資料４

有識者構成員意見

① 前田構成員意見
② 村井構成員意見
③ 小野寺構成員意見
④ 黒川構成員意見
⑤ 野原構成員意見

セキュア・ジャパン2009と今後の情報セキュリティの方向性について

首都大学東京法科大学院教授　前田雅英

１　政府のサーバの半減化について

政府機関のセキュリティ対策は、かなり徹底されてきているといえよう。ただ、前回の会議で紹介された「政府機関のＷＥＢ改ざん」に関する報告を聞くと、問題発生後の危機管理体制に関しては、まだまだ不十分なところが見られる。今回、サーバ管理の合理化の為に、サーバ管理の集約化が提案されているが、問題発生を切掛けに、速やかな対応が望まれる。各省庁の個別事情も存在するであろうが、予算の無駄をなくすという意味でも、集約化は必要であると考える。

２　ＩＣＴ社会の発展と日本の責務

ＩＣＴ社会の発展は、様々な問題において「国際的な配慮」の要請を強めることはいうまでもないし、本会議でもかなり論じられてきた。ただ、具体的認識が十分でない問題領域も存在する。その典型が、児童ポルノである。児童ポルノの害悪は、ＩＣＴと結びついて飛躍的に拡大した。被害児童にとって、まさに「忌まわしい」画像が、瞬時に世界中に広まり、永遠に消し去ることができなくなってしまうのである。そして、ネットに流れている問題画像に日本発のものが多いと、世界から指弾されている。政府が、ブロッキングなどの対策にようやく取組みはじめたことは評価できるが、アメリカをはじめ多くの国々が要請する「児童ポルノの蔓延の根を絶つ対策」、すなわち児童ポルノ所持罪の法制化などは実現していない。議員立法として提案されているが、今国会での成立は容易ではないようである。このような現状は、国際的な非難を浴びるということに止まらず、日本国民のネット社会への不信を助長することにもなりかねない。

３　青少年に有害な情報内容に対する対応について

このところ、日本の犯罪数は確実に減少してきているが、サイバー上の犯罪の増加傾向は変わっていない。ネット社会については、国民の不安は深刻化している。裏職業サイト等人身に対する犯罪の誘因の除去、詐欺等の財産被害の防止、（個人）情報の保護、名誉等の人格権への配慮等々、取り組むべき課題は多い。しかし、今最も注目が集まっているのが、児童買春を媒介するネットや、児童・生徒のいじめの手段として使われるサイトなど、青少年への影響の問題である。「青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律」が本年４月に施行されたにもかかわらず、兵庫県や石川県では、このような問題に対処する条例が独自に作られている。そして、このような規制の動きは全国に拡がっていくように思われる。国民が安心して使えるＩＣＴ社会にしていくために、具体的レベルでの対応が急がれるているのである。フィルタリングなどの対策が講じられつつあるが、「被害を本当に防いでいるのか」の検証が不可欠なのである。

意見書

2009 年 6 月 22 日
慶應義塾大学　環境情報学部
教授　村井　純

1. 民間組織とのより強力な協調・連携体制作り

インターネットなどの情報技術をとりまく状況は世界中で目まぐるしく変化しており、各国政府は新しい事象による影響への対応が求められている。このような状況において、日本は情報技術の先進国として率先して対応にあたり、その規範を世界に示していかなければならない。しかし、今日に見られる新しいサービスや活動・事故や事件は、急速に変化する社会・文化・経済・技術と相互に影響し合っている。そのため、どのような事象が発生したのか、その事象によってどのような影響がでたのか、という結果の情報だけではなく、なぜ発生したのか、どのようにして発生したのか、誰が発生させたのか、など、その事象が発生した原因となる情報を明確に意識して問題に取り組まなければ、対応はできない。このような本質を見極めた対応には、政府だけではなく、知識や経験を有する民間企業や民間団体がどのように連携・協調するのかを明らかにし、情報セキュリティ政策会議がこれらを束ねる役割を担う必要がある。さらに、このような連携・協調では従来の制度・方式に囚われることなく、恐れずに新しい体制作りに挑戦する姿勢が不可欠である。

一方、情報セキュリティ関連の組織以外との協力も視野に入れて対応しなければならない。例えば、今日の情報ネットワークの基盤はインターネットであるが、インターネット上に展開される多様なサービスも十分に普及していれば、各々が 1 つのインフラストラクチャとして位置づけられる。このようなサービスが事故や事件によって機能低下、あるいは停止した場合にはインターネットの障害と同等、もしくはそれ以上の影響を及ぼす可能性がある。したがって、情報技術の可用性を維持するためには、このような企業・団体との協力関係も構築していく必要がある。

2. グローバルガバナンスに対する情報セキュリティ面でのアプローチ

情報セキュリティに関連するコミュニティだけではなく、その他のグローバルガバナンスでも世界に日本の意見や取り組みを発信していかなければならない。情報セキュリティはあらゆる分野に関連する問題であるにも関わらず、日本から情報セキュリティに関する情報の発信が十分であるとは言い難い。このようなアプローチが積極的になされなければ、国際社会に取り残され、グローバルガバナンスにおいて日本が大きく遅れをとってしまう可能性があるという認識を持たなければならない。今後は、世界に通用する情報セキュリティのメッセージを強く発信していく必要がある。

以上

有識者構成員意見③

情報セキュリティ政策会議へのコメント

平成 21 年 6 月 22 日

ＫＤＤＩ株式会社　社長兼会長
小野寺 正

１．官民連携の更なる強化に向けて

官民連携の必要性については、「第 1 次情報セキュリティ基本計画」の当初からその重要性が認識され、官民連携に関連する施策実施の強化が進められている現状にあります。官民連携については、広い対策実施主体（政府機関・地方公共団体、重要インフラ、企業、個人）に対して適用が考えられており、これまで重要インフラ、人材育成、サイバーテロ対策などで「官民連携の取組み」が行われ成果を上げています。今後更なる官民連携の枠組みを広げ、効果的かつ実効的な取り組みとしていくために、IT 先端技術に関わる組織を有機的に連携させることにより、官民の幅広い知見を有効に活用していくことが可能になります。セプターカウンシルも機能し始めていますが個人レベルの貢献に頼る部分が多く、組織だった動きを行っていくためには、組織のトップの意識改革を図っていくことが重要と考えています。

本政策会議の成果をもっとアピールしていく方法を検討すべきです。

２．中小企業（中小通信事業者なども含む）のための情報セキュリティ

これまでの多くの情報セキュリティ確保の施策は、政府・地方自治体、重要インフラ、企業、個人と幅広く実施してきましたが、企業の中に分類される「中小企業（中小通信事業者なども含む）」にとっては、なかなか大企業と同様なレベルの対策を実施することができない現状にあります。大企業からアウトソースの関係をもつ中小企業こそ、そのセキュリティ対策に十分な関心を持ち、その実施を具体的に推進する必要があります。現在、中小企業を対象とする情報セキュリティ対策、アウトソースにおけるセキュリティ対策などの検討が始まっていますが、具体的に活用できるレベルには到達しておりません。中小企業用セキュリティ対策集の策定、簡易認証システムの整備など、具体的かつ実効的な施策をさらに推進することが望まれます。

以上

有識者構成員意見④

2009 年6月22日
富士通株式会社
黒川 博昭

第 22 回情報セキュリティ政策会議 意見書

1. 事故再発防止の観点から情報セキュリティ対策を実施・検討するべき

各府省庁では、政府統一基準に基づいてPDCAのサイクルが確立されております。しかし、各フェーズを個別に見ると、Plan Do はこの数年間で強化されましたが、まだ Check が十分でないと考えます。IT が活用されるフィールドと情報セキュリティは、組織マネジメント(プロセス)、そこで仕事をする人間系(人)、そして、システム(IT)から成り立っていると考えています。しかも、取り巻く環境は必ず変化するものなので、セキュリティレベルを高めるためには、プロセス・人・IT に対する不断の Check が必要です。小さなトラブルが生じた時でも、本質的なチェックを行い、対策していくことの積み重ねが、事故の再発防止、環境に即したセキュリティレベルの維持・向上につながると考えます。

2. 情報セキュリティの強化には政府機関トップの強い意識と実行力が不可欠

政府機関トップの情報セキュリティに対する強い意識と実行力(リーダーシップ)が重要です。民間や政府機関によらず、組織に属する人間は “上”を見て仕事をしていると思います。トップが率先して、情報セキュリティ強化の意志を常々部下に表明し、現場がどのようにセキュリティ対策を実行しているのかに関心をもち、トラブルが生じた際に事故報告と対策の実施を求める事が重要です。それが、結果として、第2次情報セキュリティ基本計画の施策を活かし、組織全体のセキュリティの強化につながると考えます。

3. 消費者庁の創設に際し、NISC は消費者庁と一体となり、電子政府の先進的なセキュリティモデルを検討するべき

消費者庁には、消費者である国民から、手紙・電話・FAX・メールなどで、ネガティブなものも含め、様々な情報が寄せられることと思います。また、製品・サービスの供給者である企業等との間でも、事実の確認・原因の追求・対策の実行などにあたって、機微な情報をやりとりすることになると思います。その際、情報提供者の権利に十分配慮したうえで、提供された情報を取扱うことが当然大事になります。それは、供給者からの情報の取扱いも同様です。

消費者庁は、国民の安全のためにあるものであり、国民本位の行政を実現するためには、機微な情報の扱いを十分考慮したうえで、行政の“見える化”を適切に図ることが大事だと思います。そのために情報セキュリティが確保された電子政府の先進的なモデルを消費者庁で構築して頂きたいと思います。

政府・自治体の何れの組織も公共性があるものですから、情報セキュリティが確保された電子行政のモデルはどこでも必要なことだと思います。NISCは消費者庁の情報セキュリティ対策について積極的に関与し、公共性の高い組織での透明性・効率性を確保した情報セキュリティのあり方、電子行政のあり方についてのモデルケースを策定してはどうかと思います。

以上

情報セキュリティ政策会議にあたっての意見

2009 年 6 月 22 日
（株）イプシ・マーケティング研究所
代表取締役社長　野原　佐和子

1. 政府機関のサーバ集約化とともに、ＩＴ戦略の国民・企業ＩＤ、「霞が関クラウド」などの積極的推進を

本日の決定事項に、公開ウェブサーバ約 1,000 台と電子メールサーバ約 1,900 台を 2013 年度末までに（5 年近くかけて）半減するという「政府機関におけるサーバ集約化」があったが、公開ウェブサーバと電子メールサーバは、多様な業務システムの中でも他システムとの関連性が低く集約化は容易な課題だと思うので、必ずしも「半減」にこだわらずそれ以上の集約化を、セキュリティ向上の観点だけでなく、行政の合理化・生産性向上の観点からも、速やかに実施していただきたい。

また、IT戦略本部では「IT 戦略の今後の在り方に関する専門調査会」でIT戦略を検討中であるし、総務省でも「ICTビジョン懇談会」で、今月ICTビジョンを取りまとめた。

それらには、電子政府推進の鍵となる国民・企業IDに関しては「国民電子私書箱」や企業コードの連携・一元化が、政府機関の業務システム最適化に関しては「霞が関クラウド（仮称）」などが書き込まれた、素晴らしい戦略が取りまとめられたと思う。

しかし、戦略・ビジョンが素晴らしくても具体的に実行されなければ意味がない。サーバ集約化とは比較にならない大きな課題なので、全体を見渡して政府がしっかり旗振りをして、縦割りの省庁間の壁を乗り越え、推進していただきたい。

国民・企業IDに関する問題や「霞が関クラウド」の施策推進段階では、セキュリティの観点を考慮することも重要で、安心と利便性とを両立させるシステム構築をお願いしたい。

2. 情報セキュリティに対する免疫力の強化を

情報セキュリティ対策をしっかり実施すればインシデントがゼロになるというのは幻想で、技術の進展や普及にしたがって新たな脅威が現れ続けるため、適切な対策を継続的に行っても事故は発生し得る。だからこそ、予防策を適切に実施するとともに、万一事故が発生した場合にも被害を最小限にできる「免疫力」を強化することが重要である。

こうした「事故前提社会」の考え方は、政府機関・重要インフラ・企業におけるセキュリティ対策だけでなく、国民一人ひとりについて考える時も同様で、安心・安全な社会を強調するあまり、個人の免疫力強化策が疎かにならないように留意すべきである。

3. 現下の経済情勢だからこそ、トンネルを抜けた時の成長につながる施策を

わが国は「技術は強いが、事業は弱い」と言われるが、情報セキュリティにおいても、研究開発した技術を事業化して成功させる力を強化する必要がある。そのためには、異なる複数領域についての知見や経験を持つ人材を産業界全体で育成し活躍できる環境を作っていくことが重要だ。

例えば、「情報セキュリティ技術力」と「事業開発力」とを併せ持つ人材、「情報セキュリティ領域での知見」と医療・教育・流通・農業等他の「産業領域での知見」を持つ人材、さらに、国際展開の経験を持つ人材などが、大学や産業界で育ち、活躍でき、キャリアアップしていける社会環境の整備が望まれる。