特集

より安全なデジタル社会を目指すために

コロナ禍を経て、日本企業のIT化が加速し、テレワークや在宅勤務、オンライン会議など、ニューノーマルと呼ばれる新しいワークスタイルが定着した。スーパーマーケットやコンビニエンスストアなどでのセルフレジ設置、ファミリーレストランの配膳ロボット導入、医療機関のオンライン診療など、私たちの身近なところでも急速にIT化が進んでいる。さらに政府は2021年9月にデジタル庁を設置。国・地方行政のIT化やDX（デジタルトランスフォーメーション）を推進し、「誰一人取り残されないデジタル社会の実現」を目指している。

このように日本社会全体でIT化が進む一方で、インターネットを経由した犯罪、いわゆるサイバー攻撃による被害が急増し、業種や規模を問わず、あらゆる組織がターゲットとなって被害を受けている。攻撃手段は巧妙化し、サプライチェーンの脆弱なところを見つけて侵入し、気づいた時には親会社などにも被害が拡大していることもある。

そこで今号のISO NETWORKでは、コロナ後の情報セキュリティについて、現状と今求められる対策がどのようなものかを探っていく。

企業を取り巻く脅威と今求められる情報セキュリティ対策

日本のIT施策を企画立案し、実践する機関として設立された独立行政法人情報処理推進機構（以下、IPA）。誰もがITの恩恵を享受できる社会の構築を目指して「IT社会の動向分析・基盤構築」「情報セキュリティ対策の実現」「IT人材の育成」の3つの柱となる事業を展開している。今回IPAにて中小企業支援を担当している江島 将和 氏に、中小企業の情報セキュリティ対策の現状と今後について聞いた。

独立行政法人情報処理推進機構（IPA）
セキュリティセンター 中小企業支援グループ
グループリーダー　江島 将和 氏

コロナ禍に伴って変化した企業のIT活用

2020年2月以降、新型コロナウイルスの蔓延に伴う行動規制を契機に日本企業のIT化が大きく進みました。これは総務省などがまとめたデータからも読み取れるように、大手企業だけでなく中小企業においてもテレワーク等の活用が伸びています。またBPR（Business Process Re-engineering）と言われる業務改革やビジネススタイルの再構築が行われて、仕事の進め方も変化しています。

一方、この変化に併せてテレワーク等で利用するシステムを狙った攻撃が増え、IPAにも多数の相談をいただいています。IPAが毎年発表している「情報セキュリティ10大脅威」にも2020年に起

■ 情報セキュリティ10大脅威 2022（組織）

2022年順位	脅威	（参考）2021年順位
1位	ランサムウェアによる被害	1位
2位	標的型攻撃による機密情報の窃取	2位
3位	サプライチェーンの弱点を悪用した攻撃	4位
4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	3位
5位	内部不正による情報漏えい	6位
6位	脆弱性対策情報の公開に伴う悪用増加	10位
7位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	NEW
8位	ビジネスメール詐欺による金銭被害	5位
9位	予期せぬIT基盤の障害に伴う業務停止	7位
10位	不注意による情報漏えい等の被害	9位

きた脅威をまとめた2021年版から「テレワーク等のニューノーマルな働き方を狙った攻撃」がランクインするようになりました。

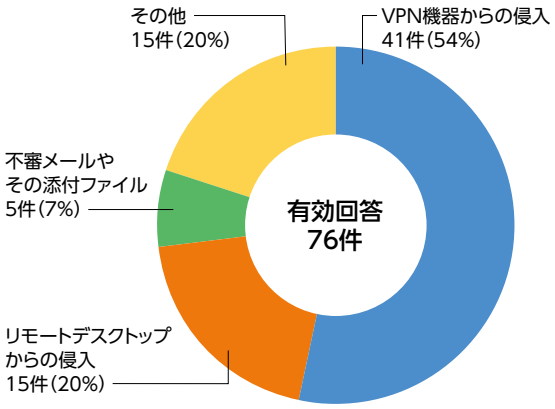
犯罪傾向も変化し、より巧妙な手口が増加

具体的には、WEB会議システムやリモートアクセスツール（VPN、RDPなど）(*)の脆弱性を悪用したサイバー攻撃が非常に増えています。1位にランキングされているランサムウェア攻撃は、データを暗号化し脅迫するだけでなく、機密情報の暴露やシステム停止などで脅迫し金銭を要求するものです。手口が非常に巧妙化しており、従来のウイルス付きのメールを送って誰かが引っかかればいいというバラマキ型ではなく、リモートアクセスツールの脆弱性を悪用するなど標的型攻撃と同様の手法が使われています。事前にポートスキャンなどの偵察行為が行われ、どこに穴があるのか、どういうシステムを使っているのかを調べてターゲットを絞ります。その上で、実在の取引者名、メールアドレスを流用し、取引相手になりすました攻撃メールにより感染を狙うような巧妙な手口の犯罪が増えています。

(*) VPN：Virtual Private Network、RDP：Remote Desktop Protocol

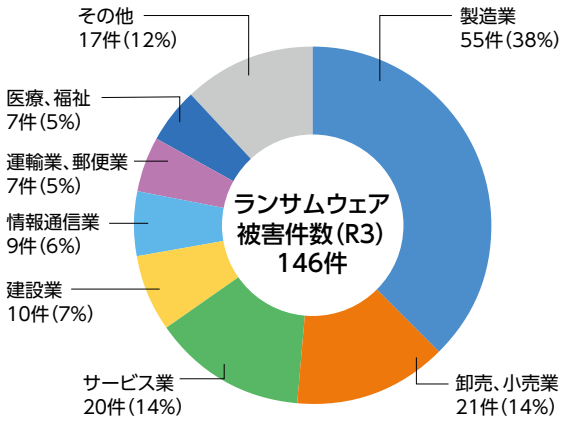
■ ランサムウェアによる被害状況

図1：感染経路



注　図中の割合は小数点第1位以下を四捨五入しているため、総計が必ずしも100にならない。

図2：業種別報告件数



注　図中の割合は小数点第1位以下を四捨五入しているため、総計が必ずしも100にならない。

図3：規模別報告件数

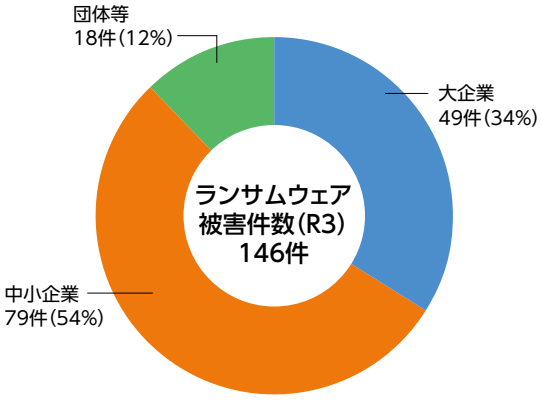
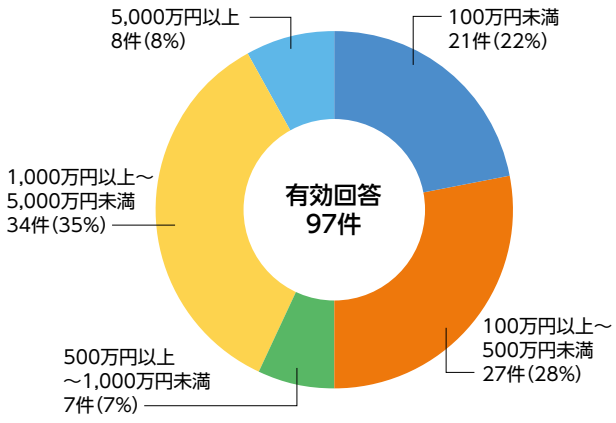


図4：調査・復旧費用の総額



出典：令和3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（警視庁）
https://www.npa.go.jp/publications/statistics/cybersecurity/index.html

「速やかな復旧」を目指す対策にシフト

全ての攻撃を見抜くことができればよいですが、今は避けられないケースがあることを前提にセキュリティ対策を取るようになってきています。いち早く攻撃に気づいて、被害を最小限にとどめて迅速に事業再開できるように復旧することが重要です。セキュリティ対策は、感染を防御するだけでなく、早期に感染を検知し、速やかに復旧する対策にシフトしているといえます。

あらゆる企業がサイバー攻撃の対象

サイバー攻撃というと、国家機密や大手企業を狙ったハッキングのイメージを持つ方も多いと思いますが、現在は業種や規模を問わず、インターネットを利用するあらゆる企業がターゲットとなっています。特にサプライチェーン攻撃は、ターゲットとなる大企業の関連会社や取引先を経由して大企業にサイバー攻撃をするもので、セキュリティが手薄になりがちな中小企業が狙われています。2022年前半の自動車製造工場の稼働停止が記憶に新しいところです。これは、取引先である部品会社の子会社が、別会社とつないでいた専用回線の機器の脆弱性を狙ったものでした。そのほか海外でも似たようなケースが相次いで発生し、サプライチェーン攻撃のリスクと被害の大きさが認知されるようになりました。このようにサイバー攻撃は、単なるシステムトラブルでは済まされない、関連企業や取引先まで巻き込む、事業継続にかかわる重大なリスクといえます。

今後、取引上の義務・要請が増加する

前出の自動車関連であれば、自動車工業会と部品工業会が共同でガイドラインを作成し、それを満たすことが推奨されています。自動車業界だけでなく、さまざまな業界に同様の動きが広がっています。背景には、取引企業間のネットワーク接続やクラウド導入が進んでいること、さらに人材不足や作業の効率を上げる手段としてロボット導入や遠隔作業などのIT活用の促進があります。今後はビジネスをする上で何らかの情報セキュリティ対策を取ることが必要不可欠になると考えられます。

中小企業の3割がセキュリティ対策を行っていない

IPAで実施した「2021年度 中小企業における情報セキュリティ対策に関する実態調査」では、約3割の中小企業がセキュリティ対策の「投資を行っていない」と答えています。その理由として「コストがかかり過ぎる」「費用対効果が見えない」などが挙げられていますが、そもそも「必要性を感じていない」と回答した企業が約4割を占めています。この調査は前回2016年に実施したのですが、情報セキュリティ対策の実施状況の改善はわずかでした。このことからも中小企業ではセキュリティ対策への投資が十分に行われていないことが伺えます。また、セキュリティ被害の有無に関する調査では、被害を受けたと回答した企業は5.7%で、84.3%が「被害にあっていない」と回答しています。しかし、IPAが実施した「サイバーセキュリティお助け隊実証事業」で企業にセンサー（ファイヤーウォールなど）を導入してもらったところ、センサーを設置したほぼ全ての企業で何らかのサイバー攻撃の兆候を確認しました。つまり、サイバー攻撃に気づかない、認識できていないケース

は少なくはないと考えられます。実際、ご協力いただいた約1,100社の中小企業に対して、不審なアクセスが18万件以上検知され、ランサムウェアやトロイの木馬などのウイルスを無害化した件数が1,345件もありました。もし気づかずに放置した場合、被害状況の把握、復旧、対策などにかかる費用を合わせると5,000万円以上の被害額が想定されるものもありました。

■ 情報セキュリティ対策に関する実態調査

図5：直近過去3期の情報セキュリティ対策投資額

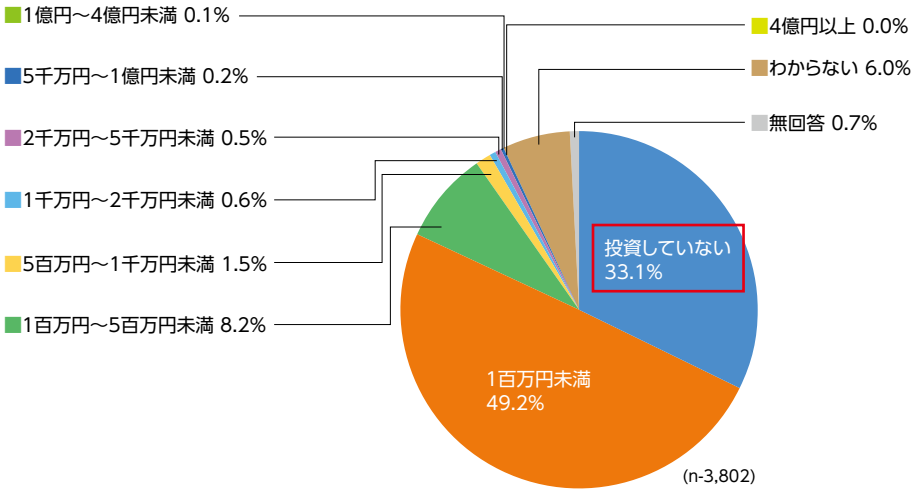
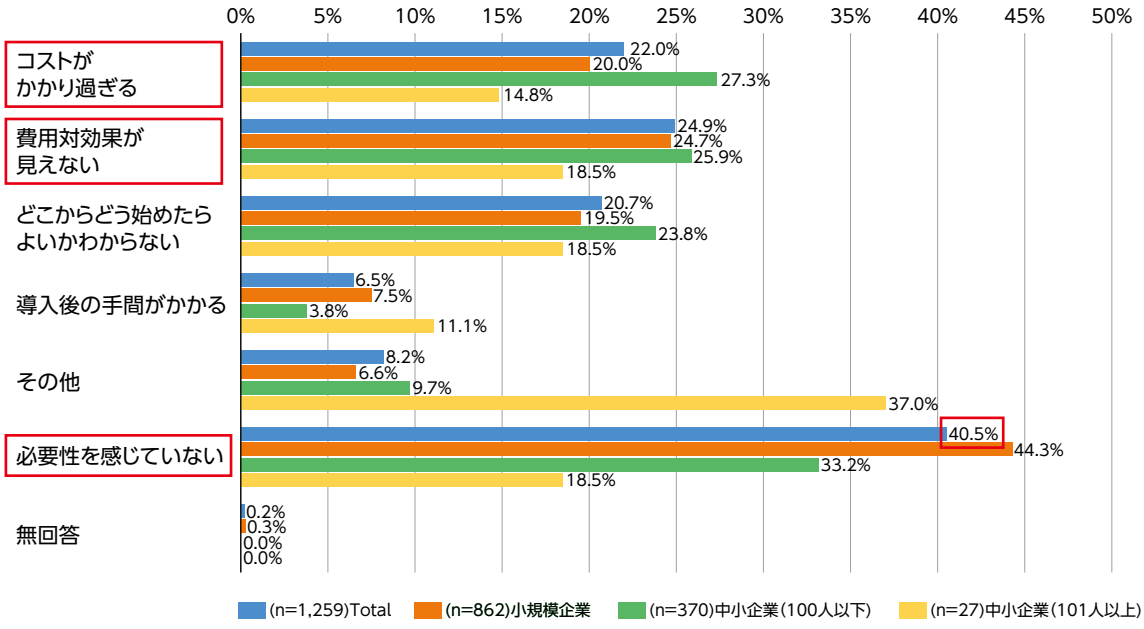


図6：情報セキュリティ対策投資を行わなかった理由（企業規模別）



出典：2021年度 中小企業における情報セキュリティ対策に関する実態調査（IPA）
https://www.ipa.go.jp/security/fy2021/reports/sme/index.html

セキュリティ対策への投資が増えない理由

経営者のセキュリティ意識に起因すると思います。先にも説明しましたが、昨今のサイバー攻撃は、非常に巧妙化しています。サイバー攻撃は、インターネットなどのサイバー空間で起きることから、物理的な事故と違って目に見えません。中小企業の経営者の平均年齢は60歳以上という調査結果もあります。先の調査結果で「必要性を感じていない」との回答が多かったことからも、IT化のスピードに付いていけない、リスクとして十分な認識を持てない、分からないからどう対処していいか判断できないという、中小企業の現状が見て取れます。いずれの企業も何らかのサプライチェーンの一端を担っていると考えると、経営者の皆さまには、サイバー攻撃が企業の事業継続にかかわる重大なリスクとして認識していただきたいです。

情報セキュリティ対策を始める

すでに対策を取られている企業も多いと思いますが、取引先や関連会社などに未対応の企業がありましたら、IPAが設けた「SECURITY ACTION制度」から取り組んでいただければと思います。この制度は、「情報セキュリティ5か条」などを企業自らがセキュリティに取り組むことを宣言することによって、ロゴマークを使えるようになります。

■ IPAが設けた「SECURITY ACTION制度」

情報セキュリティ5か条

1. OSやソフトウェアは常に最新の状態にしよう!
2. ウイルス対策ソフトを導入しよう!
3. パスワードを強化しよう!
4. 共有設定を見直そう!
5. 脅威や攻撃の手口を知ろう!

SECURITY ACTIONロゴマーク
https://www.ipa.go.jp/security/security-action/index.html

情報セキュリティ対策への取り組みを見える化するとともに、顧客や取引先との信頼関係の構築を図ります。また、補助金の申請や普及賛同企業から支援を受けられるなど、公的補助や民間支援も受けやすくなるメリットもあります。さらにステップアップできるように、「中小企業の情報セキュリティ対策ガイドライン」を公開しています。社内規定の整備や情報セキュリティマネジメントシステムの構築をカバーできるような仕組みとなっていますので、ぜひご活用いただきたいです。

IPAが提供する支援サービス

IPAには、中小企業向けの支援サービスとして、「サイバーセキュリティお助け隊サービス制度」があります。「見守り」「駆付け」「保険」などの中小企業のセキュリティ対策に不可欠なサービスをワンパッケージで安価に提供しています。お助け隊のロゴマークのある民間サービスは、IT導入補助金の対象にもなりますので、ITツール導入の際にぜひご利用いただきたいと思います。

サイバーセキュリティお助け隊サービス制度のロゴマーク
https://www.ipa.go.jp/security/otasuketai-pr/

そのほか、情報セキュリティ支援サイトの運営、情報セキュリティの脅威等を学ぶ動画配信などの啓発活動や、国家試験「ITパスポート」「情報セキュリティマネジメント試験」の実施、国家資格「情報処理安全確保支援士」の運用などに取り組んでいます。

IPAが提供するさまざまなコンテンツを多くの方にご活用いただき、来るデジタル社会に備えて、情報セキュリティ対策に取り組んでいただければと思います。

(取材日：2022年12月9日)■