戦略的イノベーション創造プログラムに係るガバニングボード（第３２回） 議事要旨

１．日　時　　平成27年８月６日（木）10：00～10：22

２．場　所　　中央合同庁舎８号館　６階623会議室

３．出席者

総合科学技術・イノベーション会議(CSTI)

久間議員（座長）、原山議員、小谷議員、内山田議員、

中西議員、橋本議員、平野議員、大西議員

内閣府　　山口大臣、平副大臣、

森本統括官、松本審議官、中西審議官、中川審議官、

真先参事官、西條参事官、岩松参事官、後藤ＰＤ候補

４．議題

平成２７年度ＳＩＰ新規課題「重要インフラ等におけるサイバーセキュリティの確保」ＰＤ候補（政策参与）の紹介

５．配布資料

資料１　ＳＩＰ新規課題候補『重要インフラ等におけるサイバーセキュリティの確保』のプログラムディレクター候補

資料２　重要インフラ等におけるサイバーセキュリティの確保

６．議事

平成２７年度ＳＩＰ新規課題「重要インフラ等におけるサイバーセキュリティの確保」ＰＤ候補（政策参与）の紹介

○久間議員　皆さんおはようございます。第32回戦略的イノベーション創造プログラムガバニングボードを開催します。

本日の議題は、平成27年度ＳＩＰ新規課題候補「重要インフラ等におけるサイバーセキュリティの確保」ＰＤ候補（政策参与）の紹介１件です。

６月18日の総合科学技術イノベーション会議において、重要インフラ等におけるサイバーセキュリティの確保がＳＩＰの新規課題候補として承認されましたが、その後のＰＤ候

補の公募、選考を経て、本日後藤厚宏さんに政策参与としての辞令が山口大臣から施行されました。

まず私のほうから後藤厚宏ＰＤ候補の経歴の紹介をさせていただきます。後藤厚宏ＰＤ候補は昭和59年、東京大学大学院工学系研究科、情報工学専攻博士課程を修了、同年日本電信電話公社、現在のＮＴＴに入社。約27年間、情報技術に関する研究開発に従事されてきました。その後平成23年に情報セキュリティ大学院大学に転身され、人材育成にも尽力され、衆議院、内閣官房、防衛省、経済産業省、総務省、文部科学省などの審議会、委員会等における委員長等、及び委員を歴任されておられます。

それでは、新規課題候補に対する現在のお考えを披露していただきたいと思います。後藤厚宏ＰＤ候補、よろしくお願いいたします。

○後藤ＰＤ候補　おはようございます。後藤でございます。それでは、これから新規課題候補の重要インフラのサイバーセキュリティへの取組について簡単に御紹介したいと思います。

お手元に資料がおありだと思いますが、こちらのスクリーンを使って御紹介したいと思います。まず背景でございます。これは私が御説明するまでもなく、重要インフラは社会を支える産業でございます。産業規模は国内においても180兆円と、一番大きな産業の一つでございます。同時にインフラシステム自体が現在は輸出産業として非常に期待が高まっております。これは第６回の経協インフラ戦略会議で目標と定められました、2020年には30兆円にしたいと、こういう動きでございます。ところがこの重要インフラ、社会インフラですね、これに対するサイバーセキュリティ攻撃の脅威が現実のものになっております。これは全体の統計でございますが、インターネット犯罪における損失は世界で53兆円と言われておりますし、先日フランスではテレビ局がのっとられるという事件もございました。そういう意味で特に2020年、オリンピック・パラリンピック東京大会を迎える我が国としましては喫緊の課題であると。実際2012年のロンドン大会では２億件の不正アクセス行為があったと伺っています。

一方セキュリティ製品の自給率、残念ながら日本は高くございません。でありながら、現在注目されておりますＩｏＴ、インターネット・オブ・シングス、これは新しい産業として非常に期待されております。この期待を現実のものにするためには、IoTのセキュリティリスクにしっかり対処しなければいけないと考えております。

この絵はあえて描いたものでございますが、重要インフラとして、通信網、電力網、鉄道を事例にしておりますが、全てそれを支えている制御のネットワークがございます。これ

を使って安全運行なり、安定供給をしているわけでございますが、この部分がもしいろいろなサイバー攻撃にさらされますと、我が国の社会インフラは非常に危険なことになります。現在この社会インフラの品質の高さというのは日本の自慢でございますので、是非これを今後ともサイバー攻撃に対しても品質が保てるようにしていくことが一番の課題だと思っております。

そういう意味で大目標・ビジョンでございます。技術的にはこちらにございますように、重要インフラの制御ネットワークを構成する機器装置、いろいろな機器装置がございますが、それらのセキュリティをしっかりと確保できる技術をつくっていきたい。それによって産業面では、当然ながらセキュリティ製品の国内自給率を上げていくことを考えておりますが、同時にセキュリティ技術を梃子にして、これを付加価値にしてインフラ産業やシステム産業全体の競争力強化につなげたいということでございます。

次の図をご覧ください。まず、サイバーセキュリティの確保という意味でいいますと、ほぼ確実に今回の五輪は狙われると思います。ただし、ここでしっかりセキュリティが確保できればそれは実績になるということでございます。そういう意味でインフラ産業を守るという意味と、これをきっかけに規模拡大につなげたい。ちょっと下手くそな絵でございますが、梃子の原理で、セキュリティ産業自体は小さいかもしれませんが、それが付加価値となってこの大きなインフラ産業の雪だるまをぐるぐるっと大きくしていきたいと。それによって将来グローバルなところでもどんどん30兆円の目標がございますが、こういうところに貢献できればというのが大きな狙いでございます。そういう意味で、社会的な目標としましては世界で最も安全な社会基盤をつくって、それの実績を2020年のオリンピック・パラリンピック東京大会で示していくということを考えております。

では、どのような取組をするのかということでございます。セキュリティに関しましてはたくさんのコア技術が必要になります。この中でもちろん、既にいろいろなところで取り組まれている技術もございます。こういうものを活用することは当然でございますが、重要インフラにおきましては、先ほど申しましたように制御機器のセキュリティを確認するような技術とか、バックドア、裏口ですね、これはアタッカーが使う裏口をしっかり見つけ出す技術。それから将来のＩｏＴに向けて低コスト化すると、こういうコア技術をつくる、これを目指したいと考えております。同時に、今回2020年のオリンピックまでに実際この技術を使いこなせるようにしなきゃいけないということを考えますと、社会実装のための準備をしっかりしたい。そのためには、例えば技術の認証制度であるとか、人材育成、

さらにはいろいろなインフラで使いこなせるためのプラットフォーム、できましたらインフラ間、分野間で共有化できるようなプラットフォームをつくっていきたいというのが今回の目標でございます。

今の繰り返しになりますが、研究開発目標としましてはシステムの起動時に加え、運用時も機器のセキュリティを守れる技術、それからバックドアの解析技術、ＩｏＴシステムに向けたセキュリティ機能の低コスト化、これをコア技術としてつくりますが、同時に社会実装に向けた公共性の高い認証制度づくり、分野間連携と運用コスト低廉化のための共通プラットフォーム、それから人材育成、こういうことについてもしっかり準備していきたいということでございます。

この次の図はちょっと技術の詳細に入りますが、今回のポイントでございます。実は機器をつくる段階から準備をしまして、そこで「信頼の起点」というのが実はキーワードでございますが、こういう技術を組み込むことによって、運用時、機器ベンダーから調達した機器がインフラ事業者の間で使われるときに正しく動作していること、改ざんされていないこと、こういうことがしっかり見つけ出せるような技術をつくっていくというところが特徴でございます。

出口としましては、これも今申し上げたとおりでございます。2020年のオリンピック大会で実際実績をつくりたい。そのために是非、政府系システムに先行導入、及びオリンピックの開催時に必要な設備、そういうところを中心に先行して入れていきたいと考えています。それをこのような強靭なセキュリティ機能を日本全体の重要インフラへ順次展開していくことと同時に、グローバル貢献、海外への展開の準備を進めていきたい。そのための国際標準化活動であり、認証制度自体の国際化、我が国の認証制度みたいなものが世界でも使えますよという、そういう形で持っていきたいと思っております。

まとめでございます。このたび重要インフラのサイバーセキュリティ脅威への耐性を根本から高めるために、このＳＩＰを活用しまして、基盤技術の研究開発から社会実装、グローバル貢献にまでオールジャパン体制で迅速かつ大胆に取り組みたいという気持ちでございます。是非御指導よろしくお願いいたします。

○久間議員　どうもありがとうございました。

それではただいま後藤ＰＤ候補からご発表いただきましたけれども、まず山口大臣からコメントいただきます。

お願いします。

○山口大臣　今お話をいただきましたが、これはＳＩＰの11個目の課題でありますが、ある意味で非常にタイムリーというか、大事なテーマに取り組むことができるなというような感じを持っております。担当大臣としてマイナンバー、個人情報保護法が停滞をしており、是非ともそこら辺も含めてしっかりしたものを出していただければ。ＳＩＰ自体がやはり出口を見ながらということもあるのですが、東京オリパラ、これはもう目の前に来ていまして、是非ともそこら辺を踏まえてしっかりと取り組んでいただければ。お話のようにやっぱりオールジャパンで、いろいろ個別の暗号化など、いろんな研究をもうやっておられますので、そこら辺をＰＤのほうでしっかり把握をしながら、取り入れながらやっていただいて、結果としてある意味で国際的にもという格好でやっていただければと思いますので、よろしくお願いいたします。

○後藤ＰＤ候補　ありがとうございます。

○久間議員　どうもありがとうございました。

それでは平副大臣からお願いします。

○平副大臣　プレゼンありがとうございました。副大臣の平です。

実は私、２年前に経済産業省の大臣政務官をやっていたときに、標的型ウイルスメールにやられまして、ほぼ今の年金機構と同じ仕組みで非常に巧妙にできていて、実在する朝日新聞の記者の名前を名乗って、私にアベノミクスにおける中小企業の話を聞きたいということで、添付ファイルを開きましたら感染をしまして、ＮＩＳＣに分析をしてもらったらそれはそのパソコンをのっとるソフトで、すぐにちょっと違和感を感じたので、実害はなかったんですが、私のパソコンは初期化し、議員会館のパソコンは取り替えました。これを官邸と共有してＮＩＳＣに実際にのっとられた実演をしてもらいました。結局政務三役のパソコンが一番脆弱なわけですね。ということで、これは困ったなと。一番強い人はパソコンも何も使っていない人ということになって、そういうことがありました。

あともう一つの事例は、選挙でインターネットの選挙運動を解禁して、これは情報発信において極めて有効なツールだということで私もやったんですが、一方でディフェンスに物すごいお金がかかるというのを実際に体験しました。経産省のほうでもＩＴ導入による生産性の向上とか様々なことがあるんですが、一方でこのディフェンスをどうしていくのか。本当にそっちはバランスがいいのか。実は「攻殻機動隊」というアニメがあって、これは近未来社会の中でハッキングとかウイルスがどういうリスクがあるかというイマジネーシ

ョンを湧かせるには非常にいい素材なので、一応経産省と内閣府の関係者には極力見るようにというふうに今言っているんですが、正に時宜を得た取組だというふうに思っています。どうやって、しっかりと制御しつつ、あと野放図にお金もかけられませんので、経済合理性も追求していかなければいけないと思いますし、また国家の威信が、東京オリンピック・パラリンピックかかっておりますので、ここでしっかりとしたディフェンスをして成果を上げて、正にＡＳＥＡＮや世界に今後打って出るということだと思いますので、期待をしておりますので是非頑張ってください。

○後藤ＰＤ候補　ありがとうございます。

○久間議員　ありがとうございました。

それでは議員の皆様から一言ずつよろしくお願いします。大西議員、どうぞ。

○大西議員　ありがとうございます。よろしくお願いします。

さっき大臣から統合化という話ありましたけれども、私が想像するにこの分野はベースのソフトというかシステムをアメリカ、マイクロソフトだとかアップルが持っているわけですよね。だから日本の中で完結しない技術という面もあると思うんですが、そういう国際連携といいますか、海外の会社との連携とか、そういうことも大事になると思うんですが、そのあたりはどういうふうにお考えなのかちょっと一言。

○後藤ＰＤ候補　おっしゃるとおりでございます。全てを今どこか一部の国でつくるという時代ではございませんので、国際連携は重要になるわけではございますが、ただその中でセキュリティの信頼の基みたいなところ、そこだけはやっぱりしっかり押さえないといけない。それは国内でちゃんと頼れるところで押さえないといけないんじゃないかというのが今回の考え方です。ですからそこをベースにしておいて、あとは本当に国際的に使えるものをどんどん使っていく。一方、これは本当に大丈夫だよねという筋だけは通せるような技術、そこに特化したいということでございます。

○久間議員　平野先生、どうぞ。

○平野議員　素人的な質問なんですけれども、セキュリティは非常に重要、当然そうなんですけれども、人間が考えることですよね、どうしても。そうすると必ず人間が破るということになるのではないかと思うのですが、理論的に究極的に絶対大丈夫なものはできるのですか。

○後藤ＰＤ候補　お説のとおりで、私は究極というか、究極的な技術のみの解決というのはな

いと思っております。だからそこはもう、常に人間の研究も含めて、技術と抱き合わせでつくっていかなきゃいけない。それが今回、社会実装のためにもいろいろセンターをつくるとか情報共有をするとか、そういう仕組みも合わせてつくらなきゃいけないというところにつながっております。

○久間議員　よろしいですか。

では橋本先生、いかがですか。

○橋本議員　特にありません。大変重要な課題ですので、私たちは応援できる限りさせていただきますのでどうぞよろしくお願いいたします。

○久間議員　ありがとうございます。

では中西議員、お願いします。

○中西議員　実は経団連でも昨年の今頃から同じようにサイバーセキュリティ問題というのが課題になるだろう、特にインフラに対するアタックがシリアスだという強烈な問題意識がありました。そこでキャリアさんをはじめ３０社近くに集ってもらい、懇談会を立ち上げて議論しました。そこでわかったことは、業界や企業によって問題意識に温度差があるということでした。経団連として、サイバーセキュリティ対策は、正に緊急でなおかつ継続的な取組みにしていかなければいけない話だと思いますので、是非しっかりご一緒にやらせていただきたいと思います。

○後藤ＰＤ候補　ありがとうございます。

○久間議員　では内山田議員、お願いします。

○内山田議員　後藤さんのプレゼンの中でもご説明がありましたけれども、セキュリティ関連の技術については、個別に技術開発が行われていますが、それらを組合せてシステムとしてどう守るかという検討が十分に進んでいないと思います。システム化については日本が今もって不得意な分野。個別の技術は良いけれども全体がなかなかうまくいかないということで、今回、ＳＩＰ新規課題の「サイバーセキュリティ」が一つの試金石として、好事例になると良いと思って期待しております。サイバーセキュリティは我々企業にとって本当に切実な問題でもありますので、大変期待しております。よろしくお願いします。

○後藤ＰＤ候補　ありがとうございます。

○久間議員　では小谷先生、お願いします。

○小谷議員　ありがとうございます。ウイルス感染といわれることからも分かるように、サイ

バーセキュリティも人間の伝染病と割と近いところあります。まず予防、それから感染させて耐性をつくること、早期に伝播を防ぐかとか、いくつかのフェーズがあります。そのそれぞれに対して十分ケアしていただけることは御専門なので当然かと思っております。

恐らくハード面については日本はやればできますので、そこは心配しておりません。ただやはり理論に関していえば、外国で開発された技術を使っているようでは、絶対に外国からのサイバー攻撃には対応できないので、是非理論面についても十分に取り込んで、日本初のすばらしい技術をつくっていただければと思います。よろしくお願いします。

○久間議員　では原山先生、お願いします。

○原山議員　既に御指摘されているように、正にこれ、エンドレスな戦いなので、ＳＩＰのプログラムのつくり方、それからマネージの仕方、動かし方というのもこれまでの課題のようにやっていては多分対応できないです。ですので、やり方そのものも新しいやり方ということも開発しながらやっていただきたいと思いますし、オリンピック、2020年とターゲットありますけれども、先ほどおっしゃったようにそれが一つの渡るべき橋であって、その先も視野に入れた形でやっていただければと思います。よろしくお願いいたします。

○久間議員　ありがとうございました。それでは私からも一言。

面接させていただいた中で、オリパラに向けた研究開発から実用化に至る構想、強靭なサイバーセキュリティシステムの開発提案、グローバル戦略、標準化戦略、研究開発体制、オペレーター、関連省庁との連携、さらに人材育成に至るまで、ほぼ完璧な提案書だったのです。

ですからこの御提案を骨格に、これからＮＩＳＣや関係省庁、オペレーターから様々なリクエストや提案が出てくると思いますので、それらを融合した具体的な計画書を策定し、スピーディーかつ確実な研究開発を推進し、強靭なサイバーセキュリティシステムの実用化に向けて頑張っていただきたいと思います。

それから、既存の10個のＳＩＰの課題に比べて関係省庁やオペレーターが多いので、事務局の支援も何倍も大変だと思います。森本統括官からも是非、事務局を代表して一言お願いします。

○森本統括官　ありがとうございます。正に関係省庁が一緒になって取り組まなければいけない課題でございまして、今事務局の人員体制も関係省庁にお願いをして強化させていただいているところでございます。しっかり体制をつくっていきたいと思います。

○久間議員

それでは皆さん、どうもありがとうございました。以上をもちまして、第32回戦略的イノベーション創造プログラムＳＩＰガバニングボードを終了します。

本日はどうもありがとうございました。