NISC NEWS

第７号（２００６年１２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

「人は城、人は石垣、人は堀」

【 人材育成･資格制度体系化専門委員会報告書(案)のパブリックコメントの募集 】

１．「人は城、人は石垣、人は堀」⇒「人はファイアーウォール、・・・」になるか？

「人は城、人は石垣、人は堀」。これは戦国時代の名将、甲斐の虎こと武田信玄が遺したと伝えられている言葉です。その意味には諸説ありますが、一般的には「乱世の戦国時代にあって国を守っていくには、優れた人材を育成・確保することが最も肝要」という信玄の考えを表していると言われています。

「守る」という意味では、概念的に共通している「情報セキュリティ」についても、同じことが言えるのではないのでしょうか。特に、近年頻発している情報漏洩や、重要システムにおけるＩＴ障害などに関する報道を見ると、情報を扱う人やシステムを構築・運用などをする人の問題が、このような事件を引き起こす主な（ほとんど全部？）要因となっていることが多いようです。ＩＴが氾濫する今の世の中にあっても、人材をしっかり育成していけば、情報を守るための心強い布陣が引けるのではないでしょうか。さしずめ、「人はファイアーウォール、人はアンチウイルスソフト、人はＩＤＳ※」といったところでしょうか。

そこで、今年の夏から秋にかけて、情報セキュリティ政策会議の下に「人材育成・資格制度体系化専門委員会」を設け、情報セキュリティに係る人材の育成について討議してきました。先日、この委員会の検討の成果である報告書の案が公表されましたので、そのポイントを紹介します。

※ＩＤＳ（Intrusion Detection System）：システムに対する不正な侵入を検知するシステムのこと。

２．報告書案のポイント

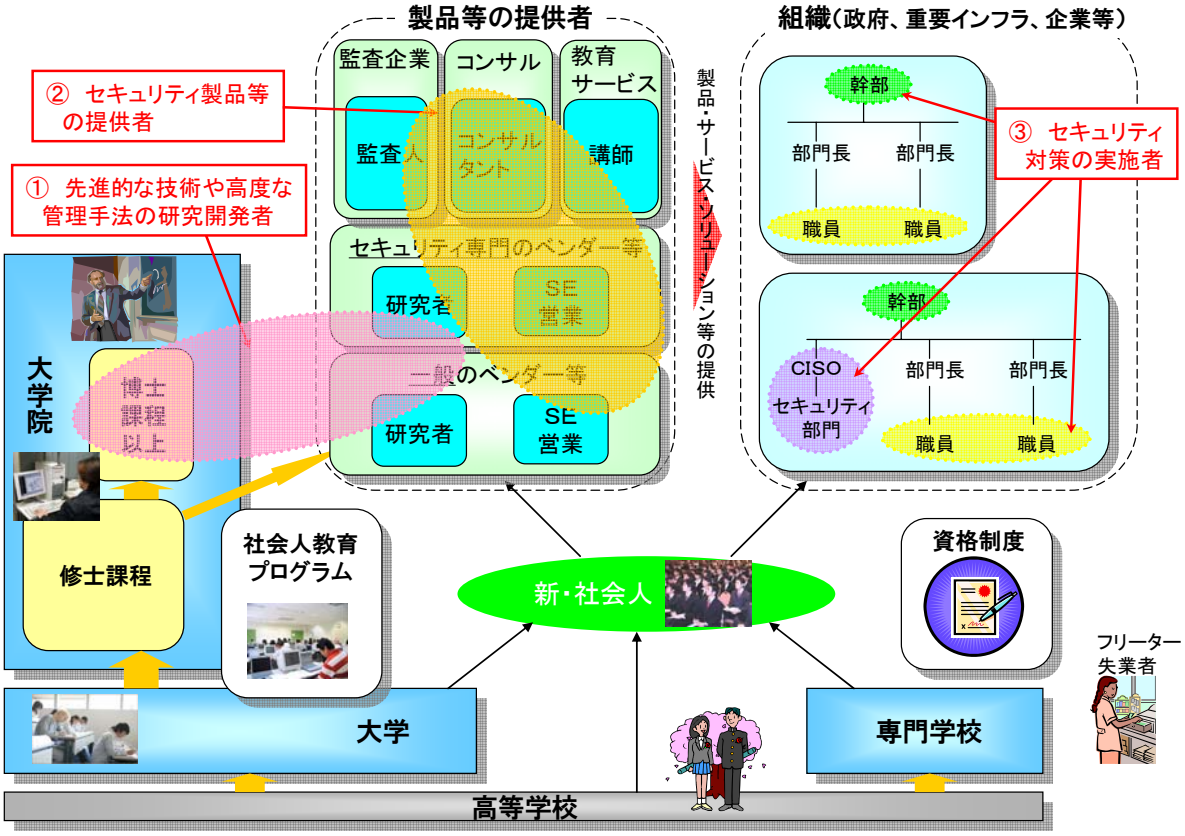
（１）情報セキュリティに係る人材って？

情報セキュリティに係る人材といった場合、皆さんはどのような人達を想像されるのでしょうか。会社にいるパソコン担当の人、アンチウイルスソフトを扱っている人・・・、色々な人を想像するかもしれませんが、この委員会では、社会経済活動の中で情報技術に触れる人であれば、全て含めることとされています。なぜなら、あなたが自宅でネットサーフィンと電子メールのためにしかパソコンを使っていなくとも、その

パソコンがコンピュータウイルスに感染し、さらにウイルスを撒き散らせば、他の人に迷惑をかけてしまいますし、サイバー攻撃の踏み台にされれば、ＩＴ障害を引き起こす要因にもなりえます。情報セキュリティを確保するためには、業務で情報技術に触れる人のみならず、全ての人達に情報セキュリティに関する知識や能力が求められるのです。

とはいえ、全ての人が同程度の知識や能力を身に付ける必要はありません。例えば、ある企業における一般社員と情報セキュリティ対策の実施を担当する社員とでは、求められるものは自ずと違ってきます。また一言でベンダーにおける開発者といっても、開発するものが一般の情報システムなのか、あるいは情報セキュリティ製品なのかで差が生じるのは当然です。その役割に応じた知識や能力が必要となるのです。そこで、委員会では、情報セキュリティに係る人材を大きく３つのカテゴリに分けて検討を進めました。

報告書案の検討におけるカテゴリ分類のイメージ



（２）どんな人材育成方策が書いてあるの？

報告書案に挙げられている人材育成方策のうちいくつかをピックアップします。

① ベンダー等における人材育成方策

セキュリティ製品等を提供するベンダー等の技術者が情報セキュリティについての能力を身につけなければならないことは当然ですが、報告書案では、セキュリティを専門としない一般のベンダー等の技術者でも、製品を製造・提供するにあたっての最低限のセキュリティに関する最低限の能力が必要であり、その方策について検討する必要があるとしています。さらに、フィールド・サービス・エンジニアの役割についても触れ、フィールド・サービス・エンジニアの情報セキュリティ能力の向上を図ることにより、顧客の情報セキュリティ対策の向上に繋がるとしています。

これらのことを踏まえ、情報セキュリティを専門とするベンダー等、一般のベンダー等、オフィス機器ベンダー等において、各種教育プログラムの活用を通じた計画的な人材の育成を図ることを期待するとともに、高等教育機関における社会人向け教育プログラムの充実・発展や連携の促進を提案しています。

② 政府機関における人材育成方策

政府機関については、実態調査を実施し、この結果に基づいて検討を進めました。アンケート結果から、政府機関では情報セキュリティに係る人材が不足しているにもかかわらず、具体的な育成・確保のための戦略が立てられず、日々の OJT のみが能力の向上のための取組みであるという現状がわかりました。

そのため、政府機関おいては、まず、政府統一的な教育プログラムの整備を行うことを提案しています。この教育プログラムは、一般職員向けの「セキュリティリテラシー教育プログラム」、幹部向けの「リスクマネジメント教育プログラム」、セキュリティ担当者向けの「情報セキュリティ担当者教育プログラム」の３点セットになっています。

③ 一般の企業における人材育成方策

一般の企業については、日本経済団体連合会「情報通信委員会」所属の企業に対してアンケートを実施し、この結果に基づいて検討を進めました。アンケート対象は我が国の企業の中でも比較的情報セキュリティ対策が進んでいると考えられる企業であるにもかかわらず、情報セキュリティに関する資格制度や各種教育プログラムについての意識が低く、基本的に OJT による能力の確保が一般的になっていることがうかがえました。

そこで、一般企業においても、一般社員に対してセキュリティリテラシーを習得できるようなプログラムを設定することと、幹部に対して情報セキュリティのリスクを認識・理解させるための教育を行うこととを提案するとともに、情報セキュリティ担当者については、各種の外部教育プログラムを活用しながら計画的な育成計画を策定することを提案しています。

④ 各種教育プログラムに関する体系図

情報セキュリティに関する人材の育成計画を立てるための目安として、情報セキュリティに係る人材のカテゴリごとに、必要とされる能力とその能力の取得等に役立つと考えられる各種教育プログラム（高等教育機関、社会人実践プログラム、資格制度等）について整理した体系図を作成しました。

３．パブリックコメントの募集

この報告書案は１１月３０日に公表され、１２月２８日までの間パブリックコメントを募集しております。このメールマガジンを読んで興味をお持ちになられた方は、是非下記ＵＲＬをご覧になって、ご意見をお寄せ下さい。

http://www.nisc.go.jp/active/kihon/training.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」

【 トラブルはあなたの力を試す時だ 】

当たり前のことだが、自分が管理運用している環境でトラブルが発生することは、できれば勘弁願いたいことだ。しかし、私たちが好むと好まざるとにかかわらず、トラブルはいつかやってくる。そして、トラブルは、私たちの管理運用の出来の良さ悪さを、冷酷に白日の下に晒すのだ。だからこそ、管理運用の設計・実装では、トラブルにどう対応するのかを真剣に考えることが必要になる。

トラブルにうまく対応できるようになるには、幾つものメカニズムを用意しておかなければならない。まず、日頃の準備が大切だ。そもそもトラブルを発生させないように、技術、管理、ルール、人的資源、予算などの観点から合理性をもった取組みを行うことが大切だ。どんなリスクが存在しているのか、そしてどの

ように対応するのかを考えて、実装するのだ。

本当にトラブルが発生したことをどのように知るのか、認知の機構も作る必要がある。特に情報セキュリティ関係のトラブルでは、発生を認知しにくいものも数多くある。トラブルの発生を知るためのメカニズムも開発し改良を続けることを行わなければならない。

そして、実際にトラブルが発生してしまった場合には、まずは緊急対応をどのように行うか。そしてトラブルの被害範囲を同定でき、トラブルを制御下に置くことができるようになれば、今度は復旧作業を効率的に行うことに努力しなければならないだろう。

ここに示した日頃の準備、トラブル認知機構の実装と運用、緊急対応、そして復旧作業は、それぞれ、その内容を設計する方法も、実施する方法も、上手に処理するテクニックも異なる。多くの英知を結集し、アイディアをまとめ、その有効性を検証することも大切であるし、実際に時間との戦いの中で作業をすることが求められる場合もある。このようなことから、トラブル対応は、まさにあなたの真の力が試される時だ。情報セキュリティ管理では、かならずトラブル対応を設計実装しなければならない。

しかし、実際にトラブルが発生してみると、意外とトラブル対応に真摯に取り組んでなかったことが露呈することが多い。どうも理由無き自信、「おれが管理運用している間は、大きなトラブルなんかないはずだ」という自信をもつ人が多いようだ。もっと小心者になろう。「思いも寄らぬ事」という言い訳をする人も多い。もっと感性と知性を働かせよう。そして、あなたの力を１００%発揮できるようにしておくことが大切だ。

（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

【 フィッシング(phishing)詐欺 】

フィッシングは最近被害が増えている、手の込んだオンライン詐欺の手口です。"phishing"とつづるのは、被害者を「釣り上げる」という"fishing"という単語に、「洗練された」という意味の"sophisticated"を組み合わせた造語であるとの説が有力です。

具体的には、銀行やクレジットカード会社、あるいはオンラインショッピング・サイトなどの名前を騙って、ユーザに「セキュリティ強化のためユーザ情報の確認を行っています。http://xxxx/にて、IDとパスワードを入力してください」というような内容のメールを送りつけ、本物のサイトに似せたデザインの偽のサイトへ誘導します。そして、ユーザがIDやパスワードを入力してしまうと、不正にお金を引き下ろされてしまったり、詐欺に悪用されたりするなどの被害に遭ってしまうのです。

正規のWebサイトを運営する側も、例えば専用のトークン（パスワード生成器）を利用して時間とともにパスワードを変化させる仕組みなどを導入したり、セキュリティ対策ソフトベンダもフィッシング・サイトを検出する機能を追加したりするなどの改善がなされています。しかし、詐欺の手法や技術は日々進化しており、例えば端末に不正プログラムを仕込み、ブラウザのアドレス欄などに表示されるURLを偽装したり、正しいURLを入力しても偽のサイトに接続させようとしたりする手口も確認されています。

結局、今のところフィッシング詐欺を回避するには、疑わしいメールを見分ける目を養い、メールの指示に安易に従わないこと、そのためにはユーザの不断の注意が一番大切ということになります。当該のサイトにアクセスしたい場合には、メールに書かれているリンクをそのままクリックするのではなく、検索エンジンで調べるか、ブックマークを利用する習慣をつけましょう。もし、何か変だなと思いつつも判断がつかない場合には、電話やFAXで確認してみるなどの慎重な対処が必要です。

4. 情報セキュリティQ

ボット（bot）は、ユーザの気付かないうちにパソコンにインストールされ、犯罪者の指令によって動くプログラムのことです。その動作がロボットに似ているところから、ボットと呼ばれています。指令者は大量のボットを束ねてボットネットと呼ばれるクラスタを作り、迷惑メールを大量に送りつけたり、標的のシステムに一斉に攻撃を仕掛ける DDoS（Distributed Denial of Service）攻撃でサービスを利用不能にしたりします。また、狙いをつけた企業内の中にボットネットを作り上げて機密情報を盗むなど、ボットネットは様々な犯罪のインフラとして使われています。

さて、ここで問題です。日本国内のパソコンの何台に１台がボットに感染していて、その総数は何台ぐらい存在すると言われているでしょうか？

１． 40 台に１台　（総数は約 50 万台）
２． 100 台に１台　（総数は約 20 万台）
３． 500 台に１台　（総数は約４万台）

（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「マルウェアを送り込まれる心配のないソフトウェアやデバイスは、どれ？」でした。
正解は「⑤ ①～④のどれも危険性がある」です。

マルウェアは、電子メールの添付ファイルを実行することで感染するものがずば抜けて多く、メール本文のリンク先のサイトから感染するものが、それに続きます。近年、IM（インスタント・メッセージ）でも悪意のある Web サイトへの URL をメッセージ中に表示するという手口も広まっており、注意が必要です。

現在のようにネットが普及する前には、ファイルに感染したウィルスをフロッピー・ディスクなどの記録メディアを通じて伝播させる手法が最も一般的でした。今となっては牧歌的とも思えるこの方法も、ファイル共有システムによって、いまだに生き残っています。それどころか、大容量のフラッシュメモリやハード・ディスク装置を内蔵した、携帯音楽プレーヤーや携帯用ゲーム機に、このタイプのマルウェアが感染したケースも既に報告されており、かつての流行がリバイバルしはじめている印象さえあります。

このように感染経路が多様化し、新しい手口も次々に出てくることから、セキュリティ対策に不安を抱かれることもあるかもしれませんが、何事も基本を守り、常識的な判断を行えば、ほとんどの危険は回避できます。「出所が不明なファイルを貰ったり、実行したりしない」、「信頼できない Web サイトにはアクセスしない」、「ウィルス対策ソフトを利用し、常に最新の定義ファイルに更新する」「OS やアプリケーションのパッチ（更新プログラム）を当てて、セキュリティホールをふさぐ」という、セキュリティ対策の基本を常に遵守しましょう。

5. NISCOLUMN（ニスコラム）

【 情報セキュリティ ＝ CIAの再確認 】

情報セキュリティとは、情報の Confidentiality（機密性、以下、Ｃという）、Integrity（完全性、以下、Ｉという）、Availability（可用性、以下、Ａという）を守ることであると言われて約２０年が経っている。他の項目を追加する例も出てきているが、これらが基本３項目であることは昔も今も変わりないだろう。しかし、各々の性質や特に互いのバランスについては、２０年前と今とが同じとは限らない。

ＣとＩとＡによって情報セキュリティ対策を考察することが定着したのは、１９８０年代に米国国防総省が定めた TCSEC という調達仕様においてであり、これは後に ISO/IEC 15408(JIS X 5070)となる。国防の情報システムを想定していたためか、機密情報に無許可でアクセスされないようにするＣについては相当の対策を求めているが、アクセスできなくならないようにするＡについては、それ程でもない。不正な書き換えがないようにするＩにも配慮しているが、機密情報へのアクセス記録を保全することに注意を払っている。

軍事機密情報が漏洩するくらいであれば、自らその情報を破壊するというのは映画などで目にするところである。米国の国防では、ＩやＡについては、その手法そのものが機密である場合もあるだろう。情報をわざと不正確にすることや、攻撃者が特定できれば防御だけではなく、攻撃している情報システムを不能にすることも考えられなくはない。その意味でも、あえて優先度を付けるとすると、Ｃ＞＞Ｉ＞Ａという順番で、情報セキュリティを検討していたように思われる。

その一方で、情報システムを民間が使用するようになった現在で考えてみると、この優先度はいささか現実に合わない場面もある。例えば、企業の新製品の機密情報について、それが競合他社に漏洩するくらいならば原本まで消去して情報を守るということは日常的なことではなさそうである。国防以外の分野での情報セキュリティの優先度は、Ａ＞Ｉ＞Ｃと考えた方が整理できやすい場合も少なくない。

このことは政府にとっても同じだ。秘密とすべき情報の漏洩は防がなければならないが、それに加えてＩやＡを軽視できない情報も多く保有している。Ｃだけに偏った対策とならないように、ＣとＩとＡのバランスを十分意識しながら全体像を設計していく必要がある。例えば、Ｃのためにデータの暗号化は重要だが、その暗号鍵の喪失は、データの喪失を招くことになり、それに備えた環境整備が先決だ。またデータの不用意な持ち出しは禁止されなければならないが、行政事務サービスとして求められている場合には必要な対策を講じて持ち出すことにも備えなければならない。Ｃだけに偏って本末転倒してはならない。情報システムは、情報を安全に活用するためにあるのだから。

今や情報システムは補助的なものではなく企業や政府のサービス提供に不可欠のものとなっている。そのような変化の中で、ＩとＡにも配慮してＣについても怠らないような情報セキュリティ対策を検討する時期に来ている。２０年前の考え方の一部の見直しも含めて、産官学の連携の下に情報セキュリティ対策の第２章を切り開かなければならない。

（すいとんろう）

＜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