NISC NEWS

第８号（２００７年１月２６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

【「情報セキュリティの日」について 】

１　制定の経緯

内閣官房長官が議長を務める情報セキュリティ政策会議において、情報セキュリティ問題を俯瞰した３年間の戦略として「第１次情報セキュリティ基本計画（以下「基本計画」と表記）」が、昨年２月２日に定められ、さらに６月には、基本計画を着実に実行に移すための年度計画である「セキュア・ジャパン２００６」が定められました。

これらの中では、まず、我が国の８千万人のインターネット利用者の情報セキュリティに対する理解が世代間で違い、そもそも一般個人にとってはＩＴの仕組みが理解し難いという問題が採り上げられています。そして、この問題に対処するには、老若男女を問わず、各人がその状況に応じて情報セキュリティに関するリテラシー向上を図ることを支援すべく、関係する各主体が様々な対策を実施することが必要である、とされています。さらに、「情報セキュリティの日」を創設し、これに伴う広報啓発的行事を全国的規模で開催するとともに、これにあわせて、個人、企業、地方公共団体、教育機関及び研究機関を表彰するための制度の創設を検討する。」ことが定められました。

これに伴い、昨年１０月の第８回政策会議において、基本計画が定められた毎年２月２日を「情報セキュリティの日」とし、情報セキュリティの向上への気運を全国的に波及・浸透させるとともに、広く官民における意識と理解を深めることを目的に、その前後の期間において、政府機関はもとより、広く他の関係機関、団体の協力の下に、国民各層の幅広い参加を得た取組みを集中的に実施することと定められました。この実施にあたっては、内閣官房が警察庁、総務省、文部科学省及び経済産業省の協力を得て推進していきます。

２　実施概要

（１）「情報セキュリティの日」功労者表彰の実施

情報セキュリティへの取組みに関し、特に顕著な功績又は功労のあった個人又は団体を顕彰するものです。これにより、情報セキュリティに関する優れた取組みを広く普及することを目的としています。

表彰の対象としては、情報セキュリティに関し、

〇地方公共団体、企業等の組織における情報セキュリティ対策への先進的な取組み
〇情報セキュリティ対策に資する技術等の研究・開発
〇情報セキュリティ対策に関する普及啓発、人材育成への貢献

以上３点のいずれかについて特に顕著な功績又は功労があり、省庁横断的な視点から情報セキュリティ政

策会議議長（内閣官房長官）が顕彰することがふさわしい個人又は団体としています。
本年度は、２月２日（金）に開催する第１０回情報セキュリティ政策会議に引き続き、総理大臣官邸内で表彰等の記念式典を実施し、議長から表彰状が授与される予定です。

（２）関連行事の開催
「情報セキュリティの日」の目的にある、「情報セキュリティの向上への気運を全国的に波及・浸透させ、広く官民における意識と理解を深める」ためには、表彰だけに限らず、様々な場所で、様々な主催者が、様々な対象に、情報セキュリティ対策の重要性を訴えていくことが必要不可欠です。そこで、２月２日の前後の期間（本年は１月２６日（金）から３月２日（金）までの間としています。）に、政府機関はもとより、広く他の関係機関、団体にもご協力いただき、国民各層の幅広い参加を得て、１月２２日現在で４３都道府県で３０２件の関連行事を集中的に開催することとしています。
関連行事の中には、「情報セキュリティ政策会議」が後援している行事、内閣官房情報セキュリティセンター（ＮＩＳＣ）職員が講演する行事もあります。関連行事の一覧はＮＩＳＣのホームページに掲載されますので、もし読者の皆様のお近くで開催予定の行事がございましたら、参加してみてはいかがでしょうか。

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」

【 不必要に勇敢なあなた 】

インターネットは本当に便利だ。
お友達とのコミュニケーションは、電子メールにチャットは定番だし、最近ではIP電話やビデオチャットなども使うようになってきている。
また、オンラインサービスも広範なものが、日々改良されつつ提供されている。ショッピングサイトを利用した買い物やオンラインバンキング、株取引、オークションサイトなどは、多くの人たちが毎日利用している。本当に多種多様な商用サービスが提供されていることに感心してしまう。
そんな便利なインターネットを多くの人たちが使い、お金が沢山動くようになると、悪人たちが参入してくるのは当然の帰結である。悪人たちは、お金の臭いが大好きなのだ。実際、今のインターネットでは、悪人たちが跳梁跋扈（ちょうりょうばっこ）している。オークション詐欺の発生件数はとても多い。いかがわしいサイトへアクセスしたと騙る架空請求の被害も広がっている。悪意あるプログラム（マルウェア）を送り込もうとするウェブサイトも沢山あるし、ウィルス付きメールを送りつけて個人のシステムを外部から悪用しようとする試みも広く行われている。冷静にインターネットの中を眺めてみれば、そこかしこに危険性があるのだ。
では、インターネットに危険が潜んでいることは異常な事なのか。読者の皆さんの期待を裏切る答えかもしれないが、私自身は異常とは思っていない。むしろインターネットが真に社会化した結果だと考える。インターネットを完全にクリーンな環境として整備維持するのは原理的に不可能だ。むしろ、大多数の善良な利用者に対して、許容しうるリスクレベルをどのように維持するのかに腐心した方が建設的であろう。そのために、インターネットに関わる技術者、サービス提供者、法律や行政も様々な取り組みをしている。不十分な面もあるけども、なんとかリスクを許容範囲内に抑えようと努力しているのだ。
だが、供給者側だけの努力だけでは不十分であることも事実だ。利用者の側でも、インターネットには危険性があるのだという「常識」を持ち、その意識に見合った行動をすることも必要だ。
みなさんが街中を歩く時を考えてほしい。銀行で大金を引き出したら、銀行を出た後の移動には気をつけるだろう。夜遅く、一人で人通りのない道を通るのは避けるだろう。一人で繁華街のいかがわしいお店には入らないだろう。普段の街中での生活では、多くの人がそれなりに気をつけて生活をしているはずだ。ところが、インターネット利用になった途端、オンラインサービスの確かさを確認するまえにクレジットカード番号を入力してみたり、相手が誰なのかを確認しないまま電子メールでのコミュニケーションを始めてみたりと、ガードが低い行動が目立つ。不必要に勇敢なユーザが多すぎる。
インターネットでも、街中で身を守るのと同じようなセンスで暮らしてみよう。インターネット利用には勇敢さは必要ない。必要なのは、自分が何をしているかを理解し、それが安全なのかどうかを考えて行動する、スマートな使い方である。

（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

【 認証と認可 】

認証と認可はよく似ている言葉で、同一の意味で使われたりする場合もあるようですが、厳密には別のものです。コンピュータシステムにおいて、認証(authentication)とは、システムの資源へアクセスしようとしている人間が誰であるのか、また本当に名乗っているとおりの人間かどうかを確認することです。一方、認可(authorization)は、その人間に適切なアクセス権が与えられていることを確認することです。認証は認可に先立って行われ、また認証なしに認可を行うことはできません。

例えば利用者があるサービスへアクセスし、証明書やID、パスワードにより本人確認が行われてサービスの利用ができるようになった場合、これは認証が行われたことになります。また、サービスの中で、利用者がいくつかのグループ（例えば、「サービス提供組織内の利用者」や「組織外の利用者」など）に分類されており、認証後に利用者がどのグループに属するかが判定され、各グループでアクセスできるファイルや利用できるサービス等のリソースが指定されるような場合には、これは認可処理の範疇となります。

認証と認可は、小さなシステムでは一体化しているものもありますが、大規模で複雑なアクセス管理を設計する場合には、適切に区別をしておいた方が有用です。認証や認可の仕組みは、様々なものが提案されており、また日々進歩しています。システムへの信頼性をどのように設定やシステム管理の手間や運用性を考慮して、認証、認可をどのように行うか、適切な方式を選択することが必要でしょう。

4. 情報セキュリティQ

生体認証は、人間の生体的な情報を用いて個人を同定し、認証するための技術です。バイオメトリクス認証とも呼ばれています。生体認証には、顔、指紋、指や掌の静脈、虹彩、網膜、DNA、声紋や筆跡など様々な特徴や特性が利用されます。個々の人間が持っていて、かつ変化しにくい特徴的な情報を使うので、パスワードのように個人の記憶力のみに頼ったり、IC カードなどの特別なデバイスを持ち歩いたりする必要がなく、また盗窃や偽造が比較的困難であるなど、多くのメリットがあります。一方、方式によっては認証精度が不十分だったり、認証時間がかかったりする問題もあり、また真正なユーザなのに正しく認証されなかった場合の運用ルールなど、幾つかの課題も指摘されています。今後、さらに技術とノウハウを蓄積し、より利便性の高い方式を実現していって欲しいですね。

さて、ここで問題です。わが国では、2006 年 3 月 20 日から IC チップを内蔵して偽変造を困難にした電子パスポート（IC 旅券）の申請受付を開始しました。IC チップには、国籍や名前、生年月日など既存の旅券面の身分事項のほか、ある生体情報が記録されています。それは一体、何でしょうか？

（1） 指紋画像　　（2） 顔写真　　（3） 署名（サイン）　　（4） 虹彩画像

（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「日本国内のパソコンがどの程度ボットに感染し、その総数は何台ぐらいあると言われているでしょうか？」でした。

正解は「1．40 台に 1 台 （総数は約 50 万台）」です。これは、テレコム・アイザック推進協議会（Telecom-ISAC Japan）と JPCERT コーディネーションセンター（JPCERT/CC）などが共同で行った「ボットネット実態把握プロジェクト」の調査レポートで報告された数値です。ただし、1年以上も前のデータですので、ボットの技術がより悪質で巧妙化している現在では、さらに多くのパソコンが感染している可能性もあります。

では、ボットにはどのように対策すれば良いのでしょうか？　言うまでもなく、先ず感染しないことが重要であり、それには不審なメールの添付ファイルを開かない、信頼できない Web ページにはアクセスしないなどの、一般の

ウィルスと同様の対策が有効です。もちろんウィルス対策ソフトも活用しましょう。

問題なのはアンチィルスソフトで発見・駆除できないケースです。ボットには、自分を発見・削除されないために、OS のパッチやウィルス対策ソフトの定義ファイルの更新を阻害するものがあります。ですので、そういう更新やダウンロードが正常に行えるかを、確認してみましょう。また、オンラインのウィルススキャンを提供しているサイトへの閲覧を妨害するボットもあります。使っているパソコンの反応が悪くなったり、ハードディスクへのアクセスが増えたりしたような気がした時には、感染を疑ってみることも必要です。

また、2006 年 12 月にはボット対策を専門とした、総務省と経済産業省との連携プロジェクトがスタートし、ボットに感染したコンピュータからの攻撃への対策情報やボット駆除のためのソフトウェアを提供するポータル・サイト「サイバークリーンセンター」の運営などを行っています。「サイバークリーンセンター」の URL は以下の通りですので、ボットについてもっと知りたい方や、対策を検討されている方は、一度訪問してみてはいかがでしょうか。

https://www.ccc.go.jp/

5. NISCOLUMN（ニスコラム）

【 ２００７年を迎えて 】

新年のご挨拶には少し遅くなってしまいましたが、明けましておめでとうございます。2007年最初のNISCニュースです。

昨年は、ウィニーによる情報漏えいを筆頭に、色々な話題が報道されたり、巷でとりあげられたことを思い出しつつ、年末・年始を過ごしておりましたが、年末に話した友人が、「うちの会社も業務情報の取り扱いとか、私物 PC の使用とか厳しくなってね、しょうがないけどね」と話しており、うちもそうだよという相槌が続々と続きました。あくまで好事例のほうなのかもしれませんが、そういったリスクへの気づきがなされてきたのかな、と思いました。

また、片田舎の親戚が、とうとう PC を購入して使い出したと言っていました。なんとなく、一応聞いてみたところ、「何か色々あるらしいので、分かる人に聞いてみて、そういうソフトも入れてもらったよ」と言っておりました。情報漏えいやフィッシングの報道によるところかと思いますが、「何か」がある、怖い、というセキュリティ対策の必要性に対する「気づき」は出てきている気がします。

ただ、この「何か」あるみたいだし、という気づきはなされてきた感がありますが、その「何か」が何なのか、ウィルス対策ソフトウェアの導入や定期的なパターンファイルの更新が、「何故必要で、何が行われているのか」について、ウィニーなど報道で一般的に知りえている脅威以外にも様々な脅威があるということも含めて、分かりやすく伝えていくことが必要だと感じています。国民の皆さんがセキュリティへの脅威と対策の必要性を正しく理解した上で、本年末に2007年を思い返すときに、わが国のセキュリティ基盤の底上げがなされてきたな、と思えるように、本年もセンターをはじめ関係する各主体が取り組んでいければと思います。

（T）

＜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