IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
第 08-10-125 号
2008 年 6 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［2008 年 5 月分］について

独立行政法人 情報処理推進機構（略称：IPA、理事長：西垣 浩司）は、2008 年 5 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

「 SQL インジェクションによる不正アクセスが多発！ 」
― あなたのウェブサイトも狙われています。対策は十分ですか？ ―

2008 年 3 月頃より、脆弱性※（ぜいじゃくせい）を抱えたウェブサイトを狙った、いわゆる SQL（Structured Query Language）インジェクションと呼ばれる不正アクセスの被害が多発しています。その傾向は 5 月も続いており、IPA にも、この不正アクセスによって情報が漏えいしたり、ウェブサイトが改ざんされてしまったりという届出や相談、改ざんされたウェブサイトの発見報告が相次いで寄せられています。

利用者が、改ざんされたウェブサイトを閲覧することでウイルスに感染させられる場合もあり、SQL インジェクションによる不正アクセスの被害がますます拡大する傾向にあります。

IPA では、これまでも利用者向けに対策の実施を呼びかけてきました。しかし**現時点でも、SQL インジェクションの脆弱性への対応が進んでいないウェブサイトが多く見られるため、利用者にとっては今もなお危険な状況が続いています**。ウェブサイトの開発者や運営者は、この問題の重大性を認識するとともに、脆弱性対策を実施するようお願いします。

※脆弱性（Vulnerability）
一般にソフトウェア等のセキュリティ上の弱点を指します。セキュリティホール（Security Hole）とも呼ばれます。

(1) SQL インジェクションの概要

データベースと連携しているウェブサイトでは、ページを表示するとき、利用者が入力した内容を基にウェブアプリケーションがデータベースにリクエストし、その結果を反映して動的にページを表示する仕組みを利用している場合があります。この時、データベース内の情報の操作に使用されるのが SQL で構成される命令文（SQL 文）です。

もし、ウェブアプリケーションに SQL インジェクションの脆弱性があると、悪意ある者から不正な SQL 文を入れられてしまい、データベース内の情報が不正に操作されてしまいます。この不正アクセス手法のことを、SQL インジェクション攻撃と呼びます。

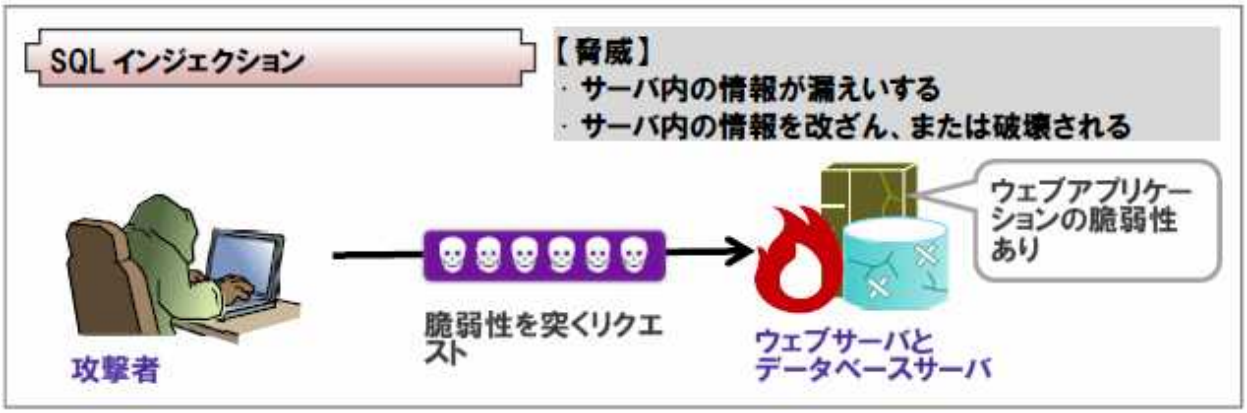

図 1-1：SQL インジェクションの説明 （出典：情報セキュリティ白書 2008）

SQL インジェクション攻撃が成功すると、**悪意ある者がデータベース内の情報を自由に操作することが可能となるため、ウェブサイトのデータベース内の情報の改ざん、消去、漏えいなどの深刻な被害を招く危険性があります。**

ウェブサイトへの攻撃は継続して発生しており、どのサイトでもいつ被害に遭ってもおかしくない状況が続いています。IPA が開発した SQL インジェクション脆弱性検出ツール「iLogScanner」を利用して解析した結果、IPA が管理しているウェブサイトへの攻撃も確認されています。

1. 解析対象のウェブサイト
   ・IPA の OSS iPedia
   (オープンソース情報データベース)
2. 解析したログの期間
   ・2008 年 1 月～5 月
3. 「iLogScanner」の解析結果
   (1) 攻撃があったと思われる件数:99 件
   (2) 攻撃が成功した可能性の高い件数:0 件
4. ログの詳細調査結果
   ・攻撃に成功した件数:0 件

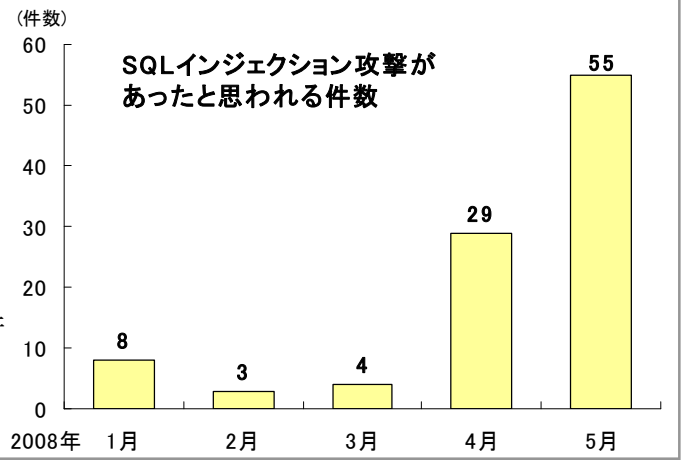

図 1-2:SQL インジェクション脆弱性検出ツール「iLogScanner」の解析事例

最近の報告では、SQL インジェクション攻撃による情報改ざんの結果、ウイルスに感染させることを目的としたウェブページへ誘導する仕掛けが埋め込まれるケースが多数見受けられます。**改ざんされたウェブサイトを閲覧した利用者は、気づかないうちにウイルスに感染してしまう**可能性があり、二次被害が拡大する恐れがあります。

このように、当該ウェブサイトだけの問題に留まらず、**利用者までをも巻き込む被害に発展することになります**。つまり、被害者であると同時に加害者にもなってしまいます。

(2)ウェブアプリケーション開発者の対策

一般的に、ウェブサイトで一度運用開始したサービスを停止するのは難しいですし、ウェブアプリケーション完成後に発覚した脆弱性の修正には多大な費用が掛かります。つまり、ウェブアプリケーションを開発する際は、**設計段階から脆弱性を作り込まないよう、セキュリティに考慮することが最も重要**になります。

ウェブアプリケーション開発を外部委託する場合にも、自組織で開発する場合と同様の対策を実施してください。

以下のサイトを参考にして脆弱性を作り込まないウェブアプリケーションの開発を実施してください。また、必要に応じて、第三者による脆弱性検査を実施することもお勧めします。

(ご参考)
「安全なウェブサイトの作り方」
http://www.ipa.go.jp/security/vuln/websecurity.html
「セキュア・プログラミング講座」
http://www.ipa.go.jp/security/awareness/vendor/programmingv2/

(3) ウェブサイトの運営者の対策

(i) 不正アクセスを防止するための事前対策

SQL インジェクションによる不正アクセスを可能な限り防止するための基本的対策として、以下の対策を実施してください。

(a)ウェブサーバの基本ソフト(OS)、インストールされているアプリケーションソフトなどを常に最新の状態にすることで、脆弱性を解消しておく。

(b)新たなサービスを公開する前に、セキュリティ監査でウェブサイト内に潜む脆弱性をあぶり出し、必要があれば修正しておく。

(ご参考)

情報セキュリティ監査企業台帳

http://www.meti.go.jp/policy/netsecurity/is-kansa/

(ii) 不正アクセスを発見するための運用対策

不正アクセスによる**被害を最小限にするために一番重要なことは、不正アクセスを早期に発見すること**です。そのためには、以下のような対策を実施することをお勧めします。

(a)ウェブサイトのリアルタイム監視を実施することで、ウェブページ、アクセスログ、データベースなどが改ざんされていないか逐一確認する。その手段として、改ざん検知ツールの導入が有効。

(b)侵入検知のため、IDS※あるいは IPS※を導入する。最近では、ウェブアプリケーションの通信監視に特化した WAF※といった製品もある。
もし、自組織で運用できない場合は、外部業者にアウトソーシングすることも考慮する。

(c)ウェブサイトを定期的に監査し、新たな脆弱性が無いかを確認する(新種の攻撃手法が発見される場合もあるため)。

※IDS: Intrusion Detection System、IPS: Intrusion Prevention System、WAF: Web Application Firewall

(ご参考)

IPA では、SQL インジェクション攻撃の痕跡を検出するツール「iLogScanner」を公開しています。このツールを利用し、管理するウェブサイトに問題が発生していないか確認することができます。

ウェブサイトの脆弱性検出ツール iLogScanner

http://www.ipa.go.jp/security/vuln/iLogScanner/

(iii) 不正アクセスの被害が発生した場合の事後対策

被害状況や影響範囲を確認するとともに、SQL インジェクションによる不正アクセスの原因箇所を特定して、修正してください。すぐに修正が難しい場合には、ウェブサイト公開の一時停止の検討をお勧めします。

注:被害状況の把握や復旧には、専門的な知識や技術が必要になりますので、自組織での対応が無理な場合は、情報セキュリティの専門企業へ調査を依頼しましょう。

データベースに個人情報を格納している場合、それらが漏えいした可能性があります。漏えいした個人情報の範囲の特定や顧客・取引先への対応が必要です。

なお、ウェブサイトが改ざんされた結果、ウイルスに感染させるページへのリンクが入れられていた場合には、当該ウェブサイトを閲覧した利用者にウイルス感染被害が拡大している可能性があります。ウイルスに感染したことに気付かない利用者も存在すると推測されるため、感染する危険性があった日時や感染の有無のチェック方法などを、**ウェブサイトなどを通じて告知することが望まれます**。

(ご参考)
「知っていますか？脆弱性(ぜいじゃくせい)―アニメで見るウェブサイトの脅威と仕組み―」
http://www.ipa.go.jp/security/vuln/vuln_contents/
「ウェブサイト運営者のための脆弱性対応ガイド」
http://www.ipa.go.jp/security/fy19/reports/vuln_handling/
「JVN iPedia 脆弱性対策情報データベース」
http://jvndb.jvn.jp/

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(届出状況及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)
・SQL インジェクション攻撃によってデータベースが改ざんされた
・ネットオークションで、誰かが自分になりすまして勝手に出品

○ 相談の主な事例 (相談受付状況及び相談事例の詳細は、8 頁の「4.相談受付状況」を参照)
・自分の USB メモリを他人のパソコンに挿したらウイルスが検知された
・自分で出していないはずのメールが、宛先不明のエラーメールとして戻って来る

○ インターネット定点観測(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。
・22/tcp を狙ったアクセスに注意！

2. コンピュータウイルス届出状況　－詳細は別紙 1 を参照－

ウイルスの検出数(※1)は、**約 20 万個**と、4 月の約 20.6 万個から 3.3%の減少となりました。
また、5 月の届出件数(※2)は、**1,737 件**となり、4 月の 1,703 件から微増となりました。

※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。
・5 月は、寄せられたウイルス検出数約 20 万個を集約した結果、1,737 件の届出件数となっています。

検出数の1位は、**W32/Netsky で約 18 万個 、2 位は W32/Mywife で約 6 千個、3 位は W32/Mytob で約 4 千 7 百個でした。**

ウイルス検出数　約20万個（約20.6万個） 前月比 － 3.3%

（注：括弧内は前月の数値）

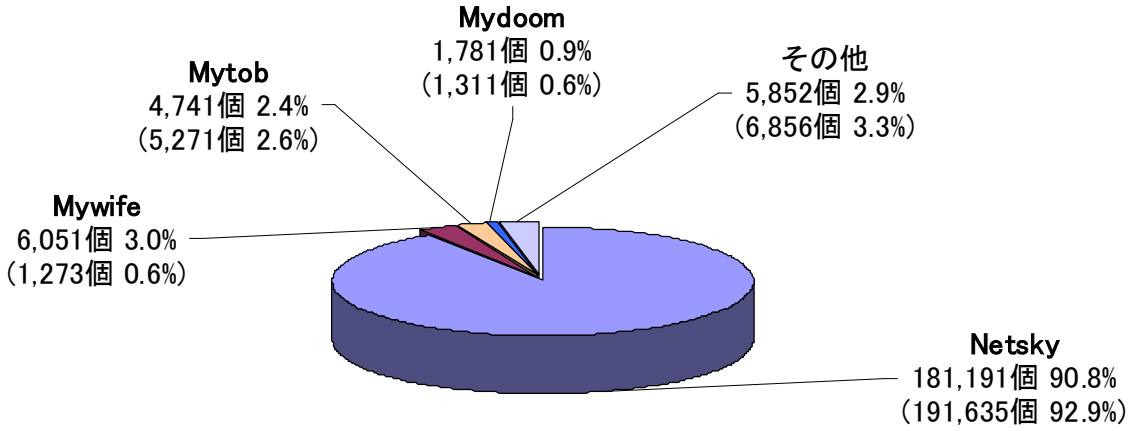

図 2-1

ウイルス届出件数　1,737件（1,703件） 前月比 ＋ 2.0%

（注：括弧内は前月の数値）

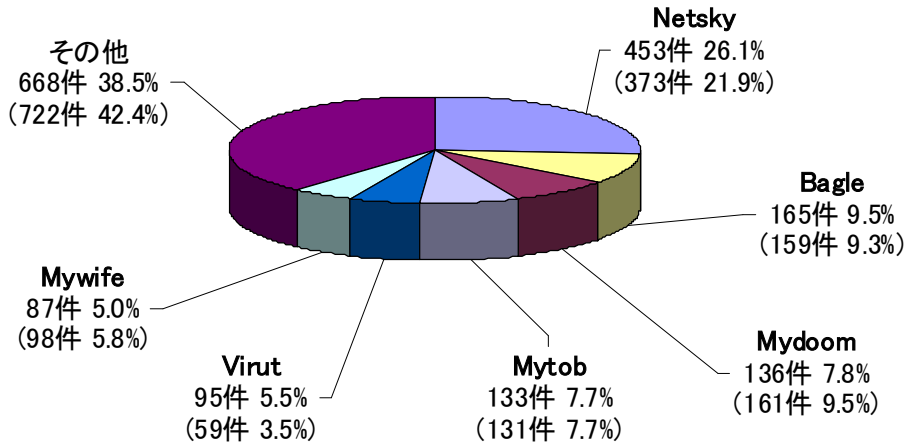

図 2-2

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

		12月	1月	2月	3月	4月	5月
届出(a) 計		14	8	4	19	14	4
	被害あり(b)	7	7	4	13	10	4
	被害なし(c)	7	1	0	6	4	0
相談(d) 計		21	24	29	35	56	37
	被害あり(e)	16	15	10	15	31	18
	被害なし(f)	5	9	19	20	25	19
合計(a+d)		35	32	33	54	70	41
	被害あり(b+e)	23	22	14	28	41	22
	被害なし(c+f)	12	10	19	26	29	19

(1) 不正アクセス届出状況

5 月の届出件数は 4 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 37 件であり、そのうち何らかの被害のあった件数は 18 件でした。

(3) 被害状況

被害届出の内訳は、**侵入 2 件、DoS 攻撃が 1 件、その他（被害あり）1 件**でした。

侵入届出の被害は、SQL インジェクション攻撃を受けて結果としてウェブページコンテンツを改ざんされてしまったものが 1 件、サーバの遠隔操作ソフトを悪用されて外部から不審なファイルを埋め込まれてしまったものが 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によるものが 1 件、ルータの設定不備によるものが 1 件でした。

その他（被害あり）の被害として、ネットオークションサイトに本人になりすまして何者かにログインされ、勝手に商品を出品されていたものが 1 件ありました。

（4）被害事例

［侵入］

（i）SQL インジェクション攻撃によってデータベースが改ざんされた

事例	・自組織で管理しているサイトは、https による暗号化通信で閲覧するように運用していた。ある日、同サイトにアクセスした際、「セキュリティで保護されていない項目があります。表示しますか？」と警告が出た。つまり、暗号化されていない、通常の http による通信も行われているということ。 ・調査したところ、自組織で管理しているサイトへの https によるアクセス時、同時に他の外部サイトへの http によるアクセスも発生していたことが判明。 ・さらなる調査の結果、ウェブサーバで動かしていた、データベースにアクセスするためのウェブアプリケーションに SQL インジェクションの脆弱性があったことが判明。脆弱性を突かれた SQL インジェクション攻撃により、データベース内のデータに悪意あるサイトへのリンク記述が埋め込まれる改ざんをされていたことが分かった（400 万件以上）。 ・**このサイトでは、ウェブページコンテンツはデータベース内のデータを利用して動的に組み立てるようになっていたため、利用者向けに表示していたウェブページ内に、改ざんで埋め込まれた記述も含まれてしまっていた**。その結果、同サイトのページを閲覧した利用者（約 3000 人）は、悪意あるサイトへ誘導されてしまった（前述の http による通信）。 ・脆弱性を解消していないパソコンで悪意あるサイトへ誘導されると、ウイルス感染するようになっていた。
解説・対策	従来、SQL インジェクション攻撃の目的は「侵入」「情報奪取」が多かったのですが、最近はこの事例のように、悪意あるサイトへの誘導のために「改ざん」することも多く見られるようになってきました。**改ざん被害を受けたサイトを閲覧した第三者である利用者がウイルス感染してしまうことで、被害が拡大**しています。**データベースを運用しているウェブサイト管理者は、脆弱性有無の確認と、確実な脆弱性対策をお願いします**。 （参考） ウェブサイトの脆弱性検出ツール iLogScanner http://www.ipa.go.jp/security/vuln/iLogScanner/ IPA － 安全なウェブサイトの作り方 http://www.ipa.go.jp/security/vuln/websecurity.html

（ii）ネットオークションで、誰かが自分になりすまして勝手に出品

事例	・自分の携帯電話に、身に覚えのない「オークション出品確認メール」が届いた。 ・オークションにログインして確認したところ、身に覚えのない商品出品があった。 ・すぐにサイト運営者に通報して対処したため、それ以上の被害は無かった。
解説・対策	**被害を最小限にするには、早い段階で気付くことが必要**です。何らかの手続きをした際、確認メールを受け取れる設定ができるサービスが用意されている場合は、有効に活用しましょう。 （参考） 警察庁 － インターネット安全・安心相談 http://www.cybersafety.go.jp/

4. 相談受付状況

5 月の相談総件数は **1080 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 **320 件**(4 月 :268 件)となり、IPA が集計を始めてから 3 番目に多い結果となりました。その他は、**『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 **1 件**(4 月 :2 件)、**Winny に関連する相談**が **8 件**(4 月 :8 件)などでした。

表 4-1　IPA で受け付けた全ての相談件数の推移

	12月	1月	2月	3月	4月	5月
合計	**389**	**408**	**350**	**654**	**938**	**1080**
自動応答システム	222	219	192	373	514	649
電話	109	151	110	214	335	379
電子メール	56	38	47	66	87	48
その他	2	0	1	1	2	4

※ 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）、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。

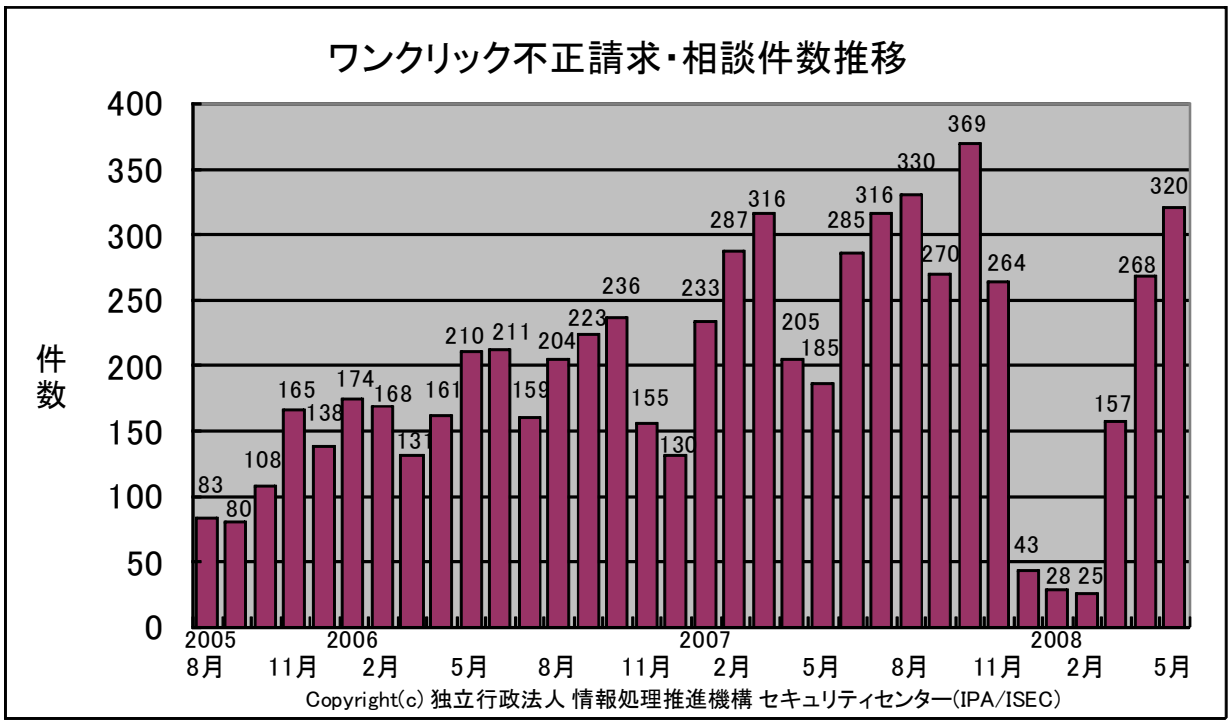

図 4-1　ワンクリック不正請求相談件数の推移

主な相談事例は以下の通りです。

（i）自分の USB メモリを他人のパソコンに挿したらウイルスが検知された

相談	自分のパソコンで使っていた USB メモリを、他のパソコンに挿したらウイルスが検知された（仮に、ウイルス対策ソフトAとする）。慌てて、自分のパソコンに挿し替えてウイルスチェックをしたが、何も検知されない（仮に、ウイルス対策ソフトBとする）。USBメモリ内に、ウイルスがあるのか？ないのか？
回答	**ウイルスかどうかの判断基準は、ウイルス対策ソフトによっては異なる場合があります**。この場合は、ウイルス対策ソフトAではウイルスが検知されているので、「ウイルス感染している」と判断して、駆除作業を実施すべきです。 **怪しいファイルをウイルスチェックする場合は、できる限り多くのウイルス対策ソフトでチェックすることをお勧めします**。「VIRUS TOTAL」は、オンラインで疑わしいファイルを解析してくれるサービスです。無償で、同時に30種類以上のウイルス対策ソフトによるチェックが可能です。 （ご参考） VIRUS TOTAL http://www.virustotal.com/jp/

（ii）自分で出していないはずのメールが、宛先不明のエラーメールとして戻って来る

相談	宛先不明でエラーとなったメールが、数時間のうちに 2000 通以上返送されて来た。差出人メールアドレスは自分のものであるが、名前は他人になっている。メールの内容は、バイアグラを格安で販売するというもの。どうすればいいのか。
回答	何者かが、何らかの方法で入手した貴方のメールアドレスを差出人として名乗り、迷惑メールを大量に配信しているものと思われます。現状では、技術的にはメールの発信自体を止めることはできません。**プロバイダやメールソフト、セキュリティ対策ソフトの迷惑メールフィルタ機能を利用**するのが、現実的な解となります。今回の場合は、返送されて来たエラーメール本文内のエラーメッセージの一部をキーワードとしてフィルタすることが有効と思われます。 **恒久的対策としては、メールアドレスを変更する**ことになります。 （ご参考） 財団法人日本データ通信協会　迷惑メール相談センター http://www.dekyo.or.jp/soudan/

5. インターネット定点観測での 5 月のアクセス状況

インターネット定点観測(TALOT2)によると、2008 年 5 月の期待しない(一方的な)アクセスの総数は 10 観測点で **186,435 件**、総発信元数(※)は **74,936 箇所**ありました。1 観測点で見ると、1 日あたり **242** の発信元から **601 件**のアクセスがあったことになります。

総発信元数(※):TALOT2 にアクセスしてきた発信元の総数。なお、同一発信元から同一観測日・観測点・ポートにアクセスがあった場合は 1 つの発信元としてカウント。

TALOT2 での1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。言い換えれば、**あなたのコンピュータは、毎日、平均して、242 人の見知らぬ人(発信元)から、発信元一人当たり約 2 件の不正と思われるアクセスを受けている**と言うことになります。

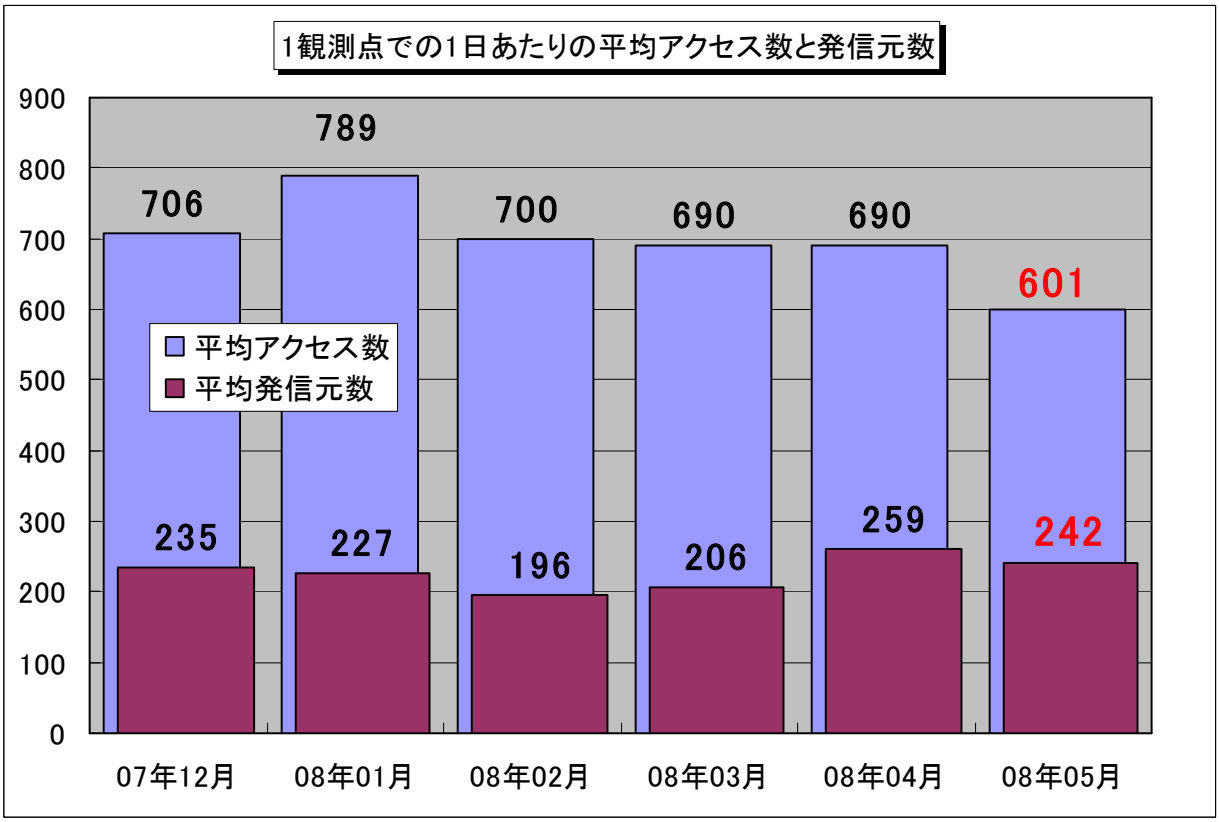

図 5-1: 1 観測点での 1 日あたりの期待しない(一方的な)アクセス数および発信元数

2007 年 12 月～2008 年 5 月までの各月の 1 観測点での 1 日あたりの平均アクセス数および、それらのアクセスの平均発信元数を図 5-1 に示します。この図を見ると、5 月の期待しない(一方的な)アクセスは 4 月と比べて若干減少しており、全体的なアクセスの内容としても、徐々に減少傾向を示していると言えます。

（１）22/tcp ポートを狙ったアクセス

22/tcp へのアクセスは SSH（Secure Shell:通信路を暗号化することで安全性を高めたリモートからのコマンド実行ツール）Server を探し出し脆弱なパスワード認証を破ることを目的としたアクセスであると考えられます。

TALOT2 でメンテナンス用に SSH を利用している観測点(※)の 22/tcp ポートへのアクセスについて 5 月にアクセスが急増している時期がありました。（図 5-2）

(※)：これらのアクセスは特定観測点に対するものであり、統計情報にそぐわない為、集計からは除外してあります。

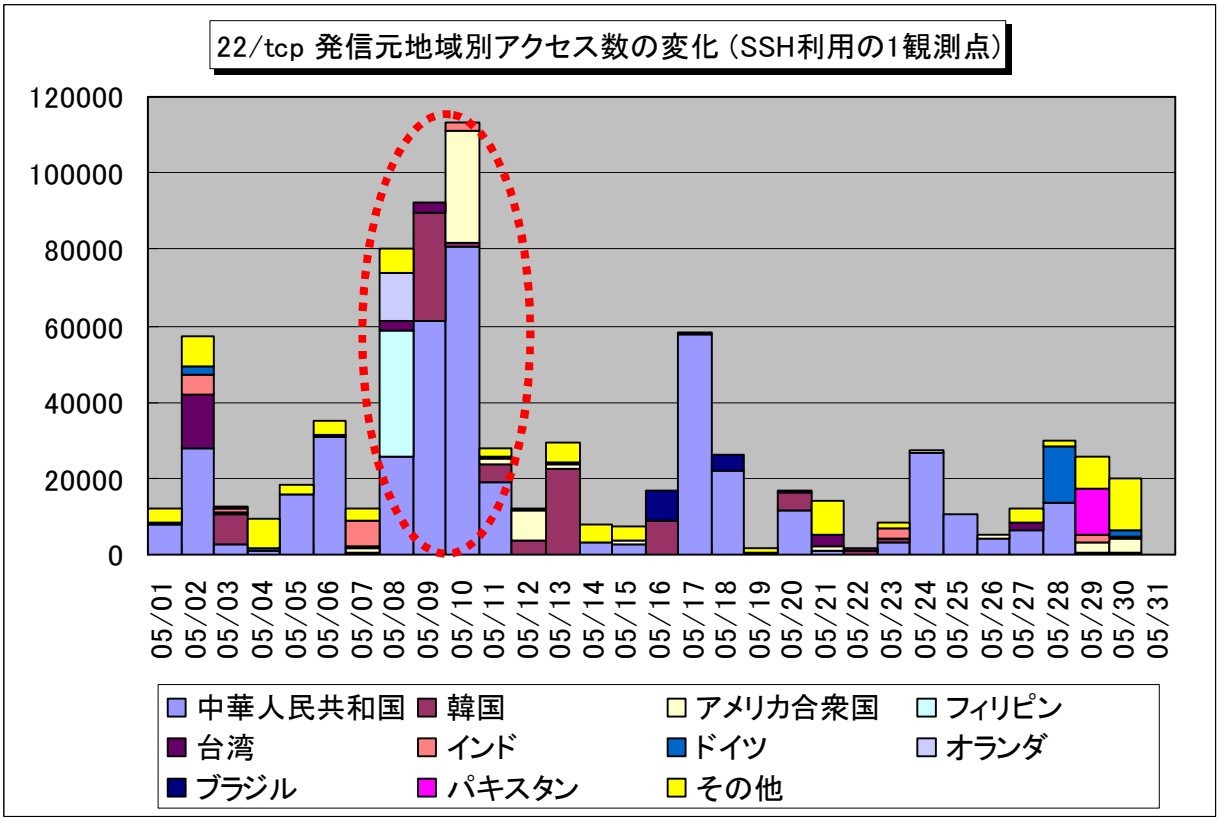

図 5-2： 22/tcp（SSH 利用の 1 観測点）発信元地域別アクセス数の変化

また、5 月の中旬に SSH に関連する脆弱性が見つかっています。この脆弱性は OpenSSL(※1)に予測可能な乱数が生成されるというもので、さらに OpenSSH(※2)にも間接的に影響します。この不具合のある Open SSL パッケージで生成された鍵を使用するアプリケーションにおいて影響があり、影響のあるシステムに対してブルートフォース攻撃(※3)を受けることで鍵情報が推測される可能性があります。

影響を受けるシステムを使用しているサーバ管理者は、ベンダより公開されている最新バージョンへのアップデートと、鍵の再生成をして下さい。

(※1)：OpenSSL グループによる SSL v2/v3 と TLS v1 を実装するオープンソースなツールキットです。

(※2)：OpenBSD グループによる SSH (Secure Shell) プロトコルを実装したクライアント／サーバプログラムです。

(※3)：ブルートフォース攻撃とは、総当り攻撃とも呼ばれ、パスワードを破るためにありとあらゆる解読方法を使用して攻撃する手法です。

（参考資料）

■ JVNVU#925211Debian および Ubuntu の OpenSSL パッケージに予測可能な乱数が生成される脆弱性

http://jvn.jp/cert/JVNVU925211/

■ IPA-情報セキュリティ白書 2007 年版

http://www.ipa.go.jp/security/vuln/20070309_ISwhitepaper.html

以上の情報に関して、詳細はこちらのサイトをご参照ください。

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/2008/documents/TALOT2-0806.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。』

@police：http://www.cyberpolice.go.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

独立行政法人 情報処理推進機構 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