IT Topics & News

「情報セキュリティ10大脅威 2017」を決定 IoT機器関連の脅威が急上昇【IPA】

独立行政法人情報処理推進機構（略称＝IPA）は、2016年に社会的影響の大きかったトピックを、10大脅威選考会の投票によりトップ10を選出。1月31日、「情報セキュリティ10大脅威2017」として発表した（図1）。

IPAによる10大脅威の選出は、2016年から「個人」と「組織」と、影響を受ける二つの対象に分けて発表。2017年版も昨年同様に異なる視点からの選出となった。

「個人」の１位は、「インターネットバンキングやクレジットカード情報の不正利用」、「組織」の１位は「標的型攻撃による情報流出」となり、昨年と変動はなかった。2位以下も順位の変動はあったものの概ね昨年と同様だ。

インターネットバンキングの被害は2015年にも総合1位となっている（図2）。最近は被害額は減少傾向にあるものの、「個人」での被害額が増加傾向にあるといえ、個人ごとの対策不足が浮き彫りとなった形だ。

「組織」では、2016年に大手旅行会社が標的型攻撃により、約678万件の個人情報が漏えいした可能性があるとの発表があった。グループ会社のオペレータ端末で、メールに添付された不正なファイルを開いたためで、標的型攻撃メールは、依然として組織にとって大きな脅威といえる。

個人にも組織にも影響を与える IoT機器の脅威が初めてランクイン

今回、「組織」8位に「IoT機器の脆弱性の顕在化」、

（図1）2017年10大脅威（2016年の10大脅威も含む）

2016年順位	個人	2017年順位	組織	2016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の不正利用	1位	標的型攻撃による情報流出	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	7位
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	3位	ウェブサービスからの個人情報の窃取	3位
5位	ウェブサービスへの不正ログイン	4位	サービス妨害攻撃によるサービスの停止	4位
4位	ワンクリック請求などの不当請求	5位	内部不正による情報漏えいとそれに伴う業務停止	2位
7位	ウェブサービスからの個人情報の窃取	6位	ウェブサイトの改ざん	5位
6位	匿名によるネット上の誹謗･中傷	7位	ウェブサービスへの不正ログイン	9位
8位	情報モラル不足に伴う犯罪の低年齢化	8位	IoT機器の脆弱性の顕在化	ランク外
10位	インターネット上のサービスを悪用した攻撃	9位	攻撃のビジネス化（アンダーグラウンドサービス）	ランク外
ランク外	IoT機器の不適切管理	10位	インターネットバンキングやクレジットカード情報の不正利用	8位

「個人」の10位に「IoT機器の不適切管理」と、IoT機器の脅威が初めてランクインした。また、「組織」9位には「攻撃のビジネス化」が、トップ10入りしている。

近年、IoTが急速に普及する一方、IoT機器を使用した大規模なボットネットが構築され、分散型サービス運用妨害（DDoS）攻撃に使用されるケースが起きている。2016年、マルウェア「Mirai」によりIoT機器が大規模なDDoS攻撃に加担させられ、標的となったDNSサーバを利用していたネットサービスが数時間にわたって接続しにくくなったり、IoT機器メーカーが対応を迫られるなど、被害が拡大した事案が発生している。Miraiの影響を受けた機器は、家庭用ルータ、ネットワークカメラ、デジタルビデオレコーダなど多岐にわたる。9月末にはMiraiのソースコードが公開され、ほかのDDoS攻撃に使用される可能性もある。

個人においては、IoT機器への適正な設定方法を知らないまま、DDoS攻撃の踏み台になったケースや、ネットサービスへの接続ができなくなったという例もあった。組織にも個人にも利用されるIoTだが、セキュリティに関してはいまだ脆弱性が見られることが明らかになっている。

マルウェア感染からIoT機器を保護するためには、パスワードを強固にし、最新のパッチを適用するなど対策が必要となる。

組織にも脅威となってきたランサムウェアによる被害

2016年には「個人」で2位、「組織」で7位となった「ランサムウェアによる被害」だが、2017年版では「組織」でも2位へと急浮上している。

パソコンやスマートフォンのデータを暗号化するなどして、ユーザーのアクセスを制限し、これを解除、復元させるためにRansom（身代金）を要求するのがランサムウェアの手口だ。感染すればパソコンだけではなく、共有サーバなどにも影響が出る。

海外で猛威をふるったランサムウェアは、2014年には日本語に対応し、急速に被害を拡大させた。IPAでもたびたびランサムウェアに対する注意を呼びかけてきたが、2016年にはランサムウェアに関する問い合わせが急増してきた。特に2016年には、個人のパソコンやスマートフォンだけではなく、企業を狙ったランサムウェアが登場してきたことが、ランクを上げた要因だ。

企業がランサムウェアによる脅威を受けた場合、その身代金額は膨大なものになる。海外では、医療機関を狙った攻撃が複数あったほか、インフラ企業などにもターゲットを絞って被害を与えている。

現時点では、いかにウイルス対策を実施していても、ランサムウェアの感染を100％防ぐことは難しい。ランサムウェアの被害を想定し、今後ますます、重要なファイルの適切なバックアップと管理が必要となっていくだろう。

（図2）2015年10大脅威

順位	脅威
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の不正利用
2位	内部不正による情報漏えい
3位	標的型攻撃による諜報活動
4位	ウェブサービスへの不正ログイン
5位	ウェブサービスからの顧客情報の窃取
6位	ハッカー集団によるサイバーテロ
7位	ウェブサイトの改ざん
8位	インターネット基盤技術を悪用した攻撃
9位	脆弱性公表に伴う攻撃
10位	悪意のあるスマートフォンアプリ

平成28年熊本地震 震災復興支援サイト「かせするもん。」のご紹介

震災復興支援サイト かせするもん。

平成28年に熊本地震により、被災された方々に謹んでお見舞いを申し上げます。JECCはこれまで、被災された方々の一日も早い復興を願い、復興支援を行ってまいりました。

この度の熊本地震の復興支援を目的に、関連する各種情報を集約して発信するために開設されたインターネットサイト「かせするもん。」（「かせする」とは熊本弁で「お手伝いする」という意味）の活動に賛同し、JECCは、これからも社員に対して当サイトへの閲覧を呼びかけるなど、活動への協力を推進していきます。

この4月で熊本地震から1年が経ちますが、JECCは今後とも、被災地の一日も早い復興を心よりお祈りし、支援を続けてまいります。