論文要旨

サイバー外交政策に関する研究
-キャパシティビルディングを中心に-
A Study on Foreign Policy on Cybersecurity Issues with an Emphasis on Capacity Building

２０１８年３月

情報セキュリティ研究科

情報セキュリティ専攻

５６４８１０２　村上　啓

Hiromu MURAKAMI

指導教員　湯淺　墾道

（日本語）

近年、「サイバー外交」という新しい外交分野が国際社会において展開されている。サイバー外交とは、二国間外交や多国間外交という従来の伝統的な外交と同様の方法により、DDoS 攻撃や標的型攻撃、マルウェア等のサイバー空間に関する国際的な諸問題を国家や国際機関、民間企業、CERT コミュニティ、市民社会等のサイバー空間のマルチステークホルダーが協力・連携して対処し、国家と国際社会の安全、安定及び繁栄を促進するために行う交渉及び政策である。サイバー空間を利用した悪意のある行為は、国境を瞬時に越え、国家の重要インフラ等の機能不全等を惹起する安全保障上の脅威として認識され、各国や国際連合を含む国際機関や民間企業、CERT コミュニティ等が協力して対処しようと取り組んでいる。サイバー外交において特に重視しているのは、従来の国際法の適用や国際規範等サイバー空間における法の支配の促進、サイバー空間における信頼醸成措置、そして、途上国に対するサイバーセキュリティ能力のキャパシティビルディングの三点である。この三点について、重点的に各国政府が取り組んでいるのが、約 20 年前に国連第一委員会に設置され、5 回の会合を行ってきたサイバーの問題を安全保障の観点から議論してきた「国際安全保障の文脈における情報電気通信分野の進展」に関する政府専門家会合（GGE）である。しかし、この GGE が 2017 年、サイバー空間を利用した国家の規制の在り方を巡り対立する米国を中心とする「西側諸国」と中露等を中心とする陣営の激しい鍔迫り合いの結果、合意に至らず、米国政府や米国のシンクタンク、また、NATO の協調的サイバー防衛センター（CCDCoE）等は「失敗」あるいは「死んだ」と表現した。この「失敗」により、ポスト GGE のサイバー外交の先行きが不透明な中、サイバー空間の脅威は日進月歩で巧妙化しており、それは明白な現在の危険として存在している。このような文脈において、日本はサイバー外交政策、開発協力政策において、東南アジア諸国等を中心とするサイバーセキュリティのキャパシティビルディングを積極的に行うべきであるというのが本論文の趣旨である。

その理由は、第一に、日本の安全保障の強化、第二に、対中露等を睨んだ外交戦略上の手段としての利用、第三に、日本の経済的基盤の構築と経済成長、第四に国際社会の安全と安定の促進にある。すなわち、サイバーセキュリティのキャパシティビルディングを開発途上国に積極的に実施することにより、被支援国の脆弱なネットワークやシステムを踏み台にして、日本政府や当該国の日本企業や日本人に対するサイバー攻撃がある現状を鑑み、システムの調達や業務のアウトソーシング等のサプライチェーンにおけるサイバーセキュリティ能力の構築、強化を支援することにより、日本のサイバー安全保障を強化することが可能である。また、サイバー空間の在り方に関するイデオロギーが異なる中露等陣営が国際社会の多数派になることを防止するため、途上国に働きかけ、サイバーセキュリティの能力支援を行うことにより、良好な関係を構築、強化し、多数派の合意形成を可能となる。さらに、条件付きのタイド政府開発援助（ODA）等により、支援主体を日本と当事国の企業等に限定することにより、被支援国における日本企業の経済基盤の確保と事業

展開を行うことができるようになる。そして、責任ある国際社会のメンバーとして、途上国のサイバーセキュリティ能力の構築を支援、強化、維持することにより、被支援国のサイバー安全保障を強化し、当該国とその地域ひいては国際社会全体のサイバーのリスクを低減することができる。このような観点から、日本はサイバーセキュリティに関するキャパシティビルディングを積極的に展開することが国際協調主義に基づく積極的平和主義を掲げる日本国の国益に資すると考えられる。

（英語）

In recent years, a new area of diplomacy called “Cyber Diplomacy” has been developed in the international community. Cyber Diplomacy is a negotiation or policy to promote security, stability and prosperity of states and the international community where states, international organizations, private sector, CERT communities and civil society cooperate and coordinate to address international issues in cyberspace such as DDoS attacks, advanced persistent threats and malware by the similar methods such as bilateral diplomacy and multilateral diplomacy used in the traditional means of diplomacy. Malicious use of cyberspace cross national borders instantaneously and it is recognized as a threat to national security that triggers malfunction of national critical infrastructure and addressed by states, international organization including the United Nations, the private sector, CERT communities. The essential agendas for Cyber Diplomacy are the following three points: a) promotion of the rule of law in cyberspace through the application of existing international law to cyberspace and international norms for cyberspace; confidence building measures in cyberspace; and cyber security capacity building. The Group of Governmental Experts on Developments in the field of information and telecommunication in the context of international security that had been discussing cyber issues from the standpoint of international security, conducted five rounds of sessions in the last two decades. However, this GGE has been “failed” or “dead” in 2017, according to the United States Government, US think tank and NATO CCDCoE, due to disagreement over some issues over the way of regulating state’s behavior in cyberspace between the US and its “allies” and China, Russia and their “companies”. Due to this “failure”, the future of post-GGE Cyber Diplomacy is uncertain but cyber threats are becoming sophisticated day by day and are clear and present danger. In this context, this paper recommends that Japan should proactively engage in cybersecurity capacity building to countries such as Southeast Asian nations in its foreign policy and aid assistance policy on cyber issues. The reasons for this recommendation are as follows:

Primarily, to strengthen Japan’s national security. Second, to use it as a means of

diplomatic strategy against China, Russia and others. Thirdly, for the development of business basis for Japan and its economic growth. Fourth, to promote security and stability of the international community. Considering the current situation where cyber attacks against Japanese government, Japanese companies in recipient country, and Japanese people are carried out via vulnerable networks and systems of recipient, assisting the development and strengthening of cybersecurity capacity in supply chain such as procurement of systems and business outsourcing enable the strengthening of Japan's cyber security by proactively conducting cybersecurity capacity building to developing countries. Further, in order to prevent China, Russia and others' ideology on cyberspace prevail and triumph in the international community, approaching to developing countries and assisting their cybersecurity capacity building will contribute to develop and strengthen amicable relations with recipients and thereby forming a majority in the international community. Moreover, tied Official Development Aid (ODA) with conditions that limit assistance provider to Japan and recipient companies will enable to form an economic basis for Japanese companies' in the recipient country and business development. Furthermore, as a responsible member of international community, assisting, strengthening, and maintaining developing countries' cyber security will strengthen recipient's cyber security and reduce the risk of recipient, the region and ultimately the entire international community. From these points, I believe a proactive engagement in cybersecurity capacity building will contribute to Japan's national interest in line with the policy of Proactive Contribution to Peace based on internationalism.