FUJITSU

Fujitsu Software Systemwalker as a Service

ユーザーズガイド

SWaaS-UG-01
2025年9月

はじめに

本書の目的

本書では、Systemwalker as a Serviceの利用方法について説明します。

本書の読者

本書は、Systemwalker as a Serviceのサービス利用者（Systemwalker as a Serviceを利用するお客様、またはSE）を対象としています。

本書を読むにあたって、ご利用の環境に応じた以下の知識が必要です。

- Linuxに関する基本的な知識
- Windowsに関する基本的な知識
- Amazon Web Servicesに関する基本的な知識
- Microsoft Azureに関する基本的な知識
- Fujitsu Software Systemwalker Centric Managerに関する基本的な知識
- Fujitsu Software Systemwalker Operation Managerに関する基本的な知識
- Fujitsu Software PRIMECLUSTERに関する基本的な知識

本書の構成

本書は、以下の構成で説明します。

第1章は、Systemwalker as a Serviceを利用するための方法について、概要を説明します。

第2章は、Systemwalker as a Serviceを利用開始するための必要な準備について説明します。

第3章は、Systemwalker as a Serviceで利用するユーザーを管理（追加、変更、削除）する手順について説明します。

第4章は、業務環境のシステム構成を変更した際の手順について説明します。

第5章は、Systemwalker as a Serviceの運用変更、統合管理機能、およびジョブ管理機能の運用を変更する際の手順について説明します。

第6章は、サービス利用者がSystemwalker as a Serviceの運用作業をする手順について説明します。

第7章は、サービス利用者がSystemwalker as a ServiceでDisaster Recoveryを利用する手順について説明します。

本書の表記について

本書では、以下の表記を使用します。

略称について

正式名称	略称
Amazon Web Services	AWS
Microsoft Azure	Azure

記号について

記号	意味
[]	画面やダイアログボックスに表示される文字およびキーボードのキーを示します。

記号	意味
	例) [設定]ダイアログボックス、[ファイル]メニュー、[項目名]、[OK]ボタン、[Enter]キー

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。

登録商標について

Amazon Web Services、その他のAWS商標は、米国その他の諸国における、Amazon.com, Inc.またはその関連会社の商標です。

Google Chromeは、Google LLCの商標または登録商標です。

Linux(R)は、米国およびその他の国におけるLinus Torvaldsの登録商標です。

Microsoft、Windows、Windows Server、Azureまたはその他のマイクロソフト製品の名称および製品名は、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。

Red Hatは、米国およびその他の国におけるRed Hat, Inc.およびその子会社の商標または登録商標です。

そのほか、本書に記載されている会社名および製品名は、それぞれ各社の商標または登録商標です。

なお、本書に記載されている会社名、システム名、製品名等には必ずしも商標表示 (TM・(R)) を付記しておりません。

改版履歴

版数	年月	変更内容
第1.0版	2025年9月	初版

著作権表示

Copyright 2025 Fujitsu Limited

目　次

第1章 Systemwalker as a Serviceの利用概要 1
1.1 各種申請書とは 1
1.2 サービスで利用するユーザーとは 4

第2章 Systemwalker as a Serviceの利用を開始する 6
2.1 サービス利用の事前準備をする 6
2.1.1 サービスの利用環境を設計する 6
2.1.2 サービス接続用仮想ネットワークを設計・構築する 7
2.1.3 仮想ネットワークピアリング設定用アカウントを設計・作成する 8
2.1.4 運用ポータルの契約者アカウントを作成する 9
2.2 サービスの利用開始申請をする 9
2.2.1 構築申請をサービス窓口へ送信する 9
2.2.2 仮想ネットワークピアリング設定用アカウントの設定を実施する 9
2.2.3 利用開始通知を受信する 10
2.3 業務環境を準備する 10
2.3.1 サービスに接続する 10
2.3.2 Systemwalkerエージェント環境を準備する 11
2.3.3 Systemwalkerクライアント環境を準備する 11
2.3.4 運用ポータルに接続する環境を準備する 11
2.3.5 ファイルサーバーに接続する環境を準備する 12
2.3.6 統合管理機能のWeb APIを発行する環境を準備する 12
2.4 サービスの利用を開始する 12
2.4.1 運用ポータルにログインする 12
2.4.2 統合管理機能にログインする 14
2.4.3 ジョブ管理機能にログインする 14
2.4.4 ファイルサーバーにログインする 15

第3章 Systemwalker as a Serviceで利用するユーザーを管理する 16
3.1 運用ポータルのユーザーを管理する 16
3.2 統合管理機能のユーザーを管理する 18
3.3 ジョブ管理機能のユーザーを管理する 18
3.4 ファイルサーバーのユーザーを管理する 18

第4章 システム構成を管理する 19
4.1 Systemwalkerエージェントの構成を管理する 19
4.1.1 Systemwalkerエージェントを追加する 19
4.1.2 Systemwalkerエージェントを変更する 20
4.1.3 Systemwalkerエージェントを削除する 20
4.2 全体監視サーバにノード情報を登録する 21
4.3 Systemwalkerクライアントの構成を管理する 21
4.4 業務環境の運用管理サーバ・部門管理サーバを追加する 22
4.4.1 業務環境の運用管理サーバを追加する 22
4.4.2 業務環境の部門管理サーバを追加する 23

第5章 Systemwalker as a Serviceの運用を変更する 25
5.1 Systemwalkerマネージャーのログ収集設定を変更する 25
5.2 Systemwalkerエージェントのログ収集設定を変更する 25
5.3 定常バックアップのタイミングを変更する 26
5.4 統合管理機能の運用を変更する 27
5.4.1 イベント監視[監視条件]の監視ポリシーを登録する 27
5.4.2 アプリケーション情報を登録する 27
5.5 ジョブ管理機能の運用を変更する 28
5.5.1 マスタスケジュール管理を変更する 28
5.5.2 ジョブネットを設定する 29
5.5.3 ローカルジョブ用スクリプトを管理する 30

第6章 運用作業を実施する 31
6.1 Systemwalkerマネージャーのログを確認する 31
6.2 Systemwalkerエージェントのログを確認する 31
6.3 任意タイミングでログを取得する 31
6.4 任意タイミングでSystemwalkerマネージャーのバックアップをする 32
6.5 フェイルオーバーを実施する 33
6.6 統合管理機能のWeb APIを発行する 34

第7章 Disaster RecoveryによりSystemwalker as a Serviceを切り替える 36
7.1 Disaster Recoveryの事前準備をする 36
7.2 Disaster Recoveryを実施する 37
7.2.1 サービスから切り替え開始通知を受領する 37
7.2.2 サービスから切り替え完了通知を受領する 37
7.2.3 サービスに接続する 38
7.2.4 運用再開準備をする 38

付録A ファイルサーバーユーザー用のキーペアの発行方法 39

付録B ファイルサーバーへのログイン方法 40

付録C ファイルサーバーでのファイル配置方法 41

付録D ファイルサーバーでのログ参照方法 42

付録E 仮想ネットワークピアリングの設定方法 43

付録F APIリファレンス 44
F.1 change-event-stat 44

付録G AWS上の業務環境接続例 48

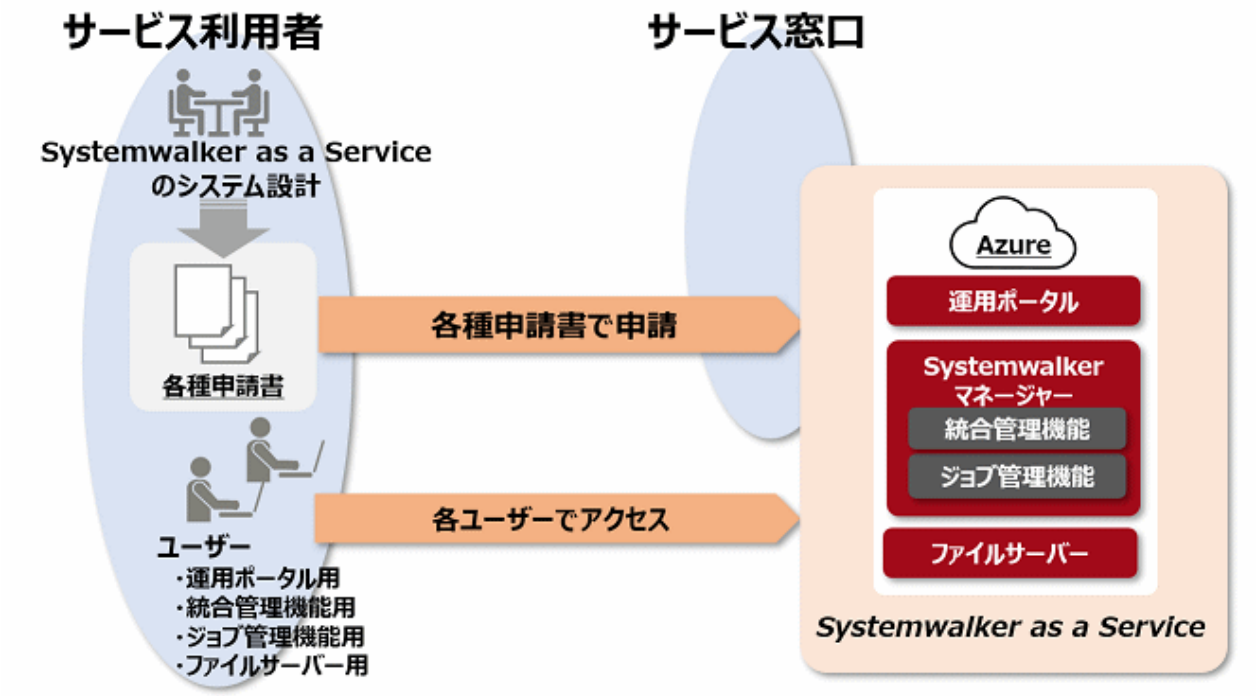
第1章　Systemwalker as a Serviceの利用概要

本章では、Systemwalker as a Serviceの利用開始までの流れと、利用開始後の運用の概要について説明します。

Systemwalker as a Serviceの利用は、以下の流れで進めます。

1. サービス利用者は、業務環境の規模や運用設定情報に基づいて、Systemwalker as a Serviceの構成を設計します。
2. 設計した内容に基づいて、サービス窓口へSystemwalker as a Service環境の構築を申請します。
3. 申請された設計内容に基づいて、Systemwalker as a Serviceのサービス環境が構築されます。
4. 環境構築後、以下の機能を利用して運用を開始できます。
   - Systemwalkerマネージャー
   - 運用ポータル
   - ファイルサーバーのユーザー機能

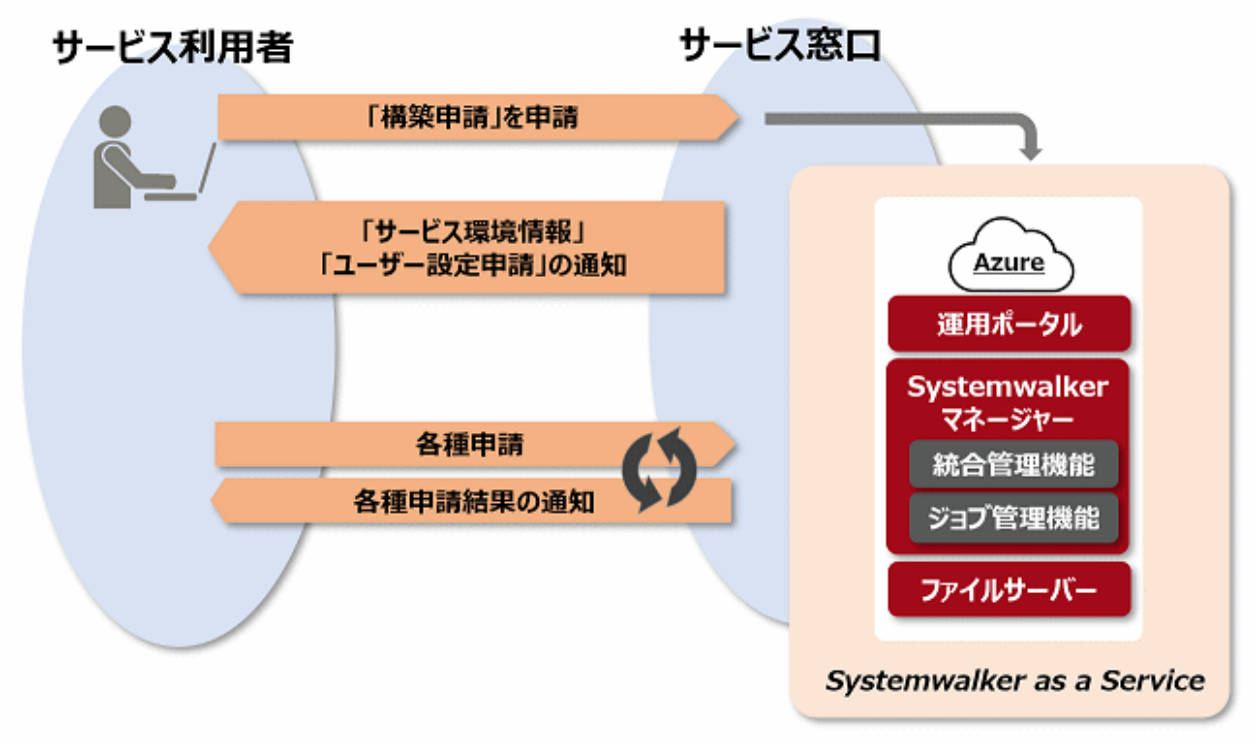
運用中に設定や構成の変更が必要になった場合、所定の申請書を提出することで対応できます。



1.1　各種申請書とは

サービス環境の構築時や運用時の各場面においては、必要に応じて各種申請書を利用してください。

申請書は、契約時にお渡しします。



サービス環境を構築する

Systemwalker as a Serviceを利用するには、以下の手順でサービス環境を構築します。

1. 構築申請の提出

   サービス利用者は、「構築申請」に必要な情報を記載し、サービス窓口へ提出します。

2. 環境の構築

   提出された申請内容に基づき、Microsoft Azure上にSystemwalker as a Serviceの環境が構築されます。

3. サービス開始の通知

   環境構築が完了すると、サービス窓口からサービス利用者に以下の情報が通知されます。

情報名	概要
サービス環境情報	Systemwalkerマネージャーおよび運用ポータルに接続するためのIPアドレス、ホスト名などの情報が記載
ユーザー設定申請	統合管理機能およびジョブ管理機能に関する初期ユーザー情報が記載

ポイント

利用前の確認事項

サービスを利用開始する前に、「サービス環境情報」と「ユーザー設定申請」の内容を必ず確認してください。
これらを事前に確認することで、接続設定やユーザー権限の確認作業を円滑に進めることができます。

申請書名	概要
構築申請	Systemwalker as a Serviceに、Systemwalkerマネージャーと運用ポータルを構築するために必要な情報を記載した申請書です。 Disaster Recoveryを利用する場合は、西日本リージョンの情報についても記載してください。

ユーザー情報の変更を依頼する

ユーザー情報を変更する場合は、以下の申請書に必要事項を記載し、サービス窓口へ提出します。

申請は、実施希望日時の5営業日前までに提出してください。

申請書名	概要
ユーザー設定申請	以下に接続するためのユーザー情報を変更する申請書です。 ・ 統合管理機能（Systemwalker Centric Manager） ・ ジョブ管理機能（Systemwalker Operation Manager） ・ ファイルサーバー

業務環境の変更を依頼する

業務環境を変更する場合は、該当する申請書に必要事項を記載し、サービス窓口へ提出します。

申請は、実施希望日時の5営業日前までに提出してください。

申請書名	概要
エージェント申請	Systemwalkerエージェントを追加、削除、または変更した場合に、Systemwalkerマネージャーのhostsファイルにその内容を反映するための申請書です。 また、業務環境において、部門管理サーバや業務環境のマネージャー経由でSystemwalkerエージェントを新たに接続する場合にも、本申請書を使用します。
クライアント申請	Systemwalkerクライアントを追加、削除、または変更した場合に、Systemwalkerマネージャーのhostsファイルにその内容を反映するための申請書です。
全体監視サーバへのノード情報登録申請	全体監視サーバに運用管理サーバのノード情報を登録するための申請書です。

サービス利用開始後の運用変更を依頼する

サービス利用開始後に運用設定を変更する場合は、該当する申請書に必要事項を記載し、サービス窓口へ提出します。

申請は、実施希望日時の5営業日前までに提出してください。

申請書名	概要
マネージャーログ定期収集設定申請	Systemwalkerマネージャーのログの定期収集設定を依頼するための申請書です。
エージェントログ収集設定申請	Systemwalkerエージェントのログの収集設定を依頼するための申請書です。
定常バックアップ設定申請	定常バックアップの設定を依頼するための申請書です。
イベント監視[監視条件]の監視ポリシー登録申請	Systemwalkerコンソールの「イベント監視[監視条件]」に監視ポリシーを登録依頼するための申請書です。
CSVファイルからのアプリケーション情報移入申請	アプリケーション情報を運用管理サーバへの登録を依頼するための申請書です。

サービス利用開始後に運用作業を依頼する

Systemwalker as a Serviceの運用操作を依頼する場合は、該当する申請書に必要事項を記載し、サービス窓口へ提出します。

申請は、実施希望日の5営業日前までに申請してください。

申請書名	概要
任意バックアップ申請	任意のタイミングにおけるバックアップを依頼するための申請書です。
任意タイミングでのログ収集申請	「マネージャーログ定期収集設定申請」にて設定した定期以外のタイミングでSystemwalkerマネージャーのログ、Systemwalkerエージェントのログを収集するための申請書です。
フェイルオーバー申請	Systemwalkerマネージャーをフェイルオーバー、フェイルバックをするための申請書です。 対象のSystemwalkerマネージャーが冗長構成のサービスプランの場合のみ申請可能です。

Disaster Recoveryに関する事前申請を依頼する

Systemwalker as a ServiceでDisaster Recoveryを利用する場合、該当する申請書に必要事項を記載し、サービス窓口へ提出します。

申請書名	概要
定常バックアップ設定申請	「サービス利用開始以降の運用変更を依頼する」内の定常バックアップ設定申請と同様の申請です。 本申請と任意バックアップ申請により、取得されたバックアップデータのうち最新のデータがDisaster Recovery時にリストアされます。
任意バックアップ申請	「サービス利用開始以降に運用作業を依頼する」内の任意バックアップ申請と同様の申請です。 本申請と定常バックアップ申請により、取得されたバックアップデータのうち最新のデータがDisaster Recovery時にリストアされます。

1.2　サービスで利用するユーザーとは

Systemwalker as a Serviceのサービスで利用されるユーザーは、以下の4種類に分類されます。

- 運用ポータルのユーザー
- 統合管理機能のユーザー
- ジョブ管理機能のユーザー
- ファイルサーバーのユーザー

運用ポータルのユーザー

運用ポータルにログインするためのユーザーです。

サービス利用者が、管理ポータルを通じて作成します。

ユーザーは、管理ポータルで管理される以下の3種類に分類されます。

- メンバー管理者（契約者）

  ユーザーグループを作成し、メンバー管理者とメンバーに紐づけることができるユーザーです。

・ メンバー管理者

メンバー管理者（契約者）の代行として、既存のユーザーグループとメンバーを紐づけることができるユーザーです。

・ メンバー

管理者権限を持たないユーザーです。

統合管理機能のユーザー

統合管理機能を利用するためのユーザーです。

ユーザーは、以下の2種類に分類されます。

・ Systemwalker管理者アカウント

サービス提供元が作成します。

各サーバ種別において、以下のロールが付与されています。

	サーバ種別		
	全体監視サーバ	運用管理サーバ	部門管理サーバ
Systemwalker管理者アカウント	DmAdmin	DmAdmin DistributionAdmin	DmAdmin DistributionAdmin

・ 利用者アカウント

サービス利用者が「ユーザー設定申請」によって作成します。

利用者アカウントへのロール付与は、Systemwalkerコンソールを使用し、サービス利用者自身で操作を行ってください。

ジョブ管理機能のユーザー

ジョブ管理機能を利用するためのユーザーで、拡張ユーザー管理機能を使用します。

ユーザーは、以下の2種類に分類されます。

・ OSユーザー（システム管理者）と対応付けた拡張ユーザー（管理者アカウント）

初期ユーザーとして、1ユーザーのみサービス提供元が作成します。

初期ユーザー以外は、サービス利用者が「ユーザー設定申請」によって作成します。

・ OSユーザー（一般ユーザー）と対応付けた拡張ユーザー

サービス利用者が「ユーザー設定申請」によって作成します。

ファイルサーバーのユーザー

ファイルサーバーを利用するためのユーザーです。

サービス利用者が「ユーザー設定申請」によって作成します。以下の用途で利用します。

・ Systemwalker Operation Managerのローカルジョブ用スクリプトの管理

ユーザーは、スケジュールサーバについてのスクリプトを管理できます。

・「マネージャーログ定期収集設定申請」または「任意タイミングでのログ収集申請」による収集されたログの参照

ユーザーは、SystemwalkerマネージャーおよびSystemwalkerエージェントについてのログを参照できます。

第2章 Systemwalker as a Serviceの利用を開始する

本章では、Systemwalker as a Serviceを利用するために必要な準備作業について説明します。

サービス契約後から利用開始までの作業プロセス

Systemwalker as a Serviceのサービス契約後から利用開始まで、以下のプロセスに沿って作業を進めてください。

1. 事前準備

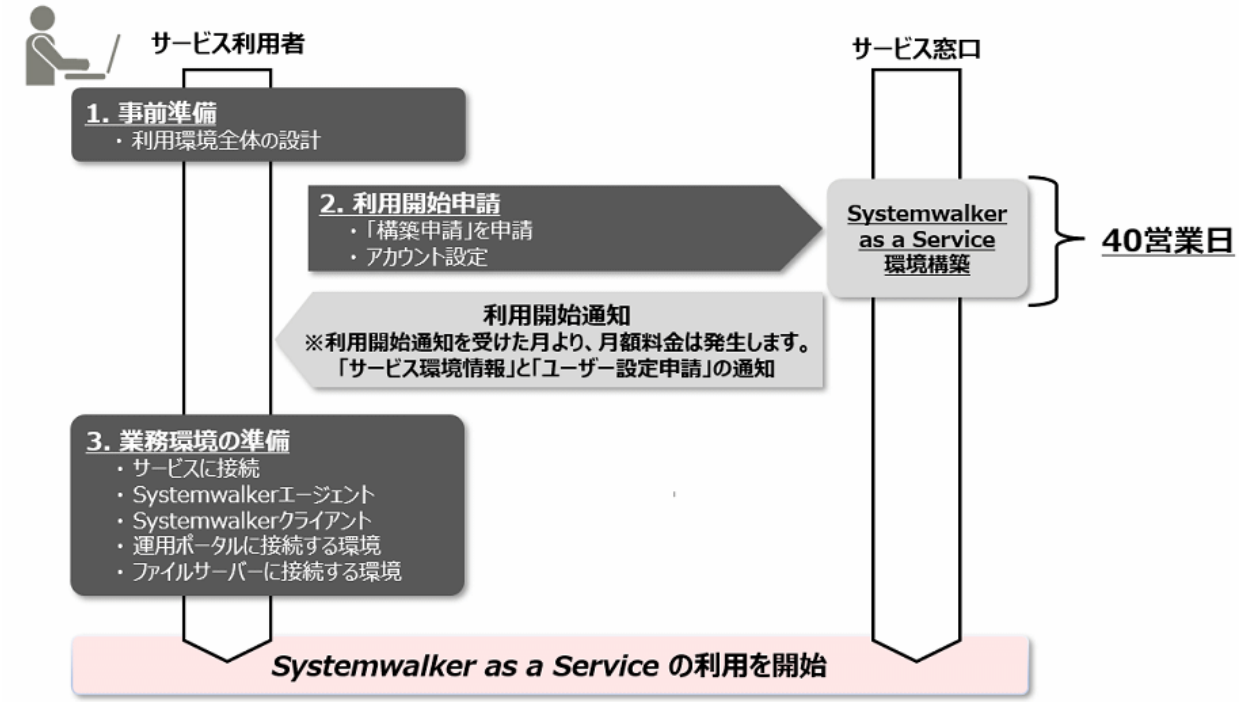
   利用環境の設計など、サービス利用に向けた準備をします。

2. 利用開始申請

   「構築申請」をサービス窓口に提出して、サービスの利用を開始します。

3. 業務環境の準備

   業務環境をSystemwalker as a Serviceに接続するための設定・準備をします。



各作業の詳細については、以降の節で詳しく説明します。

すべての作業が完了すると、Systemwalker as a Serviceを利用できます。

運用ポータル、統合管理機能、およびジョブ管理機能にログインして、サービスを利用してください。

2.1 サービス利用の事前準備をする

Systemwalker as a Serviceを利用するにあたり、事前準備が必要です。

2.1.1 サービスの利用環境を設計する

Systemwalker as a Serviceを利用するにあたり、お客様の業務環境に応じた構成を設計します。

設計内容に基づき、必要な情報を「構築申請」に記載します。

- 統合管理機能、ジョブ管理機能の構成
  - 各運用管理サーバの接続先となる全体監視サーバ
  - 各部門管理サーバの接続先となる運用管理サーバ
  - 各Systemwalkerマネージャーの冗長化の要否
- 運用ポータル
  - 表示する各Systemwalkerマネージャーの名称
- 業務環境とSystemwalker as a Serviceの接続
  - Systemwalkerマネージャーのネットワークアドレス（変更時のみ）
  - Systemwalkerマネージャーのホスト名の接頭語（変更時のみ）
  - 統合管理機能で使用するポート番号（変更時のみ）
  - ジョブ管理機能で使用するポート番号（変更時のみ）

注意

構築時に指定した上記のパラメーターは、サービス環境構築以降は変更できません。

2.1.2 サービス接続用仮想ネットワークを設計・構築する

業務環境において、Systemwalker as a Serviceと接続するためのAzure仮想ネットワーク(Azure Virtual Network)を設計・構築します。

1. 仮想ネットワークの作成

   Azure PortalなどからSystemwalker as a Serviceと接続するための仮想ネットワークを作成します。

2. リソースIDの取得と申請

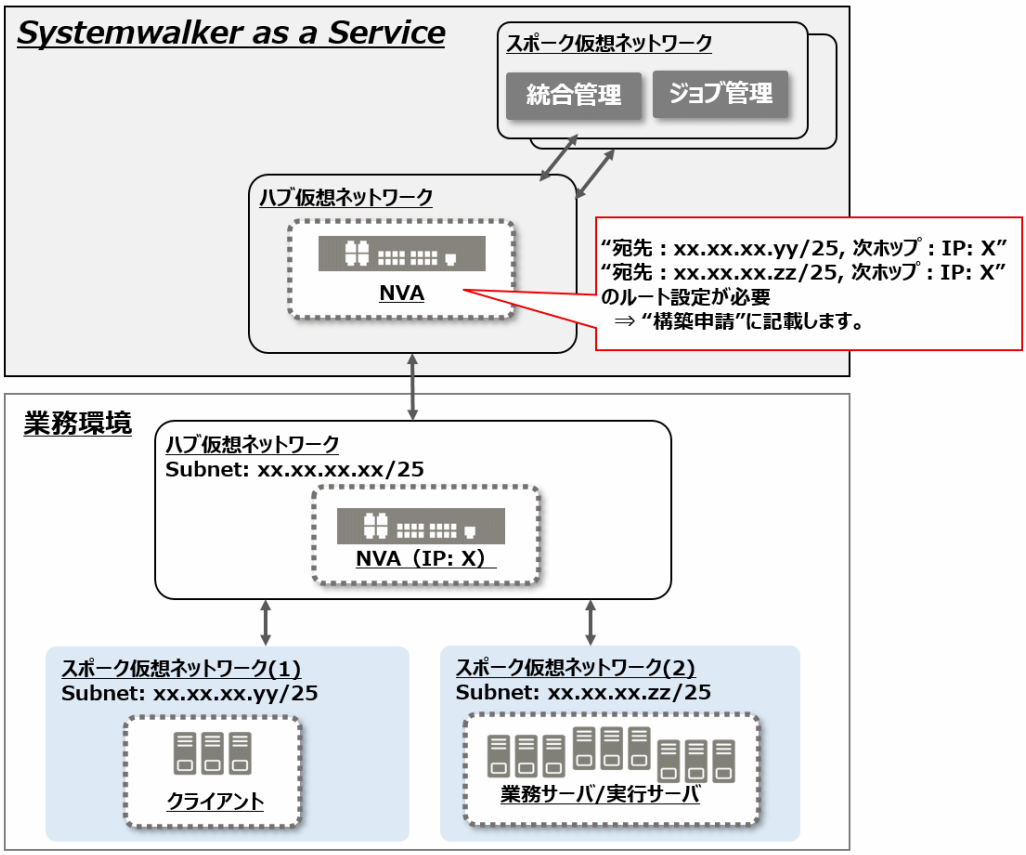
   作成したSystemwalker as a Serviceと接続するためのAzure仮想ネットワークのリソースIDを「構築申請」に記載します。
   記載されたリソースIDのAzure仮想ネットワークに対し、Systemwalker as a Serviceから仮想ネットワークピアリングを設定します。

3. ルートテーブルの設計と申請（必要な場合）

   業務環境をハブスポーク構成とし、そのハブネットワークをSystemwalker as a Serviceの仮想ネットワークに接続する場合など、Systemwalkerマネージャーが Systemwalker as a Serviceの仮想ネットワークと仮想ネットワークピアリングで直接接続しない仮想ネットワーク上の Systemwalkerエージェント、Systemwalkerクライアント、業務環境の運用管理サーバ、または業務環境の部門管理サーバと通信する必要がある場合は、Systemwalker as a Serviceの仮想ネットワークで設定が必要なルートテーブルの設計をサービス利用者にて行い、「構築申請」に記載してください。

   以下に、Systemwalker as a ServiceとSystemwalkerエージェント、Systemwalkerクライアント、業務環境の運用管理サーバ、業務環境の部門管理サーバ間を、業務環境のハブスポーク構成のハブネットワークを経由して接続する場合のルートテーブル設計の例を示します。

ルートテーブルの設定が必要な構成例



Disaster Recoveryを利用する場合は、西日本リージョン側のサービス接続点と接続するための仮想ネットワークも設計・構築します。

ポイント

- ハブ仮想ネットワークのネットワーク仮想アプライアンス(NVA)としてAzure Firewallを利用する場合は、SKUをStandard以上にしてください。
- AWS上の業務環境(Systemwalkerクライアント、Systemwalker エージェント等)を接続する場合の例は“付録G AWS上の業務環境接続例”を参照してください。

2.1.3　仮想ネットワークピアリング設定用アカウントを設計・作成する

業務環境において、Systemwalker as a Serviceとの仮想ネットワークピアリングを設定するためのアカウントを設計し、作成します。

Disaster Recoveryを利用する場合、本アカウントは西日本リージョン側のサービス接続点と接続するための仮想ネットワークピアリング設定時にも使用します。

1. “2.1.2 サービス接続用仮想ネットワークを設計・構築する”で構築した仮想ネットワークについてネットワーク共同作成者ロールを持つアカウントを作成します。
2. 作成したアカウントのユーザー プリンシパル名を「構築申請」に記載します。

ポイント

利用開始申請後、サービス窓口にて、申請されたアカウントがSystemwalker as a ServiceのMicrosoft Entra IDにゲストアカウントとして追加されます。

2.1.4　運用ポータルの契約者アカウントを作成する

運用ポータルの契約者アカウントを作成するには、管理ポータル上で「メンバー管理者(契約者)」アカウントを、以下の手順で作成してください。

1. 以下のURLにアクセスします。

```
https://portal.aispf.global.fujitsu.com/#/systemwalker-service
```

2. [新規アカウントの作成]をクリックします。
3. アカウント情報入力欄に必要事項を入力し、[アカウント登録]をクリックします。
4. 本登録用のメールが送信されますので、メール本文に記載されたURLにアクセスしてください。
5. 登録情報（[アカウントID]）を「構築申請」に記載します。

ポイント

管理ポータルと運用ポータル利用時の2段階認証を有効にする場合は、管理ポータルにログイン後、[アカウント管理]メニューの[アカウント情報変更]から設定してください。

2.2　サービスの利用開始申請をする

「構築申請」をサービス窓口に申請して、サービスの利用を開始します。

2.2.1　構築申請をサービス窓口へ送信する

必要な情報を記載した「構築申請」をサービス窓口へ送信します。

2.2.2　仮想ネットワークピアリング設定用アカウントの設定を実施する

業務環境において、仮想ネットワークピアリングを設定するためのアカウント設定を、以下の手順で実施します。

アカウントの招待と多要素認証（MFA）の設定

1. “2.1.3 仮想ネットワークピアリング設定用アカウントを設計・作成する”で作成したアカウントに対し、招待用のURLがサービス窓口より通知されます。
2. 通知されたURLにアクセスし、招待を受け入れてください。
3. 招待受け入れ後、多要素認証（MFA）の設定を行ってください。

アカウントの登録と権限付与

Systemwalker as a Serviceの仮想ネットワークピアリングに必要なSystemwalker as a Serviceのアカウント情報がサービス窓口から通知されます。

通知されたアカウントを業務環境のMicrosoft Entra IDにB2Bコラボレーションによりゲストユーザーとして登録し、必要な権限を付与してください。

Disaster Recoveryを利用する場合は、西日本リージョン側のサービス接続点と接続するための仮想ネットワークに対する権限も付与してください。

1. Azure Portalの「Microsoft Entra ID」などから、以下の設定値でユーザーを招待します。

   - メール：サービス窓口より通知されたメールアドレス
   - 招待メッセージの送信：無効

   ポイント

   上記以外の設定値については、サービス利用者にて設計し、決定してください。

2. 招待したユーザーについて、“2.1.2 サービス接続用仮想ネットワークを設計・構築する”の仮想ネットワークに対し、以下のアクセス権限を持つロールを割り当てます。

   Systemwalker as a Serviceから業務環境の複数の仮想ネットワークに対しピアリングする場合、ピアリングするすべての仮想ネットワークについてロールを割り当ててください。

   - Microsoft.Network/virtualNetworks/peer/action

3. 本操作の完了とテナントIDをサービス窓口に通知してください。

   テナントIDはAzure Portalの「Microsoft Entra ID」などで確認できます。

2.2.3 利用開始通知を受信する

サービス環境構築には、標準納期として40営業日を必要とします。

サービス環境構築完了後、サービス窓口から利用開始通知が送信されます。利用開始通知時に、「サービス環境情報」と「ユーザー設定申請」が通知されます。

利用開始通知日を受けた月より、月額料金は発生します。

2.3 業務環境を準備する

サービス利用開始通知を受信後、業務環境をSystemwalker as a Serviceに接続できます。

2.3.1 サービスに接続する

Systemwalker as a Serviceに接続するために、仮想ネットワークピアリングおよびルートテーブルを、以下の手順で設定してください。

1. サービス利用者は、“2.1.3 仮想ネットワークピアリング設定用アカウントを設計・作成する”で作成したアカウントを使用し、“2.1.2 サービス接続用仮想ネットワークを設計・構築する”で構築した仮想ネットワークについて、仮想ネットワークピアリングを作成してください。

   ピアリング作成時は、以下のように設定してください。

項目	設定値
ローカル仮想ネットワークにリモート仮想ネットワークへのアクセスを許可する	有効
ローカル仮想ネットワークがリモート仮想ネットワークへ転送されたトラフィックを受信することを許可する	有効
ローカル仮想ネットワークのゲートウェイまたはルートサーバーがリモート仮想ネットワークにトラフィックを転送することを許可する	無効
ローカル仮想ネットワークでリモート仮想ネットワークのリモートゲートウェイまたはルートサーバーを使用できるようにする	無効
リモート仮想ネットワークのデプロイモデル	Resource Manager
リモート仮想ネットワークのリソースID	「サービス環境情報」に記載のID（注）

注）Disaster Recoveryを利用する場合は、接続するリージョンの仮想ネットワークのリソースID

ポイント

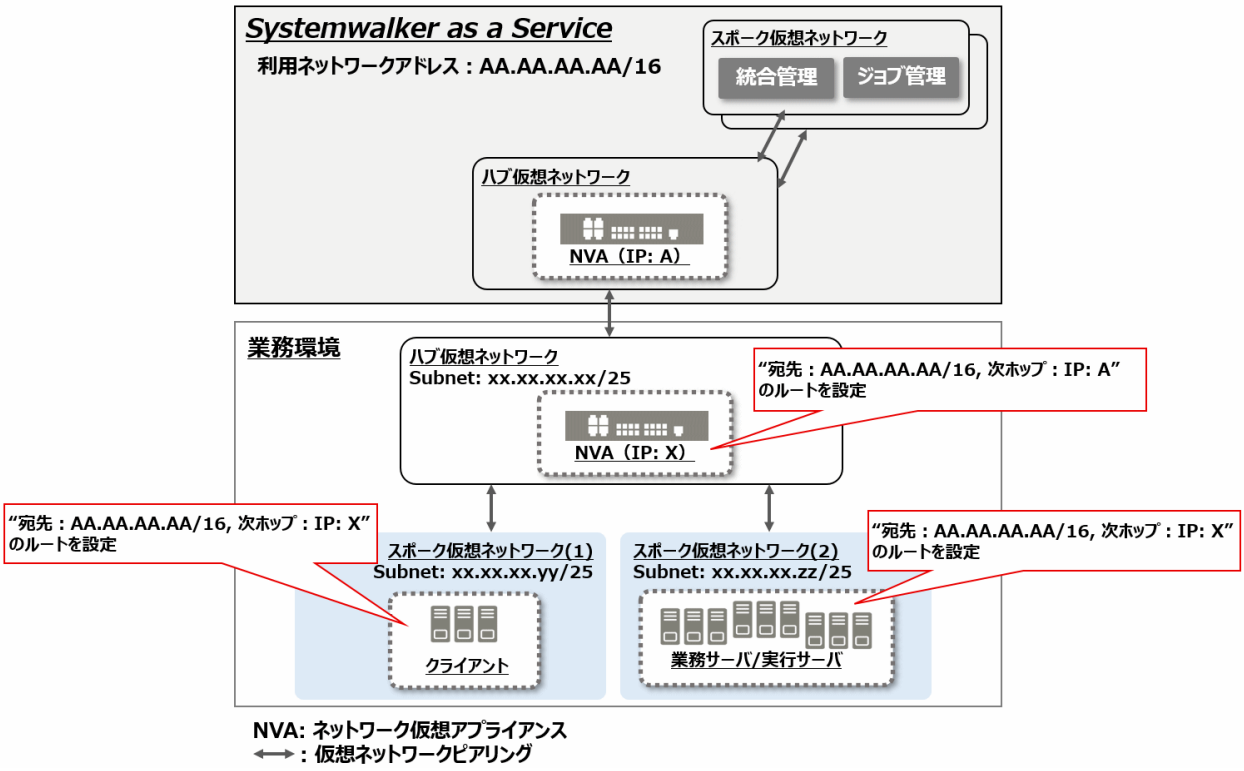
上記以外の設定値については、サービス利用者にて設計し、決定してください。

Azureコマンドラインインターフェイス（CLI）による設定例については“付録E 仮想ネットワークピアリングの設定方法”を参照してください。

2. “2.1.2 サービス接続用仮想ネットワークを設計・構築する”で作成した仮想ネットワークなど必要な個所にルートテーブルを設定します。

   設定値は「サービス環境情報」に記載の値を参照してください。

ルートテーブルの設定例



2.3.2 Systemwalkerエージェント環境を準備する

Systemwalkerエージェントの環境を準備する手順については、“4.1.1 Systemwalkerエージェントを追加する”を参照してください。

2.3.3 Systemwalkerクライアント環境を準備する

Systemwalkerクライアントの環境を準備する手順については、“Systemwalkerクライアントを追加する”を参照してください。

2.3.4 運用ポータルに接続する環境を準備する

運用ポータルに接続する端末において、以下の手順でWebブラウザを準備します。

1. 運用ポータルに接続するために必要なWebブラウザをインストールします。

   動作環境については、以下のマニュアルを参照してください。

   ー Systemwalker as a Service 機能説明書

   “Systemwalker as a Serviceのサポート範囲”

2. 「サービス環境情報」を確認し、運用ポータルのホスト名を名前解決できるようにhostsファイルを編集します。
3. 「サービス環境情報」に記載されている証明書をインポートします。

   証明書ストアは「信頼されたルート証明機関」を選択してください。

ポイント

Webブラウザから運用ポータルへのアクセスには、httpsプロトコルでTCPの443番ポートを利用します。

送信元とあて先の間にファイアウォールが存在する場合は、ファイアウォールへのポート番号の設定が必要です。

2.3.5 ファイルサーバーに接続する環境を準備する

ファイルサーバーに接続する端末には、SFTPクライアントをインストールしてください。

ポイント

SFTPクライアントからファイルサーバーへのアクセスには、TCPの22番ポートを利用します。

送信元とあて先の間にファイアウォールが存在する場合は、ファイアウォールへのポート番号の設定が必要です。

2.3.6 統合管理機能のWeb APIを発行する環境を準備する

統合管理機能のWeb APIを発行する場合は、発行元の端末を以下の手順で準備します。

1. 「サービス環境情報」を確認し、API発行先のSystemwalker Cnetric Managerのホスト名を名前解決できるよう、hostsファイルを編集します。

   対象のSystemwalkerマネージャーが冗長構成のサービスプランの場合、論理ホスト名および論理IPアドレスについて、名前解決できるようにしてください。

2. 「サービス環境情報」に記載されている証明書を、発行元の端末に配置し、API発行時に利用できるようにします。

ポイント

Systemwalker Centric ManagerへのAPI発行時のアクセスには、httpsプロトコルでTCPの443番ポートを使用します。

送信元とあて先の間にファイアウォールが存在する場合は、ファイアウォールへのポート番号の設定が必要です

2.4 サービスの利用を開始する

2.4.1 運用ポータルにログインする

ここでは、運用ポータルのログインおよびログアウトするための手順について説明します。

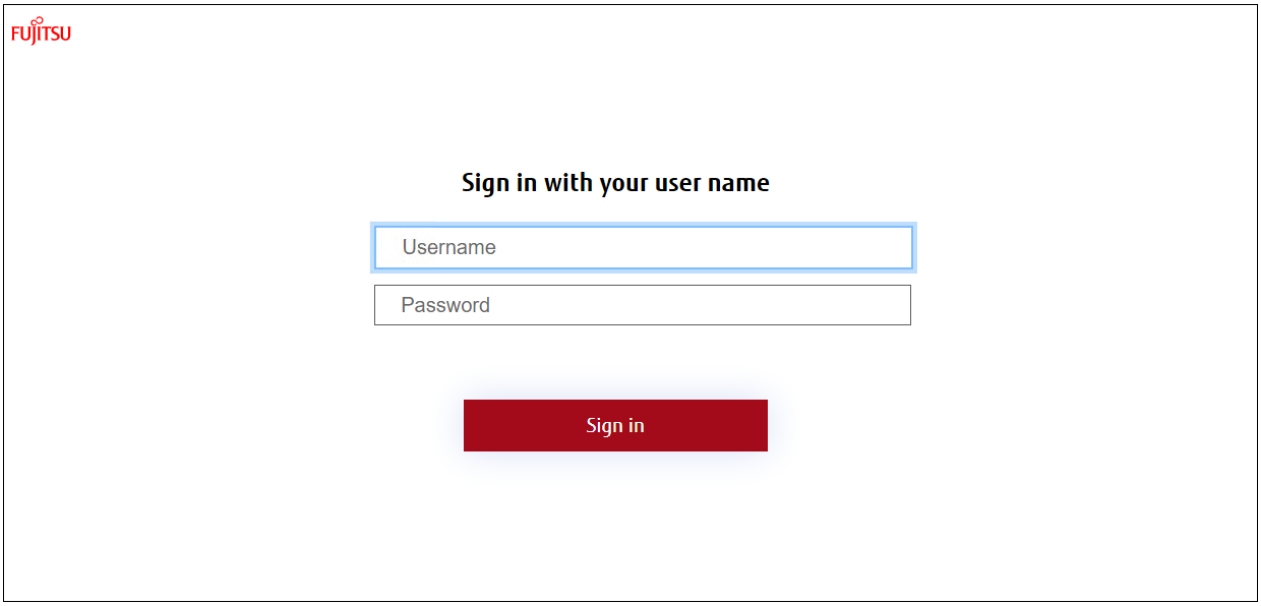
ログイン手順

運用ポータルにログインするための手順について説明します。

1. 「サービス環境情報」に記載されている運用ポータルの接続先URLを確認します。
   ブラウザで接続先URLにアクセスすると、ログイン画面へのリンクが表示されます。



2. [Username]、[Password]にアカウントIDとパスワードを入力して、[Sign in]をクリックします。



3. 2段階認証が有効である場合は、以下の手順で認証情報を入力します。
   a. 認証コードの送信先を確認する画面が表示されます。
   b. [Send verification code]をクリックすると認証コードが送付されます。
   c. 認証コードを入力し、[Verify code]をクリックします

> **注意**
>
> 複数回にわたって誤った認証コードを入力すると、「You have exceeded the number of retries allowed.」が表示されます。その場合は、しばらく待ってから再度b.の手順以降を実施してください。

d. 認証が成功するとメッセージが表示されますので、[Continue]をクリックします。

> **ポイント**
>
> 以下のアカウントが運用ポータルへのログインに使用可能です。
>
> - 契約者アカウント
> - “3.1 運用ポータルのユーザーを管理する”で作成した運用ポータルのユーザー
>
> ログイン後、[HTTP ERROR 401]のエラーが表示された場合は、上記のログインできるアカウントであることを確認した後、しばらく待ってから再度ログイン操作を実施してください。

ログアウト手順

運用ポータルからログアウトするための手順について説明します。

1. 運用ポータルの画面上部にあるユーザー名をクリックすると、[ログアウト]が表示されます。



2. [ログアウト]をクリックします。

> **ポイント**
>
> ブラウザの設定によっては、ブラウザを閉じただけではログアウトされない場合があります。
>
> 確実にログアウトするためには、本操作を実行して、ログアウトをしてください。

2.4.2 統合管理機能にログインする

統合管理機能にログインするための手順について説明します。

1. 「サービス環境情報」と「ユーザー設定申請」に記載された情報を確認します。
2. 運用管理クライアントのSystemwalkerコンソールから、全体監視サーバまたは運用管理サーバに接続してログインします。

2.4.3 ジョブ管理機能にログインする

ジョブ管理機能にログインするための手順について説明します。

1. 「サービス環境情報」と「ユーザー設定申請」に記載された情報を確認します。
2. Systemwalker Operation Manager クライアントから、スケジュールサーバに接続してログインします。

2.4.4　ファイルサーバーにログインする

ファイルサーバーにログインするための手順について説明します。

ポイント

ファイルサーバーにアクセスするユーザーは、事前に作成しておきます。

“3.4 ファイルサーバーのユーザーを管理する”を参照してください。

1. 「サービス環境情報」に記載されたファイルサーバーの接続情報を確認します。
2. SFTPクライアントを使用し、秘密鍵とパスフレーズを指定してファイルサーバーにログインします。

ファイルサーバーは2台提供されます。一方のファイルサーバーに接続できない場合は、もう一方のファイルサーバーに接続してください。

接続方法については、“付録B ファイルサーバーへのログイン方法”を参照してください。

第3章 Systemwalker as a Serviceで利用するユーザーを管理する

本章では、Systemwalker as a Serviceで利用するユーザーの管理について説明します。

3.1 運用ポータルのユーザーを管理する

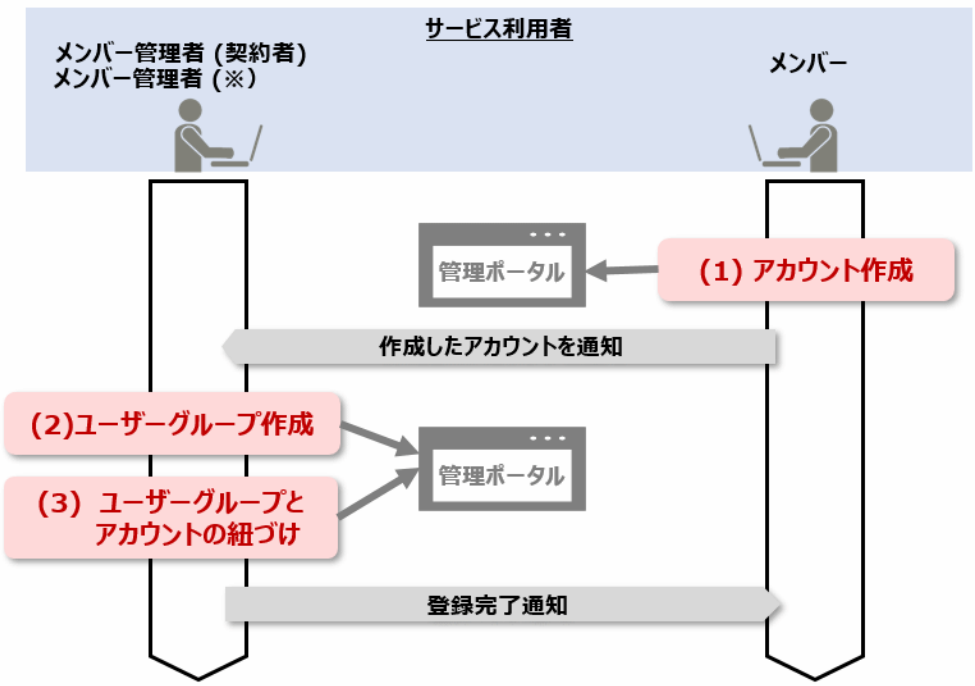
運用ポータルのユーザーは、管理ポータルを使用して作成します。

運用ポータルで作業するユーザーを追加する場合は、新規にユーザーを作成してください。作成されたユーザーは、[Systemwalker as a Service]サービスに関係付けられたユーザーグループで管理されます。

管理ポータルには、以下の3種類のアカウントがあります。それぞれのアカウントに応じた作業を実施してください。

- メンバー管理者（契約者）
- メンバー管理者
- メンバー

メンバー管理者（契約者）とは、“2.1.4 運用ポータルの契約者アカウントを作成する”で作成された契約者アカウントのことで、以下の図に示すように、他のメンバーによって作成されたアカウントを管理します。



※）メンバー管理者は「(3) ユーザーグループとアカウントの紐づけ」の操作のみ可能です。

メンバーの操作

メンバー用アカウントを作成する手順は、以下のとおりです。

1. 管理ポータルにアクセスします。

   ```
   https://portal.aispf.global.fujitsu.com/#/systemwalker-service
   ```

2. [新規アカウントの作成]をクリックします。
3. アカウント情報入力欄に必要事項を記載し、[アカウント登録]をクリックします。

4. 本登録用のメールが送信されるので、メール本文のURLにアクセスします。
5. 登録完了後、登録情報（[アカウントID]および[メールアドレス]）をメンバー管理者（契約者）に通知してください。

ポイント

管理ポータルおよび運用ポータルで2段階認証を有効にする場合

管理ポータルにログイン後、[アカウント管理]メニューの[アカウント情報変更]から2段階認証の設定を有効にします。

メンバー管理者（契約者）の操作

作成済みのユーザーグループのメンバー数が上限（1グループあたり50名）に達した場合のみ、新たにユーザーグループを作成してください。

1. 管理ポータルにアクセスし、ログインします。

```
https://portal.aispf.global.fujitsu.com/#/systemwalker-service
```

2. 左メニューの[API認証情報と利用者管理]をクリックします。
3. グループ一覧から[作成]ボタンをクリックします。
4. グループ名を入力し、利用するサービスとして[Systemwalker as a Service]を選択し、[作成]ボタンをクリックします。

メンバー管理者（契約者）とメンバー管理者の操作

メンバーのアカウントをユーザーグループに所属させます。

1. 管理ポータルにアクセスし、ログインします。

```
https://portal.aispf.global.fujitsu.com/#/systemwalker-service
```

2. 左メニューの[API認証情報と利用者管理]をクリックします。
3. グループ一覧から、対象となるユーザーグループをクリックします。
4. [メンバー管理]タブをクリックします。
5. [追加]ボタンをクリックし、サービス利用者を追加します。
6. サービス利用者に、登録が完了したことを通知してください。

ポイント

管理ポータルでは、アカウントの削除やパスワードの変更などの操作が可能です。

作成された各種アカウント情報はすべて暗号化されたうえで、安全に保管されます。

参考

メンバー管理者（契約者）は、ユーザーグループに所属するアカウントに対し、メンバー管理者のロールを付与することで、そのメンバー管理者もメンバーのアカウントをユーザーグループに所属させる操作ができるようになります。

また、運用ポータルでの実施可能な操作は、管理ポータルにおけるロール設定の影響を受けません。本操作で登録したユーザーは、運用ポータル上ですべての操作が可能です。

3.2　統合管理機能のユーザーを管理する

統合管理機能で使用するユーザーを変更する場合は、「ユーザー設定申請」に必要事項を記載し、サービス窓口へ提出してください。

なお、Systemwalker管理者アカウントは削除できません。

3.3　ジョブ管理機能のユーザーを管理する

ジョブ管理機能で使用するユーザーを変更する場合は、「ユーザー設定申請」に必要事項を記載し、サービス窓口へ提出してください。

なお、OSユーザー（システム管理者）と拡張ユーザー（管理者アカウント）は削除できません。

3.4　ファイルサーバーのユーザーを管理する

ファイルサーバーのユーザーを変更する場合は、「ユーザー設定申請」に必要事項を記載し、サービス窓口へ提出してください。

申請で必要となるキーペアの発行例については、“付録A ファイルサーバーユーザー用のキーペアの発行方法”を参照してください。

第4章 システム構成を管理する

本章では、サービス利用者が業務環境のシステム構成を管理する手順について説明します。

4.1 Systemwalkerエージェントの構成を管理する

Systemwalkerエージェントの追加、変更、および削除について説明します。

注意

業務環境における、運用管理サーバと部門管理サーバの追加については、“4.4 業務環境の運用管理サーバ・部門管理サーバを追加する”を参照してください。

4.1.1 Systemwalkerエージェントを追加する

統合管理

業務サーバの導入は、Systemwalker Centric Managerのマニュアルを参照して実施してください。

接続先となる各SystemwalkerマネージャーのIPアドレスおよびホスト名は、「サービス環境情報」を確認してください。

SNMPエージェントを利用する場合は、SNMPv3（AESによる暗号化あり）の使用を推奨します。

また、業務サーバの情報を「エージェント申請」に記載し、サービス窓口に提出します。

運用ポータルから業務サーバのノード一括追加

Systemwalkerコンソールによるノード自動検出や1ノードずつ個別に登録もできますが、Systemwalker as a Serviceでは、運用ポータルから一括での追加を推奨しています。

以下の手順で、CSVファイルを用いて一括追加を行います。

1. 構成管理を記載したCSVファイルを作成します。

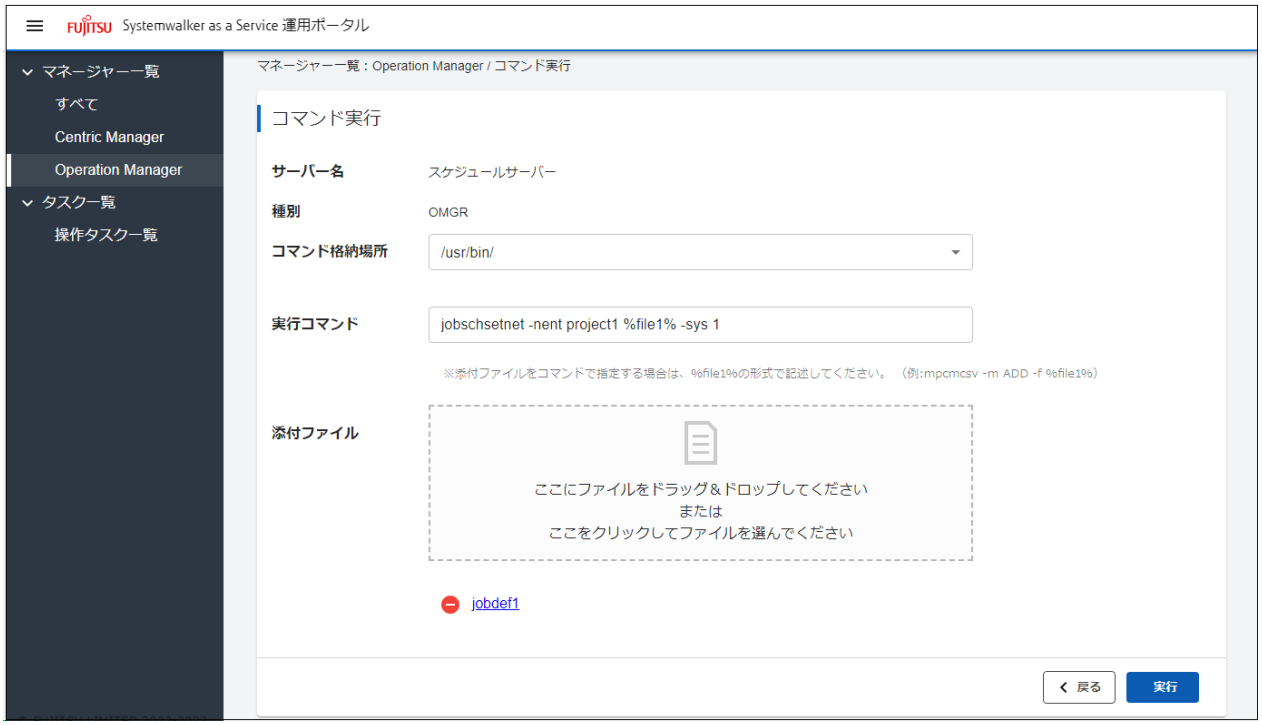
   CSVファイルについては、以下のマニュアルを参照してください。

   - Systemwalker Centric Manager リファレンスマニュアル

     “構成管理のCSVファイル”

2. 運用ポータルの[マネージャー一覧]画面で、業務サーバを追加するマネージャーの[操作]メニューから表示される[コマンド操作]をクリックします。

3. 表示された運用ポータルの[コマンド実行]画面で、以下を実施してください。



   a. 以下を指定します。

      コマンド格納場所: /opt/systemwalker/bin/

      実行コマンド: mpcmcsv -m ADD -f %file1%

   b. [添付ファイル]欄に作成した構成管理のCSVファイルを添付します。

   c. [実行]ボタンクリックします。

4. 運用ポータルの[操作タスク一覧]画面で、実施した操作が「Finished」となったことを確認します。
5. 運用管理クライアントからSystemwalkerコンソールを起動し、追加された業務サーバを確認します。

ジョブ管理

実行サーバの導入はSystemwalker Operation Managerのマニュアルを参照して実施してください。

接続先となる各SystemwalkerマネージャーのIPアドレスおよびホスト名は、「サービス環境情報」を確認してください。

また、実行サーバの情報を「エージェント申請」に記載し、サービス窓口に提出します。

4.1.2 Systemwalkerエージェントを変更する

SystemwalkerエージェントのIPアドレスまたはホスト名を変更する手順については、“4.1.1 Systemwalkerエージェントを追加する”を参照してください。

この際、追加済みのSystemwalkerエージェントを更新する操作であることを踏まえて、該当箇所を読み替えてください。

4.1.3 Systemwalkerエージェントを削除する

統合管理

業務サーバの削除は、Systemwalker Centric Managerのマニュアルを参照して実施してください。

また、削除した業務サーバの情報を「エージェント申請」に記載し、サービス窓口に提出します。

運用ポータルから業務サーバのノード一括削除

Systemwalkerコンソールで1ノードずつ個別に削除することもできますが、Systemwalker as a Serviceでは、運用ポータルでの一括削除を推奨しています。

1. 構成管理を記載したCSVファイルを作成します。

   CSVファイルについては、以下のマニュアルを参照してください。

   - Systemwalker Centric Manager リファレンスマニュアル

     “構成管理のCSVファイル”

2. 運用ポータルの[マネージャー一覧]画面で、業務サーバを削除する対象マネージャーの[操作]メニューから[コマンド操作]をクリックします。
3. 表示された運用ポータルの[コマンド実行]画面で、以下を実施してください。
   a. 以下を指定します。

      コマンド格納場所: /opt/systemwalker/bin/

      実行コマンド: mpcmcsv -m DEL -f %file1%

   b. [添付ファイル]欄に作成した構成管理のCSVファイルを添付します。
   c. [実行]ボタンをクリックします。
4. 運用ポータルの[操作タスク一覧]画面で、実施した操作が「Finished」となっていることを確認します。
5. 運用管理クライアントからSystemwalkerコンソールを起動し、業務サーバが削除されていることを確認します。

ジョブ管理

実行サーバの削除は、Systemwalker Operation Managerのマニュアルを参照して実施してください。

また、削除した実行サーバの情報を「エージェント申請」に記載し、サービス窓口に提出します。

4.2 全体監視サーバにノード情報を登録する

運用管理サーバのノード構成情報を全体監視サーバへ登録する方法について説明します。

1.「全体監視サーバへのノード情報登録申請」に必要な情報を記載します。
2. 作成した「全体監視サーバへのノード情報登録申請」をサービス窓口に提出します。

   「全体監視サーバへのノード情報登録申請」がサービス窓口で受理されると、受理完了の通知がされます。
3. 全体監視サーバへのノード情報登録が実施されると、サービス窓口から全体監視サーバへのノード情報登録通知が通知されます。

4.3 Systemwalkerクライアントの構成を管理する

Systemwalkerクライアントの追加と変更、および削除について説明します。

Systemwalkerクライアントを追加する

統合管理

運用管理クライアントの導入は、Systemwalker Centric Managerのマニュアルを参照して実施してください。

接続先となる各SystemwalkerマネージャーのIPアドレスおよびホスト名は、「サービス環境情報」を確認してください。

また、運用管理クライアントの情報を「クライアント申請」に記載し、サービス窓口に提出します。

ジョブ管理

Systemwalker Operation Managerクライアントの導入は、Systemwalker Operation Managerのマニュアルを参照して実施してください。

接続先となる各SystemwalkerマネージャーのIPアドレスおよびホスト名は、「サービス環境情報」を確認してください。

また、クライアントの情報を「クライアント申請」に記載し、サービス窓口に提出します。

Systemwalkerクライアントを変更する

SystemwalkerクライアントのIPアドレスまたはホスト名を変更した場合は、変更後の情報を「クライアント申請」に記載し、サービス窓口に提出します。

Systemwalkerクライアントを削除する

Systemwalker Centric ManagerおよびSystemwalker Operation Managerのマニュアルを参照のうえ、実施してください。

また、削除したSystemwalkerクライアントの情報を「クライアント申請」に記載し、サービス窓口に提出します。

4.4 業務環境の運用管理サーバ・部門管理サーバを追加する

業務環境の運用管理サーバおよび部門管理サーバの追加について説明します。

これらのサーバは、以下のパターンでSystemwalkerマネージャーと連携できます。

- 業務環境の運用管理サーバをSystemwalkerマネージャーの全体監視サーバと連携する
- 業務環境の部門管理サーバをSystemwalkerマネージャーの運用管理サーバと連携する

4.4.1 業務環境の運用管理サーバを追加する

業務環境の運用管理サーバをSystemwalkerマネージャーの全体監視サーバと連携する場合、構築済みの業務環境の運用管理サーバに関する「構成情報」および「エージェント申請」をもとに、必要な情報をサービス窓口へ提出します。その後、業務環境の運用管理サーバの接続を設定します。

1. 構築した運用管理サーバの情報を「構成情報」に記載します。
2. 「構成情報」をサービス窓口に提出します。
3. 業務環境の運用管理サーバ経由で接続する、業務環境の部門管理サーバおよび業務サーバの情報を「エージェント申請」に記載します。
4. 「エージェント申請」をサービス窓口に提出します。
5. 「構成情報」、「エージェント申請」の完了通知を受信後に、業務環境の運用管理サーバの接続を設定します。

   接続先となる各SystemwalkerマネージャーのIPアドレスおよびホスト名は、「サービス環境情報」を確認してください。

   設定手順については、以下のマニュアルを参照してください。

   ー Systemwalker Centric Manager 全体監視適用ガイド

   “運用管理サーバの設定”

   “全体監視サーバへの構成情報の移入”

   以下のマニュアルを確認し、必要に応じて設定してください。

   ー Systemwalker Centric Manager 使用手引書 監視機能編

   “LANカード（NIC）に複数のIPアドレスを登録した場合、およびLANカード（NIC）を複数枚搭載した場合の留意事項”

6. 運用ポータルから業務環境の運用管理サーバのノード情報をSystemwalkerマネージャー全体監視サーバに移入します。

   a. 移入元となる業務環境の運用管理サーバのノード情報を作成します。

      移入元となる業務環境の運用管理サーバからmpcmnout（ノード情報移出コマンド）を使用して、ノード情報を移出してください。

   b. 運用ポータルの[マネージャー一覧]画面で、移入先のマネージャーの[操作]メニューから表示される[コマンド操作]をクリックします。

   c. 表示された運用ポータルの[コマンド実行]画面で、以下を実施してください。

      1. 以下を指定します。

         コマンド格納場所：/opt/systemwalker/bin/

         実行コマンド：mpcmsumt.sh %file1%

      2. [添付ファイル]欄に作成したノード情報のファイルを添付します。

      3. [実行]ボタンクリックします。

   d. 運用ポータルの[操作タスク一覧]画面で、実施した操作が「Finished」となったことを確認します。

   e. 運用管理クライアントからSystemwalkerコンソールを起動し、正しく設定されていることを確認します。

4.4.2　業務環境の部門管理サーバを追加する

業務環境の部門管理サーバをSystemwalkerマネージャーの運用管理サーバと連携する場合は、「エージェント申請」に必要な情報を記載してサービス窓口に提出します。

その後、業務環境の部門管理サーバの接続を設定します。

1. 構築した業務環境の部門管理サーバ、および配下の業務サーバの情報を「エージェント申請」に記載します。
2. 「エージェント申請」をサービス窓口に提出します。
3. 上記で申請した「エージェント申請」の完了通知を受信後に、業務環境の部門管理サーバの接続を設定します。

   接続先となる各SystemwalkerマネージャーのIPアドレスおよびホスト名は、「サービス環境情報」を確認してください。

   設定手順については、以下のマニュアルを参照してください。

   ー Systemwalker Centric Manager 使用手引書 監視機能編

      “イベント通知先を設定する”

   以下のマニュアルを確認し、必要に応じて設定してください。

   ー Systemwalker Centric Manager 使用手引書 監視機能編

      “LANカード（NIC）に複数のIPアドレスを登録した場合、およびLANカード（NIC）を複数枚搭載した場合の留意事項”

4. 業務環境の部門管理サーバがクラスタ構成の場合、運用ポータルから、業務環境の部門管理サーバのクラスタ論理ノードを連携先のSystemwalkerマネージャーの運用管理サーバに登録します。

   a. 運用ポータルの[マネージャー一覧]画面で、対象となる業務環境の部門管理サーバを連携する運用管理サーバの[操作]メニューから表示される[コマンド操作]をクリックします。

   b. 表示された運用ポータルの[コマンド実行]画面で、以下を実施してください。

      1. 以下を指定します。

         コマンド格納場所：/opt/systemwalker/bin/

         実行コマンド：mpcmclst.sh -a -h 業務環境の部門管理サーバのクラスタシステムのプライマリノードのホスト名 -i 業務環境の部門管理サーバのクラスタシステムの仮想IPアドレス -n 業務環境の部門管理サーバのクラスタ論理ノードのホスト名

      2. [実行]ボタンをクリックします。

   c. 運用ポータルの[操作タスク一覧]画面で、実施した操作が「Finished」となったことを確認します。

d. 運用管理クライアントからSystemwalkerコンソールを起動し、クラスタ論理ノードが追加されていることを確認します。

第5章 Systemwalker as a Serviceの運用を変更する

本章では、Systemwalker as a Serviceの運用を変更する手順について説明します。

本マニュアルに記載のない運用変更については、サービス窓口にご連絡ください。

5.1 Systemwalkerマネージャーのログ収集設定を変更する

Systemwalkerマネージャーの定期的なログ収集のスケジュールを設定できます。

以下の手順に従って、ログ収集の設定を変更します。

1. 「マネージャーログ定期収集設定申請」に変更する情報を記載します。
2. 作成した「マネージャーログ定期収集設定申請」をサービス窓口に提出します。

   「マネージャーログ定期収集設定申請」がサービス窓口で受理されると、受理完了の通知がされます。
3. ログ収集設定変更が実施されると、サービス窓口からログ収集設定変更通知が通知されます。

注意

- スケジュールタイミングとしては、1日の運用終量（日替わり前）を推奨します。
  また、Systemwalkerマネージャーの定常バックアップのスケジュールをしているタイミングは避けて申請してください。
- 対象のSystemwalkerマネージャーが冗長構成のサービスプランの場合、Systemwalkerマネージャーのログは、プライマリノードおよびセカンダリノードごとに収集されます。

5.2 Systemwalkerエージェントのログ収集設定を変更する

Systemwalkerエージェントのログは、統合管理機能の監査ログ管理機能を使用して収集しています。

以下の手順に従って、ログ収集の設定を変更します。

1. 監査ログ管理機能を利用するために、以下のファイルを作成し、「エージェントログ収集設定申請」に必要な情報を記載します。

   ー 監査ログ管理ポリシーファイル

   ー 日付書式ポリシーファイル

   ー 接続可能一覧ファイル
2. 作成したファイルと「エージェントログ収集設定申請」をサービス窓口に提出します。

   「エージェントログ収集設定申請」がサービス窓口で受理されると、受理完了の通知がされます。
3. ログ収集設定変更が実施されると、サービス窓口からログ収集設定変更通知が通知されます。

以下のマニュアルを参照してください。

- Systemwalker Centric Manager リファレンスマニュアル

  “監査ログ管理ポリシーファイル”

  “監査ログ管理 日付書式ポリシーファイル”
- Systemwalker Centric Manager 使用手引書 セキュリティ編

  “収集対象のサーバを限定する”

注意

SystemwalkerエージェントのログはSystemwalker Centric Manager 運用管理サーバのログに含まれるため、Systemwalkerマネージャーのログ収集設定により定期的に収集されます。

Systemwalkerマネージャーのログ収集設定については、“5.1 Systemwalkerマネージャーのログ収集設定を変更する”を参照してください。

5.3 定常バックアップのタイミングを変更する

Systemwalkerマネージャーの定期的なバックアップのスケジュールは、以下の手順で設定できます。

1. 「定常バックアップ設定申請」に変更する情報を記載します。
2. 作成した「定常バックアップ設定申請」をサービス窓口に提出します。

   「定常バックアップ設定申請」がサービス窓口で受理されると、受理完了の通知がされます。
3. 定常バックアップ設定変更が実施されると、サービス窓口から定常バックアップ設定変更完了通知が通知されます。

ポイント

- Systemwalkerマネージャーのリストアを実施するために、事前にバックアップを実施しています。
  リストアを実施したい場合は、サービス窓口にご連絡ください。
- 統合管理機能をリストアする場合は、関連するSystemwalkerマネージャー（全体監視サーバ、運用管理サーバ、部門管理サーバ）がすべてリストアされます。また、Systemwalkerマネージャーのバックアップは、Systemwalker Centric Managerのmpbkc（バックアップコマンド）とSystemwalker Operation Managerのmpbko（バックアップコマンド）を使用しています。バックアップ対象範囲は、オンラインバックアップを行った場合と同様になります。

注意

- 定常バックアップを行っているタイミングで、任意バックアップを実行することはできません。また、サービス内で同時に複数実行することはできません。
  任意のバックアップのタイミング検討時には、“定常バックアップ設定申請”で定常バックアップタイミングを確認してください。
- 定常バックアップの実施時期は、Systemwalkerマネージャーが日替わり処理などの高負荷な処理を実行している時間は避けて、定常バックアップの実施時期を申請してください。
  バックアップ実行中は、Systemwalkerコンソールから以下の操作を行わないでください。
  - 監視ポリシーの変更

    未配付の監視ポリシーが残っている場合には、事前に監視ポリシー配付を済ませておいてください。
  - Systemwalkerコンソールでのノード・フォルダの追加、変更、または削除
  - 定義ファイルを使用して各種定義変更処理、および定義変更コマンドの実行
  - ネットワーク管理機能のMIB拡張操作
  - インベントリ収集

  バックアップ時にSystemwalker Operation Managerスケジュールサーバでジョブ/ジョブネットが実行中だった場合、その情報をリストアした際に、実行中だったジョブ/ジョブネットは終了コード239で異常終了になります。
- Systemwalkerマネージャーのログ収集、およびSystemwalkerエージェントのログ収集をスケジュールしているタイミングは避けてください。

- 対象のSystemwalkerマネージャーが冗長構成のサービスプランの場合、バックアップの実施に関して、以下の点に注意してください。

  ー Systemwalkerマネージャーのプライマリノードおよびセカンダリノードの両方が起動している必要があります。
  定常バックアップスケジュール時に片系運用であった場合は、定常バックアップは実行されません。

  ー バックアップの実施時には、内部的にフェイルオーバーを実施します。そのため、バックアップのタイミングでは、Systemwalker Operation Managerスケジュールサーバでのジョブスケジュールは避けてください。
  また、Systemwalkerコンソールの応答が遅延する場合があります。

- フェイルオーバーが発生した場合、ジョブ管理機能のスケジュールサーバのローカルジョブは異常終了します。

  そのため、バックアップのタイミングでは、ジョブ管理機能のスケジュールサーバでのジョブスケジュールは避けるか、スケジュールサーバの異常発生時にも業務を継続できるよう、以下のマニュアルを参照して設計してください。

  ー Systemwalker Operation Manager クラスタ適用ガイド UNIX編

    “ジョブを再起動させる設定”

5.4 統合管理機能の運用を変更する

サービス利用者は、以下の操作により運用を変更できます。

- Systemwalkerクライアントによる操作
- 運用ポータルからのコマンド実行

また、運用変更は、各種申請書を利用してサービス窓口へ依頼することも可能です。

利用できる申請書については、“1.1 各種申請書とは”の“サービス利用開始後の運用変更を依頼する”を参照してください。

ここでは、運用変更をサービス窓口へ依頼する例を紹介します。

なお、これらの運用変更は、Systemwalkerコンソールで行うこともできます。

Systemwalkerコンソールでの操作方法については、以下のマニュアルを参照してください。

- Systemwalker Centric Manager 使用手引書 監視機能編

注意

Systemwalkerクライアントから、以下の操作は行わないでください。

- Systemwalkerマネージャーの構成変更や再起動を伴う設定変更（ポリシー配付は除く）
- Systemwalkerマネージャーの定常ログ収集または任意タイミングでのログ収集における、収集対象ログの設定変更(取得要否、取得先、取得量)

5.4.1 イベント監視[監視条件]の監視ポリシーを登録する

イベント監視[監視条件]の監視ポリシーを運用管理サーバに登録します。

1. イベント監視の条件定義出力ファイルなど、「イベント監視[監視条件]の監視ポリシー登録申請」で必要なファイルを作成します。
2. 「イベント監視[監視条件]の監視ポリシー登録申請」に必要な情報を記載します。
3. 作成した「イベント監視[監視条件]の監視ポリシー登録申請」をサービス窓口に提出します。

   「イベント監視[監視条件]の監視ポリシー登録申請」がサービス窓口で受理されると、受理完了の通知がされます。
4. 監視ポリシー登録が実施されると、サービス窓口から監視ポリシー登録通知が通知されます。

5.4.2 アプリケーション情報を登録する

アプリケーション情報を運用管理サーバに登録します。

1. アプリケーション情報ファイルなど、「CSVファイルからのアプリケーション情報移入申請」で必要なファイルを作成します。
2. 「CSVファイルからのアプリケーション情報移入申請」に必要な情報を記載します。
3. 作成した「CSVファイルからのアプリケーション情報移入申請」をサービス窓口に提出します。

   「CSVファイルからのアプリケーション情報移入申請」がサービス窓口で受理されると、受理完了の通知がされます。
4. アプリケーション情報の登録が実施されると、サービス窓口からアプリケーション情報登録通知が通知されます。

5.5 ジョブ管理機能の運用を変更する

サービス利用者は、以下の操作により運用を変更できます。

- Systemwalkerクライアントによる操作
- 運用ポータルからのコマンド実行
- ファイルサーバーからのローカルジョブ用スクリプトの操作

ここでは、上記の操作の一部について紹介します。

注意

Systemwalker クライアントから、以下の操作は行わないでください。

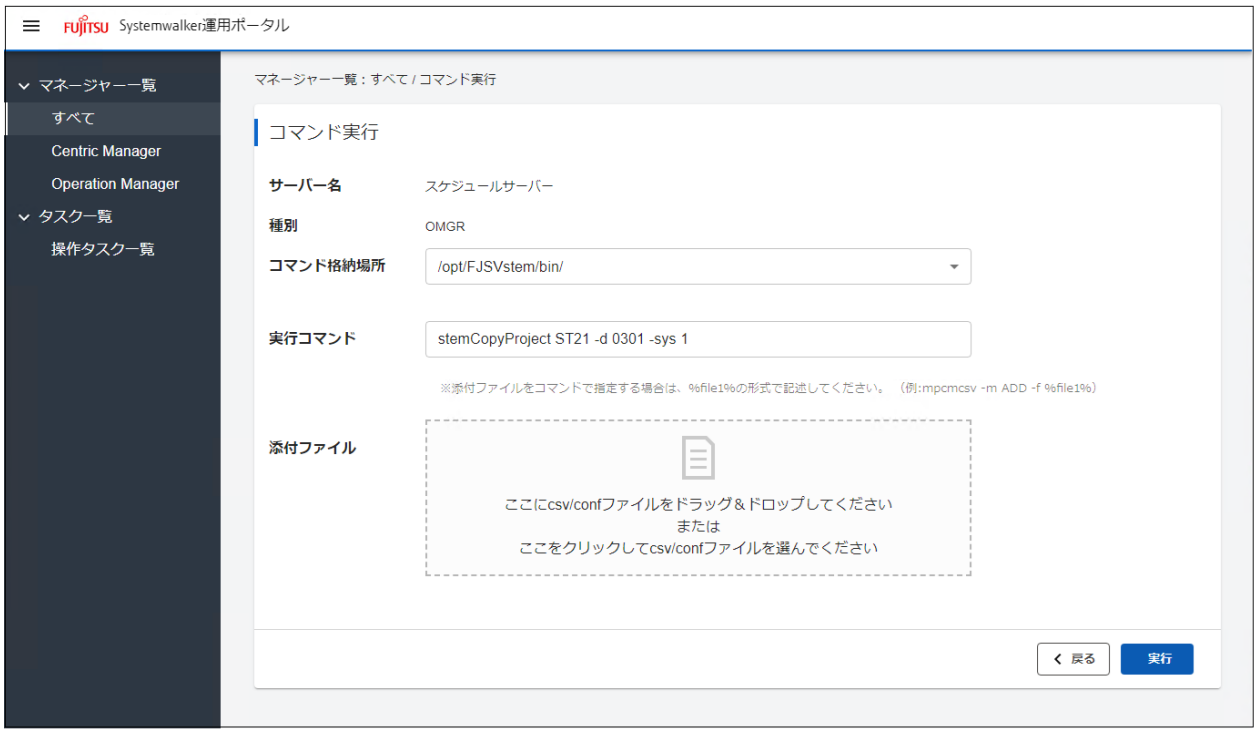
- Systemwalkerマネージャーの再起動が必要となる設定変更および再起動操作
- Systemwalkerマネージャーの定常ログ収集または任意タイミングでのログ収集における、収集対象ログの設定変更(取得要否、取得先、取得量)

5.5.1 マスタスケジュール管理を変更する

運用ポータルから、Systemwalker Operation Managerのマスタスケジュール管理の変更を実施してください。

1. 運用ポータルの[マネージャー一覧]画面で、マスタスケジュールの運用を変更するマネージャーの[操作]メニューから[コマンド操作]をクリックします。

2. 表示された運用ポータルの[コマンド実行]画面で、以下を実施してください。



   a. 以下を指定します。

      コマンド格納場所: /opt/FJSVstem/bin/

      実行コマンド: stemCopyProject プロジェクト名 -d リリース日 -sys サブシステム番号

   b. [実行]ボタンをクリックします。

3. 運用ポータルの[操作タスク一覧]画面で、実施した操作が「Finished」となったことを確認します。
4. クライアントを起動し、[Systemwalker Operation Manager]ウィンドウからマスタスケジュール管理の運用が変更されたことを確認します。

以下のマニュアルを参照してください。

- Systemwalker Operation Manager マスタスケジュール管理ユーザーズガイド
- Systemwalker Operation Manager リファレンス集

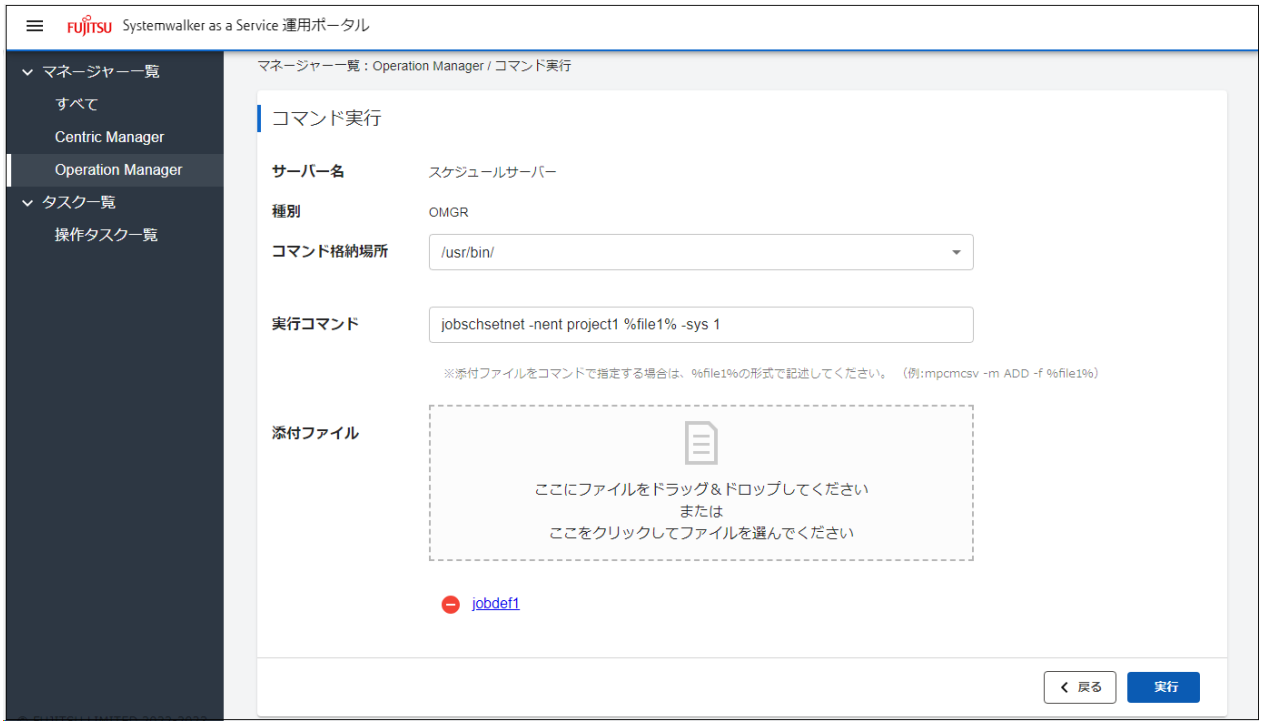
  “stemCopyProject 運用変更事前設定コマンド”

5.5.2　ジョブネットを設定する

Systemwalker Operation Managerのジョブネットを、コマンドを使用して設定する場合、運用ポータルから操作を実施してください。

1. 運用ポータルの[マネージャー一覧]画面で、ジョブネットを設定するマネージャーの[操作]メニューから[コマンド操作]をクリックします。

2. 表示された運用ポータルの[コマンド実行]画面で、以下を実施してください（ジョブネットを登録する場合の例）。



   a. 以下を指定します。

      コマンド格納場所: /usr/bin/

      実行コマンド: jobschsetnet -nent プロジェクト名 %file1% -sys サブシステム番号

   b. [添付ファイル]欄に作成した定義ファイルを添付します。

   c. [実行]ボタンをクリックします。

3. 運用ポータルの[操作タスク一覧]画面で、実施した操作が「Finished」となったことを確認します。

4. Systemwalker Operation Managerクライアントを起動し、ジョブネットが設定されたことを確認します。

以下のマニュアルを参照してください。

- Systemwalker Operation Manager リファレンス集

  “jobschsetnetコマンド”

5.5.3　ローカルジョブ用スクリプトを管理する

Systemwalker Operation Managerのジョブネット間を連携するスクリプトの管理は、ファイルサーバーから実施できます。

ファイルサーバーの操作例については、“付録C ファイルサーバーでのファイル配置方法”を参照してください。

第6章 運用作業を実施する

本章では、サービス利用者が運用作業を実施する手順について説明します。

6.1 Systemwalkerマネージャーのログを確認する

Systemwalkerマネージャーのログを確認する手順について説明します。

Systemwalkerマネージャーのログはファイルサーバーから取得します。

ファイルサーバーからのログの参照方法については、“付録D ファイルサーバーでのログ参照方法”を参照してください。

注意

対象のSystemwalkerマネージャーが冗長構成のサービスプランの場合、ログ収集に関して、以下の点に注意してください。

- 申請されたSystemwalkerマネージャーのログは、プライマリノードおよびセカンダリノードごとに収集されます。
- ログ収集を実施する際には、Systemwalkerマネージャーのプライマリノードとセカンダリノードの両方が起動している必要があります。
  ログ収集時に片系運用であった場合は、ログ収集は実行されません。

6.2 Systemwalkerエージェントのログを確認する

Systemwalkerエージェントのログを確認する手順について説明します。

Systemwalkerエージェントのログはファイルサーバーから取得します。

ファイルサーバーからのログの参照方法については、“付録D ファイルサーバーでのログ参照方法”を参照してください。

注意

- Systemwalkerエージェントのログ（Systemwalker Centric Manager業務サーバ、Systemwalker Operation Manager実行サーバ）は、監視しているSystemwalker Centric Manager運用管理サーバのログに含まれます。
  Systemwalker エージェントのログは、統合管理機能の監査ログ管理機能が提供する機能を使用して収集しています。
  そのため、ログの収集範囲は、当該Systemwalkerエージェントに対して前回実行したログ収集、または任意タイミングでのログ収集で収集したログ以降となる場合があります。
  必要に応じて、前回以前に収集したログとあわせて確認する必要があります。
  統合管理機能の監査ログ管理機能については、以下のマニュアルを参照してください。

  ー Systemwalker Centric Manager 使用手引書 セキュリティ編

    “監査ログを管理する”

- 対象のSystemwalkerマネージャーが冗長構成のサービスプランの場合、ログ収集を行うには、Systemwalkerマネージャーのプライマリノードおよびセカンダリノードの両方が起動している必要があります。
  片系運用中にログ収集を実施した場合は、ログ収集は実行されませんので、注意してください。

6.3 任意タイミングでログを取得する

SystemwalkerマネージャーおよびSystemwalkerエージェントのログは、任意のタイミングで収集できます。

1. 「任意タイミングでのログ収集申請」に必要な情報を記載します。

   収集対象となるSystemwalkerマネージャーおよびSystemwalker エージェントを記載します。

2. 作成した「任意タイミングでのログ収集申請」をサービス窓口に提出します。

   「任意タイミングでのログ収集申請」がサービス窓口で受理されると、サービス窓口から受理完了が通知されます。

3. 指定した日時でログ収集するよう設定されると、サービス窓口から設定完了が通知されます。その後、指定した日時にログ収集が実施され、対象のログをファイルサーバーから取得できます。

   ファイルサーバーからのログの参照方法については、“付録D ファイルサーバーでのログ参照方法”を参照してください。

注意

- Systemwalkerエージェントのログ（Systemwalker Centric Manager業務サーバ、Systemwalker Operation Manager実行サーバ）は、監視しているSystemwalker Centric Manager運用管理サーバのログに含まれます。

  Systemwalkerエージェントのログは、統合管理機能の監査ログ管理機能が提供する機能を使用して収集しています。そのため、ログの収集範囲は、当該Systemwalkerエージェントに対して前回実行したログ収集、または任意タイミングでのログ収集したログ以降となる場合があります。

  必要に応じて、前回以前に収集したログとあわせて確認する必要があります。

  統合管理機能の監査ログ管理機能については、以下のマニュアルを参照してください。

  ー Systemwalker Centric Manager 使用手引書 セキュリティ編

    “監査ログを管理する”

- 収集時刻については、“Systemwalkerマネージャーのログ収集設定を変更する”における“マネージャーログ定期収集設定申請”で設定した時刻の前後2時間を含めないようにしてください。
- 対象のSystemwalkerマネージャーが冗長構成のサービスプランの場合、ログ収集に関して、以下の点に注意してください。

  ー 申請されたSystemwalkerマネージャーのログは、プライマリノードおよびセカンダリノードごとに収集されます。このとき、Systemwalkerエージェントのログは、プライマリノードのSystemwalker Centric Manager運用管理サーバのログに含まれます。

  ー Systemwalkerマネージャーのプライマリノードおよびセカンダリノードの両方が起動している必要があります。片系運用中にログ収集を実施した場合、ログ収集されませんので、注意してください。

6.4 任意タイミングでSystemwalkerマネージャーのバックアップをする

任意のタイミングで、Systemwalkerマネージャーのバックアップをする手順について説明します。

1. 「任意バックアップ申請」に必要な情報を記載します。
2. 作成した「任意バックアップ申請」をサービス窓口に提出します。

   「任意バックアップ申請」がサービス窓口で受理されると、サービス窓口から受理完了が通知されます。
3. 指定した日時でバックアップするよう設定されると、サービス窓口から設定完了が通知されます。

   その後、指定した日時にバックアップが実施されます。

ポイント

- Systemwalkerマネージャーのリストアために、バックアップを実施しています。
  リストアを実施したい場合は、サービス窓口にご連絡ください。
- 統合管理機能をリストアする場合は、関連するSystemwalkerマネージャー（全体監視サーバ、運用管理サーバ、部門管理サーバ）がすべてリストアされます。また、Systemwalkerマネージャーのバックアップは、Systemwalker Centric Managerのmpbkc（バックアップコマンド）とSystemwalker Operation Managerのmpbko（バックアップコマンド）を使用しています。バックアップ対象範囲は、オンラインバックアップを行った場合と同様になります。

注意

- 定常バックアップ実行中は、任意バックアップを実行できません。また、サービス内で同時に複数実行することはできません。
  任意のバックアップのタイミング検討時には、“定常バックアップ設定申請”で定常バックアップタイミングを確認してください。
- バックアップの実施時期は、Systemwalkerマネージャーが日替わり処理などの高負荷な処理を実行している時間を避けて申請してください。
  バックアップ実行中は、Systemwalkerコンソールから以下の操作を行わないでください。
  - 監視ポリシーの変更

    未配付の監視ポリシーが残っている場合には、事前に監視ポリシー配付を済ませておいてください。
  - Systemwalkerコンソールでのノード・フォルダの追加／変更／削除
  - 定義ファイルを使用して各種定義変更処理、および、定義変更コマンドの実行
  - ネットワーク管理機能のMIB拡張操作
  - インベントリ収集

  バックアップ時にSystemwalker Operation Managerスケジュールサーバで、ジョブ/ジョブネットが実行中だった場合、その情報をリストアした際に、実行中だったジョブ/ジョブネットは終了コード239で異常終了になります。
- Systemwalkerマネージャーのログ収集、およびSystemwalkerエージェントのログ収集をスケジュールしているタイミングは避けてください。
- 対象のSystemwalkerマネージャーが冗長構成のサービスプランの場合、バックアップの実施に関して、以下の点に注意してください。
  - Systemwalkerマネージャーのプライマリノードおよびセカンダリノードの両方が起動している必要があります。
    定常バックアップスケジュール時に片系運用であった場合は、定常バックアップは実行されません。
  - バックアップの実施時には、内部的にフェイルオーバーが発生します。そのため、バックアップのタイミングでは、Systemwalker Operation Managerスケジュールサーバでのジョブスケジュールは避けてください。
    また、Systemwalkerコンソールの応答が遅延する場合があります。
- フェイルオーバーが発生した場合、ジョブ管理機能のスケジュールサーバのローカルジョブは異常終了します。

  そのため、バックアップのタイミングでは、ジョブ管理機能のスケジュールサーバでのジョブスケジュールは避けていただくか、スケジュールサーバの異常発生時にも業務を継続できるよう、以下のマニュアルを参照して設計してください。
  - Systemwalker Operation Manager クラスタ適用ガイド UNIX編

    “ジョブを再起動させる設定”

6.5 フェイルオーバーを実施する

Systemwalkerマネージャーをフェイルオーバーする手順について説明します。

なお、本申請は、対象のSystemwalkerマネージャーが冗長構成のサービスプランの場合、申請可能です。

Systemwalker Centric ManagerおよびSystemwalker Operation Managerのマニュアルにおいて、運用作業中のフェイルオーバーが必要となる場合、Systemwalker as a Serviceではフェイルオーバー申請により、Systemwalkerマネージャーをフェイルオーバーできます。

Systemwalkerエージェントの追加など、Systemwalkerマネージャーのプライマリノードとセカンダリノードで情報の整合性を取る必要がある場合に行います。

1. 対象となるSystemwalkerマネージャーに対して「フェイルオーバー申請」を記載します。
2. 「フェイルオーバー申請」をサービス窓口に提出します。

   「フェイルオーバー申請」がサービス窓口で受理されると、受理完了時にフェイルオーバー実施日時が通知されます。

フェイルオーバー実施日時に問題がある場合は、再調整通知がサービス窓口から通知されます。

通知内容を確認のうえ、実施日程を変更してサービス窓口に申請します。

3. この時点で、対象となるSystemwalkerマネージャーはプライマリノードが運用系になっています。この状態で必要な作業を実施します。

   サービス窓口から通知されたフェイルオーバー実施日時までに作業を完了してください。

   実施日時に問題がある場合は、サービス窓口に再調整依頼を申請し、実施日程の調整を実施してください。

4. フェイルオーバー実施日時にフェイルオーバーが行われます。

   フェイルオーバー完了後、サービス窓口からフェイルオーバー完了通知が通知されます。

5. この時点で、対象となるSystemwalkerマネージャーはセカンダリノードが運用系になっています。この状態で必要な作業を実施します。

6. 作業完了後、フェイルバック依頼通知をサービス窓口に申請します。

   フェイルバックが完了すると、サービス窓口からフェイルバック完了通知が通知されます。

6.6 統合管理機能のWeb APIを発行する

統合管理機能のWeb APIを発行して、Systemwalker Centric ManagerのAPIを実行する手順を説明します。

1. OAuth認証情報を発行します。

   本操作は、初回実行時のみ必要です。運用ポータルのユーザーで操作します。

   a. Webブラウザで管理ポータルにアクセスし、ログインします。

      ```
      https://portal.aispf.global.fujitsu.com/#/systemwalker-service
      ```

   b. 左メニューから[API認証情報と利用者管理]をクリックします。

   c. グループ一覧から、[Systemwalker as a Service]が利用するサービスとして設定されているいずれかのユーザーグループをクリックします。

   d. [認証情報]タブをクリックします。

   e. [APIご使用にあたって]のリンク先の手順における[OAuth 2.0を使用する場合]に沿って、Client IDとClient Secretを新規作成します。

   注意

   OAuth2.0以外の認証方式もありますが、Systemwalker as a Serviceではセキュリティⅰ強度の高いOAuth2.0のみサポートします。

2. Client IDとClient Secretを使って、アクセストークンを取得します。

   [APIご使用にあたって]のリンク先手順における[OAuth 2.0を使用する場合]に沿って、アクセストークンを取得します。

   リンク先手順はGUIですが、CLIやプログラムでトークンを取得することもできます。詳細は、上記リンク先に記載されている[API認証 APIリファレンス]を参照してください。

3. 手順2.で取得したアクセストークンを使用して、統合管理機能のWeb APIを発行します。

   Web APIの詳細は“付録F APIリファレンス”を参照してください。

ポイント

アクセストークンの有効期限は1時間です。継続的に本Web APIを発行する際は、アクセストークンをキャッシュし、有効期限内は再利用してください。

Client Secretおよびアクセストークンは、機密情報にあたります。取得したこれらの情報は、利用者の責任で適切に管理してください。

第7章 Disaster RecoveryによりSystemwalker as a Serviceを切り替える

本章では、Disaster RecoveryにおけるSystemwalker as a Serviceのリージョン切り替えのための準備・手順について説明します。

7.1 Disaster Recoveryの事前準備をする

平常時から以下の準備を実施します。

1. 西日本リージョンにおいて、サービスと接続するための業務環境の仮想ネットワークを設計・構築します。

   Azure仮想ネットワーク(Azure Virtual Network)の設計・構築については“2.1.2 サービス接続用仮想ネットワークを設計・構築する”を参照してください。

   業務環境とSystemwalker as a Serviceの接続方法には、以下の2通りがあります。

   - 同一リージョン構成

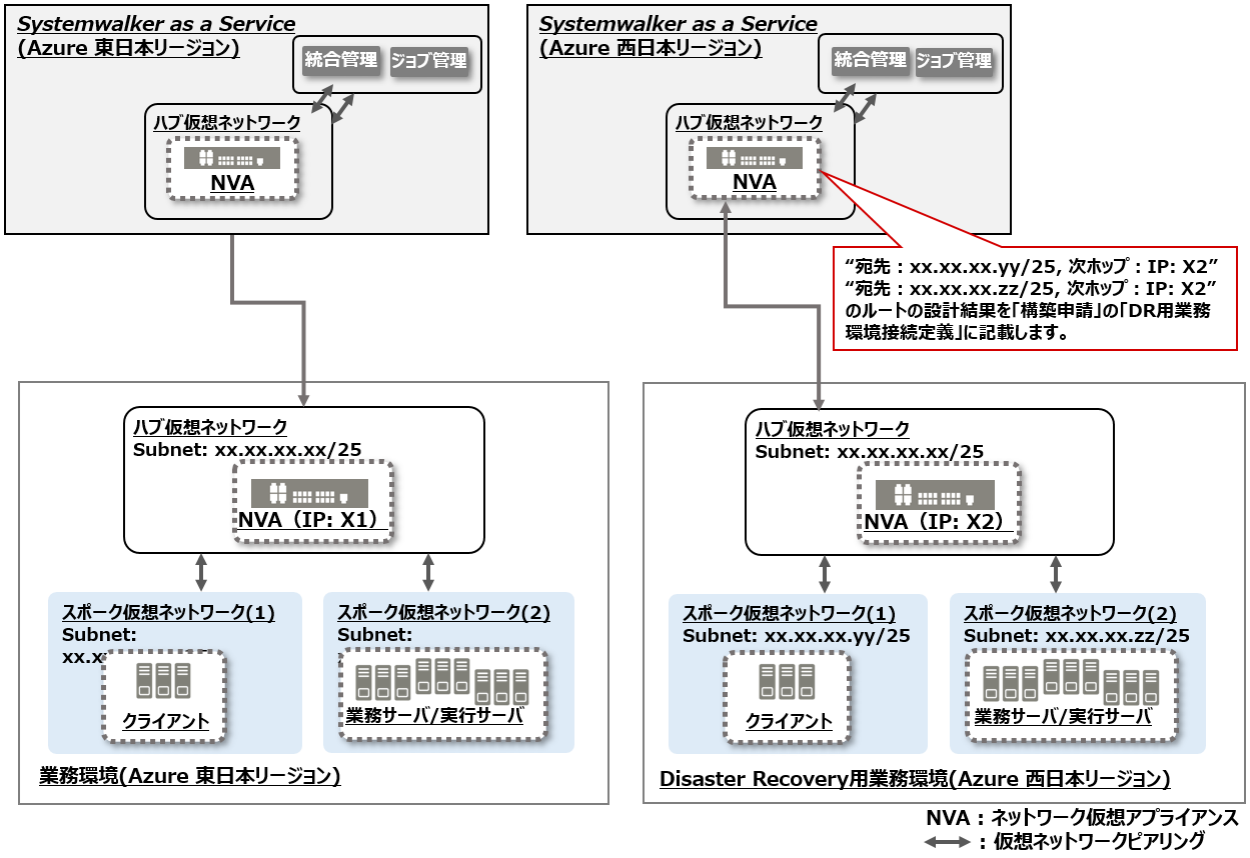
     Systemwalker as a Serviceと同一のリージョンに業務環境を稼働する構成です。

   - 可変リージョン構成

     Systemwalker as a Serviceの稼働リージョンに依存せず業務環境を稼働する構成です。
     Systemwalker as a Serviceと異なるリージョンでも、業務環境を稼働させることが可能です。

   以下に、ルートテーブルの設計例を示します。

   Disaster Recovery用のルートテーブルの設計が必要な構成例



2. 西日本リージョンで動作するサービスの仮想ネットワークと業務環境の仮想ネットワークとのピアリングを設定するためのアカウントを設計・作成します。

   “2.1.3 仮想ネットワークピアリング設定用アカウントを設計・作成する”を参照してください。

3. 2.で設計・作成したアカウントの設定を実施します。

   “2.2.2 仮想ネットワークピアリング設定用アカウントの設定を実施する”を参照してください

4. 西日本リージョンで動作するサービスの仮想ネットワークと、業務環境の仮想ネットワークを接続します。

   “2.3.1 サービスに接続する”を実施してください。

5. Systemwalkerマネージャーにリストアするデータを定期収集するために、Systemwalkerマネージャーの定常バックアップを設定します。

   “5.3 定常バックアップのタイミングを変更する”を参照してください。

ポイント

サービス窓口より災害復旧後の切り戻しの連絡があった場合、切り戻し日時に合わせ、Systemwalkerマネージャーの任意バックアップを設定しておきます。
詳細は、“6.4 任意タイミングでSystemwalkerマネージャーのバックアップをする”を参照してください。

7.2 Disaster Recoveryを実施する

Systemwalker as a Serviceにて、サービスの稼働拠点を東日本リージョンから西日本リージョンへ切り替えます。または、西日本リージョンから東日本リージョンへ切り替え(切り戻し)ます。

この際、サービス利用者は、以下の作業を実施します。なお、同一リージョン構成の場合、業務環境のリージョン切り替えも実施してください。

7.2.1 サービスから切り替え開始通知を受領する

サービス窓口から切り替え開始の通知、および以下の情報を受領します。

- サービス側のネットワーク仮想アプライアンス（NVA）のIPアドレス

  事前に通知したIPアドレスから変更がある場合のみ通知されます。
  その場合、“7.2.3 サービスに接続する”で使用します。

7.2.2 サービスから切り替え完了通知を受領する

サービス窓口から切り替え完了通知を受領します。また、通知に従い、以下の情報を契約しているオプションに応じて確認してください。

- 強制停止したジョブネットの一覧（存在する場合のみ）
- ローカルジョブ用スクリプトのデータ領域がいつ時点のデータで復旧したか
- Systemwalkerマネージャーがいつ時点のデータで復旧したか

統合管理機能やジョブ管理機能の設定の確認や更新など、必要に応じて運用再開に向けた対応を行ってください。

切り替え完了通知後も、24時間程度を目安として、サービス内部での切り替え処理を継続して実施しています。
そのため、それらの処理に伴い、発生したSystemwalkerマネージャーのイベントが、統合管理機能のSystemwalkerコンソールに通知されることがあります。

7.2.3　サービスに接続する

“7.2.1 サービスから切り替え開始通知を受領する”で受領したサービス側のNVAのIPアドレスが、切り替え前から変更されていた場合は、および可変リージョン構成においてサービス側のみリージョンが切り替えられた場合は、業務環境のルートテーブルを更新してください。

ルートテーブルの更新については、“2.3.1 サービスに接続する”の手順2を参照ください。

7.2.4　運用再開準備をする

リージョン切り替え後、運用を再開するための準備作業について説明します。

1）統合管理機能の運用準備

運用管理サーバ配下に業務環境の部門管理サーバが存在する場合、その運用管理サーバに対して、以下を実施します。

1. **構成情報配付**
    a. 運用ポータルの[マネージャー一覧]画面で、対象の運用管理サーバの[操作]メニューから表示される[コマンド操作]をクリックします。
    b. 表示された運用ポータルの[コマンド実行]画面で、以下を実施します。
        1. 以下を指定します。
            コマンド格納場所: /opt/systemwalker/bin/
            実行コマンド: mpdrpspa.sh all
        2. [実行]ボタンをクリックします。
    c. 運用ポータルの[操作タスク一覧]画面で、実施した操作が「Finished」となったことを確認します。
    d. その操作の[タスク詳細]画面における[コマンド出力]欄に以下のメッセージが出力されていないことを確認します。

```
Policy distribution error.
```

2. **ネットワーク管理ポリシー反映**
    a. 運用ポータルの[マネージャー一覧]画面で、対象の運用管理サーバの[操作]メニューから表示される[コマンド操作]をクリックします。
    b. 表示された運用ポータルの[コマンド実行]画面で、以下を実施します。
        1. 以下を指定します。
            コマンド格納場所: /opt/systemwalker/bin/
            実行コマンド: mpnmpref
        2. [実行]ボタンをクリックします。
    c. 運用ポータルの[操作タスク一覧]画面で、実施した操作が「Finished」となったことを確認します。

2）ジョブ管理機能の運用準備

切り替え時にジョブネットはすべて無効化されています。必要に応じてジョブネットを有効化してください。

付録A　ファイルサーバーユーザー用のキーペアの発行方法

ファイルサーバーに安全にログインするためには、キーペア（公開鍵と秘密鍵）が必要です。以下の手順でキーペアを発行します。

1. SFTPクライアントにログインします。
2. 以下のコマンドを実行し、ファイルサーバーユーザー用のキーペアを発行します。

```
$ ssh-keygen -t <暗号化アルゴリズム> -b <ビット数>
```

カレントディレクトリに作成される、(3)公開鍵ファイル(sw-sftpuser.pub)を「ユーザー設定申請」に添付して提出します。

(1)パスフレーズおよび(2)秘密鍵ファイル(sw-sftpuser)は、“2.4.4 ファイルサーバーにログインする”で利用します。

コマンド実行例

```
$ ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/home/testuser/.ssh/id_rsa): sw-sftpuser ※ファイルサーバーユーザー名
Enter passphrase (empty for no passphrase): <パスフレーズ>    ・・・(1)
Enter same passphrase again: <パスフレーズ>     ・・・・・・・・・・(1)
Your identification has been saved in sw-sftpuser.    ・・・・・・・(2)
Your public key has been saved in sw-sftpuser.pub.    ・・・・・・・(3)
The key fingerprint is:
SHA256:JxGRzcU/a1rZpyrOQIcdAFf9hm+Rkb7OXXdxrryXXXX testuser@testserver
The key's randomart image is:
+---[RSA 4096]----+
|      ..=*.+.  . |
|       ..oo o o  |
|        . .  = o |
|         + .. O..|
|        S +  o Oo|
|       . +    O B|
|        . E  X +=|
|         +. o B .|
|        .o++oo.. |
+----[SHA256]-----+
```



注意

- 暗号化アルゴリズムは利用者側で選定してください。
- パスフレーズは必ず設定してください。パスフレーズの要件として、以下を推奨します。
  - 文字列長：10文字以上
  - 文字種：英字、数字、記号の3種を含む

付録B　ファイルサーバーへのログイン方法

以下の手順で、ファイルサーバーへログインします。

1. SFTPクライアントにログインします。

2. SFTPでファイルサーバーに接続します。

```
$ sftp -i 〈秘密鍵〉〈ファイルサーバーユーザー〉@〈ファイルサーバーのIPアドレス〉
```

付録C　ファイルサーバーでのファイル配置方法

以下の手順で、ファイルサーバーにファイルをアップロードします。

ファイルアップロード

1. “付録B ファイルサーバーへのログイン方法”を参照して、ファイルサーバーにログインします。
2. ファイルサーバーにファイルをアップロードします。

```
sftp> put <アップロードするファイル> <アップロード先のディレクトリ>
```

コマンド実行例

```
$ sftp -i id_rsa  testuser@192.0.2.16
Enter passphrase for key 'id_rsa':
Connected to 192.0.2.16.
sftp> ls /honban-unyokanri002/mhlw/
sftp> put test-file /honban-unyokanri002/mhlw/
Uploading test-file to /honban-unyokanri002/mhlw/test-file
test-file                100%    3     1.9KB/s   00:00
sftp> ls /honban-unyokanri002/mhlw/
/honban-unyokanri002/mhlw/test-file
```

付録D　ファイルサーバーでのログ参照方法

以下の手順で、ファイルサーバーからログファイルをダウンロードします。

ログダウンロード

1. “付録B ファイルサーバーへのログイン方法”を参照して、ファイルサーバーにログインします。
2. ファイルサーバー上のログの一覧を確認します。

```
sftp> ls <ログ格納ディレクトリ>
```

3. ファイルサーバーからログをダウンロードします。

```
sftp> get <ログ格納ディレクトリ>/<ログファイル>
```

4. ダウンロードしたログを解凍します。

コマンド実行例

```
$ sftp -i id_rsa testuser@192.0.2.16
Enter passphrase for key 'id_rsa':
Connected to 192.0.2.16.
sftp> ls logs/honban-unyokanri001-1/CLOGCMGRhonban-unyokanri001-1
2024-02-27235508CLOGChonban-unyokanri001-1.tar.gz          2024-02-28143713CLOGChonban-unyokanri001-1.tar.gz
sftp> get logs/honban-unyokanri001-1/CLOGCMGRhonban-unyokanri001-1/2024-02-27235508CLOGChonban-unyokanri001-1.tar.gz
Fetching /logs/honban-unyokanri001-1/CLOGCMGRhonban-unyokanri001-1/2024-02-27235508CLOGChonban-unyokanri001-1.tar.gz to
2024-02-27235508CLOGChonban-unyokanri001-1.tar.gz
 /logs/honban-unyokanri001-1/CLOGCMGRhonban-unyokanri001-1/2024-02-27235508CLOGChonban-unyokanri001-1.tar.gz  100%
178KB   3.1MB/s   00:00
sftp> exit
$ tar -zxvf 2024-02-27235508CLOGChonban-unyokanri001-1.tar.gz
```

付録E　仮想ネットワークピアリングの設定方法

以下の手順で、仮想ネットワークピアリングを設定します。

事前準備

1. インターネットにアクセス可能なサーバーにログインします。
2. Azureコマンドラインインターフェース（CLI）をインストールします。
3. Azureにログインします。

```
$ az login --tenant <お客様Azure環境のテナントID>
$ az login --tenant <“サービス環境情報”に記載のテナントID>
```

ピアリング設定

以下のコマンドを実行します。

```
$ az network vnet peering create --name <ピアリング名> --remote-vnet <“サービス環境情報”に記載の仮想ネットワークID> --subscription <“2.1.2 サービス接続用仮想ネットワークを設計・構築する”で作成した仮想ネットワークのサブスクリプションID> --resource-group <“2.1.2 サービス接続用仮想ネットワークを設計・構築する”で作成した仮想ネットワークのリソースグループ名> --vnet-name <“2.1.2 サービス接続用仮想ネットワークを設計・構築する”で作成した仮想ネットワーク名> --allow-forwarded-traffic yes --allow-vnet-access
```

事後作業

Azureからログアウトします。

```
$ az logout
```

付録F　APIリファレンス

統合管理機能のWeb APIでは、HTTPリクエストを送信することで、Systemwalker Centric ManagerのAPIを実行し、その結果をHTTPレスポンスで受け取ることができます。

リクエスト形式は、以下のとおりです。

- リクエストおよびレスポンスのデータフォーマットは、JSONを使用します。
- 文字コードは、UTF-8を使用します。
- HTTPプロトコルは、バージョン HTTP/1.1を使用します

F.1　change-event-stat

機能説明

Systemwalker Centric Managerの監視イベントのAPIを実行し、全体監視サーバおよび運用管理サーバの監視イベントの対処を行います。

1リクエストにて、Mp_OpenEventStat（）関数、Mp_ChangeEventStat（）関数、Mp_CloseEventStat（）関数を実行します。Mp_ChangeEventStat（）関数は、複数イベントに対して実行できます。

リクエスト

エンドポイント

```
https://<操作対象の運用管理サーバまたは全体監視サーバのホスト名
```

対象のSystemwalkerマネージャーがクラスタ構成の場合、論理ホスト名を指定してください。

リクエストURI

```
/v1/cmgr/api/change-event-stat
```

HTTPメソッド

POST

リクエストヘッダ

```
Content-Type: application/json
Accept: application/json
X-Access-Token:<アクセストークン>
```

リクエストボディ

```
{
     "event_stat":[
         <イベント1に対するMp_ChangeEventStat（）関数の入力のJSON>,
         <イベント2に対するMp_ChangeEventStat（）関数の入力のJSON>,
           :
     ]
}
```

Mp_ChangeEventStat（）関数の入力のJSON

```
{
    "hisnum":<数値>,
```

```
    "keydata":<MPOPCESKEY構造体のJSON>,
    "status": "<文字列>",
    "dealer": "<文字列>",
    "memo":"<文字列>",
    "chgflag":"<文字列>"
}
```

MPOPCESKEY構造体のJSON

```
{
    "nodename": "<文字列>",
    "timerec" :<数値>,
    "eventtext":"<文字列>"
}
または null
```

- 各keyは、UNIX版のMp_ChangeEventStat（）関数のパラメーターに相当します。

  ー "status"、"chgflag"以外

  上記JSONで指定された値がMp_ChangeEventStat（）関数に入力されるため、Mp_ChangeEventStat（）関数のパラメーターとして適切な値を指定してください。

  MPOP_NODENAMELEN=128、MPOP_EVENTLEN=2047です。

  ー "status"

  以下のいずれかの文字列を指定してください。
  それぞれの意味は、Mp_ChangeEventStat（）関数のパラメーターと同一です。

  - "MPOP_CES_DEFEVT"
  - "MPOP_CES_FIXEVT"
  - "MPOP_CES_REPEVT"

  ー "chgflag"

  以下の文字列を任意に組み合わせて指定してください。
  それぞれの意味は、Mp_ChangeEventStat（）関数のパラメーターと同一です。

  - "MPOP_CES_STATUS"
  - "MPOP_CES_DEALER"
  - "MPOP_CES_MEMO"
  - "MPOP_CES_ALL"

  組み合わせる場合は、カンマで区切ってください。

  例)

```
"chgflag": "MPOP_CES_STATUS,MPOP_CES_MEMO"
```

- すべてのkeyは指定必須です。nullを指定したい場合は、JSONにおいて明にnullを指定します。
- 指定可能なイベント数の上限は100件です。

レスポンス

ステータスコード

以下のステータスコードを返却します。

コード	説明
200	リクエストボディに指定された各イベントに対する処理を実施しました。 詳細な結果は、レスポンスボディを参照してください。

コード	説明
400	リクエストパラメーターに誤りがあります。以下の誤りがないか、入力内容を見直してください。 ・ リクエストヘッダに誤りがあります。 ・ リクエストボディが{"event_stat": [{…}, {…},…]}のJSON形式でありません。 ・ リクエストボディに上限値100件を超過した数のイベントが指定されています。 ・ 対象のSystemwalkerマネージャーがクラスタ構成の場合で、エンドポイントに待機系のホスト名が指定されています。
401	認証情報の指定に誤りがあります（トークンの期限切れも含む）。入力内容を見直してください。
404	エンドポイントまたはリクエストURIに誤りがあります。入力内容を見直してください。
405	メソッドの指定に誤りがあります。POSTを指定してください。
409	すでに実行中です。同時に実行しないでください。3秒ほど待ってから、再度実行してください。
413	想定外のデータ量が送信されています。入力内容を見直してください。
429	短時間で実行し過ぎています。3秒ほど待ってから、再度実行してください。
500	一時的なシステム高負荷、内部エラー、またはクラスタの系切り替えのために、短期的な不通が発生しています。しばらく時間をおいて再度実行してください。それでも改善しない場合は、技術員に連絡してください。

レスポンスボディ（上記のコードが200の場合）

```
{
    ”event_stat”:[
        〈イベント1に対する処理結果のJSON〉,
        〈イベント2に対する処理結果のJSON〉,
         :
    ]
}
```

処理結果のJSON

```
{
   ”code”:〈数値〉,
   ”msg”:”〈詳細〉”,
   〈対象イベントの識別情報〉
}
```

- <対象イベントの識別情報>は、以下の形式でリクエストボディに指定した値がそのまま表示されます。

```
”hisnum”:〈数値〉, ”keydata”:〈MPOPCESKEY構造体のJSON〉
```

- codeおよびmsgは、以下のとおりです。

code	msg	説明
0	null	正常終了。
1～4	null	Mp_ChangeEventStat（）関数の復帰値に相当します。入力内容を見直してください。
5	"Invalid key. <key名>"	リクエストボディのJSONのkeyにおいて、Mp_ChangeEventStat（）関数の入力として過不足があります。入力内容を見直してください。
	"Invalid value. <key名>"	リクエストボディのJSONのvalueにおいて、Mp_ChangeEventStat（）関数の入力として不正な値が指定されています。入力内容を見直してください。

code	msg	説明
-2～-1	null	Mp_ChangeEventStat（）関数の復帰値に相当します。しばらく時間をおいて再度実行してください。それでも改善しない場合は、技術員に連絡してください。

注意

- 本Web APIは同期処理です。内部状態によっては処理に時間がかかる可能性がありますので、4分を目安として待ち合わせてください。
- サーバごとに1リクエストずつ実行してください。複数リクエストの同時実行はできません。
- 証明書の失効チェックは、無効にしてください。

使用例

curlコマンドによって、2件のイベントを「対処済」に変更する場合

```
curl -i -X POST https://honban-unyokanri001/v1/cmgr/api/change-event-stat -H "Content-Type: application/json" -H "Accept: application/json" -H "X-Access-Token: <アクセストークン>" -d '{"event_stat": [{"hisnum":1000, "keydata":null, "status":"MPOP_CES_FIXEVT", "dealer":"ツールA", "memo":"自動対処", "chgflag":"MPOP_CES_ALL"}, {"hisnum":0, "keydata": {"nodename":"nodeX", "timerec":1675428576, "eventtext":"*xxx errror*"}, "status":"MPOP_CES_FIXEVT", "dealer":"ツールB", "memo":"自動対処", "chgflag":"MPOP_CES_ALL"}]}'
```

ポイント

Windowsのコマンドプロンプトでcurlを使用する場合、証明書の失効チェックを無効にするため、--ssl-no-revokeオプションを指定してください。

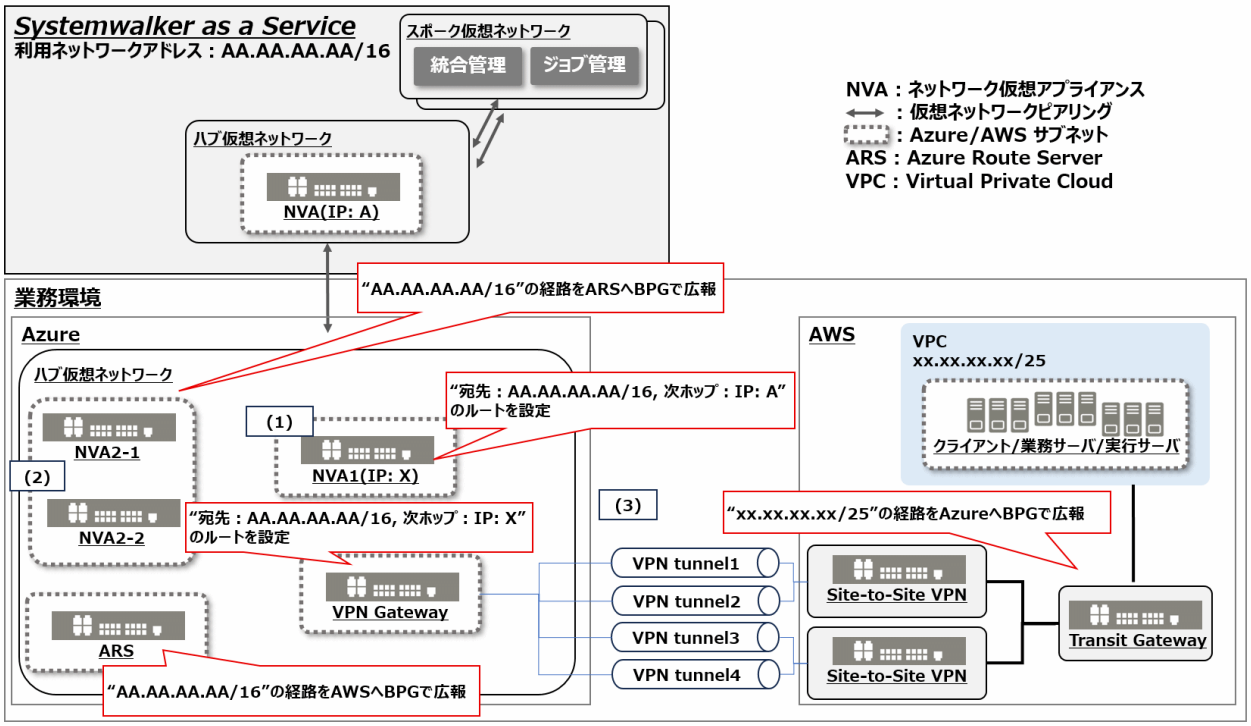
付録G　AWS上の業務環境接続例

Systemwalker as a Serviceへは、業務環境のAzure仮想ネットワークを経由して接続します。

AWS上の業務環境（Systemwalker クライアント、Systemwalker エージェント等）を接続する場合は、VPN等による閉域網を構築し、業務環境の仮想ネットワークを経由して通信できるようにしてください。

なお、通信経路の確保はお客様側の責任となります。

以下に、AWS上の業務環境の接続例を示します。この例では、AWS Site-to-Site VPNを用いて、AzureとAWSをIPsec VPNで接続しています。



(1) Systemwalker as a Serviceとの境界となるルーティング機能を持つアプライアンス：NVA1

例：Azure Firewall

(2) Systemwalker as a Serviceのアドレス空間をBGPでAWS側に広報するためのアプライアンス：NVA2-1、NVA2-2

例：Windows ServerにインストールしたBGPルート交換機能

冗長化のために2台配備し、それぞれでARSとBGPによるルート交換を行います。

BGP（Border Gateway Protocol）：AzureとAWS間で経路交換を行います。

(3) AWSとAzure間を接続するためのIPsec VPNトンネル：VPN tunnel1、VPN tunnel2、VPN tunnel3、VPN tunnel4

高可用性のため、Site-to-Site VPNを冗長構成で配備します。

各Site-to-Site VPNが2つのVPNトンネルを持つため、合計4つのVPNトンネルでAzureとAWS間のデータを送受信します。

詳細は、Azureのドキュメント、AWSのドキュメントを参照してください。