MARS アプライアンスの管理

この章では、Cisco Security Monitoring, Analysis, and Response System（MARS）の主要なメンテナンス作業について説明します。これらの作業は、MARS システム全般の状態および精度に影響するので、作業を実行するための運用計画およびプロセスを検討する必要があります。この章で説明する内容は、次のとおりです。

MARS アプライアンスのその他のすべての設定および管理作業については、使用する製品に応じて、『*User Guide for Cisco Security MARS Global Controller Version 4.1.x*』または『*User Guide for Cisco Security MARS Local Controller Version 4.1.x*』を参照してください。

コマンドラインでの管理作業の実行

ここでは、MARS アプライアンスへのコンソール接続を使用して実行する、基本的な管理作業について説明します。内容は、次のとおりです。

コンソールからのアプライアンスへのログイン

MARS アプライアンスを起動すると、コンソール サービスが開始され、ユーザにログイン プロンプトが表示されます。正常にログインすると、CLI（コマンドライン インターフェイス）を実行するコマンドライン アプリケーション（シェル）が起動します。

コンソール接続により MARS アプライアンスにログインする手順は、次のとおりです。

ステップ 1　MARS アプライアンスへのコンソール接続を確立します。方法および詳細は、「コンソール接続の確立」（p.5-6）を参照してください。

ステップ 2　`login:` プロンプトで、MARS アプライアンスの管理者の名前を入力します。

ステップ 3　`password:` プロンプトで、MARS アプライアンスのパスワードを入力します。

結果：次の形式のシステム プロンプトが表示されます。

```
Last login: Tue Jul  5 05:57:31 2005 from <host>.<domain>.com

  Cisco Security MARS - Mitigation and Response System

    ? for list of commands

[pnadmin]$
```

（注）　コンソール接続の権限がある MARS アプライアンスのログイン証明書（管理者名およびパスワード）は、1 セットだけです。

ヒント　コンソール接続を終了するには、コマンド プロンプトに **exit** を入力します。

アプライアンスの管理者パスワードのリセット

管理者名 *pnadmin* と対応するパスワードで構成された MARS アプライアンスの管理者証明書は、常に 1 セットです。他の MARS 管理者アカウントと異なり、この特別な管理者アカウントには全権限が与えられているので、削除できません。

ここでは、既存の証明書でログインしたあと、パスワードをリセットする手順について説明します。ログイン用の既存の MARS アプライアンス管理者ログイン証明書を使用できない場合、唯一の回復方法は、アプライアンスのイメージを再作成し、出荷時のパスワードにリセットすることです。最初にログインできない場合の、管理者ログインおよびパスワードのリセット方法の詳細については、「回復の管理」（p.6-31）を参照してください。

MARS アプライアンスの管理者ログイン証明書をリセットする手順は、次のとおりです。

ステップ 1　MARS アプライアンスにログインします。詳細は、「コンソールからのアプライアンスへのログイン」（p.6-2）を参照してください。

ステップ 2　システム プロンプトに、**passwd** と入力し、**Enter** を押します。

結果 : MARS アプライアンスに、次のプロンプトが表示されます。

```
New password:
```

ステップ 3　新しいパスワードを入力し、**Enter** を押します。

（注）　新しいパスワードには、管理者のアカウント名を使用すべきではありません。最低 6 文字で構成し、少なくとも 3 つの文字タイプ（数字、特殊文字、大文字、小文字）が含まれている必要があります。許容されるパスワードの例：1PaSsWoRd、*password44、Pass*word

MARS アプライアンスに、次のプロンプトが表示されます。

```
Retype new password
```

ステップ 4　新しいパスワードを再入力し、**Enter** を押します。

結果 : MARS アプライアンスにコマンド プロンプトが表示され、パスワードが変更されます。

コンソールでのアプライアンスのシャットダウン

コンソール接続経由で、アプライアンスをリモートでシャットダウンできます。ただし、アプライアンスを起動するには、装置に物理的にアクセスする必要があります。アプライアンスの電源投入の詳細については、「アプライアンスの電源投入」（p.4-13）を参照してください。

注意　電源スイッチだけを使用して、MARS アプライアンスの電源をオフにすると、データの損失または破壊の原因になります。ここに記載されている手順で、MARS アプライアンスをシャットダウンしてください。

コンソールから MARS アプライアンスをシャットダウンする手順は、次のとおりです。

ステップ 1　MARS アプライアンスにログインします。詳細は、「コンソールからのアプライアンスへのログイン」（p.6-2）を参照してください。

ステップ 2　システム プロンプトに、**shutdown** と入力し、**Enter** を押します。

ステップ 3　シャットダウンを確認する `Are you sure you want to shut down? (Y/N)` プロンプトで、**Y** を入力し、**Enter** を押します。

結果：MARS アプライアンス の電源がオフになります。

コンソールでのアプライアンスのログオフ

コンソールでログオフすると、管理者セッションが正常に終了します。セキュリティを確保するために、コンソールを使用しないときはログオフすることを推奨します。

コンソール上で MARS アプライアンスからログオフする手順は、次のとおりです。

ステップ 1　システム プロンプトに、**exit** と入力します。

ステップ 2　**Enter** を押します。

結果：コンソール接続が終了し、`login:` プロンプトが再表示されます。

コンソールでのアプライアンスのリブート

状況により、アプライアンスの手動でのリブートが必要になることがあります。たとえば、サービスが停止し、リブートにより再開できる場合などです。リブートを実行すると、サービスが安全にシャットダウンされたあと、アプライアンスが再起動します。

コンソール上で MARS アプライアンスをリブートする手順は、次のとおりです。

ステップ 1　MARS アプライアンスにログインします。詳細は、「コンソールからのアプライアンスへのログイン」（p.6-2）を参照してください。

ステップ 2　システム プロンプトに、**reboot** と入力し、**Enter** を押します。

結果：MARS アプライアンスに、次のメッセージが表示されます。

```
Are you sure you want to reboot? (Y/N)
```

ステップ 3　**Y** を入力し、**Enter** を押します。

結果：MARS アプライアンスがリブートします。リブートが完了すると、`login:` プロンプトが再表示されます。

コンソールでのアプライアンス サービス ステータスの判別

コンソール接続を使用して、システムおよびサービスのステータス情報を取得できます。

MARS アプライアンスのサービス ステータスを判別する手順は、次のとおりです。

ステップ 1　MARS アプライアンスにログインします。詳細は、「コンソールからのアプライアンスへのログイン」（p.6-2）を参照してください。

ステップ 2　システム プロンプトに、**pnstatus** と入力し、**Enter** を押します。

システムに、次のステータス情報が表示されます。

```
Module                          State           Uptime
DbIncidentLoaderSrv             RUNNING         24-00:56:29
device_monitor                  RUNNING         24-00:56:30
discover                        RUNNING         24-00:56:30
graphgen                        RUNNING         04:22:42
pnarchiver                      RUNNING         24-00:56:31
pndbpurger                      RUNNING         24-00:56:30
pnesloader                      RUNNING         24-00:56:31
pnids40_srv                     RUNNING         24-00:56:30
pnids50_srv                     RUNNING         24-00:56:30
pniosips_srv                    RUNNING         24-00:56:30
pnmac                           RUNNING         24-00:56:31
pnparser                        RUNNING         24-00:56:30
process_event_srv               RUNNING         24-00:56:31
process_inlinerep_srv           RUNNING         24-00:56:31
process_postfire_srv            RUNNING         24-00:56:31
process_query_srv               RUNNING         24-00:56:31
superV                          RUNNING         24-00:56:33
```

表示されるステート：

- **RUNNING** サービスを運用中です。
- **STOPPED** サービスは運用されていません。

コンソールでのアプライアンス サービスの停止

すべての MARS アプライアンスサービスをコンソールから停止できます。サービスとそのステータスを表示するには、**pnstatus** コマンドを使用します。詳細は、「コンソールでのアプライアンス サービス ステータスの判別」（p.6-5）を参照してください。

MARS アプライアンス上のすべてのサービスを停止する手順は、次のとおりです。

ステップ 1　MARS アプライアンスにログインします。詳細は、「コンソールからのアプライアンスへのログイン」（p.6-2）を参照してください。

ステップ 2　**pnstop** と入力します。

ステップ 3　**Enter** を押します。

結果：システムに、すぐにメッセージが表示されます。

```
Please Wait . . .
```

コマンドが完了したことを示すプロンプトが表示されます。

ステップ 4　サービスのステータスを確認するには、**pnstatus** を入力します。

superV サービスは停止しません。このサービスは、他のサービスをモニタし、必要に応じて再開します。

コンソールでのアプライアンス サービスの開始

サービスが停止した場合、コンソールからすべての MARS アプライアンス サービスを手動で開始できます。サービスとそのステータスを表示するには、**pnstatus** コマンドを使用します。詳細は、「コンソールでのアプライアンス サービス ステータスの判別」（p.6-5）を参照してください。

停止しているすべての MARS サービスを開始する手順は、次のとおりです。

ステップ 1　MARS アプライアンスにログインします。詳細は、「コンソールからのアプライアンスへのログイン」（p.6-2）を参照してください。

ステップ 2　**pnstart** と入力します。

ステップ 3　**Enter** を押します。

結果：システム プロンプトが消去されたあと、サービスの再開を示すプロンプトが表示されます。

ステップ 4　サービスのステータスを確認するには、**pnstatus** を入力します。

コンソールでのシステム ログの表示

ここでは、**pnlog show** コマンドを実行する手順について説明します。このコマンドではログのステータスが表示されるので、サポート担当者はコマンド出力を分析用に使用できます。

pnlog コマンドの詳細は、付録 A「コマンド リファレンス」の「pnlog」（p.A-17）を参照してください。次に、**pnlog show** コマンドの構文を示します。

```
pnlog show <gui|backend|cpdebug>
```

オプションにより、バックエンドで特定のログファイルが出力されます。3 種類のログを表示できます。HTML インターフェイス ログ、バックエンド ログ（**pnstatus** コマンドの報告プロセスのログ）、および CheckPoint デバッグ ログです。このコマンドを停止するには、Ctrl + C または ^C を押します。

cpdebug を使用する場合には、`pnlog setlevel` を `0` より大きい値に設定しておく必要があります。デフォルト値は 0 で、CPE デバッグ メッセージはオフです。

ログおよびシステム レジストリ情報の .cab ファイルを生成する手順は、次のとおりです。

ステップ 1　MARS アプライアンスにログインします。詳細は、「コンソールからのアプライアンスへのログイン」（p.6-2）を参照してください。

ステップ 2　**pnlog show** および対応する引数を入力します。

ステップ 3　**Enter** を押します。

結果：コンソールに、実行したコマンドの出力がスクロール表示されます。

ステップ 4　任意の時点で出力を停止するには、**Ctrl + C** を押します。

結果：システム プロンプトに戻ります。

アプライアンス ソフトウェアのアップグレードのチェックリスト

MARS アップグレード パッケージは、ソフトウェアのメジャー、マイナー、およびパッチ リリースの主要ツールです。MARS アプライアンスの管理者は、毎週、アップグレード サイトにアクセスし、パッチがアップグレードされていないかどうかを確認する必要があります。優先順位の高い修正に加え、パッチ アップグレード パッケージには、システム検査ルールとイベント タイプの更新、および最新のシグニチャ サポートが含まれています。

注意　MARS アプライアンスのハードウェア コンポーネントのアップグレードは行わないでください。身体損傷の原因になり、サポート契約が無効になります。ハードウェアのアップグレードが必要な場合には、シスコシステムズの代理店に相談してください。

次のチェックリストに、MARS アプライアンスを最新バージョンにアップグレードするために必要な手順を示します。各作業には、いくつかの手順が含まれていることがあります。作業および手順は、順序どおりに実行する必要があります。このチェックリストには、各作業を実行するための特定手順の参照先が示されています。

✓	作業
❑	**1. MARS アプライアンスをアップグレードするか、またはイメージを再作成するかを判別します。** MARS アプライアンスを最新のソフトウェア リリースにするには、2 つの方法があります。アップグレードまたはイメージの再作成です。最新リリースにするために必要な手順は、どちらの方法を使用するかによって、かなり異なります。 • *現在のコンフィギュレーションおよびイベント データを保持して、MARS アプライアンスを最新リリースにアップグレードする場合*：コンフィギュレーションおよびイベント データを保持するには、このチェックリストの作業に従ってアップグレードを実行する必要があります。作業 2 に進みます。 • *現在のコンフィギュレーションおよびイベント データを保持しないで、MARS アプライアンスのイメージを最新リリースに再作成する場合*：コンフィギュレーションおよびイベント データを保持する必要がない場合には、最新の ISO イメージを使用してアプライアンスのイメージを再作成できます。アプライアンスのイメージを再作成する手順は、「回復の管理」（p.6-31）を参照してください。 *結果*：MARS アプライアンスのアップグレードまたはイメージ再作成のどちらを実行するかが決まります。
❑	**2. 実行中のバージョンを判別します。** アプライアンスをアップグレードする前に、現在実行中のバージョンを判別する必要があります。次のいずれかの方法で判別できます。 • **HTML インターフェイス —** HTML インターフェイスのバージョンを判別するには、**Help > About** を選択します。 • **CLI —** CLI のバージョンを判別するには、MARS コマンド プロンプトに **version** を入力します。 バージョン形式は、`x.y.z (build_number)` です。例：`3.4.1 (1922)` **（注）** 3.2.2 より前のバージョンを実行している場合には、適切なアップグレード ファイルの入手情報について、シスコシステムズのサポートに問い合わせてください。3.2.2 以上を実行している場合には、このチェックリストの指示に従ってください。 *結果*：アプライアンスで実行中のバージョンが判別し、シスコ社のサポートに連絡する必要があるか、またはこのチェックリストの作業を続けるかが決定します。

✓	作業
❑	**3. アップグレードのメディアを判別します。** アプライアンスをアップグレードする前に、使用するメディアを判別する必要があります。メディアの選択により、CLI からアップグレードする必要があるかどうかが判別されます。 • **CD-ROM —** アップグレードを実行するには、ソフトウェアをダウンロードし、イメージを CD-ROM に保存する必要があります。この CD-ROM を MARS アプライアンスの DVD ドライブに挿入して、アップグレードを実行します。CD-ROM をメディアとして使用する場合には、各アプライアンスを個別にアップグレードし、CLI を使用する必要があります。 • **Internal Upgrade Server —** 使用する Internal Upgrade Server を識別します。アップグレードを実行する前に、ソフトウェア イメージを、内部 HTTP、HTTPS、または FTP サーバにダウンロードする必要があります。この内部サーバから、MARS アプライアンスをアップグレードします。各 MARS アプライアンスが迅速かつ安全にアップデートをダウンロードできるように、このサーバは特定の要件を満たしている必要があります。Internal Upgrade Server を使用する場合、特に注記がなければ、CLI または HTML インターフェイスを使用してアップグレードできます。 **（注）** 3.4.1 より前のバージョンを実行している場合、アップグレードに HTML インターフェイスを使用できません。3.4.1 より前のバージョンでは、HTML インターフェイスは、upgrade.protegonetworks.com サポート サイトへの接続専用となりますが、このサイトは現在利用できません。3.4.1 より前のバージョンからアップグレードする場合には、CLI を使用する必要があります。 *結果*：アップグレードに使用するメディアが決まります。Internal Upgrade Server を使用する場合には、サーバを識別して準備し、アップグレード対象の各スタンドアロン Local Controller または Global Controller からサーバにアクセスできることを確認します。Internal Upgrade Server とアプライアンスの間でプロキシ サーバを使用する場合、アップグレードを実行する前に、これらの設定を行う必要があります。 詳細の参照先： • アップグレード用 CD-ROM の作成（p.6-11） • Internal Upgrade Server の準備（p.6-11）
❑	**4. 必要なアップグレード パスおよび制限事項を把握します。** アプライアンスを特定のソフトウェア バージョンからアップグレードする場合、累積的なアップグレード パスに従う必要があります。アプライアンスで実行中のバージョンから、アップグレード対象のバージョンまでの間にある各アップグレード パッケージを、順番に適用しなければなりません。必要なアップグレード パスを、表 6-1 で確認してください。 また、Global Controller と、モニタ対象の Local Controller との間には、制約があります。Global Controller は、同じバージョンを実行している Local Controller だけをモニタできます。旧バージョンのソフトウェアを実行している Local Controller をモニタしようとしても、その Local Controller は、Global Controller に対してオフラインになります。ただし、MARS には、Global Controller がモニタ対象の Local Controller に同じアップグレード バージョンプッシュするというアップグレード オプションがあるので、Global Controller のユーザ インターフェイスからアップグレード プロセスを管理できます。 これで、ダウンロードする必要があるすべてのアップグレード パッケージを把握できます。 詳細の参照先： • 必要なアップグレード パスの判別（p.6-12）

✓	作業
❑	**5. Cisco.com Web サイトから、必要なすべてのアップグレード パッケージをダウンロードします。** ダウンロードするアップグレード パッケージを識別したら、Cisco.com アカウントを使用して Cisco.com にログインし、各種パッケージをダウンロードします。アップグレード パッケージをダウンロードするには、MARS アプライアンスの有効な SMARTnet サポート契約が必要です。 手順 3 での選択に応じて、これらのファイルを Internal Upgrade Server に保存するか、または CD-ROM イメージに保存します。 *結果*：実行中のバージョンから最新バージョンにアップグレードするために必要なすべてのアップグレード パッケージが、Internal Upgrade Server または CD-ROM の既知のパス上に保存されます。 詳細の参照先： • Cisco.com からのアップグレード パッケージのダウンロード（p.6-12）
❑	**6. 使用するアップグレード方法を理解します。** 次のアップグレード オプションから選択します。 **（注）** 3.4.1 より前のバージョンを実行している場合には、CLI からアップグレードできるオプションを選択する必要があります。 • Internal Upgrade Server に直接接続しているアプライアンスからのアップグレード（CLI または HTML インターフェイス） • プロキシ経由で Internal Upgrade Server に接続しているアプライアンスからのアップグレード（CLI または HTML インターフェイス） • プロキシ サーバ経由で、または直接 Internal Upgrade Server に接続している Global Controller を使用した、Local Controller のアップグレード（HTML インターフェイスのみ） • コマンドラインでの CD-ROM からのアップグレード（CLI のみ） *結果*：選択したメディアおよび現在実行中のバージョンに応じて、適切なアップグレード方法が決まります。
❑	**7. 必要なプロキシ サーバ設定を識別します。** ネットワーク上のアプライアンスと Internal Upgrade Server との間にプロキシ サーバが置かれている場合には、プロキシ サーバの設定を識別する必要があります。HTML インターフェイスを使用してアップグレードする場合には、**Admin > System Parameters > Proxy Settings** ページを使用して、これらの設定を指定できます。それ以外の場合には、アップグレード実行中にコマンドラインで指定できるように、設定を書き留めます。 **（注）** HTML インターフェイスでプロキシ サーバ設定を指定できるのは、バージョン 3.4.1 以上です。CLI を使用する場合には、バージョン 2.5.1 以上でプロキシ サーバ設定を指定できます。 *結果*：HTML インターフェイスでプロキシ サーバ設定を指定するか、以降で指定するために設定を書き留めます。 詳細の参照先： • Global Controller または Local Controller のプロキシ設定の指定（p.6-13）

✓	作業
❑	**8. アップグレード パスに従って、アプライアンスを次のバージョンにアップグレードします。** アプライアンス上で、手順 6 で選択した方法を使用し、手順 5 の結果に基づいて、希望のバージョンまで段階的にアップグレードを実行します。 *結果*：必要な各アップグレード パッケージの適用が完了します。 詳細の参照先： • ユーザ インターフェイスからの Global Controller または Local Controller のアップグレード（p.6-14） • CLI からのアップグレード（p.6-15） • Global Controller からの Local Controller のアップグレード（p.6-17）

アップグレード用 CD-ROM の作成

アップグレード用 CD-ROM の作成には、特別な要件はありません。複数のアップグレード パッケージが必要な場合、各パッケージは通常、約 200 MB なので、1 枚の CD にアップグレード パッケージを 3 種類まで保存できます。

（注）　アップグレード パッケージは、順次番号に従って順番に適用する必要があります。1 つのアップグレードが終了すると、アプライアンスはリブートします。1 つのアップグレードを完了し、システムが再起動して、次のパッチを適用できるようになるまで、30 ～ 40 分かかることがあります。

Internal Upgrade Server の準備

Internal Upgrade Server の要件は、選択したアップグレード オプションおよびアプライアンスで実行中のバージョンによって異なります。

（注）　MARS では、Internal Upgrade Server でユーザ認証を実行する必要があります。したがって、HTTP、HTTPS、または FTP 経由でサーバにアクセスする場合、認証用のユーザ名とパスワードを指定する必要があります。また、プロキシ サーバを経由する場合には、サーバでインライン認証を実行する必要があります。

バージョン 2.5.1 以上の CLI を使用するアップグレードの場合、次の要件を満たすように、Internal Upgrade Server を設定する必要があります。

- FTP、HTTP、または HTTPS サーバである。
- ユーザ認証を必要とする。
- MARS アプライアンスからの接続を受け入れる。
- ユーザ認証を必要とするプロキシ サーバ経由で接続する。

バージョン 3.4.1 以上の HTML インターフェイスを使用するアップグレードの場合、次の要件を満たすように、Internal Upgrade Server を設定する必要があります。

- HTTPS または FTP サーバである。
- ユーザ認証を必要とする。
- MARS アプライアンスからの接続を受け入れる。
- ユーザ認証を必要とするプロキシ サーバ経由で接続する。プロキシ サーバは、アップグレードの実行前に、HTML インターフェイスで設定されている必要があります。

必要なアップグレード パスの判別

1 つのソフトウェア バージョンから別のバージョンにアップグレードする場合、必須バージョンが必要になります。必須バージョンとは、最新バージョンにアップグレードするときに、アプライアンス上で実行している必要がある最低限のレベルです。表 6-1 に、最新バージョンに直接アップグレードできる必須バージョンに到達するまでの、アップグレード パスを示します。

表 6-1　アップグレード パスの表

現行バージョン	アップグレード対象[1]	アップグレード パッケージ
2.5.6 より前のリリース	シスコ社のサポートに連絡	適用外
2.5.6	3.1.1*	pn-3.1.1.pkg
3.1.1	3.2.1*	pn-3.2.1.pkg
3.2.1	3.2.2*	pn-3.2.2.pkg
3.2.2 または 3.3.2 ベータ版	3.3.3*	pn-3.3.3.pkg
3.3.3	3.3.4*	pn-3.3.4.pkg
3.3.4	3.3.5*	pn-3.3.5.pkg
3.3.5	3.4.1*	pn-3.4.1.pkg
3.4.1	3.4.2	pn-3.4.2.pkg
3.4.2	3.4.3	pn-3.4.3.pkg
3.4.3	3.4.4	pn-3.4.4.pkg
3.4.4	4.1.1	csmars-4.1.1.pkg
4.1.1	4.1.2 (2042) + スクリプト コマンド	csmars-4.1.2.pkg[2]
4.1.2 (2040) エラーなし	4.1.2 (2042)	csmars-4.1.2.pkg[2]
4.1.2 (2042)	4.1.3	csmars-4.1.3.pkg
4.1.3	4.1.4	csmars-4.1.4.pkg

1. パッケージ名の横のアスタリスク（*）は、upgrade.proteogonetwork.com サイトの終了により HTML インターフェイスがサポートされないため、コマンドラインからアップグレードする必要があることを示しています。
2. 4.1.1 または 4.1.2 (2040) から 4.1.2 (2042) にアップグレードする場合には、『*Quick Install and Release Notes for Cisco Security MARS Appliance 4.1.2 (2042)*』に記載されている特殊なアップグレードの注意事項を参照してください。

Cisco.com からのアップグレード パッケージのダウンロード

アップグレード イメージおよびサポート ソフトウェアは、MARS 専用の Cisco.com ソフトウェア ダウンロード ページに提供されています。有効な Cisco.com アカウントがあり、MARS アプライアンスの SMARTnet 契約番号が登録されていれば、次の URL からダウンロード ページにアクセスできます。

- トップレベル ページ：http://www.cisco.com/cgi-bin/tablebuild.pl?topic=279644034
- アップグレードファイル：http://www.cisco.com/cgi-bin/tablebuild.pl/cs-mars
- リカバリ イメージ：http://www.cisco.com/cgi-bin/tablebuild.pl/cs-mars-recovery
- サポート ファイル：http://www.cisco.com/cgi-bin/tablebuild.pl/cs-mars-misc

（注）　Cisco.com　に提供されているバージョンよりも前のバージョンからアップグレードする場合には、必要なイメージの入手方法について、シスコシステムズのサポートにお問い合わせください。アップグレード パスの中間バージョンを飛ばしてアップグレードしないでください。

Cisco.com アカウントの取得方法は、次の URL を参照してください。

- http://www.cisco.com/en/US/applicat/cdcrgstr/applications_overview.html

Global Controller または Local Controller のプロキシ設定の指定

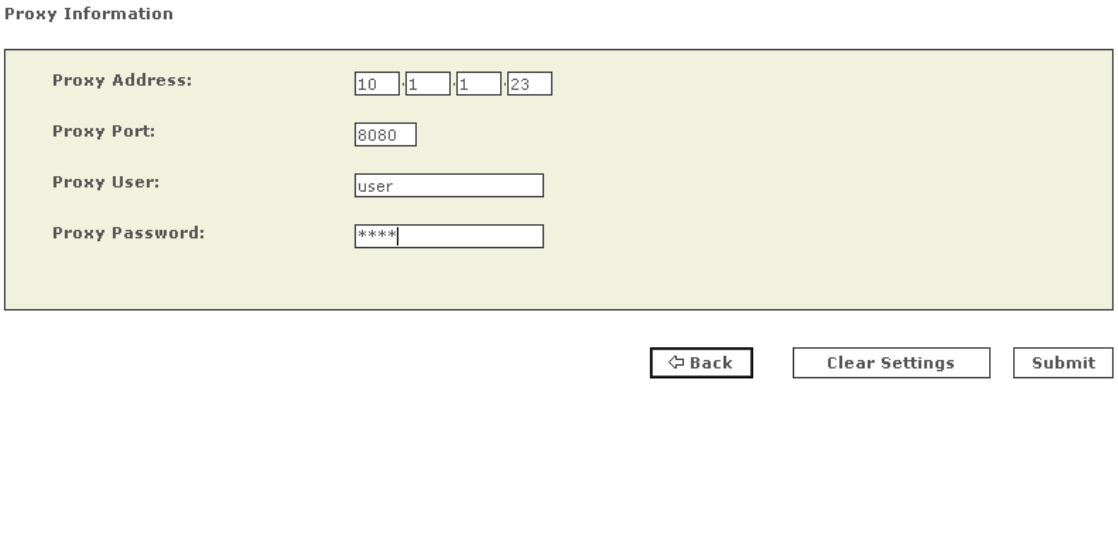
アプライアンスから Internal Upgrade Server に直接アクセスできない場合には、プロキシ設定を指定できます。ここでは、アプライアンスの関連ユーザ インターフェイスからアプライアンスをアップグレードすることを前提に、プロキシ設定の指定方法について説明します。Global Controller のユーザ インターフェイスから Local Controller をアップグレードする場合の詳細は、「Global Controller からの Local Controller のアップグレード」（p.6-17）を参照してください。

（注）　この手順は、バージョン 3.4.1 以上に適用されます。

プロキシ設定を指定する手順は、次のとおりです。

ステップ 1　ブラウザで、MARS ユーザ インターフェイスを起動します。

ステップ 2　**Admin > System Parameters > Proxy Settings** を選択します。



132536

ステップ 3　Proxy Address および Proxy Port フィールドに、アプライアンスと Internal Upgrade Server の中間にあるプロキシ サーバのアドレスおよびポートを入力します。

ステップ 4　Proxy User フィールドに、プロキシ サーバへの認証用としてアプライアンスが使用するユーザ名を指定します。

（注）　このユーザ名とパスワードの組み合わせは、Cisco.com または Internal Upgrade Server のログイン名およびパスワードとは異なります。MARS は、プロキシ サーバでのインライン ユーザ認証を必要とします。したがって、プロキシ サーバで認証されるユーザ名とパスワードを指定する必要があります。

ステップ 5　Proxy Password フィールドに、入力したユーザ名に関連付けられたパスワードを指定します。

ステップ 6　**Submit** をクリックして、変更を保存します。

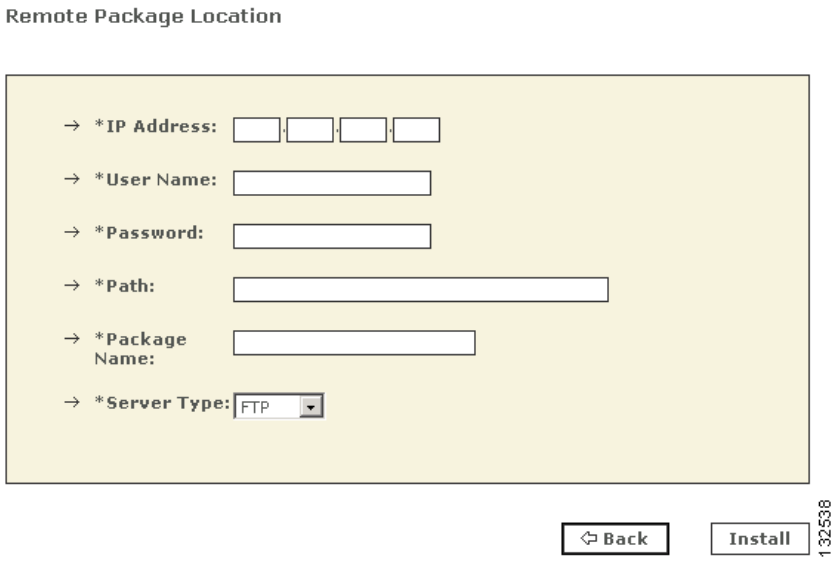
ユーザ インターフェイスからの Global Controller または Local Controller のアップグレード

（注）　この手順は、バージョン 3.4.1 以上に適用されます。

ユーザ インターフェイスからアプライアンスをアップグレードする手順は、次のとおりです。

ステップ 1　ブラウザで、MARS ユーザ インターフェイスを起動します。

ステップ 2　**Admin > System Maintenance > Upgrade** を選択します。



ステップ 3　IP Address フィールドに、アップグレード パッケージ ファイルが保存されているサーバのアドレスを入力します。

ステップ 4　User Name および Password フィールドに、Internal Upgrade Server のログイン情報を入力します。

（注）　MARS では、Internal Upgrade Server でユーザ認証を実行する必要があります。したがって、サーバで認証されるユーザ名およびパスワードの組み合わせを指定する必要があります。

ステップ 5　Path フィールドに、使用したサーバ アクセスのタイプに関連した、パッケージ ファイルの保存場所へのパスを指定します。

ステップ 6　Server Type ボックスで、対応するプロトコルを選択します。

インストール パッケージは、HTTPS または FTP のいずれかを使用してダウンロードできます。

ステップ 7　Package Name フィールドに、ダウンロードしたパッケージ ファイルの完全名を指定します。

ステップ 8　**Download** をクリックします。

結果 : パッケージのサイズによって、ダウンロードに多少時間がかかることがあります。ダウンロードが完了すると、Install ボタンがアクティブになります。

ステップ 9　**Install** をクリックします。

結果 : Install をクリックすると、システムでのアップグレード処理に多少時間がかかります。アップグレードが完了すると、システムはリブートします。また、アップグレード実行中に、ユーザ インターフェイスも再起動します。

CLI からのアップグレード

Internal Upgrade Server に接続し、HTTP または HTTPS を使用してアップグレードを完了できます。または、FTP サーバにアップグレード パッケージをダウンロードして、アップグレードを実行できます。アップグレード コマンドの詳細については、「pnupgrade」（p.A-24）を参照してください。

CLI を使用してアップグレードを実行する手順は、次のとおりです。

ステップ 1　コンソール ポートまたは SSH 接続を使用して、アプライアンスにログインします。

ステップ 2　MARS のログイン名およびパスワードを入力します。

ステップ 3　アプライアンスが必須バージョンを実行しているかどうかを確認するために、次の CLI コマンドを実行します。

```
version
```

アプライアンスは、サポートされる必須バージョンを実行している必要があります。必要な必須バージョンについては、表 6-1 を参照してください。実行していない場合、アップグレード パスに従って、必要なバージョンを導入する必要があります。

ステップ 4　次のいずれかを実行します。

（注）　MARS では、Internal Upgrade Server でユーザ認証を実行する必要があります。したがって、HTTP、HTTPS、または FTP 経由でサーバにアクセスする場合、認証用のユーザ名とパスワードを指定する必要があります。また、プロキシ サーバを経由する場合には、サーバでインライン認証を実行する必要があります。

- アプライアンスの DVD ドライブに挿入した CD-ROM からアップグレードするには、次の CLI コマンドを実行します。

pnupgrade cdrom://*package*/**pn-***ver*.**pkg**

package は *.pkg ファイルを保存した CD 上のパス、[*ver*] は 3.3.4 など、アップグレードしたいパッケージ ファイルのバージョン番号です。

- 内部 HTTP または HTTPS サーバからアップグレードするには、次の CLI コマンドを実行します。

pnupgrade https://*upgrade.myhttpserver.com*/*upgrade*/*packages*/
pn-*ver*.**pkg [***user***] [***password***]**

または

pnupgrade http://*upgrade.myhttpserver.com*/*upgrade*/*packages*/
pn-*ver*.**pkg [***user***] [***password***]**

upgrade.myttpserver.com/*upgrade*/*packages* は、もう 1 つの *.pkg ファイルをダウンロードしたサーバ名およびパスです。*ver* は、3.3.4 などのバージョン番号、[*user*] および [*password*] は、Internal Upgrade Server のログイン名およびパスワードです。

- ファイルをダウンロードしたあと、FTP サーバからアップグレードを実行するには、次の CLI コマンドを実行します。

pnupgrade ftp://*upgrade.myftpserver.com*/*upgrade*/*packages*/
pn-*ver*.**pkg [***user***] [***password***]**

upgrade.myftpserver.com/*upgrade*/*packages* は、もう 1 つの *.pkg ファイルをダウンロードしたサーバ名およびパスです。[*ver*] は 3.3.4 などのバージョン番号、[*user*] および [*password*] は、Internal Upgrade Server のログイン名およびパスワードです。

- プロキシ サーバ経由で Internal Upgrade Server からアップグレードを実行するには、次の CLI コマンドを実行します。

pnupgrade *proxyServerIP*:*proxyServerPort* [*proxyUser*:*proxyPassword*]
https://*upgrade.myhttpserver.com*/*upgrade*/*packages*/**pn-***ver*.**pkg [***user***] [***password***]**

変数の定義は、次のとおりです。

- proxyServerIP:proxyServerPort は、アプライアンスと Internal Upgrade Server の間に置かれているプロキシ サーバに接続するための IP アドレス / ポートです。
- proxyUser:proxyPassword は、プロキシ サーバでの認証に必要なアプライアンスのユーザ名およびパスワードです。
- upgrade.myttpserver.com/upgrade/packages は、*.pkg ファイルをダウンロードしたサーバ名およびパスです。
- *ver* は、3.3.4 などのバージョン番号です。
- [*user*] および [*password*] は、Internal Upgrade Server のログイン名およびパスワードです。

結果 : ダウンロードの進行状況のパーセンテージが、バーに表示されます。ダウンロード完了後、システムがアップグレードを処理するのに、多少時間がかかります。アップグレードが完了すると、システムはリブートします。

Global Controller からの Local Controller のアップグレード

Global Controller のユーザ インターフェイスから Local Controller をアップグレードする場合、Local Controller がプロキシ サーバの背後にあるかどうかを判別する必要があります。背後にある場合、Global Controller のユーザ インターフェイスで、Local Controller 用のプロキシ設定を指定する必要があります。設定を指定したあと、通常の方法で Local Controller をアップグレードできます。

（注）　Local Controller のプロキシ情報が提供されていない場合、アプライアンス用のアップグレードをダウンロードしようとすると、Local Controller は Internal Upgrade Server に接続を試みますが、しばらくすると失敗します。

Global Controller とモニタ対象の Local Controller の両方をアップグレードする場合には、最初に Global Controller をアップグレードし、Internal Upgrade Server の情報を指定する必要があります。Global Controller は、このサーバ情報を、選択したすべての Local Controller にプッシュするので、Local Controller は Internal Upgrade Server にアクセスでき、ダウンロードおよびアップグレード処理を開始できます。Local Controller は、Global Controller からはアップグレード パッケージを検索しません。

作業を始める前に

- この手順は、バージョン 3.4.1 以上に適用されます。
- 各 Local Controller が、アップグレード前の Global Controller と同じソフトウェア バージョンを実行していることを確認してください。アップグレードする Local Controller は、アップグレード前の Global Controller が実行していた必須バージョンのソフトウェアを実行している必要があります。

（注）　Global Controller/Local Controller の両方をアップグレードする場合、アプライアンスがリブートしてから最初の 10 分間、Local Controller がオフラインとして表示されることがあります。スケジューラはリブートから 10 分後に起動し、再同期化を行います。

Local Controller がオフラインとして表示されている場合には、アプライアンスのリブート後、最低 10 分が経過しているかどうかを確認してください。または、Global Controller のユーザ インターフェイスで、**Admin > Local Controller Management** を選択し、通信を再開することもできます。

Global Controller でのプロキシ設定の指定

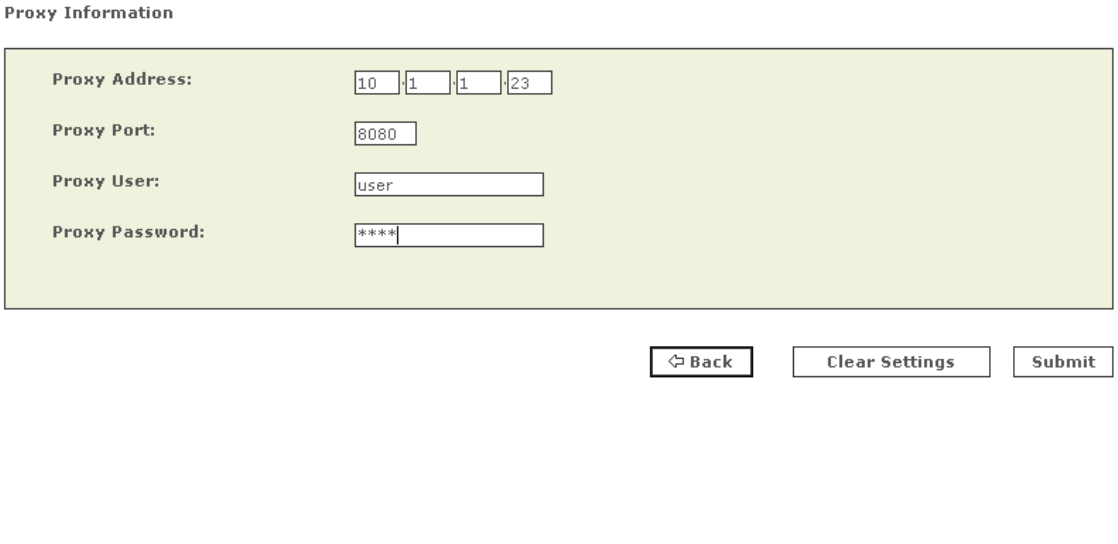
Global Controller のユーザ インターフェイスで Local Controller のプロキシ設定を指定する手順は、次のとおりです。

ステップ 1　ブラウザで、MARS ユーザ インターフェイスを起動します。

ステップ 2　**Admin > System Maintenance > Upgrade** を選択します。

ステップ 3　アップグレードしたい Local Controller の横にある **Proxy Settings** をクリックします。

結果: Global Controller のユーザ インターフェイスに、選択した Local Controller の Proxy Information ページ（**Admin > System Parameters > Proxy Settings**）が表示されます。



ステップ 4　Proxy Address および Proxy Port フィールドに、アプライアンスと Internal Upgrade Server の中間にあるプロキシ サーバのアドレスおよびポートを入力します。

ステップ 5　Proxy User フィールドに、プロキシ サーバへの認証用としてアプライアンスが使用するユーザ名を指定します。

（注）　このユーザ名とパスワードの組み合わせは、Internal Upgrade Server のログイン名とパスワードではありません。MARS では、プロキシ サーバでのインライン ユーザ認証が必要になります。したがって、プロキシ サーバで認証されるユーザ名およびパスワードの組み合わせを指定する必要があります。

ステップ 6　Proxy Password フィールドに、入力したユーザ名に関連付けられたパスワードを指定します。

ステップ 7　**Submit** をクリックして、変更を保存します。

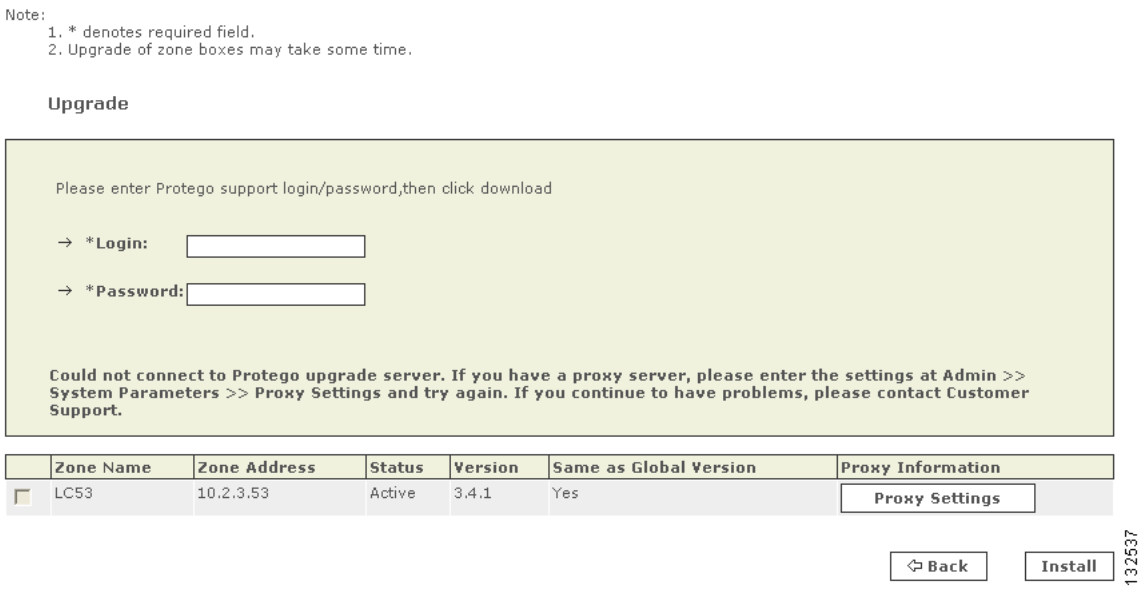
Global Controller のユーザ インターフェイスからの Local Controller のアップグレード

Global Controller のユーザ インターフェイスから、Global Controller が管理している任意の Local Controller をアップグレードできます。これにより、各アプライアンスに個別に接続しなくても、Local Controller のリストを使用して作業ができます。

ステップ 1　ブラウザで、MARS ユーザ インターフェイスを起動します。

ステップ 2　**Admin > System Maintenance > Upgrade** を選択します。

結果：アップグレード対象として選択できる Local Controller のリストが表示されます。



ステップ 3　Login および Password フィールドに、Internal Upgrade Server に割り当てた Internal Upgrade Server のログイン名およびパスワードを入力します。

（注）　MARS では、Internal Upgrade Server でユーザ認証を実行する必要があります。したがって、サーバで認証されるユーザ名およびパスワードの組み合わせを指定する必要があります。

ステップ 4　アップグレードする Local Controller の横にあるチェックボックスを選択し、**Download** をクリックします。

選択したアプライアンス用のプロキシ設定が指定されている場合には、設定を確認するためのポップアップ ウィンドウが表示されます。情報を確認し、**OK** をクリックします。プロキシ情報を指定していない場合には、**Cancel** をクリックし、Local Controller 用のプロキシ情報を入力します。詳細は、「Global Controller でのプロキシ設定の指定」（p.6-17）を参照してください。

結果 : パッケージのサイズによって、ダウンロードに多少時間がかかることがあります。ダウンロードが完了すると、Install ボタンがアクティブになります。

ステップ 5　**Install** をクリックします。

結果 : Install をクリックすると、リモート システムでのアップグレード処理に多少時間がかかります。アップグレードが完了すると、リモート システムはリブートします。また、アップグレード実行中に、ユーザ インターフェイスも再起動します。

アプライアンスのデータ バックアップの設定および実行

MARS アプライアンスからデータをアーカイブし、そのデータを使用して OS（オペレーティング システム）、システム コンフィギュレーション、ダイナミック データ（イベント データ）、またはシステム全体を復元できます。アプライアンスは、Network File System（NFS; ネットワーク ファイル システム）を使用し、外部 Network-Attached Storage（NAS）システムからデータをアーカイブして復元します。データのバックアップ時刻をスケジュール設定することはできませんが、MARS アプライアンスは毎日午前 2 時にコンフィギュレーションのバックアップを実行し、1 時間ごとにイベントをアーカイブします。コンフィギュレーションのバックアップは、完了までに数時間かかることがあります。

アーカイブをイネーブルにすると、ダイナミック データは 2 回書き込まれます。1 回はローカル データベースに、もう 1 回は NFS アーカイブに保存されます。つまり、アーカイブされるダイナミック データには、データ アーカイブ設定をイネーブルにした*あと*で、受信または生成されたデータだけが含まれます。したがって、アプライアンスがレポーティング デバイスから監査データを受信するように設定する前に、アーカイブをイネーブルにすることを推奨します。

同じ NFS サーバを使用して、複数の MARS アプライアンスのデータをアーカイブできます。ただし、アーカイブする各アプライアンスについて、NFS パスに固有のディレクトリを指定する必要があります。同じベース ディレクトリを使用すると、アプライアンスは各データを相互に書き換えるので、結果としてイメージが破壊されます。

各 MARS アプライアンスは、指定した有効期限を使用して、データをシームレスにアーカイブします。MARS の内部ストレージの容量が満杯になると、保存されているイベントおよびセッション データのおよそ 10 % にあたるデータが、ローカル データベースの最も古いパーティションから自動的に削除されます。NFS ファイル共有のデータには、指定された日数のライフ スパンが適用されます。つまり、データを 1 年間保存しておくには、Remote Storage Capcity（in Days）フィールドの値として 365 日を指定します。この場合、365 日を越えたデータはすべて、アーカイブ ファイルから削除されます。

スペース要件を検討する場合には、次のガイドラインに従ってください。1 秒間に 10 イベントを継続的に受信する場合、データを 1 年間保存するには、推定で 6 GB のストレージ容量が必要です。この推定値は、1 イベントが平均 200 バイト、圧縮係数 10 を想定しています。いずれも現実的な平均値です。

（注） データ アーカイブは、指定したアプライアンスに対してローカルです。Global Controller 上でデータ アーカイブを設定すると、そのアプライアンス用のデータがアーカイブされます。Global Controller 上で、モニタ対象の Local Controller からのデータのアーカイブを設定することはできません。

アーカイブ データの使用方法および形式の詳細については、次の項目を参照してください。

- アーカイブ データの一般的な使用方法（p.6-21）
- アーカイブ共有ファイルの形式（p.6-21）
- 復元のガイドライン（p.6-38）
- pnrestore（p.A-20）

データ アーカイブを設定するには、次の作業を実行する必要があります。

1. Windows 上での NFS サーバの設定（p.6-23）または
   Linux 上での NFS サーバの設定（p.6-27）
2. MARS アプライアンス のデータ アーカイブ設定（p.6-27）

アーカイブ データの一般的な使用方法

アーカイブの主要な用途は、破壊的なソフトウェアの障害時にアプライアンスを復元することです。そのほか、アーカイブ データには、次の使用方法があります。

- **Admin** > **System Maintenance** > **Retrieve Raw Messages** を使用し、ローカル データベースの容量を超えた時点からの履歴的な生メッセージを分析します。生メッセージから取得できるデータは、レポーティング デバイスにより提供された単純な監査メッセージです。生メッセージとは、Syslog メッセージのように、レポーティング デバイスから送信されたメッセージそのものです。
- gzip で圧縮され、アーカイブされたイベント レコードを、手動で表示します。この方法では、ローカル データベースまたはアーカイブのいずれかから生メッセージを取得するよりも、データを速く表示できます。ただし、Retrieve Raw Messages オプションにより戻される単純な生イベントに比べ、レコード形式は複雑です。メッセージをセッション、デバイス タイプ、5 タプル（送信元 IP、宛先 IP、プロトコル、送信元ポート、宛先ポート）および他のすべてのデータ ポイントに関連付けるために必要な生メッセージおよびシステム データを含め、インシデントおよび依存データを復元するために必要な全データが含まれます。詳細は、「アーカイブ共有ファイルの形式」（p.6-21）および「アーカイブしたファイル内のデータへのアクセス」（p.6-29）を参照してください。
- ハードウェア障害時にネットワークで使用できるように、または履歴期間のクエリーおよびレポート機能に完全にアクセスできるように、スタンバイまたはセカンダリ MARS アプライアンスのイメージを作成します。詳細は、「スタンバイまたはセカンダリ MARS アプライアンスの設定」（p.6-37）および「復元のガイドライン」（p.6-38）を参照してください。

アーカイブ共有ファイルの形式

MARS のアーカイブ処理は、毎日午前 2 時に実行され、アーカイブしたデータ用に日付入りのディレクトリが作成されます。データのアーカイブ時刻を指定することはできません。

pnos ディレクトリには、オペレーティング システムのバックアップが保存されます。

```
06/12/2005  11:32p      <DIR>          .
06/12/2005  11:32p      <DIR>          ..
07/09/2005  01:30a      <DIR>          pnos      <-- OS Backup Directory
07/08/2005  04:49p      <DIR>          2005-07-08<-- Daily Data Backup Directory
07/10/2005  12:09a      <DIR>          2005-07-10
07/11/2005  12:12a      <DIR>          2005-07-11
07/12/2005  12:12a      <DIR>          2005-07-12
07/13/2005  12:16a      <DIR>          2005-07-13
07/14/2005  02:02a      <DIR>          2005-07-14
07/15/2005  02:02a      <DIR>          2005-07-15
07/16/2005  02:02a      <DIR>          2005-07-16
07/17/2005  02:02a      <DIR>          2005-07-17
07/18/2005  02:02a      <DIR>          2005-07-18
07/19/2005  02:02a      <DIR>          2005-07-19
07/19/2005  09:46p      <DIR>          2005-05-26
07/20/2005  07:16a      <DIR>          2005-05-27
07/20/2005  07:17a      <DIR>          2005-07-20
07/22/2005  12:13a      <DIR>          2005-07-22
07/21/2005  12:09a      <DIR>          2005-07-21
07/23/2005  12:15a      <DIR>          2005-07-23
               0 File(s)              0 bytes
              58 Dir(s)   4,664,180,736 bytes free
```

毎日の各ディレクトリには、データ タイプごとにサブディレクトリが作成されます。次に、コメント内のディレクトリのタイプを示します。

```
Directory of D:\MARSBackups\2005-07-08

07/08/2005  04:49p      <DIR>          .
07/08/2005  04:49p      <DIR>          ..
07/08/2005  04:49p      <DIR>          CF<-- Configuration Data
07/08/2005  05:00p      <DIR>          IN<-- Incident Data
07/08/2005  05:16p      <DIR>          AL<-- Audit Logs
07/08/2005  05:16p      <DIR>          ST<-- Statistics Data
07/08/2005  05:16p      <DIR>          RR<-- Report Results
07/08/2005  05:49p      <DIR>          ES<-- Raw Event Data
               0 File(s)              0 bytes
               8 Dir(s)   4,664,180,736 bytes free
```

生イベント データ ディレクトリの .gz ファイル名には、データがアーカイブされた期間が YYYY-MM-DD-HH-MM-SS 形式で含まれています。

```
Directory of D:\MARSBackups\2005-07-08\ES

07/08/2005  05:49p      <DIR>          .
07/08/2005  05:49p      <DIR>          ..
07/08/2005  05:49p              34,861 es-3412-342_2005-07-08-16-49-52_2005-07-08-17-49-47.gz
07/08/2005  05:49p              31,828 rm-3412-342_2005-07-08-16-49-52_2005-07-08-17-49-47.gz
07/08/2005  06:49p              49,757 es-3412-342_2005-07-08-17-49-49_2005-07-08-18-49-40.gz
07/08/2005  06:49p              48,154 rm-3412-342_2005-07-08-17-49-49_2005-07-08-18-49-40.gz
07/08/2005  07:49p              24,420 es-3412-342_2005-07-08-18-49-45_2005-07-08-19-49-52.gz
07/08/2005  07:49p              22,346 rm-3412-342_2005-07-08-18-49-45_2005-07-08-19-49-52.gz
07/08/2005  08:50p              44,839 es-3412-342_2005-07-08-19-49-47_2005-07-08-20-50-04.gz
07/08/2005  08:50p              41,534 rm-3412-342_2005-07-08-19-49-47_2005-07-08-20-50-04.gz
07/08/2005  09:50p              58,988 es-3412-342_2005-07-08-20-49-55_2005-07-08-21-50-06.gz
07/08/2005  09:50p              54,463 rm-3412-342_2005-07-08-20-49-55_2005-07-08-21-50-06.gz
07/08/2005  10:50p             130,604 es-3412-342_2005-07-08-21-49-58_2005-07-08-22-50-08.gz
07/08/2005  10:50p              85,437 rm-3412-342_2005-07-08-21-49-58_2005-07-08-22-50-08.gz
07/08/2005  11:50p             114,445 es-3412-342_2005-07-08-22-49-55_2005-07-08-23-50-10.gz
07/08/2005  11:50p              58,240 rm-3412-342_2005-07-08-22-49-55_2005-07-08-23-50-10.gz
07/09/2005  12:50a             110,556 es-3412-342_2005-07-08-23-50-02_2005-07-09-00-50-14.gz
07/09/2005  12:50a              53,977 rm-3412-342_2005-07-08-23-50-02_2005-07-09-00-50-14.gz
              16 File(s)        964,449 bytes
               2 Dir(s)   4,664,164,352 bytes free
```

次に、コンフィギュレーション データ ディレクトリのデータの例を示します。

```
Directory of D:\MARSBackups\2005-07-08\CF

07/08/2005  04:49p      <DIR>          .
07/08/2005  04:49p      <DIR>          ..
07/08/2005  02:02a           2,575,471 cf_2005-07-08-02-02-02.pna
               1 File(s)      2,575,471 bytes
               2 Dir(s)   4,664,164,352 bytes free
```

Windows 上での NFS サーバの設定

Windows Services for UNIX（WSU）により、Windows ファイル サーバ上に NFS マウントを作成できます。このオプションは便利で、ラボ環境または UNIX に詳しい人材がいない場合に役立ちます。Microsoft からの無料ダウンロードおよび設定情報は、以下の URL を参照してください。

Windows Services for UNIX 3.5 のダウンロード
http://www.microsoft.com/windowsserversystem/sfu/downloads/default.mspx

WSU 3.5 のシステム要件
http://www.microsoft.com/windowsserversystem/sfu/productinfo/sysreqs/default.mspx

Microsoft Windows Services for UNIX 3.5 レビュー ガイド
http://www.microsoft.com/windowsserversystem/sfu/downloads/default.mspx

Microsoft Services for Network File System のパフォーマンス調整ガイドライン
http://www.microsoft.com/technet/interopmigration/unix/sfu/perfnfs.mspx

WSU 3.5 をインストールして設定し、MARS アプライアンスと相互運用するには、次の作業を行います。

- Windows Services for UNIX 3.5 のインストール（p.6-23）
- Windows Services for UNIX 3.5 を使用した共有の設定（p.6-25）

Windows Services for UNIX 3.5 のインストール

Windows サーバ上に NFS サーバを設定する手順は、次のとおりです。

ステップ 1　Windows Services for UNIX 3.5 をダウンロードします。

ステップ 2　Windows Services for UNIX をインストールするには、**SFU35SEL_EN.exe** をダブルクリックします。

ステップ 3　Unzip to folder フィールドにプログラム ファイルを展開するフォルダ名を入力し、**Unzip** をクリックします。

ローカル プロファイルの一時フォルダではなく、新規フォルダを定義することを推奨します。解凍処理は、数分かかることがあります。

ステップ 4　ファイルを展開したフォルダを開き、**SfuSetup.msi** をダブルクリックします。

ステップ 5　**Next** をクリックして、作業を続けます。

Customer Information パネルが表示されます。

ステップ 6　User name および Organization フィールドに値を入力し、**Next** をクリックします。

License and Support Information パネルが表示されます。

ステップ 7　**I accept the agreement** オプションを選択し、**Next** をクリックします。

ステップ 8　**Custom Installation** オプションを選択し、**Next** をクリックします。

ステップ 9　最小限、Components リストの Under Windows Services for UNIX にある次のコンポーネントについて、**Entire feature (including any subfeatures if any) will be installed on local hard drive** を選択する必要があります。**Next** をクリックします。

- **NFS**（このオプションには、Client for NFS および Server for NFS のサブ機能が含まれています）
- **Authentication tools for NFS**（このオプションには、User Name Mapping、Server for NFS Authentication、および Server for PCNFS のサブ機能が含まれています）

（注）　この手順は、NFS および Authentication tools for NFS 以外のすべてのコンポーネントについて、**Entire feature will not be available** が選択されていることを前提としています。

Security Settings パネルが表示されます。

ステップ 10　Change the default behavior to case sensitive チェックボックスが*選択されていない*ことを確認し、**Next** をクリックします。

MARS アプライアンスは、NFS 認証用に特別なアカウントを使用しないので、デフォルト設定を変更する必要はありません。

ステップ 11　User Name Mapping パネルが表示されます。

ステップ 12　Local User Name Mapping Server および Network Information Service（NIS）オプションが選択されていることを確認し、**Next** をクリックします。

2 番めの User Name Mapping パネルが表示されます。

ステップ 13　次のフィールドに値を入力し、**Next** をクリックします。

- **Windows domain name** ローカル ホスト名のデフォルト値を受け入れることを推奨します。
- （任意）**NIS domain name**
- （任意）**NIS server name**

Installation Location パネルが表示されます。

ステップ 14　インストール先の場所を入力し、**Next** をクリックします。

インストールの進行状況を示す、Installing パネルが表示されます。インストールが完了すると、Completing the Microsoft Windows Services for UNIX Setup Wizard パネルが表示されます。

ステップ 15　**Finish** をクリックしてインストールを完了し、Setup Wizard を終了します。

ステップ 16　コンピュータを再起動します。

これで、必要な NFS コンポーネントが正常にインストールされます。次に、MARS アプライアンスがバックアップおよびアーカイブに使用する共有を定義し、設定する必要があります。詳細は、「Windows Services for UNIX 3.5 を使用した共有の設定」（p.6-25）を参照してください。

Windows Services for UNIX 3.5 を使用した共有の設定

共有の設定には、共有するフォルダの識別、および適正な許可とアクセスの指定が含まれます。

WSU 3.5 を、MARS アプライアンスの NFS サーバとして設定する手順は、次のとおりです。

ステップ 1　WSU 3.5 をインストールした Windows ホスト上で、Windows Explorer を起動します。

ステップ 2　MARS のアーカイブを保存するフォルダを作成します。

フォルダの例：*C:\MARSBackups*

ステップ 3　作成したフォルダを右クリックし、**NFS Sharing** タブをクリックします。

ステップ 4　**Share this folder** オプションを選択し、Share name フィールドに名前を入力します。

MARSBackups のように、共有名はフォルダ名と同じ名前に設定できます。

ステップ 5　**Allow Anonymous Access** チェックボックスを選択します。

Windows サーバは MARS アプライアンスを直接認証できないので、このオプションを選択する*必要があります*。

ステップ 6　**Permission** をクリックします。

NFS Share Permissions ダイアログボックスが表示されます。

ステップ 7　Name で **ALL MACHINES** を選択し、Type of Access リストから **No Access** を選択します。

ステップ 8　**Add** をクリックします。

ステップ 9　MARS アプライアンスの IP アドレスを入力し、**OK** をクリックします。

ステップ 10　MARS アプライアンスの IP アドレスを選択し、Type of Access リストから **Read-Write** を選択します。Encoding リストで、**ANSI** が選択されていることを確認します。

ステップ 11　**OK** をクリックして変更を保存し、NFS Share Permissions ダイアログボックスを終了します。

ステップ 12　**Apply** をクリックして、変更を適用します。

（注）　Apply を使用できない場合、WSU 3.5 のインストール後にサーバが再起動されていません。サーバを再起動し、この手順を繰り返す必要があります。

ステップ 13　DOS command ウィンドウに、次のコマンドを入力します。

cd <*ShareFolder***>**

cacls <*ShareFolder***> /E /G everyone:F**

これらのコマンドは、**Everyone** がフォルダにローカル ファイルシステム アクセスできるように、共有フォルダの許可を変更します。

例：

```
cd C:\MARSBackups
cacls MARSBackups /E /G everyone:F
```

ステップ 14　**Start > Control Panel > Administrative Tools > Local Security Policy** をクリックします。

ステップ 15　Local Security Policy > Security オプションのもとで、**Network Access:Let Everyone permissions apply to anonymous users** をダブルクリックし、**Enabled** を選択して、**OK** をクリックします。

このオプションにより、Anonymous ユーザと Everyone ユーザが同等になります。

これで、Windows サーバ用の NFS 設定は完了です。デバッグ用のロギングをイネーブルにするには、「NFS イベントのロギングのイネーブル化」（p.6-26）に進みます。それ以外の場合には、「MARS アプライアンス のデータ アーカイブ設定」（p.6-27）に進みます。

NFS イベントのロギングのイネーブル化

トラブルシューティング用に、Microsoft Windows Services for UNIX 3.5 を実行している Windows ホスト上で、NFS サーバのロギングをイネーブルに設定できます。

Windows ホスト上で NFS サーバのロギングをイネーブルにする手順は、次のとおりです。

ステップ 1　**Start > All Programs > Services for UNIX Administration > Services for UNIX Administration** をクリックします。

ステップ 2　Services for UNIX で、**Server for NFS** を選択します。

ステップ 3　Log events in this file で、表示したいログ ファイルのフォルダを指定します。

デフォルトでは、ログ ファイルは、`C:\SFU\log` ディレクトリに表示されます。

ステップ 4　すべてのチェックボックスが選択されていることを確認します。

ステップ 5　**Apply** をクリックして、変更を保存します。

ステップ 6　「MARS アプライアンス のデータ アーカイブ設定」（p.6-27）に進みます。

Linux 上での NFS サーバの設定

NFS は、Linux ファイル システム上でネイティブにサポートされます。これには、Linux ボックスが必要です。Linux ファイル サーバは安価で構築できるので、ファイル サーバを構築して、MARS のアーカイブ データ専用として使用することを強く推奨します。

ここでは、MARS アプライアンスのデータをアーカイブするための NFS 設定について、設定例を示します。特定の NFS サーバにアーカイブしたい各 MARS アプライアンスについて、アプライアンスが読み書きできるディレクトリを NFS 上に設定する必要があります。次に、この作業に必要な手順を示します。

MARS アプライアンスからアーカイブする Linux NFS サーバを設定する手順は、次のとおりです。

ステップ 1　ルート権限のあるアカウントを使用して、NFS サーバにログインします。

ステップ 2　データをアーカイブするディレクトリを作成します。

例：

```
mkdir -p /archive/nameOfYourMARSBoxHere
chown -R nobody.nobody /archive
chmod -R 777 /archive
```

ステップ 3　/etc/exports ファイルに、次の行を追加します。

```
/archive/nameOfYourMARSBoxHere MARS_IP_Address(rw)
```

ステップ 4　NFS サービスを再起動します。

```
/etc/init.d/nfs restart
```

MARS アプライアンス のデータ アーカイブ設定

MARS アプライアンス上で実行しているデータおよびシステム ソフトウェアを、リモート サーバにアーカイブできます。このデータ アーカイブには、OS、アップグレード / パッチ データ、システム コンフィギュレーションをはじめ、システム ログ、インシデント、生成されたレポートなどのダイナミック データ、さらにアプライアンスが受信した監査イベントが含まれます。この機能は、アプライアンスのスナップショット イメージを提供します。

（注）　完全なシステム コンフィギュレーション データがアーカイブされますが、アーカイブされるダイナミック データには、データ アーカイブ設定をイネーブルにした*あと*で受信または生成されたデータだけが含まれます。したがって、アプライアンスがレポーティング デバイスから監査データを受信するように設定する前に、アーカイブをイネーブルにすることを推奨します。

アーカイブ データを使用すると、データが破壊されていなければ、障害時にアプライアンスを復元できます。この意味では、データ アーカイブは、Recovery DVD によるアプライアンスのイメージ再作成の代替手段になります。

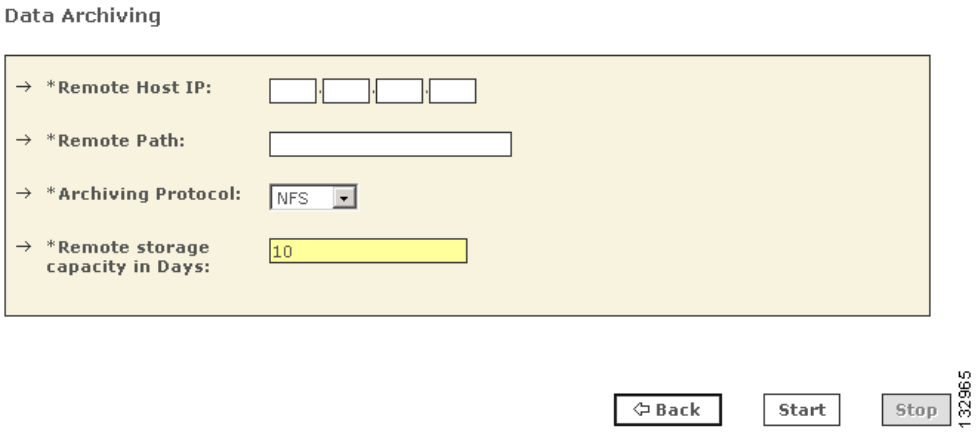
作業を始める前に

アプライアンスのデータをアーカイブするには、NFS サーバを適正に設定する必要があります。「Windows 上での NFS サーバの設定」（p.6-23）または「Linux 上での NFS サーバの設定」（p.6-27）を参照してください。

アプライアンス用に基本的なネットワーク設定を行う必要があります。

特定の MARS アプライアンスについてデータ アーカイブを設定する手順は、次のとおりです。

ステップ 1　**Admin** > **System Maintenance** > **Data Archiving** を選択します。



ステップ 2　Remote Host IP フィールドに、リモート NFS サーバ、または NFS プロトコルをサポートする NFS システムの IP アドレスを入力します。

ステップ 3　Remote Path フィールドに、アーカイブ ファイルを保存したいリモート NFS サーバまたは NAS システム上のエクスポート パスを入力します。

たとえば、*/MARSBackups* は、*MARSBackups* という名前の NFS 共有を設定した Windows ホストの有効値になります。最初のスラッシュは、UNC 共有名を解決するために必要です。

ステップ 4　Archiving Protocol フィールドで、**NFS** を選択します。

その他のオプションは、使用できません。

ステップ 5　Remote storage capacity in Days フィールドに、次のいずれかの値を入力します。

- サーバにデータをアーカイブしておく最大日数。サーバは、現在の日付より前の指定した日数分のデータを保持します。
- アーカイブ サーバが最大限保持できるデータの日数。これにより、アーカイブ サーバの容量を上限を指定します。

ステップ 6　**Start** をクリックし、アプライアンスのアーカイブをイネーブルにします。

（注）　アーカイブを開始したあと、「invalid remote IP or path」などのエラー メッセージが表示された場合には、NFS サーバが正しく設定されていません。これらのメッセージを受信した場合は、「Windows 上での NFS サーバの設定」（p.6-23）または「Linux 上での NFS サーバの設定」（p.6-27）を参照してください。

結果: ステータス ページが表示されます。**Back** をクリックして、Data Archiving ページに戻ります。

ステップ 7　このページの値を変更する必要がある場合には、値を入力して、**Change** をクリックします。

ヒント　データのアーカイブを停止するには、Data Archiving ページに戻り、**Stop** をクリックします。

アーカイブしたファイル内のデータへのアクセス

アーカイブしたファイル内のイベント データにアクセスし、イベントを検証できます。この作業は、特定の時間内のイベントを検証したり、データの後処理を実行する場合に役立ちます。

ヒント　アーカイブしたデータへの他のアクセス方法については、「アーカイブ データの一般的な使用方法」（p.6-21）を参照してください。

アーカイブしたファイル内のデータにアクセスする手順は、次のとおりです。

ステップ 1　アーカイブ サーバのコマンドライン インターフェイスで、次のコマンドを実行します。

cd <*achive_path*>

archive_path は、「MARS アプライアンス のデータ アーカイブ設定」（p.6-27）で指定したリモート パスの値です。

ステップ 2　次のコマンドを入力して、検証するアーカイブを選択します。

cd <*YYYY-MM-DD*>

YYYY-MM-DD は、アーカイブ ファイルが作成された日付です。

ステップ 3　次のコマンドを入力して、選択したデータのアーカイブ ファイルのリストを表示します。

cd ES ls -l

ステップ 4　次のコマンドを入力して、アーカイブ ファイルからデータを展開します。

gunzip <filename>

filename は、展開するファイルの名前です。使用可能なファイルのリストは、ファイル作成時のタイムスタンプに基づいています。

ステップ 5　次のコマンドを入力して、ファイルの内容を表示します。

vi <filename>

これらのファイルのデータには、任意のテキスト エディタを使用したり、スクリプトを実行できます。ただし、圧縮ファイルの内容を変更したり、展開したデータまたは追加ファイルをアーカイブ フォルダ内に置いておくべきではありません。復元を実行する場合、MARS は、新規ファイルまたは展開されたファイルを処理できません。

回復の管理

MARS アプライアンスの機能には、MARS アプライアンスの Recovery DVD-ROM を使用して実行できる作業が 2 つあります。アプライアンスを回復する方法は、回復したいデータがアーカイブされているかどうかによって異なります。MARS アプライアンスの回復方法には、2 つの状況が影響します。

- **Global Controller または Local Controller のイメージ再作成 —** イメージの再作成アプライアンスを回復する手順は、STM システムにおけるアプライアンスの役割によって異なります。Global Controller の場合、モニタ対象の各 Local Controller 上で、追加の作業が必要になります。
- **アーカイブされているデータ —** 回復したいアプライアンスのデータがアーカイブされている場合には、アプライアンスの回復後に追加の作業があります。

注意　回復処理を行うと、MARS アプライアンスのハードディスク ドライブの内容が消去されます。アーカイブまたはバックアップしていないコンフィギュレーションおよびイベント データはすべて、永久に失われます。可能ならば、アプライアンスのイメージを再作成する前に、ライセンス キーを書き留めてください。イメージを再作成したあと、初期設定中にライセンス キーを入力する必要がありますが、ライセンス キーはアーカイブしたデータからは復元されません。

ここでは、次の作業について説明します。

管理パスワードを失った場合

pnadmin アカウントに関連付けられたパスワードを失った場合、このパスワードを回復することはできません。アプライアンスのイメージを再作成して、パスワードを出荷時のデフォルト値にリセットする必要があります。詳細は、「Local Controller のイメージの再作成」（p.6-32）および「Global Controller のイメージの再作成」（p.6-33）を参照してください。「アプライアンスのデータ バックアップの設定および実行」（p.6-20）の手順に従って、MARS アプライアンスのデータのアーカイブを設定していた場合には、「MARS アプライアンスのイメージ再作成後のアーカイブ データの復元」（p.6-35）の手順を使用して、コンフィギュレーションおよびイベント データを回復できます。

Recovery DVD のダウンロードおよび作成

MARS アプライアンスに付属の MARS Appliance Recovery DVD-ROM がない場合、または新規イメージを使用して回復後のアップグレードを迅速に行いたい場合には、MARS 専用の Cisco.com ソフトウェア ダウンロード ページから最新のリカバリ イメージをダウンロードできます。有効な Cisco.com アカウントがあり、MARS アプライアンスの SMARTnet 契約番号が登録されていれば、次の URL からダウンロード ページにアクセスできます。

- リカバリ イメージ：http://www.cisco.com/cgi-bin/tablebuild.pl/cs-mars-recovery

csmars-4.1.1.iso などの ISO イメージをダウンロードしたあと、そのファイルを使用して DVD-ROM を作成できます。ファイルは通常、1.42 GB 以上です。

Local Controller のイメージの再作成

必要に応じて、MARS アプライアンス Recovery DVD-ROM を使用して、Local Controller のイメージを再作成できます。この作業を実行すると、すべてのデータが破棄され、新しいイメージがインストールされます。アプライアンスを回復するには、デバイスを準備して、アーカイブしたデータを回復する作業に加え、時間のかかる 3 つの作業を行う必要があります。

- CD からのイメージのダウンロード（約 30 分）
- ダウンロード後のイメージのインストレーション（約 90 分）
- 基本的なシステム設定（約 5 分）

注意　この手順を実行すると、MARS アプライアンスに保存されているすべてのデータが破壊されます。

作業を始める前に

アプライアンスのイメージを再作成する前に、ライセンス キーを書き留めてください。イメージを再作成したあと、初期設定中にライセンス キーを入力する必要があります。

Local Controller のイメージを再作成するには、次の作業を行います。

ステップ 1　MARS アプライアンスの VGA ポートにモニタを接続し、PS/2 キーボード ポートにキーボードを接続します（MARS アプライアンスの VGA および シリアル ポートの図は、「ハードウェアの概要」[p.1-5] の対応するモデルを参照してください）。

ステップ 2　eth0 ポートおよび eth1 ポートから、接続されているすべてのネットワーク ケーブルを取り外します。

ステップ 3　Recovery DVD を、MARS アプライアンスの DVD-ROM ドライブに挿入します。

ステップ 4　次のいずれかを実行します。

- pnadmin として MARS アプライアンスにログインし、**reboot** コマンドを使用してシステムをリブートします。
- MARS アプライアンスの電源を一度切り、再投入します。

結果：コンソールに、次のメッセージが表示されます。

```
Please Choose A MARS Model To Install...
1. Distributed Mars - Local Controller
2. Distributed Mars - Global Controller
3. Quit
```

ステップ 5　矢印キーを使用して、Recover メニューで **1. Distributed MARS — Local Controller** を選択し、**Enter** を押します。

a.　MARS100 または 100e のイメージを再作成する場合には、コンソールに次のメッセージが表示されます。それ以外の場合には、ステップ 6 に進みます。

```
Please Choose Which MARS100 Model To Install...
1.  MARS100
2.  MARS100E
3.  Quit
```

b. 矢印キーを使用して、購入したライセンスに基づいて適切なモデルを選択し、**Enter** を押します。

結果：アプライアンスへのイメージのダウンロードが開始されます。この処理には、約 15 分かかります。イメージのダウンロードが完了すると、Recovery DVD がイジェクトされ、コンソールに次のメッセージが表示されます。

```
Please remove the installation CD and press Reboot to finish the installation.
```

ステップ 6　MARS アプライアンスから Recovery DVD を取り出します。

ステップ 7　**Enter** を押して、MARS アプライアンスを再起動します。

結果：MARS アプライアンスがリブートし、Oracle データベースの構築など、コンフィギュレーションの一部が実行されます。初回のリブート後のコンフィギュレーションには、かなり時間がかかります（1 ～ 1.5 時間）。この間、フィードバックはありませんが、これはシステムの正常な状態です。

ステップ 8　eth0 ポートおよび eth1 ポートに、ネットワーク ケーブルを再接続します。

（注）　アプライアンスのイメージの再作成後、MARS アプライアンスの初期設定を再度行う必要があります。詳細は、第 5 章「MARS アプライアンスの初期設定」を参照してください。

ステップ 9　初期設定の完了後、次のいずれかを実行します。

- Local Controller に、モニタ対象のデバイスを追加します。詳細は、『*User Guide for Cisco Security MARS Local Controller Version 4.1.x*』を参照してください。
- 「MARS アプライアンスのイメージ再作成後のアーカイブ データの復元」（p.6-35）の手順を使用して、アーカイブされているデータを回復します。

Global Controller のイメージの再作成

必要に応じて、MARS アプライアンス Recovery DVD-ROM を使用して、Global Controller のイメージを再作成できます。この作業を実行すると、すべてのデータが破棄され、新しいイメージがインストールされます。アプライアンスを回復するには、デバイスを準備して、アーカイブしたデータを回復する作業に加え、時間のかかる 4 つの作業を行う必要があります。

- モニタ対象の各 Local Controller からのすべての Global Controller データの消去（「作業を始める前に」[p.6-34] を参照）。
- CD からのイメージのダウンロード（約 30 分）
- ダウンロード後のイメージのインストレーション（約 45 分）
- 基本的なシステム設定（約 5 分）

Global Controller のイメージを再作成するには、次の作業を行います。

注意　この手順を実行すると、MARS アプライアンスに保存されているすべてのデータが破壊されます。

作業を始める前に

- アプライアンスのイメージを再作成する前に、ライセンス キーを書き留めてください。イメージを再作成したあと、初期設定中にライセンス キーを入力する必要があります。
- Global Controller のイメージを再作成する前に、Global Controller がモニタ対象の Local Controller にプッシュダウンしたデータを消去する必要があります。回復する Global Controller がモニタしていた各 Local Controller について、各 Local Controller のコマンドライン インターフェイスから次のコマンドを実行します。

  ```
  pnreset -g
  ```

  このコマンドにより、Local Controller からグローバル検査ルールとユーザ アカウントが消去され、イメージを再作成した Global Controller で管理できるようになります。

ステップ 1　「作業を始める前に」（p.6-34）で説明したように、各 Local Controller 上で **pnreset -g** コマンドを実行したあと、モニタを MARS アプライアンスの VGA ポートに接続し、キーボードを PS/2 キーボード ポートに接続します（MARS アプライアンスの VGA および シリアル ポートの図は、「ハードウェアの概要」（p.1-5）の対応するモデルを参照してください）。

ステップ 2　eth0 ポートおよび eth1 ポートから、接続されているすべてのネットワーク ケーブルを取り外します。

ステップ 3　Recovery DVD を、MARS アプライアンスの DVD-ROM ドライブに挿入します。

ステップ 4　次のいずれかを実行します。

- pnadmin として MARS アプライアンスにログインし、**reboot** コマンドを使用してシステムをリブートします。
- MARS アプライアンスの電源を一度切り、再投入します。

結果：コンソールに、次のメッセージが表示されます。

```
Please Choose A MARS Model To Install...
1. Distributed Mars - Local Controller
2. Distributed Mars - Global Controller
3. Quit
```

ステップ 5　矢印キーを使用して、Recover メニューで **2. Distributed MARS — Global Controller** を選択し、**Enter** を押します。

結果：アプライアンスへのイメージのダウンロードが開始されます。イメージのダウンロードが完了すると、Recover DVD がイジェクトされ、コンソールに次のメッセージが表示されます。

```
Please remove the installation DVD and press Reboot to finish the installation.
```

ステップ 6　MARS アプライアンスから Recovery DVD を取り出します。

ステップ 7　**Enter** を押して、MARS アプライアンスを再起動します。

結果：MARS アプライアンスがリブートし、Oracle データベースの構築など、コンフィギュレーションの一部が実行されます。初回のリブート後のコンフィギュレーションには、かなり時間がかかります。この間、フィードバックはありませんが、これはシステムの正常な状態です。

ステップ 8　eth0 ポートおよび eth1 ポートに、ネットワーク ケーブルを再接続します。

（注）　アプライアンスのイメージの再作成後、MARS アプライアンスの初期設定を再度、行う必要があります。詳細は、第 5 章「MARS アプライアンスの初期設定」を参照してください。

ステップ 9　初期設定の完了後、次のいずれかを実行します。

（注）　Global Controller が、モニタ対象の Local Controller と同じ MARS ソフトウェアを実行している状態になるまでは、Global Controller を使用して Local Controller を追加またはモニタすることはできません。

- Global Controller に、すべての Local Controller を追加して、戻します。各 Local Controller から Global Controller に、すべてのデバイスおよびトポロジーの情報がプル アップされます。詳細は、『*User Guide for Cisco Security MARS Global Controller Version 4.1.x*』を参照してください。
- 「MARS アプライアンスのイメージ再作成後のアーカイブ データの復元」（p.6-35）の手順を使用して、アーカイブされているデータを回復します。

MARS アプライアンスのイメージ再作成後のアーカイブ データの復元

アーカイブ データを使用して MARS アプライアンスを復元すると、システムに、アーカイブされているデータおよびコンフィギュレーションが復元されます。コンフィギュレーション データには、アーカイブが実行された時点で有効だった OS、MARS ソフトウェア、ライセンス キー、ユーザ アカウント、パスワード、およびデバイス リストが含まれています。

復元するアプライアンス上で実行中の MARS ソフトウェアのバージョンは、アーカイブに保存されているバージョンと一致している必要はありません。ただし、復元を実行したあとでアプライアンス上で実行されるバージョンは、アーカイブの pnos フォルダに保存されていたバージョンになります。

アーカイブの復元方法の詳細は、「復元のガイドライン」（p.6-38）を参照してください。

（注）　アーカイブ データから復元を実行する場合には、アーカイブ ファイルに含まれていないすべてのデバイスを、Local Controller 上に再入力する必要があります。既存のケースを復元するには、インシデントおよびセッション データを復元する必要があります。データのタイプおよび復元モードの詳細は、「pnrestore」（p.A-20）を参照してください。

データをアーカイブし、「Local Controller のイメージの再作成」（p.6-32）または「Global Controller のイメージの再作成」（p.6-33）の手順で MARS アプライアンスを回復した場合には、次の作業を行います。

ステップ 1　回復処理の完了後、次のコマンドを実行して、最後にアーカイブしたデータから MARS アプライアンスを復元します。

```
pnrestore -p <NFSServerIP>:/<archive_path>
```

NFSSeverIP は、**Admin** > **System Maintenance** > **Data Archiving** の HTML インターフェイスの設定で、Remote Host IP フィールドに指定した値、*archive_path* は、Remote Path フィールドに指定した値です。NFS サーバは、*NFSSeverIP:/archive_path* のように、IP アドレスと :/ で区切ったパス名を指定する必要があります。設定の詳細については、「MARS アプライアンス のデータ アーカイブ設定」（p.6-27）を参照してください。

ステップ 2　復元処理が完了したあと、MARS アーカイブ ファイルに含まれていなかったすべてのデバイスを必要に応じて、削除、再入力、および再検出します。

スタンバイまたはセカンダリ MARS アプライアンスの設定

アーカイブしたデータのディレクトリ上では、クエリーの実行、およびインシデント調査のレポートまたは実行はできません。アーカイブしたデータを使用して何らかの調査を行うには、そのデータを MARS アプライアンスに復元する必要があります。そのためには、セカンダリ アプライアンスを設定することを推奨します。個別のアプライアンスを使用する理由は、古いデータを調査する場合、一定期間のデータをアプライアンスに復元し、その期間のアーカイブ設定に基づいてすべてのコンフィギュレーションおよびイベント データのイメージを復元する必要があるからです。

セカンダリ アプライアンスに復元するには、同等以上のモデルのアプライアンスを使用する必要があります。たとえば、MARS20 からのイメージは、MARS20、MARS50、MARS100、または MARS100e に復元できますが、MARS50 のイメージを MARS20 に復元することは *できません*。セカンダリ アプライアンスへの復元は、アーカイブを実行した元のアプライアンスへの復元とは異なります。セカンダリ アプライアンスに復元する場合には、次の注意事項に従ってください。

- セカンダリ アプライアンス用の新しいライセンス キーを購入する必要があります。各ライセンス キーは、そのキーを割り当てたアプライアンスのシリアル番号に関連付けられています。
- セカンダリ アプライアンスにログインするには、復元したイメージ上で新しいライセンス キーを入力する必要があります。
- セカンダリ アプライアンスにイメージを復元する場合、プライマリ アプライアンスをネットワークから切断するか、NAT を実行できるゲートウェイの背後で操作する必要があります。セカンダリ アプライアンスにはプライマリと同じ IP アドレスが割り当てられるので、セカンダリ アプライアンスの起動時にプライマリ アプライアンスが同じネットワーク上にあると、IP アドレスのコンフリクト エラーが発生します。

完全なシステム コンフィギュレーション データの単一イメージは、毎日アーカイブされ、更新されているので、アーカイブからどの期間を選択しても、システム コンフィギュレーション データには最新の変更が含まれています。つまり、365 日前の期間を選択しても、反映されるのはイベント データだけです。復元されるシステム コンフィギュレーションは、最新のアーカイブのコンフィギュレーションです。

詳細は、「復元のガイドライン」（p.6-38）を参照してください。

復元のガイドライン

アプライアンスを復元する場合には、次のガイドラインに注意してください。

- 復元処理は、いずれも時間がかかります。所要時間は、選択するオプションによって異なります。「pnrestore」（p.A-20）を参照してください。
- コンフィギュレーション データだけを復元する場合は、より短時間で実行できます。
- 復元処理では、イベント データだけを増分的に復元することはできません。対象アプライアンスのハードドライブの完全なイメージが、常に再作成されます。
- ライセンス キー、IP アドレス、ホスト名、ユーザ アカウント、パスワード、および DNS 設定を含むすべてのコンフィギュレーション情報が、常に復元されます。
- アーカイブを作成したアプライアンスとは別のアプライアンスに復元する場合には、「スタンバイまたはセカンダリ MARS アプライアンスの設定」（p.6-37）を参照してください。
- データをアーカイブしたアプライアンスとは別のアプライアンスに復元する場合には、復元したデータにアクセスする前に、新しいアプライアンスのシリアル番号に割り当てられているライセンス キーを入力する必要があります。
- 指定した日付から、最後のアーカイブの日付までの情報が復元されます。**pnrestore** コマンドの date 引数には、復元範囲の開始時刻を示す毎日のデータ バックアップ ディレクトリの名前を指定します。「アーカイブ共有ファイルの形式」（p.6-21）を参照してください。
- 特定の日付範囲を復元するには、範囲以降の不要な日付をアーカイブ フォルダから一時的に移動することを推奨します。不要な日付を除去すると、これらの日付のダイナミック データは失われますが、復元に要する時間は短くなります。
- 選択したアーカイブの復元範囲に含まれているデータが、対象 MARS アプライアンスのローカル データベースの容量を超えている場合、MARS アプライアンスはローカル データベースの最も古いパーティションのデータを自動的に削除し、復元を再開します。したがって、復元を実行する場合には、妥当な容量の日付範囲を選択する必要があります。ローカル データベースの制限を越える範囲を復元しても、最新の日付が復元されるまで古いパーティションのデータが間欠的に削除されるので、復元処理が遅くなるだけで、成果は得られません。
- **pnrestore** コマンドのモード 5 は、ローカル データベースのバックアップから復元するので、NFS アーカイブからの復元には使用できません。したがって、この復元を実行する場合には、アーカイブをイネーブルにする必要はありません。コンフィギュレーション データは、毎晩、アプライアンス上でバックアップされます。新しいリリースにアップグレードした場合、コンフィギュレーションがバックアップされる前に復元を試みると、復元は失敗するので注意が必要です。データのタイプおよび復元モードの詳細は、「pnrestore」（p.A-20）を参照してください。