21世紀政策研究所
21PPI NEWS LETTER
2018年5月発行
MAY 2018
NO.61

研究主幹に聞く 「サイバー安全社会に向けて：企業の責任・国家の責務」プロジェクト

# Society5.0時代のサイバーセキュリティを検討する

中曽根康弘世界平和研究所主任研究員
大澤　淳氏

**21世紀政策研究所では、サイバーセキュリティに関する研究プロジェクト（研究主幹：大澤淳・中曽根康弘世界平和研究所主任研究員）を立ち上げ、サイバーリスクの変容やサイバーセキュリティの在り方について研究を進めています。AI、IoT、ビッグデータ等の活用により、あらゆるモノや人がサイバー空間とつながるSociety5.0時代が到来すると、ビジネスから人々の生活に至るまで、サイバーセキュリティ上の脅威は一層高まるものとみられます。そこで、大澤研究主幹にわが国のサイバーセキュリティの現状や課題等について、お話を伺いました。（4月27日）**

――わが国のサイバーセキュリティの現状について教えてください。

2012年度にも、21世紀政策研究所のサイバーセキュリティ研究プロジェクトに携わりましたが、その頃はサイバー攻撃に対する社会の認知度がまだ低い状態でした。その後、様々な事案が発生したことで、現在はサイバーセキュリティに対する世の中の認識が高まり、「守る」という点ではセキュリティ技術の進歩や企業努力によって一定の水準に達してきたといえます。

しかし、海外では、「サイバーセキュリティ」が国の安全保障の問題として広義に捉えられており、サイバー空間で攻撃者がどのような行動を取っているのかについての「状況認識」も「サイバーセキュリティ」に含まれています。つまり、諸外国においては、日本のような受動的な防御に加え、反撃も含めたより能動的なサイバーディフェンスを行なっており、そうした視点は日本にまだ足りないと考えています。

――近年のサイバー攻撃にはどのような変化が生じているのでしょうか。

2017年にWannacry、Not-Petyaという２つのサイバー攻撃が発生しましたが、これらは国家が関与するサイバー攻撃でした。国家が自らの技術を活かして民間企業などを攻撃するという意味では、この１年間でサイバー空間におけるリスクがより一層高まっています。わが国として、果たして今までの受動的な防御だけでこうした新しい攻撃に対処できるのかという問題に直面しています。

上記の２つの事例では、ある程度セキュリティにお金をかけているであろうグローバル企業ですら、攻撃を防ぐことができず、国家が関与する攻撃に対しては受動的な防御のみでは防げないことを示しています。また、Wannacryのケースでは、１週間から10日ほどで世界的に感染が広がっていて、日本企業の一部も被害を公表しています。防げないという

（次頁に続く）

ことと、世界で一斉に感染が広がるリスクもあることから、私は、WannacryやNot-Petyaのようなケースを「サイバーパンデミック」と表現しています。昨年の事案は欧州中心に発生した事案だったため、日本企業の被害は幸い少なかったのですが、このサイバーパンデミックが仮にアジアを中心に起こった場合、日本企業の業務継続にも影響を与えかねません。

**―――わが国におけるサイバーセキュリティは、どのような課題があるのでしょうか。**

受動的な防御を越えて、サイバー空間で一体何が起こっているのかを把握することに対しては、国や企業の体制が十分に整っていないことがわが国の現状だと思います。また、日本でサイバーセキュリティの技術を導入する際には、欧米の技術をそのまま買ってくることが圧倒的に多く、オリジナルのサイバーセキュリティの産業や人材が育っていないという問題もあります。

サイバーパンデミックや国家が関与するサイバー攻撃に対しては、残念ながら企業単体では自分のネットワークを守りきることができません。そのため、国家の責務として、政府がサイバー攻撃の背後にいる国家主体に対して牽制・抑止を行なう必要があると考えています。一方、民間企業は、攻撃の様態に関する情報共有をきちんと行なっていく責任があると考えています。

キーワードは、「サイバー状況把握（CSA：Cyber Situational Awareness)」です。誰がどのような手口で何を目的に攻撃しているのかをリアルタイムに把握することによって、まだ攻撃されていないところを守ることができます。これは、今後最も重要な課題の一つです。

ここから先の10年を考えたとき、IoT、ビッグデータ、AIなどの普及により、常にネットワークと繋がる社会になる中、産業活動だけでなく、生活や国家の運営なども依拠するサイバー空間を安全に保つことができるのか、今まで以上に大きな課題となっていくでしょう。

**―――今回の研究プロジェクトの目的は何ですか。**

新しいリスクの顕在化やSociety5.0時代におけるサイバー空間というものを考えた時に、具体的にどのようなリスクが生じうるのかを把握することが、本研究プロジェクトの目的の一つとなります。近年、国家が関与するサイバー攻撃の増加や、米国大統領選挙でみられたようなサイバー空間を利用した内政干渉など、サイバーリスクが変容しています。しかしながら、こうしたサイバーリスクの変容に関し、日本の社会ではまだ理解が進んでいません。このプロジェクトでは、サイバーリスクの変容を明らかにし、会員企業をはじめとする日本の産業界の皆様と認識を共有したいと思います。

加えて、今後、ネットワークにつながった機器が自律的に社会の中で働く時代となります。その中で、サイバーリスクの変容を踏まえ、サイバー空間の安全を維持するために産業界としてどのような対応が必要なのか。具体的には、セキュリティの在り方として、どのような技術を採用すべきか、どのような体制をとる必要があるのか、どのくらい予算をかける必要があるのかといったことや、CSAの観点から、業界内あるいは業界を跨いだサイバー攻撃情報の共有をどのように行っていくのかについてもお示ししたいと思います。

また、サイバー攻撃の中には、企業がある程度のコストをかけてセキュリティ対策を講じていても防げないものがあり、国の責務としては、国家を主体としたサイバー攻撃の情報をいち早く把握して、攻撃主体であると考えられる国に対し、外交的な抗議や経済制裁などを行い、相手の国の行動を抑止することが考えられます。このような国の責務を果たす上で、どのような法制度が必要なのか、どのような官民連携が必要なのか、そういったことも議論していきたいと思います。

さらに、社会のあり方や企業の文化について、欧米諸国では、サイバー攻撃を受けた企業が被害状況

をいち早く社会に公表し、そうすることで、できるだけ他の企業が同様の被害にあわないようにすることがトレンドとなりつつあります。一方、日本の場合、サイバー攻撃による被害が生じた際には、企業が責任を感じる、あるいは被害を隠すということもあります。そうした社会のあり方や企業の文化なども、この研究プロジェクトの中で議論したいと考えています。

**――21研の研究プロジェクトだからこそ議論できることは、どのようなものがあるでしょうか。**

企業がどのような行動をすべきなのかという議論は、経団連本体でもなされていると思いますが、それとは異なる観点で、例えば国の法制度をどうするべきかという問題があります。

最近、政府が通信インフラ企業に対して漫画村のアクセス遮断を要請したという報道がありましたが、この議論には漫画家の著作権を守るという価値観と、憲法第21条に定められている「通信の秘密」を守るという価値観が衝突しています。同じことが、サイバーセキュリティの問題でも起こりうると考えています。サイバー攻撃の踏み台となるサーバからのアクセスを通信インフラ企業に遮断してもらえると、サイバー攻撃をすぐに防ぐことはできますが、そのためには通信の中身を見て攻撃サーバを特定することが必要となります。つまり、サイバー空間を守るという価値観と、「通信の秘密」を守るという相反する価値観が衝突する領域となります。このような憲法にもかかわる価値の問題に関しては、政策研究の中で十分議論することが重要であると考えています。

また、欧米諸国では、サイバー空間を守っているのはインテリジェンス（諜報）機関です。そうした国同士であれば、インテリジェンス機関の情報共有制度の中でサイバー攻撃に関する情報を共有することができ、また、民間企業においてもセキュリティクリアランス制度（情報の取扱いができる者を認定する制度）が導入されているため、政府と民間企業との間における情報共有が可能です。つまり、欧米諸国では、国家公務員だけでなく、民間企業に勤める人にもセキュリティクリアランス制度の対象を広げているため、クリアランスを持っている人同士で機微な情報を共有することができます。

一方、わが国は、特定秘密保護法によって政府におけるセキュリティクリアランス制度は確立していますが、民間企業にはセキュリティクリアランス制度がありません。そのため、国が把握している機微な情報を民間企業と共有することができません。欧米諸国の制度をみながら、日本としてどのような制度設計が良いのか、自由な議論の中で検討してみたいと思います。

**国家が関与したとみられる主なサイバー攻撃事案**

| | |
|---|---|
| 2015.12 | ウクライナ東部の電力網に機能破壊型のサイバー攻撃で22万世帯が停電<br>（国家が関与する初の重要インフラへのサイバー攻撃） |
| 2016.2 | バングラデッシュ中銀からサイバー攻撃によるSWIFT不正送金被害 |
| 2016.3 | スウェーデンニュースメディアに対する機能妨害型攻撃 |
| 2016.4 | リトアニア議会に対する機能妨害型攻撃 |
| 2016.8 | ベトナムの国際空港のシステムがサイバー攻撃により乗っ取られる |
| 2016.11 | サウジの政府機関・企業に対する機能破壊型攻撃 |
| 2016.11 | 米国民主党全国委(DNC)に対するロシアによる情報窃取型攻撃 |
| 2016.12 | ウクライナ首都の変電所へのサイバー攻撃により10万世帯が停電 |
| 2017.5 | Wannacryランサムウェアが全世界に拡大（日米英など北朝鮮の犯行と断定し非難） |
| 2017.6 | Petya亜種ランサムウェアが全世界に拡大（米英豪加などロシアの犯行と断定し非難） |
| 2017.10 | Bad Rabbitランサムウェアがロシア東欧を中心に拡大 |
| 2018.2 | 韓国平昌オリンピック委員会への機能停止破壊型攻撃 |

**インタビューを終えて**

今Society5.0時代に向かうなか、人々の生活がより便利になる一方、サイバー攻撃の脅威は一層高まり、もはや誰もが避けることのできないリスクとなりつつあります。わが国のサイバーセキュリティは、情報連携や法制度、社会の在り方など様々な課題を抱えていますが、何よりもまずは国、産業界、社会がそれぞれの立場からサイバーセキュリティの問題を自らの問題として捉え、危機意識を常に抱きながら向き合っていくことの必要性を感じました。

本プロジェクトでは、今後、シンポジウムや報告書等を通じて研究成果の報告を予定しています。

（主任研究員　松藤希代子）