

ネットワーク アクセス保護の System Center 監視パック ガイド

Microsoft Corporation

発行日: 2012 年 6 月 28 日

このドキュメントに関するご意見、ご感想を mpgfeed@microsoft.com までお寄せください。フィードバックには監視パック ガイド名を明記してください。

「[管理パック カタログ](http://go.microsoft.com/fwlink/?LinkID=82105)」(<http://go.microsoft.com/fwlink/?LinkId=82105>) の監視パックのページでレビューを投稿して、監視パックのフィードバックをお寄せください。

著作権

このドキュメントは "現状のまま" 提供されます。このドキュメントに記載されている情報や見解 (URL 等のインターネット Web サイトに関する情報を含む) は、将来予告なしに変更することがあります。お客様は、本ソフトウェアの使用に関するリスクを負うものとします。

このドキュメントで使用される例は架空のものであり、説明のためだけに使用されます。実在するものとは一切関係ありません。

このドキュメントは、Microsoft 製品の知的財産権に関する法的な権利をお客さまに許諾するものではありません。内部的な参照目的に限り、このドキュメントを複製して使用することができます。内部的な参照目的に限り、このドキュメントを変更できます。

© 2012 Microsoft Corporation. All rights reserved.

Microsoft、Active Directory、Windows、および Windows Server は、米国 Microsoft Corporation および/またはその関連会社の商標です。

その他の商標はそれぞれの所有者に帰属します。

目次

[ネットワーク アクセス保護の System Center 監視パック ガイド 4](#_Toc338764932)

[ガイド履歴 4](#_Toc338764933)

[サポートしている構成 4](#_Toc338764934)

[この監視パック内のファイル 4](#_Toc338764935)

[監視パックの目的 5](#_Toc338764936)

[監視シナリオ 5](#_Toc338764937)

[ヘルスのロールアップ方法 6](#_Toc338764938)

[ネットワーク アクセス保護の監視パックの構成 7](#_Toc338764939)

[ベスト プラクティス: カスタマイズ用の管理パックの作成 7](#_Toc338764940)

[リンク 7](#_Toc338764941)

[付録: 監視パックの内容 8](#_Toc338764942)

[HRA の検出 8](#_Toc338764943)

[NPS の検出 10](#_Toc338764944)

[サービスにサーバー グループの検出が含まれます 11](#_Toc338764945)

# ネットワーク アクセス保護の System Center 監視パック ガイド

このガイドは、ネットワーク アクセス保護の監視パック Version 7.0.8560.0 に基づいて記述されています。

### ガイド履歴

| **リリース日** | **変更箇所** |
| --- | --- |
| 2012 年 10 月 | このガイドのオリジナル リリース |

### サポートしている構成

この監視パックには、System Center Operations Manager 2007 以降が必要です。専用の Operations Manager 管理グループは必要ありません。

以下の表は、ネットワーク アクセス保護の監視パックに対してサポートしている構成の詳細内容です。

|  |  |
| --- | --- |
| 構成 | サポート |
| ネットワーク アクセス保護 | Windows Server 2012 |
| エージェントレスの監視 | サポートしていません |
| 仮想環境 | サポートされています |

### この監視パック内のファイル

ネットワーク アクセス保護の監視パックには以下のファイルが含まれています。

• Microsoft.Windows.Server.NAP.mp

• Monitoring Pack for Network Access Protection.doc

# 監視パックの目的

ネットワーク アクセス保護 (NAP) の監視パックは、NAP 展開に不可欠な以下の監視ツールを提供します。インターネット インフォメーション サービス (IIS) サービス、NAP 証明書の発行に使用する証明機関 (CA)、証明書の有効期限と証明書のバインド、正常性登録機関 (HRA) によって使用される IIS アプリケーション プールを監視するスクリプト、およびネットワーク ポリシー サーバー (NPS) サービス。

このセクションの内容

• [監視シナリオ](#z91bd2be32ea34392aa6ca6acbff0a947)

• [ヘルスのロールアップ方法](#zb2b3af3015d3447f9bfd96dd48385e12)

この監視パックに含まれる検出、ルール、監視、ビュー、およびレポートの詳細については、「[付録: 監視パックの内容](#zfa5f0ba4791f4029b528b2fd8acd13d1)」を参照してください。

# 監視シナリオ

| **監視シナリオ** | **説明** | **関連するルールとモニター** |
| --- | --- | --- |
| IIS | NAP サーバーの IIS サービスの状態を監視します。IIS サービスの状態を次のように示します。サービスが応答しない場合は赤色、それ以外すべての場合は緑色です。 | Microsoft.Windows.Server.NAP.IISService |
| NPS | NAP サーバーの NPS サービスの状態を監視します。NPS サービスの状態を次のように示します。サービスが応答しない場合は赤色、それ以外すべての場合は緑色です。 | Microsoft.Windows.Server.NAP.NPSService |
| 証明書の有効期限 | SSL 証明書の有効期限を監視します。SSL 証明書の有効期限が 1 週間以内に切れるかどうかを示します。1 週間以内に切れる場合は黄色、それ以外すべての場合は緑色です。 | Microsoft.Windows.Server.NAP.SSLCertificateExpiry |
| Web バインド | IIS の SSL 証明書バインドを監視します。バインドが HTTPS を使用しているかどうかを示します。バインドが HTTPS を使用している場合は緑色で、バインドが HTTP を使用している場合は黄色です。 | Microsoft.Windows.Server.NAP.WebBindingMonitor |
| NAP RADIUS サーバーの可用性 | RADIUS プロキシ サーバー使用可能かどうかを監視します。RADIUS サーバーが使用できない場合は赤色、それ以外すべての場合は緑色です。 | Microsoft.Windows.Server.NAP.ProxyUnavailable |

# ヘルスのロールアップ方法

以下の図では、この監視パックでオブジェクトのヘルス状態をロールアップするしくみを示します。



# ネットワーク アクセス保護の監視パックの構成

このセクションでは、この監視パックの構成およびチューニングのガイドを提供します。

• [ベスト プラクティス: カスタマイズ用の管理パックの作成](#z2)

## ベスト プラクティス: カスタマイズ用の管理パックの作成

Operations Manager の既定では、上書きなどのすべてのカスタマイズは既定の管理パックに保存されます。ベスト プラクティスとして、代わりに、カスタマイズする保護された管理パックごとに、別の管理パックを作成することをお勧めします。

封印された管理パックのカスタマイズした設定を保存する目的で管理パックを作成する場合、たとえば、「NAP 2012 Customizations」 のように、カスタマイズする管理パックの名前に基づいて新しい管理パックの名前を付けると便利です。

封印された管理パックそれぞれについて、カスタマイズを格納するための新しい管理パックを作成することで、テスト環境のカスタマイズを運用環境にエクスポートすることが簡単になります。管理パックを削除する場合は、その前に依存するすべての管理パックを削除する必要があるため、管理パックの削除も容易になります。既定の管理パックにすべての管理パックのカスタマイズを保存していて、1 つの管理パックを削除する必要がある場合、最初に既定の管理パックを削除する必要があり、それにより他の管理パックへのカスタマイズも削除されてしまいます。

# リンク

以下のリンクでは、System Center 監視パックに関連付けた共通タスクに関する情報にアクセスできます。

• [管理パック ライフ サイクルの管理](http://go.microsoft.com/fwlink/?LinkId=211463) (<http://go.microsoft.com/fwlink/?LinkId=211463>)

• [Operations Manager 2007 で管理パックをインポートする方法](http://go.microsoft.com/fwlink/?LinkID=142351) (<http://go.microsoft.com/fwlink/?LinkID=142351>)

• [上書きを使用して監視する方法](http://go.microsoft.com/fwlink/?LinkID=117777) (<http://go.microsoft.com/fwlink/?LinkID=117777>)

• [Operations Manager 2007 で実行アカウントを作成する方法](http://go.microsoft.com/fwlink/?LinkID=165410) (<http://go.microsoft.com/fwlink/?LinkID=165410>)

• [既存の実行アカウントを変更する方法](http://go.microsoft.com/fwlink/?LinkID=165412) (<http://go.microsoft.com/fwlink/?LinkID=165412>)

• [管理パックのカスタマイズをエクスポートする方法](http://go.microsoft.com/fwlink/?LinkId=209940) (<http://go.microsoft.com/fwlink/?LinkId=209940>)

• [管理パックを削除する方法](http://go.microsoft.com/fwlink/?LinkId=209941) (<http://go.microsoft.com/fwlink/?LinkId=209941>)

Operations Manager および監視パックに関する質問は、「[System Center Operations Manager コミュニティ フォーラム](http://go.microsoft.com/fwlink/?LinkID=179635)」(<http://go.microsoft.com/fwlink/?LinkID=179635>) を参照してください。

また、「[System Center Operations Manager Unleashed ブログ](http://opsmgrunleashed.wordpress.com/)」(<http://opsmgrunleashed.wordpress.com/>) では、個々の監視パックの "例示" 投稿を紹介しています。

Operations Manager のその他の情報については、以下のブログを参照してください。

• [Operations Manager チーム ブログ](http://blogs.technet.com/momteam/default.aspx) (<http://blogs.technet.com/momteam/default.aspx>)

• [Kevin Holman's OpsMgr ブログ](http://blogs.technet.com/kevinholman/default.aspx) (<http://blogs.technet.com/kevinholman/default.aspx>)

• [OperationsManager についての考察](http://thoughtsonopsmgr.blogspot.com/) (<http://thoughtsonopsmgr.blogspot.com/>)

• [Raphael Burri's ブログ](http://rburri.wordpress.com/) (<http://rburri.wordpress.com/>)

• [BWren's マネージメント スペース](http://blogs.technet.com/brianwren/default.aspx) (<http://blogs.technet.com/brianwren/default.aspx>)

• [System Center Operations Manager サポート チーム ブログ](http://blogs.technet.com/operationsmgr/) (<http://blogs.technet.com/operationsmgr/>)

• [Ops Mgr ++](http://blogs.msdn.com/boris_yanushpolsky/default.aspx) (<http://blogs.msdn.com/boris_yanushpolsky/default.aspx>)

• [Notes on System Center Operations Managerについてのメモ](http://blogs.msdn.com/mariussutara/default.aspx) (<http://blogs.msdn.com/mariussutara/default.aspx>)

重要

Microsoft 以外のサイトの情報やコンテンツについては、それぞれの Web サイトのオーナーやユーザーによるものを参照してください。この Web サイトの掲載内容について、Microsoft は明示、暗黙、法定を問わず、一切責任を負いません。

# 付録: 監視パックの内容

以下のセクションで解説しているオブジェクト タイプをネットワーク アクセス保護の監視パックで検出しました。すべてのオブジェクトが自動的に検出されるとは限りません。自動的に検出できないオブジェクトを検出するには、オーバーライドを使用します。

## HRA の検出

検出情報

| **間隔** | **有効** | **有効にするタイミング** |
| --- | --- | --- |
| 4 時間 | 有効 | 該当なし |

関連モニター

| **モニター** | **データ ソース** | **間隔** | **アラート** | **動作のリセット** | **対応ルール** | **有効** | **有効にするタイミング** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Microsoft.Windows.Server.NAP.IISService | IIS サービス | 4 時間 | 有効アラートの優先順位: 通常アラートの重要度: エラー | 自動 | IIS サービス モニター | 有効 | 該当なし |
| Microsoft.Windows.Server.NAP.WebBindingMonitor | スクリプト: IISWebBindingMonitor.ps1 | 4 時間 | 有効アラートの優先順位: 通常アラートの重要度: 警告 | 自動 | Web のバインドでは HTTP を有効にしないでください | 有効 | 該当なし |
| Microsoft.Windows.Server.NAP.SSLCertificateExpiry | スクリプト: SSLCertExpiryMonitor.ps1 | 4 時間 | 有効アラートの優先順位: 通常アラートの重要度: モニターの正常性に一致 | 自動 | SSL 証明書有効期限モニター | 有効 | 該当なし |

注

コネクタを使用している場合、モニターを無効にして、その対応ルールを有効にすればヘルス ステータスを変更せずに警告を有効にできます。

関連ルール

| **ルール** | **データ ソース** | **アラート** | **注** | **対応モニター** | **有効** | **有効にするタイミング** |
| --- | --- | --- | --- | --- | --- | --- |
| Microsoft.Windows.Server.NAP.SSLCertificateExpiry | Windows!Microsoft.Windows.EventProvider Event ID 10 | 有効アラートの優先順位: 通常アラートの重要度: エラー | — | Microsoft.Windows.Server.NAP.CAUnavailable | 有効 | 該当なし |

注

ルールを無効にし、その対応モニターを有効にして、警告、状態の変更、ヘルスのロールアップを有効にします。

関連ビュー

| **表示** | **説明** | **ビューを設定するルールとモニター** |
| --- | --- | --- |
| Microsoft.Windows.Server.NAP.AlertView | このビューは、NPS と HRA の両方に対するすべてのモニターとルールの状態を表示します。 | **•** Microsoft.Windows.Server.NAP.ProxyUnavailable**•** Microsoft.Windows.Server.NAP.NPSService**•** Microsoft.Windows.Server.NAP.CAUnavailable**•** Microsoft.Windows.Server.NAP.SSLCertificateExpiry**•** Microsoft.Windows.Server.NAP.WebBindingMonitor**•** Microsoft.Windows.Server.NAP.IISService |

## NPS の検出

検出情報

| **間隔** | **有効** | **有効にするタイミング** |
| --- | --- | --- |
| 4 時間 | 有効 | 該当なし |

関連モニター

| **モニター** | **データ ソース** | **間隔** | **アラート** | **動作のリセット** | **対応ルール** | **有効** | **有効にするタイミング** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Microsoft.Windows.Server.NAP.NPSService | NPS サービス | 4 時間 | 有効アラートの優先順位: 通常アラートの重要度: エラー | 自動 | NPS サービス モニター | 有効 | 該当なし |

注

コネクタを使用している場合、モニターを無効にして、その対応ルールを有効にすればヘルス ステータスを変更せずに警告を有効にできます。

関連ルール

| **ルール** | **データ ソース** | **アラート** | **注** | **対応モニター** | **有効** | **有効にするタイミング** |
| --- | --- | --- | --- | --- | --- | --- |
| Microsoft.Windows.Server.NAP.ProxyUnavailable | Windows!Microsoft.Windows.EventProvider Event ID 36 | 有効 または無効アラートの優先順位: 通常アラートの重要度: エラー | — | Microsoft.Windows.Server.NAP.ProxyUnavailable | 有効 | 該当なし |

注

ルールを無効にし、その対応モニターを有効にして、警告、状態の変更、ヘルスのロールアップを有効にします。

関連ビュー

| **表示** | **説明** | **ビューを設定するルールとモニター** |
| --- | --- | --- |
| Microsoft.Windows.Server.NAP.AlertView | このビューは、NPS と HRA の両方に対するすべてのモニターとルールの状態を表示します。 | **•** Microsoft.Windows.Server.NAP.ProxyUnavailable**•** Microsoft.Windows.Server.NAP.NPSService**•** Microsoft.Windows.Server.NAP.CAUnavailable**•** Microsoft.Windows.Server.NAP.SSLCertificateExpiry**•** Microsoft.Windows.Server.NAP.WebBindingMonitor**•** Microsoft.Windows.Server.NAP.IISService |

## サービスにサーバー グループの検出が含まれます

検出情報

| **間隔** | **有効** | **有効にするタイミング** |
| --- | --- | --- |
| 4 時間 | 有効 | 該当なし |

関連ビュー

| **表示** | **説明** | **ビューを設定するルールとモニター** |
| --- | --- | --- |
| Microsoft.Windows.Server.NAP.ServersView | このビューは、NAP ロールがインストールされたサーバーのリストを表示します。 | — |