10月の

インターネットセキュリティ脅威情報

情報提供：株式会社シマンテック

【 今月の概況 】

今月はマイクロソフトの製品に関連した6つの重要な脆弱性と2つのオラクル製品の脆弱性とSnortの脆弱性が公開された。

ウイルスに関しては、SymbOS.Commwarrior.C1とSymbOS.Cardblock.Aの新しいタイプの携帯電話に感染するウイルスが出てきた。また、オンラインのMySpace.comコミュニティサイト上でクロスサイトスクリプトの脆弱性を利用したワームが広がり話題になった。一方で、ウイルスは特定の大きな脅威より不正な目的のために使用される方向性が強調されている。

ランク	ワールドワイド	日本
1	NetSky.P	Netsky.P
2	Spybot	Redlof.A
3	Tooso.Q	Mytob.KU
4	Lineage	Spybot
5	Redlof.A	Mytob.EE
6	Mytob.EE	Pinfi
7	Bancos	Hybris
8	Sober.Q	Gaobot
9	Graybird	Mytob
10	Tooso	Tooso.L

表1：10月の悪意のあるコードのトップ10

【 新しく発見された主要な脆弱性 】

■Kasperskyアンチウイルスライブラリー

ロシアのKasperskyのアンチウイルスライブラリーにリモートヒープオーバフローの脆弱性が存在する。この脆弱性は.CABファイルを解析中に発生し、この脆弱なライブラリーを使用するKasperskyのデスクトップ、サーバー、ゲートウェイのすべてのWindows製品に影響する。Kasperskyアンチウイルス4.5はこの問題の影響を受けない。

■Symantec Antivirus Scan Engine

Symantec AntiVirus Scan EngineのWebベースの管理インターフェイスに存在するバッファオーバーフローの脆弱性がリモートで悪用されると、攻撃者が標的とするシステム上で任意のコードを実行できるようになる可能性がある。

この脆弱性は、Symantec AntiVirus Scan Engineの管理インターフェイス内に存在するもので、HTTP要求がScan EngineのWebサービスに渡される際にユーザー入力の検証が不十分であるために起こる。

■Computer Associatesの複数の製品

Computer Associates社のBrightStor製品を利用している環境でiGatewayコンポーネントがHTTP GETリクエストを適切に処理できない脆弱性の問題があることが確認された。この脆弱性問題により、リモートマシンから任意のコードを実行されてしまう可能性がある。

■Oracle 10g Database DBMS_SCHEDULERリモートコマンド実行の脆弱性

■Oracle Database Server dbms_system.ksdwrtリモートバッファオーバーフローの脆弱性

■Oracle Database Server ctxsys.driloadアクセス検証の脆弱性

■Oracle Database 9i SQLコマンドバッファオーバフローの脆弱性

オラクル社より今年の初めにパッチが提供されたが、David Litchfield氏から、問題がまだ残っているという新たな情報が公開された。

＜Oracleの10月のセキュリティアップデート＞

- Oracle Application Server HTTP レスポンススプリッティングの脆弱性
- Oracle Workflow 複数のクロスサイトスクリプトの脆弱性
- Oracle Workflow Wf_monitor クロスサイトスクリプトの脆弱性
- Oracle Workflow Wf_route クロスサイトスクリプトの脆弱性
- Oracle Application Server 10g emagent.exeスタックオーバフローの脆弱性

複数のOracle Database Server、Oracle Enterprise Manager、Oracle Application Server、Oracle Collaboration Suite、Oracle E-Business Suite、Applications、およびOracle PeopleSoft EnterpriseとJDEdwards EnterpriseOneが複数の脆弱性に影響された。オラクル社は10月のCritical Patch Update Advisoryをリリースし、この脆弱性に対応した。

■Kasperskyアンチウイルスエンジン

KasperskyアンチウイルスエンジンのCHMファイルパーサーにリモートバッファオーバーフローの脆弱性が見つかった。細工が施されたCHMファイルをスキャンすると、中に仕込まれた任意のプログラムが実行させられたり，正常なスキャンができなくなったりする。

■VERITAS NetBackup

VERITAS NetBackupサーバーとエージェント上で実行されるJavaユーザーインターフェイスの認証サービス、bpjava-msvcにフォーマットストリングオーバーフローの脆弱性が存在し、これをリモートから悪用すると、攻撃者は標的とするシステム上で特権を昇格し、リモートから任意のコードを実行できる。

■Snort Back Orifice プリプロセッサー

Snortの Back Orifice プリプロセッサーに、遠隔の第三者により任意のコードが実行される脆弱性がある。Back Orifice プリプロセッサーが有効になっている Snort には、受信した UDP パケットから Back Orifice の ping メッセージを検知すとき、固定長バッファにコピーするデータの長さを適切な方法で検証しないため、スタックオーバフローを引き起こし、Snortの実行権限でコードを実行される可能性がある。

【 新しく発見された主要なウイルス 】

■ SymbOS.Cardblock.A
Symbian series 60 の携帯電話に感染するトロイの木馬。ランダムなパスワードをモバイルデバイスのマルチメディアカードへ設定して、携帯電話をリブート後にパスワードを入力しないとそのカードにアクセスできないようにする。
Symbian OS の悪意のあるコードとしてはマルチメディアカードをターゲットとした最初のものである。

■ W32.Lile.A
自分自身をローカルフォルダとマップされたネットワークドライブにコピーして P2P transfer フォルダ内のファイルに感染したり、インスタントメッセージングプログラムを介して感染したりして拡散する可能性があるファイル感染ワームである。また、このワームはリモートファイルをダウンロードして実行し、www.fbi.gov の Web サイトに対してサービス拒否攻撃を試みる可能性もある。

■ W32.Opanki.AD
バックドアを作成し、遠隔の攻撃者からのコマンドを待ち受ける AOL のインスタントメッセンジャーを使って拡散するワーム。このワームは自身のプロセスをメモリーの中で隠すルートキットの機能も使っている。

■ Trojan.SilentCaller.V
侵入先のコンピューターの RAS 電話帳を改ざんし、ユーザーの許可なしに知られないように電話をかけるトロイの木馬。

■ MSIL.Idonus
.EXE ファイル上に自分自身をコピーする上書きウイルス。これは、Windows Vista ベータ 1 にデフォルトで含まれている Microsoft .NET Framework 2.0 上でのみ機能するが、これは Windows 2000、XP と 2003 用のアドオンとしても使用可能である。

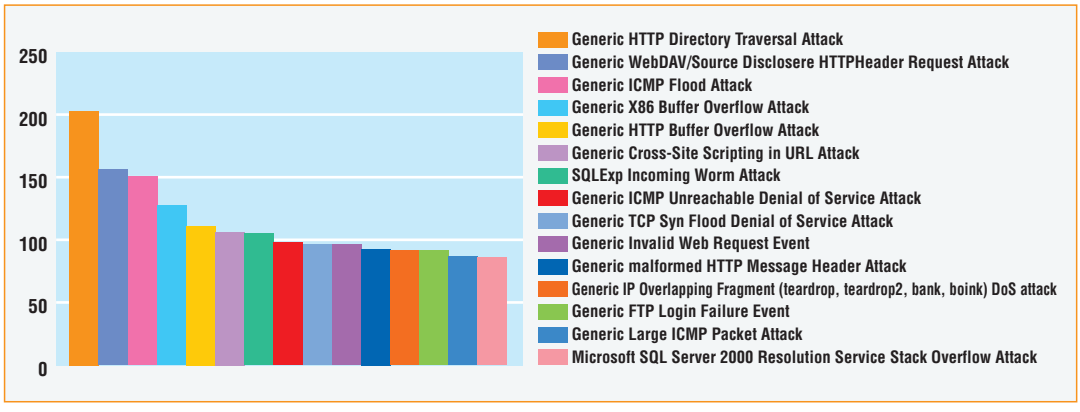
■ SymbOS.Commwarrior.C1
Symbian Series 60 を使った携帯電話上で自己複製を行うワーム。Bluetooth と Multimedia Messaging Service（MMS）を使用して拡散を試みる。携帯電話内の以前のメッセージを利用して、返信メッセージとして電話帳内のユーザーに送信される。

■ PWSteal.Banker.GD
ブラジルのオンライン銀行に関連した秘密情報を盗むトロイの木馬。

【 今月のセンサーの状況 】

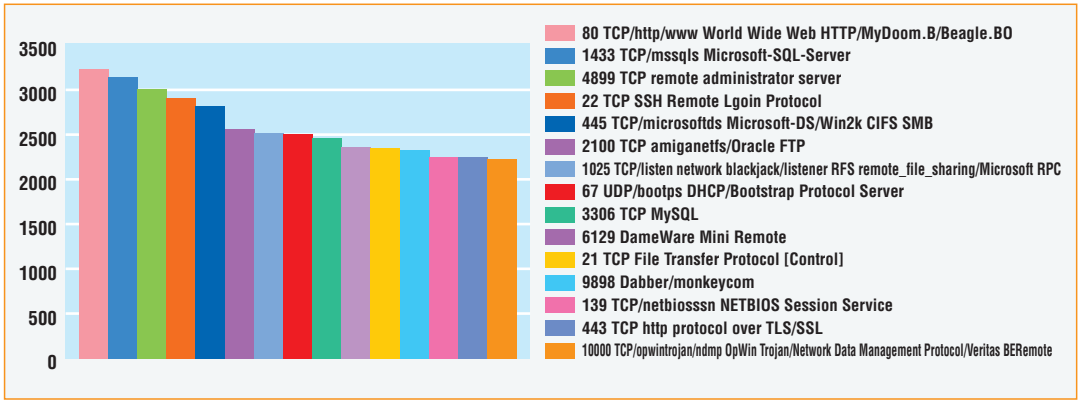
※センサーとは：インターネット上の不正な攻撃などの情報を提供する早期警告システム（Symantec DeepSight Threat Management System）。全世界 180 か国以上、19,000 ものパートナーのもとにあるファイアウォールや侵入検知システムより収集した攻撃のデータを収集、分析することで、最新の攻撃情報や、パッチの情報、その対処法などを素早く提供するもの。

グラフ 1：10 月の攻撃トップ 15（IDS）



10 月も IDS のセンサーで検知された Top アタックの主なものは古くからのワームである CodeRed、Nimda、SQLExp（Slammer）による攻撃であった。第 1 位の The Generic HTTP Directory Traversal Attack はターゲットのファイルシステム上の許可されないファイルにアクセスするための攻撃である。

グラフ 2：10 月の攻撃を受けたポートトップ 15（Firewall）



ボットネットワークを拡大しようとする試みが攻撃の統計の中にも影響が出ている。昔からの脆弱性を狙った攻撃がたびたび攻撃の対象にされている。TCP のポート 80 番は Web を狙ったワームのため、つねに 1 番か 2 番に位置する。また、TCP のポート 1433 番もよく狙われるポートである。

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp