資料 7

令和 7 年 2 月 5 日(水)

日本として喫緊に取り組むべき国家安全保障視点のサイバーセキュリティ課題

日本電信電話株式会社

松原　実穂子

今後、アジアでも紛争・戦争が十分起こり得ることを考えると、日本としてサイバーセキュリティを技術や経済安全保障の観点からだけでなく、国家安全保障の一部として取り組んでいくべきである。そのためには、今のうちから官民連携と司令部の在り方について議論を深め、方向性を決めなければならない。

ただ、重要インフラ事業者を含む民間企業には、国家安全保障の知見が足りず、国家安全保障上の大局観に立った総合的なセキュリティ対策や情報収集は非常に難しいのも事実である。政府でなければ収集し得ない機密指定情報を重要インフラ事業者のクリアランス保持者に提供し、民間企業のサイバーセキュリティ対策に役立て、国家安全保障に寄与していくことは、必要不可欠と考える。その際には、重要インフラ事業者が対象となる IT 資産を絞って対策を適時取れるよう、具体的な技術的情報に加えて、背景情報の提供も求められる。

さらに、クリアランスを持った政府関係者と民間関係者が議論するための SCIF、IT インフラ、通信・暗号、定期的な研修の整備も必要だ。これらは、仕様の一本化が肝要であり、民間企業独自の整備は不可能である。情報機関の出身者の活用も重要であろう。

また、官民がサイバー防御を高めていくには、定期的な合同演習も必要となる。目的が BCP の検証なのか、それとも有事におけるサイバー攻撃対応も含めた官民連携の在り方の確認なのかによって、参加する人の属性をリスク管理部門、事業本部、情報セキュリティ管理部門などから適切に選び、現実的なシナリオ作りをしなければならない。

NATO サイバー防衛協力センターが主催している年次国際サイバー演習「ロックド・シールズ」は、有事シナリオの中で官民連携の在り方を検証できる場であり、日本にとって非常に貴重な機会だ。官民連携の在るべき姿を司令塔として示していただき、日本のサイバーセキュリティ・安全保障の強化につなげていくために演習で浮かび上がった課題の洗い出しも進めていただくことも肝要と考える。

また、昨年 12 月末から 1 月にかけて続いた重要インフラを狙ったと思われる一連の

DDoS 攻撃は、官民連携、情報共有のタイミングと中身、司令塔に必要な機能・体制を含めた課題を見直すまたとない機会である。その検証なくして、能動的サイバー防御を含めた日本における官民連携は円滑に進め得ない。教訓を洗い出すために率直に議論し合える官民によるクローズドの勉強会が必要ではないか。

また、有事に備えるには、基盤的重要インフラ企業群（電力、通信、金融、ガス、石油、航空、鉄道、陸運、コンビニエンスストアなど大手 50 社程度）の CISO と NISC、防衛省・自衛隊、警察のサイバーセキュリティ幹部との間で、顔と名前が分かる関係作りも必要になるであろう。有事シナリオとして何が想定されうるのか、どのような連携が求められるのか、自衛隊 OB や海外の識者を招いた勉強会も一案と思料する。

以　上