|  |  |  |
| --- | --- | --- |
| ユースケース名 | | セキュリティーグループを管理する |
| 目的（ゴール） | | 仮想マシンの通信制御のために、ポートの開放やアクセス制限などを設定するセキュリティーグループを、ユーザー自身が柔軟に管理できるようにする |
| アクター | | 利用者（ユーザー） |
| 開始条件（起動トリガー) | | ユーザーが仮想マシンのネットワーク設定や通信許可設定を変更・確認要求をだす |
| 事前条件 | | 仮想マシンが少なくとも1台作成されていること |
| 事後条件 | | ユーザーが設定・変更したセキュリティールールが適用され、仮想マシンの通信制御が反映される |
| 拡張点 | |  |
| 関連ユースケース | | ・仮想マシンを作成する  ・仮想ネットワークを構築する |
| イベントフロ｜ | メインフロー | ユーザーが「セキュリティーグループ管理」画面を開く。  現在のセキュリティーグループの一覧が表示される。  ユーザーは既存のグループを選択または新規作成する。  ユーザーは各グループに対して以下のルールを設定できる： 　　- インバウンド／アウトバウンドトラフィック 　　- ポート番号（例：22, 80, 443など） 　　- プロトコル（TCP, UDPなど） 　　- 接続元／接続先IPの指定  設定後、「保存」ボタンを押して反映する。  システムは設定内容を仮想マシンに適用する。  完了メッセージを表示して処理を終了する。 |
| 代替フロー | 3a. ユーザーがセキュリティーグループの削除を選択する： 　a1. グループに紐づいた仮想マシンがないことを確認 　a2. 確認メッセージを表示し、削除処理を行う |
| 例外フロー | 5a. 入力内容に誤り（ポート番号の形式ミス、重複ルールなど）がある場合： 　a1. エラーメッセージを表示し、修正を促す  6a. 仮想マシンへの反映中にエラーが発生した場合： 　a1. エラーメッセージを表示し、再試行または管理者への連絡を促す |
| 備考 | | * セキュリティーグループの設定画面はGUI操作を前提とし、直感的に操作できるインターフェースを提供する。 * 初学者でも操作しやすいように、一般的な設定テンプレートも用意する（例：Web公開用、SSH接続専用など）。 |