はじめに第10回記念サイバーセキュリティ国際シンポジウムを開催された慶應義塾大学グローバルリサーチインスティテュートと MITRE 株式会社の皆様にお祝いの言葉を申し上げます。この場で講演させていただけることを大変光栄に思っております。外務省サイバー政策担当大使として、外務省の掲げるサイバー外交についてお話しさせていただきます。

新型コロナウイルスは、人類の情報通信技術への依存度が高まる傾向を加速させる一方で、そのような技術を悪意をもって使用することにより引き起こされるリスクや問題を顕在化しているように思われます。オンライン教育やテレワークの利活用も高まっています。世界中の外交官も実際に現地に飛び、会うことが難しいことから、テレビ会議の活用も増えています。本日のイベントもオンラインで行われています。一部の国では遠隔治療がかなり一般的になってきています。スマートフォンにも新型コロナウイルス対策アプリがあります。あるアプリは、ウイルスへの感染リスクに応じて、個人を3つの分類や3つの色に分けています。

こうしたアプリには多くの機微データが内蔵され、潜在的な被害も伴います。サイバーセキュリティの脆弱性を悪用したサイバー攻撃に対する世間の注目が高まるのも当然です。

世界的なセキュリティベンダーであるトレンドマイクロの統計によると、2020 年上半期には日本国内の約297万人の利用者がフィッシング攻撃の被害に遭っています。これは2019年下半期と比べて 60%の増加です。同統計によると、新型コロナウイルス関連のマルウェアが検出された機器は、1〜3月期の737台から4〜6月期には5,058台に増加し、ほぼ7倍に増加しています。

昨年 3 月にチェコの大学病院を襲ったランサムウェアによるサイバー攻撃では、手術や診療の遅延や中止などの大規模な被害が発生しました。また、8 月には国内 38 社が社内ネットワークへの不正アクセスに遭い、テレワークで必要な設備の VPN コードが漏洩した可能性があると報じられています。

このような状況を背景に、国際社会は自由で公正かつ安全なサイバー空間を維持するために、サイバー攻撃の抑止・対策に向けた取り組みを一層強化することがきわめて重要であると考えています。サイバー空間は、活力ある経済発展と新たな価値観・文化の創造の基盤であり、民主主義と自由を支え、国際的な平和と安定に貢献するものです。

我が国のサイバーセキュリティ戦略は、まさにこうしたサイバー空間を維持することを目的としています。この戦略に不可欠なものとして、日本のサイバー外交も同じ目標を掲げており、3 つの柱、すなわち「法の支配の推進」、「信頼醸成措置の推進」、「能力構築支援」で構成されています。

まずは、サイバー空間における「法の支配の促進」から述べたいと思います。

サイバー空間は無法地帯であってはなりません。弱肉強食であってはなりませんし、適者生存の場であってもなりません。日本の見解は、既存の国際法がサイバー空間に適用されるというものです。また国連憲章第 51 条に認められた固有の自衛権を含む国連憲章全体や、国際人道法、国際人権法が適用されるという見解です。国家責任条文草案に基づき、国家は、

サイバー攻撃が国際違法行為に該当する場合には、責任ある国家が国際的な義務を遵守するよう促すために、サイバー攻撃に対して様々な措置を講じることができます。

なぜサイバー空間において国際法が適用されると確認することが重要なのでしょうか。国際法は原則として国家を対象とします。サイバー空間においても、現実世界と同様に国家は国際法に拘束されており、違法行為には結果が伴うべきです。国際法は、国家主権の侵害、干渉、場合によっては武力攻撃を含む国際違法行為となりうるサイバー攻撃を抑止し、対抗するための手段を被害国に提供しています。不幸にして武力紛争が継続している場合であっても、国際人道法は、非軍事目標に対するサイバー攻撃を禁止しています。

国連事務総長は、国連総会の要請を受けて、サイバーセキュリティに関する政府専門家グループ（GGE）を６会期に渡り、継続的に設置してきました。日本は直近の４つの期に出席し、積極的に議論に貢献してきました。私は昨年から始まった現 GGE における 25 人の政府専門家の一人です。国際法や国際安全保障に携わってきた経験を生かし、積極的に参加し、建設的に議論に貢献しております。2013 年と 2015 年に GGE が発出した報告書では、サイバー空間において国際法が適用されることを確認しました。これは非常に重要です。国連総会全体がこの 2 つの報告書をコンセンサスで承認したのです。したがって、この確認は普遍的なものです。

昨年から、国連総会内には、サイバーセキュリティに関するオープンエンド作業部会（OEWG）が設置されています。この新しい枠組みには、すべての国連加盟国が参加可能です。2020 年６月に開催された OEWG では、日本を含む６カ国が医療サービスと医療施設に対するサイバー攻撃に重大な懸念を表明し、医療サービスと医療施設を電力や水道分野と同様に適切に保護すべき重要インフラと考えるべき提案を行いました。

サイバーセキュリティに関する国連安全保障理事会のアリアフォーミュラ会合はこれまでにも何度か開催されています。今年 5 月にエストニアが主催したアリア・フォーミュラ会合において、私は、国連加盟国は人権の尊重、紛争の平和的解決、武力行使の禁止を含む国連憲章の目的と原則へのコミットメントを再確認し、国家責任、固有の自衛権、国際人道法がサイバー空間においても適用されることを明示的に認識すべきであり、その認識がサイバー空間における紛争の予防と抑止に重要であると述べました。さらに、安全保障理事会は、サイバー活動に関わる重大な事態を予防あるいはそれに対応するために国連憲章第 6 章または第 7 章に基づいて行動する用意があるべきであると述べました。安全保障理事会が対応を求められる可能性のある個別の事例に備えて、サイバーセキュリティに関するテーマ別の議論を行うことが必要であり、適切であると私は考えております。

またサイバー空間における責任ある国家の行動原則は、既存の国際法を補完しつつ、安定的で予測可能なサイバー空間を確保するために不可欠な役割を果たします。すべての国連加盟国は、2015 年に政府専門家会合が提案した 11 の規範に合意しています。 それらを実施しなければなりません。そこで、サイバー攻撃の加害者を特定することの難しさを考える上で非常に重要な２つの具体的規範を紹介します。

規範(c)によれば、「国家は、故意に自国の領土が、ICT を利用した国際的に不正な行為に利用されることを許してはならない。」

規範(h)によれば、「国家は、重要インフラが悪意ある ICT 行為に晒されている他国からの支援要請に適切に対応すべきである。また国家は、自国の領域から行われた他国の重要インフラを狙った悪意ある ICT 活動を緩和するための適切な要請にも、支援要請国の主権を考慮して対応すべきである。」

加害国が、サイバー攻撃が自国に結びつけられないから逃げられると考えている場合であっても、被害国が加害国の領域から発せられた悪意ある活動があることを示し、支援を求めてきた場合には、前者はこれに応じなければなりません。

今回の GGE においてこれまでの GGE 報告書で合意された内容にさらに共通理解を重ねていくという議長の努力を強く支持します。また、日本は OEWG での議論を高く評価しています。ここでの議論は、これまでの GGE の成果について国連加盟国全体の理解を深め、実行を促すことに貢献しています。

しかしサイバー空間に適用される国際法や規範の議論は困難になってきていると言わざるを得ません。多くの国が、国際法がサイバー空間にどのように具体的に適用されるのか、議論を深めたいと考えています。国際的な専門家グループにより発出された、「サイバー行動に適用される国際法に関するタリンマニュアル 2.0」は、政府間で議論する際の素晴らしい参考書です。しかし、サイバー空間は新たな領域であり、新たな規範を作り最終的には新たな条約を結ぶ必要があるという意見をもつ国もあります。我が国としては、現時点ではサイバーセキュリティに関する条約の交渉を開始する必要はないと考えています。既存のルールを利用し、合意された規範を実行しようではありませんか。

サイバー攻撃を抑止するためのもう一つの手段がパブリックアトリビューションです。これは、非難や懸念を公に表明することです。パブリックアトリビューションは、攻撃者にサイバー攻撃のコストを理解させ、サイバー攻撃の実施を思い止まさせることを目的としています。

日本は 2017 年にワナクライ事案の背後に北朝鮮の関与があるとして、これを非難する外務報道官談話を発表しました。2018 年の外務報道官談話でも、中国を拠点とする APT10 といわれるグループが長期にわたる攻撃を行ったとしてこれを断固非難しています。

ルールに基づいたサイバー空間を推進するためには、サイバー犯罪対策における国際協力も重要です。我が国は、サイバー犯罪に関するブダペスト条約の締約国であり、同条約をはじめとする協力体制に基づき、国際的な捜査協力や情報共有を行っています。未加盟国に対しては、ブダペスト条約への加盟を働きかけています。

サイバー外交の第二の柱は、サイバー空間における「信頼醸成措置（CBM）の展開」です。誤算や誤解によりサイバー空間の緊張がエスカレートするのを防ぐには、各国政府がお互いの国内法、規制、政策、戦略、考え方を理解することが必要です。相互理解を深めるために、日本はこれまで 14 の国と地域とサイバー協議や対話を行ってきました。2019 年には、

オーストラリア、EU、フランス、インド、ロシア、米国との二国間協議、中国、韓国との三国間対話を実施しました。

日本は、地域的なCBMの発展を優先してきています。例えば、ASEAN地域フォーラム(ARF)では、日本はシンガポール、マレーシアとともに共同議長として、2019年3月にサイバーセキュリティに関する会期間会合での議論を主導し、2020年1月には専門家会合を開催しました。日本は、次回のサイバー専門家会合及び会期間会合の開催を予定しています。

ARFは加盟国間の信頼醸成に重要な役割を果たしています。加盟国は、(a) 実務者間の連絡先交換、(b) 国内の法律、政策、最優良実施例、戦略、規則に関する情報の共有、(c) セキュリティ事案への緊急対応に関する意識啓発と情報共有、(d) ICT利用におけるセキュリティ構築に関するワークショップの開催に合意しています。

最後の柱は「能力構築支援」です。サイバー空間の連結性から、一部の国や地域での事案対処に必要な能力の不足が世界全体にリスクをもたらす可能性があります。

日本は、これまで主にASEAN諸国を中心に、コンピュータセキュリティインシデント対応チーム（シーサート：CSIRT）や関連する行政関係者・調査機関に対する能力構築支援を行ってきました。ASEANのサイバーセキュリティ関係者や重要情報インフラ事業者の能力向上を目的として、タイに「日ASEANサイバーセキュリティ能力構築支援センター」が設立されました。また、日本とASEANの関係者は、信頼関係を強化し、政策調整を促進するために「日ASEANサイバーセキュリティ政策会議」を開催しています。また、共同の机上演習やワークショップを実施しています。日本では、JICAのグループ・地域別研修の一環として、アジア、中東、アフリカ等の政策担当者、刑事司法実務家等を対象に、講義、机上演習、施設見学等の機会を提供しています。さらに日本・ASEAN統合基金を通じて、インターポールシンガポール総局（インターポール・グローバル・コンプレックス・フォー・イノベーション：IGCI）と連携した、「ASEANサイバー犯罪捜査合同プロジェクト及びASEANサイバー能力向上プロジェクト」を実施しています。　日本は今後も政府一丸となって、戦略的かつ効果的な支援を行って参ります。

本日の講演がサイバー空間における法の支配の重要性と、サイバー空間における国際的な平和と安全のために日本が積極的に貢献していることをご理解いただく上で、お役に立てたことを願っております。菅義偉新総理は、初となる記者会見の場で、日本のデジタル化を強く促進していく意思を述べられました。総理のリーダーシップの下、日本は自由で公正で安全なサイバー空間の実現に向け、積極的なサイバー外交を継続して参ります。

ご静聴ありがとうございました。