INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

第 10-15-182 号
2010 年 4 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 [2010 年 3 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 3 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

「 ウェブサイトの管理方法を再確認しましょう！ 」
― “ガンブラー”による被害はいまだに続いています ―

「ガンブラー」の手口によるウェブサイトの改ざんは依然として続いており、いまだに「某ウェブサイトを閲覧したらウイルス検知の警告が表示された」、「顧客からの通報で自社ウェブサイトの改ざんが発覚した」などの相談や届出が IPA へ寄せられています。また、攻撃者による改ざんの手法も様々に変化し、改ざんチェックを正確に実施することが困難になってきており、改ざん対策がますます重要になってきています。

ウェブサイト管理者は自身のウェブサイトの管理方法を再確認し、改ざん被害に遭わないために、ウェブサイトを適切に管理してください。

(1)「ガンブラー」の仕組みと最近の改ざん事例

「ガンブラー」とは、特定のウイルスを指すものではなく、攻撃者が複数の攻撃手段を併用し、多数のパソコンに様々なウイルスを感染させようとするために使う、一連の手口のことです。「ガンブラー」の仕組みについては、2010 年 2 月の呼びかけで詳しく解説していますので、そちらを参照ください。

（ご参考）
「 "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）
http://www.ipa.go.jp/security/txt/2010/02outline.html#5

最近 IPA の相談窓口に寄せられた、ウェブサイト改ざんに関する事例を次に示します。

【事例 1】

相談内容	外部から指摘されたウェブサイトの改ざん箇所を修正したのち、確認のため、再度そのウェブサイトにアクセスしたところ、まだウイルス検知の警告が表示された。
解説	そのウェブサイトを確認したところ、HTML ファイル(※1)には不審な点は見つからなかったが、HTML ファイルから呼び出される JavaScript ファイル(※2)が改ざんされていた。

【事例 2】

相談内容	自分のパソコンで、あるウェブサイトを閲覧したらウイルス検知の警告が表示された。別のウイルス対策ソフトが入ったパソコンでそのウェブサイトを閲覧したらウイルスは検知されなかった。
解説	IPA でそのウェブサイトを確認したところ、改ざんされている箇所が見つかった。そのページの HTML ファイルを、複数社のウイルス対策ソフトでチェックしたところ、その時点ではウイルスを検知するウイルス対策ソフトが少なかった。後日、再度同様のチェックをしたところ、前回より多くのウイルス対策ソフトでウイルスが検知された。

【事例 3】

相談内容	HTML ファイルが改ざんされていないかチェックしてくださいと言われても、どこが改ざんされているかよく分からない。
解説	以前は改ざん箇所に「/*GNU GPL*/」や「/*LGPL*/」などといった特定の文字列が含まれていないかチェックする方法を紹介していたが、最近ではそのような特徴的な文字列が含まれていることはあまり見かけず、文字列のチェックで改ざんの有無の確認が困難となってきている。このような場合、改ざんされる前のクリーンなファイルと、ウェブサーバ上のファイルとの差分をチェックする方法が有効である。

(※1) HTML（HyperText Markup Language）ファイル： ウェブページを記述するためのマークアップ言語である HTML で記述されたファイル。

(※2) JavaScript ファイル： ウェブページ上に動きや対話性を付加する目的で使用される JavaScript で記述されたファイル。

ガンブラーは攻撃者が改ざんの手法を様々に変化させて、ウェブサイト利用者をウイルスに感染させようとするため、これまでの方法では改ざんチェックを正確に実施することが困難になってきています。

このため、ウェブサイト管理者はガンブラーによる改ざん被害を未然に防ぐために、ウェブサイトをこれまで以上に適切に管理する必要があります。

（2）ウェブサイトの具体的な管理方法

本項ではウェブサイトの改ざん被害に遭わないための具体的な管理方法を紹介します。

▼改ざんを防ぐための管理方法

- ウェブサイトの更新等に使用する ftp(※3)のパスワードは、十分な長さと複雑さをもったものにする。また、そのパスワードは、ウェブサイトを更新する人のみが知るようにする。【パスワードの強化】
- ウェブサイトを更新できる場所を組織内のみに限定するよう、ネットワークやサーバの構成を見直す。もし、インターネット経由でウェブサイトを更新する必要がある場合でも、VPN(※4)を導入するなどして、更新できる場所を限定する。【アクセス制限】
- ウェブサイトを更新するための専用パソコンを導入する。このパソコンでは、ウイルスによる被害を防止するためにウェブの閲覧やメールの確認をせず、ウイルス対策ソフトを最新の状態にし、可能な限り脆弱性を解消しておく。【更新専用パソコンの導入】

(※3) ftp（File Transfer Protocol）：ネットワークでファイルを転送するためのプロトコル。

(※4)VPN（Virtual Private Network）：安全性の高い専用回線の代わりに公衆回線を用いて、LAN 同士などを接続するサービスや技術のこと。

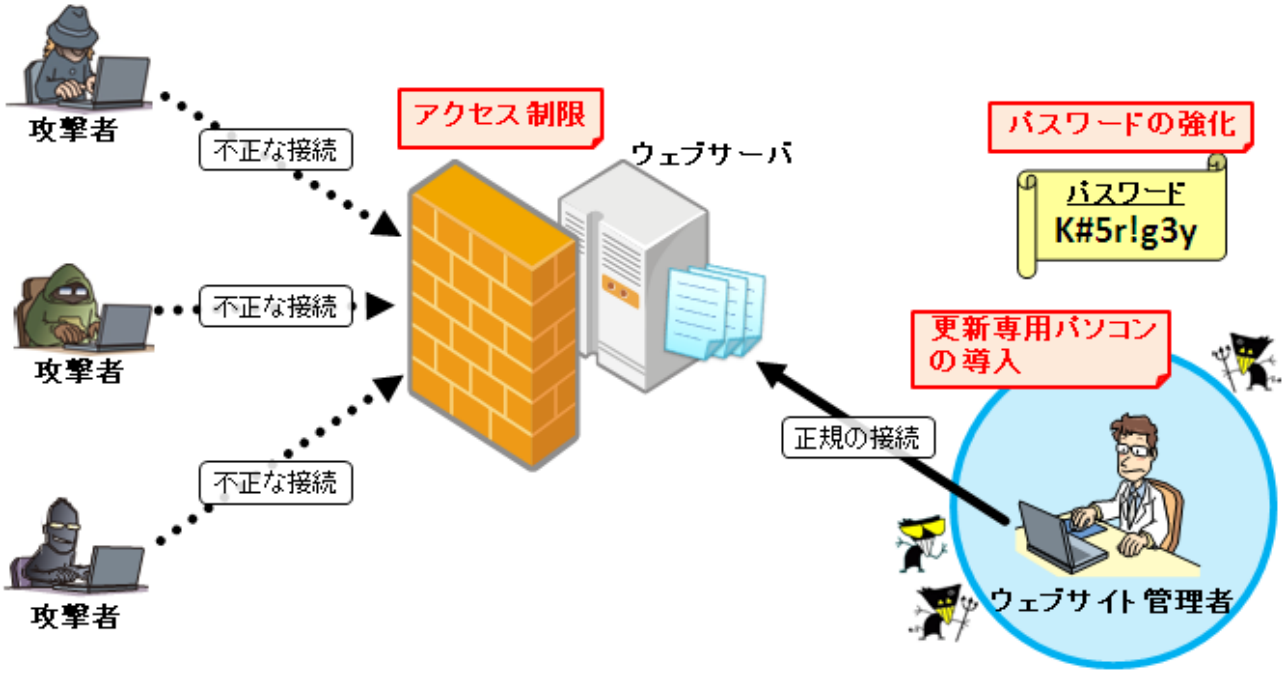


図 1-1：改ざんされないための管理方法例のイメージ図

▼改ざんに気付くための管理方法

改ざんされた状態が長くなればなるほど、利用者に被害が拡大する恐れがあります。もし改ざんされた場合でも、早期に改ざんに気付くことが出来れば、被害の拡大が防げます。一刻も早くウェブサイトの改ざんに気付くための管理方法を以下に示します。

- 最近では、（1）の【事例 3】にあるようにウェブサイトの HTML ファイルを見ただけでは改ざんの有無を確認することが困難になっています。この場合、あらかじめクリーンな状態のファイルを保管しておき、これとウェブサーバ上のファイルとを定期的に比較します。差分がないかチェックすることにより改ざんの有無が確認できます。このとき、大量にあるファイルの比較を一括で行えるようなソフトを利用することも有効です。
- ウェブサイトの更新等に使用する ftp のアクセスログを定期的にチェックすることにより、身に覚えのない接続などの不正なアクセスの有無が確認できます。

その他、費用はかかりますが、改ざんを早期に発見するためのウェブサイト改ざん検知サービスなどを利用することも一つの方法です。

また、本来はウェブサイト管理者がウェブサイトをチェックし、改ざん箇所を発見することが望まれますが、ウェブサイト利用者から指摘されることで、改ざんが発見される場合があります。このような場合を想定し、ウェブサイト上にメールアドレス等の連絡先を掲載しておくことを勧めます。

（3）ウェブサイト改ざんの被害発生時の対処

ウェブサイトが改ざんされてしまった場合、ウェブサイト管理者は被害者であると同時に、ウェブサイト利用者に対する加害者となってしまう可能性があります。被害の拡大を防ぐために、次に示すような対応が求められます。

▼まず初めに行うべきこと

まず初めに行うことは、早急にウェブサイトの公開を停止することです。同時に ftp のパスワードの変更も行ってください。このとき、これまでウェブサイトの管理に利用していたパソコンには、ftp のパスワードを盗聴するウイルスが感染している可能性があるため、別のパソコンから操作することを勧めます。

同時に、別のウェブサイトを立てるなどして、ウェブサイト利用者に対して調査状況の説明や、問い合わせ用窓口を設けるなど、随時情報提供に努めてください。

▼改ざん箇所の洗い出し等の調査

上記の対応を行ったのち、保管しておいたクリーンなファイルとウェブサーバ上のファイルの比較などの方法で、全ての改ざん箇所の洗い出しを行ってください。また、同じパソコンで管理しているウェブサイトが複数ある場合、他のウェブサイトにも改ざんが及んでいる可能性があるため、必ず全てのウェブサイトのファイルを確認してください。

また、改ざん期間等を把握するため、改ざん箇所ごとに ftp のアクセスログの確認などを行なって、被害状況等の調査を行ってください。

▼ウェブサイトを再公開する場合

上記の対応で全ての改ざん箇所の修正を行った上で、ウェブサイトの公開を再開する場合、必ずウェブサイト利用者への改ざんの事実の告知も掲載してください。ウェブサイト再開の際には、判明した範囲で、次に示す情報を告知することを勧めます。

- 改ざんの事実の説明
- 改ざんされていた箇所
- 改ざんされていた期間
- ウェブサイト利用者が改ざんされていた箇所を閲覧した場合に想定される被害（ウイルス感染など）の説明
- ウイルスのチェック方法の説明（必要に応じてオンラインスキャンサイトの紹介など）
- 問い合わせ用窓口の連絡先

参考として、セキュリティ関連の組織や企業が提供している、無料でウイルスチェックができるウェブサイトを紹介します。

（ご参考）
「ボットの駆除対策手順」（サイバークリーンセンター）
https://www.ccc.go.jp/flow/
「オンラインウイルススキャン」（カスペルスキー社）
http://www.kaspersky.co.jp/virusscanner/
「Symantec Security Check」（シマンテック社）
http://security.symantec.com/sscv6/home.asp?langid=jp
「オンラインスキャン」（トレンドマイクロ社）
http://www.trendflexsecurity.jp/housecall/
「マカフィー・フリースキャン」（マカフィー社）
http://www.mcafee.com/japan/mcafee/home/freescan.asp

ウェブサイト改ざんの被害に遭った際は、可能な限り IPA への届出を行ってください。届けられた情報は、個人や組織を特定できる情報を除いた上で分析および統計処理し、対策情報の発信のために活用します。

（ご参考）
「情報セキュリティに関する届出について」（IPA）
http://www.ipa.go.jp/security/todoke/

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、7 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
- 無線 LAN アクセスポイントに“ただ乗り”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、9 頁の「4.相談受付状況」を参照）
- ワンクリック不正請求に二度も引っ掛かってしまった
- 公共施設での個人パソコン利用について

○ インターネット定点観測（11 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

3 月のウイルスの検出数（※1）は、**約 5.8 万個**と、2 月の約 5.5 万個から 5.9%の増加となりました。また、3 月の届出件数（※2）は、**1,484 件**となり、2 月の 1,436 件から 3.3%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。
・3 月は、寄せられたウイルス検出数約 5.8 万個を集約した結果、1,484 件の届出件数となっています。

検出数の 1 位は、**W32/Netsky** で**約 3.9 万個**、2 位は **W32/Mumu** で**約 8 千個**、3 位は **W32/Mydoom** で**約 5 千個**でした。

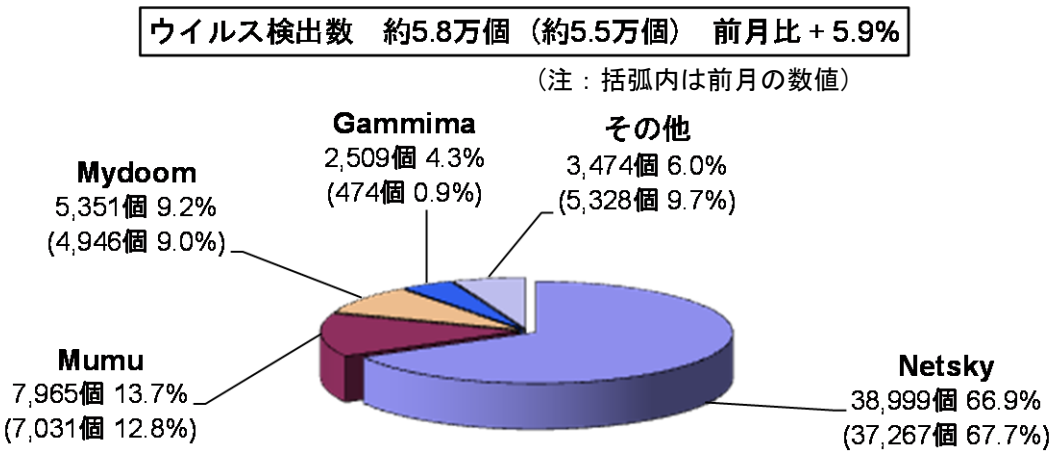


図 2-1：ウイルス検出数

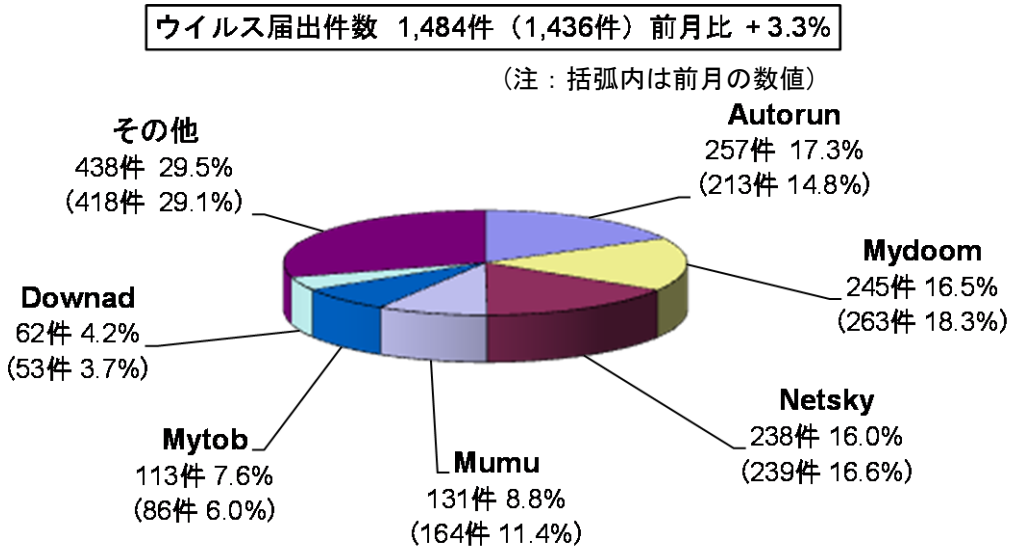


図 2-2：ウイルス届出件数

(2) 不正プログラムの検知状況

2010 年 2 月は、「偽セキュリティ対策ソフト」型ウイルス（FAKEAV）の検知件数が増加した状況が確認されましたが、3 月には大幅に減少しました（図 2-3 参照）。これらの不正プログラムは、ボットに感染したパソコンからメールの添付ファイルとして配布されるケースがあり、いつ急増するかわかりません。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。

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を実施するようにしてください。

（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/

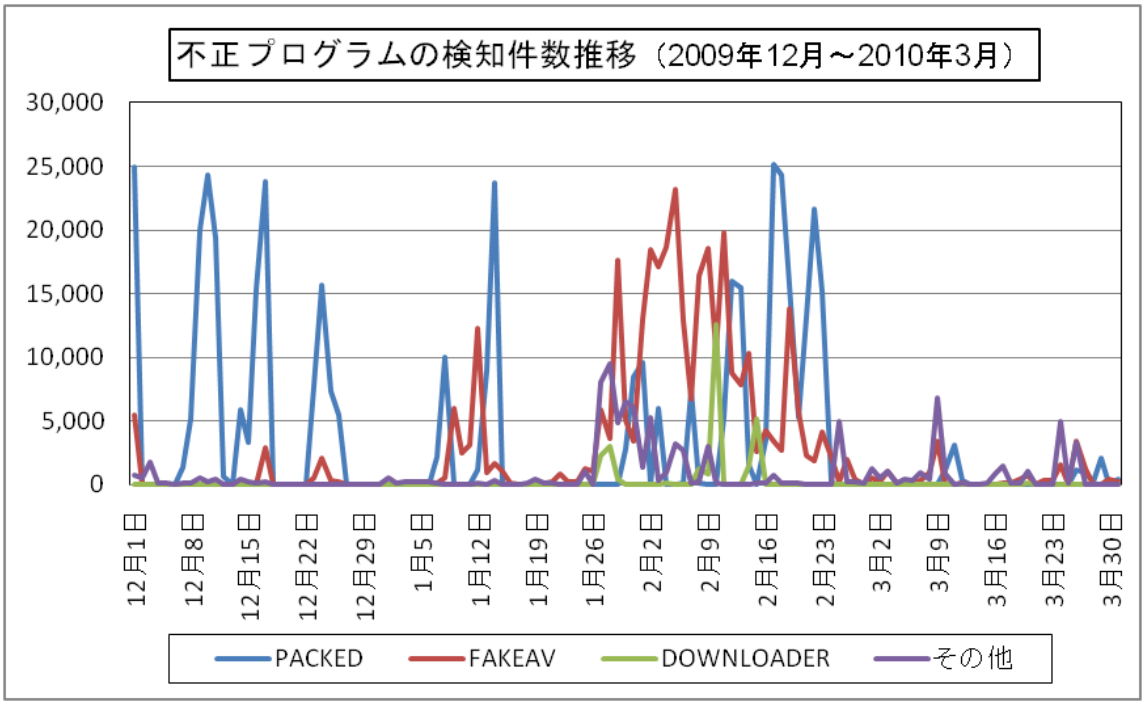


図 2-3：不正プログラムの検知件数推移

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

		10月	11月	12月	1月	2月	3月
届出(a) 計		**21**	**11**	**9**	**20**	**27**	**19**
	被害あり(b)	14	6	6	12	17	13
	被害なし(c)	7	5	3	8	10	6
相談(d) 計		**34**	**34**	**22**	**67**	**47**	**60**
	被害あり(e)	11	14	14	34	28	23
	被害なし(f)	23	20	8	33	19	37
合計(a+d)		**55**	**45**	**31**	**87**	**74**	**79**
	被害あり(b+e)	25	20	20	46	45	36
	被害なし(c+f)	30	25	11	41	29	43

（1）不正アクセス届出状況

3 月の届出件数は 19 件であり、そのうち何らかの被害のあったものは 13 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 60 件（うち 7 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 23 件でした。

（3）被害状況

被害届出の内訳は、**侵入 8 件、アドレス詐称 1 件、なりすまし 3 件、その他被害あり 1 件、**でした。

「侵入」の被害は、ウェブページに不正なコードを挿入されたものが 2 件、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 3 件、ウェブサーバ上に運営者が意図しないコンテンツを設置されていたものが 2 件（内 1 件はフィッシング※に悪用するためのコンテンツ）、メールアカウントを外部から勝手に使われて迷惑メール送信に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と思われるものが 1 件、ウェブアプリケーション（phpMyAdmin）の脆弱性を突かれたと思われるものが 1 件、設定不備が 1 件、などでした。

「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 2 件、無料ウェブメール 1 件）でした。

※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ウェブページを装い、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。

（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	・自分で開設しているホームページに自分でアクセスしたら、ウェブブラウザが「攻撃サイトとして報告されています！」と警告を出した。 ・ホームページのコンテンツファイルを置いてあるレンタルサーバ会社に問い合わせたら、「不正なコードを挿入されているようだ」との回答。 ・ホームページのコンテンツをメンテナンスするために使っている ftp アクセスのログを見ると、身に覚えのない IP アドレスからログインされていたことが判明。 ・挿入された「不正なコード」を削除したいが、HTML ファイルの中身を見ても良く分からない。
解説・対策	症状から判断すると、ガンブラーによる被害と推定されます。当該サイトを閲覧した際にウイルスが検知されたなど、異常に直面した利用者が通報したために、警告が出るようになった可能性があります。**改ざん箇所を特定するのが難しい場合、復旧するには、まずはサーバ上のホームページコンテンツファイルを全て削除した上で、お手元のパソコンに保存してある、改ざん前のホームページのコンテンツファイルを改めてアップロードするのが良い**でしょう。今後は、**改ざんを防ぐことはもちろん、改ざんに早く気付く方法や、改ざん発覚後の対処も重要**になります。次の情報を参考にしてください。 （参考） IPA - 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

［その他（被害あり）］

（ii）無線 LAN アクセスポイントに“ただ乗り”された

事例	・自宅で無線 LAN を使っている。WEP という暗号化方式はセキュリティ強度に問題があるらしいことは知っていたが、携帯型ゲーム機が WEP にしか対応していないため、仕方なく WEP 方式で運用していた。 ・ある日、オンラインゲームをプレイしていた際、急にサーバとの接続が切れるなど、不安定な状態に陥った。 ・ルータのログを確認したところ、身に覚えのない 4 台の端末がつながっていることが判明。通信の帯域幅をほとんど占有していたと思われる。 ・危険を感じたため、とりあえず暗号化方式を WPA2-PSK（AES）に変更した。
解説・対策	**WEP にはいくつかの欠点が見つかっているため、現状では使用することを推奨しません**。暗号化方式の設定は、まず初めに親機の設定をしてから、次に子機側の設定を親機に合わせる、という手順となります。親機側に「WPA2-PSK（AES）」もしくは「WPA-PSK（AES）」の項目が無い場合は、WPA2 対応の無線 LAN 機器を新たに導入することをお勧めします。 なお、**親機によっては AES、TKIP、WEP の 3 つのセキュリティ方式の混在利用時でも相応のセキュリティ強度を保てる製品もありますので、まずは無線 LAN 機器メーカに問い合わせてみましょう**。 （参考） IPA - 一般家庭における無線 LAN のセキュリティに関する注意 http://www.ipa.go.jp/security/ciadr/wirelesslan.html

4. 相談受付状況

3 月のウイルス・不正アクセス関連相談総件数は **2,000 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 **725 件**（2 月：637 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 **12 件**（2 月：26 件）、**Winny に関連する相談**が **8 件**（2 月：1 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**（2 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

	10月	11月	12月	1月	2月	3月
合計	2,049	2,315	1,794	2,150	1,789	2,000
自動応答システム	1,157	1,340	1,138	1,160	977	1,057
電話	843	918	602	910	736	846
電子メール	45	53	52	78	70	92
その他	4	4	2	2	6	5

※ 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。

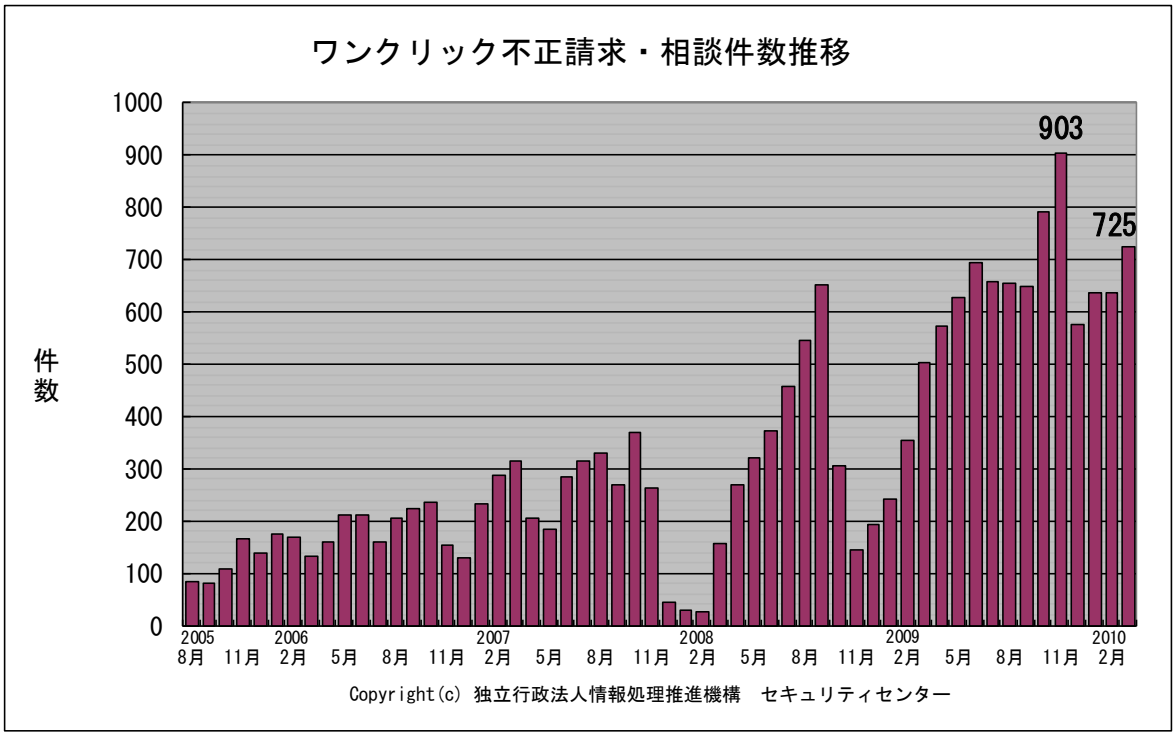


図 4-1：ワンクリック不正請求相談件数の推移

主な相談事例は以下の通りです。

（i）ワンクリック不正請求に二度も引っ掛かってしまった

相談	以前、アダルトサイトを見たことで請求書が定期的に出現するようになったため、IPA に相談して元の状態に復旧してもらった。 最近、別のアダルトサイトを見ていて、また請求書が定期的に出て来るようになった。今度は、以前と違う画面。また教えてもらえますか。
回答	**請求書が出現するのは、ウイルスに感染しているため**です。**ウイルスは勝手に入って来た訳ではなく、アダルトサイトを見ている際に、自分でダウンロードして自分で開いている**のです。**業者の手口を理解しない限り、いつまで経っても再度同じ被害に遭う**でしょう。次のページを参考にして、同じ手に何度も騙されないようにしましょう。 （ご参考） IPA -【注意喚起】ワンクリック不正請求に関する相談急増！ パソコン利用者にとっての対策は、まずは手口を知ることから！ http://www.ipa.go.jp/security/topics/alert20080909.html

（ii）公共施設での個人パソコン利用について

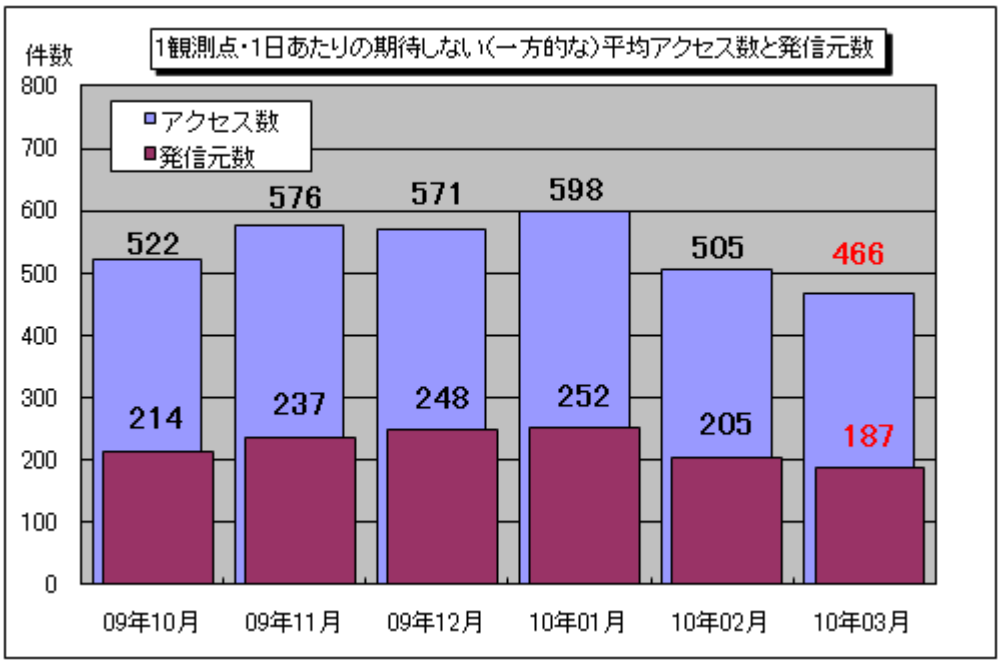
相談	当施設では、利用者サービスの一環としてパソコンを設置し、利用者自身でインターネット検索ができるようなコーナーを設けています。最近、利用者が、自分で持ち込んだ個人パソコンを施設の許可なく LAN に接続して、ネットサーフィンなどをしているようです。このような行為は想定外であって、どう扱えばよいか、悩んでいます。
回答	利用者が持ち込んだパソコンは、当然、施設の管理が行き届かないものです。ウイルスに感染していたとしても、把握し切れません。仮に、**利用者が持ち込んだパソコンにウイルスが感染していた場合、勝手に施設の LAN に接続されると、LAN に接続されている他のパソコンもウイルスに感染してしまう可能性があります**。さらに、外部から LAN 内に潜伏したウイルスを介して侵入されたりする可能性があります。このような脅威があるため、もし**外部からの持ち込みパソコンの接続を許可するのであれば、他のネットワークに影響が無い、独立したネットワークを用意することが望ましい**と考えます。

5. インターネット定点観測での 3 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 3 月の期待しない（一方的な）アクセスの総数は 10 観測点で **144,590 件**、延べ発信元数（※）は **57,950 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 187 の発信元から 466 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。

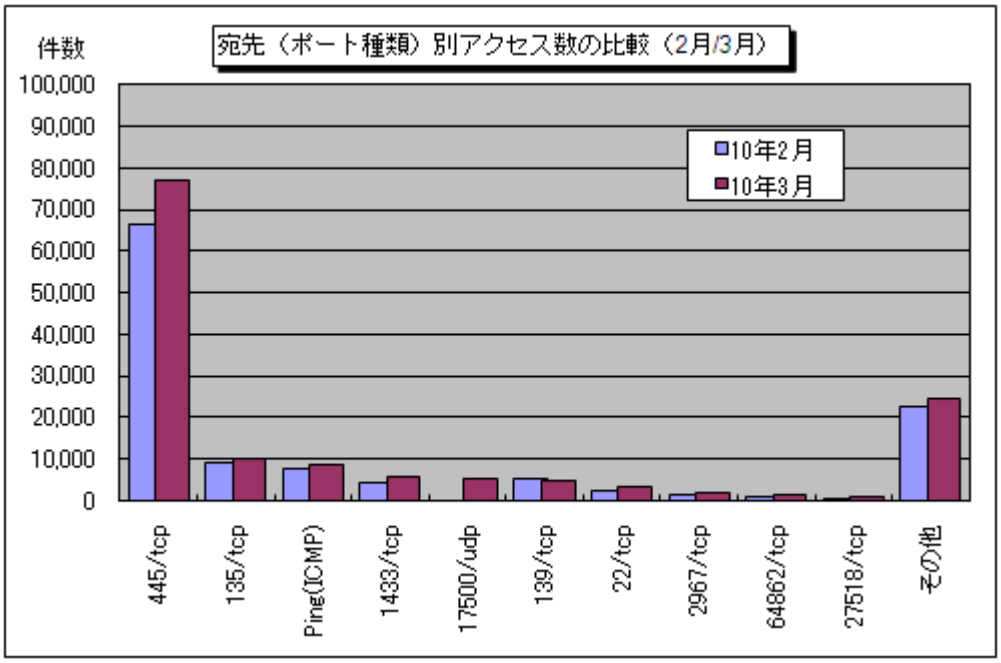
TALOT2 における各観測点の環境は、インターネットを利用される一般的な接続環境と同一なので、インターネットを利用される皆さんの環境へも同じくらいの一方的なアクセスがあると考えられます。



【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 10 月～2010 年 3 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。3 月の期待しない（一方的な）アクセスは、2 月と比べて減少しました。

2 月と 3 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、3 月はこれまであまり観測されていなかった 17500/udp、64862/tcp、27518/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く、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。これらのアクセスはいずれも、特定の 1 観測点でしか観測されていませんでしたが、1 つの発信元からというわけではなく、例えば 27518/tcp の場合、3 月だけで 350 箇所以上の発信元からのアクセス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（2 月/3 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/2010/documents/TALOT2-1004.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