サイバー・イニシアチブ東京 2023

辻外務副大臣スピーチ原稿

御列席の皆様、こんにちは。外務副大臣の辻　清人です。サイバー政策を所掌しています。

本日は、「サイバー・イニシアチブ東京 2023」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。

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、自由、公正かつ安全なサイバー空間を確保する必要性はこれまで以上に増しています。しかしながら、重要インフラの機能停止や破壊、他国の選挙への干渉、身代金の要求、機微情報の窃取等、サイバー攻撃の脅威は急速に高まっています。

特に国家等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を目的として、ロシアは軍事的及び政治的目的の達成を目的として、北朝鮮は政治目標の達成や外貨獲得を目的として、サイバ

一攻撃等を行っているとみられています。

こうした中で、サイバーセキュリティの確保は、一国のみでの対応は極めて困難です。外務省としては、4 点、①「ルール・規範の形成・深化の推進」、②「サイバー攻撃抑止のための取組」、③「能力構築支援」、そしてこれらを効果的に進めるための④「国際連携」に整理される様々な外交活動を行い、自由、公正かつ安全なサイバー空間を確保すべく努めています。

①まず、「ルール・規範の形成・深化の推進」です。国連における四半世紀にわたる議論の結果、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、11 項目の責任ある国家の行動規範に合意しています。各国がこれらの規範を具体的に実践し、国家実行を積み上げていくことが重要です。

国連においては、現在も国連全加盟国が参加するサイバー関連の作業部会が開催され、我が国も積極的に議論に参加してきています。

②第 2 に「サイバー攻撃抑止のための取組」です。特に、攻撃者の特定が難しい中、攻撃を解析し、犯人を突き止め、これを公表することが、将来の攻撃への抑止力に繋がり得ます。

我が国としては、本年 9 月末に、中国を背景とするサイバー攻撃グループ

「Blacktech」（ブラックテック）によるサイバー攻撃について、日米合同の注意喚起を発出したほか、これまでに3度、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非難しています。

サイバー攻撃者を対外的に明らかにすることで、注意を喚起し、規範を形成し、更に、こうした行為の背景にある国家等にメッセージを伝えることで、攻撃者の将来の活動のコストを高め得る効果が期待されます。多くの国が共同でメッセージを出せれば、それだけ効果も高まることになります。

③第3に、「能力構築支援」です。サイバー空間には国境がないことから、一部の国や地域の脆弱性が世界全体のリスクに繋がり得ます。このような観点から、他国及び地域全体の能力を向上させることは、日本を守ることにもつながるため、非常に重要です。

日本は、インド太平洋地域の中核となるASEANを中心に能力構築支援を行っています。具体的には、タイに設立した「日ASEANサイバーセキュリティ能力構築センター」、世界銀行の下に設立された「サイバーセキュリティ・マルチドナー信託基金」等を通じた貢献や、JICAによる研修や資金協力・技術協力などを進めています。

④最後に「国際連携」についてです。これまで申し上げた取組を進める上で、

国際連携は非常に重要です。そのために、我が国は多くの国・地域とサイバー協議を行ってきており、今年は、英国、米国、フランス等との協議に加え、新たにNATOとの協議を立ち上げました。

また、マルチの取組も重視しており、日米豪印における協力や、ランサムウェアに対抗する国際的な協力であるカウンター・ランサムウェア・イニシアティブ等に積極的に取り組んでいます。

最後になりますが、「持続可能で強靱なデジタル社会」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あり、官民で有機的に連携することが必要です。

こうした意味でも、今般、このような素晴らしいイベントが開催され、国内外の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です。外務省としても、引き続き、自由、公正かつ安全なサイバー空間の実現に向け、外交的取組を強化していきたいと思います。

御静聴ありがとうございました。