安全に資する科学技術推進プロジェクトチーム第３回会合
議事要旨

１．日時：平成１７年２月４日（金）10:00～12:00
２．場所：合同庁舎４号館　２Ｆ　共用第３特別会議室
３．出席者：

（構成員）

薬師寺泰蔵（座長）	総合科学技術会議議員
阿部博之	総合科学技術会議議員
岸本忠三	総合科学技術会議議員
柘植綾夫	総合科学技術会議議員
黒田玲子	総合科学技術会議議員

（招聘専門家）

大野浩之	内閣官房情報セキュリティ対策推進室 緊急対応支援チーム　総括・指導担当
小野正博	警察庁科学警察研究所　副所長
古城佳子	東京大学大学院総合文化研究科　教授
志方俊之	帝京大学法学部　教授
田中明彦	東京大学東洋文化研究所長
樋渡由美	上智大学外国語学部　教授
村山裕三	同志社大学大学院ビジネス研究科　教授
山里洋介	元陸上自衛隊化学学校長

以上敬称略、五十音順

（説明者）

野上久國	警察庁　長官官房技術審議官
佐々木達郎	防衛庁　防衛参事官

他、事務局

４．議事概要

（１）警察庁における安全に資する科学技術の推進について

・　資料３－２について警察庁　野上長官官房技術審議官より説明。
・　意見交換

薬師寺座長　前に勉強会で警察庁の現場の方から、今の犯罪は少年、外国人犯罪が増えていると聞いているが、その様な犯罪の環境変化に対し、科学技術としては、凶悪な犯罪の件数を下げるというような方向で研究を進めているのか、あるいは、着々と全方位的に研究しているのか。

野上技術審議官　その時々において、重点を絞った形で、資源を投入する様な研究開発を行っているところが多い。

○　伺った感じでは、テロ対策ならテロに使われる危険物への対処であるとか、サイバーテロ対策なら、こちら側の情報の中で脆弱な部分への対処といったものに重点を置いているように見えるが、そもそもテロを起こそうとする側についての情報をどうやって取ってくるかということに関する科学技術的な対策についてどのように考えているか。また、合法的な盗聴のための技術というものがあるならどのようなものか。更に、インターネットの様な誰でも見ることのできる膨大な情報の中から、日本、あるいはテロのターゲットとなり得るものに対する敵意が、どこに集中しているかといった様なことは、科学技術により相当程度、分析可能であると考えるがどうか。

野上技術審議官　犯罪捜査上、他国では認められているようなことも、日本では法制度上認められていないことが多くある。

○　科学技術に関するものではAPISというシステムを昨年までに作り上げた。航空会社から搭乗客の情報を受け取り、警察庁、財務省、入管等がそれぞれのファイルをあたるというシステムであり、既に実行に移し、効果をあげている。これは国内の指名手配者のみならず国際テロについてもターゲットにしている。盗聴については、誘拐事件等の場合に対応しての科学技術というものは当然行っている。また、麻

薬・覚せい剤取引に関して、国会に対し報告することを前提に、昨年は、四件（12 人）検挙した。警察は、捜査だけではなく、犯罪の抑止も重要であり、犯罪が起きないための対策、起きた場合の犯罪の制止、そしてその後の捜査という３つの観点で科学技術を如何に活用していくかということが課題である。

○　警視庁、東京消防庁、自衛隊第１師団、保険衛生局、地下鉄会社などが集まって化学テロやバイオテロ等の訓練を行うと、それぞれにおいて二つの違いがある。一つは、観点の違いで、警察は犯人をどう捕まえるか、再発をどう防ぐかという観点から参加し、消防庁は、被害者をどうやって隔離病棟まで搬送するかという観点で参加し、自衛隊はどの地域に危険物質が拡散しているのかという観点で参加し、保健衛生関係は顕微鏡を覗いて一生懸命調べている。このように、同じ事象に対してもそれぞれ温度差があり、酷い場合では被害想定まで違う。もう一つの違いは、それぞれの組織のディテクターが、カナダ製、ドイツ製、アメリカ製などと違っており、情報交換もできていない。先般、産学官の共同ということが出てきたが、警察、消防、防衛、医局がちゃんと連携しているようなフォーラムがあるのか。これをやっていれば能力がアップするのだろう。現場は横の連携が取れていないので、おそらく、研究、開発、オペレーションの段階すべてにおいてそうなのではないか。例えばオペレーションの段階で言うならば、地下鉄で化学テロのようなものが起こった場合の危険物質の処理の考え方一つでも、本当にどうすべきなのかは、現実にはよくわからない。バイオテロ、化学テロ対策については横並びで整合しないと研究そのものが前に進まない。

○　産学官の連携は、だいぶ進んでいる。むしろ問題は、省庁の縦割りというものがやはりあると感じる。今日は警察庁、防衛庁から話を聞いたが、本当は内閣官房（安危室）など、まとめて調整する機関の考え方などを聞いて検討するのが望ましい。

（２）防衛庁における安全に資する科学技術の推進について

・　資料３－３について防衛庁　佐々木防衛参事官より説明。
・　意見交換

○　民生技術を防衛技術に使うというのは、非常に大きな課題。デュアルユースは重要であるが、未だ個人レベルの印象が強い。組織レベルで推進するためには、どのような障害を克服しなければならないと考えているか。

佐々木防衛参事官　一点目は、国防の研究開発を特別視している人がまだいるということ。ただし、何年か前からは、急激に変わってきている感じはする。二点目は、大学の先生方と仕事をする上で、謝金や寄付ということはあるが、必ずしもレートや賃金体系がはっきりしておらず、外部との対応部署を持っている大学は別として、個人の研究室にお願いするのは難しい状況。また、近年、独立行政法人にも積極的に対応していただいているが、防衛庁の場合、防衛関係費の中で装備品の研究開発ということが前提のため、経費的な制約もあって、なかなか、基礎研究に関する仕事をお願いするということがテーマによっては非常に難しい。ただし、防衛ユーザーの考え方、将来の装備品のあり方といった観点からの独立行政法人との連携は始めつつあり、今後、実績が出るにつれ、更に進んでいけると思っている。

○　防衛庁の中の連携について、米軍にはレッドチームといわれるような、テロリストがアメリカ社会のどのような弱点を、どのように衝いて被害を与えられるかということを常に考えるチームがある。それに応じて、科学技術の発展やテロ防止のために必要な技術がわかる。この PT における話を通じて、科学技術がスタティックなものに思えて仕方がない。それは、悪意のある人間や国家を相手にするものであるため、向こうはこちらの持っている科学水準を乗り越えて、新しいことをやってくるということが絶対にあるはず。そうなると、自衛隊など現場の方たちが、どのような技術を必要としているのかということを考える、あるいはテロリストだったらこう考えるだろうということを考える部署と、そういった技術を開発している人たちとの、防衛庁内の連携というものはどの程度なのか。

佐々木防衛参事官　確かに米軍では、レッドチーム等を設けて、研究・検討を行っている。防衛庁の研究開発は、これまではどちらかといえば現在ある装備品の更新がメインであったが、今日の世界の情勢を鑑みると、在来のウェポンの能力を向上させることに加え、非対称脅威に対する装備品の必要性が出てきている。我々としても、研究開発が

ユーザー側とかけ離れては意味が無いので、例えば技術陣が考え、ある段階まで試作したものを、実際にユーザー（部隊）で使ってもらい、意見を闘わせるといったことは行いたいと考えている。

○　省庁間の縦割りに関して、先ほど警察庁がテロ対策をして、BC テロ対策を行っているとあったが、防衛庁でも同じようなことをやられているが、両者のすり合わせの必要についてどの様に考えているか。

佐々木防衛参事官　現在、横の連携については、いろいろな場での意見交換は行っているものの、技術的な中身までは踏み込んでいない。ただ、一方では、警察庁、防衛庁、あるいは他のところのバイオに対する使い方の観点の違いはある。情報交換あるいは技術的な交流というのはしておかなければならないと思っており、事務レベルでの情報交換は行っている。

○　大学も独立行政法人も変わってきているが、脅威の想定は苦手。例えば優れた研究をする人はいても、彼らは、それらの研究成果が実際に使用される場面における脅威に対しての柔軟性などにはあまり興味が無い。また、防衛庁や警察庁というところは、自分たちの活動とは違う世界の人達だという意識が強く、接触が無いばかりに脅威に対して非常にずれた議論をしている。交流や議論を通して、ナチュラルな形で脅威のことを考えられるようにする必要がある。印象的なこととして、大規模なサイバーテロが日本で起こったときにどうするかということを雑談レベルで行ったとき、大学関係の研究者等は直ぐに侵入検知システムを配備するなどの話をするが、防衛庁の方は長期戦になるから、まず、食料と水と寝袋を用意してから、対処するということをナチュラルに言うので研究者はたいへん驚く。また、縦割りの関係で、インターネットの世界でも、縦割りで行われているところを、横串できる道具は少なく、スペシャルな道具はできても、汎用的な技術は意外と少ない。要するに緊急対応のためのメカニズムを汎用化する必要があるということである。

○　米国サンディア研究所のようなものを作る必要があるのかもしれない。国が研究したものを民間にも使ってもらう、あるいは、民間の成果でも国が使うのは構わないが、別のメーカーに成果が行かない様にするといった仕切りを、国が実施すべき。

（３）安全に資する科学技術の意義・目標・方針等について

・　資料３－４－１、３－４－２について事務局より説明。
・　意見交換

○　自然災害など予防することが不可能なものもあるが、危機の中には予防できるものもあり、起きた後どうするかといった危機管理も非常に大切だが、科学技術を使ってある種のものが起きないようにするにはどうすればいいか、という観点も入れるべき。SOFT POWER、HARD POWER の記述において、「SOFT POWER として位置づけられるものである。」とあるが「SOFT POWER として　も　位置づけられるものである。」とすべき。目標達成のための手段においては、抑止、初動対処、事後対応としているが、抑止の前に情報収集や分析というものがあると思う。更に、基幹技術の精選にいくつか例が挙がっているが、シミュレーション検証技術のところで、ある種のシステム技術、様々なものを組み合わせることで、どうすれば危機が起きた際に最も効率的に対応できるかといった研究も重要である。

○　国の安全、社会・経済の安全、個人の安全とあるが、危機管理法においてもそうであるように、今は、国、自治体（県)、市町村、個人のレベルに分かれている。この文章に自治体の文言が無いので、どこかにその視点が必要。もう一つ、防衛、防災、防犯の３つは、個人のレベルでは同じであるという視点も重要。これからの世の中は、自衛隊だけが防衛を、警察だけが防犯をという時代ではない。事が起きれば、全ての組織が個人の命を守り、国家の機能を守るんだという考え方が必要。

○　本プロジェクトチームにおける招聘専門家の多くは、需要サイドの方々であり、サプライサイドが抜け落ちている感がある。安全に資する技術を研究開発し、最終的には現場にデリバーする必要があり、そのためには様々なサプライサイドをどの様に組み合わせて、現場まで流れる仕組みを作るかということが重要。そのためのサプライサイドは三者ある。まず、既存サイド（防衛産業、宇宙産業、通信産業、医薬品産業、防犯産業）をいかに活性化させるか。次に、普通の民間産業であるが、安全に資する技術に転用させることが出来る技術をもつ

企業で、彼らの目を如何に「安全分野」に向けさせるか。３つ目が基礎研究、応用研究が主体の国研、独法、大学であるが、これらの機関も「安全分野」に目を向けさせる必要がある。そして、これらの三つのグループを活用して、いかに結果重視で、問題解決型の技術開発を実施させるかということが非常に大きなポイントではないか。

柘植議員　専門家の本質的な意見に対してかなり接近していながら、まだ周辺のところに対する目標・方針の記述のレベルにとどまっているもどかしさを感じる。具体的には、横串の議論、サンディア研究所の様な機能の必要性、デマンドとサプライ、交流等、各省庁だけに任せられない、司令塔たる内閣府等がイニシアチブを持たなければといった点について、もう一歩踏み込んでもらいたい。

阿部議員　例えばテロ対策に関して、現在日本が国際水準を超えたような対応に向かっているのかどうかといった点が良くわからない。情報収集を含め、国際水準を超えることを目標に、超えてないところはどこか、あるいは得意な分野はどこかといったことを把握していなければ、それぞれの組織では重要というだけになってしまい、それだけでは国としては弱いのではないか。まず、科学技術という面で、標準化の問題は別として、国際水準に比してどの程度のレベルなのかといったことをどこが把握するか。これらには、セキュリティ上オープンに出来るものと出来ないものが当然ある訳で、その点も含め科学技術の上でどう判断していくか。また、法律上の壁の問題、外国では出来るが、日本では出来ないといった点、国際水準から見て見直すべき点があるならどう判断し、提言していくかということ。市民レベルで言えば、危機感、共通理解といった点をどう考えるべきか。以上述べたことを活かす為に、国全体としての取り組みを、問題提起にとどまるかもしれないが、もう少し踏み込んで書けないだろうか。

黒田議員　安全・安心は、第３期科学技術基本計画のキーワードになるものであり、もう少し具体的に踏み込んで欲しい。産官学連携は進んではいるが、省の縦割りというのがクローズアップされてきている感じがする。この点をどう詰めていくかが、今後の課題である。

了