

令和3年10月26日

令和3年度サイバーセキュリティ政策会議（第2回）

発言要旨

1 開会

2 事務局説明「令和3年度サイバーセキュリティ政策会議報告書骨子案」

【事務局から、「令和3年度サイバーセキュリティ政策会議報告書骨子案」について説明】

3 事務局説明「情報技術解析部門の取組」

【事務局から、「情報技術解析部門の取組」について説明】

4 事務局説明「海外からのサイバー犯罪に対する捜査の課題」

【事務局から、「海外からのサイバー犯罪に対する捜査の課題」について説明】

5 討議

委員： 国の捜査機関による国際共同オペレーションが進められることを高く評価し、強く支持したいと思う。一国のみで捜査を完結させることは、特にサイバー犯罪については不可能であるが、海外での公権力の行使は、国際法違反となるため、国際捜査は要請ベースで行う必要がある。しかし、要請に対する回答が得られるまでに長い時間を要する上に回答がなされない場合もある。国際共同オペレーションの枠組みができれば、複数の国の間で全体像を把握するための情報を融通することが可能となり、アトリビューションの更なる推進を通じて犯人の特定に至ることが大いに期待される。

このことは、我が国が直接の被害国である場合には国益にかなうということとはもとより、国際共同オペレーションの提携国が被害国である場合には、国際貢献ということにもなる。また、日本が国際共同オペレーションに加わることにより、犯人は、日本へ攻撃することを思いとどまり、攻撃への抑止効果、あるいはディスインセンティブとして作用することが、大いに期待できる。

また、これまでは、外国治安機関等から捜査要請がなされた際には、警視庁や各県警に適宜要請を振り分けて対処していたが、国が直接関与することで、業務の実効性にも、国際的な信用の向上にも資することになると思う。

国際共同オペレーションの提携先としては、法の支配、自由、民主主義といった価値観を共有する国家や国際機関と幅広く行うのが良いと思う。

事務局からの説明にあった Europol や米国をはじめとして I C P O、カナダ、オーストラリア、ニュージーランド、さらに A S E A N 諸国やインドの警察機関との連携が考えられる。

今回の報告書骨子案に記載された方向性は、本年9月28日に閣議決定された「サイバーセキュリティ戦略」で挙げられた「サイバー犯罪への対策」はもとより、「サイバー攻撃に対する実効的な抑止のための対応」及び「サイバー事案に係る国際連携の強化」にも、まさに資するものであるということを付言しておきたいと思う。

委員長： 欠席されておられる委員の方から、御意見を事務局が預かっているとのことであるので、事務局から紹介をお願いする。

事務局： 事前にお預かりしている御意見について、御紹介したい。

一人目の委員からは、サプライチェーン攻撃への対処の重要性について触れていただいた上で、例えば、中国人民解放軍が関与したとされるサイバー攻撃においては、サイバー攻撃に先立って、IT資産管理ソフトを事前に入手して、ぜい弱性を調査した上で攻撃した蓋然性が高いと報じられている事案があるということを基に、サイバー攻撃に先立つ活動の端緒等を把握することが重要であると認識しているということ。また、そのためには、ソフトウェア開発事業者とも連携し、対応していくべきではないかという御示唆をいただいた。

二人目の委員からは、国際連携に関して、海外捜査機関と信頼構築をしていくためには、重要な事案に優秀な人材を集中して投入し、高度な分析を行っていくことが必要ではないか、また、フェイク動画の作成など、実空間とサイバー空間の接点での安全の確保にも、これからは注目していくべきではないかという御意見をいただいた。

三人目の委員からは、新しい科学技術の恩恵だけではなく、どのようなリスクが生じ得るかという点に係る想定事例の集約・蓄積を民間ベースでも議論する動きがあることを御紹介いただいた。例えば、農業分野においても、農薬の散布や収穫時期の決定等がセンサーによって収集されるデータに基づいて行われるようになってきているところ、そのようなデータが窃取されることで、相場操縦に悪用されるリスクも顕在化し得るという御紹介をいただいた。

四人目の委員からは、例えば、鉄道事業者は、これまで通信手段を自ら整備・運用することとされていたところ、商用5Gネットワーク

を活用するという議論も始まっているが、これが実現した場合、通信障害が発生したときに、鉄道の営業にまで影響が及ぶこともあり得る、新技術の普及に伴い、サイバー攻撃等の影響範囲が、今までよりもかなり広がってきているということに注意をする必要がある、サイバー攻撃の影響が、どのようなところに現れるのか、警察においても、あらかじめ分析をしておく必要があるのではないかという御意見をいただいている。

また、配布した資料には記載がないが、5人目の委員からはサイバーセキュリティの人材について、地域格差があるのではないかという感覚を持っているが、サイバー局、サイバー隊の創設により、人材を増やしていくということとはもとより、高度な人材を地域に配置した上で、機動的に活用するということで、地域格差がなくなっていくことを期待したいというような御意見もお伺いしている。

委員： 民間企業においては、デジタルトランスフォーメーションの推進により、従来のICTについて専門部署だけが担う業務から、全ての事業部門が課題を認識し、対処すべきであるものに変化している。今回の骨子案に記載されている、分散したリソースを専門部署であるサイバー局に一括集中して高めていくということは、大いに推進していただきたいが、それと並行して、民間企業における事業部門に相当する捜査部門においても、実働を行っている方々が、もう少しデジタルについて課題を認識し、サイバー局という専門部門と連携していけるよう、教育等を通じた人材の底上げに関して何か盛り込む必要があると思う。

事務局： 他の委員からも御指摘をいただいているところであり、全ての警察職員が重要性を認識し、危機意識を持って対応していくことが、非常に大事なことだという認識であるので、報告書に盛り込ませていただきたい。

委員： 前回お話しした「マルチステークホルダー」の重要性について、キーワードとして記載いただきありがたい。また、海外の法執行機関等と信頼関係、顔の見える関係を構築するという方向性は重要であり応援したい。欧米の法執行機関を見ると、お互いに顔がよく見える関係を構築し、信頼し合っている。一方、日本では、人事異動の関係上、頻りに人が替わるところがあり、困難な状況にあると思われる。繰り返しになるが、国際会議の主催や顔の見える関係を構築することは非常に大事である。

さらに、AIを活用したアトリビューション等の話が記載されてい

るところ、もちろん最新テクノロジーを利活用することは大事であるが、一方で責任あるA I等の利活用という観点から、倫理観の重要性にも留意しつつ利活用いただきたい。

加えて、国連の11の規範について記載されているが、これは国際法がサイバー空間に適用されるという規範も入っており、非常に重要な規範であるので、注釈にリンクをつけるなどした方が良いと思う。

事務局： 御指摘のとおり、欧米の法執行機関等では、長い期間を経て醸成された人間関係や地理的な近接性もあり、信頼関係が構築されていることが見て取れる。我々も諸外国とそういった信頼関係を構築できるよう努めてまいりたい。

事務局： A I等技術の適切な利用という観点からの御指摘については、何らかの形で報告書に盛り込ませていただきたい。

委員： 不正なクレジットカードの注文によるECサイト被害について、「クレジットカード不正決済 個人情報悪用の実態を追う」という内容が報道されている。具体的には、総額60万円程度の被害に遭ったネットショップが警察に被害届を出そうとしたところ、対応してもらえなかったという話が出ている。

前回会議においても、警察としてこうした事案の捜査も重視されているとの話があったところであり、報告書においても、サイバー空間と実空間にまたがる脅威の1つとして、具体的な記載をお願いしたい。

また、実態把握に関連して、民間事業者の被害状況を聞き取ることに努めてほしい。現在は、事業者毎に言わば点のような状態で情報を保有しているところ、これを集約し、線や面となるような形で情報を蓄積し、分析を行って頂きたい。分析したとしても、国際的な要素が絡み、検挙が難しいことは承知しているが、通報しても相手にしてもらえない状態が続くと、ランサムウェア等の被害に遭った場合に、事業者が通報しなくなってしまうという悪循環に陥ることになるため、しっかりと対応頂きたい。

単純なカード番号の不正利用の場合、消費者は補償されることが多く、金銭的被害は、加盟店が負うことになる。一方で、QRコード決済やID決済等複数のサービスを経由している場合は、補償が行われず、最終的な被害者が消費者というケースも多々ある。消費者が警察に相談しても、警察に動いていただけないということもあるところ、サイバー局に専門の窓口を設けていただくことはできないか。あるいは、所轄の警察署において、ある程度話を聞いてもらえるよう刑事部

門、生活安全部門等との連携を行って頂き、相談を門前払いせず、適切な部署に回していただけるようなフローを作っていただきたい。

さらに、情報共有について、手口情報の集約結果を、関係事業者と共有いただき、予防・自衛に生かせるようにするということを、検討していただきたい。そのためにも、事業者と日常的な情報交換の場を設けることも必要と考える。

事務局： 警察署等で、なかなか相談に応じてもらえないとのこと、大変申し訳ない。

警察署は、必ず相談窓口を設けており、あらゆる相談を受け付けるようにしているが、相談に対してしっかり対応できるかは、相談を受ける警察官が的確に対応できるかに懸かっている。この部分については、対応が必要な状況にあると考えており、しっかり相談に応じられる体制、あるいは、警察官全体に対する教養も含めて対応していきたい。

実態把握・情報共有については、分析結果等の知見を共有していきたいと考えている。例えば、金融機関のインターネットバンキングに係る様々な犯罪類型は、J C 3と情報共有を行いながら犯行手口等を分析し、実際の捜査にまでつなげるという取組を今でも行っている。また、分析の過程で判明した手口については、都道府県警察が注意喚起等を実施させて頂いているところ、クレジットカードに係る被害については、大変増えてきているところでもあり、我々として対策を打ちたいと考えている。

他方、事業者との連携についてはまだまだ課題があると認識していることから、しっかり検討させて頂いた上で、報告書に盛り込みたい。

委員長： 相談業務を底上げするためにも、情報を早く整理して対応する取組を報告書にある程度盛り込むべきではないかと思う。

委員： 広報啓発について、セキュリティベンダーという立場から、IPA等から発表されるぜい弱性情報等を頻繁にエンドユーザーに提供しているところ。今回、警察への相談を促進するための気運づくりを進めるということについては、ぜひ協力させていただきたい。その一方で、広報啓発の中で、IPAによる情報提供と近いような形で、警察からも様々な情報提供をしていただきたい。

また、被害企業に配慮した捜査ということで、レピュテーションリスクに対する取組も重要と認識。この点について、顧客から様々な相談を受けているところであり、被害企業のレピュテーションリスクを

軽減する方針等があれば、警察への相談等を積極的にしていただけるような紹介につなげていくためにも、お伺いしたい。

事務局： 被害企業のレピュテーションリスクについて、報告書の「警察への円滑な通報・相談を可能にする環境整備」に記載したとおり、被害企業のレピュテーションリスクに配慮した初動捜査の在り方について、現場のベストプラクティスを収集・分析して検討していきたいと考えている。

また、通報・相談については、民間企業側から広報啓発というところで御協力いただければ大変ありがたい。警察では、共同対処協定を様々な企業と締結させていただき、広報啓発活動やサイバー犯罪被害防止に努めているが、そういったところとも連携して相談等の促進に係る広報啓発を進めて行きたい。例えば、サイバー保険を取り扱う損保会社と連携して、通報促進に向けた広報啓発を進めるということを都道府県レベルでは広げているところ。セキュリティベンダーを含めた民間企業から御協力をいただければ、大変ありがたいところであり、様々な御意見をいただきながら、しっかり進めていきたい。

委員： 報告書の全体的な方向性としては、大変良いと思う。特に国際パートが前面に出ておりとても良い。

他の委員からも言及があったとおり、国際連携にはやはり顔役が必要。事務局からもお話があったが、海外治安機関等と信頼関係を築いていくためには、この人が日本のサイバーの顔という人が欲しい。警察庁の中にも非常によく知られている方もいるところであり、そういった方々を、この分野に貼り付けて、顔としてつないでいていただけると良いと思う。

また、インテリジェンスの世界において、情報共有は、情報の交換を意味するものであり、どれだけ良い情報を持っているかということが、より良い情報の共有にもつながっていくと思う。

さらに、事務局より説明のあったハードウェア、ソフトウェアの解析は非常に興味深かった。警察職員全体の基盤の底上げも必要である一方で、そのような高度な専門技術を持った方々が民間に転出することをあえて認める文化をつくることも、日本全体のサイバーセキュリティの底上げ、人材育成に繋げるという点ではあり得ると思う。警察の皆様には、大きな視点で、特に技術的などところの人材育成ということを進めていただけるとありがたい。

事務局： 顔役の話について、御指摘のとおり、警察庁にもサイバー分野で著名な人材もおおり、実際にそういった人材に情報が集まってくるという

ところもある。国際的にも、そういった信頼関係を持つということが大変大事であることから、顔が見える関係の構築を、現在の技術系職員によるものだけでなく、捜査部門としてもしっかり進めてまいりたい。

情報共有については、捜査という観点からも、こちらからも情報を提供するということが重要であると認識している。これまでの経験においても、こちらから情報を提供することにより、相手方からも情報提供を頂くということも実際にある。事務局として説明させていただいた Europol 主導の国際共同オペレーションについても、各国が様々な情報を提供し合いながら分析を進め、捜査を推進し検挙している。東南アジアを含めたアジア各国は、ヨーロッパから見ると、地理的に遠く関係を構築しづらいところ、日本にとっては地理的に近く連携しやすいと思う。情報提供を推進しつつ、国際共同オペレーションを進め、犯人の検挙にも繋げていきたい。

委員： 刑事法の観点から、見解を述べさせていただきたい。

最終的には検挙がなされることが望ましいという観点から考えると、警察の捜査として、犯人の確保、証拠の収集等がなされるわけであるが、現実問題として国境を越えた証拠収集が非常に難しくなっており、実際に犯人の確保に至ることは、国際的に見てもレアケースである。また、従前、国際捜査の実績が、日本として十全ではなかったということも否定できない。もっとも、これについては、諸外国においても事情は多かれ少なかれ同じであると思われ、サイバー犯罪で犯人検挙に至る例が多いとは言えない。各国間でも、サイバー犯罪捜査への取組等に差があり、非常に状況が複雑なところである。

一方で、Emotet のテイクダウンについて、日本が参画していないことは、犯人からすれば、日本は狙っても大丈夫なのではないかという不適切なメッセージの発信にも繋がりがねない。日本は、アジア地域の国際捜査の拠点として、国際協調の枠組みに参画していくことが欧米諸国にとっても望まれていると考えている。そのような観点から、今回のサイバー局・サイバー隊新設の意義は、極めて大きい。諸外国においても、サイバー犯罪捜査の模索が続いている状況下で、日本としても、都道府県警察と連携・協調しつつ、国際共同オペレーションといった国際捜査を一層充実させていただければと思う。

事務局： Emotet のテイクダウンに日本が参画していなかったのは、日本の治安に関わる現実の問題であると危惧している。現在、警察は、サイバー犯罪の未然防止について、様々な省庁と連携して施策を推進して

いるところであるが、検挙については、我々以外にはできない。今まで、都道府県警察が検挙したいという思いがある中で、なかなか進めなかったところであるが、国の捜査機関が関わることにより、我が国が一丸となって、各国と共同しながら検挙を推進していきたい。

委員： デジタル社会が進展する中、全国民がサイバースペースとの関わりを持って活動していく、全ての分野がサイバースペースの中で活動していく、つまりカバレッジ100%を前提として考えていくことが重要。今までと何が違うのかというと、関わる人の種類が非常に多様になっているという側面がある。

例えば、オレオレ詐欺のように高齢者だけを考えていけば良いと言うことではなく、デジタル社会の推進という中で、若者、子供、教育の現場に対する展開を誰がどう担当していくのか。また、テクノロジーは便利であるが、人を傷つけることもある。こういったときに、警察の役割は、非常に重要だと思う。それと同様に、若者、子供、教育の現場に対してどういうサイバーセキュリティに関する責任を持つべきか。この役割は警察だけではないが、警察としての役割をどう考えていくのか、他省庁・関係機関等との連携をどうしていくのか考える必要がある。

また、人材に関しては、警察職員全員が、サイバーセキュリティに関する責任と役割を持っていただきたい。このことが、我が国が世界で最も安心できる社会に繋がっていくと思う。サイバー空間と現実空間が融合する中、どういうクオリティーの社会を作れるのか、これは大変大きなチャレンジではあるけれども、世界からも期待されている。

どのようにしたら全国津々浦々に、今の安心と安全を、サイバー空間と合体した後につくれるのか、そのためには警察の方や全国に事業展開している民間の方々、あらゆる人たちとの連携の体制というものが必要になると思う。さらに、知財についても、政府全体としてデジタル知財に方向転換を行う中で、経済的な被害に対してどう対処していくのか。これまでは、ブロックチェーンという議論をしてきたが犯罪として警察の立場で対処できる方向性を考えていかなければならない。

加えて、大地震等の自然災害が発生した際に、どういう態勢をつくれるかということも非常に重要。現在、避難所をネットワークで繋ぐなどインフラ整備も進めているが、サイバーセキュリティの視点でかなり隙がある。有事の際に、誰とどこで、どのように協調するのか、カバレッジ100%時代にどういう準備をしておくかが重要な視点だ

と考えている。

事務局： 全ての方々に対してサイバーセキュリティに関する責任があるという視点は、我が国が直面している大事な課題であると認識。御指摘のとおり、これは警察だけでできるものではないことから、関係省庁と連携して対策を進めていくことが大事だと思う。

サイバーセキュリティ戦略にも盛り込まれているが、警察が委嘱したサイバー防犯ボランティアが全国様々に、その地域の実態に応じて活動しているところ、小・中学生に対する教育のみならず、サイバーパトロールも実施し、違法・有害情報を通報して頂いているところもある。学校と連携している事例も多くあり、例えば、慶應義塾大学のサイバー・防犯ボランティアとも密接に連携している。このような取組については、サイバーセキュリティ施策を推進している関係省庁全体で、進めていくべきだと考えている。警察では、自治体や知事部局、教育委員会等とも既に密接な連携関係があるので、そういうところとも、しっかり進めてまいりたい。また、知財についても、警察全体としてのリテラシーを高める必要があると考えている。生活安全、刑事等全ての部門がサイバーと関わることから、警察全体として、しっかり取り組むべき体制・教育を構築することが課題と認識している。

災害対策という観点では、内閣官房事態室が大規模サイバー事案を対象としているところ、そのみならず自然災害というものがある中で、どういう取組ができるかということは、関係省庁との連携の中で、我々としても考えていきたい。

事務局： 我が国は、世界の中で最も安全な国の1つであると認識されている一方、デジタル化の進展に伴い、治安の良さがだんだん安泰ではなくなってきたと考えている。

SNSの普及、デジタルネイティブの出現等により状況は大きく変わってきており、国民生活の安全を守っていくためには、様々なことを考えていかなければならない。また、こういった中で知的財産についても保護していかなければならない。

警察の中でも、サイバーだけを見ていけばよいというものではなく、全ての部門でサイバーを見なければならぬ局面となっており、サイバー局は全ての事象をスコープに収め、関与していかなければいけない。警察だけでは解決できないこともあるので、関係省庁、民間企業等と力を合わせて、オールジャパンで対応していかなければならない。新組織をつくることは、新たな時代の流れに適応して、新しい

形の日本の在り方を考え、取り組んでいく良い機会だと思う。その結果、日本の安全・安心というものが得られれば、世界に対して、発信していけるものと考えている。

委員： 通信の世界においても、SNS等インターネット上のトラブルが海外に及んだ場合、非常に対応が難しい。また、対応が長期間にわたるケースも多い。国際連携、対応の強化の部分は、取組が一番難しいところと承知している。

海外捜査機関への照会は、大体、回答までにどのぐらいの期間を要しているのか。また、回答の中身についても御教示頂ければと思う。

また、国際共同オペレーションに我が国が参加していく上で、これまで参加されている国々がどのような取組をしてきたのか、これをしっかりと把握して、分析することが不可欠と考えているが如何か。

事務局： 照会結果の回答期間は、国によって千差万別である。また、我が国と協力関係にある国であったとしても、当該国に対して大量の照会が行われている場合は、しっかり調整しないとなかなか回答を頂けない。照会ルートも複数存在する。ICPOルートは、早いもので数週間程度で回答を頂ける一方、中央当局ルートの場合は、回答を頂けるまで数か月程度かかることもある。

ログの保全のお願いについては、24/7という方法で、各国サイバー部門が連携していることから、比較的早く返答を頂ける。

また、照会を行っても、照会結果が返ってこないことがあるほか、ログが既に消えていたという回答をする国も存在する。

国際共同オペレーションについては、これから積極的に取り組んでまいりたい。警察全体で見れば、国際捜査管理官を通じて、様々なネットワークがある一方、サイバー部門の連携はまだまだこれからというところがあり、諸外国の法執行機関等との関係作り、情報共有を進める中で、我々自身の知見を高めていきたい。

委員： 日本の警察の皆様の活躍や活動により、安心して生活できるというところは、日本にいてとてもよかったなと思う。是非、「社会全体でつくる安全・安心」の「安心」の部分に、警察庁の取組がどう繋がっていくかというメッセージも報告書に盛り込むようお願いしたい。

委員： 報告書骨子案について、新組織が果たすべき役割が唐突に出てきている印象を受けるので、情勢認識等の部分にワンクッション置いて記載されたほうが分かりやすいと思う。また、サイバー空間の脅威について全体的に焦点を当てることは、非常に結構であるが、広い意味でのサイバー犯罪をサイバー局が取り切るわけではなく、他部門も一定

の役割を果たしていくものと認識している。そういう中で、クレジットカード被害等、当事者が多数存在し、被害が多く出ているものについては、業界団体と警察という関係で、ある程度枠組みを作り、現場に落とす形を取ったほうが円滑に進んでいくのではと考えている。また、警察に対する不信・誤解を招かないためにも、警察への通報・相談について、警察の窓口をどう整理するのか検討が必要ではないか。

事務局： 我々としても、業界団体としっかりとコミュニケーションを取っているところであるが、警察庁として被害の実態把握をした上でその知見を踏まえて、現場との関係をどう作っていくかについては、相談窓口の課題と合わせて検討していきたい。

また、御指摘のとおりサイバー局が、全てのサイバー犯罪を捜査するということは困難であり、全ての捜査部門が、サイバー事案に係る基礎的な捜査をできないといけない。その中で、高度な技術を用いたサイバー犯罪について、どのように各部門を支援できるのか、民間団体との連携をどう作っていくのか、これがサイバー局の新たな課題であると思う。このような課題の整理についても、関係団体と検討を進めていければと考えている。

事務局： 報告書における「新組織が果たすべき役割」については、情勢認識パートの前に、「はじめに」という項目を設け、犯罪情勢等も追記しつつ、しっかり盛り込ませていただきたい。

委員： 報告書骨子案には、サイバー局がどういったところを目指されているのかがしっかりと記載されていると理解している。

ランサムウェアをはじめとするサイバー空間の脅威から、会社や顧客を守るため、今後のサイバー局における各種施策に非常に期待している。本報告書を踏まえ、民間側から何が御協力できるか考えていきたい。

委員： 報告書骨子案は、非常によくまとまっていると思う。その中でも、国際連携については、その強化を図らなければ、サイバー犯罪に対する施策は完成しないと思うので、是非推進して頂きたい。

裁判においても、サーバーが国境を越えたところにあることにより、事件として全く対処できなくなってしまうこともあり、国境がもたらす弊害は大きい。かかる障害を打破するための対策を強化し取り組んで頂きたい。

報告書骨子案に記載されている諸施策について、それぞれの施策の時間軸をどうするかについて、抽象的に書かれていることから、報告書では、より詳しく記載いただければと思う。

委員長： 今回の御指摘で重要な点としては、価値観を共有する国との連携を推進していくこと。この点は、今回の報告書でしっかり筋が通った。多くの委員からの御指摘で共通していることとして、サイバー局がサイバーを見ていけばいいというものではなく、全ての部門がサイバー事案に対処できるようにならなければならない。国民の安心・安全のために警察全体として、例えば、デジタルトランスフォーメーションをどう進めていくかといった点も非常に重要。さらに、サイバー人材に関連した視点として、優秀な人材の採用、海外捜査機関等との信頼関係の構築のためにサイバーの顔が必要である点など、多くの御示唆を頂いた。

事務局： 様々核心を突いた御意見等をいただいた。その中でも「社会全体でつくる安全安心」の「安心」の部分については、非常に重要であると認識している。困っている国民を助けられるということは、警察の大きな役割であると思う。そういった点で通報・相談の体制強化は、困っている方々に手を差し伸べられる、あるいは不安を受け止められるかという非常に重要な論点であり、本当に頼りがいのある警察を目指し、肝に銘じて取り組んでまいりたい。

また、これから社会の安全を守るためには、変化する社会に適応していくことが必要であり、そのために必要な組織・制度の整備をしていかなければならない。

6 閉会