NISC NEWS

第１１号（２００７年５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

1. 情報セキュリティ施策紹介

【 政策会議決定案3件に関するパブリックコメント募集中 】

４月２３日に開催された第１１回情報セキュリティ政策会議の決定に基づき、現在、情報セキュリティ政策に関係する決定案３件に関して、パブリックコメントを募集していますので、以下に簡単にご紹介します。

１．「セキュア・ジャパン２００７」（案）

我が国の情報セキュリティ対策に係る中長期戦略である「第１次情報セキュリティ基本計画（2006 年 2 月 2 日決定）」では、毎年度、より具体的な施策の実施プログラム「セキュア・ジャパン」を定めることとしています。

本年度の「セキュア・ジャパン２００７」では、昨年度の「セキュア・ジャパン２００６」に基づいた取組みに対する評価と分析を踏まえつつ検討を進めてきました。その結果、２００６年度に構築が進んだ官民の情報セキュリティ対策を推進する体制の維持や、対策が不十分な部分の底上げを含め、対策推進の安定化が課題として挙げられました。加えて、情報セキュリティ政策の人材育成・確保、及び国際連携・協調に関しては、単年度のみの施策ではなく、継続的・中期的な視点に基づく取組みが必要であると考えられます。

これらの課題に対応するために、「政府機関情報セキュリティ対策の拡充」、「広く国民も含めて遅れがちな主体の対策の普及」、「情報セキュリティ基盤強化に向けた集中的な取組み」の３点をポイントとし、４８件の新規施策と１１１件の継続施策を２００７年度の実施施策として盛り込みました。さらに、基本計画の最終年度に向け、情報セキュリティ基盤の強化を図るための集中的な取組みに向けて、２００８年度に推進する施策の方向性として、「情報セキュリティ人材の育成・確保に向けた集中的な取組み」、「情報セキュリティ政策の国際展開に向けた集中的な取組み」、「電子政府の情報セキュリティ強化のための総合的取組み」の３本を柱とした２４件の施策を盛り込み、「セキュア・ジャパン２００７」の案を作成しました。

２．「政府機関の情報セキュリティ対策のための統一基準（第２版）」（案）

「政府機関の情報セキュリティ対策のための統一基準」については、政府機関の情報セキュリティ水準を適切に維持していく観点から定期的に見直しを行うこととされています。今般、技術・環境の変化、各府省庁の情報セキュリティ対策の実施状況等を踏まえ、現行の統一基準の改定案を作成しました。

具体的には、最近の事案を検証し、現行の統一基準で対応していない脅威への対策を検討した結果、「情報システムへの IPv6 導入に伴う対策」と「踏み台対策」とを、また 2006 年度の府省庁からの対策実施状況報告を反映し、「情報システム台帳の整備」を、それぞれ新規の項目として盛り込みました。さらに、変更や明

確化などの必要な項目を洗い出し、改訂案を作成しました。

３.「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針」【改定案】
「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針（以下「指針」という。）」については、各重要インフラ分野の情報セキュリティ対策の一層の推進を図る観点から、1 年ごと及び必要に応じて適時見直すこととされています。
見直しに際しては、指針の目的・位置づけ等を踏まえ、「定常的な IT 障害の発生状況の分析」、「相互依存性解析の結果」、「関連文書の検証」、「社会的条件（環境）の変化の検証」の４つのアプローチにより抽出された論点から問題意識を整理し、計１０箇所の改定が必要と判断し、指針の改定案を作成しました。

いずれの案も、NISC のホームページで詳細を見ることができます。皆様から広く意見を募集し、必要な検討を行った上で正式決定する予定です。以上３件のパブリックコメントの締切りは５月２３日ですので、ご興味のある方は、是非ご一読の上、忌憚の無いご意見を頂戴できれば幸いです。

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」

【 プロセスとリソース 】

私のここ１０年程を振り返ると、色々なプロジェクトに巻き込まれた日々だった。関わったプロジェクトには大成功したものもあれば、ぱっとしない結果に終わったものもある。ただ結果とは関係無しに、プロジェクト活動を通して、自分自身の研究領域を超えて多種多様なことを、実際に経験して学べたことが、私にとって大きな財産となっている。

私が学んだことの一つは、運営に責任を持っているのであれば、「段取りをどのように組み立てるか」と「作業をするのに必要なものをどう確保するか」を、常に一緒に考え続けろという教えだ。あるプロジェクトで一緒に仕事した、何十人もの職人さんを率いている社長さんから、現場で何度も口酸っぱく怒鳴られて教えられたことだ。
「先生は気楽に、急げ急げっていうけども、こちとら段取りってもんがあるんだ。働いている職人だって、飯を食わせて休ませな動けなくなるし、機械だって油がいる。足りない資材だって手に入れるには時間がかかる。それをあんた考えていっているんかい？」
こんな事を言われながらも、社長さんと色々と調整しながら前に進めた。衝突したこともあったし、色々と相談したこともあった。この過程は、多くのことを私に教えてくれたのだ。

今、振り返ってみれば、段取り＝プロセスと、必要なもの＝リソースの管理の両方にしっかりと目配せをして作業を進めることを一生懸命考えることの大切さを教えられたと言える。
そして、もう一つ教えられた大事なことは、段取りを決めたり変えたりする時は、仕事に関わる人のコンセンサスをちゃんと取って、納得してから作業をさせてくれということだったと言えよう。

さて、情報セキュリティ関係の施策を組織に導入し根付かせるというプロジェクトを考えてみよう。当然、それまでの仕事の段取りとは違うやり方が沢山導入されるのが普通だ。手続きも変わる。こんな事をやるようにとか、あれをやってはいけないとか、沢山の注文がつけられる。必要となる資源も変わる。特に、人的資源に対する要求が変化することが多い。〇〇の作業をするための人員配置を行えとか、〇〇という装置を普段から利用しろとか、色々な追加的な資源の利用を求められる。さらには、私物パソコンのような利用が曖昧に定義されていた資源の利用禁止を言われることも多い。
情報セキュリティ施策を行うことで「何を実現すべきか」という達成目標設定は、トップダウンで与えられるのが普通だ。しかし、達成プロセス、すなわち「どうやるか」の段取りは、組織毎に作り方をカスタマイズすることが必要だ。このためには、トップは明確に権限委譲を部下に行い、その権限の下で、段取り、つまり業務プロセスの改善に取り組むことを指示すべきだ。同時に、トップは施策実施に必要となる資源（人、モノ、金）を適切に手当することが必須である。権限委譲された部下は、仕事に関わる全ての人たち（ステ

ークホルダ）のコンセンサスを得ることもしなければならない。このプロセスは手を抜くことは絶対にできない。

さらに、必要な資源が手に入らなかったら、その間何をするのかも考え、同時にできる限り早く資源を手に入れる方法も、知恵を絞らなければならない。段取り上手な人でも、資源確保と運用に失敗する状況に陥ることは多々ある。資源管理には、より一層の取組み強化が必要であることは、忘れてはならないことだ。

この段取りと資源の調整を、責任者と現場との間でコンセンサスを取りながら実施し、最終的な目的を達成することが、情報セキュリティ対策でも必要不可欠である。さらに経験的に分かっていることとして、大規模な組織になればなるほど、この作業プロセスを実現する手間が増大する。大きい組織ほど、知恵を絞り、手間を惜しまない取組が必要であることは肝に銘じておくべきである。

（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

【 フォレンジック（forensic） 】

フォレンジックとは、「法廷の」、「科学的犯罪捜査の」を意味する言葉です。情報セキュリティの分野では、「デジタルの世界で法的に有効な証拠情報を確保すること。またそのための手法やツール」という文脈で使われます。コンピュータ・フォレンジックまたはデジタル・フォレンジックと表現されることもあります。

全国の警察が平成１８年中に検挙した不正アクセス禁止法違反に係る不正アクセス行為のうち、その約６割が金銭目的を動機としています。攻撃を受けた被害者にとっては、コンピュータを現状復帰させると同時に、できるだけ詳細な攻撃の証拠を収集し保管しておく必要があります。というのも、自分たちが犯罪の被害者であることのみならず、例えば自社が管理しているサーバが踏み台になって何者かが他者に攻撃を仕掛けた場合には、自分たちが主体的に犯罪に関与してないことを証明する必要があるからです。我が国でも、個人情報保護法が企業に対して個人情報保護義務を課したために、情報漏洩に際して企業の賠償責任が認められやすくなったことなどから、証拠保全に対するニーズは高まっています。

破壊されたログを復元して証拠を検出したり、不正行為の追跡を行ったりするには、高度な技術と知識を要します。デジタル世界のデータは、それが正規の手続きであっても何らかの操作をしたり、時間が経ったりすると、簡単に変化・消失してしまうものが多いということも、証拠性のあるデータ保全の困難さを高めています。さらに収集したデータを分析・統合し、法的に有効な証拠として整理する必要もあります。これらの複雑かつ緊急を要する作業を支援するための、作業の手順およびツール群と、それらを使いこなすための知識などを総称してフォレンジックと呼びます。

4. NISCOLUMN（ニスコラム）

【 安心に繋がる実感を 】

近頃よく耳にする言葉として、「安全・安心な社会」という表現があります。政府の文章でもここ数年よく使用されており、ニュース番組のコメントや選挙の演説などでも頻繁に使われるようになったと感じています。

ところで、「安全」と「安心」は似ているようですが、少しニュアンスの違う言葉ですね。例えば、航空機事故と交通事故を比べたときに、航空機によって死者が出るような事故は随分と少なくなっていますが、それでも航空機に乗るときは正直に言って心配になりませんか。一方、交通事故の発生件数からすれば、自分自身に起こりうる可能性は非常に高いにも関わらず、普段はそれほど気にせずに運転したり、歩行したりしていませんか。航空機による移動は、自動車や歩行による移動よりも結構「安全」であるにもかかわらず、「安心」な方法とは認識されず、一方、自動車や歩行による移動はそれほど「安全」でないにもかかわらず、なぜか「安心」して利用されているように思います。どちらの方法も更に「安全」なものとするために日々努力していくことが重要ですが、では、「安心」かどうかの判断基準はどこにあると思いますか。私は、実感にあるのではないかと考えています。そもそも、鉄のかたまりである航空機が空を飛ぶことはとっても不思議なことですよね。どうして航空機が空を飛ぶことができるのかを十分に理解することが難しく、実感として信用できないことが、「安心」に繋がらない要因なのではないのではないでしょうか。

では、パソコンやインターネットなどの IT 基盤は「安全・安心」でしょうか。まだまだ、「安全」にも「安心」にも至っていない状況と言えるでしょう。「安全」な社会基盤とするために、技術面や普及啓発活動など様々な取組みを行っているところですが、「安心」な基盤として受け入れられていくためには、もう一つ大きな壁があると思っています。いまだに「ITを信用していないから」という言葉をきくことがあります。そして、私自身も少しそう思っています。その言葉の根源にあるのは、技術的に高度になるにつれて、何が起こっているかが見えづらくなることにあると考えています。IT 基盤が一部の特別なものではなく、社会基盤として普及していくためには、「安全」であるだけでなく、「安心」して利用されることが不可欠であり、そのためには、パソコンやインターネットなどで起こっていることについて、わかりやすく説明し、実感に訴えかける努力を行っていくことが必要ではないかと思っています。

（M. K）

【 ここは何処？、わたしは誰？ 】

A「･･･最近なぁ、おれダメダメやねん。すぐ記憶が飛んでまうねん。どぉしよ？」
B「それ飲み過ぎじゃないすか。そのうち、『ここは何処？、わたしは誰？』とか言い出すんじゃないすかぁ。深酒やめた方がいいっすよ。」
C「･･･････」(もぐもぐ、ぐびぐび)
A「そーやなぁ、からだも辛いし、睡眠時間も減るし、ダイエットの大敵やしなぁ･･･。よぉし、深酒禁止やぁ！」
B「そうした方がいいっすよ、まじで。･･･それにしても、C。おまえ、 さっきから食い過ぎちゃうかぁ？」
C「えっ･･･？！」(もぐもぐ. . .)
注） A、B、Cの3名は、実在する人物とは関係ありません。

･･･というような、赤坂の居酒屋！や六本木のバー！！でよく耳にする会話の話ではありません。ましてや、GW中にテレビ放映されていた「ルパン vs 複製人間」のようなクローン人間の話でもありません。

本人確認や認証・証明に関するお話。

実社会において、私たちはいろいろな場面で「自分が自分であること」や「自分がどんな人間であるかということ」を相手に証明し、それによってサービスや便益を受けています。 銀行での口座開設やレンタル CD ショップでの会員登録、クレジットカードの発行手続きなどなど。

そこでよく使われるのが、保険証、運転免許証、住民票、パスポート、社員証といった、いわゆる「身分証明書」ですが、そもそも保険証は社会保険制度に基づき医療費の補助を受けるための被保険者の資格の証明書であり、運転免許証は車やバイクなどの運転の許可を受けているという公文書なのです。したがって、この実社会における本人確認行為は、

（1）必要な手続きにより行われた申請行為に対して、ある機関が審査した結果、発行する「ある特定の目的のため」の証明書を、
（2）発行機関以外のサービス提供者（例えば、銀行やレンタルCDショップ、クレジットカード会社など）が信用し、その内容の確からしさを受け入れることにより成り立っている、

ということができると思います。
（特に政府のような）発行機関自体への信頼性や、その機関の行う審査の厳格性、偽造の困難性などに対して、社会通念上推定される確からしさに基づいて、発行された証明書やそこに書かれている内容を信用するということでしょうか。

今、政府では、「世界一便利で効率的な電子行政」の実現に向け、様々な施策を展開しており、その基盤として電子証明書等を活用した認証基盤の構築・普及を進めています。簡単に言うと、「電子的な身分証明書に基づく行政サービスの実現」と言えるでしょう。
実社会における身分証明書には、有効期間の長短、写真の有無、現住所のみでなく本籍地の記載の有無、世帯の記載の有無、保有者の割合や年齢層など、その発行目的や発行機関により特徴があり、各々の身分証明書は「その本来の目的以外にも活用されているという現実」があります。その身分証明書を電子化することにより、国民の利便性を向上し、行政の効率化を行おうとするわけですが、そもそもの目的や証明している内容、実社会における活用のされ方が違う身分証明書をそのままの枠組みで電子化し、行政や民間のサービスに活用しようとすることに物足りなさを感じるのは私だけでしょうか。
加えて、バーチャルな世界で（コンピュータ・ネットワークを介して）自分が自分であることを証明し、受け入れてもらうことには、証明を受け入れる側にとって、表情や態度、声の調子等による付加的な判断材料がないこともあり、証明の厳格性に対する要求は自然と高くなる傾向にあると思います。

1999 年に故小渕首相のもとで策定されたミレニアムプロジェクトにより本格化した電子行政実現への取組は、昨年策定された「IT新改革戦略」により「ITの恩恵を実感できる社会の実現」に向けて第二フェーズに入ったと言えます。今まさに、ネット社会における身分証明書や認証のあり方を考えるべき時ではないでしょうか。
日本には、長い歴史の中で「証明をするときに印鑑を押す」という、欧米とは違った文化があります。バーチャルな世界において証明を行う仕組みを作るには、ネット社会における慣習や文化、社会制度を新たに構築するという観点から、アーキテクチャ（設計思想や構造）を考え直す必要があるのではないでしょうか。

これは、NISCの仕事なのかもしれません（汗）。ですが、NISCや政府だけでできる仕事でもないような気がしています（ずるい？）。
皆さんも、「ネット社会において、自分が自分であることを証明すること」について、この機会に考えてみてください。そして、私たちと一緒に知恵を出し合って、日本全体として、ネット社会を安全・安心な社会基盤として構築していきましょう。

（2っC）

【NISCロゴマーク制定について】

平成19年4月25日、NISC設置2周年を機に職員からの公募によりNISCのロゴマークを制定しました。
このロゴでは、NISCの使命である「情報セキュリティ政策を描き、行くべき方向を示す。」というイメージを「コンパス」に例えて表現しています。既にNISCのホームページに使われていますので、是非一度ご覧下さい。

http://www.nisc.go.jp/

＜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