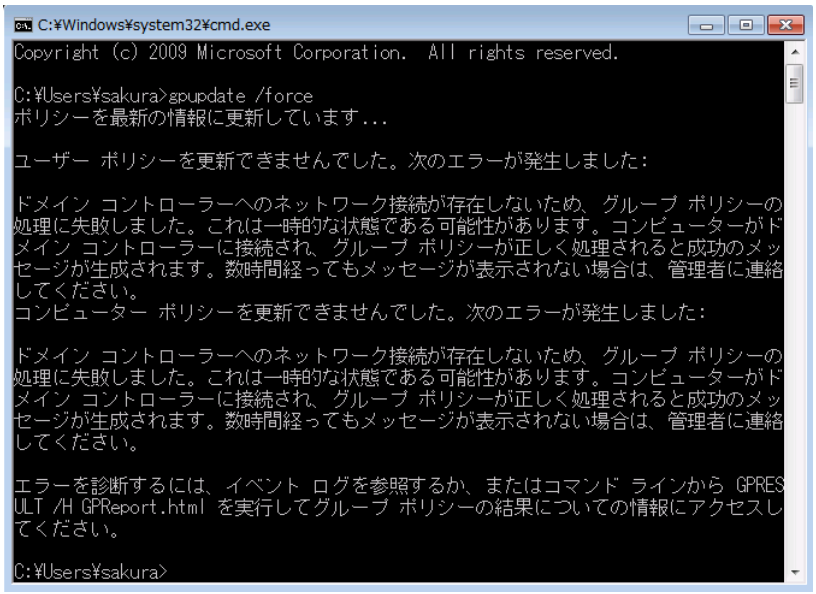
「gpupdate /force」を入力し、実行します。

※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」

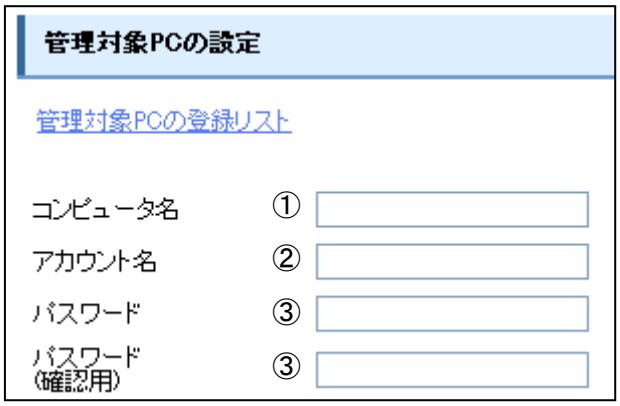
AD.local のユーザー「logvillage」

「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）



## 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**

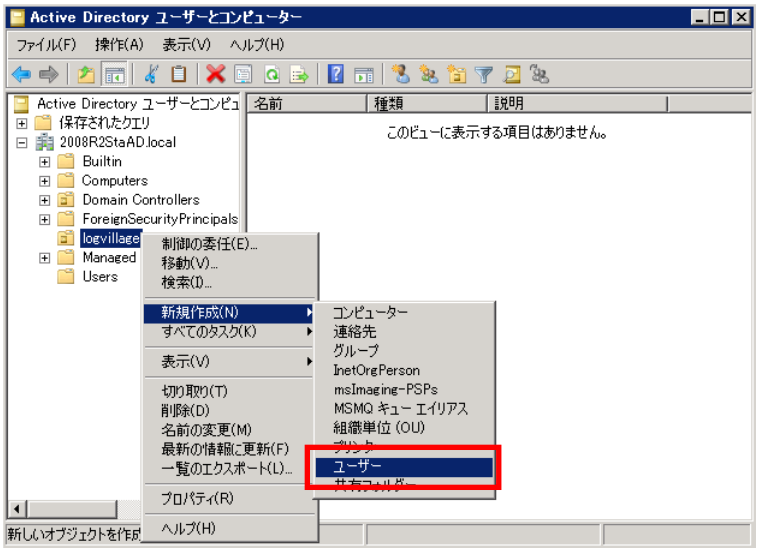
① 「Active Directory ユーザーとコンピュータ」起動します。

"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。

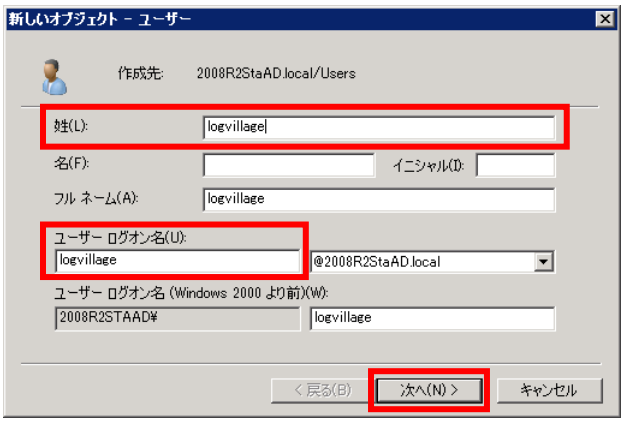
② 新規「ユーザー」を作成します。

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。

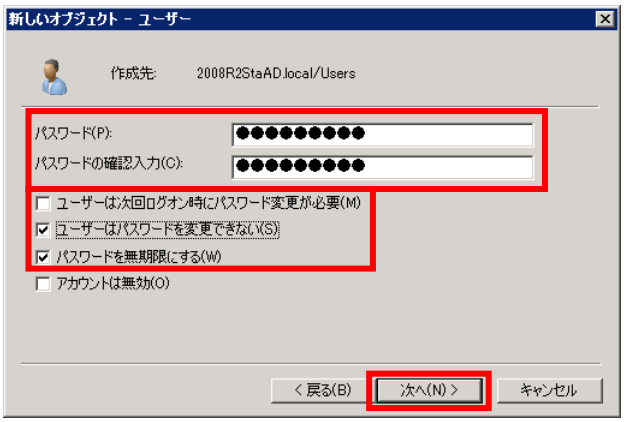
例：OU 名：logvillage



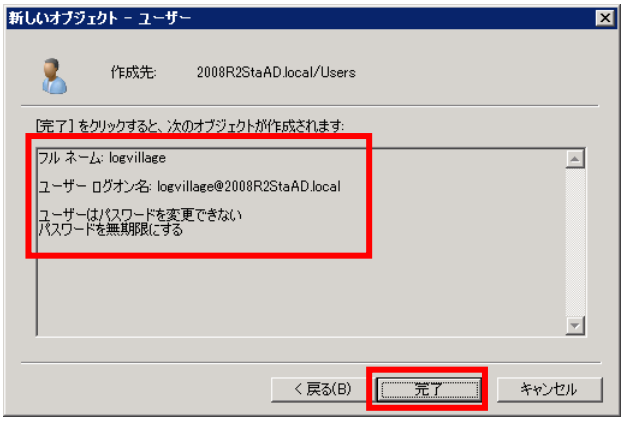
「姓」と「ユーザー ログオン名」に任意のユーザー名を入力し「次へ」をクリックします。
例：logvillage




「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。

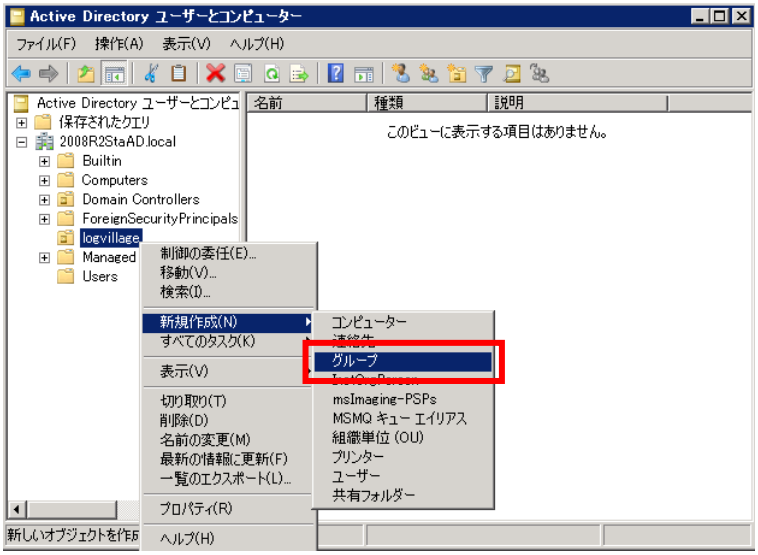


設定に間違いが無い事を確認後「完了」ボタンをクリックします。




③ 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。



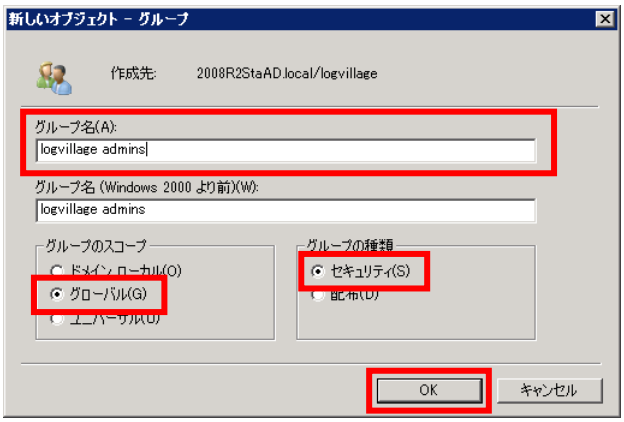
グループ名を入力します。

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。

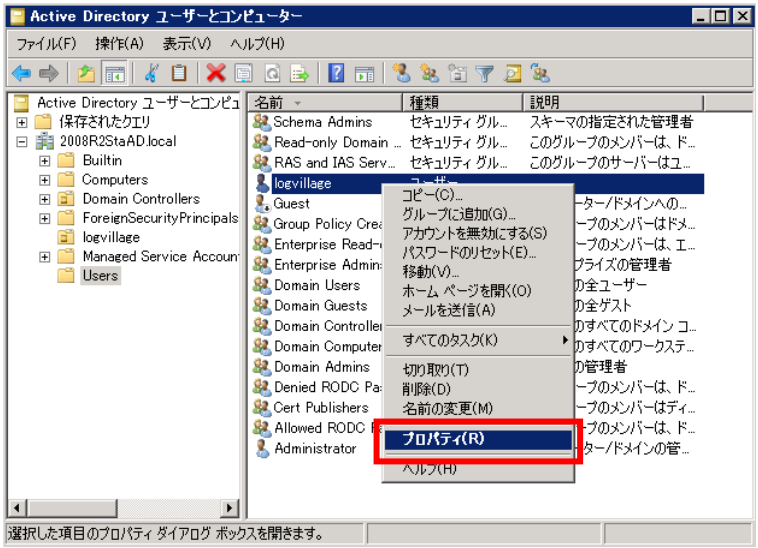
「OK」をクリックします。



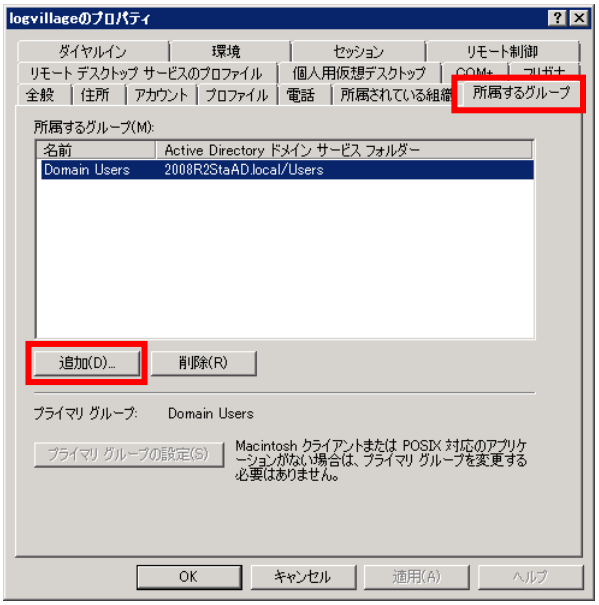

④ 権限を付与します。

「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。

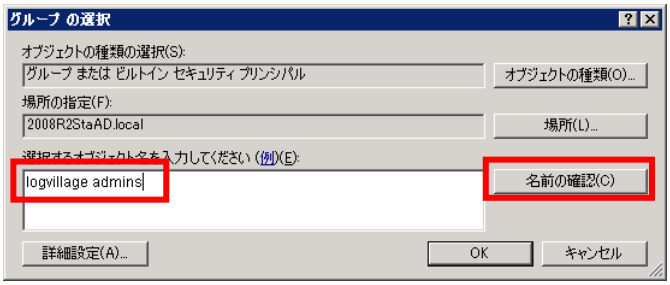
例：logvillage



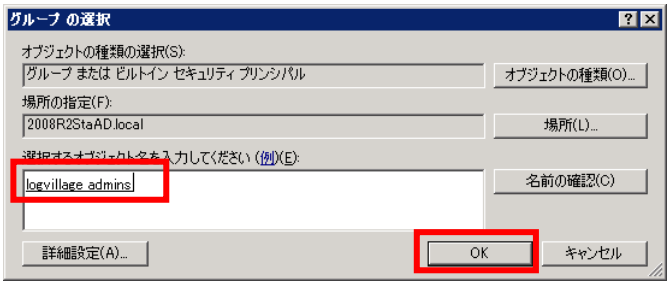
「所属するグループ」タブを開き、「追加」をクリックします。




「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。

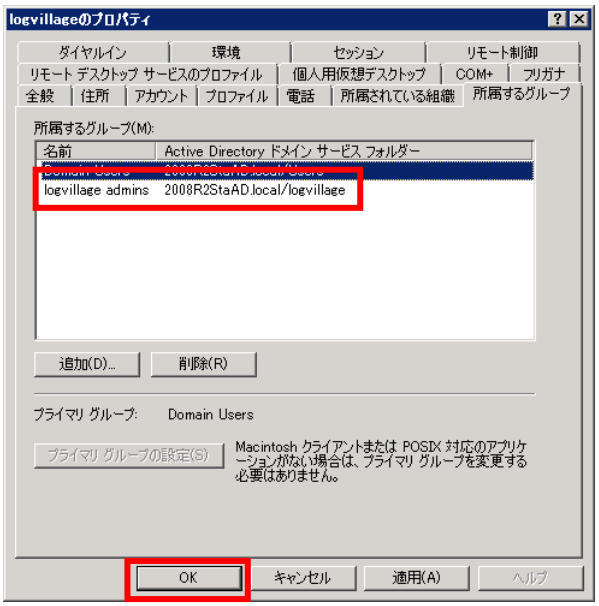



「domain admins」に下線が表示された事を確認後、「OK」をクリックします。




（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。



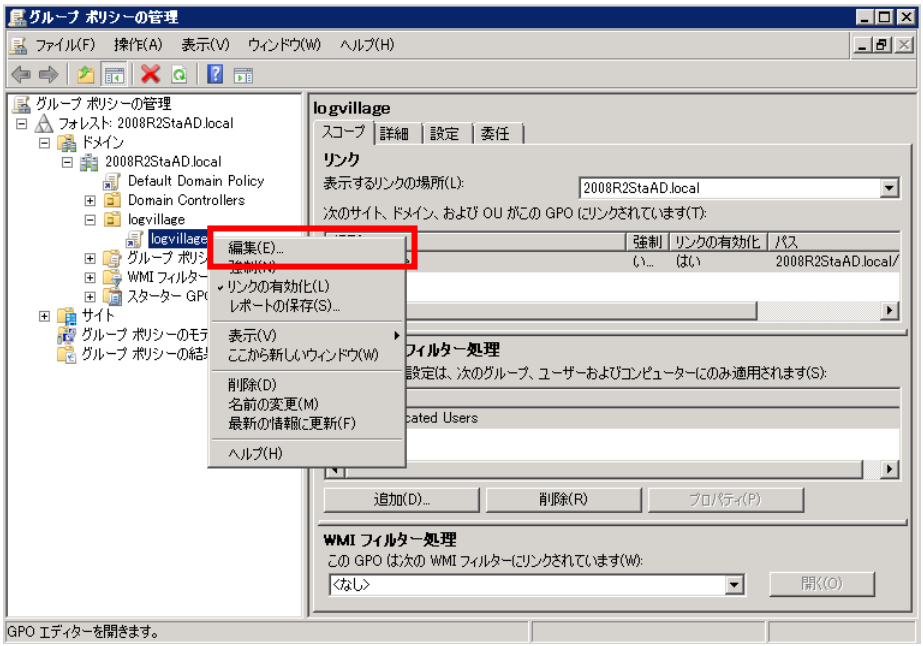

⑤ グループポリシーを編集します。

"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。

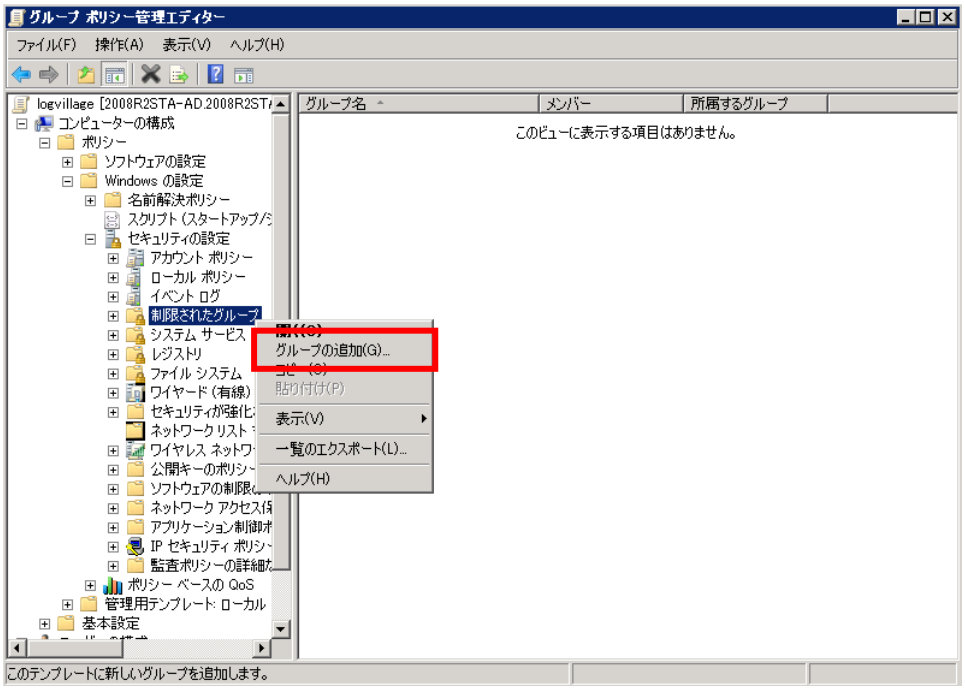
変更するポリシーを右クリックし、「編集」をクリックします。

例：OU 名：logvillage

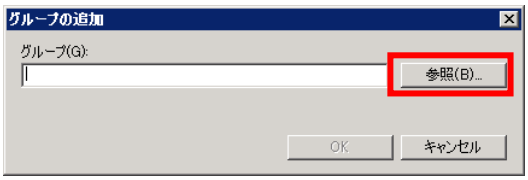


「コンピュータの構成」→「ポリシー」→「Windows の設定」→「セキュリティの設定」→「制限したグループ」を選択します。

「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。



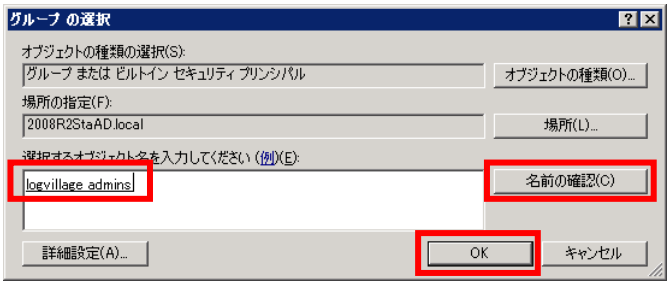

「参照」をクリックします。




作成したセキュリティグループ名を入力します。

例：logvillage admins

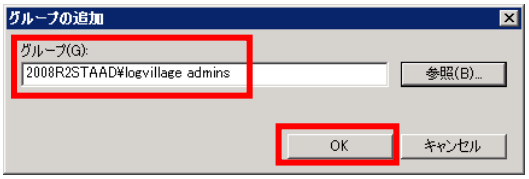
「名前の確認」をクリックし、入力文字列に下線が付与される事後、「OK」をクリックします。



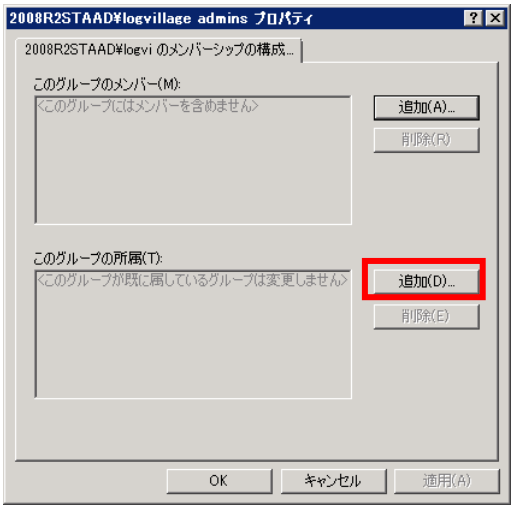

（下線が追加されない場合、セキュリティグループの指定に問題があります。入力文字列の確認、およびセキュリティグループが正しく作成されているかを確認してください）

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」

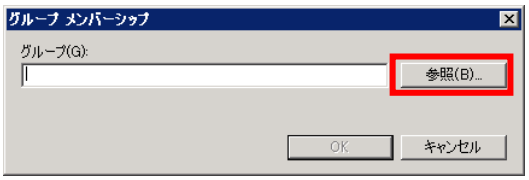
をクリックします。



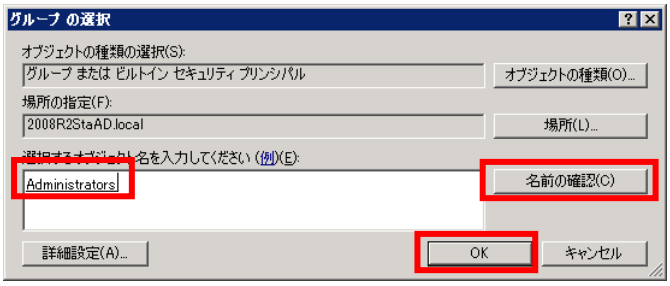

「追加」をクリックします。




「参照」をクリックします。

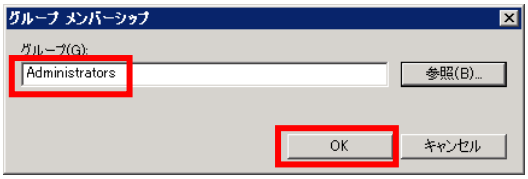



「Administrators」と入力します。
「名前の確認」を選択し、入力文字列に下線が付与される事を確認後、「OK」をクリックします。

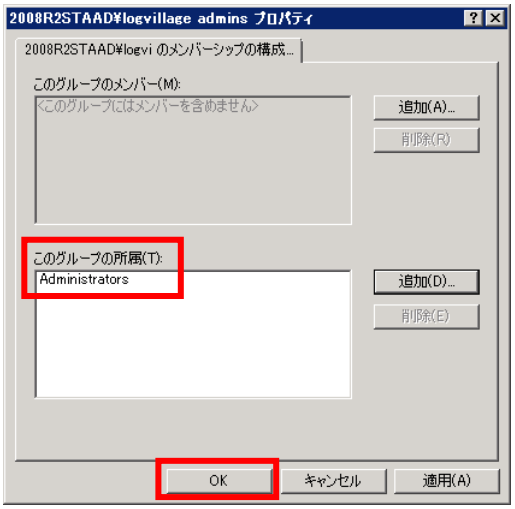



（下線が追加されない場合、セキュリティグループの指定に問題があります。入力文字列を確認してください）

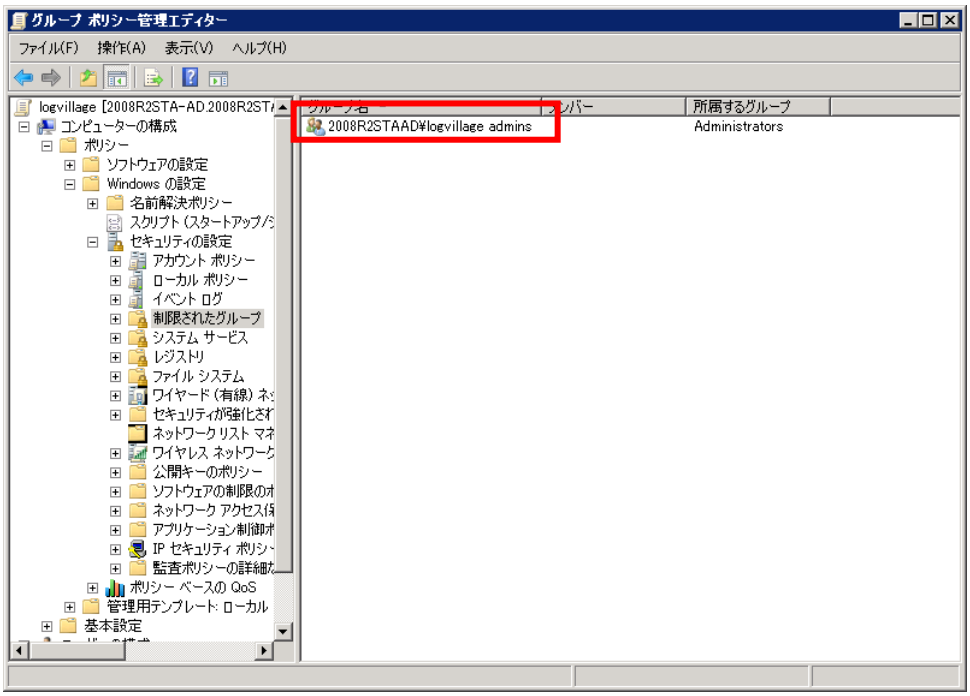
グループに「Administrators」が表示されることを確認し、「OK」クリックします。




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

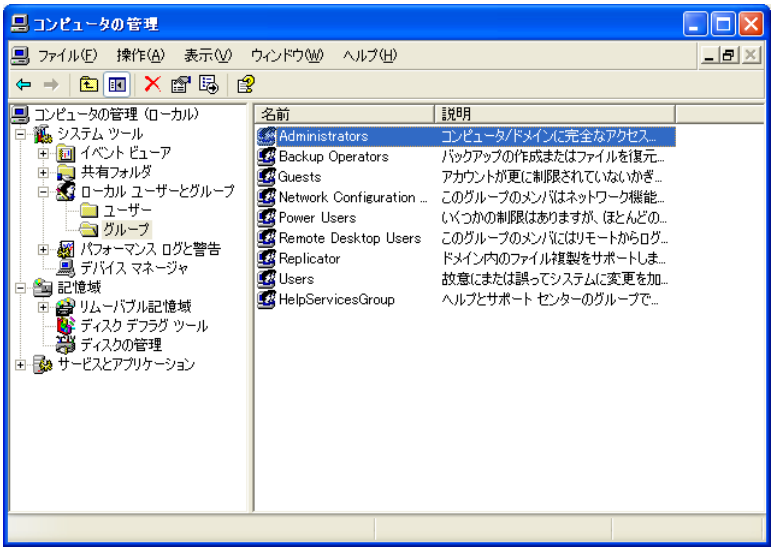


**・管理対象 PC 上で、設定反映を確認する方法**

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。

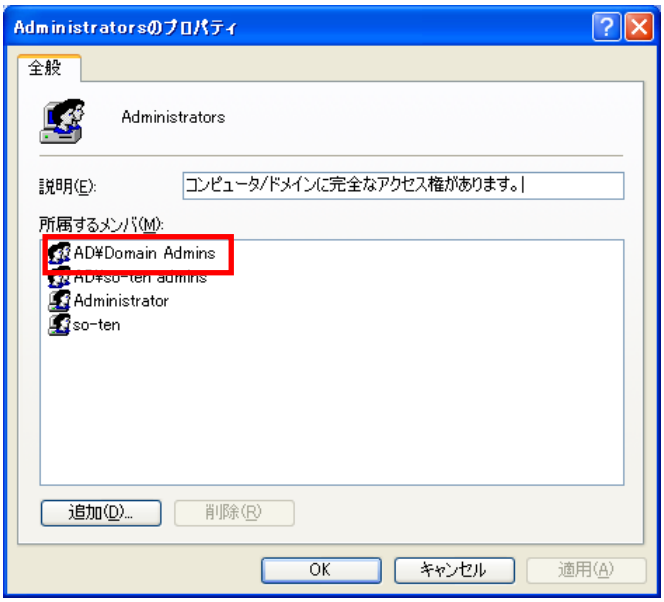
「コンピュータの管理（ローカル）」→「ローカル ユーザーとグループ」→「グループ」をクリックします。




② 「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。

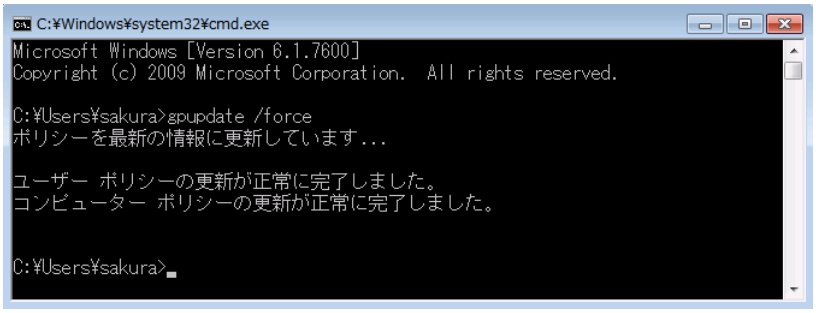
コマンドプロンプトを起動します。

"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。

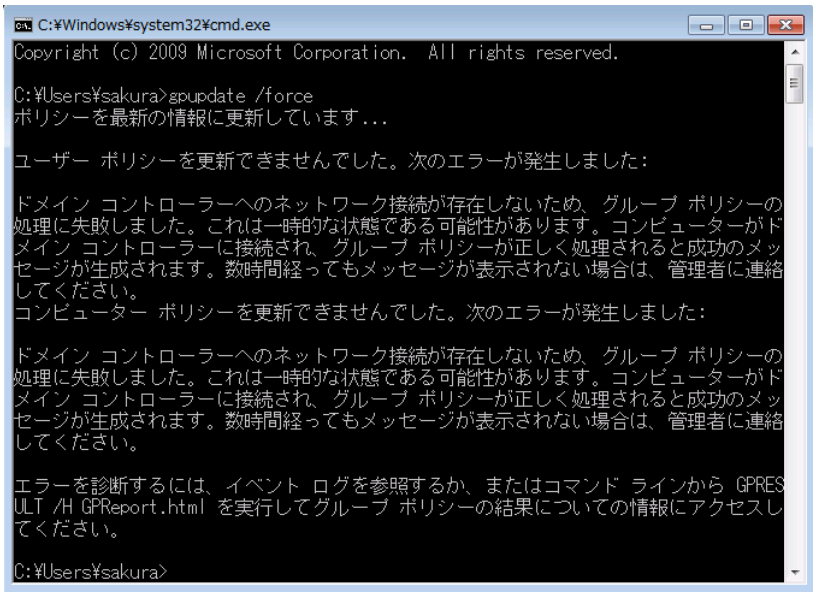
「gpupdate /force」を入力し、実行します。

※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」

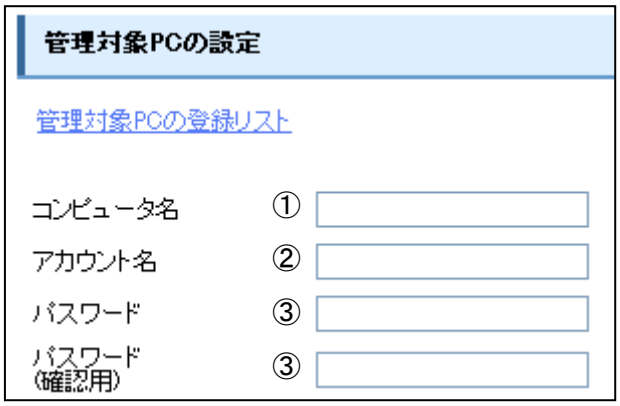
AD.local のユーザー「logvillage」

「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）



## 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。

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。

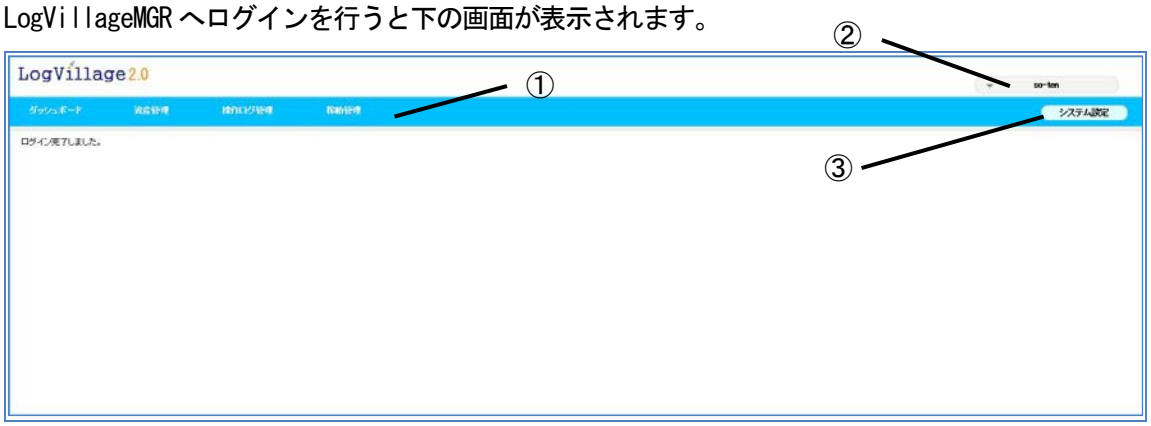
新しく設定したユーザーID とパスワードを忘れた場合、LogVillage の再インストールが必要となります。ご注意ください。

・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。**

## 8-2. 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。




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。

② 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。

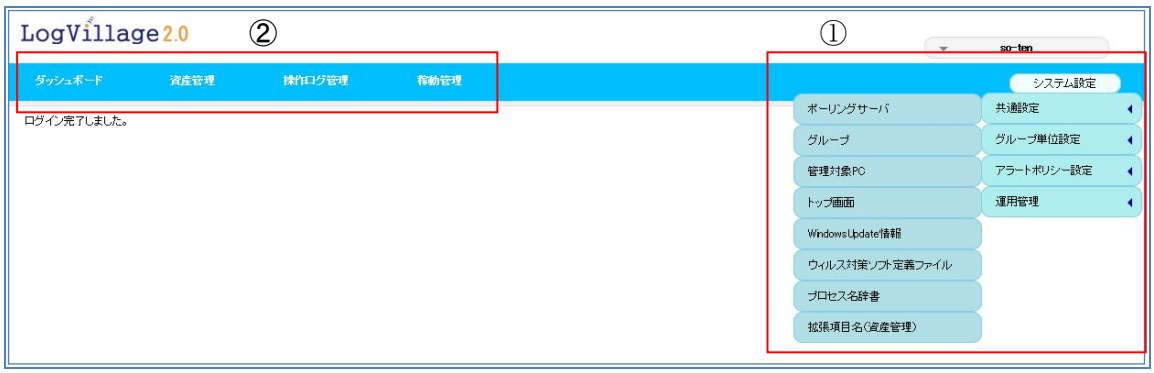
但し、ログインユーザーにシステム設定権限が付与されていない場合は表示されません。

※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




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 OS

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

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。

② ダウンロードページにアクセスします。

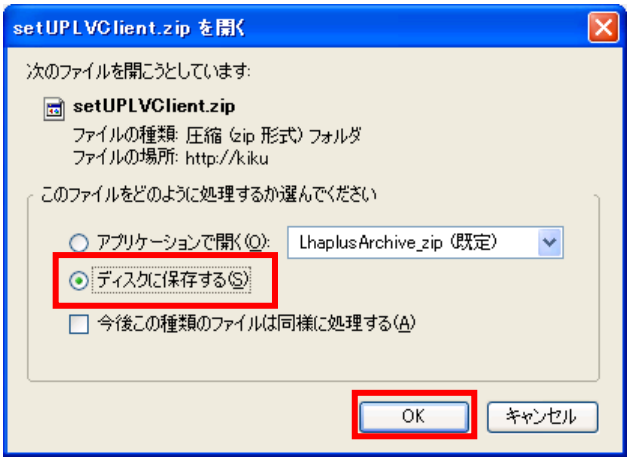
Internet Explorer を起動し、ダウンロードページを開きます。

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。

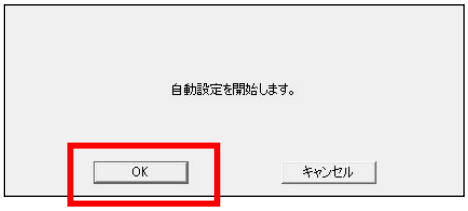
「ディスクに保存する」にチェックが入っている事を確認後「OK」をクリックします。

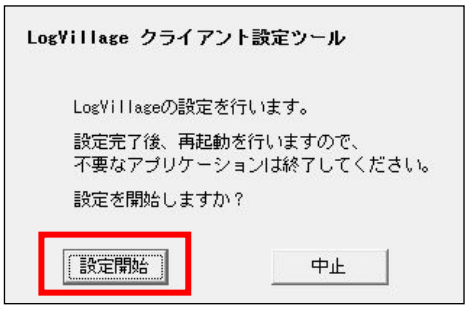


⑤ 保存したファイルを展開します。
保存したファイル「setUPLVClient.zip」を展開します。

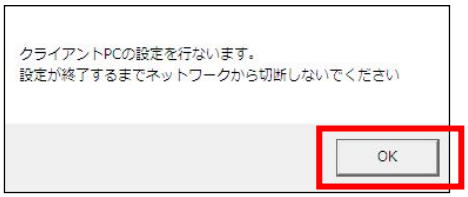
⑥ ファイルを実行します。
「LVAutoSet_WindowsVista-10.exe」をダブルクリック（実行）します。

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。

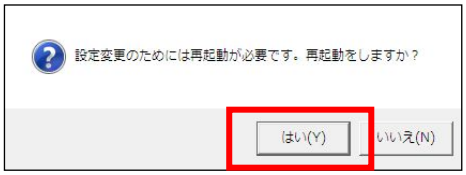


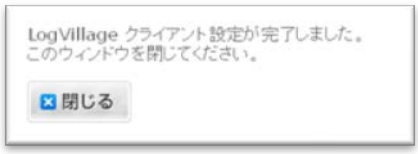

⑧ 「OK」をクリックします。




⑨ OS を再起動します。




⑩ 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。

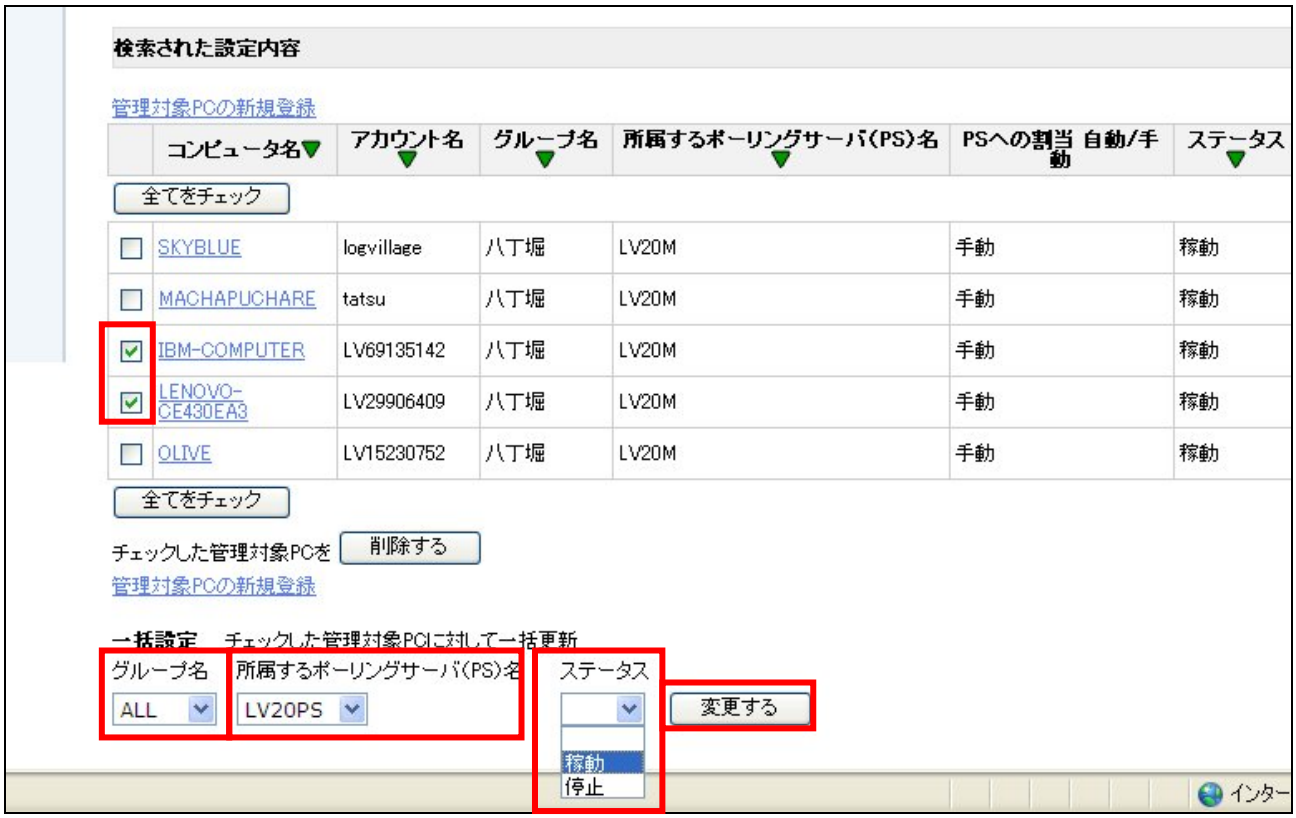

② 設定を変更します。

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。



## 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¥SO-TEN¥LogVillage となります。）

ファイル名の例： LV-PS-LOG201001230182024.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 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。

### 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. 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　：support@so-ten.co.jp
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　　＞＞

**■LogVillageMGR の再起動**

① 通知領域のアイコンを停止します。

通知領域の「LV_TaskTray(M)」アイコンを右クリックし、「終了」を押下します。

② サービスを停止します。

"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」から、以下の順番にサービスを停止します。

Apache2
LV_M_MonitorSrv
LV_ManagerServer
Embedded Database - LOGVILLAGE

③ サービスを開始します。

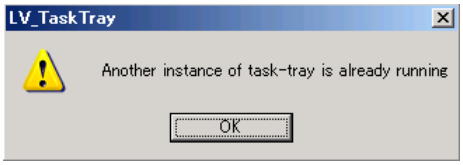
以下の順番にサービスを開始します。

Embedded Database - LOGVILLAGE
LV_M_MonitorSrv

「LV_M_MonitorSrv」起動後、「LV_ManagerServer」と「Apache2」が開始される事を確認します。

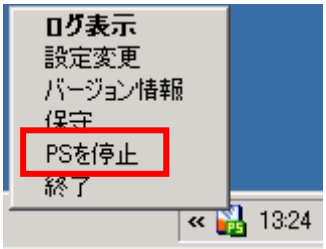
■LogVillagePS の終了と再起動

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」を起動します。
※起動中の場合、以下のメッセージが表示されます。
OK でダイアログを閉じてください。

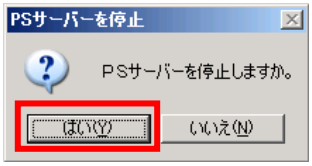



② タスクトレイ アイコンを右クリックします。

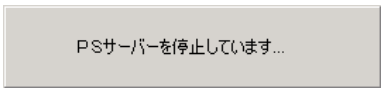
③ 「PS を停止」をクリックします。



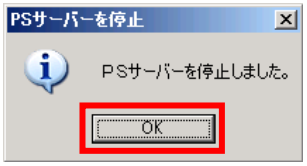

④ 「はい」をクリックします。




上図が消えるまで待ちます




⑤ OK」をクリックします。




※再起動する場合は「サービス」から「LV_P_MonitorSrv」を起動してください。

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/