



SANS: インターネットにおける攻撃の傾向と標的にされやすい脆弱性トップ 20(2006 年版)

2006 年 11 月、SANS (System Administration, Networking, and Security) Institute が、最近の重大な脆弱性に関する報告書の 2006 年版を公開しました。この報告書は、コンピュータを乗っ取って機密情報を盗み出すために、攻撃者によって悪用されることの多い脆弱性についてまとめたものです。これを元に SANS は、2006 年末の時点における主な攻撃の傾向を 6 つに分類しています。この 6 つの傾向と、その対策として有効な手段を以下に示します。

| SANS が挙げる 2006 年の攻撃の傾向 | 攻撃への対策 |
|---|---|
| 1. Internet Explorer 以外の Microsoft 社製ソフトウェアに存在するゼロデイの脆弱性(パッチ未公開の脆弱性)を標的とする攻撃の急増 | <p>チェック・ポイントでは、すべてのチェック・ポイント製品に搭載される侵入防御技術 SmartDefense を通じて、ゼロデイ攻撃に対する防御機能を提供しています。</p> <p>SmartDefense は、アプリケーションの本来の動作を理解することにより、未知の悪意ある攻撃を検出します。</p> |
| 2. PowerPoint や Excel など、広く使われている Microsoft Office 製品の脆弱性を突く攻撃の急増 | <p>チェック・ポイントの VPN-1 UTM および VPN-1 UTM Edge に搭載される UTM 機能により、電子メールや FTP、Web などの一般的な攻撃媒介を経路とするウイルスを検出できます。また SmartDefense を使用することで、同じく媒介として使用されることの多いインスタント・メッセージングやピアツーピア・ネットワークを制御することも可能になります。</p> <p>プログラムを改変しようとする悪意あるコードに対しては、チェック・ポイントのエンドポイント向けセキュリティ製品の Integrity を使用することで、それらを検出し、拡散を防止することができます。</p> |
| 3. 標的型攻撃のさらなる増加 | <p>チェック・ポイントのセキュリティ・ソリューション・ファミリーは、SmartDefense サービスを通じて、最新の攻撃に対する防御機能を提供しています。</p> |
| 4. 政府関連企業や官公庁などに対するスパイ・フィッシング攻撃の大幅な増加傾向(今後、このタイプの攻撃は他の業種の組織にも広まると予想される) | <p>Web Intelligence (VPN-1 のオプション・モジュール、Connectra には標準で付属)により、フィッシングで用いられることの多いクロスサイト・スクリプティングを防止できます。</p> |
| 5. VoIP (Voice over Internet Protocol)に対する攻撃は、現在はプロバイダに不正侵入し回線を第三者に転売するという目的で行われている他、詐欺的なメッセージを流したり、さらには一般電話網に大規模な障害を引き起こしたりする目的で行われている | <p>VPN-1 シリーズは、複数のベンダーの VoIP プロトコルを深いレベルで理解することができます。例えば、不正に無料通話を行うなどの詐欺的行為を検出したり、毎秒あたりの新規セッション数に上限を設けて VoIP に対するサービス妨害攻撃を防止したりすることが可能です。</p> |
| 6. Web アプリケーションに存在する脆弱性の悪用は引き続き多く、さらに増加中 | <p>侵入防御技術の SmartDefense は、Web Intelligence と組み合わせることにより、企業の Web アプリケーションを保護することが可能になります。また、SmartDefense サービスを通じて最新の防御機能を手に入れます。</p> <p>Connectra では、Web アプリケーションへの SSL VPN アクセス機能と、VPN-1 ゲートウェイと同じレベルの防御機能が提供されます。</p> |

インターネットで標的にされやすいセキュリティ脆弱性トップ 20(2006 年版)*

SANS Top-20 2006 は、専門家らの中で直ちに対策が必要とされた脆弱性のリストです。これは、数十人の著名なセキュリティ専門家の意見をまとめたもので、脆弱性の影響を軽減するための手順や対策、参考文献も記載されています。トップ 20 は以下のとおりです。

1. Internet Explorer
2. Windows ライブラリ
3. Microsoft Office
4. Windows サービス
5. Windows の設定上の脆弱性
6. Mac OS X
7. UNIX の設定上の脆弱性
8. Web アプリケーション
9. データベース・ソフトウェア
10. P2P ファイル共有アプリケーション
11. インスタント・メッセージング
12. メディア・プレーヤー
13. DNS サーバ
14. バックアップ・ソフトウェア
15. 企業向けソフトウェア(サーバ用セキュリティ・ソフトウェア、ディレクトリ管理サーバなど)
16. VoIP サーバおよびクライアント
17. ネットワーク・デバイスなどの機器に共通する設定上の脆弱性
18. 必要以上のユーザ権限および許可されていないデバイス
19. ユーザ(フィッシング/スパイ・フィッシング)
20. ゼロデイ攻撃および予防対策

*出典: SANS Top-20 Internet Security Attack Targets (2006 Annual Update), SANS Institute, November 2006.