

平成19年7月5日

各事業者団体あて

経済産業省商務情報政策局
情報処理振興課長 鍛冶 克彦

個人情報の安全管理措置徹底に関する会員企業への周知について（依頼）

貴協会所属の各会員事業者においては、平成17年4月に個人情報の保護に関する法律が全面施行されて以降、同法に基づき、業務上取り扱う個人情報の安全管理措置の徹底に努めているところと承知していますが、情報サービス業による個人情報流出事故が相次いでおります。

特に本年5月に山口県、愛媛県、福岡県などで発生した地方自治体の住民基本台帳システムに係る個人情報流出事故は、流出した数が大規模であるばかりでなく、生年月日、本籍地、配偶者の有無など社会生活基盤を支える重要な情報が多数含まれているものであり、今後このような事故が続けば、情報サービス産業に対する国民の信頼を著しく低下させるものであると懸念しております。

つきましては、添付資料を参考に、各会員事業者に対して個人情報の安全管理措置の徹底を周知するようお願いいたします。

平成18年2月20日 経済産業省発表

「個人情報保護法に基づく個人データの安全管理措置の徹底に係る注意喚起」

（別紙1）

平成18年3月15日 内閣官房発表

「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」

（別紙2）

また、今般の情報流出事故の原因は、ウィニーがインストールされた個人所有パソコンを使用したことを踏まえ、各会員事業者に対しては、特に以下の事項の徹底に努めるよう周知してください。

◆ 個人所有パソコンで業務上の個人データを取り扱わないこと。

やむを得ず、個人所有パソコンで業務上の個人データを取り扱う場合は、その条件、方法等に関するルールを定め、その遵守を徹底すること。

◆ 業務上の個人データが記録された業務用パソコン及び外部メモリ等を外部に持ち出さないこと。

業務の性質上、やむを得ず、業務上の個人データが記録された業務用パソコン及び外部メモリ等を外部に持ち出す場合は、その条件、方法等に関するルー

ルを定め、その遵守を徹底すること。

- ◆ 業務上の個人データをウィニーその他のファイル共有ソフトがインストールされたパソコンで処理しないこと。
- ◆ 以上3点について、委託先社員や派遣社員等、外部の者に対しても遵守させること。

個人情報保護法に基づく個人データの安全管理措置の徹底に係る注意喚起

平成18年2月20日
経済産業省

個人情報保護法が平成17年4月1日に全面施行されて以降、ほぼ1年が経過しようとしておりますが、残念ながら個人情報の漏えい事故が依然として継続的に発生しております。

特に近時において、個人データを格納したデータベースへの不正アクセス、とりわけ、いわゆるSQLインジェクション攻撃によって大量の個人データが流出する事案が相次いで発生しています。

このような事態にかんがみ、今一度「経済産業分野における個人情報保護ガイドライン」で示されている個人データの安全管理措置について、その遵守状況を可及的に点検し、遺漏なき漏えい防止対策を確保するよう徹底した取組を行ってください。

特に、下記事案について重点的に点検及び漏えい防止対策を実施してください。

記

1 データベースへの不正アクセスの除去

(1) データベースの保護の前提としては、以下の措置を講じることなどにより、自身の情報システムの外部との接点となるウェブサイトのぜい弱性の悪用を防止することが必要。

- <1>公開すべきではない情報の「非公開ファイル」としての区分保管
- <2>ソフトウェアの維持に必要な修正プログラムの適切な適用
- <3>推測可能なパスワードの排除
- <4>ファイル等へのアクセス制限措置の導入
- <5>ファイアウォールの設置
- <6>セキュリティ監査の定期的実施

詳細については、独立行政法人情報処理推進機構（以下「IPA」という。）のホームページで紹介している以下を参照。

- ◆ウェブサイトのセキュリティ対策の再確認を
～ぜい弱性対策のチェックポイント～

http://www.ipa.go.jp/security/vuln/20050623_websecurity.html

- ◆安全なウェブサイトの作り方

http://www.ipa.go.jp/security/vuln/20060131_websecurity.html

(2) データベースは、国際標準化されたSQLによって管理されているところ、当該公開された管理手法を悪用してデータベースのデータの改ざんや不正取得を行う事例（SQLインジェクション※）が散見。

このため、以下の措置を実施することなどにより、SQLインジェクションによるデータベースの不正利用を防止することが必要。詳細については、IPAのホームページで紹介している上記「安全なウェブサイトの作り方」を参照。

<1>入力欄等からのSQL文に使用される記号や文字の入力に際して、当該記号等を他の文字へ置き換えること等による不正なSQL文等の混入の防止

(上記IPA「安全なウェブサイトの作り方」2-1の1)、2)参照)

<2>ウェブサイトから利用者に渡される情報(クッキー等)にSQL文を埋め込むことの禁止(上記IPA「安全なウェブサイトの作り方」2-1の3)参照)

<3>データベースに関連するエラーメッセージの非表示(上記IPA「安全なウェブサイトの作り方」2-1の5)参照)

※ 「SQLインジェクション」とは、データベースの管理プログラムを制御するための特殊な文字言語であるSQLを用いて、外部から直接データベースを操作して、データの改ざん、書き換え、情報の搾取等を行うことをいう。

2 ウィルス感染による個人データの流出対策

自身の情報システムへのウィルス感染は個人データの流出の原因の一つ。このため、以下の措置などを講じることにより、ウィルス感染による個人データの流出を防止することが必要。

<1>業務用に個人所有パソコンを用いることについての(禁止も含む)ルールの徹底

<2>業務用パソコン(業務用個人データが保存された個人所有パソコンを含む。)でのファイル共有ソフトの使用に関する(使用禁止も含む)ルールの徹底

<3>アンチウィルスソフトの導入とウィルス定義等の常時最新化

また、社内ルールを点検するとともに、従業員への周知、徹底措置を併せて講じる必要がある。

3 パソコンの紛失・盗難による個人データの流出対策

個人データが保存されたパソコンを事業所外に持ち出し、紛失・盗難によって大量の個人データが流出する事案が数多く発生。このため、以下の措置などを講じることにより、パソコンの紛失・盗難による個人データの流出を防止することが必要。また、二次被害防止のため、個人データを保存したパソコン又はファイルに対する技術的な対策(データの暗号化、パスワードの設定等)を講じることも重要。

<1>業務用パソコン(業務用個人データが保存された個人所有パソコンを含む。)の事業所からの持ち出しの(禁止を含む)ルールの徹底

<2>事業所外に持ち出したパソコンの取扱いのルール(身体から離さない等)の徹底

<3>個人データをパソコンのハードディスクに保存して利用することの制限

なお、委託先でのパソコンの紛失・盗難防止のため、措置内容を契約上明文化するとともに、その履行状況を確認するなどの対策を講じることも必要。

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) を使用していても危険！

・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) →省略

- 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) →省略

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