

サイバー攻撃脅威分析レポート 2005 年度版

初版 2006 年 1 月 5 日

株式会社ラック
コンピュータセキュリティ研究所



目次

- 0. はじめに
- 1. エグゼクティブサマリー
- 2. 2005年のキーワード
 - (1) ウェブアプリケーションを悪用した攻撃の脅威
 - (2) ボットネットの脅威
 - (3) 政治的背景による攻撃
 - (4) フィッシングメールや偽のウェブサイトの被害
 - (5) P2P ソフトウェアを介して感染するコンピュータウイルスの被害の増加
- 3. 攻撃傾向分析
 - (1) ワーム/ボットについて
 - (2) ウェブアプリケーションへの攻撃の増加
 - (3) 2005年攻撃傾向のまとめ
- 4. 2006年への傾向予測

0. はじめに

本レポートは、株式会社ラック（以降、ラック）が定期的に発行している、インターネット上の脅威に関する最新レポート（[せきゅふり](#)）の総集編です。

ここでは、2005年に発生したセキュリティ事件・事故について、その攻撃傾向分析、脆弱性の概要などを解説し、最新の情報セキュリティの動向や今後の注意点とともに、それらに対処する推奨策をご紹介します。

本レポートの内容や数値は、2005年1月1日から2005年12月8日の間に、コンピュータセキュリティ研究所の調査・研究結果および、Japan Security Operation Center (JSOC) ^{※1}にて収集した情報を元に記載しております。

¹ JSOC (Japan Security Operation Center) とは、ラックが所有する日本最大級のネットワークセキュリティ専門の監視センターです。日本国内において約 530 センサー (2005 年 11 月現在) を配備し、リアルタイムにセンサーが検知した不正通信を解析することで、日本のネットワークに関する最新の動向を把握しています。

1. 概況

2005 年は、社会的に影響の大きな事件・事故が目立ちました。

その中で代表的なものは e-コマース（電子商取引）サイトからの情報漏洩事件です。この事件の特徴は、従来の単純なホームページ改ざん事件とは異なり、攻撃された企業が、被害者でありながら同時に加害者ともなりうる点です。

具体例として、昨年 5 月以降に多発した事件では、企業のホームページに登録されている個人情報が抜き取られただけでなく、そのホームページを見ただけで悪性プログラム^{※2}を見た人のパソコンに埋め込むよう改ざん^{※3}されてしまい、結果として、被害企業が一般の利用者に対して悪性プログラムをばらまく加害者となり、利用者のユーザ ID やパスワードなどを盗む手伝いをさせられてしまいました。

別の視点から見ますと、犯人が狙うものが、企業の保有する機密情報だけではなく、その企業のホームページを訪れる利用者の機密情報をも対象としている点が特徴として挙げられます。

つまり、犯人は、「いかに効率的に金銭を取得するか」という観点から、知名度があり、かつ信用できる企業のホームページを囮として利用し、訪れた利用者へ悪性プログラムを（見つからないように強制的に）埋め込んで、大量の換金可能な情報を盗み取ろうと考えたものと想定されます。

これら事件の主因としては、ホームページを動かしているウェブアプリケーション^{※4}のセキュリティ上の欠陥を悪用したものであり、セキュリティパッチなどの従来からある対策では防ぐことができないものでした。また、必須のセキュリティ対策項目としても、一般的に知られておりませんでした。

この欠陥が悪用された場合、従来の手口とは異なり、大量の情報流出や、データの改ざんが可能なことから、その被害は甚大なものとなります。さらに、ホームページの復旧には大量のプログラムコードの修正と、改ざんされたすべての DB データの修復が必要となり、多大な時間が必要とされます。

昨今の企業ホームページは、事業活動に密接に関係していることから、復旧に時間的な余裕はなく、場合によっては企業存続上の危機にさらされることもありえます。

この欠陥の抱える最大の問題点は、システムを保有する企業が自身で気がつくケースがほとんどないことから、今後も同様の事件が発生し続ける可能性が高いということです。^{※5}

次に注目すべきキーワードとして、ボット^{※6}と呼ばれる感染型の悪性プログラムがあげられます。ボットが従来のコンピュータウイルスと大きく異なる点は、「攻撃者は、ボットを仕込んだコンピュータを意のままに操れる」ということであり、ボットに感染したコンピュータ群（ボットネット）が、迷惑メール送信、サービス妨害、ネット詐欺等々の犯罪を行う基盤と^{※7}となっていることです。

ボット対策は、ウイルス対策と同様であり、最新のセキュリティパッチを適用し、不要なソフトはインストールせず、ウイルス対策ソフトを導入し機能させておくことなどです。しかし、現実には、100%の対策は困難であることから、ネットワーク的な対策も組み合わせて実施することが必要となります。

2 一連の事件では、個人情報を抜き取り外部へ送信するスパイウェアだった。

3 コンテンツの HTML 内に iframe タグを挿入し、悪意のあるウェブサイトから悪性プログラムをダウンロードされるようにした。

4 主に、ウェブブラウザでデータベースと連携したウェブサーバを利用するための専用アプリケーションを指し、電子商取引などビジネスにも多く利用されている。

5 JSOC での観測では、年々ウェブアプリケーションへの攻撃件数、被害件数ともに増加している。

6 迷惑メールや攻撃の踏み台としてボットの感染ホストが悪用されはじめている。特に US、中国、韓国の感染率が高い。

7 ボットに感染したコンピュータ群は、迷惑メールの踏み台などとしてネット上で取引される。

犯行の動機が、愉快犯的なものから明らかな金銭目的へシフトしてきており、その攻撃の手口は益々巧妙になってきています。昨今の防御技術の進歩が、手口の悪質化を後押ししているのも事実です。その特徴は、以下のようになっております。

- ① 特定の企業を狙うのではなく、持っている道具で侵入できる場所を広く探す。
- ② 持っている道具でどこにも侵入できなくなったら、別な道具を探す。
- ③ 極力、見つからないように、足が付かないよう行動する。
- ④ そのため、見張られている場所にはうかつに近づかない。

今現在、問題が起こっていないので大丈夫だと考えるのは早計です。

企業にとって IT がビジネス基盤となった現在、これらの特徴をよく理解し、防御体制を計画的に構築し、万一事件・事故が発生した場合にそれを検知できる手段を持った上で、臨機応変に対応できるよう準備・検討を行っておくことが求められています。

2. 2005年のキーワード

(1) ウェブアプリケーションを悪用した攻撃の脅威

2005年は個人情報保護法が施行された年でもあり、ウェブアプリケーションのプログラムの欠陥が悪用⁸されたことによる情報漏洩は重要な事件でした。これらの事件の手口多くは、SQL インジェクション⁹と呼ばれる攻撃手法であり、欠陥のあるウェブアプリケーションを利用しているウェブサイトが標的とされます。この攻撃を受けると、攻撃者はウェブサーバをバイパスし、顧客情報が記録されているデータベースに直接アクセスすることが可能となるため、顧客情報が容易に閲覧することができてしまいます。

ラックでは、前回に報告したレポート内でウェブアプリケーションを悪用した攻撃が増加し、今後も増加する懸念があることを報告しました。

(参照 URL : http://www.lac.co.jp/business/sns/intelligence/report/intrusion_trendreport_vol4.zip)

この懸念が現実のものとなり、昨年6月に発行したレポートで、ウェブアプリケーションのプログラムの不備が悪用されウェブサイトから個人情報漏洩する脅威について警告しました。

(参照 URL : http://www.lac.co.jp/news/pdf/CSL_Report20050524.zip)

電子商取引を行っているウェブサイトから、情報漏洩が多発した昨年は、ウェブサイトの運用の難しさや個人情報を取扱う責任の重さやビジネスリスクの大きさを再認識させられました。ウェブアプリケーションの欠陥は、オペレーティングシステムの脆弱性などのようにセキュリティパッチをインストールすることで修正するものではなく、開発者の手により修正しなければなりません。しかし、現在のところ公的機関の定める共通の作成基準はなく、修正作業にも膨大なコストがかかるため、全てのウェブサイトを安全にすることは困難であり、同様のリスクは暫く続くことが懸念されます。

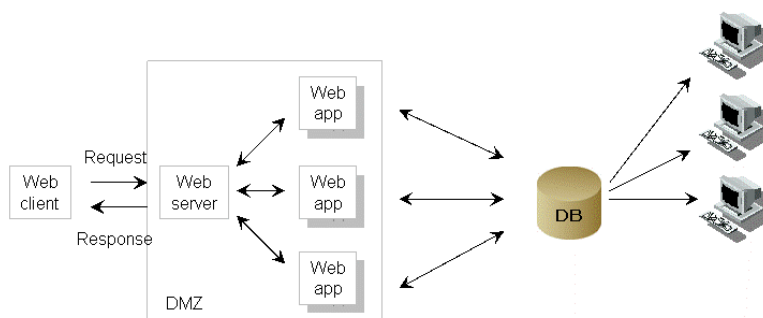


図1 ウェブアプリケーションを利用したウェブサイトの例

⁸ ウェブアプリケーションのプログラム内で、危険な文字列（プログラムの実行を示す文字列など）を含む入力から危険な文字を取り除くようになっていないと、第三者から危険な文字列を入力されてしまう。

⁹ SQL データベースに対して外部から任意のコマンドを与える操作。主に、任意のデータを抽出できてしまう事が問題視され、データベースの設定によってはデータベースのテーブルの追加/削除やユーザの追加などもできてしまう。

(2) ボットネットの脅威

次に注目すべきキーワードとして、ボットと呼ばれる悪性プログラムがあります。悪性プログラムとして代表的なコンピュータウイルスやワームの目的は感染のみでしたが、ボットは感染したコンピュータを悪意のあるユーザが操作可能であることが特徴です。このボットに感染したコンピュータ群が形成するネットワークをボットネットと呼びます。ボットを操作する攻撃者は、ボットに感染したコンピュータを悪用し、第三者に対して攻撃の実行や情報の収集、ボット自身のアップデートさえ可能です。つまり、組織が保有するコンピュータ群がボットに感染してしまった場合、実質組織のネットワークが悪意のあるユーザに乗っ取られてしまったことと同等の意味を持ちます。そのため、感染コンピュータが組織内から発見された場合、コンピュータウイルスよりも重大なインシデントとして扱う必要があります。

(3) 政治的背景による攻撃

中国や韓国と関連性のある日は官公庁を始めとし、海外のネットワークから日本のネットワークに対して攻撃が行われます。特に 2005 年は、小泉首相の靖国参拝や教科書問題をきっかけに官公庁や民間企業のウェブサイトに対して攻撃が行われました。攻撃手法は、大量のトラフィックを発生させることによるサービス妨害攻撃や OS もしくはアプリケーションの脆弱性を狙った侵入行為です。中国のクラッカー集団への参加者の急激な増加に伴い、攻撃件数も増加することが懸念されます。

(4) フィッシングメールや偽のウェブサイトの被害

クレジットカード会社や金融機関などを装った詐称メールを送信し、偽のウェブサイトに誘導させることで個人情報を収集する手口の事件が報告されました。詐称メールによる心理的誘導を行う攻撃は、今後も増加する傾向にあります。現在のアンチウイルスソフトウェアでは防御できないため、注意が必要です。また、偽のウェブサイトも巧妙化しており、一見本物のウェブサイトとは見分けがつかない上に、技術的解決も発展途上のため、現段階では不用意に個人情報の入力をするべきではありません。

(5) P2P ソフトウェアを介して感染するコンピュータウイルスの被害の増加

Winny と呼ばれる P2P ソフトウェア^{*10}を介して感染するコンピュータウイルスによる機密情報の漏洩事件が相次ぎました。Winny は、コンピュータ同士が 1 対 1 で通信を行ううえに、暗号化通信を用いるため、Winny の使用の抑制は困難です。また、コンピュータウイルスに感染し、機密情報が外部に漏洩した際も、Winny の仕様上の理由により被害範囲の特定が困難です。P2P 関連の事件・事故は今後も増加する傾向にあり、組織の管理能力が問われています。

¹⁰ 不特定多数のコンピュータ間で直接データのやり取りを行なうアプリケーション

3. 攻撃傾向分析

2005年1月1日から2005年12月8日までの期間、JSOCにおいて観測した攻撃傾向を分析しました。ここでの攻撃とはネットワーク上において、侵入検知システム、侵入防御システムで検知した悪質な通信と定義します。また、この分析結果はラック（JSOC）の顧客データを基にしているため、インターネット全体を網羅した分析結果ではありませんのでご注意ください。

表1は期間中に検知した攻撃の上位10件を表しています。

表1 攻撃検知トップ10（2005年1月1日～2005年12月8日現在）

順位	攻撃名	割合 (%)
1	Microsoft ASN.1 Library Buffer Overflow Attack (ASN.1 Library の脆弱性に対するバッファオーバーフロー攻撃:80/tcp etc)	50.4
2	RPC DCOM Interface Buffer Overflow Attack (DCOM の脆弱性に対するバッファオーバーフロー攻撃:135/tcp)	7.3
3	Windows ntdll.dll Buffer Overflow Attack (ウェブ DAV の脆弱性に対するバッファオーバーフロー攻撃:80/tcp)	6.3
4	FrontPage Extension Overflow Attempt (MS FrontPage Server Extensions の脆弱性に対するバッファオーバーフロー攻撃:80/tcp)	1.8
5	Microsoft SSL Library PCT Protocol Implementation Buffer Overflow Attack (MS SSL ライブラリの一部である PCT の脆弱性に対するバッファオーバーフロー攻撃:443/tcp)	1.6
6	FormMail CGI Accessed Attack (ウェブサーバを中継させての SPAM メールの送信攻撃 : 80/tcp)	1.5
7	OpenSSL SSLv2 Malformed Client Key Remote Buffer Overflow Attack (OpenSSL の SSL2 クライアントマスターキー処理の脆弱性に対する攻撃:443/tcp)	1.3
8	Attempt to Proxy SMTP & FTP via HTTP (HTTP を利用して SMTP や FTP をプロキシする試み : 80/tcp)	1.1
9	AWStats Command Execution Attempted (AWStats の configdir の脆弱性に対する攻撃 : 80/tcp)	1.1
10	Lupii worm attack (Lupii worm による攻撃 : 80/tcp)	0.9

※攻撃名は、JSOC 独自の定義によるものです。

(1) ワーム/ボットについて

この結果の5位～8位以外の攻撃はほとんどボットもしくはワームなどの悪性プログラムによるものです。特に1位はMS04-007の脆弱性を悪用するための攻撃コードが、昨年6月にRBOTと呼ばれるボットに組み込まれボットの感染ホストが増加したことが影響し、急激に検知数が増加^{※11}しました。4位、9位、10位の攻撃に関しても1位のものと同様に、攻撃コードが公開された後にボットやワームなどの悪性プログラムに組み込まれることによって検知数が急激に増加しています。この分析結果から、今後は攻撃コードが公開からボットなどの悪性プログラムへの組み込みまでの期間が格段に短くなっていくことが推測されます。

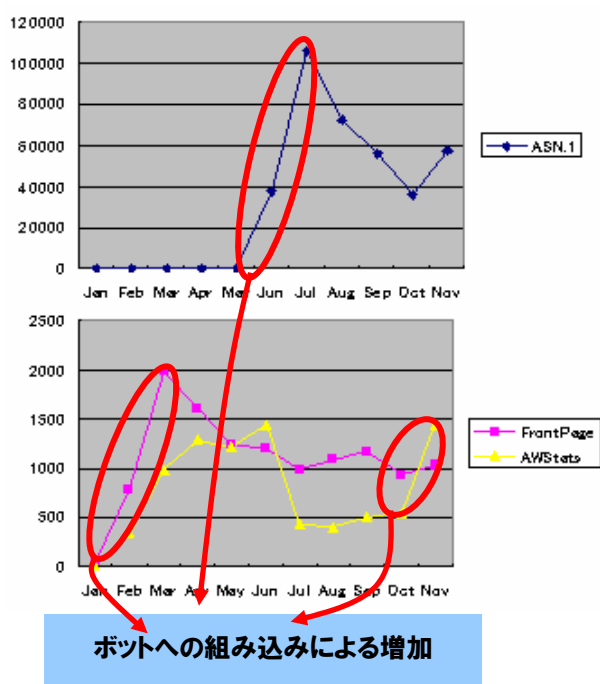


図2 ボットの検知傾向

11 ワームやボットの感染に関しては、OS やソフトウェアの脆弱性への攻撃が目されるが、感染コンピュータ数が急激に増加する場合は脆弱性の問題だけでなく、Windows の設定が脆弱であることが要因となる場合がある。特に WindowsXP の Administrator の標準パスワードが空であることがボットの感染要因のひとつであることには注意したい。

(2) ウェブアプリケーションへの攻撃の増加

昨年はウェブアプリケーションの欠陥を悪用した攻撃が大きく注目された年でした。特にウェブアプリケーションのプログラムの欠陥をついたSQLインジェクション攻撃は、いくつかのウェブサイトに被害を与え、大きな話題となりました。SQLインジェクション攻撃は、全体の攻撃数と比較すると件数は少ないですが、SQLインジェクション攻撃のみに注目してみると図3のように興味深い結果を示します。SQLインジェクション攻撃の攻撃件数、被害件数ともに右肩上がりの増加傾向を示しています。これらの件数は単純な攻撃件数ではなく、重大な事件につながる可能性があるもの、および事件が発生した件数を示しています。この結果からSQLインジェクション攻撃は比較的攻撃の成功率が高いことが分かります。

また、これらの攻撃の発信元の統計を調査しますと、図4のような結果となりました。この原因として、攻撃件数が増加しはじめた6月以前に起こった政治的問題（常任理事国入りの問題、教科書問題、靖国参拝問題など）に加え、中国のセキュリティ関連サイトによるSQLインジェクションの攻撃手順書や攻撃ツールの配布行為などが愉快犯による攻撃の増長に繋がった背景ではないかと推測します。

さらに、ウェブアプリケーションの欠陥を悪用した攻撃に関しては、クロスサイトスクリプティング攻撃と呼ばれる攻撃の件数も増加傾向を示しています。（図5参照）この攻撃手法は、最近ではフィッシング詐欺や偽のウェブサイト、悪性プログラムの配布などに悪用されています。特に偽のウェブサイトが悪用された場合、多くのウェブ閲覧者は見抜くことが困難であるため、影響は

非常に大きいと考えられます。また、偽のウェブサイトを作成されてしまった企業のブランドイメージにも影響してしまいます。

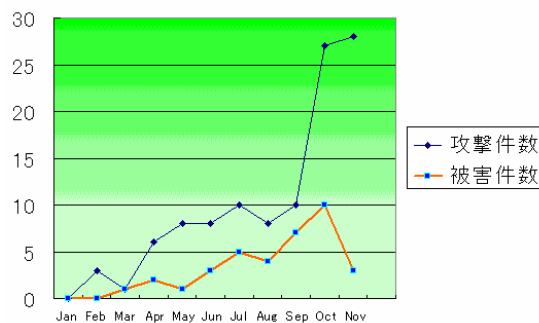


図3 SQLインジェクションの攻撃件数推移

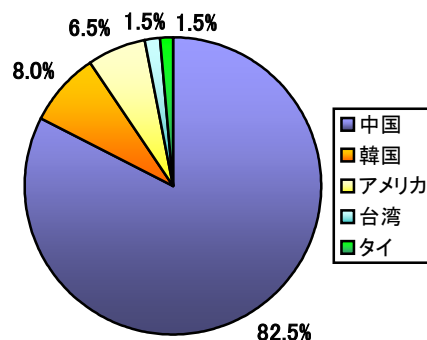


図4 SQLインジェクション攻撃の発信元統計

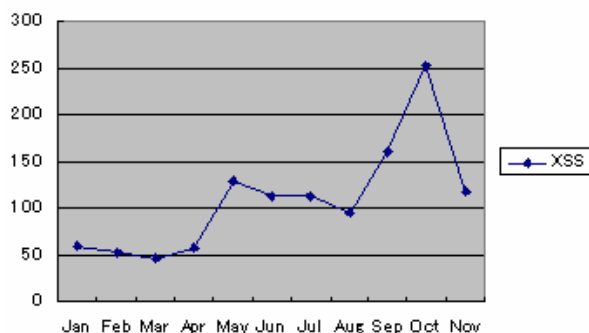


図5 Cross Site Scriptingの攻撃件数推移

(3) 2005年攻撃傾向のまとめ

昨年の攻撃検知傾向は、コンピュータウイルスやワームが上位を占めていた前年と比較し、ボットの通信が上位を占める結果となりました。また、ボットの亜種が非常に早い期間で作成されていることが検知結果に現れており、対策の難しさが懸念されます。

また、ウェブアプリケーションのプログラムの欠陥に対する攻撃に関しては、検知数、被害報告共に増加傾向にあります。日本だけでなく、世界的にCMS^{*12}が流行し、多くのユーザがウェブアプリケーションを知らず知らずのうちに利用しており、今後もさらにこの傾向は続くものと推測^{*13}され、個人情報の取扱いの多い民間企業にとっては早急な対策が重要になります。

¹² テキストやグラフィックなどのデジタル・コンテンツを収集、登録して統合的に管理し、更新・配信するソフトウェアの総称。ウェブプログラムの流行により、知名度、利用者数が急激に広まった。

¹³ ウェブアプリケーションの脆弱性の問題は、最近流行のCMSも例外ではない。実際に、CMSの脆弱性を悪用し、ソーシャルネットワークに対し悪性プログラムを配布した事件が発生している。

4. 2006 年への傾向予測

昨年は攻撃者の力量を誇示するような攻撃よりも、情報漏洩やボットのように背後にビジネス的要素が見え隠れする事件が目立ちました。攻撃を目的別に大きく 3 つに分類すると、愉快犯目的、強盗目的、ビジネス目的に分類できます。以前はホームページの改ざんやワームの作成などに代表されるように、愉快犯目的であることが多かったのですが、JSOC の観測結果によると、昨年 6 月以降に情報の不正取得などを目的としたデータベースへの攻撃 (SQL インジェクション) が増加しており、情報の売買目的やビジネス目的でのコンピュータの不正アクセス事件が主流になりつつあることが推測できます。特にウェブアプリケーションの欠陥を悪用しての攻撃は、信頼のあるウェブサイトを標的とすることで、コンピュータウイルスやスパイウェアなどの悪性プログラムの配布にも悪用可能であることから、電子商取引サイトだけでなく CMS などへの攻撃も増加することが懸念されます。

また、フィッシングメールが不特定多数に送信される「マス型」から、送信元を攻撃対象の関係者に詐称し、攻撃の標的を絞った「スパイ型」に変化してきています。このように、関係のあるユーザから送信されたメールであれば、人は油断が生じやすくなります。フィッシングメールだけに限らず、このような人間心理を悪用しての攻撃は、さらに増加すると推測されます。

■株式会社ラックについて

株式会社ラックは、ネットワークセキュリティソリューション分野でのリーディングカンパニーとして、「コンピュータセキュリティ研究所」を所有し、セキュリティに関する情報を日々、収集、蓄積・分析・検証を行い、またリモート監視センター「JSOC」にて顧客システムの24時間365日のセキュリティ監視・分析、レスポンス提供を行っています。また、先進の情報セキュリティテクノロジーを駆使し、セキュアネットサービス(SNS)事業として、官公庁・企業・団体などの顧客にサービスを提供しています。

<http://www.lac.co.jp/>

■コンピュータセキュリティ研究所

株式会社ラックに所属するコンピュータセキュリティ専門の研究所です。OSやソフトウェアの脆弱性の発見や、新技術の検証、セキュリティ情報の収集および配信などを主な業務とし、株式会社ラックのセキュリティサービスにおける技術的支援を行っています。