Strategic Peace and International Affairs Reserch Institute, Tokai University
Booklet Vol.1

特集

「グローバルパラダイムシフトとサイバーセキュリティーダイアローグ」

First issue : Cyber Security Dialogue in Global Paradigm Shift

東海大学平和戦略国際研究所 編

創刊号

目次

創刊にそえて

2017年12月1日、東海大学建学75周年記念サイバーセキュリティーシンポジウムが、東海大学平和戦略国際研究所とモスクワ国立大学情報安全保障問題研究所の共催で開催され、日本政府から、サイバーセキュリティー戦略の最高責任者である菅義偉内閣官房長官、外務省の大鷹正人総合政策局審議官兼サイバー政策担当大使、NISC・内閣サイバーセキュリティーセンターの三角育生副センター長兼内閣審議官が出席。ロシア側から、会議冒頭にエフゲニー・アファナーシエフ駐日ロシア大使よりご挨拶を頂きました。モスクワ国立大学情報安全保障問題研究所所長で、ロシア連邦「安全保障会議」顧問のヴラディスラヴP.シェルステュク氏、副所長のアナトリー・ストレルツォフ氏らが出席しました。また、サイバー先進国の英国からIISS・英国国際戦略研究所のロシア担当オフィサーが参加予定でしたが、直前に体調を崩したため、急遽、デヴィッド・エリス駐日英国大使館首席公使が出席してシンポジウム冒頭でスピーチを行ないました。サイバーセキュリティーの分野で長い研究実績のあるモスクワ国立大学情報安全保障問題研究所に比べ、研究に取り組み始めたばかりの東海大学平和戦略国際研究所の補助役として、モスクワ滞在経験の長いイギリスのインテリジェンスオフィサーの参加によりサイバーセキュリティー問題への両研究所の「取り組みの視点」の相違点を明らかにしたいと考えたもので、緊張関係にあるロシアとイギリスの両国関係の中で、日・ロ・英3カ国によるシンポジウムという基本構想を前向きに受け止めていただいたモスクワ国立大学情報安全保障問題研究所の研究機関としての基本姿勢に対し改めて敬意を表したいと思います。

東西冷戦下で情報交流の乏しかった日本とロシア(旧ソ連邦)、東ヨーロッパ各国の大学、研究機関との交流に力を注いだ東海大学創立者松前重義博士が創設した平和戦略国際研究所の向かうべき道標をそこに見る気がします。シンポジウムの最後にシェルステュク所長から山田清志学長に対してサイバーセキュリティーに関する提言書『国際条約草案の構想～インターネットの安全な機能と発展の構想』が手渡しされました。提言では―「インターネットを国連憲章に反する目的で使用することを防止するため、国際社会の努力を結集することの必要性を認識」し、「標準、技術、および通信ネットワークの発展の責任を負う国家、世界的なICT企業、会社の相互関係および役割を調和させる、新しい国際協定の必要性を認識する」「いかなる単一国家または国家群も、インターネット機能に干渉し、独自の裁量でインターネットの規範や規則を定め、社会を監視し、外国の世論を操作し、または主権国家の状況を不安定にさせる権利がないことを強調する」と記されています。大学付属の研究機関からの提言ですが、シンポジウムでモデレーターをお願いした元NHKモスクワ支局長の石川一洋氏は、ロシアでは安全保障に関わる戦略、ドクトリンはすべて「安全保障会議」が取りまとめる。その「安全保障会議」に大きな影響力を持つモスクワ国立大学情報安全保障問題研究所がシンポジウムに参加し提言を行なった意義を強調されています。

シンポジウムの議論を通じて、日本とロシア両国間で考え方の違いが改めて明らかになったのは「主権国家」概念の違いでした。この点について石川氏はブックレットへの寄稿の中で「ロシアにおける安全保障には、軍事や政治経済的なものだけでなく、文化や歴史伝統、教育や科学、環境なども含まれる。こうしたロシアの考え方からすると世界の中での「真の主権国家」はそう多くない。EUに政治経済的主権を譲り渡したヨーロッパ諸国はもちろん、日米安保の下で防衛面ではアメリカに多くを依存する日本もロシア的な主権国家の見方からすると「真の主権国家」でないのかもしれない。自ら決定権を有する「真の主権国家」でありたいロシアにとって、サイバー空間のセキュリティーは大問題である。

国境のないインターネット空間を通じた欧米の‘悪しき影響’がロシアの国家体制を揺るがすかもしれないし、逆にアメリカが握るインターネットのインフラストラクチャーからロシアが切り離されてしまう恐れもあるかもしれない」と説明されています。

この点に関して日本のサイバー専門家は逆に、ロシアや中国の「インフルエンス（影響）・オペレーション」による『誘導工作』の恐れがあると指摘します。2020年の東京五輪・パラリンピック開催に向けてサイバー攻撃への対処能力の強化を図るために昨年の臨時国会で「改正サイバーセキュリティー基本法」が成立しました。政府や地方自治体、重要インフラ事業者、サイバー事業者、教育研究機関が相互に連携し情報を共有する官民共同の「サイバーセキュリティー協議会」の創設準備が始まっています。サイバー対策の第一人者といわれるサイバーディフェンス研究所・上席分析官の名和利男氏は、欧米でのサイバー対策の関心が高い分野として、①2016年のアメリカ大統領選挙でロシアの関与が疑われたインフルーエンス・オペレーション②中国が活発化させているとされる大量の個人や組織の内部情報を集めるビッグデータの利用を挙げています。これはサイバー空間の外で起きる国家間の緊張にからみ、国家がサイバー攻撃を仕掛けたり、脅したりして相手を揺さぶって政治目的を遂げようとするもので『ハイブリッド（混合）脅威』の一つだと述べています（読売新聞2019年1月17日朝刊13面、サイバー対策に関するインタビュー記事から）。

東海大学平和戦略国際研究所とモスクワ国立大学情報安全保障問題研究所の共催によるサイバーセキュリティーシンポジウムが開かれた一年前から状況は大きく変わりました。貿易戦争から始まったアメリカと中国の衝突は「近未来の世界を誰が支配するか」という新たな冷戦、ハイテク技術の覇権争いとして全面衝突の様相を呈しています。こうした大状況の変化を受けて日本のマス・メディアでもサイバーセキュリティー関連の記事やテレビ番組が多く見られるようになりましたが、安全保障問題をセンセーショナルに扱ったものが目立っています。シンポジウムの中で政府の実務責任者の三角育生内閣サイバーセキュリティーセンター副センター長（当時）が指摘された「サイバー空間は国家ではなく民間投資によって築かれた人工空間であり、サイバーセキュリティー対策への投資はやむを得ないコストではなく、価値を生む投資として認識されるべきである」という認識が充分に共有されていないのが現状です。同盟国アメリカ同様に自由と自立の価値観を重要視する日本と国家主権を前面に出す権威主義体制のロシアや中国との基本認識の隔たりは大きいのが現状です。また日本国内でも昨年の臨時国会でのサイバーセキュリティー基本法改正論議での与野党のかみ合わない論戦や企業経営者のサイバー対策への危機意識の低さは、憂うべき状況にあります。東海大学においても建学の精神にも謳われた「文理融合」を更に推し進めた独自の研究教育体制を構築すると同時に、外部の専門機関や通信インフラ企業等との連携を急がなければならないと思います。

今般、平和戦略国際研究所のブックレット創刊号を編纂するにあたり、日本とロシアとのサイバーセキュリティー問題アプローチの「視点」の違いとその意味を正確に認識すべきであると考えて、モスクワ国立大学情報安全保障問題研究所からの「提言」をシンポジウム記録の冒頭に掲載しました。また、日本政府のサイバーセキュリティーの基本的な理念をよりよく理解してもらう狙いから、内閣サイバーセキュリティーセンターの三角育生副センター長（当時）にシンポジウムの議論を踏まえた上で、改めて寄稿していただきました。また、シンポジウムにコメンテーターとしてご参加いただき貴重なご意見をいただいた防衛研究所の河野桂子研究員、未来工学研究所の小泉悠研究員にもシンポジウムの議論から明らかになった問題点に関して寄稿をお願いした次第です。

サイバー空間の拡大が、国家の安全保障分野だけでなく世界各地で暮らす人々の生活の向上や生産システムの改善に貢献するためにも違いを明確にした上で国際協調の道を探る必要があります。この小冊子が僅かながらでも貢献できることを祈念致します。

モスクワ大学の提言

国際条約草案の構想
―インターネットの安全な機能と発展の構想―

総　則

インターネットの発展は人類にとって極めて重要である。

インターネットにおける技術、サービス、ビジネスの発展は、個人や社会、そして国家に新たな課題を生み出している。

インターネットは科学知識、教育、医学、経済、その他の分野の発展を促進している。

インターネットが適切に機能することは、あらゆる国家、およびその国民と経済にとって大変重要になっている。

しかし現在、われわれにはオープンで透明性の高いインターネットガバナンスシステムが欠如している。

われわれは、国際連合経済社会理事会（ECOSOC）2011年7月26日の決議2011/16に従い、各国政府がインターネットに関する国際公共政策問題における義務を遂行する上で行う活動やその役割に関する課題と、日常の技術・運用上の活動に関する課題とを区別する。

われわれは、インターネットのセキュリティ、継続性、安定性の重要性、ならびに潜在的な脅威や脆弱性からインターネットを保護する必要性を強調する。

われわれは、インターネットセキュリティの課題の共通理解、ならびに国内外でのさらなる協力の必要性を確認する。

2015年12月23日の国連総会決議A/RES/70/237「国際安全保障の文脈における情報および電気通信分野の進歩」、および2015年12月16日の国連総会決議A/RES/70/125「世界情報社会サミットの成果実施状況レビューに関する国連総会ハイレベル会合の成果文書」に従い、われわれは国連加盟国に、情報セキュリティ分野における既存および潜在的な脅威についての多国間検討を推進するよう勧告する。

1966年の「市民的および政治的権利に関する国際規約」は、すべての人が干渉されることなく意見を持つ自由についての権利、および国境との関わりなく、あらゆる種類の情報および考えを求め、受け、伝える自由を含む表現の自由についての権利を認めたものであるが、われわれは、この国際規約ならびにその他の国際人権条約に定められた基本的人権の尊重と法の執行との間に適切なバランスを確保する必要があることを指摘する。

われわれは、あらゆる人権、特に表現の自由、プライバシーの権利、知る権利、匿名性、オンラインおよびオフラインの両方における個人データの保護、その他関連する人権と自由を等しく尊重し、確実に実行しつつ、基本的人権を尊重し、保護し、確保すること、ならびにその経済および社会の発展における重要性を認識することの必要性を再確認する。

われわれは、インターネットを国連憲章に反する目的で使用することを防止するため、国際社会の努力を結集することの必要性を認識する。

われわれは、標準、技術、および通信ネットワークの発展の責任を負う国家、世界的なICT企業、会社の相互関係および役割を調和させる、新しい国際協定の必要性を認識する。

われわれは、いかなる単一国家または国家群も、インターネット機能に干渉し、独自の裁量でインターネットの規範や規則を定め、社会を監視し、外国の世論を操作し、または主権国家の状況を不安定にさせる権利がないことを強調する。

われわれは、インターネットガバナンスプロセスにおけるすべてのステークホルダーの役割を特定し、特にインターネット関連の公共政策問題を取り扱う政策権限は国家の主権であることを認めた「情報社会に関するチュニスアジェンダ」(35-38、51、52、69項)の重要性を確認する。

構想の目的

インターネットのさらなる発展を促進し、セキュリティを改善し、ユーザーの権利と自由を保証すること。

インターネットガバナンスにおいて、公平な国際協力を確立すること。

国内施策および国際協力の改善を通じて、より効果的で効率的なインターネットガバナンス施策の採用と強化を促進すること。

インターネットガバナンスの一般原則

インターネットガバナンスとは、一般に認められた国際法の原則と規範に基づくオープンで民主的なプロセスで、人々のニーズや、個人データの保護も含めたその権利と自由の保護を重視するものである。

インターネットガバナンスは、一方的な政治的制約または商業利益に影響されてはならない。

インターネットガバナンスは以下のことを目的としている。

自国内のインターネット部門を統治する各国の権利に配慮しつつ、国内外の規範と標準の調和をはかり、ガバナンスの全レベルにおいて相互関係を調整すること

インターネットガバナンスシステムを管理する一国の権限を、すべての国家、および必要な場合は他の国際機構の間で公平に分配すること。

インターネットガバナンスのための国際的な法的および組織的枠組みを策定すること。

インターネットのセキュリティ、継続性、安定性、堅牢性を確保すること。

インターネットガバナンスにおける国家の行動原則

各国は、国際的なインターネット関連の公共政策問題について平等の権利と責任を持つ。

国家が他の国家に影響を与える手段として、インターネットへのアクセスを用いてはならない。

各国は他国の領域内で、インターネットの運用および／またはインターネットへのアクセスを制限する行動を控える。

各国はインターネットガバナンスにおける公平性の原則を認めるとともに、自国内のインターネット部門を規制する主権はそれぞれの国家にあることを認める。

各国は、自国のインターネット部門の重要な基盤要素の機能も含めて、自国のインターネット部門の安全性、完全性、継続性、安定性、堅牢性、およびセキュリティを確保する。

各国は、基本的人権を尊重し、保護し、確保し、その経済および社会の発展にとっての重要性を認め、あらゆる人権、特に表現の自由についての権利、プライバシーの権利、知る権利、匿名性、オンラインおよびオフラインの両方における個人データの保護を等しく尊重し、確実に実行する。

各国は、主権の平等、ネットワーク主権の認識、持続可能な開発、国境を越えた影響からの保護、セキュリティの確保、および安全なインターネット機能のための施策強化に基づき、インターネットを統治する。

各国は、インターネットの情報分野に対する自国の主権を保持し、法域内の市民の保護を保証し、自国のインターネット部門のガバナンス、戦略的堅牢性、および保護を確保する。

各国は、国内のステークホルダーをバランスよく参加させながら、番号や名前資源を独自に割り当て、指定し、あるいは取り消し、インターネットのアドレス指定および識別を維持し、自国のインターネット部門の運用を支援し、監視し、発展させる権利を保持する。

各国は、適用可能技術にかかわらず、ユーザーが世界のどこにいようと関連サービスを利用できる環境を創出することを目的として、協力と相互支援の原則に従い、国際標準の開発と適用に貢献する。

各国は、内国法に従い、自国のインターネット部門のガバナンスについて責任を負う国内の

組織を指名しなくてはならない。各国はその領域内で重要なインターネット基盤要素の設置を推進する。

各国は、インターネットが安定的に機能し、ユーザーが安定的にサービスにアクセスできるようにする。

各国は、ステークホルダーのバランスの取れた参加のもと、国際社会の公平な参加に基づいて、国際的なインターネットガバナンスの向上のために国際協力を推進する。

インターネットガバナンスにおける国際協力の原則

重要なインターネット基盤が安定的に機能できるようにするための規則の策定、採択、および実行の監視は権限のある国際機関が行わなければならない。

国際社会の公平な参加に基づくインターネットガバナンスとは、下記のようにガバナンスプロセスを複数の機能に分割することであり、これらの機能はそれぞれ異なる機関が実行すべきである。

- 構成機能：インターネットガバナンスプロセスの中で生じる関係性を規制するための方針、規則、手順、標準、その他の規範の策定と採択を行う
- 重要基盤の日常的なガバナンスとは無関係の実行機能：重要資源を生み出し、さまざまな当事者の間で割り振るための意思決定機能、および紛争解決機能がこれに含まれる
- 重要基盤の日常的なガバナンスに関連した実行機能：重要資源の割り当て／割り振りについて採用された決定の実行、ならびに重要資源の管理、重要基盤の運用の監視が含まれる
- 重要なインフラ基盤の運用機能

インターネットガバナンスに関連した構成機能と実行機能は、どの国家の法域からも独立が保証された国際的地位のある機関が実行する。

重要なインターネット基盤の管理を委任された機関は、権限のある国際機関との契約に基づいて業務を遂行し、その契約は定期的に見直される。

各機能のガバナンスは、国際レベルと国内レベルの２段階で行われる。また国内レベルで基盤を規制するのは主権国家の権利であることに配慮しつつ、インターネットガバナンスプロセスは、これらのガバナンスレベルの相互作用の調整に基づいて行われている。

インターネットガバナンスを行う権限を持つ国際機関は、各国国内のインターネット部門におけるさらなる管理のために相互に合意したオープンな方法で、資源の番号、識別、アドレス指定、および名前（ドメイン名）を割り当て、関係国の同意が得られた場合には、再配分を行う。

権限のある国際機関は、インターネットが安定的に機能し、ユーザーがインターネットサービスに安定的にアクセスできるようにする。また各国は、権限のある関連国際機関の決定を実行しなければならない。

権限のある国際機関は、重要なインターネット基盤のガバナンスの分散化、セキュリティ、および国内のインターネット部門、およびインターネット全体の重要基盤の安定的な機能を確保することを目的として、規則および標準を策定し、実行し、その適用を監視する。

協力と支援の原則

各国は協力を強化することで、国内のインターネット部門の完全性と信頼性の高い機能およびセキュリティを確保し、インターネットトラフィックの中継のための直接的な関係を確立し、インターネットの基本基盤を発展させるべきである。

各国はインターネットのアクセスと使用に関する一般市民の要望に応える政策を推進し、国際協力メカニズムによるものも含めて、インターネットの運用および発展の促進を支援する。

各国は、相応のインターネット開発計画およびプログラムに関連して、要請に基づき、相互に、特に途上国に幅広い技術支援を提供して、インターネットセキュリティを向上させ、ユー

ザーの権利と自由を確保することを検討する。これには物的支援、研修、関連する経験や専門知識の相互交換なども含まれる。こうした施策は国家間の国際協力を促進することを目的とする。

各国は、国際機関および地域機関、あるいは関連する他の二国間または多国間の条約や取り決めの枠組み内で開催される実践や研修のイベントの効率を最大に高めるため、なおいっそう努力する必要がある。

各国は、要請に応じて、インターネットの分析、調査、発展、インターネットセキュリティの向上、およびユーザーの権利と自由の確保について、相互支援の機会を検討し、所轄官庁や市民の参加を得てこうした分野の戦略および計画を作成する。

付　録

用語

情報通信技術（ICTs）とは、情報の検索、収集、保存、処理、提供、普及のプロセスおよび方法、ならびにこうしたプロセスや方法の実行手段である。

情報通信ネットワークとは、リンクを介して情報を伝達することを意図とした技術システムで、電子機器による情報へのアクセスを提供する。

インターネットとは、グローバルなアドレス空間を通じて、さまざまな国々の情報システムや通信ネットワークを結んだ世界的な情報技術ネットワークである。インターネットは一連のインターネットプロトコルおよびデータ発信プロトコルに基づいて、一般市民向けの情報掲載を含むさまざまな形態の通信の実行機会を提供している。

重要なインターネット基盤とは、情報基盤の不可欠な部分で、ネットワーク、システム、インターネット資源を組み合わせたもので、その相互運用性は国内のインターネット部門における情報基盤の完全性、継続性、安定性、堅牢性、およびセキュリティに大きな影響をもたらす可能性がある。

インターネットガバナンスとは、政府やその他のステークホルダーが、それぞれの役割と責任において、インターネットの進展と利用のための条件を形成する共通の原則、規範、規則、意思決定手順、プログラム、および勧告を策定し、適用するプロセスである。

インターネットガバナンスの普遍的モデルとは、すべてのステークホルダーが、それぞれの役割と責任に従って、インターネットガバナンスプロセスを確立する統一アプローチの構想で、インターネットガバナンスのどの分野にも適用でき、こうした分野に関連した課題解決のメカニズムを確立することができる。

ステークホルダーとは、インターネットガバナンスプロセスに参加し、そのプロセスにおいて、それぞれの役割と責任を果たす国家、民間部門、市民社会、科学技術コミュニティ、政府間機関および国際機関のことである。

情報基盤とは、情報を創出し、形成し、変換し、伝達し、使用し、保管する一連の技術的手段、システム、および資源である。

ネットワーク主権とは、国内のインターネット部門の情報基盤に関する国家の権限を無条件に実行する能力である。国家は自国の主権によってその能力を保有し、自国の主権を用いてそれを行使する。

国内のインターネット部門とは、国家の領域内に位置し、その国家の国内法に準じて正式に登録された一連の情報通信ネットワーク、システム、およびインターネット資源であるが、関連する国際協定の枠組の中では、ナショナルドメインゾーンおよび資源も、その国家の国内のインターネット部門と称される。

ナショナルドメインゾーンは、階層構造のインターネットドメイン名空間の領域で、一意のドメイン名によって識別され、特定の国に割り当てられ、国名コードに一致する。

ドメイン名とは、国際的なインターネットのアドレス指定規則に従って形成された一組の文字列で、インターネット情報資源のアドレス指定に用い、特定のネットワークアドレスに合致する。

特集　東海大学建学75周年記念
サイバーセキュリティーシンポジウム

主催：東海大学平和戦略国際研究所、モスクワ国立大学情報安全保障問題研究所
協賛：笹川平和財団、東海大学西方勇雄国際活動支援基金

実施日程：2017年12月１日（金）12：30－17：10
開催場所：霞ヶ関ビル35階　東海大学校友会館（朝日の間）
通　　訳：日本語・ロシア語同時／逐次通訳
進　　行：吉川直人　東海大学副学長

12：30－13：00
開会の挨拶
- 菅　義偉　内閣官房長官
- エフゲニー・アファナーシエフ　駐日ロシア大使
- デヴィッド・エリス　駐日英国大使館首席公使

13：00－14：00
第１部「Keynote Speeches：Cyber Security Dialogue in Global Paradigm Shift」
- 末延吉正　東海大学平和戦略国際研究所所長　―　本シンポジウムの背景と狙い
- ヴラディスラヴ P.シェルステュク　モスクワ国立大学情報安全保障問題研究所所長、ロシア連邦安全保障会議顧問
- 大鷹正人　外務省総合外交政策局審議官兼サイバー政策担当大使

14：30－16：30
第２部「How information technologies contribute to socio-economic development and Quality of Life?」

モデレーター
- 石川一洋　NHK解説主幹　元NHKモスクワ支局長

プレゼンター
- 三角育生　内閣官房　内閣審議官
- アナトリー・ストレルツォフ　モスクワ国立大学情報安全保障問題研究所副所長
- 中嶋卓雄　東海大学情報教育センター所長
- カラセフ・パヴェル　モスクワ国立大学情報安全保障問題研究所

コメンテーター
- リナ・シャラポフ　モスクワ国立大学情報安全保障問題研究所部門長
- 河野桂子　防衛研究所研究員
- 小泉　悠　未来工学研究所研究員

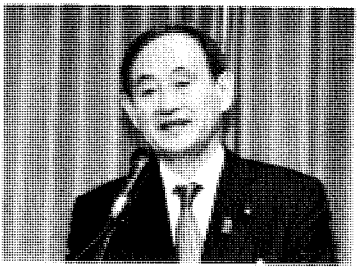
17：00－17：10
閉会の挨拶
- ウラジミール・V・ソコロフ　モスクワ国立大学情報安全保障問題研究所副所長

17：30－19：30
レセプション　東海大学校友会館（相模の間）
メディア　NHKニュース、NHK BSニュース
テレビ朝日ANNニュース、BS朝日報道番組『日曜スクープ』

開会の挨拶

東海大学建学75周年記念
サイバーセキュリティーシンポジウム　2017年12月1日

菅　義偉
（内閣官房長官）



ただいまご紹介に預かりました内閣官房長官を務めております菅義偉であります。東海大学とモスクワ国立大学の共催により東海大学建学75周年記念国際サイバーセキュリティーシンポジウムが開催されるにあたり一言ご挨拶を申し上げる次第でございます。皆さまご案内の通り安倍総理とプーチン大統領が20回にわたる首脳会談を積み重ねてきております。両首脳は平和条約の問題を解決するとの真摯な決意のもとに、我が国は4島の帰属問題を解決し平和条約を締結するという基本方針に基づいて、ロシアと交渉を致しております。こうした両国間の関係のなかで、今後一層の協力関係の構築を期待される分野がサイバーセキュリティーであります。本日、両大学の協力のもとにシンポジウムが開催されることを政府のサイバーセキュリティーの最高責任者として、大変嬉しく歓迎を申しあげる次第であります。またロシアと並びこの分野の先進国である英国からデヴィッド・エリス首席公使が参加されておりますことを心から歓迎を申しあげる次第でございます。政府は先端技術をあらゆる産業や社会生活に取り入れサイバー空間と現実空間が高度に融合したSociety 5.0を実現すべく政策資源を集中投資していくこのように考えております。一方で、このSociety 5.0の基盤となるサイバー空間では悪質なサイバー攻撃の脅威が高まっております。我が国の政府基盤だけを見ても、昨年1年間に約711万件のサイバー攻撃を受けており、これは4.4秒に1回その攻撃を受けている計算になります。またこの4月には世界中に広がる身代金型サイバー攻撃により各国のシステムやデータが利用されなくなる事案が数多く発生を致しております。このような状況のなかで、サイバーセキュリティーの確保は喫緊の課題であります。政府では私が本部長を務めるサイバーセキュリティー戦略本部において、官邸を司令塔として対策を進めているところであります。戦略本部では、本年7月、サイバーセキュリティーにおいて当面取り組みを加速し強化すべき施策取りまとめました。

本日はその中で特に重要であると考える3点についてお話をさせていただきます。

第1点目は、IoT機器のセキュリティー対策の強化であります。インターネットに接続されるIoTへの機器の種類、台数は年々増加をしており、その普及台数は2020年ごろには約300億台に上り、インターネットに繋がるものの数が人の数をはるかに上回るそのことが予想されます。IoT機器の様々な生産から得られる多様なデータはビッグデータとして活用されAIなどにより新たな知恵を生み出すこうしたことが期待されます。我が国も諸外

国と提携してIoT機器のセキュリティー対策の強化に取り組んでいかなくてはならないと考えております。

第2点目は、セキュリティー情報の共有と連携の強化であります。サイバーセキュリティー対策は自らが行うことが当然基本でありますが、逆に、一人で行うことには限界があります。そのために秘密保持など一定のルールを定めた上で管理の関係者の間で必要な情報を共有するセキュリティー対策を迅速に効果的に進めていく、このことが重要であると考えております。政府ではこうした観点から、国内外の行政機関や民間事業者と連携しつつサイバーセキュリティーを図る上で有益な情報の提供と共有を促進する枠組みを作っていきたいと考えております。

3点目は、開催まで1000日を切った2020年東京オリンピック・パラリンピック競技大会への準備であります。政府では、大会期間中にサイバー攻撃が発生しても迅速的確に対応し、大会の円滑な運営を確保することができるよう2019年度中にサイバーセキュリティー対策調整センターを構築すべく現在準備をすすめているところであります。センターは大会の成功に向けた運営をする為に必要なだけではなく、このセンターの運営を通じて得ることのできる様々なサイバーセキュリティーに関する経験を「レガシー」として残し、我が国がサイバー空間においても信頼が高く高品質な安全を提供できる国になることができるよう取り組んでいきたいと思っています。

以上3点を申し上げました。サイバー空間はグローバルに繋がっておりこのような取り組みを推進し安全なサイバー空間を構築する上で国際連携が極めて重要であります。

本日のシンポジウムでは日本、ロシアの著名な研究者や実務家の皆さまが参加し『グローバルパラダイムシフトとサイバーセキュリティー対話』をテーマに議論がなされる、このように伺っております。

私がいま申し上げました3点については、本日のテーマと密接に関係があると思っております。本シンポジウムを契機に、サイバーセキュリティー分野での協力を推進する上で両国の新たな国際的な枠組みが構築できるか政府としても大変に注目を致しております。皆さまの間で活発なご議論が行われ実り良い内容になることを期待致します。

終わりにお集まりの皆さまのご活躍を心から祈念致しまして私の挨拶とさせて頂きます。どうぞ皆さま、素晴らしい成果が出ることを期待致します。

開会の挨拶

東海大学建学75周年記念
サイバーセキュリティーシンポジウム　2017年12月1日

デヴィド・エリス
（駐日英国大使館 首席公使）

菅内閣官房長官、山田学長、アファナシエフ大使。本日はご招待いただき誠にありがとうございます。東海大学校友会館において、このようなサイバーセキュリティに関する素晴らしいシンポジウムに参加し、特にご列席の著名な研究者の皆様、政府代表者の方々、世界各国を代表する皆様の前でお話できますことを、大変嬉しく思っております。残念ながら健康上の理由でナイジェル・インクスターは出席できず、私が光栄にも、英国を代表して出席させていただきました。

今はまさに、サイバーセキュリティの問題を議論する絶好のタイミングといえましょう。昨年来、悪意あるサイバー活動は、規模においても程度においても大幅に増加しています。5月にはランサムウェアのワナクライ（Wannacry）が世界中で猛威を振るいました。フランスではマクロン大統領の政党「共和国前進（En Marche）」がハッキングされ、情報がリークされる被害にあいました。また、英国議会のメールアカウントも攻撃を受けています。

刺激的な時代になったものです。現在、英国はこうした問題に包括的に対応しています。それには短期的な解決だけでなく長期的な解決策が必要です。

同盟国と協力してサイバーインシデントに対処し、悪意ある行為者にその代償を支払わせること。ASEAN 地域フォーラムにおいて信頼構築のための施策を進んで実施し、促進すること。さらにサイバーセキュリティ分野における能力開発プログラムを通じた東南アジアのパートナーの能力強化などが、その例といえましょう。

そしてもちろん、こうした対応の中で、同盟国との協力は極めて重要な部分を占めています。我が国の首相は、夏に訪日した際、安倍首相とともに共同ビジョン声明を発表しましたが、その中で、今後の両国関係の方向性として、両国のパートナーシップを次の段階へ引き上げることをうたっています。

安全保障に関する両国の協力関係が深まりつつある中で、両首脳は世界各地でそのさらなる強化を図ることに合意しました。この合意には、防衛および外交政策も含まれています。しかし最も重要なのはサイバーセキュリティで、両国は共通の脅威に対抗し、脅威が認められた時には阻止することを公式に約束しました。

また両首脳は、経済やビジネスに関する協力関係の強化にも合意しました。サイバーセキュリティは両国の経済政策にとっても極めて重要です。新しい技術、たとえばAI、IoT、デジタルサービスなどが、成長の、そしてクオリティ・オブ・ライフの原動力として

不可欠であるということは、このシンポジウムでも取り上げられることでしょう。

アファナシエフ大使

私たちの経済は、自由でオープンで平和なインターネットに依存しています。しかしその成功には、インターネットが安全で、サイバー攻撃の脅威に対応できるものでなくてはなりません。残念ながら、先に申しましたように、現在こうした脅威の数は増加し、ますます高度化しています。サイバー攻撃の脅威に効果的に対応するためのカギは協力関係です。国家間の協力関係はもちろんのこと、官民の協力関係も重要です。

英国では、国家サイバーセキュリティセンター（NCSC)が対応の要となっています。NCSCは英国の新サイバー戦略の中心的存在です。安倍首相は4月のロンドン訪問時にNCSCを視察され、サイバー攻撃に対する英国全体の備えや、攻撃発生時の対処において、NCSCが果たす役割の説明を受けられました。

NCSCは政府、英国企業、研究機関の一元的な連絡窓口の役割を果たしています。英国社会のあらゆるところに助言と支援を与え、民間部門の能力を強化し、その技術や機能の向上を図って、世界規模のサイバー活動がもたらす機会を活かせるように取り組みを進めています。さらに、他国の政府と協力し、ベストプラクティスを共有し、脅威に対抗するという、国際的にも重要な役割を担っています。

NCSCの誕生は、2012年にロンドンオリンピック・パラリンピック大会を主催した経験がひとつのきっかけとなっています。興奮に満ちた素晴らしい大会でしたが、同時に多くのサイバー攻撃の脅威も生じました。大会を安全に成功させるために政府の安全保障関連組織と民間部門を統合したことが、サイバーセキュリティに対する英国の長期的な取り組みの変革につながったのです。

今後は2020年の東京大会に世界の注目が集まることになりますが、私は、プロフェッショナルで、革新的で、グローバルという、日本の最高の英知がそこに結集されると確信しています。メイ首相は、2012年のロンドン大会の経験をもとに、東京大会の物理的な安全とサイバーセキュリティが確保されるよう、英国が支援を提供することを約束しました。私たちは今後も共に手を携え、協力を続けます。

ご清聴ありがとうございました。

基調講演

末延　吉正
（東海大学平和戦略国際研究所 所長）

本シンポジウムの背景と狙い

東海大学平和戦略国際研究所所長の末延です。本日はご多忙中のところご参加いただきまして有難うございます。心から感謝申し上げます。貴重な時間でありますので手短に本日のシンポジウム開催の背景と狙いについてお話をさせて頂きます。

東海大学平和戦略国際研究所は、本学の創立者であります松前重義博士の建学の精神を基にヒューマンセキュリティー『人間の安全保障』を理念に活動を続けております。これまで予防医学や移民・難民問題を中心にした研究に続けてまいりましたが、今年度より、新たに喫緊の課題でありますサイバーセキュリティーを中心にした世界の「安全保障の枠組み」についても研究を始めることに致しました。

今回は建学75周年を記念しまして、東西冷戦下にあって学術交流を積み重ねて参りましたモスクワ国立大学との共催という形で今後の世界のあり方に決定的影響を与えるであろうサイバーセキュリティーに関して日本政府、この分野でアメリカを中心にした先行研究で実績があります笹川平和財団のご協力を得ましてこのシンポジウムを開催いたしました。本日、田中会長にもご出席を頂いております。重ねて感謝申し上げます。

サイバーセキュリティーに関しまして私共の認識は、アメリカ、ロシア、中国が第一列です。その後ろの1.5列に位置するのがイギリス、フランス、イスラエル、、そして日本であるという現状認識に立ちまして、今回、ややもすれば誤った情報が伝えられパイプの少なさから正確な議論がなされてこなかったロシアからモスクワ国立大学の専門家の皆さまをお呼びしてシンポジウムを行うことを企画した次第でございます。来年度以降これに加えまして笹川平和財団が強いパイプを持っておられますサイバー大国の米国、中国やイスラエル等多くのご参加を得て国際的な枠組みについての議論の場を東海大学平和戦略国際研究所が提供していきたいというのが我々の計画であります。

第一部では日本、ロシア両国の安全保障を含めた基本的な取り組み、考え方についての認識をお話いただければと思っております。その後にコーヒーブレイクを挟みまして、第2部ではそうした安全保障、政府サイドの話に加えまして経済分野、とりわけ最近大きな問題となっておりますビジネス分野におけるサイバーセキュリティーへと議論を進めて参りたいと思います。本日は、防衛研究所の河野さん始め、素晴らしいコメンテーターの方にもご出席いただいておりますので活発な本音ベースの議論が展開されますことを期待しております。　最後に、サイバー空間というのは私たちが目にすることができない世界であります。言葉を変えて言えば、そこには恐怖があり、そこには希望が隠されている世界であるという認識であります。我々がどういう形で国際的な協力関係を構築して行くことができるのか、どこに根本的隔たりがあるのか、本日のシンポジウムを第一歩として建設的な議論のスタートを切れればと思います。

【ご参考】

本シンポジウムの開催は、当日のNHKニュース、NHK BSニュース、テレビ朝日系ANNニュース、Abema TVでニュースとして放送されました。また、BS朝日では、2018年1月21日の『日曜スクープ』のなかのサイバー特集の一部として放送されました。

【ご参考】

2018年1月21日　BS朝日『日曜スクープ』放送概要

東海大学校友会館

東海大学主催　現代の国際情勢安全保障と国際的な対話

ニュースの焦点：ロシアゲート…最大の焦点を“ロシア視点”で読み解く！

菅 官房長官

「我が国の政府機関だけでみても昨年（2016年）1年間に約711万件のサイバー攻撃を受けており、これは4.4秒に1回この攻撃を受けている計算になります。」

ナレーション

「東海大学が主催したシンポジウムのテーマは、国際情報の安全保障。専門家たちが危惧するのは、将来的なサイバー攻撃の爆発的増加です。」

山田清志 学長

「我々は長年にわたりましてロシア特にモスクワ国立大学との連携を深めています。世界のサイバーセキュリティーの向上のため、さらに深めてまいりたいと思っております。」

ナレーション

「専門家からは、各国が情報を共有し、国際法を作るべきだとの声もあがっています。」

末延吉正 平和戦略国際研究所所長

「誤った情報が伝えられパイプの少なさから正確な議論がなされてこなかったロシア」

「サイバー空間というのは私たちが目にすることができない世界であります。言葉を変えて言えばそこには恐怖があり、そこには希望が隠されている世界であるという認識であります。」

ナレーション

「シンポジウムの途中、ロシアの情報安全の専門家はこんな発言も」

ストレツフォフ・アナトリー副所長

「世界中でいま悪いことが起きるとプーチンのせいだとなっている。天気が悪かったらプーチンのせい、地震が起きたらプーチンのせい、感染症が流行したらプーチンのせいになっていますよね。悲しい事実です。」

ナレーション

「さらに、小松キャスターのインタビュー中にも」

ヴラディスラヴP.シェルステュク所長

「ロシアゲートを証明する根拠というのは依然として見つかっていないのです。こんなフェイクニュースを出すようでは信頼関係は築けない。すべて止めるべきです。」

ナレーション

「ロシアゲートというトランプ政権に刺さった棘、ロシアの選挙介入はあったのか？このあとロシアの専門家とともに徹底検証します。」……（略）。

基調講演

ヴラディスラヴ P.シェルステュク
(モスクワ国立大学情報安全保障問題研究所 所長、ロシア連邦安全保障会議 顧問)

尊敬するシンポジウム主催者の方々！ 参加者の皆様！ 紳士淑女の皆様！ 同僚の皆様！

本年11月1日、モスクワ大学総長でありアカデミー会員であるヴィクトル・アントーノヴィチ・サドーヴニチィが、東海大学創立75周年を記念する催しに参加いたしました。松前重義博士がこのユニークな学園を創設したのは1942年、こんにちに続くモスクワ大学との協力事業が始まったのは1973年です。

ここに、M.V.ロモノーソフ記念モスクワ国立大学情報安全保障問題研究所を代表して、東海大学の学生、院生、教員、従業員、管理者の皆様方に記念日のお祝いを申し上げます。山田清志学長には、国際情報セキュリティの分野における現在の発展動向をテーマとするシンポジウムにお招きいただき、お礼申し上げます。

来年は国際情報セキュリティということばが生まれてからちょうど20年の節目に当たります。

この分野の研究の嚆矢となったのは、1998年9月23日、ロシア外相であったI.S.イワノフが当時のコフィ・アナン国連事務総長に送った書簡です。

1999年、国連総会において「国際安全保障の文脈における情報および電気通信分野の進歩」を議題とする決議がなされ、情報通信技術（ICT）の軍事、テロリズム、犯罪への利用という、国際情報セキュリティにおける「3つの脅威」が初めて提唱されました。

国際安全保障、軍縮とそれに伴うその他の分野という文脈においてICTが使われることによる悪影響を如何に防止するかという議論が、毎年国連総会において続けられております。

国際社会は、情報通信技術が発達し、一般に採用されている現在において、それらが国際平和を破壊する目的で使用されることの危険が高まっていると認識しています。なかでも、情報分野における新たな軍拡競争の引き金になりかねない国家間対立がおこることをなんとしても避けなければならないという考えが高まっております。

われわれの考えによれば、この問題を解くための最適の方法は、国際情報セキュリティの強化を図ることであります。

国際情報セキュリティについては、国連軍縮研究所と赤十字国際委員会が後援して行われるものを含め、国際的なコンファレンスやセミナーが開催されてきました。2001年11月29日、第56回国連総会でロシアの提唱により、各国政府から派遣される専門家による国際情報セキュリティ研究特別作業部会を設けるというきわめて重要な決定がなされ、この作業部会は2004年に創設されるに至りました。この作業部会の任務のなかには、情報セキュリティにおける脅威とその除去を可能にする共同手段を検討し、グローバル情報通信システムのセキュリティ強化を図るためのコンセプトを追求することが含まれております。

各国政府専門家をメンバーとする国連特別作業部会の研究努力により、全国連加盟国は、他国の領土保全または政治的独立を冒すことを目的とした特定の国家が、悪意によるか、もしくは敵対的関係によってICTを用いることによってもたらされうる、国際安全保障と国際平和に対する脅威に対し、注意を向けるようになりました。また国際社会は、国家に属さない組織がテロ行為などの犯罪活動にICTを利用する危険性にも留意することになりました。

長年に渡る専門家の努力は多くの点でブレークスルーといってもよい国連事務総長報告書に結実し、それは2015年に全会一致で採択されました。この報告書には、ICT環境での国家の責任ある行動原則と信頼醸成措置に関する勧告が含まれています。

いくつかのキーポイントが合意されました。

一つ目は、情報空間における紛争については法的に解釈することも規制することもせず、ICTが政治的軍事的目的で使用されることを防止する。

二つ目は、現在多々見られるような、確たる証拠もなしにサイバー攻撃を行ったとして非難し合うことを控える。

三つ目は、ICTの利用は平和目的に限定する。

四つ目は、ICT製品にバックドアを仕掛けることは不法であり、有害行為とみなす。

五つ目は、作業部会が、自国の領土内にある情報通信インフラを左右し、国際情報セキュリティ分野の政策を決定することを国家の主権に属することであると認めること。

以上の五つであります。

残念なことに、2016年に構成された作業部会はそれまでの作業速度を維持することができず、総括報告をまとめることができませんでした。だからといって、国際情報セキュリティで重要な問題の討議を停止するわけには参りません。ましてやこのことを、国連の役割を軽視する根拠にしたり、論議そのものを地域間レベルや、二国間交渉のレベルに引き下げることなどは論外です。

確言できるのは、ICTの発展と多様な分野での利用が人類にとって安全や快適な世界をもたらすものとはなっていないということです。国際的なテロ活動を支援し、国境をまたぐ違法な経済活動を行い、さらには人権侵害を顧みずに国家間の対立を暴力的に解決しようとする目的でICTが利用される危険がますます大きくなっています。フェイクニュースを流して国際間の緊張を煽ることが現代の国際政治の流行になりつつあります。国家の運営にとってきわめて重要な対象物やインフラ、金融システムへのコンピュータ攻撃はますます巧妙になり、その回数は減っていません。

ロシア連邦安全保障会議書記ニコライ・パトルシェフの報告によれば、2016年に国家機関のサイトに対するサイバーアタックの回数は増大し、5,250万回前後に上りました。2015年は1,440万回です。1年間に3倍になったことになります。ロシア連邦保安庁の2017年のデータによれば、ここ数年のハッカー攻撃による世界の損失は、評価の方法により異なりますが、3千億ドルから1兆ドルに達します。この額は世界のGDPの0.4から1.5（%）に相当し、絶えず増大する傾向にあります。国際テロ組織やいくつかの国が行う、きわめて重要な施設やインフラの運営を妨害する目的でのICTの敵対的使用のリスクは高まっております。

リアルであれ、バーチャルであれ、またフェイクであれ、こうした事件が起こるとすれば、それは情報分野を幻覚に満ちたものしてしまうこととなり、人々の政治生活に深刻な曖昧性を生じさせます。

国家、ビジネス、民間セクターの間で、サイバー空間や情報分野全体に対する信頼を醸成する作業は、政治、経済、国際状況から切り離された状態では実現不可能であります。国際安全保障という複雑な問題を議論する過程が国際協力とともに維持されなければ、信頼は決して醸成されません。既存の武器と共に情報を武器として争われる国際紛争が生じないように努めなければなりません。

信頼醸成措置を形成するための多くの研究は、ロシア連邦により、他の関心を寄せている国々が協力して、欧州安全保障協力機構を舞台として行われてきました。2016年、欧州安全保障協力機構常設理事会は、政府間協力や透明性、予見可能性や安定性といったことの向上、誤解を生むリスクの減少、ICTを利用することで起こり得る紛争がエスカレートすることを防止するなどを目的とする包括的信頼醸成措置強化プロジェクトを立ち上げる

ことを決定しました。そして関心を有している国々の参加を得て、サイバーセキュリティ分野の信頼醸成措置強化作業部会が非公式に設置されました。

ロシア連邦を含め、関心のある国々の努力により国際的な専門家の間で、各国が承認している以下のような国際法の法源から生じるところの国際的な義務を履行することが必要とされることに関する理解が生まれつつあります。その法源とは、総合的な国際条約や専門的な国際協定、国際的な慣行、開明的な国民が認める法の一般原則、法廷の判例を言います。

陸地、海洋、空域、宇宙といった主権国家間の関係が顕現する国際空間に関し、ICTが普及した国際空間がこれまでのものと異なるのは以下の点です。

グローバルなデジタル識別子の体系を通じて機能する通信手段、コンピュータ・デバイス、ソフトウェアの総体としてのICT環境が人工的な性格を有していて、そのパフォーマンスは何をおいても異なる司法権のもとにある非政府組織の力に拠るものであること。

次いで、ICTはバーチャルなプロセスであり、その結果、ICT環境に突発的事態が生起する条件を直接に観察することが不可能であること。

また、ICT環境では突発的事態が生じる淵源を見極めることが困難であること。

さらには、社会に取りきわめて重要なインフラに対してICTが悪用されたり、敵対的に使用されたり、ICT環境にある対象物やICTに関連したインフラがテロ攻撃を受けることにより社会的動揺が惹き起こされること。

最後に、テロ組織によりICTがメンバーの勧誘、資金調達、テロの訓練や扇動、実行の手段に使用されること。

これらの点であります。

ICTが主権国家の内政に干渉する手段として使われることも、国際情報セキュリティ上の脅威として認識する必要があります。ロシアを含む数カ国が、こうした脅威に対抗することの必要性を、情報セキュリティに関する二国間協議や、上海協力機構の場で一度ならず表明してきました。ロシア連邦は他のいくつかの国とともに、2011年と2015年の二度にわたって関連する決議案を国連に上程しております。

今日、専門家たちの国際社会では、国際情報セキュリティシステムの根幹を構築する原則について意見の相違が見られます。ある専門家たちは、情報空間はすでに新たな軍事行動の舞台になっており、ICTを用いた軍事的政治的紛争が不可避となったと思われるとして、こうした紛争を規制することに努力を集中するよう提言しています。その規制メカニズムは、デジタル化以前の時代に確立された国際法の既存の基準が無条件に適用されるようにしなければならないとも述べています。こうした専門家たちは、ICT環境においては、各国間で責任範囲を定めることや、国家の犯した国際義務違反を客観的にデータ化するプロセス、さらには、各国のコンピュータセキュリティインシデント対応チーム（CSIRT）の連携活動によりICT環境における国際的な事件を捜査する手順について合意形成を行う必要については特に認めていません。

コンピュータアタックの発信源を明確に突き止めることは実際上難しいので、上記のようなスタンスは、好ましくない国家に対する情報戦を挑むだけにとどまらず、軍事作戦を発動する用意をすることを事実上正当化する根拠になり得るものであるとわれわれは考えます。

ロシアの専門家が支持しているもう一つの考え方は、情報空間の軍事利用を禁止して他国の内政に干渉しないことと、国家のデジタル主権を無条件に認めることです。政治的圧力を加える手段として、証拠を示さないでコンピュータアタックを非難することは許されることではありません。

このように異なるスタンスがありますが、いずれにしてもICT環境において紛争を防止し、ICTを軍事目的の追求に利用することを禁止し、国際法の漸進的発展を図り、ICT環境を国際協力の新たな舞台として、その特性に国際法がマッチするようにすることにわれわれは注力すべきであると考えます。

以下は提案です。

われわれのみるところ、国際情報セキュリティの分野で世界の科学者や専門家が真っ先に取り組むべき課題は次のようなものです。

1．ICT 環境において諸国が負う国際的な義務やその違反を摘発したり、違反した主体を特定したりする手続きに加え、ICT 環境で起きた事件にまつわる国際紛争を平和裏に解決する手順を細かく規定する基準を採択して、国際法を ICT 環境に適合するよう漸進的に発展させるための基本的なスタンスを定めた国際情報セキュリティ保障協定を作成する。

2．諸国が ICT 環境において採るべき責任ある行動を定めた原則、基準、規則を取り決めるための指針について、その草案を用意する。

3．情報犯罪に対する対抗措置を定めた協定草案を用意する。

4．ICT 環境における国際義務の内容を国際紛争の防止とその平和的な解決に重点を置いて詳しく記述した追加項目を既存の国際条約に加えるための草案を用意する。

5．ICT 環境において国家に責任がある領域を分け、その境界（ICT 環境のなかで国家主権が及ぶ空間的境界）を法的に確定する手続きを定める一般的な国際条約を作成する。

6．ICT 環境における国際的な事件に対処するため、それらを担当する各国のセキュリティセンターどうしが連携して捜査する手続きに加え、国際法の主体にそうした事件の責任を課すための手続きに関する国際協定を準備する。

7．ICT の機能を実現する製品の安全に関わる問題や、ICT を利用して主権国家の内政に干渉した問題により生じた国際紛争を審議する国際機関を創設する。

上に列挙したうちのいくつかの調査研究は同時進行で行うことができると考えます。

第一に挙げられるのは、関心を有する国家間の双方向での提携を深めることです。こうした提携では、以下に述べる目的のために異なる国の行政機関どうしの連携関係を確立することを目指すべきでしょう。

その目的としては、犯罪行為やテロ計画と実際の犯行に対する対処、連携関係のレベルに対応した包括的信頼醸成措置の実地検証に向けたアプローチの確立、ICT 環境における国家としての責任ある行動を執るための規則の施行があります。

第二に挙げられるのは、国際情報セキュリティを保障する地域間システムを向上させることです。この作業で重要なのは、諸国が地域間連携協定の枠内で引き受けた国際義務に対応しつつ、ICT 環境における国の採るべき信頼醸成措置、自主原則、および責任ある行動の規範に関する勧告の採用方法を確立することです。

最後になりますが、提案したいことがあります。国際機構のひとつかもしくは国連総会国際法委員会に付属する組織として、国際条約の草案を作成する専門ワーキンググループを設置することを検討したらどうでしょうか。そのメンバーには、関心を有する国の法律家、エンジニア、司法機関代表を加えることが重要となるでしょう。専門ワーキンググループが作成した草案文書の審査は、「国際安全保障の文脈における情報および電気通信分野の進歩に関する国連政府専門家グループ（国連サイバー GGE）」が行うことができるでしょう。草案文書の内容の妥協点を探ることは、二国間協議や多国間協議を通じて行うことができるでしょう。

モスクワ大学と東海大学は、ここで述べた課題の解決に、共同研究を行うことも含め、一定の貢献ができるとわれわれは考えます。

こうした連携活動は、グローバルな情報社会が形成されつつあるという条件下で、国際社会を前進させて、さらに安全な世界に近づけることを可能にするでしょう。

ご清聴、ありがとうございました。

モデレーター

石川　一洋
（NHK 解説 主幹、元 NHK モスクワ 支局長）

主権民主主義とサイバーセキュリティ

この論考を 2018 年 2 月半ばにサンクトペテルブルクで執筆している。選挙の結果は現職の大統領ウラジーミル・プーチンの圧勝が明らか。しかし「後継者を誰にするのか」ポスト・プーチンにつながる「プーチンとともに歩む未来」の姿が選挙戦終盤に入ろうとする今も提示できていない。プーチンは過去の実績を誇示する守りの選挙となっている。

通常前の年の 12 月に行われる年次教書演説が 2 月の半ばの段階になっても行われていない。大統領選挙に向けての年次教書はいわば次の任期の綱領となるはずで、ワイノ大統領府長官を中心にごく少数の側近のみによって準備されている。それがまだ発表されていない。そこに天才的ポピュリスト・プーチンの迷いが見える。主権国家ロシアを守ることと同時にグローバルな競争に伍していくのか、その両立が課題であろう。

取り分け、主権と国境が曖昧になるサイバー空間のセキュリティにどのようなポジションを取るのか。主権の護持を第一にしてセキュリティ一辺倒の路線は競争力を失わせる。しかしグローバルな競争に開放することはロシアの主権を危うくする。サイバーセキュリティの問題は、「主権」の護持というプーチン路線に大きな問題を突き付けている。

昨年 12 月 1 日に東海大学平和研究所主催で「サイバーセキュリティに関する日ロシンポジウム」が行われた。ロシアでは、安全保障に関する戦略、ドクトリンはすべて安全保障会議が取りまとめる。その安保会議に大きな影響力を持つモスクワ大学情報セキュリティ学部がロシア側の主催者として参加した。日本からも政府のサイバーセキュリティセンターや外務省の責任者も参加して、サイバーセキュリティ分野における率直な日ロ対話の開始という点で画期的なイベントとなった。

1. ロシアにとって主権国家とは？

全ての国は主権国家である。主権の尊重はロシアの外交政策の基本である。ロシアと欧米の鋭い対立の場となっているシリアについてもロシアの論拠は主権国家シリアの要請に基づくロシア軍の派遣は正当であり、シリア政府の要請によらず、また国連安保理の決議にもよらないアメリカなど有志連合の介入は国際法的に不法行為と見ている。

しかしロシアが主権国家という場合、もう一つの意味がある。取り分けロシアは主権国家であるという場合、そこには特別の意味が込められている。主権とは自ら決定権を有するという意味が込められている。そのため 2015 年 12 月に定められたロシアの「安全保障の戦略」でも安全保障には、軍事や政治経済的なものだけでなく、文化や歴史的伝統、教育や科学、環境なども含まれる。こうしたロシアの考え方からすると世界の中で真の主権国家はそう多くない。EU に政治的経済的な主権を譲り渡したヨーロッパ諸国はもちろん、日米安保の下で防衛面ではアメリカに多くを依存する日本もロシア的な主権国家の見方からすると真の主権国家でないのかもしれない。自ら決定権を有する真の主権国家でありたいロシアにとって、サイバー空間のセキュリティは大問題である。

国境のないインターネット空間を通じた欧米の‘悪しき影響’がロシアの国家体制を揺るがすかもしれないし、逆にアメリカが握るインターネットのインフラストラクチャーからロシアが切り離されてしまう恐れもあるかもしれない。サイバー空間においては、ロシアは自らの‘主権’を確立できていないと言える。それは日本を含めてほかの国も同様であるが。

2.サイバー空間における国境線

そこからロシアにとってのサイバーセキュリティとは、サイバー空間において如何に主権を確立するかという問題になってくる。サイバー空間に国境線を引くことこそロシアのサイバーセキュリティにとって最大の目的と言える。同時にロシアの目的はサイバー空間における国家間の平等な権利を確立することである。情報学部の学部長でロシア安全保障会議の顧問でもあるストレツォフ氏は、今回のシンポジウムの最後に、「インターネットを安全に機能し発展するための概念」という国連コンベンションの案を提示した。「国家はインターネットへの接続をほかの国への影響を及ぼす道具として使ってはならない」「国家は、他国の領内におけるインターネットあるいはインターネットへのアクセスを制限してはならない」「国はインターネットガバナンスにおける平等の原則と国家がその国のインターネット規範を定める主権的な権利を認めなければならない」ロシアにとってのサイバーセキュリティとは、サイバー空間における主権の確立、つまり国境線の画定こそが最重要課題であることが、このロシア案にも示されている。

3.では日本のサイバーセキュリティに関するポジションはどうなのだろうか

「自由、公正かつ安全なサイバー空間は、地球規模でのコミュニケーションが可能なグローバルな共通空間であり、国際社会の平和と安定の礎である。とりわけ我が国は、サイバー空間における多様な価値観を認め、自立性を重んじ、そして人々の言論や企業行動を法の支配により保障することが、国際社会の平和と安定を実現し、ひいては繁栄に導くと確信している」(サイバーセキュリティ戦略)。日本はサイバー空間においても既存の国際法が順守されるべきだとしつつ、グローバルな共通空間と規定する。今回のシンポジウムで河野が指摘したように、そもそも国境線という概念がサイバー空間に成立するのかどうか疑問であり、日本のサイバーセキュリティ戦略の中には国境線という言葉はない。日本のサイバーセキュリティ戦略の立案者である三角はサイバー空間が国家ではなく民間投資によって築かれている人工空間であることを指摘し、民間においてサイバーセキュリティ対策への投資がやむ得ないコスト負担ではなく、価値を産む投資活動として認識されることが必要と指摘している。アメリカと同じく、自由・自立という価値観を重要視する日本と各国の主権が守られるべきだとするロシアの間では大きな考え方の違いがある。

そうした考え方の違いがあるからこそ、政府関係者も交えながらも日ロ双方の専門家がサイバーセキュリティに関して自由に討議するセカンドトラックの試みは重要である。サイバーセキュリティが国家間の対立の場でなく協調の場とするためにも、国際的なサイバーセキュリティにロシアがどのように建設的に関与していくのかが重要である。東海大学とモスクワ大学によるサイバーセキュリティ対話の果たす役割は大きく、継続に期待したい。

プレゼンター

三角　育生

（内閣審議官）

多様な者の連携によるサイバーセキュリティの取組みの重要性

1．はじめに　―背景及び認識

情報通信技術（ICT）が経済社会活動の不可欠な基盤としての位置づけが増々高まるなか、サイバーセキュリティ確保の重要性も増々高まっている。サイバーセキュリティに関わる事件・事案の報道も頻繁になされ、専門家のみならず多くの一般の者においても重大な関心事になってきている。しかし、我が国では、サイバーセキュリティを、技術的な課題と捉える者が多い。このため、サイバーセキュリティの取組みを、自らの組織の課題として、また、身近な課題として考える者が少ない。そして、サイバーセキュリティの取組みについて、どこまで対策を行うべきか、どの様な対応をすべきかの判断が困難になり、コスト負担であると考える者が多い。

こうした状況は、我が国の1960年代における公害の議論に似ていると思われる。工場からの排煙による大気汚染などの公害問題が大きな社会問題となっていた。国は公害対策のための法律や基準を整備し、また、工場は設備投資し、市民は光化学スモッグなどの注意すべき現象への対応をした。当時、公害対策は、ある意味やむを得ないコスト負担と捉えられたかもしれない。しかし、皆による努力の結果、現在は、大気もクリーンになるなど目覚ましい公害対策の成果が得られている。そして今日、多くの場合に、こうした対策はコスト負担というよりも、環境にやさしい取組みとして肯定的に認識されている。むしろ、このような取組みが、省エネによるコスト削減、さらには、環境ビジネスといった利益を生む活動と考えられるようにもなってきている。

サイバーセキュリティについて考えると、サイバー空間は、不正プログラムなどが蔓延した状態にあると言える。あらゆるところでいつでも生じうるサイバーセキュリティ事象に、特定のサイバーセキュリティ専門組織が、事象発生の都度対応していくのでは間に合わない。そこでICTを開発し、利活用している関係者の各々が力を合わせてサイバー空間を強固にしていく必要がある。

特に、サイバー空間は、その大半は民間投資によって構築された人工空間であることに留意が必要である。サイバー空間をより安全なものとしていくため、民間においても、サイバーセキュリティ対策への投資が進むことが重要である。そのためには、サイバーセキュリティ投資が、やむを得ないコスト負担ではなく、肯定的に捉えられる価値を産む投資活動として認識されるように促していく必要がある。本稿では、こうした背景から、サイバー空間の安全を確保するために、経済的側面を考慮した取り組みが重要であることを強調し、その観点からの最近の我が国におけるサイバーセキュリティへの考え方と具体的な取組みについて紹介する。

2．我が国のサイバーセキュリティ戦略

我が国のサイバーセキュリティ関連施策は、2015年9月に閣議決定したサイバーセキュリティ戦略（以下、「2015戦略」という）に基づき実施している。同戦略では、サイバー空間を「無限の価値を産むフロンティアである人工空間」と定義した。これは、ICTが、公開鍵暗号が電子商取引の発展に不可欠であったように、ビジネス上の付加価値を産む基盤となっているからである。このように定義することは、サイバーセキュリティへの民間投資を促すためにも重要である。

同戦略では、主要な政策分野として、経済社会の持続的発展に関わるもの、国民や社会の安全安心に関するもの、我が国及び国際的な安全に関するものという3つの柱と、研究開発、人材育成といった横断的・基盤的な分野に整理して戦略を示している。

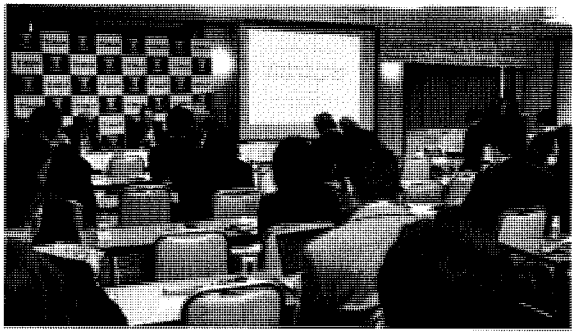
具体的には、第一に、経済社会の持続的発展に関わる施策として、企業の事業戦略にサイバーセキュリティの観点の導入を促進するものを重視した。例えば、今日、インターネット技術を活用した防犯カメラなどの機器すなわちIoT（Internet of Things）の導入が指数関数的に増大している。こうした機器には、モノとして高い安全性と品質についての顧客からの要求がある。特にIoT時代には、モノがチップとソフトウェアで機能を発現することから、モノづくりの産業において、顧客の要求に応えるためには、品質としてのサイバーセキュリティや製品やサービスの安全を保証するためのサイバーセキュリティが競争力の源泉となる。したがって、モノづくりの事業戦略として品質としてのサイバーセキュリティ確保が付加価値を産むものであるといった認識を高める経営層の意識改革の促進が重要である。関係省庁が連携して、経営者向けのガイドラインの整備などの関連施策を推進しているところである。

また、サイバー空間において経済社会活動を行っていくためには、サイバー空間が安全で信頼できるものでないとならない。このため、サイバーセキュリティ戦略の第二の柱として、サイバー犯罪から国民を守り、また、政府や、電力、通信などの重要インフラ事業者が提供するサービスの安全性・安定性を守るためのサイバーセキュリティ対策を行うことを示している。さらに、第三の柱として、インターネットはグローバルなものであるため、国際連携を推進する。加えて、安全保障にも関連することから自衛隊等実施組織において任務保障の観点からのサイバーセキュリティの取組み強化をすることとしている。さらに、我が国は、2020年開催予定の東京オリンピック・パラリンピックにおけるサイバーセキュリティ確保の観点からの体制整備も着実に行うこととしている。

3．戦略の中間レビュー

2015戦略の期間は3年間であり、決定以来概ね2年経った時点（2017年7月）で政府は戦略の中間レビューを実施した。

これは同戦略決定以来、サイバーセキュリティを巡る状況もだいぶ変化してきたから



である。例えば、2016年秋に大規模なDDoS（Distributed Denial of Service）攻撃のためにtwitterなどの事業に支障が生じた事件や、2017年5月に短時間のうちに150か国以上、数十万台のコンピュータが不正プリグラムに感染した身代金攻撃などの事件は記憶に新しい。こうした事件は、サイバー空間を利活用した円滑な企業活動を阻害し、経済の発展を阻害する。このため、このような状況の変化を踏まえて、残り1年間で2015年戦略に基づきどのような施策を優先的に促進するかを明らかにするべく中間レビューを行ったものである。

ここで基本となる考え方は、公害対策のときも同様であったが、関係者が皆で予防も含めて取組むというものである。サイバー空間を皆でクリーンにしていくという点で、公衆衛生のアプローチにも似ている。

そして、このサイバー衛生の考え方を踏まえて、特に優先的に取り組むべき事項として、①ボットの撲滅対策、②情報連携のネットワーキング、③東京2020のための準備加速、を取り上げた。

その他、サイバーセキュリティを通じた経済社会の発展を促す取り組みとして安全なIoTシステムの実現に向けた国際標準化の取り組みや、先端技術を防護すべく大学等のセキュリティを高める、国際連携を強化するなどの強化策を盛り込んでいる。

以下、優先的に取り組むべき3つの事項などについて簡単に紹介する。

まずボットの撲滅対策について述べる。ボットは、攻撃者が感染させたコンピュータやIoT機器をロボットのごとく遠隔で操ることができるようになるもので、多数のボットをネットワーク化させて、攻撃者が大規模な攻撃拠点としてサイバー攻撃をできるようになるという点で脅威となる。DDoS攻撃のみならず、その他の攻撃や犯罪の温床ともなる。特に脆弱なIoT機器が増大するなか、サイバー空間をクリーンにするための早期の取組みが求められる。

このため、総務省を中心に、サイバー攻撃観測網やネットワーク上の脆弱なIoT機器の探索手法を活用して、国民生活・社会生活に直接影響を及ぼす可能性の高いIoT機器を中心に、インターネットに接続されたIoT機器について調査を実施することとしている。そして、サイバー攻撃の対象になりやすい脆弱なIoT機器を特定した場合には、所有者等に対して注意喚起を実施し、また、必要に応じて製造事業者等に対して脆弱性に関する技術的な情報提供を実施する取組みを行う。このための必要な法改正も行ったところである。

次に情報連携ネットワークの形成である。サイバー攻撃の脅威などについて認識したときには、被害が拡大しないように、いち早く技術専門家などの関係者間で脅威情報、脆弱性情報、対策情報などを共有し、関係者皆が連携して具体的な防護の取組みを行う必要がある。しかしながら、サイバー攻撃を受けた組織は、悪い評判や影響がでることを恐れて情報共有に消極的なことが多い。そうすると当該組織に所属する技術専門家が他の組織の技術専門家との間で円滑に情報交換することが難しくなる。

このような制約を克服するために、サイバーセキュリティ専門家などから構成するコミュニティを形成し、一旦コミュニティに参加したときには、その構成員が守秘義務を負うといった制度整備が必要となる。こうしたことを担保すべく、サイバーセキュリティ基本法の改正案を閣議決定しており、現在、国会におけるサイバーセキュリティに係る審議が深めていただくことを期待しているところである。

第三に東京2020に向けた取り組みの加速化である。質の高く安全なオリンピック・パラリンピックゲームの開催を成功させるためには、セキュリティが重要である。ICTの普及に伴い、サイバーセキュリティもその重要な要素となっている。特に、ゲームが着実に行われるためには、電力、放送などの不可欠なサービスの確保が必要となる。これらサービスが途絶することなく提供されるには、例えばバックアップ電源を置くなどの物理的な対策とともに、サービス途絶の原因事象の一つとして注目されるサイバーセキュリティ事象の対策も不可欠となる。

このため、不可欠なサービスを提供する事業者に、そのサービス維持などの観点からのサイバーセキュリティ・リスクマネジメントを政府が策定したマニュアルに基づき実施していただいている。このリスク評価等の取り組みは東京2020までに計6サイクル行うこととしており、すでに第2回目が実施された。加えて、個別事業者によるリスクマネジメントは事業者毎の部分最適になってしまうと考えられることから、連関する事業者間の取組みも含めた横断的・全体的なリスク評価を政府として行っている。

また、事前の防護を十分に行ったとしても、何らかの事象が発生した場合に適切に対応する能力が必要である。このため、大会期間中にサイバーセキュリティ事象を関係者間で調整し対策を促すなどの活動を行うサイバーセキュリティ対処調整センターを2018年度中に設置することとしている。その際、現実のサービスや安全確保の取組みと緊密連携する必要があることから、物理的なセキュリティも含めて取組む組織と緊密連携していくこととしている。

4．おわりに　―次期サイバーセキュリティ戦略策定に向けた議論

2015年決定の戦略は、2018年夏頃までが戦略期間であることから、現在、次期サイバーセキュリティ戦略の検討が政府において行われている。同検討では、上述した2015戦略や中間レビューにおける基本的な考え方を維持している。そして、それぞれの者が提供するサービスや業務を全うするためにリスクベースで、サイバー関連の多様な関係者の皆が力を合わせて取組む、すなわち協働・連携といった点を強調している。

こうした取組みを着実に実現していくためには、関係者のサイバーセキュリティに係る能力を高めていくことが重要である。一般にサイバーセキュリティ人材として、高度な技術を有する人材の発掘・育成が注目されることが多い。しかし、それのみでは不十分である。ICTが経済社会の基盤として今後増々重要になっていくなか、組織の経営層の意識改革、さらに、ICTやサイバーセキュリティの観点も踏まえた経営戦略を企画立案し、実務者を率いてリスクマネジメントもしていくような指揮官的な人材である戦略マネジメント層の育成が我が国として急務である。我が国として、次期サイバーセキュリティ戦略の策定に向けての議論がさらに深められ、それを踏まえた施策が実施され、多様な者が積極的に参加できる安全なサイバー空間の実現・維持に貢献していくことが重要であると考える。

プレゼンター

アナトリー・ストレルツォフ

（モスクワ国立大学情報安全保障問題研究所 副所長）

国際情報セキュリティの法的保障に関する基本的問題

国際情報セキュリティの法的保障に関する重要問題の一つは、情報通信技術（ICT）が悪用され、国際平和と安全に脅威をもたらすことに対して国際法をどのように適用するかということです。「国際安全保障の文脈における情報および電気通信分野の進歩に関する国連政府専門家会合」の報告には、このような脅威によく対抗するには国連加盟国が共同して対処する必要があり、なかでも、国際法の然るべき規範とそうした規範から導き出される、諸国の責任ある行動を定めた規範、規則、原則の確立が必要であることを加盟国が共通の理解としなければならない旨述べられております。

1．ICT 環境における国際関係に国際法を適用する問題はまだ解決されておりませんが、国際法の規範や原則に基づかない解決法があると考えることが果たしてできるでしょうか。

こうした方法以外にないと考える理由を以下に述べます。

一つには、ICT の悪用に関わる国際関係を規制するために国際法に新たな分野を付け加えることは、そうした提案があることは承知していますが、現状では不可能、かつ不適当であると考えます。不可能な理由は、現在の国際関係が非常にダイナミックなものであるということ、加えて、国連安全保障理事会常任理事国間に蓄積された不信感により、穏当な国際関係が望める状態にないため、そのなかで、このような難しい問題でコンセンサスを得ることはきわめて困難であると思われるということです。また、不適当であるという理由は、いかなる場合でも新たな規範や原則は既存の規範や原則に基づくものになるとすることには、十分な根拠があるといえるからです。

二つ目は、既存の国際法の規範や原則は、歴史による検証に耐え、それを国際安全保障の分野における国際関係を律するメカニズムとしてみるとき、各国連加盟国の立ち位置が一定程度一致しているからです。また、個々の問題の判定に国際法の原則や規範を適用してきた経験の蓄積が各国には現存します。

三つ目は、既存の規範や原則は、ICT の悪用により生じる安全に対する脅威に各国が対抗するためにこれらが使用されることを妨げないということです。そうであれ、ICT 環境にまつわる事態を専門に取り扱う国際法の規定がないと、ICT 環境で生起する事態を誤って解釈するおそれも存在します。こうした誤った解釈の結果、国際紛争が発生する危険が

高まり、国際平和と国際安全を真に脅かす事態になるかもしれません。

以上のことから、ICTについては、その悪用に対抗して、平和を脅かす新たな脅威とはならない限りで対抗策を講じるために国際法を適用することを研究してみることが大事だと考えます。

事態がこのように望ましくない方向に発展する危険を弱めることについては、ICT環境における諸国の責任ある行動を定めた規範、規則、原則と信頼醸成措置に関する提言が国連政府専門家会合で採択されたことは、大きな一歩です。この提言はICT環境に関連した国際紛争を防止するためになされました。ICT環境における諸国の責任ある行動を定めた規範、規則、原則を普及させるための方法を研究することを目的として、ミュンヘン安全保障会議における討論（2017年）の結果、サイバー空間安定化グローバル委員会が設置されております。

国際関係の新たな分野に国際法を適用できるようにする方法を追求する次の段階では、実体法の規定を遂行する場合の国家の権利義務を定める、国際実体法と国際手続法の規範と原則とを検討対象とすることが避けられないと考えられます。

2．一連の国連政府専門家会合が作成した、「諸国が責任ある行動をとるための規範、原則及び規則」は、法律文書の体裁を整えた上で、国連加盟国が採択することになるでしょう。そうなれば、ICT環境は国際法の対象となり、ICT環境そのものの評価が関心の対象となるでしょう。

技術的な面からすれば、ICT環境とは、物理的な場所とは関係なく存在する、グローバルなIPアドレス体系の空間のなかで、統一されたプロトコールに基づいて互いに作用し合うところの、情報の処理・保存・転送・拡散・提供の対象の総体のことであります。

したがって、ICT環境は、土地、空域、水域といった国家の領域の構成要素ではありません。この環境は人工的に作られ、人々の活動にによって存在を支えられています。この意味でICT環境は、法的フィクションであるともいえ、その体裁をとった上で、国家の領域の一部とみなすこともできるのです。そうなれば、ICT環境においても「主権」という概念を通用させることが可能になるのです。

ICT環境にまつわる社会的諸関係の主要な特徴は、この環境に存在する対象（情報、情報システム、ICT、情報処理プロセス）に加え、ICT環境の対象に関わる法的諸関係の生起、変更および終了という法律行為も、その関係主体と同じく仮想的性質を持っている、つまり見えない（形がない）ものであるということです。それであれば、国家主権をもとに諸関係の法的規制を行うためには、ICT環境で生起する、法的対処を必要とする事件やプロセス、さらには諸関係の主体の帰属証明（有責帰属証明）を客観的に実現する方法を採用することが重要と思われます。

国際関係の対象となるICT環境は、グローバルなサイバー空間に包摂されていて、安全に利用されるべきものであるという特質があります。こうした性質は、一定の場面では国の領土保全や政治的独立という側面として考えてみるとよいでしょう。国ごとのインターネットセグメントをグローバルなICT環境に包摂することが妨げられると、現代社会がそれを安全に利用できなくなる上、社会生活のあらゆる分野の機能が毀損されかねません。

3．「主権」概念をICT環境に適用しようとすると、他にも問題が出てきます。次にそのいくつかをお話します。

まず、ICT環境では主権に空間的な制限がないため、いったいどこである国の主権が終わり、別の国に主権が移るかを決めることができないこと。この点が、国別のインターネットセグメントをめぐって武力抗争が発生したときに境界を確定しようとしたり、主権のある領土内や、とくに国別インターネットセグメント内においてそのセグメント独自の法的体制を定めるなどの措置をして国際的な義務を履行することを担保しようとしたりするとき、きわめて重要になってきます。

IPアドレスとドメイン名の分配システムが持続的かつ安全に機能し、そのシステムがグローバルに機能することを保障する国際的な義務を追っている国家というものが存在しないこと。この理由のひとつは、こうした機能を担っている組織は、インターネットソサエティ（Internet Society - ISOC）やワールド・ワイド・ウェブ・コンソーシアム（World Wide Web Consortium - W3C）、アイキャン（Internet Corporation for assigned names and Number - ICANN）、アイアナ（Internet assigned number Authority - IANA）というアメリカ合衆国の司法権のもとにある非営利団体であって、これらの組織は国際法上の法的能力、行為能力、不法行為責任能力を有していないことです。

国境を超えて（プライバシー権や創作物利用権などの）人権や国民の権利が尊重されることを法的に担保する分野では、包括的な国際協力法がいまだ存在しないこと。ご存知のように、これらの権利を尊重することは国家の義務ですが、もし情報が技術的原因で国外に出てしまえば、こうした国際的義務を国家が遂行することは物理的に不可能になります。

コンピュータ犯罪に対抗する分野においても包括的な国際協力法が存在しないこと。ご承知のように、こうした犯罪の大部分は国境を超えて行われるので、その捜査には他の国のインターネットセグメントにある情報が必要になりますが、現在行われている捜査方法ではそれほど効果が上がっていません。ですから、こうした困難を克服しようとしてサイバー空間に関するブダペスト会議を企画した人々の意図は理解できます。しかし、ご存知のように、ロシア連邦はこの会議に加わりませんでした。その理由は、コンピュータ犯罪の捜査主体が他国のインターネットセグメントにアクセスすれば、捜査だけにとどまらず、ついでにその国の安全保障にとって好ましくない目的を追求するのではないかという疑念を晴らすことができなかったからです。

4．結論として、情報セキュリティの司法面によるサポートを強化するための提言をまとめることができると思います。

この課題の実現は、既存の国際法の法源を必要に応じて補足し、記述をより明確にしたものを採択することで可能になると考えます。

ところで、国連憲章をよく読むと、その規定のすべてがICT環境における諸関係に適用できることがわかります。それと同時に、補足を追加し、そこで国連憲章が、ICTが「武力」および「武力攻撃」の手段として使用される場合に適用されることを明確にすることが重要であると考えます（国連憲章第2条の4および第51条にそれぞれが該当します）。ICTは武器であるとは定義されませんが、なかには軍事用ではない装置や機構であっても武器としての能力をもたせることができるものがあり、そのため国連憲章第51条の意味する武

力攻撃に使用できることを認識することが重要です。「武力攻撃」をそのように解釈した先例が、2001年9月11日にアメリカ合衆国で起きた悲劇を国連安全保障理事会で審議され、採択された決議文（2001年）にあります。この攻撃は、武器ではないことが明らかな民間航空機を使って行われたのです。

1970年の国際法の原則に関する宣言を分析した結果からも同様の結論に達することができます。この宣言が規定する内容は、ICT環境の規制にも使えます。そして同時に、新たに生じた国際的な人間活動の分野の特性を考慮するなら、補足を付け加えることも必要です。その補足では、ICT環境に適用される各条項をさらに明確に記述するとよいでしょう。例えば、「領土保全」、「政治的独立」、「主権平等」などの概念をさらに詳述することです。

また、ハーグ条約とジュネーブ条約により確立された、武力紛争法と国際人道法の原則と規範も、ICTを用いた攻撃があった場合に敵に対する「強制力」として適用することを妨げるものではありません。とはいえ、やはりより詳細な定義付けは必要でしょう。とりわけ、次のような法的メカニズムを整えることが合理的でしょう。それは、武力紛争に関係してくる国内のインターネットセグメントを中立国のインターネットセグメントから隔離する法的メカニズム、次いで、それなくしては国際人道法による軍事行動の抑制が不可能となる、ICT環境にある民間目標と軍事目標を確定する法的メカニズム、そして、戦争中の一方の側が犯した、国際人道法の制限行為に関する疑いを契機として権限ある機関によって行われねばならない国際捜査、およびICTの違法使用の事実の客観的な糾明、さらにはそうした違法使用の有責者の帰属証明を行う法的メカニズム、であります。

イラクにおける大量破壊兵器の発見（2003年）のケースであったような、国連安全保障理事会が状況判断を誤るというリスクを最小化しながら、武力攻撃の手段としてICTを違法に使用した主体を糺明するには、ICT環境で生起する、法的対処が必要な事件やプロセスを客観的に明らかにし、違法行為の主体である者の帰属を特定するシステムを創設する事が可能かどうかを考究してもよいでしょう。

これまでに述べたアプローチは、国際法をICT環境に適用できるよう強化するプログラムを形成し、法の進化の優先順位を策定することによってそうしたプログラムを実体化していくためのロードマップを作り上げる推進力となるでしょう。

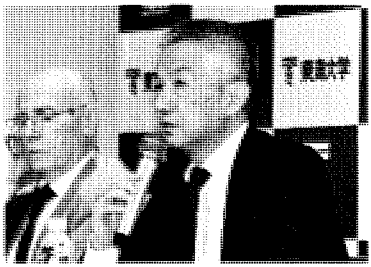
こうしたプログラムによる最初の事業は、ICT環境における諸国の責任ある行動を定める規範、規則および原則を採用するためのガイドラインの作成になろうかと思います。この事業を実現するための「ロードマップ」があれば、国連加盟国がICT環境において国際紛争を防止するために払う努力が調整され、かつ、政治学者、法律家、最優先の研究分野で実務処理を行う専門家を結集させる条件が整ってくるのではないでしょうか。

プレゼンター

中嶋　卓雄

（東海大学情報教育センター 所長）

グローバルパラダイムシフト時代におけるサイバーセキュリティ



1．はじめに

1980年代のインターネット創成期において、サイバー攻撃は攻撃者にとって利益はなく愉快犯としての試みのような傾向があったが、近年、個人から組織に対する攻撃も増え、国家レベルのサイバーセキュリティに関係した組織が作られる時代になってきている。インターネットがグローバル化し、全世界に影響を与えるインフラとして政治的にも経済的にも重要な技術となっていることがその背景にある。このようなグローバル化した時代は、言葉を変えれば種々の既存概念を超える時代、すなわちパラダイムシフトする時代となってきている。特に、最近のサイバー攻撃は国家を対象とした金銭目的や政治的な目的の攻撃も増加しており、大きな政治問題となりつつある。今回の報告では、サイバー攻撃が成立し続ける本質的な要因を検討するとともに、攻撃の検知手法について紹介する。また、我々が提案してきた攻撃検知手法について紹介する。

2．パラダイムシフト

パラダイムシフトとは、従来考えられてきた認識や価値観が劇的に変化することと言われ、インターネットの拡大と共に、国家で分離された情報がシームレスに繋がる事や、グローバル社会を対象として、組織としてのみ発信できた情報が個人として発信可能になった事により、大きなパラダイムシフトが起きていると考えることが可能である。特に、2010年から始まったアラブ地域における民主化運動である「アラブの春」は、インターネットによる情報の高速な伝播が大きな起因になっており、従来の治安統治策の一つとしての情報統治がインターネットにより大きくパラダイムシフトしたとも考えることができる。このような時代において、インターネットを媒体とした情報発信、およびその逆の意味を持つ政治的なサイバー攻撃は年々増加しており、以前より社会的および経済的な影響を持つようになってきた。

3．サイバーセキュリティ

サイバー攻撃は、以前は個人をターゲットにした攻撃であったが、現在は企業や国家を対象としており、特に経済的および政治的な効果を狙ったものにシフトしてきている。特に、国家のインフラとなる、水管理施設、原子力発電所を含む電力管理施設などへのサイバー攻撃が発生している。2015年においては、430,000,000もの新しい固有なマルウェアが発見されており、2017年5月においては、WannaCryと呼ばれるランサムウェアが150国以上に広がり、230,000以上のコンピュータに感染した。このようにサイバー攻撃の目的も、政治的な優位性の確保や経済的な利益に繋がる方向にシフトしてきており、テロリズムに繋がる可能性もある。今後、IoT（Internet of Things）と言われるように多様な電子機器がインターネットに接続する時代となり、各種の電子機器に対するセキュリティ対策が必要になってきている。

3．1　サイバー攻撃の原因

サイバー攻撃の原因として、ソフトウェアやネットワークの脆弱性が挙げられるが、攻撃が成功する要因としては、人間が持つ脆弱性、認証をしないまま信用する行為、が原因となっている場合が多い。例えば、認証もできていないUSBメモリーをそのままコンピュータに差し込んだり、確実に送信元が確認できない状況で、メールの添付ファイルを開こうとしたり、など、多くの人間の行為がサイバー攻撃を受ける要因となっている。本来、インターネットプロトコルは一部の限られたコミュニティの中で利用され、設計されてきた。そのため、相互に接続できる様々な機能を持っているが、セキュリティに関する考察が必ずしも十分ではなかった。現状においてもE-mailのデータはほぼ暗号化されずネットワークを流れているため、特定個人のメールを途中で監視することも可能である。

特に代表的な攻撃の原因は、送信元の偽造である。インターネットを流れるデータをパケットと呼び、流れる方向性を示す制御データがパケットヘッダに格納されるが、その制御データの一つであるSource（送信者）IPアドレスは、偽造が可能である。このプロトコルは郵便システムと同じであり、送り元の住所は偽造が可能である。相互通信は成立しないが、送り先に対する攻撃、嫌がらせとなる可能性がある。相手に大量のSource IPが偽造されたパケットがサーバに到着することにより、そのサーバのサービスが中断せざるを得ない状況へと強要する攻撃であるため、DoS（Denial of Service）と呼ばれている。特に、多くの攻撃元が分散して攻撃者から制御できるネットワーク上のBOTと呼ばれるホストから攻撃することを、DDoS（Distributed DoS）と呼ばれている。現在、The Onion Router（Tor）と呼ばれるパケットの流れを制御する技術と組織が存在する。これは、偽造IPを持ったパケットの流れを制御し、このネットワークからパケットを出力することによって、偽造元を突き止めようとするバックトレースを出来なくする技術であり、すでに利用されている。このような技術が悪用される事により、国家を超えたデータ転送ルートを制御することが可能となり、攻撃者を特定することを困難にさせている。

3．2　サイバー攻撃の対象

従来、サイバー攻撃の対象は個人であったが、政治的・経済的な目的の変化のため、攻撃対象も変化しており、特に生活基盤に関係する情報管理システムへの攻撃に変化してきている。基盤の情報はSCADA（Supervisory Control and Data Acquisition）システムよって管理されており、そのシステムにセキュリティ管理を強化する方向で実装が進んでいる。現在、サイバー攻撃の対象は、水やガスの供給システムだけではなく、鉄道の信号管理システム、車生産工場、さらには原子力発電所など広範囲に広がっている。今後は、各システムに対する固有な攻撃に対する防御手法を検討する必要がある。

3．3　セキュリティとプライバシー

セキュリティの強化とトレードオフの関係にあるのがプライバシーの保護である。米国では、PRISM（communication surveillance program）というプログラムがNSAにより、実施されてきたと言われており、Google、Yahoo!、Facebook、Apple、AOL、SkypeやYouTubeなどの企業も協力して個人のメッセージを監視してきた事実が表面化している。このような監視システムが存在する一方、SNS（Social Networking Service）により個人の情報を積極的に公開する流れが活発になってきている。写真をSNSにupすれば、GPSの機能により写真撮影した場所が特定できるが、そのような機能があることを認識していない人も多い。今後、このような意識せず流出した個人情報をきっかけとして犯罪に繋がる可能性もあり、各種のサービスについて正確な知識が必要となる。

3．4　サイバー攻撃の分類

サイバー攻撃はターゲットした組織のサーバへの攻撃のため、そのサーバの脆弱性をスキャンしながら情報を収集する。そのサーバが、Webサーバ、データベースサーバなどによって、異なる攻撃手法が存在する。しかし、徐々にシステム管理者にセキュリティに

関する認識が広まり、直接的なサーバへの攻撃は増加していないと思われる。しかし、特定のターゲットを決めた「標的型攻撃」が近年増加してきている。特に、メールなどにMalwareを添付し、ユーザがそのファイルを起動する事によって感染する仕組みになっている。Malwareであっても、拡張子が.pdfや.zipなどであれば、ユーザは安心してメールの内容に注意せずクリックし、Malwareを起動する結果となる場合がある。最近のMalwareは、複雑に難読化されており、添付ファイルを解析するだけでは、Malwareか否かを判定すること、およびそのMalwareの動作を解析することが困難になってきているので、ユーザのセキュリティに対する認識の強化も重要な課題である。

4．攻撃の検知手法

4．1　サイバー攻撃の検知手法

サイバー攻撃を検知する手法は、基本的にデータサイエンスで利用される手法と同様である。まず、分類では多くのデータを、攻撃データ or 通常データに分類する手法と同じであり、エントロピーなどのバラツキ度を評価する指標により、攻撃データと通常データの差を、複数のパラメータにより分析し、攻撃データを発見することが可能である。特にクラス確率推定などにより、確率的に扱うことが可能であり、また、そのクラスに属するスコアを求めるスコアリングなどにより、確率推定として扱うことができる。また、回帰手法においては、攻撃データとみなす値を推定することが可能となる。このように、データマイニングの分野で研究されてきた技術がそのままサイバー攻撃の検知手法にも適用できる。

4．2　提案してきた検知手法

我々は以前から、サイバー攻撃のネットワーク上での検知手法を研究してきた。特に注目してきたのは、DDoS/DoS攻撃であるが、検討した手法はコンピュータの挙動を変える攻撃、例えばMalwareに感染して、C&CサーバからMalware本体をダウンロードする時などにも適用可能である。

まず、特定のサイトに流れる全てのパケットのSource IPアドレスをベースとしたエントロピーによる検知手法を提案した。パケットのSource IPアドレスのバラツキ度は、組織において固有な値を持つという認識を前提としている。もし、DoS攻撃が起きれば、特定のSource IPアドレスを持つパケットの頻度が多くなるので、通常の固有なエントロピー値より小さな値となり、逆にDDoS攻撃が発生していれば、固有なエントリピー値より大きな値となる。この技法は、単にDDoS/DoS攻撃に有用なだけではなく、通常のネットワーク上の振る舞いと異なる振る舞いが発生した時の検知に有効である。また、ピアソンのχ二乗値によっても、期待する値がビンに均等に分散されるのか否かによって、データの偏りを評価することが可能であり、結果としてサイバー攻撃の状態を検出することが可能であり、そのような検知手法を提案してきた。最近は、PDFファイルに含まれるMalwareの検出を、one-class SVM（Support Vector Machine）によって検知する手法を提案・評価している[1]。

5．おわりに

本報告において、パラダイムシフトが発生している社会状況において、その原因にもなっているインターネットの功罪について考察し、さらに広範囲に広がりつつあるインターネット環境において、十分なセキュリティが保たれることが重要であることを示した。

参考文献

[1] Mai Iwamoto, Shunsuke Oshima and Takuo Nakashima, A Malware Detection Method based on OC-SVM Focusing on Features of PDF Files, ICIC Express Letters - An International Journal of Research and Surveys, Vol.11, No.11, pp.1611-1618, Nov, 2017.

プレゼンター

パヴェル・カラセフ
（モスクワ国立大学情報安全保障問題研究所 主任研究員）

グローバルパラダイムシフトの牽引力としてのICT
―社会文化・政治・経済・技術の面から見たトレンド

近年の統計データによれば、2016年から2017年にかけて、それまでの前提を覆すような顕著な変化が起こり、事態は新たな地平に移っております。それは今やすでに地球の人口の半分である39億人がグローバルネットワークであるインターネットユーザーになっているということです。デジタル・エコノミーの核となる企業の数も増えています。行政に積極的にICTを取り入れることで従来の仕組み（課税・規制・認可などの手続き）を変えて「電子政府」を目指す国も増え続けています。ICTを人間生活のすべての分野に次々に導入していった結果に待っているものは、情報通信システムは途切れることなく機能し、信頼性が高いものであるに違いない、という危険な思い込みに頼らざるを得なくなることです。そのとき、ICTにつきものの脆弱性が新たな脅威になるでしょう。

ICTはここ30年の間に、社会、文化、経済、軍事それに政治の分野にパラダイムシフトをもたらしました。ここで関連してくるのは、膨大な情報空間の獲得、国益実現に特化したICTデバイスの登場、「第六の波」、「インダストリー4.0」といった事柄です。ここで述べた分野のパラダイムシフトは、一方では社会、文化、政治、経済の発展をもたらしましたが、他方では新たな脅威を惹き起こしています。

人類の発展の今の段階においては、普及したICTが情報を進歩のための戦略的資源に変え、新しい社会や経済が形成されるところまで来たと言うことができます。まさにこの日本で「情報化社会」の概念が実際に生まれたのです。ここで東京工業大学林雄二郎教授が行った、日本の経済社会の発達理論を構築することを目指した研究を紹介したいと思います。ご存知のように、情報化社会の特徴は、情報技術があらゆる生活分野に浸透し、情報、知識、情報技術が社会生活に占める役割が大きくなる点にあります。そうなるための要因は、個人同士の情報交換の効率化、世界の情報源への個人アクセスの実現、情報機器や情報サービスに対する個人需要の充足などを可能にするグローバルな情報空間が構築されることです。

情報化社会の成立と発展は、社会文化におけるパラダイムシフトを意味します。情報というものの捉え方、コミュニケーション文化、関心を向ける範囲や交友範囲といったものが変化したのです。ソーシャル・ネットワーキング・サービスのフェイスブックには現時点で20億人以上が登録しています。フェイスブックの「ともだち」には、実際には一度も会ったことがなく、同じオンラインコミュニティに属しているだけの人も含まれます。情報空間で個人の身元を表す特異な「パスポート」とも呼べるSNSのプロフィールの裏に、誰が、あるいは何が隠れているのでしょう。ここで私達は事物の二面性に当面するわけです。ICTは現実に人々に広大な交流の場を提供します。しかし人間の能力には限りがあり、自分の周りにある情報のすべてを批判的に再評価することはできません。そこにつけ込む悪意のある情報の餌食になる恐れが出てきます。そうした情報はいろいろあり、犯罪やテロ、あるいは政治的目的をもったものもあります。

パラダイムシフトが起きた分野には他のものもあります。それは各国の対外政策です。

ICTは、新たな対立の場としての情報空間が生まれる原因になりました。サイバー空間は、すでに新たな軍事行動の舞台として国家や団体のレベルで認識されています。軍事目的や政治目的での利用のためにICTのツールを開発している国はますます増加しており、「サイバー大国」クラブのメンバー数はすでに60カ国を超え、会員になろうと受付に並んでいる国の数はさらにそれを上回ります。ICTを使って社会秩序の安定を損なったり、破壊思想を宣伝しようしたりすることで大衆心理が操作される危険も増しています。今のところサイバー兵器の拡散は放置状態で、それは現在の国際的安全保障制度の枠外でますます進行しています。それ自体がパラダイムシフトである世界の多極化はますます強まっていますが、それは国家であれ、疑似国家集団であれ、また単なる行為者であれ、ICTツールが他の分野における己の非力さをカバーしてくれるだろうと考えるからです。ロシアは長年、サイバー兵器の開発や使用を禁止するための条約案を提示してきました。つまり、紛争を正当化したり、調停したりするのではなく、防止することを主張してきました。サイバー攻撃が誰によるものかわからない状況では、政治の都合で犯人が決められてしまうかもしれません。そうして犯人とされたものは制裁だけでなく暴力的な報復に見舞われるかもしれないのです。各国政府専門家をメンバーとする国連特別作業部会が、諸国が採るべき責任ある行動を定めた基準、規則および原理を採択したことは、正しい方向への第一歩です。次に続くステップは、学者や専門家たちがこれらの基準、原理、規則がICT環境に適用されるように、具体的ないくつかの勧告を作成することではないでしょうか。

世界の最先進国の経済と技術の分野ではすでに第四次産業革命に加え、ナノ・バイオ・情報・認知の各テクノロジー（NBIC）のコンバージェンス（収斂）が進行しています。「第六の波」の時代へのシフトを目指して情報セクターが発展したことにより、世界経済の構造が変化し、マーケット規模が一気に拡大され、ダイナミック性と競争性が高まり、電子商取引などのような新たなビジネスがたくさん生まれています。2018年のインターネット取引による売上高が3兆ドルに近づくだろうと予想するデータもいくつか出ています。ICTは、ビッグデータの処理、量子コンピュータ、拡張仮想現実、ブロックチェーンなどの新しい技術や現象の基礎を構成するようになっています。これらの技術イノベーションは普及し始めたばかりですが、同時に私たちはこれらに付随する脅威やリスクについてもたびたび思いを巡らすことになるでしょう。

技術の急激な進歩に比べると、私たち人間そのものははるか後方に取り残されていることを認める必要があります。マーチン・ルーサー・キング牧師によれば、「科学の力が、私たち人間の精神的な力をしのいでいる。私たちはミサイルをコントロールすることはできても、人間をコントロールすることはできない」のです。現に起きているプロセスを理解し、その結果を洞察するには、今私たちが持っている以上の深い思考が必要となりますが、そうしたものを私たちはまだ持っておりません。フェイクニュースや、政治的誘導、テロリストや原理主義者の影響から、どうしたら人間や社会を守ることができるのか。グローバルな情報空間の戦略バランスを脅かす脅威に対抗し、平等な戦略的パートナーであり続けるためには、どうすべきか。安全を犠牲にせずに持続的な経済成長をするには、何をしたらいいのか。

こうした設問に対する答えとしてもっともよく練られたものの一つだと思われるのは、国際情報セキュリティ・システムを構築し、そのなかに、グローバルな情報空間の様々な行為主体の活動を規制する国際的な制度と国内制度を新たに創設するか、既存のものの権限を拡大することを含めることです。このシステムにおける個々の大学の任務は、今日のみならず将来予想されるものも含め、脅威に対する答えを見つけ出し、人類に提供することです。そうした方向での作業を効率的に押し進めていくには、科学に携わる者が国境を超えて団結することを怠るわけにはいかないのです。

コメンテーター

リナ・シャラポフ
（モスクワ国立大学情報安全保障問題研究所 部門長）

解説：IoTが大々的に採用される場合に予想されるいくつかのこと

尊敬する同僚の皆様、こんにちは。

以下、簡単な解説をさせていただく機会を与えてくださった主催者の方々に感謝いたしたいと思います。

皆さん、今回私たちは、国際情報セキュリティが直面している諸問題について、興味深く、また内容豊かな一連の講演を聴くことができました。ここで私は、IoTが大々的に導入された場合に社会や人間生活に及ぼすいくつかの結果について申し上げたいと思います。

Cisco社の定義によれば、*IoT、「モノのインターネット」とはインターネットに接続することのできるすべての機器ということになります*[1]。Gartner社によれば、こうした機器は2017年には84億台あります[2]。Cisco社は2020年までに500億台近くの機器がネットに繋がれることになると予測していますが、それはIoTのポテンシャルが発揮されるプロセスにおいて、臨界点に達することを意味します[3]。

IoTは、経済を発展させ、生活の質を向上させる巨大な可能性を秘めています。それにもかかわらず、IoTを大量に導入することになれば、人類、社会、国家に対して否定的な結果をもたらす大きな可能性も生じます。

世界の先進国や国際機構は、IoTによるネガティブな帰結、新たな脅威、そして難しい選択を迫られるといった事態が生じるのではないかと、はっきりとした懸念を示しています。

情報通信技術（ICT）開発指数が8.43という高い値（国際電気通信連合（ITU）の作成した2017年のICT普及度を示す指数では10位[4]）となった日本にとって、IoTが爆発的に普及するなかで情報セキュリティを確保することは、国家の安全保障の分野における戦略的課題であります。

さて、日本の内閣サイバーセキュリティセンター（NISC）[5]は2016年8月、IoTを安全に機能させるための政策の基本的要素について述べた「安全なIoTシステムのためのセキュリティに関する一般的枠組」（「安全なIoTシステムのための一般的枠組み」）を策定しました[6]。

2016年11月、アメリカ合衆国国土安全保障省（U.S. Department of Homeland Security）は、「IoTセキュリティの戦略的減速」（STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS (IoT) Version 1.0）[7]を策定し、プロの専門家が行った検討結果をまとめた提言を発表しています。

ロシア連邦においては、連邦政府が2017年7月28日に承認した「デジタル・エコノミー」プログラムに沿って、IoTの情報セキュリティを確保することなどを目的として、いくつかの規格や技術規則の見直しが進められています。

尊敬する同僚の皆様！

ひとつ質問させてください。我々人間は、普段使用する電子機器がグローバルなネットワークと繋がり、勝手にインターネットと遣り取りをする事態に十分対処できるのでしょ

うか、また、IoTで使用される技術や機器の設計者や製造者は、これらが社会や人間生活にもたらす結果に対して社会的責任を引き受ける用意があるでしょうか。こうした問いに対する答えは、おそらくまだ出来上がっていないのではないでしょうか。

第一の点、どの機器メーカーもこう言います。—すべては人類の便宜のためのものであるが、しかし機器に実装された機能のすべてを我々が知りつくしているとは言い難い、と。

ネガティブな社会科学的結果の好例が「スマートトーイ」と呼ばれるもので、米国、ドイツ、ノルウェイで問題となっています。「スマートトーイ」は断りもなくインターネットと接続されることにより、個人のプライバシーを侵害したとして訴訟になっています。

米国の連邦捜査局（FBI）は保護者に対し、子供に与えた「スマートトイ」をチェックするよう呼びかけています。FBIは、所有者の会話を録画して認識するビデオカメラとマイクを備え、インターネットに繋がる「スマートトイ」は、チャットを本人がしているように偽装すれば個人に対する深刻な脅威になり得ると言われています。

今年だけでも、米国の「スマートトイぬいぐるみ」メーカー・Spiral Toys社の製品ユーザー80万人のチャット映像がインターネットに流れています。

同じ時期、ドイツでは、連邦ネットワーク庁（Bundesnetzagentur）がスマートドール「マイ・フレンド・カイラ」について、この玩具はスパイ機器だとして、販売を禁止しています[8]。

スマート機器のこうした利用法は、あきらかに2016年12月19日の国連総会決議「デジタル化時代のプライバシーの権利」（A/RES/71/199）の規定に違反しています。

第二の点は、IoT機器の制御は外部から乗っ取られる可能性があり、個々のユーザー、グループもしくは公共の利益のためでなく、害をなすために使われる可能性が一定程度存在することです。

ご存知のように、国際社会はサイバー犯罪に対応できていません。サイバー空間では多数の犯罪者や犯罪集団が暗躍していますが、彼らはIoTでつながれる何百万台もの機器がもたらすこうした新しい技術的可能性を必死になって利用しようとしており、その結果、深刻な事態が社会に生じるかもしれないのです。

ここに例証があります。*—日本の新聞に掲載された「情報通信研究機構」の情報によれば、2016年に日本のネットワークが被ったサーバーアタックの件数は1281億回記録されています。これは2015年の2倍以上に当たるそうです。また、これらの攻撃の半分以上は、インターネットに接続された監視カメラ、家庭の無線ルータおよびその他のインターネットに接続された機器に向けられたもので、その前年からの増加割合は26%程度となっています*[9]。

第三の点は、こうした機器は完璧なコンピュータとは呼べず、その処理能力に限りはあるにしても、インターネットにつながる限りはDDoS攻撃に利用することができます。こうした攻撃を「モノのボットネット」というようになりました。

もっともよく知られた例があります。—2016年10月、マルウェアMiraiによって構築されたボットネットによる大規模なDDoS攻撃が、ドメインネームシステムの大手であるDyn社のマネージドDNSインフラストラクチャに対して行われました。約10万台のIoT機器がマルウェアに感染させられ、攻撃に利用されました。それからたった1ヶ月で新たなMiraiが現れ、ドイツの通信事業者「ドイツテレコム」の顧客の約90万台の機器のネット接続を不能にしました。

尊敬する同僚の皆様！

もう一つ質問をさせてください。—IoTが大量導入されたとき、各国政府は自国民の情報セキュリティを守ることができるでしょうか。これは困難を極める仕事になります。

ここでその遂行が重要になってくるもう一つの国連総会決議を思い出しましょう。それ

は2009年12月21日に採択された「サイバーセキュリティのグローバル文化の構築および重要情報インフラの防護のための国家の取組みの評価」(A/RES/64/211) です。

Trustlook 社の調査 (2017年9月)[10] *によると、IoT 分野で脅威が高まっているのに比べ、ユーザーの間ではその認知度はそれほど高くありません。*

調査結果を見ると、IoT 機器のユーザーの3分の1以上 (35%) が工場出荷時のままパスワードを変更しておらず、そのことでサイバーアタックに対して機器を脆弱にしています。これに加えて、54% のユーザーがサイバー犯罪防止のための追加プログラムをまったくインストールしていません。

機器の保有台数が増大するにつれ、それに伴うリスクも増大します。専門家は、2020年までにサイバーアタックの25% が IoT 機器に向けられるようになると述べています。

遺憾ではありますが、今日では、犯罪者だけでなくテロリストや軍隊もスマート機器を利用して、重要なインフラストラクチャのいかなる要素の機能に対しても、破滅的な損害を加えることができると言わざるを得ません[11]。

尊敬する同僚の皆様！

自分をリスクから守るもっとも簡単な方法の一つは、情報セキュリティ文化の基本原則を遵守することです。IoT の分野を含め、ICT を取り扱うには、情報セキュリティ文化を育てて根付かせ、必ず従うようにすることが最重要の課題です。

今回のシンポジウムは、モスクワ大学と東海大学という、科学教育では権威のある二つの大学の長年の協力の実りある成果といえます。両校とも研究開発と教育を主要な目的の一つとして活動してきました。ここで、モスクワ大学総長 V.A. サドーヴニチィ・アカデミー会員が2013年に執筆したコンセプト論文「どうしたら情報的リスク及び脅威から個人を守れる？」(日本語訳あり) にご注目ください。この論文ではこう述べられています。—*「**情報セキュリティのグローバル文化の知と技および規範の体系を創造し、体現することが、科学教育機関の務めである**」。モスクワ大学総長の見解は、情報セキュリティ分野の無知を克服するためには、科学、教育、マスコミ、実業界、インターネットユーザーのコミュニティが一致して努力することが必要だということです。そして、そこで前面に立つべきは科学と教育であり、両者で直面する課題を解決するためのツール一式、即ち、科学に裏打ちされた提言、専門的で多岐にわたる教育プログラム、教育メソッド、教科書や啓蒙書籍を提供しなければならないのです。*

ご清聴、ありがとうございました。

---

1 出典：https://www.cisco.com/c/ru_ru/about/press/press-releases/2016/02-03b.html
2 https://www.gartner.com/newsroom/id/3598917
3 出典：https://www.cisco.com/c/ru_ua/about/press/2017/05-30.html
4 出典：https://www.itu.int/net4/ITU-D/idi/2017/
5 参照：National center of Incident readiness and Strategy for Cybersecurity // http://www.nisc.go.jp/eng/
6 参照：http://www.nisc.go.jp/eng/pdf/iot_framework2016_eng.pdf
7 出典：https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf
8 参照：https://club.esetnod32.ru/news/novosti_eset/igrushki-shpiony/
9 Cyberattacks targeting Japan networks hit a record 128.1 billion in 2016. https://www.japantimes.co.jp/news/2017/02/08/national/crime-legal/cyberattacks-targeting-japan-networks-hit-record-128-1-billion-2016/#.Wgi6SrhR37k
10 http://www.securitylab.ru/news/488795.php / https://newblogtrustlook.files.wordpress.com/2017/09/iot-security-survey-infographic-2017.pdf
11 O.V.Khramov. http://www.scrf.gov.ru/news/allnews/2164/

コメンテーター

河野　桂子
（防衛省防衛研究所 主任研究官）

サイバー空間のおける主権及び不干渉原則—ロシアの過去の主張からの類推

Ⅰ　はじめに

国連のサイバーGGE（正式には、「国際安全保障の文脈における情報通信分野の発展に関する政府専門家会合」）の2015年報告書は、国際法、とりわけ国連憲章に体現された基本原則が国家によるサイバー活動に対して適用され得ることを確認している[1]。もっとも、サイバー活動に固有の様々な側面において、国際法がどのように適用されるのかについて専門家らは必ずしも合意に達していない。例えば、西側諸国は、NATO[2]及びG7[3]などの枠組みにおいて、国家の武力行使や自衛権を規律する国際法（jus ad bellum）がサイバーの文脈においても適用されることを認識しているものの、ロシアや中国は、情報通信技術（ICT）は兵器でないことを理由に挙げてその適用可能性を否定している[4]。双方の陣営の間にはこの問題に関する国際法の理解について深い溝があるのが現状である。

このような理解の乖離にもかかわらず、いずれの国も深刻な懸念と受け止めるであろう論点を本稿では取り上げ、他国のサイバー活動によって被害を受けた国家がどのような措置をとり得るのかについて、西側諸国のみならずロシアにとっても受け入れ可能であると推測される程度と範囲を探ることとする。まず、本稿では、国家の国内管轄事項に対してサイバー手段を用いて干渉することは禁止されるという原則について、今日いっそう多くの国が賛同すると考えられる背景を検討する。ロシアを始めとする一部の国々は、衛星による国際直接テレビ放送が盛んに行われ始めた1970年代において、自国領域内に到達する情報を統制する、国家の主権的権利を強固に主張したことが良く知られている。その当時の議論は、現在サイバー空間をめぐって展開されている主張にも多分に反映されている。ロシアは、さらに情報を受信する国家の主権を損なう形で不当な放送を行った加害国に対して一種の報復的措置をとる可能性にも言及しており、この点は国家の違法なサイバー活動の帰結を考察する上でも興味深い視点を提供している。ロシアが唱えた一種の報復的措置は、サイバーの文脈において被害国が取り得る（違法性阻却措置としての）対抗措置を示唆するからである。

Ⅱ　サイバー干渉禁止原則

サイバー空間における主権の論点はそれ自体、新しいものではない。例えば、宇宙からの国際直接テレビジョン放送に関する1970年代以来の米ソの対立でも指摘された通り、本質的には古くから存在する問題である。ソ連が放送内容について国家の管理権限を唱えたのに対して米国は、当時、情報の自由な流通を強く主張していたが、この構図は、基本的にサイバー主権に関する国家間の論争と同じである。

1．宇宙からの国際直接テレビジョン放送に関する受信国の主権の主張

ソ連は、1972年に「国家による直接テレビジョン放送を目的とする人口地球衛星の使用に関する原則の国際条約案」[5]を国連総会に提出した。この条約案においてソ連が主張した主要な点は以下の通りである。まず、宇宙からの国際直接テレビジョン放送という当時新たに出現した事象に対して、一般的に認められた国際法が適用されることである（2条）。この中には、国連憲章や1967年宇宙条約が含まれる。次に、国家は、人工衛星を用いて、他国の国内問題又は外交政策に干渉することを企図する放送を行ってはならない（4条）。また、国家は、直接テレビ放送を他国に流すにあたっては、当該受信国の明示的な同意を得なければならない（5条）。受信国の同意を得ない直接テレビ放送は違法であり（6条）、この違法な放送に対して被害受信国は、これに対抗するために入手可能な措置を講じることができる（9条）。この被害受信国が具体的にどのような対抗措置をとることができるのかについては、条約案の中では触れられていないが、当時この問題を議論した識者の中では、単なるジャミングによる放送妨害のみならず、衛星を破壊する措置を含むものと解釈されていたようである[6]。

同年11月には、将来の目標として国際条約を締結する観点から、直接テレビ放送に関する基本原則を考察する必要性を確認する国連総会決議2916が102カ国の賛成をもって採択された[7]。唯一反対票を投じた米国は、国家主権と情報の自由な流通という2つの概念は、対立するのではなく互いに補完すべき関係にあるにもかかわらず、本決議では情報の自由な流通という考え方が十分に反映されていないと主張して、この問題に関する国際条約を将来作成しようとする動きに反対した[8]。

この決議の10年後である1982年には、「国際直接テレビジョン放送に関する人口地球衛星の国家による使用を規律する原則」が、国連総会決議37/92として採択された[9]。本決議では、違法な直接衛星放送の受信国による対抗措置を定めたソ連の1972年条約案9条の規定は含まれていない。但しこの決議は、全体としては、放送受信国の通信主権の保障を過度に強調したものであることを理由として、ほとんどの西側諸国は、反対（13カ国）か棄権（13カ国）にまわった[10]。この決議は、ソ連が1972年に提案した基本原則を支持する内容であり、例えば、「国際直接放送衛星業務を設定しようとする場合には、各国はその意思を予定受信国に遅滞なく通報し協議に入るほか、関係国間の協定・取極めの事前締結を義務づけられている（原則J、13・14項）。しかもこれらの協定・取極めは、番組内容の規制を含む非技術的な合意を含むものと、解されている。これらの一連の動きを受けて、学説の中には、一般国際法上、「個人の情報自由または国家相互間の情報の自由流通の原則が、外国向けの番組発出の権利をみとめ受信国による妨害を禁止する効果をもつ」ことの立証は困難であるという評価が存在する[11]。この評価が正しければ、情報の受信国は、自国の主権に基づき外部から流入する情報を妨害し、統制することが可能であることを意味する。

2．ロシアや中国が主張するサイバー空間の主権

国際直接テレビジョン放送に関する当時の米国とソ連の意見の対立は、サイバー空間における情報流通の自由を唱える米国と、他方で国内の治安を脅かす情報の流入を嫌がるロシアや中国との間の対立にそのまま引き継がれている。ロシアや中国は、自国の国内統治にとって好ましくない情報が西側諸国から大量に送られることを懸念しており、そうした

有害な情報の流入を阻止することに従来から腐心してきた。政府があらゆる情報を統制することができる一種の国家領域としてサイバー空間を捉えるという理解[12]も、国際直接テレビジョン放送について行った主張と軌を一にするが、そのことを国際社会に理解させるのに国際条約を作成することは両国にとって何より理に適っているのである。もっとも、ロシアと中国は、2011年に引き続いて2015年に国連事務総長に「情報セキュリティ国際行動規範」[13]を提出するにあたり、主権原則と並んで、個人が有する情報の発受信の権利を尊重することに触れる点で、以前にもまして巧妙である。この「国際行動規範」で引用されている「市民的及び政治的権利に関する国際規約」(1966年。以下、自由権規約)は、19条3においてもともと国の安全、公の秩序又は公衆の健康若しくは道徳の保護に必要な限りにおいて、個人の権利が一定の制限に服することを認めており、ロシアや中国は、自国における情報統制措置をしくにあたり、形式的にはこの枠組みに沿った措置であると主張することが可能である(もっとも、中国は自由権規約の締約国ではない)。1970年代から米国が人権の文脈で主張した自由な情報の流通原則は、他国との関係において必ずしも絶対的なものではない。したがって、米国を含む西側諸国が、ロシアや中国に対してサイバー空間上の情報を統制したりすることはなんら許されない、と主張することは両国に対して必ずしも対抗力がない。

他方、この数年の間に米国や欧州各国に対してロシアの当局が行ったとされる国内選挙への干渉を目的とする情報活動については、情報の自由な流通の考え方がいわば悪用され、その結果、選挙という政府の固有の機能が外国政府から妨害されるリスクがあることを西側諸国の政府に考えさせる契機となった。サイバー空間における主権概念については、『サイバー活動に適用される国際法タリン・マニュアル2』も指摘するように未だに諸国の間に解釈の相違があるものの[14]、国家による通信活動が他国の国内問題に干渉してはならない、というソ連が唱えていた基本原則について、今や西側諸国も受け入れることに異論の余地はないものと思われる。このことについて国際条約を作成することは、国際直接テレビジョン放送をめぐる原則の条約化がとん挫した経緯に照らしても現実的ではないことは明らかであり、また条約化の必要も必ずしもあるとは思われない。関係国がG7、地域的機関その他の志を共にする国々と共にサイバー干渉禁止原則を確認する実行が蓄積するだけでも、一般国際法の確立に寄与するところは大きい。

3. サイバーの文脈において被害国が対抗措置を講じることは可能か

国際直接テレビジョン放送との関連で放送受信国の通信主権を主張したソ連は、当時、違法な放送を行う加害国に対して入手可能な措置をとることを1972年に国連に提出した条約案の中で主張していた。ソ連は実際にも、衛星放送が実用化される以前のラジオ放送との関連で、西側諸国から国内に届く有害な放送に対してジャミングによる妨害を行っていたことが知られている[15]。人口衛星の破壊という対抗措置は、国連憲章2条4の禁じる武力の行使に該当する可能性はあるが、その論点はさておき、ここで重要な点はソ連が伝統的に他国からの有害な放送通信に対しても対抗措置を講じてきたことである。

国家によるサイバー活動も国家間の権利義務の問題である以上、その問題を規律する国際法である国家責任法が適用されることは疑いの余地がなく、サイバー手段を用いた対抗措置や緊急避難が排除される論理的な理由はない。したがって、違法なサイバー活動の被

害国は、その加害者個人又は加害国を特定するに至った場合には、加害者個人を国内裁判所において刑事訴追するか、又は加害国に対する経済制裁を科すなどの措置に加えて、様々な措置に訴えて加害国の責任を追及することが認められる。ロシアも自国の過去の経験に照らしてこうした考え方を当然支持することが推測される。

但しラジオ放送や、衛星放送と異なり、サイバー活動は単に情報や通信の手段として機能することにとどまらず、物理的に物を破壊するという、兵器としての機能を有する点で、従来の情報通信手段とは区別される。かつて、北朝鮮の発射するミサイルをサイバー攻撃で阻止する作戦を米軍のサイバー・コマンドが行っていたという報道[16]が流布したが、北朝鮮が米国に対して行った度重なる武力行使の脅しなど、国際違法行為が北朝鮮の側にまずあり、米国が被害国として北朝鮮に対して対抗措置を講じたという側面は、確かに含まれるのかもしれない。但し、サイバー手段による対抗措置が認められ得るとしても、それが国家の重要インフラに対して物理的及び機能的に甚大な悪影響を与える恐れがある場合には、慎重な検討が必要である。同様に、サイバー対抗措置を講じるためには、加害国が特定されていることも前提条件である。対抗措置は、武力の行使を伴うものであってはならないことは、多くの国家によっても承認されており、サイバー活動における武力行使の定義をどのように定めるかによっても、サイバー対抗措置の許容される範囲は変わり得るものと思われる[17]。

Ⅲ　結びに代えて

『タリン・マニュアル2』の起草にも携わった専門家の一人によれば、ある行為がサイバー干渉とみなされるためには、「強制」の要素が伴わなくてはならない。すなわち、「国家が国際法上認められる制限の範囲で、自国の選択に基づき国内管轄事項や外交関係を推し進めることを妨げようと企図すること」である[18]。他方で、ロシアが行ったとされる各国への選挙干渉の評価については、国際法上禁止される干渉であると肯定する意見もあれば否定する意見も同様に存在する[19]。衛星による国際直接テレビ放送についても、西側諸国はなんらそれを強制的な行為とはみなさなかったにもかかわらず、当時、ソ連は「外部からの干渉」と非難した[20]。それゆえ、ソ連は、1972年に提出した条約案において不干渉原則に言及することが不可欠であると考えたのである。今日のサイバー空間をめぐる活動については、悪意を持った他国による情報操作活動を始めとする様々なサイバー攻撃によって、選挙などの政府の固有の機能が脅かされる事態に直面し、多くの国がそれを法的に禁止することに共通の利益を見出しているはずである。この問題を国際法上の不干渉原則の新たな側面として、西側諸国のみならずロシアや中国などの国々も加わり積極的な議論を進めていくことが最も望ましいと思われるが、それが不可能である場合にも利害を共有する国家の間で国際慣習法の形成に寄与する共通の国家実行を積み重ねることも一つの方法である。どのような行為が国際法上、違法とみなされるか否かの問題は、被害国が加害国に対して責任を追及するためにも先決的に解決しなければならない課題である。

1 U.N. Doc., A/70/174, July 22, 2015.
2 Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, September 5, 2014, available at https://www.nato.int/cps/en/natohq/official_texts_112964.htm
3 G7伊勢志摩サミット（2016年）成果文書「サイバーに関するG7の原則と行動」http://www.mofa.go.jp/mofaj/files/000160315.pdf
4 Andrey Krutskikh and Anatoly Streltsov, "International Law and the Problem of International Information Security," *International Affairs: A Russian Journal of World Politics, Diplomacy and International Relations*, Vol. 60 (2014), pp. 64-76.
5 Request for the Inclusion of a Supplementary Item in the Agenda of the Twenty-Seventh Session, Preparation of an International Convention on Principles Governing the Use by States of Artificial Earth Satellites for Direct Television Broadcasting, Letter dated 8 August 1972 from the Minister for Foreign Affairs of the Union of Soviet Socialist Republics addressed to the Secretary, General, U.N. Doc., A/8771, August 9, 1972.
6 "The Control of Program Content in International Telecommunications: A Discussion of General Principles," *Columbia Journal of Transnational Law*, Vol. 13 (1974), p.51; Sharon L. Fjordbak, "The International Direct Broadcast Satellite Controversy, *Journal of Air Law and Commerce*, Vol. 55 (1990), pp. 910 and 915.
7 U.N. Doc., A/RES/2916(XXVII), November 9, 1972.
8 U.N. General Assembly, 2081st Meeting Record, UN Doc., A/PV. 2081, November 9, 1972, p. 5, para.47 and 48.
9 U.N. Doc., A/RES/37/92, Annex: Principles Governing the Use by States of Artificial Earth Satellites for International Direct Television Broadcasting, December 10, 1982.
10 山本草二「国際間情報流通と通信主権の法機能」『ジュリスト増刊』（1984年）71頁。
11 同上、71－72頁。本文に引用した本決議の日本語訳も、この論文に依る。
12 Doctrine of Information Security of the Russian Federation (Unofficial Translation), Approved by Decree of the President of the Russian Federation, No. 646 of December 5, 2016, The Ministry of Foreign Affairs of the Russian Federation website, available at http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163
13 U.N. Doc., A/69/723, January 13, 2015.
14 Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017), Part 1, Section 1.
15 John B. Whitton, "Cold War Propaganda," *American Journal of International Law*, Vol. 45 (1951), pp. 151-153.
16 "The U.S. Wants to Stop North Korean Missiles before They Launch. That May Not be a Great Idea," The Washington Post, March 15, 2017, available at https://www.washingtonpost.com/news/monkey-cage/wp/2017/03/15/the-u-s-wants-to-stop-north-korean-missiles-before-they-launch-that-may-not-be-a-great-idea/?noredirect=on&utm_term=.c142927843a0
17 国連国際法委員会（ILC）「国際違法行為に対する国家責任に関する条文」50条1(a)。
18 Terry D Gill, "Non-Intervention in the Cyber Context," in Katharina Ziolkowski, ed., *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy* (NATO CCD COE Publication, 2013), p. 232.
19 シュミット教授は、ロシアが行ったと主張される米国民主党全国委員会（DNC）へのハッキング行為をめぐっては「強制」の有無について論争があることから、国際法上評価を確定しがたいグレーな問題であると評している Michael N. Schmitt, "Grey Zones in the International Law of Cyberspace," *The Yale Journal of International Law Online*, Vol. 42 (2017), p. 8.
20 U.N. Doc., A/PV. 2081, p. 4, para. 37.

コメンテーター

小泉　悠
（未来工学研究所 特別研究員）

サイバー空間をめぐる日露安全保障協力の展望

はじめに：共通の空間とすれ違う理解

今回のシンポジウムにおいて筆者が行ったコメントは、大きく分けて2点である。

第1に、日本側の関心が「サイバー安全保障」に集中しているのに対し、ロシア側の重点は「情報安全保障」にあるという概念的な食い違いが日露間には存在している。

第2に、インターネットは今や生活や安全保障を考える上で欠くべからざる領域（ドメイン）でありながら、陸海空宇宙といった他のドメインとは異なり、人工的な構築物である。しかも、この人工空間を支えるインフラストラクチャーは大部分が西側諸国によって構築されたものであり、この点が近年のロシアにとって重要な懸念事項となっている。これも西側世界の一員である日本にとってはなかなか理解されない点であり、日露間のもうひとつの食い違いにつながっている様に思われる。

要するに、日露はともにインターネットの安全保障について話し合いながら、根本的な理解においてすれ違っているのではないか。そこで以下の本稿では、前述した2点をもう少し掘り下げ、多少なりとも日露間の理解に関する架橋を試みたい。

ロシアの「情報安全保障」概念

日本におけるサイバー安全保障の主要な関心は、サイバー空間の不法な利用を阻止することにある。2018年に発覚した電子マネーの大量盗難事案や、過去に発生した個人情報の流出などが、ここで想定される主要な脅威である。あるいはサイバー攻撃によってインターネット通信の機能が損なわれたり、社会インフラが機能不全に陥るのを防ぐこともサイバー安全保障上の重要な課題である。

このような意味でのサイバー空間の安全確保は、ロシアの安全保障政策においても重視されていることは言うまでもない。ただ、ロシアと日本が大きく異なるのは、ロシアにとってのサイバー安全保障とは、情報安全保障というより上位の概念を構成するという点にある。ロシア政府の安全保障政策文書を精査すれば明らかなとおり、ロシアの安全保障コミュニティが懸念しているのは、単純な情報流出やサイバー攻撃だけではない。サイバー空間という過去に例を見ない伝達性を持った情報チャネルが出現したにも関わらず、国家がこれを完全に管理できないという点にロシア側の懸念は集中している。

サイバー空間では、サイバー攻撃やダークウェブを通じた違法な取引（たとえば盗み取られた電子マネーや違法薬物など）が行われるばかりでなく、ロシア政府にとって都合の悪い情報も飛び交う。たとえばウクライナやシリアへの軍事介入に関する外国政府からの非難、反体制派によるプーチン体制への批判的意見、宗教的・人種的な過激主義言説など

がそれである。ロシア政府から見た場合にはこうした情報の流通は敵対勢力による「情報戦争」を構成するものであり、したがってロシア政府によって適切に管理（選別、遮断等）されなければならないということになる。

翻って日本について考えてみれば、政権や国家の政策に対する非難は言論の自由の範囲であり、ここになんらかの形で国家が介入することについては社会的な合意はまず得られないであろう。ただし、宗教的・人種的差別を扇動する言説をどのように扱うのかは日本においても近年、急速な注目を集めている。国家が情報の流通にどこまで介入すべきであるのかは、今後、日露間の専門家同士で議論しうるテーマのひとつではないか。

人工物としてのインターネット：ロシアの不安

忘れられがちなことであるが、インターネットは人工物である。通信回線が切断されれば、あるいはサーバーの電源が抜ければ、インターネット空間は消滅する。もちろん、インターネット空間を支えるインフラは何重にも冗長化されているため、実際にはそう簡単に消え失せることはない。少なくとも日本がインターネット空間から完全に孤立するという事態はまず考え難いし、2011年の東日本大震災においても日本のインターネット網は実際に耐えた。

しかし、ロシアは、インターネット空間の堅牢性に対してこれほど信頼を置くことはできない。DNSルートサーバーをはじめとするインターネットの基幹インフラは米国等の「西側」諸国に握られており、政治的な理由から人為的にインターネットへのアクセスを遮断される懸念を払拭できないためである。ことに2014年のウクライナ危機後、ロシア政府はこのような事態に関する懸念を強め、同年夏には通信省を中心としてグローバルインターネットからの遮断状況を想定した演習が実施されたと伝えられる。近年、ロシア政府が「デジタル経済ドクトリン」等の政策文書において、通信回線その他のインターネット・インフラの自律性を強調しているのも、こうした懸念に基づくものであろう。

西側の一員である日本は、ロシアのこうした不安を共有してはいない。ただ、グローバル・インターネットの分裂は西側社会にとっても好ましいものではない。ロシアが危機時の非常手段としてインターネットの自律性向上を進めることは妨げ得ないとしても、少なくとも平時においては開かれたひとつながりのインターネット空間が維持されるべきである。そのために日本にできることは何か。これが今後の日露間におけるもうひとつのテーマとなり得よう。

編集後記

モスクワ国立大学情報安全保障問題研究所共催のサイバーセキュリティーシンポジウム準備からブックレット創刊号の編纂にいたるまで、東海大学平和戦略国際研究所次長、藤巻裕之政経学部政治学科準教授にお世話になりました。振り返って、サイバーセキュリティー分野もロシア研究も門外漢の自分には本当に荷が重い仕事でした。ロシア、ユーラシア地域研究をされている藤巻先生のモスクワ国立大学とのネットワークがあって何とか最低限の責任を果たせた気がします。ブックレットには掲載されませんでしたが、昨年12月のモスクワ大学主催のシンポジウムには中国からも代表団の参加があり、会議に出席された藤巻先生から報告をいただいています。米中新冷戦とも形容されるハイテク技術や通信インフラの覇権争いの中で、とりあえずロシアと中国が連帯しているという認識です。長期的視点からは北東アジア、北極海においても更なる権益を求める中国に対し日本とロシアはより一層の協力関係を構築すべきだと思います。北方領土問題の難しさから平和条約締結の道筋はいまだ明確ではありませんが、モスクワ国立大学や極東連邦大学とのネットワークの重要性を再認識しています。引き続き、学術交流を深めたいと思います。サイバーセキュリティーシンポジウムを契機に内閣サイバーセキュリティーセンターの三角育生副センター長には、サイバーセキュリティーの基礎知識から研究教育体制の構築に至るまで懇切丁寧なご指導をいただきました。改めて感謝申し上げる次第です。最後に、ジャーナリストの仕事との二束の草鞋で常に時間に追われ、原稿処理や編纂作業の大幅な遅れでご迷惑をおかけしました東海大学出版部の田志口克己さんにお礼を申し上げます。有難うございました。

2019年2月3日　末延記