Information-technology
Promotion
Agency, Japan

プレスリリース
第 11-25-223 号
2011 年 7 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［2011 年 6 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 6 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

「 サイバー攻撃への対策状況を点検しましょう！ 」

2011 年 4 月、ソニーの「PlayStation Network」からの大規模な個人情報の漏えいが報じられました。その後もサイバー攻撃による様々な組織の被害が立て続けに報じられており、犯行声明・犯行予告を出すグループ（「Anonymous〈アノニマス〉」「LulzSec〈ラルズセック〉」等）が注目を集めるなど、サイバー攻撃の脅威と対策への関心が高まっています。攻撃の標的となる可能性という点では、規模や業種に関わらず、国内のあらゆる組織や企業も同様の条件下にあります。この状況を受け、経済産業省より**情報セキュリティ対策の徹底**について、周知がなされています。

「最近の動向を踏まえた情報セキュリティ対策の提示と徹底」（経済産業省）
http://www.meti.go.jp/press/2011/05/20110527004/20110527004.html

各組織においては、経営層、システム管理部門、社員の三位一体で、サイバー攻撃への対策状況の点検と、必要に応じて体制や対策の見直しを、今一度、確実に実施してください。

（1）近年のサイバー攻撃の特徴

最近、ソニー、任天堂、Google などの大企業、IMF（国際通貨基金）や CIA（米中央情報局）といった公的機関や各国の政府関連機関など、様々な組織がサイバー攻撃の被害に遭っています。経済産業省が実施したアンケート調査※1によると、サイバー攻撃の一種である「標的型攻撃」を受けた経験のある企業は、2007 年には 5.4%でしたが、2011 年には 33%と急増しました。被害が表面化していないものも含めると、インターネットを利用している多数の組織がサイバー攻撃の標的になっていると考えられます。

※1　前述「最近の動向を踏まえた情報セキュリティ対策の提示と徹底」（経済産業省）より

企業・組織をとりまく近年のサイバー攻撃では、攻撃者の動機の変化と、攻撃に使われる手口の巧妙化が特徴的です（図 1-1 参照）。

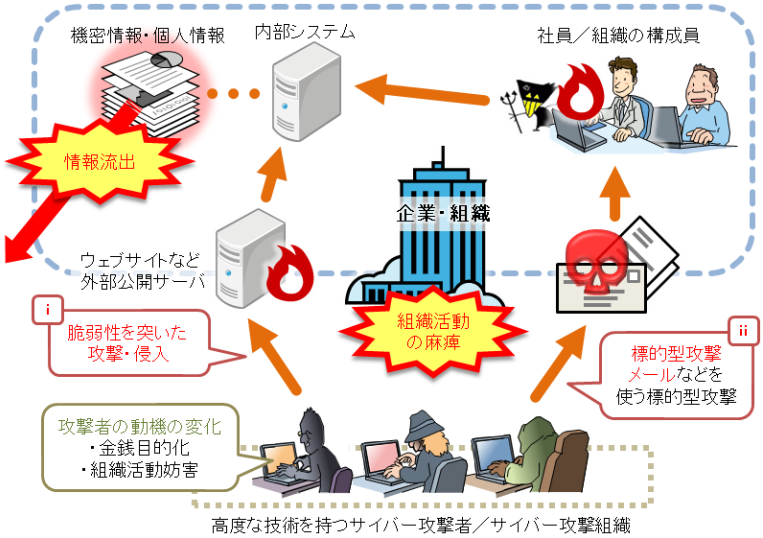


図 1-1：近年のサイバー攻撃の特徴

攻撃者の動機の変化

サイバー攻撃を行う者の動機は、「いたずら」や「能力の誇示」ではなく、数年前から「金銭目的」「組織活動の妨害」に変化しています。

金銭目的の場合、攻撃者は初めから組織の内部にある金銭的価値のある情報（機密情報・個人情報など）を狙っており、これを窃取し、最終的に金銭化することが目的です。従って、情報の流出が発生した場合、何らかの形で悪用される可能性が高く、組織活動に大きな被害を及ぼします。

ソニーの例では、1 億件を超える個人情報の流出となり、これらの不正アクセス対策にかかる費用は約 140 億円との試算が発表されています※2。そのほか、ソニーに限らず、事業の存続に関わる機密情報が狙われた組織の事例が多数報告されています。

一方で、組織活動の妨害や社会的混乱を狙ったサイバー攻撃として、政治的・思想的な動機により、標的の組織に対して何らかの打撃を与えること自体を目的とする事例も増えています。米国防長官の「サイバー攻撃を戦争行為とみなす」旨の発言※3 もあり、攻撃の激化、被害の深刻化が懸念されます。

※2　「2010 年度連結業績見通し修正のお知らせ」（ソニー）
http://www.sony.co.jp/SonyInfo/IR/financial/fr/10revision_sonypre.pdf

※3　「米国はサイバー攻撃を真剣に懸念、戦争行為として対処も＝国防長官」（ロイター）
http://jp.reuters.com/article/topNews/idJPJAPAN-21538820110606

（2）サイバー攻撃の手口

次に、図 1-1 で示した、特に最近目立っているサイバー攻撃の手口について説明します。

（i）脆弱（ぜいじゃく）性を突いた攻撃・侵入

インターネットに公開（接続）しているサーバーの OS やアプリケーション等に脆弱性が存在し、それを悪用された場合、公開サーバーを通じて内部システムの情報を窃取されてしまう可能性があり、非常に危険です。この攻撃は古くからある手口ですが、脆弱性は新たなものが発見され続けているため、継続的な対策が必要です。

「情報セキュリティ早期警戒パートナーシップ」※4 に届け出られた脆弱性関連情報では、累計件数 6,651 件（2011 年 6 月時点）のうち、8 割を超える 5,444 件がウェブサイトに関わるものでした。ウェブサイトの場合は、OS、各種ミドルウェア、ウェブアプリケーション、データベースなど、複雑に構成されている**全ての要素について脆弱性を解消する必要があり**、特に注意を要します。

※4　「脆弱性関連情報の届出」（IPA）
http://www.ipa.go.jp/security/vuln/report/index.html

（ii）標的型攻撃メール

標的型攻撃メールとは、攻撃の対象とする組織や個人を絞った上で、特別に作成したウイルスメールを送るという、「標的型攻撃」の手口の一つです。無作為にばら撒（ま）かれているウイルスメールとは異なり、本物らしい差出人やメール本文、ウイルス対策ソフトで検出されにくいウイルスを使うといった特徴があります。これに騙（だま）されてメールの添付ファイルを開いたり、メール本文に書かれているリンクをクリックしてしまうと、利用者のパソコンがウイルスに感染し、**攻撃者が内部システムへ侵入するための「踏み台」とされてしまう**場合があります。

（3）対策

サイバー攻撃への対策は、組織全体として実施しなければなりません。表 1-1 は組織の構成員の役割別の対策の指針です。

表 1-1：サイバー攻撃への役割別の対策の指針

役割	対策の指針
経営層	組織全体に関わる**経営リスク管理の一環**として、事業継続計画（BCP）と企業の社会的責任（CSR）の観点から、組織としてのセキュリティ対策の点検と見直しを進めてください。
システム管理部門、システム管理者	現在運用しているシステムやサービスについて、サイバー攻撃への対策状況を点検し、対策の強化が必要であれば早急に実施してください。
社員、一般利用者	組織内で利用しているパソコンが、ウイルス感染等により、内部システムへ攻撃者が侵入する「踏み台」となってしまう可能性があります。サイバー攻撃の脅威は**社員などの個人にまで及ぶ**という状況を認識し、セキュリティ対策を怠らないようにしてください。

続いて、（2）で示したサイバー攻撃の手口について、個別の対策を説明します。

（a）「脆弱性を突いた攻撃・侵入」への対策

（a-1）経営層、システム管理部門、システム管理者向け

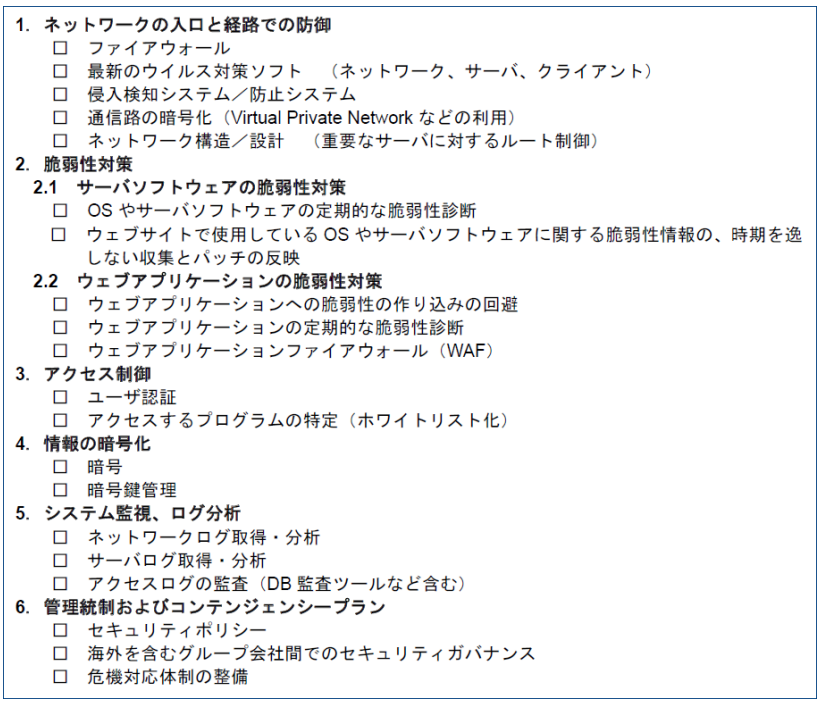
「(i) 脆弱性を突いた攻撃・侵入」で述べた通り、サイバー攻撃の主な対象の一つとして、組織が公開しているウェブサイトがあります。攻撃者は、ウェブサイトを通じた機密情報の窃取、あるいはウェブサイトをひそかに乗っ取った上での内部システムへの侵入を試みます。ウェブサイトに関する情報漏えい事件・事故が多発していることを受け、2011 年 5 月、IPA は下記の注意喚起を行いました。

（ご参考）

「情報窃取を目的としたウェブサイトへのサイバー攻撃に関する注意喚起」（IPA）

http://www.ipa.go.jp/security/topics/alert230527.html

この注意喚起には、対策の方法として、組織におけるシステムやネットワークのセキュリティ対策状況を確認するための**「チェックリスト」**を載せています（図 1-2 参照）。ウェブサイトに限らず、自組織が運用しているシステムの状況を把握するためにも、**今一度の点検をお勧めします。**



1. ネットワークの入口と経路での防御
   - □ ファイアウォール
   - □ 最新のウイルス対策ソフト （ネットワーク、サーバ、クライアント）
   - □ 侵入検知システム／防止システム
   - □ 通信路の暗号化（Virtual Private Network などの利用）
   - □ ネットワーク構造／設計 （重要なサーバに対するルート制御）
2. 脆弱性対策
   - 2.1 サーバソフトウェアの脆弱性対策
     - □ OS やサーバソフトウェアの定期的な脆弱性診断
     - □ ウェブサイトで使用している OS やサーバソフトウェアに関する脆弱性情報の、時期を逸しない収集とパッチの反映
   - 2.2 ウェブアプリケーションの脆弱性対策
     - □ ウェブアプリケーションへの脆弱性の作り込みの回避
     - □ ウェブアプリケーションの定期的な脆弱性診断
     - □ ウェブアプリケーションファイアウォール（WAF）
3. アクセス制御
   - □ ユーザ認証
   - □ アクセスするプログラムの特定（ホワイトリスト化）
4. 情報の暗号化
   - □ 暗号
   - □ 暗号鍵管理
5. システム監視、ログ分析
   - □ ネットワークログ取得・分析
   - □ サーバログ取得・分析
   - □ アクセスログの監査（DB 監査ツールなど含む）
6. 管理統制およびコンテンジェンシープラン
   - □ セキュリティポリシー
   - □ 海外を含むグループ会社間でのセキュリティガバナンス
   - □ 危機対応体制の整備

図 1-2：「チェックリスト」のイメージ（最新版は注意喚起ページを参照）

このチェックリストは、やや高度な施策を含む、包括的なものです。チェックを行い、セキュリティ対策の弱い部分が見つかった場合、可能な限りセキュリティ対策を行うことが望ましいのですが、その中でも、守るべき資産と重要性を見極め、バランスよく対策を講じることが重要です。

また、サイバー攻撃に関する最新の情報にも注意を払い、どのような攻撃手口が流行しているのか、そして、自組織におけるセキュリティ対策が陳腐化していないかを、**定期的に**チェックしてください。

（b）「標的型攻撃メール」への対策

（b-1）組織を構成する全ての人向け

標的型攻撃メールでは、細工した PDF ファイルなど、パソコン内のソフトウェアの脆弱性を悪用し、ウイルスに感染させようとする手口が使われます。一般利用者においては、IPA が公開している「MyJVN バージョンチェッカ」などを活用し、OS やアプリケーションを常に最新のものに保ち、脆弱性を解消するよう努めてください。

（ご参考）

「MyJVN バージョンチェッカ」（パソコン内のソフトウェアをチェックするツール）（IPA）

http://jvndb.jvn.jp/apis/myjvn/#VCCHECK

更に、標的型攻撃メールへの対策は、前述した脆弱性の解消や、ウイルス対策ソフトの利用といったウイルス対策とともに、「罠（わな）のメールを見抜き、開かない」、「不審なメールを受信したら組織内で周知する」といった、**人による対策**が重要になります。

IPA では日本語の標的型攻撃メールに関するレポートや対策ページを公開しています。組織内の全ての人に標的型攻撃メールが届く可能性がありますので、**全利用者において、**改めて脅威の理解と注意が必要です。また、不審なメールを受信した時、**組織としてどのように対応するのか（注意の周知手順など）**のルールを確立してください。

（ご参考）

「実例から分かる標的型攻撃メールの『違和感に気付くポイント』と『違和感に気付いた後の対策ポイント』」（IPA）

http://www.ipa.go.jp/security/vuln/report/newthreat201006.html

「情報窃取を目的として特定の組織に送られる不審なメール『標的型攻撃メール』」（IPA）

http://www.ipa.go.jp/security/virus/fushin110.html

（b-2）経営層、システム管理部門、システム管理者向け（ご参考）

“罠のメールを見抜く”ための訓練・対策として、JPCERT/CC による「IT セキュリティ予防接種」の実施結果と、効果的な実践方法に関する調査結果が公開されています。こちらも併せて参考にしてください。

（ご参考）

「IT セキュリティ予防接種調査報告書 2009 年度」（JPCERT/CC）

http://www.jpcert.or.jp/research/#inoculation

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）

・サーバーで不正なプログラムを動かされて、外部のコンピュータを攻撃していた

・オンラインショップ提供用のサーバーに、バックドア※1 を仕込まれた

○ 相談の主な事例 （相談受付状況および相談事例の詳細は、10 頁の「4.相談受付状況」を参照）

・偽のシステム診断ツールが消えない

・「コンピュータウイルス作成罪」の解釈について

○ 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）ウイルス届出状況

6 月のウイルスの検出数※1 は、**約 3.8 万個**と、5 月の約 2.3 万個から 64.9%の増加となりました。また、6 月の届出件数※2 は、**1,209 件**となり、5 月の 1,049 件から 15.3%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。
・6 月は、寄せられたウイルス検出数約 3.8 万個を集約した結果、1,209 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/Gammima** で**約 9.4 千個**、3 位は **W32/Mydoom** で**約 9.0 千個**でした。

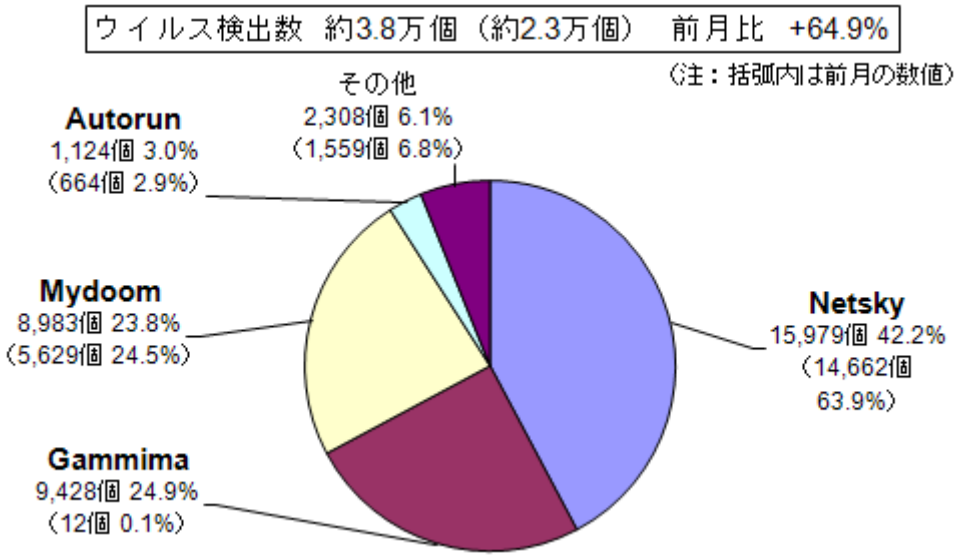


図 2-1：ウイルス検出数

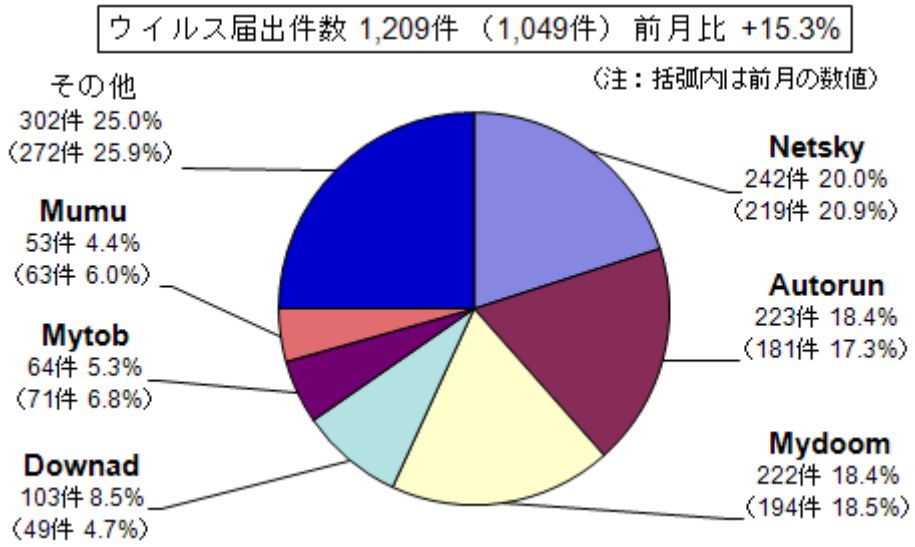


図 2-2：ウイルス届出件数

（2）不正プログラムの検知状況

6 月は、パソコン内に裏口を仕掛ける BACKDOOR といった不正プログラムが増加傾向となりました（図 2-3 参照）。

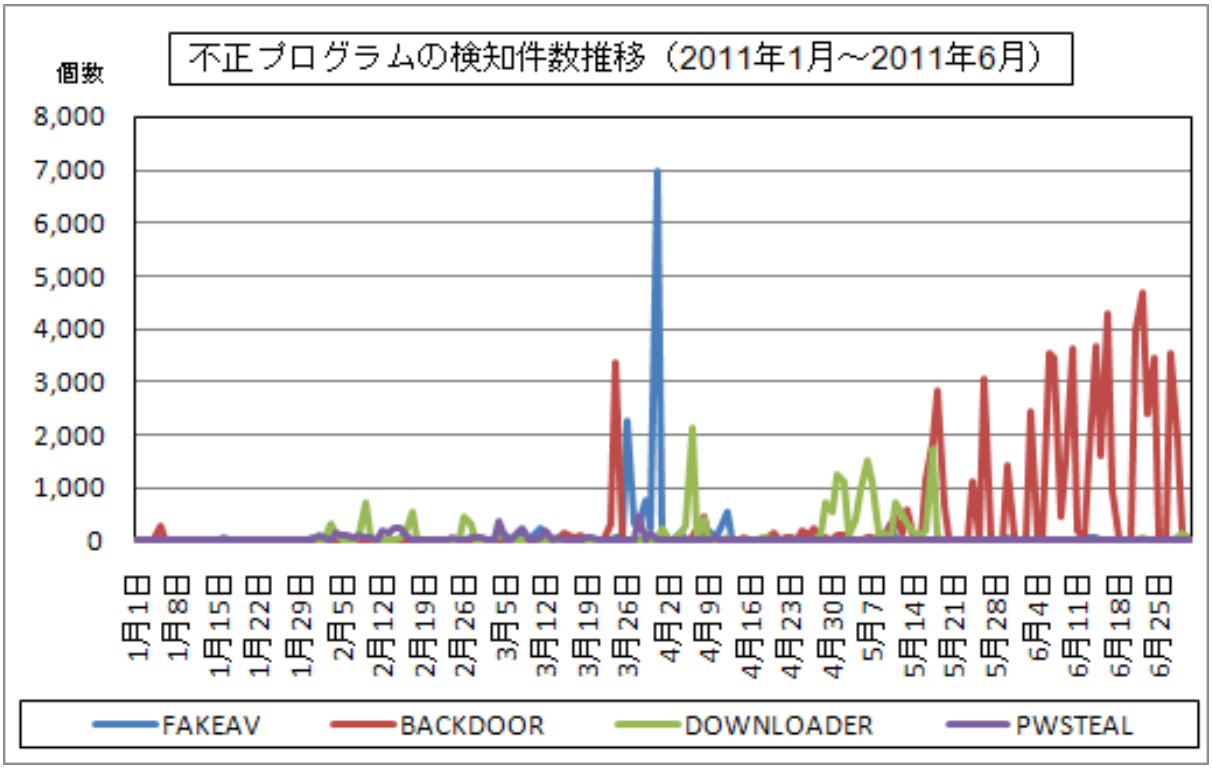


図 2-3：不正プログラムの検知件数推移

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

		1月	2月	3月	4月	5月	6月
届出(a) 計		12	10	6	5	7	9
	被害あり(b)	6	5	6	5	6	9
	被害なし(c)	6	5	0	0	1	0
相談(d) 計		41	23	45	38	55	32
	被害あり(e)	11	6	10	10	14	7
	被害なし(f)	30	17	35	28	41	25
合計(a+d)		53	33	51	43	62	41
	被害あり(b+e)	17	11	16	15	20	16
	被害なし(c+f)	36	22	35	28	42	25

（1）不正アクセス届出状況

6 月の届出件数は 9 件であり、それら全てが被害のあったものでした。

（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32件であり､そのうち何らかの被害のあった件数は７件でした。

（3）被害状況

被害届出の内訳は、**侵入 8 件、DoS 攻撃 1 件**でした。

「侵入」の被害は、データベースからクレジットカード情報等が盗まれたものが３件、ウェブページが改ざんされていたものが２件、踏み台として悪用されていたものが４件、でした。侵入の原因は、脆弱なパスワード設定が３件、ウェブアプリケーションの脆弱性を突かれたものが３件、設定不備が１件でした（他は原因不明）。

（4）被害事例

［侵入］

（i）サーバーで不正なプログラムを動かされて、外部のコンピュータを攻撃していた

事例	・外部から、「そちらのサーバーから攻撃を受けた」と連絡があった。 ・該当サーバーは実験用のサーバーであり、SSH によるリモート接続を制限する設定を実施していなかった。 ・password というパスワードのアカウントが存在し、このアカウントを使って侵入された。 ・外部のコンピュータを攻撃する、不正なプログラムを動かされていた。
解説・対策	実験用サーバーの設定不備と、パスワード不備が重なった残念な例です。SSH は、攻撃者がコンピュータを乗っ取る手段としてよく悪用されます。**リモート接続を行う必要がない場合は、SSH ポートを閉じてください**。 ID とパスワードの管理も、セキュリティ対策の上では大切なことです。**パスワードは推測されにくいものにする**と共に、**不要なアカウントは削除**してください。 （ご参考） IPA-2011 年 6 月の呼びかけ「パスワード ぼくだけ知ってる たからもの」 http://www.ipa.go.jp/security/txt/2011/06outline.html

［不正プログラム埋め込み］

（ii）オンラインショップ提供用のサーバーに、バックドア※1 を仕込まれた

事例	・オンラインショップのサーバーメンテナンス中に、不審なアクセスログが残っていることを発見した。 ・サーバー内を調査したところ、ある脆弱性を悪用されてコネクトバック※2 方式のバックドアを仕込まれていたことが判明した。サーバー上で任意のコマンドが実行可能な状態であったが、実際にどういったコマンドが実行されたかは不明。 ・ネットワーク侵入検知システムを導入していたが検知しなかった。
解説・対策	ネットワーク侵入検知システムを導入していても、通常の通信を装うコネクトバック通信は検知できないことがあり、ファイアウォールでの遮断も困難であることが多いです。 対策は**サーバーの脆弱性を解消することが第一**ですが、多段防御の一環として、万一侵入されて不正なプログラムを配置されてもすぐに気付くことができるよう、ファイル改ざん検知システムやホスト型侵入検知システムを導入することも有効です。

※1　バックドア　　：コンピュータへの侵入者が、侵入成功後にそのシステムに再侵入するために準備する仕掛け。

※2　コネクトバック：侵入者がコンピュータへ侵入する時の通信方式として、侵入者側ではなくコンピュータ側が接続元となって通信を発し、それに応答する形で侵入者がコンピュータに接続し、侵入すること。主に侵入者がファイアウォールをすり抜けるために用いられる。

4. 相談受付状況

6 月のウイルス・不正アクセス関連相談総件数は **1,692 件**でした。そのうち**『ワンクリック請求』に関する相談**が **511 件**（5 月：519 件）、**『偽セキュリティソフト』**に関する相談が **11 件**（5 月：3 件）、**Winny に関連する相談**が **7 件**（5 月：5 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 **6 件**（5 月：8 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

		1月	2月	3月	4月	5月	6月
合計		1,463	1,521	1,723	1,608	1,640	1,692
	自動応答システム	892	892	1,106	997	950	999
	電話	499	570	551	555	620	639
	電子メール	64	53	58	50	62	50
	その他	8	6	8	6	8	4

※ 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。

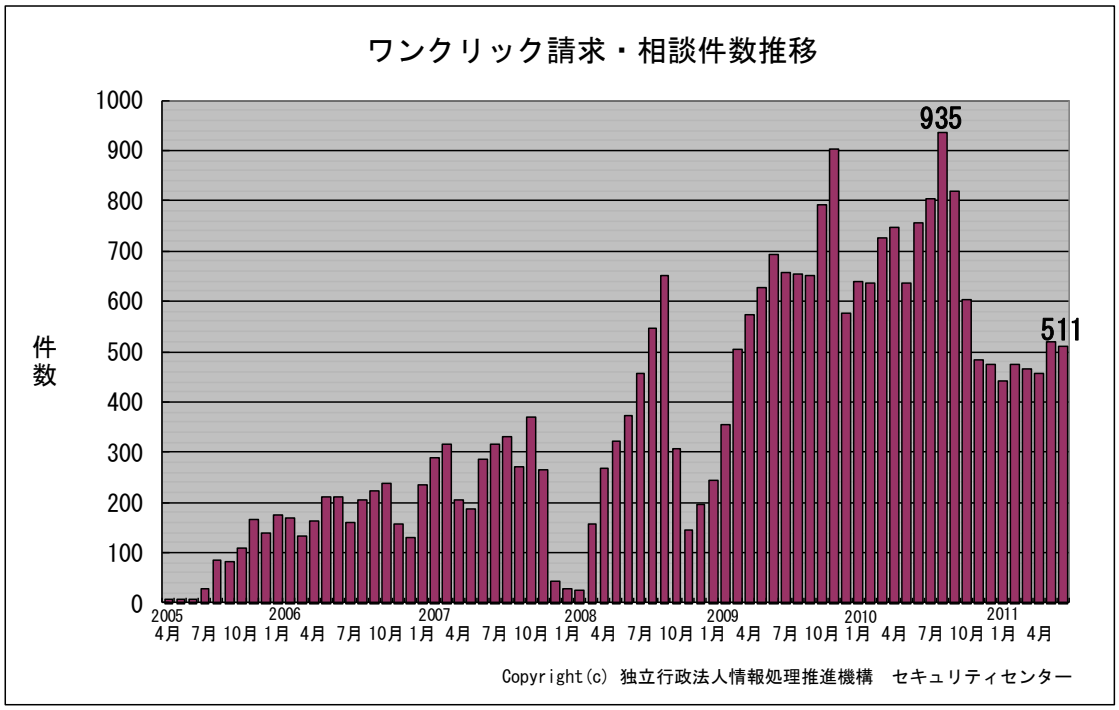


図 4-1：ワンクリック請求相談件数の推移

主な相談事例は以下の通りです。

（i）偽のシステム診断ツールが消えない

相談	インターネットをしていたときに、いつの間にか「Windows Restore」というシステム診断ツールのような画面がでてくるようになった。それによると、パソコンに致命的なエラーが多数存在していて、解消するには有料版を購入する必要があるというもの。 まるで偽セキュリティソフトのような手口であり、購入するつもりもないが、どうやって消したらいいか分からない。
回答	偽セキュリティソフトに関する相談は以前から多く寄せられていますが、最近ではウイルス検知の代わりにシステムの異常を訴える、“**偽システム診断ツール**”に関する相談も増えてきています。 対処方法については、偽セキュリティソフトの場合と同様に Windows の「システムの復元」機能を使って、パソコンの状態を以前の状態に戻すか、それができなければパソコンを初期化するということになります。 （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）「コンピュータウイルス作成罪」の解釈について

相談	2011 年 6 月に国会で「コンピュータウイルス作成罪」の新設を含む刑法などの改正案が可決されたということだが、それによると、“ウイルスの作成や提供だけでなく、取得したり保管したりする行為も刑罰の対象になる”とある。 これはつまり、第三者からメールなどでウイルスを送りつけられてしまった場合、私が取得もしくは保管したことになり、私が罪に問われかねないということか。
回答	法務省のウェブページの Q&A によれば、「Q6」にある通り、ウイルスメールを受信（あるいは受信して感染）しただけでは、この罪は成立しないとあります。 （ご参考） いわゆるサイバー刑法に関するＱ＆Ａ（法務省） http://www.moj.go.jp/content/000073750.htm

5. インターネット定点観測での 6 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 6 月の期待しない（一方的な）アクセスの総数は 10 観測点で **157,476 件**、延べ発信元数※は **69,532 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 232 の発信元から 525 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。

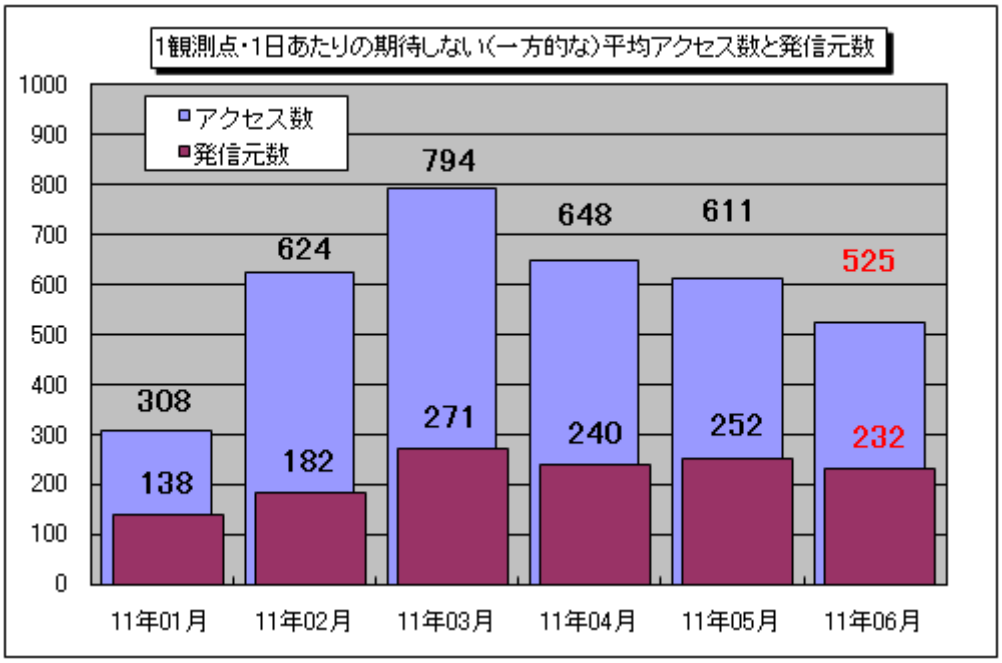


図 5-1：1 観測点・1 日あたりの期待しない（一方的な）平均アクセス数と発信元数

2011 年 1 月～2011 年 6 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。6 月の期待しない（一方的な）アクセスは、5 月と比べて減少しました。

5 月と 6 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、増加が観測されたのは 80/tcp へのアクセスでした。

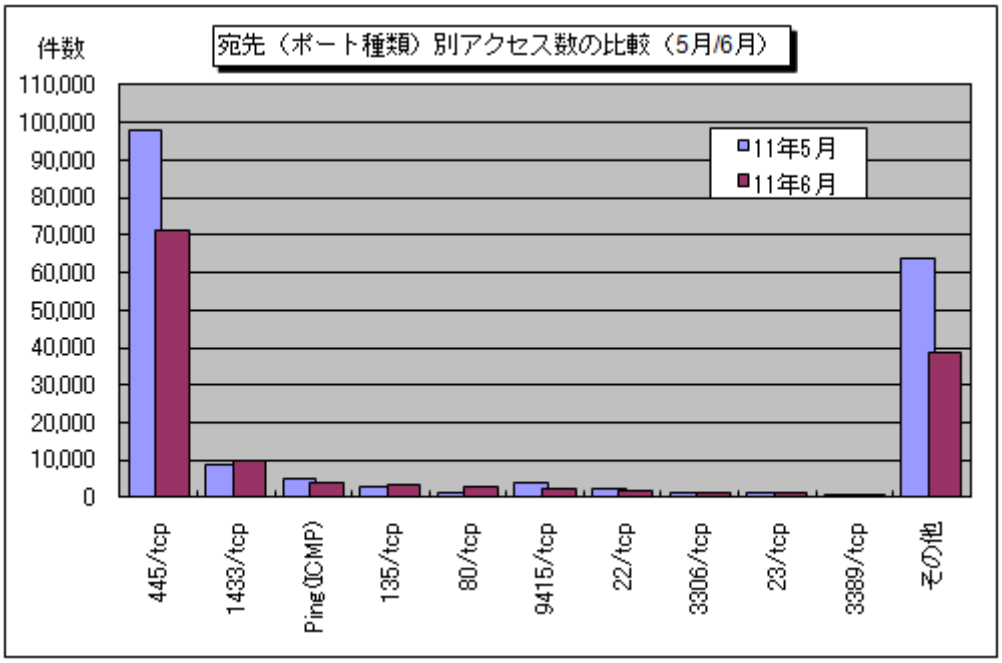


図 5-2：宛先（ポート種類）別アクセス数の比較（5 月/6 月）

80/tcp については、6 月後半に、アメリカと中国の複数の IP アドレスからのアクセスの増加が観測されました（図 5-3 参照）。これらのアクセスは、全て SYN/ACK パケットだったことから、TALOT2 で使用しているアドレスが、DoS 攻撃（SYN Flood 攻撃）(*1) の攻撃者が発信元詐称に利用したアドレスと一致したために、標的となった組織からの SYN/ACK パケット（跳ね返りパケット (*3)）が届いていた可能性があるということです。

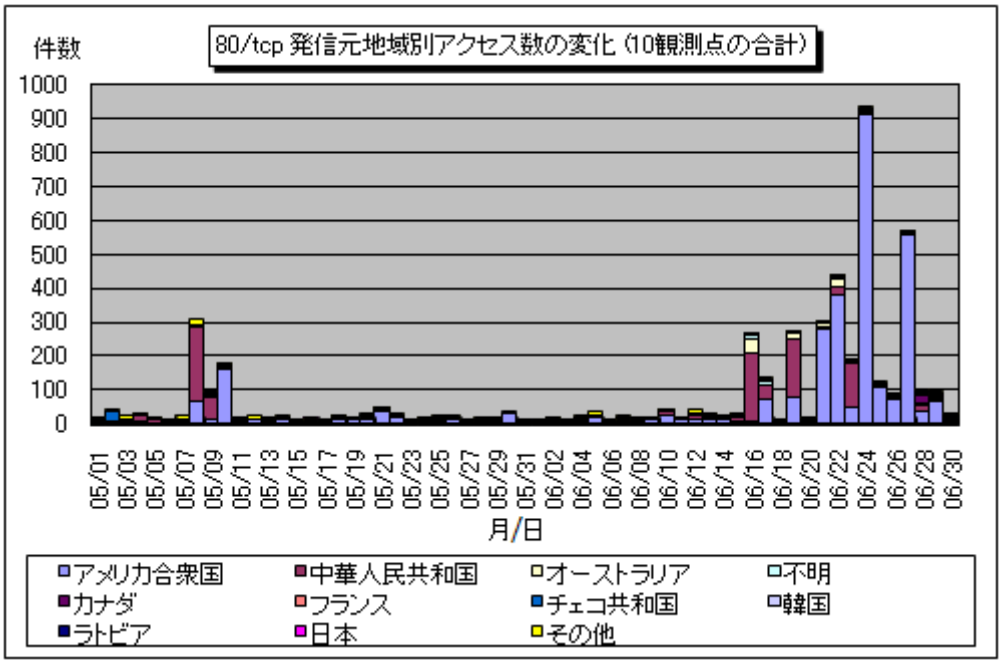


図 5-3：80/tcp 発信元地域別アクセス数の変化（10 観測点の合計）

(*1):DoS 攻撃（SYN Flood 攻撃）

「サービス妨害攻撃」Denial of Service の略から DoS 攻撃と呼ばれ、標的マシンにおけるサービス機能を停止または低下させる攻撃のこと。この DoS 攻撃の 1 つに、標的マシンに「過負荷を与える攻撃」 として SYN Flood 攻撃があります。これは、標的マシンに対して発信元アドレスを詐称した SYN パケット（3 ウェイ・ハンドシェーク (*2) での接続確立の最初に送られるパケット）を大量に送りつけ、確立途中状態の接続を大量作成するものです。

(*2):3 ウェイ・ハンドシェーク

TCP で通信を行う際に、最初に行われる通信確立のための手順を、3 ウェイ・ハンドシェークと言います。この手

順により、通信を行う相手同士が通信の準備ができたことを確認できるわけです。

以下にA とB の通信確立の手順を示します。

①A からB へSYN パケットの送信

②B からA へACK+SYN パケットの送信

③A からB へACK パケットの送信

これで、AB 双方の通信が確立されます。

(*3):跳ね返りパケット

DoS 攻撃（SYN Flood 攻撃）において攻撃者が詐称した発信元アドレスに、標的マシンから大量の SYN+ACK パケットが返信されてくることです。

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/TALOT2-1107.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／宮本
Tel:03-5978-7591 Fax:03-5978-7518
E-mail: isec-info@ipa.go.jp