ＩＰＡ／ＩＳＥＣが今年上半期のコンピュータウイルス・不正アクセスの届出状況を発表

情報処理振興事業協会　セキュリティセンター（ＩＰＡ／ＩＳＥＣ）は７月３日、２００３年6月及び２００３年上半期のコンピュータウイルス・不正アクセスの届出状況を発表した。　それによると、上半期におけるコンピューターウイルスの届出件数は7，３６６件となり、前年同期１１，５６７件から約３６％減少した。また、不正アクセスの届出件数は２０８件となり、前年同期４０９件に比べ半減した。

今年上半期におけるコンピューターウイルス及び不正アクセスの届出状況は次のとおりである。

１．　コンピュータウイルス届出状況

１－１．　２００３年上半期届出状況

２００３年上半期の届出件数は7，３６６件となり、前年同期１１，５６７件から約３６％減少した。

届出件数の上位は、依然としてメール機能を悪用するウイルスが占めており、感染するとバックドア（侵入口）を仕掛けたり、Ｐ２Ｐ等で感染を拡大するなどの複数の機能を持ったウイルスが増加している傾向がうかがえる。

なお、上半期にＩＰＡに届出のあった新種ウイルス１３種類の内、Ｗ３２／ＳｏｂｉｇやＷ３２／Ｆｉｚｚｅｒなど、セキュリティホールを悪用していない（添付ファイルをユーザが開かなければ感染しない）ウイルスが９種類と過半数を占め、件数も増えているので、「添付ファイルは安易に開かない」というウイルス対策の基本を改めて徹底するよう望む。

１－２．　６月の届出状況

６月の届出件数は１，４０１件と５月の１，４５８件より若干の減少となった。
６月の届出上位４種は、いずれも差出人アドレスを詐称するウイルスであった。これらのウイルスは、本来の送信者を特定するのが困難であり、連絡が取れないことから蔓延する可能性が高いので、継続して注意が必要である。

２．コンピュータ不正アクセス届出状況

２－１．　２００３年上半期届出状況

２００３年上半期の届出件数は２０８件となり、前年同期４０９件に比べ半減した。

ＩＰＡに届けられた２０８件のうち実害があった届出は、６５件（前年同期１２８件）であった。被害の内容は、侵入３６件、ワーム感染１件、アドレス詐称７件、ＳＰＡＭ２件、メール不正中継４件、ＤｏＳ（サービス妨害）攻撃４件、その他１１件であった。
主な被害原因は、「古いバージョン、パッチ未導入」（１３件）、「設定不備」（１０件）であった。

また、ＩＰＡで行っているネットワーク観測データでは、1月下旬に発生したＷ３２／ＳＱＬＳｌａｍｍｅｒワームによるものと思われる１４３４／ｕｄｐへのアクセスがピークを過ぎた２月以降も定常的に観測されている。
上記以外にも、８０／ｔｃｐ、４４５／ｔｃｐ、１３７／ｕｄｐ、１３９／ｔｃｐ、４４３／ｔｃｐといったワーム（Ｗ３２／ＣｏｄｅＲｅｄ、Ｗ３２／Ｏｐａｓｅｒｖ、Ｌｉｎｕｘ／Ｓｌａｐｐｅｒなど）が利用するポートへのアクセスが多く観測されている。これらのワームはＯＳやアプリケーションの脆弱性を突くタイプである。
注：試験的に運用しているインターネット公開サーバー（ＩＰアドレス範囲６）へのアクセス数であり、検出の割合は必ずしも実状を表しているとはいえません。

脆弱性を放置することにより、ワームだけでなく不正アクセスによる被害を受ける危険性もある。システム管理者は自身が管理するサーバーに脆弱性が無いか、改めて確認することが必要である。

２－２．　６月の届出状況

６月の届出件数は４３件と５月の３４件より約２６％増加した。

６月の届出のうち実害があった届出件数は１８件と今年最多であった。実害のあった届出の内訳は、侵入被害が１２件、アドレス詐称が３件、ＤｏＳ（サービス妨害）攻撃が１件、その他（ブラウザ設定改ざん）２件であった。

被害届出事例と実施すべき対策
１）セキュリティ設定をせずに無線ＬＡＮを利用していたところ、パソコンに音楽、映像ファイルなどのファイルを保存されていた。
　［対策］　アクセスポイントのセキュリティ設定を工場出荷時の状態から変更する。

２）ＳＳＬの脆弱性を突かれ、侵入された。バックドアを仕掛けられ、ＩＲＣサーバーとして不正利用されていた。また、他サイトへの攻撃の踏み台として利用されていた。ログも消去されていた。

３）Ｌｉｎｕｘサーバーの脆弱性を突かれ、侵入された。管理者権限を奪われ、不正なディレクトリが作成されていた。
　［対策］ＯＳやアプリケーションのパッチを適用し、セキュリティホールを解消する。
　企業においても、無線ＬＡＮを導入する事業所が増えてきているが、アクセスポイントの設定は勿論のこと、アクセスポイントの配置についても注意して対策を行うことが必要。

３．今月の呼びかけ：「これだけでできるウイルス対策！」
－　基本だけは押さえよう　－
　届出上位のウイルスには、添付ファイルを開かなければ感染しないウイルスがある。例えセキュリティホールを悪用したウイルスであろうと、修正プログラムさえ適用していれば自動的にファイルを実行されることはなく、感染被害に遭うことはない。

　そこで、下記の点だけはウイルス対策の基本として徹底することが必要。

○メールの添付ファイルは、開く前にウイルス検査を行うこと
　ウイルスの感染経路の９割以上はメールである。添付ファイルがある場合は、安易にクリックすることなく、ウイルス検出データファイルを最新版に更新したワクチンソフトで検査する。
ワクチンソフトには、自動的にウイルス検出データファイルを更新する設定やリアルタイムでファイルを検査する設定などが用意されているので活用することが望まれる。

○修正プログラム（セキュリティパッチ）をあてること
　セキュリティホール（ソフトウェアの欠陥）のあるブラウザやメールソフトを使用していると、そこを悪用されてウイルスに感染してしまうケースがある。このような被害を防ぐには、欠陥を修正しておけばよい。ベンダーのＷｅｂサイトなどの情報を定期的に確認し、最新の修正プログラムを適用する。

○問い合わせ先：ＩＰＡセキュリティセンター（ＩＰＡ／ＩＳＥＣ）
（ＩＳＥＣ：Ｉｎｆｏｒｍａｔｉｏｎ　ｔｅｃｈｎｏｌｏｇｙ　ＳＥｃｕｒｉｔｙ　Ｃｅｎｔｅｒ）
ＴＥＬ：０３－５９７８－７５０８　ＦＡＸ：０３－５９７８－７５１８
相談電話：０３－５９７８－７５０９