NISC NEWS

第１３号（２００７年８月１４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

巻頭言

【 NISCの第二世代に期待する 】

ＮＩＳＣ発足からの約２年間、副センター長を務めました松井です。在職中は、ＮＩＳＣニュースの読者の方々を始め、多くの方々にお世話になりました。心からお礼申し上げます。

ＮＩＳＣはわずか２０名程度でスタートしましたが、各省庁や民間企業から高い志と使命感を持った人材に結集して頂き、今や６０名を超える組織に成長しました。そして、これら第一世代の者達がこの春から夏にかけて次々と交代期を迎え、その後任として第一世代に勝るとも劣らない人材がまた集まってきました。一時的には山口補佐官が心配する組織的記憶喪失状態となりますが、人材の入れ替えはＮＩＳＣが守りに入らないための新陳代謝です。第二世代の方々には新鮮な視点でわが国の情報セキュリティ政策を考え実行して頂きたいと思います。

さて、今、情報セキュリティ対策にはトップダウン的な展開が求められています。情報セキュリティは最新のセキュリティ技術で武装すれば安心と言えるほど簡単ではありません。様々な技術や仕組みがシステムや組織の中に適切に導入され運用されることが大事です。しかし、多くの組織ではこれがおろそかにされています。この分野は技術専門的なイメージが強いため、組織のトップは情報システムの現場に任せきりというのが実情です。このような現状を改善し、トップのリーダーシップによる技術面、組織管理面、そして人事管理面という総合的観点からの情報セキュリティ対策が実施されるようなカルチャー創出が必要です。

一方、ＩＴ政策の重点課題として、電子政府の普及、医療のＩＴ化、全国ブロードバンド化が掲げられています。これは取りも直さず、セキュリティ対策の強化が最も求められている分野でもあります。この内、全国ブロードバンド化の進展によるブロードバンド人口の増大は、反面、セキュリティ意識の希薄な利用者の増大を引き起こします。最近のボットの増大などを考えるとこれは大きなセキュリティホールの出現に他なりません。国民のセキュリティ意識の向上が不可欠で、啓発活動やセキュリティ教育の重要性が叫ばれています。が、果たしてそうしたことで、ウィルス対策ソフトの導入や更新など最低限の対策を誰もが間違いなく実施するでしょうか。個人レベルで必要な最低限のセキュリティ対策を一人一人に期待するのではなく、個人が意識しなくても自動的に実施されるような技術や仕組み作りが必要なのではないでしょうか。

ＮＩＳＣの設立により、わが国全体としてのセキュリティ政策が動き始めました。情報セキュリティの確保に関してはこれだけやれば十分ということはありません。社会や技術の変化に合わせ、その時々に必要な政策を展開し続けなければなりません。私ども第一世代の者達は、このような大事な役割のバトンを第二世代に繋ぎましたので、読者の方々におかれましては、第一世代の者達に頂きましたと同様にＮＩＳＣ第二世代に対しましても温かいご支援、ご協力をお願い申し上げます。

1. 情報セキュリティ施策紹介

【 技術戦略専門委員会報告書2006の公表 】

技術戦略専門委員会は、情報セキュリティ政策会議の下に設置された専門委員会です。先日、この委員会における検討の成果として「技術戦略専門委員会報告書2006」が公表されましたので、その概要を紹介いたします。

はじめに ～これまでの経緯もふまえて～

技術戦略専門委員会は、これまでにも、技術開発に対する政府の取組みについて具体的な方向性を提言していました。この提言は、総合科学技術会議の分野別推進戦略にも反映され、また、その個別の施策についても、各府省庁において着実に取り組まれてきたといえます。

その一方で、様々な情報セキュリティに関係する事件・事故などのイベント、新たな技術の社会化などがおき、社会で活用される技術と情報セキュリティの関係も徐々に変化しつつありました。そこで、これまでに策定した提言の内容について、最新の動向に合わせたものにするとともに、より具体的な検討を行うなどのフォローアップ作業を行うことを目標として、2006年10月から本年6月まで、この委員会での議論が進められてきたものです。

以下に、この成果である「技術戦略専門委員会報告書2006」の3つのポイントについてご紹介します。

1. どういった分野を重点化していくか

研究開発・技術開発への選択と集中という考え方を明確にしていくためにも、政府の限られた投資、資源をどこに入れていくのかといった視点で検討を進めました。その際、この見直しを継続的に行うとともに、狭い意味での情報セキュリティ分野ではなく、もう少し広い情報通信分野全般として把握し、その中の情報セキュリティの立ち位置を含めた評価を行うこととしています。

また、これまでの提言の中で選定していた重点化分野についての見直しをしており、「認証技術」については単に技術開発だけではなく、社会展開までを含めた研究が必要ではないかとあらためて提言しました。さらに、色々な形で顕在化してきている新たな問題への対処についても、例えば、構成要素の検査技術の高度化により、ブラックボックス性を持った構成要素の安全性検証の確度を高めることが必要ではないかといった提言をしています。

2. 研究開発・技術開発の成果を活用する方策について

政府による技術開発の投資が色々な形で行われていますが、その技術開発の成果を、いかにして政府の中で活用していくかについて検討しました。

これはもちろん、技術開発の中で「使えないものを無理矢理使っていく」という話ではありません。実用化の少し手前にあるような開発成果と政府内での活用をどう繋いでいくかということを考えているものです。これに関しましては、調達を通して成果を活用するためのガイドラインについて、一つの試案を委員会として提言しています。

3.「グランドチャレンジ型」テーマの検討について

「グランドチャレンジ型」とは、例えば、米国のアポロ計画における「月に人を立たせる」といったような大きな目標の下で、いくつもの成果を連続して生み出していく長期間の研究開発のことです。

この具体的なテーマ検討に際しては、集中的な議論が不可欠であり、客観的な選定者（現実主義者）だけでなく、夢を見られる人（ドリーマー）が必要です。また、仮にテーマ選定が不調に終わったとしても、その過程で議論した様々な観点は、個々の研究開発に有効であると考えられます。

2007年度中に、この「グランドチャレンジ型」テーマの検討を行う、グランドチャレンジWGを開催することとしています。

終わりに

この報告書は6月29日に策定され、ホームページでも公表しております。ご興味のある方は、是非下記URLで報告書本文をご覧下さい。

http://www.nisc.go.jp/conference/seisaku/strategy/common/pdf/tech2006_rep.pdf

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」

【 ユーザは敵か味方か 】

情報セキュリティ管理では、ユーザに対して充実した教育・トレーニングを提供することが必須である。

一般に管理者がユーザに対して期待していることを分類すると、大きく分けて二つに分けることができる。一つが、日常的なシステム利用においてリスク低減のための一定の役割を負ってもらうこと。もう一つが、情報セキュリティに関わる何らかの障害が発生した時に、適切な行動をとってもらうことである。

前者は、具体的にユーザにとってのリスクは何か、そしてリスクの顕在化はどのように抑えることができるかを理解してもらい、日常的に適切な行動を取ってもらうことを教える。例えば、マルウェアの混入というリスクは、アンチウィルスソフトウェア等の防護システムだけでは完全に防ぐことができない。未知のマルウェアを、怪しげなウェブサイトから誤ってダウンロードしてしまうこともあろう。そこでユーザに対して、そもそもマルウェアの混入を引き起こしそうな行動を理解してもらい、ユーザによるその種の行動に抑制がかかるようになることを期待する。このために教育を通して、ユーザが正しくリスクを理解し、日頃から行動に注意することを促す。賢いユーザが増えれば、当然リスクを自ら顕在化させてしまうリスクを低減させることができる。賢いユーザは、管理者にとって強力な防護方策なのだ。

一方後者は、具体的にトラブルが発生した時、つまり危機的状況にユーザが直面したときに、ユーザが正しい行動をとれるように、ユーザを訓練する。危機管理の専門家の教訓として「危機的状況では人は普段していることしかできず、それすら満足にできないことも多い」というものがある。したがって、ユーザを普段から訓練し、訓練を通してユーザに対して経験を与え、危機的状況に陥った時に何をすべきかを容易く思い出させ、行動できるようにするのだ。危機的状況において、正しい行動をとれるユーザは、管理者にとってはより高いプライオリティの作業に集中できる可能性を大きくする。教育は、色々な意味で生産性向上にもつながる。

筆者はこれまで多種多様な組織での情報セキュリティについてのユーザ教育・訓練の実態を見る機会を得てきた。そして教育・訓練がうまくいかない状況に陥った組織は、実は数多くあることも知ることができた。この原因を考えるに、そもそも教育・訓練が何故必要なのかについての理解が、ユーザ側と管理者側で大きく乖離していることが主要因になっていることが多いと思う。管理者とユーザの間で、教育・訓練が行われなかった時に顕在化する可能性が上昇するリスクについての共通認識（コンセンサス）が形成できていないのだ。そもそも、そのような共通認識を形成する機会も与えぬまま、社員を業務現場に投入する事例も数多くある。また、管理者がユーザに対して過大な期待を持ちすぎているケースや、逆に職制構造によってユーザが管理者の話を全く受け入れないケースもあり、ユーザが何をしたら良いのかについて混乱を来しているケースも多々見られる。このような状況を放置すればするほど、不幸な状況になる。ユーザの不理解は、次第に管理ルールに対する違反を誘発し、さらには管理フレームワークからの完全な逸脱をも引き起こすことがある。管理者にとっては、ユーザが敵になってしまうのだ。

このような状況を防ぐためには、よく考えられた教育・訓練を提供するのはもちろんである。さらに、情報セキュリティの大切さと直面しうるリスクについての理解について、管理者とユーザでコンセンサス形成するプロセスを設計実装することが必要である。この目的のために教育・訓練プログラムを工夫することもできよう。コンセンサス形成プロセスは、ユーザと管理者の相互信頼を醸成するためにも役立つ。「お客様は神様だ」という名言があるが、情報セキュリティ管理者にとってユーザは、神様であり、同時に運命共同体を形成する同志でもある。ユーザをわざわざ「敵」にしてしまう教育をすることはない。

（山口 英　内閣官房情報セキュリティ補佐官）

3. NISCOLUMN（ニスコラム）

【 社会インフラは、一度作るとなかなか作り直せない 】

～～～　今日の情報セキュリティ環境は、「便利であれば多少の不具合には目をつぶるもやむなし」というパソコン文化と、情報を共有しそれにだれでもアクセスできることが善であるインターネット文化の宿命的な結びつき（それは宿命であったと思う）に源がある。 ＜中略＞　これが、個人的利用や学術の世界だけで使われているうちは「困ったもんだ」で済ませたかもしれないが、経済取引を始めとする社会の基本インフラに使おう、という選択がなされるところで、宿命から脱するべく何らかの抑制がかかってもよかったのではないだろうか。できの悪いインフラを使って構築した社会が、その脆弱性ゆえに後にしっぺ返しを受けるという構図は今までいたるところで経験したことなのだから。 ～～～

以上は、今を去ること7年前の 2000 年の 7 月に、筆者が情報処理学会誌の「インタラクティブ・エッセイ」という企画で書いた文章から「パソコン文化とインターネット文化の不幸で宿命的な婚姻」という副題の節からの抜粋である。当時の世相を情報化の面からみれば、電子政府という言葉が生まれて半年ほど、政府の政府サービスのネットワーク化は始まったばかり、携帯電話のｉモードが世に出て1年、情報家電が夢を売っていた時代であったが、情報セキュリティ的には、中央省庁が軒並みHPの改ざん被害を受け、新しいタイプの凶悪なウイルスが出現し始めた頃であった。このころ筆者はIPAのセキュリティセンターに在籍しており、情報セキュリティ対策が後手にまわりがちな世の中で、社会インフラに組み込まれたできの悪いシステムは、その後長く社会のお荷物になるに違いなく、多少技術を見通せる人々が先回りして安全度の高いシステムを造る努力をしなければ世の中は救われないという思いを強く持っていた。

時は巡って、7年後、7掛けのドッグイヤーなら49年後の今日、確かにいろいろな変化があるものの、基本構図はあまり変わっていないなぁと感じるのは私だけではないと思う。内閣官房で情報セキュリティ政策を2年間担当して、今、目の前にあるのは、電子政府の基盤の再構築、ますますネット依存が高まる経済取引や電子マネーの興隆などなど、情報セキュリティの裏打ちがなければ脆弱な社会インフラになってしまうもろもろのものである。脆弱性だらけのWindowsが、Microsoft Updateの定着によってようやく管理された安心状態に達するまでに要した年月や、電子署名などの基盤に使われている暗号アルゴリズム「SHA－1」の寿命が幾ばくもないことがわかってから、その対応に1両年苦労していることなどに見られるように、社会インフラは、一度定着してしまうと、作り直すことは容易ではないがゆえに、意図的に導入するならば最初が肝心である。デザインが悪いままに社会に定着してしまえば、末代まで祟ることになる。そして、最初に紹介した文章に戻るが、この節はつぎのように結んである。「運命の転換点は、もう過ぎてしまったのか。今ならまだ間に合う、というか、私には今が最後のチャンスであるように感じられる。」

さて、我々は、情報セキュリティに対する相応の問題意識を維持して必要な対処をしてきただろうか。筆者の印象では、とりあえず最悪の事態は回避してきていると思う。常に後手後手に回ってきたけれど・・・。 問題はこれからだ。残念ながら、だれもが情報セキュリティを意識しなくてもよい世の中などは当分、いや、永久にやってこないのだろう。システムの開発に従事する人々には今後とも十分な知識と技術を持って仕事をしてもらう必要がある。組織の管理者は、例えば、起こりうる最悪の事態に対する想像力を、今後ともほぼ半永久的に持ち続けてもらう必要があるだろう。そして、家庭での個人利用者などについても、使うことをためらうことにならない範囲で、適度な緊張を持ち続けてもらうことが必要であろうし、とりわけ政策関係者は、結局、「今何かをしなければ手遅れになる」という危機意識を常に持って、この悲観論をバネに（ある程度は「今ならまだ間に合う」的な楽観を持ってもよいが）、「あらゆる活動が情報化しながらつながってゆく」社会の変化を「安全・安心」なものにしていくための作戦を、「攻めの姿勢」で示していくことがこれからも求められ続けるのだと思う。

（少年探偵団長）

【 情報セキュリティ対策を巡る戦い 】

毎年6月には、いわゆる”骨太方針”が公表される。今年は、従来の「経済財政運営と構造改革に関する基本方針」から「経済財政改革の基本方針 2007」～「美しい国」へのシナリオ～へと改名されたが、この方針は、ご存知のとおり、官邸主導で予算編成すべく経済財政諮問会議にて取りまとめられたものである。

この骨太方針策定の舞台裏の様子は、『経済財政諮問会議の戦い』(大田弘子著：東洋経済新報社)に詳しいが、骨太方針は、まず民間委員が素案となる提言ペーパーを作成し、それをベースに各府省庁や政府与党との激しい折衝を経た上で策定されている。

一方、わが国の情報セキュリティ政策においても、毎年6月に「セキュア・ジャパン」が、民間有識者及び関係閣僚から構成される情報セキュリティ政策会議により決定されている。情報セキュリティ政策会議は、民間有識者及び関係閣僚から構成されており、「セキュア・ジャパン」等の決定過程においては、前述の経済財政諮問会議と類似する点が多く見られる。すなわち、民間の知見を踏まえて立案された政策をベースに、各府省庁と激しい議論・折衝が行われており、まさに『情報セキュリティ政策会議の戦い』といえよう。

その戦いを裏で支える内閣官房情報セキュリティセンター(NISC)は、現在60名程度の人員を擁しており、その約7割は、関係する府省庁からの出向者・併任者、残りの約3割は、民間企業からの出向者で構成されている。かくいう私もご縁があって民間企業からお手伝いさせていただき、約2年間、政府機関統一基準の策定・改訂、関連する個別マニュアル群の整備、自己点検や対策実施状況報告における評価方法の検討などに携わってきたが、私の周辺でもまた多くの戦いが繰り広げられてきた。

我々のグループのミッションは、各府省庁に情報セキュリティ対策を促進させることであり、主な戦いの場の1つは「各省協議」であった。各省協議では、各府省へ送付されたNISC案への「質問」から始まるが、DoS 攻撃(Denial of Service attack)のように大量の質問が文書で寄せられる場合もあり、これらに対しては文書で一つ一つ応戦していかねばならない。

続いて核心となる論点について「意見」が寄せられ、これらについても同様に文書で応戦する必要がある。正論としてどうあるべきか、現実的な内容であるか、誤解を与える表現になっていないか、齟齬はないか等の様々な論点について意見・主張が食い違う場合には、時として先方担当者との直接会話も交え、昼夜を問わず延々と熱い議論が交わされることとなる。

特に、府省庁のセキュリティ評価に関しては、その評価方法や評価値について、評価する側と評価される側の溝はなかなか埋まらず、調整は難航を極めた。最終的には「応じられない」あるいは「受け入れられない」と押し切って決着したこともあれば、意見が平行線のまま先方担当者とほとんど絶縁状態になりかけたこともあり、また、担当者同士では決着が付かずにそれぞれの上司同士での議論でようやく決着したこともあった。

その他、グループ内での事前検討における戦い、NISC外での関係省庁間の戦い、予算をめぐる戦いから、民間の常識と官公庁の常識の戦いに至るまで、さまざまな所で戦いが行われており、今日の情報セキュリティ政策は、このような戦いの賜物である。

NISCも設立2年を迎え、当初メンバーの多くがその任期を満了し、新メンバーがその戦いを引き継いでいるが、これからも骨抜きになることなく、前向きで活発な議論がなされるよう、『情報セキュリティ対策を巡る戦い』に期待するところである。

(骨ぬっきー)

＜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