平成 27 年２月 10 日

平成２６年度総合セキュリティ対策会議（第２回）
発言要旨

１．開会

２．サイバー犯罪に対処するための人材育成等について
【事務局から、サイバー犯罪に対処するための人材育成等について発表】

３．サイバーセキュリティに関する人材育成について
【委員から、サイバーセキュリティに関する人材育成について発表】

４．サイバーセキュリティに関する能力評価について
【委員から、サイバーセキュリティに関する能力評価について発表】

５．官民人事交流に関する取組状況等について①
【委員から、官民人事交流に関する取組状況等について発表】

６．官民人事交流に関する取組状況等について②
【委員から、官民人事交流に関する取組状況等について発表】

７．討議
○（田井委員）　事務局から、2020 年に、サイバー捜査員が全体で 1300 名、その中で中核が 200 名というお話がありました。ここでいうサイバー捜査員は、どんなタイプのサイバー犯罪の捜査を行うのかという想定はあるのでしょうか。例えば、サイバー犯罪の中には、会社の中から何か情報を盗もうするものもあれば、一般の方々を標的としたものもあると思います。例えばそういった２つのタイプにどんな割合で対応されるのかなど、人数比などがあれば教えていただきたいと思います。

○（事務局）　サイバー犯罪については、その時々でどんどん新たなものが出てまいります。そして、言うまでもなく、その全てが捜査の対象となります。その中には、今おっしゃられた企業の情報を窃取するというタイプのものもあるでしょうし、現状でありますとインターネットバンキングをターゲットとしたサイバー犯罪、これが一番問題になっておりますので、これが中心的な課題になっているところです。恐らく 2020 年には、インターネット・オブ・シングスが一層進んでいると思いますので、今では想定できないような

犯罪も起きていると思われます。犯罪を捜査するにあたっては、捜査員が、犯罪者に負けない知見を持っていることが大事になってまいりますので、そういう意味では、中核捜査員には、いかなる高度なサイバー犯罪に対しても対処できるようなスキルを期待するところでございます。

○（前田委員長）　我々法律家の世界からすると、サイバー犯罪は、構成要件から非常に明確に特定されたもので、例えば、昭和62年の頃は、刑法犯のうちどれとどれかというところがはっきりしていました。その後、不正アクセス禁止法が成立するなどして、だんだん広がっていったと思うのですが、今では、普通の殺人の中にもサイバー的な手法で捜査するとか、脅迫の中にもサイバーを使ったようなものが入ってくるとか、その広がり方はものすごいものがあると思うのです。その中のどこをどう捉えていくかというのは、国民の目線から、警察が、どういうところに対応する力を持って安全・安心な社会を創っていくかというところによってくるのだと思うのです。ですから今の時点で、数で示すというのは非常に難しい面があるのだと思います。

○（石井委員）　中核捜査員の育成ということに対して、既存のサービスやトレーニングで担保できるところと、特別に作っていかなければいけないところがあるのかなと思いました。中核捜査員には、日々変わるサイバー犯罪に対して、先ほど課長がおっしゃられた事件の組立て、我々の言葉で言うところのサイバー犯罪プロセスのモデル化を行っていくことが必要になってくるのだと思います。萌芽的な情報に基づいてどこに犯罪の芽や証拠があるのかということを押さえていくというところが、中核捜査員の方々のミッションになるだと思いますが、そのためには、犯罪のプロセスを追っかけ、その全体像を理解していなければならないと思います。そして、それを可能とするためには、各企業がお持ちのトレーニングを受講したり、各企業に派遣されて、それぞれICTのテクノロジー、特にセキュリティのテクノロジーを深く研修されたりすることは、非常に重要なのだと思いますけれども、個別にそれがあった上で、アップデートなものがないと、犯罪捜査に有効活用できないのかなと思いました。

　今申し上げたようなサイバー犯罪プロセスのモデル化に必要なものは、例えばラックさんのようにオペレーションをされているところも含めたいろいろな企業の中にノウハウとして貯まっているのかもしれませんけれども、それが研修サービス化、あるいはデータベース化はされていないかもしれません。あるいは、そういったもの自体がアップデートで変化していってしまうので、それをモデル化していくのは難しいのかもしれません。それでも、そういったものの中でも官民連携、もしくは官民学連携で新たにプログラムとして作っていかなければいけないところと、それから各企業さんが既にお持ちで、人材交流によって補填できるところとに分かれるのかなと思ってお

ります。まずは、あるものについてなるべく早く活用できるような手だてを講じることが重要ではないかと思います。それから、ないものについても、重要なところについては、どう作っていくかというところを話し合うことが非常に重要ではないかと思いました。

○（岩井委員）　私は、フォレンジックインベスティゲーター、あるいは解析者といった観点から少しコメントさせていただきたいと思います。

まず、サイバー犯罪に関して解析を行う際に、１人の優秀な人間だけでは解決できず、分析をする人間が、２、３人で、頭を突き合わせて議論することが結構多いです。そういった観点からすると、この目標値の 200 名プラスアルファというのは、もしかしたら足りないのではないかと感じたところです。

あと、人材育成という観点から、解析する上で結構悩ましいのが、経験値なのです。ここは量れないところだとは思うのですが、この経験値がなぜ大事かと言いますと、サイバー犯罪の場合、最新の手法、「この手口が使われたな」という、ひらめきみたいなものが出てくるかどうかは、どういう事案を扱ってきたかという経験則に基づくケースが非常に多いです。そういった意味だと、１人の中核捜査員だけに頼るというのは、少し難しいところがあるのですが、その経験値をどうやってつけていくのか。あるいは、実は、例えば解析するのに１つの製品に頼って解析するということはまずないです。というのは、それぞれのフォレンジックツールでもアルゴリズムが若干違って、Ａというツールでは出てくるけれども、Ｂというツールでは出てこない、こういったのも実は経験則に基づくところだったりもしますので、こういったところをどうやって身につけていくのかというところ。これらを踏まえると、官民連携という意味で、資格において、段階的なものを用意することに加えて、その間で OJT であるとか実施研修みたいなものが入るようにすると、より優秀な人材が育つのではないかなと感じました。そういったところも、検討いただければと思っております。

○（小屋委員）　まず事務局から「委員の御意見」と書いていただいているところについて申し上げます。基本的には、中核捜査員に必要なスキルなどがある程度洗い出せてしまえば、それに従ってできる限り既存の研修を使いつつ、また足りない部分はしつらえて、着々とやっていくのかなと思います。それに加えて、岩井委員がおっしゃったような、学問と実施の力というのは違うところがありますので、その辺りは民間からの知見と、今いる捜査員からの知見を組み合わせていけばいいだろうなというふうに思っております。その過程では、なるべく民間の資格などを使っていただいたほうがいいのではないかと思います。人材交流などをやっていく上では、スキルについてお互い理解しやすい方が、相互の理解も進むと思いますので。

人事交流については、例えば民間から警察に派遣させていただくようなことがあるとすれば、我々のような仕事であれば、技術者にとっていいキャリアになると思いますので、そういう機会があれば、私どもとしても、検討したいと思います。

まだ時間があると思いますので、先日少しお話しした私のアイディアについて、この機会に述べさせていただきたいと思います。

御存知のとおり、日本はどうも IT 活用が遅れたというか、企業や個人の IT 知識が他の先進国に比べると若干遅れているのかなという個人的な認識があります。そして　その結果、セキュリティの知識も当然向上してこなかった。更には、初等、中等及び高等教育についても、IT 及び、IT セキュリティというのはやや遅れているのではないかと思います。昨今は、初等、中等の教育の改善と、高等教育でも、新たなセキュリティの教育をしようというムーブメントが出てきていて、非常にいい傾向だと思うのですが、実際に問題となるのは、出口だと思うのです。つまり、そこで勉強した人が、どこに行って何をするのかということが非常に難しいのです。普通に初等から上がってきた人はどうするのか、そういうセキュリティ技術者を採用する企業はどこにあるのかと考えると、普通に学問を学んできて大学を卒業したセキュリティ知識の高い人を、会社のセキュリティ部門にぱっと当てはめるのは非常に使いにくいと思うのです。業務が分かっていないので、しばらく使えないのではないかと思います。では開発で使うのかというと、これもまた少し違うかもしれない。また、民間企業ですと、コストとの兼ね合いもありますので、セキュリティに割く人材をそんなに大量には採れない。ではＳＩか、あるいは私どものようなセキュリティ企業に採用されるのかというと、企業が少ないということもありまして、現状のところ、実際にそういった企業で採用される数はあまり多くないという問題があります。ISP にセキュリティ技術者を固めてしまうというアイディアもあるのですが、ここではそれは省きます。

では、ニーズがどこにあるのかと考えると、やはり２つだと思うのです。１つは警察。御案内のとおりサイバー犯罪は非常に増えていますし、ハードディスクが大容量化して、1 件の解析でも工数が非常にかかります。SSD は難易度が高くなって、更にこれから IoT も含めて機器が多様化してきますので、スキルの多様化も必要になってくると、そこには一層大きな工数が必要になってくるだろうと思います。しかし、現状のところ、頼む民間は、日本では数が限られています。数を増やそうとしても、民間は他の仕事をしたほうが儲かるかもしれません。

もう１つは、防衛です。サイバー戦争・紛争がこれから起きてくるだろうという理解はコンセンサスがあるところでしょうから、この紛争への用意と

いうのはしなければいけない。

ここでは防衛の方はおいておきまして、例えば警察で、毎年 100 名から 200 名－数は今後検討してほしいと思うのですがーセキュリティ専門ということで採用して、5年程度－期間もまた検討だと思うのですがー、セキュリティ技術者を育成するのです。例えば1年に 100 名であったら、都道府県警察に派遣したら、1年に2名となりますので、そんなに大変多い数でもないとは思うのです。また、そこで、もう少し多くの人間を採用して、都道府県警察に派遣しない部分を人事交流と言うことで2年程度民間に派遣して、仕事をさせて戻すということをすることも考えられます。彼らには、派遣先の民間企業のセキュリティ体制の構築とか、インシデントレスポンス、あるいは職員の教育等、いろいろやることはあると思うのですが、こういう形でずっと交流を続けていけば、警察側からすれば、捜査で必要なスキル以外のスキルが習得できると思います。と言いますのも、捜査というのは、どうしても後追いになりますので、事案が発生する前とか発生した直後については、捜査からは触れることが難しいケースが多いと思うのです。こういったものも、企業の中にいれば、犯罪が起きればという前提は付きますけれども、経験することができます。それからもう1つは、捜査される側を理解することができると思います。残念ながら、企業さんは、犯罪にあったとしても、「これでハードディスクを警察に持っていかれたら仕事にならないから、言わないで済むなら済ましたい」という意識があると思うのです。相互理解をすることによって、この辺りについて、「警察は理解してくれるから、ビジネスの邪魔にならないように捜査してくれる」などというふうになれば、警察への信頼度も高まって捜査の効率化が進むと思います。それから、企業との情報交流基盤ですね、フィジカルな世界では結構各企業は警察との交流があるかと思うのですが、サイバーの世界で、その窓口があるのかというとまだ分かりません。それをいろいろ作っている努力も存じあげておりますが、人材交流からより親密な情報交流基盤が生まれるのではないかと思います。それから、学問としては学べない最新の犯罪、トレンドの把握ができる可能性もあると思います。更には IT 技術です。実際に企業で IT がどのように使われているのかということを知ることは、捜査をする上でも有用だと思います。

更には、そういった方が民間に採用されるような動きがあるのであれば、技術者のキャリアパスができるのではないかと思います。企業側が得られるものは、1つはセキュリティの対策能力です。やはりコストの観点は無視できませんので、無尽蔵に人を採ることはできませんが、警察から人材として来ていただくと、一定のセキュリティ能力があるはずですから、それを社内に広めることによって、実際の即戦的な対策能力になるだろうと思います。

もう１つは、警察とのコネクションです。企業側としてもそういったところがほしいケースもあるかと思いますが、そういう基盤ができると思います。折り合いがついてその方を採用したら、採用コストを非常に安く採用できる可能性もあります。これも企業にとってはプラスになると考えられます。

このような枠組みの結果として期待される効果としては、１つは出口の拡大による高等教育への好影響です。セキュリティを勉強したいという人材が増えることが期待できます。これによって、民間のセキュリティレベルの底上げも期待でき、民間のセキュリティ自体が幅広く上がるのではないかと思います。そうすれば、結果として、セキュリティのニーズが高まり、セキュリティ産業が拡大しますから、更にセキュリティ産業側で雇用があり、出口の拡大につながるのではないかと思います。

もう１つは、捜査能力の向上です。企業とのコミュニケーションが取れるようになりますので、企業からの犯罪の申告なども増えて、初動対応がたくさんでき、捜査能力が向上すると。それによって犯罪効率が低下して、抑止効果も生まれるのではないかと考えられますので、是非どこかの機会でこういったことも御検討いただければと思います。

（坂委員）　私ども日本サイバー犯罪対策センターは、米国の NCFTA を倣って昨年の 11 月から業務を開始させていただいておりまして、先週、私は米国の NCFTA に行ってまいりました。その中で印象に残っているところを申し上げれば、まず、プレジデントのマリア・ヴェロさんはコミュニケーションが非常に重要だとおっしゃっていて、NCFTA が活躍して事件を検挙した話も本当に熱っぽく語っていただきました。その中での、産官学の連携や協力の在り方というのは、エクスクイジットと言いますか、精妙な感じがするほどですが、それが本当にさりげなく行われていることに、改めて印象を受けたところでございます。

また、本会議のテーマの育成という観点については、NCFTA の名前にも、Training が入っておりまして、トレーニングルームなどもあるのですけれども、やはり、捜査員や民間において、インシデントに対応されている方々の能力を実際に高めているのは、一緒に勤務して成果を出していく、その過程なのだなと改めて思ったところでございます。今日は捜査員の育成がテーマですので、この NCFTA、そして日本で新しく立ち上がった JC3、こういった組織で勤務することによって、捜査員が身につけられるスキルや能力を考えてみますと、１つには、脅威の大本に迫るために、いったいどのような要素や要件が必要なのか、そしてそれをどうやって組み合わせていったらいいのかということが、非常に身についていくのだなということが感じられました。この点から、中核捜査員が事件の指揮官をサポートするということを考えますと、非常に有力な能力が獲得できるのではないかと思ったところで

ございます。それに加えて、事案の分析能力、あるいは対応能力も身につくのは言うまでもないと思います。それから、産学官の連携というネットワークができる、これはもちろんそうなのですけれども、ちょっと驚きましたのは、米国は、御案内のとおり FBI や DHS などいろいろな捜査機関があって、実はそういった捜査機関が NCFTA には全部来ている。それから、外国の捜査員も来ているということで、捜査員同士のコミュニケーションも非常に高まって、捜査における協力体制も非常に充実しているのだなということを実感しました。日本の場合は、警察庁で様々なスキルの取得などを進められており、また、全国の警察が協力しながらネットワークも作っておられるので、こういった面では、米国ほど利点は大きくないのかもしれませんけれど、それでも向上するだろうなとは思っているところでございます。それから、私自身、この３か月間いろいろやってみて、あるいは米国での状況を見て、捜査員にとっては、やはり被害者の立場に立った事件捜査ができる、言い換えれば、企業の立場も、企業が接するお客様の立場もよく分かるようになるということは、非常に良いのではないかと思ったところでございます。それから、ＮＣＦＴＡの場合は、脅威の大本に迫るということに加えまして、その無力化、再発防止といったところも考えますので、要件定義の話と重なりますが、捜査ということのみならず、その後の防犯対策、再発防止対策といったところについての視点も身につけられるのではないかなと思っております。

NCFTA というのは効果のあるものだなというふうに改めて思ったところでございまして、私どもまだできたばかりですけれども、もし捜査員の方々、あるいは委員の方々と一緒に活動できるということがあれば、こういった効力を発揮できるように頑張っていきたいと思っております。

○（関口委員） 感想と、それから意見を述べさせていただきたいと思います。まず感想ですが、発表された委員の企業さんが、そういった取組をされているというのは、私もよく知らなかったのですが、大変有意義なことだと思いました。ただ、プロダクトを扱っているメーカーでの教育・研修は、どうしてもそれぞれの製品に基づいたものになってくると思いますので、技術がどんどん日進月歩でいく中で、それを超えたサイバー犯罪にどう対応していくのかということは、話を伺っていて、なかなか難しいなと感じた次第です。そして、そういう意味から、どうやって実践的な捜査能力をつけていくかということを考える必要があるのではないかなと思いました。

もう１つ感じたことは、例えば SSD の普及などの技術革新にどう対応するのかという点です。SSD もそうなのですが、今までのデジタルフォレンジックは、オンプレミスの世界を前提としてきたと思うのですが、ここのところクラウド化がどんどん進んでおり、クラウド化した中を中核捜査員が捜

査しようとしても、かなり難しいのではないかと私は率直に思っているところです。だとすると、今日ここで議論していることは、官民協力によって、警察庁ないしは警察の中核捜査員を育てるということなのですけれども、それ自体に限界があるのではないかと思います。少し話をひっくり返してしまうようで申し訳ないのですけれども。

では何を申し上げたいかと言うと、人材育成のための協力ももちろんのことなのですけれども、犯罪捜査そのものを官民協力でできるような枠組み作り、つまり、警察権は警察が持っているわけですけれども、そこに民間がNDA ベースで上手く加わっていく仕組みを作らなければならないのではないかと思いました。犯罪捜査は警察の権限であると思いますので、譲れない部分もあるかもしれませんが、あるいは、それはサイバー犯罪対策センターの仕事なのかもしれませんが、一方で民間企業、特にクラウドベンダーが協力していけるような仕組みを作らなくてはいけないと思います。ただ、クラウドベンダーを見てみますと、最近は日本でもいろいろと出て来ていますが、多くがアメリカのクラウドベンダーになってしまっています。ですから、そういった海外の企業とも、日本の警察当局がリレーションシップを作らないことにはクラウド時代におけるデジタルフォレンジックは難しいのではないかなと思います。そうした枠組みをどうやって作っていくかということも、併せて議論していく必要があるのではないかと思いました。

オンプレミスの世界でも、最近は、インメモリコンピューティングというものがどんどん増えていっております。SSD とはまた少し意味合いが違いますけれども、通常のハードディスクベースのものに比べると、やはりそういった面で捜査が難しいのではないかと思います。そういう新しい技術に対してどう対応するのか、そのあたりもまた、今後議論できればいいのではないかと思いました。

○（田井委員）　私どもマカフィーも企業様に対して、SIEM と言われるログの解析ツールを提供しまして、社内で起きたインシデントに対して、そこにいる方々がフォレンジックを進めていくというようなことを手助けしております。正に起きていることは同じです。企業様の中で、そういったことを始めるに当たっては、まず人が足りないということは明らかです。SOC という組織を作る、それから CSIRT という組織を作るとすると、そこに従事する人をどうやって教育するかということになり、私たちもセキュリティ会社としていろいろな教育を提供させていただいて、人材育成をお手伝いしているわけですけれども、どんどんインシデントが増えていく中で、やはり人はいくらいても足りません。そういう中で、今、多くの企業様が取り組んでいることを、お話をさせていただきたいと思います。

１つは、情報の共有化ということです。まず、グローバルな情報、これは、

悪いIPアドレスやスパム情報、ファイル情報などの私どものようなセキュリティの会社が持っているいろいろな情報、こういったものをいかにリアルタイムで企業様にお伝えするかということです。そして、コミュニティナレッジと言われているものもあります。これは、アメリカの金融ISACに代表されるように、あるインダストリーで持っている情報をいかに横で活用していくか、それをリアルタイムで活用していくかというものです。それから、ローカルのナレッジということで、その会社の中で見つけたナレッジを、1人が持っているのではなくて、いかにそれを集めるか、集めてそれを再利用できるようにするかというものもあります。これらは、1つ1つを紙に書いたりすることは非常に難しいですので、何かツールのようなものを使って、これらをまとめてインテリジェンスとしてどうやって活用するかということが大事だというような議論をしております。

もう1つは、情報だけではなくて、プロセスです。何か起きたときにそれに対してどう対処するのか、あるいは、こういったものに対してはどういうふうにフォレンジックを進めたらいいのか、などについても、1回プロセスとして回してみると、次に同じようなことが起きたときに、それを再利用できるような仕組みをいろいろな企業が自分で作ったり、あるいは私どものようなセキュリティ会社がいくつか作ろうと試みていたりします。

人材教育ももちろんですが、このように、いろいろと官民共同でやっていくと共に、こういった情報をいかに共有していくかというようなところも是非、御協力できたらと思っております。

○（寺田委員）　実際のサイバー犯罪などの捜査がどのような形で行われているのかということについて、本物の事例ではなくても、一般化した事例の形であっても、企業側のCSIRT等の人達に伝わるだけで、問題の解決のアプローチの一端が出てくるのではないかと思いました。その意味で、人材交流という部分については、皆様の取組の中でどういうものが求められているのかといったところも含めて一緒に議論させていただけると、警察庁さん、警視庁さんと民間もより協力できる仕組みができるのではないかと思いました。是非一緒に検討させていただければと思いました。

○（外村委員）　私からは3点ほど申し上げます。まず、セキュリティに限らず技術に携わるものとしては、人材育成というのはいちばん大きなテーマなのですけれども、人材育成というと、セキュリティに限らず、5年とか10年はかかるものだと思います。ということは、やはり2年毎に仕事が変わってしまうような、そういう場ではなかなかきっちりとした人材を育てるのは難しいところがあると思いますので、まずロングスパンで見るということが、1つ重要かなと思います。

2つ目が、前回の委員からの発表を伺っていまして、共通して言われてい

たことで面白いなと思ったのが、人材育成と言いつつトップノッチは育成ではなくて、発掘してくるという趣旨のことを共通で言われていました。もちろん育成できないという話ではないと思うのですけれども、やはり育成だけではなくて、好きでやっている人間ほど強いものはございません。1000 人のコミュニティがあれば、その中でそういう人間がいるかもしれないと思います。したがって、育成していくというだけではなくて、発掘するということを考えてみると、意外といい結果が出てくるかもしれないと思いました。

３つ目が、フォレンジック等々を踏まえて、捜査を保全と収集と分析というふうに分けると、保全と収集という部分に関してはそれぞれ個別のスキルが必要かと思うのですけれども、分析というところでは、コミュニティの力と言いますか、大きなデータを集めてくるだとか、そういった部分がどうしても必要になると思います。したがって、分析は当然１人あるいは数人だけでやるだけではなくて、我々セキュリティベンダーは膨大なデータを持っておりますし、そういうものと突き合わせたり、あるいはインテグレーションしたりする力というのが、どうしても必要になってくるのではないかなと思います。したがって、コラボレーション、あるいはインテグレーションといったところを分析については少しお考えいただいた方が、お互いにいいものができるのではないかなと思いました。

○（中野目委員）　まず、犯罪の実態という点から見ると、例えば銀行口座からお金を引き出すというようなものに限らず、国防に関係する情報を盗んでいくといったこともあります。必ずしも法制のほうがデジタルインフォメーションの保護に追いついていないという面もあるわけですけれども、そういうナショナルセキュリティに関わるものと通常の犯罪に関わるものを綺麗に分けて、「ここは別の組織がやって、ここから警察庁がやる」というふうに上手く区切りができるのかという点であります。そういう点を踏まえれば、関連する組織間で連携調整、コミュニケーションを図りながら今後の犯罪捜査に携わる人の育成ということを考えていく必要があるのではないかなということがあります。

それからもう１つは、今回官民ということで、どちらかというと大学の陰が薄い構成になっているわけですけれども、長期的に人材を育成していくことを考えた場合には、やはりサイバーに関係する種々の技術について理解をした人をどれだけ多く輩出していくかという視点を欠かすことはできないと思うのです。そういう点で、大学教育を充実させていくとすると、必要な官庁への働きかけであるとか、予算を始めとする資源の配分を考えていかなければならないということになると思います。それと、先ほど、要件定義、そしてその中で、セキュリティについてどのように対処するのかという方針が大切であるというお話があったと思います。全体として、法制度、更には

法制度がない場合の犯罪に対する包括的戦略の下で、犯罪やナショナルセキュリティにかかわる活動への対処をどういうふうに進めていくのかということも併せて大学教育等の中で学生に教育するなり、研究を進めることを促すなりしながら、企業に入っていく、あるいは警察庁に入っていく前段階で、しっかりとした見通しを持てる人材を育てていくということが重要なのではないかと思います。

短期的、中期的、長期的に見て、いろいろな人材の育成の仕方があると思いますけれども、長期的に見た場合の大学教育の意義も考える必要があるのではないかと思う次第です。

○（則房委員）　これまで発言されている方々と同じことを言うのは避けて、別の視点から、サイバーセキュリティ人材の育成について、何が重要な課題なのかというところを述べたいと思います。

幣社はICTベンダーなので、IT技術者は非常に多いです。セキュリティについても、従来からの情報セキュリティについては社として結構長く取り組んでいるので、それを扱える技術者も、100人単位でいると思います。

しかし、サイバーセキュリティ技術者がどれぐらいいるのかというと、極めて少ない。しかも、たくさんいるIT技術者とセキュリティの経験のある人達をサイバーセキュリティ技術者に換えればいいじゃないかという話は、外からは簡単に見えるのではないかと思うのですが、配置転換は非常に難しい。IT 技術者と従来のセキュリティ技術者というのは、例えば、製品かシスタムを使うために、ある技術を実装する、というようなメンタリティーでものを考えられる人達です。しかし、サイバーセキュリティ技術者がどんなことを求められているかというと、相手の攻撃に合わせて対応するというような、どちらかと言えば、物を作った後の営業の観点から作業をしなければならず、そこの部分というのは、従来のIT技術者やセキュリティ技術者にはぽかっと欠けているところなのです。このため、配置転換したとしても、そう簡単にすぐできるようにならないという悩みがあります。配置転換については、もっと他にもいろいろな話があって、そう単純な話ではないです。

サイバーセキュリティ技術者の育成を内部で考えた場合、まず、OJT 環境が非常に少ないと思います。環境が少ないので、それを受ける機会も少なく、対象となる人たちのレベルが上がっていくのも少しずつになってしまいます．このあたりが、ここ３年間ぐらいで何となく感じている状況です。サイバーセキュリティ技術者を抱える他の多くの企業でも、同じような状況ではないかと思います。

そして、日本のセキュリティ技術者の８、９割が実はどこかの企業に属しているのではないかと考えると、その人たちがサイバーセキュリティ技術者に上手く変わっていかない限り、実行する人数が極端に欠けた状況、レベル

がなかなか上がらない状況から抜け出せないというのが、日本の状況ではないかと思うわけです。そして、そこを上手く解決していくのが、人材育成の課題ではないかなと思います。

例えば大学は、10年先を考えて、いろいろな技術者を今育てて、10年後にすごく優秀な人たちが出るという形がいいのですけれど、2020年と考えてここ４、５年ぐらいで何とかしないといけないと思うと、８割、９割ぐらいのポテンシャルはあるのだけれど、サイバーセキュリティ技術者に欠けている部分がぽかっとある、この人たちをいかに官民の連携とか人材交流といった視点から上手くできるようにして増やしていくというのが非常に重要なポイントではないかなと思っている次第です。

○（藤川委員）　当社も年間数十件調査を依頼されて、企業の元に行って、改ざんされた、情報が盗まれた、不正利用されたということで、調査しております。その中で、例えばウェブのログからすぐ分かるような、攻撃として分かりやすいものであれば、全然時間はかからないのですが、最近のシステムの不正利用については、そもそもシステムが不正利用されるということを前提とした作りになっていないために、極論をすれば、調べても中々分からないところがあります。一番厄介なのは、アプリケーションのレイヤだと思っています。そういう意味では、今日、事務局の資料の中に、中核捜査員に必要な技術ということで、コンピュータ、ネットワーク、サイバー犯罪の技術、手法、コンピュータの解析というものがあるのですけれど、こういう要素技術以外のところで、一番問題なのは、システム全体を分かっている人があまりいないことだと思います。例えば、私どもが調査した案件では、ショッピングサイトの利用者から不正に利用されたという申告があったときに本当に不正利用かどうかということを、システム的に調べていくということが、非常に難しい。そのためには、我々もコンサルタントを連れて行き、どうやって不正利用が行われ得るのかという分析をしたり、あるいは、開発したメーカーさんにアプリケーションがどういうふうに動作して、どういうふうにデータベースのレコードを書き換えているのかを全部説明を受けるＳＥを連れて行ったり、それから、ウェブのログに詳しい人間を連れて行ったり、要はそういう人間が全部チームとして揃わないと、本当に何が起きているかが分からないという状態です。そういう意味では、今回の中核捜査員については、全体像をきちっと押さえられるような方を育成されるのだろうなと思います。そうすると、私どもの社内でもそうなのですが、我々のチームで全体を知っている人は実は意外に少なくて、やはりデータベースはデータベース、ネットワークはネットワーク、アプリケーションはアプリケーション、日頃それぞれの仕事をやっている人間がセキュリティも意識しながら何かことがあったときに、みんなでチームを組んで調べるしかないという状況が

あります。

育成というところで我々が今一番力を入れているのは、事例研究です。事例を見ながら、どういう不正利用が行われたのか、何を調べれば紐付けができるのか、といったところを蓄えていって、それを捜査員の皆さんが共有することで、相当効率化も図れるのではないかなと思います。そういう意味では、JC3 にそういう知見をたくさん蓄えながら、育成もできるような環境ができあがってくると、非常に効果的だと思っております。

○（別所委員）　私ども、これまで第一線の捜査員の方々の研修に協力させていただいてきておりまして、全国の各都道府県警本部さんが開催しているサイバー専科などにも、かなり精力的に講師を送らせていただいたりしております。全体感から言いますと、これまで生活安全部門に限られていたものが、次第に刑事部門などにも受講していただけるようになってきていて、非常に望ましいと思っています。その上で、中核捜査員の拡充に向けて検討が進むということは非常にありがたいことだと思っておりまして、民間企業としてできる協力はさせていただきたいと考えております。

資料１の論点に沿って若干意見を述べさせていただきます。「実践的な資格制度の整備」ですが、残念ながら本日のお話を伺っても中核捜査員に求められる資格要件、技術要件がまだ明確ではないと思っています。そこを明確にしていただくことが、次に述べる官民の人材交流でどういう人材を企業側から出したらいいかというところにも密接に結びついていきますので、何らかの形で明確にしていただきたいと思っています。なかなか難しいかもしれませんけれど、例えば、資格制度を当てはめていけば、その資格制度の中の捜査員に求められる要件が自動的に決まってきます。「こういう資格が」という形でも結構ですので、明確にしていただけるとありがたいと思っております。

「実践的な研修」ですが、今、藤川委員がおっしゃったことと少し重なりますけれども、サイバー犯罪捜査に要求される要素について、犯罪捜査経験ももちろん必要だと思っていますし、IT のセキュリティ技術も必要だと思っていますけれど、それに加えて IT ビジネスの仕組みに対する知識、いわゆる「IT ビジネス知識」というようなものも必要ではないかなと思います。実際の IT 技術が、ビジネスの中でどのように使われているのか、犯罪者がそれをどのように犯罪に悪用しようとするのかということを、見知っていただくことが非常に重要ではないかと思っております。この部分については、IT サービス企業として御協力ができるのではないかと思っています。その１つの方法としては、官民合同研修のようなものがあるのではないかと思っております。この官民合同研修において、捜査機関の方々には、IT サービスの仕組みや技術の使われ方を知っていただいて、犯罪者がそれをどのよう

に悪用していくのだろうかという視点で見ていただける機会があるのではないかなと思います。逆に民間側は、犯罪者の視点でサービスを見直すということがなかなかないので、そういう視点での見直しの機会を得ることとなるのに加えて、証拠の保全の必要性などを実感して、技術者サイドで、万一の場合に備えた仕組みを考える機会につながっていくのではないかと思っております。

人材交流については、先ほど基準を明確にというお話をさせていただきましたけれど、ミスマッチがないようにしていただきたい。特に、IT 企業側から人材を出す場合に、１年という期間はかなり長いと思います。技術の進歩は非常に激しいですし、ある程度の規模の企業になっても組織体自体をかなり柔軟に動かしていきますので、送り出した人材が１年後戻ってきたときに、浦島太郎のようになってしまうと非常に困ります。こちら側から人材を送る期間については、１年ではなくて、もう少し柔軟に考えていただきたいということと、企業からすると、第一線級を出すというのは至難の業なので、年齢層も少し若い人材の間で交流が進むようにしていただければと思います。企業側が期待していることの１つは、捜査機関でいろいろなことを勉強させていただくことと併せて、捜査機関の方々との人脈ができて、何かあったときに、お互いに相談しやすい関係を築くというところが非常に大きいと思っていますので、その辺も配慮いただければと思っております。

○（宮下委員）　ここでは当然の前提とされているのかもしれないのですけれども、サイバー犯罪捜査における中核捜査員を育成するにあたっての役割分担というのがどうなっているのかということについて、必ずしも議論が詰められないまま話が進んできたのかなと思うところもございますので、気付いた点についてお話をさせていただきたいと思います。

別所委員からもお話しがありましたけれども、サイバー犯罪捜査における中核捜査員とはいったいどのような捜査員なのか、いったいどんな業務をして、どんな知見を持ち、どんなスキルを持っているのかということについては、犯罪捜査の範疇でありますので、これを決めるのは、警察であるということに誤りはないと思います。そういう意味で、この中核捜査員というものについてどのように考えるのかということについては、今日も出されてはいるのですけれども、基本的には警察のほうで、過去の捜査の実例－これは必ずしも成功しなかったものも含めて－そういうものを十分に吟味された上で、御提示いただく話なのかなと思います。もちろん自由にしていいというわけではなくて、国民の負託に応えることができる、フィージブルなものである必要があると思いますけれども。この時間では概括的なものしか挙げることができないと思うのでが、しっかり詰めればかなり細かなものになるのだろうなと思います。これについて民間側ができるかというと、今日も御説

明いただいた民間の資格制度、非常に優秀なものでございますけれど、それが中核捜査員の資格制度、あるいは研修にそのままあてはまるかと言うと、よく分からないと思います。吟味した上であてはまるかもしれないし、あてはまらないかもしれないというところかと思います。その意味で、中核捜査員というものをどのようなものにしていくのかということについては、これはやはり捜査側あるいは警察から明確にコンセプトを出していただく必要があるのではないかというふうに感じました。

ただ、何が必要なのかということについて、官が十分に示した場合には、その要素がどのように最大あるいは最適に実行できるのかということについては、民間は助力できる部分が多分に、いろいろなレベルであるのではないかと思いましたし、本日の各委員の御発表もその点をまさに裏付けているのではないかと感じました。

今後、具体的に御検討するにあたっては、是非そのあたりを御留意いただきたいというふうに感じております。

○（徳田委員）　補足的になりますけれども、私は、IBM の中で、インシデントが発生した現場での対応を行うチームを結成しているのですけれども、その育成やそのメンバーの選定にあたっては、多様性を持たせるということに注意をしています。皆ログやフォレンジックもできるのですが、同じような人が同じインシデントにわーっと行くと、アイディアが出てこないということがあります。これに対して、例えば、昨年、データベースのスペシャリスト、ものすごいトップの技術を持っている人を１人入れただけで、非常にチームが活性化してインシデントに対する対応能力が飛躍的に大きくなったという経験がありました。こういった中核捜査員の教育にあたっては、パッケージ化はされると思うのですけれども、その次くらいのフェーズで、なるべく多様性を持たせるような進め方、個人個人の能力や方向性に見合ったやり方をした方が効果的ではないかなというところを、個人的な意見として挙げさせていただきたいと思います。

○（山下委員）　今日、事務局からサイバー犯罪捜査班の概要を説明していただいたのですが、私の担当しているCSIRTのチームに似ているなということを非常に感じました。ちなみに、私たちの方での、捜査主任官に関しましてはCSIRT指揮官、また、中核捜査員に関しましてはチームリーダーに相当します。

CSIRTの業務には、セキュリティ侵害の原因やシナリオの特定などがあり、まさしく捜査のようなこともやっております。事案が発生した場合には、指揮官とチームリーダーは、まず、人材リソースのアサインを行います。つまり、前回会議で富士通におけるセキュリティマイスター制度の20種類の人材像を御説明しましたけれども、その中から、例えば、「今回の

事案は、”フォレンジックエンジニア”は２名、”セキュリティアナリスト”が２名、”サイバーリサーチャー”が１名、”セキュアネットワークコーディネーター”が１名」といったように、大体５名から７名ぐらいの人材をアサインして事案にあたります。

また中核捜査員にあたるチームリーダーに関してはどのような育成をしているのかといいますと、20の人材像全部をカバーするのは難しいですから、最低３つはカバーさせています。最低３つをカバーさせて、なおかつ場数を踏むことが重要なので、現状としては、10から20の出動を経験させているところです。

今回、捜査機関向けの資格制度を整備されたいとのことですが、こうした進め方は必要な人材像が明確になりますので、強く推奨したいと思います。

○（前田委員長）　１点だけ御意見を伺っておきたいところがあります。今回集まった中で温度差があるのは、人材育成は火急の問題で、すぐに作らなければいけない、10 年なんて経っていたらもう時間遅れになってしまうみたいな御指摘あります。IT の人材養成という意味では、大学とか、小中高からの積み上げなのでしょうが、教育とのつながりと、即応体制の整備とのバランスをどうとっていくかということが問題だと思います。その過程で、一部、人材交流を行うのはいいことだと思います。先ほどの小屋委員の話もある意味でつながってくると思うのですが、警察が人を採ることで、キャリアパスが作られ、また、人事交流などを通じて優秀な人材がこの業界に流れ込んでくることにつながるというのは、非常に大事なことだと思いました。他方で、警察として、すぐ問題を解決するだけでいいのかという気はします。将来的な日本のサイバーセキュリティの問題を考えていく人材養成として、「民ではそれほど儲からないことにお金を使えない面があるけれども、警察として要請を請けて引っ張っていく」というところは、中核捜査員の育成とも絡めて、警察庁としてはいかがお考えでしょうか。

○（事務局）　これについては、当面の目標としては、2020 年の東京オリンピックをとりあえず挙げさせていただいておりますけれど、あくまでこれは当面の目標でございまして、ある程度長期的な視野は、警察としても持っております。

このテーマを取り上げた趣旨の１つに、昨年政府において人材育成プログラムを策定し、その中で、我が国全体のセキュリティ人材の底上げを図っていく上で、政府機関が率先して人材育成に取り組んでいく必要がある、そういうくだりがございます。　政府機関と申しましても、先ほど小屋委員のほうからお話がございましたけれど、かなりの人数を育成するようなところは、警察と防衛、自衛隊だと思うのです。そういう意味では、私ども警察、もち

ろんサイバー犯罪対処のための人材育成という部分もあるのですが、この際もう少し広い視野で、警察側の人材育成に率先して取り組むことによって我が国全体のセキュリティ人材の底上げにつながるような、ある意味で呼び水となるような取組ができないかと、そういう問題意識を持っております。そういう意味では官民人事交流についても、その中の１つの手法だというふうに考えております。従来の民間からの登用につきましては、警察で一旦中途採用した後は基本的にずっと組織の中で抱え込むということでありましたけれども、今後は、ある程度官と民間の流動的な人事政策もあり得るのではないかと考えております。そういう意味では、今回、皆様からの御意見を頂戴して、長期的なスパン、あるいは、警察のみならず我が国全体を視野に入れた報告書がまとめられればという思いを持っております。

○（前田委員長）　警察からの資料では、「民のメリット」のところが、「委員の御意見」でブランクになっております。この会で最終報告としては、官もメリットがある、民もメリットがある、その展望が報告書の中で示されていくということが、重要なのだと思います。そこのところは、表面上ではなくて、本当に民の側で「こういうことを希望する」あるいは、「こういうところがあれば、直ちに実現するものではないけれども、こういう展望がありますよ」というものが報告書で書き込めれば、力になってくると感じました。

○（林委員）　前回発表させていただいて、あまり明確には言わなかったのですが、「見える化」をしましょうということを述べていたところ、その趣旨を汲んでいただいて今回の事務局の資料が出来ているようなので、大変ありがたく御礼申し上げたいと思います。

その上で、まだいろいろ欠けているところがあるなどの御指摘もありましたけれど、私の感覚からすると、このレベルのものが一応できれば、これを何回も何回も議論していくと、あっという間により良いものができるのではないかと思っておりますので、是非そのようなことを続けていただきたいと思います。

それからもう１つは、大学は何をするのかということです。あまり偉そうなこと言えないのですが、何らかの御参考になるかと思いますので、私の経験を述べたいと思います。私は、「セキュア法制と情報倫理」という科目を教えているのですが、この科目では、最初からケースメソッドでずっとやってきているのです。2004 年から始めて、これはやはり本にしておこうと思って、2008 年に本にして、引き続きまだ使っているのです。ですから、本の中のケースのかなりがアウトオブデートになっていて、今どうやっているかというと、むしろ院生にどんどん、似たような新しいケースを出させて、それで教室で議論しているというのが実態でございます。来年は、「君たちにこの本を書き直してもらいたい」ということで、むしろ割り振ってしまっ

て、「新しいケースを入れて書き直せ」というふうにやろうかなと思っています。この過程で何が分かったかというと、こんなに変化している世の中においても、そうそうは変わらない部分があるのだということです。テーマが法律と倫理ですから、かなり普遍的なものがあるというのも事実であり、情報技術の本だとそんなに長くは使えないかもしれないですし、このテーマにしても、やはり過去のものをそのまま使えるわけではなくて書き直していく必要は出てくるわけですが。

○（前田委員長）　ですから、学と現場の交流の絶好な場だと思うのですね。他方で、全国の大学のカリキュラムを変えて云々というようなことをやったら、止まってしまうのであって、現に佐々木先生のところと、林先生のところと、あといくつか現実に警察と動いているところが、少しずつ前に動き出していくという形が現実的なのだと思います。また、その意味では、資格制度も、今日御発表いただき非常に勉強になったわけですが、警察がきちっと基準を示すということがもちろん大事なのですが、やはり現に動いている民の資格要件の重み、経験値を踏まえて、統一的な基準を作っていかなくてはいけないと思うのです。警察として資格要件をどう示すかというところで具体的なものがすぐ出てくる必要はないかもしれないけれども、そこはある程度具体化したものを示さないと、民の側としてどういう形で参加するのか、例えばそれを目指して、試験科目がどうなるかとか、司法試験はどうなるかとかといった問題も出てくると思うのです。その意味で、もちろん現実のニーズに合った資格要件でなければ駄目なのと、もう１つ大事なのは、現実にやってこられたもの、あるいは国際的にも動いているようなものを踏まえたものを、日本流というか、現実に即して、これでどうか、というものにできればよいと思います。そして、その中では、この資格要件というのは非常に大事なポイントになってくる感じはあります。

　今回の報告書の中でどこまでそれが書き込めるかという点からは、かなり難しいと思うのですが、これは１年で決着をつけるというような話ではないので、林先生がおっしゃったように、それをたたき台に何回か議論しながら、「こういう方向で進みましょう」という報告書がまとまれば良いと思います。

（石井委員）　前田委員の最後のお話というのは、先ほどの藤川委員から御紹介いただいたものと、かなり実態に近いのではないかと思っております。実際に事案に対して、中核捜査員が、包括的な対処という観点から、どういう人達をアサインメントしていくのかというところと、個別の分析は多分個別の方々がやるフォーミングになるのと、恐らく１人では判断されないので、その中のコミティをいかに作るかという２つのテーマがあります。

　ただ実際的に、実効的に対応できる部隊をどう作るのかという話と、アカデミズムの観点からどういう資格要件や認定制度を設けるのかというのは、

例えば学生さんのモチベーションを作るのかというところと、若干ギャップがあってもいいのかなと思います。そのギャップが段々埋まるようになってくれば、理想的だと思うのですが。即時性が求められるのは、藤川委員から御紹介いただいたような体制をいかに官の中で育てていただけるかというところだと思います。

○（寺田委員）　私も含めて、民間では、学術系の先生方と一緒にやっている部分があります。これは、企業の中だけで、教育だとか、人材育成もしくは発掘をやっていても間に合わないので、学術の世代から取り組もうというもので、具体的には、2008 年にマルウェア対策研究人材育成ワークショップという形で、JPCERT/CC、テレコム・アイザック、IPA に協力いただいて開始しました。当初はそんなに人数は集まっていなかったのですけれども、今では、かなりの人数が集まっています。ある分野の研究に人が集まると、そこにまた人が集まるという相乗効果があります。最近は、データベースなど分野の異なる研究者らが、興味を持ってくれるということで、すごくいい広がりになってきたかなと思っています。

先ほど、捜査についてどのように進められているのかということを教えていただきたいと申し上げたのは、捜査をする上で技術的に、こういう課題があるだとか、こういう事例があるというようなことを見せていくことで、皆さんが興味を持って寄ってくるところがあり、相乗効果につながるからです。それからもう１つ、CTF との違いというところで、与えられた問題を解くという技術は当然必要なのですが、問題そのものを見つける技術や能力を、学術の段階からしっかり身につけていただくことで、会社に入ってから、いろんな形で貢献してもらえるのではないかと思っています。マルウェア対策研究人材育成ワークショップでは、問題そのものを見つける技術や能力に留意してきましたし、今後問題そのものを見つける技術や能力を伸ばす部分について新たな取組ができれば、今回のテーマの中核には直接は関わらないのですけれども、良いのではないかと思い、発言をさせていただきました。

○（佐々木委員）　今、寺田委員から学術の人口を増やしていくという話がありましたが、サイバーセキュリティの中でもネットワークセキュリティ技術系は、寺田委員などに頑張っていただいて、シンポジウムができたりして随分人口が増えました。ところが、実を言うと、デジタルフォレンジックは全然人口は増えていないのです。未だに片手から両手で数えられるくらいの人口に過ぎないということで、今、非常に心配しています。そういう意味で、PR を兼ねて言わせていただくと、３月 19 日の情報処理学会の中で、デジタルフォレンジックが求める情報処理人材というパネルをやって、警察の方にも出てもらって、単なるセキュリティだけではなくて、音声認識だとか、あるいは人口知能だとか、そういう部分も必要になってくるという話をする

予定です。
そういう人達に是非出ていただこうという形で、動いていますので、もし都合がつけば出ていただければと思います。以上です。

○（前田委員長）　先ほどの御発言の中で、これだけクラウド化が進んだり、コンピュータの容量ですぐ消えてしまうものが出てきたりする中で、中核捜査員制度というのがどれだけ機能するかという御指摘、関口委員からあったこと、重いと思うのですが、これについては、理科系の方にお願いするしかないのですが、やはり我々は、そこの点については、大学と技術系の方に乗り越えていただけると確信しております。ネット社会はとても警察だけでは駄目なのだということで、ホットラインセンターというものも、民の協力で情報を集めてやろうということで、今でももちろん機能しているわけですが、そういうやり方もありますし、片一方で、どんなに容量が大きくなったハードディスクでも何とかしてくださる能力を日本の技術者は持っていると、そこを踏まえてタッグを組んで動かすための官民協力であって、今まで 10 年以上この会議をやってきて、初めの頃と雰囲気が全然違うのです。信頼感ができてきていますし。例えば JC3 でオンザジョブトレーニングをやると言ったら、「あんな会社のやつらに来てもらって大丈夫なのか」みたいな感覚が昔であればあるかもしれません。だけど、そんなことを言って日本のサイバーをどうやって守るのかという意識が、段々醸成されていって、もちろん様々な問題はあるのですが、やはり今回のテーマについても、これでまた半歩でも前に進めて、中核捜査員という概念を中心に、民との連携をもっと深めていっていただきたいと思います。警察大学校にも今日は来ていただいていますけれど、研修所ができ、いろいろな技術も進んでおりますので。

８．閉会