サイバーセキュリティについて

2019(平成元)年 8 月 28 日
衆議院議員　松本　純

私は、現在、自由民主党の国会対策委員会委員長代理として、また、衆議院の国家基本政策委員会筆頭理事として、「汗する人が報われるニッポンへ」をスローガンに日々奔走しておりますが、平成 28 年８月から１年間、第三次安倍内閣の国務大臣として、警察を担当する国家公安委員会委員長、防災担当大臣等を務めておりました。また、政府のサイバーセキュリティ戦略本部のメンバーとして議論に参画し、施策の方向性の検討や各種の行動計画などの策定にも取り組んでいたところです。

御承知のとおり、警察は、捜査や犯罪防止・テロ対策などを行う機関ですが、サイバー空間においてもこれらの活動を活発に展開しています。私は、大臣として、こうした取組みについての報告を受ける中で、改めてサイバーセキュリティの確保が我が国の喫緊の課題であることを痛感しました。

来年、東京 2020 オリンピック・パラリンピック競技大会を迎えるにあたり、サイバーセキュリティについて、今までの経験なども踏まえたお話をさせていただきます。

私の大臣在任中は、「ワナクライ」（WannaCry）と呼ばれるランサムウェアの感染事案が発生しました。世界約 150 か国で政府機関、社会インフラのコンピュータが不正プログラムに感染し、英国の病院では手術が中止になるなどの影響が出たとされる事案です。米国は、北朝鮮によるものであると証拠を元に関与を指摘し、菅官房長官も記者会見で「事案の背後に北朝鮮の関与があった」と述べておられました。

また、平成 27 年 12 月、また 28 年の二回にわたり、ウクライナでサイバー攻撃によるとみられる大規模な停電が発生したほか、最近では、「エーピーティーテン」（APT10）と呼ばれるグループからの攻撃が世界的に確認されたところです。

このような攻撃は、国の機能、国民生活、企業活動に大きな影響を与え、場合によっては多くの人命に危害が及ぶおそれがあるほか、国家の関与も取りざたされる例もあり、各国と緊密に連携しながら、国としてしっかりと対応していかなければならないものであります。

また、身近なところでは、私のスマホにも、個人情報の不正な入手のため偽サイトに誘導したり、覚えのない口座入金を促すようなメールが着信することがあります。こうしたことは皆さんも同じかと思いますが、多くの国民がサイバー犯罪の危険にさ

らされているわけであります。

こうしたサイバー犯罪について、インターネットバンキングを狙った不正アクセスへの対策が進み、大臣在任中の被害額はピーク時の約半分にまで減少しましたが、最近は、暗号資産を狙った犯罪が度々発生し、数百億円相当が流出した事案など、甚大な被害が出ています。

今年は、フェイスブックが主導する暗号資産「リブラ」についての報道もありました。27億人ともいわれるフェイスブックの利用者を背景に、利用が急速かつボーダレスに拡大する可能性もあります。金融システムへの影響やマネーロンダリング対策などの課題が指摘され、各国間で検討も進められるなか、利用者保護やセキュリティの確保も必須であり、今後注目していく必要があると考えています。

こうした中、昨年７月、政府は「サイバーセキュリティ戦略」を閣議決定しました。

ここではサイバー空間の持続的な発展のため、全ての主体が自律的にサイバーセキュリティに取り組み、「参加・連携・協働」する方針を定めています。平成27年の日本年金機構の保有する個人情報の流出事案は、御記憶に新しいことと思います。サイバー空間の脅威による経済的・社会的損失が多大なものとなり得る以上、外部からの侵入防止と安全性の確保のため、必要な機器・サービスを整え、内部の脅威にも対峙し、これを未然に防止する対策は極めて重要です。なかには、OS・ソフトウェアの更新、セキュリティソフトの導入、パスワードの適切な管理、適切なアクセス権の設定など、基本的な事項を遵守していれば、被害防止が可能であったとの事案も見受けられます。官民ともに、今一度、基本に立ち返り、自律的に必要な対策を確実に実施していかなければなりません。

また、こうした観点からは、タイムリーな情報の提供と共有も重要です。

いまや、例えば、内閣サイバーセキュリティセンター、警察庁、アイピーエー（情報処理推進機構（IPA））、ニクト（情報通信研究機構（NICT））等の政府関係機関、ジェーシースリー（日本サイバー犯罪対策センター（JC3））等の民間団体、「シマンテック」を始めとするセキュリティベンダーなど、官民の様々な主体から、脅威や対策に関する有益な情報が数多く発信されています。技術や攻撃の手口が日々進化する中で、これらを不断に把握し、活用していくというユーザー側の取組みも大いに求められるところであると思います。

さらに、これらの取組みを支える基盤として、なんといっても大切なのは、情報セキュリティ人材の育成・確保であります。政府機関でも取組みを強化しており、中途

採用や官民の人事交流のほか、例えば、関係省庁対抗による競技形式のサイバー攻撃対処訓練（「ナショナル・サイバー・エキデン」）が開催されるなど、全体的な能力向上に取り組んでいます。こうした分野の人材の争奪戦が官民で繰り広げられるなか、政府機関における人材確保がなかなか難しいという話を耳にすることもあり、率直なところ、当時、「民間の有為な人材を、官の側に割いていただくことも大事なのだが」と思ったこともございます。

いずれにしても、経営・管理者層の意識改革とともに、核となる人材の存在いかんで、サイバーセキュリティの水準は大きく変わりうるものであります。引き続き、官民ともに、一層力を入れていかなければならないと思います。

サイバー空間の脅威といえば、2020 年オリンピック・パラリンピック東京大会に触れないわけにはいきません。2012 年のロンドン大会、2016 年のリオ大会でも、数多くのサイバー攻撃が発生し、ピョンチャン（平昌）大会では、大会準備期間中にサイバー攻撃が多数発生し、開会式において、メインプレスセンター内でネットワーク障害が発生したとされています。大規模な国際大会がサイバー攻撃の標的となったわけであります。

2020 年東京大会においても、このような攻撃が懸念されます。政府では、脅威情報の共有などを担う「サイバーセキュリティ対処調整センター」の運用、重要サービス事業者のリスクアセスメントを行っているほか、警察においても、事業者と連携した共同対処訓練を重ね、対処能力の向上を図っています。

今まさに、クラウド、アイオーティー（IoT）、エーアイ（AI）、フィンテック（Fintech）など、サイバー空間における技術・サービスは、活用分野が拡大しつつあり、重要性を増す一方で、これに対する脅威とその影響も大きく増大しているといえます。皆様方を含め、官民のあらゆる主体が連携し、意識高く、タイムリーに対処していくことが不可欠となります。

来年の今頃は、オリンピックが終わり、パラリンピックが始まっています。2020 年東京大会とその先の未来に向けて、心を一つにオールジャパンで取組みを展開していくことが大切であると思います。

国民の生命・財産をしっかり守っていく決意のもと、出来ることは全てやるといった取り組みを進めていきたいと思います。

（以上）