INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

第 10-11-179 号
2010 年 3 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 2 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 2 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

「 ID とパスワードを適切に管理しましょう 」
― サイフと同じく大切に！ ―

オンラインサービスにおける ID とパスワードを不正利用されたことが原因と考えられる金銭的な被害が相次いで報道されており、IPA へも相談が寄せられています。ID とパスワードを不正利用されてしまった事例には、単純なパスワードを推測されてしまったものやウイルスに感染したことが原因と考えられるものなどがありますが、中には原因が特定できないケースもあります。

本人確認のために用いられる ID とパスワードは、オンラインサービスを利用する上で非常に重要なものです。不正利用対策として、パスワードを強化して破られにくくするとともに、適切に管理することが必要です。

オンラインサービスで利用する ID とパスワードは、それを悪用しようとしている者に常に狙われていることを意識し、適切に管理しましょう。

（1）不正利用された原因

報道事例や IPA への相談事例で確認されている、オンラインサービスを不正利用されたケースにおいて、その原因として推測されるものは次のとおりです。

- 単純なパスワードを設定していたため、悪意ある者に推測されたり、総当り攻撃により破られた。
- ウイルス感染により、ID とパスワードを盗まれた。
- フィッシング詐欺 (※1) に引っ掛かり、ID とパスワードを盗まれた。
- ソーシャルエンジニアリング (※2) により、ID とパスワードを盗まれた。

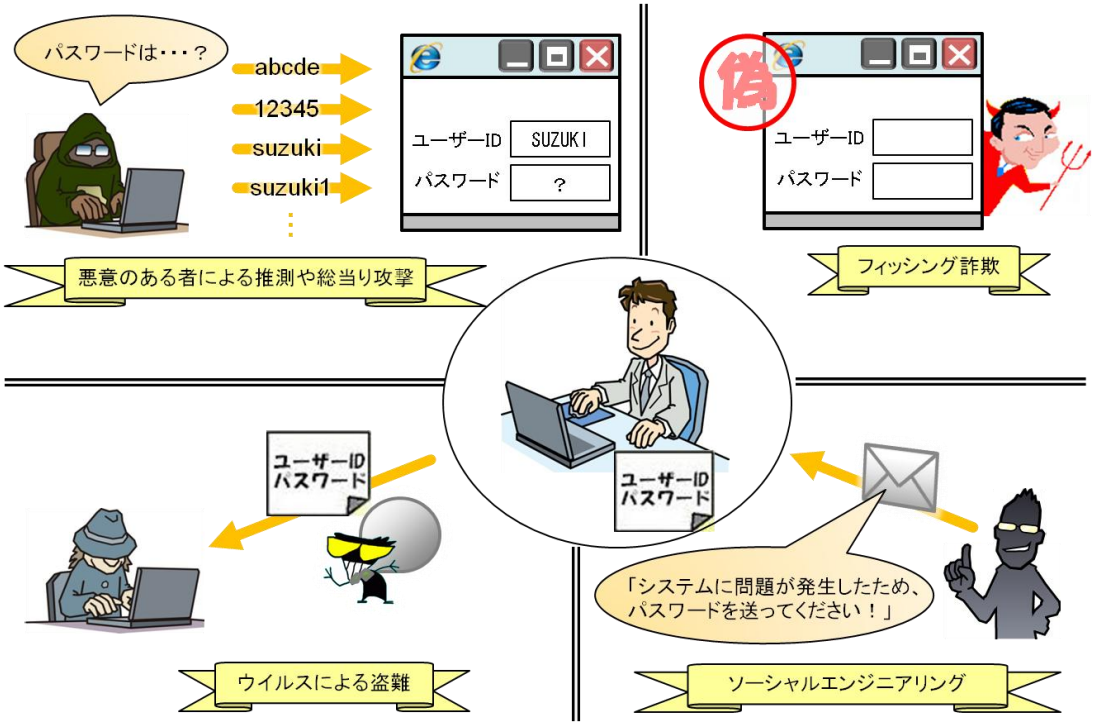


図 1-1：ID とパスワードを盗まれるイメージ図

このように、様々な原因が考えられますが、多くは自分自身が注意することで防ぐことができます。以降の項目を確認し、ID とパスワードを適切に管理してください。

※1 フィッシング（phishing）：巧妙な文面のメールなどを用い、実在する企業（金融機関、信販会社、ネットオークション等）の Web サイトを装った偽のサイトにユーザを誘導し、情報（パスワードなど）を盗みとる不正行為。
※2 ソーシャルエンジニアリング（social engineering）：ネットワーク技術やコンピュータ技術を用いずに、人間心理や社会の盲点を突いて、情報（パスワードなど）を入手する方法。

（2）パスワード認証の落とし穴

ID とパスワードのみの本人確認は、完璧な仕組みではなく、破られるリスクがあります。例えば、ID が連番で付与されるケースや、メールアドレスがそのまま ID になっているケースなど、ID は簡単に知られてしまう可能性が高く、その場合、攻撃者はパスワードが一致するかどうかを試すだけでよいことになります。このとき、パスワードを数字だけといった単純な設定にしていたり、管理に問題があったりすると、簡単に認証を突破されてしまう可能性が高くなります。

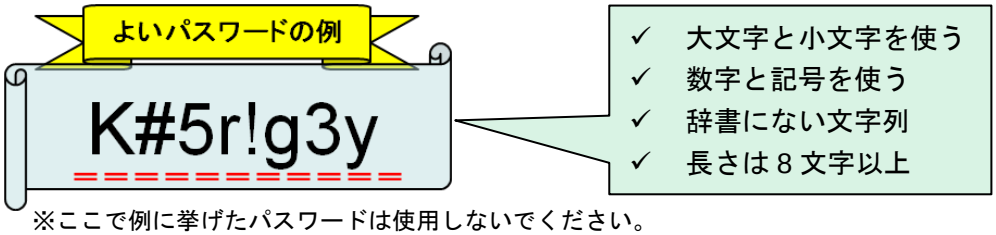
次項では、パスワード作成における注意点や運用・管理方法について紹介します。

（3）不正利用対策

ここでは（1）の不正利用された原因として推測されるものへの対策を紹介します。

- 破られにくいパスワードを作成する。

  パスワードを作成する場合は、名前や辞書に載っているような単語を避け、英字（大文字、小文字）・数字・記号など使用できる文字種全てを組み合わせて、かつ 8 文字以上にすることを心掛けましょう。辞書に載っている単語では、辞書攻撃（※3）という方法で簡単に破られてしまう可能性があります。



※ここで例に挙げたパスワードは使用しないでください。

※3 辞書攻撃（dictionary attack）：パスワードの割り出しや暗号の解読に使われる攻撃手法の 1 つで、辞書にある単語を片端から入力して試すという手法。

  また、破られにくいパスワードを作成したあとは、その運用について以下の項目にも注意してください。

  - 同じパスワードを使い回さない。パスワードは定期的に変更する。

    複数のオンラインサービスを利用している場合、同じパスワードを使い回していると、盗まれたときに被害が拡大するリスクが高まります。被害が複数のサービスに拡大することを防ぐために、それぞれ違うパスワードを設定するようにしましょう。

    また、破られにくいパスワードを使っていても、長期間変更せずにいると漏えいする危険性が高まります。パスワードは、定期的に（例えば月毎）変更するようにしましょう。

  - インターネットカフェなど、自分の管理下にない、不特定多数の人が利用するパソコンでは、パスワードを入力しない。

    破られにくいパスワードを設定していても、そのパソコンにパスワードを盗むウイルスが仕掛けられていたら簡単に盗まれてしまいます。自分の管理下にないパソコンでは、ID とパスワードを必要とするオンラインサービスの利用は避けるようにしてください。

- ウイルス対策ソフトを導入し、ウイルス感染を防ぐ。

  オンラインバンキングやオンラインゲームといった特定のサービスへのログインを監視して、

ID とパスワードを盗むウイルスがあります。また、Internet Explorer などのブラウザには、ID とパスワードを保存する機能がありますが、保存された情報を盗むウイルスも確認されています。

このようなウイルスに感染して情報を盗まれないために、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ようにしてください。また、盗まれるリスクを減らすため、ブラウザにはパスワードを保存しないようにしましょう。

- フィッシング詐欺やソーシャルエンジニアリングに騙されない。

  フィッシング詐欺やソーシャルエンジニアリングは、利用者を騙して ID とパスワードを入手しようとする手口です。パスワードは、本人しか知らないという前提のもと、本人確認に利用されるものです。たとえオンラインサービス提供会社やシステム管理者であっても、パスワードを聞いてくることはありません。メールや電話で、「システムに問題が発生したため、パスワードを送ってください」など、もっともらしい口実の問い合わせがあったとしても、パスワードを他人に教えてはいけません。

（4）オンラインサービス事業者が提供しているサービスの活用

（3）で記載した対策以外にも、ID・パスワードの不正利用対策が、利用しているオンラインサービスで提供されていることがあります。このようなサービスを活用することで、より安心してオンラインサービスを利用することが可能となります。

- ログイン履歴が確認できるサービスでは、定期的に自分以外の利用がないか確認する。

  利用しているサービスにより異なりますが、ログインすると、過去のログイン履歴を確認できる場合があります。自分がログインした覚えのない記録があるなど、不正利用に早く気がつけば、被害の拡大を防ぐことができます。定期的にログイン履歴を確認し、不審な記録があれば、直ちにオンラインサービスの相談窓口に連絡し、アカウントの利用停止の手続きなどを依頼してください。

- 不正ログインに、本人が気付くことができるサービスを利用する。

  オンラインサービスの中には、ログインしたタイミングでお知らせメールを送信する機能が提供されていることがあります。自分以外の誰かがログインした際に、お知らせメールが届けば、不正ログインに早く気付くことができ、被害を未然に防ぐことができます。

- ワンタイムパスワードのサービスを利用する。

  オンラインバンキングなどでは、その時だけ有効なパスワードを発行する「ワンタイムパスワード」というサービスを提供していることがあります。ID やパスワードを盗むウイルスに感染していても、一度きりのパスワードのため、仮に盗まれてもその後悪用されるリスクはありません。

（5）被害に遭ってしまったら

上述したように、ID・パスワードの不正利用対策は、手間がかかるという側面がありますが、被害が拡大することを防ぐためには、それぞれが有効な手段となりますので、実施するようにしてください。

なお、これまでに紹介した対策を実施していても、オンラインサービス事業者に問題があり、そこから情報が漏えいするといった、予期せぬ原因で被害に遭う可能性はゼロではありません。さらに、オンラインサービスの中には、クレジットカード情報を保存し、購入手続きを簡素化できる機能を提供しているケースがありますが、ID とパスワードが不正利用された場合、金銭的被害に直結する恐れがあります。

例えば、オンラインサービスに登録してあるクレジットカードの明細書に身に覚えのない請求があるなど、不正利用の被害に遭ってしまったら、直ちにクレジットカード会社とオンラインサービス事業者に不当な請求であることを報告し、対応を求める事をお勧めします。また、このとき消費生活センター

に相談することも有効です。

（ご参考）
全国の消費生活センター等
http://www.kokusen.go.jp/map/

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）
・“ガンブラー”被害から復旧したが、再度被害に遭った
・SQL インジェクション攻撃でクレジットカード情報などを盗まれた
○ 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）
・道で拾った USB メモリをパソコンに挿してしまった
・ファイル共有ソフトを使っていたら、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－

（1）ウイルス届出状況

2 月のウイルスの検出数（※1）は、**約 5.5 万個**と、1 月の約 7.2 万個から 23.8%の減少となりました。また、2 月の届出件数（※2）は、**1,436 件**となり、1 月の 1,154 件から 24.4%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。
・2 月は、寄せられたウイルス検出数約 5.5 万個を集約した結果、1,436 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/Mumu** で**約 7 千個**、3 位は **W32/Mydoom** で**約 5 千個**でした。

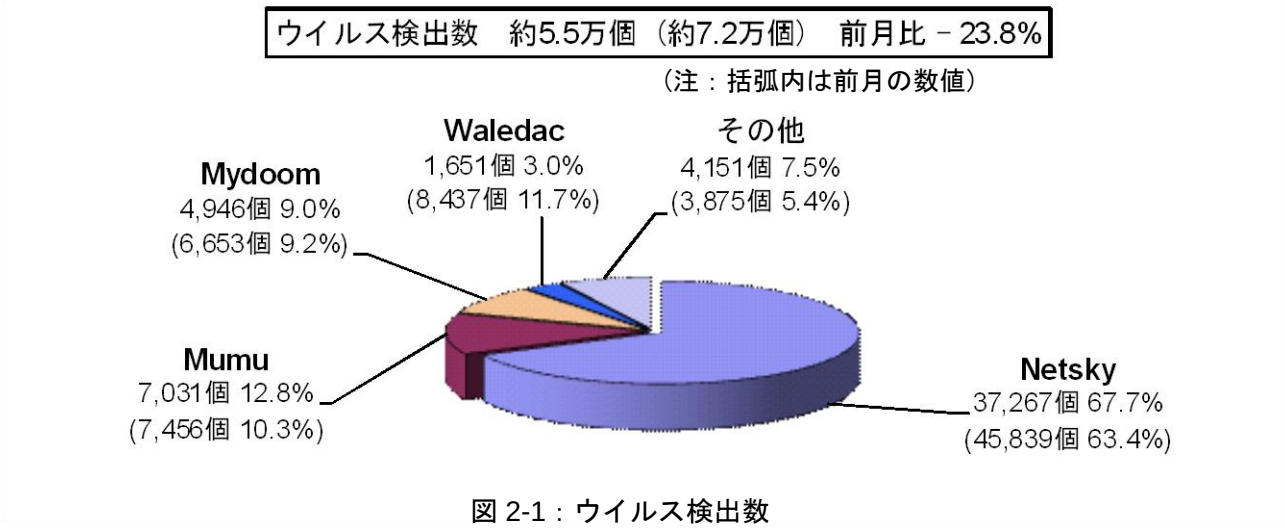


図 2-1：ウイルス検出数

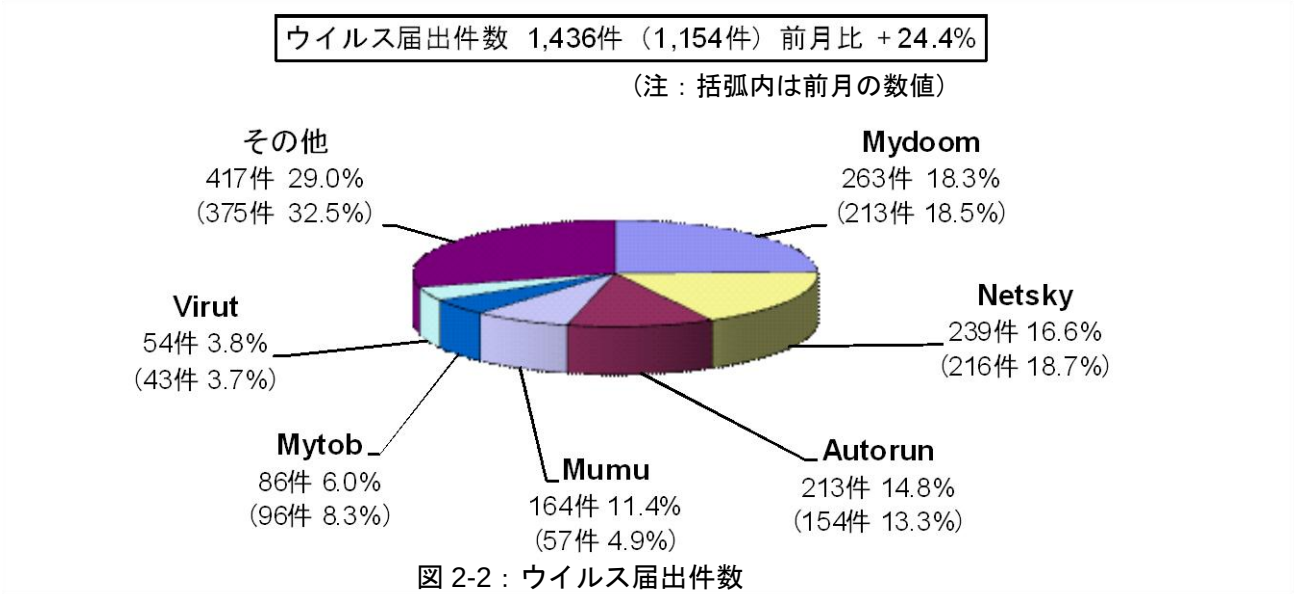


図 2-2：ウイルス届出件数

（2）不正プログラムの検知状況

「偽セキュリティ対策ソフト」型ウイルス（FAKEAV）の検知件数推移をみると、2009 年 11 月中旬以降は減少していましたが、2010 年 1 月下旬より、急増した様子が確認できます（図 2-3 参照）。

今後も、このような不正プログラムの検知件数はいつ急増するかわかりませんので、メールの添付ファイルには継続して注意を払うようにしてください。

なお、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/

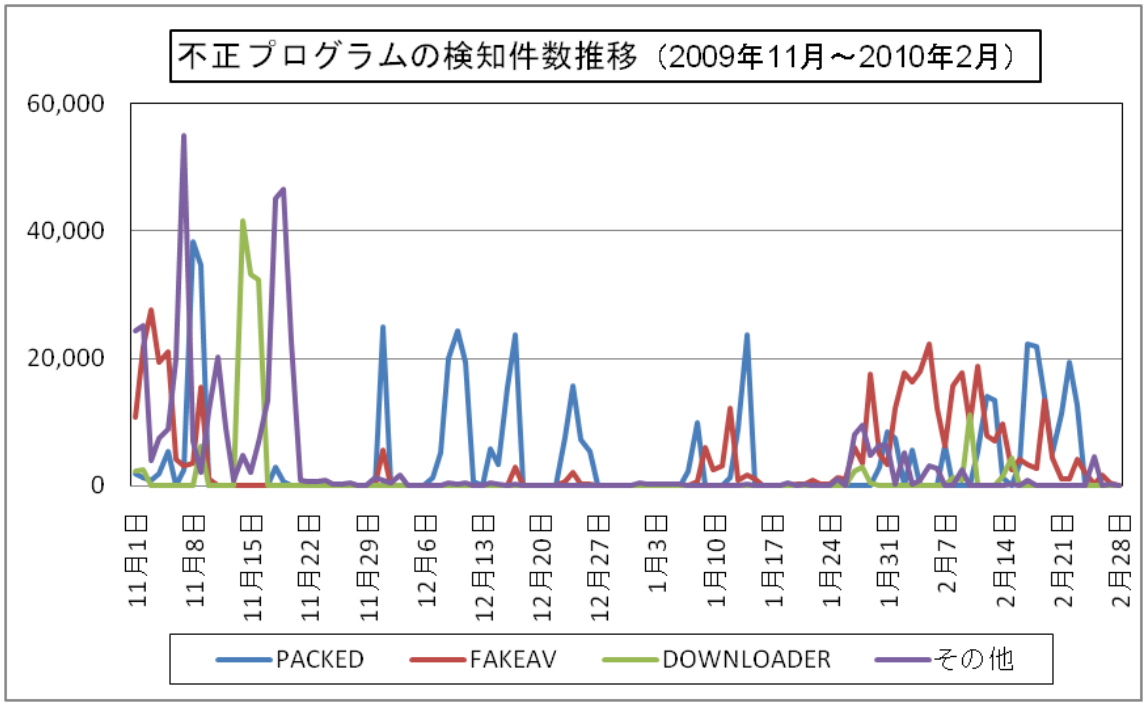


図 2-3：不正プログラムの検知件数推移

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

		9月	10月	11月	12月	1月	2月
届出(a) 計		11	21	11	9	20	27
	被害あり(b)	8	14	6	6	12	17
	被害なし(c)	3	7	5	3	8	10
相談(d) 計		44	34	34	22	67	47
	被害あり(e)	13	11	14	14	34	28
	被害なし(f)	31	23	20	8	33	19
合計(a+d)		55	55	45	31	87	74
	被害あり(b+e)	21	25	20	20	46	45
	被害なし(c+f)	34	30	25	11	41	29

（1）不正アクセス届出状況

2 月の届出件数は 27 件であり、そのうち何らかの被害のあったものは 17 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 47 件（うち 11 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 28 件でした。

（3）被害状況

被害届出の内訳は、**侵入 6 件、DoS 攻撃 2 件、なりすまし 7 件、不正プログラム埋め込み 2 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 3 件、ウェブサーバ内に他サイトを攻撃もしくは探索するための不正プログラムを置かれていたものが 2 件、SQL※インジェクション※攻撃を受けてウェブサーバ内のクレジットカード情報などを盗まれたものが 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 3 件、ID/パスワード管理不備と思われるものが 2 件、ウェブアプリケーションの脆弱性を突かれたものが 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 3 件、ブログサイト 2 件など）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）“ガンブラー”被害から復旧したが、再度被害に遭った

事例	・外部の顧客から、「そちらのウェブサイトを閲覧したらウイルス検知した」との連絡を受けた。 ・調査したところ、ウェブページ内に、悪意あるサイトへ誘導するためのスクリプトが埋め込まれているのを発見。“ガンブラー”による被害と思われた。 ・ftp アカウントのパスワードを変更するとともに、ウェブサイト上の全データを一旦削除し、手元にあるクリーンなデータをアップロードして復旧。 ・数日後、外部の顧客から、再びウェブサイト閲覧時にウイルス検知するとの連絡を受けたので、ウェブサイトを一時閉鎖。 ・原因となったマシンが特定できず、さらに社内でウイルスは見つかっておらず、原因が分からないまま、ウェブサイトを再開できないでいる。
解説・対策	ウェブページ更新用パソコンに、**ftp アカウント情報を盗むウイルスが感染していたため、変更したパスワードもすぐに漏えいしていた可能性が高い**です。原因が分からない場合は、ウェブページ更新用パソコンは一度初期化した方が良いでしょう。さらに、**ウェブページ更新用のパソコンでは、ウイルス感染のリスクを減らすために、ウェブ閲覧やメール確認をしないというルールを定めるのも、有効**です。 （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 http://www.ipa.go.jp/security/topics/20091224.html

（ii）SQL インジェクション攻撃でクレジットカード情報などを盗まれた

事例	・オンラインショッピングサイトを運営。クレジットカード会社から、カード情報漏えいの可能性を指摘されたため、セキュリティ業者に調査を依頼。 ・調査の結果、SQL インジェクション攻撃によりクレジットカード情報が 1 万件以上奪取されていたことが判明。 ・SQL インジェクション攻撃対策は実施していたが、実際は対策漏れがあったことが分かった。
解説・対策	攻撃手法は、日々進化しています。ウェブサイトの脆弱性検査は、定期的に実施することをお勧めします。 ウェブサイトを保護する運用面での方策の一つとして、WAF（Web Application Firewall）の導入も検討してみてはいかがでしょうか。 （参考） IPA - Web Application Firewall 読本 http://www.ipa.go.jp/security/vuln/waf.html

4. 相談受付状況

2 月のウイルス・不正アクセス関連相談総件数は **1,789 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**（1 月：638 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 **26 件**（1 月：37 件）、**Winny に関連する相談**が **1 件**（1 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 **0 件**（1 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

	9月	10月	11月	12月	1月	2月
合計	1,653	2,049	2,315	1,794	2,150	1,789
自動応答システム	915	1,157	1,340	1,138	1,160	977
電話	676	843	918	602	910	736
電子メール	60	45	53	52	78	70
その他	2	4	4	2	2	6

※ 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。

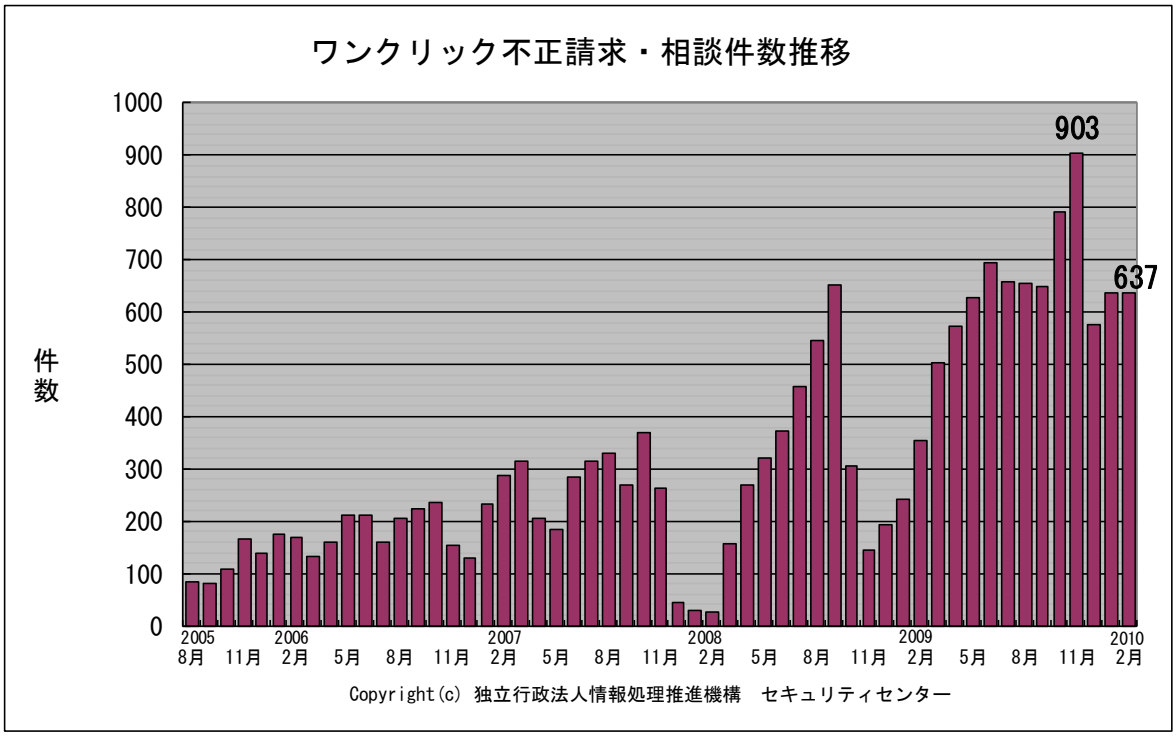


図 4-1：ワンクリック不正請求相談件数の推移

主な相談事例は以下の通りです。

（i）道で拾った USB メモリをパソコンに挿してしまった

相談	道を歩いていて、USB メモリを拾った。帰宅して、自分のパソコンに挿してみたが、中身が何も見えなかった。その後もパソコンには目に見える変化は無いが、ウイルスに感染していないだろうかと、心配。ウイルス対策ソフトは古いものを更新せず使っていた。USB メモリは、後日、交番に届けた。
回答	USB メモリ内に“USB メモリ感染型ウイルス”が入っていた場合、パソコンに挿すだけでウイルス感染してしまうかもしれません。**目に見える症状が無くても、ウイルスに感染している可能性はあるので、本当に心配であれば初期化した方が良いかも**しれません。 今後は、ウイルス対策ソフトを常に最新の状態にしておくことと、**出所の不明なファイルは自分のパソコンには入れない**ことは、ウイルス対策の基本として遵守しましょう。 （ご参考） IPA - 対策のしおりシリーズ http://www.ipa.go.jp/security/antivirus/shiori.html

（ii）ファイル共有ソフトを使っていたら、ウイルス感染？

相談	Cabos というファイル共有ソフトで音楽データをダウンロードしている。ある日パソコンを起動すると、「Control Center」というソフトが立ちあがった。英語で「ウイルスに感染している。駆除するためには有償版製品が必要」という主旨のことが書いてあり、クレジットカード番号を入れるよう促された。 ※この他にも、Cabos 利用者で同様の症状になったという相談が 3 件あり。
回答	**「Control Center」は、「偽セキュリティ対策ソフト」型のウイルス**です。**感染後は復旧作業を邪魔されることもあり、初期化するしかない場合もある**ようです。 Cabos でダウンロードしたファイルの中に、ウイルスが混ざっていた可能性が高いと言えます。**Cabos でダウンロードできるファイルは出所の不明なファイルですから、ウイルスに感染したくなければ、Cabos のようなファイル共有ソフトを使わないに越したことはありません。**

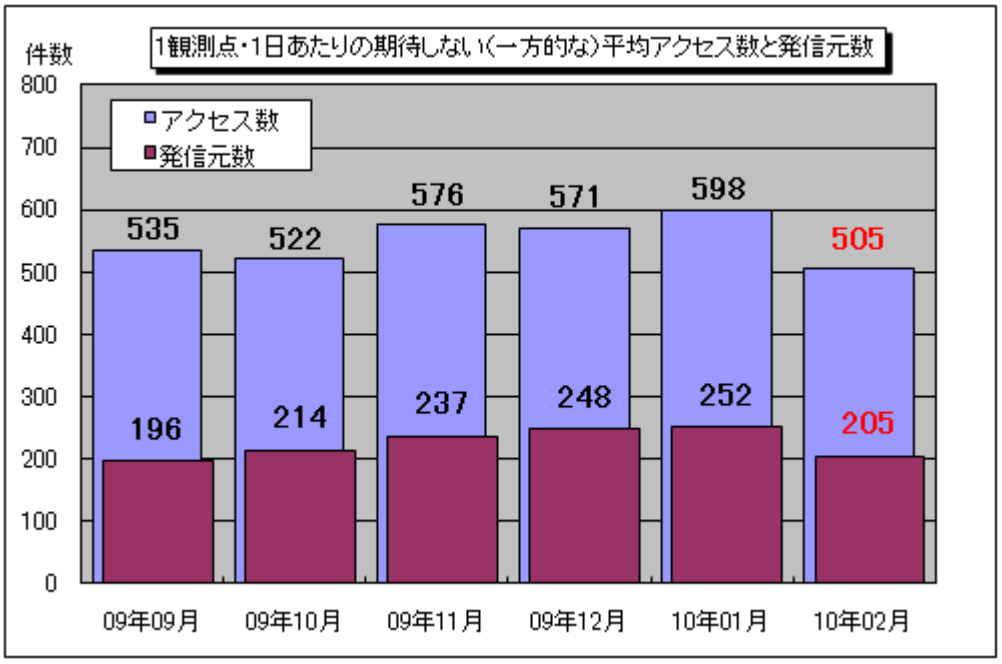
5. インターネット定点観測での 2 月のアクセス状況

インターネット定点観測（TALOT2）によると、2010 年 2 月の期待しない（一方的な）アクセスの総数は 10 観測点で **121,167 件**、延べ発信元数（※）は **49,130 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 205 の発信元から 505 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。

※2 月 5 日～8 日は保守作業のため、システムを停止しています。そのため、2 月の観測データは、この 4 日間を除外して統計情報を作成しています。なお、通常は常時稼働しています。

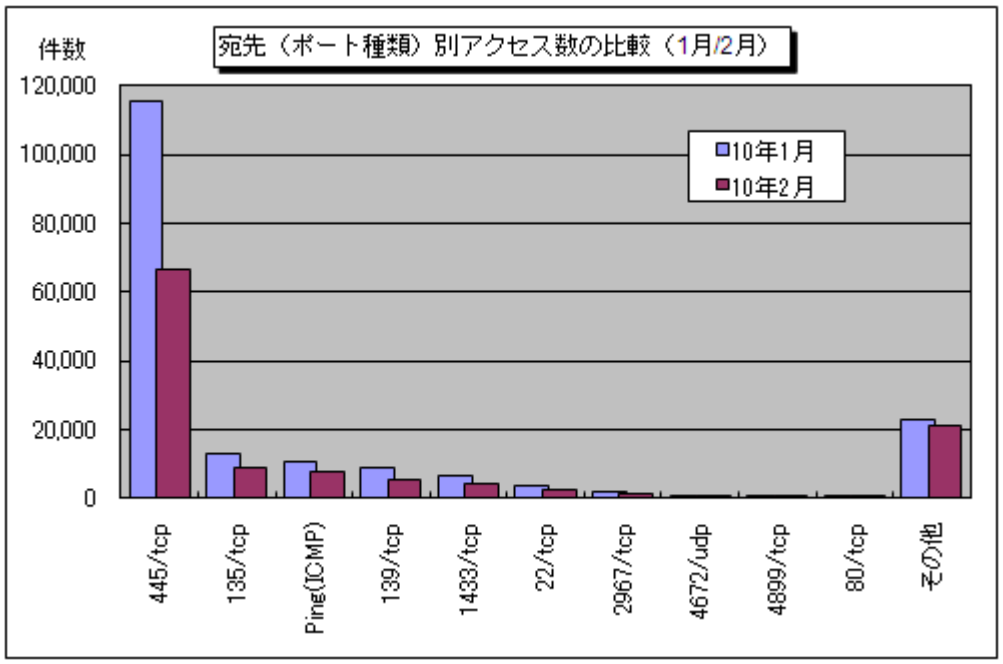


【図 5-1：1 観測点・1 日あたりの期待しない（一方的な）平均アクセス数と発信元数】

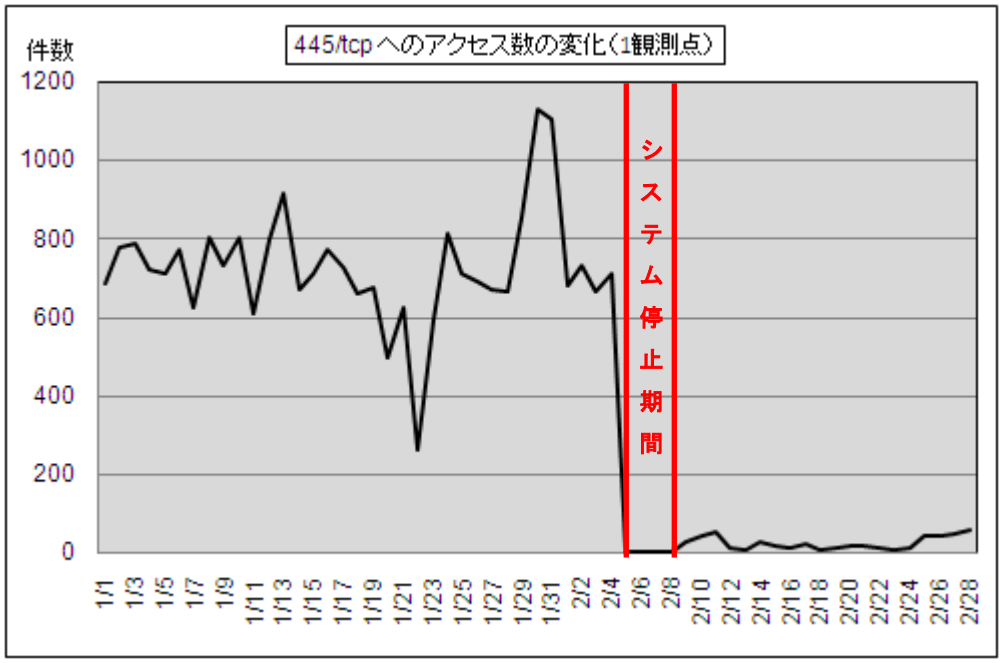
2009 年 9 月～2010 年 2 月までの各月の 1 観測点・1 日あたりの平均アクセス数とそれらのアクセスの平均発信元数を図 5-1 に示します。2 月の期待しない（一方的な）アクセスは、1 月と比べて大幅に減少しました。

1 月と 2 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、445/tcp へのアクセスが 1 月比の約 58%に減少しており、このことがアクセス数全体の減少につながったと思われます。

445/tcp へのアクセスについて詳しく見てみると、2 月 5 日～8 日のシステム停止からの復旧後に全ての観測点の IP アドレスが変更されたタイミングで、各観測点のアクセスの傾向が変化していました。今回は総合的にみて減少分が増加分を大きく上回っていたため、445/tcp へのアクセスが大幅に減少しました。参考までに、減少の度合いが比較的顕著だった観測点（1 ヶ所）のアクセス数の変化を図 5-3 に示します。



【図 5-2：宛先（ポート種類）別アクセス数の比較（1 月/2 月）】



【図 5-3：445/tcp へのアクセス数の変化（1 観測点）】

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/TALOT2-1003.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