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～

Security Incident Analysis Using CAST and FRAM
- Systems Thinking and Resilience-

リーダー：三宅　保太朗（DTSインサイト）　　須藤　智子（日立ソリューションズ）
研 究 員：大西　智久（NTTｺﾐｭﾆｹｰｼｮﾝｽﾞ）　　出原　進一（パナソニック）
　　壁谷　勇磨（日立製作所）　　金沢　昇（ﾃｯｸｽｴﾝｼﾞｿﾘｭｰｼｮﾝｽﾞ）
　　中嶋　良秀（ノーリツ）　　西　啓行（富士通）
　　藤原　真哉（NTTｺﾐｭﾆｹｰｼｮﾝｽﾞ）　　山崎　真一（富士ゼロックス）
　　山口　賢人（TIS）
主　査　：金子　朋子（情報セキュリティ大学院大学）
副 主 査：髙橋　雄志（アイダック）
アドバイザー：佐々木　良一（東京電機大学）

研究概要

IoT システムのように，複雑な相互作用をもつシステムにおいては，従来の事故モデルを前提とした分析では十分な再発防止が困難であり，新たな事故モデルに基づく分析が必要となってきている．また，IoT システムにおいてはセーフティとセキュリティを同時に考慮する必要がある．しかし新たな事故モデルによる事故分析事例が少なく，その適用が普及していないのが現状である．本稿では，公開されているセキュリティ事故事例に対して CAST および FRAM を適用し，セーフティ分野の事故分析手法がセキュリティ事故分析に有効であることを示す．さらに，分析を通じて各手法がどのような場合に有効に適用できるかを提示する．

1. はじめに

現代社会は，従来のモノの提供を通じて価値を実現するビジネスから，コトとしてサービスを提供するビジネスモデルへ大きく変化を遂げており，IoT や AI などの先進技術を組み合わせたシステムが本格的に活用され始めている．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．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]や，レジリエンス・エンジニアリングに基づく安全分析手法 FRAM（Functional Resonance Analysis Method：機能共鳴分析手法）[2]が提唱されている．しかし，国内では分析事例の少なさもあいまって，事故分析への適用は普及していない．また，システム開発段階のリスク分析においてセーフティとセキュリティを統合的に扱う手法が提案されているが[3]，事故分析においては両分野を別々に実施しているのが現状である．以上のことより我々は，IoT や AI，人間といった構成要素を含む複雑なシステムに対し，セーフティとセキュリティを垣根なく分析できる，新たな事故分析手法が必要となると考えた．

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（Casual Analysis using System Theory）[4]および，FRAM による事故分析を行った．CAST および FRAM 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．また，分析結果をもとに，各分析手法のメリットとデメリットを整理し，各分析手法の有効性を示す．

2. 関連技術

2.1. STAMP

2.1.1. STAMP/CAST

STAMP は，システム事故は構成要素の故障ではなく，システムの中で安全制御を行う要素と被制御要素間の相互作用(CA: Control Action)が適切に働かないことで起きることを前提としている．CAST (Casual Analysis using System Theory) とは，システム理論に基づく事故モデルの STAMP をベースにした原因分析手法である．

CAST は STAMP に対し，事故全体の理解のためのフレームワークとプロセスを提供し，事故の原因分析をシステムの構成要素と関連する CA の弱点にフォーカスして行う．CAST を用いることで人を含むシステムを構成する要素間の関係性や，システムが置かれた状況（コンテキスト）を考慮したシステム全体への事故分析ができると期待されている．

我々は，CAST はセーフティ分野の分析手法であるが，システムや機能間の相互作用に着目してシステム全体への事故要因を分析するという特徴から，セキュリティ事故の分析に適用できると考えた．

2.2. FRAM

FRAM とは，レジリエンス・エンジニアリングにおける分析手法であり、動的システムにおけるリスクの特定などに用いられる．FRAM では，複数の機能とそれらの関係によって分析対象のモデルを記述し，各機能が互いにどのように影響しているか（機能共鳴）を分析する．FRAM に関連して，Hollnagel は，レジリエント・セキュリティの考え方を発表し，システムのセキュリティ向上のためには，Monitor，Respond，Learn，Anticipate の 4 つの能力 （以下，4 つの能力） の向上が有効であることを主張した[5]．

FRAM を安全分析に適用する上での従来の手法と異なる特徴は，分析対象における失敗事象を予め定義しない点である．レジリエンス・エンジニアリングの考え方において，安全は意図しない入力に対する柔軟性によって実現され，失敗はその柔軟性と他の要因との予期せぬ相互作用によって生じる．FRAM ではこの考え方に基づき，予め失敗事象を定義せず，各機能の関係性及び相互の入出力の変動に着目した分析を行う．野本らは，FRAM を実製品開発における安全分析に応用するための具体的なモデリング手法と評価手法を提案した[6] ．

我々は，このような特徴に着目し，FRAM は，制御系のような動的システムだけでなく，情報システムにおけるセキュリティ事故分析に対しても有効な適用特性があると考えた．

3. 実験概要

CAST・FRAM をセキュリティ事故の分析に適用できること，および，各分析手法の有効性を示すため，共通の事故調査案件を対象に評価を行い，評価結果を比較する．

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」[7]（以下，報告書）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．

4. 適用実験

4.1. CAST を用いた分析

4.1.1. 概要

分析の目的は，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のかを検証することである．

本実験では，図 1 で示すように，Nancy G.Leveson 教授が執筆した CAST HANDBOOK に記載されている分析手順(Step1 から 5)に，一般的な CAST 分析手順(CAST1 から 8)[8]を対応付けし，分析を実施した．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．

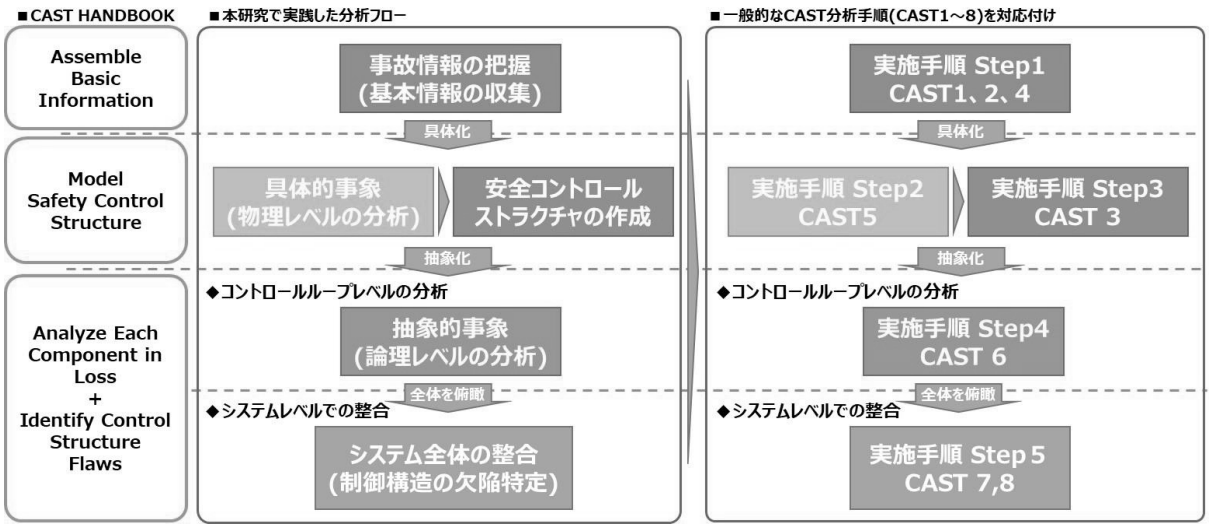

図 1：CAST 分析フロー

4.1.2. 手順

【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．

4.1.3. 結果

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ったため，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、回答する必要がありそうな質問を作成（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）

No	カテゴリ	インシデント発生対象	CAST5-1 安全上の責務(責任)	CAST5-2 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、照合結果が一致したユーザのみアクセス許可を与える ・照合結果が一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が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

【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コントロールストラクチャ(CS)を作成した結果を図 2 に示す．

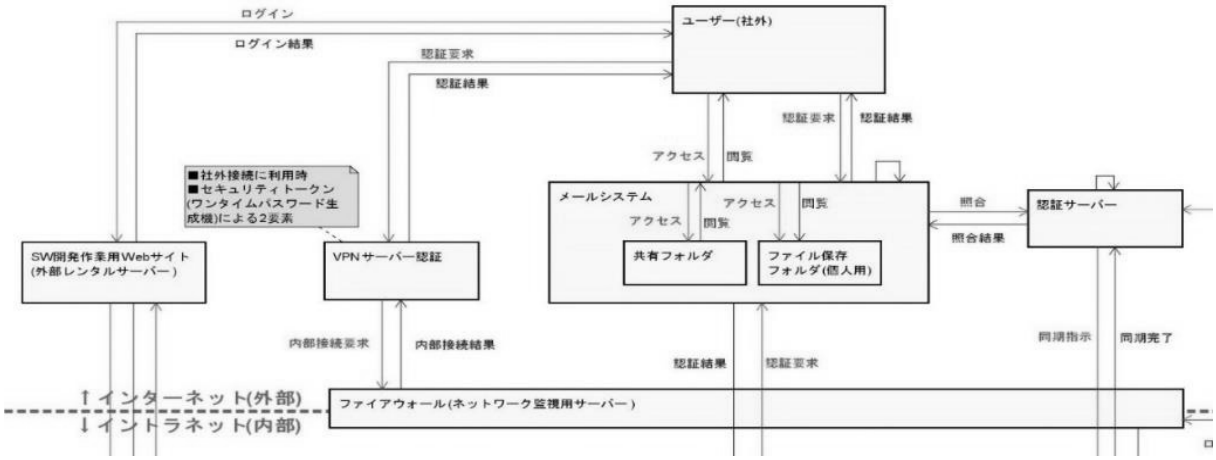

図 2：システムおよび運用保守の安全 CS（一部抜粋）

【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	インシデント発生対象	CAST6-1 安全上の責務(責任)	CAST6-2 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以下のように置き換え，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）

●： 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昇格	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		◎				●		◎		●		◎	◎

各欠陥が Step2 から 4 特定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．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：事例の特徴と分析から見える弱点とその改善案（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れる** **－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

4.1.4. 考察

我々は，CAST 分析の特長である，下記 2 つの観点に対して考察を行った.

I. 新たなリスク・課題は検出できたか

報告書では，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．CAST は非安全な 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改善案を導出できたと考える．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，システム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と考える.

II. 先入観や偏見による影響や偏り、なぜなぜ分析で発生しがちな非難などなく建設的な議論ができたか

CAST は，後知恵の影響を最小限にするため，“コンポーネントは，その CA が適切と判断して実行している”，という前提がある．そのため論理モデルの分析を進めることで，抽象化されたコンポーネントに対して非安全な 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、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と考える．

参考文献[4]が示すようにCAST分析は，従来の事故モデルの再発防止を改善する分析手法であるが，我々は，以下を行うことで未然防止の分析に繋げることができると考える．

・抽象化されたCS図の標準パターン化とそれぞれにCS図に紐づいた事例集の蓄積
・STPAを参考に、STPA/CASTで共用できるガイドワード、ヒントワードの定義

4.2. FRAMを用いた分析

4.2.1. 概要

本実験では，報告書記載の事故事例を対象とし，FRAM を事故内容の説明及び対策案の創出のために用いる．本実験の結果より，課題に対するFRAMの適用特性について考察する．

4.2.2. 手順

本実験では，野本らの提案手法[6]を基底とした，以下の手順を行う．

【手順1】コンポーネントの把握

情報システムを構成する各コンポーネントの役割や性質を把握する．この段階では，重要なコンポーネントを決定しない．

【手順2】各機能の定義

手順1で把握した各コンポーネントについて，機能を抽出する．この際，別コンポーネントで同様の性質を持つ機能がある場合は，1つの機能として抽象化して定義する．

【手順3】モデルの可視化

手順2までに定義した機能をFRAM図にまとめることで可視化する．本実験では，可視化のためのツールとしてFRAM Visualizerを使用した[9]．

【手順4】可視化したモデルを使った分析

手順3で可視化したモデルを俯瞰し，接続数が多い，ループが存在するといった構造的な特徴を持つ機能に着目する．その機能の中から，成功要因となっている機能を選び中心機能とする．また，逆に中心機能が弱点となっている側面はないか考える．必要に応じて，分析対象であるインシデント発生時の攻撃経路をシミュレートする．その結果，攻撃経路において標的とされた機能が実際に中心機能となっているか確認する．

【手順5】対策案の創出とモデルの再可視化

手順4で定義した中心機能に着目しつつモデルと俯瞰し，中心機能が弱点とならないようなモデルになるよう，対策のために機能を追加する．この際，Hollnagelが提案した4つの能力に当てはまる機能を加えられれば加える．対策案を追加した図を再作成した上で俯瞰し，弱点が克服されていることを確認する．

4.2.3. 結果

手順2を実施し，本人認証機能，産総研と各部門のデータ管理機能といった機能を定義した．抽象化の考え方に基づき，いくつかの機能をまとめ，例えば本人認証機能として，メールサーバの利用，業務システムの利用，各部門が管理するサーバへのログインを行う際の各認証につき同様の性質を持つものを1つの機能とした．

手順4において，本人認証機能，産総研と各部門のデータ管理機能の2機能は各機能との接続が多く，実際，利用者や管理者がデータ資産・職員情報に対して比較的自由にアクセスでき，運用における利便性という成功をもたらしていた．そこで，この2機能を中心機能とした．

一方で，本人認証機能のインターネットから直接アクセスできるという性質は，外部の悪意ある利用者から自由に攻撃可能なクリティカルパスとなっていた．産総研と各部門のデータ管理機能は各研究部門の研究者が利用するサーバからもログイン可能であり，サーバからサーバへと次々にログインすることが可能であった．これらの性質は，攻撃者の視点に立った時のシステムの弱点とした．

インシデント発生時の攻撃経路をシミュレートした結果，多くの段階において，中心機能である本人認証機能，産総研と各部門のデータ管理機能に対する攻撃が行われていたことがわかった．

手順5においてモデルを俯瞰し，運用系の機能と，職員が直接利用する機能との間を疎結合の状態にするため，運用系の機能と職員用の機能との間に，運用系→各システムの接続機能を対策

として追加した．さらに，4つの能力のうちMonitor，Learnにあたる機能として，各機能からの通信や認証の処理状況を入力とするモニタと，モニタが収集した情報をもとに学習し，結果によって各機能への遮断要求を出力する学習を追加した．機能の追加と変更を行ったモデル図を俯瞰し，中心機能の弱点が克服されていることを確認した．例えば，利用者と本人認証機能の間に産総研 NW アクセス機能を追加することで，本人認証機能の弱点であった，インターネット経由での攻撃が自由である，という点が克服された

4.2.4. 考察

結果より，産総研 NW アクセス機能などの複数の対策案を創出できた．この対策案は，FRAM のモデル上で接続数の多い 2 機能に着目し，さらにその機能周りのクリティカルパスから弱点に着目したことで創出できたものであり，FRAM 分析特有の構造可視性によって実現できたものである．このことから，FRAM 分析は情報システムの事故分析に有効な適用特性があると考える．

本人認証のための ID とパスワードが，攻撃以前から漏洩していた場合への対策あるいは回避策としては，書式条件付きのパスワード文字列の導入や定期的なパスワード変更による強化が考えられるが，手順 5 のモデルの俯瞰においては，パスワード強度に関する弱点や対策案は発想されなかった．これは，FRAM 分析では機能間の継続的な相互作用に着目しており，特定のタイミングで一度しか発生しない処理については着目しなくなりがちなため，パスワードの初期設定時の処理がモデルに組み込まれていなかったことが原因と考える．

なお，本ケースに対しては，4 つの能力から発想したモニタ，学習によって，以下に示すようにインシデント発生を防ぐことが可能である．漏洩した認証情報を用いて悪意ある第三者が本人認証機能へのアクセスを試みたとする．アクセス試行時の処理状況はモニタに入力され，特徴パターンとして学習に入力される．学習は適切なユーザによるアクセスパターンを学習済みであるので，悪意あるアクセスパターンと学習済みのパターンとの不一致を検知し，本人認証機能に対して遮断要求を出力する．以上のフローにより，認証情報漏洩に伴う不正アクセスを防ぐことができる．

今回，産総研の報告書の記載を確認し，パスワード強度の観点を得られた．これを FRAM モデルに組み込む場合，本人認証機能の前提条件（condition）として追加するのが適切である．追加後の図を俯瞰することでさらなる改善が見込まれる．

情報システムのような静的なシステムに対する FRAM 分析においては，システムを俯瞰的に見ることができ，各機能間での接続数の密度やクリティカルパス，ループ構造といった構造的特徴に着目することで，対策をより深く考えることができると考える．

一方で，FRAM 分析の特徴として，ループ内における頻繁な入出力による相互作用，入出力値の増加や減衰といった変動性があるが，情報システムのような静的なシステムは，基本的に入出力が一方通行になるように設計されていることが多いため，活かすことが難しいと感じた．

4.3. 各分析手法の比較

表 7 に，各分析手法の比較を示す．

表 7：各分析手法で抽出できた要因の比較

被害を発生・拡大させた要因		産総研	CAST	FRAM
① システム・機器の問題	メールシステムのログイン方法	○	◎	◎
	内部サーバと連携していた外部サイト	○	◎	○
	広域でフラットな内部ネットワーク	○	○	○
	内部ネットワークの不十分な監視	○	○	◎
	アクセス制限のなかった管理用ネットワークのサーバの存在	○	◎	◎
	情報機器の脆弱性	○	○	×
② パスワード・暗号鍵の管理と強度の問題		○	◎	×
③ 外部委託業者の管理の問題		○	○	×
④ マネジメントの課題		○	◎	×

◎は報告書の結果に対して要因を多く抽出できたもの，×は要因を抽出できなかったものを表す．CAST では，報告書で抽出されていた要因は全て抽出でき，中でも特に弱点であったと考えられる要因を特定できた．CAST はトップダウンでシステム全体を網羅的に分析する手法であることを示すことができたと考える．FRAM では，強化することでセキュリティが強靭になる要因を特定できた．FRAM はボトムアップで成功要因を特定する手法であると示すことができたと考える．

5. 今後の課題

4.1節のCASTを用いた分析では，時系列的な分析方法が言及されておらず，経時的な変化に対する欠陥を洗い出せなかった．時系列の事象をおさえた上で防護策を検討する必要があるケースでは，イベントツリーなどの時系列事象を正確に把握する別の手法の併用を検討している．

4.2節のFRAMを用いた分析では，今回の検証の過程において，それぞれの分析手法について明確な手順書が存在しておらず試行錯誤や創意工夫により実施する部分が多くあった．分析過程の事象のモデル化においては三者三様のモデルが出来上がり，個人差が大きく発生していた．（モデルとして可視化することで個人のバイアスも可視化され共通認識を構築でき極所解に陥ることが防げたとも考えられる．）抽象化の粒度の定義や分析スコープ境界の定義などに迷いも生じた．今後はセーフティとセキュリティの双方が関連する事例の分析実績を増やし，分析手法のノウハウを蓄積し手順の標準化や分析のガイドラインを提示する必要があると考える．

また，今回は１つのセキュリティ事故事例を２つのチームに分かれて，それぞれCASTとFRAMの単独手法を用いて並行して分析を実施した．CASTはトップダウン型の分析手法，FRAMはボトムアップ型の分析手法であり，分析過程も結果も大きく異なるものであった．今後は双方の手法を融合し，トップダウン・ボトムアップの分析を同時に実施できる手法を確立する，もしくは，分析対象の特徴からより適性のある手法を選択する判断基準を確立することが望まれる．例えば，CASTを用いてトップダウンで俯瞰的／網羅的に分析し，着目すべき機能を抽出，抽出された機能を中心にスコープを絞って，FRAMを用いてさらに別の視点から分析を加えることでレジリエントな対策を立案する方法が望ましいと考える．

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および，レジリエンスに基づく安全分析手法FRAMによる事故分析を行った．セーフティの手法であるCASTとFRAM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．また各分析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，5章で述べた課題に取り組むと共に，更なる分析事例作成，普及展開を図る．

参考文献

[1] IPA，はじめての STAMP/STPA～システム思考に基づく新しい安全性解析手法～，https://www.ipa.go.jp/sec/reports/20160428.html，2020年1月7日アクセス確認

[2] Hollnagel.E，社会技術システムの安全分析―FRAM ガイドブック，2013

[3] 大森淳夫，中嶋良秀ら，セーフティ＆セキュリティ開発のための技術 統合提案と事例作成，日本科学技術連盟 SQiP 研究会分科会報告書，2018

[4] Nancy G. Leveson，CAST HANDBOOK: How to Learn More from Incidents and Accidents，MIT，2019

[5] Hollnagel.E，To Feel Secure or to Be Secure，That Is the Question，2018

[6] 野本 秀樹，FRAM(機能共鳴分析手法)による成功学に基づく安全工学，SEC journal Vol.14 No.1，p.43-49，2018

[7] 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

[8] Nancy G. Leveson，Engineering a Safer World，MIT press，2012

[9] FRAM Model Visualiser (FMV)，the FUNCTIONAL RESONANCE ANALYSIS METHOD，http://functionalresonance.com/FMV/index.html，2020年1月16日アクセス確認