NISC NEWS

第２０号（２００８年５月２０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

【 評価2007とセキュア・ジャパン2008（案）について 】

４月22日に開催された第17回情報セキュリティ政策会議の決定に基づき、現在、セキュア・ジャパン2008（案）のパブリックコメントを募集していますので、以下に概要をご紹介します。我が国の情報セキュリティ対策に係る中長期の戦略である「第１次情報セキュリティ基本計画（2006年２月２日決定）」では、毎年度、より具体的な施策の実施プログラム「セキュア・ジャパン」を定めることとしています。3年目に当たる本年度の「セキュア・ジャパン2008」では、昨年度の「セキュア・ジャパン2007」に基づいた取組みに対する評価と分析（以下、評価2007と呼ぶ）を踏まえつつ、取り組むべき施策を掲げています。

１．評価2007

評価と分析のポイントは以下のとおりです。

○総評

・官民の情報セキュリティ対策のための体制維持、対策推進の安定化へ向けた取組みが懸命に進められました。
・各対策実施領域の取組み状況に一定の進展があり、「官民における情報セキュリティ対策の底上げ」も進んだものと考えられます。
・情報セキュリティに関するリスクの大幅な軽減はみられず、情報セキュリティ政策の社会的効果は十分な判断がつかない状況です。
・現行技術水準の限界もあると考えられ、対策水準の向上には体制の強化、効率的な対策の推進が引き続き求められます。

○対策実施4領域

【政府機関】2006年度と比較し対策実施に一定の成果が見られるが、対策が不十分な部分や課題は残りました。目標達成に向けた取組みが必要です。

【重要インフラ】行動計画に基づく取組みを推進、事業者等の情報セキュリティ対策の向上を確認しました。情報共有体制は活発な運用になお時間を要します。IT障害を発生させる要因や脅威は常に変化し続けることから、継続的取組みが必要です。

【企業】対策、体制の強化は徐々に進められています。しかし、対策の著しい伸びはみられず、一部に「対策疲れ」の声もあり、取組み推進の「均衡点」、現行技術水準の「限界点」に到達しつつあるとも考えられます。
【個人】総体的には、意識の向上、対策実施等は着実に進められるが、属性間に格差もあります。格差是正を含めた全体の底上げが更に必要です。

○横断的な情報セキュリティ基盤

【技術戦略】政府全体として情報セキュリティ分野へ重点投資を進める環境整備が進展しました。次世代OS環境の開発は着実に進展しており、課題解決型の技術開発も数多く行われました。
【人材育成・確保】官民における取組みを展開、展開を通じ人材育成の広まり、意識の浸透がみられました。十分な人材育成・確保には時間を要し、取組みは発展の途上です。
【国際連携・協調】日本の取組みの認知度は向上（窓口としての認識）しました。基本方針を策定し、国際連携・協調に向けた取組みを本格化し、さらに取組みの具体化を図ることが課題です。
【犯罪取締り等】捜査能力や体制の構築については、一定の取組みができましたが、取組みを継続し、加速化させる必要があります。権利利益の保護・救済についても、対応が十分とは言えないため、対策の一層の強化が必要です。

○社会情勢

【人的側面】社会ニーズに応える十分な人材の確保には、まだ時間を要します。引き続くリスクにより、情報セキュリティに係る意識は徐々に高まっています。
【物的側面】大幅な変化はないものの、堅実な投資、対策が着実に行われる状況です。研究開発・技術開発の取組みが着実に進められています。
【インシデント等】情報セキュリティに係るリスクは低減しておらず、経済的利得を狙う攻撃等、依然として攻撃の目的や、手段は変化し続けています。

○SJ2007に基づく施策の取組み結果

9割の施策について2007年の年度内に推進できました。しかし、政府機関対策に係る施策で、体制や人員に課題がある側面もありました。

2.「セキュア・ジャパン2008」（案）

評価2007を踏まえ、セキュリティ対策を推進する体制の維持や、対策が不十分な部分の底上げを含めて対策推進の安定化を図ることを目的とし、「第1次情報セキュリティ基本計画」の実現に向けた最終年度に当たる3年目の取組みをまとめたのが、セキュア・ジャパン2008（案）です。「電子政府等の情報セキュリティ強化のための総合的な取組み」と「中期的取組みを必要とする課題への集中的な取組み」をポイントとし、19件の新規施策と138件の継続施策を2008年度の実施施策として盛り込みました。さらに、3年間の取組み結果や第2次基本計画（仮称）の方向性を念頭に置きつつ、喫緊に取り組むべき課題として「持続的な情報セキュリティ対策の推進体制の構築に向けた基盤整備」を重点として、2009年度に推進する22施策を提示しました。

それぞれのポイントにおける、主な具体的施策の例を、以下に示します。

○電子政府等の情報セキュリティ強化のための総合的な取組み

・「政府機関統一基準」に基づくPDCA サイクルの定着・本格的な評価の推進及び結果の公表
・電子政府の情報セキュリティを企画・設計段階から確保する（SBD）ための方策の強化
・政府機関情報セキュリティ横断監視・即応調整チーム（GSOC）の本格運用・能力強化

○中期的取組みを必要とする課題への集中的な取組み

・長期的な視野で抜本的な技術革新等の実現を目指す「グランドチャレンジ型」のテーマの検討

・アジア地域における情報セキュリティ政策会合の創設

・分野横断的な情報共有促進のための「重要インフラ連絡協議会(仮称)」創設の促進

○持続的な情報セキュリティ対策の推進体制の構築に向けた基盤整備

・情報セキュリティ人材の重点確保

・各専門分野情報共有スキームの連携性及び情報交換モデルに関する検討

セキュア・ジャパン2008の案は、NISC のホームページで詳細を見ることができます。皆様から広く意見を募集し、必要な検討を行った上で正式決定する予定です。パブリックコメントの締切りが5月22日と近づいていますが、ご興味のある方は、是非ご一読の上、忌憚の無いご意見を頂戴できれば幸いです。

2. 誰でもわかる情報セキュリティ用語

【 送信ドメイン認証 】

昨今、巧妙な「なりすましメール」の報告が急激に増えています。特別な出来事があった場合、例えば、海外の要人が来日したり、大きな災害があったりしたような時に、もっともらしい件名で、実在する政府機関のドメインやアドレスを送信元として詐称したメールが、しばしば送付されてきます。そして、添付ファイルを実行すると、多くの場合、ウイルスなどの不正プログラムに感染することになります。

このような「なりすまし」が可能なのは、インターネットのメールの FROM ヘッダは、形式さえ合っていれば任意の値を入れることが出来るからです。攻撃メールに限らず、権威ある組織や大手プロバイダの送信元アドレスをかたったスパムメールも少なくありません。

このような問題への対策の一つが、「送信ドメイン認証」です。送信ドメイン認証は、自組織のドメインから送信されるメールに対して、それが正当なサーバから出されたものであることを、受信側で検証可能とする技術です。これによって、自組織のメールシステムに送信元を偽った攻撃メールが入り込むのを防ぐと同時に、自組織を詐称した攻撃メールが送信された場合にも、自組織には責任がないことを証明することが出来ます。送信ドメイン認証には幾つかの方式がありますが、ここでは DKIM と SPF という2つの主要な技術をご紹介します。

・DKIM （DomainKeys Identified Mail）

公開鍵／秘密鍵を利用した認証方式です。送信サーバでは、秘密鍵を用いて生成した電子署名を全てのメールに付与します。メールを受信したサーバは、DNS（Domain Name System）に置かれた送信者の公開鍵を利用して署名を検証することで、真正なメールか否かを判定できます。

・SPF (Sender Policy Framework, RFC 4408)

送信側が DNS に公開する SPF レコードを用いて、受信側がメールの差出人のアドレスの正当性を確認する認証方式です。SPF レコードには、正規の送信サーバの IP アドレスのリストや判定条件が記述されており、受信側は接続している送信サーバの IP アドレスと照合することによって、メールが正当なメールサーバから送信されたものかを判定できます。

送信ドメイン認証を利用するには、送信サーバと受信サーバの双方での実装が必要となりますが、攻撃メールは政府機関や独立法人、大手プロバイダなどを詐称するケースが多いので、これらの組織が送信ドメイン認証に対応していけば、その効果は非常に大きいと言えます。既に携帯電話事業者やプロバイダでは送信ドメイン認証の採用が進んでおり、さらなる普及が期待されます。

3. NISCOLUMN（ニスコラム）

【 情報セキュリティもポジティブに 】

社会のIT化が進んで、大変便利な世の中になってきたと感じます。仕事の面で、電子メールやグループウェアなどを活用して、業務の効率化や生産性向上が図られはじめたのは、もう大分昔の話になりますが、今はプライベートでも、ネットショップを活用すれば、わざわざ実店舗に出かけなくても日常の用はほとんど足りるようになっています。

そのような本来ポジティブに捉えるべき状況であるにもかかわらず、情報セキュリティの視点からは、「ITへの依存が更に進み、リスクが増大」とあたかも悪いことのように語られがちです。その他にも、情報セキュリティの世界では、例えば「脅威」「脆弱性」のようにどちらかというとネガティブな言葉が良く使われます。したがって情報セキュリティ対策は後ろ向きの対応と考えられやすいのだと思います。

実際にその通りで、情報セキュリティに関する教育・研修を受けたりすると「～してはいけない」のオンパレードで、制限をかけようという発想が随所に見られます。ITを活用して、まだ世の中にはない新しいサービスを作り出して活用するには、本当は自由な発想が求められるはずなのに、それとは逆行しています。

また、社会のIT化に伴って、情報セキュリティの範囲が広がっているように感じます。情報セキュリティ対策といえば、昔はコンピュータウイルス対策など技術的対策中心のイメージでしたが、ISMS認証制度の開始に伴って組織マネジメントの観点が入り、個人情報保護法に代表されるような法令順守の視点も加わり、昨今は内部統制報告制度や事業継続マネジメントなど、企業の経営全般に係わってきているテーマになってきています。そのような変化に意識が追いついていない場合に、どうしてもネガティブにとらえてしまうのではないでしょうか。

情報セキュリティはセキュア（＝安全・安心）な状態をめざすことが目標にあると思います。IT障害や情報漏えいなどが発生することを軽く考えるわけではありませんが、社会全体から見れば局所的な出来事であり、必要以上にネガティブにとらえるべきではないと思います。それより情報セキュリティ確保のために、大勢の人々が多くの対策に取り組みながら、適切に回しているという姿の方が、より現実を鳥瞰した状況ではないでしょうか。このような安全・安心を確保するための不断の努力の方にスポットライトを当てて、もっとポジティブに語られるようなものにしたいですね。

（バム）

＜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