NEC

ESMPRO/ServerAgentService Ver. 1.3
FAQガイド

iStorage

Windows Storage Server

70.109.01-028.02

目　次

表　記

本文中の記号

本書では３種類の記号を使用しています。これらの記号は、次のような意味をもちます。

	ソフトウェアの操作などにおいて、守らなければならないことについて示しています。
	ソフトウェアの操作などにおいて、確認しておかなければならないことについて示しています。
	知っておくと役に立つ情報、便利なことについて示しています。

外来語のカタカナ表記

本書では外来語の長音表記に関して、国語審議会の報告を基に告示された内閣告示に原則準拠しています。但し、OS やアプリケーションソフトウェアなどの記述では準拠していないことがありますが、誤記ではありません。

オペレーティングシステムの表記

本書では、Windows オペレーティングシステムを次のように表記します。

本書の表記		Windows OSの名称
Windows Server 2016		Windows Server 2016 Standard
		Windows Server 2016 Datacenter
		Windows Server 2016 Essentials
Windows Server 2012 R2		Windows Server 2012 R2 Standard
		Windows Server 2012 R2 Datacenter
		Windows Server 2012 R2 Foundation
Windows Server 2012		Windows Server 2012 Standard
		Windows Server 2012 Datacenter
Windows Server 2008 R2		Windows Server 2008 R2 Standard
		Windows Server 2008 R2 Enterprise
		Windows Server 2008 R2 Datacenter
Windows Server 2008	※	Windows Server 2008 Standard
		Windows Server 2008 Enterprise
		Windows Server 2008 Datacenter
Windows 10		Windows 10 Pro　(64ビット版)
Windows 8.1	※	Windows 8.1 Pro
Windows 8	※	Windows 8 Pro
Windows 7	※	Windows 7 Professional

※ 本書では、特に記載がない限り 64 ビット版/32 ビット版を含みます。

商　標

EXPRESSBUILDER と ESMPRO、CLUSTERPRO、EXPRESSSCOPE、Universal RAID Utility は日本電気株式会社の登録商標です。Microsoft、Windows、Windows Server は米国 Microsoft Corporation の米国およびその他の国における商標または登録商標です。

その他、記載の会社名および商品名は各社の商標または登録商標です。
なお、特に TM、Ⓡは明記しておりません。

本書に関する注意と補足

1. **本書の一部または全部を無断転載することを禁じます。**
2. **本書に関しては将来予告なしに変更することがあります。**
3. **弊社の許可なく複製、改変することを禁じます。**
4. **本書について誤記、記載漏れなどお気づきの点があった場合、お買い求めの販売店まで連絡してください。**
5. **運用した結果の影響については、4 項に関わらず弊社は一切責任を負いません。**
6. **本書の説明で用いられているサンプル値は、すべて架空のものです。**

この説明書は、必要なときすぐに参照できるよう、お手元に置いてください。

最新版

本書は作成日時点の情報をもとに作られており、画面イメージ、メッセージ、または手順などが**実際のものと異なることがあります。**変更されているときは適宜読み替えてください。

ESMPRO/ServerAgentService Ver. 1.3

1 概　要

ESMPRO/ServerAgentService について説明します。

1. はじめに

2. ユーザーサポート

ソフトウェアに関する不明点、お問い合わせ先について説明しています。

3. 動作環境

ESMPRO/ServerAgentService の動作を保障する環境について説明しています。

I. はじめに

本書をよくお読みになり、正しくお使いください。
本書の内容は、OS の機能、操作方法について十分に理解されている方を対象に説明しています。
OS に関する操作、不明点は、Windows ヘルプ オンラインなどをご確認ください。

ESMPRO/ServerAgentService は ESMPRO/ServerManager と連携し、サーバーの監視、および各種情報を取得するためのソフトウェアです。

ESMPRO/ServerManager の詳細は、「ESMPRO/ServerManager インストレーションガイド」を参照してください。

2. ユーザーサポート

ソフトウェアに関する不明点は、お買い上げの弊社販売店、最寄りの弊社、または NEC フィールディング株式会社までお問い合わせください。
インターネットでも情報を提供しています。

[NEC コーポレートサイト]

製品情報やサポート情報など、本製品に関する最新情報を掲載しています。

http://jpn.nec.com/

[NEC フィールディング(株) ホームページ]

メンテナンス、ソリューション、用品、施設工事などの情報をご紹介しています。

http://www.fielding.co.jp/

[NEC ファーストコンタクトセンター]

ご購入前のご相談、お問い合わせについてご案内しています。

http://www.nec.co.jp/products/express/question/top_sv1.shtml

ESMPRO/ServerAgentService の使用中に問題が発生したときは、お問い合わせ前に「3 章(1. 注意事項)」を参照してください。該当する症状があれば、記載されているように対処してください。

3. 動作環境

ESMPRO/ServerAgentService の動作を保障するハードウェア/ソフトウェア環境は、以下となります。

● ハードウェア

- インストールする装置	iStorage NS シリーズ本体装置
- メモリ	OS の動作に必要なメモリ+200MB 以上
- ハードディスクドライブの空き容量	50MB 以上

● ソフトウェア

- iStorage NS シリーズにインストールされている OS

- OS コンポーネント	SNMP サービス(簡易ネットワーク管理プロトコル)
	.NET Framework 4.6.x (4.6 以上)
	.NET Framework 4.5.2
	.NET Framework 4.0

- ESMPRO/ServerAgentService は、EXPRESSBUILDER に添付されている ESMPRO/ServerManager のバージョン以上、または、Web 公開されている最新の ESMPRO/ServerManager のバージョンで監視してください。
- 「Nano Server」はサポートしていません。

ESMPRO/ServerAgentService Ver. 1.3

2 FAQ(よくある質問について)

ESMPRO/ServerAgentService のよくある質問について説明します。

1. 基礎知識

ESMPRO/ServerAgentService の基礎知識について説明しています。

2. 基本設定

ESMPRO/ServerAgentServiceの基本設定について説明しています。

3. 動作設定

ESMPRO/ServerAgentServiceの動作設定について説明しています。

Ⅰ. 基礎知識

■サーバーへの接続方法

ESMPRO/ServerAgentService に関する各種セットアップは、「管理 PC」からリモートデスクトップ接続で行います。

1. 「管理 PC」でリモートデスクトップを起動します。
2. 接続先に iStorage NS シリーズのコンピューター名、または IP アドレスを入力します。
3. ユーザー名に「administrator」を入力します。
4. パスワードを入力して、[OK]をクリックします。

ワークグループ環境のパスワードの初期値は、本体装置に添付されている「スタートアップガイド」を参照してください。

■ESMPRO/ServerAgentService のインストール

iStorage NS シリーズは ESMPRO/ServerAgentService がすでにインストールされています。OS を再インストールすると ESMPRO/ServerAgentService も自動で再インストールされます。ただし、購入時の状態や再インストール後の状態では正しく動作しないことがありますので、「2 章(2. 基本設定)」「2 章(3. 動作設定)」の手順に従って、環境に合った設定に変更してください。

■ESMPRO/ServerAgentService のアンインストール

iStorage NS シリーズの運用に ESMPRO/ServerAgentService は必須ですので、アンインストールしないでください。

ESMPRO/ServerAgentService をアンインストールしてしまったときは、OS の再インストールが必要です。

2. 基本設定

■TCP/IP の設定

「管理 PC」からリモートデスクトップ接続で、固定の IP アドレスを設定します。

TCP/IP の設定の詳細は、Windows ヘルプ オンラインを参照してください。

■SNMP サービスの設定変更

「管理 PC」からリモートデスクトップ接続で、SNMP サービスを設定します。

本設定はイベントログ監視機能の通報手段です。他の製品と通報連携する機能の通報手段にもなりますので、必ず設定してください。

1. 「管理 PC」からリモートデスクトップで接続します。

2. 「コントロールパネル」の[管理ツール]-[サービス]をダブルクリックします。

   Server Core 環境のときは、[管理ツール]-[コンピューターの管理]をダブルクリックして表示される、左ペインのツリーの[サービスとアプリケーション]-[サービス]をクリックすると、サービス一覧が表示されます。

3. サービス一覧から[SNMP Service]を選択し、[操作]タブから[プロパティ]をクリックします。

   「SNMP Service のプロパティ」ダイアログボックスが表示されます。

4. [トラップ]プロパティシートの[コミュニティ名]ボックスに、「public」または任意のコミュニティ名を入力して[一覧に追加]をクリックします。

   ESMPRO/ServerManager 側の設定で受信するトラップのコミュニティ名をデフォルトの「*」から変更したときは、ESMPRO/ServerManager 側で新しく設定したコミュニティ名と同じものを入力します。また、ESMPRO/ServerAgentService からのトラップが ESMPRO/ServerManager に正しく受信されるためには、双方のコミュニティ名を一致させてください。

5. [追加]をクリックします。

6. [トラップ送信先]の[追加]をクリックし、[ホスト名、IP アドレス、または IPX アドレス]ボックスに送信先の ESMPRO/ServerManager の IP アドレスを入力後、[追加](または[OK])をクリックします。

   トラップ送信先に指定している IP アドレス(またはホスト名)をマネージャ通報(TCP/IP)の設定で指定すると、重複していることを警告するメッセージが表示されます。

   この設定では、指定している IP アドレス(またはホスト名)の ESMPRO/ServerManager に、アラートが重複して通報されます。

7. [OK]をクリックしてネットワークの設定を閉じます。

以上で SNMP サービスの設定は終了です。

3. 動作設定

3.1 ポートの設定

ESMRPO/ServerManager からの監視に使う WS-Man の使用ポート(5985/tcp、80/tcp)は OS インストール後から開放されますが、OS やご利用のネットワーク環境によって、アクセスがローカルサブネット内の装置に制限されます。
異なるサブネット上の ESMPRO/ServerManager で監視するときは、以下の手順に従って、ESMPRO/ServerManager の WS-Man のアクセスを許可してください。

1. 「コントロールパネル」の[管理ツール]-[セキュリティが強化された Windows ファイアウォール]をダブルクリックします。

2. [受信の規則]をクリックします。

3. [Windows リモート管理 (HTTP 受信)]を選択し、[操作]タブから[プロパティ]をクリックします。
   Windows リモート管理 (HTTP 受信)のプロパティが表示されます。

   OS によって[Windows リモート管理 (HTTP 受信)]は、ネットワークプロファイルによって複数に分かれています。ご利用環境のルールを選択してください。

4. [スコープ]プロパティシートのリモート IP アドレスで、[任意の IP アドレス]を選択します。
   [これらの IP アドレス]を選択するときは、ESMPRO/ServerManager の IP アドレスを追加してください。

5. [OK]をクリックして受信規則の設定を閉じます。

3.2 HTTPS 接続の設定

3.2.1 HTTPS 接続の設定方法

ESMPRO/ServerManager との接続に HTTPS を利用するときは、以下のいずれかの手順に従って、HTTPS 接続を設定してください。

ESMPRO/ServerManager との接続に HTTP を利用すると、WS-Man 通信で利用する Basic 認証のユーザー名とパスワードがネットワーク上に平文で流れるため、HTTPS 接続を推奨します。

認証局に署名された証明書を準備することを推奨します。

HTTPS 接続を設定すると、システムの状況により以下のイベントログが登録されますが、システムの運用に影響はありません。

ソース : HttpEvent
イベント ID : 15301
レベル : 警告
説明 : ポート 0.0.0.0:5986 の SSL 証明書設定が管理プロセスによって作成されました。

ソース : HttpEvent
イベント ID : 15300
レベル : 警告
説明 : ポート 0.0.0.0:5986 の SSL 証明書設定が削除されました。

■認証局に署名された証明書を使って HTTPS 接続を設定する

認証局に署名された証明書で HTTPS 接続を行います。証明書のインストールまでは認証局に指定された方法で行う必要があります。

1. 認証局に指定された手順に従って、証明書をインストールします。

2. ESMPRO/ServerAgentService をインストールしているサーバーに、ビルトイン Administrator(または管理者権限のあるアカウント)で、サインイン(ログオン)します。

3. 証明書ファイルを%EsmDir%¥tool(規定値は C:¥ESM¥tool)に格納します。

4. コマンドプロンプトを「管理者として実行」で起動します。

5. 以下のコマンドを実行します。

```
cd %EsmDir%¥tool
ESMHttps.bat -c [証明書ファイル]
```

■keytool.exe を使って HTTPS 接続を設定する

ESMPRO/ServerManager をインストールしている管理 PC で自己署名証明書を作成して、ESMPRO/ServerAgentService をインストールしているサーバーで HTTPS 接続設定を行います。keytool.exe は ESMPRO/ServerManager に同梱されています。

1. ESMPRO/ServerManager をインストールしている管理 PC に、ビルトイン Administrator(または管理者権限のあるアカウント)で、サインイン(ログオン)します。

2. コマンドプロンプトを「管理者として実行」で起動します。

3. 以下のコマンドを実行して、自己署名証明書を作成します。

   ESMPRO/ServerManager を"C:¥Program Files (x86)¥ESMPRO"にインストールしたとき

   "C:¥Program Files (x86)¥ESMPRO¥ESMWEB¥jre¥bin¥keytool.exe" -genkey -keystore <証明書出力先> -storepass <パスワード> -validity <証明書の有効日数> -keyalg RSA -keysize <キーサイズ> -storetype pkcs12 -ext EKU=serverAuth -dname “CN=<監視対象サーバーの IP アドレス>"

   例：ESMPRO/ServerAgentService をインストールしているサーバーの IP アドレスが 192.168.1.1 のとき

   "C:¥Program Files (x86)¥ESMPRO¥ESMWEB¥jre¥bin¥keytool.exe" -genkey -keystore C:¥temp¥esmpro.pfx -storepass secret -validity 3650 -keyalg RSA -keysize 2048 -storetype pkcs12 -ext EKU=serverAuth -dname "CN=192.168.1.1"

   - 例では C:¥temp に esmpro.pfx が作成されます。あらかじめ C:¥temp フォルダーを作成してください。
   - 32 ビット版では"Program Files (x86)"を"Program Files"に読み替えてください。

4. ESMPRO/ServerAgentService をインストールしているサーバーに、ビルトイン Administrator(または管理者権限のあるアカウント)で、サインイン(ログオン)します。

5. 手順 3.で作成した証明書ファイルを%EsmDir%¥tool(規定値は C:¥ESM¥tool)に格納します。

6. コマンドプロンプトを「管理者として実行」で起動します。

7. 以下のコマンドを実行します。

   cd %EsmDir%¥tool

   ESMHttps.bat -c [証明書ファイル] [パスワード]

■makecert.exe を使って HTTPS 接続を設定する

makecert.exe で自己署名証明書を作成して、HTTPS 接続設定を行います。makecert.exe は Windows SDK をインストールすることで利用できます。

makecert.exe はファイルバージョンが 6 以降のものを使ってください。

makecert.exe の詳細は、以下のサイトを参照してください。
Makecert.exe (証明書作成ツール)
https://msdn.microsoft.com/library/windows/desktop/aa386968.aspx

1. ESMPRO/ServerAgentService をインストールしているサーバーに、ビルトイン Administrator(または管理者権限のあるアカウント)でサインイン(ログオン)します。

2. makecert.exe を%EsmDir%¥tool(規定値は C:¥ESM¥tool)に格納します。

3. コマンドプロンプトを「管理者として実行」で起動します。

4. 以下のコマンドを実行します。

   cd %EsmDir%¥tool
   ESMHttps.bat -m [IP アドレス] [証明書の有効期限(MM/DD/YYYY)]

   例：ESMPRO/ServerAgentService をインストールしているサーバーの IP アドレスが 192.168.1.100 であり、証明書の有効期限を 2040 年 12 月 31 に設定するとき
   ESMHttps.bat -m 192.168.1.100 12/31/2040

3.2.2 ポートの開放

HTTPS 接続で使うポートを開放してください。

1. 「コントロールパネル」の[管理ツール]-[セキュリティが強化された Windows ファイアウォール]をダブルクリックします。

2. [受信の規則]を右クリックして、[新しい規則]を選択します。

3. [ポート]を選択し、[次へ]をクリックします。

4. [TCP]、[特定のローカルポート]を選択し、ポート番号に 5986 を入力して[次へ]をクリックします。

   Windows Server 2008 のときはポート番号に 443 を入力してください。

5. [接続を許可する]を選択し、[次へ]をクリックします。

6. [ドメイン]、[プライベート]、[パブリック]から ESMPRO/ServerManager との接続に使っているプロファイルを選択します。

7. 受信規則の[名前]および[説明]を入力します。

3.2.3 ESMPRO/ServerManager の設定

自己署名証明書を使うときは、ESMPRO/ServerManager の設定で WS-Man 通信の自己署名証明を許容するように変更してください。信頼されたルート証明書を使うときは、以下の手順は不要です。

1. ESMPRO/ServerManager にログインします。

2. [環境設定]を選択します。

3. [ネットワーク]タブを選択し、[編集]をクリックします。

4. [WS-Man 通信]-[自己署名証明]の[許容する]を選択し、[適用]をクリックします。

以上で HTTPS 接続の設定は終了です。

3.3 動作確認

ESMPRO/ServerAgentService の設定が正しく行われているか、別のサーバーから接続できるかを確認してください。

1. 別のサーバーのコマンドプロンプトから管理者として以下のコマンドを実行し、winrm を設定します。

```
winrm quickconfig
winrm set winrm/config/Client @{AllowUnencrypted="true"}
winrm set winrm/config/Client/Auth @{Basic="true"}
winrm set winrm/config/Client @{TrustedHosts="<監視サーバーの IP アドレス>"}
```

2. 以下のコマンドを実行して、ESMPRO/ServerAgentService をインストールしているサーバーに接続できるか確認します。

```
winrm identify -r:http://<監視サーバーの IP アドレス>:<ポート> -u:<ユーザー名> -p:<パスワード> -a:Basic
winrm e wmi/root/cimv2/Win32_ComputerSystemProduct -r:http://<監視サーバーの IP アドレス>:<ポート> -u:<ユーザー名> -p:<パスワード> -a:Basic
winrm e wmi/root/ESMPRO/AS/ESM_GeneralInformation -r:http://<監視サーバーの IP アドレス>:<ポート> -u:<ユーザー名> -p:<パスワード> -a:Basic
```

- HTTPS 接続のときは、-r オプションで https としてください。
- ポート番号は HTTP/5985、HTTPS/5986 となります。Windows Server 2008 のときは HTTP/80、HTTPS/443 です。
- ユーザー名、パスワードは監視サーバーの OS サインイン(ログオン)アカウントを使ってください。
- 自己署名証明書で HTTPS 接続設定をした監視サーバーにアクセスするときは、以下のようにコマンドの最後に"-skipCACheck"を追加してください。

  winrm identify -r:http://<監視サーバーの IP アドレス>:<ポート> -u:<ユーザー名> -p:<パスワード> -a:Basic -skipCACheck

3. 手順 2.でエラーが表示されたときは、ESMPRO/ServerAgentService の設定が間違っていないか、以下の手順で設定を確認します。

・ESMPRO/ServerManager との接続に HTTPS を利用するとき
「2 章(3.2 HTTPS 接続の設定)」の手順に従って、HTTPS 接続の設定をやりなおしてください。

・ESMPRO/ServerManager との接続に HTTP を利用するとき
ESMPRO/ServerAgentService をインストールしているサーバーで、以下のコマンドを実行してください。実行結果にエラー番号とエラー内容が表示されなければ成功です。

```
winrm quickconfig
winrm set winrm/config/service @{AllowUnencrypted="true"}
```

4. 別のサーバーから手順 2.のコマンドを再度実行し、サーバーに接続できるか確認します。

3.4 PCIeSSD の監視

PCIeSSD をご利用の環境では、PCIeSSD の構成情報(モデル名など)や寿命状態が監視できます。以下の手順に従って、監視機能を有効にしてください。

1. 「コントロールパネル」の[管理ツール]-[サービス]をダブルクリックします。

2. サービスの一覧から[ESMNVMeMonitor]を選択し、[操作]タブから[プロパティ]をクリックします。

3. [全般]プロパティシートの[スタートアップの種類]を「手動」から「自動」に変更します。

4. [開始]をクリックし、[ESMNVMeMonitor]を開始します。

5. [OK]をクリックし、サービスのプロパティを閉じます。

ESMPRO/ServerManager を使って PCIeSSD を監視するには BMC(EXPRESSSCOPE エンジン)への登録が必須です。ESMPRO/ServerManager は、PCIeSSD の構成情報や寿命状態を BMC(EXPRESSSCOPE エンジン)から取得します。ESMNVMeMonitor を停止しても ESMPRO/ServerManager では PCIeSSD に関する情報を表示しますが、寿命状態を更新しません。寿命状態を監視するときは、ESMNVMeMonitor を開始状態で運用願います。

ESMPRO/ServerAgentService Ver. 1.3

3 付　録

1. **注意事項**

   ESMPRO/ServerAgentServiceの注意すべき点を説明しています。

2. **ポート一覧**

   ESMPRO/ServerAgentServiceの使用ポートについて説明しています。

3. **サービス一覧**

   ESMPRO/ServerAgentServiceが登録するサービス一覧について説明しています。

4. **サービスの開始/停止順**

   ESMPRO/ServerAgentServiceが登録するサービスの開始順、停止順について説明しています。

1. 注意事項

1.1 イベントログ

■Alert Manager WMI Service のハングアップ および ESMCommonService の起動失敗のイベントログ(システム)

ESMPRO/ServerManager と ESMPRO/ServerAgentService を同じ装置にインストールするときなど、システムの状況により以下のイベントログが登録されますが、サービスが開始状態(実行中)に移行していれば、システムの運用に影響はありません。

ソース	:	Service Control Manager
イベント ID	:	7022
レベル	:	エラー
説明	:	Alert Manager WMI Service サービスは開始時にハングしました。

またこの場合、ESMCommonService が正常に開始しないときがあります。ESMCommonService には「遅延開始」と「エラー時の自動再起動」が設定されていますので、「エラー時の自動再起動」によってサービスが開始状態(実行中)に移行していれば、システムの運用に影響はありません。

■ESMPRO/ServerManager と HTTP 接続すると登録されるイベントログ(システム)

ESMPRO/ServerManager と HTTP 接続すると、以下のようなイベントログが登録されます。

ソース	:	Windows Remote Management
イベント ID	:	10120
レベル	:	警告
説明	:	WinRM サービスは安全でない HTTP 接続を 192.168.1.1 から 受け取りました。これはセキュリティで保護された構成ではありません。 ユーザー操作 WinRM 構成で AllowUnencrypted を False に設定し、ワイヤ上でパケットが確実に暗号化されるようにしてください。

このイベントはシステムの運用に影響はありませんが、セキュリティで保護されてない構成です。セキュリティで保護された構成を構築するときは、「2 章(3.2 HTTPS 接続の設定)」の手順に従って、HTTPS 接続を行ってください。HTTPS 接続するとイベントログは登録されません。

■ESMPRO/ServerManager との通信時に登録されるイベントログ(アプリケーション)

64 個以上の論理プロセッサを使用する環境では、ESMPRO/ServerManager と通信を行う際に、以下のようなイベントログが登録されることがありますが、システムの運用に影響はありません。

ソース	:	Microsoft-Windows-PerfNet
イベント ID	:	2006
レベル	:	エラー
説明	:	サーバー サービスからサーバー キュー パフォーマンス データを 読み取れません。データ セクションの最初の 4 バイト (DWORD) には状態コードが含まれ、2 番目の 4 バイトには IOSB.Status が含まれ、3 番目の 4 バイトには IOSB.Information が含まれています。

本件に関する詳細情報は、マイクロソフトサポートオンラインに記載されています。

- マイクロソフト サポート技術情報- 文書番号:2607486

  https://support.microsoft.com/ja-jp/help/2607486/

■シャットダウン時に登録される WinRM のイベントログ(システム)

ESMPRO/ServerAgentService をインストールしている装置で、装置のシャットダウンを行うと以下のようなイベントログが登録されますが、システムの運用に影響はありません。

ソース	:	Windows Remote Manager
イベント ID	:	10149
レベル	:	警告
説明	:	WinRM サービスは、WS-Management 要求をリッスンしていません。

意図的にサービスを停止していないときは、以下のコマンドで WinRM 構成を確認してください。

```
winrm enumerate winrm/config/listener
```

このイベントは WS-Management のリスナーが停止するときに登録されます。シャットダウン時は Windows Remote Manager サービスが停止されるためイベントログが登録されます。

■ハードウェアログ(SEL)の監視機能

ESMPRO/ServerAgentService によるハードウェアログ(SEL)の監視は、Windows Management Instrumentation (WMI)サービスを使って監視します。そのため WMI サービスが停止、再起動すると、ハードウェアログ(SEL)が監視できなくなることがあります。

WMI サービスが停止、再起動したときは、イベントログ(アプリケーション)に以下のイベントが登録されます。

ソース	:	Application Error
イベント ID	:	1000
レベル	:	エラー
説明	:	障害が発生しているアプリケーション名: svchost.exe

WMI サービスが停止、再起動したときは、OS を再起動していただくか、または「コントロールパネル」の[管理ツール]-[サービス]から「ESM System Management Service」を再起動してください。
「ESM System Management Service」を再起動することで、ESMPRO/ServerAgentService は、WMI サービスへ再接続します。

■監視イベントの通報

- アラート通報機能は、システムのイベントログに登録されたイベント情報を元に通報しています。そのためイベントビューアーのイベントログの設定で、イベントログの処理を[必要に応じてイベントを上書きする]、または[イベントを上書きしないでログをアーカイブする]に設定してください。それ以外の設定では通報されません。

- アラートマネージャ設定ウィンドウの監視イベントツリーに登録されたイベントは、Alert Manager Main Service が開始していないと SNMP トラップを受信できるマネージャーへ通報されません。Alert Manager Main Service が開始しているときであっても、各通報手段の通報有効/無効フラグが無効になっていると通報されません。通報有効/無効フラグは、アラートマネージャの[設定]メニューから[通報基本設定]-[通報手段の設定]で設定します。
  同様に、システム起動時に Event Log サービスが開始以前に発生したイベントについても通報されません。

- アラートマネージャ設定ウィンドウの[通報基本設定]-[その他の設定]で、シャットダウン開始までの時間を設定できます。初期値は 20 秒になっています。シャットダウン時に通報するには、この値を初期値より短くしないでください。

- 監視対象イベントの通報時に通報障害が発生すると、イベントログにエラーメッセージが登録されます。この通報時に発生するエラーメッセージを監視対象イベントとして新規登録すると、通報時のエラーを再度通報してしまうため、障害復旧時に大量に通報されてシステムの負荷が高くなり性能が低下します。特に以下のアラート通報機能のサービスが出力するイベントは監視対象としないでください。
  - ・Alert Manager Main Service
  - ・Alert Manager Socket(S) Service
  - ・(Alert Manager ALIVE(S) Service)*

    (*) Alert Manager ALIVE(S) Service は、エクスプレス通報サービス、または WebSAM AlertManager をインストールしているときだけ、登録されるサービスです。

- アラート通報機能のマネージャ通報(SNMP)で通報できるメッセージの長さは、511 バイトまでです。512 バイト以上のメッセージを通報すると、アラートビューアには 512 バイト目からのメッセージは表示されません。512 バイト目からのメッセージは、通報した装置のイベントビューアーで確認してください。また、512 バイト以上のメッセージをすべてアラートビューアに表示するには、マネージャ通報(TCP/IP In-Band)を使ってください。

1.2 ハードディスクドライブ・RAIDシステム・ファイルシステム

■RAID システムの監視

RAID システムの監視は、管理ユーティリティである Universal RAID Utility を使います。詳細は、Universal RAID Utility の各マニュアルを参照してください。

■SATA 接続の光ディスクドライブ

LSI Embedded MegaRAID をお使いのときは、ESMPRO/ServerManager の[サーバ状態/構成情報]のストレージツリー配下に、SATA 接続の光ディスクドライブに関する情報は表示されません。

■SCSI/IDE コントローラーのリソース情報

SCSI/IDE コントローラーの構成管理情報に含まれる[リソース情報]は、正しい情報を取得できません。OS のシステム情報やデバイスマネージャーを参照して確認してください。

■SCSI/IDE 接続以外のデバイスの監視

ストレージ監視は USB などの SCSI/IDE 接続以外のストレージデバイスを監視しません。

■ストレージ、ファイルシステム監視機能の設定変更

設定を変更するには、ESMPRO/ServerManager(Ver. 6.05 以降)が必要です。また、
ESMPRO/ServerManager で変更した、監視間隔、ハードディスクドライブ予防保守の有効/無効、ファイルシステム空き容量監視のしきい値は、変更してもすぐには反映されません。設定変更後、監視機能の次の監視間隔で変更した設定が有効になります。

■テープ監視機能

ESMPRO/ServerAgentService では、テープ装置は障害監視しません。
監視するには、バックアップソフトウェア、またはテープ監視アプリケーションをご利用ください。
ESMPRO/ServerAgentService のイベント監視機能を使うことで、バックアップソフトウェア、またはテープ監視アプリケーションが登録するイベントログを監視できます。

■ネットワークドライブの ESMPRO/ServerManager の[サーバ状態/構成情報]の表示

ネットワーク接続したドライブは、ESMPRO/ServerManager の[サーバ状態/構成情報]のファイルシステムツリー配下に表示されません。

■ハードディスクドライブ予防保守の変更

ハードディスクドライブ予防保守の有効/無効を変更すると、監視対象すべてのハードディスクドライブに対して変更した内容が設定されます。個々のハードディスクドライブごとに対しては、有効/無効を設定できません。

■メディア挿入時のファイルシステム情報

フロッピーディスクや DVD などのメディアを挿入すると、ESMPRO/ServerManager[サーバ状態/構成情報]のファイルシステム情報として、容量情報やボリュームラベルなどの情報を表示します。容量情報の最小単位を"GB"としているため、フロッピーディスクなど容量が小さいメディアは、"0.0GB"と表示されることがあります。

■容量が 100MB 未満のファイルシステム空き容量監視

ESMPRO/ServerAgentService では、容量が 100MB 未満のファイルシステムの空き容量監視をサポートしていません。このようなファイルシステムの空き容量監視設定は、初期状態で「無効(監視しない)」となります。

1.3 I/Oデバイス

■シリアルポート

ESMPRO/ServerAgentService はシリアルポートを使う機能が複数あり、これらの機能を使うとポートが不足することがあります。

それぞれの機能で使うシリアルポートは、以下となります。

- UPS : COM1～10
- APCU : COM1～2
- (ALIVE 保守)* : COM1～9

(*) ALIVE 保守はリモートアクセスサービス(Remote Access Service)を利用します。

マネージャ通報(TCP/IP Out-of-Band)でリモートアクセスサービスを利用するときに使えるシリアルポートは、以下となります。

- マネージャ通報(TCP/IP Out-of-Band) : COM1～10

このうち、シリアルポートを共有できるのは、以下の組み合わせだけです。

- ALIVE 保守+ユーザー利用リモートアクセスサービス

どちらか一方の機能で回線を使っているときはもう一方の機能は使えません。

リモートアクセスサービスを使うマネージャ通報(TCP/IP Out-of-Band)は、ほかのシリアルポートと共有すると障害情報が通知できません。共有しないでください。

1.4 他製品との共存

■CLUSTERPRO システムにおけるファイルシステム監視

CLUSTERPRO によるクラスター環境で ESMPRO/ServerAgentService を使うときは、運用系サーバーで設定した空き容量監視機能のしきい値、監視の有効/無効は、フェールオーバーが発生すると待機系サーバーへ引き継がれません。

必ず、待機系サーバーでしきい値、監視の有効/無効を設定してください。

■Oracle 製品との共存

Oracle 製品をインストールすると、SNMP Service のスタートアップが「自動」から「手動」に変更されることがあります。変更されたときは「自動」に戻した上で、Oracle 製品の説明書に従って、正しく設定してください。

1.5 通報

■アラート

アラートビューアで表示されるアラートの詳細情報は、アラートにより一部の情報が「不明」と表示されます。

■一般クライアント通報

「一般クライアント通報」は使えません。通報手段を有効にしてもエラーにはなりませんが、通報されません。

■通報設定の表示

ESMPRO/ServerManager を ESMPRO/ServerAgentService と同じ装置にインストールするときは、ESMPRO/ServerManager の[スタート]メニューにだけ[通報設定]が表示されることがあります。

1.6 OS依存

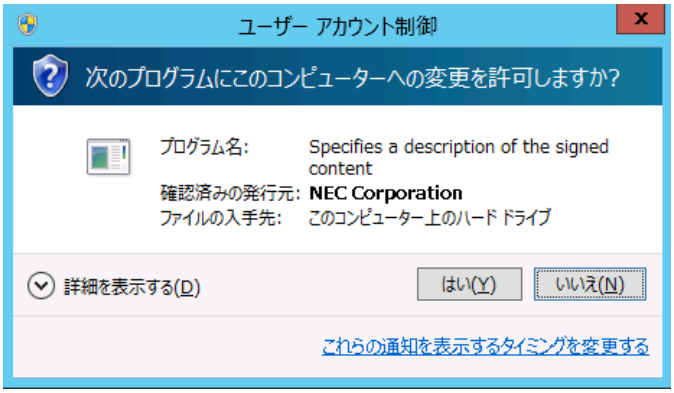
■Server Core 環境の注意事項

Server Core 環境では、以下の注意事項があります。

- アラートマネージャ設定ウィンドウ(amsadm.exe)や ESRAS ユーティリティ(rasutl.exe)のヘルプウィンドウは、表示されません。
- マネージャ通報(TCP/IP Out-of-Band)機能は使えません。
- Windows Server 2016 では、アラートマネージャ設定ウィンドウ(amsadm.exe)のコンボボックス、ラジオボタン、チェックボックスの画面が正しく表示されないことがありますが、アラートマネージャの設定や通報機能に影響はありません。

■ユーザーアカウント制御

ユーザーアカウント制御を有効にしている場合、collect を実行したときなどに、管理者権限へ昇格させるためのダイアログが表示されます。表示されたときは[はい]をクリックしてください。



■仮想化環境のホスト OS 上での注意事項

ESMPRO/ServerAgentService は連続運用が危険な障害情報を検出すると、デフォルトの設定では OS をシャットダウンします。

仮想化環境でゲスト OS を起動している環境では、ゲスト OS がシャットダウンされずにサービスコンソールがシャットダウンするため、ゲスト OS からは予期せぬシャットダウンが発生したことになります。ゲスト OS を正常に終了するには、ESMPRO/ServerAgentService からの通報によるシャットダウン機能を無効にし、障害発生時には手動でゲスト OS からシャットダウンしてください。

[通報によるシャットダウン機能の設定手順]

1. ビルトイン Administrator(または管理者権限のあるアカウント)で、サインイン(ログオン)します。

2. [スタート]メニューから[通報設定]をクリックします。
   アラートマネージャ設定ウィンドウが表示されます。

3. [設定]タブの[通報基本設定]をクリックします。
   通報基本設定のウィンドウが表示されます。

4. [その他の設定]の「シャットダウン開始までの時間設定」項目が、赤アイコン(無効)になっていることを確認します。
   緑アイコン(有効)になっているときは、アイコンをクリックして赤アイコン(無効)に変更してください。

5. [OK]をクリックして設定ウィンドウを閉じます。

1.7 その他

■ESMPRO/ServerManager Ver. 6.00 以降で WS-Man での登録検索が失敗する

ESMPRO/ServerManager Ver. 6.00 以降で WS-Man での登録検索が失敗するときは、以下の手順に従って、Windows リモート管理 (WinRM)の設定を確認してください。

1. ESMPRO/ServerAgentService をインストールしているサーバーに、ビルトイン Administrator(または管理者権限のあるアカウント)で、サインイン(ログオン)します。

2. コマンドプロンプトを「管理者として実行」で起動します。

3. 以下のコマンドを実行します。

   winrm quickconfig -q

4. 以下のコマンドを実行します。

   winrm get winrm/config/service

5. 以下の値が"true"になっているかを確認します。

   - auth 配下の Basic

6. 確認した値が"false"になっているときは、以下の Windows リモート管理 (WinRM) のコマンドを実行します。

   winrm set winrm/config/service/auth @{Basic="true"}

7. 以下のコマンドを実行します。

   winrm get winrm/config/service

8. 以下の値を確認します。

   - AllowUnencrypted

9. ESMPRO/ServerManager との接続に HTTP と HTTPS のどちらを利用するかによって、以下の Windows リモート管理 (WinRM)のコマンドを実行します。

・ESMPRO/ServerManager との接続に HTTPS を利用するとき
(「2 章(3.2 HTTPS 接続の設定)」の手順に従って、HTTPS 接続を行ってください)

```
winrm set winrm/config/service @{AllowUnencrypted="false"}
```

・ESMPRO/ServerManager との接続に HTTP を利用するとき

```
winrm set winrm/config/service @{AllowUnencrypted="true"}
```

■ESMPRO/ServerManager からハードウェアの状態監視を行うには

ESMPRO/ServerManager からハードウェアの状態監視を行うには、BMC(EXPRESSSCOPE エンジン)の登録と、SNMP 通報設定が必須です。

■ESMPRO/ServerManager で ESMPRO/ServerAgentService の自動登録に失敗する

「2 章(3.3 動作確認)」を参照して、ESMPRO/ServerAgentService の設定を確認してください。

■ハードウェアの不具合発生後の再起動

ハードウェアの不具合を検出したときは、OS をシャットダウンします。必ず不具合を対処して復旧したあとに、OS を再起動してください。シャットダウン後に不具合を対処しないで OS を再起動すると、再起動の直後にシャットダウンします。

2. ポート一覧

ESMPRO/ServerAgentServiceの使用ポートは以下となります。

ファイアウォールを有効にするときは、必要なポート間の通信を許可するように設定してください。

[ESMPRO/ServerManager <-> ESMPRO/ServerAgentService 間]

機能	ESMPRO/ServerManager	方向	ESMPRO/ServerAgentService	備考
自動登録 サーバー監視(WS-MAN/HTTP)	不定	→ ←	5985/tcp (80/tcp)*	HTTP
自動登録 サーバー監視(WS-MAN/HTTPS)	不定	→ ←	5986/tcp (443/tcp)*	HTTPS
マネージャ通報 (SNMP)	162/udp	←	不定	SNMP-trap
マネージャ通報 (TCP/IP In-Band)	31134/tcp	← →	不定	
CIM-Indication通報	6736/tcp (設定変更可能)	←	不定	

(*) Windows Server 2008 に ESMPRO/ServerAgentService をインストールしたときの使用ポートは、それぞれ HTTP/80、HTTPS/443 となります。

[エクスプレス通報サービス <-> メールサーバー間]

機能	ESMPRO/ServerAgentService	方向	メールサーバー	備考
エクスプレス通報サービス (インターネットメール)	不定	→ ←	25/tcp	SMTP
		← →	110/tcp	(POP3)*

(*) POP before SMTP を使うときだけとなります。

[エクスプレス通報サービス(HTTPS) <-> Web サーバー間]

機能	ESMPRO/ServerAgentService	方向	Webサーバー	備考
エクスプレス通報サービス (HTTPS)	不定	→ ←	443/tcp	(HTTPS)*

(*) HTTPS ポート(443)が閉じられているときは、ファイアウォールの設定を変更しポート 443 番を開け、https の接続を可能な状態に設定してください。

- 双方向のものは、上段の矢印が通信開始時、下段の矢印は折り返しの通信を示します。
- マネージャ通報(TCP/IP In-Band)、およびエクスプレス通報サービス(インターネットメール)で使うポート番号は、アラートマネージャ設定ウィンドウで変更できます。
- 「不定」の箇所はポートが決まっていません(通信開始時未使用のポートを使います)。

3. サービス一覧

ESMPRO/ServerAgentServiceが登録するサービスは以下となります。

サービス名	プロセス名	スタートアップ	機能概要	備考
Alert Manager Main Service	AMVMain.exe	自動 (遅延開始)	さまざまな障害通報に関して管理します。	
Alert Manager Socket(S) Service	amvscks.exe	手動	TCP/IPを使ってマネージャ通報(送信)します。	通報基本設定で、マネージャ通報(TCP/IP In-Band)、マネージャ通報(TCP/IP Out-of-Band)のどちらかを有効(緑)で起動、すべて無効(赤)で停止します。
ESMCommonService	ESMCommon.exe	自動 (遅延開始)	ESMPRO監視機能を有効にします。	
ESM System Management Service	esmsmsrv.exe	自動	ハードウェアログ(SEL)を監視します。	IPMI対応機種のときに登録します。
ESMNVMeMonitor	esmnvme.exe	手動	PCIeSSDの構成と寿命状態を監視します。	IPMI対応機種のときに登録します。

4. サービスの停止/開始順

サービスを手動で停止または開始するときは、以下の順序で停止または開始します。
機種により登録されるサービスは異なります。

【順序】	【サービス停止】	【サービス開始】
1.	ESMCommonService 停止	ESMCommonService 開始
2.	ESM System Management Service 停止	ESM System Management Service 開始
3.	(ESMNVMeMonitor)*1 停止	(ESMNVMeMonitor)*1 開始
4.	(Alert Manager ALIVE(S) Service)*2 停止	SNMP Service 開始
5.	Alert Manager Main Service 停止	(Alert Manager ALIVE(S) Service)*2 開始
6.	Alert Manager Socket(S) Service 停止	Alert Manager Main Service 開始
7.	SNMP Service 停止	Alert Manager Socket(S) Service 開始

(*1) PCIeSSD ご利用の環境で、ESMNVMeMonitor を開始しているときのみです。

(*2) エクスプレス通報サービス、または WebSAM AlertManager をインストールしたときに登録されるサービスです。

ESMPRO/ServerAgentService Ver. 1.3
FAQ ガイド

日　本　電　気　株　式　会　社
東京都港区芝五丁目 7 番 1 号
TEL（03）3454-1111 （大代表）