Information-technology
Promotion
Agency, Japan

プレスリリース
第 11-34-232-1 号
最終更新日：2011 年 11 月 18 日
掲載日：2011 年 11 月 4 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 10 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 10 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

「 ファイル名に細工を施されたウイルスに注意！ 」
～見た目でパソコン利用者をだます手口～

2011 年 9 月、IPA に RLTrap というウイルスの大量の検出報告（約 5 万件）が寄せられました。このウイルスには、パソコン利用者がファイルの見た目（主に拡張子）を誤認し実行してしまうように、ファイル名に細工が施されています。このような手法は決して新しいものではなく、2006 年頃には既に確認されていました。

ここでは、このような手法にだまされてウイルスに感染しないように、ファイル名偽装の手口を解説するとともに、ウイルス感染の被害を未然に防ぐための対策を紹介します。

（1）ファイル名偽装の手口

この手口は、Unicode の制御文字を利用してファイル名の拡張子を偽装し、危険なファイルを安全な別の種類のファイルだと思わせます。Unicode とは、世界中の言語を単一の文字コードで取り扱う目的で作られた規格のことです。制御文字とは、文字コードで定義される文字ですが画面には表示されず、プリンタや通信装置などを制御するために使われるものです。

ここで使われる制御文字は RLO（Right-to-Left Override）というものです。この制御文字は、ファイル名の文字の並びを［左→右］から、［右→左］に変更します。この機能は、日本語や英語に代表される、文字を左から右に読ませる言語とは逆に、右から左に読ませる言語（アラビア語など）を使用する際に用いられます。

RLO の使用例を簡単に説明します。ここに「ABCDEF.doc」という名前のファイルがあるとします。このファイル名の先頭の「A」の前に RLO を挿入します（RLO 自体は目に見えません）。するとファイル名は拡張子も含めて文字の並びが右方向から左方向に変更され、ファイル名の見た目が「cod.FEDCBA」に変わります（図 1-1 参照）。

図 1-1：RLO の使用例の図

この機能を悪用することで、「exe」形式のファイルを「pdf」形式のファイルに偽装することが可能

になります。

（2）実際に使われたウイルスメール

IPA が確認したウイルスメールを紹介します。ウイルスは ZIP 形式で圧縮されて、図 1-2 のようなメールの添付ファイルとして送られていました。

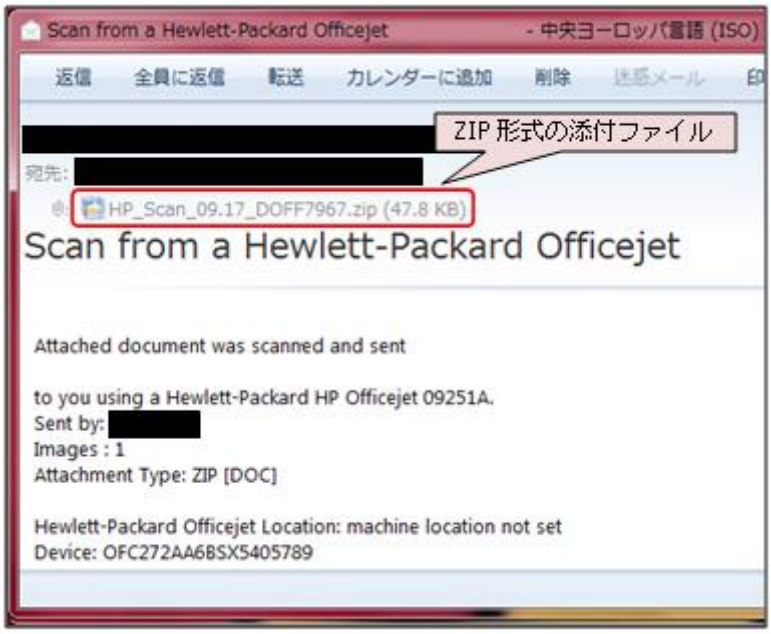

図 1-2：実際に使われたウイルスメールの本文

図 1-2 の添付ファイル（圧縮ファイル）を解凍すると、「HP_SCAN_FORM_N90952011___Collexe.pdf」というファイル名に偽装した「exe」形式のファイルが作成されます（図 1-3 参照）。

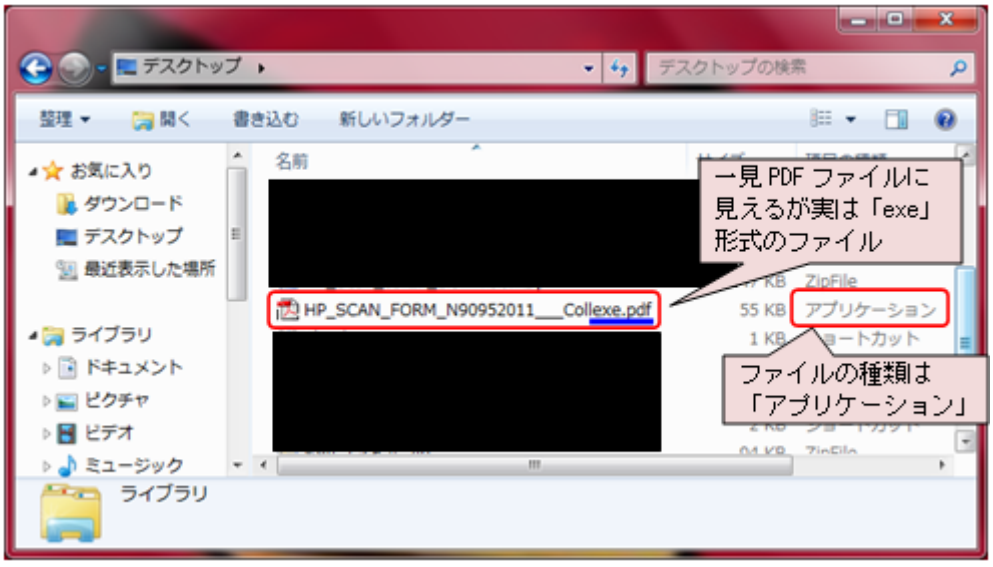

図 1-3：ウイルスメールの添付ファイルの中のファイルの表示例

なお、圧縮・解凍ソフトによっては、中のファイルが意図したとおりに表示されない場合がありました。図 1-4 は、その際の表示例です。

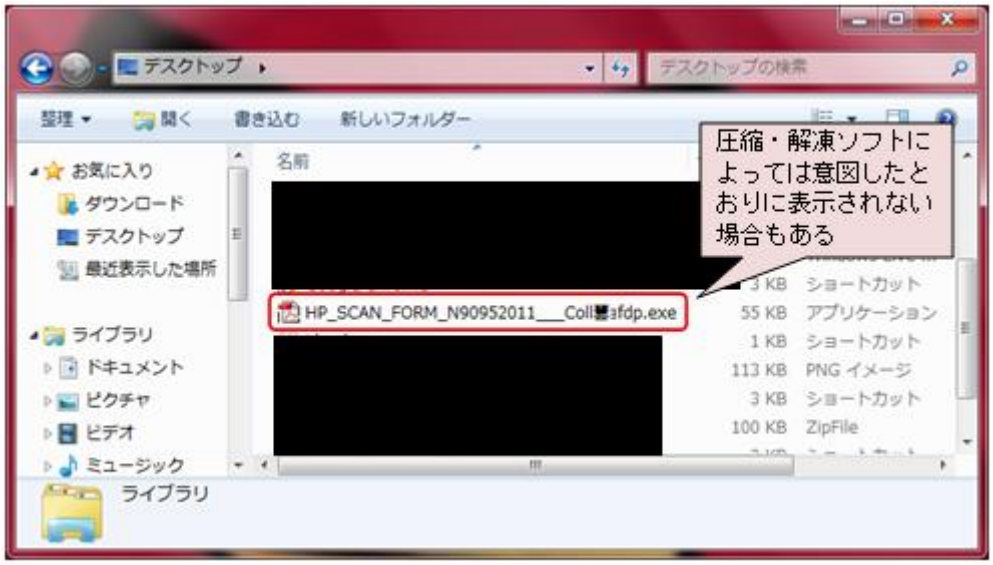

図 1-4：添付ファイルの中のファイルが意図したとおりに表示されなかった表示例

（3）RLTrap ウイルスの解析結果（ウイルスの動作概要）

IPA では RLTrap ウイルスの解析を行いました。解析の結果、このウイルスは Windows 7 環境でのみ動作し、感染すると以下の動作を行うことを確認しました。

・ロシアのあるウェブサイトと通信を試みます。ただし、解析を行った時点では既に当該サイトは存在しておらず、通信は行われませんでした。**通信が行われた場合、別のウイルスをダウンロードして感染させる可能性があります。**

・ウイルスは Windows の特定のフォルダに「csrss.exe」という名前で自身のコピーを作ります。

・ウイルスは一度実行すると、実行された自身のファイルを削除します。

（4）対策

ウイルス感染の被害を未然に防ぐための対策としては、「ウイルス対策ソフトの活用」と「脆弱（ぜいじゃく）性対策」の二点が基本的な対策になりますので、必ず実施してください。

【i】ウイルス対策ソフトの活用

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、侵入したウイルスの駆除ができます。ウイルス対策ソフトが導入済であればメール受信時や添付ファイル保存時、またはファイルを開く際にウイルスとして検出することができます。

【ii】脆弱性対策

Windows などの OS や、アプリケーションの脆弱性を解消しておくことが重要です。一般的に利用者の多いアプリケーションは狙われやすい傾向にあるため、脆弱性を解消して、常に最新の状態で使用してください。IPA では利用者のパソコンにインストールされているソフトウェア製品のバージョンが最新であるかを、簡単な操作で確認するツール「MyJVN バージョンチェッカ」を公開しています。

（ご参考）

MyJVN バージョンチェッカ（IPA）

http://jvndb.jvn.jp/apis/myjvn/vccheck.html

【iii】RLO を悪用するウイルスへの対策

上述した基本的な対策に加え、以下に示す対策を行うことで、今回のように Unicode 制御文字を悪用したウイルスの感染を未然に防ぐことができます。その手順を Windows 7 を例に解説します。

なお、この対策は、Windows のエディションによっては使用できない場合があります。

（手順 1）

スタートメニューの下部に「secpol.msc」と入力し、Enter キーを押す（図 1-5 参照）。なお、

Windows XP の場合は、スタートメニューから「ファイル名を指定して実行（R）」をクリックし、表示された画面の名前（O）の欄に「secpol.msc」と入力し、Enter キーを押します。Windows Vista の場合は、Windows 7 の場合とほぼ同様です。

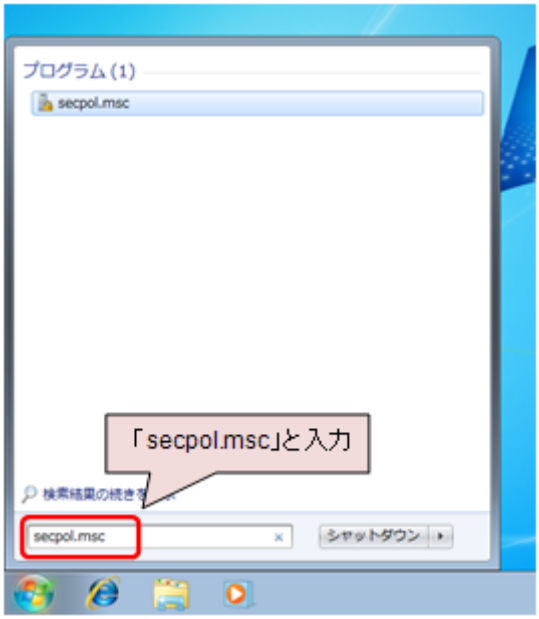

図 1-5：RLO 対策手順 1

（手順 2）

ローカルセキュリティポリシーの画面が出たら、左部の「ソフトウェアの制限のポリシー」を右クリックし、表示されたメニューから「新しいソフトウェアの制限のポリシー（S）」をクリック（図 1-6 参照）。なお、Windows XP および、Windows Vista の場合もほぼ同様です。

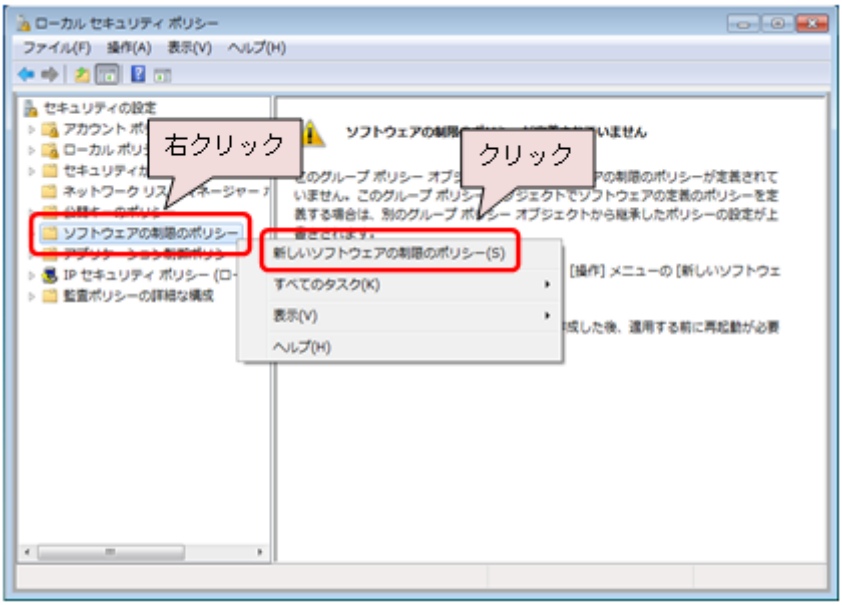

図 1-6：RLO 対策手順 2

（手順 3）

ローカルセキュリティポリシーの画面の右部の「追加の規則」を右クリックし、表示されたメニューから「新しいパスの規則（P）…」をクリック（図 1-7 参照）。なお、Windows XP および、Windows Vista の場合もほぼ同様です。

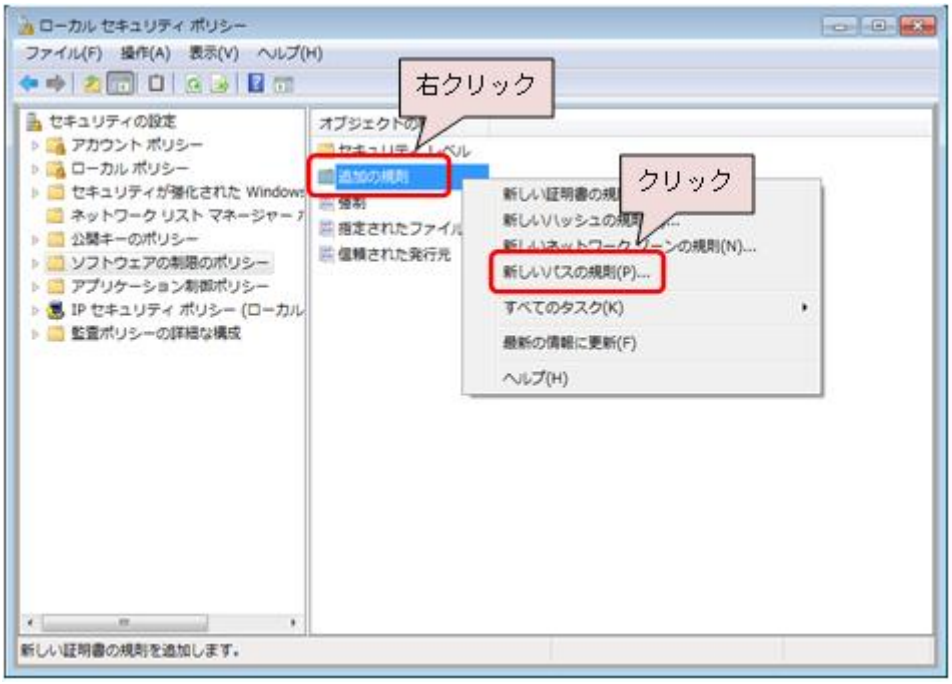

図 1-7：RLO 対策手順 3

（手順 4）

「新しいパスの規則」の画面が出たら、パス（P）の欄に「**」（アスタリスク 2 つ）を入力し、「*」と「*」の間にカーソルを合わせ右クリックし、表示されたメニューから「Unicode 制御文字の挿入」→「RLO Start of right-to-left override」を選択します。（図 1-8 参照）。なお、Windows XP および、Windows Vista の場合もほぼ同様です。

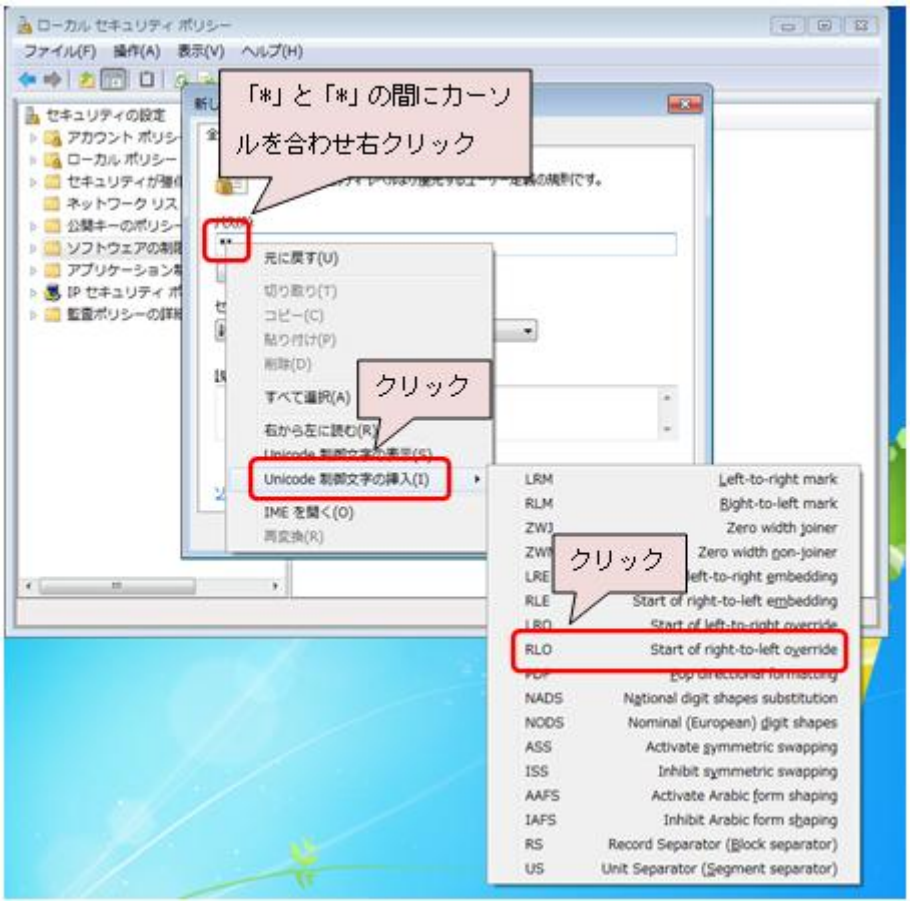

図 1-8：RLO 対策手順 4

（手順 5）

セキュリティレベル（S）の欄が「許可しない」になっていることを確認して、OK ボタンをクリック（図 1-9 参照）。なお、Windows XP および、Windows Vista の場合もほぼ同様です。

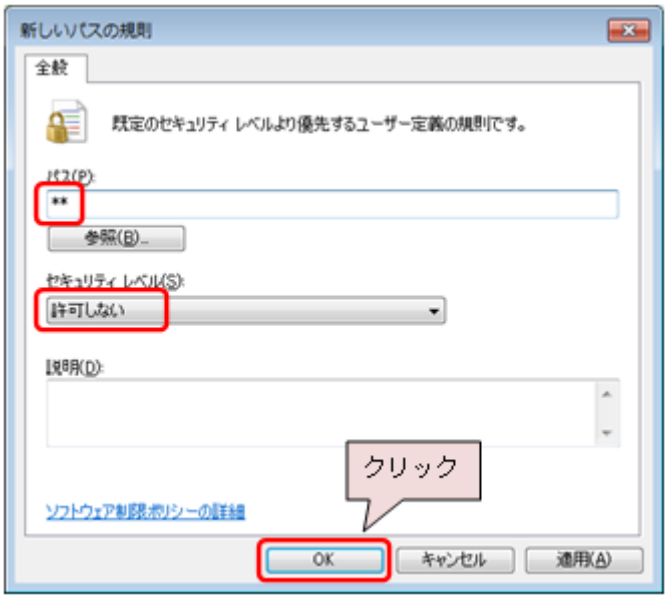

図 1-9：RLO 対策手順 5

（手順 6）

パソコンを再起動する。

上記対策を行うことで、RLO を使ってファイル名に細工が施されたファイルをクリックすると、図 1-10 のような警告メッセージが表示され、実行が制限されるようになります。

なお、この対策は組織のグループポリシーとして、組織内のパソコン全体を保護する場合でも有効です。

ここで紹介した対策は、文字を［右→左］の順番で読む言語を扱うパソコンには適用しないでください。

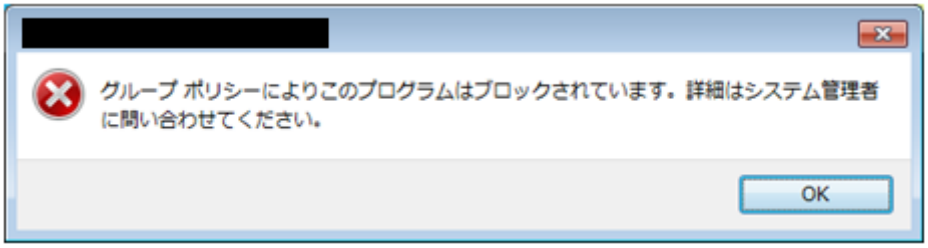

図 1-10：RLO 対策を行った状態でファイル名に細工が施されたファイルをクリックした場合に表示される警告メッセージ例（Windows 7 の場合）

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、9 頁の「3.コンピュータ不正アクセス届出状況」を参照）

・ウェブサイトのトップページが改ざんされていた

・メールアカウントに不正にログインされ、迷惑メール送信の踏み台として使われた

○ 相談の主な事例 （相談受付状況および相談事例の詳細は、11 頁の「4.相談受付状況」を参照）

・某書籍販売会社のウェブサイトからウイルスに感染した

・購入して間もないパソコンにウイルスが感染した

○ 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

10 月のウイルスの検出数※1 は、**20,409 個**と、9 月の 21,291 個から 4.1%の減少となりました。また、10 月の届出件数※2 は、**795 件**となり、9 月の 906 件から 12.3%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。
・10 月は、寄せられたウイルス検出数 20,409 個を集約した結果、795 件の届出件数となっています。

検出数の 1 位は、**W32/Netsky** で **11,079 個**、2 位は **W32/Mydoom** で **7,227 個**、3 位は **W32/Autorun** で **439 個**でした。

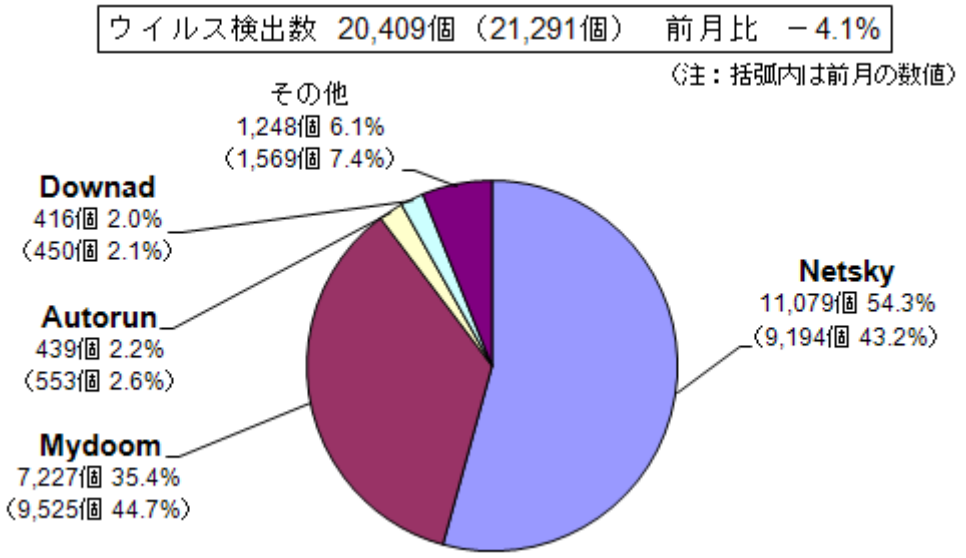

図 2-1：ウイルス検出数

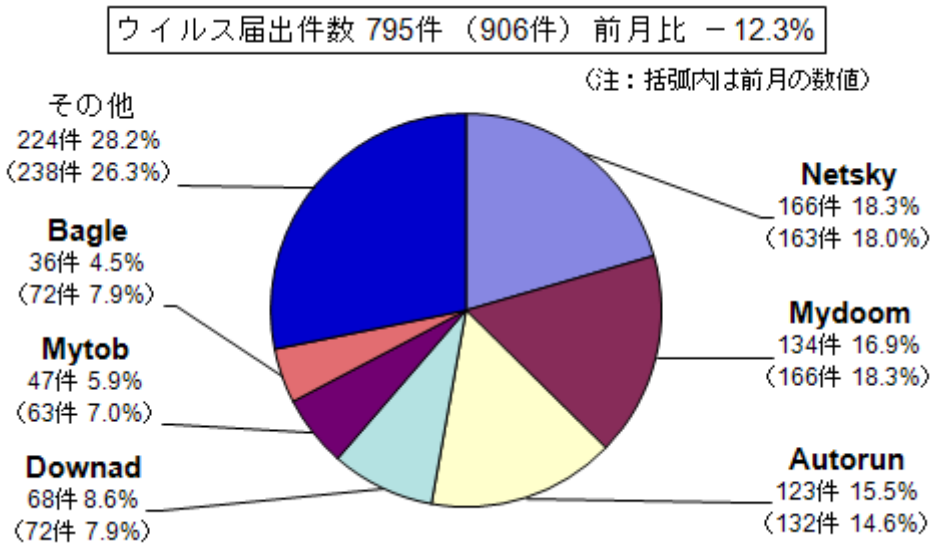

図 2-2：ウイルス届出件数

（2）不正プログラムの検知状況

10 月は、特に目立った動きはありませんでした。また、9 月に大幅に増加した RLTRAP は、10 月後半に 1 日だけ多く検知された日がありました（図 2-3 参照）。

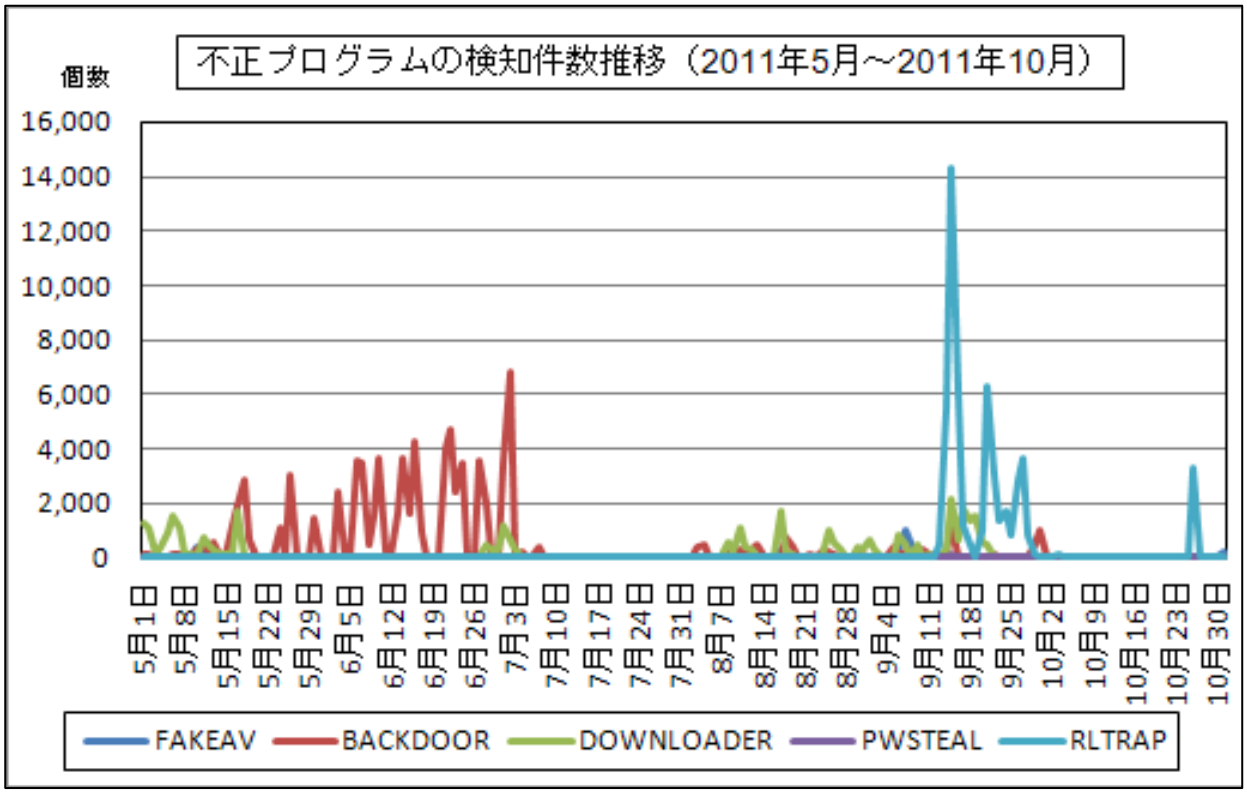

図 2-3：不正プログラムの検知件数推移

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

		5月	6月	7月	8月	9月	10月
届出(a) 計		7	9	8	10	7	15
	被害あり(b)	6	9	5	8	5	8
	被害なし(c)	1	0	3	2	2	7
相談(d) 計		55	32	47	37	31	46
	被害あり(e)	14	7	15	13	8	7
	被害なし(f)	41	25	32	24	23	39
合計(a+d)		62	41	55	47	38	61
	被害あり(b+e)	20	16	20	21	13	15
	被害なし(c+f)	42	25	35	26	25	46

（1）不正アクセス届出状況

10 月の届出件数は 15 件であり、そのうち**何らかの被害のあったものは 8 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 46 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 4 件、なりすまし 3 件、DoS 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 3 件、データベースから個人情報が盗まれたものが 1 件、でした。侵入の原因は、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、WebDAV 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、本人になりすまして何者かにログインされ、勝手にスパムメールを送信されたものが 3 件でした。

（4）被害事例

［侵入］

（i）ウェブサイトのトップページが改ざんされていた

事例	・当組織のウェブサイトのトップページが、何者かによって書き換えられた。 ・被害サーバー上で WebDAV※機能を使っていたが、保護領域の設定にミスがあり、結果的に誰でもファイルをアップロードできる状態だった。 ・ファイアウォールおよび侵入検知装置は設置していたが、サーバーは担当部門ごとに管理を一任しており、今回の被害サーバーについては特に対策は講じていなかった。

解説・対策	WebDAV 設定不備によるウェブ改ざん被害が後を絶ちません。外部に向かってサービスを公開する場合、アクセス制限の設定には細心の気配りが必要です。WebDAV に限らず、全ての機能やサービスについて定期的な棚卸しを勧めます。**現状にそぐわない設定の修正**や、**不要な機能の削除**等、公開サーバーの管理者は常にセキュリティ向上に努めてください。 また IPA では、ウェブサイト攻撃を検出するツールとして「iLogScanner」を提供していますので、活用されることをお勧めします。 （ご参考） IPA - 安全なウェブサイトの作り方 http://www.ipa.go.jp/security/vuln/websecurity.html IPA -ウェブサイト攻撃の検出ツール iLogScanner V3.0 http://www.ipa.go.jp/security/vuln/iLogScanner/

WebDAV※：HTTP を拡張し、ウェブブラウザからウェブサーバー上のファイルやフォルダの編集やバージョン管理などができるようにした仕組みのこと。

［なりすまし］

（ii）メールアカウントに不正にログインされ、迷惑メール送信の踏み台として使われた

事例	・学生と職員向けサービスとして、インターネットから利用可能なウェブメールシステムを学内で運用している。 ・ウェブメール利用者の一人の学生によって、迷惑メールが大量に送信されていることを検知した。 ・当該学生に確認したところ、自分はスパムメールを送信していない、との回答だった。しかしその後の調査で、当該学生がウェブメール画面を模したフィッシングサイト（偽サイト）に ID とパスワードを入力したことがある事実が判明した。 ・事後対策として、当該学生のウェブメールのパスワードを変更した上で一時利用停止とし、改めて全学内にフィッシングに対する注意喚起を実施した。
解説・対策	当該学生がどのようにして偽サイトに誘導されたのかが不明ですが、パスワード等の重要な情報を入力する際、常にそのサイトが正当なものかを確認するようにしていれば、防げた可能性があります。 （ご参考） IPA – フィッシング対策 http://www.ipa.go.jp/security/personal/protect/phishing.html また最近、**ウイルスを用いる新しい手口のフィッシング詐欺**が出現しました。実際にこの手口により銀行口座から総額数百万円を引き出される被害が発生しています。金融機関等から来たと思われるメールでも、内容を慎重に確認するようにしてください。特に、**カード番号や暗証番号を入力するような依頼がメールで届くことはないと考えてください**。 （ご参考） IPA -2011 年 10 月の呼びかけ「ウイルスを使った新しいフィッシング詐欺に注意！」 http://www.ipa.go.jp/security/txt/2011/10outline.html

4. 相談受付状況

10 月のウイルス・不正アクセス関連相談総件数は **1,496 件**でした。そのうち**『ワンクリック請求』に関する相談**が **419 件**（9 月：477 件）、**『偽セキュリティソフト』**に関する相談が **7 件**（9 月：2 件）、**Winny に関連する相談**が **12 件**（9 月：19 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 **9 件**（9 月：2 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

		5月	6月	7月	8月	9月	10月
合計		1,640	1,692	1,490	1,651	1,551	1,496
	自動応答システム	950	999	889	958	936	865
	電話	620	639	540	639	554	564
	電子メール	62	50	54	50	52	55
	その他	8	4	7	4	9	12

※ 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。

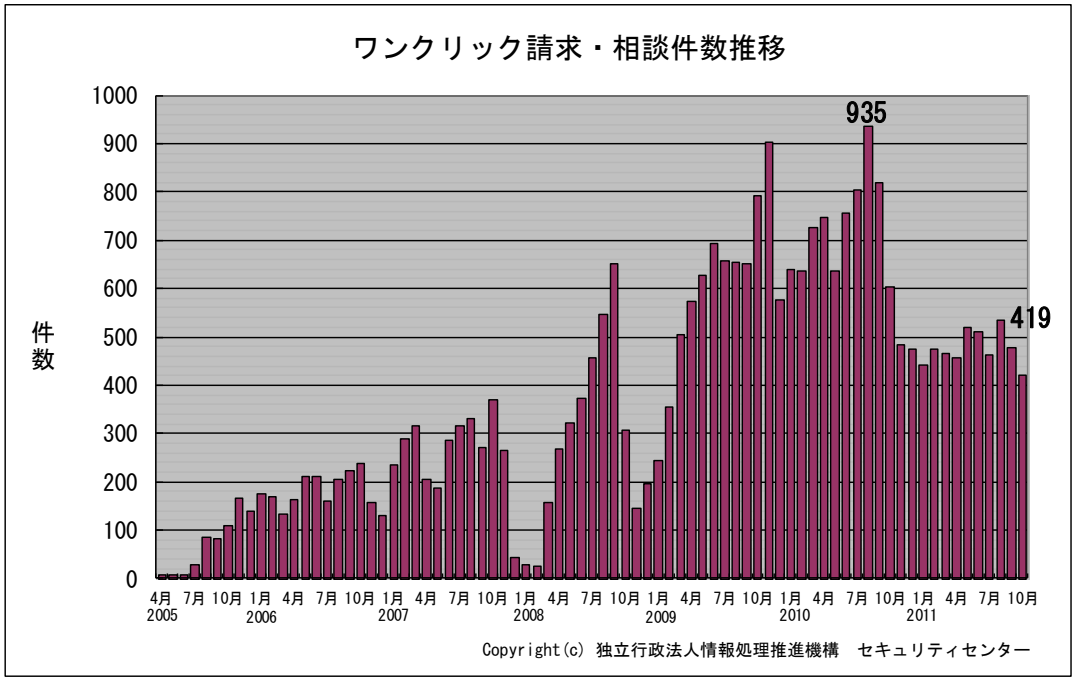

図 4-1：ワンクリック請求相談件数の推移

主な相談事例は以下の通りです。

（i）某書籍販売会社のウェブサイトからウイルスに感染した

相談	某書籍販売会社のウェブサイトを閲覧していたら、パソコンがウイルスに感染してしまい、偽のセキュリティソフトが立ち上がるようになってしまった。 大手の会社のウェブサイトであっても、こういった被害に遭う危険があるのか。一般利用者は、こういった被害に遭わないようにするためにどういったことに注意すればいいのか。
回答	この件は、セキュリティ関連のニュースサイトでの報道をこちらでも確認しています。このように企業のウェブサイトが外部からの不正アクセスで改ざんされることにより、**閲覧者にウイルスを感染させる仕掛けを埋め込まれるといった被害は数年前から後を絶ちません**。 一般利用者がこのような改ざんされたウェブサイトからのウイルス感染の被害に遭わないためには、**ウイルス対策ソフトを常に最新の状態にして使う**ことと、**OS やアプリケーションの脆弱性を解消しておく**などの基本的な対策が有効です。 （ご参考） 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

（ii）購入して間もないパソコンにウイルスが感染した

相談	購入して間もないパソコンを使っていたら、いつのまにか見覚えのないセキュリティソフトが立ち上がるようになってしまった。 よくよく考えてみると、最初の WindowsUpdate の作業が全て終わらないうちに、インターネットでウェブサイトを閲覧していたが、それがいけなかったのか。
回答	WindowsUpdate の作業が終わらないうちに、悪意あるウェブサイトを閲覧してしまったために、未解消の脆弱性を悪用されてウイルスに感染してしまったと思われます。 購入して間もないパソコンを使用する際は、**必ず全ての更新プログラムの適用を終え、ウイルス対策ソフトを最新の状態に更新してから**、他の作業を行うことをお勧めします。 感染してしまった場合の対処については、以下のページを参考にしてください。 （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

5. インターネット定点観測での 10 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 10 月の期待しない（一方的な）アクセスの総数は 10 観測点で **109,390 件**、延べ発信元数※は **42,844 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 138 の発信元から 352 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。

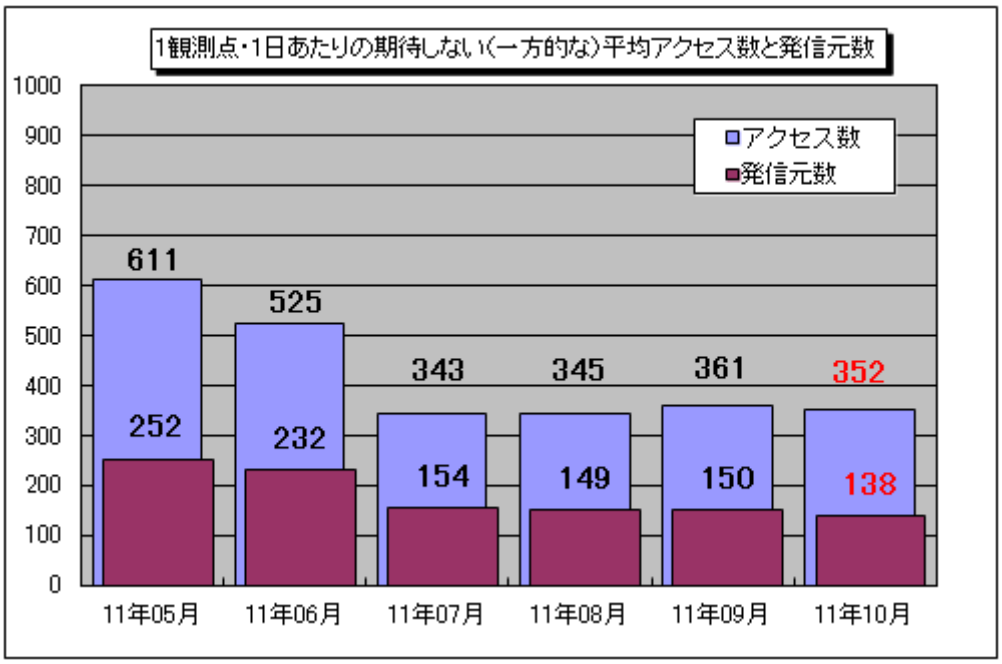

図 5-1：1 観測点・1 日あたりの期待しない（一方的な）平均アクセス数と発信元数

上記グラフは 2011 年 5 月～2011 年 10 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示しています。10 月の期待しない（一方的な）アクセスは、9 月とほぼ同程度でした。

9 月と 10 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。これを見ると 445/tcp へのアクセスが大きく減少した一方で、51499/udp、80/tcp、および 8612/udp などへのアクセスの増加が見られました。

51499/udp、および 8612/udp については、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が、ともに特定の 1 観測点のみで観測されていました。

80/tcp については、10 月の後半に TALOT2 の複数の観測点で、アメリカを筆頭に複数の国の多数の発信元からのアクセスが一時的に増加しました（図 5-3 参照）。80/tcp は、主にウェブアクセスのプロトコルである HTTP が使うポートですが、この時期にアクセスが増加していた原因は不明です。

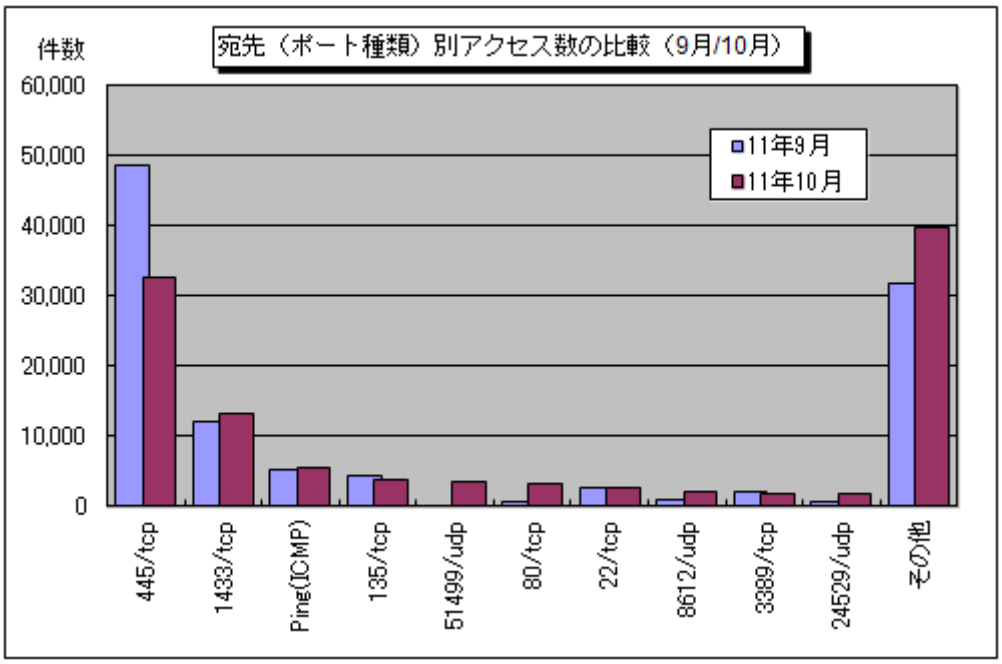

図 5-2：宛先（ポート種類）別アクセス数の比較（9 月/10 月）

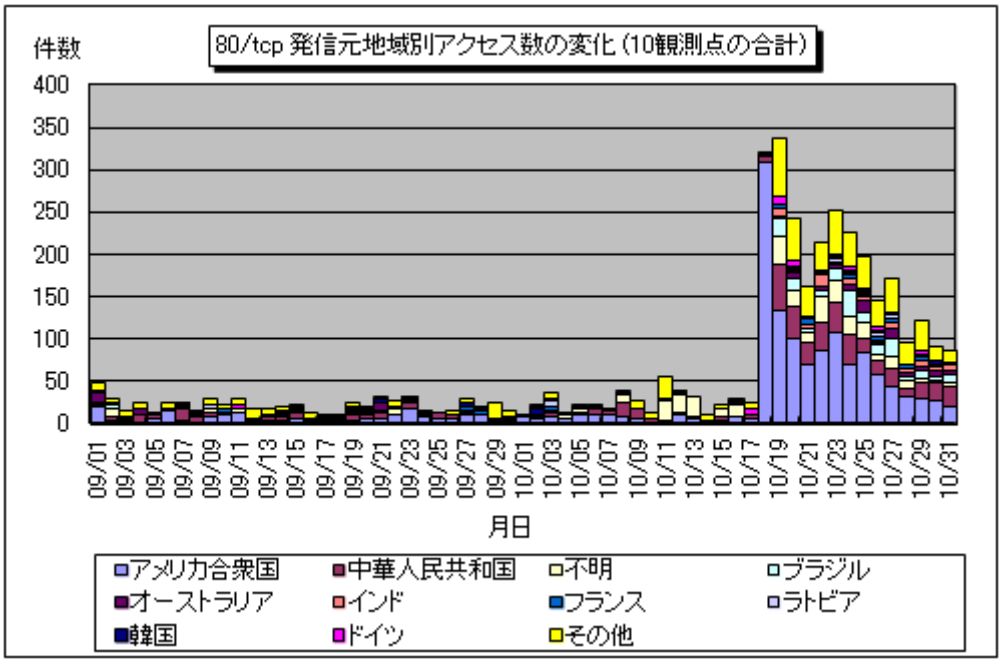

図 5-3：80/tcp 発信元地域別アクセス数の変化（10 観測点の合計）

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/TALOT2-1111.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/
株式会社カスペルスキー：http://www.viruslistjp.com/analysis/

■お問い合わせ先
IPA 技術本部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