日本の国会議院がサイバーテロ攻撃を受けた。それへの対応の鈍さは世界のトップレベル。とてもではないが、コンピュータ保有規模世界第二位の国のものではない。政治家、官僚など日本政府中枢の情報管理リスクに対する意識の低さが改めて露呈された。

大がかりなサイバー攻撃が繰り返された 2011 年

2011 年 10 月 25 日、朝日新聞が衆議院へのサイバー攻撃を報道したのが、事件の始まりであった。次いで 11 月 2 日には、参議院でもサイバー被害にあっていたことが報道され、国家の中枢機関や防衛産業が、相次いでサイバー攻撃に曝されていた事実が、国民に次々に明らかにされることになった。

衆議院の事務局によれば、ウィルス感染は今年 8 月 28 日ごろに判明していた。3 人の衆院議員のノートパソコンがウィルスに感染し、これらのパソコンからサーバー自体にウィルスが転移して国会議員の ID、パスワードが盗まれ、国会議員や秘書らの 2700 名のメールや文書が覗き見される被害に、広がってしまったのである。

この原因は、サーバーを管理している NTT 東日本が、ウィルス感染の被害を警告したにもかかわらず、衆議院事務局はなんら対策をとらず警察への届けもせず、少なくとも 1 ヶ月もの間、国会のパソコンやサーバーは、無防備の状態に放置されてきた点にある。

参議院での被害は、参議院議員のパソコン計 29 台がこの 8 月から～10 月末にかけて、中国やシンガポールのサイトに、勝手に接続されていた痕跡が確認されたという。衆議院での被害対策の遅れが、参議院にまで被害を拡大したものといえる。

被害にあったのは、衆議院や参議院だけではなかった。産経新聞（10 月 26 日付け）によれば、日本大使館など在外公館の海外の約 10 ヶ所のコンピュータも、夏以降、外部から情報を抜き取る「標的型メール」によるサイバー攻撃を受けていたのである。

NHK の調査（10 月 26 日報道）によれば、少なくとも 16 の省庁で、職員にコンピュータウィルスが添付されたメールを送りつけられるサイバー攻撃を受けていたという。国会議員だけでなく中央官庁から海外の大使館まで、日本の主要機関すべてが、サイバー攻撃

を受けていたことになる。

さらに、サイバー攻撃を受けていたのは、政府機関だけでなく、三菱重工、三菱電機、IHI、川崎重工業などの大手総合重機メーカーや、日本航空宇宙工業会や国土地理院といった組織体にまで、広がっていたのである。

三菱重工では 11 ヶ所の生産拠点でサーバーやパソコン計 83 台がウィルスに感染していたことが判明し、80 式空対艦誘導弾の耐久性や性能を記した管理報告書の一部が流出した可能性が指摘されている。今年 9 月 30 日に、警視庁に被害届を提出している。

このようにみてくると、2011 年は、我が国の様々な重要な機関が、大規模で計画的なサーバー攻撃を受けていた 1 年であったことがわかる。それにもかかわらず、今年の暮れまで、国民にその全貌が明らかにされてこなかったのである。

求めせられるサイバーテロへの意識改革

今回ここで問題提起したいのは、主要閣僚をはじめとする国会議員や官僚たちの、サイバーテロに対する危機管理意識の欠如である。事件発覚直後のテレビニュースの会見において、某大臣が「こんなことが本当にあることなのかなという思いをいたしました」と、全く他人事のように平然と発言していたことは、全く理解に苦しむ。

さらに、衆参両院でのサイバー攻撃が発覚した後、衆院事務局の呼びかけ（10 月 25 日と 27 日の 2 回）に応じて、パスワードを変更した議員は、半数以下にとどまっていたという。11 月 2 日に、同事務局が全議員に照会したところ、貸与パソコン 2 台のうち 1 台以上で「パスワードを変更した」と回答した議員は 45%。「変更していない」や無回答は 55%に上った（読売新聞）という。

今回の事件で、国会のセキュリティ対策を業者まかせになっていた実態も明らかになった。衆議院での情報漏えいが報じられた 10 月 25 日、衆院情報化推進室の加藤祐一室長は、「調査は業者に丸投げしており、具体的なことはわからない」と答えている。同室長は、8 月末にウィルス感染が見つかり、9 月初めに業者に調査を依頼し、2 ヶ月弱が過ぎた 10 月 25 日現在でも、調査結果は出ていないとも、話している。

サイバー攻撃に対する国会議員の危機意識の欠如は、2010 年 11 月に行われた行政刷新会議の事業仕分け第 3 弾でも、表面化していた。サイバーテロ対策の事業予算は強く批判され、カットすべきとされたのである。

民主党の仕分け人は、「ウィルス対策ソフトの作成なんて、民間がやっていることはやらなくていいんじゃないですか」と、独立行政法人「情報処理推進機構（IPA）」（国内唯一のコンピュータウィルスの公的届け出機関）を、強く批判したのである。

さて、サイバー攻撃が狙う一番のターゲットは、仮想敵国の最高責任者が使用する情報機器であり、パソコンよりは携帯電話やスマートフォンであるといってよい。

ギリシャでは、カラマンリス首相から閣僚そして政府高官まで 100 台の携帯電話が、2004 年から 05 年までの約 9 ヶ月の間盗聴されていたことが、2006 年 2 月に明らかにされている。

アメリカでは、バラク・オバマが大統領に選出された時、新大統領による携帯電話の使用が大問題になった。アメリカでは、国家安全のセキュリティ対策のため、前の 2 人の大統領、クリントンもブッシュも、携帯電話の使用は認められていなかったのである。

オバマ大統領については、少数の幹部および個人的な友人との連絡に限定し、かつ大幅

なセキュリティ強化を施すという条件付きで、認められたのである。これによって、オバマ大統領は、携帯電話の使用を許可された初めての大統領になったのである。

では、日本の首相の場合はどうなっているのか。これについては、民主党の加賀谷健参院議員による麻生元首相への「危機管理の観点からの麻生総理大臣の携帯電話に関する再質問主意書」（2009 年 6 月提出）によるものがある。政府側の答弁書では、躯体的な対策措置については「首相の情報の保全等に支障を及ぼす恐れがある」というだけで、セキュリティ策については、一切明らかにされていない。

首相による携帯電話のお粗末さが伺われる実態が、この 3 月に表面化している。管元首相が、松本防災相への携帯電話を一般人と間違えた事件である（週刊文春 3 月 31 日号)。この間違い電話は、3 度も繰り返されたという。国家の最高責任者の携帯電話の利用については、米大統領並みとは言わないが、厳しい対応措置が取られるべきであろう。

サイバー戦争時代への対応を急ぐべし

今回、我が国で大きな関心を集めたサイバー攻撃は、日本のみをターゲットとしたものではない。新唐人テレビ（NTDTV）は、「史上最大のサイバー攻撃 大戦に発展か」（2011 年 8 月 13 日付け）で、太平洋を取り巻く諸国へのサイバー攻撃の実態を報告している。

「ネットセキュリティ会社 McAfee（マカフィー）によると、サイバー攻撃を受けたのは、アメリカ、台湾、インド、韓国、ベトナム、カナダなどの政府と東南アジア諸国-連盟、国際オリンピック委員会と国連のほか、軍需企業など 79 に及びました。そのうち、半分以上がアメリカに集中しています」と報じている。

サイバー攻撃が世界の注目を集める事件は、2000 年前後から起きている。1999 年のコソボ紛争への NATO 軍の介入の際には、NATO 軍に対するサイバー攻撃が注目を集めた。2001 年のアメリカの同時多発テロ事件を契機に、インターネットが普及する先進諸国へのサイバーテロの危機が、大きな関心事となった。

それだけでなく、先進諸国の同盟国間の間でも、サイバー戦争が展開されている事実が表面化している。2001 年 7 月、欧州議会でエシュロンによる欧州諸国に対する通信傍受被害について報告書が発表され、米国による欧州諸国への盗聴が批判された。

現在のサイバー攻撃の脅威は、ロシア、中国、北朝鮮などからのものとされている。新唐人ニュースは、「中国とロシアの情報機関が、サイバー攻撃を通じてアメリカの機密文書を盗んでいると、アメリカ政府が批判している」（2011 年 11 月 7 日）と、伝えている。

アメリカでは、2009 年にアメリカサイバー軍（United States Cyber Command; USCYBERCOM）を設置し、2010 年 5 月には、戦略軍傘下に「サイバー司令部」の設立を発表し、各軍におけるサイバー対策の取り組みを統括する体制を整えている。日本では、2012 年 3 月に、自衛隊にサイバー空間防衛隊が新設される予定になっている。

今回のサイバー攻撃騒動では、首相から閣僚・国会議員を含めて、危機管理意識の低さが大きな問題になったが、それ以上に、中央官庁の縦割り行政の不備が表面化したといってよい。内閣官房の情報セキュリティセンター（NISC）も、その機能を果たしているとは言い難い状態であった。

政府、この 10 月 7 日に、3 ヶ月ぶりに「情報セキュリティ政策会議」を開き、サイバー攻撃に対処するために「官民連携強化のための分科会」の新設を決めている。抜本的なサイバーテロ対策が、僅々の課題になっているといってよい。 （TadaakiNEMOTO）