平成 27 年 1 月 22 日

平成 26 年度総合セキュリティ対策会議（第１回）
発言要旨

１．開会

２．生活安全局長挨拶

生活安全局長の辻でございます。委員の先生方、大変お忙しい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。

平成 26 年度総合セキュリティ対策会議の初会合を開催させていただくところでございますが、本会議は今年で 14 年目となります。これまでいただいた御提言は、例えば、平成 18 年に運用が開始されました「インターネットホットラインセンター」、あるいは昨年業務が開始されましたいわゆる日本版ＮＣＦＴＡとして御提言いただいた日本サイバー犯罪対策センター、こういった形で、多くの具体的施策に結実してきたところでございます。今回の会合には、センターからも御参加いただいております。

本年度は、「官民連携を通じたサイバー犯罪に対処するための人材育成等」をテーマとして、警察におけるサイバー犯罪に対処するための人材育成の在り方について、民間事業者等における取組などを踏まえつつ、御議論をいただきたいと考えているところでございます。

サイバー犯罪に対処するための人材育成につきましては、昨年５月、情報セキュリティ政策会議において決定されました、「新・情報セキュリティ人材育成プログラム」で、「我が国の情報セキュリティ水準を向上させるため、とりわけ、政府機関等は自ら率先して人材育成に積極的に取り組んでいくことが重要である」と明記されております。また、警察におきまして、いわゆる遠隔操作ウイルス等による犯行予告事件を受けた「サイバー犯罪対処能力の強化等に向けた緊急プログラム」の取りまとめ以降、人材育成を含めた幅広い分野について、民間事業者等の知見の活用に重点を置きつつ取組を進めてきたところでございます。

ますます深刻化するサイバー空間の脅威に的確に対処し、国民の安全・安心を確保するため、人材育成を通じて対処能力を強化することは、警察における喫緊の課題でございます。

サイバー犯罪への対処については、官民それぞれの立場で様々な取組が行われておりますが、人材育成という観点からは、官民に共通した課題やそれらへの対策もあるものと考えております。委員の皆様におかれましては、それぞれの分野での御経験や御見識を踏まえ、闊達な御意見を賜りますようお願い申し上げまして、冒頭の挨拶とさせていただきます。どうぞよろしくお願い致します。

３．委員長挨拶

４．「官民連携を通じたサイバー犯罪に対処するための人材育成等」の趣旨及び検討項目について

【事務局から、本年度の総合セキュリティ対策会議の開催趣旨について説明】

５．サイバー犯罪に対処するための人材育成について

【委員から、サイバー犯罪に対処するための人材育成について発表】

６．警察におけるサイバー犯罪対策のための人材育成の取組について

【事務局から、警察におけるサイバー犯罪対策のための人材育成の取組について説明】

７．民間企業における人材育成の取組について①

【委員から、民間企業における人材育成の取組について発表】

８．民間企業における人材育成の取組について②

【委員から、民間企業における人材育成の取組について発表】

９．質疑応答

○（西本委員）　「中核捜査員」について、年齢層や年収はどのあたりのものを想定しているでしょうか。また、昨今は技術的知見を有する者の流動化が進んでおりますが、雇う側として、そのような情勢をどのようにお考えでしょうか。終身雇用的なものを考えているのか、それともスパイラル的に民間と警察とを行き来するものを考えているのか教えていただきたいと思います。

　加えて、事務局からの説明では、「サイバー犯罪対策のための」人材育成とありますが、本来であれば、捜査そのものの IT 化・多様化、つまり、通常の捜査でもサイバーに関する知識が必要とされており、その中で更にサイバー犯罪捜査員の能力の向上というものがあるのではないでしょうか。今回のテーマの立て付けについてお考えを伺いたいと思います。

○（事務局）　年収については、警察官は公安職なので、行政職に比べればやや高くはなりますが、正確な額は都道府県によって異なります。俸給表は公開されているので、そちらを御覧いただくのが分かりやすいかと思います。

　警察では、サイバー犯罪対策のために民間での勤務経験を有する者を中途採用しており、これまでに全国で 100 人余りがそのような形で採用されております。これらの職員については、基本的には採用後ずっと警察に身を置くことが想定されています。他方で、今後は、御指摘のとおり、一定期間警察で勤務した後に民間に戻る、任期付きの採用も視野に入れるべきだと思っております。これまでは一度警察に採

用されれば、捜査の特殊性に鑑み、その後もずっと警察で雇用し続けるという考え方がありましたが、技術の進化が早い中で、それらをフォローする上では、一定期間警察で働いた後に民間に戻り、またその後に警察に戻る、というように、官民を行き来する人材の流動化も、ことサイバーについては考えるべきだと思います。

年齢層については、特にこだわりはありません。警察の場合は階級社会であり、各階級においても年齢は様々であるので、どの階級であればどの年齢層でなければならないということはありません。その点は柔軟性があると思います。

また、警察では、サイバー攻撃を担当する職員や、技術職の職員もおりますが、今回のテーマは、それらではなく、サイバー犯罪対策に従事する者、さらに、その中でも、中核となる捜査員をターゲットとしております。

○（前田委員長）　一般の捜査においても IT 技術に関する知識は必要になってきていると思いますが、今回のテーマでは、そういったものとは切り離して考える、ということでよいでしょうか。

○（事務局）　そのとおりです。警察全体の底上げも重要ですが、今回御議論いただきたいのは、サイバー犯罪捜査を専門に行ういわゆる専務員の能力の向上についてであります。

○（前田委員長）　委員からの報告の内容について確認させていただきたいのですが、御説明いただいた人材育成は、富士通を守るための職員を育てるとの発想の下でその業務に従事する人材を個別に養成されているのでしょうか、それとも、富士通の職員として必要な知見を身につけるという観点から他の業務を行いながらそういった能力を習得するということなのでしょうか。

○（山下委員）　今回説明した３種類の育成領域については、一般の SE を対象としたものもあれば、セキュリティ関係に専従する、いわば中核捜査員を対象とする領域もあります。一般の SE の底上げも当然行いますが、セキュリティ関係の業務に従事する社員については、それらとは別に、専門の教育を通じて養成しております。

○（石井委員）　企業経営の観点から見た場合、ハッキングや情報漏洩に対して、セキュリティポリシーを策定して、社員の教育を行うことが一般的だと思います。セキュリティポリシーを策定して情報を守る上では、情報資産の価値を、一定の基準に基づいて整理する必要があると思いますが、情報については、将来的に研究開発に役立つか否かなど、貨幣価値と直接に結びつかないところもあると思います。御報告いただいた各社では、情報資産の価値をどのように分類されているのでしょうか。それとも、そのあたりについてはこれから詰めていくところなのでしょうか。

○（山下委員）　弊社では、経営に対するインパクトに基づいて優先順位を決めております。

○（徳田委員）　弊社では、業務上、ある情報の全体を任せられるということはあまりありません。このため、ある情報の評価について、機密性等の観点から点数付けをして、重要性を決めるという方法もあると思いますが、そうではなく、業務に紐

付けた形でアプローチしております。例えば、オンラインゲームのようなサービスであれば、それが止められると、復旧するためにどのくらいの業務が発生してどれくらい被害が発生するのか、といったところから判断します。

○（関口委員）　今回のテーマは、警察の捜査能力を高める、その目的のために人材を官民連携してどのように育成していくのか、ということかと思いますが、そのような理解でよいのか確認させていただきたいと思います。

次に、最近では、サイバー犯罪は高度化しており、サイバー攻撃とサイバー犯罪は分けにくくなっていると思います。従来で言えば、サイバー犯罪としては、不正アクセスなどを想定しているのだと思いますが、そうではなく、例えば、政治的、あるいは経済的な財産を狙った本当の意味での攻撃が顕在化し、そしてその大半が海外から、あるいは海外を踏み台として行われている実態もあると思います。これらに対しても、何か対策を講じることが出来る捜査能力を身につけることを想定しているでしょうか。また、そこまでいくとすると、防衛省との関係をどのように整理されるでしょうか。

最後に、根本的な問題ですが、警察は、基本的に、事案が発生しなければ動けない反面、企業におけるサイバー攻撃対策とは、事案の発生を未然に防ぐことを大きな目的としております。未然に起こらないようにするために、警察が民間にどのような協力ができるのでしょうか。

以上の３点について御教示いただきたいと思います。

○（事務局）　まず、想定するサイバー犯罪については、海外から行われるものも射程に入れております。例えば、一昨年後半くらいから被害が急増しているインターネットバンキングに係る不正送金事犯についても、多くが海外から敢行されております。しかし、ウイルスを送り込んで感染させるのは正にサイバー犯罪ですが、それらについては検挙できておりません。窃取した ID・パスワードを使用して口座にアクセスし送金された金を引き出す者については検挙できていますが、それらはむしろリアル空間の話です。ID・パスワードを窃取するような犯罪、あるいは、アカウントリストを用いた不正ログイン攻撃も確認されており被害が出ており、これも海外からの攻撃が多いですが、こういったものへの対策も出来ていません。こういったものが検挙できていないのは大きな問題であります。より高度なサイバー犯罪に対しても、検挙、あるいは何らかの形で実態解明を行う必要があるという問題意識は持っており、そういった犯罪捜査を行うに足りる人材を育成できればと考えております。

サイバー犯罪については、検挙が難しいものがあることは事実ですが、例え犯人の検挙にいきつかなくても、実態解明を行うことで、将来的な犯罪の予防に資することもあると思います。捜査に当たっては、単に犯人を検挙するという視点だけでなく、被害の未然防止の観点も重要だと思います。そのために、例えば民間を通じて、未然防止に資する情報を一般のユーザーに還元するなどといったことも重要だ

と思います。

○（関口委員）　最近では、ソニーに対するサイバー攻撃が記憶に新しいところです。この件では、ソニーの現地法人と FBI が相当緊密に連絡をとって対処したとのことですが、そういう態勢をサイバー空間において創っていくということも想定に入れているのでしょうか。

○（鈴木審議官）　今具体的に動いている事件のことなので、この場でつまびらかに説明することは難しいところもありますが、警察としては、御指摘いただいたようないわゆるサイバー攻撃についても、関係事業者や海外関係機関とも緊密に連携し、被害の防止に資するような対策を講じて行くべく対応しているところです。そういったことも含めて、広くサイバー犯罪を捉えていただければと考えております。

○（前田委員長）　事務局へのお願いとして、中核捜査員の育成を軸とすることはいいし、警察が国民の声に応えて人材を確保・教育していくということも大事なことだと思いますが、この会議では、民にもプラスになる形にする必要があると思います。サイバーに関する人材を世界の中で日本がどう育てていくかという話をする中では、西本委員が仰っていたポイントで、どれくらいの給料をもらえて、どれだけ魅力的なポストを提供できるのかということは非常に重要だと思います。人を増やすと同時に質を高めていくためには、「あそこに就職できる」等といった目標があることが重要であり、そういったところに議論が向いていかないと、発展的ではないのではないでしょうか。警察のテリトリーを越えてはいけないというところはあると思いますが、議論の発展の可能性は出していただきたいと思います。若い人の能力開発など、色々な意味から、サイバーは日本に向いていると思うし、力を発揮できると思います。警察庁で、トップガンに当たる人材をどう使うのか、あるいは、国民の安全安心を守るために、これだけの予算をかけてこれだけのポストを用意している、と示すことが重要だと思います。夢のある報告書、ここに集まった全員にプラスになる報告書にしていきたいと思います。

○（小屋委員）　前田委員長の御指摘に全く同感です。私は以前から、毎年、警察と防衛で、数百人単位で新人を採用し、セキュリティの専任として育成して、５年くらいしたら民間に還元してください、民間で２年くらい働いて、そのまま民間に就職するならそれもよし、警察に戻るのであれば、民間とのパイプになってもらう、というアイデアを話していました。

それとは別に、今回の議論について整理させていただきたいのですが、「中核捜査員」というのは、事務局のイメージとして、全国で何名くらいの規模感で検討すれば良いのでしょうか。

○（事務局）　多いに越したことはないというのが正直なところですが、中途採用者が全国で 100 人余りおり、基本的にはこれくらいは必要だと考えております。今後は、この層を広げて行きたいと思っています。ちなみに、サイバー犯罪捜査に専従する者は全国で 1,300～1,400 人おりますが、その一割程度が、今回想定している中

核捜査員として活躍しているイメージです。

○（小屋委員）　対象が 1,000 人なのか、100 人なのか、10 人なのかで論点の中身が全く違ってくるので、その点は重要だと思います。

加えて、その中核捜査員に必要なスキルセット、スキルマップの定義は警察内部で行っているのでしょうか。例えば、先ほどの委員の報告の中では、「この職に就く人はこのスキルセットが必要ですよ」という提示がされていて、社員はそれに向けて、足りないところを埋めていく仕組みになっていたと思います。ターゲットがある程度明示的である方が、議論は行いやすいです。例えば、外部の資格を採用できるのか、という話をするにしても、その資格で学べるものと、警察で必要とされるものとが合ってなければ採用できないでしょう。どういうスキルセットが必要なのかを明示していただければ、議論が行いやすいのですが。

○（事務局）　必要なスキルについては、組織内で見える化していないのが実情です。民間側の資格や研修を活用していく中では、そのスキルの見える化を進める必要があると考えておりますが、捜査員に必要なスキルは一概には定義できないところがあります。人材育成方針を策定する過程で、今回の御議論を参考にさせていただきたいと考えております。

単純化して申し上げれば、捜査は、まず犯人を特定するための情報資料を集めるものであり、特定した後には集めた情報資料により裏付けを進めるものとなります。そういう意味で、中核捜査員であるためには、まずは情報資料を如何に集めるか、どこにそういう情報資料があるのかという見立てを適切に出来ることが重要であります。一定の情報セキュリティに関する知見は必要ですが、フォレンジックなども全て自分で出来る必要は必ずしもないと思います。

次回、人事交流について発表する中で、可能なものについては資料にしてお示ししたいと考えております。

○（片山委員）　基本的な質問ですが、基礎から人材育成していくことも重要ではないでしょうか。サイバー犯罪に対しては多重防御をしていかないといけないと指摘される中で、サイバー捜査員も重要ですが、そのベースとなる捜査員の育成も重要ではないかと思います。事務局からの報告資料における人材育成は、全捜査員を対象としたものなのでしょうか。やがては専門の捜査員を育てるにしても、IoT の時代になっていく中で、基本的なサイバー研修を全員に行う仕組みはあるのでしょうか。

○（前田委員長）　警察大学校の方は今日は参加していないようですが、警察大学校の研修でも、どんどんサイバーに関するところを充実させる方向で変わってきていると聞いております。今後も一層充実していき、おそらく全職員を対象とする研修にもそういったところを反映させていくのでしょうか。

○（岡部参事官）　一般的な警察官全体に対する教育の話だと思いますが、中々充実したものにできていないところはあります。採用後の警察官への教養である初任課程でサイバーの授業がありますが、実機を使って実践的なことを行うものではなく、

「サイバー犯罪とは何か」といったところから始めるものです。また、一回現場に出た後に戻ってきて受講する補修課程でもサイバーの授業がありますが、初歩的なことしかできておりません。その後の教養については、都道府県警察の各課程の中で行われていくことになるのですが、残念ながら、サイバー犯罪捜査官を育成する課程以外のところでは追いついていないのが実情です。そこをどうするのかというところも課題です。教える側のスキルも問題であり、サイバー犯罪捜査に関する十分な知見を有する人がより多く教えるようになれば、事態も変わってくると思います。こういった場での議論も参考としつつ、検討していきたいと考えております。

○（藤川委員）　当初、「中核捜査員」の役割やイメージが分かりませんでしたが、話を伺っていると、初動対応を行う者なのだと理解しました。これに関して、サイバー系の捜査の標準化（マニュアル化）はどの程度なされているのでしょうか。例えば、「インシデントが発生したときに、証拠となるログを集めるために、どういうことをする」ということが全てマニュアル化されているのであれば、何でも知っている捜査員を育成しなくても、ある程度の知識がある捜査員でも対応できると思います。他方で、マニュアル化がされていなければ、確かに豊富な知見を有する人が対応しない限りは何もできないこととなります。捜査に関して、どのあたりまでマニュアル化されていて、それを越える領域というのはどういう領域なのかを教えていただきたいと思います。

○（事務局）　いわゆるマニュアル的なものは、警察庁でもいくつか作成しておりますし、都道府県警察でも作成しているところはあります。しかし、基礎的なものを除けば、「この一冊で全て網羅されている」というものはありません。捜査のベストプラクティスを警察庁でまとめて各都道府県警察に還元したり、知見を有する者が教養を通じて経験を伝授したりするなどの取組はしているところではありますし、定型的なフォレンジックなどについては、一部マニュアル化しているところはありますが、事件捜査は言わば生き物であるので、全ての事案に応用できるようなものがあるわけではありません。

○（則房委員）　現状の制限に囚われて話をするのと、理想を目指して話をするのとでは、かみ合わないのではないでしょうか。目標設定を共有することで、ベクトルを統一できるのではないでしょうか。例えば、東京五輪の際にはサイバー犯罪も非常に増えると思いますが、それらに対応できる態勢を構築することを考えた場合に、フォレンジックの能力を高めるだけで十分なのかといえば、おそらく十分ではないと思います。海外からの攻撃もくるのでしょうから、それに対応しようとすれば、海外のインテリジェンスをどう入れるか、それらをどう分析するかというところも考えなければいけません。そうなると、警察だけでできるものではなく、国内外の民間事業者や法執行機関との協力も想定しなければなりません。現状に基づいて議論をするのか、それとも東京五輪でサイバー犯罪が急増しても対処できるようにすることを想定して議論を行うのか、そのあたりを整理しておくべきではないでしょ

うか。

○（藤原委員）　事務局の資料に書かれていることは、役所の文章に慣れている人間からすれば、現状がどうなのかということがよく分かります。他方で、現状を踏まえて、どこまでどう動かしたいか、という話が見えてきません。先ほど、1,300 人から 1,400 人のうちの 100 人、という話がありましたが、質問の趣旨は、それをどこまで広げたいのか、ということではないでしょうか。第２回会議で説明されるのかもしれませんが、現状を前提として官民交流で捜査員の層を厚くするというところに軸足が行くのか、そうではなく、最初の質問にあったように、一般の捜査手法として IT ツールを活用できる人を育て、そのような人材がサイバー犯罪にも対応できるようにするということなのでしょうか。西本委員の御質問は、後者を前提とすれば、年齢は自ずと制限されてくる、という御趣旨だったと理解しております。そういったことではなく、都道府県警察を中心としてレベルを上げていこうということであれば、現状をどこまで変えて、民間事業者等とどのように協力していくのかを、こういう場であるのでもう少しはっきりさせてもよいのではないでしょうか。

○（桑子委員）　通信業界の立場から述べさせていただきます。プロバイダーは各都道府県警察とやりとりがありますが、都道府県警察のレベルが結構違うという話をよく聞きます。今回の人材育成の議論を進めていく際に、都道府県警察間のレベルの違いをどのように引き上げて行くのかというところも重要な観点だと思います。例えば、ある都道府県警察でレベル的に無理であれば、警察庁の中に特別なチームを置いて、その都道府県警察をサポートするという仕組みも必要かと思いますが、そのあたりも含めて、今後検討いただく必要があると思います。

○（前田委員長）　何をどういう形で議論するか、というところは、やってみて分かるものでもあります。次回は、藤原委員の意見、則房委員の提案なども踏まえて議論を進めていきたいと思います。五輪に特化するということは難しいかもしれませんが、目標がある程度見えてこないと議論がかみ合わないのは仰るとおりだと思います。色々なレベルの専門家の育て方が、少し整理ができたと思うので、これを踏まえて、また、次回いただく委員の方々からの御意見も踏まえて、報告書をまとめていきたいと思います。

10　閉会

（以上）