サイバー・情報安全保障の時代

則房雅也、齋藤孝道
CYDEF 実行委員会、および明治大学サイバーセキュリティ研究所

エグゼクティブサマリー

COVID19、ウクライナ事案、社会の変化、経済不安など、世界の隅々にまで広げたサイバー空間と、そこを行きかう情報資産、これらを悪用し国や社会や経済を混乱させる活動の拡大が、複雑に絡み合って情勢を決めつつあるいま、世界は「サイバー・情報安全保障の時代」に向かうコーナーを曲がったと言える。これまでになく多くのことが互いに影響しあうので先を読みにくい。現状に至った流れを原点から振り返り、変化の本質を理解して今後を読みとく精度を上げたい。本ペーパーは、サイバー空間で起こってきた事実を俯瞰し、新しい時代に向かって何をすべきかを考えるきっかけを提供する。

誰もが利用する情報や端末環境が大きく変わると、社会を支える情報システムに革命が起こる。インターネットの出現でサイバー空間が生まれ、パソコンの普及で万人がサイバー空間を使う IT 革命が始まった。今の時代が始まった原点である。その後のブロードバンド通信、スマートフォン普及はサイバー空間を膨張させ IT 革命を加速させた。万人の参加は新しいビジネス機会を生み、新しい市場や経済が活性化する。保守的な社会システムも IT 革命に巻き込まれた。今日に至っては、世界中の人々と社会・情報システムがサイバー空間につながっている。しかしその一方で、全貌の把握が不可能な、さまざまな脆弱性がサイバー空間のあちこちに産み落とされてきた。この先向かう時代への種がまかれ、サイバー空間に闇の空間が広がり続けている。

脆弱性はいつか必ず社会に問題を起こす。技術やシステムで対処できる問題は、その都度取り除いてきたが、人に入り込む脆弱性に向き合うことはなかった。人が使う端末、端末がつながるオフィスとイントラネットの問題を解決すれば、人が引き起こす問題も解決すると解釈した。この考え方が限界に達したのが、ランサムウェアなど標的型攻撃の成功である。無防備な個人に対して攻撃は始まり、内部で攻撃者の手助けをさせると、本来の目的に向けて攻撃が本格化する。2011 年、同時多発的に日米防衛企業内部に侵入した大規模なサイバー攻撃を経験した。それにも拘わらず、その後どこの組織でも防御力にさほど進展が見られない。闇の空間から現れる攻撃者は組織化されいっそうやり口を高度化している。

2016 年なるとサイバー空間の不穏なうごめきが表舞台に出てきた。人の脆弱性をついて大勢の人々を動かす工作活動である。フェイクニュース、プロパガンダなど、一般の人たちの行動が選挙結果を左右し、暴動が誘発され、正しい言論が遮られ始めた。場所によらず効果は著しい。特にウクライナ、ロシア周辺で起こっている工作活動の結果には理解しがたいものがある。国が揺らぎ、経済が揺らぎ、数限りない国民が犠牲になる。効果的な打ち手が

無く、被害者側の対応は時機を逸して後手に回る。これがこの先 10 年続く新しい複雑なサイバー空間の特徴である。現状、防御を選択するしかない日本の防御力はあまりに不十分だが、多くの関係者が具体的な対策に取り組み始めなければ 10 年が 20 年と続くことになる。

どこでも誰でも使える対策には技術、システム、組織力が必要だが、まず今は広く先導者、関係者が現状理解と課題認識を共有する必要がある。攻撃者に劣らないサイバー空間への知見、情報システムへの知見、経済・社会システムへの知見、安全保障への知見、他にも必要な知見はあるが、いずれかだけを取り上げても新しく複雑な問題を解決する糸口は見えてこない。誰も経験したことのない時代、であれば当然のことだろう。「サイバー・情報安全保障の時代」というのは、何十年も個別単独に扱ってきたテーマを、組織化された攻撃者は一連の攻撃シナリオにまとめてくるのだから、防御する側はそれ以上に効果的に防御シナリオとして統合して準備しておく必要がある、この実現に妥協はないことを最初に強く主張しておく。簡単な話ではないが、闇の空間が広がる次の時代を生き残るために逃げ場はないのである。

サイバー、情報、安全保障に至る歴史的な流れ

1990 年誰でもインターネットが使える時代が始まってサイバー空間が出現するとセキュリティ要件が劇的に変化した。コンピュータに格納されたあらゆる情報資産がサイバー空間上で見えるため、ファイアウォールのような内部侵入を防ぐ対策が不可欠となった[1,2]。2011 年日米の主要な防衛産業が同時にサイバー攻撃を受けた。この時初めて日本社会がサイバー攻撃に国境がないことを実体験した。日本でようやく「サイバー攻撃」が一般用語として使われだした。強い動機を持った攻撃者の侵入を防ぐことはできないと実証され、侵入されることを前提にした対策が必要となった。2022 年ウクライナ事案に絡んで再びサイバー空間の常識（良識）が変わろうとしている。

振り返ると、ほぼ 15 年単位でサイバー空間に求められるセキュリティ要件が劇的に変わっている。特別な力が働いたという実感はなく、社会情勢、ビジネス、技術、人心の変化が時間をかけて生んだ結果と見ることができる。つまり、この先も周期的に変化は起こる。わずかな予兆を早く感じ取って劇的な変化に備えることがいっそう重要となる。実は 90 年代半ば、複数の大手通信企業がサイバー攻撃を受け、FBI が大追跡の末に犯人を捕まえた。用意周到な攻撃は防げないことをこの事案が示したが、犯人が捕まったためか、もっと確実な防御手法の開発に真摯に向き合う人は少なかった。2011 年のサイバー攻撃が成功したのも不思議ではないが、犯人は逮捕されていない。攻撃は対象を変えて続き、拡大、巧妙化してきたと考えられる。インターネット時代の 10 年の進化は想像を超えるものがある。近年国家が絡んだサイバー空間上の活動は、大規模にもかかわらずはるかに実態をつかみにくい。攻撃者が近づいて来てもわからないし、犯行の足跡も残さない。追っても途中で消える。多くの人は、活動に巻き込まれたことに

気づかないし、自分に降りかかることはないと信じ込んでいる。

防御手法を振り返ってみると、データを守る暗号技術、パソコンを守るアンチウィルス、イントラネットを守るファイアウォール、それらの補完技術には一定の効果があり、内部情報資産を守るためにこれからも使われ続けるだろう[3]。一方で人を守る技術や仕組みの効果は弱まり続けている。認証技術、アクセス管理は強化されてきたが、攻撃された人が攻撃者に手を貸すとは想定していない。長く目を背けてきた課題である。90 年代半ばの事案は、企業内の人を味方に変えてから侵入が始まった。20 数年を経たいま、はるかに巧妙に人を騙すさまざまな手法が編み出されている。

単独で機能し効果が限定される対策が、サイバー空間の構成要素をそれぞれ守ることに使われている。そんなサイバー空間に無防備な人が世界中でつながっている。情報資産に限らず、社会情勢もビジネスも無防備な人々の手にある。攻撃者の目が人に向くのは自然な成り行きである。この先起こることへの予兆でもある。

サイバー空間の常識を覆したウクライナ情勢

ウクライナの事案では、サイバー空間の強靭性を示した一方で、これまでにない「サイバー攻撃」が目立つ。人目につかないようにシステムへの攻撃という従来型のサイバー攻撃が行われる一方で、プロパガンダ、フェイクニュースなど、世界中の人々にあからさまに見せつける、大勢の人々への影響力工作活動が行われている。2011 年ではサイバー攻撃の範疇に入っていなかったが、2016 年以降米国大統領選挙への不正介入事案で明るみになったように、サイバー攻撃のメインストリームとなってきている。サイバー空間を使うと連続的、再帰的なシナリオが作りやすい。人手もコストもかからない。嘘でもそれがたくさんの人の話題になると信じる人が増え、影響力工作は成功に向かう。社会を揺るがすことも起こりうる。嘘を見抜く技術やシステムは未熟で、このような脅威への教育は十分に行われておらず、影響の広がりを取り締まる機関は国内では未だない。今のところ、使われれば確実にある程度成功する、としか言いようがない。

インターネットを創生した人々は利用者に「ethics（倫理）」を布教し実践することを求めた。有益な情報、技術開発と起業機会、良心に満ちた空間が広がった。それが今や嘘と危険に満ちている。ウクライナ事案はサイバー空間にこの性格を決定づけたと言ってよい。

日本を見直す立ち位置

いま、日本のサイバー、情報、安全保障への取り組み方は、大きな転換期に直面している。たとえば、2021 年 9 月に公開されたサイバーセキュリティ戦略（閣議決定）（以降、「サイバーセキュリティ戦略 2021」と呼ぶ）がその片鱗を見せている[4]。サイバーセキュリティ戦略 2021 では、不可避なリスク要因として「サイバーセキュリティ戦略」における安全保障がより強調している。最も象徴的な点は、日本の経済、社会活動をサ

イバー空間で脅かす、中国、ロシア、北朝鮮がはっきりと示されていることである。また、「安全保障」という用語は 66 回も登場しており、サイバーセキュリティが日本全体の安全保障問題であることを国内外に明言した。

また、北朝鮮のサイバー攻撃グループが搾取獲得した暗号資産総額は、これまで 20 億ドル（約 2,700 億円）以上と見積られている。元を正せば人々の生活資金が、日本を攻撃対象に含めた核兵器開発に充てられている。個々人の意識、サイバーセキュリティ対応力の欠如が、巡り巡ると国民の生命・財産などに甚大な脅威となっている現実が浮き彫りにされた。

この先サイバーセキュリティで生じる問題も解決の要件も変わってゆく。技術だけで解決は難しい。社会問題としての取り組みも求められる。多くの人が知らずに巻き込まれてしまう。データや装置、システムを課題の中心に置く話でもない。「サイバー・情報安全保障」というとらえ方は、関係する事柄を統合的、総合的に捉えて、緊急を要する課題を見極めるために不可欠である。発生事象に個別対応して終わりがちな日本の欠点を補うことができる。

「サイバー・情報安全保障」の本質

サイバー空間の価値は、高速道路網の充実、航空路線網の充実に類似するものがある。世界の隅々にまで、その先の個人にまでメリットを与え社会や生活を激変させる。史上最高の情報通信インフラを提供する。情報の価値と役割は言うまでもないが、デジタル化される情報の範囲に限りはなく、社会活動の情報依存度も限りなく深い。問題は個々に発生するが、解決には総合的な取り組みが必要である。発生する問題は、不注意から故意に、故意から組織犯罪へと広がり、国家の活動へと移り安全保障議論が必然となった。現状、この圧着され一体化した 3 領域全体を見渡して語る人は少ない。

サイバー空間は透過的で誰でも世界中の情報にアクセスできる。一方で良くも悪くも匿名性が高く、攻撃行為であっても誰かを特定するのは困難である。この特徴から攻守の非対称性が顕著になり、攻撃者は少ないコストで大きなリターンを得続けることが可能となる。事前に攻撃を知りえない守り手は致命的に不利な立場に置かれる。

このままではほぼ負ける状況を改善するために、攻撃者を特定するアトリビューション技術に期待が集まっている[5,6]。攻撃の予兆をつかむことに使え、攻撃者を絞り込むことに使える。ただ、アトリビューション技術は、一般に知られている情報技術論に閉じておらず、極めて限られたところで行われてきた諜報に関わるテーマであり、日本では体制面で課題が残る。

また、実装技術として、サイバー空間で発生し残された膨大な OSINT（Open Source Intelligence）などのデータを、高速かつ正確に処理する AI 技術の積極活用、習熟化が必要である[5,6]。精度の高い予知や特定に習熟化は不可欠で、習熟するためには現場の存在が不可欠となる。

サイバー空間上の情報を収集し、安全保障視点で分析し、問題が発生する前に次の手を打つ、これが被害を最小限にとどめるシナリオである。最大効果を得るためには、日頃から修練を積む現場の確保だけでなく、サイバーセキュリティ、情報処理、AI、安全保障、これらを扱える人材の育成、集約も欠かせない。

「サイバー・情報安全保障」の確保、維持には、一過性ではない、我が国の人材と技術力の質的量的な向上、人材と技術力の向上を評価できる国内外を問わない現場の確保、にその本質があるといえる。

サイバー空間上の安全保障には国境も組織や技術間の境界線もない。近年「ハイブリッド戦」という言葉が使われることがあるが、日本ではこの言葉の意味の深掘りが十分ではない。ハイブリッド戦は、冷戦終結後、ロシアが軍事大国アメリカへの対抗措置として採用した軍事的国家戦略であり、軍事に限定せず経済などの領域を横断する戦いであり、有事と平時を区別しないことなどを特徴とする[7]。サイバー攻撃を犯罪と見做すか、軍事行為と見做すか、法的にどう解釈するかなど、日本ではまず規範を探そうとする。その結果で対処する組織を動員する。しかし、攻撃者はそんな区別をしない、むしろ、境界にありがちな脆弱性をついて横断的に攻めてくる。国家レベルのサイバー攻撃になれば、行政組織や社会システムの脆弱性は研究しつくされており、意図的に弱いところを責めてくるはずである。日本の関係者がこの認識を共有することは出発点だと言える。

また、北朝鮮のサイバー攻撃グループは、今や数千人と見積もられている。湾岸戦争を見てきたる情報戦の重要性に気づき、すぐにサイバー人材の育成を始めた。最高峰大学で特別教育を受け実戦配備された筋金入りのエリートである。エリートが現場で獲得し続けたノウハウ、手足として確保した攻撃者を考えると、その攻撃力は計り知れない。我が国でも、「サイバーセキュリティ人材不足」「AI 人材不足」、「デジタル人材不足」という言葉が定期的に踊りだすが、具体的に取り組み成果が出ないうちに消えてしまう。果たして、人材不足は誰の課題なのか、日々変化する脅威に誰が向かい合うのか。「科学技術力は国力と比例する」と言われるが、これまでに獲得した我が国のアセットをこの先も長く維持し続けることができるのか。このような問いが社会全体に不足しているのではないだろうか。

取り組むべき課題

我が国で「サイバー・情報安全保障」を推進する上で、最初に取り組むべき課題は、状況認識レベルを高め、関係者間で状況認識を共有することである。我が国のステークホルダー間の認識は、未だ揃っていない。たとえば、サイバーセキュリティは、国際的な場では、情報技術に加え国際政治学や安全保障論の課題としても認識されている[7]。しかし、我が国では、ある人にとってサイバーセキュリティは技術論であり、別の人にとってはビジネス機会でしかない。いずれも間違いではないが、国家間での戦いの道具

としてサイバーセキュリティを悪用するアクターがいることを忘れてはならない。技術論もビジネス機会も意味がない状況に国が追い込まれることが起こりうるのである。

次に求めたいことは、「サイバー・情報安全保障」と範囲を広げたキャパシティービルディングである。個々の力、組織化力、己の位置を測る力、作戦運用術、そして、目標到達への PDCA（Plan-Do-Check-Act）が含まれる。日本の組織では、個別対応、一芸追求、走って考えろとよく下達されるので、グランドデザイン（全体設計）思考が育ちにくい。その結果、戦略思考が欠落し、目的と手段がよくすり替わる。可視化が難しいサイバー空間の問題に直面すると、この傾向はより顕著になる。サイバー攻撃は技術論を超え、サイバー空間の特質を駆使した認知領域の戦いを、実に戦略的に挑んできている。AI などの技術を用いて人の認知を直接誘導している。これらの脅威に対抗できるサイバーセキュリティ人材の要件と育成プランを見直すことが求められる。また、組織的攻撃が洗練されるなら、それ以上に洗練した組織的防御への準備が急務となる。誰が被害者かを考えれば、産官学横断的な協力での防御態勢となる。

さらに、サイバー戦や情報戦は机上の話ではないことを、ウクライナの惨事が見せつけた。実戦は 24/7 止むことがなく、想像をはるかに超えた被害が広がっている。我が国で何をすべきか議論するなら、サイバー戦、情報戦の作戦運用術を研究し、実践的な防御能力を高めることである。マネージメント（直訳の「管理」よりずっと広い）力の欠如は、我が国の隅々にまで蔓延する弱点である。「マネージメント力」はリーダーシップ、危機対応力、問題解決力、目標達成力を含む。グランドデザイン思考、戦略思考は最初に必要な素養である。これらに長け全体を統率する指揮官人材が各所に求められている。この育成も必要である。

他にも課題は多い[3]が、上記の解決は大きな成果につながるものであり、優先的に取り組むべきことである。

まとめ

COVID19、ウクライナ事案は世界中の人々の社会行動パターンとこれまでの常識を変えた。サイバー空間の使い方に大きな影響を与えた。新しい時代に向かう流れが定着するだけの十分な時間が経過した。これから何が起こるか、冷静に読み取り我が国の隅々にまで備えを広げなければならない。「失われた 20 年[9]、30 年」に見るように、近年時代の流れに乗り遅れて衰退することが多い。思い起こせば、インターネット時代にも最初数年は乗り遅れた。この時代から後発に利はなくなり、遅れは簡単に取り戻せないことが実証されている。

サイバー、情報、IT といった個々のテーマで世界の先頭を行く企業や国は揺るぎがたい。日本が遅れていなくとも、先頭集団の前方にいるわけではない。国内で安全保障の視点から既存のテーマを見直す動きが出ている。成熟度の高いテーマの扱い方の話なので、方針さえ決まれば素早く扱えるだろう。他の国や攻撃者にも同じことが言える。

「サイバー・情報安全保障」という見方に気付いたところはまだ少ない。先行の利を得る位置にいるが、1 年の猶予があるとはとても思えない。攻撃側もこちらの動きをよく見ている。過去出遅れを繰り返した轍を踏まず、各界に分散する英知を集結し、素早く方針を固めて継続性のある取り組みを始める時だと言える。

謝辞

本ホワイトペーパーをまとめるにあたって、CYDEF 実行委員会で交わしている様々な議論が重要な論点になっています。日頃の有益な意見、および本ペーパーへ助言を頂いた CYDEF 実行委員会メンバー方々に深く謝意を表します。

参考文献

1. 「ネットワークセキュリティ技術－インターネットファイアウォールの現状と展望－」、則房雅也、盧偉、電子情報通信学会誌平成 8 年 2 月号、pp115-122、1996 年
2. 「従来のセキュリティ対策の限界を破る「協調型セキュリティ」」、則房雅也、後藤淳、他、NEC 技報 Vol.60 No.1、pp11-15、2007 年
3. 「National Cyber Defense - Consideration of Possible Collaboration between Defense and Industry based on Specific Conditions of Japan」、Masaya Norifusa and Jun Goto、Proceedings of International Cyber Defense Conference CYDEF2019/2020（2022 年 11 月刊行予定）
4. 「2021 年 09 月 28 日サイバーセキュリティ戦略（閣議決定)」、内閣サイバーセキュリティセンター、https://www.nisc.go.jp/policy/materials/index.html
5. 「Issues in Applying Artificial Intelligence to Cyber Defense」、Takamichi Saito、Proceedings of International Cyber Defense Conference CYDEF2019/2020（2022 年 11 月刊行予定）
6. 「沈黙は金？」（2019 年)、齋藤孝道、https://link.medium.com/qEQRvTGVasb
7. 「近未来戦の核心サイバー戦－情報大国ロシアの全貌」、扶桑社、佐々木孝博、2021 年
8. 「マスタリング TCP/IP 情報セキュリティ編（第 2 版)」、オーム社、齋藤孝道、2022 年
9. 「失われた 20 年～資本市場停滞の要因」、大和総研、2012 年 11 月 7 日、https://www.dir.co.jp/report/research/capital-mkt/securities/12110701capital-mkt.pdf

ホワイトペーパー利用にあたっての制限