防衛計画に見るサイバーセキュリティの現状

執行役員　堀　好成

１　はじめに

穏やかに迎えたオリンピックイアー、２０２０年は、中国武漢を震源地とする新型コロナウイルスの世界的感染爆発により世界が大きく変わる年となった。1 月末には、感染は中国国内にとどまらず、欧州から米国、そして世界規模のパンデミックとなり、瞬く間に世界の動きを凍り付かせた。

日本でも 4 月 7 日には緊急事態宣言が出され、社会活動が大きく制限されることになった。世界を襲った新しい脅威を、いかに早く克服し、立ち直るかは、世界の中での覇権にもつながる。震源地と言われる中国が、多くの犠牲者を出しながらも、治療対応実績をベースに世界への影響力を拡大しようとしている。世界規模で、このような状況が作り出せたことは、バイオテロや細菌戦の脅威が現実味をおびてくる。いわゆる見えない兵器の恐ろしさであり、見えない攻撃に備えることの難しさが認識されることになった。

同様に、いつどのように攻撃が仕掛けられているのかの認識が困難な分野として、最近大きくクローズアップされてきているのがサイバーである。国家の各種システムへの攻撃から、軍事組織の混乱・破壊、生活インフラや経済活動の麻痺、身近なところでは個人情報の流出・悪用まで、そのレベルや種別は多種多様である。しかもその結果は国家の存立にも繋がりかねない。各国ともこのサイバー分野での攻撃からいかに防御するかに多くの資源を投入してきているが、気付かないうちに被害が生じているという事例が多く伝えられる。

我が国もその重要性を認識しており、２０１８年１２月に閣議決定された「31 年度以降に関わる防衛計画の大綱（以下新防衛大綱という）」において「新たな領域における能力の獲得・強化」が述べられている。「中期防衛力整備計画（平成 31 年度～平成 35 年度）（以下中期防という）」では、我が国を取り巻く防衛環境の変化により、「宇宙、サイバー、電磁領域」という新領域に関する能力向上を喫緊の課題とすることが明示された。この新たな領域の頭文字をとって「うさでん」と総称しているそうだが、自衛隊にとって、三つの領域にはそれぞれ異なる背景と歴史がある。

全く新しい領域と言える「宇宙」。これまでもその重要性は認識されながら、各自衛隊・部隊とも、能力向上が進んでこなかった中で、近年各国の能力が格段に向上し、戦力発揮の成否を左右するまでになってきた「電磁波」。日常の環境に幅広く、深く入り込んでおり、防衛の中枢までシームレスに影響を及ぼしかねなくなった「サイバー」と、それぞれ異なる。ここでは、将来の戦いの成否を握るとされるこの新領域の内、日常の問題にもつながる「サイバー」について、防衛計画のレベルから日常生活における問題点までを概観してゆきたい。

２　新防衛大綱に見る「新たな領域」

大綱策定の趣旨として、「我が国を取り巻く安全保障環境は、きわめて速いスピードで変化していて、国際社会のパワーバランスの変化は加速化・複雑化し、既存の秩序をめぐる不確実性は増大している。また、宇宙・サイバー・電磁波といった新たな領域の利用の急速な拡大は、陸・海・空という従来の物理的な領域における対応を重視してきたこれまでの国家の安全保障のあり方を根本から変えようとしている」と、環境の変化に着目している。

現在の安全保障環境の特徴について、次のように述べている。「国家間の紛争は、軍や法執行機関を用いて他国の主権を脅かすことや、ソーシャル・ネットワーク等を用いて他国の世論を操作することなど、多様な手段により、平素から恒常的に行われている。また、いわゆるグレーゾーンの事態は、国家間の競争の一環として長期にわたり継続する傾向にあり、明確な兆候のないまま、より重大な事態へと急速に発展していくリスクをはらんでいる。さらに、いわゆる「ハイブリッド戦」のような、軍事と非軍事の境界を意図的にあいまいにした現状変更の手法は、相手方に軍事面にとどまらない複雑な対応を強いている。」

脅威認識として、中国については「指揮系統の混乱等を可能とするサイバー領域や電磁領域における能力を急激に発展させるとともに、宇宙領域における能力強化も継続するなど、新たな領域における優勢の確保を重視している」と述べている。　　北朝鮮については「非対称的な軍事能力として、サイバー領域について、大規模な部隊を保持するとともに、軍事機密情報の窃取や他国の重要インフラへの攻撃能力の開発を行っているとみられる」としている。

我が国自身の防衛体制の強化としては、「あらゆる段階において我が国が持てる力を総合する防衛体制を構築する。特に、宇宙、サイバー、電磁波、海洋、科学技術といった分野における取組および強化を加速する」と述べている。また、運用コンセプトとして、「多次元統合防衛力」を掲げ、「宇宙・サイバー・電磁波といった新たな領域と陸・海・空の組み合わせによる相乗効果により全体としての能力を増幅させる領域横断（クロス・ドメイン）作戦」を提唱している。果たすべき役割としては、「平素から、宇宙・サイバー・電磁波の領域において、自衛隊の行動を妨げる行為を未然に防止するために常時継続的に監視し、関連する情報の収集・分析を行う」と平時からの監視能力（ＳＡ）の取得・向上を強調している。

３　サイバーとは

「新たな領域」として強調されている「サイバー」の言葉の意味を振り返ってみたい。「サイバー」はもともと英語の接頭語、あるいは形容詞的に用いられたもので、「コンピュータ・ネットワークに関する～」の意味をあらわす。例えば、サイバーセキュリティーやサイバーテロのようにその後に何が続くかで意味が変化する。１９８０年代中ごろから広く用いられるようになった新しい概念といえる。「サイバー攻撃」とは、コンピュータ・ネットワークを利用して不正侵入し、データを盗む、

もしくは改ざん/破壊する、といった行為であり、中でも大規模で影響が甚大で深刻なものや、政治的・社会的混乱を目的に行われるものは「サイバーテロ」と呼ばれる。

現代社会は、軍隊をはじめ、国家機関の活動を支えるシステムから、経済活動、個人の利用するパソコン、スマホまで、インターネットに支えられている。しかもこのネットワークは世界中につながっている。新防衛大綱の中で強調される新たな領域の「サイバー」で防衛省の役割、任務は、自衛隊のコンピュータ・ネットワークの活用を維持、発展させるために、外部からの侵入を阻止することにある。ただ、国家としての安全保障、防衛分野に関わる情報、データは防衛省のみにとどまることはなく、政府、国家機関から、地方自治体、警察消防等の地方組織あるいは民間の関連企業にまで、インターネット上で共有されている。このサイバー空間の運用状況をいかに掌握し、保全するかは国家としての大きな課題である。

４　近年話題になったサイバー戦

現代の戦いは、ハイブリッド戦争と言われ、正規戦、非正規戦、サイバー戦、情報戦などを組み合わせて戦われる。この概念は、中国では「超限戦」として発表され、社会を構成するすべての要素を兵器として戦う必要性が示されている。これまで語られてきた近代的な戦争モデルではない、平時でも有事でもない状態で進み、非軍事的手段の役割が増加してきている戦いでは、サイバーの果たす役割が大きくなってきている。

ハイブリッド戦争として話題になったのが、２０１４年のクリミア紛争で、ロシアはほぼ血を流すことなくクリミアを占領した。ロシアは空挺部隊と特殊作戦軍をクリミアに展開させたが、ウクライナの通信網を遮断するために物理的にケーブルを破損し、ウクライナ政府のサイトをダウンさせ、国会議員の携帯電話を使用不能にさせるほか、フェイクニュースを流し、ＳＮＳを用いて世論操作も行ったと言われている。目に見えないところで戦いの帰すうが決せられた。

２０１９年５月５日、イスラエルはガザ地区にあるイスラム組織ハマスのサイバー部隊の本拠地を空爆した。イスラエルの発表によると、ハマスのサイバー部隊がイスラエル市民に対してサイバー攻撃を行ったことから戦闘機での攻撃を実施したという。サイバー攻撃に対してハードパワーで阻止した一例である。

２００９年～１０年、イランの核開発を妨害するためにサイバー攻撃が行われ、実被害が発生した。いわゆる国家間のサイバー戦争といえる。イランの国家政策である核開発を妨害し遅延させる目的でコンピューター・ワームが使用され、イランの核燃料施設でウラン濃縮遠心分離機を破壊するという物理的な実害を引き起こした。この攻撃が何者によって実施されたか明らかではないが、イラン国内に被害が集中しており、核施設以外への被害も出ていることから、米国とイスラエルが共同した攻撃であると語られている。これまで比較的安全だと信じられていた、インターネットに接続していない独立した産業用制御システムもＵＳＢメモリーを介して感染、被害が発生すること

で衝撃を与えた。

２０１６年３月、アシュトン・カーター国防長官は、いわゆる「イスラム国（ＩＳ）」へのサイバー攻撃を行っていることを公に認めた。「サイバー戦はＩＳの戦闘員への指揮・統制能力を妨害し、通信の完全性への信頼にダメージを与え、物資補給の調整能力を奪うのが狙いだ」と述べ、サイバー攻撃の実施を政府が認めるようになった。

米国国家情報長官室の報告書と、特別検察官の調査報告書によると、ロシア政府による２０１６年大統領選挙への大規模かつ組織的な介入があった。第一の手法は、サイバー攻撃による政党・候補者に関する機密情報の窃取と暴露。第二の手法は、メディア上でのさまざまな影響工作・浸透工作。第三は、選挙関連インフラ等へのサイバー攻撃であったとしている。詳細は不明だが、世界のリーダーとなる米国大統領の選出に他国の意志が影響を及ぼす可能性があるということが示された。

５ 各国のサイバー部隊

２０１８年５月、米国はサイバー軍を統合軍へ昇格させた。サイバー軍が戦略軍から独立して１０番目の統合軍となった。地域別の統合軍とは異なる機能別の軍種として位置づけられ、サイバースペースを構成する各種のサイバーシステムは、四つ（宇宙軍が創設され、現在は五つ）の軍種、他の九つの統合軍を横断的につないでいる。サイバー軍の規模は６千～７千名程度の規模（防衛白書によると約６千８百人）と考えられ、他の統合軍と比較するとその規模は大きいものではない。

ただ、統合軍としての位置づけは、作戦を遂行する任務部隊の統合軍と対等の立場でサービスを提供し、協同して戦力発揮を行うことになり、その意義は大きい。サイバー軍が立ち上げられた当初、米軍は、自分たちがサイバー攻撃を外国に対して行っていることを認めていなかった。認めることは自軍に対する攻撃を正当化してしまうことになると考え、口をつぐんできたが、サイバー攻撃が今後の国際紛争において不可欠の要素になってきたことから、米国はサイバー攻撃の意図を隠さなくなったということは注目すべきである。司令官の交代式でシャナハン国防副長官は「千年以上もの間、軍は陸と海で支配を競ってきた。直近の百年間は、我々は空を支配してきた。今日、我々は新しい時代の夜明けに立っており、戦争が性質を変えるという現実に直面している。戦闘領域としてのサイバースペースと宇宙の登場であり、その重要性は陸、海、空に匹敵する」と述べた。

中国のサイバー部隊は、２０１５年末に設立された戦略支援部隊に含められていると考えられるが、その数は推定数万人から数十万人まで幅がありはっきりしない（防衛白書では約３万人）。２０１７年９月、中国政府機関「中国サイバースペース管理局」が発表した論文には「サイバーセキュリティと情報化における軍民統合を推進する」と書かれている。

２０１７年１２月には「サイバーセキュリティー・イノベーションセンター」が発足し、「軍が未来のサイバー戦争に勝利するのを助ける」ために民間の協力を推進する役割を担っている。人民解

放軍は通信大手のＺＴＥやファーウェイ・テクノロジーのような企業とパートナーシップを強化するとともに大学との連携も推し進めている。このような企業や大学は、中国の「サイバー民兵」の一角となっている。また、中国のサイバー民兵の中で「愛国ハッカー」と呼ばれる人たちの存在は、国家の敵にダメージを与えるうえでは有効な攻撃を行うこともあるが、当局のコントロールが利かない場合がある。このような国民のナショナリズムに突き動かされて行動する愛国ハッカーは千万人を超えるともいわれる。新防衛大綱では、中国は、「軍事力の質・量と共に、指揮系統の混乱等を可能とするサイバー領域や電磁領域における能力を急激に発展させている」と述べている。

ロシアは連邦安全局に「情報セキュリティセンター」、国防省には「ネットワークセキュリティ部隊」を有している。それぞれの担当任務は異なり、情報セキュリティセンターはサイバーテロ等に対抗する横断的な任務を有し、軍のセキュリティ部隊は連邦軍の保全を任務としているとみられるが、実態はよく分かっていない。ただ、ロシアからの活動と見られるサイバー攻撃は多数確認されており、防衛白書によると、サイバー部隊として約千人の人員を有しているとしている。２０１６年１２月、ウクライナで大規模な停電を発生させたサイバー攻撃はロシアの関与が指摘されており、２０１７年のランサムウエア（データを使えなくして身代金を要求）によるサイバー攻撃については、米英両政府はロシア軍によるものと発表した。軍や情報機関、治安機関などがこれらのサイバー攻撃に関与しているとされ、敵の指揮・統制システムへのマルウエア（破壊プログラム）の挿入等の攻撃活動も実施していると言われている。

北朝鮮サイバー軍は朝鮮人民偵察総局に所属しており、統括センターは参謀部所属とされるが、全容は分かっていない。人員規模は諸説あり、２０１４年時点での５千９百人規模から毎年千人ほどが増強されているといわれている（防衛白書では約３千８百人）。暗号解読、各国の機密情報、産業技術情報の入手、世論操作等幅広く活動している。サイバー部隊を利用しての資金獲得の活動が報告され、世論操作では韓国の国政選挙、大統領選挙への巧みな情報操作が行われたことが分かっている。
また、バックドア（ターゲットとなるコンピュータに侵入するための入り口）の取り付けやスマホにマルウエア（不具合を起こす意図で作られているソフトやプログラムの総称）を感染させる等、世界中にウィルスを溢れさせようとしていた事例が報じられている。２０１６年９月に発生した韓国軍内部ネットワークへのサイバー攻撃は、北朝鮮ハッカー組織によるものと韓国軍は結論付けた。また、２０１７年、世界１５０ヵ国以上の病院、学校、産業などのコンピュータが使えなくなるマルウエア攻撃が行われたが、米国は、北朝鮮によるものと結論付けた。新大綱では、北朝鮮について、「非対称的な軍事能力として、サイバー領域について、大規模な部隊を保持するとともに、軍事機密情報の窃取や他国の重要インフラへの攻撃能力の開発を行っているとみられる」と述べている。

６　米国のサイバー戦略

世界最強のサイバー大国と言われる米国のサイバー予算の規模はかなり大きく、２０２０年度の国防予算の伸びが約６・６%の中、１０%増の９５億ドル（約１兆円）を要求した。ほかに、宇宙を含めた各種研究費は１０４３億ドルと最大規模となった。中国やロシアの動きをにらんだ「将来の戦い」に備える姿勢を示したと言える。

米国防省は、２０１１年と２０１５年にサイバー戦略を策定してきたが、サイバー体制見直し（Cyber Posture Revie）を実施し、２０１８年９月連邦政府機関におけるサイバー対策の指針となる「国家サイバー戦略」を公表した。平時においては、第一に情報を収集し、危機あるいは紛争時に使用する軍事的サイバー能力を整える。サイバー空間におけるＩＳＲ活動と、ターゲッティング情報の収集を行う。第二に武力紛争以前の悪意あるサイバー活動を、その発信源で破壊または阻止するため前方で防衛する。第三に米国の軍事的優位を維持するため、ネットワークとシステムの安全、強靭性を向上させる。第四に他省庁、産業界、諸外国の当局と協力して共通の利益を追求する。有事においては、攻撃的なサイバー能力を駆使して、紛争の全スペクトラムでサイバー作戦を展開する。特に注目されるのが、基幹インフラや最先端産業などを脅かす攻撃には「すべての手段」を駆使して報復するとともに、「前方防衛（defend forward）では、紛争が発生していない状況下においても加害国のネットワークに侵入してサイバー作戦を行う」と明記したことである。

ロシアや中国、北朝鮮を名指しし、米国や同盟国に対するサイバー攻撃は「重大な犠牲を伴う結果となる」とけん制した。「米国が持つすべての手段を活用し、サイバー活動を抑止し、対応する」と明言し、外交的報復や経済制裁だけではなく、サイバー攻撃や軍事攻撃も含まれるとしている。当時のボルトン大統領補佐官は記者会見で「我々はサイバー攻撃をしたいのではなく、米国を攻撃すれば、耐えがたいほどの代償を支払うと敵対勢力に思い知らせ、攻撃を抑止することが狙いだ」と説明した。国防総省もサイバー戦略の中で悪意ある攻撃を防ぐためには「前方防衛」も辞さないと明記し、先制（サイバー）攻撃をためらわないとした。

７　日米間のサイバーをめぐる議論

２０１９年４月、ワシントンで２年ぶりに開かれた日米安全保障協議委員会（日米２プラス２）において、宇宙、サイバー、電磁波など軍事利用の進展著しい「新たな領域における協力」を打ち出した。

共同声明では次のように述べている。「サイバー空間に係る課題に関し、閣僚は、悪意のあるサイバー活動が、日米双方の安全及び繁栄にとって、一層の脅威となっていることを認識した。この脅威に対処するために、閣僚は、抑止および対処能力を含むサイバーに係る課題に関する協力を強化することにコミットしたが、優先事項として、おのおのの国が国家のネットワークおよび重要インフラ防護のための関連能力の向上に責任を負っていることを強調した。閣僚は、国際法がサイバー

空間に適用されるとともに、一定の場合には、サイバー攻撃が日米安保条約第５条の規定の適用上武力攻撃を構成し得ることを確認した。閣僚はまた、いかなる場合にサイバー攻撃が第５条の下での武力攻撃を構成するかは、他の脅威の場合と同様に、日米間の緊密な協議を通じて個別具体的に判断されることを確認した」。

日本へのサイバー攻撃が、米国の日本防衛義務を定めた日米安保条約第５条の適用対象だと初めて確認した。ただ、どのようなサイバー攻撃が日米の安全保障を脅かす武力攻撃を構成するか、どのような対応が日米で取られるのか、あるいは取り得るのかは今後の課題であり、抑止力を発揮するためにもその議論・調整が急がれる。サイバー防衛を含め同盟を強化するには、日本が積極的攻勢を含め、能力向上へ踏み出すことが求められている。

８　日本としてのサイバーセキュリティへの取り組み

本年２月、三菱電機がサイバー攻撃を受けて防衛関連情報が盗まれた可能性があると、報じられた。ハッカーはウィルス対策ソルトウエアの脆弱性をついて侵入した。数年前から継続していた疑いがあり、防衛関連情報に加えて個人情報と企業機密がハッカーに盗まれてしまった可能性が高い。

狙われているのは三菱電機だけではなく、ＮＥＣや神戸製鋼等の防衛関連情報が外部からのアクセスを受けている。三菱電機は「従来の監視や見地をすり抜ける高度かつ巧妙な手法であったため、攻撃を完全に防御できなかった」と述べているが、日本を代表する防衛関連企業で、サイバー分野には高い能力と意識を有しているはずの三菱電機がこのような事態を引き起こしたことは、他の産業分野への攻撃が認知されないままに拡散している恐れがある。

政府は２０１８年７月、「サイバーセキュリティ２０１８」を公表した。サイバーセキュリティ基本法に基づく２回目の「サイバーセキュリティに関する国家戦略であり、基本計画」である。サイバー空間と実空間の一体化に伴う脅威の深刻化と、２０２０年東京オリンピックを見据えた戦略の必要性が述べられている。本戦略の目的は「自由かつ安全なサイバー空間の堅持」である。脆弱性対策に係る体制の整備として「国民・社会を守るための取組や重要インフラ、政府機関、大学におけるセキュリティ対策の推進」、サイバー防御の観点からは、「積極的サイバー防御の構築、サイバー犯罪への対策、官民一体となった重要インフラの防護、大規模サイバー攻撃事態等への体制強化」が述べられている。

しかし、基本的な姿勢は、自由かつ開かれたサイバー空間の利用を促進することにある。推進体制として、内閣総理大臣の下に官房長官を本部長、関係大臣を本部員とするするサイバーセキュリティ戦略本部が設けられる。事務局の内閣サイバーセキュリティセンター（ＮＩＳＣ）は、戦略本部に閣僚が参加する、閣僚本部員５省庁（警察庁、総務省、外務省、経済産業省、防衛省）や重要インフラ所管省庁（金融庁、総務省、厚生労働省、経済産業省、国土交通省）、その他関係省庁（文部科学省等）の協力を得て総合調整および連携促進の要として主導的役割を果たす。このＮＩＳＣは、

必要な予算の確保と執行に当たるが、政策実行は、各省庁に任せられる構図になっていて、サイバー戦を戦う組織とはなっていない。

大規模サイバー攻撃事態等への対処においてもその精神は、「自由、公正かつ安全なサイバー空間の理念の発進・サイバー空間における法の支配の推進」であり、コンピュータネットワーク上で行われるサイバー犯罪へ安全確保は政府機関、各事業者等が実施することとされている。我が国の防衛力・抑止力・状況把握力の強化の中で、防衛省の果たす役割として、「対処機関としてのサイバー攻撃対処能力向上のため、最新技術を活用して、サイバー防護分析装置、サイバー情報収集装置、各自衛隊の防護システムの機能の拡充を図る」と具体的な方向性が見えるが、「防衛情報通信基盤（ＤＩＩ）のクローズ系およびネットワーク監視器材へ常続監視等を強化するための最新技術を適用していく」と続いていることから、防衛省のサイバーセキュリティの責任範囲はあくまでも他省庁と同じく、防衛省内のシステムに対する監視と防御態勢の確保と見ることができる。

サイバー攻撃に対する抑止力の向上として、「自衛隊が保有する情報通信ネットワーク等に対する侵入試験（ペネトレーションテスト）の実施や、サイバー攻撃対処部隊の対処能力の練度を向上させるため、指揮システムを模擬し、実戦的な演習環境を整備する」を挙げている。その際、「悪意ある主体によるサイバー空間の利用を妨げる能力の保有の可能性についても視野に入れる」とされていて、初めて対処能力の保持を匂わせる内容となっている。ただし、その責任範囲は自衛隊のシステムに限られているようで、国家としての組織的なサイバー戦について、本戦略の中では全く触れられていない。国際的なサイバー犯罪や攻撃が頻発している現状における国家戦略、基本計画としては、踏み込んだ対応策が示されていない。

９　中期防衛力整備計画と年度予算におけるサイバー

中期防では、サイバー領域の能力として、「サイバー攻撃に対して常時十分な安全を確保し、我が国への攻撃に際して相手方によるサイバー空間の利用をさまたげる能力を保持し得るよう、サイバー防衛隊の体制を拡充するとともに、自衛隊の指揮通信システムやネットワークの抗たん性の向上、実践的な訓練環境の整備等、所用の態勢整備を行う」とし、「優秀な人材の育成と部外の優れた知見を活用し、自衛隊のサイバー防衛能力を強化する」と述べている。また、「政府全体として統合的な対処を行い得るよう、関係府省庁との密接な連携を強化するとともに、訓練・演習の充実を図る」と国家サイバー戦略を受けた内容となっている。ただ、我が国に対するサイバー攻撃に対し、積極的攻勢を取り得る能力の保持を目指しつつも、現実的には防衛省保有の各種システムの防護能力の強化に留まっている。

中期防を受けた２０２０年度予算におけるサイバー関連経費は２５６億円、サイバー防衛隊の体制拡充（約２２０名から約２９０名に増強）、陸自サイバー防衛隊（仮称の新編）、サイバー情報収集装置の整備（34 億円）、サイバー攻撃対処に係るＡＩ運用システムの設計（０・３億円）、サイバー

コンテストの開催（４００万円)、防衛情報通信基盤（ＤＩＩ）の整備（クローズ系）(76 億円）等となっている。

サイバー領域は日本の安全保障上喫緊の課題であり、自衛隊にとって不可欠の能力であることは防衛計画の諸所で述べられている。ただし、現実の中期防、予算の状況を概観すると、重要性は認識されているものの、実際の人員規模、予算内容は非常に限られたものであり、自衛隊の現状は能力整備の緒に就いたばかりと言える。国家としてのサイバーセキュリティ能力を向上するには、前項のサイバーセキュリティ戦略で国家としての対処の方向性を明示するとともに、自衛隊としては、任務と役割を明確にし、組織的な対応能力を整備していくことが不可欠である。道は遠い。

１０　身近な問題としてのサイバーセキュリティ

新型コロナウイルスの感染拡大により、今後の世界は大きく変わっていく可能性がある。以前の日常が戻ることを期待したいが、感染拡大再発の恐れが残った社会では、新たな社会活動様式が求められ、経済活動、その他の全ての面で影響を受けてくる。

国際政治から科学・文化等、多くの会議がインターネット上のバーチャル（仮想空間）で実施されている。企業活動は、在宅勤務、テレワークが推奨され、休校となった学校では、ＩＴ機材が導入され、オンライン教育、リモート学習が進むこととなった。各家庭においては、インターネットショッピング（ネット通販）の利用が大きく伸び、買い物の支払いは、現金からクレジットカードや、スマホ決済が普及することになった。これまでの世界の基軸通貨の後ろには、法定通貨としての国家が存在するが、電子データのみでやり取りされるビットコインのような仮装通貨がインターネット上で取引されている。世の中が、インターネットを前提にした社会に大きく変わりつつあり、その安定的・安全な運用が担保される事が不可欠である。

新型コロナウイルス感染が世界で急拡大した２～４月にかけて、金融機関を狙ったサイバー攻撃が２３５%急増したという報道があった。テレワークの広がりに照準を合わせるように、不正サイトに誘導するサイバー攻撃の被害が、４月末には国内で６千５百件を超えたと伝えられ、世界で４万７千件を超える被害が報告される中、日本の被害件数は米国に次ぐ多さになる。セキュリティが十分整わないままテレワークの導入に踏み切った場合、サイバー犯罪者の標的となる危険にさらされる。誤って不正サイトにアクセスしてしまうと、情報を盗み取るコンピュータウイルスに感染するなどの被害が生じる。

話題になっているビデオ会議サービス「Zoom」は、外出規制や在宅勤務が広がる中、２０１９年１２月に１千万人だった世界の利用者が２０２０年４月には３０倍の３億人に増えた。フェイスブックはビデオ会議システム「メッセンジャールーム」の提供を、グーグルはビデオ会議システム「Meet」の無償提供を開始した。ただ、急拡大で悪意のあるハッカーの妨害なども多数発生している。不正侵入や情報流出などのサイバー被害が報告されているが、セキュリティ設定が正しく使用されてい

ないことによる場合が多い。不正プログラムに対する注意と、パスワードの適切な設定と管理・使用がセキュリティ対策の基本である。

今年３月頃からランサムウエア攻撃が急増している。ランサムウエアとは、感染したＰＣをロックしたり、ファイルを暗号化したりすることによって使用不能にしたのち、元に戻すことと引き換えに「身代金」を要求する不正プログラムを言う。脆弱なパスワードを設定しているリモートデスクトップが多く狙われている。これらの攻撃に対する対策と予防は基本的なセキュリティ対策である。

１１　まとめとしての身近なサイバー対策

コンピュータシステムの普及と、我が国においてはスマートフォンの各個人への浸透により、本人の自覚の有無にかかわらず、インターネット環境は常に身近で必須の物になってきており、今後その果たす役割は大きく広がり、依存度も深くなっていく。メールやＳＮＳでの会話、情報発信、情報検索から、ＷＥＢブラウズというネットサーフィン、ショッピング、そしてゲーム等、スマートフォンや携帯電話を日常的に使用しているが、そのすべてがインターネットを利用しており、サイバー攻撃を受ける可能性が存在する。しかし、そのことはほとんど意識されていない。インターネットショッピングや、テレホンバンキング、その他の決済を伴うサイトでの巧みな誘導や、偽装サイトで個人情報が盗まれ、実際に多額の被害にあう事例の報告が後を絶たない。我々各個人も、サイバー攻撃の真っただ中にあると言う現実を認識する必要がある。

サイバー攻撃に対する対処（防衛）方法は、国家レベルの組織的な攻撃への対処も個人レベルの対処方法も基本的には変わらない。今回、新防衛大綱で強調されているサイバーへの取り組みについて現状と世界の取り組みについて書き始めたが、目に見えない世界での戦い・活動であり、実態については開示されない内容が多いことから、表に出てきたサイバー攻撃の実態の一部と、公表された国家戦略という対処要領の紹介に終わらざるを得なかった。

この報告書に最後までお付き合いいただいた方へ、自らの身を守り、被害にあわないために、我々ができるサイバー攻撃対処法を紹介して報告書を終えることにしたい。

考えられる対策は、全てのサイバー攻撃に共通である。

① こまめにバックアップする。重要なファイルのコピーは常に予備を保管しておく。

② ＯＳやソフトの脆弱性を修正する。更新プログラムが提供されたら速やかに適用し、脆弱性を修正する。

③ 信頼できるセキュリティ対策プログラムを最新の状態で活用してランサムウエア等の攻撃を検出する。新たな脅威に対抗するため、セキュリティソフトは最新の状態にしておく。

④ 不正サイトへのアクセスをブロックすることにより、ランサムウエアや他の不正プログラムの侵入、認証情報の送信などを防ぐ。

⑤ 電子メールや添付ファイルを安易に開かない。一見それらしく装ったものが送られてくることを常に警戒し、少しでも不審に思った場合は、内容の事実確認を実施する。

⑥ 信頼度の高いパスワードを使用し、パスワードは使いまわしをしない。