Information-technology
Promotion
Agency, Japan

第 12-23-259 号
2012 年 9 月 5 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［2012 年 8 月分］について

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）は、2012 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。

1. 今月の呼びかけ

「 情報を抜き取るスマートフォンアプリに注意！ 」
～ スマートフォンの中の個人情報が狙われています ～

2012 年 8 月は、スマートフォン（Android OS）の電話帳の中身を窃取する不正なアプリケーション（以下、アプリ）の情報が多く見受けられました。これは悪意を持った攻撃者が、不正なアプリをダウンロードさせるリンク先が書かれたメールを、不特定多数の利用者にばら撒いていたためです。

この不正なアプリは、ウイルスそのものですが、発見当初、セキュリティ対策ソフトを導入していても検知されないことがあり、インストール後に起動してしまうと情報窃取の被害に遭ってしまうものでした。なお、アプリの名前や送られてきたメールの文章は全て日本語であるため、日本人を狙った攻撃だと考えられます。

IPA では、この不正なアプリを入手し解析を行いました。ここでは、攻撃者が不正なアプリを利用者のスマートフォンへインストールさせるまでの手口と、解析結果をもとに不正なアプリの動作の一例を解説し、被害に遭わないための対策を紹介します。

図 1-1：不正なアプリが情報を流出させるイメージ図

（1） 不正なアプリをインストールさせるまでの手口

不正なアプリを利用者のスマートフォンへインストールさせるまでの手口は、次の二種類を確認しています。

（a）メールから不正なアプリのダウンロードを誘導する手口

新しいアプリの紹介と偽ったメール（図 1-2、1-3 参照）が不特定多数に送りつけられたようです。このメールに記載されたリンク先をクリックすることで不正なアプリがダウンロードされ、利用者にインストールさせようとします。

いつもご利用有難うございます。
皆さんが一度は経験のある、電波の圏外！

山や屋内、地下等々…

電話を掛けたくても繋がらない。。
メールを送りたくても届かない。。
ネットを見たくても接続出来ない。。

この度、この様な状況でお困りの方の為に開発されたのがっ！

▼コチラ！！
http://[redacted]

その名も！《電波改善（デンパカイゼン）》

その名の通り、電波の悪い状況であっても、改善してくれるアプリなんです。

簡単にアプリの説明をさせて頂きますと、

通常の各回線(NTTやKDDI等々…)からの電波が届いていない場所で、このアプリを起動しますと近くの別回線を検索。
そのまま、その回線に繋がるという仕組みになっております。

これで、もう繋がらないという問題は無くなります！！
是非一度、お試しください！！

※一部、未対応端末が御座いますのご了承ください。

図 1-2：メール文例 1

いつもGoogle playをご利用有難うございます。

この度、Androidをご利用の皆様より最も多かった、《充電がすぐ切れる》と言うご意見を基に、新アプリを開発致しましたのでご紹介させて頂きます。

〔充電が長持ちするアプリ〕 ↓ダウンロードはコチラ
ttp://[redacted].apk

設定方法や項目名は端末によって異なることがありますので、ご了承下さい。

設定方法を紹介しておりますがAndroidの利便性を損なってしまう設定もあるので、 バッテリー消費と自分にあった設定のバランスを見つける参考にしてみて下さい。

※一部、未対応端末が御座いますのご了承ください。

図 1-3：メール文例 2

（b）SNS（ソーシャルネットワーキングサービス）を悪用した手口

趣味などの情報を共有する目的の SNS コミュニティサイトに、興味を引く内容と共に不正なアプリをダウンロードさせるリンク先が書かれた文章（図 1-4 参照）が投稿されていました。

コミュニティに参加している利用者は、同じ趣味を持つ人の投稿だと思い、あまり警戒をしないでリンク先をクリックしてしまう可能性があります。

図 1-4：SNS への投稿文例

（2） 不正なアプリの動作

IPA は、届出を受け付けた不審なメール（図 1-2 参照）から「電波改善」という不正なアプリがダウンロードされることを確認し、このアプリを解析しました。

1.図 1-2 のメール内に書かれているリンク先をタッチすると、不正なアプリ（.apk ファイル）のダウンロードが開始されます。ダウンロードされた.apk ファイル名をタッチすると、インストール開始の有無を聞いてきます（図 1-5 参照）。**ここで注意しなければならないことは、このアプリは電波を改善するものと謳っているにもかかわらず、個人情報の読み取り許可を求めていることです。**［インストール］をタッチすると、不正なアプリがインストールされてしまいます。

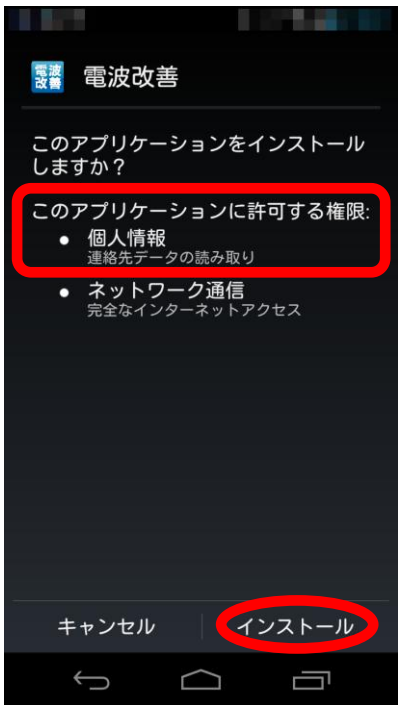

図 1-5：インストール開始有無画面

図 1-6：インストール完了画面

2.インストールが完了（図 1-6 参照）すると、スマートフォンのアプリ一覧画面にアイコンが表示されます（図 1-7 参照）。このアイコンをタッチするとアプリが起動します。

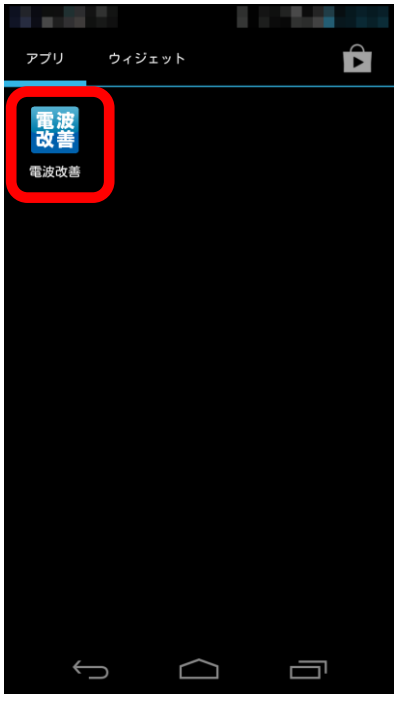

図 1-7：インストールされたアプリのアイコン

3.アプリを起動すると、初期設定を行う画面が表示されます（図 1-8 参照）が、すぐに「この端末では未対応のためご利用できません」というメッセージが表示され（図 1-9 参照）、アプリが終了してしまいます。**このアプリは、実際は「初期設定」のような処理は行わず、必ず「未対応」の画面を表示してアプリが終了するようになっています。さらに、図 1-8 の画面が表示されている間に、電話帳の内容を窃取し、外部のサーバーへ送信します。**

図 1-8：初期設定を装った画面

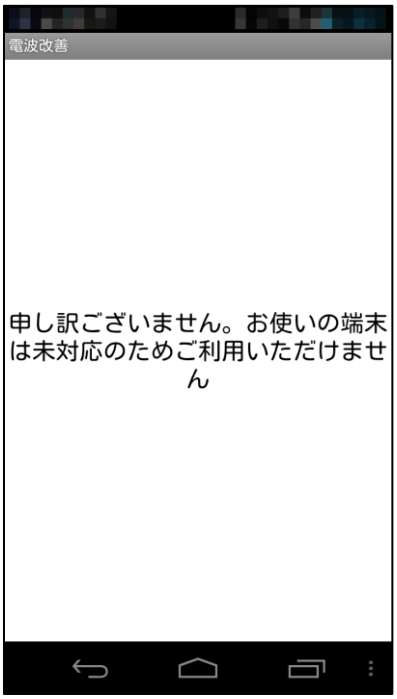

図 1-9：未対応を装った画面

図 1-10 が、不正なアプリが電話帳の内容を外部のサーバーへ送信する際の通信です。図 1-10 の②を見ると、：（コロン）を区切りにして、［名前：電話番号：メールアドレス］の順となっており、数字と／（スラッシュ）の間で一人分の情報となっていることが分かります。

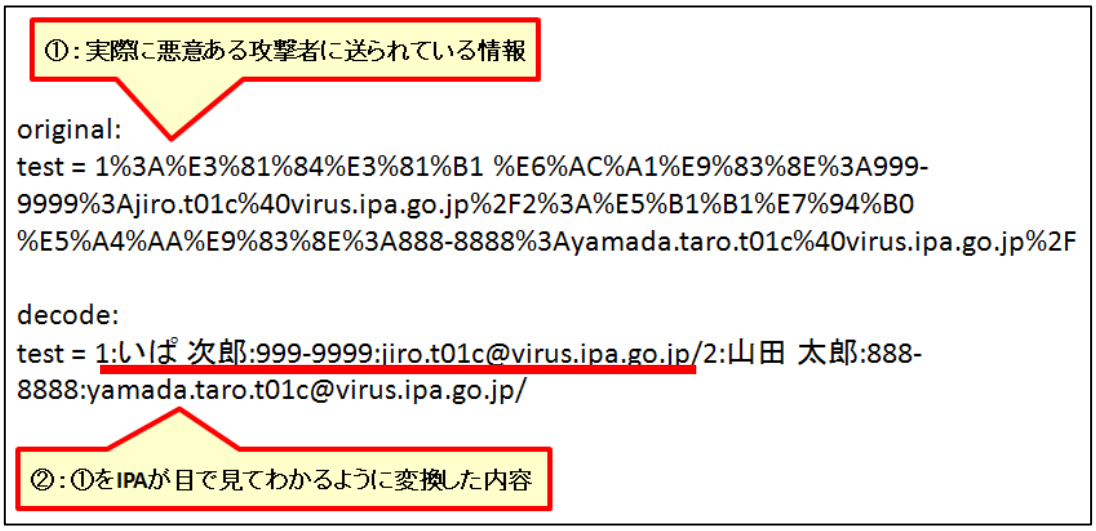

図 1-10：不正なアプリが電話帳の内容を外部のサーバーへ送信する際の通信

このように、**このアプリは実際には電波を改善する機能は持っておらず、単純に電話帳の内容を窃取するための不正なアプリだと言えます。**2012 年 9 月現在、この不正なアプリは Ackposts の名称で、ほとんどのウイルス対策ソフトにより検知されます。

（3）不正なアプリの被害に遭わないための対策

今回解析した不正なアプリは、**Android OS 用アプリの公式マーケットサイトではない、不正なサイトに置かれていました。**このようなウイルスに感染しないためには、以下に示す対策が有効です。

●**信頼できる場所からアプリをインストールする。**

スマートフォンで使用するアプリは、**Android 端末であればアプリの審査や不正アプリの排除を実施している Android OS 用アプリの公式マーケット「Google play」、iPhone であれば米 Apple 社の「App Store」、あるいは通信事業者等が公式に運営するマーケットなど、信頼できる場所からインストール**しましょう。

●**Android 端末では、アプリをインストールする前に、アクセス許可を確認する。**

Android 端末の場合、**アプリをインストールする際に表示される「アクセス許可」（アプリが Android 端末のどの情報／機能にアクセスするか定義したもの）の一覧には必ず目を通しましょう（図 1-11 参照）。**過去発見された Android 端末を狙ったウイルスには、個人情報などを不正に盗み取るため、アプリの種類から考えると不自然なアクセス許可をユーザーに求めるものがありました。**今回解析した不正なアプリも、名前はスマートフォンの電波の改善を連想させるものですが、電話帳の内容へアクセスするための「連絡先データを読み取り」の許可を求めていました。**

Android 端末にアプリをインストールする際に、不自然なアクセス許可や疑問に思うアクセス許可を求められた場合には、そのアプリのインストールを中止しましょう。

図 1-11：「アクセス許可」の表示画面の例

●**セキュリティソフトを導入する。**

スマートフォンにセキュリティアプリを入れて最新の状態に保っておくことで、このようなウイルスの感染を事前に食い止めてくれる場合があります。**ウイルス感染の可能性をより低減するためにセキュリティソフトを導入してください。**

（ご参考）

「スマートフォンを安全に使おう！」（IPA）

http://www.ipa.go.jp/security/keihatsu/pr2012/general/03_smartphone.html

なお、万が一このような不正なアプリをインストールして起動させてしまった場合は、すみやかにアプリをアンインストールして、ダウンロードした.apk ファイルを削除して下さい。

しかし、**一度でもアプリを起動させると、ウイルス感染の被害に遭い情報が窃取されてしまいます。そしてそれらの情報は戻ってくることはありません。**くれぐれもアプリを安易にインストールしないよう心掛けましょう。

（4）こんなときは…

図 1-1、図 1-2 のようなリンク先が書かれている怪しいメールや DM（ダイレクトメール）が届いた、怪しいリンク先が書かれている SNS やブログなどの投稿文を見つけた、などがありましたら、IPA 安心相談窓口までご連絡をいただければと思います。

まずは、ご相談ください。

	安心相談窓口の問合せ先
電話	03-5978-7509 （オペレータ対応は、平日の 10:00～12:00 および 13:30～17:00）
E-mail	anshin@ipa.go.jp ※このメールアドレスに特定電子メールを送信しないでください。
FAX	03-5978-7518
郵送	〒113-6591 東京都文京区本駒込 2-28-8 文京グリーンコート　センターオフィス 16 階 IPA セキュリティセンター「情報セキュリティ安心相談窓口」宛

今月のトピックス

○ コンピュータ不正アクセス被害の主な事例（届出状況および被害事例の詳細は、10 頁の「3.コンピュータ不正アクセス届出状況」を参照）
- 遠隔操作ツールを埋め込まれ、結果としてフィッシングに悪用するページを設置された
- 特定の IP アドレスから大量のアクセスを受けた

○ 相談の主な事例　（相談受付状況および相談事例の詳細は、12 頁の「4.相談受付状況」を参照）
- Booking.com から、心当たりのないメールが届いた
- USB メモリの中にウイルスが入っていないか確認したい

2. コンピュータウイルス届出状況　－詳細は別紙 1 を参照－

（1）ウイルス届出状況

8 月のウイルスの検出数※1 は、**24,189 個**と、7 月の 25,487 個から 5.1%の減少となりました。また、8 月の届出件数※2 は、**961 件**となり、7 月の 877 件から 9.6%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。

検出数の 1 位は、**W32/Mydoom** で **15,441 個**、2 位は **W32/Netsky** で **5,888 個**、3 位は **W32/Mytob** で **966 個**でした。

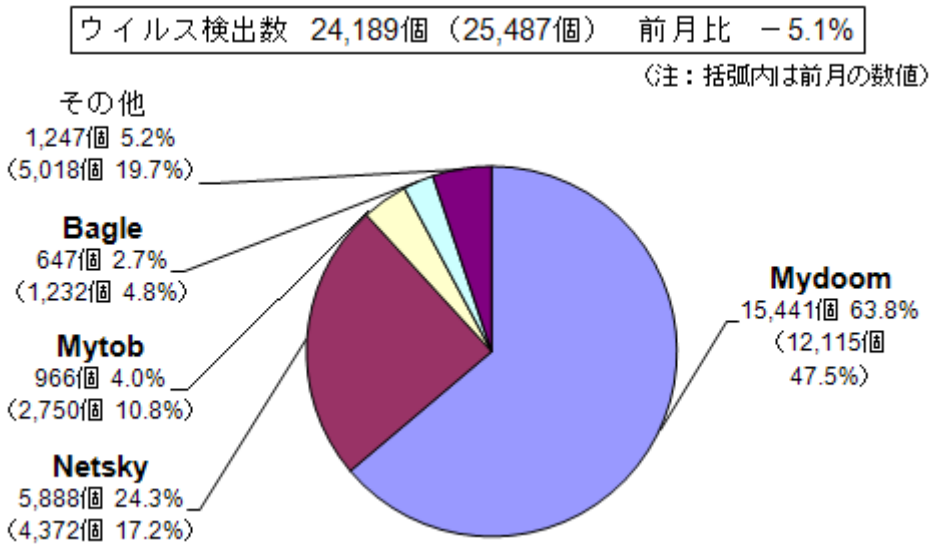

図 2-1：ウイルス検出数

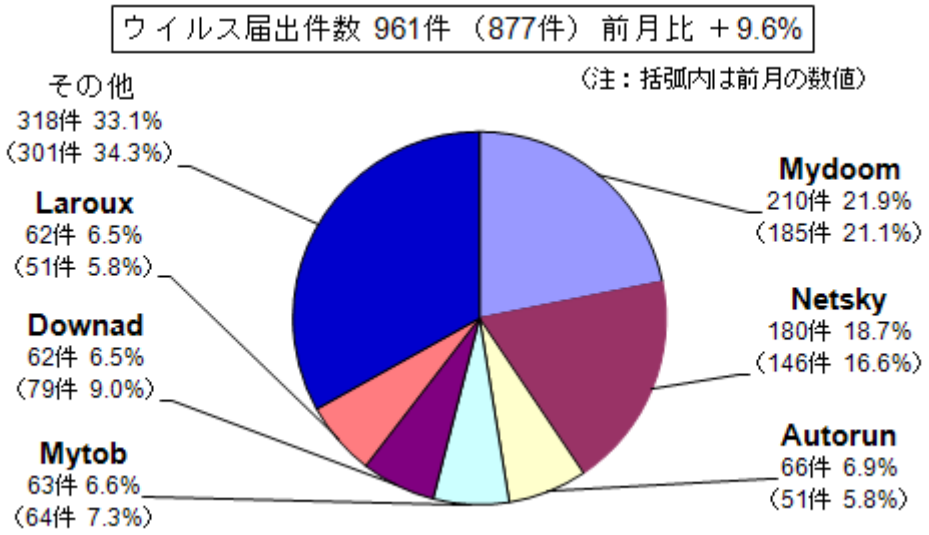

図 2-2：ウイルス届出件数

（2）不正プログラムの検知状況

8 月の不正プログラムの検出数※1 は、**21,437 個**と、7 月の 100,367 個から 78.6%の減少となりました。

検出数の 1 位は、偽セキュリティソフトの検知名である **Fakeav** で **2,504 個**、2 位は、パソコン内に裏口を仕掛ける **Backdoor** で **1,850 個**、3 位は、宅配会社の伝票情報を装って感染を試みる **Invo** で **1,710 個**、でした。

以下、正規のソフトウェアなどを装って感染を試みる Trojan/Horse、広告を表示させるプログラムの総称である Adware、偽の警告画面から偽セキュリティソフトのサイトに誘導する Katusha、の順でした。

※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）

∴ここでいう「不正プログラムの検知状況」とは、IPA に届出られたものの中から「コンピュータウイルス対策基準」におけるウイルスの定義に当てはまらない不正なプログラムについて集計したものです。

∴コンピュータウイルス対策基準：平成 12 年 12 月 28 日（通商産業省告示 第 952 号）（最終改定）（平成 13 年 1 月 6 日より、通商産業省は経済産業省に移行しました。）

「コンピュータウイルス対策基準」（経済産業省）
http://www.meti.go.jp/policy/netsecurity/CvirusCMG.htm

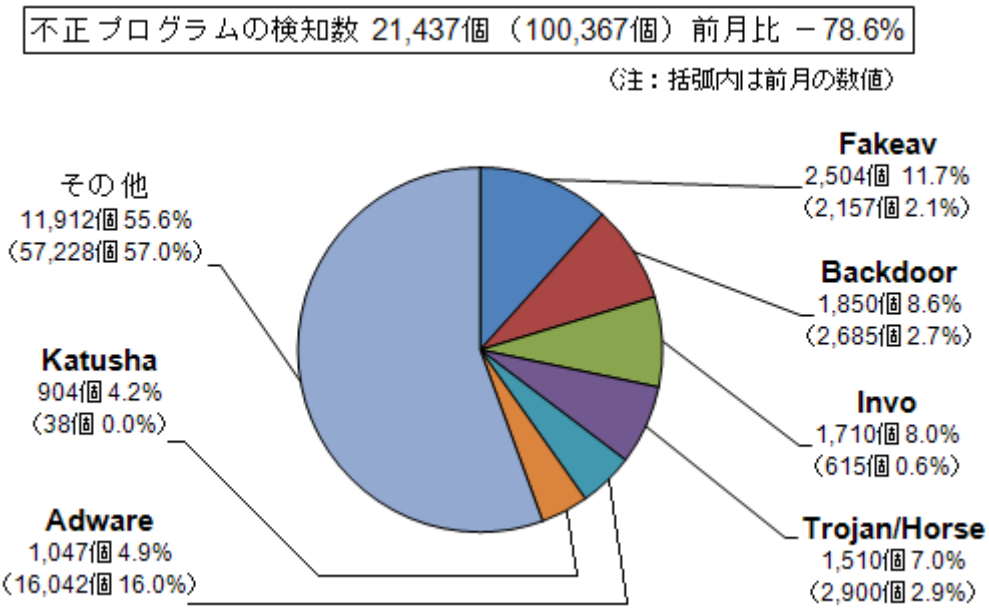

図 2-3：不正プログラムの検知数

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－

表 3-1　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		5	9	10	2	19	9
	被害あり(b)	4	7	6	2	18	9
	被害なし(c)	1	2	4	0	1	0
相談(d) 計		54	46	50	38	54	44
	被害あり(e)	10	9	17	12	26	13
	被害なし(f)	44	37	33	26	28	31
合計(a+d)		59	55	60	40	73	53
	被害あり(b+e)	14	16	23	14	44	22
	被害なし(c+f)	45	39	37	26	29	31

（1）不正アクセス届出状況

８月の届出件数は９件であり、それら**全てが被害のあったもの**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44件であり､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６件、なりすまし２件、DoS 攻撃１件**でした。

「侵入」の被害は、ウェブページが改ざんされていたものが４件（内、フィッシングに悪用するためのコンテンツ設置１件）、SQL インジェクション攻撃を受けてデータを参照されたものが１件、SSH リモートログインに成功していたものが１件、でした。侵入の原因は、脆弱なパスワード設定が１件、ファイルへのアクセス権限の不備が１件でした（他は原因不明）。

「なりすまし」の被害は､メールアカウント悪用されてスパムメールを送信されたものが２件でした。

（4）被害事例

［侵入］

（i）遠隔操作ツールを埋め込まれ、結果としてフィッシングに悪用するページを設置された

事例	・組織外から「そちらのウェブサイトに、フィッシングに悪用するためのページがある」との連絡が入った。すぐに確認すると、クレジットカード会社を模倣したページの中に、カード番号などの入力欄が設置されていた。さらにその情報を外部にメールで送信する機能が施されていた。 ・調査したところ、WordPress のプラグインを、遠隔操作プログラムに置き換えられていた。 ・当該サイトはテスト運用中で、URL を外部に公表していなかったが、社外からのアクセスが可能な状態だった。さらに暫定的にコンテンツ部分の全領域を書き込み可能な設定にしていた。
解説・対策	開発中で URL を公開していなくても、インターネットからアクセス可能な場合は、悪意ある者に狙われて悪用されるかもしれない、と念頭に置く必要があります。 特に今回のように**ウェブサイトとして公開していなくても、一旦侵入を許すと、悪意あるウェブサイトとして利用されてしまいます**。 フィッシングサイトへの改ざんは外部からの指摘により初めて気が付くことも多く、発見の遅れが被害の拡大につながる恐れがあります。 システム管理者は以下の対策を実施するよう心がけてください。 ・適切なパスワード設定と管理を行う ・脆弱性を解消する（OS だけではなく、ウェブアプリケーションなども忘れずに） ・外部からのアクセス制限やセキュリティ設定を適切に行う （不要なサービスは停止する、書き込み権限・閲覧権限を適切に設定する） ・こまめなログの確認 ・ファイル改ざん検知システムや WAF などの、防御システムの導入

［DoS］

（ii）特定の IP アドレスから大量のアクセスを受けた

事例	・特定の IP アドレスから、基幹サーバーに大量のアクセスを受け、その影響で学内から学外への通信に遅延が発生し、業務に支障が生じた。 ・アクセスの内容は、そのほとんどが UDP だったが、中には SSH によるログインを試行するアクセスもあった。 ・対策として、ファイアウォールの上流のネットワーク機器において、送信元 IP アドレスに対するフィルタリングを実施した。
解説・対策	第三者のパソコンを踏み台にして攻撃している可能性も考えられますので、**特定の IP アドレスからのアクセスであれば、該当 IP アドレスを管理しているプロバイダに相談することをお勧めします**。また大量のアクセスが受けつつもシステムの停止は許されないといった場合には、上位のプロバイダでの対処が有効になる場合があります。 （ご参考） IPA - 「サービス妨害攻撃の対策等調査」報告書について http://www.ipa.go.jp/security/fy22/reports/isec-dos/ JPCERT/CC - 技術メモ - サービス運用妨害攻撃に対する防衛 http://www.jpcert.or.jp/ed/2001/ed010005.txt また、SSH ログインのアクセス試行への対策として、学生と職員に複雑なパスワードを強制させるとともに、SSH 用プログラムを常に最新バージョンで動作させるようにしてください。

4. 相談受付状況

8 月のウイルス・不正アクセス関連相談総件数は **980 件**でした。そのうち**『ワンクリック請求』に関する相談**が **255 件**（7 月：216 件）、**『偽セキュリティソフト』**に関する相談が **41 件**（7 月：23 件）、**Winny に関連する相談**が **9 件**（7 月：4 件）、**「情報詐取を目的として特定の組織に送られる不審なメール」に関する相談**が **3 件**（7 月：3 件）、などでした。

表 4-1　IPA で受け付けた全てのウイルス・不正アクセス関連相談件数の推移

		3 月	4 月	5 月	6 月	7 月	8 月
合計		**772**	**750**	**934**	**1,097**	**921**	**980**
	自動応答システム	427	428	490	578	530	515
	電話	287	270	363	439	342	417
	電子メール	49	50	78	79	46	48
	その他	9	2	3	1	3	0

※ IPA では、「情報セキュリティ安心相談窓口」を開設し、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：anshin@ipa.go.jp
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。

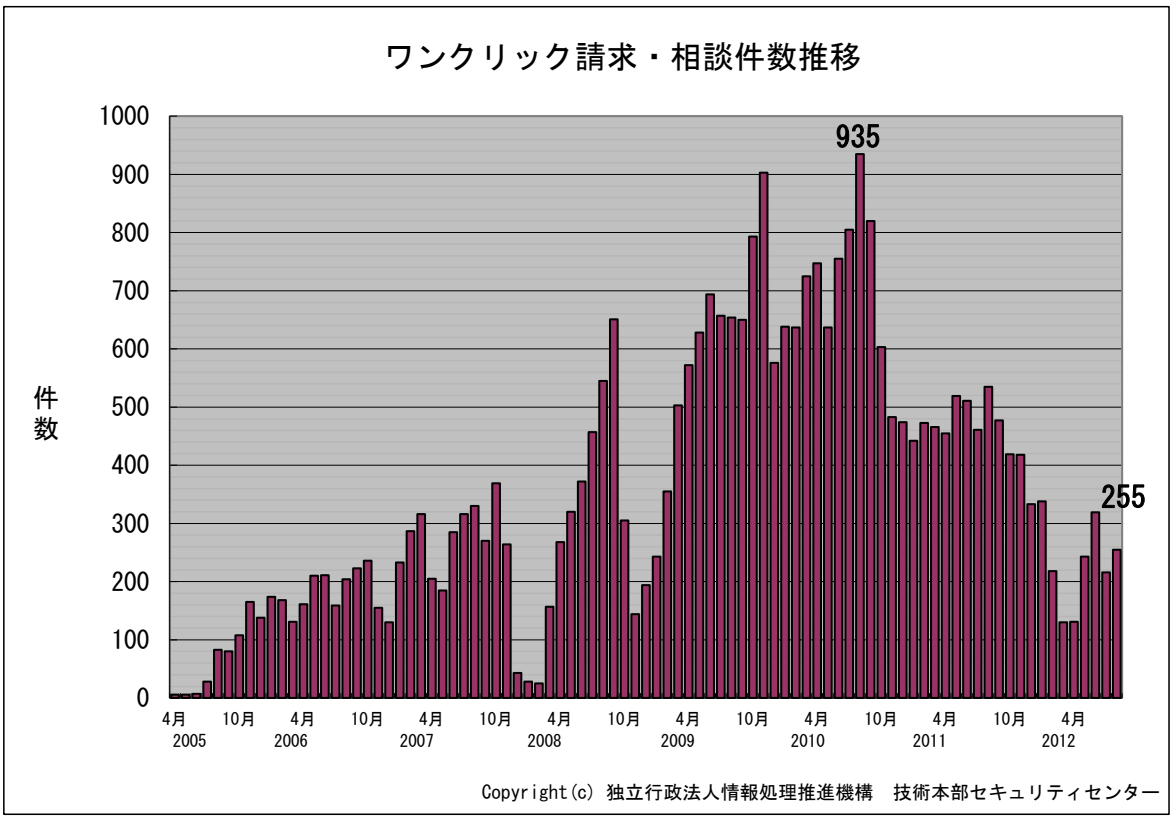

図 4-1：ワンクリック請求相談件数の推移

主な相談事例は以下の通りです。

（ｉ）Booking.com から、心当たりのないメールが届いた

相談	先日、ホテル予約サイトの Booking.com を名乗る、心当たりのない予約確認メールが届きました。そのメールには exe ファイルを zip 圧縮したファイルが添付されていました。セキュリティ対策ソフトがトロイの木馬を検知したため、そのソフトの指示に従いウイルスの駆除を行いましたが、ウイルスに感染していないでしょうか。
回答	セキュリティ対策ソフトの指示に従い、不審な添付ファイルを開かずに駆除したとのことで、ウイルスに感染していないと考えられます。**不安な場合は**、ご利用のセキュリティ対策ソフトを**最新の状態にして全体をスキャン**して下さい。また他社製品のオンラインスキャンを併用するなど**多角的にスキャン**をしてください。 最近、利用してもいない運送会社の配送状況を伝える英文のメールが届いた等、当機構に同様の相談がよせられています。**心当たりのないメールや不審なメールが届いた場合**は、**ウイルス感染などの危険を避けるために、すぐに削除してください。**削除しないで残しておくと、**本文中に危険なリンクや危険な添付ファイルを誤って開いてしまう危険性**が残ります。 メールにおいて不審かどうかの判断に迷われることがありましたら、メールヘッダを見ることで判断をすることが出来る場合があります。それでも判断に迷われるようでしたらメール全文を eml 形式や msg 形式などで保存し、パスワードつき圧縮ファイルにして（相談・届出内容のメールに添付し）当機構までご送付ください。 （ご参考） 「 コンピュータウイルスや不正アクセスの届出にご協力ください！ 」 ～　セキュリティに関する相談も受け付けています　～（IPA） http://www.ipa.go.jp/security/txt/2012/08outline.html

（ii）USB メモリの中にウイルスが入っていないか確認したい

相談	Windows パソコンから USB メモリの中にデータを保管したのですが、ウイルスが含まれていないか心配です。確認する方法を教えてください。
回答	お使いのパソコンが Windows の場合は「**USB メモリ感染型ウイルス**」が感染しないように、**自動実行機能を無効化**してください。次に OS のアップデートやご利用されているアプリケーションを最新の状態にして、**インターネットなど外部のネットワークから隔離した環境**で、USB メモリ内を**チェック**してください。この時点でウイルスを検知していない場合は、インターネットや外部のネットワークに接続しなおして、他社製品のオンラインスキャンを併用するなど**多角的にスキャン**してください。 （ご参考） Windows での「自動実行」機能の無効化手順（IPA） http://www.ipa.go.jp/security/virus/autorun/

『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。』

一般社団法人 JPCERT コーディネーションセンター：http://www.jpcert.or.jp/
@police：http://www.cyberpolice.go.jp/
フィッシング対策協議会：http://www.antiphishing.jp/
株式会社シマンテック：http://www.symantec.com/ja/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/japan/
株式会社カスペルスキー：http://www.viruslistjp.com/analysis/

■お問い合わせ先
IPA 技術本部セキュリティセンター 加賀谷／青木
Tel:03-5978-7591　Fax:03-5978-7518
E-mail: isec-info@ipa.go.jp