ISSN 1883-5937

日本公庫総研レポート　No.2022-1
2022年1月

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

日本政策金融公庫　総合研究所

はしがき

いまや、われわれの暮らしに情報通信技術は欠かせない。総務省の『令和3年版情報通信白書』によれば、2020年におけるスマートフォンの世帯保有率は90％に迫り、インターネットの利用率は80％を超える。情報通信技術の発達は企業活動にも影響している。情報通信技術は、企業の業務を効率化するだけではなく、事業機会を増やし、起業や新規事業の開発を促進している。情報機器とインターネットなしには、事業を続けられないという企業も少なくない。2020年以降は、新型コロナウイルス感染症の影響で世界的にテレワークやインターネットショッピングの利用が増え、情報通信技術は一段と普及したとみられる。

一方、情報通信技術の発達と普及は、大量の個人情報を盗み出したり、預金を不正に引き出したりといったサイバー犯罪も増加させてしまった。コンピューターウイルスに感染して工場が操業停止に追い込まれたり、企業のホームページが書き換えられて個人情報が流出してしまったりといった例は枚挙にいとまがない。企業であっても個人であっても、情報機器やインターネットを利用するならサイバーセキュリティ対策が不可欠である。

中小企業も例外ではない。そこで、当研究所では、情報機器を利用している中小企業を対象にインターネットアンケートを実施し、中小企業におけるサイバーセキュリティ対策の現状を調査した。本レポートはその結果をまとめたものである。

本レポートの構成は、次のとおりである。第1章では、サイバー攻撃の種類や動向と、サイバーセキュリティ対策の基本について解説した。第2章は、アンケート結果を整理したものである。アンケートでは、自社のサイバーセキュリティ対策が遅れていると判断している中小企業が多いこと、遅れている理由が必ずしも明確ではなく、サイバーセキュリティ対策に消極的な企業が多いことが明らかになった。第3章は、アンケートの結果を踏まえ、どうすれば中小企業のサイバーセキュリティ対策が進むのかについて考察した。

最後になったが、多忙にもかかわらず、アンケートに回答していただいた中小企業経営者の皆さまには、この場を借りてお礼申し上げる。

（日本政策金融公庫総合研究所　竹内 英二）

目　次

第1章　高まるサイバーセキュリティの重要性 …… 1
　1　増加するサイバー攻撃 …… 1
　　(1) デジタル化とサイバーセキュリティ …… 1
　　(2) 脅威・攻撃の例 …… 1
　　(3) データでみるサイバー攻撃 …… 3
　2　基本は脆弱性対策と手口の学習 …… 4
　　(1) 脆弱性 …… 4
　　(2) 心の隙 …… 5
第2章　中小企業におけるサイバーセキュリティの現状 …… 7
　1　アンケートの要領と回答企業の属性 …… 7
　　(1) 調査要領 …… 7
　　(2) アンケート回答企業の属性 …… 7
　2　デジタル化の現状 …… 8
　　(1) コミュニケーション …… 8
　　(2) テレワーク …… 9
　　(3) ホームページの運営 …… 10
　　(4) 社内ネットワーク …… 10
　　(5) 文書の保存 …… 11
　3　サイバーセキュリティ対策の実施状況 …… 11
　　(1) ソフトウエアのアップデート …… 11
　　(2) ソフトウエアや機器を使った対策 …… 12
　　(3) オンライン会議・テレワークに関する対策 …… 13
　　(4) 情報機器に保存した書類のバックアップ …… 14
　　(5) 情報セキュリティ体制 …… 15
　4　インシデントの発生状況 …… 17
　　(1) 不審メール・メッセージによる被害 …… 17
　　(2) 不正アクセス・攻撃 …… 18
　5　情報セキュリティ体制と取引への影響 …… 18
　6　サイバー保険への加入 …… 19
　7　中小企業における問題の所在 …… 20
　　(1) 自社への評価 …… 20
　　(2) 情報セキュリティ対策を行ううえでの障害 …… 20
第3章　まとめ―政策的含意― …… 23
　1　環境整備 …… 23
　2　消極的な企業の動機づけ …… 24
　3　スモールスタート …… 25

第1章　高まるサイバーセキュリティの重要性

1　増加するサイバー攻撃

(1) デジタル化とサイバーセキュリティ

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）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。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（ろうえい）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（かいざん）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。

(2) 脅威・攻撃の例

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（消費者）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企業への攻撃に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。

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	ランサムウエアによる被害	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（ひぼう）・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（ろうえい）	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（ぜいじゃく）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

資料：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）

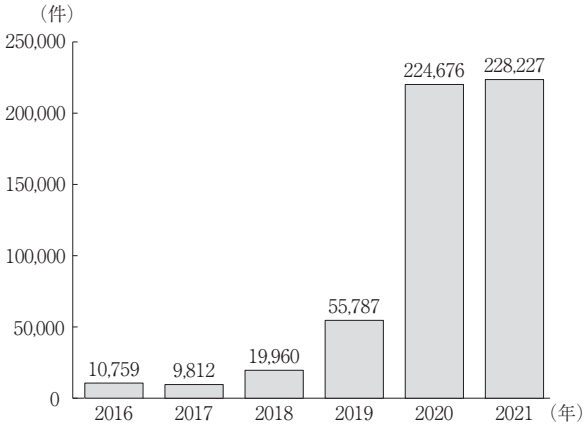
「ランサムウエア」は、不正プログラム（コンピューターウイルスやスパイウエアなど悪意のあるプログラムの総称。マルウエアともいう）の一種で、侵入したパソコンの内部にあるファイルを暗号化したりパソコンをロックしたりしてデータを「人質」にとり、データの復旧と引き換えに身代金（ランサム）を要求するものである。近年は、身代金を支払ったかどうかにかかわらず、人質にしたデータを暴露するものもみられる。

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に対するものである。狙う企業の情報を収集・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なるような内容を書いたメールを送りつける。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。

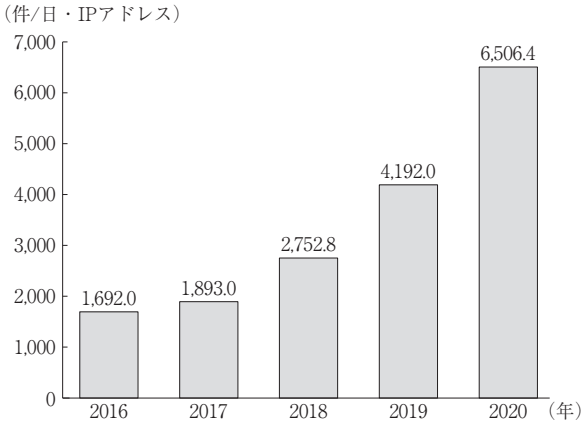
「フィッシング」は、実在する企業や役所をかたってメールやSMS（携帯電話やスマートフォンのショート・メッセージ・サービス）を送信し、偽のホームページに誘導して、クレジットカードや預金口座の番号、IDやパスワードといった情報を入力させる詐欺である。被害に遭うと、情報が盗まれるだけではなく、不正送金に使われるなど金銭の被害が発生することも少なくない。フィッシングメールは不特定多数に送信されるものであり、消費者に限らず、企業や企業の従業員が被害に遭う可能性も十分にある。

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。

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：警察庁広報資料「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）

なお、フィッシングメールは大手のECモールや金融機関、宅配業者など、有名企業をかたるものが大半であるが、なかには中小企業を装う例もある。実際、筆者は楽天市場に出店している実在の中小企業をかたったフィッシングメールを受け取ったことがある。

(3) 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[1]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。

同協議会によれば、報告件数が増加している要因として、インターネットショッピングの需要が増え、その利用者を狙ったフィッシングが増えていることや、攻撃側の設備が整ってきていることが考えられるという。

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（ぜいじゃく）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。

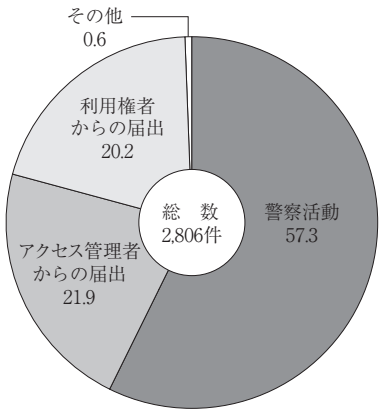
なお、警察庁はサイバー攻撃やその準備行為が急増している要因として、ウェブカメラや無線LANのルーターなどIoT機器[2]やリモート・デスクトップ・サービスを狙った攻撃が増えていることを指摘している。どちらも、コロナ禍で増加したとされるテレワークやリモートワークで利用が増えた機器やサービスである。

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

[1] 一般社団法人JPCERTコーディネーションセンターが運営する団体。2005年4月の発足。フィッシングに関する情報収集や対応策の検討などを行っている。
[2] 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。

図－3　端緒別不正アクセス行為の認知件数

（単位：%）



資料：警察庁、総務省、経済産業省「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）

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。

不正アクセスの認知件数は、日本全体の企業数に比べればわずかなものに思えるかもしれない。だが、具体的な被害がなかったり、被害に気づかなかったりするだけで、実際にはもっと多くの企業が不正アクセスを受けていると考えられる。

例えば、不正アクセス行為が認知された端緒をみると「警察活動」が57.3%を、「利用権者からの届出」が20.2%をそれぞれ占めるのに対し、「アクセス管理者からの届出」は21.9%にとどまっている（図－3）。つまり、不正アクセスは企業が自ら気づくよりも、警察の捜査や企業が提供しているサービスのユーザーからの申し立てがあって判明する方がずっと多い。企業が不正アクセスを受けたことがないと思っていても、実は気づいていないだけなのかもしれないのである。

また、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[3]やEDRソフト[4]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。このことからもサイバー攻撃に気づいていないだけで、実際には攻撃を受けたり脅威にさらされたりしている企業が少なくないことがわかる。

2　基本は脆弱性対策と手口の学習

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

脆弱性は、多くのソフトウエ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エアであるが、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、グーグルの「クローム」やアップルの「サファリ」、マイクロソフトの「エッジ」など、インターネットを閲覧するためのブラウザーがあれば

[3] UTMはUnified Threat Management（統合脅威管理）の略。ファイアウオールやアンチウイルスなど複数のセキュリティ機能をもち、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。

[4] 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エ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）をとるソフトウエア。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。

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エア製品については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[5]。

ソフトウエアの脆弱性は、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、ソフトウエ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、ソフトウエ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をついてくるサイバー攻撃もあり、これを完全に防御することは難しいが、それでもソフトウエ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エアだけではなく、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エア（ファームウエア）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エ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機器もファームウエアを更新し、最新の状態にしておく必要がある。

なお、脆弱性が発見されても開発者が不明だったり、連絡がつかなかったりして、セキュリティパッチが配布されなかったり、配布されるまでに時間がかかったりすることもある。IPAは一般社団法人JPCERTコーディネーションセンターと共同で脆弱性に関するデータベース「JVN iPedia」[6]を運営している。このデータベースには日本製品だけではなく、海外製品についても脆弱性と対策の状況が掲載されている。

自社が利用しているソフトウエアやIoT機器に関する脆弱性の有無や対策の状況が開発者のホームページをみてもわからない場合には、このデータベースで確認し、もし対策がとられていないのであれば、そのソフトウエアや機器の利用を中止することも必要である。

(2) 心の隙

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。

---

[5] 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。

[6] https://jvndb.jvn.jp

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[7]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」[8]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）」[9]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」[10]がある。また、標的型攻撃については訓練サービスがいくつもあり、中小企業でも利用しやすい料金のものも少なくない。

＊　＊　＊

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。ただ、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と思われる。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。対策が不十分だとすれば、どこに問題があるのか。当研究所が実施したアンケートの結果を用い、次章で確認していこう。

[7] https://www.antiphishing.jp/news/database/
[8] https://www.antiphishing.jp/report/consumer_antiphishing_guideline_2021.pdf
[9] https://www.ipa.go.jp/files/000081866.pdf
[10] https://www.ipa.go.jp/files/000043331.pdf

第2章　中小企業におけるサイバーセキュリティの現状

本章では、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、中小企業におけるサイバーセキュリティ対策の現状をみていく。

1　アンケートの要領と回答企業の属性

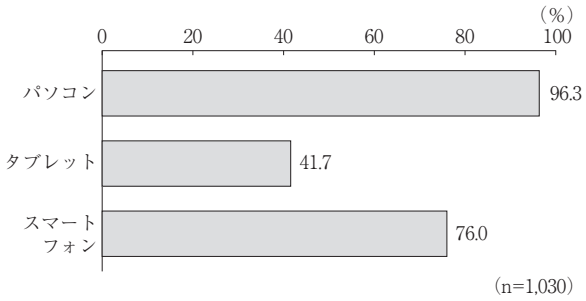
(1) 調査要領

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。

調査の対象をパソコンやタブレット、スマートフォンを利用している企業に限ったのは、これらの機器を利用していなければ、サイバーセキュリティ対策はほぼ必要ないからである。もちろん、インターネットに接続したゲーム機や家電もサイバー攻撃の対象になるが、これらを仕事で利用している企業は少ないと考えられる。また、携帯電話（いわゆるガラケー）は利用者が大きく減少している。

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した。

図－4　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は回答者数（以下同じ）。

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。

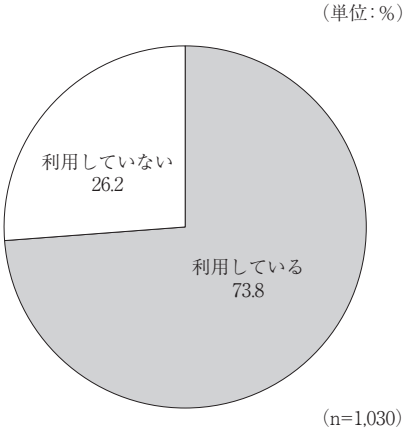
(2) アンケート回答企業の属性

アンケートに回答した企業の形態は、個人事業主が78.3%、会社が21.7%となっている。従業者規模の構成比をみると、「1人」が58.3%、「2～4人」が25.8%、「5～9人」が7.7%、「10人以上」が8.3%となっている。

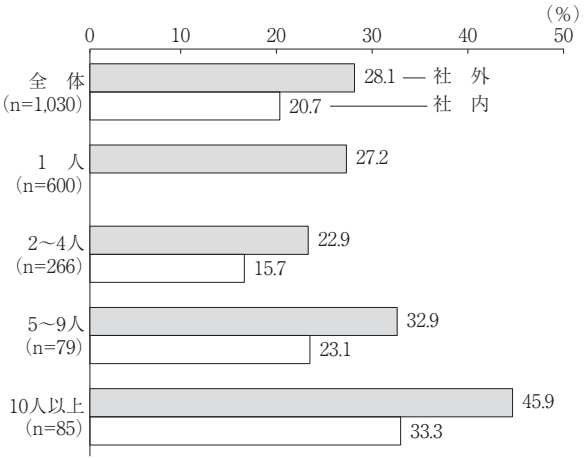
回答企業の業種構成比をみると、「専門技術サービス、学術研究」が20.4%で最も多く、以下「小売業」の12.5%、「建設業」の10.3%と続く。ほかの業種は、いずれも10%に満たず、比較的分散している。

最後に各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－4）。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。

図－5　社外の人とのコミュニケーションにメールやメッセージアプリを利用しているか



図－6　オンライン会議用ソフトウエアを利用している企業の割合（従業者規模別）



（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エアの利用について「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エアを利用している企業の従業者規模ごとの割合も、「従業員はいない」と回答した企業を除いて算出した。

2　デジタル化の現状

サイバーセキュリティ対策の状況をみる前に、まず中小企業における業務のデジタル化の現状をみておこう。

(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－5）。

メールやメッセージアプリを利用している企業の割合は、「小売業」で55.8%、「飲食サービス」で54.5%、「医療、福祉」で55.6%と少ない。これらは消費者を対象とするビジネスであるが、消費者とのコミュニケーションは、電話や対面で行うことが多いのだろう。

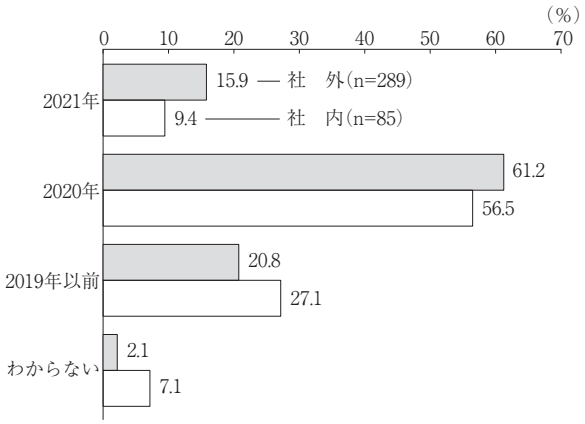
高速の通信回線が普及したことや無料または安価なサービスが提供されていることもあり、近年はオンライン会議（ウェブ会議）が容易に実施できるようになっている。そのため、企業の内外を問わず、コミュニケーションの手段としてオンライン会議を利用する企業が増えている。

アンケートで、オンライン会議用ソフトウエ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－6）。

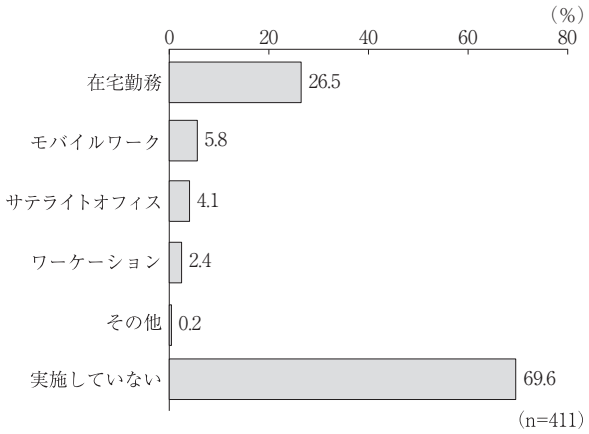
図に示したとおり、オンライン会議用ソフトウエアを利用している企業の割合は、おおむね従業者数が多いほど多くなる。また、業種別に利用企業の割合をみると、社外については「情報通信業」が51.1%、「専門技術サービス、学術研究」が41.4%と多く、「小売業」は14.0%と少ない。社内についても、「情報通信業」が41.9%、「専門技術サービス、学術研究」が32.2%と多く、「小売業」は11.6%と少ない。

オンライン会議用のソフトウエアを利用し始めた時期をみると、社外は「2021年」が15.9%、

図－7　オンライン会議用ソフトウエアを利用し始めた時期



図－8　実施しているテレワークの種類（複数回答）



「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－7）。

ただし、オンライン会議の頻度は高くない。社内のオンライン会議では「週に5日以上」と回答した企業の割合が21.2%あるものの、「週に1日もない」と回答した企業が21.2%を、「週に1日」と回答した企業が20.0%を、それぞれ占めている。また、社外とのオンライン会議では「週に5日以上」と回答した企業の割合は5.9%にとどまり、「週に1日もない」と回答した企業が54.0%を、「週に1日」と回答した企業が20.1%を、それぞれ占めている。

(2) テレワーク

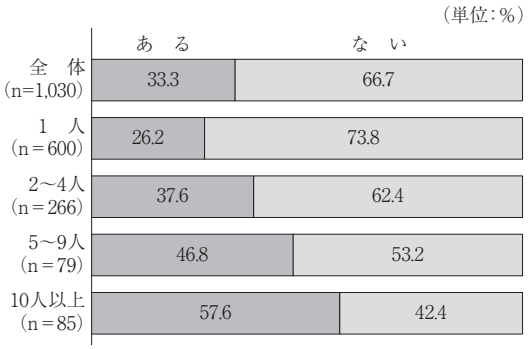
日本では、通勤ラッシュの緩和、ワーク・ライフ・バランスの実現、人材の確保などいくつかの目的から、雇用者の働き方としてテレワークが推奨されてきた。一般社団法人日本テレワーク協会によると、テレワークとは「ICTを活用した、場所や時間にとらわれない柔軟な働き方のこと」であり、業務のデジタル化が進むほどテレワークも導入しやすくなる。

従業員がいる企業について、テレワークを実施している企業の割合をみると、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－8）。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。

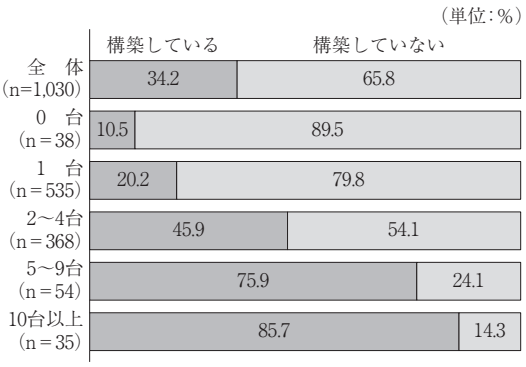
テレワークのうち、「在宅勤務」を導入した時期をみると、「2019年以前」に「在宅勤務」を導入した企業の割合が38.5%を占めているものの、「2020年」が53.2%、「2021年」が8.3%となっており、オンライン会議と同様に、新型コロナウイルス感染症対策として「在宅勤務」を導入した企業が多いことがわかる。

なお、在宅勤務時に従業員が使用する情報機器が誰のものかをみると、企業が従業員に貸与しているケースが37.6%、従業員の私物を利用しているケースが29.6%、両者を併用しているケースが20.0%となっている。従業員の私物を利用しているとする企業の割合は、従業者数が「10人以上」の企業では8.7%であるが、同「2～4人」の企業では43.8%に上る。小規模な企業では、資金制約

図－9　企業ホームページの有無



図－10　社内ネットワークの構築（使用しているパソコンの数別）



が大きく、従業員の私物を利用せざるを得ないと考えられる。

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%と多く、「情報通信業」は18.2%と少ない。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を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と、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－9）。ホームページがあると回答した企業の割合は、従業者規模が大きいほど多くなっており、「1人」の企業では26.2%であるが、「10人以上」では57.6%となっている。

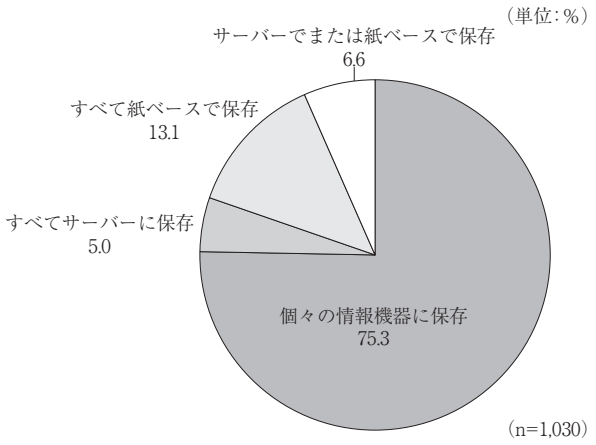
ホームページを運営するには、ウェブサーバーが必要である。ウェブサーバーは自社で設置することもできるし、ホスティング会社から借りることもできる。アンケートでは、レンタルサーバーなど外部のサーバーを借りている企業の割合が68.2%、「社内にある」とする企業の割合が28.6%、「社内にも社外にもある」とする企業の割合が3.2%となっている。

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。

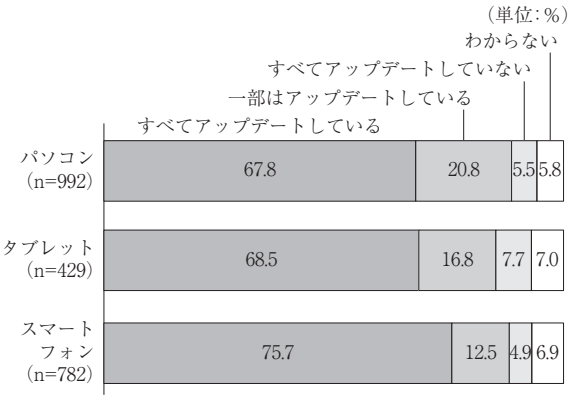
(4) 社内ネットワーク

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－10）。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

図－11　文書の保存方法



図－12　OSのアップデート状況



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。スマートフォンやタブレット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%、「サーバーで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（図－11）。

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。

ちなみに、個々の情報機器に保存している書類の種類をみると（複数回答）、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

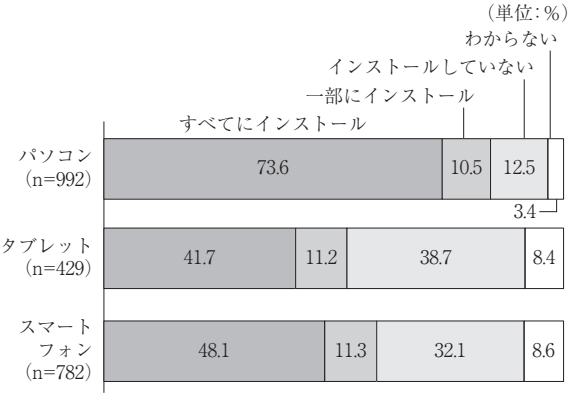
本節では、中小企業におけるサイバーセキュリティ対策の実施状況をみていく。

(1) ソフトウエアのアップデート

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エ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みると、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いる」とする企業の割合は8割に満たない（図－12）。

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

図－13　セキュリティソフトのインストール



てアップデートしている」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エ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い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以外のソフトウエアやアプリには、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とがある。後者の場合、ソフトウエ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エ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エアやアプリを「すべてアップデートしている」とする企業の割合は74.8%にとどまる。OS以外のソフトウエ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) ソフトウエアや機器を使った対策

サイバー攻撃の多くは、専用のソフトウエアや機器を使用することでほぼ自動的に防ぐことができる。アンケートで導入状況をみていこう。

① セキュリティソフト

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エアの総称である。

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」している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－13）。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。

② 社内ネットワークの不正アクセス対策

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、特に外部からの不正アクセス対策も必要になる[11]。

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オ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－14）。

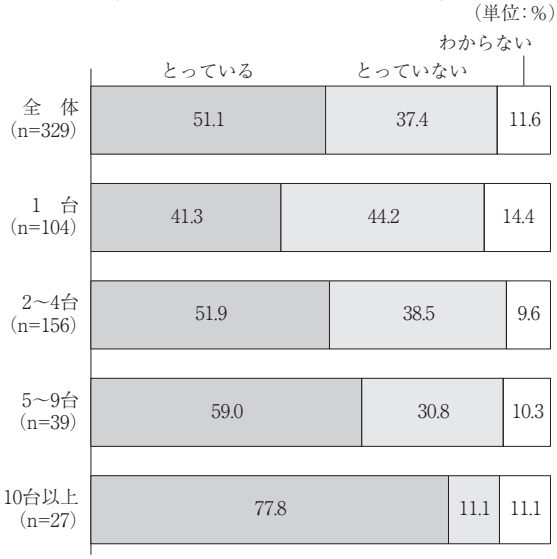
不正アクセス対策を「とっていない」企業の割合は、使用している情報機器の数が少ないほど多くなる傾向があり、特にパソコンについて顕著である。この傾向は、セキュリティソフトのインストールについても認められる。情報機器をあまり使っていない企業ほどサイバーセキュリティへの関心が低いようである。

③ ウェブサーバーの不正アクセス対策

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は343社で、そのうちウェブサーバーを社内に設置している企業は109社と少ないのであるが、ウェブサーバーの不正アクセス対策についてもみておこう。

アンケートによると、ウェブサーバーにファイアウオ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－14　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社しかないので記載を省略した。

(3) オンライン会議・テレワークに関する対策

新型コロナウイルス感染症への対策として、中小企業でもオンライン会議やテレワークを導入する企業が増えている。これらを狙ったサイバー攻撃も増えており、IPAも注意を促している[12]。

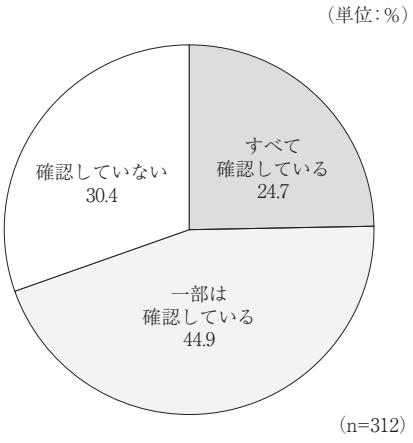
① オンライン会議用ソフトウエアの安全性

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、使用するソフトウエアやアプリ、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

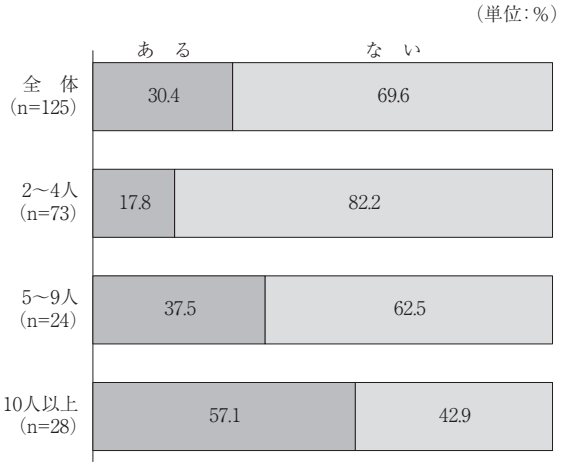
[11] インターネットに接続していなくても、例えばUSBメモリを介して不正プログラムに感染することはあるので、ネットワークのサイバーセキュリティ対策が不要になるわけではない。

[12]「Web会議サービスを使用する際のセキュリティ上の注意事項」（https://www.ipa.go.jp/files/000083955.pdf）、「テレワークを行う際のセキュリティ上の注意事項」（https://www.ipa.go.jp/security/announce/telework.html）

図－15　オンライン会議用ソフトウエアやアプリの安全性



図－16　テレワークに関する規定やルールを定めた文書の有無（従業者規模別）



はどうなっているのか、ソフトウエ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エ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－15）。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ものの、関心のない企業も少なくない。

② テレワークのルール

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[13]。

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－16）。規定やルールを定めた文書があるとする企業の割合は、従業者数が多いほど多く、「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。

なお、テレワークを実施している企業が少ないので断定はできないが、テレワークに関する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がテレワークで使用する情報端末を企業が貸与している企業では47.5%を占めるが、従業員の私物を使用している企業では11.5%、両者を併用している企業では18.2%にとどまっている。

本来、従業員の私物をテレワークで利用する場合にこそ、ルールを明確にすべきなのだが、私物の情報機器を利用している企業には小規模な企業が多く手が回らないのか、ルールを明文化していない企業が多い。

(4) 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

[13] テレワークにおける情報セキュリティ対策については、総務省の「テレワークセキュリティガイドライン（第5版）」に詳しい。（https://www.soumu.go.jp/main_content/000752925.pdf）

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。

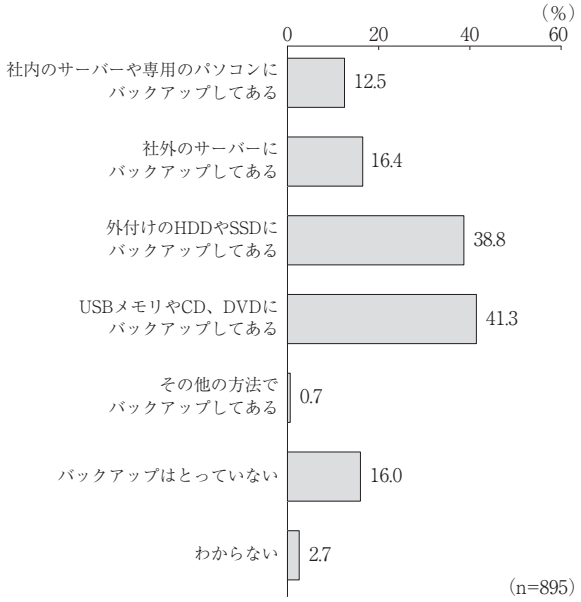
アンケートで、情報機器に保存した書類のバックアップをとっているかどうかをみると、「バックアップはとっていない」とする企業の割合は16.0%、「わからない」とする企業の割合は2.7%であり、81.3%の企業はバックアップをとってあるとしている（図－17）。

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[14]にバックアップしてある」の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とより安全であるが、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。

図－17　情報機器に保存した書類のバックアップ（複数回答）



(5) 情報セキュリティ体制

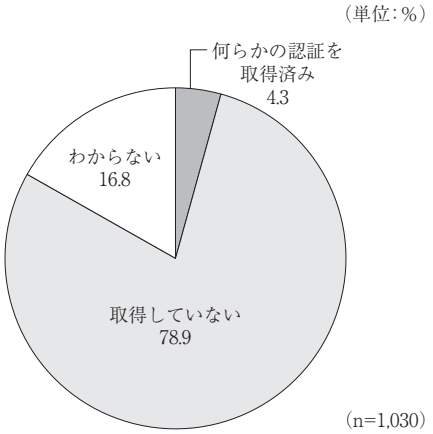
サイバーセキュリティ対策または情報セキュリティ対策は、特定の従業員に依存したり、インシデントが発生してから場当たり的に対応を考えたりするのではなく、責任者を置き、さまざまなことを想定してルールを定め、従業員全員で取り組める体制をつくっていくことが必要である。

アンケートで、まず情報セキュリティに関する責任者についてみると、「置いている」とする企業の割合は4.7%、「経営者が兼ねている」とする企業の割合は40.0%、「特に置いていない」とする企業の割合が55.3%となっている。責任者を置い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おり、例えば使用しているパソコンの数が「1台」の企業では2.2%であるのに対し、「10台以上」使用している企業では37.1%となっている。

次に、情報セキュリティポリシーについてみてみよう。情報セキュリティポリシーとは、企業や官公庁などが「どのような情報資産をどのような脅威から、どのようにして守るのかについての基本的な考え方並びに情報セキュリティを確保する

[14] HDD（ハード・ディスク・ドライブ）もSSD（ソリッド・ステート・ドライブ）も記憶装置。SSDはHDDより高価だが、読み書きの速度が速い、衝撃に強いなどの特徴があり、普及してきている。

図－18　情報セキュリティのマネジメントシステムに関する認証



ための体制、組織及び運用を含めた規定[15]」のことである。

アンケートによれば、この情報セキュリティポリシーを「定めている」企業の割合は12.5％にすぎない。情報セキュリティポリシーを「定めている」企業の割合も、情報機器が多いほど多くなっており、パソコンを例にとれば、使用しているパソコンの数が「1台」の企業では8.6％であるのに対し、「10台以上」の企業では48.6％となっている。不正アクセス対策と同様に、情報機器をあまり利用していない企業では情報セキュリティへの関心も薄いことがうかがえる。

情報セキュリティ体制については、品質管理や環境マネジメントと同様の認証制度がある。認証の取得には費用も時間もかかるが、取得すれば情報セキュリティ体制が整備されていることを取引先や消費者にアピールできる。

主な認証は、国際標準化機構（ISO）と国際電気標準会議（IEC）が共同で策定した国際規格である「ISO/IEC 27001（日本語訳はJIS Q 27001）」に基づくISMS（インフォメーション・セキュリティ・マネジメント・システム）であるが、ほかにクレジットカード業界の「PCI DSS（ペイメント・カード・インダストリー・データ・セキュリティ・スタンダード）」、産業用オートメーションおよび制御システムを対象とする「CSMS（コントロール・システム・セキュリティ・マネジメント・システム）」など、いくつかある。

アンケートによると、情報セキュリティのマネジメントシステムに関する何らかの認証を取得している企業の割合は4.3％である（図－18）。ISMSの場合、認証取得にかかる費用は、認定機関や事業規模にもよるが、審査登録費用だけで50万円から200万円はかかるとされる。コンサルタントを起用すれば費用はさらにかさむし、毎年の更新費用も必要になる。よほど明確なメリットがない限り、中小企業がこうした認証を取得することはないだろうから、4.3％という数字が少ないとは必ずしもいえない[16]。

最後に、サイバーセキュリティや情報セキュリティに関する学習や研修の実施状況についてみておこう。サイバーセキュリティ対策や情報セキュリティに関するセミナーや研修はさまざまな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18.0％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

[15] 内閣サイバーセキュリティセンター情報セキュリティ対策推進会議「情報セキュリティポリシーに関するガイドライン（2000年7月18日）」による。（https://www.kantei.go.jp/jp/it/security/taisaku/guideline.html）

[16] 公益財団法人日本適合性認定協会によると、2020年12月末時点のマネジメントシステムの認証件数は、品質管理が3万9,680件、環境が2万842件、ISMSが6,977件となっている。

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。

4　インシデントの発生状況

本節では、不審メールによる被害や不正アクセスなどサイバーセキュリティに関するインシデントの発生状況についてみていく。

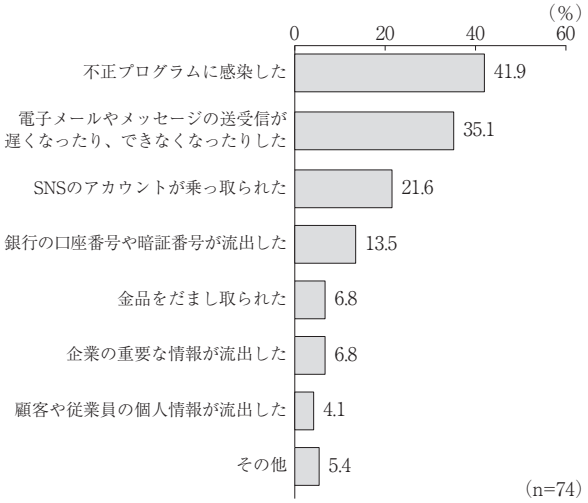
(1) 不審メール・メッセージによる被害

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。被害の内容をみると（複数回答）、「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－19）。

不正プログラムに感染したことがあると回答した企業31社について被害の内訳をみると（複数回答）、「パソコンやタブレット、スマートフォンが使用できなくなった」が14社、「取引先のパソコンやタブレット、スマートフォンをコンピューターウイルスに感染させた」が8社と、数

図－19　不審メール・メッセージによる被害（複数回答）



は少ないものの深刻な被害が生じている。

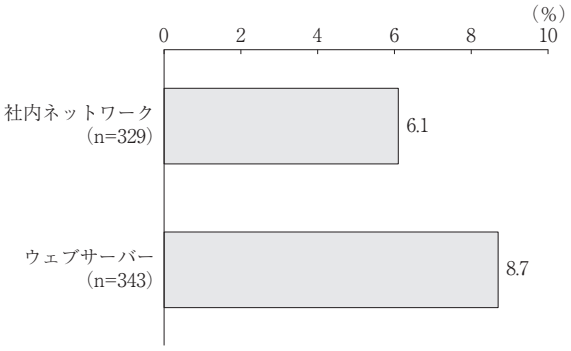
該当する企業の数が多くないので断定はできないが、不審なメールやメッセージによる被害はセキュリティ対策をしていない企業で特に多いというわけではない。例えば、すべてのパソコンにセキュリティソフトをインストールしている企業の場合、不審なメールやメッセージで何らかの被害が生じたことがあるとする企業の割合は11.9%であるが、まったくインストールしていないとする企業でも、この割合は11.3%である。

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。

例えば、NRIセキュアテクノロジーズ㈱が株式上場企業と従業員数350人以上の企業、合計で1,794社を対象に行った「企業における情報セキュリティ実態調査2019[17]」によると、過去1年間に実施した情報セキュリティ対策のきっかけとして最も回答が多かったのは「自社でのセキュリティインシデント」の33.6%だった。同調査におけるインシデン

[17] https://www.nri.com/jp/news/newsrelease/lst/2019/cc/0718_1

図－20　不正アクセスの経験がある企業の割合



トは、サイバー攻撃による被害に限らないが、中小企業よりも情報化が進んでいると思われる規模の大きな企業でも、事故や被害に遭ってはじめて情報セキュリティ対策の必要性に気づくということが少なくないのである。

なお、同調査によると米国とシンガポールの企業の場合、過去1年間に実施したセキュリティ対策のきっかけとして最も多かったのは、両国ともに「経営層のトップダウン指示」で、米国が55.4%、シンガポールが66.1%となっている（日本は23.7%）。米国やシンガポールの企業に比べて、日本の企業は情報セキュリティに対する経営層の関心が薄いことがうかがえる。

(2) 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－20）。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。

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。

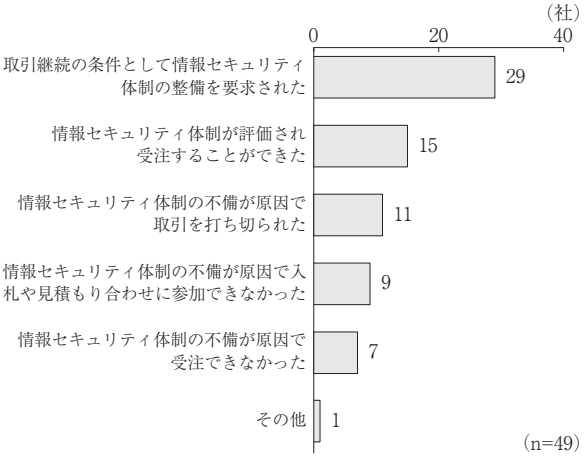
5　情報セキュリティ体制と取引への影響

IPAの「情報セキュリティの10大脅威」で組織に対する脅威に挙げられているもののうち、中小企業が注目すべきものとして「サプライチェーンの弱点を悪用した攻撃」がある（前掲表参照）。自社の情報セキュリティ対策を徹底したとしても取引先の情報セキュリティ対策が甘ければ、そこから機密情報や顧客情報が漏れる可能性がある。情報セキュリティの甘い取引先を通して、部署名や担当者名、取引先とやりとりしたメールなど、標的型攻撃に必要な情報が犯罪者の手に渡ることも考えられる。事業内容にもよるが、情報化が進むほど、サイバーセキュリティ対策を含む情報セキュリティ対策の程度は、取引する際の重要な判断材料になっていくはずだ。

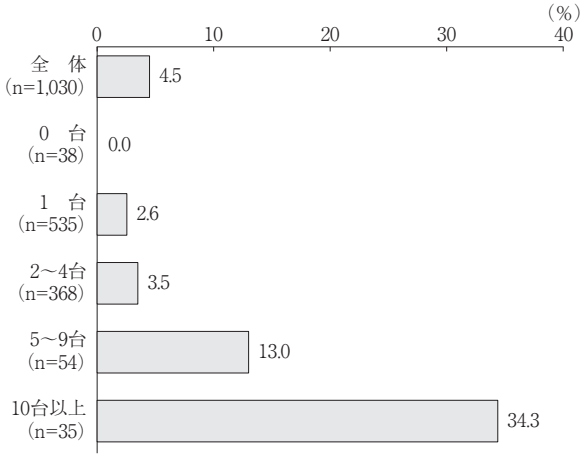
アンケートで、自社の情報セキュリティ体制が受注や販売先との取引に与えた影響についてみると、何らかの影響があったとする企業の割合は回答企業全体では4.8%にとどまっている。ただし、この割合は使用している情報機器の数が多いほど多く、例えばパソコンを「10台以上」使用している企業では20.0%を占めている。

何らかの影響があったと回答した49社について、その内容をみると（複数回答）、最も多かったのは「取引継続の条件として情報セキュリティ体制の整備を要求された」で29社が回答した（図－21）。また、「情報セキュリティ体制の不備が原因で取引を打ち切られた」ことがある企業も11社ある。一方で、「情報セキュリティ体制が評価され受注することができた」とする企業も15社

図－21　情報セキュリティ体制が受注や販売先との取引に与えた影響（複数回答）



図－22　サイバー保険・個人情報漏洩保険に加入している企業の割合（使用しているパソコンの数別）



あり、少数ながら、情報セキュリティ体制が取引に影響を与えていることがわかる。

なお、アンケートでは仕入先や外注先に情報セキュリティ体制の整備を求めているかどうかも質問したが、その結果「すべてに求めている」とする企業の割合が5.4%、「一部には求めている」とする企業の割合が11.2%となった。

6　サイバー保険への加入

前節でみたように、サイバー攻撃に遭う確率はそれほど大きなものではない。だが、窃盗や火災など、現実社会の犯罪や災害に比べて起こる確率が小さいというわけでもない。しかも、被害の程度によっては、事業の存続が危うくなることもある。そこで登場したのがサイバー保険である。

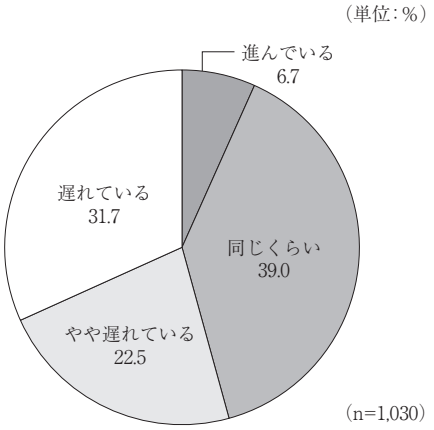
一般社団法人日本損害保険協会によると、サイバー保険はサイバー攻撃によって生じた各種の損害を補償するものである。補償の対象は、個人情報等の漏洩事故による損害の賠償、不正プログラム付きのメールを送信したことにより取引先で発生した損害の賠償、情報機器が使用できなくなったことによって生じた逸失利益、データの復旧費用など幅広い。ただし、ランサムウエアや詐欺に遭って支払った金は補償されない。なお、サイバー攻撃全般ではなく、個人情報の漏洩事故にかかわる損害賠償金や費用だけを補償する個人情報漏洩保険もある。

サイバー保険の保険料は、業種や事業規模、補償範囲によって異なるので一概にいえないが、第三者への賠償責任の上限が1億円であれば、年間で10万円を下回ることが多い。中小企業でも加入できる料金であろう。

アンケートで、サイバー保険または個人情報漏洩保険のいずれかに加入している企業の割合をみると、全体では4.5%となっている（図－22）。サイバー保険または個人情報漏洩保険のいずれかに加入している企業の割合も、情報機器を多く利用しているほど多くなっている。

なお、サイバー保険や個人情報漏洩保険を提供している保険会社には、付帯サービスとして情報セキュリティ診断を提供しているものもある。情報セキュリティ対策が充実しているほど、保険料は安くなることが多いので、サイバー保険や個人情報漏洩保険に加入することは、攻撃に備えるだけではなく、自社の情報セキュリティ対策を見直すきっかけにもなる。

図－23　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。

7　中小企業における問題の所在

中小企業におけるサイバーセキュリティ対策の状況は、多少のばらつきはあるものの、総じて充実しているとは言い難い。本節では、サイバーセキュリティに限らず、情報セキュリティ全般について、自社をどう評価しているのかをみた後、なぜ対策が進んでいないのかを探る。

(1) 自社への評価

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－23）。

「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い。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ようだ。

なお、情報セキュリティ対策の現状を「同じくらい」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いない」と回答した企業でも27.3%を占めている。「進んでいる」や「同じくらい」というのは、あくまで同業の中小企業に比べてのことであり、情報セキュリティ対策に問題がないということではない。

自社の情報セキュリティ対策の現状に対する評価は、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。

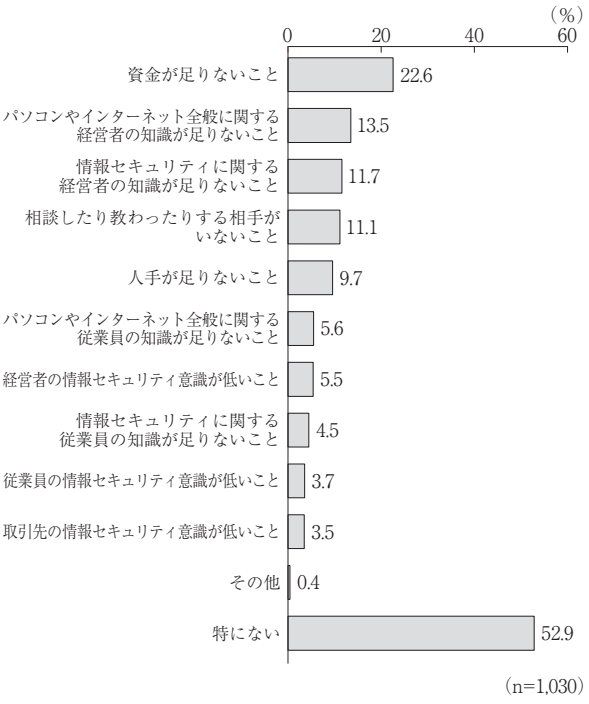
使用している情報機器の数と業務の情報化の度合いは必ずしも比例するわけではないが、これまでもみてきたように、情報化が進んでいる企業ほど情報セキュリティ対策にも熱心であり、逆に情報化が進んでいない企業ほど、情報セキュリティ対策に問題があるといえそうである。

(2) 情報セキュリティ対策を行ううえでの障害

中小企業では、サイバーセキュリティ対策が不十分な企業が多く、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企業も多い。遅れているとわかっているのに、なぜ対策が進まないのだろうか。

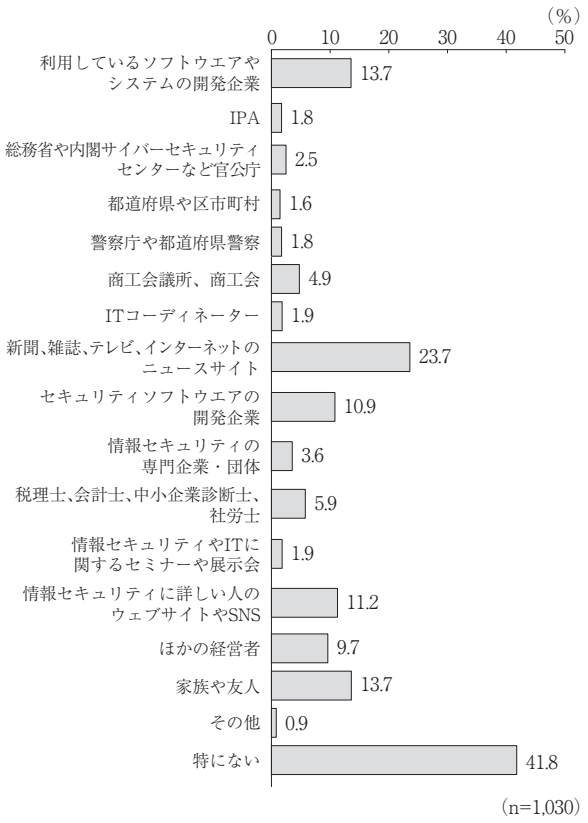
アンケートで、情報セキュリティ対策を進める

図－24　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）従業員に関する項目もn値を1,030とした。

図－25　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）



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－24）。

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「特にない」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「特にない」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。前述のとおり、「同じくらい」と回答した企業でも情報セキュリティ対策が十分ではない企業は多い。

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－25）。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%程度と少ない。

しかし、より注目すべきは情報の入手先がどこかではなく、入手先が「特にない」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「特にない」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「特にない」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いのは、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、ランサムウエ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、第1章で述べたように、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がある。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、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。

第3章　まとめ―政策的含意―

世界的に情報化が進むなか、サイバーセキュリティ対策の重要性は年々高まっているが、第2章でみたように、中小企業ではサイバー攻撃に対して無防備な企業が少なくない。サイバー攻撃は、セキュリティの甘い企業を経由してほかの企業や消費者、官公庁に広がっていく。サイバーセキュリティの甘い企業が存在することは社会経済にとってリスクであり、放置することはできない。第3章では、調査のまとめとして、どうすれば中小企業のサイバーセキュリティ対策が進むのかを考える。

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だ。

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エ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一つのパッケージにして提供している。

また、東京商工会議所は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メール訓練、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な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。

地域を限れば、東京都には最大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。機器やソフトウエアだけではなく、標的型攻撃に備えた訓練費用も対象になる。また、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「サイバーセキュリティ対策支援ローン」がある。対策費用を最大5億円まで融資するもので、サイバー保険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どころか、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エ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を区別することだ。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悪用した攻撃」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。

金融機関の融資においても、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と思われる。中小企業でも、ランサムウエ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し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だ。現実世界なら、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だし、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」では、中小企業がサイバーセキュリティ対策に取り組む場合は、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している。すなわち、①OSやソフトウエアのアップデート、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。

もし、よくわからない、費用がかかるといった理由からサイバーセキュリティ対策が後回しになっているのであれば、五つのうち一つでも、自社にすぐできることはないか考えてほしい。サイバーセキュリティ対策は習慣づけることが重要であり、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」が有効だ。

情報機器やインターネットを利用する限り、誰でも、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。

日本公庫総研レポート　No.2022-1

発行日　2022年1月31日
発行者　㈱日本政策金融公庫 総合研究所
〒100-0004
東京都千代田区大手町1-9-4
電話　03(3270)1269

日本公庫総研レポート No.2022-1 2022年1月

日本政策金融公庫