資料１０

有識者構成員意見

① 野 原 構 成 員 意 見
② 前 田 構 成 員 意 見
③ 村 井 構 成 員 意 見
④ 小 野 寺 構 成 員 意 見
⑤ 黒 川 構 成 員 意 見

第 21 回情報セキュリティ政策会議にあたっての意見

2009 年 5 月 8 日
㈱ 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. 「セキュア・ジャパン 2009」における成長の各段階のイメージを支持。「セキュア・ジャパン 2009」のポイントに沿って積極的に施策推進を

「セキュアジャパン 2009」の「3箇年を通じた方向性及び取組みの流れ」で整理された「自覚」→「協働」→「成熟」という各段階のイメージに賛成である。

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環境にあるため、適切な対策を継続的に行っても事故は発生し得ること、だからこそ予防策を適切に実施し、万一事故が発生した場合の対応策を準備することが重要という「事故前提社会」の考え方を、政府機関・重要インフラ・企業に関わるトップから個々の従業員まで、あるいは国民一人ひとりまで、社会全体に広く浸透させることが重要である。そうした視点で、「セキュア・ジャパン 2009」のポイントに書かれている「新たなテーマに対する官民の共通認識の形成」にしっかり取り組んでいただきたい。

また、その他のポイント「電子政府の推進」「情報セキュリティ人材の確保・育成」「国際連携・協調の推進」「情報セキュリティ技術戦略の推進」についても、フォーカスの仕方として適切だと思うので、しっかり実施していただきたい。

2. 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。トップが明確なビジョンを示し、ぶれることなく旗を振り続けることが重要

昨今の厳しい経済情勢への対応策として、失業者対策や中小企業支援策などが重要であるが、短期的・局地的視点だけのいわば「パッチ」を当てるような施策を行うのではなく、トンネルを抜けたときの成長につながるような将来を見越した施策を重視して推進していくことが重要である。

情報セキュリティ対策においても、あるいは IT 戦略においても同様で、「パッチ」ではなく全体の将来像を踏まえた施策を、ぶれることなく継続的に推進していくべきである。

一組織だけにとって最適化された情報セキュリティ環境作り、あるいは、他社製品との連携が困難なツール提供にならないように、「全体最適」のイメージを描いて、それに向けて様々な関係者が連携していく推進することが重要である。例えば、個々には充分な環境整備が困難な中小企業向けに、SaaS/ASP などで情報セキュリティ対策を含んだ業務用サービスを推進することなどが考えられる。

いずれにせよ、「パッチ」ではなく将来に向けて「全体最適」を実現するためには、政府などトップが明確なビジョンを示し、ぶれることなく旗を振り続けることが極めて重要である。

第21回　情報セキュリティ政策会議資料　2009/5/8

2008年度のセキュリティ政策の評価とセキュア・ジャパン2009について

首都大学東京法科大学院教授　前田雅英

1　2008年度の情報セキュリティ政策の総合的評価としては、［インシデントは減少しておらず不安も残っているとはいえ、セキュリティ基盤の強化に向けた十分な取組がなされた］とすることは許されよう。

サイバー上の犯罪対策に関しては、犯罪数を一定の範囲に抑え込むことも重要であるが、新しい態様のものの出現に対応しうる体制を今よりさらに強化することが望まれる。

2　政府機関のセキュリティ対策は、その実施状況報告によれば、かなり徹底されてきているといえよう。ごく一部の省に不十分さが見られるものの、かなり高い実施率、到達率を示しているといえよう。

ただ、政府機関のWEB改ざんに対する対応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。失敗の経験をムダにすることなく、サーバー管理の合理化など、ＮＩＳＣによる強い指導を行うべきである。

3　政府機関のセキュリティをいかに高めても、情報共有の必要な組織、とりわけ地方公共団体における情報のセキュリティに欠缺があれば、国民にとって大きな問題が生じる。地方分権の流れとの整合性を意識しつつも、「情報網の不可分性」という視点からは、公共団体についても、内閣が一定の提言をすることは許されるように思われる。

さらに、扱う情報量が多くかつ公共的性格を有する「大学における情報セキュリティ」もあらためて検証する必要があろう。その関連で、文科省のセキュリティの取組が、今回の実施状況報告を見る限り、消極的に見える点は気になる。

4　これまでの情報セキュリティ政策の中核が、重要インフラの分野での対応であり、セプターカウンシルの創設は、非常に重要な意味を持つと思われる。「すべての領域の参加と合意」が望ましいが、現在の「可能な範囲で積極的に前に進める」という姿勢が実践的であり、情報通信分野、金融分野等を中心に、具体的な活動の蓄積が期待される。

5　原子力発電における安全性と同様、ＩＣＴ（産業）におけるセキュリティ技術は非常に重要なものであり、技術戦略専門委員会による「情報セキュリティ技術のグランドチャレンジに繋がる方向性」の提示が強く期待される。

有識者構成員意見③

意見書

2009．5．8　村井　純

１．政府情報セキュリティ対策構造と体制の評価

情報セキュリティにおける脅威の把握、対策の考案、緊急時の対応を効率的に実施するために、日本全体の情報セキュリティ対策には次の３点が必要であった。

（１）組織的・構造的・体制的に確立すること。

（２）持続的に運用すること。

（３）かつ、継続的に発展すること。

内閣情報セキュリティ政策会議、ならびに、NISC の体制作りの取り組みは、国際的にも高い評価がなされており、成果を上げている。

しかし、現在情報セキュリティ政策を牽引している NISC 自身に対する持続性や継続性（上記、（２）と（３））に関しては、課題は常時指摘されるものの、安心できる状態にあるとは言えない。

また、 NISC を持続的に運用するための評価や見直しも必要である。例えば NISC における人材の確保・育成は重要な課題である。

これは NISC や政府全体の対策力が強化されないばかりか、変化し続ける情勢への対応力が低下する恐れがある。セキュリティの本質は持続であるため、定期的に全体の構造やその中心となる組織を評価し、改善する取り組みが必要である。

２．高度かつ十分な人材と機動性の確保とその体制作り

上記の解決には高度な人材が継続的に確保され、活動を日常的に続けることが必要である。これは直接雇用とともに、官民学の専門組織、専門家との持続的な体制作りも必要である。他国では実現されている、このような体制を常時担保する組織連携の契約的関係が結ばれていない点を改善し、組織内、組織外の体制向上をもって、上記の課題に取り組む必要がある。

３．グローバル空間での日本の情報セキュリティの責任

情報セキュリティのガバナンスに関する新しい動きが、中国やインドなど、近隣諸国から生まれている。このことが、グローバル空間のポリシーに大きな影響を与えるのは言うまでもないが、そのための体制、場所、知恵集め、意思決定の十分な体制作りに取り組むことが重要。

以上

情報セキュリティ政策会議へのコメント

2009年5月8日
KDDI株式会社
代表取締役社長兼会長
小野寺 正

(1) セキュアジャパン2009について

「セキュアジャパン2009」の現案でのパブリックコメント付与を支持する。今後の具体的な施策推進に当っては、分野横断的にIT障害が発生した際に想定されるいくつかの対処・復旧ステップの「対応目標時間」を政府として策定・管理することの必要性を検討してはいかがか。たとえば、重要インフラ事業者、セプター、所管省庁、NISC間での情報連絡・提供が遅滞なく行われるべく、情報を受けてから送るまでの各主体での目標時間を設定する等が考えられる。情報伝達スピードは迅速な事象把握、解決に向けた重要な要素であり、分野横断的演習でも目標時間を考慮したシナリオを作成し検証することが望まれる。

(2) 政府機関における情報セキュリティ対策について

2008年度に報告対象を全府省庁の55万人に拡大し、さらに把握率を向上させたことを評価する。一方で評価を基本的に各府省庁の自己申告に頼っていることは、「実態通りの評価ができているか」という観点から不安が残る。よって評価の正確性を高める意味でも一部「実査」を可能な範囲で検討してはいかがか。たとえばWEB改ざん等情報セキュリティ事故が実際に起きた機関・拠点にはNISCと関係府省庁にて実査に入り、直接問題の指摘と解決の助言を行うことも考えられる。また今後、各府省庁が自主的にリスク評価して対応計画を策定、実施する方向に進めるための更なる働きかけが必要と考えるが、その際は、各府省庁に数値的な目標設定、たとえば「実施率を○○%に向上」、「教育受講率を○○%に向上」等を自主的に策定してもらい、取組みを促進・評価して行くことも得策と考える。

(3) セプターカウンシルについて

セプターカウンシルの創設を通じ重要インフラ領域の情報共有体制強化に向けた基礎作りを推進した各セプターおよびNISCの取組みを評価する。セプターカウンシルが今後、有効に機能し続けるために、各セプターと重要インフラ事業者の積極的な取組み、またNISC、所管省庁の強い支援を求めたい。ついては今後、平時、有事の情報共有に関して、情報内容、体制、仕組み作り等の更なる具体化を進めるとともに、その有効性の検証が可能となるよう演習実施や、将来は諸外国セプター(相当)との情報共有、連携も期待したい。

以上

有識者構成員意見⑤

2009 年 5 月 8 日
富士通株式会社
黒川 博昭

第 21回情報セキュリティ政策会議 意見書

「2008年度の情報セキュリティ政策の評価」では、第１次基本計画の３年間の総評もあわせて報告されました。情報セキュリティ政策は、NISC のリーダシップのもと、政府機関の分野をはじめ確実に成果が出てきていると思います。一方、今回の会議では、政府機関の WEB 改ざんについての報告と改善方策が示されました。以下、今回の事故と改善方策に関して 3 つのポイントを盛り込みコメントさせて頂きます。

事例を共有し、組織ルールの見直しやサーバ集約等の改善を実施頂きたい

(1) ハインリッヒの法則をふまえ事例の共有を

今回のように事故の報告を行うこと自体が重要であり評価します。併せて、根本原因の分析を行い今後の改善につなげて頂きたいと思います。一方、2 件の WEB 改ざん事例が報告されておりますが、ハインリッヒの法則*を用いれば、この 2 件の事故以外に報告されてない事例やもしくは軽微なシステムトラブルが多数存在していると思われます。事故が生じたから改善を実施するのでなく、その事故の背景にたくさんのヒヤリ・ハットが存在すると認識し、組織内で事例や改善策を共有することが大切だと思います。

注) ハインリッヒの法則: 1 件の重大な事故の陰に 29 件の小さい事故があり、さらにその奥に 300 件の小さな異常が隠れている。労働災害の事例の統計を分析した結果、導き出されたもの。

(2) 組織は劣化するもの

システムは、IT だけでなく、組織とそれに属する人が支えています。一方、IT の根幹となる技術自体が時代遅れになることもありますが、それ以上に異動等で組織は簡単に劣化するものです。例えば、開発担当者やシステム運用の初期段階に携わっていた人が異動等でいなくなるようなケースです。そのような状況で、システムの責任者がセキュリティを守れと指示しても、その指示は組織内にうまく浸透するはずがありません。そして、必ず問題が起きるのです。今回、報告された事故については、起きた問題の本質を探って頂きたいと思います。かなりの数の同種のシステムが残っていると思います。ぜひ、組織・人の面での見直しを行い、情報システムのセキュリティ対策や情報の取り扱いルール、更には事故時のエスカレーションルール等マニュアルの見直しを実施して頂きたいと思います。

(3) ウェブサーバ及び、メールサーバの集約

政府機関全体のウェブサーバ台数が約 1000 台、電子メールサーバが約 1900 台と報告されていますが、昨年も指摘したとおり、ユーザ数からすると数が多く、情報漏えいのリスクの低減とサーバの管理コストの低減の観点からサーバ集約を進めるべきであると思います。管理台数が多いと当然のごとく管理する人の数もコストも増えます。限られた人員で安定運用を実施するためにも、サーバ集約を進めるべきであると思います。

以上