笹川平和財団

2020年度TTX（Table Top Exercise）報告書

サイバー攻撃に端を発する台湾危機における日米共同対処の課題

TTX プロジェクト メンバー一覧

小原　凡司

笹川平和財団　安全保障研究グループ　上席研究員

プロジェクトリーダー、報告書執筆

大澤　淳

笹川平和財団　安全保障研究グループ　プロジェクトコーディネーター

シナリオ監修、報告書執筆

深津　真紀子

笹川平和財団　安全保障研究グループ　研究員　（当時）

プロジェクトメンバー、報告書執筆

注：

本報告書は、笹川平和財団が2020年11月30日から12月3日まで、米国のヘリテージ財団と協働で実施したTTXプロジェクトで見いだした点をまとめたものである。国内外の政府・学術・研究機関や有識者等の方々から幅広くコメントを頂くことを意図している。

なお、本書の内容、意見、提言は執筆者の見解に基づくものであり、笹川平和財団または本プロジェクト参加者の現在もしくは過去の所属組織の見解ではない。

目次

はじめに

本報告書は、TTX2020 の結果をまとめたものである。

笹川平和財団では、2018 年以降、米国のシンクタンクと TTX（Table Top Exercise）を共同開催しており、2020 年以降はヘリテージ財団をカウンターパートとしている。笹川平和財団は、安全保障問題に関する意思決定過程に存在する日米間の差異を明らかにし、演習で示された課題を克服するための日米両国の対応策を両国政府に提言することを目的としてこれらの TTX を実施してきた。

一般的に TTX は、仮定の状況について、情勢認識および政策の選択肢を議論し、行動を決定することができるため、想定すべき様々な事案について、事前に、政策決定過程における課題を抽出し解決策を導くための有効なツールである。そのため、政府や軍、リスク管理機関、シンクタンクおよび大学などにおいて、政策立案に携わる人の教育訓練に広く利用されている。

演習期間は、2020 年 12 月 1 日～3 日（東京）、11 月 30 日～12 月 2 日（ワシントン D.C.）である。2020 年度は中国の台湾武力統一を仮定の事象とし、実際の武力行使に至る前の段階である、いわゆるグレーゾーンにおける日米両国の政策決定上の課題、共同作戦の制約を明らかにし、それらの解決策を探ることを目的とした。

日米両国は、トランプ政権下（当時）での米中対立の激化により、アジア太平洋地域における台湾の戦略的重要性がこれまで以上に高まったと認識している。台湾を見ると、1980 年以降に生まれた若年層が「天然独（生まれながらにして自らを「台湾人」と考え、そもそも中国と台湾は別の国と捉える若者たちを言う）」を形成し、「1992 年コンセンサス」を否定する蔡英文氏が総統に再選されたことで、中国との対立が激化する可能性がある。大国として台頭する中国による台湾武力統一の可能性も否定できない。このような状況下で、実際の武力行使の前に中国が台湾社会を不安定化する有効な手段としてサイバー攻撃を選択する可能性は高く、台湾がサイバー攻撃を受けた場合にどのように共同対処するかを日米間でシミュレーションすることが有意義であると考えたのである。

TTX によって明らかになった日米間の認識の差異および日米共同作戦を行う上での課題が、日米両政府および社会で広く共有され、特に、日本の安全保障政策に関する議論が活性化されることを期待している。

1　概　要

TTX は、現実に近い状況を模擬して、意思決定の演練あるいは政策・行動の検証（課題の抽出）等のために行われるが、各チームが個別の部屋に入り、各参加者がチーム内の「大統領、首相、外相、国防相、各軍指揮官など」の役割を演じる「マルチ・プレイヤー（Multi-Player）」形式のもの、明確な役割を決めず参加者全体の議論を通じて政策を決定するセミナー形式もの、あるいはその中間的なワークショップ形式など様々な形式で実施することができる。

2020 年度 TTX は、コロナ禍の影響により対面での実施を避けてオンラインで実施したこともあり、マルチ・プレイヤー形式ではなく、少人数のチーム（日本チームおよび米国チーム）が議論して政策を決定し、その政策を提示し合って次の政策を議論するワークショップ形式で実施した。マルチ・プレイヤー形式のゲームは、コントロール・チームが常に各チームの議論を把握し、意図された意思決定の演習が実施できるように新たな状況を付与する等して誘導しなければならないが、オンラインのゲームではこの仕組みの構築が困難だったからである。

2020 年度 TTX においても、参加者は、シナリオを提示してゲームを統制するコントローラー、与えられたシナリオに基づいて意思決定や判断を行う日本チームおよび米国チームのプレイヤーに分かれて演習を行った。

日米両チームは与えられたシナリオに基づいて政策決定のための議論を行い、コントロールチームの日本人メンバーが日本チームの、米国人メンバーが米国チームのゲームを統制し、日米合同ミーティングにおいて双方の意思決定の結果およびその背景を報告し、課題等について議論した。

ゲームで用いるシナリオは、新たな状況付与によるコントロール・チームの誘導がなくとも議論が発散しないよう一つに絞り込んだ。シナリオは、中国による台湾武力統一における実際の武力行使に至る前から繰り返し実行されると考えられる中国のサイバー攻撃に焦点を当てている。

シナリオの概要

ゲームに先立って、以下の背景シナリオを各チームに付与した。

- 香港情勢の台湾問題への波及
- 台湾独立運動の拡大と社会の分断
- 中国軍事演習の活発化

ゲーム開始後、各チームが情勢を認識し行動を決定するための状況として、以下のシナリオを付与した。

- 台湾に対するサイバー攻撃
  - 金融・交通システムに対するサイバー攻撃により台湾社会が混乱、中国系企業への襲撃
- 外国企業への影響

➢ マルウェアへの対処と調査

- 米国家安全保障局およびサイバー・セキュリティ企業の、台湾に対するサイバー攻撃が中国本土から行われているとする解析結果等

➢ 中台政府および台湾政府の対応

気付きおよび教訓

➢ **日米チーム間の共通点**

✓ 台湾に対するサイバー攻撃を武力行使とは認定しなかった

日本はサイバー攻撃を武力攻撃事態とみなす統一的な政策や基準が自国にはないとし、米国チームはサイバー攻撃を人道的危機と認識した。

✓ 中国による台湾武力侵攻の抑止を目的とした

✓ 情報共有を日米協力の主要な内容とした

米国チームが決定した米軍の任務は、通常の行動の中での情報収集と監視の強化に限定された。ただし米国は、抑止力が破綻した場合、台湾を軍事的に支援するとした。日本チームは米国と協力して情報収集に当たった。

✓ 日米首脳の直接対話による意思疎通を図った

米国チームは、危機の初期段階で、日米電話首脳会談を実施し、米国の視点、戦争回避の意図、台湾に対する義務などを説明することを提案し、日本チームは、台湾の状況をコントロールする政治的・軍事的協力のために、両国首脳が意思疎通する必要性に同意した。

✓ 在日米軍とインド太平洋軍の関係に対して懸念を示した

日米両チームは、在日米軍は戦略的問題に対応できず、ホノルルのインド太平洋軍が責任を持つため、危機の初期段階で東京、ホノルル、ワシントン D.C.の間で十分な意思疎通ができないのではないかとの懸念を示した。

✓ QUAD、ファイブ・アイズ、G7 等の多国間枠組みの活用を模索した

日本チームは、サイバー攻撃が世界的なリスクであることから、米国のイニシアティブによる QUAD、ファイブ・アイズ、G7 等の連携を提案し、米国チームは本事案が単に米中あるいは日米対中国の問題ではなく国際的問題であることに同意した。

➢ **日米チーム間の相違点**

✓ 日米間のサイバー空間における作戦能力に乖離が見られた

米国チームは日本のサイバー攻撃能力に懸念を示した。日本チームは、アクティブ・サイバー・ディフェンスの国内議論は十分でないとし、米国と同等の作戦は実施しできなかっ

た。

✓ 日本側により大きな法的制約が見られた（国内法の制限、国際法の解釈等）

米国チームは、日本における法的制約や必要とされる膨大な評価が、必要な行動を妨げたり遅らせたりする可能性があることに懸念を示した。

✓ 台湾との関係または台湾の位置付けについて差異が見られた

米国が有する『台湾関係法』と同様の法案制定に日本チームは消極的であり、台湾の位置付けについて日米間に差異が残ったままであった。

提　言

日米両チームは、台湾危機への対処においても日米同盟の存在が重要であることを強調した。

米国チームは、中国の武力侵攻を抑止するための日米同盟の重要性を強調し、日本が米国と共通の発想および思考を持ち、米国の目標を政治的、軍事的にサポートすることを求めた。日本チームは、台湾の状況にどう対処するかについて、日米間の調整を強化することの意義を指摘した。

➢ 日本政府に対する提言

✓ サイバー・セキュリティ担当機関の組織改編を実施すべきである。

日本では、サイバーセキュリティを所掌する複数の省庁が存在している。それらは、内閣サイバーセキュリティセンター　（NISC）、国家安全保障局（NSS）、総務省、経済産業省、警察庁、防衛省などである。列度の高いサイバー攻撃の際には、省庁間の相互連携を可能にし、日本全体のサイバー対処を指揮する合同本部等の組織が必要である。

✓ サイバー安全保障対処基本法を整備すべきである。（特に域外サイバー行動の規定）

日本には『サイバーセキュリティ基本法』が制定されているが、同法は、国内のサイバーセキュリティのみが対象であり、純粋防御的な行動を超える国内における対処や国外における対処を想定していない。国外からの烈度の高いサイバー攻撃に対処するためには日本国外でのサイバー行動も必要であり、これを規定した基本法の策定が必要である。

✓ 「台湾関係リスト」を作成すべきである

日本は、法的、政治的、制度的制約により台湾問題への軍事的介入は困難であるが、状況を把握して対応策を決定する必要があるため、台湾と関係がある官民のプレーヤーを網羅したリストを作成し、ポイント・オブ・コンタクト(POC)を定め、状況に応じて利用できる対話のチャンネルを把握する。

✓ 日本社会に対する啓発活動を実施すべきである。

本事案への対処についても、国民の支持を早急に得ることが日本政府の最重要課題の一つである。そのため、①サイバー攻撃の脅威の現実味、②台湾の地政学的重要性、③中国の台湾武力侵攻の日本への影響等について国民の理解を得るための活動を実施する。

- **米国政府に対する提言**

✓ インド太平洋軍から在日米軍へ権限を委譲すべきである。

米軍が本事案等の戦略的問題に効果的に対処するため、インド太平洋軍から在日米軍に権限を委譲する。

- **日米両政府に対する提言**

✓ インド太平洋地域におけるサイバー戦対処のための多国間枠組みを構築すべきである。

インド太平洋地域にはサイバー攻撃およびディスインフォメーション・キャンペーンに対処する多国間枠組みが存在しない。そのため、同地域において民主主義および公共のサイバー空間等を守るための多国間枠組みを構築する。

2　ゲーム・デザイン

2.1　ゲームの枠組みと参加者

2020 年度 TTX は、マルチ・プレイヤー形式からワークショップ形式の机上演習へと方式を変更し、Microsoft Teams を使用したバーチャル・ミーティングを複数回実施した。

ワークショップ形式を採用した今回のゲームでは、マルチ・プレイヤー形式のように大統領府・首相官邸、国務省・外務省、国防総省・防衛省、各軍種（陸・海・空軍および海兵隊または陸上・海上・航空自衛隊）といった役割を個々の参加者に付与しなかったが、日本チームおよび米国チームそれぞれが少人数のチーム内でインタラクティブに発言し、各参加者はそれぞれのキャリアと経験に基づき議論した。

各チーム内の議論は時差を考慮して日本・米国それぞれで、日米間の議論は合同ミーティングで実施した。ゲームの進行スケジュールを図表 1 に示す。

図表 1：ゲーム説明、状況付与、ラップアップはいずれも日米合同ミーティングにて実施

日程	1日目(11/30)		2日目(12/1)				3日目(12/2)		
時間帯	夜間		午前	午後	夜間	深夜	午前	午後	夜間
米国チーム	・ ゲーム説明 ・ 状況付与			・ チーム内議論 ・ 報告書作成	・ 1日目の結果について議論(政策、アクション等)			・ チーム内議論 ・ 報告書作成	・ ラップアップ

日程	1日目(12/1)				2日目(12/2)				3日目(12/3)
時間帯	早朝	午前	午後		早朝	午前			早朝
日本チーム	・ ゲーム説明 ・ 状況付与	・ チーム内議論 ・ 報告書作成			・ 1日目の結果について議論(政策、アクション等)	・ チーム内議論 ・ 報告書作成			・ ラップアップ

※ 青色：合同ミーティング、黄色：各チーム・ミーティング

2020 年度 TTX のプレーヤーは、日米両国から元政府高官、退役将官、シンクタンク研究員、大学教授等を招聘した。プレーヤーは国別に 2 チームに分かれ、日本チームは 6 名、米国チームは 7 名構成となった。

コントローラーの責務は、各チームの議論の方向性をフォローしつつ、シナリオに記載されていない点に関するプレーヤーからの質問対応に限定した。笹川平和財団のスタッフが日本チームのコントローラーを、ヘリテージ財団のスタッフが米国チームのコントローラーを、それぞれ務めた。

2.2　背景シナリオ

現実に即した政策決定の演練が実施できるよう、背景シナリオは可能な限り現状を基に作成した。

香港情勢の台湾問題への波及

✓　香港で逃亡犯条例改正案に反対する大規模デモが 2019 年に始まり、3 カ月にわたって続いた

ことから、キャリー・ラム香港行政長官が逃亡犯条例改正案の撤回を発表したが、同改正案の正式撤回後も香港でのデモは収束しなかった。

- ✓ デモの性質はその後、逃亡犯条例改正案への反対から、一方的な一国二制度の変質に対して異議を唱える広範な意義を持つ市民活動へと変化を遂げ、香港政府は弾圧を開始した。
- ✓ 2020 年 1 月、現職の蔡英文総統（民主進歩党）が、デモに対する香港政府の対応を見て中国共産党と「一国二制度」に対する信頼を失った有権者の支持を集めて再選を果たした。

台湾独立運動の拡大と社会の分断

- ✓ 台湾では第二の香港となることを防ぐべく独立への機運が高まり、多くの SNS サイト上で独立問題が広く取り上げられるようになった。
- ✓ 数々の独立賛成派政治インフルエンサーが様々な SNS、新聞、報道番組上で台湾独立を主張し、「台湾は台湾」ハッシュタグがツイッターの台湾トレンドランキングの 1 位となった。
- ✓ 一方で、台湾には中国との経済関係を重視する親中派が存在し続け、独立賛成派と独立反対派がデモの際に小競り合いを起こすようになった。
- ✓ 台湾の蔡英文総統は独立の動きをけん制し、「台湾の分断は避けるべきで、今こそ一丸となるべきだ。国の未来を考え、『独立』という語の使用には慎重であるべきだ」と述べた。
- ✓ 独立賛成派の動きは、独立表現の自由運動や反検閲運動へと発展した。台北、台中、高雄をはじめとする全土で独立賛成派による大規模集会が開かれ、独立反対派との衝突も生起した。
- ✓ 蔡総統が台北での集会に参加し「民意に耳を傾ける」と約束したことについて、香港メディアが「蔡総統は独立に傾き始めている」と報じた。独立反対派は台北で緊急集会を開催した。
- ✓ 中国版 SNS である対話アプリ「ウィーチャット」では、国民党を支持する学者やジャーナリストのアカウントから投稿ができなくなった。

中国軍事演習の活発化

- ✓ 台湾・米国の報道機関は、中国人民解放軍海軍が東シナ海から台湾海峡にかけての海域で上陸訓練を含む軍事演習を実施したと報じた。
- ✓ ドイツの地方紙が、「米国が台湾に防衛目的での核弾頭配備を提案した」と報じた。しかし、米国政府当局者（国防総省報道官）はこれを公式に否定した。
- ✓ 国連事務総長、カナダ首相、ドイツ首相、フランス大統領、英国首相が、いかなる国や地域への核兵器拡散も容認できないと述べる一方、台湾への核兵器配備に関する報道の信ぴょう性は低いとした。

3　ゲームの内容

3.1　ゲーム内で付与したシナリオ

台湾に対するサイバー攻撃

- ✓ 台湾の 19 時のニュース番組が「多くの場所で ATM から現金が引き出せなくなっており、主要都市で台湾鉄道や地下鉄の運行にも大幅な遅れが生じている」と報じた。
- ✓ さらに、台湾の 21 時のニュース番組が「多くの台湾企業がランサムウェア（身代金要求型ウイルス）によるサイバー攻撃を受けている（パソコン画面に『データを暗号化した。解除して欲しければ身代金をビットコインで支払え』というメッセージが表示された）」と報じた。
- ✓ こうした事態は、台湾の国家サイバーセキュリティ技術センターから日本の NISC や米国の国土安全保障省にも報告された。これを受けて日米両政府は関連省庁に対し、台湾での事態を確認して至急対策を検討するよう命じた。
- ✓ 台北で台独派の活動家の一部が暴徒化し、中国系企業のオフィスを襲撃した。中国政府は、台独派による中国系企業襲撃を暴動と断定し、暴動を抑えられない台湾政府を非難するだけでなく、台湾政府が台独派を支援している可能性に言及した。
- ✓ コンビニやデパートから人が消え、閉店も相次いだ。ATM が機能停止に陥るなか、台湾の一部銀行は週末も窓口でサービスを提供した。交通遅延と ATM 障害が続き、台湾メディアは「政府が十分な対策を講じているか疑問だ」と報じた。
- ✓ 台湾の報道番組でサイバー専門家が「台湾の国家サイバーセキュリティ技術センターは北朝鮮軍の関与を疑っているようだ」と述べた。台湾や香港で、今回の事態を北朝鮮の攻撃とする報道が増加した。

外国企業への影響

- ✓ 在台湾の日系金融機関・商社や米系金融機関のパソコンもマルウエアに感染したが、これら企業の多くは本国との回線を遮断するために適切な措置を講じたため、感染は日本や米国本土に拡大しなかった。
- ✓ 一方、台湾との通信網を遮断したため、日米企業は一部の事業活動（各種発注、決済業務、管理業務）を適時に行うことができなくなった。

- ✓ 台湾に支店や子会社を置く日本の中小企業の一部では、適切な対策が取られていなかったため、月曜日にパソコンを立ち上げると、ランサムウエア「キーナクライ（仮想ランサムウェア）」の画面が表れた。
- ✓ アイルランドにあるマイクロソフト社のサーバールームで空調装置が一時停止した。その結果、室温が上昇し、サーバーが止まる事態となった。空調装置はサーバー停止後間もなく復旧したが、サーバーの再起動には半日を要した。空調装置停止の原因は現在調査中である。

マルウェアへの対処と調査

- ✓ タピオカ・マルコ社（架空のサイバー・セキュリティ会社）が感染したマルウエアを解析し、復旧プログラムの提供を開始した。これにより、感染したシステムは続々と再開され、ネットワークの再設定も始まった。
- ✓ しかし、機能停止中に変更のあったデータの更新やバックアップデータの復元が必要であることから、完全な回復は翌週初めになると見込まれた。
- ✓ 米国家安全保障局の解析結果が米国政府から日台両政府に報告された。その内容は、タピオカ・マルコ社のマルウエア対策更新プログラムは中国・南京市（南京理工大学に置かれた人民解放軍管区第 33610 部隊）で作られた、とするものであった。
- ✓ ある民間のサイバー・セキュリティ企業が台湾におけるシステム障害の調査を行い、「台湾のシステム障害は中国本土からのサイバー攻撃によるものである可能性が高い」と発表した。
- ✓ SNS での呼び掛けに呼応し、台北、台中、高雄で、再度、大規模な集会やデモが行われた。高雄では中国系企業が襲撃された。

中台政府の対応

- ✓ 中国外交部報道官は「独立運動を食い止めるべく、台湾当局があらゆる措置を講じることを強く希望する」「台湾当局には、今回の襲撃を黙認している疑いがある」と述べた。
- ✓ 台湾政府の報道官は「台湾でのシステム障害は、中国本土からのサイバー攻撃によるものである可能性が高い」「ただし、台湾のサイバー・セキュリティ企業の分析には根拠がなく、一方的に事態を悪化させている」と発表した。

3.2　ゲームの展開（2日目）

上述のシナリオに基づき、日米各チームは「意思決定」「意思決定の根拠」「行動」の点からチーム内で議論を行った後、それぞれの議論の結果を日米合同ミーティングの場で共有した。「意思決定」は国家目標を実現するための大局的戦略である。「意思決定の根拠」は、その戦略の決定にかかわる背景の説明であり、「行動」はどのように戦略を達成するのかの方策を意味している。

日米両チームは、付与されたシナリオの中で一貫して中国の脅威から台湾を守るという姿勢を共有しており、同盟調整メカニズム（ACM）等の二国間調整メカニズムや米国大統領と日本の首相との直接対話（電話を含む）を通じて日米協力を深化させることの重要性について一致していた。しかし、両国とも、中国政府や台湾政府の意図に関する情報が不十分であると考え、具体的な行動に至る前の準備にとどまった。

日米チーム間の認識の最大の違いは、主要政策の意思決定に表れた。米国チームの意思決定は単純明快で、中国を侵攻国と見なす一方、台湾内で独立についていかなる議論が展開されようと攻撃的ではないとした。米国政策の中核は、中国による台湾への差し迫った侵攻を抑止することとされた。米国は、中国との戦争は回避したいものの台湾防衛に対して一定の義務を負っており、抑止に失敗して中国が武力侵攻を開始した場合には、台湾を軍事的に支援する準備があるとした。

対照的に、日本チームの意思決定は、台湾の事態を見守り、近い将来の展開を予測した上で不測の事態に備える、というものであった。第 1 の理由は、日本チームが、現在の台湾内の不安定な状況を日本にとって慎重を要する非常に複雑な問題と捉えたことである。第 2 の理由は、シナリオに示された段階では中国政府の政策の方向性が明確でなく、加えて、台湾内で継続する小競り合いは日本が軍事作戦を実施するために満たすべき法的要件に達していないと見なしたことである。台湾における日本企業の経済的利益や事業活動が危機にさらされ、経済的被害が日本にも及びつつあるにもかかわらず、日本チームは今回のサイバー攻撃事案は武力攻撃相当の攻撃ではないと判断した。

両国チーム間のこうした認識の違いや日本を縛る法的制約ゆえに、米国チームからは数多くの質問が投げ掛けられた。日本チームからは、台湾が今回のような曖昧な状況にある場合に、日本がどのような方法で中国への抑止効果に貢献し、米国を支援しうるかについて、説明がなされた。

以下、日米各チームの議論の詳細を説明する。

3.2.1　日本チームの議論

意思決定

1. 台湾の独立運動が今後どのように展開するのかを予測するとともに、日本単独で、および米国や国際社会と協力して、不測の事態に備える。これには幅広い活動が含まれる。
2. サイバー空間における状況についての政府全体や民間部門の認識を高めるとともに、日本の重要インフラの防護態勢を引き上げる。
3. 今回の事案への対処方法に関し、ACM 等、日米同盟の各レベルで日米間の調整を強化する。

4. 中国共産党がさらなる冒険主義へと突き進むのを抑止するため、日本の国内外で戦略的コミュニケーションを展開する。
5. 今回のサイバー事案では中国軍の関与が疑われることから、サイバー攻撃をはじめ、台湾社会をかく乱させようとする中国政府の策謀に特に焦点を当てる。

意思決定の根拠

1. 日米同盟の枠組みでは、台湾が不安定な状況に陥った場合の基本方針について未だ議論されていない。日米両政府は、例えば、台湾政府の将来の政治的実体がどうあるべきか（現状維持か独立国か）、米国政府は台湾をサイバー攻撃から守るために軍事介入を行うのか等といった重要な問題について意見交換すべきであり、もし軍事介入を行うのであれば、そのタイミングや米軍が日本に求める支援についても議論すべきである。
2. 日本政府には、台湾問題への関与を控えざるを得ない法律・政治・制度的制約がある。なかでも最大の制約は、日本政府が 1972 年日中共同声明を現在まで堅持してきたことであろう。中国政府は、この声明の「台湾が中華人民共和国の領土の不可分の一部である」という表明を、以降 48 年間繰り返してきた。共同声明は続けて「日本国政府は、この中華人民共和国政府の立場を十分理解し、尊重する」としている。
3. その他にも、法律・制度的制約は、サイバー防護の導入を複雑化するだけでなく、政府のサイバー作戦の妨げとなっている。
4. 台湾は、日本政府にとって常に政治的に慎重を要する問題である。例えば、日本が台湾を積極的に支援すると、中国は必ず報復措置を取り、それが民間部門に重大な損害を及ぼすことになる。今回のシナリオでは、台湾に対する中国の政治的方向性は公式には発表されていない。
5. 日本のいかなる軍事行動も、適用国際法の順守に加え、国内法が付与する法的権限が必要となる。しかし、今回の台湾の事態は、日本が補給やサイバー作戦を含む対外軍事行動を行うための法的権限を生じさせない。日本が台湾に軍事的に介入するためには、暴力行為が日本の安全保障に波及しかねないほど深刻化・激化することが条件となる。また、台湾内の小競り合いは国際法上の国内紛争とみなされるための要件も満たしていない。
6. 日本は、自衛隊をはじめとする国家機関が日常的に行っている警戒監視活動など、すでにある手段を活用すべきである。米国とはこれまでに数多くの合同演習を行っており、QUAD 参加国による演習の経験もある。したがって、米国が求める場合には、日本はこれら一連の活動を利用し、中国への抑止効果をもたらす数多くの行動を取ることができる。

行　動

1. 日本首相は、台湾事案の制御に向け、同盟調整メカニズム（ACM: Alliance Coordination Mec

hanism）[1]各レベルでの日米間の調整強化を命じる。これには、2015 年「日米防衛協力のための指針」に基づく、動向やサイバー事案に関する情勢認識共有の向上が含まれる。

2. サイバー攻撃は世界的リスクと評価されることから、日本政府は、米国、ファイブ・アイズ（米国、英国、カナダ、オーストラリア、ニュージーランド）、G7（米国、英国、カナダ、フランス、ドイツ、イタリア、日本）を通じ、国際社会に向けてサイバー・セキュリティ意識を高めるよう提唱する。国連安全保障理事会に関しては、日本は現在理事国ではないため、志を同じくする米国その他の理事国に依頼する必要がある。
3. 戦争までエスカレートするといった最悪のシナリオを回避すべく、事態の制御・緩和に向け、日米同盟の枠組みを通じて台湾に対する政治・軍事協力に関する基本方針を共有する。
4. 自衛隊の対外行動の法的権限が生じないため、日本は軍事行動を取ることができない。こうした状況下、日本は最悪のシナリオに備えた即応性向上に止まらねばならない。中国の強圧的な独立阻止の動きに対応するための防衛態勢強化である。また、弾道ミサイル発射や中国の作戦と同期させたサイバー攻撃等、想定される北朝鮮の動きに対し、警戒レベルを引き上げる。

3.2.2　米国チームの議論

意思決定

1. 中国の台湾武力侵攻を抑止する。抑止に失敗して台湾が攻撃された場合、米国には台湾を軍事的に支援して市民を守る準備がある。米国は中国による軍事的台湾併合を容認せず、これを阻止するために軍事介入する、という点を米国として極めて明確にすべきである。これは米国が長年取ってきた、そして今後も維持していく姿勢であり、米国の意思決定の根幹を成す。
2. 目的達成のための米国の行動に対する日本の政治的・軍事的支援を確保する。台湾問題について、日米は共通の考えを持つ必要がある。

---

[1] ACM は、「閣僚レベルを含む二国間の上位レベル」、内閣官房、外務省、防衛省、自衛隊、関係省庁の代表（日本側）、国家安全保障会議、国務省、在日米大使館、国防省国防長官府、統合参謀本部、太平洋軍司令部、在日米軍司令部、関係省庁の代表（米国側）から構成される「同盟国調整グループ（ACG: Alliance Coordination Group）」、外務省北米局長（日本側）、在日米軍副司令官（米国側）を代表とする「日米合同委員会（JC: Joint Committee）」、統合幕僚監部、陸上・海上・航空幕僚監部（日本側）、太平洋軍司令部、在日米軍司令部（米国側）の代表から成る「共同運用調整所（BOCC: Bilateral Operations Coordination Center）」、各自衛隊及び米各軍の構成組織の代表による「各自衛隊及び米軍各軍間の調整所（CCCs: Component Coordination Centers）」によって構成される。

3. 日米台３カ国間で軍事・情報・政策面での調整を行う。特に日本に対して、こうした調整への関与を要請する。米国は台湾との間ではある程度の統合をすでに実現しており、こうした枠組みを拡大して日本の参入を目指す。

意思決定の根拠

1. 台湾内で独立について議論されようと、台湾は武力行使しているわけではない。重要なのは蔡総統が独立支持か反対かではなく、台湾が自由で民主的な政治体制であり、人々が自由に意見を述べられることである。台湾で何が論じられようと、中国が台湾に武力行使する理由にはならない。台湾独立回避を企図した中国の行動が正当なものか、米国は注意している。
2. 今回のサイバー攻撃は日本に直接影響を及ぼしており、そのことは同盟国間で調整を行う新たな理由となる。
3. 日米同盟における米国の目的遂行能力（日米安全保障条約で定められた日本に対する責務を遂行する能力）が、中台間の危機によって脅かされている。

行　動

1. 米国大統領が直ちに日本の首相と電話会談を行い、米国の認識、意図およびその根拠を説明する。その説明は、米国は戦争回避の意図を有しながらも、台湾に対して一定の義務を負っていることを明確にし、戦争を回避できない場合、中国の攻撃から台湾を防衛するために戦う準備があることを示すものである。
2. 日米二国間調整メカニズムを重視し活用する。これは防衛協力に止まらず、政策調整も含む。
3. サイバー・防衛分野の人材を台湾に追加派遣するとともに、日本と台湾に対し、インド太平洋軍への人員派遣を要請する。

図表２：日米チームの意思決定と行動の比較

	日本チーム	米国チーム
意思決定	1. 台湾事案の今後の展開を予測するとともに、不測の事態に備える(政治・軍事・経済面を網羅し、日本単独と米国との協力の両方で実施)。 2. 政府全体や民間部門のサイバー状況認識を高め、日本の重要インフラ防護態勢を引き上げるとともに、エストニア、ウクライナ、韓国での過去のサイバー事案を参照する。 3. 本事案への対処方法に関し、ACM 各レベルで日米間の調整を強化する。 4. 中国共産党の冒険主義を抑止するため、日本内外で戦略的コミュニケーションを展開する。	1. 中国による台湾への軍事侵攻を抑止する。抑止に失敗して台湾が攻撃された場合、米国には台湾を軍事的に支援する準備がある。 2. 米国の目的に対する日本の政治・軍事面での支援を確保する。 3. 日米台３カ国間で軍事・情報・政策面での調整を行う。日本には、こうした調整への関与を要請する。
意思決定の根拠	1. 日米同盟では、台湾内が不安定な状況に陥った場合の基本方針について、未だ議論されていない。 2. 台湾への踏み込んだ関与に対しては複数の制約がある（法律・政治・制度面）。 3. 台湾は政治的に慎重を要する問題である。また、今回の動向の背景や方向性が不明確であり、台湾に対する中国の政治的方向性も公式には発表されていない。 4. 日本の軍事行動には、法的制約（国内法・国際法）が課されている。 5. 台湾の事態は武力攻撃とは見なされないため、日本が中国抑止に向けて米国を支援する際には、自衛隊の日々の警戒監視活動のような既存手段を活用し、法的制約を伴わない行動を取るべきである。	1. 独立についていかなる議論が展開されようと、台湾は武力行使を行っていない。 2. 3. 今回のサイバー攻撃は日本に直接影響を及ぼしており、同盟国間での協力の理由となる。密な協力は主目的である抑止の強化につながる。 4. 台湾危機によって、米国の日本に対する責務の遂行が脅かされている。
行動	1. 首相は台湾事案の制御に向け、「日米防衛協力のための指針」に基づく動向やサイバー事案に関する情勢認識共有の向上	1. 大統領は首相と電話会談を行い、米国の根拠や意図を説明する。

	を含む、ACM 各レベルでの日米間の調整強化を命じる。 2. 米国、ファイブ・アイズ、G7 等を通じ、国際社会にサイバーセキュリティ意識を高めるよう提唱する。 3. 事態の制御・緩和に向け、日米同盟で台湾の政治運動や政治・軍事協力に関する基本方針を共有する。 4. 中国の独立阻止の動き（北朝鮮による弾道ミサイル発射やサイバー攻撃等も含む）に対する防衛態勢を強化するとともに、当面起こりうるシナリオを検討する。	2. 単なる防衛協力にとどまらず政策調整をも含んだ二国間調整メカニズムを発動すべく、同意を要請する。 3. サイバー・防衛分野の人材を台湾に追加派遣するとともに、日本と台湾に対してインド太平洋軍への人員派遣を要請する。

出所：日米各チームのプレゼン資料と議論

3.2.3 議論の中で見いだされた課題（日本チーム報告）：台湾の独立運動

日本特有の課題

日本チームは、日本政府が台湾の独立運動に対する方針を決定する際、以下の 4 つの要因が円滑な意思決定の妨げになると懸念を示した。

1. 日本と台湾の間には、情報交換のための正式な枠組みが存在しない。このため、台湾内の動向に関する正確な情報が適時に伝わらない。
2. 1972 年の日中共同声明発表以降、日台間では正式な外交関係が中断している。以来、日本には、日中共同声明に基づく政治原則に従うこと、中国が台湾との平和的解決を追求する限り、台湾との関係を非政府間のものに止めることが求められている。このため、台湾での独立運動や中国の強制的な再統一への対応を含め、日本政府の対台湾方針は未だ議論もされていない。
3. 日台間の交流は極めて限定的で、経済交流が中心である。自衛隊と台湾軍の交流は行われていない。
4. 日本政府は、その必要性を認識しているにもかかわらず、未だ戦略的コミュニケーション戦略を策定しておらず、戦略的コミュニケーションを計画・指揮する本部も創設していない。

日米双方に関連する課題

1. 台湾海峡危機は、日本および日本に駐留する在日米軍を必然的に巻き込む事態であるにもかかわらず、日米間の対話が進んでいない。
2. 中距離核戦力（INF）全廃条約後の米国の地域核抑止態勢について、ほとんど議論が進んでいない。米国の中距離核兵器の開発が完了すれば、日本は当該兵器の配備先候補の 1 つとなる可能性があるが、日本政府が自国領土への INF 配備を認めるか否かについて議論が必要である。

3. 台湾の将来的な位置付けについて、日米間で協議が行われていない。これには、独立運動が国家解放戦争と捉えられるか否かといった点が含まれる。
4. 日米協力を通じた台湾情勢のエスカレーション制御については、日米間で政治目的や優先順位（経済安定性、民主主義、自国民の救助・輸送など）が異なる可能性がある。
5. 台湾周辺で作戦を遂行する米国艦艇への後方支援（燃料補給、物資・人員輸送など）に関する協議も不足している。将来台湾への武力攻撃が発生した場合、日本は米国が要求するものすべてを提供できない恐れがある。
6. 中国の台湾武力侵攻などの台湾海峡危機への対応を含め、中国の冒険主義の抑止を目的とした日米協力態勢の整備がほとんど進んでいない。

3.2.4　議論の中で見いだされた課題（日本チーム報告）：サイバー事案

日本の要因

日本チームは、日本政府がサイバー事案への対応を決定する際、以下の 8 つの要因が円滑な意思決定の妨げになると考えた。

1. 日本で安全保障上のサイバー防衛を担当する政府機関（NISC、NSS、警察庁、防衛省の 4 つ）は、それぞれがほぼ独自に取り組みを進めており、相互の調整はあまり行われていない。
2. これら政府機関に認められているのは、受動的なサイバー対処の実施に限られ、平時における国外での攻撃的サイバー作戦の実施は禁じられている。
3. 本来、日本全体のサイバー作戦を指揮すべき合同本部が存在しない。
4. 日本ではサイバーセキュリティ基本法こそ制定されたものの、詳細な手続きは定められていない。また、同法は日本国内に適用されるが、国外への適用が可能か否かに関する規定はない。
5. 自衛隊のサイバー防衛隊は、日本に対する武力攻撃に該当するものでない限り、重要インフラ関連の事案に関与できない。重要インフラの防護については、産業界や各企業が自らの保有資産をサイバー攻撃から防護する責任を負い、自衛隊のサイバー防衛隊は平時には企業による防護を支援する責任さえ負っていない。サイバー防衛隊の対象範囲は自衛隊に限定されている。
6. サイバー防衛作戦と宇宙防衛作戦は切り離すことができないにもかかわらず、日本では別々に扱われている。
7. サイバー攻撃を武力攻撃事態と見なすための具体的な基準がない。
8. 日本では、デジタルインフラ整備に向けた政策が定められたにもかかわらず、個人情報や通信の秘密保護に関する議論が進んでいない。

日米双方に関連する要因

1. サイバー攻撃を日米安全保障条約第 5 条に規定される「武力攻撃」事態と見なす上での、統一方針も政治的基準も存在しない。

2. 中国軍が関与するサイバー事案についての日米政府間での協議が不足している。
3. サイバー担当の連絡調整官が置かれていないため、日米の担当者間における運用面での協力が脆弱である。

3.2.5　議論の中で見いだされた課題（米国チーム報告）

1. 台湾への攻撃がもたらす軍事的脅威や最適な対処法について、日米間で合意を形成すること。ここで言う「合意」は必ずしも協定の締結ではなく、意見の一致を意味している。
2. 危機の発生時だけでなく、事前に日米台間で戦術協力の強化を図ること。３カ国（米国チーム報告のママ）共同での調整、シナリオ検証、装備の事前配置、演習のやり方など、いずれにとっても抵抗のない範囲で、考え得る限りの事案について考察する。
3. 事案対処は最終的に政治判断となるため、日米政治高官レベルでの政策調整を推進すること。
4. 武力行使が開始される以前に、議会と協議し、適切に議会の関与を得ること。米国大統領は、日本首相と電話会談をする必要があるほど事態が深刻な場合、軍事委員会委員長、外交委員会委員長、議会指導部に連絡して話し合いを始める準備ができていなければならない。
5. 戦略的状況についてパートナー国と協議し、戦略を最大限有効なものとすること。危機の発生前にパートナー国や同盟国に米国と同様の意見を表明するよう説得するだけではないが、ひとたび危機が発生すれば混乱が生じて説明が難しくなる。今回のシナリオにも描かれているように、相反する情報が飛び交い、（パートナー以外の）別の国や関係者も関係してくる。中国は、誤情報や偽情報を流布するだけではなく、地域全体に互いへの非難の種を植え付け、事態を複雑化しようとするだろう。

3.3　ゲームの展開（3日目）

日米両チームは、2 日目の日米両国の意思決定と行動に基づき、継続した政策決定のための 3 日目のゲームを実施した。

米国チームは、抑止政策の継続を強調するとともに、日本等の同盟国に対し、引き続き米国を政治的・軍事的に支援するよう要請した。米国チームはまた、日本の法的制約やサイバー攻撃への対処能力に懸念を示し、共同作戦の障害になりかねないとした。

一方、日本チームは、現状の制約の下で日本がいかにして米国の要請に応じ得るのかにつき、時間を割いて説明した。

以下、日米各チームの議論の詳細を説明する。

3.3.1　米国チームの議論

意思決定

1. 基本方針は２日目から変化はない。米国は、新たに大規模な軍事行動を起こすといった劇的で挑発的な動きは一切取らず、現行の抑止政策をそのまま続けるべきである。情報収集と警戒監視の強化に最大限の努力が必要であるが、これらは通常の行動の範囲内で行うべきである。

2. 引き続き、同盟国やパートナー国に対して追加アセットを要請する。台湾や地域の安定は多くの国の関心事であることから、米国は台湾事案を多国間の問題とするべきである。

3. 今回の台湾事態を、進行しつつある人道的危機と見なす。この危機は、サイバー攻撃、軍事行動の脅威、国民全体の混乱状況から見て、適切な人道的対応が正当化されるだけでなく、そうした対応が余儀なくされるほどの水準にある。（したがって米国や日本、その他の国々は、別の形で台湾を支援すべき理由が生じる。各国は、事態に対する関心を引き続き示すとともに、中国のさらなる行動への抑止となるような形で行動することができる。）

4. 事態がさらにエスカレートしても対応できるよう、地域における影響力工作を強化する。今回の事態が中国政府の壮大な計画の一部である可能性が高く、事態がエスカレートする恐れを認識すべきである。また、中国政府が今回の事態に関与していないとしても、中国によるエスカレーションは依然として起こり得る。外交やパブリック・ディプロマシー等の手段を用い、マスコミも巻き込み、日米の考えを明確にする戦略的メッセージを発信することが重要である。

意思決定の根拠

1. 直近の展開は危機の性質を根本から変えるものではなく、米国側が新たに積極的な行動に出ることを正当化するだけの劇的な変化は見られなかった。

2. 今回のサイバー攻撃が台湾や台湾社会に引き起こしたあらゆる混乱を考えると、事態は正に人道的危機へと至りつつあり、人道支援実施の理由となる。

3. 米国防兵站局へのサイバー攻撃は、中国によるさらなる軍事活動を示唆している。

4. 米国はすでに当該地域にアセットを有し、水面下で進行中の危機に対処する許可も得ている。

行　動

1. 米沿岸警備隊長官による台湾訪問を実施する。これは、米国が台湾への支援を約束するという意思を目に見える形で示すものであり、具体的事態への支援を提供する。米国は、日本にも同様の行動を取るよう勧める。このように非軍事的でありながら軍が絡んだ方法で支援表明を行うのは、挑発的になり過ぎない効果的なやり方である。（中国は抗議すると思われる。）

2. 米各省庁の人道問題の担当職員や専門家を人道支援・災害救援調整官として台湾に派遣し、助言を提供する。さらに、こうした行動を正当化するほど深刻な人道的危機が発生しているという認識に日本等の同盟国や友好国が同意することを前提として、これらの国々にも同様の行動を取るよう提案する。

3. 今回の事態に関心を持つ東南アジア諸国連合加盟国や欧州の同盟国と協調外交を展開し、情報を交換することで、こうした国々に台湾の持つ重要性を理解させるとともに、本事案は台湾の

国内問題ではなく、安全保障や経済のサプライチェーンという点から地域全体の問題である点を理解させる。

3.3.2　日本チームの議論

日本チームは、新たな意思決定をするのではなく、いかに日本の状況や努力を米国に理解してもらうかについて議論を重ねた。

議論の焦点

1. 今回の危機において円滑な日米協力を阻みかねない法的制約等の障害を減らす一方、本シナリオ上の不測の事態に米国や同盟国と連携して対処できるよう現行の法的枠組みを最大限活用するという日本側の意欲につき、米国の理解を深める。
2. 本事案への対処方法に関する日米間の調整を強化するとともに、日本は米国の要請に応じて迅速に支援を提供する準備があるという点につき、米国の理解を深める。
3. 日本のサイバー攻撃対処能力についての米国側の懸念を踏まえ、サイバー攻撃に対する日本の備えのレベルに関し、米国が抱く不安を緩和する。

3.3.3　議論の中で見出された課題（日本チーム報告）

日本の要因

1. 日本が法的問題やその影響について膨大な評価を行うことは、多大の時間を費やすことによって適時に必要な行動をとる妨げとなりかねない。（政策決定に過大な時間を要する。）
2. 日本における法制度・組織面での縦割り現象が、意思決定をより煩雑で難しく時間がかかるものとしかねない。

米国の要因

1. 在日米軍は、戦略的問題については、扱うことも答えることもできず、こうした懸念への対処に必要な関心をワシントン D.C.政界から引き出せるとも思えない。在日米軍は実際には、米国チームが望むほど迅速にも的確にも対応できないのではないかと懸念される。
2. ワシントン D.C.からの遠さという点では、ホノルルのインド太平洋軍司令部も東京と同じくらい離れている感がある。今回の危機の初期段階で機敏に対応できるだけの十分な連携が米国側の各種関係者や指揮系統に存在するのかを、米国チームは疑問に感じている。
3. どの時点をもってサイバー攻撃を軍事攻撃として扱うべきかが明確ではない。この部分は非常にあいまいで、いまだかつて適切な定義がなされていない問題である。

4　教訓と課題

4.1　日米チームの共通点

1）サイバー攻撃は武力攻撃ではない

米国チームは、どの時点をもってサイバー攻撃を軍事攻撃と見なすべきかは不明確であり、未だ適切な定義はされていないとした。その上で、台湾社会で発生したあらゆる混乱を考慮し、今回のサイバー攻撃を人道的危機と見なした。

日本チームも今回のサイバー攻撃を武力攻撃と認識せず、サイバー攻撃を日米安全保障条約第5条に規定される「武力攻撃」事態と認定する統一方針も政治的基準も存在しないとした。また、現在の日本法の下では、日本国外でのサイバー攻撃は武力攻撃とは見なされないとした。

2）抑止政策と情報収集の必要性

米国チームは、中国による台湾武力侵攻を抑止するため、大規模な軍事行動を起こすといった挑発的な手段を取らず、通常の行動の範囲内で情報収集と警戒監視の強化を行うとした。ただし抑止に失敗して台湾が攻撃された場合、米国は台湾を軍事的に支援する準備があるとした。

日本チームは、台湾で何が起きているのか、背後に存在するのは何者か、攻撃者の目的は何かを理解するための情報収集強化が必要とした。日本チームの政策は米国チームと同様、さらなる情報収集を行うと同時に、米国と連携して中国武力侵攻を抑止するというものであった。

情報収集の重視は両チームの一致点であるが、米国の情報収集は中国の新たな行動を察知するためであり、日本のものは事案の背景を理解するためであるところに差異がある。この差異は、日米間の政策決定の思考過程の差異とそれに伴う政策決定に要する時間の差異を示すものである。

3）日米同盟の重要性

米国チームは、中国の侵攻を抑止し台湾を防衛するための日米同盟の重要性を強調し、日本が米国と同じ考えを持ち、米国の目的を政治面・軍事面で支援するよう求めた。同時に、日本における法的制約や事態評価の膨大な作業が、政策決定と行動を遅らせる恐れがあると懸念を示した。

日本チームは、台湾事態への対応について日米間での調整強化の重要性を指摘し、平時と重要影響事態のそれぞれにおける米国の後方支援要請を検討した。また、米国チームの懸念を理解し、今回の目的に向けた既存の法的枠組みの活用方法を説明することで、米国側の不安緩和に努めた。

4）両国トップによる直接対話の重要性

米国チームは、危機の初期段階で米国大統領と日本首相との間で電話会談を実施し、米国の視点、戦争回避の意図、台湾に対する義務といった米国の意図と根拠を説明することを提案した。

日本チームは、台湾事態の制御・緊張緩和に向けた政治的・軍事的協力に関して共通認識を得るべく、両国首脳が直接意思疎通を行うことに同意した。

5）在日米軍とインド太平洋軍への懸念

米国チームは、今回の危機の初期段階において、在日米軍、インド太平洋軍、国防総省およびホワイトハウス間で十分かつ円滑な意思疎通が図れるかどうか疑問を呈した。

日本チームも、在日米軍とインド太平洋軍の関係について同様の懸念を示した。日本チーム内には、インド太平洋軍から在日米軍への権限委譲を望む声もあった。

6）QUAD、ファイブ・アイズ、G7 等の多国間協力の重要性

米国チームは、今回の事案を多国間の問題とするべきであるとした。

日本チームも、サイバー攻撃という性質に鑑み、米国の主導の下で QUAD、ファイブ・アイズ（米国、英国、カナダ、オーストラリア、ニュージーランド）、G7（米国、英国、カナダ、フランス、ドイツ、イタリア、日本）をはじめとする国際社会と連携することを提案した。

4.2　日米チームの相違点

1）サイバー作戦能力に関する日米間格差

米国チームは、日本のサイバー攻撃対処能力に懸念を示し、攻撃的サイバー作戦を実施する場合、どの機関や省庁が遂行し、どこがその権限を与えるのかという問いを投げ掛けた。

日本チームは、攻撃力を行使する能力と権限を有しているのは自衛隊だけであると説明したが、内閣官房にも攻撃的サイバー作戦を指揮する本部は存在せず、日本は武力攻撃事態においてすら攻撃的作戦の実行が難しく、米国と連携して攻撃的サイバー作戦を実施する準備ができていない。

日本チームはさらに、日本にはアトリビューション（攻撃者の追跡・特定）に代表されるサイバー諜報能力が欠如しており、米国のサイバー諜報能力とは大きな開きがあると認めた。

2）日米間の法的制約の差異（国内法、国際法）

日本が軍事行動を起こす際の、国際法の解釈は極めて厳密であり、法的権限を付与する国内法の規定は極めて厳格であり、日本の安全保障協力に対する米国チームの懸念を増大させた。

3）台湾との関係

日本には米国の「台湾関係法」と同様の法律が存在しないため、台湾の位置付けが明確でなく、台湾との協力について議論もなされていない。

こうした課題を解決するため、米国は日本も「台湾関係法」と同様の法律の制定を提案したが、日本は消極的で、台湾との情報共有のために「台湾関係リスト」を作成すべきであると主張した。

5 提　言

2020 年度 TTX に基づき、以下の点を本報告書の結論として日本政府と米国政府に提言する。

日本政府に対する提言

1）サイバーセキュリティ担当機関の組織改編

サイバーセキュリティ担当機関の構造を縦割り型から相互連携可能な水平型へと改編することを提言する。

日本政府で協調的サイバー防衛作戦を担当する機関としては、NISC、NSS、警察庁、防衛省などがそれぞれほぼ独立して存在し、他機関との調整は少ない。加えて、サイバー事案を制御すべく日本全体のサイバー作戦を指揮する合同本部も存在しない。こうした状況では、突然のサイバー攻撃に対し、米国やその同盟国と手を組んで効率的に対処することは難しい。

2）サイバー安全保障対処基本法の整備

サイバー安全保障対処基本法の整備を提言する。（特に域外サイバー行動の規定）

日本には『サイバーセキュリティ基本法』が制定されているが、同法は、国内のサイバーセキュリティのみが対象であり、純粋防御的な行動を超える国内における対処や国外における対処を想定していない。国外からの烈度の高いサイバー攻撃に対処するためには日本国外でのサイバー行動も必要であり、これを規定した基本法の策定が必要である。

3）台湾関係リストの作成

日台関係の全体像を把握し、情報共有のチャンネルを確保するため、日本の政府機関や民間企業を含むあらゆる主要関係者を網羅した包括的なリスト「台湾関係リスト」の作成を提言する。

台湾は日本にとって常に政治的に慎重を要する問題であり、日本政府には、台湾問題への関与を控えざるを得ない法律・政治・制度的制約がある。日本政府は 1972 年の日中共同声明の調印後、台湾は中国の領土の不可分の一部であるという方針を尊重せざるを得ず、その結果、台湾との関係は経済活動に限られているため、情報共有のチャンネルを確保することが重要である。

4）日本国民の啓発

日本国民に対する啓発活動の実施を提言する。

第一に、破壊的なサイバー作戦の脅威がすでに日本における現実的な問題となっていること、第二に、台湾が日本の安全保障にとって戦略的・地政学的に重要であること、第三に、中国人民解放軍による台湾武力侵攻が予想され、日本に多大の影響を及ぼすことを認識してもらう必要である。

日本政府にとって、危機への対処策を決定する上で重要な課題の 1 つは国民の支持を早急に得ることであるが、日本国民は、一般に、中国や北朝鮮といった近隣諸国からのサイバー攻撃という差

し迫った脅威だけでなく、中国の台湾再統一の意図についても、台湾の戦略的重要性についても認知度が低い。

米国政府に対する提言

1）インド太平洋軍から在日米軍への権限委譲

太平洋地域における台湾その他の友好国を守るため、その権限をインド太平洋軍から在日米軍に移すことを推奨したい。

在日米軍は、戦略的問題に対応する権限を有していないため、戦略的問題に関してはハワイのインド太平洋軍に助言を求める必要があり、インド太平洋軍がワシントン D.C.に援軍要請等を行う。こうした体制では、適時に事態に対応することが難しくなる可能性がある。

日米両政府に対する提言

1）インド太平洋地域におけるサイバー戦対処のための多国間枠組みの構築

日米両政府に対し、サイバー攻撃からインド太平洋地域の国や地域を守るための枠組み構築を検討するよう提案する。

インド太平洋地域には、欧州のようなサイバー戦対処のための枠組みが存在しない。例えば欧州連合（EU）は、ロシアの偽情報戦に対処する枠組みを構築した上で、偽情報に対抗し EU の民主主義制度や公共サイバー空間を守るための活動を展開している。

6　結びに代えて

バーチャルでの実施による種々の制限にもかかわらず、中国の台湾に対するサイバー攻撃をめぐって幅広く実り多い議論を行うことができた。

ゲームの中で、台湾の戦略的重要性、中国の侵攻を抑止し台湾を守る上での日米同盟の必要性、および QUAD、ファイブ・アイズ、G7 との多国間協力の意義に関して意見の一致を見た。加えて、日米連携を妨げかねない課題に関する認識を共有した。第 5 章に記した日米両政府に対する提言は、ゲームによって抽出された課題を解決するためのものである。

サイバーセキュリティ政策を策定する際、本報告書が日米両国の政府、省庁、政策立案者、研究者等への有益な示唆となれば幸甚である。

最後に、2020 年度 TTX に日米両国から快く参加してくださったすべての方々に心から感謝の意を表したい。

【補足資料】

米国チームの補足コメント

1. 軍事衝突が発生すれば台湾の南北両側から作戦が進められる可能性が高いため、危機発生より十分に前に、地域内の友好国や同盟国（フィリピン、シンガポール、マレーシア、太平洋諸島）との間で通行や上空飛行に関する調整を行っておく必要がある。フィリピンを挙げたのは、戦略的要衝に位置し、米国と緊密な関係にあることが大きい。シンガポールも同様の理由で挙げており、加えてフィリピンよりキャパシティが大きいことも背景にある。マレーシアは、シンガポールから発進する航空機による領空利用に関してマレーシアの許可が必要になるためだ。太平洋諸島は、米国の対応における重要な戦略的結節点として選ばれた。ほかにも数多くの国との調整の必要性が考えられるため、米国は政治的・外交的視点から地域全体を巻き込むとともに、何らかの調整的取り組みが必要である。
2. 米国と同盟国は、その他のパートナー国から米国の考えに対する支持を得るべく、米国の姿勢や目的を説明する広報文化外交を展開すべきである。
3. 今回の紛争は台湾のせいではなく、責めを負うべきは中国である。今回のシナリオでは、問題を引き起こしたのは中国であることを認識し、惑わされないようにせねばならない。

日米両チームは、認識や考え方の差異を埋め、より広く意見の一致を見られるよう、３日目にもジョイント・ミーティングを開催した。

日本チームによる意思決定の背景説明

1. 平時連携の法的枠組み

日本チームは、平時の日米連携に資する国内の関連枠組みを重視したいと考えている。2 日目のジョイント・ミーティングで説明したように、日本の軍事行動にはいかなるものであれ、日本の国内法に則った国内法上の法的権限が必要となる。これは基本的な憲法上の制約であり、米国側にとっては期待を裏切る点かもしれない。それでも日本には現状、今回のシナリオに適用可能な関連枠組みが以下の 3 つ存在する。

1 つ目は情報収集活動という枠組みである。自衛隊は、任務の遂行に向けて調査や研究を行う柔軟な権限をすでに有している。自衛隊は実際これまで、中東や東シナ海を含む世界各地で警戒監視活動を数多く行い、情報を収集してきた。こうした活動は、他国の領土主権の尊重や武力行使の禁止といった国際法の規定を順守して行わなければならない。したがって、公海、公海上の空域、宇宙空間で行う必要があり、さらに、サイバー空間には領土主権が適用されないとする米国と同様の立場を取れば、おそらくサイバー空間でも実施可能となる。

2 つ目は、米国やその他の国々のアセットを防護するための武器使用であり、これも特に平時においては重要な枠組みである。自衛隊にはこの枠組みの下、米国やその他パートナー国の艦艇、船

舶、航空機を含む武器・装備品等を防護するための武器使用が認められている。ただしその際には、以下の 6 つの条件を満たす必要がある。

1） 防護されるアセットが、自衛隊と連携して日本の防衛に資する活動に現に従事していること。よって、米国の全アセットがこの場合の自衛隊による防護範囲に該当するわけではない。

2） 現に戦闘行為が行われている現場以外で防護が行われること。この条件は、平時の話である限りは問題とならないが、政府が状況をどう判断するかによっては影響を及ぼす。

3） アセット所有国（今回の場合は米国）から要請か同意を得ること。

4） 日本の防衛大臣の許可を受けて防護が行われること。

5） 他国の領土主権を侵害しないこと。つまり、防護は公海上などで行われなければならない。

6） 武器使用は受動的であること。すなわち、反撃は許されない。

最も重要なのは国会の承認を得る必要がない点で、そのため、より円滑に即時の行動を取ることが可能となる。

3 つ目は、重要影響事態という枠組みである。この枠組みの下、内閣が日本の平和と安全に重要な影響を与える事態が存在すると判断した際には、自衛隊に対し、米国その他の国々に必要な支援活動を提供する権限が付与される。こうした事態には、日本や米国に対する武力攻撃に至る可能性や確率が高い場合が含まれる。このような事態が認められた場合、自衛隊は、後方支援、捜索救助、船舶検査を含む支援活動を行う権限を持つ。この枠組みについては国会による承認が必要で、状況に応じて、事前または事後の承認が必要になる。

日本は平時においては、これら 3 つの法的枠組みを組み合わせて使うこともできる。これらの枠組みの使用は純粋な法律問題ではなく、むしろこうした法的枠組みをどう活用し運用するのかという政治問題である。したがって、これらの法的枠組みを生かすも殺すも、日本の政府や内閣次第であり、ある程度は国会にもかかってくる。

要約すると、これらの枠組みは法的制約であるかもしれないが、それと同時に、現実の事案に即して柔軟に運用できるよう、日本政府にある程度の自由裁量を与えている。その点では、日本の安全保障上の利益を国民に説明可能な方法で最大化するための、国策意思決定のツールとなるものでもある。

日本が平時に攻撃的サイバー能力を展開するための余地

日本は、不当な国家や非国家主体に対して攻撃的サイバー作戦を展開するための合法的選択肢については、少なくとも国際法上合法なものについてはすでに数多く有している。日本政府はまた、サイバーセキュリティに関する国連政府専門家会合やサイバーセキュリティに関する国連オープン・エンド作業部会をはじめとする多国間会議でも、サイバー空間に適用される国際法規定の明確化や定義に向け、強力な指導力を発揮している。その目的は、日本や攻撃の標的となり得る国々が、外

国や非国家主体による悪意あるサイバー攻撃に対し、より幅広い報復措置を取れるようにすることにある。

今回のシナリオでは、悪意あるサイバー活動の被害が日本国内の民間企業にも及んでおり、その発生源は中国本土の南京と考えられている。たとえこうした活動が中国のせいではないとしても、日本は依然として、中国が自国領土を発生源とする越境サイバー攻撃の防止・停止・収束に向けた適切な注意義務を履行しなかったという理由で、何者がサイバー攻撃や偽情報作戦を仕掛けたかにかかわらず、攻撃停止に向けた合法的対抗措置として攻撃的な越境サイバー作戦を展開する権利を持つ可能性がある。

ただし日本には現在、こうした行動を取る国内法上の権限はない。日本がサイバー空間における敵の活動を妨害すべく攻撃的サイバー能力を開発しているのは事実であるが、日本法の下でそうした能力の行使が許されるのは、武力攻撃に対して国を自衛する場合に限られる。

したがって、平時においては、日本は攻撃的サイバー能力の行使を許されていない。しかしこれは、日本法がこうしたサイバー能力の行使を禁じていることを意味するものではない。憲法における通信の秘密条項や「不正アクセス行為の禁止等に関する法律」をはじめ、サイバー作戦への国内法上の制約は存在するが、こうした法律の域外適用については明らかにされないままとなっている。その意味では、平時における攻撃的サイバー能力を許可し最大限に活用する道を選んだ場合、日本にはそのための国内法を策定・制定する可能性が残されていると言えるかもしれない。

結論としては、日本が米国だけでなく米国防総省の前方防衛戦略とすら歩調を合わせて非物理的サイバー攻撃能力を行使できるだけの権限を法制化するという改善の余地は、理論的には存在する。さらに、調査や研究を行う権限はすでに現行法制の下で付与されていることも強調したい。

2. 米国の要請に応じた自衛隊の後方支援

可能な行動の一覧

米国から要請があった場合、日本は平時でも重要影響事態でも米国を多彩な手段で支援することができる。こうした手段には、共同声明、共通の地域図、情報共有、後方支援、弾薬提供、燃料補給、戦闘作戦行動のために発進準備中の航空機に対する整備が含まれ、下記の図表 3 に示している。

平時や重要影響事態での政策問題に関する共同声明は、日米共同声明については制約なく行えるが、3 カ国共同声明の場合には日本側の政治判断が必要となる。軍事問題に関しては、平時に共同声明を出すのは非常に難しい。共通の地域図や情報共有については、平時に日本が台湾当局と直接情報を共有するのは難しいため、米国を介することが望ましい。後方支援に関しては、日本はほぼ全ての米国の要求に対して対応可能である。弾薬提供や燃料補給は平時には不可能であるが、米国は日米安全保障条約第 6 条に基づき事前協議を要請できるため、必要であれば平時であっても、こうした支援に関して事前協議を要求・要請することが可能である。

さらに重要影響事態の下では、米軍だけでなく、国連憲章の目的達成に寄与する活動を行う諸外国の軍隊に対しても日本は支援を提供可能となる。「防衛白書」によれば、平時から緊急事態や武力攻撃事態に至るまで、日本はあらゆる後方支援を米軍に提供可能とされている。

図表 3：活動一覧

	平時	重要影響事態	
日米共同声明（政策問題）	○	○	3 カ国共同声明：政治判断
日米共同声明（軍事問題）	△	○	3 カ国共同声明：政治判断
共通の地域図	△	○	米国、海上保安庁、警察庁経由
情報共有	△	○	米国、海上保安庁、警察庁経由
後方支援	○	○	宿泊、保管、施設の利用、訓練業務、補給、輸送、修理・整備、医療、通信、空港・港湾業務、基地業務
弾薬提供、燃料補給、戦闘作戦行動のために発進準備中の航空機に対する整備	*1	○	米軍および国連傘下の外国軍

*1 日米安全保障条約第 6 条に基づく事前協議が必要

出所：日本チームのプレゼン資料

平時における海上自衛隊の活動

日本は尖閣諸島周辺の防衛能力を高めるべく、南西諸島での防衛体制を強化している。海上自衛隊は日本周辺海域での情報収集・警戒監視・偵察活動を、P-3C 哨戒機や P-1 哨戒機、汎用護衛艦、イージス・システム搭載護衛艦を用いて日々行っている。こうした活動の目的は、東シナ海から太平洋に向かって航行する中国海軍艦艇についての情報収集と、北朝鮮籍船舶による「瀬取り」の監視であり、尖閣諸島周辺で警備を行う海上保安庁と協力の上で実施している。瀬取りとは、北朝鮮籍船舶による洋上での物資積み替えであり、国連安全保障理事会決議で禁じられている。

海上自衛隊は平時においても、「自由で開かれたインド太平洋」ビジョンに貢献すべく、ソマリア沖・アデン湾での海賊対処行動、中東地域における日本関係船舶の安全確保のための情報収集活動など、多彩な活動に従事している。こうした平時の活動は、今回のシナリオにおける台湾のサイバー事態でも、戦略的コミュニケーションの伝達に役立てることができる。日米共同演習も適時に実施でき、米海軍艦艇の防護も可能である。

今回の事態が台湾から尖閣諸島や南西諸島へと広がった場合、日本政府は事態の波及を抑止すべく、海上自衛隊を活用することになる。米国政府が日本に対しこの問題への対応を促した場合、日本はより行動しやすくなると思われる。

ただし、米海軍と海上自衛隊が連携する際、両者の目的は異なることもあり得る。例えば、米海軍の目的が台湾の防衛と支援であるのに対し、海上自衛隊の目的は中国の侵攻抑止や尖閣諸島・南西諸島の防衛に置かれるといった状況である。したがって両者間での誤解を避けるため、両国がより緊密に情報を共有することが肝要となる。

加えて重要影響事態においては、後方支援、捜索救助、船舶検査が実施可能である。武力攻撃事態や存立危機事態の場合は、交戦規則を見直し、サイバー戦や宇宙・電磁波領域と組み合わせたハイブリッド戦で可能な行動を定める必要がある。

3. サイバーセキュリティの現状と制約

国としての体制構築

英国政府は 2020 年 10 月 19 日、ロシア軍参謀本部情報総局（GRU）が東京オリンピック・パラリンピックを標的としたサイバー攻撃を仕掛けていたと発表した。標的は東京オリンピック・パラリンピック競技大会組織委員会、スポンサー企業、運営支援企業で、東京オリンピック・パラリンピックの運営妨害が目的とみられる。2018 年平昌冬季五輪に対しても同様の攻撃があり、開会式の際にマルウエアを使ったデータ消去攻撃を受けて、ネットワーク上のコンピューターが使用不能となった。

内閣官房傘下の NISC は行政各部に対する包括的な調整を担っているが、こうしたサイバー危機の際には、日本には国としての防御体制を築くべく官民一体となった取り組みが求められている。

サイバーセキュリティに関する課題

日本ではサイバー空間、宇宙空間、電磁波が新たな防衛分野と認識され、新領域と呼ばれている。こうした防衛の特徴は、領空や領海のように国家主権を守るのではなく、グローバル・コモンズとして誰もが自由かつ平和裏に利用できる空間として保障することにある。したがって、これらに関する安全保障は、脅威を排除し、脅威時の強靱性を確保するとともに、機能保証を確保することが課題となる。

中国、ロシア、北朝鮮は近年、サイバー攻撃能力を軍として強化しており、今や軍事力の一部を成すと考えられる。米司法省はサイバー攻撃に歯止めをかけるため、2020 年 10 月、GRU 情報部員 6 名のマルウエア拡散容疑での起訴をはじめとする攻撃者の特定・公表に踏み切った。とはいえ、「金盾」と呼ばれる監視システムを用いて国外インターネット情報を遮断し攻撃リスクを低く抑えている中国とは異なり、表現や通信の自由を尊ぶ民主主義国家がこうした攻撃を食い止めるのは至難の業である。

サイバー空間は日本の「防衛計画の大綱」では、自衛隊が多次元統合防衛力戦略の一環として取り組む領域として、宇宙空間や電磁波とともに位置付けられているが、日本ではまだ検討段階にすぎない。

アジア太平洋地域での多国間協力

サイバー・宇宙領域に関するアジア太平洋地域での多国間協力については、本地域での安全保障体制を強化するため、アジア版北大西洋条約機構を創設すべきとの意見もある。こうした新領域における脅威は喫緊の課題となっており、多国間での即応体制が求められている。日米同盟を土台とし

て既存の多国間安全保障枠組みを活用するとともに、このような宇宙防衛体制を新たに本地域で築くべきである。