平成 28 年２月 22 日

平成２７年度総合セキュリティ対策会議（第３回）
発言要旨

１．開会

２．ＦＢＩの取組について

【ＦＢＩから、ＦＢＩの取組について発表】

３．マイクロソフトとセキュリティについて

【委員から、マイクロソフトとセキュリティについて発表】

４．オランダ等の欧州諸国におけるサイバー犯罪対策の取組について

【事務局から、オランダ等の欧州諸国におけるサイバー犯罪対策の取組について説明】

５．サイバーセキュリティの向上と捜査情報の活用について

【委員から、サイバーセキュリティの向上と捜査情報の活用について発表】

６．質疑応答

○（中野目委員）　星委員の御発表でプロアクティブな措置が必要という御指摘には私も賛成ですが、プロアクティブな措置というのは様々考えられるところ、具体的にどのくらいまでのものをお考えでしょうか。

○（星委員）　私は法律家なので、サイバーの世界で実際何が起こっているかということを、熟知しているわけではありませんが、例えば民間の側でこういうことを是非やってもらいたいという要請があった場合に、法執行機関又は公的な機関の側でどういうことができるのかということを常にリンクさせながら考えていくことが重要だと思います。ボットネットのテイクダウンはある意味、サイバー空間における管理権を侵害し得る積極的な措置だと思

いますので、管理権の侵害といったことも含めて、それを法的な根拠なく実施できるのか、あるいは令状を要した上でやるのかといったところの整理が必要なのではないかと思っております。

○（中野目委員）　サイバーセキュリティ上の安全に対する脅威、あるいは被害が生じている場合には、その原因となっているものを除去するとか、排除するとか、無害化とかという措置を講じないことには、最終的な解決にはならないと思います。星委員の御指摘は非常に重要であると思います。

○（林委員）　サイバーセキュリティ確保への積極的措置を、個人の権利の侵害度等の低いものから高いほうに並べられている点がポイントかと思います。通信の秘密との関係も指摘されましたが、もし通信の秘密を同じ表に並べるとしたら侵害度を踏まえ、どこに位置づけられるとお考えですか。あるいはそもそもディメンションが違うとお考えでしょうか。

○（星委員）　まさに通信の秘密との関係がキーになると思っております。現実世界での利益侵害を考えた場合に、例えば交通一斉検問は、警察法２条に基づきつつも公道を利用することに伴う負担という一般法理を立てた上で、それに基づく限りで行えるということになっております。道路を走る際に止めるわけですから、移動の自由という観点からすると侵害性が高いのですが、これは許されるとなっています。それ以上の立入ということになると個別の根拠規定が必要となり、ここで１つ大きな線が引けると思います。通信の秘密は、内容の秘密であるか他人の秘密であるのかという点を含めて、どこに位置付けるかということを個別の事象を含め検討できるのではないかと思っております。ただ、今までの議論を踏まえると、通信の秘密は絶対視されているところもあって、場合によってはディメンションの違う形でのアプローチもあり得るのかもしれません。この点は、立場によってもいろいろ見解が分かれてくるところだと思います。

○（前田委員長）　この問題も非常に重要で、正にサイバーセキュリティをどう考えるかにおいて一番の要だと思います。他方、この会議の報告書でどこまで記述するかということは議論の余地があると思います。ただ、これから御議論いただく前提としては、警察庁生活安全局長の諮問の委員会として、今回の報告の射程として議論して構わないと思います。今回、事務局で報告

書の骨子を作成していると思いますが、今回の議論をまとめていく方向性という観点から御説明をお願いいたします。

７．　報告書骨子案について

【事務局から、報告書骨子案について説明】

８．　討議

○（前田委員長）　　大枠の方向性は、今は御説明いただいたものになると思うのですが、問題は中身をどう盛り込むかです。諸外国のサイバー犯罪対策の調査研究を今回の報告書に全部織り込むわけにはいかないわけですが、諸外国といっても、アメリカとヨーロッパの差は大きいし、また、その他の国、例えばアジアはどうなのだということまで考え出すと切りがないのですが、やはりアメリカ、ヨーロッパそして日本だけまとめるだけでも非常に重要な意味があると思います。その前提として行政法と刑事法の関係をどう考えるか、事前的なものと事後的な捜査との関係をどう考えるかが重要な観点となると思います。

○（桑子委員）　　御説明いただいた報告書の骨子の方向性については、特に異論はございません。ただ、やはり通信業界全体で見たときに大手事業者の取組という観点での話ですので、全体を考えるとやはり規模とか事業の形態等含めて非常にまちまちであるという状況で、現実にどこまで対応できるのかということは難しいところがあると思います。また、同様に都道府県警察においても、レベルが様々あるということも聞いているところです。ですから、事業者間等の差があるという前提で報告書を取りまとめる必要があると考えております。特に通信の秘密をどう考えるかというところが非常に重要だと思っておりますので、引き続きじっくりと検討して、取組を始めるということになれば、ＩＳＰも警察もしっかりと理解いただく機会が必要であると思っております。

○（中野目委員）　　サイバー空間を安全にするという点ではやはり、官民の連携が必須、不可欠なものであるという方向性は揺るぎがないと思います。先ほど、通信の秘密に関していくつか御指摘がございましたけれども、他方

で、ＩＳＰを含めた民間業者にはサイバー空間についての安全を保つという点でのレスポンシビリティがあるというお話がございました。そういう点でバランスをうまくとってサイバー空間をより安全なものにする議論になればいいのではないかと思います。これはネット空間におけるプライバシーをどの程度認めていくのかという点で、アノニミティなどにも関係する問題だと思いますのでよく詰めていく必要があると思います。

○（西本委員）　本日、非常に示唆に富むお話をいただきました。１つ目としては効率化、効果的のような費用対効果について、自動化、システム化については即座に実施すべきということです。２つ目は通信傍受と覆面捜査で、これもできる範囲でできることを実施しないと費用対効果が非常に悪いという話でした。３つ目が共謀罪と司法取引の話で、これも効率化という部分で有効とのことでした。日本の場合はサイバー犯罪の本犯ではなく、出し子ばかり捕まるという状況ですので。特にサイバー犯罪関係においては、そういった状況が顕著に出ているので、このあたりを早目に整備しておかないと、犯人の思うつぼということになると非常に危惧しております。加えて効率化、費用対効果の観点から、星委員が御指摘された用心からプロアクティブの部分、これは守り方を多様化すべきということだと思います。痴漢防止の防犯ブザーのようなものを配備する。これを、例えばサイバー空間上で行うとウイルスではないかと言われたりするわけで、どこまでやっていいのかについてもしっかり議論しておかなければいけない点であると思います。もう１点、犯罪を仕掛けている側については、個人、組織、国家というものがあろうかと思いますが、特にサイバー犯罪となるとテロ、国家転覆といった観点になると我々は国も含めて縦割りで対応するわけですが、相手方から見ると転覆に見せかけて、実は金銭目的であると、それは大きな資金源となり得るわけです。この点、金を盗み取られるというサイバー犯罪のテリトリーであっても、その類いの犯罪は非常に大きな意味を持つものなので、縦割りを排し、うまく連携をとれる体制が要るのだろうと思います。

○（則房委員）　民間との連携が重要という話は、本日も再確認されたところですが、民間との信頼関係が重要という話もあり、どう信頼関係を高めていくべきかということも論点であると思います。民間からの期待という話で

あれば、民間で情報提供できるといっても犯罪が起こってから、その起こった犯罪に関する情報しか提供できず、後手感が出てしまう。民間側として法執行機関と協力関係を組むときのメリットは、元を断つか、元を減らすか、犯罪が行われる前に危なそうだというところを教えてもらうということが見えると信頼、期待が出てくると思います。報告書の中でも現状の課題が多く出てくるということは理解できるのですが、民間の人が読んだときに、協力したときにどうメリットがあるのかについて方向性が示されていると今後の連携において、具体的に考えるところに行き着くのではないかという感想を持っています。

○（林委員）　先に御質問したことと関連して、通信の秘密を別ディメンションとして扱うのではなくて、星委員御指摘の権利侵害度の低いところから高いところのいずれかにまず位置付けて、議論を始めるべきではないかと思います。骨子案を見ますと非常によくできておりますが、第３章の今後の方向性のところは､今日の議論を踏まえて変える部分があると理解しています。特に、星委員の御発表の中には論点が多く含まれていると思いますので、ここを詰めると第３章の構成自体が少し変わるのではないかという印象があります。

○（藤川委員）　今後の方向性の中で、背景的なところで気になる部分があります。１つはサイバー犯罪に関しては、御承知のとおり件数の多さや、ＪＣ３でもいろいろ分析をしておりますが、データ量が圧倒的に多いという背景の中で電子化やシステムの自動化というインフラの整備を早急にしていくべきだと思います。例えばユーロポールやＦＢＩとのデータ連携や、情報共有する上で、そのインフラ整備が追いついているのかというところがすごく気になりました。前回の別所委員の御発表の中で、照会業務の効率化、電子化という提案があったときに､局長からハードルが高いという御説明もあり、法律の議論は当然していかなければいけないと思うのですが、その背景にある圧倒的な物量、データ量をどうさばいていくかというところも今後の方向性の中にあるといいのではないかと感じました。

○（藤原委員）　今後の方向性に戦略が複数ありますが、その前提となるのではないかと思うことを２つほど申し上げます。１つは民間部門との信頼関

係を時間をかけて構築していく必要があるということですが、他方で時間はそれほどないので、取組内容、情報の共有、あるいは共同作業について国民の間で多くの企業や事業者が参加して当然だという雰囲気を醸し出していくということも前提として必要だと思います。まだまだ事業者、あるいは有識者の中にもバーチャルの世界は特別で、リアルな世界とは異なって、警察と共同、あるいは情報を共有することについてネガティブであるという方向もあるような気がします。しかし、それが世界的に変わってきているということを示していくべきだと思います。レスポンシビリティという言葉が出てきましたが、例えば企業にはＣＳＲというものがあって、その方向でもよいかと思います。そして、さらに広く大規模の事業者から中規模、そして小規模事業者まで広げていかないと構想は実現しませんし、事業者は加害者にも被害者にもなり得るということを認識していくべきだと思います。事業者にとっても一定の優良な企業だけが相当な負担をしているという現実を社会に広く知ってもらう必要があると思います。２つ目は、法制のことで、例えばドイツはログの保存が憲法裁判所の判例もあって大変厳しいです。厳しいが、同時にリアルの傍受のところで帳尻を合わせているというお話がありました。プライバシーの問題についてはアメリカとＥＵの間に緊張関係はあるのですが、サイバーの捜査は双方でお互いに進展していって、捜査手法そのものは相当共通している部分もあると思います。法制はかなり違いますが我が国での議論でも外国で可能となっている手法を多く調べた上で、我が国ではできない理由を考える必要もあると思います。国際的な共助の時代において、それで大丈夫なのだろうかということも１つの視点だと思います。オンラインによる手続等はそのような一例であると思います。確かにプライバシーの問題となると、ＥＵという鏡を見て、アメリカという鏡を見て日本の立ち位置を決めなければいけないのですが、捜査手法や、犯罪から国民を守るというところになると、共通しているベースはあると思います。以上のような実態調査等を含めて、法令のレベルで詰めた議論をしていく必要があると思います。

○（宮下委員）　非常に難しい問題であると思っておりますが、２点ほど申し上げたいと思います。１点目は、今回のテーマがサイバー犯罪捜査及び被

害防止対策における官民連携の更なる推進ということで、先ほど西本委員からもお話があったとおりサイバー犯罪にはいろいろな類型があって、基本的には国が仕掛けてくるものもある。いろいろな主体がいろいろ仕掛けてきて規模や深刻さもいろいろあると思います。それらに関する官民連携は、同じアプローチとは直感的には思われないのですけれども、官民連携というのは、それに対してどう対応すべきかということについて、内容があると思います。そのあたりを１つの視点にできるか否かということもありますが、検討に値しないことはないと考えております。第２点目としては、この報告書で現状と課題、今後の方向性ということで基本的には、ある問題を解決するために不足することが１つ１つ列挙されて、解決に向けてすべきことが述べられたものになると理解しております。その中で特に今後の方向性の最後のところで、諸外国のサイバー犯罪対策についての手法に関する調査研究の実施についてundercover investigation、plea bargaining、conspiracyといった日本でも検討はされているものの、必ずしも正面からはまだ制度として認められていないものが捜査手法ないしはその他の対策に対する前提となっているというものがございました。それについては、やや飛躍した言い方かもしれませんが、そういう捜査のツールというものがない限り実態解明や検挙が難しいということをより多く公に訴えていただきたい。そのような制度をそのまま、あるいは修正しながら受容することができるのか、どのような条件であればそれが可能であるのかということについて、この報告書に書くのは課題としては行き過ぎかもしれませんが、是非御検討いただきたいと思います。

○（若江委員）　私もサイバー空間の安全確保のために捜査の効率化を進めることについては大いに賛成していまして、星委員がおっしゃったようにいろいろな法的な制度の検討も必要だと思っています。その中で担保してもらいたいと思うこととして透明性と結果の検証ということがあります。いろいろなルールの見直しが必要になるのではないかと思います。電子化やインターネット化が進む中で、捜査側ができる能力というものも潜在的には飛躍的に大きくなっていて、例えばＧＰＳ発信機を尾行に活用する捜査についても、人間が今まで尾行しているのと変わりはないような気もするのですけれども、実はできることはものすごく大きくなるし、誤った場合の人権侵害も大きく

なってしまいます。私はできることはできるように進めるべきだと思うのですが、その際に、アクセス権者の設定や令状制度との整合性の整理をＩＴ化に伴って全面的に見直す必要があると思いました。そういう点も含めて効率的にやっていける法的整備の検討をするという要素も盛り込んでもらいたいと思います。

○（前田委員長）　報告書を取りまとめるに際し、今日の段階で、次回出てくる議論の糸口等を出しておいていただけると議論が効率化するという面がありますので、御発言のある方はお願いします。

○（寺田委員）　事務局から欧州諸国における主なサイバー犯罪捜査手法として、通信傍受が述べられましたが、これはどの程度の技術的なレベルのものが行われているのでしょうか。また、外国との協力において、日本ができないとなった場合の不利益や困ることがあれば教えてください。

○（事務局）　被疑者及び犯罪に協同していると思われる者の通信状況をモニタリングして、かつその内容についてもチェックをするということで、どういったメールのやりとりをしているか、どういったアンダーグラウンドサイトに書き込みをしているかといったことを把握するものになっております。

○（寺田委員）　暗号通信等に踏み込むことまではやられていないということでよろしいでしょうか。

○（事務局）　そこは国によって違うのと、事業者によっては複号してくれる場合もありますが、例えばＴｏｒのように全く暗号化されて情報をとれないということももちろんございます。法的な部分は、日本でもいろいろ検討課題があるというところだと思います。

○（前田委員長）　課題を全て解決して報告書で書き上げるということではなく、解決の方向性をどうするか、今後の調査研究をどうするかという議論におさめざるを得ない部分もあると思いますので、これまで御議論いただいた問題が全て報告書の中できれいに整理されて答えが出るというのは、かなり難しいと思います。ただ、この会議が意味のある発展的な方向性につながるものであるということは御認識いただきたいと思います。

○（種谷局長）　報告書は、前田委員長がおっしゃったとおり、この中で全て解決できるものではないですが、ただ、各分野で大変御活躍されている方

からお話を聞きながら問題提起されたということを対外的に公表していくということは、それだけで非常に大きな意味があると考えております。先ほど星委員の御議論も解決するにはいろいろな問題があるのは事実で、問題提起という形のまとめ方にならざるを得ないと思うのですけれども、非常に有意義なものになると考えております。

○（前田委員長）　事務局で、本日まで御議論いただいたことをまとめていただき、次回会議の前に委員にお送りいたします。それを御確認いただいた上で次回の会議で更に議論して、報告書として取りまとめるという段取りで進めたいと思います。

９．閉会