NISC NEWS

第１５号（２００７年１１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

【 我が国の情報セキュリティ分野における国際協調・貢献に向けた取組みの公表 】

はじめに

情報セキュリティ政策の国際的な展開は、国民生活・社会経済活動がますますITへの依存度を高めてきている現在、特に重要な意味を持つようになってきている。IT基盤は、24時間・365日、常時世界ともつながっているため、仮に我が国のIT基盤に何らかの障害が発生した場合に、その影響が我が国に留まらず、急速に諸外国にも拡大する可能性がある。逆に、諸外国において、IT基盤に何らかの障害が起こった場合には、我が国の国民生活・社会経済活動に負の影響が生じる可能性もある。さらに、非意図的な要素に起因するIT障害に限らず、意図的な攻撃が、国境と関係なく容易に国・地域内の重要なビジネスインフラに被害を発生させる可能性がある。今般、情報セキュリティ政策会議において決定された「国際協調・貢献に向けた取組み」は、このような状況を踏まえ、我が国を含む各国が連携・協調を図っていくためのグランドデザインを描いたものである。

取組の方向性

国際的に取り組むべき情報セキュリティ政策の課題は、IT利用者のモラル・認識の形成・向上、IT利用環境の整備、IT利用に際してあるいはITを利用して被害を発生させる行為への対応など、多岐にわたる。また、情報セキュリティの向上に関わるプレーヤーは国際機関、各国政府、重要インフラ事業者、企業、個人、非営利組織（NGO,NPO）等、様々である。これらの政策課題に、プレーヤーがグローバルまたは地域規模、あるいは二国間等の様々なスケールで取り組むとなると、その対象は膨大なものとなる。その中で、我が国の政策資源を投入すべき分野を選択・集中を通じて明確化するという視点から、本取組みはまとめられた。

代表的な政策

このような観点から情報セキュリティ政策会議で議論された国際協調・貢献に向けた取組みのうち、いくつかの重要な政策をここに記載する。

① セキュア・アジア・ビジネス構想

近年、日本と日本以外のアジア地域との経済関係は深化しており、企業活動のアウトソーシングやオフショアリングもアジア間で積極的に行われている。このような企業活動は、信頼性の高い情報セキュリティ水準に支えられて初めて活発化する。アジア地域での企業活動や投資を支援するため、アジア地域の政府機関、国際機関、企業等に働きかけ、情報セキュリティ水準の高いビジネス環境を構築していくものである。

② ICT Risk Free 構想

国民生活、社会経済活動がインターネットへの依存度を高めている中で、そのネットワークへ打撃を与えるサイバー攻撃等、ITに起因するリスク・脅威に関しては、一国のみではなく、グローバルに対応策を検討する必要がある。そのためには、主要なIT先進国のハイレベル等で問題意識を共有した上で、適切に対処していくべく議論を進めていく必要がある。このような取組みは、実際に問題が生じた際に、各国と協力しながら適切な対応をとることを可能とするものである。

③ 情報セキュリティに関する諸権利論の検討

情報セキュリティ水準の向上を通じたビジネス環境の信頼性の確保は、消費者や企業等の主体が安心・安全に活動を行うためにも不可欠となってきている。一方、ある程度の情報セキュリティ水準を期待するという価値観は、あらゆる規制から自由であるべきインターネットの価値観や、市場における自由競争等の価値観と相反する可能性がある。このような新たな価値観をインターネット上で活動を行う際のユーザーの権利ととらえることに関し、プライバシーを重要な権利と捉える OECD 等において議論が始まりつつある。当該施策は、このような議論を更に喚起し、日本が主体的な役割を果たしていくこと目指すものである。

④ 情報セキュリティに係るグローバルなルールや標準の形成への貢献

情報セキュリティの分野では、今後も制度面や技術面等において、グローバルなルールや標準の形成が進む可能性が高い。具体的には、IT基盤に係る技術面、グローバルに展開する企業の情報セキュリティマネジメント体制の構築に係るガバナンス面、一定規模以上の企業や政府に課される調達等に関する基準などが考えられる。このようなグローバルなルールの形成過程に積極的に参加し、我が国の進んだ取組みをベストプラクティスとしてグローバルなルールに反映するよう努力することは、IT社会全体の情報セキュリティレベルを向上させるとともに、我が国の成長力にも寄与していくものである。

⑤ 国際フォーラムへの積極的参加

情報セキュリティについては、様々な国際フォーラムが立ち上げられている。このようなフォーラムに積極的に参加し、日本の情報セキュリティの取組みをアピールすることは、国際的な舞台での日本のプレゼンスを高め、政策決定に関与していくことができる土台を作ることとなる。更に、会合を通じて世界の動向を把握することによって、国内の政策への示唆を得ることができる。

取組みをまとめた文書はホームページで公表しております。ご興味のある方は、是非下記 URL で御覧ください。
（http://www.nisc.go.jp/active/kokusai/pdf/international_approach.pdf）

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」

【 アウトソーシングを再点検する 】

「近年社会や組織において情報システムは急激に基盤化してきている」ことは、最近私が講演するときに必ず述べていることだ。どんな組織でも、どんな業務でも情報システムを使用して実施する傾向が強まってきている。もはや情報システムによって、ビジネスが駆動される状況は、どんな組織にとっても特別なものではない。新しいビジネスモデルは、情報システム上に実装され、企業活動として展開されていく。企業活動は情報システムを活用して記録され、性能が測定され、企業行動決定の妥当性検査も情報システムを通じて行われる。組織におけるありとあらゆる活動が、情報システム上に形成される状況になっているということもできる。このような状況から、情報システムの構築と活用は、ビジネスそのものであるという認識を示す企業トップも増えてきている。

ところが、多くの組織では情報システム構築は内製化されておらず、外部のシステムインテグレータを活用することが通例となっている。さらには、組織内に情報システムそのものを保有することなく、情報処理そのものをアウトソーシングすることも行われている。このような状況は、新たなリスク要因となりつつあるのではないかと考えている。

一つは、適切な情報管理が行われないリスクである。実際、情報処理を委託した企業から情報漏洩が発生したケースは、ここ数年国内で数多く見られる。特に個人情報漏洩については、情報処理の外部委託がかなり高いリスクとして認識されるようになっている。

二つめに、情報システムの障害による停止といった運用上のリスクを挙げることができるだろう。基盤化した情報システムは、基本的に「止められないシステム」に変貌する。特に、システムの停止＝企業活動の停止という状

況にまで基盤化してしまった場合で、かつ、企業活動がグローバル化していたり、大規模化していたりする場合には、システム停止によって引き起こされる損害は甚大なものとなってしまう。このようなリスクを、アウトソーシング先が左右するような状況になっている。

三つ目に、アウトソーシング先がビジネス能力のボトルネックとなってしまうリスクである。先に述べたように、情報システム上にビジネスが形成されるような状況では、情報システムの出来不出来が、そのままビジネスの出来不出来に直結することになる。仮にアウトソーシング先の能力が低い場合、企業活動がそれに足を引っ張られることになることもあるだろう。このようなリスクも考えるべき時となっている。

このようなことから、情報システム構築と運用におけるアウトソーシングについても、今一度本当にビジネスのリスク管理との関係でどのように行うのかを考え直し、再点検すべき時がやってきていると思う。特に情報システム開発と運用を丸投げの状態で行っている組織では要注意だ。

（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

【 ポリモーフィック型ウイルス (Polymorphic Virus) 】

Polymorphic は、「多様な形体を持つ」と言う意味です。ポリモーフィック型ウイルスとは、ウイルスの機能の実態は変えずに自らの形を変えることによって、パターンマッチングで検出されないようにするウイルスのことで、別名ミューテーション型ウイルス（Mutation ＝ 変異する）とも呼ばれます。ポリモーフィック型とミューテーション型は厳密な定義では異なるものですが、現在では区別されないで使われることが多いようです。

パターンマッチングは、殆どのウイルス対策ソフトで用いられている有力なウイルスの検出方法です。具体的には、チェックすべきファイルと、「ウイルス定義ファイル」や「パターンファイル」などと呼ばれる、既知のウイルスのコードの「特徴（パターン）」を記録したデータベースとを比較（マッチング）し、そのファイルがウイルスに感染してないかを調べます。ポリモーフィック・ウイルスは、感染するたびに、自らをランダムに選択された暗号鍵で暗号化したり、異なる圧縮方式で自己解凍型に圧縮したり、コードの内容の一部を自分で書き変えたりするなどの方法で、パターンマッチングでの検出を無効、あるいは非常に困難にします。

しかし、このようなポリモーフィックのメカニズムは非常に複雑なので、現実に何代にもわたって変化し感染し続けるウイルスを作成することは容易ではありません。ところが、完成度の高いポリモーフィック・エンジンの開発者は、ネットのサイトを用いてソースコードや再利用可能なモジュールを販売したりします。インターネットは、悪意を持ってウイルスを作成する人にも、区別無く恩恵を与える、という悩ましい現実があります。このようにして、別のウイルス作者が「優秀な」ウイルスを参考に、簡単に亜種のウイルスを作ることが出来てしまうのです。

したがって、ウイルス対策ソフトも単純なパターンマッチングのみならず、さまざまな検出方法を組み合わせたものを利用することが有効です。無論、怪しげなホームページを訪問したり、不審なメールの添付ファイルを安易に実行したりしないよう常に心がけることが、セキュリティ対策の基本であることは言うまでもありません。

4. NISCOLUMN（ニスコラム）

【 まず被害に遭ってみる！？ 】

皆さんはパソコンがウイルスに感染したり、コンピュータ犯罪に巻き込まれたり、といった何らかのセキュリティ被害に遭ってしまったことがありますか？このメルマガの読者の方にはほとんどいないかもしれません。

両手では数えられないぐらい何年も前、まだインターネットが一般的になっていない頃、私の普段使っていたフロッピーディスク（以下、FD）がウイルスに感染してしまったことがあります。その頃のウイルスには、パソコンか

ら FD に感染し、その FD が別のパソコンで使われるとパソコンにも感染するという方法で感染を広げるものがありました。私の FD もその類のウイルスにどこかで感染したのでしょう。自分の FD からウイルスを駆除すると共に、FD を貸し借りしそうな心当たりのある友人達に頼んで、彼らのパソコンでウイルスを探しましたが結局どこからも見つけることができませんでした。いつからウイルスに感染していたのかも、感染元がどこなのかも確認できなかったことで、すっきりしない気持ちだけが残りましたが、これ以降は他人とのデータのやり取りにはかなり注意を払うようになりました。

次は片手で十分足りるぐらいの数年前、コンピュータを使った犯罪についての注意喚起を身近でもよく聞くようになってきた頃、ワンクリック不正請求のサイトにアクセスしてしまったことがあります。ドギツイ色を使った画面、あなたの身元を特定した旨のメッセージを見て一瞬だけドキッとしました。当時は既に情報セキュリティに関する仕事に就いていたためサイトにアクセスする場合は注意していたつもりだったのですが足りなかったのでしょう。もちろんお金は振込みませんでしたが、これ以降は、必ず URL を目視する等より注意を払うようになりました。いずれの場合も実害は無かったため、私にとっては情報セキュリティの意識を向上させる経験として有益でした。

最近、情報セキュリティ意識の向上を図る教育、啓発の活動が活発に行われています。そういった活動の成果もあってか、パソコンを使う場合には情報セキュリティ対策を何かしなければいけなさそうだ、という認識はかなり広まってきたように感じています。しかし意識は高まっても、どんな対策をして良いのかわからない人も、やり方がわからない人もいるでしょう。さらに、ウイルス対策ソフトをパソコンに入れても、ソフトウェアの脆弱性を全て修正しても、ソーシャルエンジニアリングのように回避できない脅威も残ってしまいます。これについては、狙われた人が気づいて被害に遭わないようにするしかないという点でより高度な知識やセンスが必要そうです。

情報セキュリティ対策の知識や、その対策だけでは足りないところを「怪しい」と感じるセンスを身につけるのは、自分の体験から考えると、経験してみることが近道なのではないかと思ったりします。もちろん本当に被害に遭ってみる訳には行かないですから、教材のようなもので被害体験をしてみるのが良いのではないでしょうか。もっとも、こういった被害体験の教材を安易にネット上に公開すると、教材に見せかけた不正なプログラム、教材を騙った不正な振込み請求といったややこしいものが生み出されたりしてしまう懸念もあります。隙があれば犯罪者に狙われてしまうであろうことが容易に想像できますので、十分にやり方を練らないといけないでしょう。せっかく情報セキュリティ対策の意識が広まってきた感じがするタイミングですから、この機を逃さずに色々な方策を考えて定着を図っていきたいですね。

（白銀）

【前号の「情報セキュリティＱ」の答え】

前号の問題は「デマ情報を意味する hoax（ホークス）の語源は、何？」でした。

正解は「② 魔術師の呪文」です。

「ちちんぷいぷい」とか「アブラカターブラ」など魔術師が使う掛け声には色々ありますが、ラテン語が起源の「hocus pocus（ホーカス・ポーカス）」もその一つです。この hocus が詰まって hoax となったと言われています。

「いっぱい食わされた」と笑える hoax なら良いですが、パソコンに重大なダメージを与えたり、個人情報を盗まれるような「デマウィルス」は困りますよね。ジョークを素直に楽しめない風潮は残念ですが、自分のパソコンや情報を護るために、常に情報の真偽を見極める態度を忘れないようにしたいものです。

＜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