

平成17年7月20日
内閣官房
警察庁
金融庁
総務省
経済産業省

夏休み期間における情報セキュリティにかかる注意喚起
～ フィッシングやスパイウェアへの対応について ～

近年、フィッシング詐欺と呼ばれる行為やスパイウェアと呼ばれる個人情報等を盗み取るようなプログラムの流布が海外を中心として大きな問題となっており、昨今、日本国内においても被害が発生しております。これらは非常に巧妙に行われるため、インターネットの利用者が主体的に対応しなければ、被害の予防や拡大防止はできません。つきましては、インターネットを利用する皆様におかれましては、下記を参考に適切に対応して頂きますようお願い致します。

記

～ 被害にあわないための3か条 ～

- 1 ウイルス対策ソフトとオペレーティングシステム（OS）を必ず最新のものにする
 - ・情報セキュリティ問題は、最新のウイルス対策ソフトと最新のOSを使用することなく回避するのは困難です。
 - ・新しいウイルスが頻繁に登場しますので、ウイルス対策ソフトとOSをアップデートし常に最新の状態にするとともに、ウイルス対策ソフトを停止しないよう、心がけてください。
- 2 メールはひとまず疑ってみる
 - ・企業から一方的に送られてくる「重要なお知らせ」などの電子メールを安易に開くのは危険です。インターネットショッピングでの「購入確認」など心当たりのあるメール以外は、ひとまず疑って不用意に開かない（プレビュー表示もしない）習慣をつけてください。
 - ・返答や個人情報の入力を求めるようなメールには安易に応答しないようにしましょう。利用している銀行やカード会社のお客様窓口を日頃から確認しておき、怪しいメールが来たときにはすぐに問い合わせることも一案です。
 - ・特に「添付ファイル」は極めて危険です。ウイルスや、スパイウェアである可能性もありますので、信用できる相手から送られたもの以外は、絶対に開かないようにしましょう。

3 怪しいサイトには近づかない

- ・スパイウェアの多くは「サイトを見るだけ」でインストールされます。怪しいサイトには近づかないようにしましょう。特にウイルス対策ソフトを停止してから閲覧するように要求するサイト（「ウイルス対策ソフトを停止しないと正常に表示されません」等を表示しているサイト）は絶対に見てはいけません。
- ・また、いわゆる「ワンクリック詐欺」などの原因にもなりますので、メール中のリンクをクリックする前に、そのサイトは信頼できるか、ひとまず考える習慣をつけましょう。

利用明細などの金銭等の出入りの分かる資料を日頃からよく確認することで、万が一被害にあってしまった場合でも、被害に早く気付くことができます。

【参考】

（警察庁 サイバー犯罪対策）

<http://www.npa.go.jp/cyber/>

（警察庁 セキュリティポータルサイト@police）

<http://www.cyberpolice.go.jp/>

（警察庁 インターネット安全・安心相談）

<http://www.cybersafety.go.jp/>

（総務省 国民のための情報セキュリティサイト）

http://www.soumu.go.jp/joho_tsusin/security/index.htm

（総務省 電気通信消費者情報コーナー）

http://www.soumu.go.jp/joho_tsusin/s-iyoho.html

（経済産業省 情報セキュリティ政策室）

<http://www.meti.go.jp/policy/netsecurity/index.html>

（情報処理推進機構セキュリティセンター（スパイウェアに係る注意喚起））

http://www.ipa.go.jp/security/topics/170720_spyware.html

（フィッシング対策協議会）

<http://www.antiphishing.jp/>

フィッシングについて

「フィッシング (Phishing)」とは、金融機関（銀行やクレジットカード会社）などを装った電子メール（このメールを「フィッシングメール」と言います。下記参照）を送り、住所、氏名、銀行口座番号、クレジットカード番号などの個人情報を詐取する行為です。電子メールのリンクから偽サイトに誘導し、そこで個人情報を入力させる手口が一般的に使われています。これにより、口座からの不正な出金、クレジットカードの不正な利用等が行われるおそれがあります。

既に大きな被害が発生している米国では、年間で約7,300万人が平均50件以上のフィッシングメールを受け取り、その被害額は約9億3千万ドル（約1,000億円）に達しています（米国ガートナー社調べ）。また、日本国内でも既にインターネットバンキングのIDやパスワード、クレジットカードのカード番号を盗み取ることを狙った事案が発生しており、今後の被害の拡大が懸念されます。

【 フィッシングメール等の例 】

のようにサービスの提供者を装ったサイトに誘導するフィッシングメールの他、のように真正なサイトに誘導しパスワードを変更させるものもあります。

サービスの提供者を装ったサイトでIDとパスワードを入力させるもの

このお知らせは サービスをご利用のお客様に発送しています。
この度、 サービスのセキュリティの向上に伴いまして、オンライン上の本人確認が必要となります。
この手続きを怠りますと今後のオンライン上での操作に支障をきたす恐れがありますので一刻も早いお手続きをお願いします。
<https://www. .co.jp/login/index.htm>

一見 サービスのサイトへのリンクのようですが、クリックすると サービスを装った偽のサイトが表示されます。

サービスの提供者の本来のサイトでパスワードを変更させるもの

このお知らせは サービスをご利用のお客様に発送しています。
この度、 サービスにおいては、セキュリティの向上のため、お客様にパスワードの変更をお願いしています。お客様の新しいパスワードは、

となりますので、以下のパスワード変更のページよりパスワードの変更作業を行ってください。
<https://www. .co.jp/login/passchange.htm>

この手続きを怠りますとお客様が安全に サービスをご利用いただく上で支障をきたす恐れがありますので一刻も早いお手続きをお願いします。

このケースでは、クリックすると本来の サービスのサイトが表示されます。ここでパスワードをメールの指示通り「*****」に変更してしまうと、パスワードが「第三者も知っているもの」になってしまいます。

スパイウェアについて

いわゆる「スパイウェア」によって、日本国内では既にインターネットバンキングのIDやパスワードを盗み取ることを狙った事案が発生しており、今後の被害の拡大が懸念されます。

具体的な手口は、特定のプログラムを利用者のコンピュータにインストールすることにより、例えば、カード番号をはじめとした各種サービスの利用者ID、これに付随するパスワード等の情報を盗み取り、この情報をもとに口座からの不正な出金、クレジットカードの不正な利用等を行うものです。このようなスパイウェアは、怪しいサイトやメールの閲覧、出所が明確でないプログラムのインストールにより、その利用者のパソコンにインストールされます。

【 スパイウェアをインストールされる状況の例 】

スパイウェアのインストールは、代表的なものとして のようにサイトを閲覧することでインストールされるものと、 のようにメールを閲覧することでインストールされるもの、 のようにインターネット上からファイルをダウンロードし実行する際にインストールされるものがあります。

サイトを閲覧することでインストールされる例

十分な対策を講じていない場合、

サイトを閲覧するだけ

でスパイウェアをインストールされる可能性があります。そのため、

- 1 掲示板などに貼り付けてあるリンク先
- 2 検索エンジンで検索した結果のリンク先

のサイトが、悪意を持った者がスパイウェアをインストールさせるために作成したものであった場合、無闇にリンク先をクリックすることで、スパイウェアをインストールされてしまう可能性があります。

メールを閲覧することでインストールされる例

十分な対策を講じていない場合、

メールを閲覧するだけ

でスパイウェアをインストールされる可能性があります。特に、

メールを一覧表示させるときにメールの内容をプレビューする設定となっている

場合には、メールを選択するだけで、スパイウェアをインストールされてしまう可能性があります。

ファイルをダウンロードすることでインストールされる例

出所が不明のゲーム、怪しいサイトを閲覧する際に Web サイト側が「閲覧するために

必要」としてインストールを要求してくるソフトウェアをダウンロードし、インストールする場合、利用者が本来期待する機能以外の機能を持つスパイウェアも同時にインストールされてしまう可能性があります。