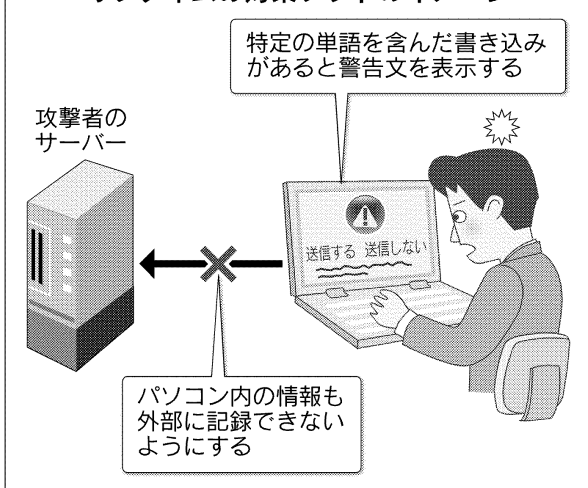


「なりすまし」被害防止

ウイルス感染後も対策

2012年、他人のパソコンを勝手に遠隔操作する「なりすまし」事件が世間を騒がせた。誤認逮捕に発展し社会問題にもなるなか、ソフトウェア各社は相次ぎ対策ソフトを開発。感染を防ぐのではなく、感染してから対策をとるのが特徴だ。掲示板への不正書き込みを防いだり、通信記録を保存して冤罪（えんざい）にならないようにしたりする。

オプティムの対策ソフトのイメージ



「不適切とみられる内容を送信しようとしています」「あなたのPCを遠隔操作しようとしているプログラムを発見しました」……。

オプティム（東京・港）が対策ソフトとは異なるが13年1月に発売する遠隔操作防止ソフト「オプティマルガード」は、特定のウイルスの侵入を防ぐ（菅谷俊二社長）。



遠隔操作などに有効な対策ソフト

会社名	製品名	内容
オプティム	オプティマルガード	ネット掲示板への不正書き込みを阻止
ハミングヘッズ	ディフェンプラットフォーム	登録外のソフトでパソコンが動くことができない
ソフトイーサ	パケット警察	通信情報やソフトの起動情報などを全て記録。無償で提供
AOSテクノロジーズ	スペクタープロ7 Plus	パソコンの操作画面を全て記録。再生し無罪を証明

不正書き込み防止 ■ 通信記録保存

「傷害」や「殺人」、「無差別」など、事前に登録した不穏な単語を使用すると、警告文を表示。意図しない書き込みだった場合はその場でキャンセルボタンをクリックして阻止できる。キーボードで打った情報を外部サーバーに記録するような動きがあった際も、画面上に警告文を表示する。これまでウイルス対策としては、情報セキュリティ企業が開発する感染防止ソフトをダウンロードするのが一般的だった。だがネット上では日々数千万のウイルスが発行されており、100%感染を防ぐことは不可能だ。そこで必要となっているのが、オプティムの「遠隔操作による冤罪対策としての利用を想定しているのは、筑波大発ベンチャーのソフトイーサ（茨城県つくば市）の「パケット警察」。

警視庁と3府県警がネット掲示板に襲撃予告を書き込んだとして4人を逮捕したのは、7月以降のことだった。その後遠隔操作によるものと判明し、いずれも謝罪する事態となったが、今年、横行したのは「なりすましウイルス」だけではない。ほかにも様々なウイルスがネット上にまん延し、ウイルス被害はひとごとではなくなっている。

ログイン情報盗難や金銭要求… 悪質ウイルス続々

「ランサム（身代金）ウェア」は特定のファイルを使用不能にし、解放と引き換えに身代金を要求する。グのログイン情報を盗むウイルスだ。感染したパソコンでインターネットバンキングにアクセスすると、「システムメンテナンスや機能の向上のためにお客様情報の再入力をお願いします」と各種ログイン情報の入力をお願ひします。最近の例では、捜査当局の侵入してくださいと友人を装ってメッセージを送る攻撃がある。SNSの個人情報からパスワードそのものやパスワード再発行のヒントを類推される場合もある。2012年の被害総額は少なくとも500万円（4億3000万円）。日本でも6月に見つかったとおり、13年の要注意ウイルスの一つだ。サイバー犯罪者の出す広告を強制的にクリックさせられて犯罪者に広告収入が入る被害があった。「マックを狙うウイルスは無い」という通信は禁物だ。

新しい対策ソフトだ。ソフト開発のハミングヘッズ（東京・中央）が発売した「ディフェンプラットフォーム」は使用するソフトの動きのみを事前に記録。未登録のソフトがパソコン内で動こうとすると、異常と見なし動きを停止する。業務で使用する文書作成ソフトやメールソフトなどはあらかじめ登録しておく。遠隔操作ウイルスに感染しても登録外のため、パソコン内では動かない。

遠隔操作による冤罪対策としての利用を想定しているのは、筑波大発ベンチャーのソフトイーサ（茨城県つくば市）の「パケット警察」。

パソコンの通信記録やソフトの起動記録を見張り、全て自動的にハードディスク上に蓄積。第三者に不正に操作された場合でも、ウイルスの起動記録や通信記録が残るため、「警察に提出すれば無実の証明や真犯人の追跡に役立つ」（同社）。

十分。感染後の対策ソフトなどを駆使して二重三重に自己防衛を図る必要がありそうだ。

許諾番号30036726 日本経済新聞社が記事利用を許諾しています。

(C) 日本経済新聞社 無断複製転載を禁じます。