

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1回）
議事要旨

1. 日時

令和6年7月1日（月）10時から12時までの間

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）河野国務大臣挨拶

- 本日は御多用のところお集まりいただきまして誠にありがとうございます。本日は、アクセス・無害化措置に関するテーマ別の会合となります。実効性、効果的に対処するという観点から、政府としてどのように事案を把握し、アクセスあるいは無害化措置を含め、どのような措置・対応を講ずるべきかをどう判断したら良いのか。さらに、措置の検討に当たっての留意すべき点などについて集中的に御議論をお願いしたいと思います。
- それぞれの皆様のお立場からの知見を発揮いただいて、新しい制度整備の方向性について闊達に御議論をお願いしたいと思います。どうぞよろしくお願いいたします。

(2) 事務局説明

事務局より、サイバー攻撃の現状と対策について、【資料2】を用いて説明があった。

(3) 討議

有識者より、事務局説明を踏まえ、以下のような発言があった。

- 「攻撃インフラ」の構成要素として末端の通信機器や一般利用者の機器からなる「ボットネットワーク」が存在することは確かであると思われるが、それに加えてクラウド、ホスティングサービスも利用、悪用というのも非常に多いと思っている。その際、例えば、漏えいしたクレジットカード情報を勝手に利用して、これを契約して、占有的に利用した事例もあると承知している。
- また、有償・無償のようなものがあるが、間に色々なホストを介して通信をするためのプロキシサービスが存在しており、例えば、レジデンシャルプロキシと呼ばれる、わざわざ家庭のインターネット回線を提供するというのをうたったものもあるが、実際は脆弱な機器を悪用してそのサービス自体を提供しているなど、サービス自体も悪意を持っている可能性もあるとも言われている。さらには、脆弱なシステム、機器を探索し、侵入を行い、その先の環境の下調べをした上で、アクセス権限を別の攻撃者に売る、アクセスブローカーと呼ばれる存在もあると理解。
- このように、攻撃側のインフラは、攻撃者が直接的に管理・運用するコア部分に加えて、それを取り巻く関連のリソース、サービスから成り立つ多重的なものと理解。そのため、攻撃者とそれ以外という二値ではなく、その間には、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、様々なグラデーションの中間地帯があると思われる。
- このような中間地帯での攻防も重要。全てが攻撃グループによる完全な支配下にあるものではないので、一部情報収集の余地もあり、サービスによっては対策に協力的な場合もあると思われる。日常的なコミュニケーションにより、どこのプロバイダー等が協力的なのかを見極め、どこから先をアクセス・無害化措置というような強い対策を取らなければならないのかという境界を明らかにする必要がある。
- また、攻撃者のグループも、国家を背景とする高度な攻撃を行うグループから、ティーンエイジャーの小遣い稼ぎのような攻撃もある。そうしたものの区別を早い段階でしておくことで、より適切な運用に資するのではないか。攻撃グループのアトリビューションが必要。
- 他方、アクセス・無害化措置の実施主体には、相当な情報と権限が集約されることとなるため、実施主体の活動の妥当性や正当性を厳しく審査、判断する別組織が必要であり、その別組織にも専門性と情報へのアクセスが必要と思われる。

(4) 警察庁からのプレゼンテーション

警察庁より、警察におけるこれまでの取組等について、【資料3】を用いて説明があった。

(5) 防衛省からのプレゼンテーション

防衛省より、防衛省・自衛隊におけるこれまでの取組等について、【資料4】を用いて説明があった。

(6) 討議

有識者より、事務局による説明、警察庁及び防衛省からのプレゼンテーションを踏まえ、以下のような発言があった。

- サイバー空間における措置には、C N A (Computer Network Attack)・C N D (Computer Network Defense)・C N E (Computer Network Exploitation) が挙げられる。Attack と Defense の中間的な位置付けとして Exploitation が存在するが、C N E は全ての国家にとって必要なツールであるなどの指摘もある。
- Exploitation は辞書的な意味では、利己的な利用ということであるが、様々なシステムを上手く使うことにより、様々な情報を収集することが可能であり、公開情報のみの収集には限界。例えば、政府によるダークウェブにおける情報収集やゼロデイ脆弱性の購入等にも踏み込んでいかなければ、国家安全保障戦略が求める欧米主要国と同等以上という目標を達成するのは難しいのではないかと。
今までできたことを乗り越え、C N E の分野を広げていき、これを合法的にできるかどうかということが重要ではないか。そのための法整備を進めていただきたい。
- 措置には、事前の予防に当たる作用から何か起こったときの措置まで幅広い措置が含まれ得るものであり、整理し切れない領域もあり、非常に難しい議論。ただ、作用法にしていくという視点からは、①要件を書ききり、その要件判断を経て、命令により実施する方法、②司法・準司法手続を経て許可や令状の仕組みを導入し、許可や令状を根拠に権限行使を行う方法、③警察官職務執行法のように、義務を課するというルートを取る時間がない場合に即時に執行するという方法の、大きく3つのやり方が考えられるように思われる。
- 警察庁に対する質問として、無害化措置が実施できれば被害を防止することができた可能性があったと説明された事例について、これは許可・令状を得て措置を実施することで対応可能であったと考えるか、それとも、法執行官が即時の判断で実施することで対応する必要があったと考えられるのか、お伺いしたい。
- 事務局に対する質問として、諸外国の制度の例が示されていたが、英国・カナダにみる大臣による許可や、豪州にみる司法・準司法的手続のほかに、諸外国には、許可や

令状を介さずに、つまり、即時強制に近い仕組みが存在していそうかどうか、お伺いしたい、また、許可を得て措置を講じるという手法は、全体の対応のなかでどの程度のウエイトを占めるのかといった点について、情報があれば教えていただきたい。

警察庁より回答

- 紹介した事例への対応の選択肢は様々なものがあると思われる。ケースバイケースで判断・対処する必要があると思料。また、先ほど言及された警察官職務執行法は、一定の要件の下で、即時強制を含む必要な措置を執る権限を警察官に付与する法律であるが、これがサイバー攻撃の実態に適合するのかどうか、また、何がどこまで対応可能なのか、内閣官房を中心に検討を進めているところ、警察としても、できること・できないことの整理に貢献してまいりたい。

事務局より回答

- 英国や豪州では、許可・令状制とされている一方、緊急の場合には口頭による許可や代理の者による許可等、緊急時にも対応できるような措置の規定が設けられている。他方、我が国にいう即時強制のような制度が存在するか否かは確認する必要があると考えているが、ウエイトについては、情報機関が実施するものについては、許可制度が多い印象。

(7) 有識者からのプレゼンテーション

早稲田大学法学学術院酒井教授より、国際法との関係について、【資料5】を用いて説明があった。

(8) 討議

有識者より、事務局、警察庁、防衛省及び有識者からのプレゼンテーションを踏まえ、以下のような発言があった。

- 第1として、サイバー空間のセグメントは、必ずしも国ごとにできているわけではなく、攻撃側・被害側ともに必ずしも同じ国に属しているわけではない。また、攻撃側のサーバ等もネットワークのどこに位置付けられるのか明確でなく、フローティングしており、サイバー攻撃の技術的な複雑さが増しているのが実情。
- また、サイバー空間では、基本的には送信側のセグメントと受信側のセグメントで構成されているものの、通信を中継するネットワークも存在する。インシデントが発生した場合に、攻撃側の追及を行い、アクセス・無害化措置を行っていくことになるが、サイバー攻撃を実施する国の特定には不確実性をはらむため、中継ネットワークが所在する国との連携が重要。
- 第2として、アクセス・無害化措置を実施する体制作りを進める上で、極めて高い専門性を有する専門家の協力が必要不可欠であり、その活用が必須。他方、こうした専門家が政府のアクセス・無害化措置に協力するに当たって危険に晒されることもあ

り得るため、こうした協力をする人材を保護する、プロテクションシステムが重要であり、こうしたシステムが政府に協力するインセンティブにもなり得る。

- アクセス・無害化措置の検討に当たっての留意事項のうち、「第三者への影響等」について、国民の皆さんの御懸念は、財産権やプライバシー権の侵害が挙げられるのではないかと懸念は、サイバー攻撃があたかも何でも実現可能なものと受け止められているのではないかと推測する。
- しかしながら、サイバー空間でできることは無制限ではない。例えば、IPアドレスがわかれば簡単にアクセスできるというものでもなく、仮にアクセスできたとしても常に細やかに端末を遠隔操作できるというものでもない。技術的な制約が多い。
- そのため、技術的にできること・できないこと、できることの中でもすること・しないことを整理し、具体的なユースケースで検討することが重要ではないか。
- その意味では、本日紹介のあった事例は、サイバー攻撃に利用されている端末の内部をいたずらに探索しているわけではなく、プライバシー権の侵害度合いは限りなく低いのではないかと、また、マルウェアのみを無害化させ、他の機能に影響を及ぼす可能性も非常に低いため、財産権に対する侵害度合いも低いのではないかと。こうしたわかりやすい事例を積み重ねて議論していくことが重要。
- 本日の議論のテーマのうち、外国所在のサーバ等に対する措置と国際法との関係に関連して、「アクセス・無害化措置」はワンフレーズとして扱われているが、「アクセス」と「無害化措置」との間には大きな壁があり、本質的に性質が異なるものと理解。
- すなわち、「アクセス」は、いわゆるインテリジェンス活動、あるいは、Exploitationとして位置付けられる。国際法においても、データへのアクセスや参照・複写については必ずしも主権侵害ではない可能性等について言及があったように、「アクセス」と「無害化措置」の国際法上の評価はケースバイケースであるものの、双方は異なる考え方、あるいは、異なるプロセスが必要ではないか。
- 他方、「アクセス」と「無害化措置」は本質的に異なると理解する一方、両者の違いは紙一重とも言えると思われる。アクセスの延長に無害化措置があるとすれば、国際法の観点から、「アクセス」と「無害化措置」にどのような境界があると言えるのだろうか。単に情報を複写することと権力的作用を及ぼすことの閾値、両者の境目は何か。
- また、本日の議論のテーマのうち、どのような事案に対処すべきかという点については、国際法上の緊急避難と見なされるような事例、すなわち、重要インフラに対する妨害や破壊工作といったものが当てはまるものと思われる。これに対してアクセス・無害化措置を講じるためには、広範なアクセスが必要であるとともに、通信情報の活用が前提となると考える。

- 「アクセス」と「無害化措置」が本質的に性質が異なるというのは重要な指摘。他方、国際法の観点から、「アクセス」と「無害化措置」の区別は難しい。しかも、それぞれにおいて具体的な措置が関係国の主権侵害行為となるかも問題となる。
- 例えば、国内に正当なアクセス権限を有する者があり、当該者への捜査に当たって、海外のサーバに保存されたデータにアクセスし、単にこれを参照するだけであれば、権力的作用を伴うか伴わないかがメルクマールとなり、そのため相手国の領域主権の侵害とはならない。
- 一方、「無害化措置」は、データを参照するに止まらず、必要な措置を講ずるものである点で「アクセス」とは一応区別できるものの、その影響の程度に応じて主権侵害にならないということも理論的にはあり得るであろう。技術的な観点からの検討が必要だが、そうであるなら領域国側の主権侵害の主張に対しては抗弁できる。
- いずれにせよ、両者を明確な基準により区分することは困難であり、複合的な考慮要素を加味して、ケースバイケースで判断するほかないだろう。

- 警察や自衛隊がこれまでも様々な取組を実施しているところ、現場の視点から、何を実施することを理想としているのか、具体的に何がしたいのかを明確化・具体化する必要。無害化措置のイメージが臆気であり、各省庁がイメージする無害化措置と議論に参加する者がイメージする無害化措置が一致しているのかが判然としない。

- アクセス・無害化措置と国際法との関係について、「タリン・マニュアル」の話があったが、このように、国際的な議論の結果として、ルールを形成していくことは有用ではないか。
- 実施主体に求められる要素に関連して、警察官職務執行法の例を挙げたが、これをサイバーの領域にそのまま適用すべきだという議論をしたいわけではない。ただ、これまで、実際に現実空間において通用し、現場における実力行使を可能とする法的仕組みとして、警察官職務執行法は非常に参考になるのではないかと考えている。
- 警察官職務執行法を参考とするに当たっては、その背景や周辺にある警察制度、警察官の教練、日常の警らの活動、様々な制度の中で、日本の社会が警察官による即時執行を受容している（即時執行が可能となっている）という視点が重要と考える。
- サイバー空間においても、無害化措置という手法のみ（単体）ではなく、連続するプロセスにおいて段階的な権限行使をしていく中で、無害化措置というものをどう位置付け、どう正当性を担保していくのか、前後の一連のプロセスのなかで、手続も含めて議論していくべきではないか。

以上