Q スパイウェアやファイル共有ソフトの危険性について教えてください

A

スパイウェアとは

ウイルスの一種と思われがちなスパイウェアですが，ウイルスとは異なるものです．両者を合わせてマルウェア（malware：悪意のあるプログラム）といわれることもあります．一番の違いは，ウイルスは感染してユーザの気付かぬうちに拡大してしまうことがあるのに対し，スパイウェアはユーザの承認を得てPCに侵入するということです．ほとんどのユーザが承認した記憶はないと感じていますが，実際には巧妙な手口によってスパイウェアのインストールを承認させられているのが実情です．承認をさせる主な手口を２つ挙げます．１つは，異常に長い使用許諾文や英語などの分かりにくい使用許諾文により承認させる方法です．利用者が使用許諾文を読み切らないことを逆手に取り，知らぬ間に承認させてしまいます．もう１つは，Webアクセスをした際に大量のダイアログを表示させ，その１つに悪意のダイアログを忍ばせ承認させる方法です．これもユーザの無意識を利用して承認させるものです．

では，スパイウェアにはどのような危険性があるのか．一概にスパイウェアといっても，さまざまな種類が存在します．スパイウェアの代表的なものとして，ユーザのパスワードやクレジットカードなどの情報を収集し，収集した情報を特定の送信先に送信するソフトウェアが挙げられます．主なスパイウェアの種類を**図１**に示します．また通常，スパイウェア対策はウイルス対策とは別に扱われるため，アンチウイルスソフトとは別にスパイウェア対策ソフトを導入するか，スパイウェア対策機能が付いたアンチウイルスソフトを導入しなければなりません．

ファイル共有ソフトとは

ファイル共有ソフトとは，インターネットにつながったPC間どうしで，自由にファイルを転送できる機能を持ったP2P（peer-to-peer）ソフトを指します．代表的なソフトとしてWinnyやWinMXといったソフトが挙げられます．

ではなぜ，このファイル共有ソフトが危険なのか．ファイル共有ソフトをインストールすること自体にリスクはありません．しかし，このファイル共有ソフトを使ってファイル共有ネットワークにアクセスすることが，大きなリスクとなります．ファイル共有ネットワークには，大量のウイルスが存在しています．もっとも有名なものでは，ファイル共有ソフトWinnyを対象としたAntinny（アンチニー）ウイルスです．最近ニュースで騒がれているインターネット上での個人情報漏洩事件のほとんどが，このWinny経由によるAntinnyウイルス感染が原因のものです．このウイルスに，日本国内で約30万台のPCが感染しているといわれています．

不正ソフトの管理

では，ファイル共有ソフトを使っていても，ウイルス対策を行っていれば問題は起きないのか．ウイルスは全く新しいものから，亜種といった改変されたものまで，毎日新しいウイルスがつくられています．ウイルス定義パターンファイルが公開されるまでは新たなウイルスに対して未対処の状態となり，どうしてもタイムラグが存在します．そのため，ウイ

図１　スパイウェアの種類

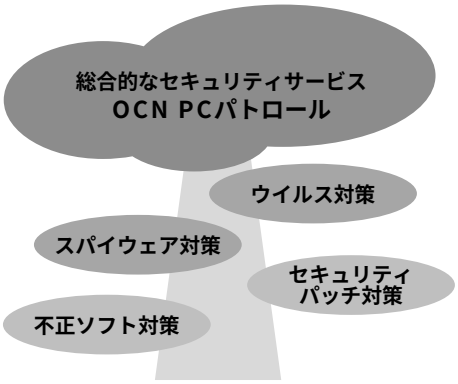

図２　OCN PCパトロール

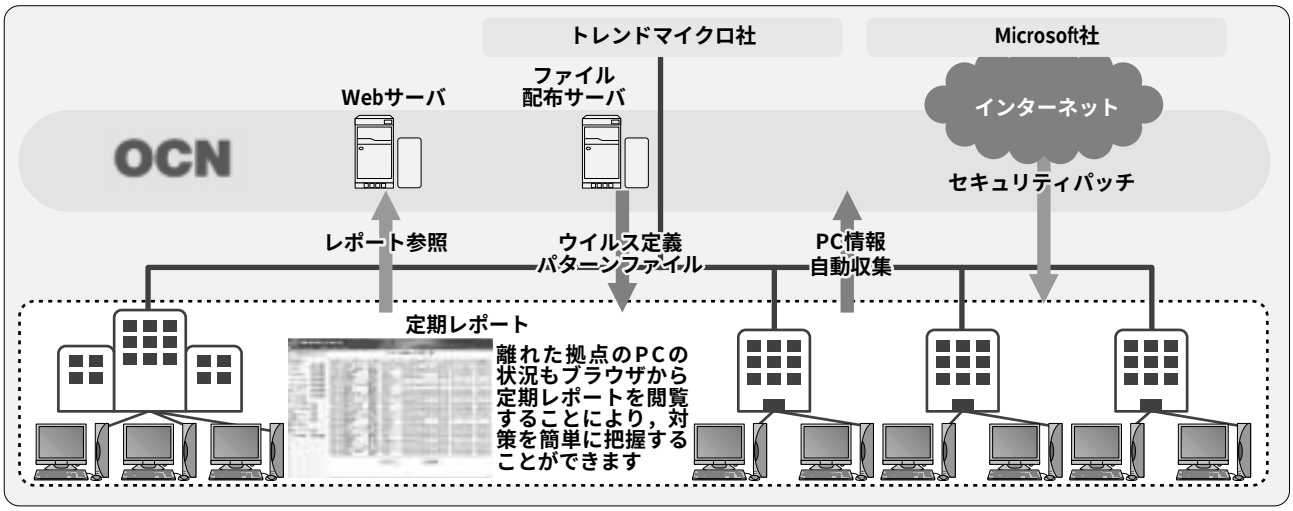

図３　OCN PCパトロールの仕組み

ルス駆除対策を限りなく100％に近づけることはできますが，100％の対策を打つことはできません．このことからもウイルス対策を行うだけでなく，リスクの原因となるファイル共有ソフトを含む不正ソフトの管理を徹底することが重要となります．

PCに必要なセキュリティ対策

現在のインターネットに接続するPCのセキュリティを確保するためには，ウイルス対策だけでは不十分なのが実情です．ウイルス対策のほか，前述したスパイウェアの対策と，ファイル共有ソフトを含んだ不正ソフトの管理，そしてOSパッチを含めた各種セキュリティパッチの適用といった，総合的なセキュリティ対策が必要となっています．

OCN PCパトロールによる統合的セキュリティ管理

NTTコミュニケーションズの開発したOCN PCパトロール（**図２**）は，LAN内のPCの情報を定期的に収集することによりPCに必要な「ウイルス対策」「セキュリティパッチ対策」「スパイウェア対策」「不正ソフト対策」の総合的セキュリティ管理を実現し，その結果を定期レポートによりお知らせします（**図３**）．これにより，LAN内PCへのセキュリティ管理の徹底と，管理稼働の低減を実現します．

OCN PCパトロールの機能

■セキュリティ機能

(1)　ウイルス対策

アンチウイルスソフトの提供のほか，LAN内の日々のウイルス定義パターンファイルの更新を一元的に管理し，ウイルス対策稼働の低減を実現します．

(2)　セキュリティパッチ対策

OSやブラウザの未適用セキュリティパッチを知らせるとともに，Microsoft UpdateやWindows Updateの自動更新設定状況を知らせます．これにより，セキュリティパッチの管理稼働を低減します．

(3)　スパイウェア対策

スパイウェア対策機能の付いたアンチウイルスソフトの提供により，スパイウェアの検出・駆除を実現します．

(4)　不正ソフト対策

LAN内PCに存在する，Winnyなどのセキュリティ上脅威となるソフトの検知を可能とします．

■レポーティング機能

上記セキュリティ機能の結果を，Web上のユーザ専用画面にて，全PCの状況を一括して閲覧可能なレポートとして随時提供します．

さらに今後は，インターネット経由での利用だけでなく，クローズドなネットワークでの利用に対応したメニューの検討を進めていきます．

このコーナで取り上げて欲しい質問をE-mailで編集部までお寄せください．
●(社) 電気通信協会内　NTT技術誌事務局　E-mail　jrr@tta.or.jp