「演習コースⅣ：セーフティ＆セキュリティ」活動報告
“Course for Practitioner IV：Safety & Security”
Activity Report

リーダー：安樂　啓之（ｲﾝﾌｫﾃｯｸ）　　倉田　優輝（日立ｿﾘｭｰｼｮﾝｽﾞ・ｸﾘｴｲﾄ）
研 究 員：杜　馨瓏（ｺﾆｶﾐﾉﾙﾀ）　　伊達　大輝（ｵﾑﾛﾝ）
大谷　雅和（ﾃﾞﾝｿｰｸﾘｴｲﾄ）　　水野　浩之（東芝）
草薙　明彦（ﾀﾞｲﾆﾁ工業）　　堤　智也（TIS）
浜田　泰之（TIS）
主　査　：金子　朋子（創価大学）
副 主 査：髙橋　雄志（日本 AI システムサービス）
アドバイザー：佐々木　良一（東京電機大学）

研究概要
セーフティ・セキュリティの重要性が日々高まる中，我々が抱える業務課題解決に対するアプローチとして，STAMP/STPA，CAST，FTA，ATA 等の各種分析手法を学習した．しかし，実務レベルでの分析を行うためには座学だけでは不十分だと認識した．そこで，各種分析手法を体得するため，業務課題に近い事例を分析した．その結果，課題解決への道筋と継続して必要な取り組みがわかった．さらに各自の理解を深めるため，得られた知見・結果等を共有した．本稿では，各自の取り組みと，そのうち Web システムのセキュリティ要件分析，およびネットワーク機器撤去時の作業リスク抽出について STAMP/STPA を用いて行った結果を報告する．

1. はじめに
我々は，ソフトウェアに関する製品の開発や運用，あるいはそれらの教育や監査の業務を担当している．その中で，IoT 化の進行にともない，セーフティやセキュリティといった安全性に対する考え方や取り組みを改める必要性を感じている．例えば，担当製品の安全性確保のために製品に関係する様々な危険を分析する必要があるが，IoT 化によって担当製品を含むシステムが多様化し，ステークホルダも拡大することで，分析が複雑になってきている[1]．また，従来インターネットに接続しないためにサイバー攻撃とは無縁だった製品をインターネットなどのネットワークにつなげる必要が生まれ，新たにセキュリティ対策が必要となっているが，自分たちの対策に不足がないか不安を感じている．
我々は，本コースで製品を安全に開発するための考え方や分析手法を体系的に学んだ．また，学んだ手法を実事業で活用できるよう，手法を使った分析に取り組み，手法の理解をより深めたことで，前述の課題や不安を解消した．
次章以降では，学んだ手法および各自が実践した分析の事例を紹介する．事例のうち STAMP/STPA（Systems-Theoretic Accident Model and Processes / System-Theoretic Process Analysis）を用いた 2 件については本稿で詳細に紹介し，他は付録にて紹介する．

2. 関連技術
2.1. STAMP (Systems-Theoretic Accident Model and Processes)
STAMP とは，MIT の Leveson 教授が提唱したシステム理論に基づく事故（アクシデント）モデルのことである．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する要素と制御される要素の相互作用が適切に働かない事によって起きるとしている．その前提を持って，要素（コンポーネント）と相互作用（CA：Control Action）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 CA 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手法となる[2]．
2.1.1. STPA (System-Theoretic Process Analysis)
STPA とは，STAMP のアクシデントモデルを前提とし，システムのハザード要因を分析する安全

解析手法である．分析に用いるシステム構成図の抽象度に応じた分析が可能なため，システムの大まかな構成要素が決まる概念設計の段階から適用できる．複数の機器や組織（人間）が，相互作用を行う複雑なシステムにおいて，相互作用に潜むハザード要因を識別する特徴をもち，過去のアクシデント事例データに基づくガイドワードにより網羅的に分析できる．またシステム全体の振る舞いを確認しながら分析できる[3]．

我々は，開発の上流段階から利用できるという特徴やガイドワードによって網羅的に分析できるという特徴が，事前分析による未然防止のためのセーフティ・セキュリティ要件の抽出，および発生した事象を体系立てて網羅的に整理することに役立つと仮定して事例を通して確認を行った．また， STAMP Workbench[4]を用いた効率化の検証や教育コンテンツの作成を通じて手法の理解を深めた．

以下に，STAMP/STPA の手順を示す．

・Step0：

分析対象となるシステムのアクシデント，アクシデントに繋がるシステムの状態または条件一式であるハザード，ハザードを防止するために満たす必要があるシステムの条件または動作を示す安全制約を定義する．その後，対象システムにおいて，安全制約の実現に関係するコンポーネントや，コンポーネント間の相互作用を洗い出し，コントロールストラクチャー（CS：Control Structure）図を作成する．

・Step1：

CS から CA を識別し，4 種類のガイドワードを適用して，ハザードにつながる非安全な CA（UCA：Unsafe Control Action）を抽出する．

・Step2：

UCA ごとに，関係するコントローラーと被コントロールプロセスを識別し，コントロールループ図を作成し，ヒントワードを適用してハザード要因（HCF：Hazard Causal Factor）を特定する．

2.1.2. CAST (Causal Analysis using System Theory)

CAST とは，STAMP のアクシデントモデルを前提とし，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する事故要因分析手法である．事故の要因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特定する．STPA は発生したシナリオだけでなく，損失に繋がる可能性のあるすべての潜在的なシナリオを特定するのに対し，CAST は発生した特定のシナリオのみを特定するのに役立つ[5]．

我々は，事故要因の可視化として既に用いたことのあるなぜなぜ分析手法との比較を行った．

2.2. FTA (Fault Tree Analysis)

JIS Z8115:2000[6]で「下位アイテム又は外部事象，若しくはこれらの組合せのフォールトモードのいずれが，定められたフォールトモードを発生させ得るかきめるための，フォールトの木形式で表された解析．」と定義されている．頂上事象の発生頻度の分析のため，故障原因を論理的にたどる手法．

我々は，分析対象システムの詳細が自明で故障木図の作成に見通しが立っていたことや手法の認知度の高さから，本手法による分析結果を第三者認証機関の認証取得に用いた．

2.3. ATA (Attack Tree Analysis)

FTA と同様の木形式を取るが，故障原因ではなく，攻撃手段を木構造で示す．インシデントに対する原因調査ではなく，主に脅威分析を行うために用いられる．

我々は，STRIDE(Spoofing「なりすまし」，Tampering「改ざん」，Repudiation「否認」，Information Disclosure「情報漏えい」，Denial of Service「サービス拒否」，Elevation of Privilege「権限昇格」の 6 つの脅威観点の頭文字)を用いた脅威分析結果に対し，複数の攻撃行動の関連性を管理する必要性を感じており，本手法を用いた整理内容が有用であると考え具体的な事例に適用した．

3. 実践した手法と事例

本章では，我々が学んだ手法を適応した事例を紹介する．内訳は STAMP/STPA 6 件（事例 1 か

ら 6），STAMP/CAST 1 件（事例 7），FTA 1 件（事例 8），ATA 1 件（事例 9）となる．

- 事例 1：STAMP/STPA を用いた Web システムのセキュリティ要件分析
  AWS(Amazon Web Services)が発行しているリファレンスアーキテクチャをベースとし，いくつかの前提条件を加え，セキュリティ要件の分析の進め方や，対策の立案などを行い，評価を行った．
- 事例 2：STAMP/STPA を用いたネットワーク機器撤去時の作業リスク抽出
  ネットワーク環境撤去時の作業リスク低減のため，STAMP/STPA を用いて体系立てて発生しうる事象を抽出し，その対策を検討した．
- 事例 3：STAMP/STPA による Web アプリケーションソフトウェアのリスク分析
  Web アプリケーションソフトウェア製品に，STAMP Workbench を用いて，DB 及びサーバに対するリスク分析を行い，分析結果を基に取り組むべき対策の検討を実施した．
- 事例 4：STAMP/STPA 教育コンテンツの作成
  教育コンテンツとして「ダム管理用制御処理設備（ダムコン）」をモチーフにした演習課題を通して手法を習得するチュートリアル，および「電動アシスト自転車」をモチーフに hands-on 形式で学ぶ座学教育資料を作成．分科会内で両コンテンツのレビューを実施し，フィードバックを得た．
- 事例 5：STAMP/STPA による不具合分析となぜなぜ分析の比較
  ツールのアンインストール時に，他ツールのレジストリを破壊という不具合に対して，STAMP/STPA を用いた分析を実施した．また，現場でよく使われているなぜなぜ分析と結果を比較して評価した．
- 事例 6：STAMP/STPA による障害分析
  2023 年 10 月 10 日から 11 日にかけて発生した全銀ネットの RC(リレーコンピュータ)障害について，12 月 01 日に発表されたプレスリリース資料[7]等を元に STAMP Workbench を用いて障害とその対策について可視化を試みた．
- 事例 7：CAST による障害分析
  過去発生障害に対して CAST を用いた分析を実施した．障害内容は，検証環境からテストデータを用いて本番接続するインシデントが発生したもの．
- 事例 8：FTA を用いた製品安全に関する脅威の可視化
  FTA を用い，自社製品の第三者認証取得の際に，製品安全に関する脅威を第三者に表現し，第 3 者認証機関の試験に合格した．
- 事例 9：ATA を用いた所定作業におけるサーバへの攻撃構造の可視化
  ATA を用い，サーバ/クライアントモデルのソフトウェアサービスに対するなりすまし攻撃を題材とした．ATA を用いて攻撃ルートの洗い出しと各種行為の関係性（AND，OR）を可視化した．

「事例１と事例２」については次章にて詳細を述べる．

4. 分析事例の紹介

4.1. STAMP/STPA を用いた Web システムのセキュリティ要件分析

4.1.1. 分析概要

STAMP/STPA による非機能要求分析を行い，机上では分からなかった実践のための知見を得ることを目的として分析を行った．分析対象は一般的で応用しやすい AWS のリファレンスアーキテクチャ[8]を参考にした．

4.1.2. 分析手順

本事例の分析にあたり，2.1.1 項の手順に対して一部変更を加え，以下のように分析を行った．

Step0 では，クラウド上に構築された Web システムをベースとし，運用の前提としてサービス提供者，利用者などの関係者の設定，システムのアーキテクチャなどを設定した．その後にシステムやそれを運用する利用者にとって望ましくないことの検討を Step0 のインプットとした．

Step1 では，2.1.1 項の Step1 に従い，分析を実施した．

Step2 では，2.1.1 項の Step2 に従い，分析の後，セキュリティ誘発要因(SCF: Security

Causal Factor)の特定を行った．SCF は，ハザード要因である HCF に対してセキュリティインシデントの要因を区別したものである．SCF については，STRIDE を攻撃者の意図をとらえるためのヒントワードとしてリスクの洗い出しを行った[9][10]．これらのリスクへの対策の検討については，分析にて洗い出された HCF，SCF に対して以下のようにして行った．

(1) 各 HCF，および SCF のリスク対応方針の決定
各 HCF，および SCF に対しての対処方針（回避，軽減，共有/転嫁，受容）を決める．

(2) 4STEP/M[11]に基づく対策の想起と具体的な対策案の立案．

(3) 洗い出した各項目について，表 1 の対策をキーワードとして，対策案を考えて洗い出す．
4STEP/M とは，大きく 4 つの段階（(1)機会最小，(2)最小確率，(3)多重検出，および(4)被害局限）に従った対策のキーワードをヒントとして，漏れなく対策を考え出す方法である．

表 1 4STEP/M

優先度	ステップ	対策
1	(1) 機会最小	やめる（なくす）
2	(2) 最小確率	できないようにする
3		わかりやすくする
4		やりやすくする
5		知覚能力を持たせる
6		認知・予測させる
7		安全を優先させる
8		できる能力を持たせる
9	(3) 多重検出	自分で気づかせる
10		検出する
11	(4) 被害局限	備える

4.1.3. 分析結果

分析を行った結果は下記の通りであった．

- Step0

今回のシステムのステークホルダは外部委託先(システム開発，運用などを実施)/エンドユーザ（提供するサービスを利用）/オーナ（システムの運用主体となる企業）/クラウドプロバイダの 4 者とした．システムのアーキテクチャは，一般的な Web システム構成を前提とした．Step0 で作成した CS 図を図 1 に示す．作成に当たっては，コンポーネントを CS 図に 1 つずつ要素追加しながら，CA を逐次的に追記することで，スムーズにモデルを作成出来た．

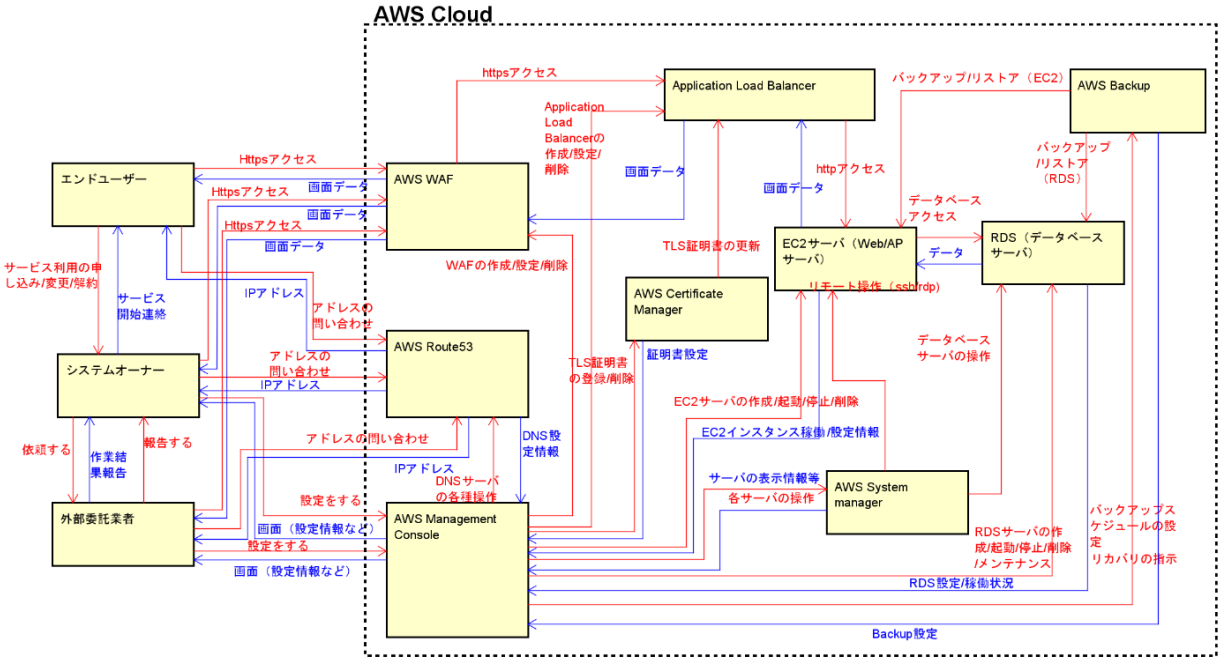

図 1 CS 図

・ Step1
分析の中で，UCA の抽出を行ったものについて，表 2 にその一部を示す．

表 2 UCA の抽出結果（抜粋）

No	CA/From/To	CA提供条件	Type	Description
5	設定をする/外部委託業者/AWS Management Console	システムのメンテナンス操作時	Not Providing	(UCA5-N-1) システムのメンテナンスに関する機能を操作することが出来ないため適切な保守が実施出来ない /[SC11][SC3][SC6][SC8][SC9]
			Providing causes hazard	(UCA5-P-1) 操作を誤ることによって誤ったアプリケーションを配布・動作させてしまう/ [SC1] (UCA5-P-2) 要件を満たさないパスワードの設定が行われる。/ [SC10] (UCA5-P-3) 誤操作により、システムが保有する情報が外部からアクセス可能になる / [SC12] (UCA5-P-4) 誤操作により、誤った検知設定が行われる / [SC13] (UCA5-P-5) 誤操作により、操作履歴（ログなど）が消えてしまう / [SC2] (UCA5-P-6) アクセス権の設定を間違える / [SC3][SC6][SC8][SC9] (UCA5-P-7) 通信許可の設定を誤ることで通信による操作、利用などが出来なくなる / [SC3][SC4][SC5][SC6][SC7][SC8][SC9] (UCA5-P-8) クラウド上のバックアップを誤って削除する / [SC9]
			Too early / Too late	(UCA5-T-1) 不正アクセス監視の問題発生～検知に時間がかかりすぎる / [SC13]
			Stop too soon / Applying too long	

・ Step2
HCF，および SCF の洗い出しを行った．表 3 に HCF/SCF の一部を示す．

表 3 HCF/SCF の抽出（抜粋）

ID	HCF/SCF	ヒントワード	シナリオ
HCF5-N-1-4	ルートユーザでログインしようとしたところ、別のユーザがパスワードを変更してしまいログインが出来ない	(2)コントロールアルゴリズムの生成の欠陥、プロセス変更、不正確な修正や適応	保守作業者A（外部委託業者、あるいはシステムオーナー）がAWS Management Consoleのルートユーザのログイン画面を表示する 保守作業者Aはログイン後、何らかの理由（パスワードの有効期限切れなど）によりパスワードを変更した 保守作業者Aは、パスワード変更に関する内容についての引継ぎを失念した、あるいは保守作業者Bの引継ぎ確認漏れ等の理由により情報の共有がなかった。 保守作業者B（外部委託業者、あるいはシステムオーナー）がAWS Management Consoleのログイン画面を表示する 保守作業者Bは、変更後のパスワードをしらないので、AWS Management Consoleにログインすることが出来ない。
HCF5-N-1-5	成りすましによって、アカウントが乗っ取られてしまい、正規の利用者（保守作業者）がログイン出来ない	(16) Spoofing Identify：なりすまし	攻撃者がパスワードアタック（辞書によるパスワード推測、あるいは総当たり攻撃）によりルートユーザアカウントのID、およびパスワードを入手する 攻撃者はルートユーザによるログインに成功する 攻撃者はルートユーザのパスワードを変更する。 攻撃者は管理権限を持つIAMユーザのアカウントをロックアウト、あるいはパスワードを変更を変更し、ログインをできなくする 保守作業者（外部委託業者、あるいはシステムオーナー）がルートユーザー、あるいはIAMユーザでログインを試みるがパスワードの変更、あるいはアカウントロックアウトによりログインに失敗する

4.1.4. 考察
モデル作成にあたり，予め以下に挙げる前提を決めないと分析が困難になることがわかった．
(1) ステークホルダとその関係
(2) システムのコンポーネント（関係者，システムを構成するサービス構成）
(3) 望ましくないリスクの考え方・前提条件
また，CS 図作成においては，ステークホルダの追加，他のコンポーネントとのつながりを一度に書くのではなく，逐次的に追加することで楽に分析することが出来た．
HCF，SCF の追加，および対策立案は一度 CS 図を作成した後に行ったが，CS 図にコンポーネントを追加しながら，HCF，SCF に逐次統合することによって，分析の複雑さが減るはずである．
対策の立案の為，リスクの扱いを決めてから，4STEP/M を使う方法は本分析手法とは相性が良い．もれなく対策を検討する為には効果的であると感じた．

4.1.5. 課題
今回は分析が目的であったので，作成されたモデルについての品質を担保するためには，洗い出されたリスクやその対策の十分性について検証までは行わなかった．その為，今回の分析に加えて出来上がったモデル，および導かれた内容に対する検証による評価を行いたいと考えている．

4.2. STAMP/STPA を用いたネットワーク機器撤去時の作業リスク抽出
4.2.1. 分析概要
本コースで学習した手法を実践し理解を深めることを目的として，ネットワーク機器撤去作業における作業リスク抽出とリスクへの対策検討を STAMP/STPA を用いて分析する．

4.2.2. 分析手順
本事例の分析手順を以下に示す．なお、前提条件として，分析想定環境には現在稼働中の新基

盤環境（以降，新基盤とする）と，撤去対象である旧基盤環境（以降，旧基盤とする）の 2 つの基盤環境があり，エンドユーザは新基盤を経由してサービスへアクセスすると想定した．また今回の分析では稼働状況に影響するアクシデントのみをリスクとし抽出し，リスクへの対策の検討を目的として分析した．

(1) アクシデント・ハザード・安全制約の設定
(2) 分析対象登場人物の抽出
(3) CS 図の作成
(4) UCA の抽出
(5) HCF および SCF の特定
(6) 対策検討
対策検討後，実際の機器撤去作業時に検討した内容と相違がないかを確認する．

4.2.3. 分析結果

(1) アクシデント・ハザード・安全制約の設定
アクシデントとして，新基盤からネットワーク機器を誤って撤去してしまうケースと，旧基盤のネットワーク機器を撤去した際に想定外のサービス停止を定義し，それにつながるハザード，およびそれを抑止するための安全制約を設定した．

(2) 登場人物の抽出
登場人物として，各基盤およびそれを接続するネットワーク機器，基盤を利用するエンドユーザ，各基盤を設計した設計部署，基盤撤去作業者，作業者の作業の正当性を確認する再鑑者が抽出された．

(3) CS 図の作成
(2)で抽出された登場人物の CA およびフィードバックを整理した結果を図 2 に示す．

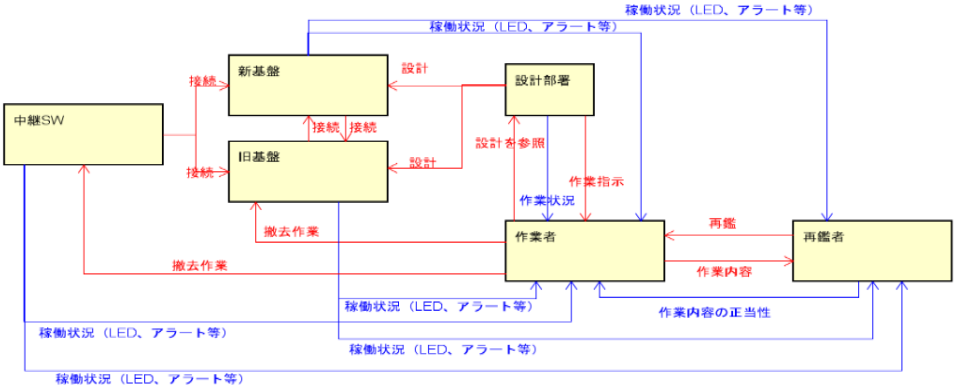

図 2 コントロールアクションおよびフィードバックの整理結果

(4) UCA の抽出，(5)HCF および SCF の特定，(6)対策検討
対策検討結果の一部を表 4 に示す．また，これらの検討結果は，実際の運用作業で策定している対策内容と相違ないことを確認した．

表 4 UCA の抽出，HCF の特定，および対策検討結果一覧

HCF	UCA	対策	対策対象 登場人物
撤去対象機器として事前に確認した機器に誤りがある	撤去予定ではない機器が撤去される	作業前に現地調査および設計書との突き合わせを実施し相違がないかを確認する	作業者 設計部署
作業者の不注意で撤去対象機器とは異なる機器を撤去してしまう		作業対象機器を手と声を出して確認する	作業者 再鑑者
		再鑑者が作業者の作業を確認する	再鑑者
作業者が作業手順書に存在しない手順を実施する	不正な作業手順が実行される	再鑑者が作業者の作業を確認する	再鑑者
作業前に現地調査を実施していない	意図しない通信経路や機器が存在する	作業前に現地調査および設計書との突き合わせを実施し相違がないかを確認する	作業者 設計部署
ケーブルタグ等現地機器の記載情報が古い			
設計書に記載された情報が古い			
設計当初の意図を確認せず設計する	設計時の思想とは異なる経路を作成する	作業前に現地調査および設計書との突き合わせを実施し相違がないかを確認する	作業者 設計部署
作業前の影響調査時に確認する設計書が異なる	誤った設計書を参照し誤った機器が撤去される	設計内で影響調査、資材作成に使用した資材を確認する	作業者 再鑑者 設計部署
ユーザが利用している機器・経路かどうかの確認をせずに撤去する	ユーザが利用しているネットワーク機器・経路が撤去される	作業前に現地調査および設計書との突き合わせを実施し相違がないかを確認する	作業者 設計部署
		撤去前に機器の状態が抜線可能かどうかを確認する・確認する手順にする	作業者 再鑑者 設計部署

4.2.4. 考察

アクシデントやハザード，および UCA を体系的かつ網羅的に抽出できたため，その結果として実際の運用作業と同等の対策を抽出できた．一方，CS 図の作成にあたっての前提情報である，アクシデント，ハザードおよび登場人物の設定が難しく，これらの検討や抽出を何度も繰り返し構築には時間がかかった．よって有用ではあるが，全作業時に検討することは現実的に難しいため，事前に検討されるアクシデントおよびリスクの大小により，適用要否の判断が必要である．

4.2.5. 課題

旧基盤に対する撤去作業では，旧基盤内のネットワーク機器を撤去する．だが，このネットワーク機器には稼働状態を LED や機器へのログインにより事前・作業時に確認できる機器と，そうではない ABC スイッチやパッチパネルなどの機器が混在しているため，現実的な事象への適用のためには複数人の有識者でのレビューや作業者の経験なども必要である．

5. 全体考察と課題

本章では，4 章で紹介できなかった事例についての考察及び課題について述べる．

- 事例 3：STAMP/STPA による Web アプリケーションソフトウェアのリスク分析
  - ○ STAMP/STPA による脅威分析/リスク分析を実施することで，情報漏洩の誘発要因を洗い出して，対策を立てることができた．
  - ○ コントローラーと被コントロールの関係性を固定していないシステムに対して柔軟に分析できる FRAM（Functional Resonance Analysis Method）も利用してみたいと思った．
- 事例 4：STAMP/STPA 教育コンテンツの作成
  - ○ 教育コンテンツについて，理解度，有益度の両面で高評価を得ることができた．
  - ○ 具体的事例を使って，演習・説明をする形式が，高い学習効果を得られることが分かった．
  - ○ 一部の教育コンテンツは，教師を介することを想定していたため，これを読むだけでは，想定した効果が得られない可能性があるとの指摘を受けた．
- 事例 5：STAMP/STPA による不具合分析となぜなぜ分析の比較
  - ○ STAMP/STPA による不具合分析を実施することで，なぜなぜ分析では気づけなかった観点を導くことができた．
  - ○ なぜなぜ分析の結果と比べて，分析結果の抽象度が高いため，具体的な再発防止策を求められる現場で適用するには課題があると感じた．
- 事例 6：STAMP/STPA による障害分析
  - ○ 分析対象の関係の整理が容易になり，対策の漏れに気づきやすいと感じた．
  - ○ 技術的背景のモデル化ができず，障害の発生メカニズムを検証できなかった．

- 事例 7：CAST による障害分析
  - ○ 障害分析手法（CAST）を知り，実践することができた.
  - ○ CAST 分析はモデルを始めに考えなければならないが，なぜなぜ分析はモデルを意識せずに開始できるので，CAST 分析の方が導入のハードルが高いと感じた.
  - ○ 他の手法についても試行して，なぜなぜ分析の代替策となるかを検証したい.
- 事例 8：FTA を用いた製品安全に関する脅威の可視化
  - ○ 第三者認証機関による試験に合格したので，脅威の表現手法として FTA が有効であると証明できた.
- 事例 9：ATA を用いた所定作業におけるサーバへの攻撃構造の可視化
  - ○ 複数の攻撃アプローチと，その攻撃アプローチ中の様々な行動をツリー上に可視化できた.
  - ○ 対策箇所と対策結果の関係が可視化できたので，考えが整理しやすかった.
  - ○ ツリーの依存関係の表現に技能が必要と感じた.
  - ○ 技能に依存せずモデルが作成できるようなフレームワークがあると良いと思った.

6. まとめ

本コースでは，安心安全に関わる様々なテーマについて学び，実際に事例の分析を行った．その結果，2 章で述べた手法を中心に多くの手法に関する知見を得ることができた．また，各種手法を用いた事例の作成，教育コンテンツなどを作成した．今後は 5 章で述べた課題に取り組むと共に，本コースで学んだ技術・手法について理解を深めて，実務経験を通じてスキル向上を図り，システムの複雑性を踏まえ，システム全体を含めた脅威分析/リスク分析を検討する一方で，運用とのバランスを取りつつ，更なる事例の分析や普及展開などを行っていきたい.

参考文献

[1] 独立行政法人情報処理推進機構（IPA）社会基盤センター，つながる世界の開発指針～安全安心な IoT の実現に向けて開発者に認識してほしい重要ポイント～第 2 版，SEC BOOKS，2018
[2] Nancy G. Leveson, Engineering a Safer World: Systems Thinking Applied to Safety, The MIT Press, 2012
[3] 独立行政法人情報処理推進機構（IPA）ソフトウェア高信頼化センター（SEC），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～，2016
[4] 独立行政法人情報処理推進機構（IPA）デジタル基盤センター，STAMP 向けモデリングツール STAMP Workbench https://www.ipa.go.jp/digital/stamp/stamp_workbench.html，2018，2024/1/30 参照
[5] Nancy G. Leveson, CAST HANDBOOK: How to Learn More from Incidents and Accidents, MIT, 2019
[6] JIS Z8115:2000，ディペンダビリティ（信頼性）用語，2000
[7] 全国銀行資金決済ネットワーク・NTT データ，全国銀行データ通信システムの障害について，https://www.zengin-net.jp/announcement/pdf/announcement_20231201.pdf，2024/1/30 参照
[8] AWS，AWS のウェブアプリケーションアーキテクチャ，https://d1.awsstatic.com/architecture-diagrams/ArchitectureDiagrams/web-application-architecture-on-aws-ra.pdf?did=wp_card&trk=wp_card，2023/12/24 参照
[9] 金子朋子・高橋雄志・大久保隆夫・勅使河原可海・佐々木良一，安全解析手法 STAMP/STPA に対するセキュリティ視点からの脅威分析の拡張提案，Computer Security Symposium2017，pp.1273-1279，2017.10
[10] 金子 朋子，セーフティ＆セキュリティ入門 AI，IoT 時代のシステム安全，日科技連出版社，p.61，2021
[11] 河野龍太郎，医療におけるヒューマンエラー 第 2 版 なぜ間違える どう防ぐ，医学書院 p.72，2004