CPSのサイバーセキュリティにおける脅威分析への活用に向けたSTPA-Sec手法の改善

Improving the STPA-Sec Method for Application to Threat Analysis in CPS Cybersecurity

福島祐子

要　約　サイバーフィジカルシステム（CPS）のサイバーセキュリティを確保するには，早期の段階から安全分析を行わなければならない．STPAは早期から適用できる安全分析手法であり，これをセキュリティ向けに拡張した手法としてSTPA-Secが提案されている．しかしSTPA-Secには，分析結果において攻撃シナリオの洗い出しに漏れが生じうるという課題がある．この課題に対して，攻撃の種類の導出を後続の脅威分析に委ねる案を示す．また，STPA-Secには，脅威分析につなぐ方法が示されていないという課題もある．改善案として，STPA-Secの分析結果を脅威分析のデータフロー図の作成や攻撃手法の導出に活用する方法を提案する．

Abstract　Ensuring the cybersecurity of cyber-physical systems (CPS) requires safety analysis from an early stage. The safety analysis method STPA is a method that can be applied from an early stage, and STPA-Sec has been proposed as an extension of this method to address security. However, STPA-Sec has the issue that some attack scenarios may be omitted in the analysis results. In response, we propose to leave the derivation of attack types to subsequent threat analysis. Another issue is that no way for linking the results of STPA-Sec analysis to threat analysis is shown. As an improvement, we propose a method to use the results to create data flow diagrams of threat analysis and to derive attack methods.

1. はじめに

2010年代以降，自動運転車やスマート工場など，様々なコンポーネントがインターネットでつながるサイバーフィジカルシステム（以降，CPS）の活用が広がりつつある．従来の自動車や工場などは外部ネットワークから隔絶していたため，サイバー攻撃にさらされることはまれであった．しかし，CPSではそれらがインターネットに接続されているため，サイバー攻撃を受けやすく，攻撃を受けた場合には物理的に甚大な影響を及ぼす可能性がある．従来のセキュリティではITシステムが中心であり，情報の保護を重視してきたが，CPSのセキュリティでは，情報だけでなく実世界の人や機械，社会インフラなども保護の対象に含めなければならない．

CPSのセキュリティの指針として，経済産業省は，「サイバー・フィジカル・セキュリティ対策フレームワーク」[1]を公開した．この中では，「セキュリティ上の問題が物理的な危害等の安全性に関する問題につながる可能性がある」[1]と述べられている．そして，セキュリティと安全の両立のためには，システム開発の早期の段階から，安全に関するリスク分析を実施し，セキュリティが影響を与える安全性の側面を特定して対応することが重要とされている[1]．

開発の早期の段階から安全に関するリスク分析に適用できる手法として，MIT[*1] の Leveson 教授が開発した安全分析手法 STPA（System-Theoretic Process Analysis）[2, 3] があり，米国を中心に幅広い分野で普及している．そして，STPA をセキュリティへ活用するために拡張した手法として提案されたのが，STPA-Sec である[4]．しかし，その具体的な手法[5]には，分析結果である攻撃シナリオ[*2] の洗い出しに漏れが生じうるという課題（課題 1）がある．また，セキュリティリスクを導出するための代表的な手法である脅威分析につなぐ方法が示されていないという課題（課題 2）もある．本稿では，これらの課題に対する改善案を提示する．まず，2 章で STPA と STPA-Sec の概要について述べ，3 章では課題 1 とその改善案を，4 章では課題 2 とその改善案をそれぞれ提示する．

今後，CPS のセキュリティを検討する上で，脅威分析に先立って STPA-Sec の適用が増えることが予想される．その際に，本稿で述べる改善策は，STPA-Sec を脅威分析に効果的かつ効率的につなげるのに役立ち，CPS のサイバーセキュリティに有用となる．

2. STPA および STPA-Sec の概要と分析ステップ

本章では，STPA と STPA-Sec の概要について述べる．最初に STPA と STPA-Sec の特徴を挙げた後，STPA-Sec で用いる分析ステップについて説明する．

2.1 STPA と STPA-Sec の概要

安全分析手法とは，事故が起きる前に潜在的な事故の原因を識別し，予防や対策に活かすことを目的としたもので[2, 3]，1960 年代以前には，FTA（Fault Tree Analysis）や FMEA（Failure Mode and Effect Analysis）などがあった．ただし，その時代のシステムはハードウエアのみの単純な構成であったため，事故は故障が原因で発生するものという想定だった．その後，システムにソフトウエアや人が含まれるようになり，故障だけでなく不適切な要求や相互作用による事故も増えてきたが，従来の安全分析手法ではそのような新しいシステムを対象としていなかった．こうした背景から，システムの不適切な要求や相互作用による原因を見つけることを目的として，システム理論に基づく安全分析手法である STPA が開発された．

STPA は，米国を中心に欧州やアジアにも広がりつつあり，航空・自動車・医療など様々な分野で活用されている．SAE（Society of Automotive Engineers）[*3]，SOTIF（Safety of the Intended Functionality）[*4] など，STPA を参照する国際的な業界標準も増えつつある[6]．

STPA は，不適切な要求や不適切な相互作用による事故を含めた損失の原因を見つけることを目的としている．その分析には次の特徴がある．

ア）分析の対象とする損失（事故）には，人命の損失，物的損害にとどまらず，環境汚染，ミッションの喪失も含まれる．

イ）分析の抽象度を物理レベルではなく機能レベルに上げて，システムの構成要素をハードウエア，ソフトウエア，人で区別することなく，機能レベルのコンポーネントとして捉える．これにより，コンセプトや要求分析といった開発の早期段階から安全分析ができるようになるため，不適切な要求による事故原因を見つけやすくなる．また，抽象度を上げることにより，識別する原因の網羅性が高まるというメリットも生まれる．つまり，最初から物理レベルのコンポーネントを対象とした場合には，物理レベ

ルの詳細な原因しか識別することができないが，機能レベルのコンポーネントを対象とすることにより，物理レベルの詳細な原因も網羅した機能レベルの原因を捉えることができる．

ウ）事故をコントロールの問題と捉える．コントロールする側の上位のコンポーネントから，コントロールされる側の下位のコンポーネントへのコントロール関係を相互作用としてモデル化し，事故につながる上位コンポーネントのコントロールを識別する．そして，上位コンポーネントが，その事故につながるコントロールを実行する原因を識別する．事故につながるコントロールが実行される主な原因は，上位コンポーネントが認識しているシステムの状態（以降，プロセスモデル）が，実際のシステムの状態と一致しないことにある．ではなぜそのように認識したのか，というように，原因を深掘りすることにより，不適切な相互作用による事故の原因を識別する．

STPA における，事故が発生するプロセスについての考え方は次のとおりである．まず，事故が起きる原因は，安全制約が破られてハザードが発生するためである．安全制約とは，システムが安全に保たれるためのルールであり，ハザードとは，最悪の場合に事故につながるシステムの状態である．ハザードが発生する原因は，上位コンポーネントから下位コンポーネントへの非安全なコントロールが実行されるためである．そして，そのコントロールが実行される主な原因は，先に述べたとおり，上位コンポーネントが持つプロセスモデルが，実際のシステムの状態とは異なることによる．

STPA-Sec は，STPA の分析結果をセキュリティに用いるために，STPA を拡張した分析手法である．サイバーセキュリティ対策において重点的に取り組むべき損失シナリオ（損失につながる因果関係要因を説明するもの）を特定することにより，従来のセキュリティアプローチを強化する[4]．しかし，その具体的な強化方法は，これまで提示されていなかった．

そこで，STPA-Sec の考案者である Young 博士は，STPA で識別した損失シナリオを攻撃者が故意に生じさせるという視点で分析し，攻撃シナリオを導出する具体的な強化方法を示した[5]．本稿では，この具体的な強化方法まで示されたものを STPA-Sec として扱う．

なお，この参考文献[5]では，攻撃シナリオからセキュリティリスクを導出し対策を策定するために，Young 博士が所属する米軍を中心に使われているウォーゲーミング手法[*5] につなぐ方法も提示されている．しかし，日本においてウォーゲーミング手法は「教育されたこともなく，業務に活用したこともない馴染の薄い存在」[7]と称されたこともあり，よりセキュリティリスクの導出に利用されることの多い脅威分析につなぐ方法が望まれる．

STPA-Sec の攻撃シナリオ導出を含む分析手順については次節で説明する．筆者の論文[8]でも STPA-Sec について紹介しているので参考にされたい．

2. 2　STPA-Sec の分析ステップ

STPA の分析ステップは Step1 から Step4 までの四つに分かれている．STPA-Sec では，STPA の 4 ステップに加え，攻撃シナリオを導出するためのステップ（Step5）を実施する．

STPA-Sec の分析ステップの概要を以下に示す．

Step1：分析目的の定義

分析の目的として，受け入れがたい損失（事故）を定義し，システムのハザード，安全制約を識別する．

Step2：コントロールストラクチャの作成

システム全体の機能レベルのコンポーネントを特定し，コントロールストラクチャ（Control Structure．以降，CS）によりコンポーネント間のコントロール関係を明確にする．

安全制約を守るためのコンポーネントの責任を明らかにし，コントローラ（上位コンポーネント）からコントロール対象のプロセス（下位コンポーネント）へのコントロールアクション（Control Action．以降，CA）を識別する．

Step3：非安全な CA の識別

CA がハザードにつながる条件（タイミングなど）を導出し，非安全な CA（Unsafe Control Action．以降，UCA）を識別する．

Step4：損失シナリオの識別

UCA につながる原因（不適切なプロセスモデルなど）を識別することで，ハザードを引き起こし損失につながるシナリオ（Loss Scenario．以降，LS）を識別する．

Step5：攻撃シナリオの導出

サイバー攻撃を行う攻撃者の立場から，Step4 で識別した LS を実現するための攻撃の影響，ターゲット，種類，目的，タイミングを攻撃シナリオとして導出する．

これ以降，攻撃シナリオをウォーゲーミング手法につなげる．

3. 課題 1：攻撃シナリオ漏れの可能性がある

STPA-Sec では LS から攻撃シナリオを導出するが，分析結果として導出される攻撃シナリオの洗い出しに漏れが生じうるという課題がある（課題 1）．本章では，参考文献[5]で示された「空中給油」を題材とした STPA-Sec の分析例を用いて，課題 1 の原因とその改善案を提示する．最初に，STPA-Sec の分析例を説明し，その後，原因と改善案を述べる．

3. 1 STPA-Sec の分析例

参考文献[5]で示された，航空機における「空中給油」を題材とした STPA-Sec の分析例について説明する．空中給油とは，給油機が装備するブーム（給油機から受油機に対して給油するために伸ばして接続するパイプライン）を操作して受油機（給油を受ける航空機）に接続し給油する方式である．空中給油を行うことで受油機の航続距離を増やすことができるが，難易度が高く，事故のリスクがある．なお空中給油は，人間がブーム制御装置（BCU）を介して物理的なブームを操作する CPS と捉えることができる．

分析例の抜粋を以下に示す．

Step1：分析目的の定義

空中給油を分析対象としたときの，損失，ハザードは以下のとおりである．

損失：人の死傷，航空機の損傷，給油ミッションの喪失

ハザード：航空機が給油のための最小間隔に違反

航空機の機体の完全性（性能を維持する能力）の低下

Step2：CS の作成

空中給油の中心となるブーム操作を対象とした CS を示す（図 1 左）．楕円で囲んだ CA は，Step3 で示す UCA の分析例の対象である．

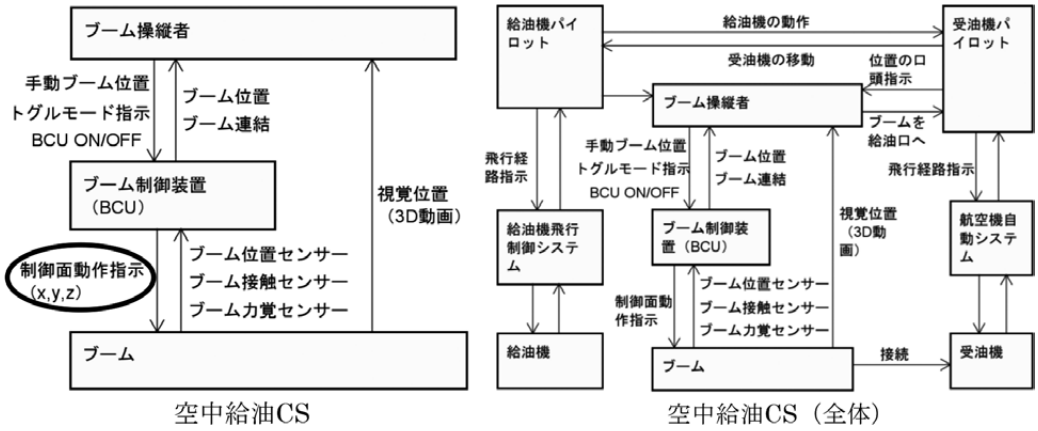

図 1　空中給油 CS

最終的には，ブーム操作を取り巻く，給油機や受油機を含めたシステム全体の CS を作成する（図 1 右）．

Step3：UCA の識別

「ブーム制御装置（BCU）」から「ブーム」への「制御面動作指示」（図 1 左の楕円で囲んだ CA）を対象とした，ハザードにつながる UCA を示す．今回の UCA は以下となる．

UCA1：ブームが受油機に接触しているのに，BCU が必要以上の動作指示を出す

Step4：LS の識別

UCA1 の原因の一つとして，不適切なプロセスモデルによる原因「BCU は，ブームが接触しているのに接触していないと認識している」を導出し，識別したシナリオを示す．今回の LS は以下となる．

LS1：パルスのフィードバックの遅延により，BCU は，ブームが接触しているのに接触していないと認識し，必要以上の動作指示を出す

Step5：攻撃シナリオの導出

まず，攻撃者がプロセスモデルを不適切にするため，つまり「ブームが接触していないと認識させる」ための，攻撃対象の要素，攻撃の影響，攻撃の種類を導出する（表 1）．種類の導出には，脅威モデル STRIDE[*6] を適用する．

表 1　空中給油の攻撃対象の要素，影響，種類

要　素	影　　響	種類
ブーム接触センサー	パルスのフィードバックの遅延	DoS 改ざん
ブーム制御装置	ブーム接触センサーのパルスの処理の遅延	DoS

次に，攻撃者による攻撃の効果が高いタイミングを識別する．ここでは「ブームが接触しているとき」というタイミングで，「ブームは接触していない」と認識させるように攻撃すると効果がある，といった分析をする．

まとめると，攻撃シナリオの一つとして，以下が導出される．

攻撃シナリオ 1：攻撃者は，ブームが接触しているときに，BCU に必要以上の動作指示を出させるために，ブーム接触センサーに対してパルスのフィードバックを遅延させるように Dos 攻撃を行う．

3. 2　課題 1 の原因と改善案

STPA-Sec では，攻撃シナリオを導出する段階で，STRIDE を適用して攻撃の種類を導出する．3. 1 節で示した空中給油の分析例では，Step5 で攻撃の種類として「DoS」，「改ざん」まで導出している．しかし，STRIDE はもともと，「IT のシステムの脅威を洗い出す目的で考案された手法」[9]であるため，CPS の場合には，センサーなどの IoT 機器に対する不正アクセスや不正改造などの脅威を抽出することが難しい．したがって，STPA-Sec において STRIDE のみを使って攻撃の種類の導出まで行うと，攻撃の手段を限定し過ぎてしまう．これが課題 1（攻撃シナリオ漏れの可能性がある）の原因である．なお，経産省の「脅威分析及びセキュリティ検証の詳細解説書」では，STRIDE では抽出されない脅威も存在するため「STRIDE 以外の手法も組み合わせて脅威抽出の網羅性を向上させることも検討するべき」とされている[9]．

課題 1 に対する改善案として，STPA-Sec で導出する攻撃シナリオには STRIDE による攻撃の種類を含めず，後続の脅威分析において脅威を抽出する際に，STRIDE 以外のモデルも組み合わせて攻撃の種類（手段）を導出することを提案する．つまり，3. 1 節で示した分析例では，攻撃の種類（Dos，改ざん）の導出を Step5 で行っていたが，これを STPA-Sec では行わず，後続の脅威分析に委ねるということである．こうすることで，STRIDE のみで攻撃の種類まで導出することにより起こりうる，攻撃シナリオの導出漏れを防ぐことができる．

3. 1 節で示した空中給油の分析例に，上記の改善案を取り入れた分析例を示す．攻撃シナリオ 1 については，具体的な「Dos」の文言を除き，次のように記載する．

攻撃シナリオ 1′：攻撃者は，ブームが接触しているときに，BCU に必要以上の動作指示を出させるために，ブーム接触センサーに対してパルスのフィードバックを遅延させるように，攻撃を行う．

攻撃シナリオを上記のように記述することで，このシナリオでは，「Dos」などの具体的な攻撃の種類まで導出せずに，「ブーム接触センサーに対してパルスのフィードバックを遅延させる」攻撃を行うことだけが表される．このように，記述の抽象度を上げることにより，攻撃の種類の導出を，後続の脅威分析に委ねることができる．なお，脅威分析における攻撃手段の導出については，4 章で述べる．

3.3　課題 1 の改善案に関する考察

3.2 節では，STRIDE のみでは抽出できない脅威があること，それが課題 1（攻撃シナリオの導出で漏れが生じる可能性がある）の原因であることを述べた．また，それに対する改善案として，STPA-Sec の攻撃シナリオには攻撃の種類を含めず，脅威分析において STRIDE 以外のモデルも用いて攻撃手段を導出する案を提示した．

この改善案により，攻撃シナリオの抽象度が上がり，網羅性が高まることになる．そしてこれを，脅威分析における攻撃ツリーのルートノードに設定し，STRIDE 以外のモデルを適用することにより（4.2 節で後述），攻撃の種類の漏れを減らすことが期待できる．

なお，本改善案では，セキュリティ専門家が実施する脅威分析に先立って，STPA-Sec の分析を実施することを前提としている．そのため，STRIDE 以外のモデルも用いた攻撃手段の導出を，後続の脅威分析に委ねることにした．一方で，脅威分析そのものを STPA-Sec に取り込むという考え方もあり得る．その場合には，STPA-Sec の攻撃シナリオ導出の段階から，セキュリティ専門家の参加が必須となる．

4.　課題 2：脅威分析につなぐ方法が示されていない

STPA-Sec は，STPA をセキュリティ向けに拡張するために，攻撃シナリオを導出し，ウォーゲーミング手法につなぐ方法を提示している[5]．しかし，セキュリティリスクを導出するための代表的な手法である脅威分析につなぐ方法は示されていないという課題がある（課題 2）．そこで本章では，3 章で述べた課題 1 に対する改善案を取り入れた上で，STPA-Sec を脅威分析につなぐ方法を改善案として提示する．

脅威分析のアプローチとして，経産省の脅威分析手法[9]，米国の航空機・宇宙船の開発製造会社である Lockheed Martin が考案した Threat Driven Approach[10]，OWASP が公開している Thread Modeling Process[11]などがある．これらのどのアプローチもデータフロー図（Data Flow Diagram．以降，DFD），STRIDE，攻撃ツリー[*7] を使用している点が一致しており，このようなアプローチが脅威分析として一般的であると考えられる．本章では，その代表として経産省の脅威分析手法[9]を紹介し，その手法に STPA-Sec の結果をつなげる方法を提案する．

4.1　経産省の脅威分析手法

経産省の脅威分析手法[9]の手順は，次のとおりである．

- 資産の洗い出し
  作成した DFD に基づき，脅威分析の対象と守るべき資産を洗い出す．
- データフローの可視化
  詳細なデータの入出力を知るために，DFD を作成し，データフローの可視化を行う．
- 脅威の洗い出し
  守るべき資産に対してどのような脅威が発生しうるか，STRIDE を用いて洗い出す．
- 攻撃手法の調査
  攻撃ツリーを用いて，脅威を実現する攻撃手法を調査する．攻撃者の目標を攻撃ツリーのルートノードに配置する．

4.2　課題2に対する改善案

課題2に対する改善案として，STPA-Secを脅威分析につなげる方法を提案する．STPA-Secのそれぞれの分析結果を，4.1節で示した脅威分析の手順につなげる方法は次のとおりである．

a）損失を，資産の洗い出しに利用

STPAのStep1で識別した損失には，利害関係者にとって失いたくないもの，価値のあるものが記載されている．それらは，脅威分析における守るべき資産に相当するため，資産の洗い出しに利用する．

b）CSを，DFD作成の入力として利用

STPAのStep2で作成した，全体的なCSで洗い出したコンポーネントやCA/フィードバックを，脅威分析で作成する初期のDFDに反映する．たとえば，CSのコンポーネントがDFDのエンティティやプロセスになり得るか，また，CSのCAやフィードバックがデータフローになり得るかを検討する．CSの広範な分析範囲を，セキュリティリスク分析に反映することにより，幅広く脅威の洗い出しができるようになる．

c）攻撃シナリオを，攻撃ツリーのルートノードに設定し，攻撃手段を導出

STPA-SecのStep5で導出した攻撃シナリオを，攻撃ツリーのルートノードに設定する．攻撃シナリオにおける攻撃のターゲットと影響を，ルートの次の階層（サブルート）に設定し，攻撃手段の分析に利用する．一方で，攻撃者は攻撃シナリオにおける攻撃タイミングを知らなければならないことから，これをサブルートに設定し，攻撃タイミングを知る手段も分析する．3.2節で示したとおり，攻撃手段および攻撃タイミングを知る手段の分析においては，STRIDEだけではなく，MITREのCAPEC[*8]やATT&CK[*9]などの，物理面も対象としたモデルも利用する．

課題2に対する改善案の全体像を図2に示す．

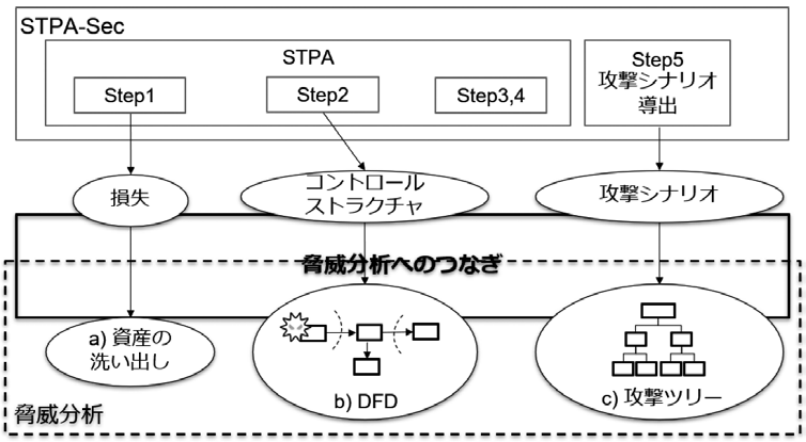

図2　課題2に対する改善案の全体像

4.3　課題2に対する改善案の適用例

4.2節で述べた改善案の適用例を示す．3.1節で示した「空中給油」を題材としたSTPA-

Sec の分析結果を入力とした改善案 a），b），および 3.2 節で示した改善案による攻撃シナリオ 1′ を入力とした改善案 c）の適用例は以下のとおりである．

a ）損失を，資産の洗い出しに利用

3.1 節の Step1 の分析結果「損失：人の死傷，航空機の損傷，給油ミッションの喪失」から，資産として「人，航空機，給油ミッション」を洗い出す．

b ）CS を，DFD 作成の入力として利用

3.1 節の Step2 の CS（図 1 右）で導出したコンポーネント，CA/フィードバックを，初期の DFD に反映する（図 3）．

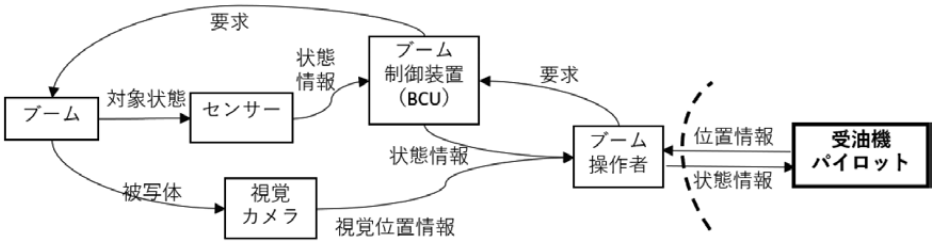

図 3　空中給油の DFD（初期）

たとえば，CS の「ブーム操作者」，「受油機パイロット」などのコンポーネントを，DFD のエンティティとして記述する．また，「受油機パイロット」から「ブーム操作者」への CA「位置の口頭指示」から，「位置情報」といったデータフローを導出する．「受油機パイロット」と「ブーム操作者」の間に信頼境界（破線曲線）を引き，「受油機パイロット」が攻撃者の候補（太線の四角）であることを示す（図 3）．

c ）攻撃シナリオを，攻撃ツリーのルートノードに設定し，攻撃手段を導出

3.2 節で示した改善案による攻撃シナリオ 1′ を，攻撃ツリーのルートノードに設定する．攻撃シナリオにおける攻撃のターゲットと影響「ブーム接触センサーに対してパルスのフィードバックを遅延させる」をサブルートに設定し，これを基に攻撃手段を分析していく．一方で，攻撃シナリオにおける攻撃タイミングである「ブームが接触している」ことを知ることを別のサブルートに設定し，これを基に，攻撃タイミングを知る手段も分析する（図 4）．

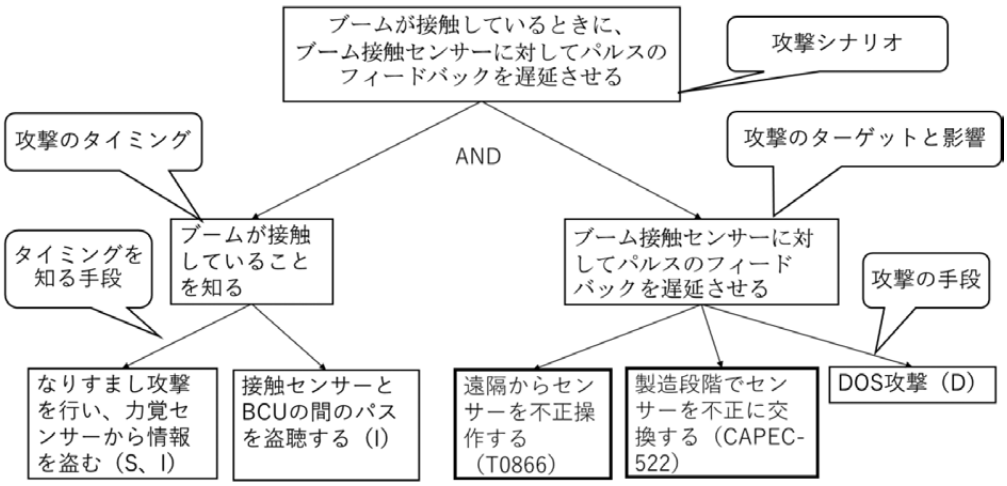

図 4　空中給油の攻撃ツリー

攻撃手段および攻撃タイミングを知る手段の分析においては，STRIDE のほか，MITRE の ATT&CK，CAPEC も使用する．たとえば図 4 では，「ブーム接触センサーに対してパルスのフィードバックを遅延させる」ための手段として，ATT&CK の「T0866：リモートサービスの悪用」を参照することにより「遠隔からセンサーを不正操作する」，あるいは，CAPEC のサプライチェーン攻撃領域における「CAPEC-522：悪意のあるハードウエアコンポーネントの交換」を参照することにより，「製造段階でセンサーを不正に交換する」というように，STRIDE では導出が難しい手段を導出することができる．

4. 4　課題 2 の改善案に関する考察

課題 2 に対して 4.2 節で提示した改善案は，3.2 節で示した課題 1 に対する改善案である STRIDE 適用を脅威分析に委ねた点を除き，STPA-Sec に変更を加えていない．そのため，開発の早い段階で分析できるという STPA-Sec のメリットを維持できる．

改善案 b）では，CS を入力として DFD を作成する方法を提示した．STPA による CS は，システムを取り巻く環境までも含む．そのため，これを参考にして DFD を作成することで，分析範囲を広範に捉えることができ，脅威をより幅広く捉えられる．

改善案 c）では，攻撃シナリオを攻撃ツリーのインプットにする方法を提示した．攻撃シナリオに，攻撃の影響以外に攻撃のタイミングが含まれている点は STPA-Sec の特徴である．改善案 c）によって，脅威分析において，攻撃シナリオに含まれている攻撃のタイミングも加えた分析ができるようになる．

5. お　わ　り　に

従来のサイバー攻撃は情報流出などのデータの被害が多かったのに対して，最新の事例ではイラン核燃料施設のウラン濃縮用遠心分離機破壊[12]に見られるような機器損壊とそれに伴う操業停止や，ウクライナの大規模停電[12]のようなインフラの停止に伴う企業のビジネスや人命に対する影響，さらには事業継続を脅かすランサムウエアによる攻撃など，様々な被害をもたらすサイバー攻撃が増えている．それに伴い，サイバーセキュリティ対策のために脅威分析の導

入が進むことが予想される．しかし，脅威分析は IT システムを主な分析対象としており，物理的なシステムや，事業などのミッションは分析の対象から外れてしまうことがある．一方で STPA-Sec は，人命や物理的なシステム，および，システムを超えた事業・ミッションの損失をも対象としている．そのため，STPA-Sec を脅威分析につなぐことにより，分析の対象範囲，ひいては対策の範囲を広げることができる．したがって，CPS のセキュリティリスク分析においては，脅威分析に先立って STPA-Sec による分析を実施することと，本稿で提案した改善案を活用することを薦める．

なお，本稿では CPS のサイバーセキュリティを対象とした STPA-Sec の適用をテーマとしたが，STPA-Sec は IT システムのセキュリティにも有効である．従来，IT システムでは攻撃者がどのように侵入するかという観点の分析が中心であったが，STPA-Sec では，仮に攻撃者に侵入されたとしても，損失につながるアクションが起きないようにコントロールすることに重点を置き，システム全体を俯瞰して相互作用を分析する．そのため，堅牢なセキュリティ・バイ・デザイン[*10]を実現することができる．

今後，CPS も含め，IT システムはますます複雑化していく．そのようなシステムのセキュリティや安全性を守るためには，従来の手法だけでは限界がある．STPA や STPA-Sec の手法はそうした未来の状況における希望の光であり，国内にも広まることが望まれる．本稿が，この新しいアプローチの普及や発展の一助になれば幸いである．

最後に，本研究にご協力いただいた関係者各位，本稿の執筆にご指導いただいた皆様に，深く感謝申し上げる．

＊1　MIT（Massachusetts Institute of Technology）：マサチューセッツ工科大学
＊2　攻撃者の立場から，一連の攻撃の流れや手順を示したもの．
＊3　モビリティ専門家を会員とする米国の非営利団体．
＊4　ISO21448 で定義されている意図した機能の安全性の規格．
＊5　米軍を中心に使われている，軍事戦略における意思決定を訓練するためのアプローチ．
＊6　Microsoft 社による脅威を識別するための 6 種類の分類（なりすまし，改ざん，否認，情報漏洩，DoS 攻撃，権限昇格）．
＊7　攻撃者がどのようにして脅威を達成するかを可視化する手法．
＊8　CAPEC（Common Attack Pattern Enumeration and Classification）：MITRE が公開するセキュリティ攻撃パターンを網羅的に分類したもの．https://capec.mitre.org/
＊9　ATT&CK（Adversarial Tactics, Techniques, and Common Knowledge）：MITRE が公開するサイバー攻撃の戦術やテクニックなどを攻撃のライフサイクル別に整理・体系化したもの．https://attack.mitre.org/
＊10　システムの企画・設計段階からセキュリティ対策を組み込み，初期段階から安全性を確保する考え方．

参考文献
［1］ 経済産業省，「サイバー・フィジカル・セキュリティ対策フレームワーク」，2019 年，p.31-47，https://www.meti.go.jp/policy/netsecurity/wg1/cpsf.html
［2］ Leveson, N. G., “Engineering a Safer World”, MIT Press, 2012（兼本，福島監訳，『システム理論による安全工学』，共立出版，2024 年）
［3］ Leveson, N. G. and Thomas, J. P., “STPA Handbook”, 2018,（白坂ほか訳，http://psas.scripts.mit.edu/home/get_file2.php?name=STPA_handbook_japanese.pdf）
［4］ Young, W., Leveson, N. G., “Systems Thinking for Safety and Security”, Proceedings of the 29th Annual Computer Security Applications Conference (ACSAC 2013), 2013, p.1-8
［5］ Young, W., “BASIC INTRODUCTION TO STPA FOR SECURITY (STPA-SEC)”, MIT 2020 STAMP Workshop, 2020, http://psas.scripts.mit.edu/home/wp-content/uploads/2020/07/STPA-Sec-Tutorial.pdf

［6］ Thomas, J. P., “STPA in Industry Standards”, MIT STAMP Workshop, 2020, http://psas.scripts.mit.edu/home/wp-content/uploads/2020/07/JThomas-STPA-in-Industry-Standards.pdf
［7］ 岸本覚，「Wargaming」，エア・アンド・スペース・パワー研究，防衛省・自衛隊，第 10 号，2023 年，p.77，https://www.mod.go.jp/asdf/meguro/center/aspw10/aspw06.pdf
［8］ 福島祐子，「CPS のサイバーセキュリティに求められる安全分析と STPA-Sec の有効性」，BIPROGY 技報，BIPROGY，通巻 149 号，Vol.41 No.2，2021 年 9 月，https://www.biprogy.com/pdf/tec_info/14902.pdf
［9］ 経済産業省，「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き 別冊 1 脅威分析及びセキュリティ検証の詳細解説書」，2021 年，p.9-12，https://www.meti.go.jp/policy/netsecurity/wg3/2_bessatsu1_20210419.pdf
［10］ Muckin, M. and Fitch, S. C., “A Threat-Driven Approach to Cyber Security”, Lockheed Martin Corporation, 2019, https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Threat-Driven-Approach.pdf
［11］ Larry Conklin, “Threat Modeling Process”, OWASP community, https://owasp.org/www-community/Threat_Modeling_Process
［12］ IPA 産業サイバーセキュリティセンター，「安全・安定操業を脅かしたサイバー攻撃事例 10 選」，IPA，2021 年 6 月，https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2021/hjuojm0000004uyq-att/000092521.pdf

※ 上記参考文献に示した URL のリンク先は，2026 年 1 月 28 日時点での存在を確認.

執筆者紹介 福 島 祐 子（Yuko Fukushima）
1985 年，日本ユニバック（株）入社．大規模システム開発プロセス，エンタープライズ・アーキテクチャ開発方法論の適用に従事．2015 年より，総合技術研究所にてシステムズエンジニアリング，MBSE，STAMP/STPA の適用研究．Leveson 教授著『システム理論による安全工学（原著名：Engineering a Safer World）』監訳，『CAST HANDBOOK』共訳．STAMP 関連の講演・講義・執筆多数.