2022 年 9 月 1 日

ハイブリッド脅威分析のフレームワーク
―欧州ハイブリッド脅威対策センターのコンセプト・モデルを通じて―

主任研究員
川嶋　隆志

はじめに

本稿は、「欧州ハイブリッド脅威対策センター」（The European Centre of Excellence for Countering Hybrid Threats: Hybrid CoE。以後、「対策センター」とする。）の研究成果を通じて、日本が今後ハイブリッド脅威に対応して行く上で必要な態勢及び機能について考察するものである。

ロシアのウクライナ侵攻に際して、当初注目されたのがハイブリッド戦争である。2014 年のクリミア危機において、ロシアは正規軍による軍事侵攻に先立ち非正規の手段（通信網の遮断、フェイクニュース、SNS を用いた世論操作）を駆使し、ほぼ無血でクリミアを占領・併合した。

2022 年 2 月のロシアによるウクライナ侵攻開始時にも同様の展開が予測されていたが、ロシアによるハイブリッド戦争は成功せず、クリミア侵攻とは対照的に軍事侵攻に発展した。この 2014 年と 2022 年の違いを生んだ要因の一つとして考えられるのが、「ハイブリッド脅威のコンセプト・モデル」[i]（以後、「コンセプト・モデル」とする。）である。当該コンセプト・モデルは、「対策センター」が欧州委員会の共同研究センターの協力を得て、2018 年 7 月から約 2 年間をかけて作成したもの[ii]で、ロシアによる侵攻への対応に活用された可能性がある。

以下、本稿では「コンセプト・モデル」の主要素について解説し、最後に日本におけるハイブリッド脅威対策に資する提言を行いたい。

1　「対策センター」の概要

本センターは、ハイブリッドの脅威に対抗するための政府及び社会全体のアプローチを推進するための国際的な自立型ネットワークで、本部はフィンランドのヘルシンキに所在する。センターの活動には、31 の参加国、EU、NATO、民間企業、学術界等から 1500 名を超える実務家および専門家が参画している。また、ハイブリッドの脅威に対抗するための専門的知見の涵養及び教育を提供している[iii]。

２　コンセプト・モデルの必要性

上記の参加国・機関がハイブリッド脅威コンセプト・モデルの必要性を認識し、上記対策センターの活動を推進することとなった理由として、以下の３点が挙げられている。

（１）ハイブリッド脅威に対する関係国・組織間の共通理解の確立

クリミア併合で注目されることとなったハイブリッド脅威であるが、その手段（SNS上での世論操作やサイバー攻撃）、主体（通常戦争と異なる軍以外の様々な主体）、領域（陸海空でなく、サイバー、経済、社会、認知領域等）等が多方面に亘り、さらには軍事的手段とも連動するという曖昧さ・捉えどころのなさが特徴であった。後述するように、攻撃側にしてみればこの曖昧さによって脅威対象の状況認識を困難にし、さらに各種手段を組み合わせることで、脅威対象の意思決定や対応を困難にすることにハイブリッド脅威を利用する意義があると考えられる。逆に言えば、直面しうるハイブリッド脅威を理解し、各手段への対応について同盟国・友好国間で予め共有できていれば、脅威が検出された際に攻撃側の目的を一定程度無力化することができる可能性があると考えられる。このため、関係国・組織間の共通の理解を確立するため明確なコンセプトを構築することとなったのである[iv]。

上記のとおり、ハイブリッド脅威は複数の領域において多数の手段が利用される状況が想定される、非常に広い概念である。他方、「ハイブリッド戦争」はハイブリッド脅威活動がエスカレーションした結果として至った戦争状況である。この広義の概念である「脅威」と、脅威活動のエスカレーションの結果である「戦争」の両概念が同義に認識される傾向があり、このことが概念を複雑化し、共通理解の妨げになっていることも対策センターは指摘している。さらに、経済社会等を対象とするハイブリッド脅威は対象や時代により変化していくことが予想され、一般的な定義づけや概念の固定化をすることでその変化に対応することができなくなる恐れがある[v]。

したがって、ハイブリッド脅威の共通理解の確立とは具体的な脅威の事例研究の様な知識的なものというよりは、ハイブリッド脅威の可能性のある事象が発生した際に、脅威を検出し、その目的や影響を評価し、対応を提示するための分析フレームワークの形成であると言える。

（２）ハイブリッド脅威への対応策構築

本コンセプト・モデルの分析フレームワークを活用することによって、脅威を可視化し、意思決定者が正確な状況認識・理解に基づく判断（Informed decision making）をすることが可能となる[vi]。その結果、ハイブリッド脅威に係る活動の早期特定、予防、準備、対応の問題点を特定し、情報を共有することによって、１国だけでなく、EU、NATOといったあらゆるレベルでレジリエンスを強化することが可能となる[vii]。

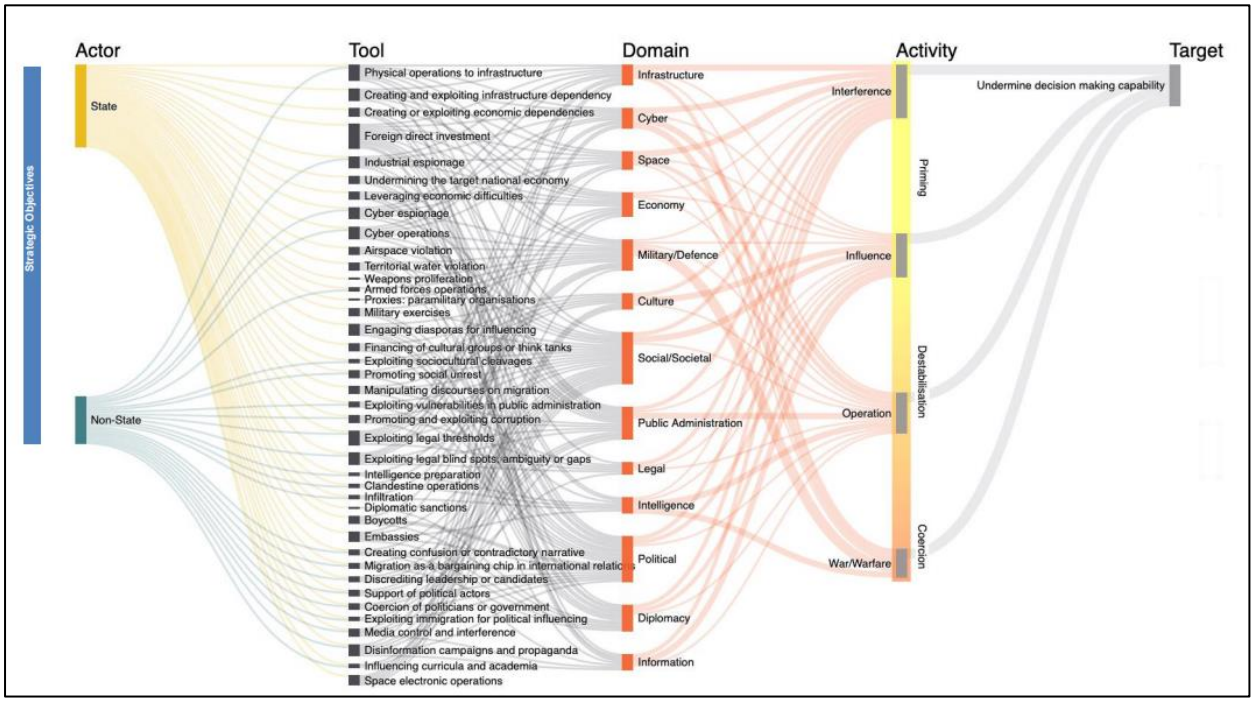
（３）ハイブリッド脅威の概念発展の基盤提供

既述のとおり、ハイブリッド脅威は経済社会の状況や技術の進歩（特にサイバーや宇宙等の新領域の状況）に応じて変化し、さらに多様化していくことが予想される。したがって、ハイブリッド脅威の概念もこの変化に対応し、発展させていくことが必要である。将来、これまで想定されてこなかった形態の脅威が発動された際には、本コンセプト・モデルを用いてさらなる研究を推進するための基盤となることが期待されている[viii]。

３　コンセプト・モデルの概要

以上のような目的のため、対策センターが作成した「コンセプト・モデル」の全体像は下図のとおりとされている。

図１　ハイブリッド脅威のコンセプト・モデルの全体像



出典：The landscape of Hybrid Threats: A conceptual model Public Version, p. 13

このコンセプト・モデルの分析フレームワークには、（１）アクター、（２）ツール、（３）ドメイン、（４）フェーズ（図１の Activity の部分がフェーズに該当する）が４本柱として掲げられている、以下、各項について概説する。

（１）アクター

アクターは、国家主体と非国家主体の２つのアクターに分かれる。

ここでいう国家主体とは、EU、NATO 等を構成する民主主義国家に敵対する権威主義国家を主に指す。その特徴としては、政権の目的は権力の維持であり、民主主義国

家に対する恐れを抱いているという傾向が見られる[ix]。具体例としてロシア、中国、イラン、北朝鮮が挙げられており、特にロシア及び中国はハイブリッド脅威の主要なアクターとされている[x]。

非国家主体とは、国際関係に関与し、国家の確立された機関に所属することなく、干渉し、影響を与え、変化を起こすのに十分な力を行使する実体をいう。特徴としては、国家が非国家主体を通じて、他国に対して有害な性質の活動を実施していることが多いということが挙げられる[xi]。代表例としては、ヒズボラ、ISIL、民間軍事会社（PMC）等が挙げられている[xii]。

ハイブリッド脅威に対応する上では、上記の国家主体・非国家主体のアクター特定に加えて、アクターの戦略目的を分析することが重要とされている[xiii]。

（２）ツール

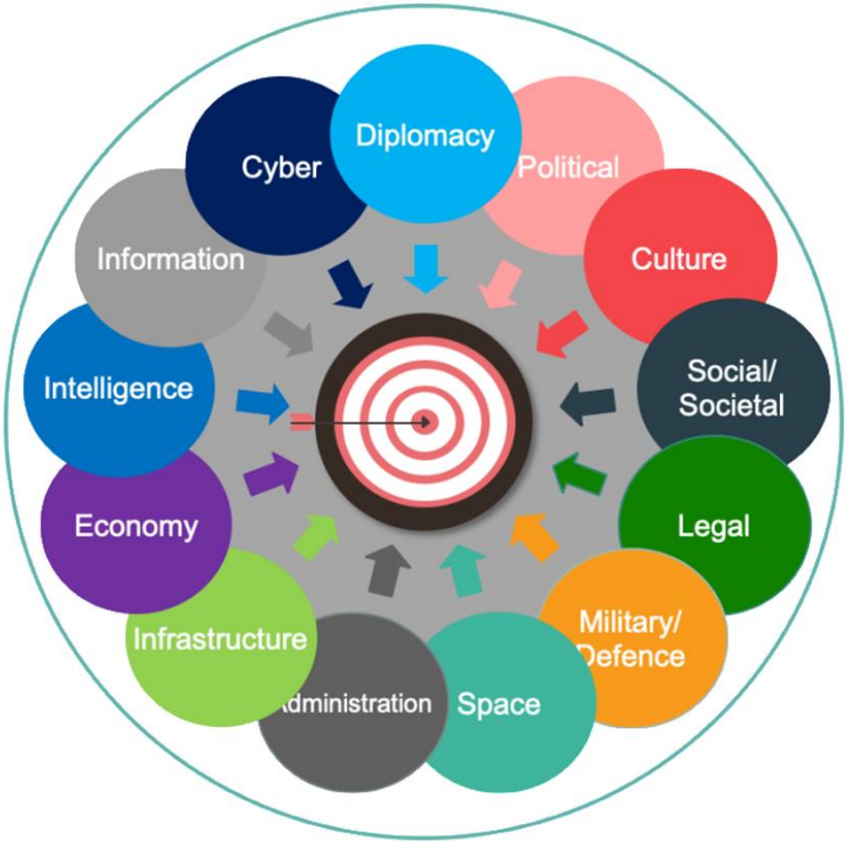
ツールとは国家主体および非国家主体がハイブリッド脅威を対象に及ぼすために利用する手段をいう[xiv]。このコンセプト・モデルでは、過去の事例に基づき 40 個のツールが示されている。アクターはこのツールを組み合わせて、ハイブリッド脅威をもたらす。このツールとドメインの関係については、後述する。

（３）ドメイン

ドメインは日本では安全保障の文脈で「領域」と呼ばれているが、ここでは国力の要素をグループ化したもので、アクターがツールを利用してハイブリッド脅威を及ぼす標的となるものをいう[xv]。このドメインをハイブリッド脅威の標的とすることによって、アクターは最終的に目標を達成する。

下図のように、ドメインとして軍／防衛のほかに、インフラ、サイバーといった政治、経済、社会を形成する要素が 13 項目列挙されており、アクターは各ドメインに属する複数のツールを組み合わせて目標（図の中央）を達成しようとする。

図２　ドメインとアクターの目標のイメージ図



出典：European Commission, & Hybrid CoE, *The Landscape of Hybrid Threats: A Conceptual Model Public Version*, 2021, p. 27

本コンセプト・モデルにおいて、ドメインについては理論的根拠に基づいたグループ化はできなかったことが明記されている。したがって、ケースに応じて変更・見直しが必要とされている[xvi]。

（４）ハイブリッド脅威活動のツールと影響を受けるドメイン

敵対するアクターが目的を達成するために使用可能なツールの一覧と影響を受ける可能性のあるドメインについて、まとめたものが以下の表である。

表１　ツールの一覧と影響を受ける可能性のあるドメイン

	ツール	影響を受ける可能性のあるドメイン
1	インフラに対する物理的打撃	インフラ、経済、サイバー、宇宙、軍事／防衛、情報、社会、行政
2	インフラへの依存（民軍間の依存を含む）の構築と利用	インフラ、経済、サイバー、宇宙、軍事／防衛、行政
3	経済的依存関係の構築又は利用	経済、外交、政治、行政
4	外国への直接投資	経済、インフラ、サイバー、宇宙、軍事／防衛、行政、インテリジェンス、情報、政治、法律
5	産業スパイ	経済、インフラ、サイバー、宇宙、インテリジェンス、情報
6	相手国経済活動の阻害	経済、行政、政治、外交
7	経済的困窮の利用	経済、行政、政治、外交
8	サイバー・スパイ	インフラ、宇宙、サイバー、軍事／防衛、
9	サイバー・オペレーション	インフラ、宇宙、サイバー、社会、行政、軍事／防衛
10	領空侵犯	軍事／防衛、社会、政治、外交
11	領海侵入	軍事／防衛、社会、政治、外交
12	兵器拡散	軍事／防衛
13	軍隊の通常型／準通常型の行動	軍事／防衛
14	準軍事組織（傀儡組織）	軍事／防衛
15	軍事演習	軍事／防衛、外交、政治、社会
16	在留民による影響戦略の関与	政治、外交、社会、文化、インテリジェンス、情報
17	文化団体やシンクタンクへの財政支援	社会、文化、政治、外交
18	社会的・文化的分裂（民族、宗教、文化）の利用	社会、文化
19	社会不安の増長	インフラ、社会、経済、政治
20	社会の分極化、リベラル民主主義弱体化のため移住に関する言説を操作	社会、文化、政治、法律
21	行政における脆弱性の利用	行政、政治、社会

	（危機管理を含む）	
22	汚職の助長と悪用	行政、経済、法律、社会
23	法の閾値、非帰属、缺欠および争点の利用	インフラ、サイバー、宇宙、経済、軍事／防衛、文化、社会、行政、法律、インテリジェンス、外交、政治、情報
24	法による規制、プロセス、制度、議論の利用	インフラ、サイバー、宇宙、経済、軍事／防衛、文化、社会、行政、法律、インテリジェンス、外交、政治、情報
25	作戦遂行上必要な情報の収集整理	インテリジェンス、軍事／防衛
26	隠密活動	インテリジェンス、軍事／防衛
27	潜入	インテリジェンス、軍事／防衛
28	外交的制裁	外交、政治、経済
29	ボイコット	外交、政治、経済
30	大使館	外交、政治、インテリジェンス、社会
31	混乱・矛盾した筋書きの生成	社会、情報、外交
32	国際交渉の切り札としての移住	社会、情報、外交
33	リーダーシップや候補者の信用失墜	政治、行政、社会
34	政治的アクターへの支援	政治、行政、社会
35	政治家および／または政府への強制・強要	政治、行政、法律
36	政治的影響力のための移民の利用	政治、社会
37	メディア・コントロール及び干渉	情報、インフラ（メディア）、社会、文化
38	情報操作とプロパガンダ活動	社会、情報、政治、サイバー、文化、行政
39	カリキュラムと学会への影響	社会、文化
40	電子戦（GNSS 妨害及びなりすまし）	宇宙、サイバー、インフラ、経済、軍事／防衛

出典：European Commission, & Hybrid CoE, *The Landscape of Hybrid Threats: A Conceptual Model Public Version*, 2021 , pp. 33-35 を元に執筆者作成

この表は、対策センターが過去の事例に基づき使用実績のあったツールを列挙した

ものである。

アクターはこのツールを利用して１つ以上のドメインに影響を及ぼしたり、ドメインの脆弱性を標的としたりする。また、直接対象とするドメインに対する効果だけでなく、関連する他ドメインへも波及的に影響を及ぼす「カスケード効果」をもたらす場合もある[xvii]。

この表で注意しなければならないのは、この表に列挙されたツール使用の兆候があるからと言って、ハイブリッド脅威であるとは限らないという点である。例えば、サイバー・オペレーションは、ハイブリッド脅威の活動の一部として他のツールと連動して行われる場合と、単体で行われる場合がある[xviii]。あるハッカーがサイバー攻撃を仕掛けてきたときに、戦略目的をもったアクターと関連性があり、そのアクターが用いる他のツールと連動するのかを分析し、これらが組み合わさった結果生じうる影響の全体像を早期に予測する必要がある。

（５）フェーズ

最終的に戦争状況に入るまでの活動の段階・タイムラインを指し、アクティビティの強度と脅威の性質の違いから３つに分かれるとされる[xix]。各フェーズで行われるアクティビティは次の図のとおりである。

表２　フェーズとアクティビティの関係

フェーズ	アクティビティ
①　プライミング・フェーズ	干　渉 影　響
②　不安定化フェーズ	活　動
③　強制フェーズ	戦　争

出典：European Commission, & Hybrid CoE, *The Landscape of Hybrid Threats: A Conceptual Model Public Version*, 2021, p. 13 を元に執筆者作成

①プライミング・フェーズ

プライミング・フェーズにおいて、アクターは対象国に対して各種ツールを用いた「干渉」を行う。これにより対象国が状況認識を失い、首脳部を自滅的な意思決定を行うような状況に導くことがこのフェーズにおけるアクターの最終目標である[xx]。この「干渉」の結果生じる効果が「影響」である[xxi]。

このプライミング・フェーズにおけるアクティビティはハイブリッド脅威として即座に評価することが難しい、曖昧且つ目立ちにくいものである。このため、本コンセ

プト・モデルを用いることで早期に兆候を察知し、アクターの目的を分析することで他ドメインへの波及等を含む状況の進展を予測することが、ハイブリッド脅威への対応上非常に重要となる[xxii]。

②不安定化フェーズ[xxiii]

不安定化フェーズは、アクターが各ドメインにおいて、各ツールを用いた活動を強化する段階である。活動は顕在的且つより攻撃的となり、多くの物理的な打撃・暴力を伴うようになるが、アクター自身は関与をしていることを秘匿することが想定されている。

プライミング・フェーズから不安定化フェーズへの移行例として、以下のようなシナリオが考えられる。ある武力衝突や小競り合い等が発生した際に死者数の報道、遺族や負傷した兵士のコメントなどの情報が出回る（干渉）。そして死者数増加の報道、遺族のコメント等が増えていくと、兵士を送り出している家族の不安が高まる（影響）。さらに、この不安が社会全体に波及すると、反戦ムードが高まり、デモ等を煽る活動も見られるようになる（活動）。

不安定化フェーズでのアクターの目標は、対象国を揺るがし、容易に屈服させられるレベルまで不安定化させることであるが、所要の効果が得られない場合にはプライミング・フェーズに一旦戻り、より効果的なツールの組み合わせに変更することも考えられる。

③強制フェーズ[xxiv]

政治的・経済的措置、破壊、情報、偽情報活動（プロパガンダ）、特殊部隊の隠密行動・公開展開、対象国の敵対勢力に対する軍事支援が行われ、対象国に対して戦争目的を最終的に強制・強要する段階である。潜在的にすべてのドメインが利用される。テロ、妨害、転覆、ゲリラ戦争、通常戦争等を含むより一般的な戦争状態に発展した状況である。

（6）ハイブリッド脅威に対する分析の視点

以上、「コンセプト・モデル」の主要素について説明してきたが、最後にハイブリッド脅威に対する分析の視点について言及する。

このハイブリッド脅威を「コンセプト・モデル」を用いて分析する際、まずドメインを標的とするツールとアクティビティの全体像を明らかにする必要がある。このためには平素から研究に取り組み、各ドメインにおけるハイブリッド脅威に対する脆弱性を予め特定し、使用されうるツールのチェックリストを準備しておくことで、アクティビティを検出可能なフレームワークを構築することが重要である。「コンセプト・モデル」は、このための基盤を提供することができる。

また、各種アクティビティとアクターとの関連性を明らかにするためには、アクター

の意図を看破し、目的達成のためのシナリオを説明する必要がある。このため、潜在的なアクターのドクトリンや行動原理に関する理解を、ハイブリッド脅威が具体的に生起する前に深めておく必要がある。

さらに、アクティビティが発生した際には上記のチェックリストやアクターの意図に照らし、ハイブリッド脅威として検出するための警戒監視態勢が必要である。

以上のとおり、ハイブリッド脅威の分析に当たっては①コンセプト・モデルを用いた分析枠組みの構築、②アクターの戦略目的・意図を理解するための総合分析機能の強化、③ハイブリッド脅威に対する警戒監視態勢の構築、が重要と言えるだろう。

おわりに

最後に、コンセプト・モデルと分析態勢を効果的に運用し、ハイブリッド脅威の兆候を察知した際の対応について述べたい。

本コンセプトのとおりハイブリッド脅威が段階的に発展していくことを踏まえれば、「③強制フェーズ」にアクターを踏み切らせないために、「①プライミング・フェーズ」及び「②不安定化フェーズ」の段階でどのような対応を行うべきかが課題であると言える。このため、日本としてのハイブリッド脅威への対応について、以下を提言したい。

（１）本コンセプト・モデルの活用

日本に隣接するロシアや中国等はコンセプト・モデルにおいてハイブリッド脅威の主要アクターとされているのみならず、日本にとっては実際的・具体的な脅威である。他方、日本単独でハイブリッド脅威の分析フレームワークを構築するのは、時間・人材といった観点からも困難である。このため、今回紹介したコンセプト・モデルを活用して直面しうる脅威の分析・対応検討を進めつつ、友好国との情報共有を促進することで状況認識・警戒監視能力を高め、さらに状況に応じて分析態勢を修正可能な柔軟な組織を構築していくことが合理的である。

（２）ハイブリッド脅威への省庁横断的対応方針の明示

本コンセプト・モデルのドメインに関する分析・記述からも明らかな通り、ハイブリッド脅威はサイバー攻撃のような明示的な行動のみならず、極めて広範且つ戦争との関連性が不明瞭な干渉を含む。このため、特定の主管省庁による対策は困難であるため、政府或いは官民共通のハイブリッド対策の指針に従って、各省庁・企業等の専門性を集約することが必要である。この先行事例として、例えば EU の安全保障・防衛政策に係る共通の指針である「戦略的羅針盤（Strategic Compass）」では、「対策センター」のコンセプトと同様、広範なハイブリッド脅威への対応を謳っている。また、このための具体策として対処チームの設置等について記載されている[xxv]。

日本においても、この様な省庁横断的対応を可能にしていくための指針・根拠を明

確化するために、令和４年度中に閣議決定予定の国家安全保障戦略に、ハイブリッド脅威への対応を規定する必要がある。

（３）ハイブリッド対策センターの設立

最後に、ハイブリッド脅威は様々な専門分野を多角的な視点から分析することが不可欠である。そのためには、官・民問わず、多彩な人材を確保して、分析・研究するセンターを設立し、「対策センター」と連携を図っていく必要がある。

以上、ハイブリッド脅威への対応について述べたが、日本は安全保障上及び災害への対応を通じ、当該脅威の監視・対応に必要な知見等を相当程度蓄積していると言える。政府内の既存の危機管理態勢と官民学が個別に有する知見を効果的に集約・調整する機能が、上記対策センターが今後設立された際にはまず求められることになるだろう。

---

[i] European Commission, & Hybrid CoE, *The Landscape of Hybrid Threats: A Conceptual Model Public Version*, 2021, https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf (2022 年 5 月 1 日閲覧)

[ii] Ibid., p. 7

[iii] "What is Hybrid CoE? ", Hybrid CoE, https://www.hybridcoe.fi/who-what-and-how/ (2022 年 8 月 25 日閲覧)

[iv] European Commission, & Hybrid CoE, *op cit* , p. 4

[v] Ibid., p. 6

[vi] Ibid., p. 14

[vii] Ibid., p. 6

[viii] Ibid., p. 6

[ix] Ibid., pp. 16-18

[x] Ibid., p. 16

[xi] Ibid., p. 22

[xii] Ibid., p. 16

[xiii] Ibid., p. 15

[xiv] Ibid., pp. 32-33

[xv] Ibid., p. 26

[xvi] Ibid., pp. 26-27

[xvii] Ibid., pp. 11-12

[xviii] Ibid., pp. 32-33

[xix] Ibid., p. 10

[xx] Ibid., p. 37

[xxi] Ibid., p. 38

[xxii] Ibid., p. 5

[xxiii] Ibid., p. 40

[xxiv] Ibid., p. 41

[xxv] "A Strategic Compass for a stronger EU security and defence in the next decade", Council of European Union, 21 March 2022. https://www.consilium.europa.eu/en/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/ （2022 年 8 月 25 日閲覧）