資料３

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

我が国は戦後最も厳しく複雑な安全保障環境に直面している。ロシアによるウクライナ侵略により、国際秩序を形作るルールの根幹がいとも簡単に破られるとともに、我が国周辺では核・ミサイル戦力を含む軍備増強が急速に進展し、力による一方的な現状変更の圧力が高まっている。

このような中、サイバー空間においては国家を背景としたサイバー攻撃による重要インフラの機能停止や不正アクセス等による機微情報の窃取などが世界中で常態的に行われている。これらのサイバー攻撃は、攻撃の事実や背景が露見しにくく、攻撃者が優位に立ちやすいという特性を持つため、国家の安全保障に対する脅威として対処する必要がある。

このような認識から、2022 年 12 月に策定された国家安全保障戦略では、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させることが明記された。特に、武力攻撃に至らないものの、国や重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合には、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために、能動的サイバー防御を導入することとされた。2025 年 5 月には、これらの内容を実現するための法律として、「重要電子計算機に対する不正な行為による被害の防止に関する法律」及び「重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律」が成立した（以下、２つの法律をまとめて「法」と呼称する。）。同年 7 月には、内閣サイバー官が新設されるとともに、官民のサイバーセキュリティの確保と、サイバー安全保障分野の政策の一元的な総合調整を行う新たな司令塔組織として、国家サイバー統括室が設置された。

今般のサイバーセキュリティ戦略は、上記の取組によって我が国のサイバー安全保障体制が大きく変化したことを踏まえ策定されるものであり、能動的サイバー防御を含む今後のサイバー安全保障の具体的な取組の在り方を示すものとなる。サイバーセキュリティ戦略本部は、同戦略の策定に際し、以下の視点を十分に踏まえられたい。

１．サイバー安全保障環境の現状認識

(1)現在の安全保障環境とサイバー空間

現在の安全保障環境においては、軍事と非軍事、有事と平時の境目が曖昧になり、ハイブリッド戦が展開されている。サイバー攻撃はハイブリッド戦の主要な手段であり、平時から国家を背景として情報窃取等を目的としたサイバー攻撃が行われている。

窃取された情報は、影響力工作等、ハイブリッド戦の別の手段に転用されることもある。さらには、重要インフラ等の機能妨害や機能破壊を目的とした攻撃もしばしば行われており、これらの攻撃により重要インフラ等の機能に支障が生じた場合、我が国の国民生活や社会経済活動、また有事における作戦の遂行等にも深刻な影響を与える可能性がある。こうした攻撃は、有事に先んじて開始され、対立する国家間の緊張の高まりに応じて烈度を増し、有事においてはキネティックな手段とも合わせて行われるようになる。また、一定の場合においては、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日米で確認している。

国家安全保障上特に注目すべき国・地域も、サイバー攻撃等の国家的利用を行っている。ロシアはウクライナ侵略に際して、サイバー攻撃を活用し、通信・電力網への攻撃を実施している。中国を背景とするサイバー攻撃アクターに対しては、我が国及び同志国・同盟国がパブリック・アトリビューションや注意喚起を行っている。これらのサイバー攻撃は主に情報窃取を目的としたものとされているが、同国のサイバー能力は重要インフラ等の機能妨害・機能破壊も視野に入れたものであるという評価もある。また、北朝鮮については、暗号資産の窃取や、身分を偽った IT 労働者の外国への派遣等を通じて得られた収入が核・ミサイル開発の資金源として利用されていることが指摘されており、2024 年には国内でも多額の暗号資産が窃取される事案が発生している。

(2)サイバー脅威の高度化

国家背景のサイバー攻撃は、技術的に極めて高度化しており、従来と比較して防御が更に難しくなっている。具体的には、ゼロデイ脆弱性を活用した攻撃や、システム内寄生(Living Off The Land)戦術等、ベンダーから提供されるパッチの適切な適用や、EDR 等の防御技術をもってしても検知・防御できない攻撃手法が用いられるようになっている。さらに、生成 AI を利用したサイバー攻撃や、量子計算機による従来の公開鍵暗号の安全性の低下等、技術の進展に伴う新たなリスクも指摘されており、サイバー攻撃の手法は今後ますます高度かつ防御困難なものとなっていくことが予想される。

(3)社会全体のデジタル化によるリスク要因の拡大

上記のように、重要インフラ等が現に攻撃対象とされているなど、国際情勢の複雑化、社会経済構造の変化等により、安全保障の裾野は経済分野にも急速に拡大している。社会全体におけるデジタル化の進展も、こうした状況に拍車をかけており、例えば、企業資源計画ツールの導入をはじめとする事業者内のシステム統合は、セキュリティリスクの一点集中を招いているほか、コロナ禍等が加速させたテレワークやオンラインサービスの利用は、IoT 機器やクラウドサービス等を社会全体に浸透させ、

サプライチェーンの広がりや複雑化とも相まって、あらゆる主体にサイバー攻撃被害のリスクを生じさせている。

2. サイバー安全保障の基本的考え方

これまでのサイバーセキュリティ戦略策定に際し、国家安全保障会議として意見を提出してきたとおり、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、(1)サイバー攻撃に関する各種情報を集約し、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つの力を強化する必要がある。サプライチェーンが複雑化していることや社会全体のデジタル化が進展していること、また安全保障上懸念となるサイバー攻撃対象には多くの民間施設が含まれることに鑑みれば、民間事業者等とも密接に連携した上で、これらの力を着実に向上させることは、安全保障面でも重要な取組となる。法によって可能になった(ア)官民連携の強化、(イ)通信情報の利用及び(ウ)アクセス・無害化措置は、これらの力を抜本的に向上させることに資する。なお、(ア)(イ)(ウ)の運用において、法の規定が遵守されなければならないことは言うまでもない。

サイバー対処能力を向上させるための取組を実施するに当たっては、サイバーセキュリティの確保に関する総合調整等の事務を掌理する職として新たに設置された内閣サイバー官の指揮を受け、新たな司令塔組織として設立された国家サイバー統括室の総合調整の下、政府の各機関が緊密に連携しなければならない。内閣サイバー官は国家安全保障局次長も兼務しており、国家サイバー統括室の総合調整は国家安全保障局と連携して実施される。また、各取組の実施に当たっては、国家サイバー統括室を中心とする関係府省庁は、官民双方の関係機関・主体と平素から連携し、民間の知見を活用することも必要である。こうした体制を前提として、サイバー攻撃キャンペーンへのアクセス・無害化措置に係る対処方針の策定を含む、重要な政策判断が求められる場合等、必要な場合には、国家安全保障会議で議論・決定を行う。

3. サイバー安全保障を確保するために必要な取組

(1)サイバー空間の状況を把握する力の強化のための取組

サイバー空間における状況把握力は、防御力及び抑止力を支える基盤であり、深刻化するサイバー脅威に対抗するために、引き続き重要となる。それゆえ、状況把握の能力を強化するために従前から行われてきた取組の重要性については、能動的サイバー防御の導入あるいは法の成立を経ても変わることはなく、更なる強化が必要である。具体的には、関係政府機関においては、引き続き、サイバー攻撃の検知・調

査・分析を行う能力の向上や、捜査・調査機関の質的・量的な拡充、官民におけるインシデントや脆弱性の情報集約、及び外国機関等とのサイバー脅威情報の共有等、状況把握のための取組を推進する必要がある。こうした情報は、政府部内での情報共有を促進することを通じて、国家サイバー統括室に集約され、同室における分析を通じて、サイバー空間の状況把握のために役立てられなければならない。また、これらの取組全てにおいて、民間等の先行する知見を絶えず参照し、活用する必要がある。

その上で、法で強化された、又は新たに可能になった権限も、状況把握力を抜本的に高めるために活用されなければならない。特に、（ア）官民連携の強化における、基幹インフラ事業者による特定重要電子計算機の届出及びインシデント報告の義務化等や、（イ）通信情報の利用によって、政府はこれまでをはるかに超える規模の情報にアクセス可能となる。これらの情報は、従前の取組によって収集・分析されたインシデント、脆弱性及びサイバー攻撃の情報や、民間や外国機関等から提供された情報と組み合わせることで、サイバー攻撃の準備活動や、主体の推定、被害の未然防止に資する情報提供等に役立てることができるようになる。国家サイバー統括室をはじめとする関係府省庁は、このことを念頭に、（ア）や（イ）について必要な体制やプロセスの整備、人材育成及び機材の調達等を進める必要がある。

また、このような技術的な情報を安全保障面での政策に活用するためには、地政学的な脅威分析と組み合わせる必要がある。特に、特定国の政治的・軍事的な動向からサイバー脅威の動機や動向を推測し、防御や抑止に関する取組に活用することは、サイバー攻撃がハイブリッド戦における主要な手段であることに鑑みれば不可欠である。サイバー空間のみならず、政治的・軍事的側面も交えた分析を政府一体として行えるよう体制の整備や人材の育成などを行う必要がある。

更に、情報収集の各段階において、分析された情報が、適切な形で、民間の被害防止に役立つ形で提供され、これをもって民間において政府に情報提供を行うインセンティブを付与し、政府において更なる情報集約が進み、より早期かつ精度の高い攻撃の把握や未然防止が可能になり、民間の被害防止に資する情報提供が可能になるといった好循環が生まれるよう取り組む必要がある。さもなければ、法によって基幹インフラ事業者を対象に新たに設けられた義務は民間の労力を空費するものとなり、任意の協力が必要になる取組（情報共有・対策のための協議会や、当事者協定に基づく通信情報の取得等）の運用にも支障を来す。

最も重要なことは、こうした情報収集、分析及び提供等の取組の経験が、国家サイバー統括室をはじめとする関係府省庁において長期的に蓄積され、我が国を狙うサイバー攻撃者への対処手法の改善に活用されていくことである。このためには、単純な情報の蓄積・データベース化及び攻撃者単位での情報整理は勿論のこと、情報の分析や提供の内容や在り方等について、関係府省庁間及び民間事業者等からのフィ

ードバックを常に活用することが肝要である。

（2）サイバー脅威から国家を防御する力の向上

国家のサイバー防御力を更に高めるためには、上記のような状況把握に関する取組を通じて収集・分析した情報を、防御に関する取組に活用することが求められる。具体的には、政府や重要インフラ等のシステムを重大なサイバー攻撃から防御することを目的として情報収集・分析が行われ、その結果把握されたサイバー空間に関する情報をもとに、政府機関及び民間に対して、具体的なサイバーセキュリティ対策が可能になる情報が積極的に提供等されなければならない。さらに、こうした情報提供の取組は、各主体が様々な攻撃者の存在やサプライチェーン・リスクを含むサイバーセキュリティ上のリスクについて、可能な限り正確な現状認識を持つことを助け、もって機器の適切な選定や設定、脆弱性への対応といった行動が着実に行われるようになることを促すことにもつながる。また、収集した情報をもとに、政府において各種のサイバーセキュリティ基準を絶えずアップデートすることで、各主体の防御力を高めることができる。こうした官民における行動を通じ、最新のサイバー脅威に対する官民全体の防御力を高めていくことが肝要である。

このようなサイバー防御力向上のためにサイバー空間の情報を活用する取組を進めることで、システム内寄生戦術等、従来のサイバーセキュリティ対策では検知や防御が難しい戦術に対しても対策を行えるようになる。特に、収集・分析した情報をもとに、特定のサイバー脅威アクターの攻撃基盤（C2 サーバ等）や手法を解明し、システムへの攻撃有無を探るといった、いわゆる脅威ハンティングの取組は、このような高度な攻撃による被害の未然防止にとって非常に重要になる。更に、脅威ハンティングは、能動的サイバー防御に資する情報を得る手段としても有効である。官民で脅威ハンティングを行い、結果として発見・解明されたサイバー攻撃アクターの Indicator of Compromise（IoC）や攻撃手法の情報は、サイバー空間の状況把握を更に精緻化させ、精緻化した状況把握をもとに、更に高度な情報提供、技術基準の策定、及び最新の攻撃手法に対応した脅威ハンティング等ができるようになる。このように、防御力向上の観点においても、状況把握と情報提供における正のフィードバック・ループが意識されなければならない。

また、サイバー空間の状況把握は、法によって新たに可能になったアクセス・無害化措置の効果を最大限発揮するために不可欠であることは十分に意識されなければならない。アクセス・無害化措置は、サイバー空間において、武力攻撃に至らない事態においても、自衛隊による通信防護措置を含む安全保障上の対応が可能になったという点において、サイバー防御力の向上に対して大きな意義を有する。他方で、政府において攻撃サーバ等の情報を把握できなければ、アクセス・無害化措置の効果を最大限発揮することが困難となる。また、把握したサイバー攻撃の態様によっては、

アクセス・無害化措置ではなく、C2 サーバ管理者による任意のサーバ停止（テイクダウン）や、攻撃を受けているシステムのネットワーク接続からの遮断等、他の手段が被害防止の最適な方法となることも十分にあり得る。アクセス・無害化措置によって、安全保障上の懸念となるサイバー攻撃を未然に防ぐべきことは言うまでもないが、その効果を最大限発揮するためには、実際に対処を行う警察や自衛隊における平素からの訓練や人材育成と並んで、サイバー空間の状況把握及び情報連携の取組が徹底されなければならない。

更に、これらのサイバー空間の状況把握に基づく防御の取組に加え、国家全体のレジリエンスを高めるために、重要インフラ等への重大なサイバーインシデントが現に発生した場合についても準備を進める必要がある。具体的には、政府において、そのようなインシデントが実社会に与える影響、その影響がさらに波及する複合的事態まで念頭に対応を検討するとともに、重要インフラ事業者等も参加する演習の実施等の必要な取組を進めるべきである。

（3）サイバー脅威を抑止する力の強化

サイバー空間はその匿名性・隠密性により、攻撃者側に有利な競争環境となっている。この非対称性を緩和するために、攻撃者側にコストを課し、攻撃を抑止する取組が重要となることは従前から指摘されているとおりである。こうした攻撃者へのコスト賦課の取組において、短期的には適時適切な攻撃側の戦術・技術・手順に関する情報提供や、サーバ管理者と連携した任意のテイクダウン、法に基づくアクセス・無害化措置による攻撃基盤の機能低下等により、攻撃者に技術的・運用的コストを課すことが肝要である。同時に、国際協調の下、パブリック・アトリビューション等を行い、国際場裡での責任追及を進めることも、攻撃者に対してコストを賦課する上で重要な取組となる。これらの取組のいずれも、サイバー空間の状況把握を基礎とする取組であり、収集・分析されたサイバー情報が、これらの取組に活用されるべきことは絶えず意識されなければならない。また、中長期的には、国際場裡における議論を通じて、サイバー攻撃に関して我が国に有利な規範やルール形成を推進することも、抑止の観点で重要となる。我が国は、国連等の場でのルール形成に引き続き積極的に関与し、同盟国・同志国との政策調整・共同声明等を通じて、悪意ある行為主体に対する抑止の効果を強化することを目指し、もってサイバー攻撃の可能性を低減することを目標とすべきである。

これら各種の取組は、一度行えばサイバー攻撃者を抑止できるものではない。むしろ、サイバー攻撃者の抑止に当たっては、当該攻撃者に対し、継続的にコストを賦課し続ける必要がある。このためには、攻撃者の仕掛けるキャンペーンの各段階において、上記のような手段を組み合わせて対処し続けなければならない。国家サイバー統括室は、先述した攻撃者単位での情報の整理・蓄積に加え、司令塔組織として、どの

ような情報に基づき、どのようなタイミングで、どのような対処を行うことが、攻撃者へのコスト賦課として最も効果的になるのかについて、組織として経験を蓄積し、態勢を強化していくことが期待される。また、こうした攻撃者への対抗に加え、刑事訴追等が行われることで、より強力な抑止効果が期待できる。

（4）新しい技術への対応

デジタル技術の加速度的な進歩により、サイバー空間の脅威の技術的な高度化もまた加速度的に進んでいる。今般のサイバーセキュリティ戦略は策定後5年を対象としているところ、今後5年で急速な進歩が予想され、結果としてサイバー攻撃への悪用が見込まれる技術については、早急に対策を進めていくことが記載される必要がある。

例えば、量子計算機の発展により、従来の公開鍵暗号の安全性に中長期的なリスクが顕在化している。政府は、耐量子計算機暗号の技術的・社会的な利用可能性を十分に検討したうえで、政府機関における段階的移行計画を策定し、高度な量子計算機が実現した場合においても、暗号化を前提とする各種の行政サービスや技術等が問題なく運用されるようにするとともに、民間における耐量子計算機暗号への移行を後押しすることが求められる。

また、生成 AI を含む AI の高度化は、フィッシングメールの巧妙化を招き、また明確な悪意のあるコードを含まないマルウェアの作成を可能にするなど、新たな攻撃の手法を可能にする。こうした手法の一部は、ある国家を拠点とするサイバー攻撃者が、対立する国家を標的にする際に既に用いられており、今後サイバー安全保障において問題となると予想される。これに対し、AI を防御側でも積極的に活用し、自動かつ高度な異常検知を社会実装していく必要がある。

（5）サイバーセキュリティ分野への危機管理投資の促進等

高度なサイバー脅威等に対応し、我が国のサイバーセキュリティを確保するためには、セキュリティが堅牢な情報システム（セキュアなクラウドを含む。）や、脅威への対処に必要な資機材の導入・整備を早急に進める必要がある。

また、国家安全保障の観点から、我が国のサイバーセキュリティ能力を中長期的に成長させていくためには、国内のサイバーセキュリティ関連産業を育成し、その供給能力を抜本的に強化する必要がある。そのため、サイバーセキュリティ分野に対する大胆な危機管理投資等を促進してサイバーセキュリティ人材の育成・確保やサイバーセキュリティ関連技術の研究開発等を戦略的に推進するとともに、国内企業の技術力・競争力を強化し、海外展開を視野に入れた優れた国内製品・サービスを創出する取組が必要である。

4. 結語

我が国周辺の安全保障環境がますます厳しく複雑になる中、我が国のサイバー安全保障の必要性も高まっている。国家背景のサイバー攻撃アクターは、以前よりも更に高度な攻撃手法を獲得しており、キネティックな手段との連携の可能性も考えれば、我が国がこれらの攻撃者に対し、能動的に対処することは不可欠である。こうした背景のもと、法の成立や、内閣サイバー官及び国家サイバー統括室の設立も含む、我が国の新たなサイバー安全保障体制がスタートしたところである。他方、こうした体制においても、従前どおりサイバー空間の状況把握が防御や抑止の基礎となることは変わらない。法によって政府に付与された権限は、状況把握力・防御力・抑止力の関係性を踏まえ、それぞれの力を高めるために運用されなければならない。このような状況認識に立ち、関係機関がそれぞれ必要な取組を全うすることが、我が国のサイバー安全保障の確保のために最も重要なことである。