ロシアの対ウクライナサイバー作戦の先進主要７国サイバーセキュリティ政策への影響

三　角　育　生*

Impacts on Cybersecurity Policies of G7 States by Russian cyber operations

Ikuo MISUMI

Abstract

This paper examines how the situation in Ukraine caused by Russian cyber operations had affected cybersecurity policies implemented by G7 states. It is found that there are no substantial / major changes in the cybersecurity strategies of these states. Instead, G7 states implement responsive policies such as issuing cybersecurity alerts and technical guidance triggered by major incidents in Ukraine by Russian cyber operations and potential threats on domestic critical infrastructures in a timely and effective manner. These responsive policies are developed by cyber authorities by cooperating with ally countries and intelligence agencies. Such cooperations increase trustworthiness of the information and are important to be taken seriously by the private/ public sectors.

要旨

ロシアのサイバー作戦によるウクライナ情勢がＧ７国のサイバーセキュリティ政策に与えた影響について分析した。これまでのところ、Ｇ７国の戦略的なサイバーセキュリティ政策の実質的な変更は見られない。一方、Ｇ７国は適時、国際連携やインテリジェンス組織等とサイバーセキュリティ組織との連携を図りつつ、国内の重要インフラ事業者など官民の組織に緊急性・深刻さの伝わる方法で、ロシアのサイバー作戦を踏まえた迅速な注意喚起を発行するといった対処的政策を執っていることが分かった。

キーワード：ウクライナ、ロシア、サイバー作戦、G7国、サイバーセキュリティ政策

＊東海大学情報通信学部長、教授（Tokai University）

1．はじめに

2022年２月24日、ロシアはウクライナの主権及び領土の一体性を侵害し、武力の行使を禁ずる国際法の深刻な違反である軍事行動を開始した[1)]。サイバー空間の状況をみると、軍事行動開始以前から、ウクライナの政府機関を含む様々な組織に対してロシアの国家が関与したとみられる活動者によるサイバー攻撃は多発していた。ロシアが米欧に対してウクライナがNATOに加盟しないことの保証を求めている交渉の段階[2)]で、ロシアは武力紛争にまでエスカレートしてしまうダメージにはつながらないサイバー攻撃の利用を志向していたとみる説もある[3)]。これらのサイバー攻撃は、大部分が攻撃対象とされたウクライナ政府機関や重要インフラのデバイスをコードの上書きなどにより動作不能とする、破壊型のものである。軍事侵攻後も、ウクライナの政府機関や重要インフラに対する破壊型サイバー攻撃などが観測されている。

こうしたサイバー攻撃が、経済制裁等の措置を行っている国の政府機関や重要インフラに対しも行われないとは言い切れない。そこで、本稿では、制裁措置をとっている先進主要７国（G７国）のサイバーセキュリティ政策が、ウクライナ情勢を受けてどの様な影響を与えられたかについて分析し、今後の日本のサイバーセキュリティ政策の策定、対処等にあたっての示唆を検討することとする。

2．分析の方針

（1）データの収集　ロシアのウクライナ侵攻に関連して制裁措置をとった主要国としてG７国に着目する。ただし、仏・独・伊については基本的にはEUの政策や指令を受けて具体的施策を実施すると考えられることから、まとめてEUの政策の動きを主たる分析対象とする。サイバーセキュリティ政策は、インテリジェンスや軍事に関するものも含むことがあるが、本稿では、ウクライナの政府機関、重要インフラなどがサイバー攻撃を受けていることがG７国に与える影響を広く全般的に分析することを目的とし、特に軍事・インテリジェンスに焦点をあてるのではなく、サイバーセキュリティ政策一般を分析の対象とする。

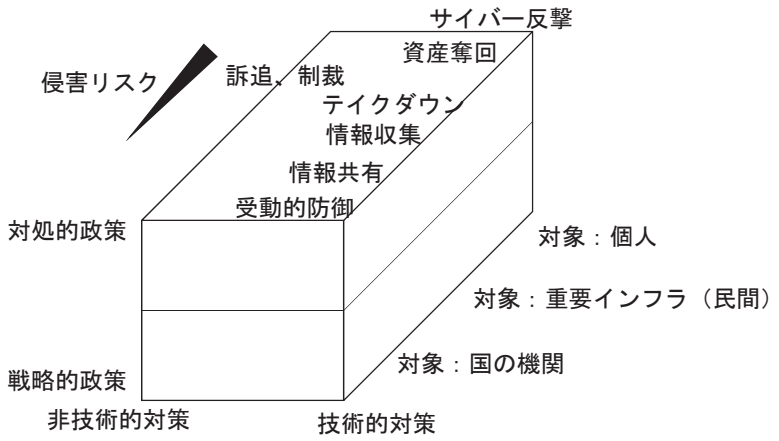
具体的には、米については、サイバーセキュリティ政策がホワイトハウス主導の下で政策が包括的にパッケージ化されるなどの傾向がみられること［三角2021b］から、主としてBriefing Roomにおける大統領報道官等の説明、政策公表などに着目し、必要に応じてサイバーセキュリティ政策を推進するCybersecurity and Infrastructure Security Agency

（CISA）や連邦捜査局（FBI）が公表する施策をデータとして用いる。英については、サイバーセキュリティに係る戦略を従来からとりまとめてきている Cabinet Office と、Government Communications Headquarters（GCHQ）傘下で民間セクターなどのサイバーセキュリティ対策などをミッションとする National Cyber Security Center（NCSC）が公表する施策を用いる。EU については、欧州議会、欧州委員会及び EU におけるサイバーセキュリティの推進や構成国等を支援する組織である European Union Agency for Cybersecurity（ENISA）が公表する施策を用いる。カナダについては、Canadian Centre for Cyber Security（CCCS）が公表する施策を用いる。日本については、主として内閣サイバーセキュリティセンター（NISC）が公表する施策を用いる。

データとして用いる政策の検討対象期間については、基本的に、米政府がロシアによるウクライナへの軍事侵攻の可能性について警告[4)]を発した2021年11月以降本稿執筆時点（2022年９月末）までとし、主としてその間に公表されたサイバーセキュリティ政策を検討する。

（２）分析フレームワーク　サイバーセキュリティ政策は、コンピュータウイルス対策などの技術的対策と法令などの非技術的対策が要素にあり、また、戦略の策定・実施など戦略的政策と顕著なサイバーセキュリティインシデントの影響緩和などを図る対処的政策に分類できる。これらの政策の内容は、受動的防御といったプライバシー等権利への侵害リスクの低いものから攻撃的・反撃的な人権侵害のリスクの高いものまでスペクトラムがある［三角2021b］。本稿では、これらを軸とするサイバーセキュリティ政策分析フレームワーク（図表１参照）を念頭におき各国・地域の政策を比較分析する。

図表１　サイバーセキュリティ政策分析フレームワーク



（出典：三角2021b: 15）

3．ウクライナ侵攻前の各国・地域の政策

2021年11月以降、サイバー空間ではウクライナに対するロシアの国家が関与したとみられる破壊的なサイバー攻撃などが観測された。例えば、2022年１月13日にウクライナ政府機関等に対して行われた破壊型のマルウェアを用いた攻撃があった。これについては、マイクロソフト社が１月15日に分析情報[5)]を公表しており、ウクライナ政府はこれをロシアの仕業であるとしている[6)]。このサイバー攻撃のあった日は、ロシア提案の欧州安全保障案に対して欧州安保協力機構会合から適切な回答を得られていないとロシア大使が述べた日[7)]である。マイクロソフト社分析によれば、この攻撃に用いられたマルウェアは、ランサムウェアを装っているが、実際には攻撃対象となるデバイスを動作不能とするなどの破壊型のものである解析としている。

軍事侵攻前日の２月23日にも、顕著な破壊型のマルウェアによる攻撃があった。ブロードコム社シマンテックのブログ記事[8)]によると、破壊型マルウェアが、ウクライナの金融、IT サービス分野の企業などで展開されたとしている。その手口は、2021年11月以降メールサーバーソフトウェアの脆弱性を悪用するなどして侵入し、破壊動作のときまで潜伏していたというものであった。またクラウドフレア社によると、同日にキエフに対して大規模な分散型サービス拒否（DDoS）攻撃もあったとしている[9)]。

（１）米の政策　バイデン政権は、従来から SolarWinds 事件[10)]などロシア政府等に帰責されるとするサイバー攻撃事件などを踏まえて、戦略的政策として、米のサイバーセキュリティの向上に関する大統領令（EO14028、2021年５月12日）[11)]や、重要インフラ制御システムのサイバーセキュリティ強化に関する安全保障メモランダム（2021年７月28日）[12)]を発出してきた。これらを受けて民間の重要インフラ事業者に関しては、例えば、事業者のサイバー攻撃の検知、対処能力の強化を図る電力インフラサイバーセキュリティ強化100日計画[13)]を推進していた。そして、エネルギー省は、サイバー攻撃の情報などを踏まえた制御システムの設計・構築段階からのエンジニアリングを推奨する National Cyber-Informed Engineering Strategy（2022年６月）[14)]を公表するなどしてきている。また、大統領令 EO14028を受けた連邦政府自身の対策強化策として、2022年１月26日にゼロトラストアーキテクチャに移行する連邦の戦略[15)]を取りまとめて公表した。

対処的政策としては、2022年１月11日に、CISA が FBI と共同で、ロシアが用いるサイバー攻撃の様々な手法などを示した「米国重要インフラに対するロシア国家が支援するサイバー脅威の理解と緩和」についての注意喚起を公表[16)]し、英[17)]とカナダ[18)]が同注意喚

起を支持した。また同月18日にCISAが、前述のマイクロソフト社の分析情報に言及しつつ、ウクライナの公的機関や重要な機能を担う民間組織が破壊的なサイバー攻撃を受けていることなどの情勢にかんがみ、直ちに深刻な潜在的脅威から保護するためのサイバーセキュリティ対策の実施を呼びかけた[19]。これは、リモートアクセスなどで多要素認証を要求することを確実にするなど有害なサイバー攻撃による侵入の可能性を低減すること、ウクライナの組織と協力関係がある場合に当該組織から送られる通信のアクセス制御監視強化など潜在的な侵入の迅速な検知のための取組み実施、侵入があった場合の対処の着実な準備、破壊的なサイバー事象に対する組織の回復力の最大化などを内容とする。

また、2022年２月15日に、ウクライナ情勢に関してバイデン大統領が、もしもロシアが企業や重要インフラに対する破壊的なサイバー攻撃といった非対称的な活動を通じて米や同盟国を攻撃した場合に我々は対応する用意があると発言[20]した。そして２月18日のアン・ノイバーガー国家安全保障会議サイバーセキュリティ担当副国家安全保障顧問[21]の説明によれば、国内における具体的なサイバー攻撃を認識しているものではないものの、大統領の指示を受けて2021年11月からサイバー攻撃の可能性に備えるよう努めており、

①潜在的脅威に対する緊急のサイバー防御強化の取組み、

②サイバー攻撃への対応やネットワークの復旧などに関するウクライナ支援の取組み強化、

③情報共有などの同盟国等と緊密な協力による悪意あるサイバー活動の防御・抑止

をしてきたとしている。

（２）その他の国の政策　英は、戦略的政策として2021年12月15日に新たな「サイバー戦略2022」[22]を発表した。本戦略は、サイバー空間内及びサイバー空間を通じて国益を守り促進する能力であるサイバーパワーを中心としたもので、政府主導のサイバーセキュリティの取組みを示した従来のサイバーセキュリティ戦略とは一線を画するものである。安全で強靭な国家、革新的で繁栄したデジタル社会などの目標実現のために民主的なサイバー大国でありつづけることを重視している。そのために、社会全体のアプローチとして、

①人材への投資などのサイバーエコシステムの強化、

②サイバーセキュリティと強靭さを基盤とした繁栄したデジタルUK、

③人工知能やマイクロプロセッサ、量子コンピューティングなどサイバーパワーに不可欠な技術の優位性、

④国際秩序のためのグローバルリーダーシップ、

⑤敵を検知・途絶・抑止することにより、サイバー空間内及びサイバー空間を通じて国家安全保障を強化すること

を戦略の柱としている。同戦略では、ロシアに関してはSolarWinds社事件などに言及しつつも、より広くサプライチェーンの課題などに取組むことを示している。また、2021年に設置された国家サイバーフォースにも焦点を当て、英の攻撃的なサイバー能力を継続的に強化するとしている。

同国の対処的な政策としては、2022年１月17日にNCSCがロギングや監視、システムのパッチ適用やアクセス制御の確認などを内容とする「サイバー脅威が高まった場合の対応」という、ロシアのウクライナ侵攻に先立ち全ての英の国内組織に対するサイバー防衛強化の要請[23]がある。また、２月15日、16日にウクライナの金融分野に対してDDoS攻撃があったが、NCSCは、ほぼ確実にロシアのインテリジェンス組織の仕業であると分析している旨公表[24]した。

EUの戦略的政策としては、今回の検討対象期間以前の2020年12月に欧州委員会により取りまとめられたサイバーセキュリティ戦略（The EU's Cybersecurity Strategy for the Digital Decade）[25]がある。同戦略は、サイバー攻撃の兆候を十分早期に検出、被害が発生する前に予防的な対応を行うことを目的としたサイバーセキュリティシールドの構築、IT製品等の認証制度[26]を通じたセキュリティの強化などを推進するとともに、サイバー攻撃を防護、抑止し、対応のための運用能力として合同サイバーユニットの整備や外交的措置のフレームワークの活用などを定めている。加えて、同戦略は、EU全体で共通にサイバーの強靭さを高めるべく構成国に緊急時対応体制（CSIRT）の整備や不可欠なインフラやサービスの事業者のサイバーインシデントの報告を義務付けることなどを規定していたNIS（Network and Information Security）指令を改定することにつき提案した。なお、改訂NIS指令案[27]は、適用対象を拡大し、不可欠・重要なインフラやサービス事業者の拡大、加盟国毎に判断していた対象事業者のばらつきをなくすための明確化を図り、サプライチェーン問題への対応などを強化するものとなっている。案については、2022年５月13日に欧州委員会と議会とで暫定合意[28]されたところであり、構成国との間でのプロセスが進められている。

EUにおける対処的な政策としては、明示的にウクライナ情勢を受けたものとして発行されたものではないが、2022年２月14日にENISAがCERT-EU（Computer Emergency Response Team for the EU institutions, bodies and agencies）と共同で、全ての公的・民間組織に対して、多要素認証の導入などを図ることでサイバーレジリエンスを強化するためのベストプラクティスを提示[29]した。

日本の戦略的政策としては、2021年９月にサイバーセキュリティ戦略の改訂版[30]を閣議決定している。同戦略では、ロシアが軍事的・政治的目的達成に向けて影響力行使のためにサイバー攻撃等を行っているとみられるなどの国際情勢認識を示し、すべての国民、

セクター等においてサイバーセキュリティ確保が必要であり、デジタル化の動きと呼応し誰一人取り残さないサイバーセキュリティ確保の取組みを進める必要性を示した。そして、デジタルトランスフォーメーションとサイバーセキュリティの同時推進、産業横断的なサプライチェーン管理やナショナルサート機能強化等による安全・安心の確保、中国・ロシア・北朝鮮からの脅威などを踏まえた外交・安全保障上のサイバー分野の優先度向上や自衛隊におけるサイバー防衛能力の抜本的強化、日米同盟の維持・強化などによる安全保障の観点からの取組強化といった方針を示している。対処的な政策としては、２月23日に経済産業省が、昨今のウクライナ情勢を踏まえた技術的対策等を示した注意喚起[31]を行った。

（３）各国・地域の政策の分析　検討対象期間（ウクライナ侵攻前）において、各国・地域の戦略的政策としてとりまとめられたもの[32]は、英の「サイバー戦略2022」である。本戦略において、ロシアに関連する懸念としてはSolarWinds事件やランサムウェアを用いた犯罪などを挙げており、ロシア国家が支援するサイバー攻撃であることの特定などをグローバルな協力国の機関などと共に実施してきていることを説明している。こうした事態への対処として、敵を検知・途絶・抑止することなど上述の方針を英は決定している。しかし、ロシアによるウクライナ侵攻の可能性や関連した破壊型のマルウェアなどについて特段の言及はみあたらない。一般に、サイバーセキュリティ戦略は、その国の基本的価値観や方針を国の内外に示して国内関係組織間の政策調整や同盟国等との連携促進などに資するものといえる。そしてそのとりまとめ決定プロセスは関係者間での議論などを行うことから一定の期間を要するものである［三角2021a］。日本年金機構への不正アクセスによる情報流出事件を受けて策定中のサイバーセキュリティ戦略の内容を修正した日本の例［三角2020］を見ると、具体的な情勢変化や大規模なサイバー攻撃事件などが自国に発生したときには、その情勢変化や事件への対応戦略が盛り込まれる可能性があるといえよう。しかしながら、ウクライナ侵攻前の緊張が高まった段階で策定された英のサイバー戦略の場合には、そうした内容修正の発生理由があったとはいえないと考えられる。英のサイバー戦略は、防御的なものから国家サイバーフォースなどの攻撃的な活動まで幅広く方針を示しており、戦略策定段階での変更はなくても国際情勢の変化に対応できるものとされたと思われる。

英以外の戦略的政策についてみると、米では、2021年の大統領令等に基づき具体的な施策を実施する段階にあり、また、EUでも同様に、2020年のサイバーセキュリティ戦略に基づく施策を実装するフェーズとなっている。日本では本稿の検討対象期間の２か月前に新たな戦略が決定されたばかりであり、検討対象期間は戦略に基づく施策実施に着手した

時期である。従って、戦略の見直しが行われてはいない。これらの国において具体的な情勢変化や大規模なサイバー攻撃事件が顕在化していない状況下では、中長期的視点でとりまとめられた戦略的政策について特段の見直し行うのではなく、戦略に基づく具体的な施策の実施内容の充実などで対応することが妥当であるといえよう。

対処的な政策としては、破壊型のマルウェアを用いたウクライナの組織へのサイバー攻撃を踏まえて、米、英などが連携して、民間のIT会社の技術情報なども参照しつつ、具体的な技術的対処策を迅速に公開している。そして、当該サイバー攻撃がロシアの国家機関に帰責されるとの分析結果も英などが公表している。帰責に関する分析にあたっては侵害リスクの高い活動も含まれると考えられるところ、インテリジェンス組織とサイバーセキュリティ当局の連携もあったと思われる。

4．ウクライナ侵攻日以降の各国・地域の政策

ロシアの軍事侵攻当日、侵攻直前に、サイバー攻撃があり、米の衛星通信会社Viasatがウクライナ及び一部の欧州で展開している通信サービスが途絶[33]した。この攻撃は、米英のインテリジェンス組織によってほぼ確実にロシアが関与したものと評価されている[34]。

ロシア侵攻後には、マイクロソフト社の分析[35]によると、物理的（Kinetic）攻撃と一定の相関がみられる複数のサイバー攻撃がみられた。例えば、ロシアは3月1日にキーウのTV塔をミサイルで攻撃したが、同日、キーウの放送局が破壊型のマルウェアによるサイバー攻撃を受けている。また、同分析によると、エネルギー関連などの重要インフラ施設も物理的及びサイバー攻撃の対象となっている。例えば、3月上旬チョルノービリやザポリージャの原発がロシア軍に占拠されたが、ロシアの国家が関与しているとみられるサイバー攻撃者は2021年12月以降継続的にウクライナの原子力安全組織から情報を窃取していたと分析されている。

（1）米の政策　2月24日、ウクライナ侵攻に関連してバイデン大統領は、ロシアが米の企業や重要インフラへのサイバー攻撃を行おうとすれば我々は対応する用意をしている、何か月もロシアによるサイバー攻撃への対処も含めて米政府は民間部門とともに緊密にサイバー防衛の強化を図ってきた旨発言[36]をした。3月21日には、米等によるロシア経済制裁への対抗の趣旨を含めてロシアによるサイバー脅威が高まっているとのインテリジェンス情報を踏まえて、改めてバイデン大統領は、ロシアによる潜在的サイバー攻撃への対策を呼びかけた。重要インフラが民間によって所有・運営されていることから、これ

らの事業者などによるサイバーセキュリティの取組みを加速するべく、CISA の Shields-up キャンペーン[37] を含めて米政府が積極的に協力していくとしたものである[38]。この大統領の声明に併せて米政府は、多要素認証、脆弱性対策、コンピュータ等における脅威を継続的に検知・緩和するための最新のセキュリティツールの配備などの方策による対策の強化を改めて要請[39] している。

なお、３月21日の大統領の声明に先立ち、その前の週に、バイデン大統領は重要インフラのサイバーインシデントの報告義務化等に向けた Cyber Incident Reporting for Critical Infrastructure Act of 2022に署名し、また、政府は米企業100社以上を集めて脅威インテリジェンス情報の提供を行っている[40]。また、個別セクターに関する注意喚起として、３月17日に、CISA が FBI と共同で国際衛星通信ネットワークに対する脅威の可能性を指摘して、通信機器への入出力ポイントの監視強化、最小権限の徹底など呼びかけている[41]。

（２）その他の国の政策　英 NCSC は、2022年３月18日に、ウクライナ侵攻を踏まえて英の組織において高まっているサイバー脅威への対応強化を呼びかけた[42]。その基本的な対策内容は１月17日に公表した「サイバー脅威が高まった場合の対応」（前述）を参照するものであるが、改めて、脅威は時間の経過によって変化するものであり現在の脅威に対応した組織全体のリスクに見合った防御対策の必要性を指摘している。４月20日には、英の NCSC と National Crime Agency（NCA）が、米 CISA、FBI、National Security Agency（NSA）、豪 Australian Cyber Security Centre（ACSC）、カナダ CCCS[43]、ニュージーランド National Cyber Security Centre（NCSC-NZ）及び Computer Emergency Response Team New Zealand（CERT-NZ）と共同で、ロシアにおける国家が支援する攻撃者やサイバー犯罪者による重要インフラへのサイバー攻撃の脅威に関する技術的な情報を公表した[44]。なお、同情報は、米 CISA による、ロシア連邦保安局といったロシア政府・軍事組織などのサイバー脅威の行為者の手法についての解説[45] を参照している。さらに、2022年７月５日、英 NCSC は、情勢が長期化するなかリスク判断の再評価、要員の業務バランスや休養の確保など、潜在的なサイバー脅威の高まりに対応して強化した体制の維持にあたっての注意喚起[46] を行っている。

EU は、2022年３月８、９日にパリとヌヴェールで開催された欧州電気通信及びデジタル問題担当閣僚非公式会合において[47]、ウクライナ支援、偽情報への対処などを表明している。そして、EU の通信ネットワークとサイバーセキュリティの強靭性を高めることの重要性に留意し、欧州電子通信規制当局（BEREC）及び ENISA に対して、EU の通信ネットワーク及びインフラを脅かすリスクの範囲を特定し、その強靭性を高める方法について勧告を行うように要請した。

EU 構成国である独では、連邦情報技術セキュリティ庁（BSI）がロシアのウクライナ侵攻に関連した注意喚起を発信[48]しつづけている。技術的なサイバーセキュリティ対策について示しつつ、２月25日時点でウクライナ情勢に関連する情報セキュリティに関する深刻な脅威はないものの警戒と対応の強化を独の企業等に求めた。３月４日に同注意喚起を更新して抽象的に増大する脅威状況を認識していること、５月12日の更新では重要インフラなどを含めて独における脅威の状況が増大していること、IT セキュリティインシデントが発生しているが深刻な影響はないことなどを、８月３日の更新では、エネルギー部門などがサイバー攻撃の標的となりやすいことなどを含めて一層の注意喚起を行った。

日本は、対処的な政策として、３月24日に、経済産業省、総務省、警察庁及び NISC が連名で注意喚起[49]を発出している。これは、２月23日の経済産業省による注意喚起、３月１日に国内の自動車部品メーカーがサイバー攻撃の被害にあった旨の発表がなされたことも踏まえた NISC 等による注意喚起[50]に続く一連のものとなっている。

（３）各国・地域の政策の分析　ロシアのウクライナ侵攻後の各国のサイバーセキュリティ政策は、対処的政策が中心となっている。これらの対処的政策の公表は迅速に行われている。その一つの理由として、侵攻直後のバイデン大統領の声明を見ても、自国の重要インフラ事業者等へのロシアからのサイバー攻撃の潜在的リスクを警戒している点が考えられる。特に、３月７日にロシア政府は日本や米欧を「非友好国」に指定[51]したが、この時期から各国政府が、重要インフラ事業者や民間企業等に対する潜在的なサイバー攻撃への一層の対策強化を要請していることについて、特に留意するべきと考える。

ロシアのサイバー攻撃は、SolarWinds 事件や、ウクライナ侵攻前にロシアが同国組織にしかけた破壊型マルウェアを用いたサイバー攻撃の例を見ても、事前に十分に時間をかけてマルウェアを検知されないような方法で仕込むものが多い。このことから考えると、ロシア政府によって非友好国とされた各国において、すでに重要インフラ事業者のネットワークなどに破壊型のマルウェアが検知されないような方法で仕込まれている可能性を考えることは妥当である。対策としては、仮にマルウェアが仕込まれたとしても、それが重要インフラサービスの途絶といった事態に及ばないように、不審な兆候を検知し、ネットワーク内の更なる侵入が困難となるような技術的な緩和措置を採ることなどが考えられる。３月に、米 CISA の Shields-up キャンペーンを始めとして各国政府が重要インフラ事業者や民間企業等に技術的対策の迅速な対応を強く求めたことには理由があるといえよう。

こうした要請は、実効性を担保するためにも、重要インフラ事業者や民間企業等に真剣に受け止められる必要がある。そのためには注意喚起の受け手にとって信頼でき真剣に受

け止められるような形での情報発信が重要であろう。Shield-up キャンペーンの様な訴求力のあるメッセージを大統領自ら言及することなどはその一つと言える。また、米、英、カナダなどが連携して対応を呼び掛ける方法も同様に有益である。こうした国際連携は、ある国が特定の脅威インテリジェンス情報を得たときに、迅速にそれを他国とも共有し、これらの国においても対応の検討をできるようになる点からも有益である。

なお、サイバー攻撃に対する高い警戒態勢を長期間継続することは、サイバーセキュリティ担当者の緊張が長く続くことによる疲労などが原因の不注意が引き金となるインシデントが発生するリスクも高まるものである。また、脅威やリスクは、一般に、時間の経過とともに情勢変化や新たな情報が得られることなどから、当初想定したものから変化する。こうした点に留意した英の事態の長期化に対応した体制維持に関する注意喚起の発出などは有益な施策であると考える。

5．まとめ

ロシアによるウクライナ侵攻に関連し、侵攻前からロシアに帰責されるサイバー攻撃が多数観測されたことを受け、米等の先進主要国において、対処的なサイバーセキュリティ政策が採られた。侵攻前にウクライナの組織に対する破壊型のマルウェアなどによるサイバー攻撃が行われたとき、サイバー攻撃と連携した物理的攻撃が開始されたとき、ロシア政府が非友好国の指定を公表したとき、侵攻が長期化してきたときなどそれぞれの時点において、重要インフラや民間企業等に対して技術的な防御策の適用の要請、防御策の強化の要請、サイバーセキュリティ担当者の負荷分散やリスクの再評価の要請など情勢に応じたものを迅速に発出してきている（図表２参照）。

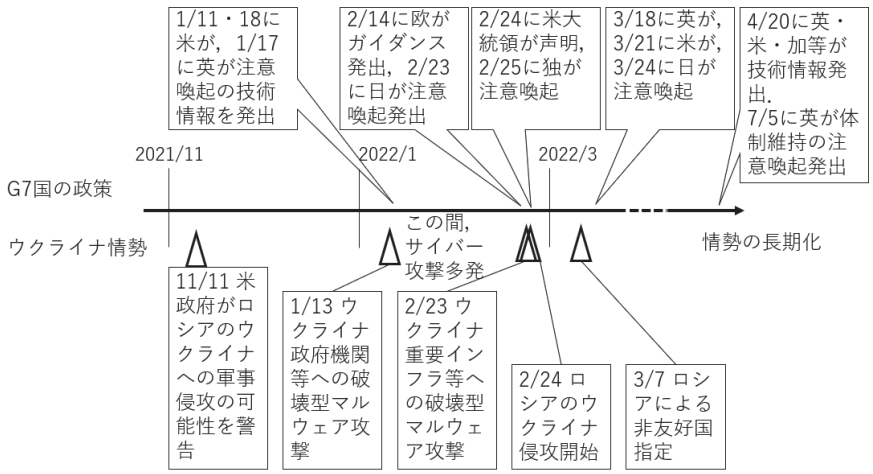
一方、中長期的視点から企画立案される戦略的な政策については、ウクライナ情勢を受けた各時点で特に内容を見直すということはなされていない。戦略的に検討・決定された政策の範囲内で対応していると考えられる。しかし、今後、ウクライナ情勢が更に長期化し、かつ、サイバー空間内又はサイバー空間を通じて生じる情勢が大きく変化するようなこととなれば、戦略的政策の見直しが生じる可能性は否定できないだろう。

各国・地域の政策の分析を踏まえて、以下に日本の政策として参考となるものをまとめる。

①緊急性、深刻さの伝わる注意喚起　米大統領自ら情報発信をする、Shiels-up といった分かりやすく緊急性が伝わるキャンペーンの実施などは、民間企業等が対策を講じなければならないことの動機付け、意識付けに有益であると考えられる。

②外交・軍事などの安全保障当局やインテリジェンス組織との適切な関係　米英などは

図表２　対処的サイバーセキュリティ政策とウクライナ情勢との時系列関係



（出典：筆者作成）

サイバー攻撃が誰に帰責されるものかについての分析を行って情報発信している。こうした活動を行うにはインテリジェンス組織などとの連携が必要になると考えられる。また、侵攻前後の情勢分析などを適時情報発信していくときにも、インテリジェンス組織や安全保障当局との連携が重要である。サイバーセキュリティ当局は技術的な事項に専門性を発揮できるが、ウクライナ情勢のような事態においては安全保障当局などとの適切な連携が適切なサイバーセキュリティ政策を実施していくためにも重要になろう。

③官民連携　政府が広く技術的な対策情報を発信するにあたり、民間の IT 企業が行った公表された解析結果なども参照していることは、対策を実施する民間企業等の技術者においても分りやすいものである。また、政府が保有する脅威情報などを民間企業等との会合において提供することも有益である。こうした政府からの情報提供等は官民連携を促進し、国内のサイバーセキュリティ体制の強化に資するものと考える。

④国際連携　注意喚起などを同志国などと共同で、または、歩調を合わせて発信し、参照しあうなどの取組みは、国内外に対するメッセージとして強いものとなる。こうした歩調を合わせた共同した取組みを行う過程では、脅威情報の共有なども行われるものと考えられ、発信する内容も、より信頼性の高いものとなると考える。

⑤調査・分析能力　対策情報の発信や、情勢を踏まえた適切なタイミングでの対策強化要請などを適切に行うためには、情勢分析や技術的な解析の結果が、要請された対策内容の質に影響する。そのため、調査・分析能力を充実させ高めていくことは常に必要なことである。また、国際連携などを円滑にするためにも、情報を積極的に共有することが必要

であり、そのためにも調査・分析能力の一層の充実は不可欠である。

本稿では、G７国（ただし仏独伊についてはEUを中心として）におけるサイバーセキュリティ政策当局が特定の期間に公表した内容を中心に分析した。サイバーセキュリティに関する政策は、本稿で取り上げた組織以外も企画立案実施しているため、今回の分析は網羅的なものではない。したがって、ロシアのウクライナ侵攻に伴うサイバー情勢が各国のサイバーセキュリティ政策に与えた影響についても、その一面を捉えることができたに過ぎない。この点は更なる調査・分析が必要であると考えている。しかしながら、こうした各国の政策を分析することで、日本にとって有益な方向性を抽出することは一定程度できたと考える。今後、国際情勢が一層変動していくようなときに、日本としても、上述した方向性を念頭においたサイバーセキュリティ政策の企画立案実施が一層円滑かつ着実に行われることを期待する。

参考文献

三角育生（2020）「大規模ITセキュリティインシデント対処の政策的影響」『日本セキュリティ・マネジメント学会誌』34巻2号22-28頁

三角育生（2021a）「我が国のサイバーセキュリティ戦略策定の背景」『日本セキュリティ・マネジメント学会誌』34巻3号39-46頁

三角育生（2021b）「米国バイデン政権のサイバーセキュリティ政策と我が国の政策への示唆」『ヒューマンセキュリティ（東海大学平和戦略国際研究所紀要）』12号2021/2022，13-33頁

註

１）外務省、
https://www.mofa.go.jp/mofaj/press/danwa/page6_000666.html, (Last visited, October 10, 2022)

２）Bloomberg 2022年11月11日記事、https://www.bloomberg.com/news/articles/2022-01-10/first-round-of-u-s-russia-security-talks-ends-amid-war-fears?, (Last visited, October 10, 2022)

３）Mandiant 2022年1月20日ブログ記事、
https://www.mandiant.com/resources/ukraine-crisis-cyber-threats, (Last visited, October 10, 2022)

４）Bloomberg 2021年11月11日記事、https://www.bloomberg.com/news/articles/2021-11-11/u-s-warns-europe-that-russian-troops-may-plan-ukraine-invasion, (Last visited, October 10, 2022)

５）Microsoft 2022年1月15日ブログ記事、
https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/, (Last visited, October 10,2022)

６）Bloomberg 2022年1月17日記事、https://www.bloomberg.com/news/articles/2022-01-16/biden-aide-stops-short-of-blaming-russia-for-ukraine-cyberattack, (Last visited, October 10, 2022)

7）日経 2022年1月14日記事、
https://www.nikkei.com/article/DGXZQOGR13DQO0T10C22A1000000/, (Last visited, October 10, 2022)

8）Symantec Enterprise 2022年2月24日ブログ記事、
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia, (Last visited, October 10, 2022)

9）Cloudflare 2022年3月5日ブログ記事、https://blog.cloudflare.com/internet-traffic-patterns-in-ukraine-since-february-21-2022/, (Last visited, October 10, 2022)

10）攻撃者が何らかの方法によって脆弱性を仕込んだ SolarWinds 社が提供する IT 管理を効率的に実施するソフトウェアのアップデートソフトが2020年3月から6月の間に配給され、最大18千社の顧客がこれをインストールした可能性があった事件。2020年12月に、本企みが表面化して、米 Cybersecurity and Infrastructure Security Agency (CISA) が対策を公表している。CISA, https://www.cisa.gov/uscert/ncas/alerts/aa20-352a, (Last visited, October 10, 2022)

11）Federal Register, https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity, (Last visited, October 10, 2022)

12）White House, https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/, (Last visited, October 10, 2022)

13）White House, https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/20/statement-by-nsc-spokesperson-emily-horne-on-the-biden-administrations-efforts-to-protect-u-s-critical-infrastructure/, (Last visited, October 10, 2022)

14）Department of Energy, https://www.energy.gov/sites/default/files/2022-06/FINAL%20DOE%20National%20CIE%20Strategy%20-%20June%202022_0.pdf, (Last visited, October 18, 2022)

15）White House, https://www.whitehouse.gov/omb/briefing-room/2022/01/26/office-of-management-and-budget-releases-federal-strategy-to-move-the-u-s-government-towards-a-zero-trust-architecture/, (Last visited, October 10, 2022)

16）CISA, https://www.cisa.gov/uscert/ncas/alerts/aa22-011a, (Last visited, October 10, 2022)

17）National Cyber Security Centre (NCSC), https://www.ncsc.gov.uk/news/ncsc-us-partners-promote-understanding-mitigation-russian-state-sponsored-cyber-threats, (Last visited, October 10, 2022)

18）Canadian Centre for Cyber Security (CCCS), https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-centre-reminds-canadian-critical-infrastructure-operators, (Last visited, October 10, 2022)

19）CISA, https://www.cisa.gov/sites/default/files/publications/CISA_Insights-Implement_Cybersecurity_Measures_Now_to_Protect_Against_Critical_Threats_508C.pdf, (Last visited, October 10, 2022)

20）White House, https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/02/15/remarks-by-president-biden-providing-an-update-on-russia-and-ukraine/, (Last visited, October 10, 2022)

21）White House, https://www.whitehouse.gov/briefing-room/press-briefings/2022/02/18/press-briefing-by-press-secretary-jen-psaki-deputy-national-security-advisor-for-cyber-and-emerging-technology-anne-neuberger-and-deputy-national-security-advisor-for-international-economics-and-dep/, (Last visited, October 10, 2022)

22）UK.Gov, https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022, (Last visited, October 11, 2022)

23）NCSC, https://www.ncsc.gov.uk/guidance/actions-to-take-when-the-cyber-threat-is-heightened, (Last visited, October 11, 2022)

24）NCSC, https://www.ncsc.gov.uk/news/russia-ddos-involvement-in-ukraine, (Last visited, October 11, 2022)

25）European Commission, https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0, (Last visited, October 12, 2022)

26）European Union Agency for Cybersecurity (ENISA) は、2019年に IT 製品、サービスなどに対するサイバーセキュリティ認証制度の整備・運用といった業務拡大が図られている。European Union (EU), https://eur-lex.europa.eu/eli/reg/2019/881, (Last visited, October 12, 2022)

27）EU, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN, (Last visited, October 13, 2022)

28）European Parliament, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333, (Last visited, October 13, 2022)

29）ENISA,“Boosting your Organisation's Cyber Resilience - Joint Publication”https://www.enisa.europa.eu/publications/boosting-your-organisations-cyber-resilience, (Last visited, October 13, 2022)

30）内閣サイバーセキュリティセンター (NISC), https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021.pdf, (Last visited, October 13, 2022)

31）経済産業省 , https://www.meti.go.jp/press/2021/02/20220221003/20220221003-1.pdf, (Last visited, October 14, 2022)

32）カナダのサイバーセキュリティ戦略は2018年のものである。

33）Viasat, https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview, (Last visited, October 14, 2022)

34）UK.Gov, https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion, (Last visited, October 14, 2022)

35）Microsoft“Special Report: Ukraine”（2022年4月27日発行）、https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd, (Last visited, October 14, 2022)

36）White House, https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/02/24/remarks-by-president-biden-on-russias-unprovoked-and-unjustified-attack-on-ukraine/, (Last visited, October 14, 2022)

37）CISA, https://www.cisa.gov/shields-up, (Last visited, October 14, 2022)

38）White House, https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/, (Last visited, October 14, 2022)

39）White House, https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/fact-sheet-act-now-to-protect-against-potential-cyberattacks/, (Last visited, October 14, 2022)
40）White House, https://www.whitehouse.gov/briefing-room/press-briefings/2022/03/21/press-briefing-by-press-secretary-jen-psaki-and-deputy-nsa-for-cyber-and-emerging-technologies-anne-neuberger-march-21-2022/, (Last visited, October 14, 2022)
41）CISA, https://www.cisa.gov/uscert/ncas/alerts/aa22-076a, (Last visited, October 16, 2022)
42）NCSC, https://www.ncsc.gov.uk/news/organisations-urged-to-bolster-defences, (Last visited, October 16, 2022)
43）CCCS, https://www.cyber.gc.ca/en/news-events/joint-cyber-security-advisory-russian-state-sponsored-and-criminal-cyber-threats-critical, (Last visited, October 16, 2022)
44）NCSC, https://www.ncsc.gov.uk/news/uk-joins-international-partners-to-issue-advice-on-latest-russian-cyber-threat-, (Last visited, October 16, 2022)
45）CISA, https://www.cisa.gov/uscert/ncas/alerts/aa22-110a, (Last visited, October 16, 2022)
46）NCSC, https://www.ncsc.gov.uk/blog-post/preparing-the-long-haul-the-cyber-threat-from-russia, (Last visited, October 16, 2022)
47）EU, https://presidence-francaise.consilium.europa.eu/en/news/member-states-united-in-supporting-ukraine-and-strengthening-the-eu-s-telecommunications-and-cybersecurity-resilience/, (Last visited, October 16, 2022)
48）Bundesamt für Sicherheit in der Informationstechnik (BSI), https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220225_Angriff-Ukraine-Statement.html, (Last visited, October 16, 2022)
49）NISC, https://www.nisc.go.jp/pdf/press/20220324NISC_press.pdf, (Last visited, October 16, 2022)
50）国立国会図書館（NISC の web ページのアーカイブ）、https://warp.da.ndl.go.jp/info:ndljp/pid/12213293/www.nisc.go.jp/press/pdf/20220301NISC_press.pdf, (Last visited, October 16, 2022)
51）日経2022年3月7日記事, https://www.nikkei.com/article/DGXZQOCB07CGF0X00C22A3000000/, (Last visited, October 16, 2022)