プレスリリース
第 10-24-188 号
2010 年 6 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 [2010 年 5 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、2010 年 5 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

「 深刻化する偽セキュリティ対策ソフトの被害！ 」

この数か月にわたり、過去の「呼びかけ」で複数回取り上げている「偽セキュリティ対策ソフト」型ウイルスによる被害の相談が増加しています（図 1-1 を参照）。最近の「偽セキュリティ対策ソフト」型ウイルスに関する相談の傾向として、復旧のための操作ができなくなるなど、被害に遭ったパソコンの症状が以前より深刻化しています。また、感染経路が「ガンブラー」(※1)の手口によるものだと考えられる事例が多く、セキュリティ対策が不十分なパソコンでは、改ざんされたウェブサイトを閲覧しただけで、この種のウイルスに感染させられてしまう可能性があります。

「偽セキュリティ対策ソフト」型ウイルスの被害に遭わないための対策は、このウイルスに限った特別なものではなく、基本的なセキュリティ対策を漏れなく実施することです。ここでは、被害の実例を紹介し、対策について説明します。

(※1) ガンブラー： 「"ガンブラー" の手口を知り、対策を行いましょう」（IPA, 2010 年 2 月の呼びかけ）を参照
http://www.ipa.go.jp/security/txt/2010/02outline.html#5

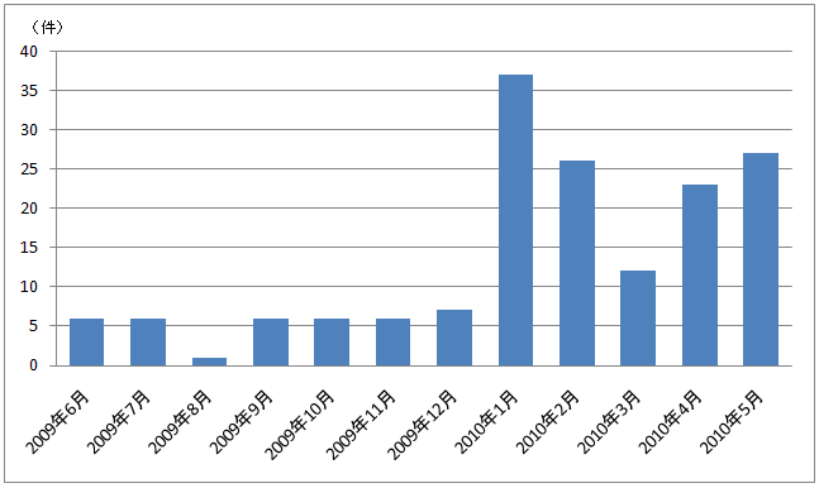


図 1-1：「偽セキュリティ対策ソフト」型ウイルスに関する過去 1 年分の相談件数

(1)「偽セキュリティ対策ソフト」型ウイルスの概要

「偽セキュリティ対策ソフト」型ウイルスとは、“ウイルスに感染している”といった虚偽の警告メッセージを表示し、それらを解決するには有償版の製品が必要であるとして、例えばクレジットカード番号の入力を要求し、金銭を騙し取るタイプのウイルスです。正規のセキュリティ対策ソフトと見分けがつかないような見栄えの画面と共に、「Security essentials 2010」や「XP Smart Security 2010」など、いかにも本物らしいソフトの名称（他にも多くのソフト名が確認されています）が表示されるため、注意が必要です。

この種のウイルスの中には、ウイルスの駆除やパソコンからのデータの退避（バックアップ）作業を妨害するものもあるため、深刻な被害となる場合があります。「偽セキュリティ対策ソフト」型ウイルスについての詳細は、2009 年 11 月の呼びかけも参照してください。

（ご参考）
「 偽のセキュリティ対策ソフトの脅威が再び拡大！ 」（IPA, 2009 年 11 月の呼びかけ）
http://www.ipa.go.jp/security/txt/2009/11outline.html#5

（2）被害の実例

具体的な相談と届出の事例を示します。次の図 1-2 は、下記の事例で相談者が感染させられた「偽セキュリティ対策ソフト」型ウイルスの画面（一部）です。

【事例1】偽セキュリティ対策ソフト「Security essentials 2010」の画面

【事例2】偽セキュリティ対策ソフト「Control center」の画面

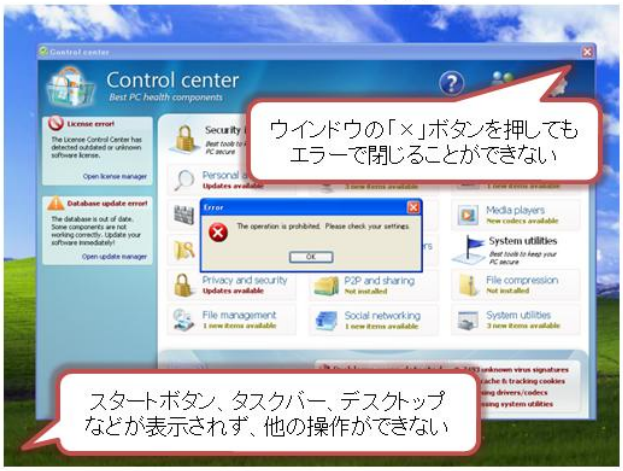


図 1-2：「偽セキュリティ対策ソフト」型ウイルスの感染画面例

【事例 1】

相談内容	**ウェブサイトを閲覧していたら、突然英語の画面になり**、再起動させても消えない。「YOUR SYSTEM IS INFECTED」などと表示されている。「セーフモード」(※2)で起動しても、英語の警告メッセージが表示される。「タスクマネージャ」(※3)や「システムの復元」(※4)も起動できず、パソコンが正常に利用できない。
ソフト名	Security essentials 2010
解説	相談者が感染させられた「Security essentials 2010」は、5 月に最も相談が多かったウイルスです。マイクロソフト社が提供しているセキュリティ対策ソフトの「Microsoft Security Essentials」とは関係なく、紛らわしい名前で有用なソフトと勘違いさせようとしていると考えられます。このウイルスについては、今年の 2 月から IPA へ相談が寄せられています。

(※2) セーフモード： パソコンの復旧作業などを行うための Windows の特殊な起動方法。

(※3) タスクマネージャ： パソコン上で動作しているプログラムの一覧表示や、任意のプログラムの停止を行うためのツール。

(※4) システムの復元： Windows に付属している、パソコンの設定などを以前の状態に巻き戻すツール。

【事例 2】

相談内容	パソコンを起動すると､ウイルス対策ソフトのライセンスが切れているため料金を支払うよう書かれた画面が表示されるようになった。「セーフモード」でも同じ状況で、それ以上の操作ができない。パソコン内に必要な情報が残っており、初期化するわけにもいかなかったため、クレジットカード番号を入力した。そうすると、操作できるようにはなったが、デスクトップ上のファイルが消えていた。
ソフト名	Control center　（Control center - Best PC health components）

解説	パソコンやその中のデータだけでなく、金銭的な被害まで発生した事例です。ウイルスの作者は、感染させたパソコンを操作不能に陥れることで、料金を支払わせようとしています。本件の感染経路は不明ですが、感染の直前に**不審な添付ファイルの付いたメールを開いた**、とのことでした。なお、ライセンスを購入しても状況が改善する保証はなく、支払いをすべきではありません。

【事例 3】

相談内容	インターネットを利用していたら、画面に英文のメッセージが大量に表示され、正しく動作しなくなった。パソコンのメーカーに問い合わせたところ、初期化を指示されたので、その通りにした。「Security Tool」というものらしいが、対処はこれで良かったのか。
ソフト名	Security Tool
解説	「Security Tool」は水色の画面が特徴的なウイルスで、IPA へは 2009 年の末ごろから相談が寄せられています。対処としては、初期化で問題ありません。ただ、**セキュリティ対策が不十分な状態でウェブサイトを閲覧していて感染した**とのことで、相談者の方が自分自身でセキュリティ対策を実施できるようにならなければ、また同じ被害に遭う可能性があります。

このほか、5 月に相談・届出があった「偽セキュリティ対策ソフト」型ウイルスは次の通りです。多種のウイルスが広くばら撒かれていることが推測されます。

- XP AntiMalware 2010
- XP Smart Security 2010
- Live Security Suite
- Data Protection
- Digital Protection
- Desktop Security 2010

事例に似た症状が現れたり、図 1-2 のような身に覚えのないウイルススキャンの画面が表示された場合は、「偽セキュリティ対策ソフト」型ウイルスに感染させられた可能性が高く、加えて、「偽セキュリティ対策ソフト」型ウイルス以外のウイルスも同時にパソコンに侵入している可能性があります。次の（3）に示す対処を実施してください。

このような「偽セキュリティ対策ソフト」型ウイルスなどの被害に遭わないための事前対策については、（4）を参照してください。

（3）感染時の対処

事例で示したように、「偽セキュリティ対策ソフト」型ウイルスに一旦感染させられてしまうと、復旧や駆除が難しい場合があります。感染時の対処の指針を次に示しますので、これを参考に、症状の改善や復旧を試みてください。

- パソコンが操作できる状態であれば、最新のウイルス対策ソフトでパソコンのスキャンを行い、ウイルスの駆除を試みます。
  - ウイルス対策ソフトが手元にない場合は、各ウイルス対策ソフトのベンダーがウェブサイトで提供している「オンラインスキャン」を使うこともできます。
- ウイルス対策ソフトでの駆除ができない場合は、「システムの復元」（下記（iii）を参照）による復旧を試みます。
- パソコンが操作できない、ウイルス対策ソフトによる駆除ができない、あるいは「システムの復元」がうまくいかない、といった場合は、パソコンを「セーフモード」（下記（ii）を参照）で起動した上で、これらの作業を再度試みます。
  - パソコンのシャットダウン操作すらできない状態であれば、本体の電源ボタンをしばらく押し続け、強制的に電源を切ってから、「セーフモード」での起動を行います。
- これらの作業で復旧しない場合は、パソコンの初期化（購入した時の状態に戻す作業）を行います。「偽セキュリティ対策ソフト」型ウイルスに感染している状態のパソコンは、例えある程度

操作ができたとしても、ウイルスによる情報漏えい等が発生する可能性があるため、そのまま使用することは危険です。

以下、対処における個別の注意点や手順について（i）～（iv）に示します。

（i）「偽セキュリティ対策ソフト」のライセンス料は支払わないこと

ライセンス料を支払ったとしても、状況が改善するとは限りません（事例 2 を参照）。クレジットカード番号を入力した場合は、その情報が更に悪用される可能性もあります。悪意のある人物の行為を助長することにもなりかねないため、料金を支払うことは避けてください。

（ii）「セーフモード」の利用

Windows を「セーフモード」で起動することで、ウイルスの動作を制限できる場合があり、通常の状態ではウイルスによる妨害で正しく動作しなかったツールを利用できる可能性があります。「セーフモード」を利用し、**データのバックアップ**、**ウイルス対策ソフトによる駆除**、または**「システムの復元」**などを試してください。

「セーフモード」の利用方法については、下記のウェブページを参照してください。パソコンの機種により「セーフモード」での起動方法が異なる場合がありますので、不明な点はパソコンのメーカーへお問い合わせください。

（ご参考）
「Windows XP を セーフ モードで起動する方法」（Windows XP）（マイクロソフト社）
http://support.microsoft.com/kb/880414/ja
「コンピュータをセーフ モードで起動する」（Windows Vista）（マイクロソフト社）
http://windows.microsoft.com/ja-jp/windows-vista/Start-your-computer-in-safe-mode
「コンピューターをセーフ モードで起動する」（Windows 7）（マイクロソフト社）
http://windows.microsoft.com/ja-JP/windows7/Start-your-computer-in-safe-mode

（iii）「システムの復元」による復旧

最新のウイルス対策ソフトを使用しても症状が治まらない場合、「システムの復元」を行うことで、状況を改善できる場合があります。「システムの復元」とは、Windows XP、Windows Vista、Windows 7 に付属しているツールで、パソコンの動作が不安定になるなど、使用に支障がある状態に陥った場合に、以前の状態に戻すことができる機能です。

（ご参考）
「Windows XP 機能別紹介：システムの復元」（Windows XP）（マイクロソフト社）
http://www.microsoft.com/japan/windowsxp/pro/business/feature/performance/restore.mspx
「システムの復元とは」（Windows Vista）（マイクロソフト社）
http://windows.microsoft.com/ja-JP/windows-vista/What-is-System-Restore
「Windows 7 の機能：システムの復元」（Windows 7）（マイクロソフト社）
http://windows.microsoft.com/ja-JP/windows7/products/features/system-restore

なお、下記のウェブページにて、Windows を「セーフモード」で起動し、「システムの復元」を実施するための具体的な手順を案内しています。

（ご参考）
「Windows での「システムの復元」の実施手順」（IPA）
http://www.ipa.go.jp/security/restore/

（iv）パソコンの初期化

症状が改善しない場合はパソコンの初期化を行ってください。

なお、「偽セキュリティ対策ソフト」型ウイルスでは、複数のウイルスに感染させられている場合があり、復旧できたように見えている場合でも、ウイルスの一部がパソコンに残っている可能性はゼロではありません。全てのウイルスを確実に消去するために、IPA では原則として初期化を推奨しています。特に、パソコンの動作が不安定であったり、使用していて違和感を覚えた場合は、初期化を検討してください。

初期化を実施する場合、パソコン内のデータは全て消えてしまいますので、通常の操作が可能であれば、できる限り重要なデータのバックアップを取得することを勧めます。初期化の手順については、パソコンの取扱説明書に記載されている「購入時の状態に戻す」などの手順を参照してください。

なお、初期化を行った直後は、パソコンのセキュリティ対策が不十分な状態となります。再び被害に遭うことのないよう、下記（4）の事前対策を確実に実施してください。また、バックアップしたデータを初期化したパソコンに戻す前に、必ずウイルスチェックを行ってください。

（4）事前対策

パソコンのセキュリティ対策に不備が有る場合、インターネット接続中には、今回紹介した事例のような被害に繋がる危険にさらされています。「偽セキュリティ対策ソフト」型ウイルスに限らず、ウイルス全般への防御策として、次に挙げる基本的な対策を漏らさず実施してください。

（i）データの定期的なバックアップ

パソコンの故障など、原因はウイルスに限りませんが、パソコン内のデータはいつでも失われる可能性があることを意識し、重要なデータは定期的にバックアップを行ってください。今回取り上げた「偽セキュリティ対策ソフト」型ウイルスの中には、パソコンからのデータのバックアップ作業を妨害するものもあり、被害に遭った後では手遅れとなってしまう場合があります。

（ii）ウイルス対策ソフトの導入

ウイルス対策ソフトは万能ではありませんが、重要な対策の一つです。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に保つことで、ウイルスの侵入阻止や、侵入してしまったウイルスの駆除ができます。近年のウイルスは、パソコンの画面の見た目では感染していることが分からないものが多いため、ウイルスの発見と駆除には、ウイルス対策ソフトが必須です。

一般利用者向けのウイルス対策ソフトとしては、ウイルスの発見と駆除だけでなく、危険なウェブサイトを閲覧しようとした時にブロックを行う機能などを備える、「統合型」と呼ばれるものを推奨します。

（iii）脆弱性の解消

「ガンブラー」の手口などで使われる、ウェブサイトを閲覧するだけでウイルスに感染させられてしまう「ウェブ感染型ウイルス」は、パソコン内にある**「ウイルスの侵入を許してしまう弱点」**、すなわち**脆弱性**を悪用して侵入してきます。従って、この脆弱性を解消することが、重要な対策の一つです。

脆弱性は、OS（Windows など）、ブラウザ（Internet Explorer など）、その他のアプリケーションソフト、それぞれに存在する可能性があります。パソコンに導入しているソフトウェアについては、できる限り全てを最新版に更新し、脆弱性を解消しましょう。

ソフトウェアの更新の方法について、次に補足します。

- Windows（OS 本体）、Internet Explorer、Microsoft Office（Word や Excel）の更新
  - パソコンの設定によっては「自動更新」の機能がオンになっており、その場合は自動的に最新版に更新されます。手動で更新を行う場合は、「Windows Update」または「Microsoft Update」を使用します。詳しくは、下記のマイクロソフト社のウェブペ

ージを参照してください。

- （ご参考） 「Microsoft Update 利用の手順」（マイクロソフト社）
  http://www.microsoft.com/japan/security/bulletins/j_musteps.mspx

- 「MyJVN バージョンチェッカ」による確認
  - IPA では、Adobe Flash Player など、ウイルスによって狙われることが多いソフトウェアについて、それらがパソコンに導入されているか、および最新版となっているか否かをチェックできるツールを公開しています。詳しくは、下記の「MyJVN バージョンチェッカ」のウェブページを参照してください。また、「MyJVN バージョンチェッカ」の使い方や、個々のソフトウェアを最新版にする手順については、下記の「ホームページからの感染を防ぐために」のページを参照してください。
  - （ご参考） 「MyJVN バージョンチェッカ」（IPA）
    http://jvndb.jvn.jp/apis/myjvn/#VCCHECK
    ※ 2010 年 6 月現在、Windows XP と Vista に対応しています。
  - （ご参考） 「ホームページからの感染を防ぐために」（CCC）
    https://www.ccc.go.jp/detail/web/index.html
- その他のソフトウェア
  - ソフトウェアの更新の方法は、それぞれ異なります。自分のパソコンに導入されているソフトウェアを把握し、定期的に更新を行うことが理想です。パソコン初心者がすぐに実施することは難しいですが、自己防衛のために知識や操作方法の習得を心掛けてください。
- 脆弱性の情報の収集
  - IPA では、一般利用者の多いソフトウェアに脆弱性が発見された場合、注意喚起を行っています。定期的に下記の「緊急対策情報・注意喚起 一覧」のウェブページを参照し、注意喚起が行われた場合は、自分のパソコンに該当するソフトウェアが入っているかを確認し、対応してください。
  - （ご参考） 「緊急対策情報・注意喚起 一覧」（IPA）
    http://www.ipa.go.jp/security/announce/alert.html
  - 「脆弱性が発見されてから、その修正プログラムが公開されるまでの期間」は、脆弱性を解消できない状態となります。この期間を狙う攻撃を「ゼロデイ攻撃」と呼び、防御することが非常に難しく、流行した場合はインターネットを利用することが危険な状態となります。
    「ゼロデイ攻撃」に対しては、修正プログラムが提供されるまでは脆弱性を解消できないため、できる限りの「回避策」を取ることで対応します。「回避策」は、問題となっているソフトウェアによって様々です。例えば、該当ソフトウェアの設定を変更して問題のある機能を停止する、該当ソフトウェアを悪用されないようパソコンから削除するといった対処があります。
    上記の「緊急対策情報・注意喚起 一覧」のウェブページでは、「ゼロデイ攻撃」に関する情報も発信しています。「回避策」を取ることで他の機能に影響を及ぼす場合もありますので、情報をよく確認した上で、対応してください。
  - 「ゼロデイ攻撃」についての詳細は、下記のウェブページを参照してください。
    （ご参考）「修正プログラム提供前の脆弱性を悪用したゼロデイ攻撃について」（IPA）
    http://www.ipa.go.jp/security/virus/zda.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、10 頁の「3.コンピュータ不正アクセス届出状況」を参照）
- “ガンブラー”によるものと思われる被害
- 無料オンラインゲームのアカウントが乗っ取られた

○ 相談の主な事例 （相談受付状況および相談事例の詳細は、12 頁の「4.相談受付状況」を参照）
- パソコンを知り合いに貸したら、アダルトサイトの請求画面が表示されて戻ってきた！
- 自分のウェブサイトが改ざんされていないか確認したい

○ インターネット定点観測（13 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）ウイルス届出状況

5 月のウイルスの検出数（※1）は、**約 5 万個**と、4 月の約 4 万個から 26.8%の増加となりました。また、5 月の届出件数（※2）は、**1,084 件**となり、4 月の 1,077 件から同水準での推移となりました。

※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。
・5 月は、寄せられたウイルス検出数約 5 万個を集約した結果、1,084 件の届出件数となっています。

検出数の 1 位は、**W32/Netsky** で**約 3.7 万個**、2 位は **W32/Koobface** で**約 7 千個**、3 位は **W32/Mydoom** で**約 4 千個**でした。

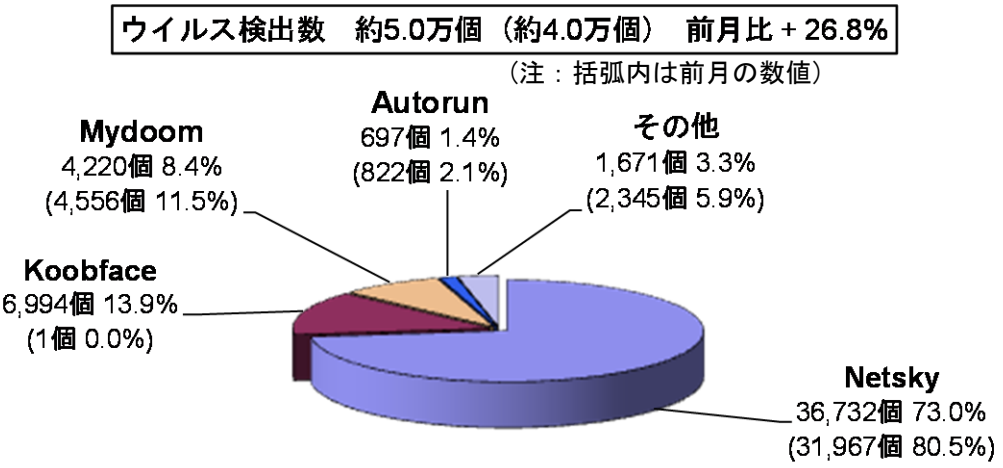


図 2-1：ウイルス検出数

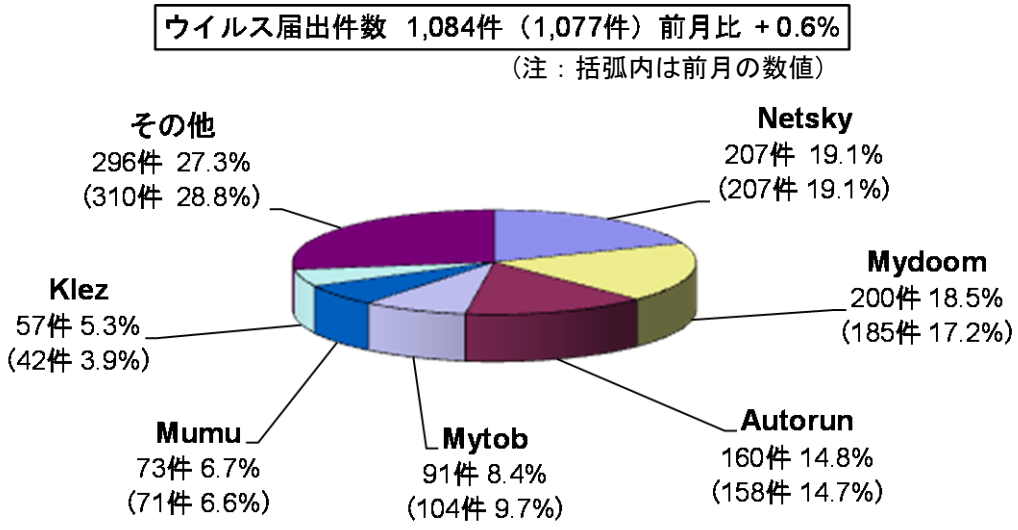


図 2-2：ウイルス届出件数

（2）不正プログラムの検知状況

2010 年 5 月の不正プログラムの検知状況は、4 月と同様に大きな変化はありませんでしたが、「偽セキュリティ対策ソフト」型ウイルスである FAKEAV の検知数の増加が複数確認されました。（図 2-3 参照）。

不正プログラムはメールの添付ファイルとして配布されるケースが多いため、メールの添付ファイルの取り扱いには継続して注意を払う必要があります。また、不正プログラムの配信には、ボットに感染したパソコンが悪用されることがあります。

サイバークリーンセンター※では、ボットに関する対策や駆除ツールを提供しています。不正プログラムのメール配信に加担することがないよう、ボットに感染していないか確認するとともに、不正プログラムを取り込まないようにするなど、感染防止のための対策実施が必要です。

（ご参考）
「感染防止のための知識」（サイバークリーンセンター）
https://www.ccc.go.jp/knowledge/

※サイバークリーンセンターとは、総務省・経済産業省が連携して実施するボット対策プロジェクトです。
（参考）サイバークリーンセンターについて
https://www.ccc.go.jp/ccc/

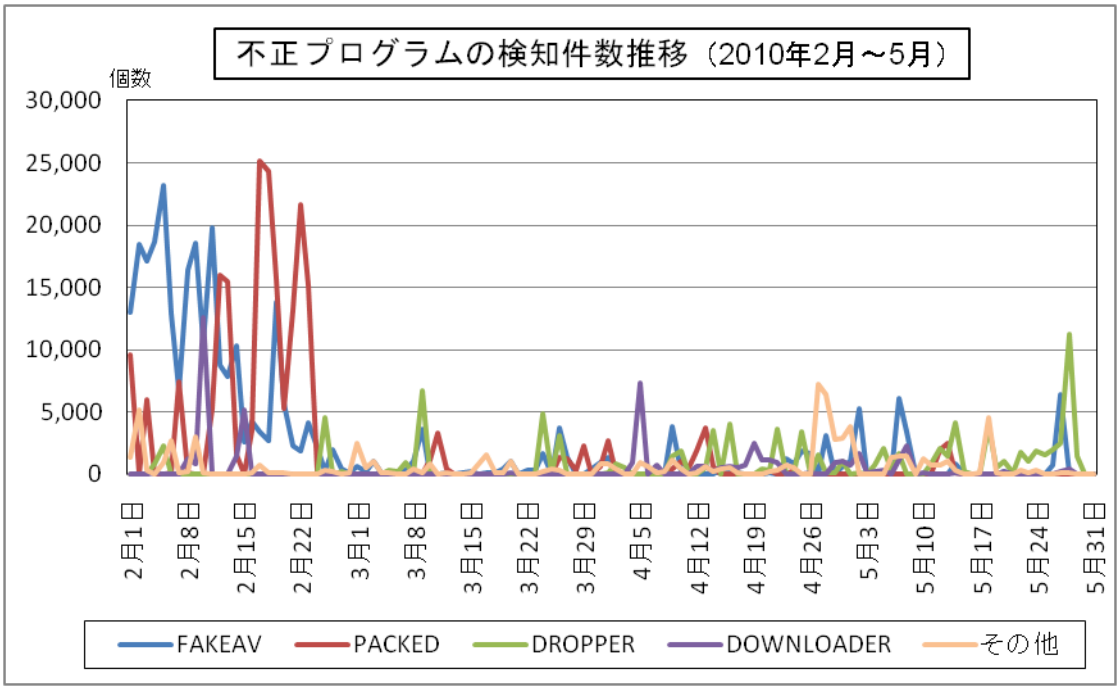


図 2-3：不正プログラムの検知件数推移

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

		12月	1月	2月	3月	4月	5月
届出(a) 計		9	20	27	19	11	8
	被害あり(b)	6	12	17	13	10	5
	被害なし(c)	3	8	10	6	1	3
相談(d) 計		22	67	47	60	39	52
	被害あり(e)	14	34	28	23	16	22
	被害なし(f)	8	33	19	37	23	30
合計(a+d)		31	87	74	79	50	60
	被害あり(b+e)	20	46	45	36	26	27
	被害なし(c+f)	11	41	29	43	24	33

（1）不正アクセス届出状況

5 月の届出件数は 8 件であり、そのうち何らかの被害のあったものは 5 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 52 件（うち 2 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 22 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 1 件、その他被害あり 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 2 件（全て不正なコードの挿入）、ウェブサーバ内に他サイトを攻撃するための不正プログラムを置かれ踏み台として悪用されていたものが 1 件、でした。侵入の原因は、詳細は追い切れていないが“ガンブラー”の手口だと推測されるものが 2 件、ID/パスワード管理不備（SSH※で使用するポートへのパスワードクラッキング※攻撃と思われる）が 1 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 1 件）でした。

※SSH (Secure Shell)：ネットワークを介して遠隔のコンピュータと通信するためのプロトコルの一つ。
※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。ブルートフォース攻撃(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）被害事例

［侵入］

（i）“ガンブラー”によるものと思われる被害

事例	・自社サイトを閲覧した顧客から、「ホームページを見ていたら、ウイルス警告が出た」と通報が入った。 ・ウェブサイトのコンテンツを調査したところ、HTML ソースに、悪意あるサイトへ誘導するためのスクリプトが挿入されていることが判明。 ・ウェブコンテンツ更新用の ftp アクセスのログを見ると、見知らぬ IP アドレスからのログインが成功していた。ftp アカウントは、社員用に発行されていたもの。なぜ ftp アカウント情報が漏れたのかは、現状では原因不明。 ・今後の対策として、ftp 接続を許可するアクセス元 IP アドレスに制限を加えることとした。
解説・対策	典型的なガンブラーの被害を防ぐための対策として、「**ftp アクセスの制限**」は有効です。その他、「**ftp アカウントのパスワード強化**」や「**ウェブサイト更新専用パソコンの導入**」も有効な対策です。 （参考） 2010 年 4 月の呼びかけ「ウェブサイトの管理方法を再確認しましょう！」 http://www.ipa.go.jp/security/txt/2010/04outline.html

［なりすまし］

（ii）無料オンラインゲームのアカウントが乗っ取られた

事例	・無料のゲームサイトに登録している。ある日、ログインしようとしたが、「パスワードが違います」となり、ログインできなかった。 ・ゲーム運営会社に問い合わせたところ、パスワードが変更されているとのこと。原因は分からない。 ・自分がゲームサイトに登録していた情報を基に、ゲーム運営会社側が、当該アカウントの元々の持ち主が自分であることを確認してくれた。しかし、パスワード再発行手数料として 1,000 円掛かるという。
解説・対策	どんな場面でも、ゲーム内で使うアイテムを狙っている輩がいることを忘れてはいけません。**パスワードを簡単なものに設定していると、この例のように自分のアカウントが乗っ取られてしまうことになってしまいます**。無料のサービスだからといっても、油断は禁物です。 （参考） IPA -「ID とパスワードを適切に管理しましょう」 http://www.ipa.go.jp/security/txt/2010/03outline.html

4. 相談受付状況

5 月のウイルス・不正アクセス関連相談総件数は **1,881 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 **637 件**（4 月：747 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 **27 件**（4 月：23 件）、**Winny に関連する相談**が **5 件**（4 月：11 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 **4 件**（4 月：4 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

	12月	1月	2月	3月	4月	5月
合計	1,794	2,150	1,789	2,000	2,110	1,881
自動応答システム	1,138	1,160	977	1,057	1,194	1,091
電話	602	910	736	846	835	714
電子メール	52	78	70	92	81	76
その他	2	2	6	5	0	0

※ 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。

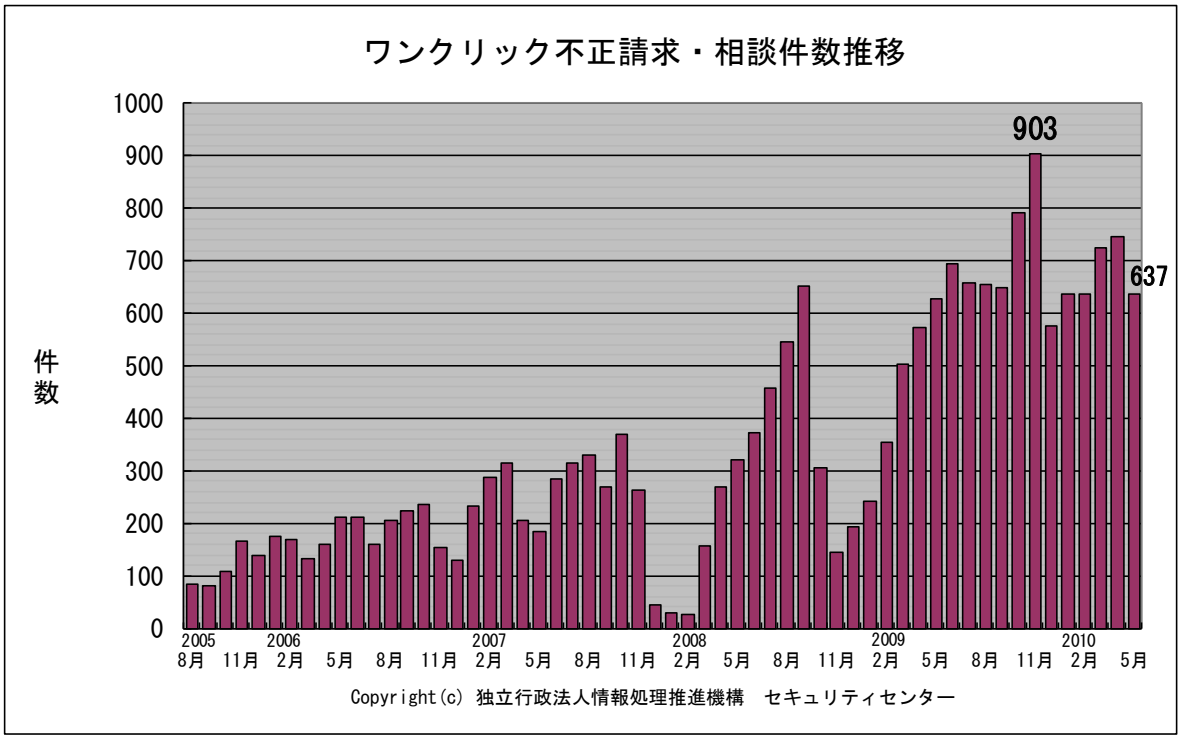


図 4-1：ワンクリック不正請求相談件数の推移

主な相談事例は以下の通りです。

（i）パソコンを知り合いに貸したら、アダルトサイトの請求画面が表示されて戻ってきた！

相談	パソコンを知り合いに数日間貸してあげたところ、アダルトサイトの請求画面が表示され、消えない状態で戻ってきた。このパソコンはどうしたらいい？
回答	パソコンを貸した相手は、アダルトサイトの閲覧中に、セキュリティの警告メッセージが表示されていたにもかかわらず、ワンクリック不正請求のウイルスを自ら取り込むという、危険な行為を平気で実行しています。**システムの復元機能を使って、パソコンを貸した日よりも前の日の状態まで戻すことをお勧めします。** 上記相談の場合、ワンクリック不正請求のウイルスだけの感染で済んでいますが、仮に**パソコン内のデータを漏えいするウイルスに感染していたら大変な被害**に結びつきます。特に、**漏れたら困る情報を扱っているパソコンであれば、他人に貸さない**のが一番です。 （参考） IPA - 【注意喚起】ワンクリック不正請求に関する相談急増！ http://www.ipa.go.jp/security/topics/alert20080909.html

（ii）自分のウェブサイトが改ざんされていないか確認したい

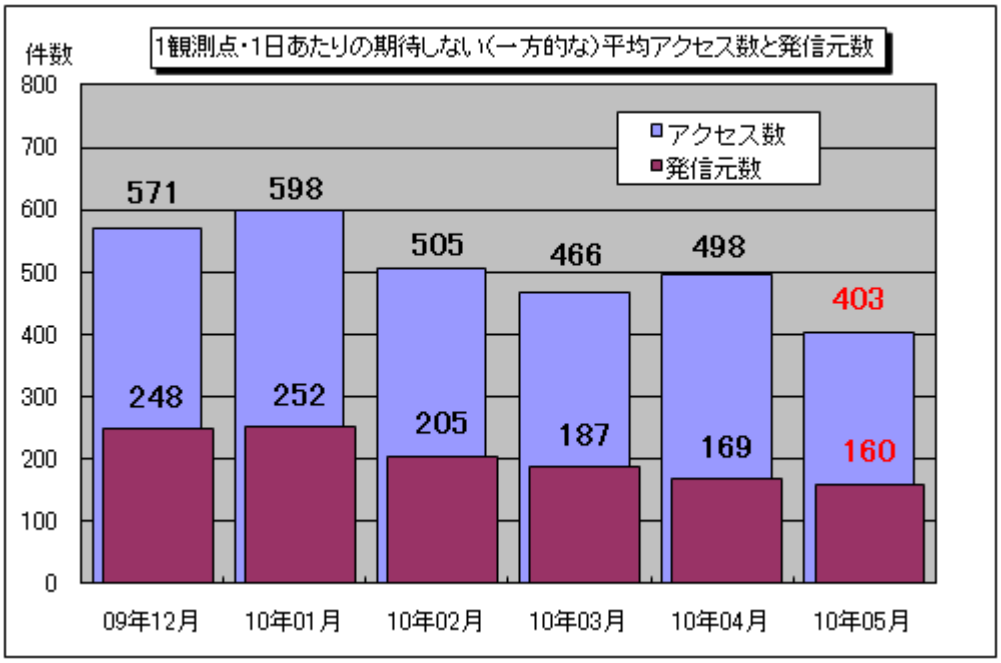
相談	顧客から、“貴社のウェブサイトが改ざんされているのではないか？”と指摘を受けた。ウェブサイトが改ざんされているか、簡単に調べられる方法はないか。
回答	改ざんされていないと確証の持てるウェブページファイルが手元にある場合、最新のウェブページファイルと比較することで調べられます。そうしたファイルがない場合、**ウェブサイトに置いてある全ページのファイルを手元のパソコンにコピーし、最新のウイルス定義ファイルでウイルススキャンをしてみましょう（できれば複数ソフトで）。**無料のオンラインスキャンでも良いでしょう。 改ざんされていると、ウイルスが検知される場合があります。しかし何も検知されなくても、改ざんされていないとは限りません。あくまでも簡易的な方法となります。**今後、確実な比較を行うためにも、安全を確認できたファイルは CD や DVD に書き込み、改ざんされない状態で手元に置くと良いでしょう。** （参考） IPA - ウェブサイト管理者へ：ウェブサイト改ざんに関する注意喚起 一般利用者へ：改ざんされたウェブサイトからのウイルス感染に関する注意喚起 http://www.ipa.go.jp/security/topics/20091224.html

5. インターネット定点観測での 5 月のアクセス状況

インターネット定点観測（TALOT2）によると、2010 年 5 月の期待しない（一方的な）アクセスの総数は 10 観測点で **125,020 件**、延べ発信元数 (※) は **49,574 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 160 の発信元から 403 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。



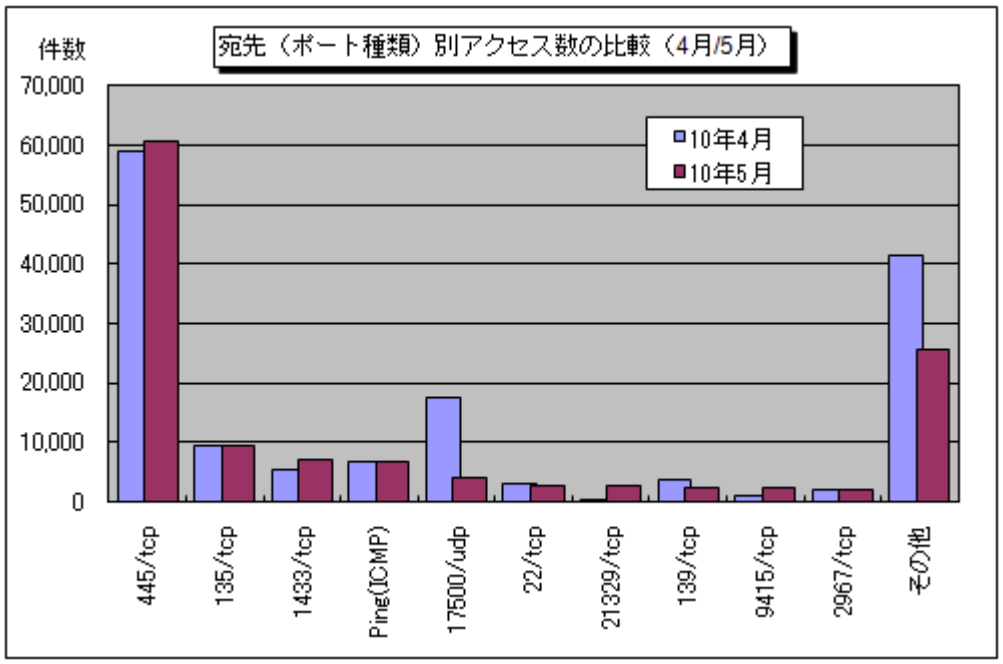
【図 5-1：1 観測点・1 日あたりの期待しない（一方的な）平均アクセス数と発信元数】

2009 年 12 月～2010 年 5 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。5 月の期待しない（一方的な）アクセスは、4 月と比べて減少しました。

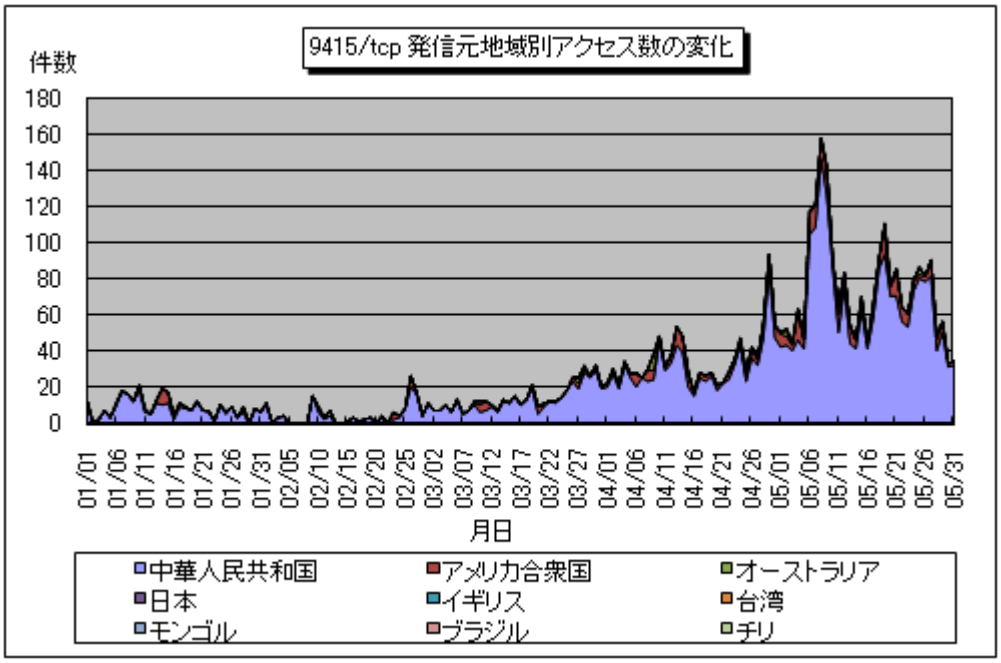
4 月と 5 月の宛先（ポート種類）別アクセス数の比較を図 5-2 に示します。これをみると、5 月はこれまであまり上位に挙がってこなかった 9415/tcp や、21329/tcp といったポートへのアクセスが上位にランクされました。これらのポートはいずれも、特定のアプリケーションで使用されるポートというわけではないため、このアクセスが何を目的としたものだったかは不明です。

9415/tcp に関しては、TALOT2 の複数の観測点に対して海外（主に中国）の複数の発信元からのアクセスの増加傾向が 3 月頃から継続していたといった特徴がありました（図 5-3 参照）。定点観測を行っている他の組織においても同様の増加傾向が観測されていたことから、広範囲に発生していたことが予想されるため、引き続き観測状況に注意する必要があります。

21329/tcp に関しては、5 月の中旬にアメリカ合衆国の 1 か所の発信元から TALOT2 の 1 つの観測点のみにアクセスの急増が観測されていました。



【図 5-2：宛先（ポート種類）別アクセス数の比較（4 月/5 月）】



【図 5-3：9415/tcp 発信元地域別アクセス数の変化】

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/2010/documents/TALOT2-1006.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