

平成 18 年 3 月 15 日
内 閣 官 房

Winny を介して感染するコンピュータウイルスによる情報流出対策について

近時、ファイル交換ソフトウェア Winny でやりとりされるファイルを介して感染するコンピュータウイルス (Antinny) により、政府機関や企業が扱う業務資料や個人情報、さらには、パソコン利用者本人のプライバシー等に関する情報が、家庭のパソコンなどから流出する事案が多発しています。

Antinny は、利用者がそれと気付かずに、あるいは安全であると勘違いしてウイルスに感染するよう巧みに仕組まれており、現状では Antinny による被害を防ぐための技術的に完全な対策はありません。そのため、Winny を使用している限り、情報流出の危険を避けることはできません。そこで、インターネットを利用する皆様におかれましては、下記のとおり Winny の危険性を認識し、適切に対応して頂きますようお願い申し上げます。

記

Winny の危険性

—最も確実な対策は Winny を使わないこと—

1. Winny の使用は危険！

・Winny で入手したファイルは、誰が、いつ、どこで作成したのかもわからない信頼できないファイルです。悪意のある者にとってこのようなファイルに Antinny を紛れこませることは簡単であるため、**Winny で入手したファイルを実行（ダブルクリック）したり、閲覧したりすることは非常に危険**です。

・Antinny が入ったファイルは、紛らわしいファイル名であったり、アイコンを偽装するなど、人間の心理を巧みに利用し、誰もが、つい、実行（ダブルクリック）したり閲覧したりしたくなるように仕組まれていますので、**Winny を使用してファイルを入手することそのものが危険**です。

・パソコンを電子メールやウェブページの閲覧などの通常の用途で使用している場合であっても、個人のプライバシーに関する情報や重要な情報がパソコンの中に入っているため、**Antinny による情報の流出は絶対に防ぐ必要があります**。そのための**最も確実な対策は Winny を使わないこと**です。

2. 最新のウイルス対策ソフトやオペレーティングシステム（OS）を使用しても危険！

・Antinnyの中には、最新のウイルス対策ソフトでも対応していないものも多くあるため、最新のウイルス対策ソフトを使用しても安心できません。

・Antinnyの大半は、OSのセキュリティホールとは関係なく感染し情報を流出させるものであるため、OSを最新の状態にしても被害を防ぐことはできません。

・また、ウイルス対策ソフトが対応していない Antinny も数多くあることから、ウイルス対策ソフトでは完全に Antinny の感染を防いだり、検出・削除したりすることができません。そのため、確実に Antinny に感染していないと言えるようにするためにはOSをクリーンインストール^{注)}する必要があります。

注) ハードディスク上のソフトウェアやデータを完全に消去してから、OSを再びインストールすること。なお、クリーンインストールした後は、OSをアップデートして最新の状態にするようにしましょう。

3. 自分がWinnyを使用していなくても危険！

・パソコンを家族と共同で使用している場合は、自分がWinnyを使用していなくても、自分が知らないうちに家族がWinnyを使用している可能性があります。そのため、日頃から家族のパソコンの使用状況を把握し、家族がWinnyを使用していないか確認するようにしましょう。

※ Winny 以外のファイル交換ソフトウェアについても、上記と同様の危険性があります。

(添付資料)

資料1 昨今頻発しているWinny利用による情報流出とは

資料2 身に覚えのない情報流出の典型例

資料3 コンピュータウイルス (Antinny) の脅威

資料4 あなたは大丈夫？(今すぐできるセルフチェック)

資料5 対策参考リンク集

(参考)

Winny 及び Antinny の検出・削除方法等

本件問合せ先

内閣官房 情報セキュリティセンター

担当：大矢参事官、佐藤(隆)、川口

電話：(直通)03-3581-3768 FAX：03-3581-7652