NISC NEWS

第１６号（２００７年１２月２５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

【 重要インフラにおける情報セキュリティ確保対策の動向 】

我が国の重要インフラにおける情報セキュリティ確保に係る施策について、以前「NISC NEWS 第3号（2006年6月8日発行）」（http://www.nisc.go.jp/nisc-news/0003/news0003.pdf）にて、ご紹介しました。

重要インフラの横断的な情報セキュリティの水準向上を図るために、個別設計図として「重要インフラの情報セキュリティ対策に係る行動計画」（以下「行動計画」）が策定されてから、本年12月で丸2年が経過します。そこで、本号では重要インフラにおける情報セキュリティ対策に関するこの2年間の施策の動き等についてご紹介します。

（注）重要インフラ：「行動計画」においては、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、物流の10分野を、施策の対象たる「重要インフラ」としています。

（1）安全基準等の整備

各重要インフラ分野における、情報セキュリティ対策の項目及び水準が示されている文書類である「安全基準等」の策定・見直しを支援するため、昨年2月に「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」（以下「指針」）が策定されています。これを踏まえ、各重要インフラ分野では、昨年度中に「安全基準等」の策定又は見直しが行われました。

情報セキュリティを巡る状況は常に変化をすることから、「指針」は1年ごとにその内容について見直しを行うこととなっています。そこで本年6月に第1回目の改定が行われました。各重要インフラでは、本年9月までに改定後の「指針」を踏まえた「安全基準等」の見直しが完了しています。

（2）情報共有体制の強化

政府内では、2006年8月から、各重要インフラ所管省庁に「リエゾン」と呼ばれる情報連絡要員が置かれ、NISCとの間での情報連絡・提供を行うための体制が強化されました。

また、重要インフラ分野10分野のうち7分野では、IT障害に関する情報を共有するための「情報共有・分析機能（CEPTOAR：セプター）」が、昨年度中に整備されました。残る3分野においても、本年度中に整備が完了することとなっています。さらに、セプター間での横断的な情報共有の場を設けるべく、現在検討の場にてそれぞれのセプターの代表や業界の代表者による検討が現在鋭意進められているところです。

（3）相互依存性解析

ここで言う依存関係とは、ある分野で生じたIT障害の影響が他の分野に波及することです。2006年6月から2

007年12月にかけ、まずは各重要インフラ分野同士の依存関係を可視化するための検討(「静的依存性解析」)を行いました。その結果、通信分野、電力分野、水道分野が、それぞれ他の重要インフラ分野の一部と情報セキュリティの観点で依存関係にあることが確認されました。

今後は、この「静的依存性解析」の結果を踏まえ、障害発生から波及・拡大という連鎖的な伝播プロセスを把握する「動的依存性解析」に取り組むこととしています。

(4)分野横断的演習

2006年7月から10月にかけて演習課題の設定や演習手法の理解等を主眼とした「研究的演習」を実施したのに続き、2007年2月に、各重要インフラ分野と重要インフラ所管省庁等が参加して、具体的なIT障害発生シナリオを元に会議形式で課題討議を行いながら実施する「机上演習」を実施しました。

本年度は、この「机上演習」と先に述べた「静的依存性解析」の結果等を踏まえ、重要インフラのサービスの維持・早期復旧に向けた現状の情報共有の仕組みを検証する「機能演習」(実際の組織の指示判断系統機能を用いて模擬的に検証するための演習)を2008年2月に実施することとしています。

以上が、行動計画策定後の2年間での主な動きです。

なお、「行動計画」に関しては、策定後2年を経過した2007年12月から、およそ1年をかけて見直しのための検討を行うこととしています。具体的には、2008年の4月頃の論点整理、9月頃の素案取りまとめを経て、12月頃には見直しの内容を確定させ、パブリックコメントの募集を行うこととなります。有意義な行動計画へのバージョンアップに向けて、読者の皆さんからのご提案もお願いしたいと思います。

これらの活動の詳細は重要インフラ専門委員会の資料で公開しておりますので、ご興味のある方は、次のURL で御覧ください。

http://www.nisc.go.jp/conference/seisaku/ciip/index.html

2. 誰でもわかる情報セキュリティ用語

【 DNS (Domain Name System) 】

DNS とは、人間にフレンドリな「ドメイン名」と、インターネット上の住所である「IP アドレス」とを対応させる(これを「名前解決」といいます)ためのシステムです。DNS は、世界に 13 台だけ存在しているルートサーバから、全世界の DNS サーバが階層的に接続され、相互連携することで、ドメイン名から IP アドレスを引いたり、その逆の操作をするサービスを提供します。いわばインターネットの導(しるべ)であり、Web へのアクセスも電子メールの配送も、DNSなしには成り立たないと言って良いでしょう。しかし、これだけ聞くとDNSとセキュリティにはあまり関係が無さそうですが、実は脆弱な DNS に関連した様々な攻撃が近年急激に増加しているのです。

攻撃の一つのパターンは、DNS の情報の書き換えです。キャッシュ・ポイズニングなどの手法で、設定を偽の情報にすりかえられた DNS サーバを利用したユーザは、真正な Web サイトにアクセスしたつもりで悪意のある Web サーバに接続してしまったり、メールを不正に転送されてしまったりすることになります。

もう一つは、DNS サーバを踏み台にした DDoS(分散 DoS)攻撃です。DNS が管理する情報は多くのサーバに分散して保持されているので、DNS には名前解決を行うためにサーバの階層をたどって他のサーバに順に問い合わせを行う、再帰検索という機能を持っています。攻撃者は、再帰検索を許しているDNS サーバに、被害者(攻撃を受けるサーバ)を返信先にした要求を大量に送ります。DNS サーバがこの要求に対する返答を被害者に送信した結果、被害者はサービス不能状態に陥ることになります。

これらの問題に対処するには、先ずは DNS サーバの OS やソフトウェアの脆弱性を無くすべく、最新のパッチを当てること。また、DNS サーバを、管理下にないネットワークや信頼できないネットワークからの要求を受け付けないようにするか、不要と判断できるならば再帰検索を拒否するように設定することです。

3. NISCOLUMN（ニスコラム）

【 リスクについて 】

皆さん「リスク」と聞いて何を思いうかべますか・・・・まず本題に入る前に次のケースを思い浮かべて、一緒に考えてみてください。

某企業に勤める A さんは、社内のセキュリティ管理を担当する責任者で、日々、業務におわれています。ある日、今までに経験したことのないトラブルに遭遇し、今、まさに会社全体の通常業務が止まろうとしています。そのトラブルは、法定管理が不要な利便性重視の設備から発生していて、会社としてあまり気にしていなかったことから、対応マニュアルすらなく、A さんは対応に苦慮します。その騒動の中、このトラブルに詳しい社員が運良く A さんの部下にいてくれたことで、事態は急速に沈静化。事無きを得て通常業務に戻すことができました。 さて、A さんは、今回の対応を社長に報告しなければなりません。

以下に示す①、②の報告のうち、あなたが A さんならどちらの報告をされますか？ はたまた、あなたが報告を受ける管理職なら、どちらの報告を受けたいですか？

①「・・・であり。今回のトラブルは、事無く対処できましたので、我が社の業務への影響はありません。」
②「・・・であり。今回のトラブルの問題点は、認識できましたので、我が社の業務への影響は最小限に抑えています。」

私が思うに、日本社会においては①のケースが多いのではないかと思います。それは、万全を期すことを美徳と考える日本企業において、問題を残すということを嫌う傾向があることと、十分な検討と対策を実施しているという自負に要因があると考えるからです。そのために、法的に関係する事象以外の、すぐに沈静化するようなトラブルは、管理者として責任を負うような事象としたがらず、セキュリティ担当者としてもできれば運用の範疇で納めたがるなど、どうしても組織として事を荒立てないマインドになりがちのようです。

では、このようなケースのトラブルは、どこまでが企業として責任を持つリスクとして認識すべきなのでしょうか、それともリスクはないのでしょうか。私は、リスクを主観的でなく客観的に評価するプロセスさえ取り入れれば、ある程度明確な線引きができるのではないかと思うのです。すでに、リスクに対する投資効率を管理するために、リスクの見える化（リスク分析）を始めている企業も存在していますが、社会全体としてはまだまだのようです。

今年は報道等で、企業の法違反行為が世間を賑わせていますが、なぜ問題が起きたのでしょう。たぶん、社会との繋がりの深さを忘れ、リスクの意識が薄れたからではないでしょうか。私もこの社会に１つ不安を抱いています。近年の IT 化の進展はすさまじく、企業の飽くなき利益追求と相まって IT による効率化は企業の根幹部分のみならず組織全般にまで浸透しており、IT 化による便利さ（業務の効率改善）は、十二分に感じ、言われないと気づかないくらい当たり前のこととなっています。

しかし、この IT 化による便利さには、それだけでなく、便利さ故のリスクも混在しており、内在するリスク認識の甘さからセキュリティ対策を疎かにしてしまうと、想像もしがたいトラブルを引き起こすこともあるということを忘れてはいけません。気付いた時には、今まで積み重ねてきた信頼を全て失うこともあるのです。自社だけが被害に遭うのであれば何とかなるかも知れませんが、企業は一般的に、お客様や、取引先等多くの関係において社会と繋がっていて、その繋がりも今や IT が深く関与しており、リアルタイムに影響が伝播されてしまうなど、益々自社だけの責任では済まされない社会環境になりつつあります。

故に、企業のセキュリティ対策は、リスクを曖昧に考えないことをお勧めしたいと思います。そうしないとどうでしょう。リスクに対して、どう対応していいかわからなくなる部分が増え、どうしてもセキュリティ対策が疎かになりがちになると思うのです。逆に、リスクを客観的に認識さえすれば、どう対処すればよいかが自ずと見えてくると考えます。更に、客観的にリスクと向き合いリスクを意識しだすと、どんなに対応してもリスクというものは完全には無くせないことと共に、極めれば極めるだけ、時間と費用が掛かることに気付くと思います。これを解決するのは、是非、事業の経営判断と社会との繋がりの深さを再確認して頂き、組織として対応すべき責任の限界を見極

めていただければと思っています。これこそが社会的責任（CSR：Corporate Social Responsibility）ではないかと私は考えます。

最後に、来年は皆さんにとって良い年であることをお祈りします。

（HH）

【編集後記】

２００７年も残すところあとわずかとなりましたが、皆様にとって今年はどんな年でしたでしょうか？

NISC のホームページでも既にお知らせしていますが、「政府機関の情報セキュリティ対策のための統一基準」については、定期的な見直しの結果、第３版の案が公開され、皆様からのパブコメを募集しております。ご興味のある方は、ご一読の上、忌憚ないご意見を賜れれば、幸いです。

http://www.nisc.go.jp/active/general/kijun3.html

＜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