資料２－５

○　横断的課題

本章では、国家安全保障戦略において能動的サイバー防御の実現のための検討事項とされていた各措置に加えて、普段から対応することが求められる横断的な課題について述べる。

①サイバーセキュリティ戦略本部・NISC・関係省庁が連携した施策の推進

深刻化するサイバー攻撃の脅威に対処するには、事案発生時に加えて、普段から対策を強化して備えることが重要であり、これまでサイバーセキュリティ戦略本部（以下、「戦略本部」という。）により、内閣サイバーセキュリティセンター（NISC）を事務局として、政府機関等や重要インフラを中心に、総合的かつ効果的な対策の推進が図られてきたところである。そこで、能動的サイバー防御の実現と併せて、各組織における普段からの対策を抜本的に強化するため、戦略本部の在り方等を含め、見直しを行うことが求められる。

まず、戦略本部が一般的な政策立案や助言に加え、事案発生に備えた普段からの対策について、政府としてより責任を持って意思決定を行っていくには、その構成の在り方から検討すべきである。具体的には、大臣と有識者を戦略本部の構成員としている現在の構成を改め、**基本的な方針や枠組みを大臣による戦略本部で決定し、それに対して普段から助言をする民の有識者からなる組織が別途存在するという形が考えられる**。また、諸外国の取組も参考に、官が主導しつつも、民とあるべき姿をディスカッションする場を平常的に設けることが、サイバーセキュリティ対策の価値を高め、改善に資することになる。

また、NISC については、サイバー安全保障分野の政策を一元的に総合調整する**政府の司令塔として発展的に改組するに当たり、インテリジェンス能力を高め、技術・法律・外交等の多様な分野の専門家を官民から結集し、強力な情報収集・分析、対処調整の機能を有する組織とする必要**がある。その際、NISC や関係する政府機関、地方公共団体等、それぞれの役割と責任範囲を明確に整理することが求められる。さらに、官と官の連携強化の観点からは、関係省庁のサイバーセキュリティ部局が物理的に同じ場所で協働できるよう、基盤となるしっかりとしたインフラ（建物、スペース、勤務環境、セキュリティ等）の確保を図るべきと考えられる。

②重要インフラ事業者等の対策強化

重要インフラ事業者等においては、国民視点でサービス提供を継続できることが肝要であり、重大なサイバー攻撃に対処するためには、攻撃が発生する前の段階から防護を強固にし、実際の攻撃発生時におけるインフラの補完・代替・復旧等の計画をはじめとしたレジリエンスの強化に取り組む必要がある。

この点、まず、**国民視点でサービス継続が求められる重要インフラ分野の防護範囲を定義するにあたっては、重要性の優先順位とともに、新しい分類やデジタル空間の構造*を踏まえた検討が不可欠**である。また、政府として、普段から重要インフラの国民生活や社会経済に対する影響度や相互依存関係を適切に把握しておき、重大なサイバー攻撃の発生時にどのように連携するか、優先度のガイドラインを作って対応できるよう備える必要がある。

＊例えば、国民生活や経済活動における衛星測位関連システム（GPS や準天頂衛星システム（QZSS））の役割は増大しているほか、事業者等の DX により、クラウドサービス等、デジタルアーキテクチャがあらゆる環境の基盤になっている。

また、重要インフラのレジリエンスの強化のためには、普段から求められるサイバーセキュリティ対策の質の保証の観点から、基準、ガイドラインという手法により、行政が達すべきと考える水準を分かりやすく示し、誘導していくことが必要である。この点、近年、欧米主要国では、特に重要な事項として事業者等が実施すべき対策につき、政府が優先順位をつけてベースラインを明示する取組が行われていることも参考になる。策定した基準等については、関係者の声を聞き、常に見直しを図るとともに、遵守の実効性を確保するため、認証、資格の活用や遵守状況の公表など、実効性を高める仕組みを設けることが考えられる。併せて、重要インフラ分野の中で優れた取組があれば、監督権限やリソースの差も考慮しつつ、他の分野に展開することも有効である。

さらに、重要インフラ事業者等のサプライチェーンを構成する中小企業のレジリエンス強化のためには、政府が基準等を策定するのみならず、その実行に必要なリソース支援、政府調達要件への採用等の方法論を用意し、それらを中小企業が活用できるようにすることも求められる。

なお、重要インフラ分野の防護範囲の決定や基準等の策定は、戦略本部でなされているところ、我が国や諸外国で重要インフラとなっている分野を所管する大臣全てが構成員となっていない点について見直しを図ることも考えられる。

③政府機関等の対策強化

政府機関においては、重大なサイバー攻撃事案の発生時においても、その機能を維持することが不可欠となる。国家安全保障戦略では「世界最先端の概念・技術等を常に積極的に活用する」ことが掲げられているが、政府機関等の情報システム内で行われる不正活動を監視・制御する技術の導入を進め、今まで以上にサイバー攻撃に関する膨大かつ詳細な状況の観測・分析の積み重ねを行っていくことが必要となる。

また、政府機関が自らのサイバーセキュリティ水準を強固にすることが必要であり、例えば、政府機関等の脅威対策やシステムの脆弱性等を随時是正するため、府省横断的なリスク評価結果や注意喚起についての対応が個々の政府機関に委ねられている点を改め、対応の実効性を確保する仕組みを設けることが重要である。

これら政府機関等の対策の強化にあたっては、日本発のサイバーセキュリティ関係のソフトウェアや中核的なセキュリティ技術がほとんどなく、公に使われているものもないという我が国の状況を踏まえると、国家安全保障の観点からも政府主導で高品質な国産セキュリティ製品、サービス供給の強化を支援すべきと考えられる。その際、大学等で開発された技術等の社会実装と、知見のフィードバックによる更なる技術開発の促進というエコシステムの構築を図ることも重要となる。また、欧米主要国では、政府が公共機関や国民向けに、セキュリティ対策を強化するための多様な支援サービスを提供している例もあり、現行法制度下でも実施可能な施策は積極的に取り入れることが望ましいと考えられる。

④サイバーセキュリティ人材の育成・確保

重要インフラ事業者等や政府機関等における事案発生時の対応や普段からの対策強化に当た

っては、サイバーセキュリティ人材の育成・活用の促進が不可欠である。国家のサイバーセキュリティの力とは、その国におけるサイバーセキュリティ人材の層の厚さであるとも考えられ、人材の重要性が叫ばれて久しいが、セキュリティ分野に実際に人材が流入するような状況にはなっていない。これまでにも幅広い取組がなされてきたところであるが、依然として大幅な不足が指摘されるサイバーセキュリティ人材の育成を官民で効果的に行っていくためには、まずは、政府が官民の人材育成の取組をしっかり把握した上で、**産学官の共通認識を醸成するため、政府主導で技術者に限らず、経営等に関わる者も含めたサイバーセキュリティに関わる人材の定義（役割、知識、技術等）付けや資格の活用による可視化等を行う**とともに、必要な人数・規模についてもメッセージを示すべきである。

具体的な育成・確保のための方策としては、企業・組織の視点として、長期的なキャリアパスの明示、待遇の改善、経営層の理解の促進、人材の重要性の周知、企業等の組織への当該分野人材採用のための支援等が必要となる。その際、非技術者の巻き込みも重要となるため、専門用語だけでなく、分かりやすい比喩や統計データの活用などにより、サイバーセキュリティ対策の重要性について、経営層を含めた非技術者にも広くわかりやすく説明することが求められる。一方、制度面や給与面だけでなく、サイバーセキュリティを担う人材のインセンティブも重要であり、現場でサイバーセキュリティの実務に携わる人の生の声を聞き、それらを集約して政策に活かすことも重要である。これらの観点から、CISO を重要視することは、組織のセキュリティ強化とともに、魅力的なキャリアパスを提示することにつながる。このほか、若年層から教育を行うことも重要である。

また、**サイバー攻撃に関する情報や危機感の共有によるトラストの醸成等を目的として、NISC 等の政府機関との官民人材交流に関する枠組みを導入すべき**であり、政府においては、関係省庁のサイバーセキュリティ部局の人材の任期の長期化等についても検討すべきと考えられる。さらに、海外では産学間の移動も多く、民間の優秀な人材が大学で学び、さらに専門的な能力を身につけるという流れが存在し、我が国においても、大学における教育や人材育成の取組を重視しつつ、産学官での人材交流・流動化を推進することが重要となる。

⑤中小企業や地域における対策強化とその他の検討課題等

サイバー攻撃は、セキュリティ対策が十分でないところが狙われることがあるため、サプライチェーンの弱点を突いたサイバー攻撃が増加しているなど、その被害は重要インフラ事業者等に限らず、中小企業等にも及んでいる。社会全体の強靭性を高める観点からは、我が国において数の上で 90%以上を占める中小企業や地域の企業を含むサプライチェーン全体での対策が必要であるが、資金や人材等のリソースが限られている中小企業が自らのみでセキュリティ対策を進めていくことは困難である。

そのため、**中小企業等のセキュリティ対策については、政府によるツールの提供などを含めた支援拡充の検討や、大企業による下請企業のセキュリティ対策の支援・要請に係る独占禁止法等の明確な整理、サプライチェーン企業の対策水準の検討を行うべき**であると考えられる。

また、中小企業等については、サイバーセキュリティの対策・情報共有を実施できる人材育成が必要と同時に、政府がそのような中小企業等の活動を支援しつつ情報連携を行う施策を検討することが望ましいと考えられる。