資料２－５

サイバーセキュリティ戦略の策定に際しての国家安全保障会議意見

現代の我が国の経済社会において、サイバー空間はあらゆる活動に不可欠な社会基盤となっており、全国民が参画する「公共空間」として、その重要性及び公共性はますます高まっている。こうしたサイバー空間の「公共空間化」は、新型コロナウイルス感染症の感染拡大に伴うテレワークの増加や社会のデジタル化の推進によりその勢いを加速化させており、今後ともこのような傾向は継続するものと考えられる。

一方、国家安全保障の観点からは、急速に厳しさを増す安全保障環境の中、サイバー空間の「公共空間化」は、経済社会全体がサイバー空間への依存度を高めることにより、サイバー攻撃が我が国の経済社会に甚大な影響を与え得るという点で、安全保障上のリスクとなり得る側面もあわせ持つ。実際に、サイバー攻撃は一層複雑化・巧妙化しており、重要インフラに対するサイバー攻撃により経済社会活動に大きな影響が発生した事例も存在する。また、引き続き、国家を背景に持つサイバー攻撃は特に深刻な脅威であり、サイバー空間は、地政学的な緊張も反映した国家間の競争の場となっている。我が国としても、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、サイバーセキュリティの推進においても安全保障の観点からの取組を更に強化することが不可欠である。

以上の観点から、サイバーセキュリティ戦略の策定に際し、内閣サイバーセキュリティセンターは、国家安全保障局と密接な連携を図るとともに、以下の視点を十分に踏まえられたい。

１．サイバー空間を巡る安全保障環境

サイバー空間を巡る近年の安全保障環境の特徴として、（１）国家の関与と平素からの国家間の競争、（２）サイバー空間の「公共空間化」に伴う社会的影響の増大、（３）サイバー攻撃の複雑化・巧妙化が挙げられる。いまやサイバー空間も平素からの国家間の競争の「主戦場」であり、国家関与や社会的影響の増大等により、サイバー攻撃が国家や民主主義の根幹を揺るがす国家安全保障上の重大な事態へと急速に発展するリスクが顕在化している。安全保障の根幹となる極めて重要な課題として、サイバー空間における安全保障の確保に取り組む必要がある。

（１）国家の関与と平素からの国家間の競争

軍事関連情報を含む機微な情報の窃取や、ランサムウェア（身代金要求型マルウェア）等の攻撃による社会経済活動の基盤の機能停止など、近年、国家の関与が疑われるものを含む組織化・洗練化されたサイバー攻撃の脅威が増大している。匿名性・隠密性を確保しやすいサイバー空間では、地政学的緊張を反映した国家間の競

争が展開されており、有事と平素の境界はますます曖昧になってきている。
　また、サイバー空間に自由や公正等を求める国家と、国家によるサイバー空間の統制・強化を主張する国家との間で国際ルール形成を巡る対立が深まる状況となっている。

（2）サイバー空間の「公共空間化」に伴う社会的影響の増大
　サイバー空間の「公共空間化」が進み、重要インフラを含む経済社会全体がサイバー空間への依存を高めるにつれ、サイバー攻撃が甚大な社会的影響を及ぼすリスクが増大している。特に、クラウドサービスの利用拡大やテレワークに伴う遠隔でのシステム利用により、サイバー空間の「公共空間化」は急速に進展しており、このような足下の環境変化に伴う脆弱性を悪用した攻撃も顕著である。

（3）サイバー攻撃の複雑化・巧妙化
　ランサムウェアの販売や身代金の要求などを分業して行う「産業化」された集団が形成されるなど、サイバー攻撃の組織化・洗練化が一層進んでいる。加えて、ソフトウェアサプライチェーンやクラウドサービス等の普及を突いたサイバー攻撃が行われるなど、侵入経路や得られる効果、攻撃のピンポイント性や隠密性を高度・精巧に練り上げた攻撃事案が見られる。

2. サイバー安全保障の基本的考え方

　上記の安全保障環境認識の下、攻撃者や国家関与の有無・程度の特定が容易ではなく、また、国家関与の有無に関わらず急速に安全保障上のリスクが顕在化するというサイバー空間の特性を踏まえると、サイバー攻撃から我が国の安全保障上の利益を守るためには、（1）サイバー攻撃対応の基盤として、各種情報を集約し、サイバー空間の動きを把握する力（状況把握力）、（2）サイバー攻撃による被害・影響を減殺し、国家の強靭性を確保する力（防御力）、（3）我が国にサイバー攻撃を行うリスク及びコストを攻撃者に認識させ、サイバー攻撃のハードルを高める力（抑止力）の3つの力を抜本的に強化し、対応を進める必要がある。
　上記の取組に関しては、内閣官房国家安全保障局による全体取りまとめの下、状況把握は情報収集・調査を担う省庁、防御は NISC を中心として官民を問わず全ての関係機関・主体、抑止は対応措置を担う省庁が、急速な情勢の変化に迅速かつ柔軟に対応するため、平素から連携しサイバー安全保障に取り組む。また、重大な政策判断が求められる場合を含め、必要な場合には、国家安全保障会議で議論・決定を行う。

3. サイバー空間における安全保障の確保のための取組

「自由、公正かつ安全なサイバー空間」の確保は、サイバー空間の状況を把握する能力の強化を基礎とした上で、サイバー攻撃に対する防御力やサイバー攻撃に対する抑止力の向上を総合的に推進することにより、達成されるものである。また、以上3つの力を強化するとともに、平素から有事に至るまでサイバー政策を効果的に推進するためには、国内体制の強化及び国際連携の推進が不可欠である。

(1)サイバー空間の状況を把握する力の強化

サイバー空間の状況把握力は、防御力及び抑止力の基盤であり、深刻化するサイバー攻撃の脅威を防御・抑止していくためには、官民が保有する事案情報等のあらゆる情報を集約・共有した上で分析を行うことにより、攻撃者を特定する能力が求められる。よって、関係機関におけるサイバー攻撃を検知・調査・分析する能力を引き続き向上させ、サイバー攻撃の更なる実態解明を推進するために、政府全体として状況把握力を更に強化する。

そのため、関係機関の全国的なネットワーク、技術部隊も駆使しながら、捜査・調査機関の能力を質的・量的に向上させ、情報収集・情報分析能力を強化する。また、その役割を十分に果たすため、人材育成・確保を含めた有効な手段について、幅広く検討を進める。さらに、平素からNISCを中心として官民の情報の集約を行い、それらの情報を国家安全保障局を含めた政府機関に対して情報共有を適時・適切に行う。

隠密性が高く攻撃者優位と言われるサイバー空間を、平和で安全な空間にしていくために、サイバー攻撃の主体を特定する可能性を高める必要がある。そのため、攻撃に係る痕跡の確保や活用に必要となる措置を検討するとともに、民間を含めたより広い情報源を活用するなどの方策を検討する。

政府内の情報共有体制の強化、外国政府機関とのサイバー脅威情報(CTI)の共有等、サイバー攻撃に対する対応能力向上のための情報連携を進める。

(2)サイバー攻撃から国家を防御する力の向上

サイバー空間に係る安全保障の確保のためには、国家の関与が疑われるものを含むサイバー攻撃から、政府機関、重要インフラ等の任務・機能を保証するなど、サイバー空間の防護のための取組を一層強化し、サイバー攻撃から国家を防御する力を向上させていくことが肝要である。

国民生活や経済社会活動を支える政府機関は、その機能停止や、保有する機微な情報の窃取を厳に回避しなければならないことは言うまでもない。また、重要インフラシステムを担う事業者は、政府機関の任務遂行はもちろん、国民生活や経済社会活動に不可欠なサービスを持続的に提供するという重要な任務を有している。

そのため、政府機関についてはその任務を保証する観点から、政府自らが保有す

るネットワーク・インフラの防護の強化、政府機関の行政遂行上必要なシステムに対するサイバーセキュリティの確保等、政府機関の対策を強化する。特に、安全保障上の活動を担う要である防衛省・自衛隊については、2018 年に策定された「平成 31 年度以降にかかる防衛計画の大綱」（以下「防衛大綱」という。）に基づき、サイバー分野に関する各種の取組を進め、サイバー防衛に関する能力を抜本的に強化する。

重要インフラに関しては、政府への報告や安全基準等の改善、事業者等による対応の強化を含め、重要インフラ防護の対策を徹底する。

また、ランサムウェアなどの複雑化・巧妙化したサイバー攻撃に対応するために、サイバーセキュリティ分野における基盤強化を行う。具体的には、産学官連携により、サイバー攻撃データの収集・蓄積・活用を大規模に行うとともに、人材育成や国産技術の開発を併せて実施する。

さらに、警察をはじめとする対処機関の能力を質的・量的に向上させ、攻撃者の特定、被害の未然防止・拡大防止を行うために必要な体制を確保する。

（3）サイバー攻撃を抑止する力の抜本的強化

現在、サイバー空間では、国家の関与が疑われるものを含め、組織的かつ周到に準備された高度なサイバー攻撃の脅威が増大している。また、サイバー空間は、その匿名性・隠密性により、攻撃者にとって「攻撃が露見するリスク」及び「仮に露見した場合のコスト」がいずれも低い状況にある。このような攻撃者圧倒的優位の状況の中、サイバー空間における安全保障を確保するためには、攻撃者との非対称な状況を看過せず、サイバー攻撃に対する防御力のみならず、平素から有事に至るまでのシームレスな対応力を強化し、抑止力を抜本的に強化することが不可欠である。

近年、米英等の諸外国においては、攻撃者を公表し、非難することで抑止する、いわゆるパブリック・アトリビューションが行われている。我が国としても、悪意あるサイバー攻撃に対しては警察等による捜査・分析の成果を踏まえて適切に対応してきている。2021 年 4 月に警察において書類送致した事件の捜査を通じ、国内企業への攻撃を実行したサイバー攻撃集団の背景組織として、中国人民解放軍が関与している可能性が高いと評価するに至ったことから、その旨を公表した。同年 7 月には、我が国も攻撃対象としていた APT40 と呼ばれる組織が中国政府を背景にもつと評価し、外務報道官談話を発出している。

また、我が国は、悪意ある主体の行為を抑止し、国民の安全・権利を保障するため、国家の関与が疑われるものも含め、サイバー空間における脅威について、平素から同盟国・同志国と連携し、政治・経済・技術・法律・外交その他取り得る全ての有効な手段と能力を活用し、断固たる措置をとる。この点に関し、2019 年の日米「2+2」において、一定の場合には、サイバー攻撃が日米安全保障条約第 5 条の規定の適用上武力攻撃を構成し得ることを確認したところである。また、防衛大綱に基づき、我が国

への攻撃に際して当該攻撃に用いられる相手方によるサイバー空間の利用を妨げる能力も活用していく。さらに、サイバー攻撃者が攻撃に活用するサーバーなどの機器を特定の上、それら機器を足掛かりとして攻撃の全容を解明し、鎮圧するなど、サイバー攻撃者にコストを課すための対応措置を検討する。

国際場裡における議論等を通じ、国際社会の平和と安定及び我が国の安全保障に資する国際社会のルール形成及びその運用を図ることは、サイバー攻撃を抑止する観点からも重要である。一部の国家が、当該国発と考えられるサイバー攻撃に対して自国の関与及び責任を否定する現状においては、国家を含む攻撃者に国家責任の追及やパブリック・アトリビューションに繋がる予見可能性を与えるなど、攻撃者側のコストを高める必要がある。そのためには、サイバー攻撃が国家に帰属しない場合でも、サイバー攻撃が自国の領域から行われた場合には、一定の条件の下で国家責任が認められるような国際社会のルールの形成及び運用を目指す必要がある。以上の考えに基づき、国連の場におけるものを含め、同盟国や同志国とも協力・連携しながら関連の議論に引き続き積極的に参加する。

（4）国内体制の強化及び国際連携の推進

サイバー空間においては、国家と非国家主体間の境界が明瞭でない攻撃事案が増加している。また、犯罪捜査や技術的対応などの平素からの対応を必要な場合に国家安全保障上の対応に速やかに引き上げることを考慮すると、政府一体となったシームレスな対応が不可欠である。そのため、政府全体の総括を行う国家安全保障局の機能を強化し、関係機関と日頃から連携することで有事に備える。また、重大な政策判断が求められる場合を含め、必要な場合には国家安全保障会議の下で対処する。さらに、国家安全保障局の総合調整の下、状況把握力・防御力・抑止力のそれぞれについて、関係機関がそれぞれの役割に応じて能力を向上させる。

また、サイバー空間における脅威は容易に国境を超えることから、一国のみで自らの平和と安定を守ることには限界があり、国際社会が連携・協力して対応していくことが重要である。同盟国・同志国と密接な連携がとれるよう、政府内における様々な階層において、各国のカウンターパートとの日常的な情報共有・政策調整のための連携体制を強化する。加えて、偶発的な衝突を防ぐとともに国家間の信頼を醸成する見地から、各国と情報交換、政策対話、交流などを進める信頼醸成措置を推進する。

（5）経済安全保障の観点からのサイバー空間の信頼性確保に向けた取組

近年、政府・企業が保有する個人情報や知的財産を目的とするサイバー攻撃の脅威が深刻であることから、国は経済安全保障の観点からもサイバー攻撃に対する対策を講じる必要がある。

また、国民生活や社会経済活動を支える事業者等の IT システムがサイバー攻撃

を受けると、社会全体に影響が及ぶ可能性があることから、我が国としても経済安全保障の観点から、脆弱性を有するサイバー空間を把握するとともに、その信頼性確保に向けた対応を検討する。

4. 結論

サイバー空間における脅威の高まりを踏まえ、「自由、公正かつ安全なサイバー空間」を確保するために、我が国として状況把握力・防御力・抑止力の3つの力を抜本的に強化し、高度化するサイバー攻撃に対応できる実効性の高い取組を政府横断的に進めていかなければならない。

状況把握力は、防御力及び抑止力の基盤であり、複雑化・巧妙化するサイバー攻撃に対応するために、各政府機関における情報収集力の底上げを図るとともに、官民が保有するあらゆる情報を集約・共有し、分析を行うことが重要である。そして、政府機関及び重要インフラ事業者等の防御力を抜本的に強化する。また、警察をはじめとする関係機関は、サイバー攻撃に対する防御力を向上させる観点から、攻撃者を特定するための取組をより進める。その上で、サイバー攻撃が国家の関与により行われたことが十分な根拠に基づき強く疑われる場合には、抑止力強化の観点から、パブリック・アトリビューションを行うなどの毅然とした対応が必要である。また、平素から有事に至るまでサイバー政策を効果的に推進するためには、国内体制の強化及び国際連携の推進が不可欠であり、特に、平素における事案は常に国家安全保障上の事態に進展し得ることから、必要な場合には国家安全保障会議による政策判断の下、迅速かつ有効な対応をとらねばならない。