INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
2006 年 9 月 4 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 8 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 8 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：
「セキュリティ上の弱点（ぜい弱性[A]）が公開されたら直ちにアップデートを！」
― ぜい弱性や修正プログラムの情報をこまめにチェックしよう ―

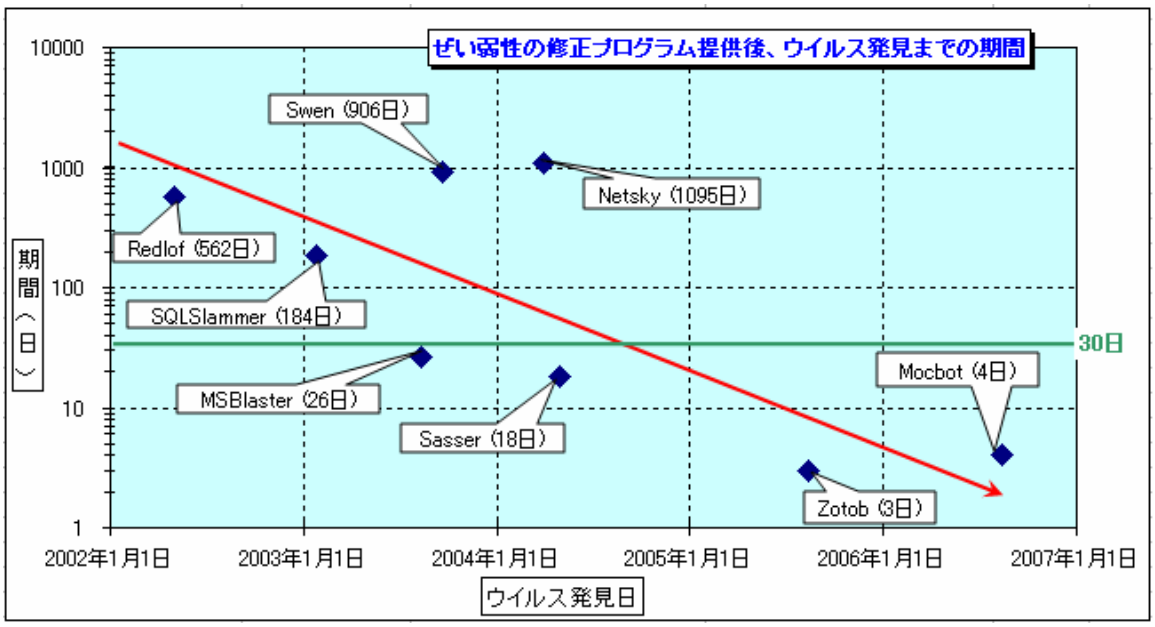
2006 年 8 月、マイクロソフト社より Windows のぜい弱性（セキュリティホール）が公開されるのとほとんど同時に、そのセキュリティホールを突いた攻略コードが発見されるケースが複数あり、中には、4 日後に、当該のセキュリティホールを突くウイルスが発生したものもありました。

通常、セキュリティホールの情報が公開されるときは、それを解消するための修正プログラムが提供されます。マイクロソフト社の場合は、Microsoft Update のサイトから修正プログラムを入手することができます。

Microsoft Update（マイクロソフト社）
http://update.microsoft.com/

セキュリティホールを解消していないと、ウイルスが侵入してくる可能性などを抱えたままになってしまい、危険な状態にあるといえます。また、下表からもわかるように、近年の傾向として、セキュリティホールの情報が公開されてからウイルスが発生するまでの期間※が短くなっています。ウイルス等による被害を防ぐため、セキュリティホールの情報が公開されたら、直ちに解消するようにしましょう。

※2003 年、2004 年は数週間から数ヶ月あったものが 2005 年、2006 年は数日間に短縮されています。



図：セキュリティホールの情報が公開されてからウイルスが出回ったものの内
IPA が今まで緊急対策情報で公表した過去の事例

[A]ぜい弱性（vulnerability）とは、システム、アプリケーションなどのセキュリティを損なうような、予定外の望まない事象を起こせる弱点が存在することをいう。セキュリティホールともいう。

企業・組織においては、システム全体の管理をしている管理者の指示にしたがって、ぜい弱性対策を行うようにしてください。

なお、修正プログラムを適用することにより、グループウェア等の業務システムに不具合が発生する可能性もあります。ベンダーが提供する不具合に関する情報を確認し、修正プログラムの適用が困難な場合は、回避策を実施するなど、柔軟に対応するようにしてください。

◆サポートの終了した OS の使用について

Windows 98/Me については、マイクロソフト社の製品サポートが終了しており、仮にぜい弱性が発見されても、それを修正するためのプログラムが提供されることはありません。ぜい弱性を抱えたままでは、インターネットへの接続やメールのやり取りにおいて、被害に遭う危険性があります。

詳しくは以下のサイトをご参照ください。

マイクロソフト社の情報
Windows 98、および Windows Me に対するサポート終了のご案内
http://www.microsoft.com/japan/windows/support/endofsupport.mspx

対策のしおりシリーズに
(4)不正アクセス対策のしおり、(5)情報漏えい対策のしおりを追加し、IPA のホームページで公開しています。

企業組織において、また、個人のユーザにおかれてもご活用ください。

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

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 110 万個**と、7 月の 154 万個から 28.4%の減少となりました。
また、8 月の届出件数(※2)は、**3,434 件**となり、7 月の 3,455 件から 0.6%の減少となりました。

※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。
・8 月は、寄せられたウイルス検出数約 110 万個を集約した結果、3,434 件の届出件数となっています。

検出数の1位は、**W32/Netsky で約 92 万個 、2 位は W32/Mytob で約 6 万個、3 位は W32/Bagle で約 5 万個でした。**

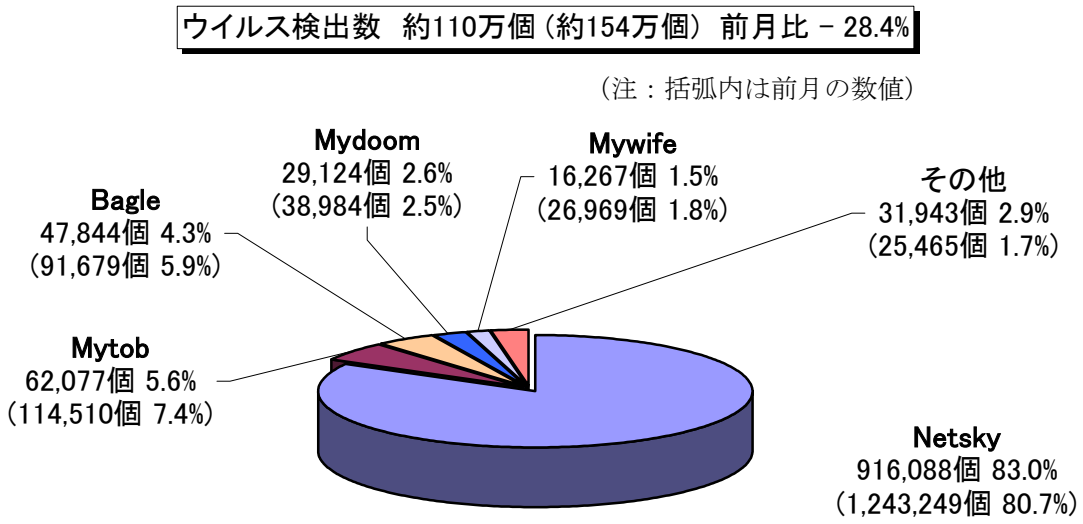


図:1-1

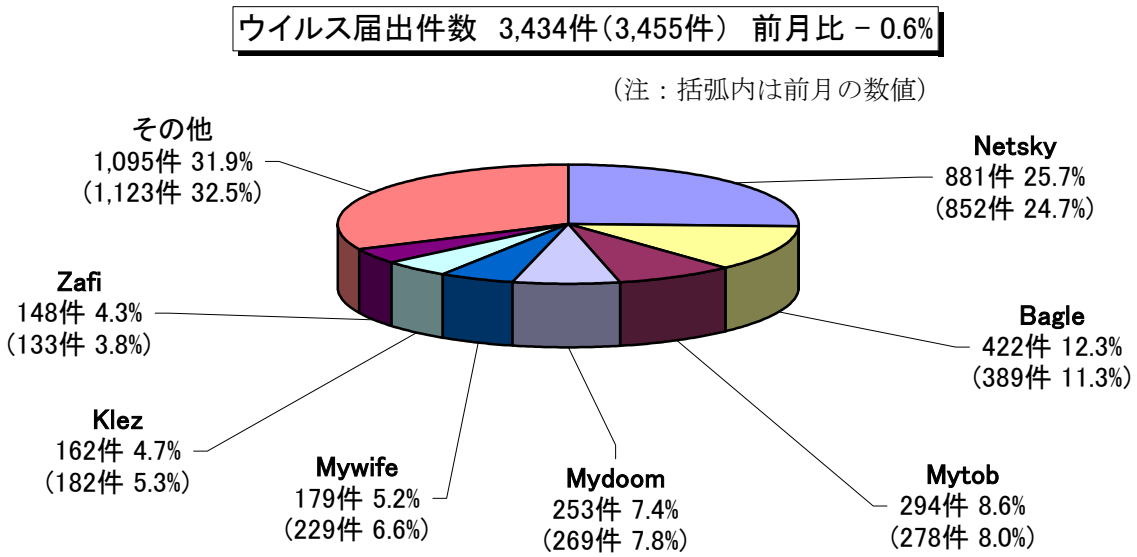


図:1-2

2. 依然として相談の多いワンクリック不正請求による被害

依然として、**「ワンクリック不正請求」**に関する相談が多く寄せられています。これらの相談には、画像をクリックしただけで料金を請求されてしまうものや、パソコンを起動したときや一定時間毎にデスクトップに請求書が表示されてしまうものなどがあります。

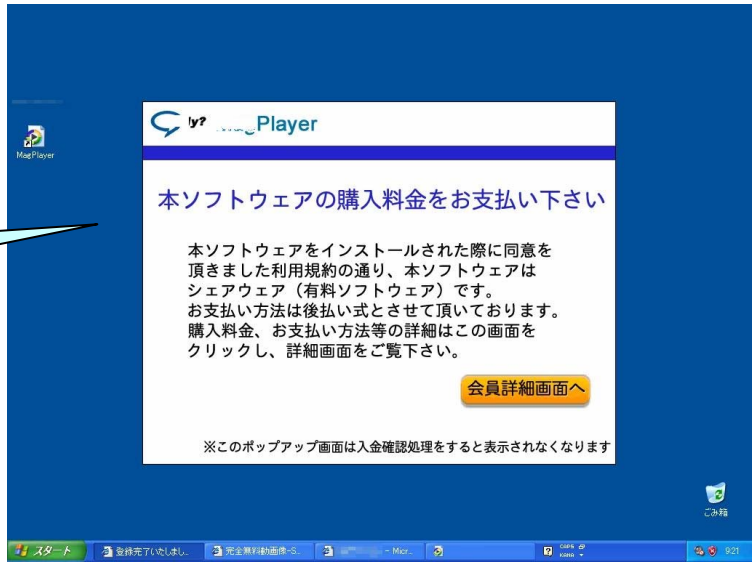
料金を請求する同じような手口として、押し売り行為があります。2006 年 8 月には、新しい押し売り行為の手口が確認されました。

【新しい押し売り行為の手口】

- 動画を見るために必要な専用プレイヤーとしてダウンロードさせる。その後、一定時間毎に請求書が表示されるようになってしまう。

「Download」をクリックしてプレイヤーをインストールすると、動画を見ることができると案内されている。

その手順通りにプレイヤーをインストールすると、下図のように料金を請求されることになる。



請求書画面は、一定時間毎に表示されるようになる。

有料・無料の記載もないような怪しいソフトはダウンロードしないようにしましょう！

これらの被害に遭わないよう、信頼できないサイトからの安易なダウンロードは避けるようにしましょう。

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、ご連絡ください。(P7.相談受付状況を参照)

(参考)
スパイウェア対策のしおり
http://www.ipa.go.jp/security/antivirus/shiori.html

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

		3月	4月	5月	6月	7月	8月
届出(a) 計		**38**	**15**	**13**	**22**	**15**	**50**
	被害あり(b)	10	7	6	20	8	30
	被害なし(c)	28	8	7	2	7	20
相談(d) 計		**24**	**27**	**23**	**32**	**31**	**24**
	被害あり(e)	12	15	11	19	18	13
	被害なし(f)	12	12	12	13	13	11
合計(a+d)		**62**	**42**	**36**	**54**	**46**	**74**
	被害あり(b+e)	22	22	17	39	26	43
	被害なし(c+f)	40	20	19	15	20	31

(1) 不正アクセス届出状況

8 月の届出件数は 50 件であり、そのうち**被害のあった件数は 30 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 24 件（うち 3 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 13 件でした。

(3) 被害状況

被害届出の内訳は、**侵入 17 件、ワーム感染 3 件、DoS 攻撃(*1) 2 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 ページの改ざんが 9 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 6 件でした。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 5 件ありました。

被害事例

［侵入］

（i）踏み台として悪用された？

事例	・通信ログ(*6)をチェックしていたところ、自組織で運用しているセカンダリ DNS(*7)サーバに対して、接続を許可していない IP アドレスからの接続記録があることを発見。 ・当該サーバを調査したところ、ルートキット(*8)と思われるファイルが置かれ、IRC(*9)サーバ環境が構築されていたことが判明。 ・サーバマシン更新時に実施した、接続を許可・拒否する IP アドレスのフィルタリング設定が不適切だったために外部からの攻撃をもろに受け、さらにログインパスワードが推測容易だったのが、侵入の原因と思われた。
解説・対策	この事例は、サーバマシンの入れ替え時の設定不備と、推測されやすいパスワードを設定してしまったことの**2 つのミスが重なったために起きています**。IRC サーバ環境を構築されていたということは、ボット(*10)ネットワークの一員の踏み台として使われていた可能性もあります。**日常あまり実施しない作業の際には、ミスや抜けの無い適切な設定を行えるように、手順書などをあらかじめ用意しておく**と良いでしょう。 （参考） IPA － 情報セキュリティ白書 2006 年版 http://www.ipa.go.jp/security/vuln/20060322_ISwhitepaper.html

（ii）ホームページ改ざん

事例	・ホスティングサービス(*11)を利用してウェブサイトを運用していたが、サイト上のホームページが改ざんされた。 ・同一サーバに収容されていた他ユーザのウェブサイトに設置されていたウェブアプリケーションのぜい弱性を突かれ、サーバ上のファイルを外部から不正に操作されていたとの連絡が、ホスティングサービス会社から入った。
解説・対策	この事例では、**本人に落ち度は無いにもかかわらず、ホームページ改ざんの被害を受けてしまっています**。このような場合の補償について、事前に確認しておくと良いでしょう。また、**ホスティングサービス業者選定の際には、ウェブアプリケーションのぜい弱性対策などのセキュリティ対策がきちんと実施されているかどうかを確認する**と良いでしょう。 （参考） IPA － 情報セキュリティ対策ベンチマーク http://www.ipa.go.jp/security/benchmark/

［アドレス詐称］

（iii）送信した覚えの無いメールが、エラーとして大量に返送されてくる

事例	・「宛先メールアドレスが存在しない」旨のエラー通知メールが、大量に送られて来た。 ・エラーが生じたというメールの詳細を見ると、広告・宣伝メールのスパム(*2)メールと思われた。送信元アドレスとして、自身のメールアドレスが設定されていた。しかし、全て自身では送信した覚えが無いもの。 ・あまりにも大量にエラー通知メールが送られて来るため、メールサーバの応答が遅くなることがある。
解説・対策	この事例のように、自身が送信したメールでない場合でも、エラー通知メールは送信元として書かれているアドレス宛に送られてしまいます。**極端に大量のエラー通知メールが送られてくると、メールサーバが過負荷に陥り、障害が起こる可能性もある**ため、注意する必要があります。普段よりも多くのメールが届いた場合に、その原因と送信元を特定し、場合によっては送信元の IP アドレスなどでフィルタリングを掛けるなどの対処を準備しておくべきでしょう。 なお、「特定電子メールの送信の適正化等に関する法律の一部を改正する法律（平成 17 年法律第 46 号）」が 2005 年 11 月 1 日に施行されました。これによれば、”送信者情報を偽った送信の禁止”が新たに謳われている（第 6 条）ため、今回のような違法メールの取締りが強化されると思われます。 （参考） （財）日本データ通信協会 － 迷惑メール相談センター http://www.dekyo.or.jp/soudan/top.htm IPA －「IP アドレス、メールアドレス等の詐称への対策」 http://www.ipa.go.jp/security/ciadr/cm01.html#spoofing

4. 相談受付状況

8 月の相談総件数は **793 件**でした。内訳は、**『ワンクリック不正請求』に関する相談**が**204 件**（7 月：159 件）、**『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**33 件**（7 月：43 件）、**Winny に関連する相談**が**14 件**（3 月：196 件、4 月：83 件、5 月：28 件、6 月：15 件、7 月：12 件）などでした。

IPA で受け付けた全ての相談件数の推移

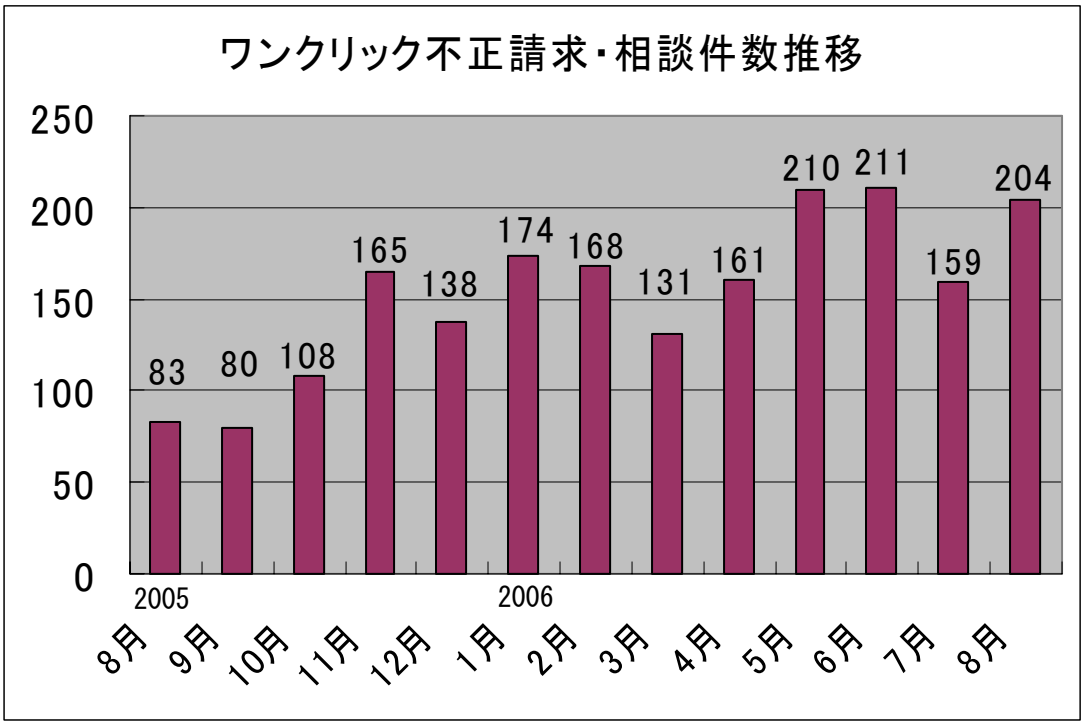
	3月	4月	5月	6月	7月	8月
合計	1056	904	846	773	767	793
自動応答システム	659	510	484	423	444	460
電話	296	306	295	283	257	280
電子メール	99	86	63	64	66	48
その他	2	2	4	3	0	5

※ 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）

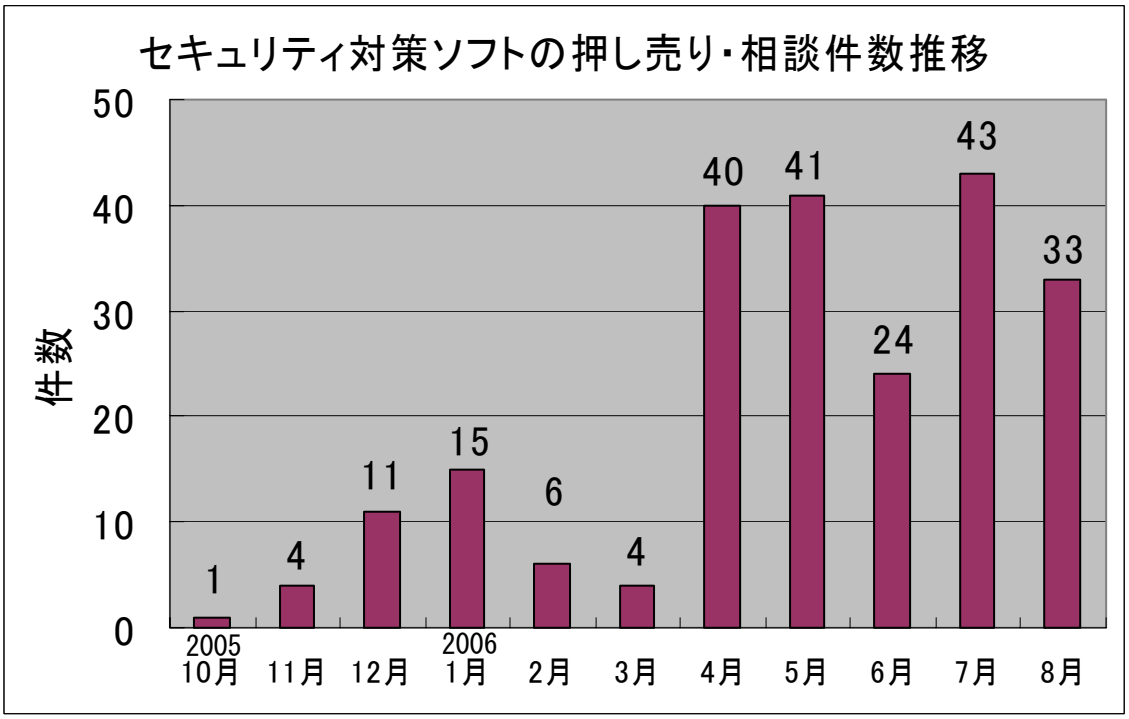
※ 「自動応答システム」： 電話の自動音声による応対件数
「電話」： IPA セキュリティセンター員による応対件数

※ 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。

ワンクリック不正請求相談件数の推移



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）新手のワンクリック不正請求？

相談	あるリンクをクリックしたらアダルトサイトにジャンプした。**画面をよく確認しないままクリックしていったら、料金を請求された**。パソコンを再起動しても、数分おきに請求書画面が表示される。登録したつもりはないのでお金は払いたくないし、請求書画面を消したい。
回答	連絡のあったサイトにアクセスしてみたところ、**「このサイトは有料」である旨トップページに表示がしてあるうえ、複数回、確認画面を経て登録完了画面に到達する**ことが分かりました。**お金を払うつもりが全く無いのであれば、トップページから先へは進んではいけません**。このようなケースですと、本人が登録をしたつもりは無くても、言い逃れができない可能性もあります。

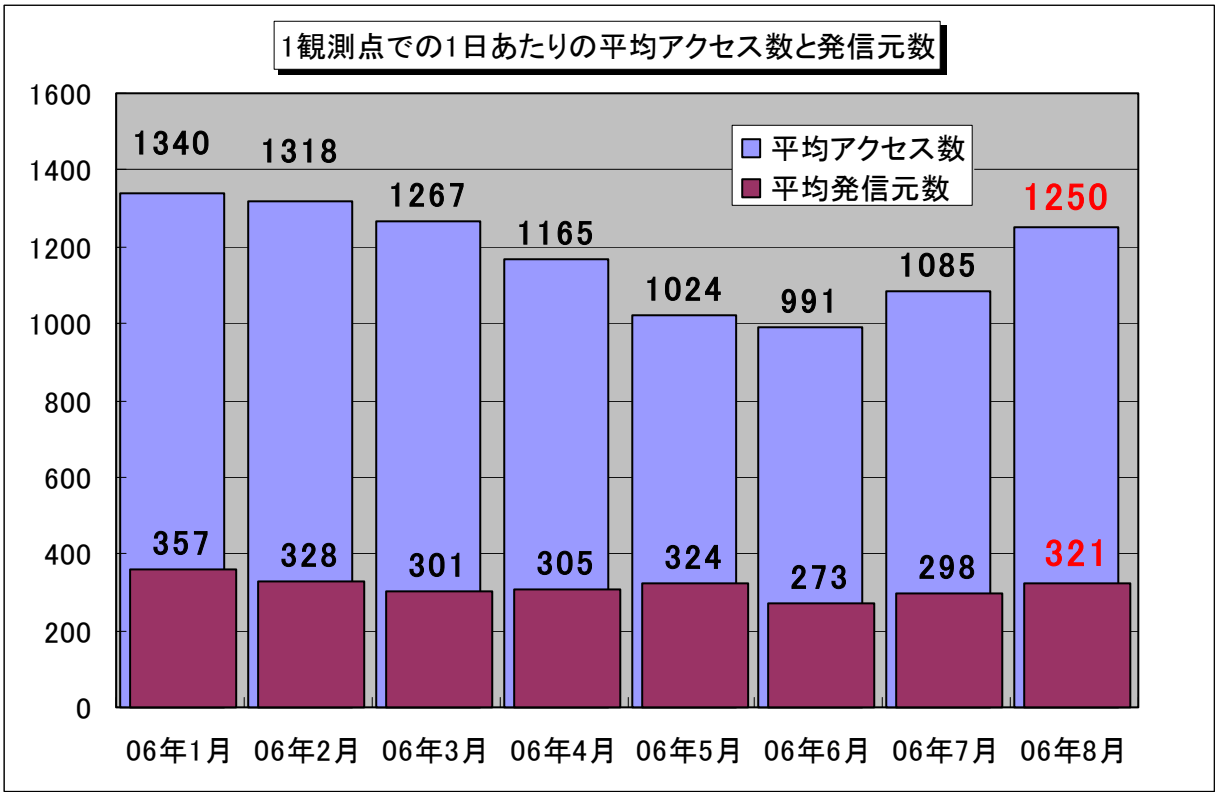
（ii）押し売りされたセキュリティ対策ソフトは削除したはずなのに・・・

相談	「あなたのパソコンはウイルスに感染しています」などという警告画面が出たので、言われるままにセキュリティ対策ソフトをダウンロードしインストール。しかしテレビのニュースで見て、それが信頼できないものだと知った。すぐにコントロールパネルの[プログラムの追加と削除]からアンインストールした。でもタスクバー内にはアイコンがあるし、購入を促す画面が出現する。 **※同様の相談が計 10 件寄せられました**。
回答	コントロールパネルの[プログラムの追加と削除]からアンインストールしようとすると、**リストから無くなるだけで、ソフトウェア自身は残ってしまうようです**。**プログラムがインストールされたフォルダの中にアンインストーラープログラムがある場合は、そのプログラムファイルを直接実行することでアンインストールできる場合があります**。IPA の相談窓口までご連絡ください。

5. インターネット定点観測での 8 月のアクセス状況

インターネット定点観測(TALOT2)によると、2006 年 8 月の期待しない(一方的な)アクセスの総数は、10 観測点で **387,534 件**ありました。1 観測点で 1 日あたり **321** の発信元から **1,250 件**のアクセスがあったことになります。

TALOT2 での1観測点の環境は、インターネットを利用される一般的な接続環境と同一なので、インターネットを利用される皆さんの環境へも同じくらいの一方的なアクセスがあると考えられます。言い換えれば、**あなたのコンピュータは、毎日、平均して、321 人の見知らぬ人(発信元)から、発信元一人当たり 4 件の不正と思われるアクセスを受けている**と言うことになります。



【図 5.1　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】

2006 年 1 月～2006 年 8 月までの各月の 1 観測点での 1 日あたりの平均アクセス数および、それらのアクセスの平均発信元数を図 1 に示します。この図を見ると、**期待しない（一方的な）アクセスは、先月より増加しました**。全体的なアクセス内容については、定常化していると言えますが、新しい Windows のぜい弱性を狙ったと思われるアクセスが発生しています。ご注意下さい。

8 月のアクセス状況は、全体的には 7 月とほぼ同じ状況ですが、**新しい Windows のぜい弱性を狙ったと思われる 139(TCP)ポートへのアクセスが発生しています**。既存の Windows のぜい弱性を狙っていると思われる不正なアクセスもあいかわらず多いようで、これらのアクセスの多くは、ボットに感染したコンピュータから送信されていると思われます。さらに、先月末からのアクセス(数)の増加傾向が続いており、パスワードクラッキングによるコンピュータへの侵入を狙う 22(TCP)ポートへのアクセスも増加しています。

139(TCP)ポートへのアクセスについては、新しい Windows のぜい弱性(MS06-040)を狙ったものと考えられます。このぜい弱性に対する攻撃(検証)コードが公開されており、ぜい弱性を狙った新しいワームや、攻撃コードが仕込まれたボットが広がっている可能性があります。

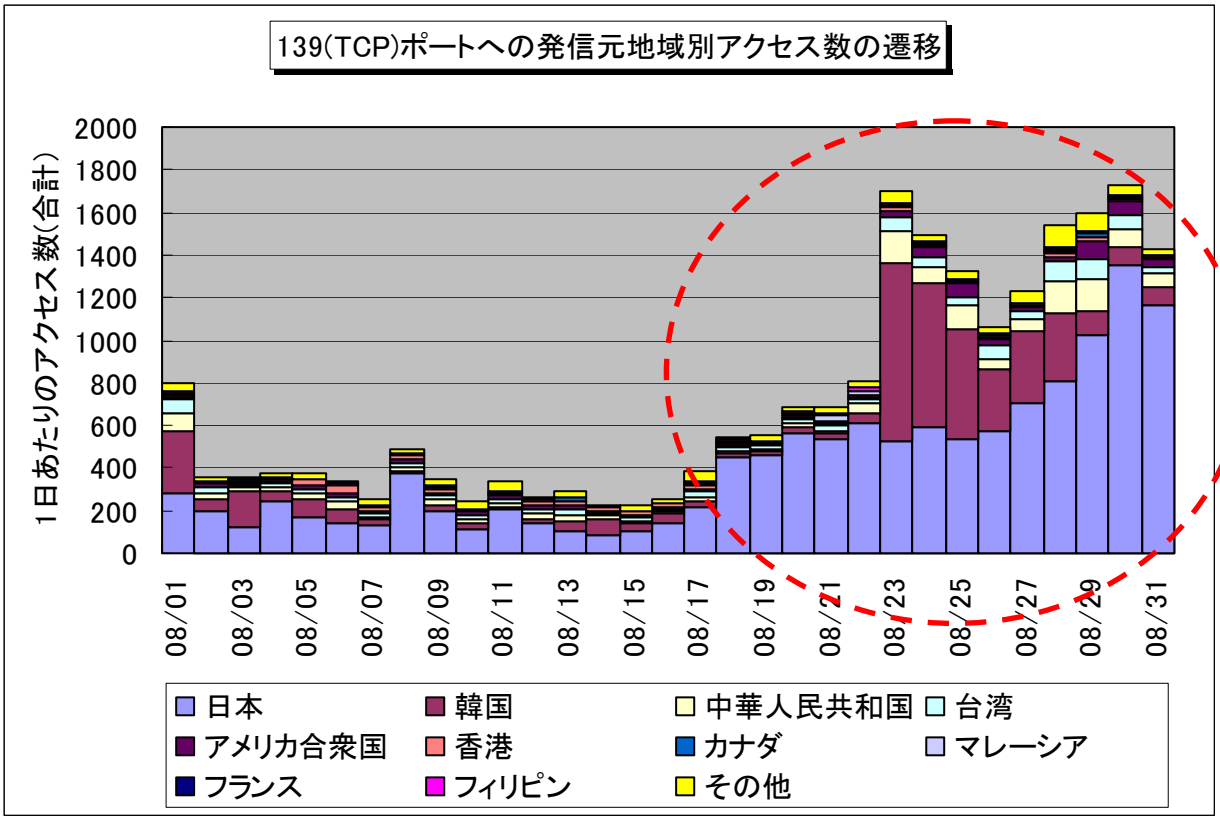
図 5.2 および図 5.3 に、139(TCP)ポートへの発信元地域別アクセス数と発信元数の遷移を示します。これらの図を見ると、8 月 18 日前後から発信元を国内とするアクセスが増加し、8 月 23 日から韓国方面を発信元とするアクセスが急増しています。実際には、国内からは被害報告や問い合わせがないため、国内での被害状況については分かりませんが、発信元となっている国内のコンピュータにはワームあるいはボットが感染しているものと思われます。国内のアクセス数が増加傾向にあることが危惧されます。韓国方面からのアクセスについては、発信元数から見ると、終息方向にあるようです。アクセスのパターン(同一の観測点に対するアクセス回数)によると、国内からのアクセスと韓国方面からのアクセスは、少し違う様子なので、種類の違う攻撃コード(ワームあるいはボット)と思われます。

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、8 月 10 日に Microsoft から発信されている Windows のぜい弱性を解消するパッチを適用し、さらに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。

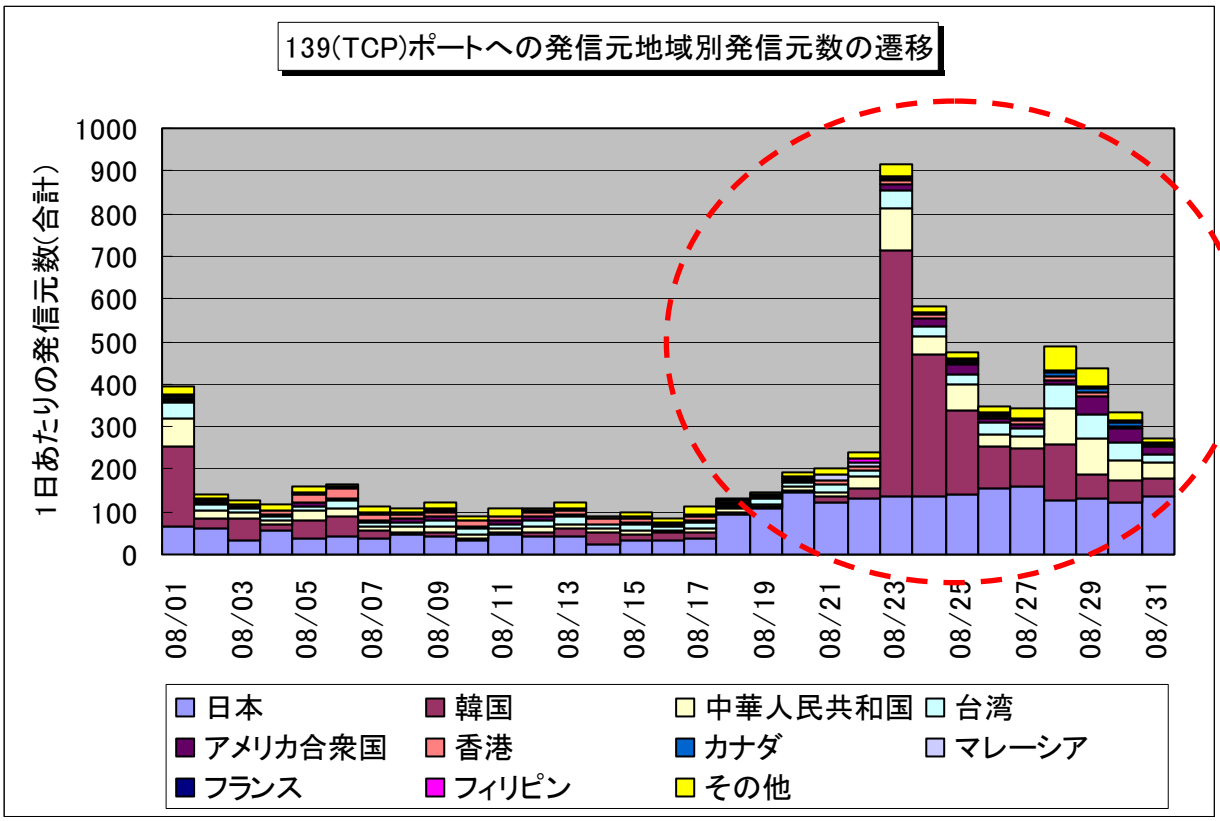
コンピュータの個人利用者は、以下の資料を参考にして、不正アクセス対策を実施して下さい。

■ 不正アクセス対策のしおり

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



【図 5.2 2006 年 8 月の 139(TCP)ポートへの発信元地域別アクセス数の遷移】



【図 5.3 2006 年 8 月の 139(TCP)ポートへの発信元地域別発信元数の遷移】

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/TALOT2-0609.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) **DoS 攻撃** (Denial of Services attack)
サーバに大量のデータを送って過大な負荷をかけ、サーバのパフォーマンスを極端に低下させたり、サーバを機能停止に追い込んだりする攻撃のこと。

(*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。

(*6) **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。

(*7) **DNS** (Domain Name System)
インターネットにおけるホスト名と IP アドレスとを対応させるシステムのこと。インターネット上にある全世界の DNS サーバが協調して動作する、階層的な分散型データベースシステムである。

(*8) **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。

(*9) **IRC** (Internet Relay Chat)
チャット(接続者同士のリアルタイムな会話)システムのこと。インターネット上の IRC サーバに、専用のソフトウェアを利用してアクセスすることで、複数のユーザとの間でメッセージの交換が出来る。ファイル通信にも対応する。

(*10) **ボット** (bot)
コンピュータウイルスの一種で、コンピュータに感染し、そのコンピュータを、ネットワーク(インターネット)を通じて外部から操ることを目的として作成されたプログラムのことである。

(*11) **ホスティングサービス** (hosting service)
事業者がインターネットに接続し公開しているウェブサーバ内のディスク容量の一部を、顧客に間貸しするサービスのこと。レンタルサーバとも呼ばれることがある。

■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）
https://isec.ipa.go.jp/benchmark-new/

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

「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）