論　　文

# 中小企業へのサイバー攻撃の現状とその被害調査結果に関して

## ―IPAおよび大阪商工会議所の調査結果から見えること―

森　井　昌　克
（神戸大学大学院工学研究科教授）

＜要　旨＞

最近の(独)情報処理振興機構（IPA）や大阪商工会議所の中小企業に対するサイバーセキュリティに関するアンケート調査を受けて、中小企業のサイバーセキュリティ意識の実態を考察するとともに、2018年9月から翌年1月にかけて行われた、大阪市内中小企業30社のサイバー攻撃の実態調査結果を報告する。さらにその結果から得られた傾向と分析結果を与える。本調査は実質的には著者らのグループが行なった。この調査は個々の中小企業のネットワークを観測し、その分析を第三者的に行い、かつ相互比較、相互分析したところに新規性があり、同様の調査実験は国内初であり、その実現は画期的である。

今回、過去に例を見ない、種々の業種での中小企業30社において、約4ヶ月という長期間、しかも各中小企業にセンサを設置し、出入りしているパケットを全て観測し、それぞれの中小企業に対するサイバー攻撃の現状だけでなく、不正アクセスの可否についても詳細に調査を行った。その結果、

・外部から社内の端末をリモート操作
・社内端末と悪性サイトとの通信
・DDoS攻撃を目的としたパケットを受信

等の被害を受けたとされる中小企業がそれぞれ複数存在することが明らかになった。さらに、ポートスキャンやSSH等のサービスへのパスワード試行といった攻撃だけではなく、OpenSSLの脆弱性「HeartBleed」を狙った攻撃や、SSL3.0の脆弱性「POODLE」を狙った攻撃、あるいはエクスプロイットキットというハッキングツールを利用した高度な攻撃手法も観測されている。決して中小企業がサイバー攻撃されていないわけではなく、それどころか高度な攻撃手法を用いての攻撃に常にさらされていることが判明し、その中のいくつかに関しては攻撃が成功し、被害を受けている可能性が高いことを示した。

目　次



## １．はじめに

IoT（Internet of Things）はすべての「モノ」をインターネットにつなげることによって社会変革を促す概念である。身近なところでは、テレビ録画機（ハードディスクレコーダー等）はインターネットと結ばれ、出張先等で、スマホ（スマートフォン）等を用いて遠隔から録画予約をすることが可能である。また録画された番組をスマホで見ることも可能になっている。これだけでテレビ番組を見るという時間的制約から解放される。すべてがインターネットにつながることによって、時間や場所から解き放たれるだけでなく、そのつながった「モノ」自体が新たな情報を生み出す、新たな循環を築こうとしている。情報が価値を生み、さらにその価値が「モノ」を生むという循環が新たな産業構造を構築する。いわゆるindustry4.0（インダストリー・ヨン・テン・ゼロ）と呼ばれる第四次産業革命である。

CPS（シー・ピー・エス）はCyber Physical System（サイバー・フィジカル・システム）の略で、サイバー空間とフィジカル空間の連携を超え、さらに融合した社会を目指すシステム（体系）のことである。それが第四次産業革命の舞台となるのである。フィジカル空間とは人間がその行動を基本に、実体のある「モノ」と接することによって生活する空間である。サイバー空間とは「モノ」ではなく、情報を介して人間が生活する空間である。フィジカル空間は人間が意識を持って社会を形成して以来、数万年にわたる歴史があり、それに対してサイバー空間はたかだか数十年の歴史しかない。これらを融合した社会の実現には課題が山積している。特にサイバー空間の急激な成長は、人間との関わり、そしてフィジカル社会を鑑みたとき、大きなひずみを生んでいる。その一つがサイバー攻撃なのである。

近年の政府における政策もあって、行政組織及び地方自治体、並びに社会全体の運営に密接に結びつくインフラ企業、そしてそれに関連する大企業においてはサイバー攻撃への対策は十分とは言えないまでも、その脅威への意識が根付くようになってきた。しかしながら、上記以外の組織、特に中小企業においてはその不十分さが指摘されることとなった。その契機の

一つがサプライチェーンの構造にある。重要視している社会関連インフラを担う大企業も、自社の関連会社のみで製品やサービスを行なっているわけではなく、多数の中小企業がその製品群を有形無形に支えている。その一端が崩れることにより、全てに影響することが避けられない。つまり中小企業へのサイバー攻撃の可否が予想もしなかった重要社会インフラへのサイバー攻撃に転化することもあり得る。

本稿では、最近の情報処理振興機構（IPA）や大阪商工会議所の中小企業に対するサイバーセキュリティに関するアンケート調査を受けて、中小企業のサイバーセキュリティ意識の実態を考察するとともに、2018年9月から翌年1月にかけて行われた、大阪市内中小企業30社のサイバー攻撃の実態調査結果を報告する。さらにその結果から得られた傾向と分析結果を与える。本調査は実質的には著者らのグループが行なった。この調査は個々の中小企業のネットワークを観測し、その分析を第三者的に行い、かつ相互比較、相互分析したところに新規性があり、同様の調査実験は国内初であり、その実現は画期的である。また得られた結果についても中小企業に対するセキュリティ攻撃の実態と、その被害、すなわちセキュリティ対策の実情をあらわにし、今後のセキュリティ対策全般に対して十分な知見を与えるものである。

## ２．サイバー攻撃とは

フィジカル空間、つまり今までの「モノ」を中心とした社会において、例えば深夜に泥棒が入り、現金や重要書類を盗んでいくということは滅多にない。有り得るとしても、その対策や予防方法は十分理解でき、対応可能である。警察や警備会社等を含む社会組織として、それらの脅威を排除できる構造になっているのである。残念ながらサイバー空間はまだまだ十分成熟しておらず、すべての脅威を排除できるほどにはなっていない。特に脅威に相対する社会としての構造が未熟ゆえ、エンティティ（サイバー社会を構築する機械や、その機械の恩恵に与る人間）それぞれが脅威に対して十分な対策を取る必要がある。そしてその最大の脅威こそ、サイバー空間に対する不正行為、つまりサイバー攻撃なのである。

「サイバー攻撃」について、特に中小企業にとって無縁と考える人は少なくないであろう。しかしサイバー攻撃はすべての組織、企業、人にとって身近な存在となっている。「情報漏えいの事実はなく、不審なことは起こってない」と反論する人も少なくないが、それは気づいていないだけなのである。現在のサイバー攻撃は気づかせることなく、ひそかに活動する。日本年金機構や㈱JTBの個人情報漏えい等大きく報道された事件も、ほとんど例外なく、第三者からの通報である。

最も身近で、注意すべき攻撃は標的型メール攻撃であろう。やはり「私は標的にならないから。漏れては困る情報もないので…」と考える人も少なくない。しかし、現在の標的型メール攻撃は標的を選ばない。また現在のところ、メールを含めて漏れては困る情報がないとしても、今後、未来永劫ないとは言い切れない。標的型メール攻撃では、その被害に遭ったとしても、いきなり情報漏えいすることはまれで、バックドアと呼ばれる、いつでも再度遠隔から情

報を盗み取る「抜け穴」を作られることもある。数年後、改めて情報が盗み取られるのである。またパソコン等が遠隔操作され、そのパソコンを踏み台（起点）にし、他をサイバー攻撃することもあり得る。その場合、そのパソコンが警察に押収されて長期間戻されることなく、業務に大きな差支えが出てくることが考えられる。

## 3．中小企業の直接的被害

本章では特に中小企業へのサイバー攻撃による直接的被害について解説する。

### 3.1　不正送金の手口と仕組み

ネット銀行が国内でも利用されるようになった10数年前、フィッシングと呼ばれる手口が登場した。「フィッシング」とはPhishingと綴られ、sophisticated（洗練された）とfishing（釣り）の造語だと言われている。つまり、洗練された方法で、相手を詐欺の罠に捕らえる、釣るのである。具体的には、メールを使って、不特定多数に例えば「あなたの口座が不正アクセスを受けて、パスワードが改ざんされた可能性があります。至急、確認して下さい」という内容のメールに、ネット銀行を装ったURLのリンクが貼られているのである。驚いて正気を失ったユーザは、そのリンクをクリックしてしまい、ネット銀行を装ったログインページにIDとパスワードを入力してしまうのである。大概の場合、それらを入力した後は「エラー（間違い）」の表示が出て、正しいネット銀行のログインページに移動させられる。IDとパスワードを入力してしまった人は、最初の入力は自分の入力ミスだと勘違いし、それを盗まれたことにまったく気づかないのである。

現在では、その対策としてIDとパスワードだけでなく、「2要素認証」と呼ばれる、さらにもう一段階の認証を組み合わせることが一般的である。例えば、あらかじめ登録されたSMS（ショートメッセージサービス）やメールアドレスに「ワンタイムパスワード」と呼ばれる、その1回限りのパスワードを送り、その入力を確認する方式である。

しかしながら新たな手口も登場している。それはコンピュータウイルス（マルウェア）に感染させて、事実上、パソコンを乗っ取り、不正送金を行う手口である。マルウェアによってパソコンが乗っ取られれば、そのパソコンは自由に操られてしまう。例えば、乗っ取られたパソコンで、正しいネット銀行のサイトにIDとパスワードを入力したとたんに、勝手に動作して、ワンタイムパスワードの操作を含め、不正な送金手続きを行うのである。これは「MITB（Man in the Browser）攻撃」と呼ばれるもので、まさにブラウザのなかに人（犯罪者）がいるように、不正送金の仲介をしてしまうのである。

2017年12月中旬、日本航空㈱（JAL）が振り込み詐欺の被害に遭い、約3億8千万円を奪い取られる事件が発覚した。取引先に成りすまし、航空機リース料の請求メールを送られ、騙されたのである。一連の取引メールも本物と見分けがつかず、請求書も本物に酷似した従来通りの形式で、発信者も従来の取引先の名前とメールアドレスが表示されていた。明らかに、サイバー空間を利用した周到な準備に基づく詐欺なのである。このような詐欺を「ビジネスメール詐欺」（BEC、Business E-mail Compromise）と

呼ぶ。この事件は著名な大企業であること、そして被害が多額であることで注目を浴びたが、事件自体は決して珍しくも、新しくもなく、企業の電子決済、ネット送金が一般化してから多発している。ここ数年では、少なくない数の中小企業が数百万円から数千万円の単位で被害に遭っており、いくつかは被害届を警察に届け、事件化しているものの、さまざまな理由から公にしていない事例も少なくない。JALに代表されるように、被害に遭った企業自体がサイバーセキュリティ対策をおろそかにしていたわけではなく、手口が巧妙化し、その被害を防ぐことが極めて難しくなっているのである。ましてやその対策をほとんど取っていない、被害を想定すらしていない企業を欺くことは極めて容易であろうことは想像に難くない。

ビジネスメール詐欺を行うためには、通常の詐欺と同様、周到な準備が必要である。特に公開・非公開情報、さらに秘匿されるべき情報を収集する必要がある。具体的には決済に関わる人の氏名、役職、メールアドレスに始まる個人情報、それに取引相手の同様な情報、そして決済形式等の決済情報等である。その情報を得るためにはマルウェアが利用される。マルウェアに感染させることによって、メールや社内情報を漏洩させ、収集するのである。

### 3.2　ランサムウェア

マルウェアはサイバー攻撃を成功に至らしめる要である。つまり攻撃する側にとって、如何にマルウェアを感染させるか、そのマルウェアにどのような不正をはたらかせるか、そして如何に発見されないように動作させるかが重要となる。改めてマルウェアを概説する。

マルウェアは利用者の意図に反する不正なプログラム一般を指す言葉であるが、「利用者の意に反する行動を取るプログラムであり、その行動としては、許可なくパソコンに侵入する行為（感染）、プログラム自体をパソコンに保存する行為（潜伏）、そしてプログラムを起動して何らかの意に反する作業を行う行為（発症）であり、その一つにでも当てはまれば該当する」と定義される、「コンピュータウイルス」と以前には称された不正プログラムを指すことが一般的である。マルウェアの悪意とは、主にこの意に反する作業のことである。2000年前後までは感染させること自体が目的であり、発症は感染したことを示す、そして誇示するための行為であった。したがって発症にも悪意があるとはいえ、「いたずら」程度であった。この十数年になってからは、発症が目的になり、その発症に伴う悪事は金銭目的や相手に対して何がしかの損失(ダメージ)を与えることとなった。「いたずら」から「犯罪」になったのである。具体的にはパソコンを遠隔操作して、他のパソコンやサーバを攻撃したり、パソコン内の情報を搾取（漏えい）したり、パソコンについているカメラやマイクを利用して盗撮・盗聴したりする。そのマルウェアの発症行為の中でも、特に問題となっている行為が「身代金要求」である。身代金と言っても人間を誘拐するわけではなく、パソコンを誘拐するのである。パソコンを使用不能にして、復旧を条件に金品を要求する行為である。このようなマルウェアを「ランサムウェア」と呼ぶ。その仕組みは、ランサムウェアに感染するとパソコンの中のファイルを暗号化

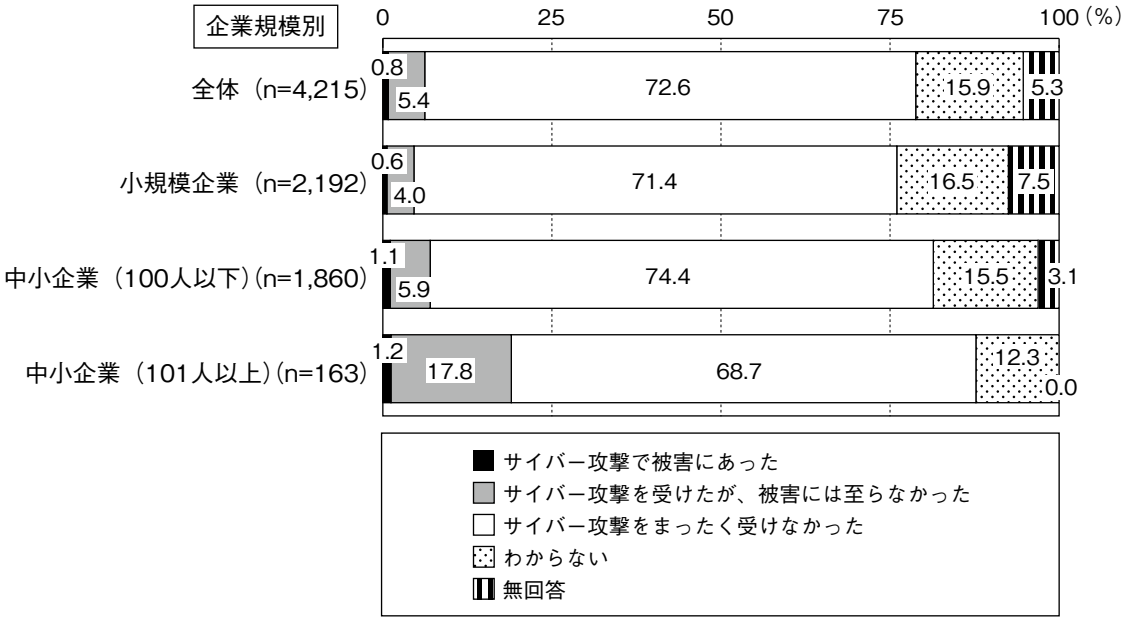
し、この暗号を解かなければパソコンは動作不能とさせる。この暗号を解く方法を質に金品を要求する。後述するように、このランサムウェアの被害が中小企業では多発しているのである。さらに最近ではこのランサムウェアが進化し、パソコンを動作不能にするという明示的な行為ではなく、自覚がないままパソコンの計算能力を奪い取ってしまう行為である。奪い取った計算能力は仮想通貨の採掘（マイニング）に用いられる。詳細は省くが、話題の仮想通貨を作り出す（発行する）ために大きな計算能力を必要とするため、その計算を小分けして、感染させたパソコンに行わせる。感染したパソコンは気づかれることなく計算を繰り返し、その結果を送り続ける。感染したパソコン側では、無用な計算を行うことによって、動作が遅くなったり、ソフトウェアが動かなくなったりする場合がある。

## 4．中小企業のセキュリティ意識

（独）情報処理推進機構（IPA）では従業員300人以下の中小企業を対象にした情報セキュリティに関する調査報告を行っている。セキュリティ対策や意識等、多岐にわたるアンケート調査であり、中小企業に対するサイバー攻撃の現状としては興味深い結果を表している。

その要点として、中小企業ではその規模にほとんど関わらず、サイバー攻撃の被害に遭っていない、正確には1%前後の企業しかサイバー攻撃の被害に遭っていないと答えている。しかし、被害はともかく、サイバー攻撃を受けたと答えている企業においては、101人以上300人以下の規模であれば19.0%であるのに対して、100人以下の企業では7.0%であり、規模の小さい企業ほどサイバー攻撃を受けていないと答えている（**図1**）。また、規模が同じであれば、情

**（図1）企業規模別のサイバー攻撃被害の有無**




（出所）「2016年度中小企業における情報セキュリティ対策の実態調査報告書」（2017年6月）
（注）中小企業と小規模企業の定義は、「中小企業基本法」第2条及び同法第2条第5項による。
小規模企業は20人以下の従業員数とし、中でも卸売業、サービス業、小売業では5人以下とする。

報通信関連の企業ほどその割合は多い。中小企業ではなく、大企業であれば、昨今のほとんどの調査で、少なくとも70%以上の会社が何がしかのサイバー攻撃を受けたと報告されている。すなわち、規模が小さい企業ほどサイバー攻撃を受けていないのではなく、規模に関わらずサイバー攻撃を受けているものの、気付いていないと考えるほうが妥当である。

さらに興味深い調査結果が「中小企業におけるサイバー攻撃対策に関するアンケート調査」として大阪商工会議所から報告されている。

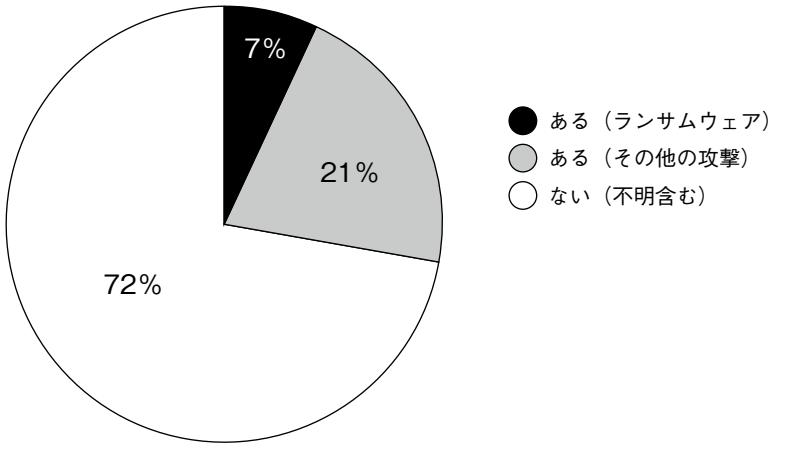
大阪商工会議所の調査は、中小企業でも従業員数50人以下の企業を対象にしており、建設、製造、卸売、そしてサービス業を中心に各種業種に及んでいる。その中で、（**図2**）のように30%近くが攻撃に遭っている。大阪商工会議所の調査では、設問数を15以下の選択制で行い、回答が容易で、かつ事実を述べやすいように工夫している。その中で実数として315社中87社がサイバー攻撃の攻撃を受けており、特にランサムウェアに感染したと述べている企業が22社（7%）もあることが注目に値する。

前章で述べたように、ランサムウェアに感染するとパソコンのハードディスク上のデータが暗号化され、指定された口座に現金、もしくは仮想通貨を振り込まなければ、その暗号化鍵を取得できず、永久に使用不能となる。以前からこのランサムウェアの被害が深刻であると言われていたものの、実際の被害については明確になっていなかった。今回の調査では具体的に22社も感染していたことが明らかになるとともに、公開していないものの、その約半数である10社近くが、実際に仮想通貨を振り込んでいるのである。

大阪商工会議所の調査では、約80%の企業がサイバー攻撃のリスクを認識しているものの、アンチウイルスソフトの導入だけで、対策を済ませている企業が全体の30%に達していることである。つまりリスクを認識している企業ですら、アンチウイルスソフトの導入程度の対策しか取られていないのである。

IPAの調査と大阪商工会議所の調査を合わ

**（図2）サイバー攻撃を受けたことがあるか？**




（出所）「2017年中小企業におけるサイバー攻撃対策に関するアンケート調査結果」

せて考察するに、規模の小さな中小企業ほどサイバー攻撃に対するリスクは認識しているものの、実際にサイバー攻撃を受けていても、それを認識できず、さらに少なくない割合で、そのサイバー攻撃が成功していると考えられる。

深刻なのはサプライチェーン上の中小企業である。大阪商工会議所が2019年5月、サプライチェーン上にある従業員100名以上の大企業、中堅企業118社における、質問回答文書及びヒアリングによる調査結果を発表した。その要旨としては

*(1) 4社に1社がサプライチェーン上の取引先のサイバー攻撃被害が自社に及んだ経験がある*
*(2) 約7割の企業がサプライチェーン上の取引先のサイバー攻撃に対する取り組み、被害について把握していない*
*(3) 約6割の企業がサプライチェーン上の中小企業自身が対策を担うべきと回答*

である。従来から、サプライチェーンにつながる中小企業へのサイバー攻撃が、その上位の大手企業、さらに鉄道、道路、電力、通信等のインフラ関係企業に影響を及ぼし、特に中小企業を踏み台に、本来、サイバー攻撃対策が十分に行われているにもかかわらず、不正アクセスが成功する可能性が危惧されていた。この危惧が現実のものであることが明らかとなった。4社に1社という少なくない企業が、自社のサプライチェーンにある中小企業のサイバー攻撃対策不備によって危険に晒されていたのである。改めてサプライチェーン上の中小企業におけるセキュリティ対策の重要性が示され、看過できない現状が露呈される結果となった。さらにこのような現状にも関わらず、自社のサプライチェーン上の中小企業のサイバー攻撃対策の現状をほとんど把握していないという状況も明らかになった。言わば、この危機的な状態の一因が、必ずしも中小企業のサイバー攻撃対策の不備ではなく、その状態を把握し、管理すべき大企業の無責任でもある。大企業が積極的に中小企業のサイバー攻撃対策に関与する必要性が露わとなった。

さらに報告書を読み解くと次の結論が導出される。

(1) サイバー攻撃対策について、6割以上の会社が取引先に求めることは「注意喚起」程度

サプライチェーン上の中小企業の脆弱性を狙って、不正アクセスを成功させ、その中小企業を踏み台に攻撃するサプライチェーン攻撃の深刻さがこの数年、大きく取り上げられ、今回の調査結果でも被害に結びつくことが明らかにされたにも関わらず、取引先のサイバー攻撃対策に関心を示さないことは大きな問題である。被害が及んだ場合でも、5割以上の企業が「注意喚起」程度の対策しか取らないことを考慮すると、関心を示さない理由としてはサイバー攻撃、及びその被害について、その深刻さを理解していないことが推し量られる。

(2) 大企業においても、必ずしもサイバー攻撃の被害とその深刻さについて理解がない

「取引先がサイバー攻撃被害を受け、それが自社に及んだ経験がある」と回答した企業は

30社であった。その30社において、被害ではないが、おそらく中小企業から自社のメールアドレス等が漏洩し、マルウェア感染や詐欺等を目的としたスパムメールが届いたという件数が半数以上であるものの、不正アクセスが9社、導入した製品自体にマルウェアが混入していたという企業が6社も存在した。しかしながら30社中、被害と認識した企業は6社に過ぎず、「情報漏洩、システムダウン、あるいはデータの損壊」に及んだ企業は8社であることと大きく矛盾する。明らかに被害を受けたにも関わらず、少なくとも2社はその被害を認識していないのである。それ以外にも「不正アクセス、ウイルス混入、ランサムウェア感染」のいずれかに陥った企業も少なくとも9社あり、やはり被害と認識している企業数6社よりも多くなっている。これは明らかにサイバー攻撃の被害というもの自体を認識していない、あるいは非常に被害内容を軽んじていることに他ならない。大企業がサプライチェーン上での取引先のサイバー攻撃の深刻さに対して無関心であることを表す一つの証拠として、「取引先のWindows7/Windows Server2008サポート終了への対応に関して把握しているか」との問いに、6割以上の会社が把握していないと回答し、対応済を把握していると回答したのは、たったの5社に過ぎなかったことが上げられる。

## 5．中小企業30社への実地調査とその方法

### 5.1　調査の背景

先に解説した、大阪商工会議所の「中小企業におけるサイバー攻撃対策に関するアンケート調査」により、中小企業であっても、標的型攻撃メールの受信（18%）やランサムウェアによる被害（7%）が示された。そして、「現在実施している情報セキュリティ対策で十分でない」と回答した企業も約7割（68%）となっており、その理由として「経費がかけられない」(60%)、「専門人材がいないのでわからない」(48%)を挙げた回答が多い。この調査によって、多くの中小企業がサイバー攻撃を受け、その被害を危惧していることが判明した。一方で、人材がいない、経費がかけられないといった理由から対策が十分に行われず、サイバー攻撃を受け、不正アクセスの被害を受けている事自体を把握していない可能性がある。2018年、調査対象機関である中小企業のネットワークにセンサを置いて、パケット情報を収集し、それを直接分析することで、それぞれの中小企業に対するサイバー攻撃の有無を調査することにより、中小企業に対するサイバー攻撃の現状を把握することを目的とした。

### 5.2　調査方法

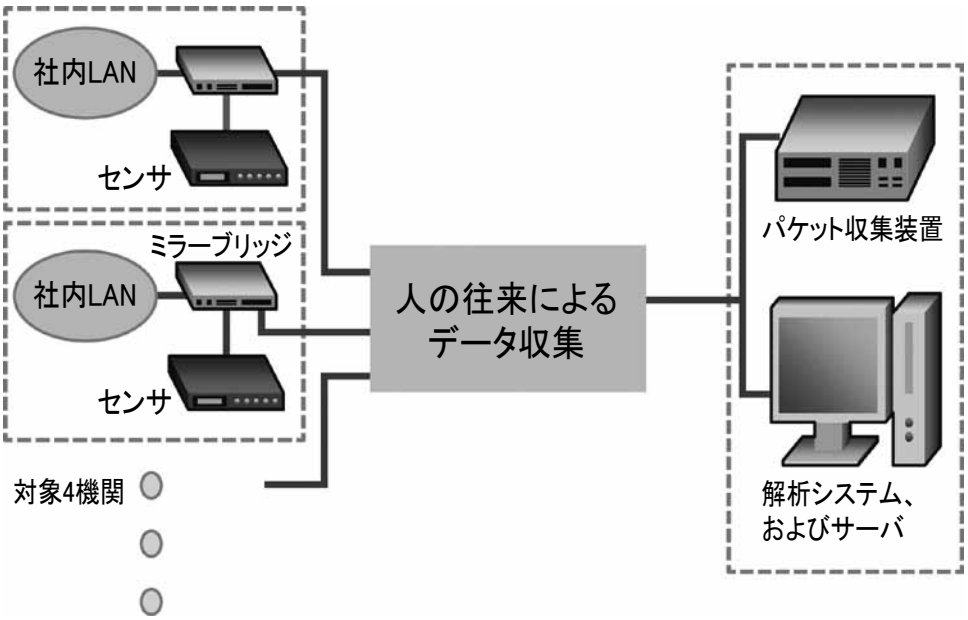
調査対象中小企業にセンサを設置し、パケット情報を収集、それを直接分析する（**図3**）。本調査では、オープンソースの侵入検知システム（IDS）であるSuricataを利用したセンサを用いて、パケット情報を収集する。さらに、解析システムを構築することによって、サイバー攻撃の分析を行う。センサで取得したパケット情報に基づくIDSのアラート情報は、定期的に係員が蓄積媒体（USB等）でコピーして収集した。いわゆる民間のSOC（セキュリティオペレーションセンター）サービスと同様、ネットワーク

を介してアラート情報を自動的に収集する方法も考えられたが、対象中小企業のネットワークを間接的にも利用することになり、ネットワーク設定を少なからずも変更することへの不安を取り除くとともに、係員を定期的に派遣することによって、ネットワークやそれを取り巻く機器の状態を実際に観測（監視）でき、また中小企業のIT機器に関する利用方法や問題点に素早く対応できる副次的な作用を期待して、今回の収集方法となった。なお、パケットはヘッダと呼ばれる送受信先IPアドレス、パケットの種類等を観測し、ペイロードと呼ばれるパケットの内容については原則観測することはない。収集したデータを分析して、レポートとして、定期的に中小企業に送付することとし、調査期間の中間及び終了後に、全体の詳細解析を行い、サイバー攻撃の現状を分析した。本調査で設置するセンサは、各機関の現有ネットワークに流れるパケットを複製、分岐させ収集するため、現有ネットワークには影響を与えないことを確認している。

Suricataはノートパソコン上で機能させる。ノートパソコンにはUbuntu 16.04 LTSをインストールし、Windows Update等による、予期しない端末の再起動などを避けるため、LinuxOSを利用している。UbuntuにSuricata 4.04をインストールし、セットアップを行う。Suricataで監視するネットワークアドレス空間は機関ごとに設定する必要がある。

本調査で取得するログは**表1**のとおりである。解析には主に①と②のログデータを利用する。①は観測した全てのパケットの送信元IPアドレスやポート、宛先IPアドレスやポート、利用プロトコルなどのパケットの情報を記載したログデータである。Suricataでは、観測した各パケットをルールに従って悪性か悪性でないかを判定し、悪性である場合、アラートを出力している。②はアラートの情報を記載したログデー

**（図3）センサ及び解析システムネットワークのイメージ**




筆者作成

（表1）取得ログの一覧とその概要

| | ログファイル名 | 概要 |
|---|---|---|
| ① | eve. json | アラート、http、DNS、TLS、fileの送受信などのパケット及びイベント情報のログである。 |
| ② | fast. log | アラート情報を記載したログである。 |
| ③ | alert-debug. log | パケットのペイロードを含む詳細なアラートイベントのログである。 |
| ④ | http. log | ①からhttpトラヒックを抽出したログである。詳細ログ出力のために、extendを有効にしている。 |
| ⑤ | dns. log | ①からDNSイベントを抽出したログである。 |
| ⑥ | stats. log | 統計情報のログである。デフォルトの8s間隔から1h間隔に変更している。 |
| ⑦ | files-json. log | ファイルの送受信に関するログである。 |

筆者作成

タである。③から⑦のログデータは、必要に応じて参照し、発生したアラートの詳細な解析に利用する。

## 6．調査結果

### 6.1　概要

大阪商工会議所では2018年から2019年にかけての4ヶ月間、実証実験を行なった。これまでの調査は、アンケート、つまり自己申告による調査であり、必ずしも中小企業がサイバー攻撃自体の理解が十分ではなく、その攻撃や被害自体に気づいていないことも考えられ、必ずしもサイバー攻撃の実態を示すには十分ではなかったのである。この実証実験では、企業規模としては数人から数百人となる中小企業30社を、様々な業種に亘って選択し、その企業のネットワーク（パソコン）に出入りする情報（パケット）を調べ上げ、不正な通信が行われていないかを調査した。業種は飲食、製造、運輸、食品卸業等各種であった。その結果、ほぼ全ての企業が毎日のように、「ポートスキャン」という一種の脆弱性検査を始めとする各種のサイバー攻撃に晒されており、数社以上の企業が何らかの被害に及んでいるという結果が示された。

(1) 数社の被害は調査側が提示するまで気がつかなかった
(2) 被害を受けた数社はマルウェア対策ソフトを利用するパソコンに適用していた。少なくともパソコンに適用していると信じていた。
(3) スマホ等による不正の可能性が高い通信が確認された。
(4) パソコン以外の複合機（コピー、FAXマシン）の不正な通信が確認された。

本調査においては、企業のネットワーク（パソコン）とインターネットを介した外部との通信について調査しており、パソコンがマルウェアに感染しているか否かを決定づけることはできないが、通信状況からマルウェアに感染しているパソコンが存在している可能性が極めて高い。また不正な通信の多くが、悪性サイトと呼ばれる、マルウェアを感染させ、情報を不正に

取得しようとするサーバ群との通信である。さらに具体的にどのサイトと、例えば、どの国に登録されているサーバと通信しているかも調査している。30社の中には、自社及び取引先、並びにネットワークサービスを受けているネット関係会社と全く無関係な国との通信が大部分を占める企業もあり、明らかに正常とは言えない状況も見られた。

### 6.2　アラートログの分析

Suricataはオープンソースのネットワーク侵入検知システム（IDS）であり、公開されているルールセットを利用して、ネットワークトラフィックを監視し、悪性が疑われるイベントが発生したときに、アラートを出力するシステムである。ここでは対象とする中小企業がどのような攻撃にさらされているかを検証するために、複数企業で共通したアラートが検出された事例を分析する。疑いのあるサイバー攻撃の内訳は、大きく分類すると以下のとおりである。それぞれ複数の中小企業から検出されている。

①外部から社内の端末をリモート操作
（概要）A社等では、アラートの分析からラトビアから管理者権限でのパスワードアクセスを繰り返し、RDPに接続が成功している。
②社内端末と悪性サイトとの通信
（概要）B社等では、マルウェア等を配布する悪性サイトとの通信が確認されており、アラートからマルウェアをダウンロードしたと考えられる。
③DDoS攻撃を目的としたパケットを受信
（概要）C社等ではNTPのmonlist機能を用いたDDoS攻撃を受けており、通常のアクセスではありえない。

サイバー攻撃には様々な攻撃手法が存在するが、最も憂慮すべきは、パソコンを含むネットワーク機器やOS（基本ソフトウェア）、それに運用しているシステムの脆弱性に対する攻撃である。アラートログを分析した結果、複数企業に対して、下記の8種類の脆弱性やポートを狙って攻撃されている事例が存在した。

（ア）OpenSSLの脆弱性「HeartBleed」に関するアラート
（イ）リモートデスクトッププロトコル（RDP）に関するアラート
（ウ）ネットワークタイムプロトコル（NTP）を利用した攻撃のアラート
（エ）SSL3.0の脆弱性である「POODLE」に関するアラート
（オ）不正なファイルの送受信に関するアラート
（カ）Server Message Block（SMB）の脆弱性に関するアラート
（キ）Gh0st RATに関するアラート
（ク）エクスプロイトキットに関するアラート

利用された脆弱性は2014年に発見されたOpenSSL通信の脆弱性であるHeartBleedや同じく2014年に公開されたSSL3.0の脆弱性であるPOODLEなど、既に広く周知され対策が公開されているものも存在した。中小企業に対して大阪商工会議所が実施した、先のアンケート調査で判明した、セキュリティ人材不足やセキュリティ経費がかけられないなどの理由から多

くの中小企業では既知の脆弱性が放置されていると考えられる。（ア）～（ク）の各事例において、若干の補足を行う。

（ア）OpenSSLの脆弱性「HeartBleed」に関するアラート

OpenSSLとは、インターネット上で標準的に利用されている暗号通信のプロトコルであるSSL/TLSの機能を実装したオープンソースのライブラリである。インターネット上での通信は第三者が盗聴及び改ざんできないように、やり取りするデータを秘匿する技術が暗号化されており、これを実現するプロトコルがSSLである。2014年にOpenSSLを利用した通信で、接続状態を維持するための機能であるHeartBeatに脆弱性HeartBleed（CVE-2014-0160）が発見された。HeartBleedは外部からの要求に対して、必要以上にデータを送信してしまい、メモリ上にあるデータが漏洩してしまう脆弱性である。大量の要求を繰り返し実行することで、サーバの秘密鍵を始めとして、クレジットカード番号やユーザID及びパスワードなどの秘匿すべき情報を盗み出される可能性がある。OpenSSLを対策が施されたバージョンにアップすることで、この脆弱性を解決することができる。システムの都合により、すぐにバージョンアップできない場合は、HeartBeat機能を無効にして運用する方法もある。

（イ）リモートデスクトッププロトコル（RDP）に関するアラート

リモートデスクトップ接続を利用すると、ある端末から同じネットワークまたはインターネットに接続されている別の端末に接続することができる。リモートデスクトップ接続ためのプロトコルがRDPである。このプロトコルを利用するためにはユーザIDとパスワードが必要であるが、不正なユーザにID/パスワードを知られてしまうと、簡単に端末に接続されてしまう。端末に接続できれば、なりすまし、アカウントの不正利用、認証情報の収集やマルウェアの配布などを容易に実行できてしまうため、この機能を利用する場合は十分にセキュリティを確保する必要がある。確実なセキュリティ確保の方法は、接続させる端末のIPアドレスを許可制にし、事前に登録したIPアドレスからのみにリモート接続を許可することやローカルのIPアドレスのみを許可し、VPNを利用して安全な回線でローカルネットワークに接続した後にリモート接続することなどがある。固定のIPアドレスやVPN接続が必要であり、セキュリティを確保するために一定のコストが必要となる。RDPは3,389番ポートを利用している。つまり、RDPを利用している端末では3,389番ポートが開いている状態になっている。一方RDPを利用しない場合、3,389番ポートは閉じており通信することができない。攻撃者はまず、対象のIPアドレスのどのポートが開いているかを調べるポートスキャンを行い、RDPが利用されているかどうかを確かめる。3,389番ポートが開放されている場合、攻撃者はIDやパスワードを変えながらログインを試みる。

（ウ）ネットワークタイムプロトコル（NTP）を利用した攻撃のアラート

Network Time Protocol（NTP）は正確な現

在時刻を取得するためのプロトコルである。NTPのmonlist機能はサーバへのリクエストに対して、サイズの大きなデータを送信元IPアドレスへ返送する。攻撃者は攻撃対象の端末を送信元IPアドレスに偽装した問い合わせパケットをNTPサーバに送信することで、サイズの大きなデータを送信元に設定した端末にデータを送りつけることができる。これを利用して、複数のNTPサーバから攻撃対象にデータを送りつけて、大量の処理負荷を与えることでサービスを停止させるDDoS攻撃が行われる。また、脆弱性のあるNTPサーバを運用している場合、第三者を攻撃する際の踏み台として利用される場合もある。NTP Projectからmonlist機能を一部修正し、DDoS攻撃の影響を低減させたバージョンが公開されているため、NTPサーバを公開している場合は、修正済みのバージョン以降にアップデートしたほうが良い。

（エ）SSL3.0の脆弱性である「POODLE」に関するアラート

「POODLE（Padding Oracle On Downgraded Legacy Encryption）」とは通信の暗号化、認証、改ざん検知を行うSSL3.0に見つかった脆弱性（CVE-2014-3566）である。SSL3.0を利用する暗号化通信において、リクエストの送信を繰り返すことで、暗号化通信の一部を解読できる。また、SSL/TLSを用いた通信ではサーバとクライアントの双方のバージョンを合わせるために、どちらかが新しいバージョンのSSL/TLSに対応していない場合は、使用するバージョンを下げて接続を試みるという特徴がある。そのため、新しいバージョンを利用していたとしてもSSL3.0までバージョンを下げて攻撃を実行される危険性がある。Webサイト管理者はSSL3.0を無効にすることでこの脆弱性の利用を回避できる。また、エンドユーザもブラウザの設定により、TLS1.0以上のバージョンを利用するように変更できる。調査対象の一社では長期間に渡りアラートが検出していることから、SSL3.0を利用しているサーバと恒常的に通信している可能性が高いことが示された。

（オ）不正なファイルの送受信に関するアラート

マルウェアの感染経路は、Webサイトからのダウンロード、メールの添付ファイル、ファイル共有ソフト、USBメモリなどが多岐にわたる。マルウェアは.exeファイルや.dllファイルであることが多く、このアラートは別のファイルダウンロードに関するアラート「ET POLICY PE EXE or DLL Windows file download HTTP」とともに同じIPアドレスとの通信が継続している場合に、Webから悪性なファイルをダウンロードした可能性があるとして発生する。マルウェアのダウンロードを検知するためには、定期的にウイルスの定義ファイルを更新しスキャンを行う必要がある。

（カ）Server Message Block（SMB）の脆弱性に関するアラート

SMBはネットワークを通じてファイル共有やプリンタ共有を実現するプロトコルである。SMBにはEternalBlueという脆弱性があり、暗号化型ランサムウェア「WannaCry」で利用されたことでも知られている。SMBは445番ポートを利用しているため、ポートスキャンにより

445番ポートが開放されていることを確かめた後、マルウェアの共有する攻撃などに利用される恐れがある。本調査では、WannaCryによるアラートは発見されなかったが、別の脆弱性SMBLorisが利用された可能性を示すアラート「ET DOS SMBLoris NBSS Length Mem Exhaustion Attempt（PoC Based)」が検出された企業もある。SMBLorisを利用されると大量のメモリが消費され、攻撃にさらされている間はサーバ全体の負荷が高くなる被害が考えられる。

（キ）Gh0st RATに関するアラート

Gh0st RATは「remote administration tool（RAT)」として知られるバックドアの機能を持つマルウェアの一種で、マルウェアに感染した端末をコントロールするために利用される。キーの入力操作情報やオペレーティングシステム（OS）のバージョン、CPUの性能などのシステムに関連する情報などを収集し、Gh0st RATが管理するコマンド＆コントロール（C＆C）サーバに送信する。

（ク）エクスプロイトキットに関するアラート

エクスプロイトキット（EK）は、サイバー犯罪者がパソコンやデバイスの脆弱性を利用する際に利用するツールのことである。攻撃者はユーザにリンクをクリックさせエクスプロイトキットがホストされたWebサイトにリダイレクトさせ、そこでユーザのデバイスにインストールされたソフトウェアの脆弱性を確認する。さらに、確認された脆弱性を利用してデバイス上でエクスプロイトコードが実行され、不正プログラムがデバイス上で作成および実行される。

### 6.3　送受信先の通信に関して

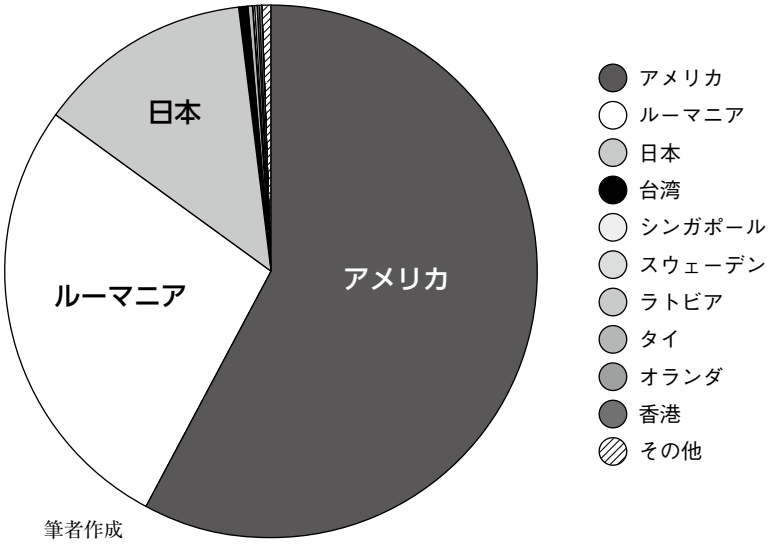
中小企業のネットワークにおいては主に取引先との通信、つまりパケットの送受信が中心となる。通常、ネットワークサービスに必要な通信を含めて、取引先以外との通信は不正な通信である可能性が高い。特に様々な調査等、検索によって正当なサービスとして広く認知されているWebサービスではない場合は顕著であろう。

例えば、中国のサイトとして登録されているIPアドレス122.228.***.***（*は伏字）から調査対象企業に通信が行われている。なお、上記のIPアドレスサイトは悪性サイト、つまりマルウェア等を配布するために使われる悪意を持ったサイトとして認定されている。さらに、このサイトからは、調査対象となった30社のうち、4社と通信を行っており、この4社については、業種も含めて、全く相互関係がない企業である。

調査対象30社については、送受信元IPアドレス毎、サービス（ポート番号）毎について、そのIPアドレスの詳細とともに、各社及びIPアドレスの時系列的な相関についても調査している。複数の企業において、悪性と判定されているIPアドレスとの通信が確認され、悪性と判定されなくとも、通信の必要性が認められない大量のIPアドレスとの通信が確認された企業も複数存在する。

例えばD社では（**図4**)、インバウンド通信（企業外から企業内への通信）はアメリカが約60％、ルーマニアが約25％、日本が約15％を占める。アウトバウンド通信（企業内から企業

（図4）観測数上位10か国の内訳




筆者作成

外への通信）は日本が約50%、アメリカが約25%、ルーマニアが約20%を占める。他の企業と比較して、ルーマニアと通信が多く見られている。H社では外部から社内のPCにアクセスし、リモートで操作を試みるための通信が検知されていた。

## 7．むすびにかえて

先にも述べたように、2017年度において、大阪商工会議所ではアンケート形式によって、大阪市内の中小企業に対するサイバー攻撃実態調査を行った。回答は事実上、サイバー攻撃に少なからず関心を有する企業群であって、その中でもサイバー攻撃を受けていると回答した企業が少なくなく、特にランサムウェアによる被害が7%に及んだことで、その実態が明らかになった。しかしながら目に見えるランサムウェア等の被害ではなく、目に見えないサイバー攻撃の被害、例えば情報流出やバックドア等の設置、あるいはBot等のリモート操作の被害については企業の自覚がないゆえに実数に現れないことが予想された。セキュリティ関連会社の技術者、有識者の知識、経験から、中小企業の少なくとも1割はすでにサイバー攻撃の被害、つまり不正アクセスに遭遇しているということが言われているものの、実際の調査事例はなく、その実態は不明のままであった。今回、過去に例を見ない、種々の業種での中小企業30社において、約4ヶ月という長期間、しかも各中小企業にセンサを設置し、出入りしているパケットを全て観測し、それぞれの中小企業に対するサイバー攻撃の現状だけでなく、不正アクセスの可否についても詳細に調査を行った。その結果、

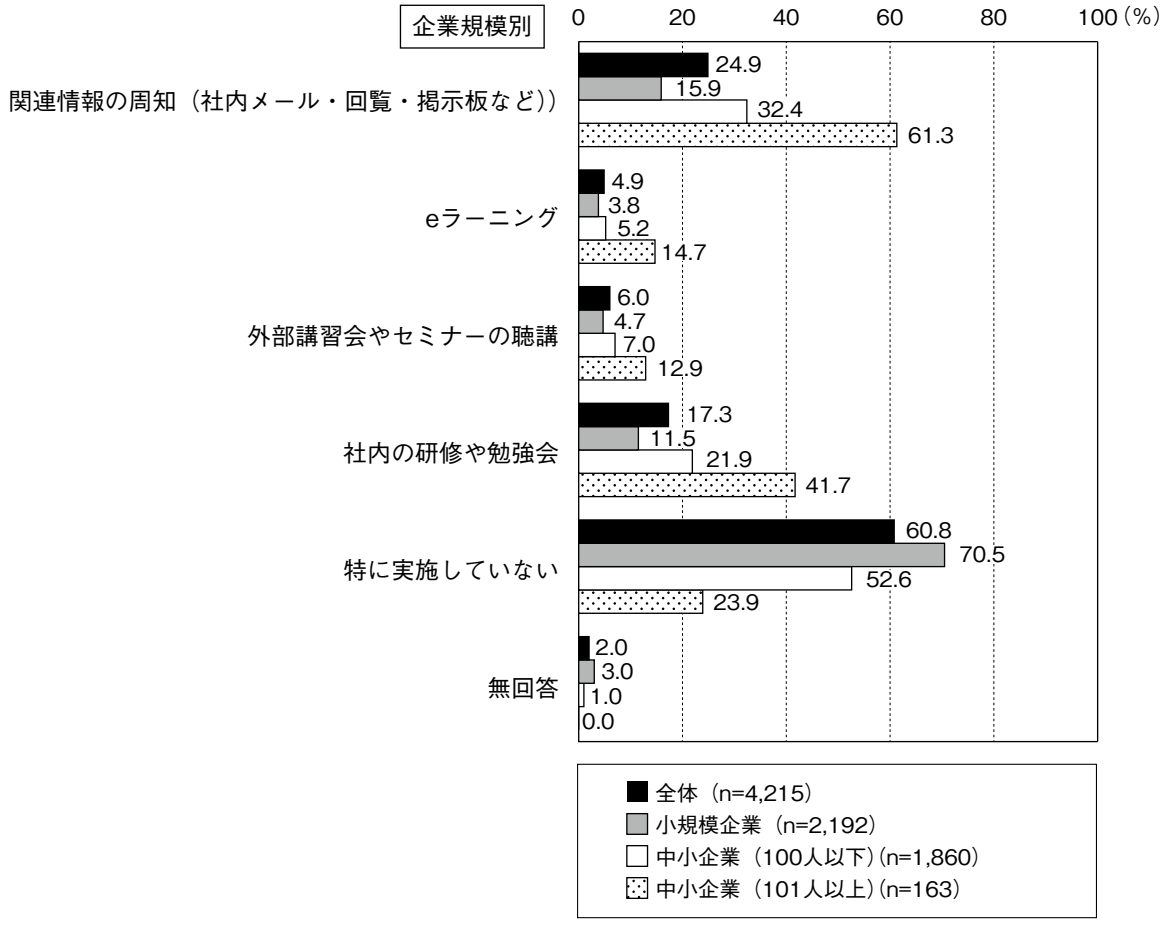
・外部から社内の端末をリモート操作
・社内端末と悪性サイトとの通信
・DDoS攻撃を目的としたパケットを受信した

とされる中小企業がそれぞれ複数存在することが明らかになった。外部からのリモート操作に関しては、海外からのアクセスであり、通常ではありえないアクセス手法を取っていることから、正常な企業活動とは程遠く、悪意のある端末（パソコン）操作であると考えられる。悪性

サイトとの通信に関しても、公に悪性と認定されているサイトであり、正常な企業活動としてアクセスすることはありえない。DDoS攻撃に関しても、それに全く気づかない状況である。また、その通信に関しては、ほとんど双方向の通信であり、社内情報が漏洩している可能性も捨てきれない。さらに攻撃としては、ポートスキャンやSSH等へのサービスへのパスワード試行といった攻撃だけではなく、OpenSSLの脆弱性「HeartBleed」を狙った攻撃や、SSL3.0の脆弱性「POODLE」を狙った攻撃、あるいはエクスプロイットキットというハッキングツールを利用した高度な攻撃手法も観測されている。決して中小企業がサイバー攻撃されていないわけではなく、それどころか高度な攻撃手法を用いての攻撃に常にさらされているのである。

大阪商工会議所の実証実験結果から言える、中小企業におけるセキュリティ対策の課題の第一はサイバー攻撃自体に気づいていない、さらに被害にも気づいていないということである。セキュリティ対策において、「マルウェア対策ソフトを導入する」、「OSを含めてソフトウェアのバージョンを常に最新にする」、「怪しい添付ファイルを開かない、怪しいサイトにアクセスしない」等が要求されているものの、本実証実験の30社全てが、これらの対策を行なってい

**（図5）情報セキュリティ教育（企業規模別）**




（出所）「2016年度中小企業における情報セキュリティ対策の実態調査報告書」（2017年6月）

たと回答している。対策を行なっていることと、それを確実に実行していることとは別なのである。この30社ではないが、いくつかの中小企業に調査に入った際に、経営者や管理者がマルウェア対策ソフトを導入していると回答したものの、実際に調べた結果、パソコンの操作者が過負荷を理由にマルウェア対策ソフトを止め、あるいは使用期限が切れていたまま利用していたこともあった。

今回の30社における実証実験で被害に在っていると推測される数社のパソコンがマルウェアに感染している可能性が高いことを述べた。その感染経路については推し量るべくもないが、おそらくメールの添付ファイルやマルウェアをダウンロードさせるサイトのURLをクリックしたことが原因であろう。いわゆる無差別に送られるタイプを含めた標的型メール攻撃によるものである。標的型メール攻撃を完全に排除することは非常に難しい。昨今、標的型メール攻撃による被害が深刻化することとなって、その練習（演習）が中小企業でも勧められている。定期的に企業の管理者が標的型メールを模した練習用のメールを従業員に投げて、それに騙された人に対して注意を喚起する演習である。しかし、この演習を行なっているからといって、標的型メール攻撃に対して完璧な対策を行なっていることにはならない。たった一人が一度でもこの攻撃に欺かれてマルウェアに感染すれば、そのパソコンを起点に次々と他のパソコンが感染し、しかも誰も気づかないのである。

結局のところ、中小企業にとって、現実的に可能でかつ、実効力のある対策は経営層を含む従業員全体のセキュリティ意識を高めることはもちろん、サイバー攻撃と見えない被害の正しい認識なのである。

IPAの調査結果からもわかるように、規模が小さな中小企業ほど従業員の教育と呼べるほどの従業員対策、利用者対策を怠っている（**図5**）。たとえ管理者が細心の注意と可能な限りの対策を行なったとしても、利用者である従業員が、それに従わない、あるいは反する行為を無意識に行うことで、セキュリティ対策は水泡に帰するのである。さらに規模が小さな中小企業になればなるほど、高度なファイヤーウオールやUTM（統合脅威管理システム）の設置、SOC（セキュリティオペレーションセンター）といったネットワーク管理の外部委託という物理的対策はもちろん、管理者を置くこと自体も難しい。その二重苦、三重苦が中小企業のセキュリティ対策の足を引っ張るのである。

**【参考資料】**


○（独）情報処理推進機構（2017）『2016 年度中小企業における情報セキュリティ対策の実態調査報告書』
https://www.ipa.go.jp/files/000058502.pdf
○大阪商工会議所（2017）『中小企業におけるサイバー攻撃対策に関するアンケート調査結果』
http://www.osaka.cci.or.jp/Chousa_Kenkyuu_Iken/Iken_Youbou/k290630cyb_ank.pdf
○大阪商工会議所（2019）『サプライチェーンにおける取引先のサイバーセキュリティ対策等に関する調査』
http://www.osaka.cci.or.jp/Chousa_Kenkyuu_Iken/press/190510sc.pdf
○大阪商工会議所（2019）『中小企業に対するサイバー攻撃実情調査報告』
http://www.osaka.cci.or.jp/Chousa_Kenkyuu_Iken/press/20190703cyber_h30.pdf