NISC NEWS

第６号（２００６年１１月７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

【「政府機関統一基準適用個別マニュアル群」ってナニ？】

2005 年 12 月 13 日の情報セキュリティ政策会議において、各府省庁が遵守すべきセキュリティ対策事項を明記した「政府機関の情報セキュリティ対策のための統一基準（2005 年 12 月版（全体版初版））」（以下、政府機関統一基準という）が策定されました。政府機関の情報セキュリティ対策は、各府省庁が自らの責任において対策を講じていくことが原則ですが、政府機関統一基準は各府省庁の情報セキュリティ対策の強化・整合化を支援し、政府全体の情報セキュリティ水準の向上を図るための枠組みとなります。各府省庁は、政府機関統一基準を踏まえ、自らの情報セキュリティポリシーの見直しを行い、政府機関全体として整合性のある情報セキュリティ対策に取り組んでいます。

情報セキュリティポリシーによって、各府省庁における情報セキュリティ対策の基本スタンスが組織内に表明されます。この際、実際に職員一人ひとりが情報セキュリティ対策をきちんと実行していくためには、情報システムや業務に対して、どのような手順に従って対策を推進するかを具体的に定めた実施手順（規程、マニュアルなど）が必要となります。しかし、各府省庁では情報セキュリティに関する知識の豊富な人材が不足しているという課題があり、各府省庁がそれぞれ一から実施手順を作成するのは容易ではありませんでした。そこで、内閣官房情報セキュリティセンターに専門家を配置して知見と情報を集め、実施手順を作成する際に参考となる手引書や雛形を、各府省庁と協力して作成し提供することにしました。これらのマニュアルを「政府機関統一基準適用マニュアル群」と呼んでいます。

本マニュアル群は、各府省庁の情報セキュリティ担当部門やシステム管理部門の担当者が、政府機関統一基準で求められている事項を満たす手順書を作成する際に、盛り込むべき事項や手直しのポイントを挙げ、一部には雛形も付けています。また、解説資料としても活用することもできます。各マニュアルを大きく分けると、以下のように分類されています。

- DM2：組織・体制について
  （自己点検、情報セキュリティ監査、違反報告、例外措置など）
- DM3：情報の取扱いについて
  （情報の格付け、情報取扱手順など）
- DM4：情報システムの情報セキュリティ要件について
- DM5：情報システムの構成要素について
  （ウェブサーバ、モバイルPC、電子メール、ウェブブラウザなど）
- DM6：個別事項について
  （機器等の購入、外部委託、ソフトウェア開発など）

なお、表内のDM[数字]は、各マニュアルの文書番号（DM[数字]－XX－XXX）の冒頭を示しています。

本マニュアル群は、新たな脅威の発生や各府省庁における運用の実態等を踏まえて、適時見直していきたいと考えています。また、本マニュアル群は、政府機関以外の皆様にもご活用いただけるよう、下記のWebページ（http://www.nisc.go.jp/active/general/kijun_man.html）に掲載していますので、是非一度ご覧下さい。

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」

【見えないものをみる】

情報システムの管理作業では、どのようにシステムが使われているかを把握することが必要だということは、どんな管理者も分かっていることだ。しかしながら、実態を本当に把握しようとすると、数多くの壁に突き当たる。

現在の情報システムの作り方は、分散型システムが基本である。機能を集約した単一のシステムに端末からアクセスする形態は年々少なくなり、情報処理の一部を自前で行う高機能なユーザ側システム（例えばデスクトップPC）と、サービスを提供するサーバ群とから構成されることが多い。さらには、サーバ群もクラスタ化していたりすることもある。このためシステム利用実態を把握するにしても、観測データとして収集すべきものが爆発的に増加している。そしてシステム間の相互関係を正しく理解して、解析する作業が必要となる。

以前このコラムでシステム構築時には「観測系」を上手く作ることが必須だと述べた。その観測系が構築できている上でさらに必要になってくるのが、観測データを解析する力である。時々刻々収集される観測データを単純に眺めているだけで分かるものも数多くある。管理作業に役立つものも多いだろう。しかし、複数の観測データを突合せて、初めてそこから浮き彫りにされる実態も少なくない。これを知るには、たとえば、システム利用では「全体の1割の利用者が、全体の9割のリソースを消費している」という経験則があるが、これは分散型システムになったときにも引き続き事実であろうか。あるいは、利用者の行動はパターン化されるケースが多く、そこから逸脱した行動した時には、セキュリティ上のリスクを抱えた状態にあることが多い、という経験則もあるが、これは本当だろうか。こういった数多くの仮説をたてた上で、データを関連づけて解析することで、単純には見えてこないシステムの実態を「みる」作業が大切だ。そして、これは高度な経験やノウハウが要求される作業である。システムが大規模化し、複雑化し、業務の多くがシステム上で行われるようになればなるほど、利用実態把握のための解析作業が重要になる。このための人員確保、教育、資源割り当てについて、経営者は怯むことなく取り組むことが必要である。

（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

【CP/CPS（証明書ポリシー／認証局運用規定）】

最近では電子証明書がかなり普及して、一般的な技術となってきました。この証明書を発行しているのが認証局ですが、その運用において、発行する証明書の利用目的を定める証明書ポリシー（CP：Certificate Policy）や、認証局運用規定（CPS：Certification Practice Statement）と呼ばれるドキュメントがあるのをご存知でしょうか。これらの文書に関するガイドラインは IETF の RFC 3647 に示されており、個々の認証局の運用形態にあわせて適切なものが作成されます。CP/CPS で規定されるのは、証明書のフォーマットや証明書の発行・失効の手順だけではありません。例えば、認証局システムが設置されている環境の物理的なセキュリティ条件や、認証局が正しく運営されているかどうかをチェックする監査の実施に関する条件、さらには認証局運用に関する責任や責務にまで及んでいます。

証明書は数学的にその強度が保証されたものですが、これに CP/CPS が加わることによって、運用の観点からも客観的に信頼性レベルが確認できるようになります。CP/CPS を作成し公開することは認証局の運用にあたって必須のものではありませんが、Web 上で一般に閲覧できるものも多数あります。今、あなたのお使いになっている証明書がどのようなルールの下で発行されたものなのか、確認してみるのも一興ではないでしょうか。

4. 情報セキュリティQ

マルウェア（malware）という言葉をご存知でしょうか？ ウィルスやワーム、トロイの木馬などの不正なプログラムの総称です。「mal-」は「悪い」という意味を持つ接頭辞であり、これとソフトウェアを意味する“ware”を繋げて作られた造語です。攻撃者は、あの手この手で、あなたのパソコンにマルウェアを送り込もうとしており、その手口は近年ますます多様化・巧妙化しつつあります。

それでは、現時点で考えた場合、以下のソフトウェアやデバイスのうち、それを利用したり、接続したりしても、パソコンにマルウェアを送り込まれる心配をする必要がないものは、どれでしょうか？

① IM（インスタント・メッセージ） ② 携帯用ゲーム機 ③ ファイル共有システム
④ 携帯音楽プレーヤー ⑤ ①～④のどれにも危険性がある

（なお正解は次号にて掲載致します。）

【前号の答え】

前号の問題は「Code Red ウィルスの語源は何か？」でした。正解は「② 解析者の好きな飲み物」です。

「Code Red」の発生時、あるセキュリティ関連会社の２人の社員がこのウィルスの解析作業中に、よく飲んでいたのが「マウンテンデュー・コードレッド（Mountain Dew CODE RED）」だったため、ここから「コードレッド（Code Red）」という名称がついたと言われています（因みに、この飲み物は、チェリー味の炭酸飲料とのこと）。ペプシ社は、自社の製品の名前を有名にしてくれたこの２人に、コードレッドを5ケースずつプレゼントしたそうです。

命名自体にあまり時間がかけられないから、というのが理由なのかもしれませんが、やはり解析作業は炭酸だけに「気が抜けない」等という裏の意味もあったのか否かは定かではありません。

5. NISCOLUMN（ニスコラム）

【誰でも安全にITを活用できるように】

わたしの父は昭和9年生まれで今年で72歳です。昔から写真を趣味としています。最近は仕事の合間を縫ってライカの単眼カメラやポジフィルムのカメラを使って全国の祭りや桜、紅葉を撮っています。そんな父が最近デジタルカメラを購入しました。さて、これがことの始まりです。デジタルカメラはフィルムを気にせずにたくさんの写真を撮ることができます。連写も容易にできます。これは便利です。ところが、撮った写真をより鮮明に見ようと思えば、パソコンに接続しなければなりません。家には仕事で使っているパソコンがありますが、今まで父はパソコンに近づくことさえしていなかったようです。しかし、「撮ってきた写真がどうしても見たい」と、いうことで、ついに一念発起してパソコンを使うことになりました。

カメラの画像データをパソコンに取り込んで、スライドショーで内容を確認したり、色調を変えたりと結構楽しんでいます。パソコンを使い始めたときは、ダブルクリックもままならなかったのですが、最近ではかなりなれて「カチカチ」とパソコンを駆使して撮ってきた写真を楽しんでおります。

そんな父を見ていてふっと、「最新のセキュリティパッチがあたっていることを確認しなければならない」、「ウイルス対策ソフトのパターンファイルが最新であるかを確認しなければならない」という、セキュリティ業界では常識といわれることが果たして理解した上でできるのかなぁ・・・と思いました。

創刊号のニスコラム「知る人ぞ知るセキュリティ」では*「情報セキュリティとは「知る人ぞ知る」ものであると感じるのは筆者だけではないと思います。誰もが、ある程度得心して自発的に対策をすることが望ましいのならば、国民に対し、もっと理解しやすい言葉で「情報セキュリティ」を解説していくことが、内閣官房情報セキュリティセンターの責務だと感じている今日この頃です。」*と結ばれています。言葉の問題だけでなく、製品やサービスにも問題があるのではないだろうか、脆弱性やウイルスを気にせずにパソコンが使える環境をみんなで作っていくことはできないものなのだろうかと思いました。ネットワーク環境が全世界的に良くなってくると案外早く実現するかもしれませんね。でもそんな時代がきたら、内閣官房情報セキュリティセンターはなくなっているかもしれませんね。それはそれでいいか・・・。

（まるちゃん）

＜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