



shaping tomorrow with you

# Fujitsu SPARC M12/M10 Plug-In for Oracle Enterprise Manager Cloud Control 導入ガイド

2019年 3月

2.2版

富士通株式会社

## ■ 使用条件

- 著作権・商標権・その他の知的財産権について

コンテンツ(文書・画像・音声等)は、著作権・商標権・その他の知的財産権で保護されています。

本コンテンツは、個人的に使用する範囲でプリントアウトまたはダウンロードできます。ただし、これ以外の利用(ご自分のページへの再利用や他のサーバへのアップロード等)については、当社または権利者の許諾が必要となります。

- 保証の制限

本コンテンツについて、当社は、その正確性、商品性、ご利用目的への適合性等に関して保証するものではなく、そのご利用により生じた損害について、当社は法律上のいかなる責任も負いかねます。本コンテンツは、予告なく変更・廃止されることがあります。

## ■ 輸出管理規制について

- 本ドキュメントを輸出または第三者へ提供する場合は、お客様が居住する国および米国輸出管理関連法規等の規制をご確認のうえ、必要な手続きをおとりください。

## ■ 高度な安全性が要求される用途への使用について

- 本製品は、一般事務用、パーソナル用、家庭用、通常の産業等の一般的用途を想定して開発・設計・製造されているものであり、原子力施設における核反応制御、航空機自動飛行制御、航空交通管制、大量輸送システムにおける運行制御、生命維持のための医療用機器、兵器システムにおけるミサイル発射制御など、極めて高度な安全性が要求され仮に当該安全性が確保されない場合、直接生命・身体に対する重大な危険性を伴う用途(以下「ハイセイフティ用途」という)に使用されるよう開発・設計・製造されたものではありません。

お客様は本製品を必要な安全性を確保する措置を施すことなくハイセイフティ用途に使用しないでください。また、お客様がハイセイフティ用途に本製品を使用したことにより発生する、お客様または第三者からのいかなる請求または損害賠償に対しても富士通株式会社およびその関連会社は一切責任を負いかねます。

## ■ 商標

- UNIX は、米国およびその他の国におけるオープン・グループの登録商標です。
- SPARC Enterprise, SPARC64, SPARC64 ロゴ、およびすべての SPARC 商標は、米国 SPARC International, Inc. のライセンスを受けて使用している、同社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。
- Oracle と Java は、Oracle Corporation およびその子会社、関連会社の米国およびその他の国における登録商標です。
- その他記載されている製品名などの固有名詞は、各社の商標または登録商標です。

## 目次

1. はじめに .....	1
2. インストールの準備 .....	2
2-1. サポートする環境およびシステム .....	2
2-2. サポートする管理対象の富士通サーバ .....	3
2-3. ソフトウェア要件 .....	4
3. SPARC M12/M10 Plug-in for EMCC のインストール.....	4
3-1. OPAR ファイルのインポート.....	4
3-2. プラグインの OMS へのデプロイ.....	4
3-3. プラグインの OMA へのデプロイ.....	5
3-4. SPARC M12/M10 の XSCF のターゲット手動追加 .....	6
3-5. ターゲットからの SNMPv3 トラップ受信のための設定 .....	7
3-6. ターゲットからの SNMPv1 トラップ受信のための設定 .....	8
4. SPARC M12/M10 の XSCF ターゲットの削除 .....	10
4-1. ターゲットの削除 .....	10
4-2. ターゲットの SNMPv3 トラップ送信設定の削除.....	10
4-3. ターゲットの SNMPv1 トラップ送信設定の削除.....	10
5. SPARC M12/M10 Plug-in のアンインストール .....	11
5-1. OMA および OMS からのアンデプロイ .....	11
5-2. SPARC M12/M10 plug-in の削除.....	12

# 1. はじめに

## 本書の内容

- 本書は SPARC M12/M10 Plug-In for Oracle Enterprise Manager Cloud Control 13.2.1.0.0 のインストール手順を記載した資料です。
- 本資料は、Oracle Enterprise Manager Cloud Control(以下、EMCC)および SPARC M12/M10 の基本知識を有するシステム管理者を対象としています。EMCC に関する詳細については、以下の URL を参照ください。  
<http://docs.oracle.com/en/enterprise-manager/>
- SPARC M12/M10 Plug-in for EMCC は以下のサーバをサポートします。
  - SPARC M12
  - SPARC M10

## 留意事項

- 本書では、Oracle Solaris を Solaris と記載することがあります。また、Oracle VM Server for SPARC を Oracle VM または OVM と記載することがあります。

## 2. インストールの準備

SPARC M12/M10 Plug-in for EMCC をインストールするためには、以下が必要です。

- 以下のコンポーネントを含む EMCC のインストールおよび環境設定:
  - Oracle Management Server (OMS)
  - Oracle Management Agent (OMA)

### 2-1. サポートする環境およびシステム

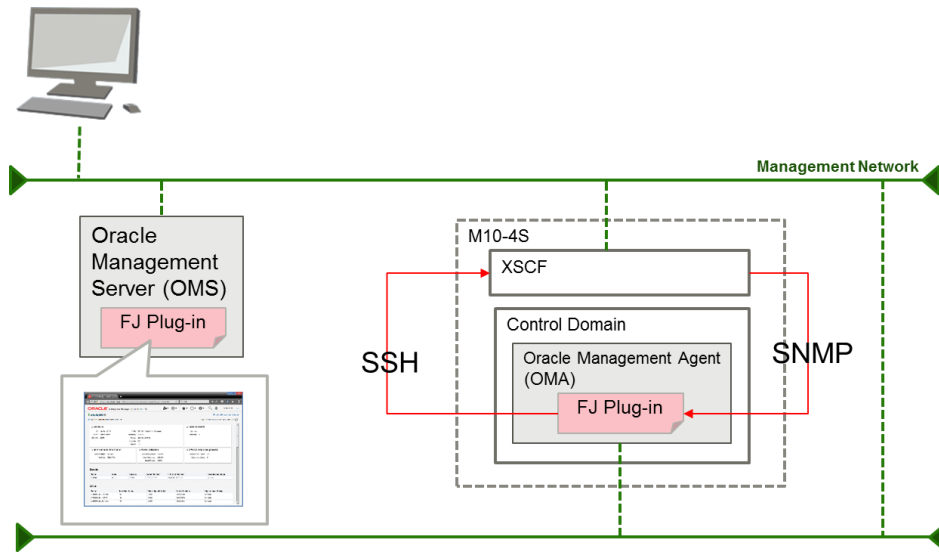
SPARC M12/M10 Plug-in for EMCC は以下のバージョンのソフトウェアをサポートします。

- EMCC:
  - Oracle Enterprise Manager Cloud Control 13c Release 3
  - Oracle Enterprise Manager Cloud Control 13c Release 2 (OMS のパッチ 25453518 が必要です)
- OMS:
  - Oracle Solaris 11.1 以降
  - Oracle Solaris 10 1/13 以降
- OMA:
  - Oracle Solaris 11.1 以降
  - Oracle Solaris 10 1/13 以降

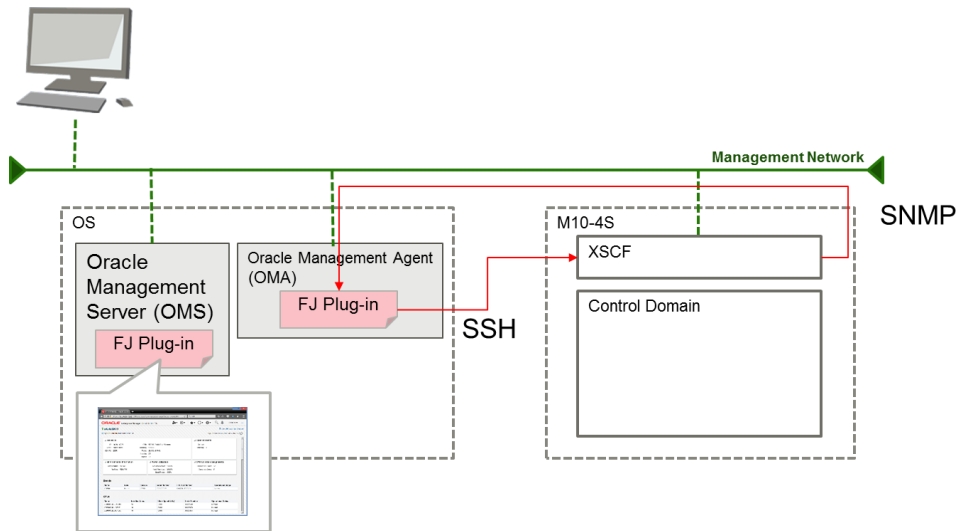
注 1: OMA は、SPARC M12/M10 の制御ドメインへのインストールを推奨します。以下の例 2 の構成の場合、  
"Disk Controllers"および"Storage"の表は表示されません。

注 2: Oracle Solaris 10 の制御ドメインに OMA はインストールできないため、Oracle Solaris 10 に対して  
以下の例 1 の構成は組めません。

[例 1 : 推奨]



[例 2 : 制御ドメインから XSCF へのネットワーク経路がない環境]



## 2-2. サポートする管理対象の富士通サーバ

SPARC M12

SPARC M10

## 2-3.ソフトウェア要件

- Web ブラウザ:
  - Mozilla Firefox 49 以降
  - Google Chrome 55 以降

# 3. SPARC M12/M10 Plug-in for EMCC のインストール

## 3-1.OPAR ファイルのインポート

1. 最新の Oracle Plug-In Archive (zip) ファイルを、以下のサイトからダウンロードします。  
[https://updatesite.jp.fujitsu.com/unix/jp/download/software/unix\\_soft/emcc\\_plug-in/download/index.html](https://updatesite.jp.fujitsu.com/unix/jp/download/software/unix_soft/emcc_plug-in/download/index.html)
2. ダウンロードした zip ファイルを OMS の任意のディレクトリに配置し、展開します。展開先に OPAR ファイルが配置されます。
3. EMCC のコンソールにログインし、**設定(⚙)** → **拡張性** → **自己更新** を選択します。
4. **自己更新** 画面で、**アクション** → **インポート元** → **管理対象ホスト** を選択します。
5. **管理対象ホストからの更新インポート**画面で、インポートするプラグインを選択します。
  - 5-1. ホスト (必須)  
**検索と選択:** ホスト ウィンドウを開き、一覧から**ターゲットタイプ**がホスト、かつ**ターゲット名**が OMS の行を選択します。
  - 5-2. 場所 (必須)  
**リモート・ファイル・ブラウザ:** ウィンドウを開き、以下を実行します。
    - **ログイン**を選択し、OMS にログインする認証情報(ホスト資格証明)を選択します。認証情報が存在しない場合、**新規**を選択し、以下を設定します。
      - **ホスト資格証明ウィンドウ**で、**ユーザー名**および**パスワード**を設定し、**OK**を選択します。
    - **リモート・ファイル・ブラウザ** ウィンドウで、OPAR ファイルを配置したディレクトリに移動し、OPAR ファイルを選択し、**追加**を選択します。
    - **選択されたファイルまたはフォルダ**の一覧に、選択した OPAR ファイルが表示されていることを確認し、**OK**を選択します。
6. **管理対象ホストからの更新インポート**ウィンドウで**インポート**を選択します。しばらくすると**確認**ウィンドウが開きますので、**閉じる**を選択します。

## 3-2.プラグインの OMS へのデプロイ

1. EMCC のコンソールにログインし、**設定(⚙)** → **拡張性** → **プラグイン** を選択します。

2. プラグイン画面で、一覧のサーバー、ストレージおよびネットワークの下の **Systems Infrastructure XSCF** を選択します。
3. デプロイ先から**管理サーバー...**を選択します。



4. **管理サーバー上のプラグインのデプロイ:** プラグイン画面で、一覧からデプロイするプラグインの行を選択し、**次**を選択します。
5. **管理サーバー上のプラグインのデプロイ:** 前提条件チェック画面で、前提条件チェックに"正常に完了"が表示されるまで待ち、表示された後に**次**を選択します。
6. **管理サーバー上のプラグインのデプロイ:** リポジトリ画面で、ロールが SYSDBA のリポジトリの SYS 資格証明を選択し、**次**を選択します。SYS 資格証明が存在しない場合、**新規**を選択して SYS ユーザの資格証明を作成します。
7. **管理サーバー上のプラグインのデプロイ:** 確認画面で、設定値が正しいことを確認し、**デプロイ**を選択し、**ステータスの表示**を選択します。
8. **デプロイメント・アクティビティ画面**で、自動リフレッシュをオフ以外に設定し、一覧のステータスの列の全ての行が**成功(✓)**になるまで待ちます。
9. **設定(⚙️) → 拡張性 → プラグイン** を選択します。プラグイン画面で、一覧のサーバー、ストレージおよびネットワークの下の **Systems Infrastructure XSCF** の管理サーバー上の列に表示されたバージョンを確認します。

名前	最新の使用可能	最新ダウンロード	管理サーバー上
 Systems Infrastructure XSCF	13.2.1.0.0	13.2.1.0.0	13.2.1.0.0

### 3-3. プラグインの OMA へのデプロイ

1. EMCC のコンソールにログインし、**設定(⚙️) → 拡張性 → プラグイン** を選択します。
2. プラグイン画面で、一覧のサーバー、ストレージおよびネットワークの下の **Systems Infrastructure XSCF** を選択します。
3. デプロイ先から**管理エージェント...**を選択します。



4. **管理エージェント上のプラグインをデプロイします画面**で、バージョンのプルダウンにてデプロイするバージョンを選択し、**続行**を選択します。



5. **管理エージェントの一覧**からプラグインをデプロイする OMA を選択し、**続行**を選択します。2-1の例 1 の場合は M12/M10 の OMA を選択してください。
6. **前提条件チェック**画面でデプロイする OMA のステータスが**成功(✓)**であることを確認し、**次**を選択します。
7. **確認**画面で、これまでの設定内容が正しいことを確認し、**デプロイ**を選択します。
8. **確認**画面で、**ステータスの表示**を選択します。
9. **デプロイメント・アクティビティ**画面で、**自動リフレッシュ**をオフ以外に設定し、一覧のステータスの列の全ての行が**成功(✓)**になるまで待ちます。
10. EMCC コンソールの上部の**設定(⚙️)** → **拡張性** → **プラグイン** を選択します。**プラグイン**画面で、一覧のサーバー、ストレージおよびネットワークの下の **Systems Infrastructure XSCF** のプラグイン付き管理エージェントの列の数値を選択します。
  - ☛ ブラウザの優先言語設定が日本語の場合、数値を選択しても、プラグイン情報画面に遷移しない場合があります。遷移しない場合、プラグイン画面の任意のフォルダ(例: データベース)を展開表示後、該当の数値を選択してください。
11. **プラグイン情報**画面で、OMA にデプロイされたプラグインのバージョンを確認します。

管理エージェントのプラグ  
イン・バージョン

13.2.1.0.0

### 3-4.SPARC M12/M10 の XSCF のターゲット手動追加

1. EMCC のコンソールにログインし、**設定(⚙️)** → **ターゲットの追加** → **ターゲットの手動追加** を選択します。
2. **ガイド付きプロセス**を使用した**追加**を選択し、**システム・インフラストラクチャ・サーバー-XSCF** を選択し、**追加...**を選択します。
3. **Fujitsu XSCF 検出**画面で、XSCF(SPARC M12/M10 上のサービスプロセッサ)に対するプラグインからの接続に関して設定し、**追加**を選択します。

#### 3-1. ターゲット(必須)

- ターゲット名 : XSCF に対する一意の名前。
- XSCF の FQDN または IP アドレス : XSCF の FQDN(完全修飾ドメイン名)または IP アドレス。

☛ 冗長構成の SPARC M12-2S/M10-4S の XSCF をターゲットとされる場合、引継ぎ IP アドレスを使用ください。

#### 3-2. モニタリング・エージェント(必須)

- モニタリング・エージェント EMD URL : デプロイ先の OMA に対するモニタリング・エージェント EMD URL を選択。

#### 3-3. SNMPv3 資格証明プロパティ(オプション)

- SNMP エンジン ID : エンジン ID(16 進数の文字列)

☛ EMCC 13c Release 2 の場合、エンジン ID 先頭は 8~F の範囲の値を設定してください。

4. **システム・インフラストラクチャ・サーバー-XSCF モニタリング資格証明**画面が表示されます。追加するターゲットに対する **SSH モニタリング資格証明**の行を選択し、**資格証明の設定**を選択します。

5. **モニタリング資格証明の入力画面が表示されます。以下を入力し、保存を選択します。**
  - ユーザー名 : XSCF 上のユーザー名。
  - パスワード/Confirm パスワード : ユーザーのパスワード
  - ☛ 入力項目の文字列が"Username"、"Password"および"Confirm Password"と表示される場合がありますが、問題ありません。そのまま、入力項目に XSCF 上のユーザー名とユーザーのパスワードを入力してください。(プラグインの OMA へのデプロイ後、通常 20 分程度で日本語表示されます。)
6. **ターゲット(🎯) → すべてのターゲット** を選択し、**すべてのターゲット画面の一覧から、追加したターゲット名** を選択します。
7. **ターゲットのシステム・インフラストラクチャ・サーバー-XSCF** 画面が表示されます。全ての項目が表示できるようになるまで約 20 分待ちます。その後画面右上のリフレッシュアイコン (🔄) を選択します。

### 3-5.ターゲットからの SNMPv3 トラップ受信のための設定

1. EMCC のコンソールにログインし、**設定(⚙️) → セキュリティ → モニタリング資格証明** を選択します。
2. モニタリング資格証明画面で、**ターゲット・タイプ**の列が**システム・インフラストラクチャ・サーバー-XSCF**の行を選択し、**モニタリング資格証明の管理**を選択します。
3. **システム・インフラストラクチャ・サーバー-XSCF** **モニタリング資格証明**画面で、**資格証明セット**の列が**SNMP v3** **モニタリング資格証明**の行を選択し、**資格証明の設定**を選択します。
4. **モニタリング資格証明書**の入力ウィンドウで、以下を設定し、**保存**を選択します。
  - ユーザー名 : ユーザー名
  - 認可パスワード/認可パスワードの確認 : 認証パスワード
  - 認可プロトコル: 認証プロトコル(SHA または MD5 を選択)
  - プライバシ・パスワード/プライバシ・パスワードの確認 : 暗号化パスワード
  - プライバシ・プロトコル: 暗号化プロトコル(DES または AES128 を選択)
  - ☛ プライバシ・プロトコルは EMCC 13c Release 3 以降の場合に選択できます。EMCC 13c Release 2 の場合、プライバシ・パスワードは表示されません。常に DES で動作します。
5. **ターゲット(🎯) → すべてのターゲット** を選択し、**すべてのターゲット画面の一覧から、トラップを受信するターゲット名**を選択します。
6. **ターゲットのシステム・インフラストラクチャ・サーバー-XSCF** 画面で、**システム・インフラストラクチャ・サーバー-XSCF → ターゲット設定 → モニタリング構成**を選択します。
7. **モニタリング構成の SNMP エンジン ID** に、エンジン ID を 16 進数の文字列で設定し、**OK** を選択します。
  - ☛ EMCC 13c Release 2 の場合、エンジン ID 先頭は 8~F の範囲の値を設定してください。
8. **正常に保存しました**ウィンドウが起動された場合、**OK** を選択します。

9. 任意の端末から SSH にて XSCF にログインし、SNMP サービスを有効にします。

例:

```
XSCF> setsnmp enable
```

10. Trap Hosts を設定します。Trap Hosts はプラグインのターゲットの OMA を設定しなければなりません。OMA のポート番号の初期値は 3872 です。4. および 7. で登録した値を、XSCF の Trap Hosts に設定します。

例:

- ユーザー名 : username
- 認証パスワードおよび暗号化パスワード : passwd
- 認証プロトコル : SHA
- 暗号化プロトコル : DES
- エンジン ID : 9876543210

```
XSCF> setsnmp addv3traphost -u username -n 0x9876543210 -r SHA -a passwd -e passwd -p 3872 -x DES 192.168.10.20
```

11. SNMP の設定を確認します。

例:

```
XSCF> showsnmp
```

```
Agent Status:      Enabled
Agent Port:        161
System Location:   Unknown
System Contact:    Unknown
System Description: Unknown
```

Trap Hosts:

Hostname	Port	Type	Community String	Username	Auth	Encrypt
192.168.10.20	3872	v3	n/a	username	SHA	DES

SNMP V1/V2c: None

Enabled MIB Modules:

SP MIB

### 3-6.ターゲットからの SNMPv1 トラップ受信のための設定

SNMPv3 トラップ受信を設定済みの場合、基本的に本設定は不要です。次節に進んでください。

1. EMCC のコンソールにログインし、設定(⚙️) → セキュリティ → モニタリング資格証明 を選択します。
2. モニタリング資格証明画面で、ターゲット・タイプの列がシステム・インフラストラクチャ・サーバー XSCF の行を選択し、モニタリング資格証明の管理を選択します。
3. システム・インフラストラクチャ・サーバー XSCF モニタリング資格証明画面で、資格証明セットの列が **SNMP v1** モニタリング資格証明の行を選択し、資格証明の設定を選択します。
4. モニタリング資格証明書の入力ウィンドウで、コミュニティ文字列を設定し、保存を選択します。

5. 任意の端末から SSH にて XSCF にログインし、SNMPv1 サービスを有効にします。

例:

```
XSCF> setsnmp enable
XSCF> setsnmp enablev1v2c public
```

6. Trap Hosts を設定します。Trap Hosts はプラグインのターゲットの OMA を設定しなければなりません。OMA のポート番号の初期値は 3872 です。また、-s オプションのコミュニティ文字列は、4. で設定したコミュニティ文字列を設定します。

例:

```
XSCF> setsnmp addtraphost -t v1 -p 3872 -s public 192.168.10.20
```

7. SNMP の設定を確認します。

例:

```
XSCF> showsnmp

Agent Status:      Enabled
Agent Port:        161
System Location:   Unknown
System Contact:    Unknown
System Description: Unknown

Trap Hosts:

Hostname      Port Type  Community String Username      Auth Encrypt
-----
192.168.10.20 3872 v1    public          n/a          n/a  n/a

SNMP V1/V2c:

Status:          Enabled
Community String: public

Enabled MIB Modules:

SP MIB
XSCF>
```

## 4. SPARC M12/M10 の XSCF ターゲットの削除

### 4-1. ターゲットの削除

1. EMCC のコンソールにログインし、ターゲット(🎯) → **すべてのターゲット** を選択し、**すべてのターゲット画面**の  
一覧から、削除する**ターゲット名**を選択します。
2. ターゲットの**システム・インフラストラクチャ・サーバー-XSCF** 画面で、**システム・インフラストラクチャ・サーバー-XSCF**  
→ **ターゲット設定** → **ターゲットの削除**を選択します。
3. **確認**ウィンドウで、**はい**を選択します。
4. **すべてのターゲット画面**に、以下のメッセージが表示されることを確認します。

#### 情報

ターゲット (システム・インフラストラクチャ・サーバー-XSCF)が削除されました。

### 4-2. ターゲットの SNMPv3 トラップ送信設定の削除

1. 任意の端末から SSH にて XSCF にログインし、Trap Hosts から OMA に対する SNMPv3 トラップ送信設定を  
削除します。

例:

```
XSCF> setsnmp remv3traphost -u username 192.168.10.20
```

### 4-3. ターゲットの SNMPv1 トラップ送信設定の削除

1. 任意の端末から SSH にて XSCF にログインし、Trap Hosts から OMA に対する SNMPv1 トラップ送信設定を  
削除します。

例:

```
XSCF> setsnmp remtraphost -t v1 192.168.10.20
```

## 5. SPARC M12/M10 Plug-in のアンインストール

### 5-1. OMA および OMS からのアンデプロイ

#### [OMA]

1. EMCC のコンソールにログインし、**設定(⚙️)** → **拡張性** → **プラグイン** を選択します。
2. **プラグイン**画面で、一覧のサーバー、ストレージおよびネットワークの下の **Systems Infrastructure XSCF** を選択します。
3. **アンデプロイ元**から**管理エージェント...**を選択します。
4. **管理エージェントからのプラグインのアンデプロイ**ウィンドウの一般画面で、**追加...**を選択し、**ターゲットの選択画面**の一覧から削除する全ての**ターゲット名**を選択し、**選択**を選択します。
5. **管理エージェントからのプラグインのアンデプロイ**ウィンドウの一般画面で、**続行**を選択します。
6. **管理エージェントからのプラグインのアンデプロイ**ウィンドウの**前提条件チェック**画面で、すべてのステータスの列の表示が**成功(✔️)**であることを確認し、**次**を選択します。
7. **管理エージェントからのプラグインのアンデプロイ**ウィンドウの**確認**画面で、**アンデプロイ**を選択し、**ステータスの表示**を選択します。
8. **デプロイメント・アクティビティ**画面で、**自動リフレッシュ**を**オフ**以外に設定し、ステータスの列の全ての行が**成功 (✔️)**になるまで待ちます。

#### [OMS]

9. **設定(⚙️)** → **拡張性** → **プラグイン** を選択します。
10. **プラグイン**画面で、一覧のサーバー、ストレージおよびネットワークの下の **Systems Infrastructure XSCF** を選択します。
11. **アンデプロイ元**から**管理サーバー...**を選択します。
12. **管理サーバーからのプラグインのアンデプロイ**ウィンドウの一般画面で、リポジトリ **SYS** パスワードにデータベースの **SYS** ユーザのパスワードを入力し、**続行**を選択します。
13. **管理サーバーからのプラグインのアンデプロイ**ウィンドウの**確認**画面で、**アンデプロイ**を選択し、**ステータスの表示**を選択します。
14. **デプロイメント・アクティビティ**画面で、**自動リフレッシュ**を**オフ**以外に設定し、ステータスの列の全ての行が**成功 (✔️)**になるまで待ちます。

## 5-2.SPARC M12/M10 plug-in の削除

1. EMCC のコンソールにログインし、**設定(⚙)** → **拡張性** → **自己更新** を選択します。
2. **自己更新** 画面で、一覧から**タイプ**の列の**プラグイン**を選択します。
3. **プラグイン更新**画面で、**プラグイン名**の列の **System Infrastructure XSCF** の行を選択し、**アクション** → **削除** を選択します。
4. **更新の削除**ウインドウで、**削除**を選択し、**確認**ウインドウで、**OK**を選択します。

## 改版履歴

改版年月	版数	改版内容
2017.04	1.0	新規作成
2017.07	1.1	SNMP v3トラップ対応
2018.03	2.0	- Adobe Flash コンテンツから Javascript/HTML コンテンツへの移行。 - 日本語表示対応
2018.11	2.1	サポートする Oracle Enterprise Manager Cloud Control バージョンを変更。
2019.03	2.2	Oracle Enterprise Manager Cloud Control 13c Release 3 対応



**FUJITSU**

shaping tomorrow with you