サイバー安全保障分野での対応能力の向上に向けた有識者会議
アクセス・無害化措置に関するテーマ別会合（第３回）
議事要旨

1. 日時

令和６年８月 27 日（火）16 時 00 分から 16 時 45 分までの間

2. 場所

オンライン開催

3. 出席者

（有識者）

遠藤	信博	日本電気株式会社特別顧問
川口	貴久	東京海上ディーアール株式会社主席研究員
酒井	啓亘	早稲田大学法学学術院教授
佐々江	賢一郎	公益財団法人 日本国際問題研究所理事長
篠田	佳奈	株式会社 BLUE 代表取締役
土屋	大洋	慶應義塾大学大学院政策・メディア研究科教授
野口	貴公美	一橋大学副学長、法学研究科教授
丸谷	浩史	株式会社日本経済新聞社常務執行役員 大阪本社代表
村井	純	慶應義塾大学教授
山岡	裕明	八雲法律事務所弁護士
山口	寿一	株式会社読売新聞グループ本社代表取締役社長
吉岡	克成	横浜国立大学大学院環境情報研究院/先端科学高等研究院教授

4. 議事概要

（１）事務局説明

事務局より、これまでの議論を整理して作成したアクセス・無害化措置に関する提言（案）について、資料を用いて説明が行われた。

（２）討議

各有識者より、事務局説明を踏まえ、アクセス・無害化措置に関する提言（案）について、以下のような発言があった。

○　第１に、29―32 行目について、今回の措置を被害の未然防止・拡大防止の目的で実施するとしても、当方の措置がエスカレーションを促してしまうこと、そこから事態が

拡大してしまうことも想定され、例えば、攻撃側から反撃してくること、その結果としてサイバー空間に収まらないこともあり得るのではないか。そのような場合には、国家安全保障会議（NSC）や国家安全保障局（NSS）等の関係する組織との連携が重要であり、こうした状況も事前に想定した上で、連携の在り方について検討しておく必要がある。

○　第2に、60―62行目の措置の対象について異論はないが、実際問題として、どこまで普段の観察の対象としておくかは難しい課題がある。どこまで平素から観察することができるかは、人員の確保状況、人員の個々の能力、対象企業が協力的かどうかにも依存する。

例えば、経済安全保障推進法では、その対象を重要インフラとしつつ、港湾は対象としていなかった。しかしながら、名古屋港の事案を受け、急遽その対象に含めることとした。その意味でも何を対象とするのかは結構難しいのではないか。

また、国民の生命・安全のみならず、国民の財産についての取扱いにも留意する必要がある。今回は、国民の生命・安全に絞るということもあり得るが、例えば、金融システムがサイバー攻撃を受けた場合は対象とならないのかとの意見が出てくることも想定される。少し頭の体操をしておくことが重要である。

○　第3に、77―81行目の緊急状態について、他の委員からも指摘されているような警察業務に照らした場合、例えば、犯罪の現場で、拳銃らしきものを手に持っている容疑者に対して対応すべく、警察官が発砲した場合には大きな議論となると思われるが、同様にサイバー攻撃への対処についても、その場では緊急に見えたが、実際には緊急ではなかった場合ということもあり得る。自衛隊がPKO活動を行うときにも、発砲が許容される状況について常に議論されてきた。国会でも同様の議論になり得ることを頭に入れておく必要があるのではないか。

○　49―50行目の措置の主体について、これまで実施主体を「警察、防衛省・自衛隊」とワンフレーズで議論されてきたが、もし役割分担があるのであれば、今後の考え方として記載することも一案ではないか。警察は平素から、防衛省・自衛隊は有事を念頭に、公共の秩序の維持の観点から、必要に応じて措置を講じることなどが考えられる。ただし、事態認定方式を避け、幅広いグレーゾーンに対処する観点から、警察が対処する状況、自衛隊が対処する状況を明確化することは避けるべき。

○　本文書は諸外国政府や国家支援のサイバー攻撃グループに対する宣言政策の側面を有するとして理解している。今回の検討対象では（ア）官民連携、（イ）通信情報の利用、（ウ）アクセス・無害化措置は全て重要だが、その中でも特に、アクセス・無害化措置に関する提言は最もシグナリングの要素が強い。

○　措置の対象については重点化することが重要である一方、これに限定されないこと、幅広いインフラや対象を含む点には言及する必要があると思う。また、我が国が法的確

信のある国家実行としてアクセス・無害化を実施するという点について、日本が国際規範を作るという意識の表れと理解しているが、そうであれば、国連憲章を含む既存の国際法はサイバー空間にも適用され、サイバースペースの新しい規範を作るという日本の姿勢を記載・強調すべきではないか。加えて、今回の措置は平時から行うものと認識しているものの、武力攻撃未満・グレーゾーンから実施していくという点については、可能な範囲でくり返し記載すべきではないか。

○　35－36 行目の「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」という記載について、アクセス・無害化の制度を構築するため、即時強制の権限を行政作用法で定めて対処するという考え方自体は妥当。

○　しかしながら、現行の警察官職務執行法は、警察官個人の現場判断で権限を行使する法律といった印象が強い。他方、今回の措置に関しては、110―111 行目には「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」、134―135 行目には「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」、140～141 行目には「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」とされている。

○　これらを踏まえると、これから導入しようとしている新たな執行制度は、現行の警察官職務執行法が定めるような警察官個人の判断で行う職務質問等とは相当程度異なり、警察、防衛省・自衛隊という組織で判断を行い、関係機関の日頃からの連携の下に実施されるものと考えている。

○　このため、「警察官職務執行法を参考とすべきと考えられる」という記載にとどめるのではなく、例えば、幹部職員が関与することや警職法がこれまでも災害時の避難措置や切迫した事態での犯罪予防に用いられて機能してきたということを補足することについて、検討した方がよいのではないか。

○　アクセス・無害化の制度構築に当たって、警職法の改正も選択肢の１つとなるとすると、それ自体は妥当と考えているが、現在の記載内容では、人によっては、唐突感を持たれるように思われるため、丁寧に記載することが求められるのではないか。

○　第１に、35―36 行目の警職法に関する記載の後の箇所について、ここで書いてあるように、「法制度のみならず、法執行に係る全体のプロセス・システムも参考とすべきと考えられる」という部分について、これも大変重要であることから、当該箇所を強調（太字・下線）していただきたい。措置自体も重要だが、措置を講じた後の手続・手当も同様に極めて重要、ということである。

○　第２に、幹部職員の関与や独立した立場からの監督について、措置自体が極めて高度な専門的知識や判断を要するものであるのであれば、その措置の適正性を監督する者

についても、実施者と同等、またはそれ以上の専門的・技術的な判断能力を有していることが求められるということに留意する必要があるだろう。

○　法制度の構築に際しては、「事後的な監督」と表現されている「監督」の内容についてよく検討する必要があるのではないか。「監督」には、①第三者が実施者とは異なる立場で独立・中立の立場から監視するというものもあれば、②実施者の上位に在る者が、下位にある者の実施の在り方を上級機関として統御・コントロールするというものもあり得るのではないか。サイバー空間における無害化に関する「監督」に関しては、後者としての管理・統御の場面が多くなると考えられるのではないか。

○　「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」という記載は、能動的サイバー防御に限定しているものと理解しているが、サイバー空間の状況がリアルな状況と連動した場合の対応についても整理しておくと、今後の措置を検討する上で有効ではないか。

○　「警察官職務執行法を参考とすべき」という記載について、防衛省・自衛隊は本来、個人の判断で権限を行使する組織ではないため、仮に、サイバー空間の状況がリアルな状況と一体化した場合、防衛省・自衛隊が、どのように判断を行い、権限を行使するのか、整理しておくとよいと思料。

○　55 行目の「措置の対象」について、サイバーセキュリティに関する守備範囲の問題が 1 つあり、「国民の生命・安全に関わる重要インフラ」という限定をかけていることに対して多少の不安がある。

　サイバー空間あるいはデジタル技術の守備範囲が非常に広範で、また国全体あるいは国土全体に関わる様々なインフラも含めた活動、産業、地域のサイバーセキュリティに対する脅威がある中、サイバーセキュリティに関する守備範囲も、現在は、「国民の生命・安全に関わる重要インフラ」に限られず、「国土」、「国の機能」などを含め、もっと拡大しているというのが実態ではないか。

○　また、「自衛隊や在日米軍の活動が依存するインフラ等」の記載について、防衛という意味から考えるとそのとおりだと思うものの、今やこの国のデジタルアセットを国自体が持っているという可能性が出てくる中で、国が所有する、また、国が運用するデジタルアセットに対するサイバーセキュリティの状況をどのように捉えるのかという意味での措置の対象の議論は重要となる。

○　第 1 に、123―125 行目の「平素からの情報収集」について、官民協力、国際協力、さらに「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」とされているが、それぞれの国家機関が収集した情報について相互に必ず共有を行うということは言うまでもなく、官官での協力ということは当然のこととされていると

は思うが、あえてここで申し上げたい。

○　第２に、149―151 行目にかけての人材育成について、司令塔たる組織に必要な人材の能力を構築すべきであるということ、また、アクセス・無害化の実行組織に必要な専門性を有する人材を育て上げなければならないことは極めて重要であり、正しい認識。

　他方で、この２つの人材を、相互交流という形式を含め、どのように活かしていくかという視点が重要。すなわち、司令塔を担う人材もまた専門的な知識が必要である以上、それぞれのルートから入ってきた人材がそれぞれの役割を担っていくといった棲み分けのようなものが固定されてはならないであろう。それぞれのルートを独立させていればよいとの認識なのであれば、ややミスリーディングになるのではないか。

○　その他、他の委員から指摘のあった、国連憲章を含む国際規範が適用されるということを前提として活動を行っていくことを明記したほうがいいのではないかという点については、そのとおり。まっさらなところで活動を行い、その内容が実行として醸成され、後の法形成につながっていくということだけではない。内外に安心感を持たせるためにも、多くの部分はやはり現行の国際法規範が適用される限り、それに則って活動していくということを前提としているということに言及するということは一案と思料。

○　提言素案で用いられている「緊急性」という概念は、既存の法執行システムとの接合性・連続性、「緊急状態」という国際法との整合性、担当者の臨機応変な対応という観点から、極めて重要なポイントであり、要件にも関わるものと認識。

○　他方で、サイバー攻撃の特殊性として、必ずしも「緊急性」を伴わないものも想定されるのではないか。例えば、2024 年８月に 100 台のボットを把握し、調査の結果、そのボットには 2025 年１月１日に同時に DDoS 攻撃を仕掛けるようプログラムが組まれていたような場合、半年後に攻撃するプログラムであるため、緊急性はないものの、把握した時点において対処する必要性があるだろう。この点、「緊急性」というものが必須の要件だとすると、現場での対応を躊躇せざるを得ないのではないか。また、攻撃者側に「緊急性」の要件を満たさない限り無害化されないとの認識が形成された場合には、抑止力が弱まってしまうのではないかとの懸念もある。

○　このように、あらゆる面から「緊急性」というのは重要な要件である一方、「緊急性」を過度に強調しすぎること、必須の要件とすることについては、サイバー攻撃の特殊性を踏まえると、気になった。

○　「措置の対象」の記載内容について、「国民の生命・安全に関わる重要インフラ」は重要であり、何らかのリソースを集中させなければいけないという観点も理解するが、措置の対象をもう少し広げることを検討してもよいのではないか。

○　また、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ため、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ところ、実際に行った対応がどういうものであったかということを事後でも良いので、専門的な観点で検証をしっかりするということが極めて重要。111 行目の「独立した立場から事後的な監督を受けること」については、「独立した立場」という用語が、組織を意味しているのか、それとも機能を意味しているのか、表現が若干曖昧であるとの印象を受けたので、記載がもう少しできるようであれば、検討していただきたい。

（以　　上）