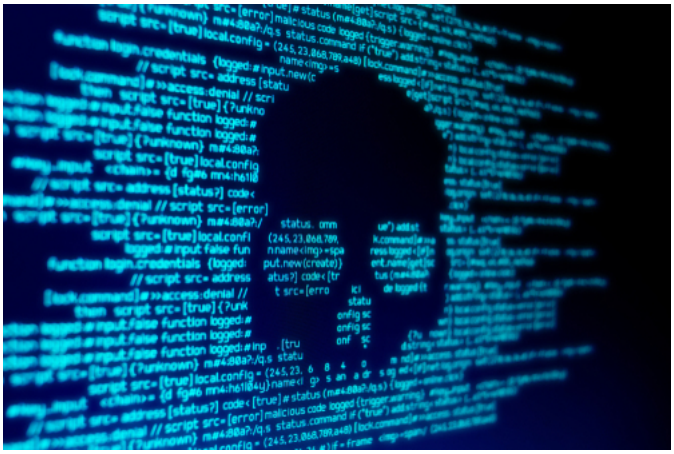
HARBOR BUSINESS Online
ハーバー・ビジネス・オンライン

IPA 情報セキュリティ10大脅威 2021 から考える「ポストコロナ社会のセキュリティ」

2021.02.06

柳井政和



shutterstock

IPAが恒例の情報セキュリティ10大脅威を発表

IPA（独立行政法人 情報処理推進機構）が、1月下旬に恒例の情報セキュリティ10大脅威を発表した。前年に発生した情報セキュリティ事案をIPAが選出して、情報セキュリティ分野の研究者、企業の実務担当者などが、脅威候補に対して審議・投票を行い、決定したものだ。

2016年以降は、個人部門と組織部門に分かれて発表しているが、それ以前は総合順位の発表となっている。この情報セキュリティ10大脅威を見ると、どういったセキュリティの問題が、それぞれの時代で起きているのかが分かる。

というわけで、今回の10大脅威を見たあと、それらが、過去にどのような順位変動をしていたのか、たどっていこう。

今年の情報セキュリティ10大脅威 個人部門

まず、個人部門である。順位は以下のようになっている。

1位　スマホ決済の不正利用
2位　フィッシングによる個人情報等の詐取
3位　ネット上の誹謗・中傷・デマ
4位　メールやSMS等を使った脅迫・詐欺の手口による金銭要求
5位　クレジットカード情報の不正利用
6位　インターネットバンキングの不正利用
7位　インターネット上のサービスからの個人情報の窃取

8位　偽警告によるインターネット詐欺
9位　不正アプリによるスマートフォン利用者への被害
10位 インターネット上のサービスへの不正ログイン

1位の「**スマホ決済の不正利用**」は、昨年の2020年に1位として初登場したものだ。スマホ決済にまつわるトラブルは、2020年、2019年に巨大なものが相次いで報道された。

2位の「**フィッシングによる個人情報等の詐取**」は、長い年月にわたって上位に君臨している。フィッシングはインターネット上の詐欺の方法の1つだ。偽装サイトに誘導して、情報を抜き取る手法を指す。

2020年、2019年は2位、2018年は「**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**」と名前が変わるが1位となっている。

この「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」は、**被害の増加と手口の多様化**に伴い、2019年には「インターネットバンキングの不正利用」「クレジットカード情報の不正利用」「仮想通貨交換所を狙った攻撃」「仮想通貨採掘に加担させる手口」「フィッシングによる個人情報等の詐取」に分割された。

「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」は2017年、2016年、2015年も1位になっている。2015年から2012年は、個人、組織と部門が分かれておらず、総合しか掲載されていないが、2014年に「オンラインバンキングからの不正送金」が5位、2013年に「フィッシング詐欺」が10位に入っている。この10年弱、ずっと大きな被害が続いている攻撃手法と言える。

3位の「**ネット上の誹謗・中傷・デマ**」も根強く被害の多い脅威だ。2020年7位、2019年5位、2018年5位、2017年7位、2016年6位となっている。誹謗中傷により、自殺に追い込まれる人もいるなど、生命に危険がおよぶ脅威だ。

4位の「**メールやSMS等を使った脅迫・詐欺の手口による金銭要求**」は、2020年には5位、2019年には4位で初登場になっている。「あなたのPCをハッキングしました」「未納料金があります」などのメッセージで、金を払わせる手法だ。古くから見られるやり方だが、上位の方にあるのは、まだまだ有効な手法なのだろう。

5位の「**クレジットカード情報の不正利用**」は、2020年には3位、2019年には1位だった。それ以前は、「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」と名前が変わるが、ずっと1位にある。近年順位が徐々に下がっているのは、それ以外の脅威が大きくなってきたせいだろう。

6位の「**インターネットバンキングの不正利用**」は、2020年に4位、2019年に7位で、それ以前は、「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」と名前が変わる。

インターネットバンキングは、認証アプリの改良など、年々セキュリティが厳しくなっている。新興のスマホ決済よりも、セキュリティは厳格だと感じる。

7位の「**インターネット上のサービスからの個人情報の窃取**」は、IDやパスワード、住所、氏名、電話番号、クレジットカード番号などを盗む行為だ。

8位の「**偽警告によるインターネット詐欺**」は、2020年に9位、2019年に6位、2018年に10位となっている。順位は上位ではないが、私自身もちょくちょくと見かける。インターネットを閲覧しているときに「ウイルスに感染しています」という表示を急に出すような手法だ。慌てた人が連絡を取ったり、誘導されるままに対策ソフトをインストールすることで被害に遭う。

9位の「**不正アプリによるスマートフォン利用者への被害**」は、モバイルの公式アプリストアの審査をすり抜けた悪意のあるアプリが、重要な情報などを盗んだりする攻撃だ。有名企業の公式アプリに見せかけた偽アプリも多い。年々、アプリストアの審査は厳しくなっているが、イタチごっこになってしまっている。

この脅威は、2020年には6位、2019年には3位、2018年には4位、2017年、2016年には3位になっている。また、総合順位のみの2015年では10位、2014年は6位、2013年には3位、2012年には6位と、古くから被害が続いている。

10位の「**インターネット上のサービスへの不正ログイン**」は、2020年、2019年は8位、2018年は5位、2017年は4位、2016年は5位、2015年は4位、2014年は2位になっている。傾向としては、順位が徐々に下がっている。

しかし、安全になってきているというわけではない。インターネットサービスでのパスワードの流出は、毎年のように起きている。パスワードの使い回しをしないといった自己防衛が必要になる。

次のページ>　**組織部門では「テレワーク狙い」の被害が上位に**

今年の情報セキュリティ10大脅威 組織部門

次に、組織部門である。

1位　ランサムウェアによる被害
2位　標的型攻撃による機密情報の窃取
3位　テレワーク等のニューノーマルな働き方を狙った攻撃
4位　サプライチェーンの弱点を悪用した攻撃
5位　ビジネスメール詐欺による金銭被害
6位　内部不正による情報漏えい
7位　予期せぬIT基盤の障害に伴う業務停止
8位　インターネット上のサービスへの不正ログイン
9位　不注意による情報漏えい等の被害
10位 脆弱性対策情報の公開に伴う悪用増加

組織部門で注目すべき点は、3位の「**テレワーク等のニューノーマルな働き方を狙った攻撃**」だ。これまで社内のパソコンで仕事をして、社内のネットワークでデータをやり取りしていたのが、自宅勤務により、各自の自宅で仕事をしてインターネット経由でデータをやり取りするようになった。

仮想専用回線などを利用してデータをやり取りする企業もあるだろうが、全ての企業が、そうした措置をとるわけではない。また、個人のパソコンで仕事をしているところもあるだろう。セキュリティのルールをどうするかなど、慌ただしく移行した場合には、適切なルールが存在しないこともあるはずだ。

そうした状態での、新しいセキュリティ的な脅威が多数発生していることは、想像に難くない。

さて、残りの順位も見ていこう。1位の「**ランサムウェアによる被害**」は、ファイルを暗号化するなどして重要なデータを人質に取り、その救出のために身の代金を払わせるという攻撃だ。

この脅威は、2020年は5位、2019年は3位、2018年、2017年は2位、2016年は7位になっている。データをもとにサービスを提供している会社にとって、データが人質に取られるのは致命的だ。個人を狙う攻撃が、広く浅く金を得るやり方だとすると、組織を狙う攻撃は、大きな金額を一発で得るやり方だと言える。こうした攻撃は、成功したときの金額が大きいので、攻撃者側にとって旨味が大きい。

2位は「**標的型攻撃による機密情報の窃取**」だ。先ほどと同じ理由で、金を持っている企業は、攻撃対象として狙われやすい。標的型攻撃は、攻撃対象の情報を集めて、カスタマイズした攻撃をおこなう方法だ。こうした攻撃は、金銭目的だけではなく、国家間の諜報でも用いられる。防衛関係の企業などが狙われているのは、そうした背景がある。

この脅威は、2020年から2016年にかけて連続1位だ。2015年に3位になっているが、それ以前はずっと1位か2位が続いている。企業が最も気を付けなければならない脅威だと言える。

4位は「**サプライチェーンの弱点を悪用した攻撃**」だ。サプライチェーンは、調達や製造、在庫管理や物流、販売といった企業間のつながりのことだ。こうした繋がりの弱点を足掛かりにして、攻撃を広げていく手法を指す。

この脅威は、2020年、2019年ともに4位で、2019年から10大脅威に登場した。一社だけで防備を固めていても防げない厄介な攻撃だと言える。

5位は「**ビジネスメール詐欺による金銭被害**」だ。「口座が変わった」などの嘘の情報を送り、攻撃者の口座にお金を振り込ませるといった手口だ。直接的にお金を盗まれるので、高額な被害になることが多い。

この脅威は、2020年には3位、2019年には2位、2018年には3位となっている。近年脅威が警告されている攻撃手法だ。

便利にするはずのIT化が生み出すコスト

6位は「**内部不正による情報漏えい**」だ。廃棄予定のHDDの販売や、情報を盗んでの販売や転職などが当たる。内部不正は、内部事情を知り尽くしている人がおこなうので防ぐのは難しい。内部の管理がずさんになっていたり、経営陣が恨みを持たれていたり、理由も千差万別だろう。

この脅威は、2020年には2位、2019年には5位、2018年には8位、2017年には5位、2016年、2015には2位、2013年には9位、2012年には7位となっている。大きな内部不正があると順位が高くなるが、基本的には常時発生していて、問題になっている脅威だと言える。

7位は「**予期せぬIT基盤の障害に伴う業務停止**」だ。東証の停止などは記憶に新しい。他にもクラウドの停止など、業務が止まることはたびたび発生する。こうしたトラブルを完璧に防ぐことは難しいだろう。停止を少なくすることは当然として、停止する前提で、日頃から準備をしておく必要がある。

この脅威は、2020年に6位で初登場している。世の中の仕組みが、IT中心になってきたことの、ある意味証拠かもしれない。

8位は「**インターネット上のサービスへの不正ログイン**」だ。この年、10大脅威に初登場したが、常時どこかで起きている脅威だ。

9位は「**不注意による情報漏えい等の被害**」だ。よくあるトラブルは、ノートパソコンを入れた鞄を忘れる、添付付きメールの誤送信などだ。人間なので、どんなに注意していても発生してしまう。意識を高めることも重要だが、ルール作りや運用、ソフトウェアによるチェックなど、システム側で被害を減らす工夫も必要になる。

この脅威は、2020年は7位、2019年は10位となり、近年注目され始めたことが分かる。

10位は「**脆弱性対策情報の公開に伴う悪用増加**」だ。この年に初登場した10大脅威だ。脆弱性対策情報が公開されたら、素早くその対策を実施しなければならない。しかし、その脆弱性への対策をおこなわない人や組織も多い。その結果、脆弱性だけが悪用されて、攻撃の材料になる。

ITが業務の中心になると、こうした対策を常時おこなわなければならなくなる。仕事を楽にするためにITを導入しているのに、仕事が増えるという皮肉が発生する。それでもIT化しなければ時代に取り残されるので、こうしたところに経営者がコストを割かなければならない。

次のページ>　**ポストコロナ社会のセキュリティ**

ポストコロナ社会のセキュリティ

2020年、新型コロナウイルスの登場により、世の中は大きく変わった。多数の人を集めて、一ヶ所で密集して仕事をするという様式は、感染症を蔓延させて業務を停止させてしまうというリスク要因となった。その結果、自宅からリモートで仕事をおこなうという分散様式が求められるようになった。

集中して管理するよりも、分散して管理する方が、当然管理は難しくなる。そして、それぞれの仕事場所の状況が異なるとなると、対策も多岐にわたる可能性があり、難易度は上昇する。

自宅勤務をしていると、それこそ家族間で別会社のデータが丸見えになるというリスクだってある。気分転換にカフェで仕事をしていて、そのままノートパソコンを忘れて帰ることもあるだろう。

まだ、コロナ禍から1年ほどだが、分散型の仕事環境に完全に移行できた会社はどのぐらいあるのだろうか。まだまだ模索の時期だと思うが、緊急事態宣言が伸びた今、今後のセキュリティについて、考えていく必要があるだろう。

＜文／柳井政和＞