NISC NEWS

第２号（２００６年５月１８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．トピックス

【「セキュア・ジャパン2006」（案）について】

「セキュア・ジャパン2006」（案）とは

2006年4月28日の**第5回情報セキュリティ政策会議**(注)**において、「セキュア・ジャパン2006」のパブリックコメント案が決定**されました。**「セキュア・ジャパン2006」（案）は、**我が国の情報セキュリティ問題全般についての3年間の計画（2006年度～2008年度）である「第1次情報セキュリティ基本計画」（2006年2月2日情報セキュリティ政策会議決定）を実現するための、**2006年度における実施プログラム**であり、**「2006年度の実施計画」**と**「2007年度の重点施策の方向性」**から構成されています。

「2006年度の実施計画」では**「官民における情報セキュリティ対策の体制の構築」を重点**として、**133の具体的施策**を推進することとしています。また、**「2007年度の重点施策の方向性」**では、**「官民における情報セキュリティ対策の底上げ」を重点として、2007年度に推進する施策の方向性**として、**26の施策**の方向性を提示しています。

これらの主な施策例は、「政府機関・地方公共団体」、「重要インフラ」、「企業」、「個人」の各主体に対し、「個別推進施策」「横断的推進施策」及び「2007年度重点施策の方向性」として、図1に示してあります。

「セキュア・ジャパン2006」（案）の詳細については、

- 「セキュア・ジャパン2006」（案）の概要
  http://www.bits.go.jp/conference/seisaku/dai5/pdf/5siryou0301.pdf
- 「セキュア・ジャパン2006」（案）
  http://www.bits.go.jp/conference/seisaku/dai5/pdf/5siryou0302.pdf
- 第1次情報セキュリティ基本計画と 2007 年度の重点施策の方向性との対応
  http://www.bits.go.jp/conference/seisaku/dai5/pdf/5siryou0303.pdf

を御参照下さい。

この、「セキュア・ジャパン2006」（案）については、**5月26日までパブリックコメントを実施**しております。
※詳細は、http://www.bits.go.jp/active/kihon/sj2006.html をご参照下さい。

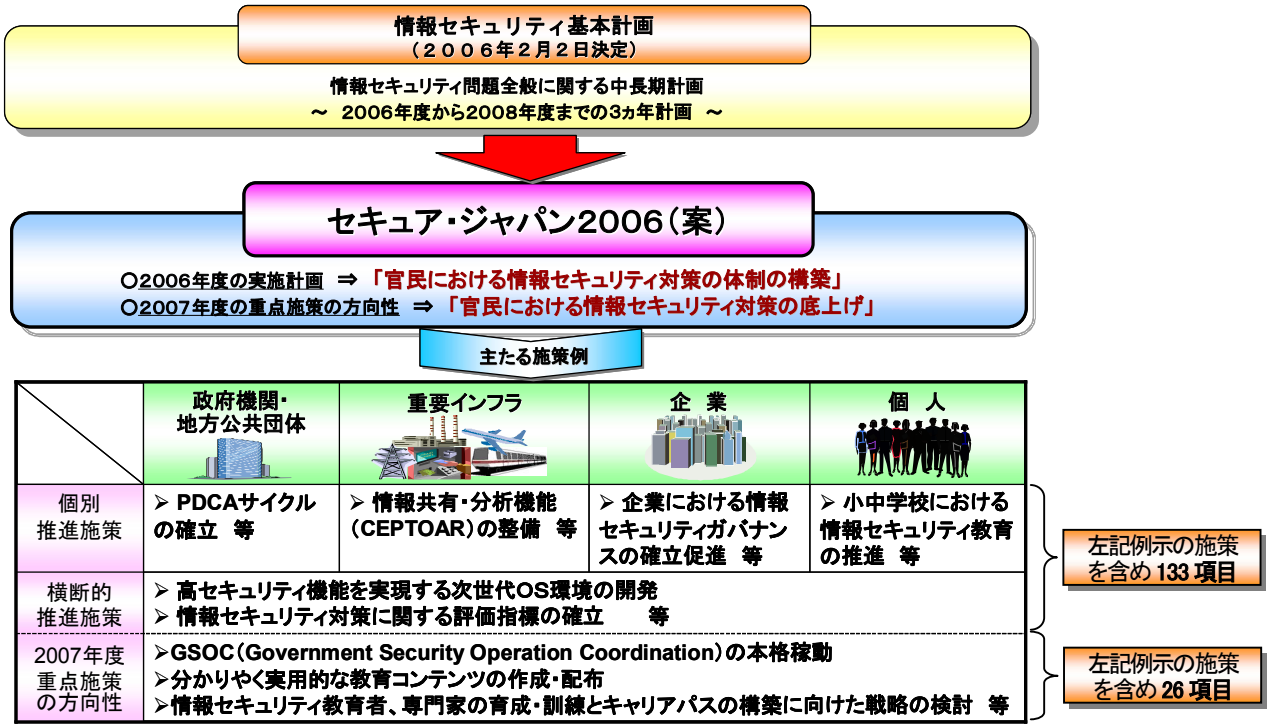

図1 「セキュア・ジャパン2006」（案）と各主体に係る主な施策例

（注）情報セキュリティ政策会議

情報セキュリティ政策会議は、我が国の情報セキュリティ基本戦略等、**情報セキュリティに関する問題の根幹に関する事項を決定する母体**として、2005年5月30日に高度情報通信ネットワーク社会推進戦略本部（IT戦略本部）の下に設置されました。本会議は、**内閣官房長官を議長、情報通信技術（IT）担当大臣を議長代理とし、情報セキュリティに係る国務大臣及び民間有識者から構成**されています。

情報セキュリティ政策会議は、関係省庁と連携しながらその事務局を務める内閣官房情報セキュリティセンター（NISC）と共に車の両輪として、我が国の情報セキュリティ問題に関する中核機能を形成します。

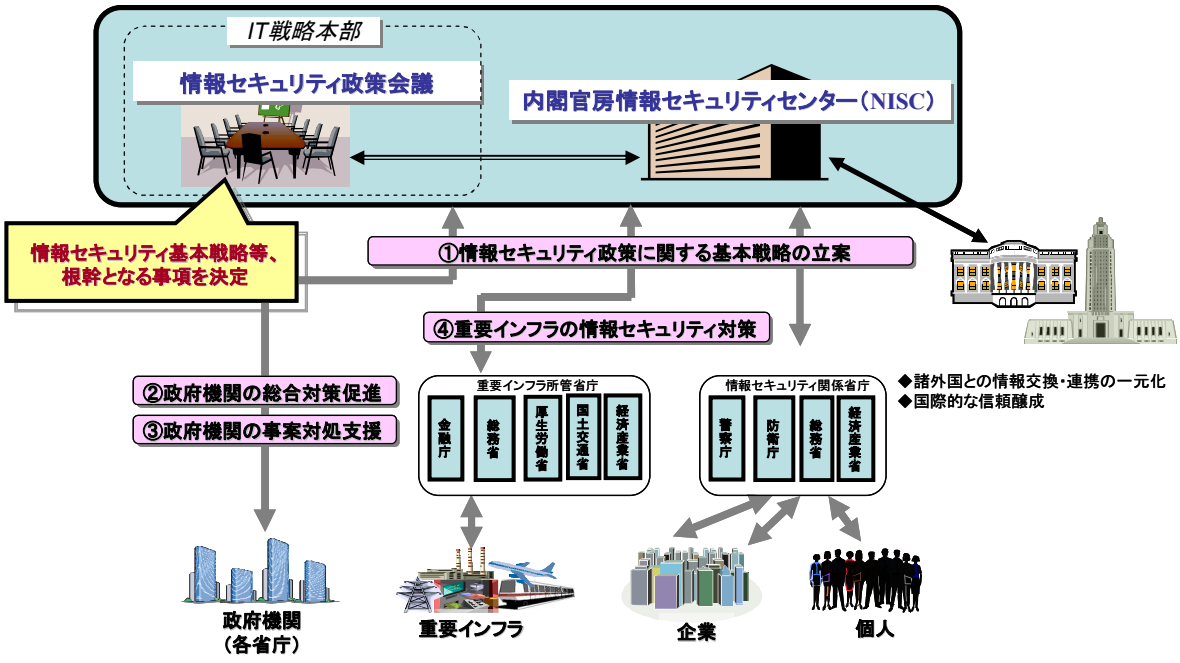

図2 情報セキュリティ政策会議と内閣官房情報セキュリティセンター

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」

【観測無くしてセキュリティ対策無し】

情報セキュリティ対策における「技術」の役割は多種多様である。ファイアウォールのように通信制御を行うものや、ネットワークへのアクセスを管理するVPNゲートウェイやRADIUS等の認証システム、不審な通信を検知する侵入検知装置（IDS）等が真っ先に思いつくものだろう。更には、様々なセキュリティ対策が施されたメールサーバやWWWサーバも、当然情報セキュリティ対策の一環として技術が積極的に活用されるところだ。

情報セキュリティ管理者の重要な役割として、管理対象のネットワーク環境において、どのような技術を導入し、どのように運用するのかを体系的に設計し、実装することが挙げられる。別の言い方をすれば、情報セキュリティ対策のための技術活用フレームワークを決めて、運用することと言える。

このフレームワークを決めるときには、組織の規模、業務内容、情報システムの利用形態、従業員数等、数多くの要素を考慮しつつ、同時に情報セキュリティ対策に投じる事ができる予算や人員の制限にも気配りしながら設計を行う。このため、組織毎にカスタマイズされ、特色あるフレームワークが生まれる。

ところが、このフレームワーク設計の段階で、管理者が陥りやすい失敗が幾つかある。その代表的なものが、現在の情報システムとネットワークがどのように使われているかを知るための観測系（監視系）システムを体系的に組上げることに失念した結果、個々のシステムの運用状態は分かっても、全体として何が起きているかが分からない状況が頻発する状況を自ら作り出してしまうことだ。特に情報セキュリティ対策に投じる予算が限られた状況では、この失敗をしやすい。

情報セキュリティ対策のPDCAサイクルを回すためには、現状のシステムがどのような状況に置かれているのかを把握し、さらに情報セキュリティ対策を施した事により何が変わったのかを知る事が必須だ。このプロセスが実行できなければ、実装した対策が適切な対策だったかどうかを検証することができず、結果として改善方策も適切なものにならない可能性が高まってしまう。

情報セキュリティ対策のフレームワークを考えるときには、必ず観測系をどのように構築するのかを真剣に考えなければならない。暗闇の中をライトも持たずに歩き回るような状況を作り出すのは愚の骨頂である。

（山口　英　内閣官房情報セキュリティ補佐官）

3. 情報セキュリティQ

暗号文に対する攻撃方法も様々あり、例えば「X個のデータの中からY個をランダムに選択した際に、その中に同じデータが2個以上存在する確率」の考えを利用した攻撃方法として、「暗号文一致攻撃」というものがあります。そこで、この考えに基づいた場合、少なくとも何名集まれば、同じ誕生日の人が含まれる確率が約1/2になるでしょうか。

①　13名　　②　23名　　③　53名　　④　103名　　⑤　365名　　⑥　①～⑤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「④　パキスタン」でした。コンピュータウイルスの発祥国は諸説ありますが、現時点で最も有力な説と

しては、パキスタンのとあるプログラマーが、1986 年に自分で作成したソフトウエアが不正コピーされていたことに対し、警告の意味で作った自己感染プログラムが最初と言われています。つまり現在のような悪質なコンピュータウイルスを意図して作られたわけではありません。その証拠に、コードの中には「駆除ワクチンが欲しい方は当方まで連絡を下さい」というメッセージとプログラマーの電話番号を入れてあったそうです。

4. NISCOLUMN（ニスコラム）

【障害対応時にこそ真剣に考えたい本当の情報セキュリティ対策の意味】

この4月から政府統一基準を担当することになったが、それまでは当センター発足以来、重要インフラの情報セキュリティ対策の推進を担当してきた。その間、何度となく重要インフラの IT 障害が発生し、国民生活や経済活動に大きな混乱を巻き起した。

そのたびに、IT が未完の技術であること、その IT が重要インフラのサービス提供の中枢部に浸透しつつある現状を考えると、情報システムの構築・利用に関わる組織全体の「人間力」によってこれを御していく意外に方法がないことを痛感させられる。

障害を起こした企業（主として情報システムの利用企業）の記者会見では、カメラを前に企業幹部が深々と頭を下げるという光景が最近ではすっかり定着してしまった。さらに、多くの会見の最後に企業経営者の口にする言葉も、「想定外だった。」、「あってはならないこと。」、「徹底した原因究明と再発防止に万全を期す。」など決まり文句でくくられる。言葉の意味する内容が不明確なこと以上に、本当の原因や責任の所在に経営層が気づいているのか？本当に適切な再発防止策が講じられるのか？私の不安はますます増大する。

対策基準を考える立場からみると、「想定外」とは脅威想定が問題だったという意味だし、「あってはならないこと」とは、ルール（規程）はあってもその運用実態がチェックされていなかったことを意味する。さらに、「遺憾だ」と自分に責任があるのかないのか曖昧な言葉で締めくくるトップも多いが、これも情報セキュリティに関わる組織体制と責任分担が明確に決まっていなかったことを意味する。組織力で情報セキュリティを確保する仕組みの重要な基礎が欠落していたことを各社のトップが公然と認めているのだ。

情報セキュリティには重要度が増す反面、経営資源（人・モノ・金）が十分に配分されないという構造的な問題がある。こうした状況に、都合の悪い情報ほど経営幹部に伝わりにくいという大企業の病理が加わるために、経営者層に適切なアセスメントと処方箋を考える機会は何か起こらない限り訪れることはない。不幸にして既に障害を起こしてしまった企業の経営者にも、万が一、「当面の嵐をやり過ごす」という感覚で受けとめられているとしたら、国民の IT 障害に対する不安は永久に解消することはないだろう。

（弁慶号）

＜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.bits.go.jp/nisc-news/

＜御意見、御感想＞

http://www.bits.go.jp/mail.html