様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

# 科学研究費助成事業　　研究成果報告書

令和　５ 年　 ６ 月 ２１ 日現在

機関番号：３２６１５
研究種目：基盤研究(C)（一般）
研究期間：2017～2022
課題番号：１７Ｋ０３５５５

研究課題名（和文）サイバースペースと国際関係：日本とヨーロッパ，NATOの安全保障協力

研究課題名（英文）Cyberspace and International Relations: Japan, Europe and NATO Security Cooperation

研究代表者
ＶＯＳＳＥ　Ｗｉｌｈｅｌｍ（Vosse, Wilhelm）

国際基督教大学・教養学部・教授

研究者番号：７０３２７７３２

交付決定額（研究期間全体）：（直接経費）　　2,400,000円

研究成果の概要（和文）：この初期調査は、サイバーセキュリティの国際協力とサイバー外交の強化における日本の取り組みを包括的に概観するものであった。調査結果は、「信頼あるデータの自由な流れ」（DFFT）やEUのGDPRのようなサイバー規範やルールの開発と実施の成功、特にASEANやアフリカ諸国におけるサイバー能力構築の重要性、政府機関、CERT、開発援助機関間の技術的・実務的協力、法執行や技術訓練を通じたサイバー犯罪との闘いの促進などを示している。サイバー攻撃の課題は、人工知能（AI）や量子コンピューティングのようなまだ発展途上の課題に対する最初の政策調整分野としても機能する。

研究成果の学術的意義や社会的意義
This study developed a better understanding and a theoretical model of how cyber attacks, cybercrime, and other emerging technologies have begun to undermine national and international security, classical deterrence, alliance dynamics, and international norms and rules.

研究成果の概要（英文）：This initial study provided a comprehensive overview of Japanese initiatives in international cybersecurity cooperation and the strengthening of cyber diplomacy. The main focus was Japan's cooperation with the European Union and many of its member states, and NATO. The findings demonstrate the successful development and implementation of cyber norms and rules such as "Data Free Flow with Trust" (DFFT) and the EU GDPR, the importance of cyber capacity building especially in ASEAN and African countries, technical and practical cooperation between government agencies, CERTs, development assistance organizations, facilitating the fight against cybercrime through law enforcement and technical training. The challenges of cyber attacks can also serve as the first policy coordination field for still-developing challenges like artificial intelligence (AI) or quantum computing. This research project has developed a better theoretical model on cyber deterrence and security partnerships.

研究分野：international relations

キーワード：security studies　cybersecurity　cyber diplomacy　EU　Japan　EU-Japan　NATO

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

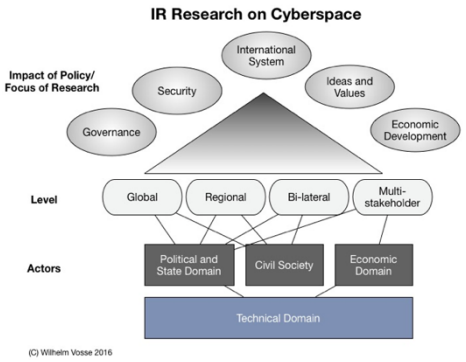
## １．研究開始当初の背景

This was a study in foreign policy analysis. Over the last decade, Japan has been deepening new security partnerships with countries in Europe, the EU, and NATO, as well as countries in the Asia-Pacific. One reason is a shared concern about issues of cyberspace and cybersecurity. This study asks: In what ways have cyberspace-related problems deepened Japan's bi- and multilateral security ties? The broader theoretical objective is to integrate better the new demands posed by cyberspace issues into foreign policy analysis and IR theory.

Since the early 2000s, Japan has gradually broadened and intensified its diplomatic ties with a range of middle powers, which has intensified further since 2007. Most prominent are Japan's bilateral security partnerships with Australia, India, the EU, the UK, France, and some SE Asian nations. Japan's 2013 National Defense Strategy (NSS) emphasizes "strengthening diplomacy and security cooperation with Japan's partners for peace and stability in the international community" (NNS 2013). The New Security Laws (2015) also allow Japan closer and more pragmatic cooperation with new security partners.

This deepening and broadening of security partnerships also influenced the academic debate. Some have described the recent changes as a shift from a "hub and spokes" model to a "webs and wheels" configuration (Bisley 2008). Others see new security alignments or partnerships (Wilkins 2010, 2012). The PI analyzed Japan's new security partnerships (see methodology) with experts from Australia, India, the Philippines, Vietnam, and Europe and published an innovative analysis of the views in Japan and each of the partner countries and an overall assessment of broader security policies and specific areas of cooperation in Vosse and Midford (2017). Closer collaboration is usually induced by a changing security environment or collective challenges which require a governance response, such as the governance of the global commons. Central among those are the challenges of cybersecurity and cyberspace (i.e., the information infrastructure) more broadly.

## ２．研究の目的




This project wanted to analyze the contents of agreements and interaction styles, and government initiatives in the partner countries, particularly in the EU and NATO, Australia, and India. It was expected to fill this gap by (a) analyzing how Japan's international cooperation in the area of cyber politics with new security partners in Europe and Asia has intensified, reflecting the specific demands of cyber diplomacy, and (b) further the development of a theoretical framework for IR research which better reflects cyber politics. Specifically, how state, societal, and economic actors with their often-diverse objectives shape their cooperation or competition in global, regional, bi-lateral, and multi-stakeholder institutions and forums, and finally, how this will shape governance, security, ideas and values, economic development, and eventually the international system which might become a less or more hierarchical system.

## ３．研究の方法

This study used an interdisciplinary approach (from social sciences to science and technology) as cyberspace features challenge contemporary IR theory, foreign policy, and practice. Other security analysts had predicted a coming cyber war since the 1990s, requiring states to protect and defend their I.T. infrastructure while preparing to attack I.T. systems of potential enemy states, making offensive strategies the only option. However, cyberattacks do not necessarily target industrial or military infrastructure. Still, the tactical or strategic release of hacked data during an election campaign can also weaken the foundations of a political system by affecting the chances of specific candidates. The empirical part of this project was purposely limited to Japanese security ties with Europe and NATO. Still, it will integrate the

assessment from experts from Australia and other countries in the Asia-Pacific and the United States.

The PI began with analyzing official government documents, laws, and research reports and the challenges in implementing some of these policies. Special attention was given to the problems and deficiencies and the significance of international cooperation in Japan and Europe through expert interviews and observations in Japan and the EU. The PI interviewed government officials, cyberspace and cybersecurity analysts in Japan and several European countries, the EU, and NATO in Brussels. The focus was on finding out more about the practical implementation of cyberspace policies and regulations and their international cooperation components of many European countries, the EU, NATO, but also the United Nations, ARF, ASEAN, and other international bodies. These were then compared with those in Japan.

Another focus was the discourse in inter-governmental bodies and multi-stakeholder settings and how differences in standpoints, for example, on cyber intelligence gathering or public attribution of cyber-attacks, were solved.

Finally, the project aimed to develop a better theoretical framework for how cybersecurity and potentially other emerging technologies influence alliance dynamics, regional and inter-regional cooperation, threat perception, and deterrence dynamics in Europe, Japan, and their relations with the broader Indo-Pacific region.

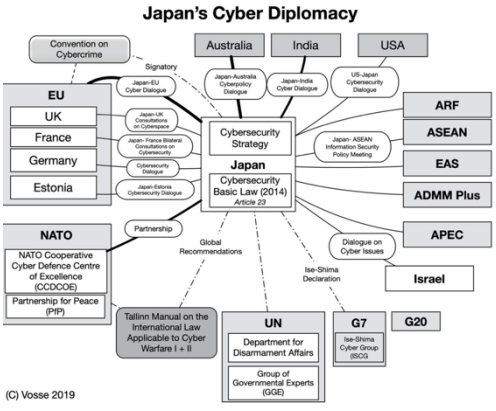
To discuss the empirical finding and the theoretical models, the PI organized and co-organized a series of workshops in Japan and Europe and presented his findings in these workshops, public lectures, and international academic conferences in Japan, Europe, and the United States.

## ４．研究成果

The research findings of this project were published in journal articles and book chapters, and the PI is currently working with three co-editors on the “Handbook on Cyber Diplomacy” (Palgrave), expected to be published in 2024.

The main findings include are as follows.

(1) Japan has become one of the world's most active cyber diplomatic actors. The significant number of bilateral cyber dialogues have led to a further strengthening of Japan’s domestic I.T. infrastructure through the exchange of security practices, a better understanding of the implementation of cybersecurity training on private companies in Japan and Europe, but also in the United States and many countries of Southeast Asia.




(2) Through Japanese participation and effective initiatives in Internet governance through multilateral settings, such as the UNGGE, OWEG, WSIS, GCSC, or IGF, Japan has contributed to the protection of a free, open, and secure cyberspace to defend and strengthen international law and Internet governance, to enhance confidence-building measures, and most recently, to bolster data privacy. Demographically challenged, Japan sees cyberspace, information technology, artificial intelligence (AI), Fintech, robotics, and the IoT as core components of its vision of the information society - or, as Japan has begun to call it, "Society 5.0."

(3) As far as EU-Japan cyber diplomacy is concerned, the EU-Japan Strategic Partnership Agreement (2018) lists cooperation on cyber issues (Art. 36) and information society (Art. 21) as being among the fields of intended closer EU-Japan security cooperation. What is essential in this regard is to foster collaboration in the areas of capacity-building and training (e.g., on the EU side with ENISA), universities and think tanks (with programs such as Horizon 2020 and Horizon

Europe), and EU CERT and Japan CERT (such as with the EUNITY project). In essence, EU-Japan SPA is an ideal framework for expanding and deepening EU involvement and its role in further developing better solutions for common security challenges, including cybersecurity and information society.

(4) The EU and Japan have become core partners in strengthening data privacy and security in their own countries and spreading norms. Core in this regard is the EU GDPR, the EU-Japan Data Adequacy Law (2019), and Japan's Osaka Track or "Data Free Flow with Trust" (DFFT) initiative.

Table 1: Japan's Cyber Diplomacy (Areas of Cooperation)

| Initial Year | Partner Country | Cyber Dialogue | Capacity Building | Internet Governance Cooperation | Technical and Training Cooperation | Confidence building | Whole of government approach |
|---|---|---|---|---|---|---|---|
| 2013 | USA | O | | O | O | | O |
| 2014 | EU | O | O | O | O | | O |
| 2018 | NATO | | O | | O | | |
| 2018 | Estonia | O | O | O | | | |
| 2012 | UK | O | O | O | O | | O |
| 2014 | France | O | | O | | | |
| 2015 | Australia | O | O | O | | O | O |
| 2012 | India | O | O | | | O | O |
| 2009 | ASEAN | O | O | | O | O | |
| 2014 | Israel | O | | O | O | | O |

(5) Japan, in many cases in cooperation with the EU, have become the main actors and norm entrepreneurs in the strengthening and spreading cyber confidence-building measures. Japan is building international communication channels, increasing transparency, and deepening policy dialogues in bilateral and multilateral consultations as central components. For example, through capacity-building, the corresponding confidence-building measures are heavily focused on ASEAN and the ASEAN Regional Forum (ARF). In 2017 and 2018, the Cabinets Office and MOFA held bilateral consultations within the ARF framework to share policies on threat awareness and cybersecurity strategies to build trust.

(6) Japan and the EU have closely cooperated to deal with cybercrime, Convention on Cybercrime and mutual legal assistance treaties, and the International Criminal Police Organization (ICPO). Japan and the EU have cooperated in developing "new investigative techniques" and strengthening their "digital forensics capabilities" to analyze digital devices or malicious software better to predict threats. Important in this regard is also the ASEAN-Japan cooperation to combat cybercrime, and the involvement of third countries, such as the UK, the USA, and Australia, in these activities. The PI published one of the first book chapters in a volume on EU-Japan cooperation in law enforcement.

(7) Capacity-building is another area where Japan has been a pioneer, especially in strengthening the training of I.T. professionals working for governments and private companies in ASEAN countries. The EU has or is going to cooperate more with Japan, as most internet users are now located in the Indo-Pacific. Japan takes a more strategic view of cyber capacity-building. Japan uses multilateral fora such as the G-7 and G-20 summits, as well as its security and that of its nationals, as a core incentive to strengthen the improvement of cyber capacities in developing countries, as attacks on the IT infrastructure of trade partners in the region can adversely affect Japan. In addition, spreading norms and rules on data handling and access control needs to be strengthened in many less cyber-secure countries. Japan itself has recently benefitted from its participation in NATO CCDCOE cyber exercises.

(8) The EU and Japan have also been central in developing and implementing digital development assistance. The PI developed this concept and has been spreading the necessity to finance and implement such projects in less cyber-secure countries in the Indo-Pacific and Africa together with a collaborator at the Netherlands Institute of International Affairs (see: publications).

(9) The broader theoretical framework dealing with the actual and potential influence of cybersecurity and cyber threats on national security, deterrence theory, and alliance and alignment models was developed by the author in Vosse (2021). He argued that the still-nascent Indo-Pacific "security order" should be extended from traditional, predominantly maritime, security concerns to include information and digital security because the Indo-Pacific security order is potentially undermined by information technology and an AI duopoly potentially more so, or at least equal to threats of maritime or territorial security. Classical studies on Asian security order and regional security argue that regional security complexes have to be in some way distinct and separate from the global security order. The PI argued that regional players like the European Union and its member states or Japan are, if not geographically, but in terms of the impact of the region on their own economic security and survival of the liberal world order closely related to the Indo-Pacific region.

Cyberspace and the way cyber power can influence political order, social and political attitudes, views of other countries, or the political leadership of one's own country and government much more fundamentally than it was ever possible through traditional media or soft power in the past.

５．主な発表論文等

〔雑誌論文〕　計10件（うち査読付論文　9件／うち国際共著　10件／うちオープンアクセス　4件）

| | |
|---|---|
| １．著者名<br>Wilhelm Vosse and Maaike Okano-Heijmans | ４．巻<br>3 |
| ２．論文標題<br>Promoting open and inclusive connectivity: The case for digital development cooperation | ５．発行年<br>2021年 |
| ３．雑誌名<br>Research in Globalization | ６．最初と最後の頁<br>1-10 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1016/j.resglo.2021.100061 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>該当する |

| | |
|---|---|
| １．著者名<br>Wilhelm Vosse and Maaike Okano-Heijmans | ４．巻<br>May 14, 2020 |
| ２．論文標題<br>Digital connectivity going global: The case for digital ODA | ５．発行年<br>2020年 |
| ３．雑誌名<br>Clingendael Policy Brief | ６．最初と最後の頁<br>1-7 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>なし | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>該当する |

| | |
|---|---|
| １．著者名<br>Wilhelm Vosse | ４．巻<br>October 2019 |
| ２．論文標題<br>Japan’s Cyber Diplomacy | ５．発行年<br>2019年 |
| ３．雑誌名<br>European Institute of Security Studies (EUISS), Research in Focus | ６．最初と最後の頁<br>1-21 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>なし | 査読の有無<br>無 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>該当する |

| | |
|---|---|
| １．著者名<br>Wilhelm Vosse | ４．巻<br>19 |
| ２．論文標題<br>Renewable Energy Strategies Leading to Closer Europe-Japan Cooperation after 3/11 | ５．発行年<br>2018年 |
| ３．雑誌名<br>Asian International Studies Review | ６．最初と最後の頁<br>61～85 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.16934/isr.19.2.201812.61 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>該当する |

| | |
|---|---|
| 1．著者名<br>Vosse Wilhelm M. | 4．巻<br>31 |
| 2．論文標題<br>Learning multilateral military and political cooperation in the counter-piracy missions: a step towards de-centering of Japan's security policy? | 5．発行年<br>2018年 |
| 3．雑誌名<br>The Pacific Review | 6．最初と最後の頁<br>480～497 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1080/09512748.2017.1371213 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>該当する |

| | |
|---|---|
| 1．著者名<br>Wilhelm Vosse | 4．巻<br>1 |
| 2．論文標題<br>EU-Japan security partnership in practice: The counter-piracy mission off the coast of Somalia | 5．発行年<br>2018年 |
| 3．雑誌名<br>Japan's new security partnerships: Beyond the security alliance | 6．最初と最後の頁<br>219-235 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>なし | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>該当する |

| | |
|---|---|
| 1．著者名<br>Wilhelm Vosse and Paul Midford | 4．巻<br>1 |
| 2．論文標題<br>Introduction | 5．発行年<br>2018年 |
| 3．雑誌名<br>Japan's new security partnerships: Beyond the security alliance | 6．最初と最後の頁<br>1-15 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>なし | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>該当する |

| | |
|---|---|
| 1．著者名<br>Wilhelm Vosse and Paul Midford | 4．巻<br>1 |
| 2．論文標題<br>Conclusion | 5．発行年<br>2018年 |
| 3．雑誌名<br>Japan's new security partnerships: Beyond the security alliance | 6．最初と最後の頁<br>236-242 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>なし | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>該当する |

| | |
|---|---|
| 1．著者名<br>Vosse Wilhelm M. | 4．巻<br>31 |
| 2．論文標題<br>Learning multilateral military and political cooperation in the counter-piracy missions: a step towards de-centering of Japan's security policy? | 5．発行年<br>2017年 |
| 3．雑誌名<br>The Pacific Review | 6．最初と最後の頁<br>480～497 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1080/09512748.2017.1371213 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>該当する |

| | |
|---|---|
| 1．著者名<br>Vosse, Wilhelm | 4．巻<br>53 |
| 2．論文標題<br>A conceptional broadening of security order in the Indo-Pacific: The role of EU-Japan cooperation in IT and cybersecurity | 5．発行年<br>2022年 |
| 3．雑誌名<br>Asian Affairs | 6．最初と最後の頁<br>561-582 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1080/03068374.2022.2090683 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>該当する |

〔学会発表〕　計12件（うち招待講演　10件／うち国際学会　5件）

| |
|---|
| 1．発表者名<br>Wilhelm Vosse |
| 2．発表標題<br>Japan's Cyber Diplomacy |
| 3．学会等名<br>Webinar: Japan’s proactive diplomacy in cybersecurity and data governance（招待講演） |
| 4．発表年<br>2020年 |

| |
|---|
| 1．発表者名<br>Wilhelm Vosse |
| 2．発表標題<br>Cybersecurity Policy in Japan and Asia |
| 3．学会等名<br>Norwegian University of Science and Technology (NTNU)（招待講演） |
| 4．発表年<br>2019年 |

１．発表者名
Wilhelm Vosse

２．発表標題
UK-Japan cooperation in cybersecurity and/or the development and governance of artificial intelligence

３．学会等名
Post(?)-Brexit: UK-Japan Relations（招待講演）

４．発表年
2019年

１．発表者名
Wilhelm Vosse

２．発表標題
Cybersecurity and AI: Core drivers for the EU-Japan SPA?

３．学会等名
The EU-Japan Strategic Partnership Agreement - Prospects for Future EU-Japan Cooperation on Cyber Security and AI（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
Wilhelm Vosse

２．発表標題
From defensive to offensive cyber operations? Japan's cybersecurity cooperation with the US, EU, and NATO”

３．学会等名
Annual Conference of the International Studies Association (ISA) International Security Studies Section（国際学会）

４．発表年
2019年

１．発表者名
Wilhelm Vosse

２．発表標題
Japan-UK Cooperation on Cybersecurity and AI: What impact from Brexit?

３．学会等名
Japan-EU 2020 Forum: The European Union and Japan in a fluid Global Liberal Order.（招待講演）

４．発表年
2020年

１．発表者名
Wilhelm Vosse

２．発表標題
EU-Japan Cyber Diplomatic Cooperation

３．学会等名
EU-Japan Forum, Universite libre de Bruxelles (ULB), Brussels,（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
Wilhelm Vosse

２．発表標題
EU-Japan Cooperation in Cyber Diplomacy

３．学会等名
What is Japan’s Place in a Changing Global Order?

４．発表年
2018年

１．発表者名
Wilhelm Vosse

２．発表標題
EU-Japan Co-operation on Cyber Security

３．学会等名
EU-Japan Agreements: What Now? Joint Conference by the Konrad-Adenauer Stiftung (KAS) and European Japan Advanced Research Network (EJARN)（招待講演）（国際学会）

４．発表年
2018年

１．発表者名
Wilhelm Vosse

２．発表標題
Cyberspace and Security Partnerships: The Case of Japan, EU, and NATO Cooperation

３．学会等名
Annual Conference of the International Studies Association (ISA),（招待講演）（国際学会）

４．発表年
2018年

１．発表者名
Wilhelm Vosse

２．発表標題
The Importance of New Security Partnerships for Japan’s National Defense

３．学会等名
School of Oriental and African Studies (SOAS), University of London（招待講演）

４．発表年
2019年

１．発表者名
Wilhelm Vosse

２．発表標題
Japan’s New Security Partnerships

３．学会等名
School of Oriental and African Studies (SOAS), University of London,（招待講演）

４．発表年
2018年

〔図書〕　計3件

１．著者名
Wilhelm Vosse and Paul Midford

４．発行年
2020年

２．出版社
Routledge

５．総ページ数
265

３．書名
New Directions in Japan’s Security: Non-U.S. Centric Evolution

１．著者名
Wilhelm Vosse

４．発行年
2019年

２．出版社
Routledge

５．総ページ数
15

３．書名
Japan's Future and a New Meiji Transformation: International Reflections

| | |
|---|---|
| １．著者名<br>Japan's new security partnerships: Beyond the security alliance | ４．発行年<br>2018年 |
| ２．出版社<br>Manchester University Press | ５．総ページ数<br>247 |
| ３．書名<br>Wilhelm Vosse and Paul Midford | |

〔産業財産権〕

〔その他〕

―

６．研究組織

| | 氏名<br>（ローマ字氏名）<br>（研究者番号） | 所属研究機関・部局・職<br>（機関番号） | 備考 |
|---|---|---|---|

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

| 共同研究相手国 | 相手方研究機関 |
|---|---|