CLUSTERPRO XによるLogstorage X/SIEMの冗長構成構築手順

本資料は、CLUSTERPRO Xを利用したLogstorage X/SIEM
冗長構成の作成手順についての情報を記載しています。

Version1.7.0対象
2021/01/21
文書番号:PDT-L1002-202101-01

Infoscience インフォサイエンス株式会社

本資料について

CLUSTERPRO Xを利用したLogstorage X/SIEM冗長構成の作成手順について説明します。

対象読者

本資料は、Logstorage X/SIEMの冗長化構成の導入/運用を検討する方を対象としています。
Logstorage X/SIEM、CLUSTERPRO Xについて基本的な操作を行える事を前提としています。

商標及びお願い

- CLUSTERPRO Xは日本電気株式会社の登録商標です。
- その他、本資料に記載されている会社名・商品名などは一般的に各社の商標または登録商標です。
- 本資料では ™、©、® を割愛します。
- 本資料の一部または全部を著作権法の定める範囲を超え、出版元から文書による承諾を得ずに無断で複写、複製、転載することを禁じます。

免責事項

- 本資料の内容は、予告なしに変更されることがあります。
- CLUSTERPRO Xの操作および設定については弊社サポート対象外となります。
- 本資料は、導入環境がLogstorage X/SIEM及びCLUSTERPRO Xのシステム要件を満たすことを前提としています。
- インフォサイエンス株式会社は、本資料の技術的あるいは編集上の誤り、欠落について責任を負いかねます。
  本資料の内容は、特定の環境において正確である事を当社で確認しておりますが、
  お客様の環境に適当する場合、本資料の利用はお客様自身の責任により行って頂く必要があります。

表記規則

- マニュアルの表記規則は以下の通りです。

表1 表記規則

表記	説明
等幅ゴシック体	コマンドラインや実行例などユーザの入力実行結果を表わす
文頭の文字「#」「>」	その文がコマンドラインでの入力コマンド、またはスクリプト内のコメント文であることを示す。
文末の文字文字「↵」	その文がコマンドラインでの入力コマンドの場合は[Enter キーの入力]を示し、スクリプト内の入力文字列の場合は[改行]であることを示す。

また、製品についての注意事項は、以下のように表記しています。

製品の仕様やプラットフォームに関する注意事項を表わします。

当該の機能を利用するにあたり、重大な問題につながる可能性がある事項を表します。

目次

図の一覧

表の一覧

第1章 はじめに

本資料では、HAクラスタリングソフトウェアであるCLUSTERPRO　Xを使用し、システム停止時間の最小化を目的としたLogstorage X/SIEMの冗長化設定について説明します。

システム構成としてはサーバ2台での片方向スタンバイ型を想定しています。
尚、HAクラスタや、その用語については「CLUSTERPRO Xインストール＆設定ガイド」や「CLUSTERPRO Xスタートアップガイド」などを参照して下さい。

製品名称の表記について

以降、CLUSTERPRO Xを「CLUSTERPRO」、Logstorage X/SIEMを「X/SIEM」と表記します。

1.1. 動作環境

本資料では、下記環境での冗長化設定について確認しています。これ以外の環境では、お客様にて動作の確認をお願い致します。

- Logstorage X/SIEM 1.7
- CLUSTERPRO X 4.2
- Windows Server 2019

1.2. X/SIEM冗長化におけるシステム構成

サーバ2台を現用系/待機系として動作させる構成です。
通常時、クライアントやログソースは現用系サーバにアクセスします。

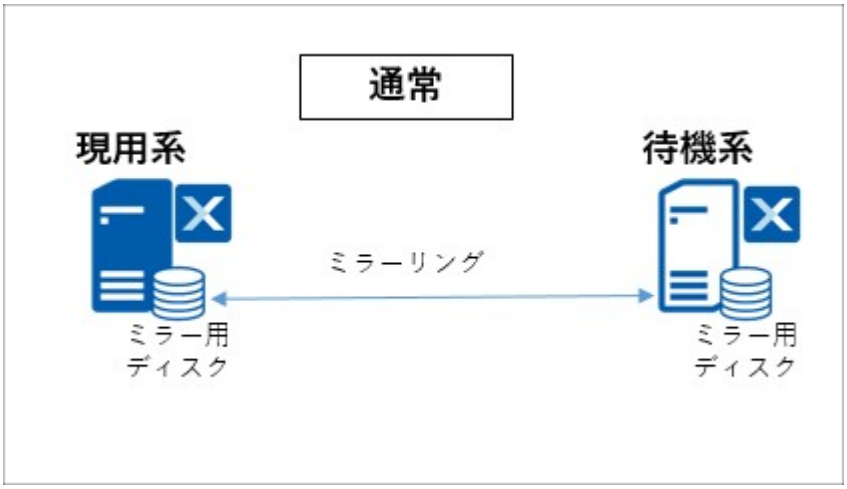

図1 システム構成（通常時）

現用系に障害が発生するとフェイルオーバして待機系が起動し、以後、クライアントやログソースは待機系サーバにアクセスするようになります。

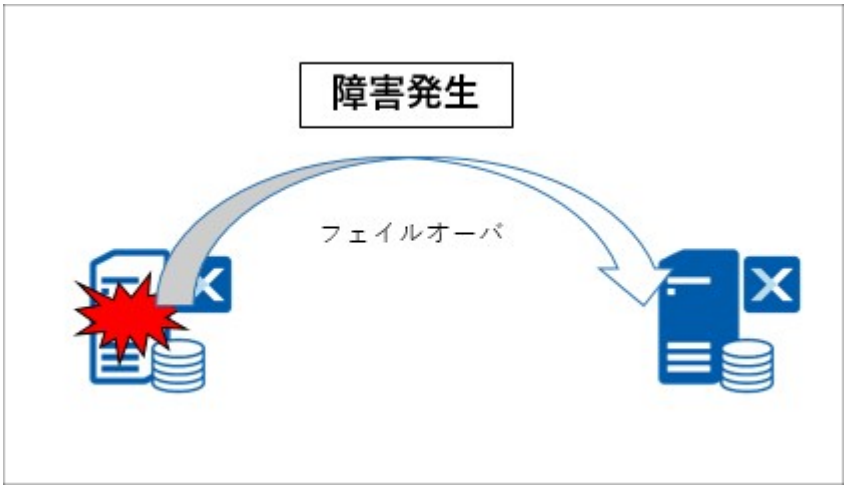

図2 システム構成（障害発生時）

CLUSTERPROでフローティングIPアドレスを設定する事で、クライアントやログソースからはフェイルオーバ完了後も同じアドレスでX/SIEMに接続できます。

第2章 設定手順

X/SIEMとCLUSTERPROの設定手順について説明します。

作業実施前に、Logstorage X/SIEM 及び CLUSTERPRO X のシステム要件及び注意事項をご確認下さい。また、必要に応じ上記製品のマニュアルをご参照下さい。

2.1. X/SIEMの冗長化

X/SIEMの冗長化として、サーバ2台を使用した片方向スタンバイ型での設定方法を説明します。

ディスク障害、サービスダウン、サーバ自体のダウンやストールを検出するとフェイルオーバし、待機系サーバがディスク内容を引き継いでサービスと共に起動します。また、フローティングIPの設定を行い、フェイルオーバ時にIPアドレスも引き継ぐようにします。

冗長化方式にはミラーディスク方式を使用しますが、共有ディスク方式でも可能です。

X/SIEM はオールインワン構成でのインストールを前提としています。インデクサークラスター構成の場合は必要に応じ各ノードをそれぞれ冗長化して下さい。

2.2. 設定構成例

以下の構成でCLUSTERPROとX/SIEMの設定を行います。

表2 設定構成例_サーバ設定情報

サーバ設定情報		
系列	現用系サーバ	待機系サーバ
サーバ名	server01	server02
IPアドレス	192.168.2.11	192.168.2.12
システムドライブ	C	
データパーティション	E	
クラスタパーティション	F	

表3 設定構成例_X/SIEM設定情報

X/SIEM設定情報	
インストール先	E:\xsiem
インデックス	E:\xsiem\cell\work\index\data [1]
バックアップ	E:\xsiem\cell\work\index\backup [1]
X-SIEMサービスの起動設定	手動

[1]簡易インストールの場合は表示されません。

表4 設定構成例_CLUSTERPRO設定情報

CLUSTERPRO設定情報	
フェイルオーバグループ	
起動可能サーバ	server01 server02
グループリソース	
ミラーディスクリソース	データパーティションのドライブ文字 **E:** クラスタパーティションのドライブ文字 **F:**

CLUSTERPRO設定情報	
サービスリソース	Logstorage-XSIEM Main
フローティングIPリソース	192.168.2.10

2.3. システム環境の設定

ミラーディスク方式でディスクを用意します。「CLUSTERPRO X インストール&設定ガイド」を参照し設定して下さい。

- データパーティション用ドライブ: **E**
- クラスタパーティション用ドライブ: **F**

X/SIEMは引継対象となるデータパーティション上にインストールします。データパーティションには十分な空き領域をご用意ください。

2.4. X/SIEMのインストールと設定

現用系/待機系の両方でX/SIEMをインストールします。事前に必要なOS設定や、インストール手順の詳細は「Logstorage X/SIEM 管理者マニュアル」を参照して下さい。

現用系サーバへのX/SIEMインストール

1. 現用系サーバでX/SIEMのインストーラを起動し、画面に従って進めます。インストール先はデータパーティション上を指定します。
   - インストール先: **E:\xsiem**

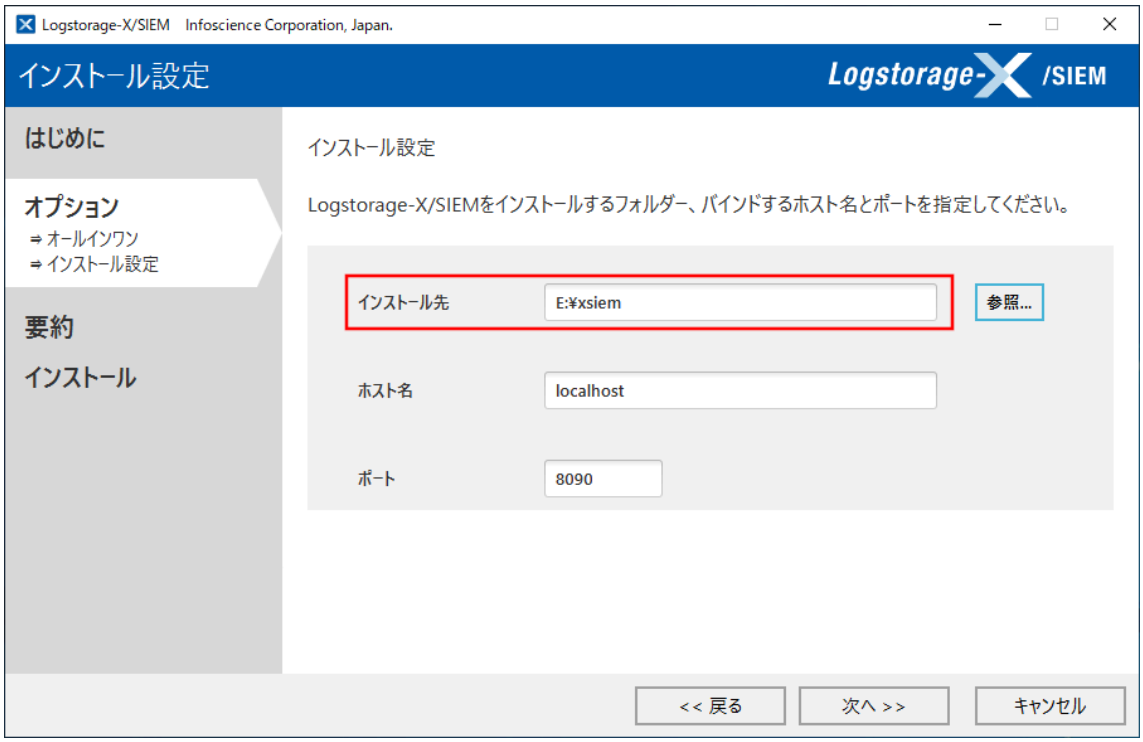

図3 インストール先の指定

2. インストール方法で詳細インストールを選択した場合、インデックスとバックアップの保存先を指定します。デフォルトでインストール先に指定したパス配下となっていますが、変更する場合もデータパーティション上に指定するようにして下さい。
   - インデックス: **E:\xsiem\cell\work\index\data**
   - バックアップ: **E:\xsiem\cell\work\index\backup**

図4 インデックス/バックアップ保存先の指定

簡易インストールの場合、設定画面は表示されません。保存先は自動でインストール先配下になります。

3. インストール完了後、X/SIEMサービスを手動起動に変更します。
   Windowsの管理ツールからサービスを開き、「Logstorage-XSIEM Main」をダブルクリックまたは右クリックからプロパティを表示します。
   スタートアップの種類を自動から手動に変更し、OKボタンをクリックして下さい。

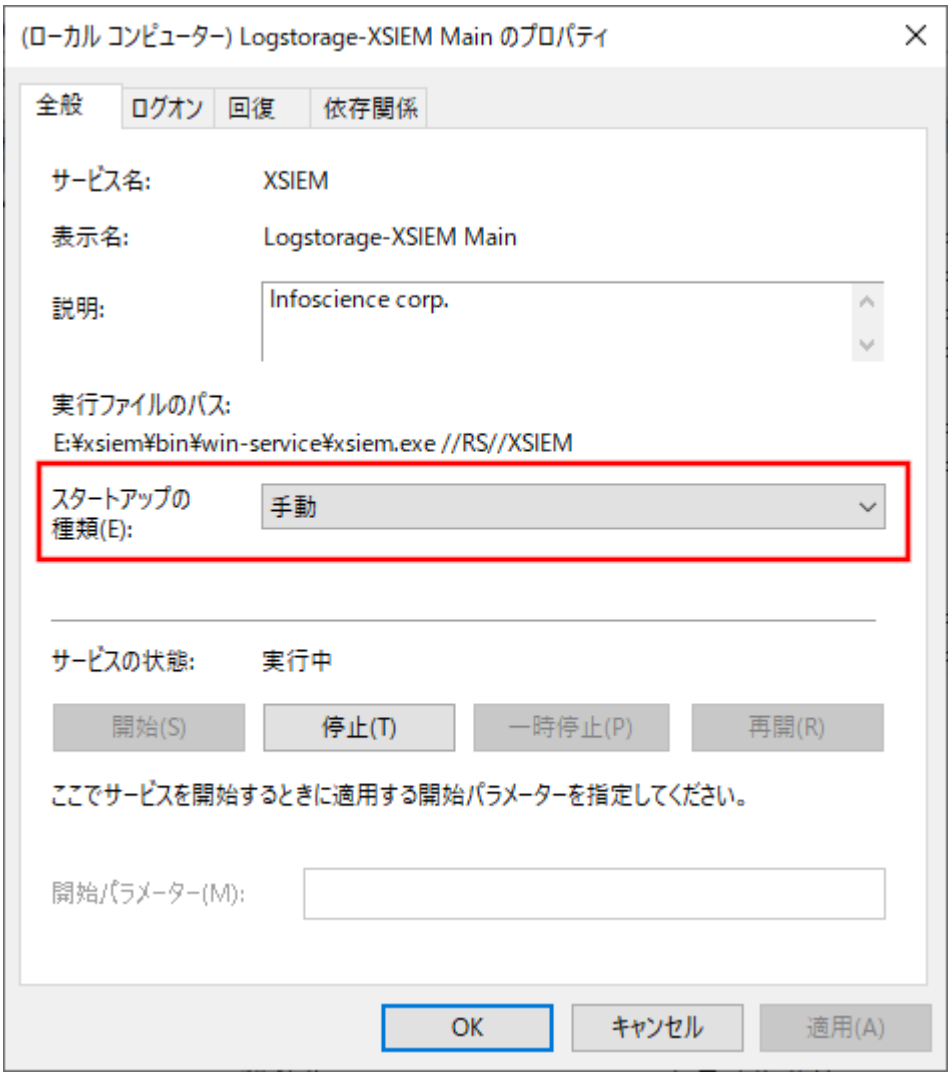

図5 サービス手動起動

4. サービス一覧で、Logstorage-XSIEM Mainのスタートアップの種類が手動になっている事を確認します。

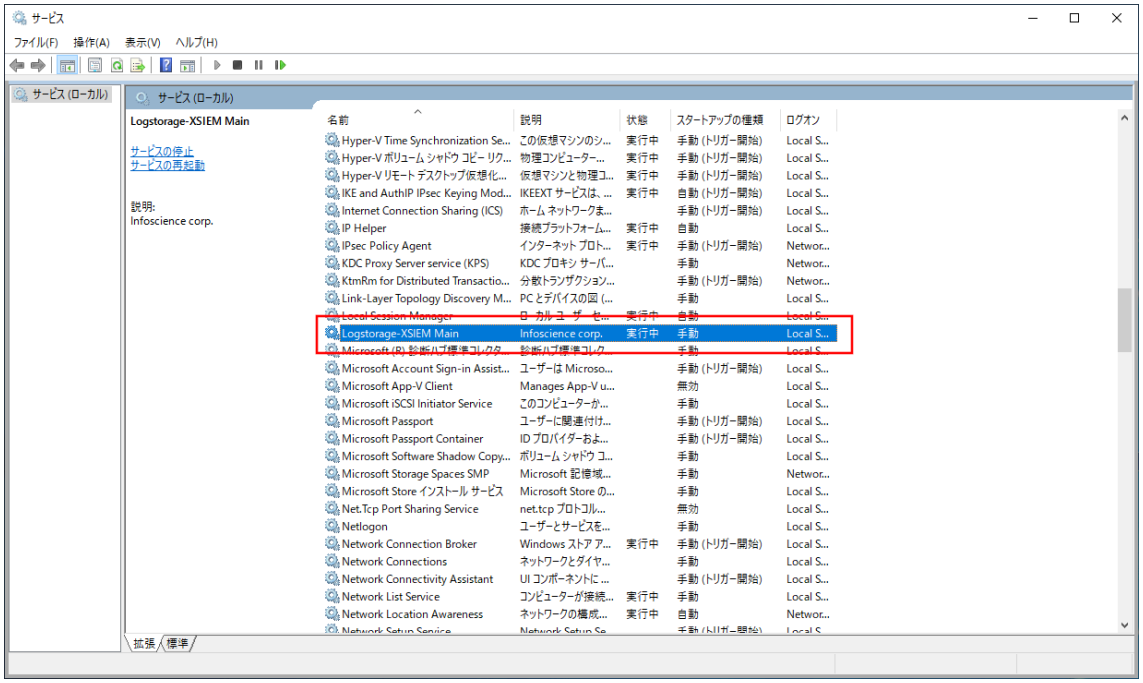

図6 スタートアップの種類

待機系サーバへのX/SIEMインストール

1. 待機系サーバも同じ手順でインストールし、サービス起動を手動に変更して下さい。
   インストール先は現用系サーバと同一のパスになるよう指定する必要があります。

2.5. CLUSTERPROのインストールと設定

「CLUSTERPRO X インストール&設定ガイド」を参照し、CLUSTERPROのインストールとライセンス登録を行って下さい。現用系/待機系ともに、インストール完了後は再起動して下さい。

以下、前述の構成例でのX/SIEM冗長構成に必要な部分を説明します。特に説明の無い部分はデフォルト値のままです。

変更の必要がある場合や、設定の詳細については「CLUSTERPRO X インストール&設定ガイド」を参照して下さい。

2.5.1. クラスタの作成

ブラウザで現用系のCluster WebUIを開きクラスタ生成ウィザードを開始します。

サーバの基本設定

1. サーバの定義一覧で、待機系サーバを追加するため追加ボタンをクリックします。

図7 サーバの基本設定1

2. 待機系サーバのアドレスを入力し、OKボタンをクリックします。
   - サーバ名またはIPアドレス: **192.168.2.12**

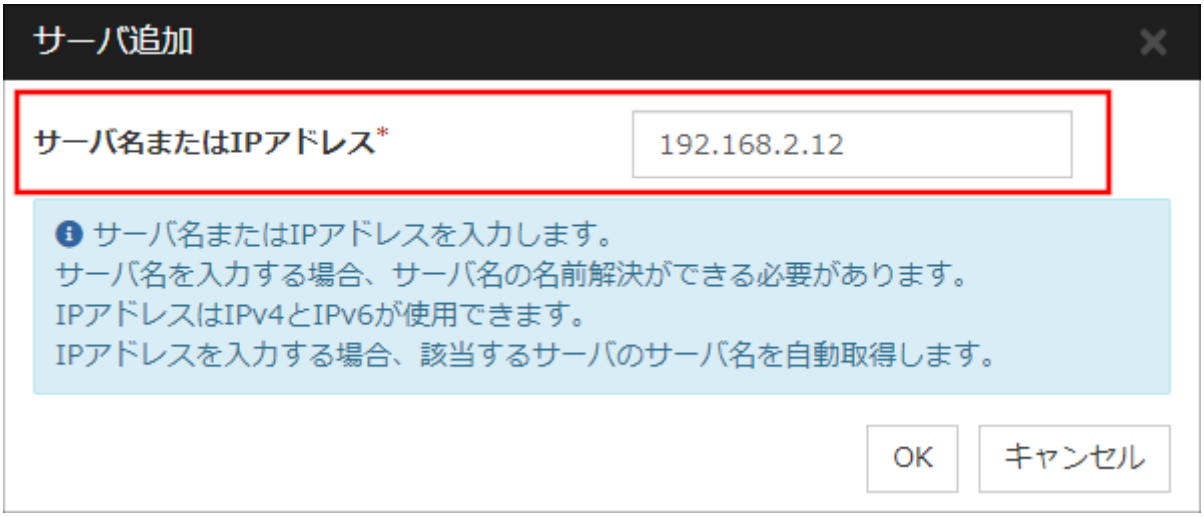

図8 サーバの基本設定2

3. サーバの定義一覧で待機系サーバの表示を確認します。

図9 サーバの基本設定3

インタコネクト

1. ミラーディスクを使用しますのでMDCを設定します。
   - MDC: **mdc1**

図10 インタコネクト

MDCの設定が無いと後述のミラーディスクリソースを設定できません。忘れずに設定して下さい。

2.5.2. フェイルオーバグループの作成

グループ一覧画面でフェイルオーバグループを追加し、グループリソースの設定を行います。 設定するグループリソースは次の3つです。

- ミラーディスクリソース
- サービスリソース
- フローティングIPリソース

フェイルオーバグループ

1. フェイルオーバグループを作成するためグループ一覧で追加ボタンをクリックします。

図11 グループ一覧

2. フェイルオーバが選択されている事を確認し、次へボタンをクリックします。
   - タイプ: **フェイルオーバ**

図12 グループの定義

ミラーディスクリソース

1. グループリソース一覧まで進み、追加ボタンをクリックします。

図13 グループリソース一覧1

2. グループリソースの定義でミラーディスクリソースを選択します。
   - タイプ: **ミラーディスクリソース**

図14 ミラーディスクリソース1

3. 詳細まで進み、起動可能サーバに現用系サーバを追加します。

図15 ミラーディスクリソース2

4. パーティションを選択し、OKボタンをクリックします。
   - データパーティション: **E:**
   - クラスタパーティション: **F:**

図16 ミラーディスクリソース3

5. 待機系サーバも同様に追加して下さい。
   - データパーティション: **E:**
   - クラスタパーティション: **F:**

図17 ミラーディスクリソース4

6. 待機系サーバを追加したら完了ボタンをクリックします。

図18 ミラーディスクリソース5

サービスリソース

1. グループリソース一覧で追加ボタンをクリックします。

図19 サービスリソース1

2. グループリソースの定義でサービスリソースを選択します。
   - タイプ: **サービスリソース**

図20 サービスリソース2

3. 詳細まで進みサービスを指定します。

   接続ボタンをクリックしてから「Logstorage-XSIEM Main」サービスを選択し完了をクリックします。

   - サービス名: **Logstorage-XSIEM Main**

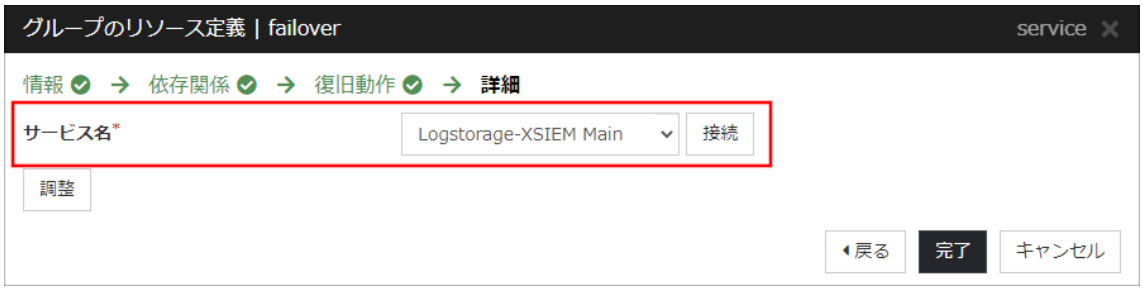

図21 サービスリソース3

フローティングIPリソース

1. グループリソース一覧で追加ボタンをクリックします。

図22 フローティングIPリソース1

2. グループリソースの定義でフローティングIPリソースを選択します。
   - タイプ: **フローティングIPリソース**

図23 フローティングIPリソース2

3. 詳細まで進んだらフローティングIPアドレスに割り当てるIPアドレスを指定し、完了ボタンをクリックします。
   - IPアドレス: **192.168.2.10**

図24 フローティングIPリソース3

モニタリソース

モニタリソース設定は自動的に追加されます。完了をクリックします。

図25 モニタリソース

2.5.3. クラスタの開始

Cluster WebUIで設定の反映を行い、完了したらクラスタを開始して下さい。

Cluster WebUIなどからクラスタを開始する事ができます。

2.6. 動作確認

フェイルオーバ動作の確認方法です。

1. Cluster WebUIのステータス画面からフェイルオーバグループが現用系サーバで起動しており、クラスタ状態が正常である事を確認します。

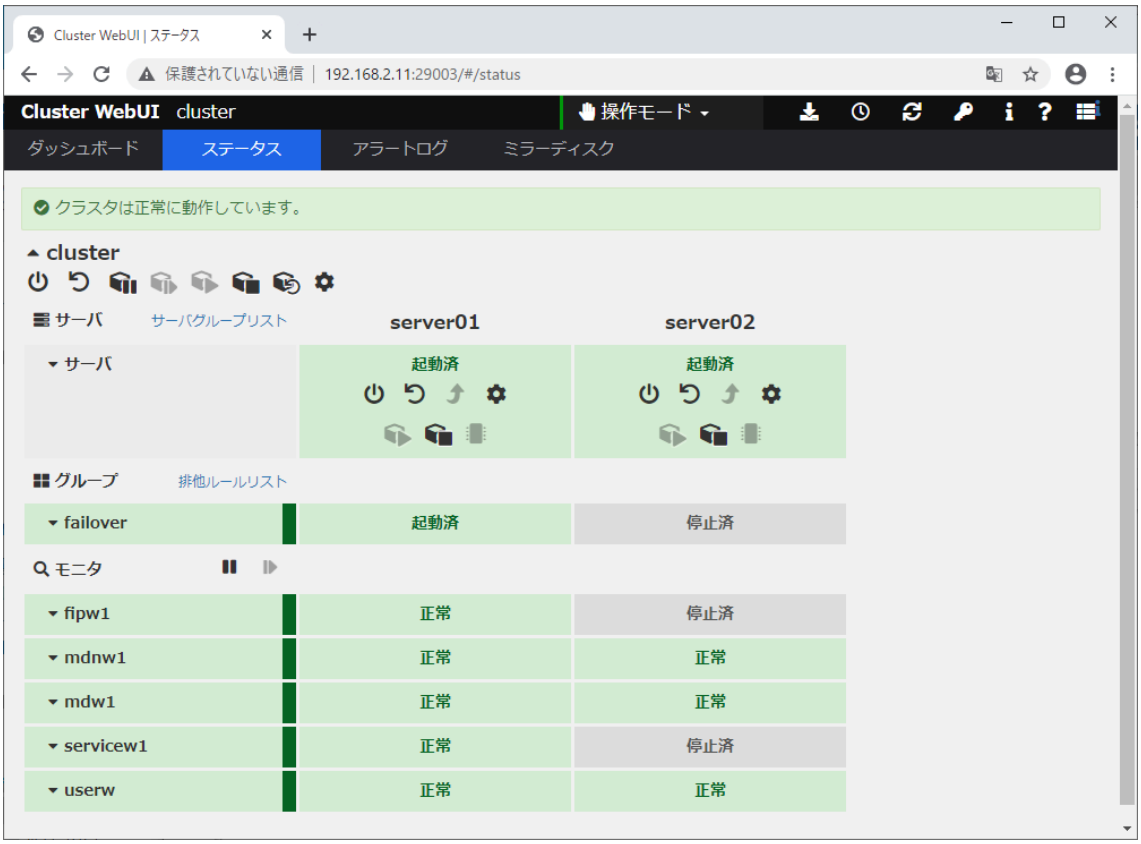

図26 クラスタ状態1

2. フローティングIPアドレスでブラウザからX/SIEM画面にアクセスできる事を確認します。

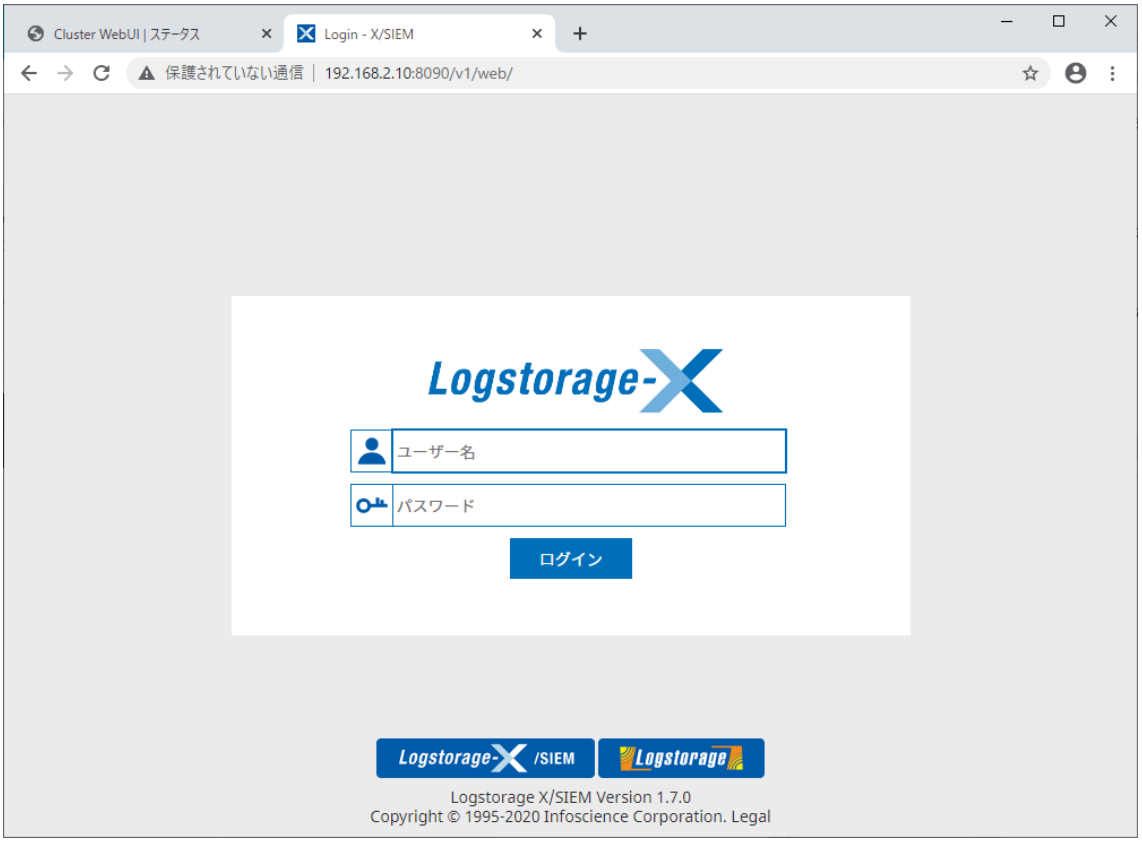

図27 X/SIEM画面

3. 現用系サーバをシャットダウンし、フェイルオーバを発生させます。

4. Cluster WebUIのステータス画面から、フェイルオーバグループが待機系サーバで正常に起動している事を確認します。

図28 クラスタ状態2

5. フローティングIPアドレスでブラウザからX/SIEM画面にアクセスできる事を確認します。

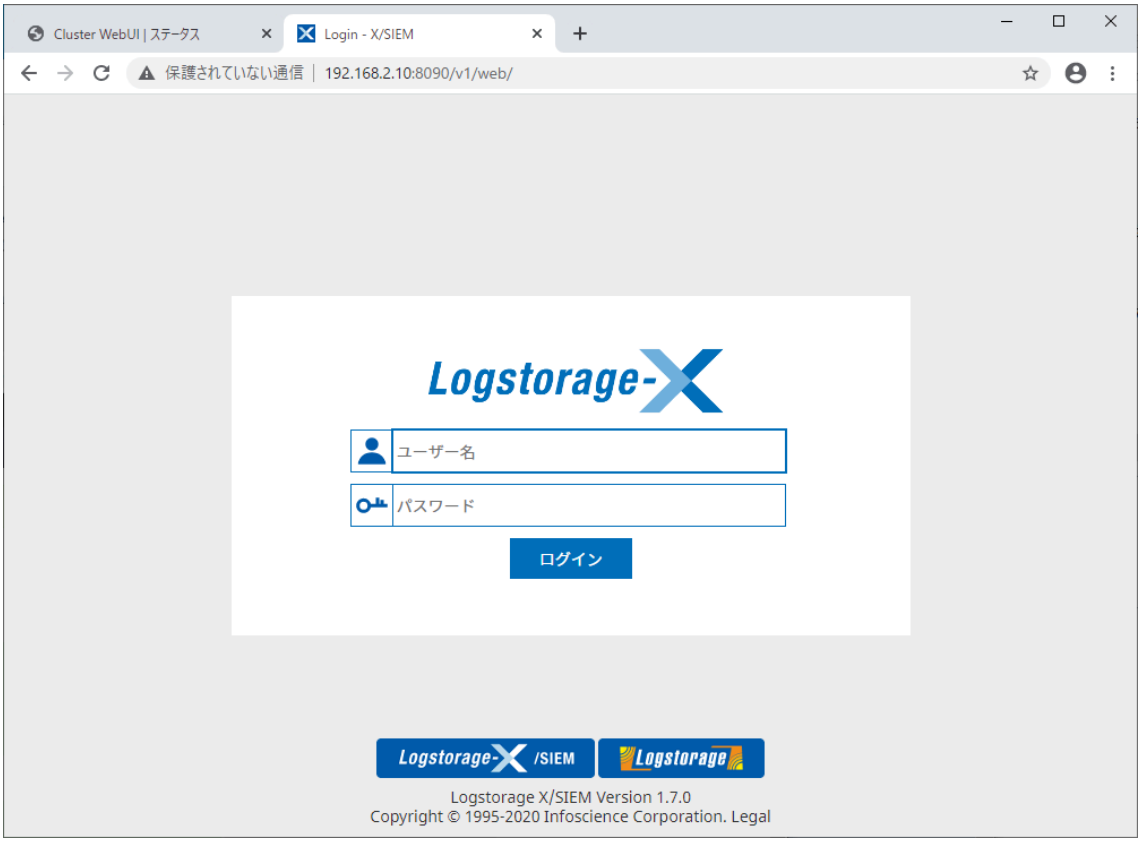

図29 X/SIEM画面

6. 現用系サーバを起動します。

7. Cluster WebUIでフェイルオーバグループを現用系にグループ移動します。

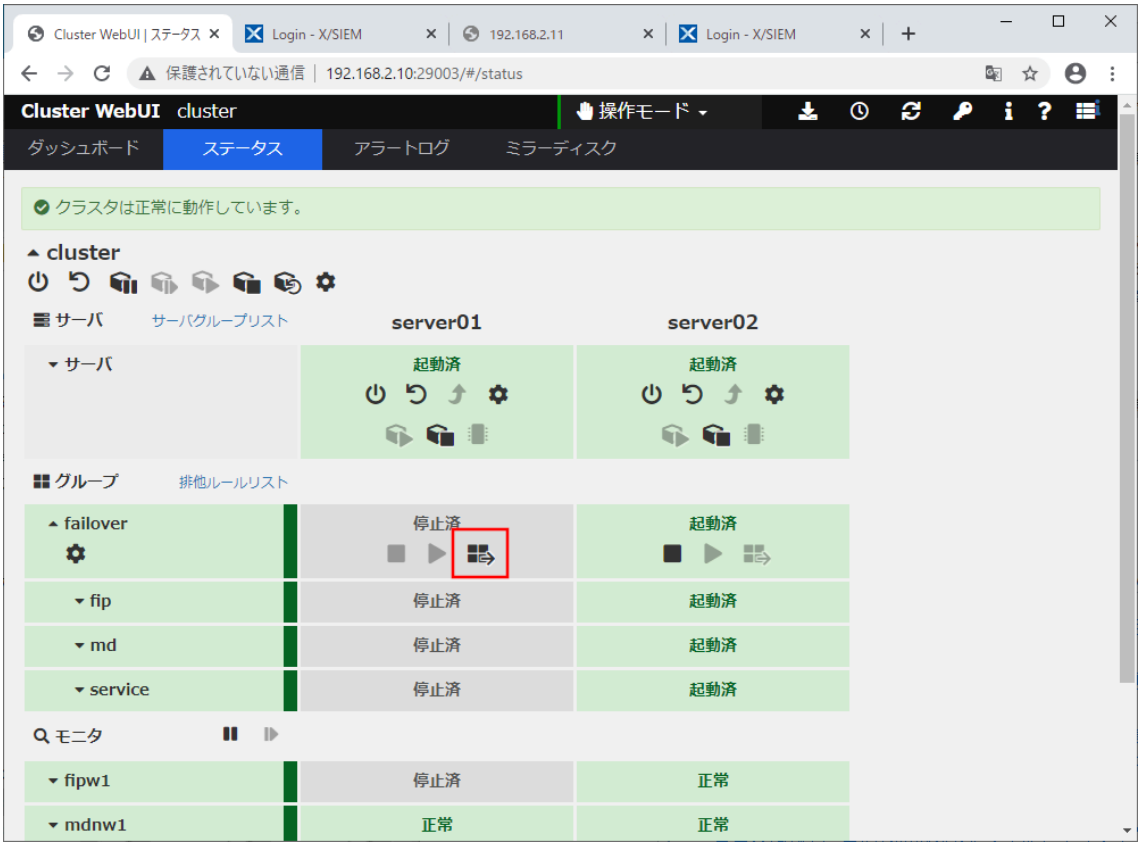

図30 クラスタ状態2

動作確認は以上です。

第3章 制限事項

以下の制限事項があります。ご注意下さい。

ログ受信

- ファイルレシーバでファイルの読込中にフェイルオーバが発生した場合、フェイルオーバ完了後に読込を再開します。この時、最大1000件重複の発生する可能性があります。
- LLTPレシーバの受信中にフェイルオーバが発生した場合、フェイルオーバ完了後に送信元からの送信が再開されます。
- Syslog(UDP)レシーバの受信中にフェイルオーバが発生した場合、フェイルオーバ完了までのログデータは失われます。
- Syslog(TCP)/Logstorageレシーバの受信中にフェイルオーバが発生した場合、フェイルオーバ完了までの間に再送制限に達したログデータは失われます。

引継ぎ内容

フェイルオーバではディスク内容を引き継ぐ事ができますが、メモリ内容は引き継がれません。

- 受信コマンド実行中のログは失われる可能性があります。
- フェイルオーバ時点で処理中のアラートは通知が行われない可能性があります。
- memjoinコマンドで読み込んだ外部データのキャッシュはクリアされ、次回コマンド実行時に読込が発生します。
- その他、メモリにキャッシュされたログなどのデータは引き継がれません。
- スパイクイベントやレアイベントの検出状態も初期化されます。

kv_setコマンドで作成するキーバリューテーブルは管理データベースに保存されるため引継ぎ対象になります。但し、受信コマンドやアラート内でkv_set, kv_deleteを呼び出している場合、その実行中にフェイルオーバが発生すると正しく反映されない可能性があります。

尚、ディスク障害などでデータに不整合が発生した場合はフェイルオーバに失敗する可能性があります。

付録A. 共有ディスク方式での設定

ここでは、共有ディスク方式で冗長化する場合の設定を説明します。

A.1. 共有ディスク方式での設定構成例

表5 共有ディスク方式での設定構成例_サーバ設定情報

サーバ設定情報		
系列	現用系サーバ	待機系サーバ
サーバ名	server01	server02
IPアドレス	192.168.2.11	192.168.2.12
システムドライブ	C	
ディスクリソース用切替パーティション	E	
ディスクハートビート用パーティション	F	

表6 共有ディスク方式での設定構成例_X/SIEM設定情報

X/SIEM設定情報	
インストール先	E:\xsiem [1]
X-SIEMサービスの起動設定	手動

[1]インデックス、バックアップ保存先も同パーティション上に指定する必要があります。

表7 共有ディスク方式での設定構成例_CLUSTERPRO設定情報

CLUSTERPRO設定情報	
フェイルオーバグループ	
起動可能サーバ	server01 server02
グループリソース	
ディスクリソース	ドライブ文字 **E:**

CLUSTERPRO設定情報	
サービスリソース	Logstorage-XSIEM Main
フローティングIPリソース	192.168.2.10

A.2. 共有ディスク方式での設定手順

ミラーディスク方式との違いのみ説明します。記載の無い部分は本文または各製品のマニュアルをご参照ください。

A.2.1. システム環境の設定

共有ディスク方式でディスクを用意します。「CLUSTERPRO X インストール&設定ガイド」を参照し設定して下さい。

- ディスクリソース用切替パーティションのドライブ: **E**
- ディスクハートビート用パーティションのドライブ: **F**

A.2.2. X/SIEMのインストール

1. 現用系サーバでX/SIEMを共有ディスク上にインストールします。
   - インストール先: **E:\xsiem**
2. インストールが完了したら、サービス起動を手動に設定し現用系サーバをシャットダウンします。
3. 待機系サーバを起動し、共有ディスク上のX/SIEMモジュールを全て削除します。
   - E:\xsiem ディレクトリを削除
4. 待機系サーバも同じ手順で X/SIEM をインストールします。
   - インストール先: **E:\xsiem**
5. インストールが完了し、サービス起動を手動に設定して下さい。

A.2.3. CLUSTERPRO のインストールと設定

「CLUSTERPRO X インストール&設定ガイド」を参照し、CLUSTERPROのインストールとライセンス登録を行って下さい。

インストール時のフィルタリング設定では共有ディスクを指定して下さい

A.2.3.1. クラスタの作成

インタコネクト

1. ミラーディスク方式と違い、MDCは設定しません。

図31 共有ディスク方式_インタコネクト

NP解決

1. DISK方式のNP解決機能を設定します。
   - 種別: **DISK**
   - server01: **F:**
   - server02: **F:**

図32 共有ディスク方式_NP解決

A.2.3.2. フェイルオーバグループの設定

フェイルオーバグループで使用するグループリソースは次の3つです。

- ディスクリソース
- サービスリソース
- フローティングIPリソース

サービスリソース、フローティングIPリソースの設定方法はミラーディスク方式の場合と同様のため省略します。

ディスクリソース

1. グループリソース一覧で追加ボタンをクリックします。

図33 ディスクリソース1

2. グループリソースの定義でディスクリソースを選択します。

図34 ディスクリソース2

3. 詳細まで進み、起動可能サーバに現用系サーバを追加します。

図35 ディスクリソース3

4. ディスクリソース用切替パーティションを選択し、OKボタンをクリックします。
   - パーティション: **E:**

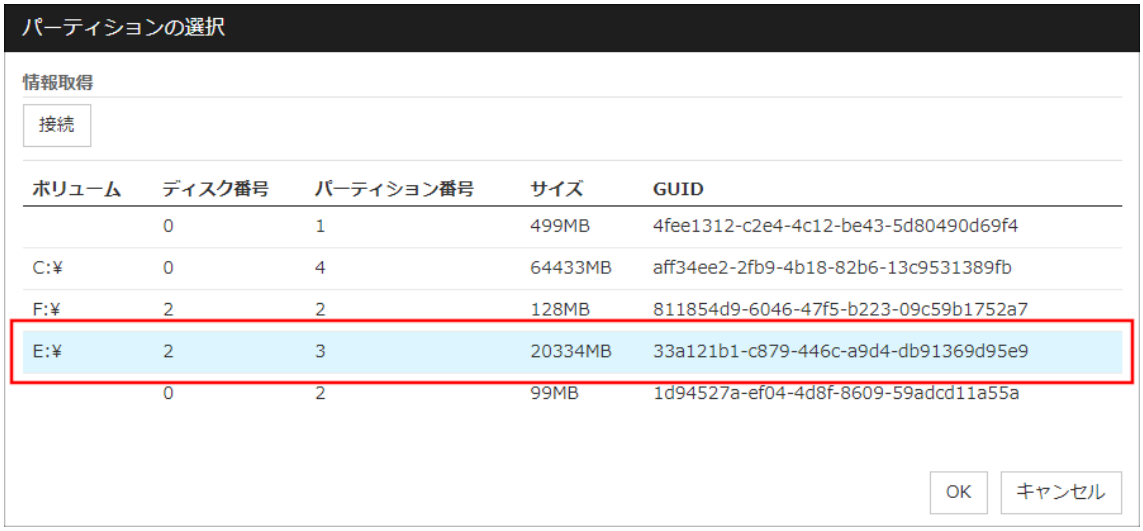

図36 ディスクリソース4

5. 待機系サーバも同様に追加し、完了をクリックします。
   - パーティション: **E:**

図37 ディスクリソース5

以降はミラーディスク方式と同様に設定・動作確認を行って下さい。

付録B. Linux版でのCLUSTERPRO設定

ここでは、Linuxでのクラスタ構築におけるフェイルオーバグループ設定の違いについて説明します。

CLUSTERPROのLinux版ではWindows版でのサービスリソースに相当するものが無く、代わりにEXECリソースを使用します。システム環境、インストール、EXECリソース以外のリソース設定についてはWindows版と同様です。本資料の該当箇所や製品マニュアルを参照して下さい。

B.1. Linux版での設定手順

ここではEXECリソースを使用するための手順を説明します。

設定の流れは次の通りです。

- ファイルディスクリプタ設定
- X/SIEM起動/停止スクリプトの準備
- EXECリソースの追加
- プロセス名モニタリソースの追加

X/SIEMは下記の通り設定されているものとします。

表8 Linux版での設定構成例_X/SIEM設定情報

X/SIEM設定情報	
インストール先	/mnt/disk1/xsiem
自動起動設定	設定しない [1]

[1]CLUSTERPRO制御以外でのサーバシャットダウンの際は後述のスクリプトなどでX/SIEMを停止させてからシャットダウンするようにして下さい。

B.2. X/SIEMの設定

ファイルディスクリプタ設定

X/SIEMは通常systemdによるプロセスの起動/停止を行いますが、EXECリソースを使用する際は起動スクリプトを使用します。 そのため現用系／待機系サーバの両方でファイルディスクリプタの設定を行う必要があります。設定方法は「Logstorage X/SIEM 管理者マニュアル」を参照して下さい。

X/SIEMの起動/停止スクリプトの準備

CLUSTERPROのLinux版では、X/SIEMの起動をスクリプトから行います。ここでは例として次のスクリプトを作成し使用します。

起動スクリプト例(start.sh)

```
#!/bin/bash
sudo -u xsiem /mnt/disk1/xsiem/bin/xsiem.sh start
```

停止スクリプト例(stop.sh)

```
#!/bin/bash
sudo -u xsiem /mnt/disk1/xsiem/bin/xsiem.sh stop
```

起動/停止スクリプトはX/SIEMインストールパス直下のbinディレクトリに配置して下さい。

- 起動スクリプト配置パス例: **/mnt/disk1/xsiem/bin/start.sh**
- 停止スクリプト配置パス例: **/mnt/disk1/xsiem/bin/stop.sh**

B.3. CLUSTERPROの設定

EXECリソース

1. グループリソース一覧で追加ボタンをクリックし、リソース定義画面でEXECリソースを選択します。
   - タイプ: **EXECリソース**

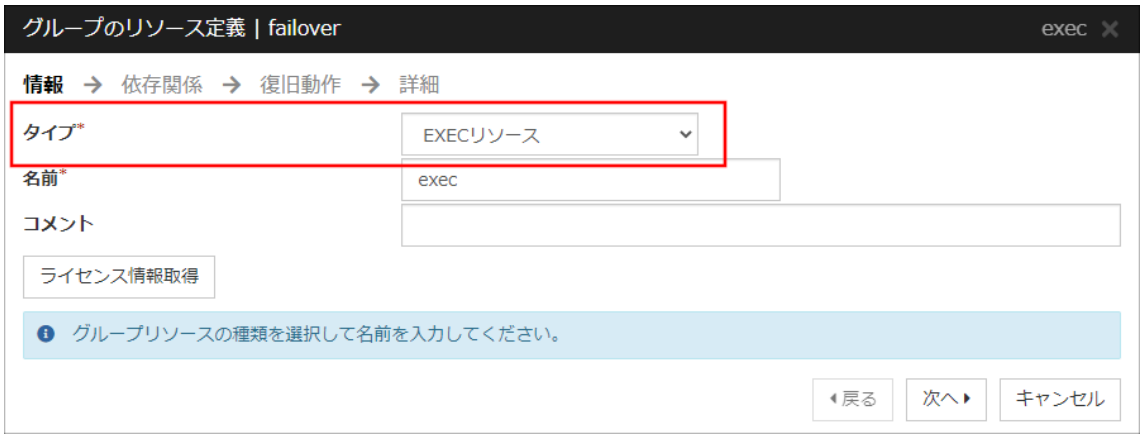

図38 EXECリソース1

2. 詳細まで進み、ユーザアプリケーションを選択、編集ボタンをクリックします。
   - 詳細: **ユーザアプリケーション**

図39 EXECリソース2

3. アプリケーションパスの入力では、用意した起動/停止スクリプトを指定します。
   - 開始: **/mnt/disk1/xsiem/bin/start.sh**
   - 終了: **/mnt/disk1/xsiem/bin/stop.sh**

図40 EXECリソース3

4. スクリプト一覧を確認し、完了ボタンをクリックします。

図41 EXECリソース4

プロセス名モニタリソース

1. モニタリソース一覧で追加ボタンをクリックします。

図42 プロセス名モニタリソース1

2. モニタリソースのタイプにプロセス名モニタを指定します。

図43 プロセス名モニタリソース2

3. 監視(共通)ではタイムアウト/待ち時間と、監視対象はX/SIEM用に設定したEXECリソースを指定します。
   - タイムアウト: **60秒**
   - 監視開始待ち時間: **120秒**
   - 監視タイミング: **活性時**
   - 対象リソース: **exec**

図44 プロセス名モニタリソース3

4. 監視(固有)ではX/SIEMプロセス名とプロセス数の下限値を指定します。
   - プロセス名: **/mnt/disk/xsiem/java/j2sdk-image/bin/java***
   - 下限: **2**

図45 プロセス名モニタリソース4

5. 回復動作と回復対象を指定し完了ボタンをクリックします。
   - 回復動作: **回復対象を再起動、効果がなければフェイルオーバ実行**
   - 回復対象: **exec**

図46 プロセス名モニタリソース5

他の部分はWindows版の手順と同様に設定・動作確認を行って下さい。

モニタリソース設定の監視開始時間やタイムアウト値は環境によっては長めに設定する必要があります。

開発元

インフォサイエンス株式会社
〒108-0023
東京都港区芝浦 2-4-1
Tel: 03-5427-3503 Fax: 03-5427-3889
info@logstorage.com
https://www.infoscience.co.jp
Infoscience Corporation 2-4-1, Shibaura Minato-ku, Tokyo 108-0023 Japan