

中小企業におけるサイバーセキュリティ対策の実態*

日本政策金融公庫総合研究所特任研究員

竹 内 英 二

要 旨

いまや経済社会の発展に情報通信技術の利用は欠かせない。政府の「成長戦略実行計画」（2021年6月）では、デジタル化への集中投資とその成果を社会に実装することが新たな成長への原動力になるとしている。中小企業も、情報通信技術を活用して、業務を効率化するだけでなく、新たな製品やサービスを開発し、あるいは新しいビジネスを開発していくことが期待される。ただし、デジタル化を進めれば、サイバー犯罪に遭うリスクも増す。不正プログラムに感染して工場が操業停止に追い込まれたり、ホームページが書き換えられて個人情報流出してしまったりといった例は枚挙にいとまがない。デジタル化にサイバーセキュリティ対策は欠かせないのであるが、果たして中小企業はどれだけサイバー犯罪に備えているだろうか。

そこで、日本政策金融公庫総合研究所は、パソコンやスマートフォンなど情報機器を利用している中小企業を対象に、サイバーセキュリティ対策の実施状況に関するインターネットアンケートを実施した。アンケートの主な結果は次のとおりである。第1に、ソフトウェアのアップデートやセキュリティソフトの利用など基本的なサイバーセキュリティ対策すら実施していない企業が少なくない。第2に、利用している情報機器の数が多い企業ほど、必要な対策をとっている企業の割合が多くなる。業務のデジタル化を進めるほど、サイバーセキュリティ対策の必要性を理解するようになるのだと思われる。第3に、中小企業のサイバーセキュリティ対策は総じて遅れているが、明確な理由があるわけではなく、対策を進めるうえでの障害は特にないとする企業の割合は半数を超える。サイバーセキュリティ対策が必要なことはわかっている、取り組む優先順位が低い課題だと考える中小企業が少なくないのだと思われる。

中小企業のサイバーセキュリティ対策を強化するには、中小企業のデジタル化とサイバーセキュリティ対策をセットにして支援するだけでなく、中小企業がサイバーセキュリティ対策を進めざるを得ないような環境をつくっていくことも重要である。

* 本稿は、当研究所発行の『日本公庫総研レポート』No. 2022-1「中小企業に求められるサイバーセキュリティ対策の強化」（2022年1月）の一部に手を加えて再掲したものである。本稿で紹介しているアンケート結果の詳細については、同レポートを参照されたい。

1 問題意識

情報通信技術（ICT）の活用は、国にとっても企業にとっても重要な課題になっている。例えば、政府の「成長戦略実行計画」（2021年6月）は、デジタル化への集中投資とその成果を社会に実装することが新たな成長への原動力になるとしている。ICTを活用することで、企業や行政におけるコストダウンや作業効率の向上を図るだけではなく、新たな製品やサービスを開発し、さらには新規のビジネスを創造することで生産性や賃金の上昇、社会的な問題の解決が期待できるからだ。

ICTを活用し、業務のデジタル化を進めていくうえで欠かせないのが情報セキュリティ、なかでもサイバーセキュリティである。デジタル化が進めば、それだけ情報の詐取や不正アクセスといった犯罪も増える。個人情報や取引情報が漏洩すれば企業は信用を失い、損害賠償を求められることもある。データが消去されたり紛失したりすれば、業務の遂行に支障を来す。

情報セキュリティは、アクセスを認められた者だけが情報にアクセスできる状態を確保する「機密性」、情報が改竄されたり消去されたりしていない状態を確保する「完全性」、情報へのアクセスを認められた者が必要な時に中断されることなく情報にアクセスできる状態を確保する「可用性」の三つを維持することをいう。紙の書類などデジタル化されていない情報も対象になるし、停電やパソコンの故障など偶発的な事故や自然災害に対する備えも検討しなければならない。

サイバーセキュリティは、情報セキュリティの一部で、パソコンに記録されたデータなどデジタルデータをコンピューターウイルスや不正アクセス、従業員による持ち出しといった脅威や攻撃から守ることをいう。2015年に施行されたサイバーセキュリティ基本法は、国や地方公共団体にはサ

イバーセキュリティに関する施策を策定し、実施する責務があるとするだけではなく、国民にもサイバーセキュリティの重要性に関する関心と理解を深め、サイバーセキュリティの確保に注意を払うよう求めている。

中小企業ではICTの活用が遅れているとされる。業種や事業の規模によってはICTを活用する必要が乏しい場合もある。しかし、携帯電話やスマートフォンの普及とともに、ICTは中小企業の日常に浸透してきている。2020年からは新型コロナウイルス感染症の影響で、テレワークを始めたりオンライン会議を行ったりする中小企業も増えているだろう。それだけサイバー攻撃のリスクにさらされる中小企業も多くなる。世界的にデジタル化が進行するなか、中小企業はどれだけ外部からのサイバー攻撃に備えているだろうか。本稿では、日本政策金融公庫総合研究所が実施したアンケートの結果をもとに、中小企業におけるサイバーセキュリティ対策の実態を探る。

2 増加するサイバー攻撃

（1）デジタルデータに対する攻撃・脅威の例

デジタルデータに対する脅威や攻撃にはさまざまなものがある。次ページの表は独立行政法人情報処理推進機構（IPA）が毎年発表している「情報セキュリティ 10大脅威」の2021年版である。

IPAは、個人に対する脅威と企業や官公庁など組織に対する脅威の二つに分類しているが、必ずしも個人に対する脅威は組織に対する脅威ではないということではない。例えば、個人に対する脅威で上位に挙げられている「スマホ決済の不正利用」や「フィッシングによる個人情報等の詐取」は、企業でも起こり得る。特に私物のパソコンやスマートフォンを業務で利用している場合は、経営者や従業員への攻撃がそのまま企業への攻撃に

表 情報セキュリティの10大脅威（2021年）

順 位	組織に対する脅威	個人に対する脅威
1	ランサムウェアによる被害	スマホ決済の不正利用
2	標的型攻撃による機密情報の窃取	フィッシングによる個人情報等の詐取
3	テレワーク等のニューノーマルな働き方を狙った攻撃	ネット上の誹謗・中傷・デマ
4	サプライチェーンの弱点を悪用した攻撃	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	ビジネスメール詐欺による金銭被害	クレジットカード情報の不正利用
6	内部不正による情報漏洩	インターネットバンキングの不正利用
7	予期せぬIT基盤の障害に伴う業務停止	インターネット上のサービスからの個人情報の窃取
8	インターネット上のサービスへの不正ログイン	偽警告によるインターネット詐欺
9	不注意による情報漏洩等の被害	不正アプリによるスマートフォン利用者への被害
10	脆弱性対策情報の公開に伴う悪用増加	インターネット上のサービスへの不正ログイン

出所：独立行政法人情報処理推進機構（IPA）のホームページ（<https://www.ipa.go.jp/security/vuln/10threats2021.html>）

もなる可能性が大きい。

10大脅威を個々にみていくと、多くが外部からの攻撃（サイバー攻撃）となっている。サイバー攻撃の種類や手口は多く、変化も激しい。詳細はIPAのホームページなど専門のサイトに任せ、ここでは代表的な攻撃について簡単に説明するにとどめたい。

「ランサムウェア」は、不正プログラム（コンピューターウイルスやスパイウェアなど悪意のあるプログラムの総称。マルウェアともいう）の一種で、侵入したパソコンの内部にあるファイルを暗号化したりパソコンをロックしたりしてデータを「人質」にとり、データの復旧と引き換えに身代金（ランサム）を要求するものである。近年は、身代金を支払ったかどうかにかかわらず、人質にしたデータを暴露するものもみられる。

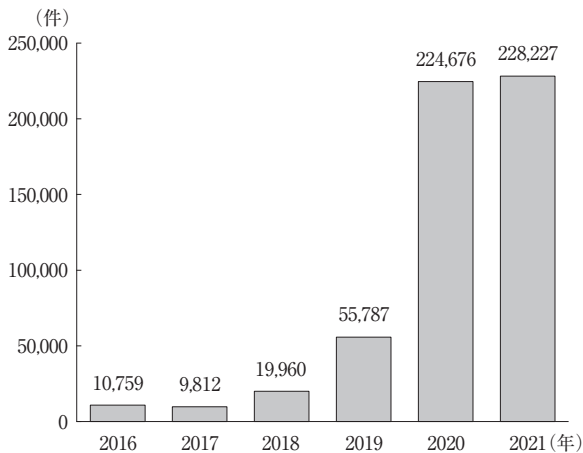
不正プログラムの多くが不特定多数にばらまかれるのに対し、「標的型攻撃」は特定の個人や組織を対象とする。標的にした企業の情報を収集・

分析したうえでターゲットを定め、実在する取引先やターゲットの上司をかたり、ターゲットが開きたくするような内容を書いたメールを送る。ターゲットが添付ファイルを開いたり、メール本文に記されたリンクを開いて不正なホームページを閲覧したりするとウイルスに感染し、重要な情報が盗まれる。周到に準備したうえで攻撃してくるため、完全に防ぐのは難しいとされる。

「サプライチェーンの弱点を悪用した攻撃」は、狙った企業のセキュリティが強固である場合に、標的の企業と取引のある企業のなかからセキュリティの甘い企業を探して侵入し、そこを足がかりに本来の標的を攻撃するものである。大規模なサイバー攻撃は大企業が標的になることが多いが、この攻撃では中小企業も標的になる。

「フィッシング」は、実在する企業や役所をかたってメールやSMS（携帯電話やスマートフォンのショート・メッセージ・サービス）を送信し、偽のホームページに誘導して、クレジットカード

図－1 フィッシング報告件数の推移



資料：フィッシング対策協議会「フィッシング報告状況」
(注) 2021年は6月までの報告件数。

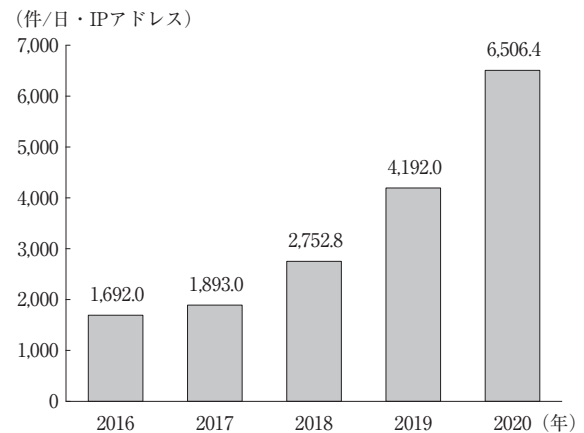
や預金口座の番号、IDやパスワードといった情報を入力させる詐欺である。被害に遭うと、情報が盗まれるだけではなく、不正送金に使われるなど金銭の被害が発生することも少なくない。フィッシングメールは不特定多数に送信されるものであり、消費者に限らず、企業や企業の従業員が被害に遭う可能性も十分にある。

(2) データでみるサイバー攻撃

サイバー攻撃の動向について、いくつかデータをみていこう。図－1は、フィッシング対策協議会に消費者や企業から寄せられたフィッシング報告件数の推移を示したものである。2020年は前年の約4倍に増え、2021年は6月までの半年で前年を上回った。

サイバー攻撃は、昼夜を問わず、休むことなく行われている。そこで、警察庁は全国の警察施設にあるインターネットとの接続点にセンサーを設置して24時間体制でインターネットを監視し、通常のインターネット利用では考えられない接続情報を検知している。その集計結果をみると、年々増加傾向にあり、近年は増加のペースも増してい

図－2 警察庁のセンサーが検知したアクセス件数の推移



資料：警察庁「令和2年におけるサイバー空間をめぐる脅威の情勢等について」(2021年3月4日)

ることがわかる(図－2)。

検知したアクセスがすべて不正なものとは限らないが、警察庁は検知したアクセスの大半は、不特定多数のIPアドレスを対象とするサイバー攻撃やインターネットに接続された機器の脆弱性を探索するサイバー攻撃の準備行為とみられるとしている。

なお、警察庁はサイバー攻撃やその準備行為が急増している要因として、ウェブカメラや無線LANのルーターなどIoT機器¹やリモート・デスクトップ・サービスを狙った攻撃が増えていることを指摘している。どちらも、コロナ禍で増加したとされるテレワークやリモートワークで利用が増えた機器やサービスである。

膨大な数のサイバー攻撃が行われているのであるが、犯罪として認知される攻撃の数はそれほど多くはない。警察庁・総務省・経済産業省の報道資料「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」(2021年3月4日)によると、不正アクセス行為の認知件数は、2020年で2,806件であり、そのうち2,703件は企業に対するものであった。

¹ インターネットに接続された機器の総称。ウェブカメラやルーターのほかにスマート家電や自動運転車などがある。

不正アクセスの認知件数をみると、サイバー攻撃の被害に遭うのはごく一部の企業に思えるかもしれない。だが、具体的な被害がなかったり、被害に気づかなかつたりするだけで、実際にはずっと多くの企業が不正アクセスなど、さまざまなサイバー攻撃を受けている。

例えば、経済産業省がIPAを通じて2020年度に実施した「中小企業向けサイバーセキュリティ対策支援体制構築事業」では、参加した中小企業1,117社にUTM機器²やEDRソフト³などセキュリティ機器を設置したところ、企業規模や業種を問わず、ほとんどの企業で不正アクセスの試みや不正プログラムへの感染、フィッシングサイトへのアクセスなど、何らかの脅威・攻撃が検知されたという。

3 対策の基本：脆弱性の解消と手口の学習

サイバー攻撃の種類や手口は多いが、公安調査庁の「サイバー空間における脅威の概況2021」によれば、大半の攻撃はコンピューターシステムの脆弱性か、人間の心の隙をついて行われる。つまり、この二つについて対策をとればサイバー攻撃の多くは防ぐことができる。

(1) 脆弱性をついた攻撃

脆弱性は、多くのソフトウェア製品やウェブアプリケーションで確認されている。ウェブアプリケーションもソフトウェアであるが、パソコンやスマートフォンにインストールする必要がなく、「グーグルクローム」や「サファリ」「マイクロソ

フトエッジ」など、インターネットを閲覧するためのブラウザがあれば利用できる。ウェブアプリケーションは、ホームページを閲覧している人が何らかの行動をとることを可能にするもので、電子掲示板やSNS、通販サイトでの買い物やレビューの投稿、サービスの申し込みフォームなど多くの種類がある。

IPAは、2004年7月から、開発者を含めて脆弱性を発見した人や企業からの報告を受け付けているが、2021年9月末までにソフトウェア製品については4,947件、ウェブアプリケーションについては1万2,042件、合わせて1万6,989件の報告が寄せられている⁴。

ソフトウェアの脆弱性は、多くの不正プログラムで利用されている。ウェブアプリケーションの脆弱性は、ホームページを書き換える、個人情報情報を盗み取る、他人に成り済ましてサービスを利用する、ホームページの閲覧者を詐欺サイトに誘導する、ウェブ上のサービスを停止させるといった攻撃に利用される。

脆弱性が発見されると、ソフトウェアやウェブアプリケーションの開発者は、その事実を公表するとともに、脆弱性を解消するための追加プログラム（セキュリティパッチ）を作成し、インターネットを通じて配布する。セキュリティパッチを適用すれば、脆弱性は解消できる。サイバー攻撃の犯人は公表されたことで脆弱性の存在を知り、攻撃を仕掛けてくることも多いので、ソフトウェアは常に最新の状態にし、判明した脆弱性を解消しておく必要がある。

開発者も知らない脆弱性についてくるサイバー

² UTMはUnified Threat Management(統合脅威管理)の略。ファイアウォールやアンチウイルスなど複数のセキュリティ機能を持ち、サイバーセキュリティを一元的に管理する機器をUTM機器という。

³ EDRはEndpoint Detection and Responseの略。パソコンなど端末(endpoint)の挙動を監視してマルウェアなどに感染していないかを調べ(detection)、感染していると判断した場合は不正なファイルを削除したり、感染が疑われる端末を社内ネットワークから遮断したりするなど必要な対応(response)をとるソフトウェア。アンチウイルスソフトは既知の不正プログラムにしか対応できないが、EDRソフトは新種の不正プログラムに感染した場合でもセキュリティを確保することが可能とされる。

⁴ IPAホームページ(<https://www.ipa.go.jp/security/vuln/report/vuln2021q3.html>)。なお、脆弱性として報告されても開発者などが検討した結果、脆弱性ではないと判断されるものもある。

攻撃もあり、これを完全に防御することは難しいが、それでもソフトウェアを最新の状態にしておくことや、セキュリティソフトを導入することなどで、ある程度防ぐことはできるとされる。

脆弱性はパソコンやスマートフォンで使うソフトウェアだけではなく、インターネットに接続して使う各種のIoT機器にも存在する。IoT機器を制御するソフトウェア（ファームウェア）に欠陥が存在することがあるのだ。前述したIoT機器を対象とするサイバー攻撃はファームウェアの脆弱性を悪用している。パソコンやスマートフォンと同様に、IoT機器もファームウェアを更新し、最新の状態にしておく必要がある。

（2）心の隙をつく攻撃

人間の心の隙をついたサイバー攻撃の典型は、標的型攻撃やフィッシング、ビジネスメール詐欺である。フィッシングは多くの消費者や企業が利用している金融機関やインターネットショッピングのサイト、宅配業者をかたってIDやパスワードなどを盗もうとするのに対して、ビジネスメール詐欺は、標的型攻撃と同様に、取引先や経営者に成り済まし、指定する銀行口座（多くは海外の口座）に送金させようとする。

偽のホームページに誘導するフィッシングについては、不正なホームページを検出するセキュリティソフトがあるが完璧ではない。不正プログラムにはアンチウイルスソフトがあるが、標的型攻撃では新種の不正プログラムが利用されることが多いため、アンチウイルスソフトでは防ぎきれない。また、不審なメールを受信しないようにするメールのフィルタリングサービスやセキュリティソフトもあるが、やはり完全に防御することはできない。

従って、人の心の隙をつくサイバー攻撃を防ぐには、セキュリティソフトを使うだけではなく、犯罪目的のメールやSMSが存在すること、そし

て具体的な文面など、手口を知っておくことが重要だと思われる。

フィッシングについては、フィッシング対策協議会が事例を収集し、ホームページで公開しているほか、「利用者向けフィッシング詐欺対策ガイドライン」を作成している。ビジネスメール詐欺については、IPAの『ビジネスメール詐欺「BEC」に関する事例と注意喚起（第三報）』に詳しい。標的型攻撃についても、IPAの「標的型攻撃メールの例と見分け方」がある。

4 中小企業におけるデジタル化の状況とサイバーセキュリティ対策の実態

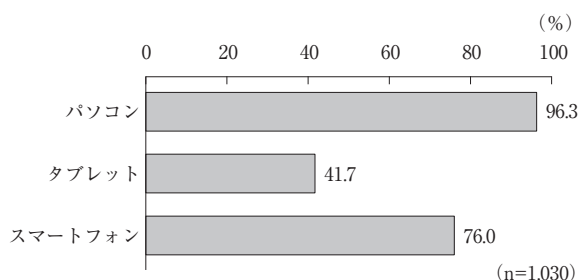
本節では、当研究所が2021年4月にインターネット調査会社を通じて実施した「情報セキュリティに関するアンケート」（以下ではアンケートという）の結果を用い、中小企業におけるデジタル化の状況とサイバーセキュリティ対策の実態をみていく。

（1）調査要領と回答企業の属性

アンケートの結果をみていく前に、アンケートの実施要領と回答した企業の属性を簡単に説明する。まず調査対象は、中小企業基本法で定める中小企業のうち、仕事で情報機器（パソコン、タブレット、スマートフォン）を利用している企業である。ただし、従業員や会社役員の私物だけを利用している企業は含まない。

私物の情報機器を仕事で使用することは、機器の盗難や紛失による情報漏洩のリスクを高めるなど、サイバーセキュリティ上というよりは情報セキュリティ上問題がある。しかし、役員や従業員が所有する情報機器とその利用状況を企業がすべて把握し、サイバーセキュリティ対策を実施することは難しい。そのため、従業員や役員の私物を利用しているだけという企業は調査対象から除外

図－３ 仕事で利用している情報機器（複数回答）



資料：日本政策金融公庫総合研究所「情報セキュリティに関するアンケート（2021年4月）」（以下同じ）

（注）nは回答数。また、回答割合は小数第2位を四捨五入している（以下同じ）。

した。調査方法は、インターネットを使ったアンケートで、1,030社から回答を得た。

1,030社の内訳は、個人事業主が78.3%、会社が21.7%となっている。また、従業員規模の構成比は、「1人」が58.3%、「2～4人」が25.8%、「5～9人」が7.7%、「10人以上」が8.3%である。業種構成は、「専門技術サービス、学術研究」が20.4%で最も多く、以下「小売業」の12.5%、「建設業」の10.3%と続く。ほかの業種は、いずれも10%に満たず、比較的分散している。

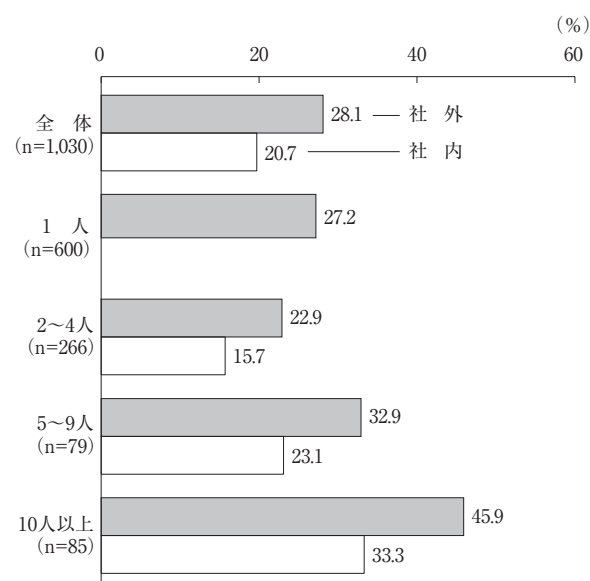
最後に情報機器を仕事で利用している企業の割合をみると、パソコンが96.3%、タブレットが41.7%、スマートフォンが76.0%となっている（図－3）。スマートフォンやタブレットの利用が増えているとはいえ、パソコンの方が作業しやすい業務も多い。中小企業におけるICTの利用は、依然としてパソコンが中心となっている。

（２）業務のデジタル化

① コミュニケーション

サイバー攻撃によく使われるのが、メールやSMSである。LINEなどメッセージアプリは、アカウントの乗っ取りなどサイバー攻撃の対象にもなる。取引先など社外の人とコミュニケーションをとるために、メールやメッセージアプリを使っている企業の割合をみると、73.8%が利用していると回答した。

図－４ オンライン会議用ソフトウェアを利用している企業の割合（従業員規模別）



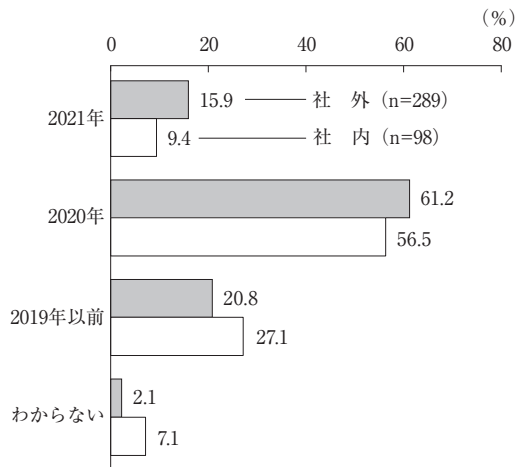
（注）n値は「社外」についてのもの。「社内」については「全体」が411、「2～4人」が249、「5～9人」が78、「10人以上」が84。これは従業員がいるにもかかわらず、社内でのオンライン会議用ソフトウェアの利用について「従業員はいない」と回答した企業を除いたためである。オンライン会議用ソフトウェアを利用している企業の従業員規模ごとの割合も、「従業員はいない」と回答した企業を除いて算出した。

高速の通信回線が普及したことや無料または安価なサービスが提供されていることもあり、近年はオンライン会議（ウェブ会議）が容易に実施できるようになっている。そのため、企業の内外を問わず、コミュニケーションの手段としてオンライン会議を利用する企業が増えている。

アンケートで、オンライン会議用ソフトウェアを利用している企業の割合をみると、全体では取引先など「社外」とのコミュニケーションに利用している企業の割合が28.1%、従業員との会議など「社内」でのコミュニケーションに利用している企業の割合が20.7%となっている（図－4）。

オンライン会議用ソフトウェアを利用している企業の割合は、おおむね従業員数が多いほど多くなる。また、業種別に利用企業の割合をみると、社外については「情報通信業」が51.1%、「専門技術サービス、学術研究」が41.4%と多く、「小売業」は14.0%と少ない。社内についても、「情

図－5 オンライン会議用ソフトウェアを利用し始めた時期



報通信業」が41.9%、「専門技術サービス、学術研究」が32.2%と多く、「小売業」は11.6%と少ない。

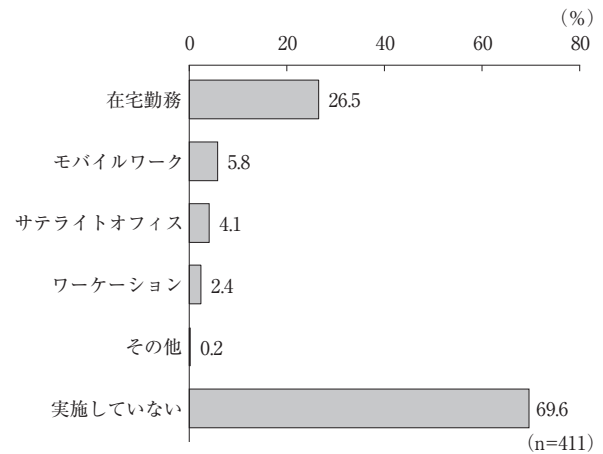
オンライン会議用のソフトウェアを利用し始めた時期をみると、社外は「2021年」が15.9%、「2020年」が61.2%、社内は「2021年」が9.4%、「2020年」が56.5%となっており、新型コロナウイルス感染症が広がるなかでオンライン会議を始めた企業が多いことがうかがえる（図－5）。

② テレワーク

一般社団法人日本テレワーク協会によると、テレワークとは「ICTを活用した、場所や時間にとられない柔軟な働き方のこと」であり、業務のデジタル化が進むほど導入しやすくなる。

従業員がいる企業について、テレワークを実施している割合をみると、従業員が自宅で就業する「在宅勤務」が26.5%、出張先や移動中の電車のなかなどで仕事をする「モバイルワーク」が5.8%、本社から離れた場所に設けた事務所やレンタルオフィスなどで仕事をする「サテライトオフィス」が4.1%、リゾートなどバケーションも楽しめる場所で仕事をする「ワーケーション」が2.4%となっている（図－6）。また、何らかのテレワークを実施している企業の割合は30.4%となっている。

図－6 実施しているテレワークの種類（複数回答）



テレワークのうち、「在宅勤務」を導入した時期をみると、「2019年以前」が38.5%を占めているものの、「2020年」が53.2%、「2021年」が8.3%となっており、オンライン会議と同様に、新型コロナウイルス感染症対策として「在宅勤務」を導入した企業が多いことがわかる。

一方、テレワークを「実施していない」企業の割合は69.6%と多くを占める。業種別にみると、「建設業」が89.8%、「医療、福祉」が89.7%、「生活関連サービス、娯楽業」が81.2%と多い。生産と消費が同時に行われるサービス業や現場でなければ作業ができない建設業でテレワークの導入が進んでいないのは仕方のないことだろう。

③ ホームページの運営

ホームページは、企業や製品のPR、通信販売や受注の獲得、採用活動など、多様に使える便利な道具である。一方で、ホームページはウェブアプリケーションの脆弱性につかれて顧客情報が盗まれたり、改竄されて不正プログラムが仕込まれたり、サイバー攻撃の対象になる。

アンケートで、ホームページがある企業の割合をみると、全体では33.3%となっている（図－7）。ホームページが「ある」と回答した企業の割合は

図－７ 企業ホームページの有無（従業者規模別）

(単位:%)

	あ る	な い
全 体 (n=1,030)	33.3	66.7
1 人 (n=600)	26.2	73.8
2～4人 (n=266)	37.6	62.4
5～9人 (n=79)	46.8	53.2
10人以上 (n=85)	57.6	42.4

従業者規模が大きいくほど多く、「1人」の企業では26.2%であるのに対し、「10人以上」では57.6%となっている。

ホームページを運営するには、ウェブサーバーが必要である。ウェブサーバーは自社で設置することもできるし、ホスティング会社から借りることもできる。アンケートでは、レンタルサーバーなど外部のサーバーを借りている企業の割合が68.2%、「社内にある」とする企業の割合が28.6%、「社内にも社外にもある」とする企業の割合が3.2%となっている。

レンタルサーバーやクラウドサーバーといった外部のサーバーは、社内にサーバーを設置して運用するよりも、初期費用や管理費用が安く済むことが多い。データの暗号化や不正アクセスの防止、改竄を検知するサービスなど、ホームページを運営するために必要なサイバーセキュリティ対策のツールも提供されている。そのため、外部のサーバーを利用することは、コストの面でもセキュリティの面でも中小企業にとって使い勝手がよい。ただし、レンタルサーバーが不正プログラムに感染した例もあり、外部のサーバーを使えば安心というわけではない。

④ 社内ネットワーク

情報機器は、単独で使うよりもネットワークを組んで利用する方が便利である。半面、1台が攻撃を許すとほかの情報機器も攻撃されるリスクが

図－８ 社内ネットワークの構築
(使用しているパソコンの数別)

(単位:%)

	構築している	構築していない
全 体 (n=1,030)	34.2	65.8
0 台 (n=38)	10.5	89.5
1 台 (n=535)	20.2	79.8
2～4台 (n=368)	45.9	54.1
5～9台 (n=54)	75.9	24.1
10台以上 (n=35)	85.7	14.3

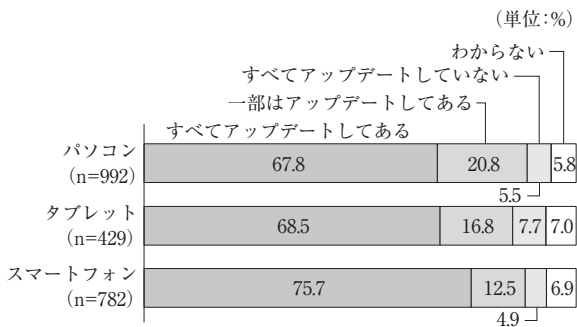
ある。アンケートで、情報機器の社内ネットワークを構築している企業の割合をみると、全体では34.2%にとどまっている（図－８）。構築している企業の割合は、使用している情報機器の数が多いほど多くなっている。パソコンを例にとると、「1台」の企業では20.2%であるのに対し、「2～4台」の企業では45.9%、「10台以上」の企業では85.7%となっている。タブレットやスマートフォンについても同様である。

⑤ 文書の保存

情報機器、特にパソコンの利用方法として最も一般的なものは、書類の作成と保存だろう。情報機器に保存した書類は、サイバー攻撃の対象になる。そこで、アンケートで書類の保存方法をみると、「個々の情報機器に保存」している企業の割合が75.3%と最も多く、「すべてサーバーに保存」している企業の割合は5.0%、「すべて紙ベースで保存」している企業の割合は13.1%、「サーバーまたは紙ベースで保存」している企業の割合は6.6%となっている。

文書を個々の情報機器に保存することは、サイバーセキュリティだけではなく、情報機器の盗難や紛失、故障といった情報セキュリティ上のリスクも高める。テレワークを実施する場合には、特

図－9 OSのアップデート状況



に望ましくないことであるが、アンケートによると、文書を個々の情報機器に保存している企業の割合は、テレワークを実施している企業でも81.6%を占めている。

また、個々の情報機器に保存している書類の種類（複数回答）をみると、帳簿や確定申告書など「経費や資金に関する書類」が54.2%で最も多く、以下、見積書や請求書など「受発注に関する書類」の45.6%、顧客名簿や購買履歴など「顧客に関する書類」の38.4%と続いている。取引先や顧客に関する情報など、重要度の高いデータを個々の情報機器に保存すれば、それだけサイバーセキュリティ対策の必要性も大きくなる。

（3）サイバーセキュリティ対策の実施状況

① ソフトウェアのアップデート

サイバーセキュリティの基本の一つは、使用しているソフトウェアをアップデートし、常に最新の状態に保つことである。まず、OS（WindowsやiOS、Androidなど）のアップデート状況を見ると、パソコン、タブレット、スマートフォンのいずれも、「すべてアップデートしてある」とする企業の割合は8割に満たない（図－9）。

一般に、情報機器を動かすための基本ソフトであるOSは、情報機器の購入時には自動的に更新されるように設定されている。そのため、「すべてアップデートしてある」とする企業の割合は、100%であってもおかしくない。

ただ、OSを更新すると、使用していたソフトウェアが動かなくなったり、データが紛失したりといった不具合が生じることがある。そのため、自動更新を無効にしたり、更新プログラムがあっても、すぐにはアップデートせず、様子見したりする企業もある。パソコンの場合は、使い勝手が変わるのが嫌だとか、買い替える費用がもったいないとかといった理由で、サポートが終了し、セキュリティパッチが配布されなくなった古いOSを使い続ける企業もある。それぞれに事情はあるにせよ、中小企業にOSのアップデートをしていない情報機器が少なからず存在することは、当該企業だけではなく、その取引先や顧客にとっても脅威となり得る。

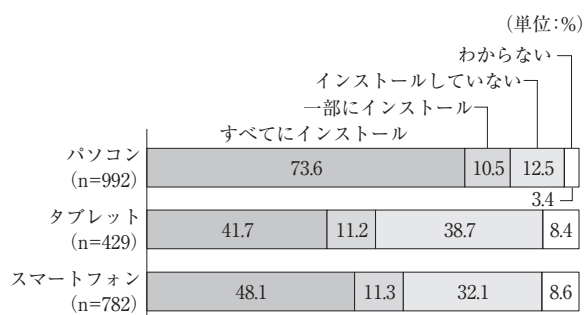
OS以外のソフトウェアやアプリには、情報機器にインストールして使うものと、インストールせずにクラウドサービスやウェブサービスとして使うものがある。後者の場合、ソフトウェアやアプリは常に最新の状態で利用できるが、前者の場合はアップデートが必要になる。

アンケートによると、クラウドサービスで利用しているソフトウェアやアプリがあるとする企業の割合は19.5%と少ない。一方、情報機器にインストールしてあるソフトウェアやアプリを「すべてアップデートしてある」とする企業の割合は74.8%にとどまる。OS以外のソフトウェアやアプリについても、サイバーセキュリティ上問題のある中小企業が少なくない。

② セキュリティソフトのインストール

セキュリティソフトは、不正プログラムへの感染を防いだり、不正なホームページの閲覧を阻止したり、不審なメールを検出したりと、各種のサイバー攻撃からデータやシステムを守るソフトウェアの総称である。セキュリティソフトを使用すれば、サイバー攻撃の多くを自動的に防ぐことができる。

図-10 セキュリティソフトのインストール



アンケートで情報機器にセキュリティソフトをインストールしているかどうかをみると、「すべてにインストール」とする企業の割合は、パソコンが73.6%、タブレットが41.7%、スマートフォンが48.1%となっている（図-10）。一方、「インストールしていない」とする企業の割合はパソコンが12.5%、タブレットが38.7%、スマートフォンが32.1%となっている。

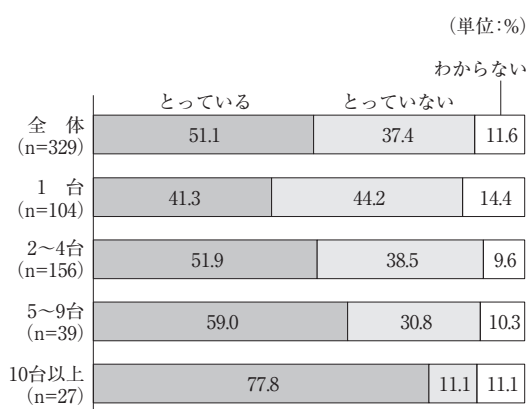
パソコンは、「Windows」「Mac」ともに最新のOSにはセキュリティソフトが組み込まれており、不正プログラム対策など基本的なセキュリティ機能はあるので、セキュリティソフトをインストールしていないからといって、必ずしもパソコンが無防備だというわけではない。タブレットやスマートフォンのうち、日本で広く利用されているアップルの製品についても同様である。

ただ、サイバー攻撃にはOSの機能では防ぐことができない、フィッシングなど詐欺目的のホームページもある。サイバーセキュリティに万全を期すならすべての情報機器にセキュリティソフトをインストールし、最新の状態を保つことが望ましい。

③ 不正アクセス対策

アンケートに回答した企業のうち、352社は社内ネットワークを構築しており、さらにそのうち329社は社内ネットワークをインターネットに接続している。この場合、個々の情報機器だけではなく、ネットワークのセキュリティ対策、特に外

図-11 社内ネットワークの不正アクセス対策（使用しているパソコンの数別）



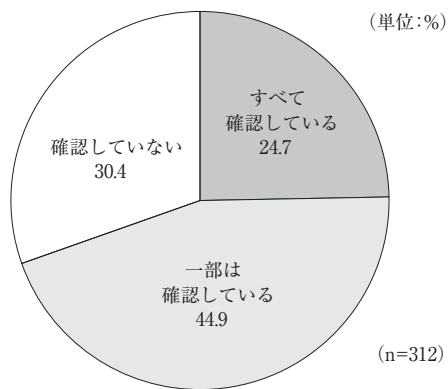
(注) パソコンを使っていない企業は3社しかないので省略した。

部からの不正アクセス対策も必要になる。

社内ネットワークをインターネットに接続していると回答した企業のうち、サーバーにファイアウォールソフトをインストールしたり、UTM機器を設置したりして、不正アクセス対策を「とっている」企業の割合をみると全体では51.1%となっている（図-11）。不正アクセス対策を「とっていない」企業の割合は、使用している情報機器の数が少ないほど多くなる傾向があり、特にパソコンについて顕著である。この傾向は、セキュリティソフトのインストールについても認められる。情報機器をあまり使っていない企業ほどサイバーセキュリティへの関心が低いと思われる。

また、今回のアンケートでは、ホームページを開設している企業が343社あり、そのうちウェブサーバーを社内を設置している企業が109社あった。アンケートによると、ウェブサーバーにファイアウォールソフトをインストールしたり、UTM機器を設置したりして不正アクセス対策を「とっている」企業の割合は44.0%で、「とっていない」とする企業の割合は31.2%、「わからない」とする企業の割合は24.8%だった。社内ネットワークと同じく、中小企業には無防備なウェブサーバーが少なくない。

図-12 オンライン会議用ソフトウェアやアプリの安全性



④ オンライン会議に関する対策

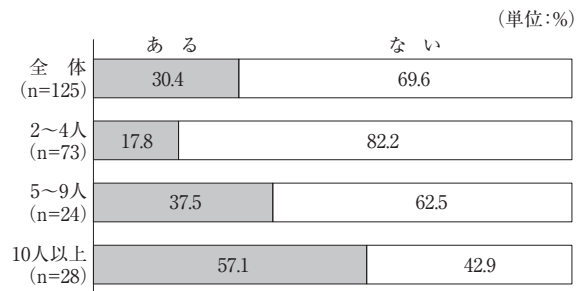
オンライン会議のセキュリティに関する注意点はいくつかあるが、基本的な事項として、使用するソフトウェアやアプリ、サービスが安全なものかどうかを確認することが挙げられる。具体的には、オンライン会議の音声や映像、共有資料など使用したデータはどこに格納されるのか、データは暗号化されているのか、会議参加者の認証方式はどうなっているのか、ソフトウェアに脆弱性はないかといったことを確認する。

オンライン会議用のソフトウェアやアプリを使用していると回答した企業について、その安全性を確認しているかをみると、「すべて確認している」企業の割合が24.7%、「一部は確認している」企業の割合が44.9%、「確認していない」企業の割合が30.4%となっている（図-12）。オンライン会議の安全性に関心のある企業が過半を占めてはいるが、関心のない企業も少なくない。

⑤ テレワークに関する対策

テレワークは、多かれ少なかれ、情報を企業の外に持ち出すことになるので、情報セキュリティ上のリスクを高める。従って、実施に当たっては就業規則を明確にするとともに、サイバーセキュリティ対策を含めた情報セキュリティ対策につい

図-13 テレワークに関する規定やルールを定めた文書の有無（従業員規模別）



ても規則を定め、従業員が判断に迷わないように明文化することが望ましい。

従業員のテレワークを実施していると回答した企業について、テレワークに関する規定やルールを定めた文書があるかどうかをみると、「ある」と回答した企業の割合は、全体では30.4%となっている（図-13）。規定やルールを定めた文書が「ある」とする企業の割合は、従業員数が多いほど多く、「2～4人」の企業では17.8%であるのに対し、「10人以上」の企業では57.1%となっている。

⑥ 情報機器に保存した書類のバックアップ

サイバーセキュリティ対策としても、また情報セキュリティ対策としても、情報機器に保存してある書類のバックアップをとっておくことは重要である。バックアップをとっていれば、不正プログラムに暗号化されてしまったとしても、また書類をうっかり削除してしまったとしても、業務への被害を最小にとどめることができる。

アンケートで、情報機器に保存した書類のバックアップをとっているかどうかをみると、「バックアップはとっていない」とする企業の割合は16.0%、「わからない」とする企業の割合は2.7%であり、81.3%の企業はバックアップをとっているとしている（図-14）。

バックアップ方法をみると「USBメモリやCD、DVDにバックアップしてある」が41.3%で最も多

く、次が「外付けのHDDやSSDにバックアップしてある」が38.8%となっている。いずれも一般的なバックアップ方法であるが、パソコンと常時接続しているのであれば、サイバーセキュリティ対策にはならない。あるパソコンが不正プログラムに感染すれば、そのパソコンに接続しているHDDやUSBメモリも感染してしまう可能性が大きいからである。社内ネットワークのサーバーにバックアップしている場合も同様である。

一方、クラウドサーバーやストレージサービスなど、社外のサーバーにバックアップを保存しておけば、社内の情報機器が不正プログラムに感染しても重要な書類が失われることはない。だが、「社外のサーバーにバックアップしてある」とする企業の割合は16.4%にすぎない。

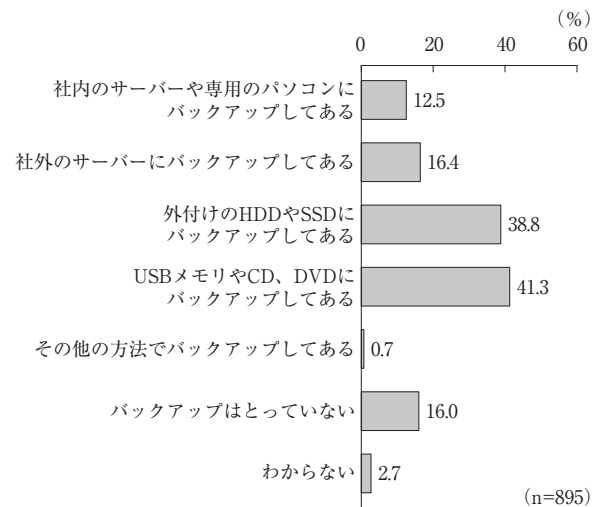
また、バックアップは複数箇所に作成しておくよりも安全であるが、これを実行している企業の割合は、バックアップを作成していると回答した企業のうち27.3%にとどまっている。

⑦ セミナーや研修の経験

サイバーセキュリティ対策または情報セキュリティ対策に関するセミナーや研修は多くの企業や団体が実施している。インターネットを使って学ぶeラーニングという方法もあり、中小企業がサイバーセキュリティについて学ぶ機会はいくらでもある。

しかし、アンケートで情報セキュリティに関するセミナーや研修に参加したり、eラーニングを受講したりしたことがある企業の割合をみると、経営者については11.6%、従業員については一部でも参加したことがある企業を含めても15.9%となっている。ただし、これらの割合も情報機器を多く利用している企業ほど多くなっており、パソコンを「10台以上」使用している企業の場合、経営者については31.4%、従業員については54.3%となっている。

図-14 情報機器に保存した書類のバックアップ（複数回答）



（４）インシデントの発生状況

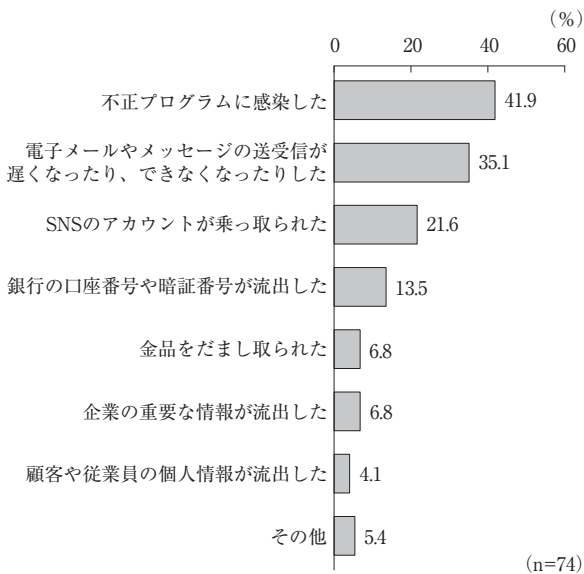
① 不審メール・メッセージによる被害

アンケートで、不正プログラム付きのメールや取引先をかたるメール、個人情報の詐取を目的とするメッセージなど、不審なメールやメッセージを受信する頻度をみると、「届いたことはない」とする企業の割合が16.3%、「わからない」とする企業の割合が6.4%あるものの、「毎日何通か届く」とする企業の割合が25.8%、「週に何通か届く」とする企業の割合が19.3%となっており、頻繁に受信している企業が少なくない。

不審なメールやメッセージを受信したことがある企業のうち、具体的な被害があったとする企業の割合は12.6%（アンケート回答企業全体の7.2%）となっている。被害の内容（複数回答）をみると、「不正プログラムに感染した」が41.9%で最も多く、「電子メールやメッセージの送受信が遅くなったり、できなくなったりした」の35.1%、「SNSのアカウントが乗っ取られた」の21.6%が続いている（図-15）。

該当する企業の数が多くないので断定はできないが、不審なメールやメッセージによる被害はセ

図-15 不審メール・メッセージによる被害
(複数回答)



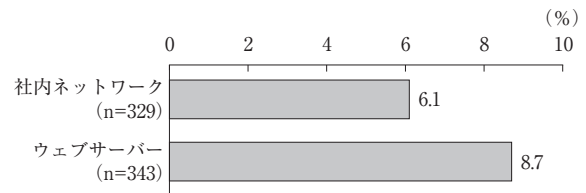
セキュリティ対策をしていない企業で特に多いというわけではない。例えば、すべてのパソコンにセキュリティソフトをインストールしている企業の場合、不審なメールやメッセージで何らかの被害が生じたことがあるとする企業の割合は11.9%であるが、まったくインストールしていないとする企業でも、この割合は11.3%である。

これはサイバーセキュリティ対策をしてもしなくても同じだということではなく、実際に被害を受けたことで対策をとるようになった企業が少なくないためではないかと考えられる。

② サーバーへの不正アクセス・攻撃

アンケートに回答した企業のうち、社内ネットワークを構築しており、かつ社内ネットワークをインターネットに接続している企業は329社である。これらの企業のうち、社内ネットワークに不正にアクセスされたことがあると回答した企業の割合は6.1%である（図-16）。また、企業のホームページを開設している企業343社のうち、ウェブサーバーへの不正アクセスや攻撃があったとする企業の割合は8.7%となっている。

図-16 不正アクセスの経験がある企業の割合



不正アクセスについても、不審なメールやメッセージによる被害と同様に、不正アクセス対策をしている企業の方が被害に遭ったとする企業の割合が多い。例えば、ウェブサーバーへの不正アクセスや攻撃があったとする企業の割合は、不正アクセス対策をとっていない企業では11.8%であるのに対し、不正アクセス対策をとっている企業では20.8%となっている。

(5) サイバーセキュリティ対策に関する

自己評価と対策を進めるうえでの問題

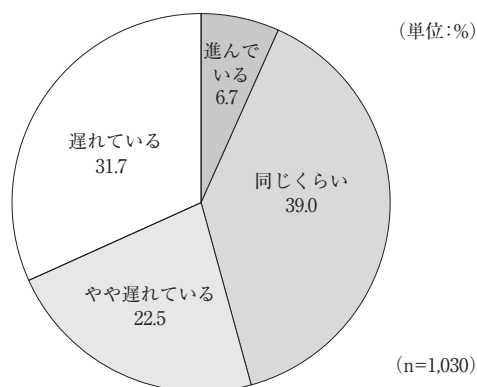
① サイバーセキュリティ対策に関する自己評価

アンケートで、同業の中小企業に比べて自社の情報セキュリティ対策の現状をどう思うかについてみると、回答企業全体では「遅れている」とする企業の割合が31.7%を、「やや遅れている」とする企業の割合が22.5%をそれぞれ占め、「進んでいる（「やや進んでいる」を含む）」とする企業の割合は6.7%にとどまっている（図-17）。

「遅れている」または「やや遅れている」と回答した企業の割合は、サイバーセキュリティ対策に問題のある企業で多くなっている。例えば、「遅れている」と回答した企業の割合は、パソコンのOSを「すべてアップデートしてある」と回答した企業では26.4%であるが、「すべてアップデートしていない」と回答した企業では45.5%となっている。サイバーセキュリティ対策が不十分である企業は、自社の情報セキュリティ対策が遅れているという自覚はあると思われる。

自社の情報セキュリティ対策の現状に対する評

図-17 同業の中小企業に比べた自社の情報セキュリティ対策の現状



(注)「進んでいる」には「やや進んでいる」と回答した企業の割合(4.7%)を含む。

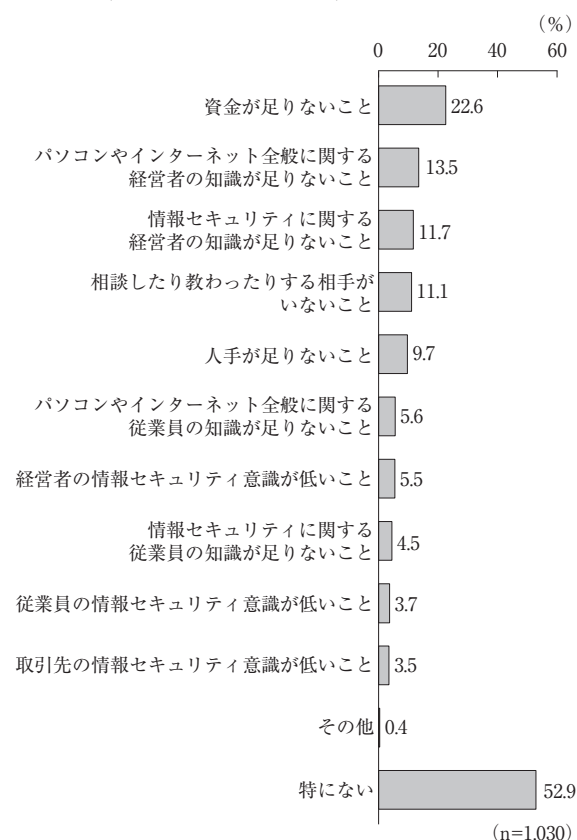
価値は、仕事で使用している情報機器の数が、多いほど高く、少ないほど低い傾向がみられる。例えば、「進んでいる」と評価した企業の割合は、使用しているパソコンの数が「1台」の企業では3.7%であるが、「5～9台」の企業では11.1%、「10台以上」の企業では25.7%となっている。逆に、「遅れている」とする企業の割合は、使用しているパソコンの数が「1台」の企業では34.4%を占めるが、「5～9台」の企業では22.2%、「10台以上」の企業では11.4%となっている。

② 情報セキュリティ対策を行ううえでの障害

アンケートで、情報セキュリティ対策を進めるうえで障害になっているものをみると(三つまでの複数回答)、「資金が足りないこと」を挙げた企業の割合が22.6%で最も多く、以下「パソコンやインターネット全般に関する経営者の知識が足りないこと」の13.5%、「情報セキュリティに関する経営者の知識が足りないこと」の11.7%と続いている(図-18)。

情報セキュリティ対策には、資金も人手も知識も必要であり、資源に制約がある中小企業でその不足が障害になることは当然といえる。だが、そ

図-18 情報セキュリティ対策を進めるうえでの障害(三つまでの複数回答)



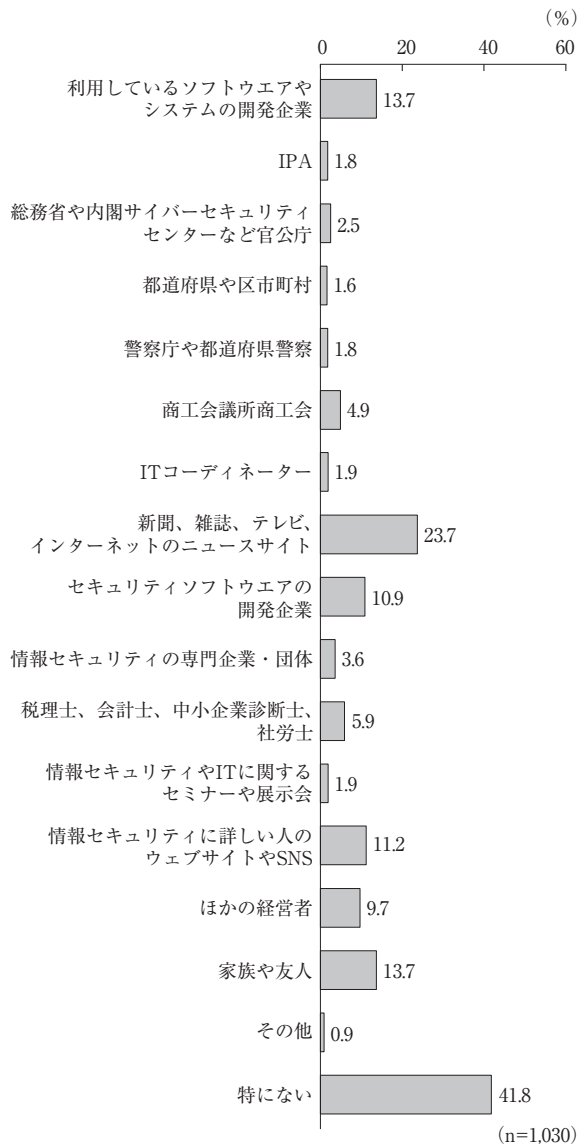
(注) 従業員に関する選択肢もn値を1,030として算出。

これらの不足が解消されれば中小企業全体の情報セキュリティ対策が進むかは疑問である。なぜなら情報セキュリティ対策を進めるうえでの障害が「特になし」と回答した企業の割合が52.9%と過半を占めているからである。

障害が「特になし」と回答した企業の割合は、自社の情報セキュリティ対策が「進んでいる」と回答した企業では36.2%であるのに対し、「やや遅れている」と回答した企業では44.4%、「遅れている」と回答した企業では49.8%、「同じくらい」と回答した企業では63.2%となっている。

つまり、特別な障害があるわけではないのに情報セキュリティ対策に適切に取り組んでいない企業が多くを占めているのである。これは、情報セキュリティ対策が遅れていても、大した問題ではないと考えている中小企業、あるいは優先して取

図-19 情報セキュリティ対策に必要な情報の入手先
(三つまでの複数回答)



り組むべき課題ではないと考えている中小企業が多いことを示していると考えられる。

こうした情報セキュリティ対策に関する問題意識の低さは、必要な情報の入手先からもうかがえる。アンケートで、必要な情報の入手先として最も回答割合が多かったのは「新聞、雑誌、テレビ、インターネットのニュースサイト」の23.7%である（図-19）。これらのメディアでも、情報セキュリティやサイバー攻撃に関する記事や番組が掲載・放送されることもあるが、多くは実際に起き

た事件や事故の報道である。一方的に情報が発信されるだけで、その頻度も低く、情報の入手先としては心もとない。

一方、サイバー攻撃や情報セキュリティ対策について、ホームページで詳細に解説し、警告もしているIPAや警察庁、内閣サイバーセキュリティセンターを情報の入手先として挙げた企業の割合は、いずれも2%にすぎない。

しかし、より注目すべきは、情報の入手先が「特になし」と回答した企業が41.8%を占めることである。「情報セキュリティ」や「サイバー攻撃」といったキーワードでインターネットを検索すれば、必要な情報はすぐに見つかる。情報の入手先が「特になし」というのは積極的に情報を入手しようとしていないからにすぎない。IPAや警察庁、内閣サイバーセキュリティセンターを情報の入手先として挙げた企業が少ないのも、中小企業自身が情報を求めようとしていないからではないか。

情報セキュリティに関する情報の入手先が「特になし」と回答した企業の割合は、自社の情報セキュリティに関する評価が低い企業で多くなっている。具体的には、「進んでいる」と回答した企業では13.0%であるが、「同じくらい」と回答した企業では39.1%、「やや遅れている」と回答した企業では34.9%、「遅れている」と回答した企業では56.3%となっている。自社の情報セキュリティ対策が「遅れている」と認識しているにもかかわらず、積極的に情報を入手しようとしなのは、情報セキュリティ対策に関する問題意識が低いからと考えるのが妥当だろう。

もっとも、情報セキュリティ対策に関する問題意識が低いからといって中小企業を責めることはできない。中小企業はさまざまな問題に直面しており、必ずしも売り上げや利益につながらないサイバーセキュリティ対策や情報セキュリティ対策に割ける時間や手間は限られる。

また、情報セキュリティ対策やサイバーセキュ

リティ対策は、覚えるべきことや実行すべきことが広範にわたるうえに、専門用語が多い。情報機器を使ってはいるが、メールやメッセージをやりとりしたり、定型的な文書を作成したりする程度という、情報化が進んでいるとはいえない企業にとって、情報セキュリティ対策やサイバーセキュリティ対策はハードルが高い。

あまり情報化が進んでいない中小企業は、自社がサイバー攻撃の対象になるとは想定していないことも考えられる。実際、個人情報や重要な文書を情報機器に保存していなければ、ランサムウェアを警戒する必要はないし、不正プログラムに感染したとしても顧客や取引先に迷惑をかける可能性は小さい。

ただ、サイバー攻撃には「サプライチェーンの弱点を悪用した攻撃」もある。中小企業が直接、攻撃の対象になることはなくても、取引先を攻撃する手がかりを与えてしまう可能性はある。また、使用している情報機器が遠隔操作され、犯罪などに利用されれば、容疑者と誤解され、逮捕されるおそれもある。オフィスや工場と同様に、情報機器にも防犯対策は欠かせないのである。

5 インプリケーション

今回のアンケート結果から、中小企業ではサイバーセキュリティへの問題意識が乏しく、対策が充実していない企業が多いことがわかった。どうすれば、中小企業でサイバーセキュリティ対策が進むのか、最後に考えてみたい。

(1) 環境整備

中小企業のサイバーセキュリティ対策は、総じて遅れているのだが、同じ遅れている企業であってもサイバーセキュリティ対策に関心のある企業もあれば、これといった理由もないのに消極的な企業もある。前者のサイバーセキュリティ対策を

強化する方策は明確であり、中小企業を支援する環境を整備すればよい。

すでに実施されているものも多いが、①相談窓口を設けたり、専門家を派遣したり、研修やセミナーを開催したりして、中小企業における人材や知識の不足を補う、②安価で使いやすいセキュリティソフトやセキュリティ機器を開発する、③対策にかかる費用を助成する、といったことが考えられる。

ただし、こうした施策がばらばらに実施されていると、中小企業は必要な情報を見つけにくい。総合的なサービスやワンストップで相談できる窓口があると便利である。

例えば、大阪商工会議所は2020年2月から「サイバーセキュリティお助け隊」という有料のサービスを開始し、UTM機器の貸与や遠隔操作によるソフトウェアのアップデートからインシデントが発生した場合の対応まで、必要なサイバーセキュリティ対策をパッケージにして提供している。また、東京商工会議所では2021年7月に「東商サイバーセキュリティコンソーシアム」を設立し、人材の育成、コンサルティング、脆弱性の診断や標的型攻撃の訓練、セキュリティソフトやUTM機器の導入など、サイバーセキュリティ対策に必要な相談を総合的に提供できるようにした。

一方、サイバーセキュリティ対策にかかる費用を助成する制度は少ない。中小企業の情報化を支援する国の助成金としては、最大450万円の「IT導入補助金」があるが、これは業務の効率化や生産性の向上を主目的とするものであり、サイバーセキュリティ対策だけでは利用できない。

自治体の制度としては、東京都に最大1,500万円の「サイバーセキュリティ対策促進助成金」がある。機器やソフトウェアだけではなく、標的型攻撃に備えた訓練費用も対象になる。サイバーセキュリティ対策の費用そのものではないが、ISMSやプライバシーマークの取得費用

を助成する自治体もいくつかある。民間による支援制度もほとんどないが、広島銀行には最大5億円まで融資する「サイバーセキュリティ対策支援ローン」があり、サイバー保険⁵もセットになっている。

中小企業政策では、これまでサイバーセキュリティ対策よりも情報化を進めることが優先されてきた。だが、サイバー攻撃が日常化している今日、情報化投資とサイバーセキュリティ対策は一体的に行わなければならない。費用の助成も情報化とサイバーセキュリティ対策をセットにして行うことが望ましい。

（2）消極的な企業の動機づけ

サイバーセキュリティ対策に消極的な企業に対する施策はなかなか難しい。サイバー攻撃に遭った中小企業の例を紹介するなどして、危機感をもたせるのも一つの手だが、被害の大きさばかりを強調すると、中小企業を委縮させてしまい、サイバーセキュリティ対策を進めさせるところか、情報化そのものを後退させることになりかねない。

アンケート結果からは、情報機器を多く利用している企業ほどサイバーセキュリティ対策に取り組んでいる傾向がみられた。情報化が進むほど、企業がサイバーセキュリティ対策の必要性を実感するからだと思われる。

従って、中小企業の情報化を促進することが中小企業にサイバーセキュリティ対策を促すことにもなると考えられる。自治体や中小企業支援機関には、今まで以上に中小企業の情報化を支援することが求められる。各ベンダーには、中小企業が情報化を進めやすいよう、より操作しやすい機器、より便利なソフトウェアやアプリを開発すること

が期待される。

ただ、情報化の必要性は企業ごとに異なる。情報化したからといって、必ず具体的な成果があるわけでもない。環境を整えたところで、情報化にもサイバーセキュリティ対策にも消極的な企業は一定数残るだろう。

そこで考えられるのが、さまざまな取引においてサイバーセキュリティ対策が充実している企業と充実していない企業とで区別することだ。すでに、国や自治体では、個人情報を扱う事業の委託先を入札で決める場合、プライバシーマークを取得していることを入札条件にすることは当たり前になっている。

民間企業同士の取引でも、例えば業務の委託先で個人情報の漏洩が発生した場合に責任を負うのは発注した企業であるから、サイバーセキュリティ対策の甘い企業は不利になる。さらに、「サプライチェーンの弱点を利用した攻撃」が大きな脅威となっていることを考えると、今後は直接の発注先だけではなく、再委託先や二次、三次の下請け企業のサイバーセキュリティ対策も問われるようになり、対策の甘い企業はどのサプライチェーンからも排除されることになるだろう。

金融機関の融資でも、企業のサイバーセキュリティ対策は重要な審査項目になっていくだろう。中小企業でも、ランサムウェアの被害に遭って身代金を支払ったり、個人情報の漏洩で賠償金を負担したりする例がみられる。被害の程度によっては融資金の返済が遅れ、最悪の場合、回収が困難になることもあり得る。また、セキュリティの甘い融資先を通じて、金融機関自身がサイバー攻撃に遭う可能性もある。金融機関はサイバー攻撃を融資先が抱えるリスクとして考慮せざるを得なく

⁵ サイバー攻撃によって生じた損害を補償する。補償の対象は、個人情報等の漏洩事故による損害の賠償、不正プログラム付きのメールを送信したことにより取引先で発生した損害の賠償、情報機器が使用できなくなったことによって生じた逸失利益、データの復旧費用など幅広いが、ランサムウェアや詐欺に遭って支払った金銭は補償されない。なお、サイバー攻撃全般ではなく、個人情報の漏洩事故にかかわる損害賠償金や費用だけを補償する個人情報漏洩保険もある。

なっているのだ。サイバーセキュリティ対策の程度に応じて、金融機関が金利や融資期間など融資条件を変えるのは合理的な判断といえる。

金融機関がサイバーセキュリティ対策は企業の評価にかかわることを融資先にアピールすれば、サイバーセキュリティ対策に取り組む中小企業は増えていくだろうと思われる。関心をもった中小企業を融資やコンサルティングなどで支援すれば、金融機関にとってはビジネスチャンスにもなる。

こうして、サイバーセキュリティ対策をしないと損をする、あるいはサイバーセキュリティ対策をしっかりとっておけば有利になるという状況が出来上がれば、情報化に熱心ではない中小企業もサイバーセキュリティ対策に関心をもつようになるのではないか。

(3) スモールスタート

サイバー犯罪が、現実世界の犯罪と異なるのは、被害が広い範囲に及ぶことである。現実世界であれば、自宅に鍵をかけなかったとしても、空き巣に入られるのは自分の家だけで済む。だが、サイバー空間では、セキュリティの甘い情報機器は、インターネットでつながっている、すべての情報機器への扉になる。

これまで述べてきたように、不正プログラムに感染した情報機器が遠隔操作され、ほかの情報機器への不正アクセスに使われたり、メールや文書が盗まれて標的型攻撃の材料にされたりと、侵入された企業ではなく、ほかの企業に損害を与えて

しまうこともある。取引先や顧客のメールアドレスが漏れて、フィッシングメールの新たな送付先になることもある。サイバーセキュリティ対策に消極的な企業は、犯罪者に機会や道具を与えていることになる。いまやサイバーセキュリティ対策は社会経済に不可欠なものであり、中小企業といえども後回しにしてよいものではない。

もちろん、中小企業にとってサイバーセキュリティ対策を厳密に実施することは簡単ではない。専門知識をもった人材が必要であるし、費用もかかる。全社員が対策を理解し、実行できるようにしなければならない。

こうした中小企業の事情を踏まえ、IPAの「中小企業の情報セキュリティ対策ガイドライン」は、中小企業がサイバーセキュリティ対策に取り組む場合、最初からすべてを実行しようとするのではなく、「情報セキュリティ 5 か条」から始めればよいとする。すなわち、①OSやソフトウェアのアップデート、②ウイルス対策ソフトのインストール、③パスワードの強化、④共有設定の見直し、⑤脅威や攻撃の手口を知るの五つである。

最初は、5項目のうち一つでもよい。サイバーセキュリティ対策は習慣づけることが最も重要であり、そのためには、まずできることから始め、次第に対策を増やしていく「スモールスタート」が有効である。情報機器やインターネットを利用する限り、どの企業でもサイバー攻撃の対象になる可能性がある。中小企業には、ぜひサイバーセキュリティ対策に関心をもってもらい、少しでも対策を強化してもらいたい。