



侵入傾向分析レポート

Vol. 1

2003年7月1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	7

1 . はじめに

本レポートは、JAPAN Security Operation Center (以降 JSOC) での Security Monitoring サービスにおいて検知された Intrusion Detection System (以降 IDS) と Firewall 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調査し、分析を行ったレポートです。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。一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。

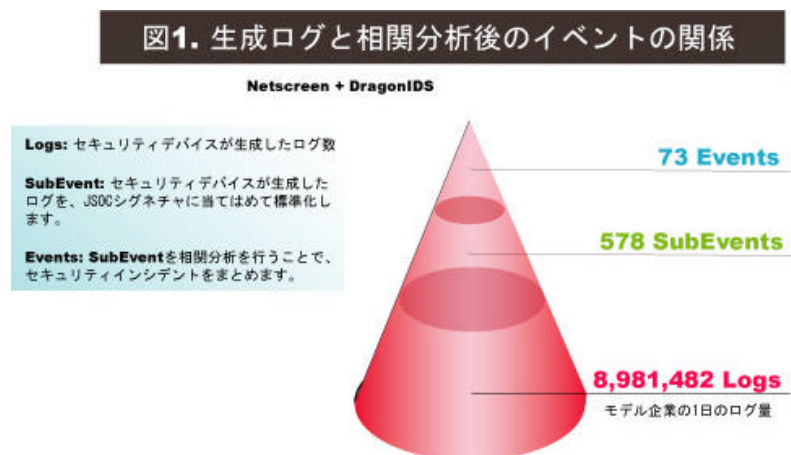
分類	説明
Emergency	攻撃が成功し、侵入されたことを示します。侵入の根拠となる Session data および Raw data などの侵入を証明する複数の条件が揃うことが条件となります。
Critical	攻撃が成功した可能性が著しく高い状況を示します。Emergency との違いは、決定的となる証拠が欠けている、もしくは攻撃は成功しているが侵入には至っていないなどがあります。
Warning	攻撃未遂および予備調査に成功し、サーバの設定情報など、後に攻撃を行う要素として考えられる情報が漏洩した場合などがあります。
Informational	攻撃であるかは不明であるが、悪意のあ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

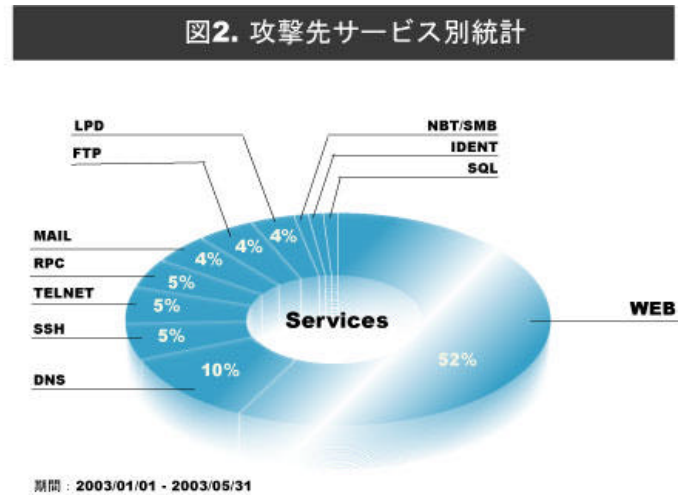
図 1 は、あるモデル企業の 1 日のログ量と、セキュリティアナリストが分類を必要としたセキュリティインシデント数を示しています。

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

図2は、攻撃者がどのサービスを利用して侵入を試みてきたかを調査したものです。ワームによる感染は除いたデータであるにも関わらず、WEBへの攻撃が圧倒的に多いことが分かります。WEBに続いて、DNSとSSHが続きます。SSHやSSLなどの暗号化による通信は、IDSが検知を苦手としています。そのため、攻撃者はバージョンの古いSSHサーバを攻撃の標的とすることが多いようです。SSHへの攻撃で最も多く確認されたのが、X2と呼ばれる攻撃ツールを用いたものでした。SSHはネットワーク管理者が自宅から社内のサーバをメンテナンスができるように、許可をしている組織を多く見かけます。攻撃の標的とされ、侵入を許してしまった組織の多くが、不特定のインターネットユーザがサーバにアクセスできるようになっており、Firewallのアクセス制御が適切に行っていなかったことがあげられます。



参考 URL: X2 Analysis Report
<http://www.incidents.org/diary/diary.php?id=118>

SSHと同様のことが、TELNETにも言えます。TELNETへの攻撃は、主に研究機関等で目立っていました。特に標的とされたOSが多かったものは、Solaris 7、Solaris 8です。原因のひとつとして、上述のSSHのようにアクセス制御が適切に設定されていなかったことや、パスワードが盗聴されたなどがありました。多くの組織は、盗聴行為を嫌い、キー認証により少しでも信頼性のある認証ができるようにSSHのような暗号による通信を好み、ファイアウォールなどによりアクセス制御をかけるなどの対策を行いますが、一部の研究機関では研究内容などの理由により、ファイアウォールが設置されていなかったなどの社会的背景も原因の一つのようです。

侵入を許してしまった多くの場合が、アプリケーションがアップデートされていなかったということ以前に、FirewallのACLが適切に設定されていなかったことがあげられます。特に、外部に公開するべきでないサービスを、インターネット上に公開してしまった場合、攻撃者はいち早くそのサーバの存在を確認し、攻撃を行ってきます。ありきたりですが、セキュリティデバイスは設置するだけでなく、定期的な維持、運用が最も重要な要素です。

4 . 攻撃傾向推移

4月から5月にかけて、OpenSSL や IIS WebDAV への攻撃が増加している傾向にあります。図3は、WEB への攻撃をさらに分類したものです。

OpenSSL の脆弱性が報告されたのは、2002年7月です。昨年は Slapper ワームが報告された後に、OpenSSL の脆弱性を攻撃するための攻撃ツールが、メーリングリストに投稿されましたが、特に目立つほどの攻撃はありませんでした。しかし、今年に入りこれらの攻撃ツールの改良版が公開され、攻撃対象が大幅に増えるとともに、OpenSSL へのスキャンや侵入行為が多く試みられるようになってきました。

参考 URL : Slapper ワームと攻撃ツール
<http://www.incidents.org/diary/?id=177>

また、今年3月に報告されました WebDAV ですが、4月頃から IIS 5.0 を狙った WebDAV に対する脆弱性 Scan が増加してきています。ワームであるかは不明ですが、IIS 5.0、5.1 を使用している組織にとっては大きな脅威となるかもしれません。IIS 管理者にとっては、しばらく目が離せない脆弱性です。

参考 URL : WebDAV
http://www.lac.co.jp/security/intelligence/SNSSpiffy/New_Attack_Vectors_and_a_Vulnerability_Dissection_of_MS03-007.html
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms03-007.asp>
<http://www.microsoft.com/japan/technet/security/bulletin/MS03-018.asp>

Nimda ワームでもお馴染みの IIS への Unicode の脆弱性を利用した攻撃ですが、3月までは WEB への攻撃の中では最も攻撃者が使用する手法でした。このグラフから、ワームの通信を装った侵入行為を試みた通信が如何に多いかが分かります。IIS の比較的容易に遠隔から権限を奪取できるような脆弱性が報告されれば、攻撃者全体の攻撃傾向に変化が見られるようです。

図4は3月に JSOC の顧客を標的とした攻撃者が、侵入の際に用いた攻撃手法の傾向を示したものです。内訳を見ると、Nimda ワームでも使用されていることで有名な、Unicode の脆弱性を利用した攻撃が2割を占めていることが分かります。このことは、前に記述した通り、ワームの通信を隠れ蓑として攻撃者が攻撃を行っているケースが多いことを裏付けています。

図3. WEBからの侵入傾向

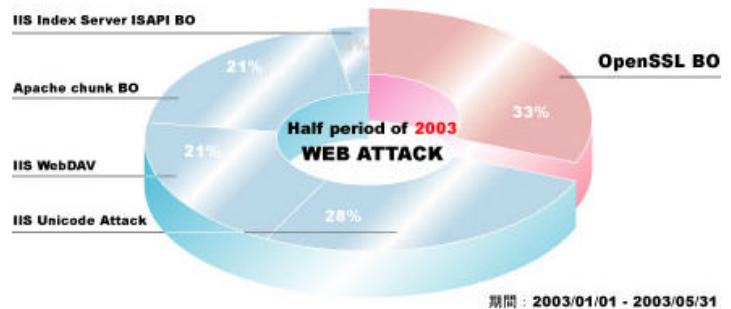
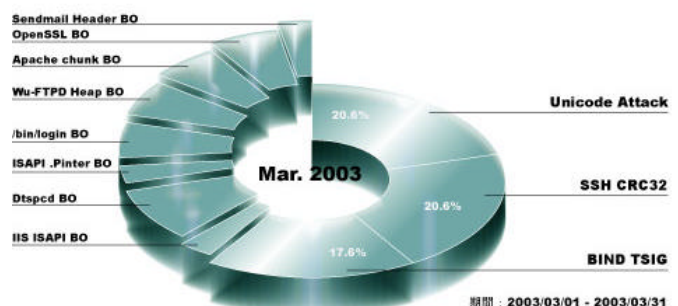


図4. 2003年3月の侵入手法統計



次に、図5は5月の侵入時の傾向を示したものです。3月までは2001年度に報告された脆弱性による攻撃が圧倒的に多かったことに対し、比較的新しい脆弱性を利用した攻撃が多いことが分かると思います。

2001年度に報告された脆弱性を利用した攻撃は、現在でも多く見られるのですが、少しずつ昨年から今年にかけて報告された脆弱性を利用した攻撃が増えてきました。図6のグラフは、5月の侵入傾向を示したもので、OpenSSLとIIS WebDAVへの攻撃が3月と比較して明らかに増加していることが分かります。

また、最近の特徴としてOpenSSLへの攻撃と共に、Apacheへの攻撃も増えてきており、WEBへの攻撃が75%を超えていることがあげられます。この数値は、Firewallだけで攻撃を防ぐ、あるいは侵入を発見することは非常に困難であること顕著に表しています。

今後、どのように攻撃傾向が変化するかは分かりませんが、WEBへの攻撃はこれからもワームを含め、増え続けていく可能性は間違いないと言えるかもしれません。

図5. 2003年5月の侵入手法統計

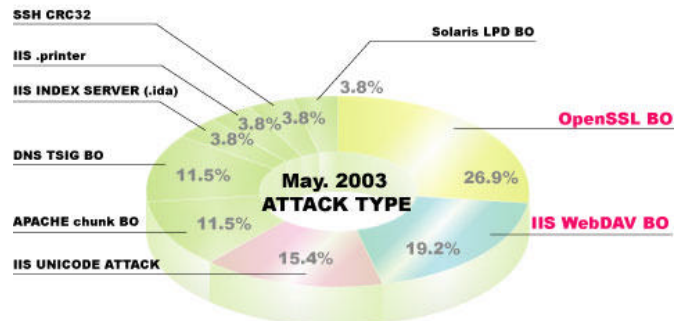
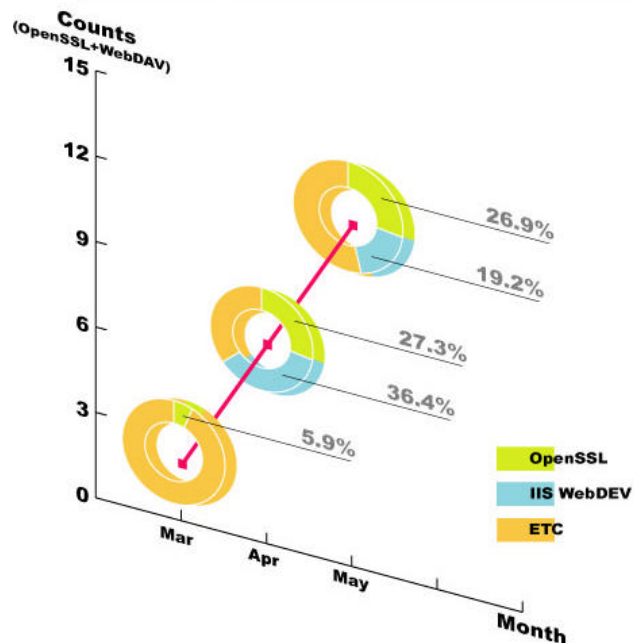


図6. OpenSSL / WebDAVへの攻撃推移



5 . 業界別攻撃傾向

教育機関を含む研究機関が突出しています。研究員個人にサーバの管理が委託されていることもあり、システム管理者が全てのホストを把握できないことが一番の原因のようです。また、一部の研究機関では研究課題の問題から、ファイアウォールが適切に設定されていないなどがありました。また、このような研究機関には重要なデータを所持している場合があります。特に

国家機関である場合、非常に狙われやすい傾向にあるようです。また、意外にも理系の教育機関の方が、文系の教育機関よりも狙われやすい傾向にあるのも特徴的でした。

次に、製造業が多くセキュリティインシデントが発生していますが、多くがワームの感染によるものです。原因のひとつとして、工場や海外セグメントを持つ場合などは、ホスト一台一台の管理が困難であることなどがあるようです。

全体的に、第三者中継を目的とした攻撃を多く検知をしていました。特に出版、サービス業界は知名度もある企業が多いため、CGI を用いたホームページを標的とした攻撃が多くみられました。日常で多くみられる攻撃としては、少々古いですが、Formmail を利用した攻撃が未だに多く見られます。特に多く見られるものとして、Formmail Scanner を使用したログです。一部のIDSでは検知できないためか、古典的な攻撃ですが現在でも多く利用されている攻撃のひとつです。WEB アプリケーションは、特に狙われやすい傾向にあるようで、XSS を利用した攻撃もみられました。

対策面に目を向けたとき、WEB への攻撃に対し、Apache や IIS ばかりに気をとられている傾向が多かったように感じます。Apache のバージョンのみ最新版にしており、OpenSSL や PHP といったアプリケーションに対し、全く対策をとられていないサーバは現在でも多く存在し、今後も攻撃は増加することが予想されます。

表 1 . 業界別イベント数

2003/01/01 - 2003/05/31

学術研究機関	47.2%
製造	14.4%
情報	10.2%
金融	7.4%
卸売り	5.1%
出版	4.2%
官公庁	3.7%
サービス	2.8%
エネルギー	2.3%
小売	2.3%
運輸	0.5%