NISC NEWS

第２１号（２００８年６月２７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

【 次期基本計画に向けた第1次提言の公表 】

情報セキュリティ政策は、現在、2006年度からの3か年を対象とする「第1次情報セキュリティ基本計画（以下「第1次基本計画」という。）」のもと、取組みが進められています。しかし、取組みが進展する一方で、現実社会においては、ITの活用方法やITに対する脅威・リスクなどの状況が、刻一刻と変わってきています。このため、情報セキュリティ政策会議の下に設置された「基本計画検討委員会（以下「検討委員会」という。）」において、2009年度以降を念頭に置いた次期基本計画（「第2次基本計画」と仮称する。）を策定するための検討が進められています。6月19日に開催された情報セキュリティ政策会議において、第2次基本計画の基本理念など、いわば「総論」に関する検討結果である「第1次提言」が報告されたことから、以下にそのポイントをお伝えします。

●第1次基本計画からの「継続」と「発展」

第1次提言では、第2次基本計画は第1次基本計画の「継続」とともに「発展」の側面を併せ持つべき、とされています。第1次基本計画が重点を置いていた事前予防の取組みに加えて、情報セキュリティ上の問題が万が一現実となった際に備えること（＝「事故前提社会」への対応力強化）、情報資産の重要性とリスクの的確な評価に基づいて、合理性を担保した形で最適な水準の対策を効果的・効率的に実施すること（＝合理性に裏付けられたアプローチの実現）などが、今後のポイントとなります。

●第2次基本計画の基本理念について

第2次基本計画の下での取組みにおいて、我が国のあり方として重要なことは無謬性の追求ではなく、『冷静で迅速な対応、最適な水準の対策の効果的・効率的な実施と説明責任の明確化、主体ごとに求められる最適なセキュリティ水準を達成できる高品質や高信頼性、利用者にとっての安心・安全の確保』という概念です。検討委員会では、こうした概念のもと、より現実に即した実効的な情報セキュリティ対策が冷静に実現される「成熟した情報セキュリティ立国」を目指すべきとの結論を得ました。

そして、成熟した情報セキュリティ立国を実現するためには、ITに係る技術や制度の側面での対策に加えて、社会や国民の意識改革として「ITルネサンス」※が不可欠です。その上で、我々は自国の取組みに自信を持って世界と協調し、IT先進国として相応しいイニシアティブを発揮していくべきと考えられます。

※ITルネサンス：（1）人間が必要以上にセキュリティ問題に振り回されず、むしろ、冷静かつ主体的にITを使いこなせるようになること（＝「ITからの人間性解放」の実現）、（2）結果、最適な水準のセキュリティ対策を実施することで、人間が可能化装置であるITを最大限使って、人間の英知に基づく様々なアイデアの実現が可能化・容易化されること（＝「ITによる人間性解放」の実現）

●次期基本計画の実効性の確保に向けた今後の検討

検討委員会ではこれまで「総論」部分に関する議論が中心でしたが、今後は来年2月の第2次基本計画の決定を目指し、「各論」部分の検討を進めていく予定です。第1次提言は、現在パブリック・コメントにかかっており、頂いたコメントを今後の議論に反映していきたいと考えていますので、皆様からの忌憚のないご意見をお待ちしています。

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」

【 なぜシステム化するのか 】

私の生活には音楽が欠かせない。といってもディープなマニアではなく、いわゆる「ながら族」である。特に、原稿執筆時にはヘッドホンで周りの音をシャットアウトして、アップビートな曲を聞きながらノリノリで原稿を書くのが癖なのだ。音楽があった方が、スランプに陥りにくく、書き続けることができて調子が良いのだ。

音楽を手放さない生活を 20 歳代からしていたら、20 年後の現在、家には 1000 枚を超える音楽 CD がある状況だ。正直なところ、どんな CD を持っているかを正確には把握できていない。これだけの枚数となると、今さら一覧表を作ることは、事実上不可能だ。いつか時間があるときに整理整頓をしようと思っているが、その時間がこれまでやってきたことは無い。

資産管理、特に資産台帳作りは、とてつもないコストが発生する。人手をかけ、十分に工夫をしても、膨大な手間が発生することは避けられない。さらに、完全性を求めた瞬間に、その作業は何倍にも膨れあがる。膨大な作業量を消化するためには、その作業量を、時間的に拡散させるか、人員に分散させるかしか解決方法は無い。すなわち、日々の業務の中で少しずつ片付けていくか、組織構成員の多くを巻き込んで作業をするかしか無いということだ。このどちらの方法でも、一定の作業品質を維持するためには、作業の定形化が必要になる。別の言い方をすると、長期間にわたって、数多くの人たちが並列に作業をする状況で、ある一定の作業品質を確保するために業務をシステム化するのだ。

情報セキュリティ管理では、情報資産や情報処理機器の管理台帳、利用者台帳といったデータベースの構築と運用作業、そして棚卸しなどの保守作業が頻繁に発生する。この時に、資産台帳などをどのように管理するのか、すなわち、誰が情報の追加削除を行い、誰が検証し、どのように完全性を確保するのかということを真剣に考え、設計した手順で作業をしないと、無駄な作業が何度も発生することにもなる。実際、管理台帳の作成や保守の手順設計の段階で手を抜いたことで、手戻りが何度も発生し、結局、管理台帳作成を諦めてしまった事例もある。

上手に管理台帳を作るためには、いくつかのコツがある。

・既存の物品調達や廃棄の手続きの中に、資産台帳への登録や削除が行われる手続きを組み入れる。
・誰もが理解し、実行できる作業プロセスとし、必ずマニュアルを作る。
・最初は完全性を求めず、多くの人たちが新しいシステムに慣れることを目標とする。
・どの時点まで遡及するのかは作業量と相談する。どんな資産でも、何年も、何十年も保有し運用するものはわずかだ。

現実的に使い続けられるかどうかを念頭に、システムを設計して欲しい。関係者が我慢ならないシステムは、絶対に使われないシステムになってしまうのだから。

（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

【 IEEE 802.1X 】

重要な情報の漏洩を防ぐために、情報持ち出しの制限や USB メモリやノートパソコンの HDD の暗号化などの対策を取っている組織も多いでしょう。しかし、もし悪意を持った者がオフィスの中に入り込み、組織内のネットワークに接続できてしまったら、意外と簡単に情報が盗まれてしまうのではないでしょうか？ 特に無線 LAN を使っているオフィスでは、建物の外からでも容易に組織内 LAN に接続できてしまうケースすらあります。

IEEE 802.1X は、端末を認証してから LAN に接続させるための技術です。IEEE 802.1X に対応した LAN スイッチや無線 LAN のアクセス・ポイントを使用することにより、不正なユーザの LAN への侵入を防ぐことができるようになります。802.1X 認証を行なうためには、サプリカント、認証装置、そして認証サーバの3つの要素が必要となります。それぞれの要素に関して、以下に簡単に解説しましょう。

・サプリカント

端末に搭載される、認証を行うクライアント・ソフトのことです。サプリカントがユーザ情報を認証装置とやり取りすることで、LAN への接続が可能となります。 Windows2000（SP4 以降）や WindowsXP（SP1 以降）、Mac OS X などには標準でサプリカントが付属しています。

・認証装置

IEEE802.1X に対応した LAN スイッチや無線 LAN アクセス・ポイントが、これに相当します。サプリカントから受信したユーザ情報を認証サーバへ転送し、認証サーバでの判断結果に応じて、端末からのフレームを通すか否かを制御します。別名、オーセンティケータとも呼ばれます。

・認証サーバ

ユーザ情報を集中管理しているサーバです。認証装置から受け取ったユーザ情報に基づいて、接続の可否を判定します。 この認証装置との間の通信には、RADIUS というプロトコルが用いられています。

最近は、IEEE802.1X に対応したネットワーク機器も安価になってきているので、オフィスの LAN 環境を見直す機会があれば、導入を検討されることをお勧めします。

4. NISCOLUMN（ニスコラム）

【 情報セキュリティと外来語 】

私たちは、情報処理や情報セキュリティについて書いたり話したりするときに、多くの外来語を使います。「パソコン」や「データ」が広く通用し、「ソフトウェア」や「コンピュータウイルス」も一般紙やテレビの報道で使われています。この分野でも外来語は欠かせないものになっており、物ごとや概念、意志を伝えるために必要である限り、外来語の使用を前向きに考えたいと思います。

その一方で、「セキュアなシステムを構築する」、あるいは「情報をセットする」という表現は、どこか違和感があります。「ポリシーをリアルタイムにアップデートする」という例を見ると、度が過ぎていないかと思います。

外来語を使うことについて、その可否や適否にいくつかの観点があります。

第一に、必要性です。新しいものや概念を表すために使える既存の語が無ければ、外来語も選択肢に入ります。

第二に、場の考慮です。業界や専門家集団の中であれば、外国語の専門用語を導入する必要性が高く、また、受け入れられる傾向にあるのではないでしょうか。しかし、集団の外の人に対しては、未熟な外来語は不適切かもしれない、という配慮が大切です。

最後に、美しさの観点です。人それぞれの意見があると思いますが、私は、文章中に外来語が多すぎないよう

にしたいと思います。漢字の凝縮した表現が好きだからです。また、動詞として外来語を使わないようにしています。名詞の外来語は、安定感を得やすいようです。

前掲の例は、「安全なシステムを構築する」、「情報を設定する」、「ポリシーを逐次更新する」とします。

外来語の現状と言い換えについては、国立国語研究所の研究成果がウェブに掲載されていています。

○「外来語」言い換え提案 第1回～第4回総集編 （平成 18 年 3 月）

http://www.kokken.go.jp/gairaigo/index.html

この言い換え提案から、情報処理や情報セキュリティに関するものをいくつか取り出してみました。それぞれの外来語に対して、その他の言い換え語の案も示されているのですが、ここでは省略しています。

外来語	言い換え語
アクセシビリティー	利用しやすさ
インタラクティブ	双方向的
コンテンツ	情報内容
セキュリティー	安全
デジタルデバイド	情報格差
バーチャル	仮想
フィルタリング	選別

自身でも採用するかどうかはともかく、この提案を見ると、外来語によらない表現の可能性を感じ取ることができます。皆様はどのような感想をお持ちでしょうか。

（S.Y.）

＜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