エンタープライズ系システムを対象としたSTAMP/STPA分析試行

IPA/SEC IoTシステム安全性向上技術WG委員／日本電気株式会社　向山 輝

1 はじめに

STAMP/STPAが分析対象とするアクシデントは「損失につながるような意図せざる事象」とされている。「損失」の定義には、人命やけがにかかわる損失だけでなく、ミッションの未達や経済的な損失、所有物の毀損なども含まれ、広範囲のシステムが分析対象となる［Leveson2015］。金融、流通、運輸、情報通信などの分野で利用されるエンタープライズ系システムは、社会を支えるインフラの一部となっており、サービスが停止した場合には日常生活や経済活動に大きな損失が生じる。上述のアクシデントの定義に従えば、これらのシステムのサービス停止を「アクシデント」としてSTAMP/STPA分析を行うことは可能であり、分析によって危険要因を認識し、対策を打つことができれば有益である。

しかしながら、これまでに公開されているSTAMP/STPA分析の事例は制御系システムを対象としたものが多く、エンタープライズ系に適用する場合に参考にできる事例がほとんどない。そこで、IoTシステム安全性向上技術WGでは、エンタープライズ系システムにSTAMP/STPA分析を適用する場合のコツや注意点を明らかにすることを目的とした試行を実施した。本編では、実施した試行の概要と、得られた知見について解説する。

2 分析対象とするシステム

分析対象には、多くの人に利用経験があり、仕様を理解しやすいという理由で、ネット通販システムを取り上げる。試行に用いる例題として、表 1に示すような典型的な機能を持つ架空のネット通販を想定する。

表1　分析対象とするネット通販システムの仕様

機 能	内 容
販売管理機能	・利用者からの注文を受けると、在庫管理に引当て指示を出す ・引当て可であれば受注ステータスを「確定」とし、出荷機能に対して出荷指示を出す ・引当て不可であれば受注ステータスを「不可」として利用者に通知する
在庫管理機能	・商品の在庫データ（総在庫数、引当て済み数）を管理する ・引当て指示を受けると、在庫データを確認し、引当て可否を応答する
出荷機能	・出荷指示を受けると、商品をピックアップし、配送機能に引き渡す（出荷する） ・出荷後、在庫データを更新する
配送機能	・出荷機能から商品を受け取り、指示された宛先に配達する

図 1は、表 1に示す仕様を、エンタープライズ系システムの仕様記述でよく用いられるUMLアクティビティ図で表したもので

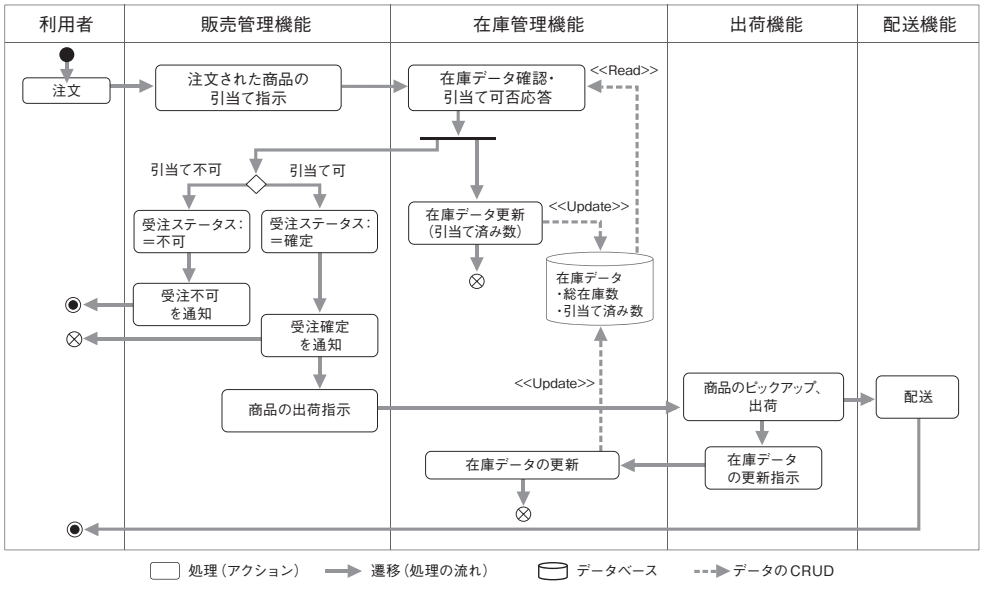

図1　ネット通販システムの仕様を表すUMLアクティビティ図

ある。この図には、データのCRUD※1に関する情報も付記している。本来のUMLアクティビティ図には含まれない情報であるが、各機能間の相互関係を分かりやすくすることを意図したものである。

表1及び図1に示す4つの機能のうち、販売管理機能と在庫管理機能は電子化され自動処理されるものとし、出荷機能と配送機能は人手によって処理されるものとする。

3 STAMP/STPA分析

IPA/SECより公開されているSTAMP/STPAの解説書[IPA 2016]に示される手順に沿い、ネット通販システムの分析の様子を示す。

3.1 Step0 準備1 アクシデント、ハザード、安全制約の識別

アクシデントとしては、期待されるサービスが遂行されず損失を生じる状況が相当する。ネット通販システムの場合は、「注文した商品が利用者に配送されない」ことがアクシデントの一つとして考えられる。

ハザードは、アクシデントにつながる可能性の高いシステムの状態のことであり、今回の分析では「受注が確定した注文に対して商品が出荷されていない状態」とする。出荷が遅れているだけでいずれ出荷されるならアクシデントにはならないが、そのまま忘れられたり、商品が足りなくなったりした場合は、定義したアクシデントにつながる。安全制約は、ハザード状態を起こさないことであり、「受注が確定した注文に対して、速やかに商品が出荷されなければならない」となる。以上を表2にまとめる。

表2 アクシデント、ハザード、安全制約

アクシデント	注文した商品が利用者に配送されない
ハザード	受注ステータスが「確定」である注文に対して、商品が出荷されていない状態
安全制約	受注ステータスが「確定」である注文に対して、速やかに商品が出荷されなければならない

3.2 Step0 準備2 コントロールストラクチャーの構築

コントロールストラクチャーはSTAMP/STPA分析で用いるモデルであり、ここで表現する情報が分析のすべてに反映されるため、どのようにモデル化するかは重要である。しかしながら、モデリングのスキルは属人性が高く、ノウハウを明文化することが困難である。コントロールストラクチャーの構築は、STAMP/STPA分析における最も難易度の高い作業と言える。

今回の試行では、分析対象とするシステムの仕様がアクティビティ図で表現されることに着目し、コントロールストラクチャーの構成要素であるコンポーネント、コントロールアクション、フィードバックデータの3つをアクティビティ図から抽出することを試みる。具体的には次に示す手順である。

(1) アクティビティ図から、安全制約に関係する「処理」を抽出する。

(2) 抽出された処理のうち、その処理から発する矢印(遷移)が機能間をまたぐものについて「コントロールアクションを発行する処理」と「フィードバックデータを発行する処理」のいずれかに該当するかどうかを判定する。

(3) コントロールアクションまたはフィードバックデータに該当する矢印(遷移)の矢元と矢先の機能を「コンポーネント」と識別する。

この手順を図1のUMLアクティビティ図に適用した結果を図2に示す。青く色付けした処理は、表2に示した安全制約が依存

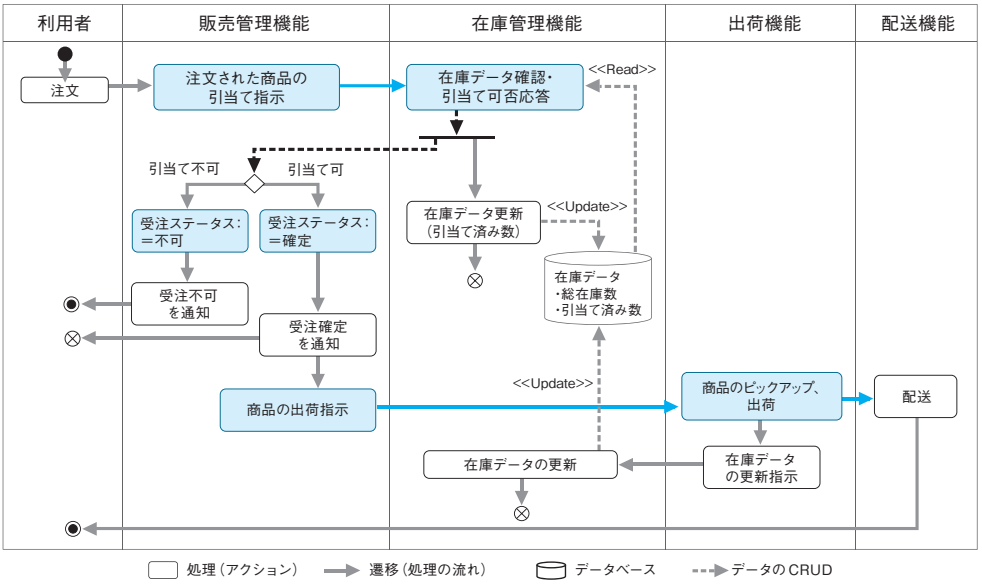

図2 コンポーネント、コントロールアクション、フィードバックデータの識別

※1 データのCreate(生成)、Read(参照)、Update(更新)、Delete(削除)を指す略語

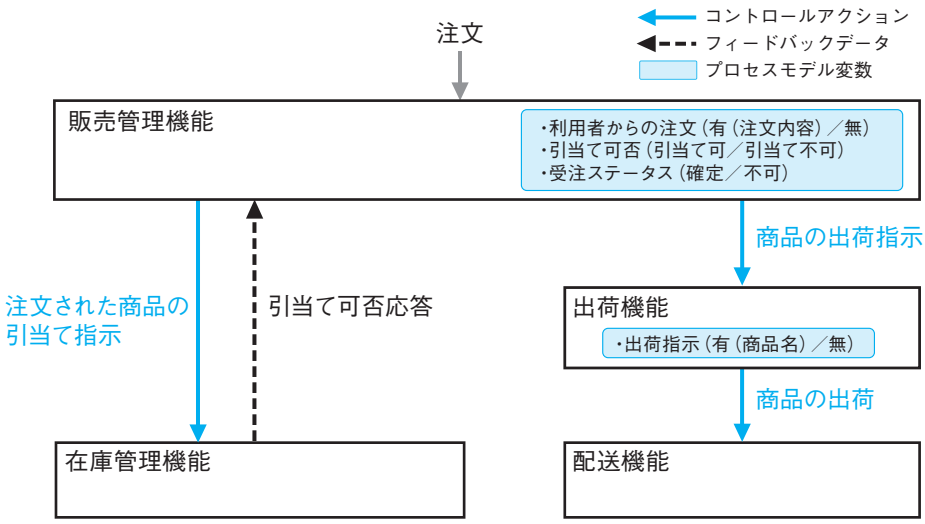

図3　コントロールストラクチャー

する「受注ステータス」と「商品の出荷」にかかわると判断した処理である。これらの処理から発する矢印のうち、機能間をまたぐものは、機能間の相互関係を表すものと考えられる。青で示す矢印はコントロールアクションに相当すると判断されるものであり、黒の破線で示す矢印はフィードバックデータに相当すると判断されるものである。例えば、「注文された商品の引当て指示」は、販売管理機能から在庫管理機能に対するコントロールアクションに相当する処理と解釈でき、「在庫データ確認・引当て可否応答」は、引当て指示のコントロールアクションに対する結果をフィードバックする処理と解釈できる。コントロールアクションとフィードバックデータの矢元と矢先に該当する「販売管理機能」「在庫管理機能」「出荷機能」「配送機能」の4つの機能がコンポーネントに相当する。

このようにして識別したコンポーネント、コントロールアクション、フィードバックデータを用いると、図3に示すようなコントロールストラクチャーを構築できる。プロセスモデル変数は、コンポーネントが認識するシステム内外の状態を表す変数であり、コントロールアクションを実行するかどうかの判断にかかわるものを列挙する。

3.3　Step1　非安全なコントロールアクションの抽出

3つのコントロールアクションのそれぞれに対して、STAMP/STPAが定める4つのガイドワードを利用して、安全制約に反する非安全なコントロールアクション（Unsafe Control Action, 以下UCAと略記）を洗い出す。IPA/SECのWGで実施した試行では7つのUCAを識別したが、本編では紙面の制約上「商品の出荷指示」というコントロールアクションに関するUCAのみを示す（表3）。実際の試行で抽出した7つのUCAは［IPA2017］を参照されたい。

UCAの抽出は、コントロールアクションにガイドワードを当てはめ、それがどのような状況でハザードにつながるかを考えることによって行う。「状況」は、プロセスモデル変数を手がかりとして考える。プロセスモデル変数の値、すなわち、コンポーネントが認識する状況が、現実と食い違っている場合にハザードが起きやすい。例えば、現実には「引当て不可」の状況で、販売管理機能が「引当て可」と誤認識すると、受注ステータスが確定となり「商品の出荷指示」が与えられてしまうが、実際には在庫が足りないため、「受注ステータスが確定にもかかわらず出荷されない」というハザード状態となる。表3に示したUCAのうち、「与えられてハザード」に該当するUCAはこのような分析から導かれる。

表3　抽出されるUCAの一部

コントロールアクション	ガイドワード			
	与えられずにハザード	与えられてハザード	早過ぎ／遅過ぎ／誤順序でハザード	長過ぎる／短過ぎる適用でハザード
商品の出荷指示	受注ステータスが確定となった注文に対して出荷指示が出ない	引当て不可の状況で受注ステータスが確定となり、出荷指示が発行される	受注ステータスが確定となった後、出荷指示が遅れ、速やかに出荷されない	該当なし

3.4　Step2　UCAの原因の特定

Step1で抽出したUCAのそれぞれに対して、その原因を分析する。本編では、紙面の制約上、表3に示したUCAのうち、「引当て不可の状況で受注ステータスが確定となり、出荷指示が発行される」のUCAの原因分析を解説する。

このUCAは、販売管理機能が、現実には引当て不可であるにもかかわらず引当て可と誤認識すると発生する。誤認識の要因の一つとして、在庫管理機能から販売管理機能に入力される「引当て可否応答」の情報が誤っていることが考えられる。

その原因の分析には、図2のアクティビティ図を参照することが役立つ。アクティビティ図の中で、在庫管理機能が引当て可否応答を行う個所に注目する（図4）。引当て可否応答は、在庫データを参照（Read）して行われる。一方、在庫データの一部である「引当て済み数」は、引当てが行われると更新（Update）される。ここで、もしも、在庫データが最新の状態に更新される前に参照されることがあれば、不正確な引当て可否応答が行わ

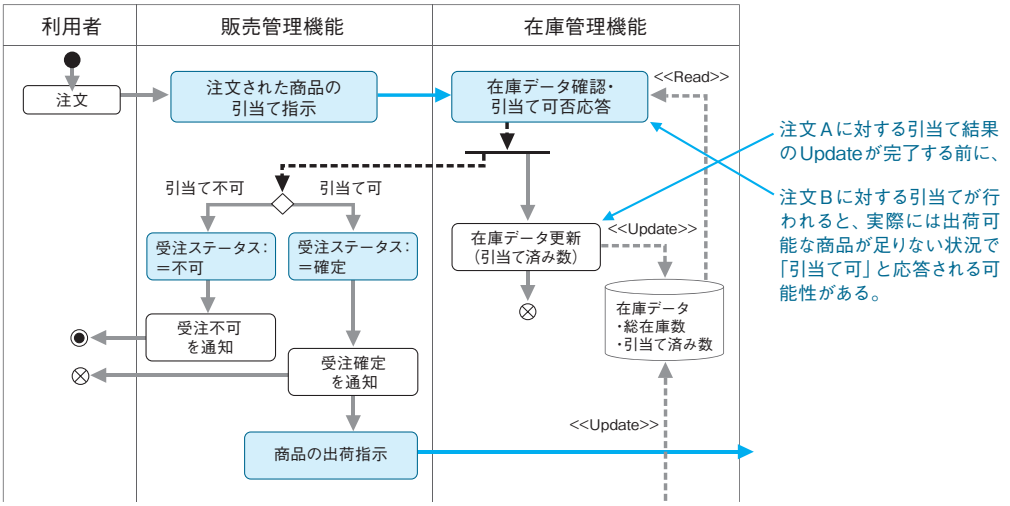

図4　引当て可否を誤認する要因の分析

れる可能性があることに気づく。例えば、注文Aと注文Bの2つを並行して処理するとき、注文Aに対する引当て済み数で在庫データを更新する前に、注文Bに対する引当て指示を受けて在庫データを参照すると、実際には在庫が足りない（引当て不可である）状況にもかかわらず「引当て可」と応答する可能性がある。「引当て不可の状況で受注ステータスが確定となり、出荷指示が発行される」のUCAの原因の一つとして、このようなシナリオが考えられる。

4　試行によって得られた知見

冒頭に述べた通り、本試行は、エンタープライズ系システムにSTAMP/STPA分析を適用する場合のコツや注意点を明らかにすることを目的として行った。この経験から、次のような知見が得られた。

- アクティビティ図で表される情報は、コントロールストラクチャーの構成要素であるコンポーネント、コントロールアクション、フィードバックデータを識別する手がかりとなる。
- Step2のUCAの原因特定には、アクティビティ図の情報が役立つ。とくに、データの更新、参照に関する依存関係に着目することが有効であった。従って、アクティビティ図にはデータのCRUD情報も含まれると良い。
- 分析対象のシステムを構成する機能が、自動処理されるか人手によって処理されるかは、分析に影響するため、明確化されていることが望ましい。

以上の知見は、今回実施した試行の経験から得たものであるが、いずれもエンタープライズ系システムに特徴的な要素に関するものであるため、汎用的に通用するものと予想する。

なお、上記の3番目は、本編で取り上げなかった別のUCAの分析で経験した結果によるものである。架空のシステムを対象としたため、当初、各機能が自動処理か手動処理かが未定であった。その状態で分析を行うと、UCAが現実に起こり得るか否かの判断が難しいことに気づき、第2節に示したような自動処理/手動処理の前提を加えた。自動処理/手動処理の区別が暗黙的には決まりにくいエンタープライズ系に特徴的な注意点と考えられる。

5　まとめ

例題としたネット通販システムとそれにかかわるアクシデントは、冒頭に述べたような「社会インフラのサービス停止」のイメージとは距離があるかもしれない。しかし、エンタープライズ系システムを対象としたSTAMP/STPA分析の特徴を理解し、知見を得る目的としては、今回実施した試行は有意義であった。

また、STAMP/STPA分析の価値について、次のような理解も得られた。本編で示した分析は、従来から行われているアクティビティ図で書かれた仕様のレビューと変わらないようにも見える。しかし、アクティビティ図のどの部分に着目し、どのような問題意識を持ってレビューするかを、レビュアの主観ではなく、システムレベルのアクシデントからトップダウンに導出したUCAの観点で、理由付けと網羅性を持って説明できる点にSTAMP/STPAを用いる価値があるのだと考えられる。

なお、WGで行った分析では、Step2で識別したハザードシナリオに基づく対策の検討や、業務効率を改善することを目的としたSTAMP/STPA分析の応用の検討も行った。詳細は［IPA 2017］を参照いただきたい。

【参照文献】

［Leveson2015］ Nancy Leveson, An STPA Primer v1, 2015.
［IPA2016］ IPA, はじめてのSTAMP/STPA, 2016.
参照先：https://www.ipa.go.jp/files/000055009.pdf
［IPA2017］ IPA, はじめてのSTAMP/STPA（実践編）, 2017.
参照先：https://www.ipa.go.jp/files/000058231.pdf