日本大学大学院総合社会情報研究科紀要　No.14, 001-012 (2013)

サイバー空間の施策に関するロシアと欧米諸国のアプローチ

佐々木　孝博
日本大学大学院総合社会情報研究科

Russia's and Major Western Countries' Approach to the Policy of Security concerning Matters in Cyberspace

SASAKI Takahiro
Nihon University, Graduate School of Social and Cultural Studies

In this article, the author is concerned with the Russia's and the US-Western Europe's approach to constructing an international framework of establishing security and stability (both international and individual) in cyberspace.　In the first place, proceedings of two international conferences - "London Conference" of 2011 and "Budapest Conference" of 2012 - are surveyed in order to see how international cooperation has been going on in the field of cyberspace.　Next, attention is turned to "Draft Convention on International Information Security (Concept)", a document which Russia presented to the United Nations.　What matters here is to note the differences between Russian proposal and the West's proposal, and policy ideas underlying the proposals of the two for international cooperation in cyberspace.　Lastly, what remains to consider is what Russia aims at by leading the way to the establishment of the international framework of defense and security in cyberspace.　In the final analysis, it is made clear that Russia is taking advantage of the differences between the national defense in cyberspace and that in geographical territory, and that all the situations above make "Draft Convention on the International Information Security (Concept)" quite similar in policy ideas to "Strategic Arms Reduction Treaty (START)".

はじめに

サイバー空間での脅威がクローズアップされ、これに対応するための国際協力が重要となってきている。そのような中、ロシアのニコライ・プラトーノヴィッチ・パトルシェフ（Николай Платонович Патрушев）国家安全保障会議書記は、2011 年 9 月 22 日に、52 カ国が参加した「安全保障問題を担当する高官による国際会議（於：エカテリンブルク）」において、国際連合主導の下に「国際情報安全保障条約」を制定すべきとの考えを示した。

これに先立ちロシアは、中国、ウズベキスタン及びタジキスタンと共同して、国連総会に「情報安全保障のための国際行動規範(1)」を提出した。同規範案は、情報空間（サイバー空間(2)）での国際協力の重要性を謳うとともに、同空間における各国の主権の尊重を強調しているところが特徴的であった。

他方で、2001 年に欧州評議会が提案した、サイバー犯罪に関する国際協力を主眼とした「サイバー犯

(1) 国際連合「情報安全保障のための国際行動規範」『国際連合 HP』2011 年 9 月 14 日<http://www.un.org/ga/search/view_doc.asp?symbol=A%2F66%2F359&Lang=E >（2013 年 3 月 27 日アクセス）。

(2) プーチン露大統領は大統領選前の公約とも言える安全保障論文「強くあれ－ロシアの国家安全保障」(『ロシア新聞』2012 年 2 月 20 日）において、「情報空間」と「サイバー空間」をほぼ同義語として使用している。したがって、本稿においては必要に応じ「情報（空間）」と「サイバー（空間）」を併記、または読み替える。

罪条約[3]」には、ロシアは断固として反対している。ここで、「サイバー犯罪条約」の求める国際協力には反対し、「情報安全保障のための国際行動規範」で提案する国際協力は推し進めるという、相反するロシアの施策には如何なる理由が込められているかの疑問が生じてくる。

サイバー空間を巡るこれらのロシアの動きは、一見すると情報安全保障分野における国際的枠組みの実現に主体的に貢献しているとの肯定的な動きにも見える。しかし、実際には、サイバー空間において、他国に先んじて国際的枠組みを設定し、如何に国益を確保するかという視点で、自国の事情を最優先する姿勢が見え隠れしている。

本稿においては、まず、サイバー空間における国際的枠組みの実現を巡る各国・機関の動きを概観する。特に、ここ2年間に活発化してきたサイバー空間における国際協力を討議する2つの国際会議と欧米諸国とは反対の立場で顕著な動きをみせるロシアの動きを考察していく。また、ロシアが政府高官などを活用し、国際会議等において積極的に自国の考えを広めようとする動きを考察する。この中で、ロシアが国連加盟国に提示した「国際情報安全保障条約（案）[4]」を取り上げ、サイバーに関する諸定義、情報安全保障を確保するための原則、情報空間での軍事衝突を回避・解決するための施策及び情報安全保障における国際協力に焦点を当て分析していく。そして、このロシアの提案と欧米諸国が推し進める国際協力との相違を、主としてロシアの立場から考察する。

最後に、これらの考察を踏まえ、国際連合主導の下に「国際情報安全保障条約」の制定を目指すロシアの狙いを、地理的な領土・領海の防衛とサイバー空間の防衛の相違から明らかにする。また、戦略兵器削減条約（START）制定の経緯と国際情報安全保障条約制定に向けたロシアの動き、双方の類似性からも明らかにしていきたい。

1　サイバー空間の国際的枠組みを巡る動き

（1）欧州評議会による「サイバー犯罪条約」の制定

サイバー攻撃は、紛争の一部でもありテロや犯罪でも用いられる国際的な脅威となってきている。国境は関係なく、しかも攻撃源を秘匿して被害を及ぼし得る。そのため、その防止や抑止のためには、緊密なる国際協調の下、迅速かつ的確な情報交換や情報共有の措置をとる必要がある。とりわけ、犯罪として立件するには、デジタル・フォレンジック（電子的な証拠保全）やその捜索に、法的拘束力のある国際文書が不可欠であるとの認識が広がった。

欧州評議会が中心となり、1997年から日米欧はサイバー空間での国際協力を行うための条約策定作業を実施してきた。2001年11月、「サイバー犯罪条約」の条約文が同評議会閣僚委員会において採択された。この中で、「コンピューター・システムに対する違法なアクセス等の行為を犯罪とすること」、「コンピューター・データの迅速な保全、捜索、押収等の手続きを整備すること」、「サイバー犯罪の犯罪人引渡等の国際協力を推進すること」などが謳われた[5]。

本条約は、2004年7月に批准国数の条件を満たし、既に発効済みであり、締約国は、米国、英国、ドイツ、フランスなどの欧米主要国をはじめ37カ国である[6]。我が国においても、2001年に署名後、法整備を進め2012年に効力が発している[7]。

（2）欧米主要国の動き

ア　サイバー空間に関するロンドン会議[8]

(3) 欧州評議会「サイバー犯罪条約」『欧州評議会 HP』2001年11月23日<http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>（2013年3月27日アクセス）。
(4) ロシア外務省「国際情報安全保障条約（案）」『ロシア外務省 HP』2011年9月<http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument>（2013年3月27日アクセス）。
(5) 欧州評議会「サイバー犯罪条約」。
(6) 2012年11月1日現在。
(7) 外務省「告示第231号」『外務省 HP』2012年7月4日<http://www.mofa.go.jp/mofaj/gaiko/treaty/treaty159_4.html>（2013年3月27日アクセス）。
(8) この項、外務省「サイバー空間に関するロンドン会議」『外務省 HP』2011年11月2日<http://www.mofa.go.jp/mofaj/annai/honsho/fuku/yamane/cyber_1111.html>（2013年3月27日アクセス）を参考としている。

2011年11月、「サイバー空間に関するロンドン会議」が開催された。同会議は、英国が主催し、60カ国の政府機関のほか、国際機関、民間セクター、NGO代表など約700名が参加した。会議の中で、インターネットの経済的・社会的恩恵を維持し、また、サイバー空間における犯罪及び安全保障上の脅威から如何に自身を防護すべきかという問題などについて活発な議論が行われた。

会議の冒頭、開催国のウイリアム・ヘーグ（William Haigh）英外相は、「サイバー空間の安定を図るにあたり、基本的人権、特に表現の自由が守られることが重要であり、検閲といった国家による過度な規制は不適切である。また、サイバー空間の発展と安定に向けた取組は、政府、企業、国際機関等が一体となって取り組む必要がある」と述べた。続いて、デーヴィッド・キャメロン（David William Donald Cameron）英首相は、サイバー空間の発展があらゆる地域の人々に対して経済発展の機会を提供することや、サイバー犯罪への対応が世界の国々にとっての喫緊の課題であること、そして、サイバー脅威への安全保障上の対策が必要であることの3点が特に重要だと強調した。

米国代表のジョセフ・バイデン（Joseph Robinette Biden Jr.）副大統領は、「サイバー空間における政府の排他的な権限の行使は、同空間の発展を停滞させ、かつ各国との信頼関係を破壊するものである。既存の国際法の原理・原則はサイバー空間にも適用されるべきである。サイバー空間の安全確保は各国政府のみの取組だけでは困難であり、時間をかけてグローバルな基準や合意を形成する必要がある」と述べた。そのために、「『サイバー犯罪条約』の促進やサイバー空間での信頼醸成措置が重要である」とも言及した。

イ　サイバー空間に関するブダペスト会議(9)

ロンドン会議の1年後の2012年10月、「サイバー空間に関するブダペスト会議」が開催された。同会議は、ロンドン会議のフォローアップ会議としてハンガリーが主催したものである。60カ国の政府機関のほか、20の国際機関、民間セクター、学者、NGO代表など約600名が参加した。会議は、「自由と繁栄のために信頼と安全を」というテーマの下で行われた。その中で、サイバー空間における自由と安全保障の両立、開放性や透明性の重要性、サイバー空間における国際行動規範の確立、「サイバー犯罪条約」の有効性の向上と締約国の拡大、サイバー空間における従来の国際法や国家間関係を律する伝統的な規範の適用、信頼醸成の促進などについて活発な議論が行われた。

会議の冒頭、開催国のマルトニ・ヤーノッシュ（Martonyi János）ハンガリー外相は、「サイバー空間の社会的・経済的側面の潜在力、サイバー空間を使用することの自由やそれにより得られる経済的繁栄とセキュリティ確保のバランス、市民社会と政府との協調・協力、国際機関・地域機関の関与の重要性、サイバー空間での諸課題に対するグローバルな解決・協力、人材育成の必要性」について問題提起した。続いて、オルバーン・ヴィークトル（Orbán Viktor）ハンガリー首相は、サイバー空間が国家の経済成長に欠かせないものであることや、サイバー空間の安全を確保するための国際協力の重要性、自由やセキュリティ確保とプライバシー保護の両立の必要性、「サイバー犯罪条約」の有効性などについて述べた。

前年に引き続き、ヘーグ英外相がスピーチを行い、「サイバー空間は社会的・経済的成長の原動力になっているが、同空間の負の部分に関する議論を積極的に行う時期になった」と指摘し、サイバー空間における国際規範の必要性について言及した。また、その理由として、「サイバー空間における紛争（争い）の可能性が現実性を帯びてきたこと、企業のみならず政府機関をも対象とした組織的なサイバー攻撃がより大きな脅威として現実に発生していること」、そして最も大きな理由として、「経済的脅威や安全保障上の脅威に対処するだけではなく、サイバー空間での開放性や自由を探求する国と国家管理を強めようとする国との意見・行動の相違が高まっていること」を挙げた。

(9) この項、外務省「サイバー空間に関するブダペスト会議」『外務省HP』2012年10月10日<http://www.mofa.go.jp/mofaj/gaiko/soshiki/cyber/cyber_1210.html>（2013年3月27日アクセス）を参考としている。

これは、後述するが、安全保障や治安維持のためにはサイバー空間の国家管理が必要だとする、ロシアや中国を念頭においた発言である。なお、同外相のスピーチは、国家が直接的または間接的に関与するサイバー攻撃（State sponsored cyber attack）や犯罪、国家による表現の自由やプライバシーの侵害、そして、国家の管理・規制について強く批判するなど、前年のロンドン会議よりも踏み込んだ内容であった。また、この発言を後押しするように、キャサリン・アシュトン（Catherine Margaret Ashton）欧州連合（EU）外務・安全保障政策上級代表は、サイバー空間を独裁的な国家体制により国民を抑圧するために使用することについての批判を述べた(10)。

閉会にあたり、議長のマルトニ・ハンガリー外相は、「国連の専門家会合等におけるサイバー空間に関する行動規範作りの議論を評価するとともに、安全かつ回復可能な信頼できるグローバルなデジタル環境を構築するためのアジェンダを設定することが必要である」、「サイバー空間の恩恵の享受と基本的人権へのコミットメントを失うことなく、これらとサイバー空間におけるリスクの最小化との適切なバランスが重要である」との声明を出した。また、「サイバー空間の経済的・社会的便益を認識し、人々の安全とプライバシーを保護する場合を除き、サイバー空間での開放性が確保され続けるべきであること」を強調した。

さらに、同会議において合意できた事項として「サイバー空間の更なる発展のためには開放性が鍵であること」、「国際的な協力が必要であること」、「既存（物理的な空間）の法令や伝統的な規範はサイバー空間でも適用されること」、「継続的かつより包括的な対話が必要であること」などを挙げた。その他、「サイバー空間における表現の自由と結社の自由の重要性、『サイバー犯罪条約』の加盟国拡大、プライバシーとデータ保護の問題における透明性の確保、『サイバー犯罪条約』の価値及び国際協力の拡大」についても一定の合意が得られたとした。

（3）ロシアの動き

ロシアは、サイバー問題で中国と歩調を合わせ、前述のような欧米主要国を中心とした動きに否定的な姿勢を見せている。特に「サイバー犯罪条約」の締結には反対の立場から、サイバー犯罪対策に関する条約は、欧州評議会が主導して国際秩序を設定するのではなく、国連において策定すべきだとの主張を行っている。また、欧州評議会で採択された同条約では時代遅れで、サイバーテロや新たな手口でのサイバー犯罪には対応できないとしている。さらに、「相互援助のために、自国にあるコンピューターから他国にあるコンピューターにアクセスすることができる」とした本条約を受け入れることはできないと強く反対の立場をとっている。これは、後述するが、サイバー空間における内政干渉につながるものとロシアと中国は捉えて、自国の安全保障の根幹にも関わる問題として強く反対していることによる。

「サイバー犯罪条約」に反対するだけでなく、ロシアと中国は、次々と政策レベルでの動きを活発化させている。この動きは、特にここ3～4年に顕著になってきている。2009年には、露中両国が加盟する上海協力機構（SCO）において、「国際情報安全保障の政府間協力協定」に署名し、露中両国とこの問題において歩調を同じくする国家間グループの拡大を図った。

その後、前述のように、露中両国は2011年9月には国連総会に対し「情報安全保障のための国際行動規範」を提出した。同規範案において、国家によるサイバー空間での主権管轄（国家によるサイバー空間における権利や自由の管理）、サイバー兵器や関連技術の規制、サイバー空間における資源の公平な配分などを主張している。

その1か月後の2011年10月、ロシアは、冒頭に述べた「国際情報安全保障条約（案）」を国連加盟各国に提示した。その後もあらゆる国際場裡において、同条約案を含むロシアの主張をまとめた2分冊

(10) アシュトンEU上級代表の発言は、特定の国家を名指ししたものではなかった。だが、ヘーグ英外相のスピーチがサイバー空間の国家管理を強めようとしているロシア及び中国を念頭に行ったものであったことから、同様に、同国等を念頭にした行き過ぎた国家管理に対する警鐘的意味合いで行った発言と考えられている。

の本[11]（ロシア語、英語双方で記述）を各国代表団に配布し、ロシアの主張の拡大を図っている。

また、前述のブタペスト会議においては、ロシアや中国の参加者は、会議全般を通じて、サイバー空間での国家主権の尊重や規制実施の必要性を強調した。さらに、人権を議論の焦点にすることに疑問を呈するとともに、前述の「情報安全保障のための国際行動規範」を規範作りのたたき台とすべきであるという主張を繰り返し行った。

2　国際情報安全保障に関するロシアの基本的な立場

ロシアは、国際情報安全保障に関する自国の主張を広めるために様々な国際会議の場を活用している。その一環として、2012 年 10 月 30 日の東海大学・モスクワ国立大学共催「国際情報安全保障シンポジウム（於：東京）[12]」において、ロシア側代表団長ウラジースラフ・ペトローヴィッチ・シェルスチュク（Владислав Петрович Шерстюк）国家安全保障会議書記補佐官兼モスクワ国立大学情報安全保障問題研究所所長[13]は、「国際情報安全保障－ロシアのイニシアティブ－」との表題で発表し、ロシアの主張を詳細に述べた。その中で、同問題に関するロシアの基本的な立場は、2 つの政治的な文書「ロシア連邦情報安全保障ドクトリン[14]」及び「ロシア連邦における情報社会発展戦略[15]」に示されていると強調した。また、欧州評議会が主導する「サイバー犯罪条約」になぜロシアは反対しているのか、さらに「情報安全保障のための国際行動規範」や「国際情報安全保障条約」の制定をなぜ推し進めるのかなどの理由にも言及した。

（1）欧州評議会による「サイバー犯罪条約」への反発

シェルスチュク補佐官は、欧州評議会が採択した「サイバー犯罪条約」にロシアが同意できない理由を 2 つ述べた。

まず、同条約の第 32 条 b 項を引用し、「『一方は他の一方の同意なしに、他の一方の領土内に存在するコンピューター・データにアクセスする権利を有する』の条項は、欧州安全保障協力会議の基本原則『主権の平等、主権がもつ固有の権利』に反している」とした。また、この条項では、「コンピューター犯罪の危険性を軽減させる一方で、コンピューターテロや情報通信技術の『侵略的な利用』を増長する」との理由で同意できないと強く反発した[16]。

ロシアが反発する「サイバー犯罪条約」第 32 条は、「蔵置されたコンピューター・データ（Stored computer data）に対する国境を越えるアクセス（当該アクセスが同意に基づく場合又は当該データが公に利用可能な場合）」を規定する条項である。その内容を「締約国は、他の締約国の許可なしに、次のことを行うことができる。 a 項：公に利用可能な蔵置されたコンピューター・データにアクセスすること（当該データが地理的に所在する場所の如何を問わない）。b 項：自国の領域内にあるコンピューター・システムを通じて、他の締約国に所在する蔵置されたコンピューター・データにアクセスし又はこ

(11) 2 冊の本の題名は、「International Information Security: Problems and Decisions」及び「The International Legal Instruments and Documents on International Information Security」である。
(12) 同シンポジウムにおいて、筆者は日本側プレゼンターとして「米国、ロシアのサイバー戦略」について発表し、シェルスチュク国家安全保障会議書記補佐官はじめロシア代表団と意見交換した <http://www.u-tokai.ac.jp/TKDCMS/News/Detail.aspx?code=news&id=5805> (2013 年 2 月 23 日アクセス)。
(13) 同氏は、プーチン大統領が安全保障会議書記を務めていた際、同第 1 副書記として活躍、それ以前には通信傍受を任務とする連邦政府通信情報局（FAPSI）の局長を務めたロシア政府内のサイバー問題の第 1 人者である。なお、シンポジウム参加時には既に安保会議書記補佐官職を離れていたとの情報もあるが、同氏の使用した発表資料で同職の肩書を使用していたため、本稿では同職にあったものとして記述する。
(14) ロシア安全保障会議「情報安全保障ドクトリン」『ロシア安全保障会議 HP』2000 年 9 月 9 日<http://www.scrf.gov.ru/documents/5.html>（2013 年 3 月 27 日アクセス）。
(15) ロシア安全保障会議「情報社会発展戦略」『ロシア安全保障会議 HP』2008 年 2 月 7 日<http://www.scrf.gov.ru/documents/90.html>（2013 年 3 月 27 日アクセス）。
(16) 東海大学におけるシンポジウムでのシェルスチュク補佐官の発言。

れを受領すること。ただし、コンピューター・システムを通じて当該データを自国に開示する正当な権限を有する者の合法的なかつ任意の同意が得られる場合に限る」と定めた(17)。

前者は、ごく当たり前のことであり、後者は、グローバル企業の本社と外国所在の支社などを連接するネットワーク・システムでのアクセスを想定したものである。

このうちロシアはb項に疑義を唱えている。ロシアは例えば次のような事例を危惧していると考えられる。

第1は、A国に本社をもつB社があるとする。そして、B本社とロシア国内のB支社との間でコンピューター・システムを構築している場合を想定する。この状況下において、本条約を適用すると、A国側からA国所在のB本社システムを利用し、ロシア所在のB支社システムにアクセスすることにより、そこを通じて、ロシア国内に対し悪意のある行為（犯罪、テロ、情報活動をはじめとするサイバー攻撃）をすることが可能になってしまう。つまり、「侵略的な利用」を増長してしまうのではないかということである。

第2は、その反対に、ロシア所在のB支社システムを利用し、A国所在のB本社のシステムを通じてA国に対し、悪意のある行為がなされた場合、ロシア側の同意なしに、A国のB本社におけるアクセス権限を有する者の同意が得られれば、A国官憲によるロシア国内の調査・捜査が可能になってしまう。そうなると、地理的な領土・領海の概念に当てはめれば、主権の侵害にもつながり、なし崩し的に安全保障の根幹にも影響が及ぶことも考えられる。そのため、ロシアは本条項に否定的なのである。

(2)「情報安全保障のための国際行動規範」の推進

他方で、ロシアは情報安全保障における国際協力の発展を支持する姿勢も打ち出している。特に、同協力を規定する国際的枠組みを実現するには、国連加盟国すべてが採択する多国間協定に立脚すべきであると主張している。そのような見地から、ロシアをはじめとする中国、タジキスタン及びウズベキスタンの4カ国は、国連事務総長宛に「情報安全保障のための国際行動規範」を提出した。

同規範案では、加盟各国に対し自発的に次のような義務を負うことを規定している。第1は、国連憲章にもある、主権の尊重、領土の保全、すべての国家の政治的独立性、人権及び基本的自由の尊重、並びにすべての国の歴史、文化及び社会制度の多様性を尊重すること。第2は、敵対行為を実施するために情報通信技術を使用しないこと。第3は、情報通信技術を使った犯罪またはテロ行為に対する戦いで協力すること。第4は、自国の法律に従って、情報を探索、入手、伝達及び伝搬する権利と自由を含め、情報空間における権利と自由を完全に尊重すること。

ここで、第1と第4の規定を取り上げたい。

第1の規定において、情報空間（サイバー空間）の「主権の尊重」及び「領土の保全」を強調している。グローバルなサイバー空間では「主権の尊重」と「領土の保全」との間でどのようにバランスをとればよいのか国際的な議論となっている。例えば、我が国所在の外国企業の支社がサイバー攻撃のターゲットになり、安全保障上重要な情報が窃取される場合を考える。この事例は、我が国に対する攻撃なのか、その会社の旗国への攻撃なのか、どのように扱えばよいのか国際的な合意がなされていない点である。また、前述の「サイバー犯罪条約」第32条の規定は、解釈によっては「主権の尊重」や「領土の保全」を一部制限しているようにも受け取れる。従来の地理的な領土・領海の概念が全く当てはまらない領域がサイバー空間であるとも解釈できる。そのような中、ロシアは、従来の領土・領海及びそれを基準とする主権の概念をサイバー空間にも適用しようとしている。

第4の規定においては、情報空間における権利と自由を完全に尊重するとある。だが、「自国の法律に従って....」と前提条件を被せ、自国の法律による制限の余地を残している。これは、後述する「国際情報安全保障条約（案）」において、情報空間における情報交換の自由を謳う一方、同空間は治安・安全保障のためには国家が管理すべき領域との但し書きの付記につながっている。

(17) 欧州評議会「サイバー犯罪条約」。

(3)「国際情報安全保障条約（案)」の提案

「情報安全保障のための国際行動規範」の提案の後ロシアは、国連加盟各国に対し、「国際情報安全保障条約（案)」を提示した。同文書は、シェルスチュク安保会議書記補佐官によれば、同氏が主導し、兼務するモスクワ国立大学情報安全保障問題研究所の支援を得てまとめあげたものである。彼によれば、本条約において、ロシアがもつ国際情報安全保障枠組みに対する基本的な立場を示しているとのこと。ここでは、同補佐官が強調した「情報空間における情報交換の自由」について取り上げたい。

ロシアがこの問題を取り上げる際の根拠概念は、彼によれば、「市民的及び政治的権利に関する国際規約」（1966 年 12 月 16 日付、国連決議 2200A[XXI]）第 19 条である。同条第 2 項に「すべてのものは表現の自由についての権利を有する。...（中略）... 国境との関わりなく、あらゆる種類の情報及び考えを求め、受け及び伝える自由を含む」とある。第 3 項に但し書きとして「本条第 2 項に定める権利の行使には、特別の義務及び責任を伴う。したがって、この権利の行使については、一定の制限を課すことができる。ただし、その制限は法律によって定められ、かつ、次の目的のために必要とされるものに限る。(a) 他の者の権利及び信用の尊重、(b) 国の安全、公共の秩序または公衆の健康もしくは道徳の保護」とある(18)。彼によれば、ロシアはこの条項を情報空間における情報交換の自由にも適用させようとしているのである。この背景には、ロシアが国家としてコントロールできない領域において情報交換がなされることは国家安全保障上重大な影響があると捉えていることがある。つまり、アラブ諸国において、SNS（ソーシャル・ネットワーキング・サービス）を使って、いわゆる「アラブの春」が生起し、時の政権が崩壊した事実を非常に深刻に受け止めたからである。

国際情報安全保障に関するロシアの基本的な立場において一貫しているのは、情報空間というものは自由な空間ではあるものの、安全保障や治安維持を理由として国家の管理下に置くべき領域であるということである。そして、それを具現化するための国際的枠組みの実現が、ロシアの国益に適うという強い姿勢である。そのために、「国際情報安全保障条約（案)」を提案したのである。

3　ロシアの提案する「国際情報安全保障条約（案)」の内容

(1) 条約案の構成

ロシアが国連加盟国に提示した「国際情報安全保障条約（案)」は 5 つの章から成る。

第 1 章の「主節」は、本条約の主題と目的、用語の定義、本条約の適用除外、情報空間における脅威、情報安全保障を確保するための原則などである。

第 2 章は「情報空間における軍事衝突を回避及び解決するための主な施策」である。

第 3 章は「テロ目的での情報空間の使用を防止する主な施策」である。

第 4 章は「情報空間における違法行為を阻止するための主な施策」である。

第 5 章では「国際情報安全保障分野における国際協力」について言及している。

(2) サイバー関連用語の定義

本条約案の冒頭で、サイバー関連の用語を定義している。主たる定義は、2011 年にロシア国防省が発表した「情報空間におけるロシア軍の活動に関するコンセプト(19)」の定義とほぼ同じである。ロシアが示す複数の公文書での定義に齟齬がないことから、国家としてのサイバー問題の定義や解釈は、ほぼ確定したものと考えられる。それを国際社会に認知させたいとの思惑が見られる。主な定義の内容は次のとおりである。

(18) 国際連合「市民的及び政治的権利に関する国際規約」『国際連合 HP』1966 年 12 月 16 日 <http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en>（2013 年 3 月 27 日アクセス)。

(19) ロシア国防省「情報空間におけるロシア軍の活動に関するコンセプト」『ロシア国防省 HP』2011 年<http://www.ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle&_print>(2013 年 3 月 27 日アクセス)。

①「情報保全」: 国家、社会及び個人的な利益が、情報空間における破壊的な行為や否定的な行動による脅威に対して防護されている状態

②「情報戦」: 情報システム、情報プロセス及び情報資源、その他の重要インフラの破壊を目的とした情報空間における 2 国以上の国家間紛争（争い）

③「情報インフラ」: 情報の収集、作成、処理、伝達､使用及び保管のために使用される技術的手段(ツール）やシステム

④「情報兵器」: 情報戦での使用を目的とする情報技術、技術的手段（ツール）及び方法

⑤「情報空間」: 個人と社会、情報インフラと情報自体に影響を与えるような情報の収集､作成､処理、伝達、使用及び保管に関連する活動の空間

⑥「情報資源」: 情報インフラだけでなく、情報自体とその情報の流れ

⑦「国際的な情報安全保障」: 情報分野において世界の安定や国家の安全保障を阻害するような脅威を排除できる国際関係の状態

⑧「情報空間における違法行為」: 情報空間において、違法目的のために情報資源に影響を与える行為

⑨「情報空間におけるテロ行為」: 情報空間において、テロ目的のために情報資源に影響を与える行為

⑩「情報空間への脅威」:情報空間において､国家、社会、個人の利益に危険を及ぼす要因

この中で「情報戦」の定義を取り上げたい。情報戦を、情報空間におけるテロや犯罪と捉えているのではなく、2 国以上の国家間の紛争と捉えている点である。ロシアは情報空間における最大の脅威を国家間紛争としているのである。以後の本条約の記述も国家を主体とした考え方が続く。つまり、情報空間におけるロシアの主眼が、非国家主体のサイバーテロやサイバー犯罪よりは、国家主体による情報戦（サイバー戦）を最も脅威と考えていることがこれらの記述から分かる。

(3) 国際情報安全保障を確保するための原則

本条約案第 5 条の国際的な情報安全保障の基本原則において、「情報空間は公共的な領域（パブリック・ドメイン）であり、その安全保障は世界の文明の持続的発展のための基盤を作るものである」と総論的には情報空間を誰もが利用できるパブリック・ドメインと位置付けた。

しかし、同条第 5 項に「締約国は、主権的な規範を定めており、国の法律に従って、情報空間を管理する権利を与えられる。その主権や法律は、締約国の領域内に配置される情報インフラに適用される。また、締約国は、国内法と信頼性・安全性の高い情報空間を構築するための道筋への障害がないように両者を調和することに努力しなければならない」と付言し､ネットワーク主権の概念を打ち出している。この条項によって、国家は国内法によりその国家の領域内にある情報インフラを管理する権利を有するということを定めた。そして、このネットワーク主権の考え方の行間には、ネットワーク分野における他国の介入を回避するための枠組み作りという本質が隠れている。

また、同条第 2 項においては、情報安全保障不可分の原則を打ち出している。「締約国は、国際的な情報安全保障体制を形成しながら、他の国すべての安全保障と切り離せないことに留意する必要がある」とした点である。すなわち､「締約国は、他の国の安全保障を犠牲にして、情報空間におけるセキュリティを強化することはしない」ということを強調している。この条項はサイバー能力の高い国が突出してその情報優越の体制を構築し、他の能力の低い国が不利益を被らないようにするための対抗措置である。これをロシアが持ち出す背景としては、欧米主要国が強大なサイバー監視・防護体制を構築してしまった場合、ロシアは自国の情報優越を十分に確保できず、情報安全保障上不利な状況に落ち入ってしまうことが挙げられる。これを危惧した条項である。

これに類似した考え方は、戦略核戦力とミサイル防衛に関する問題を議論するときにロシアが必ず持ち出す理論である(20)。ロシアは、情報空間においても同様の国際的枠組みを作り上げたいとの考えの下

(20) ロシアは、米国がグローバルなミサイル防衛網を構築してしまった場合、核抑止理論の根本である戦略核戦力の均衡が崩れるということを危惧している。そのため、戦略核戦力とミサイル防衛問題は不可分であると主張している。

に、このような提案を打ち出してきたのである。

(4) 情報空間での軍事衝突を回避・解決するための施策

本条約案第 6 条の情報空間での軍事衝突を回避する施策において、「締約国は、情報空間において平和的に危機や紛争を解決するために共同行動を採らなければならない」として、国際協力の重要性を謳った。特に、同条第 5 項では「他国の内政に干渉するために情報通信技術の使用を控える」、第 6 項では「他国を脅したり、紛争を解決するための手段として他国の情報空間に対しての力の行使は控える」とある。この 2 項目は、軍事衝突を回避する手段として物理的な軍事力にも当てはまるもっともな記述である。ロシアが自国向けにサイバー兵器が使用されることを恐れ、それを防止するための国際的枠組みとして、最も訴えたい項目と捉えることができる。

また、本条約案第 7 条においては、情報空間での軍事紛争を解決するための措置について規定している。第 1 項では「締約国は、交渉、調査、調停、和解、仲裁裁判所の裁判、地域機関や協定へ提訴することにより、情報空間における軍事紛争を解決する」、第 2 項では「いかなる国際紛争においても、『情報戦』の手段を選択するような紛争に関与している締約国の権利は、国際人道法により制限される」とある。これも、紛争を解決するための一義的な手段としてはもっともな手段である。だが、ロシアが敢えてこの条項を打ち出した背景には、国家間の争いが情報戦のレベルにまで激化した場合、ロシアのサイバー防護能力だけでは対処できないのではないかという欧米主要国に対する脅威感がある。

(5) 情報安全保障における国際協力

本条約案第 13 条は、情報空間の軍事利用の分野における信頼醸成措置についてである。第 1 項において、「締約国は、情報空間における国家安全保障コンセプトを（互いに）交換すること」、第 2 項で「締約国は、情報空間における危機的な事例や脅威、及びそれらの解決や安定化のためにとられた措置について適時に交換すること」、第 3 項で「締約国は、軍事的性質の紛争を解決する際の当事者間の懸念や協力を呼び起こすような情報空間における活動について協議すること」の 3 つを規定している。

ロシアが信頼醸成のために敢えてこのような 3 つのことを提示した背景には、欧米主要国や本問題で歩調を合わせる中国など、サイバー能力の高い国の情報戦略を把握できていないことがある。そのため、信頼醸成の名目で何とかこの種の情報を得て、自己のサイバー防護に活用したいと考えているのである。

これら 3 つの規定は、ロシア国防省が定めた「情報空間におけるロシア軍の活動に関するコンセプト」でも、ほぼ同じ条文が謳われている(21)。国内向けの公文書及び国際社会向けの公文書ともにほぼ同じ記述があることから、ロシアが情報空間において、他国の情勢が把握できないことに非常に危機感を持っていることが分かる。

4　サイバー空間の施策に関するロシアと欧米諸国の相違

(1) 自由な空間としてのサイバー空間と国家の管理・統制

これまで述べてきたように情報空間（サイバー空間）の問題に関し、ロシアと欧米主要国との間で大きな対立点となっているのは、サイバー空間を自由な空間として扱うべきか、国家が管理する空間として扱うべきかの問題である。

サイバー空間に関する 2 つの国際会議、すなわち 2011 年の「ロンドン会議」と 2012 年の「ブダペスト会議」においても大きな論点であったのがこの問題である。前述したように、ロシアの主張については、東海大学・モスクワ国立大学共催のシンポジウムにおいてロシア側シェルスチュク安保会議書記補佐官の発言により明らかになった。

その中で、同補佐官が特に強調していたのは、「情報安全保障のための国際行動規範」や「国際情報安全保障条約（案）」の条文を引用し、情報空間においては国家の安全保障及び治安維持のためには、自由

(21) 拙稿「ロシアのサイバー戦略－『サイバー戦コンセプト』を中心に－」『日本大学大学院総合社会情報研究科紀要第 13 号』電子紀要版、2012 年 7 月 1 日<http://atlantic2.gssc.nihon-u.ac.jp/kiyou/pdf13/13-001-012-Sasaki.pdf>（2013 年 4 月 30 日アクセス）。

な空間たる情報空間を如何に国家が管理していくべきかということであった。

（2）情報セキュリティとコンテンツのセキュリティ

今 1 つ、ロシアと欧米主要国との間で大きく解釈が異なっているのが、情報セキュリティとコンテンツ（サイバー空間を行き交う中身）のセキュリティの問題である。

シェルスチュク補佐官によれば、ロシアは情報セキュリティとサイバーセキュリティを分別して考えている。すなわち、サイバーセキュリティとは情報空間（サイバー空間）そのものにおけるセキュリティのことであり、同空間を使用するネットワークやコンピューター・システムそのもののセキュリティと考えている。それに加え、情報セキュリティの用語を使用した場合には、その空間を行き交うコンテンツのセキュリティをも含むと捉えている。この考えは、欧米主要国の考えと対立しており、欧米主要国では、コンテンツのセキュリティは通信の秘密の保護や個人情報の保護などの観点から、情報セキュリティの対象外としている。

ロシアがこれを持ち出す狙いは、ネットワークやシステムのセキュリティだけでなくコンテンツのセキュリティも国家により管理しないと、国家の安全は担保できないと考えていることにある。この考えは、前述したサイバー空間を自由な空間と捉えるか、国家が管理・統制すべき空間と捉えるかの議論にリンクしている。

（3）紛争解決のためのサイバー空間の不使用

ロシアは「国際情報安全保障条約（案）」において、紛争解決のためのサイバー空間の不使用を掲げている。これを持ち出したロシアの狙いは、どの国に対しても紛争解決のためのサイバー攻撃を封じることにある。自国のサイバー防護体制がままならない中、如何に国外からのサイバー脅威を低減できるかの見地から、サイバー兵器を核兵器、生物・化学兵器等と同様に軍備管理の対象にし、国際的枠組みで制限（または禁止に）することが、国益に合致していると考えたからである。ただし、攻撃者を断定できないサイバー攻撃においては、核兵器や生物・化学兵器のような抑止は限定的にならざるを得ない(22)。特に懲罰的抑止が効かず、他の兵器と同様な軍備管理の理論が当てはまらないため、紛争そのものへのサイバー兵器の使用を禁止する国際的枠組みがあれば、サイバー脅威を低減できると考えたのである。

（4）サイバー空間を利用する不正規軍の組織編成の制限

さらにロシアは、サイバー空間を利用する不正規軍の組織編成の制限にまで「国際情報安全保障条約（案）」で言及している。同条約案第 6 条第 7 項において、「他国の情報空間において違法な活動を実施する目的をもつ如何なる不正規軍（Irregular Forces）の組織編成とその奨励を控えること」とした。

サイバー攻撃は、物理的な攻撃と異なり、大部隊の軍隊や組織、それに付随するような装備は必要ない。ごく少数の能力のある者を不正規軍として秘密裏に行動させることで、国家インフラそのものを麻痺させたり、敵の軍事作戦そのものを遂行不能にもできる。

他方で、不正規軍の活動については、既に「侵略の定義に関する国連総会決議（1974 年 12 月 14 日付、国連決議 3314[XXIX]）」において、「他国に対して武力行為を行う不正規兵（Irregulars）または傭兵の使用を国際的な非行（International Delinquency）である」と認定している(23)。ロシアが敢えてサイバー空間においてもこれを取り上げる理由は、欧米主要国が秘密裏にロシアに対し不正規軍を用いたサイバー攻撃を行うのではないかという脅威感からきている(24)。

---

(22) James A. Lewis, Conflict and Negotiation in Cyberspace, Center for Strategic and International Studies (CSIS), Feb 2013 及び 2013 年 1 月 29 日筆者と同氏の意見交換（於：CSIS）における同氏の発言。

(23) 国際連合「侵略の定義に関する国連総会決議」『国際連合 HP』1974 年 12 月 14 日<http://untreaty.un.org/cod/avl/ha/da/da.html＞（2013 年 4 月 14 日アクセス）。

(24) モスクワ国立大学情報安全保障問題研究所と英国紛争学研究センターの共同報告「Russia's "Draft Convention on International Information Security"-A Commentary」において、ロシア側は「国家というものは情報空間における不正規軍の秘密使用を断念しようとしないことを認識しなければならない」と本条項を

したがって、この条項は、サイバー空間の国際的な安定のために、ロシアが主体的に不正規軍に関する軍備管理を推し進めようという考えに基づくものではない。ロシアが欧米主要国のもつサイバー攻撃能力を封じるために、前項同様に国際的枠組みを設定することで不正規軍を用いたサイバー攻撃行為そのものに足枷をかけたいとの考えに基づくものである。

（5）物理的な領域の防衛とサイバー空間の防衛

サイバー空間というものは、米国が主張するように、物理的な陸・海・空及び宇宙に次ぐ第5の領域（ドメイン）ではあるものの、全く同じようには扱えない人工の領域である。物理的な領域には、国家成立の根幹たる領土・領海の概念とそれを基盤とする国家主権の概念というものが確立している。その概念に基づきロシアは、自国の安全を確保するために、従来から勢力圏というものを拡大する政策を採ってきた(25)。しかしながら、サイバー空間ではそれらの概念の適用が困難で、国際合意も確立していないため、勢力圏を拡大することによって、自国の安全を確保するといった政策は採れない。

サイバー空間が物理的な領域と同等に扱えないという具体例としては、前述したように、グローバル化した情報社会故の問題がある。さらに、前述と異なる例を挙げれば、サイバー攻撃の1つの形態に分散型サービス拒否攻撃（DDoS 攻撃(26)）というものがある。攻撃に利用するコンピューターは自分のコンピューターを使うことはなく世界各地の乗っ取ったコンピューターを利用することが多い。そのような状況では、攻撃が例えばA国所在のコンピューターから行われ、B国所在のコンピューターを乗っ取ってC国に対して行われた場合、被攻撃側のC国では、通常B国から攻撃が行われたことしか分からない。その場合攻撃国はB国なのかということである。

「サイバー空間に関するロンドン会議」や「ブダペスト会議」をはじめあらゆる国際会議においてもこれらの問題は討議されているが、どのように取り扱えばよいのか結論には至っていない。各国は自国の都合のいいように本件を解釈している。

ロシアは、地理的にロシア国内にある情報空間及びその中を行き交うコンテンツは国家の管理下に置くべきとの立場を明らかにしている。ロシア領内にある情報空間はロシアの主権により管轄する領域と考えているのである。国家の管理下に置くべきか否かについては、前述のように、情報空間の自由を第1に掲げる欧米主要国と対立している。

（6）戦略兵器削減条約（START）と国際情報安全保障条約の類似性

ロシアが情報安全保障に関する国際的枠組みの実現やサイバー兵器の軍備管理に力を注ぐ様子は、戦略兵器削減条約（START）や欧州安全保障条約(27)の交渉において、ロシアに有利な形での安全保障秩序を目指す姿と重なる。

すなわち、物理的な軍備管理の世界においてロシアは、STARTで戦略核の弾頭数や運搬手段数の上限を定め、米国がロシアの核戦力を上回ることのないようにくさびを打った。中距離核戦力（INF）についても米露双方が全廃することにより米国の中距離核戦力の脅威を排除した。ミサイル防衛問題については現在如何に有利な形で米国に制限をかけるか交渉中である。

また、軍備管理の各種条約により脅威の軽減を図るとともに、安全保障枠組み全般を国際社会に見直させ、ロシアに有利になるような枠組みの再構築を

設けた理由を説明している< http://www.conflictstudies.org.uk/files/20120426_CSRC_IISI_Commentary.pdf >（2013年4月14日アクセス）。

(25) ソ連時代には国境の外側にワルシャワ条約機構（WTO）加盟国などを、また、ソ連崩壊後も独立国家共同体（CIS）諸国などを「特権的利害地域」と位置づけ、国境の外側に勢力圏を確保する政策を採ってきた。

(26) DDoS（Distributed Denial of Service）攻撃とは、分散された複数のコンピューターから、サーバーに大量のデータを送って多大な負担をかけ、機能停止に追い込むサイバー攻撃法。

(27) ロシア外務省「ラブロフ露外相のOSCE年次会合開始時の安全保障分野の課題に関するステートメント」『ロシア外務省HP』2009年6月23日<http://www.mid.ru/brp_4.nsf/2fee282eb6df40e643256999005e6e8c/aded9c34ee795d2bc32575de003decd1?OpenDocument>（2013年3月27日アクセス）。

目指している。具体的には、「欧州安全保障条約」を締結し、締結国間における領土の不可侵など、安全保障の根幹にかかわる原則を決定できる枠組みの実現を目指している。それによって、欧米主要国の脅威を削減できると考えたのである(28)。

この動きと、近年の情報空間における国際的枠組みの実現を主導しようとするロシアの動きとを比較すると、非常に類似していることが分かる。

まず「情報安全保障のための国際行動規範」を制定することにより、情報通信技術やサイバー技術を使った敵対行為の禁止を目指している。サイバー攻撃というものは如何にその防護能力を高めても、100%防護することは不可能である。そうであるならば、サイバー兵器を使用した敵対行為そのものを禁止する国際行動規範を設定できれば脅威は低減できるということである。

また、「国際情報安全保障条約」を制定することにより、欧米主要国の一般的な考え方である「情報空間は自由な空間」という概念に制限を設け、「国家が管理、監視できる領域（情報空間を行き交うコンテンツを 24 時間監視できること）」との国際合意を達成しようとしている。この背景には、情報空間を国家が管理できなければロシアの安全は保てないとの危機感がある。したがって、ロシアは国際的枠組みを自国に有利な形で実現できればサイバー分野においても安全を確保できると考えたのである。

おわりに

サイバー空間というものは、陸・海・空及び宇宙と並ぶ第 5 の領域（ドメイン）であるとともに、地理的な領土・領海とは異なり、主権の概念や安全保障のために自己の勢力圏を拡大するという概念が適用できない領域である。ロシアは、ソ連時代には国境の外側にワルシャワ条約機構（WTO）加盟国や友好国などを勢力圏として確保し、また、ソ連崩壊後も独立国家共同体（CIS）諸国などを「特権的利害地域」と位置づけ、国境の外側に勢力圏を確保することで自国の安全をより確実なものにしてきた。だが、領土・領海と同様の施策を適用できないのが、サイバー空間での戦いであり、サイバー兵器の特性である。

そのような情勢下、ロシアは、「国際情報安全保障条約」の制定を訴え、表面上、サイバー空間における軍備管理や信頼醸成措置を推し進め、国際貢献に積極的な関与をしていく姿勢を強く示した。この動きは、国際的なサイバー空間での戦いを防止し、国際協力に貢献するなどといった非現実主義的な考えに基づくものではない。

その狙いは、サイバー空間における他国の脅威（主として欧米主要国及び本問題で同調する中国をも念頭）を自己の情報通信技術の向上のみによって抑えきれないため、同条約により、ロシアにとっての不利益な行動を封じることにある。

この考えは、戦略核兵器における技術や財源に劣ることから、戦略兵器削減条約（START）、中距離核兵器（INF）全廃条約、ミサイル防衛問題への対応などを推し進め、米国の脅威を抑える施策を採用し、米国との対等を目指した経緯と類似している。また、欧州安全保障条約の提案のように、安全保障分野全般にわたる国際的枠組みをロシアに有利に導こうとしている動きにも類似している。

このような類似性からロシアが物理的な空間における脅威とサイバー空間における脅威を同等に扱っているのは明らかである。欧米主要国に比してサイバー防護技術に劣り、財源も限定されているロシアは、それをどう切り抜けるか、どう対等であろうとするのかという見地で、サイバー空間における国際的な枠組み作りを主導しようとしているのである。

(Received:May 31,2013)
(Issued in internet Edition:July 1,2013)

(28) 拙稿「ロシアの目指す国際的な安全保障秩序」『日本大学大学院総合社会情報研究科紀要第 11 号』電子紀要版、2010 年 7 月 1 日< http://atlantic2.gssc.nihon-u.ac.jp/kiyou/pdf11/11-001-013-Sasaki.pdf>（2013 年 5 月 10 日アクセス）。