プレスリリース
第 09-40-164 号
2009 年 10 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 [2009 年 9 月分] について

IPA（独立行政法人情報処理推進機構、理事長：西垣 浩司）は、2009 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。

1. 今月の呼びかけ

「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！」
― ある日突然、ログインしたらアイテムが空っぽに？！ ―

最近、オンラインゲームを利用していて不正アクセスの被害に遭ったという相談や届出が、IPA に多く寄せられています。被害内容としては、一般に**アカウントハッキング**と呼ばれる、「オンラインゲームを利用する際に必要なユーザーID とパスワードを第三者に悪用され、ゲーム内のキャラクターが所持するアイテム（ここでは、ゲーム内のキャラクターが使用する武器などの持ち物やゲーム内の通貨を指します）を盗まれてしまう」というものです。

こうした被害が増えている背景として、ゲーム内のアイテムが、現実世界の通貨で売買取引（RMT:Real Money Trading）されているということが挙げられます。アイテムによっては高値で売買されるため、金銭目的の犯罪者に狙われているのです。

オンラインゲーム利用者は、自分が「狙われている」という実態を認識し、自己防衛策を講じて被害に遭わないようにしましょう。

（1）オンラインゲーム被害例

オンラインゲームとは、インターネットを利用して、不特定多数の利用者が同時に参加して行うゲームです。IPA に寄せられた、2009 年 1 月から 9 月までのオンラインゲーム関連の相談・届出件数の合計は、31 件です。このうち半分以上の 16 件は 7 月から 9 月に受けたものであり、被害は増加傾向にあります。

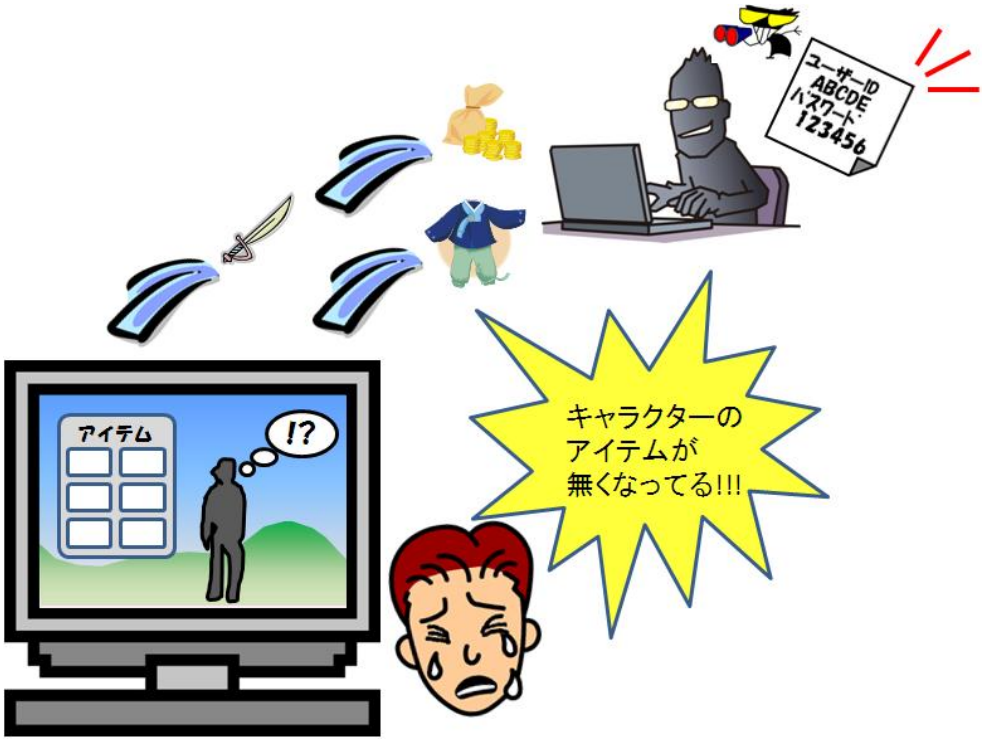


図 1：アカウントハッキングでアイテムが盗まれてしまった様子のイメージ

IPA の相談・届出窓口に寄せられた、具体的な被害の例を下記に示します。

事例 1：**【キャラクターのアイテムが盗まれる被害】**

ゲーム内で知り合った利用者とチャット中に、“ゲームをするには便利なツールだから”としつこく言われて、しかたなくダウンロードしてインストールをしてしまった。そのツールは実はゲームのユーザーID とパスワードを盗むウイルスだった。後日オンラインゲームにアクセスしてみると、キャラクターのアイテムが全て盗まれてしまっていた。

事例 2：**【ゲームサイトのログイン ID とパスワードを聞き出される被害】**

ゲーム中、“サイト運営者”と名乗る人物からチャット要求があり、運営者がサイト内をパトロールしているのかと思いチャットに応じた。その際、確認と称してユーザーID とパスワードを尋ねてきたので教えてしまった。“サイト運営者”と名乗っていた人物は、実は悪意ある利用者だった。気付いた時には既に遅く、キャラクターのアイテムが全て盗まれてしまっていた。

上述した事例の場合、アカウントハッキングの原因はユーザーID とパスワードの漏えいになります。次に、ユーザーID とパスワードの漏えいの原因について考えられる手口を記述します。

（2）考えられる手口

上記（1）の事例 1 に対応する手口は以下のとおりです。

手口 1：【ユーザーID とパスワードを盗むウイルスに感染】

ウイルスが存在するメールの添付ファイルを開く、ウイルスが仕掛けられているウェブサイトにアクセスする、ウイルスに感染している USB メモリなどの外部記憶媒体をパソコンに繋げるなどの行為から、利用者側のパソコンに感染させられることが考えられます。ゲーム攻略サイトにウイルスが仕掛けられている場合もあります。

上記（1）の事例 2 に対応する手口は以下のとおりです。

手口 2：【ソーシャルエンジニアリングや悪意ある利用者との直接取引でパスワードを聞き出される】

“アイテムをあげる”、“アイテムを高値で買い取る”など、言葉巧みに言い寄られ、ユーザーID やパスワードを悪意ある利用者に教えてしまうことが考えられます。“ゲーム管理者”、“サイト運営者”と偽っている場合もあります。

（3）オンラインゲーム利用者の対策

オンラインゲーム利用者は、被害に遭わないように以下の対策を行ってください。

（i）予防策

上記（2）の**手口 1** に対する予防策は、下記の通り一般的なウイルス対策と同様です。

- OS やアプリケーションの脆弱性を解消する
- ウイルス対策ソフトを導入し、ウイルス定義ファイルを最新の状態にして使用する
- 自分が管理していない USB メモリなどの外部記憶媒体を、自分のパソコンに接続しない、または自分が管理していないパソコンに、自分の USB メモリなどの外部記憶媒体を接続しない

（ご参考）

「知っていますか？脆弱性（ぜいじゃくせい）」（IPA）

http://www.ipa.go.jp/security/vuln/vuln_contents/

「ウイルス感染を防ぐためのポイント」（IPA）

http://www.ipa.go.jp/security/personal/know/virus.html

上記（2）の**手口 2** の被害を防ぐためには、常日頃から以下の事項に注意してください。

- **知り合いの利用者でも、自分のユーザーID とパスワードは教えない**
  たとえ家族・身内でも教えないでください。
- **条件の良い取引を持ちかけられても相手にしない**
  うまい話の裏には罠があると思ってください。
- **ゲーム内の会話での誘導尋問に注意する**
  相手は、巧みな話術でユーザーID やパスワードを聞き出そうとします。相手からの質問に素直に答えた場合、内容によってはユーザーID やパスワードにつながるヒントを言ってしまっている場合がありますので、用心しましょう。また、パスワードも、大小英文字と数字に加え、入力が可能であれば記号も混ぜて、推測されにくいものにしましょう。
  （ご参考）
  「今一度、パスワードを点検しましょう！」（2008 年 10 月の呼びかけ）
  http://www.ipa.go.jp/security/txt/2008/10outline.html
- **ユーザーID とパスワードを尋ねられたら要注意**
  悪意ある利用者が、ゲーム管理者になりすまして聞いてきているかもしれません。信頼できるか分からない相手からユーザーID とパスワードを尋ねられたら、自分でゲーム管理者に直接確認を取りましょう。

その他に、利用者自身が管理していないパソコンからゲームを利用する場合、そのパソコンがウイルスに感染していて、知らないうちにユーザーID とパスワードの情報が漏えいする可能性があります。そのため、自身が管理していないパソコンからの利用は推奨しません。また、より実効性の高いセキュリティ対策（例えば二要素認証(※)を行っているなど）が実施されているゲーム運営業者を選ぶことも、自己防衛策の一つになります。

※　二つの要素により認証を行う方式。例えばオンラインバンキングでパスワード（暗証番号）に加えてワンタイムパスワードを併用する方式が広く使われています。

（ii）事後対策

アカウントハッキングの原因のほとんどは、ユーザーID とパスワードの漏えいにあります。従って、アイテムが盗まれたことに気づいたらすぐにパスワードの変更を行って下さい。また、被害の原因の一つであるウイルス感染の確認を行い、ウイルスに感染している場合は駆除をしてください。さらに、パソコンの OS や使用しているアプリケーションの脆弱性を解消してください。

同時に、IPA へ不正アクセス被害の届出をお願いします。IPA では、被害に遭った場合の対処方法の案内に努めています。

（ご参考）

「不正アクセスに関する届出について」（IPA）（TEL:03-5978-7509）

http://www.ipa.go.jp/security/ciadr/

上述した対策を行ってもまだ同じ被害に遭う場合は、ゲーム運営業者側の問題の可能性も考えられます。その場合、まずゲーム運営業者から当該被害の対応策が発表されていないか確認し、発表されていればその指示に従ってください。

ゲーム運営業者から当該被害の対応策が発表されていない場合、ゲーム運営業者からオンラインゲームを利用するための基本的なポリシーを記述したガイドラインが示されている場合がありますので、その内容を参考にし、被害に遭った場合の一般的な対応策について確認してください。また、対応策やガイドラインがない場合は、直接、利用者自身でゲーム運営業者に問い合わせてください。

（ご参考）

「オンラインゲームガイドライン」（日本オンラインゲーム協会）

http://onlinegameforum.org/guideline090903.pdf

被害内容の復旧については、ゲーム運営業者に問い合わせていただくことになります。場合によっては、警察に被害状況を申告するように指示されることもありますので、まずは最寄りの警察署に電話し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。

（ご参考）

「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/

オンラインゲームでの不正アクセス全般の被害相談窓口は、以下の通りです。

（ご参考）

「インターネット安全・安心相談」（警察庁）

http://www.npa.go.jp/cybersafety/

「都道府県警察本部のサイバー犯罪相談窓口等一覧」（警察庁）

http://www.npa.go.jp/cyber/soudan.htm

（4）ゲーム運営業者側の対策

アカウントハッキング被害の原因は、ゲーム運営業者側にある場合も考えられます。その場合、下記の手口が考えられます。

手口 1：【ゲーム運営業者側にあるサーバーへの攻撃（ブルートフォース攻撃等）】

ゲーム運営業者の管理しているサーバーが、大量のログイン試行攻撃（ブルートフォース攻撃等）への耐性を十分に備えていない場合、悪意ある者に不正にログインされ、オンラインゲーム利用者のアイテムが盗み取られます。

手口 2：【ゲーム運営業者側のウェブサイトに存在する脆弱性への攻撃】

ゲーム運営業者の管理しているサーバーが、OS やアプリケーションの脆弱性を突いた攻撃を受け、その結果サーバー内に侵入され、オンラインゲーム利用者の情報が盗み取られます。

ゲーム運営業者は、サーバーが上述した手口によって攻撃されることを認識し、**手口 1** の対策として、ログイン認証失敗の回数制限設定、IDS/IPS などの侵入検知システム導入などの対策を施しましょう。また、**手口 2** の対策として、使われていない機能やサービスが稼働していないか、OS やアプリケーションの脆弱性は解消されているかなど、管理しているサーバーの設定に不備がないか、今一度確認をしましょう。

（ご参考）

「ウェブサイト運営者のための脆弱性対応ガイド」（IPA）

http://www.ipa.go.jp/security/fy19/reports/vuln_handling/

「安全なウェブサイトの作り方」（IPA）

http://www.ipa.go.jp/security/vuln/websecurity.html

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、6 頁の「3.コンピュータ不正アクセス届出状況」を参照）

・ブラインド SQL インジェクション攻撃を受け、データベース内の情報を閲覧された疑い

・SQL インジェクション攻撃でクレジットカード情報が盗まれ、不正使用された

○ 相談の主な事例 （相談受付状況および相談事例の詳細は、8 頁の「4.相談受付状況」を参照）

・チャット中に教えてもらったサイトにアクセスしたらアダルトサイトの請求書が・・

・iPod にウイルス感染？

○ インターネット定点観測（10 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－

9 月のウイルスの検出数（※1）は、**約 7.6 万個**と、8 月の約 7.6 万個から同水準での推移となりました。また、9 月の届出件数（※2）は、**1,301 件**となり、8 月の 1,222 件から 6.5%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。
・9 月は、寄せられたウイルス検出数約 7.6 万個を集約した結果、1,301 件の届出件数となっています。

検出数の 1 位は、**W32/Netsky** で**約 6.8 万個**、2 位は **W32/Mydoom** で**約 2 千 7 百個**、3 位は **W32/Mytob** で**約 2 千 6 百個**でした。

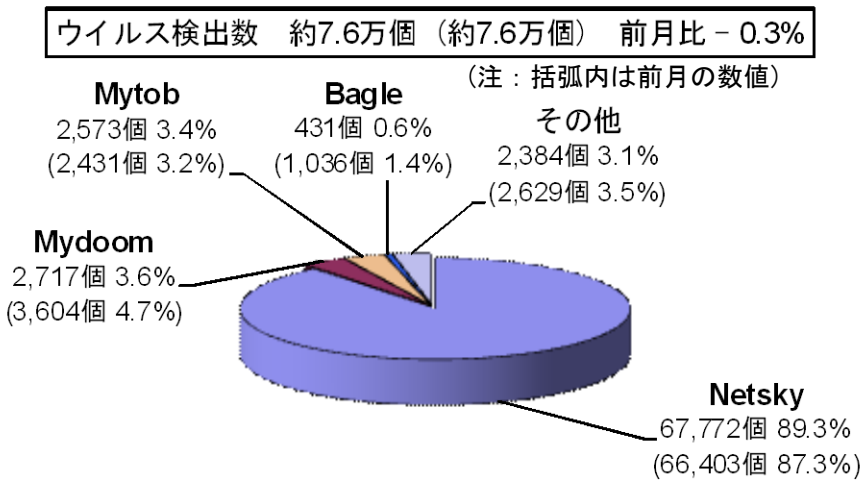


図 2-1：ウイルス検出数

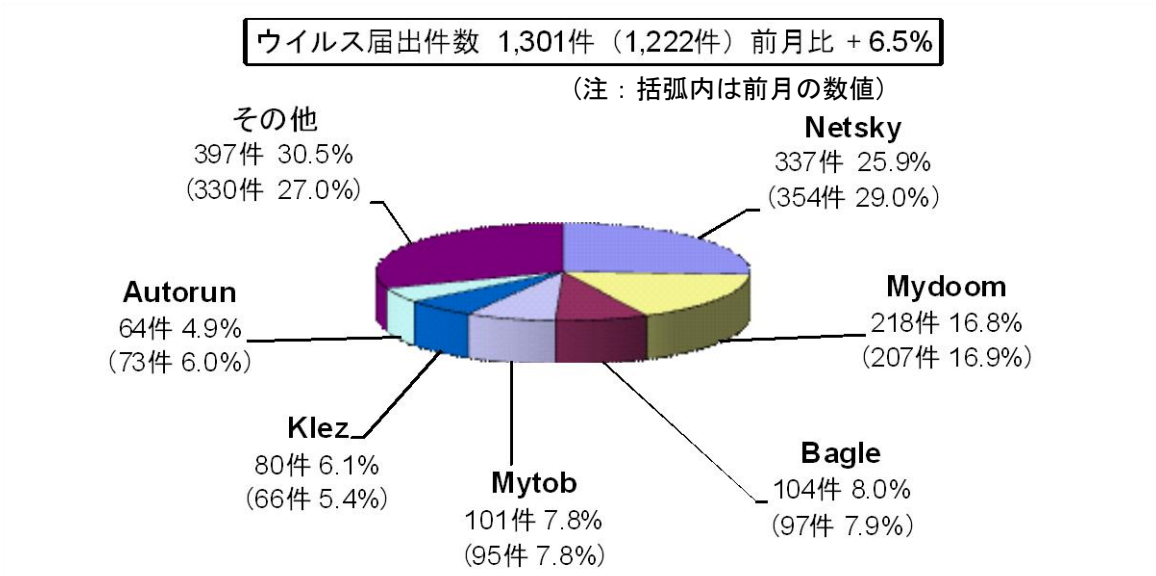


図 2-2：ウイルス届出件数

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

		4月	5月	6月	7月	8月	9月
届出(a) 計		9	8	7	14	20	11
	被害あり(b)	6	6	6	6	12	8
	被害なし(c)	3	2	1	8	8	3
相談(d) 計		39	45	35	24	39	44
	被害あり(e)	11	16	9	3	17	13
	被害なし(f)	28	29	26	21	22	31
合計(a+d)		48	53	42	38	59	55
	被害あり(b+e)	17	22	15	9	29	21
	被害なし(c+f)	31	31	27	29	30	34

（1）不正アクセス届出状況

9 月の届出件数は 11 件であり、そのうち何らかの被害のあったものは 8 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 44 件（うち 4 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 3 件、なりすまし 4 件、その他（被害あり）1 件、**でした。

「侵入」の被害は、SQL※インジェクション※攻撃を受け、ウェブサーバー内のクレジットカード情報などを閲覧されたり盗まれたりしたものが 2 件、ウェブページの改ざんが 1 件（不正なタグ埋め込み）、でした。侵入の原因は、ウェブアプリケーションの脆弱性を突かれたものが 2 件、などでした（残りの 1 件は原因不明）。

「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 4 件）でした。

※SQL (Structured Query Language)：リレーショナルデータベースマネジメントシステム(RDBMS)において、データの操作や定義を行うための問合せ言語のこと。
※SQL インジェクション：データベースへアクセスするプログラムの不具合を悪用し、正当な方法以外でデータベース内のデータを閲覧したり書き換えしたりする攻撃のこと。

（4）被害事例

[侵入]

（i）ブラインド SQL インジェクション攻撃を受け、データベース内の情報を閲覧された疑い

事例	・自部門のネットワークを管理する組織から、「ウェブサーバーへの SQL インジェクション攻撃を多数観測した」旨の連絡が入った。 ・保守業者が簡易ログ検査ツールで調査したが異常は無かった。しかし、別の業者に詳細解析してもらったところ、データベースへ不正なアクセスがあったことが判明。データベース内にあった、サイトへのログイン時に使う ID とパスワード情報が漏えいした可能性がある。 ・原因は、ウェブサーバー内で動かしていた cgi に脆弱性があり、SQL インジェクション攻撃が成功してしまったことであった。今回は、**ブラインド SQL インジェクション攻撃という手法が使われていた**。 ・cgi では一般的な SQL インジェクション攻撃などへの一通りの脆弱性対策を施していたが、ブラインド SQL インジェクション攻撃への対策は漏れていた。
解説・対策	**あまり知られていない攻撃手法だったため、対策が漏れてしまっていた**例です。攻撃手法は、日々進化しています。定期的に、専門業者にウェブサイトの脆弱性検査を依頼することをお勧めします。 （参考） 【ブラインド SQL インジェクションについての解説記事】 http://gihyo.jp/dev/serial/01/php-security/0006 経済産業省 - 情報セキュリティ監査企業台帳 http://www.meti.go.jp/policy/netsecurity/is-kansa/

（ii）SQL インジェクション攻撃でクレジットカード情報が盗まれ、不正使用された

事例	・オンラインショッピングサイトを運営している。クレジットカード会社から、カード不正利用に関する照会があり、社内でウェブサーバーを調査したが、異常は見つからなかった。その後も同様の照会が来たため、セキュリティ専門業者にアクセスログを調査してもらったところ、SQL インジェクション攻撃が成功しており、サーバー内で運用していたデータベースに登録されていたクレジットカード情報にアクセスされていたことが判明。 ・オンラインショッピングサイト構築用のウェブアプリケーションパッケージを購入し利用していたため、開発元に問い合わせるも、脆弱性は無いとの回答。しかしその後、そのウェブアプリケーションに、脆弱性があったことが判明。 ・現状の環境でのサイト再開は断念。セキュリティ要件が担保された別の ASP サービスの利用を検討中。
解説・対策	金銭の決済をするサイトでは、一度事故が発生すると被害甚大となります。サイト運用の際には、侵入検知システム（IDS/IPS など）や WAF を導入し常に監視の目を光らせるとともに、定期的に、専門業者にウェブサイトの脆弱性検査を依頼することをお勧めします。今後の**リスク回避策として、決済業務を外部委託する**手もあります。 （参考） IPA -ウェブサイト運営者のための脆弱性対応ガイド http://www.ipa.go.jp/security/fy19/reports/vuln_handling/ IPA - 安全なウェブサイトの作り方 http://www.ipa.go.jp/security/vuln/websecurity.html

4. 相談受付状況

9 月のウイルス・不正アクセス関連相談総件数は **1,653 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 **650 件**（8 月：654 件）でした。その他は、**『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 **6 件**（8 月：1 件）、**Winny に関連する相談**が **0 件**（8 月：3 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 **0 件**（8 月：2 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

		4月	5月	6月	7月	8月	9月
合計		1,668	1,765	1,898	1,708	1,792	1,653
	自動応答システム	962	992	1,081	923	1,015	915
	電話	651	710	777	736	702	676
	電子メール	55	58	37	47	68	60
	その他	0	5	3	2	7	2

※ 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）、fushin110@ipa.go.jp（不審メール 110 番）、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。

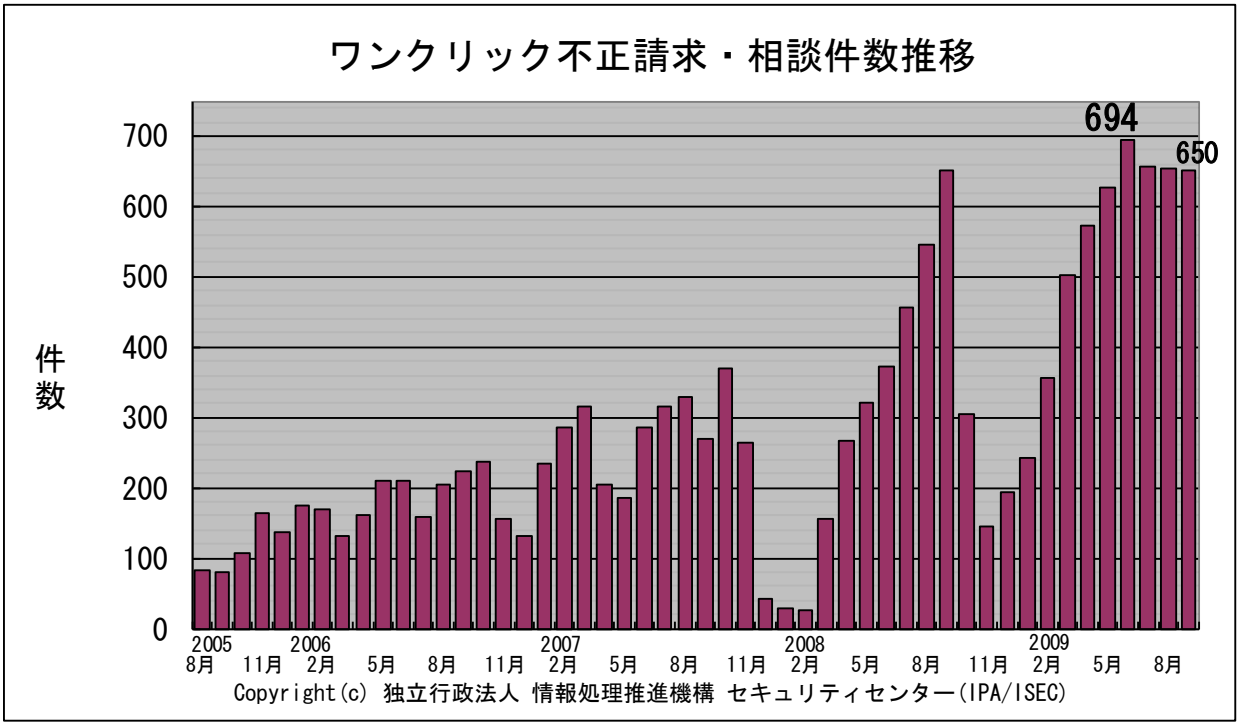


図 4-1：ワンクリック不正請求相談件数の推移

主な相談事例は以下の通りです。

（i）チャット中に教えてもらったサイトにアクセスしたらアダルトサイトの請求書が・・

相談	【子どもからの相談】あるサイトで、面識の無い相手とチャットで会話をしていた。相手から、あるサイトへのリンク（URL）を示されたので、クリックして先に進んで行った。アダルトサイトだった。その後、パソコンを再起動しても、当該アダルトサイトの利用料金請求書画面が表示されるようになった。ウイルス感染していた。
回答	ネット上には残念ながら、相手を騙そうとする悪意あるパソコン利用者が存在します。特に子どもは騙され易いと言えます。**パソコンを共有し、子どもにも操作させるという家庭では、ウイルス対策ソフトの導入はもちろんのこと、有害サイトへのアクセスをブロックすること（フィルタリング）が重要**になります。単体のフィルタリングソフトがありますが、総合ウイルス対策ソフトの機能として装備されていたり、インターネット接続業者（プロバイダ）のサービスとして提供されている場合もあります。 （ご参考） IPA - 2007 年 8 月の呼びかけ「忘れずに、ネットと心のファイアーウォール」 http://www.ipa.go.jp/security/txt/2007/08outline.html

（ii）iPod にウイルス感染？

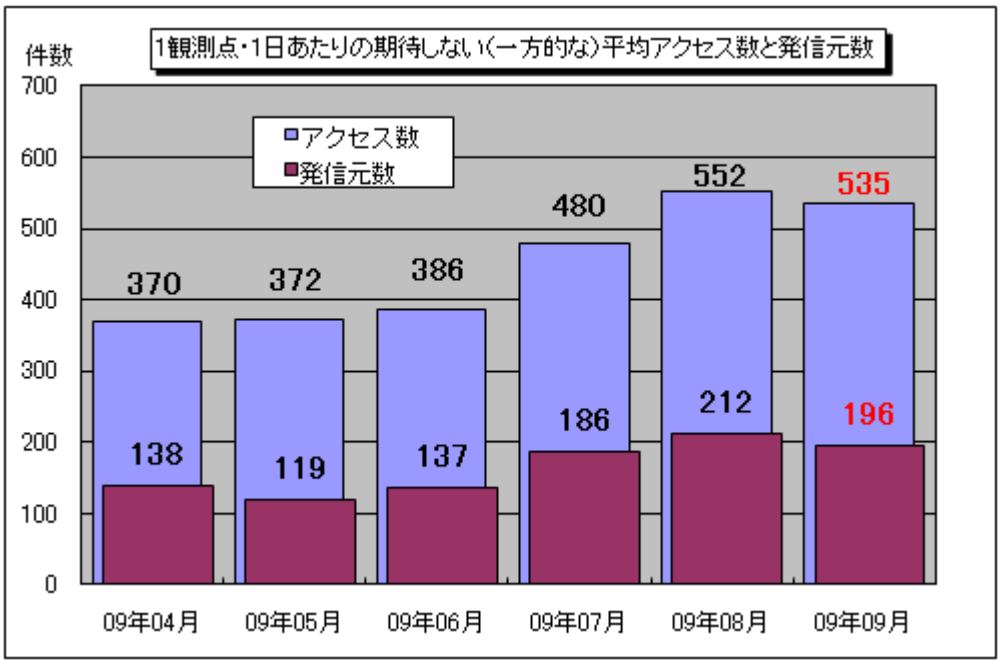
相談	中国のサイトから、ある音楽ファイルをダウンロードした。その後、気のせいか、パソコンの調子がおかしい。相談したら初期化を勧められたので、iPod（携帯音楽プレーヤー）経由でパソコン内のデータを他のパソコンに退避することにした。iPod にファイルをコピーし、他のパソコンに接続した瞬間、ウイルス対策ソフトがウイルスを検知した。iPod にウイルスが感染していたのでしょうか。
回答	ウイルスファイルが iPod に置かれていただけですので、**iPod がウイルスによって悪影響を及ぼされる訳ではありません**。何らかの原因で、元のパソコンにウイルスが感染していたようです。そのウイルスは、**USB メモリなどの外部記憶メディアを介して感染を拡大していくタイプ**であり、iPod にもウイルスファイルがコピーされていました。この場合、無意識のうちにウイルスを他のパソコンにばら撒いてしまうことになりますので、まずは自身のパソコンのウイルス対策を確実にしましょう。その上で、**USB メモリなどを接続した際に、ウイルスが勝手に起動しないように、Windows の「自動実行機能」を無効にするのが良い**でしょう。 （ご参考） IPA - 2009 年 5 月の呼びかけ「USB メモリのセキュリティ対策を意識していますか？」 http://www.ipa.go.jp/security/txt/2009/05outline.html

5. インターネット定点観測での 9 月のアクセス状況

インターネット定点観測（TALOT2）によると、2009 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 **160,487 件**、延べ発信元数（※）は **58,770 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 196 の発信元から 535 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】

2009 年 4 月～2009 年 9 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 1-1 に示します。9 月の期待しない（一方的な）アクセスは、8 月と比べて若干減少しました。

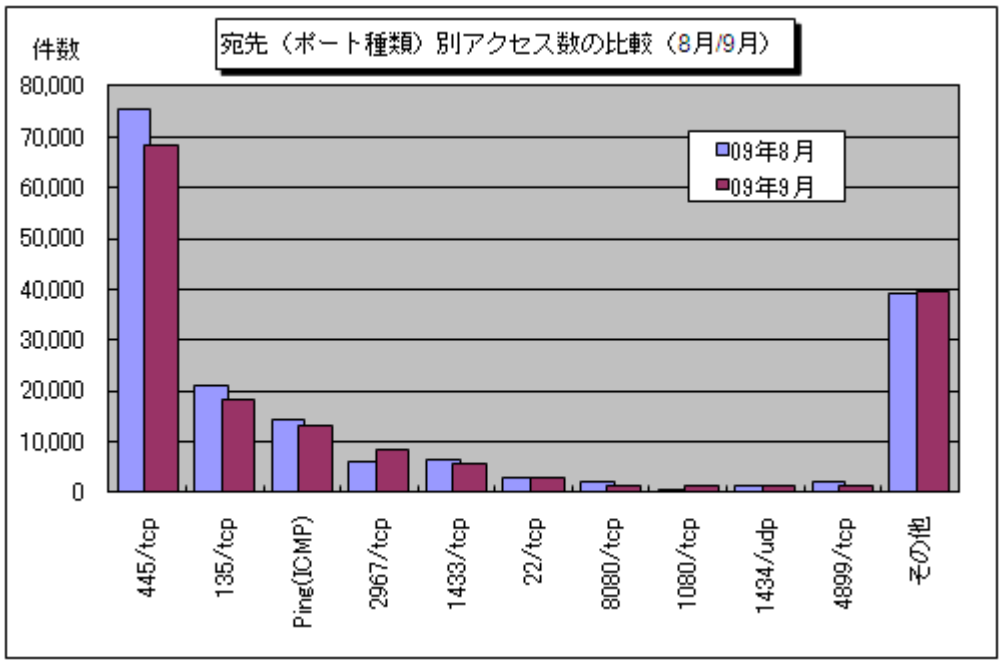
8 月と 9 月の宛先（ポート種類）別アクセス数の比較を図 5-2 に示します。

8 月と 9 月のアクセス数を比較して、大きく変化したポートへのアクセスはありませんでした。4 ヶ月前から増加傾向が続いていた 445/tcp へのアクセスは、9 月に入り減少に転じました。

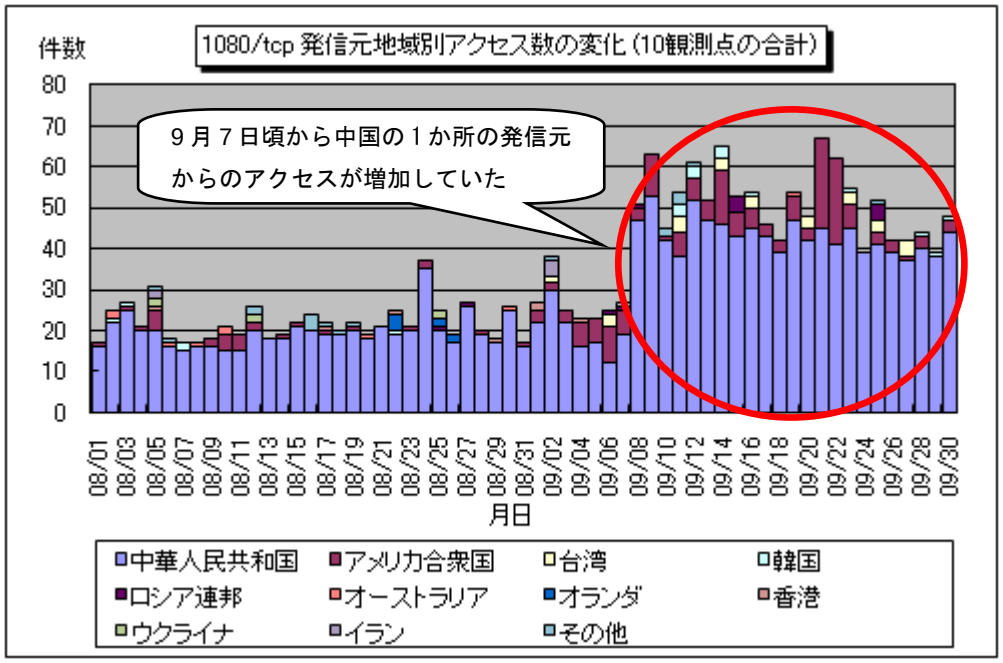
また、これまではアクセス数の上位に挙がってこなかった 1080/tcp へのアクセスが、普段より多く観測されました。これは中国の 1 か所の発信元から送られるアクセスが、9 月 7 日頃から継続的に観測されていたため（図 5-3 参照）であり、この発信元からは同じ観測点の 1025/tcp へもほぼ同時にアクセスしていたことが分かっています。これらのアクセスは TALOT2 の 10 観測点中 7 観測点で観測されていたことから、同じ現象が広範囲で発生していたことが予想されます（図 5-4 および図 5-5 参照）。

1080/tcp は SOCKS サーバー（※）が使用するポートとして一般的であり、1025/tcp は 2005 年に Windows の脆弱性（MS05-051）を悪用するウイルスが攻撃を行ったポートです。この発信元がこれらのポートに継続的にアクセスしていた目的は不明です。

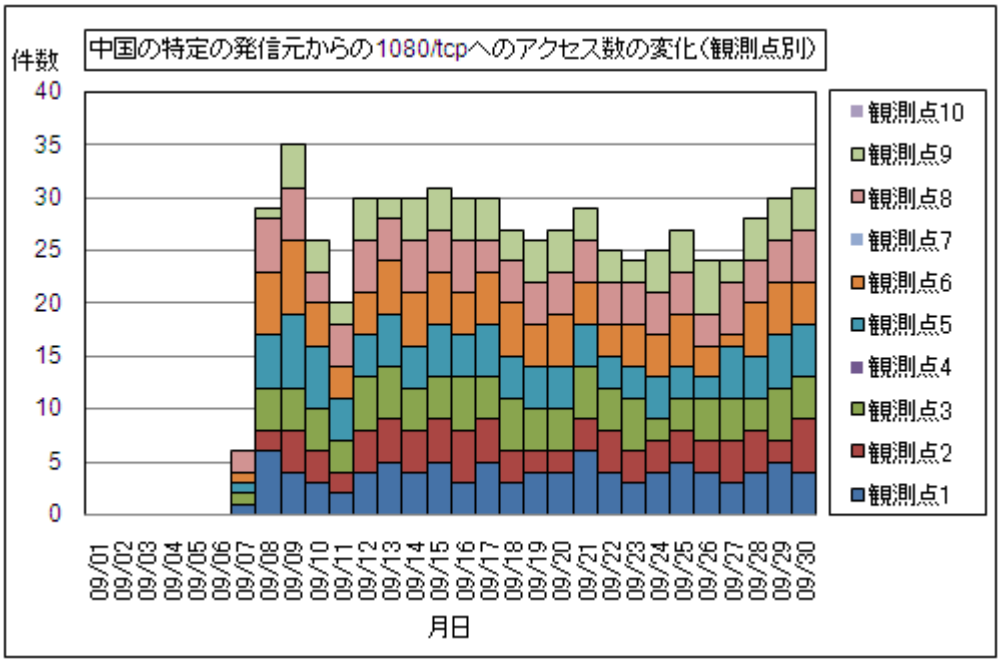
SOCKS サーバー（※）：社内 LAN などからインターネットへの通信を代理で行うためのプロキシサーバの一つ。



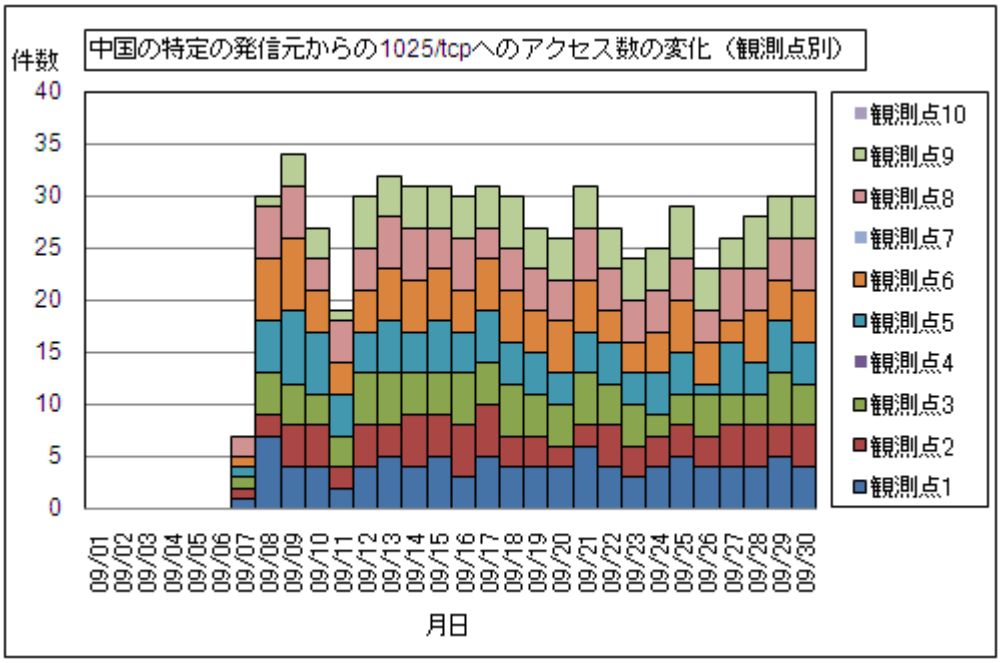
【図 5-2：宛先（ポート種類）別アクセス数の比較（8 月/9 月）】



【図 5-3：1080/tcp 発信元地域別アクセス数の変化（10 観測点の合計）】



【図 5-4：中国の特定の発信元からの 1080/tcp へのアクセス数の変化（観測点別）】



【図 5-5：中国の特定の発信元からの 1025/tcp へのアクセス数の変化（観測点別）】

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/2009/documents/TALOT2-0910.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　花村／加賀谷／大浦
Tel:03-5978-7527 Fax:03-5978-7518
E-mail: isec-info@ipa.go.jp