特集2／情報セキュリティ対策

「サポート終了のOS、ソフトは使わない」が原則

2020年にサポート終了するWindows7、Office2010

パソコンOS「Windows7」と業務用ソフト「Office2010」が、2020年にサポート終了となります。今回はサポート終了の影響と情報セキュリティ対策について特集しました。

サポートサービスが終了すると？

会員企業の皆さまのオフィスには、ほぼ間違いなくパソコンが設置されていると思います。会社によっては社員全員がパソコンを使っているところも、珍しくないでしょう。

さまざまな調査によれば、企業で使っているパソコンのOSのほとんどは、マイクロソフト社が開発した「Windows（以下、ウィンドウズ）」です。そしてその中でも使用されている割合が高いのが、最新OSであるウィンドウズ10と、2009年リリースのウィンドウズ7です。

新しいOSが発表されると、古いOSのサポートは順次終了していきます。ウィンドウズ7も、2012年に後継のウィンドウズ8が発売されたことを受けて、2015年にサポートが終了しましたが、新機能の追加やセキュリティ関係についてのアップデートやサポートは現在も続いています。

また、ほとんどのウィンドウズPCには、ワープロソフトや表計算ソフトなどオフィス業務に必要なアプリケーションソフトのセットである「Office（以下 オフィス）」もインストールされていることでしょう。ウィンドウズと同様にオフィスにもいろいろなバージョンがありますが、古いオフィス2010を使っている企業も少なくないと思われます（現行製品はオフィス2016）。オフィス2010の正式サポートはすでに終了しており、現在は延長サポートが行われています。

ウィンドウズ7とオフィス2010の延長サポートが、2020年に終了します。これまではサポートによって、セキュリティやプログラムの不具合などに対応してもらえましたが、終了後はそれらすべてが行われなくなります。そのパソコンがインターネットに接続されている場合は、無防備のまま外からの脅威に向かい合うことになります。

期限のきたOS、ソフトは使わない

地域行政や学校、企業などに地域情報化支援サービスを行っている㈱スキットの山田義治会長は「セキュリティを考えれば、サポート終了したOS、アプリケーションは使用しないことが重要です」と言います。

「現代社会では、インターネット接続せずにビジネスを行うことは難しいでしょう。ですから中小企業といえども、セキュリティ対策はできるかぎり対応しておく必要があります。万が一情報漏えいを起こしたり、顧客にウィルス感染をさせたりしたら、取り返しがつきません」

パソコンの価格は、現在ではかなり安価になっています。ビジネスで使用するパソコンには多機能なものよりも基本的性能を重視したものを選ぶといいでしょう。またリース制度を活用する方法もあります。全社員がパソコンを使っている場合は少々大変ですが、通常は計画的に順次入れ替えていけば、大きな負担にならずに済むでしょう。

株式会社スキット
代表取締役会長
山田　義治さん

図1　情報セキュリティ10大脅威2018（https://www.ipa.go.jp/より）

昨年順位	個人	順位	組織	昨年順位
1位	インターネットバンキングやクレジットカード情報等の不正利用	1位	標的型攻撃による被害	1位
2位	ランサムウェアによる被害	2位	ランサムウェアによる被害	2位
7位	ネット上の誹謗・中傷	3位	ビジネスメール詐欺による被害	ランク外
3位	スマートフォンやスマートフォンアプリを狙った攻撃	4位	脆弱性対策情報の公開に伴う悪用増加	ランク外
4位	ウェブサービスへの不正ログイン	5位	脅威に対応するためのセキュリティ人材の不足	ランク外
6位	ウェブサービスからの個人情報の窃取	6位	ウェブサービスからの個人情報の窃取	3位
8位	情報モラル欠如に伴う犯罪の低年齢化	7位	IoT機器の脆弱性の顕在化	8位
5位	ワンクリック請求等の不当請求	8位	内部不正による情報漏えい	5位
10位	IoT機器の不適切な管理	9位	サービス妨害攻撃によるサービスの停止	4位
ランク外	偽警告によるインターネット詐欺	10位	犯罪のビジネス化（アンダーグラウンドサービス）	9位

大手企業による情報漏えいは、年に数回はニュースとなっています。いずれの企業も企業イメージに大きな傷がつき、ビジネスに多大な悪影響が生じています。資金力の弱い中小企業の場合は、倒産するといった最悪のケースも考えられます。

「もちろん最新にしたから絶対に安心というわけではありません。しかし、やらないことで生じる損失を考えれば、やれることはきちんとやっておくことが、求められると思います。言うまでもなく、ウィルスソフトはすべてのパソコンに必須、大前提ですね」

さらに、OSやアプリケーションが古いままで使っていると、急に止まってしまったり、簡単な作業に時間がかかるなどの弊害も生じます。

「作業効率の面から考えれば、パソコンはOSが更新されるタイミングで、入れ替えの検討が必要でしょう」

パスワード管理もセキュリティ対策

また、IDやパスワードの管理も必要です。「パスワードは、以前は『定期的な変更を』というのが常識でしたが、最近では逆にひんぱんに変えないようにと言われています。また『アルファベットの大文字や小文字、数字、記号を混ぜる』とも言われていましたが、これではふつうの人はとても覚えきれません。自分に覚えやすい言葉をアルファベットにして、そこにアレンジを少し加えることで、覚えやすく破られにくいパスワードを作ることが勧められています」

総務省では「国民のための情報セキュリティサイト」（http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/）を運営して、さまざまなセキュリティ知識を公開しています。また独立行政法人情報処理推進機構（IPA）でも、セキュリティに関するさまざまな情報を公開しています（図1「情報セキュリティ10大脅威」は、IPAのウェブサイトに掲載されていたものです）。

さらに山田会長は「セキュリティからは少し話がそれますが」と前置きして、「最近では、SNSを企業活動に取り入れることも、珍しくなくなりました。どんな企業でも効果があるわけではありませんが、自分から情報発信を行うことには意義もあります。現代では、企業の情報はさまざまな形でネット上に広がっています。自社からは発信していなくとも、誰かが発信し、広まっていきます。いい情報、正しい情報だったら問題はありませんが、間違った情報を広められては大きなダメージになります。そういう場合に、ふだんからウェブやSNSで情報を発信していれば、すぐに対応することも可能です。いまや当たり前の存在になったSNSも、うまく使うことでプラスにできるのです」

※　※　※

とはいえ、どれだけ対策を講じても、セキュリティ問題から完全に逃れることはできません。そんな場合、どうしたらいいのでしょうか。山田会長は「いざという時のために、保険に加入しておくことも必要でしょう」と言います。例えば当所では「全国商工会議所ビジネス総合保険制度」を扱っています。事業活動に関わるさまざまなリスクに対応する保険で、被害者への賠償補償や事業休業への補償などが行われます。もちろん「情報漏えい」も含まれています。詳しくは日本商工会議所公式サイトの中にある説明ページをごらんください（https://hoken.jcci.or.jp/business）。

備えあれば憂いなし、とは昔から伝わることばですが、パソコンについてもまさにそのとおり。今回の記事を参考に、ぜひ企業活動のアップデートを図ってください。

総務省「国民のための情報セキュリティサイト」