特集3　サイバー空間の広がりに伴う脅威の拡散

1　公共空間としての重要性を増すサイバー空間

宇宙・海洋分野で拡大するサイバー空間

機密情報の窃取、金銭の獲得、業務の妨害などを狙ったサイバー攻撃は、国内外で常態化するとともに、その手口も巧妙化している。また、国家が政治的、軍事的目的を達成するため、サイバー諜報や重要インフラの破壊といったサイバー戦能力を強化しているとされており、安全保障の観点でも、サイバー攻撃の脅威は深刻化している。

加えて、昨今のデジタル化の加速で、「公共空間」としてのサイバー空間の位置付けは重要性を増しており、人工衛星の稼働数の増加やその活用の拡大、ナビゲーションシステムやエンジン制御システム等の導入といった海事産業のIT化の進展も相まって、宇宙・海洋分野にもサイバー空間は拡大を続けている。そのため、サイバー攻撃が社会に及ぼす影響もあらゆる場面に拡大していると言える。

宇宙関連のサイバー攻撃については増加傾向にあるとされているところ、ロシアによるウクライナ侵略の1時間前、米国情報通信企業「Viasat」が運用する衛星通信網のネットワークがサイバー攻撃を受け、ウクライナで数千件、欧州全体で数万件の顧客に対する通信サービスが停止し、ドイツでは、数千基の風力タービンの遠隔監視ができなくなった（2月）。ウクライナの軍及び警察も同社の衛星を使用していたとされるところ、米国や英国は、同攻撃はロシアが関与したものであると発表し、ウクライナ軍の指揮管制の混乱が目的と指摘した（5月）。

海事関連のサイバー攻撃も増加している。セキュリティ企業の報告によると、海事産業の運用技術システムに対するサイバー攻撃は、平成29年（2017年）から令和2年（2020年）にかけて約10倍に増加したとされる。平成31年（2019年）2月には、米国・ニューヨークなどの港に向かって航行中の船舶のコンピュータシステムがマルウェアに感染し、その機能が大幅に低下する事案が発生した。同事案を受けて、米国沿岸警備隊が海事業界に対してセキュリティ対策の強化を勧告した（令和元年〈2019年〉7月）。令和4年（2022年）も、ドイツ、ベルギー及びオランダの港湾施設が相次いでサイバー攻撃を受け、石油ターミナルの業務などに支障が出たとの報道がある（1月）ほか、インドの港湾でも、ランサムウェアとみられるサイバー攻撃によって一部ターミナルの管理システムが停止する事案が発生した（2月）。

サイバー空間を通じた偽情報の拡散が継続

宇宙・海洋分野におけるサイバー空間の拡大も含めて、サイバー空間の現実社会への拡大・浸透がより一層進む中にあって、悪意ある主体の活動は、社会・経済の持続的な発展や国民生活の安全・安心に対する深刻な脅威となっている。サイバー空間における悪意ある主体の活動には、サイバー攻撃だけでなく、「偽情報（ディスインフォメーション）」の拡

散も含まれる。偽情報については、社会不安を利用し、人々の認知、意思決定、行動などに影響を及ぼし、更なる混乱をじゃっ起する可能性があるほか、これが選挙に際してオンラインで流布されることについて、民主主義の基盤を脅かすとして欧米を中心に警戒が強まっていたところ（P.22「COLUMN：民主主義の基盤を脅かす懸念のある偽情報」）、令和4年（2022年）は、国際的な事象に関連して流布された偽情報にも注目が集まった。

例えば、ロシアによるウクライナ侵略に際して、ロシア外務省報道官が「ウクライナがロシアとの国境付近で生物化学兵器の開発を行っていた証拠を得た」との主張を展開したが、米国大統領報道官はこれを否定した（3月）。また、「ウクライナ人武装勢力の拠点を襲撃した際、米国パスポートを持つ外国人傭兵の遺体が発見された」（4月17日付けロシア紙「コムソモリスカヤ・プラウダ」）との報道もなされたが、ワシントンポスト紙は、同パスポートの所持者にインタビューを行い、ロシア紙の報道が誤りであると報じた（4月）。

また、米国のペロシ下院議長の台湾訪問（8月2～3日）に際して、中国国営メディアCCTVの記者が「中国軍機が台湾海峡を横断」などとブログに投稿し、同メディア等で拡散されたが、台湾の国防部は同報道を否定する発表を行った（8月）。加えて、台湾の国防部は、「台湾の桃園国際空港が中国人民解放軍によるミサイル攻撃を受けた」、「中国軍機が台湾軍機を撃墜した」といったSNS投稿は偽情報であるとして、台湾の市民に注意を呼び掛けた（8月）（P.49「COLUMN：台湾の偽情報（ディスインフォメーション）対策」）。

台湾国防部が「中国軍機が台湾海峡を横断」という投稿を「偽情報」と発表（台湾国防部ウェブサイト〈https://air.mnd.gov.tw〉）

我が国でも、同時期にTwitterで「ペロシ議長搭乗の航空機撃墜」との投稿（8月）が確認されたが、同投稿は、「Yahoo!Japan」のニュースサイトを装ったアカウントによるもので、公式アカウントにそのような投稿はなく、同ニュースサイトは、偽アカウントが発する情報への注意を呼び掛けた（8月）。

COLUMN 民主主義の基盤を脅かす懸念のある偽情報

米国では、平成28年（2016年）の大統領選挙に際して、ロシアが米国の有権者に向けて偽情報を拡散するなどして選挙に干渉した疑惑が浮上し、調査が行われた。平成31年（2019年）3月にムラー特別検察官は報告書を公表し、ロシアがSNS上でキャンペーンを展開し、大統領選挙に偽情報の拡散などで干渉したことを明らかにした。また、令和2年（2020年）の大統領選挙に際しても、米国当局は、選挙結果に影響を及ぼすものではなかったものの、偽情報の拡散などでロシアを始めとする外国勢力の干渉が行われたなどと結論付けた。さらに、米国国家情報長官室が公表した報告書「2020年米連邦選挙に対する外国の脅威」では、ロシア大統領が、バイデン候補（当時）及び民主党を中傷する一方でトランプ前大統領を支援するなどして、選挙プロセスに対する米国民の信頼を傷つけ、米国内の社会的・政治的分断を悪化させることを目的としたインフルエンス・オペレーションを裁

可し、ロシア政府機関が同オペレーションを実行したものとみられると指摘された。

また、欧州では、平成29年（2017年）のフランス大統領選挙に際して、ロシア国営通信社からマクロン候補（当時）に不利な偽情報が流布されたとの報道も見られた。

このような事態に対して、米国では表現の自由に配慮し、政府による情報発信内容の規制には慎重である一方、プラットフォーム事業者が偽情報対策のため自主的な取組を進めている。FacebookやInstagramを運営する米国Meta社は、ウクライナ及びその支援国を批判する内容の投稿を行うロシアと関連する1,000以上のアカウントや、保守とリベラル双方の米国人を装った中国と関連する約100のアカウントなどを削除した旨公表した（9月）。

また、欧州連合（EU）は平成27年（2015年）、ロシアの偽情報キャンペーンに対応するため、ウェブサイト「EU vs Disinfo」を立ち上げ、選挙干渉について「民主主義社会が直面する最も深刻な偽情報による脅威の一つ」との認識を示し、流布されたとする偽情報を13言語で公表している。

今後とも偽情報が民主的プロセスに及ぼす影響には注意が必要である。

2　活動主体の多様化が進むサイバー空間

国家が関与・支援するサイバー攻撃

国家が関与・支援するサイバー攻撃について、その実行者と所属する国家機関等を特定・公表する欧米当局の取組（パブリック・アトリビューション）は、令和4年（2022年）も以下のとおり継続している。

■ 中国

マッカラム英国保安局（MI5）長官とレイ米国連邦捜査局（FBI）長官は、中国政府及び中国共産党の脅威について共同会見を実施し、その中で、国家が背景にあるサイバー脅威主体による政府、民間部門への攻撃が観測されており、その活動が大規模かつ洗練されている旨指摘した（7月）。その際、MI5長官は、中国による航空宇宙企業への高度なサイバー攻撃を阻止した（5月）とも言及した。

■ ロシア

英国は、ウクライナ政府機関等を標的としたウェブサイトの改ざん及びマルウェアの感染（1月）に関して、また、米国及び英国は、オンライン決済や銀行アプリの使用にも支障を来したとされるウクライナの金融機関等に対するDDoS攻撃（2月）に関して、

MI5長官（左）とFBI長官（右）の共同会見
（MI5ウェブサイト〈https://www.mi5.gov.uk/news/speech-by-mi5-and-fbi〉）

それぞれロシアの軍情報機関が関与したと発表した（2月、5月）。また、ウクライナの政府機関や重要インフラ関連組織にマルウェアを感染させた（2月）とされるロシアの軍情報機関と関連を有するサイバー脅威主体について、ウクライナ政府は、同脅威主体がマルウェアを使用してウクライナの高圧変電所の制御システムを停止させようと試みたと発表した（4月）。さらに、ウクライナ侵略前から、ロシアの情報機関と関連を有するサイバー脅威主体が、NATO加

盟国の外交機関から情報を窃取したとされるところ、これらロシアによる一連のサイバー攻撃について、英国国家サイバーセキュリティセンター長は、「ロシアは、2月のウクライナへの侵略を支援するため、一連の大規模なサイバー攻撃を開始した。おそらく史上最も持続的かつ集中的なサイバー作戦である」と評した（9月）（P.10「特集1 ロシアによるウクライナ侵略をめぐって揺れ動いた世界」）。

■ 北朝鮮

国連安保理北朝鮮制裁委員会専門家パネルは、令和3年（2021年）度の最終報告書及び令和4年（2022年）度の中間報告書を公表し（4月、10月）、北朝鮮のサイバー脅威主体が、関連する国連決議に違反して機微技術の入手を企図したサイバー攻撃を行っていることや、金融機関や暗号資産交換事業者を狙った活動を継続し、令和3年（2021年）から令和4年（2022年）にかけて、毎年数億ドル相当の暗号資産を窃取していることなどを指摘した。

FBIは、3月に発覚した約6億ドル相当の暗号資産の窃取事案について、北朝鮮のサイバー脅威主体が実行したものと認められる旨の見解を表明した（4月）。また、米国財務省は、同主体に対する制裁措置を更新し、事案で用いられた暗号資産ウォレットアドレスを制裁リストに追加した（4月）ほか、北朝鮮が窃取した暗号資産の資金洗浄を支援したとされる暗号資産事業者を制裁対象に指定した旨発表した（5月、8月）。

暗号資産関連事業者等を標的とした北朝鮮のサイバー攻撃に関しては、我が国金融庁、警察庁及び内閣サイバーセキュリティセンターも、暗号資産取引に関わる個人・事業者に向けた注意喚起を行った（10月）ほか、外務省、財務省及び経済産業省も、北朝鮮のサイバー脅威主体「ラザルス・グループ」を資産凍結等の措置の対象者に追加する旨の発表を行った（12月）。

■ イラン

アルバニアのラマ首相は、同国政府機関等に対するサイバー攻撃（7月）に関して、イランによって組織・支援されたグループが関与した証拠が得られた旨の声明を発出し、イランとの即時断交を発表した（9月）。併せて、米国国家安全保障会議報道官は、アルバニアに対するサイバー攻撃について、責任はイランにあると結論付けたほか、米国財務省が、サイバー攻撃の実行を指揮したイラン情報省及び同長官を制裁対象に指定した旨発表した（9月）。

多様化する非国家主体の活動

国家が関与・支援するサイバー脅威主体だけでなく、国際的な事象に関連して活動する非国家主体にも注目が集まった。非国家主体の中には、「アノニマス」のような国際ハッカー集団のほか、政府の呼び掛けに応じて攻撃に加わるIT技術者らなど、多様な思想的・社会的背景を持つ集団や個人が存在している。

例えば、ロシアのウクライナ侵略以降、サイバー空間には、ロシア又はウクライナ支持派の集団・個人が現れ、それぞれが、ロシア又はウクライナ及びその支援国に対するサイバー攻撃に参加した。

ロシアを支持し、「Killnet」を名のるハッカー集団は、ウクライナへの支援を理由に、米国の国際空港（3月）、ルーマニアの国防省等（4月）のウェブサイトにDDoS攻撃を実行したと報じられた。その後も、同集団は、ウクライナやNATO加盟国をサイバー攻撃の標的として名指しし（5月）、実際にリトアニアの行政機関（6月）、エストニアの200以上の組織（8月）等にDDoS攻撃を実行し

たとされる。

他方、ウクライナのミハイロ・フェドロフ副首相は、自身のツイッターで、同国IT軍の創設を告知し、世界中のIT技術者らに同軍への参加を要請するとともに、Telegram内のチャンネル「IT ARMY of Ukraine」では、ロシア及びベラルーシに対するサイバー攻撃等を実施するよう呼び掛けた。

加えて、ベラルーシの反体制派ハッカー集団が反ロシアを掲げ、ロシア軍のベラルーシ領内での進行を阻止するため、ベラルーシ鉄道を攻撃したと主張した（1月）ほか、「アノニマス」の中には、ロシア政府を標的としている旨表明し(2月)、ロシア国内のプリンターを攻撃したと主張する（3月）グループも見られた。

また、米国のペロシ下院議長の訪台当日以降、台湾の総統府、外交部、桃園国際空港等のウェブサイトに対するDDoS攻撃事案が発生したほか、ハッキングされた駅やコンビニのテレビモニターに同訪台を批判するメッセージが映し出された。その後、中国の愛国的ハッカー集団が、総統府、警察等に対するサイバー攻撃を実行した旨主張した（8月）。

非国家主体がもたらす脅威が我が国にも波及

我が国では、行政機関、行政情報ポータルサイトのe-Gov、鉄道会社等の20以上のウェブサイト、地方税ポータルシステムのeLTAXにおいて、一時的に閲覧障害が発生した（9月）。これらの攻撃の一部に関し、前述の「Killnet」がサイバー攻撃の実行を認め、攻撃理由として我が国による「反ロシアキャンペーン」の実施、「ウクライナへの支援とクリル諸島（千島列島及び北方領土）への侵略」などを挙げた。同集団は、我が国が、ロシア政府による自由訪問及び四島交流に係る合意の効力の停止に係る政府令の発表に対して抗議したことを取り上げ、我が国を「米国の手先」と断じたほか、「日本政府全体への宣戦布告」を主張する動画を投稿した（9月）。

3　サイバーセキュリティ意識の向上に加え、メディア情報リテラシーの向上も課題

社会のデジタル化の流れが継続する中で、「公共空間」としてのサイバー空間の位置付けはより重要性を増すとみられる。それに伴い、サイバー攻撃がもたらす脅威も深刻度を増すと考えられるところ、今後も、国家が関与・支援するサイバー脅威主体も含めた様々なサイバー脅威主体による我が国に対するサイバー攻撃は継続するとみられ、デジタル化の進展と並行してサイバーセキュリティ意識の向上が課題である。

また、民主主義の基盤を脅かすおそれもある偽情報に対しては、他の情報との比較や情報の発信元の確認などを通じて、情報の真偽を適切に判断する力、いわゆるメディア情報リテラシーの向上が必要である。