# NISC NEWS

**第９号（２００７年３月２３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

### 【 情報セキュリティ政策のＰＤＣＡサイクル構築 】

**１　政策のサイクルとは？**

このメルマガ読者の皆さんは、政策のサイクルというコンセプトをイメージされたことがあるだろうか？政策なんて企画して実施するだけだろうと思われる方も少なくないと思うが、最近の政策運営では、実施した政策の評価やそれを受けた改善を行って、次の新しい企画段階につなげていくという一連のサイクルを構築することが半ば常識となりつつある。こうしたサイクルは、政策のＰＤＣＡサイクル※1と呼ばれ、一つの政策において過去との継続性を持たせながら、より有効な企画を実現していくための手法なのである。政府が、スポンサーである納税者（tax payer）すなわち国民に対して、政策に取り組んだ結果としてどういう効果を実現できたのかといったことを説明し、また過去の取組みの反省に立って次の企画を行うのは当然であり、政府の説明責任という観点からも至極真っ当な手法と言えるだろう。

※１（計画(Plan)、実施(Do)、点検(Check)、改善処置(Act)）

**２　情報セキュリティ政策のＰＤＣＡサイクルの構築**

環境の変化の早い情報セキュリティ政策についても、ＰＤＣＡサイクルが必要であることは、疑いがない。情報セキュリティ政策は、内閣官房が総合調整を行いながら政府全体が協力して推進する体制が２００５年から稼動している。翌２００６年に、３ヶ年の中長期計画やそれに基づいた年度計画※2が策定されたことをもって、政策の計画と実施の段階は既に完了していた。

そして本年２月、情報セキュリティ政策会議はＰＤＣＡサイクル全体を完成させるために、点検段階（評価）、および改善処置段階についてどのようなスケジュールや方法で行うのかという枠組みを決定した。今後は、この枠組みに沿って継続的な取組みが進むことで、我が国の情報セキュリティが世界最高水準のレベルとなることが期待される。

※２　中長期計画は「第１次情報セキュリティ基本計画」、年度計画は「セキュア・ジャパン 2006（施策集）」をそれぞれ指す。

**３　評価及び改善処置の取組み**

情報セキュリティ政策のＰＤＣＡサイクルの下では、評価等の作業を毎年行うこととしている。具体的には、毎年９月を目途にＮＩＳＣがその年度の作業方針を策定し、それに基づいて各府省庁が必要なデータを把握した後にＮＩＳＣが取りまとめと分析等を行い、情報セキュリティ政策会議へ結果を報告する。また、評価の対象ではなくとも、社会の実情を把握したい点についてはＮＩＳＣが補完調査を各府省庁の協力を得ながら行うこととしている。

その上で、情報セキュリティ政策会議はＮＩＳＣからの報告に基づいて、省庁の対応を促したり、ＰＲのための情報発信を行うなど、改善のための取組みを推進することとなる。

### ４　２００６年時のリスクの認識、２００９年時の我が国社会の姿

今回のＰＤＣＡサイクル構築に際しては、他にも重要な検討がなされている。政策を企画する際には、通常、政策を必要とする現状の把握や、取組みを行った結果として目標時期に社会がどうなっているのかといった点についての検討が行われる。もちろん、情報セキュリティ政策においてもこれらの把握や検討はなされてきたが、今回、「基本計画策定時の現状（リスク）」と「目標時期の社会の姿」という形で改めて可視化がなされた。これによって、関係者以外にもＩＴ利用に関し社会が直面しているリスクが何であり、それが情報セキュリティ政策によってどう変わると考えられるのか、ということが理解しやすくなったと考える。

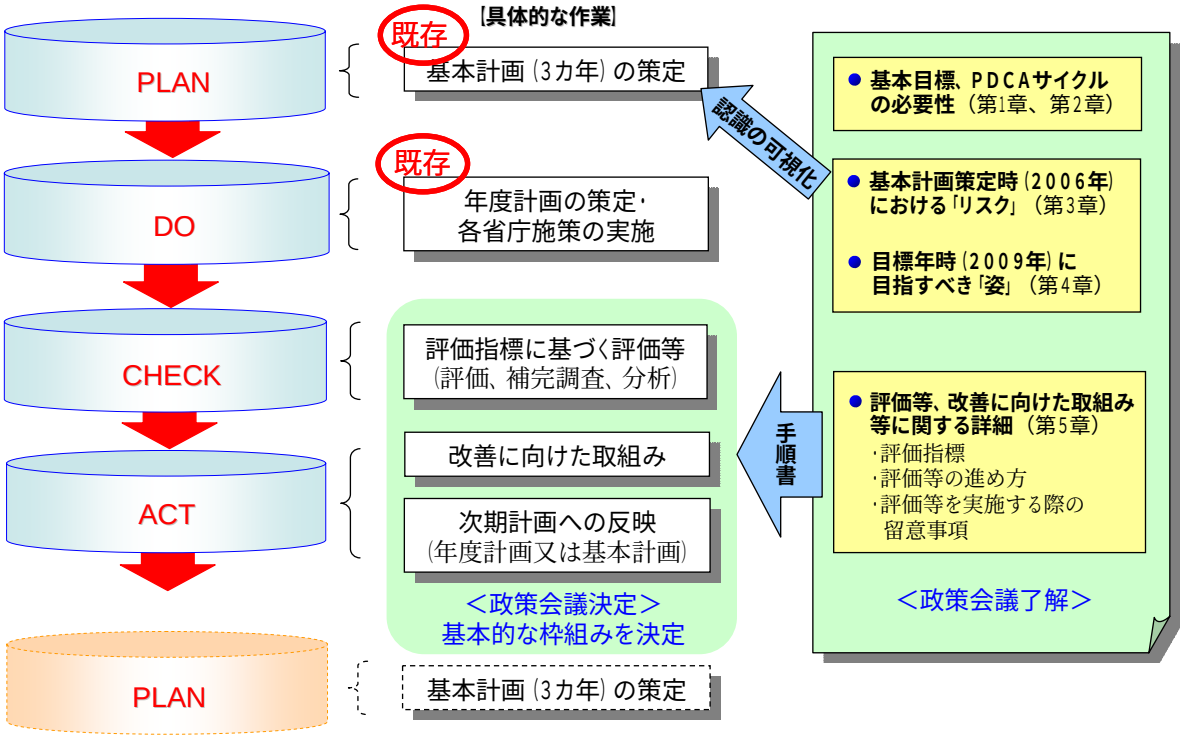


図　情報セキュリティ政策のＰＤＣＡサイクルと評価等の枠組み

このＰＤＣＡサイクルと評価等の枠組みについてまとめた文書は、ＮＩＳＣの以下のページにも掲載されているので、一度ご覧いただきたい。

http://www.nisc.go.jp/conference/seisaku/index.html#seisaku10
（資料２－１から２－４参照）

## 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」

### 【 ユーザは何もしてくれない 】

私が大学でコンピュータを学んだのは20年も前のことになってしまった。当時のコンピュータは本当に不親切だった。コンピュータに付随して提供される道具も限られ、使う側もそれなりの勉強をしなければ何もできない代物だった。しかし、コンピュータが何をしているかは良くわかったし、思い通りに使いこなすプログラムを書くのは幸せだった。ところが、最近のコンピュータは、本当に親切で便利なツールだ。ユーザは、誰かが作ったアプリケーションを使って色々な仕事ができる。何よりも、ユーザがプログラムを書かなくてもいいのだ。

こんな話をある方にしたら「これはね、自動車と同じ発展をたどっているんだよ」と言われた。昔は自動車を乗る

というのは知識と能力が求められたが、最近は、ユーザはユーザ以外の何者でもないものなのだと仮定して自動車は作られているのだと。確かに、最近の自動車でボンネットを開けてエンジン周りを何かしようと考える運転者はそんなにいない。何かトラブルがあれば、プロに任せようと考えるのが普通だ。そして、そんなユーザばかりだから、自動車メーカー達も通常の運転者に何かメンテナンス作業をさせようということを減らして、どんどん楽にしようとする傾向が強まっている。一部メーカーが提供している、メンテナンスサービスパッケージ付き販売などは、その典型だ。

自動車のことを考えると、今のコンピュータが提供している「かゆいところに手が届くサービス」の内容は、今の自動車が提供しているレベルまで達していないと言わざるを得ない。まだまだ、ユーザにシステムを直接さわらせ、いろいろなメンテナンス作業をさせようという気持ちがたっぷりある。そして、そのことが実は多くのセキュリティ関連のトラブルを生み出していることにもなっているように、私は考えている。ユーザが何らかのメンテナンス作業を、製品提供側が期待するようにやってくれるという仮定をおくことは、そろそろ限界なのではないか。

もちろん、激烈な市場競争をしている現在、製造コストが上がる方向に向かうのは、製品供給者としては向かいたくない方向であろう。しかし、ユーザは製品供給者が思うがごとく、素直に何かをしてくれると期待できるのだろうか。そんな仮定を置かずに、何もしないユーザでも、最新の技術を活用して快適に安全に利用できるコンピュータ環境が手に入り、かつ、その後も維持できるようになる方向に進むべきではないだろうか。

コンピュータ関連の製品開発をしている皆さんも、このメールマガジンを読まれているであろう。どうでしょう。そろそろそんなことも考えていただけたらなと、淡い期待を持っているのです。

（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

### 【　標的型攻撃　】

「標的型攻撃」は、不特定多数の相手ではなく、特定の企業や組織を狙ってかけられる攻撃のことです。英語では一般に”targeted attack”と表現されます。また、スピア(spear)という単語が槍を意味し、狙い定めたポイントを突いてくる様を表すことから、「スピア型攻撃」と言われることもあります。近年、マルウェア（悪意のあるプログラム）を配布する動機がビジネスすなわち金銭目的に移行しつつあることに伴い、このスピア型攻撃が数多く発生し、たいへん深刻な脅威となっています。

この攻撃の特徴は、マルウェアを添付したメールやフィッシング・メールを送りつける対象を絞ることで、被害者が罠にかかりやすくするための工夫、すなわちカスタマイズを行うことにあります。例えば、狙った会社の内部の部署名で、業務に関連がありそうな文面のメールを送れば、それを受け取った社員が添付ファイルを開く可能性は高くなるでしょう。また、オンラインショップのカスタマーサービスに、顧客を名乗る人物から「送付された商品が、添付の写真のように破損していた」という内容のメールが来れば、担当者は画像データに見せかけたトロイの木馬を実行してしまうかも知れません。このように、攻撃対象に関する「知識」を用いて、技術面だけでなく心理面からも攻撃をかけてくるのが、スピア型攻撃なのです。

スピア型攻撃のもう一つの問題は、セキュリティ対策ソフトが無効な場合も少なくないことです。対策ソフトのベンダーは、新しいマルウェアが発生した際に、その検体を解析することで新しいパターンファイルを作成し提供します。しかし、スピア型攻撃の場合には被害の対象が狭いので、そもそもベンダーが検体を入手することができず、その結果、有効なパターンファイルが作成できないために被害が拡大する可能性があります。このような攻撃に対しては、「セキュリティ対策ソフトをインストールし、最新のパターンファイルに更新しさえすれば安心」と気を抜くのではなく、添付ファイルの扱いにこれまで以上に思慮深い行動が必要になります。

## 4. NISCOLUMN（ニスコラム）

### 【 暖かい冬に熱い情報流出 】

今年の冬はかなり暖かく、街中に暮らすものにとっては過ごしやすい気候が続きましたが、ファイル共有ソフトを悪用するウイルスによる情報流出は変わらず熱い様相を呈していたようです。そんな中、情報流出の防止と対策に携わっておられる複数の方々とお話をする機会があったのですが、体感的にはこの1年ほどの間で流出自体はあまり減っていないとのことです。さすがに一時期に比べて世間を大きく騒がせるような事案は減ったものの、それでも決して少ないといえる状況にはないとのこと。全国的には報道されないものも結構あるようです。

推測される流出時の状況を伺うと、パソコンに重要な情報が残っていたことを失念していたと思われる場合もあるようですが、多くはウイルスの怖さを軽視しているか、パソコンに保存している情報の重要性を認識していないかのいずれかと思われるとのこと。中には、セキュリティ関連ソフトを入れているにもかかわらず、その機能を切って流出を起こしたことが推測されるものも少なからずあるようです。ファイル共有ソフトのネットワーク上には結構な数のウイルス付のファイルが流れていると言われます。そうしたウイルスを検知するセキュリティ関連ソフトの動きを鬱陶しいと感じてこれを停止してしまう方もいるようで、ファイル共有ソフトを利用する際にはセキュリティ関連ソフトを停止するのが便利などと書いているホームページすらあります（この行為がセキュリティ上大きな問題であることは言うまでもありません）。

また、最近は流出した情報と、既にインターネット上で公開されている（必ずしも実名で公表されていないものを含めた）情報とを連動させることで、様々な情報が白日の下にさらされてしまうケースもあります。こういったことはインターネット以外でも発生しないわけではありませんが、その情報の連動及び拡散の速さにおいてインターネットは他を大きく上回っています。自分に関する情報が自分の意識しないうちにインターネット上で流れていることを経験された方もおられると思いますが、そうした情報があっという間に纏め上げられ、ある場合には興味本位で広い範囲に拡散されてしまった場合の被害は図り知れません。個人情報保護法の施行をきっかけとして、現実世界での自分の個人情報の取扱については相当意識が進んできたと感じられますが、インターネット上では、画像等も含め、現実世界にも増した慎重な対応が必要と痛感しました。

以上、とりとめの無いお話をしましたが、お終いに冒頭でお話しした情報流出の防止と対策に携わっておられる方々の一言を紹介します。

*「不適切な方法で入手したファイルはある程度見当がつくものです。専用パソコンに専用回線を用意すればファイル共有ソフトの利用は安全などという人もいますが、実社会において生じるリスクまで考えれば、タダほど高いものは無いという諺がこれほど当て嵌る場合はないと思います。」*

それでは皆さんセキュリティ対策は終わりのない厳しい道ですが、体を壊さないよう共に励みましょう。

［声の大きさがセキュリティホール（仕様？）のおっさん］

【第8号の『情報セキュリティQ』の答え】

前回の問題は、「わが国のIC旅券に記録されている生体情報は何でしょうか？」でした。答えは、「（2）顔写真」です。現在、電子パスポートの国際標準策定は国連の専門機関である ICAO（International Civil Aviation Organization：国際民間航空機関）が担当しており、その中で顔写真のデータを記録することが必須と定められています。現在日本を含め 27 カ国が米国の査証免除対象国となっていますが、これらの国が2006年10月26日以降に発給するパスポートには、生体情報を IC チップに埋め込むことが求められています。また、現在の日本の IC 旅券では対応していませんが、ICAO では指紋画像や虹彩画像を記録するための仕様も策定しています。

---

**＜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