Vol.2021-SPT-41 No.9
2021/3/1

攻撃者観点での STAMP/STPA の制御構造分析と攻撃木分析の系統的統合の試み

日下部 茂[1]　小松 文子[1]　相馬 大輔[2]　佐川 陽一[2]

概要：システム理論に基づく STAMP/STPA は，安全性の分析手法として提唱されたが，セキュリティとの統合的な分析手法としての発展的活用もなされている．我々は，STAMP/STPA の制御構造の分析と，非安全なコントロールアクションに着目した攻撃者観点の分析を取り入れ，攻撃木分析との系統的な統合を試みている．ケーススタディとして，制御システムの一例である，産業用ロボットに対して提案手法の試行を行った．

キーワード：脅威モデリング，ハザード分析，システム理論

Integration Trial of Attack Tree Analysis and Control Structure Analysis of STAMP/STPA with Attacker's Point of View

SHIGERU KUSAKABE[†1]　AYAKO KOMATSU[†1]
DAISUKE SOUMA[†2]　YOUICHI SAGAWA[†2]

Keywords: Threat modeling, Hazard analysis, System theory

1. はじめに

Cyber-Physical Systems (CPS) 社会では，セキュリティやセーフティを含む “Trustworthiness” が重要な課題の一つと考えられている[1]．情報システムのセキュリティでは，悪意のある攻撃者からの情報資産を保護するための取り組みが以前から行われている．セーフティに関して，これまでも信頼性工学や安全性工学の領域を中心に，利用する人間の信頼性を含め，様々な取り組みが行われてきた．制御機構が電気機械的なものからソフトウェア集約型へ移行が進んでいること，人や組織の問題も重要であることなどから，セーフウェアという考えも提唱されている[2]．CPS 社会のシステムにおける Trustworthiness を実現するためは，個別に考慮されてきたセキュリティとセーフティについて統合的な検討が必要である．このような背景の下，攻撃木分析と攻撃者観点での STAMP/STPA[3]の制御構造分析の系統的統合の試みを行った．

セキュリティの脅威分析の一つの手法である，攻撃木 (Attack Tree (AT)) 分析は Fault Tree 分析をベースにした手法である[4]．Root ノードから詳細化していくが，何を Root にするかは，分析者に依存する．多くは，攻撃ゴールとし，下位ノードに攻撃目的，攻撃手法を識別し，最終的なノードに資源を特定する．攻撃者の立場になって体系的に記述することで，特定の資源に可能な攻撃を抽出することができる．このような分析を分析者依存の属人的な手法から体系立てたものにするため，システム理論によるアプローチである STAMP/STPA と組み合わせて用いることを考えた．

システム理論によるハザード分析の手法 STAMP/STPA は，セーフウェアの実現に向けた具体的な分析手法として提唱された．ハザード分析の知見を広く活用するため，損失を人命などに限定せず，ミッションの未達や組織の評判などの分析も視野に入れたものになっており，実務家を中心に経験的な評価により普及してきた[5]．セキュリティの観点は当初含まれていなかったが，セキュリティ観点の分析法である STPA-Sec [6]が提唱され，セキュリティに関する分析も盛んになっている[7]．

本稿では，そのような STAMP/STPA の制御構造の分析に，攻撃面に着目した攻撃者観点の分析を取り入れ，攻撃木分析との系統的に統合することについて論じる．制御システムの一例である，産業用ロボットに対して提案手法を試行したケーススタディも紹介する．産業用ロボットは，「隔離の安全」,「停止の安全」という安全原則が確立していたが，人間共存型ロボットなどではそのような安全原則は成り立たない[8]．また，ICT 化の進展に伴い情報セキュリティの分析も必要になっており，安全性とセキュリティの統合的分析を目指し，本稿のような試みを行った．

本稿の構成は次の通りである．第 2 節では，産業用ロボットのセキュリティ分析の関連研究を紹介し，第 3 節では事例の対象である産業用ロボットについて紹介する．第 4 節では，STAMP/STPA を説明した後，制御構造を中心に，産業用ロボットシステムの STAMP/STPA 分析の事例の一部を説明する．第 5 節では STAMP/STPA の制御構造図を活用した攻撃木分析について論じた後，第 6 節ではそのよう

1 長崎県立大学
University of Nagasaki.
2 住友電気工業株式会社
Sumitomo Electric Industries, Ltd.

な攻撃木分析の例を示す．第 7 節では，まとめと今後の課題について述べる．

2. 関連研究

産業用ロボットに関するサイバーセキュリティリスクについては，トレンドマイクロ社がミラノ工科大学と共同で実施した攻撃実験[9][10]がある．ここでは，ネットワークに接続されたロボットに対して，脅威分析を行い，実際に攻撃を試みている．脅威分析では，以下の攻撃者のゴールを設定し，それぞれにシナリオを描いている．

① 製品成果の改ざん（Production Outcome Altering）
- ✓ 製品の成果を変更することで，ランサムウエアで利用することもある

② 物理被害（Physical Damage）
- ✓ 工場を中断させ経済損失を生じさせること

③ 製品工場が中断（Production Plant Halting）
- ✓ ロボット自身や工場設備に損害を与えること

④ 不正アクセス（Unauthorized Access）
- ✓ 攻撃者に狙われる機微データを含む

また，遠隔からのネットワーク攻撃と操作員や悪意のある契約者などによる物理攻撃を攻撃面（Attack Surface）として区別した．これは，[11]においても「侵入口」として定義された検討項目である．結果として以下の攻撃ベクトルについて可能性があるとし，実際に攻撃を成功させている．

- 攻撃１：コントロールループパラメータを変更
- 攻撃２：カリブレーションパラメータを改ざん
- 攻撃３：製品ロジックを改ざん
- 攻撃４：ユーザが認知するロボット状態を変更
- 攻撃５：ロボット状態を変更

本研究との違いは，標準的なロボットアーキテクチャを対象としていること．攻撃面を想定して攻撃者の侵入から開始して攻撃ベクトルを分析していることだが，その分析内容について詳細には述べられていない．

3. 産業用ロボット

事例とした産業用ロボットは，対象のシステムは対象部材を特定の場所 A から特定の場所 B へ移動させるシステムで，その概要は以下の通りである．(図 1 参照)

(1) 機能概要

- 動作実行 ：動作プログラムに従い動作を行う
- 動作プログラム作成 ：動作実行で行う一連の動作を設定する
- 異常検知停止 ：動作実行中に異常を検知したら動作を停止，停止状態でロボットアームを固定する
- 非常停止 ：非常時に動作を停止し，停止した状態でロボットアームを固定する

(2) コンポーネント概要

対象システムは，以下のようなコンポーネントからなる．

- ロボットアーム本体：ロボットアームコントローラからの制御メッセージに従い動作する．動作は，サーボ作動による対象部材の移動に加え，サーボ情報や位置，速度，電流，電圧などのフィードバックのロボットアームコントローラへの送信も行う．
- ティーチングペンダント：ロボットアーム本体を操作しながら動作プログラムを作成するための機器．ロボットアームを操作し，その際の動き，通過位置，速度，停止位置などをロボットアーム動作データとしてロボットアームコントローラへ送信する．
- ロボットアームコントローラ：操作 PC からのシステム制御命令に従い，待機，動作，動作プログラム作成，停止などロボットアーム本体の制御を行う．ティーチングペンダントの制御も行う．動作プログラムとロボットアーム本体から受信するサーボ情報に従い，ロボットアーム本体へ制御メッセージを作成し，ロボットアーム本体へ送信する．また，サーボ情報リクエストをロボットアーム本体へ送信し，ロボットアーム本体からサーボ情報（サーボモータ位置，速度など）

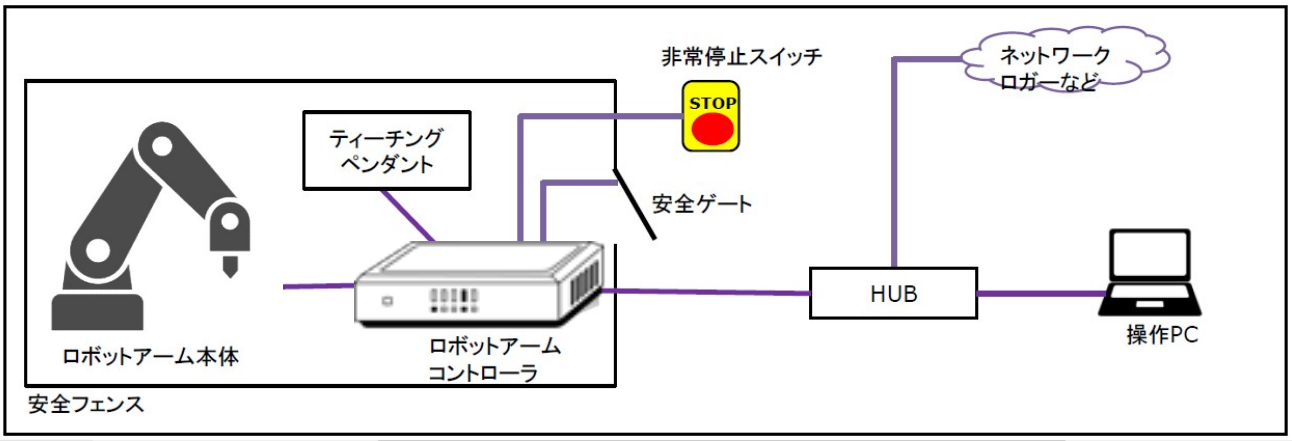

図 1 事例の産業用ロボットの構成概要

Figure 1 The configuration of industrial robot.

を受信する．受信したサーボ情報や送信した制御メッセージはロボットアームログデータとして操作 PC または外部のロガーへ送信する．ティーチングペンダントを用いた動作プログラム作成時には，ティーチングペンダントからのロボットアーム本体操作命令とロボットアーム本体から受信するサーボ情報から制御メッセージを作成し，ロボットアーム本体へ送信する．また，ティーチングペンダントからのロボットアーム動作データを元に動作プログラムを作成し，操作 PC へ送信する．

- 安全ゲート およびフェンス：動作時に人との接触を防ぐためにロボットアーム本体を覆う安全フェンスに取り付けられているゲート．安全フェンスはロボットアーム本体およびロボットアームコントローラを，金属のフレームおよびアクリル板で上部を含み完全に覆っている．動作プログラム作成などを行う際にロボットアーム本体を操作したり，ワークペイロードを設置するなどの際に開放する．安全ゲートの開閉を検知するセンサーがあり，ゲートの開閉を一定周期でロボットアームコントローラへ送信する．
- 操作 PC：オペレータの操作でロボットアームコントローラと通信し，各機能の開始，制御ログの取得などを行う．また，ロボットアーム本体の動作プログラムの作成も行う．操作 PC は一般的な PC の持つ USB ポートなどを持つ．
- 非常停止スイッチ：非常時にロボットアーム本体の動作を即時停止するためのスイッチ．手動でスイッチを押すと，非常停止信号がロボットアームコントローラへ送信される．

4. STAMP/STPA による分析

4.1 STAMP/STPA 概要

近年の IoT 化やシステムの複合化の進展などによって，従来の解析的還元論や信頼性理論ではカバーできない範囲が拡大している．コンポーネントの直接的な相互作用だけでなく，間接的，非線形な相互作用による創発的な問題によるハザードも識別する必要がある．また，ソフトウェアによって，システムの開発や運用における人の役割が大きく変わってしまう，より高い効率や生産性の追求で本来重視されるべきものが軽視される，といったことに起因する問題も識別する必要がある．このような背景のもと，STAMP/STPA がシステム理論に基づく新しいアクシデントモデルとその分析法が提唱されている．STAMP/STPA はハンドブック[12]も公開され，すでに多数の実システムへの適用が行われている．セキュリティの分析に関しては STPA-Sec が提唱されその適用と研究がなされている[13].

STAMP/STPA の基本的なステップは，以下の 4 つである．(図 2 参照)

1. 解析目的の定義，
2. 制御構造(コントロールストラクチャ)のモデル化，
3. 非安全なコントロールアクション(UCA: Unsafe Control Action)の識別，
4. 損失シナリオの識別

ここでは，損失シナリオの識別において，セキュリティ観点の分析と系統的な統合を行うため，後述するように制御構造図を活用する．識別された UCA に至るパスに着目し，攻撃面や攻撃木の分析を行う．これにより STAMP/STPA を用いたセキュリティ観点のシナリオ分析で，攻撃木分析の系統的な統合を目指す．

4.2 解析目的の定義

事例において，安全性に加え，セキュリティの側面も加えた，考慮すべき損失は以下のようなものとした．

① 人の死傷
② 生産計画が実現できずミッションが未達
③ 対象部材の損壊 (落下，衝突などによる)
④ システムの損壊
⑤ 重要な保護対象情報の損失

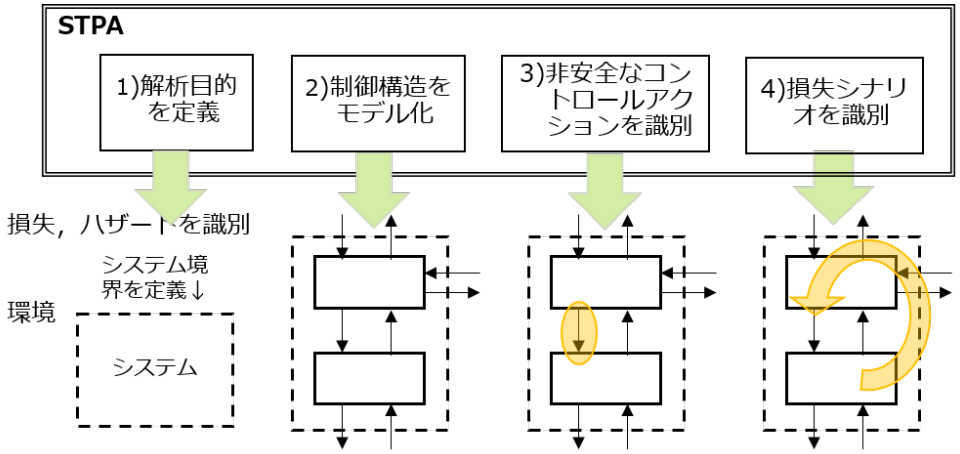

図 2 STAMP/STPA の基本的な分析ステップ[12]

Figure 2 Basic steps of STAMP/STPA

以下が，避けるべき状態，条件であるハザードである．
① 稼働時における最少間隔違反
② 制御の劣化・逸脱
③ 制御情報に不備
④ 重要な保護対象への保護の欠落
このようなハザードにもとづいて，安全制約を考える．
① 稼働時は最少間隔が保たれる
② 制御の劣化や逸脱はない
③ 制御情報に不備はない
④ 重要な保護対象は保護されている

4.3 制御構造のモデル化

要求レベルのシナリオ分析などを行い，送受信される命令やデータなども明らかにした上で制御構造のモデル化を行った．図 3 にその制御構造の図を示す．図中の数字がシステムのマンマシンインターフェイス境界の中でのやりとり，アルファベットのものが外側でのやり取りで、外側の破線は今回の分析対象の範囲を示している．制御構造上のマンマシンインターフェイス境界内でやり取りされる通信については付録に表を記載している．

4.4 非安全なコントロールアクション

非安全なコントロールアクションの分析は，コントロールアクションに対して以下の 4 つの観点で行う．

1. コントロールアクションを与えないことがハザードにつながる．
2. コントロールアクションを与えることがハザードにつながる．
3. 潜在的には安全なコントロールアクションだが，早過ぎ，遅過ぎ，または間違った順序で与えられ，ハザードにつながる．
4. （連続的なコントロールアクションであり離散的なものではない）コントロールアクションがあまりにも長く続くあるいは，あまりにも早く止まることで，ハザードにつながる．

一般に，この分析はかなりの規模になる．ここでは，説明のため，網羅的でなく，部分的な例として，以下のような産業用ロボットの安全原則をベースとした例考える[8].

- 停止の原則：機械は止まっていれば安全である
- 隔離の原則：人がそばにいなければ安全である

図 3 の⑧に関して，隔離の原則に関する例として，ゲートが閉じられていない時にサーボ動作命令が出されるという UCA がある．停止の原則に関する例として，非常ボタンが押されたのに非常停止命令が実行されないという UCA がある. セキュリティの観点では, このような状況が，コンポーネントの不具合によるものだけでなく，セキュリティ上の問題で発生するか，悪意のある攻撃者によって引き起こされうるかということを分析する必要がある．

5. STAMP/STPA と攻撃木分析の併用

5.1 STPA-Sec

セキュリティのための STAMP/STPA である，STPA-Sec も STPA の基本ステップを共有している．例えば，[13]では以下のようなステップ構成を紹介している．

- Problem framing
- Identify accidents and hazards
- Draw the functional control structure
- Identify unsafe/unsecure control actions
- Identify security-related causal scenarios
- Wargame

上記で，下線部が STPA-Sec 固有のものでそれ以外は共通のものである．最初に Problem framing が追加され，損失シナリオの識別にセキュリティ関連のものを行い，最後に Wargame を行うといった違いがある．

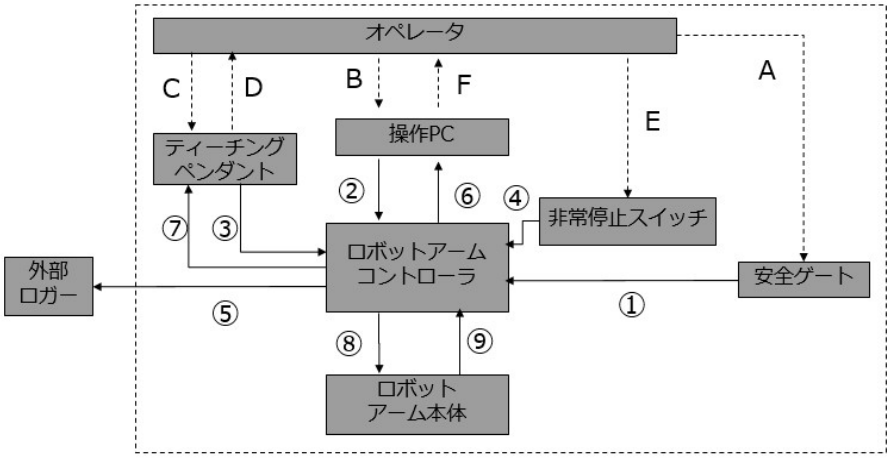

図 3 制御構造

Figure 3 Control Structure

セキュリティ関連のシナリオ分析において，慣習的な手法を用いる場合の懸念事項の一つに，完全かそれに近いアーキテクチャを必要とする点が指摘されている[13]．しかしながら，本研究の産業用ロボットの例題は，アーキテクチャは完成のものに近く，慣習的な手法との併用も可能と考えた．これまでの分析法で培った専門家の知見の活用も念頭に，攻撃木分析を系統的に併用することを考える．

5.2 UCA と制御構造を用いた攻撃木の分析

セキュリティの分析において，攻撃者観点のコントロールアクションを考えるため，STAMP/STPA の制御構造と UCA の分析結果を用いる．その概要を図 4 に示す．UCA の分析結果を用いて，攻撃木の Root ノードの候補を系統的に検討し，攻撃木分析において制御構造図を活用する．

非安全なコントロールアクションが出されてしまうシナリオの分析として，例えば，ゲートが閉じられていない時に制御構造図の⑧でサーボ動作命令が出されるケースを考える．これは，制御構造図上で，ゲートと⑧の間のパスにある，①か，ロボットアームコントローラのロジックかプロセスモデル(状態変数)が関係するシナリオを検討する．

文献[8]のエピソードにある，強力な電波によってメモリに不具合が起き暴走したような例だとプロセスモデルに不具合が生じた例になる．セキュリティの観点では，このような状況が，コンポーネントの不具合によるものだけでなく，セキュリティ上の問題で発生するか，悪意のある攻撃者によって引き起こされうるかということを分析する必要がある．

6. 攻撃木分析

攻撃木分析では攻撃者の攻撃目標をルートノードとし，その目標を達成するための手段を詳細化していく．制御システムのリスク分析ガイドラインである[11]では，資産ベースと事業被害ベースの 2 種類の手法を紹介しているが，事業被害ベースでは，シナリオ分析の手法として攻撃木分析を FTA とともに活用している．このリスク分析では，システムの機器構成図をもとに「事業被害を引き起こす可能性のある攻撃拠点・攻撃対象・最終攻撃を具体化した」攻撃シナリオを検討し，攻撃木としてノードを確定し，重要な攻撃木を選定していくプロセスである．「最終攻撃」は，一般的な攻撃木においてはルートノードである攻撃目標に相当し，最初の段階で設定するが，[11]では，攻撃者（の種類），侵入口，侵入ルート，攻撃対象・拠点を特定しつつ最終攻撃を確定している．事業被害は，STAMP/STPA における，損失に相当する．

本研究では，対象ロボットアームシステムについて，STAMP/STPA での制御構造（CS）と UCA をベースに，攻撃木であるトップ事象を導き，この事象を引き起こす手段や制御について詳細化した．

図 5 は，非安全なコントロールアクションとして 4.4 で述べた「ゲートが閉じられていない時にサーボ動作命令が出される」場合の攻撃木である．図 3 の制御構造から安全ゲートへのインターフェイスは①であり，サーボ動作命令は，ロボットアームコントローラからアーム本体へ⑧で出される．図 5 では，トップ事象（AT-UCA1）が発生する条件を AT1-1 コントローラの安全ゲート状態が不正，または AT1-2 コントローラが動作命令時に安全ゲート状態を無視する，場合を抽出し，それぞれの発生する条件（または手段）を詳細化している．次に各ノードにおいて，セキュリティ侵害を原因とするかを検討する．その結果，機器の故

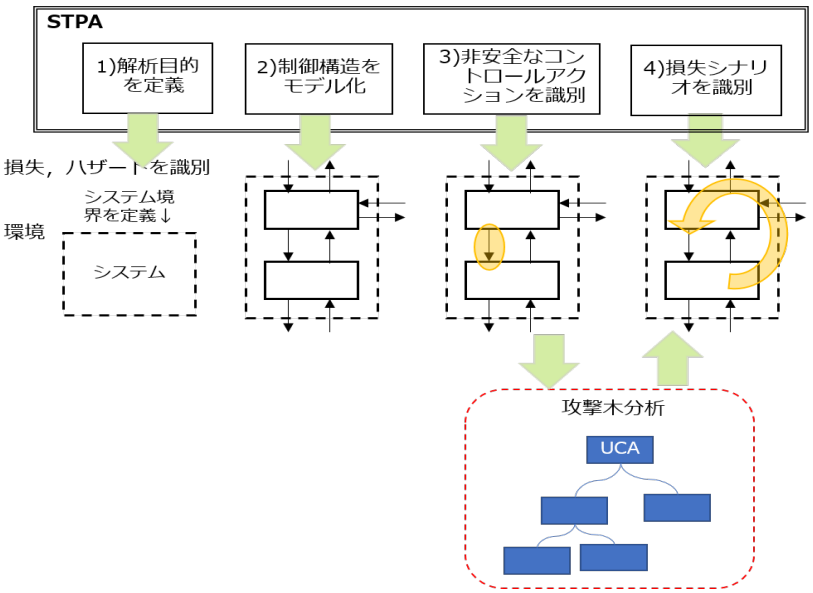

図 4　STAMP/STPA と攻撃木分析の併用

Figure 4　STAMP/STPA with ATA

	AT-UCA1	ゲートが閉じられていない時にサーボ動作命令が出される					
AT	1-1		コントローラの安全ゲート状態が不正				
	1-1-1			安全ゲートの開閉信号が正しくコントローラに伝わらない			
	1-1-1-1				ケーブル不具合		
	1-1-1-2				安全ゲートセンサー不正		
	1-1-1-2-1					安全ゲートセンサーが騙される[SEC]	
	1-1-1-2-2					安全ゲートセンサーの機器故障	
	1-1-1-3				安全ゲート信号制御プログラムが改ざん[SEC]		
	1-1-1-4				安全ゲート開閉信号が改ざん[SEC]		
	1-1-2			コントローラの安全ゲート状態処理プログラムが不正動作			
	1-1-2-1				安全ゲート状態処理プログラムが改ざんされる[SEC}		
	1-1-3			コントローラの安全ゲート状態が改ざんされる[SEC}			
	1-2		コントローラからの動作命令時に安全ゲート状態を無視する				
	1-2-1			安全ゲート状態処理プログラムが改ざんされる(1-1-2-1と同じ)			

図 5 安全ゲートが閉じられていない間にサーボ動作命令が出される攻撃木
Figure 5 Attack Tree, Operation command while gate open

障（1-1-1-1 ケーブル不具合，1-1-1-2-2　ゲートセンサーの機器故障）の他，以下のセキュリティ侵害の可能性のある最終ノードを抽出した．図 5 では該当ノードに[SEC]と付記した．

1-1-1-2-1　安全ゲートセンサーが騙される
1-1-1-3　安全ゲートにおける信号制御プログラムが改ざんされる
1-1-1-4　安全ゲート開閉信号が改ざんされる
1-1-2-1　安全ゲート状態処理プログラムが改ざんされる
1-1-3　コントローラの安全ゲート状態が改ざんされる

これらの抽出されたノードは，[9]では＜攻撃の攻撃３：製品ロジックを改ざん＞，＜攻撃２：カリブレーションパラメータを改ざん＞の一つである安全ゲートの状態を改ざんすることに対応している．

それぞれの攻撃シナリオは，攻撃木のノードをトップ事象である AT-UCA1 迄たどり図 6 の例に示すように記述することができる．

攻撃木では，各ノードの実現可能性を検討し，最も起こりやすいシナリオを抽出することができる．この際に，高度な情報技術レベルを持つか，一般の技術レベルの攻撃者かといった①攻撃者の属性を想定すること，各ノードを実現するために，②特別な装備が必要か，③攻撃者にとってコストがかかるか，などの攻撃者の観点からの検討の条件を設けてリスクを分析していく．こうして，同じ攻撃ターゲットに対しても攻撃者にとって最も攻撃しやすいシナリオを識別し，対策の優先順の検討に役立てることが可能となる．

図 6 の例では，攻撃面（Attack Surface）[9]としては物理侵入（契約者や操作員）攻撃であるが，ネットワーク経由の攻撃の場合はシナリオを作成後，さらに侵入口を特定することが必要となる．図 5 の攻撃木において，「1-1-3　コントローラの安全ゲート状態が改ざんされる」を例にとると，CS 上のロボットアームコントローラへのコントロールである②，③，⑨をチェックする必要がある．操作 PC からの②については，操作 PC の USB 経由でのマルウエア感染などが想定できる．しかし，ネットワーク上での外部ロガーへのデータ送信⑤については，CS 上はネットワークからの制御はないが，通信プロトコルの脆弱性による侵入を検討する必要がある．

7. おわりに

システム理論に基づくハザード分析 STAMP/STPA と攻撃木分析を統合的に行う試みを行った．STAMP/STPA の制御構造の分析に，UCA に着目した攻撃者観点の分析を取り入れ，攻撃木分析との系統的な統合を試みた．ケーススタディとして，制御システムの一例である，産業用ロボットに対して提案手法の試行を行った結果，制御構造をベースに非安全なコントロールアクションをトップ事象とした攻撃木を作成し，攻撃シナリオを作成することができた．

一般に攻撃木分析では，トップ事象を決めてその事象への手段を下位ノードとして詳細化していく．したがってトップ事象を漏れなく抽出できることが重要であるが，これは分析者に依存していた．提案手法では，損失からハザードを導き，制御構造上で非安全なコントロールアクションを検討することでトップ事象を抽出できるため，攻撃木の網羅的なトップ事象の抽出が可能と考える．

ただし，多くのサイバー攻撃はネットワーク経由であるため，利用する通信プロトコルの脆弱性に起因する攻撃については，上流の制御構造では表現できない．攻撃木に基づき，作成したシナリオで，ネットワーク侵入による可能性がある場合は，追加の攻撃シナリオを作成する必要があるといえる．

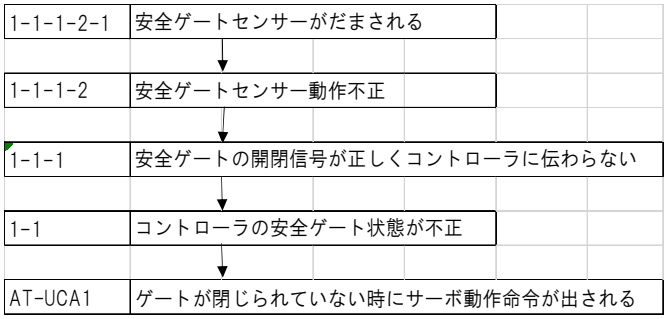

図 6 攻撃シナリオの例

Figure 6 An example of Attack Scenario

参考文献

[1] NIST,“Framework for Cyber-Physical Systems Release 1.0,” NIST, 2016.3, https://s3.amazonaws.com/nist-sgcps/ cpspwg/files/ pwgglobal/CPS_PWG_Framework_for_Cyber_Physical_Systems_ Release_1_0Final.pdf (参照 2021-01-20).
[2] Leveson, N..著; 片平真史他 訳, Safeware : system safety and computers, セーフウェア ：安全・安心なシステムとソフトウェアを目指して, 翔泳社, 2009.10
[3] Leveson, N.. Engineering a Safer World. MIT press, 2012.
[4] Schnier, B., Attack Trees: Modeling Security Threat, 1999, https://www.schneier.com/academic/archives/1999/12/attack_trees. html (参照 2021-01-20).
[5] MIT Partnership for Systems Approaches to Safety and Security (PSASS), STAMP Workshop, http://psas.scripts.mit.edu/home/ stamp-workshops/ (参照 2021-01-20)
[6] Young, W. and Leveson, N., An Integrated Approach to Safety and Security Based on Systems Theory, CACM, VOL.57, NO.2
[7] Span, M., Mailloux, L., Mills, R. ＆ Young, W., “Conceptual Systems Security Requirements Analysis: Aerial Refueling Case Study”, IEEE Access, Vol. 6, 2018
[8] 向殿政男, ロボットの安全技術の概要と最新動向, ロボット, No.211, 2013.
[9] Quarta, D., Pogliani, M., Polino, M., Maggi, F., Zanchettin, A. and Zanero, S. “An Experimental Security Analysis of an Industrial Robot Controller,” 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, 2017, pp. 268-286, doi: 10.1109/SP.2017.20.
[10] Pogliani, M., Quarta, D., Polino, M. et al. Security of controlled manufacturing systems in the connected factory: the case of industrial robots. J Comput Virol Hack Tech 15, 161–175 (2019). https://doi.org/10.1007/s11416-019-00329-8
[11] IPA, 制御システムのセキュリティリスク分析ガイド第 2 版, https://www.ipa.go.jp/files/000080712.pdf (参照 2021-01-20)
[12] Leveson, N.. & Thomas, J., STPA Handbook 日本語版(translated by JAXA), http://psas.scripts.mit.edu/home/get_file2.php? name= STPA_handbook_japanese.pdf / (参照 2021-01-20)
[13] Young, W., “Introduction to STPA for Security (STPA-Sec), tutorial in STAMP Workshop 2020, http://psas.scripts.mit.edu/ home/2020-stamp-workshop-presentations/ (参照 2021-01-20)

付録

付録 A 制御構造図（図 3）上での通信

番号	データ・命令・他		
1	安全ゲート開閉信号	6	ロボットアームログデータ1
2	ログデータ要求命令	6	動作プログラム作成準備完了1
2	動作実行命令	6	動作プログラム2
2	動作プログラム作成命令1	6	非常停止完了1
2	動作停止命令	7	サーボ情報2
2	電源OFF命令1	7	動作プログラム作成命令3
2	電源ON命令1	8	サーボ動作命令
2	動作プログラム1	8	サーボ状態リクエスト
3	ロボットアーム動作データ	8	電源OFF命令2
3	ロボットアーム本体操作命令	8	電源ON命令2
3	動作プログラム作成準備完了3	8	非常停止解除命令
3	動作プログラム作成完了	8	動作プログラム作成命令2
4	非常停止信号	8	非常停止命令
5	ロボットアームログデータ2	9	サーボ情報1
6	移動完了(待機状態位置)	9	動作プログラム作成準備完了2
6	電源OFF命令に対するAck1	9	電源OFF命令に対するAck2
6	電源ON不可メッセージ	9	電源ON完了
6	動作実行命令に対するAck	9	非常停止完了2