NetCrunch は追加エージェントをインストールすることなく、Microsoft Windows のシステムを監視することができます。しかし、セキュリティルールが厳格なため、初期設定のみでリモート監視が可能となるのかは、ユーザーの Windows 環境に依存します。

## 監視サーバー

NetCrunch サーバーは、Windows Server 2016 以降にインストールすることができます。ユーザーが Active Directory 環境でほとんどのサーバーを管理している場合、Active Directory ドメインに参加したマシンに、NetCrunch をインストールすることを推奨します。理由は、容易に設定することができるためです。

## 監視対象システム

### サーバー

サーバーでは一般的にファイアウォールが有効なため、リモート管理がブロックされています。まず、この項目を変更する必要があります。最も簡単な方法としては、Active Directory グループポリシーで管理する方法です。その他の方法を採用する場合、ユーザーは AdRem Software 社が用意するスクリプトを使用して、個々のサーバーを設定する必要があります。（Web サイトからダウンロード: https://www.adremsoft.com/download/SetWinForNC.zip）

### ワークステーション

ユーザーが対象のワークステーションを Active Directory で管理している場合、サーバーと同様に、監視設定する必要があります。（Active Directory グループポリシーの編集、もしくはスクリプトの実行）

ワークグループに所属しているワークステーションを監視する場合、Windows Vista 以降に追加された UAC（ユーザーアクセス制御）のために、設定が多少困難となっています。この機能により、ローカルアドミニストレーショングループから管理者権限を継承しているリモート接続を許可しません。この場合、ユーザーはローカルのビルトイン Administrator アカウントを利用する、もしくは新しいアカウントを作成し、手動で必要な権限をこの新規アカウントに割り当てるなどの方法を取ることができます。

# 設定方法の概要

1. **アクセス権限の設定**
   NetCrunch では **DCOM**、**WMI**（root\cimV2）と（Read Access）、レジストリキー（HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib）へのアクセス権限を持つユーザーアカウントが必要となります。最も簡単な方法は、ローカル Administrators グループへ使用するユーザーを追加することです。

2. **ファイアウォール設定**
   ファイアウォールルールとして、RPC、パフォーマンスモニタ、名前付きパイプ、WMI のトラフィックを許可する必要があります。

3. **PerfMon 監視の有効化**
   Remote Registry サービスはスタートアップの種類を自動として設定し、実行中でなければなりません。

4. **UAC のリモート制限を無効化**
   UAC（ユーザーアクセス制御）のリモート制御をドメイン参加していないサーバー上で無効にする必要があります。以下のレジストリキーの値の変更が必要となります。以下のレジストリキーの値を 1 に変更する必要があります。設定変更後、コンピュータの再起動が必要になります。もしレジストリキーに LocalAccountTokenFilterPolicy キーが存在しない場合は、右側のウィンドウを右クリックし、「新規」→「DWORD」を選択します。次に LocalAccountTokenFilterPolicy という名前を入力し、値を 1 に設定します。

   KEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy

## ACTIVE DIRECTORY ドメインの設定方法

この手順は *Active Directory のユーザー、コンピュータおよびグループポリシー管理アドミニストレーションツール* の知識が必要となります。

もしユーザーが Active Directory を用いてほとんどのサーバーを管理している場合、一番良い方法は Active Directory ドメインに参加しているサーバー上に NetCrunch をインストールし、監視専用のアカウントを作成することです。**この場合、NetCrunch のインストールを中断し、まず Active Directory の設定をする必要があります。**設定の変更が全てのサーバーに反映された後、NetCrunch のインストールを再スタートしてください。設定の反映には**約 2 時間程度**必要になります。

この方法により、NetCrunch は Active Directory に参加している全てのサーバーの検出と監視設定を自動的に行うことが出来ます。他のドメインやワークグループのサーバーについては、別の設定が必要になります。（設定方法に関しては独立した Windows サーバーの項を参照ください。）

## アクセス権限の設定

### STEP 1 – 監視専用ユーザーの作成

NetCrunch サーバーで使用する監視専用ユーザーを Active Directory ユーザーアカウント（例：nc-mon-user）として作成します。NetCrunch のインストール中、このユーザー認証を求められるでしょう。

### STEP 2 – ユーザーの権限を設定

NetCrunch サーバーがインストールされているサーバーを含む全ての監視対象 Windows マシンを監視するためには、ユーザーアカウントは管理者権限が必要となります。設定方法としては、Active Directory 構成およびお客様のニーズに依存して、2 種類の方法があります:

#### 監視対象の全てのマシンが単一のドメインに参加している場合

Active Directory の定義済み Domain Admins グループにユーザーアカウントを追加する。

#### 監視対象のマシンが一部のサブセットであるか、複数のドメインがある場合

各監視対象の Windows マシン上でローカル Administrators グループを変更するために、グループポリシーを使用します。

a) Monitoring Users という名前の Active Directory グループを作成します。そのグループに作成したユーザーアカウント（例：nc-mon-user）を追加します。

> グローバルグループはフォレスト内のドメインにあるリソースへの許可を設定するために利用されるため、ドメインフォレスト、デフォルト Active Directory スコープ(グローバル)はこのグループに対して、十分な権限が必要です。

b) グループポリシーオブジェクト（GPO）を新しく作成し、名前（例えば Local Administrators group membership for NetCrunch ）を付けます。

c) Monitoring Users グループメンバーシップのルールを下記の手順で作成します。

手順：

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 → 制限されたグループ

ローカル Administrators グループへ Monitoring Users を「このグループは下記のメンバーです」のセクションを利用して追加します。

d) お客様の Active Directory ドメイン上にある適切な組織ユニット（OU）に、Local Administrators group membership for NetCrunch を GPO にリンクさせます。

## ファイアウォールの設定方法

1. 新しいグループポリシーオブジェクトを作成して、名前を付けます。例えば Windows Firewall rules for monitoring by NetCrunch などです。

2. 監視したい Windows マシンのビルトインファイアウォールタイプ両方を設定するために、GPO に 2 つの異なるブランチを使用します:

   a. **XP と Server 2003 R2 の場合**

   手順:

   コンピュータの構成→ 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 プロフィール

   以下を”有効”に設定します:

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

   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

   b. **Windows 7, 8, 10,11, Server 2008/2008 R2, Server 2012/2012 R2, Server 2016, Server 2019,Server 2022 の場合**

   手順:

   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→ セキュリティが強化された Windows ファイアウォール

   受信の規則に事前定義された規則のリストから以下の規則を追加:

   ファイルとプリンタの共有

リモート管理

デフォルトでは、Windows 標準のファイアウォールは送信トラフィックをブロックしません。もしデフォルトから変更を加えている場合、送信の規則の事前定義済みリストから同名のルールを追加する必要があります。

3. Windows Firewall rules for monitoring by NetCrunch GPO を Active Directory ドメイン上の適切な組織ユニット（OU）にリンクします。

セキュリティを強化する方法として、NetCrunch サーバーのアドレスのみ、リモート管理ルールの許可アドレスに指定することを推奨します。

## PERFMON 監視の有効化

1. 新しいグループポリシーオブジェクトを作成し、名前を付けます。例えば、Windows services for monitoring by NetCrunch です。

2. Remote Registry サービスを設定します。
   手順:

   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

   Remote Registry サービスの Windows スタートアップの種類を 自動 に設定します。

3. Windows services for monitoring by NetCrunch GPO を Active Directory ドメイン上の適切な組織ユニット（OU）にリンクさせます。

ポリシーを更新した直後に、このサービスは全てのコンピュータ上で即座にスタートします。

## 独立した WINDOWS サーバーの設定

全てのコマンドは管理者用コマンドプロンプトから実行する必要があります。

完全なスクリプトは下記 WEB サイトからダウンロード可能です。:

http://www.adremsoft.com/download/SetWinForNC.zip

## アクセス権限の設定

以下のコマンドをシェルコマンドより実行、nc-mon-user アカウントを作成し、ローカル Administrators グループに追加します。

```
net user /add nc-mon-user <Password>
net localgroup Administrators /add nc-mon-user
```

## ファイアウォールの設定

Windows Server 2003 と Server 2003 R2 の場合:

```
netsh firewall set service type=fileandprint scope=all profile=all
netsh firewall set service type=remoteadmin scope=all profile=all
```

Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019,Windows Server 2022 の場合, NetCrunch サーバーの IP アドレスにのみ有効なルールを作成することができます。

```
netsh advfirewall firewall add rule name="NC-Mon" dir=in action=allow remoteip="%IP%"
netsh advfirewall firewall add rule name="NC-Mon" dir=out action=allow remoteip="%IP%"
```

## PERFMON 監視の有効化

Remote Registry サービスのスタートアップを設定し、サービスを起動します。

```
WMIC SERVICE where name=”RemoteRegistry” call ChangeStartMode StartMode=Automatic
WMIC SERVICE where name=”RemoteRegistry” call StartService
```

## UAC リモート制御の無効化

Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019,Windows Server 2022 の場合、UAC の動作を修正します。

(http://support.microsoft.com/kb/951016)

```
WMIC /Namespace: \\Root\Default Class StdRegProv Call SetDWORDValue hDefKey="&H80000002"
sSubKeyName="SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
sValueName="LocalAccountTokenFilterPolicy" uValue=1
```

## NETCRUNCH が使用している WINDOWS テクノロジー

Windows テクノロジーは多層構造を持っており、それぞれの層が組み合わさっています。例えば、RPC は名前付きパイプの上で動作しており、Remote Registry は RPC を必要としています。WMI もまた、通信のために RPC を使用している DCOM を使用しています。全ての機能が適切なファイアウォールとセキュリティ設定を必要とします。NetCrunch で使用されているテクノロジーと必要な設定のリストを以下に記載します。

1. **RPC と 名前付きパイプ** – (ファイル共有の有効化とファイアウォールの設定が必要です。)
2. **Remote Registry** – (ファイアウォール設定と Remote Registry サービスの実行が必要です。)
3. **WMI と DCOM** – (ファイアウォール設定、DCOM と WMI のセキュリティ設定が必要です。)

本ドキュメントに記載した通り、監視で使用するユーザーがローカル Administrators グループのメンバーである場合は、設定方法はシンプルなものとなります。それは、監視のために最も単純なサーバーの設定方法となりますが、必ずしも完全に安全ではありません。もしセキュリティ上懸念がある場合、監視アカウントに必要な権限のみ割り当てることができます。