自動販売機モデル

開発プロセスについて

- 本ドキュメントで前提している開発プロセスは下記の通りです。
  - MBSEベースでPlantUMLで表現可能なダイアグラムのみで構成しています。
  - 作成、検証はAIを利用することを想定して構成しています。
    - ダイアグラムをPlantUMLに限定したのはAI検証を行う為です。
  - FMEAおよびFTAは、ステートマシン図およびシステム構成図を基に実施したリスク分析であり、初期設計を評価・改善するための後工程です。
    - 分析結果をもとに必要に応じて設計にフィードバックを行います。

各ダイアグラムをPlantUMLで記述することで、AIにより以下の検証支援を想定しています。

一貫性チェック:

- 用語・ID整合性: 要求図、ユースケース図、ユースケース記述、システム構成図、ステートマシン図、用語集 にわたる用語（アクター名、ユースケース名、コンポーネント名、状態名など）及びID（要求ID、ユースケースID等）の表記揺れや不整合を自動検出します。
- 図間整合性:
  - 要求図 で定義された要求と、ユースケース図 でリファインされたユースケース間のトレーサビリティを検証します。
  - ユースケース記述内のフロー（基本フロー、代替フロー、例外フロー） と、対応するアクティビティ図（ユースケース） のステップが整合しているかを確認します。
  - ステートマシン図 で定義された状態やイベントが、関連するユースケース記述やアクティビティ図（機能） と矛盾なく対応しているかを検証します。
  - システム構成図 のコンポーネントと、シーケンス図 のライフラインが一致しているか、またコンポーネント間のメッセージがシステム構成図で示唆されるインターフェースと整合しているかを確認します。

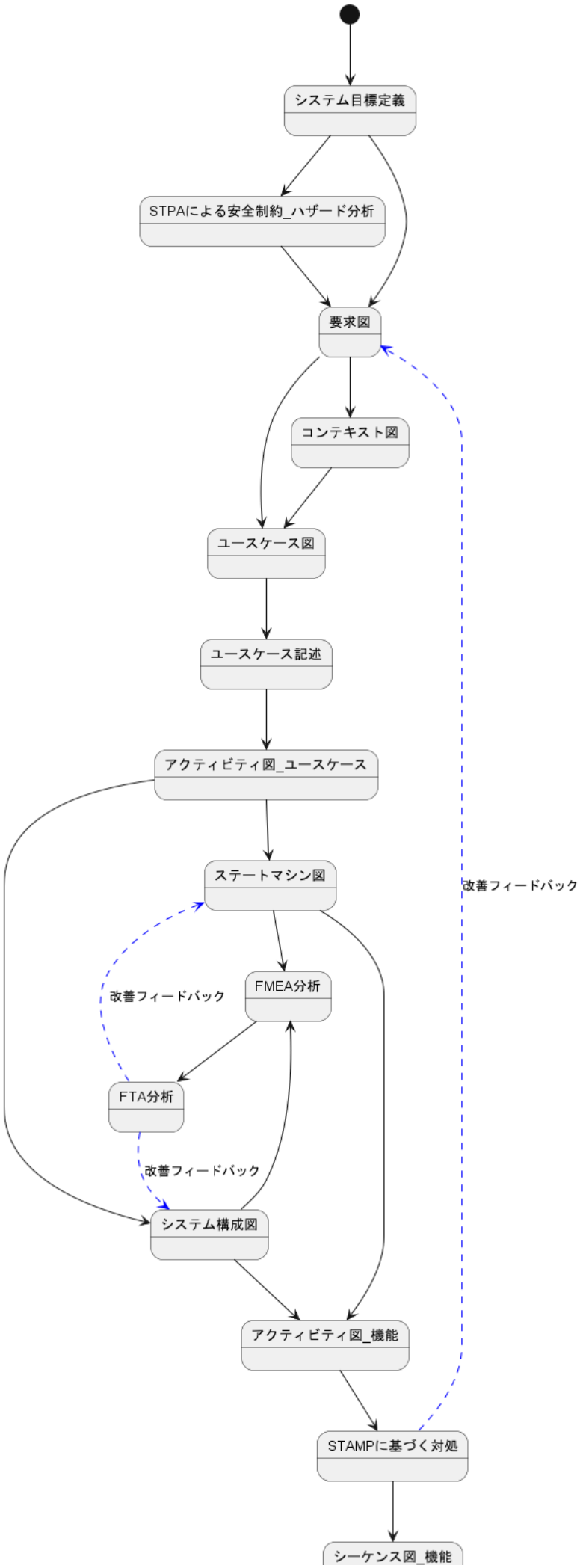
網羅性チェック:

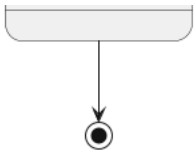
- 要求カバレッジ: 要求図 に記載された全てのシステム要求が、少なくとも一つのユースケースによってカバーされているかを検証します。
- フローカバレッジ: 各ユースケース記述で定義された全てのフロー（特に例外フローや代替フロー）が、アクティビティ図で適切に表現されているか、また、考慮漏れがないかを検証します。
- 状態・遷移カバレッジ: ステートマシン図 において、定義された全ての状態が到達可能であるか、また予期せぬデッドロックや意図しない状態遷移が存在しないかを（限定的ながら）静的に解析します。
- リスク対応カバレッジ: FMEA分析 やFTA分析 で特定されたリスクや故障モードに対し、対応する処理（例：ユースケースの例外フロー、ステートマシン図の故障処理状態など）が設計に盛り込まれているかを検証します。

シミュレーションベースの検証:

- シーケンス図の妥当性検証: 現在の記述「AIでpythonコードを自動生成し、人手による修正を加えたpythonコードの実行結果です」 を拡張し、AIが複数のユースケースシナリオ（正常系、異常系）を生成し、それに基づいてシーケンス図のシミュレーションを実行し、期待される結果と照合することで、動的な振る舞いの妥当性を検証します。
- ステートマシン図の動的検証: AIがイベントシーケンスを生成し、それをステートマシンモデルに入力することで、特定の条件下での状態遷移パスを探索し、デッドロックやライブロック、特定の制約違反（例：不正な状態遷移）が発生しないかを動的に検証します。」

プロセスフロー

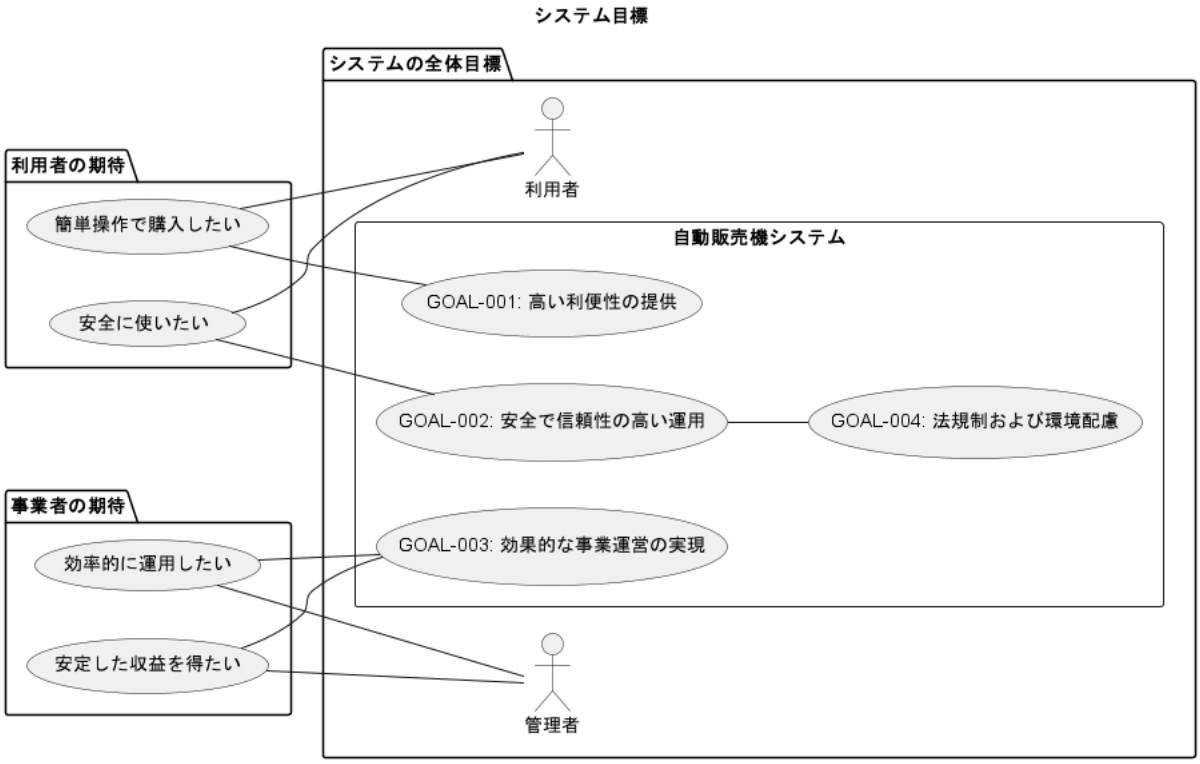

システム目標定義
STPAによる安全制約_ハザード分析
要求図
コンテキスト図
ユースケース図
ユースケース記述
アクティビティ図_ユースケース
ステートマシン図
FMEA分析
FTA分析
システム構成図
アクティビティ図_機能
STAMPに基づく対処
シーケンス図_機能
改善フィードバック
改善フィードバック
改善フィードバック



ダイアグラム	内容
システム目標	開発するシステムが達成すべき最上位の目的、ゴール、および主要なステークホルダー（利用者、管理者、設置者など）の期待を明確にする初期の活動です。
STPAによる安全制約・ハザード分析	システム全体の制御構造に着目し、「なぜ安全でない制御が行われたのか？」を分析することで、より網羅的かつ効果的な安全制約を導出することを目的とします。
要求図	自動販売機に対して関係者（利用者、管理者、メンテナンス担当者など）が持つ要求や期待事項を整理し、システムが満たすべき要件を視覚的にまとめた図です。これにより、システムの目的や全体像、関係者ごとのニーズを俯瞰的に把握できます。
コンテキスト図	自動販売機システムと外部システムやアクターとの情報のやり取りや関係性を俯瞰的に表現します。
ユースケース図	自動販売機の利用者や管理者などのアクターと、システムが提供する主要な機能（ユースケース）との関係を視覚的に示します。
ユースケース記述	各ユースケース（機能）の具体的な流れや条件、例外などを文章で詳細に記述します。
アクティビティ図(ユースケース)	各ユースケース（機能）の具体的な流れや条件、例外などをフローチャート形式で表現します。
ステートマシン図	ステートマシン図は、自動販売機システムが持つさまざまな状態（例：待機中、販売中、故障中、メンテナンス中など）と、それらの状態間の遷移（イベントや条件による変化）を視覚的に表現した図です。これにより、システムがどのような状態を持ち、どのようなタイミングで状態が変化するのかを俯瞰的に理解できます。
システム構成図	自動販売機システムを構成する主要なハードウェア・ソフトウェア要素や外部システムとの接続関係を示します。
FMEA	自動販売機システムにおける各コンポーネントや機能に対して、想定される故障モードとそれが引き起こす影響を体系的に洗い出し、リスクを数値化して優先的な対策を立案する。
FTA	特定の障害事象（Top Event）が発生する原因を論理的に分解し、**「なぜその問題が起こるのか？」**を視覚的に追跡・解析する手法です。
アクティビティ図(機能)	各機能の処理手順やワークフローをフローチャート形式で表現します。
STAMPに基づく対処	UCA（安全でない制御行動）やその発生原因を防ぐための対策を検討し、具体的な安全制約や安全要求として定義します。これらが要求図に反映されます。
シーケンス図_機能検証	システム内外のオブジェクト間でやり取りされるメッセージや処理の時系列的な流れを示します。

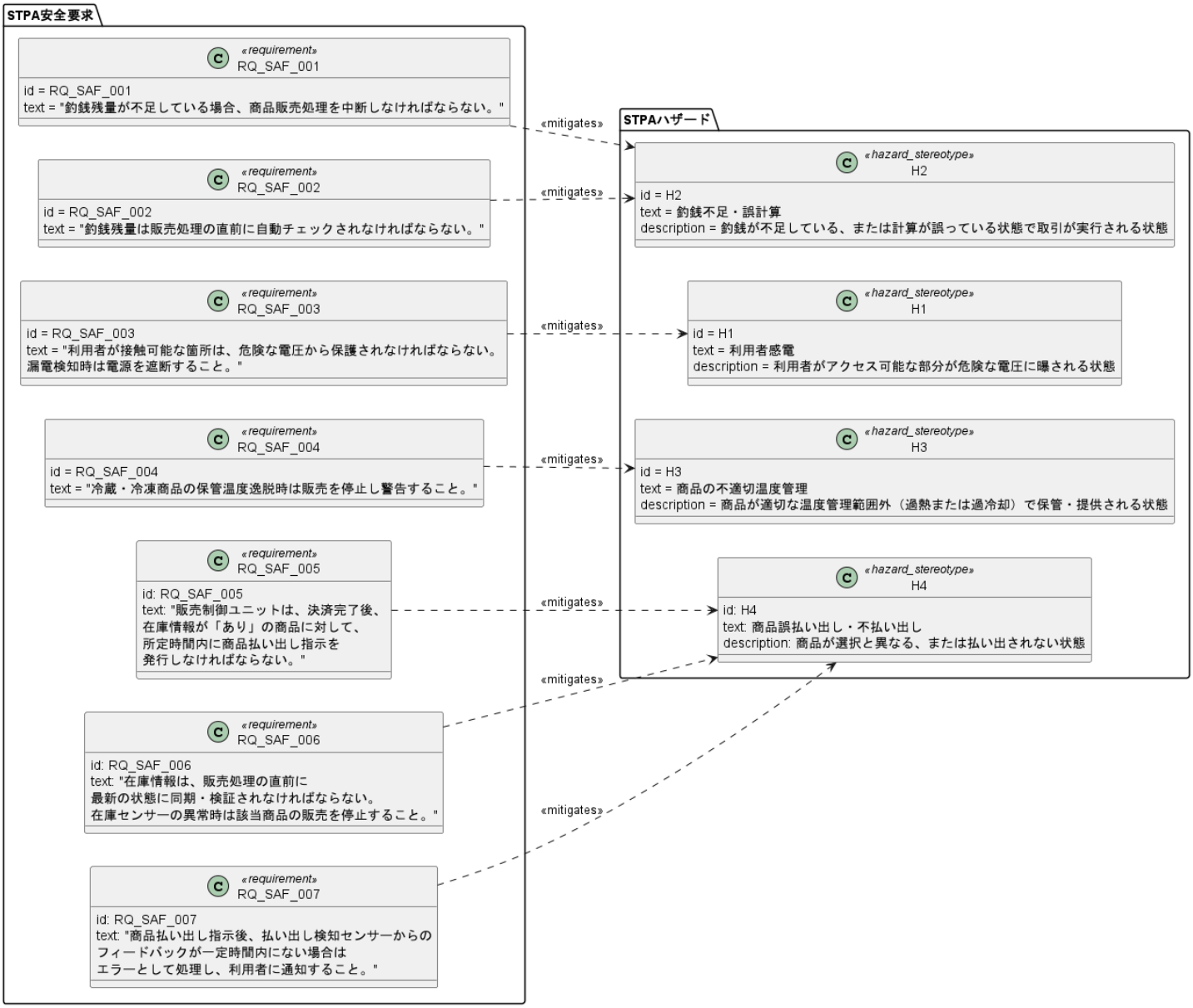
システム目標

- 開発するシステムが達成すべき最上位の目的、ゴール、および主要なステークホルダー（利用者、管理者、設置者など）の期待を明確にする初期の活動です。



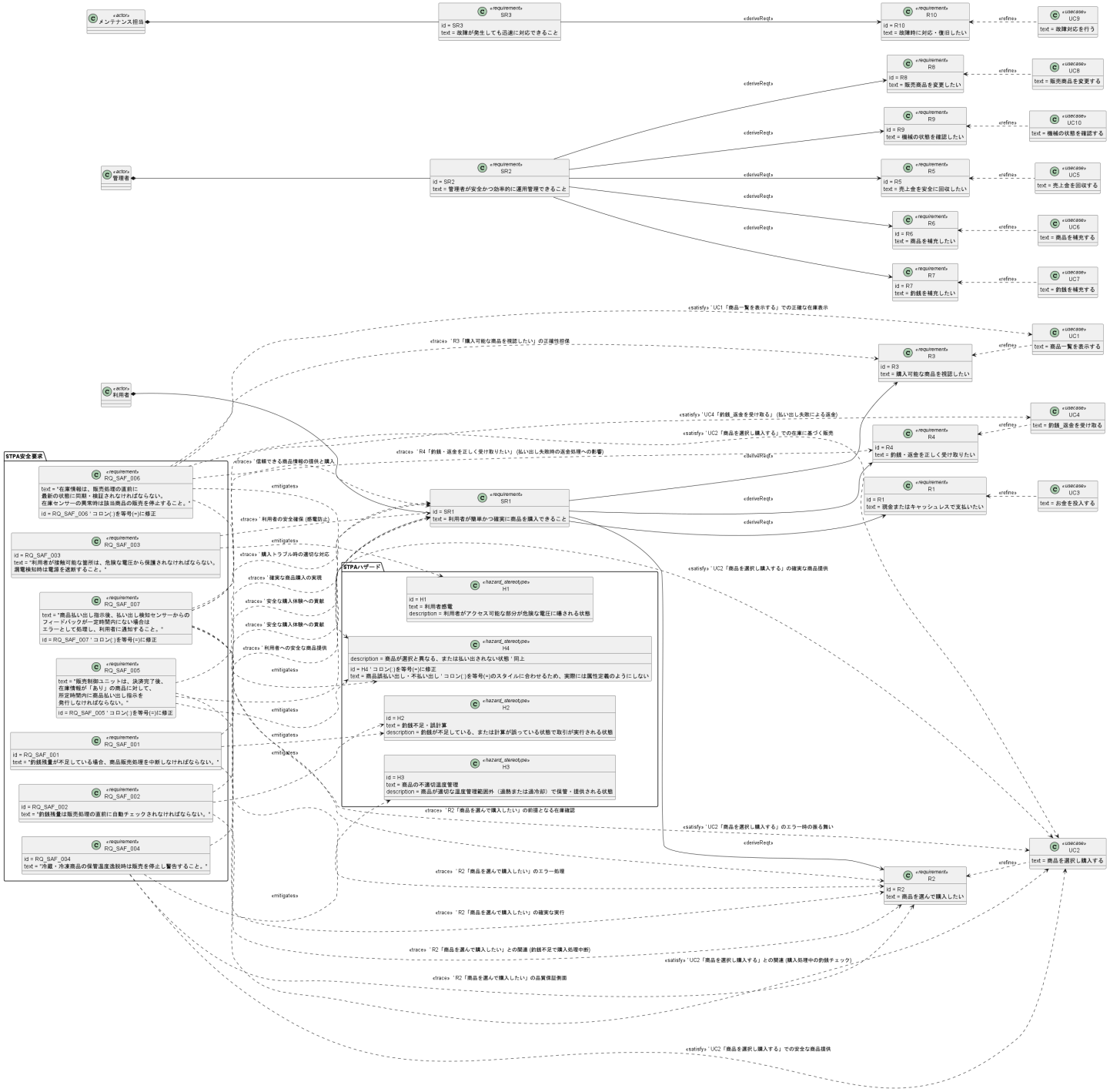
STPAによる安全制約・ハザード分析

システム全体の制御構造に着目し、「なぜ安全でない制御が行われたのか？」を分析することで、より網羅的かつ効果的な安全制約を導出することを目的とします。



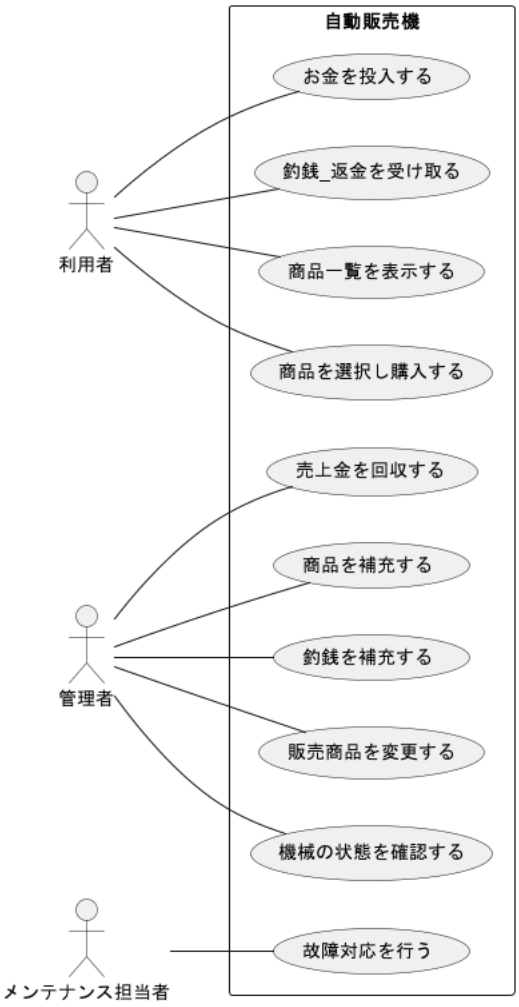
要求図

- 自動販売機に対して関係者（利用者、管理者、メンテナンス担当者など）が持つ要求や期待事項を整理し、システムが満たすべき要件を視覚的にまとめた図です。これにより、システムの目的や全体像、関係者ごとのニーズを俯瞰的に把握できます。



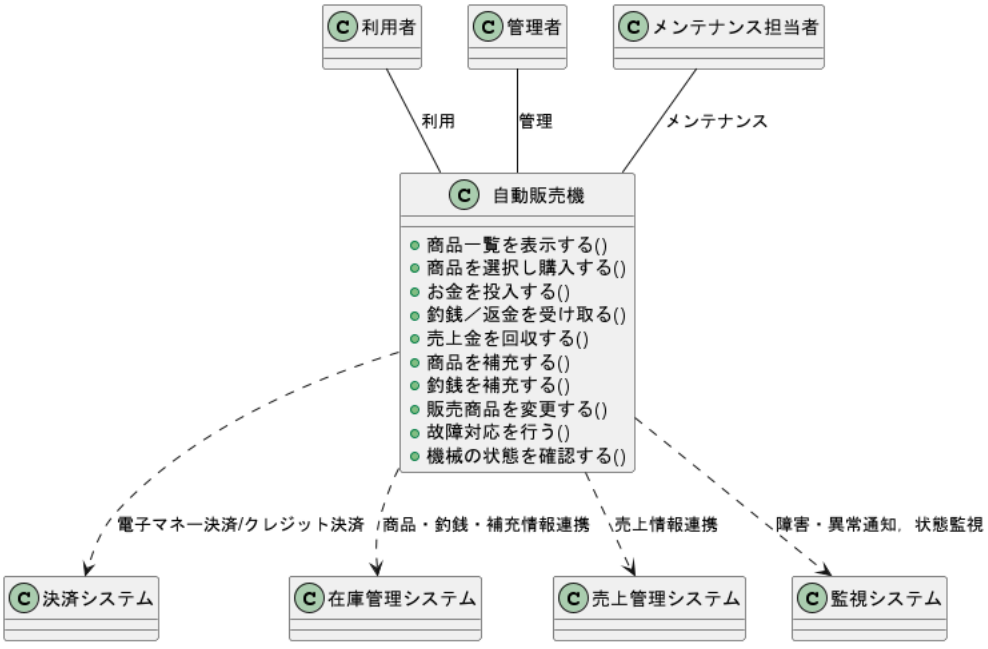
ユースケース図

- 自動販売機の利用者や管理者などのアクターと、システムが提供する主要な機能（ユースケース）との関係を視覚的に示します。



コンテキスト図

- 自動販売機システムと外部システムやアクターとの情報のやり取りや関係性を俯瞰的に表現します。



ユースケース記述

- 各ユースケース（機能）の具体的な流れや条件、例外などを文章で詳細に記述します。

ユースケース: お金を投入する

概要

利用者が自動販売機に現金もしくはキャッシュレス手段でお金を投入し、投入金額が増えるごとに選択可能な商品の選択状態を更新する。

アクター

- 利用者

事前条件

- 自動販売機が稼働中であること

事後条件

- システムが投入された金額を正しく認識し、現時点で購入可能な商品を表示する。

基本フロー

フローID	内容
BF-1	利用者は現金（硬貨・紙幣）またはキャッシュレス決済手段で支払い操作を行う。
BF-2	システムは投入された金額を認識し、画面やディスプレイに合計投入金額を表示する。
BF-3	システムは現在の投入金額で購入可能な商品ボタンを点灯/選択可に、金額不足の商品ボタンを消灯/選択不可にする。
BF-4	利用者は投入を継続するか（【BF-1】）、商品選択（「商品を選択し購入する」ユースケースへ遷移）を行う。

分岐

- 【BF-1】で受け入れ不可なコイン・紙幣・カードの投入、不正操作、読み取りエラーの場合→例外フロー【EF-1】へ
- 【BF-2】で金額認識不能の場合→例外フロー【EF-2】へ
- 【BF-4】で取引キャンセルや一定時間無操作の場合→代替フロー【AF-1】へ

代替フロー

フローID	内容
AF-1-1	利用者がキャンセルボタンを押す、または一定時間無操作の場合。
AF-1-2	システムは投入済みの金額（未使用分）を返却する。
AF-1-3	処理終了。

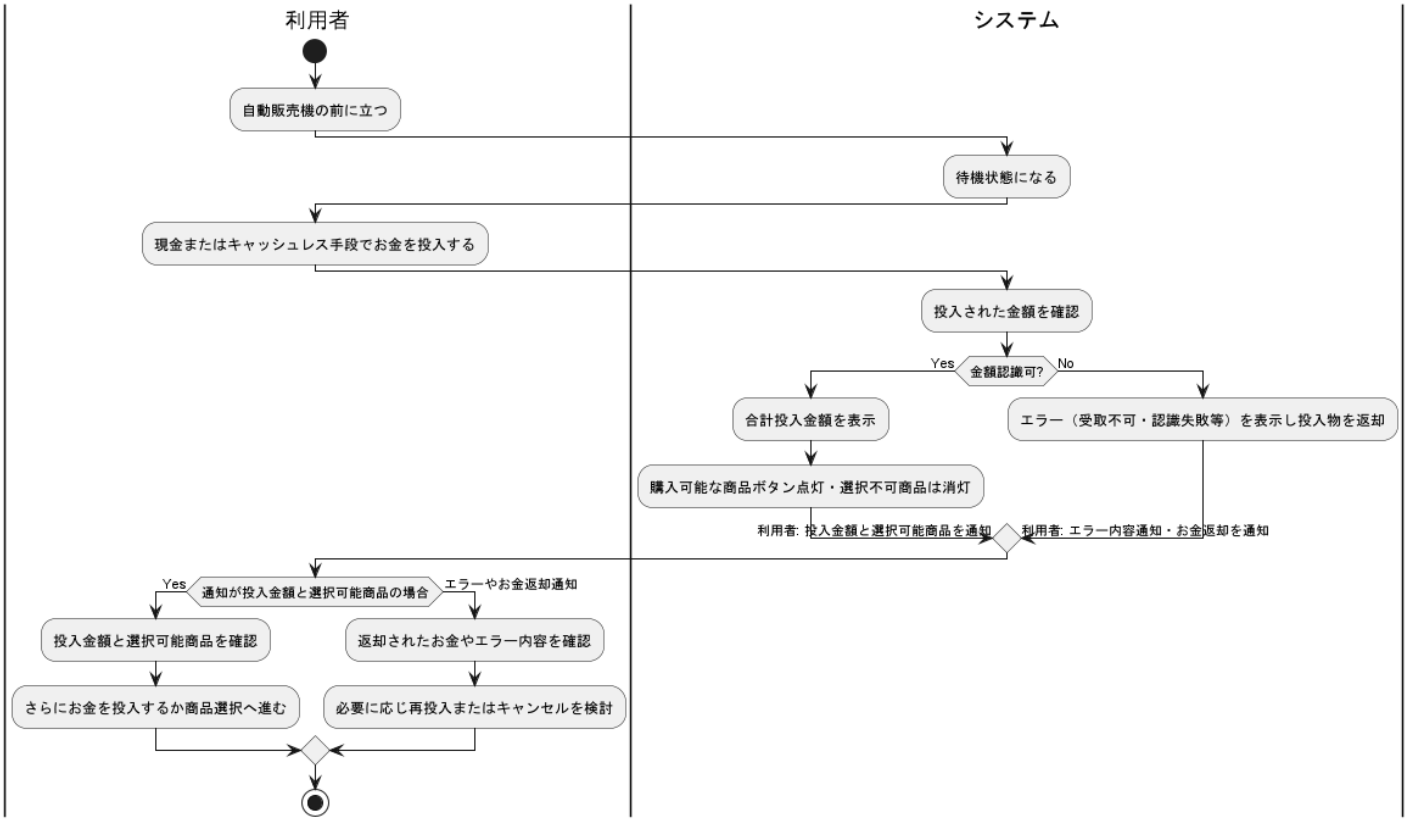
例外フロー

フローID	内容
EF-1-1	投入されたお金・カード等が使用不可能（破損、異物、規格外等）の場合、システムは該当投入物を返却し、「使用できません」と通知する。
EF-1-2	利用者は再度投入するか、取引をキャンセルする（必要に応じてAF-1-1へ）。

フローID	内容
EF-2-1	金額認識機構に障害が発生した場合、システムは全投入金額を返却しエラー表示を行う。
EF-2-2	処理終了。

備考

- 硬貨・紙幣は受入不可額を自動で返却し、金額認識不能時はシステムエラーとする。
- 商品購入までに投入額を超える商品は自動的に選択不可状態に制御されている。
- 商品選択後も追加投入できる仕様の機種もあるが、その場合はフロー調整が必要。



ユースケース: 商品一覧を表示する

概要

自動販売機の前面には、現在購入可能な商品の一覧が常時表示されており、利用者は任意のタイミングで商品を確認できる。

アクター

- 利用者

事前条件

- 自動販売機の電源がONになっていること。
- 商品が陳列・表示されていること。

事後条件

- 利用者が購入可能な商品を視認できる。
- 最新の在庫状況・金額が反映された商品情報が表示されている。

基本フロー

フローID	内容
BF-1	自動販売機は商品の一覧（商品名・価格・在庫状況等）を前面パネルやディスプレイに常時表示している。

フローID	内容
BF-2	利用者は自動販売機の前面を通じて、現在購入可能な商品を確認する。

分岐

- 【BF-1】で商品の情報取得や表示に障害が発生した場合、例外フロー【EF-1】へ。

代替フロー

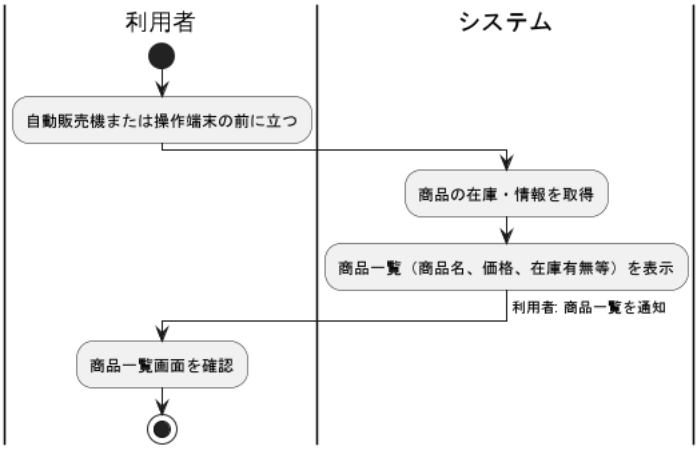
- 本ユースケースは代替フローを持ちません（利用者の操作を必要とせず、自動/常時表示であるため）。

例外フロー

フローID	内容
EF-1-1	システムが商品の情報取得や表示に失敗した場合、画面もしくはLED表示により「一部商品情報が表示できません」 等のエラー情報を表示する。
EF-1-2	システムは対応可能な場合、自動的に情報の再取得や再表示を試みる。

備考

- 売切れ商品には「売切」などの明示的な表示を行う。
- 故障やエラーが発生した場合は「販売停止中」等のステータス表示が行われる。
- 利用者による明示的な操作（ボタン押下等）は不要であり、アクションは観察（視認）のみ。



ユースケース: 釣銭・返金を受け取る

概要

利用者が自動販売機の釣銭レバー（返金レバー）を操作し、釣銭または投入金額の返金を受け取るまでの流れ。

アクター

- 利用者

事前条件

- 自動販売機に投入済みの金額があること
- 商品を購入し終え釣銭が発生している、または商品未選択でキャンセル（返金）希望の状態であること

事後条件

- 利用者が釣銭または返金金額を受け取る
- システム（自動販売機）は釣銭・返金処理を完了状態とする

基本フロー

フローID	内容
BF-1	利用者は釣銭レバー（返金レバー）を操作する。
BF-2	システムは釣銭または投入する金額分の返金を釣銭・返金取り出し口に払い出す。
BF-3	システムは釣銭・返金ランプ点灯やブザー音等で「お釣り（返金）をお取りください」と案内する。
BF-4	利用者は釣銭または返金金額を取り出し口から受け取る。

分岐

- 【BF-2】釣銭詰まりや釣銭切れ等で正常に払い出せない場合、例外フロー【EF-1】へ。
- 【BF-4】で一定時間受け取りがなかった場合、代替フロー【AF-1】へ。

代替フロー

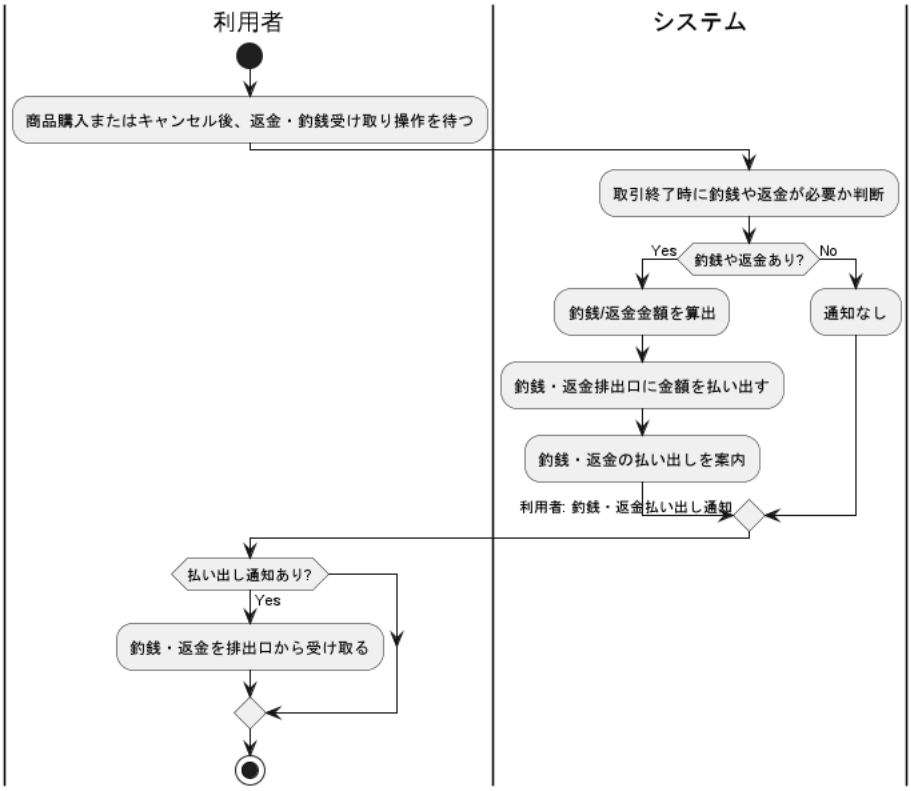
フローID	内容
AF-1-1	一定時間釣銭や返金未受領の場合、システムは再度音声やランプで受け取りを促す。
AF-1-2	さらに一定時間経過後、釣銭・返金金額を内部保管へ移し、管理記録として残す。
AF-1-3	フロー終了。

例外フロー

フローID	内容
EF-1-1	釣銭・返金の払い出しに障害（釣銭切れ、詰まり等）が発生した場合、システムはエラーメッセージや警告ランプ等で通知する。
EF-1-2	利用者への返金不能・トラブル内容をディスプレイ等で案内し、必要に応じて管理会社への連絡先も表示する。
EF-1-3	利用者は連絡先への問い合わせ等を行う。

備考

- 釣銭レバーは現金投入後のキャンセルや購入可能商品が選択されなかった場合にも返金操作として利用可能。
- 古い形式の自動販売機では釣銭レバー操作で投入分全額返却される。
- 一部の自動販売機ではタッチパネルやボタン式の返金操作もあるため、必要に応じて名称や操作内容は調整可。
- 釣銭レバー操作を複数回行った場合や物理的不具合時の動作は設計により異なる。



ユースケース: 商品を選択し購入する

概要

利用者が自動販売機へお金（現金またはキャッシュレス）を投入し、希望する商品を選択して購入・受け取るまでの一連の流れ。

アクター

- 利用者

事前条件

- 自動販売機が稼働中であること

事後条件

- 利用者が選択した商品を受け取るか、未購入分のお金が返却される

基本フロー

フローID	内容
BF-1	利用者は現金（硬貨または紙幣）、もしくはキャッシュレス決済を投入・認証する。
BF-2	システムは投入金額（または決済可否）を確認し、選択可能な商品を表示する。
BF-3	利用者は購入したい商品の選択ボタンを押下する。
BF-4	システムは選択された商品の在庫および釣銭状況を確認する。
BF-5	購入可能な場合、商品を払い出し、必要に応じてお釣りを払い出す。
BF-6	利用者が商品（とお釣り）を受け取る。

分岐

- 【BF-2】や【BF-4】で商品在庫切れや釣銭不足時、例外フロー【EF-1】【EF-2】へ。
- 【BF-1】や【BF-2】で投入金額不足時、基本フロー【BF-1】へ戻って追加投入を促す。
- 【BF-1】【BF-2】【BF-3】～で利用者取引キャンセル時、代替フロー【AF-1】へ。

代替フロー

フローID	内容
AF-1-1	利用者がキャンセル操作をする、または一定時間操作がなかった場合取引タイムアウトとなる。
AF-1-2	システムは投入金額のうち未使用分の金額を全額返却する。
AF-1-3	処理終了。

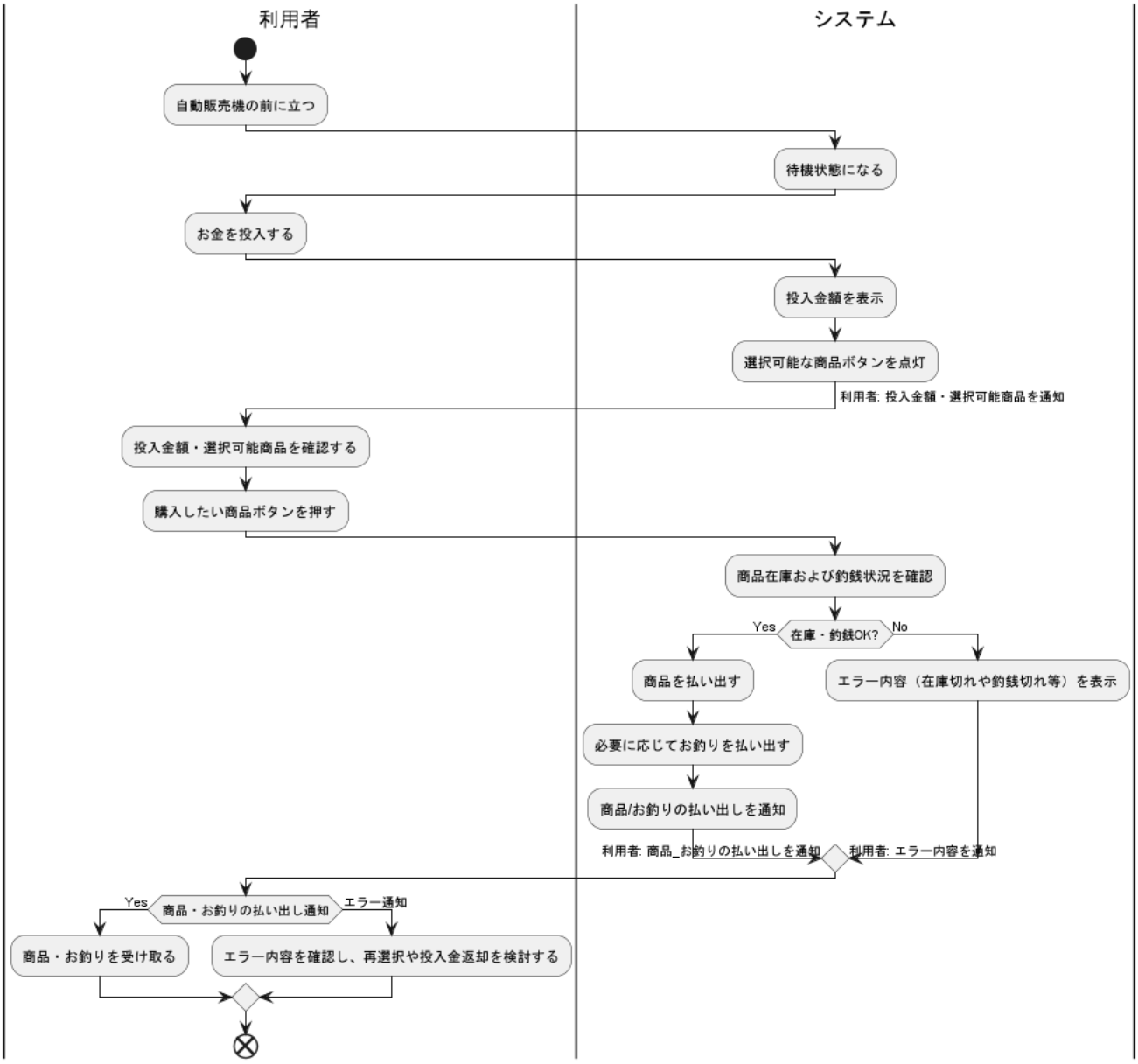
例外フロー

フローID	内容
EF-1-1	商品ボタン押下時【BF-4】、在庫切れまたは販売停止・メカトラブル等で購入できない場合、エラーを表示し再選択を促す。
EF-1-2	利用者は別の商品を選択（【BF-3】へ戻る）または取引終了時はAF-1に進む。

フローID	内容
EF-2-1	商品選択時【BF-4/5】釣銭切れでお釣りが払えない場合、エラー通知・購入不可を表示。
EF-2-2	利用者は別の商品（お釣り不要な商品等）を選択（【BF-3】へ）、または取引キャンセル（AF-1へ）。

備考

- 投入金額未満の商品ボタンは選択できないよう照明消灯等で制御されている場合が多い。
- キャッシュレス決済の場合は投入→商品選択→認証→商品払い出し、となる場合もある（運用に応じて要調整）。
- 商品受領やお釣り取り忘れ時のアラート等は省略。



ユースケース: 売上金を回収する

概要

管理者が自動販売機から売上金（硬貨・紙幣等）を安全かつ適切に回収し、売上金管理の記録を行う一連の流れ。

アクター

- 管理者

事前条件

- 管理者が自動販売機の解錠権限を持っていること
- 自動販売機が回収作業可能な状態にあること（メンテナンスモード等）

事後条件

- 売上金が適切に回収・封入され、売上履歴・回収履歴が更新される

基本フロー

フローID	内容
BF-1	管理者は自動販売機の施錠を解除し、回収用ドアを開く。
BF-2	システム（機械内部）は売上金（現金収納箱・釣銭ボックス等）へのアクセスを許可する。
BF-3	管理者は売上金（硬貨・紙幣）収納箱を取り外し、売上金を回収する。
BF-4	必要に応じて釣銭ボックスに釣銭を補充、または点検する。
BF-5	管理者は収納箱をもとの位置に戻し、ドアを閉じて施錠する。
BF-6	システムまたは管理者は回収日時・回収担当などの回収履歴を記録する（自動記録、または紙の記録）。

分岐

- 【BF-2】【BF-3】でエラーや不具合（収納箱が外れない、現金詰まり等）が発生した場合→例外フロー【EF-1】へ
- 【BF-6】で記録機能が正しく作動しない場合→例外フロー【EF-2】へ

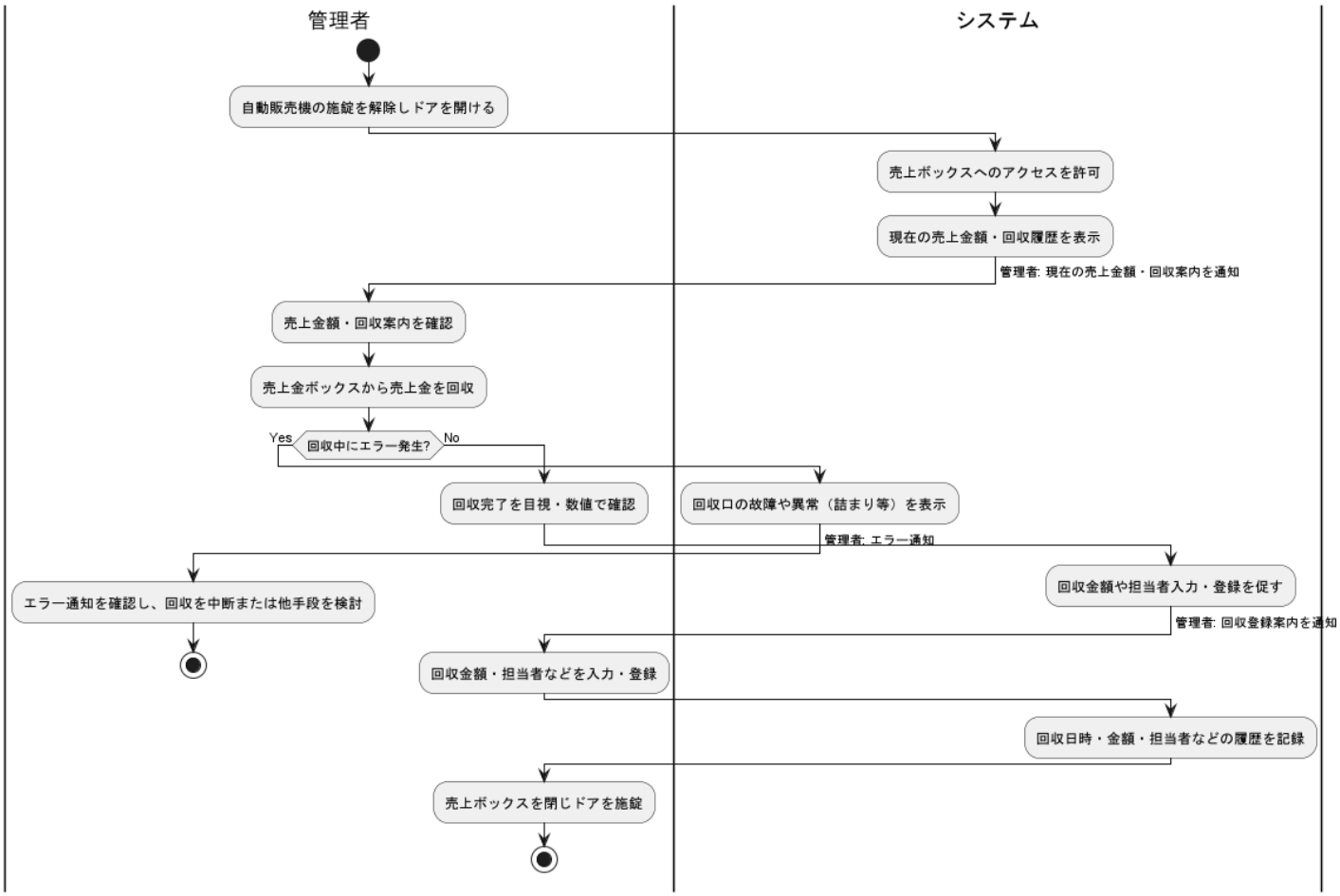
例外フロー

フローID	内容
EF-1-1	機械内部故障、収納箱が詰まっている等で売上金が取り出せない場合、システムは警告を表示しメンテナンス担当への対応を促す。
EF-1-2	管理者は現地での対処、または別途メンテナンス依頼を行い、処理終了。

フローID	内容
EF-2-1	回収履歴の記録ができなかった場合、管理者は紙で記録する、管理者に報告する等別手続きをとる。
EF-2-2	処理終了。

備考

- 売上金回収時には回収袋等への封入や、作業記録票への記入などの現場運用が伴う場合がある。
- 最新機種では回収時に自動で現金残高や回収時刻が端末・コネクタ等に記録されることも多い。
- 防犯上、回収操作時は必ず施錠・解錠管理や警報システム連動が行われている場合がある。
- 管理者が釣銭補充・商品補充を同時に行う場合もあるが、本ユースケースでは現金回収にフォーカスしている。



ユースケース: 商品を補充する

概要

管理者が自動販売機に新たな商品を補充し、補充内容や在庫状況をシステムに記録するまでの流れ。

アクター

- 管理者

事前条件

- 管理者が自動販売機の解錠権限を持っていること
- 補充する商品が補充担当者に用意されていること

事後条件

- 商品が自動販売機に正しく補充され、在庫数・補充履歴などが記録される

基本フロー

フローID	内容
BF-1	管理者は自動販売機の施錠を解除し、補充用ドアを開ける。
BF-2	システムは商品収納庫へのアクセスを許可し、在庫状況を表示する（在庫数表示など）。
BF-3	管理者は各商品ごとに在庫補充が必要かを確認し、該当商品を補充する。

フローID	内容
BF-4	補充完了後、必要に応じてシステムに補充内容や在庫数を入力・登録する（自動検知/手動入力）。
BF-5	管理者は商品収納庫の蓋を閉め、ドアを施錠する。
BF-6	システムまたは管理者は補充日時・担当者などの履歴を記録する。

分岐

- 【BF-3】で収納庫の故障やスペース不足（満杯）などが発生した場合→例外フロー【EF-1】へ
- 【BF-4】で補充情報の入力ミスや登録不能の場合→例外フロー【EF-2】へ

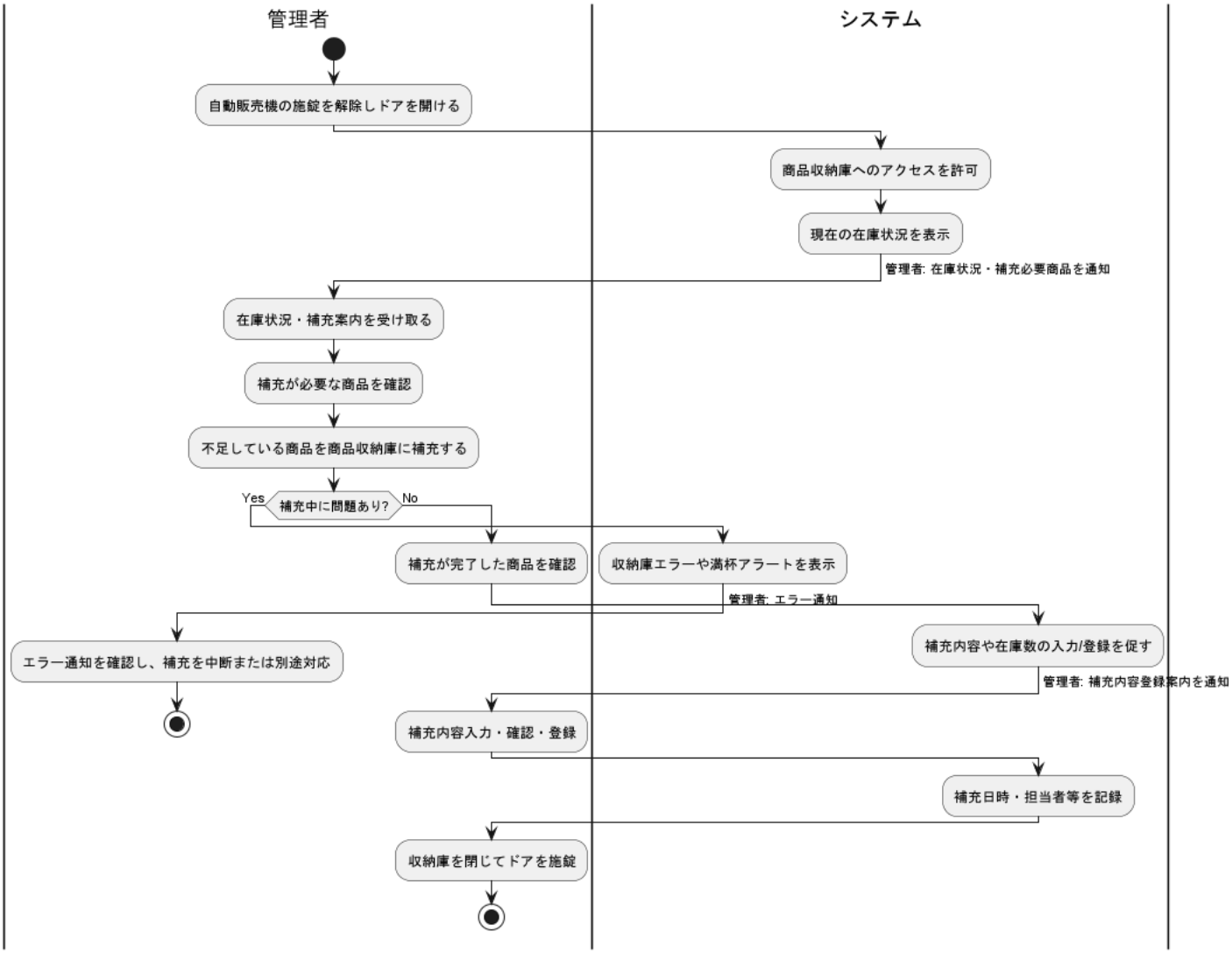
例外フロー

フローID	内容
EF-1-1	商品収納庫の機械的な故障や満杯でこれ以上補充できない場合、システムはエラー表示またはアラートを発し、管理者へ通知。
EF-1-2	管理者は当該商品について補充を中断し、処理終了またはメンテナンスを依頼。

フローID	内容
EF-2-1	システムへの補充内容入力や在庫登録に失敗した場合、再入力や異常記録を促す。
EF-2-2	必要に応じて管理者または本部へ連絡し、処理終了。

備考

- 商品補充は一般的に売上金回収や釣銭補充と同時に行われることが多い。
- 在庫管理・補充履歴は機種により自動登録や手入力登録のいずれの場合もある。
- 温度管理や賞味期限チェックが必要な商品についても適宜点検が行われる。



ユースケース: 釣銭を補充する

概要

管理者が自動販売機の釣銭装置へ必要な硬貨や紙幣を補充し、釣銭切れを防止する業務の流れ。

アクター

- 管理者

事前条件

- 管理者が自動販売機の解錠権限を持っていること
- 補充用の硬貨および紙幣が準備されていること

事後条件

- 必要な釣銭が適切に補充され、釣銭残量・補充履歴などが記録される

基本フロー

フローID	内容
BF-1	管理者は自動販売機の施錠を解除し、釣銭補充用ドアまたはカバーを開ける。
BF-2	システムは釣銭装置へのアクセスを許可し、現在の釣銭残量を表示する（システム自動表示または目視確認）。
BF-3	管理者は不足する硬貨や紙幣をそれぞれの釣銭ユニットに適切な枚数補充する。
BF-4	補充完了後、必要に応じて補充内容をシステムに入力・記録する（自動/手動選択可）。
BF-5	管理者は釣銭装置の状態を点検し、補充用ドアを閉じて施錠する。
BF-6	システムまたは管理者は補充日時・担当者などの補充履歴を記録する。

分岐

- 【BF-3】で釣銭ユニットの故障や満杯、誤投入などが発生した場合→例外フロー【EF-1】へ
- 【BF-4】で補充内容の記録ミスや登録不能の場合→例外フロー【EF-2】へ

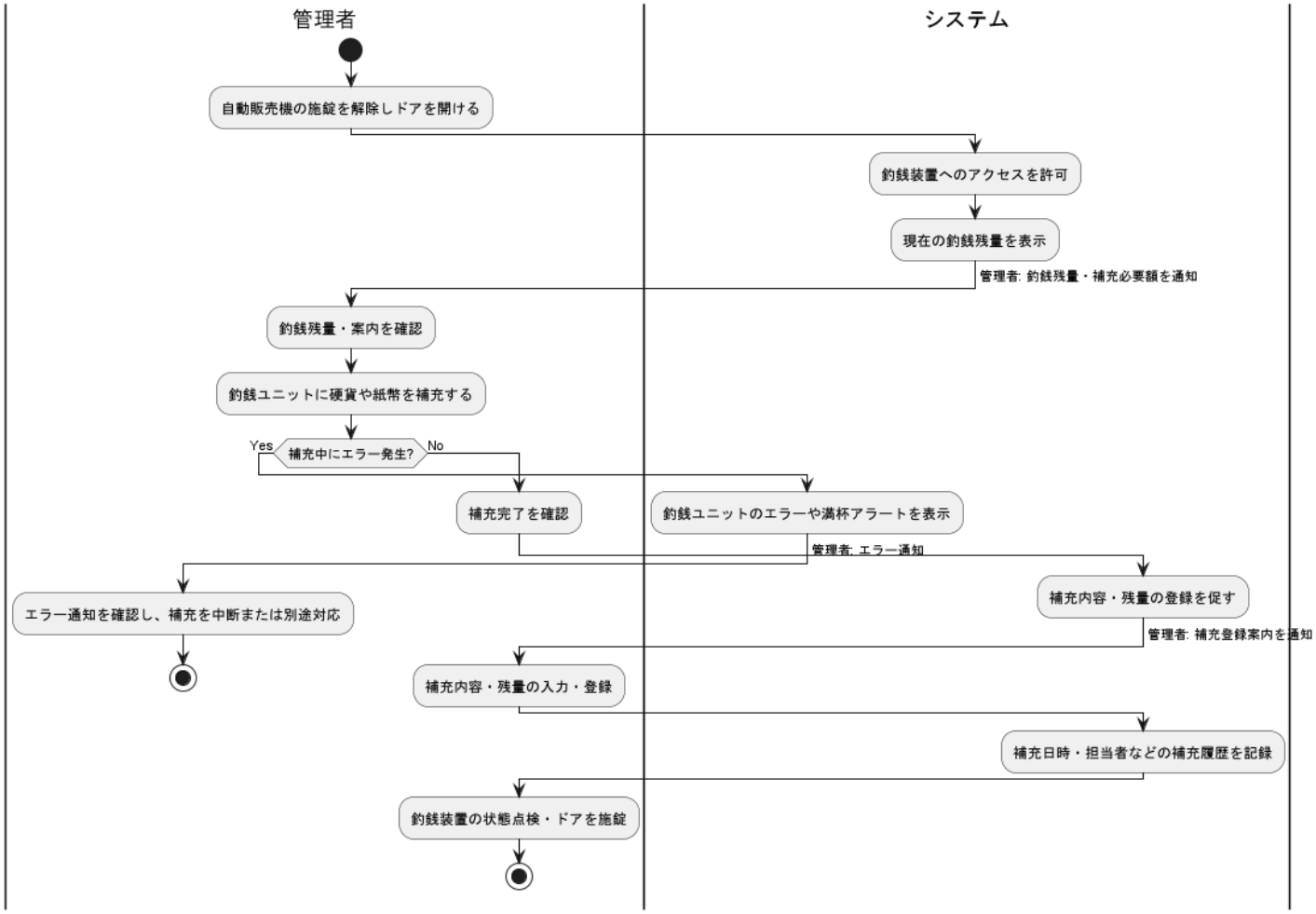
例外フロー

フローID	内容
EF-1-1	釣銭ユニットの機械的な故障や満杯、誤投入が発生した場合、システムはエラー表示・アラートを発し、管理者へ通知。
EF-1-2	管理者はそのユニットの補充を中断し、必要に応じてメンテナンス依頼、または報告を行い処理終了。

フローID	内容
EF-2-1	システムや帳票への補充内容入力や在庫登録に失敗した場合、再入力や異常記録を促す。
EF-2-2	必要に応じて現地管理者や本部等へ連絡し、処理終了。

備考

- 釣銭補充は商品補充や売上金回収業務とあわせて実施することが多い。
- 補充後の動作確認（テスト払い出し等）を実施する運用もある。
- 機種によっては釣銭装置ごと交換する方式や補充量自動入力方式も存在する。



ユースケース: 販売商品を変更する

概要

管理者が自動販売機内の販売商品を入替え、変更内容をシステムに登録・反映させるまでの流れ。

アクター

- 管理者

事前条件

- 管理者が自動販売機の管理・解錠権限を有している
- 新たな販売商品の在庫が準備されている

事後条件

- 新しい販売商品が自動販売機内にセットされ、システムにも正しく登録・反映される

基本フロー

フローID	内容
BF-1	管理者は自動販売機の施錠を解除し、補充・設定用ドアを開ける。
BF-2	システムまたは現物確認で現在販売されている商品のリストと配置を確認する。

フローID	内容
BF-3	販売を終了する商品を取り出し、新たな販売商品と差替え・補充する。
BF-4	必要に応じて商品ごとの価格や商品名、ボタン・ディスプレイの表示などを設定・変更する。
BF-5	システムに商品変更内容を登録・入力する（自動連動または手動入力）。
BF-6	管理者は商品の配置・数量・表示など最終確認を行い、ドアを施錠する。
BF-7	システム（または管理者）は変更日時や担当者・変更内容等を履歴として記録する。

分岐

- 【BF-3】で商品収納部に商品が残っており交換不能、または新商品がうまくセットできない場合 → 例外フロー【EF-1】へ
- 【BF-4】や【BF-5】で設定や登録時にエラーが発生した場合 → 例外フロー【EF-2】へ

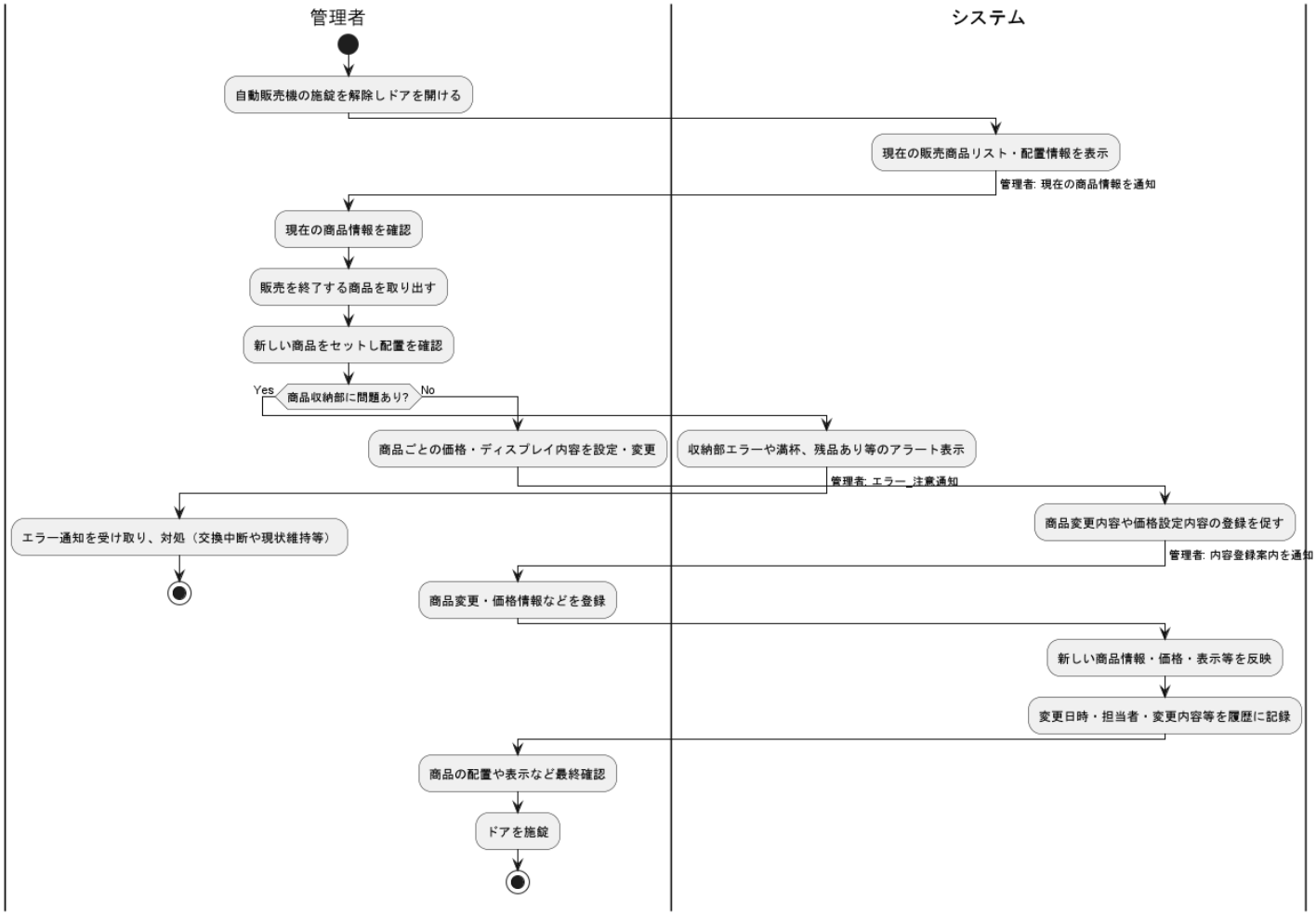
例外フロー

フローID	内容
EF-1-1	商品収納部のトラブル・満杯・残品等で新商品への切替ができない場合、管理者は現場措置またはメンテナンス担当へ連絡する。
EF-1-2	対象商品の交換を中断し、必要に応じて該当行のみ現状維持とする。

フローID	内容
EF-2-1	システムへの商品情報登録や、価格・表示情報変更に失敗した場合、再登録または紙帳票記入を行う。
EF-2-2	必要に応じて管理者または本部へ報告し、処理終了。

備考

- 商品変更後は在庫数や価格・キャンペーン情報等も同時に調整・登録する場合がある。
- 一部機種ではネットワーク経由で本部システムから商品設定が可能なものもある。
- 商品名や画像ラベル、ボタンプレート等の物理的な入替え・貼り替えなども必要な場合がある。



ユースケース: 機械の状態を確認する

概要

管理者（担当者）が自動販売機の稼働状況、内部在庫、エラー状況、売上や釣銭残量などを現地または遠隔で点検・確認するまでの流れ。

アクター

- 管理者

事前条件

- 管理者が自動販売機の確認権限を有している
- 確認に必要な機器（ICカード/認証キー/遠隔監視端末等）が準備されている

事後条件

- 機械状態が確認され、必要であれば点検・保守等の次の業務に情報提供される

基本フロー

フローID	内容
BF-1	管理者は現地に赴く、または遠隔システムにログインして、指定の自動販売機を選択する。
BF-2	現地の場合はドアロック解除や点検モードへの切替などの操作を行う。

フローID	内容
BF-3	システムから最新の状態情報（稼働中/停止中、在庫数、売上、釣銭残量、エラーログ等）を一覧で表示・取得する。
BF-4	管理者は画面・ログ・LEDランプ等を確認し、必要な情報（異常・不足・警報など）を点検票や管理端末に記録する。
BF-5	必要に応じて現場で調整・補充・保守等の後続作業に着手する。

分岐

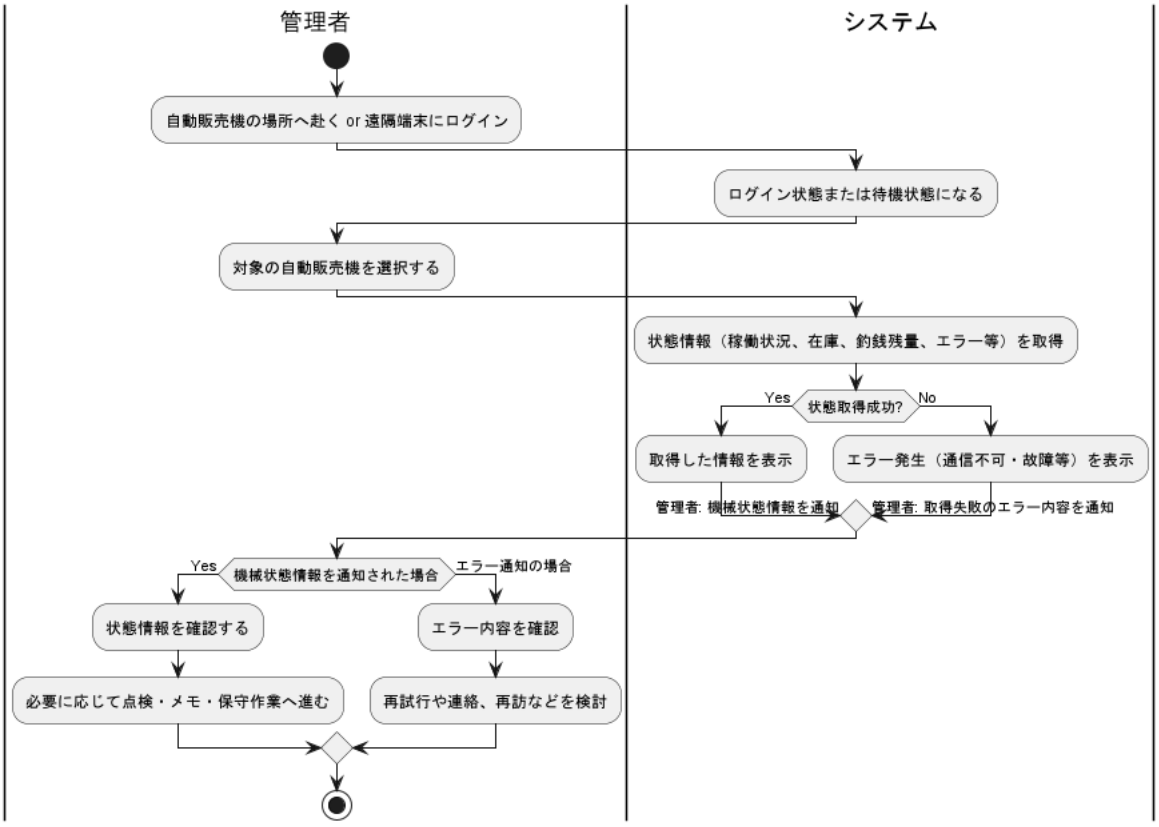
- 【BF-3】で状態取得に失敗（通信不可・端末故障等）の場合 → 例外フロー【EF-1】へ
- 【BF-4】で異常や複数の問題が検出された場合、関連するユースケース（故障対応、商品・釣銭補充など）へ遷移

例外フロー

フローID	内容
EF-1-1	システムまたは現地端末で状態情報が取得できない場合、管理者は通信再試行等を行う。
EF-1-2	改善できない場合はメンテナンス担当や管理部門に報告し、必要に応じて再訪や機器交換等を手配する。

備考

- 遠隔監視システムにより複数台の状態を一括管理できる場合もある
- 状況確認後に、そのまま商品の補充・売上金回収・故障対応・釣銭補充等の保守作業に移行することが多い
- 状態確認には温度、ドア開閉状況、防犯センサー等の確認も含まれる場合がある



ユースケース: 故障対応を行う

概要

メンテナンス担当者が自動販売機の故障・障害報告を受け、現地または遠隔操作により点検・原因調査、必要な修理・復旧対応を実施する。

アクター

- メンテナンス担当者

事前条件

- 故障や異常を示すアラートが利用者や監視システムから報告されている
- メンテナンス担当者が自動販売機の解錠・操作権限などを有している

事後条件

- 故障・障害が解決され、正常運用状態へ復旧し、対応内容・履歴が記録される

基本フロー

フローID	内容
BF-1	故障・異常の通報または自動アラートをメンテナンス担当者が受信する。
BF-2	メンテナンス担当者は現地に赴くか、遠隔システムから該当自動販売機の状態を確認する。
BF-3	メンテナンス担当者はエラーランプやメッセージ、ログデータ等から故障箇所や不具合の内容を調査・特定する。
BF-4	必要に応じて自動販売機を解錠し、内部の点検・テスト（部品交換、清掃、配線確認など）を実施する。
BF-5	小修理（詰まり解除、リセット、ユニット交換など）を行い、不具合を解消する。
BF-6	システムや現場で動作確認テストを行い、正常稼働を確認する。
BF-7	再発防止のための対応や消耗部品交換、必要に応じて故障原因・対応内容をシステムへ記録する。

分岐

- 【BF-3】で現場対応不能（重大故障・専用部品不足等）が判明した場合→例外フロー【EF-1】へ
- 【BF-5】【BF-6】で問題が解決しない場合→例外フロー【EF-2】へ

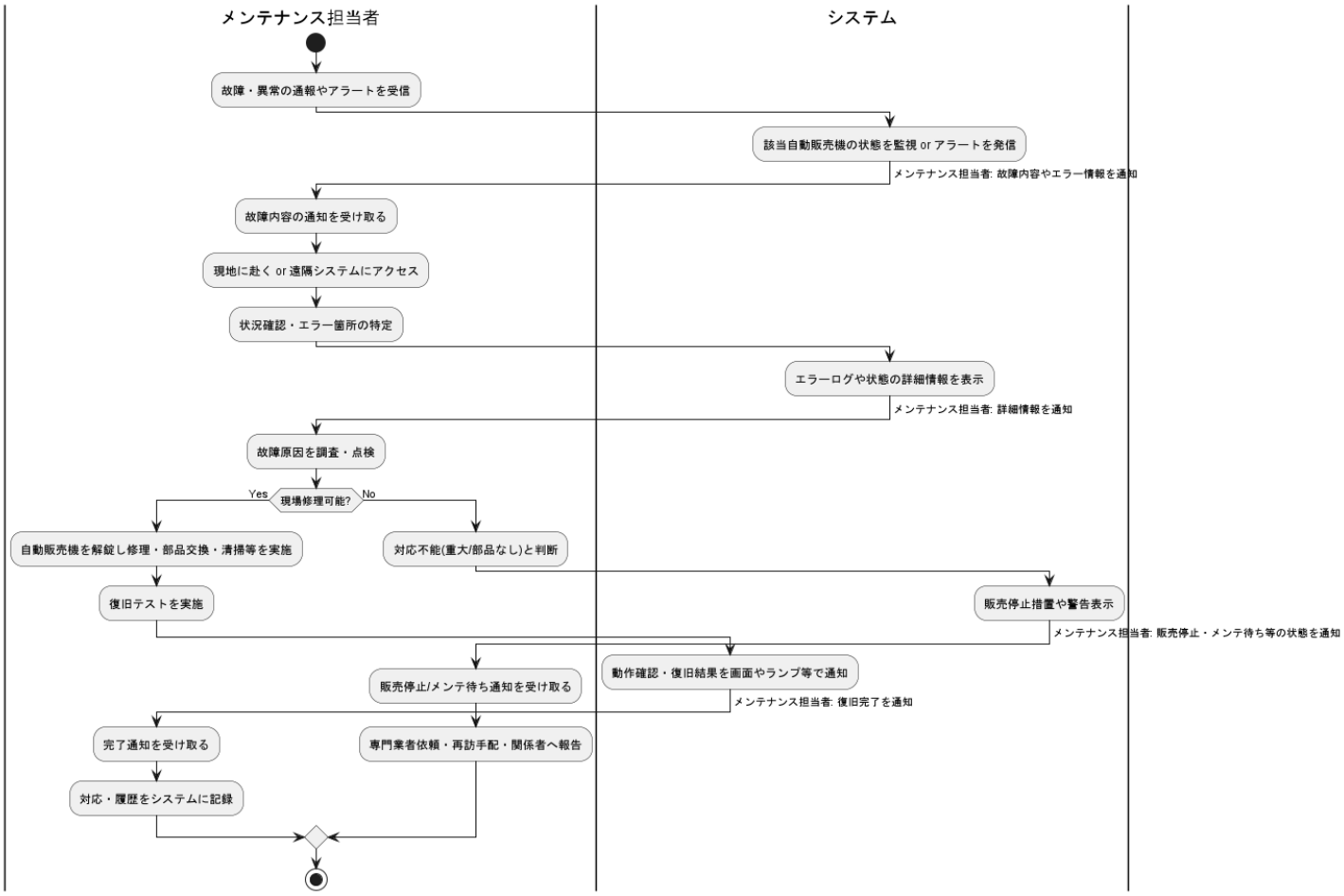
例外フロー

フローID	内容
EF-1-1	専門技術や部品手配が必要な重大故障の場合、メンテナンス担当者は本部や専門業者に修理依頼を行う。
EF-1-2	必要に応じて、一時的に販売停止措置・警告表示をセットする。

フローID	内容
EF-2-1	現地での故障対応・小修理によっても復旧不可の場合、機器の交換や運用停止・再訪問手配など中長期対応に切り替える。
EF-2-2	関連部署へ報告し、現場での安全確認を行う。

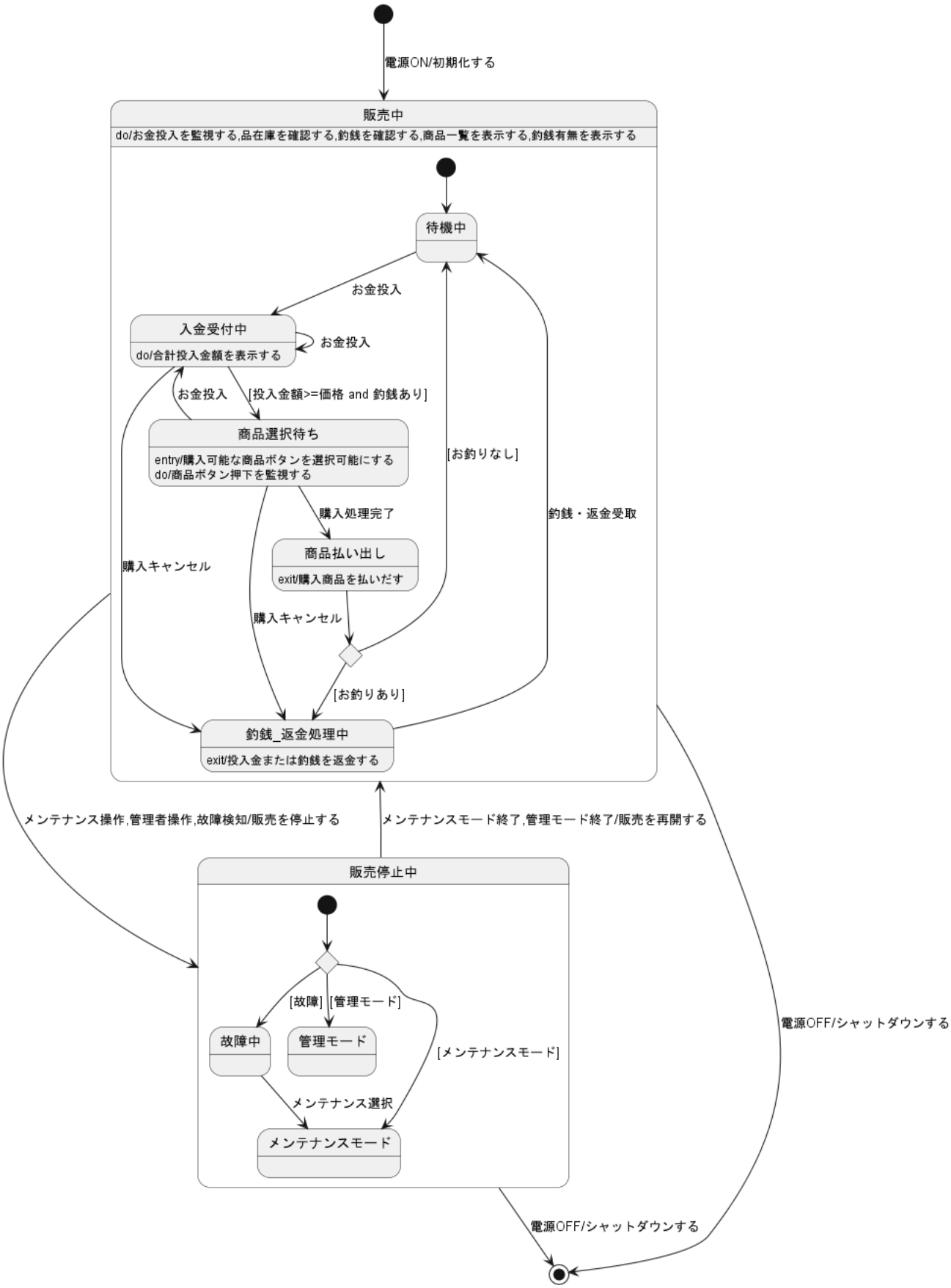
備考

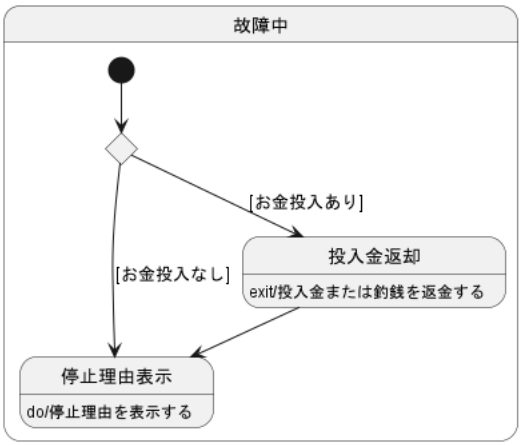
- 故障原因や対応内容はシステムに履歴として残し、今後の予防保全に活用することがある
- 利用者から現金・商品等の未払い出しや損失があった場合は別途対応（返金・商品提供など）も同時進行となる
- 遠隔監視・リモートリセット対応が可能な機種では現場作業と組み合わせて運用される

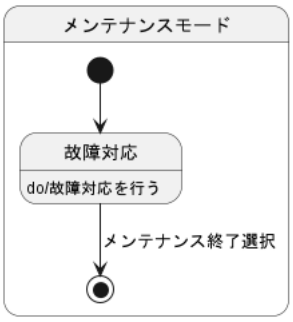


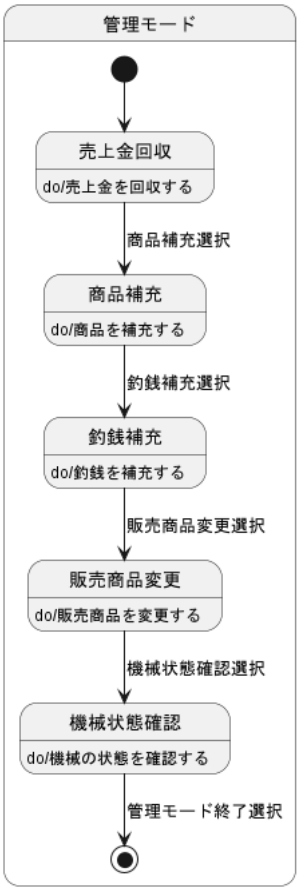
ステートマシン図

- ステートマシン図は、自動販売機システムが持つさまざまな状態（例：待機中、販売中、故障中、メンテナンス中など）と、それらの状態間の遷移（イベントや条件による変化）を視覚的に表現した図です。これにより、システムがどのような状態を持ち、どのようなタイミングで状態が変化するのかを俯瞰的に理解できます。


電源ON/初期化する
販売中
do/お金投入を監視する,品在庫を確認する,釣銭を確認する,商品一覧を表示する,釣銭有無を表示する
待機中
お金投入
入金受付中
do/合計投入金額を表示する
お金投入
お金投入
[投入金額>=価格 and 釣銭あり]
商品選択待ち
entry/購入可能な商品ボタンを選択可能にする
do/商品ボタン押下を監視する
[お釣りなし]
購入処理完了
釣銭・返金受取
商品払い出し
exit/購入商品を払いだす
購入キャンセル
購入キャンセル
[お釣りあり]
釣銭_返金処理中
exit/投入金または釣銭を返金する
メンテナンス操作,管理者操作,故障検知/販売を停止する
メンテナンスモード終了,管理モード終了/販売を再開する
販売停止中
[故障]
[管理モード]
故障中
管理モード
[メンテナンスモード]
メンテナンス選択
メンテナンスモード
電源OFF/シャットダウンする
電源OFF/シャットダウンする

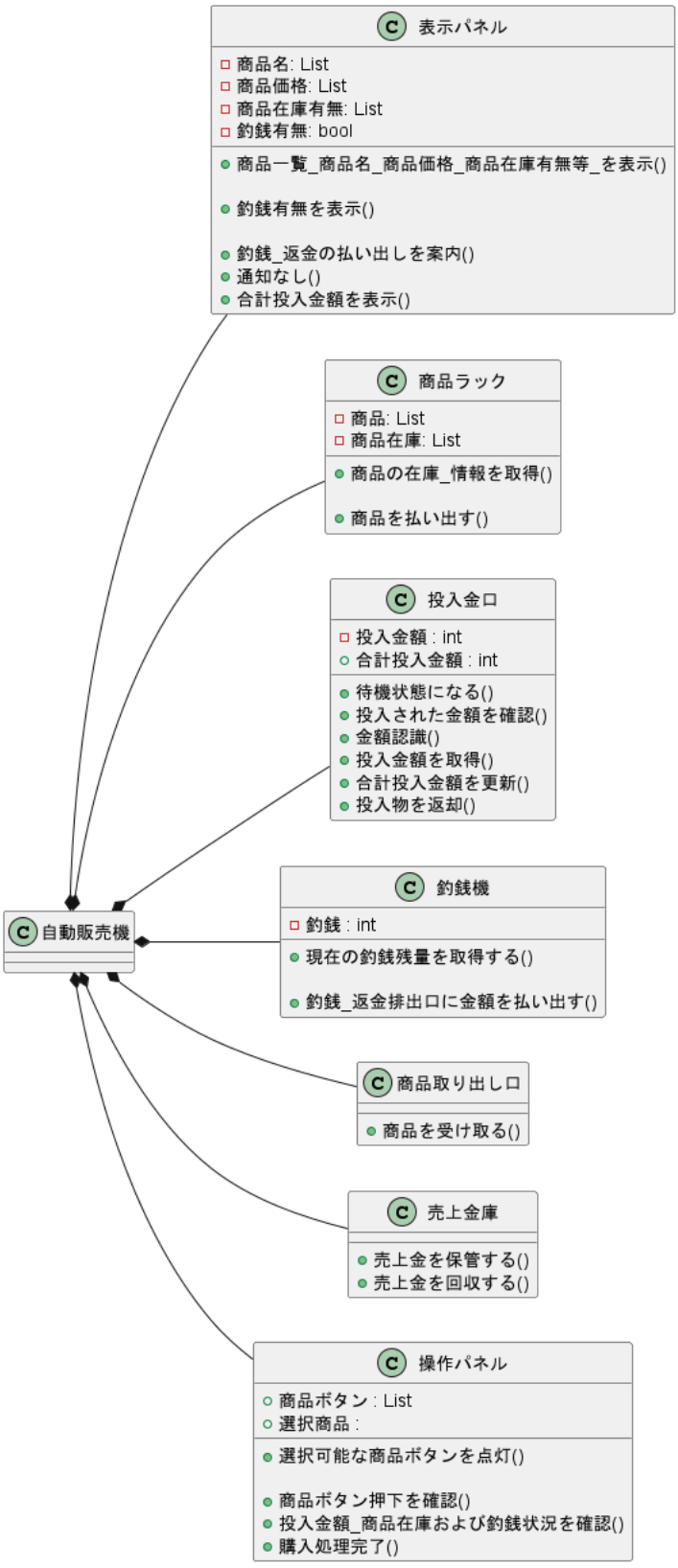






システム構成図

- 自動販売機システムを構成する主要なハードウェア・ソフトウェア要素や外部システムとの接続関係を示します。



FMEA分析

- FMEA（Failure Mode and Effects Analysis）は、自動販売機システムにおける各コンポーネントや機能に対して、想定される故障モードとそれが引き起こす影響を体系的に洗い出し、リスクを数値化して優先的な対策を立案するための分析手法です。

FMEA

機能・部品名	故障モード例	故障の影響例	発生度	重大度	検出度	RPN	備考
釣銭機	釣銭切れ/排出不良	釣銭不足・返金不可	4	9	4	144	釣銭残量監視

機能・部品名	故障モード例	故障の影響例	発生度	重大度	検出度	RPN	備考
商品ラック	商品詰まり/在庫誤検知	商品が出ない/誤表示	5	7	4	140	在庫センサーで検出可
投入金口	硬貨詰まり/認識不良	投入不可・金額誤認識	4	8	3	96	投入金センサー
表示パネル	表示が出ない/誤表示	操作不可・誤購入	3	8	3	72	定期点検・自己診断で検出可
商品取り出し口	商品取り出し不可	商品受け取り不可	2	7	5	70	取り出しセンサー
操作パネル	ボタン反応なし/誤動作	商品選択不可・誤選択	3	7	3	63	ボタン自己診断
売上金庫	金庫開閉不良/盗難	売上金紛失・回収不可	2	10	2	40	ロック・開閉ログ

RPN（Risk Priority Number）について

RPN = 発生度 × 重大度 × 検出度
数値が大きいほどリスクが高く、優先的な対策が必要です。

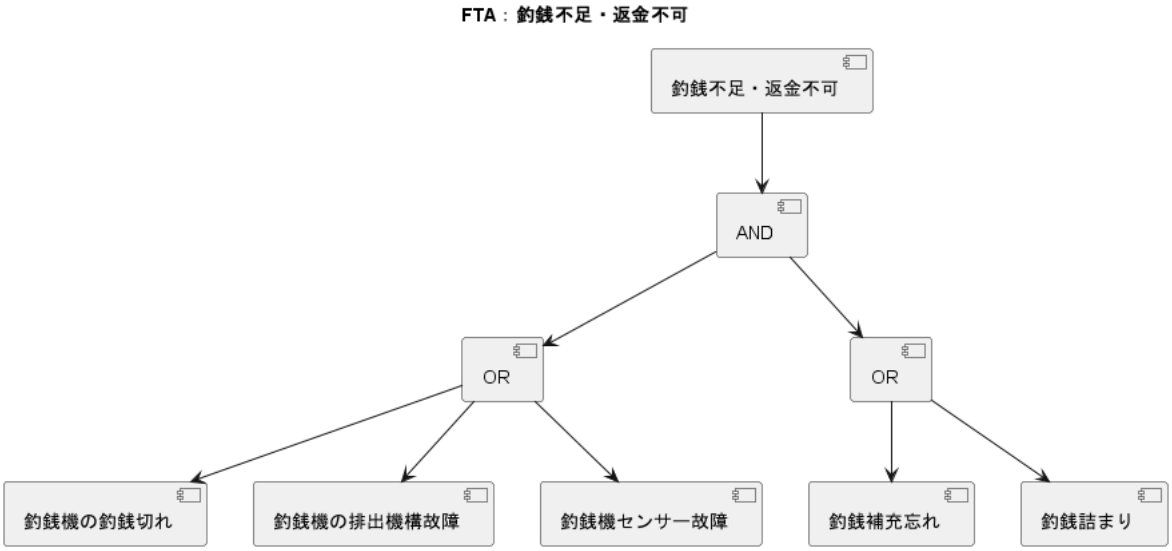
凡例

発生度：その故障がどれくらい発生しやすいか（1:まれ〜10:頻繁）
重大度：故障が発生した場合の影響の大きさ（1:軽微〜10:致命的）
検出度：故障が検出されにくいほど高い（1:容易に検出〜10:検出困難）

FTA分析

- FTA（Fault Tree Analysis）は、特定の障害事象（Top Event）が発生する原因を論理的に分解し、**「なぜその問題が起こるのか？」**を視覚的に追跡・解析する手法です。
- 論理ゲート（AND/OR）を用いて構成され、システムの故障に対する原因の組み合わせを構造的に示します。

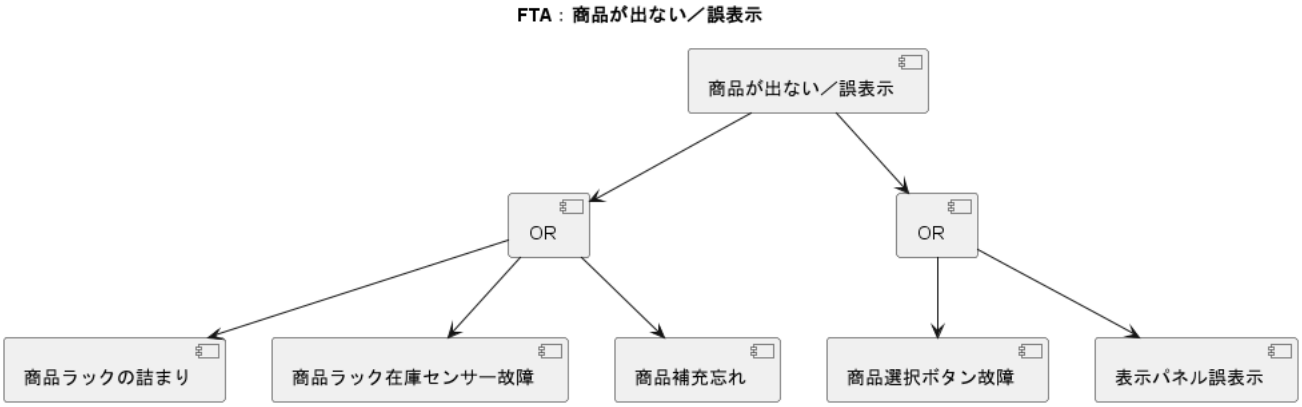
釣銭不足・返金不可 ⇒ 「FMEAのRPN=144」



原因	要因分類	詳細	対応策	トレーサビリティ先
釣銭機の釣銭切れ	運用ミス	補充忘れ・不足	・残量センサー導入 ・補充履歴管理	システム構成図（釣銭機）、 ユースケース「お金の投入」EF-4、 FMEA（RPN=144）
釣銭排出機構の故障	機器故障	排出モーター異常	・モーター異常検知・定期点検	ステートマシン図 （異常状態遷移）、 ユースケース「商品選択と購入」EF-2

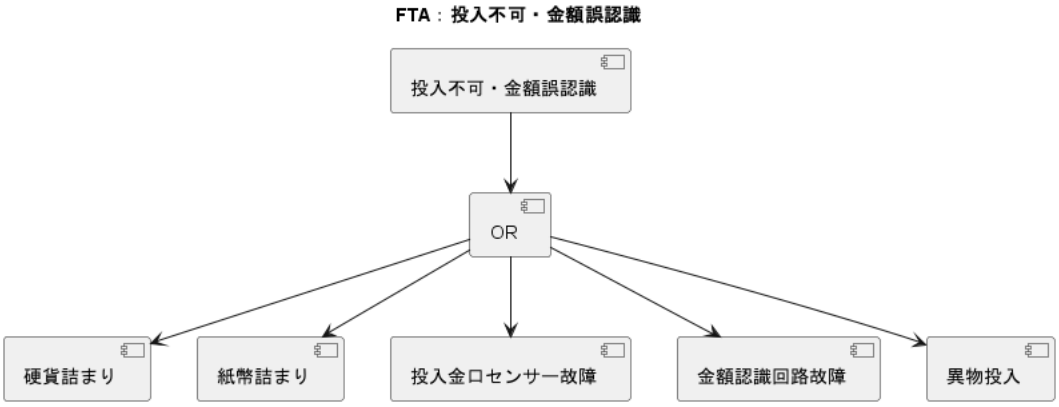
原因	要因分類	詳細	対応策	トレーサビリティ先
センサー誤検知	機器故障	実残量があるのに検出されない	・センサー冗長化・自己診断	システム構成図（センサー）、FMEAと連動
利用者誤操作／不正行為	利用者	連打・取り忘れなど	・釣銭一括払い出し制限、アラート通知	ユースケース「釣銭の受け取り」備考、シーケンス図（操作ログ）

商品が出ない/誤表示 ⇒ 「FMEAのRPN=140」



原因	要因分類	詳細	対応策（改善案含む）	トレーサビリティ先
商品ラックの詰まり	機器故障	商品が機構内で引っかかる、変形・異物混入	・取り出し機構の定期点検・清掃 ・異物検知センサーの導入 ・ 商品形状の事前チェックルール化	システム構成図（商品払い出し機構）、ステートマシン図（異常検知状態）、ユースケース記述「商品選択と購入」EF-2
商品ラック在庫センサー故障	機器故障	商品があるのに「なし」と誤認識	・センサー二重化 ・異常判定時のアラート ・販売停止制御	システム構成図（在庫センサー）、ステートマシン図（販売可否遷移）、ユースケース記述「商品一覧表示」備考
商品補充忘れ	運用ミス	管理者が補充を怠った	・補充アプリに確認機能 ・遠隔監視での在庫残量確認	ユースケース記述「商品補充」備考、システム構成図（管理者用補充機能）
商品選択ボタン故障	機器故障	押下信号が伝達されない	・入力エラー検出機能追加 ・異常時の販売停止制御	システム構成図（入力デバイス）、ステートマシン図（入力異常検知）、ユースケース「商品選択と購入」EF-3
表示パネル誤表示	機器故障	表示が欠落、誤った情報が表示される	・自己診断機能の実装 ・遠隔監視でのパネル状態監視	システム構成図（表示部）、ユースケース記述「商品一覧表示」EF-1

投入不可・金額誤認識 ⇒ 「FMEAのRPN=96」

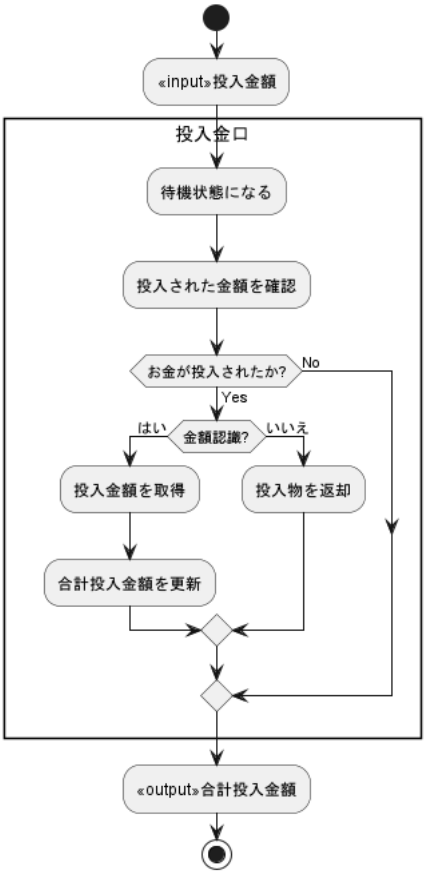


原因	要因分類	詳細	対応策（改善案含む）	トレーサビリティ先
硬貨の詰まり	機器故障	投入口に異物が詰まる	・詰まり検知センサー追加 ・自動返却処理	システム構成図（投入口）、 ユースケース「お金の投入」EF-1
金額認識センサー故障	機器故障	正しく金額を読み取れない	・高精度センサー化 ・再確認処理	システム構成図（認識センサー）、 ユースケース「お金の投入」EF-2
投入口破損	機器故障	硬貨が物理的に通らない	・筐体強化 ・物理保護構造	システム構成図（投入口構造）
不正なコイン投入	利用者操作	外貨や偽造コイン	・磁気・重量判定機能 ・使用不能物の即時返却	ステートマシン図（不正検出遷移）、 ユースケース「お金の投入」EF-3
キャッシュレス認証失敗	通信／認証	通信遅延、IC読み取りエラー	・再試行機能、異常表示	シーケンス図（決済認証）、 ユースケース「お金の投入」備考欄

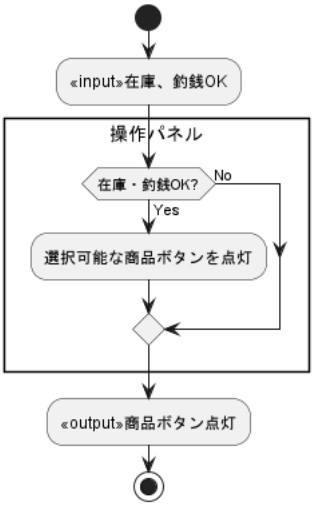
アクティビティ図(機能)

- 各機能の処理手順やワークフローをフローチャート形式で表現します。

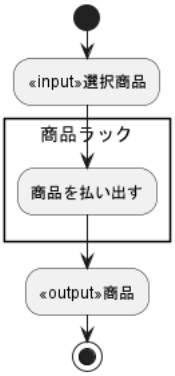
お金投入を監視する



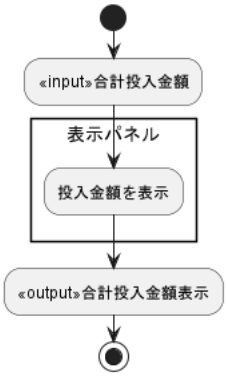
購入可能な商品ボタンを選択可能にする



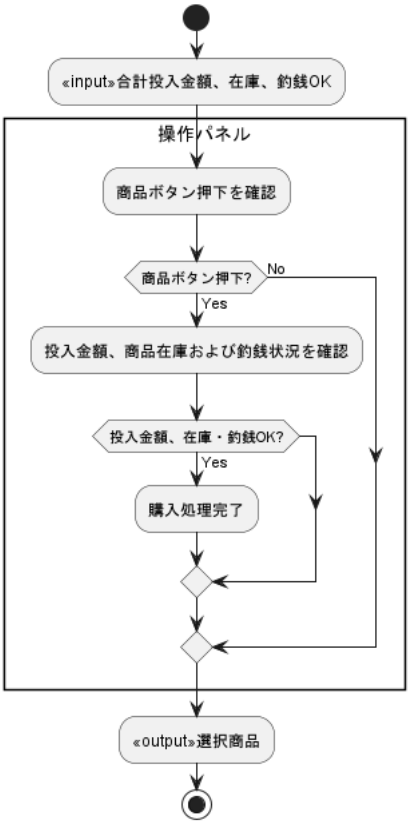
購入商品を払いだす



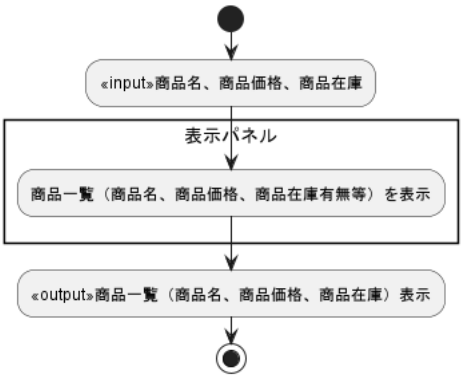
合計投入金額を表示する



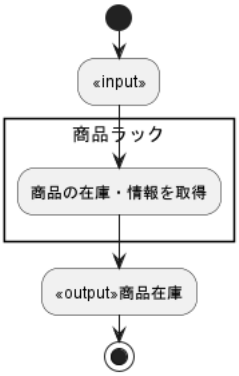
商品ボタン押下を監視する



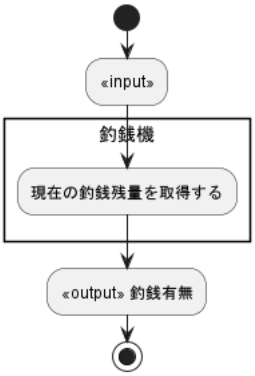
商品一覧を表示する



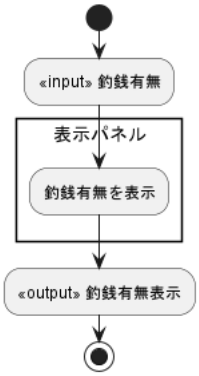
商品在庫を確認する



釣銭を確認する



釣銭有無を表示する



STAMPの考え方に基づく対処

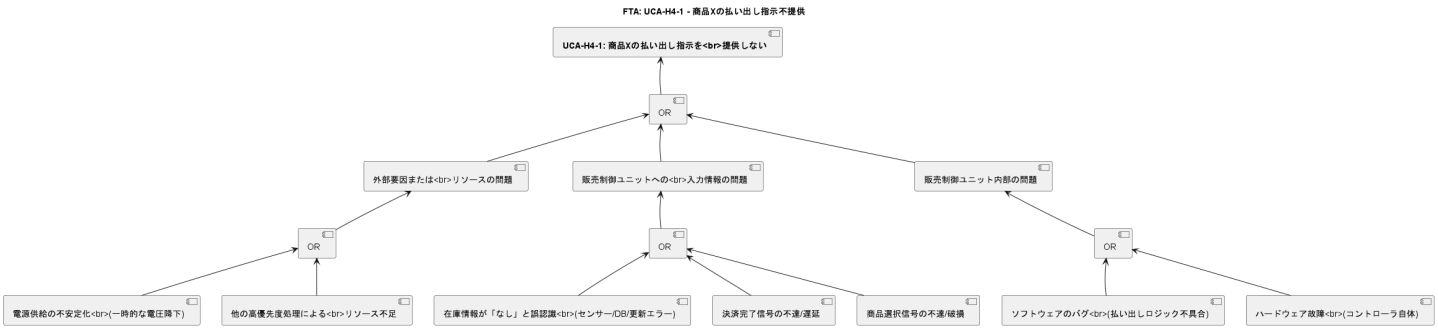
1. UCA（安全でない制御行動）の抽出: 各コントローラの制御行動が、提供されない、提供される、間違ったタイミング/順序、間違った継続時間の場合にハザードを引き起こすかを分析します。
2. 原因分析（Causal Analysis / Loss Scenarios）: UCAが発生するシナリオや原因（なぜコントローラが安全でない制御行動を発行しか、フィードバックの問題、設計の欠陥など）を特定します。
3. 対策と安全制約/要求の導出: UCAやその発生原因を防ぐための対策を検討し、具体的な安全制約や安全要求として定義します。これらが要求図に反映されます。

UCA（安全でない制御行動）の抽出

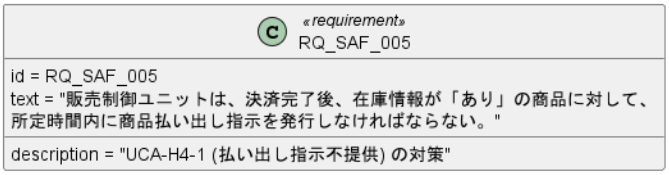
ハザード: H-4 商品誤払い出し・不払い出し
コントローラ: 販売制御ユニット
制御行動: 特定商品（例：商品X）の払い出し指示

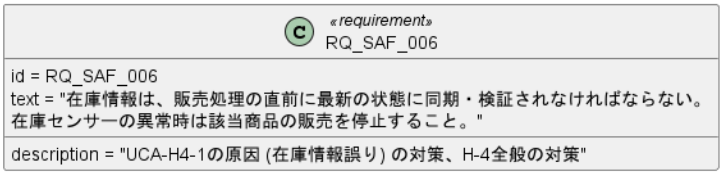
UCA ID	制御行動	安全でない制御のタイプ	UCA記述
UCA-H4-1	商品Xの払い出し指示	提供されない (Not Provided)	決済完了後、在庫があるにも関わらず、 販売制御ユニットが商品Xの払い出し指示を提供しない。
UCA-H4-2	商品Xの払い出し指示	提供される (Provided)	在庫がない、または利用者が商品Yを選択したにも関わらず、 販売制御ユニットが商品Xの払い出し指示を提供する。
UCA-H4-3	商品Xの払い出し指示	タイミング/ 順序が不適切	決済完了前に、販売制御ユニットが商品Xの払い出し指示を提供する。
UCA-H4-4	商品Xの払い出し指示 (モーター制御信号)	継続時間が不適切 (Stopped too soon)	販売制御ユニットが商品Xの払い出しモーターへの制御信号を早期に停止するため、 商品が完全に払い出されない。

原因分析（Causal Analysis / Loss Scenarios）



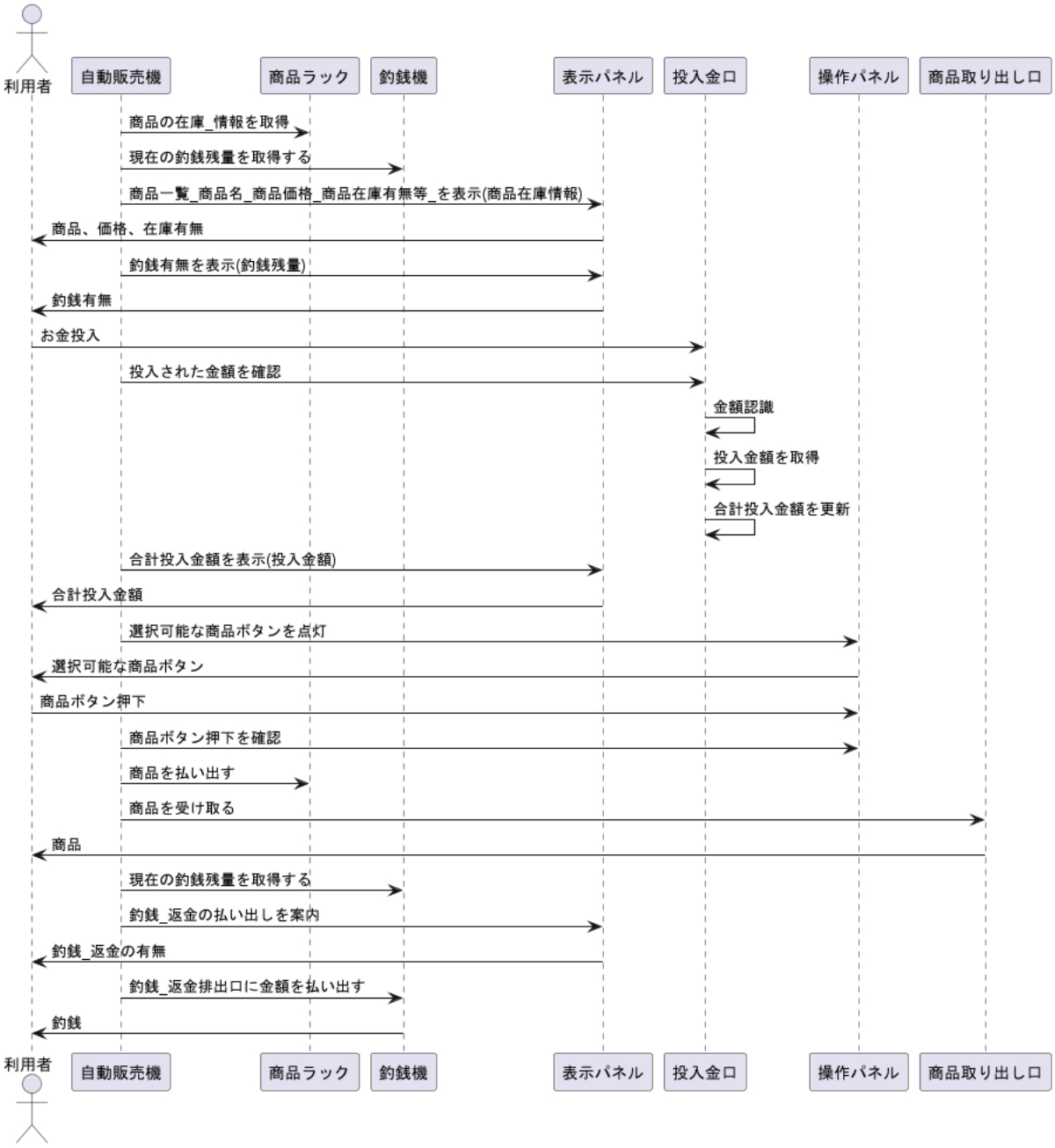
対策と安全制約/要求の導出





シーケンス図_機能検証（シミュレーションによる検証）

- システム内外のオブジェクト間でやり取りされるメッセージや処理の時系列的な流れを示します。
- AIでpythonコードを自動生成し、人手による修正を加えたpythonコードの実行結果です。
  ました



自動販売機モデル 用語集

- 本モデルで使用する用語や概念の定義をまとめています。

アクター (Actors)

用語	概要
利用者 (User):	自動販売機で商品を購入する人物 。お金を投入し 、商品を選択・購入し 、釣銭や返金を受け取ります 。
管理者 (Manager):	自動販売機の運用管理を行う人物 。売上金の回収 、商品や釣銭の補充 、販売商品の変更 、機械の状態確認を行います 。
メンテナンス担当者 (Maintenance Staff):	自動販売機の保守や修理を行う人物 。故障対応を担当します 。

システム (Systems)

用語	概要
自動販売機 (Vending Machine):	このモデルの中心となるシステム 。商品の販売、金銭の授受、在庫管理などを行います。

用語	概要
決済システム (Payment System):	電子マネーやクレジットカードによる決済を処理する外部システム。
在庫管理システム (Inventory Management System):	商品や釣銭の在庫情報、補充情報を連携する外部システム。
売上管理システム (Sales Management System):	売上情報を連携する外部システム。
監視システム (Monitoring System):	自動販売機の状態監視や、障害・異常通知を行う外部システム。

ユースケース / 機能 (Use Cases / Functions)

用語	概要
お金を投入する (Insert Money):	利用者が現金やキャッシュレス手段で支払いを行うこと。
釣銭・返金を受け取る (Receive Change/Refund):	利用者がお釣りや投入金額の返金を受け取ること。
商品一覧を表示する (Display Product List):	自動販売機が購入可能な商品情報を表示すること。
商品を選択し購入する (Select and Purchase Product):	利用者が希望の商品を選び、購入処理を行うこと。
売上金を回収する (Collect Sales):	管理者が自動販売機から売上金を回収すること。
商品を補充する (Replenish Products):	管理者が商品を自動販売機に追加すること。
釣銭を補充する (Replenish Change):	管理者が釣銭用の現金を補充すること。
販売商品を変更する (Change Sales Products):	管理者が販売する商品の種類や価格を変更すること。
機械の状態を確認する (Check Machine Status):	管理者が自動販売機の稼働状況や在庫などを確認すること。
故障対応を行う (Handle Malfunctions):	メンテナンス担当者が故障の調査や修理を行うこと。

内部コンポーネント (Internal Components)

用語	概要
表示パネル (Display Panel):	商品一覧や投入金額、エラーなどを表示する部分。
商品ラック (Product Rack):	商品を格納し、払い出す機構。
釣銭機 (Change Machine):	釣銭の計算や払い出し、残量管理を行う部分。
投入金口 (Money Slot/Input):	現金やカードを受け入れる部分。
操作パネル (Control Panel):	商品選択ボタンなど、利用者が操作する部分。
商品取り出し口 (Product Dispenser/Outlet):	購入した商品が出てくる部分。
売上金庫 (Sales Vault):	回収されるべき売上金を保管する部分。

フロー種別 (Flow Types)

用語	概要
基本フロー (Basic Flow):	ユースケースにおける最も標準的で、成功した場合の処理の流れ。
代替フロー (Alternative Flow):	基本フローから分岐する、別の正常な処理の流れ（例：キャンセル）。
例外フロー (Exception Flow):	エラーや予期せぬ事態が発生した場合の処理の流れ。

その他 (Others)

用語	概要
キャッシュレス決済 (Cashless Payment):	現金以外の支払い方法（電子マネー、クレジットカードなど）。
釣銭レバー (Change Lever):	釣銭や投入金の返金を要求するためのレバー。
在庫切れ (Out of Stock):	商品が売り切れている状態。
釣銭切れ (Out of Change):	お釣りを支払うための現金が不足している状態。

用語	概要
メンテナンスモード (Maintenance Mode):	故障対応などの保守作業を行うための動作モード 。
管理モード (Management Mode):	売上回収や補充など、管理者作業を行うための動作モード 。
ステートマシン図 (State Machine Diagram):	システムの状態とその遷移をモデル化した図 。
ユースケース図 (Use Case Diagram):	アクターとシステムの機能（ユースケース）との関連をモデル化した図 。
アクティビティ図 (Activity Diagram):	システムやビジネスプロセスのワークフローをモデル化した図 。
シーケンス図 (Sequence Diagram):	オブジェクト間のメッセージのやり取りを時系列でモデル化した図 。