高度情報通信ネットワーク社会推進戦略本部　情報セキュリティ政策会議
第29回会合　議事要旨

１　日時

平成24年4月26日（火）　9：00～9：42

２　場所

総理大臣官邸4階大会議室

３　出席者（敬称略）

藤村　修	内閣官房長官
古川　元久	内閣府特命担当大臣（科学技術政策）
松原　仁	国家公安委員会委員長
川端　達夫	総務大臣
玄葉　光一郎	外務大臣
枝野　幸男	経済産業大臣
田中　直紀	防衛大臣
	（下条　みつ　防衛大臣政務官代理出席）
遠藤　信博	日本電気株式会社代表取締役執行役員社長
小野寺　正	KDDI株式会社代表取締役会長
土屋　大洋	慶応義塾大学大学院教授
野原　佐和子	株式会社イプシ・マーケティング研究所代表取締役社長
前田　雅英	首都大学東京法科大学院教授
村井　純	慶応義塾大学教授

（その他出席者）

長浜　博行	内閣官房副長官
竹歳　誠	内閣官房副長官
米村　敏朗	内閣危機管理監
佐々木　豊成	内閣官房副長官補
櫻井　修一	内閣官房副長官補
篠田　陽一	内閣官房情報セキュリティ補佐官

４　議事概要

⑴　討議事項

○　「政府機関の情報セキュリティ対策のための統一基準群」の改定について

○　「重要インフラの情報セキュリティに係る第２次行動計画」の改定について

○　「情報セキュリティ 2012」の骨子案について

⑵　報告事項

○　「政府機関の情報セキュリティ対策のための統一技術基準」の改定について

○　その他

上記⑴～⑵について、資料を配付し、事務局より説明が行われた。

⑶　構成員意見交換

構成員から以下のような意見が述べられた。

○　行政機関の情報公開を通じて、行政情報の二次利用が可能になることは重要である。その際、その情報公開メカニズムをどうやって脅威から守り、信頼性を担保していくかが課題である。米国国土安全保障省（DHS）では、政府の情報公開と情報セキュリティの確保に同時に取り組んでいる。日本において情報公開の取組が進んでいることは評価するが、行政情報のセキュリティを確保するメカニズムも重要である。

○　日本の行政機関には、昨年標的型不審メール訓練を実施したが、標的に合わせた攻撃をしてくるシミュレーションとして省庁ごとに異なる内容で実施し、また、訓練結果を評価したのは重要なことである。防災については訓練する仕組みが一般的にマニュアル化されているが、情報セキュリティに関する項目はほとんどそのマニュアルに含まれていない。有事の際のマニュアルやガイドラインに情報セキュリティに関する項目を盛り込む統一的な動きが必要である。

○　新たな技術である M2M や IPv6 は、日本では既に市民生活に入り込むなど、いずれも世界で最も進んでいる。最先端技術に関する情報セキュリティは日々変わるので大事であり、日本はこの分野において世界に貢献することができるので、その道筋を立てることが必要である。

○　サイバー情報共有イニシアティブ（J-CSIP）の取組が始まったが、今後、参加団体の増加を期待したい。情報をどのようにリアルタイムに展開するかが重要であり、これにより攻撃の予測や予兆が可能になる。また、J-CSIP が海外と連携することができるようになれば、日本における被害拡大防止の強い防御壁となる。今後ともこの仕組みを強化して欲しい。

○　ICT が行政機関の様々な業務に利用されている現状において、セキュリティの高いシステムを作っていくためには、各省庁が連携して、人材を育成することが重要である。優秀な人材を育てるよう、政府をあげて人材育成に取り組んで欲しい。

○　M2M は利便性の高いシステムであるが、人を介した従前のネットワークに対するサイバー攻撃対策とは異なる情報セキュリティが求められる。産業界、政府をあげて人材育成に取り組み、M2M 環境の情報セキュリティを向上させなければならない。

○　昨年 2 月にミュンヘンで開催された安全保障会議を含め、サイバー空間の在り方をテーマに数多くの国際会議が開催されている。日本においては、個々の情報セキュリティ対策は進んでいるものの、情報セキュリティに対する基本理念やスタンスが明らかになっていない。英国のサイバーセキュリティ戦略のように、情報セキュリティに対する日本の基本理念を明確にすべきである。

○　英国は、サイバー空間に関する７つの原則の１つとして国民のリテラシーの強化を盛り込んでいる。資料 3-1 の３(8)に「国民・利用者の保護の強化」とあるが、「保護」という表現では国民は何もしなくてよいという誤った安心感を生んでしまうので、情報リテラシーの向上を強調した表現にすべきである。経団連では、(独)情報処理推進機構(IPA)が実施している IT パスポート試験の点数を就職活動に際してエントリーシートに記入させることを検討しており、これにより情報セキュリティ教育が盛んになることを期待している。政府においても国民の情報リテラシーの向上方策を考えて欲しい。

○　クラウドの活用に向けて情報セキュリティ指針を作るべきである。データの格納場所については、既に国際的に議論が始まっており、日本も早急に考え方を整理すべきである。

○　サイバー攻撃により技術情報や経済情報が盗まれていることから、サイバー攻撃による被害は史上最大の富の移転と言える。情報は一たび盗まれてしまうと取り消すことはできない。日本の技術情報や経済情報が盗まれることに対しては、看過できない重要な問題として取り組むべきである。

○　国民は、東日本大震災と同様にサイバー攻撃についても自衛隊が対処してくれると期待しているが、サイバー攻撃について防衛出動の定義はされていない。日米同盟等の防衛や外交上の観点を含め、サイバー攻撃が行われたときに何ができるのか考えておく必要がある。

○　経済産業省では重要インフラ事業者との情報共有に取り組んでいるが、重要インフラ事業者、IPA、内閣官房情報セキュリティセンター(NISC)の間の情報共有が迅速に行われなければ、官邸に情報が伝わらないことになる。情報の機密性とのバランスもあるかもしれないが、迅速な対応できるような態勢を構築して欲しい。

○　資料 3-1 の施策例⑩に掲げられている国際的な規範作りへの関与は重要である。そのためには、海外から見ても情報セキュリティの顔と言える人材を育成しなければならな

い。しかしながら、現状では政府の職員は人事異動の期間が短く、そのような人材を確保することは困難である。したがって、政府は、人事異動の在り方、キャリアパスを見直し、日本の情報セキュリティ対策の顔になる人材を窓口として、海外のコミュニティで意見を言える態勢を構築する必要がある。

○　スマートフォン、タブレット端末などの普及が進み、世代間のリテラシー格差が拡大している。年配者は、若者と比較して新しいものを取り入れるのに時間が掛かる。従前のような、年配者が若輩者に教えるという教育ではなく、共に学び、リテラシーを向上させるという発想とする必要がある。リテラシー向上のためには、年配層や若年層等、ターゲットを考えながら取り組む必要がある。

○　資料3-1の施策例⑧に掲げられているサイバーセキュリティに係るテストベッドの構築は、制御システムのセキュリティ上重要であるが、日本企業が海外のシェアを確保できるよう、グローバルな連携を通じて取り組む必要がある。

○　資料3-1の施策例⑩に掲げられているように、国際規範づくりに積極的に関与することは重要である。その際、様々な角度で国益を考えて基本理念を持って臨むことが重要である。また、サイバーに関する法律については、最大公約数を日本の意見とするのではなく、リーダーシップを持って考える必要がある。

○　国益を担う人材が、人事異動により頻繁に変わってしまうようなことがあってはならない。国益を考えて、警察庁、総務省、経済産業省、防衛省をまとめられる人材が必要である。

○　情報通信技術は、現代社会を支える最も重要な基盤の一つである。昨年12月に国家戦略会議において取りまとめた「日本再生の基本戦略」においても、情報セキュリティを確保した情報通信技術の利活用を推進し、我が国の更なる競争力強化を図ることとしている。

　また、社会保障・税番号制度を導入するための「マイナンバー法案」を国会に提出しているところであり、番号制度について、国民の理解を得て、定着するうえでも、制度面とシステム面の両面からセキュリティ対策について万全を期すことが重要である。

　マイナンバーシンポジウムにおいて、最大の懸念事項として、情報流出や、それによる損害の回復が不可能である旨が指摘されている。情報セキュリティは、情報通信技術により効率化や競争力強化を図っていく上で、最大のキーコンポーネントである。

○　昨今の政府機関や防衛産業関連事業者等へのサイバー攻撃は、国の安全保障やサイバー空間における経済活動に影響を及ぼしかねない大きな社会問題である。

　このような情勢の下、「政府機関の情報セキュリティ対策のための統一基準群」が改定されたことは大変意義深いことと認識している。警察では、今回の改定を踏まえ、引き続き、情報セキュリティ対策を強化する。

また、今般改正された不正アクセス禁止法の今年５月１日の施行に向けた準備を進め、施行後は、同法に基づき、取締りの徹底や防御措置を支援する団体への援助等を推進するとともに、サイバー攻撃に関する情報収集・分析や違法行為に対する捜査態勢の強化、重要インフラ事業者等や先端技術を有する事業者等との連携強化によるサイバー攻撃への対処能力の更なる向上を図り、政府の取組に貢献するよう警察庁を督励してまいりたい。

○　サイバー攻撃への本質的な対処には、国際連携を推進することが重要である。本年３月に「インターネットエコノミーに関する日米政策協力対話第３回局長級会合」において、サイバー攻撃に関する情報の共有と研究開発の協力加速について合意した。これを受け、米国国土安全保障省（DHS）との協力関係を構築した。

また、先月、「日 ASEAN 情報セキュリティ人材育成ワークショップ」を開催したところであり、情報セキュリティ人材育成の国際的な協力にも貢献してまいりたい。私自身も国会の同意が得られれば、欧州委員会等を訪問し、情報セキュリティ協力及びサイバー空間のルールに関し議論する予定である。

さらに、国内外のインターネットにおいて、近年サイバー攻撃の手法はますます複合化・複雑化している。お手元の資料にあるとおり、総務省と経済産業省が連携して、サイバー攻撃を多面的かつ総合的に高度解析するための枠組みを検討している。このような取組を含め、引き続き情報セキュリティ対策の強化に努めてまいりたい。

我が国は M2M, IPv6 等の技術で最先端を進んでいるが、技術がガラパゴス化する例もあり、技術だけではなく国際連携のイニシアティブを取ることの重要性も述べておきたい。

○　国際連携の強化として、まず、サイバー空間に関する行動規範の作成に積極的に取り組んでいきたい。これにあたっては、表現の自由などの人権の尊重、知的財産権の保護等を重視しながら、関係国と協力していく考えである。

国連総会決議に基づき、本年８月に開催が予定されているサイバーに関する政府専門家会合に、我が国として篠塚サイバー政策担当大使を派遣する。また、本年秋には，昨年 11 月のロンドン会議のフォローアップとしてハンガリーでサイバー問題に関する国際会合が開催される予定であり、現在、この会合に向けた準備を行っている。

先日開催されたＧ８外相会合の議題の１つがサイバーであったが、この問題は今やＧ８外相会合でも主要議題になっている。二国間でも、サイバーの議論は積極的に行っていきたいと考えている。結果として我が国は若干後から入ってきたが、少なくとも今後はアジア諸国との議論をリードしていく考えである。

今日国際社会においてはサイバー空間に従来の国際法が適用されるかという根本的な議論がある。外務省としてあらゆる検討を行った結果、この問題については、基本的には、サイバー空間にも従来の国際法が当然適用されるとの立場を取るのが適当と考える。同時に、サイバー空間の特性に鑑み、個別具体的な法規範がどのように適用されるかについては、引き続き、議論していく必要があるとの立場である。この問題について、各国としっかり議論を行う。

最後に，サイバー犯罪条約については，締結に向けた準備を進めており，本条約の国

際的な普及にも協力していく考えである。

○　重要インフラ機器製造業者等の間でサイバー攻撃に関する情報共有を行う枠組みとして昨年10月に発足した、サイバー情報共有イニシアティブ（J-CSIP）の下、この３月末に情報共有ルールに合意した。今後、本ルールを踏まえつつ、重要インフラ等の分野にも枠組みを拡大していく。

近年、攻撃手法がますます複合化、複雑化するサイバー攻撃を高度解析する枠組みについて、総務省等と連携して構築していく。

重要インフラ等で活用されている制御システムのセキュリティ強化を図るため、セキュリティ検証施設であるテストベッドを今年度中、米国とも協力しつつ、宮城県多賀城市復興パーク内において構築する。また、テストベッドにおいて、評価・認証手法に関する研究を行い、競争力強化に資する国際標準化を推進する。合わせて、評価・認証機関同士の国際相互承認実現に向けた取組を促進する。

今日いただいた指摘も踏まえ、我が国の情報セキュリティ強化に努めてまいりたい。

○　今回の「情報セキュリティ２０１２」の骨子案や本年１月に報告を受けた「情報セキュリティ対策に関する官民連携の在り方について」を踏まえ、各府省庁でのＣＳＩＲＴ体制の整備及び連携の強化が求められており、連携強化の一環としてＣＳＩＲＴの要員確保が困難な省庁への支援等、能力を持った者が組織を超えて機動的に支援できるサイバーインシデント版DMAT（ディーマット）を設置することになっている。

防衛省・自衛隊としては、既にＣＳＩＲＴは設置済みであり、また、現在の防衛大綱において、「サイバー攻撃に関する高度な知識、技能を集約し、政府全体として行う対応に寄与する」としていることから、防衛省・自衛隊からのサイバーインシデント版DMＡT（ディーマット）への要員派遣や自衛隊の施設、設備を利用した要員の訓練等、政府が一体となって対処する際の活動について、有意な貢献を行ってまいりたい。

○　本日は、非常に有意義なご意見をいただいたことについて、深く感謝申し上げる。

本日、「政府機関の情報セキュリティ対策のための統一基準群」及び「重要インフラの情報セキュリティに係る第２次行動計画」を改定することになった。これらは、標的型攻撃、東日本大震災等の新たな脅威や重大な環境変化を踏まえたものであり、内閣官房及び各府省にあっては、具体的な対策を速やかに実行していただきたい。

また、次回会合においては、「国民を守る情報セキュリティ戦略」の年度計画である「情報セキュリティ2012」を取りまとめる予定であり、本日いただいた貴重なご意見を踏まえ、その策定作業にもしっかりと取り組んでいただきたい。

－　以　上　－