システム理論に基づく事故分析手法 CAST による情報セキュリティ・インシデント分析

金子朋子[†1] 髙橋雄志[†1] 吉岡信和[†1] 佐々木良一[†2]

概要：複雑なシステムに対する新たな事故分析手法として注目を集めている理論とその安全分析手法に STAMP （System Theoretic Accident Model and Processes）がある.STAMP はシステム理論に基づく事故モデルであり,その主要な手法の１つであり,ハザード分析手法である STPA （System Theoretic Process Analysis）は近年普及展開が図られ,国内外で一定の認知度を得ている.しかし,原因分析手法である CAST（Causal Analysis using System Theory）は STPA と並んで STAMP の主要手法の一つだとされているが,日本国内においてはほとんど認知されていない.情報セキュリティ・インシデント案件「産総研の情報システムに対する不正なアクセスに関する報告」を調査対象とし,CAST の分析手法を用いて事故調査を行い,手法の有効性および課題に対する適用特性を定性的に評価した.また，セーフティの手法を用いてセキュリティの事故分析を行った例は少ない.そこで CAST を用いてセキュリティに関する事故報告書を対象として事故分析を行い,CAST の有効性について検討を行った.

キーワード：STAMP,CAST,セキュリティ・インシデント,事故分析,システム理論

Information security incident analysis by accident analysis method CAST based on system theory

TOMOKO KANEKO[†1] YUJI TAKAHASHI[†1] NOBUKAZU YOSHIOKA[†1]
RYOICHI SASAKI [†2]

Abstract: STAMP (System Theoretic Accident Model and Processes) is one of the theories that has been attracting attention as a new safety analysis method for complex systems. STPA (System Theoretic Process Analysis) is one of its main methods. STPA has been popularized in recent years and has gained a certain degree of recognition in Japan and overseas.However, CAST (Causal Analysis using System Theory), which is a causal analysis method, is hardly recognized in Japan. So we targeted the Information security incident case "Report on unauthorized access to the information system of AIST" for investigation, and accident investigation is carried out using the analysis method of CAST. The effectiveness of the method and the application characteristics of the task were qualitatively evaluated.In addition, there are few examples of security accident analysis using the safety method. Therefore, using CAST, we conducted an accident analysis on security-related accident reports and examined the effectiveness of CAST.

Keywords: STAMP, CAST, Security Incident, Accident Analysis, System Theory

1. はじめに

システムの重要性が増す一方で,システム障害や事故が発生した場合,原因は個々の構成要素の故障に留まらず,構成要素間や,システムと人間との間の複雑な相互作用,さらには悪意を持ったサイバー攻撃に起因することがあり,原因究明が困難になりつつある.本稿では,セーフティとは,偶発的なミス,故障などの悪意のない危険に対する安全を示し,セキュリティとは,悪意をもって行われる脅威に対しての安全を示すものとする.

従来の事故モデルを前提とした事故分析手法では,先入観や偏見による影響や偏りがあり,人への非難が発生し,建設的な議論とならないことに陥りやすい.また事故モデルは,セーフティ分野の考え方なのでそのままセキュリティ分野に適用することが難しい.

複雑なシステムのセーフティを扱う新しい理論として,システム理論に基づく事故モデル STAMP（System-Theoretic Accident Model and Processes）[1]が提唱されている.その主要な手法の１つであり,ハザード分析手法である STPA

†1 国立情報学研究所 National Institute of Informatics
†2 東京電機大学 TOKYO DENKI UNIVERSITY

（System Theoretic Process Analysis）[1]は政府機関などにより広く普及展開が図られ,日本国内で一定の認知度を得ている.しかし,原因分析手法である CAST（Causal Analysis using System Theory）[1] [2]は STAMP の主要手法の一つだとされているが,日本国内においてはほとんど認知されていない.CAST は,MIT 関係者が執筆した論文も様々な手順と記法で表現されており,どの点がどのように良いのか分かりづらい.よって国内でもほとんど論文化はされていなかった.そこで本稿では,まず CAST 手順と概要を明確化をする.

本稿では，産業技術総合研究所（以下,産総研）によって作成された,「産総研の情報システムに対する不正なアクセスに関する報告」[3]（以下,報告書）として公開されているセキュリティ事故事例を対象に,STAMP に基づく事故分析手法 CAST による事故分析と[4]実験を行い,検討･考察をした.CAST はセーフティ分野の分析手法であるが,人間を含むシステムや機能間の相互作用に着目して事故要因／成功要因を分析するという特徴に着目し,セキュリティ事故の分析に適用できることを示す.

本稿は 2 章で STAMP 他各種分析手法と考え方を紹介する.続く 3 章では,セーフティの事故分析手法である CAST の説明と課題を提示する.4 章では情報セキュリティマネジメントインシデントに適用した実験とその結果を示し,5 章では従来手法と比較した CAST の事故故分析手法としての特徴やセキュリティに用いることの意義，社会への影響も含めた階層的モデルの必要性について考察を行う.6 章でまとめや今後の方針について述べる.

2. 関連研究

2.1 STAMP と関連手法

STAMP とはシステム理論に基づく事故モデルであり,STPA は STAMP モデルにもとづく代表的な手法として,ハザード分析を行うものである.前提として,システム事故の多くは,構成要素の故障ではなく,システムの中で安全のための制御を行う要素（制御要素と被制御要素）の相互作用が働かない事によって起きるとし,「要素（コンポーネント)」と「相互作用（コントロールアクション)」に着目してメカニズムを説明し,「アクションが働かない原因」が「コントロールアクションの不適切な作用」に等しいという視点を持つことで原因を有限化している.

STAMP に基づく分析の道具立てプロセスとして,仕様記述,安全性ガイド設計,設計原理などのシステム工学,リスク管理の運用,管理の原則／組織設計の規制を利用する.

手法に,事故／イベント分析(CAST),ハザード分析（STPA[5]）,早期概念分析（STECA: Systems-Theoretic Early Concept Analysis）,組織的／文化的リスク分析,先行指標識別,セキュリティ分析（STPA-Sec[6]）が提示されている.CAST は事故が起きてからイベントとして分析する手法,STPA-Sec は STPA のセキュリティ版である.セーフティとセキュリティを統合する手法としては STPA-SafeSec が提案されている[7].また,脅威分析のコントロールストラクチャー(以下,CS)に STRIDE を適用した事例[8]やハザード分析としてのセーフティ・セキュリティ統合の手法[9]なども提案されている.

2.2 従来の安全モデル

従来の代表的安全モデルは,図 1 のドミノモデルとスイスチーズモデルである.一連の因果関係（以下の原因）はドミノモデルと呼ばれ,このドミノ倒しのどこかに手をかざせば事故を回避できる.原因分析と言われている事故分析の各手法はこの考え方を用いている.スイスチーズモデルと呼ばれ,穴が重なると事故となり予見される.これは個々の穴を塞ぐことで対処される.防御壁や漏れはチーズの穴のようなものである.これは従来の分析方法が,事故連鎖イベントモデルで事故が発生する理由に関する仮定に基づいて構築されているのと同じように従来の安全分析手法（フォールトツリー分析,イベントツリー分析, HAZOP,FMECA 等）の基礎となっている.

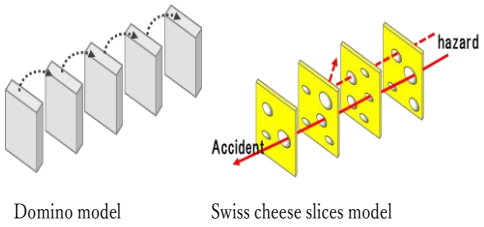

図 1. ドミノモデルとスイスチーズモデル

3. CAST の概要と手順

3.1 CAST の概要

システム理論に基づく原因分析手法である CAST は事前分析手法である STPA とは異なり,STAMP 事故モデルの考えに基づいた事後分析手法である.CAST は事故全体の理解 を可能とするフレームワークとプロセスを提供し,事故の原因分析を安全制御構造の破綻にフォーカスし,先入観や偏見による影響や偏りを小さくする事故分析技術である. CAST の決定すべきゴールは,人々が事故を起こした理由や事故発生を許した安全コントロールストラクチャーの弱点を明らかにすることである.具体的にはコンポーネント間のインタラクションの不備を分析するために,安全制約,発生した非安全なコントロールアクション,その行動の前後関係に基づく理由,それを引き起こしたメンタル（プロセス）モデルを明確化していく.なお,コントローラーには制御するコンポーネントが認識するシステムや外部環境の状態を表すプロセスモデルが含まれており,特に人間が行うプロセスモデルはメンタルモデルと呼ばれている.CAST は下位の物理レベルと上位の論理レベルで分けて考える特徴をもち,事故に関連した安全制約と各レ

ベルの CS を分析することで,様々な観点から分析を行い,事故の要因がどの時点から発生しているかわかるようになっている.

3.2 CAST 手順

参考文献[1]に提示されたアクシデント分析への一般的な STAMP 適用プロセス(CAST 手順)によると CAST の分析は,後述の CAST 1 から CAST 9 まで の手順になる.この分析手順は必ずしも一つが完了してから次のステップへというように逐次 に実施されることを意味するものではない.最初の 3 つの手順（CAST 1-3）はハザード,安全制約,CS 図の明確化であり,全ての STAMP ベース技術で共通に実施する.

CAST 1. 損失に関連するシステムとハザードを明らかにする
CAST 2. ハザードに関連したシステムの安全制約やシステム要求を明らかにする
CAST 3. ハザードを制御し安全制約を課すよう整備されている安全コントロールストラクチャーを記述する.*1
CAST 4. 損失につながる近接したイベントを決定する
CAST 5. 損失を下位（物理）レベルで分析する
・発生した事象に対する次のものの寄与を識別 : 物理的,運用的な操作,物理的な障害,機能が損なわれた相互作用,コミュニケーション,共同作業の欠陥,処理されなかった外乱
・損失を防止するさいに何故,物理的なコントロールが効果的でなかったかを定義
CAST 6. 安全コントロールストラクチャーの上位（論理）レベルに移り,如何にして,そして何故, より上位のレベルが現在（物理）のレベルにおける不適切な制御を許したかもしくは寄与したかを決定する
CAST 7. 損失に関与した共同作業,コミュニケーションの寄与者すべてを調査する
CAST 8. 損失に関連するシステムと安全コントロールストラクチャーの時間経過による 動的な特性や変化,および安全コントロールストラクチャーの長期間での弱化を正確に定める
CAST 9. 改善勧告を出す
*1) これはコントロールとフィードバックの実行と同様に各コンポーネントの構造上の責任と権限を含む.このステップは以降のステップと並行して実施できる.

図 2.一般的な CAST 手順

また一般に CS の各コンポーネントの役割は以下の記述を含む.コントローラーには制御するコンポーネントが認識するシステムや外部環境の状態を表すプロセスモデルが含まれており,特に人間が行うプロセスモデルはメンタルモデルと呼ばれている.

- 安全要求と制約
- コンテキスト：意思決定がされた状況
- 責任と権限
- 環境や行為形成の要素
- コントロール：非安全なコントロールアクション
- 誤ったコントロールアクションをひきおこす機能が損なわれた相互作用,故障,欠陥のある決定
- 欠陥のあるコントロールアクションと機能が損なわれた相互作用の理由
- 制御アルゴリズムの欠陥
- プロセスやインターフェイスモデルの不備
- 複数のコントローラー間の不適切な調整やコミュニケーション
- 参照チャネルの欠陥
- フェードバックの欠陥

図 3. コンポーネントの役割として記述事項

4. 評価実験

4.1. 実験概要

CAST をセキュリティ事故の分析に適用できることや手法としての有効性を示すため,事故調査案件を対象に分析を行い,評価する.

本稿では,産総研の報告書[3]を対象として分析を行う.報告書は,2018 年 2 月に発行された情報システムに対する外部からの不正なアクセスについて被害状況,原因等について整理するとともに,情報セキュリティ対策を取りまとめたものである.なお分析の前提として,分析者は,報告書に記載されている調査結果等の事実を既知情報として入手している上で分析を実施している.

4.2. 実験の目的

本実験の目的は,セキュリティの従来分析（報告書の結論）とは違う観点で問題点を抽出し分析を行うことで,報告内容だけでは見えていない問題を抽出できることをもって有効性を示す.

4.3. 実験の手順

本実験では,分析手順(Step1 から 5)に,参考文献[1]に示される CAST 分析手順(CAST1 から 8)[1]を対応付けし,分析を実施した(図 4).手順をステップに変換したのは分析手順(Step1 から 5)は最近発刊された実務者用ハンドブックに沿っているが,元来の意図も踏まえて分析するためである.

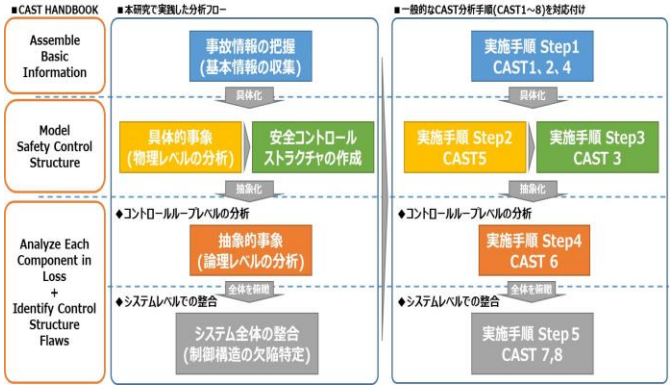

図 4：CAST 分析フロー

【Step1】事故情報の把握（基本情報の収集）

CAST1,2：損失に関与したシステムと分析対象の範囲を定義し,識別したハザードからハザードを防止するために必要なシステムレベルの安全制約を特定する.

CAST4：損失につながるイベントチェーンを究明する.結論付けずまた避難せずに,発生した事象を調査し,各イベントが発生した理由の説明に対して,回答する必要があり

そうな質問を作成する.

【Step2】具体的事象（物理モデルの分析）

CAST5：重要なイベント(障害および安全でない相互作用)とこれらのイベントから生じる質問を特定して,物理的な設計の欠陥と状況要因を説明する.具体的には実際に損失があったコンポーネント単位で,以下 3 つの観点から分析する.

・この事故の防止のためのすべての物理的な安全要件と制約を識別

・物理的な装置のあらゆる故障もしくは不適切な制御を識別

・物理的な故障もしくは不適切な制御を説明するコンテキスト要因を識別

【Step3】安全コントロールストラクチャの作成

CAST3：システムの構成要素間の構造と相互作用を表すために,既存の安全制御構造をモデル化する.

【Step4】抽象的事象（論理モデルの分析）

CAST6：安全コントロールストラクチャで損失があったコンポーネントとその周辺のコンポーネントを抽象的事象と捉え,なぜ不適切な制御に寄与したかを解明するために,以下 4 つの観点から分析を行う.

・抽象化レベルの制御に対する,安全制約の責務を識別

・非安全な決定と制御アクションを識別

・非安全な決定と制御アクションを説明するプロセスモデルの欠点を識別

・その時点でなぜその振る舞いが適切に思えたか説明するコンテキスト要因を識別

【Step5】システム全体の整合（制御構造の欠陥特定）

CAST7：損失の原因となったシステミック要因を調査することで制御構造全体の欠陥を特定する.システム全体を俯瞰し,Step2 から 4 の結果から個々のコンポーネントが個々の安全責任を果たせなかった理由,コンポーネントの動作が一緒になってシステムの安全制約を満たせなかった理由を抽出し,以下 4 つのシステミック要因に分類する.

・情報交換と相互連携

・安全な情報システム

・安全なマネジメントシステムの設計

・安全な文化

CAST8：経時変化により劣化し事故に至る要因となった制御構造全体の欠陥を特定する.CAST7 と同様に Step2 から 4 で抽出した欠陥から,CAST8 のシステミック要因（経時的な変化とダイナミクス）に当てはまる欠陥があるか確認する.

4.4. 実験の結果

Step2 から 4 まではシステムと運用保守,セキュリティマネジメントに分けて分析を行い,Step5 では両方を組み合わせて分析結果をまとめた.

【Step1】事故情報の把握（基本情報の収集）

CAST1,2：産総研の不正アクセス事例は,情報セキュリティに対する意識が低いことで発生した事例であるため,アクシデントを「不正に内部システムに侵入される」と定義し,アクシデントとなりえるハザードとハザードの裏返しとなる安全制約を導き出した結果を表 1 に示す.

表 1：アクシデント/ハザード/安全制約

アクシデント	ハザード	安全制約
A1.不正に外部から内部システムに侵入する	H1.外部から内部システムに入る経路に防御策がない	SC1.外部から内部システムに入る経路に防御策がある
	H2.外部から内部システムの入り口に攻撃を受ける	SC2.外部から攻撃を受けない
		SC3.外部から攻撃を受けていることを検知できる

CAST4：What-Why 分析により,What（何が起きたのか）と Why（原因究明のため明らかにしたいこと）を明らかにし,各イベントが発生した理由に対して,調査の結果回答が必要と思われる質問を生成した結果を表 2 に示す.

表 2：イベントチェーンと質問生成（一部抜粋）

ID	損失に近接する「システム運用保守」上の発生イベント（What？：何が起きたのか）	各イベントが発生した理由の説明に対して、回答する必要があるような質問を作成（Why？：原因究明のため明らかにしたいこと）
0	何らかの手法により職員のアカウントへ不正ログインされた	Q0-1. なぜ、不正ログインを検知できなかったか？
1	外部ネットワークに構築した認証サーバに対して、パスワード試行攻撃（ブルートフォース攻撃）が行われた	Q1-1. なぜ、パスワード試行攻撃を検知できなかったか？ Q1-2. なぜ、認証サーバは外部ネットワークに構築されていたのか？リスクは考慮されていたか？ Q1-3. なぜ、認証サーバのアドレスが特定されたのか？

【Step2】具体的事象（物理モデルの分析）

CAST5：3 点の観点を安全上の責務,非安全なコントロールアクション,意思決定された状況と背景と置き換え,プロセス／メンタルモデルの欠陥も加えて,具体的なコンポーネントに対し,コントロールループを分析した結果を表 3 に示す.

表 3：具体的コンポーネントレベルでの分析（一部抜粋）

●：直接的な要因, ◎：直接的な要因から影響すると思う要因

	システム/運用					セキュリティマネジメント			CAST7				CAST8
欠陥	ログイン認証機能	不正監視機能	内部ネットワークへの侵入	内部システムへのログイン制御	内部システムのアクセス権限付与	マネジメント体制（本部）	マネジメント体制（各研究部門）	情報セキュリティ監査体制	情報交換と相互連携	安全な情報システム	安全なマネジメントシステムの設計	安全な文化	経時的な変化とダイナミクス
攻撃者からの攻撃に対し、監視者は「攻撃は失敗している」と判断した		◎				●		◎		●		◎	◎

【Step3】安全コントロールストラクチャの作成

CAST3：対象システムにおいて,安全を保つために存在したと考えられる CS を作成した結果を図 5 に示す.

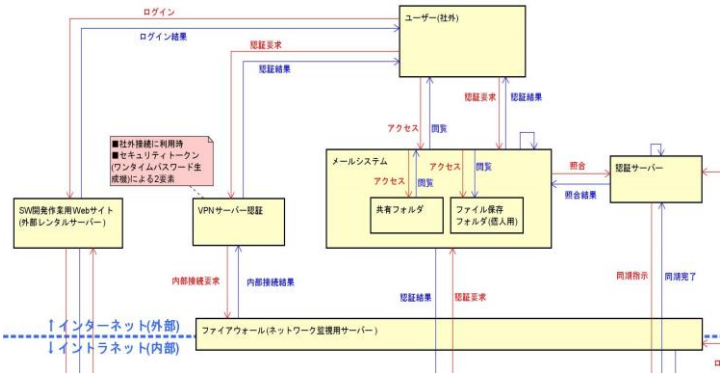

図 5：システムおよび運用保守の安全 CS（一部抜粋）

【Step4】抽象的事象（論理モデルの分析）

CAST6：コンポーネント単体ではなく,複数のコンポーネントが関わり合って発生した事象を抽象的事象と捉え,Step2 と同様に 4 つの観点（安全上の責務,非安全なコントロールアクション,プロセス/メンタルモデルの欠陥,意思決定された状況と背景）を基に分析した結果の一部を表 4 に示す.

表 4：抽象的コンポーネントレベルでの分析（一部抜粋）

No	カテゴリ	インシデント	CAST6-1	CAST6-2
		発生対象	安全上の責務(責任)	非安全なコントロールアクション
2	システム(外部)	内部ネットワークへの侵入	・ログインIDおよびパスワードの照合を行い、ユーザに認証結果を返す。 ・ソフトウェア開発の自動化をサポートするために、X研究サーバ内の仮想マシンを遠隔操作して任意のコマンド実行を行う。 ・FWの内側と外側を接続する場合はしかるべき機関に申請し、所有者・設定・IPアドレスなどを管理する。	・IPアドレスの全域に対してポートスキャンを実施された ・FWが外側から内側のマシンを遠隔操作できた ・逆向き接続の設定を想定外の環境下で使用した ・FWの内側と外側を接続するサーバを構築した際、所定の手続きを行っていなかったため、サーバの存在が隠蔽された

【Step5】システム全体の整合（制御構造の欠陥特定）

CAST7,8：CAST6 で識別した 8 つの抽象化コンポーネント（システム／運用：5 コンポーネント,セキュリティマネジメント：3 コンポーネント）と 4 つのシステミック要因を表 5 のように置き換え,Step2 から 4 で特定した欠陥がどのコンポーネント,どのシステミック要因に当てはまるかを分類した結果を表 5 に示す.

表 5：システムの俯瞰分析（一部抜粋）

No	カテゴリ	インシデント	CAST5-1	CAST5-2
		発生対象	安全上の責務(責任)	非安全なコントロールアクション
1	システム(外部)	メールシステム	・認証サーバでユーザIDおよびパスワードの照合を行い、照合結果がｰ致したユーザのみアクセス許可を与える ・照合結果がｰ致しないユーザにはアクセス許可を与えない ・ログイン用の ID を各職員が独自に決める任意の文字列である「パスワードが二つある」のに近い設計となっていたことから、「リスト型攻撃」に耐えられる想定だった	(1)同一ユーザIDのログイン試行失敗に対して何もしなかった (2)アクセスしているのが正規ユーザか攻撃者か判別できなかった (3)キーボード配列のままのパスワードを許容していた (4)攻撃者からの攻撃に対し、監視者は「攻撃は失敗している」と判断した (5)サーバ所有者(産総研)は攻撃を受けたことに対して何もしなかった (6)正規ユーザが不正ログインされていることに気付かなかった

各欠陥が Step2 から 4 実施時に分類したものを●,Step5 分析で他コンポーネントや他システミック要因に影響する可能性があるものを◎として分類したものである．◎分類はログイン認証機能，不正監視機能，内部ネットワークへの侵入などから多くあがった.Step2 から 4 のコントロールループレベルの分析によりシステムレベルに着目した影響範囲を分析することができた.

この◎がついた他コンポーネントや他システミック要因に影響する可能性があるものについて分析を行うと,事故時の産総研のシステムでは,表 6 のような弱点の傾向がみられ,新たな改善案を導き出すことができた.

表 6：事例の特徴/分析結果と改善案（一部抜粋）

項	特徴	分析から見える弱点	新たな改善案
1	侵入に関するもの	アクセス元の信頼性の欠如 VPNや二段階認証の導入を対策としているが、固定のID、パスワードでは下記手段により解読の可能性があると考えらえる －盗み見 －キーロガー －総当たり攻撃　など	●正規ユーザー認証の強化 認証要求元が、産総研が認めた正式なユーザであることを証明できるを認証要求データに組み込む。 例：ワンタイムパスワードの導入 電子証明書によるアクセス元の信頼性の向上

4.5. 評価

産総研の不正アクセス事例は,システムだけの問題ではなく運用保守やセキュリティマネジメントの点においても欠陥があり,各コンポーネントで顕在化した欠陥の対応策が多かった(表 6).CAST は非安全なコントロールアクション（以下,CA）とコンテキスト要因を同時に分析し,問題の直接原因と問題を発生させる背後要因を抽出できる手順であり,その結果,背後要因に対して報告書にはない新たなリスク・課題の検出ができた.特にマネジメント面は,強化,見直し等の曖昧な表現が多かったが,システミック要因からマイスター認定制度など導入によるスキルアップなど,具体的なシステム上の対応策を導出できた.CAST には“CA はそれが適切と判断して人を含めた各コンポーネントが実行している”という前提があるため,非安全な CA を適切と判断させた状況やその原因に対する議論が中心となり,特定の人のミスであるといった具体的なコンポーネントへの議論の偏りや非難は発生しなくなった.またコンポーネントの判断状況をシステム全体に視野を広げたことで,仮説が自由に発想でき,議論の停滞も少なかった.

表 6. CAST 分析で新たに導きだした改善案（一部抜粋）

被害を発生・拡大させた要因（本文と連動）	6止のための対策(産総研の報告 7.1. 現時点で措置済の対策（応急的対策）	CAST分析で新たに導きだした改善案
6.1.システム・機器の問題		
6.1.1 メールシステムのログイン方法	○外部からはVPN 接続を必須とする運用とし、さらに、内部ネットワークからログインする場合でも、一定期間ごとに二段階認証を求めるよう認証方式を強化した。	●正規ユーザー認証の強化 認証要求元が、産総研が認めた正式なユーザであることを証明できるデータを認証要求データに組み込む。 例：ワンタイムパスワードの導入 電子証明書によるアクセス元の信頼性の向上
6.4.マネジメントの課題		
組織・体制上の課題	対策なし	●意識改革・スキルアップ インシデント訓練に加え、ワークショップやマイスター認定制度など導入などの対策を組み込む。 ●常時監視・常時検知・常時追従が行える仕組みの検討 アクションの頻度を上げ、セキュリティ監査1回のアクションでの差分追従が可能な状況にする 例： ・監視情報をデリーで取得・検知条件を設定値化し、照合を行う ・監査対象の変更の登録箇所を制定し、変更発生時は必要関係部署へ通知する ・監査側のセキュリティ監査内容見直しも適次で行う ●当事者意識の醸成 ゼロトラストネットワークの前提に基づいた設計を行い、その理念を共有することで、責任者に対する当事者意識を育てる

5. 考察

5.1. 事故分析手法としての特徴

CAST は発生した事故の原因を明確にして,以降の事故を予防するための原因分析手法の 1 つである.事故分析のベースとなる考え方は 2.3 節の従来の安全モデルのように因果関係をたどり,原因に対して対処するものである.伝統的に最も用いられているなぜなぜ分析[9]も同様に因果関係を探るものである.しかしその分析手順は「必ず 5 回のなぜを繰り返すなど」長年,各組織で様々な工夫はなされてきたが,原因深堀するための系統だった方式はオーサライズされてはいない.そのため,なぜなぜ分析は局所的な原因自体の深掘りとなることが多い.

CAST ではその手順のうち CAST1 から CAST3 は STAMP に共通の実施事項であり,システム思考によりシステム全体をとらえ,安全制約を明確にし,安全構造を可視化できる CS を記述する.CAST4 で発生した事故の経緯を明確にしたうえで,安全構造の破綻を原因分析を行う.なお CAST4 で行う損失につながるイベントチェーン究明は,ドミノモデル

に基づくなぜなせ分析の一種である.CAST5 から CAST9 の部分はシステム全体を捉えた原因分析に相当すると考えられる.つまり CAST はシステム思考によりシステム全体をとらえ,安全構造を可視化したうえで系統的に原因を行うアプローチをとっている.CAST 分析は事故のあった物理的なコンポーネントに対する他のコンポーネントの要素を洗い出せる空間的な広がりのある原因分析である.そのため,運用上のミスなど,直接の原因のみに焦点が当たりがちな傾向性を回避し,相互作用の検討の中で見逃されがちな原因を見出せる特徴をもつ.「なぜなぜ分析」の適用は簡単に利用でき,問題発生時の原因分析に役に立つ手法であり汎用されているが,複雑化したシステムを対象を本格的に分析したい場合には,CAST の適用／評価も実施していくべきである.

5.2. セキュリティインシデントに用いる意義

CAST はセーフティの事故分析手法であるが,本稿ではセキュリティインシデントへの適用を試みた. セーフティはフィジカル、セキュリティはサイバーを主たす対象としている[11].そこで本稿ではサイバーの相互作用を捉えることでセキュリティも扱えるようにした.従来,IT セキュリティーは発生したインシデントに対する対応が中心であり,そのインシデント対応は主にソフトウェアの脆弱性に対する攻撃にシステム運用段階で対処することである.稿で分析対象にした事例もシステム運用段階でのインシデントである.ミッションクリティカルなシステムでは運用段階でのインシデント発生はその社会的影響は甚大である.また,この事例は IT システムのインシデントであるため,人の生命や健康などセーフティに関わるインシデントになってはいないが,自動運転や医療機器などを含めたシステムのセキュリティ攻撃ではセーフティに影響を与えることが大いに発生しうる.それゆえ,CAST 分析手法を今後,セキュリティに用いることは重要である.

5.3. 社会への影響も含めた階層的モデルの必要性

筆者らはシステム理論に基づく安全性,リスク,事故分析などの様々な分析技術とその技術による取り組みを STAMP S&S として提案している[10] [11]. STAMP S&S は,Safety, Security の統合の他,ソフトウェア, システム,業務（サービス）,組織・事業（ステークホルダ）,社会の 5 階層でモデル化して CS を用い,異なる層へ相互作用分析を行うことも提案している.CAST の特徴は物理層と論理層の 2 段階アプローチである. これは STAMP S&S にあてはまると主に物理層はシステム層,論理層はサービス層 (or ステークホルダ層) に相当する.本稿の実験でもステークホルダ層とサービス層,システム層で主に分析している.今後は, CAST に対してもこの 5 層モデルの考え方を適用し,システムとそのソフトウェア構成のみならず,運用者や管理組織に至るまでの各コンポーネントの責任と役割を吟味したうえで,社会への影響を分析できるようにしていきたい.さらに CAST を用いた発生した事故の詳細な分析をもとに STPA を用いて詳細なリスク分析を連動的に実施していく方法を確立したいと考えている.俯瞰してより普遍性をもって,事故の原因と対策を検討できる CAST は今後の IT セキュリティにおいて,損失を防ぎ,ミッションを達成するのに役立つ役立つと考える.

6. まとめ

本稿では,報告書として公開されているセキュリティ事故事例を対象に,STAMP に基づく事故分析手法 CAST による事故分析を行った.セーフティの手法である CAST を,情報システムのセキュリティ事故分析に適用し,報告書には無い要因や対策を抽出できた.また手法のメリットとデメリットを整理し,どのような場合に有効であるかを示した.今後は 5 章にあげた観点での取り組みを実施していく.

謝辞　適用評価実験の実施にあたり多大なご協力をいただいた，日本科学技術連盟ソフトウェア品質管理研究会（SQiP 研究会）演習コースⅢの 2019 年度研究員の皆様に謹んで感謝の意を表する.

参考文献

[1]Nancy G. Leveson, Engineering a safer world, MIT Press
[2]Nancy G. Leveson, CAST-Tutorial, Nancy-Leveson,Nancy-Leveson_CAST-Tutorial-2017.pdf
[3]国立研究開発法人 産業技術総合研究所,産総研の情報システムに対する不正なアクセスに関する報告,https://www.aist.go.jp/pdf/aist_j/topics/to2018/to20180720/20180720aist.pdf,2018,2019 年 12 月 17 日アクセス確認
[4]SQiP 研究会演習コースIII," CAST と FRAM によるセキュリティ事故分析 ～システム思考とレジリエンス～ ",http://www.juse.jp/sqip/library/shousai/?id=431
[5]STPA handbook, http://psas.scripts.mit.edu/home/
[6]William Young, Nancy G. Leveson. Systems Thinking for Safety and Security, Proceedings of the 29th Annual Computer Security Applications Conference (ACSAC 2013), pp.1-8 2013.
[7]Ivo Friedberg, Kieran, Paul Smith, David Laverty, and Sakir Sezer. STPA-SafeSec: Safety and security analysis for cyber-physical systems, Journal of Information Security and Applications, Volume 34, Part 2, pp.183-196 (2017).
[8]Tomoko Kaneko, Yuji Takahashi, Takao Okubo, and Ryoichi Sasaki," Threat analysis using STRIDE with STAMP/STPA," The International Workshop on Evidence-based Security and Privacy in the Wild 2018
[9]小倉仁志「なぜなぜ分析 実践編」,日経 BP 社,2010/12/6
[10]Tomoko Kaneko, Nobukazu Yoshioka, "STAMP S&S: Layered Modeling for the complexed system in the society of AI/IoT," JCKBSE2020
[11]Tomoko Kaneko, Nobukazu Yoshioka, Ryouichi Sasaki, "STAMP S&S: Safety & Security Scenario for Specification and Standard in the society of AI/IoT," The 2020 IEEE International Workshop on Cyber Forensics in Software Engineering (CFSE)