CLUSTERPRO® X *for Windows*

Symantec™ Endpoint Protection 12.1 連携ガイド

2013.09.05
第 3 版

CLUSTERPRO

改版履歴

版数	改版日付	内 容
1	2012/09/18	新規作成
2	2013/02/05	「サンプルスクリプト」スクリプト内容の更新
3	2013/09/05	「サンプルスクリプト」注釈を追記

免責事項

本書の内容は、予告なしに変更されることがあります。
日本電気株式会社は、本書の技術的もしくは編集上の間違い、欠落について、一切責任をおいません。
また、お客様が期待される効果を得るために、本書に従った導入、使用および使用効果につきましては、お客様の責任とさせていただきます。
本書に記載されている内容の著作権は、日本電気株式会社に帰属します。本書の内容の一部または全部を日本電気株式会社の許諾なしに複製、改変、および翻訳することは禁止されています。

商標情報

CLUSTERPRO® X は日本電気株式会社の登録商標です。
Microsoft、Windows は、米国 Microsoft Corporation の米国およびその他の国における登録商標です。
Symantec、Symantec ロゴ、Symantec Endpoint Protection は、Symantec 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。 他の名称は、それぞれ各社の商標です。
本書に記載されたその他の製品名および標語は、各社の商標または登録商標です。

目次

はじめに

本書は、Symantec Endpoint Protection クライアントによりセキュリティ保護されたサーバを用いてクラスタを構築するための手順について説明します。

注：Symantec Endpoint Protection Manager をクラスタリングする手順ではありません。

対象読者と目的

『CLUSTERPRO X 連携ガイド』は、クラスタシステムに関して、システムを構築する管理者、およびユーザサポートを行うシステムエンジニア、保守員を対象にしています。
本書では、CLUSTERPRO 環境下での動作確認が取れたソフトウェアを紹介しています。ここで紹介するソフトウェアや設定例は、あくまで参考情報として提供するものであり、各ソフトウェアの動作保証をするものではありません。

関連資料

CLUSTERPRO マニュアル

CLUSTERPRO のマニュアルは、以下の 4 つに分類されます。

『CLUSTERPRO X スタートアップガイド』(Getting Started Guide)
CLUSTERPRO を使用するユーザを対象読者とし、製品概要、動作環境、アップデート情報、既知の問題などについて記載します。

『CLUSTERPRO X インストール & 設定ガイド』(Install and Configuration Guide)
CLUSTERPRO を使用したクラスタシステムの導入を行うシステムエンジニアと、クラスタシステム導入後の保守・運用を行うシステム管理者を対象読者とし、CLUSTERPRO を使用したクラスタシステム導入から運用開始前までに必須の事項について説明します。実際にクラスタシステムを導入する際の順番に則して、CLUSTERPRO を使用したクラスタシステムの設計方法、CLUSTERPRO のインストールと設定手順、設定後の確認、運用開始前の評価方法について説明します。

『CLUSTERPRO X リファレンスガイド』(Reference Guide)
管理者、および CLUSTERPRO を使用したクラスタシステムの導入を行うシステムエンジニアを対象とし、CLUSTERPRO の運用手順、各モジュールの機能説明、メンテナンス関連情報およびトラブルシューティング情報等を記載します。『インストール & 設定ガイド』を補完する役割を持ちます。

『CLUSTERPRO X 統合 WebManager 管理者ガイド』(Integrated WebManager Administrator's Guide)
CLUSTERPRO を使用したクラスタシステムを CLUSTERPRO 統合 WebManager で管理するシステム管理者、および統合 WebManager の導入を行うシステムエンジニアを対象読者とし、統合 WebManager を使用したクラスタシステム導入時に必須の事項について、実際の手順に則して詳細を説明します。

CLUSTERPRO マニュアルに関しては、以下を参照してください。
『CLUSTERPRO Web サイト』
http://jpn.nec.com/clusterpro/

『CLUSTERPRO X 3.1 for Windows インストール&設定ガイド』
http://jpn.nec.com/clusterpro/clp/windows/document/x31_w.html

Symantec Endpoint Protection ドキュメント

Symantec Endpoint Protection の詳細については、以下のドキュメントを参照してください。

『Symantec™ Endpoint Protection v12.1、Symantec Endpoint Protection Small Business Edition v12.1、Symantec Network Access Control v12.1 リリースノート』
http://www.symantec.com/business/support/resources/sites/BUSINESS/content/live/DOCUMENTATION/4000/DOC4332/ja_JP/Release_Notes_SEP12.1.pdf

『Symantec™ Endpoint Protection および Symantec Network Access Control 実装ガイド 12.1』
http://www.symantec.com/business/support/resources/sites/BUSINESS/content/live/DOCUMENTATION/4000/DOC4321/ja_JP/Implementation_Guide_SEP12.1.pdf

『Symantec Endpoint Protection 12 簡単インストールガイド』
http://www.symantec.com/content/ja/jp/enterprise/images/theme/endpointsecurity/sep12_install_guide.pdf

『SEP 12.1 バッチファイルを利用して SEP 関連のサービスを停止する方法』
http://www.symantec.com/docs/TECH172688

以下の URL では過去および最新のリリースノートおよびマニュアル類が掲載されています。

『Symantec Endpoint Protection』サポート提供ページ
http://www.symantec.com/business/support/index?page=landing&key=54619

本書で用いる用語

本書で用いる用語について説明します。

用語	説明
SEPM	Symantec Endpoint Protection Manager の略。
SEP クライアント	Symantec Endpoint Protection クライアント の略。

第1章 システム概要

2 ノードのデータミラー型クラスタを構築します。

本書では、データミラー型クラスタ構成を前提とした手順で記載しておりますが、**共有ディスク型クラスタ構成**においても、同様の手順でセキュリティ保護されたクラスタシステムの構築を行うことが可能です。

1.1. システム構成

本書で想定するシステム構成を以下に示します。
SEP クライアントによりセキュリティ保護しているサーバをクラスタ構成にします。現用系と待機系の 2 台のサーバはミラーディスクを用いてデータを共有します。また、ミラーディスクに対するセキュリティ保護は、現用系の SEP クライアントが行い、各 SEP クライアントのセキュリティポリシーは SEPM が制御を行います。

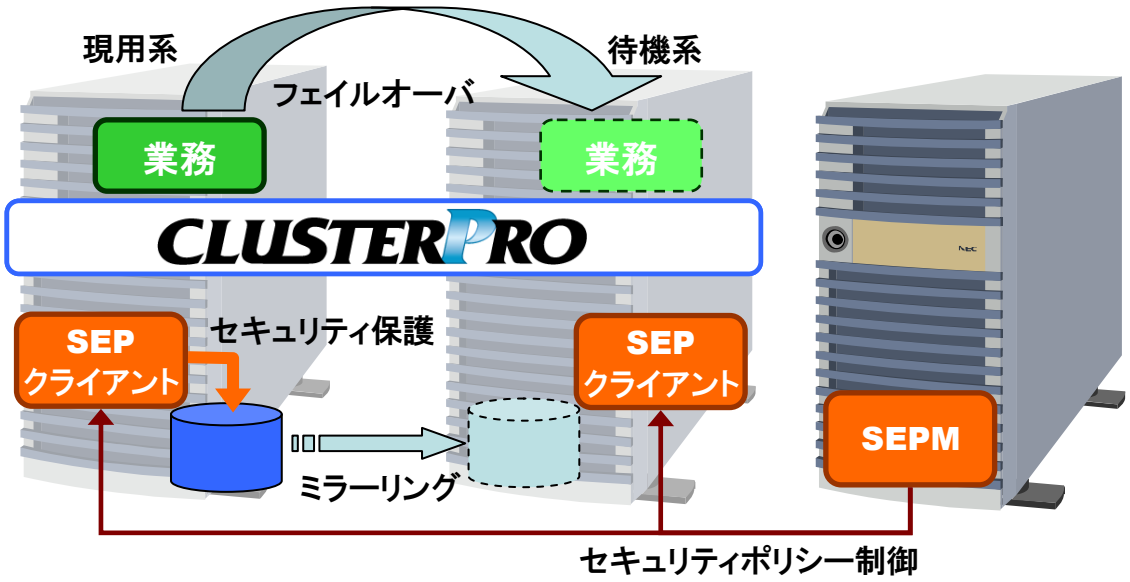

図 1-1 システム構成概要

1.2. ソフトウェア構成

本書では、以下のソフトウェアの組合せで動作確認を行っています。

OS	Windows Server 2008 R2
アプリケーション	Symantec Endpoint Protection 12.1
クラスタウェア	CLUSTERPRO X 3.1 for Windows

第2章 クラスタ構築

SEP クライアントを導入済みのサーバで 2 ノードのデータミラー型クラスタを構築します。
SEP クライアントがミラーディスク内のファイルをウィルススキャン中にフェイルオーバが発生すると、ミラーディスクの非活性処理に失敗する可能性があります。この非活性処理の失敗を回避するために、SEP クライアントを一時停止させてからミラーディスクの非活性処理を行います。

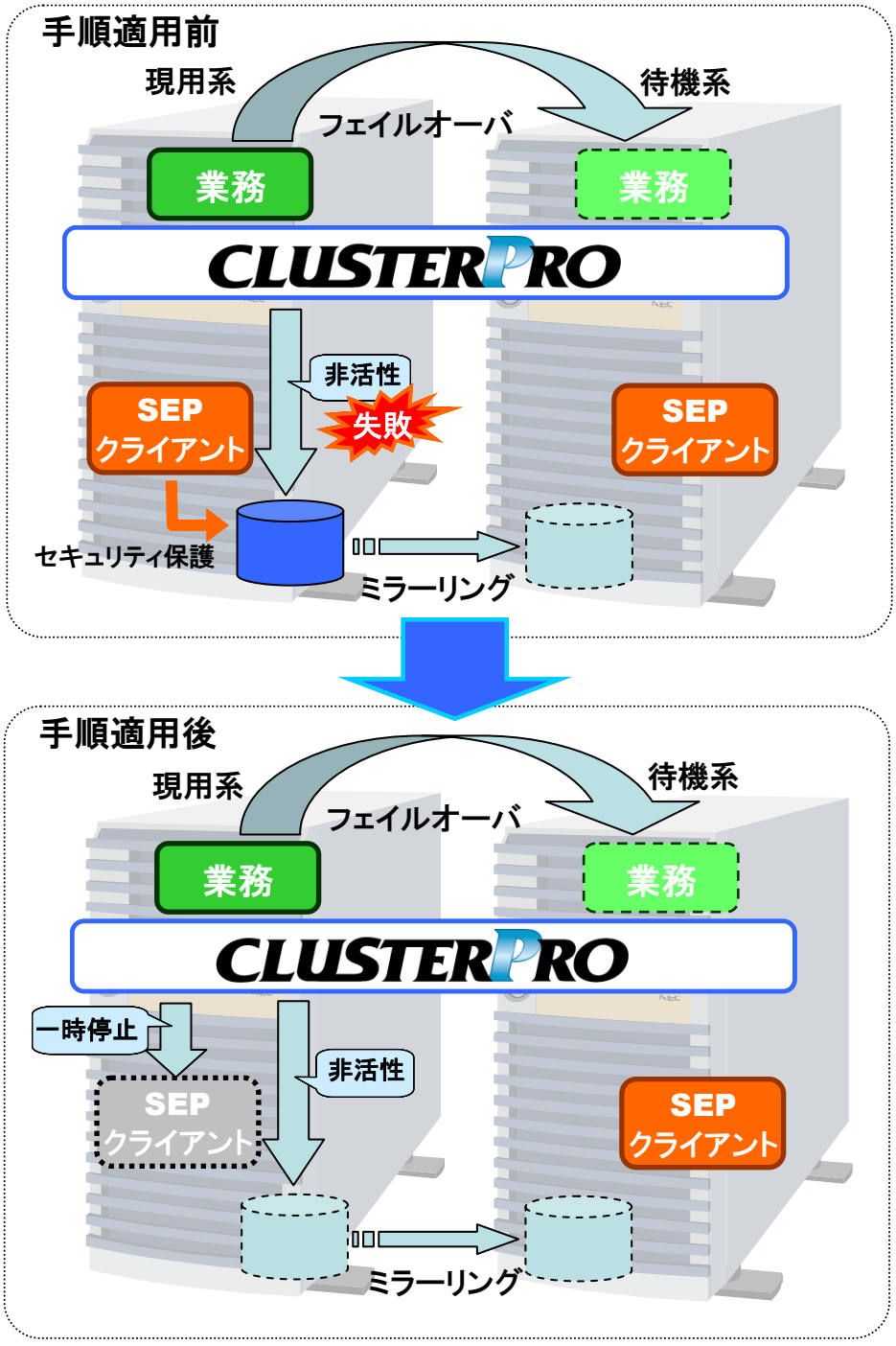

図 2-1 手順適用後のイメージ

2.1. SEPM の設定

CLUSTERPRO から SEP クライアントの制御を行うため、SEPM にてポリシーの設定変更を行います。

SEPM でクライアントグループを作成し、クラスタを構成するサーバをメンバとして登録してください。
ここで作成したグループに対してポリシーの設定変更を行います。

(1) SEPM で対象のクライアントグループを選択し、[ポリシー]タブを選択します。
(2) [ポリシーと設定を親グループから継承する]の設定を「オフ」に変更します。
(3) [場所固有のポリシー]を展開し、このグループで固有な設定をするポリシーを「共有」から「非共有」に変更します。

以下の表を参考に SEP クライアントのポリシー設定を行ってください。

[場所に依存しないポリシーと設定] – [設定] – [全般の設定]

項目		設定内容
再起動の設定	[再起動方法]	「再起動なし」
セキュリティの設定	[クライアントパスワード保護]– [クライアントサービスを停止するためのパスワードを要求する]	「オフ」
	[セキュリティの設定]– [ファイアウォールの停止後にファイアウォールが起動するまですべてのトラフィックを遮断する]	「オフ」

[場所固有のポリシーと設定] – [場所固有のポリシー]

項目		設定内容	備考
ファイアウォールポリシー	[ファイアウォールルール]	CLUSTERPROが使用するポート *1	CLUSTERPROが使用するポートが「遮断」されてないことを確認してください。
侵入防止ポリシー	[ネットワーク侵入防止を有効にする]– 「除外ホスト」	クラスタを構成する2台のサーバ	
例外ポリシー	[例外]– 「フォルダ例外」	CLUSTERPROのインストールフォルダ 「C:¥Program Files¥CLUSTERPRO」	すべてのスキャンを除外するように設定してください。 CLUSTERPROのインストールフォルダをデフォルトから変更している場合は、変更後のフォルダを設定してください。

*1: CLUSTERPRO が使用するポート番号については、『スタートアップガイド』の「第 5 章　注意制限事項　CLUSTERPRO インストール前」を参照してください。

2.2. CLUSTERPRO の設定

フェイルオーバグループには、ミラーディスクリソース以外に、SEP クライアントを制御するためのスクリプトリソースが必要です。また、下図で示す順序で処理が実行されるように、グループリソースの依存関係を設定する必要があります。
本書では、フェイルオーバグループが1つの構成を前提に記載しています。

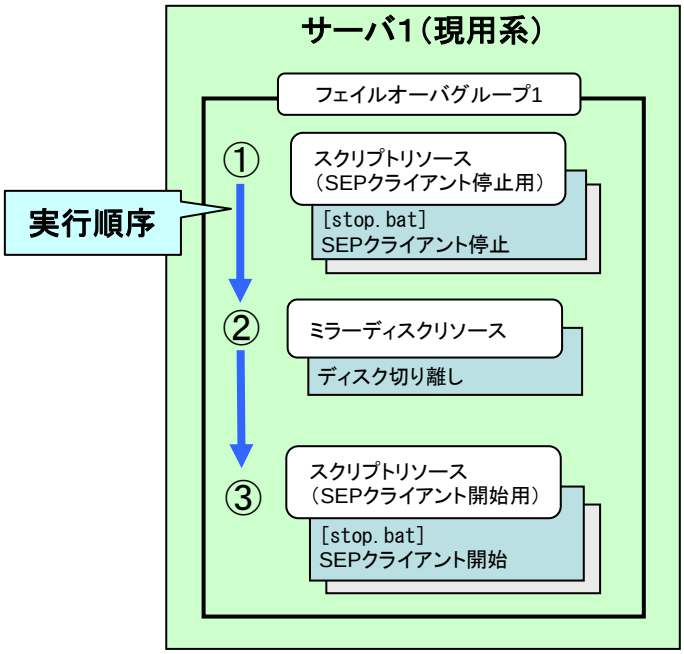

図 2-2 フェイルオーバ時の非活性処理の流れ

2.2.1. フェイルオーバグループへのスクリプトリソース追加

SEP クライアントの停止用と開始用に 2 つのスクリプトリソースを追加します。
SEP クライアントの開始や停止の制御は、各スクリプトリソースの「stop.bat」に記述します。

なお、ミラーディスクの活性時には、SEP クライアントの開始や停止の制御を行いませんので、各スクリプトリソースの「start.bat」は既定のままで利用します。

スクリプトリソース（SEP クライアント停止用）の設定

スクリプトリソース（SEP クライアント停止用）の「stop.bat」には、「付録 サンプルスクリプト」-「SEP クライアント停止用(stop.bat)」のサンプルスクリプトを参考に設定してください。

スクリプトリソース（SEP クライアント開始用）の設定

スクリプトリソース（SEP クライアント開始用）の「stop.bat」には、「付録 サンプルスクリプト」-「SEP クライアント開始用(stop.bat)」のサンプルススクリプトを参考に設定してください。

2.2.2. グループリソースの依存関係の設定

以下のようにグループリソース間の依存関係を設定します。

グループリソース	依存するリソース
スクリプトリソース（SEPクライアント開始用）	none *2
ミラーディスクリソース	スクリプトリソース（SEPクライアント開始用）
スクリプトリソース（SEPクライアント停止用）	ミラーディスクリソース

*2: スクリプトリソース（SEP クライアント開始用）には、依存するリソースを設定しないでください。
「既定の依存関係に従う」のチェックを外して、「依存するリソース」には何も設定しないでください。

2.3. 注意事項

(1) フェイルオーバが正常に完了した後しばらくしてミラーディスク監視/ミラーコネクト監視で「異常」を検知することがあります。
SEP クライアント起動時に一時的にネットワーク通信が遅延する場合がありますが、ミラーディスク監視リソースのリトライ回数（既定値 0 回）を増やすことで一時的な異常検知を回避することができます。

(2) 次の場合、スクリプトで SEP クライアントを停止できないことがあります。
フェイルオーバが異常終了した場合、SEP クライアントの実行状況を確認して適切な対処を行った後、再度フェイルオーバを実行してください。

- SEP クライアントを停止しようとしているサーバで、SEP クライアントの「クライアントユーザーインターフェース」が開いている場合。
「クライアントユーザーインターフェース」を終了させてください。

- SEP クライアントがセキュリティの異常を検知して、次のアクションをユーザに問い合わせ中の場合。
SEP クライアントから通知されたメッセージを確認し、適切なアクションを実行してください。

付録 サンプルスクリプト

各スクリプトには設定変更が必要な箇所を変数として定義しています。**アンダーライン**の箇所を適宜編集してお使いください。

・変数名: SMC_PATH
SEP クライアントのインストールディレクトリを指定します。
SEP クライアントのインストールディレクトリをデフォルトから変更している場合は、変更後のインストールディレクトリを指定してください。

・変数名: LOOP_NUM
SEP クライアントが開始もしくは停止状態になるまで待ち合わせを行う上限回数を指定します。
本サンプルスクリプトでは 60 回(60 秒)を設定していますが、必要に応じて回数を調整してください。
その際、スクリプトリソースのタイムアウト(既定値は 1800 秒)以内にスクリプトが終了するようにしてください。
『SEP 12.1 バッチファイルを利用して SEP 関連のサービスを停止する方法』を参考に、既定値の 60 回(60 秒)を設定しています。

SEP クライアント停止用(stop.bat)

アンダーラインの箇所を適宜編集してお使いください。
注:サンプルスクリプトの以下の記述は、網掛け部分に空白文字2つが含まれます。
スクリプトを使用する際は、同様に反映ください。
FIND /C /I "1 STOPPED"

```
REM ****************************************
REM For STOP SEP
REM SMC_PATH  : Path of smc.exe
REM LOOP_NUM  : Number of loops
REM ****************************************

SET SMC_PATH="C:¥Program Files (x86)¥Symantec¥Symantec Endpoint Protection"
SET LOOP_NUM=60

SET RETVAL=0
SET LOOPCOUNT=-1

REM ****************************************
REM CHECK STARTUP ATTRIBUTES
REM ****************************************
IF "%CLP_EVENT%" == "START" GOTO NORMAL
IF "%CLP_EVENT%" == "FAILOVER" GOTO FAILOVER

REM CLUSTERPRO Server is not started
ARMBCAST /MSG "CLUSTERPRO Server is offline" /A
GOTO EXIT

REM ****************************************
REM NORMAL AND FAILOVER STOP PROCESS
REM ****************************************
:NORMAL
:FAILOVER
```

```
REM ********************
REM SMC STOP
REM ********************

%SMC_PATH%¥SMC.EXE -STOP

REM ********************
REM SMC SERVERCE STATE
REM ********************
:SMC_LOOP
ARMSLEEP 1
FOR /f %%B IN ('SC QUERY smcservice ^| FIND /C /I "1  STOPPED"') DO SET SMC_STATE=%%B
IF %SMC_STATE% EQU 1 SET RETVAL=0
IF %SMC_STATE% EQU 0 SET RETVAL=1

IF %RETVAL% EQU 0 (
          CLPLOGCMD -m "SMC STOP Command Success(%RETVAL%)" -l INFO
          GOTO SMC_EXIT
)

SET /A LOOPCOUNT=%LOOPCOUNT%+1
IF %LOOPCOUNT% LEQ %LOOP_NUM% GOTO SMC_LOOP

:SMC_EXIT
IF %RETVAL% EQU 1 (
          CLPLOGCMD -m "SMC STOP Command Failed(%RETVAL%)" -l ERR
          GOTO EXIT
)

REM ********************
REM SRTSP SERVICE STOP
REM ********************

SC STOP SRTSP

REM ********************
REM SRTSP SERVICE STATE
REM ********************

FOR /F %%A IN ('SC QUERY SRTSP ^| FIND /C /I "1  STOPPED"') DO SET SMC_STATE=%%A
IF %SMC_STATE% EQU 1 SET RETVAL=0
IF %SMC_STATE% EQU 0 SET RETVAL=1

IF %RETVAL% EQU 0 (
          CLPLOGCMD -m "SRTSP STOP Command Success(%RETVAL%)" -l INFO
) ELSE (
          CLPLOGCMD -m "SRTSP STOP Command Failed(%RETVAL%)" -l ERR
)

:EXIT
SET ERRORLEVEL=%RETVAL%
```

SEP クライアント開始用(stop.bat)

アンダーラインの箇所を適宜編集してお使いください。

注:サンプルスクリプトの以下の記述は、網掛け部分に空白文字2つが含まれます。
スクリプトを使用する際は、同様に反映ください。
FIND /C /I "4 RUNNING"

```
REM ****************************************
REM For START SEP
REM SMC_PATH  : Path of smc.exe
REM LOOP_NUM  : Number of loops
REM ****************************************

SET SMC_PATH="C:¥Program Files (x86)¥Symantec¥Symantec Endpoint Protection"
SET LOOP_NUM=60

SET RETVAL=0
SET LOOPCOUNT=-1

REM ****************************************
REM CHECK STARTUP ATTRIBUTES
REM ****************************************
IF "%CLP_EVENT%" == "START" GOTO NORMAL
IF "%CLP_EVENT%" == "FAILOVER" GOTO FAILOVER

REM CLUSTERPRO Server is not started
ARMBCAST /MSG "CLUSTERPRO Server is offline" /A
GOTO EXIT

REM ****************************************
REM NORMAL AND FAILOVER STOP PROCESS
REM ****************************************
:NORMAL
:FAILOVER

REM ********************
REM SRTSP SERVICE START
REM ********************

SC START SRTSP

REM ********************
REM SRTSP SERVICE STATE
REM ********************

FOR /F %%A IN ('SC QUERY SRTSP ^| FIND /C /I "4  RUNNING"') DO SET SMC_STATE=%%A
IF %SMC_STATE% EQU 1 SET RETVAL=0
IF %SMC_STATE% EQU 0 SET RETVAL=1

IF %RETVAL% EQU 0 (
        CLPLOGCMD -m "SRTSP START Command Success(%RETVAL%)" -l INFO
) ELSE (
        CLPLOGCMD -m "SRTSP START Command Failed(%RETVAL%)" -l ERR
        GOTO EXIT
)
```

```
REM ********************
REM SMC START
REM ********************

%SMC_PATH%¥SMC.EXE -START

REM ********************
REM SMC SERVICE STATE
REM ********************
:SMC_LOOP
ARMSLEEP 1
FOR /F %%B IN ('SC QUERY smcservice ^| FIND /C /I "4  RUNNING"') DO SET SMC_STATE=%%B
IF %SMC_STATE% EQU 0 (
          SET RETVAL=1
) ELSE (
          SET RETVAL=0
)

IF %RETVAL% EQU 0 (
          CLPLOGCMD -m "SMC START Command Success(%RETVAL%)" -l INFO
          GOTO SMC_EXIT
)

SET /A LOOPCOUNT=%LOOPCOUNT%+1

IF %LOOPCOUNT% LEQ %LOOP_NUM% GOTO SMC_LOOP

:SMC_EXIT
IF %RETVAL% EQU 1 (
          CLPLOGCMD -m "SMC START Command Failed(%RETVAL%)" -l ERR
)

:EXIT
SET ERRORLEVEL=%RETVAL%
```