

NISC NEWS

第19号 (2008年3月31日発行)
内閣官房情報セキュリティセンター
National Information Security Center (NISC)

★目次

1. 情報セキュリティ施策紹介 ～ 基本計画検討委員会について ～
2. 補佐官ノート 「情報セキュリティにおける次の一手とは」 ～ ぼくにはできません ～
3. 誰でもわかる情報セキュリティ用語 ～ ルート証明書 ～
4. NISC COLUMN (ニスコラム) ～ 雑感 ～

1. 情報セキュリティ施策紹介

【 基本計画検討委員会について 】

「第1次情報セキュリティ基本計画」(以下、「第1次基本計画」と呼びます)は、我が国における情報セキュリティ対策を抜本的に強化するための、中長期的な戦略です。平成18年2月2日に決定された第1次基本計画では、我が国が情報セキュリティ問題に取り組む上での基本理念、情報セキュリティ対策実施主体(政府機関・地方公共団体、重要インフラ、企業、個人)及び問題の理解・解決を促進する主体(政府機関・地方公共団体、教育機関・研究機関、情報関連事業者・情報関連非営利組織、メディア)の役割と連携の整理、政府が平成18年度からの3年間に取り組むべき重点政策、そして、これらの政策の推進体制について述べています。セキュア・ジャパンは、この第1次基本計画を実現するために、各府省庁が年度ごとの情報セキュリティに係る具体的な施策の実施計画及び翌年度の重点施策の方向性を示したものです。現在、NISC においては、各府省庁の協力を得て、セキュア・ジャパン 2007 の評価及びセキュア・ジャパン 2008 の策定を進めているところです。

一方、第1次基本計画は、平成20年度が最終年度であるため、官民における各種の取組み、技術革新の動向、及び制度改正等を含めた社会環境の変化等を踏まえて、平成21年度以降の次期基本計画(「第2次基本計画」と仮称する)を新たに策定する必要があります。そのための調査検討を行う「基本計画検討委員会」を政策会議の下に設置することが、平成19年12月12日の情報セキュリティ政策会議にて決定されました。

第1次基本計画では、体制整備を中心とした我が国の情報セキュリティ政策の取組み開始に重点を置きましたが、第2次基本計画の策定においては、高度情報通信ネットワーク社会を迎えた我が国に適した「情報セキュリティ政策」を幅広く検討する予定です。同委員会は、以下に示すスケジュールのように、平成20年1月より検討を開始し、議論の状況を政策会議に報告しつつ、平成21年2月に第2次基本計画を決定することを目指します。

○ 政策会議及び検討委員会での検討スケジュール

- | | |
|-------------|---------------------------------|
| 平成19年12月12日 | 第15回情報セキュリティ政策会議(委員会設置決定) |
| 平成20年1月16日 | 第1回委員会～ 以後、数回開催 |
| 平成20年2～5月 | 産業界、消費者、府省等の関係者からのヒアリング |
| 平成20年3～5月 | 論点の整理及び検討 |
| 平成20年6月 | 「第1次提言」(仮称)(政策会議) |
| 平成20年6、7月頃 | 検討再開～ 以後、数回開催 |
| 平成20年12月頃 | 「第2次基本計画(仮称)」(パブリックコメント案)(政策会議) |

現在、基本計画検討委員会においては、産業界、消費者、府省等の関係者からのヒアリングと並行して、第2次計画の検討の範囲の確定、大括りの検討項目の設定、項目毎の検討論点を抽出・列挙の順で検討が進められており、引き続き第1次提言に向けて議論を進める予定となっています。

下記ページには同委員会で用いられた資料や議事要旨などを随時掲載して参ります。議事要旨等をご覧になっていただければ、様々な経歴をお持ちの委員や関係者の方々から、多様な切り口のご意見が出て、熱く議論が進められている状況を実感いただけたと思います。また、第2次基本計画のパブリックコメント案が決定された際には、皆様から忌憚の無いご意見をお寄せいただければ幸いです。

<http://www.nisc.go.jp/conference/seisaku/kihon/index.html>

2. 補佐官ノート「情報セキュリティにおける次の一手とは」

【 ぼくにはできません 】

私は情報セキュリティ補佐官を務めているが、本業は奈良先端科学技術大学院大学で教授をしている。私の大学は、大学院だけから構成される独立大学院で、日本全国の大学、高等専門学校から、多彩なバックグラウンドを持った学生が集まってくる。異なる分野から挑戦してきたり、企業を退職して学位取得をねらったりする若者達も多い。今年も4月に、新入生として、どんな若者達がやってくるのかと楽しみだ。

学生諸君と一緒に活動をしていると、本当に興味深い事象に出会い、そして私が常々心に持っている、ある考えを強化してくれる。その考えとは、「知的生産活動の限界は与えられるものではなく、大半は、自分が勝手に設定している」ということだ。

私たちの日常は、挑戦の連続である。その挑戦はわずかなことから、自分の人生を左右する重大なものまであるだろう。個人的な挑戦もあれば、自分が所属する組織が行っている挑戦の一部を分担することもあるかもしれない。自己生存をかけた挑戦も含まれているのは、言うまでもない。さらに、厳然たる事実として、競争社会の中に私たちは生きている。その競争も多種多様なものがある。それぞれの挑戦に対して、良い結果を出すかどうか、常に試されている。挑戦しながら、良い結果を出すためにはどうしたらよいかを考えることは、日常そのものだ。

その中で、私たちは、時々「特定の挑戦を辞める」ということで、全体成績を向上させる戦略を取ることもある。別の言い方をすれば、挑戦についてポートフォリオ管理を行い、芳しくない挑戦については、損切りを実施するという表現もあるだろう。戦略的撤退という言い方もある。それ自体を否定する気はない。ただ、その時に、状況がどうなっているかを正確に把握する努力を行い、何が問題だったのかを理解することは大切だ。しかし、人間は機械ではないので、時に感情という波にさらわれ、撤退を決めてしまうこともある。本来すべき状況解析を放棄し、挑戦を途中で断念してしまうのだ。また、同時に、自己否定をすることによって、断念することを正当化することもある。

私が向き合ってきた学生の中にも、時に状況判断無く「ぼくにはできません」という一言を感情的に吐き出して、挑戦をあきらめてしまう学生が何人もいた。しかし、だからといって、そんな彼らが本当にダメ人間ではないのだ。事実、そんな弱音を吐いてしまった学生に、「まあ、そうは言うけど、冷静に問題を考えてごらんよ」と研究の現状把握と方向性を検討して、そこから本当に良い研究活動を成し遂げた学生も沢山いるのだ。そして、一度挑戦を断念した学生が育っていくことに出会う度に、私は「ああ、知的生産活動の限界は自分が作ってしまうのだなあ」という信念を強めてきた。

情報セキュリティ管理の多くは、膨大な知的生産活動を要求する。情報セキュリティ管理に、これぞ決定

版というものはない。組織の構造、文化、特性、業務、歴史、人々、経済状況など、無数のパラメータを考慮して、さまざまな施策を複合的に実装して、何とか一定の信頼性を担保するのが普通だ。知的生産活動無くして、情報セキュリティ管理はできない。ところが、「私は文系なのでできません」、「私はコンピュータをしらないのでできません」といった、自分で限界を設定して断念する言い訳を聞くことが多い。しかし、はっきり言おう。それは単に自分に対して限界を設定して、断念を正当化しているだけに過ぎない。私たちの知的生産活動には限界はないのだ。「じゃあ、どうしたらいいのだ？」と、あなたは私に問いたくなるだろう。

私からは三つのアドバイスをしたい。

(1) 根源的理解を得る努力をする。

自分が取り組んでいる事項について理解を深めることは、常に努力しなければならない。多面的に問題を知る努力をし、問題がどこにあるかを常に考え続けることが必要だ。

(2) 考えを深める時間を長く確保する。

普通に暮らしていると、15分に一度ぐらいの間隔で誰かに割り込まれる。問題を考えているように思っても、実は考えている作業ができていないことが多い。真剣に考えるということには、誰にも邪魔されず長時間深く、深く考えることが必要だ。

(3) 議論をしよう。

自分の考えていることを、仲間と議論して、方向性、考え方、視点などをチェックすることが必要だ。

これは、情報セキュリティ管理で、壁にぶち当たった時にも、必ず有効な方法である。そして、この三つに忠実なあなたなら、単純な放棄はしなくなるだろう。

もう一度、ポイントを。知的生産活動の限界は与えられるものではなく、大半は、自分が勝手に設定しているのだ。はい、今日の授業はここまで。

(山口 英 内閣官房情報セキュリティ補佐官)

3. 誰でもわかる情報セキュリティ用語

【 ルート証明書 】

確定申告の季節ですね。メルマガ読者の皆さんの中にも、e-Tax(確定申告の電子申請)を利用された方もいらっしゃるのではないのでしょうか。さて、この e-Tax を利用するには、納税者は電子証明書を格納した住民基本台帳カードを用意するほかに、クライアントPCの中に、財務省認証局と財務省運用支援認証局のルート証明書をインストールしておく必要があります。では、そのルート証明書とはどのようなものなのでしょうか？

Web サイトなどに対して暗号通信を行う際に、相手が送ってきたデジタル証明書が正当なものか調べるには、まずその証明書の発行機関を調べ、続いてその発行機関が信用できるかどうかを調べるために発行機関の証明書を調べ、という具合に順々に遡っていきます。そして、信頼できる認証局が自己署名した証明書にたどり着けば、当初の証明書は信頼できるものとみなせます。この信頼の要として使われる証明書をルート証明書と言います。しかし、証明書を受け取った時に、ユーザ自身がどの認証局からその証明書が発行されたものかなどを順に確認していくことは簡単ではありません。そのため、代表的な Web ブラウザには、実績のある大手認証局のルート証明書があらかじめ組み込まれており、ユーザが上記の手順を意識することなく証明書の信頼性を確認できるようになっています。

ルート証明書は、e-Tax の場合のように、ユーザが必要に応じて自分でインストールすることもできます。e-Tax では2つの認証局を信頼の基点とし、配付されたプログラム、受付システムから送信されたデータ、電子納税証明書、接続先のサーバが、本当に国税庁のものであるかを確認しているのです。

4. NISCOLUMN (ニスコラム)

【 雑感 】

早いもので、NISC も創設 3 周年を迎えようとしている。平成 17 年(2005 年)、情報セキュリティ政策会議を設置すべく走り回っていた創設時には 30 人にも満たなかったメンバーだったが、現在約 70 名。この間、本コラムで触れるにはとても書ききれないほどの出来事があった。

本コラムの執筆に際し、何をメッセージとして残すか、どんな話題とすべきか、いつかはコラムを書くべく、本メールマガジンの創刊時から日々構想を練り、考えてきた。なぜかと言えば、これを読んでいただいている大勢の読者の皆様のことをよくよく考えてのこと。NISC の活動ぶりは、霞が関の中央官庁は当然のこと、地方公共団体や重要インフラ事業者、一般企業や個人といった、情報セキュリティ対策に関与している多くの皆様から様々な視点で日々注目されている。執筆している私自身、NISC 創設時以降、数え切れないほどの関係者の皆様の顔が浮かび、浮かぶごとにキーボードの手が思わず止まってしまう。

NISC 創設以降、様々な場で情報セキュリティ対策の重要性がより深く認識されてきているものとする今日、情報セキュリティ対策のことを考えている皆様も日に日に増えてきていると感じている。一方で、どんなに技術が発達しても、情報システムは「人」の関与無くして動かない。その意味において、情報セキュリティ対策は「人」あってこそはじめて成立するものであると言える。

現在推進している「第 1 次情報セキュリティ基本計画」は、平成 20 年度(2008 年度)が最終年度。今年の年明けからは次の基本計画の検討も開始されている。この 1 年は、当面の情報セキュリティ政策を立案していく上で、大変重要な、正念場の年である。

NISC は、情報セキュリティ政策に係る基本戦略の立案、官民における統一的、横断的な情報セキュリティ対策の推進、そして、これらに関する総合調整を行う組織と位置付けられている。その政策の推進に当たっては、「人」あつての政策であることを肝に銘じつつ、様々な皆様の考え方をよくお伺いし、その視点をつぶさに捉え、日々丁寧なメッセージとして説明し発信していく。時には足踏みしてでも、関係者の協力を得て何らかの答えや方向性を見つけつつ、着実に一步一步、前向きに進んでいく。これが NISC の前進なのではないか、と改めて感じている。

(だにえる)

<バックナンバー・配信先変更・配信中止>

本メールマガジンにおけるバックナンバーの取得及び配信先の変更、配信の中止等は下記の URL から可能です。

<http://www.nisc.go.jp/nisc-news/>

<御意見、御感想>

<http://www.nisc.go.jp/mail.html>