INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
2006 年 10 月 3 日
独立行政法人 情報処理推進機構

コンピュータウイルス・不正アクセスの届出状況［2006 年 9 月分］について

独立行政法人 情報処理推進機構(略称:IPA、理事長:藤原 武平太)は、2006 年 9 月のコンピュータウイルス・不正アクセスの届出状況をまとめました。

今月の呼びかけ：
「修正プログラムの配信を装ったウイルスメールに注意！！」

― 正しいサイトから修正プログラムをダウンロードしてセキュリティホールをふさごう ―

最近、マイクロソフト社製品のセキュリティホール(セキュリティ上の弱点)をふさぐ**修正プログラムを配信すると称したメール(下図参照)が多数発見**されています。実は、当該修正プログラムに見えるファイルはウイルス(**W32/Stration**)です。誤って添付ファイルをクリックすると、ウイルスに感染してしまいます。**決してクリックしないようにしてください**。

通常は、ソフトウェアを提供しているベンダーのサイトにユーザがアクセスして、修正プログラムをダウンロードします。**修正プログラムがメールの添付ファイルとしてベンダーから提供されることはありません**。親切を装った内容のメールには十分注意して、だまされないようにしてください。

なお、Windows であれば、「Microsoft Update」 http://update.microsoft.com/ のサイト、Macintosh であれば、「ソフトウェアアップデート」http://www.apple.com/jp/ftp-info/のサイトのように、**各ベンダーのサイトから修正プログラムをダウンロードするようにしてください**。

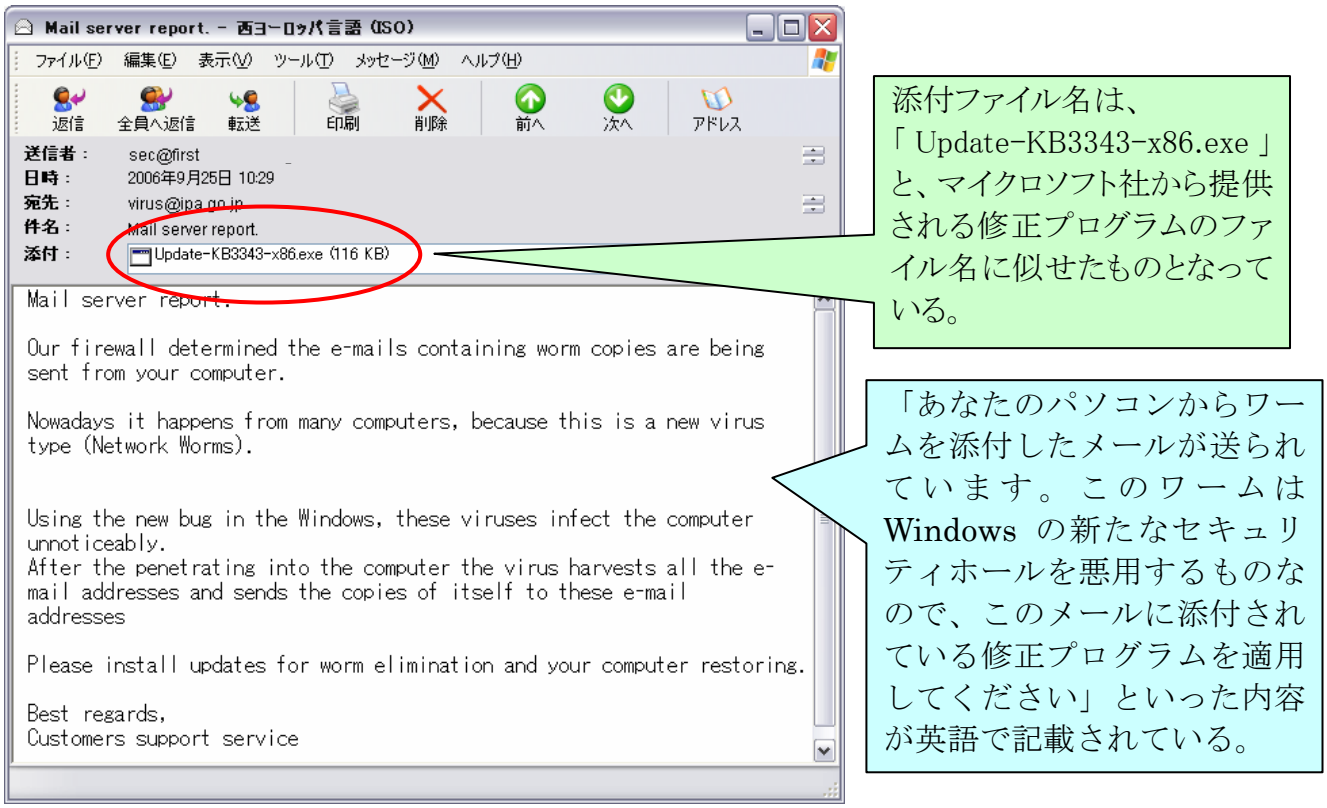


図:W32/Stration の亜種が送信するメールの例

W32/Stration の解説

2006 年 8 月に発生した W32/Stration の亜種が 9 月に多数出現し、出回っていますので、注意が必要です。

このウイルスは、自分自身を添付したメールを送信することで拡散します。その添付ファイルを開くとウイルスに感染することになり、アドレス帳に保存されているメールアドレス宛に同様のウイルスメールを送信することになってしまいます。

また、亜種の中には、ウイルスの作者が用意したと推測されるサイトへアクセスさせ、勝手に感染した PC にスパイウェアなどをダウンロードする機能を持ったものなどもあり、情報漏えいが生じるなどの被害に遭う可能性があります。

IPA で確認した亜種には、P1 の図にあるように、送信するウイルスメールの本文、添付ファイル名をマイクロソフト社が提供するセキュリティホールを修正するプログラムに見せかけるパターンがあります。この添付ファイルを開くと、「Update successfully installed.」といった修正が成功した旨のダイアログを表示し、ウイルスに感染したことに気付かせないようにしています。

さらに、ルートキット(*1)も同時にコンピュータにインストールするため、感染してからでは発見することが困難になります。また、見た目にわかる症状もでないため、感染していることに気付かずに、ウイルスメールを撒き散らし続けることになってしまいます。

感染してからでは対処が困難になるなど、被害が拡大する恐れがありますので、メールの添付ファイルを安易に開くことは決してしないようにしてください。

1. コンピュータウイルス届出状況　－詳細は別紙 1 を参照－

ウイルスの検出数(※1)は、**約 105 万個**と、8 月の 110 万個から 4.6%の減少となりました。
また、9 月の届出件数(※2)は、**3,551 件**となり、8 月の 3,434 件から 3.4%の増加となりました。

※1 検出数　：届出にあたり届出者から寄せられたウイルスの発見数(個数)
※2 届出件数：同じ届出者から寄せられた届出の内、同一発見日で同一種類のウイルスの検出が複数ある場合は、1 日何個検出されても届出 1 件としてカウントしたもの。
・9 月は、寄せられたウイルス検出数約 105 万個を集約した結果、3,551 件の届出件数となっています。

検出数の1位は、**W32/Netsky で約 84 万個 、2 位は W32/Stration で約 6 万個、3 位は W32/Mytob で約 5 万個でした。**

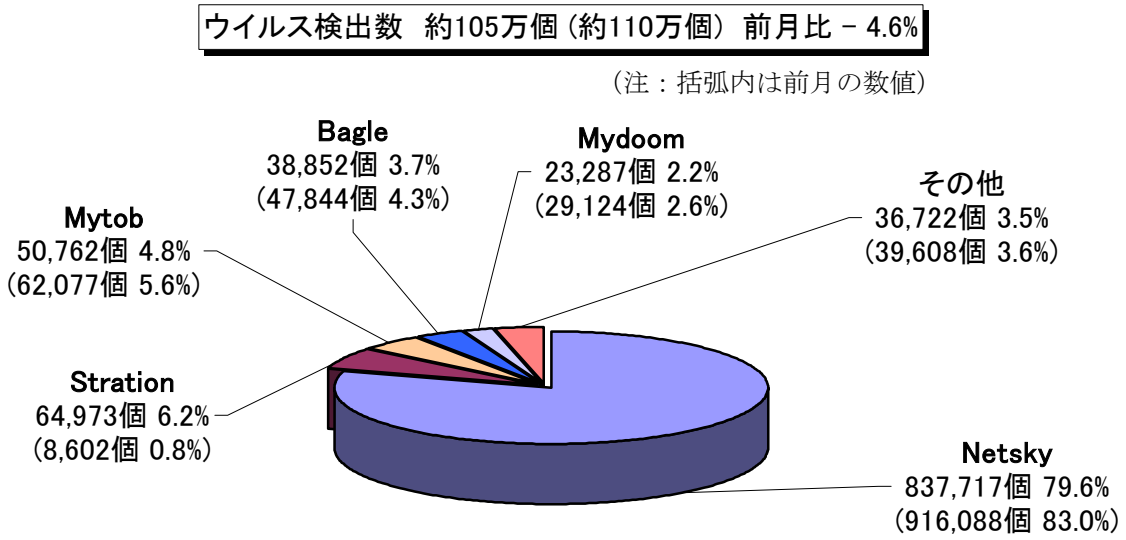


図:1-1

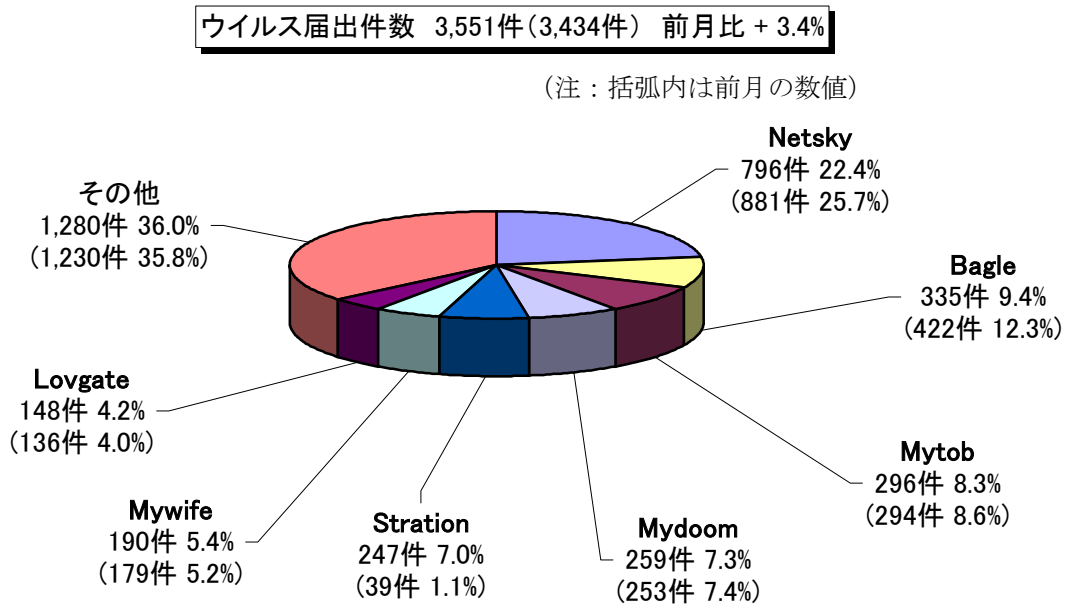


図:1-2

2. ワンクリック不正請求

2006 年 9 月、**「ワンクリック不正請求」**に関する相談が **223 件も寄せられ、今までで最も多い相談件数**となりました。(4 月:161 件、5 月:210 件、6 月:211 件、7 月:159 件、8 月:204 件)

～　危ないサイトはアダルトサイトだけではない　～

このようなワンクリック不正請求の被害は、主にアダルトサイトで発生しています。ところが、アダルトサイト以外の投資関係のサイトでも同様の手口が確認されました。当該サイトでは、確実に利益をあげられる株式情報を提供するという案内を記載し、会員登録をするように促しています。この会員登録という項目をクリックすると、ウイルスなどの悪意のあるプログラムをダウンロードさせる仕組みになっています。

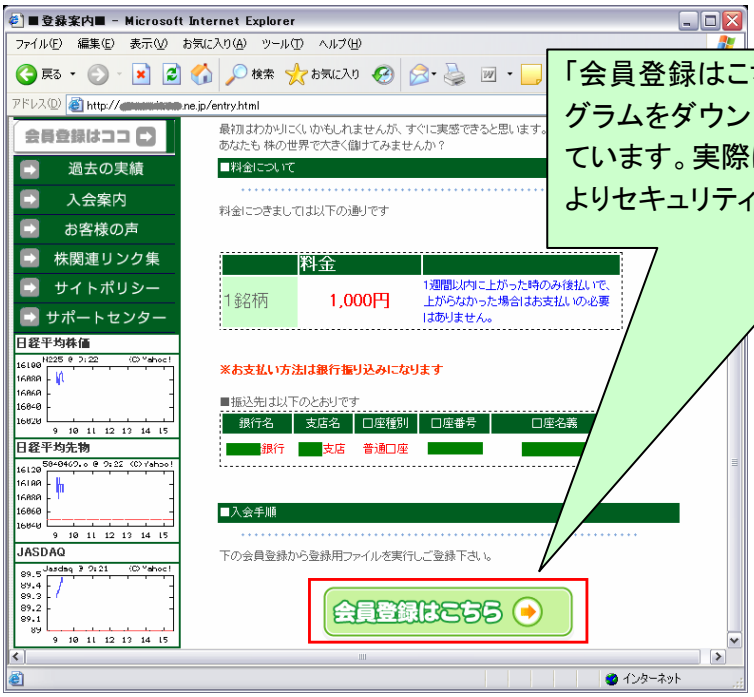
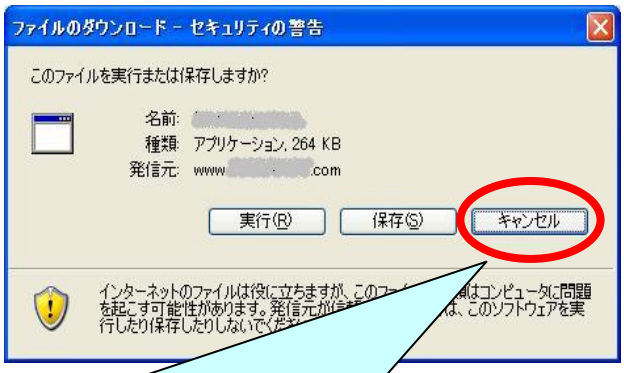


図 2-1:悪意あるプログラムをダウンロードさせるサイト

「会員登録はこちら」をクリックすると、悪意あるプログラムをダウンロードさせるための仕掛けが施されています。実際にクリックすると、Windows の機能によりセキュリティの警告画面が表示されます。

図2-2:Windowsによるセキュリティの警告画面



「セキュリティの警告」画面で、「実行」をクリックして進むと、悪意あるプログラムをインストールすることになってしまいます。この警告画面を無視せずに、「キャンセル」をクリックするようにしましょう。

IPA で受け付けている相談事例にも、芸能人の動画や画像を検索していて、ワンクリック不正請求の被害にあったというものがありました。アダルトサイトを閲覧する目的以外の人も遭遇する危険がありますので、注意が必要です。

これらの被害に遭わないよう、信頼できないサイトにはアクセスしない、アクセスしてしまっても、安易なダウンロードは避けることを心がけてください。図 2-2 に示す Windows によるセキュリティの警告画面が表示された場合は、決して「実行」をクリックすることなく、**「キャンセル」をクリック**して先に進まないようにしてください。

悪意あるプログラムなどによる被害に遭われた場合は、IPA で相談を受け付けておりますので、ご相談ください。
(P7:相談受付状況を参照)

3. コンピュータ不正アクセス届出状況（相談を含む）　－詳細は別紙 2 を参照－

不正アクセスの届出および相談の受付状況

		4月	5月	6月	7月	8月	9月
届出(a) 計		15	13	22	15	50	46
	被害あり(b)	7	6	20	8	30	21
	被害なし(c)	8	7	2	7	20	25
相談(d) 計		27	23	32	31	24	35
	被害あり(e)	15	11	19	18	13	26
	被害なし(f)	12	12	13	13	11	9
合計(a+d)		42	36	54	46	74	81
	被害あり(b+e)	22	17	39	26	43	47
	被害なし(c+f)	20	19	15	20	31	34

(1) 不正アクセス届出状況

9 月の届出件数は 46 件であり、そのうち**被害のあった件数は 21 件**でした。

(2) 不正アクセス等の相談受付状況

不正アクセスに関連した相談件数は 35 件（うち 5 件は届出件数としてもカウント）であり、そのうち何らかの被害のあった件数は 26 件でした。

(3) 被害状況

被害届出の内訳は、**侵入 7 件、ワーム感染 8 件、アドレス詐称 1 件など**でした。

侵入届出の被害内容は、Web ページやサーバ内データの改ざんが 2 件、他サイト攻撃やスパム(*2)メール発信の踏み台になっていたものが 3 件、などでした。侵入の原因として、SSH(*3)で使用するポート(*4)へのパスワードクラッキング(*5)攻撃を受けてパスワードが破られた事例が 1 件ありました。

被害事例

［侵入］

（i）他サイト攻撃の踏み台として悪用された

事例	・「あなたの組織が管理している IP アドレスのコンピュータが、外部のサーバに対して SSH(*3) で不正にログイン試行している」と、自身が契約しているプロバイダから連絡が入った。 ・調査したところ、SSH 経由の辞書攻撃(*6) でパスワードが破られて侵入されていたことが判明。さらに自身のサーバ内に SSH 用の辞書攻撃ツールを埋め込まれ、他サイトを攻撃するための踏み台となっていた。ログ(*7) ファイルは削除されており、詳細は分からなかった。
解説・対策	パスワードクラッキング(*5) の際には自動攻撃ツールが用いられるためか、SSH で使用するポート(*4) が狙われる機会はなおも多いようです。パケットフィルタリングの実施や IDS(*8) /IPS(*9) の導入なども大事ですが、まずは**日々アクセスログをチェックして一刻も早く攻撃の兆候を掴み、必要な対策を講じることが重要**です。**SSH 運用時には、ログインの際に公開鍵認証(*10) などの強固な認証を採用することを推奨**します。 （参考） IPA － 今月の呼びかけ（7 月分） 「パスワードを一つ残らず、きちんと管理しましょう！」 http://www.ipa.go.jp/security/txt/2006/07outline.html IPA － 安全なウェブサイトの作り方 http://www.ipa.go.jp/security/vuln/20060131_websecurity.html

（ii）ホームページ改ざん

事例	・「貴方のホームページが改ざんされているのでは？」との通報が、組織外から入った。調査したところ、英文の政治的主張らしきページが、自身のウェブサイトに置かれていたことが判明。 ・自身のサイトでは、OSS(*11) （オープンソースソフトウェア）の CMS(*12) （コンテンツ管理ツール）である DNN（DotNetNuke）を最新版に更新して使っていた。さらに DNN 向けのサードパーティ(*13) 製モジュールを追加して使っていた。 ・DNN 向けサードパーティ製モジュールに存在していたぜい弱性を突かれたのが原因と思われた。ぜい弱性解消のための修正プログラムは既にリリースされていたので、即対処した。
解説・対策	**ぜい弱性解消のための修正プログラムは、OS やアプリケーションソフトウェアのみならず、アプリケーションに組み込んで使うライブラリ(*14) やモジュール(*15) に対しても必要に応じて用意されています**。ぜい弱性や修正プログラムに関する情報をこまめにチェックし、対応が遅れないようにしましょう。 （参考） IPA － 今月の呼びかけ（9 月分） 「ぜい弱性が公開されたら直ちにアップデートを！」 http://www.ipa.go.jp/security/txt/2006/09outline.html

［その他］

（iii）アカウント(*16)を勝手に使われた

事例	・大手ポータルサイトで作成した自身のアカウントが、第三者に勝手に使われた。 ・自身が作成したブログや登録情報を改ざんされるとともに、ネットオークションに勝手に出品されていた。 ・パスワードを破られたことが原因。
解説・対策	ポータルサイトを利用する際には、ID（Identification）によってユーザを識別します。サイトによっては、ID があらかじめ第三者にも分かるようになっているものもあり、この場合はパスワードだけ分かれば、その人に成りすましてログインされてしまいます。パスワードは推測されにくいものにするとともに、**特に用事が無くても定期的にアクセスし、勝手に使われていないかどうか確認する**と良いでしょう。定期的にパスワードを変更することも、有効な対策となります。また、**スパイウェアによってパソコン内の ID/パスワード情報を盗み出されるケースもありますので、ウイルス/スパイウェア対策ソフトによるチェックも欠かさないようにしましょう。** (参考) IPA － 今月の呼びかけ（7 月分） 「パスワードを一つ残らず、きちんと管理しましょう！」 http://www.ipa.go.jp/security/txt/2006/07outline.html

4. 相談受付状況

9 月の相談総件数は **933 件**でした。そのうち**『ワンクリック不正請求』に関する相談**が **223 件**(8 月：204 件)と、今までで最悪の件数を記録しました。その他の内訳は、**『セキュリティ対策ソフトの押し売り』行為**に関する相談が **23 件**(8 月：33 件)、**Winny に関連する相談**が **9 件**(3 月：196 件、4 月：83 件、5 月：28 件、6 月：15 件、7 月：12 件、8 月：14 件)などでした。

IPA で受け付けた全ての相談件数の推移

	4月	5月	6月	7月	8月	9月
合計	904	846	773	767	793	933
自動応答システム	510	484	423	444	460	575
電話	306	295	283	257	280	302
電子メール	86	63	64	66	48	51
その他	2	4	3	0	5	5

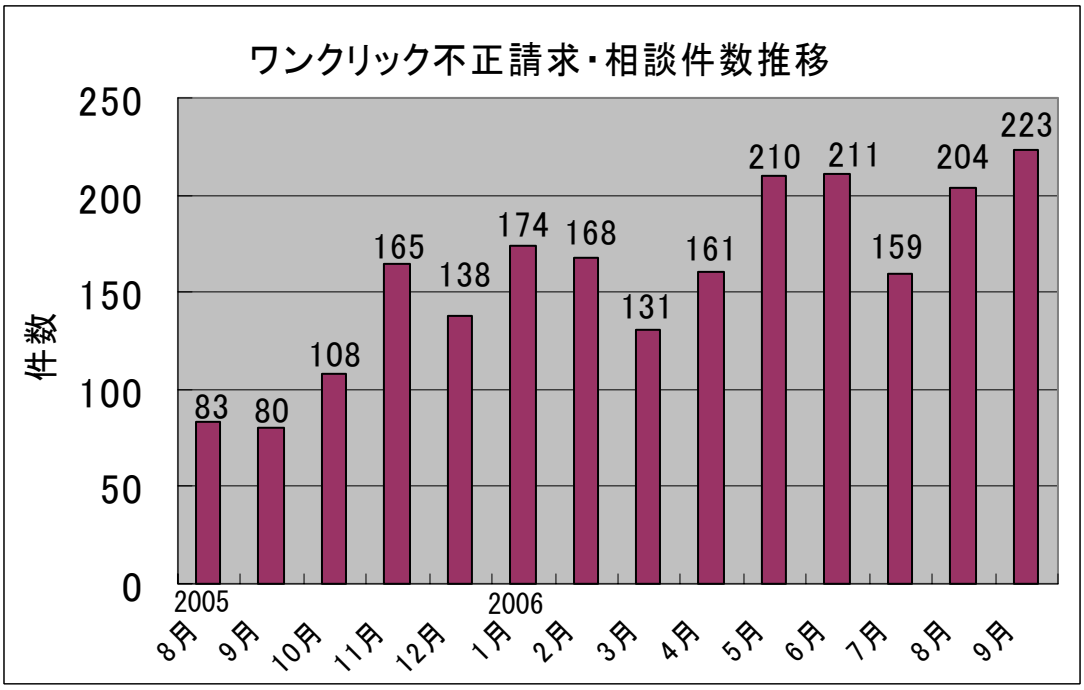
※ IPA では、コンピュータウイルス・不正アクセス、Winny 関連、その他情報セキュリティ全般についての相談を受け付けています。
メール：virus@ipa.go.jp（ウイルス）、crack@ipa.go.jp（不正アクセス）、
winny119@ipa.go.jp（Winny 緊急相談窓口）、isec-info@ipa.go.jp（その他）
電話番号：03-5978-7509（24 時間自動応答、ただし IPA セキュリティセンター員による

相談受付は休日を除く月～金の 10:00～12:00、13:30～17:00 のみ）
FAX：03-5978-7518（24 時間受付）

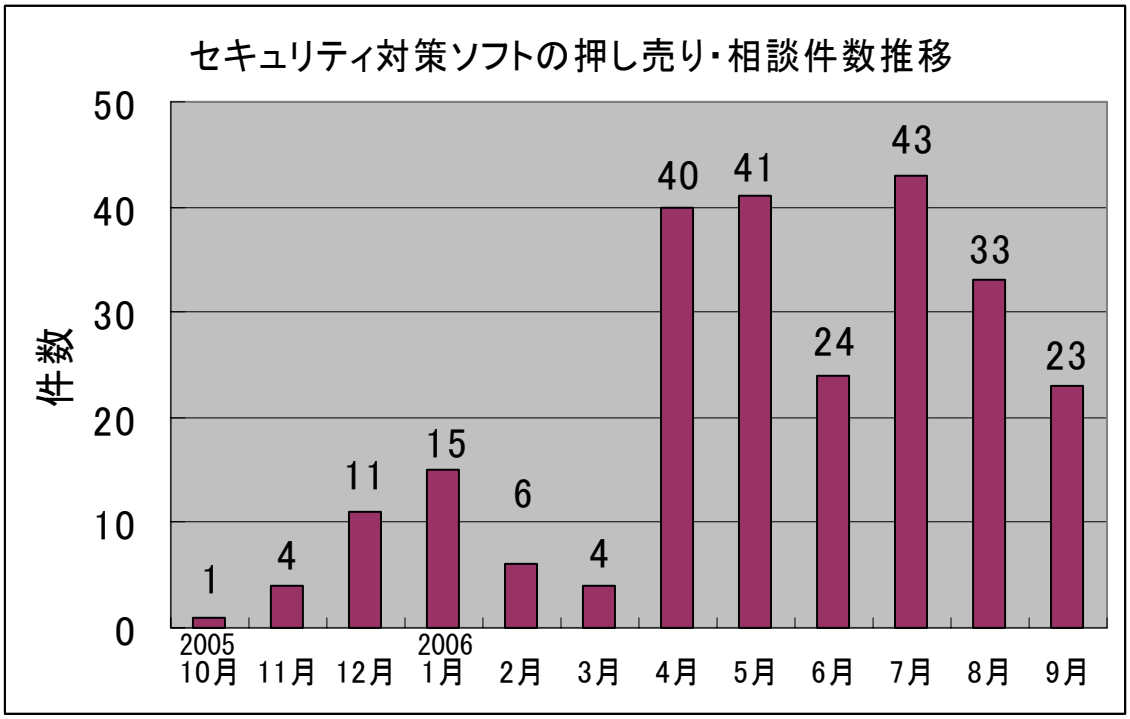
※「自動応答システム」： 電話の自動音声による応対件数
「電話」： IPA セキュリティセンター員による応対件数

※ 合計件数には、「不正アクセスの届出および相談の受付状況」における『相談[d] 計』件数を内数として含みます。

（参考）ワンクリック不正請求相談件数の推移



（参考）セキュリティ対策ソフトの押し売り・相談件数の推移



主な相談事例は以下の通りです。

（i）ウイルス対策ソフトが“cookie(*17)”を検出

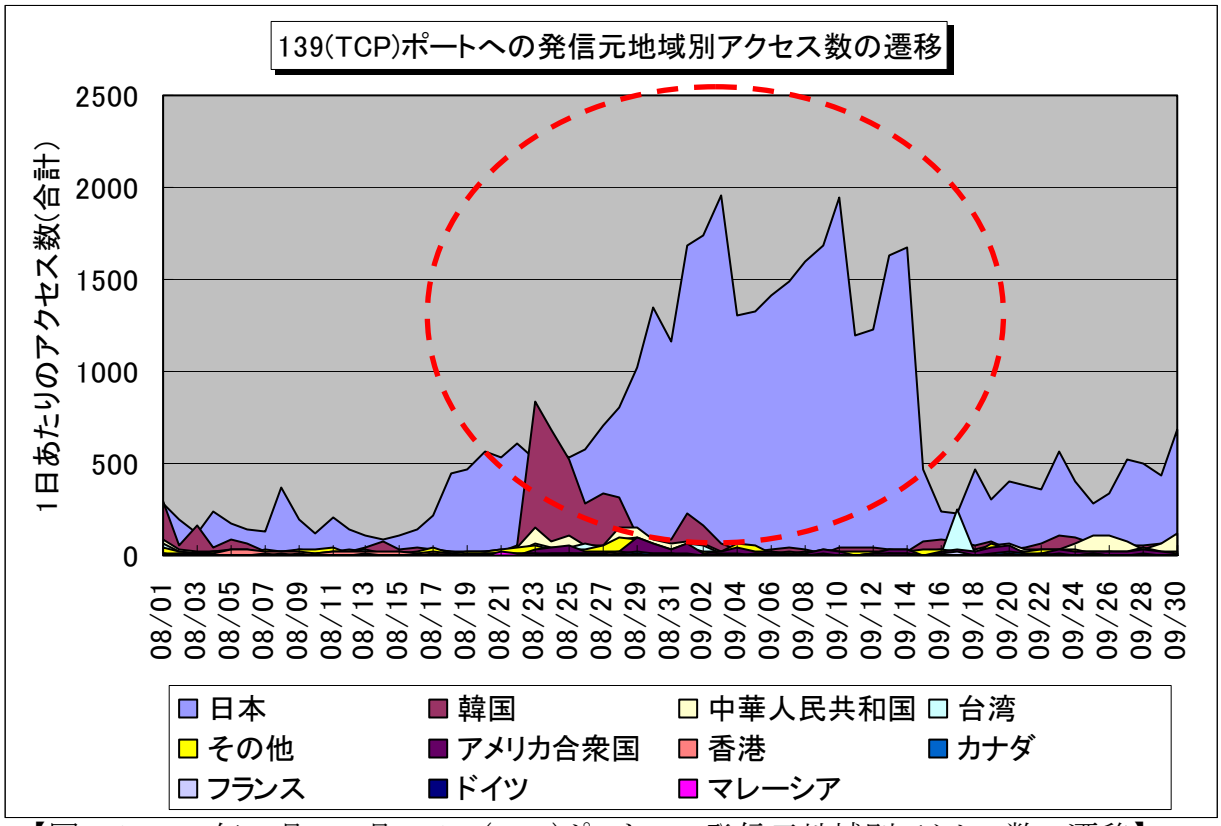
相談	インターネットへの接続ができなくなった。ウイルス対策ソフトでスキャンしたところ、“cookie”というものが多数検出された。何か情報が流出しているのか？
回答	**cookie はウイルスではありません**。なおかつ、cookie はプログラムではありませんので、cookie によって不正な命令を実行されたり、パソコンが操られたり、ということはありません。 インターネットに接続出来ない理由は他にあるはずです。**プロバイダへの接続設定を見直す**とともに、**セキュリティ対策ソフトがインターネット接続をロックしていないか、確認**してください。

（ii）Winny 以外のファイル共有ソフトなら情報は漏れない？

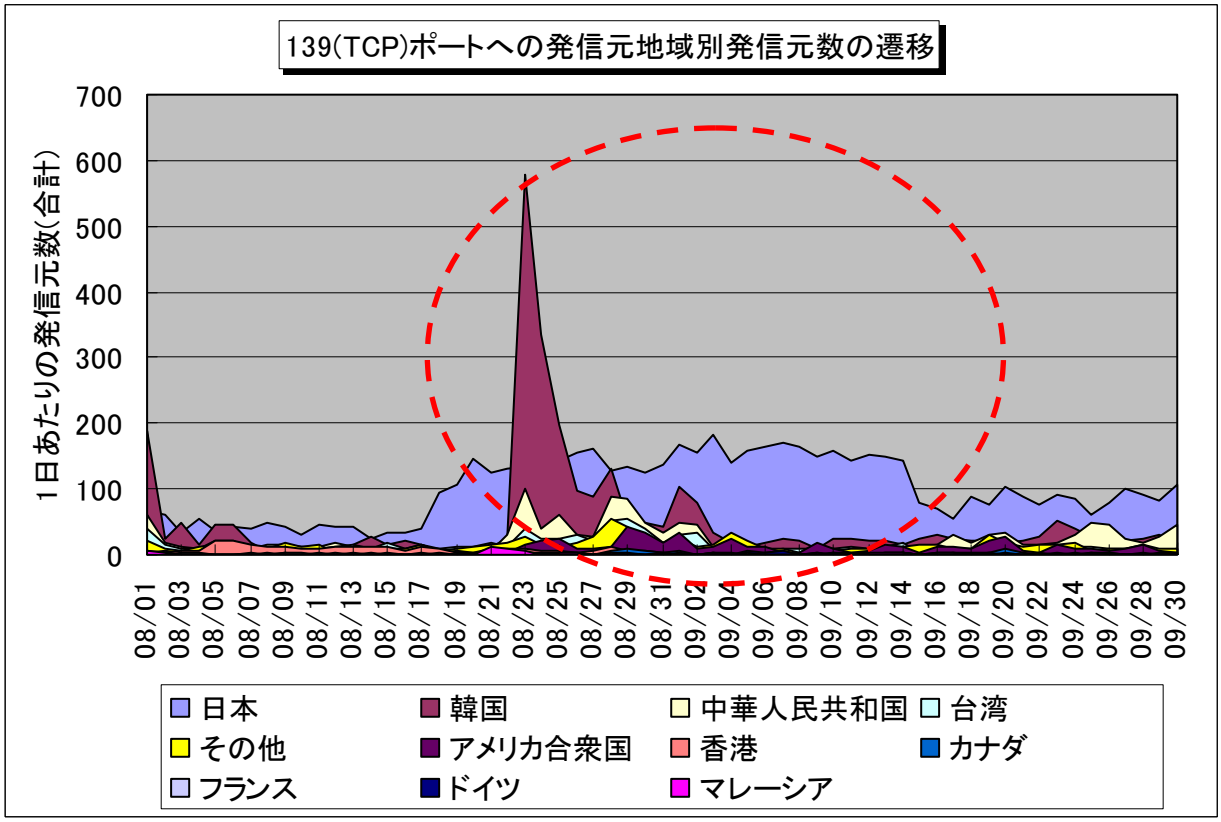
相談	Winny はウイルスに感染して情報が漏れる危険があると理解していたので、Winny 以外のファイル共有ソフトなら大丈夫だと思って使っていました。今は使っていませんが、この考え方は正しかったでしょうか。
回答	情報流出を引き起こすウイルスの多くはパソコンに感染し、Winny の機能を悪用して情報を流出させてしまいます。しかしながら、**Winny 以外のファイル共有ソフトの機能を悪用して情報を流出させるウイルスも出現しています**。つまり、Winny 以外のファイル共有ソフトなら安全という訳でもありません。 **ファイル共有ネットワークに流出してしまったデータの回収は、事実上不可能**と言えます。ファイル共有ソフトの利用は、こうした危険と隣り合わせな行動であることを改めて認識しましょう。 さらに、**情報流出の際にファイル共有ソフトの仕組みを使わないウイルスも出現しています**。つまり、ファイル共有ソフトを使っていないから大丈夫という訳でもありません。**ウイルスに感染しないことが最も重要**であり、そのためには**出所の不明なファイルを安易にダウンロードしたり開いたりしないことが最も基本的な対策**となります。 （ご参考） IPA－Winny による情報漏えいを防止するために http://www.ipa.go.jp/security/topics/20060310_winny.html IPA－ パソコンユーザのためのウイルス対策 7 箇条 http://www.ipa.go.jp/security/antivirus/7kajonew.html

5. インターネット定点観測での 9 月のアクセス状況

2006 年 8 月中旬から始まった 139(TCP)ポートへのアクセスは、Windows のぜい弱性(MS06-040)を狙ったものと考えられます。これらのアクセスの増加は、9 月 15 日前後に終息した模様です(図 5.1 および図 5.2)。



【図 5.1 2006 年 8 月～9 月の 139(TCP)ポートへの発信元地域別アクセス数の遷移】



【図 5.2 2006 年 8 月～9 月の 139(TCP)ポートへの発信元地域別発信元数の遷移】

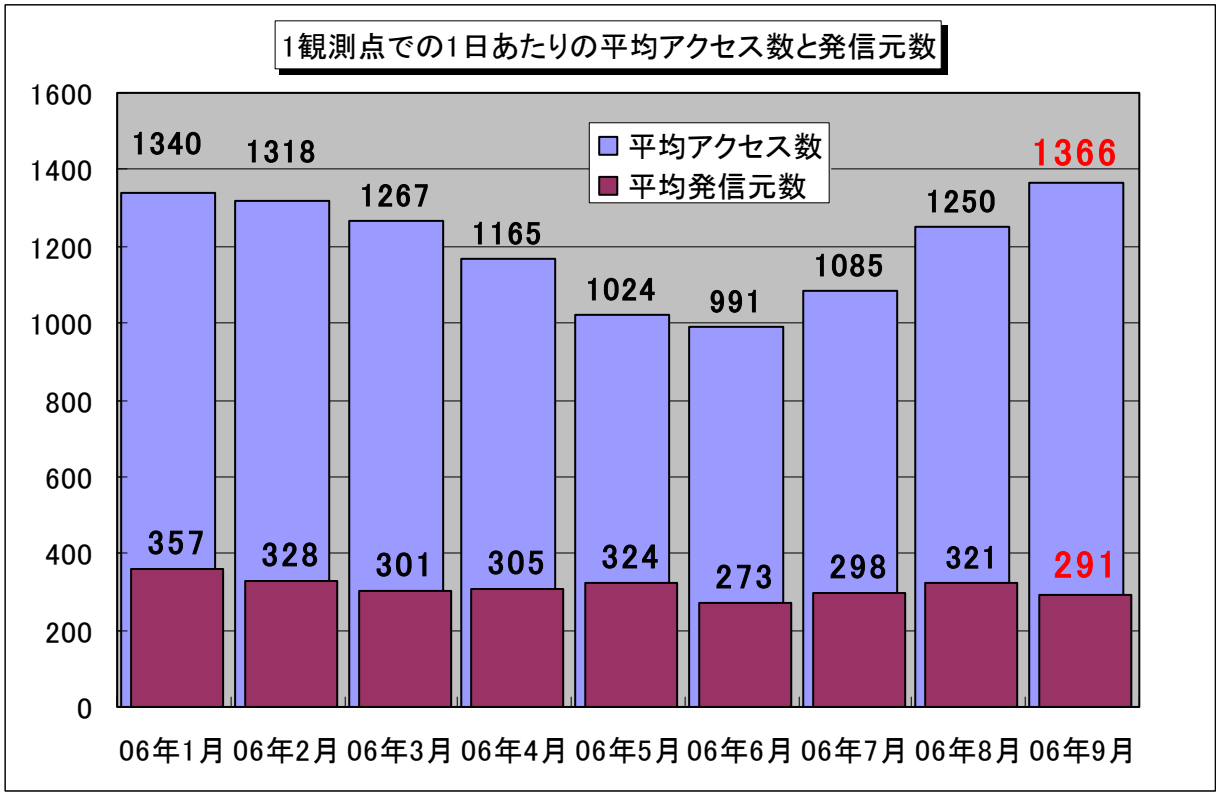
国内を発信元とする 139(TCP)ポートへのアクセスについて、発信元を基準に分析すると、
A) 139(TCP)ポートのみへのアクセスパターン
B) 複数のポートへのアクセスを組み合わせて狙ったアクセスパターン
の 2 つのパターンが存在しました。

A)の場合は、ワームと呼ばれる特定のぜい弱性を狙ったものである可能性が高いと考えられます。また、B)の場合は、数種類の攻撃コードを装備したボットからのアクセスの可能性が高いと考えられます。

さらに、これらのアクセスの発信元(発信 IP アドレス)を調べると、各 ISP から個人利用者に提供される IP アドレスが多いことが分かりました。これは、個人利用者がボットに感染している可能性が高いことを示していると考えられるので、最近コンピュータの反応が遅い等の症状に不安のある方は、以下の資料を参考にして、ボット対策をお願いします。

■ ボット対策のしおり
http://www.ipa.go.jp/security/antivirus/shiori.html

8 月および 9 月の平均アクセス数が増加傾向にありますが(図 5.3)、この原因は、これらのアクセスによるものと考えられます。



【図 5.3 1 観測点での 1 日あたりの期待しない(一方的な)アクセス数および発信元数】

インターネット定点観測(TALOT2)によると、2006 年 9 月の期待しない(一方的な)アクセスの総数は、10 観測点で **409,772 件**ありました。1 観測点で 1 日あたり **291** の発信元から **1,366 件**のアクセスがあったことになります。

外部からの不正なアクセスを明確に防御している企業(組織)の場合は、特に問題にはなりませんが、インターネットにモデムなどで直接接続する形態の Windows コンピュータを利用されている方は、コンピュータのぜい弱性を解消し、ファイアウォール機能の利用など、被害に遭わないように心掛けて下さい。

コンピュータの個人利用者は、以下の資料を参考にして、不正アクセス対策を実施して下さい。

■ 不正アクセス対策のしおり

http://www.ipa.go.jp/security/antivirus/shiori.html

以上の情報に関して、詳細はこちらのサイトをご参照ください。

別紙 3_インターネット定点観測（TALOT2）での観測状況について

http://www.ipa.go.jp/security/txt/2006/documents/TALOT2-0610.pdf

『他機関・ベンダーの各種統計情報は以下のサイトで公開されています。』

@police：http://www.cyberpolice.go.jp/

トレンドマイクロ株式会社：http://www.trendmicro.com/jp/

マカフィー株式会社：http://www.mcafee.com/jp/default.asp

『用語の解説』

(*1) **ルートキット**（rootkit）

攻撃者がコンピュータに不正侵入した後に利用するためのソフトウェアをまとめたパッケージのこと。一般的には、ログ改ざんツールやバックドアツール、改ざんされたシステムコマンド群などが含まれる。

(*2) **スパム**（spam）

ジャンクメール、バルクメール、また単に「迷惑メール」とも呼ばれる。商用目的かどうかによらず、宣伝や嫌がらせなどの目的で不特定多数に大量に送信されるメールのこと。

(*3) **SSH** (Secure SHell)

ネットワークを介して別のコンピュータにログインしたり、遠隔地のマシンでコマンドを実行したり、他のマシンへファイルを移動したりするために使うプロトコルもしくはプログラムのこと。ネットワーク上を流れるデータは暗号化されるため、インターネット経由でも一連の操作を安全に行なうことができる。

(*4) **ポート**（port）

コンピュータが外部との情報の受け渡しの際に使う、コンピュータ内の各種サービス窓口のこと。ポートは 0 から 65535 までの値が使われるため、ポート番号とも呼ばれる。

(*5) **パスワードクラッキング**（password cracking）

他人のパスワードを、解析するなどして探り当てること。総当り攻撃や辞書攻撃といった手法があり、クラッキング用のプログラムも存在する。

＊:総当り攻撃

何らかの規則にしたがって、文字の組み合わせを総当りで試行する攻撃方法のこと。いわゆる力ずくの攻撃方法のことで、ブルートフォース攻撃ともいう。

(*6) **辞書攻撃**

パスワードを破るために、辞書にある単語などを片端から試行する攻撃方法のこと。

(*7) **ログ**（log）

コンピュータの利用状況やデータ通信の記録のこと。一般的に、操作を行った者の ID や操作日

時、操作内容などが記録される。

(*8) **IDS** (Intrusion Detection System)
システムに対する侵入／侵害を検出・通知するシステムのこと。システムを監視し、セキュリティポリシーを侵害するような行為を検出した場合に、その行為を可能な限り早く管理者に伝えるとともに、調査分析の作業を支援するために必要な情報を保存・提供することが目的である。

(*9) **IPS** (Intrusion Prevention System)
システムに対する侵入／侵害を阻止するシステムのこと。異常を検知した際に自動的に通信を停止する機能を有したものであり、一般的には IDS の発展形と言える。

(*10) **公開鍵認証**
公開鍵と秘密鍵のペアでユーザ個人の認証を行う方式のこと。公開鍵はサーバ側で管理し、秘密鍵は個人で管理し、これらによりユーザ認証を行う。

(*11) **OSS** (Open Source Software)
ソフトウェアのソースコードが公開されており、再頒布が自由であるソフトウェアのこと。

(*12) **CMS** (Contents Management System)
公開したいコンテンツ(テキスト、画像など)を用意できさえすれば、技術的知識をさほど必要とせずにウェブで情報発信を可能とする、サイト構築支援ツールのこと。コンテンツ情報(テキスト、画像、レイアウトなど)などを一元管理できる。広い意味では、デジタルコンテンツの管理に使うソフトウェアやシステムの総称としても使われる。

(*13) **サードパーティ** (3rd party)
他社製のソフトウェア／ハードウェアに対応する製品を作っているメーカーのこと。

(*14) **ライブラリ** (library)
汎用性のある複数のプログラムコードを、他のプログラムからでも利用できるように部品化して一つのファイルにまとめたもののこと。ライブラリ単体ではプログラムとして実行させることはできないが、他のプログラムから呼び出され、他のプログラムの機能の一部として動作する。

(*15) **モジュール** (module)
システムを構成する要素のこと。ソフトウェアの分野では、インターフェースが標準化されていて容易に開発・追加・削除ができるようになっている、一連の機能をひとまとめにしたソフトウェア部品のことを指す。

(*16) **アカウント** (account)
コンピュータやネットワーク上の資源を利用出来る権利のこと。

(*17) **cookie** (クッキー)
ウェブサーバとウェブブラウザとの間で、ユーザ情報やアクセス情報などをやり取りする仕組みのこと。

■お問い合わせ先
独立行政法人 情報処理推進機構 セキュリティセンター
花村／加賀谷／宮本
Tel:03-5978-7527 Fax:03-5978-7518 E-mail:isec-info@ipa.go.jp

お知らせ

『自社のセキュリティ対策自己診断テスト』

～　情報セキュリティ対策ベンチマーク　～

IPA では、**「自社のセキュリティ対策自己診断テスト（情報セキュリティ対策ベンチマーク）」**を Web サイト上に公開しております。

自社のセキュリティ対策自己診断テスト（情報セキュリティ対策ベンチマーク）
http://www.ipa.go.jp/security/benchmark/

本システムは、企業を対象としたもので、セキュリティ対策状況及び企業情報に関する設問(計 40 問)に答えることにより、セキュリティ対策の取組状況を自己採点できるシステムです。

診断結果は、「貴社のスコア」と「望まれる水準」とが同時に表示され、各社が優先的に取り組むべきセキュリティ対策項目が明らかになります。また、推奨される取り組み事例も提示しますので、今後の対策を強化する上での具体的な改善策がわかります。

30 分程度で自己採点できますので、ぜひ、今後のセキュリティ対策の参考とすべく、ご活用ください。

お知らせ

IPA では、対策のしおりシリーズを提供しています！

情報セキュリティ対策のための「ウイルス対策のしおり」、「ボット対策のしおり」、「スパイウェア対策のしおり」、「不正アクセス対策のしおり」、「情報漏えい対策のしおり」を作成・提供しております。

本対策のしおりは、一般のご家庭や企業（組織）内でパソコンをご利用する方々を対象に、情報セキュリティ上の様々な脅威への対策を分かりやすく説明したものです。気軽に読んでいただけるよう、挿絵を多用し、それぞれの脅威の概要、仕組み、対策を理解し、把握できるように工夫しております。これらの脅威への対策を実践するために、ぜひご活用ください。

対策のしおりシリーズ

(1)ウイルス対策、(2)スパイウェア対策、(3)ボット対策、(4)不正アクセス対策、および
(5)情報漏えい対策
http://www.ipa.go.jp/security/antivirus/shiori.html

お知らせ

「情報セキュリティ標語 2006」の入選作品

コンピュータウイルスの感染やコンピュータへの不正な侵入、 ワンクリック詐欺などの被害に遭わないよう、 特に若年層の「情報セキュリティ対策」の意識を高めるために、本年 3 月より全国の小学生・中学生・高校生から募集していたもので、全国 118 の小・中・高等学校の中から 1, 101 件の応募があり、以下の 10 作品が入選しました。

区分	作品	学校 / 受賞者氏名
大賞	ネットで繋がる無限の世界　明暗決めるはあなたの手	神奈川・慶應義塾湘南藤沢高等部 / 清水　優香子（しみずゆかこ）
高校生の部		
金賞	人々の　意識で変わる　セキュリティ	埼玉県・県立越谷北高等学校 / 浅井　慧（あさいあきら）
銀賞	ケータイは持って天国　落として地獄	岐阜県・県立可児工業高等学校 / 田口　史武（たぐちふみたけ）
銅賞	手軽でも　忘れるなかれ　セキュリティ	埼玉県・立教新座高等学校 / 松下　成昭（まつしたしげあき）
中学生の部		
金賞	ネットワーク　便利と危険は　紙一重	茨城県・つくば市立吾妻中学校 / 藤井のど佳（ふじいのどか）
銀賞	情報は　流れだしたら　止まらない	埼玉県・三郷市立早稲田中学校 / 増田　恵子（ますだあやこ）
銅賞	気をつけよう　インターネットの落とし穴	兵庫県・加古川市立中部中学校 / 遠入　和也（えんにゅうかずや）
小学生の部		
金賞	ぼくだけは　感染しないよ　大間違い	岐阜県・大垣市立墨俣小学校 / 古澤健太郎（ふるさわけんたろう）
銀賞	パスワード　ともだちにだって　ないしょだよ	愛知県・名古屋市立滝ノ水小学校 / 森　明日翔（もりあすか）
銅賞	セキュリティ　あなたが守る　あなたの身	千葉県・千葉市立若松台小学校 / 山崎　緑（やまざきみどり）

これは、韓国の韓国情報保護振興院（KISA）との共同事業の一環として実施したものです。

KISA とは、韓国の情報通信部（日本の総務省に相当）の外郭団体で、韓国国内の情報や情報システムを保護するための政策を実施し、インターネット上での事件・事故への対応をするなど、安全なネットワーク環境を提供するために必要な技術の普及及び研究開発を行う韓国政府出資の機関です。

KISA では、毎年 6 月を情報化月間と定め、6 月第 3 週及び第 4 週をセキュリティ週間として、情報セキュリティを主題とする各種イベントを実施しています。その中に、情報セキュリティ標語・ポスターの公募展があり、2006 年 6 月に実施した公募展の結果、次ページ以降の作品の入選が決定しました。

KISA 情報セキュリティ標語入選作品一覧

大賞(高)「정보보안 생명처럼 정보윤리 가훈처럼」
(情報セキュリティ　生命のように　情報倫理　家訓のように)
장미연（Jang,Mi-Yeon）/ 서울세종고등학교（SeoulSeJong 高等学校）

金賞(小)「건전한 사이버문화 어린이들 눈귀 된다」
(健全なサイバー文化　子供たちの目鼻となる)
윤여은（Yun,Yeo-Eun）/
남원교룡초등학교（NamWonGyoRyong 初等学校）

(中)「클릭! 정보보호, 엔터! 건전문화」
(クリック!　情報セキュリティ、エンター!　健全文化)
김동욱（Kim,DongWook）/ 배재중학교（BaeJae 中学校）

(高)「조심앞에 웃는 정보 방심앞에 우는 재산」
(用心前に笑う情報　油断前に泣く財産)
모윤광（Mo,Yun-Kwang）/ 안산공업고등학교 AnSanGongUp 高等学校）

銀賞(小)「로그아웃 안된 나의 정보 내 재산이 로그아웃 됩니다」
(ログアウト　気の毒な私の情報　私の財産がログアウトになります)
노은지（No,Eun-Ji）/ 송호초등학교（SongHo 初等学校）

(中)「안전하게 다운받고 건전하게 사용하자」
(安全にダウンして　健全に使用するようになる)
김지현（Kim,Ji-Heun）/ 청하중학교（ChungHa 中学校）

(高)「정보유출! 오늘의 무관심 내일의 큰재앙」
(情報流出! 今日の無関心　明日の大災害)
이세미（Lee,Se-Mi）/ 국립국악고등학교（GookRipGookAk 高等学校）

銅賞(小)「컴퓨터속 폭력 세상 어린이가 죽어가요」
(コンピュータの中の暴力　世の中では子供が死んでいきます)
유지은（Yu,Ji-Eun）/ 춘당초등학교（ChoonDang 初等学校）

(中)「정보유출 한순간 정보보호 한평생」（情報流出一瞬　情報保護一生）
박하연（Park,Ha-Yeon/ 울산옥현중학교（WoolSanOkHyun 中学校）

(高)「전자서명 생활화로 전자거래 안전하게」
(電子サイン習慣化で　電子商取引安全に)
심재표（Sim,Jae-Pyo）/ 북평고등학교（BookPyung 高等学校）

MS 賞(小)「몰래 빼낸 남의정보 썩어가는 나의양심」
(密かに抜き取った他人の情報　すぐに認める私の良心)
이연수（Lee,Yeon-Soo）/ 풍천초등학교（PoongChun 初等学校）

(中)「새나가는 개인정보 사라지는 신용」（漏れる個人情報　消える信用）
황민욱（Hwang,Min-Wook）/ 별망중학교（ByulMang 中学校）

(高)「정보 보호의 지름길! 보안 패치의 생활화」
(情報保護の近道！　保安パッチの習慣化)
김상엽（Kim,Sang-Yeop）/ 인덕고등학교（InDuk 高等学校）

IPA 賞（小）「버릴 것은 인터넷 범죄 지킬 것은 사이버 예절」
（捨てることはインターネット犯罪　守ることはサイバーの礼儀）
이두리（Lee,Doo-Ri）/ 금오초등학교（GeumO 初等学校）

（中）「쉽게얻는 남의정보 쉽게잃는 나의정보」
（簡単に貰うのは他人の情報　簡単に失うのは自分の情報）
황지혜（Hwoang, Ji-Heo）/ 상일중학교（SangIl 中学校）

（高）「매주 토요일 바이러스 점검 매일 매일 개인정보 점검」
（毎週土曜日　ウイルス点検　毎日毎日　個人情報点検）
김윤아（Kim, Yun-A）/ 안산공업고등학교（AnSanGongUp 高等学校）