プレスリリース
第 11-05-207 号
2011 年 2 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 [2011 年 1 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、2011 年 1 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

「 スマートフォンのウイルスに注意！ 」

利用者が自由にアプリケーションをインストールし、様々な用途に利用できる、「スマートフォン」と呼ばれる携帯端末の普及が進んでいます。スマートフォンは、見た目は携帯電話に似ていますが、その中身（機能）はパソコンに近いものです。そのため、スマートフォンの利用者は、パソコンの利用者と同様に、コンピュータウイルスによる被害に遭う可能性があります。

2011 年 1 月 21 日、IPA はスマートフォンのウイルスに関する注意喚起※1 を公開しました。これは、Android（アンドロイド）という OS※2 を採用している、一部のスマートフォンやタブレット型端末に感染する可能性のある危険性の高いウイルスが発見され、国内の利用者でもその被害に遭う可能性が高まったためです。

今月の呼びかけでは、一般利用者向けに、まずスマートフォンにまつわるウイルスの脅威について説明します。その後、最近発見された、Android に感染するウイルスの特徴とともに、その感染予防策について、具体的に説明します。

※1 「Android OS を標的としたウイルスに関する注意喚起」（IPA）
http://www.ipa.go.jp/security/topics/alert20110121.html

※2 OS：Operating System の略で、「基本ソフトウェア」とも呼ぶ。スマートフォンを含む、コンピュータなどの機器（ハードウェア）の基本的な制御をつかさどり、様々なアプリケーションソフトウェアを動作させる基盤部分。

（1）スマートフォンを標的としたウイルスの脅威

これまで、国内における従来型の携帯電話については、ウイルス感染等の被害はほとんど確認されていませんでした。一方、スマートフォンにまつわるウイルスの脅威は、現在、パソコンに似た状況にあります（図 1-1）。この状況について簡単に説明します。

図 1-1：様々な電子機器へのウイルスの脅威

まず、従来型の国内の携帯電話は、機種ごとに様々に異なる仕様となっているほか、利用者の自由度をある程度制限することで、セキュリティを強固にしています。このため、悪意のある者によるウイルスの作成が難しく、またウイルスに感染しにくいという特徴があります。例えば 2004 年頃から海外の一部の携帯電話においてウイルス感染の事例が複数ありましたが、それらウイルスの国内の携帯電話への感染事例はごく少数となっています。

スマートフォンの機能や仕組みはパソコンとの共通点が多く、特に次の点については、パソコンと同様、悪意のある者によってウイルス感染の標的にされる要因となっています。

- 海外製を含む多くの機器で共通の仕様となっている
  - パソコンは様々な機種が販売されていますが、Windows や Mac OS など、機器の制御をつかさどる OS は共通のものが搭載されています。ウイルスは、より多くの機器に感染させるため、広く普及した OS 上で動作するよう作られる傾向があります。
    スマートフォンにも、Windows Phone（旧 Windows Mobile）、iOS（旧 iPhone OS）、Android、Symbian OS といった OS が搭載されています。最近のスマートフォンは、同じ OS を搭載している機種が多く、これらを標的としたウイルスが作られやすくなると思われます。また、例えば海外で作られたウイルスが、そのまま国内のスマートフォンでも動作する可能性も高いといえます。

- 端末の自由度を高めていることと引き換えに、セキュリティ面に影響がある
  - スマートフォンの一般的な特徴として、利用者が自由にアプリケーションを追加できる点や、アプリケーションを開発するための情報が公開されているといった点が挙げられます。パソコンと比較すると、スマートフォンでは、ウイルスのような悪意のあるソフトウェアの動作を限定したり、そもそも入り込みにくくしたりするような工夫がなされています。しかし、自由度が高い分、セキュリティ面への影響も従来型の携帯電話と比較して高くなっています。

高機能なスマートフォンの利用者が増え、その中に重要なデータが保存されるようになると、悪意のある者にとっては、情報を盗み出したり、機器の制御を奪って（乗っ取って）悪用したりするようなウイルスを作成する動機となります。

このように、スマートフォンは従来型の国内の携帯電話とは性質が異なり、パソコンと同様、ウイルスによる脅威にさらされています。そして、この脅威は、今後も増していくものと考えられます。

（2）Android を標的としたウイルスへの被害予防策

冒頭で述べた通り、IPA は「Android OS を標的としたウイルスに関する注意喚起」を公開しました。この時発見されたウイルスは、既存の正規のアプリケーションにウイルスが混入させられた状態で流通しており、そのアプリケーションをインストールしてしまうと、最悪の場合、スマートフォンを乗っ取られてしまう可能性があるという危険なものでした（詳細は冒頭「※1」の注意喚起文書を参照）。なお、今回発見されたものを含め、現状発見されているウイルスは、スマートフォンの端末同士での感染や、利用者の操作なしでの侵入をするものではありません。

ここでは、この種のウイルスの被害予防策について、一般の利用者向けに詳しく説明します。

（i）信頼できる場所から、正規版のアプリケーションを入手しましょう

Android には、Google 社が運営している「Android Market」というアプリケーション配布の仕組みがあります。また、第三者が独自に運営しているものとして、使用中の携帯電話の契約先（以下、携帯電話キャリア）や、ゲーム会社などによるマーケットが存在しています。

その一方で、正規のアプリケーションの改造版・海賊版などを不正に配布しているウェブサイト等もあり、そういった場所において、アプリケーションにウイルスが混入された状態で配布されて

いることを確認しています。アプリケーションの入手元の信頼性と、それが正規版であるか否かは、ウイルス感染を防ぐ上で重要なポイントになります（図 1-2）。

- 信頼できる場所、正規のアプリケーション
  - Google 社による Android Market では、個々のアプリケーションについて、マーケットへの登録時の事前審査はありません。ただし、悪意のあるアプリケーションなど、Android Market のポリシーに違反するものは削除される仕組みがあるため、一定の信頼があると考えられます。
  - 携帯電話キャリアなどの第三者が運営しているマーケットについては、そのポリシーは様々です。ある程度の期間を要してアプリケーションの審査をしているマーケットもありますので、各マーケットの運営会社の信頼性やポリシーを確認した上で利用するとよいでしょう。
  - 改造版や海賊版を配布しているようなウェブサイトについては、アプリケーションにウイルスが混入している可能性があるため、利用すべきではありません。改造版や海賊版は、見た目だけでは安全か危険かを判断するのは難しく、信頼性の判断に困る場合は、基本的に利用を控えるべきです。

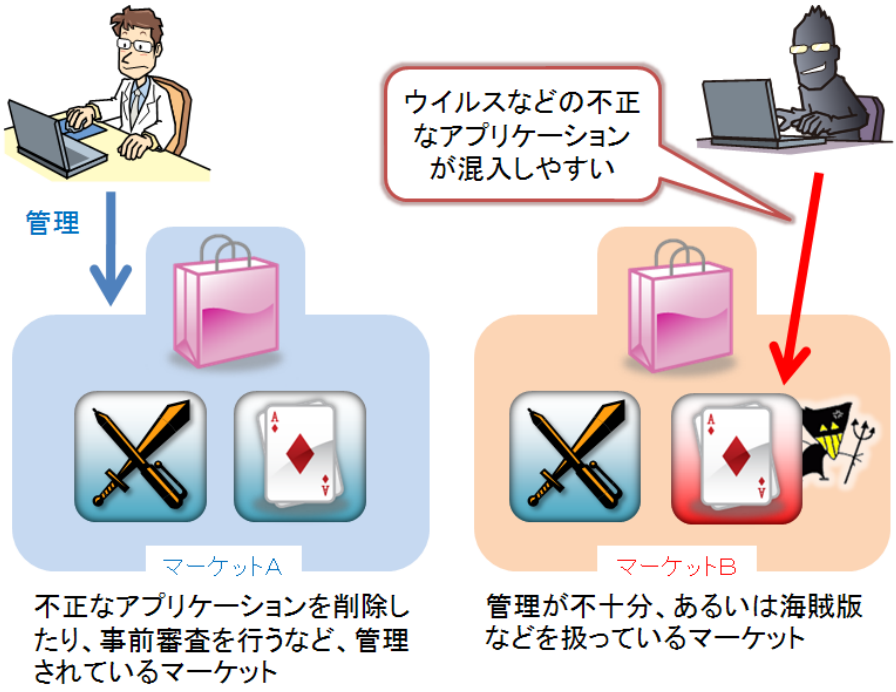

図 1-2：様々なマーケット

その他、アプリケーションを安全に入手するためのポイントは次のとおりです。

- アプリケーションの評価、コメント、ダウンロード回数
  - Android Market を含む各種マーケットやアプリケーション紹介サイトでは、アプリケーションに対する他の利用者からの評価、コメント、ダウンロード回数が併せて表示されることがあります。これらの情報は、あくまで参考にとどまりますが、安全かどうかを判断する手がかりとなります。

- メールの添付ファイルにも注意
  - 一部の Android の機種では、パソコン同様、メールの添付ファイルとして送られてきたアプリケーションを簡単な操作でインストールできます。知人からのメールのように見えても、送信元を偽りウイルスを送信してくる可能性もあるため、アプリケーションが添付されたメールには注意してください。

（ii）普段は「提供元不明のアプリ」設定のチェックを外しておきましょう

Android の設定画面に「提供元不明のアプリ」という項目があります。この項目のチェックを外しておくと、Android Market 以外で入手したアプリケーションのインストールが阻止されます（初期状態ではチェックは外れた状態になっています）。「提供元不明のアプリ」の設定の確認・変更手順は、図 1-3 を参照してください。

操作を誤るなどして不正なアプリケーションをインストールしてしまわないよう、普段はこの項目のチェックを外した状態にしておくことを勧めます。

なお、信頼できる第三者のマーケットであっても、Android Market 以外で入手したアプリケーションをインストールする際は、一時的にこの設定を変更する（チェックを入れる）必要があります。その場合、インストール終了後、再度チェックを外してください。

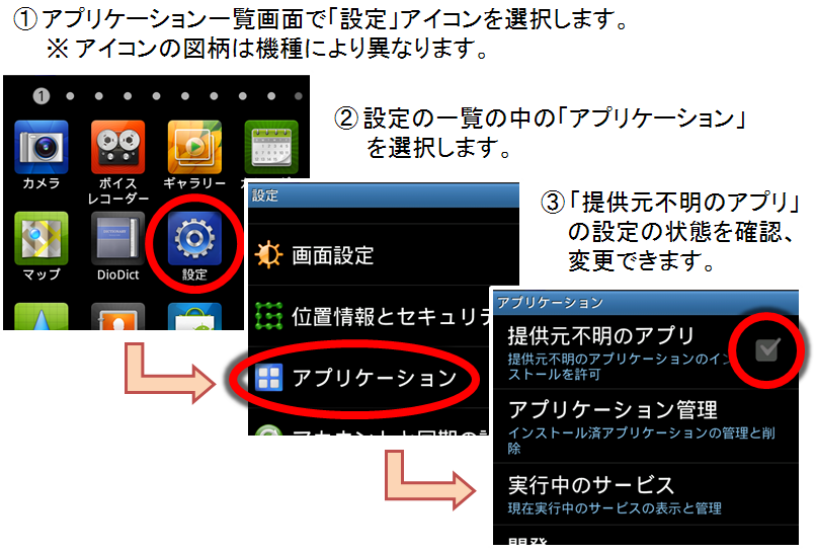

図 1-3：「提供元不明のアプリ」設定の確認、変更方法

（iii）アプリケーションのインストール時の「アクセス許可」に注意しましょう

Android のアプリケーションにおけるセキュリティの考え方は次の通りです。

- Android のアプリケーションは、そのアプリケーションがスマートフォンの中のどの情報／機能へアクセスするかを、「アクセス許可」を求めるという形で宣言します。
- アプリケーションの利用者は、自身の責任によって、インストールの時に表示される「アクセス許可」を確認し、問題がないと判断した場合は許可を与えます。
- アプリケーションは、許可が与えられてインストールされた後は、利用者への通知なしに「アクセス許可」の範囲の情報／機能に自由にアクセスできます。

これまでにあった Android のウイルスには、ゲームなどの無害なアプリケーションに見せかけて、「アクセス許可」として「あなたの個人情報」や「料金が発生するサービス」などへのアクセスを求め、これらをよく確認せずにインストールすると、被害に遭う可能性があるというものがありました。

この「アクセス許可」を求める画面の例は、図 1-4 を参照してください。

図 1-4：「アクセス許可」の表示画面の例

アプリケーションの入手元に関わらず、インストール時に表示される「アクセス許可」の一覧には必ず目を通してください。そのアプリケーションの機能と照らし合わせて、要求される「アクセス許可」が不自然な場合や、疑問に思う点があれば、インストールを中止することを勧めます。

なお、アプリケーションの中には、広告の表示などのために、本来のアプリケーションの機能とは関係がなさそうな「アクセス許可」を求めるものがあります。「アクセス許可」について代表的なものや、意味が分かりにくいものを、表 1-1 に示します。

表 1-1：「アクセス許可」の説明（一部）

項番	「アクセス許可」の表示	説明
1	電話発信 電話の状態を読み取る	電話の着信状況に応じて再生中の音楽を停止するといった用途に使われていると考えられます。 この許可が与えられたアプリケーションは、スマートフォンの電話番号、機器ごとに付けられている端末識別番号といった情報を読み取ることもできます。
2	あなたの場所 粗い（ネットワークベース）場所	「粗い場所」というのは、携帯電話の基地局や、周囲にある無線 LAN の設備から推測できる位置情報を意味しており、およそ数十 m から数 km 程度の誤差の範囲でスマートフォンの位置情報を得られます。 この位置情報は、アプリケーションの画面に表示する広告の内容を決めるために使われることがあります。
3	ネットワーク通信 完全インターネットアクセス	文字通り、インターネットへのアクセスにより情報を送受信するという機能です。広告に関するデータのやりとりにも使われます。

※ 「アクセス許可」の表示内容（表現）は機種により若干異なる場合があります。

スマートフォンのアプリケーションは、インターネットとの通信ができてはじめて役に立つものが多いのですが、例えば上記の項番 1 や 2、あるいは「あなたの個人情報」といった項目と合わせて項番 3 の許可を求められた場合は、インターネットを通じて、電話番号やスマートフォンの位置の情報が何処かへ送信されてしまう可能性があるということになります。

「アクセス許可」の一覧だけでは、それが正当な目的のみに使用されるのか、不正なアプリケーションなのかを判断するのが難しい場合があります。アプリケーションの入手元や開発元の信頼性、他の利用者の評判などを参考にしつつ、万が一を考慮し、悪用されても困らない範囲の「アクセス許可」を与えるようにしてください。

（iv）セキュリティソフトを導入しましょう

近年、スマートフォンのセキュリティが注目されており、Android 向けの様々なセキュリティソフトが公開中、もしくは公開予定となっています。ウイルス対策の機能を含む、これらのセキュリティソフトの導入を検討してください。

参考として、パソコン用のセキュリティソフトを日本で販売している主なベンダーについて、Android 向けのセキュリティソフトの対応状況をまとめました。現時点では海外版のみとなっていても、近い時期に国内向けに販売される予定のものもあります。

（ご参考：五十音順）

- 株式会社アンラボ「V3 Mobile」
  http://global.ahnlab.com/en/site/product/productSubDetail.do?prod_seq=1023 （英語）
  ※ 現在、海外版のみ
- 株式会社カスペルスキーラブスジャパン「Kaspersky Mobile Security」
  http://www.kaspersky.com/kaspersky_mobile_security （英語）
  ※ 現在、海外版のみ
- 株式会社シマンテック「ノートン モバイル セキュリティ」
  ※ 日本語版（現在ベータ版）、Android Market にて「ノートン」で検索して入手可能
- トレンドマイクロ株式会社「Trend Micro Mobile Security for Android」
  http://jp.trendmicro.com/jp/about/news/pr/article/20110112023725.html
  ※ 現在、海外版のみ
- マカフィー株式会社「McAfee VirusScan Mobile for Android」
  http://www.mcafee.com/japan/about/prelease/pr_10b.asp?pr=10/12/09-1
  ※ 日本語版、現在ソフトバンク社の機種に提供中

（3）まとめ

現在、広く普及した Windows を標的にして作成されるウイルスは、何年もかけて巧妙化・悪質化が進んできました。そこで発生した様々な手口は、そのままスマートフォンへ応用される可能性が高く、場合によっては急激に危険な状態となりえます。

スマートフォンの利用者は、パソコンと同様、まず利用している機種にどのような OS が搭載されているのかを認識してください。そして、必要なウイルスなどへの予防策を実施し、セキュリティ関連のニュース等にも注意を払いながら、安全に使用するよう心掛けてください。

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、8 頁の「3.コンピュータ不正アクセス届出状況」を参照）
- ・オンラインゲーム専用通貨の残高が全て無くなっていた
- ・突然、オンラインゲームにログインできなくなった

○ 相談の主な事例 （相談受付状況および相談事例の詳細は、10 頁の「4.相談受付状況」を参照）
- ・SystemTool というソフトウェアが勝手に立ち上がるようになった
- ・Winny 経由でウイルスに感染してしまった

○ インターネット定点観測（12 頁参照。詳細は、別紙 3 を参照）

IPA で行っているインターネット定点観測について、詳細な解説を行っています。

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 月のウイルスの検出数※1 は、**約 2.3 万個**と、12 月の約 2.3 万個から同水準での推移となりました。また、1 月の届出件数※2 は、**1,106 件**となり、12 月の 874 件から 26.5%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。
・1 月は、寄せられたウイルス検出数約 2.3 万個を集約した結果、1,106 件の届出件数となっています。

検出数の 1 位は、**W32/Netsky** で**約 1.6 万個**、2 位は **W32/Mydoom** で**約 3 千個**、3 位は **W32/Autorun** で**約 1 千個**でした。

ウイルス検出数 約2.3万個 （約2.3万個） 前月比 －0.5%

（注：括弧内は前月の数値）

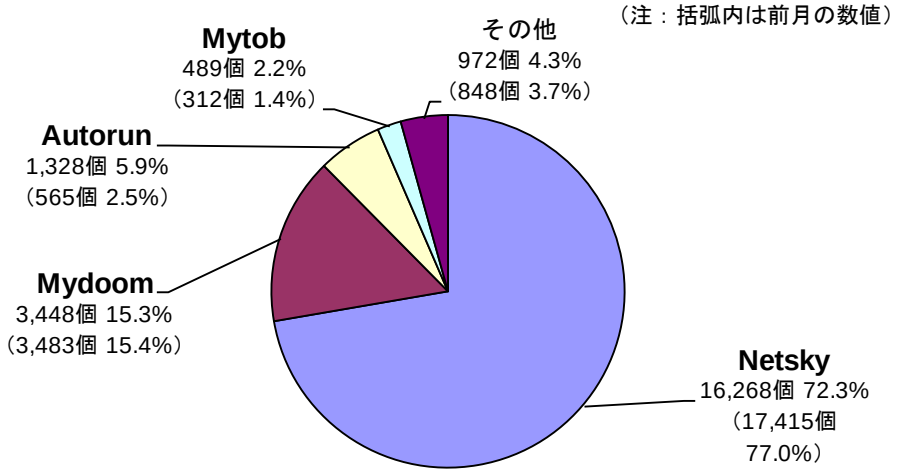

図 2-1：ウイルス検出数

ウイルス届出件数 1,106件 （874件） 前月比 ＋26.5%

（注：括弧内は前月の数値）

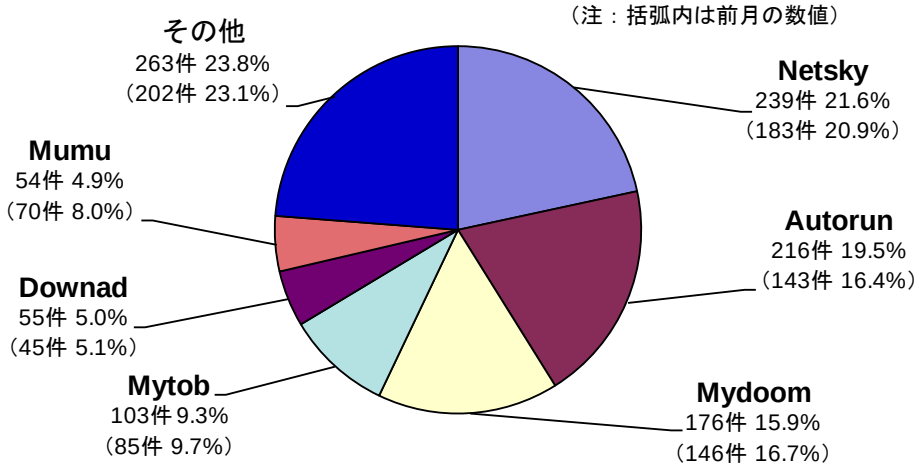

図 2-2：ウイルス届出件数

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

		8月	9月	10月	11月	12月	1月
届出[a] 計		18	15	14	14	22	12
	被害あり[b]	12	10	8	7	7	6
	被害なし[c]	6	5	6	7	15	6
相談[d] 計		56	47	40	45	27	41
	被害あり[e]	16	8	15	12	7	11
	被害なし[f]	40	39	25	33	20	30
合計[a+d]		74	62	54	59	49	53
	被害あり[b+e]	28	18	23	19	14	17
	被害なし[c+f]	46	44	31	40	35	36

（1）不正アクセス届出状況

1 月の届出件数は 12 件であり、そのうち何らかの被害のあったものは 6 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 41 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 11 件でした。

（3）被害状況

被害届出の内訳は、**なりすまし 6 件、**でした。

「なりすまし」の被害は、オンラインサービスのサイトに本人になりすまして何者かにログインされ、サービスを勝手に利用されていたもの（オンラインゲーム 5 件、無料 IP 電話 1 件）、でした。

（4）被害事例

［なりすまし］

（i）オンラインゲーム専用通貨の残高が全て無くなっていた

事例	・あらかじめ購入しておいた、オンラインゲーム専用通貨の残高が、全て無くなっていた。 ・ゲームサイトで通貨の使用履歴を確認したところ、身に覚えのない購入記録が残っていた。 ・パスワードは、忘れないようにするため、変更をしないで使っていた。 ・セキュリティ対策は、特に講じていなかった。
解説・対策	**ゲーム開始時にゲーム運営業者が設定したパスワードは、安易に推測される場合もあるため、そのまま使用し続けることはお勧めしません。また、パスワードは定期的な変更を心がけましょう。** オンラインゲームのアカウント情報を盗むウイルスも多く確認されています。セキュリティ対策の基本である、ウイルス対策ソフトの導入、OS や使用しているアプリケーションソフトの脆弱性の解消は必須です。 （参考） IPA-「あなたのオンラインゲームのキャラクターは狙われています！」 http://www.ipa.go.jp/security/txt/2009/10outline.html

（ii）突然、オンラインゲームにログインできなくなった

事例	・ある日突然、オンラインゲームへのログインができなくなった。 ・自分のキャラクターが所持していたアイテムが、売買取引されていた。 ・原因は不明だか、何者かに不正にアクセスをされ、パスワードを変更されたと考えられる。 ・こうしたなりすまし行為は、警察に被害届けを出すと受理してくれるのか？
解説・対策	自分では気がつかないうちに、他人にアカウント情報が知られてしまったと考えられます。アカウント情報は、他人に教えないのは当然ですが、**SNS（ソーシャルネットワーキングサービス）などのアカウント情報と同じものを使っていると、そうしたサービスの自己紹介などから推測される可能性もあります。**面倒でも、一つのサービスごとにアカウント情報の変更をお勧めします。 **被害届けの提出は、ゲーム運営業者側で行うことになりますので、まずはゲーム運営業者に問い合わせをしましょう。**場合によっては、警察に被害状況を申告するようにゲーム運営業者から指示されることもありますので、その際には最寄りの警察署に対処方法について相談してください。なお、ゲーム運営業者に問い合わせても、あまり良い対応を行ってもらえない場合、最寄りの消費生活センターに相談することをお勧めします。 （参考） IPA-「あなたのオンラインゲームのキャラクターは狙われています！」 http://www.ipa.go.jp/security/txt/2009/10outline.html 「全国の消費生活センター等」（国民生活センター） http://www.kokusen.go.jp/map/ 警察庁-インターネット安全・安心相談 http://www.npa.go.jp/cybersafety/

4. 相談受付状況

1 月のウイルス・不正アクセス関連相談総件数は **1,463 件**でした。そのうち**『ワンクリック請求』に関する相談**が **442 件**（12 月：474 件）、**『偽セキュリティソフト』**に関する相談が **17 件**（12 月：10 件）、**Winny に関連する相談**が **3 件**（12 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 **1 件**（12 月：0 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

		8月	9月	10月	11月	12月	1月
合計		2,432	2,102	1,813	1,692	1,536	1,463
	自動応答システム	1,298	1,142	1,065	1,036	954	892
	電話	1,053	872	675	580	531	499
	電子メール	75	85	69	72	49	64
	その他	6	3	4	4	2	8

※ 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。

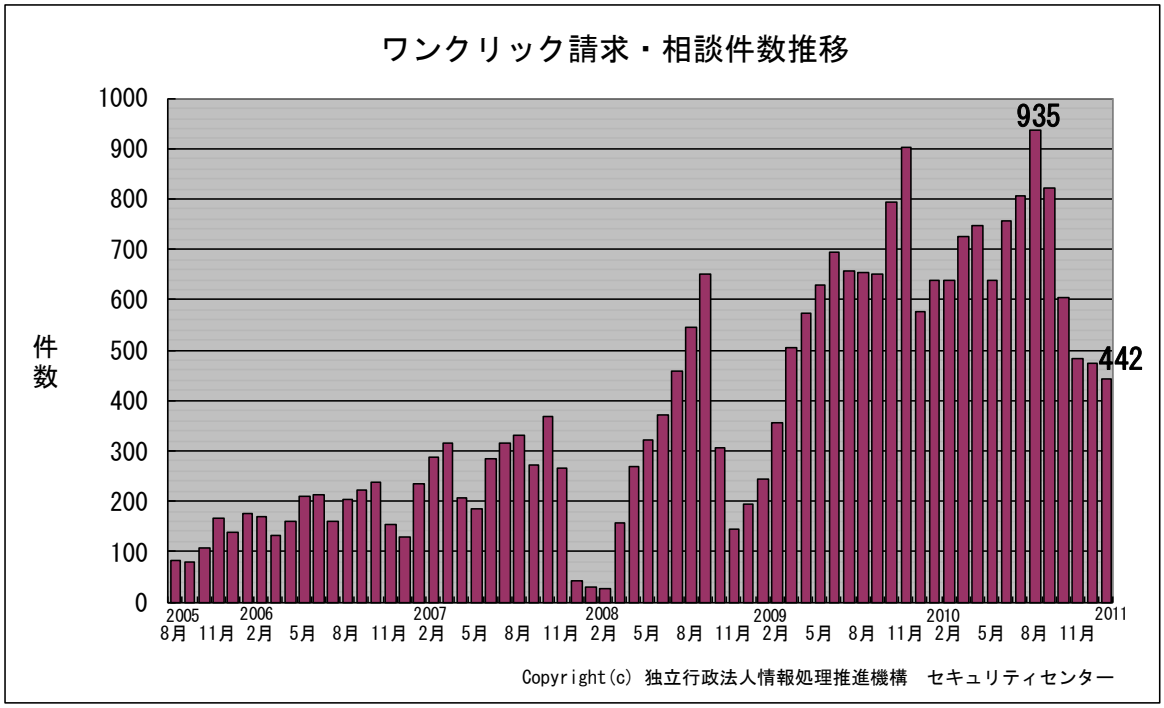

図 4-1：ワンクリック請求相談件数の推移

主な相談事例は以下の通りです。

（i）SystemTool というソフトウェアが勝手に立ち上がるようになった

相談	ネットサーフィンをしていたら、画面に突然 Warning という警告メッセージが出てきて、SystemTool という見覚えのないウイルス対策ソフトらしき画面が出てくるようになった。パソコンを再起動しても症状が消えない。どうしたらいいか。 （このほか、同様の事例が 13 件）
回答	相談者はいわゆる「偽セキュリティソフト」型ウイルスの感染被害に遭っています。**1 月に入り、SystemTool に関する相談が多数寄せられていることから、被害に遭っている方が多いと予想されます**。 症状としては、インターネットに接続できなくなったり、特定のアプリケーションが起動できなくなったり、勝手に壁紙が変えられたりとパソコンに様々な異常が発生するようです。 このようなウイルスに感染した場合の解決策としては、Windows の「システムの復元」機能を使って、パソコンがウイルスに感染した日よりも前の日の状態に戻すか、それができなければパソコンを初期化することをお勧めします。 （ご参考） IPA－2010 年 6 月の呼びかけ「深刻化する偽セキュリティ対策ソフトの被害！」 http://www.ipa.go.jp/security/txt/2010/06outline.html

（ii）Winny 経由でウイルスに感染してしまった

相談	Winny でダウンロードしたファイル（ISO イメージ※）を DVD にコピーし、その DVD をパソコンで開いたら怪しい画像の画面が大量に出てくるようになった。ダウンロードしたファイルが原因でウイルスに感染したと思う。 症状を解消するには初期化するしかないか。Winny の使用がよくないという自覚はありつつもあまり気にしてはいなかった。 ※ISO イメージ：CD や DVD 等の内容を正確に取りだしたファイル形式。ディスクイメージ。
回答	この状態から復旧させるには、パソコンを一度初期化することをお勧めします。 また、Winny などのファイル共有ソフトを使用していると、今回のように**ウイルス感染の被害に遭う**だけでなく、**場合によっては著作権侵害という犯罪を行っている可能性があります**。ファイル共有ソフトを使用することの危険性を認識し、Winny 等ファイル共有ソフトの使用は控えましょう。 （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

5. インターネット定点観測での 1 月のアクセス状況

インターネット定点観測（TALOT2）によると、2011 年 1 月の期待しない（一方的な）アクセスの総数は 10 観測点で **95,509 件**、延べ発信元数※は **42,791 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 138 の発信元から 308 件のアクセスがあった**ことになります（図 5-1 参照）。

延べ発信元数※：TALOT2 の各観測点にアクセスしてきた発信元を単純に足した数のことを、便宜上、延べ発信元数とする。ただし、同一発信元から同一の観測日・観測点・ポートに複数アクセスがあった場合は、発信元数を 1 としてカウントする。

TALOT2 における各観測点の環境は、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。

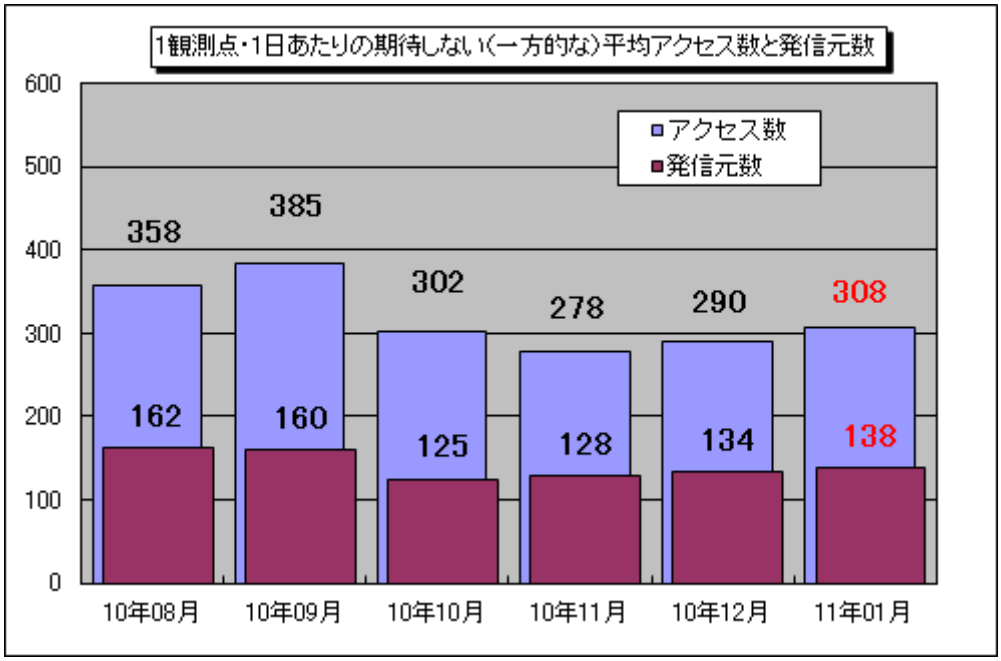

図 5-1：1 観測点・1 日あたりの期待しない（一方的な）平均アクセス数と発信元数

2010 年 8 月～2011 年 1 月までの各月の 1 観測点・1 日あたりの平均アクセス数とそれらのアクセスの平均発信元数を図 5-1 に示します。1 月の期待しない（一方的な）アクセスは、12 月と比べてほぼ横ばいでした。

12 月と 1 月の宛先（ポート種類）別アクセス数の比較を図 5-2 に示します。12 月に比べ、特に増加が観測されたのは 445/tcp へのアクセスでした。

445/tcp の増加について、12 月との発信元地域別アクセス数の変化を比較したところ、主に日本、アメリカと上位 10 ヵ国以外からのアクセスが増えたことによるものでした（図 5-3 参照） 。

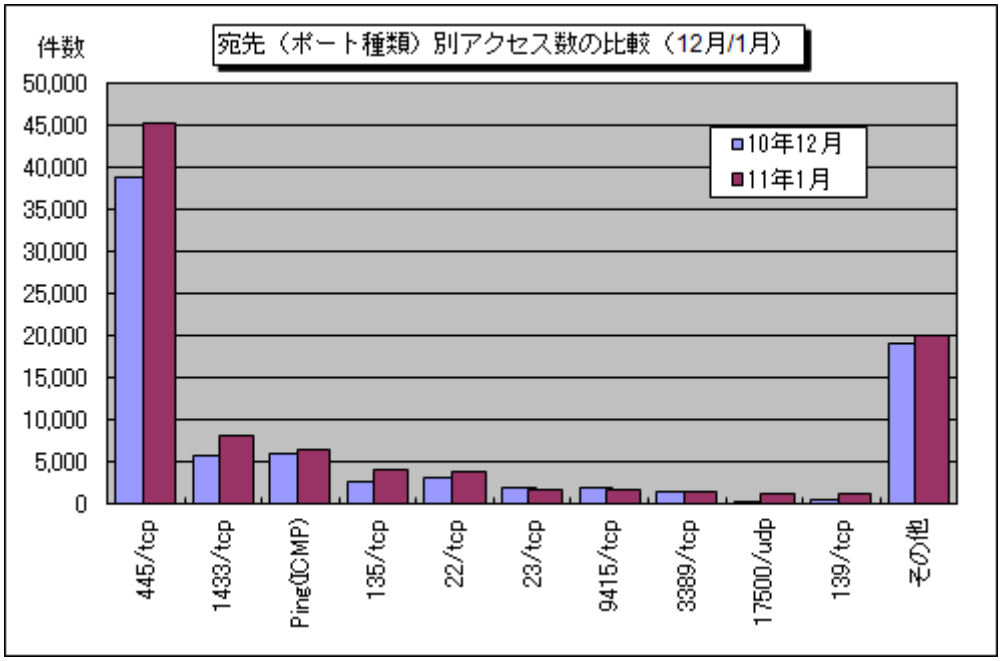

図 5-2：宛先（ポート種類）別アクセス数の比較（12 月/1 月）

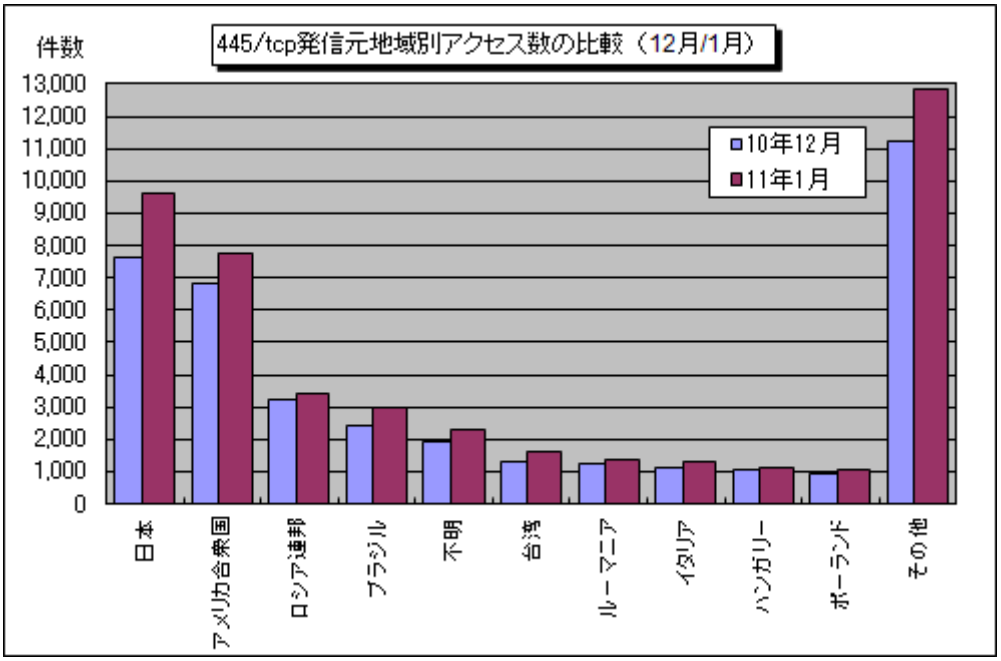

図 5-3：445/tcp 発信元地域別アクセス数の比較（12 月/1 月）

以上の情報に関して、詳細はこちらをご参照ください。
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/2011/documents/TALOT2-1102.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。』
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/

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