サイバー・イニシアチブ東京 2022
山田外務副大臣スピーチ原稿

御列席の皆様、こんにちは。
外務副大臣の山田　賢司です。

本日は、「サイバー・イニシアチブ東京 2022」においてスピーチする機会をいただき、誠にありがとうございます。産官学の垣根を超えて日本国内を始め、世界中の著名なサイバーセキュリティ関係者を集めた国際的なイベントを日本企業が主催していることを大変うれしく思います。主催者の皆様におかれましては、本イベントの開催に、改めてお祝い申し上げます。

さて、本イベントのテーマである「複雑化するハイブリッド社会　身近に迫るサイバーリスクに立ち向かう」にあるとおり、今やサイバー空間はあらゆる活動に不可欠な社会基盤となっています。全国民が参画する「公共空間」として、その重要性及び公共性がますます高まっている一方、国内でもランサムウェアによる攻撃を始めとするサイバー攻撃事案の増加や「エモテット」と呼ばれるマルウェアの増加が見られるなど、多様なインシデントが発生しており、我々の身近に迫るリスク、そして、サイバー攻撃が我が国の経済社会に甚大な影響を与えるリスクが増大しています。外交当局としても、こうした問題意識を平素からしっかりと持って取り組んでいく必要があります。

また、本年は、ロシアによるウクライナ侵略の関連でも、サイバー空間の安全の重要性が浮き彫りになりました。ウクライナの政府機関等のウェブサイトの改ざんや閲覧障害が発生したほか、米国の衛星通信事業者が提供する衛星通信サービスに対するサイバー攻撃により、ウクライナを含むヨーロッパでシステム障害が発生し、これらの事案については、ロシアによるウクライナ侵略との関連性が指摘されています。このように烈度が上がった状況にも関連する形で、平素から国家間の争いにおけるサイバー空間利用の本格化も顕著になっています。

現下の国際情勢において特に強調すべきなのは、国家を背景に持つサイバー攻撃は特に深刻な脅威であるということです。国家の関与が疑われるサイバー活動として、中国は軍事関連企業、先端技術保有企業等の情報窃取のため、ロシアは軍事的及び政治的目的の達成のため、北朝鮮は政治目標の達成や外貨獲得のため、サイバー攻撃等を行っているとみられています。さらに、これらの国等は軍を始めとする各種機関のサイバー能力の構築・増強を継続していると考えられます。

このような状況を踏まえ、外務省としては、自由、公正かつ安全なサイバー空間を実現するために、幾つかの柱から外交的取組を推進してきています。具体的には、「法の支配の推

進」、「サイバー攻撃抑止のための取組」、「信頼醸成措置の推進」、「能力構築支援」といった柱です。

①まず、サイバー空間における「法の支配の推進」です。本年９月にも岸田総理が国連総会一般討論演説で国際社会における法の支配の重要性を訴えましたが、国際社会において、法の支配を確立することは、国家間の関係を安定させる上で、重要な意義があります。日本はこれまで、国際社会における法の支配を強化すべく、様々な分野において二国間・多国間でのルール作りとその適切な実施を推進してきています。

これと同様のことを、サイバー空間においても推進することが重要です。サイバー空間への既存の国際法の適用とルールの在り方については、国連において議論が進められてきており、関連の作業部会において、既存の国際法がサイバー空間に適用されることを確認するとともに、既存の国際法を補完する 11 項目の責任ある国家の行動規範を確認しました。

この規範には、例えば、「重要インフラに対するサイバー攻撃を受けている国から支援要請があれば協力すべき」であるとか、「国家は、自国の領域が ICT を用いた国際的な違法行為に利用されることを知りながら、それを許すべきではない」といったものが含まれます。これらの規範は、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すもので、それぞれの国家が責任を持って履行することが期待されています。

現在も 2021 年から 2025 年までを会期とする国連全加盟国が参加するオープンエンド作業部会が開催され、様々な議論が行われており、我が国も法の支配を推進する立場から積極的に議論に参加してきています。

②次に「サイバー攻撃を抑止するための取組」としてのパブリック・アトリビューションです。これは、各国がサイバー攻撃を行った主体に対する非難や懸念を公に表明することであり、その表明により、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らせることを目的としています。

我が国としては、これまで、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公に非難したり、2018 年に APT10 といわれるグループが長期に亘る攻撃を行ったことを公に非難しています。昨年７月には APT40 といわれるサイバー攻撃グループや中国人民解放軍 61419 部隊を背景に持つ Tick というサイバー攻撃グループが関与した可能性が高いサイバー攻撃について、外務報道官談話を発出し、同盟国・同志国と連携してこれらの行動を断

固非難しています。

また、先ほど申し上げた「法の支配の推進」は、サイバー攻撃を抑止する観点からも重要です。

サイバー空間では、その匿名性・隠密性により、攻撃者にとって「攻撃が露見するリスク」及び「仮に露見した場合のコスト」がいずれも低い状況にあります。一部の国家が、当該国発と考えられるサイバー攻撃に対して自国の関与及び責任を否定している現状においては、サイバー攻撃が国家に帰属しない場合でも、サイバー攻撃が自国の領域から行われた場合には、一定の条件の下で国家責任が認められるような国際社会のルール形成を行うことができれば、サイバー攻撃の抑止に資することになります。

③次に、サイバー空間における「信頼醸成措置の推進」です。サイバー空間は匿名性、隠密性が高く、意図せず国家間の緊張が高まり、事態が悪化するリスクがあります。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、国内法、規制、政策、戦略等について相互理解を深め、国家間の信頼を醸成することが必要です。

そのために、我が国はこれまで 14 の国・地域とサイバー協議や対話を行ってきました。また地域的な取組も重視しており、例えば、ASEAN、米国、豪州、EU 等が参加する ASEAN 地域フォーラム（ARF）では、我が国はシンガポール、マレーシアとともに共同議長を昨年 8 月まで務め、①サイバーセキュリティ環境に対する見方、②各国の取組、③国連等の国際社会の議論を踏まえ、今後取り組むべき信頼醸成措置等について議論を行いました。

④最後に「能力構築支援」です。世界中が繋がるサイバー空間においては、セキュリティに対する意識や対処能力が十分でない箇所、いわゆるセキュリティホールを経由して、サイバー攻撃が行われる可能性があります。サイバー空間におけるこのセキュリティホールが、日本を含む世界全体にとってのリスク要因となります。そのような観点から、他国及び地域の能力を向上させることはその国や地域だけではなく、世界全体の安全を守ることにつながるため、非常に重要なものです。

我が国は、開発途上国に対するサイバー分野での能力構築支援に係る基本方針に基づき、インド太平洋地域の中核となる ASEAN を中心に、外務省を含む関係省庁がその専門性を活かして能力構築支援を行っています。

具体的には、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」を設立し、共同の机上演習やワークショップ等の取組を行っています。また、国際協力機構（JICA）を

通じて、サイバーセキュリティ対策強化のための国際法・政策形成能力向上等を目的とした能力構築支援も実施しています。さらに、日本と ASEAN の関係者間の信頼関係強化及び政策調整促進のために「日 ASEAN サイバーセキュリティ政策会議」を開催しています。

引き続き、政府一丸となって、能力構築を必要とする国々に対して、戦略的かつ効果的な支援を行っていく予定です。

最後になりますが、「自由、公正かつ安全なサイバー空間」を実現するためには、政府だけの取組では十分とは言えません。

サイバー空間は、国、地方公共団体、民間企業、教育機関及び個人を含めマルチステークホルダーが築き上げてきた空間です。一部の国においては、国家によるデータ収集・管理・統制を強化する動きも見られますが、このような国家による過度な管理・統制は、国際的なマルチステークホルダーの取組に対する対抗であり、サイバー空間の発展を阻害することになります。民間企業、学術機関等の取組と政府の努力を有機的に結合させることによって、「自由、公正かつ安全なサイバー空間」を実現していくことが必要です。

こうした意味でも、今般日本において、日本経済新聞社様及び日経ＢＰ様により Cyber Initiative Tokyo 2022 という素晴らしいイベントが開催され、海外を含む産学官から多くの方々が参加し、様々な議論がなされることは大変意義深いものだと考えます。今後とも、「自由、公正かつ安全なサイバー空間」の実現に向け、外務省として積極的に活動して参ります。

御静聴ありがとうございました。