プレスリリース
第 10-34-195 号
2010 年 9 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 8 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、2010 年 8 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

「新たな攻撃手口で、USB メモリなどを介して感染拡大するウイルスが出現！」

マイクロソフト社は、2010 年 6 月と 7 月に 1 件ずつ、Windows の脆弱性に関する情報と攻撃からの回避策を緊急に公開しました。これは、**それらの脆弱性を悪用して感染を拡げるウイルスの攻撃、いわゆる「ゼロデイ攻撃」が確認され、危険な状態が続いていたためです。IPA においても、これら 2 件の脆弱性に関する緊急対策情報※を発表しています。**

特に、7 月に公開された「Windows シェルの脆弱性により、リモートで処理が実行される（2286198）」脆弱性（MS10-046）を悪用するウイルスは、**今までになかった手口で、USB メモリなどを介して感染を拡大することが確認されています。**

こうしたウイルスの被害に遭わないよう、普段から脆弱性の情報、修正プログラムや回避策の情報を注意深く確認し、対策情報が公開されたら、できるだけ速やかに対応しましょう。

※「Windows のヘルプとサポートセンターの脆弱性（MS10-042）について」
http://www.ipa.go.jp/security/ciadr/vul/20100705-windows.html
「Windows シェルの脆弱性（MS10-046）について」
http://www.ipa.go.jp/security/ciadr/vul/20100803-ms10-046.html

（1）新たに発見されたウイルスとその感染手口について

W32/Stuxnet（以下、Stuxnet）は、Windows シェルの脆弱性（MS10-046）を悪用して感染を拡げるウイルスです。この脆弱性は、Windows がショートカットファイル※を扱う際に問題があるというものです。具体的には、エクスプローラなどで、ショートカットファイルのアイコンを表示しようとする際、アイコン画像の参照先ファイルを Windows が正確に解析しない、という問題です。このため、悪意あるコードを含むファイルをショートカットファイルのアイコン画像の代わりに参照されると、脆弱性を突かれて任意のプログラムを実行される恐れがあります（図 1-1 参照）。

※ファイルやフォルダ、アプリケーションへの参照となるファイルのこと。実体がそこになくても、見掛け上はショートカットファイルを実体そのものとして扱え、ファイルへのアクセスを簡単にすることができる。

図 1-1：マイコンピュータからフォルダなどを開きファイルを参照した例

IPA では、Stuxnet ウイルス検体を入手して解析を行いました。感染手口の詳細を次に示します。

顕著な特徴として、「細工されたショートカットファイル（lnk ファイル）が入っているフォルダをエクスプローラで開くだけで、ウイルスが動き出す」ということが挙げられます。これは、今までに無い、新たな攻撃手口と言えます。

例えば、USB メモリに Stuxnet ウイルスファイルが入っている場合、この USB メモリを Windows シェルの脆弱性（MS10-046）のあるパソコンに挿し、USB メモリ内のファイルを参照しようとしてエクスプローラで**ウイルスファイルを含むフォルダを開くだけで、ファイルに触れなくても Stuxnet ウイルスの攻撃が開始されます**（図 1-1 参照）。

USB メモリ経由で感染するウイルスとしては、過去に W32/Autorun をはじめとして複数のウイルスが確認されています（便宜上、ここでは「従来の USB メモリ感染型ウイルス」と呼びます）。従来の USB メモリ感染型ウイルスは、Windows の「自動実行」機能※を無効にすることで対策が可能ですが、**今回見つかった新たな攻撃手法では「自動実行」機能は使われませんので、「自動実行」機能を無効化するだけでは、Stuxnet ウイルスの攻撃を回避することはできません。**

※USB メモリをパソコンに挿した時、または USB メモリのアイコンをダブルクリックして開こうとした時、ファイルが自動的に実行される Windows の機能のこと。Autorun（オートラン）機能と呼ぶ場合もある。

（ご参考）

「Windows での「自動実行」機能の無効化手順」（IPA）

http://www.ipa.go.jp/security/virus/autorun/

また Stuxnet ウイルスは、USB メモリ経由以外でも、以下の手口によっても感染することが判りました（図 1-2 参照）。

（a）**ネットワークの共有フォルダを経由した感染**

ネットワークの共有フォルダに、ウイルスファイルが置かれると、その共有フォルダを開いてフォルダの中身を表示しただけでパソコンが感染します。

（b）**メール添付で送られて来たファイルを保存、フォルダを開いて感染**

ウイルスファイルがメール添付されて来た場合、添付ファイルをパソコン内のフォルダに保存した後、当該フォルダの中身を表示しただけでパソコンが感染します。

（c）**細工された文書ファイルを開いて感染**

ウイルスファイルが埋め込まれた文書ファイル（オフィスソフトのファイルなど）を開いただけで、そのパソコンが感染します。

（d）**改ざんされたウェブサイトを閲覧して感染**

ウイルスファイルを開くスクリプトが書き込まれた、罠のウェブサイトを閲覧しただけでパソコンが感染します。悪意ある者に改ざんされた正規サイトを閲覧した場合でも同様です。

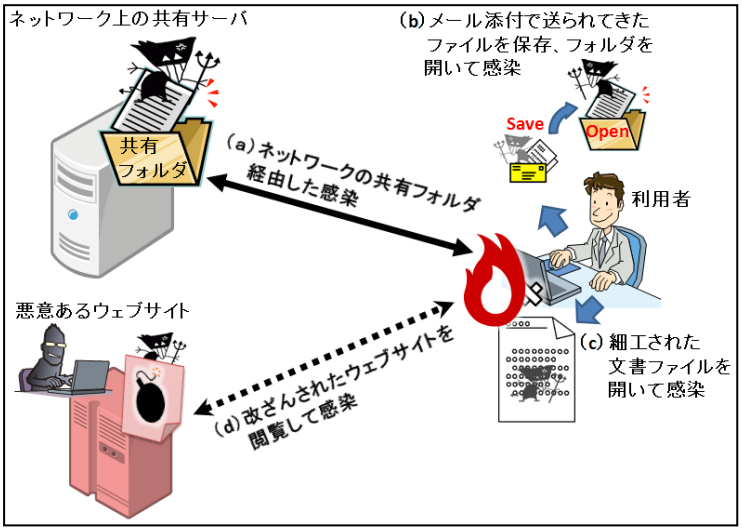


図 1-2：USB メモリ以外での感染手口のイメージ図

（2）対策

●脆弱性の解消

Stuxnet ウイルスへの対策は、このウイルスが悪用する Windows の脆弱性を解消することのみです。この脆弱性の修正プログラムは既に公開されています（対象：Windows XP SP3、Windows Vista SP1 以降、Windows 7）。できるだけ速やかに対応しましょう。

（ご参考）

「MS10-046：Windows の重要な更新」

「Windows シェルの脆弱性により、リモートでコードが実行される(2286198)」（マイクロソフト社）

http://www.microsoft.com/japan/security/bulletins/ms10-046e.mspx

上記脆弱性だけではなく、未対応の脆弱性がないか確認し、できるだけ速やかに対応しましょう。

（ご参考）

「Microsoft Update を使用してコンピューターを最新の状態に保つ」（マイクロソフト社）

http://www.microsoft.com/japan/protect/computer/updates/mu.mspx

「マイクロソフト　セキュリティ情報センター」（マイクロソフト社）

http://www.microsoft.com/japan/security/sicinfo/default.mspx

●基本的なウイルス対策

重要な対策の一つである、ウイルス対策ソフトの導入、最新の定義ファイルでの運用を忘れずに行いましょう。一般利用者向けのウイルス対策ソフトとして、危険なウェブサイトの閲覧防止機能などを備えた、「統合型」と呼ばれるものを推奨します。

（3）ゼロデイ攻撃への対策

Stuxnet ウイルスは、この脆弱性を解消するための修正プログラムや回避策が公開される前から存在が確認されており、修正プログラム等が公開されるまでは「ゼロデイ攻撃」の状態でした。

「ゼロデイ攻撃」とは、OS（オペレーティングシステム）やアプリケーションソフトなどの脆弱性が見つかっている状態で、その弱点が修正される前にそれを悪用する攻撃を指します。

「ゼロデイ攻撃」を受けないためには、悪用されている脆弱性の情報がいつ公開されても適切に対応できるように、ベンダーからの情報を迅速に収集することが重要です。ベンダーから発信されているメールマガジンの購読や、ニュースサイトやポータルサイトに掲載されている記事を定期的に確認することをお勧めします。

（ご参考）

「情報処理推進機構　新着情報メール配信」（IPA）

https://ipa-mn-web.ipa.go.jp/b/0001/fu/0/input_email.jsp

「セキュリティ ニュースレター」（マイクロソフト社）

http://technet.microsoft.com/ja-jp/security/cc307424.aspx

IPA では、ベンダーから公開される脆弱性情報を分析して、緊急性が高いと判断されたものを「緊急対策情報」としてウェブサイトから発信しています。日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供している JVN などの脆弱性情報ポータルサイトも参考にしてください。

（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

「JVN（Japan Vulnerability Notes）」（脆弱性情報ポータルサイト）

http://jvn.jp/

「セキュリティ TechCenter」IT プロフェッショナル向け（マイクロソフト社）

http://technet.microsoft.com/ja-jp/security/default.aspx

「セキュリティ At Home」一般家庭向け（マイクロソフト社）
http://www.microsoft.com/japan/protect/default.mspx

詳しくは、下記ウェブページの“(3)「ゼロデイ攻撃」を受けないための注意点”を参照してください。また、「ゼロデイ攻撃」を受けたと感じた場合は、“(4)「ゼロデイ攻撃」を受けてしまったことに気がついたときは”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、7 頁の「3.コンピュータ不正アクセス届出状況」を参照）
・外部サイト攻撃ツールを埋め込まれ、踏み台として悪用された
・Skype アカウントが乗っ取られたようで、身に覚えのない通話料金を請求された

○ 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）
・ワンクリック請求の被害で、当該ユーザアカウントを削除すれば請求画面も消える？
・メッセンジャーサービスで、友人からのメッセージ内のリンクをクリックしたらパソコンが勝手にシャットダウンした！？

○ 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

8 月のウイルスの検出数※1 は、**約 4.5 万個**と、7 月の約 4.7 万個から 5.5%の減少となりました。また、8 月の届出件数※2 は、**1,177 件**となり、7 月の 1,209 件から 2.6%の減少となりました。

※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。
・8 月は、寄せられたウイルス検出数約 4.5 万個を集約した結果、1,177 件の届出件数となっています。

検出数の 1 位は、**W32/Netsky** で**約 2.9 万個**、2 位は **W32/Waledac** で**約 7 千個**、3 位は **W32/Mydoom** で**約 6 千個**でした。

ウイルス検出数　約4.5万個（約4.7万個）　前月比－5.5%

（注：括弧内は前月の数値）

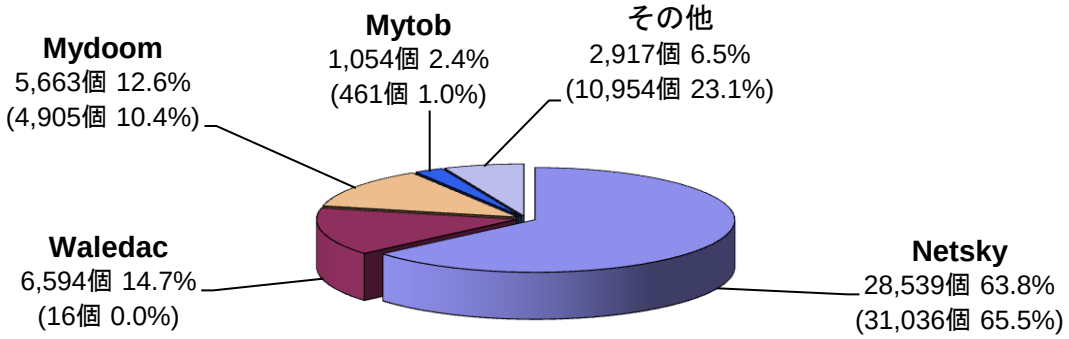


図 2-1：ウイルス検出数

ウイルス届出件数　1,177件（1,209件）前月比 －2.6%

（注：括弧内は前月の数値）

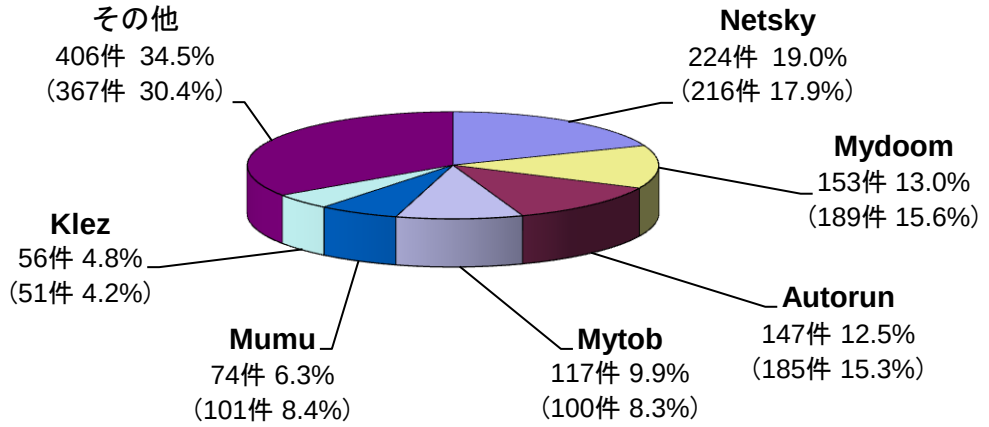


図 2-2：ウイルス届出件数

（2）不正プログラムの検知状況

2010 年 8 月の不正プログラムの検知状況は、DOWNLOADER や FAKEAV、BACKDOOR など、急増した事例が確認されました（図 2-3 参照）。

このような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く、そのメールの配信にはボット※3 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※4 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/

※3　ボットとは、コンピュータウイルス等と同様な方法でコンピュータに感染し、そのコンピュータをネットワークを通じて、外部から操ることを目的として作成されたプログラムです。

※4　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/

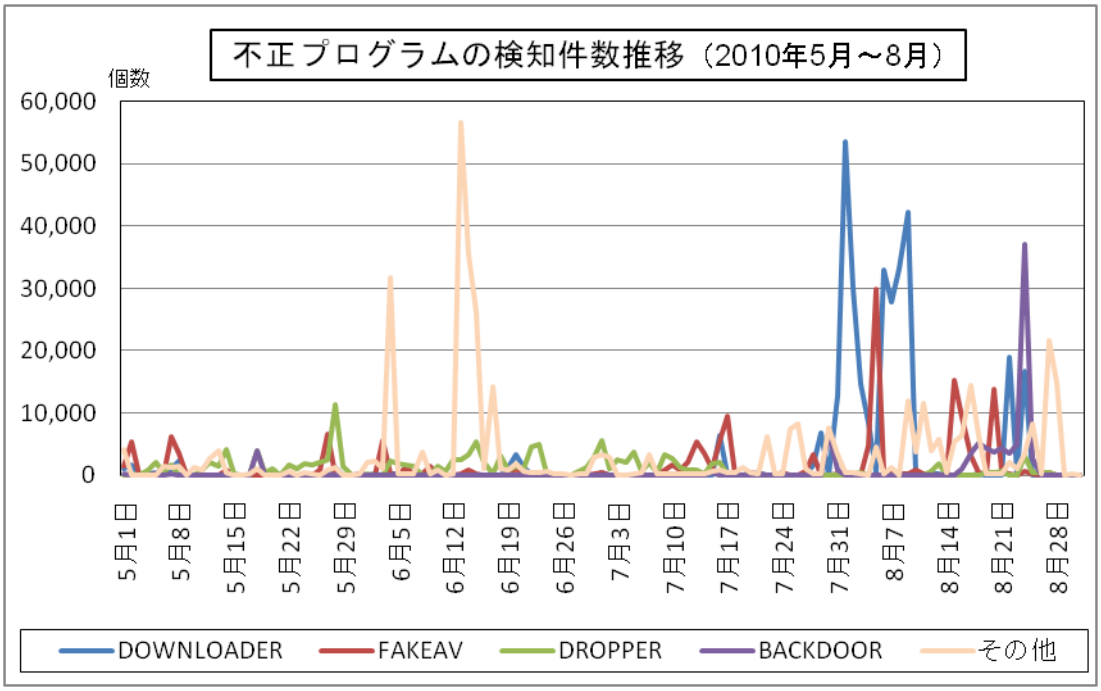


図 2-3：不正プログラムの検知件数推移

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

		3月	4月	5月	6月	7月	8月
届出(a)　計		19	11	8	15	14	18
	被害あり(b)	13	10	5	13	9	12
	被害なし(c)	6	1	3	2	5	6
相談(d)　計		60	39	52	77	44	56
	被害あり(e)	23	16	22	50	23	16
	被害なし(f)	37	23	30	27	21	40
合計(a+d)		79	50	60	92	58	74
	被害あり(b+e)	36	26	27	63	32	28
	被害なし(c+f)	43	24	33	29	26	46

（1）不正アクセス届出状況

8 月の届出件数は 18 件であり、そのうち何らかの被害のあったものは 12 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 56 件（うち 8 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 16 件でした。

（3）被害状況

被害届出の内訳は、**侵入 7 件、アドレス詐称 1 件、なりすまし 4 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が盗まれたものが 2 件、ウェブページが改ざんされていたものが 2 件（内、フィッシング※に悪用するためのコンテンツ設置 1 件）、外部サイトを攻撃するツールを埋め込まれ、踏み台として悪用されていたものが 2 件、SQL※インジェクション※攻撃が成功していたもの（被害内容不明）が 1 件、でした。侵入の原因は、脆弱なパスワード設定が 2 件（内、SSH※で使用するポートへのパスワードクラッキング※攻撃 1 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、アクセス制限の設定不備が 1 件でした（他は原因不明）。

「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 1 件、Skype1 件、フリーのウェブメール 1 件など）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。

※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。

※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）外部サイト攻撃ツールを埋め込まれ、踏み台として悪用された

事例	・外部向けサービスを提供しているサーバで、サービス品質低下が確認された。 ・調査したところ、当該サーバから、外部サイトの SSH で使うポートへの攻撃が行われていることが判明。 ・セキュリティ専門業者に詳細調査を依頼。その結果、2 台のサーバに、サイト攻撃ツールの埋め込みが確認された。さらに、外部からコントロールするためのバックドア「psyBNC」（IRC network bouncer）が設定されていたことが判明。 ・当該サーバの SSH で使うポートに、外部からパスワードクラッキング攻撃を受け、パスワードが破られていた。パスワードが、ベンダーの既定値のままだったことが原因と思われる。
解説・対策	被害事実確認後、早々にセキュリティ専門業者に対処を依頼したおかげで、被害内容の詳細分析および原因究明が素早くできた例です。 なお、パスワード認証は、時間を掛ければいつかは破られる、という原則を再認識しましょう。ログのチェック、接続許可制限などの対策が有効ですが、**SSH 運用時には、ログインの際に公開鍵認証※などの強固な認証の採用を推奨**します。 （参考） IPA - 安全なウェブサイトの作り方 http://www.ipa.go.jp/security/vuln/websecurity.html

※公開鍵認証 ： 公開鍵と秘密鍵のペアで利用者個人の認証を行う方式のこと。

［なりすまし］

（ii）Skype アカウントが乗っ取られたようで、身に覚えのない通話料金を請求された

事例	・IP 電話サービスである Skype を利用している。4 月頃、自分のアカウントにサインインできなくなった。仕方なく、別のアカウントを作成して使っていた。 ・7 月に届いたクレジットカード利用明細を見ると、自分がサインインできなくなったアカウントでの通話料チャージ料金として 3 万円以上、請求されていた。何者かに、勝手にアカウントを使われて通話利用されていたようだ。 ・なぜアカウントが乗っ取られたのか、原因は分からない。
解説・対策	**自分のアカウントにサインインできないという異常事態だったにも関わらず、対処せずそのまま放置していたために、被害が拡大してしまった**例です。 今後の対策として、まずは **ID とパスワードの管理を見直すことが重要**です。さらに、脆弱性の解消やウイルス対策もきちんと実施しましょう。 （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

8 月のウイルス・不正アクセス関連相談総件数は **2,432 件**と、**過去最多**でした。そのうち**『ワンクリック請求』に関する相談**が **935 件**（7 月：805 件）と**過去最多**、**『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 **15 件**（7 月：5 件）、**Winny に関連する相談**が **4 件**（7 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 **2 件**（7 月：1 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

		3月	4月	5月	6月	7月	8月
合計		2,000	2,110	1,881	1,983	2,133	2,432
	自動応答システム	1,057	1,194	1,091	1,022	1,142	1,298
	電話	846	835	714	829	924	1,053
	電子メール	92	81	76	129	66	75
	その他	5	0	0	3	1	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。

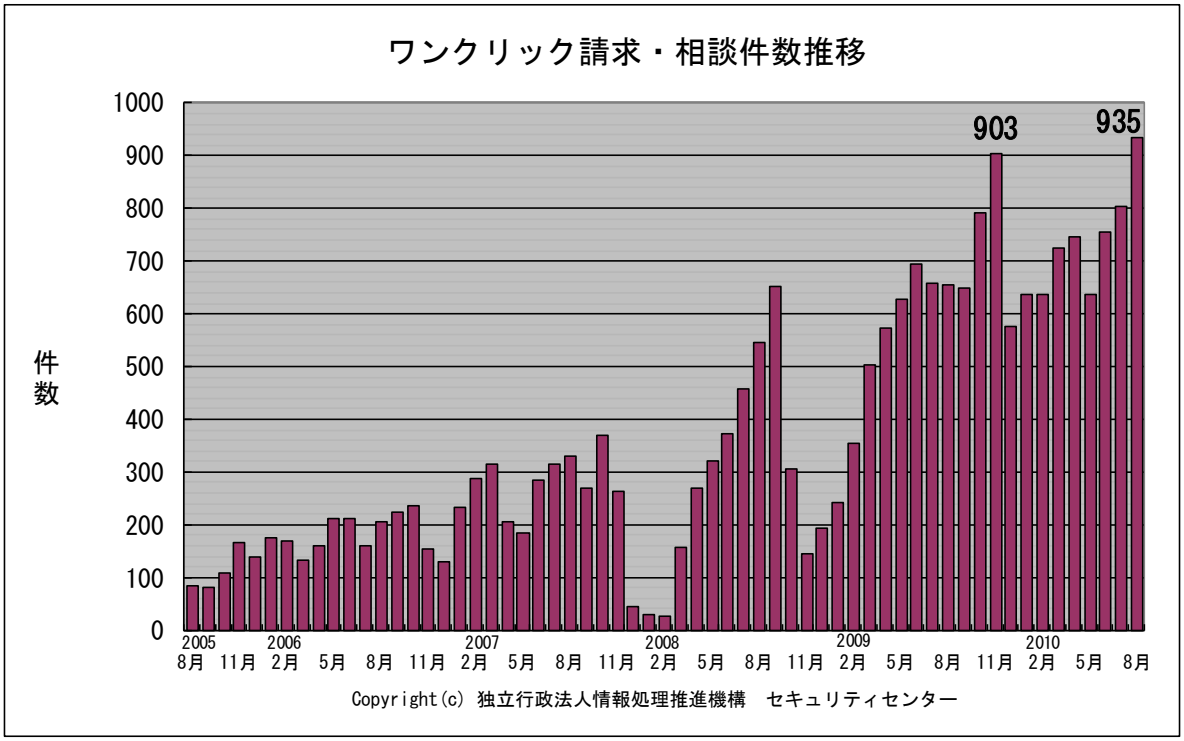


図 4-1：ワンクリック請求相談件数の推移

主な相談事例は以下の通りです。

（i）ワンクリック請求の被害で、当該ユーザアカウントを削除すれば請求画面も消える？

相談	アダルトサイトの請求画面が表示され続けて、消えない。請求画面が表示される自分のユーザアカウントを削除すれば、請求画面は消えますか？
回答	相談者は、ワンクリック請求のウイルス感染被害に遭っています。OS が Windows XP/Vista/7 であれば、システムの復元機能を使って、パソコンを請求画面が表示された日よりも前の日の状態まで戻すことをお勧めしています。 **なお、自分のログインユーザアカウント以外のアカウントでログインをして、請求画面が表示されなければ、自分のアカウントを削除することで請求画面が消える場合もあります。ですが、デスクトップ上にあるファイルや、「マイドキュメント」フォルダの中身も消えてしまいますので、アカウントを削除する前に、必要なファイルのバックアップを実施しましょう。** （参考） IPA – ワンクリック請求に関する注意喚起 http://www.ipa.go.jp/security/topics/alert20080909.html

（ii）メッセンジャーサービスで、友人からのメッセージ内のリンクをクリックしたらパソコンが勝手にシャットダウンした！？

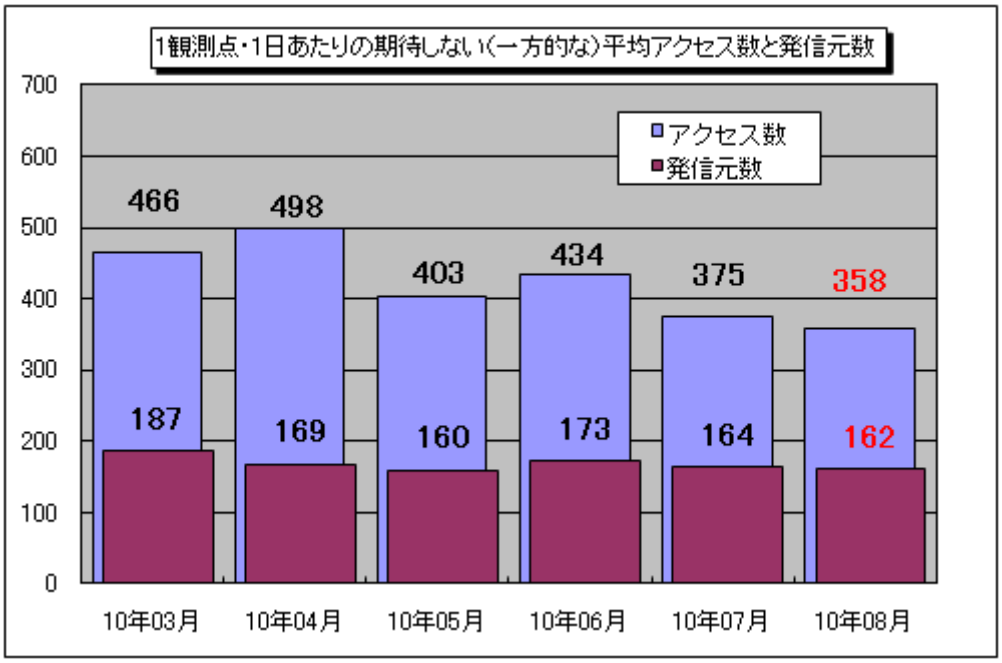
相談	メッセンジャーサービスを利用している。友人が差出人だったので、特に警戒せず、メッセージ内に書かれていた URL をクリックしたら、パソコンが勝手にシャットダウンしてしまった。ウイルスに感染したのか？
回答	相談者は、友人からのメッセージということで URL を確認しないでクリックをしていますので、**ウイルス感染の疑いが高いと言えます。もし今後の利用が心配であれば、パソコンを初期化することをお勧めします。また、アカウント乗っ取りの可能性も否定できないため、初期化後はメッセンジャーサービスにログインする際のパスワードを変更しておきましょう。**万が一、メッセンジャーサービスにログインできない場合は、メッセンジャーサービス運営元に問い合わせてください。 **たとえ友人が差出人となっていても、メッセージ中にある URL を不用意にクリックすることは危険です。悪意ある者が、他人のアカウントを乗っ取って悪意あるサイトへ誘導するためのリンクをばら撒いている可能性がある**ためです。これはメールでも同じ事が言えます。不自然と思われるメッセージが届いた場合は、まずは送ってきた相手に確認することをお勧めします。 （参考） IPA – 2010 年 5 月の呼びかけ「流行のサービスを狙った攻撃に注意！」 http://www.ipa.go.jp/security/txt/2010/05outline.html

5. インターネット定点観測での 8 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 8 月の期待しない（一方的な）アクセスの総数は 10 観測点で **111,085 件**、延べ発信元数※は **50,147 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 162 の発信元から 358 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】

2010 年 3 月～2010 年 8 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。8 月の期待しない（一方的な）アクセスは、7 月と比べて減少しました。

7 月と 8 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、これまでは上位に挙がって来なかった 44274/udp が上位にランクされました。これは、8 月下旬に TALOT2 の 1 つの観測点で観測された、アメリカの 1 つの発信元からのアクセスでした。このポートは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。

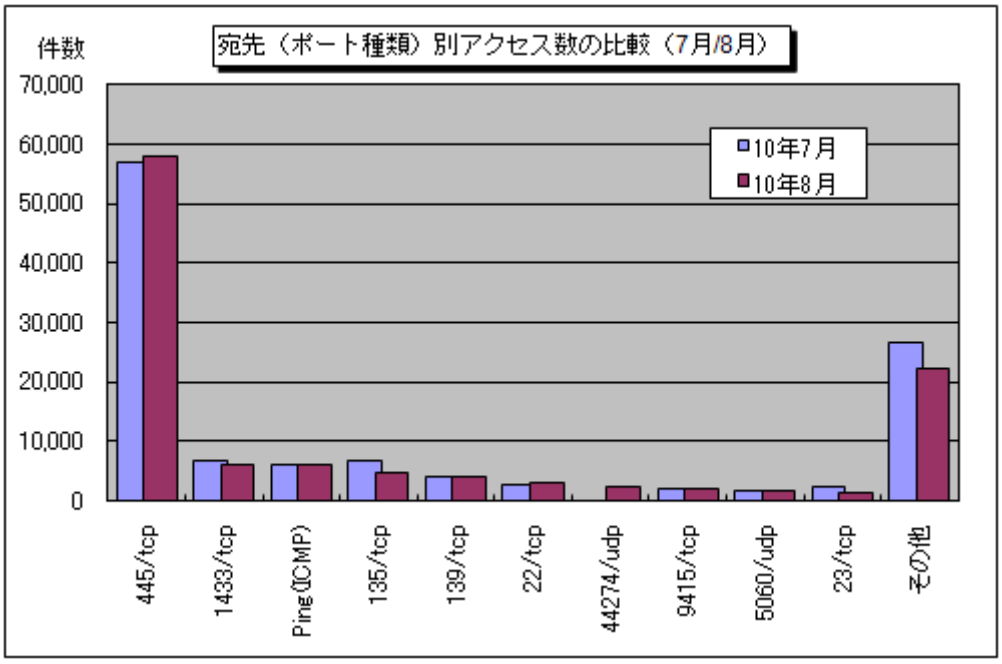
また、8 月 8 位にランクされている 9415/tcp へのアクセスは、6 月の報告でも取り上げましたが、それ以降も継続して観測されていました（図 5-3 参照）。このアクセスは、TALOT2 の複数の観測点に対して、海外（主に中国）の複数の発信元から送られていたという特徴があり、定点観測を行っている他の組織においても、ほぼ同様の傾向が観測されていました。なお、9415/tcp については、中国のあるサイトで公開されている、プロキシ機能を持つソフトがこのポートで待ち受けを行うことが確認されています。可能性として、悪意ある者がこのプロキシ機能を持つソフトを踏み台として、ウェブサーバ等への攻撃に使うために、このソフトがインストールされたパソコンを探索していたものだったと考えられます。

（ご参考）

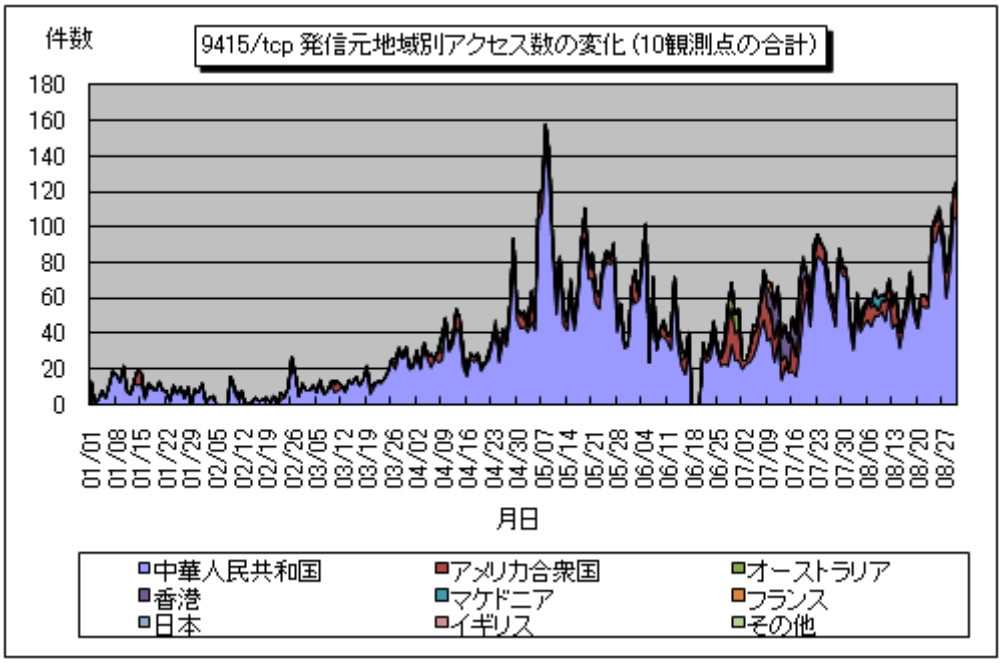
2010 年 5 月のインターネット定点観測（TALOT2）での観測状況について（IPA）

http://www.ipa.go.jp/security/txt/2010/documents/TALOT2-1006.pdf

9415/TCP に対するアクセスの増加について（警察庁）
http://www.npa.go.jp/cyberpolice/detect/pdf/20100615.pdf



【図 5-2：宛先（ポート種類）別アクセス数の比較（7 月/8 月）】



【図 5-3：9415/tcp 発信元地域別アクセス数の変化（10 観測点の合計）】

※6 月 18 日～20 日は保守作業のため、システムを停止しています。

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/2010/documents/TALOT2-1009.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／花村／古川
Tel:03-5978-7527 Fax:03-5978-7518
E-mail: isec-info@ipa.go.jp