

FAQガイド

iStorage NSシリーズ

ESMPRO/ServerAgentService Ver. 1.0

1章 概 要

2章 FAQ(よくある質問について)

3章 付 録




目 次

目 次	2
本書で使う表記	3
本文中の記号	3
外来語のカタカナ表記	3
オペレーティングシステムの表記	4
商 標	5
本書についての注意、補足	6
最新版	6
1 章 概 要	7
1. はじめに	8
2. ユーザーサポート	9
3. 動作環境	10
2 章 FAQ(よくある質問について)	11
1. 基礎知識	12
2. 基本設定	13
3. 動作設定	15
3.1 ポートの設定	15
3.2 HTTPS 接続の設定	16
3.3 動作確認	24
3 章 付 録	26
1. 注意事項	27
1.1 イベントログ	27
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	31
1.3 I/O デバイス	33
1.4 他製品との共存	33
1.5 通報	35
1.6 OS 依存	35
1.7 その他	38
2. ポート一覧	41
3. サービス一覧	42
4. サービスの停止/開始順	43

本書で使う表記

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、次のような意味を持ちます。

	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。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(以降、OS)を次のように表記します。

本書の表記	Windows OSの名称
Windows Server 2012 R2	Windows Server 2012 R2 Standard
	Windows Server 2012 R2 Datacenter
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 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。Avago、LSI および LSI ロゴ・デザインは Avago Technologies(アバゴ・テクノロジー社)の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、® は明記していません。

本書についての注意、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場合があります。変更されているときは適宜読み替えてください。

ESMPRO/ServerAgentService Ver. 1.0

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 が動作する環境について説明しています。

1. 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、iStorage NS シリーズの監視、および各種情報を取得するためのソフトウェアです。

このソフトウェアは、機種に関係なくすべての iStorage NS シリーズにインストールされています。

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 フィールドイ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 フィールドイング(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 が動作するハードウェア/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 4.5.2 |
| | .NET Framework 4.5.1 |
| | .NET Framework 4.5 |
| | .NET Framework 4.0 |



ESMPRO/ServerAgentService は、ESMPRO/ServerManager Ver. 6.00 以上で監視してください。

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。

1. 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。

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。



- SNMP サービスをインストールするときに Windows サービスの一覧を開いていると、「SNMP Service のプロパティ」ダイアログボックスの[エージェント]プロパティシートや[トラップ]プロパティシート、[セキュリティ]プロパティシートが表示されません。表示されていないときは、Windows サービスの一覧を開いてから、もう一度 Windows サービスの一覧を開いてください。
- Windows Server 2012 以降の OS では、SNMP サービスの機能管理ツールをインストールしていないと「SNMP Service のプロパティ」ダイアログボックスが正しく表示されません。「コントロールパネル」の[プログラムと機能]-[Windows の機能の有効化または無効化]-[機能]-[リモート サーバー管理ツール]-[機能管理ツール]から[SNMP ツール]を追加してください。

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 マシンの 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マシンに制限されます。

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

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

- 1) 証明書の準備、または自己署名証明書を作成する。
- 2) 証明書を登録する。
- 3) 証明書を確認する。
- 4) HTTPS Listener を作成する。
- 5) ポートを開放する。
- 6) ESMPRO/ServerManager の設定を変更する。



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。

■ 証明書の準備

HTTPS を利用するときは、認証局(CA)に署名された証明書、または自己署名証明書が必要になります。認証局(CA)に署名された証明書が準備できないときは、次項の「■ 自己署名証明書の作成」の手順に従って証明書を作成してください。



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。

■ 自己署名証明書の作成

自己署名証明書の作成は、makecert.exe(証明書作成ツール)を利用する方法と ESMPRO/ServerManager を利用する方法があります。あらかじめ証明書を準備しているときは、本項目は不要です。

・ makecert.exe を利用する方法

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 を利用し ESMPRO/ServerAgentService をインストールしている監視対象サーバーで証明書を作成します。

監視対象サーバーに管理者権限のあるアカウントでサインイン(ログオン)し、Windows SDK のコマンドプロンプトで以下のコマンドを実行してください。

```
makecert.exe -r -pe -n "CN=<監視対象サーバーの IP アドレス>" -e <有効期限> -eku  
1.3.6.1.5.5.7.3.1 -ss my -sr localMachine -sky exchange -sp "Microsoft RSA SChannel  
Cryptographic Provider" -sy 12 certificate name.cer
```

例：監視対象サーバーの IP アドレスが 192.168.1.1 のとき

```
makecert.exe -r -pe -n "CN=192.168.1.1" -e 01/01/2020 -eku 1.3.6.1.5.5.7.3.1 -ss my -sr  
localMachine -sky exchange -sp "Microsoft RSA SChannel Cryptographic Provider" -sy 12  
C:¥temp¥esmprosas.cer
```



- 例では C:¥temp に esmprosas.cer が作成されます。あらかじめ C:¥temp フォルダを作成してください。
- makecert.exe を利用する方法では、証明書の作成から登録までを自動で実行します。
- 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)

[http://msdn.microsoft.com/ja-jp/library/bfskty3\(v=vs.100\).aspx](http://msdn.microsoft.com/ja-jp/library/bfskty3(v=vs.100).aspx)

・ ESMPRO/ServerManager を利用する方法

ESMPRO/ServerManager をインストールしている管理 PC で、証明書を作成します。

管理 PC に管理者権限のあるアカウントでサインイン(ログオン)し、コマンドプロンプトで以下のコマンドを実行してください。

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：監視対象サーバーの 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。

■ 証明書の登録

ESMPRO/ServerAgentService をインストールしている監視対象サーバーで、Microsoft 管理コンソール(MMC)から証明書を登録してください。



makecert.exe を利用する方法のときは、「■ 証明書の登録」は不要です。次項の「■ 証明書の確認」以降の手順に従ってください。

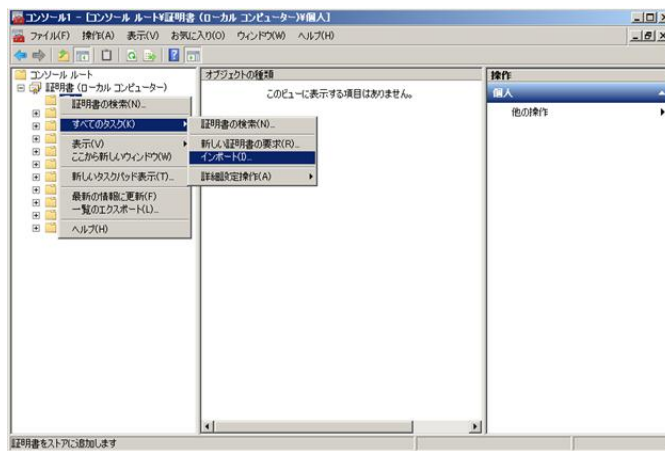
1. 監視対象サーバーに証明書を格納します。
2. [ファイル名を指定して実行]で"mmc"と入力し、[OK]をクリックします。
3. メニューの[ファイル]-[スナップインの追加と削除]をクリックします。
4. [利用できるスナップイン]から[証明書]を選択し、[追加]をクリックします。
5. [証明書スナップイン]で[コンピューター アカウント]を選択し、[次へ]をクリックします。

6. [ローカルコンピュータ]を選択し、[完了]をクリックします。
7. [選択されたスナップイン]に[証明書(ローカル コンピュータ)]が追加されたことを確認し、[OK]をクリックします。
8. [証明書(ローカルコンピュータ)]-[個人]を選択し、マウスの右ボタンをクリックします。



認証局(CA)によって署名された証明書を入手したときは、[証明書(ローカルコンピュータ)]-[信頼されたルート証明機関]を選択し、右クリックしてください。

9. [すべてのタスク]-[インポート]をクリックします。



10. 表示されたウィンドウに従い、作成した証明書を指定します。
11. 秘密キーのパスワードを入力します。
12. [証明書をすべて次のストアに配置する]を選択し、[次へ]をクリックします。
13. [完了]ボタンをクリックします。

■ 証明書の確認

登録した証明書の拇印を確認してください。

・ makecert.exe を利用しないで証明書を登録したとき

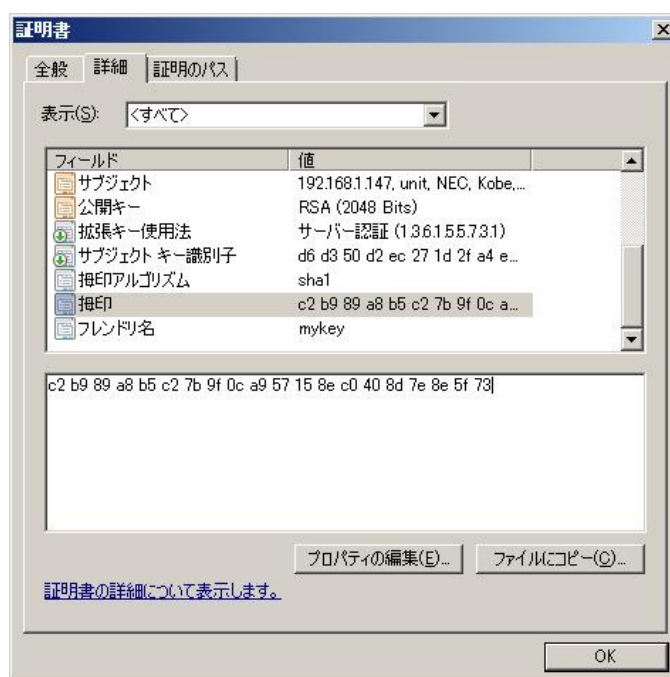
Microsoft 管理コンソール(MMC)から登録した証明書の拇印を確認してください。

1. [証明書(ローカルコンピュータ)]-[個人]-[証明書]で「■ 証明書の登録」で登録した証明書を選択します。



信頼されたルート証明機関から証明書を入手したときは、[証明書(ローカルコンピュータ)]-[信頼されたルート証明機関]-[証明書]から証明書を選択してください。

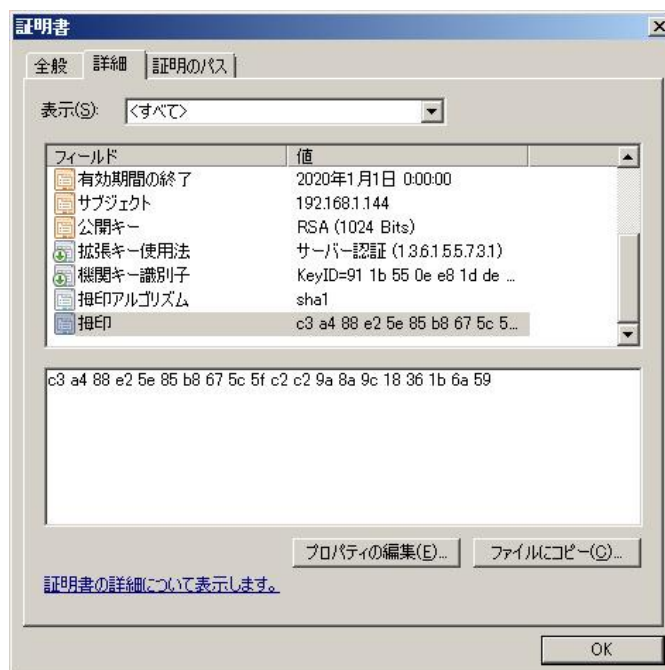
2. 証明書をダブルクリックし、[詳細]タブを選択します。
3. [拇印]を選択し、表示される値をコピーして、メモ帳などに保存します。



・ makecert.exe を利用して証明書を登録したとき

ESMPRO/ServerAgentService をインストールしている監視対象サーバーで、証明書を確認してください。

1. [ファイル名を指定して実行]で"mmc"と入力し、[OK]をクリックします。
2. メニューの[ファイル]-[スナップインの追加と削除]をクリックします。
3. [利用できるスナップイン]から[証明書]を選択し、[追加]をクリックします。
4. [証明書スナップイン]で[コンピューター アカウント]を選択し、[次へ]をクリックします。
5. [ローカルコンピュータ]を選択し、[完了]をクリックします。
6. [選択されたスナップイン]に[証明書(ローカル コンピュータ)]が追加されたことを確認し、[OK]をクリックします。
7. [証明書(ローカルコンピュータ)]-[個人]-[証明書]で「■自己署名証明書の作成」で作成した証明書を選択します。
8. 証明書をダブルクリックし、[詳細]タブを選択します。
9. [拇印]を選択し、表示される値をコピーして、メモ帳などに保存します。



■HTTPS Listener の作成

ESMPRO/ServerAgentService をインストールしているサーバー上で、WS-MAN 通信で HTTPS 接続ができるように HTTPS Listener を作成してください。

1. 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ます。その際、「■証明書の確認」で確認した拇印の値を使います。

```
winrm create winrm/config/Listener?Address=*&Transport=HTTPS @{Hostname="監視対象サーバーの IP アドレス";CertificateThumbprint="拇印の値"}
```

例：監視対象サーバーの IP アドレスが 192.168.1.1 のとき

```
winrm create winrm/config/Listener?Address=*&Transport=HTTPS  
@{Hostname="192.168.1.1";CertificateThumbprint="30 ab a3 7a 87 1e 5c ea aa 3d 83 74  
d0 ba 19 46 6f 6c 37 ab"}
```

コマンド実行に成功すると、プロンプト上に以下のように表示されます。

ResourceCreated

Address = http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous

ReferenceParameters

ResourceURI = http://schemas.microsoft.com/wbem/wsman/1/config/listener

SelectorSet

Selector: Address = *, Transport = HTTPS



HTTPS Listener を設定すると、HTTP Listener は不要になります。暗号化されていない HTTP 通信を行わないよう、以下のコマンドを実行してください。

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

■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 ESMPTRO/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。

例：[名前]ESMPTRO/ServerAgentService(HTTPS)、[説明]ESMPTRO/ServerAgentService と ESMPTRO/ServerManger が HTTPS で通信するときの受信規則です。

■ESMPTRO/ServerManager の設定

自己署名証明書を使うときは、ESMPTRO/ServerManager の設定で WS-Man 通信の自己署名証明を許可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. ESMPTRO/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[許可する]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。



- 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 ログイ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
```

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
```


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。

ESMPRO/ServerAgentService Ver. 1.0

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。

ただし、この時 ESMPRO/ServerAgentService のサービスの 1 つである ESMCommonService が、正常に開始しないときがあります。この現象への対処として、以下の手順に従って「遅延開始」と「エラー時の自動再起動」を設定してください。

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. サービス一覧から[ESMCommonService]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「自動(遅延開始)」に設定します。
4. [回復]プロパティシートの[最初のエラー]と[次のエラー]を「サービスを再起動する」に設定します。
5. [OK]をクリックします。

設定により、ESMPRO/ServerAgentService の監視は、OS 稼働して 2 分程度経過後に開始となります。

■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いない構成です。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。

■シャットダウン時に登録されるイベントログ(システム)

ESMPRO/ServerAgentService をインストールした装置で、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。

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が、システムの運用に影響はありません。

■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]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。
- アラート通報機能の設定ツール(アラートマネージャ)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。
- アラート通報機能の設定ツール(アラートマネージャ)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、アラートビューアーには 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ーに表示するには、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

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した時、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、以下のとおりです。

- ・ 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、以下のとおりです。

- ・ 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。

■Microsoft SQL Server がインストールされている環境で CIM Indication 通報に失敗する

Microsoft SQL Server を ESMRPO/ServerAgentService と同一サーバーにインストールすると、ESMPRO/ServerManager への CPU 負荷監視、ファイルシステム監視、ストレージ監視の CIM Indication 通報に失敗することがあります。

Microsoft SQL Server をインストールするときは、以下の手順に従って ESMPRO/ServerAgentService をインストールするサーバーの環境変数 Path に値を追加し、OS を再起動してください。

1. 「コントロールパネル」の[システム]を選択します。
2. [システムの詳細設定]を選択します。
3. [環境変数]を選択します。
4. [システム環境変数]の[Path]を選択し、[編集]をクリックします。
5. [システム変数の編集]画面で、[変数値]に";"で区切って以下の値を追加します。

64bit OS の場合(※1)

%EsmDir%\bin\x64

32bit OS の場合(※2)

%EsmDir%\bin\x86

6. [OK]をクリックして[システム変数の編集]画面を閉じます。
7. [OK]をクリックして[環境変数]画面を閉じます。
8. [OK]をクリックして[システムのプロパティ]画面を閉じます。
9. OS を再起動します。

(※1) Windows Server 2008 64-bit、Windows Server 2008 R2、Windows Server 2012

Windows Server 2012 R2、Windows 7 64-bit、Windows 8 64-bit、Windows 8.1 64-bit

(※2) Windows Server 2008 32-bit、Windows 7 32-bit、Windows 8 32-bit、Windows 8.1 32-bit

■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。

- 設定ツール(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 7 (x64) / Windows Server 2008 R2 への更新プログラムの適用

ESMPRO/ServerAgentService をインストールしている環境に、Windows 7 (Service Pack 1) / Windows Server 2008 R2 (Service Pack 1)、または更新プログラムを適用するときは、「KB2487426」の更新プログラムを先に適用してください。「KB2487426」を適用しないと、OS 再起動時に ESMPRO/ServerAgentService のサービスの AP エラーが、イベントログに登録されます。ただし、再起動後の ESMPRO/ServerAgentService の動作に影響はありません。

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。
以下のサポート技術情報の修正プログラムを適用してください。

- マイクロソフト サポート技術情報 - 文書番号:2487426

<http://support.microsoft.com/kb/2487426>

更新プログラムに関する情報および適用手順の詳細は、以下にも公開しています。

■ Windows Server 2008 R2 および Windows 7 の Service Pack 1 について

<http://support.express.nec.co.jp/os/w2008r2/sp1.htm>

■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. コマンドプロンプトを「管理者として実行」で起動します。

2. 下記のコマンドを実行します。

```
winrm quickconfig -q
```

3. 下記のコマンドを実行します。

```
winrm get winrm/config/service
```

4. 以下の値が"true"になっているかを確認します。

```
- auth 配下の Basic
```

5. 確認した値が"false"になっているときは、下記の 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"}
```

6. 下記のコマンドを実行します。

```
winrm get winrm/config/service
```

7. 以下の値を確認します。

```
- AllowUnencrypted
```

8. ESMPRO/ServerManager との接続に HTTP と HTTPS のどちらを利用するかによって、以下の手順に従って 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。

■メモリリーク(Windows Server 2008)

Windows Server 2008 で、ESMPRO/ServerAgentService が動作すると、メモリリークが不定期に発生します。

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:955515

<http://support.microsoft.com/kb/955515/ja>

上記サポート技術情報の修正プログラム、または Windows Server 2008 (Service Pack 2)を適用してください。Windows Server 2008 (Service Pack 2)には、上記技術情報の修正プログラムが含まれているため、Service Pack 2 の適用を推奨します。

■メモリーリーク(Windows Server 2012)

Windows Server 2012 では、WMI サービスが含まれる Svchost.exe プロセスでメモリーリークが発生します。

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:2793908

<http://support.microsoft.com/kb/2793908/ja>

上記サポート技術情報の修正プログラムを適用してください。

■二重化システム管理

CLUSTERPRO を使った二重化システム管理を使うときは、運用/待機両系別々のローカルディスクに ESMPRO/ServerAgentService をインストールします。

2. ポート一覧

ESMPRO/ServerAgentServiceの使用ポートは以下のとおりです。

ファイアウォールを有効にするときは、必要に応じて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	不定	→	5985/tcp	HTTP
サーバー監視(WS-MAN/HTTP)		←	(80/tcp)*	
自動登録	不定	→	5986/tcp	HTTPS
サーバー監視(WS-MAN/HTTPS)		←	(443/tcp)*	
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。

[ESMPRO/ServerAgentService <-> 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。

- 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のとおりです。

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	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	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.	(Alert Manager ALIVE(S) Service)* 停止	SNMP Service 開始
4.	Alert Manager Main Service 停止	(Alert Manager ALIVE(S) Service)* 開始
5.	Alert Manager Socket(S) Service 停止	Alert Manager Main Service 開始
6.	SNMP Service 停止	Alert Manager Socket(S) Service 開始

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

iStorage NS シリーズ

ESMPRO/ServerAgentService Ver. 1.0
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)

©NEC Corporation 2015

日本電気株式会社の許可なく複製・改変などを行うことはできません。