IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
2006 年 7 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 6 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 6 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：**
**「パスワードを一つ残らず、きちんと管理しましょう！」**
**―パスワード　ともだちにだって　ないしょだよ※―**

**※（情報セキュリティ標語 2006 入選作　愛知県・名古屋市立滝ノ水小学校 / 森 明日翔さん）**

最近の不正アクセス届出や相談の内容を振り返ると、パスワードを破られたことによる被害が非常に多くなっています。

**【不正アクセス**届出で**被害のあったもののうち、ID やパスワードの不備**が原因であったもの】

| | |
|---|---|
| 2004 年 | 約 13%　(72 件中 9 件) |
| 2005 年 | 約 24%　(176 件中 42 件) |
| 2006 年 | 約 34%　(71 件中 24 件)　※1 月～6 月まで |

インターネットに接続したり、メールを受信したり、インターネット上のサービスなどを利用したりする際には、利用者を判別するための ID(Identification)と、利用者本人であることを証明するためのパスワードが必要なことがほとんどです。つまり、ID やパスワードが何らかの原因で盗まれたり他人に知られたりすると、**悪意を持った人が正規の利用者になりすますことができてしまう**ため、様々な被害が発生する恐れがあります。

**【IPA に寄せられた直近の相談のうち、パスワードが破られたことが原因の被害事例】**

- **フリーメール**(*1)**サービス**の自分のアカウント(*2)が、**誰かに勝手にログインされて使われた**。パスワードを変更しようとしても、既にパスワードが勝手に変更されていてログインできない。
- **ネットオークション**の自分のアカウントが、誰かに勝手に使われて**不正出品に悪用**された
- メールでやり取りしていた秘密の情報が、インターネット上の掲示板に書かれていた。誰かに**メールサーバに勝手にアクセスされ、メールを読まれていた**気配がある。

この他、過去には次に挙げるような被害なども報告されています。

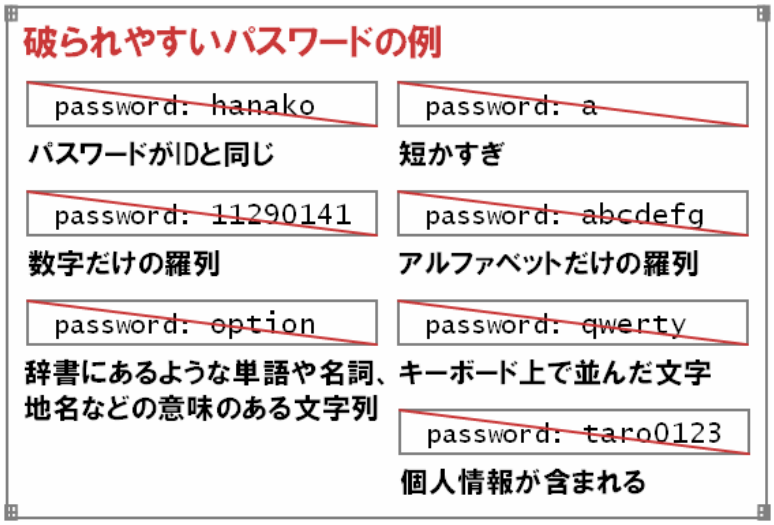
- **預金を勝手に引き出される**
- **ホームページやブログなどの内容が書き換えられる**
- **パソコンが外部から乗っ取られる**

パスワードが破られる理由としては、推測が容易な内容だったり他人に教えてしまったりしたというのはもちろんのこと、**総当り攻撃**や**辞書攻撃**(次ページ参照)といった手法で自動的にパスワードを調査する**パスワードクラッキング**(*3)**ツール**の存在が挙げられます。

このような被害を最小限に食い止めるには、まずは**自身が持っている ID やパスワードを全て洗い出し**、次に挙げたようになっているかどうかチェックするとともに、**何か問題が起こった時の連絡先を事前に調べておく**ことが大切です。

**【パスワードの設定・管理方法】**

- **安易な語句の選択を避ける（ID と同じ文字列など）**
- **語数をできるだけ長く**
- **できる限りアルファベットの大文字小文字、数字、記号を混ぜる**
- **辞書に載っていない語句を選ぶ**
- **語列に規則性を持たせない**
- **個人情報を含むものを避ける（氏名、誕生日、電話番号など）**
- **定期的に変更する（初期パスワードをそのまま使わない）**
- **絶対に他人に教えない**
- **パスワードが書いてある紙などを他人の目に触れさせない**




（参考）

＊1：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です。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います。

語数を長くする、大文字小文字・数字・記号を混ぜることにより、総当り攻撃に対して強いパスワードとなります。また、パスワードを定期的に変更することは、総当り攻撃に対して非常に有効です。

＊2：辞書攻撃

辞書にある単語などを片端から試行する攻撃方法です。

もし、パスワードの文字列に辞書にあるような単語や、人名、商標名といったものを使用している場合、辞書攻撃によってパスワードを解析される可能性が高くなります。一般的な英和辞典が約 5 万語ですが、辞書攻撃に使われるワードリストは 80 万語とも 100 万語とも言われています。

パスワード解析に使用される辞書には、英和辞典などに掲載されている単語だけでなく、人名、地名といったものや、よく使われるユーザ名などが登録されています。さらに、規則性を持たせた文字列も登録されています。たとえば″12345″ や″abcde″といったものです。これを順に試していくわけです。

この辞書には、変換規則を考慮したデータもあります。たとえば、″orat″のように″taro″の文字列を逆順にしたり、″tAro″のように一部の文字を大文字にすることや、″taro1″のように先頭や末尾に数字を付けるというものもあります。

ユーザ名や固有名詞を使用していても数字や大小文字を使用しているから大丈夫ということはありません。

## 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 164 万個**と、5 月の 178 万個から 7.9%の減少となりました。
また、6 月の届出件数(※2)は、**3,547 件**となり、5 月の 3,651 件から 2.8%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。
・6 月は、寄せられたウイルス検出数約 164 万個を集約した結果、3,547 件の届出件数となっています。

検出数の1位は、**W32/Netsky で約 133 万個 、2 位は W32/Mytob で約 14 万個、3 位は W32/Bagle で約 7 万個でした。**

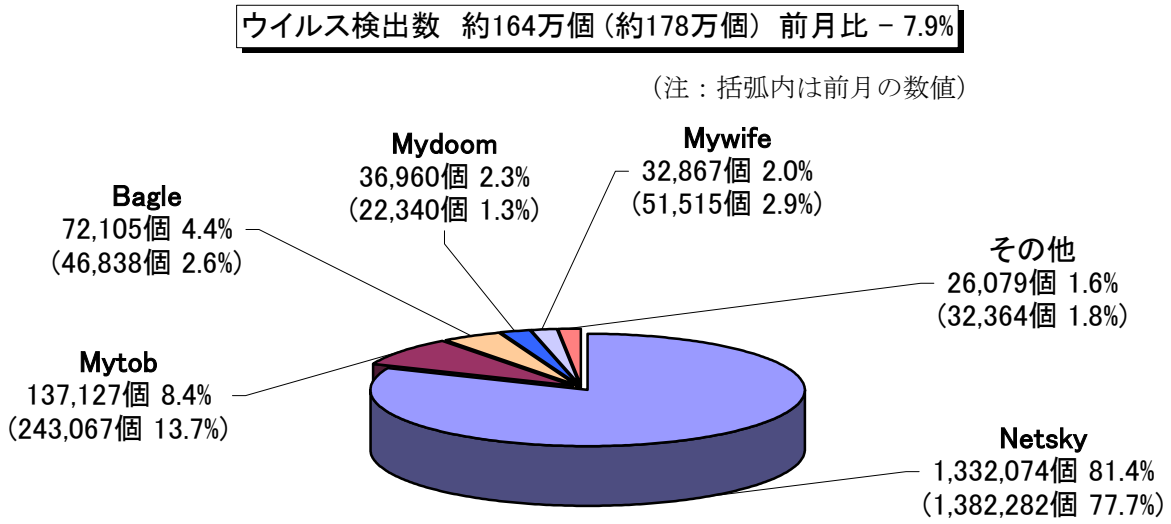



図:1-1

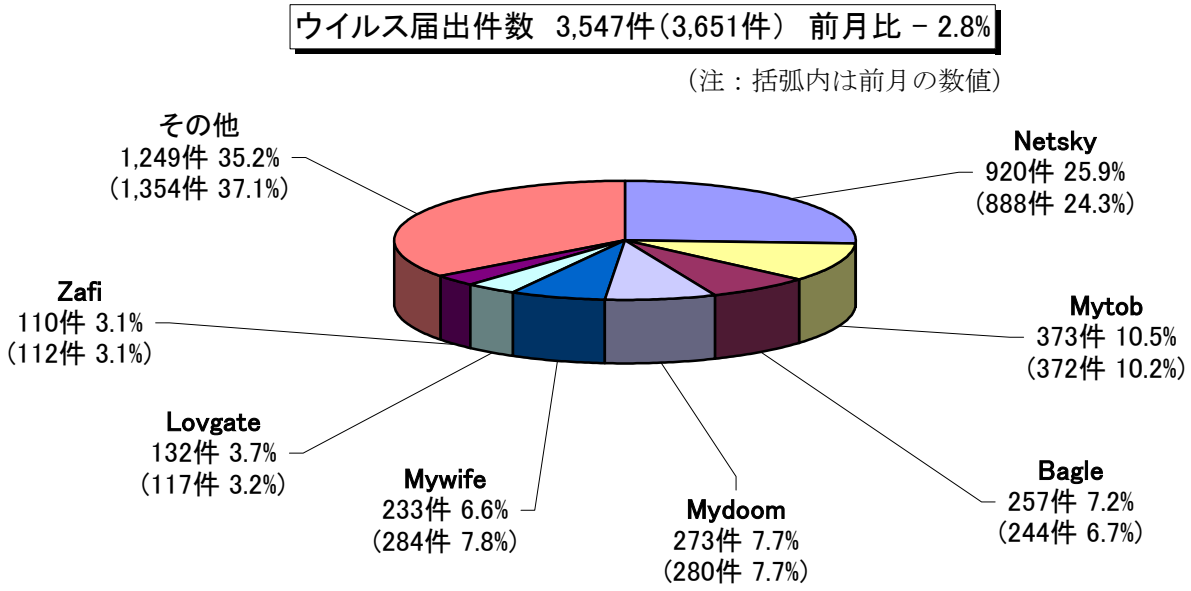
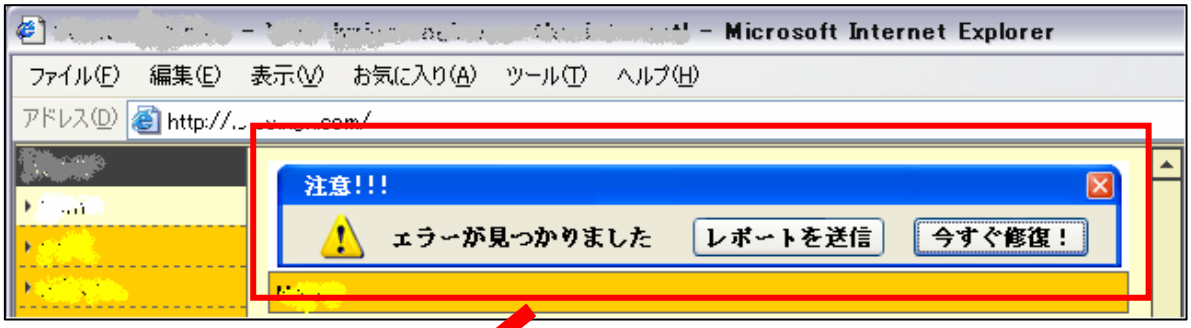


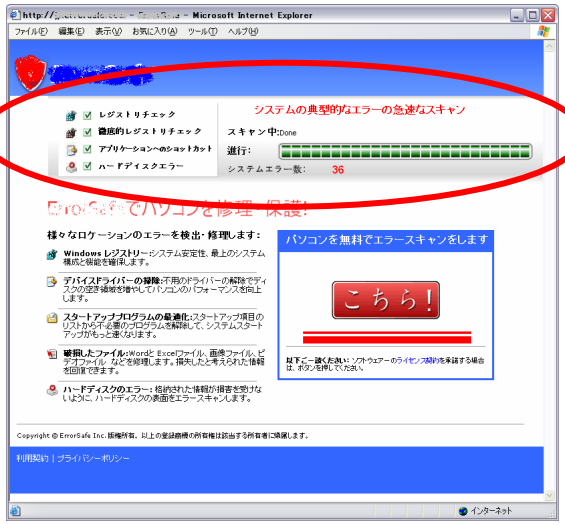

図:1-2

## 2. セキュリティ対策ソフトの押し売りについて

「エラーが見つかりました」、「感染している可能性があります」などのメッセージを表示して、「セキュリティ対策ソフトウェア」と称するものを購入させようとする、押し売りに関する相談が 2006 年 4 月頃より多く寄せられています。(2006 年 3 月:4 件、4 月:40 件、5 月:41 件、6 月:24 件)
これらは、以下のような手順で対策ソフトをダウンロードさせようとするものです。

【事例:エラーが見つかったと表示するケース】

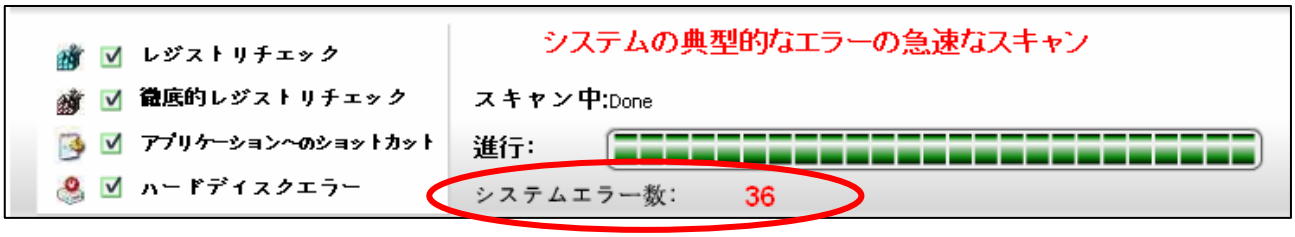



ホームページのバナー広告(上図)をクリックすると、当該対策ソフトのサイトにアクセスしてしまう。

サイトにアクセスすると、パソコン内をスキャンしているかのような表示がされる。(下の拡大図参照)

その結果、システムエラーが見つかったという表示がされ、さらにチェックするには「**こちら!**」(左図)から対策ソフトをダウンロードするように促している。




このようなメッセージが表示されても、実際には、ほとんどの場合、パソコンにエラーは発生していません。ユーザを脅して押し売りをするようなものです。このメッセージに従い、対策ソフトウェアをインストールすると、「エラーを修復するためにはソフトを購入する必要があります」となり、クレジットカード決済を求める画面が表示されます。

**正規のセキュリティ対策製品の製造・販売者からは、脅しのようなメッセージをユーザに表示して購入を迫るようなことはありません。**ましてやいきなりプログラム(対策ソフト)をダウンロードさせるような販売方法はとられていませんので、慌ててダウンロードしないようご注意ください。

「インストールしてしまったかもしれない」、「感染しているかもしれない」と心配な場合は、以下のサイトで無料のオンラインスキャンを利用できますので、検査してください。

オンラインスキャン（ウイルス検査サービス）

◆シマンテック　セキュリティチェック
http://www.symantec.com/region/jp/securitycheck/
◆トレンドマイクロ　オンラインスキャン
http://www.trendmicro.co.jp/hcall/
◆マカフィー　フリースキャン
http://www.mcafee.com/japan/mcafee/home/freescan.asp
◆スパイウェアガイド － オンライン スパイウェア検出
http://www.shareedge.com/spywareguide/txt_onlinescan.php

（ご参考）
今月の呼びかけ：「セキュリティ対策ソフトウェアの押し売りに注意！！」
― 怪しげな警告を真に受けるな！！ ―　【2006 年 4 月分】
http://www.ipa.go.jp/security/txt/2006/05outline.html
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**

| | | 1月 | 2月 | 3月 | 4月 | 5月 | 6月 |
|---|---|---|---|---|---|---|---|
| **届出(a) 計** | | **50** | **26** | **38** | **15** | **13** | **22** |
| | 被害あり(b) | 13 | 15 | 10 | 7 | 6 | 20 |
| | 被害なし(c) | 37 | 11 | 28 | 8 | 7 | 2 |
| **相談(d) 計** | | **43** | **42** | **24** | **27** | **23** | **32** |
| | 被害あり(e) | 23 | 24 | 12 | 15 | 11 | 19 |
| | 被害なし(f) | 20 | 18 | 12 | 12 | 12 | 13 |
| **合計(a+d)** | | **93** | **68** | **62** | **42** | **36** | **54** |
| | 被害あり(b+e) | 36 | 39 | 22 | 22 | 17 | 39 |
| | 被害なし(c+f) | 57 | 29 | 40 | 20 | 19 | 15 |

### （1）不正アクセス届出状況

**6 月の届出件数は 22 件**であり、そのうち**被害のあった件数は 20 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 32 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 19 件でした。

## （3）被害状況

被害届出の内訳は、**侵入 12 件、ワーム感染 4 件、DoS 攻撃 1 件、その他（被害あり）3 件**でした。

侵入届出の内訳は、SSH(*4)で使用するポート(*5)への攻撃を受けた結果侵入されたというものが 5 件、フィッシング(*6)に悪用するための Web コンテンツを設置させられていたというものが 1 件、ウイルス添付のフィッシングメール送信の踏み台にされたものが 1 件、などでした。

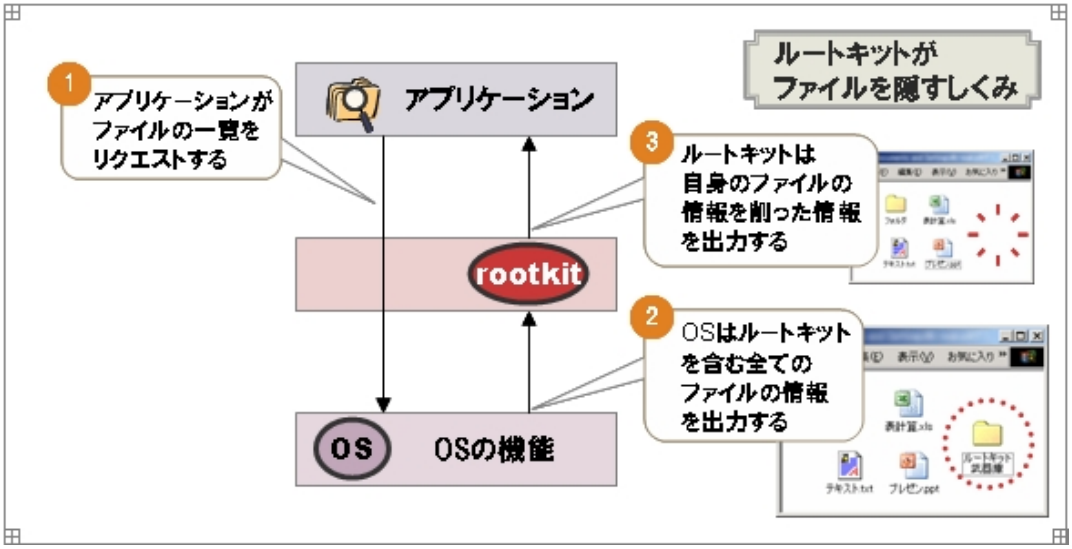
## 被害事例

### ［侵入］

#### （i）SSH(*4)で使用するポート(*5)への攻撃

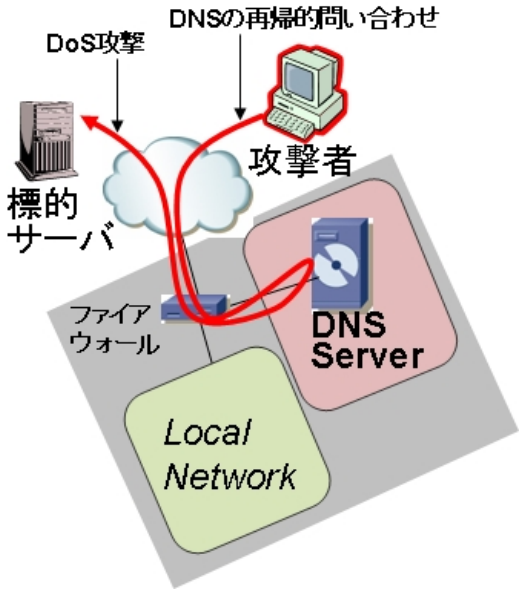
| | |
|---|---|
| **事例** | ・「あなたの組織のマシンが、不特定多数のマシン宛に SSH スキャン(*7)を行っている」と組織外から通報が入った。このため、自組織内の当該マシンのログ(*8)を調査したところ、SSH(*4)で使用するポート(*5)からパスワードを破られて侵入された形跡があることを発見。<br>・他にも、侵入までは至らなかったものの、多数のパスワードクラッキング(*3)攻撃の形跡も発見。<br>・調査を進めた結果、当該マシン内から SSH スキャンツールやウイルスなどの不正プログラムを発見したため、削除した。<br>・推測が容易だったパスワードが設定されていたことが原因と思われた。<br>・組織外から SSH 経由でログインを許可する通信を制限するため、パケットフィルタリングを強化することとした。 |
| **解説・対策** | この事例は、推測容易なパスワードを破られて侵入され、他のマシンへの攻撃の踏み台とされてしまった典型的なものと言えます。**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。**<br>自動攻撃ツールが用いられるためか、SSH で使用するポートが狙われる機会はなおも多いようです。**SSH 運用時には、ログインの際に公開鍵認証(*9)などの強固な認証を採用することを推奨します。**<br>（参考）<br>IPA - 安全なウェブサイトの作り方<br>http://www.ipa.go.jp/security/vuln/20060131_websecurity.html |

### （ii）ルートキット(*10)の埋め込み

| | |
|---|---|
| **事例** | ・「組織外のマシンへの攻撃パケットが観測された」と自組織のネットワーク管理者から通知を受けた。自組織内を調査したところ、外部へ攻撃を行っていたマシンを発見。このマシンは、ウイルスに感染していた。<br>・念のため当該マシン以外についても不正プログラムチェックツールを用いて調査したところ、Linux をインストールした複数のマシン内からルートキット(*10)と思わしきプログラムが検出された。<br>・ルートキットが仕込まれていた恐れのあるマシンは、即、ネットワークから切り離し、初期化することとした。 |
| **解説・対策** | この事例は、ウイルス感染マシンを発見したついでに調査範囲を広げたおかげで、他の重大な問題が明るみに出たという幸運な例です。特に**ルートキットは自分自身を見付かりにくくするため、通常はその存在になかなか気付くことができないものです**。ルートキットが仕込まれると、**システムファイルそのものが信頼できないものにすり替わっている可能性も高い**ことが、その理由の一つです（下図参照）。ルートキットを検出するには、Linux 系の OS であれば、chkrootkit や Rootkit Hunter といったツールが有効です。もしルートキットが検出された場合、前述の理由から一般的には**マシンを初期化するのが最善の方法**となります。<br>  <br><br>図 3-1：ルートキットがファイルの存在を隠すしくみ<br>（参考）<br>IPA － 情報セキュリティ白書 2006 年版<br>http://www.ipa.go.jp/security/vuln/20060322_ISwhitepaper.html<br>chkrootkit<br>http://www.chkrootkit.org/<br>Rootkit Hunter<br>http://www.rootkit.nl/projects/rootkit_hunter.html |

[DoS 攻撃(*11)]

### （iii） DNS(*12)サーバの設定ミスを利用した攻撃

| | |
|---|---|
| **事例** | ・「DNS(*12)サーバに対する組織外からの再帰的問い合わせ(*13)を、毎分 50 件ほどの頻度で受けており、組織外のサーバに対する DoS 攻撃(*11)をする結果となっている」との指摘を、自組織のネットワーク管理者から受けた。<br>・メールサーバとして使用しているマシンの設定変更の際、当該マシンにおいて通常は停止してあるはずの DNS サーバ機能を誤って起動させてしまった。さらに、DNS サーバの設定が組織外 DNS クライアントからの再帰的問い合わせを受け付けるようになっていたことが原因。<br>・DNS サーバ機能が誤って起動された場合でも不正に使用されないよう、設定を変更した。 |
| **解説・対策** | この事例では、ある設定変更の際の誤操作と、普段は使用しない機能を初期設定（この場合は外部からの再帰的問い合わせを許可する）のまま放置しておいたことが、同時に起こったことが原因でした。**他サーバへの攻撃の踏み台として悪用されないためにも、DNS サーバの設定や動作状況を再確認して適切な対策をしましょう。**<br>  <br><br>図 3-2：DNS サーバへの再帰的問い合わせを利用した攻撃<br>（参考）<br>JPRS - DNS の再帰的な問合せを使った DDoS 攻撃の対策について<br>http://jprs.jp/tech/notice/2006-03-29-dns-cache-server.html |

## 4. 相談受付状況

6 月の相談総件数は **773 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 **211 件**(5 月 :210 件)と、先月に記録した今までの最高件数をさらに更新しました。また、セキュリティ対策ソフトの押し売りのような行為に関する相談は **24 件**(5 月 :41 件)と、なおも高い水準で推移しています。その他は、**Winny に関連する相談**が **15 件**(3 月 :196 件、4 月 :83 件、5 月 :28 件)などでした。

### IPA で受け付けた全ての相談件数の推移

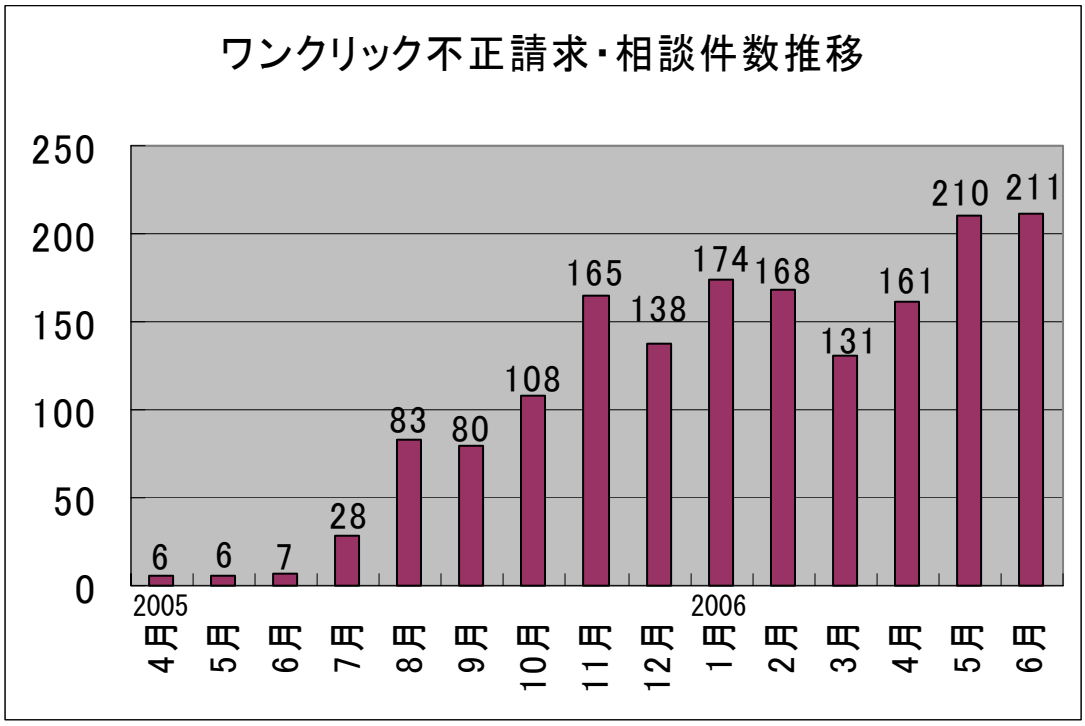
| | 1月 | 2月 | 3月 | 4月 | 5月 | 6月 |
|---|---|---|---|---|---|---|
| 合計 | 748 | 834 | 1056 | 904 | 846 | 773 |
| 自動応答システム | 425 | 479 | 659 | 510 | 484 | 423 |
| 電話 | 228 | 258 | 296 | 306 | 295 | 283 |
| 電子メール | 87 | 90 | 99 | 86 | 63 | 64 |
| その他 | 8 | 7 | 2 | 2 | 4 | 3 |

※ 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



主な相談事例は以下の通りです。

### （i）あるサイトの登録 ID とパスワードが知られている？

| | |
|---|---|
| **相談** | あるサイトで、サービスを利用するために ID とパスワードを登録した。ある日、自分は何も利用していなかったはずなのに、明らかに誰かが利用したと思われるような形跡があった。このサイトでは、パスワードを忘れてしまった場合には、あらかじめ登録してあるメールアドレス宛にパスワード情報を送信してくれるようになっている。しかし、そのメールアドレス宛に届いているメールも読まれている可能性がある。どうすればよいか。 |
| **回答** | この事例では、**サイトに登録したパスワードそのものが知られていた**か、その**サイトに登録したメールアドレスとメール受信のパスワードが知られていた**か、この両方が心配です。念のため両方のパスワードを変更しましょう。何らかの二次被害が発生した場合は、それぞれのサイト管理者に相談しましょう。状況に応じて、警察機関に相談するのも良いでしょう。<br>(ご参考)<br>都道府県警察本部のサイバー犯罪相談窓口等一覧<br>http://www.npa.go.jp/cyber/soudan.htm |

### （ii）フリーメール用のパスワードが変更されてしまった？

| | |
|---|---|
| **相談** | 自分が登録していたフリーメールサービスアカウントのパスワードが何者かによって変更されたらしく、ログインできなくなった。さらに、自分の名を騙られて嘘の情報が発信されてしまっている。アカウントを削除してもらおうと思ったが、フリーメールサービスの登録時に自身を証明できる情報を記入しなかったために、取り合ってもらえない。 |
| **回答** | **フリーだからといって、ユーザ登録時に嘘の情報や個人を特定できる情報を記入しなかった場合、最初に登録したのが自分自身であることを証明できません**ので、取り返しの付かないことになりかねません。とは言え、個人情報をやみくもに相手に知らせるのも危険ですから、登録先サイトが信頼できるのかを十分確認するとともに、必要最低限の情報しか書き込まないようにしましょう。 |

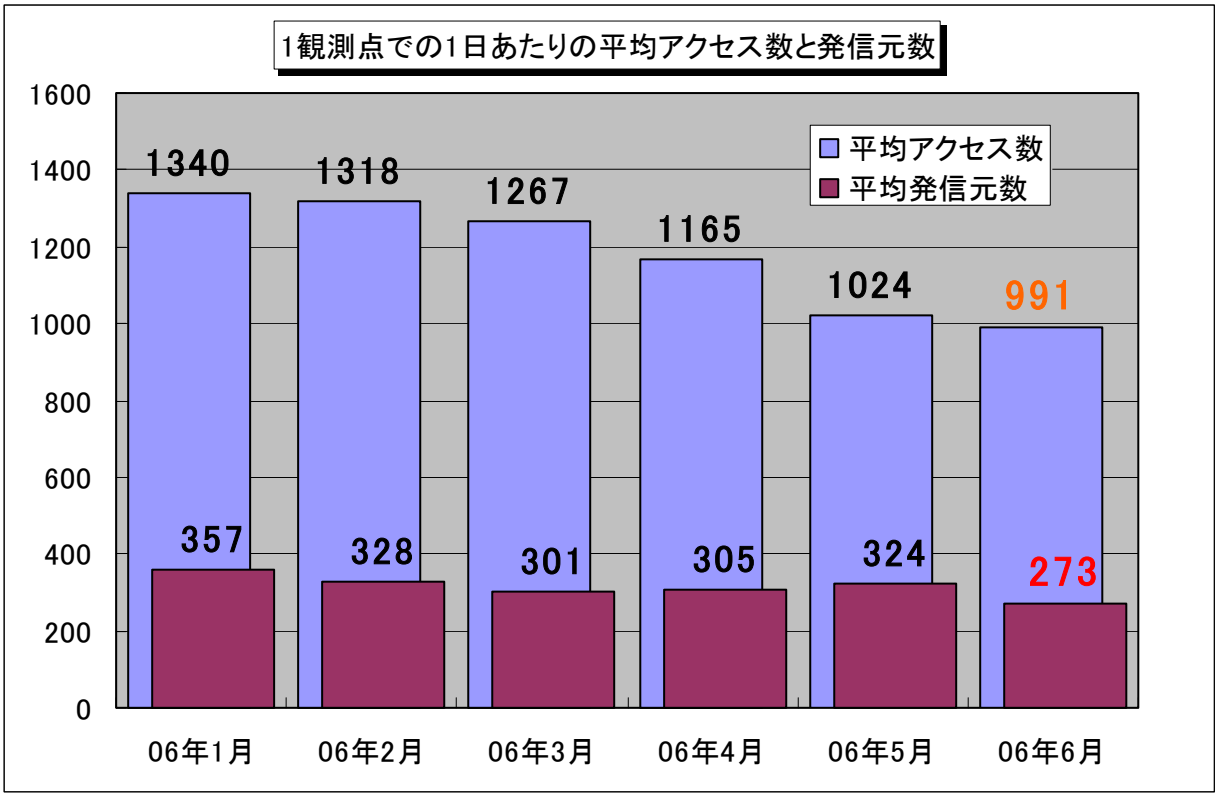
### （iii）アダルトサイトでワンクリックしたら・・・

| | |
|---|---|
| **相談** | アダルトサイトで画像をクリックしたら料金請求書が表示された。その後もパソコン上に数分おきに請求書が表示される。複数のウイルス対策ソフトでスキャンしても、何も検出されない。パソコンを初期化するしかないのでしょうか。 |
| **回答** | ウイルス対策ソフトで何も検出できなくても、**請求書に書かれている「サイト名」「サービス名」「連絡先」などの情報が分かれば、ほとんどの場合は不正プログラムを特定し削除できます**。あきらめずに、IPA セキュリティセンターに相談してください。また、Windows XP や Me であれば、**「システムの復元」機能を使うと、当該アダルトサイトを訪れる以前の状態に戻すことができる場合があります**。Windows XP であれば、<br>[スタート]－[すべてのプログラム]－[アクセサリ]－[システムツール]－[システムの復元]で、実行できます。 |

## 5. インターネット定点観測での 6 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 6 月の期待しない(一方的な)アクセスの総数は、10 観測点で **297,445 件**ありました。1 観測点で 1 日あたり **273** の発信元から **991 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、273 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 6 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、緩やかに減少傾向にあるようです**。アクセス内容については、定常化していると言えます。

6 月のアクセス状況は、5 月とほぼ同じ状況です。Windows の脆弱性を狙っていると思われる不正なアクセスが多いようで、これらのアクセスの多くは、ボット(*11)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。

特にアクセス数の多い 135(TCP)ポート,445(TCP)ポートへのアクセスは、Windows の脆弱性を狙っています。また、Windows Messenger サービスを悪用したポップアップスパムメッセージの 1026(UDP)/1027(UDP)ポートへのアクセスは、継続しています。

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/TALOT2-0607.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) フリーメール（free mail）
インターネットを利用して、無料で電子メールをやり取りできるサービスのこと。

(*2) 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。

(*3) 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。

(*4) 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。

(*5) 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。

(*6) フィッシング（Phishing）
正規の金融機関など実在する会社のメールや Web ページを装い、それを見た利用者の ID やパスワードなどを詐取しようとする行為のこと。「釣り」を意味する「fishing」が語源だが、ハッカーの命名規則に則って"f"を"ph"に置き換えたという説、「洗練された」という意味の英語 "sophisticated"と"fish"とを組み合わせた造語という説、"password harvesting fishing"の短縮形という説、などがある。

(*7) SSH スキャン
サーバで SSH サービスが動作しているかを調べるための操作。パスワードを破るための操作を同時に行う場合もある。

(*8) 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。

(*9) 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。

(*10) 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。

(*11) DoS 攻撃 (Denial of Services)
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。

(*12) 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。

(*13) DNS の再帰的問い合わせ (Recursive DNS Query)
DNS における再帰的問い合わせとは、DNS クライアントからの問い合わせのことを指す。組織外部にあるクライアントからの問い合わせには応答しない設定にするのが一般的。DNS サーバはその機能から、キャッシュサーバ(Recursive Server)とコンテンツサーバ(Authoritative Server)の 2 つに分類されるが、再帰的問い合わせを処理するのはキャッシュサーバである。

■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


## 『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

これは、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 /<br>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 /<br>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 /<br>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 /<br>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 /<br>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 /<br>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 /<br>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 /<br>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 /<br>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 /<br>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）