平成 30 年２月 20 日

平成 29 年度サイバーセキュリティ政策会議（第３回）
発言要旨

１．　開会

２．　仮想通貨を利用した犯罪の事例について

【警視庁から発表】

○（委員）　クレジットカードでビットコイン等を購入した場合、現金化を抑制する目的から、取引所で出金制限をかけていたと記憶しているが、本事件当時はまだ、そのようなことはなかったということか。

○（警視庁）　出金制限自体はあったと思うが、そこに至るまでに、どうしてもタイムラグがある。あるカード番号を使って一気に買い、モニタリングの中で判明して止められると次の番号を使うという形で、なりすましのアカウントを幾つか作り、できるまで繰り返す。

○（委員）　取引所で、そもそもクレジットカードで買ったビットコインはしばらくの間出金をさせないという規制をしていたと思うのだが。

○（警視庁）　本事件のときに、即時から１日か２日後にするという制限が、かかってきたように思う。

○（委員）　取引所の中でビットコインを買った場合、その直後には買った本人のアカウントは、あくまでもビットコインのオフチェーンのアカウントが設定されるだけであって、そのアカウントからさらに外部、例えば海外の取引所に送るときには、取引所の持つ大きな財布から送られるということか。

○（警視庁）　そのとおり。

○（委員）　その後、本人名義のアカウントに戻ってきてから出金されているが、この本人名義のアカウントも取引所のアカウントということか。

○（警視庁）　そのとおり。海外の取引所の大きな財布からの入金になる。

○（委員）　つまり、本取引の中では、ビットコインのアカウントとして実際に表に出ているのは取引所の大きな財布のアカウントだけであって、個人が入金するなどの部分は、同人が取引所に対して持っているオフチェーンのアカウ

ントというか、口座番号といったものに対しての指示により行われるということか。
○（警視庁）　そのとおり。
○（委員）　その場合、海外の取引所への出金のアカウントは、この国内の取引所のアカウントになり、出金先も海外の取引所のアカウントになる。つまり、表面上は取引所のアカウント同士でやりとりをしており、個人の口座番号と、同人が持っている価値とを紐付ける情報で個人を特定しているということか。
○（警視庁）　海外の取引所の中を詳しく見ていくと、単純に送られたところから次の送金が始まるわけではなく、着金したアドレスと、次の送金をするアドレスが異なっていることが多い。
　したがって、外形的にブロックチェーンだけを見ると、どこかで途切れるが、海外の取引所の履歴をあわせて見ると、つながってくるということになる。
○（委員長）　ブロックチェーンを追っていくツールを開発しているという話があったが、警察の対応も急速に変化しているということか。
○（警視庁）　アメリカやヨーロッパといった海外の事例を参考に、ツールの導入や、自前での作成をここ一、二年行っている。
○（委員長）　国際的な情報共有に関しても、警視庁単独で行っているのか。
○（警視庁）　情報収集については、例えばヨーロッパで行われた仮想通貨に関する会議に、警察庁とともに参加したり、警察庁で海外から人を招いた会議があった場合に警視庁も参加したりといった形で行っている。
○（委員）　ビットコインのブロックチェーンを可視化するツールを作成している、あるいは導入しているという話について、ビットコインの他にも仮想通貨はたくさんの種類があるが、それぞれに対して個別にツールを導入していかなければならないということか。
○（警視庁）　そのとおり。それぞれの仮想通貨で全く仕組みが違っている。
○（委員）　仮想通貨の問題は、海外との連携を十分に考えていかなければ、上手く規制ができないのではないかと思うが、その点で何か海外の機関と連携をとるといった対応は行っているのか。
○（委員）　捜査という意味では、ＩＣＰＯといったルートを通じて捜査協力を求めたりしている。

さらにその先の連携というところになると、国の機関ということになるので、都道府県警察が単独でできることではないが、いずれにせよ、日本単独ではなく、海外との連携による対策が必要であると感じている。

○（委員）　関係者が情報共有するということは、それぞれの立場の違い等によりハードルがある程度高いものではあるが、仮想通貨という新しい分野、若い業界においては、官民の連携や民間での情報共有のような仕組みづくりについて、やりやすい面もあるのではないかと思う。仮想通貨に関する犯罪を防ぐための民民や官民の情報共有のやり方やそれを支える法はどうあるべきと考えているか。

○（警視庁）　１つは、協会との連携ということになると思う。現在、大きく２つの協会があり、統合されるのではないかという報道もあったが、いずれにせよ、官民という意味では、そういったところとの情報共有から入っていくことになると思う。

本事件は、それぞれの取引所に対して仮想通貨に関する犯罪の情報を個別に聞いた結果判明したものであるが、例えばクレジットカード業界であれば、犯罪対策協議会のようなものがあり、そことの連携ということで情報共有を行っているように、仮想通貨についても、個々の取引所というよりは協会単位で情報共有ができるような方向に行くのが良いのではないかと思う。

また、捜査員と取引所の担当者は、日ごろから情報共有を顔と顔でやっていったほうがいいとも思う。会議の場だけで会ってやりとりするというよりは、日頃からの接触や信頼関係の構築が大切であると思う。

３．　ボットネット・テイクダウンにおけるシンクホール実施等に関する法的課題について

【委員から、ボットネット・テイクダウンにおけるシンクホール実施等に関する法的課題について発表】

○（委員）　シンクホールの実施のところで、検証に係る必要な処分と考えるという説明があったが、この場合、ボットネット全体の状況把握をするということが検証で、シンクホールがそのために必要な処分になるということか。

○（委員）　そのとおり。直接、感染端末との間で状況を把握するということ

であれば、シンクホールを実施する必要はないが、ボットネット全体を把握するためには、シンクホールを実施しなければならない。シンクホールの実施自体は検証そのものではなく、その前提の必要な処分として行い得ると考えている。言わば、遺体を損壊しないとその状況がわからないという場合に、その遺体を損壊することができるかどうかということと同様である。

○（委員）　状況の把握というのは基本的に必要なものだと思っており、それが検証だということは理解できる。しかし、シンクホールの用途は、その後の遮断や感染端末への能動的なアクション等、もう少し踏み込んだところまであり、それをボットネット全体の状況把握という言葉でくくるには、少し違和感がある。

○（委員）　発表の趣旨は、まずそもそも入り口のところが難しいということである。実際シンクホールをやらなければ、感染端末に対して、通知や修繕のためのソフトを送ることもできない。

○（委員）　シンクホール後の対応を行うとすると、検証のところで、もう少し別の議論が必要かもしれないということか。

○（委員）　そのとおり。

○（委員）　状況を把握するための検証ということであれば、ある程度の期間が必要な気がするが、これも既存の検証の扱いの中で実行可能なものなのか。

○（委員）　通常、令状の有効期間は１週間や１４日となるため、それで本当に足りるのかどうかは議論の余地がある。

○（委員）　実際では、一月や半年ぐらい必要だという話が出るのではないかと思う。

○（委員）　かつての通信傍受のように、検証許可状に様々な条件をつけて行うことも考えられるが、それは、本来定めている検証を事実上新しい形の処分に書きかえて行うことになってしまうため、現行法の解釈としてはなかなか難しいところも出てくるのではないかと思う。

○（委員）　シンクホールの使い方として、感染者の特定や当該感染者への通知を行う場合と、その先のボットネットのテイクダウンといったところまで行う場合とでは、通信の秘密の侵害や法的な部分での違いは出てくるのか。

○（委員）　マルウェアは、感染端末とＣ＆Ｃサーバとの間の通信をさせるも

のである。シンクホールは、そこに介入して通信を遮断し、シンクホールサーバへリダイレクトするという形で実施されるので、その使い方よりもむしろ、シンクホールを実施する際にＣ＆Ｃサーバの管理権を奪ってしまうことが、通信の秘密の侵害に当たるのかというところが問題になってくるのではないかと考えている。

○（委員）　例えば、あるドメインがマルウェアの接続先で、当該ドメインを偶然入手した場合、それも介入ということになるのか。

○（委員）　第三者が勝手に介入する場合、厳格に考えれば、通信状況を把握していることは通信の秘密の侵害だという解釈にもなり得る。

一方で、Ｃ＆Ｃサーバと感染端末との間の通信状況が、コミュニケーションなのかというと、あるアドレスからあるアドレスに電気信号が流れているということだけであれば、手紙で言えば住所の部分を見るだけということになるため、必ずしも通信の秘密の侵害に当たらないという整理もあり得ると考えられる。いずれにせよ、その点は、議論がまだ十分でないところである。

○（委員）　発表の中で、プライバシーの利益という話があったが、ボットネットがそもそも有害な情報を流しているという状況で、その対処を考えるに当たり、プライバシーとして保護しなければならないという前提は必要なのか。

通信傍受法や最高裁判所の通信傍受法に関する判例の場合、通信の中身がブラックボックスで、保護されるべき通信もその中に入っている可能性があるため、一般探索的な捜査目的の傍受のようなことにならないように対処するという考え方だと思うが、基本的に有害な情報を外部に流していることが明らかなボットネットの場合、通信の中身が関係する場合と類型的に異なるという区別をしたほうが良いのではないかと思う。

○（委員）　サイバー空間のプライバシーというものが何か、現実空間のプライバシーと同じでいいのか、つまり、犯罪者の家であっても簡単には踏み込んではならず、捜索差押許可状がなければ入れないというのと同じ程度のレベルで、Ｃ＆Ｃサーバのような有害な情報を使うだけのサーバの管理権にプライバシーの利益を認める必要があるのかは、議論の余地が十分あると思う。

アメリカは、その点で比較的踏み込んだ議論も一部あり、少なくともマルウェアのようなものは何ら利益を生まないものであるから、それに対する法的な

利益や、プライバシーのようなものは認められないという考え方もあり得る。

一方で、今までのサイバーの議論はどうしても現実空間とのアナロジーから出発しているところがあり、そこを簡単に切ってしまうと、かなり雑な議論だとされてしまいかねないため、まずサイバー空間におけるプライバシーとは何なのかということを整理した上で、可能であれば、少なくともこのボットネットの通信に関しては、通信の秘密で保護しなければならないような利益性は認められないという方向に持っていければ良いと思う。

○（委員）　国外の活動が関係している場合の対処については、アバランチ事件等で見られたように、共同捜査をすることで、国境に関係するバリアを取り除くという方法はあるのではないかと思う。

○（委員）　現状、刑事手続としてボットネットのテイクダウンを行うことは難しく、実際にはアメリカのマイクロソフトの努力により、様々なボットネットのテイクダウンができているという状況である。アメリカの捜査として具体的にこれに乗り出すという例がほとんどない中では、捜査という枠組みでできるということ、まずそれ自体を示した上で、捜査の協力関係をつくっていくことが必要になると思う。

○（委員）　発表の最後にあった、ＪＰＲＳについての話では、一国のレジストリサービスを担う機関が、営利企業とまでは言わないものの、通常の株式会社である現状で、同社に登録取消や差止請求を要求する形になっている。どちらかというと捜査側に協力してもらって、具体的にアクションを起こしてもらいたいような存在だと思うが、そのような形の協力を、マイクロソフトの例のように、ＪＰＲＳに対しては求めることは可能か。

○（委員）　現状、ＪＰＲＳが自らの判断で行うことは難しい。捜査機関からの協力依頼により行ったのであり、何かあったとしても、少なくともＪＰＲＳの責任ではないという枠組みができれば、ＪＰＲＳも安心して登録の取消や停止を行うことができると思う。

実際、その点についての議論もまだあまり進んでおらず、今後このようなことが、例えば民事訴訟の枠組みの中でできるかということを、考えていかなければならないと思う。

○（委員）　現状、ＪＰＲＳが、ドメイン名だけではなく、ＩＰアドレスも含

めて広範な権限を持っており、インターネット空間における管理者に当たる存在となっている。一方で、その管理者が、そのような他人行儀な形でなければ犯罪捜査に協力してくれないのは、仕組みとして少し間違っていると感じる。

○（委員）　ＪＰＲＳは、インターネットの世界の交通管理者であり、私的な営利企業、要するにＩＳＰとは位置付けが違うという指摘だと思う。そのような考え方が通用するのであれば、非常にありがたいと思うが、一方で、株式会社であるということを考えると、やはりワンステップ必要なこともあると思う。

○（委員）　ＪＰＲＳでの対応の可能性について、既にＪＰＲＳやＪＰＮＩＣと検討は始まっているのか。

○（事務局）　昨年の夏以降から、ＪＰＲＳやＪＰＮＩＣとは、このことについて複数回話をしている。発表にあったとおり、ＪＰＲＳは、制度的な担保がなければ、自分たちが主体的に行うことは難しく、逆にいうと、制度的な担保があれば可能であるというスタンスのようである。

汎用ドメインの停止については、裁判所の確定判決等があれば、可能ということである。また、汎用ドメイン名登録等に関する規則第 29 条については、それを確かめるために１度連絡をするというものが、第 22 条にあったかと思うが、そこで連絡が通じなければ、確かめようがないとして停止が可能ではないかという意見は、ＪＰＲＳとしてオーソライズされたものではないが、事務局との打ち合わせの中で出ている。

一方で、停止した後、その管理権限を新たに警察あるいは他者に渡すことは、また別の議論になるかもしれないという話も出ている。

○（委員）　ＪＰＲＳでの対応の件は、大量に登録され、機械的に悪用される無数のドメインの存在を考えると、対策のスピード感に課題があると思う。対策のスピード感にある程度の目標設定ができなければ、手続論で遅れをとってしまい、実効性が保てない。また、正規のドメインを乗っ取ってＣ＆Ｃサーバにするようなケース等には対応できないため、こういった面を含め、社会的許容性を欠く場合とはどのようなものなのかという議論は、並行して始めるべきだと思う。

マイクロソフトの著作権違反の申告に頼った取組しか、世界中でまだ実行できていないということに関しては、新しい手続論が世界でまず必要であると思

う。日本だけの努力では、かなり難しい面があり、マイクロソフトの取組により進んできたことを考えると、将来が不安に感じる。

通信の秘密については、現在、総務省の指導のもと、円滑なインターネットのあり方という検討の中で、議論が始まっており、Ｃ＆Ｃサーバを検知して対策につなげるということにおいて、通信の秘密に配慮した方法の議論が正に行われている。その中では、Ｃ＆Ｃサーバの技術的な判定根拠に関することや、正常な通信をも止めた場合に別の問題が生じうるといったことが課題とされており、技術面の研究や、それに加えて、社会的なコンセンサスを醸成していくことが必要だと思っている。

一方で、シンクホールに通信を曲げるということは、このこと自体が検閲等を想起させるものであることから、そういったことを含めて議論をしっかり行っていかなければ、実行は難しいと思う。

○（委員長）　ネット社会で国民が困る問題が起こったとき、警察としてどこまで介入するべきかという議論はずっと続いてきている。例えば、ログの保存であれば、あったほうが国民の利益を守れるけれども、コストの問題などを別にしても、通信の秘密といった様々な問題がある。

発表の中で、通信の秘密があっても、違法性阻却事由があれば警察は介入できるという話があったが、一方で、緊急避難しか許されないという議論もこれまで存在した。違法性阻却事由が複数ある中で、なぜ正当行為では許されないのか分からないが、表現の自由や通信の秘密というのは、憲法の権利の中で一番重く、絶対にこれ以外方法がないというときにしか通信の秘密は犯してはならないという考え方だと思う。検閲の問題といったもののハードルを軽々しく考えることは避けるべきだと思うが、緊急避難をほとんど認めない日本においてこれまで行われてきた、緊急避難しか許されないという言い方、つまり、通信の秘密は絶対であり、一切介入していけないという議論が、現在変わってきていると思う。ネット社会を国民の利益のために発展させていくためには、不適当なものは排除しなければならず、そのためのツールは認める必要があるという議論と、これまでの議論とのバランス論だと思う。

発表の中では、シンクホールを適用するときに、令状をどう呈示するかという話や、どの程度の範囲のものに絞り込むかという話があり、先ほどの指摘で

は、シンクホールの実行には様々な問題があるところ、国民が納得する形で社会的に有害性があることを、誰が、どの程度のものとして把握するかという話があったが、検閲の問題も含めたバランスのとれた議論が重要である。そして、ボットネットのテイクダウンの法的問題は、相当な時間をかけて制度的に練っていく必要がある。

一方で、これだけのことが起こって、一切介入できないのかと問題提起をし、議論を始めなければならない。その中で、様々な立場からの議論を踏まえ、調和させていかなければならないと思う。

個人的な意見だが、今までの日本の手続から考えると、検証でできないことはないと考える。通信傍受も元は検証であった。これについては、法的根拠を与えようとした結果、厳しく絞り込んだ立法をしてしまったために、逆に行いにくくなってしまった。法改正で少し行いやすいように戻ってはいるが、見方によれば、長いタイムスパンで見て、紆余曲折を経ながらいい方向に向かっているとも言える。

また、ボットネットのテイクダウンについては、他の国々も困っているはずであり、今後どのようにネックを突破していくかということが日本にも参考になると思う。

○（委員）　日本だけに限らず、民間企業や一般人がシンクホールを運用しているケースを見かけるが、こういったシンクホールを捜査の対象にするケースを考えたときに、捜査上の注意点や懸念点はあるのか。

○（委員）　既になされているシンクホールが適法になされたものであれば、そのシンクホール実施者から任意の協力をいただいて、捜査に利用するということは十分あり得る。

一方で、法的な根拠が曖昧なまま実施されているシンクホールの場合、捜査機関としてその提供を求めることは、難しいと思う。結局は、そのシンクホールがなぜ実施できているのかというところに、大きく依存する話になる。

日本の刑事手続では、違法に集めたものは証拠として使えないという違法収集証拠排除法則というものがある。よほど重大な違法でなければ証拠排除はされないが、こういった議論も詰めておかなければ、このような捜査には簡単には踏み込めないということになってしまうと思う。

○（委員）　民事訴訟での差止めはシャットダウンで止まってしまい、ボットとＣ＆Ｃサーバ間の通信の把握という話になると、傍受で十分という話で終わってしまうように感じており、その後のアクションに続けていくために、考え方や手当ての在り方を検討していく必要があると思う。また、現状のテイクダウンはマイクロソフトが献身的な努力をされているが、今後ＩｏＴが普及してきたときに、マイクロソフトに代わる主体が出てくるかと考えると、かなり悲観的な状況だと感じるので、そういった点も早めに手当てをしておく必要があると思う。

○（委員）　ボットネットは状況を把握するだけではなく、最終的な解体、テイクダウンというところまで持っていかなければならない。現行の捜査という観点では、既に行われた犯罪に対して被疑者を探していくことが捜査であるため、その後の被害の発生防止は、従来、犯人を捕まえることによる更なる犯罪行為の物理的な停止の効果でしかなかった。一方で、ボットネットのテイクダウンの場合、それ以上に更なる被害の拡大を防止するための措置が必要という意味で、従来の捜査とは少し違う側面も考えられる。

○（委員）　多くの顧客のサーバやドメインを預かっている場合、セキュリティ対策を行う上で攻撃を検知したら遮断することは組み込んでいく必要があるが、一方で、本当にその通信が攻撃かどうかを見極めるためには、通信自体を見なければならず、通信の秘密という問題が出てくることになる。しかしながら、どのような仕掛けで、どのように対策をとっていくかを検討する際に出てくる総務省のガイドラインや判例、過去の電話の話といったものは、現代にあまりマッチしていない。発表の中で、通信の秘密との調整が必要という話があったが、非常に重たい議論のように感じる。

また、通信の両当事者の有効な同意があるかどうかについても、１つのアプローチとして議論になるが、立ち上がっているウェブサーバに対して、一般の人が次々とアクセスしてくる状況では、誰がそもそもアクセスしてきているかわからないため、両当事者の同意を得ることは、インターネットの世界では、会員制でしか認めていないものを除けば、無理なのではないかと思う。

しかしながら、逆に、この両当事者の同意を得るというところを、例えば、同意を前提としたサーバやシステムといった何らかの形で制度化し、これにつ

いては､捜査も可能とするといった新たな形も考えられるのではないかと思う。
○（委員）　これまで行われてきた個別の特定の電話番号同士の通信といったものを前提にした議論と、インターネットをパラレルに論じることは難しい。他にも似たような話として、現実空間では令状の発行を受けて実施する場合には、対象が特定されていなければならないが、その点も現実空間と同じイメージの「特定」をサイバー空間で要求することは難しく、サイバー空間における特定性が何かということを考えていかなければならないという議論もある。

また、有効な同意についても、このような通信をしていれば同意しているものと見なすといった包括的な枠組みがなければ、実際それぞれ個別に同意をとることは、現実的ではないと思う。

こういった点も含め、現実空間とのアナロジーから切り離した議論をしていかなければならないと思う。
○（委員）　同意に関しては、現在のガイドラインで新しい考え方が整理されており、従来は、たとえ契約約款等で事前の包括同意があったとしても、個別の同意なく通信の秘密の侵害に当たる行為をしてはならないということであったが、現在は変わっている。

約款等で事前に、Ｃ＆Ｃサーバやマルウェア感染が疑われる通信の場合はＤＮＳで止めるということが書いてあり、これを望まない場合には、そうでないＤＮＳを選ばせるような代替措置を用意している場合、前者の事前の包括同意を有効な同意とみなす形で、現在、運用が行われている。これは、犯罪対策につながるものではないが､結果として被害者の救済には十分有効な取組である。

４．　討議

【事務局から、報告書の骨子案について説明】
○（委員）　本日の議論にもあったが、ボットネット対策が最も重要な対応と考えている。

まず、アメリカやドイツを中心にボットネット対策が行われているということだが、今後具体的にどういった対策、取組が行われていくのか、これをしっかり把握することが、検討の前提になると思う。

さらに、シンクホール等を行ったとしても、その結果として利用者の正常な

通信に支障が出るというようなことはあってはならないが、例えばドメイン単位で宛先を変えるということになると、そういった事態になる可能性もある。したがって、こういった場合にどうするべきかという検討も重要である。

また、諸外国における具体的な制度や実施状況、課題に対しての議論といったものを調査した上で、問題の生じないような方策を検討していくべきだと思うが、一方で、対応方法があったとしても、通信事業者の設備負担や運用負担の問題が出てくる可能性も考えられるため、そういった負担について、妥当な範囲かどうかを検討していくことも重要である。

報告書には、こういった点を、今後の検討のあり方という観点で、盛り込んでもらいたい。

○（委員長）　事業者側の負担を考慮しない結論はあり得ない。その点を詰めて報告書に書き込むことまでは難しい部分もあるが、留保した書き方にはしてもらいたいと思う。

また、ボットネット対策についても、終着点までの絵を描くというところまでは、本会議の報告書では、予定していないところである

○（委員）　民間が警察に期待することは、犯人を捕まえ、犯罪者にとって安全なところに逃げ込むことを許さないということだと思う。

したがって、報告書の中に直接盛り込むかどうかは別として、これまでの議論で取り上げた課題や手法、あるいは対策について、海外とも協力しながらになると思うが、犯人にいかにたどり着くかといった視点を念頭に置きながら、取りまとめをしてもらいたい。

○（委員長）　警察における会議の報告書であるため、当然そのような視点も入れるべきだと思う。

○（委員）　本会議のテーマに、新たな傾向のサイバー犯罪、官民連携という言葉が入っている。レンタルサーバを利用した犯罪の現状と対策の中で、今後の方向性については、レンタルサーバ事業者間の連携といったことが書かれているが、民間事業者とどのようなフレームワークやスキームで進めていくのかという部分は、例えばこのような協会、団体と連携するといったことや、あるいは新たにそのようなスキームをつくるといったこと等、何らかの進め方にまで踏み込んでも良いのではないかと思う。報告書にどこまで書き込めるかは別

として、官民連携のスキームの在り方といったものについて、もう一歩入れても良いのではないかと感じる。

○（委員長）　可能な範囲でその方向を検討してもらいたいと思う。

○（委員）　最近、多額の仮想通貨が不正に送金される事案が発生しているという記載がある。仮想通貨取引所から多額の仮想通貨が不正に送信される事件があったが、この事件で気になるのは、盗まれた仮想通貨が、現にインターネット上に価値として存在しており、その所有者が誰であるかはわからないが、どこかの誰かが所有していて、それは現に盗まれたものであるにもかかわらず、おそらくどうすることもできないという現状である。

これが通常の国内犯罪であれば、盗まれたお金が某銀行の某口座にあるとわかった時点で、そこにすぐに警察が行き、盗まれたものとして差し押さえるなどして、盗まれた本人に返す、犯人を逮捕するといった形になるが、そうではない世界があるということである。普通の銀行や官庁、警察等によって支えられた社会と、そのような支えを期待しないかわりに、放置しておいてほしいと考えている人たちの集合があり、その接点が仮想通貨になっている。後者の人々が運用しているものが仮想通貨の原点にあったということを考えると、そこに発生する一種のコンフリクトが、現在起こっている状況なのではないかと思っており、大変注目されている分だけ、こういったことが存在するという認識を持つことが大切だと考えている。

○（事務局）　仮想通貨の件は、今回の事案で、これまで漠然として先々問題になると感じられていた部分が、現実のものになってきたという点で、フェーズが１つ変わったのではないかと認識している。

この部分については、捜査上の様々な問題と、業を所管している金融庁の立場とで違うと思うが、警察としては、捜査を尽くしていく一方で、仮想通貨に関わる問題をどのようにしていくかという、所管する省庁だけではなく、国民全体で考えていく必要があるものについて、考える材料を提供していきたいと思うとともに、マネロン等の様々な問題についても議論に加わっていきたいと考えている。

５．　閉会