NISC NEWS

第１２号（２００７年７月９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

【「セキュア・ジャパン2007」の正式決定 】

前号の本項において、「政策会議決定案３件に関するパブリックコメント募集」の内容をご紹介しました。これらの募集に対して、多くの方々から様々なコメントをいただき、厚く御礼を申し上げます。頂戴したパブリックコメントについては、政策会議の事務局である内閣官房情報セキュリティセンター（ＮＩＳＣ）において精査の上、対応案を策定し、第１２回情報セキュリティ政策会議にて正式決定したことを、ご報告します。

今号では、これらの決定のうち、本年度の具体的な施策の実施プログラムである「セキュア・ジャパン２００７」に掲載されている代表的な施策をご紹介いたします。

「セキュア・ジャパン２００７」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、「第１次情報セキュリティ基本計画」の達成に向けた２年目の取組みをまとめた本年度の実施プログラムです。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た対策推進の安定化を図るために、２００７年度に実施する具体的行動計画と、２００８年度の重点施策の方向性を示しました。

①「２００７年度の実施計画」
基本計画に掲げた目的を達成するために、3か年計画の２年目である２００７年度においては、「官民における情報セキュリティ対策の底上げ」を重点として１５９の具体的施策を推進します。主な具体策としては、「政府機関情報セキュリティ対策の拡充」、「広く国民も含めて対策が遅れがちな主体の対策の普及」が挙げられます。

②「２００８年度の重点施策の方向性」
２００７年度までの施策を持続するとともに、取組みを一層加速化すべく、「情報セキュリティ基盤の強化に向けた集中的な取組み」を重点として、２００８年度に推進する施策の方向性として、２４の施策の方向性を提示しています。主な具体策としては、「情報セキュリティ基盤強化に向けた集中的な取組み」が挙げられます。

今後、内閣官房及び各府省庁は、「セキュア・ジャパン２００７」に基づき、情報セキュリティに係る具体的施策を実施していきます。また、ＮＩＳＣとしては、２００７年度に以下のような施策を推進していく予定です。

① 政府機関については、「政府機関統一基準」に基づくＰＤＣＡサイクルの定着化及び対策実施状況等の報告を受け、必要な対策を促していくほか、２００８年度における本格運用に向け、政府横断的な情報収集、攻撃等の分析・解析、各政府機関への助言、各政府機関の相互連携促進及び情報共有を行うための体制（Government Security Operation Coordination team（ＧＳＯＣ））を整備します。
② 重要インフラについては、「安全基準等」の定期的見直しや更なる情報共有体制の整備などを通じて、情報セキュリティ対策の向上を図っていきます。
③ 企業・個人については、「情報セキュリティの日」の実施や多種多様な広報啓発・情報発信など、情報セキュリティ対策の普及・啓発に繋がる施策を積極的に実施します。
④ 情報セキュリティ政策の評価のあり方の基本方針として本年２月に決定された「『セキュア・ジャパン』の実現に向けた取組みの評価等及び合理性を持った持続的改善の推進について」等に基づき、ＮＩＳＣにおいてこれらの評価等を実施してまいります。

2. 補佐官ノート

【 次世代（？）の情報セキュリティ脅威 】

○ 真夜中の訪問者

とあるオフィスに、ビデオ会議専用システムがある。このシステム、普段は電源が入っていないはずなのだが、ディスプレイとスピーカーをテレビと共用しているので、会議直後にテレビ側に切り替えたりすると、電源が入りっぱなしの状態になっていることがよくある。

先日、何かの拍子に、このシステムの通話履歴を見てみたら、身に覚えのない通話の着信がときどき記録されている。なんじゃこれは？と思っていたら、先日ついに現場に出くわした。深夜に突然着信し、数分間にわたって無言・無映像通話を続けてから切るところに遭遇したのである。履歴に残った発信アドレスは、やはり身に覚えがないもので、何かの間違いなのかも知れないが、ビデオ会議用の通信プロトコルはある程度複雑なものなので、単純なスキャンパケットを投げ付けられただけでは着信しない。意図的にこちらの様子を探っていたのかも知れない。会議でもしていたら、会話も映像も筒抜けになってしまっただろう。

その夜は、そういう通話が合計で３回あった。電源を切っておけば問題ないのだが、今までの経緯から切り忘れることも必ずあるということで、カメラ用に跳ね上げ式の目隠しデバイスを作ろうと思い、クリーニングから帰ってきたYシャツの芯に入っていたボール紙を切り抜きながら考えた。

○ 古くて新しいマルチメディアな情報漏洩

最近は、コンピュータの形をしていない機器によるセキュリティ脅威の発現も予想されており、組込みシステムのセキュリティという分野にも注目が集まるようになっている。そのようなシステムは、PCに比べて人の生活に密着したところで動作するため、重大な問題になることが予想されている。

このような懸念とは直交する形で、ドキュメントという形をした情報が漏れる伝統的な情報漏洩ではなく、音声、映像に限らず、多種多様な表現形式を持つ情報が、ネットワークを通して漏洩する、いわばマルチメディアな情報漏洩という現象も一般的になっていくのだろう。オフィスの音声や映像は言うに及ばず、ホームセキュリティシステムの人感センサーからの情報など、漏れてしまっては本末顛倒なものも数多くあるに違いない。

これらの情報漏洩は、古典的な盗聴と共通するものがある。いわば、盗聴のメディア・コンバージェンスとでも言うのだろうか。すると、伝統的なメディアがインターネットへ収斂し、数々のイノベーションがもたらされたのと同じ理屈で、盗聴にもイノベーションが訪れる可能性もある。

○ マルウェアのマルチメディア・イノベーション

冒頭のテレビ会議システムやパーソナルコンピュータに限らず、メディア機能を備えているネットワーク機器、ネットワーク機能を備えたメディア機器は増加するばかりである。このような環境は、マルウェアの侵入経路にもイノベーションをもたらすだろう。

個人的に危ないと思っているのは、デジタル放送である。意識していないと気がつかないが、ソフトウェアによるマルチメディア処理に伴う脆弱性は定期的に発見されている。記憶に新しいところでは、某著名オペレーティングシステムのアニメーションカーソルに伴う問題があった。もし、ビデオデコーダの脆弱性を突くようなデータストリームが放送されたとしたら、非常に多数の機器が一瞬にして感染し、接続しているネットワークを利用して活動を始めるだろう。

デジタル放送におけるファイアウォールの概念や、ホームネットワークにおける脅威モデルの整理など、早急に考え始める必要がある。

テレビ会議システムに繋いでいる最新式の液晶テレビを見ながら、こいつがプリンタへの出力データを密かに取り込んで外流しするようなことがあったらちょっとまずいなと、カメラの目隠しに最後のテープを貼りながら思った。

○ 頭隠して・・・

コンピュータらしい形をしたコンピュータに手こずっているようでは先が思いやられる。ネットワークやデジタル機器のユビキタス化、マルチメディア化に伴う情報セキュリティ脅威のイノベーションは、すぐそこにある危機なのだから。

こんなエラそうなことを考えながら、とりあえず完成した目隠しをカメラにセロテープで固定していたら大変なことに気がついてしまった。

「マイクはどうしようか？」

（篠田陽一　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

【 タイポスクワッティング（typosquatting） 】

タイポ(typo)はキーボードの打ち間違いを、スクワット(squat)は不法占拠をそれぞれ意味します。タイポスクワッティングとは、有名なサイトとよく似たURLのドメインを取得し、URL をタイプミスした利用者を自分のサイトへ誘導して、不正な行為を働くことです。具体的には、有名なサイトのURLの一文字だけをキーボードの隣の文字に変えたり、本来は「.co.jp」のドメインを「.com」に変えたりしたサイトが用意されます。このようなサイトにうっかりアクセスしてしまうと、バナー広告だらけのページだったり、ワンクリック詐欺を狙う有料のアダルトサイトだったりすることがあります。また、ポップアップを表示して本物のサイトによく似せたフィッシングサイトに誘導したり、スパイウエアを送り込んだりするような、さらに悪質なケースもあるので注意が必要です。

ドメイン名は最初に登録を願い出た者に与えられるために、転売による利益などを狙って、無関係な人間や会社が、有名な企業や商品のブランドの名前が入ったドメイン名を取得することは、以前から行われていました。世界知的所有権機関(WIPO)は、サイバースクワッティングと呼ばれるこの行為を排除するために、WIPO 仲裁調停センターを1999年に開設しました。それでも、紛らわしいURLのドメインを取得することまでは防げないため、タイポスクワッティングには利用者が自己防衛をするしかありません。と言っても、対策は単純で、よく利用するサイトはブラウザの「お気に入り」に登録しておいてそれを利用することと、初めてアクセスするサイトの場合には、URL を入力する際に打ち間違えないよう注意することの二点です。また、URL の一部を入力すれば、過去にアクセスしたサイトの中から候補の一覧を表示してくれる機能や、フィッシング対策機能を持つセキュリティ対策ソフトも多いので、それらを活用することも有効です。

4. NISCOLUMN（ニスコラム）

【 バックアップノスゝメ 】

NISC NEWS の読者諸兄姉の皆さまは業務で情報セキュリティに携わっている方が多いと思いますが、業務を離れた自宅においても CISO 兼 SE として情報セキュリティ対策に取り組んでいるのではないかと思います。情報漏えい事件が多い昨今なので、自宅 PC で利用している「プライベート」な情報の機密性には十分配慮されていることは想像に難くないですが、情報の可用性への配慮＝バックアップの対策は十分でしょうか？

というのも、最近我が家のバックアップ体制を刷新したところ、自宅に蓄積される情報の多くがデジタル化された情報だという事実を再認識したしだいであります。デジカメで撮影された画像、デジタルビデオカメラで撮影された動画、PC に保存された電子メールなどなど。デジタル化された情報は、コピーが容易で劣化がなく、PC で処理・加工しやすく、保存に場所をとらない等のメリットがありますが、機器や媒体の故障・破損、誤操作等で一度に大量の情報を失う可能性があります。「プライベート」な情報は、人々の思い出に深く関わりあうものが多いので、失った場合の精神的ダメージは甚大です。事が起こってから後悔しても失ったデータは戻ってきません。読者諸兄姉の皆さまにおかれましても、大切な思い出を守るためにバックアップの実施又は再点検をしてみてはいかがでしょうか。

参考までに、我が家のバックアップ体制をご紹介しましょう。まず、失いたくない情報と当該情報をどれくらい保存したいのかを決めました。我が家では、⑴デジカメ及びデジタルビデオカメラで撮影した画像及び動画の情報は永年保存、⑵電子メール等の他人に知られたくない情報は生涯保存、⑶住所録などの適宜更新されるデータは 3 年保存となりました。そして、オリジナルデータは定めた保存期間だけ PC 内の HDD に保存しておき、毎月 1 回～2 回程度 USB で接続された外付け HDD にフルバックアップをとります。最悪の場合、直近 1 ヶ月分の情報は失っても仕方ないと決断しました。ちなみに、この外付け HDD は誤操作による情報の削除、ウイルス感染による情報の破壊（最近はあまり見かけませんが）等を避けるため、必要な時にしか接続しません。そして、毎年 1 回は DVD-R にフルバックアップを、半年に 1 回は差分バックアップをとり、最新のバックアップ DVD-R は自宅に置いておきますが、過去のバックアップ DVD-R は私の実家で保管します。これは、火災や地震に配慮した遠隔地保管のつもりです。以上が我が家のバックアップ体制ですが、このコラムが読者諸兄姉の皆さまの大切な思い出の保存のお役に立てれば幸甚です。

（のりみり）

【 言葉の問題 】

「情報セキュリティ」に関する仕事に携わって約2年が経過しましたが、正直に告白すると、実は未だに「情報セキュリティ」という語の意味をうまく説明できません。独立行政法人国立国語研究所による「外来語」言い換え提案によれば、セキュリティは「安全」と言い換えることが提案されているようですが、これに「情報」という言葉をつけて「情報安全」とすると、かえって意味が分からなくなってしまう気がします。結局のところ、「情報セキュリティ」という語に、2年間この仕事に携わった自分の経験をリンクさせて、「情報セキュリティ」の概念を頭の中で作り上げて仕事をしているような感覚があります。

一方、海外では、「情報セキュリティ」と同じような意味合いで、情報保証(Information Assurance)や、サイバーセキュリティ(Cybersecurity)という用語が使われているケースがあります。おそらく「情報セキュリティ」を含めたこれらの言葉は、受け止める個人の属する集団や文脈によってニュアンスが大きく異なるものであり、それらを理解しておかなければ、まったく異なるものを対象とした会話をしてしまったり、見当外れの議論が展開されてしまったりするおそれがあるようです。

個人的な経験では、海外の情報セキュリティ政策担当者と話をしているときよりも、むしろ国内で「畑」の違う政策担当者と話をしているときの方が、会話が噛み合わないケースが多いように感じます。おそらく、情報セキュリティ政策の担当者であれば、多かれ少なかれ、各国とも日本と同じような問題に直面しているため、悩みどころ

や直近のトピックにかなりの共通点があり、言語の壁を越えてお互いの言いたいことが「分かり合える」からではないでしょうか。一方、言語の壁がない国内での会合などで、まったく議論が噛み合わないというケースも多々あります。「情報セキュリティ」というものについて、内容の理解や重要性の位置づけが異なっていれば、当然の結果と言えるでしょう。

また、情報セキュリティに限らず、IT（情報技術）分野に携わっていると「用語の意味が分かりにくい」「理解できる言葉で言ってほしい」「日本語で説明してほしい（！）」などという指摘をよく受けます。先ほどの、「情報セキュリティ」に関する概念のような話ではなく、個々の用語や言い回しについて、どうしても一般ユーザーには分かりづらい説明になっている傾向があるようです。小説のようにすらすらと理解できるような説明をするのは至難の業でしょうが、このような指摘は真摯に受け止め、我々政策担当者としても万人に分かりやすい言葉で説明できなければと肝に銘じています。

翻って、情報セキュリティセンターのウェブサイトに掲載されている政策文書を読んでみますと……正直言って、「日本語で説明してほしい！」と叫びたくなる部分も少なからずありますね……。公式な文書だと、どうしても堅苦しくなってしまう部分があることをご理解の上、当NISCメールや広報資料の充実など、少しでも情報セキュリティ政策を身近に感じていただくような努力を行っていく予定ですので、皆様と一緒に「ITを安心して利用可能な環境」の構築を進められるよう、当センターの分かりづらい部分などにはどんどんご意見を頂ければと思っております。よろしくお願い申し上げます。

（Tak）

＜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