Information-technology
Promotion
Agency, Japan

プレスリリース
2014 年 8 月 6 日
独立行政法人情報処理推進機構

2014 年夏休みにおける情報セキュリティに関する注意喚起

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）は、本日、夏休みの長期休暇中およびその前後における情報セキュリティに関する注意喚起を発表しました。

この注意喚起はパソコン、スマートフォン、タブレット等の利用により休暇中や休暇明けに、企業など組織内でのトラブルや顧客へのウイルス感染、情報漏えい、および家庭でのトラブルに遭わないようにするため、また万が一トラブルが発生した場合に被害が拡大しないよう、（1）システム管理者、（2）企業など組織の一般利用者、（3）家庭での利用者、（4）スマートフォン、タブレットの利用者、を対象にした情報セキュリティ対策で構成しています。

URL：http://www.ipa.go.jp/security/topics/alert260806.html

概要は以下の通りです。

（1）システム管理者向け対策について

［緊急対応体制、盗難・紛失時の連絡体制］

・ 不測の事態が発生した場合に備えて、委託先企業を含めた緊急連絡体制や、パソコン、スマートフォン、タブレットの盗難・紛失時の連絡体制などの対応手順が明確になっているか再確認してください。

［最新バージョンの利用］

・ 管理しているサーバーやパソコンの OS（オペレーティングシステム）に修正プログラムを適用し、最新のバージョンに更新することで、脆弱性を解消してください。Windows ユーザーは、「Windows Update」や「Microsoft Update」を利用してください。

［修正プログラムの適用］

・ 管理しているサーバーやパソコンのアプリケーションソフト（インターネット閲覧ソフト、メールソフト、動画閲覧ソフト、ドキュメントファイル閲覧ソフト、CMS［Content Management System］、サーバー管理ツール等）に修正プログラム(※)を適用し、最新のバージョンに更新してください。

注(※) 8 月 13 日（水）はマイクロソフト製品の月例更新日です。

［パターンファイルの更新］

・ 管理しているサーバーやパソコンで使用しているセキュリティソフトの定義ファイル（パターンファイル）を最新な状態に設定すると共に、休み明けにも確認してください。

［情報持出しルールの徹底］

・ 業務用のパソコンやスマートフォン、タブレットやデータ等を組織外に持ち出す場合のルールを明確にし、従業員に再徹底してください。
・ パソコンやスマートフォン、タブレットに本来入れてはいけないデータが入っていないか、貸し出す前にその都度確認してください。
・ 個人が所有するパソコンやスマートフォン、タブレットを業務に活用している場合、組織のルールから逸脱していないか確認してください。
・ パソコン、スマートフォン、タブレットやデータを保管した USB メモリ等の外部記憶媒体を紛失した場合に備え、適切な暗号化を施してください。また、その手続きが適切に運用されているかを確認してください。

［アクセス権限の再確認］

・ 組織の情報システムにアクセスできる権限が適切に割り当てられているか再確認してください。

・ 外部から接続できるサーバーで不要なサービスが動作していないか再確認してください。
・ 休暇中に使用しないサーバーやパソコンの電源は切るよう従業員に再徹底してください。

［情報取扱いルールの徹底］

・ Winny 等のファイル共有ソフトによる情報漏えいが起きないよう、業務関係の情報を扱う場合の注意点を従業員に再徹底してください。

［パスワード管理の徹底］

・ 業務で使用している ID やパスワードと同じものを他の業務や私的に利用しているインターネットサービスなどでも使っている場合、速やかにパスワードを変更してください。
・ パスワードを初期設定のままで利用していないかどうか確認してください。

［サイバー攻撃対策の点検］

・ 現在運用しているシステムやサービスについて、サイバー攻撃への対策状況を点検し、対策の強化が必要であれば早急に実施してください。

(2) 企業など組織内の一般利用者が行う対策について

［インターネットバンキング利用時の注意］

・ インターネットバンキングにおいて、パソコンのウイルス感染により、不正送金の被害に遭うケースが法人口座でも急増しています。
パソコンのウイルス感染を防ぐために、パソコンの OS と各種ソフトウェアは常に最新の状態で使ってください。

［修正プログラムの適用］

・ 休暇中に OS やアプリケーションソフトの修正プログラムが公開される可能性があります。休暇明けには、修正プログラムの有無を確認し、必要な修正プログラム(※)を適用してください。なお、更新を行う場合は、システム管理者の指示に従ってください。

注(※) 8 月 13 日（水）はマイクロソフト製品の月例更新日です。

［パターンファイルの更新］

・ 休暇中に電源を切っていたパソコンは、セキュリティソフトの定義ファイル（パターンファイル）が休暇前の古いままになっていることがあります。電子メールの送受信および、ウェブサイト閲覧前にセキュリティソフトの定義ファイルを更新し、最新の状態にしてください。

［利用前のウイルスチェック］

・ 休暇中に持ち出したパソコンや、データを格納していた USB メモリ等の外部記憶媒体にウイルスが感染している可能性があります。ウイルスチェックを行ってから使用してください。

［メールの取り扱いの徹底］

・ 特定の企業や組織を装い、ウイルスメールを送りつける“標的型攻撃”が多く見受けられます。当該メールは、政府機関や関連企業を思わせる組織名やメールアドレスを詐称し、一見もっともらしいタイトルや本文、業務に関連するキーワードを使っています。また実はウイルスが仕込まれた本文中のリンクや、マイクロソフトワード文書やエクセルファイルなどに見せかけたファイルの添付など、メール受信者が信じてクリックや開封してしまうような巧妙な仕掛けがされています。添付ファイルを開いたり、リンクをクリックしたりすることで、パソコンがコンピュータウイルスに感染する可能性があります。少しでも不自然だと感じたメールの添付ファイルやリンクは、絶対開いたりクリックしたりしないでください。

(3) 家庭でパソコンを使用する方の対策について

［インターネットバンキング利用時の注意］

・ インターネットバンキングにおいて、パソコンがウイルスに感染してしまったことが原因で、不正送金の被害に遭うケースが増えています。
パソコンのウイルス感染を防ぐために、パソコンの OS と各種ソフトウェアは常に最新の状態で使って

ください。

・ インターネットバンキングなどの金融機関が、第二認証情報（乱数表や合言葉など）すべての入力を利用者に求めることはありません。第二認証情報「すべて」の入力を促す画面が表示された場合は、絶対に情報を入力しないようにしてください。

・ 通常の利用時と異なる入力の要求があった場合は、入力せずに、サービス提供元に電話などで確認をしてください。

［最新バージョンの利用や修正プログラムの適用］

・ 使用しているパソコンの OS（基本ソフト）に修正プログラムを適用し、最新のバージョンに更新することで、脆弱性を解消してください。Windows ユーザーは、「Windows Update」や「Microsoft Update」を利用(※)してください。

注(※) 8 月 13 日（水）はマイクロソフト製品の月例更新日です。

・ 使用しているパソコンのアプリケーションソフト（インターネット閲覧ソフト、メールソフト、動画閲覧ソフト、ドキュメントファイル閲覧ソフト等）にも修正プログラムを適用し、最新のバージョンに更新してください。さらに、セキュリティソフトの定義ファイル（パターンファイル）を常に最新の状態にして使用してください。

［USB メモリ等の取り扱いの徹底］

・ 所有者が不明もしくは自身が管理していない USB メモリ等の外部記憶媒体は自身のパソコンに接続しない、また自身が管理していないパソコンに自身の外部記憶媒体を接続しない、などでウイルス感染を防いでください。

［必要データのバックアップの推奨］

・ ウイルス感染等でパソコンそのものが動かなくなってしまう場合に備え、必要なデータは外部記憶媒体等へバックアップすることをお勧めします。

特にランサムウェアと呼ばれるウイルスに感染すると、ウイルス自体を駆除しても、ファイルやフォルダは暗号化されたままの状態となって元に戻せない可能性があります。

［情報取扱いルールの徹底］

・ Winny 等のファイル共有ソフトを使っているパソコンが、Antinny 等の暴露ウイルスに感染すると、パソコン内に保存してあるファイルがインターネット上に流出してしまいます。業務関係のデータを扱ったことのあるパソコンで Winny 等のファイル共有ソフトを使うのは情報漏えいの危険性が高いのでやめましょう。家族と共用しているパソコンの場合、自分がファイル共有ソフトを使っていなくても家族が使えば情報漏えいする可能性がありますので、業務関係のデータを共用パソコンで扱うのは絶対に避けるべきです。

［SNS 利用上の注意］

・ SNS（ソーシャルネットワーキングサービス）は、人と人とのコミュニケーションツールであり、信頼関係で成り立っていますが、それを悪用して相手の個人情報を収集したり、ウイルスに感染させようとする人もいます。SNS において他人のページ等に書かれている URL を不用意にクリックしないようにしましょう。特に Twitter では、本来の URL がわからない“短縮 URL”を悪用した手口が確認されています。不用意に“短縮 URL”をクリックしないように注意しましょう。また、SNS から情報を発信する場合は、情報公開の範囲を確認し、不用意に情報が公開されてしまうことのないようにしましょう。

［ウェブサイト利用時の注意］

・ 「ワンクリック請求」などの年齢確認の同意を求める、『はい』か『いいえ』のボタンをクリックさせる画面が表示された場合、年齢確認以外にウェブサイト利用時の規約も表示されていますので、この利用規約をよく読み、その先のウェブサイトの利用を判断してください。利用規約内に料金が明示されていれば有料サイトかもしれませんので、トラブルに巻き込まれたくなければ、それ以上先に進まず、そのウェブサイトの利用は中止することをお勧めします。

［パスワード管理の徹底］

・ 複数のインターネットサービスで同じ ID やパスワードを使っている場合、異なるパスワードに変更し

てください。

(4) スマートフォン、タブレットを利用される方が行う対策について

［スマートフォン、タブレット使用ルールの徹底］

・ スマートフォンやタブレットで使用するアプリには、内部の情報を窃取するものが存在します。個人利用のスマートフォンやタブレットを業務に利用している場合は、所属する組織の業務規程に従ってください。

［スマートフォン、タブレット使用時の注意］

・ 不正アプリのインストールを防ぐためには、パソコンと同様に信頼できない場所からアプリをダウンロードしないことが重要です。さらに、アプリをインストールする際に表示される「パーミッション」（アプリがスマートフォンやタブレットのどの情報／機能にアクセスするのか、許可を定義したもの）の一覧には必ず目を通し、不自然なアクセス許可や求めているアクセス許可を疑問に感じた場合には、そのアプリのインストールを中止しましょう。

・ スマートフォンやタブレットを机などに置いたままでその場を離れた際、誰かに不正に使用されることのない様、スマートフォンやタブレットはパスワードロック機能を必ず有効にし、ロックまでの待ち時間を１分程度の短い時間で設定しましょう。

［セキュリティアプリの導入］

・ 不正アプリの被害以外では、正規のアプリ名に似せた偽のアプリをインストールしてしまうことでウイルスの感染被害に遭ってしまう場合があります。こうした被害に遭わない様に、Android OS のスマートフォンやタブレットの利用者は、ウイルス感染の可能性をより低減させるためにセキュリティアプリを導入してください。セキュリティアプリを入れて最新の状態に保っておくと、ウイルスの感染を事前に食い止められる場合があります。

詳細は下記の URL をご覧ください。

URL：http://www.ipa.go.jp/security/topics/alert260806.html

■本件に関するお問い合わせ先

IPA　技術本部　セキュリティセンター　加賀谷／田中

Tel: 03-5978-7591　Fax: 03-5978-7518　E-mail: isec-info@ipa.go.jp

■報道関係からのお問い合わせ先

IPA　戦略企画部　広報グループ　横山／白石

Tel: 03-5978-7503　Fax: 03-5978-7510　E-mail: pr-inq@ipa.go.jp