特集

オンライン化を支えるセキュリティ

新しい「サイバーセキュリティ戦略」について

内閣官房　内閣サイバーセキュリティセンター
副センター長
吉川　徹志

I. 概論

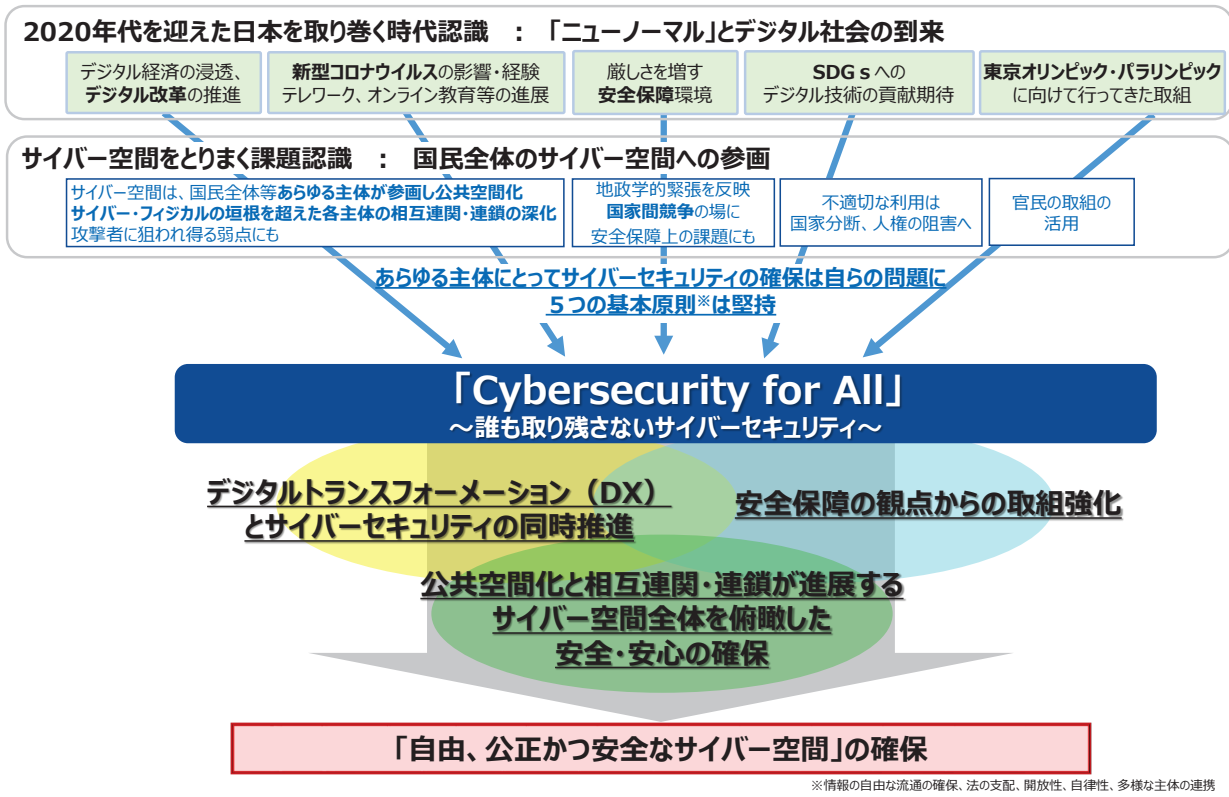
2021年9月28日新しいサイバーセキュリティ戦略を閣議決定した。サイバーセキュリティ基本法の施行とともにサイバーセキュリティ戦略本部が設置されてから、ほぼ7年が経過し、この間、サイバーセキュリティに関する情勢の変化を踏まえ、同法の改正も含めて、対策の強化を図っている。2016年には、日本年金機構の個人情報流出問題が発生したことを踏まえ、同本部が、政府機関及び独立行政法人に加えて、指定法人も含めて直接監査・監視することになり、また、2018年には、サイバーセキュリティに対する脅威の深刻化に対抗すべく、官民の多様な主体が相互に連携し、より早期の段階で、サイバーセキュリティの確保に資する情報を迅速に共有するサイバーセキュリティ協議会を創設した。本年は、東京オリンピック・パラリンピック競技大会（以下「東京大会」という。）が開催されたが、事前の準備と期間中の対応により、大会期間中において、大会運営に影響を与えるようなサイバー攻撃は確認されていない。

我が国をとりまく状況に目を向ければ、新型コロナウイルスの感染拡大に伴い、テレワークをはじめとする多様な働き方や教育によるICT活用等が大きく進展している。本年9月には、「誰一人取り残さない、人に優しいデジタル化」の実現を目指すべく、デジタル改革の司令塔としてデジタル庁が発足した。また、我が国の安全保障環境は厳しさを増し、サイバー空間は、地政学的緊張も反映した国家間の競争の場にもなっている。サイバー空間の安全・安定を確保するため、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ともに、取組を一層強化していくことが求められている。

これからのサイバーセキュリティ政策は、これまでサイバーセキュリティに関する施策の立案及び実施にあたって従うべき基本原則として掲げた5つの原則である①情報の自由な流通の確保、②法の支配、③開放性、④自律性、⑤多様な主体の連携等の基本的な立場を堅持するとともに、誰もが利用する公共空間としての側面を意識して、国民に寄り添った「Cybersecurity for All ～誰も取り残さないサイバーセキュリティ～」を具体的に実現していくことが必要である。

本戦略は、中長期的視点から、先に述べた時代認識に立ち、2020年代初めの今後3年間にとるべき諸施策の目標や実施方針を示すものであり、同時に、未曽有のコロナ禍への対応から得られた教訓、デジタル改革、そして東京大会という大規模国際イベントでの対応を通じた経験を踏まえ、我が国としてのサイバーセキュリティに取り組む決意を、あらゆる主体、各国政府、そして攻撃者に対して発信していくものでもある。以下に今回の戦略の概要について説明する。

図表1　新しい「サイバーセキュリティ戦略」の課題と方向性



（出典）サイバーセキュリティ戦略本部　第31回会合資料より抜粋

Ⅱ. 新しいサイバーセキュリティ戦略の概要

戦略では、まず、前半部分で、中長期的な視点から2020年代を迎えた日本をとりまく時代認識を含めた「策定の趣旨・背景」、「本戦略における基本的な理念」、「サイバー空間をとりまく課題認識」について示し、後半部分で、それらを踏まえて、戦略期間である3年間にとるべき「目的達成のための施策」と、施策を実施するにあたっての「推進体制」を示す形をとっている。以下に順番に説明する。

1．新戦略策定の趣旨・背景

1.1．2020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～

（1）デジタル経済の浸透、デジタル改革の推進

新設されたデジタル庁を司令塔とし、「デジタルの活用により、一人ひとりのニーズにあったサービスを選ぶことができ、多様な幸せが実現できる社会」をビジョンとしたデジタル改革が強力に推進されていくことになる。

（2）SDGsへの貢献に対する期待

SDGsで重点事項として挙げられている様々な分野において、デジタル技術の活用が課題解決に寄与することが期待される。特に、「グリーン成長」の実現に向けては、スマートグリッドや製造自動化をはじめ、強靭なデジタルインフラが不可欠であるとされている。

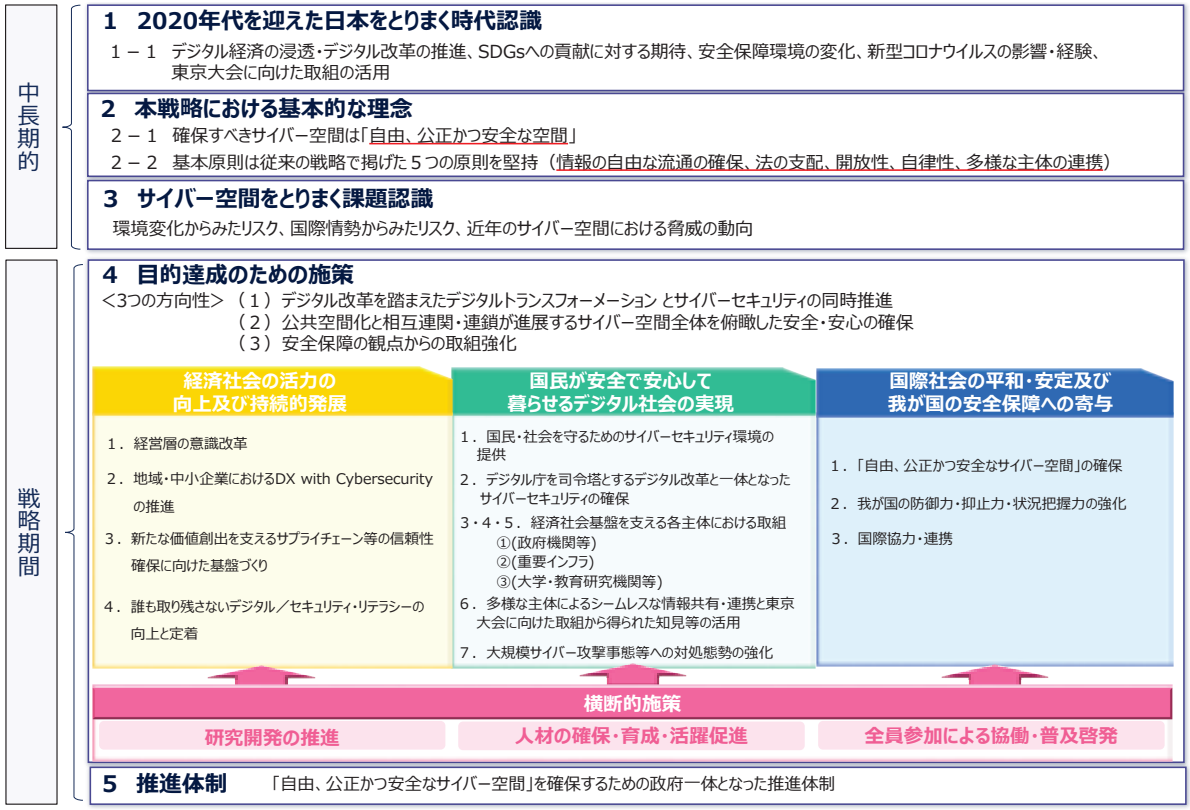
（3）安全保障環境の変化

政治・経済・軍事・技術をめぐる国家間の競争の顕在化を含め、国際社会の変化の加速化・複雑化が進展しており、サイバー空間をめぐる情勢が重大な事態へと急速に発展していくリスクをはらんでいる。

（4）新型コロナウイルスの影響・経験

「ニューノーマル」とも呼ばれる新しい生活様式が Society5.0の実現を部分的にも体現しており、具体的には、テレワークをはじめとする多様な働き方や教育におけるICT活用、遠隔診療などの取組が、コロナ禍以前と比べて大きく進展している。

図表2　新しい「サイバーセキュリティ戦略」の構成



（出典）サイバーセキュリティ戦略本部　第31回会合資料より抜粋

（5）東京大会に向けた取組の活用

2021年に開催された東京大会に向けて官民が連携して行ってきた対処態勢の整備やリスクマネジメントの促進等の取組は、我が国にとって貴重な経験となった。こうした経験を、今後、2025年日本国際博覧会等の大規模国際イベントを含め、我が国におけるサイバーセキュリティの向上に活用していく必要がある。

2. 本戦略における基本的な理念

新戦略では、我が国の基本的な立場として、サイバーセキュリティ基本法で示している「経済社会の活力の向上及び持続的発展」、「国民が安全で安心して暮らせる社会の実現」、「国際社会の平和・安定及び我が国の安全保障への寄与」という3つの目的や、過去2回のサイバーセキュリティ戦略で「確保すべきサイバー空間」として示した「自由、公正かつ安全なサイバー空間」という考え方、そして、「基本原則」として示した、(1) 情報の自由な流通の確保、(2) 法の支配、(3) 開放性、(4) 自律性、(5) 多様な主体の連携という5つの原則については引き続き堅持する。

3. サイバー空間をとりまく課題認識

3.1. 環境変化からみたリスク

（1）脅威の観点

新たなデジタルサービスの浸透は、生命、身体、財産に関わる情報を、これまで以上にサイバー空間の場に委ねることを意味する。これらのデータは今後一層、攻撃者にとって、サイバー攻撃の対象となる誘引性が増すこととなる。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増大する可能性も考えられる。

（2）経済社会が抱える脆弱性の観点

デジタル化の進展により、これまでサイバー空間とは繋がりのなかった様々な業種・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る。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、攻撃者に狙われ得る弱点となる可能性がある。また、クラウドサービス利用、グローバルなサプライチェーン、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る。

3.2. 国際情勢からみたリスク

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おり、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など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の増大がみられるなど、足元では、サイバー空間をめぐる情勢は、有事とは言えないまでも、最早純然たる平時とも言えない様相を呈している。

3.3. 近年のサイバー空間における脅威の動向

VPN機器の脆弱性の悪用、クラウドサービスが攻撃の標的とされるケースの増加、ワクチンに関するフィッシングなどのコロナ禍に乗じたサイバー攻撃や、海外拠点を経由した攻撃、匿名性の高いインフラを通じて行われる攻撃など、足元の環境変化を捉えたサイバー攻撃もみられている。また、標的型攻撃の被害や、「二重の脅迫」を行うランサムウェア、匿名化技術や暗号技術の悪用による事後追跡の回避など、従来の脅威が複雑化・巧妙化している。

4. 目的達成のための施策～Cybersecurity for Allと3つの方向性～

サイバー空間は量的に拡大・質的に進化するとともに、実空間との融合が進み、あらゆる国民、セクター、地域等において、サイバーセキュリティの確保が必要とされる時代（Cybersecurity for All）が到来している。今後、あらゆる主体がサイバー空間に参画することとなる中で、「誰一人取り残さない」サイバーセキュリティの確保に向けた取組を進める必要がある。

この考え方の下、「自由、公正、かつ安全なサイバー空間」を確保するため、（1）デジタル改革を踏まえた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、（2）公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保、（3）安全保障の観点からの取組強化という3つの方向性に基づき、施策を推進する。これらは主として、サイバーセキュリティ基本法における3つの目的である「経済社会の活力の向上及び持続的発展」、「国民が安全で安心して暮らせる社会の実現」、「国際社会の平和・安定及び我が国の安全保障への寄与」に向けた取組にそれぞれ対応するものでもあり、以下に目的に沿った形で今後3年間の目的達成のための主な具体的施策を説明する。

4.1. 経済社会の活力の向上及び持続的発展～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～

デジタル化が大きく推進されるためには、サイバー空間への信頼を醸成し、参加・コミットメントを得ることが重要となる。また、サイバーセキュリティは企業価値に直結する営為になっており、「セキュリティ・バイ・デザイン」の重要性は一層増し、デジタル投資とセキュリティ対策の一体性は高まる。このため、デジタル化の進展と併せて、サイバーセキュリティ確保に向けた取組を、あらゆる面で同時に推進することが重要である。

これに対応するための主な具体的施策として、①経営層の意識改革、②地域・中小企業におけるDX with Cybersecurityの推進、③新たな価値創出を支える「サプライチェーン」、「データ流通」、「セキュリティ製品・サービス」、「先端技術」等の信頼性確保に向けた基盤づくり、④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等を進める。

4.2. 国民が安全で安心して暮らせるデジタル社会の実現～公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心確保～

サイバー空間の公共空間化、相互連関・連鎖の深化、サイバー攻撃の組織化・洗練化を踏まえ、国は、様々な主体と連携しつつ、①自助・共助による自律的なリスクマネジメントが講じられる環境づくりと、②持ち得る手段の全てを活用した包括的なサイバー防御の展開等を通じて、サイバー空間全体を俯瞰した自助・共助・公助による多層的なサイバー防御体制を構築し、国全体のリスク低減、レジリエンス向上を図る。

これに対応するための主な具体的施策としては、以下の通り、横断的・基盤的取組を、「国民・社会を守るためのサイバーセキュリティ環境の提供」として示し、分野に着目した取組を、「デジタル庁を司令塔とするデジタル改革と一体となったサイバー

セキュリティの確保」、「経済社会基盤を支える各主体における取組」、「多様な主体による情報共有・連携と大規模サイバー攻撃事態等への対処体制強化」として示した。

（1）国民・社会を守るためのサイバーセキュリティ環境の提供

① 安全・安心なサイバー空間の利用環境の構築

サプライチェーン管理（ガイドライン策定、産業界主導の取組）、IoT、5G等の新技術実装に伴う安全確保や利用者保護の観点から安全かつ信頼性の高い通信ネットワークを確保するための方策の検討を行う。

② 新たなサイバーセキュリティの担い手との協調（クラウドサービスへの対応）

政府情報システムのためのセキュリティ評価制度（ISMAP）の取組等の民間展開による一定のセキュリティが確保されたクラウドの利用を促進するとともに、信頼性が高く、オープンかつ使いやすい高品質クラウドの整備を推進する。

③ サイバー犯罪への対策

サイバー空間を悪用する犯罪者やトレーサビリティを阻害する犯罪インフラを提供する悪質な事業者等の摘発を推進し、実空間と変わらぬ安全・安心を確保する。また、警察におけるサイバー事案対処体制の強化を行う。

④ 包括的なサイバー防御の展開

サイバー攻撃対処から再発防止等の政策措置までの総合的調整を担うナショナルサート機能の強化、包括的サイバー防御のための環境整備（脆弱性対策、技術検証、制御システムのインシデント原因究明機能の整備等）を行う。

⑤ サイバー空間の信頼性確保に向けた取組

個人情報や知的財産を保有する主体への支援、経済安保の視点を踏まえたITシステム・サービスの信頼性確保を行う。

（2）デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保

デジタル庁が策定する国等の情報システム整備方針にサイバーセキュリティの基本的な方針も示し実装を推進する。

（3）経済社会基盤を支える各主体における取組

① 政府機関等

クラウドサービスの利用拡大を見据えた政府統一基準群の改定・運用やクラウド監視に対応したGSOC機能[1]を強化する。

② 重要インフラ

「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」を改定し、環境変化に対応した防護の強化や経営層のリーダーシップを推進する。また、地方公共団体情報システムの標準化や行政手続きのオンライン化等に対応したガイドラインの見直し等の諸制度を整備する。

③ 大学・教育研究機関等

サプライチェーンリスク対策を含む、先端情報を保有する大学等への対策強化支援等を行う。

（4）多様な主体による情報共有・連携と大規模サイバー攻撃事態等への対処体制強化

東京大会での対処態勢や運用により得た知見やノウハウを広く全国の事業者等に対する支援として積極活用するとともに、平素から大規模サイバー攻撃事態等へのエスカレーションを念頭に、国が一丸となったシームレスな対処態勢を強化する。

4.3. 国際社会の平和・安定及び我が国の安全保障への寄与～安全保障の観点からの取組強化～

サイバー空間は、地政学的緊張も反映した国家間の競争の場となっており、中国・ロシア・北朝鮮は、サイバー能力の構築・増強を行い、情報窃取等を企図したサイバー攻撃を行っているとみられている。同盟国・同志国においても、サイバー脅威に対応するため、サイバー軍や対処能力の強化が進められ、サイバー事案やサイバー空間に関する国際ルール等をめぐる対立等に対して連携して対抗している。今後、サイバー空間の安全･安定の確保のため、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ていく。これに対応した主な具体的施策として､「自由･公正かつ安全なサイバー空間の確保」「我が国の防御力・抑止力・状況把握力の強化」「国際協力・連携」の3つの観点から以下の通り推進する。

① 自由・公正かつ安全なサイバー空間の確保

サイバー空間における法の支配の推進のため、国際法の適用に関する議論・規範の実践の普及、サイバー犯罪に関する条約の普遍化等を推進する。また、サイバー空間におけるルール形成として、Data Free Flow with Trustや5Gセキュリティ等国際的

な取組の進展を踏まえた我が国の基本理念に沿う国際ルールの策定を推進する。

② 我が国の防御力・抑止力・状況把握力の強化

サイバー攻撃に対する防御力の向上として、防衛省・自衛隊におけるサイバー防衛能力の抜本的強化等を行う。また、サイバー攻撃に対する抑止力の向上として、相手方によるサイバー空間の利用を妨げる能力の活用や外交的手段・刑事訴追等を含めた対応を活用する。サイバー空間の状況把握力の強化として、全国的なネットワーク・技術部隊・人的情報を駆使したサイバー攻撃の更なる実態解明を推進する。

③ 国際協力・連携

知見の共有・政策調整として、米豪印やASEAN等同志国との府省庁横断的・各府省庁における国際連携の重層的な枠組みの強化を行うとともに、国際サイバー演習の主導等による国際的なプレゼンスの向上を行う。また能力構築支援としてASEANを含むインド太平洋地域における取組強化を行う。

4.4. 横断的施策

3つの方向性に向けた施策を推進するにあたり、横断的・中長期的な視点で、研究開発や人材育成、全員参加による協働・普及啓発に取り組む。研究開発の推進については、(1) 産学官エコシステム構築による国際競争力の強化、(2) サプライチェーンリスクへの対応、国内産業の育成・発展、攻撃把握・分析・共有基盤、暗号等の研究の推進といった実践的な研究開発の推進、(3) AI技術や量子技術等の中長期的な技術トレンドを視野に入れた対応を行う。

人材の確保、育成、活躍促進については、(1)「プラス・セキュリティ」知識を補充できる環境整備といったDX with Cybersecurityの推進、(2) 巧妙化・複雑化する脅威への対処、(3) 公務員の新試験区分「デジタル区分」の積極活用等政府機関における取組を行う。これにより、「質」・「量」両面での官民の取組を一層継続・深化させつつ、環境変化に対応した取組の重点化や、官民を行き来しキャリアを積める環境整備を行う。

5. 推進体制

我が国のサイバーセキュリティ政策により、自由、公正かつ安全なサイバー空間を確保するためには、政府一体となった推進体制が必要。公的機関が限られたリソースを活用しその役割を果たせるよう、関係機関の一層の対応能力強化・連携強化を図る。また、サイバー攻撃等に対して国全体として網羅的な対処が可能となるよう、ナショナルサートの枠組み整備を行う。

[1] Government Security Operation Coordination teamの略。政府関係機関情報セキュリティ横断監視・即応調整チーム。各機関に設置したセンサーを通じた政府横断的な監視、攻撃等の分析・解析、各機関への助言等を行う。

Ⅲ. まとめ

今後、これまでサイバー空間とは繋がりが薄かった方々も含め、あらゆる方々がサイバー空間に参画することが見込まれる中、本戦略のコンセプトでもある「誰も取り残さないサイバーセキュリティ」の確保のため、内閣サイバーセキュリティセンターを始めとして政府において、戦略に掲げられた各種の取組をしっかり進めていく。

そのためには、政府が一丸となって取り組んでいくことが重要であることはもちろん、外国政府機関や民間部門といった国内外の関係者との緊密な連携を行うこと、取組の進捗の検証についてもきちんと実施し、その結果に基づいて取組を更に前に進めていくことが極めて重要になると考えている。

吉川　徹志（よしかわ　てつし）

神奈川県出身。平成3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参事官などを経て、令和3年10月から現職。