NISC NEWS

第３号（２００６年６月８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

★ 当センターのドメインは、6/1 を以って、bits.go.jp から nisc.go.jp に変更になりました。

1. 情報セキュリティ施策紹介

【重要インフラのサービスと情報セキュリティについて】

内閣官房情報セキュリティセンター（NISC）が規定した重要インフラ 10 分野（情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道及び物流）は、文字通り国民生活・社会経済活動の基盤であり、サービスが停止すると国民生活に大きな影響を与えることから、あらゆる脅威に対し、その安定的供給を確保しなければなりません。

特に、近年発生した大地震を含めた事例を見ても、重要インフラ分野間における相互の依存関係の増大等に伴い、各重要インフラ事業者等が個別に対策を講じるだけでは、我が国全体としての重要インフラの安全性が確保できない状況が生じています。

その一方で、各重要インフラ分野におけるＩＴ化の進展は目覚ましく、政府としても重要インフラ事業者におけるＩＴが原因で重要インフラ事業者のサービスが停止する障害（以下、「ＩＴ障害」と言う。）に対して、分野間を越えた横断的情報セキュリティ対策を一層強化していくことが喫緊の課題と認識しています。

しかしながら、現在の状況を見ると、ＩＴ障害への対策について、官民の情報共有体制が十分に構築されていない等の問題を抱えており、政府として、2009 年度初めには、重要インフラにおけるＩＴ障害の発生を限りなくゼロにすることを目指すことを目標として、2008 年度までの今後３年間に、我が国の重要インフラ横断的な情報セキュリティ水準の向上を図るための「個別設計図」として、以下に示される４つの柱を掲げた「重要インフラの情報セキュリティ対策に係る行動計画」（2005 年 12 月 13 日 情報セキュリティ政策会議決定。以下、「行動計画」と言う。）を策定しました。

重要インフラにおける情報セキュリティ確保に係る「行動計画」の４つの柱
（１）安全基準等の整備
（２）情報共有体制の強化
（３）相互依存性解析の実施
（４）分野横断的な演習の実施

（１）安全基準等の整備

重要インフラ事業者等においては、提供するサービスの性質上、それぞれの特性を踏まえつつ、日頃から高いレベルでの情報セキュリティ対策が求められます。

そこで「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針」（2006 年 2 月 2 日 情報セキュリティ政策会議決定）を踏まえ、**それぞれの重要インフラ事業分野ごとに、必要な又は望ましい情報セキュリティ対策の水準について、「安全基準等」に明らかにし、重要インフラ事業者は**

自らが「安全基準等」を参考に、十分な対策が実施されているかを自己検証しつつ、重要インフラを防護する対策を進められるようにします。

（２）情報共有体制の強化

ＩＴ障害に関する情報について、１）ＩＴ障害の未然防止、２）ＩＴ障害の拡大防止・迅速な復旧、３）ＩＴ障害の要因等の分析・検証による再発防止の３つの観点から、**政府等は重要インフラ事業者等に対し適宜・適切にＩＴ障害に関する情報を提供し、重要インフラ分野間においてはこれらの情報を共有する体制を整備・強化します**。

（３）相互依存性解析の実施

我が国全体としての重要インフラ対策の向上に向けた、分野横断的な状況の把握のため、相互依存性の解析・把握を導入します。この相互依存性解析は、**それぞれの重要インフラに起こりうる脅威が何であるかを把握するとともに、ある重要インフラにＩＴ障害が生じた場合に、他の重要インフラに、いかなる影響が波及するかということを解析するものです**。

（４）分野横断的な演習の実施

各重要インフラ所管省庁、各重要インフラ事業者等と共に、**想定される具体的な脅威シナリオに対する重要インフラ横断的な演習を行い、演習を通じ、安全基準等、情報共有体制、情報共有・分析機能、相互依存性解析等の各施策の実効性・妥当性を定期的に検証します**。

表1 「重要インフラの情報セキュリティ対策に係る行動計画」の概要

●2000年12月に策定された**「重要インフラのサイバーテロ対策に係る特別行動計画」**は、増大するサイバーテロの脅威から7つの重要インフラ分野の防護のための初めての官民協力の枠組みについて規定。

●その後の各重要インフラ分野におけるIT利用の飛躍的進展とITへの依存度の増大、重要インフラ間相互の依存性の増大等の変化を踏まえ、**「重要インフラの情報セキュリティ対策に係る基本的考え方」（2005年9月15日情報セキュリティ政策会議決定）**に基づき、新たな行動計画を策定。

対象分野・脅威の見直し

基本的考え方	行動計画
➢ 重要インフラ分野として、医療・水道・物流を加えた10分野を設定 ➢ 想定する脅威を、「サイバー攻撃」に加えて、人為的ミス等の「非意図的要因」、「自然災害」へと拡大	➢ 重要インフラ分野として10分野*を指定し、具体的対象事業の範囲を設定 ➢ 想定する脅威及び各分野別重要システムを例示

新たな体制の構築

1. 情報セキュリティ水準の向上	
➢ 技術的基準及び運用基準についての「安全基準・ガイドライン」の策定・見直し等を実施	➢ 2005年度中に、内閣官房情報セキュリティセンターは「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針」を策定 ➢ 各分野は、上記指針を踏まえて、必要又は望ましい情報セキュリティ対策の水準を2006年9月を目処に「安全基準等」に明示するよう努力
2. 情報共有体制の強化	
➢ 情報提供体制の整理・強化、情報充実・質の向上 ➢ 「情報共有・分析センター」（仮称）等の各分野内情報共有機構の創設 ➢ 重要インフラ横断的な情報共有の推進（「重要インフラ連絡協議会（仮称）の設立等）	➢ IT障害発生時における連絡体制等、官民の情報共有、連絡・連携の仕組みについて具体的に規定 ➢ 2006年度末まで**に各重要インフラ分野ごとに「情報共有・分析機能（CEPTOAR）」の整備を推進 ➢ 「重要インフラ連絡協議会（CEPTOAR-Council）」（仮称）の設立の場を内閣官房に設置
3. 相互依存性解析	
➢ 内閣官房情報セキュリティセンターを中心に重要インフラ分野横断的な状況把握（相互依存性解析等）を実施	➢ 相互依存性解析の効果・実施の流れを記載 ➢ 内閣官房情報セキュリティセンターを中心に、2006年度から相互依存性解析を試行
4. 分野横断的演習の実施	
➢ 想定脅威に対応した具体的脅威シナリオの類型を元に、毎年度、重要インフラ分野横断的な演習を実施	➢ 2006年度に「研究的演習」、「机上演習」、2007年度に「機能演習」を段階的に実施 ➢ 内閣官房において「演習実施計画」を立案、内閣官房の監修の下、各重要インフラから参加する形態で実施

今後は、上記に示した行動計画に基づき活動を進めると共に、それぞれの対策の進捗状況の評価・検証を踏まえて３年ごと又は必要に応じて行動計画の見直しを行い、ＩＴ障害に関する重要インフラのサービス停止から国民生活や社会経済活動を守るための活動を引き続き行ってまいります。

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」

【「もし○○だったら」思考の大切さ】

悪意あるプログラム（スパイウェアやウィルス等）は、色々なところからシステムに入り込む可能性がある。その大部分は、利用者が何かをすることでシステムに入り込むケースだ。例えば、ファイル交換ソフトウェアを使って手に入れたファイルの圧縮展開、ダウンロードサイトから落とした出所不明ソフトウェアのインストール作業、SPAM に添付されたファイルを開く行為等々が挙げられる。

しかし、だからといって利用者に「見慣れぬファイルは開くな」と注意喚起したところで、それだけでは悪意あるプログラムがシステムに入り込む事を防止する事はできない。私がしてしまった実例を紹介しよう。

仕事で物品購入をしようとして、ある会社に見積りをお願いしていた時のことだ。夜中にメールをチェックしていると、見積り依頼していた会社からメールが送られて来ている。件名には「お願いされたもの」とかかれ、本文には「依頼されていた見積書です」とだけ書かれ、添付ファイルがあった。「やけに素っ気ないメールだなぁ」と思いつつ添付ファイルをダブルクリックで開いてしまった。「あ、もしかして…」と思ったときには後の祭り。私が受信したメールは、送信アドレスを偽装したウィルス付きメールで、しかも SPAM でばらまかれていたものだった。
確かに不注意。確かに軽卒。そう言われる方もいるだろう。しかし、心の隙間は誰でもできうる。そして、その心の隙間にぴったりはまる状況が生まれれば、自分の手で何も疑う事無く素性の分からないファイルを開いてしまう事もあるのだ。注意していれば大丈夫というだけでは十分な対策にはならない。

私の場合には、ウィルス対策ソフトを導入しており、幸いな事にファイルを開いた瞬間に、警告ウィンドウが表示され「ウィルス付きファイルは開けない」ということが表示され事なきを得た。

しかし、ウィルス対策ソフトウェアの導入だけで全部大丈夫だろうか。「もしも、パターンファイルの更新を怠ったままの利用者がいたら」、「もしも、OS インストール直後のシステムが接続されたら」というようなことを考えていけば、ウィルス対策ソフトウェアだけではない、色々な対策を考える必要があることは直ぐに分かるはずだ。このような「もしも〇〇だったら」を考え、種々のリスクからシステムを幾重にも防護することが、最近の情報セキュリティ対策では当たり前になっている。「大丈夫なはずだ」で自分を無理矢理納得させるのではなく、常に「もし〇〇だったら」を考え、解決方法を考える姿勢を持とう。

最後に一つ。「利用者は自分が考えた対策に従うはずだ」ではなく、「もしも利用者が、自分が考えた対策に強い不満をもっているとしたら」を考える事は絶対に忘れてはならない。実は、セキュリティ管理者が一番目をつぶりやすく、本当は一番真剣に考え続けなければならない問題である。

（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

【共通鍵暗号と公開鍵暗号】

暗号は人類が古くから知恵を絞って用いてきました。昔、とある国の王が別の国の王に対し、秘密情報を伝える際に、従者の頭髪を剃り、情報を刺青として刻んでから、髪を伸ばさせ、先方で再び頭を剃ってもらい、双方で情報の送受をしていたという記録も残っているそうです。

近年インターネット上で様々な情報をやり取りするようになってから、暗号の重要性が再認識されるようになりました。暗号の技術は第三者からの盗聴を防ぐためだけでなく、送信者の真正性（なりすましでないこと）を確認する目的にも利用できます。ここでは二つの暗号化方式について説明します。

（1）共通鍵暗号

暗号化と復号化に同じ鍵を用いるのが共通鍵暗号です（ドアの鍵を閉める時と開ける時に共通の鍵を使うことに相当）。有史以来、人類は長い間この共通鍵暗号という方式を用いてきました。この方式は暗号化のための計算量が比較的少なく、多くのデータを一括して暗号化できる等の利点がありますが、通信相手に鍵を送付しなければならず、送付の段階で第三者に如何に鍵を取られないようにするのか、の工夫が必要になります。公開鍵暗号が発明されるまでは、暗号といえば共通鍵暗号を指すことがほとんどでした。

（2）公開鍵暗号

暗号化用と復号化用とで異なる一対の鍵を用いるという、今までとは全く異なる発想の暗号方式が1970年代に発明されました。片方（公開鍵）を公開し、自分は他方（秘密鍵）を大切に保管することにより、誰でも自分宛の暗号文を作成して送付することができますが、それを正当に復号化できるのは自分だけということになります。またその暗号文をさらに送信者の秘密鍵で暗号化して送った場合には、受信者は送信者の公開鍵で復号化したものが、さらに自分の秘密鍵で復号化できることを確認することにより、送信者が真性であり、第三者がなりすまして送ったものではないことが分かります。

暗号の強度を高めるには鍵の長さ（情報量）を多くする必要がありますが、計算量やシステムの効率を考慮し、

適切な規格を用いることが重要になります。

4. 情報セキュリティQ

SPAM メールで知られる「SPAM（スパム）」とは一般にメールを無差別に大量配信することにより、受信者に対し被害を及ぼす悪質な行為を指しますが、この「SPAM」という言葉の由来は次のうちどれが正しいでしょうか。

① 温泉のように湧き出る大量のメール（Spa+Mail）が由来
② 迷惑メールをやり始めたのが G. Maps という人で、それを逆さから読んだのが由来
③ 海外のコメディ番組が由来
④ spamnend（息が詰まるような）というドイツ語が由来
⑤ 上記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「② 23 名」でした。数学的な論述は省きますが、求める確率は、異なる n 個の集合から選ばれた i 個が全て異なる確率を 1 から引くことで得ることができます。その確率を p とすると、$p = 1 - (1-1/n)(1-2/n)\cdots(1-(i-1)/n)$ となり、p=0.5、n=365 として、近似等を利用して i について解くと、i≒23 と出てきます。これは一般に「バースデーパラドックス」と呼ばれるものであり、一見 365 や 365/2 だと考えがちですが、それよりももっと少ない数の人数が集まれば、誕生日の一致するペアが高い確率で存在するというのは何とも不思議な感じがしますね。

5. NISCOLUMN（ニスコラム）

【「揚げ足をとる」セキュリティから「誉める」セキュリティへ】

４年前、情報セキュリティ政策の担当に就いた時、PKI、IDS、ISO15408、ISO17799、・・・といったよく分からない言葉のオンパレードの渦に巻き込まれ、一つ一つはなんとなく分かるものの、全体として何がポイントなのか全く分からず、かなり凹んだものだった。加えて、この業界の方々は新人にはとても厳しく、教えを請いにいくと、「前任の人がようやく分かってきたところなのに、また一からやり直しですか」と冷たく突き放され、背筋が寒くなったこともあった。

一方で、「小さな政府」が声高に言われる中、政府が情報セキュリティ問題への取り組みを強めていくことについて、否定的な意見は皆無に近く、「これから大事な分野だ」と口々に言われたことは記憶に新しい。また自分自身も、この分野にはこの国にとっての何か大きな本質がある、と直感的に感じたものである。

そこから今日まで、「情報セキュリティが重要だということは分かったが何が重要なのか」、「情報セキュリティと『国益』の接点はどこなのか」ということを考え、政策への反映を模索してきたが、正直に言って、未だに明確な答えは出ていない。ただ、一つだけ確信を持って言えるのは、情報セキュリティの分野は、この国が持っている強みを最大限に生かせる分野だということである。世界的にも例がない「速くて安い」接続環境、そして高い品質の製品を作る産業力、人と人との信頼を起点にした良好な治安などなど。

最近、情報漏洩や情報システムのダウンなどの事件・事故が多く起こっている。メディアをはじめとして、事件・事故系の入口から入る方が分かりやすいゆえに、どうしても、情報セキュリティというものは暗いイメージがつきまとう。しかしながら、高い品質や良好な治安は、悪い部分をモグラたたきにし、危機感を煽るといった、「揚げ足を取る」姿勢から生まれてきたものだろうか。この国の強みを生かすということを考えたとき、良いところを伸ばし、人々の心にちょっとした明るさを与えながら、言ってみれば「誉める」ことで前進するモデルが必要だと思う。

難しい命題だが、これに対する答えを見付けながら、将来へ向かっていくことが必要であると、そして、内閣官房情報セキュリティセンターの役割は、そのための全体戦略を考えて、日々前進することであると改めて思うところである。

（Y. 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