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28回会合　議事要旨

１　日時

平成24年1月24日（火）　17：30～18：00

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）

齋藤　勁	内閣官房副長官
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

(1)　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
(2)　重要インフラ防護のための取組強化について
(3)　情報セキュリティ月間について
(4)　その他

上記(1)～(4)について、資料を配付し、事務局より説明が行われた。

(5)　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。

○　官民連携については、民間事業者に対してもサイバー攻撃が相次いだということで不可欠であり、資料1-1の内容は当面の間の対策として適切である。また、すでに運用開始して、効果の現れている警察のネットワークや各省庁のネットワークの核としてNISCを置き、それが機能することが重要である。

○　サイバー攻撃対策においては、予防も重要であるが、事案への対処能力を強化することも重要である。事案への対処能力を強化するためには、重要インフラ事業者における連携強化も重要であるが、単に強化するだけでなく、防衛省や警察庁等の事案対処官庁も入れた取組を明確にして欲しい。

○　不正アクセス禁止法の改正が進められているところ、対策として非常に重要なものが含まれており、是非今回の国会で成立させていただきたい。

○　先般のサイバー攻撃においては、情報の不正取得が機密情報に向けられたが、我が国ではその取扱いに不十分なところがある。国家の基盤に関する情報保全体制を踏まえた上で、インターネットの安全を考えていく必要がある。

○　標的型メールの訓練やウェブサーバの脆弱性検査等については、サイバー攻撃対策としてとても有効であり、その取組み自体は高く評価すべきであると思う。これら内容を継続的に実施し、分析評価することが重要なので、今後、継続と評価のサイクルを検討していただきたい。

○　政府調達に関してセキュリティ要件を満たすことが盛り込まれたことは、とても重要な一歩であると思う。ただし、技術の進歩とその技術の対応するインフラは常に変わっており、諸外国でもその進歩は早いことから、クオリティの継続的な向上を目指していただきたい。

○　国際的な会議において、情報セキュリティの議論は非常に重要となっている。そのような場では、経済、人権、文化、環境等と情報セキュリティがセットになって議論され

ているため説得力のあるメッセージを発信できる。これから国際舞台では、益々そのような議論がなされることになると思うので、それぞれの省庁が、その役割を通じて議論を進めていくことが非常に重要である。情報セキュリティはリスクがあることだが、リスクを受けとめながら前に進むこともまた重要であるため、是非議論を進めていただきたい。

○　標的型メール攻撃の対策として、いかに二次災害を防ぐかということが重要である。そのためには、迅速な情報の共有化とその共有化が広い範囲に及んでいることが必要。今回の官民連携の取組において、各省庁にCSIRTを作って情報共有するとともに、防衛省、警察庁、総務省、経済産業省等の持っている情報を共有化し、民間の我々もその情報共有の一員として加えていただくということは、プロテクションという意味からも非常に重要。ポイントは、日本の国として情報セキュリティのレベルが上がったといえるかという観点であり、どこまでメンバーを広げていくかを検討することが必要である。

○　今後、クラウド化により機器間の膨大な情報のやり取りが増えていく。重要インフラでもクラウドを通して情報がやり取りされ、これについてのセキュリティを確保する機能が重要となると思う。

○　日本の中において、セキュリティを高めるシステムを作るということは、日本の製品、ソフト、サービスの信頼性が確保され、その価値を上げることとなり、ひいては経済成長に繋がるという観点からも重要である。

○　　官民連携の在り方について、トップダウンの形は整ったが、ボトムアップも整わないと実行が伴わない。具体的な連携に係るフォーマットを決めていかないと、具体化がなかなか進まないと考える。標的型メール攻撃については、訓練が非常に重要であると思うが、一方で企業においては大量のメールがやり取りされており、メールをクリックする前に、全て自らでチェックすると言うことが難しい状況になりつつある。このため、標的型メールを事前検査できる技術的な方策や、仮に感染した場合でも検知できる技術、他サイトへの不正なトラフィックを監視する技術の開発を進めていただきたい。

○ 公開ウェブサーバの脆弱性検査については、２年に１回はあまりに少な過ぎる。常に技術は進歩しているので、少なくとも半年に１回は行わないと技術の進歩について行けない。半年に１回は行うことができる体制をNISCに整備して欲しい。

○　　インターネットは国民生活に欠かせない基盤になってきており、経済成長の要ともなっている。このため、政府内でサイバー攻撃に対する安全保障の検討をする際には、電気通信事業者や、通信サービスを利用して日々の事業活動を行っている様々な国内企業の意見に耳を傾けていただき、セキュリティ確保の議論がビジネスの成長の阻害要因にならないように、バランスをとった形で検討いただきたい。

○　エストニアは、2007 年に大規模なサイバー攻撃を受けて以降、北大西洋条約機構（NATO）の研究施設（CCDCOE）を誘致した。そこではサイバー戦争の交戦規定を作っている。日本においても、サイバー戦争というものが本格的に始まったときにどうするべきか、これから法制度の問題を詰めていかなければならない。

○　各国は、日本を通じて同盟国や友好国の情報が漏れてしまうのではないかということを懸念している。この観点から考えると、情報セキュリティは、国家的な信用の問題にもなってきている。内閣官房情報セキュリティセンターから説明のあった内容は、非常に重要であるが、できることはまだ限られているので、その範囲を広げていって欲しい。

○　情報セキュリティ政策会議の上にある IT 戦略本部は、持ち回り開催されているだけで、震災のかなり前から開かれていない。インターネットについては色々なテーマがあり、日本の戦略を考えていく必要があるので、IT 戦略本部のリスタートを考えていただきたい。

○　情報セキュリティ月間について、多様な対象に対して行う啓発活動は重要であり、今後も継続して行っていただきたい。また、この際にぜひ、官房長官から政府として情報セキュリティ対策に取り組むという分かりやすいメッセージを出していただきたい。

○ 情報セキュリティの向上とシステムの利便性確保の両立を図りつつ、情報セキュリティ産業の輸出拡大を目指していただきたい。現在、政府において社会システムの輸出促進を進められているが、これと併せて、情報セキュリティ産業のレベルアップと輸出促進も進めていただきたい。

○　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と考えている。ご指摘のあった IT 戦略本部については、２年前に戦略を作って実務的には動いているものの、もう一度リスタートできるよう内々に議論しているところであり、できるだけ早く再スタートしていきたいと考えている。

　昨年 12 月、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」の中でも、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て、我が国の更なる競争力強化を図ることとなっている。

　本日ご議論いただいた取組が、この再生戦略と整合性の取れる形でしっかり成果をあげられるよう、政府内で緊密に連携して取り組んでいくように努力したい。

○　昨今、政府機関や防衛産業関連事業者等がサイバー攻撃を受けていたことが明らかになるなど、サイバー空間の脅威が高まる中、官民における対策の強化について取りまとめられたことは大変意義深いことと認識している。警察では、先端技術を有する全国約四千の事業者等との「サイバーインテリジェンス情報共有ネットワーク」の構築によるサイバー攻撃事案に関する情報の集約・分析等の実施、全国の都道府県警察と重要インフラ事業者等で構成されるサイバーテロ対策協議会の定期的開催等、官民

連携した取組を推進している。
　また、不正アクセスを始めとしたサイバー攻撃への対策を強化するため、今国会上程を目指し、フィッシング行為の禁止、不正アクセス罪の法定刑の引上げ等を内容とする不正アクセス禁止法の改正を検討しているところ。
　国家公安委員会としては、情報セキュリティ月間における集中的な広報啓発はもとより、引き続き、官民連携を強化して、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。

○　サイバー攻撃への対処における情報共有に関しては、昨年11月に立ち上げた「テレコムアイザック官民協議会」を活用し、内閣官房が中心となって進める官民連携の強化に貢献してまいりたい。同時に、サイバー攻撃への本質的な対処には、情報共有に加え、技術開発や国際連携を推進することも重要である。技術的な面からは、現在、NICTにおいて、サイバー攻撃の観測情報を収集するnicterを運用しているが、これをウェブサイト上で年度内に一般公開することとした。国際連携の側面からは、サイバー攻撃発生の予知や即応を可能とする技術の研究開発について諸外国との連携を強化する予定であり、既にASEAN諸国等との調整を開始しており、これらの取組を通じ貢献してまいりたい。同時に、先般の総務省におけるウイルス感染事案を踏まえ、感染を防止するのは中々難しいところもあるので、早期発見、重症化しないための早期修復、感染の拡大防止、万一情報が流出した際の流出した情報の把握といった各フェーズの対策について、自治体クラウドに関する対策も含めて、強化を行ってまいりたい。
　また、セキュリティに直接関係した話ではないが、「アラブの春」などを受けて、サイバー空間のルールに関する国際的な議論が活発化しており、例えば、米国のクリントン国務長官はインターネット上でも人権弾圧は許されないとして、サイバー空間における人権の保護の重要性についてスピーチしている。これ以外にも色々な会議で、各国は大臣級が戦略的に発言をしている。日本政府においても、総理や閣僚が、意識して戦略を持ってメッセージを出すことをしっかりと考えていかなければならないと思う。

○　サイバー空間については国際協力が重要であり、国際社会の関心の高まる中、外務省は英国、米国等との二国間レベルの協議を行っている。また、省内体制も課長級から大使級のタスクフォースを立ち上げた。国際的には、様々なメッセージが発せられており、特に安全保障面では、陸・海・空・宇宙と並んでサイバーの分野は極めて重要との意識を持つことが必要であり、国際社会の中でもきちんと規範をしっかり作っていくことが重要と考えており、アジアにおいては、日本がリードするという考えの下、進めているところ。

○　官民連携の情報共有については、昨年10月25日、セキュリティ対策の実施を要請すると同時に、民間の重要インフラ利用機器の製造業者等に対して、サイバー情報共有イニシアティブ（J-CSIP）を発足し、（独）情報処理推進機構（IPA）との間で、情報共有をしっかりと行っていくということで、IPAを情報共有の集約点として、しっかりと連携を進めている。今後、年度内を目途に、J-CSIPとIPAとの情報共有ルール等を整備す

るべく、鋭意進めている。なお、IPA は三菱重工業に対するサイバー攻撃に対する分析と対策レポートを公表して、約３万社に情報を提供している。

重要インフラ等のセキュリティ対策について、原子力発電所の制御システムについて、実態としては遮断されていたが、外部からのアクセス遮断を内容とする関係省令の改正を実施した。また、電力・ガス等の個別分野ごとのサイバー演習を、24 年度目途で実施するということで準備を進めている。

情報セキュリティ月間については、各種セミナー等で周知をしたいと考えている。

○　防衛省・自衛隊においては、平成 20 年３月より、24 時間体制の自衛隊指揮通信システム隊でネットワーク入口出口の監視を行うなど、サイバー攻撃対処に日々努力しており、幸いにして被害を被ることは防げているが、昨年の防衛産業などに対するサイバー攻撃事案は、日本でのサイバー対策強化を行う上で、重要な警鐘を鳴らすものであった。今回、本会議において、政府内のみならず、民間のセキュリティ事業者との連携強化策等が取りまとめられたことは、大変意義深いものである。また、防衛省では、昨年の事案を踏まえ、私が中心となり、防衛産業における情報セキュリティの強化を進めてきた。被害を受けた企業から事情を聞くとともに、その反省を踏まえ、昨年 11 月には、防衛関連企業 140 数社のトップを集め、企業における情報セキュリティ強化について要請を行うとともに、先月には関係規則の改正を行ったところである。今回の報告を踏まえ、今後、具体策を検討していくこととなるが、政府全体のセキュリティ向上に向けて、防衛省としても検討に積極的に参加し有意に貢献していきたい。

○　本日は、限られた時間にもかかわらず、非常に有意義な議論ができたことについて、深く感謝申し上げる。

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」に掲げられた各取組については、本日の御議論を踏まえつつ、速やかに実行に移していきたいと考えている。

重要インフラについては、環境の変化に的確に対応し、国民の安寧な生活を守るという観点から、重要インフラ専門委員会等における精力的な検討を期待している。

まもなく２月から始まる情報セキュリティ月間は、情報セキュリティに関する普及啓発という本来の目的はもちろんのこと、これらをはじめとする様々な取組を進めていく上でも絶好の機会である。私も、本会議の議長として先頭に立って参るとともに、分かりやすいメッセージを出していきたいと思う。

内閣官房及び関係府省庁にあっては、これらの取組をしっかりと実行し、然るべき成果を上げていただきたい。

－ 以 上 －