



侵入傾向分析レポート

vol.7

2006 年上半期サマリ

2006 年 10 月 30 日

JSOC Analysis Team

1 .	はじめに	3
2 .	概要	4
3 .	2006 年セキュリティイベント発生状況	5
4 .	インターネットからの攻撃	6
4.1 .	インターネットからの攻撃	6
4.2 .	FTP サーバに対する攻撃状況	7
4.3 .	ウェブサービスに対する攻撃状況	8
5 .	内部ネットワークからの攻撃	11
5.1 .	ワームやボットの攻撃	11
5.2 .	P2P アプリケーションの脅威	12
付録	JSOC とセキュリティ監視の説明	13

1. はじめに

JSOC 侵入傾向分析レポート（以降、本レポートと呼ぶ）は、株式会社ラック JSOC（Japan Security Operation Center）より提供するセキュリティ監視サービスにおいて、日々蓄積された IDS、IPS 及びファイアウォールのログから、攻撃者の攻撃手法や侵入手法の傾向を分析したレポートです。

JSOC では、日本国内において、セキュリティの専門家が 24 時間 365 日休むことなくすべてのデータを分析しています。従って、本レポートでは単なる定点観測ではなく、実際に設置された多数のデバイスからの情報を元にした、日本独特の傾向を加味したレポートとなっております。

本レポートが皆様方のセキュリティ対策における有益な情報としてご活用いただけることを願っております。

【集計期間】

2006 年 1 月 1 日～2006 年 6 月 30 日

【条件】

本レポートの対象は、当社が監視・運用を行っているセキュリティデバイスです。

また、本レポートの対象とするセキュリティデバイスは次の通りです。

IDS:

ISS RealSecure シリーズ, Proventia シリーズ,
Enterasys Dragon Network Sensor,
McAfee IntruShield,
Cisco Secure IDS,
Snort

IPS:

ISS ProventiaG シリーズ,
McAfee IntruShield,
Cisco Secure IPS

Firewall:

Checkpoint Firewall-1,
JuniperNetworks Netscreen,
Cisco ASA 5500 シリーズ
Cisco PIX Firewall

*Japan Security Operation Center
Analysis Team*

2. 概要

2006 年度上半期は、主に内部ネットワークにおける攻撃の傾向が変化しました。

2005 年までは、脆弱性が新たに見つかり、その脆弱性はワームやボットなどの侵入経路としてすぐに悪用されていたため、対象の脆弱性に関する対策がとられていない社内ネットワークでは、社内全体が被害を受ける事件がありました。

一方、2006 年に入ってから、大規模な被害を及ぼすワームやボットなどは見られなくなりました。これは、ワームやボットが簡単に発見されないよう、感染活動などの動作を変更したためと考えられます。また、内部ネットワークで発生する脅威として、P2P アプリケーションの利用による情報の漏えいやワーム・ボット感染などがあります。なお、P2P アプリケーションの利用に関する割合については、教育機関が半数以上を占めているため、該当機関の管理者は特に注意が必要といえます。

また、内部ネットワークだけでなく、インターネットからの攻撃に関する傾向も変化しています。2005 年まではソフトウェアベンダが公開・発売しているアプリケーションにおける脆弱性への攻撃が主流でした。ソフトウェアベンダが公開・発売しているアプリケーションの脆弱性は、アプリケーションに関する情報が広く公開されており、脆弱性情報の公開とあわせて修正プログラムも公開される傾向にあることから、利用者は脆弱性への対策が行いやすく、一般的にも対策のスピードは向上してきています。2006 年に入ってから、企業が独自に開発したアプリケーションが攻撃の対象になる傾向が強くなりました。特に、ウェブサービスが対象となっており、脆弱なウェブアプリケーションを狙った SQL インジェクションが激増しています。そのため、企業が独自に開発したウェブアプリケーションに存在する脆弱性の有無を確認するため、セキュリティ診断を実施する必要があります。

さらに、ウェブサーバへの攻撃以外にも、FTP サーバを狙った攻撃が 4 月以降に急増しています。これは、推測可能な ID とパスワードを狙った総当たり攻撃を行うことで FTP サーバの運用の不備を狙う攻撃です。このような攻撃に対しては、基本的な対策である「アクセス制御」や「パスワードの管理」の実施が重要となります。

ここまで述べてきた攻撃の変化について、表 1 にまとめます。

表 1 攻撃の変化

	攻撃の内容	攻撃の特徴	攻撃対象
~2005 年	ウェブ改ざん 大規模に感染するワーム	目立ちやすい	<ul style="list-style-type: none"> ベンダが公開しているアプリケーション 脆弱性情報が広く公開される 多くの企業が対応に慣れてきた
2006 年	SQL インジェクション 攻撃者の命令で動くボット お金を目的としている	目立ちにくい	<ul style="list-style-type: none"> 企業が独自に作成したアプリケーション サーバの設定ミス、設定不備 <p>脆弱性発見には診断を行う必要がある 対応・対策が漏れやすい</p>

3 . 2006 年セキュリティイベント発生状況

2006 年上半期に JSOC で検出した、Critical 以上の重要イベントの割合を図 1 に示します。

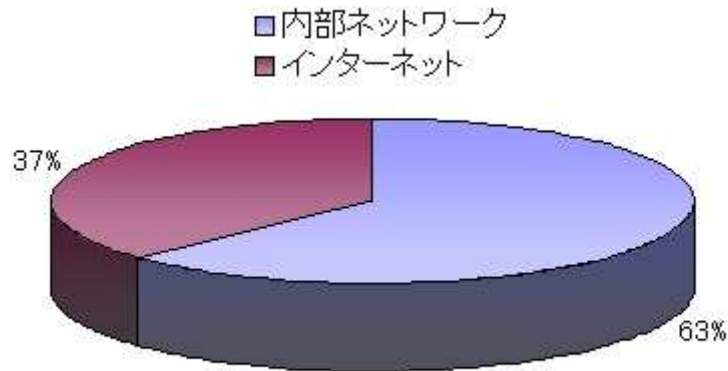


図 1 Critical 以上の重要イベントが発生したポイント

重要イベントの半数以上は内部ネットワークで発生しており、この傾向については従来から大きな変化はありません。内部ネットワークにおいて、ポットやワームの感染通信を多く検出したため、イベントの内訳がこのような結果となっております。

なお、次々とワームやポットの亜種が発生するため、今後もこの傾向は続くと想定されます。ポットやワームの感染を防ぐためにも、教育、啓蒙とともに感染を想定した対応の準備、訓練が重要な対策となります。

4 . インターネットからの攻撃

4.1. インターネットからの攻撃

インターネットからの攻撃に対して、重要イベントとして検出した攻撃の割合を図 2 に示します。

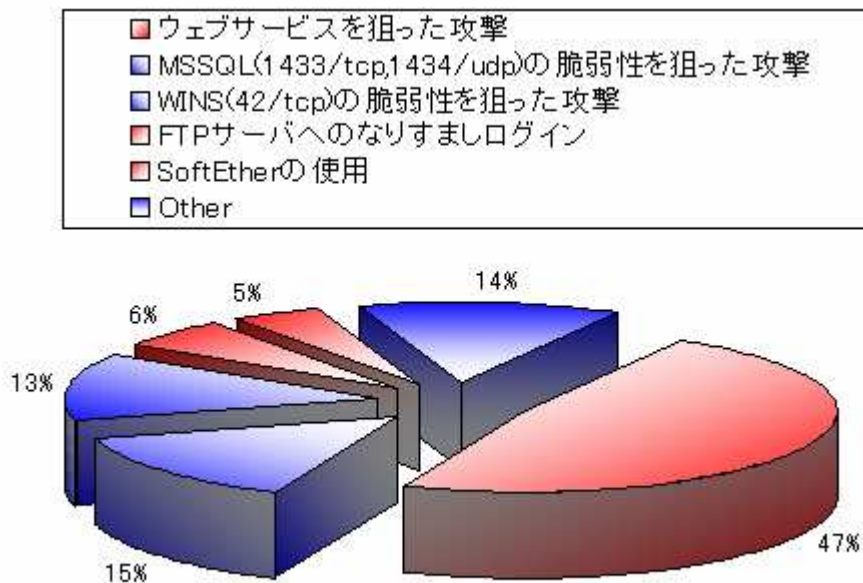


図 2 インターネットからの攻撃状況

インターネットからの攻撃対象となったサービスのうち、重要イベントが最も多く発生したものは、ウェブサービスでした。ほとんどの組織において様々な目的でウェブサービス（ホームページ）が公開されており、一般的にユーザを制限することなく公開されているため、ファイアウォールによるアクセス制御の対象にはなっておりません。従って、ウェブサービスはインターネットから攻撃しやすく、重要イベントとなる件数が多くなっていると考えられます。

次に多かった攻撃は、データベースサービスを狙うものでした。この攻撃は、ウェブサーバ経由でデータベースの操作を狙う SQL インジェクションとは異なり、データベースサーバへ直接行われた攻撃です。そのなかでも特に、Microsoft SQL Server(1433/tcp)の脆弱性を狙った攻撃が多く行われました。これは、比較的古い脆弱性（2003年以前）を狙った攻撃ではありますが、現在でも数多く攻撃が行われ、成功に至ることがあります。

4.2. FTP サーバに対する攻撃状況

2006年4月以降、FTPサーバに対する攻撃が急増しています。これは、インターネットに公開されたFTPサーバに対し、総当たり方式（ブルートフォース）という手段で推測可能なIDとパスワードを全て試す攻撃です。図3にありますように、検出した件数は4月頃より増加し始め、以後も増えつづけております。なお、JSOCからは過去にも、注意喚起としてFTPサーバを狙った攻撃が増加していることをお伝えしております¹（2006年6月13日）。

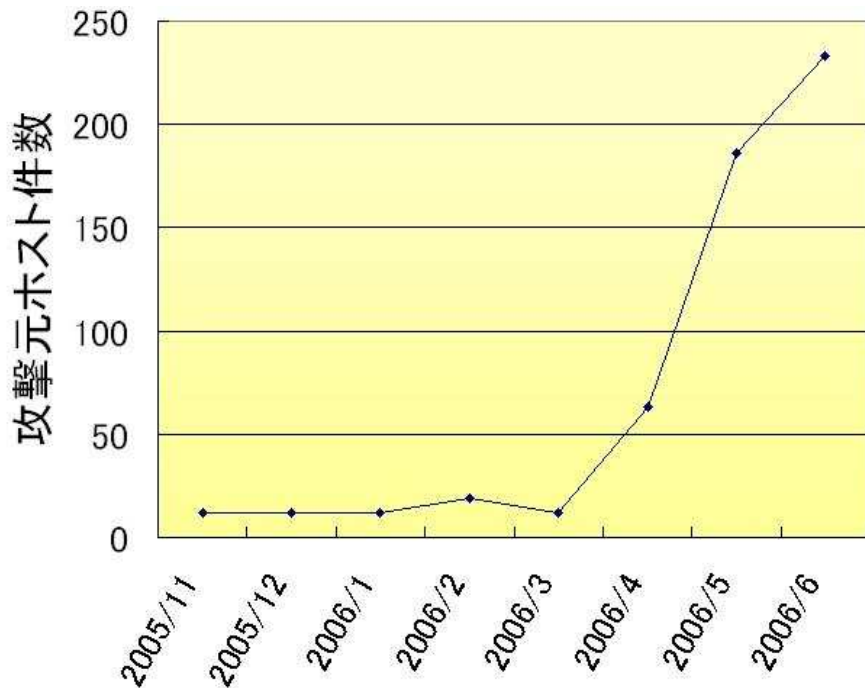


図3 FTPサービスに対する攻撃

FTPサーバへの攻撃が増加している原因として下記の事項が想定されます。

- ・ボットや著作権侵害の可能性のある不正なファイル交換サーバ
- ・フィッシングサイトを構築するための脆弱なサーバ
- ・FTPサービスで判別した脆弱なユーザを悪用し、SSHやTelnetサービスへ侵入

当社の監視対象においては特別に重大な事件は発生しておりませんが、必要のないFTPサーバが公開されていないか確認を行い、FTPサーバを公開する場合は、推測可能なIDとパスワードを利用しないことを推奨します。

¹ http://www.lac.co.jp/business/sns/intelligence/report/ftp_admin.txt

4.3. ウェブサービスに対する攻撃状況

ウェブサービスに対する攻撃において、重要イベントとして検出された攻撃対象の割合を図 4 に示します。

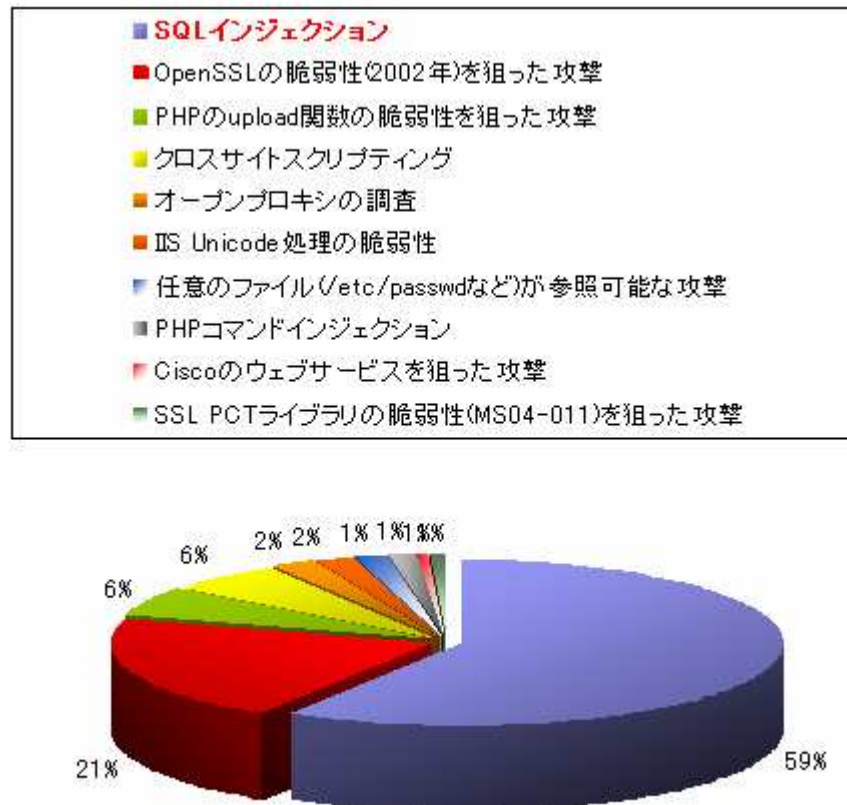


図 4 ウェブサービスに対する攻撃の割合

ウェブアプリケーションを攻撃対象としたもののうち、最も多かったものは SQL インジェクションでした。その他、クロスサイトスクリプティングや PHP コマンドインジェクションなど、ウェブアプリケーションの脆弱性を狙った攻撃も多くなってきております。なお、これらの攻撃の中には、情報の一部を取得することに成功した例もあり、情報漏えいに繋がる恐れのある Critical イベントも発生しております。

IIS や Apache などのウェブサーバソフトウェアは、開発したベンダから脆弱性情報が公開されることが一般的ですが、独自に開発したウェブアプリケーションに存在する脆弱性を発見するには、自発的にセキュリティ診断を実施し、脆弱性の有無を確認する必要があります。

SQL インジェクションの攻撃件数と被害を受けた可能性のある件数を図 5 に示します。グラフの件数は単純な攻撃件数ではなく、重要なイベントに繋がる危険性のあるイベントを集計しており、送信元ホストの数でカウントされています。

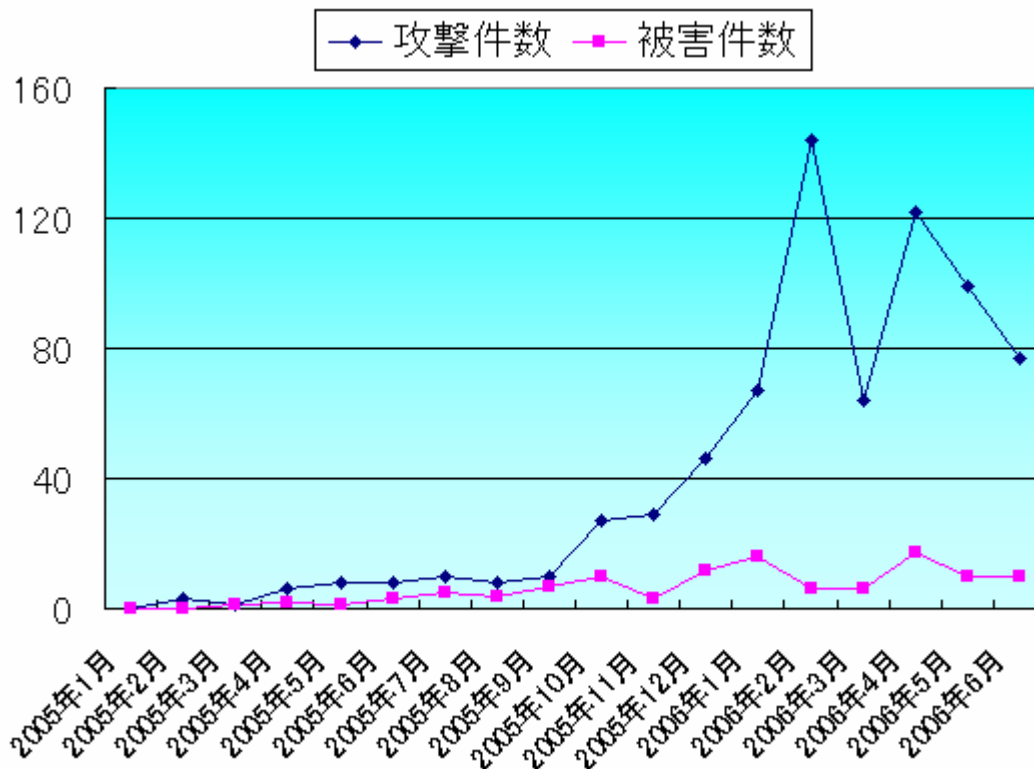


図 5 SQL インジェクションの攻撃件数の推移

2005 年の侵入分析レポート²では、年末に SQL インジェクションが増加していました。2006 年に入ってから、増加傾向に拍車がかかり、攻撃の件数が激増しております。しかしながら、被害件数の傾向は、攻撃件数の増減と関係のない推移となっております。これは、JSOC よりお客様へ、SQL インジェクションを重要イベントとしてご連絡し、対象のウェブアプリケーションに存在する脆弱性の確認・修正が行われた結果だと考えます。そのため、同様の攻撃が行われたとしても被害を受けることがないためです。

また、SQL インジェクションを検出する場合には、同時に複数のリクエストを検出することが非常に多くあります。一度に送信されてくるリクエスト数は、少ない場合で数件、多い場合には数百件にも達します。利用ユーザ数が多く、PHPなどで Web ページを動的に生成するウェブサイトは攻撃の対象となる箇所が多くなるため、攻撃が長時間に渡って継続し、結果的にリクエスト数が非常に多くなります。

² http://www.lac.co.jp/business/sns/intelligence/report/20060614_lac_report.pdf

SQL インジェクションの攻撃元に関して、国別分類を図 6 に示します。

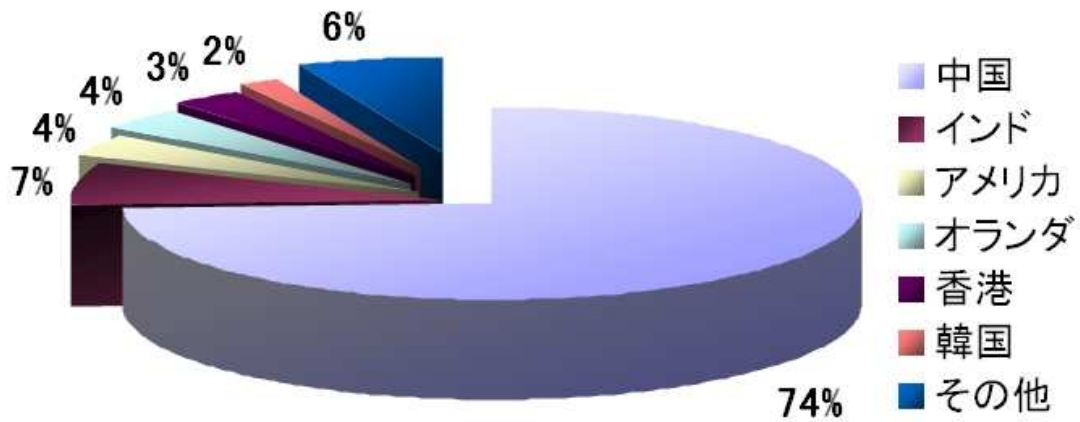


図 6 SQL インジェクションの攻撃元の国別分類

図 6 から明らかな通り、中国からと思われる攻撃が大部分を占めています。なお、この傾向は 2005 年とあまり変化しておりません。これは、中国語のサイト上で SQL インジェクションを実行する攻撃ツールが配布されていることが原因の一つであると考えられます。

5．内部ネットワークからの攻撃

5.1．ワームやボットの攻撃

ファイアウォール（FW）で検出した、内部ネットワークにおけるワームの感染活動の推移を図 7 に示します。

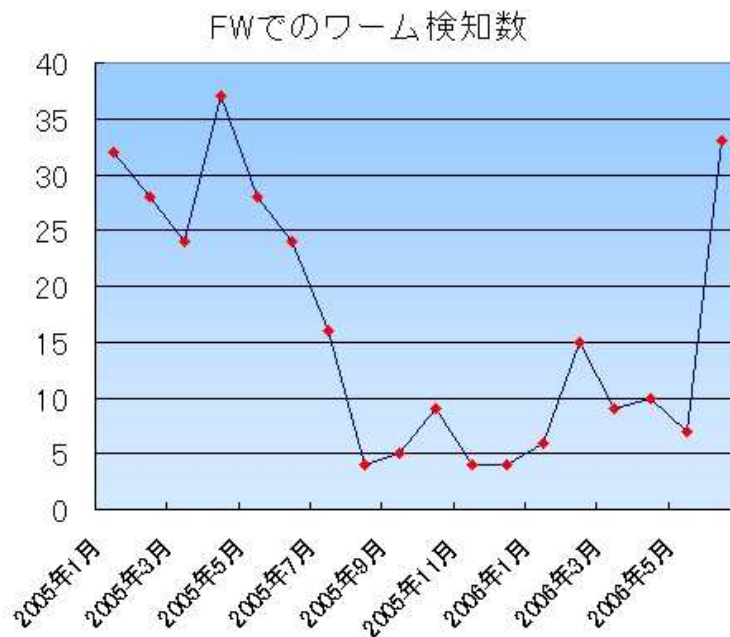


図 7 FWで検出したワームの件数

頻繁にワームが発生していた 2005 年より、全体的に減少傾向にあります。2005 年前半、頻繁に検出していたお客様におけるイベント発生件数が減少したことが要因と推測されます。JSOC によるセキュリティ監視を開始し、個々の事件についてリアルタイムに対策できることで、内部ネットワークの管理レベルが向上したものと考えられます。

2006 年 6 月の件数増加は、ある特定のお客様において多数のワーム通信を検出したためです。6 月の通信には特徴的な傾向がみられなかったことから、特定のお客様における独自の問題と考えられます。

5.2. P2P アプリケーションの脅威

P2P アプリケーションの検出状況を図 8 に示します。

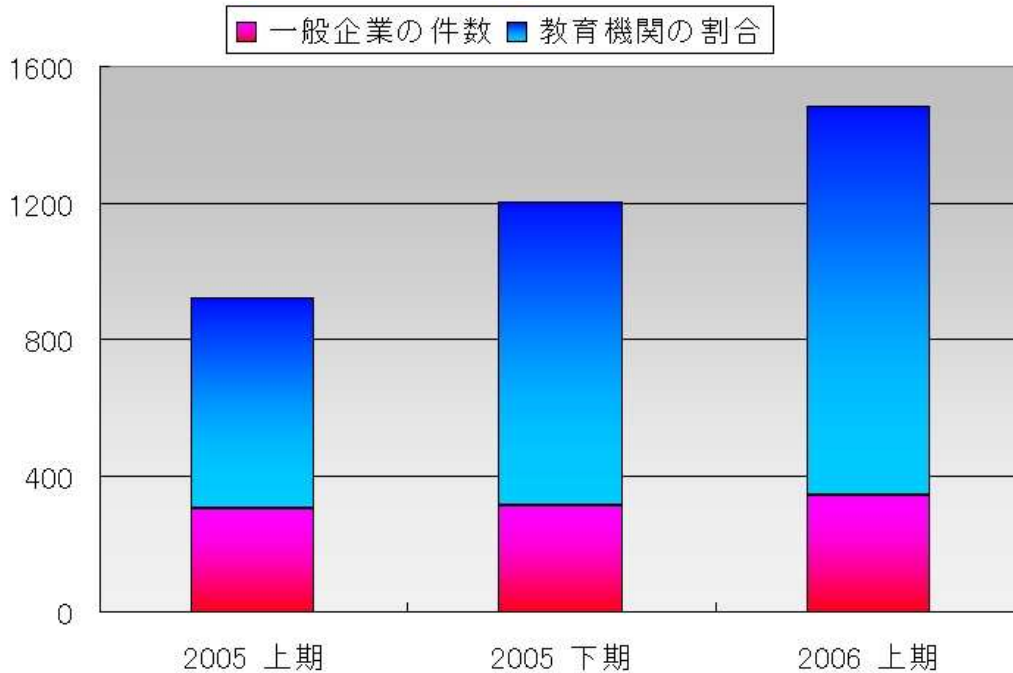


図 8 P2P アプリケーションの検出状況

全体的に教育機関における P2P アプリケーションの検出割合は増加傾向にあり、P2P アプリケーション利用の大半は教育機関において検出しています。多くの企業においては、ネットワークの利用に関する組織のポリシー、ルールまたはガイドラインなどが全社的に定められており、P2P アプリケーションの利用は認められていないことが多いと考えます。一方、教育機関においては、ネットワークの管理は各部局や研究室の単位で行われており、ネットワークの利用に関する組織のポリシーが統一されていないことなどから、P2P アプリケーションの利用が多く行われる傾向があります。

以上

付録 JSOC とセキュリティ監視の説明

JSOC では、攻撃行為のひとつひとつがセキュリティアナリストにより分析され、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ます。一日に検出する大量のセキュリティログから、誤検出を取り除き、攻撃手法やワーム/ウイルスの識別、分析を行うためには、高度な技術を用いたシステムと、専門の技術者による分析が必要です。JSOC では全顧客のセキュリティデバイス（ファイアウォール、IDS、IPS）が生成するログを調査し、全攻撃のシーケンスをリアルタイムに分析しています。セキュリティアナリストは、分析の結果に基づいてセキュリティイベントの重要度を表 2 のように分類し、Critical 以上のセキュリティイベントを重要イベントと定義しています。

表 2 セキュリティイベントの重要度の分類

分類	説明
Emergency	攻撃が成功し、侵入されたことを示します。侵入の根拠となるセッションデータもしくはパケットデータなどの侵入を証明する情報を元に判断しています。
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	攻撃失敗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すが、悪意のあるコードは含まれていない通信。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。

ログ分析方法

図 9 は、あるモデル企業の 1 日のログ量と、システムによって生成されたセキュリティイベントの数を示しています。セキュリティデバイスが生成したログの中には、多くの誤検出が含まれ、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（誤検出）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分析を行っています。

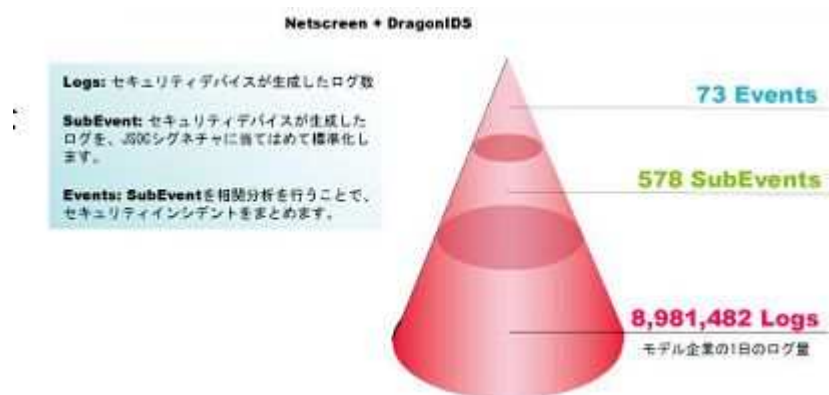


図 9 生成ログと相関分析後のセキュリティイベントの関係