Vol.2020-SPT-36 No.39
2020/3/2

ドローンにおける セーフティ・セキュリティの統合リスク分析の試み

和田健治，小松文子

概要：ドローン市場は 2021 年には世界で 48 億ドルの市場規模になると予測されており、農業やエネルギー、鉱業、建設、不動産、メディアといった様々な業界で使用されている。また、都市においても重要な役割を担うと予測されている。そこで、ドローンに潜む脅威をセーフティ、セキュリティの両面から明らかにし、それらを統合した形でドローンのセキュリティ・セーフティを、STAMP/STPA を用いてより効果的なリスク分析を試みた。その結果、マルウェア感染をはじめとしたサイバーセキュリティ脅威は統合が可能であったが、物理的な脅威はこの分析手法では統合が困難であった。これらの結果により、システム構築段階でサイバーセキュリティ脅威を含めて統合的なリスク分析を行う際に留意すべき内容を明らかにし、想定される被害の予測を立てることができ、より安全なシステム構築をすることが可能となる.

キーワード：ドローン，STAMP/STPA

A study on integrated risk analysis of safety and security for drone

KENYA WADA，AYAKO KOMATSU

Abstract: The drone market is projected to grow to $ 4.8 billion globally by 2021, and is used in a variety of industries, including agriculture, energy, mining, construction, real estate and media. It is also expected to play an important role in cities. Therefore, we clarified the threats lurking in the drone from both aspects of safety and security, and tried to analyze the security and safety of the drone more effectively by using STAMP / STPA. As a result, cyber security threats such as malware infections could be integrated, but physical threats were difficult to integrate with this analysis method. Based on these results, it is possible to clarify what should be taken into consideration when conducting an integrated risk analysis including cyber security threats at the system construction stage, make predictions of possible damage, and build a more secure system. It is possible to do.

Keywords: drone，STAMP/STPA

1. 背景

近年，自動車や航空機，ドローンなどの乗り物に対するハッキングの成功例が国際会議で発表[1]されており、サイバーセキュリティ対策の重要性が像増大している．乗り物のセキュリティ対策のうち、自動車業界はサイバーセキュリティ脅威から自己資産を守るためのセキュリティガイドブックが発行されている[2]．ドローンについては、農業，エネルギー，鉱業，建設，不動産，メディアなど幅広い業界で使用されており，2015 年から 2020 年で年平均 19%の成長率が見込まれ、ドローン市場は 2021 年には世界で 48 億ドルの市場規模になると予測されている[3].

ドローンは IoT の普及により人々の生活を豊かにするスマートシティにおいては重要な役割を果たし，市内の監視や商品輸送として機能すると予測されている．しかし，スマートシティにドローンを使用することは，サイバーセキュリティ，プライバシー，公共安全の分野を含め，技術的および社会的課題に対処する必要がある[4]とされ，解決すべき課題が多い.

一方で，IoT 機器に対しては，セーフティの観点からの分析として，FTA(Fault Tree Analysis)や FMEA(Failure Mode and Effect Analysis)といった安全性分析が実施されてきたが，システムの複雑化に従って，不十分であるといわれ，STAMP（Systems-Theoretic Accident Model and Processes:システム理論に基づくアクシデントモデル）/STPA（System-Theoretic Process Analysis）による新たな安全性分析

ⓒ 2020 Information Processing Society of Japan

が提唱されている[5].

本論文では，今後必要とされるドローンを対象にセーフティとセキュリティの観点からこれを統合することを目的に行ったリスク分析について報告する.

2. 関連研究

2.1 セーフティ分析

乗り物や，制御システムなどでは，機器の安全，人命，事故防止のためのセーフティと、機密性，安全性，可用性について分析するセキュリティをそれぞれ一方からのアプローチのみで考えられているものが多く，セキュリティ対策は，保守・運用段階での脆弱性対処が中心である現状がある[6]．その為システム構築段階はセキュリティよりもセーフティの方が重視されてきた．なお、本論文では、セーフティを「受入れ不可能なリスクが存在しないこと」，「人への危害または資機材の損傷の危険性が，許容可能な水準に抑えられている状態」とする。受入れ不可能なリスクが存在しないことを目的に、リスクを基準以下に低減する機能の働きにより「機能安全」を確保しようという方法がとられてきた[7].

2.2 セキュリティ分析

セキュリティ分析においては常に攻撃者が悪意を持って対象のシステムに意図しない動作をさせることを前提にリスク分析を行う[7]．脅威分析でよく知られているのは、STRIDE や攻撃木などの分析手法[8]である．ドローンに対しては、国家空域での民間ドローンの使用に関連する主なセキュリティ，プライバシー，および安全性の側面について、民間ドローンシステムの物理的脅威とサイバー脅威の両方を特定し，それらの運用環境に関わるセキュリティ特性(セキュリティ，プライバシー，セーフティ)について議論している[9]．ドローンを戦闘に活用する場合，無人航空機(Unmanned Aerial Vehicles:以下 UAV と記載)には，軍隊の動きやデータ，戦略的作戦までの幅広い情報を収集，保存することができ，そこに含まれる情報の量や種類は，UAV の窃盗や攻撃の標的となっているとの報告もある[10].

2.3 分析対象としたドローン

ドローンには様々な種類がある．娯楽の一部として使用されているトイドローンをはじめ，農業・エネルギー・メディア・インフラ向けに開発された産業用ドローン，軍事利用を目的とした軍事用ドローンなど，目的によって搭載されるセンサーや機能の違いがあるが、本論文でドローンを分析する際に必要となる抽象的な構成については，[11]を参考とした．図 1 にドローンシステムの３つの構成要素を示す.

図 1：ドローンシステム

ドローンシステムは主に以下の 4 つのコンポーネントによって成り立っている.

- 機体上のフライトコントローラ
- 機体上のコンパニオンコンピュータ
- 地上側の PC，タブレット，スマートフォン
- クラウド

2.4 STAMP

従来、機器に発生するアクシデントは根本の原因となる機器の故障や人間の操作ミスの発生がシステム内の他の機器や人間に伝搬し起こると捉えられていた．しかし，現代においては，システム規

模の拡大や構成要素の増大により、システムが複雑化し 1 つの構成要素だけではなく、複数の要素間の相互作用による要因を考える必要があるとされている。マサチューセッツ工科大学の Levson 教授は，著書「Engineering a Safer World」[12]の中で，「現代のシステムにおけるアクシデントはシステムの中で安全のための制御を行う要素(コントローラ:Controller)と制御される要素(被コントロールプロセス:Controlled Process)の相互作用が働かないことによって起きる」と述べた．このモデルを「STAMP(System-Theoretic Accident Model and Process):システム理論に基づくアクシデントモデル」と呼ぶ．STPA(System-Theoretic Process Analysis)は STAMP アクシデントモデルを前提として，システムのハザード要因を分析する安全性解析手法である[5].

3. 研究課題

既述の通り、セーフティとセキュリティそれぞれの安全性は，別々に分析をする傾向にある．ドローンに対して行われている STAMP を用いたセーフティ分析に加えて，セキュリティに関連した脅威を分析し，既存の STAMP だけでは考慮されていなかったセキュリティの観点からのリスク分析を行い，統合できるかを検討していく．すなわち，ドローンを対象に STAMP/STPA を用いたセーフティ・セキュリティ統合リスク分析を研究課題とする． 使用したリスク分析のソフトウェアは，情報処理推進機構(IPA)が STAMP 支援ツールとして web サイトにて公開している，STAMP Workbench(STAMP 向けモデリングツール STAMP Workbench)である[13]．今回分析対象とするドローンは，基本的な構成に加えて以下の機能を備えているものとする．

- 視野外飛行(BVLOS:Beyond Visual Line of Sight).
- GPS によって飛行地点を把握する機能.
- フェールセーフ機能(バッテリー残量が低下した場合は離陸地点に戻る)
- 衝突回避機能

また，一般的なドローン操作においてドローン所持者が機体操作，機体整備，機体管理を行うことから以下の条件を加える．

- 操作者とグランドコントロールステーション(GCS)は同一人物による．
- 地上にて飛行制御するソフトウェアと機体のファームウェアは定期的にアップデートを行う．

4. セーフティ・セキュリティ分析

STPA で決められたようにセーフティ分析[5]し，次にセキュリティ分析を組み込み，最終的にセーフティとセキュリティの統合化を目指すものとする．全体の手順としては図 2 である．

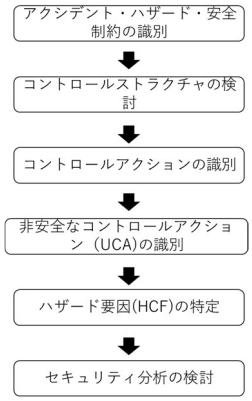

図 2：分析手順

4.1 アクシデント，ハザード，安全制約の識別

ドローンにおけるアクシデントは様々な要因による結果として，2 つ考えられる．ドローンの衝突とドローンの墜落である．

ドローンの衝突をもたらすハザード，アクシデント，安全制約は図 3 に示す．これらの安全制約 ID を SC1 とした．ドローンの墜落をもたらすハザード，アクシデント，安全制約は図 3 に示す．これら

の安全制約 ID を SC2 とした．不適切な環境条件とは，ドローンが飛行するにあたって安全な飛行が望めない環境下(暴風や豪雨といった荒天時)のことである．不安定なドローン機体条件とは，ドローンが水平になっていない条件で離陸し安全な飛行を望めないことである

アクシデント	ハザード	安全制約 ID	安全制約
ドローンの衝突 (アクシデントとは望んでいないイベント，不計画，損失に繋がるようなイベント)	障害物を検知しても停止や回避が間に合わない(ハザードとは環境のある最悪な条件と重なることでアクシデントに繋がる)	SC1 (安全制約とはハザードからシステムを安全に保つための要件，制約)	衝突防止が間に合う範囲で障害物を検知して減速する．
ドローンの墜落	(不適切な環境条件や不安定なドローン機体条件などで)制御不能に陥る．	SC2	制御不能に陥らない為に，不適切な環境条件や不適切なドローン機体条件などでは指定されたコマンドの操作を実行させない．

図 3：アクシデント・ハザード・安全制約表

4.2 コントロールストラクチャ

ドローンの制御を行う要素(コントローラ:Controller)と制御される要素(被コントロールプロセス:Controlled Process)を把握し，リスク分析をするため作成した，コントロールストラクチャ図を図 4 に示す。 コンポーネントは，操作者，制御プログラム，アクチュエータ，UAV(ドローン)，コントローラ(センサー)である．アクチュエータ，コントローラ(センサー)に関しては UAV に搭載されているものであるが，詳細化し具体的に分析する為に，別々のコンポーネントとしている．赤線で示している矢印は後述するコントロールアクション(CA:Control Action)である．青線で示している青矢印は CA ではなく機械的に情報を返すフィードバックである．

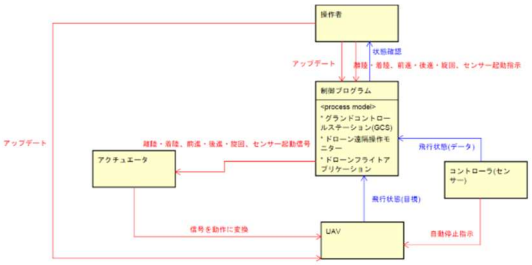

図 4：コントロールストラクチャ図

4.3 コントロールアクションの識別

図 4 のコントロールストラクチャ上で，以下に示すコントロールアクションを識別した．

- CA1:離陸・着陸，前進・後進・旋回，センサー起動指示

操作者とグランドコントロールステーション(GCS)を同一人物としている為，離陸・着陸，前進・後進・旋回，センサー起動指示については状況認知から操作入力までのコントロールアクションである．

- CA2:離陸・着陸，前進・後進・旋回，センサー起動信号

制御プログラムからアクチュエータに対して信号を送るコントロールアクションである．

- CA3:信号を動作に変換

CA2 で与えられたコントロールアクションを実際に信号から動作へと変換するコントロールアクションである．

- CA4:自動停止指示

コントローラ(センサー)に搭載されている衝突回避機能が作動する場合に発動されるコントロールアクションである．

- CA5:アップデート

操作者から UAV のファームウェアをアップデートする際に使われるコントロールアクションである．アップデートは UAV をインターネットに接続し行われるものとする．

- CA6:アップデート

操作者から制御プログラムのアプリケーションを

Vol.2020-SPT-36 No.39
2020/3/2

アップデートする際に使われるコントロールアクションである．アップデートは制御プログラムをインターネットに接続し行われるものとする．

4.4 UCA の識別

策定したコントロールアクションを識別し，図 5 の 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コントロールアクション(UCA: Unsafe Control Action)を抽出した。図 6 に示す。

非安全なコントロールアクション			
Not Providing	Providing causes hazard	Too early/Too late, causes hazard	Stopping too soon/ Applying too long causes hazard
与えられないとハザード	与えられるとハザード	早過ぎ，遅過ぎでハザード	早すぎる停止，長すぎる適用でハザード

図 5：非安全なコントロールアクションのガイドワード

No	CA	From	To	CA提供条件	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying long
1	離陸・着陸，前進・後進・旋回，センサー起動指示	操作者	制御プログラム	離陸・着陸，前進・後進・旋回，センサー起動指示はコントローラ（ハードウェア）操作で制御	UCA1-N-U1)操作者の指令入力や操縦・後進・旋回操作を時間までに実行する [NU]	UCA1-P-U1)不適切な操縦命令、不安定なドローン操作による離陸・着陸，前進・後進・旋回時刻によって発生する [PU] UCA1-P-U2)操作者の指令入力や操縦・後進・旋回操作をかたまるまで実行する [PU]	UCA1-T-U1)操作者の入力や操縦・後進・旋回時刻が遅すぎて実行する [TU]	UCA1-S-U1)あすぎる離陸・着陸・旋回時刻で操作者に渡す(UCA-P-U2参照) [SU]
2	離陸・着陸，前進・後進・旋回，センサー起動指示	制御プログラム	アクチュエータ	操作者からの離陸・着陸，前進・後進・旋回，センサー起動指示をそのまま流しているだけとする	UCA2-N-U1)操作者の指令通信を完全まで実行する [NU]	UCA2-P-U1)操作者の指令通信を誤ったタイミングで実行する [PU] UCA2-P-U2)不適切な操縦命令、不安定なドローン操作による離陸・着陸，前進・後進・旋回時刻によって発生する [PU]	UCA2-T-U1)操作者の指令時間が遅すぎて実行する [TU]	該当なし
3	信号を動力に変換	アクチュエータ	UAV	操作者から送られた信号をそのまま動力に変換しおくるだけとする	UCA3-N-U1)操作者の指令通信を完全まで動力に変換しおくる [NU]	UCA3-P-U1)操作者の指令通信を誤ったタイミングで変換する [PU] UCA3-P-U2)不適切な操縦命令、不安定なドローン操作による動力に変換してしまい発生する [PU]	UCA3-T-U1)操作者の指令時間から出力信号を動力変換するのに遅すぎて発生する [TU]	該当なし
4	自動停止指示	コントローラ(センサー)	UAV	異常状態検知による自動停止	UCA4-N-U1)自動停止指示を完全まで実行する [NU]	UCA4-P-U1)不適切な異常検知やドローン操作結果で停止し発生する [PU] UCA4-P-U2)不適切な異常検知やドローン操作結果で停止しまい発生する [PU]	UCA4-T-U1)自動停止時刻の遅れや停止指示の遅すぎで発生する [TU]	該当なし
5	アップデート	操作者	UAV	操作者からアップデート指示があった時点から実行する	UCA5-N-U1)古いバージョンのファームウェアに脆弱性を残り情報漏えいすることで発生する	UCA5-P-U1)アップデートを行いウイルス感染をしっかりチェックせずに行ったら，情報が流出，改竄される UCA5-P-U2)アップデートを行いウイルス感染をしっかりチェックせずに行ったら，機能が破壊される	UCA5-T-U1)ファームウェアの更新が遅すぎて脆弱性を改善されることで発生が発生する	該当なし
6	アップデート	操作者	制御プログラム	操作者からアップデート指示があった時点から実行する	UCA6-N-U1)古いバージョンのソフトウェアに脆弱性が残り攻撃されることで発生が発生する	UCA6-P-U1)アップデートを行いウイルス感染をしっかりチェックせずに行ったら，機能が破壊される	UCA6-T-U1)ソフトウェアの更新が遅すぎて脆弱性を改善されることで発生が発生する	該当なし

図 6:非安全なコントロールアクション表(UCA 表)

4.5 HCF(Hazard Causal Factor)ハザード要因の特定

UCA 表から考えられるハザード要因を特定した．具体的なハザード要因は図 7 に示す．なお，シナリオとは非安全なコントロールにつながるシナリオである．ヒントワードとは HCF 導出のためのガイドワードからの引用であり，これらは HCF 導出にあたり STPA 手順に示されているものである[14]．また図 7 のうちの赤字で示している部分に関しては，ヒントワードに該当しない為，斜線にした．

ID	HCF	ヒントワード	シナリオ
HCF1-N-1-1	操作ミス	(1) Not Providing(操作忘れ)	操作者のミスまたは見による重要時の見落しし中止の判断忘れ無を犯されてのミス
HCF1-N-1-2	操作ミス	(2) Providing causes hazard(操作ミス)	障害物のある前で間違って前進操作，障害物のある方向に操作をしないといけないと思い込み，誤った認知をしてしまう。
HCF1-P-1-1	操作ミス	(2) Providing causes hazard(操作ミス)	重要時の前で間違って重要時の方に操作入力を間違えてしまう。
HCF1-P-1-2	操作ミス	(2) Providing causes hazard(操作ミス)	指示の不安定な状況による離陸・着陸，前進・後進・旋回操作を行い指示バランスが崩れ，結果として故障に陥る
HCF1-T-1-1	操作ミス	(2) Providing causes hazard(操作ミス)	操作者の重要物判断が遅れ，前進・後進・旋回操作が遅くなる。
HCF1-T-1-2	操作ミス	(2) Providing causes hazard(操作ミス)	指示の不安定な状況による離陸・着陸，前進・後進・旋回操作を行い指示バランスが崩れ，結果として故障に陥る
HCF1-S-1-1	操作ミス	(1) Not Providing(操作忘れ)	操作者の重要時の前で間違って前進操作，障害物のある方向に操作をしないといけないと思い込み，誤った認知をしてしまう。
HCF1-S-1-2	操作ミス	(2) Providing causes hazard(操作ミス)	障害物のある前で間違って前進操作，障害物のある方向に操作をしないといけないと思い込み，誤った認知をしてしまう。
HCF2-N-1-3	制御プログラムの故障	(3) ミッションエラー	制御プログラムの故障により，指定した動作指令が正常に送られない。
HCF2-N-1-4	制御プログラムの故障	(4) ミッションエラー	制御プログラムの故障により，入力した動作と異なった動作する。
HCF2-N-1-5	通信不良	(5) 指示操作，スイッチやキーボードなど	通信遮断が原因，指令サイズ及び通信速度が高くなる。
HCF2-P-1-1	操作ミス	(2) Providing causes hazard(操作ミス)	重要時の前で間違って重要時の方に操作入力を操作をしてしまう。
HCF2-P-1-2	操作ミス	(2) Providing causes hazard(操作ミス)	指示の不安定な状況による離陸・着陸，前進・後進・旋回操作を行い指示バランスが崩れ，結果として故障に陥る
HCF2-T-1-1	操作ミス	(2) Providing causes hazard(操作ミス)	操作者の重要物判断が遅れ，前進・後進・旋回操作が遅くなる。
HCF2-T-1-2	制御プログラムの故障	(4) ミッションエラー	制御プログラムの故障により，指定どおりの間だけできなかったり，遅れたりする。
HCF2-T-1-3	通信不良	(5) 指示操作，スイッチやキーボードなど	通信遮断により，重要時認識が不遅れる。
HCF3-N-1-1	アクチュエータの故障	(1) アクチュエーターの不適切なオペレーション	アクチュエータの故障により指定された動作が実行されない。
HCF3-P-1-1	アクチュエータの故障	(1) アクチュエーターの不適切なオペレーション	アクチュエータの故障により，指定とはプラスマイナス間違いによって正常に動作しない。
HCF3-P-1-2	センサーの故障	(1) アクチュエーターの不適切なオペレーション	障害物認知センサーによる誤検知機能が正常に動作しない。
HCF3-P-2-1	アクチュエータの故障	(1) アクチュエーターの不適切なオペレーション	プログラム異常やキーボード異常によって正常な指示ではない。
HCF3-T-1-1	通信不良	(7) 遅れたアクション	通信下良により，制御信号から動作するまでの時間が遅延することで正常なコントロールができない
HCF4-N-1-1	センサーの故障	(3)不適切な送っているフィードバック，フィードバックの遅れ	障害物の特徴は
HCF4-P-1-1	機能の不全	(3)不適切な送っているフィードバック，フィードバックの遅れ	不適切な環境条件によって，センサーが機能しない。
HCF4-P-1-2	センサーの故障	(3)不適切な送っているフィードバック，フィードバックの遅れ	ドローンの自然環境が悪で，正常に反応が働かない。
HCF4-T-1-1	機能不良	(3)不適切な送っているフィードバック，フィードバックの遅れ	機能不良によって障害物検知の遅れや停止指示の遅れ。
HCF5-N-1-1	セキュリティ対策		海賊の機関銃を攻撃され，墜落等の被害を受ける。
HCF5-P-1-1	セキュリティ対策		アップデートによってウイルス感染をしっかりとチェックせずに行ったら，情報や破壊される
HCF5-T-1-1	セキュリティ対策		セロドリ対策といったファームウェアの更新をするまでに脆弱性を悪意に晒される。
HCF6-N-1-1	セキュリティ対策		ソフトウェアのアップデートをしないことで，脆弱性を悪意される。
HCF6-P-1-1	セキュリティ対策		アップデートを行うことでウイルス感染をしっかりチェックせずに行ったら情報や破壊の原因となる
HCF6-T-1-1	セキュリティ対策		ソフトウェアの更新が遅すぎて脆弱性を悪意される。

図 7：HCF 表

4.6 セキュリティ分析

RIHAM ALTAWY らの研究[9]では，ドローンに対しての脅威は図 8，UAV システムに対する脅威は図 9 を報告しており、我々の研究は、これを参考とした．脅威はフライトコントローラ，GCS(グラウンドコントロールステーション)，UAV，のそれぞれのコンポーネントに対して存在する．サイバーセキュリティ，物理的セキュリティの脅威は以下の通りである．

・GPS 信号のなりすまし
・UAV に対する送信の妨害やなりすまし
・GCS 制御信号の権限のない不当開示
・フライトコントローラデータの改ざん
・悪意のあるソフトウェアやトロイの木馬が GCS に入る
・GCS から出される制御信号の妨害やなりすまし
・GCS におけるシステムの攻撃
・サービス拒否
・身近なドローンの衝突
・窃盗や破壊行為

ⓒ 2020 Information Processing Society of Japan

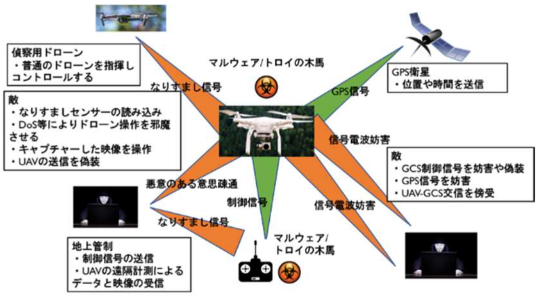

図 8：フライトコントローラや GCS(グラウンドコントロールステーション)，データ通信を標的としたサイバー攻撃の例(出典: Security, Privacy, and Safety Aspects of Civilian Drones: A Survey　邦訳は著者)

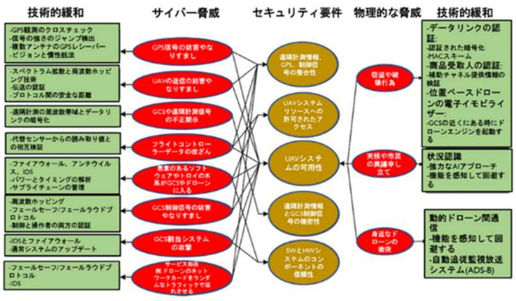

図 9：UAV システムに対するサイバーセキュリティ，物理的セキュリティの脅威(出典: Security, Privacy, and Safety Aspects of Civilian Drones: A Survey　邦訳は著者)

図 8，図 9 の脅威を図 10 コントロールストラクチャ全体図にまとめた．ここで，セキュリティ脅威に含めたコントロールストラクチャ図に攻撃者のコンポーネントを追加した．

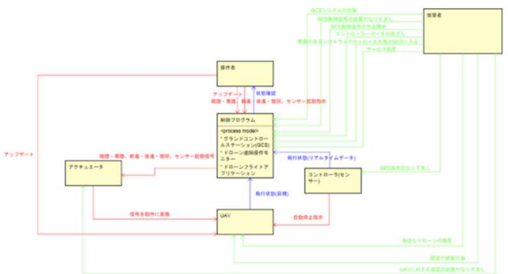

図 10：コントロールストラクチャ全体図(セキュリティ脅威)

緑色に示したものがサイバーセキュリティ脅威，物理的セキュリティ脅威である．制御プログラムに対しての脅威が多数を占めるが，コントローラ(センサー)，UAV，アクチュエータに対しての脅威があることが分かる．

また、これらの脅威を図 11UCA 表に示す。

No	CA	From	To	CA提供条件	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too long
1	コントローラーデータの改ざん	攻撃者	制御プログラム	マルウェア感染		フライトアプリケーションのデータを改ざんし、操作ボタンの表示を変更したり、飛行情報を変更したりする事で、正常な動作の妨害を行う。		
2	悪意のあるソフトウェアやトロイの木馬がGCSに入る	攻撃者	制御プログラム	アップデート		マルウェア感染によって結果的に墜落や衝突の引き金となる。		
3	サービス拒否	攻撃者	制御プログラム			通信混雑による通信不良となり、正常な通信ができない。		
4	GCSにおけるシステムの攻撃	攻撃者	制御プログラム	マルウェア感染		GCSのフライトアプリケーションが起動しない。		
5	GCSから出される制御信号の妨害やなりすまし	攻撃者	制御プログラム	マルウェア感染		指定された操作指示が想定通りに動かず、墜落や衝突の原因となる。		
6	GCS制御信号の権限のない不当開示	攻撃者	制御プログラム	マルウェア感染		マルウェア感染によって、権限割当が書き換えられ、情報の不当開示に繋がる。		
7	身近なドローンの衝突	攻撃者	UAV			想定しないドローンの衝突や事故の原因となる。		
8	窃盗や破壊行為	攻撃者	UAV			窃盗や破壊行為により正常な制御ができない。		
9	GPS信号のなりすまし	攻撃者	コントローラ(センサー)	マルウェア感染		不正確な位置情報により実際の飛行ルートと大きく外れ衝突や墜落の原因となる。		
10	UAVに対する送信の妨害やなりすまし	攻撃者	アクチュエータ			電波銃のようなもので攻撃され、モーター停止に繋がる。		

図 11：セキュリティ・物理的脅威を含めた UCA 表

これらのセキュリティ脅威がなければハザードに繋がることは無いため，Providing causes hazard のガイドワードに当てはまる．また，CA 提供条件によって発生するセキュリティ脅威もあれば，CA 提供条件に関係なく当てはまるセキュリティ脅威もある．

4.7 セーフティ・セキュリティ統合化

セキュリティ脅威の中でも赤字で示したものは CA5，CA6 のコントロールアクションによってマルウェア感染が起こり(青線部)，ハザードに繋がるものである．よって，これらは統合化できる．また，図 12 よりアップデートによるマルウェア感染が引き金となってセキュリティ脅威にさらされているものが多いこともわかる．これらはセーフティ・セキュリティ統合可能である．

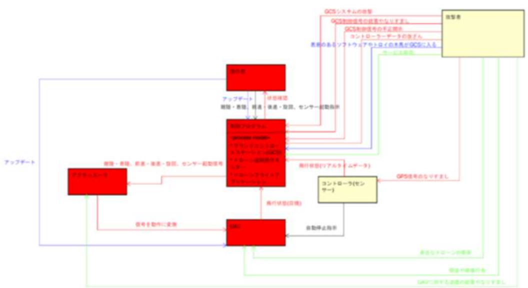

図 12: コントロールストラクチャ図(統合化)

5. 考察

HCF 表（図８）より 31 個の HCF のうち，操作ミス 11 個，セキュリティ対策 6 個，制御プログラムの故障 3 個，通信不良 3 個，アクチュエータの故障 3 個，センサーの故障 3 個，機能の不発 1 個，接続不良 1 個に分類される．この結果より，操作者に直接的に原因があるものは操作ミスとセキュリティ対策にある．これらの HCF は全体の半数以上を占めていることが分かる．セキュリティ分析をするにあたって，攻撃者のコンポーネントが必要である．セーフティとセキュリティの決定的な相違点には，悪意の存在の仮定がある．また，攻撃の種類によって攻撃対象となるコンポーネントが異なるため，それぞれの攻撃先を把握しておく必要がある．

リスク分析の統合化については，攻撃者によって危険にさらされる脅威を想定可能なものは統合できると考える．STAMP/STPA はコントロールストラクチャ図を基に UCA や HCF を特定する手法の為，何の引き金もなく自然と発生するような詳細の分からない脅威(物理的脅威など)は分析することは難しいと考える．また，今回は分析対象のドローンに一般普及しているものを用いたが，多くの実機に触れ様々なドローンの構造を理解しリスク分析を行うことで，さらに踏み込んだ安全性解析を行うことが可能となる．

6. まとめ

ドローンは市場規模が拡大していき，大いに活用されていく．そこでセキュリティとセーフティを統合し分析することを目的として STAMP/STPA の手段で実際にリスク分析を実施した。アクシデントにはドローンの墜落と衝突がある．操作ミスや機器の故障によるアクシデントは起こり得る．しかし，STAMP/STPA を用いて安全性分析を行いドローンシステムの機密性・安全性・可用性についての脅威が多くあることを示すことができた．それらの脅威は，攻撃者の悪意によってマルウェア感染を引き起こし，ドローンの制御をハッキングしようとすることである．マルウェア感染の源流は更新プログラムによるものが想定できる．これらの脅威は STAMP/STPA により HCF 特定を行うことができたが物理的脅威は HCF 特定ができなかった．ドローンの開発段階でこのような脅威を把握しておけばアクシデントにつながるケースを減らすことができる．また、様々な安全性分析手法を取ることや，多種多様なドローンの実機に触れることで，より具体性を増したリスク分析が可能となる．

参考文献

[1]大久保隆夫．“乗り物の情報セキュリティと安全性 1”．情報セキュリティと乗り物，情報処理学会，2016，vol57， No.7，小特集セーフティとセキュリティ．

[2]独立行政法人情報処理推進機構(IPA)．“自動車の情報セキュリティへの取組みガイド第 2 版”，https://www.ipa.go.jp/files/000058198.pdf，(参照 2020-1-5).

[3]Anastasios Plioutsias,Nektarios Karanikas, and Maria Mikela Chatzimihailidou．Hazard Analysis and Safety Requirements for Small Drone Operations: To What Extent Do Popular Drones Embed Safety? Risk Analysis An international journal An official publication of the society for Risk analysis Risk Analysis, Vol. 38, No. 3, 2018.

[4]Edwin Vattapparamban, smail Guvenc, Ali. Yurekli,KemalAkkaya, and Selcuk Uluagac．Drones for Smart Cities Issues in Cybersecurity,Privacy, and Public Safety

Department of Electrical and Computer Engineering, Florida International University, Miami, FL, USA, 2016.
[5]独立行政法人情報処理推進機構(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/files/000051829.pdf, (参照 2019-10-20).
[6]金子朋子. “IoT 時代の安全解析手法 STAMP/STPA とセキュリティーへの STPA 適用”, 独立行政法人情報処理推進機構（IPA）技術本部ソフトウェア高信頼化センター（SEC）, https://www.ipa.go.jp/files/000062863.pdf, (参照 2020-01-05).
[7]大久保隆夫. “乗り物の情報セキュリティと安全性 2”. 情報処理学会, 2016, vol57, No.7, 小特集セーフティとセキュリティ.
[8]小松 文子,日下部 茂,佐川 陽一,山本 秀樹,畑洋一. “サイバーフィジカルシステムにおけるシステム理論による脅威分析の検討-2”. SCIS2019.
[9]RIHAM ALTAWY and AMR M. YOUSSEF. ” Security, Privacy, and Safety Aspects of Civilian Drones: A Survey”. 2016, ACM Transactions on Cyber-Physical Systems, Vol. 1, No. 2, Article 7.
[10]Kim Hartmann, Christoph Steup . “The Vulnerability of UAVs to Cyber Attacks - An Approach to the Risk Assessment”, 2013, 2013 5th International Conference on Cyber Conflict.
[11]春原久徳, “日本におけるドローンの現状<後編>-技術的解説”. ITU ジャーナル 2016 年 Vol.46 No.11(2016,11)スポットライト.
[12]Nancy G.Leveson. “Engineering a Safer World:Systems Thinking Applied to Safety(Engineering Systems)”. 2012, The MIT Press.
[13]“STAMP 向けモデリングツール STAMP Workbench”. https://www.ipa.go.jp/sec/tools/stamp_workbench.html(参照 2019-10-1).
[14]独立行政法人情報処理推進機構(IPA) , “はじめての STAMP/STPA(実践編)~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/files/000059652.pdf, (参照 2019-10-20).