



侵入傾向分析レポート

Vol. 3

- 2003年度サマリレポート -

2004年2月2日

JSOC ANALYSIS TEAM

目次

1. はじめに	2
2. 攻撃とイベントデータ	3
3. 攻撃先サービス別サマリー	4
4. 攻撃傾向推移	5
5. 業界別攻撃傾向	8

1 . はじめに

本レポートは、JAPAN Security Operation Center（以降 JSOC）でのセキュリティ監視サービスにおいて蓄積された侵入検知システム（IDS：Intrusion Detection System）のログに基づき、攻撃者の侵入傾向を分析したものです。これらのデータは、定点観測によるログではなく、攻撃が成功した可能性が著しく高いセキュリティインシデントを対象に分析されています。本レポートは、日本国内および JSOC の全顧客に対し行われている攻撃および侵入手法の傾向を分析することで、JSOC アナリストの分析業務の精度を向上することや、JSOC 全体のデータのサマリーを全顧客にフィードバックすることで、セキュリティ担当者様や経営者様のセキュリティ啓蒙活動のお役に立つことを目的としています。今やセキュリティは、一企業だけで行うものではなく、日本国内や世界の同じ境遇に立つ人たちと向上していくものです。その中で、僅かでも情報を提供することで皆様の助けとなれば幸いです。

*JAPAN Security Operation Center
ANALYSIS Team*

2. 攻撃とイベントデータ

本レポートでの特徴は、攻撃行為のひとつひとつがJSOCのセキュリティアナリストにより評価され、その行為が本当に攻撃を示すものであるのか、および攻撃対象のサーバに影響があるのかが検証されていることがあげられます。1日に検知する大量のセキュリティインシデントを、攻撃、ワーム/ウイルスまたは誤検知であるかを識別し分析を行うことは、複雑な技術を利用し、専門の技術者の分析を含む高度なプロセスが必要です。このプロセス間において、JSOCは全顧客のセキュリティデバイスが生成するログ(Firewall、IDS)を分析し、全攻撃のシーケンスをリアルタイムに調査します。アナリストは、ひとつのイベントに対し、下表のような分類を行います。

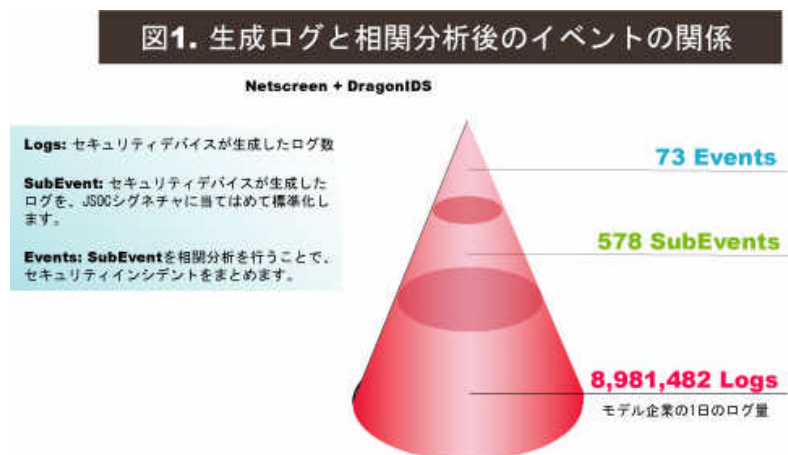
分類	説明
Emergency	攻撃が成功し、侵入されたことを示します。侵入の根拠となる Session data および Raw data などの侵入を証明する複数の条件が揃うことが条件となります。
Critical	攻撃が成功した可能性が著しく高い状況を示します。Emergency との違いは、決定的となる証拠が欠けている、もしくは攻撃は成功しているが侵入には至っていないなどがあります。
Warning	攻撃未遂および予備調査に成功し、サーバの設定情報など、後に攻撃を行う要素として考えられる情報が漏洩した場合などがあります。
Informational	攻撃であるかは不明であるが、悪意のあるコードは含まれておらず、アプリケーションによる通信や日常通信である可能性が高く、情報通知レベルのものを示します。

これらは IDS などのイベント名が基準ではなく、攻撃時の Session Data および Raw Data から分析を行い分類します。

ログ分析方法

図1は、あるモデル企業の1日のログ量と、セキュリティアナリストが分類を必要としたセキュリティインシデント数を示しています。

セキュリティデバイスが生成したログの中には、多くの誤検知が含まれ、ログ分析の妨げとなります。しかし、攻撃者はこれらの日常通信(誤検知)を隠れ蓑にして攻撃を行ってくることは珍しくありません。JSOCでは、これらの膨大なログを、複数の視点から相関分析を行うことで、効率良くリアルタイムにログ分析を行っています。



3. 攻撃先サービス別サマリー

2003 年度の攻撃先をサービス別にまとめた結果を図 2 に示します。(ワーム通信は除く) 公開サーバの多くは、WEB(HTTP/HTTPS) への通信に関してはファイアウォールの ACL でも許可している場合が多いため、攻撃の標的となることは予想できたことでした。しかし、意外であったのは、2 番目に多かった Telnet への攻撃ではないでしょうか。意外かと思われるかもしれませんが、実際に現在でもリモートからのサーバ等のメンテナンス用に Telnet を使用している組織は多く存在します。Telnet による通信がネットワーク上を平文で流れ、ユーザ ID やパスワード等の情報が盗聴される危険性があるとしても、多くの OS では標準で付属されており、少しばかりの作業であれば利便性も良いために、内部からだけではなくインターネットからの利用も許可していることが多いのが現状のようです。

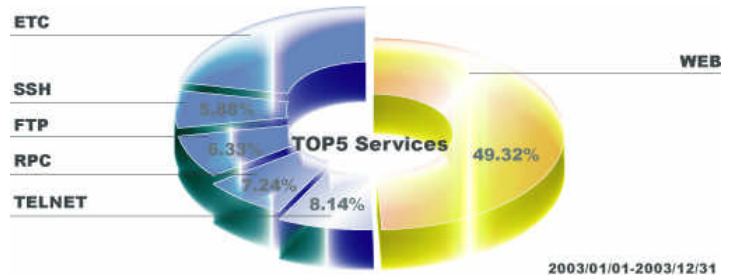


図 2. サービス別攻撃先 (JSOC 観測データから)

2003 年は Microsoft Windows の比較的大きな脆弱性が多く報告されており、2001 年の Codered や Nimda ワームが登場した年と似ていたことが特徴としてあげられると思います。攻撃傾向も、そのことを反映してか Blaster ワームが感染活動の際に利用した MS-RPC の脆弱性を利用した攻撃も多く検知しております。

参照：<http://www.microsoft.com/japan/technet/treeview/default.asp?url=/japan/technet/security/bulletin/ms03-026.asp>

dcom.c のユニバーサルバージョンがリリースされた後に Blaster ワームが登場しましたが、Nimda ワームのときと同様に、Blaster ワームの通信を隠れ蓑にした攻撃は後を絶ちません。

続いて、FTP への攻撃が多く確認されましたが、FTP への攻撃に関しては過去の攻撃傾向とは若干異なるデータが出ました。例年の傾向からすると、wu-ftpd への BufferOverflow 攻撃等が多かったところですが、2003 年 10 月頃から FTP に対するブルートフォース攻撃が増えてきています。違法コピーソフトウェアが多く世に出回りつつある現在、WAREZ を置くための物置探しをしているとの見方もできますが、現在のところ原因は不明です。

warez: インターネットを通じて行なわれるソフトウェアの違法コピー。インターネットサービスプロバイダのディスクスペースや、無料の Web スペースレンタルサービスを使い、不特定多数の人間にソフトウェアを配布する行為のこと。

5 番目に多かったのが SSH への攻撃です。この多くが CRC32 の脆弱性を狙った攻撃でした。2001 年に報告されている脆弱性ですが、今でもこの攻撃が通用するサイトは多く、SSH は攻撃者の標的となりやすいといえます。SSH の通信は暗号化されており、盗聴などに関しては確かに有効な手段ですが、アプリケーション自身の脆弱性まで補えるわけではありません。そのため、通信元および通信先を特定したアクセス制限を行うなどの処置は可能な限り行ったほうがよいでしょう。また、ありきたりですが SSH に限らず、アプリケーションは可能な限りセキュリティ上安全なバージョンを使用することをお勧めします。

4 . 攻撃傾向推移

2003 年度の侵入事例を図 3 に示します。最も利用された手法は OpenSSL への BufferOverflow 攻撃でした。この攻撃に利用されている脆弱性自体は 2002 年に報告されたものであり、2003 年 4 月を境に急激に増えてきました。原因の一つとして、Exploit ツールの攻撃対象が、比較的多くの Linux と FreeBSD をカバーしていることがあげられます。そのため、それを一度手にした Script Kiddie は、可能な限り多くの Web ページの改ざんやシステムへの侵入を試み、クラッカー仲間とその数を競おうとします。その数は、Web ページ改ざん追跡ページを参考にして頂くと、いかに多いかがお分かり頂けるかと思えます。(図 4 参照)

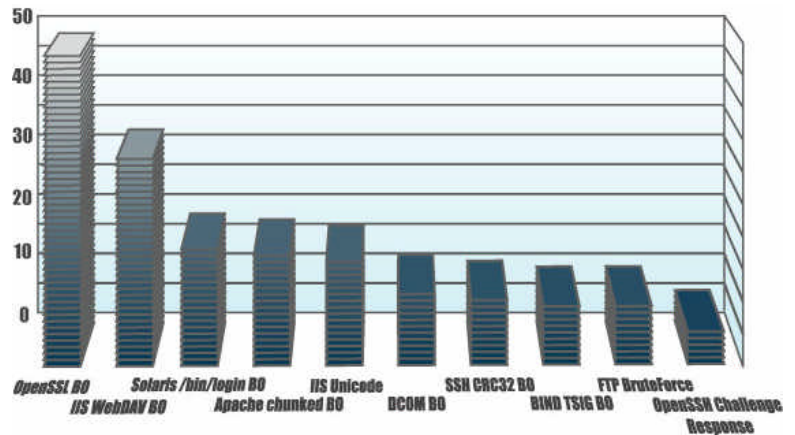


図 3. 2003 年攻撃傾向

また、OpenSSL だけのことではなく、IIS WebDAV や IIS Unicode、DCOM 等にもいえることですが、Mass-Exploit ツールが一昔前に比べて、比較的早くリリースされてしまうことも、攻撃件数の増加理由の一つと考えられます。いずれにせよ、クラッキングという行為がよりゲーム感覚に近づいてきており、高度なコンピュータ技術を持ち合わせていなくともクラッキングが可能となりつつあることに対し、我々は注意の目を向けなければならなくなったことだけは確かなようです。

Time	Attacker	Domain	OS	View
2003/12/30	SHADOW BOYS	H	Linux	view mirror
2003/12/30	SHADOW BOYS	H	Linux	view mirror
2003/12/30	SHADOW BOYS	H	Linux	view mirror
2003/12/30	SHADOW BOYS	H	Linux	view mirror
2003/12/30	SHADOW BOYS	H M	Linux	view mirror
2003/12/30	SHADOW BOYS	H	Linux	view mirror
2003/12/30	SHADOW BOYS	H	Linux	view mirror
2003/12/30	SHADOW BOYS	H	Linux	view mirror
2003/12/30	SHADOW BOYS	H	Linux	view mirror
2003/12/30	SHADOW BOYS	H	Linux	view mirror
2003/12/30	SHADOW BOYS	H	Linux	view mirror
2003/12/30	SHADOW BOYS	H	Linux	view mirror
2003/12/30	SHADOW BOYS	H	Linux	view mirror
2003/12/30	SHADOW BOYS	H	Linux	view mirror
2003/12/30	SHADOW BOYS	H M	Linux	view mirror
2003/12/30	SHADOW BOYS	H	Linux	view mirror
2003/12/30	SHADOW BOYS	H M	Linux	view mirror
2003/12/30	SHADOW BOYS	H M	Linux	view mirror
2003/12/30	SHADOW BOYS	H M	Linux	view mirror
2003/12/30	SHADOW BOYS	H M	Linux	view mirror
2003/12/30	SHADOW BOYS	H M	Linux	view mirror
2003/12/30	SHADOW BOYS	H M	Linux	view mirror
2003/12/30	SHADOW BOYS	H M	Linux	view mirror
2003/12/30	SHADOW BOYS	H M	Linux	view mirror

図 4. Web ページ改ざん追跡例

(Zone-H [http://www.zone-h.org/] より)

2003 年の攻撃傾向において、もうひとつの特徴は設定ミスにつけ込んだ攻撃が増えたことがあげられます。Blaster ワームの登場以降、多くの Windows ユーザーは慌ててセキュリティパッチを適用し始めたことは記憶に新しいと思います。しかし、人間は全てのセキュリティホールを埋められる程、器用な生き物ではなかったようです。つまり、攻撃者

は Exploit することで、Web 改ざんを行うのではなく、設定の甘いサーバに対して「正規」の方法で大量改ざんを行ったということです。有名な手法として、MS Web Publishing Wizard を使ったものがあります。実際に被害を受けた管理者は、最初は「パッチは全て適用されているのに・・・」と思うようです。しかし、大した原因ではなく、匿名ユーザに書き込み権限を与えていたことや、パスワードが推測可能なものになっていたなどの単純な理由が殆どです。JSOC で検知した、このような設定ミスにつけ込んだ攻撃は約 15% でした。その内訳は、パスワードクラックに関係した攻撃が約 5%、アクセス権限に関してのものが約 10% でした。特にアクセス権限に関しては、大きな組織程甘くなっている傾向にあり、攻撃者にとっては格好の標的となっているようです。



図 5. 設定ミスを狙った攻撃の割合

上述までのデータから、WEB への攻撃が非常に多いことが分かって頂けたかと思えます。しかし、実際に攻撃が成功した件数と、攻撃が行われている件数は必ずしも比例しているわけではありません。図 6 に攻撃件数と侵入(攻撃成功)件数を示したグラフを示します。このグラフは、皿一枚あたりが 50 件の攻撃試行があったことを示しています。また、皿の最上部に記載されている数値が侵入件数を示しています。OpenSSL への攻撃は、約 10%の確率で攻撃が成功していることとなります。OpenSSLへの攻撃に次いで侵入件数が多かった IIS WebDAV BufferOverflow の成功率は約 30%、続いて Apache chunked BufferOverflow においては約

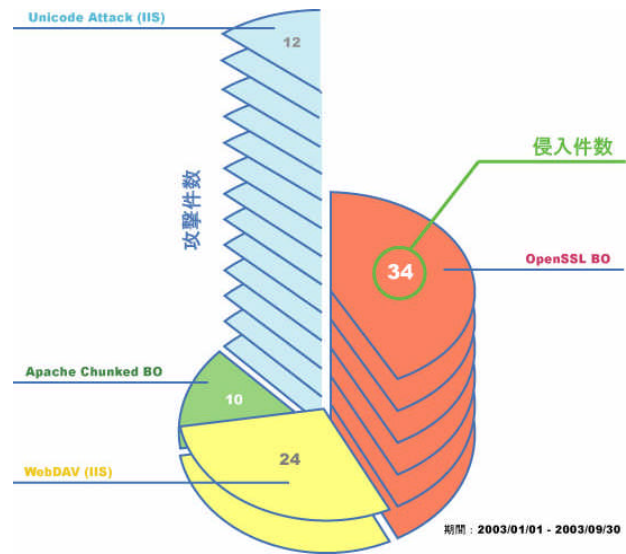


図 6. Web への攻撃成功率

77%と高い数値を示していました。これらの数値は、攻撃の手軽さにより変動するものと考えられます。例えば、IIS Unicode Attack に関しては、セキュリティパッチが適切にインストールされていない IIS であれば、インターネット上で多く公開されている Nimdaワームの通信を偽装した通信を送信する攻撃ツールにより容易に侵入が可能です。そのため、攻撃者は 1クリックで標的のサーバに侵入し、Web ページの改ざんを行うことが可能となります。対照的なのは、Apache chunked BufferOverflowがあげられます。この脆弱性を利用する攻撃ツールの多くは、FreeBSDやOpenBSDを標的としたものであるため、攻撃者は攻撃前にバナー情報や OS Fingerprint により OS を特定する必要があります。そのため、この攻撃を受けた場合の多くは、攻撃者が侵入可能である可能性が高いと踏んで攻撃を仕掛けてきていると考えられます。そのため、わずかな攻撃件数であった割に侵入件数が多かったといえます。これらの結果から、標的対象が少ないものほど攻撃を受ける確率は低くなる反面、確信犯に狙われるために攻撃成功率は高くなるように受け取れます。

5 . 業界別攻撃傾向

表1は、侵入を許してしまった業界の比率です。学術研究機関への攻撃は相変わらず多く、新しい脆弱性の登場ごとにインシデントが発生しているような状態が続いています。インシデントレスポンスの体制が、母体となる組織そのものに存在するのではなく、組織の中のグループ毎に存在する場合、各々でのセキュリティポリシーやモラル、環境、意識等の多くの部分のパラメータが異なるために、セキュリティマネジメントに非常に苦労することになるようです。同様のことが、他の業界でもいえ、特に卸売りや情報、製造といった業界で最も多かったパターンは、海外支社からセキュリティインシデントが発生した場合でした。

表1. 業界別攻撃傾向

2003年1月1日 - 12月31日	
学術研究機関	40.61%
卸売り	15.45%
情報	13.03%
製造	7.88%
出版	7.58%
金融	7.27%
官公庁	2.73%
小売	2.73%
サービス	1.21%
エネルギー	1.21%
運輸	0.30%

また、全体の傾向として、Webを利用しての取引を頻繁に行っている業界では、セキュリティへの意識も高いようで、大きなセキュリティインシデントは殆どありませんでした。また、比較的大きな組織では、組織公認のインシデントレスポンスチームが存在するか、セキュリティポリシーがあるかがインシデント発生率にも反映されていたように思います。

今後、どこの業界が狙われやすくなるかは分かりませんが、海外ではテロへの警戒とともにサイバーテロへの関心も高まりつつあります。このような世界情勢から考えますと、やはり重要インフラに携わる業界が攻撃対象となるかもしれません。標的は、何もWebサイトだけとは限らず、銀行のATMや電話、電力等多く存在します。万一を考えた上での体制作りは今や必須事項の一つと成ったのではないのでしょうか。