2022 年 7 月

シリーズ 「日本のサイバーセキュリティ政策史」

誰も取り残さない「サイバーセキュリティ戦略」実現に向けた政府の決意

【概要】
サイバーセキュリティ政策分野に詳しい三角育生氏が日本の同政策史をひもとくシリーズ。初回は、最新の「サイバーセキュリティ戦略」策定において中核を担った内閣サイバーセキュリティセンター（NISC）副センター長の吉川審議官をお迎えし、話をうかがいます。いまやあらゆる人がサイバー空間に参画する時代。戦略に込められた、サイバーセキュリティ確保のために推進する施策の内容・意図および根底にある理念、そして政府の決意とは。

【出席者】

吉川 徹志氏
内閣サイバーセキュリティセンター（NISC）
副センター長 内閣審議官

聞き手：
三角 育生氏
東海大学情報通信学部長・教授

戦略策定の背景──デジタル社会の到来

三角 本日（2022 年 4 月 27 日）は、最新の日本のサイバーセキュリティ政策の基礎となる 2021 年9月に閣議決定された「サイバーセキュリティ戦略」（以下「戦略 2021」という）について取り上げたいと思います。「戦略 2021」の策定において中核を担った吉川審議官に、その策定経緯・背景、哲学、主要な方針等についてお聞きします。

一つ前の戦略（以下「戦略 2018」という）が 2018 年 7 月に閣議決定されて以降、日本の経済社会をめぐってさまざまな出来事がありました。2020 年東京オリンピック・パラリンピック競技大会（以下「オリパラ」という）開

催、新型コロナウイルス（COVID-19）の蔓延に伴うリモートワーク等で加速されたともいわれるデジタルトランスフォーメーション（DX: デジタル化による変革）の急速な進展、デジタル庁設置等日本におけるデジタル政策の強力な推進、そして米中関係をはじめ国際情勢の変化等です。こうした社会情勢の変化は、「戦略 2021」の策定過程でどのような影響を及ぼしたのでしょうか。

吉川 ご指摘いただいたような情勢変化を踏まえ、2020 年代を迎えた日本を取り巻く時代認識「ニューノーマル（新たな常態）の出現とデジタル社会の到来」を足がかりに、政策の基となるサイバー空間をとりまく課題認識を議論しました。

まず脅威の観点です。デジタル改革が進む中で、新たなデジタルサービスが次々と生み出され、人々の生活に浸透していくということは、自らの生命、身体、財産に関わる情報等をこれまで以上にサイバー空間の場に委ねることを意味します。これらのデータは今後いっそう、攻撃者にとって、サイバー攻撃の対象となる誘因性が増すこととなります。また、攻撃手法も多様に変化・高度化し、技術革新の果実を攻撃側が活用することで、脅威が拡大する可能性も考えられます。

もう一つは、日本の経済社会が抱える脆弱性の観点です。DX の進展により、これまでサイバー空間とは繋がりのなかったさまざまな業種・業態の企業や、若年層・高齢者を含めた個人までもが不可避的にサイバー空間に参画することとなります。サイバーセキュリティに関するリテラシーの差異や人材不足・偏在等が、攻撃者に狙われる弱点となる可能性があります。また、技術の進展によってクラウドサービスの利用、グローバルなサプライチェーン、あらゆるモノがネットワークにつながる「IoT」機器の利用等の拡大により、インシデントが発生した場合の経済社会活動への影響は、より広範に、多様な主体・場面に及ぶおそれがあります。

加えて、国際情勢からみたリスクの観点です。サイバー空間は平素から、地政学的緊張を反映した国家間の競争の場の一部ともなっています。重要インフラの機能停止、国民情報や知的財産の窃取、民主プロセスへの干渉等国家の関与が疑われるものをはじめとする組織化・洗練化されたサイバー攻撃の脅威が増大しています。サイバー空間をめぐる情勢は、有事とはいえないまでも、もはや純然たる平時ともいえない様相を呈しています。

このような課題認識に基づいて、政策を 2018 年の段階から見直す作業に取り組みました。

海外の国家の関与が疑われる攻撃の実態

三角 2021 年 5 月、米石油製品パイプライン最大手コロニアル・パイプライン（CP）社の情報システムがサイバー攻撃を受けて、その結果、一時石油の供給停止を余儀なくされました。こうした他国の事例等も考慮されたのでしょうか。

吉川 2021 年 1 月のジョー・バイデン政権発足前後に米国で大きな事件がありました。2020 年末、米政府機関や企業の多くが使っているソーラーウインズ社のネットワーク管理ソフトの更新プログラムにマルウェアが仕込まれました。最大で 1 万 8,000 組織が影響を受けたと聞いています。CP 社の事案も石油製品の供給が1週間停止されました。

また、このようなサイバー攻撃が経済社会に大きな影響を与えた事例を踏まえて、バイデン大統領は 2021 年 5 月 12 日に大統領令「国家サイバーセキュリティの強化」に署名し、サイバー防衛力の大幅な強化策を打ち

立てました。従来の重要インフラそのものだけでなく、それを支えるサイバー関連事業者、ソフトウエア等の産業、あるいはシステムの運営・管理を代行する事業者「マネージドサービス・プロバイダ（MSP）」のセキュリティ強化も謳われています。「戦略 2021」においても、それらを新たなドメインとして取り入れました。

一方、海外からの国家の関与が疑われる日本に対するサイバー攻撃も顕在化しています。それらに対して日本は、パブリックアトリビューション（サイバー攻撃の実行者の公表）、刑事訴追等で対応しています。例えば、2017 年 12 月、北朝鮮が関与したとみられる身代金を要求するマルウェア「Wannacry（ワナクライ）」を使ったサイバー攻撃、また 2021 年 7 月、中国政府と関係のあるグループ「APT40」によるサイバー攻撃等について、外務報道官談話等でパブリックアトリビューションを行いました。また、2021 年 4 月、警視庁がサイバー攻撃に使われたサーバーを契約していた中国共産党員 2 人を東京地方検察庁に書類送致しました。

国一丸での対応へ

三角　米国の状況等も踏まえ、日本における脅威を考慮して戦略を策定されたということですね。いま言及された新たなドメインには何が含まれるのでしょうか。

吉川　サイバーセキュリティ上守るべき重要なドメインとして、サイバーセキュリティ基本法（以下「基本法」という）において政府機関や重要インフラ事業者等のシステムを位置づけています。後者については、重要インフラに関わる各主体がそれぞれ責務を果たすことを基本としつつ、官民一体で堅牢な重要インフラの実現に向けて取り組むこととしています。

それ以外に、「戦略 2021」では新たにサイバー関連事業者、そして重要技術を保有する主体も重要ドメインとして位置づけ、今後政府として一元的に対応していくこととしています。

三角　新たな重要ドメインについての具体的な政策や担当省庁は決まっていますか。

吉川　いま「重要インフラの情報セキュリティ対策に係る第 4 次行動計画」（2017 年 4 月策定。以下「重要インフラに係る行動計画」という）の改定作業を進めています。今夏にも発表したいと考えていますが（注：2022 年 6 月 17 日にサイバーセキュリティ戦略本部が「重要インフラのサイバーセキュリティに係る行動計画」を決定）、その中で方向性の出るところもあります。また、それ以外のところも、「戦略 2021」を踏まえた対応について関係省庁と精力的に議論を進めているので、どこかのタイミングで打ち出せればと思っています。

三角　関係省庁との議論は従来から重要な点でした。私が情報セキュリティセンターおよび内閣サイバーセキュリティセンター（NISC）に在任していたのは 2012～20 年ですが、そのときも関係省庁間での認識共有に腐心しました。重要ドメインといえば、経済安全保障推進法が国会で議論されています（注：2022 年5月 11 日に成立）。同法は、サイバー脅威等も念頭に基幹インフラの役務の安定的な供給に関して重要設備導入時に審査すること等の規定が盛り込まれるようです。そういった一連の流れと符合して議論が進んできているということでしょうか。

吉川　そうですね。経済安全保障推進法とサイバーセキュリティ戦略とでカバーできることは多少重複します。サイバーセキュリティ戦略でカバーできないところを経済安全保障の体制で対応していくと思いますので、両者補完しながらやっていくのだろうと思います。

また、海外からの悪意を持った主体によるサイバー攻撃への対応強化は日本のサイバーセキュリティ政策の

一つのポイントです。そこに対していろいろなツールを使ってやっていくということだと思います。

関係省庁についていうと、2022 年 4 月に警察庁にサイバー警察局が新設され、体制を強化して取り組むとしています。「戦略 2021」でもそれに関して言及しています。各省庁が持ちうるツールを総動員して国として一丸となって対応していくモチベーションは、サイバー攻撃の米国の事例および日本の現状を踏まえて高まってきていると実感しています。

三角　ホール・オブ・ガバメント・アプローチ、つまり政府一体となって取り組む重要性が認識されて進められているということですね。

吉川　そうですね。2014 年 11 月に基本法が成立し、同法に基づいて翌年 1 月、内閣にサイバーセキュリティ戦略本部が設置され、同時に内閣官房に内閣サイバーセキュリティセンター（NISC）が設置されました。当初はそれぞれの関係省庁が自分の役割を考えながら進めてきたところ、そろそろ、それぞれが自らのおよび他の関係省庁の役割を認識して、大きな脅威に対してどういう風にリソースを共有しながら対応していくかを具体的に考え、調整できるようになってきたのだろうと思います。

三角　オリパラという大規模国際イベントのサイバーセキュリティ対策における役割分担、協力関係の調整等の経験も経ましたね。

吉川　そうですね。準備過程で構築されたオリパラのサイバーセキュリティ体制は「戦略 2021」にも活かされています。それまで国がサイバーセキュリティ上守るべき重要ドメインの対象としてこなかった主体に対するアプローチについて、一つの解を示し、海外でも高く評価されていると認識しています。それをしっかり受けとめて、新たなドメインへの対応に活かしたい思います。

戦略の哲学――Cybersecurity for All

三角　「戦略 2021」では、2020 年代を迎えた日本をとりまく時代認識「ニューノーマルとデジタル社会の到来」、サイバー空間に対する課題認識「国民全体のサイバー空間への参画」を踏まえて、「あらゆる主体にとってサイバーセキュリティの確保は自らの問題に」とし、「Cybersecurity for All～誰も取り残さないサイバーセキュリティ～」を主たるコンセプトとして掲げています。このコンセプトは政府や重要インフラ事業者だけではなくて、新たなドメイン、国民全体を含めて取り組んでいくことを意味するのでしょうか。

吉川　守るべき分野をカバーし、若年層、高齢者等新しく参画してくる主体に対応していくということです。

三角　従来、「全員参加による協働」でサイバーセキュリティに取り組むといわれてきました。その場合、for all ではなく by all のようにも思われます。for all としたのには意図がおありですか。

吉川　その意味での by all の重要さは変わっていません。「戦略 2021」でも「全員が自らの役割を主体的に自覚してサイバーセキュリティに取り組む」という考え方を for all の概念に含むことを明示しています。新たに参画してくる主体を守るとともに、自らの役割を主体的に自覚してサイバーセキュリティに取り組むこともあわせた形で for all という言葉を使っています。

三角　新たな参画者も含めてサイバー空間が安心・安全になるというイメージでしょうか。

吉川　おっしゃる通りかと思います。

経済社会の活力を高める施策

三角　そのコンセプト実現のために、今後展開していかれる具体的施策についてうかがいます。

各論の最初の柱に「経済社会の活力の向上及び持続的発展」が挙げられています。政府として DX に関わる政策を積極的に進める中で、DX の推進とあわせてサイバーセキュリティ確保に向けた取り組みを同時に推進する DX with cybersecurity のコンセプトが戦略文書として初めて示されました。DX による利便性等の向上とサイバーセキュリティの確保は、いわば、アクセルとブレーキのバランス問題のようにも思います。このコンセプトを通じて、誰に何を意識、理解、実行してほしいと考えているのでしょうか。

吉川　2021 年 9 月、デジタル庁が設置されました。これが日本の経済社会の DX を大きく推進する絶好の機会となっていると思います。そのためにもサイバー空間への信頼性が醸成され、DX への参加・コミットメントをしっかり得ていくことが大事です。

製品・サービスのデジタル化が進む中で、サイバーセキュリティ自体が企業価値に直結する営為になってきています。その意味で、「戦略 2021」を通して言及している「セキュリティ・バイ・デザイン」、すなわちサイバーセキュリティを業務、製品・サービス等のシステムの企画・設計段階から確保するという考え方はいっそう重要となり、デジタル投資とセキュリティ対策の一体性は増すと考えられます。それゆえ DX with cybersecurity があらゆる主体において意識され、取り組みが推進される必要があると考えます。

そのための具体的施策として進めるのが、第 1 に、経営層の意識改革です。DX with cybersecurity に向けた取り組み状況の可視化、あるいはそうした取り組みに対しインセンティブが生まれることが大事だと思っています。

第 2 に、取り残されがちな地域・中小企業における DX with cybersecurity の推進です。地域のコミュニティづくりにおける共助の促進や中小企業向けセキュリティサービスの充実等に取り組みます。

第 3 に、サイバー空間全体の信頼性確保に向けた基盤づくりです。新たな価値創出を支える「サプライチェーン」の信頼性を高める取り組み、例えば産業界主体のコンソーシアムの取り組みへの支援、重要な製品の安全性の検証。また、「データ流通」の信頼性確保の取り組み、例えば、信頼性のある自由なデータ流通（DFFT）、データマネジメント、トラストサービス等によるデータの信頼性確保等を行います。

その上で、誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着への取り組みが必要です。教育現場におけるデジタルの活用をサポートする仕組み、例えば GIGA スクール（児童生徒の一人一台端末と学校における高速大容量の通信ネットワークを一体的に整備する構想）、あるいは高齢者に対してのきめ細やかな取り組み、例えば携帯ショップを通じて相談しやすい環境をつくること等も含んでいます。こういった取り組みを含めて、全体での DX with cybersecurity を進めていきたいと考えています。

サイバーセキュリティは経営の重点事項

三角　DX with cybersecurity を推進する主体は企業等の組織を想定しているのでしょうか。それとも社会全体ですか。

吉川　両方です。目にみえる体制をつくって進めるという意味では企業が中心になるでしょうが、それを踏まえて社会全体が進めるということです。

三角　そのためにも、企業・組織内の DX 推進者が DX とサイバーセキュリティ対策を同時達成すべきであり、業務と収益の中核を支える基本事項であるという認識を持つことを重視されているのでしょうね。

吉川　先ほどの CP 社の事例もそうですが、日本においてもサイバーセキュリティへの対応が不足したことで、ビジネスチャンスを逃した、あるいは新サービスのローンチ後に頓挫して機会損益を招いた、といった事例が注目されてきています。特に経営者にはサイバーセキュリティ対策をコストとしてとらえるのではなく、おろそかにした場合の遺失利益や損失の大きさを考慮して投資することを促すことが重要だと思います。

三角　それについては経営層や DX 推進者に一歩踏み込んで訴求していく必要がありそうです。

吉川　先ほど紹介した「重要インフラに係る行動計画」の改訂においてそこを意識しています。

　また、NISC では「サイバーセキュリティ関係法令 Q＆A ハンドブック」をつくり、ウェブサイトで公開しています。経営層の責任については、「組織の意思決定機関が決定したサイバーセキュリティ体制が、当該組織の規模や業務内容に鑑みて適切でなかったために会社が保有する情報が漏えい、改ざん又は滅失（消失）若しくは毀損（破壊）されたことにより会社に損害が生じた場合、体制の決定に関与した経営層は、会社に対して、任務懈怠（けたい）に基づく損害賠償責任を問われ得る」と記述しています。サイバーセキュリティ投資を促すというよりも、経営者の内部組織体制の構築義務に絡むことを訴求し、今後、経営層の参考になるような具体的な方策を改訂版「重要インフラに係る行動計画」の関連規定等で明記していければと考えています。

三角　いま「重要インフラに係る行動計画」の改訂「案」が意見公募（パブリックコメント）のために NISC のウェブサイトで公開されています。経営層から現場まで、組織としてガバナンス体制をしっかりつくっていくという意思が読み取れました。

吉川　サイバーセキュリティは経営者だけの責任ではありません。重要インフラ事業者全体に対して、経営層、最高情報セキュリティ責任者（CISO）、また経営マネジメント層と「現場」をつなぐ分野、システム担当者を含めた組織全体での対応を促進していきたい。特に経営の重点事項としてサイバーセキュリティを取り込むことを明確にしていきたいと思っています。

安全安心なデジタル社会を実現する施策

三角　いま欧米を中心に多くの国が重要インフラのサイバーセキュリティ強化に取り組んでいます。日本も同様にいっそう強化していくということですね。

　そこで、各論の 2 つ目の柱「国民が安全で安心して暮らせるデジタル社会の実現」についてお聞きします。国民・社会を守るためのサイバーセキュリティ環境を提供するために、サプライチェーンやサイバー犯罪への対策等を行うことを示し、それにつづいて、デジタル庁を司令塔とするデジタル改革とサイバーセキュリティの確保、さらに政府機関等（国）・重要インフラ・大学・教育研究機関等の対策が示されています。この主体別の対策の順番については、従来は、国民・重要インフラ・国でした。今回、国が前に出てきているのは、より国が前面に出てやっていくという意思の表れでしょうか。

吉川　これまでのサイバーセキュリティの考え方である、自助・共助による自律的なリスクマネジメントは引き続き重要です。それが進むような環境づくりを国がやっていくということが基本です。国として重大なサイバーセキュリティ事案が発生した時にしっかり対応できるような仕組みを準備しておく。持ちうるすべての手段を活用して

包括的なサイバー防御を展開していく。サプライチェーンを含めてサイバー空間を俯瞰して、あらゆる主体の自助・共助・公助からなる多層的なサイバー防御体制を構築することが必要だと思っています。このように国全体のリスクの低減、レジリエンスの向上を図るために、国が主導的に取り組むということも「戦略 2021」で打ち出しました。

三角　多層的な防衛体制を構築していくとなると、それぞれの担当省庁がしっかりやっていかなくてはなりません。この点についても先ほど話題にした各省庁の役割やサイバーセキュリティの重要性が認識される中で話がまとまってきたと考えてよいでしょうか。

吉川　「包括的なサイバー防御の展開」の項目で、包括的なサイバー防御の総合的な調整を担うナショナルサート（CSIRT/CERT）機能等を強化することとしています。ナショナルサートとは、省庁のリソースを結集し、連携を強化していくということで、「情報収集・分析から、調査・評価、注意喚起の実施および対処と、その後の再発防止等の政策立案・措置にいたるまでの一連の取り組みを一体的に推進するための総合的な調整を担う機能」と位置づけられています。これは NISC だけでできるものではありません。NISC はナショナルサート機能のコーディネーションセンターとしてしっかり活動して、対処については各省庁の政策リソース等、用いうる手段すべてを活用した形での多動的なサイバー防御を構築していきたいと考えています。

三角　まさに政府一体でやろう、その時に NISC がナショナルサートのコーディネーションセンターとして機能するということを意思表示したということでしょうか。

吉川　そうですね。「戦略 2021」の重要な柱の一つだと思っています。

三角　ナショナルサートというと、例えばオリパラの時にインシデント情報等を収集し対処支援調整を行うサイバーセキュリティ対処調整センターという体制が設置されました。「戦略 2021」でいうナショナルサートはこうした個別の体制をいうのではなく、政府全体のコーディネーションセンターとしての機能を指すのですね。

吉川　そうですね。NISC は内閣官房として内閣の重要政策の企画立案・総合調整等を担う立場です。コーディネーションセンター機能を強化し、政府一体で多層的なサイバー防衛体制をつくるということを意味しているとご理解いただければと思います。NISC 自体、調整機能が発揮できるような体制強化をあわせて進めていこうと思っています。

三角　オリパラの時の NISC の経験は今後レガシーとしてどのように活かしていくのでしょうか。

吉川　オリパラでの調整機能の経験を活かした形は考えているところです。

また、2023 年に主要国首脳会議（G7 サミット）、2025 年に日本国際博覧会（大阪・関西万博）が日本で開催される予定です。大きな国際イベントはサイバー活動も活発になる傾向があるので、それに向けた体制強化においてもオリパラの経験が役立つと思っています。

さらに、今後、オリンピック・パラリンピックの夏季大会は 2024 年にフランスのパリ、2028 年に米国のロサンゼルスで、また冬季大会は 2026 年にイタリアのミラノ＆コルティナ・ダンペッツォで開催される予定です。そこで生かせるような形で日本の経験を伝えていければと思っています。いま申した国等とは既に、ウェブ会議の形式でコミュニケーションをとっているところです。

日本と世界の安全保障に寄与する施策

三角　各論の3つ目の柱で「国際社会の平和・安定及び我が国の安全保障への寄与」が挙げられています。

　総論で、国際情勢等からみたリスクとして中国、ロシア、北朝鮮への懸念を特記し、各論に安全保障のパートをおいて、サイバー攻撃に対する抑止力の向上に関し、パブリックアトリビューション等の外交的手段や刑事訴追等の手段も含め対応していくこと等を明記しています。ここは従来の戦略以上に強く記述しているように思われます。その背景についてお聞かせください。

吉川　脅威として具体的にみえてきたものについてはしっかり記述すべきだということです。日本に限らず世界各国の状況をみても、外国からの脅威は高まってきているので、総合的にということだと思います。ご指摘の通り、「戦略 2021」で外交安全保障上のサイバー分野の優先度をこれまで以上に高めるとしっかり記述したのもそういった背景です。

三角　ロシアによるウクライナへの侵攻や重要インフラへのサイバー攻撃に対する懸念、各国の政策動向等に対応していくためにも安全保障をしっかりやっていくことを強調されたということですか。

吉川　国際的な連携を求められる機会が増えてきています。2021 年 10 月 13・14 日、米国家安全保障会議主催のランサムウェア対策イニシアチブ（Counter-Ransomware Initiative: CRI）が開催され、30 カ国以上が参加しました。重要インフラを狙うランサムウェアへの対応を強化する必要があるということで、レジリエンスの向上、官民パートナシップ（PPP）、法的対応等の観点から議論が行われました。米国からはジェーク・サリバン大統領補佐官（国家安全保障担当）やアン・ニューバーガー国家安全保障担当副補佐官（サイバー・先端技術担当）が出席されました。日本からも私も含め政府関係者が議論に参加しています。こうした国際連携に向けた情報や課題の共有も引き続き行っていくことになっています。レジリエンスの向上、重要インフラの PPP、協働における法的対応については国際的な対応からも求められています。

三角　国際的な対応とは、情報や経験の共有等が中心になるのでしょうか。

吉川　いくつかアプローチはあると思います。事案への対処情報の共有や事案が起こる前のいわゆる脅威インテリジェンスの共有、また攻撃者に協働で対応することも含め、さまざまな協力の仕方があります。さらに、将来的には技術的なスタンダードについての議論も起こると思います。まずは知見の共有、次は脅威情報の共有ということです。

　重要インフラの多くがプライベート（企業）だからでしょうが、各国とも民間との協力をどう進めるかを重視しているようにみえます。官民それぞれの役割を果たしながら、国としてできること、重要インフラ企業として自らやることを認識しながら対応していくことが求められているところです。PPP について NISC は以前から「重要インフラのサイバーセキュリティに係る行動計画」で明記して取り組んできています。外国との関係で必要があれば、官民の連携・協力をさらに高めていく必要があると思っています。

三角　行動計画において、重要インフラ事業者のみではなく、サイバー関連事業者も含めて PPP のメカニズムを重視していくわけですね。

吉川　そのとおりです。

官民協力をより高める

三角　そのメカニズムとして、2018 年に基本法の一部を改正する法律が成立して「サイバーセキュリティ協議会」が設立されました。政府機関や重要インフラ事業者、大学機関等を集めて、サイバー防衛力を高めるため官民で攻撃の手口や対処法を共有する組織として設立されたわけですが、どう評価されていますか。

吉川　法的な枠組みとして、官民の情報共有の枠組みをつくったという意味で極めて画期的な取り組みであったと思います。構成員数は当初の約 100 組織から現在は約 300 組織にまで増えました。そういう意味では入会するメリットは感じられてきているでしょうし、重要インフラ分野の方には入会していただいているだろうと思います。そろそろ次の段階に入ると思っています。いままでの情報共有の役割をみながら、今後どういう形で進めていくのが望ましいのかを検討していきます。

今年4月 20 日、「サイバー攻撃に係る情報の共有・公表ガイダンス検討会」を開催し、サイバー攻撃被害に関する情報の共有・公表ガイダンスの策定に向けて動き出しました。経産省、総務省、警察省、NISC が所掌し、「サイバーセキュリティ協議会」の枠組みの中でやろうと思っています。サイバー攻撃被害組織等の現場にとっては、自組織のレピュテーションに影響しかねない情報共有・公表には慎重であるケースが多いと思います。そこで、被害に関する情報のうち、どのような情報を、どのタイミングで、どのような主体と共有すればよいか、担当者の判断に資するガイダンスを策定しようということです。例えば、技術情報等組織特定に至らない情報に関しては共有・公表の枠組みに積極的に流すことを促す仕組みにしたいと思っています。それを活用することで情報共有が活発化することも期待しています。

三角　米国では米国土安全保障省傘下のサイバーセキュリティインフラセキュリティ庁（CISA）が民間企業とサイバー防衛のための連携強化を図っています。

吉川　そうですね。米国の例はよくみていきます。ウクライナ危機において、2021 年 8 月につくられた Joint Cyber Defense Collaborative（JCDC）の枠組みがきわめて効果的だったとニューバーガー国家安全保障担当副補佐官が発言しています。JCDC は CISA が主導するサイバーセキュリティ強化に向けた官民連携の取り組みです。どのように効果的であったのかを勉強しながら生かせるところは生かしていきたいと思っています。

三角　いま、一般人が、サイバーセキュリティの何についてどのように警戒すべきかを知ろうしても、わかりやすい情報を入手しにくいと思います。技術的な情報であれば JPCERT コーディネーションセンター（JPCERT/CC）や独立行政法人情報処理推進機構（IPA）の情報をみればよいのですが、それらを理解できるのは主として現場の技術者です。経営層や戦略マネジメント層、管理職レベルに遡及できる情報のシングルポイントがあればよいと思います。NISC のポータルサイト「STOP! RANSOMWARE」のような、関係省庁の情報等を集めたウェブページをつくる方向にはいかないでしょうか。

吉川　そうですね。CISA は JCDC のほかに、ウクライナ侵攻後ロシアによるサイバー攻撃に備えてポータルサイト「シールズアップ（SHIELDS UP）」を設置し、警告を発して対策強化を呼びかけたり、被害を受けた組織を支援したり、その他参考となる情報を発信しています。こうした他国の取り組みも参考にしながら何ができるかを考えたいと思います。

ご指摘のように、経営者層、CISO、担当者それぞれに刺さる情報を必要とする人に届くルートで流すほか、民間が国に期待する国ならではの情報があると思うので、それは何で、それをどこまで出せるか等も一緒に考

えたいと思います。ナショナルサートの機能はその中核にもなると思っています。

人材育成の新たな観点「プラス・セキュリティ」

三角　重要な取り組みですね。そういう方向性が「戦略 2021」の一つの目玉になっているわけですね。

DX with cybersecurity の推進にあたっては、突出した高度技術者の育成だけでなく、組織的な対応ができるように経営層、戦略マネジメント層、実務者層等が行動できることが重要です。「戦略 2021」で「プラス・セキュリティ」とのキーワードが入りました。その目的や背景等についてお聞かせください。

吉川　複雑化・巧妙化する事案、脅威に対して、いわゆるトップガン人材を育てるのは引き続き重要です。情報通信研究機構の主催する若手セキュリティイノベーター育成プログラム「SecHack365」や実践的サイバー防御演習「CYDER」、あるいは社会インフラや産業基盤のサイバーリスクに対応する人材を育成する「IPA 産業サイバーセキュリティセンター（ICSCoE）」等の取り組みを含め、これまでの政策である質・量の強化を継続しつつも、さらに環境変化に対応していく観点から、プラス・セキュリティという方向性を出しています。

すべての企業がデジタル化していくという観点からすると、サイバーセキュリティ担当と明示的に割り当てられていない人でもその知識は必要です。それぞれの業務をするにあたって必要なサイバーセキュリティの知識を、時宜に応じてプラスして身につけていただこうという観点で、プラス・セキュリティ知識というキーワードを出しています。それにより DX with cybersecurity も進んでいくと思っています。

また、政府内の取り組み、例えば、政府内でサイバーセキュリティを身につけた人が必要な部署で育っていく仕組みをつくることも大事です。2022 年度より、国家公務員採用総合職試験に新たに「デジタル区分」が設けられました。同区分からの採用者は、情報系の知識を持って、デジタル庁や NISC、その他省庁に配置され、各省でさまざまな経験を積み、できれば民間企業と行き来する「回転ドア（リボルビングドア）」を可能にして、官民の両方で必要な経験・知識を学びながら育っていける取り組みをやっていきたいと思っています。

日本は既に相当なレベルにある

三角　今日のお話から「戦略 2021」の構想の中核は、「世の中の DX の趨勢を踏まえて DX with cybersecurity が大事である。セキュリティの恩恵を受けるのは国民みんなである。その中でナショナルサートがコーディネーションセンター機能をしっかり果たして、全体をドライブしていく」ということでしょうか。

吉川　そうですね。全体を守るためにも、みなさんに対して必要な知識や人の行動を促していく「プラス・セキュリティ」もあわせてやっていきたいと思っています。

三角　ウクライナ情勢をはじめ先行きの見通せない状況にあって、「戦略 2021」は懸念する諸外国の名前が明示されていることから、どうしてもそこにフォーカスされがちでした。しかし、それだけではなくて、「戦略 2021」の根底には、Society 5.0 が進展する中で、「デジタル敗戦」などといわれないように、DX を奏功させるセキュリティの仕組みをつくっていく、という意思があるということですね。そのことも強調しなくてはいけませんね。

吉川　そうですね。サイバーセキュリティ戦略というと、どうしても日本にはサイバー攻撃能力があるのか、攻撃することに法的問題はないのかといった論点に注目が集まりがちです。しかし、「戦略 2021」において、今後 3 年間でやるべき政策を示しています。しっかり中身を普及させていきたいと思っています。「デジタル敗戦」とい

われますが、日本社会のレジリエンスを高めてしっかり守っていくことについて、日本は既に相当なレベルにあります。それを引き続きしっかりやっていくのだということを認識してもらうのも大事だと思っています。

三角 「戦略 2021」は A4 版で 45 頁に及びます。これを読み解くのは大変です。込められた思いを世の中に訴求するのも大変だと思います。今回、JCIC と私として日本のサイバーセキュリティ戦略の根底のところをしっかり伝えていくことの重要性がわかりました。ありがとうございました。

（2022 年 4 月 27 日収録。取材・構成：一般社団法人 日本サイバーセキュリティ・イノベーション委員会［JCIC］）

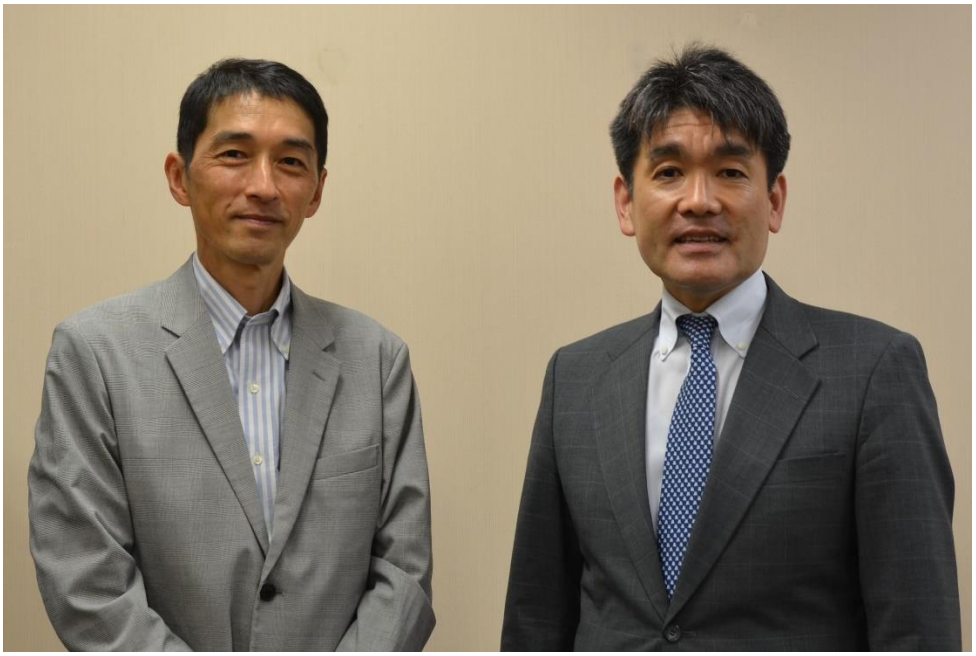
【出席者 略歴】

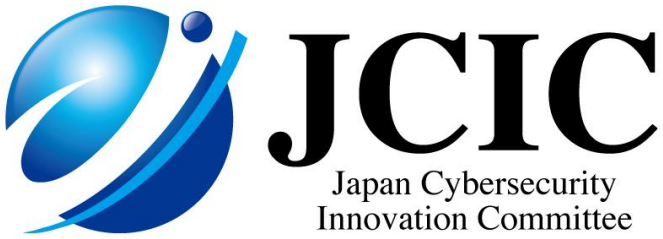
吉川 徹志（よしかわ てつし）

1991 年京都大学大学院工学研究科修了。同年通商産業省（現経済産業省）入省。在韓国日本大使館経済部参事官、内閣官房副長官補室内閣参事官、資源エネルギー庁省エネルギー新エネルギー部政策課長、内閣サイバーセキュリティセンター内閣参事官等を経て、2021 年 10 月より現職。

三角 育生（みすみ いくお）氏

1987 年通商産業省入省。内閣サイバーセキュリティセンター（副センター長等）や経済産業省（サイバーセキュリティ・情報化審議官等）等において、サイバーセキュリティ、安全保障貿易管理といった行政に長く携わり、サイバーセキュリティ戦略の策定、サイバーセキュリティ基本法制定・改正、日本年金機構のインシデント対応等に従事。2020 年 7 月退官。2022 年 4 月～東海大学情報通信学部長・教授。博士(工学)、MA in Management。





[本調査に関する照会先]

JCIC 事務局　info@j-cic.com