外交・安全保障調査研究事業費補助金（調査研究事業）
補助事業実績報告書

<table>
<tr><td colspan="6">１．基本情報</td></tr>
<tr><td colspan="2">事業分野</td><td colspan="4">A:国際政治及び国際情勢一般</td></tr>
<tr><td colspan="2">事業の名称</td><td colspan="4">国際秩序にサイバー空間が与える影響の評価、対抗策研究</td></tr>
<tr><td colspan="2"></td><td colspan="4">※下記の期間から１つを選択し「○」を記入
（　）１年間（平成　　年度）
（　）２年間（平成　　年度～平成　　年度）（うち　　年目）
（○）３年間（平成 29 年度～平成 31 年度）（うち 3 年目）</td></tr>
<tr><td rowspan="8">責任機関</td><td colspan="2">組織名</td><td colspan="3">株式会社三菱総合研究所</td></tr>
<tr><td colspan="2">代表者氏名
(法人の長など)</td><td>森崎　孝</td><td>役職名</td><td>代表取締役社長</td></tr>
<tr><td colspan="2">本部所在地</td><td colspan="3">〒100-8141
東京都千代田区永田町二丁目 10 番 3 号</td></tr>
<tr><td colspan="2">法人番号</td><td colspan="3">6010001030403</td></tr>
<tr><td rowspan="4">①事業代表者</td><td>フ リ ガ ナ</td><td colspan="3">ムラノ　マサヤス</td></tr>
<tr><td>氏　　名</td><td colspan="3">村野　正泰</td></tr>
<tr><td>所属部署</td><td>デジタル・イノベーション本部</td><td>役職名</td><td>副本部長
主席研究員</td></tr>
<tr><td>所在地</td><td colspan="3">〒100-8141
東京都千代田区永田町二丁目 10 番 3 号</td></tr>
<tr><td rowspan="4">②事務連絡担当者</td><td>フ リ ガ ナ</td><td colspan="3">マルタ　カオリ</td></tr>
<tr><td>氏　　名</td><td colspan="3">丸田　佳織</td></tr>
<tr><td>所属部署</td><td>デジタル・イノベーション本部</td><td>役職名</td><td>主任研究員</td></tr>
<tr><td>所在地</td><td colspan="3">〒100-8141
東京都千代田区永田町二丁目 10 番 3 号</td></tr>
</table>

事業総括、グループリーダー、研究担当、渉外担当等の別	氏名	所属機関・部局・職	役割分担
事業総括	村野　正泰	デジタル・イノベーション本部　副本部長	事業総括
研究担当、事務連絡担当	丸田　佳織	デジタル・イノベーション本部　サイバーセキュリティ戦略グループ	基礎情報収集、研究会開催
研究担当	篠原　巧	デジタル・イノベーション本部　サイバーセキュリティ戦略グループ	基礎情報収集、研究会開催
研究担当	持永　大	慶応義塾大学	基礎情報収集、分析
研究指導	土屋　大洋	慶応義塾大学	研究指導

２．事業の背景・目的・意義

【事業の背景】

- サイバー空間は、今や経済、産業、生活、軍事等の近代社会のあらゆる活動にとって不可欠なものであり、陸、海、空、宇宙と並ぶ新たな「領域」として認識されている。
- サイバー空間は国際協調と国際紛争が起こる最前線の領域であり、国家は安全保障政策、外交政策、インテリジェンス、国際競争力において幅広い影響を受ける。
- 国際情勢の観点から、サイバー空間の安定的利用とサイバーセキュリティ強化にむけた国際ルールや国際連携が必要となっている。
- 政府・重要インフラ、企業の情報通信ネットワークへの依存度が一層増大していく中、サイバー攻撃によって、国家の経済・安全保障が深刻な脅威にさらされている。
- サイバー空間における動向は国家のパワーバランスに影響を与えている。そのため、国際秩序にサイバー空間が与える影響を調査し、サイバー空間における国際情勢把握に向けた政策研究能力の強化が必要である。
- 2017 年 1 月に米国家情報長官から発表された報告書では、米国においても米大統領選を標的にしたロシアにおけるサイバー攻撃が行われるなど、国家及びテロリストによるサイバー攻撃の脅威はますます高まっている（図１）。

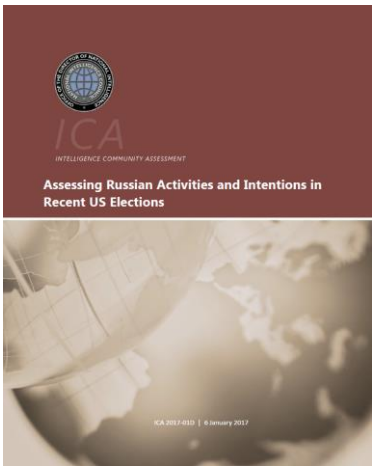

図 1　米国政府によるロシアよる米国選挙への干渉に関する報告書

サイバー空間には国境がなく、国際法の適用について議論が行われている。例えば、国連におけるサイバー空間における新たな行動規範の作成に向けた議論では政府専門家会合の結果として、サイバー空間における行動規範について、既存の国際法が適用されるとしつつも ICT の独特な特性に鑑みれば追加的な規範が発展しうると指摘されている。

サイバー空間における安全保障は、研究分野として新しく、学際的な研究が必要である。例えば国立情報学研究所による学術論文や図書・雑誌などの学術情報データベース CiNii によると、「サイバー」というキーワード検索結果が 16,386 件、「安全保障」というキーワードの検索結果が 11,743 件ある。一方、両分野にまたがる研究数を示す「サイバー」と「安全保障」の両方を含む検索結果は 70 件となり、サイバー空間の安全保障は研究の蓄積が途上であることを示している。

【事業の目的・意義】

● 事業の目的：サイバー空間における国際情勢把握、サイバー空間における安全保障に関する提言

本事業の目的は、国際情勢把握に向けた政策研究能力の強化と「サイバー空間に関する安全保障」を議論するための基盤づくりに向けた政策提言である。特に安全保障分野とサイバーセキュリティ分野にまたがる領域で基礎的情報収集や専門的調査研究を行うことで、国際情勢把握に向けた政策研究能力の強化を行う。サイバー空間における安全保障は、安全を提供する客体が国家だけでなく、民間企業などとの連携が必要となること、経済的利益といった価値観が多様であることが特徴的なため、国際行動規範などの議論が成熟していない分野であり強化が必要である。

● 日本外交にとっての意義①：サイバー空間の安定的利用にむけたルール作りや国際連携が行われており日本外交にとって国際情勢の観点から国際秩序にサイバー空間が与える影響の研究は重要

国際情勢の観点において、学際的な研究能力底上げは、今後の国際的な課題に向けた我が国の外交政策立案・遂行の基盤に欠かせない。しかし、サイバーセキュリティと安全保障の両分野にまたがる研究を行っている研究者の人数は少なく、研究の蓄積も不十分である。そのため、本事業では民間シンクタンクが学際的な分野をつなぎ、サイバー空間における国際情勢把握に資する資料を整理することで基盤構築を行い、今後の国際的な課題検討に向けた政策提言を行う。サイバー空間の安全保障と国際規範づくりに関する政策提言を行うことは、論点整理のみならず今後の我が国の外交政策の立案・遂行に資する。

本事業で実施する国際秩序にサイバー空間が与える影響の研究は、国際的なサイバー空間の安定的利用に向けた議論に向けた政策研究能力向上において重要である。例えば、サイバー空間における安全保障に関する議論ではサイバー攻撃の法的位置付けが国際的に整理されていない。また、我が国ではサイバー攻撃が自衛権発動の対象となるかなど多数の論点がある。さらに、我が国は日米同盟や専守防衛等の独特の安全保障環境にあることから、諸外国の議論の引き写しでは不十分であり、従来の安全保障分野のみならず、学際的な研究による政策研究力底上げが必要である。

● 日本外交にとっての意義②：情報通信先進国である日本はサイバー空間に関する外交を展開するため国際情勢を分析する必要がある

我が国は日米同盟、専守防衛といった独特の安全保障環境を有することから、サイバー空間に関する外交を展開するにあたって、国際情勢を分析する必要がある。サイバー空間に関する外交の展開については、2013 年のサイバーセキュリティ戦略、2014 年の国家安全保障戦略においてサイバーセキュ

リティの強化、国際規範形成や信頼醸成措置への積極的関与、開発途上国の能力構築を行うことが謳われている。また、我が国の情報通信技術は世界的に見ても高い水準にあり、我が国は国際社会においてサイバー空間に関する外交安全保障分野で幅広い活動を期待されている。

国際情勢にサイバー空間が与える影響は、インターネット利用拡大に伴う情報の流通を通じて社会・経済・国家全体へ広がっている。民間企業は積極的にインターネットを活用したサービスを提供し、政府機関もインターネットを利用した活動を拡大している。情報通信技術への依存度が高い我が国では、サイバー空間における影響が分野横断的に拡大する。さらに、影響範囲は我が国にとどまらず、他国へ影響することも想定される。また、近年は米国大統領選挙や欧州における選挙でロシアがサイバー空間を通じて関与しているとの報道に加え、フェイクニュースの拡散、政治広告の不透明性等によって国際情勢にサイバー空間が与える影響度が増している。このような状況を鑑み、国際情勢を分析し、日本が戦略的な外交を展開してくために必要な対抗策についての研究をふまえて、サイバー空間の安全保障と国際規範形成にむけた提言をとりまとめる。

- 本事業の卓越性：日本外交におけるサイバー空間の国際情勢への影響は大きく、本事業は安全保障とサイバー空間に関する政策研究の第一歩となる

安全保障とサイバーセキュリティに分かれて議論されていた分野を繋ぎ、学際的研究基盤を作る本事業の取り組みは新規性、および今後の日本外交における重要性の点から卓越している。内外の学術研究に加え、技術研究を行う研究者および実務者のネットワークを有する民間シンクタンクがサイバー空間における国際情勢について研究を行うことは新規性があり、サイバー空間の特性を鑑みても適切かつ効果的である。

３．事業の実施状況（ページ制限なし）

（１）研究会の開催（研究委員による小規模研究会等。研究会毎に以下の項目を要記載。）

●日程，場所

2019 年 5 月 14 日 10:00 - 11:00

三菱総合研究所　会議室

●テーマ

平成 31 年度事業の方針

●主要参加者

慶應義塾大学　土屋大洋　先生、持永大（遠隔より参加）

三菱総合研究所　村野正泰

●議論／研究内容の概要

平成 31 年度事業として、海外研究者の招聘、英語による発信、海外で開催する会議参加を想定する。外務省からの要請により、年度内に事業成果を共有する機会を設定する。

●公開・非公開の別

非公開

●日程，場所

2018 年 6 月 20 日

●テーマ

サイバー空間における秩序構築の状況、アウトリーチ活動

●主要参加者

慶應義塾大学　土屋大洋　先生、持永大（遠隔より参加）

三菱総合研究所　村野正泰、丸田佳織

●議論／研究内容の概要

サイバー空間における秩序構築においては、秋頃に GCSC 会合の結論が出る予定である。ロンドンプロセスの延長線上にある新たな会合が開催される。東京では 2019 年 12 月に公開イベントが開催される。それに合わせて、関係者を招聘する案を議論した。

●公開・非公開の別

非公開

（3)海外シンクタンクとの連携(海外シンクタンクや調査研究機関と協力した非公開のセミナーやワークショップ等。セミナーやワークショップの形式ではない連携については自由記述。案件毎に以下の項目を要記載。）

- 日程：2019 年 9 月 9 日 14:00 -15:30
- 場所：米国ワシントン DC 笹川平和財団米国
- テーマ：Japan’s Cyber landscape: International Security, and Geotechnology
- 登壇者：慶應義塾大学教授　土屋大洋、慶應義塾大学 SFC 研究所主席研究員　持永　大
- 参加人数：米国研究者等 8 名
- 議論の概要：
  - インド太平洋地域は世界経済にとっての重要性を増している。安倍総理は自由で開かれたインド太平洋を掲げ、法の支配、経済的発展、平和、及び安定性の確保に向けて取り組んでいる。サイバー空間は自由で開かれたインド太平洋ビジョンにおいても注目されている分野であり、特に法の支配と能力開発を通じた安定性確保に貢献できる。
  - サイバー空間は民間が運営するインフラから構成されており、経済と安全保障の基盤をなしている。近年起こったサイバー攻撃は、サイバー空間の脆弱性と、その社会的影響の大きさを証明した。
  - 我々はサイバー空間における支配要素を技術・政策／産業・数（データ）として特定した。これらの支配要素における主導権を分析したところ、90 年代までの米国による支配から、2000 年代以降、欧州、中国が台頭してきたことがわかる。その推移を分析することで、サイバー空間の支配者は次第に中国になりつつあることがわかる。
  - 日米政府は 2019 年 4 月 19 日に開催した日米安全保障協議委員会（日米「2＋2」）において、サイバー攻撃が日米安保条約第 5 条にいう武力攻撃に当たり得ることを確認した。これは、サイバー攻撃が集団的自衛権を発動させる要因となることを示している。
  - 2018 年に発表された「平成 31 年度以降に係る防衛計画の大綱について」では、サイバー空間における攻撃的能力について言及している。我々は日本が行えるサイバー攻撃はどのようなものとなるか、整理を試みた。
  - 内閣サイバーセキュリティセンターはあらゆるレベルでのサイバーセキュリティ対策の必要性を認識している。昨年日本政府は 5G に関する調達に関してガイドラインを発表し、サプライチェーンリスクに備える姿勢を見せている。

- 選挙に対する介入が米国で問題となっている。その背景には投票に用いられるコンピュータや選挙人の選定にかかるシステムの脆弱性がある。日本の場合、これらの情報は住民票を元に整理されており、投票に紙を用いているため米国と同様の脆弱性があるとは言い難い。しかしながら、インターネットを用いた政治活動が与える影響について、注目する必要がある。

- 日程：2019 年 9 月 11 日 16:30 -18:00
- 場所：米国ワシントン DC ジョンズホプキンス大学高等国際問題研究大学院
- Japan’s Response to Cyber Threats: Mega Events and Beyond
- 慶應義塾大学教授　土屋大洋、慶應義塾大学 SFC 研究所主席研究員　持永　大
- 参加者：米国研究者等 30 名
- 概要：
  - 日本のサイバーセキュリティ環境は 2020 年に開催される東京オリンピックパラリンピックを前にして、様々な脅威に直面している。その運営にかかる先進技術は大会の成否に影響を与えるほど大きくなっている。
  - 東京オリンピックパラリンピックはサイバー攻撃の標的となる。その影響はウェブサイト等の情報通信分野だけでなく、電気・水道・ガス・交通等の重要インフラに広がっている。重要インフラへの攻撃は大会の運営に直接被害を与えることを可能としている。例えば、2018 年に開催された平昌オリンピックではサイバー攻撃を通じて、インターネットアクセスの切断、会場チケットの発券、ウェブサイトの障害が起こり、大会運営に支障が出た。
  - サイバー空間は、コンピュータ、これらを接続するネットワーク、及びこれらを通じて交換される情報から構成される。また、そのほとんどは民間のインフラである。そのため、政府、民間、海外組織との連携が必要である。
  - サイバー空間は経済及び安全保障の基盤である。サイバー攻撃により発生するインシデントを乗り切ることは、技術、政策、及び組織的強さが必要になる。
  - 日本では、内閣サイバーセキュリティセンターが政府の中心となってサイバーセキュリティに関する施策を実施している。現在、日本政府は様々なレベルでのサイバーセキュリティ対策の必要性を認識している。近年では、サプライチェーンリスク、5G、量子コンピューティングといった分野が与える地政学的な影響を議論している。
  - 2020 年の東京オリンピックパラリンピックに向けて、国、自治体、民間の間で新しい組織を立ち上げている。彼らはサイバー攻撃を想定した演習などを実施し、対処能力を向上させている。

- 日本ではラグビーワールドカップの開催など、大きなイベントが続けて開催される予定である。そのため、2020 年は日本にとって、通過点であり政策の再構築、対抗策の洗練、レジリエンスの向上を継続的に実施することが必要である。

図 2 ジョンズホプキンス大学における会議の様子

（4）公開の主催／共催シンポジウム(開催している場合。案件毎に以下の項目について要記載。）

（４－１）Cyber Diplomacy, EU Japan Cyber Workshop（共催）

●日程，場所

2019 年 12 月 9 日　17:00 - 18:00

慶應義塾大学三田キャンパス東館 8F ホール

●テーマ

サイバー空間における外交課題

●主要参加者

Eneken Tikk, Head of normative, power, and influence studies, Cyber Policy Instiute

STANIECKI, Wiktor, Head of Cyber Policy Division, European External Action Service

TAALAS, Janne Ambassador Cyber Diplomacy, Finland

持永　大，上席所員，慶應義塾大学 SFC 研究所

●議論の概要

2019 年 12 月 10 日に欧州連合対外行動局と慶應義塾大学グローバルリサーチインスティテュートが共同で開催した日 EU サイバーセキュリティワークショップにおいて、サイバー空間における外交について議論を行った。当日は、一セッションを本事業における専門セッションとし、タリンマニュアルの作成に関係した Eneken Tikk 氏、欧州連合対外行動局の Wiktor Stankiecki 氏、フィンランドのサイバー大使 Janne TAALAS 氏、慶應義塾大学 SFC 研究所上席所員の持永大氏（元三菱総合研究所研究員）によるラウンドテーブルを開催した。

図 3　日 EU サイバーセキュリティワークショップの様子

ワークショップにおける主な議事内容は４－１．事業の成果に示す。

●その他特記事項

会議の開催後の懇親会を主催し、参加者間の交流を深めると共に国際的なネットワークを強化した。

（４－２）国際秩序にサイバー空間が与える影響の評価、対抗策研究会（主催）

●日程，場所

2020 年 2 月 26 日　10:00 - 12:00

株式会社三菱総合研究所

●テーマ

国際秩序にサイバー空間が与える影響の評価

●主要参加者

サイバー空間関連の官公庁職員、民間研究者等 20 名程度

●議論の概要

（コロナウイルス感染拡大のため直前に中止）

４．事業の成果（公開部分。ページ制限なし）

(１)本事業全体の成果（定量的な成果について記載があることが望ましい)。

- 成果の概要、定量的な成果

本研究では、国際秩序にサイバー空間が与える影響の分析と評価を行った。3 年間の事業を通じて分析と評価を行うに当たって、有識者へのインタビュー、国際会議における情報収集、文献調査を実施した。事業を通じて、国際会議への参加 1 回、国内における研究会を 4 回、うち 1 回は 20 名以上が参加する会議を開催した。さらに、事業の結果を活用した 360 ページの書籍を 1 冊出版し、広く一般向けの情報発信活動を行った。また、Web サイトを通じて 13 カ国のサイバー分野の政策動向を発信している。

書籍については、新聞、雑誌、SNS、書籍のレビューサイトに書評が掲載されている。本書のレビュー結果は、概ね好評である。新聞や雑誌には 3 件取り上げられ、これらのレビューでは、本書が今までに無い取り組みであることを指摘するとともに、産学融合取り組みによる力作との評価を得た。

平成 31 年度事業では、サイバー空間における秩序構築に貢献すべく、日 EU トラック 1.5 会議にお

いてサイバー外交に関するセッションを主催した。ここでは、EU 対外行動局のサイバー担当大使、EU 加盟国のサイバー大使とともにサイバー外交に関する課題を議論した。

- 国際秩序にサイバー空間が与える影響の分析、評価

現代社会の機能は、サイバー空間なしには成り立たない。例えば、金融機関の決済、航空機の予約、交通機関の管制といった社会基盤に加え、企業の業務システム、研究機関の活動、日々のメールなど、サイバー空間を利用した情報交換は重要な役割を果たしている。

サイバー空間の影響が、社会・経済・国家全体へ広がったことで、サイバー空間は国際情勢の構成要素のひとつとなった。従来、国際情勢を理解することは、国家間のパワーバランスを理解することとほぼ同義であったが、サイバー空間の理解には技術、企業、および個人の影響力を無視することはできない。

サイバー空間のうち、特にインターネットでは、米国を中心とした勢力がサイバー空間を支配していたといえる。世界に拡大したサイバー空間の利用によって、個人が従来よりも自身の情報を世界に発信しやすくなり、企業がさまざまなサービスを提供することができるようになった。

そして情報通信技術の発展普及によって勢力争いに新しいプレーヤーが登場し、サイバー空間における勢力図は変わりつつある。米国や米国企業はインターネットの発展に多大な貢献を行い、サイバー空間の覇者として活躍してきた。しかし、中国や欧州の台頭により、米国のサイバー空間における影響力は低下しつつある。影響力低下の原因は、技術面、政策面などにおいて、両者の影響力が高まり、相対的に米国の影響力が弱まっているからと考えられる。特に、中国などの勢力は、サイバー空間の統治は不十分であり、その影響が秩序を乱すと考えている。このような勢力は、米国に代わって次第にサイバー空間を支配しつつある。

このようなサイバー空間やサイバーセキュリティに関する話題には、技術的な項目に加え、法律や制度などの非技術的な項目もある。サイバー空間では、国家のほか、企業、組織、個人が重要なプレーヤーとなる。従来の「勢力均衡論」や「地政学」をはじめとする国際政治、安全保障論の概念では捉えられないのがサイバー空間である。新たな理解の枠組みが求められているといってよい。

このサイバー空間の勢力図を俯瞰し、支配状況を明らかにするのが本研究の目的のひとつであり、本研究ではサイバー空間の支配要素を定性的、定量的に分析した。分析では、身近なサイバー空間のイメージを整理するため、その定義を示すとともに、成立過程を紹介し、国家や企業の動向について分析を行った。この分析の目的は、米国が近年までサイバー空間の覇者となることができた要因、中国や欧州が台頭できた要因を理解することで、サイバー空間の支配要素を特定することにある。また、サイバー空間という身近で重要な空間について切り込み、今後サイバー空間の支配者となるため

の要素を備えているのは誰なのかを明らかにすることは、政治・経済・安全保障などにわたり今後の国際情勢を分析する際にも役立つ。

また、サイバー空間の支配要素を特定する過程で得られた分析のフレームワークを整理し、サイバー空間に関する分析の視点を提案する。本書では、サイバー空間における支配要素を「技術、産業、政策、数」として提示する。これらのどれが欠けても、サイバー空間の支配者となることはできないだろう。

- サイバー空間の支配要素

国際政治におけるパワーの源泉からサイバー空間の要素を覧としてまとめた。これらは国際政治からみたパワーの源泉をサイバー空間の要素として読み替えたものである。国家、組織、個人の関係性が変化したことにより、サイバー空間には、国家、組織、個人が単体で影響力を発揮することが可能な領域と、複数のプレーヤーが協力することが求められる要素がある。また、デジタル化された情報を中心に考えたとき、コンテンツやプラットフォームは、個人と組織と密接な関係にある。そのため、これらの要素を分類し、再構成することでサイバー空間の支配要素を特定することができる。

まず、サイバー空間の要素は、技術的優勢を確保するための要素と政策／産業的優位性を確保するための要素に分類できる。この 2 つに分類するのは、影響力を与えるプレーヤーを特定するためである。技術は個人や組織に紐づく要素とし、政策／産業は国や組織に紐づく要素とした。

技術的優位性を確保する要因は、ハードパワーとしての産業、技術、ソフトパワーとしての技術が相当する。この技術的優位性において影響力をもつプレーヤーは個人、組織である。国が主導的な役割を担う技術開発もあるが、サイバー空間で利用される技術は個人と企業等の組織が開発したものが多い。

また、政策／産業的優位性を確保するための要因は、ハードパワーの政策、産業、ソフトパワーのコンセプト、コンテンツ、国際標準が相当する。これらは国や組織が主に影響力を発揮するプレーヤーとなっており、従来の国際政治からみたパワーを多く包含している要素である。

そして、構造パワーでいう国際標準やプラットフォーム、ソフトパワーのコンテンツは、国家、組織、個人の三者のつながりを中心とした要素である。例えば、ソーシャルメディアはプラットフォームとして、情報が共有される場を提供する。この場を利用するのは、国家、組織、個人であり、情報の量や利用者数において優位な立場を確保するための要素である。本研究では、この要素を「数の要素」として、国、組織、個人の関係性が影響力を発揮する分野として定義する。この数の要素には、コンテンツなどの情報量だけでなく、コンテンツをめぐる市場規模、利用者数といった内容を含む。

技術、政策／産業、数（データ、市場、利用者数）の 3 つの要素は、互いに影響を与える関係でも

ある。例えば、政策／産業と技術の影響例では、インターネットで利用した商取引である電子商取引、暗号技術を応用したビットコインなどの暗号通貨がある。技術と数の影響例では、インターネットの普及がデータ、市場、利用者を増加させ、これに対応するための技術も開発された。携帯電話などの国際標準は、標準化に至る技術開発だけでなく、その結果として作られる市場規模も大きい。さらに、政策／産業と数の影響例は、GDPR をはじめとするパーソナルデータの保護、中国の金盾などの利用規制、プラットフォームビジネスへの規制がある。

表 1　サイバー空間の支配要素とプレイヤーの関係

サイバー空間の支配要素	影響を与える要因	具体的な影響分野
技術	個人、組織の能力	技術開発
政策／産業	組織、国家の能力	政策、規制、国際法
数（市場、利用者、データ量）	個人、組織、国家の関係性	データ量、国際標準、プラットフォーム

出所：三菱総合研究所作成

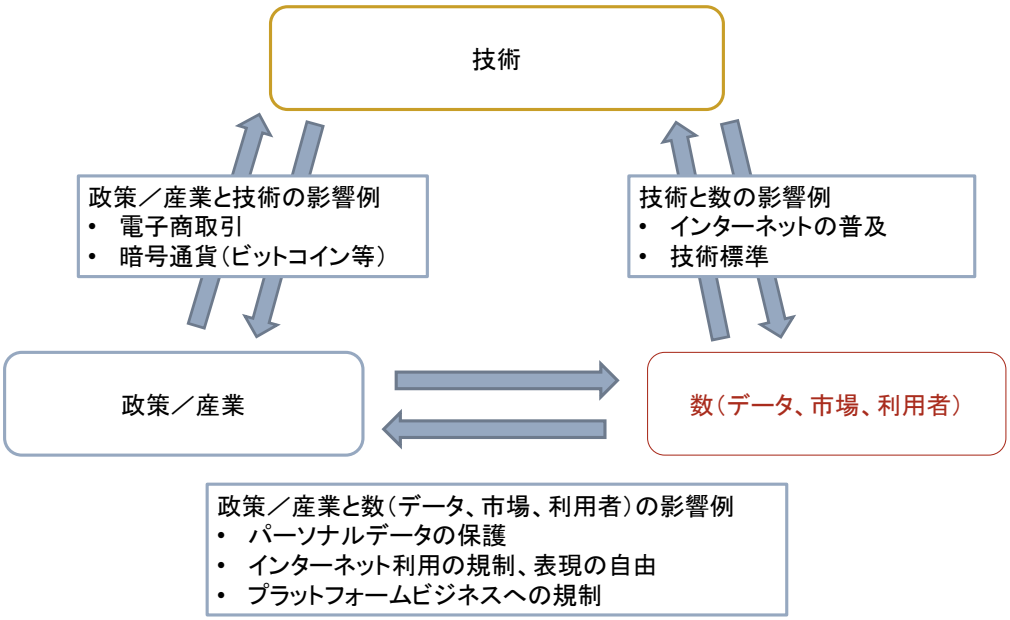

図 4　サイバー空間の支配要素間の影響例

出所：三菱総合研究所作成

- 米国は 1990 年代まで 3 要素における圧倒的優位性を持っていた

インターネットの誕生以来、米国はサイバー空間における技術、産業／政策、数のすべての面において優位性を持っていた。そのため、1990 年代までサイバー空間の支配者は米国であったといえる。米国は、サイバー空間で利用される機器、デジタル化された情報いずれにも影響を及ぼしていた。例えば、インターネットの通信中継機器であるルーターを製造するシスコシステムズ（Cisco Systems, Inc.）は、1984 年にスタンフォード大学コンピュータサイエンス学部の計算サービス部長のレン・ボサック（Len Bosack）と同大学のビジネススクールの学生であり、彼の妻であったサンディ・ラーナー（Sandy Lerner）によって設立された。シスコシステムズは、シリコンバレーのベンチャーキャピタルから融資を受け成長し、自身の技術開発に加え、関連企業の買収を通じた技術獲得を通じて技術力を高めている。このような、大学、ベンチャー企業、投資家のエコシステムによって技術力の強化が行われてきた。

産業／政策面においても標準化やインターネットガバナンスをはじめとする分野で、米国は主導的な地位を確立していた。米国が主導的な地位を確立できた要因は歴史的な経緯に加え、技術力や利用者数を背景とした競争力がある。これに加えて、1980 年代以降、米国では連邦政府が高性能コンピューティングに対して政策的な支援と投資を行い、全米の大学にスーパーコンピュータのための資金援助や、コンピュータを相互接続するためのネットワークの整備を行った。

1990 年代の米国では、HPC 法（High Performance Computing Act of 1991）が成立し、全米情報基盤（National Information Infrastructure: NII）を 2015 年までに整備することを掲げたビル・クリントン政権が誕生するなど、一般家庭におけるインターネット利用が推し進められた。HPC 法は情報化の推進による全米情報基盤の整備や大学を結ぶネットワーク整備を定めたもので、アルバート・ゴア上院議員を中心として法案成立が推進された。後に副大統領となったゴアによって、さらに情報スーパーハイウェイ構想が打ち出された。クリントン政権の発足後、HPC 法に基づき、米国政府は研究者以外も使える情報通信ネットワークの整備を進めた。米国政府は全米情報基盤整備に向けた行動計画（NII Agenda for Action）を掲げ、民間企業が中心となって NII を整備すること、政府は研究開発や競争環境整備などの支援を行うことを原則とした。米国政府は、HPCC（High Performance Computing and Communications）計画、CIC（Computing, Information, and Communications）計画、NGI（Next Generation Internet）計画として、毎年 10 億ドル程度を予算化し、支援していた。

インターネットガバナンスの分野においても、米国は影響力の強さを示している。例えば、1998 年に米国政府が発表したインターネットの名前およびアドレスの技術的管理の改善についての提案（Improvement of Technical Management of Internet Names and Addresses: Proposed Rule）では、米国の投資によって作られたインターネットの重要部分は米国政府機関との契約に基づいて運営されていると強調している。さらに、1999 年には米国のインターネット利用者数は 100 万人を超え、数の要素

についても、米国は絶大な力を持っていた。魅力的なコンテンツ、利用者、そこから生まれる市場も米国において急成長した

- 2000 年代以降崩れる米国の支配、欧州の影響力拡大によって変わるパワーバランス

しかし、2000 年代以降に米国の優位性は崩れ、EU 勢力が拡大した。EU の影響力は政策面で特に目立ち、1995 年の EU データ保護指令が EU 加盟国のみならず米国、日本など世界中に影響した。

EU データ保護指令第 25 条には、EU 加盟国から域外の第三国へ個人データを移転するときの規定があり、データ保護が EU の水準に達していない場合、第三国やその国の企業には個人データ移転を禁じることが定められていた。この指令に基づく EU 加盟国の立法により、日本や米国などは EU 加盟国からデータを移転できなくなる可能性が生じた。そのため、各国は個人情報保護制度の確立を急いだ。

このように、EU 地域で適用されるルールが世界規模で影響を与えたことから、欧州の政策／産業の要素は強まった。このデータ保護指令への対応として、2000 年には米国と EU の間で個人情報の移転を許容するセーフハーバー協定が結ばれている。日本も EU データ保護指令の影響から個人情報保護法を制定した。

そのほか、ISO や ITU におけるサイバー空間に関連するデジュール標準では 1 国 1 票の投票制度を利用した議決方式となり、欧州の影響力が拡大した。しかし、技術や数の側面では米国の一極集中が続いていた。その背景にはコンテンツ産業の強さがある。2000 年代後半からインターネットトラフィックの中心は動画に代わり、Google の Youtube や Comcast による動画配信サービスが台頭し、世界中のインターネット利用者は米国へのインターネットアクセスを求めるようになった。

2010 年代に 3 要素すべてで台頭する中国

2010 年代以降になると、中国がすべての面で影響力をもつようになる。技術に関しては、世界の工場として他国由来の技術を吸収、技術力を洗練させた。Huawei や ZTE による人材確保、技術開発力、多くの人口を抱える巨大市場、その市場でのテストを経た技術標準化（4G 携帯電話など）など、多くの面で中国の影響力は拡大している。中国は技術力に裏打ちされた産業政策や標準化、サイバーセキュリティ法や金盾（グレートファイアウォール）の稼働により産業／経済分野でも影響力を強化した。

標準化における中国の台頭は、IETF（Internet Engineering Task Force）における RFC（Request for Comments）の著者の割合からわかる。1990 年代、2000 年代、2010 年代の RFC 著者を国別に比較したとき、中国は 1990 年代の 4 名から 2010 年代の 587 名に増えている。IETF における標準化手続きは、1 年以上の時間が必要であり、さらに IETF 内での発言力やビジネス戦略も必要となる。RFC 著者における 2010 年代の中国の拡大は、技術や産業の要素における影響力拡大を意味している。

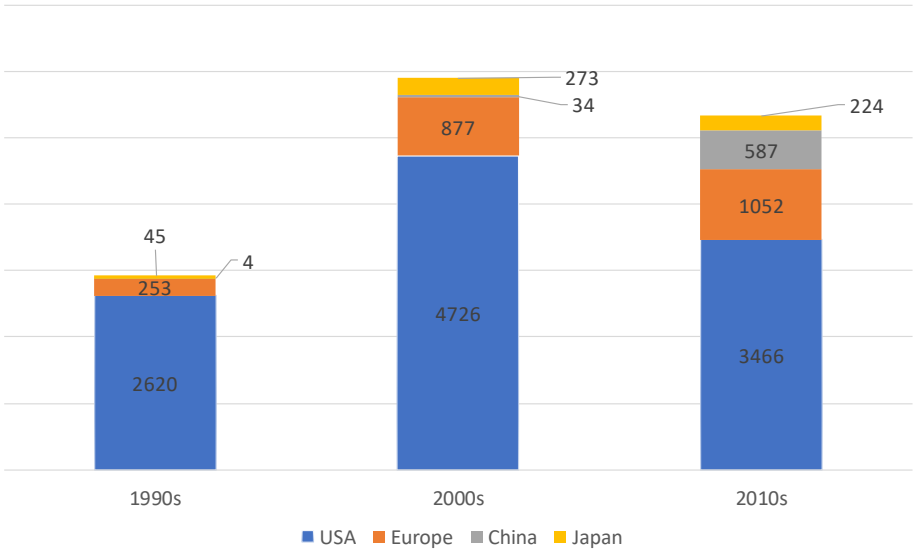

図 5 RFC の国別執筆者数の推移

出所：arkko.com から三菱総合研究所作成

また、コンテンツの面では世界最大の人口による利用者増大を背景とした世界第二のインターネット上での使用言語となった中国語により、膨大なコンテンツを生成するようになった。これらのコンテンツは中国国内のみならず国外の中国コミュニティに受け入れられる環境を作り出した。

最も特徴的なことは、中国が産業／政策面で米国主導のサイバー空間を必要としなくなりつつあることである。2000 年台後半以降、金盾によって Google をはじめとする米国由来のコンテンツを遮断、中国製メーカーによる割安な機器の普及、コンテンツ産業において百度（バイドゥ）、阿里巴巴（アリババ）、騰訊（テンセント）などを台頭させることで、サイバー空間上に中国由来の機器、コンテンツを増やした。その結果、中国はサイバー空間における支配要因のすべてにおいて影響力を発揮することが可能となった。

- 米国と中国の対立

米国と中国の間ではサイバー空間をめぐる対立が継続しておこっている。2015 年 9 月のオバマ・習会談において、軍事的な誤解を避ける取り組みを両国が進めるとともに、経済的利益を目的としたサイバー攻撃を行わないことで合意した。しかしこの合意は中国から米国への一時的なサイバー攻撃の減少という結果をもたらしたものの、引き続きサイバー攻撃が行われているといわれている。

2018 年 12 月、ポンペオ国務長官とニールセン DHS 長官は、中国国家安全部の関係のある者が、少なくとも 12 カ国のマネージドサービスプロバイダやクラウドプロバイダを攻撃していると指摘した。これ

に合わせて司法省は、中国籍の人物2名が主導し、45の米国企業、政府組織、12カ国以上にある企業を攻撃したとする起訴状を公開した。

中国国家安全部を背景としたサイバー攻撃であるとの指摘は、国際的な協力によって行われた。イギリスNational Cyber Security Center（NCSC）もAPT10が中国国家安全部と関係あると指摘している。英国外務省の発表によれば、NCSCが同盟国と共にAPT10は中国国家公安部の関係をつきとめたとしている。これまでにもNCSCは北朝鮮によるWannaCry、イランを拠点とするMabna Instiuteによる世界中の大学に対するネットワーク攻撃、ロシア軍事諜報部GRUによるNotPetya、WADA、及びBadRabbitを突き止めてきた。これに対して中国は、自身がサイバー攻撃の被害者であると主張し続けている。

日本は内閣サイバーセキュリティセンター、外務省がAPT10による攻撃への警戒を表明した。外務報道官談話で、国内企業や学術機関などを狙ったAPT10からの攻撃を長期に渡って確認していると説明した。「中国を含むG20メンバー国は、サイバー空間を通じた知的財産の窃取などの禁止に合意しており、国際社会の一員として責任ある対応が求められている。今後とも政府として国内サイバーセキュリティ対策の徹底に関する注意喚起を実施する予定」と表明した。この外務報道官談話は、米国や英国と同様にAPTが中国を拠点としていることを指摘しているが、中国国家公安部の関係とAPT10の関連については言及しなかった。

米国と中国の対立は以前から明らかであったが、近年中国が行うサイバー攻撃の戦略的目標を分析している。国家情報長官の下にあるNational Counter Intelligence And Security Centerは中国のサイバー攻撃目標の戦略的な目的を包括的な国力の向上、イノベーションを通じた経済成長モデルの確立、軍備の近代化にあると指摘している。そこで使われる手法には、非伝統的な情報収集、ジョイントベンチャーの設立、共同研究、学術連携、科学技術分野の投資、吸収合併（M&A)、フロントカンパニー、優秀者の採用プログラム、インテリジェンスサービス、法律・規制環境といったものがあると指摘している。

この報告書では、ほとんどの中国からのサイバー攻撃の標的は軍事、IT、通信関連企業であると指摘している。この報告書でもAPT10の活動について触れているほか、Windowsの不要ファイルや不要レジストリを削除するCCleanerのバックドアを利用して、Google、Microsoft、Intel、及びVMware等の米国企業を狙った攻撃を仕掛けることが可能と指摘している。

また、中国のサイバーセキュリティ法についても批判をしており、同法がアメリカの知的財産の窃盗に利用されていると指摘する。具体的には同法が海外企業に対してICTに関する安全保障上の検査を受けること、中国で運営する企業に中国国内でデータを保管することを定めたことを指摘している。このような法律は、中国へのデータのローカライゼーションを強制しているほか、非常に高いリ

スクがあると指摘した。実際に外国企業が中国で運営するためには、安全保障上の検査を通過し全てのデータを中国で保存した上で、ジョイントベンチャーの設立、データ転送に関する中国政府の許可、中国政府が許可する暗号製品、VPN の購入を行った上で初めて海外と米国の知財・データにアクセスできると指摘している。

China's Strategic Goals

Non-Traditional Collectors	China uses individuals for whom science or business is their primary profession to target and acquire US technology.
Joint Ventures (JV)	China uses JVs to acquire technology and technical know-how.
Research partnerships	China actively seeks partnerships with government laboratories-such as the Department of Energy labs-to learn about and acquire specific technology, and the soft skills necessary to run such facilities.
Academic Collaborations	China uses collaborations and relationships with universities to acquire specific research and gain access to high-end research equipment. Its policies state it should exploit the openness of academia to fill China's strategic gaps.
S&T Investments	China has sustained, long-term state investments in its S&T infrastructure.
M&A	China seeks to buy companies that have technology, facilities and people. These sometimes end up as Committee on Foreign Investment in the United States (CFIUS) cases.
Front Companies	China uses front companies to obscure the hand of the Chinese government and acquire export controlled technology.
Talent Recruitment Programs	China uses its talent recruitment programs to find foreign experts to return to China and work on key strategic programs.
Intelligence Services	The Ministry of State Security (MSS), and military intelligence offices are used in China's technology acquisition efforts.
Legal and Regulatory Environment	China uses its laws and regulations to disadvantage foreign companies and advantage its own companies.

図 6 中国のサイバー攻撃の戦略的目標

出所：Foreign Economic Espionage in Cyberspace 2018,

● パリコール

2018 年 11 月 12 日から 14 日、フランス・パリで、2018 年のインターネットガバナンスフォーラム(IGF)が開催された。 2018 年 11 月 12 日、この会議の開会セレモニーにおいて、フランスのエマニュエル・マクロン大統領がサイバー空間の信頼性と安全性のためのパリ・コールを宣言した。これに対して、発表時点で 50 カ国、民間企業や団体 300 組織以上が支持を表明した。た、パリ・コールに参加する日本企業は富士通と日立の 2 社であり、日本政府もパリ・コールを支持したが、米国と中国は支持していない。例えば、民間企業のマイクロソフトはパリ・コールを支持しており、インターネット関連団体では、ISOC、APNIC、LACNIC が支持者となっている。パリ・コールでは支持者に対して次のような課題に取り組むことを掲げている。

- ✧ 悪意あるオンライン活動の予防と強靭性を向上
- ✧ インターネットのアクセシビリティと完全性を保護
- ✧ 選挙プロセスへの干渉を防ぐために協力
- ✧ サイバー空間を通した知的財産権侵害に協力して対抗
- ✧ 悪意あるプログラムやオンライン技術の拡散を防止
- ✧ デジタル製品やデジタルサービスの安全性ならびにすべての人の「サイバー衛生」を向上
- ✧ サイバー傭兵や非国家主体の攻撃に対する対抗措置を実施
- ✧ 適切な国際規範の強化に協力して取り組む

パリ・コールにおける問題意識に対して、国家がその対応に動く意思を表したものといえる。問題意識とは広く社会に浸透し、人々の生活が大きく依存しているインターネットが悪意のある活動に対して脆弱であることを指し、様々なステークホルダーが集う IGF の対話以上に実効性のある対応を国家が行っていくことを訴えている。また、国家による「正しい規制」について多く言及しており、巨大プラットフォーム事業者による利用者の権利の侵害への懸念、中国のインターネット統制モデルを取り上げている。しかしながら、マクロン大統領が行った IGF におけるパリ・コールの発表では、国による規制に言及したことで IGF の参加者に動揺が広がったように、ステークホルダー全体の共通見解ではないことから今後の議論を注視する必要がある。特に、パリ・コールにおけるアプローチは緒に就いたところであり、サイバー空間において大きな存在である米国政府、中国政府、中国企業の支持が得られていないことは、大きな課題である。

パリ・コールを支持するマイクロソフトは、この動きを市民や民間インフラをサイバー攻撃から守る明確な原則（Clear Principles）と強い規範（Strong Norm）であると評した。また、世界中の企業がパリ・コールを支持することに賛同した。

● 提言：サイバー空間における秩序構築の試み

サイバー空間における国際秩序の構築について、現状、課題を議論し、その実現に向けた解決策を提言としてとりまとめた。

- サイバー空間に関連したルールは数多く存在しており、外交や安全保障分野との共存が必要である。さらにサイバー空間で利用される技術は進展が早い。また、サイバー空間におけるステークホルダーは、国家だけでなく、技術開発・インフラの運用に関わる民間、これらを利用する個人も含まれる。
- そのため、サイバー空間における国際秩序構築には、国際政治だけでなく、技術、議論にかかる時間軸、及びステークホルダーの多様性等の異なる要素を考慮することが必要である。
- 既存のルールとの整合性、マルチステークホルダの重要性、既存秩序構築の限界を課題として挙げ、これに向けた解決策として、国際機関の機能正常化、技術開発への投資、政策研究能力の底上げを提言する。
- 国際秩序構築に向けて、国際機関の正常な運用と技術開発投資の強化を提言する。また、サイバー空間における秩序構築にむけた日本への提言として、競争力強化に向けた政策研究能力の底上げを取り上げる。
    - まず、各国政府は国際機関、標準化機関の運営を正常化し、議論と合意が可能な状態を確保すべきである。サイバー空間における自由・公正で透明性のあるルールに基づいた国際秩序の構築には、様々な知見や新しい発想に基づく議論と合意ができる場が必要であり、その一つが国際機関や標準化機関である。このような場を運営し、技術と既存のルールの整合性とマルチステークホルダという課題に立ち向かう環境を整備することが重要である。
    - 国連におけるサイバー空間の規範に関する議論の停滞は、サイバー空間における価値観や制度の分極化を推し進めつつある。中国は、2014 年から世界インターネット大会を開催し、サイバー空間における新たなルールを、民間企業、学術界等と共に議論している。2015 年 12 月に中国政府が開催した第 2 回世界インターネット大会で、習主席はサイバー空間運命共同体の構築を宣言し、中国がインターネットガバナンスに積極的に関与していく姿勢を示した。また、2019 年 10 月の第 6 回世界インターネット大会では、中国現代国際関係研究所等が、サイバー空間運命共同体に関する報告書を発表した。この報告書はサイバー空間における国家主権の意味は変わったと主張し、基本原則、実行の道筋、ガバナンスのフレームワークを解説した。

- このような活動を通じた新たなルール作りはデファクトスタンダードとなり、国際機関の議論に影響を与え、これまで積み上げてきた議論を覆すことにもつながりかねない。そのため、国際機関の運営を正常化することが解決策の一つとして考えられる。
- 次に、公正な競争環境を構築するため、国や企業はサイバー空間を支える技術に対する研究開発を強化すべきである。なぜなら、自由・公正で透明性のあるルールや公正な競争環境は複数の先進的な技術をもつプレーヤーが市場にいてこそ成立するからである。サイバー空間に関するルール作りでは、国連で進むサイバー空間の規範の作りの他に、5G の標準化のように技術的な洗練度が要求されるものもある。
- 中国が 5G の標準化において台頭した要因のひとつは、研究開発に対する積極的な投資である。通信機器製造を行うファーウェイは、年間売上高の 10%以上を研究開発に投資し、積極的な研究開発を行っている。2018 年にファーウェイが行った研究開発投資は約 1015 億元であり、これは同社の売り上げの約 14.1%に相当する。これは NEC の 4.0%、トヨタ 3.5%と比較して大きい。また、全従業員のうち 45%が研究開発に従事していることも、同社が研究開発に重点を置いていることを示している。
- サイバー空間のルール形成においては、ルールが技術的に実現・検証可能かも重要である。ルールを作ったとしても社会に実装することが困難な場合、ルール自体の見直しを迫られるだろう。インターネットで利用される技術が、デファクトスタンダードによりルール化し世界に普及したのは、その技術が実現し、市場に受け入れられたからである。また、技術力はサイバー空間における自由・公正で透明性のあるルールを作る上で欠かせない。例えば市場において決定権を持つような技術の場合、一つの勢力に独占的な地位を持たせないようなルールを作っていないかを技術の側面から検証が可能である。また、悪意をもった技術を標準化しないようにする際にも技術力は必要である。
- そして、日本は競争力強化に向けた政策研究能力の底上げが必要である。サイバー空間における安全保障は研究分野として新しく、国際政治、技術、法律分野による学際的な研究が必要である。また、学際的な研究能力底上げは、今後の国際的な課題に向けた我が国の外交政策立案・遂行の基盤に欠かせない。しかし、サイバーセキュリティと安全保障の両分野にまたがる研究を行っている研究者の人数は少なく、研究の蓄積も不十分である。その原因は学際的な研究の場の欠如、限定的な活躍の場、研究キャリアの不安定さ等が挙げられる。そこで、政府が主導し、国際政治、技術、法律分野の博士、弁護士による政策研究を実施し研究成果を積み上げ、海外や国際機関を通じて知的・人的ネットワークを形成し交渉力を強化することが考えられる。これによって研究の蓄積、国際的な交渉の場で活

躍できる人物の育成、日本のサイバー空間の秩序構築におけるプレゼンスの向上が可能になる。

- 書籍出版（平成 30 年度）

情報収集結果、分析結果をとりまとめ、2018 年 8 月書籍として出版した。情報収集においては、各国の政策の他、サイバー空間が経済に与える影響に関する情報、サイバー空間の性質、サイバー空間における国際秩序に関する情報を収集し、分析結果としてサイバー空間を支配する要素を取り上げて、米国、中国、欧州の勢力図の変化に関する分析、台頭する中国に関する分析、暗号通貨に関する分析を行った。

（4）本事業を通して達成された研究基盤・体制の強化

- アウトリーチ活動を通じた研究基盤・体制の強化

当研究事業の研究成果として、書籍で取り上げた研究成果の共有と、関連するテーマに関する意見交換を行う研究会を 2018 年に開催した。意見交換の際には、2019 年 6 月 G20 サミット首脳会議を見据え、今後サイバー空間をめぐる安全保障、国際政治、ガバナンスについて、日本が取り組むべき課題を多様な視点から議論した。会議には外務省、内閣官房、総務省、経済産業省、研究機関、民間企業、大学等でサイバーセキュリティ、サイバー空間における安全保障に取り組む専門家が一堂に会した。

また、本年度は海外の研究会等に参加あるいは主催し、米国において気鋭の研究者と本研究成果に基づきディスカッションを行いその成果を研究内容にフィードバックするとともに本研究の認知度向上を目指した。加えて、EU Japan Cyber Workshop を共催し、その一セッションにおいて、本研究の紹介と日 EU の研究者とのディスカッションを行った。このような機会を通じて、互いの取り組みを認識すると共に、一つのテーマに関して議論できたことは今後の研究基盤・体制の強化につながると考える。

５．事業成果の公表(ページ制限なし)

●テーマ

（５－１）書籍出版

サイバー空間を支配する者　21 世紀の国家、組織、個人の戦略

●執筆者

持永大、村野正泰、土屋大洋

●概要

✧　サイバー攻撃、スパイ活動、情報操作、国家による機密・個人情報奪取、フェイクニュース、そしてグーグルを筆頭とする GAFA に象徴される巨大 IT 企業の台頭――。われわれの日常生活や世界の出来事はほとんどがサイバー空間がらみになっています。サイバー空間はいまや国家戦略、国家運営から産業・企業活動、個人の生活にまで、従来では考えられなかったレベルで大きな影響を及ぼしつつある。

✧　サイバー空間では、国家も企業も、集団も、個人もプレイヤーとなる。その影響力はそれぞれの地理的位置、物理的な規模とは一致しない。そして、経済やビジネスでもデータがパワーをもつ領域が広がっていますが、その規模は GDP では測れない。本書は、これほど重要になっているのに、実態が不透明なサイバー空間を定量・定性的に初めて包括的にとらえ、サイバー空間の行方を決める支配的な要素を突き止めるものである。果たして、そこから見えてくるもの

は何か? 日本はサイバー空間で存在感を発揮できるのか?

✧ 未来を制するのは誰か?後退する米国、台頭する欧州、支配力を高める中国。そして国家だけでなく、企業などの組織、個人がパワーを発揮するサイバー空間。その実態、支配力をめぐる競争の構図をはじめて明らかにする。

●発信手段

2018 年 8 月に日本経済新聞社から書籍として出版した。流通形態は従来の紙媒体に加え、Amazon、Apple、紀伊國屋等が電子書籍として提供している。

●国内外の有識者／他シンクタンク／メディアからの反応

出版後、紙媒体において 3 件のレビューが掲載された。そのほか、SNS や書籍のレビューサイトに書評が掲載されている。本書のレビュー結果は、概ね好評である。各メディアにおけるレビューでは、本書が今までに無い取り組みであることを指摘するとともに、産学融合取り組みによる力作との評価を得た。レビューの抜粋は次の通り。

週刊東洋経済（2018 年 11 月 3 日）　レビュー欄に掲載

“サイバー空間が抱える諸問題を深くかつ広範に描いた本書は日本が置かれた深刻な状況を伝える必読の一冊だ”　北海道大学大学院教授　橋本努

日本経済新聞（2019 年 1 月 5 日）　書評欄に掲載

“インターネットは我々の生活にとって必要不可欠なものだ。書店には「サイバー・セキュリティー」や「IoT」について解説する書籍が溢（あふ）れているが、全体を俯瞰（ふかん）する書が意外と見当たらない。本書はサイバー空間の実態を総合的に分析した力作である。”　日本大学教授　小谷賢

PHP　Voice　（2019 年 3 月号）　書評欄に掲載

“日本のサイバー研究は遅れている。本書のような産学融合の取り組みに期待したい。”

（５－２）Web を通じた情報発信

昨年度に引き続き、Web サイトによる研究成果の発信を行っている。政策担当者向けにサイバー空間

における政策をわかりやすく分類し、絞り込みをしやすいインタフェースを備えている。

図 7　Web を通じた情報発信

６．事業総括者による評価（２ページ程度）

本事業は3年の計画期間中にサイバー空間の安全保障に係る研究を行うとともに、その成果を書籍等としてとりまとめ発信していくことにより、我が国における研究の裾野を広げることを主な目的としている。本年度はその3年目として、共同研究者との定例研究会を開催すると共に、米国研究機関や米国在住研究者とのディスカッションを実施した。また、本事業のアウトリーチ活動の一環として、日EUサイバーセキュリティワークショップの一セッションにおいて本研究の紹介とディスカッションを行った。

計画との対比で総括すれば、当初設定していた3年計画の最終年度として、アウトリーチ活動や海外活動に力点を置いた成果を出したものと考えている。

本事業を開始した2017年の時点ではサイバー空間に関する政策的なプライオリティは国際政治の様々な課題の中では傍流を占めるに過ぎなかったが、米中の対立やGAFAやBAT等影響力の拡大等を背景に、サイバー空間の政策に占めるプライオリティは近年ますます高まる一方である。これにより当初我々が本事業の目的として提起していた「サイバー空間に関する安全保障」を議論するための基盤の必要性もますます高まってきている。

しかしながら、我が国におけるサイバー空間に関する言説はジャーナリスティックなものに偏る傾向にあり、体系的にとらえる活動はまだ不十分なものと言わざるを得ない。本事業の目的としている国際情勢把握に向けた政策研究能力の強化はまことに時宜にかなったものであるということができる。また、研究の成果を書籍として刊行することができたのも、我が国におけるサイバー空間に関する政策に関する体系的な研究の嚆矢の一つとなったものと考えている。

効率性という観点から本事業を評価すると、初年度を、研究活動にあて、その成果を二年目の書籍化につなげ、三年目にその成果を国内外の研究者と共有できたことは大きな成果であると考える。また書籍化を通じて、当該分野に興味をもつ数千人もの人間に効果的に研究成果を普及させたことは、他の手段（セミナー等の開催）に較べて効率的であったと評価している。反面、研究コミュニティの形成という観点からは、書籍のような一方通行のメディアは適していない点には留意する必要がある。コロナウイルスで中止を余儀なくされた研究会もあるが、最終年度に実施したような国内外の研究者とのディスカッションと書籍化は相補的なものであり、どちらも有効に機能したと思われる。

本分野をめぐる状況はめまぐるしく変化しており、しかもその重要性は増すばかりである。三年目以降の活動については、状況の変化に柔軟に対応し、事業としての有効性・効率性を常に意識しながら、事業の成果を最大化することに努める必要がある。