2014 年は、世界中でサイバー攻撃が急増した一年であった。政府機関や民間企業だけでなく、国民の被害も急増し、我が国も含め欧米各国はその対応に迫られた。日本では、特に 2020 年の東京オリンピックに照準を合わせ、サイバーセキュリティの推進体制を整えようとしている。しかし、政府主導のサイバーセキュリティ体制の強化は、諸刃の剣であり、政府による国民監視体制の強化にもつながりかねない。今回はこの部分に焦点を合わせ、最近の動向について紹介する。

東京五輪をめざし政府もサイバーセキュリティに取り組みはじめたが

日本政府は、2015 年を迎え、サイバーセキュリティ対策に取り組む体制を、ようやく整えた。2015 年 1 月に、サイバーセキュリティ戦略本部と、その事務局である内閣サイバーセキュリティセンター（NISC）を発足させた。

同時に、議員立法で「サイバーセキュリティ基本法」を施行させた。この基本法は、ＩＴ基本法（2001 年 1 月施行）と補完関係に位置するもので、サイバー攻撃に関する国の責任などを明確にしたものである。

この背景には、最近の政府・企業に対するサイバー攻撃の急増がある。情報通信研究機構（NICT）によれば、サイバー攻撃に関連するとみられる通信は、2014 年に約 256 億 6 千万件（観測点約 24 万アドレス）と急増した。それまで最高であった 2013 年の約 128 億 8 千万件（同約 21 万アドレス）から、ほぼ倍増している。

政府が対応を急いでいるのは、それだけではない。NHK が、「東京五輪へサイバー攻撃対策の戦略本部を設置」（2015 年 1 月 9 日ニュース、下線は筆者）と報じているように、2020 年の東京五輪に向けてのサイバーセキュリティ対策が、急務になっている。

政府首脳自らも、この点を強調している。安倍首相は、上述のサイバーセキュリティ戦略本部の会合の冒頭で「東京五輪・パラリンピックを成功させるためにもサイバーセキュリティに万全を期す必要がある」と述べている。東京五輪組織委員会会長の森喜朗（元首相）も、「オリンピックでの最大の問題はサイバーセキュリティだ」と断じている。

これには、前回の 2012 年のロンドン五輪におけるサイバー攻撃が、念頭にある。ロンドン大会の公式サイトが 2 億件以上のサイバー攻撃を受けていただけでなく、開会当日には、ロンドンの電力システムが狙われ、停電の危機に直面していたからである。

2008 年の北京五輪の時に比べて、サイバー攻撃は 7 倍にも増えていたと指摘されている程、この 4 年間の間に、サイバー攻撃は急増していた。パソコンからスマホの時代に移り、インターネットに接続するデバイス数が、急増したことが背景にある。

インターネットへの接続台数は、2010 年に 125 億台、2015 年に 250 億台と倍増し、2020 年には 500 億台（予測）になると予想されている（出所 Cisco IBSG、2011 年 4 月）。これは、接続台数が増えるといった単純な問題ではなく、質的な変化を意味している。

IoT（もののインターネット）の時代を迎えているからである。単純に考えて、東京五輪のサイバー攻撃は、ロンドン五輪とは量的にも質的にも異なると危惧される。オリンピックだけでなく、競技に関連するサービスやシステム、更に市民生活までもが、サイバー攻撃の対象となる。一歩対応を間違えれば、お祭り騒ぎどころではなくなってしまう。

このように日本政府がサイバーセキュリティ対策を整えようとしている矢先の 2015 年 5 月に、日本年金機構の年金個人情報流出事件が起きてしまった。ウィルス Emdivi（エンディヴィ）に感染したもので、流出した個人情報（基礎年金番号、氏名、生年月日、住所など）は、同機構によれば、6 月 1 日時点で 125 万件に達しているという。

残念ながら、この事件は氷山の一角に過ぎなかった。政府や厚生労働省のその後の調査で、政府関連組織、地方自治体、民間企業も被害を受けていた事実が判明している。三上洋（IT ジャーナリスト）は、「34 組織で年金機構と同じウィルス感染か」（YOMIURI ONLINE 、2015 年 6 月 26 日）と報じている。

ちなみに、ウィルス感染もしくは情報流出した組織体には、法務省、長野県上田市、ひろしま国際センター、健康保険組合連合会、香川大附属病院、国立精神・神経医療研究センター、早稲田大学、石油連盟、東京商工会議所などの名前が、挙がっている。

サイバーセキュリティの推進は、国民の監視強化に繋がりかねない

政府のサイバーテロ対策の体制強化は、同時に、国民の監視や個人のプライバシー侵害に繋がりやすい。この両方のバランスをうまくとるのは、非常に難しい。

テロリストやサイバーテロの脅威が高まると、政府による国民のメールやスマートフォンの通信傍受が強化される。それは、テロとは無関係な国民への無差別な通信傍受へと発展しやすい。何かの拍子に、この行き過ぎた実態を世間が知る所となると、国民から一斉に反発を招くことになる。

分かりやすい前例が、アメリカである。2001 年 10 月の「米国愛国者法（USA PATRIOT Act）」から、2015 年 6 月の「米国自由法（USA Freedom Act）」（愛国法の失効に伴う新法）に到る経緯が、大きな教訓になる。

米国愛国者法は、2001 年 9 月 11 日の同時多発テロ事件への対処として、事件後わずか 45 日後という超スピードで成立した。同時多発テロへのアメリカ国民の怒りが、この立法化を後押ししたといってよい。

これにより、NSA のテロ監視に係る権限は大幅に拡張され、多数の米国市民の電話、ネッ

トにおける通話記録などが、収集されることになった。この結果、それまでの常識からは考えられないような事件や事実が、相次いで暴露され表面化したのである。

たとえば、米紙ワシントン・ポストは「NSA が 1 日で全世界の携帯電話 50 億台の位置情報を収集していた」（2013 年 12 月 5 日）と報じた。また、FBI や地域警察が、携帯電話基地局になりすまして、スマホから情報収集する「スティングレー（Stingray）」という装置と監視プログラムを使い、米国民を秘密裏に監視し捜査していた事件が、訴訟で明らかにされた。

これは対岸の火事ではない。日本でも同種の事件で、訴訟が相次いでいる。警察による GPS 機器による容疑者・関係者の車両に対する監視である。これは、警察の内規に基づいて行われているが、その違法性を巡って各地で訴訟がなされている。

この訴訟の中で、兵庫県小野市の郵便局での収入印紙盗み事件について、大阪地方裁判所は「令状なしに長期間、行動を監視したのはプライバシーの侵害にあたり違法だ」という判断を下している。

さて、アメリカの話に戻すと、2013 年 6 月、元 CIA 職員スノーデンの告発事件で、米国民に対する NSA の情報収集の実態が暴露された。テロ容疑に関係なく米国民の膨大な個人情報収集の実情が次々と明るみになり、米国民の批判が NSA に集中した。この結果、それまでの NSA による情報収集を大幅に制限する形で、今年、米国自由法が成立したのである。

この問題は、アメリカだけではない。フランスの風刺週刊紙銃撃事件（2015 年 1 月）など、欧米での相次ぐテロ事件の発生である。これらの事件を受けて、オバマ米大統領と英国のキャメロン首相のホワイトハウスでの会談で、テロリストによるサイバー攻撃への対策を強化していくことで一致した。

キャメロン首相は､暗号化通信を制限する意向を表明している。「危機的な状況においても、内務大臣本人が署名した令状をもってしても内容を知ることのできない通信手段を、わが国で許可すべきなのだろうか」と述べている（CNET Japan 2015 年 1 月 13 日）。つまり、英国は、政府による国民のスマホ監視を容易にしようとしているのである。

最後に、日本の現状を見ておこう。日本では 2013 年 12 月に「特定秘密保護法」（秘密保全法を名称変更）が成立し、さらに、2000 年に施行された通信傍受法の改正案が、今国会で審議中である。

このなかで、「盗聴法拡大を閣議決定　警察施設内で警察だけの盗聴を認める通信事業者の立ち会い（監視）が不要に」（2015 年 3 月 14 日）のニュースにあるように、「盗聴法の拡大」も、閣議決定されている。

この「盗聴法の拡大」は、小渕政権下での「通信傍受法」(1999 年に、強行成立させ問題となった)で制限していた警察の盗聴範囲を、大幅に緩和している(「通信傍受法の改正 盗聴拡大が招く監視社会 」（信濃毎日新聞、2015 年 5 月 31 日）を参照)。これまでの歴史的経緯を振り返ると、政府は無理を重ねてきているという印象をぬぐえない。

我が国のサイバーセキュリティ対策が功を奏し､2020 年の東京オリンピックを成功理に終わらせるためには、国民の信頼と協力を勝ち取ることが不可欠といってよい。

もし、年金個人情報流出事件のようなお粗末な事件が繰り返されたり、警察による一般人の盗聴や GPS 監視などが行き過ぎて、国民の信頼を失う事件が発生すれば、2020 年の東京オリンピックを平穏無事に終わらせることは、難しくなるかもしれない。

（TadaakiNEMOTO）