NISC NEWS

第４号（２００６年７月１１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

【情報セキュリティ政策における国際連携・協調とは】

情報通信基盤が整備され、ITの利活用と経済活動のグローバル化が進展する中、個人間のコミュニケーションや企業の経済活動が従来にもまして国境をまたいで行われるようになっていますが、その裏では情報セキュリティに関する諸問題も国境をまたぐ拡がりを見せています。一例を挙げれば、世界中に散在していると言われ、悪意のある攻撃者に自由に操られてしまうコンピュータ（ボットネット）を使っての企業のホームページへの集団的な攻撃や、国際的な詐欺サイト（フィッシングサイト）による被害など、もはや一国では対応しきれない問題として顕在化しています。これらに対処するためには、情報セキュリティ問題に対処する諸機関の間でも、起こりうる事案を想定して日頃から連携・協調を行う必要があります。

政府機関における取り組みとしては、OECD（経済協力開発機構）やG8、APEC（アジア太平洋経済協力）、ARF（ASEAN地域フォーラム）等で、情報セキュリティ問題に焦点を当てた取り組みが行われています。例えば、OECDは、「情報システム及びネットワークのセキュリティのためのガイドライン」を発表し、すべての参加者の間に「セキュリティ文化」を普及することを目標として活動していますが、分野別委員会である情報・コンピュータ・通信政策委員会（ICCP）においては、情報セキュリティ・プライバシー作業部会において、2006年には、電子政府のセキュリティや重要情報インフラ防護等が議論されています。NISCでは、発足1年を迎え、日本政府における情報セキュリティ政策の進捗と周知のため、このような国際会議の場を利用し、各国政府機関に対して日本政府の取組みや国際的な窓口の明確化を図っているところです。

一方、情報セキュリティ問題への対処は、いわゆる「官」だけで対応できる問題ではなく、「第1次情報セキュリティ基本計画」においても、官民連携の必要性が強調されています。民間分野主導での取り組みとしては、例えば、コンピュータセキュリティ事案対応チーム（CSIRT）の国際連携組織であるFIRST（Forum of Incident Response and Security Teams）等の場において、情報セキュリティ事案に対する国際連携体制の構築が進められており、政府機関とも認識を共有し、連携・協力を行いながら情報セキュリティ対策が進められています。NISCも、FIRSTの一員として情報共有を図るとともに、最新の情報セキュリティに関する事案の傾向や技術動向等を幅広く収集しています。

さらに、情報セキュリティ事案への対処だけではなく、幅広い情報セキュリティ問題を予防する観点からも、今後はIT先進国としての日本が他国に先駆けて直面した諸問題に対する解決策等を情報発信することが求められて

います。具体的には、情報セキュリティ問題を解決するための技術の活用や、ベストプラクティス（模範例）の普及・啓発などを通じて、国際社会における日本の役割を積極的に果たしていくことが挙げられます。そこで、国際的な情報発信の一環として、NISCはこのたびホームページに、NISCの概要や「第１次情報セキュリティ基本計画」等を英訳したコンテンツを掲載しました（http://www.nisc.go.jp/eng/index.html）。今後は、上記の趣旨を踏まえて、徐々にコンテンツを増やしていきたいと考えています。

このような国際連携・協調を進めるにあたり、官民を問わずキーワードとしてよく使われるのが'Trust'（信頼）という言葉です。情報セキュリティ問題の性格上、情報の共有や共同での事案対応を行う際に、協力者が信頼に値するかどうかということの重要性は他の分野よりも大きいのかもしれません。NISC も、今後は国内のみならず、国際的にも信頼に値する組織となるよう、より一層の努力をして参ります。

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」

【あなたは誰ですか】

日常生活の中では、「あなたは誰ですか」と問いかけられる場面がたくさんある。例えば、銀行口座を開設する場合や、携帯電話を購入する場合には、必ず本人確認が行われる。また、ちょっとしたサービスを受ける場合にも、本人確認が行われる場合も多い。

本人確認には、多種多様な方法が用いられている。一つは、本人しか持ち得ないものを提示する方法である。例えば、運転免許証や、組織が発行する身分証明書などは、その代表例である。もう一つは、本人しか知らない情報を提示し、事前に本人が登録していたものと一致するかどうかで判断する方法も広く使われている。例えば、様々なサービスでも散られている暗証番号やパスワードは、この方法に合致する。前者は、発行手続きの厳格さと複製困難な発行されるものの存在が、後者は本人以外が知り得ない情報の存在が、本人確認の確かさを保証する基盤となっている。

さて、最近、この本人確認の方法が急速に高度化している。例えば、生体認証技術を利用した方法や、セキュリティ・トークンといった特別なデバイスを用いた方法が、日常生活に登場してきている。数年前であれば、厳重な情報管理が求められる一部の特殊なシステムでしか使われてなかった方法が、まさに私たちが利用するような状況になってきているのだ。これは同時に、高度な方法を利用しなければならない程、リスクの高まりや変化が発生していることを物語っている。

このリスクの変化については、サービスを提供する企業や、行政でも分かりやすく説明する努力をしている。しかし、まだまだ多くの人に理解される状況にはなっていない。どのような変化なのか、何が問題となっているのか、どのような対抗措置があるのかを、ぜひとも多くの人たちに学んでもらいたい。そして、情報システムの構築・運用に関わるひとたちには、その状況の変化をフォローアップするような努力をしてもらいたいと思う。

（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

【ソーシャルハッキング】

「ハッキング」は本来「高い技術を駆使してシステムを操作する」ことですが、現在では「コンピュータを不正に利用する」意味を表す「クラッキング」と区別せずに用いられることが多いようです。

ハッキング手法の一つである「ソーシャルハッキング」とは、「ソーシャルエンジニアリング（社会工学）を利用したハッキング」と解釈されていますが、特に情報セキュリティの分野における「ソーシャルエンジニアリング」とは、

人を騙す等、情報システムの脆弱性等とは一見無関係な手段を用いて、必要な情報を不正に入手することを意味する用語として用いられています。例えば、パスワードを入力するのを肩越しに盗み見る「ショルダーハッキング」がよく知られていますが、他にも手口としては電話を用いて聞き出したり、席を外した僅かな間にパソコンを操作したり、あるいは郵便受けにたまった郵便物から情報を得たりする場合もあります。

ソーシャルハッキングに遭わないようにするための決定的な対策はありませんが、普段から周囲に危険が潜んでいることを常に意識し、自分の身は自分で守る必要性を改めて認識する必要があります。

4. 情報セキュリティQ

Cookie はWebページの利便性を高める用途でよく用いられていますが、(Webブラウザに脆弱性がある際など)場合によってはハッキングに悪用されることがあるため、利用にあたっては注意が必要です。ところで、このCookie が初めて組み込まれたWebブラウザは次のうちどれでしょうか。

① Mosaic　② Netscape Navigator　③ Internet Explorer　④ Opera　⑤ ①～④以外

(なお正解は次号にて掲載致します。)

【前号の答え】

正解は「③ 海外のコメディ番組が由来」です。

「SPAM(スパム)」とは味付け豚肉の缶詰の商品名であり、イギリスのコメディ番組において、レストランに入ってきた夫婦がメニューを選んでいると、近くに座っていたバイキングの集団が「SPAM！、SPAM！」と大声で歌いだし、それに釣られてレストランの店員も「SPAM！！」を連呼しだして、最後にはその夫婦も SPAM を注文せざるを得なくなる、というコントがありました。ここから、当人が欲していないのにも関わらず、大量に送りつけられてくる広告メールが「SPAM メール」と名づけられたのが由来とのことです。因みに、ドイツ語で「息が詰まるような」は“spamnend”ではなく、本当は”spannend”が正しいつづりです。念のため。

5. NISCOLUMN(ニスコラム)

【先ずは「セキュリティ」という意識を持つことから】

私が「情報セキュリティ」という得も知れぬ世界に初めて足を踏み入れたのは、大学 4 年生に研究室に入った時だった。その当時の研究室では、情報理論、符号理論とならんで暗号理論を核とする技術オリエンティドな情報セキュリティが主たる研究テーマであり、例えば暗号関連だと RSA や ElGamal 等、今までの暗号方式の発想とは全く異なる公開鍵暗号と呼ばれる方式が研究対象としてはメジャーであり、また認証関連でいえば、Fiat-Shamir 法に代表されるゼロ知識対話型証明等がホットな話題だったと記憶している。その頃これらの方式はまだ机上における研究・検証の段階であって、自分自身も本格的な実用化は随分と先のことなのだろうなぁ、という思いを漠然と抱いていた。

それから十数年の年月が経ち、上記を含めた情報セキュリティに係る技術の多くが研究、実用化されて、現在の IT を利用した社会活動や経済活動の基盤の安全性を支える要素の一つとして機能するに至っている。一方ユーザー側の意識は、そういった変化に応じて何が変わったのかといえば、個人的にはそれ程変わっていない、すなわち個々のユーザーによって情報セキュリティに対する温度差は相変わらず大きいような気が

する。もちろん、ユーザーは暗号化アルゴリズムや認証方式の仕組み等、技術の細部について知っている必要はないし、それらは専門家の仕事である。しかしそのことと「セキュリティ」という意識を自分の中に何ら持たず、自分の安全を人任せにすることとは別問題であると思う。「どうもセキュリティは難しそう」⇒「何だか面倒くさい」⇒「結局何の対策も講じない状態のまま」というユーザー側の思考の流れに即して、使い手がなるべくセキュリティを意識せずに使用できる製品やサービス等も提供されてはいるものの、それだけでカバーするには限度がある。利便性のあるシステムがますます増え、それを安全に使用する技術も検討を繰り返しつつ進歩はしているのに、ユーザー側がセキュリティを全く意識しない、あるいは「誰かが守ってくれているだろう」という意識しかないが故に、起こるべくして起こってしまう事件は枚挙にいとまがない状況である。このような事件にできるだけ巻き込まれないためにも、「セキュリティは難しいからやらない」と端からそこで思考を停止するのではなく、先ずは「セキュリティって何？」「自分の使っているシステムや環境って本当に大丈夫？」という些細な意識を持つことから始めることが重要だと切に感じる。そしてそのことが「自分の身は自分で守る」ことを考えるという自立的な姿勢にも繋がっていくのでは、と信じている。

「無」に何を乗じても「無」のままであり、何の変化もない。この「無」を少しでも「有」に変えることで初めて「対策」として一歩前進できるような気がする。その一助を担う役割も当センターに与えられた大切なミッションの一つであり、今後はユーザーの意識のみならず、解りやすい情報提供という観点で、センター側の意識の持ち様も同様に問われることになると思う。

（F.C.）

＜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