資料４－１

○　アクセス・無害化

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措置のうち、重大なサイバー攻撃について未然に対処するための攻撃者サーバ等へのアクセス・無害化についての権限付与*について述べる。

＊同戦略では「侵入」・無害化と表現されているが、本提言では、ネットワークにおける活動であることをより客観的に示す表現として、「アクセス」の語を採用する。

＊同戦略において、能動的サイバー防御は、武力攻撃には至らないものの、国、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、これを未然に排除し、また、発生した場合の被害拡大を防止するために導入するものとされているところ、この項の「アクセス・無害化」についても、武力攻撃事態に至らない状況下における対処を念頭に置いている。

①サイバー空間の特徴を踏まえた実効的な制度構築の必要性

近年、サイバー攻撃は巧妙化・高度化している。具体的には、サイバー攻撃は、複雑化するネットワークにおいて、国内外のサーバ等を多数・多段的に組み合わせ、サーバ等の相互関係・攻撃元を隠匿しつつ敢行されている。また、ゼロデイ脆弱性の活用等により、高度な侵入が行われるほか、侵入後も高度な潜伏能力により検知を回避するなど、高度化している。このため、サイバー攻撃の特徴としては、現実空間における危険とは質的に異なり、**実際にある危険が潜在化し認知しにくい**ということが挙げられる。また、潜伏の高度化等により、**攻撃者の意図次第でいつでもサイバー攻撃が実行可能**であるとともに、ネットワーク化の進展により、**一旦攻撃が行われれば、被害が瞬時かつ広範に及ぶおそれ**がある。

もとより、これまで、政府等においては、サイバー攻撃に対して防御側での対処のほか、攻撃側への対処として、サーバ等の管理者と連携した任意のテイクダウン、パブリックアトリビューション、攻撃手口の公表等を積極的に行ってきたところであるが、上記のような状況のほか、外国においてもアクセス・無害化の取組が行われていることなどを踏まえれば、これまでの取組に加え、**重大なサイバー攻撃による被害の未然防止・拡大防止を目的とした、攻撃者サーバ等へのアクセス・無害化を行う権限を政府に付与することは必要不可欠であり、我々が価値創造するための安全なサイバー空間を守る観点から極めて重要な取組**と考えられる。

新たな権限を制度化するに当たっては、**既存の法執行システムとの接合性や連続性を意識**しつつも、**サイバー空間の特徴を踏まえた実効的な制度とする必要**がある。**新たな制度の目的が、被害の未然防止・拡大防止であることを踏まえると、インシデントが起こってから令状を取得し、捜査を行う刑事手続では十全な対処ができないと考えられ、新たな権限執行には、緊急性を意識し、事象や状況の変化に臨機応変に対処可能な制度とする必要がある。**法形式としては、具体的な権限執行法（作用法）として構想されるべきものと考えるが、個別の要件を法定し、あらかじめ具体的な無害化の手法を法律上にメニューとして用意するという形の法制度ではなく、目前に存在する危険に対して、**状況に応じた危害防止のための措置を即時的に実施することを可能としている警察官職務執行法を参考とすべきと考えられる。**その際には、サイバー空間の特性を踏まえた必要な調整が図られるべきであるとともに、法制度のみならず執行に係る全体のプロセスやシステムも参考とすべきと考えられる。

また、平時と有事の境がなく、事象の原因究明が困難な中で急激なエスカレートが想定されるなどのサイバー攻撃の特性から、制度全体としては、事態を細かく区切り事態を認定するという従来の事態認定方式ではなく、**平素から我が国を全方位でシームレスに守るための制度の**

構築が必要と考えられる。

②措置の実施主体

サイバー空間の脅威は深刻であり、これへの対処は喫緊の課題である。先に述べたように、これまでに様々な主体が様々な取組を実施してきたところではあるものの、新たな取組であるアクセス・無害化の措置の性格や、新たな執行制度を既存の法執行システムとの接合性や連続性をもつものとして構成すべきとの考え方を踏まえ、権限の執行主体は、現に組織統制、教育制度等を備え、サイバー脅威への対処に関する権限執行や有事への備えを行っている、警察や防衛省・自衛隊とし、その保有する能力・機能を十全に活用すべきである。これらの組織が執行権限の主体となることについては、諸外国において、同種のアクセス・無害化を担っている主体がインテリジェンス機関、軍、法執行機関であることを考慮すれば、国際的なスタンダードにも合致するものである。

③措置の対象

サイバー脅威の深刻性と対処の困難性は、質的な要因と量的な要因の両方に起因するものである。②の措置の実施主体の能力や機能の向上を強力に進めて行くことは極めて重要であるが、その上でもなお能力やリソースが限られることを勘案すべきであり、措置を講じる事案の優先順位を考える必要がある。具体的には、アクセス・無害化の対象としては、社会全体の機能維持（レジリエンス）と安全保障能力の基盤確保という安全保障上の必要性を念頭に、国民の生命・安全に関わる重要インフラや有事において自衛隊や在日米軍の活動が依存するインフラ等に対するサイバー攻撃を重点とすべきものと考えられる。

④アクセス・無害化と国際法との関係

サイバー脅威は国境を越えて発現する。攻撃主体や攻撃に用いられるサーバなどの機器が海外に所在し、国境を越えて我が国に重大なサイバー脅威をもたらす場合においては、新たな措置は国境を越えて実施され得るものであるところ、アクセス・無害化と国際法との関係を整理する必要がある。

この点、アクセス・無害化の対象サーバ等が海外に所在した場合において、同措置が当該国に対する主権侵害に当たるか否かは、個別の措置についてどういう影響が生じるかを踏まえた上で、措置の目的、あるいは相手方の対象の性質を加味して個別具体的に判断される必要があり、どのような行為が他国の主権侵害に当たるかをあらかじめ確定しておくことは困難である。

このため、アクセス・無害化の国際法上の評価について一概に述べることは困難であるが、当該措置がそもそも国際法上禁止されてない合法的な行為に当たる場合も考えられるほか、他国の主権侵害に当たり得るものである場合であっても、国際法上の違法性が阻却される場合がある。

その違法性阻却事由としては、「対抗措置（Countermeasures)」や「緊急状態（Necessity)」（※）が考えられるが、「対抗措置（Countermeasures)」については、相手国の先行する違法行為の存在や被害の程度との均衡性を証明しなければならないなどの点を踏まえると、実務上、

援用する違法性阻却事由としては、「緊急状態（Necessity）」の方が援用しやすいものと考えられる。

※　対抗措置（Countermeasures）

国際違法行為により被害を受けた国が、その限りにおいて、当該行為の責任を負う相手国に対して、その行為を中止させ、自国が受けた被害の回復を図る際に、被った被害と均衡する措置を一定の条件の下で措置をとる場合に違法性阻却が認められるという考え方

※　緊急状態（Necessity）

当該措置が、重大かつ急迫した危険から不可欠の利益を守るための唯一の手段であり、当該行為が相手国又は国際共同体の不可欠の利益を深刻に侵害せず、状態の発生に寄与していない場合に違法性阻却が認められるという考え方

アクセス・無害化に関する国際法は未だ発展途上である。今後我が国が目指す新たな措置の制度導入とその執行は、我が国の国家実行として国際法規則の形成に影響を与える事項であることから、サイバー空間での活動の特徴を踏まえ、慎重な法制度の発展が図られるべきものと考える。

⑤制度構築に当たっての留意点

アクセス・無害化の制度については、サイバー空間の特徴を踏まえた実効的なものとする必要があるが、そのほか、制度構築に当たって留意すべき点は以下のとおりである。

まず、アクセス・無害化は、上述のサイバー攻撃の特性を踏まえ、実効性確保の観点から、専門的能力を有する者により、具体的な状況に応じ臨機応変な判断で適切な手法が選択され実施されるべきものと考える。政治によるマイクロマネジメントと権限行使の主体への白紙委任の双方を避ける観点から、政府としての適切な方針の下で、専門的能力を有する者らによりオペレーションを回せるようにする必要がある。また、こうした措置は、比例原則を遵守し、必要な範囲で実施されるべきである。

加えて、こうした政府のアクセス・無害化の取組には、国民の理解を得ることが重要である。そのためには、公正性・透明性の確保、プライバシー保護との両立が不可欠であるところ、サイバー攻撃における緊急性・切迫性等を踏まえた実効性のある対処の観点から、独立機関による事前の審査や承認によらずに臨機応変な対応を行うことが求められることを考慮しつつも、透明性や公正性の担保、プライバシー保護の観点から、アクセス・無害化の適正性を確保するための枠組みを検討する必要がある。この点については、既存の法執行システムとの整合性も考慮しつつ、措置の迅速性とその公正性・適切性の両立の観点から、例えば、措置の実施について幹部職員が関与することや独立した立場から事後的な監督を受けることなどが考えられる。

さらに、仮に、結果的に関係のないサーバ等を無害化の対象にしてしまった場合、不正プログラムを消去したことによってそのサーバ等自体が使用できなくなってしまった場合など、意図せず、措置を行うことで達成しようとしていたものとは異なる結果に至った場合に、どのようなセーフティーネットがあるのかについても十分検討しておく必要がある。

⑥運用面の留意点を含めた今後の検討課題

サイバー安全保障分野での対応能力を向上させるという目標の実現に向けては、アクセス・無害化に係る制度の構築に加え、アクセス・無害化を効果的かつ実効的なものとしていくため、その運用においても以下の点に留意すべきである。

まず、アクセス・無害化の実施に当たっては、**平素からの情報収集やサイバー空間に限らないオールソースデータの蓄積・活用を含む総合的な情報収集が必要**であり、その際には、**官民協力・国際協力も重要**となる。平素からの情報収集においては、公開情報の収集に加え、**警察、防衛省・自衛隊やその他の関係機関等による多様な能力を活用することを前提とし、サイバー空間に限らず、必要なインテリジェンスを収集・分析し、活用していくことが重要**である。

また、アクセス・無害化を優先的に実施すべき事象か否かを判断するに当たっては、攻撃グループにも、国家を背景とする高度な攻撃を行うグループからそうでないものまで存在することから、アクセス・無害化の権限がより効果的に運用されるには、攻撃グループの属性を把握することが必要である。

加えて、攻撃側のインフラは多重的なものであり、インフラが第三国に存在する場合もあるほか、正規のサービスの悪用やずさんな管理のサービスのように中間地帯があるところ、関係国を含む多様な主体との連携も重要となる。

このほか、アクセス・無害化については、臨機応変な対応を可能としつつも、政府としての適切な方針の下で行われる必要がある。特に強度の高い措置の実施を選択するに際しては、政治、外交等の他の枠組みの可能性を追求し、それを踏まえた**総合的な判断が求められるとともに、その判断の下で実施主体が措置を講ずることが必要となる場合もあることから、政府においてリーダーシップを発揮するための司令塔の存在が極めて重要**となる。

このように平素の情報収集からアクセス・無害化に至るまでには、司令塔や措置の実施機関を始め、関係機関が相互に連携する必要があると同時に、迅速かつ臨機応変な対応を必要とするアクセス・無害化の実効性を確保するため、関係機関が有機的かつ円滑に連携することが可能な組織体制の整備を図っていく必要がある。

さらに、今後の検討課題として、アクセス・無害化を実施していくに当たっては、多岐にわたる高度な専門性を有する人材の育成・確保に取り組んでいく必要がある。

司令塔となる組織に関していえば、地政学の分析や通信ネットワークの分析の専門家、ネットワークの中を通る情報のアナリスト、無害化に関する技術的理解を有する人材等、**多様な機能・人材が集まり、総合力を発揮することにより、状況の把握と予測を行うことができ、無害化を含むサイバー脅威への対処の戦略ができあがることに留意し、司令塔たる組織にはそのために必要な人材・能力を構築すべき**である。

また、アクセス・無害化の実行組織に関していえば、**個別のアクセス・無害化のオペレーションは、専門的能力を有する者らにより回していくことが必要**となるが、効果的なアクセス・無害化を行うためには、**極めて高度な専門性を有する人材の育成が必要不可欠**である。

こうした人材の育成・確保に当たっては、**官民交流の中で人材を教育していくことも含め、全体としてどのように人材を育成していくのか検討を進めていく**ことが求められる。