NISC NEWS

創刊号（２００６年４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)

創刊にあたって

読者の皆さん、こんにちは。

内閣官房情報セキュリティセンター（NISC）センター長の栁澤です。「NISC NEWS」の創刊にあたり、当センターが進める情報セキュリティ政策について紹介させていただきます。

昨今、高度情報通信ネットワーク社会が現実のものとなり、我が国の国民生活・社会経済活動において情報技術（IT）への依存度が高まってきています。こうした状況の下、最近では、情報通信基盤の急速なブロードバンド化や電子商取引の浸透などに伴って、世界規模でのコンピュータウイルスの蔓延、サイバー犯罪の増加、国民生活・社会経済活動の基盤となる重要インフラにおける情報システムの障害、大量の個人情報の流出等が社会問題化していることはご存知のことだと思います。そのため、ITを安全・安心に活用するための取組み、すなわち情報セキュリティ対策の強化が、我が国にとって喫緊かつ重要な課題になっています。

こうした流れの中で、2005年4月25日に当センターが設置され、同年5月30日に設置された情報セキュリティ政策会議（議長：内閣官房長官）の事務局を務めながら、車の両輪として我が国の情報セキュリティ対策の中核機関として、我が国全体としての情報セキュリティ対策の抜本的な強化に取り組んでいます。

そして今年の2月2日には、情報セキュリティ政策会議において、我が国の情報セキュリティ問題についての今後3年間（2006年度～2008年度）の中長期戦略として、「第1次情報セキュリティ基本計画」が決定されました。これからは、「第1次情報セキュリティ基本計画」に沿って、政府が一丸となり、我が国全体の情報セキュリティ対策に取り組んでいくこととなります。このNISC NEWS は、情報セキュリティ問題について広く皆さんに知っていただく場となることを目的として、発行することとしました。

今後は、官民を問わず幅広い情報セキュリティ対策に関する取組みの紹介、情報セキュリティに関する基礎知識や時節にあったトピックスなど、様々な内容を盛り込むことを予定しております。また、内容に対するご要望・ご質問等ありましたら、当センターまで遠慮なくお知らせいただけると幸甚です。

目次

1．情報セキュリティ施策紹介

（1）「第１次情報セキュリティ基本計画」って何？

証券取引所の取引システムが停止したり、飛行場の管制システムが正しく動作しなかったり、あるいは学校や役所から個人情報が流出したり、これらはすべて情報セキュリティを巡る問題としてとらえることができます。ますます複雑化し、そして多発する傾向にあ

るこれらの問題に取り組むために、２００６年２月２日に「第１次情報セキュリティ基本計画－『セキュア・ジャパン』の実現に向けて」が策定されました。

まずは次の３つの柱を、我が国が情報セキュリティ問題に取り組む上での基本理念として定め、今後「情報セキュリティ先進国」となることを目指します。

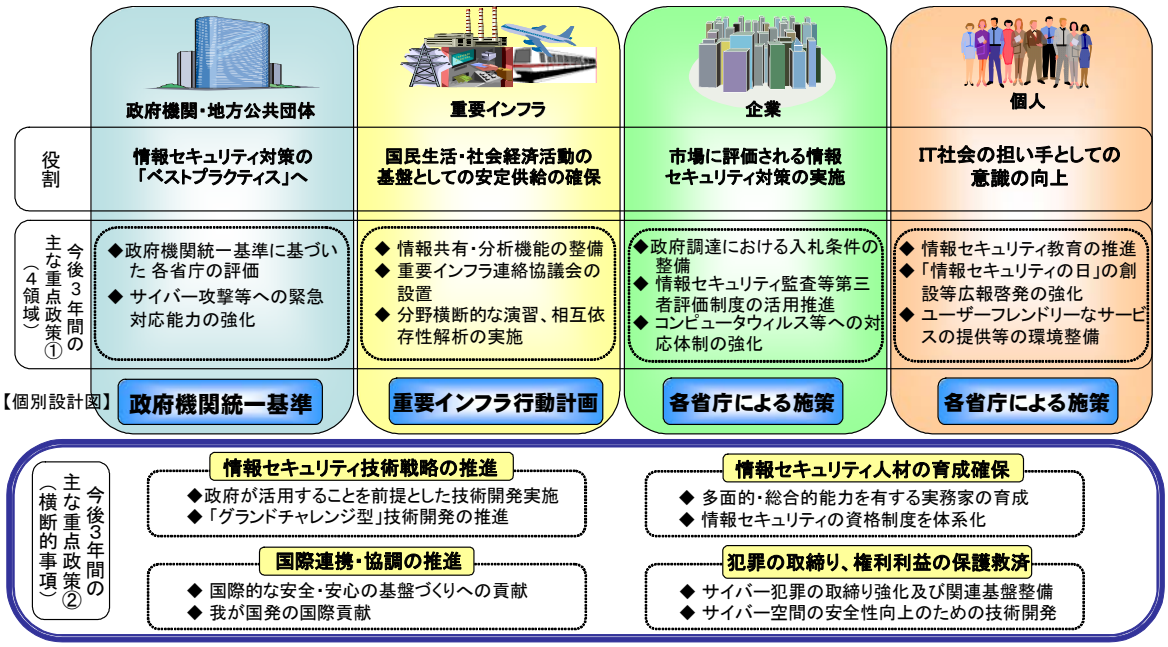
＜３つの基本理念＞

１）経済国家日本の持続的発展を支える情報セキュリティ
２）安全・安心で、より良い国民生活を実現するための情報セキュリティ
３）我が国の安全保障におけるＩＴに起因する新たな脅威に対応するための情報セキュリティ

その上で、２００９年度初めまでに達成する目標として次の４つを掲げました。

- すべての政府機関が「政府機関統一基準」が求める水準の対策を実施
- 重要インフラにおけるＩＴ障害の発生を限りなくゼロに
- 企業における情報セキュリティ対策の実施状況を世界トップクラスの水準に
- 「ＩＴ利用に不安を感じる」とする個人を限りなくゼロに

これらを踏まえた上で「新しい官民連携モデル」の構築に向けて、今後３年間、各種の対策を強化していきます。情報セキュリティ問題への取組みは、政府だけが行うものでも、民間主体だけが行うものでもなく、我が国全体として、英知を結集しながら行うことが必要です。



(2)「政府機関の情報セキュリティ対策のための統一基準」って何？

今やITは国民生活、行政活動に必要不可欠な基盤として発展しているところですが、その一方で、例えばファイル交換ソフトウェア「Winny」を介して感染するコンピュータウイルス「Antinny」によってパソコンから行政機関等の重要情報が流出する事案が発生するなど、情報セキュリティに関する問題が国民生活や社会経済活動に対して多大な影響を与える存在となっています。こうした中、昨今増大する情報セキュリティに対する脅威に対して、政府機関における情報セキュリティ対策は欠くことができないものとなっています。

これまで、政府機関の情報セキュリティ対策については、各府省庁がそれぞれ独自に情報セキュリティ対策の基本的な考え方と対策基準を定める「情報セキュリティポリシー」を作成し、個別に取り組んできました。これによって、各府省庁において情報セキュリティ対策が実施されていたものの対策内容・水準はまちまちでした。また、急激なIT環境の変化に対して情報セキュリティ対策を実施する人材が全体的に不足しているなどの問題も指摘されています。

こうした状況を受けて、政府機関全体としてより高い情報セキュリティ水準を確保するための取組みを進めるため、共通に採るべき情報セキュリティ対策として、昨年12月情報セキュリティ政策会議において「政府機関の情報セキュリティ対策のための統一基準」を定めました。これを踏まえて各府省庁が情報セキュリティポリシーを見直すことにより、政府機関全体での底上げを図ることとしました。

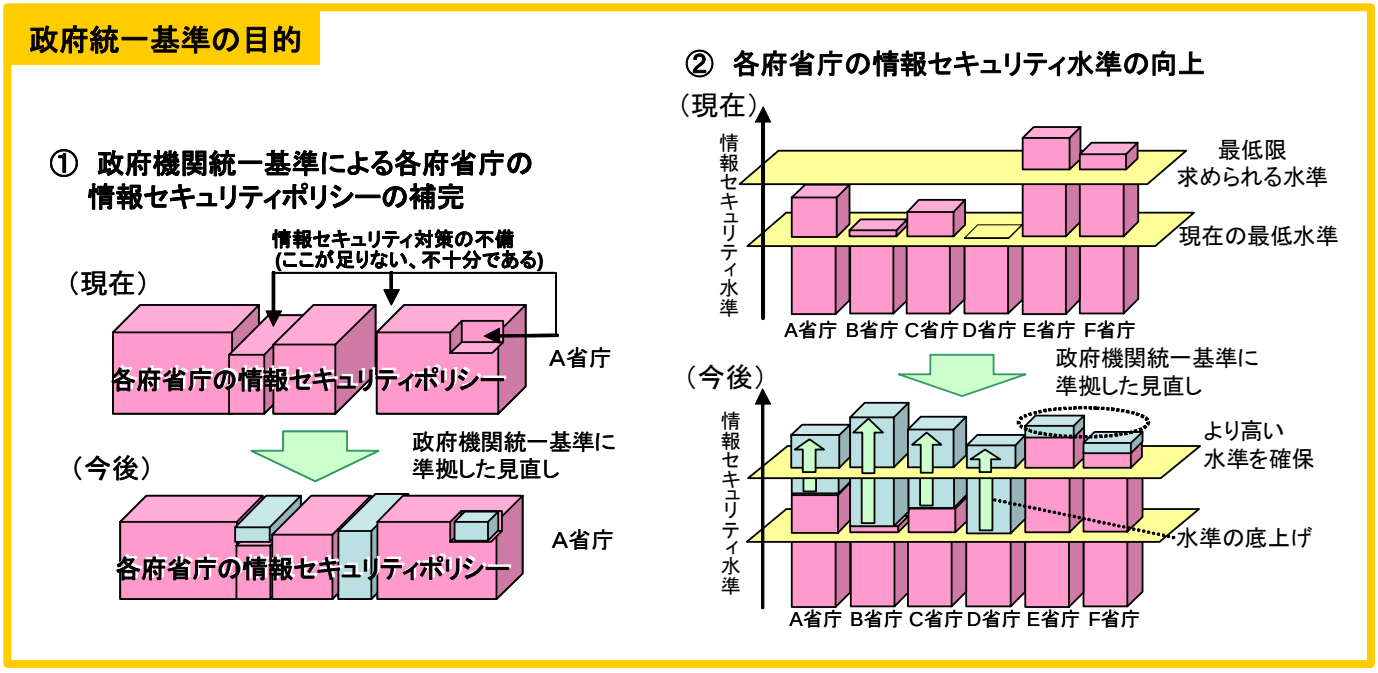
では、政府機関統一基準にはどんなことが盛り込まれているのでしょうか。Winny を介した情報流出を例に、対応する政府機関統一基準の

対策を挙げてみると

- 情報の持ち出しに関する規定の整備
- 私物パソコンを業務に使用する場合の安全管理措置の整備
- 情報システムに対するアクセス制御・権限管理機能の付与
- 重要な情報の暗号化
- 外部委託を実施する際の、委託先が遵守すべき事項を含めた契約書の取り交わし

などです。このように幅広く情報セキュリティ対策に必要な対策基準を定めています。

さらに今後は、各府省庁において自己点検や監査によって、これらの対策の実施状況を把握するとともに、内閣官房情報セキュリティセンター(NISC)が、各府省庁における対策状況を検査・評価して、情報セキュリティ政策会議に報告していく予定です。これによって、政府全体での政府機関統一基準に基づいた対策の徹底を図っていきます。



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」

【教育・啓発活動を忘れてはならない】

最近多くの方々が、情報セキュリティ管理の基本的な考え方を、従来の「性善説」から「性悪説」に変えなければならないと指摘している。昨今の情報システムに関わるトラブル発生の状況を見れば、利用者が何か悪いことをするかもしれないという仮説を立ててシステムを構築・運用するのは当然だと考えるのも納得できる。また、万が一トラブルが発生すれば、そこから直接損失を被る状況になっており、トラブル発生回避に全力を尽くし、結果として幾重にもシステムを守る対応をすることになってしまうのもよくあることだ。

しかし、手厚い対策を施しても、やはりトラブルを引き起こしやすい環境ができてしまうことがある。情報システムを取り巻く状況には、どのようなリスクがあり、そのリスクが顕在化したときには、具体的にどのようなトラブルが発生し得るかという考え方が、システム構築運用側と利用者側で共有されていない環境では、対策の厚さと関係なくトラブルが発生しがちなのだ。この意味で、情報セキュリティ対策では、必ず利用者のスキルアップ、認識改善を目的とした教育・啓発活動が必須になっている。

この教育・啓発活動は短期間には目に見える効果が現れないかもしれないが、長期的には着実な効果を上げることは言うまでもない。現在、大学や企業において、情報セキュリティ教育・啓発活動をどのように効果的に行うのかという点について、数多くのチャレンジが生まれてきている。しかし、やらねばならぬ事が山積である。教育方法とその内容について十分に体系化されているわけではなく、取組みに携わる人達の間でノウハウや種々の知見を共有し、全体の底上げが必要である。その観点から、さまざまな取組みについて「恥ずかしがらず」情報交換をするようになっても良いのではないかと思っている。とかく、大企業や行政組織となると「ちゃんとやっています」と言う嫌いがあるが、教育・啓発活動だけは見栄を張らず、より積極的に情報交換を行い、正しい現状認識を持ち、本当の意味で解決方法を考えることが必要になってきていると考える。

（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

【ウイルス、ワーム、トロイの木馬】

コンピュータウイルス（ここでは単に「ウイルス」と記述します）については、平成7年に当時の通商産業省が発表した「コンピュータウイルス対策基準」に明確に定義されています。詳しい内容はここでは省略しますが、要約すると「意図的に何らかの被害を及ぼすように作られた」プログラムのことです。一方で、「ワーム」や「トロイの木馬」という言葉もよく耳にしますが、それではこのワームやトロイの木馬はウイルスなのでしょうか。答えはイエスでもあり、ノーでもあります。

ワームは自己増殖し続ける不正プログラムの総称です。これ自体で直接的に被害を及ぼす訳ではないことから、狭義のウイルスには当てはまらないとされています。

トロイの木馬はどうでしょう。これは正体を偽ってコンピュータに侵入し実行されるのを待つプログラムですので、これも狭義のウイルスには当てはまりません。ただ、どちらも通常のウイルスと組み合わせて仕掛けられることが多く、それが新たな破壊活動のための窓口として利用されることも多いので、広い意味でウイルスと呼ばれることもあります。なお、これら悪意のあるプログラムから自分たちのパソコンを守るためにも、少なくともウイルス対策ソフトは常に最新の状態にしておき、対脆弱性パッチを速やかに適用することを心掛けるとともに、怪しげなサイトにアクセスしたり、不審なメールやファイルを安易に開かないこと等に日頃から注意することも大切です。

4. 情報セキュリティQ

ファイル交換ソフトウェア「Winny」を介して感染し情報流出を引き起こすコンピュータウイルス「Antinny」や、ネットワークを介して次々とコンピュータに侵入し、乗っ取った後に、さらに別のコンピュータに感染して DoS 攻撃（サービス拒否攻撃）を誘発する恐れのある「Blaster」等、現在世界中で深刻な被害を及ぼしているウイルスは枚挙にいとまがありません。

そもそもウイルスは、1986 年にその存在が初めて確認されたと言われていますが、そのウイルス発祥（発症？）の国とは次のうちどれでしょうか。

① アメリカ　② 日本　③ イスラエル　④ パキスタン　⑤ インド　⑥ ①～⑤以外の国

（なお正解は、次号にて掲載致します。）

5. NISCOLUMN（ニスコラム）

【知る人ぞ知る情報セキュリティ】

先日、食品添加物に関する書籍を読む機会がありました。その中で、むやみに添加物のことを非難するのではなく、我々の現在の生活が添加物から切り離せないものであり、ただ消費者はあまりにその実態を知らされていないことが問題であるという内容が述べられていました。私自身、これまではラベルに記載されている原材料のうち、日本語で書かれているものは安全で、カタカナ表記のものは不安であるという漠然とした感覚を持っていましたが、それは大きな誤りだと悟りました。知らなければ消費者としての選択すら出来ず、日々口にするものの管理すらままならないというのがどうやら現状のようです。

翻って、情報セキュリティとはリスクが存在することが前提であり、リスクそのものを認識し、その対策の選択肢を知らなければ、リスクを適切に回避することができないという点では、先述の食品添加物の例と類似しています。

筆者を含め、市民レベルで接する情報セキュリティとは、パソコンにウイルス対策ソフトウェアをインストールして定期的にパターンファイルを更新することや OS のアップデートに機敏に反応すること等が主な「すること」になっていると思いますが、実質その中身はというとよくわからない、多くの謎に包まれている、と感じる方も数多くいらっしゃるのではないでしょうか。

確かに対応マニュアルはあるし、最近では情報セキュリティを取り上げた雑誌等も多数発行されています。しかしながら、内容が難解で、訳も解らぬまませき立てられるように対策しているのが実情であり、何が脅威として存在し、それに対する対策はどこまで自分の使用している環境に備わっているのかが、しっかりと理解されていないことが問題であると感じざるを得ません。

ウイルス対策に限らず、情報セキュリティとは「知る人ぞ知る」ものであると感じるのは筆者だけではないと思います。誰もが、ある程度得心して自発的に対策をすることが望ましいのならば、国民に対し、もっと理解しやすい言葉で「情報セキュリティ」を解説していくことが、内閣官房情報セキュリティセンターの責務だと感じている今日この頃です。

（A. Y. ）

＜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