ＩＴ利活用セキュリティ総合戦略推進部会
第１回会合　議事要旨

１　日時

平成 26 年２月 24 日（月）　13：00～14：00

２　場所

中央合同庁舎４号館２階共用第３特別会議室

３　出席者（敬称略）

	菅　　義偉	内閣官房長官
（主催）	山本　一太	情報通信技術（ＩＴ）政策担当大臣
（座長）	徳田　英幸	慶応義塾大学教授、内閣官房情報セキュリティ補佐官
（委員）	淺野 正一郎	国立情報学研究所名誉教授
	有村　浩一	（一社）JPCERT コーディネーションセンター常務理事
	鵜飼　祐司	（株）FFRI 代表取締役社長
	後藤　厚宏	情報セキュリティ大学院大学教授
	齋藤 ｳｨﾘｱﾑ 浩幸	（株）インテカー代表取締役社長、内閣府参与
	下村　正洋	NPO 法人日本ネットワークセキュリティ協会　事務局長
	中尾　康二	KDDI（株）情報セキュリティフェロー、 （独）情報通信研究機構　主管研究員、研究統括
	名和　利男	（株）サイバーディフェンス研究所　上席分析官
	前田　雅英	首都大学東京法科大学院教授
	松原 実穂子	（株）日立システムズ
	安田　　浩	東京電機大学教授

（その他出席者）

遠藤　紘一	内閣情報通信政策監
髙見澤 將林	内閣官房副長官補
向井　治紀	内閣審議官
谷脇　康彦	内閣審議官
藤山　雄治	内閣審議官
三角　育生	内閣参事官
二宮　清治	内閣参事官

警察庁
総務省
外務省
経済産業省
防衛省

４　議事概要

(1)　内閣官房長官冒頭挨拶

2020 年のオリンピック・パラリンピックについては、我が国への招致が決定された。

６年後に「その時」が来るわけであるが、その頃には同時に画期的なＩＴサービスの登場が期待される。その反面、これまで以上のリスクが懸念されるところであり、その対処には今からありとあらゆるリスクを予見し、官民の総力を結集して取り組んでいくということが極めて大事である。

そこで、今般、ＩＴ政策担当大臣であり、また、情報セキュリティ政策会議の議長代理でもある山本大臣のもとに、本会議を立ち上げ、我が国が目指す「世界最高水準のＩＴ社会」が、安全で安心なものになるように、御議論を賜りたい。

皆様におかれては、山本大臣のもとに結集いただき、活発な御議論を通じて、成果を取りまとめていただくようお願いを申し上げる。

(2)　情報通信技術（ＩＴ）政策担当大臣冒頭挨拶

主催者であるＩＴ政策担当大臣として、本部会の発足目的を述べる。

昨年の６月の「世界最先端ＩＴ国家創造宣言」を決定するにあたり、「サイバーセキュリティなくしてＩＴ戦略なし」を痛感した。

現在、サイバーセキュリティの問題は、政府の情報セキュリティ政策会議が一元的に取り扱っており、その長は内閣官房長官である。その事務方としてはＮＩＳＣが機能しており、関連部会も活発に開催されている。

しかし、残念ながら情報セキュリティ政策会議で議論する時間は限られており、さらに議長である内閣官房長官は多忙を極める。ここは、議長代理であるＩＴ政策担当大臣が役割を果たし、議論する場を設ける必要があると考えた。そこで、ＩＴセキュリティに関してグローバルな視点からの御意見をいただける方々にお集まりいただき、各部会における議論を総合的見地から検討することとしたものである。

本部会で皆さんに御議論いただいた内容は、責任を持って、サイバーセキュリティ政策に反映をさせてまいりたい。関係各省庁においても、全面的に御協力をいただきたい。

本日は最初の会合ということで、お集まりをいただいた皆さんから、テーマも含めて自由な意見を言っていただき、ブレインストーミングを行いたいと思う。また、６年後の2020年オリンピック・パラリンピック東京大会に向けてどういう対応をするのかについても、大きなテーマの一つになると考えている。

(3)　討議

・　情報セキュリティ政策会議の各専門委員会等の取組状況について
・　今後のＩＴ利活用を見据えたセキュリティ対策に関する論点について

上記について、事務局より資料に基づき説明が行われるとともに、構成員より意見が述べられた。

○　人材育成について、１点述べる。

資料２に、「コンピュータサイエンスを身につけた人材の育成を強化する必要がある」とあるが、我が国の国内には、海外と比べコンピュータサイエンスを教えることができる教員、コース、又は学科が圧倒的に不足している点について、解決する必要があると考える。

また、サイバーセキュリティは、あくまで安全保障の一部であり、攻撃者側は人間の過信や心理的な盲点等を突いた攻撃を行う。そのため、技術的なコンピュータサイエンスにとどまらず、例えば、地政学、安全保障、政策、犯罪心理学、法律学等の観点から多角的に分析し、情報セキュリティインシデントが経営や国にどのような影響を及ぼすのかについて分かりやすく説明できるよう、技術的な人材と経営層あるいは意思決定者との間で橋渡しをできる通訳的人材も育成する必要もあると考えている。

○　研究開発戦略の見直しにおいて、サイバーセキュリティの脅威が社会や組織に与える影響を認識できるための社会科学の研究とも連携していく方向性が示されたことは、大変よいことである。

さて、各部会で検討を進める上で、昨年までと異なる点として共通するのが 2020 年のオリンピック・パラリンピック東京大会を見据える必要である。そこで、実践的にどのようにセキュリティ対策を進めていくかを考える上で、リスク管理・対策の強化が最も重要であると考える。もちろん、各対象省庁が動く必要があることであり、国がスクラムを組む必要がある。したがって、内閣官房にはスクラムの中心として是非頑張っていただきたい。

○　サイバー攻撃に対し、現場で緊急対処を行う者としての経験から、１点述べる。

幾ら資金を投じても、サイバー攻撃の実態を知らない人々が研究開発や人材育成を行うことには意味がない。やはり、実際に現場を経験をしていることが一番重要である、というのが私の考え方である。

○　研究開発について１点述べる。「脅威に対応した研究開発の推進」は、非常に重要な課題である。研究のデータは、生のデータでないとほとんど意味がない。予め想定される脅威があり、それに対する何らかの仕組みを入れることは当然である。一方、事前には想定できない脅威もあることから、それらを発見するための観測、検知、さらには新たに発見された脅威に対し、動的に対策を講ずるためには、単純な研究にとどまらず、運用や分析をしているメンバーとの連携が必要不可欠である。そのため、今後はこれらの連携を強化する必要があると考えている。

○　人材育成、研究開発及び2020年オリンピック・パラリンピック東京大会を見据えたセキュリティについて述べる。

人材育成に関連し、政府機関において率先して外部人材の登用を行う旨の記載があるが、これは是非進めていただきたい。さらに、できれば十把一絡げに「セキュリティ人材」とくくるのではなく、各々の人材をそれぞれカテゴライズした上で、

「こういうスキルの人が必要である」ときちんと明示して欲しい。さらに、人材の育成にあっては環境が大事であり、例えば外部のシステムに悪影響を与えないよう隔離された環境で、実際にマルウェアやサイバー攻撃のログを体験できる、そういう仮想的な研究用ネットワークを設けていただきたい。また、経営者層の認識を高めるために情報セキュリティの重要性を啓発することが挙げられている。私見であるが、啓発だけではなかなかうまくいかない可能性も高く、経営者としては利益追求と事業継続が一番の目的であることを考えると、可能であれば一定の強制にまで踏み込む必要があると考える。

研究開発については、国際標準化を見据えた戦略が必要である。そうしないと、せっかく良い技術を研究開発したとしても、標準化という切り口で採用を見送られてしまう。一般に、研究開発と標準化作業は車の両輪であり、標準化に関する様々な場が海外にあることから、これらの場に対してきちんとメッセージを出していくことが重要である。

2020年オリンピック・パラリンピック東京大会については、我が国としての体制づくりが課題であり、何かが起こったときの指揮命令系統や各省庁の役割を早く決め、組織を整備しつつ、ＩＴ・ＩＣＴの投資を行い、さらに教育や演習といった人材育成に取り組む必要がある。そのため、一番トップになる人を早期に決定しめ、そこからの命令に基づき活動する体制をつくっていただきたい。

○　人材育成について、情報セキュリティに関する海外の教育事例では、生物学などを参考にしている例もあり、コンピュータサイエンスに限定する必要はないと考える。

また、法制度上の整備も必要と考える。現在、情報セキュリティインシデントが発生したという事実は、仮に公言したとしても、公言した主体にとってメリットはない。しかし、そうした情報セキュリティインシデントが持つ被害が潜在化しやすいという特性を乗り越え、どのように経験を共有していくか、情報の共有のインセンティブを付与するかを考える必要がある。特に、我が国であれば、レジリエンスに資する情報を共有するほうが現実的であろう。

科学技術政策の観点からは、各省庁に横串を刺しつつ、我が国の国内をまず統一した上で、国際標準化を進めることが非常に大事である。また、サイバー関連技術については、一国でゼロから研究開発することは無理なところもいろいろあり、海外からも学ぶところが多いと考える。ＩＴ利活用の充実は、成長戦略も含め、サイバーセキュリティと一体であり、本当に大事な基礎の技術としてぜひ考え、直接我が国の競争力につながるよう、検討していきたい。

○　人材育成について述べる。現在、数少ないエキスパートを各所で取り合ってしまっている状況である。根本的に人材の絶対数を増やす必要があると考えている。

そのためには、継続して育成に取り組まなければならないが、大学を始めとした教育機関、企業、民間、政府機関を見回しても、全体の人材育成の循環を回すエンジンが足りない状況である。

資料にも「需要と供給の好循環」とあるが、そこで、エンジン役を担うことができるのは政府だと考える。政府機関がみずから、２～３年後にこういう人材がこれだけ必要である、旨を明白に宣言し、さらにその人材像を目指そうという学生をサポートする仕組みを作りさらに、政府機関から民間へ、優秀な学生のエキスパートを循環させるような仕組みをつくるべきである。

そうすることでグーグルやフェイスブックといった企業にばかりに行きたがる日本の優秀な若手を、我が国のサイバーセキュリティのための人材としていくよう努められたい。

また、情報セキュリティ人材の育成のためには、学生に対して実践的な教育が必要である。現在、情報セキュリティ大学院大学では実践教育を進め、事案対処の最前線で活躍している方やセキュリティベンダーで最前線の問題を解いている方に実際のログ等を持ち込んでもらい、学生に分析させるという教育をしている。そうすると、学生の目も輝いてくる。したがって、実践的な教育は、サイバーセキュリティの人材を増やす上でも非常に大事であると実感する次第である。

○　サイバーの分野で研究開発を行う企業の立場から述べる。

我が国の民間企業におけるサイバーセキュリティの研究開発能力は、海外と比較して弱い。

サイバーセキュリティの領域の基礎技術に関する研究開発は非常に重要であるが、従来は米国等の海外の主に民間企業の技術に頼り切っており、非常に懸念を持っている。

今回、人材や産業の育成の話題が出てきたが、これまで我が国における特に民間におけるサイバーセキュリティに関する研究開発が低調であった中で、ここから何とかグローバルにも出していけるような研究開発をしていくためには、官民一体となって基礎技術をしっかりやっていく必要がある。そしてその技術を産業に生かした上で、海外に輸出していく力を蓄えていかなければならない。

そこで、グローバルなコミュニティとしっかり連携し、国際連携することが重要なポイントとなる。さらに、サイバー脅威を取り巻く環境は厳しさを増していくことから、何かが起きてからその対策技術を研究開発するという受け身の姿勢ではなく、もっとプロアクティブに、あらかじめ敵をしっかりと研究し、攻撃技術に関する知見を蓄えることで、実際に攻撃を受けるよりも前に対策技術を実用化していけば、サイバーセキュリティの産業分野でグローバルを牽引していくことができる。

○　３点、所感を述べる。

ＩＴセキュリティの戦略を考える上で６年後のオリンピックは中期的な目標として非常に良いテーマである。

第一に、オリンピックが人材育成にもたらす影響について。現在セキュリティの分野では総合調整をすることのできる人材が必要とされている。オリンピック・パラリンピック東京大会はその経験を得るのにぴったりであり、オリンピックのセキュリティ確保に挑むために集め、それをなし遂げた人材が、また各分野に戻って

いけば、それらの人材がコアになり、その後のセキュリティを担っていくであろう。特に、オリンピック・パラリンピックロンドン大会を成功させたサイバーセキュリティの担当者と話をすると、準備が早いにこしたことはないと言っていることからも、今が準備的にはちょうどいいタイミングだと考える。

第二に、産業の育成について。オリンピックに向けて整備した各種の施設等は、開催終了後も使い続けることになる。単純な情報システムに限らず、そうした施設に付随した制御系システム、例えばビルのオートメーション等においてセキュリティを確保し、サイバー攻撃から守ることができれば、開催終了後は格好のショーケースとして機能するであろう。

第三に、国際連携について。オリンピックは、全世界が注目するとともに、全世界が協力してくれるイベントである。丁度ソチオリンピックでも各国のＣＥＲＴがロシアのＣＥＲＴと連携をしたところであるが、若い世代に是非こうしたオリンピックの中での総合調整やグローバル協力を経験させたい。そして、オリンピックの機会を捉え、我が国の産業のあるいは人材の底力を上げていく起爆剤としたいと考えている。

○　「重要インフラの情報セキュリティ対策に係る第３次行動計画」には、経営層、意思決定層に対して期待する在り方が入っており、また、情報セキュリティ対策に係る取組の海外同業他社への展開や海外の動向把握等の国際的な中で自分をどういう位置づけで見るのかという視点についても記載されていることから、これが十分達成できるよう、今後見守っていきたい。

さて、2020 年を目標にすると、それまでの間に様々な画期がある。例えば、次世代のＥＴＣが運行されるのは 2020 年だし、準天頂衛星が本格運用されるのも 2020 年である。したがって、2020 年までの間に各種の新しいシステム基盤として活用できなければならない。

現在、これらの議論は縦割りで行われている。しかし、防御・防衛するという観点からは、新しい技術を総合的に考えながら、もう少し幅広に考えていかなければならない。

例えば、人工衛星による測位システムは、脆弱性を持ちやすい。また、航空機の運航管制システムも 2020 年には新しい管制に切りかわると考えられるが、そのリスクも考えなければならない。こうして考えると、2020 年は、目標として非常に適していると考えている。

少なくとも、重要インフラの情報セキュリティ対策に係る行動計画的に言うと、今から数えてあと２回ぐらい行動計画を見直すことになる。恐らく、同じように新しい技術に関するチャレンジも、２回ほど見直しの時期が来る。このときに、セキュリティ技術と総合化の歩調うまくを合わせることができるかが重要なことである。

○　３点お願いしたい。

第一に、人材育成について。我が国ではなかなか人材が育たない。育つ土壌としては、皆がセキュリティの重要性を理解し、セキュリティを手がける人材に尊敬の

念を抱くような社会が必要である。

そこで、仮に2020年には、我が国の国民全員がＩＣＴを使っているとしよう。すると、今度は、皆が「セキュリティが確保されていないと困る」と言うだろう。その結果として、情報セキュリティ人材の育成も、大いに伸びていくだろう。要するに、ＩＣＴの利活用なくしてサイバーセキュリティは不要である。ＩＴ政策担当大臣には、是非、まずＩＣＴの利活用を伸ばすということをお願いしたい。

第二に、研究開発について。今、我が国で使われているセキュリティソフトは全部外国製という状況である。そのため、その中には、我が国では分からない部分がある。その我々では分からない箇所から攻められると、どんなに頑張っても勝てない。つまり、何が起ころうと、独自のセキュリティソフトを持たない限りは負け戦になる。そのため、2020年のオリンピック・パラリンピック東京大会で発生するサイバー空間上の攻防に本当に勝つためには、独自のソフトをいかに埋め込むか、使うかということが一つの大きな課題である。これから６年しかないから、相当をつぎ込んでセキュリティ技術の開発をおこなわなければ、いいものはできない。そのため、まず、独自ソフトをいかにつくるかということについて、大きく旗を振っていただきたい。

第三に、オリンピック・パラリンピック東京大会で使用するソフトウェアと情報システムの仕様策定について。オリンピックほどの規模であれば、やはり新しいシステムにならざるを得ない。システムを新しく立ち上げ、きちんと稼働するまでには３年かかる。逆算すれば、2020年の３年前にオリンピック用システムの仕様が出ていなければいけない。そのとき、同時に「オリンピックで使うシステムはこういうセキュリティ状態になっていないといけない、こういうことは絶対守れ」ということを是非提示をしていただきたい。本部会がその場になるかもしれないし、ならないかもしれないが、少なくとも３年前の段階でターゲット仕様がなければ、いいシステムにはならない。歯を食いしばって、３年後に想定される新しい技術を見据え、それを仕様化し、皆がそれを利用するという意識を持つようにして欲しい。

○　セキュリティソフトが外国製であることについて、補足したい。犯罪捜査の上で、遠隔操作ウイルスによる脅迫事件等の問題が発生したときに、いろいろなベンダーから力を貸してもらった。その際、最後はやはり本国の本社に聞かないと答えられない、という事態が発生した。インターネットの世界はグローバルであり、インターナショナルである。しかし、我々は国益も守らなければならない。いわゆる経済力をつける意味でも、その研究開発と人材育成を通じて我が国に底力を付けることが一番基本的であると考える。

(4)　情報通信技術（ＩＴ）政策担当大臣締め括り挨拶

本日は本当にありがとうございました。やはり１時間では足りないという気もするし、例えば、グローバルな視点が必要であれば、外国の専門家を呼びたいので、本部会の進め方については、今後工夫をしたい。

本部会では、夏までに提言を行う予定であるが、良い知恵が出てきたら、そのま

ままとめて提言しても構わないと思う。
　また、本日の論点に加え、「こういうことをやるべきだ」ということがあれば、ぜひ有識者の方々から出していただければと思う。
　さらに、「ＩＣＴの利活用なくしてセキュリティなし」は目からうろこであり、2020年に向けて、我が国の国民全員がＩＣＴを使うことについては、ＩＴ政策担当大臣としてまさに使命である。現在、オリンピック担当大臣のところに、各大臣がプロジェクトを持ち込む形になっているから、私も一生懸命やっていきたい。
　それから、セキュリティソフトが全て外国製であるという点について。現在、科学技術イノベーション政策も担当している。そこで、SIP と ImPACT という２つのプロジェクトを作っているので是非 ImPACT にも御提案いただきたい。
　また、オリンピック・パラリンピック東京大会で使用するソフトウェアと情報システムの仕様を早期に策定するべきであるという点について。本当に歯を食いしばってやらなければいけないことであり、ここの会議が中心となり、各省庁の取組の背中を押すことができるような、発信力のある会議にしていきたいと思う。その総合調整については、ＮＩＳＣの強化と同時に、内閣情報通信政策監ももっと協力し、司令塔機能の下、各省庁と連携していきたい。
　サイバーセキュリティは、コンピュータサイエンスに加えて、安全保障の専門家、犯罪心理学の専門家、経営学の専門家等も必要だということであり、防衛省ともよく連携をとっていきたい。さらに、本部会からは、セキュリティ技術に関する研究開発の議論等を通じ、産業競争力強化につながり、成長戦略につながるアイデアを是非提言していきたい。

－　以上　－