日経・CSISバーチャル・シンクタンク
CSIS-NIKKEI VIRTUAL THINKTANK

潜伏型サイバー・テロに備えよ

―「信頼のインターネット」構築に向けて ―

2016年10月21日

土屋大洋　アカデミックアドバイザー
今泉宣親　清水丈司　持永大　ほか
第3期サイバーセキュリティー研究チーム

エグゼクティブサマリー

サイバー空間に対する脅威は主体が個人的な愉快犯から国家や犯罪組織などに変わるとともに、攻撃手法も侵入を悟られずに水面下で進む「潜伏型サイバー・テロ」にシフトしつつある。その特徴はシステムへの侵入・潜伏・攻撃準備の各段階において探知が極めて難しく、ひとたび攻撃が顕在化すると金融・運輸・通信・エネルギーなど社会基盤を構成するシステムが広範かつ甚大な被害を受ける恐れが高いことにある。ＩｏＴ時代が本格化するなかで、「潜伏型サイバー・テロ」に万全の備えをしておくことが死活的な重要性をもつという問題意識から、日経･ＣＳＩＳバーチャル･シンクタンクのサイバーセキュリティー研究チームでは、政府および産業界に対して以下の７点を提言する。

提言１：潜伏型サイバー・テロは侵入・潜伏されること自体を問題視するのではなく、攻撃の存在を検知し、適切な対策をとることに焦点を当て、この目標に向かって官民が高度な連携を図るべきである。

提言２：すべての対策の前提になる企業の自助努力を促すため、政府は企業統治に関する規制の中に、サイバーセキュリティーへの配慮を欠いた経営者への責任明確化や最高情報セキュリティー責任者（CISO）の経営参画などを盛り込むべきである。

提言３：情報通信業界と金融業界が確立したサイバー攻撃に関する情報共有・分析の仕組み「ＩＳＡＣ」を他の業界でも早期に確立・発展させるため、政府・所管官庁は必要な支援を提供すべきである。さらに、業界横断的な対サイバー･テロ統合連携プラットフォームの構築も政府主導で進めることが必要である。

提言４： 重要インフラのサービス停止などが発生した場合、サイバー攻撃の可能性を常に念頭に置き、同種の事業を行う企業、監督官庁、内閣サイバーセキュリティセンター（ＮＩＳＣ）をはじめとする複数の政府機関で即時の情報共有を義務付け、国家安全保障会議（ＮＳＣ）の開催を含む迅速な初動対応を行えるような態勢を整備すべきである。

提言５：ひとたびサイバー・テロが発生すれば国民の生命や社会・経済生活に甚大な影響が生じかねない状況が生まれていることに鑑み、攻撃者が使用するコンピューターへのアクセスなどサイバー攻撃者に関するより深い情報収集を可能とするための法制を

検討すべきである。

提言６：国としてサイバー空間に関する分析能力を保持し、維持・強化していくため、政府は今後、大学・研究機関、セキュリティー関連企業の知見を集積する学際的研究拠点を整備し、その成果を様々な主体が利用できるよう検討すべきである。

提言７：２０２０年の東京五輪・パラリンピックまでに、潜伏型サイバー攻撃の防御につながる官民の高度な連携体制を確立するとともに、攻撃者の特定を可能とする法制の整備を目指して国会などでの議論を進めるべきである。

水面下で進む潜伏型サイバー・テロ

サイバー空間は我が国の社会・経済の重要な基盤であり、この安全確保は国益を守る上で欠かせない。情報通信、金融、電力などの重要インフラストラクチャーサービスはサイバー空間を構成し、市民生活と密接な関係を持つ経済基盤として活用されている。すなわち、サイバー空間の安全性と信頼性を確保し、安定的に運用することは信頼性の高いサイバー空間を確立するとともに我が国の国益確保においても重要である。

サイバー空間の重要性が高まるにつれて、その脅威は変化している。その脅威は、主体が個人的な愉快犯から国家や組織に変わるとともに、攻撃手法が侵入を悟られずに水面下で進む「潜伏型サイバー・テロ」にシフトしていく。

従来の物理的なテロであれば、攻撃が行われた瞬間に被害が見える。それに対し、潜伏型サイバー・テロは、コンピュータシステム内に長期間にわたって潜伏・影響をおよぼし、多大な被害をもたらすサイバー攻撃を利用したテロリズムであり、その特徴はシステムへの侵入・潜伏・攻撃準備の段階において探知をすることが難しく、影響を受けている期間、影響の範囲、今後起きる被害の大きさの予測が難しいことである。

今後は脅威の検知が難しく、水面下で活動する潜伏型サイバー・テロの脅威が顕在化する。これまで長い準備期間を経た時限式のマルウェアによる被害として潜伏型サイバー・テロは発生しており、2013 年に韓国では周到な準備期間を経て銀行・放送局の 6 組織が同時に攻撃を受け、利用しているシステムが停止した結果、銀行 ATM やモバイル決済が行えなくなった。また、セキュリティー関連企業の調査によれば 2015 年以降、日本を標的にしたサイバー攻撃により発電、石油・天然ガス、輸送、金融等の企業ネットワークに攻撃者が既に侵入していると報告されている[1]。そのため、我が国でも重要インフラストラクチャーシステムへの潜伏型サイバー・テロの準備が人知れず進んでいる可能性がある。

潜伏型サイバー・テロは「いつから」「どこまで」「何を標的として」攻撃されているかがわからない。また、これらの脅威は検知が難しいだけではなく、攻撃の時間単位、被害の影響範囲も従来とは異なる。そのため、複数の重要インフラストラクチャーに対して同時に潜伏型サイバー・テロを仕掛けることで、我が国の事業継続性を著しく低下させることができる。

潜伏型サイバー・テロに備え、日本の経済基盤であるサイバー空間を守るためには民間

---

[1] ジョン・グロスおよび Cylance SPEAR チーム「砂嵐大作戦（Operation Dust Storm）」Cylance <https://www.cylance.com/hubfs/2015_cylance_website/assets/pdf/Op-Dust-Storm_JAPANESE_FINAL_1.pdf?t=1467901683326>、2016 年。

事業者の対策、政府の支援、両者の連携が欠かせない。国際的に活用されるボーダレスなサイバー空間の運営主体は民間企業である。そのため、サイバー空間を構成する民間企業はセキュリティーの確保、事業継続性、およびコストのバランスのもとで最大限の対策を講ずることとなる。一方、政府は潜伏型サイバー・テロをはじめとする脅威に備えて、我が国の経済基盤を守る態勢を整備する必要があるが、サイバー空間において政府単体では影響力を行使できないという課題がある。

そこで、潜伏型サイバー・テロに対抗し、我が国の社会・経済の基盤となる官・民の事業継続性を確保するための連携・支援を行う等、官民連携の一段の高度化が必要である。特に今後は民間と官の連携を通じて官民の業務継続の支援、情報共有の高度化、分析力の向上を高度化することが不可欠である。

1. 民間事業者が構成するサイバー空間

1.1. 事業継続の後押し

重要インフラストラクチャーと位置づけられる民間事業者のシステムをサイバー攻撃から防御し、事業の継続性を確保することは、国家の安全保障、危機管理上も見過ごすことのできない課題となっている。それは、一義的には各民間事業者の責任と判断の下、取り組むべきものである（「自助」）。しかしながら、サイバーセキュリティー対策は、およそ目下の収益上の効果が期待できるものではないため、通常の投資のようにベネフィットとの関係でコストを決めることが容易ではない。特に、潜伏型サイバー・テロに対しては、意識が低く、対策が未熟であればあるほど、侵入・潜伏の検知が困難となり、結果として対策の必要性を認識しなくなるという負の循環が生じる傾向にある。

したがって、民間事業者間で連携・協力することで意識の醸成と負担の共有を図っていくこと（「共助」）、短期的な収益追求ではなく潜伏型サイバー・テロにより中長期的に収益が蝕まれていくのを防ぐ観点から、経営層がサイバーセキュリティー対策は重要な責務であると認識することが重要であり、このために政府が果たすべき役割は小さくない（「公助」）。

これまでも政府は、重要インフラをはじめとする民間事業者のサイバーセキュリティーにつき、サイバーセキュリティ基本法第 13 条において「基準の策定、演習及び訓練、情報の共有その他の自主的な取組の促進その他の必要な施策を講ずる」こととして、内閣サイバーセキュリティセンター（NISC）や各事業所管省庁が、それぞれの所掌に応じた施策に取り組んできた。

しかし、依然、我が国民間事業者によるサイバーセキュリティー投資は、グローバルに

見て小規模に留まっているといわれる[2]ほか、経営者がセキュリティー対策に対して十分なリーダーシップを発揮していない点が大きな課題として指摘されている[3]。

1.2. 企業統治の再考

サイバーセキュリティー対策は損益の観点からはコストとして認識されるため、民間事業者に自主的な取組みを促していくことは容易ではない。しかしながら、事業の中長期的な持続可能性の視点からは、潜伏型サイバー・テロにより収益基盤が蝕まれたり、ある日突然破壊されたりする事態へ備えることは無視できるものではない。例えば、職場の安全衛生管理と同様、短期的にはコストであっても、企業が事業を継続していく上で不可欠となる投資といえる。

ただし、サイバーセキュリティーの困難さは、法令違反や事務ミス、システムの安定稼動などの内部向けの対応と異なり、悪意ある攻撃者の存在や攻撃側の進化の早さを踏まえた外部向けの対応が求められる点にある。特に、潜伏型サイバー・テロは、対策が未熟であると却って攻撃を検知できず、企業が自らの対策に満足しかねない。

したがって、サイバーセキュリティーについては潜伏型サイバー・テロの存在を前提として、侵入・潜伏されること自体が問題なのではなく、これらを適切に検知する能力を身につけ、検知した際に対策を取れることが必要であり、これらができていない企業は経営の持続可能性に必要な投資を怠っている、ということが企業の経営層の共通認識とならなければならない。

このため、政府は、企業統治に関する規制（各種自主規制を含む各業法における監督や会社法制など）の中に、以下の考え方を盛り込むことを検討すべきである。

- サイバーセキュリティーへの配慮を欠いた企業経営者（CEO）の責任の明確化（情報システムの開発・整備におけるセキュリティーへの配慮の欠如を含む）
- 実行能力（自社のビジネスとサイバーセキュリティーについての理解を兼備）を有するセキュリティーに関する最高責任者 CISO（Chief Information Security Officer）の経営への参画
- サイバーセキュリティーの取組み状況についての外部への開示・報告

---

[2] PwC「グローバル情報セキュリティ調査 2015」<http://www.pwc.com/jp/ja/advisory/research-insights-report/assets/pdf/information-security-survey2015.pdf>、37 頁、図表 12。

[3] 経済産業省「サイバーセキュリティー経営ガイドライン Ver 1.0」<http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf>、2015 年 12 月 28 日、1 頁。

2. 情報共有の高度化

2.1. 民間事業者間での情報共有

民間事業者の取組みの向上には、各事業者の「自助」だけではなく、民間事業者同士が連携・協力する「共助」が非常に有効となる。この問題意識から、ICT 業界や金融業界等は、ISAC（Information Sharing and Analysis Center）と呼ばれる情報共有・分析機関を立ち上げた。ISAC では、ある事業者が受けた攻撃手法を共有することで他の事業者が防御策を講じたり、取組みの遅れている事業者に進んでいる事業者からノウハウを移転したりすることで、リソースシェアリングとノウハウシェアリングが進められている。

これらの枠組みは、同種の事業を行う事業者間では、類似した攻撃が予想されることからは十分に効果が期待できる。他方で、侵入を悟られないように進められる潜伏型サイバー・テロでは、各事業者自身のシステムへの直接の侵入だけではなく、サプライチェーンや利用するインフラ基盤を経由した攻撃にも目を向けていくことが必要となる。また、昨年の日本年金機構の事案においては他の複数の組織で類似の攻撃があったと指摘されるように、業種・業界を問わず同時多発的に攻撃が行われることも少なくないため、他業界で発生している事例を迅速に把握し、水面下で進む攻撃を未然に察知する必要性も高まっている。

このため、情報共有・分析は、将来的には業界の垣根を越えた分野横断的なものへと進化していくことが必要となる。ただし、既存の ISAC の中で、各社が自社にとって外部に出しがたいネガティブ情報を競合他社と共有できている大きな要因として、参加者相互の信頼性（顔の見える関係）の存在が指摘されている。これを踏まえると、広範な単一の枠組みを設けて、異業種の企業が直接共有する仕組みを講じたとしても直ちに効果を発揮できるか疑問である。

そこで、分野横断的な情報共有・分析の枠組みとしては、各 ISAC の間で、信頼関係の醸成を計り、相互連携を進めていくことで、各 ISAC をハブとして業界横断的にリソースシェアとノウハウシェアが図られるネットワークを形成していくことが早道と考えられる。

この前提として、ICT 業界や金融業界に留まらず、その他の業界においても、所管省庁のリーダーシップの下、実際に機能する ISAC を設置することが必要となる。さらに、ISAC 間での相互連携を進めるのに合わせて、それぞれの所管省庁の間でも NISC を交えて、各業界におけるサイバーセキュリティー上の課題を日常的に共有するチャネルを形成していくことが求められる。

2.2. 平時の情報共有の高度化

平時の業界横断的な情報集約・共有の具体策として、政府や既存組織の情報収集・共有の仕組みを活用し、各組織で分散的に収集しているインシデント情報（予兆やヒヤリハットを含む）を迅速かつ統一的に共有する対サイバー・テロ統合連携プラットフォームを政府主導で設けるべきである。そして、インシデント発生状況を広域に俯瞰し、複眼的な分析を通じて、潜在的なテロの脅威を抽出する機能を強化する。

このプラットフォームは、潜伏型サイバー・テロの「防止」と「抑止」の双方の観点から重要である。「防止の観点」については、例えば、半年後に発生するように計画された大規模 IT 障害や複数業界の重要インフラストラクチャーへの同時多発攻撃といった潜在的なテロの脅威について、業界を越えて予兆を含めた脅威情報を網羅的に収集・共有することにより、潜在的脅威に対する検知能力を日本全体で高めることである。また、集約され分析された脅威情報とリスク軽減に向けた対応アプローチについては、同プラットフォームを通じて各業界の民間企業等に迅速にフィードバックされ、リスクの顕在化防止に寄与することになる。

「抑止の観点」については、潜伏型サイバー・テロの検知能力が相対的に脆弱な民間企業等を狙った攻撃においても、予兆や懸念情報の同プラットフォームへの報告により日本政府も状況を把握する仕組みとなることから、リスク対策上のボトルネックを減らすと共に、攻撃主体に対する牽制としても有効である。これらの相乗効果として、潜伏型サイバー・テロに対する国家の防衛態勢強化が促進される。

平時における情報共有態勢を構築・運用していくためには、第一ステップとして、既存組織における本案の意義に対する理解を得て協力に向けた合意形成を図ることが重要となる。第二ステップは、各組織における情報収集基準・プロセスのレビューを行い、統一化に向けたポイントの洗い出しを行う。第三ステップは同プラットフォームへの報告基準・プロセス・統一報告フォーム等の整備となるが、潜伏型サイバー・テロの特性を鑑み、特に重要インフラストラクチャーに関係する予兆やヒヤリハットも含めることが適切であり、簡便な仕組みを構築することが重要である。そして、第四ステップとして、同プラットフォームの運用となるが、「オンライン・データベース」の構築も一案であり、政府機関や各組織が各々付与された権限の範囲の情報にアクセスすることも想定される。その場合、各組織が報告する情報の共有範囲、機密保持態勢、管理責任等に関する事前の協議・調整が必要になり、重層的な不正アクセス対策も必須となる。最後に、本案の運用に対する監督モニタリング・評価等を経て、改善を図りながら高水準の運用性を担保することを目指す。

2.3. サイバー・テロ発生時の情報共有

サイバー・テロにより生じる現象として、例えば、テレビ局の放送が停止する、銀行 ATM が使用できなくなる、航空会社のシステムが停止して運行できなくなる、といったものが想定されるが、こうした事態が発生した場合、これがサイバー攻撃によるものであるのか、システム障害によるものであるのか判断するためには、一定の時間を要するものと思われる。一方、こうした原因究明の結果を待ち、その間他の事業者等との情報共有を行わないでいたとすると、実際にはその事態がサイバー攻撃に起因するものであり、複数の事業者において同様の事態が発生していたとしても、他の事業者は警戒・対処する機会を失ったまま、被害が拡大し続けてしまうおそれがある。

サイバー攻撃に対して迅速に対処し、被害拡大を防止するためには、重要インフラストラクチャーにおけるサービスの停止等が発生した場合において、サイバー攻撃の可能性を常に念頭に置きつつ、速やかに関係者との情報共有を図る必要がある。具体的には、こうしたサービス停止等が発生した場合には、同種の事業を行う事業者や、監督官庁、内閣サイバーセキュリティセンター（NISC）を始めとする複数の政府機関間で即時の情報共有を行うことを義務付けるほか、事態の規模や程度によっては安全保障上の問題となり得ることを念頭に、国家安全保障会議（NSC）の開催を含む迅速な初動対応を行うことを可能とするための幅広い情報共有態勢を構築するべきである。また、官民各組織で行われた情勢的・技術的分析を持ち寄り、より総合的な分析を行うため、NISC、NSC 等の機関に対し、各組織の専門家を招集してアドホックなチームを生成することを可能とする権限を付与することも重要である。

3. 集約した情報を活かす分析能力

3.1. 情報収集能力の強化

サイバー・テロが行われた場合、攻撃を行った主体を可能な限り特定し、攻撃者の公表、訴追や攻撃者への圧力、反撃等、あらゆる手段により攻撃をやめさせるための対応をとる必要がある。さもなくば、被害に遭った事業者等が一定の防御策をとったとしても、攻撃者は新たな手法により攻撃を継続し、又は防御策がとられていない他の事業者等に対して攻撃を行うなどして、被害が拡大し続けることも想定される。

そうした観点から、攻撃主体の特定に向けた情報収集は極めて重要であるが、現状では被害者側のサーバや端末を調査し、ログやマルウェアの解析等を行うことしかできないため、一般的には、攻撃者の使用するインフラストラクチャー（C&C サーバ等）や攻撃主体の特徴（使用言語等）といった外形的な性質を把握することまでしかできない。他方、そ

れ以上に深い情報を獲得し、正に攻撃を行った個人・組織まで特定するためには、攻撃者の使用するコンピューターに侵入し、記録されたデータの取得や攻撃者の通信内容を確認するなどの必要があるが、現行法上、こうした行為は我が国の刑法（いわゆるマルウェア作成・供用罪等）や不正アクセス禁止法等に違反するものと評価される可能性が高い。しかしながら、分析能力を高める前提として、情報収集能力の強化が欠かせない。

現行法は、一般的な犯罪の防止を目的とすることはもちろんであるが、プライバシーや通信の秘密の保護を極めて重視する考え方の下、制定されたものとなっている。一方、現行法は、サイバー攻撃が安全保障上の脅威となるにまで至っている中、こうしたサイバー攻撃を行う者の特定までも禁ずることを念頭に置いて制定されたものではないと思われる。現在、ひとたびサイバー・テロが発生すれば、国民の生命や社会・経済生活に甚大な影響が生じかねない状況にまでなったことにかんがみれば、現行法上の保護法益との均衡も考慮しつつ、サイバー攻撃者に関するより深い情報を収集するための法制を検討すべきである。具体的には、攻撃者が使用するコンピューターへのアクセスや、攻撃者が使用するコンピューターから情報を得るためのプログラムの作成・使用、攻撃者が行う通信の傍受等について、一定の要件・手続の下で行われることを前提とした上で許容することが必要である。無論、行き過ぎを防ぐための監査制度も合わせて作るべきである。

3.2. 多様な知見の蓄積

サイバー空間に関する分析能力を保有し、維持・強化するためには、継続的に知見を蓄積する必要がある。前述のとおり、サイバー空間から収集する情報を適切に分析するためには、サイバー攻撃に関する膨大な断片情報を総合するとともに、技術、政策、社会制度、人間行動等、実空間における多様な知見を活用する必要があるが、このような多様な知見を活用した分析は容易に行うことができるものではない。そのため、国は、今後、サイバー攻撃に係る適時適切な分析を行うための態勢を整備する必要がある。具体的には、NISC等を中心に、人間行動や社会制度について知見を持つ大学・研究機関、そしてIT技術に関する分析の知見を有するセキュリティー関連企業について、それぞれの知見を集積する学際的研究拠点を整備し、その上で、一定のクリアランスの下、様々なユーザーが当該学際的研究拠点を使用可能となるよう維持することが望ましい。

3.3. 多層的な分析能力の確保

集約されるサイバー攻撃に関する情報は膨大な量になる可能性がある。サイバー攻撃は、個人による犯罪からテロリスト・国家機関による組織的な攻撃まで様々であるが、その分析にあたっては、(1) タイムリーに分析・プロダクト化を行う必要がある場合と、(2) サ

イバー攻撃に関する膨大な断片情報を総合し、実空間における彼らの活動等も踏まえつつ、目的・主体・手法等について詳細な分析を行う必要がある場合の 2 パターンが存在し、ユーザーのニーズや事態の様相に応じ柔軟に使い分けていくことが重要である。特に、サイバー攻撃の主体を特定することは、さまざまな観点から困難であることが指摘されているが、今後、他の情報収集能力との連携やメタデータ分析[4]、ダイヤモンド・モデル[5]の活用を通じて分析能力を高め、このような困難を克服していく努力が不可欠である。

サイバー空間から収集する情報は、広範囲なユーザーが様々な切り口から分析を加えることが可能であり、分析に必要となるスキルも様々である。したがって、サイバー空間から収集する情報については、単一の機関が一元的に分析能力をストックするのではなく、官民問わず各ユーザーがそれぞれの目的に応じた分析能力をカスタマイズして保有することが重要である。戦術的（技術的）レベル、作戦術的レベル、戦略的レベルにおける多層的な分析能力の確保が必要である[6]。

4. 信頼のインターネットへ

潜伏型サイバー・テロは将来の話ではない。すでにその準備は行われていると想定すべきである。瞬間的に多大な被害をもたらすテロと違い、その存在に気づくことすら難しい、しかしながら、潜伏型とはいえ、それは瞬間的に巨大な破壊をもたらすものに転じたり、長期にわたって低強度のダメージを加えたりするものでもあり得る。

確実に存在すると分かっているものを探すことは比較的容易である。しかし、どこにあるか、どんなものかも分からない脅威を探し、未然に除去するのは困難である。そして、「IoT（Internet of Things）」といわれるように、多種多様なモノが大量につながる時代に入ると、それは「脅威のインターネット（Internet of Threats）」にもなりかねない。相互接続されたネットワーク機器の部品一つ一つ、プログラムの一行一行にさかのぼって脅威を特定することは困難であるにもかかわらず、いったん発症したコンピューター・ウイルスはネットワークを通じて急速に広がり、システム、プラント、インフラストラクチャー、そして社会全体を麻痺させることすらあるかもしれない。

---

[4] 情報の「中身」（例：メール本文）ではなく「属性」（例・メールの宛先・IP アドレス）を収集し相関関係等を分析する手法。多数の情報が氾濫するインターネット上においては、「中身」を一つ一つ分析するコンテンツ分析よりも迅速かつ適切な手法と考えられている。

[5] 米国で主流となっている攻撃源探知のための分析手法。敵対者・被害者・攻撃使用ツール・技術の 4 要素について総合的に分析していくことで攻撃源を推定していくもの。

[6] トマス・リッド、ベン・ブキャナン（土屋大洋訳）「サイバー攻撃を行うのは誰か」『戦略研究』第 18 号、2016 年 5 月、59～98 頁。

潜伏型サイバー・テロの脅威は将来にわたって増大するのが確実だが、とりわけ日本が攻撃のターゲットとなりうるのが 2020 年東京五輪・パラリンピックである。

2012 年のロンドン大会では、数え方にもよるが、2 億件のサイバー攻撃が行われたとされる。4 年後の 2016 年のリオデジャネイロ五輪では、ロンドン大会の 2 倍の IT セキュリティー事象が発生したとされる。ブラジルは元々サイバー攻撃が多発している国であるが、五輪開催期間中はサイバー攻撃発生件数が通常時に比べ約 3 倍に増加し、DDoS 攻撃に関しては通常の 4.3 倍に達したとの情報もある。東京大会ではさらに多くの高度な攻撃を受けると想定すべきだろう。

サイバー攻撃を行う者は常に有利な立場にある。特にオリンピック・パラリンピックのようなイベントに合わせた潜伏型サイバー・テロを計画する場合、与えたい被害から逆算して様々な手法を用意することが可能である。また、サイバー攻撃によりセキュリティー計画等が窃取された場合、物理的なテロ攻撃の発生に繋がる恐れもある。一方、防御側は「いつから」「どこまで」「何を標的として」攻撃されているかがわからない状況と様々な可能性をもとに対策を講じなければならない。さらに、防御側は被害を最小限に抑え、時々刻々と変化する技術を含めた状況に対応する必要がある。従って、潜伏型サイバー・テロの防止のためには準備や計画に加え、変化に対応できる態勢を整備する必要がある。

ロンドン五輪で深刻な被害が発生しなかったのは、英国政府が策定した包括的な戦略的リスク評価結果に基づき、通信事業者を含む官民を中心とした重要な利害関係者が機動的な連携プラットフォームを早期に確立し、網羅的な対策を構築・実践したこと、そしてサイバー攻撃からの回復力を担保・保障するための危機管理を徹底したことが背景にある。リオデジャネイロ五輪においても、先端技術と既存の情報収集・分析機能を有機的に結びつけた官民連携態勢を構築し、プロアクティブかつ即応性の高い防御を実現させたことが奏功したためだと考えられる。日本も東京五輪・パラリンピックに向けて政府、企業、個人が連携できる態勢を整備し、大会運営を乗り切ることを目指し行動する時だ。

そのうえで、本提言で提唱したＩＳＡＣと業界横断的な対サイバー・テロ統合連携プラットフォームの構築、および攻撃者が使用するコンピューターへのアクセスなどサイバー攻撃者の特定に向けた情報収集を可能にする法制の確立の 2 点については、2020 年までの実現を目標とすべきである。後者については国会の議論を通じた国民の理解の深まりが必要不可欠であり、時間的な制約から実現が難しいと判断される場合は五輪期間中に限定した「特別措置法」の導入も検討対象とすべきだろう。

以上のような行動をとることでリスクをチャンスに変えることができれば、東京五

輪・パラリンピックを一つの画期として潜伏型サイバー・テロに対する日本のレジリエンスは大幅に高まることが期待できる。

ただ、2020 年の東京オリンピックは通過点に過ぎない。潜伏型サイバー・テロと、それが転じた爆発的サイバー・テロのリスクはその後も形を変えながら日本社会を脅かし続けるだろう。脅威のインターネットを「信頼のインターネット(Internet of Trusts)」へと変えていく不断の努力が我々に求められている。