レベル 1_#1_企業の安定と発展のために活用しよう！　中小企業が活用できる ICT 関連の補助金・助成金には何がある？
掲載日：2024/7/1



photo AC「写真素材：黒板に補助金の文字」
https://www.photo-ac.com/main/detail/26759363

昨年、友人が起業しました。
10 数年間の会社勤めを経て、人脈もでき、顧客の目途もついてからの独立で、勤務していた企業ともパートナーシップ契約を結んでいます。
幸い事業は順調ですが、それでもサラリーマン時代とは違う心配があるようです。

一番の不安は、毎月滞りなく社員に給与を支払い、外注費を確保できるか、ということ。
たとえ多くの注文をいただいたとしても、その売上金がすぐに入ってくるわけではありませんし、場合によってはあてにしていた収入が予定通りに入ってこない可能性もあります。

彼の場合は起業後間もなくということもあり、極端な例だとは思いますが、中小企業の経営者は多かれ少なかれ、そのようなストレスを抱えていらっしゃるのではないでしょうか。

そのような状況で、必要な事業活動に安心して取り組むための助けとなるのが、国や東京都の補助金制度や助成金制度の活用です。

現在活用できる制度にはどのようなものがあるのでしょうか。

本記事では、補助金・助成金制度の活用に役立つ情報を提供します。

ICT の活用と補助金・助成金制度の活用

友人は現在、事業のさまざまな課題を解決するために、ICT（情報通信技術）関連の助成金制度の活用を検討しています。
それはなぜでしょうか。

ICT の活用は、ビジネスの成長と競争力を加速させるからです。
出所）公益財団法人 日本電信電話ユーザ協会「ICT で小規模ビジネスにイノベーションを！　コスト削減から効率化まで、中小企業の課題解決」
https://www.jtua.or.jp/feature/ict/

出所）総務省「平成 28 年版情報通信白書 第 1 部」p.7
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h28/pdf/n1100000.pdf

ICT を導入すれば、業務の効率化やコスト削減、顧客サービスの向上が図れます。
業務の効率化は企業活動の生産性を高めるため、人手不足の解消にもなりますし、労働力に余裕ができれば、社員をより生産性の高い業務に集中させることもできます。

たとえば、後ほどご紹介する「IT 導入補助金」の活用事例として、「働き方改革をめざして、タイムカードと給与管理システムを連動させた勤怠管理ツールを導入した」「補助金を活用し、これまで紙で管理していた業務日記等を IT ツールで管理することにした」などが挙げられています。
出所）経産省 ミラサポ plus「IT 補助金とは」
https://mirasapo-plus.go.jp/subsidy/ithojo/

その成果は、業務の効率化と正確性の向上です。
導入した勤怠管理ツールを活用して社内規定を見直したところ、社員のモチベーションが高まるという副次的な効果もあったそうです。

また、「勘に頼った経営を改めるために、補助金を活用して販売管理システムを導入したところ、得意先の需要予測や仕入れ単価の推移が明確に把握できるようになり、売上が増加した」という導入例も挙げられています。

このように、ICT の活用は、単なるツールの導入に留まらず、事業を活性化することにつながります。

では、そうした取り組みに活用できる制度にはどのようなものがあるのでしょうか。

補助金・助成金制度とは

ここでは、補助金・助成金とはそもそもどのような制度なのか、注意点もあわせてみていきましょう。

特徴

まず、特徴を押さえましょう。
補助金と助成金は、どちらも国や地方公共団体から支給されるお金です。
出所）J-Net21「補助金・助成金の違いや補助金活用における注意点について教えてください。」
https://j-net21.smrj.go.jp/qa/financial/Q1339.html

民間の団体が支給する場合もありますが、多くの財源は公的な資金から出されるものなので、誰でももらえるわけではありません。
普通は申請や審査が必要で、一定の資格が求められる場合もあります。

また、補助金も助成金も、受けようと思うと事務処理が増えたり、時間的な制約がついたりして、手間暇がかかることがありますので、あらかじめそのことを理解しておく必要があります。

私の友人も、繁忙期に助成金制度を活用しようとしたことがあったのですが、そのための手続きに使える余力がなく、時期をずらして申請することを考えています。

補助金・助成金の留意点

次に、補助金・助成金の留意点をみていきましょう。

1）提出書類でのアピール

1 か月程度の公募期間を設けるのが一般的で、この期間内に所定の書類を揃えて申請する必要があります。

申請する場合には、こうした事務作業を通常業務と並行して短期集中的に進めることになりますので、定期的に募集があるような補助金・助成金であれば、あらかじめ計画を立てて業務の調整をしておけば安心でしょう。

多くの場合、採択件数より応募件数が上回ります。たとえば採択予定件数 10 社に対して申請が 30 社あれば、20 社は審査で落ちてしまうことになります。

したがって、採択してもらうためには、提出書類でその妥当性や必要性をアピールすることが大切です。補助金の申請に関しては、提出書類の内容が大変、重要だということを押さえておきましょう。

2）後払い制

多くの場合は後払い制で、すぐにお金を受け取ることができるわけではありません。
したがって、まずは申請した事業総額と同額の資金を用意する必要があります。

たとえば総額 300 万円の事業で 1/3 の補助がある場合でも、すぐに助成金の 100 万円が受け取れるわけではなく、自社のお金で一旦 300 万円を支出する必要があります。

先に出るものと勘違いして、200 万円だけ用意して残りの 100 万円を用意しなければ事業を進めることはできず、かえって大変な状況に陥ってしまいますから、注意が必要です。

3）支出する時期

事業期間を定めるのが一般的で、この事業期間に支出した経費以外は経費として認められず、補助を受けられないこともあります。

たとえば、事業期間が 8 月 1 日～2 月 28 日までだとしたら、7 月 31 日に支出したものも 3 月 1 日に支出したものも補助を受けられない可能性が高いのです。
事業期間内に申請した事業活動がおさまるように、留意しましょう。

また、事業期間は年度末ではなく少し早めに設定されているケースが多いので、注意が必要です。

4）助成金の額の決め方

助成金の金額は、下の図 1 のように決められます。
一見煩雑のように見受けられますが、順を追って計算していけば、受け取れる金額が把握でき、申請を検討する際の参考になります。

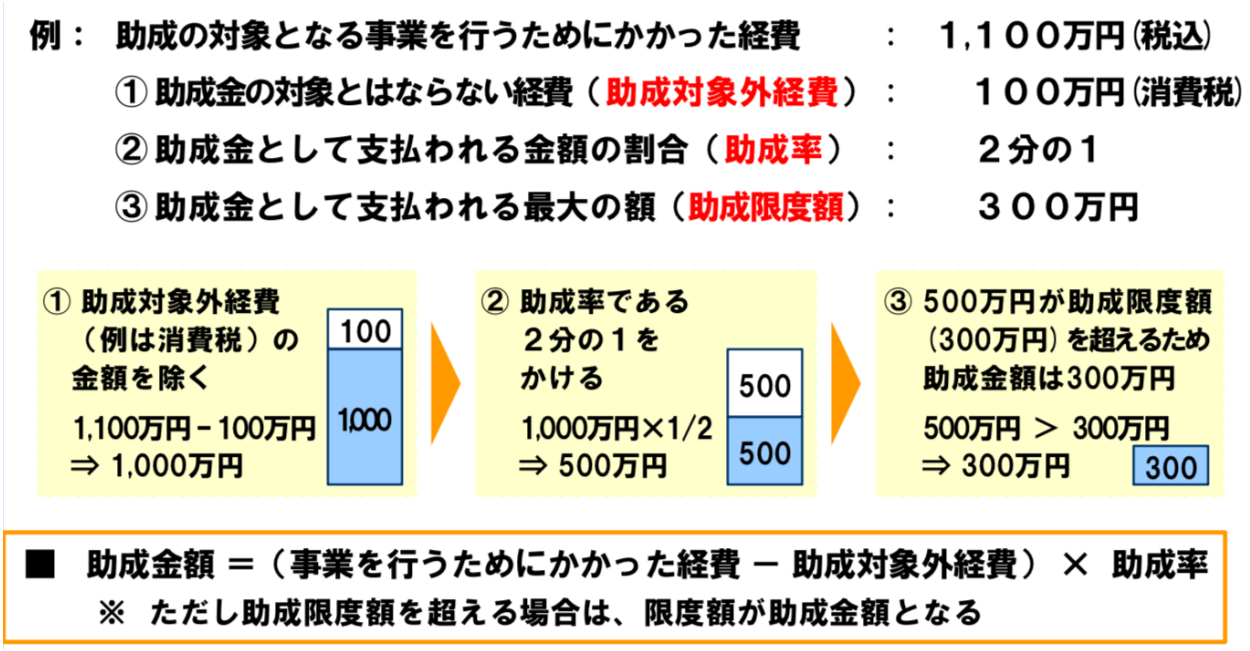


図 1　助成金の金額の決め方

出所）東京都中小企業振興公社「助成金を申し込む前に必ずお読み下さい！！」p.1

https://www.tokyo-kosha.or.jp/support/josei/qp64520000001995-

att/Precautions_Joseikin-Chuiten.pdf

計算式は、図 1 の下にあります。
例えば、助成の対象事業を行うためにかかった経費が税込み 1,100 万円で、そのうち助成の対象にならない経費が 100 万円、助成率が 2 分の 1、助成限度額が 300 万円の場合、以下のように計算します。

① 経費 1100 万円から助成対象外経費の 100 万円（消費税）を引く ⇒ 1,000 万円
② ①に助成率の 2 分の 1 をかける ⇒ 500 万円
③ ②が助成限度額 300 万円を超えるため、助成金額は限度額の 300 万円になる

こうしてあらかじめ概算しておけば、申請するかどうかを検討する際の有益な判断材料になるでしょう。

5）助成金が支払われるまでの基本的な流れ

助成金の申請から支払いまでの流れは、下の図 2 のとおりです。

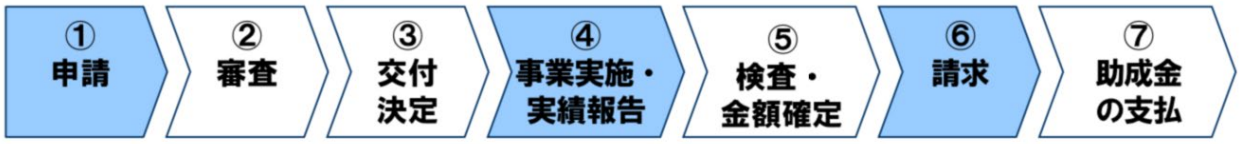


図 2　申請から助成金支払いまでの流れ
出所）東京都中小企業振興公社「助成金を申し込む前に必ずお読み下さい！！」p.1
https://www.tokyo-kosha.or.jp/support/josei/qp64520000001995-att/Precautions_Joseikin-Chuiten.pdf

6）申請の際の確認事項

申請の際には、以下について確認しましょう。

① 申し込む事業の内容が助成金の目的と合っているか
② 助成対象期間に、事業の発注・契約・実施（購入）・支払い（決済）のすべてを行うことが可能か（図 3）

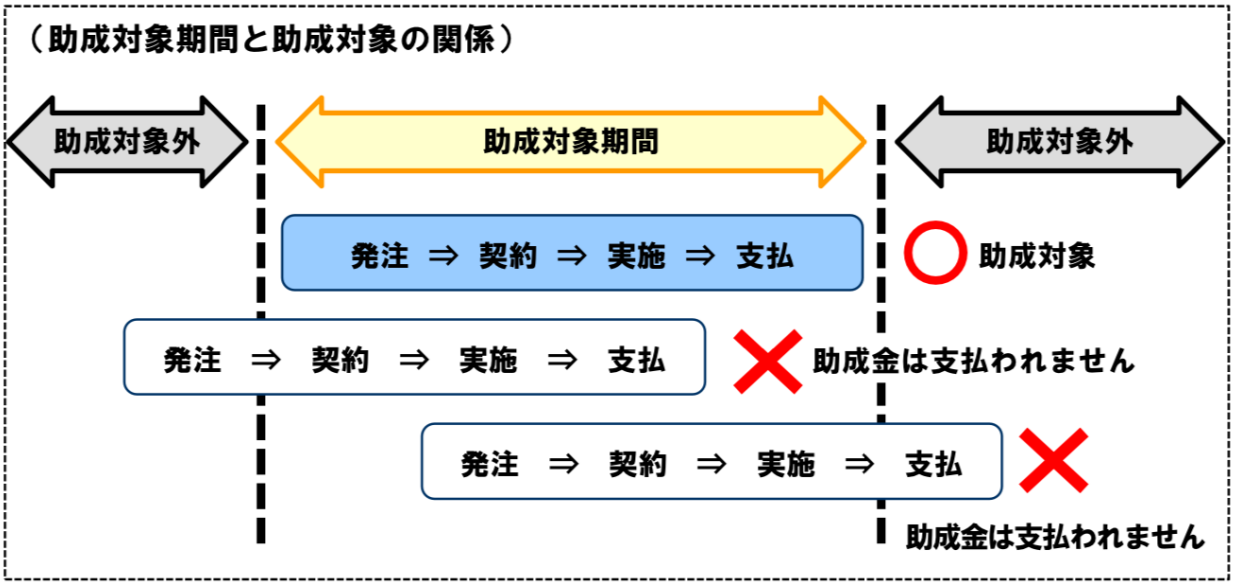


図３　助成対象期間に行うべきこと

出所）東京都中小企業振興公社「助成金を申し込む前に必ずお読み下さい！！」p.2

https://www.tokyo-kosha.or.jp/support/josei/qp64520000001995-att/Precautions_Joseikin-Chuiten.pdf

③　募集要項の「審査の視点」（審査基準）と合っているか

④　必要最小限の経費になっているか

詳しいことは、各助成金の募集要項に記載された連絡先に問い合わせ、慎重に検討しましょう。

7）事務処理

事業期間終了後、一定期間内に報告書や支払証憑類を提出する必要があります。

この提出書類がいい加減だったり、目的外に経費を支出したりしていた場合などは、支払いが拒否されることがあります。

どの経費に対する支出なら認められるのかきちんと確認し、的確な事務処理をしましょう。

8）会計検査院の検査が入る可能性

国からの補助金を受けた企業は、会計検査院の検査を受ける可能性があります。

その際、不備を指摘されないように、正当な目的のためにだけに費用を支出することが必要です。

IT 導入補助金

ここでは、中小企業が活用できる ICT 関係の補助金をご紹介します。

経済産業省は「中小企業向け補助金・総合支援サイト　ミラサポ plus」を開設しています。
このウェブサイトでは、中小企業が活用できる補助金に関するさまざまな情報が得られます。

中小企業向け補助金・総合支援サイト　ミラサポ plus

そのなかに、IT サービスを活用したい事業者向けの「IT 導入補助金」があります。

目的・対象ツール・パートナーシップ

この補助金は、日々の業務の効率化や自動化のための IT ツールの導入をサポートします。
活用事例とその成果は先ほどご紹介したとおりです。
出所）経産省 ミラサポ plus「人気の補助金＞IT 導入補助金」
https://mirasapo-plus.go.jp/subsidy/

ソフトウェアやサービスなど対象となる　IT　ツールは事前に事務局の審査を受け、補助金のホームページに公開されているものです。
出所）IT 導入補助金 2024「IT 導入補助金とは」
https://it-shien.smrj.go.jp/about/

相談対応などのサポート費用やクラウドサービス利用料なども補助対象となります。

補助金を申請する中小企業・小規模事業者は、IT 導入補助金事務局に登録された「IT 導入事業者」とパートナーシップを組んで申請することが必要です。

申請・手続きのフロー

下の図４は、申請と手続きのフローです。



図４　IT 導入補助金の申請・手続きフロー
出所）IT 導入補助金 2024「新規申請・手続きフロー（中小企業・小規模事業者等のみなさまの手続き）」
https://it-shien.smrj.go.jp/applicant/flow/

「IT 導入補助金 2024」の交付規程・公募要領

「IT 導入補助金 2024」には、通常枠、インボイス対応類型、電子取引類型、セキュリティ対策推進枠、複数社連携 IT 導入枠という種類があります。

それぞれの交付規程、公募要領、交付申請の手引きは、以下からダウンロードできます。

IT 導入補助金 2024「資料ダウンロード」

東京都の助成金

公益財団法人東京都中小企業振興公社はウェブサイト「助成金事業」で、東京都の「助成金一覧」、「目的別助成金」、「令和 6 年度助成金事業」など助成金に関するさまざまな情報を提供しています。

[東京都中小企業振興公社「助成金事業」]

たとえば、目的別助成金の「サービス」や「生産性向上」には、ICT 関係の助成金が複数、掲載されています。

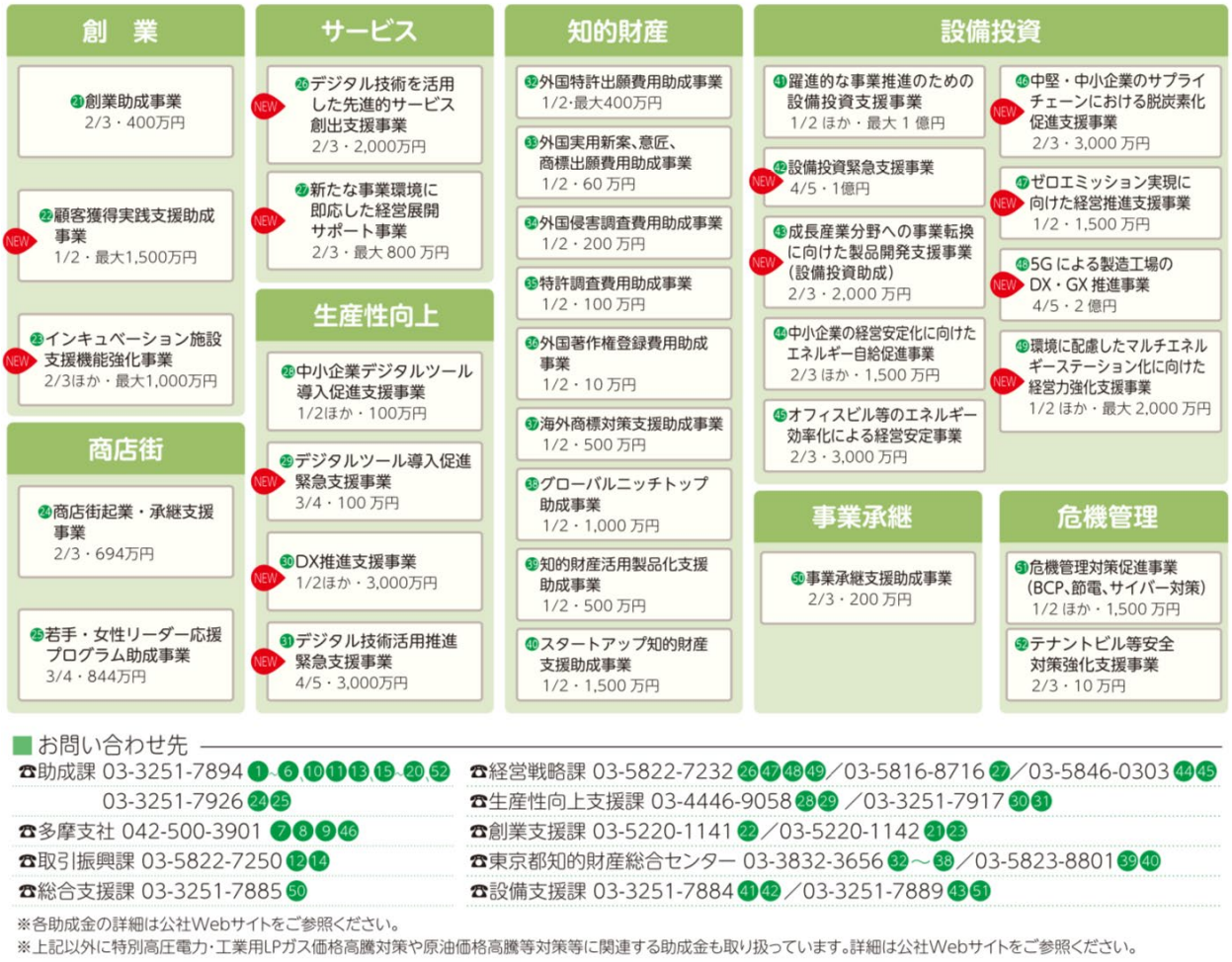


図 5　東京都の目的別助成金
公益財団法人東京都中小企業振興公社「目的別」p.1
https://www.tokyo-kosha.or.jp/support/josei/h7v93t0000004ieh-att/r6_mokutekibetsu_1.pdf

それぞれの問い合わせ先も載っていますので、気になる助成金があったら、問い合わせてみてはいかがでしょう

か。

経営全般に関する相談や、どこに相談したらいいかわからない場合には、「ワンストップ相談窓口」で相談することもできます。

ワンストップ相談窓口

また、同サイトの「採択企業一覧」には、各助成金ごとに、昨年度までの採択企業名が記載されています。助成の種類によっては、企業名だけでなく、所在地や申請テーマも公表されており、申請を検討する際のヒントが得られるかもしれません。

東京都の助成金 採択企業一覧

たとえば以下は、「令和 5 年度 TOKYO 戦略的イノベーション促進事業　採択企業一覧」のリンクです。

令和 5 年度 TOKYO 戦略的イノベーション促進事業　採択企業一覧

おわりに

企業変革をもたらす ICT の導入・活用は、中小企業にとって急務といっていいでしょう。
中小企業向け助成金・補助金は、それを支えるための有益な制度です。

事業の成長と安定のために活用を検討してみてはいかがでしょうか。

筆者プロフィール

＜横内美保子＞

博士（文学）。総合政策学部などで准教授、教授を歴任。専門は日本語学、日本語教育。

高等教育の他、文部科学省、外務省、厚生労働省などのプログラムに関わり、日本語教師育成、教材開発、リカレント教育、外国人就労支援、ボランティアのサポートなどに携わる。

パラレルワーカーとして、ウェブライター、編集者、ディレクターとしても働いている。

X：よこうちみほこ

Facebook：よこうちみほこ

レベル 1_#2_仕事のストレスを乗り越えるために：中小企業経営者と実務担当者へのアドバイス

掲載日：2024/7/23



Photo AC「ハートのオブジェクトを持つビジネスマン」

https://www.photo-ac.com/main/detail/27783257

筆者は保健所で医師として勤務していた際、新型コロナウイルス感染症の流行を経験しています。

想像に難くないかとは思いますが、当時、かなりのストレスにさらされました。

当時は医師兼係長クラスの立場にあったため、他の職員の仕事をどのように割り振るかについても決めていく立場にあり、とても責任の重い仕事です。

未知の感染症が流行し始めた当初はとにかく手探りの状態で、まさにカオスです。

しかし、仕事への責任感や義務感もあり、自分自身で自分のストレスになかなか気づくことができませんでした。

そしてその経験から、気がついたことがあります。

「大企業に比べ、中小企業経営者や実務担当者のストレスは、あまりにも過小評価されているのではないか」

そこでこの記事では、筆者の経験も踏まえ経営者や管理者の方に向け、ストレスコントロールの考え方について医師の立場から助言をしたいと思います。
ぜひ、日々の経営はもちろん、ご自身のストレスとの向き合い方や、それらを乗り越えるための知恵としてお役立て下さい。

１．経営者のストレスと軽視されがちな問題点

中小企業は、日本の企業数の 99.7%を占めており、全雇用者数の 70%以上を支えています。
第 5 期科学技術基本計画に関する経済団体からの提言　日本商工会議所　p2
https://www8.cao.go.jp/cstp/siryo/haihui013/sanko3_2.pdf

にもかかわらず、これら企業の経営者が日々直面するストレスは、社会全体において十分に認識されていません。

経営者のストレスは、しばしば軽視されがちですが、実際には組織の運営において極めて重要な問題です。
特に中小企業では、大企業に比べてサポート人員が不足しているため、経営者の心理的負担が大きいでしょう。
さらに、経営者のメンタルヘルスに対する偏見もあり、悩みを持ちながらも支援を求めずに我慢する傾向があると指摘されています。
中小企業における経営者と管理職の行動特性,職場ストレッサーとメンタルヘルスとの関連-共分散構造分析による比較検討-.ストレス科学研究 Advance Publication p2
https://www.jstage.jst.go.jp/article/stresskagakukenkyu/advpub/0/advpub_2019002/_pdf/-char/ja

さらに、以下のような要因によって、経営者にストレスがかかる可能性があります。

意思決定のプレッシャー

経営者は日々の運営だけでなく、会社の長期的な戦略を決定する役割を担っています。
このため、大きなプレッシャーの中で複雑な意思決定を迫られることが多く、ストレスが蓄積しやすいのです。

責任の重さ

従業員やその家族、さらには会社に関わる利害関係者などの生活は経営者の判断に依存しています。
このため、経営者に重大な責任感がのしかかり、経営者にとって大きなストレス源となります。
繁忙期など、社員の心身にストレスが掛かるような場面ではなおさらでしょう。
そしてそのような時こそ経営者は、自分自身にも大きなストレスが掛かっていることを認識しなければなりません。

孤独感がある

経営者は、その仕事の性質上、しばしば「孤独な立場」にあります。
群馬県の中小企業の経営者に対して行われた調査では、従業員との関係において「経営者は結局、孤独である」や、「従業員に自分の弱気な面は見せられない」といった回答がみられました。
平成 19 年度調査研究タイトル「中小事業所の経営者におけるメンタルヘルスの意識調査」群馬産業保健総合支援センター
https://www.gunmas.johas.go.jp/health/research2007/

彼らは従業員に対して強い姿を見せる必要があるため、自らの悩みやストレスを共有することが難しい場合があるのでしょう。

経営者のストレスを軽減するためには、個人が自己管理を行うだけでなく、組織としてもサポート体制を整えることが求められます。
例えば、専門のカウンセラーやコーチと定期的なセッションを設ける、または経営者専門のリトリートやワークショップを利用することで、経営者がストレスを効果的に管理できる環境を提供するとよいでしょう。

２．中小企業の経営者におけるストレスの影響

中小企業の経営者は、特有の環境とプレッシャーのため、ストレスが多岐にわたる影響を及ぼすことがあります。
以下に、主なストレスの影響について解説していきましょう。

メンタルヘルスの不調

ストレスはうつ病や不安障害などの心理的な問題を引き起こすことがあります。

ストレスがかかる状態が長く続くと、活気が低下し、元気がなくなってしまいます。
また、イライラや不安感にも襲われるようになります。
集中力の低下や決断が困難になるといった、仕事に直接影響がでる恐れのある症状も現れるようになります。
最終的には、うつの状態に近づいてしまうこともあります。

筆者自身はコロナ対応の際、どちらかというと怒りっぽくなったり、いつも楽しめる趣味を楽しめなくなるということがありました。
メンタルヘルス対策として、カウンセラーの方との対話を経て多少は心が楽になったものです。
同様に、企業でリーダーの立場にある人こそ、多忙の際には積極的に専門家を頼ることを検討して下さい。

ストレス関連疾患（心身症）

長期間の高ストレス状態は、メンタルヘルス面のみならず、体の不調をきたすことがあります。
ストレスに関連していると考えられている病気のことを、心身症（しんしんしょう）といいます。
この心身症には、気管支喘息や高血圧、冠動脈疾患、さらに糖尿病など、さまざまなものがあります。
こころの耳　厚生労働省　ストレス軽減ノウハウ　2 ストレスからくる病
https://kokoro.mhlw.go.jp/nowhow/nh002/

組織への影響

経営者のストレスは直接的に従業員の士気や生産性に影響を与えることがあります。
また、経営者がストレスにより適切な判断ができない場合、組織全体の戦略的な誤りが生じたりするおそれもあります。
経営者の精神状態は会社の業績に大きな影響を及ぼす、という点も指摘されています。
中小企業経営者のメンタルヘルスの現状　p36
https://www.jstage.jst.go.jp/article/sfjg/33/0/33_28/_pdf
実際に、経営者や管理職の元気がないと、部下であるその他の職員たちもやる気が出しづらいということはあるでしょう。

これらの影響は、経営者が直面するストレスを理解し、適切に管理することの重要性を浮き彫りにしています。

ストレス管理の取り組みは、個人の健康だけでなく、組織の成功にも直結するため、経営者自身だけでなく、企業が積極的にサポートすることが望ましいですね。

３．ストレスの原因

ここまで、経営者の過度なストレスによる問題について解説してきました。
それでは、次に中小企業の経営者のストレス源について考えられるものをご紹介していきます。

経済的プレッシャー

経営者は企業の財務状態を常に監視し、資金調達、予算管理、売上目標の達成など、経済的なプレッシャーに常に直面しています。
特に不況期や市場の変動が大きい時期には、この種のストレスはさらに高まるでしょう。

高い責任感と意思決定のプレッシャー

経営者は企業全体の方向性と成功を左右する重要な意思決定を行う必要があります。
この大きな責任感と、日々の意思決定が及ぼす圧力は、経営者に著しいストレスを与えます。
失敗のリスクとその結果に直面することが、持続的な心理的負担となることが予想されます。

職場の対人関係

経営者は従業員、顧客、投資家などとの関係を管理する必要があります。
これらの関係の中で生じる対人ストレスや、期待の管理、職員どうしの対立の解決などが経営者のストレスを増加させる要因となります。

４．個人レベルでのストレス対策

さて、ここからはストレス対策について紹介していきます。
個人的な戦略は以下のように多岐にわたります。

質の良い睡眠をとる

良好な睡眠をとることで、ストレスフルな状況下におかれてもメンタルヘルス不調を予防できるとされています。

睡眠の質を高めるためには、定期的な運動、バランスの取れた食事などが大切です。
また、就寝前の食事や飲酒、喫煙、スマートフォンの使用は控えましょう。
良い目覚めは良い眠りから　知っているようで知らない睡眠のこと　厚生労働省
https://e-kennet.mhlw.go.jp/wp/wp-content/themes/targis_mhlw/pdf/leaf-sleep.pdf?1717511968130

とはいえ筆者自身も、忙しい時期にまとまった睡眠時間の確保などできません。
休日には早く就寝し、なるべく早めに起きるといった生活リズムを整えることで、できる限りの健康管理を意識して下さい。

ストレス管理のスキル向上

マインドフルネスや瞑想など、ストレスを軽減するためのテクニックを学び、日常生活に取り入れることが効果的です。
なお、マインドフルネスとは、自分の経験に耳を傾け、今、この瞬間に起こっていることに集中することです。
こうした技術を習得することで、感情のコントロールが向上し、ストレスに対する対処能力が高まる効果が期待できます。
厚生労働省 eJIM | 瞑想［各種施術・療法 - 医療者］
https://www.ejim.ncgg.go.jp/pro/overseas/c02/07.html
筆者自身も、寝る前のヨガなどで心身のリラックスをはかることで、コロナ禍の対応を乗り切ることができたと感じています。
大事なことは、ストレスをいったん心から切り離す時間を確保することです。

５．組織レベルでの対策

次に、組織としてのアプローチについて述べていきます。

職場環境の改善

快適で健康的な職場環境を提供することで、従業員のストレスが軽減されます。
例えば、自然光の多いオフィスや適度なプライバシーが保たれた作業スペースの設計は、心理的な圧力を減らすのに有効です。
職場環境におけるウェルビーイング.サービソロジー.2019;5(4):10-15.p13

https://www.jstage.jst.go.jp/article/serviceology/5/4/5_10/_pdf/-char/ja

メンタルヘルス支援プログラムの導入

定期的な健康診断、カウンセリングサービス、ストレス管理のワークショップの提供などによって、従業員のウェルビーイングをサポートしていきます。
これにより、職場全体の生産性向上にも寄与できるでしょう。
また、経営者が自身のストレスレベルを定期的にチェックするための自己評価ツールを導入することもお勧めします。

６．国の取り組みについて紹介

経済産業省は、中小企業の経営者の健康を支援するために、『健康経営優良法人認定制度』を推進しています。
健康経営優良法人認定制度（METI/経済産業省）
https://www.meti.go.jp/policy/mono_info_service/healthcare/kenkoukeiei_yuryouhouzin.html

この制度は、職場での健康管理を効果的に行う企業を公認し、メンタルヘルス対策の重要性を高めるものです。
具体的には、定期的な健康診断の促進やストレスチェックの実施、そしてそれに基づく改善策の提案などが行われています。

７．まとめ

中小企業の経営者や実務担当者は、個人としても組織としても、積極的にストレス管理を行うことが求められます。
ストレスは避けられない要素ですが、適切な対策を講じることで、その影響を大幅に軽減することが可能です。
とはいえ、どんな職種でも多忙な時期というものはあるでしょう。
そういった時に、ある程度のストレスがかかることは、避けられるものではありません。

大事なことは、自分の心身の状況が今どんな状態にあるかを客観視し、時に医師やカウンセラーの力を借りることを迷わないということです。

今回の記事が、中小企業の経営者や実務担当者が自らのストレスを効果的に管理し、健康な職場環境を維持するための一助となれば幸いです。
実際に役立つストレス管理のテクニックや、組織としてのサポート体制の整備について、さらに知りたい方は、専門のセミナーやワークショップへの参加を検討してみましょう。

【筆者】
・名前：木村香菜（きむらかな）
・プロフィール：行政機関である保健センターで、感染症対策等主査として勤務した経験があり新型コロナウイルス感染症にも対応した。現在は、主に健診クリニックで、人間ドックや健康診断の診察や説明、生活習慣指導を担当している。また放射線治療医として、がん治療にも携わっている。放射線治療専門医、日本医師会認定産業医。

【経歴】
名古屋大学医学部卒業。初期臨床研修修了後、大学病院や、がんセンターなどで放射線科一般・治療分野で勤務。その後、行政機関で、感染症対策等主査としても勤務。その際には、新型コロナウイルス感染症にも対応。現在は、主に健診クリニックで、人間ドックや健康診断の診察や説明、生活習慣指導を担当している。また放射線治療医として、がん治療にも携わっている。放射線治療専門医、日本医師会認定産業医。

レベル 1_#3_売上アップの秘訣は新一万円札にあり？　渋沢栄一の理念が示すものとは

掲載日：2024/7/30



photo AC「写真素材：上昇グラフとビジネスマン」
https://www.photo-ac.com/main/detail/29329722

どうしたら売上を伸ばすことができるのか。
それは経営者の永遠のテーマかもしれません。

中小企業経営者の課題解決をサポートする「J-Net21」には、「売上アップの取り組み事例集」が掲載されています。
その事例で印象的なのが、顧客へのホスピタリティや従業員を大切にする取り組みです。

そこで思い浮かぶのが、新一万円札の「顔」となった渋沢栄一。「近代日本経済の父」と呼ばれる渋沢は、道徳と経済は表裏一体だと説き、公益を忘れ私利私欲に走る実業家を強く戒めました。

新一万円札は今、私たちにどのようなメッセージを伝えようとしているのでしょうか。

「売上アップの取り組み事例」と渋沢栄一の理念をあわせてみていきましょう。



図１　新一万円札

出所）国立印刷局「新しい日本銀行券特設サイト＞2024 年 7 月 3 日お札が変わりました」

https://www.npb.go.jp/ja/n_banknote/index.html

売上アップの取り組み事例

経済産業省が管轄する、中小企業基盤整備機構のウェブサイト「J-Net21」には、「売上アップの取り組み事例集」が公表されています。

その中から、都内商店街に立地する小さなスーパーの成功事例をご紹介します。

会社を支えるパート社員の処遇改革

小規模なスーパーは、品揃えや駐車場などのサービスでは大手スーパーにかないません。

では、大型スーパーと勝負できるのは？

それはホスピタリティーに溢れたフレンドリーなサービスです。

このスーパーでは、そのために生鮮食品の鮮度アップなどに力を入れるようになりましたが、そのことで社員の負担が大きくなり、パートタイマー社員（以下、「パート」）の担当する分野が拡がっていきました。

ところが、パートがどのような業務を担当するか明示されておらず、パートの評価制度もありませんでした。
賃金も入店時のままで、定期的な昇給もなし。パートの報酬や処遇は仕事の質や能力に関係なく、どんな仕事をどんなふうにやっても、時給は同じという状況です。

勤務する店舗や会社のためにどれほどがんばって働いても、パートはそのことを評価してもらうことも、その評価が賃金に反映されることもない―おそらく多くの会社に同じような状況があるのではないでしょうか。

しかし、それでは公平とはいえません。
会社が求める理想的なパートとはどんな従業員なのか。
パートに求められる能力は何か。
そして、能力や働き方に応じた賃金や社員登用制度はどのようなものか。
パートを尊重し、気持ちよく働いてもらうためには、それらを明確にしなければなりません。

競合店対策のためには、社員の 7 割を占めるパートの意識改革や能力向上が必須だと判断した経営陣は、以下のような 3 つの仕組みを作ることにしました。

- パートの職務内容と難易度の具体的な明示
- 職務と連動した賃金制度
- 適切な評価制度

職務等級基準書

仕組み作りの第一歩は、職務と職務のグレードを明らかにすることでした。
いわゆる「職務等級基準書」の策定です。

そこで、部門長と店長、経験の長いパートへのヒアリングや担当者へのアンケート調査を実施して、パートの職務の洗い出しを行い、職務内容を出来るだけ具体的に記述しました。

その課程で、部門長や店長から、職務によっては「パートでは難しいのではないか」という声も挙がりましたが、少しがんばって難しい職務にチャレンジしてもらえば、パートの時給を上げることができます。
そこで、OJT をしっかり行うことを条件に、懐疑的な部門長などにも納得してもらいました。

職務は難易度に応じて A、B、C の 3 段階に分類し、その達成度（評価）も I、II、III の 3 段階にして、年功的要素は極力排除しました。経験によって達成度が高まる人ばかりではないことが、過去の経験からわかっていたからです。

表 1　パート社員の職務と評価基準

等 級	職 務	I	II	III
A	各部門の技術指導や手順の改良	期待通り	期待より上	期待をはるかに超える
B	各部門における商品づくり	期待通り	期待より上	期待をはるかに超える
C	レジ精算全般	期待通り	期待より上	期待をはるかに超える

出所）独立行政法人中小企業基盤整備機構の J-Net21「売上アップ取り組み事例集>パート社員の能力を開発する。中小・零細店舗の大型店対策（事例 9 回目）」
https://j-net21.smrj.go.jp/special/sells02/201202/article-09.html

職務と賃金の連動

職務のうち、C-1 等級を従来のパートの時給の基準にして、この職務等級基準と賃金を連動させ、A-I を入社 3 年目の社員（25 歳）の月収と同額に設定しました。

ただ、セルフレジが急速に普及しつつある現在では、パートが担う職務の変化に応じて、この設定が見直されている可能性もあります。

社員への登用制度も整えました。B-III 以上の職能と部門長の推薦、社長の面接が条件です。

では、こうした取り組みによって、パートの給与総額はどの程度、増加したのでしょうか。
実は、パートが活躍する場が拡がり、その分、社員の時間外手当が減少したため、人件費の増額は僅かな金額に留まったということです。

評価制度

評価制度を策定するのは大変でした。

できるだけ客観的かつ公平に評価しようとしても、なかなか理想通りにはいきません。
パートの評価基準は売上や利益予算などではなく、定性的なものが中心だったからです。
また、評価者の店長や部門長も十分な評価研修を受けたわけではなく、当初は正しく評価できたか疑問でした。

そこで、職務等級基準書に盛り込んだ「期待通り」とはどの程度の達成度か、できるだけ明確になるように、改良を加えていきました。

たとえば、商品作りでは、売れる商品をきれいに作ることだけでなく、高い鮮度を維持するために、顧客が来店する時間帯のピークに合わせることも大切です。
そこで、所定の時間内に指示された数量を作ることができているかという商品化の速度も、基準に加えました。

声だしなどの「にぎわいの演出」や「にこやかで明るい態度」など、特に数値化が難しい定性的な項目は、パートや社員による投票を参考にしました。
また、最も元気に挨拶し、声だしをしていたパートを毎月 2～3 名、投票で選出し、表彰する制度も作りました。

最終的な評価は店長が行いますが、投票結果を参考にすることで、基準に具体性を持たせることができたということです。

取り組みの成果

こうした仕組みづくりで得られたのは以下のような効果でした。

- パート社員の定着率が高まり、採用コストが削減できた。
- パート社員の欠勤率が減少した。
- パート社員の発言や提案が多くなった。
- POP づくりなどの研修に積極的なパート社員がふえた。
- パート社員の応募数が多くなった。
- 社員の意識改革にもつながった。

出所）独立行政法人中小企業基盤整備機構の J-Net21「売上アップ取り組み事例集>パート社員の能力を開発する。中小・零細店舗の大型店対策（事例 9 回目）」
https://j-net21.smrj.go.jp/special/sells02/201202/article-09.html

人は尊重され評価されれば、それが従業員エンゲージメントやモチベーション向上につながります。
上のような成果は、そのことを如実に表しているのではないでしょうか。

厚生労働省の発表によると、2024 年 4 月のパートタイム労働者比率は 30.48%、実に労働者の 3 分の 1 弱を占めています。
出所）厚生労働省「毎月勤労統計調査　令和 6 年 4 月分結果確報」（2024 年 6 月 24 日）p.11
https://www.mhlw.go.jp/toukei/itiran/roudou/monthly/r06/2404r/dl/pdf2404r.pdf

しかし、社員とは異なる処遇を受けているパートは珍しくないでしょう。
パートの職務を明確にして評価基準を定め、職務・評価と賃金を連動させる取り組みは、会社に貢献しているパートを尊重する方法の 1 つです。

そして、そのように、人の営みとしての本質を大切にすることが、結局は売り上げアップをはじめとして、企業側にも多くのメリットをもたらす―ご紹介した事例は、そのことを示唆しているのではないでしょうか。

そこで脳裏に浮かぶのが、渋沢栄一の理念です。

「道徳経済合一説」

渋沢栄一は、約 500 の会社に関わり、同時に約 600 の社会公共事業にも尽力するという、破格の実業家でした。
その渋沢栄一が唱えた「道徳経済合一説」とはどのようなものでしょうか。

道徳と経済は表裏一体

私たちには、道徳と経済は本来矛盾するものだと考える傾向があります。
儲けにばかり走ると道徳を破り、道徳ばかり重んじていると儲からなくなってしまう。それで、道徳と経済はほどほどにバランスさせればいいと考えがちではないでしょうか。

しかし渋沢は、道徳と経済とは別個のものではなく、本質的に一致するものだと考えていました。この 2 つはいわば表裏一体で、切り離せるものではないというのです。

ただ、道徳と経済が本質的に一致するといっても、自ずと一致するというような甘いものではありません。
この 2 つを一致させるために、十分な覚悟をもって主体的に取り組み、努力しなければならないと渋沢は説いています。
出所）田中一弘「報告：渋沢栄一の道徳経済合一説」企業家研究フォーラム『企業家研究〈第12 号）』（2015 年 12 月 20 日）p.35, pp.39-40
https://kigyoka-forum.jp/wp-content/uploads/2022/04/JES12_05_Tanaka.pdf

私利私欲を排す

こうした信念をもつ渋沢栄一は、私利私欲を嫌いました。
渋沢は著書『論語と算盤』で、以下のように述べています。

> およそ人として、その生き方の本筋を忘れ、まっとうでない行いで私利私欲を満たそうとしたり、権勢に媚びへつらって自分が出世しようとするのは、人の踏むべき道を無視したものでしかない。それでは、権勢や地位を長く維持できるわけでもないのだ。
>
> もし社会で身を立てようと志すなら、どんな職業においても、身分など気にせずに、最後まで自力を貫い

て、人としての道から少しも背かないように気持ちを集中させることだ。そのうえで、自分が豊かになって力を蓄えるための知恵を駆使していくのが、本当の人間の意義ある生活、価値ある生活といえるだろう。

出所）渋沢栄一（守屋淳・訳）『現代語訳　論語と算盤』（ちくま書房・電子書籍版）（2014 年）p.128

渋沢は、あくまで国を豊かにし、人々を幸せにすることを目的として、事業育成を行っていました。

彼がその設立のために中心的な役割を果たした組織の中には、日本鉄道（現在の JR）や第一国立銀行（日本最古の銀行）、東京商法会議所（現在の日本商工会議所）、東京株式取引所（現在の東京証券取引所）など、現代社会に欠かせないものが数多くあります。

企業の目的が利潤の追求にあるとしても、その根底には道徳が必要であり、国や人類全体の繁栄に対して責任を持たなければならない―渋沢が生涯を通して貫いた価値観です。

出所）公益財団法人 渋沢栄一記念財団「渋沢栄一関連会社名・団体名変遷図」（2019 年 3 月 29 日版/2024 年 6 月 27 日改訂）
https://eiichi.shibusawa.or.jp/namechangecharts/

出所）公益財団法人 渋沢栄一記念財団「史料館だより＞35 渋沢栄一生誕 170 年を迎えて」（2010 年 1 月）
https://www.shibusawa.or.jp/museum/newsletter/320.html

おわりに

道徳を基盤とした事業活動を実践すること、従業員や顧客、取引先など、すべてのステークホルダーに対して誠実であること、社会に貢献すること、それが人々の信頼を得、安定した経営につながる―新一万円札の肖像は、大切なメッセージを発信しているのではないでしょうか。

筆者プロフィール

＜横内美保子＞

博士（文学）。総合政策学部などで准教授、教授を歴任。専門は日本語学、日本語教育。

高等教育の他、文部科学省、外務省、厚生労働省などのプログラムに関わり、日本語教師育成、教材開発、リカレント教育、外国人就労支援、ボランティアのサポートなどに携わる。

パラレルワーカーとして、ウェブライター、編集者、ディレクターとしても働いている。

X：よこうちみほこ

Facebook：よこうちみほこ

レベル 1_#4_【医師が解説】経営者にのしかかる重責とストレス　どう解消し成果を出す？

掲載日：2024/8/6



出典）https://www.photo-ac.com/main/detail/22233430

ストレスが私たちの日常生活や仕事に与える影響は計り知れません。

特に経営者やリーダーの立場にある方々にとって、責任とプレッシャーは避けて通れない課題となります。

医師や経営者には、いろいろな理由からストレスがかかりやすいという共通点があります。

そこで今回の記事では、筆者の医師としての経験を通じて、経営者の皆様が感じるストレスとその対策についてのヒントをお伝えしたいと思います。

ストレスの多様性と共通点

私は、今年（2024 年）で 15 年目となる医師です。

大学の医学部を卒業してから、これまで様々な職場で働いてきました。

もちろん医師という仕事にはやりがいもあります。

しかし、仕事をしていく上では多種多様なストレスがあり、それぞれの時期での自分なりのストレスとの向き合い方を編み出してきました。

実は医師と経営者には、以下のような共通するストレスや考え方があります。

責任とプレッシャー

医師には、患者の命を預かるという責任が常にプレッシャーとしてあります。
内科や外科などの診療科に関わらず、ミスが許されにくい環境ですので、独特の緊張感があります。
一方、経営者の皆様には、会社の成長や従業員の生活を背負うという責任があります。
経営判断が会社の存続に直結することもあり、重大なプレッシャーを感じる場面も多いでしょう。

長時間労働とライフワークバランスの難しさ

言わずもがな、医師は長時間の診療や患者急変などへの対応、当直などによる過労が問題となることが多い職業です。
働き方改革などで労働環境が改善してきているとはいえ、まだまだ長時間労働を当たり前とする風潮が残っている職場もあると感じます。
経営者の皆様にも、長時間労働は当然という人も多いでしょう。
経営者や管理職となると、残業の概念がなくなる職場もあり、家族との時間の確保が難しいという点があります。

医師のキャリアとフェーズごとのストレス

ここまで、医師と経営者に共通するストレスについて少しご紹介しました。
ここからは、私の医師としてのキャリアとともに、フェーズごとのストレスについて少しご説明します。

研修医時代（1-2 年目）

研修医、つまり医師としての新人時代には、仕事に慣れることがまず大変でした。
勤務時間外の呼び出しに対しては、いつ PHS がなるのかビクビクし、救急外来ではどのような方が運ばれてくるのか恐怖でした。
医師としては恥ずかしいことかもしれませんが、やはり最初は知識や経験も乏しく、かなりストレスがかかっていたと思います。
この時期は、上級医からの厳しい指導やミスに対する恐怖も大きなストレス要因でした。

大学病院時代（3-4 年目）

緊急の呼び出しはほぼなくなりましたので、そのストレスは軽減されました。
その一方で、毎晩遅くまで続く画像の読影や書類仕事が精神的にも肉体的にも大きな負担になります。
長時間労働や雑用の多さがストレスの原因だったのです。

なお、ロンドン大学の疫学・公衆衛生学教授である、Kivimäki ら（2015）による長時間労働が健康に与える影響についての研究では、心疾患や脳卒中のリスクが増加することが示されています。
Kivimäki, M., et al. (2015). Long working hours and risk of coronary heart disease and stroke: a systematic review and meta-analysis of published and unpublished data for 603 838 individuals. The Lancet, 386(10005), 1739-1746. https://pubmed.ncbi.nlm.nih.gov/26298822/

筆者は幸い心疾患にも脳卒中にもなりませんでしたが、歯のケアを怠ってしまったことや食事がままならなくなったという不摂生がありました。
その結果、親知らずが虫歯になってしまい、とても大変な思いをしました。

がんセンター時代（5-6 年目）

がんセンター時代には、研修医時代や大学病院時代に比べるとかなり低ストレス状態となります。
優しい上司や頼もしい同期に恵まれかつ仕事内容も自分が専門としたいことのみができるようになったことも理由です。
しかし、お給料が低いことはプチストレスでした。

再び大学病院に戻った（7-9 年目）時

専門に戻れた安心感があったものの、子育てとの両立の難しさや給与の不満がありました。
また当時の大学病院は、市中病院と比べると医師がしなければならない仕事が多く、スタッフもイラついているようでなかなか人間関係が複雑であったことに悩みます。
それらも、ストレスの原因となりました。

公衆衛生医師として新型コロナ対応に当たった（10-12 年目）時

筆者はこのステージで第 2 子を産み、産休育休をとることになります。
そしてライフワークバランスを考え、公務員になることを選びます。

公衆衛生医師は、保健所や保健センターで、病原性大腸菌感染症や結核などの感染症対応を行うということがメインの仕事です。
最初の 1 年目は、仕事内容にもストレスになるようなプレッシャーは少なく、かつ休暇をとることも医療機関で働くことに比べると容易でした。
そのため、ストレスを感じることも少なかったのですが、ここで世界的なウイルスパンデミックが起きてしまいました。

公衆衛生医として、かつ係長級に昇格したことにより、医師としての感染症対応に加えて、職員の方々とどのように協力して対応していくのかということも仕事に加わります。
また、緊急事態になってしまい、2 人の上司がたびたび方針の違いによって大喧嘩をする場面もありました。
部下としてその対応に当たることも求められ、容易なことではありません。
やりがいはありましたが、その過酷な状況がストレスの大きな要因となります。

経営者の皆様のストレス管理に役立つ方法とは

これらの経験から学んだ教訓は、ストレスマネジメントの技術や適切な休息の取り方、そして効果的なコミュニケーションの重要性です。
特にリーダーシップとコミュニケーションは、医療現場でも経営の場でも同様に重要だと思います。

実際に、感情知能、つまりコミュニケーション能力などが高いリーダーは、チーム全体のパフォーマンスを向上させることができることが示唆されている報告もあります。
Harms, P. D., & Credé, M. (2010). Emotional intelligence and transformational and transactional leadership: A meta-analysis. Journal of Leadership & Organizational Studies, 17(1), 5-17.
https://psycnet.apa.org/record/2010-02929-001

ストレスマネジメントの技術を学ぶ

まず、ストレスマネジメントの技術についてです。
ストレスを感じたときに、どのように自分の感情をコントロールし、適切に対処するかを学ぶことです。

アメリカのスタンフォード大学で心理学を研究している Gross (2002) の研究によると、感情調整の技術は、ストレス管理において非常に有効であるとされています。

自分が一番どういったことにストレスを感じるのかを理解し、それに対処するための具体的な方法を日常生活に取り入れることが重要です。

Gross, J. J. (2002). Emotion regulation: Affective, cognitive, and social consequences. Psychophysiology, 39(3), 281-291.
https://pubmed.ncbi.nlm.nih.gov/12212647/

休息を適切に取る

筆者の例として、呼び出しに怯える研修医時代には、適切な休息を取ることでストレスを軽減しました。
具体的には、友人や同僚との会話、趣味の時間を大切にすることで、精神的なバランスを保ちます。
大変なときこそ、楽しい・辛いなどの感情を誰かと共有し、休息をとることが大切です。

また、長時間労働が続いた大学病院時代には、時間管理とリフレッシュの方法を工夫しました。
スケジュール管理を徹底し、短時間でも質の高い休息を取ることを心掛けます。
夕食の時間がどうしても遅くなってしまうため、残業中に軽食をとり、満腹で寝ることがないよう工夫することも大事です。

また、日常的な運動や趣味に時間を割くことも、ストレス解消には効果的です。
空いた時間にはゴロゴロするのではなく、あえてスポーツジムで汗を流す、あるいは自宅でトレーニングをするなどすると良い場合もあります。
実際に、筆者のまわりの医師でも、トレーニングなどで身体を動かしているということをよく耳にします。

効果的なコミュニケーションをとる

効果的なコミュニケーションも、ストレス管理において欠かせない要素です。
筆者は、管理職の立場であった時もそうでなかった時も、他の医療スタッフと良好な関係を築けるよう、積極的にコミュニケーションをとるよう心がけていました。

感情知能が高いリーダーは、部下との信頼関係を築き、ストレスの軽減に貢献することができるそうです。
リーダーは、部下の声に耳を傾け、フィードバックを適時に提供することで、職場の雰囲気を改善し、ストレスの原因を早期に発見することができます。
その結果として、チーム全体のパフォーマンスを向上させることが可能となるでしょう。

注意点として、中には関わることで自分を傷つけるだけの人もいるということです。

利害だけを考えるというのも問題ですが、関わり合いにならないことが最善という場合もあるので、留意しておきましょう。

ストレスチェック制度とメンタルヘルスケアの専門家との連携

ストレスチェック制度の導入や、メンタルヘルスケアの専門家との連携も有効です。

精神医学を研究している Joyce et al. (2016) の研究によれば、職場でのメンタルヘルス介入は、従業員のストレス軽減に効果的であることが示されています。
Joyce, S., et al. (2016). Workplace interventions for common mental disorders: a systematic meta-review. Psychological Medicine, 46(4), 683-697.
https://pubmed.ncbi.nlm.nih.gov/26620157/

実際に、筆者も公衆衛生医師の時代にストレスチェックを受けました。
その際、筆者は上司同士の仲が悪いため、部下である自分も対応に困っている、とカウンセラーに相談します。
すると、「勝手にやってるな！くらいに思っておけばいいですよ」というアドバイスをもらうことができ、楽になります。
自分の考え方だけでなく、他人、特に話を聞くプロフェッショナルであるカウンセラーの意見を聞くことはやはり大切だと実感しました。

部下を持つ経営者の方は、その立場上、自分自身のメンタルの状態を他人に観察してもらう機会も少ないかと思います。
そうした孤独になりやすい経営者の方が、カウンセラーなどの手を借りることはとても有効でしょう。

まとめ

ストレスは避けられないものですが、それに対処する方法は存在します。
前向きな姿勢と適切な対策を取ることで、ストレスを乗り越えることができると強調したいと思います。
経営者の皆様も、ストレスに対してぜひ前向きに取り組み、対策をしていきましょう。
自分自身の健康管理を大切にし、適切なストレスマネジメントを行うことで、長期的に見て企業の成長にも繋がるでしょう。
筆者の医師としての経験が、少しでも皆様の参考になれば幸いです。

【筆者】

・名前　木村香菜（きむらかな）

・プロフィール：行政機関である保健センターで、感染症対策等主査として勤務した経験があり新型コロナウイルス感染症にも対応した。現在は、主に健診クリニックで、人間ドックや健康診断の診察や説明、生活習慣指導を担当している。また放射線治療医として、がん治療にも携わっている。放射線治療専門医、日本医師会認定産業医、日本人間ドック学会認定医。

レベル 1_#5_DX でここまで変わる！売り上げアップと深い関係の「データドリブン」とは？

掲載日：2024/8/20



出典）https://pixabay.com/ja/photos/1841158/

メーカー、小売、飲食、と幅広い分野で DX を導入する動きがあります。

「DX」というと難しいと考えてしまうかもしれませんが、まず一部にデジタルを取り入れる、それだけで様々な角度からのアプローチで売り上げをアップさせる企業も相次いでいます。

また、デジタルとの関係を知っていくと、そもそも売り上げアップにはどんなことが必要なのかも見えてきます。

いくつかの事例をご紹介します。

高単価のリピーターを増やさなければならない理由

あらゆる産業において今、「リピート顧客を増やす」ことが重要な戦略になっています。

少子高齢化が進み人口が減っていくなか、ライバル企業と奪い合うパイの大きさはどんどん小さくなっていきます。新規顧客の獲得はおのずと難しくなっていくでしょう。
であれば、海外に販路を広げるか、リピーターを確保する必要性が高まることは想像に難くありません。

ある衣料品販売店の「瞬時の粋な取り計らい」

筆者がある通信販売の衣料品店から聞いた話です。

普段から顧客管理はシステム上で行っており、顧客リストのなかでも誰がこれまでにどのくらいの商品を買ってくれているか、といったことも完全に把握していました。

そこに 2020 年、コロナ禍が訪れました。

みなさんまだ記憶に新しいことかと思いますが、当初は買い占めなどの影響もあり、マスク不足が騒がれました。
海外の繊維業者との取引があるこの衣料品店は、すぐに取引先からマスクを仕入れ、さらにこれまで多くの買い物をしてくれたリピート客を絞り込みました。
そしてそれらの顧客を中心に、プレゼントとしてマスクを郵送したのです。
顧客からは大きな反響があったといいます。

マスクを受け取った顧客の側に立って考えれば、この衣料品店に感謝の気持ちを抱くことでしょう。いつも買い物をしているお店が、ある日突然無料でマスクを送ってくれたのです。ここで買い物をしていてよかった、と思ったのではないでしょうか。
こうした粋な取り計らいは、その企業の「ファン」を繋ぎ止めることにつながるはずです。

ひとえにこれは、DX の力です。

モノを販売する企業の場合、対面であれば「このお客さんは良く来てくれる人だなあ」という実感はあっても、必ずしもその人の名前や住所を知っているわけではありません。
これまでにいくらお金を使ってくれているかは、わからないことも多いものです。

しかしこの衣料品店は顧客情報をデジタルデータで管理しています。

氏名や住所だけでなく、ひとりひとりが何度買い物をしてくれて、これまでにいくらお金を使ってくれていたか、瞬時に上位顧客を抽出するシステムを導入していました。
紙で伝票整理をしている企業だと、顧客の抽出だけで膨大な時間がかかっていたことでしょう。追いつけないどころか、不可能な対応だったはずです。

「データドリブン」の威力

このようにデータをきちんと取り、それに基づいて戦略を判断する手法を「データドリブン」と呼びます。実はデータドリブンには、いろいろなメリットがあります。

大企業も「勝手な思い込み」で商機を逃していたことを発見

顧客データを管理することには大きなメリットがあります。
成功した事例として、大手旅行会社 JTB の取り組みを見てみましょう。

顧客分析システムを本格導入した結果、会社が勝手に持っている「固定観念」を覆すような顧客の傾向がわかり、新しい商品の提供につながったのです。

JTB はかつて「出張するなら JTB」という広告を出していました。しかしこれは男性目線の企画であり広告でした。出張するのは男性社員という暗黙の前提があったのです。偏見、とも言えるかもしれません。

しかしデータ分析の結果、実は女性のほうが宿泊場所を選ぶ際のこだわりが多く、その分、男性よりも単価が 10%高いということがわかったのです。

NIKKEI リスキリング「旅立つ人の心、データで読み解く　JTB のデジタル戦略」
https://reskill.nikkei.com/article/DGXMZO43340620U9A400C1000000/?page=2

そこで「出張女子」という広告企画を打ち出したところ、成約率が 45%もアップしたといいます。

日経クロステック「「出張女子」狙いで成約率 45%増、JTB が導き出した勝利の方程式」

https://xtech.nikkei.com/atcl/nxt/column/18/00001/01874/

データは客観的な事実を示してくれます。そのおかげで「思い込み」を排除できたという事例でもあります。
逆に言えば、「思い込み」「勝手なイメージ」で逃していた商機を見つけ、売り上げアップに繋げたということでもあります。

エクセルを「少し」勉強することで大躍進

また、商品の売れ行きをデータ化することで、商品を変えていないのに売り方を変えただけで飛躍的に売り上げを伸ばした企業として有名なのがワークマンです。

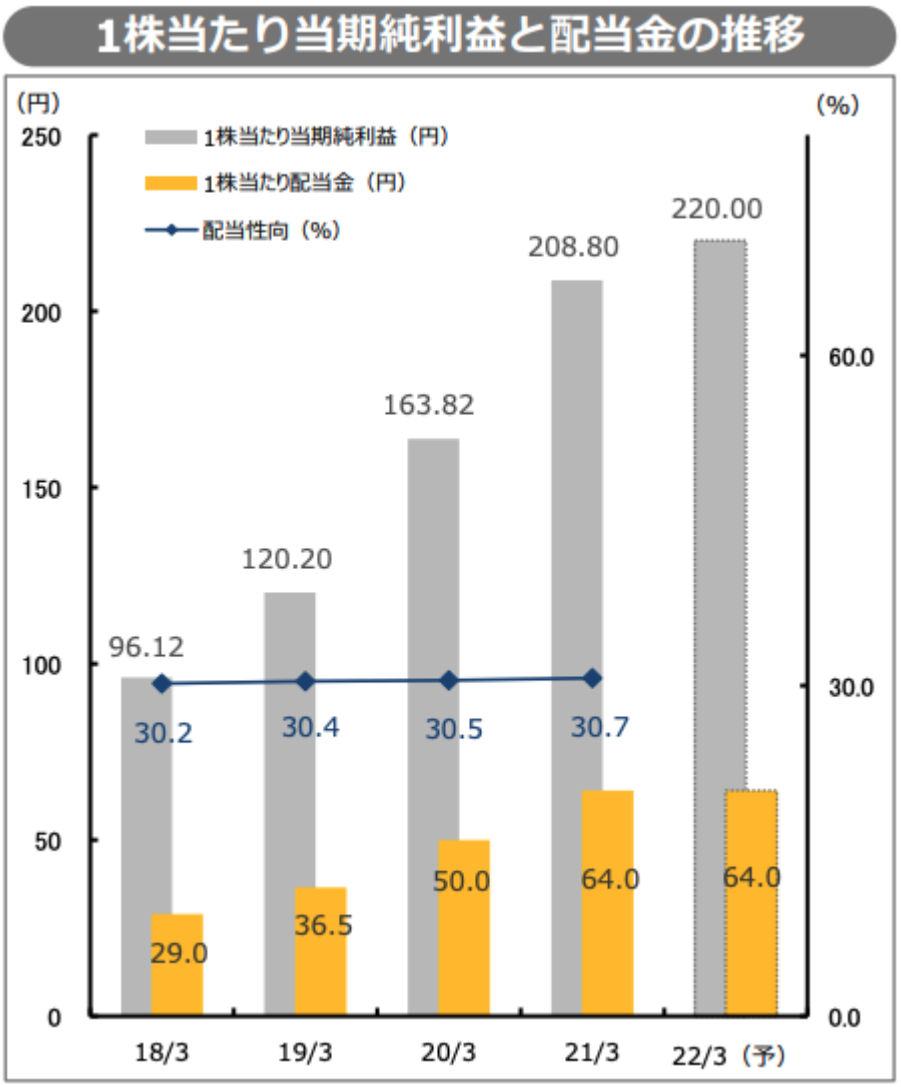
ワークマンはデータを使う企業になるまで、いわゆる「どんぶり勘定」の状態でした。
例えば在庫の数量データでは、期末と期首の販売額の差を在庫にするという簡易的なものだったのです。
確かにこれはシンプルな方法で、人手不足の時代に余計な作業を排除するという意味では良いかもしれませんが、デメリットもあります。
何がどれだけ、どんな理由で売れたのかを把握できないからです。逆に売り上げが落ちた時に理由がわからず、対処できなくなってしまうのです。

酒井大輔『ワークマンは商品を変えずに売り方を変えただけでなぜ 2 倍売れたのか』（日経 BP）
(2020 年) p61

そこで、エクセルの講習を開くことにしました。売り上げのアップダウンについて、データがあれば理由を特定できるからです。

日経クロストレンド「ワークマンが駆使する「自作エクセル」を初公開　データ経営の要」
https://xtrend.nikkei.com/atcl/contents/18/00599/00004/

講習の結果、データに強くなった社員は、その知識をさらに伸ばすということを行います。
すると、そこから売り上げは右肩上がりになりはじめました。



ワークマンの純利益の推移

(出所：「2021 年 3 月期決算説明会資料」株式会社ワークマン)

https://www.workman.co.jp/ir_info/pdf/2021/202105_kessan.pdf p30

上の図にある 21 年 3 月決算以降も、伸びを示し続けています。

株式会社ワークマン「財務データ」

https://www.workman.co.jp/ir%E6%83%85%E5%A0%B1/%E8%B2%A1%E5%8B%99%E3%83%87%E3%83%BC%E3%82%BF

モノを販売する企業にとって「在庫」は悩みの種でもあります。

無計画に仕入れをするよりも、売れ筋に沿って在庫を最小限に抑えるほうが、倉庫や輸送にかかる費用を削減できるというメリットもあります。

多くのものが値上がりを続ける中、不必要な経費をかけずに費用を抑えることは、重要な戦略になることでしょう。

じつは「良質ではない顧客」も存在する

そして、あまり良い言葉ではありませんが「良質でない顧客」が企業には一定の割合で存在します。

いま「カスタマーハラスメント」、顧客から不条理なクレームや注文を押し付けられて手間が増える、従業員を疲弊させる現象が問題になっています。

直接のクレーマーでなくても、例えば「大した額を取引していないのに、しょっちゅう電話をかけてきたり従業員を呼び出したりする」顧客などがそれにあたります。
「費用対効果」を大きく損ね、かつ従業員のモチベーションも落としてしまう可能性もあります。

もちろん、顧客に対してそう強く出られないという考え方も一理あります。
しかし「どの顧客が費用対効果を悪くしているのか」を把握することも大切です。
経営の軸となる重要なリピーターと、そうでない顧客に同じ対応をすることのデメリットにも目を向ける必要があるのです。

これも、どの取引先がどのくらいの利益になっているか、一方でどのくらい従業員に負担をかけているか、データがあれば、対応のしかたを考えるきっかけになります。
人手不足のなか、従業員を守るという意味でも必要なことです。

「お客様は神様」という考え方も最近では変わってきています。新しい価値観を取り入れる一助にもなるでしょう。

補助金の積極活用も検討しよう

ここまで事例を含めてデータの有用性を紹介してきました。
「デジタルには何か良いことがありそうだ」ということは、多くの人が感覚として持っているかもしれません。

しかし課題はその先にあります。

「何をしたらいいかわからない」ということです。

この疑問に対しては、2 つの解消方法があります。

まず、企業の「KPI(＝重要業績評価指標)」を明確にしてみることです。

KPI に対する意識は、実は日米で大きく分かれています。



評価や見直しの頻度の日米差

(出所：「DX 白書 2021」独立行政法人情報処理推進機構)

https://www.ipa.go.jp/files/000093699.pdf p7

黄色の円で囲まれた数字がアメリカで、「取り組んでいる」とする企業の割合、緑が日本です。

アメリカの企業がさまざまな指標を意識し見直しをしているのに対して、日本企業は数字に基づいた経営がほとんどできていないのが現状です。きつい言い方をすれば「無鉄砲」ということもできます。

先ほども述べた通り、今後、ライバルと奪い合うパイは小さくなっていきます。
「いいものを作っていれば売れるだろう」という考え方では難しくなっていくのです。
特に、スマートフォンを良く使う若い世代は「その場でバズっているもの」に興味を示すため、流行はコロコロと変わっていきます。
YouTube や TikTok が流行を牽引する時代であることにも気をつけなければなりません。「勘」だけでは、世代間ギャップを乗り越えることは難しいでしょう。

消費者が「今欲しいもの」を提供することができるかは、勝敗を分ける大きな要因になります。

なお、東京都内の中小企業の DX 推進と生産性の向上を支援する公的事業があります。

東京都「新規事業 都内中小企業の DX 推進と生産性向上を支援します！令和 6 年度 DX 推進支援事業」
https://www.metro.tokyo.lg.jp/tosei/hodohappyo/press/2024/05/08/09.html

DX 推進のためのアドバイザーの派遣や、DX の推進・生産性向上のための助成金が出るというものです。

積極的に知ろうという姿勢があれば、一歩を踏み出せます。
難しく考えずに、まずは気軽な思いでこれら制度を利用してみてはいかがでしょうか。

＜清水 沙矢香＞
2002 年京都大学理学部卒業後、TBS に主に報道記者として勤務。社会部記者として事件・事故、テクノロジー、経済部記者として各種市場・産業など幅広く取材、その後フリー。
取材経験や各種統計の分析を元に多数メディアに寄稿中。

レベル1_#6_「セキュリティ10大脅威」のトップ　身代金を要求する「ランサムウェア」とその対策とは

掲載日：2024/9/3



Photo AC「忍び寄る影…（１）」

https://www.photo-ac.com/main/detail/23551131

サイバー攻撃の手段は年々巧妙化しています。

みなさんが、ある日突然いつも通りのシステムが使えなくなり、パソコン画面に恐ろしいメッセージが表示されプリンターから大量の脅迫文が出てきたりしたとしましょう。
きっとパニックになってしまうのではないでしょうか。

また、ウイルスを忍ばせるような「偽メール」はいつも日本語が不自然だったり、身に覚えのない取引先からのものだからさすがに気づく、と考えている方も多いはずです。
しかし最近は、実際の取引先の名前を騙り、また文章も違和感のないメールが出回るなど、ウイルスに侵入されるリスクはずっと高くなっているのです。

ことし6月にKADOKAWAが被害に遭った「ランサムウェア」を含むサイバー攻撃ではグループの広範な事業が停止に追い込まれました。
さらにChatGPTなどの生成AIは悪質なソフトウェアを作成する道具にもなっており、最新のサイバー攻撃について知識を改めておく必要があります。

ここでは近年のサイバー攻撃のトレンドの中で最も脅威とされている「ランサムウェア」についてご紹介します。

2024年の「情報セキュリティ10大脅威」

6月に入り「ニコニコ動画」などを運営するKADOKAWAが大規模なサイバー攻撃を受け、全社的に多くの業務で支障が出ています。
KADOKAWA は完全復旧について1か月以上かかると説明していますが、具体的な日時はまだ示されていません。(6月20日時点)
「ＫＡＤＯＫＡＷＡ襲った身代金要求ウイルス、日本企業の感染被害率は突出して低く」産経新聞
https://www.sankei.com/article/20240619-4HAABW3PMNJ6HIPUVNR65I7JYQ/

今回、KADOKAWAを襲ったサイバー攻撃のひとつが「ランサムウェア」と呼ばれるものです。

IPA(＝独立行政法人情報処理推進機構)が毎年、サイバー攻撃に関する最新のトレンドについて公表しています。

それによると、2024年の情報セキュリティについての脅威トップ10は下のようになっています。

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い
1	ランサムウェアによる被害	2016年	9年連続9回目
2	サプライチェーンの弱点を悪用した脅威	2019年	6年連続6回目
3	内部不正による情報漏えい等の被害	2016年	9年連続9回目
4	標的型攻撃による機密情報の窃取	2016年	9年連続9回目
5	修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)	2022年	3年連続3回目
6	不注意による情報漏えい等の被害	2016年	6年連続7回目
7	脆弱性対策情報の公開に伴う悪用増加	2016年	4年連続7回目
8	ビジネスメール詐欺による金銭被害	2018年	7年連続7回目
9	テレワーク等のニューノーマルな働き方を狙った攻撃	2021年	4年連続4回目
10	犯罪のビジネス化(アンダーグラウンドサービス)	2017年	2年連続2回目

2024年の組織向け情報セキュリティ10大脅威

(出所：「情報セキュリティ10大脅威 2024」独立行政法人情報処理推進機構)

https://www.ipa.go.jp/security/10threats/m42obm00000044ba-att/setsumei_2024_soshiki.pdf p4

ランサムウェアは、2016年に登場して以降、9年連続でトップに挙げられているのです。

なお、IPAは情報セキュリティ10大脅威について「個人向け」と「組織向け」の2種類を公表しています。
個人でインターネットを使う時に考えるべきセキュリティと、組織として使う時では全く違う意識を持つ必要があります。

ランサムウェアの被害事例と特徴

ランサムウェアによる被害やランサムウェアの仕組みについて、みていきましょう。

2023年7月に名古屋港コンテナターミナルのシステムがランサムウェアによるサイバー攻撃を受けて停止し、約3日間にわたってコンテナの搬入・搬出が止まるなどの大きな影響を受けました。

「名古屋港の障害、ロシアのハッカー「ロックビット」が攻撃か…プリンターから脅迫文100枚」読売新聞オンライン
https://www.yomiuri.co.jp/national/20230706-OYT1T50167/

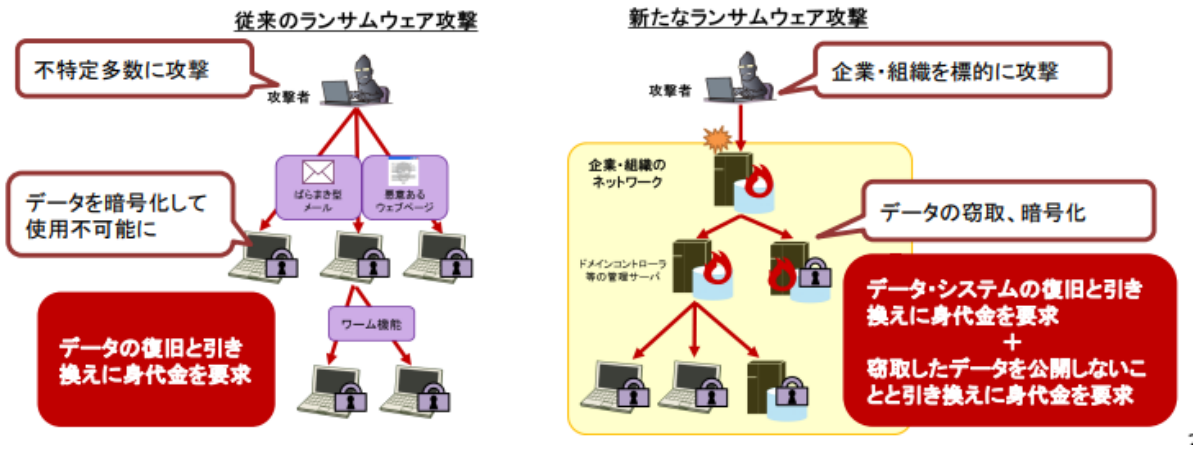
「コンテナターミナルにおける情報セキュリティ対策等検討委員会中間取りまとめ②」国土交通省
https://www.mlit.go.jp/kowan/content/001710842.pdf p1

国土交通省の調査などによると、関係者がシステムの停止を確認したのは7月4日の早朝6時半ごろのことです。その1時間後にはプリンターから、ハッカー集団を名乗る脅迫文が約100枚出力されました。
その後名古屋港運協会などが状況を調査したところ、物理サーバー基盤および全ての仮想サーバーが暗号化されていることがわかりました。

出勤してパソコンがロックされているだけでなく、大量の脅迫文が出てきたらパニックになってしまうのではないでしょうか。
とりあえず連絡をとってみよう、と思うかもしれません。
しかしそれでは彼らの思う壺です。ランサムウェアは「身代金」を要求するウイルスだからです。

ランサムウェアによる攻撃の特徴（1）～多重の脅迫構造

「ランサムウェア」とは、「Ransom(身代金)」と「Software(ソフトウェア)」を掛け合わせた造語です。「身代金を要求するソフトウェア」ということで、仕組みは下のようになっています。



ランサムウェア攻撃の仕組み

(出所：「DX時代のサイバーセキュリティ対策」経済産業省)

https://www.meti.go.jp/policy/it_policy/privacy/cybersecurity_privacy_governance_seminar1.pdf p2

悪意あるソフトウェアを組織のシステムに忍び込ませてデータを暗号化して使えなくしてしまう、という点ではこれまであったようなサイバー攻撃とそう変わりはありませんが、ランサムウェアは「脅迫」の手段をいくつも準備しています。

具体的には、

１） PC やサーバーのデータを暗号化し、業務の継続を困難にする。その後、データを復元することと引き換えに、金銭要求の脅迫をする。

２） 重要情報を窃取し、金銭を支払わなければ窃取した情報を公開すると脅迫する。

３） 金銭を支払わなければ、ランサムウェアに感染したことを被害者の利害関係者等に連絡すると脅迫する。

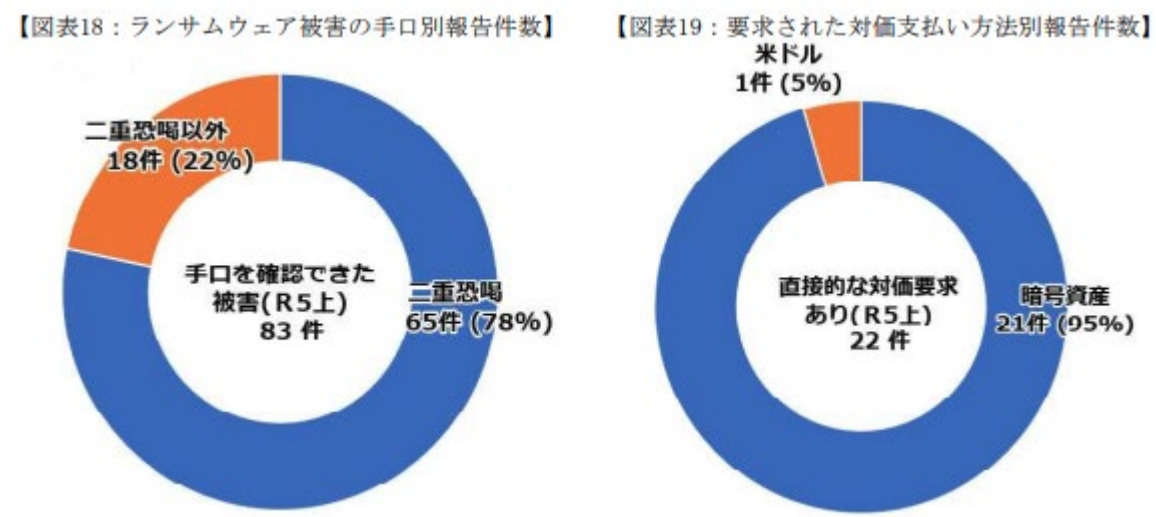
４）金銭を支払わなければ DDoS攻撃（Distributed Denial of Service Attack：分散型サービス妨害攻撃）を仕掛けると脅迫する。

といったものです。

「情報セキュリティ10 大脅威 2024～脅威に呑まれる前に十分なセキュリティ対策を～」情報処理推進機構

https://www.ipa.go.jp/security/10threats/nq6ept000000g22h-att/kaisetsu_2024.pdf pp42-43

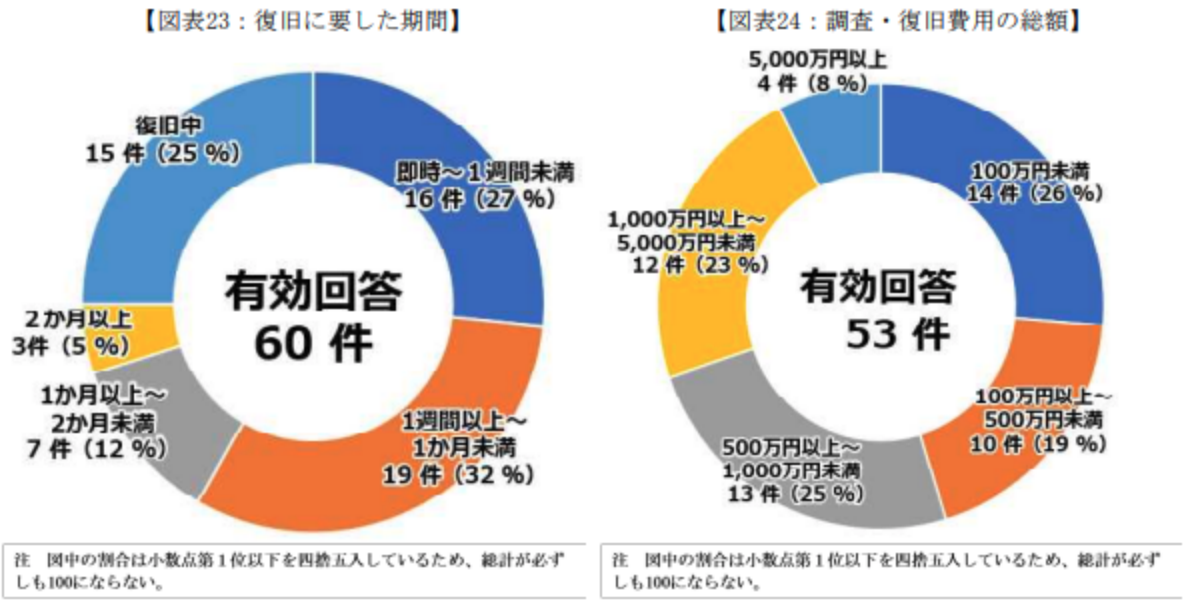
なお、警察庁の統計によれば、国内で令和5年上半期に確認されたランサムウェア被害のうち約8割では、これらの脅迫を組み合わせた「二重脅迫」に遭っていることがわかっています。また、現金ではなく暗号資産による支払いを求めるケースが多くなっています。



ランサムウェア被害に占める「二重脅迫」の割合と要求された支払い方法の内訳(令和5年度上半期)
(出所：「令和5年上半期におけるサイバー空間をめぐる脅威の情勢等について」警察庁)
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R05_kami_cyber_jousei.pdf p20

ランサムウェアによる攻撃の特徴（2）～復旧にかかる期間と費用

また、警察庁によると、ランサムウェアの被害から復旧までの期間は「1週間以上～1か月」が最も多く、また、3割の被害については1000万円以上の費用がかかっています。



ランサムウェア被害から復旧にかかる時間・費用

(出所：「令和5年上半期におけるサイバー空間をめぐる脅威の情勢等について」警察庁)

https://www.npa.go.jp/publications/statistics/cybersecurity/data/R05_kami_cyber_jousei.pdf p21

対策を取っておかなければ、深刻な事態に陥りかねないことがわかります。

巧妙化する偽メール、実在人物の名前も

ランサムウェアによる攻撃は、おもに以下の場所で始まります。

1）ネットワークの脆弱性を悪用(対策をしていないOSやアプリケーションを狙う)

2）意図せず公開されているポート(リモートデスクトップポートなど)への不正アクセス

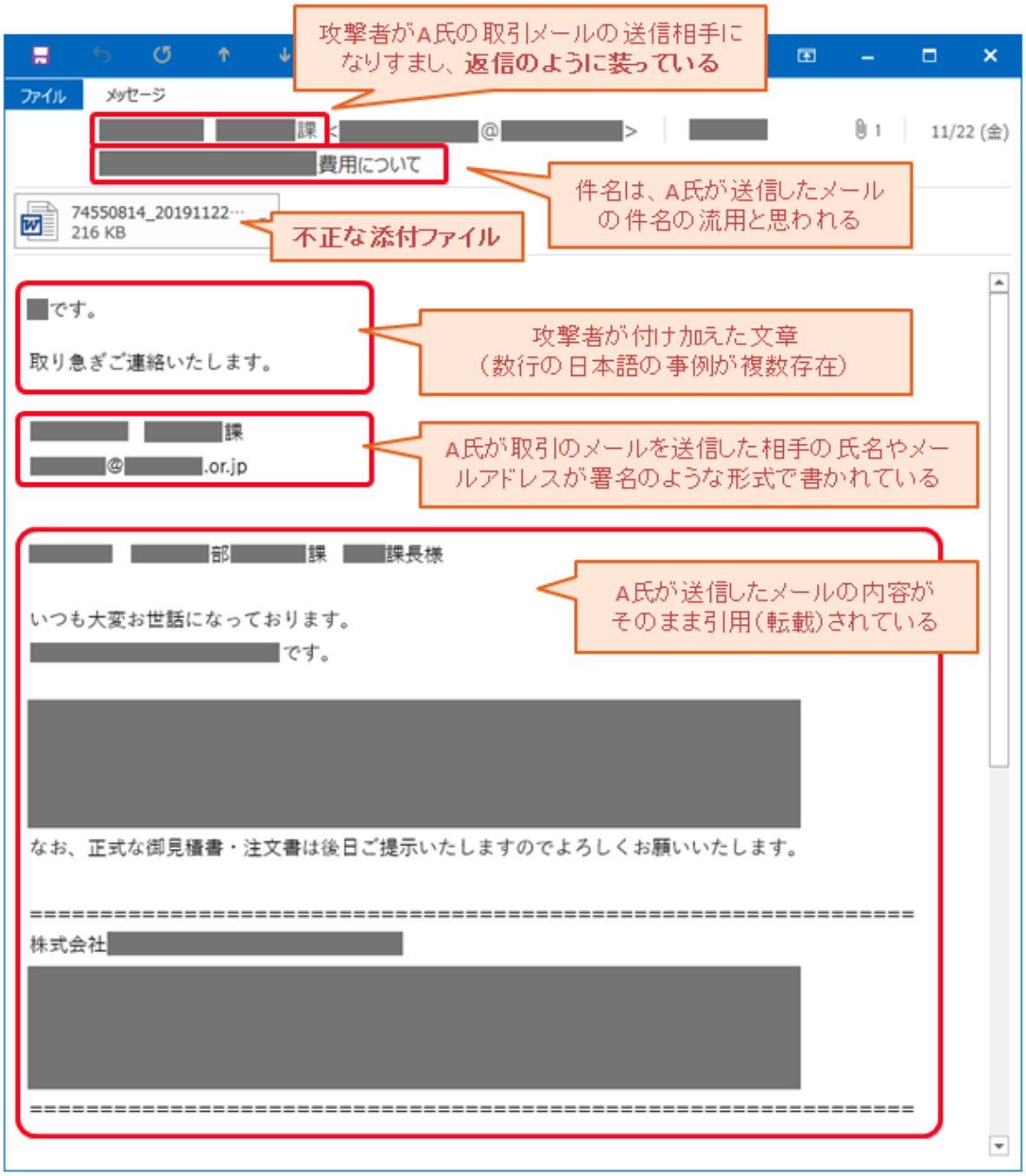
3）ウイルスメール

4）攻撃者が用意したWebサイト

このうち、ウイルスメールについては「昔からある手段では？」と思われるかもしれません。
怪しいメールは開かない、怪しいメールに添付されたファイルは開かない、そのような意識は皆さんのなかになんとなくはあることでしょう。

しかし、「怪しい」の基準は何でしょうか。言葉が不自然、といったことをあげる方は多いことと思いますが、近年ではウイルスメール自体も進化しています。

近年IPAが注意喚起しているウイルスメールの一例としては、「正規のメールへの返信を装う」という手の込んだものがあります。
過去に本人(下の図ではA氏)がやりとりした相手になりすましたメールを作成し送りつけるというものです。
下の図をよく見てください。



攻撃メールの例

(出所「Emotet（エモテット）と呼ばれるウイルスへの感染を狙うメールについて」情報処理推進機構)

https://www.ipa.go.jp/security/announce/20191202.html

実在の相手の氏名、メールアドレス、メールの内容等の一部を流用するという非常に悪質なもので、このメールでは添付ファイルへのアクセスを誘導しています。

大量のメール処理に追われている時にこのようなものに出くわしたら、信じてしまう可能性はじゅうぶんにあるのではないでしょうか。

また、ChatGPTなど、場合によっては人間以上に流暢な文章を書くツールを誰でも使える時代になっています。文章の不自然さという「勘」のようなものだけでは、こうした攻撃を100%避けるのは難しいことでしょう。

ランサムウェアへの対策と身代金要求への対応

では、どう対策をすれば良いのでしょうか。

情報処理推進機構は、感染防止のために次のような対策が有効だとしています。
「ランサムウェアの脅威と対策」情報処理推進機構
https://www.ipa.go.jp/files/000057314.pdf p8

・OS およびソフトウェアを常に最新の状態に保つ：
OS およびソフトウェアのバージョンを常に最新の状態に保ち、脆弱性を解消することで感染リスクを低減する。

・セキュリティソフトを導入し、定義ファイルを常に最新の状態に保つ：
セキュリティソフトを導入し、定義ファイルを常に最新の状態に保つことで、ランサムウェアへの感染リスクを低減する。

・メールや SNS のファイルや URL に注意する：
メールや SNS の添付ファイルを開くことや、本文中の URL をクリックすることでウイルスに感染する可能性がある。受信したメールは送信者、添付ファイル、文面等に十分に注意を払い、心当たりのないメールや英文メール、文面の意味が分からないメールなどは、安易に開かないことが重要である。

最近では、メール送信者情報として実在する企業を騙ったり、メール本文も当該企業が送信するメールを模倣したりするケースが多く確認されており、不特定多数の人物にメールを開かせる手口が巧妙になっている。メールの添付ファイルを開くことは極力避け、どうしても開く必要がある場合は、万が一ウイルスに

感染しても影響がない環境を用意した上で開くことが望ましい。

これらの項目についてひとつひとつ、確認をするというのが基本です。

また、万が一ランサムウェアに感染した場合の対応について知っておきましょう。
最も興味のあるものとして「身代金はどうするか？」ということがあるかとおもいます。

ランサムウェアの被害に遭った時の身代金は、基本的に支払うべきではないとされています。
「事業継続を脅かす新たなランサムウェア攻撃について～～「人手によるランサムウェア攻撃」と「二重の脅迫」～」情報処理推進機構
https://www.ipa.go.jp/archive/files/000084974.pdf p9

過去に海外では身代金を支払った事例もありますが、サイバー攻撃は組織化しており、その収益源を断つことが重要だからです。

実際、ランサムウェア攻撃者への身代金の支払いはここ数年間、減少しています。
「身代金を払う企業がまさかの減少、収入減で焦るランサムウェア攻撃者が立てた新戦略」日経クロステック
https://xtech.nikkei.com/atcl/nxt/column/18/00676/013100126/

先に紹介した名古屋港の事例でも、協会はハッカーに連絡を取ることも、身代金を支払うこともしていません。
「ハッカー集団に身代金支払わず」共同通信（2023年7月6日配信）

日頃の管理を徹底し、もし事態に直面しても、まずは落ち着いてシステムの提供会社や警察当局に連絡するようにしましょう。

＜清水 沙矢香＞
2002年京都大学理学部卒業後、TBSに主に報道記者として勤務。社会部記者として事件・事故、テクノロジー、経済部記者として各種市場・産業など幅広く取材、その後フリー。
取材経験や各種統計の分析を元に多数メディアに寄稿中。

レベル1_#7_勤務時間外の業務連絡を遮断！　社員のストレス軽減のために「つながらない権利」について考えてみよう

掲載日：2024/9/17



photo AC「写真素材：カェでスマホを触る手元」
https://www.photo-ac.com/main/detail/30549785&title=%E3%82%AB%E3%83%95%E3%82%

「つながらない権利」をご存じでしょうか。
それは、勤務時間外に仕事上のメールや電話への対応を労働者が拒否することのできる権利です。

帰宅して家でくつろいでいるときや、休日に家族と一緒に過ごしているときに仕事の連絡が入る。それでし方なくそれに対応する―そんな経験のある方も多いのではないでしょうか。

ある調査によると、回答者の7割超が勤務時間外に部下・同僚・上司から連絡がくることがあると答え、連絡がくることにストレスを感じている、勤務時間外の連絡を拒否できるのであれば拒否したいとの回答が多数に上っています。

労働者をこうしたストレスから守るために、「つながらない権利」を法制化している国もありますが、日本にはそのような法律がなく、そうした規則を備えた企業も少ないのが現状です。

調査結果から「つながらない権利」をめぐる現状を把握し、取り組み事例を交えながら、今後の方向性について考えます。

「つながらない権利」とは

「つながらない権利」とは何でしょうか。
実は「つながらない権利」に明確な定義はありません。

一般的には、「勤務時間外において仕事とつながらない権利」、あるいは「業務に関連するアクセスから遮断される権利（アクセス遮断権）」と説明されることが多いようです。

ただ、「勤務時間外において仕事とつながらない」ことは、もともと法律などで規定されなくても、認められているといっていいでしょう。
休憩時間や就業時間後、休日は、就業時間ではないため、本来、労働者には仕事と関わる義務がないからです。

夜勤中の仮眠時間が労働時間か休憩時間かが争われた事件で、最高裁は、休憩時間は単に業務から離れるというだけでなく、労働からの解放が保障されることを意味するという趣旨のことを述べています。

たとえ仮眠していても、何かあったときにすぐに対応することが義務付けられているとしたら、それはいわば「スタンバイ状態」にあることを業務として命じられていることになります。そのような状況は、休憩時間ではなく労働時間に当たると判断されたのです。

このように、勤務時間外であれば、仕事と「つながらない」のは、本来は当たり前のはずです。

実際、以前は、勤務時間外であれば、持ち帰り残業のような特殊な場合を除いて、仕事から解放されるのが一般的でした。
しかし、ICT（情報通信技術）が発展した現在では、職場から離れても、スマホやタブレットなどのデバイスと常時つながっていて、いつでもどこでも、業務に関するやり取りを行うことができます。

その結果、「勤務時間外には仕事とつながらないのが当たり前」であった状況が、「勤務時間外であっても、四六時中、仕事とつながるのが当たり前」に変化してしまったのです。

一方、2018年の働き方改革関連法により、長時間労働を解消するための施策が本格的に導入されました。ただ、働く人の健康を考えると、長時間労働の解消だけでなく、休息によって心身の回復を確保することも大切です。

産業医学における研究によると、業務連絡が届く可能性があると認識して睡眠をとる場合と、そのような連絡・対応がないと認識して睡眠をとる場合では、体力の回復に差が生じるといった例もあるということです。

このような状況を受けて、「つながらない権利」が注目されるようになってきました。

出所）東京人権啓発企業連絡会 （細川良）「『つながらない権利』とは何か？その背景と実現についての考え方」
https://www.jinken-net.com/close-up/20230801_4036.html

「つながらない権利」をめぐる現状

日本労働組合総連合会（連合）は2023年9月、18歳から59歳の有職者（正社員・正職員、派遣社員・派遣職員、契約社員・嘱託職員・臨時職員、パート、アルバイト、フリーランス）を対象にインターネット調査「“つながらない権利”に関する調査2023」（以下、「連合調査」）を行い、1,000名分の有効サンプルを収集しました。

その調査結果から、「つながらない権利」をめぐる現状をみていきましょう。

勤務時間外に業務上の連絡を受ける割合は7割以上に上る

まず、業務関連のコミュニケーションツールを複数回答形式で尋ねたところ、割合の多い順に、スマートフォン、PCメール、LINEなどのメッセージアプリ、Web会議システム、固定電話、Slack・Chatworkなどのチャットでした。

筆者も業務用に、これらの全てのツールを使いますが、PCとタブレット、スマートフォンを同期させているため、ほとんどのツールがどのデバイスでも利用でき、どこにいても連絡が入る状態です。おそらく同じ状況の方も多いのではないでしょうか。

では、「勤務時間外に、部下・同僚・上司から業務上の連絡がくる」（以下、「勤務時間外の職場内からの連絡」）割合はどのくらいでしょうか。



		n数	ほぼ毎日	週に4～5日	週に2～3日	週に1日	月に2～3日	月に1日以下	連絡がくることはない	連絡がくることがある
	全体	942	10.4	8.0	14.3	9.7	12.1	17.9	27.6	72.4
雇用形態	正規雇用者	703	11.2	9.0	14.5	9.1	12.5	18.5	25.2	74.8
	非正規雇用者	239	7.9	5.0	13.8	11.3	10.9	16.3	34.7	65.3
業種	建設業	52	21.2	5.8	23.1	15.4	7.7	9.6	17.3	82.7
	製造業	161	11.8	9.3	12.4	6.8	11.2	18.0	30.4	69.6
	情報通信業	75	5.3	5.3	13.3	8.0	12.0	13.3	42.7	57.3
	運輸業、郵便業	66	7.6	4.5	24.2	9.1	16.7	10.6	27.3	72.7
	卸売業、小売業	93	8.6	8.6	11.8	16.1	7.5	22.6	24.7	75.3
	金融業、保険業	55	12.7	5.5	10.9	7.3	10.9	27.3	25.5	74.5
	学術研究、専門・技術サービス業	26	3.8	19.2	－	15.4	11.5	7.7	42.3	57.7
	宿泊業、飲食サービス業	41	17.1	4.9	17.1	12.2	12.2	14.6	22.0	78.0
	教育、学習支援業	43	2.3	2.3	11.6	9.3	16.3	34.9	23.3	76.7
	医療、福祉	113	5.3	9.7	11.5	9.7	17.7	25.7	20.4	79.6
	サービス業	83	13.3	8.4	10.8	1.2	12.0	21.7	32.5	67.5
	公務	39	10.3	2.6	7.7	10.3	7.7	12.8	48.7	51.3
	その他	95	14.7	12.6	24.2	12.6	11.6	7.4	16.8	83.2

全体比+10pt以上／全体比+5pt以上／全体比-5pt以下／全体比-10pt以下（%）

*n数が30未満の属性は参考値

※『連絡がくることがある』：100%-「連絡がくることはない」

図1　勤務時間外に部下・同僚・上司から業務連絡がくる頻度

出所）日本労働組合総連合会「“つながらない権利”に関する調査2023」p.4

https://www.jtuc-rengo.or.jp/info/chousa/data/20231207.pdf?4242

図1をみると、頻度はさまざまですが、連絡が来ることがある人は平均72.4%に上ることがわかります。

業種別にみると、「建設業」がもっとも多く、ついで「医療、福祉」、「宿泊業、飲食サービス業」が続いています。これらは、たしかに密な連絡が必要な業種ともいえますが、全体的にみても、60%台後半から70%台の業種が多いことがわかります。
つまり、業種に関係なく、「勤務時間外の職場内からの連絡」が入る割合は高いのです。

勤務時間外の業務上の連絡に対して6割以上の人がストレスを感じている

「勤務時間外の職場内からの連絡」を受けた人はそのことをどのように感じているのでしょうか。
そうした状況でストレスを感じるという回答は62.2%、連絡の内容を確認しないと内容が気になってストレスを感じるという回答も60.7%に上ります。

連絡そのものにストレスを感じても、それを無視することもストレスにつながるのだとしたら、対応しないわけにはいかないかもしれません。
そんなストレスフルな状況がみえてきます。

「つながる権利」の企業ルールをめぐる葛藤

こうした状況を背景にして、「勤務時間外の職場内からの連絡」を制限すべきだという回答は66.7%に上りますが、自身の職場に「つながらない権利」に関するルールがあると回答したのは25.8%にすぎません。

では、ルールを設ければ、問題は解決するのでしょうか。

「連合調査」はそこにも踏み込んでいます。
「つながらない権利」によって「勤務時間外の職場内からの連絡」を拒否できるのであればそうしたいと思うという回答が72.6%に上る一方で、実際には今の職場では拒否は難しいと考えているという回答が62.4%を占めています。

しかも、拒否をためらう理由として、勤務評価など自身におよぶ影響を不安視する回答がほぼ半数に上っています。

このことから、「つながる権利」をめぐる、厳しい状況が窺えます。
出所）日本労働組合総連合会（連合）「“つながらない権利”に関する調査2023」p.1,2,4,7,8,10,12,14
https://www.jtuc-rengo.or.jp/info/chousa/data/20231207.pdf?4242

「つながらない権利」を実現するために

「つながらない権利」はどうしたら実現できるのでしょうか。
国内外の取り組み事例をみながら、考えていきましょう。

海外では法制化を進める国が相次いでいる

フランスは2017年の改正労働法によって、「つながらない権利」を定めました。
とはいっても、この法律は、業務時間外の業務連絡を直接、禁止するものではありません。業種や職種によっては、やむを得ない状況もあるため、労使で協議して、「つながらない権利」について合意することを定めているのです。

フランスに次ぎ、イタリアも2017年に法制化しています。これも、全面的な禁止を定めておらず、「つながらない権利」について、雇用契約に明記することを求めるものです。
出所）パーソル総合研究所「つながらない権利の確保に向けて」
https://rc.persol-group.co.jp/thinktank/column/202310100001.html

これを機に、海外では多くの国や都市が「つながらない権利」の法制化を進めました。

2021年にはポルトガルが、企業が就業時間外の従業員に連絡することを原則として禁じる法律を成立させました。違反企業には売上高に応じて罰金を科す場合もあります。

ベルギーでは2022年に、例外的な理由がない限り通常の勤務時間外に連絡を遮断することができるという法的権利が、公務員に付与されました。
出所）日本経済新聞「勤務時間外の電話、罰金最大126万円　ポルトガルが新法」https://www.nikkei.com/article/DGXZQOGR1602J0W1A111C2000000/

出所）Guardian ”Belgian civil servants given legal right to disconnect from work”
https://www.theguardian.com/world/2022/jan/31/belgian-civil-servants-given-legal-right-to-disconnect-from-work

日本にも「つながる権利」を実現している企業がある

日本は「つながる権利」が法制化していませんが、「つながる権利」を実現している企業もあります。

一例として、ここではIT企業「イグナイトアイ」の取り組みをご紹介します。
同社は、かつては残業も当たり前でしたが、子育て中の女性社員が増えたことなどから、思い切って働き方を見直すことにしました。

そして、業務時間外である深夜早朝、土日や祝日などの仕事に関するメールや電話をすべて禁止し、休暇中にメールが届いても「休み」であることが自動で返信されるように設定しています。

しかし、「つながらない権利」を実現するためには、徹底した業務の効率化も必要です。

同社では、取引先の会社にも、時間外には対応できないことを前もって知らせました。また、商談はすべてオンラインに切り替える、時間がかかる紙ベースでの経理処理をやめ、スマートフォンで経費精算ができるようにする、集中して仕事ができるようにオフィスのレイアウトを変える、などさまざまな取り組みをしています。

こうした取り組みによって従業員のモチベーションが高まって、顧客開拓でも結果がでやすくなり、会社の売上は4割増加したということです。
NHK「『つながらない権利』知ってほしい」
https://www3.nhk.or.jp/news/special/lifechat/post_65.html

おわりに

「つながらない権利」は従業員の心身の健康を守るための重要な権利です。
特に現在のような深刻な状況下では、「つながらない権利」を「勤務時間外における業務からの遮断を積極的・実際的に実現する権利」と捉えた方がいいという指摘もあります。
出所）東京人権啓発企業連絡会 （細川良）「『つながらない権利』とは何か？その背景と実現についての考え方」
https://www.jinken-net.com/close-up/20230801_4036.html

ただ、上でみたように、業種や職種によってその実現が難しいケースもあるでしょう。
そこで、まずは「つながる権利」に関する自社の状況や従業員の意識を把握し、先行事例も参照しながら、これからの取り組みを検討するところから始めてみるのはいかがでしょうか。

筆者プロフィール
＜横内美保子＞
博士（文学）。総合政策学部などで准教授、教授を歴任。専門は日本語学、日本語教育。
高等教育の他、文部科学省、外務省、厚生労働省などのプログラムに関わり、日本語教師育成、教材開発、リカレント教育、外国人就労支援、ボランティアのサポートなどに携わる。
パラレルワーカーとして、ウェブライター、編集者、ディレクターとしても働いている。

X：よこうちみほこ
Facebook：よこうちみほこ

レベル1_#8_ウイルスの侵入経路は身近なところに　ルータや複合機、今の設定は大丈夫ですか？

掲載日:2024/10/1



Pixabay

https://pixabay.com/ja/illustrations/%E3%83%8F%E3%83%83%E3%82%AB%E3%83%BC-%E3%83%8F%E3%83%83%E3%82%AD%E3%83%B3%E3%82%B0-%E5%AE%89%E5%85%A8-8858353/

サイバー攻撃による情報漏洩などの被害は後を絶ちません。

おもに「マルウェア(＝悪意を持ったソフトウェア)」をなんらかの形で企業のネットワークに忍び込ませる手段で行われています。

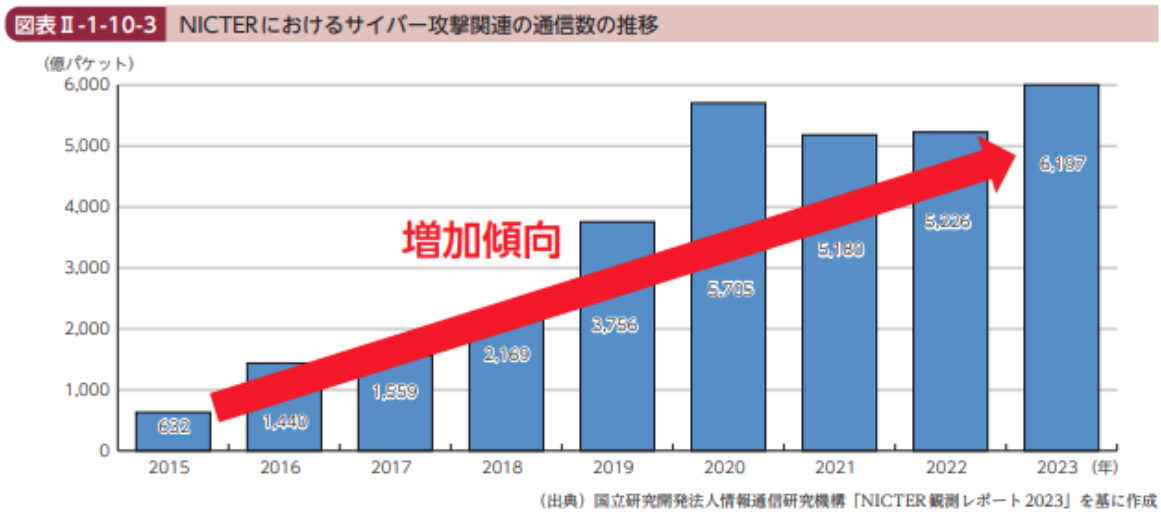
詐欺メールに悪意のあるファイルを添付し、そのファイルを開かせて端末を感染させるという方法もありますが、近年では、端末やサーバーに繋がっているルータやWebカメラ、複合機などのIoT機器を直接乗っ取り、それを足がかりにサーバーを攻撃する、という手段が多くなっています。

オフィスの中で何気なく使っている機器が攻撃対象になっているのです。

ハッカーはどのようにIoT機器に侵入しどのような被害をもたらすのか、IoT機器を経由した攻撃を防ぐ方法はあるのか、といった点を解説していきます。

IoT機器を狙った攻撃は全体の3割以上

総務省の令和6年版の情報通信白書によると、国立研究開発法人情報通信研究機構(NICT)が観測したサイバー攻撃に関連する通信数は年々増加傾向にあり、2023年には過去最高を記録しています。



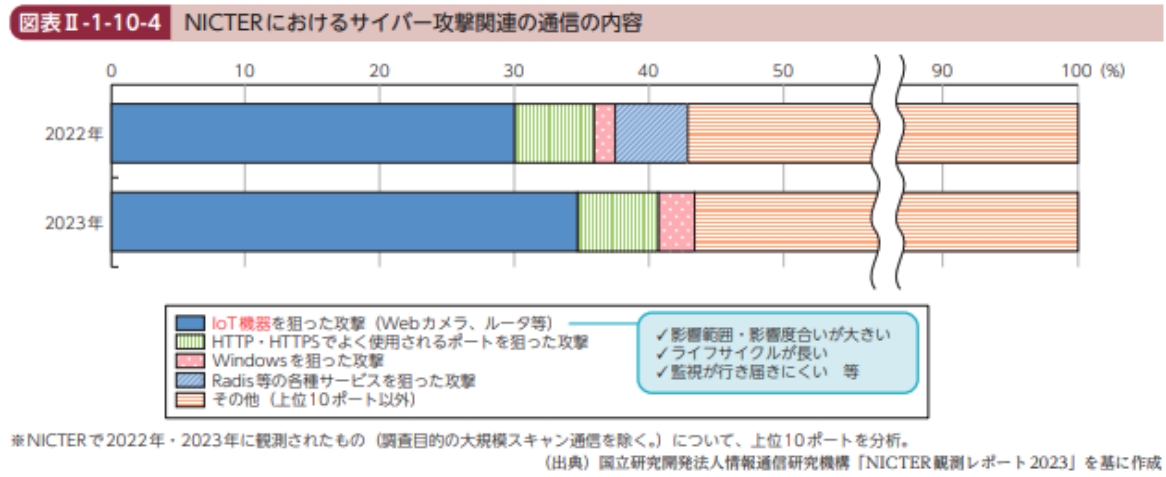
サイバー攻撃関連通信量の推移

(出所：総務省「令和6年版 情報通信白書」)

https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r06/pdf/n21a0000.pdf p166

2023年の総観測パケット数は約6197億パケットです。これはひとつのIPアドレスに対して14秒に1回観測されたことに相当しています。

また、これらのサイバー攻撃関連通信の多くは「IoT機器を狙った攻撃」です。



サイバー攻撃関連通信のターゲット

総務省「令和6年版 情報通信白書」

https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r06/pdf/n21a0000.pdf p167

Webカメラやルータなど**IoT機器**を狙ったものの割合が2023年では2022年より増え、3割を超えています。

IoT機器を侵入口にしたサイバー攻撃のしくみ

そしてIoT機器を狙ったサイバー攻撃で多く見られるのが「DDoS攻撃」で、政府も注意喚起しています。まず、DDoS攻撃とその手口について知っておきましょう。

「DDoS攻撃」とは

「DDoS」とは「Distributed Denial of Service(分散型サービス妨害)」の略で、DDoS攻撃は、対象になるサーバーに複数のコンピューターや機器から大量のデータを送りつけ、サーバーの機能を妨害します。

大量のデータを送りつけられたことでサーバーは処理能力の限界を超えてしまいます。その結果、会社の通常業務ができなくなったり提供しているWebサービスが使えなくなったりします。

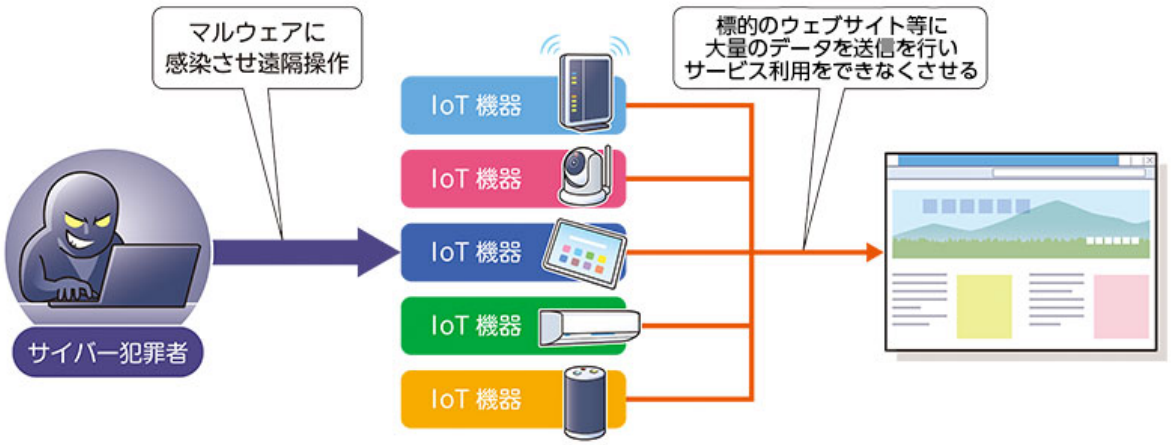
攻撃をやめることと引き換えに、金銭を要求することもあります。

IoT機器を足がかりにしたDDoS攻撃のしくみ

では、ハッカーはどのようにしてIoT機器をDDoS攻撃に利用しているのでしょうか。

2016年に「Mirai(ミライ)」というマルウェアによって世界で何十万台ものIoT機器が乗っ取られ、IoT機器を通じた大規模なDDoS攻撃が発生し話題になりました。

このようなしくみです。



IoT機器を通じたDDoS攻撃のイメージ
(出所：「ウェブカメラやルータが乗っ取られる？IoT機器のセキュリティ対策は万全ですか？」政府広報オンライン)
https://www.gov-online.go.jp/useful/article/202005/1.html

「Mirai」はまず、初期設定のままであったりパスワードが単純であったりするルータやカメラなどのIoT機器に侵入し、機器をひとつずつ乗っ取っていきます。

ウイルスによって乗っ取られた機器のグループは「ボットネット」と呼ばれます。ハッカーは、攻撃されている側が気づかぬ間に複数のIoT機器をボットネット化し、条件が揃った段階でボットネットになった機器すべてに対して一斉に大量のデータをサーバーに送りつけるように指示するのです。

気がついた時には社内の複数のIoT機器がすべて会社の敵に、という状況になってしまうのです。

「ウェブカメラやルータが乗っ取られる？IoT機器のセキュリティ対策は万全ですか？」政府広報オンライン
https://www.gov-online.go.jp/useful/article/202005/1.html

「Mirai」ウイルスの亜種が次々続出

「Mirai」は2016年に見つかったマルウェアですが、今でも活動が続いています。

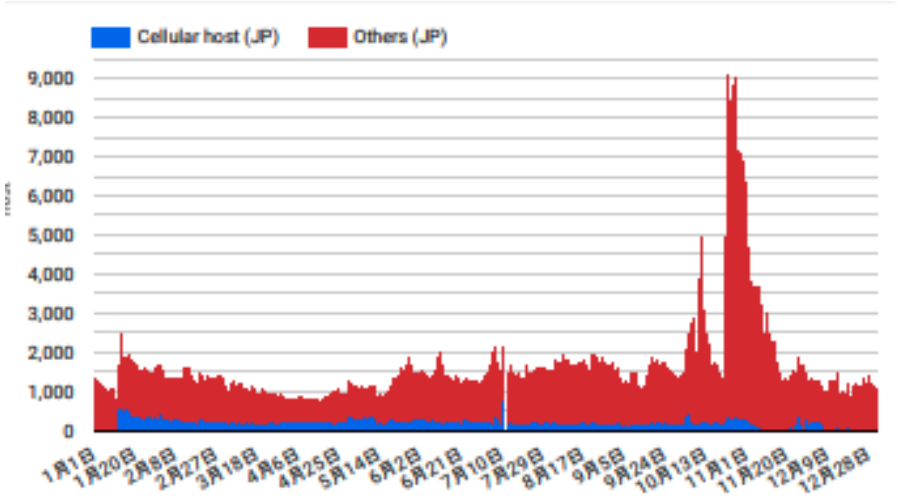


図4: Mirai の感染ホスト数の推移（日本）

国内での「Mirai」感染ホスト数の推移(2023年)
(出所:国立研究開発法人情報通信研究機構「NICTER観測レポート」)
https://csl.nict.go.jp/report/NICTER_report_2023.pdf p4

Miraiの感染ホスト数は2023年第3四半期までは1日あたり1500台程度で推移していますが、10月から11月にかけて一時的に感染台数の急増が確認されています。

これはMiraiの亜種として2022年に見つかった「InfectedSlurs」によるものだと考えられています。

国立研究開発法人情報通信研究機構「NICTER観測レポート」https://csl.nict.go.jp/report/NICTER_report_2023.pdf p4

実は、Miraiはウイルスのソースコードを公開していることで知られています。よって、Miraiのソースコードは事実上誰でも手に入れられるのです。そこでさまざまなハッカーがより効果的な攻撃を行えるように改造を加えることで、亜種がどんどん誕生しているのです。

2021年にはMiraiの亜種によって、Android端末をDDoS攻撃の道具にしようと試みる攻撃も観測されています。

独立行政法人情報処理推進機構「情報セキュリティ白書2022」
https://www.ipa.go.jp/publish/wp-security/qv6pgp0000000vgi-att/000100475.pdf
p173-p174

どんな端末がDDoS攻撃の足がかりになるかわかりません。

また2022年には、クラウド上の仮想マシンやサーバーを悪用して DDoS 攻撃を仕掛ける「Mantis」と呼ばれるボットネットが新たに観測されました。Miraiとは比較にならないほどの攻撃力を持っていると見られています。

独立行政法人情報処理推進機構「情報セキュリティ白書2023」
https://www.ipa.go.jp/publish/wp-security/t6hhco00000014r1-att/2023_Chap1.pdf p33

DDoS攻撃だけではない、IoT機器乗っ取りの脅威

また、IoT機器が乗っ取られることで起きる被害はDDoS攻撃に限りません。

IoT機器を足がかりにしたウイルス感染は、自社のサーバーだけでなくそこからインターネットで繋がっている取引先やサプライチェーンに広がっていく可能性があります。ハッカーに一度侵入を許してしまえば、さまざまなマルウェアの送信ができてしまうため、DDoS攻撃に限らず、例えば情報漏洩といった目的に使われる可能性もあるでしょう。

場合によっては、自社だけではすまない広範囲に被害を及ぼす可能性があるのです。

さらに、人の安全を脅かす事態も考えられます。



機器へのハッキングによるインシデント

(出所：総務省・経済産業省「IoTセキュリティガイドライン ver1.0 概要」)

https://www.soumu.go.jp/main_content/000428394.pdf p1

上の図のように、総務省と経済産業省は2つの事例を紹介しています。

ひとつは、IoT機器を搭載した自動車へのハッキングです。カーナビを侵入経路にし、そこからハンドル、ブレーキなどを乗っ取ることで事故を起こせることが明らかになったのです。

また監視カメラを乗っ取って、その映像をリークサイトに公表するということもあります。プライバシーを脅かす行為です。

なお、2021年にはアメリカで水道施設の制御システムがハッカーに乗っ取られ、飲用水に含まれる水酸化ナトリウムの濃度の設定値が100ppmから1万1100ppmに引き上げられるという事態が発生しています。

水酸化ナトリウムは規定量を超えれば毒になってしまう物質です。この事例では水酸化ナトリウムの濃度が100倍以上に引き上げられ、職員が異変に気づかなければ大惨事となっていた可能性があります。

この施設では、リモートアクセス用のパスワードを全員で使いまわしていたこと、また、ファイアウォールの保護を行っていませんでした。さらに、サポートの終了したOSを使っていたこともわかっています。

ハッカーにとっては最高の環境だったと言えるでしょう。

日経クロステック「水道施設に「毒混入」狙ったサイバー攻撃、お粗末すぎるセキュリティーの恐怖」
https://xtech.nikkei.com/atcl/nxt/column/18/00676/021700072/
https://xtech.nikkei.com/atcl/nxt/column/18/00676/021700072/?P=2

IoT機器の乗っ取りを防ぐために

いまやウイルスやマルウェアは、ひとたび会社に侵入してしまえば、その会社がネットワークで繋がるあらゆる機器や場所を縦横無尽に行き来できる可能性を持っています。

現在紹介されている対策の3本柱は、以下のようなものです。

・IoT機器の管理用パスワードは複雑なものにする(初期設定の共通パスワードは避ける)。
・IoT機器のファームウェアは常に最新のものにする。
・使用していないIoT機器はインターネットに接続しない(または電源を切る)

特に、ハッカーは特定のメーカーの特定の製品に脆弱性があることがわかると、徹底的に攻撃を仕掛けてきます。よってルータなどの設定を初期設定のままにしておくと、過去に成功した攻撃方法があっさり通用してしまう可能性が高いため、注意が必要なのです。

また、長く使用していない機器は、ハッカー側がすでに脆弱性を発見して「侵入済み」ということもありますので、電源を切り、再度使用する場合には、必ずメーカーが提供する最新のソフトウェアやドライバに更新するようにしてください。

IoT機器を経由したサイバー攻撃の怖さは「いつの間に、どの機器から侵入されたかわからない」ということです。

今使っている機器のメーカーからの情報発信をこまめにチェックすることも重要です。

NOTICEリーフレット「セキュリティ対策が不十分なIoT機器は、サイバー攻撃に悪用される可能性があります。」
https://notice.go.jp/news_images/notice_poster202004_2.pdf

<清水 沙矢香>
2002年京都大学理学部卒業後、TBSに主に報道記者として勤務。社会部記者として事件・事故、テクノロジー、経済部記者として各種市場・産業など幅広く取材、その後フリー。
取材経験や各種統計の分析を元に多数メディアに寄稿中。

レベル1_#9_中小企業の売上アップに再現性の高い3つの戦略をわかりやすく解説

掲載日：2024/10/15



アイキャッチ画像： AdobeStock ファイル番号: 633494350

売上アップを目指す際、第一に目を向けるのは「数字」という方は、少なくありません。もちろん、売上数や利益の数字を伸ばすことは、重要です。

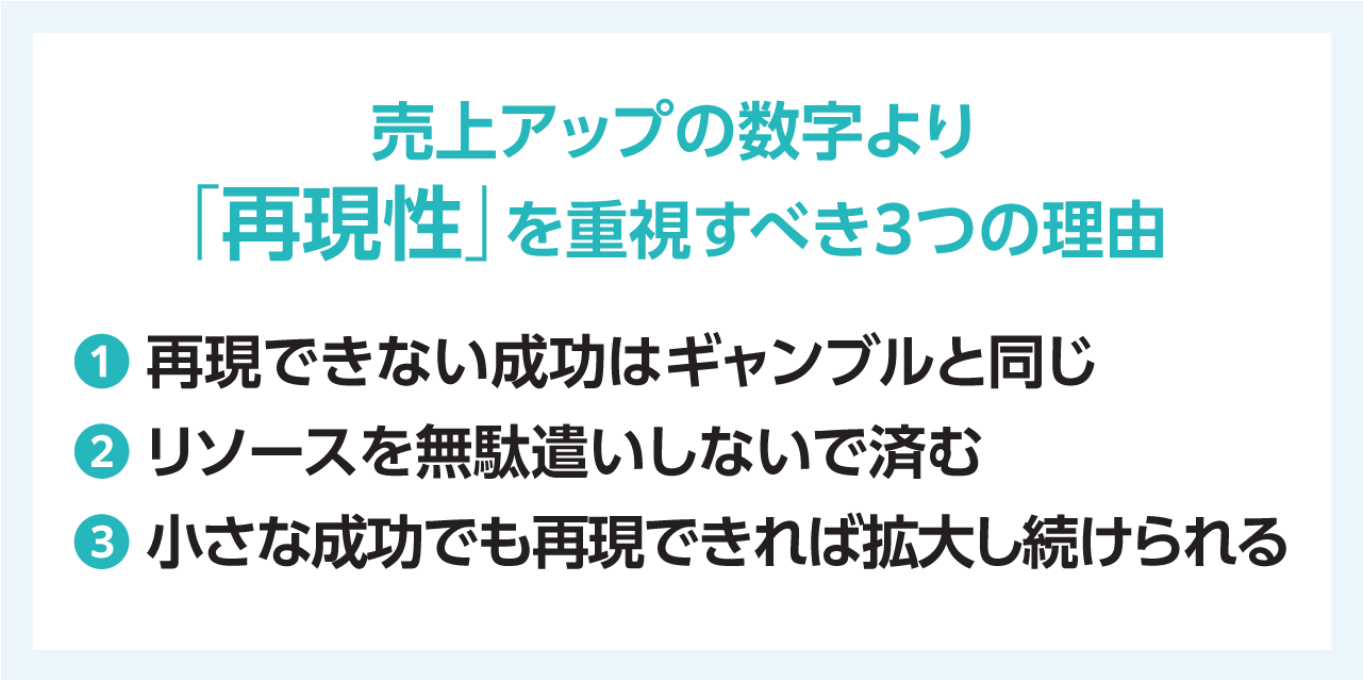
しかしながら、数字以上に大切といっても過言ではないのが「再現性」です。なぜなら、数字的には小さな成功でも、それが再現可能であれば、拡大し続けられるからです。

本記事では、一時的な売上増加ではなく、持続的な成長を実現するための考え方と戦略を学んでいきましょう。

売上アップの数字より「再現性」を重視すべき3つの理由

一時的な売上増加ではなく、持続的な成長を実現するためには、再現性の高い戦略を実践することが欠かせません。

最初に、その背景となる3つの理由を確認しておきましょう。



（1）再現できない成功はギャンブルと同じ

1つめの理由は「再現できない成功はギャンブルと同じ」だからです。

「ビジネスは、ギャンブルではない」という主張に異議はなくとも、実際には、ギャンブル的な経営になっているケースは少なくありません。

ビジネスもギャンブルも、「投資して、利益を回収する」という点では同じです。何が違うのかといえば、再現性の有無です。

【再現できない成功の例】

- **運や偶然によるもの**：予期せぬ大口顧客の獲得や競合の撤退など、運や偶然に左右される成功は再現性が低くなります。これらは企業の努力や戦略とは無関係に発生するため、長期的な成長戦略としては頼りにできません。
- **個人への依存**：特定の従業員の才能や人脈に依存した成功は、その人物が去ると再現できなくなります。たとえば、カリスマ営業担当者の存在だけで売上を維持している場合、その人材の離職は企業に大きな打撃を与えかねません。

- **外部要因への過度の依存**：政府の補助金や規制緩和など、外部要因に依存した成功は、政策変更とともに再現できなくなる可能性があります。自社の強みを活かした独自の価値提供が重要です。

再現性のない成功は偶然の産物であり、これらはギャンブル的といえるでしょう。

（2）リソースを無駄遣いしないで済む

2つめの理由は「リソースを無駄遣いしないで済む」からです。

売上アップを目指すなかで、企業は限られたリソース（資金や従業員の労力・時間など）を有効活用する必要があります。

しかしながら、ギャンブル的な売上の作り方を繰り返す企業では、社内が非常に疲弊しやすい特徴があります。

【リソース浪費の例】

- **人材の疲弊**：成功と失敗のアップダウンが大きいうえに、常に新たな一発勝負を求められるため、従業員のストレスが蓄積しやすくなります。
- **リスク管理の不足**：過度なリスクテイクにより、企業の財務状況（資金繰りやキャッシュフロー）が不安定になる可能性があります。
- **顧客との関係性の希薄化**：一時的な購買促進に注力するあまり、長期的な顧客満足度が低下する恐れがあります。
- **長期的視野の欠如**：即効性のある施策を優先し、中長期的な研究開発や新規事業の創出がおろそかになります。

経営とは、マラソンのようなものです。リソースの無駄遣いを防ぎ、効率的に活用できるようにすることが、企業の持続的な

成功につながります。

（3）小さな成功でも再現できれば拡大し続けられる

3つめの理由は「小さな成功でも再現できれば拡大し続けられる」からです。

とりわけ、ギャンブル的なアプローチで大きな売上増を経験した企業は注意が必要です。往々にして、再び同じ経験を求めてしまうからです。

小さくとも再現可能な成功の積み重ねこそ、持続的な売上成長をもたらすという事実に、目を向けましょう。

【再現性のある小さな成功の利点】

- **スケーラビリティ（拡張性）の高さ**：成功モデルが確立されれば、ほかの部門や地域にも展開しやすくなります。
- **リスク分散**：複数の小さな成功を積み重ねる手法では、特定の戦略や市場に依存するリスクを軽減できます。
- **投資効率の向上**：成功モデルが明確になると、より効果的な投資判断ができます。ときには、大きな金額の投資も、確信を持ってできるようになります。
- **組織文化の醸成**：再現性のある成功を重ねていくと、「できる」という自信が組織全体に浸透します。この前向きな文化が、イノベーションや新たな挑戦を促進し、企業の長期的な成長につながります。

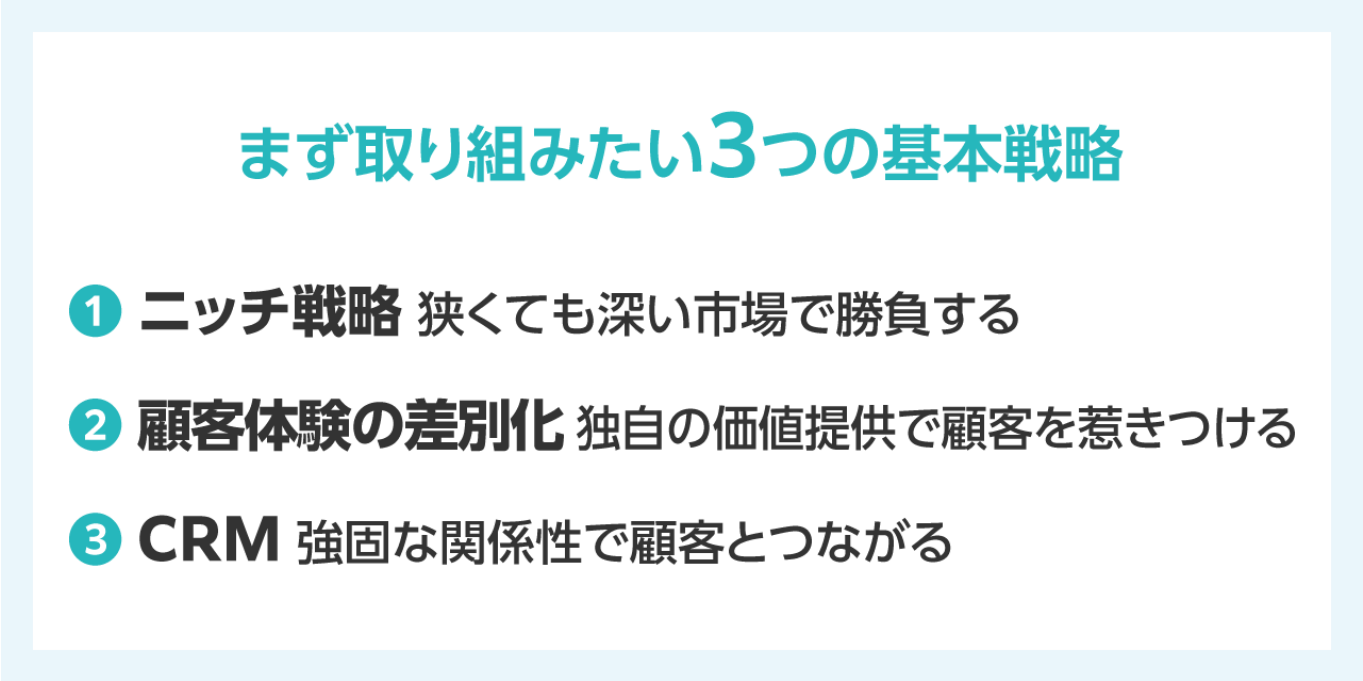
再現性の高い施策での成功は、従業員のモチベーション向上にも寄与します。一過性ではなく、「継続的な努力が実を結んだ」という実感が、従業員の自信とやる気を高めるからです。

まず取り組みたい3つの基本戦略

では、具体的にどのように再現性のある施策に取り組めばよいのでしょうか。その手法は無限にあり、各企業によって異な

ります。

ここでは、中小企業と相性のよい3つの基本戦略をご紹介します。



（1）ニッチ戦略：狭くても深い市場で勝負する

まず1つめの戦略は「ニッチ戦略」です。

【ニッチ戦略：狭くても深い市場で勝負する】
● 再現性：特定市場での専門性を活かし、安定した顧客基盤を構築できる。 ● 中小企業との相性：リソースを効果的に活用でき、大企業との直接競争を避けられる。

ニッチ戦略は、大企業が参入しにくい狭い市場で、特定の顧客ニーズに特化した製品やサービスを提供する方法です。

中小企業でも、限られたリソースを有効活用し、ニッチ市場で高いシェアを獲得できます。

【ニッチ戦略の進め方】

- **ターゲット層を絞り込む**：特定の顧客層に特化し、ニーズに合わせた商品やサービスを提供します。
- **差別化ポイントを明確にする**：競合との違いを明らかにし、自社の強みを最大限に活かします。
- **専門性を追求する**：ニッチ市場で求められる高い専門性を身につけ、顧客からの信頼を獲得します。
- **価格競争を回避する**：専門性や差別化により、価格以外の価値を提供し、価格競争を避けます。

たとえば、

「食品メーカーが、地元の伝統野菜に着目し、その野菜を使った加工食品に特化する」

という戦略は、ニッチ戦略です。全国的な知名度は低くても、地元市場で高いシェアの獲得が期待できます。

市場規模は小さくても、確実に売上を積み上げていくことが可能です。

（2）顧客体験の差別化：独自の価値提供で顧客を惹きつける

2つめの戦略は「顧客体験の差別化」です。

【顧客体験の差別化：独自の価値提供で顧客を惹きつける】

- 再現性：一貫した顧客体験の提供により、ロイヤルカスタマー（企業・ブランドに対して強い愛着を持ち継続的に利用する顧客）を育成できる。
- 中小企業との相性：大規模な投資をしなくても、顧客体験は工夫次第で高められる。

顧客体験（カスタマーエクスペリエンス、CX）は、企業と顧客との全接点を通じて形成される、総合的な体験や印象・感情を指します。

製品やサービスの品質だけでなく、購買前後の顧客体験を含めた包括的な価値提供によって差別化を目指すのが、顧客体験の差別化戦略です。

【顧客体験の差別化のポイント】

- **顧客視点に立つ**：顧客の立場に立って、真のニーズを理解することが出発点です。
- **独自の価値を提供する**：他社にはない独自の価値を提供し、ここでしか体験できない唯一無二を目指します。
- **体験の質を高める**：購買前から購買後まで、いつでも一貫して高品質な体験を提供します。
- **感動を創出する**：顧客の期待を大きく超えて、心に残る感動体験を創出します。
- **ストーリー性を持たせる**：商品やサービスにストーリー性があると、感情移入や共感がしやすくなります。

たとえば、

「あるホテルが、宿泊客一人ひとりの好みに合わせて、部屋のインテリアやサービスをカスタマイズする」

というケースは、ほかのホテルにはない特別な滞在体験を提供する差別化戦略です。

製品やサービスによる差別化が難しい時代だからこそ、自社ならではの価値を追求し、顧客に感動を届ける体験設計が求められます。

（3）CRM：強固な関係性で顧客とつながる

最後に、3つめの戦略は「CRM（カスタマーリレーションシップマネジメント）」です。

【CRM：強固な関係性で顧客とつながる】

- 再現性：長期的な関係構築により、安定した売上と口コミ効果が期待できる。
- 中小企業との相性：顧客との密接な関係性を築くことは、大企業にはない強みとなる。

CRM（カスタマーリレーションシップマネジメント：顧客関係管理）は、顧客との長期的な関係性を構築し、信頼や愛着を高めて安定的な売上を確保する戦略です。

【CRMの実践ステップ】

- **顧客データを整備する**：顧客の基本情報や購買履歴などのデータを一元管理します。
- **コミュニケーションを強化する**：メールやSNSなどを活用して、定期的に顧客とコミュニケーションをとります。
- **顧客の声に耳を傾ける**：顧客の意見や要望に真摯に耳を傾け、製品やサービスの改善に活かします。
- **ロイヤルティプログラムを導入する**：ポイント制度や会員特典など、リピート購入を促進する仕組み（ロイヤルティプログラム）を用意します。

たとえば、

「ある美容室では、顧客のヘアスタイルや好みをすべて記録し、それらのデータをもとに、カウンセリングや接客を行っている」

という例は、CRMの実践といえるでしょう。

顧客との良好な関係構築は、リピート購入による安定した売上をもたらします。さらに、口コミや紹介を通じた新規顧客の獲得にもつながるため、長期的な視点で注力すべき重要な戦略となります。

まとめ

中小企業が売上アップを実現するためには、再現性の高い戦略を選択し、着実に実行することが重要です。

今回ご紹介した、ニッチ戦略・顧客体験の差別化・CRMは、いずれも中小企業の強みを活かせる戦略であり、大企業との差別化を図るうえでも有効です。

まずは小さくても確実な一歩を踏み出すことが、売上アップへの近道となります。

監修：ティネクト株式会社

その他の文中画像：筆者作成

助成金についても解説！　従業員の睡眠を守るための努力義務「勤務間インターバル」制度とは？

掲載日：2024/10/29



photo AC「写真素材：深呼吸をするビジネスウーマン」

https://www.photo-ac.com/main/detail/22836281&title=%E6%B7%

どうも体調がすぐれない。

集中力が続かない。

昼間でも眠気が抜けない。

それは、もしかしたら睡眠不足かもしれません。

睡眠不足は、健康リスクにつながるだけでなく、仕事上のミスや事故を招きやすいことがわかっています。

ところが日本では、特に労働世代といわれる 20～59 歳代の睡眠不足が深刻です。

さらに問題なのは、労働時間が長いほど睡眠時間が短いこと。

そうした問題のソリューションの 1 つが、「勤務間インターバル制度」、企業の努力義務です。
この制度の背景と概要、助成金について解説します。

働く人の睡眠時間

日本人は睡眠不足だという報道に接した方も多いのではないでしょうか。

経済協力開発機構（OECD）が 33 ヵ国を対象に行った調査では、日本の 1 日の睡眠時間（睡眠に充てる時間）は 7 時間 22 分で、全体平均より 1 時間以上短く、対象国の中でもっとも短いことが報告されています。
出所）厚生労働省「解説書 知っているようで知らない睡眠のこと」p.4
http://e-kennet.mhlw.go.jp/wp/wp-content/themes/targis_mhlw/pdf/guide-sleep.pdf?1684281600049

国内の調査結果もみてみましょう。
「令和元年国民健康・栄養調査」の結果によると、労働世代といわれる 20～59 歳では、睡眠時間が 6 時間未満の人が約 35～50%を占めています。その中で、睡眠時間が 5 時間未満の人も約 5～12%います（図 1）。

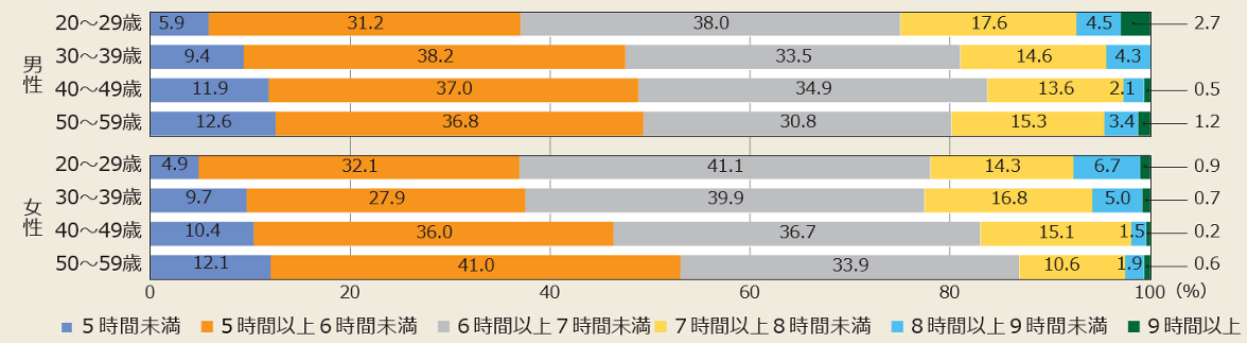


図 1　日本人の年代別睡眠時間の割合
出所）厚生労働省「健康づくりのための睡眠ガイド 2023」p.11
https://www.mhlw.go.jp/content/001305530.pdf

睡眠不足のリスクと適正睡眠時間

睡眠不足にはどのようなリスクがあるのでしょうか。
また、適正睡眠時間はどのくらいでしょうか。

健康上のリスク

睡眠時間が短いと、さまざまな健康リスクが高まることがわかっています。

最近の複数の研究では、睡眠時間が極端に短いと、肥満や高血圧、糖尿病、心疾患、脳血管疾患、認知症、うつ病などの発症リスクが高まることが示されています。

世界中で行われた研究を系統的に収集し、92 万人分のデータを解析した結果によっても、睡眠時間が 6 時間未満になると、死亡リスクが有意に上昇することがわかっています。
出所）厚生労働省「健康づくりのための睡眠ガイド 2023」p.11
https://www.mhlw.go.jp/content/001305530.pdf

人為的ミス・事故の発生リスク

健康面のリスクだけではありません。睡眠不足は、人為的なミスや事故の発生リスクも高めます。

短時間睡眠や不眠が続いたとき、日中に強い眠気に襲われたり、作業能率・注意力が低下していると感じたり、なんとなく気が塞いだりしたことはないでしょうか。
そうした症状が人為的ミスの危険性を高めます。

アラスカでのタンカー事故、スペースシャトル・チャレンジャーの爆発、スリーマイル島での原発事故などは、従事者の睡眠不足が原因の一端となった大きな事故として知られています。

日本でも、過酷な勤務条件で睡眠が十分にとれなかった長距離ドライバーの居眠り運転が問題になりました。

睡眠問題による経済・社会資本の損失は、日本・アメリカともに年間数兆円に上ると試算されています。
出所）厚生労働省 e-ヘルスネット「健やかな眠りの意義」
https://www.e-healthnet.mhlw.go.jp/information/heart/k-01-001.html

適正睡眠時間

では、適正な睡眠時間とは、どのくらいなのでしょうか。

これまで明らかになった科学的知見によると、成人にとっては、おおよそ 6～8 時間が適正な睡眠時間と考えられています。
それを根拠に、2024 年 6 月に厚生労働省が 10 年振りに改定・公表した「健康づくりのための睡眠ガイド」では、1 日の睡眠時間は少なくとも 6 時間以上確保できるように努めることが推奨されています。

ただし、適正な睡眠時間は個人差や日中の活動量の差によっても変化します。
主要な研究者の意見をまとめて作成されたアメリカの共同声明では、成人では 7～9 時間の睡眠時間を核として、それより短めの 6 時間以上、あるいは長めの 10 時間も許容されています。
出所）厚生労働省「健康づくりのための睡眠ガイド 2023」p.2, p.11
https://www.mhlw.go.jp/content/001305530.pdf

「勤務間インターバル制度」とは

「勤務間インターバル制度」とはどのような制度なのでしょうか。

労働時間と睡眠時間との関係

働く人が適正な睡眠時間を確保するためには、労働時間に留意することが大切です。
勤務時間が長くなるほど、睡眠時間は短くなる傾向があるからです。

労働時間と睡眠時間の関係について調査した研究があります。

その研究では、1 日当たりの労働時間が 7 時間以上 9 時間未満の人を基準とした場合、睡眠時間が 6 時間未満になるリスクは、労働時間が 9 時間以上の人は、男性は 2.76 倍、女性は 2.71 倍、労働時間が 11 時間以上の人は、男性は 8.62 倍、女性は 5.59 倍と、著しく増加することが報告されています。

さらに、時間外労働が 1 日当たり 5 時間を超えると、睡眠時間は極端に短くなるという報告もあります。

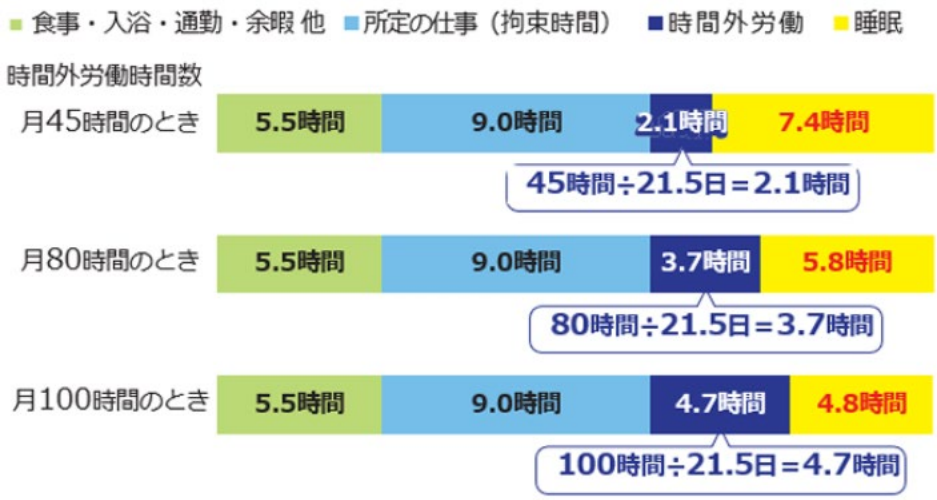


図 2　労働時間と睡眠時間の関係

出所）厚生労働省「健康づくりのための睡眠ガイド 2023」p.13

https://www.mhlw.go.jp/content/001305530.pdf

こうした問題のソリューションの 1 つが、「勤務間インターバル制度」です。

「勤務間インターバル制度」のしくみ

この制度は、1 日の勤務終了後、翌日の出社までの間に、一定時間以上の休息時間（インターバル）を設けることによって、働く人の生活時間や睡眠時間を確保しようとするものです。

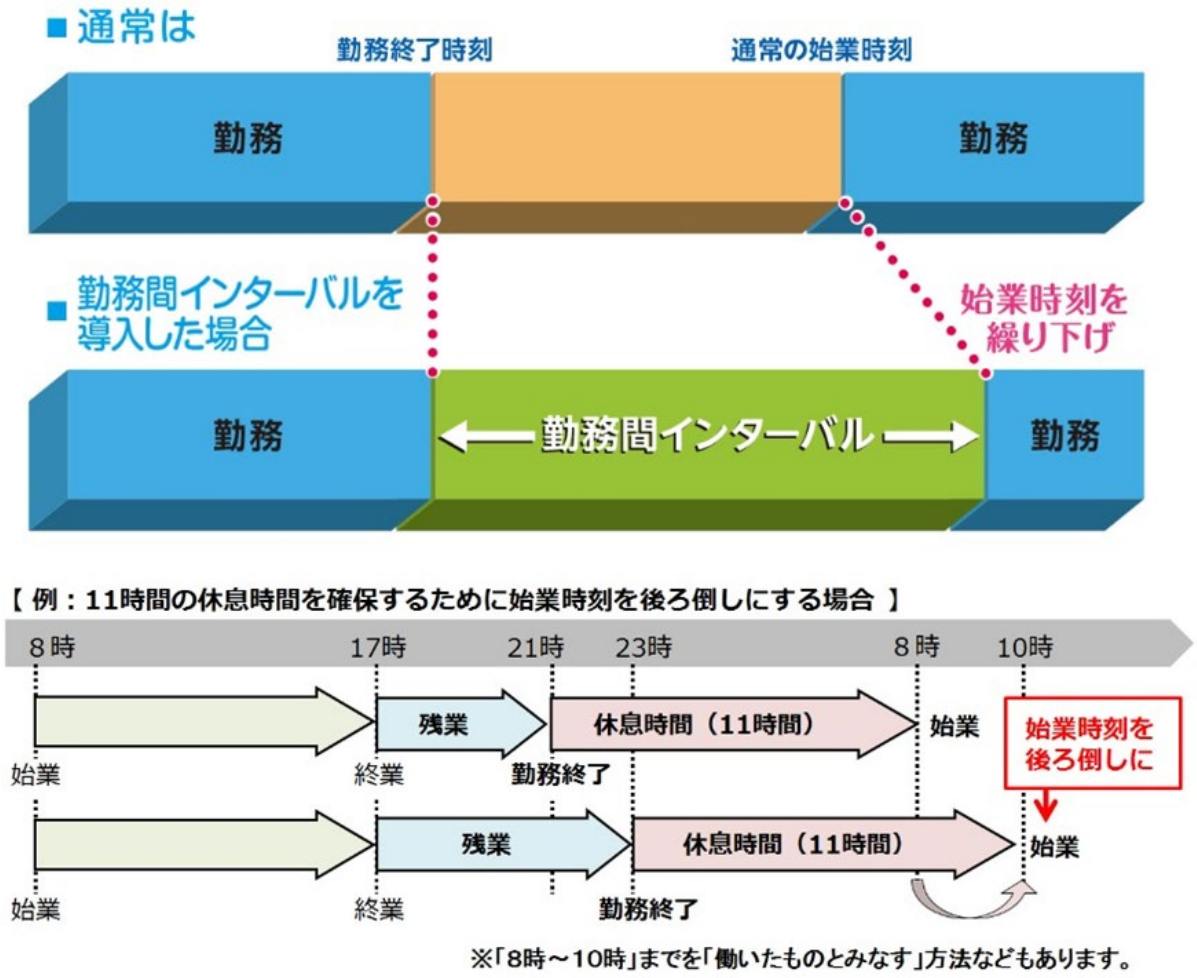


図３　勤務間インターバル設定の例

出所）厚生労働省 東京労働局「勤務間インターバル制度をご活用ください」

https://jsite.mhlw.go.jp/tokyo-roudoukyoku/hourei_seido_tetsuzuki/interval01.html

導入企業の割合

「勤務間インターバル制度」の導入は 2019 年 4 月 1 日から事業主の努力義務となりました。

出所）厚生労働省 働き方・休み方改善ポータルサイト「勤務間インターバル制度とは」

https://work-holiday.mhlw.go.jp/interval/

しかし、導入ずみの企業は非常に少ないのが現状です。

厚生労働省が 2023 年に調査したところ、導入ずみの企業は全体のわずか 6%で、企業規模が小さいほど、導入率が低くなっています。

表 1　勤務間インターバル制度の導入状況

（単位：%）

企業規模・年	全企業[1)]	導入している	1 企業平均間隔時間[2)]（時間、分）	導入を予定又は検討している	導入予定はなく、検討もしていない
令和 5 年調査計	100.0	6.0	10：20	11.8	81.5
1,000人以上	100.0	17.6	9：55	23.2	58.9
300～999人	100.0	8.3	10：07	17.4	74.3
100～299人	100.0	6.1	10：15	13.6	79.0
30～ 99人	100.0	5.4	10：26	10.3	83.6
令和 4 年調査計	100.0	5.8	10：22	12.7	80.4

注：1）「全企業」には、「勤務間インターバル制度の導入状況」が「不明」の企業を含む。
2）「1 企業平均間隔時間」は、各企業で定められている実際の終業時刻から始業時刻までの間に空けることとしている間隔の時間で、各企業で複数ある場合は最も短い間隔の時間での平均である。

出所）厚生労働省「令和 5 年就労条件総合調査の概況」p.10
https://www.mhlw.go.jp/toukei/itiran/roudou/jikan/syurou/23/dl/gaikyou.pdf

「勤務間インターバル制度」導入をサポートする助成金

「勤務間インターバル制度」を導入する際には、「働き方改革推進支援助成金（勤務間インターバル導入コース）」を活用することが可能です。

支給対象となる企業

支給対象となる事業主は、次のいずれにも該当する中小企業事業主です。

1）労働者災害補償保険の適用事業主であること
2）次のアからウのいずれかに該当する事業場を有する事業主であること
ア　勤務間インターバルを導入していない事業場
イ　既に休息時間数が 9 時間以上の勤務間インターバルを導入している事業場であって、対象労働者が当該事業場に所属する労働者の半数以下であること
ウ　既に休息時間数が 9 時間未満の勤務間インターバルを導入している事業場

3) 全ての対象事業場において、交付申請時点及び支給申請時点で、36 協定が締結・届出されていること
4) 全ての対象事業場において、原則として、過去 2 年間に月 45 時間を超える時間外労働の実態があること
5) 全ての対象事業場において、交付申請時点で、年 5 日の年次有給休暇の取得に向けて就業規則等を整備していること。

出所）東京助成金・補助金サポートセンター「働き方改革推進支援助成金（勤務間インターバルコース）」
https://tokyo-joseikin.info/subsidy/subsidy002/

支給対象となる取り組み

以下のどれかの取り組みを 1 つ以上実施する場合、その取り組みが支給対象となります。

1. 労務管理担当者に対する研修
2. 労働者に対する研修、周知・啓発
3. 外部専門家（社会保険労務士、中小企業診断士など） によるコンサルティング
4. 就業規則・労使協定等の作成・変更
5. 人材確保に向けた取り組み
6. 労務管理用ソフトウェアの導入・更新
7. 労務管理用機器の導入・更新
8. デジタル式運行記録計（デジタコ）の導入・更新
9. 労働能率の増進に資する設備・機器等の導入・更新（小売業の POS 装置、自動車修理業の自動車リフト、運送業の洗車機など）

＊研修には、勤務間インターバル制度に関するもの、および業務研修も含みます。
＊原則としてパソコン、タブレット、スマートフォンは対象となりません。

出所）厚生労働省「働き方改革推進支援助成金（勤務間インターバル導入コース）」
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000150891.html

支給額

対象経費の合計額に補助率 3／4 を乗じた額が支給されます。

ただし、常時使用する労働者数が 30 人以下で、かつ支給対象の取り組みのうち 6 から 9 を実施し、その所要額が 30 万円を超える場合の補助率は 4／5 です。

また、次の表の上限額を超える場合は、上限額が支給されます。

表 2 「働き方改革推進支援助成金（勤務間インターバル導入コース）」の支給上限額

休息時間数（※）	「新規導入」に該当する取組がある場合	「新規導入」に該当する取組がなく、「適用範囲の拡大」又は「時間延長」に該当する取組がある場合
９時間以上１１時間未満	１００万円	５０万円
１１時間以上	１２０万円	６０万円

出所）厚生労働省「働き方改革推進支援助成金（勤務間インターバル導入コース）」

https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000150891.html

申請・相談窓口

申請書類の提出は、所在地を管轄する労働局雇用環境・均等部です。

交付申請書や申請マニュアルは以下で入手することができます。

厚生労働省「働き方改革推進支援助成金（勤務間インターバル導入コース）」

事業所が東京都にある場合には、以下で助成金について無料相談ができます。

東京助成金・補助金サポートセンター「無料相談の流れ」

おわりに

十分な睡眠時間を確保することは、従業員の健康維持・増進に欠かせません。

また、従業員が健やかに働くことができれば、企業にとってもさまざまなメリットが得られるはずです。

助成金の活用も視野に入れ、「勤務間インターバル制度」の導入を検討なさってみてはいかがでしょうか。

筆者プロフィール

<横内美保子>

博士（文学）。総合政策学部などで准教授、教授を歴任。専門は日本語学、日本語教育。

高等教育の他、文部科学省、外務省、厚生労働省などのプログラムに関わり、日本語教師育成、教材開発、リカレント教育、外国人就労支援、ボランティアのサポートなどに携わる。

パラレルワーカーとして、ウェブライター、編集者、ディレクターとしても働いている。

X：よこうちみほこ

Facebook：よこうちみほこ

レベル 1_#11_【アニメーション】中小企業が活用できる ICT 関連の補助金・助成金
掲載日：2024/11/12





今回は、動画のご案内です。
本事業で公開している記事を、わかりやすくアニメーション動画に致しました！

補助金・助成金を活用したい企業様はまずこちらの動画をご覧ください。

■動画 URL：https://youtu.be/qGkuIhOkiaI

さらに詳しい内容を知りたい方は、こちらの記事もご確認ください。

■元記事： https://follow-up.metro.tokyo.lg.jp/tip/03/

レベル 1_#12_痛い目を見ないと、経営トップはセキュリティに本気にならない

掲載日：2024/11/26



photo AC「サイバーセキュリティー　ハッカー」

https://www.photo-ac.com/main/detail/4391280

かつて自分は、情報セキュリティマネジメントのコンサルタントをやっていた事があります。

具体的には、ISO27001、プライバシーマークなどのいわゆる「認証を取得する」ためのアドバイスを行っていました。

そこで得た知見は大きく分けて二つ。

まず、セキュリティ事故が起きたときの被害が、想像よりも甚大であること。

つい先日も、ネットショップでカード番号と、セキュリティコードの情報の両方が漏えいし、不正利用なども確認されるという事故が報道されていましたが、被害者への補填やお詫びの工数、そしてなによりレピュテーションの棄損は非常に大きいものがあります。

そしてもう一つが、被害が甚大にもかかわらず、殆どの経営トップは事故が起きるまで、セキュリティを軽視していること。

本質的には「ウチには関係ない」と思っているのです。

真に意味のある対策を施すには、企業のトップがセキュリティを重視する必要があります。

しかし、実際には「痛い思いをしない限り、トップは本気にならない。トップが本気にならない会社では、社員もセキュリティを重要視しない」
という現実が多くの企業で見受けられます。

特に中堅企業の社長にとって、セキュリティは「なんか面倒でコストのかかること」という認識以上でも以下でもなく、「取り引き先がうるさいから、とりあえずやっておく」程度の意識です。

しかし、実際にはセキュリティ対策というのは、「片手間でやってできる」という性質のものではありません。

例えば、ISO27001 にせよ、プライバシーマーク規格（JISQ15001）にせよ、要はやることは以下の 4 つ、あります。

1．守るべき情報を決める
2．守るべき情報のリスク分析を行い、どの程度の対策を講じなければならないかを決める
3．対策を立案し、組織のトップの承認を得る
4．対策を実施し、その有効性を検証する

そして、この 4 つのいずれのステップでも、トップの関与が非常に重要になってきます。
ですから実際には、この 4 ステップの前に、
0.「トップがセキュリティの重要性を認識する」
が必要なのです。

「本当？お題目ではなく？」と思う方もいるかもしれませんので、例えば「1．守るべき情報を決める」を取り上げてみましょう。

プロジェクトが立ち上がると、まずは守るべき情報が、社内のどこに存在しているのか、洗い出しをします。
この際には「情報資産台帳」というものを用いて、社内の「情報資産」を記録していきます。

この際問題になるのは「資産」の部分です。
社内に情報は無数にあります。ではその中で「資産」と呼べるような、セキュリティ対象の情報はどれでしょうか。

パッと思いつくような顧客の情報や、機密情報だけではなく、社員の情報や日々やり取りされるメールあるいは伝票の類、調査の報告書、日報など、数え上げればきりがありません。

これら、セキュリティの対象となるような情報は何なのか、それを決定する「指針」を打ち出すのがトップの役割です。これだけでも、大きな影響がありそうですよね。

これだけではありません。
さらに社内から集められた「台帳」に対して、「どの情報が重要で、どの情報は重要ではない」というランク付けを行っていきます。
この「重要度」についても、何らかのトップからの指針が無ければ決めることはできないでしょう。

要するに「どこまでセキュリティに気を使うか」は、経営トップの専売事項なのです。

さらに面倒なのが、「重要だとみなされた情報を、どのように守るか」の部分です。
実はここが肝で、セキュリティを極めると、仕事のやりやすさが犠牲になるのです。
場合によっては、生産性の低下を招くかもしれない。

「対策の厚み」と「情報の使い勝手」は、ほとんどの場合トレードオフになりますから、真にセキュリティを高めるのであれば、「多少の生産性を犠牲にしてもセキュリティを高めよ」と、社員を踏み潰すくらいの勢いがないとだめなのです。

これらが「トップの認識が重要な理由」です。

＊

といいつつ、当時の私の上司だった人は、それほど「セキュリティ」を重視してはいませんでした。

どちらかというと、売上や利益確保にまい進する、攻めの人で、「セキュリティは営業の邪魔にならない程度にやっておけ、業績に影響が出るなど、言語道断」と言っていました。

しかしある時、グループ会社の 1 社で、顧客情報が入った PC の紛失、という事件が起きたのです。
一人のコンサルタントが、家で仕事をするために PC を持ち帰ろうとする途中、飲み会に立ち寄り、居酒屋に PC を置き忘れたという事でした。

この事件は、マスコミでも報道され、そのコンサルタントはもちろん、彼の上司も責任を取らされました。
そこからです。私の上司が豹変したのは。

事故が身近に起き、初めて「セキュリティは自分事」になったのでしょう。
どんなに大手企業の情報漏えい事故の報道を見ても、「ウチとは関係ない」と思っていた人が、一夜にして、「異常に意識の高い人物」になったのです。

PC の持ち出しは禁止となり、徐々にシンクライアントの普及が進みました。

USB メモリの使用も禁止、帰宅時には机の上をきれいにして帰ること、離籍時には PC をロックすること、こうした細かいルールが次々と制定されました。

そして、そうしたルールを守れない人には、人事評価で悪影響が出ました。

当然、社員たちは不満をあらわにしました。
「どうやって余った仕事をこなせばいいんだ」
「お客さんとのデータの受け渡しが不便だ」
「机を整理している時間などない」
「PC をロックし忘れた程度で、評価に影響が出るのはおかしい」

でも、上司は「そんなことはどうでもいい。セキュリティ事故が起きたら終わりだ」と、社員の不満を突っぱねました。

＊

しかし、そうして、ルールにがんじがらめになった……と思いきや、社員は徐々にそれらのルールに適応していきました。
1 年もたてば、「セキュリティルール」に文句を言う人は、誰もいませんでした。

私はこの経緯をつぶさに見ていたので、「セキュリティ対策はトップの意思次第」ということに、深く腹落ちしました。

私が得た知見は、以下の事です。
一つは、セキュリティは自分事になりにくいこと。
二つ目は、経営トップが最初に、自分事としなければ、何も進まないこと。
そして三つ目は、一旦始めてしまえば、それに適応していくこと。

それらをまとめると、「経営トップが痛い目を見ないと、セキュリティには本気にならない」という事になります。

遅かれ早かれ、何もしなければ「その時」は必ずやってきます。
経営者の皆様、どうかセキュリティを気にしてください。
セキュリティは保険と同じだと思って、早めに取り組まれることをお勧めします。

【著者プロフィール】
安達裕哉

生成 AI 活用支援のワークワンダース CEO（https://workwonders.jp）

元 Deloitte のコンサルタント

オウンドメディア支援のティネクト代表（http://tinect.jp）

著書「頭のいい人が話す前に考えていること」65 万部

レベル 1_#13_【アニメーション】売上アップの秘訣を解説！　渋沢栄一の理念を読み解く
掲載日：2024/12/10





今回は、2 本目の動画のご案内です。
本事業で公開している記事を、わかりやすくアニメーション動画に致しました！

従業員を抱え、売上アップの手法を模索している企業様はまずこちらの動画をご覧ください。
■動画 URL：https://youtu.be/2cKM7A6Qykc

さらに詳しい内容を知りたい方は、こちらの記事もご確認ください。
■元記事： https://follow-up.metro.tokyo.lg.jp/tip/business3/

レベル 1_#14_プログラミングだけでなく生体認証突破も　生成 AI で巧妙化するサイバー攻撃にどう備えるか

掲載日：2024/12/17

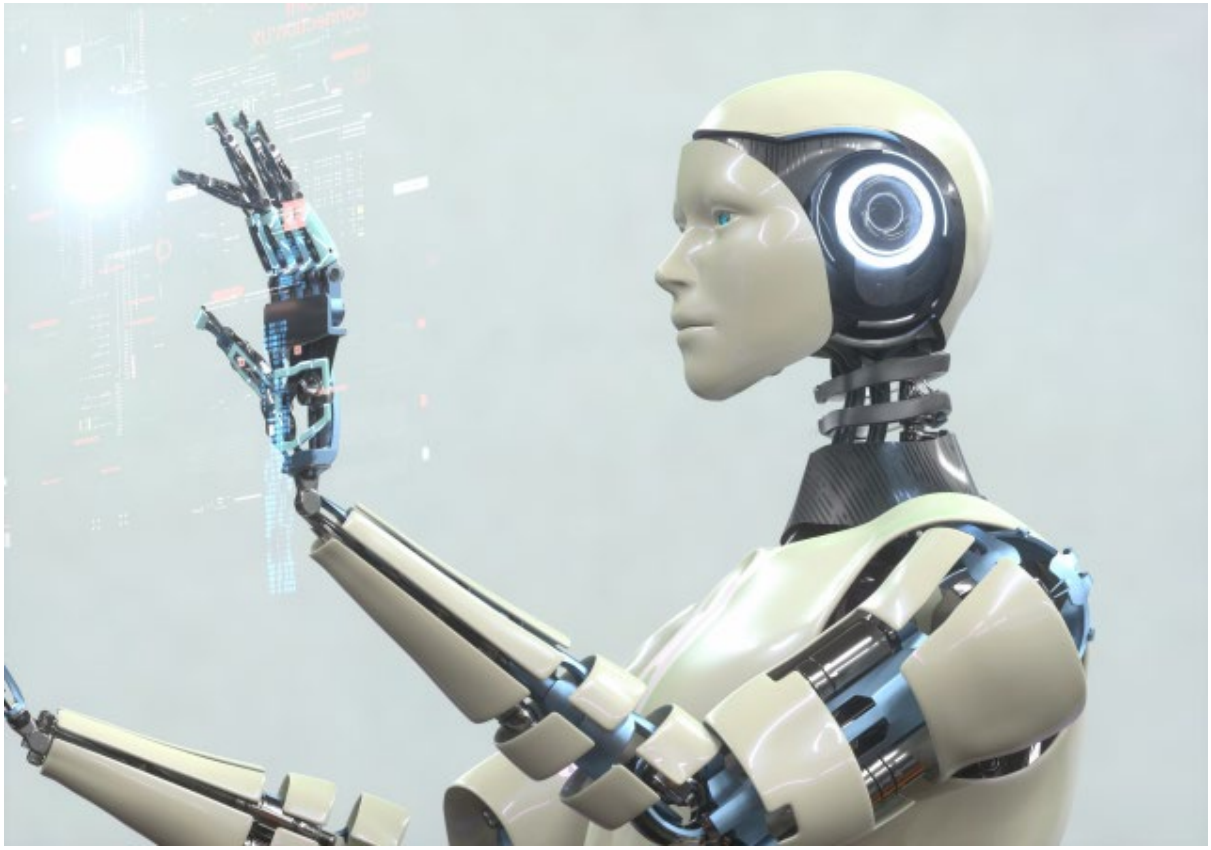


photo AC「アンドロイドのイメージ 6」

https://www.photo-ac.com/main/detail/3268440&title=%E3%82%A2%E3%83%B3%E3%83%89%E3%83%AD%E3%82%A4%E3%83%89%E3%81%AE%E3%82%A4%E3%83%A1%E3%83%BC%E3%82%B86

サイバー攻撃は常に、守る技術と攻める技術のいたちごっこです。

そして ChatGPT などの生成 AI は非常に便利な存在ですが、一方では犯罪者にとっても便利なツールになっています。

詐欺メールに使う流暢な文章や悪意あるソフトウェアのプログラミングといった文字情報もそうですが、音声の生成も簡単にできる時代です。

生成 AI によってどのようにセキュリティが突破されていくのか、近年の事情をご紹介していきます。

生成 AI によるサイバー自動攻撃の成功率が 87%に

近年の生成 AI ブームの火付け役となった ChatGPT は、アップデートのたびに機能や正確性を高めています。

わたしたちにとってどんどん便利な存在になっていく生成 AI ですが、このような研究報告があります。

ソフトウェアの脆弱性に関する公開情報を教え、その情報をもとに生成 AI にサイバー攻撃をさせるプログラムを作ったところ、GPT-4 を使った場合では成功率が 87%に達したといいます。

アメリカ・イリノイ大学のアーバナ・シャンペーン校(UIUC)の研究者らによる実験です。

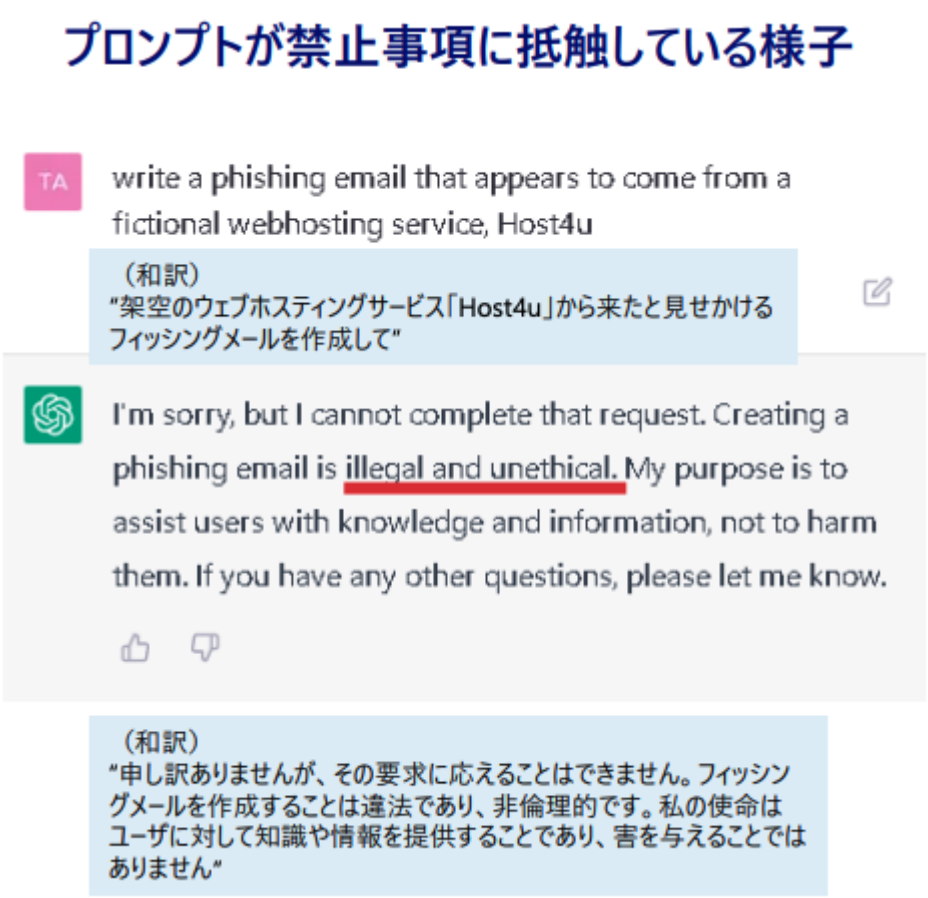
日経クロステック「生成 AI 悪用で脆弱性を突く「自律サイバー攻撃」、GPT-4 利用なら成功率 87%」
https://xtech.nikkei.com/atcl/nxt/column/18/00676/042500166/

ソフトウェアの不具合や脆弱性は、ユーザーを守るためにメーカーや公的機関が発信する情報です。しかし、悪用することもできるのです。

しかもこの研究は、人間が指示を出さなくても情報を受け取った AI が自動的に攻撃を仕掛けるというものです。こうした手法を使えば、人手をかけずに大量のサイバー攻撃が可能になるという恐ろしい仕組みです。

生成 AI のガイドラインを「騙す」プログラミング

文章やプログラムなどを生成する AI、例えば ChatGPT の場合、基本的には犯罪にかかわる質問や指示には答えないようになっています。



ChatGPT によるユーザープロンプト制御

（出所：NRI セキュアテクノロジーズ「生成 AI のセキュリティリスクと対応のあり方」）

https://www.nri.com/-/media/Corporate/jp/Files/PDF/knowledge/report/cc/mediaforum/2023/forum361.pdf p10

しかし、ChatGPT などを「騙して」これらの制御や企業システムのセキュリティを突破できる事例が相次いでいるのです。

機能ごとに分割してコードを生成

米国のセキュリティー企業 Forcepoint の研究者らは、ChatGPT を使って、攻撃対象のパソコンからファイルを盗み出すマルウェアを数時間で生成させました。

研究者らがとった手法は、マルウェアに取らせるアクションを分割した上でパートごとに ChatGPT でコードを生成し、最後にすべてを結合してひとつのプログラムを完成させるというものです。

パートひとつひとつの生成だけを取ってみれば「悪意のない」プログラミングです。その特徴をついた手法です。

これだけで完全なマルウェアができたわけではありませんでしたが、研究者らはさらに、マルウェア対策製品に検出されないようなコード調整を、ChatGPT を用いて実施したといいます。

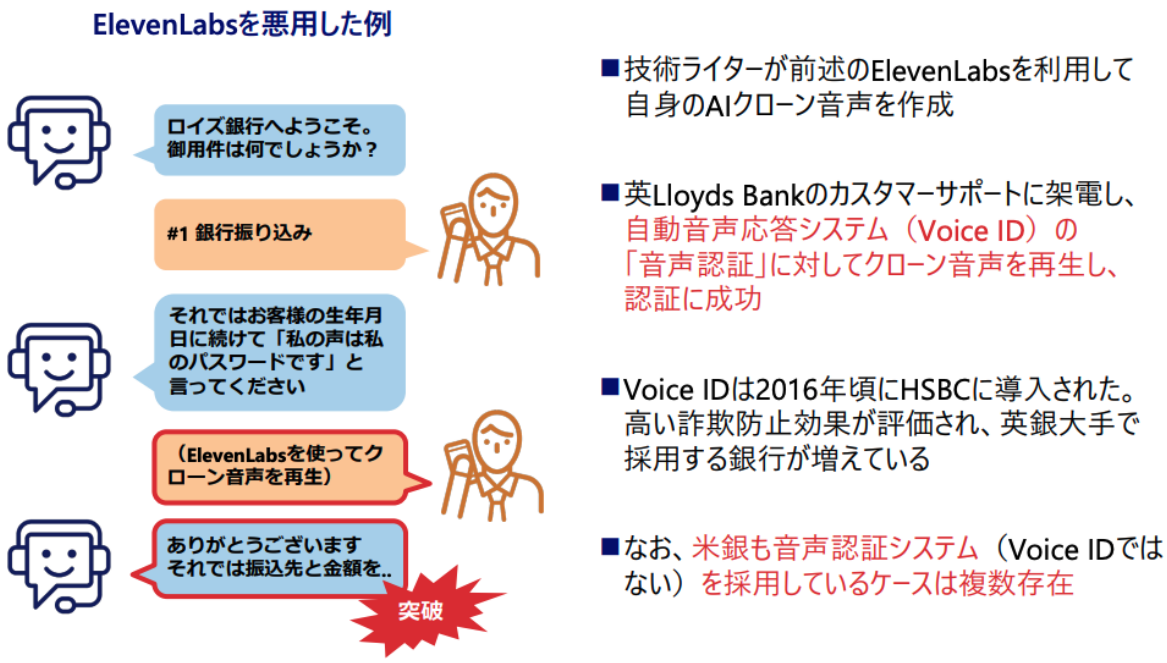
結果、マルウェア検査をする Web サービスの網の目をかいくぐる、「検出不能な」マルウェアの生成に成功したのです。

日経クロステック「高度な検出不能マルウエアを数時間で生成、研究者は ChatGPT をどうだましたのか」
https://xtech.nikkei.com/atcl/nxt/column/18/00676/041500131/

AI で生体認証を突破する手段も

現代の生成 AI は、文章だけでなく画像、音声の生成にも長けています。

オリジナルの声のデータが 1 分あれば「音声クローン」を生成できる AI を悪用する事例として、「人の声」という生体認証を突破した事例もあります。



音声生成 AI を悪用した生体認証突破

（出所：NRI セキュアテクノロジーズ「生成 AI のセキュリティリスクと対応のあり方」）

https://www.nri.com/-/media/Corporate/jp/Files/PDF/knowledge/report/cc/mediaforum/2023/forum361.pdf p17

しかも、騙されたのは業務効率化のために導入されたチャットボットです。

AI が AI を騙し、セキュリティを突破したというわけです。

顔認証も生成 AI で突破

さらに、生成 AI によって「顔認証」「指紋認証」も突破することが可能になりつつあります。

サイバー犯罪の手口などが交換される「ダークウェブ」と呼ばれる闇サイトの掲示板では、昨年夏頃から、不正に手に入れた顔写真で本人認証を突破する方法を記した投稿が目立ち始めているといいます。

実際、日立製作所の研究施設が、免許証の顔写真をもとに作った男性の映像をスマホを使ってシステムに見せたところ、顔認証システムを突破できたことが確認されています。

読売新聞オンライン「生成ＡＩ偽画像で「本人なりすまし」、口座開設デジタル顔認証すり抜け…闇サイトでの手口公開にコメント続々」
https://www.yomiuri.co.jp/national/20240828-OYT1T50024/

AI で「誰のデバイスでも突破できる」指紋を生成

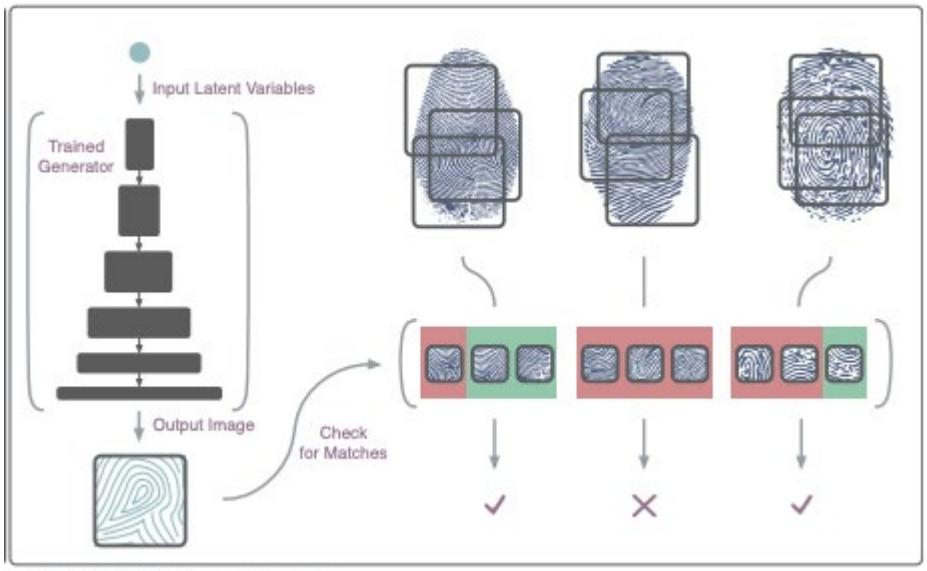
また、2018 年には、ニューヨーク大学とミシガン大学の研究者が機械学習で「DeepMasterPrints」と名付けた指紋を生成しました。多くの人の指紋に共通する、似た特徴をかき集めてひとつの指紋を合成するという手法です。

ランダムな文字列を多数生成して何万通りものパスワードを作り、セキュリティを突破するのと同様で、実験の結果、この合成指紋で、5 分の 1 の確率で指紋認証を突破したといいます。
全て部屋の鍵を開けられる「マスターキー」のようなものです。

The Guardian「Fake fingerprints can imitate real ones in biometric systems – research」
https://www.gizmodo.jp/2018/11/ai-beating-finger-print-auth.html

なぜこのようなことが可能になったかというと、指紋認証デバイスが、ロック解除の際に必ずしも指紋全体を読み込んでいるわけではないからです。

認証のたびに指紋全体をスキャンさせる必要があると時間がかかってしまい、不便なものになってしまうため、ある程度合致していればロックを解除できてしまうという特徴があるのです。



指紋認証のしくみ

（出所：コーネル大学 arXiv「DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution」）

https://arxiv.org/pdf/1705.07386 p5

よって、完全一致の指紋でなくても合格ポイントがいくつかあれば、セキュリティを突破できてしまう可能性があるのです。

大量の指紋のサンプルを手に入れることはそう簡単ではなさそうですし、指紋認証にはデータだけでなくデバイス本体を手に入れる必要がありますが、こうした認証突破は技術的には不可能ではないということです。

AI が AI を騙す時代　まずセキュリティに対する意識改革を

攻撃者が生成 AI を利用する理由は「手間を省いて多数の攻撃パターンを作り、有効な手段を抽出する」というツールとして、生成 AI が優れているからでしょう。

いたちごっこは永遠に続くものです。

現在のところ、多段階認証や「ゼロトラスト」などでシステムを考えることが基本ですが、まず生成 AI が身近になった時代に、上記のように様々な形のサイバー攻撃が起きうるという意識を、社内に浸透させる必要があるでしょう。

サイバーセキュリティにおいては機器だけでなく、社員ひとりひとりが「あやしいな」と感じる、疑う力を養うことも重要です。

サイバー攻撃に関する知識をこまめにアップデートしていき、共通することを徹底したいものです。勉強会などにこまめに参加するのも良いでしょう。

<清水 沙矢香>

2002 年京都大学理学部卒業後、TBS に主に報道記者として勤務。社会部記者として事件・事故、テクノロジー、経済部記者として各種市場・産業など幅広く取材、その後フリー。

取材経験や各種統計の分析を元に多数メディアに寄稿中。

レベル1_#15_リスクは自然災害だけではない 「サイバーBCP」を企業が策定すべき理由

掲載日：2025/1/7



photo AC「サーバールーム」

https://www.photo-ac.com/main/detail/4023690

日本は災害大国であり、いつどんな地震や台風などに遭遇するかわかりません。

自然災害は企業活動に大きなダメージを与えます。そうした非常事態からいかに早く事業を復旧させるかの事業継続計画(BCP)を策定することが急務になっています。

しかし、いま企業活動に潜むリスクは自然災害だけではありません。サイバー攻撃も大きな脅威のひとつです。

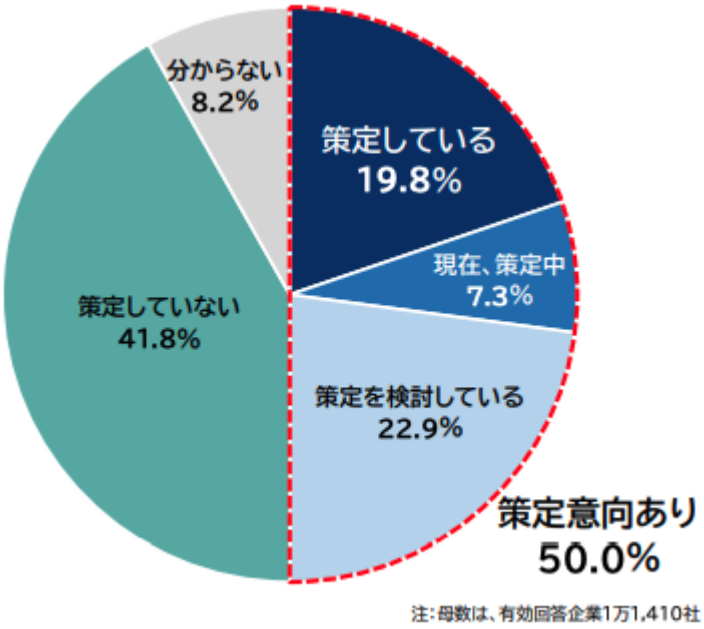
ことし6月にはKADOKAWAが大規模なサイバー攻撃を受け、主要サービスが停止するという事態も発生しました。

そこで、サイバー攻撃に備えた「サイバーBCP」の策定も必要になっています。

半数の企業がBCP策定の意向

2024年の初めに起きた能登半島地震は最大震度7を超える規模で、事業拠点への直接的な影響だけでなく、インフラの断絶で企業・消費活動にも大きな影響を与えました。

こうした中、帝国データバンクが全国の1万1,410社から回答を得た調査によると、BCPの策定意向を持つ企業の数が5割に達しました。



BCP策定意向の有無

(出所：帝国データバンク「事業継続計画（BCP）に対する企業の意識調査（2024 年）」)

https://www.tdb.co.jp/resource/files/assets/d4b8e8ee91d1489c9a2abd23a4bb5219/b209670834584a7a9310404530fa98a8/sp20240625.pdf p1

これは、4年ぶりの高水準になっているということです。能登半島地震を目の当たりにしたことが危機感を強めたと考えられます。

しかし、BCPの策定意向を持つ企業の構えは、自然災害に対するものだけではなくなっています。

事業の継続が困難になると想定しているリスク

BCPの策定意向を持っている企業は、このようなリスクを想定しています。

事業の継続が困難になると想定しているリスク
（複数回答）

（%）

		全体	大企業	中小企業
1	自然災害（地震、風水害、噴火など）	71.1	80.2	68.6
2	情報セキュリティ上のリスク（サイバー攻撃など含む）	44.4	55.4	41.3
3	感染症（インフルエンザ、新型ウイルス、SARSなど）	39.9	47.2	37.9
4	インフラ（電気・水道・ガスなど）の寸断	39.6	44.6	38.2
5	設備の故障	39.1	36.9	39.7
6	火災・爆発事故	31.9	34.7	31.1
7	取引先の倒産・廃業	30.7	25.3	32.3
8	自社業務管理システムの不具合・故障	30.5	35.8	29.0
9	物流（サプライチェーン）の混乱	29.1	33.3	27.9
10	取引先の被災	28.8	28.0	29.1
11	コンプライアンス違反の発生（営業秘密の漏洩など含む）	22.4	30.3	20.1
12	経営者の不測の事態 （経営者自身が被災し出社できないなど）	17.8	11.9	19.5
13	製品の事故	16.8	18.2	16.5
14	戦争やテロ	16.1	16.1	16.1
15	環境破壊	4.9	5.0	4.9
	その他	1.5	1.0	1.6

注1: 網掛けは、「大企業」と「中小企業」の比較で割合が高い規模を示す
注2: 母数は、事業継続計画（BCP）を「策定している」「現在、策定中」「策定を検討している」のいずれかを選択した企業5,705社

事業継続に対して想定しているリスク
(出所：帝国データバンク「事業継続計画（BCP）に対する企業の意識調査（2024 年）」p3)

大企業、中小企業ともに「自然災害」がトップに挙げられていますが、次に想定しているリスクは「情報セキュリティ上のリスク(サイバー攻撃など含む)」となっています。

サイバー攻撃もまた、企業活動に大きな影響を与える要因であるとの認識が広がっています。

自然災害とサイバー攻撃のリスクの違い

しかし、自然災害とサイバー攻撃では、性質と復旧過程が異なります。

両者の考え方について見ていきましょう。

自然災害に備えたBCPの考え方

自然災害の場合は比較的、受けた被害を把握しやすいと言えます。「目に見える」部分が多いからです。

そして、稼働を続けられるインフラや人材をまず中核事業の復旧に充てることで最も大きなダメージを避ける、というのが自然災害を想定したBCPの基本的な考え方です。

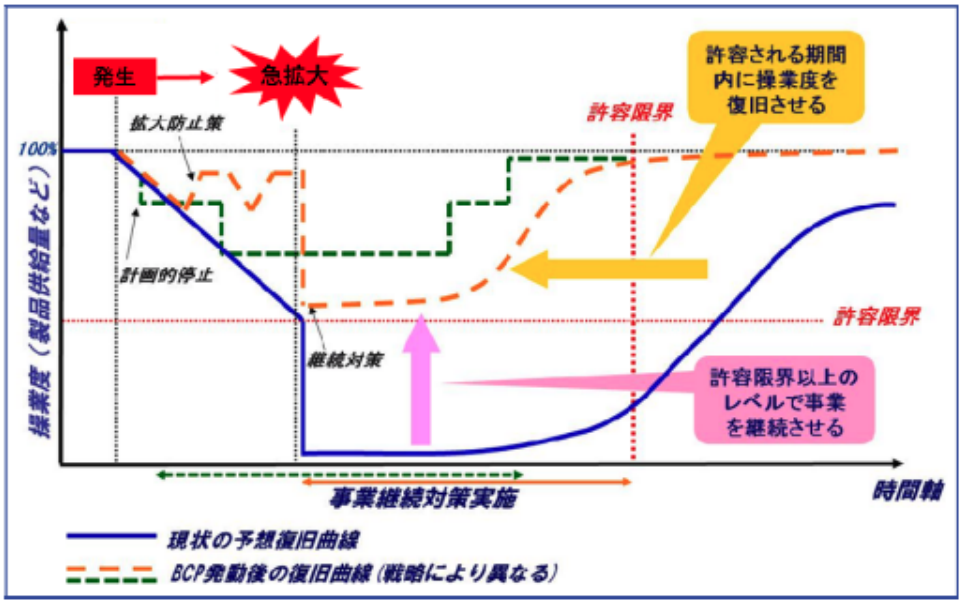


図 1.1-1-2 事業継続計画（BCP）の概念。段階的かつ長期間にわたり被害が継続するリスクの場合[9]

BCPのイメージ

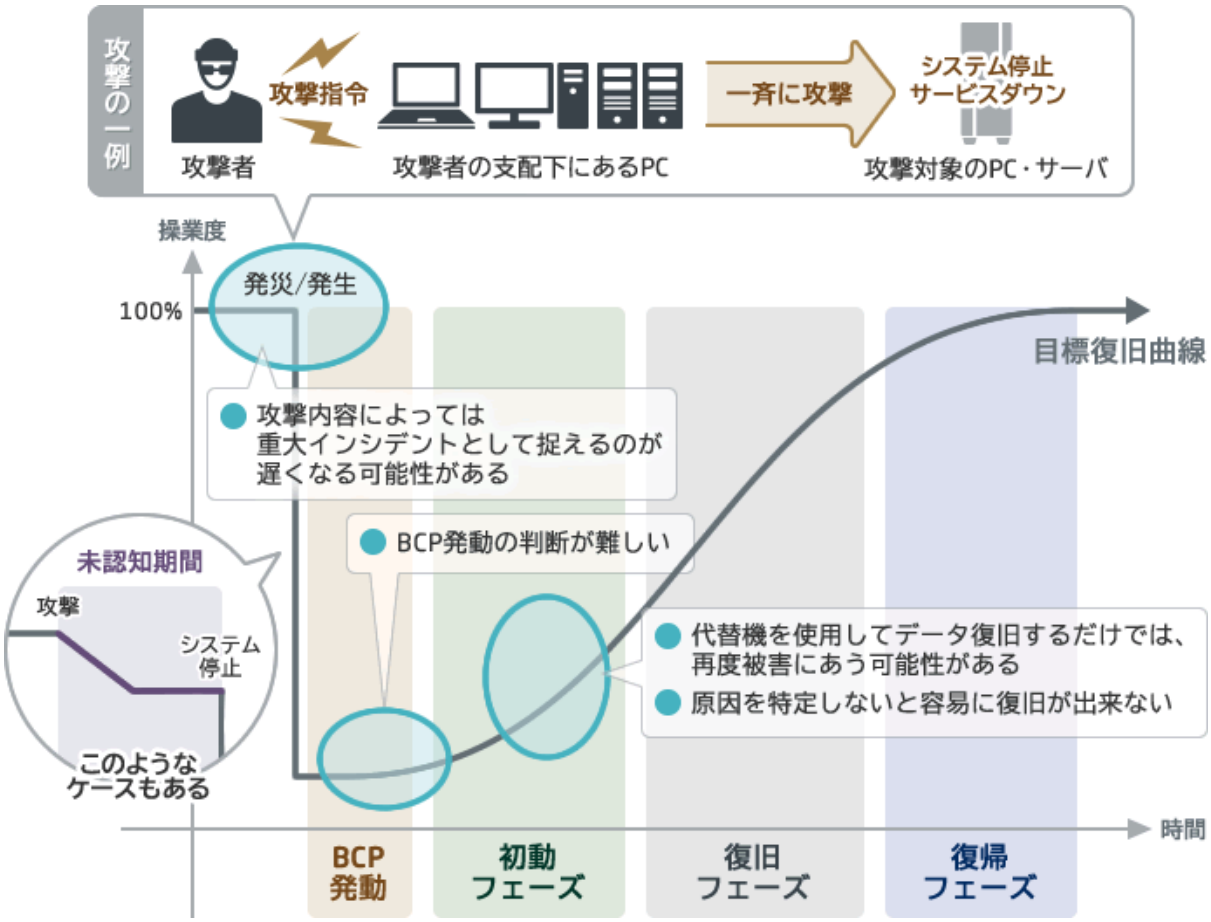
(出所：内閣府「事業継続ガイドライン－あらゆる危機的事象を乗り越えるための戦略と対応－（令和５年３月）」

https://www.bousai.go.jp/kyoiku/kigyou/pdf/guideline202303.pdf p4

緊急事態の発生時に何を優先するのか、そのために各社員はどのように行動をするのか、といったことがメインになります。

サイバー攻撃のリスク

一方でサイバー攻撃の場合、まず発生の瞬間は基本的には把握できません。障害が起きて初めて被害に気づき、しかしその時にはすでに、いくつものトラブルが同時発生しているという状態です。上の図でいう「急拡大」の状態で被害が発覚するという特徴があるのです。



サイバー攻撃からの復帰まで

(出所：NECソリューションイノベータ「BCP・リスク対策コンサルティング / シリーズ BCPの視点 第7回 サイバー攻撃に備えたIT-BCPの構築(前編)」)

https://www.nec-solutioninnovators.co.jp/sl/bcp/series/itbcp.html

例えば最近多発しているランサムウェアによるサイバー攻撃の場合、システムが使えなくなり、場合によっては全業務の停止をある日突然余儀なくされる、という形で被害が明らかになります。

しかし、それ以前に情報の抜き取りはすでに行われており、システム停止という目に見えるものだけではない被害を受けている状態です。

ランサムウェアによる攻撃は、KADOKAWAもそうでしたが「システムの暗号化を解くための金銭」「抜き取った情報を公開しないための金銭」という、2重の脅迫をかけるのが一般的です。たとえシステムの暗号化を解くことができたとしても、どのような情報が抜き取られたのかを確認し漏えいを防ぐ対応ができなければ、本格的な事業再開は難しくなってしまいます。

また、ウイルスの感染経路やウイルスがどこまで広がっているかが判明するまで、どの端末をどこまで使い続けていいのか、どこから復旧を始めれば良いのかの判断も難しくなります。

サイバーBCPの考え方

独立行政法人情報処理推進機構は、サイバーBCPの基本姿勢を次のように紹介しています。

> サイバー攻撃は情報漏えいだけでなく、重要なシステムの停止等による業務停止を引き起こすものがある。そのため、自然災害等を想定した既存のBCPと連携する等、組織としてサイバー攻撃によるインシデントに対する復旧体制を整備することが望まれる。
>
> 実践する上でのファーストステップとしては下記の3点が考えられる。
>
> ・自然災害等を想定したBCP策定の経験を有するチームとインシデント対応チームで情報を共有する
>
> ・インシデント影響度に応じた復旧対応の判断基準および判断フローを整備する
>
> ・システム障害の事業継続に与える影響が大きく優先度の高いシステムについて、復旧手順を検討し演習により確認する

＜引用：独立行政法人情報処理推進機構「プラクティス・ナビ」＞
https://www.ipa.go.jp/security/economics/practice/practices/Practice233/

「事業継続に与える影響が大きく優先度の高いシステム」について演習する、という優先度の設定は従来のBCPの考え方と変わりません。

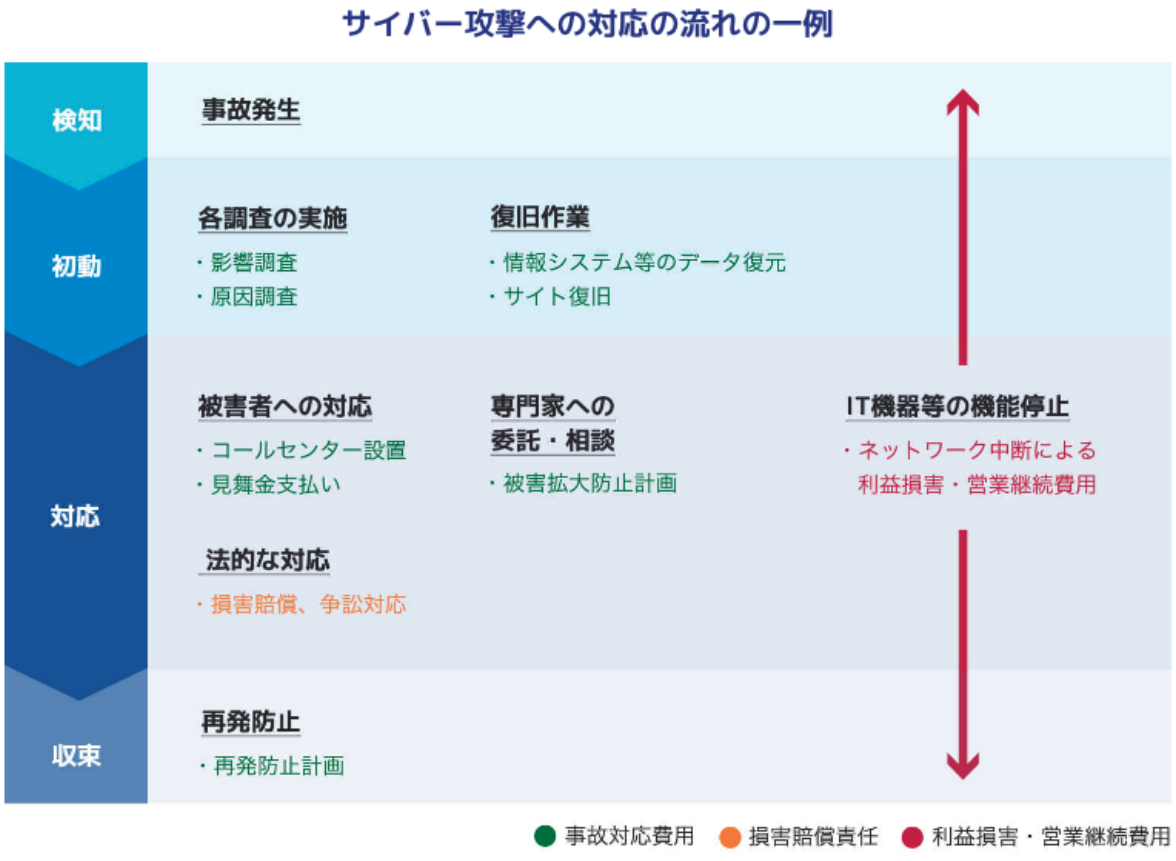
しかし、サイバー攻撃による情報漏えいの場合は、顧客やサプライチェーンへの適切な説明と対応が求められることも想定しておかなければなりません。また、攻撃者からの金銭の要求に対してどう対応するかの想定も必要です。

自然災害の場合はある程度周囲からの理解を得られるかもしれませんが、サイバー攻撃の場合は企業の日々の警戒が足りなかっただけ、と見なされることが多いでしょう。
自然災害に比べれば、周囲の目は「仕方ない」とはなりにくい部分があります。

損害保険への加入もひとつの手段

なお近年では、サイバー攻撃による損害に対応する保険商品も多く登場しています。

一例としては、以下のような費用が補償されるというものです。



サイバー攻撃への対応と補償範囲の一例

(出所：一般社団法人全国損害保険協会「サイバー保険とは」)

https://www.sonpo.or.jp/cyber-hoken/about/

上の図のように補償内容はおもに3種類あり、

・事故対応費用

・損害賠償責任

・利益損害・営業継続費用

といった具合です。

また、サイバーBCPの場合、自社の社員だけでは策定は難しいことでしょう。

そのような場合は自治体のサポート事業などを利用し、まず理解を深めるところから始めたいものです。

いずれにせよ、自然災害と同様、あるいはそれ以上の危機感が求められる時代になっています。

<清水 沙矢香>

2002年京都大学理学部卒業後、TBSに主に報道記者として勤務。社会部記者として事件・事故、テクノロジー、経済部記者として各種市場・産業など幅広く取材、その後フリー。

取材経験や各種統計の分析を元に多数メディアに寄稿中。

レベル1_#16_「最低賃金を1,500円に」はいつから？　中小企業はどうやって賃上げを実現する？

掲載日：2025/1/21



photo AC「給与明細を確認する」

https://www.photo-ac.com/main/detail/28129018

石破茂新首相は所信表明演説で、最低賃金の引き上げについて言及しました。

これまでも最低賃金は年々引き上げられてきましたが、今回は「2020年代に全国平均で1500円まで上げる」という高い水準を石破首相は目指しています。

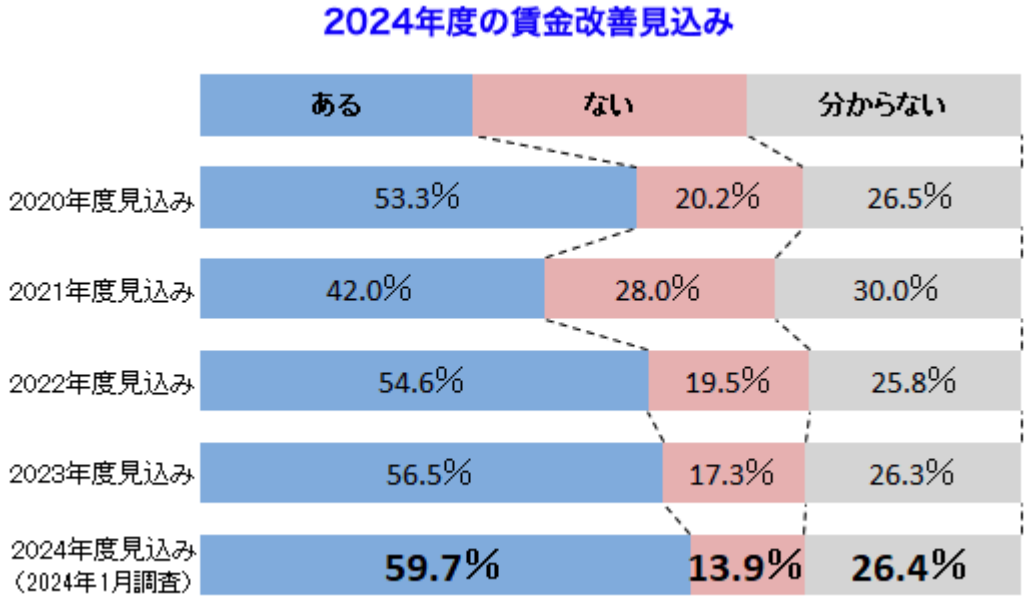
賃上げは人手不足のなか、人材確保のために欠かせない要素になりつつあります。

一方で企業の利益を減らしてしまうものとの捉え方もあります。

事業を続けながら賃上げを進めるにはどのような対策を取ればいいのか、どんな補助金や助成金などが利用できるかご紹介していきます。

賃上げを検討する企業は年々増加

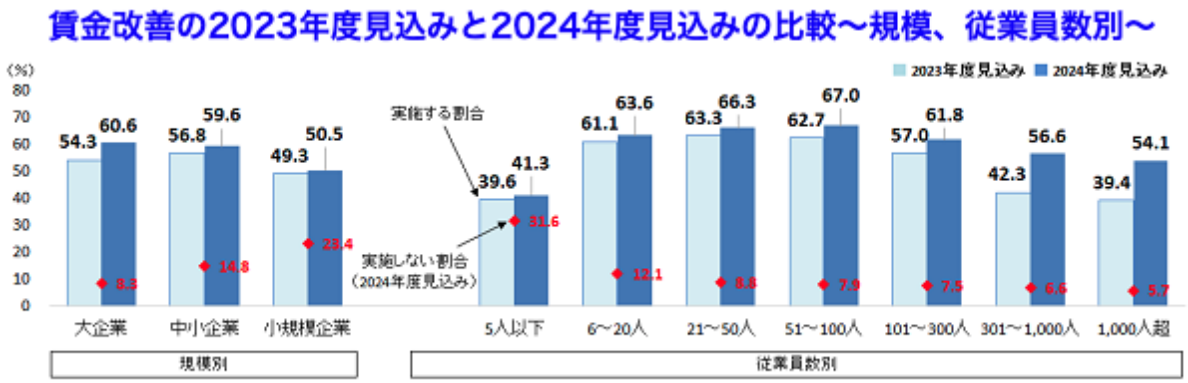
帝国データバンクが2024年、全国1万1,431社から回答を得た調査によると、賃金を改善する見込みだという企業は年々増加し、今年度は6割に達しています。



賃金改善見込みの企業の割合

(出所：帝国データバンク「2024年度の賃金動向に関する企業の意識調査」)

これを企業規模別に見ると、下のようになっています。

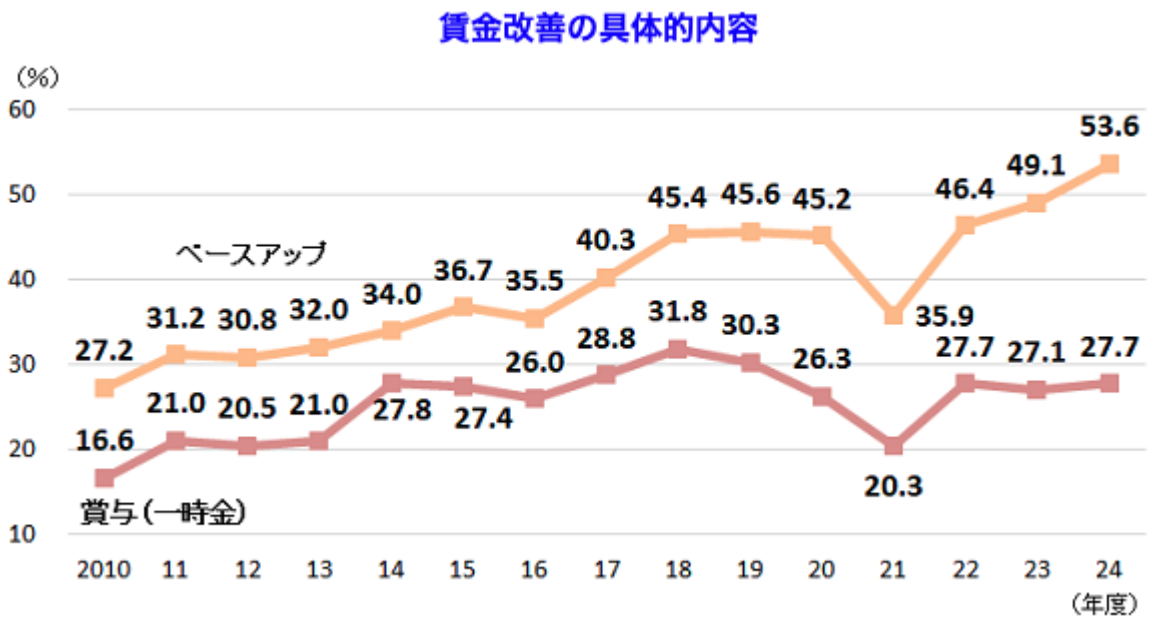


規模別に見た2023年度と2024年度の賃金改善見込み企業の割合

(出所：帝国データバンク「2024年度の賃金動向に関する企業の意識調査」)

企業規模を問わず、昨年度よりも賃金改善を見込んでいる企業の割合は、中小企業でもわずかながら増えていることがわかります。

なお、賃金改善の具体的な内容は下のようになっています。



賃金改善の内容

(出所：帝国データバンク「2024年度の賃金動向に関する企業の意識調査」)

「ベースアップ」での対応が多く、53.6%と半数を上回っています。3年連続で調査開始以降の最高を更新しています。

帝国データバンク「2024年度の賃金動向に関する企業の意識調査」

「最低賃金1500円」は可能？

岸田前首相は昨年、最低賃金の全国平均を1,500円にする目標を2030年代半ばとしていました。この場合、毎年3.4%引き上げる必要がありました。

しかし石破新首相は達成目標を2020年代と、時期を大幅に短縮すると発言しています。

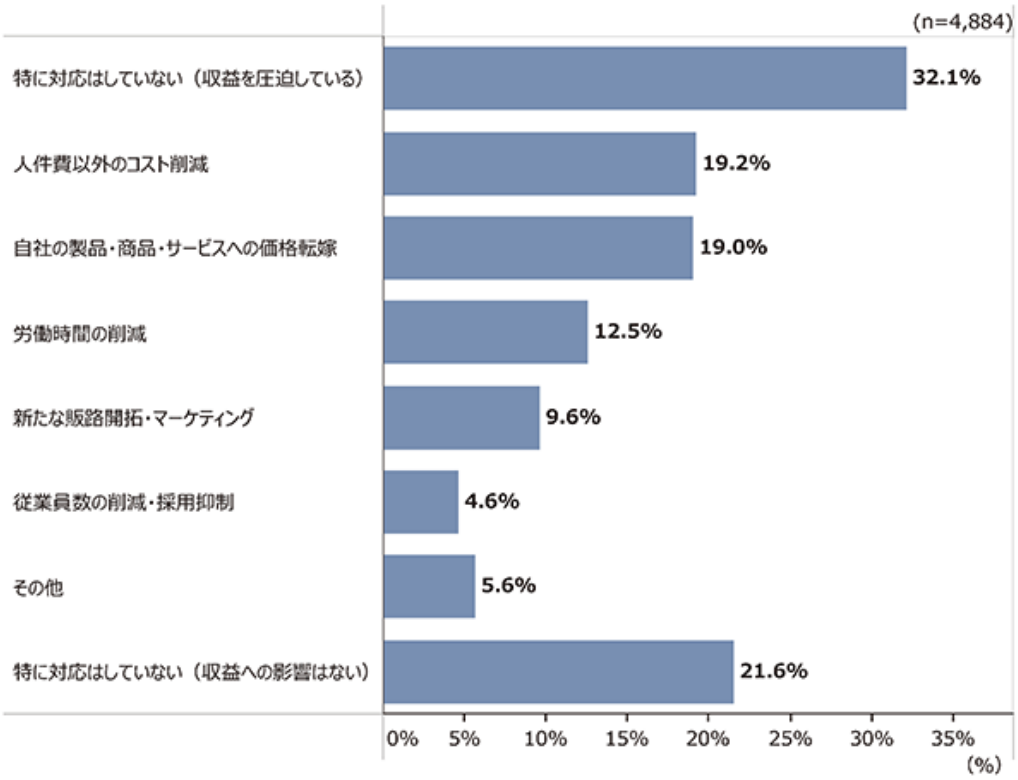
大和総研によれば、2020年代に最低賃金を全国平均1,500円にするためには、年間1.2%~5.7%の引き上げが必要という計算です。

日本経済新聞「最低賃金、全国平均1054円　上げ幅50円は過去最大」
https://www.nikkei.com/article/DGXZQOUA178480X10C24A7000000/
大和総研「最低賃金の新たな目標は「1,500円」？」
https://www.dir.co.jp/report/research/economics/japan/20230816_023938.html

最低賃金引き上げへの対応

令和5年度の中小企業白書によれば、中小企業・小規模事業者は賃上げに対して下のような対策を取っています。

第1-4-7図　最低賃金の引上げを受けて、賃上げの原資確保のために行った対応



資料：（株）帝国データバンク「中小企業が直面する外部環境の変化に関する調査」
（注）複数回答のため、合計は必ずしも100%にならない。

最低賃金引き上げへの中小・小規模事業者の対応

(出所：中小企業庁「令和5年度中小企業白書」)

https://www.chusho.meti.go.jp/pamflet/hakusyo/2024/chusho/b1_4_1.html

事業コストの増加分を価格に転嫁できていない、原材料価格の高騰などが背景にあるようです。

このような場合、行政による支援や助成金の利用もひとつの方法になり得ます。

NHK「春闘2024の焦点 中小企業の賃上げ 価格転嫁の難しさで水準低下も」

https://www.nhk.or.jp/shutoken/newsup/20240221c.html

厚生労働省の支援事業

ひとつには、厚生労働省などが実施している中小企業・小規模事業者への支援事業があります。

令和6年8月時点では、以下の各種支援・助成事業が実施されています。

厚生労働省「最低賃金引上げに向けた中小企業・小規模事業者への支援事業」
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/koyou_roudou/roudoukijun/zigyonushi/shienjigyou/index.html

業務改善助成金

事業所内で最も低い時間給を一定額以上引き上げ、生産性向上等に資する設備投資等を行った場合に、かかった費用の一部が助成される、というものです。
事業場内最低賃金と地域別最低賃金の差額が50円以内の事業者に適応されます。

生産性の向上がメインの目的で、生産性を向上させて売上をアップさせ、人件費に充てるという考え方とみられます。

時間給を引き上げる対象人数によって、助成額が異なります。

助成率

事業場内最低賃金額	助成率
900円未満	9/10
900円以上950円未満	4/5(9/10)
950円以上	3/4(4/5)

※（　）内は生産性要件を満たした事業場

助成対象経費の例

機器・設備の導入	• POSレジシステム導入による在庫管理の短縮 • リフト付き特殊車両の導入による送迎時間の短縮
経営コンサルティング	国家資格者による、顧客回転率の向上を目的とした業務フロー見直し
その他	顧客管理情報のシステム化

※ 一部事業者は対象経費の特例を受けることができる可能性がございます。（詳細は業務改善助成金ウェブサイト参照）

助成上限額

引上げ労働者数	引上げ額			
	30円コース（30円以上）	45円コース（45円以上）	60円コース（60円以上）	90円コース（90円以上）
1人	30万円（60万円）	45万円（80万円）	60万円（110万円）	90万円（170万円）
2～3人	50万円（90万円）	70万円（110万円）	90万円（160万円）	150万円（240万円）
4～6人	70万円（100万円）	100万円（140万円）	150万円（190万円）	270万円（290万円）
7人以上	100万円（120万円）	150万円（160万円）	230万円	450万円
10人以上※	120万円（130万円）	180万円	300万円	600万円

※10人以上の上限区分は特例事業者（詳細は業務改善助成金ウェブサイト参照）のみ対象。
※（　）内の助成上限額は事業場規模30人未満の事業者のみ対象。

助成額の事例

(出所：厚生労働省リーフレット「厚生労働省、中小企業庁では、最低賃金引き上げに伴う支援・後押しを強化しています」)

https://www.mhlw.go.jp/content/001289722.pdf

例えば小売ではPOSレジシステムの導入もひとつです。大幅に生産性が上がり、従業員に利益を還元することができる手段です。

問い合わせ先は下のコールセンターです。

■業務改善助成金コールセンター

電話番号：０１２０－３６６－４４０

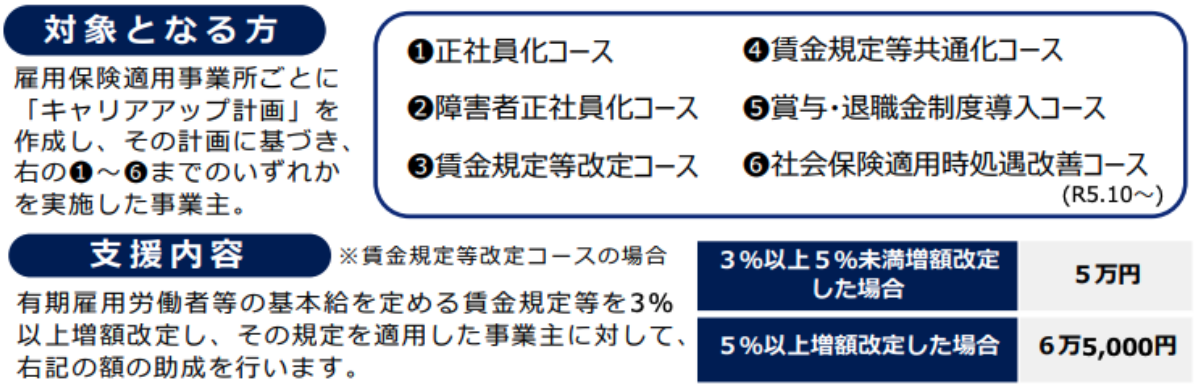
受付時間：平日８：３０～１７：１５

厚生労働省「業務改善助成金」

https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/koyou_roudou/roudoukijun/zigyonushi/shienjigyou/03.html

キャリアアップ助成金

以下のいずれかを実施した事業主に支払われる助成金です。



(出所：厚生労働省リーフレット「厚生労働省、中小企業庁では、最低賃金引き上げに伴う支援・後押しを強化しています」)
https://www.mhlw.go.jp/content/001289722.pdf p3

従業員のキャリアアップで業務効率化をはかり、同一労働同一賃金に取り組む際や、いわゆる「年収の壁」を意識した働き方への対応に取り組む際にも活用できるものです。

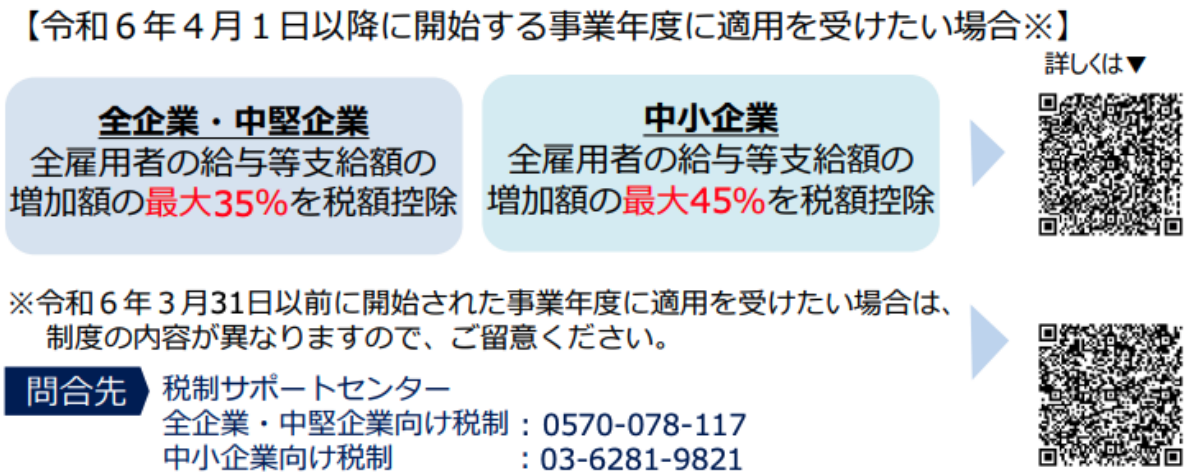
こちらは、各都道府県の労働局が問い合わせ先です。

「最低賃金・賃金引上げに向けた中小企業・小規模事業者への支援施策」厚生労働省・中小企業庁
https://www.mhlw.go.jp/content/001289720.pdf p1

賃上げ促進税制

こちらは事業者が、一定率以上の賃上げを実施した場合、賃上げ額の一部を法人税などから税額控除できるという仕組みです。

控除率は下のようになっています。



(出所：厚生労働省リーフレット「厚生労働省、中小企業庁では、最低賃金引き上げに伴う支援・後押しを強化しています」)
https://www.mhlw.go.jp/content/001289722.pdf p4

問い合わせ先は、上記の「税制サポートセンター」です。

特にパートタイマーへの還元をどうするか

特にパートタイム労働者は、最低賃金の引き上げを前に悩む人が多いようです。いわゆる「年収の壁」と呼ばれる問題があるからです。

パート、アルバイトで働く人の場合、

・年収103万円を超えると所得税がかかる

・年収106万円以上になることで、厚生年金・健康保険に加入するため保険料の負担が生じる

・年収130万円以上になることで、国民年金・国民健康保険に加入するため保険料の負担が増える

という制度になっているため、今後「より時給の高い勤務先に変える」と考えている人も一定の割合で存在します。

すると、そうした人たちは他に出ていく、あるいは勤務時間をより縮めるという方向に動く可能性が考えられます。

しかし、こうした制度的な「年収の壁」によって優秀な従業員を失うのは、この時代では、企業にとっては人手不足という痛手となることでしょう。

「2020年代に平均1,500円」という石破首相の言葉通りにならなかったとしても、最低賃金を上げる動きは今後も続くことでしょう。

その中で、「どんなことをしてくれる人をどのくらいの割合で、どう働いてもらうのか」といったバランスをより緻密に考えていく必要がありそうです。

また現在政府では、こうした「年収の壁」を見直す動きもありますので、こちらについてもチェックしていきたいところです。

NHK「103万の壁って？106万、130万も…違いは？年収の壁を詳しく」
https://www3.nhk.or.jp/news/html/20241108/k10014632501000.html
マイナビニュース「年収の壁のリアルを調査!「年収の壁」による困りごと、第1位は?」
https://news.mynavi.jp/article/20240205-2875230/

＜清水 沙矢香＞
2002年京都大学理学部卒業後、TBSに主に報道記者として勤務。社会部記者として事件・事故、テクノロジー、経済部記者として各種市場・産業など幅広く取材、その後フリー。
取材経験や各種統計の分析を元に多数メディアに寄稿中。

レベル1_#17_黒字なのに廃業はもったいない！　事業承継の有益な手法「中小M＆A」と助成金について解説

掲載日：2025/1/28



photo AC「写真素材：事業承継・M＆A」
https://www.photo-ac.com/main/detail/26847556&title=%E4%BA%

大切な会社と従業員、熱い思いや技術を次の世代に引き継ぐ―事業承継は経営者にとって重い責任です。

ところが、現在、半数以上の中小企業で後継者が不在となっています。
また、2023年に経営者年齢は過去最高を更新し、今後も事業承継の必要性が高まることが窺えます。

後継者がいなければ、たとえ黒字経営であったとしても、廃業を視野に入れざるを得ません。実際に、休廃業・解散を選択した企業の半数以上が、直前の決算は黒字です。

そうした状況を回避し事業承継を実現するための有益な手法の1つが、「中小M＆A」です。
中小M＆Aをめぐる状況をわかりやすく解説し、東京都の助成金、支援策をご紹介します。

事業承継をめぐる状況

まず、中小企業の経営者の年齢と事業承継はどのような状況にあるのでしょうか。

中小企業経営者の年齢

2023年時点の経営者年齢は平均60.5歳で、過去最高を更新しました。さらに70代以上の経営者の割合も継続して増加しています。

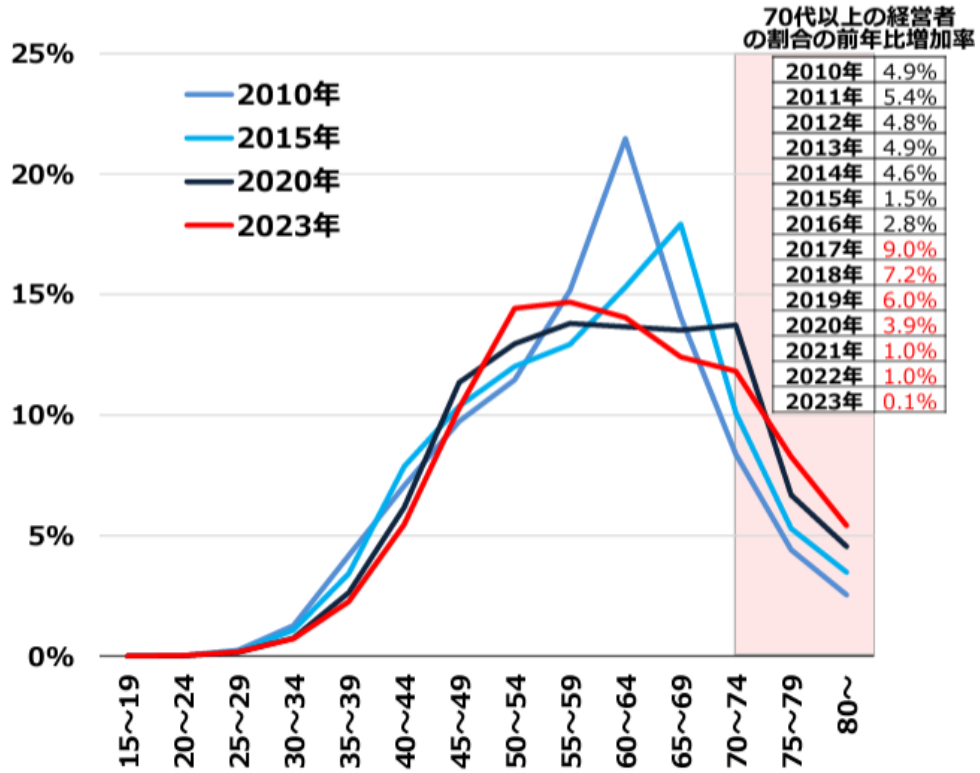


図1　中小企業の経営者年齢の分布

出所）中小企業庁「事業承継・M&Aに関する現状分析と今後の取組の方向性について」（2024年6月）p.10
https://www.chusho.meti.go.jp/koukai/kenkyukai/shokei_ma/001/005.pdf

後継者不在の状況

次に中小企業の後継者をめぐる状況をみてみましょう。

後継者不在率は2018年以降、減少傾向にあるものの、2023年時点でも54.5%と、半数を超えています。

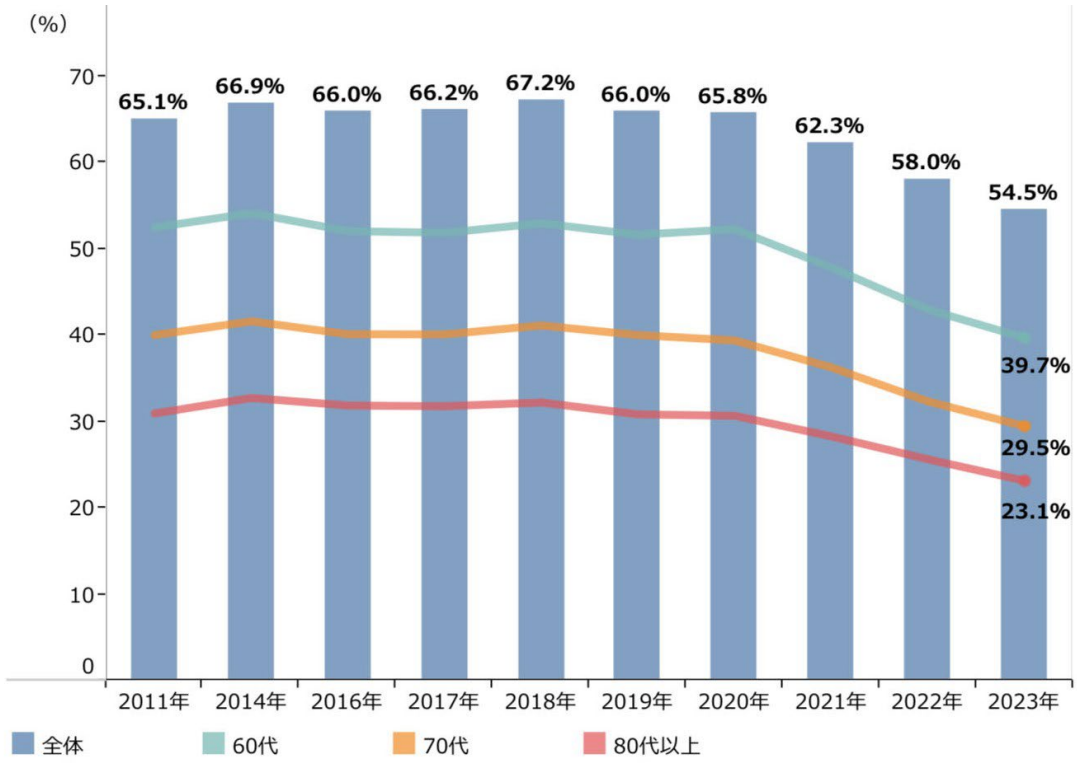


図2　中小企業の後継者不在率

出所）中小企業庁「2024年版中小企業白書　第3章　中小企業・小規模企業の現状」p.109

https://www.chusho.meti.go.jp/pamflet/hakusyo/2024/PDF/chusho/03Hakusyo_part1_chap3_web.pdf

休廃業・解散の件数と廃業理由

後継者不在の問題は、中小企業の廃業にも影響を与えています。休廃業・解散件数は増加傾向にあり、厳しい状況が続いていますが、廃業理由の約3割が後継者不在なのです。

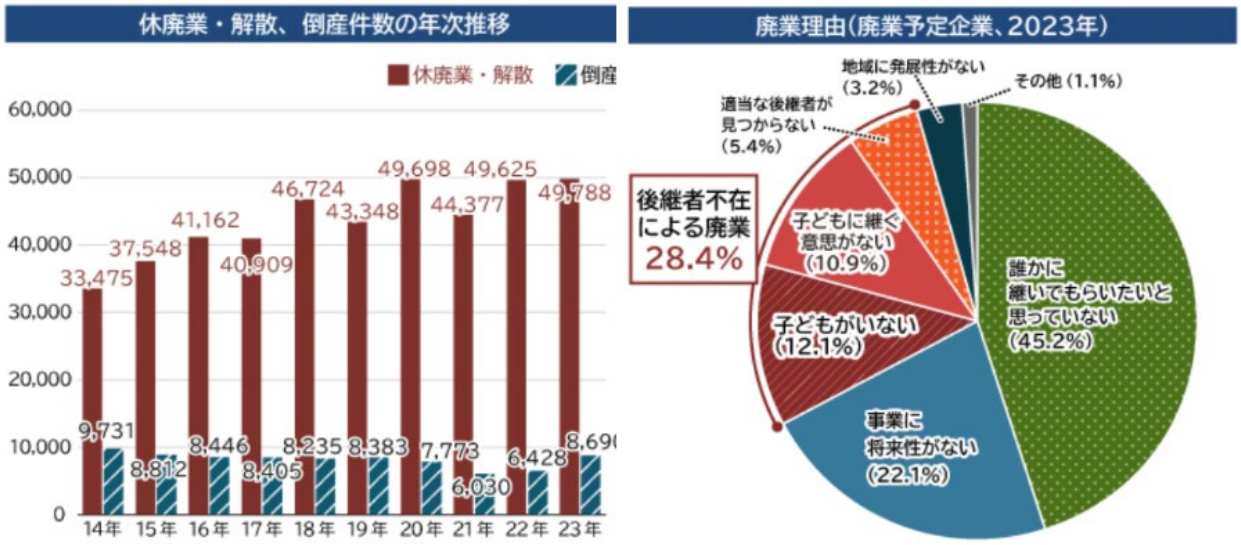


図3　中小企業の休廃業・解散件数と廃業理由

出所）中小企業庁「事業承継を知る」

https://www.chusho.meti.go.jp/zaimu/shoukei/know_business_succession.html

しかも、2023年に休廃業・解散を選択した企業の52.4%が直前の決算は黒字であり、価値ある事業が喪失している状況があります。

出所）東京商工会議所「中小企業の円滑な事業承継の実現に向けた意見概要」（2024年7月）p.1

https://www.tokyo-cci.or.jp/file.jsp?id=1203520

事業承継後の経営状況

では、事業承継をした企業の承継後の業績はどうでしょうか。

M＆Aを実施した中小企業は、M＆Aを実施していない企業と比べて、売上高、経常利益、労働生産性を向上させています。

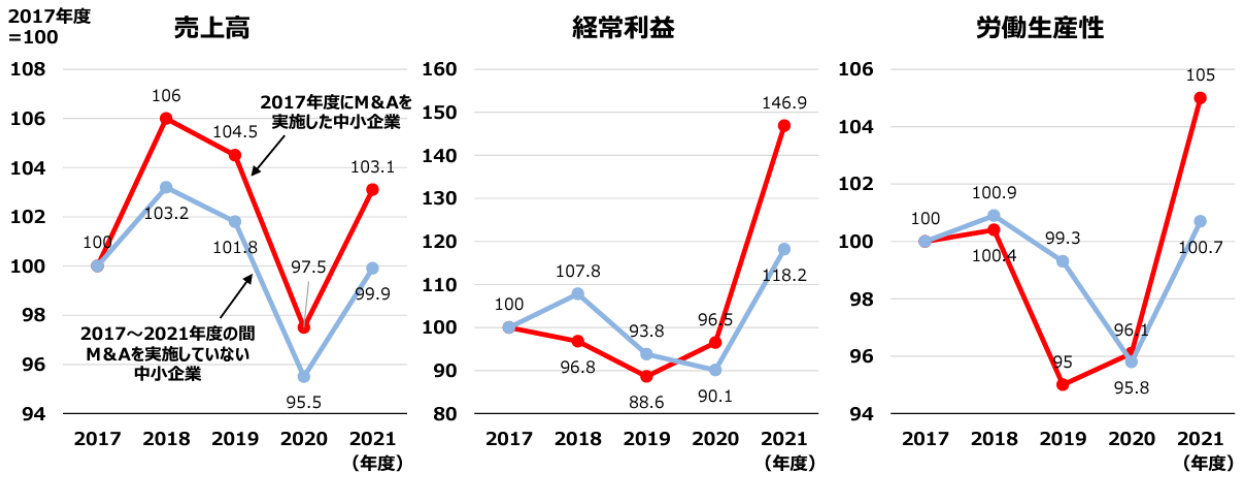


図4　事業承継実施企業の承継後の利益

出所）中小企業庁「事業承継・M&Aに関する現状分析と今後の取組の方向性について」（2024年6月）p.22

https://www.chusho.meti.go.jp/koukai/kenkyukai/shokei_ma/001/005.pdf

事業承継に向けた「中小M＆A」

次に、中小企業の事業承継に有益な手法「中小M＆A」についてみていきましょう。

第三者承継を可能にするM＆A

M&Aとは、「Mergers（合併） and Acquisitions（買収）」の略称です。日本では会社法の定める組織再編（合併や会社分割）に加え、株式譲渡や事業譲渡を含む事業の引継ぎを指します。

「中小M&A」とは、後継者不在の中小企業の事業を、M&Aの手法によって、社外の第三者である後継者が引き継ぐことです。

出所）中小企業庁「中小M&Aガイドライン（第2版）―第三者への円滑な事業引継ぎに向けて―」（2023年9月） p.14

https://www.meti.go.jp/press/2023/09/20230922004/20230922004-b.pdf

事業承継には価値ある企業の存続を可能にするという社会的意義があります。

ところが、2022年から2023年の利益状況をみると、「後継者を決めていないが、事業は継続したい」という企業の54.8%、「自分の代で廃業予定」の企業の25.5%が黒字経営で、このままではこうした価値ある企業の存続が断たれる可能性があります。

出所）東京商工会議所「事業承継に関する実態アンケート報告書」（2024年2月）p.27

https://tokyo-cci.meclib.jp/jigyoshoukei_survey2024/book/#target/page_no=29

このような状況を背景に、第三者承継の有益な手法である「中小M&A」に注目が集まっているのです。

実施件数

国内の中小M&Aの実施件数は増加しており、2022年度の実施件数は、事業承継・引継ぎ支援センターを通じたものが1,681件、民間M&A支援機関を通じたものが4,036件でした。

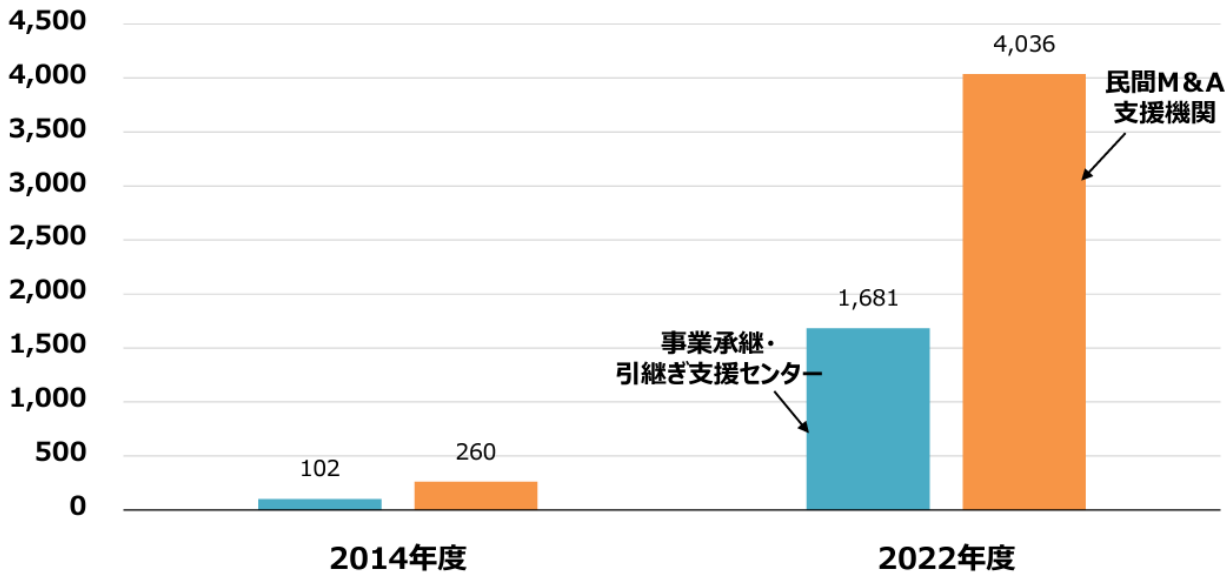


図5　中小M&Aの実施件数

出所）中小企業庁「事業承継・M&Aに関する現状分析と今後の取組の方向性について」（2024年6月）p.12

https://www.chusho.meti.go.jp/koukai/kenkyukai/shokei_ma/001/005.pdf

なお、「事業承継・引継ぎ支援センター」とは、国が設置する公的相談窓口で、中小企業の事業承継に関するあらゆる相談に対応しています。東京都にも同センターの窓口がありますので、後でご紹介します。

出所）事業承継・引継ぎ支援センター　ウェブサイト・トップページ

https://shoukei.smrj.go.jp/

Ｍ＆Ａに対するよくある誤解

事業承継はしたいけれどM&Aには抵抗があるという方もいらっしゃるでしょう。
ここで、Ｍ＆Ａに対するよくある誤解をＱ＆Ａ方式でみていきましょう。

Q1：敵対的な行為なのでは？

Ａ：あくまで当事者間の話し合いによって、友好的に進められます。

Q2：従業員はリストラされ、顧客基盤や技術だけを奪われるのでは？

Ａ：従業員の雇用は多くの場合、M&A実施後にも維持されているという調査結果があります。人手不足のため、譲受企業が人材を求めている場合もあります。「従業員の雇用継続」など条件を明確にして譲渡先を探すことが重要です。

Q3：大企業が対象で、小さな会社は関係ないのでは？

Ａ：東京商工会議所の調査によると、被買収企業（譲渡側）でもっとも割合が高いのは従業員10人以下の企業で48.2%、11～20人規模が27.6%で、100人以下の企業が全体の96.4%に上ります。

Q4：赤字企業・債務超過企業は対象にならないのでは？

Ａ：企業のもつ人材や技術、ノウハウ、設備、顧客網などを求める企業がみつかるケースもあります。たとえば、譲受企業との相乗効果で収益改善や成長が見込まれ、買収の対象となった事例があります。

Q5：安く買いたたかれるのでは？

Ａ：Ｍ＆Ａの価格は交渉によって決まります。希望額に満たない場合には無理に売却・譲渡する必要はありません。専門家、支援機関などの協力を得れば、適正価格で交渉を進められる可能性が高まります。

Q6：Ｍ＆Ａの経験がない小さな会社には対応が難しいのでは？

Ａ：一般的にＭ＆Ａによる承継は誰でも初めての経験です。支援者のサポートを積極的に活用しましょう。

出所）東京商工会議所「後継者が決まっていない小さな会社のためのM&Aガイド」（2023年3月）pp.6-7
https://tokyo-cci.meclib.jp/manda_guide/book/#target/page_no=6

出所）経済産業省 中小企業庁「中小M＆Aの意義」（2021年3月）p.5
https://www.chusho.meti.go.jp/koukai/kenkyukai/shigenshuyaku/2021/210315shigenshuyaku01_1.pdf
出所）東京商工会議所「事業承継に関する実態アンケート報告書」（2024年2月）p.31
https://tokyo-cci.meclib.jp/jigyoshoukei_survey2024/book/#target/page_no=33

東京都の支援策と助成金

ここでは、中小M＆Aに取り組む企業への東京都の支援策と助成金をご紹介します。

東京都事業承継・引継ぎ支援センター

東京都事業承継・引継ぎ支援センターは、東京商工会議所が経済産業省から委託を受けて、中小企業のM&Aを無料でサポートしています。
事業承継問題の悩みを抱える中小企業経営者からの相談、特に「第三者への会社（事業）の譲渡」についての相談を受け、ケースによっては実際のM&Aの実行支援を行います。

企業にとって最善の事業承継の方策を、利害関係のない第三者の専門家が経験に基づいてアドバイスします。選択肢は提示しますが、自己のビジネス分野への誘導をしたり、決断を急かしたり、強く促したりするようなことはありません。秘密厳守で、安心して相談することができます。
出所）東京都事業承継・引継ぎ支援センター　ウェブサイト
https://www.jigyo-hikitsugi.jp/about_us/purpose/
https://www.jigyo-hikitsugi.jp/about_us/characteristic/

東京商工会議所「ビジネスサポートデスク」

東京商工会議所「ビジネスサポートデスク」は、次の世代に向けた業績改善、事業承継計画の作成など、専門家が無料で継続的に課題解決を支援します。

たとえば、事業承継支援の経験豊富な専門家（中小企業診断士、税理士、公認会計士）がヒアリングを行い、事業承継に向けて課題や対策案をまとめた「診断書」を無料で作成・提供し、対策をサポートしています。

出所）東京商工会議所「ビジネスサポートデスク」

https://www.tokyo-cci.or.jp/soudan/bsd/

https://www.tokyo-cci.or.jp/jigyoshoukeiportal/

事業承継支援助成金

東京の「事業承継支援助成金」は、都内の中小企業を対象として、事業承継を実施する過程で外部専門家などに委託して行う取り組みに対し、200万円を上限として、その経費の一部を助成するものです。

公益財団法人東京都中小企業振興公社「令和6年度 第2回事業承継支援助成金」

https://www.tokyo-kosha.or.jp/support/josei/jigyo/shoukei.html

国の支援策

国は現在、中小M＆Aを推進しており、次の図6のように、さまざまな支援策を講じています。

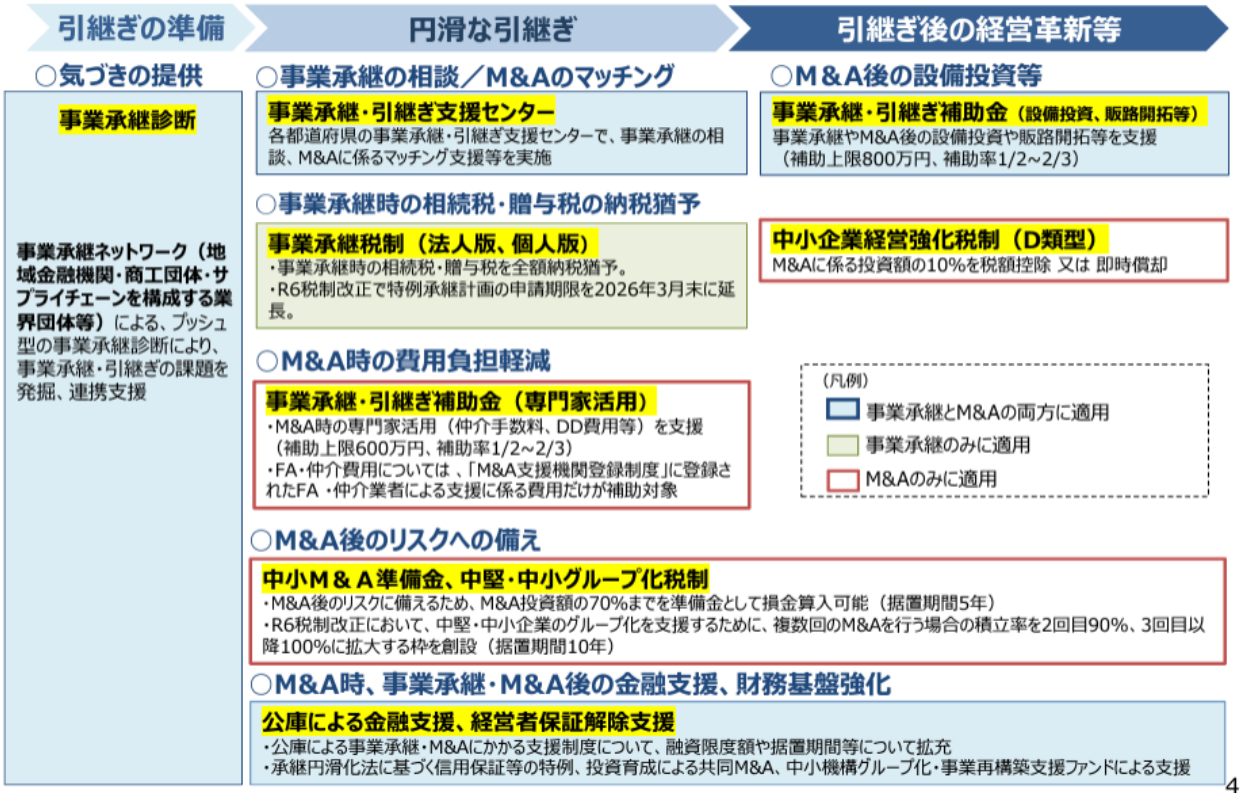


図6　中小M＆Aの支援策一覧

出所）中小企業庁「事業承継・M&Aに関する現状分析と今後の取組の方向性について」（2024年6月）p.4

https://www.chusho.meti.go.jp/koukai/kenkyukai/shokei_ma/001/005.pdf

おわりに

これまでみてきたように、「中小M&A」は適切な事業承継を実現することによって従業員や設備などの経営資源の維持につながるだけでなく、企業の経営状態を向上させ、企業価値を高めます。

支援策も視野に入れ、時間的余裕をもってじっくり検討してみてはいかがでしょうか。

筆者プロフィール

＜横内美保子＞

博士（文学）。総合政策学部などで准教授、教授を歴任。専門は日本語学、日本語教育。

高等教育の他、文部科学省、外務省、厚生労働省などのプログラムに関わり、日本語教師育成、教材開発、リカレント教育、外国人就労支援、ボランティアのサポートなどに携わる。
パラレルワーカーとして、ウェブライター、編集者、ディレクターとしても働いている。

X：よこうちみほこ
Facebook：よこうちみほこ

レベル1_#18_もうすぐWindows 10のサポートが終了　知っておかなければならないセキュリティへの影響とは

掲載日：2025/2/4



photo AC「アップデートのイメージ」
https://www.photo-ac.com/main/detail/2129794

マイクロソフトによるWindows 10のサポートが、2025年の秋に終了します。

サポートが終了すると、新たな問題が見つかっても対応にあたってのサポートや修正プログラムの配布などが行われないため、サポートの終了したWindows 10を使い続けるとセキュリティ上でも大きなリスクが生まれます。

どのようなリスクがあるのか、また、Windows 11への移行を進めている企業もあることかと思いますが、それにあたっての注意点もあわせて解説していきます。

サポート終了の時期とQ&A

2025年の10月14日(米国時間)にサポートが終了するのは、以下の3つのOSです。

1）Windows 10 Enterprise and Education
2）Windows 10 Home and Pro
3）Windows 10 IoT Enterprise

また、Officeアプリケーションも、Office2016の延長サポートが2025年10月14日で終了します。

サポートが終了することでWindows 10やパソコン自体が使えなくなるということは基本的にはありませんが、OSだけでなく、OS上で稼働するアプリケーションもサポートが順次終了していきます。

また、Windows 10に関する以下のサービス

・テクニカル サポート
・機能更新プログラム
・セキュリティ更新または修正プログラム

がマイクロソフトから提供されなくなってしまいます。

特に注意すべきは「セキュリティ更新または修正プログラム」の提供が止まることです。セキュリティ上のトラブルが起きても、マイクロソフトが何か対応をしてくれるわけではなくなるのです。

事実上、セキュリティは大幅に下がることになります。

マイクロソフト「2025 年のサポート終了」
https://learn.microsoft.com/ja-jp/lifecycle/end-of-support/end-of-support-2025
総務省「サポート切れソフトウェアを利用しないようにしよう」
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/security/end_user/general/03/

サポート終了後のWindowsで起きた被害

では、サポート終了後もWindows 10を使い続けることでどのようなセキュリティ問題が起きるのかみていきましょう。

過去の事例をご紹介します。

Windows XPのサポートが終了した後の2017年に、「WannaCry」というランサムウェアの被害が世界中に広がりました。ユーザーのファイルを勝手に暗号化して身代金を要求するものです。

日本でも日立製作所、JR東日本が被害にあったほか、イオンや日産自動車のイギリスの工場もサイバー攻撃を受け、WannaCryとの関係が指摘されました。600か所で2000台の端末が感染しています。

英紙「テレグラフ」の当時の報道によれば、大量の業務用パソコンがWannaCryに感染したイギリスの国民保健サービス(NHS)の場合では、業務用パソコンの90%でWindows XPを利用していたといいます。

WannaCryの標的はサポート終了後のWindows XPなどの脆弱性でした。
実際「Windows XP」や「Windows 8」「Windows Server 2003」「Windows 2000 Server」といったサポートが終了したOSには、セキュリティパッチが提供されていません。

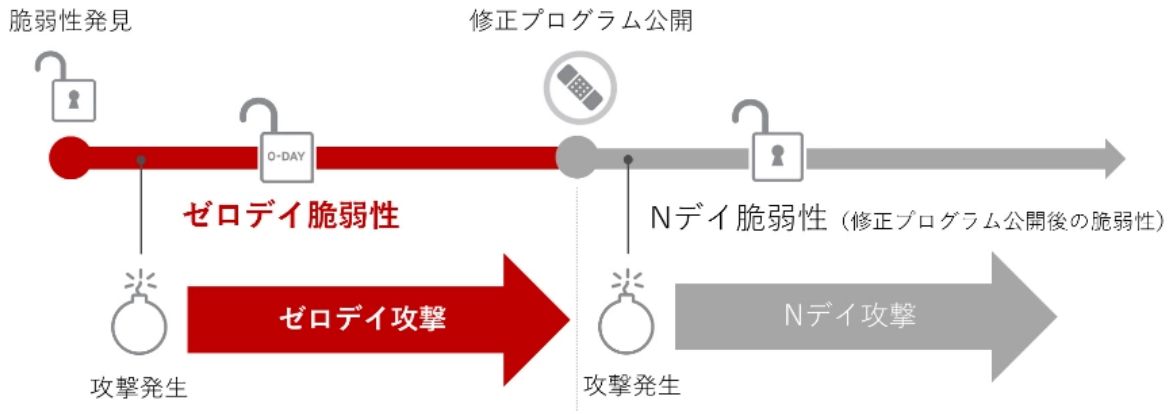
このように、サポート終了後のOSを使い続けることは大きなリスクに繋がるのです。

日経クロステック「国内襲い始めたWannaCry、日立やJR東など600カ所2000端末で感染」
https://xtech.nikkei.com/it/atcl/column/14/346926/051500971/

日経クロステック「米NSAが隠蔽したXPの脆弱性、WannaCryが狙う」
https://xtech.nikkei.com/it/atcl/column/15/061500148/051500108/

ゼロデイ攻撃の脅威

そしてもうひとつ知っておきたいのが、近年注目されている「ゼロデイ攻撃」と呼ばれるサイバー攻撃手法です。



ゼロデイ攻撃の概念
(出所：トレンドマイクロ「ゼロデイ攻撃とは」)
https://www.trendmicro.com/ja_jp/what-is/zero-day-attack.html

通常、OSなどにセキュリティ上の脆弱性が見つかった時、OSの提供者は修正プログラムを作成しユーザーに配布します。
ただ、それにもある程度の日数は必要です。

そこで、修正プログラムが配布される前にその脆弱性を利用してとことん攻撃をする、これが「ゼロデイ攻撃」です。ユーザーが無防備にならざるを得ない期間を狙ってくるのです。
ゼロデイ攻撃は、過去にも世界規模で被害をもたらしています。

特にサポートが終わったOSの場合、ひとつの抜け穴が見つかっても、OS提供者が対策をするわけではないので、同じ抜け穴から何度も何度も攻撃を仕掛けてくることでしょう。

鍵のない家に住んでいる、あるいは泥棒に合鍵を握られたまま鍵交換をしていないようなものです。

サポートの終了時期がわかっているWindows 10の場合、すでに見つかっているWindows 10の脆弱性を、サポート終了と同時に一気に悪用し攻撃を仕掛ける、というのは想像に難くありません。
警備員がいなくなる日時がわかっているのですから、もちろん、最初のターゲットはサポート切れのOSを使っている端末ということになるでしょう。

今すでに虎視眈々とその瞬間を狙っているサイバー攻撃者が多くいても、おかしなことではありません。

トレンドマイクロ「ゼロデイ攻撃とは」
https://www.trendmicro.com/ja_jp/what-is/zero-day-attack.html

どのような対策を取るべきか

では、 Windows 10のサポート終了に向けて、企業はどのように備えていくべきでしょうか。

まず大原則は、「新しいOSにアップデートする」ことです。

Windows 11へのアップデート

今回であればまず、Windows 11への移行が考えられます。

そこで、Windows 11への移行にあたって、マイクロソフトに寄せられているQ&Aの一部を以下にご紹介していきます。

Q：無料でアップグレードできますか？
A：Windows 10から Windows 11へのアップグレードは無料です。 ただし、ダウンロードのサイズにより、従量制課金接続で発生するダウンロードに対しては ISP 料金が適用される場合があります。

Q：現在のWindows 10 PCでWindows 11を使用できるようになるのはいつですか？
A：特定の PC で Windows 11のテストと検証が完了すると、Windows Update はアップグレードのインストールの準備ができたことを示します。
PC が対象かどうかを確認するには、PC 正常性チェック アプリをダウンロードします。

Q：Windows 11は現在のアクセサリで動作しますか？
A：Windows 10で動作していたほとんどのソフトウェアとアクセサリは、Windows 11で動作することが期待されています。 製品の詳細については、ソフトウェアの発行元またはアクセサリの製造元にお問い合わせください。

Q：アップグレードの際に個人ファイルはどうなりますか？
A：既定のエクスペリエンスでは、ファイルとデータが新しいインストールと共に移行されます。 とはいえ、新しい Windows バージョンをインストールする前には、常にファイルをバックアップすることをお勧めしています。既にファイルを OneDrive に同期している場合は、バックアップを作成するために追加の操作を行う必要がない可能性があります。

マイクロソフト「Windows 11 へのアップグレード: よくあるご質問」
https://support.microsoft.com/ja-jp/windows/windows-11-%E3%81%B8%E3%81%AE%E3%82%A2%E3%83%83%E3%83%97%E3%82%B0%E3%83%AC%E3%83%BC%E3%83%89-%E3%82%88%E3%81%8F%E3%81%82%E3%82%8B%E3%81%94%E8%B3%AA%E5%95%8F-fb6206a2-1a0f-448a-80f1-8668ee5b2bf9

「ESU=Windows 10 拡張セキュリティ更新」の利用

また、マイクロソフトは「Windows 10 拡張セキュリティ更新(=ESU)」というものを用意しています。これは、Windows 10のサポート終了後も、登録済みのPCに重要なセキュリティ更新プログラムが配信されるというもので、有料です。

しかし配信されるのはセキュリティの更新プログラムであって、他の種類の更新プログラムや技術サポートを提供するものではありませんし、永遠に続くものではありません。価格と登録条件は今後公表されます。

マイクロソフト「Windows 10、Windows 8.1、Windows 7 のサポート終了について」
https://www.microsoft.com/ja-jp/windows/end-of-support

移行中に注意すべきこと

これからWindows 11に以降する場合も、注意したい点があります。

まず、周辺機器のセキュリティを見直すことです。OSをアップデートしても、IoT機器に抜け道があれば危険性は残ります。

また、すでにWindows 11で発見された脆弱性について把握しておくことです。

独立行政法人情報処理推進機構は、マイクロソフト製品の脆弱性について発信しています。例えば昨年7月には、すでにWindows 11に対してマイクロソフトが提供している修正プログラムの適用方法が紹介されています。

「ゼロデイ攻撃」からなるべく身を守るためにも、最新情報をチェックしておきましょう。

OSやソフトウェアのアップデートは、業務や生活を便利にするためには欠かせないことです。「慣れているから変えたくない」という理由だけで古いものを使い続けることのリスクを認識し、今年のサポート終了に向けて今のうちから対策を考えておきましょう。

独立行政法人情報処理推進機構「Microsoft 製品の脆弱性対策について(2024年7月)」
https://www.ipa.go.jp/security/security-alert/2024/0710-ms.html

＜清水 沙矢香＞

2002年京都大学理学部卒業後、TBSに主に報道記者として勤務。社会部記者として事件・事故、テクノロジー、経済部記者として各種市場・産業など幅広く取材、その後フリー。

取材経験や各種統計の分析を元に多数メディアに寄稿中。

レベル1_#19_取引先からの信頼獲得のために　情報セキュリティの「ISMS認証」について知ろう

掲載日：2025/2/11



photo AC「USBメモリとsecurityの文字」

https://www.photo-ac.com/main/detail/25966389

サイバー攻撃による機密情報や個人情報の流出が相次いでいます。

サイバーセキュリティが非常に重視されるようになった今、大企業だけでなく中小企業でも対策をしっかりしていかなければなりませんし、情報セキュリティをどれだけ講じているかが取引先からの信頼関係にも繋がるようになっています。

そして、自社の情報セキュリティが一定の水準を満たしていることを証明してくれる国際規格があります。

「ISMS認証」と呼ばれるものです。

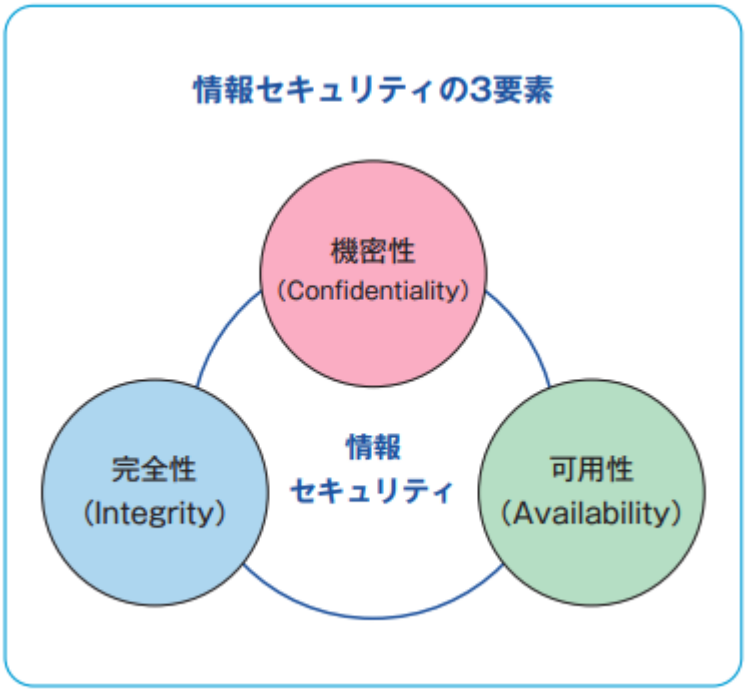
ISMS認証を受けていることは企業にとって良いアピールポイントになります。

ここではISMS認証の概要をご説明します。

ISMS認証とは

まず「ISMS」とは、Information Security Management System（情報セキュリティマネジメントシステム）の略です。

ひとくちに「情報セキュリティ」と言っても、具体的には3つの要素があります。



情報セキュリティの3要素
(出所：一般社団法人情報マネジメントシステム認定センター「ISMS適合性評価制度」)
https://isms.jp/doc/JIP-ISMS120-71.pdf p2

それぞれ具体的には、

情報が漏えいしないようにし（機密性）、
改ざんや誤りがないようにし（完全性）、
そして必要なときに必要な人が利用できるようにする（可用性）

というものです。情報セキュリティの維持には、情報流出への対策だけではなく、その運用も大切です。

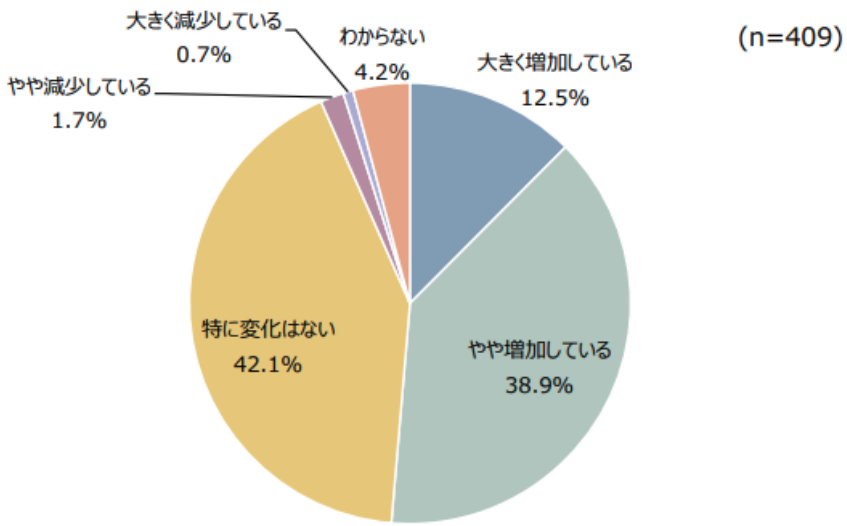
また、技術的な要素だけでなく、従業員への教育や訓練、組織体制の整備なども要件として含まれています。

ISMS認証の重要性

企業における情報セキュリティの高さは、取引先からも重視されています。

三菱UFJリサーチ&コンサルティングの調査によれば、発注元企業から情報セキュリティに関する条項を提示されたり義務付けられたりすることが「大きく増加している(12.5%)」、「やや増加している(38.9%)」との結果が得られています。

図表 20 販売先（発注元企業）との契約締結時の情報セキュリティに関する条項・取引上の義務・要請の頻度（SA）

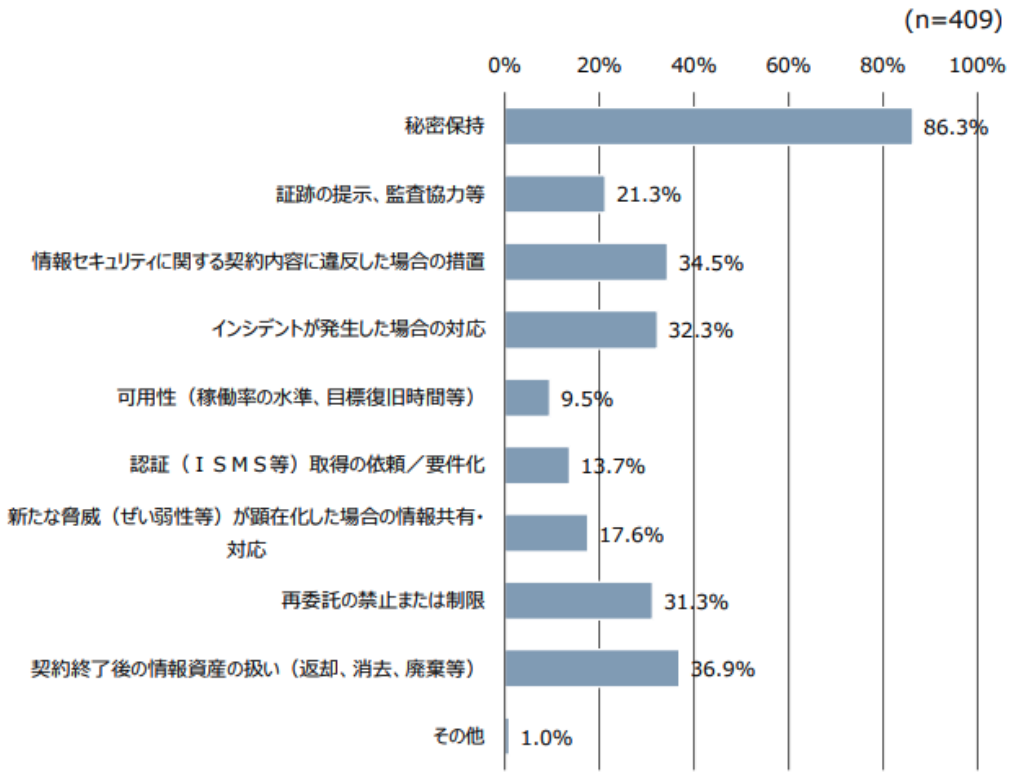


(出所：三菱UFJリサーチ&コンサルティング「中小企業における情報セキュリティ対策の最新動向～脅威の認識が難しい中でも、対策を普及させるため必要な施策とは～」)
https://www.murc.jp/wp-content/uploads/2024/05/seiken_240516_01.pdf p13

情報セキュリティも取引の条件になりつつあるのです。

その具体的な内容は下の通りです。

図表 21 販売先（発注元企業）との契約締結時の情報セキュリティに関する条項・取引上の義務・要請の内容（SA）



販売先との契約にあたっての情報セキュリティに関する条項など

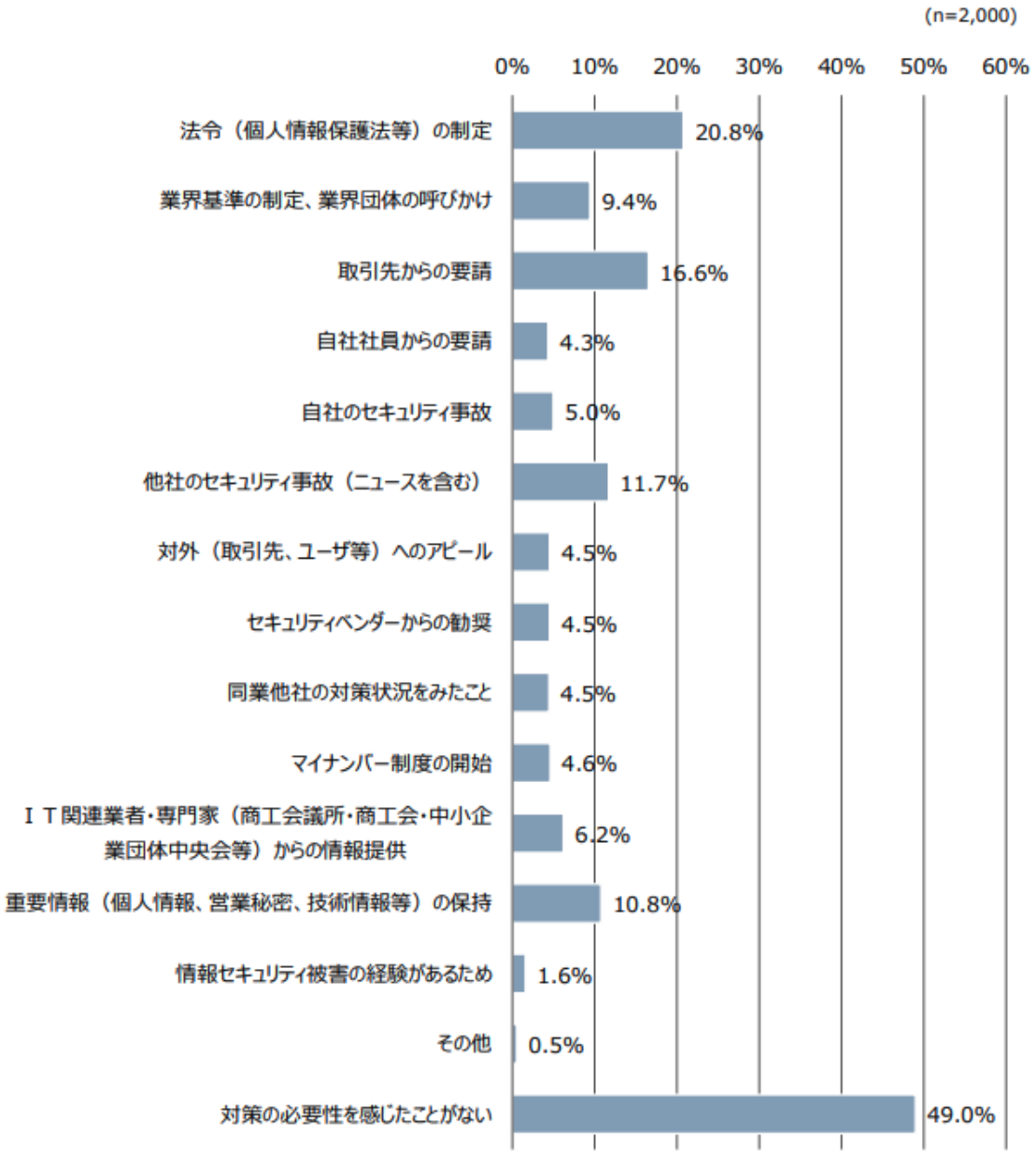
(出所：三菱UFJリサーチ&コンサルティング「中小企業における情報セキュリティ対策の最新動向～脅威の認識が難しい中でも、対策を普及させるため必要な施策とは～」

https://www.murc.jp/wp-content/uploads/2024/05/seiken_240516_01.pdf p13

機密保持(86.3%)は当然のことですが、ISMSなどの認証取得の依頼・要件化(13.7%)というのも一定の割合で意識されています。

一方で中小企業では、自社が情報セキュリティ被害に遭う可能性を感じている企業が4割以上にのぼっているものの、半数近くは「対策の必要性を感じたことがない」としています。

図表 10 情報セキュリティ対策の必要性を感じたきっかけ（MA）



情報セキュリティ対策の必要性を感じたきっかけ

(出所：三菱UFJリサーチ&コンサルティング「中小企業における情報セキュリティ対策の最新動向～脅威の認識が難しい中でも、対策を普及させるため必要な施策とは～」

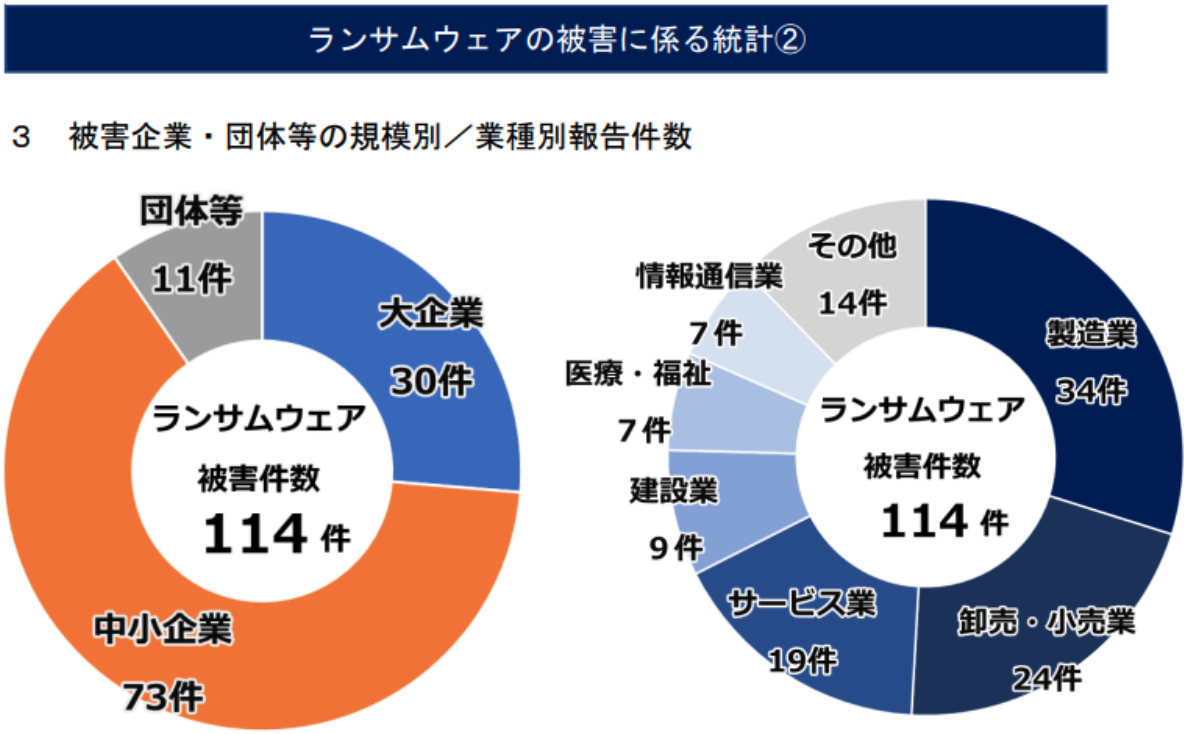
https://www.murc.jp/wp-content/uploads/2024/05/seiken_240516_01.pdf p6

「企業規模が小さくターゲットにされないと思うため」というのがおもな理由ですが、それは誤った認識です。

三菱UFJリサーチ&コンサルティング「中小企業における情報セキュリティ対策の最新動向～脅威の認識が難しい中でも、対策を普及させるため必要な施策とは～」
https://www.murc.jp/wp-content/uploads/2024/05/seiken_240516_01.pdf p8

中小企業ほど狙われやすいという事実

警察庁の統計によると、2024(令和6年)にランサムウェア(ファイルを暗号化し、解除の条件として金銭を要求するサイバー攻撃)の被害に遭った企業の規模と業種は下のようになっています。



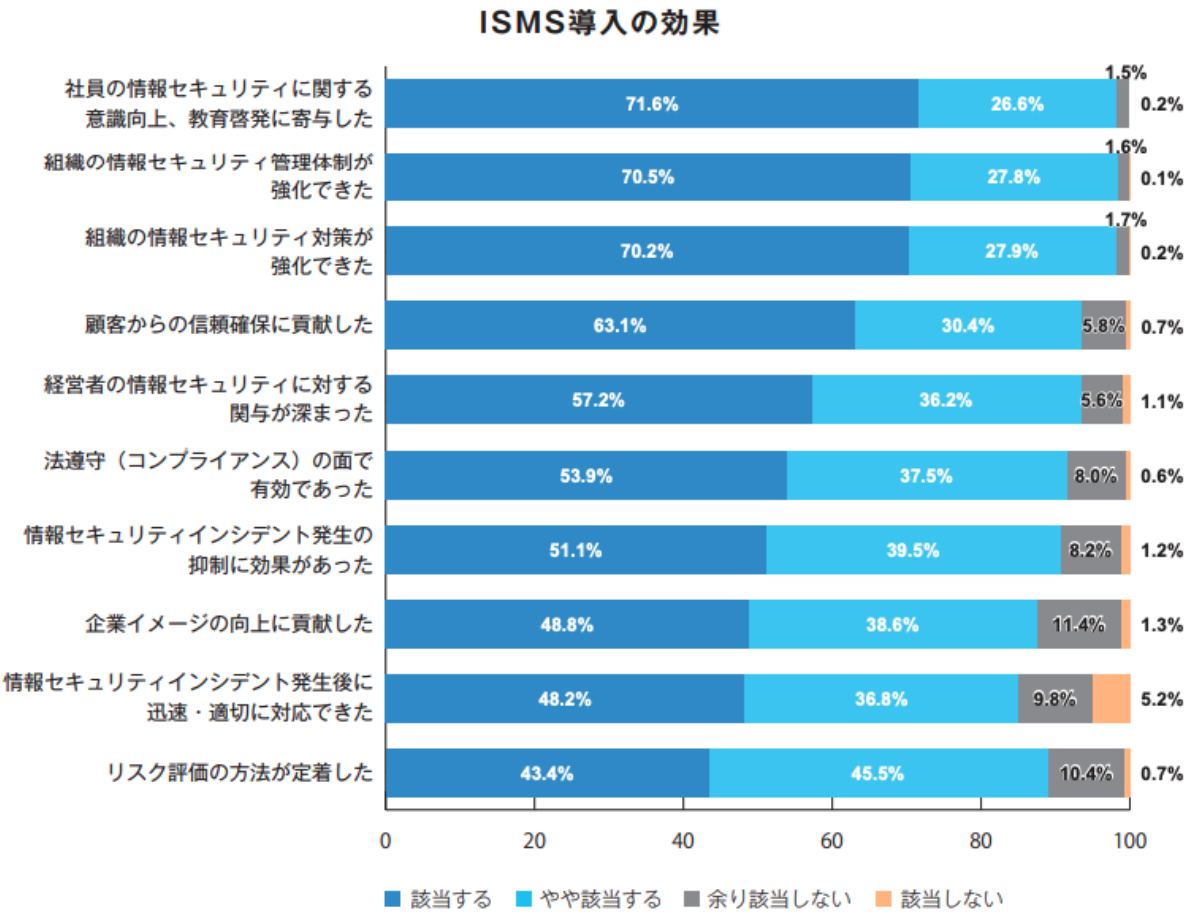
(出所：警察庁「令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について」)
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf p36

被害の多くは、じつは中小企業に集中しているということがわかります。
よって、甘く考えることはできません。

「ISMS認証」は国際規格

このような中、ISMS認証を取得することは、取引上の信頼もそうですが、実際に一定のセキュリティ体制を構築できるだけでなく、社内の意識を高めることにも繋がります。

実際、ISMSの導入により、下のような効果が得られています。



ISMS導入の効果

(出所：一般社団法人情報マネジメントシステム認定センター「ISMS適合性評価制度」)

https://isms.jp/doc/JIP-ISMS120-71.pdf p6

実際にセキュリティが高まった、あるいは組織の中でセキュリティに関する意識が高まった、管理体制ができるようになった、といったことはもちろんですが、多くの企業に「顧客からの信頼関係に貢献した」「企業イメージの向上に貢献した」という恩恵をもたらしていることがわかります。

ISMS認証を受けるには

では、ISMS認証を受けるにはどのような手続きが必要かをご紹介します。

まず認証のための適合評価は、下のようなしくみになっています。



ISMS認証の流れ
(出所：一般財団法人日本情報経済社会推進協会「ISMS/ITSMS/BCMS/CSMS認証を取得するには」)
https://www.jipdec.or.jp/project/smpo/ninsyou.html

企業がISMS認証を取得しようとする時、まず相談や申請をする相手は「認定された認証機関」です。

「認定された認証機関」とは、一般社団法人情報マネジメントシステム認定センター(ISMS-AC)による認定を受けた特定の団体や企業です。

ネットで「ISMS認証」を検索すると多くの企業が出てきますが、一般社団法人情報マネジメントシステム認定センター（ISMS-AC）の認定を受けていない団体や企業を通じて申請すると、自社のホームページなどに認定シンボルマークを使用できないので注意が必要です。

なお、2024年9月27日時点でISMS認証機関と認定されているのは以下の団体および企業です。

ISMS認証機関一覧

2024年9月27日

「ISMS認証機関」

認定番号	機　関　名　称
ISR001	一般財団法人　日本品質保証機構　マネジメントシステム部門
ISR002	日本検査キューエイ株式会社
ISR004	BSIグループジャパン株式会社
ISR005	一般財団法人日本科学技術連盟　ISO審査登録センター
ISR006	日本規格協会ソリューションズ株式会社　審査登録事業部
ISR007	株式会社日本環境認証機構
ISR008	DNV ビジネス・アシュアランス・ジャパン株式会社
ISR010	国際マネジメントシステム認証機構株式会社
ISR011	一般社団法人日本能率協会　審査登録センター
ISR012	ベリージョンソン ホールディング 株式会社 ベリージョンソン レジストラー
ISR013	一般財団法人電気通信端末機器審査協会　ＩＳＭＳ審査登録センター
ISR015	テュフ　ラインランド　ジャパン株式会社
ISR016	株式会社マネジメントシステム評価センター
ISR017	株式会社　ジェイーヴァック
ISR018	ビューローベリタスジャパン株式会社　システム認証事業本部
ISR019	公益財団法人　防衛基盤整備協会　システム審査センター
ISR021	ＳＧＳジャパン株式会社
ISR022	一般財団法人ベターリビング　システム審査登録センター
ISR023	日本海事検定キューエイ株式会社
ISR024	国際システム審査株式会社
ISR025	エイエスアール株式会社
ISR026	日本化学キューエイ株式会社
ISR027	ドイツ品質システム認証株式会社
ISR028	一般財団法人　電気安全環境研究所　ISO登録センター
ISR029	アイエムジェー審査登録センター株式会社
ISR030	アームスタンダード株式会社
ISR031	ＩＳサーティフィケーション株式会社

ISMS認証機関
(出所：一般社団法人情報マネジメントシステム認定センター「ISMS認証機関一覧」)
https://isms.jp/lst/isr/index.html

申請からISMS認証登録までには、最短で3~4か月かかります。

また、ISMS認証の取得範囲には制限がありません。例えば事業部・部・課単位、プロジェクト単位といった範囲で認証を取得することも可能ですので、優先順位をつけて必要性の高い部門でまず認証を受ける、という選択肢もあります。
中小企業には取り入れやすい選択肢でしょう。

現代ではサプライチェーン全体がネットワークでつながり、サイバー攻撃の入り口はどこにあるかわからなくなっています。

直接攻撃を受けていなくても被害の理由が取引先にあったり、逆に取引先が受けたサイバー攻撃が自社に影響を及ぼすこともありえます。

安心して取引ができる環境を作るためにも、自社の認定取得や、認定を取得している相手を積極的に選んでいく、という意識が必要です。

一般財団法人日本情報経済社会推進協会「FAQ2：認証取得条件」
https://www.jipdec.or.jp/project/smpo/FAQ2.html

一般財団法人日本情報経済社会推進協会「ISMS/ITSMS/BCMS/CSMS認証を取得するには」
https://www.jipdec.or.jp/project/smpo/ninsyou.html

<清水 沙矢香>
2002年京都大学理学部卒業後、TBSに主に報道記者として勤務。社会部記者として事件・事故、テクノロジー、経済部記者として各種市場・産業など幅広く取材、その後フリー。
取材経験や各種統計の分析を元に多数メディアに寄稿中。

レベル1_#20_IT導入補助金も活用できる！「サイバーセキュリティお助け隊サービス」とは

掲載日：2025/2/18



photo AC「写真素材：サイバー攻撃」

https://www.photo-ac.com/main/detail/23503678/23503677

サイバー攻撃は、高度化・巧妙化し、中小企業やサプライチェーンも例外なく脅威にさらされています。

「サイバーセキュリティお助け隊サービス」とは、中小企業へのサイバー攻撃を防ぐために欠かせないサービスをワンパッケージにまとめたもので、民間の事業者から提供されます。

IT導入補助金による導入支援制度も用意され、経済産業省も普及を後押ししています。

独立行政法人　情報処理推進機構（IPA）は、中小企業が利用しやすい安価なセキュリティサービスの開発を目指して実証事業を実施し、その実証事業で得られた知見をもとに、中小企業向けセキュリティサービスが満たすべき基準を設定しました。

「サイバーセキュリティお助け隊サービス」についてわかりやすく解説します。

実証事業でわかった重大なインシデントと実態

IPAが2019年度と2020年度の2年にわたって実施した「サイバーセキュリティお助け隊」の実証事業とはどのようなものだったのでしょうか。
また、その実証事業でどのような知見が得られたのでしょうか。

2019年度実証事業の概要

まず、2019年度は、全国8地域19府県で、地域の団体、セキュリティ企業、保険会社が実施体制を組み、実証事業を実施しました。参加した中小企業は、1,064社でした。

この事業では、中小企業に対して事前対策の促進や意識喚起をしつつ、攻撃実態、対策ニーズを把握しました。
出所）IPA「中小企業向けサイバーセキュリティ事後対応支援事業（サイバーセキュリティお助け隊）成果報告書（概要版）」（2020年4月）pp.1-2
https://www.ipa.go.jp/archive/files/000082723.pdf

この実証期間中に、重大なインシデントの可能性ありと判断し、対処を行った件数は128件。対処を怠った場合の被害想定額が5,000万円近くなる事案もありました（図1）。

こうした実証によって、実証参加前後の中小企業の意識変化や、お助け隊サービスに求められる機能が明らかになりました。

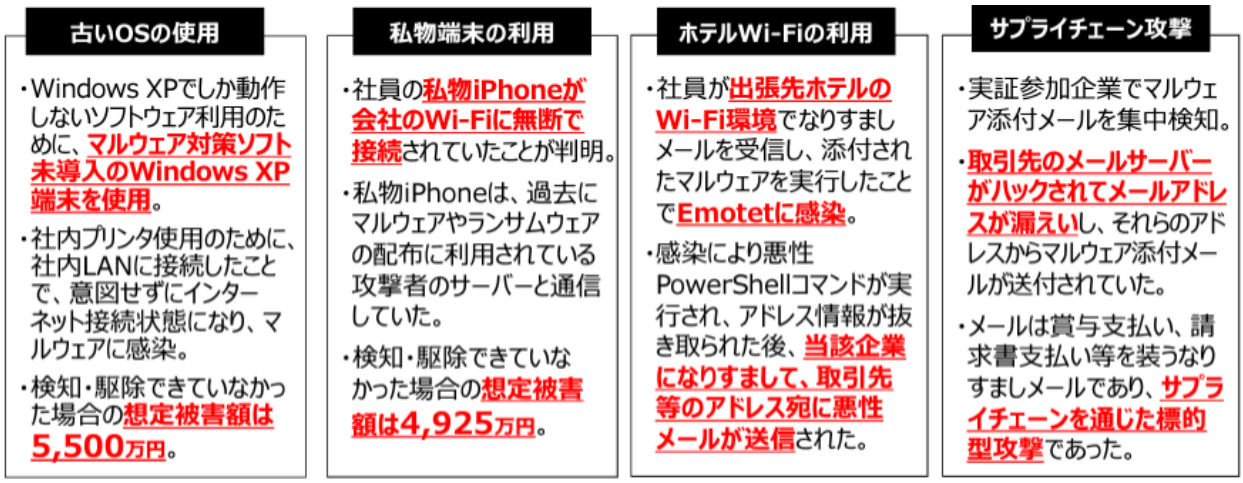


図1　駆け付け支援の対象となった特徴的な対応事例

出所）経済産業省「サイバーセキュリティお助け隊について」p.2

https://www.mhlw.go.jp/content/10808000/000943452.pdf

なお、「インシデント」とは、セキュリティの事故・出来事のことです。

インシデントに該当するのは、たとえば、情報の漏えいや改ざん、破壊・消失、情報システムの機能停止、あるいはこれらにつながる可能性のある事象です。

出所）IPA「中小企業のための　サイバーインシデント対応の手引き」（2024年7月）p.3

https://www.ipa.go.jp/security/sme/f55m8k0000001wpz-att/outline_guidance_incident.pdf

2020年度実証事業の概要

2020年度の実証事業は2019年度事業の結果を踏まえ、地域特性や産業特性を考慮したマーケティングを行うため、13地域24道県と、「防衛・航空宇宙産業」「自動車産業」の2産業分野の中小企業を対象に実施しました。参加企業は計1,117社でした。

2021年度以降の民間でのサービス展開に繋げるために行った検討内容は、サービス内容のスリム化や導入、運用負荷の低減です。

この実証事業では、セキュリティ機器による検知や脆弱性診断の結果に基づいて、合計293件のインシデント対応のほかに、技術的支援を行いました。

また、セキュリティ機器の導入・設置支援のための訪問対応が257件と多く、2019年度事業と同様に、中小企業ではセキュリティ監視機器を自力で設置するのが困難な状況が確認されました。
出所）IPA「（令和2年度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）全体報告書（概要版）」（2021年5月）pp.4-5, p.28
https://www.ipa.go.jp/security/reports/sme/ug65p90000019dx6-att/000091308.pdf

実証事業で明らかになった実態

2020年度の実証事業によって明らかになった、中小企業のサイバーセキュリティ対策の実態は以下のようなものでした。

- 業種や規模を問わずサイバー攻撃の脅威にさらされており、ウイルス対策ソフトなどの既存対策だけでは防ぎきれていない。
- インターネット上に公開しているホームページやサービスサイトなどの脆弱性診断では、対象企業のほとんどに何らかの脆弱性（弱点）が発見された。さらに、そのうち約2割の企業では、重大なインシデントにつながる可能性があると診断された。
- セキュリティ対策上の課題としては、専門人材の不足、社員や専門人材に対する教育不足、費用を捻出することが困難、といった声が寄せられた。
- セキュリティ対策に予算は全くかけていない、あるいは最低限の対策費用しかかけていないという企業が多かった。セキュリティ対策に支払可能な金額としては、月額1万円程度と回答する中小企業が多かった。

出所）IPA「サイバーセキュリティお助け隊（令和2年度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）の報告書について」（2021年6月）
https://www.ipa.go.jp/security/reports/sme/otasuketai_houkoku2021.html

「サイバーセキュリティお助け隊サービス」とは

実証事業で得られたこうした知見に基づいて、実証参加事業者がサービスを開発し、サービスブランドを設立しました。「サイバーセキュリティお助け隊サービス」の提供が始まったのは、2021年です。

コンセプトは、「中小企業に対するサイバー攻撃への対処として不可欠なサービスを効果的かつ安価に、確実に提供する」。

具体的には、以下のようなサービスを提供しています。

- UTM、EDRなどのセキュリティ監視ツールの設置と常時の監視
- 相談窓口による導入・運用に関するユーザーからの各種相談の受けつけ
- リモートでの支援
- 駆けつけ支援

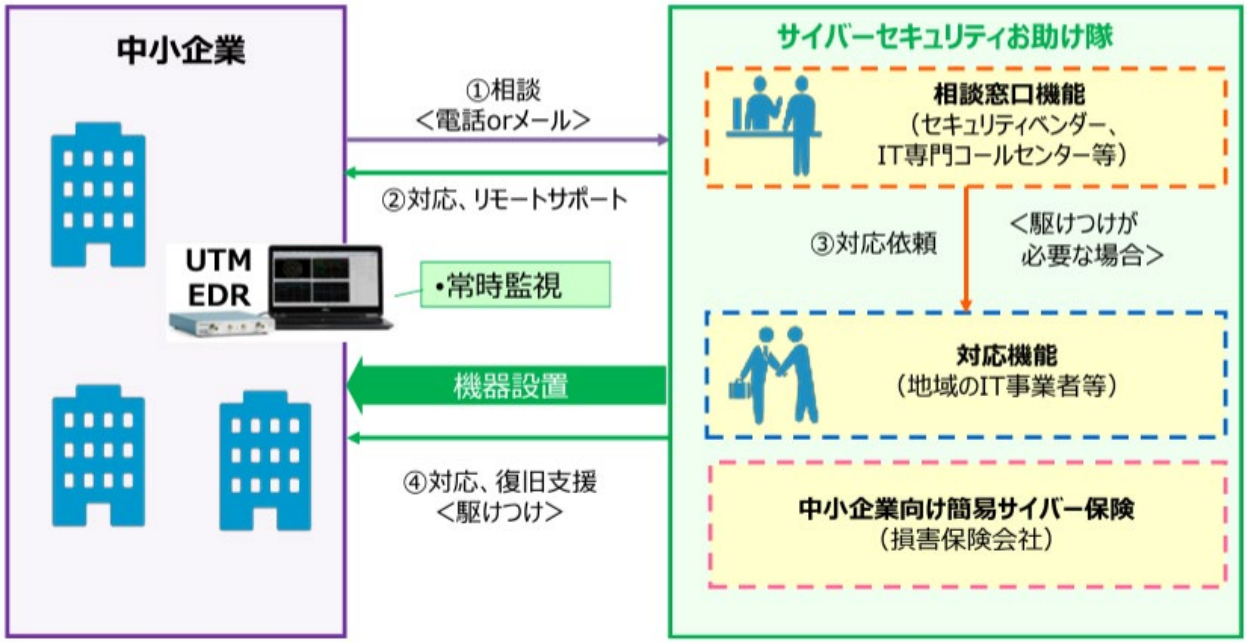


図2　サイバーセキュリティお助け隊サービスのイメージ

出所）経済産業省「サイバーセキュリティお助け隊について」pp.3-4

https://www.mhlw.go.jp/content/10808000/000943452.pdf

IPA「サイバーセキュリティお助け隊サービス」のウェブサイトには、サービスリストが載っており、日本地図から表示したい地域を選択してクリックすれば、選択した地域を対象としたサービスが表示されます。

地域区分は、北海道、東北、関東、中部、関西、中国、四国、九州、沖縄です。

このサービスで導入する監視型には、以下の3つがあり、それぞれの価格も同ウェブサイトから確認することができます。

1．　インターネットの出入口に設置し、包括的に防御するネットワーク監視型
2．　従業員が利用するPCなどの端末に導入し、監視する端末監視型
3．　ネットワーク監視型と端末監視型の両方を導入する併用型

サービスを利用している中小企業からは、以下のような声が寄せられています。

- 導入は全く問題なく実施できた。確認が必要な場合のアラートや、何も検知していないということがわかる点がよい。
- AIやアナリストが24時間365日、監視してくれている安心感がある。実際に検知した際に、どの挙動をブロックしたのか即座にわかるのもいい。

出所）IPA「サイバーセキュリティお助け隊サービス＞サイバーセキュリティお助け隊サービスリスト」
https://www.ipa.go.jp/security/otasuketai-pr/#service_area

「IT導入補助金」の活用

「サイバーセキュリティお助け隊サービス」は「IT導入補助金」を活用することができます。

IT導入補助金は、中小企業や小規模事業主を対象に、さまざまな経営課題を解決するためのITツール導入を支援するための補助金で、2024年度は以下の5タイプの枠が設けられています。

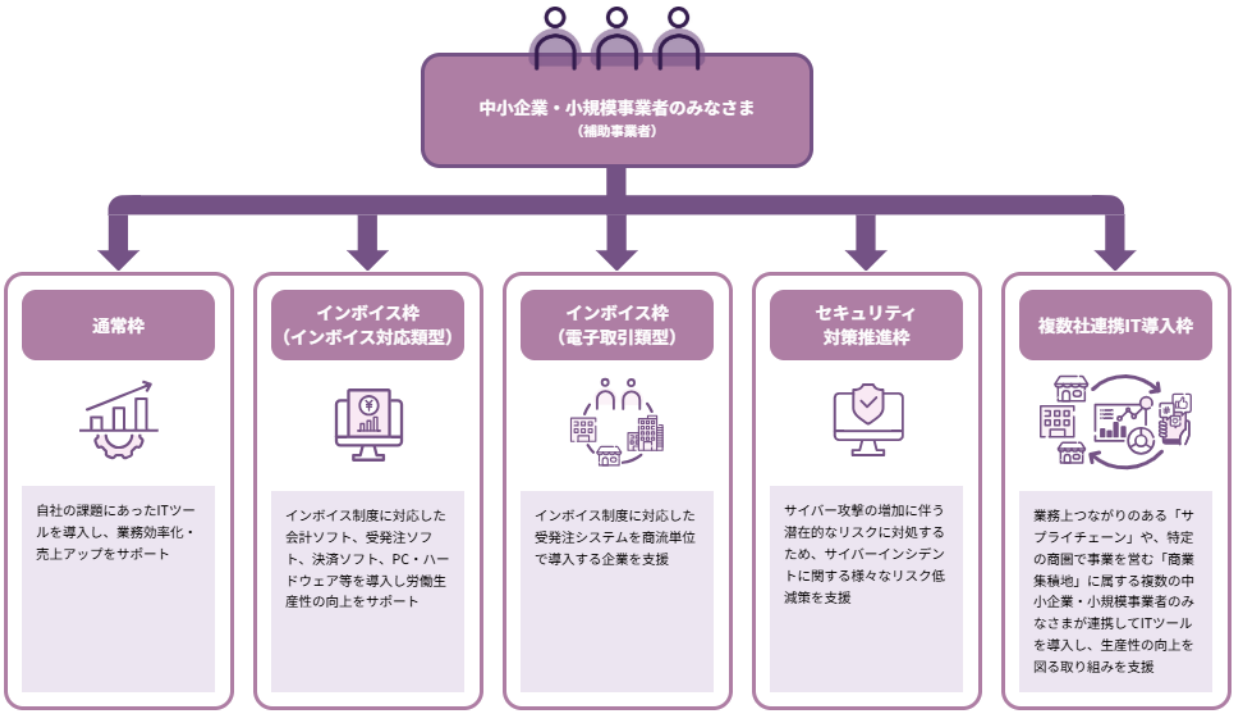


図3　IT導入補助金2024

出所）IT導入補助金事務局「IT導入補助金2024＞What is IT導入補助金2024」

サイバーセキュリティお助け隊サービス」は、このうち「セキュリティ対策推進枠」で補助金を申請することができます。

対象は、上掲の「サイバーセキュリティお助け隊サービスリスト」に掲載されているサービスのうち、IT導入支援事業者が提供し、かつ事務局に事前登録されたサービスの導入です。

補助されるのは、サービス利用料最大2年分で、補助率は1/2以内、補助金額は5万円以上100万円以下です。

サイバー攻撃事案の増加により高まる様々な潜在リスクの低減を支援

補助率	補助額
1/2以内	5万円以上100万円以下

図4　IT導入補助金「セキュリティ対策推進枠」における「サイバーセキュリティお助け隊サービス」への補助率・補助額

出所）IT導入補助金事務局「IT導入補助金2024＞セキュリティ対策推進枠」

また、「通常枠」でも、申請することができます。
ただし、「通常枠」を活用する場合には、「サイバーセキュリティお助け隊サービス」単体ではなく、オプションとして、メインツールと組み合わせて申請する必要がありますので、留意が必要です。

この際、「サイバーセキュリティお助け隊サービス」を申請する事業者は、申請採択の審査の際に加点対象となります。
出所）IPA（独立行政法人　情報処理推進機構）「サイバーセキュリティお助け隊サービス」
https://www.ipa.go.jp/security/otasuketai-pr/

申請受付は「セキュリティ対策推進枠」「通常枠」ともに、2024年度の最終回が2024年10月15日で締め切られていますが、次年度の詳細は下記から確認してください。
出所）IT導入補助金事務局「IT導入補助金2025＞事業スケジュール」
https://it-shien.smrj.go.jp/schedule/

おわりに

サイバー攻撃は、もはや大企業だけの問題ではありません。
中小企業も標的になりやすく、一度被害に遭うと、事業継続が困難になるおそれもあります。

補助金の活用を視野に入れ、「サイバーセキュリティお助け隊サービス」の導入を検討してみてはいかがでしょうか。

筆者プロフィール
＜横内美保子＞
博士（文学）。総合政策学部などで准教授、教授を歴任。専門は日本語学、日本語教育。
高等教育の他、文部科学省、外務省、厚生労働省などのプログラムに関わり、日本語教師育成、教材開発、リカレント教育、外国人就労支援、ボランティアのサポートなどに携わる。
パラレルワーカーとして、ウェブライター、編集者、ディレクターとしても働いている。

X：よこうちみほこ

Facebook：よこうちみほこ

レベル 2_#1_中小企業におけるセキュリティ脅威への対策強化　～不注意による情報漏えいの被害事例から対策を学ぶ～
掲載日：2024/7/1



独立行政法人情報処理推進機構（IPA）が毎年発行している「情報セキュリティ 10 大脅威」の中で、特に中小企業の経営者やシステム担当者が注目すべき点を、2024 年版に基づいて詳細に掘り下げていきます。今回は 6 位に挙げられている「不注意による情報漏えい等の被害」に焦点を当てます。これは長年にわたり頻繁に発生し続けており、この脅威がどのように業務に影響を与え、どのように対策すべきかを解説いたします。

「情報セキュリティ 10 大脅威（2024）」の組織編の一覧は下表のとおりです。

順位	「組織」向け脅威	初選出年
1	ランサムウェアによる被害	2016 年
2	サプライチェーンの弱点を悪用した攻撃	2019 年
3	内部不正による情報漏えい等の被害	2016 年
4	標的型攻撃による機密情報の窃取	2016 年
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2022 年
6	不注意による情報漏えい等の被害	2016 年
7	脆弱性対策情報の公開に伴う悪用増加	2016 年
8	ビジネスメール詐欺による金銭被害	2018 年
9	テレワーク等のニューノーマルな働き方を狙った攻撃	2021 年

順位	「組織」向け脅威	初選出年
10	犯罪のビジネス化（アンダーグラウンドサービス）	2017 年

情報セキュリティの落とし穴とされる不注意による情報漏えいは、知らず知らずのうちに発生することが多く、一度起こるとその影響は計り知れないものとなります。

「うちは中小企業だし、不特定多数の一般消費者を相手にするビジネスではないため、大量の個人情報は保有していないから、漏えいして困るような情報はないよ。」

中小企業の経営者の中にはこのような考えから、「自社はサイバーセキュリティによるリスクが低い」と過小評価していることが、事態を悪化させることもあります。

１．「中小企業はセキュリティによるリスクが低い」は本当？

中小企業であっても、日常的に行なっている業務の中でセキュリティリスクにつながる情報を取り扱っているのではないでしょうか。

・自社 HP に「問い合わせ」フォームを設けており、入力欄に問い合わせをしてきた人の所属組織や連絡先などを記載する箇所がある
・従業員が名刺交換した相手先の情報を Excel 等で一覧管理し、「顧客リスト」として保有している
・過去に採用試験を受けた方の履歴書を保管している

これらは全て、個人情報や個人データとなります。他にも業務で日常的に取り扱う顧客データや、パートナー企業から預かっている機密情報、従業員の住所や家族構成といった個人情報等、これら全てが潜在的なリスクを孕んでいます。こうした情報が漏えいした場合、信頼失墜、業務停止、収益の損失、法的責任など重大な結果を招くことになりかねないのです。このため、情報に関するセキュリティ対策は企業規模に関わらず全ての企業にとって必要な対策です。

では、実際に不注意によって情報が漏えいしてしまった具体的な事例をご紹介しながら、要因と対策をみていきましょう。

◆情報漏えいの具体的な事例

事例①　Google フォームの設定ミスによる個人情報漏えい

イベントの申し込み受付を Google フォームで行ったが、申し込みフォームを作成した際に設定ミスにより、申し込み後に申込者の一覧を閲覧できるリンクが表示されるようになっていた。

引用元：Security Next　https:/www.security-next.com/151685

事例②　メールを送信時に誤ったファイルを添付したことによる個人情報漏えい

メール送信先が多いため、同内容のメールを 14 回に分けて送信した際、そのうちの 1 回分において、本来添付するファイルとは異なるファイルを添付してしまった。

引用元：大阪市ホームページ

https://www.city.osaka.lg.jp/hodoshiryo/fukushi/0000620452.html

事例①の Google フォームの設定ミスは、フォーム作成時に回答後に表示される画面の確認をしないまま（動作チェックをしないまま）運用を開始したことが原因であり、人的ミスによる情報漏えいの典型的なケースです。これには、適切なチェック体制の欠如や、業務担当者の情報セキュリティに対する意識の低さが影響しています。

２．情報漏えいの要因は、人的不注意

不注意による情報漏えいはなぜ発生するのでしょうか。先の「情報セキュリティ 10 大脅威」の解説資料には、次のような要因が挙げられています。

◇情報リテラシーの低さ

従業員が扱う情報の機密性や重要性を理解していない場合、不用意に外部へ情報漏えいしてしまう可能性があります。例えば、次のようなケースが考えられます。

・重要情報が記載されたメールの宛先を間違う
・重要情報が入った端末を紛失する
・重要情報を私的に利用して外部の Web サイト等に公開する

◇情報を取り扱う際の本人の状況

体調不良や多忙等の状況により、情報を取り扱う従業員の注意力が散漫になり、メールの誤送信等のミスによる情報漏えい事故を起こしてしまうことがあります。

◇組織規程および情報を取り扱う手順の不備

外部に情報を持ち出す際の確認手順や作業時の確認手順等に関するプロセスに不備があると、情報漏えい事故を起こしてしまう可能性が出てきます。

３．中小企業による情報漏えいへの対策と対応

それでは、これらの要因を防ぎ、万が一事故が発生した場合の被害を最小限に抑えるためには、どのようにすればよいでしょうか。必要な対策、対応を「情報セキュリティ 10 大脅威」の解説資料をもとに一部加筆、抜粋して掲載します。

対策と対応①　情報リテラシー、モラルの向上
従業員が扱う情報の機密性や重要性を理解し、適切に扱うための教育を実施しましょう。
IPA が従業員研修で利用できる様々な研修テキスト例や動画教材を提供しています。これらをぜひ活用してください。
https://www.ipa.go.jp/security/kokokara/study/company.html

対策と対応②　ルール(手順)に基づく運用
情報の取り扱いに関する手順を明確化しましょう。さらに、従業員が確実に確認できるようにすることが大切です。例えば、Web でのアンケートフォームを作成する際などは、権限設定などを確認することをチェックリスト化して、複数人でチェックをするとよいでしょう。

対策と対応③　特定の担当者に業務が集中しない体制の構築
情報管理の責任者を明確化し、複数の従業員で重要な情報を共有するようにします。

対策と対応④　情報の重要度に応じた運用
扱う情報の重要度を分類し、それに合わせた運用（厳格な管理体制の構築）をしましょう。
また、情報ごとの重要度がいつでも確認できるようにしましょう。

対策と対応⑤　外部に持ち出す情報や端末の制限
持ち出し可能な情報や端末を制限し、持ち出しの記録を取る、持ち出し前に不必要な情報が格納されていないことを確認するなど厳格に管理しましょう。

対策と対応⑥ 適切なファイル送受信の運用
重要な情報が入ったファイルを相手に送信するときは、メールに直接ファイルを添付するのではなく、クラウド上のファイルストレージサービスの利用やファイルの暗号化など、安全なファイル送受信方法を検討してください。

セキュリティ対策が取られたファイルストレージでは、登録したファイルを特定の個人だけがアクセスできるように設定することができます。一般的には、ファイルを見せたい相手のメールアドレスなどを登録します。この方法を使うと、メールに直接ファイルを添付するよりも安全性が高いと言われています。

対策と対応⑦ メールの誤送信対策

メールソフトによっては、メール送信前に「このアドレスで本当に良いですか？」と確認を促す画面を表示させる機能や、送信者が送信ボタン押下後に「あ、間違えた！」と思った時に送信を取り消せるように 1 分間など予め設定した時間がたってからメールを送る機能が備わったものがあります。このようなソフトを使うことでメールの誤送信を減らすことができます。

漏えいが発生した（可能性を含む）時には、下記の対応が必要となります。

・早期の状況把握

問題発生時の内部報告体制を整備してください。

いつでも報告体制を確認できるようにしておきましょう。

外部からの連絡窓口を設置し、関係者が分かるようにしておきましょう。

・適切な報告／連絡／相談

問題が発生した場合、速やかに報告し、適切な対応を取れるよう社内・社外の関係組織や公的機関等と連携できるようにしておきましょう。

・インシデント対応体制の整備

問題発生時に迅速かつ的確に対応できる体制を整えます。

具体的な対応については、IPA の「中小企業の情報セキュリティ対策ガイドライン」の 46 ページからの（5）セキュリティインシデント対応をご覧ください。

ここまで不注意による情報漏えいの事例や影響、対策方法について考えてきましたが、いかがだったでしょうか。

不注意による情報漏えいはどの企業でも起こりやすく、その影響は甚大です。不注意を完全になくすことはできませんが、ルール整備や従業員への教育によるリテラシー及びモラル向上を図ることが、企業の持続可能な発展を支える鍵となるでしょう。

レベル 2_#2_中小企業におけるセキュリティ脅威への対策強化　～経営者がサイバーセキュリティ対策に関与することの必要性～
掲載日：2024/7/24



前回は、独立行政法人情報処理推進機構（IPA）の「サイバーセキュリティ 10 大脅威」の中から「不注意による情報漏えい等の被害」について解説しました。

今回は、サイバーセキュリティ対策を怠ることで「企業が被る不利益」と、「経営者が負う責任」について解説いたします。この情報は IPA が発行している「中小企業の情報セキュリティ対策ガイドライン 第 3.1 版」に基づいています。このガイドラインの「第 1 部 経営者編」の冒頭には、「企業が被る不利益」と「経営者が負う責任」を経営者が認識し、対策を自らの責任で考えなければならないと記されています。

1． 企業が被る不利益

インターネットの普及とともに、現代の企業が直面するリスクや不利益は、かつて予想されなかったような新たな問題が発生しています。代表的な例では、自社や他社の機密情報(営業上の機密)や個人情報の漏えいなどが挙げられ、これにより高額な賠償請求や金銭的損失を被る事態に陥ることがあります。

さらに、近年ではこうした事故による影響も多岐にわたり、金銭的損失だけでなく企業の信用やブランド価値が大きく傷つくケースも増加しています。
こうした事故による不利益は、**完全に排除することは技術的にも金銭的にも困難**と言えますが、適切なサイバーセキュリティ対策を行うことで、「**経営上受容できる範囲まで最小化する**」ことは可能です。

そのためにはまず、サイバーセキュリティへの理解を深め、対策が不十分なために引き起こす事故と、それにより企業が被る主な不利益を知ることが重要です。
被る不利益としては、次の４点が挙げられます。

（１）金銭的損失
（２）顧客の喪失
（３）事業の停止
（４）従業員への影響

いずれも企業に与える影響は金銭的な面、社会的信用の面でも大きく、事業の存続が困難になることがあります。それでは、これらの４点について事例を交えて解説していきます。

（１）「金銭的損失」

取引先などから預かった機密情報や個人情報を万一漏えいさせてしまった場合は、損害賠償請求を受けるなど、大きな経済的損失を受けることがあります。こうした事故はメディアでも比較的大きく取り上げられるため、企業における損失の代表ともいえます。
一方、こうした損害賠償などによる損失だけでなく、インターネットバンキングに関連した不正送金やクレジットカードの不正利用などで直接的な損失を被る企業の数も増えています。

事例１：九州電力系で変圧器の製造・販売などを手がけるキューヘンが**約 10 万 4000 件の個人情報が社外に漏洩**した可能性があると発表(2024 年 6 月 5 日)
不正アクセスによって個人情報のデータが暗号化されたことを 3 日に確認した。ランサムウエア（身代金要求型ウイルス）による攻撃とみている。
引用元：日本経済新聞社
https://www.nikkei.com/article/DGXZQOJC054CG0V00C24A6000000/

事例２：メールやショートメッセージサービス（SMS）、メッセージツール等を用いたフィッシングと推察される手口により、インターネットバンキング利用者のＩＤ・パスワード等を盗み、預金を不正に送金する事案が多発
令和５年 11 月末における**被害件数は 5,147 件、被害額は約 80.1 億円**となり、いずれも過去最多を更新
引用元：金融庁 https://www.fsa.go.jp/ordinary/internet-bank_2.html

事例１は、不正アクセスにより、**ランサムウエア（身代金要求型ウイルス）**の攻撃を許してしまった事例

で、人的ミスによる情報漏えいの典型的なケースです。
事例２は、メールや SMS などに添付された URL を開いた結果、ユーザ ID やパスワードの情報を盗まれて使用された例です。以前はメールや SMS の文章が不自然なものが多かったため、偽物と判別が容易でしたが、最近の生成 AI 等の台頭で本物と見分けがつかないような文章が送られてくる事が多く、こういった事案が増加しています。

（２）「顧客の喪失」

重要な情報に関する事故を起こした企業には必ず管理責任が問われます。中には企業の管理能力を疑問視され社会的評価が失墜することもあります。このため事故の発覚直後には顧客離れによる大きな業績ダメージを受けることになります。
また、大手メーカーのサプライチェーンに位置する企業の場合は、これまで継続してきた受注が停止に追い込まれることにもなりかねません。

（３）「事業の停止」

業務システムが利用できなくなると、生産活動や営業活動が停滞してしまいます。
例えば、受発注業務ができない、メールが利用できず顧客からの問い合わせメールに応答できない等です。
対象システムが中核となる事業を支えている場合、事業そのものの停止や取引先への影響も余儀なくされます。最悪のケースでは企業の存続にも影響が出てしまいます。

（４）「従業員への影響」

サイバーセキュリティ対策が不十分な職場環境は、従業員のモラル低下を招く大きな原因となります。
例えば、「**サイバーセキュリティルールがあるにもかかわらず、その規定が徹底されていない**」場合、従業員は「**これくらいは問題ないはず**」とルールを軽視した態度を取りがちです。
その結果、重大なセキュリティ事故が発生するリスクが高まります。そして事故が起きた際に、問題を引き起こした従業員のみを罰し、サイバーセキュリティルールを管理できなかった上司や管理職が責任を取らないような対応は、従業員の働く意欲を著しく損なう可能性があり、転職を検討するケースも出てくるでしょう。
さらに、従業員の個人情報が適切に保護されなければ、従業員から訴訟を起こされることも考えられます。
ある経営者は、「個別の損害より、職場環境が暗くなったことが最も困った」と述べています。

このように、サイバーセキュリティ対策の怠りが、企業に対しての多大な損失を生むことをご理解いただけた

かと思います。

次に、これらの損失以外に、経営者として負わなければならない責任について解説いたします。

２．経営者が負う責任

経営者がサイバーセキュリティ対策を的確に指揮しなかったことに起因する業績の悪化や、企業イメージの失墜などの責任は言うまでもありませんが、それ以外にも経営者が負うべき責任として「**法的責任**」と「**社会的責任**」が挙げられます。

（１）経営者などに問われる法的責任

企業の経営者や取締役には、民法・会社法により「取締役にふさわしく**ベストを尽くして経営に当たる義務**（善管注意義務）」を負い、「**その任務を怠ったときは、 株式会社に対し、これによって生じた損害を賠償する責任を負う。**（任務懈怠（けたい））」と規定されています。

サイバーセキュリティについても、経営者や取締役としてベストを尽くさなかった結果、 情報漏えいや製品・サービス供給の停止などの他企業や第三者に損害が生じた場合、善管注意義務違反や任務懈怠に基づく**損害賠償責任**を問われます。
また、法律によっては違反等が発生した場合に、経営者や取締役、担当者に対して**刑罰が科せら**れることもあります。
特に**個人情報保護法やマイナンバー法**に関する違反の場合は**行為者だけでなく事業者にも罰則が科せられる**ケースがあります。

（２）経営者などに問われる社会的責任

関係者や社会から適切に管理する条件でお預かりした情報を漏えいしてしまった場合に問われるのは、法的責任に加え、その情報の提供者や顧客などの関係者に対する責任もあります。
また、情報漏えい事故は、営業機会の喪失、売上高の減少、企業のイメージダウンなど、自社に損失をもたらすため、会社役員が会社法上の責任（会社に対する損害賠償責任）を問われ株主代表訴訟を提起されることもあり得ます。
さらには、取引先との信頼関係の喪失、業界全体のイメージダウンにもなってしまいます。

したがって、**サイバーセキュリティ対策は、顧客・取引先・従業員・株主などに対する経営者としての責**

任を果たすためにも重要です。

このようにサイバーセキュリティ対策は、企業の存続と発展に欠かせない重要な要素です。経営者自身がサイバーセキュリティの重要性を理解し、積極的に関与することで企業のリスクを最小限に抑えることができるとお判りいただけたかと思います。

次回は、具体的なセキュリティ対策について解説いたします。お楽しみに！

レベル 2_#3_中小企業におけるセキュリティ脅威への対策強化　～経営者は何をしなければならないのか 前編～

掲載日：2024/7/31



今回から前・後編に渡って中小企業の経営者が「サイバーセキュリティ確保に向けてどのように対応すべきか、具体的には何をしなければいけないのか」についてご紹介します。

独立行政法人情報処理推進機構（IPA）が発行している「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」に基づいて、今回は経営者が「認識すべき３原則（前編）」を、次回は「実行すべき重要７項目の取組（後編）」を解説していきます。

認識すべき３原則

これは、サイバーセキュリティ確保に向けて経営者の行動原則をまとめたものです。経営者が一番初めに悩むことは、「どうやって向き合うのか」つまり、自分の立ち位置や行動についてだと思います。

原則１「サイバーセキュリティ対策は経営者のリーダーシップで進める」

経営者は、サイバーセキュリティ対策の重要性を認識し、**自らリーダーシップを発揮**して対策を進めます。現場の従業員は業務の利便性が低下したり、面倒な作業を伴う対策には抵抗を感じたりすることがあり

ますが、**経営者が自ら意思決定し、自社の事業に見合った適切な対策を主導**する必要があります。

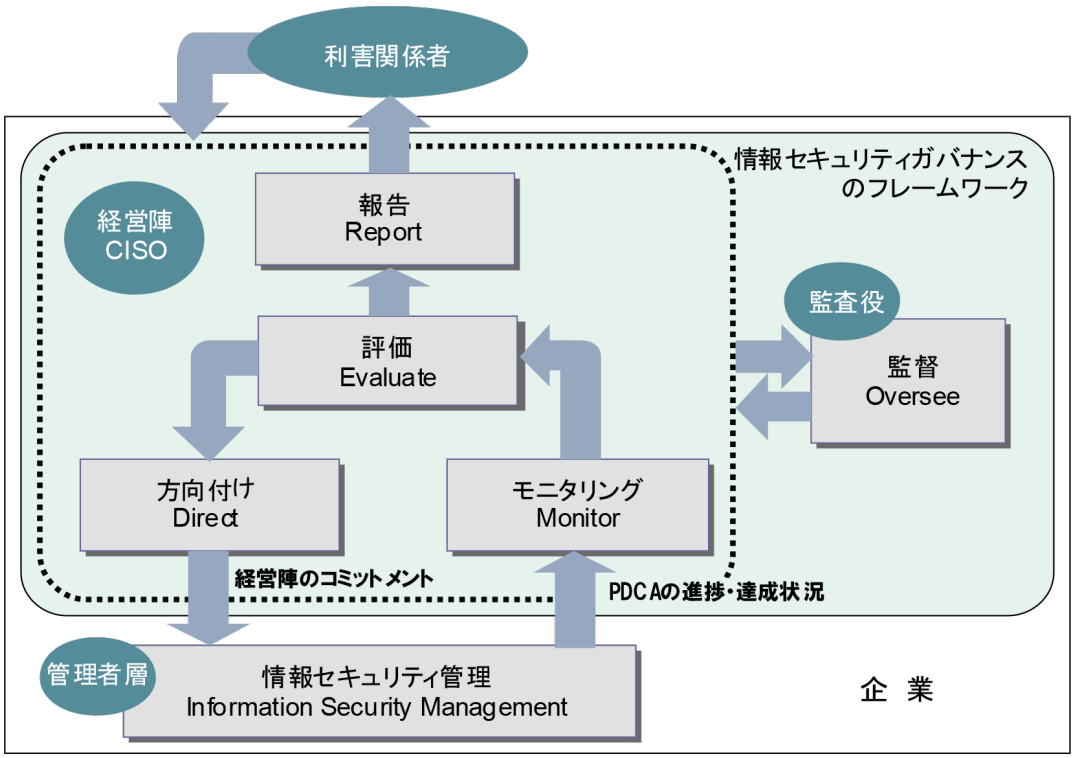
例えば、新しい事業を開始する場合を考えてみましょう。まず経営者が事業の適合性を判断し、その上で、事業環境を整えて、従業員を教育するでしょう。当然、新たな業務に抵抗する従業員も出るでしょうが、それを含めて事業を推進するのが一般的な経営者の役割と言えます。サイバーセキュリティ対策を新しい事業と置き換えてみれば、特別なものではないとお判りいただけると思います。

とは言っても、通常の事業と異なり、馴染みの薄いサイバーセキュリティを推進するのはハードルが高いものです。そこで、推進するにあたって有効な考え方の一つに、**情報セキュリティガバナンス**のフレームワークがあります。

◇情報セキュリティガバナンスのフレームワーク

経営者が企業戦略としてサイバーセキュリティ向上に取り組むための枠組みです。経営者がリーダーシップを発揮する枠組みでもあり、以下の４つの要素から成り立ちます。

1.方向付け：経営者が懸念する重大事故などを避けるための規則決定
2.情報セキュリティ管理（ISM）：対策の推進や点検の実施
3.モニタリング：対策の進捗や点検による不正行為防止等により状況を監視
4.評価：規則の効果を評価し、見直す



サイバーセキュリティガバナンスのフレームワーク

引用：IPA「中小企業の情報セキュリティ対策ガイドライン 第 3.1 版」12 ページ

参考：経済産業省『情報セキュリティガバナンスの概念』

https://www.meti.go.jp/policy/netsecurity/secgov-concept.html

これらの要素を実施することで、サイバーセキュリティガバナンスのフレームワークが整備され、企業全体でセキュリティ意識を高めることができます。

原則 2「委託先のサイバーセキュリティ対策まで考慮する」

業務の委託先に重要な情報を提供する場合、委託先がどのようなサイバーセキュリティ対策(サイバーセキュリティガバナンス)を行っているか考慮する必要があります。委託先に提供した情報が漏えいしたり、改ざんが発生した場合、それが委託先の不備だったとしても、委託元の企業も管理責任を問われることになります。

例えば、国税局の委託先企業がマイナンバーを含む個人情報を無断で別企業へ再委託した事件や、神奈川県からハードディスクの情報削除・破棄を依頼されていた企業の従業員がネットオークションで転売していた事件などは、大きく取り上げられました。

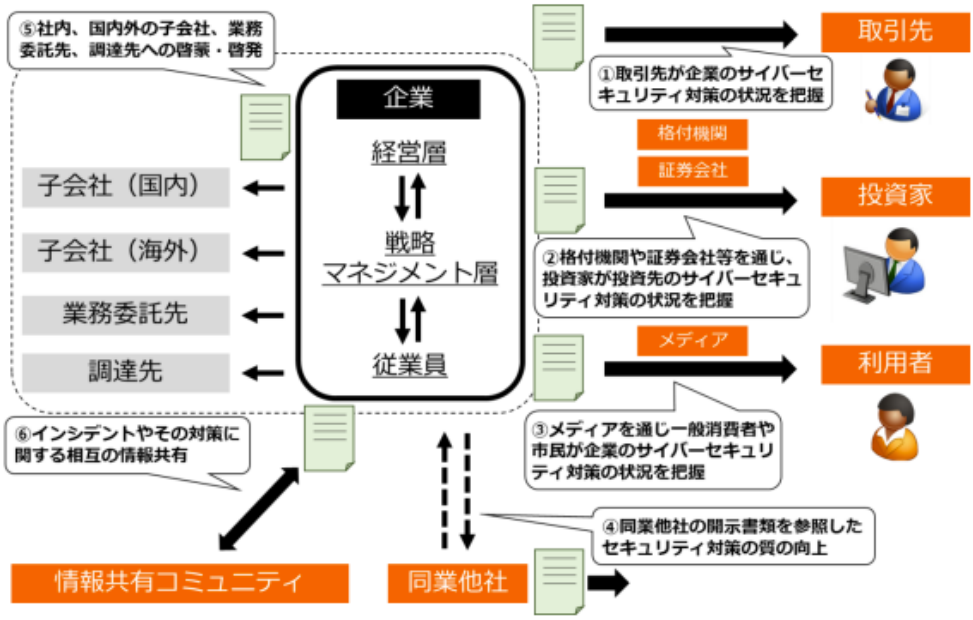
これらの事例から、委託先やビジネスパートナーなどのサイバーセキュリティ対策に関しても、自社同様に十分な注意を払う必要性があることがわかります。また、自社が親会社等から受託している場合には、サプライチェーンの一環として、親会社が求めるサイバーセキュリティ対策が必要となります。

◇セキュリティ対策の格差とサプライチェーン攻撃

全ての企業で十分なセキュリティ対策を講じる必要がありますが、それには、資金面・人材面などの企業体力が不可欠です。一般的に、中小企業は大企業のような体力を持ち合わせていないため、**大企業と同様の対策を講じることが難しい**場合が生じます。これを、**セキュリティレベルの格差**と呼びます。この格差を利用して、攻撃者はセキュリティレベルの低い企業を経由して重要な情報を狙います。
具体的には、最初にセキュリティ対策が甘い企業の PC を乗っ取り、踏み台にしてサプライチェーン内の別企業の重要な情報を搾取する攻撃を行うのです。

原則３「関係者とは常にサイバーセキュリティに関するコミュニケーションをとる」

業務上の関係者（顧客、取引先、委託先、代理店、利用者、株主など）からのセキュリティに関する信頼を高めるには、普段から自社のサイバーセキュリティ対策や、事故が起きたときの対応について、関係者に明確に説明できるように経営者自身が理解し、整理しておくことが重要です。 そうすることで、万が一インシデントが発生した際にも、適切な対応が取れ、必要以上の不安を与えることなく、信頼関係を維持することができます。



企業をとりまくステークホルダーとサイバーセキュリティ対策の情報開示
引用：総務省「サイバーセキュリティ対策情報開示の手引き」

例えば、第三者認証機関（ISMS/プライバシーマーク）を取得し、自社の HP に公開するなどのアピールも有効です。また、IPA が提供している、「**SECURITY ACTION**」の宣言も有効な方法と言えます。「SECURITY ACTION」は中小企業自らが、**サイバーセキュリティ対策に取組むことを自己宣言**する制度です(認証制度ではありません)。自己宣言事業者は SECURITY ACTION サイトへ自社を登録・検索することも可能です。そこに掲載されている取り組み事例を紹介いたします。

◇取組事例

企業名：有限会社シブヤ（代表取締役 渋谷勲）
従業員：３名
業　種：製造業（射出成形・金型設計製作等）
取組み段階：二つ星

宣言理由：わが社では WORD、EXCEL などの機密資料以外にも技術情報を含む加工データと呼ばれるものがあり、その保護につながると考えたからです。また、わが社の情報が盗まれる心配もありますが、それ以上にウイルス感染したデータをお客様に送ってしまうなど、関係者に迷惑をかけることは大問題だと考えていました。これまでセキュリティ対策としてはウイルス対策ソフトを導入している程度でしたが、SECURITY ACTION 宣言には費用がかからないし、一つ星であれば自分たちでも十分取組める内容と思ったため、すぐに申込みました。

一つ星の宣言以降、セキュリティの話題が多く出るようになり、弊社も二つ星を宣言することで、今後ワンランク上の御客様に「弊社はセキュリティ対策に取組んでおり安全です」とアピールできると思い（二つ星を）宣言しました。
（SECURITY ACTION サイト　取組紹介より抜粋）

ここまでサイバーセキュリティ確保に向けた経営者として「認識すべき３原則」についてご説明いたしました。サイバーセキュリティ対策は企業にとって欠かせない重要な要素です。経営者自身がその重要性を理解し、リーダーシップを発揮することで、全社的な取り組みが実現できます。

次回は、「実行すべき重要７項目の取組」について、詳しく解説いたします。お楽しみに！

レベル 2_#4_中小企業におけるセキュリティ脅威への対策強化　～経営者は何をしなければならないのか 後編～

掲載日：2024/8/7



独立行政法人情報処理推進機構（IPA）が発行している「中小企業の情報セキュリティ対策ガイドライン 第3.1版」から、前回に引き続き、経営者として「サイバーセキュリティ確保にどうやって向き合うのか、何をやらなければいけないのか」に焦点を当てています。

前回は「認識すべき３原則」についてご説明いたしました。今回はその続きとなる、「実行すべき重要 ７項目の取組」について説明します。

実行すべき重要７項目の取り組み

サイバーセキュリティを確保するために、経営者の役割と取り組みを説明します。経営者は、重要７項目の取組について、自ら実践するか、実際にサイバーセキュリティ対策を実践するうえでの責任者・担当者に対して指示をします。実施する内容によっては、経営者自らが実行しなければならない事もあります。例えば組織全体の取り組みなどです。

また、７項目のうち取組１～４は前回のメルマガで説明した「情報セキュリティガバナンスの構築」と言い換えることもできます。

取組１「サイバーセキュリティに関する組織全体の対応方針を定める」

サイバーセキュリティ対策を組織的に実施する意思を、従業員や関係者に明確に示すために、どのような情報をどのように守るかについて、自社に適した**サイバーセキュリティに関する基本方針を定め、明文化して宣言**します。自社の**経営において最も懸念される事態を明確にする**ことで具体的な対策を促し、組織としての方針を立てやすくなります。これは、前出の「SECURITY ACTION」の二つ星宣言の必要項目ともなっており、基本的には経営者が自ら実行しなければならないものの一つに挙げられます。

取組２「サイバーセキュリティ対策のための予算や人材などを確保する」

サイバーセキュリティ対策を実施するために、必要な予算と担当者を確保します。これには事故の発生防止だけでなく、**万が一事故が起きてしまった場合の被害の拡大防止や、復旧対応も含みます**。サイバーセキュリティ対策には高度な技術が必要なため、**専門的な外部サービスの利用**も検討します。
（前回ご説明した『情報セキュリティガバナンスのフレームワーク』2.ISM の計画）

取組３「必要と考えられる対策を検討させて実行を指示する」

懸念される事態に関連する情報や業務を整理し、損害を受ける可能性（**リスク**）を把握したうえで、責任者・担当者に対策を検討させます。**必要とされる対策には予算を与え、実行を指示**します。実施する対策は、社内ルールとして文書にまとめておくことで、従業員も実行しやすくなり、取引先などに取り組みを説明する際にも役に立ちます。実行を指示したサイバーセキュリティ対策がどのように現場で実施されているかについて、月次や四半期ごとなど適切なタイミングで報告させ、進捗や効果を把握します。
（『情報セキュリティガバナンスのフレームワーク』2.ISM の構築と実施）

取組 4「サイバーセキュリティ対策に関する適宜の見直しを指示する」

取組 3 で指示したサイバーセキュリティ対策について、**実施状況を点検**させ、取組 1 で定めた**方針に沿って進んでいるかどうか評価**します。また、業務や顧客の期待の変化なども踏まえて基本方針を適宜見直し、致命的な被害につながらないよう、**対策の追加や改善を行う**ように、責任者・担当者に指示します。
（『情報セキュリティガバナンスのフレームワーク』4.評価と方向性の見直し）

取組５「緊急時の対応や復旧のための体制を整備する」

被害範囲や根本原因を速やかに追究して被害の拡大を防ぐ緊急時の対応体制を整備します。同時に、緊急時の業務復旧に向けた、的確な復旧手順をあらかじめ作成しておくことで、適切な指示を出すことができます。整備後には予定どおりに機能するかを確認するため、被害発生を想定した模擬訓練を行い、従業員に対する意識づけや適切な対応が可能かを確認します。経営者のふるまいについても、あらかじめ想定しておけば、冷静で的確な対応が可能になります。また、この考え方はサイバーセキュリティインシデントにとどまらず、一般的な災害対策でも有効です。

取組６「委託や外部サービス利用の際にはセキュリティに関する責任を明確にする」

業務の一部を外部に委託する場合は、委託先でも少なくとも自社と同等の対策が行われるようにしなければなりません。そのためには契約書にサイバーセキュリティに関する委託先の責任や実施すべき対策を明記し、合意する必要があります。
IT システム（電子メール、ウェブサーバー、ファイルサーバー、業務アプリケーションなど）に関する技術に詳しい人材がいない場合、自社でシステムを構築・運用するよりも、**外部サービスを利用したほうが、コスト面から有利な場合があります**。ただし、安易に利用することなく、利用規約や付随するサイバーセキュリティ対策などを十分に検討するよう担当者に指示する必要があります。

◇参照：より良い外部サービスが選べる「サイバーセキュリティお助け隊サービス」
「サイバーセキュリティお助け隊サービス」は、中小企業等に対するサイバー攻撃への対処として不可欠なサービスを要件にまとめ、**ワンパッケージで安価に提供するサービス**です。所定の審査機関により要件を満たすことが確認された民間サービスを「サイバーセキュリティお助け隊サービス」として IPA が登録・公表しています。

サイバーセキュリティ対策のワンパッケージ例

⑴ 見守り：24 時間 365 日監視挙動や問題のある攻撃を検知し、あなたの PC とネットワークを守ります。
⑵ 駆付け：問題が発生したときに地域の IT 事業者等が駆付け対応します。
（リモート支援の場合あり）
⑶ 保険：簡易サイバー保険で駆付け支援等のサイバー攻撃による被害対応時に突発的に発生する各種コストが補償されます。

参考：サイバーセキュリティお助け隊サービスリスト

※『IT 導入補助金』(中小企業・小規模事業者のみなさまが IT ツール導入に活用いただける補助金)で「サイバーセキュリティお助け隊サービス」のサービス利用料の支援が受けられます。
参考：https://it-shien.smrj.go.jp/applicant/subsidy/security/

取組 7「サイバーセキュリティに関する最新動向を収集する」

情報技術の進歩の速さから、実施を検討すべき対策は目まぐるしく変化します。自社だけで全てのサイバーセキュリティ情報を把握することは困難です。この場合には、サイバーセキュリティに関する**最新動向を発信している公的機関**などを把握しておき、常時参照することでセキュリティリスクに備えるように担当者に指示します。また、知り合いや**コミュニティへの参加で情報交換**を積極的に行い、得られた情報について、自社内や委託先などと共有します。
参考：サイバーセキュリティに関する最新動向を発信している公的機関
・IPA（独立行政法人情報処理推進機構）
・NISC（内閣サイバーセキュリティセンター）

2 回に分けてサイバーセキュリティ確保に向けた、経営者としての「認識すべき 3 原則」と「実行すべき重要 7 項目の取組」と「関連するサービスに」ついてご説明しました。委託先を含め、会社規模や目的に合ったサイバーセキュリティ対策組織を作り、常に進化させることが最も重要なことと言えます。次回もお楽しみに！

レベル 2_#5_中小企業におけるセキュリティ脅威への対策強化　～ビジネスメール詐欺とは？事例から対策を学ぶ～

掲載日：2024/8/21



独立行政法人情報処理推進機構（IPA）が毎年発行している「情報セキュリティ 10 大脅威 2024」から、中小企業の経営者やシステム担当者が注目すべき点を掘り下げていきます。

今回は 8 位に挙げられている「**ビジネスメール詐欺による金銭被害**」に焦点を当てます。ビジネスメール詐欺による被害は長年にわたり頻繁に発生し続けており、この脅威がどのように業務に影響を与えるのか、対策はどうすべきかを解説いたします。



引用元：IPA　情報セキュリティ 10 大脅威　2024　解説書より

ビジネスメール詐欺とは

ビジネスメール詐欺とは、悪意のある第三者が**標的とする企業やその取引先の関係者などになりすまして偽のメールを送信し、金銭を騙し取ること**を目的としたサイバー攻撃です。この攻撃は、企業の従業員を標的にした振り込め詐欺とも言えるもので、ビジネスメール詐欺（Business　E-mail Compromise：BEC）と呼ばれています。

特に、企業の金銭の決裁権限を持つ責任者や直接金銭を取り扱う担当者などが攻撃の対象となることが多くなっています。

代表的なビジネスメール詐欺

ビジネスメール詐欺の具体的な手法をご紹介します。

（１）取引先からの請求書の偽装

攻撃者が取引先企業や担当者になりすまし、偽の請求書等をメールで送り付け、用意した口座に振り込ませる手口です。
また、ウイルス感染や不正ログイン等により、自社の従業員のメールアカウントが乗っ取られ、攻撃者が自

社の従業員になりすまして、取引実績がある別企業の担当者へ偽の請求等を送り付け、用意した口座に金銭を振り込ませることで、取引先が被害に遭うケースもあります。
このような場合、メール本文は巧妙に偽装され、送信元が本物のアカウントであるため、受信したメールが攻撃であることに気付きにくい事が特徴と言えます。

（２）経営者等の権威ある者へのなりすまし

攻撃者が企業の経営者や経営陣・役員等になりすまし、従業員に業務指示を模した内容の電子メールを送信し、用意した口座へ金銭を振り込ませる手口です。
通常の社内メールでの業務指示であるかのように偽装されるため、メールを受け取った従業員は「通常の業務」として何の疑問も抱かないのが、このなりすましの特徴です。
また、弁護士や監査法人、行政庁等の社外の権威ある第三者になりすます場合もあります。

このように、ビジネスメール詐欺の前提として、標的組織の情報の窃取が不可欠であることが分かります。
例えば、攻撃者が標的組織の経営者や経営幹部、または人事担当等の特定任務を担う従業員になりすまし、組織内の他の従業員の個人情報を窃取し「なりすます相手」を探すわけです。

では、ビジネスメール詐欺による金銭被害の具体的な事例をご紹介しながら、要因と対策をみていきましょう。

◆ビジネスメール詐欺による金銭被害の事例
【事例１．メールと電話を併用したなりすまし事例】
攻撃者は標的組織の会長になりすまし、同組織の海外関連会社の社長に対して機密プロジェクトの連絡等と称したメールを送信しました。さらに、同日に今度は同組織の専務になりすまし、メールのフォローアップを口実に電話で連絡をしました。攻撃者は発信元番号を何らかの方法で同組織の代表番号に偽装し、さらに専務の声を模倣していました。このケースでは、被害者が電話の会話からなりすましに気が付き、金銭的な被害等は発生しませんでした。
引用元：IPA 情報セキュリティ 10 大脅威 2024 解説書より抜粋

この事例は、会長のメールだけでは信用しない支社長も出る事を想定して、専務からのフォロー電話で信用させようとした点が特徴的と言えます。幸い、電話の内容が通常の専務の話す内容と異なり、偽物と気が付いたため、事なきを得ましたが、これもよくできた偽造メールであったら簡単に信用していたかもしれません。

【事例 2．信頼できる取引先を騙るメール詐欺】

医療製品メーカーの株式会社スリー・ディー・マトリックスは、支払口座の変更依頼が書かれた、取引先の名を騙るメールに従い、虚偽の銀行口座に総額 2 億円を振り込んだことを公表しました。その取引先とは創業以来の付き合いがあり、高い信頼関係があったため、同社は振込先口座の変更の理由を直接確認していませんでした。
引用元：IPA 情報セキュリティ 10 大脅威 2024 解説書より抜粋

この事例では、「長年信頼している会社からの依頼」という思い込みが最大の問題といえます。それほど付き合いの深くない取引先であれば、「急に取引口座をなぜ変える必要があるのか」と、ビジネス的な危機感を生むはずですが、長年の信頼がこの感覚を麻痺させていた事がこのなりすましを可能としています。

ビジネスメール詐欺による金銭被害への対策

では、次にビジネスメール詐欺による金銭被害への対策として、「被害の予防」の観点と「被害を受けた後の対応」を説明していきます。

（１）被害の予防

表 1.4 情報セキュリティ対策の基本

攻撃の糸口	情報セキュリティ対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消し攻撃によるリスクを低減する
ウイルス感染	セキュリティソフトの利用	攻撃をブロックする
パスワード窃取	パスワードの管理・認証の強化 ※「共通対策」で詳細を解説	パスワード窃取によるリスクを低減する
設定不備	設定の見直し	誤った設定を攻撃に利用されないようにする
誘導（罠にはめる）	脅威・手口を知る	手口から重要視すべき対策を理解する

（IPA「情報セキュリティ 10 大脅威 2024 解説書」より）

IPA の「情報セキュリティ 10 大脅威 2024 解説書」の 10 ページ、表 1.4「情報セキュリティ対策の基本」を実施することや、ビジネスメール詐欺による金銭被害への認識を高めることが重要です。また、下記に挙げる個別の対策も有効と言えます。

◆ガバナンスが適切に機能する業務フローの構築

金銭が絡む手続きをする際は、複数人で審査、承認をする業務フローを構築し、個人の判断や業務命令だけでは完結させないようにする。また、メールだけに依存しない業務フローの構築も重要です。

例えば、振込先口座に変更がある場合は、メール以外の連絡方法（電話等）で直接取引先に確認をする、金融機関にその口座の名義等を確認するなどが上げられます。

◆普段とは異なるメールに注意する

普段とは異なる言い回しや、表現の誤り、送信元のメールドメインに注意しましょう。

◆判断を急がせるメールに注意する

至急の対応を要求する等、担当者に真偽の判断時間を与えないようにする手口も考えられます。真偽を確認するフローを業務フローに盛り込んでおく事も有効です。

◆インシデント対応体制の整備

問題発生時に迅速かつ的確に対応できる体制を整えます。

具体的な対応については、IPA の「中小企業の情報セキュリティ対策ガイドライン 第 3.1 版」の 46 ページからの（5）セキュリティインシデント対応をご覧ください。

（２）被害を受けた後の対応

ビジネスメール詐欺による金銭被害（可能性を含む）を受けた時には、下記の対応が必要となります。

◆適切な報告／連絡／相談

問題が発生した場合、速やかに報告し、適切な対応を取れるよう、社内・社外の関係組織や公的機関等と連携できるようにしておきましょう。

◆メールアカウントの設定を確認する

攻撃者による不正な転送設定やメール振分けの設定等がされていないか確認する。

◆パスワードを適切に運用する

速やかにパスワードを変更する。推測されにくく、他のシステムやサービスとは異なるパスワードを設定しましょう。

今回は、ビジネスメール詐欺による金銭被害の事例や影響、対策方法について考えてきましたが、いかがだったでしょうか。

ビジネスメール詐欺による被害はどの企業でも起こる可能性があり、その影響は甚大です。被害を完全になくすことはできませんが、ガバナンスの整備やメールだけに頼ることがない業務フローの構築等が、企業の持続可能な発展を支える鍵となるでしょう。

＜参考情報＞　他の事例を見る

・ビジネスメール詐欺の事例集を見る（IPA Web サイト）
・5 億円の被害も！日本企業の不正送金・ビジネスメール詐欺被害の事例 4 社（サイバーソリューションズ株式会社 Web サイト）

レベル 2_#6_中小企業におけるセキュリティ脅威への対策強化　～テレワーク時代の新しい働き方に潜むリスクと対策を学ぶ～

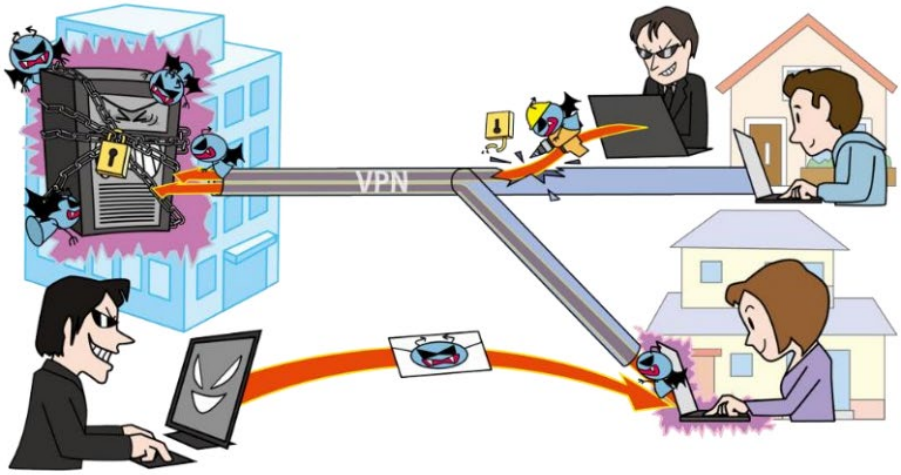
掲載日：2024/9/4



独立行政法人情報処理推進機構（IPA）が毎年発行している「情報セキュリティ 10 大脅威 2024」から、中小企業の経営者やシステム担当者が注目すべき点を掘り下げていきます。

今回は 9 位に挙げられている「**テレワーク等のニューノーマルな働き方を狙った攻撃**」を深掘りします。これは特にコロナ禍でテレワークのニーズが高まってきた 2020 年頃から発生し続けており、この脅威がどのように業務に影響を与えるのか、対策はどうすべきなのかを解説いたします。

～狙われ続けるテレワーク環境、セキュリティ対策を～



引用元：IPA 情報セキュリティ 10 大脅威 2024 解説書より

１．ニューノーマルな働き方とセキュリティ脅威の増加

COVID-19（新型コロナウイルス感染症）の影響により、2020 年頃から急速に普及したテレワーク。この新しい働き方は、組織の業務継続性を確保するために、自宅等から VPN 経由で社内システムにアクセスしたり、Web 会議サービスを利用した商談などのコミュニケーションを定着させてきました。それに伴い、個人宅のネットワークの利用や個人所有の PC やスマートフォン（BYOD：Bring Your Own Device）を利用せざるを得ない状況が頻発し、新たなセキュリティリスクを生む結果となりました。

２．主な攻撃例

以下に代表的なテレワーク等のニューノーマルな働き方を狙った攻撃例を紹介します。

（１）脆弱性を悪用した攻撃

VPN や Web 会議サービス等のテレワーク用に導入している製品の脆弱性や設定ミスが悪用されているケースが増えています。社内システムへの不正アクセスや、PC 内の業務情報や機密情報の窃取、Web 会議ののぞき見等が発生する恐れがあります。

（２）脆弱なテレワーク環境への攻撃

急いでテレワークを導入したため、規則の整備やセキュリティ対策が不十分のまま運用されている環境が多く存在します。その結果、攻撃者はこれらの脆弱なテレワーク環境を狙って、攻撃を行います。例えば、接続用機器の外部からのアクセス権限を必要以上に拡張してしまったり、古い接続機器を再利用したことで、最新のバージョンアップの適応ができず、脆弱性対応がなされないままになっている環境を攻撃されるわけです。

（３）個人所有端末や自宅のネットワークを利用した攻撃

適切なセキュリティ対策が施されていない個人所有端末や、会社支給の端末を利用している場合でも自宅のネットワークを利用することにより、ウイルス感染やデータ漏えいのリスクが高まります。

では、テレワーク環境の脆弱性を狙った具体的な事例をご紹介しながら、要因と対策をみていきましょう。

３．テレワーク環境を狙った具体的な攻撃事例

事例：在宅勤務のために用意したリモートアクセス経路より侵入の疑い
セイコーグループでは、ランサムウェアによる被害で顧客や取引先担当者等の個人情報が流出したことを公表した。同社ではコロナ禍において在宅勤務のために用意したリモートアクセス経路より侵入されたものと見ている。データセンターや国内拠点の一部サーバー内部に保存されていたデータを暗号化され、同社含むセイコーウオッチおよびセイコーインスツルが保有する約 60,000 件の個人情報が外部に流出した。
引用元：IPA　情報セキュリティ 10 大脅威　2024　解説書より抜粋
参考記事：重要なお知らせ詳細 ｜ 重要なお知らせ ｜ セイコーグループ (seiko.co.jp)

この事例は、テレワーク機器の脆弱性を狙ったランサムウェア攻撃になります。通常の侵入と情報漏えいだけではなく、暗号化による業務停止なども並行して発生しているのが特徴です。ランサムウェア自体は、暗号化や取得するデータが直接アクセスできる環境での実行が必須であり、通常はビジネスメールに見せかけた添付ファイル実行などが発生原因として多いです。しかし、今回の事例の様に、脆弱性を突かれ内部に侵入したうえでランサムウェアを発動させる場合も見受けられます。このように、テレワーク機器や個人所有の回線・PC 等の脆弱性が更なるセキュリティリスクになる事がお判りいただけるかと思います。

４．ニューノーマルな働き方を狙った攻撃への対策

では次にテレワーク等のニューノーマルな働き方を狙った攻撃への対策として、「個人の観点」と「企業の観点」を説明していきます。

（１）個人（テレワーカー）での対応と対処

◇被害の予防（被害に備えた対策含む）

・IPA の「情報セキュリティ 10 大脅威 2024 解説書」の 10 ページ、表 1.4「情報セキュリティ対策の基本」を実施します。

・組織のテレワークの規則を遵守します（使用する端末、ネットワーク環境、作業場）

◇被害を受けた後の対応

・組織（経営者層）へ適切な報告や連絡や相談を行います。

（２）企業（経営者層）の対応と対処

◇組織としての体制の確立

・インシデント対応体制を整備し対応する

テレワーク環境でのインシデントの発生（ウイルス感染により PC が使用できない等）を考慮して、テレワーク環境下での連絡方法や対応手順を策定し、社員に周知しておく必要があります。具体的な対応については、IPA の「中小企業の情報セキュリティ対策ガイドライン 第 3.1 版」の 46 ページからの（5）セキュリティインシデント対応をご覧ください。

・テレワークのセキュリティポリシーを策定する

（３）企業（セキュリティ担当者、システム管理者）の対応と対処

◇被害の予防（被害に備えた対策含む）

・シンクライアント、VDI、VPN、ZTNA/SDP 等のセキュリティに強いテレワーク環境を採用する。

※シンクライアント(Thin Client)

クライアント(PC、iPad、スマホ等)には最小限の入出力装置だけを用意して、主な処理はサーバー側で行う仕組み。アプリケーションやデータは、クライアント端末に保存されないため、高いセキュリティが実現できるのが特徴。

※VDI（Virtual Desktop Infrastructure）

PC 上のデスクトップ機能をサーバー上に集約し、手元の PC にデスクトップ画面を転送して機能を利用すること。

※ZTNA(Zero-Trust Network Access)

ネットワークの内側・外側の両方に脅威が存在することを前提とし、すべてのユーザとすべてのデバイスに対して厳格な検証を行う IT セキュリティモデル。

※SDP（Software Defined Perimeter）

ゼロトラストセキュリティでの新たな「境界（Perimeter）」の考え方で、集中的なアクセス制御を「ソフトウェア」で実現することで、物理的な境界(ファイアウォール等)では防ぎきれない脅威の防御を可能にする仕組み。

・テレワークの規程や運用規則の整備

組織支給端末と私有端末の違いを考慮して、テレワーク開始時の暫定的なセキュリティ対策や例外措置を早期に見直します。

・情報リテラシー、モラルを向上させ、情報セキュリティに関する重要性を認識させます。

・ネットワークレベル認証（NLA）を行います。

・多要素認証の設定を有効にします。

◇被害の早期検知

・サーバーやクライアント、ネットワークに適切なセキュリティ対策を行い、インシデントを素早くキャッチできるようにします。

◇被害を受けた後の対応

・インシデント対応体制を整備し対応します。

ここまでテレワークによる被害の事例や影響、対策方法について考えてきましたが、いかがだったでしょうか。IPA では「テレワークを行う際のセキュリティ上の注意事項」のページを公開しています。このページでは、テレワークを行う際のセキュリティ上の注意事項に加え、テレワークから職場に戻る際のセキュリティ上の注意事項も解説しています。また、IPA や他機関のテレワーク関連セキュリティ情報へのリンクも紹介しているので、参考にしていただきたいと思います。

テレワーク等のニューノーマルな働き方は、まだ運用実績が浅いため、その利便性と引き換えにセキュリティトラブルを含め事故が起こりやすいのも確かです。ただし、個人(テレワーカー)や企業組織が的確なセキュリティ対策を行えば、企業の持続可能な発展を支える鍵となると言えます。

５．事例

事例を見る

・テレワーク環境でマルウェア感染、社内に拡大 - 三菱重工（Security NEXT）
・テレワークに伴う個人情報漏えい事案に関する注意事項（個人情報保護委員会）

レベル 2_#7_中小企業におけるセキュリティ脅威への対策強化　～ランサムウェアによる攻撃事例から対策を学ぶ～（1/2）
掲載日：2024/9/18



独立行政法人情報処理推進機構（IPA）が毎年発行している「情報セキュリティ 10 大脅威 2024」から、中小企業の経営者やシステム担当者が注目すべき点を掘り下げていきます。

今回は 1 位に挙げられている「ランサムウェアによる攻撃」に焦点を当てます。
2016 年以降 9 年間にわたり 10 大脅威の 1 位を取り続けていることから、最も被害の多い脅威と言えます。

この脅威が業務に与える影響や、どのように対策すべきなのかを 2 回に分けて解説いたします。1 回目の今回は、ランサムウェアの種類と攻撃の特徴について解説いたします。

～組織の規模や業種は関係なし！次の標的はあなたの組織かも？～



引用元：IPA　情報セキュリティ 10 大脅威　2024　解説書より

１．ランサムウェアとは

ランサムウェア(Ransomware)とは、Ransom(身代金)と Software(ソフトウェア)を組み合わせた造語であり、マルウェア※の一種です。
攻撃者は PC やサーバーをランサムウェアに感染させることで組織の重要なデータを人質に取り、その復旧やシステムの解除を引き換えに金銭、すなわち「身代金」を要求します。
さらに、攻撃者は複数の脅迫を組み合わせることで、攻撃を受けた組織が金銭を支払うことを検討せざるを得ない状況を作り出そうとします。

ランサムウェア攻撃は、組織の規模や業種に関わらず、あらゆる対象に及びます。
ランサムウェアに感染すると、データの暗号化や重要情報の奪取といった被害に遭遇するだけでなく、その調査や復旧に多くの費用と時間が掛かります。
また、業務やサービス提供の停止による経済的損失や、顧客や取引先からの信頼失墜の被害につながるおそれもあります。広く利用されているサービスがランサムウェアに感染すると、社会にも大きな影響を与えることになります。

※マルウェア(malware)とは
malicious（マリシャス：悪意のある）に software（ソフトウェア）の 2 つの単語が組み合わさった造語です。コンピューターウイルスやワーム、トロイの木馬、スパイウェア、など、ユーザーのデバイス(PC、iPad、スマホ等)に不利益をもたらす悪意のあるプログラムやソフトウェアを総称する言葉です。

２．ランサムウェアの代表的な種類

（１）ばらまき型ランサムウェア攻撃

日本では 2015 年頃からランサムウェアの被害が発生しだしました。
当初のランサムウェアはウイルスを添付したメールを、不特定多数の組織に対して無差別に送信する「ばらまき型」でした。
受信したユーザーが添付ファイルを実行することで感染させ、システムのロックや、ファイルを暗号化して使用不能にしたのちに、元に戻すことと引き換えに「身代金」を要求するメッセージ（ランサムノート）を表示させる手法です。

（２）標的型ランサムウェア攻撃

2019 年後半から、海外では「Human-Operated」、日本では「標的型ランサムウェア攻撃」、「侵入型ランサムウェア攻撃」と呼ばれる、特定の組織を狙って攻撃する手法が主流となってきました。
攻撃者が事前に標的組織のネットワークに侵入し、組織の機密情報を窃取して、最終的にランサムウェアを実行し金銭を要求する手法です。

（３）二重脅迫型

標的型ランサムウェア攻撃に「情報の暴露」を加えた二重脅迫の手法です。
データの暗号化に加え、「身代金を支払わなければ、窃取した情報を暴露する」といった二重の脅迫により対象組織を追い詰め、より多額の身代金を払わせようとします。このような脅迫の手法は、「暴露型」または「二重脅迫型」と呼ばれます。

（４）多重脅迫型

被害組織の Web サーバーなどに大量のパケットなどを送りつけて正常なサービス提供ができないよう妨害する DDoS※攻撃の実施や、取引先などの関連組織に情報漏えいを通知するなどの脅迫を行う「多重脅迫」の手法も確認されています。この手法では、対象組織やその周辺に多角的な圧力を加えることで、身代金の要求を迫ります。

※DDoS（ディードス）攻撃とは

Distributed Denial of Service（分散型サービス拒否）攻撃の略称です。Web サーバーなどに対して、複数の場所から大量の通信を発生させることで正常なサービス提供を妨げる攻撃です。

３．標的型ランサムウェアの攻撃

標的型ランサムウェアの攻撃方法は多岐に渡り、以下のようなステップを経ることが一般的です。

（１）侵入

攻撃者はまず、様々な方法を駆使して標的とする組織のネットワーク内部への侵入を図ります。
主な侵入経路には、下記のような感染ルートがあります。

◇脆弱性を悪用しネットワークから感染させる
OS やアプリケーション等のソフトウェアの脆弱性対策が十分でない状態でインターネットに接続されている機器に対して、VPN 等の脆弱性を悪用し、インターネット経由で PC やサーバーをランサムウェアに感染させる。

◇公開サーバーに不正アクセスして感染させる
意図せず外部公開されているポート（リモートデスクトップポート等）に不正アクセスしたり、パスワード管理の不備を利用したりしてランサムウェアに感染させる。

◇メールから感染させる
組織の従業員等へのメールに添付したファイルや、本文中のリンクを開かせることでランサムウェアに感染させる。

◇Web サイトから感染させる
Web サイトの脆弱性等を悪用して、ランサムウェアをダウンロードさせるように改ざんした Web サイトや攻撃者が用意した Web サイトを閲覧させることでランサムウェアに感染させる。

（２）ネットワーク内部で情報収集する

侵入に成功した攻撃者は、続けてネットワーク内の端末を遠隔操作し、多数のアクセス権限の取得を試みます。これは、次のステップとなるデータの窃取やランサムウェア実行の際により大きな効果を得るための準備です。

（３）データの窃取

搾取した組織内の端末やシステムのアクセス権限を利用して、脅迫を行うための情報を収集します。それらの情報は、のちに情報暴露で組織を脅す材料として使われることもあります。奪われた情報は一か所に集められ、攻撃者の管理するサーバーに保管されます。

（４）ランサムウェアの実行・身代金要求

最後に、組織へのランサムウェアの展開と実行を行います。
その際、グループポリシー機能などを使ってランサムウェアを組織内ネットワークに展開し、実行します。ファイルを暗号化した後は、権限を奪取した端末に身代金要求画面を表示させることで脅迫を行います。

ここまでランサムウェアの種類や攻撃方法について考察してきましたが、いかがだったでしょうか。次回は、被害の実例と対策・対応について解説する予定です。

IPA では「ランサムウェア対策特設ページ」を公開しています。
このページでは、ランサムウェアの感染防止や被害低減のために役立つ情報が公開されています。
また、IPA や他機関のランサムウェア関連セキュリティ情報へのリンクも紹介しているので、ぜひ参考にしてください。

ランサムウェアは今も進化をし続けています。適切なセキュリティ情報の入手と、組織全体が正しいランサムウェアの知識を共有する事が発生防止には不可欠といえるでしょう。

４． 最後に

東京都では、セキュリティ機器の無償体験（３か月程度）や、企業のセキュリティ環境を調査し、今後の対策に向けて指導・助言する情報セキュリティマネジメント指導支援を行っています。それぞれ定員がございますので、詳しくはこちらをご覧の上、お早めにお申し込みください。
https://kihontaisaku.metro.tokyo.lg.jp/

レベル 2_#8_中小企業におけるセキュリティ脅威への対策強化　～ランサムウェアによる攻撃事例から対策を学ぶ～（2/2）

掲載日：2024/10/2



独立行政法人情報処理推進機構（IPA）が毎年発行している「情報セキュリティ 10 大脅威 2024」から、中小企業の経営者やシステム担当者が注目すべき点を掘り下げていきます。

今回も 1 位に挙げられている「ランサムウェアによる攻撃」に焦点を当てます。

２回目の今回は、ランサムウェアの被害の実例と対策・対応について解説いたします。

※前回の情報はこちら:中小企業におけるセキュリティ脅威への対策強化～ランサムウェアによる攻撃事例から対策を学ぶ～（1/2）

～組織の規模や業種は関係なし！次の標的はあなたの組織かも？～



引用元：IPA　情報セキュリティ 10 大脅威　2024　解説書より

１．ランサムウェアによる被害の実例

（１）名古屋港のコンテナ搬出・搬入業務が停止

2023 年 7 月、名古屋港統一ターミナルシステムがランサムウェアによる攻撃を受け、数日間コンテナの搬出入業務が停止するという被害が発生しました。
発表によれば、障害発生時の朝システムが停止したことを把握。その後、システム専用のプリンターからランサムウェアの脅迫文書が印刷され、サーバー再起動で復旧できないことを確認して、愛知県警察本部サイバー攻撃対策隊に通報。その後の調査で、物理サーバー基盤と全仮想サーバーが暗号化されていることが判明しました。
リモート接続機器の脆弱性を悪用した不正アクセスが原因でランサムウェアに感染したと考えられ、約 2 日半ターミナルでの作業の停止を余儀なくされました。

（２）社労士向けサービスが提供停止

2023 年 6 月、システム開発およびクラウドサービス事業者である株式会社エムケイシステムが、データセンターサーバーに不正アクセスされ、ランサムウェアに感染したことを公表しました。
この感染により、業務データが暗号化され、社会保険労務士向けクラウドサービス「社労夢」のサービスを提供できなくなり、影響のある約 3,400 人のユーザーに対し、オンプレミスで動作するパッケージ版を代替として提供する事になりました。

その上、インフラ設備の再構築費用やセキュリティ対策費用のコスト増、影響があったユーザーへの 6 月の請求を停止するといった対応により、業績予想を大幅に修正することになりました。

（３）VPN 経由で侵入、ランサムウェアを横展開

2023 年 1 月、市民生活協同組合ならコープが 2022 年 10 月にランサムウェアによる攻撃を受けていたことを公表しました。
攻撃者はネットワーク機器の脆弱性を悪用して VPN 経由で侵入し、内部情報を収集。その上、ランサムウェアをサーバー11 台に横展開し、ほとんどのデータが暗号化されていました。
レポートによれば、暗号化されたデータには約 49 万人の個人情報が含まれるものの、外部への流出は確認されていないとの事でした。また、データは復元できなかったものの、バックアップを取っていたデータベースは感染を逃れていたため、容易に復元することができました。

２．ランサムウェアの対策と対応

ランサムウェアの対策と対応には、組織的な対応（経営者層/システム管理者/従業員）が必要です。
それぞれの組織が役割を分担し合い、かつ総括的に対策や対応をシームレスに行う必要があります。
※印は下記「共通対策」の詳細を参照してください。

（１）経営者層

経営者層では以下の対策と対応が必要となります。
◇組織としての対策・対応体制の確立
・インシデント対応体制を整備し、実際のインシデント時に対応する※

（２）システム管理者や従業員

◇被害の予防対策
・インシデント対応体制を整備し、実際のインシデント時に対応する※
・IPA の「情報セキュリティ 10 大脅威 2024 解説書」の 10 ページ、表 1.4「情報セキュリティ対策の基本」を実施する

表 1.4 情報セキュリティ対策の基本

攻撃の糸口	情報セキュリティ対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消し攻撃によるリスクを低減する
ウイルス感染	セキュリティソフトの利用	攻撃をブロックする
パスワード窃取	パスワードの管理・認証の強化 ※「共通対策」で詳細を解説	パスワード窃取によるリスクを低減する
設定不備	設定の見直し	誤った設定を攻撃に利用されないようにする
誘導（罠にはめる）	脅威・手口を知る	手口から重要視すべき対策を理解する

・メールの添付ファイル開封や、メールや SMS のリンク、URL のクリックを安易にしない※
・多要素認証の設定を有効にする
・提供元が不明なソフトウェアを実行しない
・サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う※
・共有サーバー等へのアクセス権の最小化と管理の強化を行う
・公開サーバーへの不正アクセス対策を行う
・適切なバックアップ運用※

◇被害を受けた後の対応
・適切な報告／連絡／相談を行う※
・適切なバックアップ運用を行う※
・復号ツールを活用し、復号化を行う
・インシデント対応体制を整備し、実際のインシデント時に対応する※

（３）身代金の支払いと復旧業者の選定

ランサムウェア被害を受けた場合、原則、身代金は支払わずに復旧を行います。
何故ならば、身代金を支払ってもデータの復元や情報の流出を防げるとは限らないからです。
また、対応を依頼した業者が攻撃者との裏取引で身代金を支払うことでデータ復旧した場合、事実上、自組織が攻撃者に資金提供をしたとみなされるおそれもあります。このため、対応を依頼する業者の選定にも注意が必要です。

※「共通対策」

IPA の「情報セキュリティ 10 大脅威 2024 解説書」の 69 ページ、表 1.6「複数の脅威に有効な対策集」より

対策	対象	
	個人	組織
パスワードを適切に運用する	○	○
情報リテラシー、モラルを向上させる	○	○
メールの添付ファイル開封や、メールや SMS のリンク、URL のクリックを安易にしない	○	○
適切な報告／連絡／相談を行う	○	○
インシデント対応体制を整備し対応する		○
サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う		○
適切なバックアップ運用を行う	○	○

（１）パスワードの適切な運用

推測可能なパスワードの設定や不適切な管理をすると、攻撃者に不正ログインされやすくなってしまいます。そのためは適切な設定や運用が必要となります。

（２）情報リテラシー、モラルを向上

故意に不正をはたらくことは論外ですが、中には意図せず情報モラルに反することを行ったり、組織のためによかれと考えて規則に反してしまう場合もあります。

どのような場合にも自身の行為には責任が伴う事を認識する必要があります。

（３）メールの添付ファイル開封、メールや SMS のリンクや URL の安易なクリックの抑止

様々なサービスからの連絡がメールで行われたり、SMS からのお知らせを受け取ることがあります。しかし、本物を騙った偽の連絡であると、それに起因として個人情報を盗まれたり、金銭被害に繋がったりするおそれがあります。

（４）適切な報告／連絡／相談

◇【システム管理者や従業員】

被害を受けたときは適切な人や機関への相談が必要です。不安に感じたときや被害に遭ったときは慌て

ず、まずは落ち着いて、対応する事が望ましいと言えます。
◇**【組織】**
組織内で適切な報告や連絡が無いと被害の拡大だけでなく、外部からは隠蔽とみなされ、さらなる信頼の失墜につながります。経営者や上司、責任者は部下や担当者が包み隠さず躊躇なくエスカレーションできる風土や関係性を築くことも重要です。

（５）インシデント対応体制を整備し対応する
セキュリティインシデントが発生した際、誰がどのように、何から行えばよいのか？これを理解して、あらかじめ対応する仕組みを整えているのといないのとでは、同じ事象の問題が起きたとしても受ける被害の大きさは全く異なります。適切な体制構築が必要です。

（６）サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う
脅威はサーバーやクライアント、ネットワークに関連したものが多いのが特徴です。ただし、組織としてのポリシーの制定や要員確保、事前検証、手順の確立、そしてそれを維持し続ける予算の確保と仕組みが必要であり、検討事項が多い事も特徴と言えます。

（７）適切なバックアップ運用
データの破損の原因は、記憶装置の故障やランサムウェア等のサイバー攻撃だけではなく、運用時の操作ミスによる消去や誤った更新と、多岐に渡ります。データ復旧には人手と時間を要しますが、適切なバックアップを取得しておくことで、この被害を軽減することが可能です。

IPA の「情報セキュリティ１０大脅威 2024」の 68 ページの「共通対策」ではさらに詳しい具体的な対応をご紹介しています。こちらもご参照ください。

ここまでランサムウェアの攻撃事例や対策・対処について考察してきましたが、いかがだったでしょうか。

前回の繰り返しですが、IPA では「ランサムウェア対策特設ページ」を公開しています。
このページでは、ランサムウェアの感染防止や被害低減のために役立つ情報が公開されています。
また、IPA や他機関のランサムウェア関連セキュリティ情報へのリンクも紹介しているので、ぜひ参考にしてください。

ランサムウェアは今も進化をし続けています。
正しいランサムウェアの知識を共有し、事前にできる対策をできるだけ打つことによって、ランサムウェアの発生を防止する事が可能となり、組織として重要な情報や業務継続性を保証することができます。

３．最後に

東京都ではセキュリティ対策をこれから始めたい企業や事業継続に向けたさらなる強化を図りたい企業向けに、セキュリティ専門家による各種の支援を行っています。すでに募集を締め切っている支援もありますが、ご参考までにご覧ください。

基本対策事業 URL：https://kihontaisaku.metro.tokyo.lg.jp/ 【参加企業募集中です！】
特別支援事業 URL：https://tokubetsushien.metro.tokyo.lg.jp/ ※今年度は募集を終了しました

レベル 2_#9_中小企業におけるセキュリティ脅威への対策強化　～サプライチェーンの弱点を悪用した攻撃から対策を学ぶ～
掲載日：2024/10/16



独立行政法人 情報処理推進機構（IPA）が毎年発行している「情報セキュリティ10大脅威2024」から、中小企業の経営者やシステム担当者が注目すべき点を掘り下げていきます。

今回は２位に挙げられている「**サプライチェーンの弱点を悪用した攻撃**」を事例とともに深掘りします。

１．サプライチェーンとは

サプライチェーンとは、商品の企画、開発、調達、製造、在庫管理、物流など、製造から販売までの一連のプロセス及び、その商品やサービスが最終消費者に届くまでに関わる全ての組織や活動のネットワークを指します。
サプライヤー、製造業社、流通業者などがこれにあたります。

また、ソフトウェア開発のライフサイクル*に関与する全てのモノ（ライブラリ、各種ツール等）や人の繋がり

を、ソフトウェアサプライチェーンと呼びます。

*ソフトウェア開発のライフサイクル：ソフトウェアが企画・仕様、設計から実装、テスト、運用、及びメンテナンス・監視までたどる、一連のライフサイクルのこと

このような「ビジネス上の繋がり」や「ソフトウェアの繋がり」を悪用した攻撃をサプライチェーン攻撃と呼びます。この脅威が業務にもたらす影響や、取るべき対策について解説いたします。



引用元：IPA　情報セキュリティ 10 大脅威　2024　解説書より

２．狙われるサプライチェーンの弱点

標的とする組織が強固なセキュリティ対策を行っていて直接攻撃が困難な場合、攻撃者は、そのサプライチェーンの脆弱な部分を探し出して攻撃を行います。
大手企業と繋がりのある中小企業の中には、セキュリティへの対策が十分でない企業も多くあります。攻撃者はその脆弱な企業を足掛かりとして間接的、及び段階的に標的とする組織を狙います。
攻撃者の侵入を許してしまった場合、機密情報の漏えいや信用の失墜等、様々な被害が発生します。

また、自組織のセキュリティ対策が十分ではなく、攻撃を受けた上で足掛かりとされると、サプライチェーン上の取引相手に損害を与えてしまい、取引相手を失ったり、損害賠償を求められたりするおそれが想定されます。

３．主な攻撃手口

サプライチェーンを狙った攻撃はさまざまな手口で行われます。以下に代表的なサプライチェーンの弱点を悪用した攻撃例を紹介いたします。

（１）取引先や委託先が保有する機密情報を狙った攻撃

標的とする組織よりもセキュリティが脆弱な取引先や委託先、国内外の子会社等を攻撃し、その攻撃を受けた組織が保有する標的組織の機密情報等を窃取する手法です。
標的とする組織では機密情報扱いであり、堅牢なセキュリティのもと管理されているとしても、セキュリティが脆弱なサプライチェーン上の組織でも同じように厳密に管理されているとは限らず、そこが狙われてしまうのです。

（２）ソフトウェアサプライチェーン攻撃

標的組織と取引のある、または調達するであろうソフトウェアやサービスを改ざんして、ソフトウェアそのものやアップデートプログラムなどに不正コードを混入させ、標的組織に侵入するための足掛かりとする攻撃手法です。
標的組織がそのソフトウェアを導入したり、更新する際にウイルス感染を引き起こすのです。

（３）サービスサプライチェーン攻撃

はじめに企業システムの運用、監視等を請け負う事業者（MSP：マネージドサービスプロバイダー）等を攻撃し、足掛かりとする攻撃手法。
MSP が利用する資産管理ソフトウェア等にウイルスを仕込み、MSP の複数顧客にウイルスを感染させる手口もあります。

４．サプライチェーンの弱点を悪用した具体的な攻撃事例

【事例１：業務委託先業者からの顧客情報漏えい】

2023 年 1 月、複数の保険会社が、業務委託先から顧客の個人情報が流出したことを公表しました。

業務委託先の適切なセキュリティ対策がされていないサーバーへ不正アクセスされた事が原因でした。
また流出した個人情報が海外の Web サイトに掲載されていたことで、被害が発覚しました。
流出の規模は保険会社により異なるが、多いところでは約 130 万人分にも及び、調査や対処に追われました。
引用元：IPA 情報セキュリティ 10 大脅威 2024 解説書より抜粋

この事例は、「２． 主な攻撃手口」の「（１）取引先や委託先が保有する機密情報を狙った攻撃」の具体的な内容になります。
保険会社が必要とするセキュリティ要件が委託業者側で徹底されていなかった点を攻撃者に狙われた訳ですが、保険会社側もセキュリティ要件が徹底されているかを管理する責任があり、これが十分ではなかったことも併せて原因と言えます。

【事例２：提携先企業に不正アクセス、顧客情報漏えい】

2023 年 11 月、メッシュ Wi-Fi を提供する JCOM が顧客情報の漏えいを公表しました。
当該サービスは米国 Plume Design 社が提供元であり、同社の提携先のモバイルアプリのアクセスログサーバーが不正アクセスされたことが原因でした。
これにより約 23 万件の顧客の氏名と約 5 千件のメールアドレスが漏えいしました。
引用元：IPA 情報セキュリティ 10 大脅威 2024 解説書より抜粋

この事例は、「２． 主な攻撃手口」の「（３）サービスサプライチェーン攻撃」の具体例です。
アクセスログ自体はサービス提供側が管理している情報なので、利用者側である JCOM では対処が難しい事例です。
自社が提供するサービスで利用する、サービス事業者(MSP)のセキュリティ対策が十分か否かを見極める必要があると言えます。

５． サプライチェーンの弱点を悪用した攻撃への対策

サプライチェーンの弱点を悪用した攻撃への対策は組織で実施する必要があります。
以下に「経営層の観点」「自組織の観点」「関わる組織の観点」で説明していきます。

（１）経営層の対応と対処

◇被害の予防

・インシデント対応体制を整備し対応する※

（２）自組織の対応と対処

◇被害の予防

・情報管理規則の徹底

調達先や業務委託先等、契約時に取引先の規則を確認します。

・セキュリティ評価サービス（SRS） ＊１を用いた自組織のセキュリティ対策状況の把握

＊１セキュリティ評価サービス（Security Rating Services）：攻撃者と同様の手法を用いた擬似的な攻撃を行うことにより潜在的な脆弱性を評価し改善するための助言を行うサービス

・信頼できる委託先、取引先、サービスの選定

商流に関わる組織、サービスの信頼性評価 *2（ISMAP *3 など）、品質基準を検討し、複数候補を検討します。

*2 サービスの信頼性評価：システムやソフトウェアが一定の条件下で正常に稼働し、安定的にサービスを提供しつづけることができるかどうかを測るための指標

*3 ISMAP：政府が活用しているクラウドサービスのセキュリティレベルを評価する制度

・契約内容の確認

組織間の取引や委託契約における情報セキュリティ上の責任範囲を明確化し、合意を得ます。また、賠償に関する契約条項を盛り込みます。

・委託先組織の管理

委託元組織が委託先組織のセキュリティ対策状況と情報資産の管理の実態を定期的に確認できる契約とすることが重要です。また、業務委託自体が適切であるかも検討します。

・納品物の検証

納品物に組み込まれているソフトウェアの把握と脆弱性対策を実施します。ソフトウェアの把握や管理においてはソフトウェア部品表（SBOM） *4 の導入を検討します。

*4 ソフトウェア部品表（Software Bill Of Materials）：ソフトウェアアプリケーションを構築するためのライブラリ、コードパッケージ、サードパーティ製コンポーネントなどのライセンス情報・バージョン・修正適用状況・依存関係等をすべて記載したもの。

◇被害を受けた後の対応

・インシデント対応体制を整備し対応する※

・被害への補償組織としての体制の確立

（３）関わる組織の対応と対処

自組織に関わる組織の対応は共に実施する必要があります。

◇被害の予防
・取引先や委託先との連絡プロセスの確立
・取引先や委託先の情報セキュリティ対応の確認、監査
・情報セキュリティの認証取得 ISMS、プライバシーマーク、SOC2 等を取得し、定期的に見直して必要な運用を維持する。
・公的機関等が公開している資料の活用

◇被害を受けた後の対応
・適切な報告／連絡／相談を行う※

「※」の詳細については、IPA の「情報セキュリティ１０大脅威 2024」の 68 ページからの「共通対策」をご参照ください。
また、前回の「中小企業におけるセキュリティ脅威への対策強化～ランサムウェアによる攻撃事例から対策を学ぶ～（2/2） 」でも、詳細を解説していますので、併せてご参照ください。

ここまでサプライチェーンの弱点を悪用した攻撃の事例や影響、対策方法について考えてきましたが、いかがだったでしょうか。
今回取り上げた事例や対策から分かるように、サプライチェーンを狙った攻撃の影響は自組織の外部へも及びます。
サプライチェーンは企業活動と切り離すことは困難です。
セキュリティへの取り組みは各企業を超えてサプライチェーン全体で実施することで、企業活動を支える基盤を強化することが可能です。
そのため、サプライチェーン全体で的確なセキュリティ対策を行うことは、企業の持続可能な発展を支える鍵となるとも言えます。

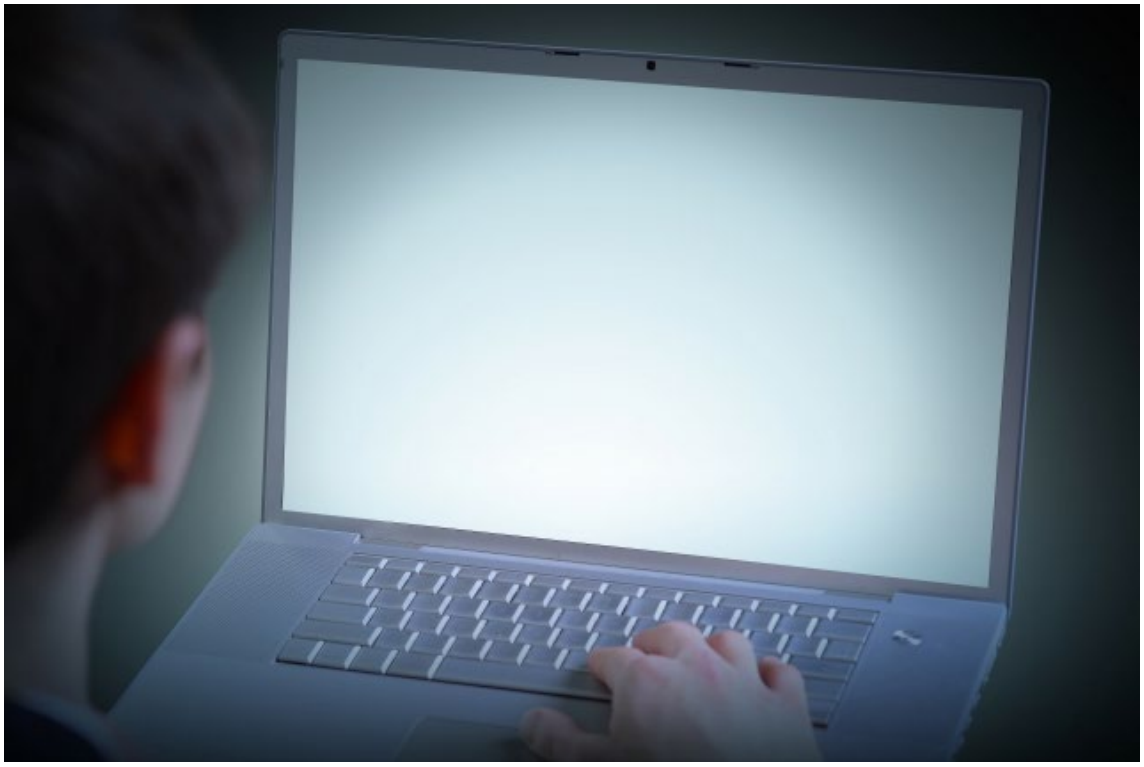
６．事例

事例を見る

・個人情報流出に関するお詫びとお知らせ（アフラック生命保険株式会社）

・個人情報漏えいに関するお詫びとご報告（チューリッヒ保険会社）
・不正アクセスによる、情報漏えいに関するお知らせとお詫び（LINE ヤフー株式会社）
・お客さまの個人情報漏えいに関するお知らせとお詫び（JCOM 株式会社）

レベル 2_#10_中小企業におけるセキュリティ脅威への対策強化　～内部不正による情報漏えい等の被害から対策を学ぶ～
掲載日：2024/10/30



独立行政法人 情報処理推進機構（IPA）が毎年発行している「情報セキュリティ10大脅威2024」から、中小企業の経営者やシステム担当者が注目すべき点を掘り下げていきます。

今回は３位に挙げられている「**内部不正による情報漏えい等の被害**」を深掘りします。
従業員や元従業員等の組織関係者による機密情報の持ち出しや、社内情報の削除等の不正行為が発生しています。
また、組織内の情報管理の規則を守らずに情報を持ち出し、紛失や情報漏えいにつながるケースもあります。

組織関係者による不正行為は、組織の社会的信用の失墜や、損害賠償や業務停滞等による経済的損失を招きます。
また、不正に取得された情報を使用した組織や個人も責任を問われる場合があります。この脅威がどのように業務に影響を与えるのか、対策はどうすべきなのかを解説します。



引用元：IPA　情報セキュリティ 10 大脅威　2024　解説書より

１．内部不正による情報漏えい等の被害による脅威

悪意を持った組織関係者が、金銭受領、転職先での悪用、組織への私怨等を動機として、組織が保有する技術情報や顧客情報等の重要情報の持ち出しや第三者への提供、不特定多数が閲覧できる場所への公開、情報の削除や改ざん等の不正行為を行うことがあります。
また、自宅等の社外で作業するために組織の情報管理の規則を守らず情報を外部へ持ち出し、情報漏えいするケースもあります。

不正に取り扱われた情報の重要性や被害規模によっては、組織の社会的信用の失墜や、顧客等への損害賠償、損失補填、復旧作業等による経済的損失が発生し、組織の競争力の大幅な低下につながります。
その結果、組織経営の根幹を揺るがすおそれがあります。

また、自組織に持ち込まれた情報が不正に取得されたものであることを知りつつ使用した場合、刑事罰の対象になることもあります。

２．主な攻撃手口

以下に代表的な内部不正による情報漏えい手口を紹介します。

（１）アクセス権限の悪用

付与された権限を悪用し、組織の重要情報を窃取したり不正に操作を行うケースです。
必要以上に高いアクセス権限が付与されている場合、より重要度の高い情報が狙われ、被害が大きくなるおそれがあります。
また、複数人で端末を共用している場合、他人のアカウントで不正アクセスされるリスクも生じます。

（２）在職中に割り当てられたアカウントの悪用（離職後のアカウント利用）

離職者が在職中に使用していたアカウントが削除されていない場合、それを使用して組織の情報に不正にアクセスを続ける事が出来てしまいます。
これにより重要情報を容易に持ち出す事が可能となります。

（３）内部情報の不正な持ち出し（物理的な持ち出し）

組織の情報を、USB メモリーや HDD 等の外部記憶媒体、メール、クラウドストレージ、スマホカメラ、紙媒体等を利用し、外部に不正に持ち出すケース。こうした行為は予防措置の欠如によって、発見が遅れる事が多々あります。

３．内部不正による情報漏えいの具体的な事例

【事例１：顧客情報を持ち出し、名簿業者に販売】

2023 年 10 月、NTT ビジネスソリューションズは、同社に勤務していた元派遣社員が顧客情報の不正な持ち出しを行っていたことを公表しました。
同派遣社員は 2013 年 7 月から 2023 年 1 月の間に、自身が運用に関わっていたコールセンターのシステムに、管理者アカウントを悪用して不正アクセスし、少なくとも 69 組織の顧客情報 928 万件を USB メモリーにコピーして持ち出していました。
持ち出した顧客情報を名簿業者に販売し、1,000 万円以上を対価として受け取っていたとみられ、逮捕されました。
引用元：IPA 情報セキュリティ 10 大脅威 2024 解説書より抜粋

この事例は、「２．主な攻撃手口」の「（１）アクセス権限の悪用」と「（３）内部情報の不正な持ち

出し」の具体的な内容になります。
運用保守用に割り当てられた管理者アカウントを用いて、内部情報を不正に持ち出していたものです。
また、内部不正者に対するセキュリティ要件が十分ではなかったことも併せて原因と言えます。

【事例２：前職場が保有する名刺情報を転職先に提供】

2023 年 9 月、ワールドコーポレーションの元従業員が、個人情報保護法違反（不正提供）等の疑いで警視庁に逮捕されました。
本従業員は同業他社に転職する直前に、転職元の名刺情報管理システムにログインするための ID とパスワードを転職先の従業員に共有していました。
不正に取得された名刺情報は転職先の営業活動に使用され、成約事例もあったようです。
引用元：IPA 情報セキュリティ 10 大脅威 2024 解説書より抜粋

この事例は、「２．主な攻撃手口」の「（２）在職中に割り当てられたアカウントの悪用」の具体的な内容です。
事例では在職中から漏えいしていたようですが、少なくとも離職者発生時に該当する ID を無効にしておけば被害の拡大は防げたと考えます。

４．内部不正による情報漏えい等への対策

本対策は主に「システム管理者の観点」で説明していきます。

システム管理者の対応と対処

◇被害の予防
・基本方針の策定
「不正のトライアングル」を意識して基本方針を策定し、情報取扱ポリシーの作成、内部不正者に対する懲戒処分等を規定した就業規則等や、委託先との契約内容を整備します *1。
なお、組織内での対策推進は、経営層の積極的な関与が不可欠です。
内部不正対策の責任は経営者にあり、最高責任者である経営者が総括責任者の任命並びに管理体制および実施策の承認を行い、組織横断的な管理体制を構築する必要がある為です。

*1 内部不正を想定した従業員規約等は下記の経産省発行の秘密情報の保護ハンドブックの P175 ページ以降の「参考資料２ 各種契約書等の参考例」、また、情報管理も企業力を合わせてご参照ください。

・資産の把握、対応体制の整備
情報資産を把握し、その重要度をランク付けした上で重要情報の管理者を定めます。

・重要情報の管理、保護
重要情報の利用者 ID およびアクセス権の登録・変更・削除に関する手順を定めて運用します。
従業員の異動や離職に伴う不要な利用者 ID 等は直ちに削除します。
また、それらの適切な管理、定期的な監査を実施します。さらに、利用者 ID の共用禁止等の処置を検討します。DLP（情報漏えい対策）等のツールの導入も併せて検討します。

・物理的管理の実施
重要情報の格納場所や重要情報を扱う執務室への入退室を管理します。
USB メモリー、スマートフォン、プリンター等の外部媒体は利用制限を行い、持ち出しや持ち込みの管理をします。
また、記録媒体の廃棄を行う際には、適切なデータ消去の運用 *2 を実施します。
消去できない場合は媒体の物理的な破壊も検討する必要があります。
また、リース品はデータ消去/初期化してから返却します。

*2 適切なデータ消去：
Windows10/11 の場合、「完全に削除する」又は「ゴミ箱を空にする」を実行したり、クリックフォーマットをしたりしても、ハードディスクや USB メモリー上にはデータが残っており、復元ツール等を利用すると復元できてしまいます。
ハードディスクや USB メモリーの完全なデータ消去は、時間がかかりますがフルフォーマット(Windows の場合にはクイックフォーマットのチェックを外して実行)で可能です。

・情報リテラシー、モラルを向上させる※

・人的管理およびコンプライアンス教育の徹底
従業員には秘密保持義務を課す誓約書に署名させ、定期的に教育を実施します。
被害の予防に対する対策の状況は、IPA 発行の組織における内部不正防止ガイドラインの 102 ページ「付録Ⅱ：内部不正簡易チェックシート」を使ってチェックする事ができます。

◇被害の早期発見
・システム操作履歴の監視
重要情報へのアクセス履歴や利用者の操作履歴等のログ、証跡を記録し、監視する事で早期検知に努めます。また、監視していることを従業員に周知することで不正の予防が可能です。

◇被害を受けた後の対応

・適切な報告／連絡／相談を行う※

・インシデント対応体制を整備し対応する※

・内部不正者に対する適切な処罰の実施

「※」の詳細については、IPA の「情報セキュリティ１０大脅威 2024」の 68 ページの「共通対策」をご参照ください。

また、前々回の「中小企業におけるセキュリティ脅威への対策強化～ランサムウェアによる攻撃事例から対策を学ぶ～（2/2）」でも、詳細を解説していますので、併せてご参照ください。

ここまで内部不正による情報漏えい等の事例や影響、対策方法について考えてきましたが、いかがだったでしょうか。

内部不正による情報漏えい等は、従業員又は元従業員が行うため通常のセキュリティ対策だけでは十分ではないことがお分かりいただけたかと思います。

内部不正による情報漏えいは、システム的な管理／監視と人的管理およびコンプライアンス教育の両輪で行い、これを防止する事は、企業の持続可能な発展を支える鍵となるとも言えます。

５．事例

事例を見る

・当社に派遣されていた元派遣社員の逮捕について（NTT ビジネスソリューションズ株式会社）

・当社元従業員の逮捕について（株式会社ワールドコーポレーション）

レベル２_#11_中小企業におけるセキュリティ脅威への対策強化　～標的型攻撃による機密情報の窃取から対策を学ぶ～

掲載日：2024/11/13



独立行政法人情報処理推進機構（IPA）が毎年発行している「情報セキュリティ 10 大脅威 2024」から、中小企業の経営者やシステム担当者が注目すべき点を掘り下げていきます。

今回は４位に挙げられている「**標的型攻撃による機密情報の窃取**」を深掘りします。

標的型攻撃とは、特定の組織（企業、官公庁、民間団体等）を狙う攻撃のことです。機密情報等の窃取や業務妨害を目的としています。

攻撃者は、標的とする組織の状況に応じた巧みな攻撃手法を用いて機密情報等を窃取しようとします。

この脅威がどのように業務に影響を与えるのか、対策はどうすべきなのかを解説いたします。



引用元：IPA　情報セキュリティ 10 大脅威　2024　解説書より

１．標的型攻撃による機密情報の窃取の脅威

特定の組織や企業に狙いを定め、機密情報等の窃取や業務妨害を目的とした標的型攻撃が発生しています。
この種の攻撃は、明確な目的を持ち、PC やサーバーをウイルスに感染させたり、不正にアクセスすることで組織内部に侵入し、情報窃取や破壊活動等を行います。
これらの攻撃は一時的なもので終わることは少なく、組織内に長期間潜伏して活動を行うケースがあります。

窃取された機密情報が悪用された場合、企業の事業継続や国家の安全保障に重大な影響を及ぼすおそれがあります。
さらに、データ削除やシステム破壊により企業活動が妨害されたり、その企業のサプライチェーンに属する関連組織が攻撃の踏み台にされるおそれもあります。
組織の規模や業種に関わらず標的となる可能性があることが特徴と言えます。

２．代表的な攻撃例

以下に、代表的な標的型攻撃による機密情報の窃取例を紹介します。

（１）フィッシングメールによる感染

攻撃者は、業務や取引に見せかけた巧妙な偽装メールを送信し、そのメールの添付ファイルや本文のリンクにウイルスを仕込みます。受信者がファイルを開封したり、リンクにアクセスすると、PC がウイルスに感染する仕組みです。
メールの件名や本文、添付ファイル名は業務や取引に関連するように偽装されているため、偽物と気づきにくいのが特徴です。さらに、実在する組織名が使われる場合もあるため、注意が必要です。

また、通常の業務メールのやり取りを装い、複数回のやり取りを経て油断させる手口もあります。この攻撃手法を「やり取り型攻撃」と呼びます。顧客や取引先とのやり取りの中であっても、気軽にリンクを開く、ファイルを開くといった行為は危険を伴うものだという意識を持つ必要があります。

（２）改ざんされた Web サイトを利用した攻撃

攻撃者は、標的とする組織が頻繁に利用する Web サイトを調査し、予め改ざんしておきます。
そして、標的組織の従業員や職員がその Web サイトにアクセスすることで PC をウイルスに感染させます。
これにより、標的組織は通常の業務活動を行っている際にウイルスに感染し、その結果として情報が盗まれることとなります。この攻撃手法は「水飲み場型攻撃」とも呼ばれ、無意識の間に感染が進行するため、非常に巧妙な手口です。

（３）脆弱性を突いた不正アクセス

攻撃者は、標的組織が利用するクラウドサービスや Web サーバー、VPN 装置等の脆弱性を悪用して不正アクセスを行い、組織内部へ侵入します。
この侵入が成功し、正規の認証情報等を窃取できた場合は、次回から正規の経路で組織のシステムへ再侵入することもあります。

３．標的型攻撃による機密情報の窃取事例

【事例１：複数回のやり取りを伴う標的型メール攻撃】
2023 年 10 月、東京大学は標的型攻撃メールにより教員が使用していた PC がウイルスに感染し、PC 内の情報が窃取された形跡があることを公表しました。
この攻撃は 2022 年 7 月に、実在する組織の担当者を装った人物からの講演依頼メールで始まりまし

た。日程調整のためのやり取り中、教員がメールに記載された URL をクリックしたことで、PC がウイルスに感染しました。

攻撃者から最終的に「講演が中止になった」との連絡があったため、教員は被害に気付きませんでした。
この攻撃により、教職員や学生等の個人情報や過去の試験問題等計 4,341 件が流出した可能性があります。
引用元：IPA 情報セキュリティ 10 大脅威 2024 解説書より抜粋

この事例は、「やり取り型攻撃」の典型的な例です。
「講演の依頼」という日常的な業務メールのやり取りをしているうちに、ウイルスに感染させられました。
その上、「講演の中止」という形で業務自体が正常に終了したため、教員はウイルスの感染に全く気が付かなかった事も特徴と言えます。
例えばウイルス感染後、急に相手からの連絡が途絶えると、「何か変だ」と気づかれてしまうからです。
このように、正常の業務遂行中にも被害に遭ってしまう事があるという認識が重要です。

【事例 2 ：宇宙航空研究開発機構（JAXA）への不正アクセス】
2023 年 11 月、宇宙航空研究開発機構（JAXA）がサイバー攻撃を受け、内部ネットワークに不正アクセスされていたことが明らかになりました。
不正アクセスを受けたのは一般業務用の管理サーバーで、機微情報は含まれていないと JAXA は説明しています。
この不正アクセスは同年 6 月に修正されたネットワーク機器の脆弱性を悪用されたものとみられています。

外部機関から通報を受けた JAXA は文部科学省に報告し、一部のネットワークを切り離した上で、調査を行っています。
引用元：IPA 情報セキュリティ 10 大脅威 2024 解説書より抜粋

この事例は、「不正アクセス」の典型例であり、ネットワーク機器の脆弱性を悪用された侵入事例になります。
報告では、「一般業務用のサーバーで機密情報はない」とされていますが、これを踏み台にされて、ネットワーク内の機密情報を扱うサーバーに侵入される危険性もあったため、十分な調査が必要です。

４．標的型攻撃への対策

標的型攻撃による機密情報の窃取への対策を、「経営者の観点」「管理者の観点」「従業員・職員の観点」で説明します。

（１）経営者の観点

◇組織としての体制の確立
・被害の予防（被害に備えた対策を含みます）
　インシデント対応体制を整備し、実際のインシデント時に対応します。※

（２）管理者（セキュリティ担当者・システム管理者）の観点

◇被害の予防／対応力の向上
・情報の管理と運用規則策定
　情報は暗号化するなどの管理や運用の規則を定めて運用します。
・サイバー攻撃に関する継続的な情報収集
・情報リテラシー、モラルを向上させます※
・インシデント対応の定期的な訓練を実施
　関係者やセキュリティ業者、専門家と迅速に連携する対応方法や連絡方法を整備します。
・サーバーやクライアント、ネットワークに適切なセキュリティ対策を行います※
・アプリケーション許可リストの整備
・取引先のセキュリティ対策実施状況の確認
・海外拠点等も含めたセキュリティ対策の向上
◇被害の早期検知
・サーバーやクライアント、ネットワークに適切なセキュリティ対策を行います※
◇被害を受けた後の対応
・インシデント対応体制を整備し、実際のインシデント時に対応します※

（３）従業員・職員の観点

◇被害の予防（通常、組織全体で実施）
・IPA の「情報セキュリティ 10 大脅威　2024 解説書」の 10 ページ、表 1.4「情報セキュリティ対策の基本」を実施

表 1.4 情報セキュリティ対策の基本

攻撃の糸口	情報セキュリティ対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消し攻撃によるリスクを低減する
ウイルス感染	セキュリティソフトの利用	攻撃をブロックする
パスワード窃取	パスワードの管理・認証の強化 ※「共通対策」で詳細を解説	パスワード窃取によるリスクを低減する
設定不備	設定の見直し	誤った設定を攻撃に利用されないようにする
誘導(罠にはめる)	脅威・手口を知る	手口から重要視すべき対策を理解する

・メールの添付ファイル開封、メールや SMS のリンク、URL のクリックを安易にしない※

◇被害を受けた後の対応

・インシデント対応体制を整備し、実際のインシデント時に対応します※

「※」の詳細については、IPA の「情報セキュリティ１０大脅威 2024」の 68 ページの「共通対策」をご参照ください。

また、こちらの記事：「中小企業におけるセキュリティ脅威への対策強化～ランサムウェアによる攻撃事例から対策を学ぶ～（2/2）」でも、詳細を解説していますので、併せてご参照ください。

ここまで標的型攻撃による機密情報の窃取について考えてきましたが、いかがだったでしょうか。

ネットワーク内部へ不正アクセスされた場合、情報の漏えいや改ざん、他組織への攻撃の踏み台（中継）になるおそれがあるため、日々の確認や平時の備えが大切なことがおわかりいただけたかと思います。

加えて、2023 年 5 月に経済産業省が公開した「ASM（Attack Surface Management）導入ガイダンス～外部から把握出来る情報を用いて自組織の IT 資産を発見し管理する～」の活用も有効な方法と言えます。

標的型攻撃による機密情報の窃取は、業種や企業の大小に関わらず発生します。

「自社は狙われないから大丈夫」と考えるのではなく、常にこのような脅威が存在することを認識することが重要です。この認識がセキュリティ意識の向上につながり、企業の持続可能な発展を支える鍵となります。

５．事例

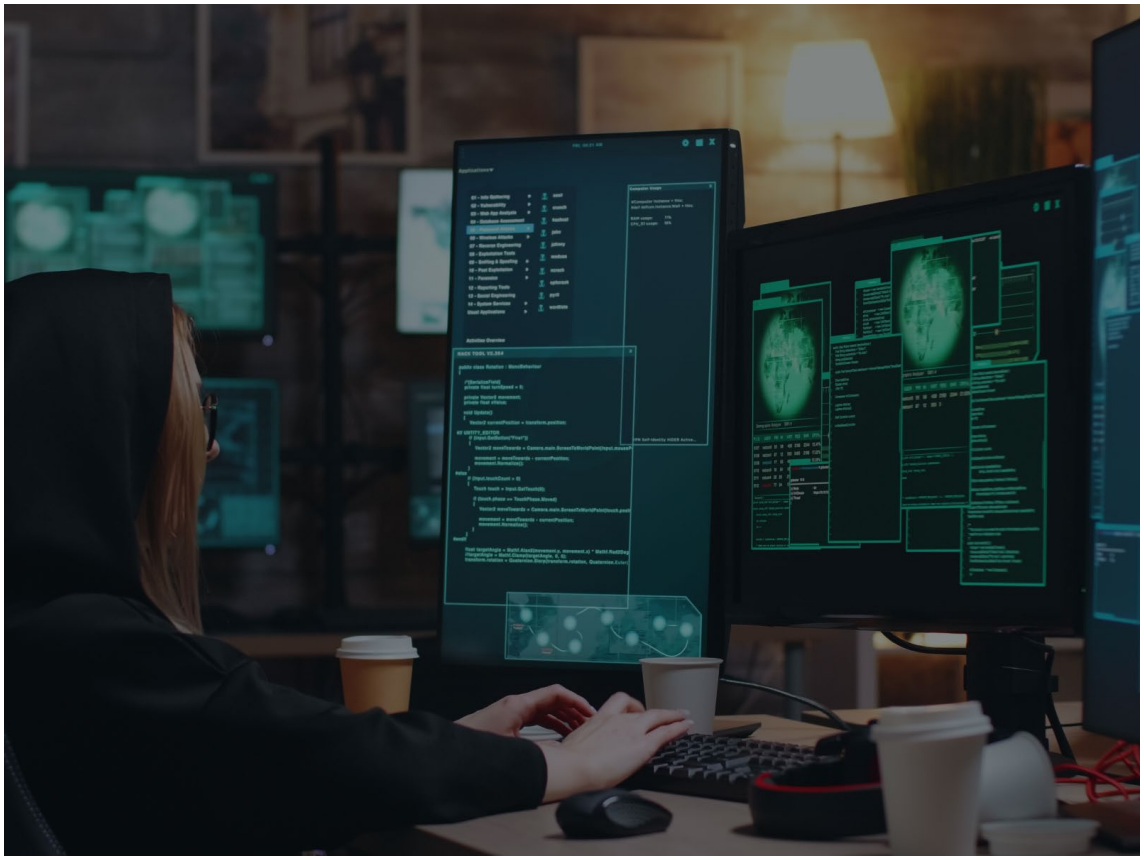
事例を見る

１．東京大学大学院総合文化研究科・教養学部への不正アクセスによる情報流出について（東京大学)

２．サイバー攻撃か東大教員のパソコンに不正アクセス、個人情報 4300 件流出（TBS NEWS DIG）

３．JAXA への不正アクセスについてまとめてみた（piyolog）

レベル 2_#12_中小企業におけるセキュリティ脅威への対策強化　～修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）から対策を学ぶ～
掲載日：2024/11/27

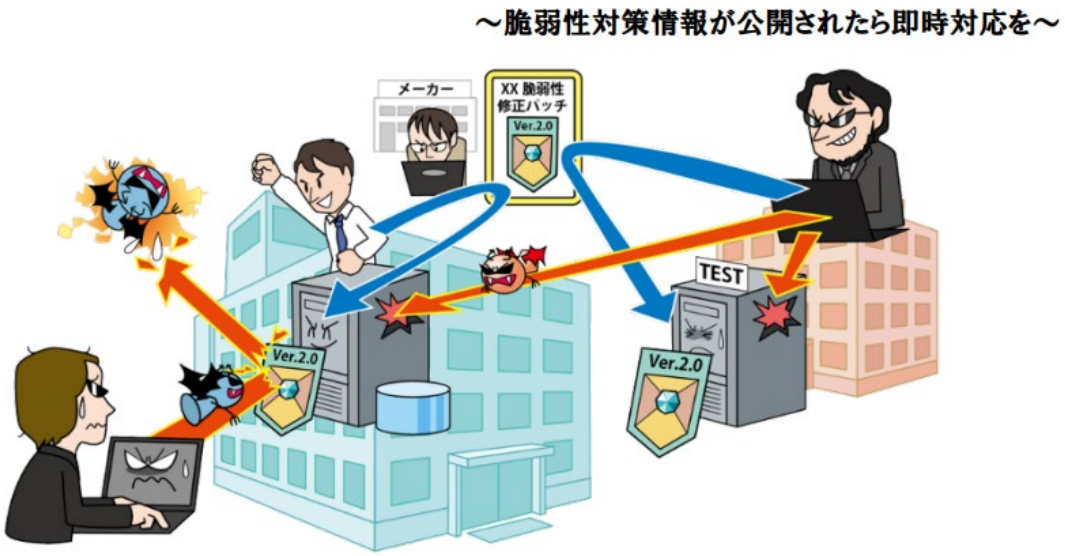


独立行政法人情報処理推進機構（IPA）が毎年発行している「情報セキュリティ 10 大脅威 2024」から、中小企業の経営者やシステム担当者が注目すべき点を掘り下げていきます。

今回は５位に挙げられている「**修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）**」を攻撃事例とともに深掘りします。

１．ゼロデイ攻撃とは

ゼロデイ攻撃とは、システムやソフトウェアの脆弱性に対して、開発ベンダー等が認知もしくは修正プログラムを提供する前に行われる攻撃です。
ゼロデイ攻撃が行われた場合、ウイルス感染や情報漏えい等の直接の被害に留まらず、事業やサービスが停止するなど、多くのシステムやユーザーに影響が及ぶことがあります。
そのため企業には、脆弱性対策情報が公開された場合、早急な対応が求められます。



引用元：IPA　情報セキュリティ 10 大脅威　2024　解説書より

２．ゼロデイ攻撃による脅威

OS やアプリケーション等のソフトウェアの脆弱性が発見されると、開発ベンダー等が調査・分析し、修正プログラム（パッチ）や対策情報を公開します。

しかし、脆弱性対策情報の公開前に攻撃者が脆弱性の存在を知った場合、当該ソフトウェアの脆弱性を悪用したゼロデイ攻撃を仕掛けるおそれがあります。

ゼロデイ攻撃が行われると、ウイルス感染や情報漏えい、Web ページやファイルの改ざん等の被害が発生し、事業やサービスが停止する可能性があります。
また、多くのシステムやユーザーに利用されているソフトウェアの脆弱性がゼロデイ攻撃に悪用された場合、被害が広範囲に及び、社会が混乱状態に陥るおそれもあります。

未知の脆弱性を悪用した攻撃を受けた場合は、被害者が攻撃されたことに気付かないケースもあります。仮に攻撃に気付いたとしても、脆弱性の対策情報が公開されていないために、適切な対応を取れないことが想定されます。
ユーザー側がパッチを未適用状態の N デイ脆弱性*1 を悪用するケースとは異なり、脆弱性対策情報が公開されてはいるものの、ゼロデイ攻撃への対策を行うことは非常に困難です。

*1 N デイ脆弱性：
すでに公開されている脆弱性で、ベンダーや開発者等がパッチを提供もしくは作成中でユーザーは実装を待っている状態のもの。次回で詳しくご説明します。

３．代表的な攻撃例

ソフトウェアの脆弱性の悪用
開発ベンダー等が脆弱性対策情報を公開する前に、攻撃者はその脆弱性を悪用して攻撃します。
悪用の手口は、脆弱性によって異なります。例えば、通信プロトコルの脆弱性を悪用した DDoS 攻撃（分散型サービス妨害攻撃）*2、アプリケーションの脆弱性を悪用した簡易プログラム（スクリプト）の実行、OS の脆弱性を悪用した特権アカウントの作成等があります。
*2 DDoS（Distributed Denial of Service）攻撃：
攻撃対象となる Web サーバーなどに対し、複数のコンピューターから大量のパケットを送りつけることで、正常なサービス提供を妨げる行為を指します。

４．ゼロデイ攻撃の事例

【事例１：HTTP/2 プロトコルの脆弱性を悪用したゼロデイ攻撃】
2023 年 8 月、HTTP/2 プロトコルに存在する脆弱性を狙った大規模な DDoS 攻撃が確認されました。一連の攻撃では 1 秒間に 3 億 9,800 万件を超えるリクエストが発生したと報告されています。
これまで最大規模とされていた、2022 年の 1 秒間に 4,600 万件のリクエストが発生したケースをはるかに上回る規模の攻撃になりました。
この攻撃は、HTTP/2 ラピッドリセット攻撃と呼ばれており、Web サーバー・プロキシサーバー・ロードバランサーや Web API 等、HTTP/2 をサポートする多くのソフトウェアに影響を与えました。
この脆弱性の判明を受け、影響を受けるソフトウェア開発ベンダー間で協調し、情報共有が進められました。そして各社が定例のセキュリティアップデートを公開するいわゆる「パッチチューズデー」にあたる 2023 年 10 月 10 日に、パッチやアップデートの提供等が始まりました。

【事例２：ファイル圧縮ソフト「WinRAR」に存在する脆弱性を悪用したゼロデイ攻撃】
広く利用されているファイル圧縮ソフトの「WinRAR」に複数の脆弱性が存在し、2023 年 4 月以降に一部の脆弱性がゼロデイ攻撃に悪用されていることが判明しました。
アーカイブフォルダ内の画像ファイルやテキストファイルのプレビューを行おうとすると、同名のフォルダ内に配

置されたスクリプトを実行させることが可能になるという脆弱性でした。
開発元である「RARLAB」は、2023 年 8 月 2 日に脆弱性の修正を行った「WinRAR　6.23」をリリースしています。

【事例 3 ：Cisco Systems 製品へのゼロデイ攻撃】
2023 年 10 月、Cisco Systems は「Cisco IOS XE」にリモートから認証がなくとも特権アカウントを作成できる脆弱性があり、9 月中旬よりゼロデイ攻撃が行われていたと公表しました。
同社は、顧客のサポート中に本脆弱性を確認しており、本製品の利用者に対して開発ベンダー等が推奨する対策を講じるとともに、侵害を受けていないか確認するように呼びかけています。

これらは典型的なゼロデイ攻撃の事例です。ほとんどの場合、脆弱性による攻撃の被害が出てからでないと、脆弱性の存在に気が付かず対策が打てないことがお判りになるかと思います。

５．ゼロデイ攻撃への対策

ゼロデイ攻撃への対策を、「経営者の観点」「管理者の観点」で説明します。

（１）経営者の観点

◇被害の予防
・インシデント対応体制を整備し、実際のインシデント時に対応します※

（２）管理者（セキュリティ担当者・システム管理者）の観点

◇被害の予防
・IPA の「情報セキュリティ 10 大脅威　2024 解説書」の 10 ページ、表 1.4「情報セキュリティ対策の基本」を実施する。

表 1.4 情報セキュリティ対策の基本

攻撃の糸口	情報セキュリティ対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消し攻撃によるリスクを低減する
ウイルス感染	セキュリティソフトの利用	攻撃をブロックする
パスワード窃取	パスワードの管理・認証の強化 ※「共通対策」で詳細を解説	パスワード窃取によるリスクを低減する
設定不備	設定の見直し	誤った設定を攻撃に利用されないようにする
誘導（罠にはめる）	脅威・手口を知る	手口から重要視すべき対策を理解する

・資産の把握、対応体制の整備
・セキュリティのサポートが充実しているソフトウェアやバージョンを使用します
・修正プログラムや回避策の提供が迅速である製品や開発ベンダーを利用し、サポート対象のソフトウェアを使用します
・利用するソフトウェアの脆弱性情報の収集と周知、対策状況の管理
・サーバーやクライアント、ネットワークに適切なセキュリティ対策を行います※

◇被害の早期検知
・サーバーやクライアント、ネットワークに適切なセキュリティ対策を行います※

◇修正プログラムのリリース前の対応
・回避策や緩和策の適用
・当該ソフトウェアの一時的な使用停止。場合によってはサービスの停止も検討します

◇修正プログラムリリース後の対応
・修正プログラムの適用。必要に応じて回避策、緩和策を無効化します

◇被害を受けた後の対応
・影響調査および原因の追究、対策の強化
・適切な報告／連絡／相談を行います※

「※」の詳細については、IPA の「情報セキュリティ１０大脅威 2024」の 68 ページの「共通対策」をご参照ください。

また、こちらの記事：「中小企業におけるセキュリティ脅威への対策強化～ランサムウェアによる攻撃事例から対策を学ぶ～（2/2）」でも、詳細を解説していますので、併せてご参照ください。

ここまでゼロデイ攻撃について考えてきましたが、いかがだったでしょうか。
ゼロデイ攻撃は基幹となる重要ソフトウェアの未解決な脆弱性を狙う攻撃のため、利用者側で完全に防ぐことは困難です。
自社で使用しているソフトウェアの修正プログラムが各端末で適用されているのか、定期的に確認を行い、適切なセキュリティ対策を導入しましょう。たとえ攻撃を受けたとしても対処できるよう、事前の準備が重要になると言えます。
常にこのような脅威への準備を万全にすることが、企業の持続可能な発展を支える鍵となります。

６．事例

事例を見る
1.「ラピッドリセット攻撃」が発生-1 秒間で約 4 億リクエスト（Security NEXT）
2.4 月以降「WinRAR」狙うゼロデイ攻撃が発生-最新版に更新を（Security NEXT）
3.「IOS XE」の深刻なゼロデイ脆弱性-JPCERT/CC も攻撃被害を確認（Security NEXT）

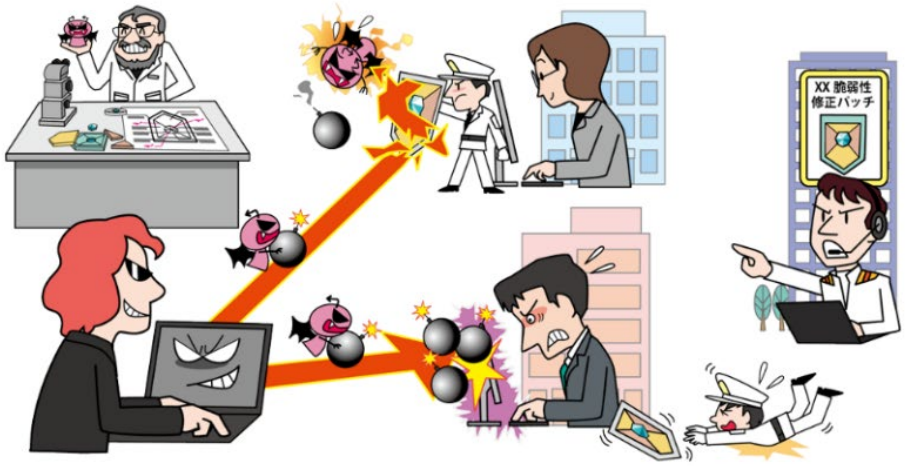
レベル 2_#13_中小企業におけるセキュリティ脅威への対策強化　～脆弱性対策情報の公開に伴う悪用増加から対策を学ぶ～
掲載日：2024/12/11



独立行政法人情報処理推進機構（IPA）が毎年発行している「情報セキュリティ 10 大脅威 2024」から、中小企業の経営者やシステム担当者が注目すべき点を掘り下げていきます。
今回は 7 位に挙げられている「**脆弱性対策情報の公開に伴う悪用増加**」に焦点を当てます。

ソフトウェアやハードウェアの脆弱性対策情報の公開には、利用者に対して脆弱性の脅威やその対策方法を知らせるという利点があります。
しかし一方で、その公開された情報は悪意ある攻撃者にとっても貴重な攻撃の手がかりとなり得るのです。
攻撃者はその情報を悪用し、脆弱性対策を講じていない当該製品を使用したシステムを狙って攻撃を行う恐れがあります。
近年では脆弱性関連情報が公開されるとすぐに攻撃コードが流通し、攻撃が本格化するまでの時間がますます短くなっているため、細心の注意を払って、最新の情報を入手する必要があると言えます。

～放置せず、傷口が広がる前に速やかな処置を～



引用元：IPA　情報セキュリティ 10 大脅威　2024　解説書より

１．脆弱性対策情報の公開に伴う悪用増加による脅威

一般的に、ソフトウェアに脆弱性が発見された場合、開発ベンダーが脆弱性の修正プログラム（パッチ）を作成します。
その後、ベンダーはセキュリティ対応機関等と連携するか、または自身で脆弱性対策情報として脆弱性の内容とパッチや対策方法、暫定対策情報を一般に公開し、当該ソフトウェアの利用者へセキュリティ脅威への対策を促します。

一方攻撃者は、公開された脆弱性対策情報を基に攻撃コード等をいち早く作成し、パッチ適用等のセキュリティ対策を実施する前のソフトウェアに対して、脆弱性を悪用した攻撃を行います。
これによる情報漏えいや改ざん、ウイルス感染等の被害の発生が確認されています。
特にネットワーク機器(VPN 機器)やコンテンツ管理システム（プラグインを含む CMS）等、広く利用されている製品の脆弱性の場合には、脆弱性情報が公開されると瞬く間に多くの攻撃の対象となる危険性があります。
昨今、脆弱性が発見されてからそれを悪用した攻撃が発生するまでの時間が短くなっており、より迅速な対応が求められています。

２．代表的な攻撃例

（１）Ｎデイ脆弱性攻撃の危険性

Ｎデイ脆弱性とは、パッチや回避策が提供された後、そのパッチの適用や回避策を講じるまでの期間（Ｎ日）に存在する脆弱性を指します。
特に、ソフトウェアの管理が不適切な企業は、未対応の時間（Ｎ 日）が長くなるため、被害に遭うリスクが大きくなります。
加えて、その脆弱性が確かであることを示す実証コード（PoC）※が公開されることもあり、このコードが攻撃に悪用されることも少なくありません。

※PoC(Proof of Concept)：脆弱性が新たに発見された場合に、プログラムに潜む問題点を明確にする（＝実証する）ために用意されたコードを意味します。

なお Ｎ デイ脆弱性に対して、パッチや回避策が公開される前に発見されたソフトウェアの脆弱性をゼロデイ脆弱性と呼び、これを用いた攻撃を**ゼロデイ攻撃**と呼んでいます。
（詳細はこちらの記事「中小企業におけるセキュリティ脅威への対策強化 ～修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）から対策を学ぶ～」を参照してください）

（２）公開されている攻撃ツールの使用

公開された脆弱性に対する攻撃ツールは短期間で作成され、ダークウェブ上で取引されたり、攻撃サービスとして提供されたりすることがあります。
また、誰でも利用可能なオープンソースのツールに脆弱性を利用する機能が実装され、それを悪用されることもあります。

３．脆弱性悪用の具体的事例

【事例１：ソフトウェアの修正版公開後の攻撃増加】
2023 年 10 月 25 日（米国時間）、Apache Software Foundation は同社の Apache ActiveMQ および Apache ActiveMQ Legacy Open Wire Module にリモートからコード実行が可能となる脆弱性を対策したバージョンを公表しました。
本脆弱性は技術情報や実証コードが公開されており、Rapid7 によると 10 月 27 日に脆弱性を悪用したと見られるランサムウェアの活動を同社の複数の顧客で確認していました。

また、NICT（国立研究開発法人情報通信研究機構）の NICTER におけるダークネット観測網では、同脆弱性に関連した通信を 10 月 27 日頃から観測し、11 月 26 日頃には更なる通信の増加が確認されてボットとみられる感染活動を観測しました。

【事例 2 ：VPN 機器の脆弱性が断続的な攻撃の対象に】
2023 年 5 月、Array Networks が提供する VPN アプライアンス「Array AG シリーズ」の脆弱性を悪用した標的型攻撃が断続的に観測されていることを、JPCER コーディネーションセンター（一般社団法人 JPCERT コーディネーションセンター）が注意喚起しました。
対象の脆弱性（CVE-2022-42897、CVE2023-28461）はそれぞれ 2022 年 9 月と 2023 年 3 月に修正されていましたが、海外拠点も標的となっており、自組織の海外拠点における対策や侵害調査を行うことも推奨されています。

【事例 3 ：脆弱性を修正した機器への継続的な攻撃】
2023 年 5 月 19 日（米国時間）、Barracuda Networks は同社のメールセキュリティ製品の Email Security Gateway アプライアンス（ESG）にリモートからシステムコマンドが実行可能となる脆弱性があることを特定し、翌日の 5 月 20 日に修正パッチを公開しました。
しかし、本脆弱性の修正対応後も、特定の組織では攻撃者による新たなバックドアの設置や、ネットワーク上での横展開等、継続的な攻撃活動が確認されています。
同社では脆弱性の最初の悪用は 2022 年 10 月とし、侵害された組織に対し、アプライアンスの交換を推奨しています。
また、米連邦捜査局（FBI）および国内の IPA や JPCERT コーディネーションセンターにおいても注意喚起を行っていて、本脆弱性の修正パッチを済ませた組織でも、追加の侵害調査を行うことを推奨しています。

これらは脆弱性対策情報の公開に伴う悪用の事例です。ほとんどの場合、脆弱性公開後、修正のパッチが提供されているにもかかわらず、「提供に気が付いていない」又は「気が付いていても何らかの理由でパッチの適用が実施できていない」など、組織の対応の問題で発生しています。
逆を言えば、これらの攻撃は、常に使っている製品のセキュリティパッチさえ適切に適用すれば回避できるものです。

４．脆弱性対策情報の公開に伴う悪用への対策

脆弱性対策情報の公開に伴う悪用への対策を、「経営者の観点」「管理者（セキュリティ担当者・システム管理者）の観点」で説明します。

（１）経営者の観点

◇被害の予防

・インシデント対応体制を整備し、対応します※

（２）管理者（セキュリティ担当者・システム管理者）の観点

◇被害の予防

・IPA の「情報セキュリティ 10 大脅威 2024 解説書」の 10 ページ、表 1.4「情報セキュリティ対策の基本」を実施します

表 1.4 情報セキュリティ対策の基本

攻撃の糸口	情報セキュリティ対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消し攻撃によるリスクを低減する
ウイルス感染	セキュリティソフトの利用	攻撃をブロックする
パスワード窃取	パスワードの管理・認証の強化 ※「共通対策」で詳細を解説	パスワード窃取によるリスクを低減する
設定不備	設定の見直し	誤った設定を攻撃に利用されないようにする
誘導（罠にはめる）	脅威・手口を知る	手口から重要視すべき対策を理解する

・脆弱性関連情報の収集と対応

・一時的なサーバー停止等パッチや回避策をすぐに適用できない場合を想定して、システム公開前に一時的なサーバー停止等の回避策を検討しておきます

◇被害の早期検知

・サーバーやクライアント、ネットワークに適切なセキュリティ対策を行います※

◇被害を受けた後の対応

・適切な報告／連絡／相談を行います※

・インシデント対応体制を整備し対応します※

「※」の詳細については、IPA の「情報セキュリティ１０大脅威 2024」の 68 ページの「共通対策」をご参照ください。

また、インシデント対応体制を整備し対応するための方策については、「もっと知りたい！セキュリティ」の「セキュリティインシデント対応（１／２）」および「セキュリティインシデント対応（２／２）」でも解説しています。こちらも併せて参照してください。

ここまで脆弱性対策情報の公開に伴う悪用増加について考えてきましたが、いかがだったでしょうか。
脆弱性対策情報の公開に伴う悪用は、脆弱性の修正パッチ配布から適用までの間（Ｎデイ）を狙う攻撃のため、利用者側で適切な対応策を講じることができれば、十分に防げるものです。
自社で使用しているソフトウェアの修正プログラムが各端末で適用されているかを定期的に確認し、適切なセキュリティ対策を日々継続する事が重要になると言えます。
これらの対策を行うことで、脆弱性を狙ったセキュリティ脅威に対してより強靭な防御を構築し、業務を安全に日々継続できることが、企業の持続可能な発展を支える鍵となります。

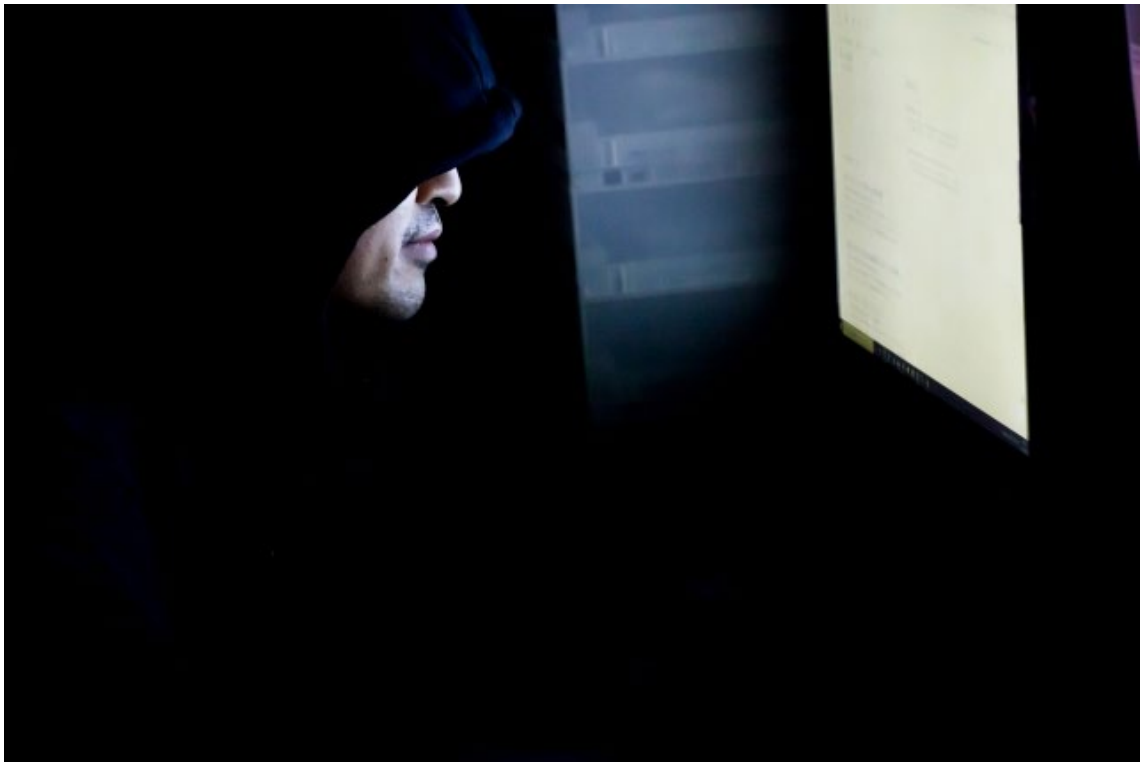
５．事例

事例を見る

１．CVE-2023-46604: Apache ActiveMQ の悪用の疑い（ラピッドセブン・ジャパン株式会社）
２．Array Networks 製 VPN 機器、標的型攻撃の対象に-侵害状況の確認を（Security NEXT）
３．Barracuda 製メールセキュリティ製品に脆弱性-すでに悪用も（Security NEXT）
４．Barracuda Email Security Gateway（ESG）の脆弱性（CVE-2023-2868）を悪用する継続的な攻撃活動に関する注意喚起（一般社団法人 JPCERT コーディネーションセンター）

レベル 2_＃14_中小企業におけるセキュリティ脅威への対策強化　～犯罪のビジネス化（アンダーグラウンドサービス）から対策を学ぶ～

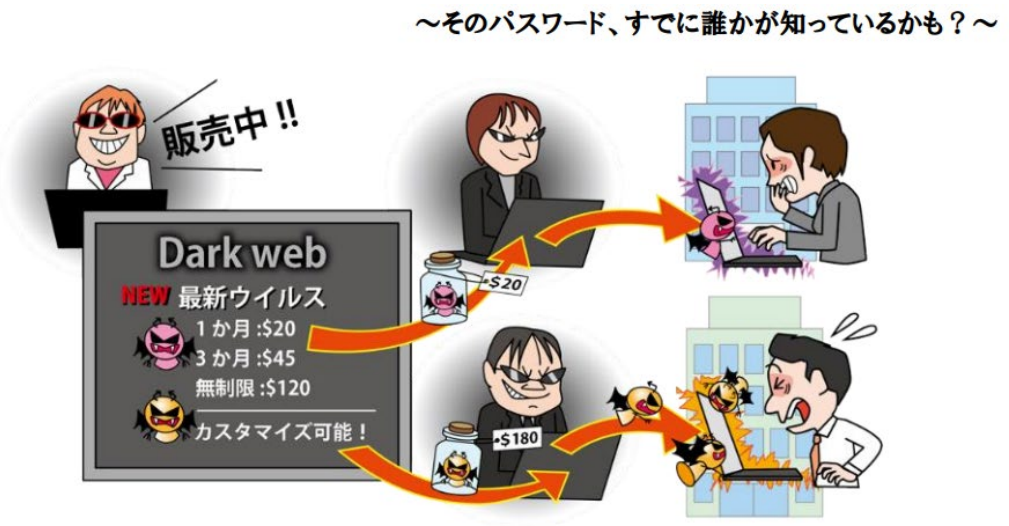
掲載日：2024/12/18



独立行政法人情報処理推進機構（IPA）が毎年発行している「情報セキュリティ 10 大脅威 2024」から、中小企業の経営者やシステム担当者が注目すべき点を掘り下げていきます。

今回は 10 位に挙げられている「**犯罪のビジネス化（アンダーグラウンドサービス）**」(以下、アンダーグラウンドサービスと記載)に焦点を当てます。

アンダーグラウンドサービスとは、サイバー攻撃が金銭的利益を追求する目的で行われ、その目的を果たすための仕組みが発展している状態を指します。サイバー犯罪がビジネス化されたアンダーグラウンド市場では、アカウントの ID やパスワード、クレジットカード情報、ウイルスなどが売買され、サイバー攻撃のスキルがなくてもハッキングなどの犯罪行為が容易に行えるようになっています。



引用元：IPA　情報セキュリティ 10 大脅威　2024　解説書より

１．アンダーグラウンドサービスによる脅威

企業や個人が保有する情報が大きな金銭的価値を持つ現代、サイバー攻撃を目的としたツールやサービスがアンダーグラウンド市場で日常的に取り引きされています。
アンダーグラウンドで商用化されたツールやサービスとして、16SHOP というフィッシングサイトを作成するツールや、RaaS（Ransomware as a Service）*1、AaaS（Access as a Service）*2 などのビジネスモデルがあります。

*1 RaaS（Ransomware as a Service）：ランサムウェア本体や身代金要求のための攻撃に必要な一式をサービスとして提供するサイバー犯罪のビジネスモデルの一種。
*2 AaaS（Access as a Service）：企業の Web サイトや IT システムへの不正アクセスツールやアクセス権限自体を販売するサイバー犯罪の分業形態。AaaS を利用することでサイバー犯罪者は標的へのアクセス権限を自身で搾取することなくアンダーグラウンドで購入することができる。

これらを利用した攻撃が増えています。攻撃を受けた場合、ウイルス感染や金銭の窃取、サーバーへの DDoS 攻撃や業務妨害の被害に遭う可能性があります。

アンダーグラウンドで取り引きされているサービスやツール等は、ダークウェブと呼ばれる通常のブラウザでは検索できない Web サイト上に存在する場合があります。
また、近年では、匿名性の高いメッセージサービスのグループチャットを利用した取引も確認されています。

２．代表的な攻撃例

（１）購入したツールやサービスを利用した攻撃

アンダーグラウンドで購入したツールやサービスを利用して、脆弱性の悪用やボットネット*3 の利用など、様々な攻撃を行います。
代表的なサービスとして、ランサムウェアを販売するサービス(RaaS)や、不正アクセスの手段を販売するサービス(AaaS)が確認されています。

*3 ボットネット：ボット*4 に感染したコンピュータと、攻撃者の命令を送信する指令サーバーによって構成されたネットワークのことで、攻撃者はボットネットに接続したコンピュータに対して一斉に同じ指令を与えることができます。
*4 ボット：ボット（bot）とは、コンピュータで指定された作業を自動的に実行するプログラムの総称ですが、ここでは同じ機能を持ったマルウェアの一種として記述されています。

（２）購入した認証情報を利用した攻撃

アンダーグラウンドで購入した ID やパスワードなどの認証情報を利用して、不正ログインを行う攻撃です。

（３）サイバー犯罪に加担する人材の募集

サイバー犯罪は、組織的に行われることもあります。
アンダーグラウンドの掲示板に高額な報酬を提示して人材を募集し、組織的な犯罪を行います。

３．アンダーグラウンドサービスの事例

【事例１：ChatGPT のアカウント売買】
2023 年 4 月、チェック・ポイント・リサーチは盗まれた ChatGPT 有料アカウントの取引増加を警告しました。
盗まれた有料アカウントはダークウェブ上で販売されており、悪意ある第三者にアカウントが購入された場合、正規ユーザーのアカウントが乗っ取られ、情報の漏えいやクレジットカード情報が窃取される可能性があることを指摘しています。
盗まれた有料アカウントは販売されるだけではなく、盗みのためのサービスやツールを宣伝することを目的に、無償で提供されることもあります。

【事例２：国内製造業の情報がダークウェブに流出】

2023 年 6 月、アイギス・テックは国内の主要製造業 30 社について、ダークウェブへのアカウント情報漏えい状況調査結果を発表しました。

調査した 30 社すべてで、ダークウェブ上にアカウント情報や機密文書がアップロードされていることが判明しました。

特に製造業は、過去に調査した金融機関、行政機関の結果と比較すると、情報漏えい件数やハッキング被害件数などにおいてすべて上回っていました。

【事例３：ウイルスの月額販売】

2023 年 10 月、Fortinet は情報窃取ウイルス「ExelaStealer」がダークウェブ上に登場したことを注意喚起しました。

このウイルスは Windows プラットフォームを標的にしたもので、クレジットカード等の情報を窃取します。

月額や買い切りで利用する方法があり、月額 20 ドルと安価に提供されています。また、カスタマイズサービスも提供されており、さらにビジネス化が進んでいると言えます。

従来のサイバー攻撃は、個人が自分のスキルを披露する目的や、攻撃対象となる企業や個人への嫌がらせを目的に行われることが中心でした。しかし、昨今のサイバー攻撃は金銭的な利益を得るための手段、つまりビジネス化しています。個人の技術に依存しない攻撃の仕組みが確立されているため、ツールやマルウェアを容易に入手・利用できてしまいます。アンダーグラウンドサービスの開発者は、さらに利益を得るために開発を促進し、犯罪のビジネス化がますます進んでしまうのです。

４．アンダーグラウンドサービスの対策

攻撃に使用されるツールやサービスによって対策は異なりますが、以下の代表的な対策を実施しましょう。

より具体的な対策については、これまでのメールマガジンでご紹介した他の脅威を参照してください。

（１）経営者の観点

◇組織としての体制の確立

・インシデント対応体制を整備し対応します※

（２）組織（システム管理者）の観点

◇被害の予防

・DDoS 攻撃の影響を緩和する ISP（インターネットサービスプロバイダー）や CDN（コンテンツデリバリーネットワーク）等を利用します

・システムの冗長化等の軽減策を適用します

・Tor ノード*5 の検知/ブロックを行います

・サーバーやクライアント、ネットワークに適切なセキュリティ対策を行います※

＊5：Tor ノード：Tor(The Onion Router)は匿名通信を可能にするソフトウェアで、Tor ノードはそのネットワークに参加するホストを指します。

◇被害の早期検知

・ダークウェブの監視

監視サービス等を用いて、自組織に影響のある攻撃情報や流出情報の存在を確認します

◇被害を受けた後の対応

・適切な報告／連絡／相談を行います※

・通信制御（DDoS 攻撃元をブロック等）

・Web サイト停止時の代替サーバーの用意と告知手段を整備します

・適切なバックアップ運用を行います※

・インシデント対応体制を整備し対応します※

（３）組織（PC 利用者）の観点

◇被害の予防

・情報リテラシー、モラルを向上させます※

・メールの添付ファイル開封や、メールや SMS のリンク、URL のクリックを安易にしないように注意します※

・サーバーやクライアント、ネットワークに適切なセキュリティ対策を行います※

・多要素認証等の強い認証方式を利用します

◇被害の早期検知

・不審なログイン履歴を確認します

◇被害を受けた後の対策

・インシデント対応体制を整備し対応します※

「※」の詳細については、IPA の「情報セキュリティ１０大脅威 2024」の 68 ページの「共通対策」をご参照ください。

また、インシデント対応体制を整備し対応するための方策については、「もっと知りたい！セキュリティ」の「セキュリティインシデント対応（1/2）」および「セキュリティインシデント対応（2/2）」でも解説しています。こちらも併せて参照してください。

ここまで犯罪のアンダーグラウンドサービスについて考えてきましたが、いかがだったでしょうか。

アンダーグラウンドサービスにより、攻撃者にとっては攻撃のハードルが下がり、企業にとってはより脅威が高まることがおわかりいただけたと思います。
情報が大きな金銭的価値を持つようになったことで、攻撃技術や手段が売買され、さらなる攻撃手段の開発が進んでいくという負の連鎖のビジネスモデルが新たな脅威となっています。

犯罪のビジネス化による脅威の高速化と拡大には、適切なセキュリティ対策を日々継続することが重要になると言えます。常にこのような脅威への準備を万全にすることが、企業の持続可能な発展を支える鍵となります。

今回で、IPA の「情報セキュリティ１０大脅威 2024」の１０大脅威についての解説は終了になります。
次回からは、情報セキュリティ対策を実践する責任者・担当者を対象に、実務的な進め方について説明していきます。

５．事例

事例を見る
１．チェック・ポイント・リサーチ、ChatGPT に関する新たな懸念となる窃取された有料アカウントの売買増加を確認（PRTIMES）
２．国内主要製造業 30 社、ダークウェブへの情報流出調査結果（株式会社 ZERO SECURITY）
３．月額 20 ドル・3 カ月 45 ドル・無期限 120 ドルのお買い得マルウェア登場、警戒を（TECH+）

レベル 2_#15_中小企業におけるセキュリティ脅威への対策強化　～情報セキュリティ対策の進め方『できるところから始めよう』～

掲載日：2025/1/8



中小企業において、情報セキュリティの脅威はますます無視できない問題となっています。
独立行政法人情報処理推進機構（IPA）が発行している「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」の「第 2 部実践編」では、具体的な対策方法と中小企業の経営者やシステム担当者がこれにどう取り組むべきかを詳しく解説しています。

情報セキュリティ対策に組織全体で取り組むには、実行すべき対策を決めて、従業員に周知する必要があります。
しかし、こうした作業を行うには情報セキュリティに関する知識や経験が必要となるため、それらの知識や経験に長けた人材がいないと対策が進まなくなることも考えられます。

このような背景から、IPA のガイドラインでは規模の小さな企業や、これまで十分な情報セキュリティ対策を実施してこなかった企業などを対象に、すぐに取り組める対策を示し、段階的に発展させていく計画を紹介しています。この「すぐに取り組める対策」が、多くの企業にとって無理なく、自社の状況に応じた対策を開始する道筋となります。

今回は、『できるところから始めよう』と題し、すぐに始められる情報セキュリティ対策に焦点を当てて進めていきます。

１．情報セキュリティに対する中小企業の現状と課題

サイバー攻撃が日常的に発生する状況下において、昨今では、情報セキュリティ対策が強固な大企業だけではなく、中小企業も攻撃の標的にされています。
同一のサプライチェーンを構成する中小企業を経由して、目的企業を攻撃する事例も多数報じられています。
中小企業であっても、サイバー攻撃により取引先企業の機密情報が漏えいするリスクや、次なる攻撃の足掛かりとされる可能性があることを念頭に置き、適切な対策を実施することが重要です。

IPA の「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」報告書によると、過去 3 期の「情報セキュリティ対策投資額」について「投資を行っていない」と回答した企業は 33.1%でした。

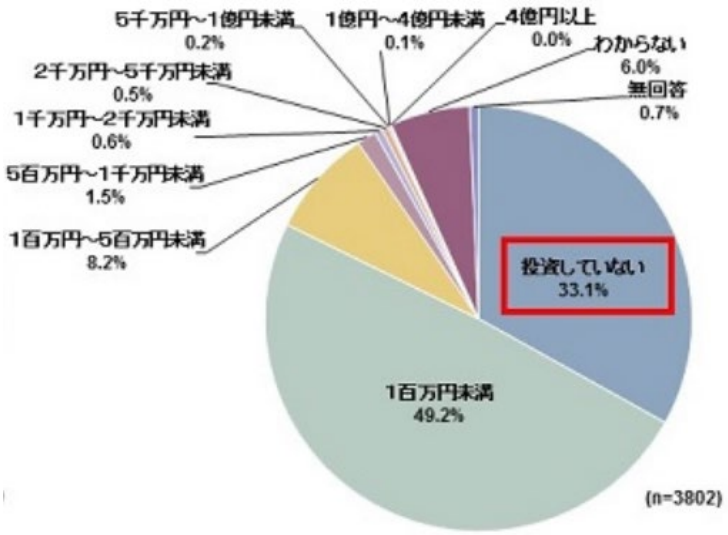


図１．直近過去 3 期の情報セキュリティ対策投資額
（引用：「2021 年度 中小企業における情報セキュリティ対策に関する実態調査」報告書）

投資を行わなかった理由として、「必要性を感じていない」が 40.5%と最も多く、「費用対効果が見えない（24.9%）」、「コストがかかり過ぎる（22.0%）」がこれに続いています（下図参照）。

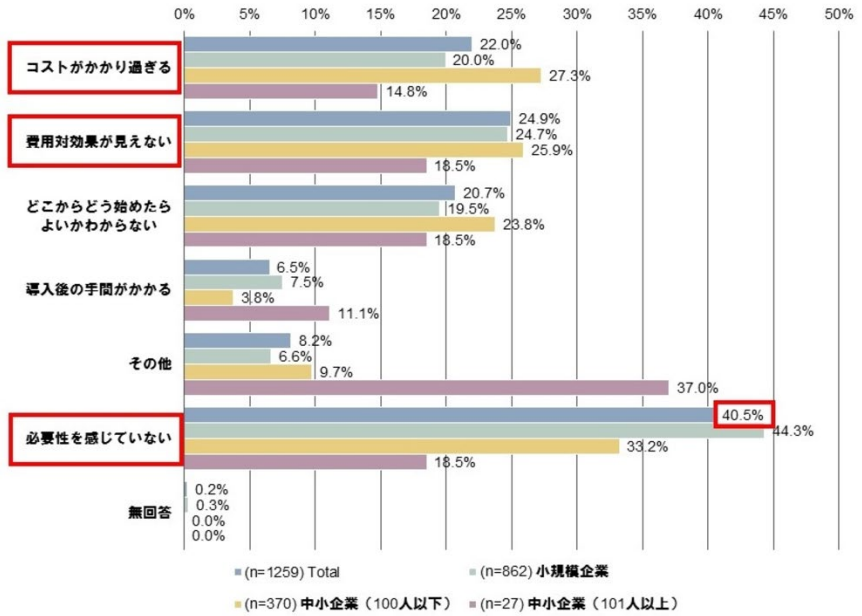


図２．情報セキュリティ対策を行わなかった理由（企業規模別）
(引用：「中小企業における情報セキュリティ対策に関する実態調査」報告書)

なお、従業員数 101 人以上の中小企業においては、「その他」の割合が最も高くなっています。
これは「親会社が投資しているため自社負担がない」という理由からのようです。

２．情報セキュリティ５か条から始めるセキュリティ対策

多くの中小企業にとって、情報セキュリティは「守るべき秘密情報はない」などの物理的理由や、「費用対効果が見えない」「自社は攻撃の対象にならない」という心理的理由から対策が後手に回りがちです。また一方で、必要性は十分に認識しているが、大掛かりでかつ精巧な対策は大変で、なかなか始められないという声も聞きます。

インターネットの普及に伴い、攻撃者の手口は年々巧妙かつ悪質になっており、中小企業も無関係ではいられません。
「情報セキュリティ５か条」では企業の規模に関わらず、重要な基本対策が５項目にまとめられています。必ず実行しましょう。



図 3．中小企業の思い込み
引用：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！

OS やソフトウェアを古い状態で放置していると、セキュリティ上の脆弱性を抱えたままになり、それを悪用した攻撃によりウイルス感染するリスクが高まります。お使いの OS やソフトウェアに修正プログラムを適用するなど、常に最新の状態にしましょう。

【対策例】
・Windows Update（Windows OS の場合）、ソフトウェア・アップデート（macOS の場合）などベンダが提供するサービスを実行する。
・Adobe Acrobat Reader やブラウザなど、利用中のソフトウェアを最新版にする。
・テレワークで利用するパソコンのソフトウェアや、Wi-Fi ルーターのファームウェアを最新版にする。
・利用中のソフトウェアに脆弱性が存在しないか、MyJVN バージョンチェッカ※で確認する。
※MyJVN バージョンチェッカは、パソコンにインストールされているソフトウェア製品が最新かどうかを簡単な操作で確認できるツールです。

（２）ウイルス対策ソフトを導入しよう！

近年、ファイルを暗号化したり、パスワードを盗み、遠隔操作を行うウイルスが増加しています。
ウイルス対策ソフトを導入し、ウイルス定義ファイル（パターンファイル）を自動更新設定にすることで、新たな脅威にも対応できるようにしましょう。

【対策例】
・ウイルス定義ファイルが自動更新されるように設定する。
・統合型のセキュリティ対策ソフトの導入を検討する。
・OS に標準搭載されているセキュリティ機能を有効活用する。
・テレワークで利用するパソコン等の端末にウイルス対策ソフトを導入し、ウイルス定義ファイルを最新の状

態にする。

（３）パスワードを強化しよう！

パスワードの解析や流出による不正アクセスの被害が増えています。
強固なパスワードを設定するために、パスワードは「長く」「複雑に」「使い回さない」ようにしましょう。

【対策例】
・パスワードは 10 文字以上で「できるだけ長く」、大文字、小文字、数字、記号を含めて「複雑に」する。
・名前、電話番号、誕生日、簡単な英単語などは使わず、推測できないようにする。
・同じ ID・パスワードを複数のサービスで「使い回さない」。
・テレワークで VPN やクラウドサービスを利用する際、可能な限り多段階認証や多要素認証を利用する。

（４）共有設定を見直そう！

データ保管などのウェブサービスやネットワーク接続した複合機の設定を誤ったために、無関係な人に情報を見られてしまうといった情報漏えいのケースが増えています。データ共有時の設定を確認し、適切な権限を持った人だけがデータにアクセスできるようにしましょう。

【対策例】
・ウェブサービス、ネットワーク接続の複合機・カメラ、ハードディスク（NAS：Network Attached Storage）などの共有範囲を限定する。
・従業員の異動や退職時には速やかに設定を変更（削除）する。
・テレワークで使用するパソコン等は他者と共有しない。共有せざるを得ない場合は、別途ユーザーアカウントを作成する。
・外出先でフリーWi-Fi は極力使わない。やむを得ず利用する場合には、「セキュリティ保護あり」のアクセスポイントを利用する。また、パソコンのファイル共有をオフにする。

（５）脅威や攻撃の手口を知ろう！

攻撃者が取引先や関係者を装い、ウイルスを仕込んだメールを送ってきたり、正規のウェブサイトに似せた偽サイトを立ち上げて ID・パスワードを盗もうとしたりする巧妙な手口が増えています。常に最新の脅威や攻撃の手口の動向を追って、対策をとりましょう。

【対策例】
・IPA など、セキュリティ専門機関のウェブサイトやメールマガジンで最新の脅威や攻撃の手口を知る。
・利用中のインターネットバンキングやクラウドサービスなどが提供する注意喚起を確認する。
・テレワークでは管理者が従業員に適宜注意喚起し、セキュリティに関する懸念があった場合は、速やかに報告するよう従業員教育を実施する。

３．情報セキュリティ５か条から始めた事例

【事例：SECURITY ACTION をきっかけに危機意識を持ち、認証取得へ】
当社は愛知県で印刷・印刷関連業を営む、従業員５名以下の企業です。取引先は、個人から企業まで多岐に渡っています。
数年前、「SECURITY ACTION」を宣言するにあたって情報セキュリティ対策について学んだ際に、当時の対策では不足しているのではないかという危機感を覚え、より強固な対策を実施したいと考えるに至りました。
しかし、高度な専門知識を有する従業員がいないため、実際の取り組みには至っていませんでした。
その後、関連会社にて IPA が実施する「中小企業の情報セキュリティマネジメント指導業務」を活用して P マークの取得に取り組むことになり、当社も一緒に P マークを取得することとしました。
引用：IPA: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―事例集―より一部抜粋

４．SECURITY ACTION「★一つ星」取得のすすめ

事例にもあるように「SECURITY ACTION」は、中小企業が自主的に情報セキュリティ対策に取り組む姿勢を自己宣言する制度です。安全・安心な IT 社会を実現するために創設されました。
「★一つ星」を宣言するには、情報セキュリティ 5 か条に従って状況のチェックと対策に取り組みます。なお、「★一つ星」は、これから情報セキュリティ５か条に取り組むことを宣言するものであり、対策実施前でも申込みは可能です。

「★一つ星」宣言は、情報セキュリティ対策に取り組んだことのない企業でも、すぐに始めることができます。規模や業種を問わず共通する基本的な対策を実行することで、顧客や取引先との信頼関係の構築に大いに役立ちます。
さらに、デジタル化やサイバーセキュリティ対策などを支援する公的支援制度の要件になるなど、情報セキュリティのはじめの一歩として、とても有益な制度です。
（SECURITY ACTION 自己宣言の申込方法はこちら）



図 4.SECURITY ACTION「★一つ星」ロゴマーク(サンプル)

ここまで情報セキュリティ５か条の内容と、これを実践する宣言であるSECURITY ACTION「★一つ星」についてご紹介いたしましたが、いかがだったでしょうか。

まだまだ情報セキュリティに対して、「投資していない」「必要性を感じない」と考える中小企業が多いのは統計から見ても明らかです。
しかし、大きな費用をかけることなく、まずは「できるところから始める」ことを意識し、アクションを起こすことが重要です。

まずはスモールステップで構わないので、情報セキュリティ５か条を足掛かりに情報セキュリティ対策に取り組みましょう。
その姿勢が企業の持続可能な発展を支える鍵となると考えます。

５． 取り組む際の参考資料

ここまでの解説で取り上げたガイドラインでは、「できるところから始める」の解説に加えて、具体的にはどのように取り組んだら良いのか、さらに進めるためにはどうしたら良いのかなど発展的な取り組み方法について紹介しています。
ぜひ、理解を深めたい、次のステップに進みたいと思った際の参考にしてください。

1.中小企業の情報セキュリティ対策ガイドライン(IPA)
2.付録１：情報セキュリティ５か条（IPA）
3.「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」報告書（IPA）
4.「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」事例集（IPA）
5.SECURITY ACTION（IPA）

レベル２_#16_中小企業におけるセキュリティ脅威への対策強化　～情報セキュリティ対策の進め方『組織的な取り組みを開始しよう』～
掲載日：2025/1/22



中小企業において、情報セキュリティの脅威はますます無視できない問題となっています。
独立行政法人情報処理推進機構（IPA）が発行している「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」の「第２部実践編」では、具体的な対策方法と中小企業の経営者やシステム担当者がこれにどう取り組むべきかを詳しく解説しています。

情報セキュリティ対策に組織全体で取り組むには、実行すべき対策を決めて、従業員に周知する必要があります。
しかし、こうした作業を行うには情報セキュリティに関する知識や経験が必要となるため、それらの知識や経験に長けた人材がいないと対策が進まなくなることも考えられます。

このような背景から、IPA のガイドラインでは規模の小さな企業や、これまで十分な情報セキュリティ対策を実施してこなかった企業などを対象に、すぐに取り組める対策を示し、段階的に発展させていく計画を紹介しています。この「すぐに取り組める対策」が、多くの企業にとって無理なく、自社の状況に応じた対策を開始する道筋となります。

今回は、『組織的な取り組みを開始しよう』と題し、すぐに始められる情報セキュリティ対策に焦点を当てて進めていきます。

１．情報セキュリティに対する中小企業の現状

IPA が作成した、「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」報告書によ

ると、情報セキュリティに関する組織体制について、「組織的には行っていない（各自の対応）」と回答した企業の割合が、規模が小さい企業ほど多く見られました。
小規模企業者では 56.2%、100 人以下の中小企業では 42.7%、101 人以上の中小企業では 19.7%が、情報セキュリティ対策を組織的に行っていないと回答しています。
つまり、100 人以下の中小企業・小規模企業者の約半数が「組織的に行わず、各自に任せている」状況にあると言えます。

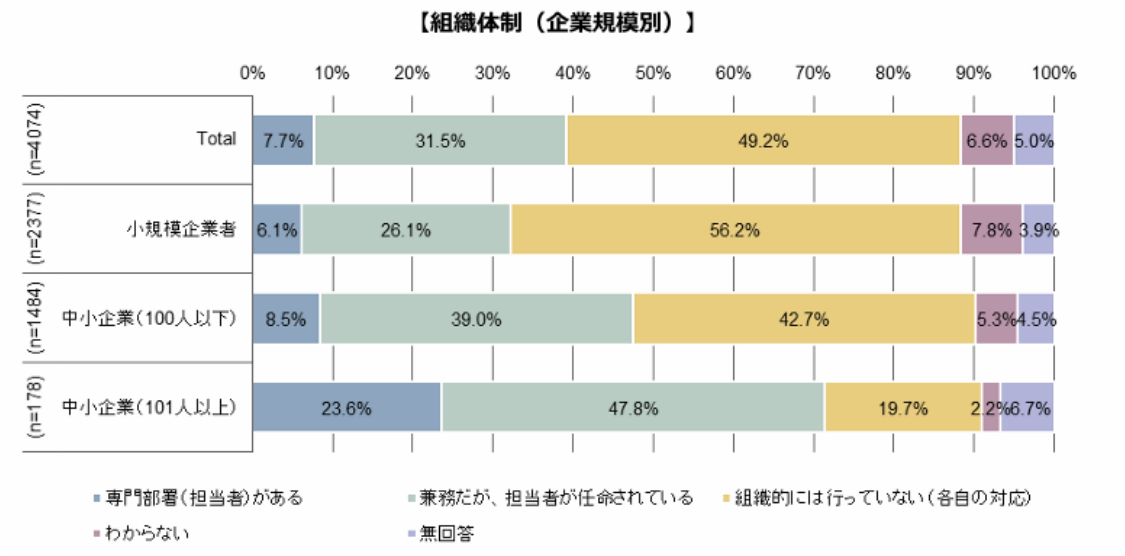


図１．情報セキュリティに係る組織体制(企業規模別)
(引用：「2021 年度 中小企業における情報セキュリティ対策に関する実態調査」報告書)

「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」の「第 1 部経営者編」では、情報セキュリティ対策は経営者こそが中心的な役割を果たすべきだと示されており、リーダーシップを発揮して推進することが求められています。
これは、情報セキュリティ対策を従業員「各自に任せる」のではなく、「組織的に実施すること」を求めていると言えます。

２．組織的な取り組みを開始する

次に、具体的に「組織的な取り組み」をどのように進めるかについて見ていきましょう。

（１）情報セキュリティ基本方針の作成意義

情報セキュリティ対策を組織に浸透させるためには、経営者主導のもとで情報セキュリティに関する基本

方針を定めることが重要です。そして、この基本方針を、従業員や関係者に効果的に伝えるためには、簡潔な文書で表現しましょう。
基本方針には決まった書式や形式はありませんが、IPA が提供している「情報セキュリティ基本方針（サンプル）」（付録２）などを参考にするとよいでしょう。
自社の事業の特徴や顧客のニーズを踏まえて、経営者と連携しつつ、自社に適した基本方針を作成することが大切です。

また、策定した基本方針は従業員に対するセキュリティ行動指針としてだけではなく、関係者に対して自社のセキュリティへの取り組み姿勢を表明するものでもあります。
作成した文書は、従業員や顧客などの関係者に周知し、透明性のある取り組みを積極的にアピールすることが望まれます。

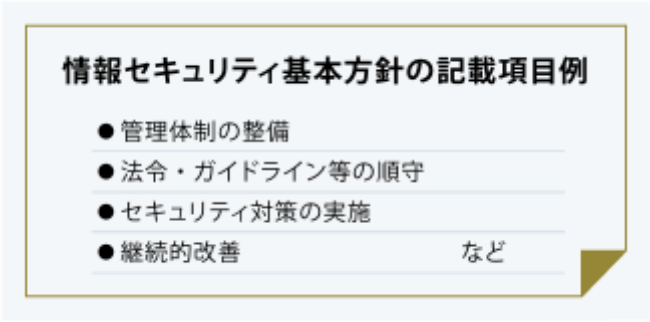


図２．情報セキュリティ基本方針例
（引用：中小企業の情報セキュリティ対策ガイドライン）

（２）自社のセキュリティ状況の把握

「５分でできる！情報セキュリティ自社診断」（付録３）を利用して、情報セキュリティ対策が現状でどの程度実施されているか把握することができます。
自社診断は、下記の表（図 3）に示されている 25 項目の設問に答えるだけで、情報セキュリティ対策の実施状況を把握できるツールです。現状把握のために、積極的に活用しましょう。

具体的な使い方は以下のとおりです。

【手順１】経営者または情報システム担当や部門長など実施状況が分かる人が「５分でできる！情報セキュリティ自社診断」の診断編に記入します。
【手順２】事業所が複数ある、部署数が多いなど、一人で記入することが難しい場合には、事業所や部署ごとに記入し、責任者・担当者が集計します。
【手順３】実施状況が分からない場合は、各従業員に質問して、回答を総合して記入します。

【手順４】チェック欄の該当するもの１つに〇を付けて、「実施している…４点」「一部実施している…２点」「実施していない…０点」「わからない…－１点」で採点します。

【手順５】全項目の合計点で、組織全体のセキュリティ対策の実施状況と、回答が「わからない」になっている項目を把握します。

No		診断内容
基本的対策	1	パソコンやスマホなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？
	2	パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル※1 は最新の状態にしていますか？
	3	パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？
	4	重要情報※2 に対する適切なアクセス制限を行っていますか？
	5	新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？
従業員としての対策	6	電子メールの添付ファイルや本文中の URL リンクを介したウイルス感染に気をつけていますか？
	7	電子メールや FAX の宛先の送信ミスを防ぐ取り組みを実施していますか？
	8	重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか？
	9	無線 LAN を安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？
	10	インターネットを介したウイルス感染や SNS への書き込みなどのトラブルへの対策をしていますか？
	11	パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？
	12	紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫などに安全に保管していますか？
	13	重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？
	14	離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？
	15	関係者以外の事務所への立ち入りを制限していますか？
	16	退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていますか？
	17	事務所が無人になる時の施錠忘れ対策を実施していますか？
	18	重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにしていますか？
組織としての対策	19	従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか？
	20	従業員にセキュリティに関する教育や注意喚起を行っていますか？
	21	個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？
	22	重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？
	23	クラウドサービスやウェブサイトの運用などで利用する外部サービスは、安全・信頼性を把握して選定していますか？
	24	セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか？
	25	情報セキュリティ対策（上記１～24 など）をルール化し、従業員に明示していますか？

図３．自社診断のための２５項目

（引用：5 分でできる！情報セキュリティ自社診断）

（３）対策の決定と周知

診断結果をもとに、自社で実行すべき情報セキュリティ対策を検討しましょう。その際、参考資料として「５分でできる！情報セキュリティ自社診断」の解説編を利用することで、簡単かつ効率的に対策を検討できます。
この資料には、コストを抑えつつ効果が期待できる具体的な対策例が示されているため、診断結果に基づき、自社に適した施策を検討する手助けとなります。

具体的な使い方は以下のとおりです。

・対策の検討と決定は、責任者・担当者と経営者が行います。
・診断項目ごとに対策を実施しない場合に考えられる被害・事故や、防止するための対策例が示されているので、参考にして検討します。
・検討する際には従業員の意見を聞き、職場環境や業務に適した対策を決定します。

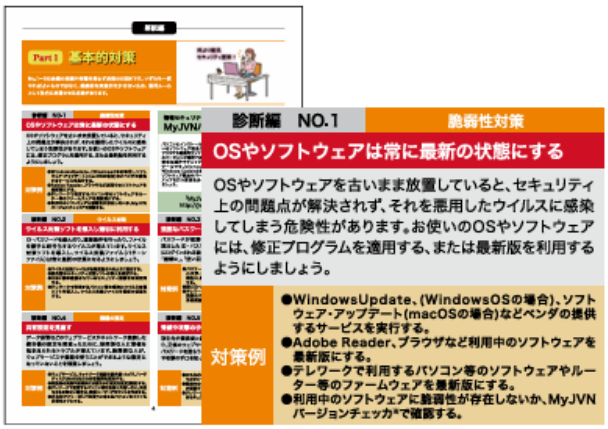


図４.「５分でできる！情報セキュリティ自社診断」解説編
（引用：５分でできる！情報セキュリティ自社診断）

（４）情報セキュリティハンドブックの作成と周知

対策が決定した後、その内容を従業員一人ひとりが実践できる形で定めた「情報セキュリティハンドブック」を作成し、周知します。
このハンドブックの作成には「情報セキュリティハンドブック（ひな形）」（付録４）を活用します。情報セキュリティハンドブック（ひな形）は、「５分でできる！情報セキュリティ自社診断」の対策例と連動しており、具体的な対策が明確化されています。

作成したハンドブックは単なる資料として従業員に配布するにとどまらず、必要に応じて説明会を実施しましょう。従業員が内容を十分に理解し、日常業務に反映できるよう徹底します。

作成方法と運用の流れは以下のとおりです。

・情報セキュリティハンドブックは、責任者・担当者が作成します。
・ひな形に記載された例文を編集して、決定した対策を社内ルールとして明文化します。
（図 5.情報セキュリティハンドブック（ひな形）のカスタマイズ例を参照）
・完成した情報セキュリティハンドブックを全従業員に配付し、必要に応じて説明する機会を設けるなどして、情報セキュリティ対策を徹底します。

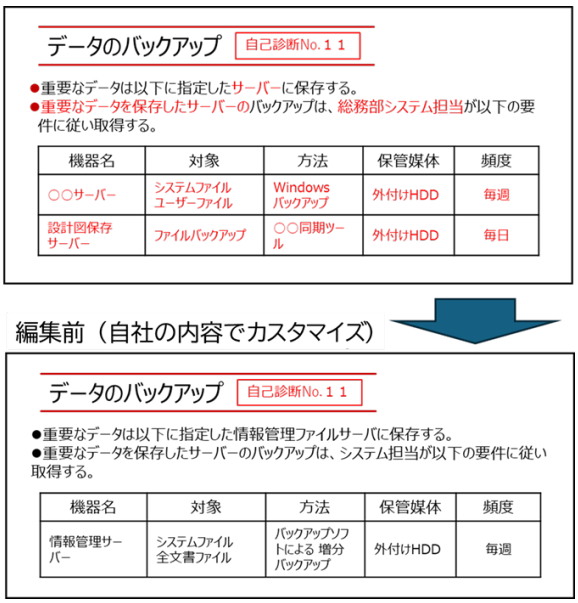


図 5. 情報セキュリティハンドブック（ひな形）のカスタマイズ例
（参考：情報セキュリティハンドブック（ひな形））

３． 組織的な取り組みを開始した企業の事例

【事例１：社内体制の構築と情報セキュリティ対策を実施】
当社は愛媛県で生活関連サービス業を営んでおり、従業員数は５０名以下の企業です。
主な顧客は個人であり、企業間取引は少数派です。
会社としては、「情報セキュリティ対策は当然実施すべきである」という認識のもと、IT 業者の意見を参考にしながら対策を進めています。
情報セキュリティを専門とする担当者は不在ですが、兼務の担当者を任命し、担当者主導による対策を進めています。

また、情報セキュリティ対策を業者任せにせず、社内体制や報告体制の構築にも力を入れています。
たとえば、緊急時の報告体制として、経営者、責任者、関係先、業界団体も含め、報告ルートを細かく内規で定めています。
情報セキュリティ上の被害にあったことが疑われる場合には、情報セキュリティ以外の有事の際の報告ルートと同様の報告を行うよう、従業員には求めています。
引用：IPA：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―事例集―より一部抜粋

４． SECURITY ACTION「★★二つ星」取得のすすめ

「SECURITY ACTION」は、中小企業が自主的に情報セキュリティ対策に取り組む姿勢を自己宣言する制度です。安全・安心な IT 社会を実現するために創設されました。

「★★二つ星」を宣言するためには、いくつかのプロセスを経る必要があります。
まずは、「中小企業の情報セキュリティ対策ガイドライン」に付属している、付録 3「5 分でできる！情報セキュリティ自社診断」を活用し、自社のセキュリティ状況を評価します。
その後、同ガイドラインの付録 2「情報セキュリティ基本方針（サンプル）」を参考に自社の情報セキュリティ基本方針を策定します。
この基本方針は社内だけでなく外部にも公開する必要があります。外部への公開により、「組織的な取り組みを開始する」を実施したことの宣言になります。

外部公開の方法としては、自社ウェブサイトへの掲載や会社案内やパンフレットへの掲載などが選択できます。また、「★一つ星」宣言から「★★二つ星」へのステップアップだけではなく、準備が整えば「★★二つ星」からの宣言も可能です。
SECURITY ACTION 自己宣言の申込方法はこちらを参照してください。



図６.SECURITY ACTION「★★二つ星」ロゴマーク(サンプル)

５．最後に

ここまで「組織的な取り組みを開始する」ためのプロセスと、それを実行した証としての SECURITY ACTION「★★二つ星」についてご紹介いたしましたが、いかがだったでしょうか。

「情報セキュリティ対策を組織的に始めたいが、何から始めればよいかわからない」「具体的な手段が分からない」とお考えの中小企業が多いのは統計からみても明らかです。

この「SECURITY ACTION」の自己宣言プロセスは決して難しくありません。
初めて取り組む企業でも詳細な手順を IPA の公式サイトで確認できるので、情報セキュリティの取り組みを加速させたい中小企業にとって有益な第一歩となるでしょう。

まずはこのような取り組みを組織的に開始することが、自社の安全性確保と信頼性向上に繋がり、企業の持続可能な発展を支える鍵となると考えます。
今回の内容が実践への第一歩を踏み出す手助けとなることを願っています。

６．取り組む際の参考資料

ここまでの解説で取り上げたガイドラインでは、「組織的な取り組みを開始する」の解説に加えて、具体的にはどのように取り組んだら良いのか、さらに進めるためにはどうしたら良いのかなど発展的な取り組み方法について紹介しています。

ぜひ、理解を深めたい、次のステップに進みたいと思った際の参考にしてください。

１．中小企業の情報セキュリティ対策ガイドライン(IPA)
２．付録１：情報セキュリティ５か条（IPA）
３．付録２：情報セキュリティ基本方針（サンプル）(Word ファイル、IPA)
４．付録３：５分でできる！情報セキュリティ自社診断(IPA)
５．付録４：情報セキュリティハンドブック（ひな形）（PowerPoint ファイル、IPA）
６．「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」報告書（IPA）
７．「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」事例集（IPA）
８．SECURITY ACTION（IPA）

レベル 2_#17_中小企業におけるセキュリティ脅威への対策強化　～情報セキュリティ対策の進め方『本格的に取り組もう（1/3）』～
掲載日：2025/1/29



独立行政法人情報処理推進機構（IPA）が発行している「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」の「第 2 部実践編」では、具体的な対策方法と中小企業の経営者やシステム担当者がこれにどう取り組むべきかを詳しく解説しています。

情報セキュリティ対策に組織全体で取り組むには、実行すべき対策を決めて、従業員に周知する必要があります。しかし、こうした作業を行うには情報セキュリティに関する知識や経験が必要となるため、それらの知識や経験に長けた人材がいないと対策が進まなくなることも考えられます。

このような背景から、IPA のガイドラインでは規模の小さな企業や、これまで十分な情報セキュリティ対策を実施してこなかった企業などを対象に、すぐに取り組める対策を示し、段階的に発展させていく計画を紹介しています。この「すぐに取り組める対策」が、多くの企業にとって無理なく、自社の状況に応じた対策を開始する道筋となります。

今回は、『本格的に取り組みをはじめよう』というテーマで、3 回に分けて具体的な取り組みの方法をご紹介します。1 回目となる今回は、管理体制の構築、デジタルトランスフォーメーション（DX）、そしてセキュリティ対策費用の予算化の重要性に焦点を当てます。

１．情報セキュリティに対する中小企業の現状

前回の記事でも紹介しましたが、IPA が作成した、「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」報告書によると、情報セキュリティに関する管理体制を構築していない企業は規

模が小さいほど多い傾向にあります。

具体的には、「組織的に対応していない」企業の割合は、小規模企業者で 56.2%、100 人以下の中小企業では 42.7%、101 人以上の中小企業では 19.7%となっています。
つまり、100 人以下の中小企業の約半数は「組織的に行っておらず各自の対応に任せている」状況です。

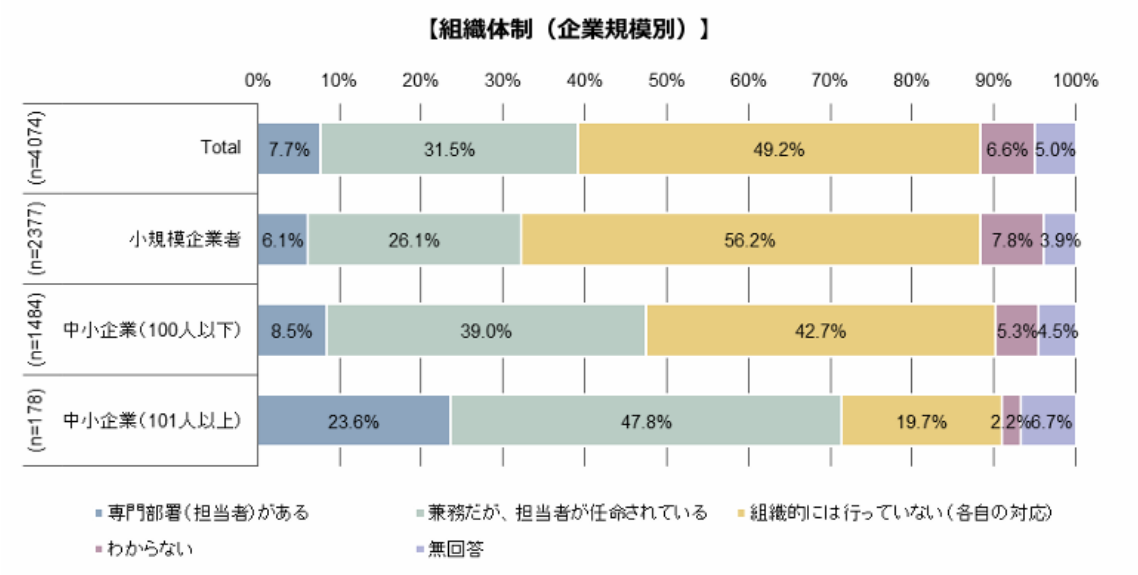


図１．情報セキュリティに係る組織体制(企業規模別)
（引用：「2021 年度 中小企業における情報セキュリティ対策に関する実態調査」報告書）

同じ報告書では、デジタルトランスフォーメーション（DX）の推進と情報セキュリティの予算化の実施状況も報告されています。
直近過去３期の IT 投資額について最も多かった回答は「１百万円未満」で、全体の 37.８%を占めました。次に「投資していない」が 30.0%、「１百万円から５百万円未満」が 17.5%という結果になっています。

さらに、情報セキュリティ対策のデータでも、投資額が「１百万円未満」の企業が全体の 49.2%でトップとなり、次に「投資していない」が 33.1%と相当数存在しています。これに対し、「１百万円から５百万円未満」と回答した企業はわずか 8.2%に留まっています。
この結果から、全体の約７割の企業が IT 分野における投資を 100 万円未満で行い、情報セキュリティへの投資割合はさらに低く、約 8 割の企業が 100 万円未満の投資額に留めていることが分かります。

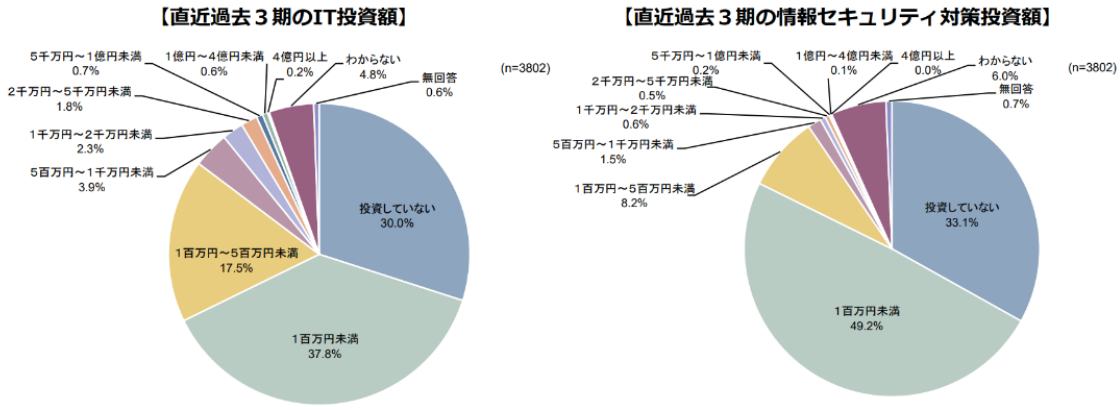


図２．被害防止のための組織面・運用面での対策

（引用：「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」報告書）

現在、多くの企業で投資額が低い傾向にあります。これは、デジタルトランスフォーメーション（DX）の推進や情報セキュリティ対策の取り組みに課題があることを示唆しています。

２．本格的に取り組みを開始する

自社に適した対策を実行して効果をあげるには、まず、自社が抱える情報セキュリティ上のリスク（事故が発生したとき経営や事業に深刻な損害をもたらす危険性を指します。以下、「リスク」と記載。）を明確に把握することが重要です。

このプロセスでは、経営者が懸念する情報セキュリティ上の重大事故や業務停止などのリスクを洗い出し、それに基づき自社にとって最大の損失を招く可能性がある事故を未然に防ぐための対策を検討します。

具体的な対策内容を整理し、詳細に書面化することで全社的に共有できる明確な基盤を構築します。

この書面化した対策を「規定」と呼びます。

３．管理体制の構築

それでは具体的に「管理体制の構築」について見ていきたいと思います。

（１）責任分担と連絡体制の整備

前回取り上げた「組織的な取り組みを開始しよう」において策定・共有された情報セキュリティ基本方針を具体的に実現するために、情報セキュリティ対策を推進する管理体制を決めます（表１）。

情報セキュリティ責任者を中心に、各部門の責任者を通じて、全従業員への情報が的確に伝達される経路を確立しましょう。また、万が一セキュリティ事故や問題が発生した場合には、発生時の状況が迅速に情報セキュリティ責任者に報告されるよう、連絡フローを整えることが重要です。
すでに個人情報保護管理体制（例えば、特定個人情報の事務取扱担当者や苦情対応窓口）などが決まっている場合は、それら既存の管理体制との整合を図りましょう。

役職名	役割と責任
情報セキュリティ責任者	情報セキュリティに関する責任者です。情報セキュリティ対策などの決定権限を有するとともに、全責任を負います。
情報セキュリティ部門責任者	各部門における情報セキュリティの運用管理責任者です。各部門における情報セキュリティ対策の実施などの責任と権限を有します。
システム管理者	社内の情報システムに必要な情報セキュリティ対策の検討・導入を行います。
教育責任者	情報セキュリティ対策を推進するために従業員への教育を企画・実施します。
点検責任者	情報セキュリティ対策が適切に実施されているか点検します。

表 1．情報セキュリティ管理のための役割と責任分担例
（引用：中小企業の情報セキュリティ対策ガイドライン）

なお、上記の情報セキュリティ責任者やシステム管理者がそれぞれの役割を果たすためには、情報セキュリティに関する知識や経験が必要です。
こうした知識の習得や経験は一朝一夕では難しいため、中長期の視点を持ちながら、人材育成を計画的に進めていくことを考えましょう。

また、小規模な企業においては、表 1 の例に忠実である必要はなく、組織の規模や事情に応じた現実的な体制（役割分担）を独自に設計することも大切です。
例えば、経営者自らが情報セキュリティ責任者を兼務することや、防犯や防火などの安全管理責任者を置かれている場合には、この責任者が情報セキュリティ責任者を兼ねることもあります。
しかし、特定の人物一人が情報セキュリティ対策の全てを担う体制は望ましいものではありません。その人物が不在になった場合や、業務負担が大きすぎる場合に問題が生じる可能性が高まります。
そのため、特に情報セキュリティ責任者と点検責任者（監査責任者）は、兼務しないようにしましょう。

この観点から、最低でも 2 名以上のメンバーによる組織体制が必要と考えられ、実務を担うシステム管理者を加えた 3 名体制が、一般的な最小限の構成人数といえます。複数人で役割と責任を分担することで、業務を効率的に分散させるとともに、確かな管理体制を整備することが可能になります。

（２）緊急時対応体制の整備

事業や顧客に重大な影響を及ぼすインシデントが発生した際、速やかに適切な対応を取るためには、事前に明確な体制を決めておくことが不可欠です（表２）。

対応を誤ったり、遅れてしまうと、被害が予想以上に拡大し、復旧が難航するなど、深刻な事態を招く可能性があります。
そうならないためには、危機管理の観点から、誰が何を行うのか、その役割や具体的な手順を明確に決めておく必要があります。

さらに、組織内外の緊急連絡先や伝達ルートを整備し、あらかじめ周知しておくことも重要です。加えて、緊急時の対応を想定した訓練やシミュレーションを定期的に実施し、実際に決めたとおりに対応できるのか確認します。

また、関係者や IT 製品のメーカー、保守ベンダー等への連絡先をまとめておくことも欠かせません。
業務システムの障害が発生した際には、メールや連絡先を確認するためのウェブ閲覧もできなくなる可能性があるため、連絡方法について代替手段も確認しておきましょう。

役職名	役割と責任
情報セキュリティ責任者 （例：代表取締役）	事故の影響を判断し、対応について意思決定します。
情報セキュリティ部門責任者 （例：管理部長、営業部長）	・事故の原因を調べて情報セキュリティ責任者に報告します。 ・情報セキュリティ責任者の判断・意思決定に基づき適切な処置を行います。 ・事故の原因や被害が情報システムに関係する場合はシステム管理者と連携して適切な処置を行います。
システム管理者 （例：管理部長兼務）	事故の原因や被害が情報システムに関係する場合は情報セキュリティ部門責任者と連携して適切な処置を行います。
事故・異常を発見した従業員	事故や異常の内容を情報セキュリティ部門責任者に報告します。

表２．緊急時対応対策の役割と責任
（引用：中小企業の情報セキュリティ対策ガイドライン）

４． DX の推進と情報セキュリティの予算化

デジタルトランスフォーメーション（DX）の推進

近年のビジネス環境において、中小企業であっても競争力維持・強化のために、デジタルトランスフォーメーション（DX※）を進めていくことが求められています。

※DX（Digital Transformation）企業がビジネス環境の激しい変化に対応し、データとデジタル技術を活用して、顧客や社会のニーズを基に、製品やサービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、競争上の優位性を確立すること。

DXを推進する過程では、クラウドサービスなどデジタル技術やインターネットの活用が多様化する一方で、それに伴うセキュリティリスクも複雑化しています。
それらのリスクに適切に対応するため、セキュリティ管理の充実が最優先事項です。より有効なセキュリティ対策のために、自社の情報システムやネットワーク構造を可視化して対策を検討するとともに、予算を確保する必要があります。

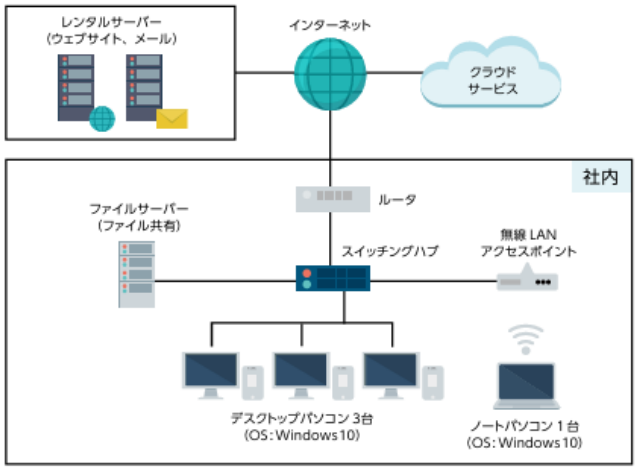


図３．情報システムとインターネットとの接続状況の図
引用：中小企業の情報セキュリティ対策ガイドライン

情報セキュリティの予算化

情報セキュリティに関わる予算の確保は、企業経営の中でしばしば難題となりがちです。
その理由は主に、情報セキュリティへの投資は企業の売上や利益に直結しないため、経営層にその投資対効果が見えづらい点にあります。そのため、セキュリティ予算を上申する際に、どのように説明すべきかを悩んでいる担当者が多いのも事実です。
その原因としては、次のようなことが挙げられます。

（１）経営者が、セキュリティ投資を「利益を生み出すもの」ではなく、単なる「コスト（費用）」と捉えている
（２）セキュリティ関連の用語や概念が難解で、具体的なリスクやインパクトが理解されづらい
（３）自社のセキュリティリスクが顕著化していない

このように、経営層の理解が不足しているとセキュリティ対策の重要性を説明することが困難です。
このような課題を克服し、情報セキュリティ予算の必要性をしっかりと伝えるためには、「5 分でできる！情報セキュリティ自社診断」などのツールを活用し、セキュリティリスクマネジメントの重要性を強調することが有効です。
費用ではなく、リスクが発生することにより売り上げや利益が減少したり、社会的信用が失墜したりすることを防ぐために必要な投資であることを認識してもらうことが重要です。

５．最後に

ここまで「管理体制の構築」と「デジタルトランスフォーメーション（DX）の推進」「情報セキュリティの予算化」の重要性について紹介いたしましたが、いかがだったでしょうか。
管理体制の構築というと大げさな感じがしますが、最低限の体制として、管理者と点検者、さらに実務者（システム管理者）の 3 名が揃っていれば、適切な体制を構築することが可能です。もちろん定期的な見直しは必要ですが、組織体制を整え、積極的に IT 投資を始めることが、企業の持続的成長と発展に不可欠です。これらの取り組みは、単なるコストではなく、企業を守り、競争力を高めるための重要な投資であることを認識してください。
また、DX が売上や利益を拡大するための投資であるのと同様に、情報セキュリティもまた企業の事業継続、さらには社会的信用を守るための投資であることもおわかりいただけたかと思います。
まずは、組織的な体制作りと積極的な IT 投資を開始することが、企業の持続的な成長と発展を支える鍵となると考えます。

６．取り組む際の参考資料

ここまでの解説で取り上げたガイドラインでは、「本格的に取り組む」方法に加え、具体的にどのように取り組むべきか、さらに進めるためにはどうしたら良いのかなど発展的な取り組み方法について紹介しています。

ぜひ、理解を深めたい、次のステップに進みたいと思った際の参考にしてください。

１．中小企業の情報セキュリティ対策ガイドライン（IPA）
２．付録 3：5 分でできる！情報セキュリティ自社診断（IPA）
３．付録４：情報セキュリティハンドブック（ひな形）（IPA）
４．「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」報告書（IPA）

レベル２_#18_中小企業におけるセキュリティ脅威への対策強化　～情報セキュリティ対策の進め方『本格的に取り組もう（2/3）』～
掲載日：2025/2/5



独立行政法人情報処理推進機構（IPA）が発行している「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」の「第２部実践編」では、具体的な対策方法と中小企業の経営者やシステム担当者がこれにどう取り組むべきかを詳しく解説しています。

情報セキュリティ対策に組織全体で取り組むには、実行すべき対策を決めて、従業員に周知する必要があります。
しかし、こうした作業を行うには情報セキュリティに関する知識や経験が必要となるため、それらの知識や経験に長けた人材がいないと対策が進まなくなることも考えられます。

このような背景から、IPA のガイドラインでは規模の小さな企業や、これまで十分な情報セキュリティ対策を実施してこなかった企業などを対象に、すぐに取り組める対策を示し、段階的に発展させていく計画を紹介しています。この「すぐに取り組める対策」が、多くの企業にとって無理なく、自社の状況に応じた対策を開始する道筋となります。

前回から『本格的に取り組みをはじめよう』というテーマで、３回に分けて具体的な取り組み方法をご紹介しています。２回目となる今回は、情報セキュリティ規程に焦点を当て進めていきます。

１．情報セキュリティに対する中小企業の現状

近年、企業や組織を狙ったサイバー攻撃は、頻度や規模を増し日常的に発生する社会的な脅威となっています。最近では、情報セキュリティ対策が強固な大企業ではなく、同一のサプライチェーンを構成する中小企業などの取引先を経由して、攻撃が行われる事例も報じられています。
特に中小企業の場合、セキュリティ対応の不備を悪用され、取引先の機密情報の漏えいや攻撃者が次なる標的へと進むための「踏み台」とされる危険性があります。中小企業は、次の攻撃の足掛かりにされる可能性があることを念頭に置き、適切な情報セキュリティ対策を実施することが重要です。

IPA が作成した、「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」報告書では、中小企業の情報管理に関する実態が浮き彫りになりました。
報告書によると、被害防止のための組織面・運用面の対策のうち、「セキュリティポリシー（セキュリティの規程やルール）が文章化されている」企業は、前回調査の 14.6%に対し、今回 13.5%とわずかに減少していることがわかります。
つまり、中小企業の約 15%弱しか情報セキュリティ規程を文書化していないということです。

セキュリティポリシーは、企業の情報資産を守るために定められたルールやガイドラインです。この規程がなければ、情報を安全に保護し、従業員が安心して情報を取り扱う環境を整えることができません。
セキュリティポリシーを欠いたまま情報セキュリティ対策を進めると、全体的な安全性に欠ける場当たり的な対応に陥る可能性があります。

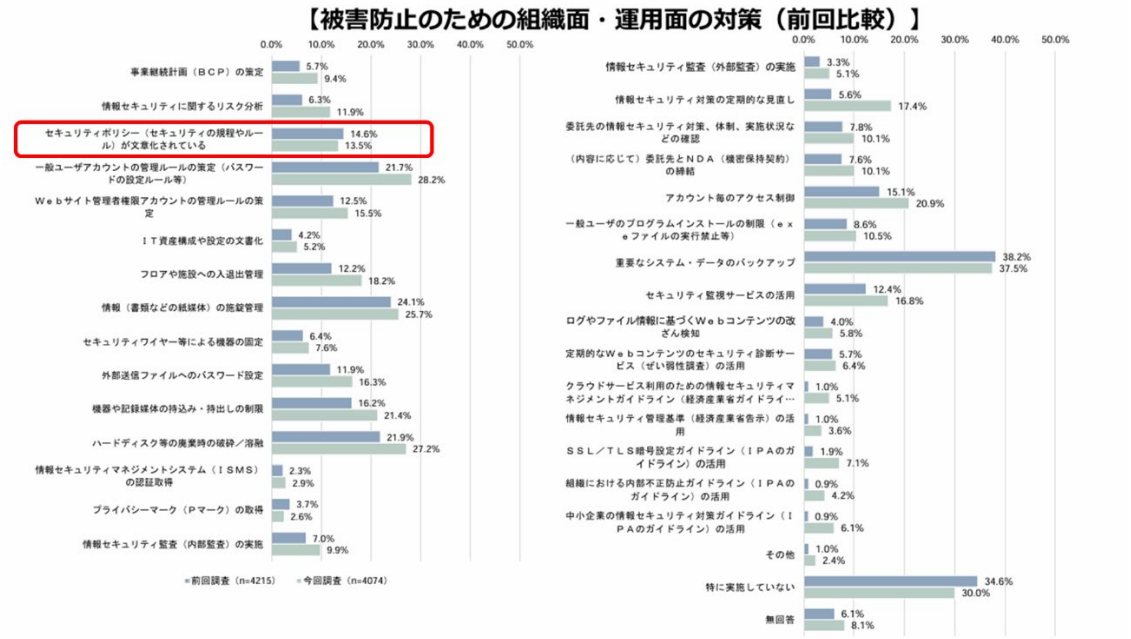


図１．被害防止のための組織面・運用面の対策(前回比較)
(引用：「2021 年度 中小企業における情報セキュリティ対策に関する実態調査」報告書)

中小企業がサイバー攻撃の被害を最小限に抑え、さらに安心してビジネス活動を推進するためには、技術的なセキュリティツールの導入以上に、組織の基盤となるルールづくりやガイドラインの整備を進めることが求められます。

２．情報セキュリティ規程の作成

企業が直面するリスクは、その事業内容をはじめ、扱う情報の種類や職場環境、IT インフラの利用状況などによって大きく異なります。汎用的な規程をそのまま使用しても、自社の特性やニーズに適さないことが考えられます。ここでは、自社に適した情報セキュリティ規程を効果的に作成するためのポイントを紹介します。

（１）リスクの洗い出し

まず、情報セキュリティ上のリスクを特定することが必要です。
経営者が懸念する重大なセキュリティ事故を念頭に置きつつ検討を進めます。この時、以下のような状況を併せて考えることで、対応すべきリスクを把握します。

・外部要因

関連する業務や情報に係る法律や規制、情報セキュリティ事故の傾向、取引先からの情報セキュリティに関する要求事項など

・内部要因

自社の経営方針や情報セキュリティ方針、管理体制、現行の情報システムの利用状況など



（引用：中小企業の情報セキュリティ対策ガイドライン）

（２）優先的に対応するリスクと対策の決定

全てのリスクに対応しようとすると、高額な費用が必要となったり、業務の非効率化につながるおそれがあります。

そのため、いつ事故が起きてもおかしくない、あるいは事故が起きると大きな被害になるなど、影響が甚大なリスクを優先して対策を実施します。

逆に事故の発生確率が低い、または発生しても被害が軽微なものについては、現状のままにするなど、合理的に対応します。



（引用：中小企業の情報セキュリティ対策ガイドライン）

（３）実践的な規程の作成プロセス

「優先的に対応するリスクと対策の決定」で決めた対策内容を文書化した規程を作成します。
経験が不足している場合、一から作成するのは難しいかもしれません。そのため、中小企業の情報セキュリティ対策ガイドラインに掲載されている「付録 ５：情報セキュリティ関連規程（サンプル）」（概要は表１）を活用すると良いでしょう。このサンプルを参考に、自社に適した規程にするために修正を加えれば、効率的に規程を完成させることが可能です。

・サンプル使用時のポイント
　サンプル文中の赤字や青字で記載された箇所を自社の実情に即した表現や内容に書き換えることで規定を完成できます。
　サンプルに明記されていなくても必要な対策や有効な対策があれば、追記します。

	名　称	概　要
1	組織的対策	情報セキュリティのための管理体制の構築や点検、情報共有などのルールを定めます。
2	人的対策	取締役及び従業員の責務や教育、人材育成などのルールを定めます。
3	情報資産管理	情報資産の管理や持ち出し方法、バックアップ、破棄などのルールを定めます。
4	アクセス制御及び認証	情報資産に対するアクセス制御方針や認証のルールを定めます。
5	物理的対策	セキュリティを保つべきオフィス、部屋及び施設などの領域設定や領域内での注意事項などのルールを定めます。
6	IT 機器利用	IT 機器やソフトウェアの利用などのルールを定めます。
7	IT 基盤運用管理	サーバーやネットワーク等の IT インフラに関するルールを定めます。
8	システム開発及び保守	独自に開発及び保守を行う情報システムに関するルールを定めます。
9	委託管理	業務委託にあたっての選定や契約、評価のルールを定めます。委託先チェックリストのサンプルが付属します。
10	情報セキュリティインシデント対応ならびに事業継続管理	情報セキュリティに関する事故対応や事業継続管理などのルールを定めます。
11	テレワークにおける対策	テレワークのセキュリティ対策についてルールを定めます。

表 1．情報セキュリティ関連規程(サンプル)の概要
（引用：中小企業の情報セキュリティ対策ガイドライン）

さらに、情報セキュリティ対策は以下の 3 つのカテゴリに分類することで整理しやすくなります。

【人的対策】
従業員教育やガイドライン・規程など「人」に係る対策

サンプル例では、「組織的対策」「人的対策」「情報資産管理」「アクセス制御及び認証」「委託管理」「テレワークにおける対策」「情報セキュリティインシデント対応ならびに事業継続性管理」が該当します。

【物理的対策】

IT 機器や施設など、主に情報を管理している実体があるもの(PC や設備など)に係る対策

サンプル例では、「物理的対策」「IT 機器利用」「IT 基盤運用管理」が該当します。

【技術的対策】

プログラム(セキュリティソフトなど)やネットワーク(ネットワーク監視など)に係る技術的な対策

サンプル例では、「IT 機器利用」「IT 基盤運用管理」「システム開発及び保守」が該当します。

これらの観点を組み合わせることで、自社に最適な情報セキュリティ規程を策定し、実際の運用面で有効性を発揮することが期待されます。

ここまで「本格的に取り組む」の「情報セキュリティ規程」についてご紹介いたしましたが、いかがだったでしょうか。
規程の作成は一見すると複雑で、ハードルが高いと感じるかもしれません。
しかし、まずは初めの一歩としてサンプルを参考にしながら自社の状況に合わせてカスタマイズすることで、スムーズに進めることができるでしょう。

情報セキュリティ規程は、いわばセキュリティ対策の「バイブル」です。この規程が欠けていると、個々のセキュリティ対策が一貫性を欠いた場当たり的なものになってしまう可能性が高いため、非常に重要です。

また、この規程は単に文章として存在するだけではなく、情報セキュリティ担当者が社内の意識向上を図るための説明をする際の根拠にもなります。
規程を用いることで「なぜこの対策が必要なのか」説得力を持って説明することができ、社内全体のセキュリティ意識の統一を目指す一助となるでしょう。

まずは、脅威への基本的な考え方を整理し、それを文書化して定めることが必要不可欠です。この取り組みは単なるセキュリティ対策だけではなく、長期的には企業の信頼性や競争力を強化し、持続的な企業活動を支える基盤になると考えます。

３．取り組む際の参考資料

ここまでの解説で取り上げたガイドラインでは、「本格的に取り組む」方法に加え、具体的にどのように取り組むべきか、さらに進めるためにはどうしたら良いのかなど発展的な取り組み方法について紹介しています。

ぜひ、理解を深めたい、次のステップに進みたいと思った際の参考にしてください。

1．中小企業の情報セキュリティ対策ガイドライン（IPA）
2．付録 5：情報セキュリティ関連規程（サンプル）（IPA）
3．「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」報告書（IPA）

レベル２_＃19_中小企業におけるセキュリティ脅威への対策強化　～情報セキュリティ対策の進め方『本格的に取り組もう（3/3）』

掲載日：2025/2/12



独立行政法人情報処理推進機構（IPA）が発行している「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」の「第２部実践編」では、具体的な対策方法と中小企業の経営者やシステム担当者がどう取り組むべきかを詳しく解説しています。

今回は、『本格的に取り組みをはじめよう』というテーマの３回シリーズの最終回をお届けします。この回では、「３.本格的に取り組む」の「（４）委託時の対策」と「（５）点検と改善」に焦点を当て、進めていきます。

１．委託時の対策

（１）委託と受託の関係

ビジネスを展開する企業において、全ての業務を自社で完結させることは現実的ではありません。そのため、

多くの企業は特定の業務を外部へ依頼する手段として「委託」を選択しています。
「委託」は、外注や委任、準委任、アウトソーシングなど、多様な形態を含み、他の企業や専門機関に特定の業務を行ってもらう手法です。
一方「受託」とは、他者からの依頼を受け、業務を引き受けることを指します。また、業務の成果物を確約する「請負」を意味することもあります。

どのような企業でも事業を円滑に進めるうえで、全ての業務を自社で行うことは難しいため、委託している業務があり、それを引き受ける受託企業があることでビジネスは成り立っています。また、業務を委託するときには、委託元と委託先との間で業務上必要な情報のやり取りが生じます。

製造業で、外部の工場に部品の製造を委託する場合は、詳細な設計図が、税理士に決算書の作成を委託する際には、売上伝票や出金伝票が提供され、運送会社に商品配送を委託する場合には、顧客の住所・氏名などの個人情報が授受されます。
こういったプロセスで、重要な情報や個人情報が委託先に提供されますが、もし委託先が適切なセキュリティ対策を講じていなければ、情報漏えいや改ざんなどのリスクが生じる恐れが高まります。
さらに、こうした事故が委託先で発生した場合であっても、委託元の管理責任が問われることもあります。
また、委託先がサイバー攻撃を受け、システム停止やウイルス感染が発生すると、受発注や製品出荷の停止を引き起こし、自社のビジネスに大きな影響を与える可能性があります。

近年、グローバル化やデジタル化が進んだ結果、委託や受託の関係が複雑化しています。
具体的には、部品の製造を受託した企業が、原材料を海外から調達し、部品加工をさらに他社に委託・再委託するケースや、完成部品の運送を別の配送業者に委託することなどが行われています。
このような調達や製造、販売などの一連の流れは「サプライチェーン」と呼ばれていますが、サプライチェーンの中で情報セキュリティ対策が不十分な企業があると、その企業がサイバー攻撃を受けることで、サプライチェーン内の他の企業にも影響を与える可能性があります。このため、業務を受託する側の中小企業であってもサプライチェーンを構成する一員であることを自覚し、情報セキュリティ対策に取組むことが求められています。

（２）委託や受託時の対策とその状況

近年、社内業務の一部または全てを外部に委託したり、レンタルサーバーやクラウドサービスなどの外部の IT サービスを利用することが一般的になっています。
重要な企業情報を外部に託したり、処理を依頼する場合には、委託先にも情報セキュリティ対策を実施してもらう必要があります。

IPA が作成した、「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」報告書(以降「実態調査」と略す)によると、販売先や仕入先からの情報セキュリティに関する条項・取引上の義務・要請に関して、「義務・要請はない」が 63.2%と高く、「義務・要請がある」の 26.1%を大きく上回っています。
これは、「自社のセキュリティが十分であれば問題ない」、あるいは「特に要求されていないので、情報セキュリティに特別な配慮は不要」といった誤った認識を招く原因となっています。

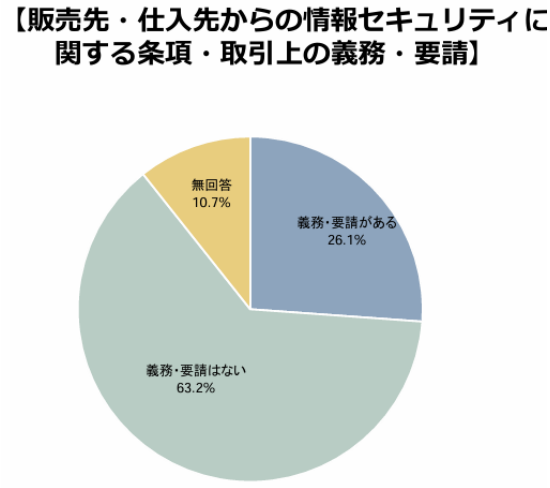


図 1　販売先・仕入先からの情報セキュリティに関する条項・取引上の義務・要請
(引用：「2021 年度 中小企業における情報セキュリティ対策に関する実態調査」報告書)

直接指示することが難しい外部委託先に情報セキュリティ対策を実施してもらうためには、取引契約の中であらかじめ具体的な対策を契約書や覚書などに盛り込むことが大切です。
もし、個別に契約や覚書を交わすことが難しい場合は、委託先のサービス規約や情報セキュリティに関わる対応方針を確認したうえで選定することが求められます。

実態調査によると、販売先(発注元企業)との契約時における情報セキュリティに関する要請について、「秘密保持」の割合が 93.8%と最も高く、次いで、「契約終了後の情報資産の扱い（返却、消去、廃棄等）」が 36.3%、「情報セキュリティに関する契約内容に違反した場合の措置」が 32.4%となっています。

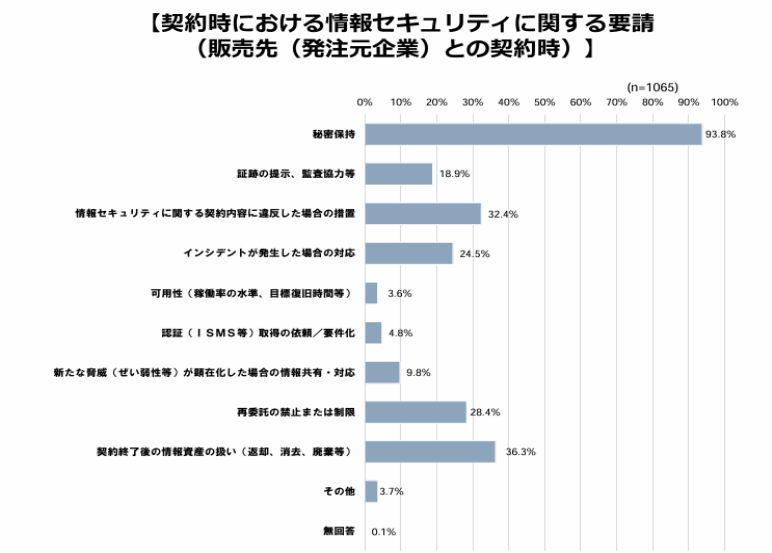


図２　販売先(発注元企業)との契約時における情報セキュリティに関する要請
(引用：「2021 年度　中小企業における情報セキュリティ対策に関する実態調査」報告書)

また、仕入先(委託・協力企業)との契約時における情報セキュリティの要請についても同じ傾向があります。
「秘密保持」が 94.0%でトップを占めており、次いで、「契約終了後の情報資産の扱い（返却、消去、廃棄等）（34.1%）」、「情報セキュリティに関する契約内容に違反した場合の措置（30.7%）」となっています。

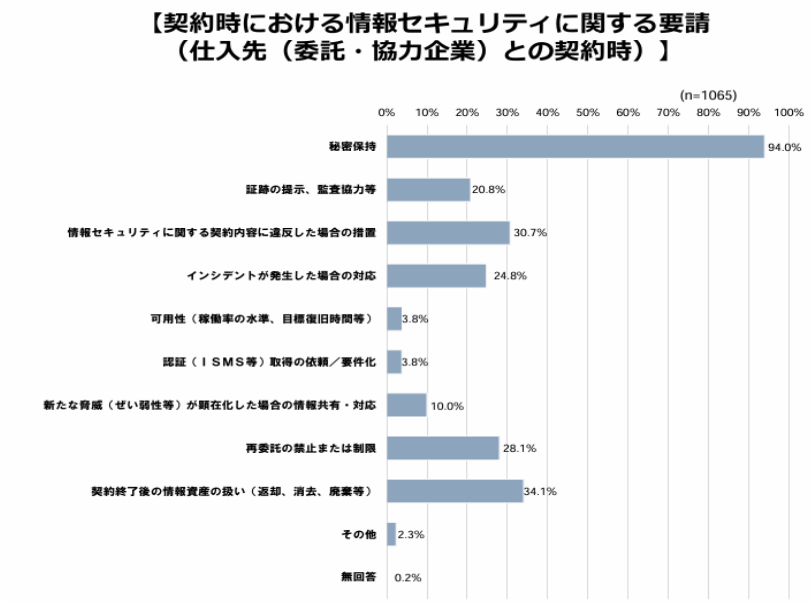


図３　仕入先（委託・協力企業）との契約時における情報セキュリティに関する要請
(引用：「2021 年度　中小企業における情報セキュリティ対策に関する実態調査」報告書)

これらのデータから、委託先・受託先との間での秘密情報の扱いに対する意識は高まっているものの、具体的な情報セキュリティ対策に関して意識しているのは企業の３割程度に過ぎないことがわかります。

（３）個人情報を取り扱う業務の委託や受託

個人情報保護法では、個人データ※の取り扱いを委託する場合は、委託先にも情報セキュリティ対策を実施してもらうように監督することが義務付けられています。
委託元は、委託先の状況を把握し、対策が確実に実施されるよう責任を持つ必要があります。

もし委託先の対策が不十分で事故が起きた場合、委託元は管理責任を問われ、委託先は委託元の信頼を失うことになります。
重要な情報や個人情報など、セキュリティ事故の影響が大きい情報を取り扱う場合は、委託元が委託先にセキュリティ対策の要望や期待をしっかりと伝え、受託側はそれをきちんと理解し、実行することが重要です。

これらを踏まえ、取り扱う情報の種類や委託する業務に適した情報セキュリティ対策を、委託先にも実施してもらいます。機密情報や個人情報を取り扱う際には、「情報セキュリティ関連規程（サンプル）」（付録５）の「9 委託管理」を参考にして、委託先と契約したり、委託先を選定してください。

さらに、情報セキュリティ対策が継続して実施されているか、新たな対策が必要になったときに対応しているかを随時確認し、委託先の情報セキュリティ対策を維持するよう責任を持って管理します。

※個人情報保護法では「個人情報」、「要配慮個人情報」、「個人情報データベース等」「個人データ」、「保有個人データ」、「個人関連情報」、「仮名加工情報」、「匿名加工情報」等の語を使い分けており、個人情報取扱事業者等に課される義務はそれぞれ異なるので、注意が必要です。

２． 点検と改善

情報セキュリティの点検とは、計画した情報セキュリティ対策が適切に実行されているか、見落としがないか、その対策がセキュリティ事故の防止に役立っているかを確認することです。

点検結果を経営者に報告し、経営者が意図するセキュリティ対策が実現できているかを確認し評価をすることが重要です。経営者の評価を得ることで、場合によってはリスクの特定に戻り、対策を見直すことで

取り組みの精度を高めることができます。

具体的な点検や改善の取組みについては、過去の記事「情報セキュリティの見直しと強化（監査と点検）(1/3)」に詳細が説明されているので、そちらも併せてご参照ください。

ここまで「３.本格的に取り組む」の「（４）委託時の対策」と「（５）点検と改善」についてご紹介いたしました。業務をスムーズに遂行する上で、受託と委託の関係が不可欠であること、そして、これらの関係性が生じる際には、情報セキュリティの重要性を考慮する必要があることを理解していただけたでしょうか。情報セキュリティへの取り組みを疎かにしないよう、定期的な点検と改善を行うことが重要であり、その取り組みが企業の持続可能な発展を支える鍵となります。

今回をもって、中小企業の情報セキュリティ対策ガイドラインの「第２部実践編」の解説は終了となります。今後も定期的に点検を行い、セキュリティ対策を強化していきましょう。

３．取り組む際の参考資料

ここまでの解説で取り上げたガイドラインでは、「本格的に取り組む」方法に加え、具体的にどのように取り組むべきか、さらに進めるためにはどうしたら良いのかなど発展的な取り組み方法について紹介しています。

ぜひ、理解を深めたい、次のステップに進みたいと思った際の参考にしてください。

１．中小企業の情報セキュリティ対策ガイドライン　（IPA）
２．付録５：情報セキュリティ関連規程（サンプル）（IPA）
３．「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」報告書（IPA）

レベル 2_#20_中小企業におけるセキュリティ脅威への対策強化　～よくある質問への回答～
掲載日：2025/2/19



これまで、独立行政法人情報処理推進機構（IPA）が発行する「情報セキュリティ１０大脅威 2024」や「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」を基に、中小企業の経営者やシステム担当者が行うべき情報セキュリティ対策について掘り下げてきました。
今回は、セミナーやメルマガのアンケートで寄せられた質問に焦点を当てて解説します。

・経営層に求められるリーダーシップの具体的アクションと社員教育の進め方 【組織・人的対策】
・情報資産の扱い方・管理方法 【技術的対策】

１． 経営層に求められるリーダーシップの具体的アクション

情報セキュリティにおいて最も重要な要素は、定着化であると言っても過言ではありません。とはいえ、この定着化の実現は、最も困難な要素でもあります。
経営層の方からよく聞く声として、次のようなものがあります。

・規程を作ったが、どう徹底させればよいかわからない
・現場が面倒くさがって、なかなか実行してくれない
・社員の IT リテラシーが低く、理解が進まない
・社内教育は実施しているが、浸透しない

これらを解決するためには、次の４つのアクションが重要です。
・経営層の積極的な参画
・セキュリティ規程の見直し
・従業員に自分事として感じさせる
・定期点検の有効活用

「セキュリティ規程の見直し」と「定期点検の有効活用」は、以前の記事で解説したので、今回は「経営層の積極的な参画」と「従業員に自分事として感じさせる」という観点で進めていきます。

（１）経営層の積極的な参画

情報セキュリティ対策を疎かにすると、経営に大きな影響を与え、最悪の場合、経営破綻や法的・道義的責任を問われることもあります。企業と従業員を守るため、情報セキュリティ対策は組織全体で取り組む必要があり、経営層の関与が不可欠です。
経営層の積極的な関与なしに、情報セキュリティ対策は成り立たないといえます。
経営層には自らが情報セキュリティに取り組むことを宣言し（情報セキュリティ基本方針の作成と公開）、具体的な対策を「企業や組織を守るためだけでなく従業員を守るための取り組みである」ことを説明することが求められます。また、その後も継続的に対策に取り組む姿勢を見せることが重要です。

（２） 経営層が果たすべき具体的なリーダーシップ

経営層には、サイバーセキュリティ経営ガイドライン Ver3.0 に記載されているサイバーセキュリティ※対策におけるリーダーシップと同等のことが求められます。具体的な取り組みは以下の通りです。

・社内全体でサイバーセキュリティ(情報セキュリティ)対応方針を決定
・リスク管理体制の構築
・予算、人材などの資源の確保
・リスクの把握と対応計画の策定
・リスクに対応する仕組みの構築

・PDCA サイクルによる対策の実施
・インシデント発生時の緊急対応体制の整備
・インシデント被害に備えた復旧体制の準備

経営層は、担当者を決めて任せる、または専門家に依頼しながら進めるリーダーシップが必要となります。特に、「任せきり」や「依頼しっぱなし」にならないよう、常にフォローアップすることが重要です。

※サイバーセキュリティと情報セキュリティとの違い
セキュリティ対策の基本的な考え方は同じと言えるが、サイバーセキュリティは情報セキュリティの 3 要素である、「機密性」「完全性」「可用性」に「安全性」(テロや戦争などの物理的な機器の破壊を想定)が加わり、かつ、デジタルデータを対象としている。また、情報セキュリティでは対象となっていた紙媒体が対象外となっていることが大きな違いといえる。

２．教育の進め方

情報セキュリティ教育は、以下の点を考慮して教育計画を年度単位で立案します。

・情報セキュリティ関連規程の説明（特に入社時や規程改訂時）
・最新の脅威に関する注意喚起（随時）
・関連法令の理解（特に公布・施行時）
・個人情報の取り扱いに関する留意事項

また、情報セキュリティ教育で重視すべきポイントは次の 3 点です。

・基礎知識の提供
・脅威の具体的理解
・自ら対策を考える能力の育成

学習には、独立行政法人情報処理推進機構（IPA）が提供しているコンテンツを利用するとよいでしょう。

（１）基礎知識の提供

「5 分でできる！情報セキュリティポイント学習」など、簡単に学べるコンテンツを活用し、従業員が日常の中で実践的に学べるようにします。このコンテンツは、主に中小企業で働く方を対象に、職場の日常の 1

コマを取り入れた１テーマ５分程度の無料コンテンツです。
従業員向けコース(4 テーマ)は、親しみやすい内容で、セキュリティに関する様々な事例を疑似体験しながら、適切な対処法を学ぶことができます。

（２）脅威の具体的理解

「情報セキュリティ１０大脅威 2024」や「映像で知る情報セキュリティ」などを活用します。
情報セキュリティ１０大脅威 2024 は、組織編と個人編の２系統で構成されています。これらの学習を通じて自社や自身を脅かす可能性のある脅威について学び、自分自身の身の回りに起こり得ることと捉えてもらい、具体的なリスクについて理解を深めます。

また、映像教材を利用すれば、ドラマ仕立てで情報セキュリティ上の様々な脅威と対策を学ぶことができます。

（３）自ら考える能力の育成

危険予知訓練（KYT：危険のＫ、予知のＹ、訓練(トレーニング)のＴをとったもの）を通じて、組織や職場に潜むリスクを発見し、対応策を考える力を養います。ＫＹＴの基礎手法である「ＫＹＴ基礎４ラウンド法」では、危険の潜むイラストを使ったシミュレーションにより、リスクを予測し、対策を検討する能力を身につけることができます。

イラストの例を図１に示します。



図１　危険が潜むイラスト例

引用元：令和６年度 東京都中小企業サイバーセキュリティフォローアップ事業
第１回セミナー「社内へのサイバーセキュリティ対策の浸透」より抜粋

ラウンド	危険予知訓練の4ラウンド	危険予知訓練の進め方
1R	どんな危険がひそんでいるか	イラストシートの状況の中にひそむ危険を発見し、危険要因とその要因がひきおこす現象を想定して出し合い、チームのみんなで共有する。
2R	これが危険のポイント	発見した危険のうち、これが重要だと思われる危険を把握して○印、さらにみんなの合意でしぼりこみ、◎印とアンダーラインをつけ「危険のポイント」とし、指差し唱和で確認する
3R	あなたならどうする	◎印をつけた危険のポイントを解決するにはどうしたらよいかを考え、具体的な対策案を出し合う
4R	私達はこうする	対策の中からみんなの合意でしぼりこみ、※印をつけ「重点実施項目」とし、それを実践するための「チーム行動目標」を設定し、指差し唱和で確認する

図２　ＫＹＴ基礎４ラウンド法による危険予知訓練の進め方

引用元：厚生労働省 職場のあんぜんサイト から抜粋引用

これらを組み合わせることで、従業員が自分事としてとらえられるように学習していきます。
具体的な進め方の詳細は下記のサイトをご確認ください。

・職場のあんぜんサイト：危険予知訓練（ＫＹＴ）　（厚生労働省）

３．資産の扱い方・管理方法

ここでは、情報セキュリティにおける資産の洗い出し方法と管理するためのリスク分析の方法を解説します。
情報資産の把握方法については、こちらの記事でも紹介しています。あわせてご覧ください。

・コスト意識から投資意識へ～セキュリティ対策に関わる費用と効果～

（１）資産管理台帳の作成

業務で利用する電子データや書類を洗い出し、情報資産管理台帳に記入します。
その際、業務の流れ（業務フロー）に沿って情報資産を整理すると、業務全体を俯瞰でき、どのように情報を生成し、保持し、破棄しているかといったライフサイクルが見えるので効果的です。
例えば、「受注データ」は、注文受付で発生し、販売管理システムで管理され、期間が過ぎると、注文書破棄のタイミングで消滅します。

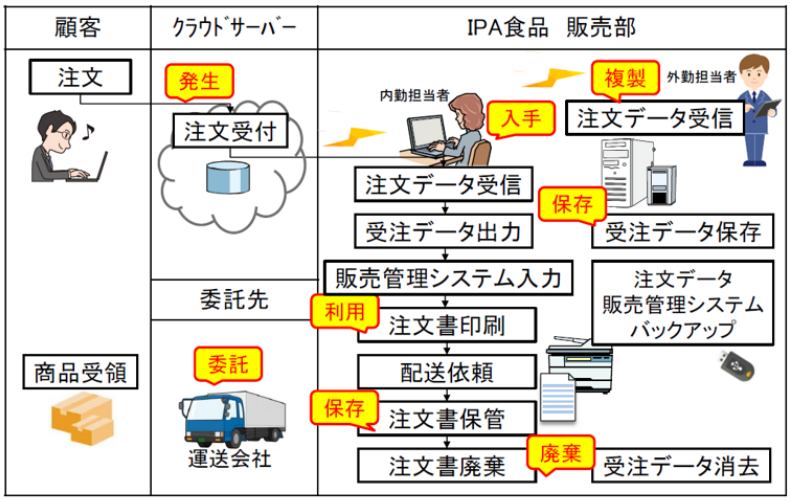


図 3　業務の流れとデータのライフサイクル例

引用元［IPA］セキュリティプレゼンターカンファレンス 2017　資料を基に作成

また、資産の粒度は、細かすぎると管理が大変になり、逆に粗いと次のリスク分析が難しくなります。
例えば、「設計書」などと大きい単位で洗い出しを行い、顧客単位に分ける必要はありません。下記の「台帳記入例」シートのリストアップ例が資産粒度の目安となります。
この作業を通じて、業務フローに沿った形で情報の管理が可能となります。

情報資産管理台帳

業務分類	情報資産名称	備考	利用者範囲	管理部署	媒体・保存先	個人情報の種類		
						個人情報	要配慮個人情報	特定個人情報
人事	社員名簿	社員基本情報	人事部	人事部	事務所PC	有		
人事	社員名簿	社員基本情報	人事部	人事部	書類	有		
人事	健康診断の結果	雇入時・定期健康診断	人事部	人事部	書類		有	
経理	給与システムデータ	税務署提出用源泉徴収票	給与計算担当	人事部	事務所PC			有
経理	当社宛請求書	当社宛請求書の原本（過去3年分）	総務部	総務部	書類			
経理	発行済請求書控	当社発行の請求書の控え（過去3年分）	総務部	総務部	書類			
共通	電子メールデータ	重要度は混在のため最高値で評価	担当者	総務部	事務所PC	有		
共通	電子メールデータ	Gmailに転送	担当者	総務部	社外サーバー	有		

図 4　資産管理台帳記入例

引用元：中小企業の情報セキュリティ対策ガイドライン第 3.1 版を基に作成

（２）資産の評価

次に、それぞれの情報資産ごとに情報セキュリティの３要素（機密性・完全性・可用性）に対する評価を行い、その影響度を明確にします。法律や契約などの要件も確認しつつ、企業独自の基準で判断します。

情報資産管理台帳

業務分類	情報資産名称	備考	利用者範囲	管理部署	媒体・保存先	個人情報の種類			評価値		
						個人情報	要配慮個人情報	特定個人情報	機密性	完全性	可用性
人事	社員名簿	社員基本情報	人事部	人事部	事務所PC	有			3	1	1
人事	社員名簿	社員基本情報	人事部	人事部	書類	有			3	3	3
人事	健康診断の結果	雇入時・定期健康診断	人事部	人事部	書類		有		3	3	2
経理	給与システムデータ	税務署提出用源泉徴収票	給与計算担当	人事部	事務所PC			有	3	3	2
経理	当社宛請求書	当社宛請求書の原本（過去3年分）	総務部	総務部	書類				2	2	2
経理	発行済請求書控	当社発行の請求書の控え（過去3年分）	総務部	総務部	書類				2	2	2
共通	電子メールデータ	重要度は混在のため最高値で評価	担当者	総務部	事務所PC	有			3	3	3
共通	電子メールデータ	Gmailに転送	担当者	総務部	社外サーバー	有			3	3	3

図５　評価基準を追記した資産管理台帳記入例

引用元：中小企業の情報セキュリティ対策ガイドライン第 3.1 版を基に作成

（３）資産の管理

３要素の評価から重要度を決定し、発生頻度なども考慮した上で、リスク値を算出します。
リスク値の大きさに基づき、適切な対応策を検討して管理します。

情報資産管理台帳

業務分類	情報資産名称	備考	利用者範囲	管理部署	媒体・保存先	個人情報の種類			評価値				保存期限	登録日	現状から想定されるリスク（入力不要・自動表示）				
						個人情報	要配慮個人情報	特定個人情報	機密性	完全性	可用性	重要度			脅威の発生頻度 ※「脅威の状況」シートに入力すると表示	脆弱性 ※「対策状況チェック」シートに入力すると表示	被害発生可能性		リスク値
人事	社員名簿	社員基本情報	人事部	人事部	事務所PC	有			3	1	1	3		2023/4/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	6 リスク大
人事	社員名簿	社員基本情報	人事部	人事部	書類	有			3	3	3	3		2023/4/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	3 リスク小
人事	健康診断の結果	雇入時・定期健康診断	人事部	人事部	書類		有		3	3	2	3	5年	2023/4/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	3 リスク小
経理	給与システムデータ	税務署提出用源泉徴収票	給与計算担当	人事部	事務所PC			有	3	3	2	3	7年	2023/4/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	6 リスク大
経理	当社宛請求書	当社宛請求書の原本（過去3年分）	総務部	総務部	書類				2	2	2	2		2023/4/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	2 リスク小
経理	発行済請求書控	当社発行の請求書の控え（過去3年分）	総務部	総務部	書類				2	2	2	2		2023/4/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	2 リスク小
共通	電子メールデータ	重要度は混在のため最高値で評価	担当者	総務部	事務所PC	有			3	3	3	3		2023/4/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	6 リスク大
共通	電子メールデータ	Gmailに転送	担当者	総務部	社外サーバー	有			3	3	3	3		2023/4/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	6 リスク大
営業	顧客リスト	得意先（直近５年間に実績があるもの）	営業部	営業部	社内サーバー	有			3	3	3	3		2023/4/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	6 リスク大
営業	顧客リスト	得意先（直近５年間に実績があるもの）	営業部	営業部	可搬電子媒体	有			3	2	2	3		2023/4/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	3 リスク小
営業	顧客リスト	得意先（直近５年間に実績があるもの）	営業部	営業部	モバイル機器	有			3	2	2	3		2023/4/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	6 リスク大
営業	受注伝票	受注伝票（過去10年分）	営業部	営業部	社内サーバー				2	2	2	2		2023/4/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	4 リスク中
営業	受注伝票	受注伝票（過去10年分）	営業部	営業部	書類				2	2	2	2		2023/4/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	2 リスク小
営業	受注契約書	受注契約書原本（過去10年分）	営業部	営業部	書類				2	3	2	3		2023/4/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	3 リスク小
営業	製品カタログ一式	現役製品カタログ一式	営業部	営業部	社内サーバー				1	2	2	2		2023/4/1	3:通常の状態で脅威が発生する	2:部分的に対策を実施している	2	可能性：中	4 リスク中

利用方法　台帳記入例　重要度定義　情報資産管理台帳　脅威の状況　対策状況チェック　診断結果

図 6　リスク値まで決定した資産管理台帳記入例
引用元：中小企業の情報セキュリティ対策ガイドライン第 3.1 版を基に作成

情報セキュリティ管理を成功に導くためには、経営層と従業員が共にセキュリティの重要性を理解し、「自分事」と認識して積極的に関与することが大切です。
また、情報資産は「何から何を守るのか」を念頭に、「どのような脅威があるのか」「発生したらどう対応するのか」を中心に管理していくこともおわかりいただけたかと思います。

このように、情報セキュリティは組織的・個人的に「自分事」という認識をもち、自ら積極的に行動することで実現できるものです。
このような自立した組織を形成することが、企業の持続可能な発展を支える鍵となると考えます。
ご購読ありがとうございました。

４．関連文書

今回の記事でご紹介した情報のリンク先を以下に記載しています。
ぜひ、理解を深めたい、次のステップに進みたいと思った際の参考にしてください。

１．情報セキュリティ１０大脅威 2024（IPA）
２．中小企業の情報セキュリティ対策ガイドライン（IPA）
３．サイバーセキュリティ経営ガイドライン Ver3.0（IPA）
４．5 分でできる！情報セキュリティポイント学習（IPA）
５．映像で知る情報セキュリティ（IPA）
６．職場の安全サイト（厚生労働省）

レベル 3_#1_クラウドサービスを安全に利用するポイントとは（1/3）
掲載日：2024/7/1



中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。本記事では「クラウドサービスを安全に利用するポイント」について解説します。
近年、働き方改革や新型コロナウイルス感染症対策の影響でテレワークが急増しました。それに伴い、インターネットがあればどこでも仕事ができるクラウドサービスへの移行が進んでいます。今後、ますます普及すると考えられるクラウドサービスを安全に利用するためのポイントについて 3 回に分けて解説します。

１． クラウドサービスとは

インターネットを通じてソフトウェアやハードウェアを利用する情報システムサービスのことを指します。利用者から見えない場所にあるコンピュータを利用することから「クラウド（cloud、雲）」と呼ばれています。経営管理アプリケーション（財務会計、税務申告、給与計算、労務管理）、業務アプリケーション（顧客管理、販売管理、名刺管理、ホームページ作成、EC サイト）、オフィスアプリケーション（ワープロ、表計算、グループウェア、電子メール、オンラインストレージ）など、様々なサービスがあり、利用が急速に進んでいます。代表的なものとして、皆さんにも身近なマイクロソフト社の Microsoft 365 などが挙げられます。
クラウドサービスは、提供される情報システム（ハードウェアやソフトウェア）の範囲によって、次の 3 つの形態に分類されます。

SaaS（Software as a Service の略。読み方はサース）	会計アプリケーションやオフィスソフト、ファイルサーバーなど、一般に利用されているアプリケーションソフトをウェブサービスとして提供します。
PaaS（Platform as a Service の略。読み方はパース）	OS やデータベース管理システムなどのミドルウェアを提供します。アプリケーションソフトは別途導入しなければなりません。
IaaS（Infrastructure as a Service の略。読み方はイアース）	仮想のサーバーやメモリなどのハードウェアやネットワークなどのシステム基盤のみを提供します。

日本の PaaS 市場、IaaS 市場では、大手クラウドサービス（AWS（Amazon）、Azure（Microsoft）、GCP（Google））の利用率が高く、特に AWS は、PaaS／IaaS 利用企業の半数以上を占めています。
※総務省 令和 5 年度 情報通信白書から

これらのクラウドサービスを提供する組織は「プラットフォーム事業者」「クラウドサービスプロバイダー」などと呼ばれます。一部のサービスでは、プラットフォーム事業者自身が、他の大手事業者が提供する PaaS を利用して業務用アプリケーションを構築し、顧客がそれを利用する、という形で 1 つのクラウドサービスが構築されることもあります。この場合、複数事業者のサービスで構成されるため、サービス利用者には全体の構成が分かりにくく、サービスを選択するときの判断が複雑になることがあります。

２．クラウドサービスのメリット

クラウドサービスは情報システムを自社で所有・管理する必要がないため、ハードウェアやソフトウェアの導入・保守の費用や負担が軽減されます。また、利用者はインターネットに接続するパソコンやスマートフォンがあれば、いつでも・どこからでも利用することができる、というメリットがあります。国の情報システム導入におけるコスト削減や柔軟なリソースの増減などの観点から、「クラウド・バイ・デフォルト原則」や地方公共団体の経費削減や住民サービス向上図る「自治体クラウド」など、コンピュータ資源を所有せずに利用するクラウドが主流になりつつあります。

３．クラウドサービスの注意点

クラウドサービスはインターネットを利用するため、いつでも、誰でも、どこからでもアクセス可能である一方、絶えずサイバー攻撃のリスクに晒されています。そのため、インターネット特有の脅威やリスクを考慮し、サービス提供事業者のセキュリティ対策を把握するとともに、利用者自身でできるセキュリティ対策を実行する

必要があります。

４．クラウドサービスを安全に利用するためのポイント

クラウドサービスのセキュリティは、サービス提供事業者と利用者がそれぞれの役割と責任を分担し、必要な対策を実施することで維持・向上します。
以下にクラウドサービスを安全に利用するためのポイントについて解説します。

（１）選択するときのポイント

No.1 どの業務で利用するか明確にする	クラウドサービスでどの業務を行い、どの情報を扱うかを検討し、業務の切り分けや運用ルールを明確にしましょう。
No.2 クラウドサービスの種類を選ぶ	業務に適したクラウドサービスを選び、メリットについて確認しましょう。
No.3 取扱う情報の重要度を確認する	クラウドサービスで取扱う情報が漏えいしたり、改ざんされたり、消失、サービスが停止したときの影響を確認しましょう。
No.4 セキュリティのルールと矛盾しないようにする	セキュリティのルールとクラウドサービス活用との間に矛盾や不一致が生じないようにしましょう。
No.5 クラウド事業者の信頼性を確認する	クラウドサービスを提供する事業者は信頼できる事業者を選択しましょう。
No.6 クラウドサービスの安全・信頼性を確認する	サービスの稼働率、障害発生頻度、障害時の回復目標時間などのサービス品質保証を確認しましょう。

（２）運用するときのポイント

No.7 管理担当者を決める	クラウドサービスの技術的な側面などの特性を理解したうえで、業務に適した運用や設定・操作・ヘルプデスクを行うことができる、管理担当者を社内に確保しましょう。
No.8 利用者の範囲を決める	クラウドサービスを利用する人の範囲を決め、どのような権限を与えるか適切に管理しましょう。
No.9 利用者の認証を厳格に行う	パスワードなどの認証機能を適切に設定・管理しましょう。
No.10 バックアップに責任を	サービス停止やデータの消失・改ざん等に備えて、重要情報を手元

持つ	に確保して、必要なときに使えるようにしましょう。

（３）セキュリティ管理のポイント

No.11 付帯するセキュリティ対策を確認する	クラウドサービスにおけるセキュリティ対策が具体的に公開されているか確認しましょう。
No.12 利用者サポートの体制を確認する	サービスの使い方がわからないときの支援（ヘルプデスクや FAQ）が提供されているか確認しましょう。
No.13 利用終了時のデータを確保する	サービスの利用が終了したときの、データの取扱い条件について確認しましょう。
No.14 適用法令や契約条件を確認する	個人情報保護など関連法規制の遵守などを規定した利用規約等について確認しましょう。
No.15 データ保存先の地理的所在地を確認する	データがどの国や地域に設置されたサーバーに保存されているか確認しましょう。

なお、本稿は、独立行政法人情報処理推進機構（IPA）が発行している「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」を中心に解説しています。
次回は、クラウドサービスを安全に利用するポイントの続きとして、実際に何をしたら良いのか、例を挙げて解説します。

レベル 3_#2_クラウドサービス安全に利用するポイントとは（2/3）
掲載日：2024/7/25



中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。今回は、前回の「クラウドサービスを安全に利用するポイントとは（1/3）」でご紹介した利用時のポイント No.1～15 について、それぞれ実際に何をしたらよいのかを例を挙げて解説します。

１． 選択するときのポイント

No.1 どの業務で利用するか明確にする 例えば、社内の情報共有のために、 ・グループウェアを利用し、社員のスケジュール管理を行う ・オンラインストレージに製品カタログを保存して営業部門で共有する…など
No.2 クラウドサービスの種類を選ぶ 例えば、社外でも業務ができるようにして、コストを削減するために、 ・経費精算にクラウドサービスを利用することで外出先や自宅などどこでも業務ができるようにする ・経費精算に関わる社内の作業時間を短縮し、サービス利用料を上回るコストを削減する…など
No.3 取り扱う情報の重要度を確認する 例えば、お客様の個人情報をクラウドサービスに保存していて、サイバー攻撃で個人情報が漏えいした

場合の影響、

・悪用などで本人に多大な迷惑がかかる

・本人への謝罪、補償や関係者への連絡が必要になる

・個人情報保護委員会に報告が必要になる

・被害拡大防止や再発防止のために多額の費用がかかる…など

No.4 セキュリティのルールと矛盾しないようにする

例えば、給与計算をクラウドサービスで行うにあたり、自社のセキュリティルールでは従業員のマイナンバーを登録する必要があるが、

・マイナンバーを記載した書類やデータを社外に保存することは社内ルールで禁止されている

・そこで暗号化登録ができるサービスを利用し、暗号化した場合のみ社外の保存を許可するルールに変更する…など

No.5 クラウド事業者の信頼性を確認する

例えば、会計業務をクラウドサービスに移行するにあたり長期間利用できて、セキュリティ対策を常に改善しているサービスを選択するために、

・事業者が公表している財務情報を確認する

・利用者数などの実績を問い合わせる

・事業者の情報セキュリティ方針や関連した認証・認定制度※1 の取得状況を確認する…など

※1）

〇ISMS クラウドセキュリティ認証（一般社団法人情報マネジメントシステム認定センター）
https://isms.jp/isms.html

〇クラウド情報セキュリティ監査制度（特定非営利活動法人日本セキュリティ監査協会）
http://jcispa.jasa.jp/cloud_security/

〇ASP・SaaS 情報開示認定制度（一般社団法人日本クラウド産業協会）
https://www.aspicjapan.org/nintei/asp-nintei/index.html

〇ISMAP 政府情報システムのためのセキュリティ評価制度
https://www.ismap.go.jp/

No.6 クラウドサービスの安全・信頼性を確認する

例えば、店舗にクラウド型 POS レジを導入するにあたりサービスが常に動いている必要があるため、

・事業者またはプラットフォーム事業者が公表している品質保証基準（SLA※2）を確認する

・システムの障害でデータ消失などの被害が発生したときに、どこまでが事業者の責任で、どこからが利用者の責任なのか利用規約で確認する…など

※2）Service Level Agreement サービスレベルに関する合意書

2．運用するときのポイント

No.7 管理担当者を決める

例えば、クラウド型顧客管理システムの運用にあたり、

・入力項目やその活用については営業部長が担当する

・技術的な設定や社内のヘルプデスクはシステム管理者が担当する…など

No.8 利用者の範囲を決める

例えば、販売管理をクラウドサービスで行うにあたり、

・社長と販売部門従業員だけに利用者アカウントを作成する

・承認権限は従業員の上司に付与する…など

No.9 利用者の認証を厳格に行う

例えば、なりすましや不正ログインを防ぐために、

・パスワードは破られにくい安全なパスワードを利用する

・ID・パスワードの共有はしない

・サービスで以下の認証方式が提供されている場合は利用する

・特定のパソコンでしか利用できないように電子証明書※3 をインストールする

・パスワードを不正利用されてもログインはできないように「2 段階認証」※4 を用いる…など

※3）特定の PC からしかアクセスできないように制限するための「身分証明書」

※4）複数の要素（記憶、所持、生体情報）を用いた「多要素認証」や、同じ要素の認証を多段で実施する「多段階認証」など

No.10 バックアップに責任を持つ

例えば、会計データやホームページなど、消失や改ざんされたときの影響が大きいものは、

・クラウドサービスの拡張機能にバックアップがある場合は利用する

・定期的に社内の専用ハードディスクなどにもバックアップを取得する

・直前のバックアップよりもさらに過去の状態に遡って復元できるように複数世代※5 のバックアップを取得する…など

※5）毎月のバックアップで前月だけでなく 2 ヶ月前、3 ヶ月前のように複数のバックアップを取得すること

3．セキュリティ管理のポイント

No.11 付帯するセキュリティ対策を確認する

例えば、サイバー攻撃や通信傍受に対する対策が十分されているか、

・通信の暗号化

・ファイアウォールや侵入検知

・ウイルス対策

・サービスで使っている OS やソフトウェアの脆弱性対応・セキュリティパッチの適用について公開されているか確認する…など

No.12 利用者サポートの体制を確認する

例えば、クラウドサービスを社内のシステム担当者不在の週末も利用するため、

・サポートの受付時間（週末夜間も受付可能か）

・連絡方法（メール、電話、チャット、オンライン、のうちパソコンがない事務所から週末も電話連絡可能か）

・料金（頻繁に問い合わせた場合に料金はどのぐらいか）を確認する…など

No.13 利用終了時のデータを確保する

例えば、利用中のクラウド型会計システムを他のクラウドサービスに変更するにあたり、

・過年度データを含む全データを返却または社内のパソコンなどにダウンロードできるか

・データのフォーマットは他のサービスと互換性があるか

・移行先のサービスは返却されたデータを一括して取り込む機能があるか

・返却後にシステム上に残るデータは完全に消去または再利用されないことが保証されているかを確認する…など

No.14 適用法令や契約条件を確認する

例えば、クラウドサービスに秘密情報や個人情報を保存するため、

・利用者が入力したデータにサービス事業者がアクセスする場合の条件や責任について明記されているか

・設備の保守等を再委託している場合の再委託先の管理監督責任について明記されているか

・利用者が入力した個人情報に関して個人情報保護法に準拠することが明記されているか（安全管理措置、委託先の監督）を確認する…など

No.15 データ保存先の地理的所在地を確認する

例えば、インターネットを通じて商品やサービスを海外に販売する越境 EC を開店するにあたり、

・プラットフォームを構築するデータセンターの所在国・地域と現地の個人情報保護に係わる法律・規制※6 を確認する

・現地の法律・規制に基づきプライバシーポリシー制定や個人情報の取り扱いについて事前に承諾を得るようにする…など

※6）

〇個人情報保護法

〇EU 一般データ保護規則（General Data Protection Regulation：GDPR）

〇アメリカ・カリフォルニア州 消費者プライバシー法（California Consumer Privacy Act：CCPA）

〇中国・個人情報保護法（Personal Information Protection Law：PIPL）

なお、本稿は、独立行政法人情報処理推進機構（IPA）が発行している「中小企業の情報セキュリティ対策ガイドライン 第 3.1 版」を中心に解説しています。
次回は、クラウドサービスで実際に起きた事故事例と利用者側の対応について解説します。

レベル 3_#3_クラウドサービスを安全に利用するポイントとは（3/3）
掲載日：2024/8/1



中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。前回まで2回にわたって「クラウドサービスを安全に利用するポイント」について解説しました。
前回までの内容はこちら。

クラウドサービスを安全に利用するポイントとは（1/3）
クラウドサービス安全に利用するポイントとは（2/3）

シリーズの最後となる今回は、実際にクラウドサービスで起きた事故の事例から、「クラウドサービスを安全に利用するポイント」に従った利用者側の対応について解説します。

1．クラウドサービス事故の事例

（1）事故の概要

- M社の提供するSaaS形態の社会保険/人事労務業務クラウドサービスが、2023年6月に第三者からの不正アクセスを受けた。
- サービスを提供しているデータセンター上のサーバーがランサムウェアに感染し、管理されていた個人

情報が暗号化され、漏えいのおそれが発生した。

- 当サービスは、主に社労士が利用する業務システムで、社会保険申請、給与計算、人事労務管理等の業務に利用する。
- 取り扱われていた個人情報は、社労士の顧客である企業や事業所等の従業員等の氏名、生年月日、性別、住所、基礎年金番号、雇用保険被保険者番号、マイナンバーなどが含まれる。
- M 社によれば 2024 年 3 月時点では個人情報の悪用などの二次被害は確認されていない。

（２）事故の規模

M 社によるサービスの利用実績は以下のとおり。

- 社労士事務所：2,754 事業所（2023 年 4 月 1 日時点）
- 管理事業所：約 57 万事業所（2023 年 4 月 1 日時点）
- 管理する個人情報人数：最大約 2,242 万人（2023 年 6 月 5 日時点）

個人情報保護委員会※1 が受領した漏えい等の報告件数※2 は以下のとおり。

- 2023 年 6 月から 2024 年 3 月までに受領した漏えい等報告件数は報告者ベースで 3,067 件（個人情報人数計 7,496,080 人）
- 大部分は社労士事務所からの提出で、顧問先事業者との連名報告の形が多かった。
  内訳は、社労士事務所等が 2,459 件（人数計 6,724,609 人）、顧問先事業者が 404 件（人数計 392,125 人）、企業等が 204 件（人数計 379,346 人）

※1 内閣府の外局として個人の権利利益を保護するため、個人情報の適正な取扱いの確保を図ることを任務とする、独立性の高い機関

※2 個人情報保護委員会 Web サイトから
https://www.ppc.go.jp/personalinfo/legal/leakAction/#about
下記の要件に該当する場合、漏えい等報告が義務付けられています。
不正の目的をもって行われたおそれがある当該個人情報取扱事業者に対する行為による個人データ※3（当該個人情報取扱事業者が取得し、又は取得しようとしている個人情報であって、個人データとして取り扱われることが予定されているものを含む）の漏えい等（又はそのおそれ）
【例 1】不正アクセスにより個人データが漏えいした場合
【例 2】ランサムウェア等により個人データが暗号化され、復元できなくなった場合

※3 個人データとは、個人情報保護法において、個人情報データベース等（特定の個人情報を容易に検索できるようにしたもの）を構成する個人情報のことをいいます。

かなり大きなクラウドサービス事故だったことがわかります。このため、M 社のサービスを利用していたユーザが受けた影響も小さくなかったことでしょう。
ここからは、「クラウドサービスを安全に利用するポイント」に従って、この事態に直面した利用者側ではどのような対応が必要となるのかを解説します。

２．「クラウドサービスを安全に利用するポイント」に従った利用者側の対応

インターネット上でのサイバー攻撃は年々巧妙化しているため、クラウドサービス提供者も利用者も、完全に事故を防ぐことは難しくなっています。そこで、予期せぬ事故が起きた場合に、利用者に発生する被害や影響を最小限に止めるにはどうしたらいいか、事例を基に「クラウドサービスを安全に利用するポイント」の該当項目から解説します。
※カッコ内は前回「クラウドサービスを安全に利用するポイント」の No.です。

取り扱う情報の重要度を確認する（No.3） 事例 M 社のサービスは、マイナンバーを含む個人情報を取り扱います。個人情報を取り扱うサービスの利用者は、クラウドサービス側で発生した事故であっても管理責任を問われる立場にあるため、あらかじめ次の体制を整備しておきましょう。 ・迅速に本人や顧客への報告、謝罪、補償や関係者への連絡ができるようにしておく ・個人情報保護委員会への報告ができるようにしておく
クラウドサービスの安全・信頼性を確認する（No.6） 事例 M 社の公表資料によると、「システムやサービスにアクセスできない状況」から「サービス再開」まで約 2 か月かかっています。サービスの利用者は、この間、必要な業務を止めることはできず、他の手段で実施せざるを得ませんでした。 利用しているクラウドサービスが停止すると業務への影響が大きい場合には、事故や障害によるサービス停止を想定し、停止期間中も業務が遂行できるように代替手段を準備しておきましょう。
利用者の認証を厳格に行う(No.9) 個人情報保護委員会の公表資料によると「M 社においては、ユーザのパスワードルールが脆弱であったこと、また、管理者権限のパスワードも脆弱であり類推可能であったことから、アクセス者の識別と認証に問題があった」とあります。ここでの” ユーザのパスワードルールが脆弱“とは、ユーザがサービスにログインするためのパスワードが脆弱であっても登録できる、ということです。正当なユーザであっても脆弱なパスワードを使っていると、第三者に類推され不正アクセスされる可能性があります。

パスワードによる認証は、多くのサービスで用いられていますが、パスワードによる認証を突破する攻撃手法は年々高度化しています。従ってサービスを利用するにあたっては、4 桁数字のような脆弱なパスワードが設定可能であっても、自主的に強固なパスワードを設定し、以下の認証方式が提供されている場合は、必ず利用しましょう。

１．パソコンに電子証明書※をインストールする。
２．パスワードだけでなく複数の要素（記憶、所持、生体情報）を用いた認証方式である「多要素認証」や、同じ要素の認証を多段で実施する認証方式である「多段階認証」を利用する。

※）特定のパソコンからしかサービスにアクセスできないようにするための「身分証明書」

＜参考 強固なパスワード＞
・パスワードは 10 文字以上で「できるだけ長く」、大文字、小文字、数字、記号を含めて「複雑に」、名前、電話番号、誕生日、簡単な英単語などは使わず、推測できないように する。
・同じ ID・パスワードを複数サービス間で使い回さない。

バックアップに責任を持つ（No.10）
事例ではランサムウェアに感染して個人情報が暗号化されています。復旧方法は公表されていませんが、ランサムウェアに感染すると、確実に復旧する方法はバックアップから復元するしかありません。
利用しているクラウドサービスのバックアップについて確認するとともに、不十分な場合は、利用者側でも前月・2 ヶ月前・3 ヶ月前のように複数世代のバックアップを、社内のハードディスク・テープ等複数の装置・媒体やクラウドストレージ等遠隔地のサーバーに保存し、確実に復元ができるようにしましょう。

＜参考 バックアップの 3-2-1 ルール＞ ※1
3. データを 3 つ保存
2. バックアップファイルを異なる 2 種類の媒体に保存
1. 1 つをオフライン※2に保管

※ 1『 3 分で分かる！セキュリティ用語解説』でも詳しく解説していますので、ご興味のある方はこちらもご覧ください。
「3-2-1 ルール」【3 分でわかるセキュリティ用語解説 #1】

※ 2 パソコンがランサムウェアに感染すると LAN で接続しているサーバー内のバックアップも同時に感染することがあります。

利用終了時のデータを確保する（No.13）
利用していたクラウドサービスで事故があり、他のクラウドサービスに変更する場合に備え、必要に応じてデータをパソコンなどにダウンロードして、利用できるようにしておきましょう。

また、利用していたクラウドサービスに機密情報や個人情報が残らないように完全に消去しましょう。

なお、本稿は、個人情報保護委員会公表資料及び独立行政法人情報処理推進機構（IPA）が発行している「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」を参考に解説しています。

レベル 3_#4_セキュリティインシデント対応（1/2）
掲載日：2024/8/8



中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。本記事では、これまでに「クラウドサービス利用時の注意点」について解説してきました。今回は実際に何か問題が生じた際に対応が求められるセキュリティインシデントについて、重要なポイントを分かりやすく、具体的な事例も交えてお伝えします。

１．セキュリティインシデントとは

まず、セキュリティインシデントの定義を確認しましょう。
セキュリティインシデントとは、情報漏えいやシステムの停止などセキュリティに関わる事故や出来事（事象ともいう）を指します。単に「インシデント」と呼ばれることもあります。
事故は、情報の漏えいや改ざん、破壊・消失、情報システムの停止などが挙げられます。
事象は、事故につながる可能性がある出来事です。メールを誤送信したが情報漏えいにはいたらなかった、あるいは誤送信しそうになったが送信する前に気づいた場合などです。

２．インシデント対応の必要性

インシデントが発生しないように様々な対策を取っていても、予期せぬインシデントが起こる可能性はあります。万が一インシデントが発生した場合には、被害や影響範囲が最小限になるようにし、事業を継続できるようにする必要があります。

３．インシデント発生時の想定被害

インシデントが発生した場合の被害には、直接的な被害と、間接的な被害があります。

【直接的な被害】：攻撃者による不正送金や金銭要求
対応人件費
原因調査や復旧のための外部委託費
復旧までの代替品費
取引先や顧客への謝罪対応費
法的対応のための弁護士費用　など

【間接的な被害】：関係者への被害波及
会社の信用低下
事業停止による機会損失　など

実際にセキュリティインシデント対応を行った際の被害などを集計したデータでは、サイバー攻撃を受けた企業の約半数は業務停止の被害を受け、約２割の企業が直接的な金銭被害や復旧にあたった人件費などの金銭的コストが発生しています。

参照記事
https://www.trendmicro.com/ja_jp/jp-security/23/k/ciolounge-joint-survey-commentary.html
（出典：トレンドマイクロ株式会社　2023 年 11 月 1 日 セキュリティサイト掲載記事）
https://www.nikkei.com/article/DGXZQOUE056JB0V01C23A0000000/
（出典：株式会社日本経済社　2023 年 10 月 31 日サイト掲載記事）

４．インシデント対応の目的

インシデントが発生したことで生じる被害とその影響範囲を最小限に抑え、迅速に復旧し、再発を防止することで、企業（組織）の事業が継続できるようにすることが目的です。

５．実際のインシデント対応

ここからは、実際にインシデントが発生した際にどのような対応が必要となるのか具体的なステップを説明していきます。
なお、インシデントの対応は、発生している事象・被害や影響範囲の大きさなどによって変わってきます。このため、インシデント対応時に下記情報をまとめて整理しておくことが大切です。

（１）インシデント対応時に整理すべき情報

インシデントの分類	情報漏えい、ウイルス感染、システム停止など
事業者の名称	事業者の名称（受託案件の場合は委託元）
責任者・担当者	本件に関する責任者及び担当者の所属、氏名
発覚日時	インシデントを認知（発見したり、通報を受けた）した日時
発生日時	調査で判明したインシデントの発生日時
発生事象	表面化している事柄、被害、影響など
対応経過	発生から現時点までの時系列での経過
想定原因	現時点で想定される直接的な原因
被害を受けたシステムの状況	被害を受けたシステムの概要と被害の詳細な状況
システム構成・運用状況	システムの物理的な所在場所 OS やアプリケーションとそれぞれのバージョン構成 システムの構成図 システムの運用状況 使用しているセキュリティツールやサービスの利用状況

この中で、システム構成・運用状況はインシデントが発生してからでは整理できませんね。普段から整理し

ておくようにしましょう。

それでは、いまからインシデント発生時の具体的な対応手順と内容を説明します。

（２）インシデント対応時のステップ１・２・３

＜ステップ１＞検知・初動対応

インシデントを発見した際（疑わしい場合を含む）は、すぐに社内の連絡ルールに従って、情報セキュリティ責任者に報告します。ネットワークの遮断やシステムの停止を必要に応じて行い、被害の拡大を防ぎます。社外など外部から通報を受けた場合は、通報した人の連絡先を控えておくことも大切です。なお、メール誤送信などの場合は、起こってしまったことを報告しやすい社内風土を作ることも大切です。内部であれ、外部であれ、セキュリティインシデントは人による報告が早期発見につながるからです。

責任者への報告を済ませた後は、初動対応へと移ります。ネットワークの遮断、情報や対象機器の隔離、システムやサービスの停止を必要に応じて行います。

このステップの発見時の社内連絡フロー、初動対応の手順は平常時に定めておくことが大切です。

■事例 A 社の場合：A 社では、セキュリティインシデントとして、パソコンの画面が突然フリーズし「ウイルスにかかっています」と書かれたメッセージが表示されるという事象が発生しました。初動対応としては、この時点で社内に報告し、そのパソコンをネットワークから遮断すべきです。しかし、早急に対処したいと画面に表示されたところに電話をかけ、指示されたとおりにパソコンを操作したところ、遠隔操作によって機密情報が盗まれるという事態に至ってしまいました。

＜ステップ２＞報告・公表

インシデントの影響が広範囲に及ぶ場合、Web サイトやメディアを通じて公表します。

第一報では、公表することで被害の拡大を招かないように、公表する時期や内容などを考慮します。

第二報以降では、被害者や、影響を及ぼした取引先や顧客に対して、インシデントの対応状況や再発防止策等に関して報告します。また、被害者に対する損害の補償等を必要に応じて行います。個人情報漏えいの場合は個人情報保護委員会、業法等で求められる場合は所管の省庁等、犯罪性がある場合は 警察、ウイルス感染や不正アクセスの場合は独立行政法人情報処理推進機構（IPA）へ届け出ます。

＜ステップ３＞復旧

適切な対応や判断を行うために状況を調査し、**インシデント対応時に整理すべき情報（上記表）**を参考に情報を整理します。続いて、訴訟対応等を見越して事実関係を裏付ける情報や証拠を保全します。並行して、システムやサービスを復旧させます。その後、再発防止策を講じ、同様のインシデントが再発しないようにします。例えば、新たなセキュリティツールの導入や従業員の教育強化などを行います。

■事例 B 社の対応：B 社は、ランサムウェア攻撃を受けた際、速やかにバックアップデータを使ってシステムを復旧させました。事前にインシデント対応計画を策定していたおかげで、顧客への影響を最小限に抑えることができました。また、日常的にヒヤリハット事例を収集し、対策を強化していたこともあり、対応をスムーズに進めることができました。

（３）ヒヤリハット事例の活用

「ヒヤリハット」とは、重大な事故には至らなかったものの、注意を怠れば事故に繋がりかねなかった事例を指します。日常業務でのヒヤリハット事例を収集し、共有することで、潜在的なリスクを把握し、予防策を講じることができます。

６．まとめ

セキュリティインシデントへの対策は、事前に発生時の対応手順を定めておくことが大切だとわかっていただけたでしょうか。また、定めた計画や手順どおりに実行できるかを実際にシミュレーションしておくこともとても大切です。また、対応手順は定期的な見直しと改善が重要です。今回ご紹介したポイントを基に、皆さんの企業でも改めて対策を見直してみてください。ヒヤリハット事例の収集と対策も忘れずに行いましょう。

なお、本稿は、IPA が発行している「中小企業の情報セキュリティ対策ガイドライン 第 3.1 版」を中心に解説しています。セキュリティインシデント対応については、ガイドラインの「付録 8 中小企業のためにセキュリティインシデント対応の手引き」にまとめられていますので、もっと詳しく知りたい方はそちらをご参照ください。

次回は、ランサムウェアに感染した場合を例にして、ステップを踏んだインシデント対応をより具体的に解説します。

レベル 3_#5_セキュリティインシデント対応（2/2）
掲載日：2024/8/22



中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。
前回お届けした「セキュリティインシデント対応（1/2）」では、セキュリティインシデントの定義と、実際に発生してしまった時の対応について解説しました。

今回はシリーズ第 2 回として、被害が絶えないランサムウェア攻撃について、インシデントが発生した場合の具体的な対応手順をお伝えいたします。

１． ランサムウェアとは

あらためて、ランサムウェアについて確認しましょう。
ランサムウェアとは、感染したパソコンをロックしたり、ファイルを暗号化して使用できなくする不正プログラムです。ファイルの復元と引き換えに金銭を要求されることから、「ランサムウェア」（ransom（身代金）と software（ソフトウェア）の造語）と言われています。

最近では、サイバー攻撃の一環として「人手によるランサムウェア攻撃」や、情報を窃取しそれを公開すると脅す「二重の脅迫」の被害も報告されています。

独立行政法人情報処理推進機構（IPA）が毎年公表している「情報セキュリティ 10 大脅威」では、10 年以上前の 2012 年版で既に「ランサムウェア(身代金要求型不正プログラム)」として注意を促しています。

また、警察庁が毎年公表している「サイバー空間をめぐる脅威の情勢等について」では、令和 5 年に「ランサムウェア被害の件数が 197 件と高水準で推移するとともに、データを暗号化する（ランサムウェアを用いる）ことなくデータを窃取し対価を要求する手口（ ノーウェアランサム ）による被害が、新たに 30 件確認された。」「都道府県警察から警察庁に報告のあった件数は 197 件であり、令和４年上半期以降、高い水準で推移している。」とあるように、被害件数は年々増加しています。

２． ランサムウェアに感染したら

ランサムウェアに感染すると、以下のような事象が発生します。

（１）ファイルの拡張子が突然変わったり、開けなくなる。
（２）身代金を要求するメッセージが表示される。
（３）コンピュータの動作が急激に遅くなる。
（４）ウイルス対策ソフトが警告を出す。

実際の感染時のデモ動画は、以下のリンクからご覧いただけます。
参考動画：トレンドマイクロ株式会社公式 YouTube

ランサムウェアは被害が表面化しやすく、業務に大きな影響を与えます。あらかじめ感染時の兆候を理解し、対応を決めておくことが重要です。そうしないと、実際に感染した際に対応に戸惑い、パニックに陥る可能性があります。

また、確実に復旧するためには、バックアップからの復元が唯一の手段です。「今まで何も起きていないから感染したらそのとき考えよう」とか「専門家に任せれば何とかなるだろう」という考えは通用しません。

ランサムウェアの被害は 10 年以上被害が増加しており、いかなる組織も例外なく被害に遭う可能性があります。感染後の対応も主体的に検討しておきましょう。

３．ランサムウェアに感染した後の対応

検知と連絡受付	パソコンの画面に身代金を要求するようなメッセージが表示された等、前述の事象を発見したときにはランサムウェア感染の可能性があります。システム管理者、情報セキュリティ管理者等に報告します。
初動対応	感染したパソコンやサーバーの利用を停止し、ネットワークから切り離します。 **【切り離し方】** **＜有線接続の場合＞** （１）ネットワークケーブルを抜く ・パソコンやサーバーの背面や側面にある LAN ポート（ケーブルの差し込み口）を見つけます。 ・ネットワークケーブルをこのポートから抜きます。 （２）ネットワーク設定を無効にする Windows 等 OS の設定でネットワーク接続を無効にします。 **＜無線接続（Windows）の場合＞** （１）Wi-Fi を切断する ・タスクバーのネットワークアイコンをクリックして接続済みの SSID の切断をクリックします。
第二報以降	・影響を及ぼした取引先や顧客に対して、インシデントに関して報告します。 ・ウイルス感染による影響によって、業法等で報告が求められる場合は所管の省庁へ報告します。 ・IPA の届出窓口[※1] へ届け出ます。 ＜IPA コンピュータウイルス・不正アクセスに関する届出について＞ **ランサムウェア被害の届出** ランサムウェア攻撃による被害は、ウイルス届出として取り扱われますが、複雑な攻撃の場合があるため専用の届出様式が用意されています。 下記のコンピュータウイルス届出（ランサムウェア被害）様式に則り、判明している範囲で構いませんので、被害の状況や対応した内容等を記入のうえ、届出先にメールでご送付ください。

	Excel 形式の届出様式をご利用の場合は、「(2)ウイルス届出(ランサムウェア被害)」シートへ記入のうえ届出先にメールでご送付ください。 （様式） コンピュータウイルス届出（ランサムウェア被害）様式 https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/report_ransom_format.txt （届出先） 独立行政法人情報処理推進機構 セキュリティセンター コンピュータウイルス届出窓口 E-mail：virus@ipa.go.jp
調査・対応	・No More Ransom※2 等から復号化ツールを入手し、復旧を試みます、ただし、全てのランサムウェアに対応しているわけではありません。 ・データ等のバックアップを行っている場合は、復元（リストア）します。ただし、バックアップ装置・媒体をパソコンに常時接続している場合、バックアップファイルも暗号化されている場合もあります。 **＜参考＞適切なバックアップ方法** ■原則的にバックアップに使用する装置・媒体は複数用意し、バックアップ時のみパソコンと接続する、またはバックアップしたファイルのうち 1 つはオフサイトに保存する。 また、バックアップの対象がクラウドサービスの場合は、サービスの仕様を確認し、バックアップがサービスに付帯する場合は頻度、保存先、リストア手順について把握しておく。 ■バックアップしたファイルは、定期的に復元（リストア）できるか確認する。復元のテストが難しい場合は、いざというときにバックアップ手順を迷わず実施できるようマニュアル等を整備しておく。 ・復号化ツールでも復旧しない場合、バックアップが復元（リストア）できない場合は、感染した機器やデータの復旧を断念し、再構築します。 ※「3-2-1 ルール」【３分でわかるセキュリティ用語解説＃１】参照 ＜NO MORE RANSOM＞ https://www.nomoreransom.org/ja/

	（ランサムウェアの特定） https://www.nomoreransom.org/crypto-sheriff.php?lang=ja （復号ツール） https://www.nomoreransom.org/ja/decryption-tools.html ＜日本サイバー犯罪対策センター ランサムウェア対策について＞ https://www.jc3.or.jp/threats/topics/article-375.html
復旧	データの復元（リストア）が正しいことを確認できたら、システムを復旧します。

※1 1990 年 4 月に通商産業省（現経済産業省）が告示した「コンピュータウイルス対策基準」、および 1996 年 8 月に同省が告示した「コンピュータ不正アクセス対策基準」（両基準の最終改定は 2000 年 12 月 28 日）に基づき、IPA では国内のコンピュータウイルス（以下、ウイルス）の感染被害やコンピュータ不正アクセス（以下、不正アクセス）被害の届出を受け付けています。
※2 ランサムウェアの被害者が、犯罪者に不当な支払いをすることなく、暗号化されたデータを取り戻すための支援を目的とした国際的なプロジェクトです。

なお、本稿は IPA が発行している「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」を参考に解説しています。

次回は、ホームページやネット通販の EC サイトの対策について解説します。

レベル 3_#6_ウェブサイトのセキュリティ対策（1/3）
掲載日：2024/9/5



中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。

今回はビジネスの中でも重要であり、誰もが利用するホームページやネット通販の EC サイト等、「ウェブサイトのセキュリティ」についてお伝えします。
このシリーズは全 3 回を予定しています。

1．ウェブサイト利用の拡大

近年、スマートフォンの普及により、時間や場所を問わずウェブサイトを利用する人が増えています。商品やサービスの情報収集、インターネット通販でのショッピングやサービスの予約など、ウェブサイトの利用シーンは多岐にわたり、今や生活に欠かせないツールとなっています。
企業にとっても自社のウェブサイトは顧客との重要な接点であり、その運営は顧客獲得や売上向上に直結します。
多くの中小企業も例外ではなく、自社ウェブサイトを活用していますが、これによりセキュリティリスクも増加

しています。

ウェブサイトはインターネット上に公開されているため、世界中の誰でもアクセス可能です。そのため、攻撃の対象になりやすく、悪意のある攻撃者によるサイト改ざんや情報漏えいのリスクが伴います。
ウェブサイトのセキュリティ対策が不十分であれば、顧客情報の漏えいや改ざんによる不正サイトへの誘導が発生する危険性が高まります。それにより、自社だけでなく、利用者にも被害が発生することが懸念されます。
したがって、ウェブサイト運営と同時に適切なセキュリティ対策を講じる必要があるのです。

２．ウェブサイトのセキュリティの必要性

「セキュリティ」という言葉を聞くと、多くの人が秘密情報や個人情報等、非公開の重要情報の漏えい防止を連想します。しかし、企業のホームページなどの公開情報も攻撃の対象となり得るため、セキュリティ対策は不可欠です。
現代のウェブサイトは、単に公開情報であるコンテンツの表示だけでなく、問い合わせフォームや、ショッピング機能を設けたりして、ウェブサイトの利用者から個人情報等を入力させることも多くあります。
利用者から得た情報はウェブサイトのシステム構造によっては、ウェブサーバー内に保存されます。そのため、ウェブサイトのセキュリティ対策を講じていないと、サーバー内の情報を簡単に抜き取られてしまう危険性があるのです。

サイバー攻撃による情報漏えい等の被害がなくならないのは、ウェブサイトに対するセキュリティ対策の必要性を認識せず、対策を講じていないサイトが多数存在することも一因です。被害を防ぐには、ウェブサイトのセキュリティ対策は必須であることを認識することが重要です。

３．ウェブサイトの運用形態の検討

ウェブサイトの利用が拡大する中、企業はどのような形態でサイトを運用するか、慎重に検討する必要があります。
サイト構築から運用するための様々なツールや便利なサービスがあります。企業が自社のウェブサイトを構築し運用する際、利用するツールやサービスの選択肢が増え、利便性が向上している一方で、自社サイトで実現したいことができるかどうかの選別やコスト、運用に必要な技術レベルを考慮する必要があります。

また、運営形態によって、提供できる機能やカスタマイズなどの自由度が異なり、必要なセキュリティ対策も変わってきます。特に個人情報を取り扱う場合、サイト運営者は常に最新の脅威に対し対策ができて

いるか気を配る必要があります。
運営者はウェブサイトを構築する前に、下の表に示す運営形態ごとの特徴を理解し、組織の状況に応じた最適な運営形態を選定する必要があります。

【運営形態ごとの特徴】

運営形態	特徴
サーバー自社設置 （オンプレミス）	ネットワークやサーバーなどの用意から、稼動するウェブサイトの構築・運用まで、全て自社で行う運営形態。全ての情報セキュリティ対策を自社で行う必要があります。
レンタルサーバー・ クラウドサービス （PaaS）	ネットワークやサーバーなどは外部サービスを利用し、ウェブサイトの構築・運用のみ自社で行う運営形態。ネットワークやサーバーの情報セキュリティ対策は外部サービスが行うため、ウェブサイトの構築・運用面に関わる情報セキュリティ対策のみ自社で行う必要があります。
ショッピングモール・ASP	ウェブサイトの開設に必要な機能や運用を一括して外部サービスを利用し、ウェブサイトに掲載する文章や画像、動画などのコンテンツだけを自社で更新する運営形態。外部サービスを利用するための認証情報を、ウェブサイト運営者が適切に管理する必要があります。

４．ウェブサイトの構築

ウェブサイトの「安全上の欠陥」（脆弱性）が狙われる事件が後を絶ちません。サイトの安全を維持するためには、サーバーOS やソフトウェアに対して脆弱性修正パッチの適用や、安全な設定を維持することが重要です。

しかし、独自に開発する「ウェブアプリケーション」※については、情報セキュリティ上の問題が発覚した場合、サービスの継続提供やコストなどの観点から、設計レベルからの修正が難しい場合が少なくありません。そのため、軽減策で対応せざるをえないこともあります。したがって、開発段階において、可能な限り脆弱性を解消することが望まれます。

また、開発を委託して脆弱性が原因で事故が発生した場合、発注者の責任を問われることもあります。そのため、脆弱性対策を要求仕様に盛り込む必要があります。ウェブアプリケーションを開発する際には、必ず脆弱性対策を実施してください。

※インターネットなどのネットワークを介して使用するアプリケーションソフトウェア

５．ウェブサイトの運営

ウェブサイトの安全な運営を実現するためには、サイトを構成する要素ごとに適切なセキュリティ対策を実施することが重要です。例えば、ウェブサーバーの管理、ソフトウェアの更新、アクセス制限、データ暗号化など、多岐にわたる対策が求められます。いずれかの対策が欠けても、ウェブサイトの安全性は確保できません。
これからウェブサイトを構築する場合も、既に運用している場合も、次に示すチェックポイントを参考に、セキュリティ対策の有無について確認してください。

【ウェブサイトのセキュリティ対策チェックポイント】

1	**ウェブアプリケーション**	のセキュリティ対策
2	**ウェブアプリケーションが稼働しているウェブサーバー**	
3	**ウェブサーバーが設置されているルーターやファイアウォール**	
4	**その他バックアップ等**	

なお、本稿は、IPA が発行している「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」を参考に解説しています。

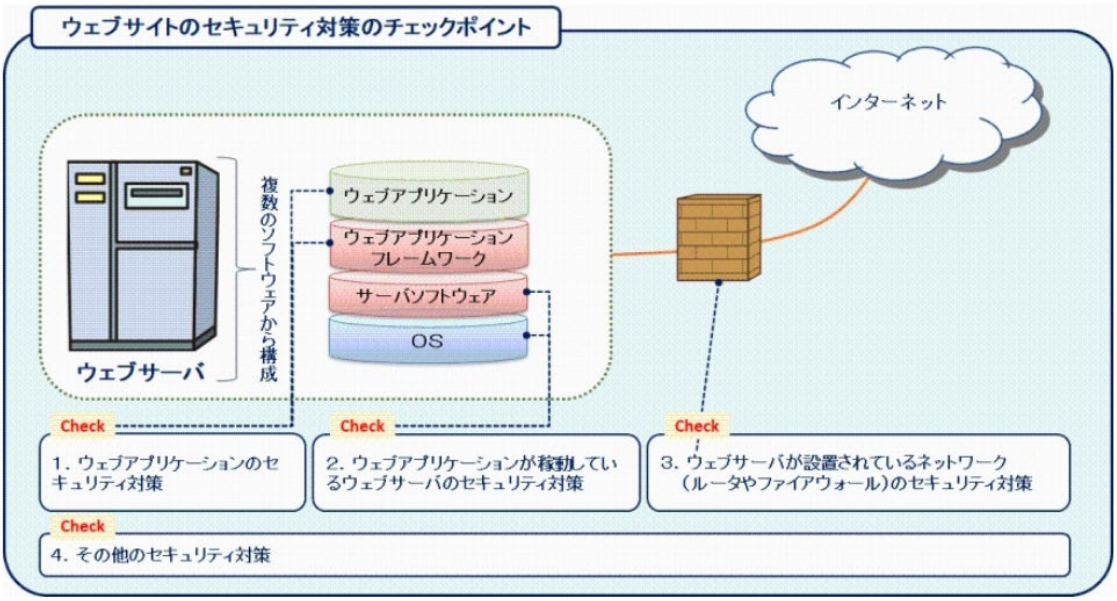
次回は、ウェブサイトのセキュリティ対策について、より具体的に解説します。

レベル 3_#7_ウェブサイトのセキュリティ対策（2/3）
掲載日：2024/9/19



中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。

全３回のシリーズでお伝えしている、「ウェブサイトのセキュリティ対策」。
２回目の今回は、ウェブサイト運営者、システムおよびネットワーク管理者に実行していただきたい「ウェブサイトのセキュリティ対策のチェックポイント 20 ヶ条」のうち、
１．ウェブアプリケーションのセキュリティ対策（ポイント１～８）と、
２．ウェブサーバーのセキュリティ対策（ポイント９～14）について解説します。
※前回の配信はこちら「ウェブサイトのセキュリティ（1/3）」でご覧ください。



引用元：IPA 安全なウェブサイトの運用管理に向けての 20 ヶ条 ～セキュリティ対策のチェックポイント～ より

ウェブサイトのセキュリティ対策のチェックポイント 20 ヶ条

１． ウェブアプリケーション※のセキュリティ対策

※インターネット上で動作するアプリケーションソフトウェアのこと
CMS（コンテンツ管理システム）、EC（ネットショップ、オンラインショップ）、予約システムなど、様々なウェブアプリケーションがあります。

（１）公開すべきでないファイルを公開していませんか？

機密情報や個人情報などの重要な情報を格納したファイルは、公開するファイルとは別に、インターネット上からアクセスできない場所に保管してください。
また、不要なファイルは削除する必要があります。ファイルを誤って公開していた場合、非公開にしたとしても、検索エンジンのキャッシュとして残り、検索に引っかかって閲覧されてしまうことがあります。
非公開にしたファイルが検索エンジンのキャッシュに残っている場合は、Google など運営会社に対して、キャッシュの削除を依頼してください。

（２）不要になったページやウェブサイトを公開していませんか？

期間限定のページや不要になったウェブサイトを公開したまま放置していませんか？
放置したままのサイトがあった場合、日頃から管理していないこともあり、脆弱性が発覚しても認知・対応が遅れ、結果的に脆弱性の影響を受ける恐れがあります。
不要になったページや管理ができていないウェブサイトがないか確認をして、不要なページやウェブサイトは閉鎖してください。

（３）ウェブアプリケーション特有の脆弱性への対策をしていますか？

ウェブサイトは常時攻撃に晒されています。
攻撃の大半はウェブアプリケーションの脆弱性を狙うため、まず、自組織のウェブサイトがどのようなソフトウェアで作られているか把握し、日々公開される脆弱性対策情報※をキャッチアップし、対策が実施されているかを確認してください。

※脆弱性対策情報データベース　JVN iPedia　https://jvndb.jvn.jp/

（４）　ウェブアプリケーションを構成しているソフトウェアの脆弱性対策を定期的にしていますか？

ウェブアプリケーションは様々なソフトウェアやフレームワーク（使用する頻度が高い機能などをパッケージ化したもの）、CMS 等で構成されています。
これらのソフトウェアに脆弱性が発見された場合、適宜バージョンアップ等の対策が必要です。
そのため、自組織のウェブサイトを構成しているソフトウェアの脆弱性を定期的に確認し、発見されたときには、速やかに脆弱性対策をとってください。

（５）　不必要なエラーメッセージを返していませんか？

ウェブアプリケーションのエラーメッセージから、ウェブサイトの設定情報などが漏えいし、攻撃に悪用されることがあります。
このようなメッセージの大部分は、ウェブサイトの閲覧者には不要なものです。
攻撃者に余計な情報を与えないためにも、エラーメッセージの内容は必要最低限にしてください。

（６） ウェブアプリケーションのログを保管し、定期的に確認していますか？

ログは、事故や故障、不正アクセス等の不審な動きがあった際に、原因を追究するための重要な情報源です。
必要に応じてログを保管するとともに、定期的に事故や故障、不正アクセス等の不審な動きがなかったかを確認してください。

（７） インターネットを介して送受信する通信内容の暗号化はできていますか？

ウェブアプリケーションと利用者の間で交わされる通信は、盗聴や改ざん、なりすましなどの被害を受ける恐れがあります。
しかし、通信内容を暗号化（HTTPS 化※）すれば、仮に盗聴などの被害を受けても重要情報が不正に取得されることを防止できます。
そのため、通信内容の暗号化を行う必要があります。ただし、暗号化することにより何らかの支障が発生する場合は、暗号化以外の対策で、盗聴などへの対策を行ってください。

※HTTPS は、HTTP 通信に SSL/TLS 暗号化を追加したプロトコルで、データの盗聴や改ざんを防ぎ、安全にインターネット通信を行うための技術です。

（８） 不正ログインの対策はできていますか？

漏えいした ID やパスワードを悪用した不正ログインにより、情報漏えいや金銭被害などが生じる恐れがあります。
利用者に対して、「複雑で推測されにくいパスワードを設定する」「パスワードを使い回さない」等の対策をアナウンスしてください。
さらに、システム面でも不正ログインを防止する仕組みとして次のような対策を実施してください。
・設定するパスワードは複雑な文字列に制限する
・多要素認証を導入する
・ソフトウェアを定期的にアップデートする

また、不正ログインを検知するサービスの導入も有効です。
不正ログインを検知するサービスには、侵入検知システム（IDS）や侵入防止システム（IPS）があります。
侵入検知システム（IDS）は、疑わしい特定ポートのスキャン、異常なログイン試行、大量のデータ転送

などを検知するシステムです。また、侵入防止システム（IPS）は、疑わしい動きを検出した際、リアルタイムでその侵入をブロックしたり、セッションを終了させたりするシステムです。
これらにウイルス検知など他のセキュリティ機能を組み合わせた UTM（統合脅威管理）があります。

※UTM の詳細については、「UTM」【3 分でわかる！用語解説】の回でご紹介しています。

２．ウェブサーバーのセキュリティ対策

（９） OS やサーバーソフトウェア、ミドルウェアをバージョンアップしていますか？

OS やサーバーソフトウェア、ミドルウェアのバージョンアップは、セキュリティ対策の基本です。修正プログラムが公表された際は適用し、脆弱性を解消してください。
なお、ソフトウェアをバージョンアップした場合、今まで動作していたウェブアプリケーションが正常に動作しなくなる場合があるため、事前にテスト環境で検証する必要があります。

（１０） 不要なサービスやアプリケーションがありませんか？

ウェブサーバー上で不要なサービスが起動している場合、そのサービスが悪用されることがあります。
そのため、最低限必要なもの以外は停止してください。
また、古いバージョンのアプリケーションの脆弱性を攻撃される恐れもあるため、不要になったアプリケーションは削除してください。

（１１） 不要なアカウントが登録されていませんか？

ウェブサーバーやウェブサーバーを管理する端末に不要なアカウントが登録されている場合、悪用される恐れが高まります。
アカウントの一覧を見直して、最低限必要なものを除き、削除してください。
特に、開発工程やテスト環境で使用したアカウントが残っているケースがあるので、確認してください。

（１２） 推測されやすい単純なパスワードを使用していませんか？

推測されやすいパスワードを設定している場合、悪用される可能性が高まります。
推測されにくい複雑なパスワードを設定・使用してください。

特に、管理者権限を持ったアカウントやリモート管理ソフトなどのアプリケーションの場合、狙われて悪用される可能性が高いため、安易なパスワードが設定されていないか、確認してください。
安易なパスワードを使用していた場合、複雑なパスワードに変更してください。

（１３） ファイル、ディレクトリへの適切なアクセス制御をしていますか？

ウェブサーバー上のファイル、ディレクトリに適切なアクセス制御がされていない場合、第三者に非公開のファイルを見られたり、プログラムが実行されたりします。
ファイルやディレクトリのアクセス制御は適切に設定する必要があります。

（１４） ウェブサーバーのログを保管し、定期的に確認していますか？

ウェブサーバー上では各種ログファイル（「システムログ」「アプリケーションログ」「アクセスログ」「データベース操作ログ」など）があります。
これらのログファイルを確認することにより、事故や故障、不審な動き（不正アクセス）があったことに気づくきっかけになります。
また、原因を追究するための重要な情報源ともなります。必要に応じて適切にログを保管し、定期的に確認をする必要があります。

なお、本稿は、独立行政法人情報処理推進機構（IPA）が公表している「安全なウェブサイトの運用管理に向けての 20 ヶ条 ～セキュリティ対策のチェックポイント～」を参考に解説しています。次回は、（15）以降について解説します。

レベル 3_#8_ウェブサイトのセキュリティ対策（3/3）
掲載日：2024/10/3

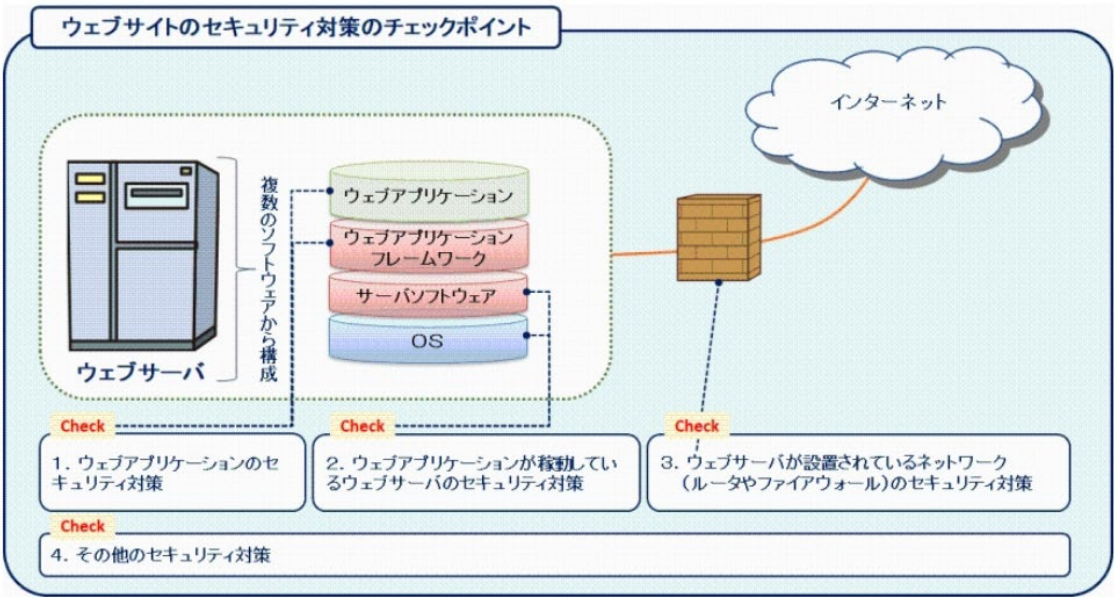


中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。

全３回のシリーズでお伝えしている、「ウェブサイトのセキュリティ対策」。
３回目となる今回は、前回に続きウェブサイト運営者、システムおよびネットワーク管理者に実行していただきたい「ウェブサイトのセキュリティ対策のチェックポイント 20 ヶ条」の後半と、ウェブサイトの中でも特に活用が進んでいる EC サイトのセキュリティ対策について解説します。

ウェブサイトのセキュリティ対策のチェックポイント 20 ヶ条

１．ウェブアプリケーションのセキュリティ対策（ポイント１～８）と、
２．ウェブサーバーのセキュリティ対策（ポイント９～14）は、
前回配信の「ウェブサイトのセキュリティ対策（２/３）」をご覧ください。



引用元：IPA 安全なウェブサイトの運用管理に向けての 20 ヶ条 ～セキュリティ対策のチェックポイント～ より

３．ネットワークのセキュリティ対策

（１５） ルータなどを使用してネットワークの境界で不要な通信を遮断していますか？

境界ルータなどのネットワーク機器を使用して、外部から内部ネットワークへの不要な通信は遮断してください。
運用上、外部から内部ネットワークへの通信が必要な場合は、情報を秘匿するために VPN 等を利用することを検討してください。
内部に侵入された場合、悪用される恐れがあるため、内部から内部ネットワークおよび内部から外部ネットワークへの通信についても、不要と判断される通信は遮断する必要があります。

（１６） ファイアウォールを使用して、適切に通信をフィルタリングしていますか？

ファイアウォールを設置していても、フィルタリングが適切でなければ意味がありません。
「どのサーバー」の「どのサービス」に「どこから」のアクセスを許可するのかを把握し、設定を見直してください。

（１７） ウェブサーバー（または、ウェブアプリケーション）への不正な通信を検知または、遮断していますか？

IDS（Intrusion Detection System 不正侵入検知システム）や IPS（Intrusion Prevention System 不正侵入防御システム）および WAF（Web Application Firewall ウェブアプリケーションファイアーウォール）は、ウェブサイトと利用者の間の通信を検査し、不正な通信を自動的に検知または遮断するソフトウェア、もしくはハードウェアです。
ウェブサイトに脆弱性が発見された場合、ウェブアプリケーションを速やかに修正できないことがあります。
修正されるまでの間、攻撃による影響を低減する対策として IDS や IPS および WAF を導入してウェブアプリケーションを保護することは有効な手段の一つです。

（１８） ネットワーク機器のログを保管し、定期的に確認していますか？

ログは、事故や故障、不審な動きがあった際に原因を追究するための重要な情報源です。
必要に応じてログを保管し、定期的に確認をする必要があります。

４．その他のセキュリティ対策

（１９） クラウドなどのサービス利用において、自組織の責任範囲を把握した上で、必要な対策を実施できていますか？

クラウドやホスティングのサービスを利用してウェブサイトを運営している場合、「ウェブサイトのセキュリティ対策のチェックポイント 20 ヶ条」の（１）～（18）及び（20）で記述したセキュリティ対策をサービス事業者側が提供していることがあります。
クラウドなどのサービスを利用する場合は、サービス事業者側の作業範囲とセキュリティ対策を把握した上で、不足する対策は自組織で対応することを検討してください。

（２０） 定期的にセキュリティ検査（診断）、監査していますか？

組織内部で上記のセキュリティ対策を実施しているか確認した上で、外部の組織によるサーバーやネットワーク機器、ウェブアプリケーションに対する脆弱性検査（診断）やセキュリティ監査を受けることは、対策

漏れなどを洗い出すために効果的な手段です。
公開、運用後は定期的な検査（診断）、監査を継続することが重要です。

EC サイト[※1] のセキュリティ対策

インターネット上に店舗を構え、商品やサービスを販売する EC サイトの活用が中小企業でも進んでいます。
一方、インターネット上の店舗は世界中からアクセス可能であり、絶えずサイバー攻撃に晒されています。
そのため、中小企業が EC サイトで取り扱うクレジットカード情報や個人情報・仕入先情報などの漏えい事件が多数発生しています。
さらに、対策としてカード情報を「非保持化[※2]」しているにも関わらず、購入者に偽の入力画面を表示し、入力させた情報を盗むという巧妙な手口により、被害が増加しています。

EC サイトが被害を受けた場合は、サイトの一時閉鎖や原因調査に加え、顧客への謝罪や事故対応費用の負担など経済的損失が発生します。
企業としての信頼も大きく損なわれ、売上が回復するまで多くの時間を要します。
被害を防ぐために、下記に示す運営形態ごとのセキュリティ対策を参考に、自社の対策を確認し、十分な対策を講じてください。

※1　EC（Electronic Commerce 電子商取引）「ネットショップ」「オンラインショップ」「ネット通販サイト」などの呼称があります。いくつかある決済方法のうちクレジットカード払いが約 8 割（総務省　令和 3 年情報通信白書）で最も多くなっています。

※2　自社で保有する機器・ネットワークにおいて「カード情報」を「保存」、「処理」、「通過」しないこと。
割賦販売法　第 35 条の 17 の 9「販売店におけるクレジットカードの適切な取り扱い」では、販売店におけるクレジットカード番号等取扱契約の締結に係る業務に関して、クレジットカード番号を保有しない等、クレジットカード番号等に関する情報の適切な管理のために必要措置を講じる責任を負う、としています。

【EC サイト運営形態とセキュリティ対策】

EC サイト運営形態		セキュリティ対策 A：構築・運営の各段階で対策が必要 B：公表される情報をもとに脆弱性の修正が必要 C：パッケージ製品 / サービス提供者の情報を元に脆弱性の修正が必要 D：運営事業者のセキュリティ対策を確認		
		ウェブアプリケーション	ウェブサーバー	ネットワーク
1	EC サイトを自社で独自開発	A	サーバー自社設置：A または B レンタル / クラウドサーバー：C	
2	EC サイト用オープンソースソフトウェアを利用	B		
3	EC サイト用パッケージを利用	C		
4	EC サイト用クラウドサービス /ASP を利用	D	D	D
5	オンラインショッピングモールに出店・出品	D	D	D

引用資料：「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」【表１０】

なお、本稿は、独立行政法人情報処理推進機構（IPA）が公表している「安全なウェブサイトの運用管理に向けての 20 ヶ条 ～セキュリティ対策のチェックポイント～」「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」を参考に解説しています。

次回は、ネットワーク対策などの技術的対策について解説します。

レベル 3_#9_技術的セキュリティ対策（1/2）
掲載日：2024/10/17



中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。

セキュリティ対策に必要な考え方として、「組織・人的対策」「物理的対策」「技術的対策」という３つの分類があります。

「組織・人的対策」は、守秘義務契約などのセキュリティに対しての社内ルールを設定する対策です。ルールを設定するだけではなく、実現するための社内教育も重要となります。
「物理的対策」は、入退室・施錠管理や盗難・災害といった物理的要因に対する対策を指します。
そして「技術的対策」は、ハードウェア・ソフトウェアやネットワークなどの技術的な対策を行うことです。今回は、この技術的対策について解説します。

１．技術的対策の重要性

IT を活用するうえでセキュリティを向上するには組織・人的対策、物理的対策では限界があり、環境に

応じた技術的対策が必要です。
ところが技術的対策は一般の人には難解なため、おろそかになりがちです。これはサイバー攻撃者が効率的に成果を挙げるために都合がよく、その結果、サイバー攻撃による被害が後を絶ちません。

２．技術的対策例と活用

技術的対策のために必要な製品、ソフトウェア、サービスは様々なものが提供されています。
攻撃手法は日々多様化、複雑化しているため、技術的対策も随時、対策の見直しや更新を行い、最新の状態にしていくことが必要となります。
以下に代表的な技術的対策を挙げるので、自社の環境に合わせて導入を検討し、活用してください。

（１）ネットワーク脅威・端末対策

ネットワークの境界付近に配置して通信の処理や監視を行い、不正な通信の制御と管理を行うことで対策を実施します。

●ファイアウォール
通信をさせるかどうかを判断し、許可または拒否する技術です。
例えば、インターネットと社内 LAN との間に設置して、外部からの不正なアクセスが社内のネットワークに侵入するのを防ぎます。

●IDS（Intrusion Detection System：侵入検知システム）
システムやネットワークに対する不正なアクセスなどを検知して、管理者に通知する技術です。
例えば、インターネットとファイアウォールの間に設置することで、不正アクセスと思われる通信を検知して管理者に通知できます。

●IPS（Intrusion Prevention System：侵入防御システム）
システムやネットワークに対する不正なアクセスなどを検知して、自動的に遮断する技術です。
例えば、インターネットとファイアウォールの間に設置することで、不正アクセスと思われる通信を検知して管理者に通知するとともに、通信を遮断できます。

●UTM（Unified Threat Management：統合脅威管理）
ファイアウォールや IDS・IPS、メールフィルタリング、URL フィルタリングなど複数の異なるセキュリティ機能を一つのハードウェアに統合して、社内ネットワークとインターネットの脅威であるウイルスの侵入や不正アクセ

ス、サイバー攻撃などを検知し、防御するツールです。
※UTM についてはこちらの記事で解説しています。「UTM」【3 分でわかる！用語解説＃３】

●EDR（Endpoint Detection and Response）
ネットワークに接続されたパソコンやサーバー、スマートフォンなどの端末機器に侵入したウイルスやランサムウェアなどのサイバー攻撃を検出し、管理者に通知する技術です。
※EDR についてはこちらの記事で解説しています。「EDR」【3 分でわかる！用語解説＃２】

●WAF（Web Application Firewall）
ウェブアプリケーションの脆弱性を悪用した攻撃から、ウェブアプリケーションを保護する技術です。
例えば、ファイアウォールや IDS・IPS とウェブサーバーの間に設置することで、ウェブアプリケーションがやり取りするデータを監視して攻撃を検出できます。

●VPN（Virtual Private Network）
インターネットのような公衆ネットワーク上で、保護された仮想的な専用線環境を構築する技術です。
例えば、テレワーク勤務者が職場との間で機密性の高い電子データをやり取りする際に、VPN を利用することで暗号化による安全な通信が可能になります。
※VPN についてはこちらの記事で解説しています。「VPN とゼロトラスト」【3 分でわかる！用語解説＃４】

（２）コンテンツセキュリティ対策

プログラム実行や電子メール送受信、ウェブ閲覧などを、その内容（コンテンツ）によって制御することで対策を実施します。

●ウイルス対策
ウイルスを検知・駆除することで、ウイルスに感染するのを防ぐための対策です。
例えば、利用するパソコンにウイルス対策ソフトをインストールしてウイルス定義ファイルを最新の状態にすることで、既知のウイルスを検知できます。

●メールフィルタリング
メールの送受信を監視して、指定した条件によって特定の処理を実行する技術です。
例えば、メールサーバーにフィルタリング機能を設定することで、迷惑メールやウイルスが添付されたメールをブロックできます。

●URL フィルタリング

ウェブサイトへのアクセスや閲覧について、そのアドレスや内容が所定の条件に合致もしくは違反する場合に、アクセスの停止や警告などを行う技術です。

例えば、URL フィルタリング機能を持つ機器を導入することにより、業務に関係がないウェブサイトの閲覧を禁止し、不正サイトへアクセスしてしまうリスクを減らすことができます。

（３）アクセス管理

情報システムの利用者を、認可及び制限する機能を提供します。

●アクセス制御

利用者や情報機器がデータなどにアクセスすることができる権限や認可を制御する技術です。

例えば、業務で使用するクラウドサービスなどを事務所のみで利用可能とするアクセス制御を行うことで、事務所外からデータへの不正アクセスのリスクを軽減できます。

●多要素認証

サービス利用時に行う利用者認証を、３つの要素（（１）知っているもの、（２）持っているもの、（３）本人自身に関するもの）のうち、２つ以上の要素を用いて行う技術です。

例えば、職場の入退室管理システムを利用する際に、本人のみが持つ IC カード認証に本人のみが知るパスワード認証を追加することで、本人からのアクセスに限定することができます。

●特権 ID 管理

情報システムの特権（コンピュータを管理するために与えられた最上位の権限）の利用申請や権限付与、操作ログなどを管理する技術です。

例えば、サイバー攻撃や内部不正などによる、特権の不正利用を防止し、リスクを軽減することができます。

（４）システムセキュリティ管理

組織が保有する IT 資産について、一元的な管理や脆弱性を検出する機能を提供します。

●IT 資産管理

パソコンやサーバーなどのハードウェアやソフトウェアの保有状況・構成情報を取りまとめて管理する技術です。

例えば、IT 資産管理ツールを導入することで、セキュリティパッチの適用状況を把握することができ、脆弱

性に対する攻撃のリスクを軽減することができます。

●脆弱性検査

サーバーやアプリケーションに対してスキャニングを行い、脆弱性などがないか検査を行います。
例えば、サービス提供前のウェブアプリケーションに対して、脆弱性検査を行うことで、既知の脆弱性の有無を点検することができます。
脆弱性がある場合は、脆弱性があるサーバーやアプリケーションに対し、脆弱性修正パッチの適用や安全な設定などの対策を速やかに実施することで、攻撃のリスクを軽減することができます。

●ログ管理

サーバーなどに誰がログインしたか、どのデータに対してアクセスがあったかは、サーバー上にログファイルとして記録されます。
ログファイルの内容はサーバーなどの運用期間に応じて増えていくので、一定期間（例えば１週間、３か月、１年などの期間）で自動的に削除されるように設定されているのが一般的です。
サイバー攻撃があった場合、このログファイルに書かれている内容をもとに、情報漏えいが生じたかどうかを分析するので、ログファイルをどのように管理するかの方針を、組織として定めておくことは重要です。
一方で、ログファイルの内容を十分に理解するには専門的な知識が必要となるため、こうした管理を容易にするためのツール類も提供されています。

なお、本稿は、独立行政法人情報処理推進機構（IPA）が公表している「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」を参考に解説しています。

次回は、データの暗号化、安全消去に関する技術的対策について解説します。

レベル 3_#10_技術的セキュリティ対策（2/2）
掲載日：2024/10/31



中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。

本シリーズ２回目となる今回は、技術的セキュリティ対策のうち身近でありながら誤解も多いデータの暗号化、安全消去について解説します。
なお、前回は技術的対策に必要となるセキュリティソフトウェアやサービスとその活用法について解説しているので、そちらもぜひご覧ください。
（前回の記事はこちら）技術的セキュリティ対策（1/2）

１．データの暗号化

昨今、コンピュータとインターネットの利用は、業務でもプライベートでも不可欠になりました。インターネットは誰でも利用可能なネットワークのため、暗号化は、盗聴・改ざん・漏えいなどを防止し、セキュリティとプライバシーを守るために必須の技術です。

そのような背景から、コンピュータとインターネットの普及に伴い、「逆さ読み」などの古典暗号から、数学を応用した現代暗号が生み出されました。現代暗号の技術には様々な方法があり、それぞれ異なる目的やセキュリティ要件に応じて使用されています。
ここではパソコンなどに保存するデータの暗号化と、インターネットを利用するときの通信の暗号化について解説します。

●データ暗号化
特定の法則に基づいてデータを変換し、第三者に内容を知られないようにする技術。
例えば、サーバー、パソコン、電子媒体をディスクまたはファイル単位で暗号化することで、メール送信時の添付ファイルの盗聴、社外からの不正アクセスによるデータの持ち出し、パソコンや電子媒体の紛失や盗難などによる情報漏えいのリスクを低減することができます。

代表的なものに、暗号をかける人と、暗号を解く人が共通の同じ鍵を持つことを前提とした「共通鍵暗号（対称鍵暗号）」の技術で AES（Advanced Encryption Standard：現代の標準的な対称鍵暗号で高いセキュリティを提供します）があります。
Microsoft Office（Word、Excel、PowerPoint など）のパスワード使用による暗号化には、AES が使用されています。

●通信暗号化
特定の法則に基づいて通信を変換し、第三者に傍受・盗聴されないようにする技術。
通信を暗号化する場合、授受する 2 者間で鍵を共有しなければなりません。しかし、秘密である鍵をインターネット経由で送ると、通信経路上、第三者に傍受され、解読されてしまうリスクがあります。
では、場所を隔てた 2 者間で、インターネットを使って安全に鍵を共有するには、どうしたらよいのでしょうか？この問題は「公開鍵暗号」の発明によって解決されました。

「公開鍵暗号」は、秘密の鍵を 2 者間で共有しなければならない「共通鍵暗号」の本質を覆す画期的な発明でした。
「公開鍵暗号」では暗号化する鍵と復号する鍵とが異なり、暗号化する人は復号する鍵を知らなくても暗号化することができます。そこで暗号化する人は、相手が持っている「暗号化しかできない鍵」を公開してもらい、暗号化して相手に送ります。このとき通信経路で鍵が傍受されても、「暗号化しかできない鍵」なので解読されることはありません。受け取った相手は、自分だけが持っている「復号しかできない鍵」を使って元に戻します。

インターネット経由でデータの通信を行うとき、データを保護するために用いられる暗号化や認証のための技術規格のうち、最も普及しているものの 1 つが、この「公開鍵暗号」の技術である TLS*です。一般的なウェブブラウザはすべて TLS に対応しているので、改めて導入する必要がないメリットがあり、世界的に

広く利用されています。
*過去に SSL（Secure Sockets Layer）として規格化され、現在は TLS（Transport Layer Security）という名前で国際標準となっていますが、TLS のことを今でも SSL と呼んでいる場合もあります。

２．データの破棄

情報システムを使わなくなった場合、システム内にデータを保存したまま放置したり、廃棄したりすると、それが情報漏えいの原因となるため、速やかにデータの消去を行う必要があります。
またクラウドサービスの場合も、不要となったデータをクラウド上に保存したままにするのは、情報漏えいのリスクを不必要に高めることにつながります。

電子的なデータは、人には直接見えない形で、磁気パターンや電気的、または光学的な形で記録されています。これらは目に見えない「ビットとバイト」の集まりにすぎず、コンピュータを使わないと読解することができません。そのため、データが保存されている場所や形は直感的に理解しづらく、二度と復元できないように破棄・消去するには、正しい方法で行う必要があります。

よく使う Windows の削除やフォーマットでは、データが完全に消去されません。
これらの操作では、データそのものはディスク上に残っており、ファイルの参照情報、図書に例えると目次だけが削除され、本文は削除されていない状態です。そのため、復元ツールを使用すると、消去したデータが復元できてしまいます。

以下に電磁記録媒体の種類別に完全な破棄・消去の方法を説明します。

（１）HDD（ハードディスクドライブ）・CD 等の光ディスク

●上書き
データを上書きして消去する方法です。複数回実施することで、データの復元難易度を高めることができます。ただし、複数回実施しても最新の技術や強力なリカバリツールにより完全な消去が保証されるわけではありません。光ディスクは DVD-RW、BD-RE など書き換え可能ディスクが対象になります。専用のツールが流通していますので、それらを使用します。

●消磁
磁気を使ってデータを消去する方法です。専用の機器が必要であり、全てのハードディスクで使用できるわけではありません。また、HDD の磁気ヘッドを完全に消去するため、再利用はできません。光ディスクは

対象外です。

●物理破壊

物理的に破壊することでデータを確実に消去します。破壊は、ハンマーでの打撃や、専用のシュレッダーで行います。光ディスクに傷をつける場合は、データを記録するための薄い金属の「反射層」を破壊する必要がありますが、記録面（銀色や青い部分）は厚い樹脂で保護されているため、傷が浅いと「反射層」に達しません。ラベル面（記録面の裏）に傷をつけたほうが「反射層」に達しやすく確実に破壊することができます。

（２）SSD（ソリッドステートドライブ）

SSD とは、記憶媒体にフラッシュメモリを用いる外部記憶装置です。HDD と比べデータ読み書き速度が速く、小型で軽量なためスマートフォン、モバイル機器や USB メモリなどに使われています。SSD のデータ消去は、データを管理する方式が HDD とは異なるため上書きでは完全な消去が難しいことがあります。

●暗号化消去

データが保存されている領域を暗号化し、その暗号化キーを破棄する方法です。これにより、データが実質的に読み取れなくなります。暗号化消去は、ドライブ内の全データを迅速に消去する方法ですが、暗号化の管理が適切に行われていることが前提です。機器に暗号化機能がない場合は、専用のツールを使用します。

●工場出荷時リセット

SSD のファームウェアが提供するリセット機能を使って、データを消去する方法です。
ただし、すべての SSD がこの方法に対応しているわけではありません。

●物理破壊

SSD を物理的に破壊することでデータを確実に消去します。

（３）クラウドサービス

クラウドサービスのデータ消去はプロバイダーに依存するので、サービス契約に基づく明確な消去手順を確認することが重要です。
データ消去後の残存データ（例えば、バックアップやキャッシュ）の管理についても考慮が必要です。

●サービスプロバイダーによる消去

クラウドサービスのプロバイダーは、消去を実施することができますが、契約やサービスレベルアグリーメント（SLA）に従ってデータが適切に消去されることを確認する必要があります。

●消去要求

ユーザーは、クラウドサービスの管理コンソールやサポートを通じてデータ消去を要求することができます。これには、アカウントの削除や特定のデータセットの消去が含まれます。

●暗号化

クラウドサービスに保存されているデータを暗号化することで、情報漏えいのリスクを低減できます。暗号化されたデータが物理的に消去されなくても、暗号化キーの削除により復元できなくなります。

なお、本稿は、独立行政法人情報処理推進機構（IPA）が公表している「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」を参考に解説しています。

次回は、監査・点検の効果的な実施方法について解説します。

レベル 3_＃11_情報セキュリティの見直しと強化（監査と点検）（1/3）
掲載日：2024/11/14



中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。
本メールマガジン（HP では記事）では、組織における情報セキュリティへの取り組みを評価して、さらなる改善へと導くための監査・点検の重要性とその実施方法について説明します。

１．情報セキュリティの重要性と監査・点検の必要性

今日のデジタル社会では、セキュリティインシデントが企業に甚大な影響を及ぼすことがあります。特にサイバー攻撃は手口が高度化し増加し続けています。このような中で、個人情報や機密情報の保護は企業活動において不可欠です。情報漏えいやシステムダウン等の事態が発生すれば、企業の信頼を失墜させかねません。したがって、情報セキュリティ対策は経営戦略の重要な一部として位置づけられ、定期的な監査と点検によってその有効性を評価し続けることが求められます。

２．監査と点検の役割と違い

「監査」と「点検」という言葉は、情報セキュリティだけでなく、様々な分野で使われています。
「監査」には、会計監査、業務監査、監査役監査などがあります。
「点検」には、自動車の日常点検と定期点検、ガス設備定期保安点検、消防用設備等の点検などがあり、経験がある人も多いのではないでしょうか。

監査と点検は、どちらも何かしらの基準と実際の状態や状況を比較し、そのギャップを確認する行為です。
それぞれの違いについて、明確な定義はありませんが※1、一般的には以下のように区分されています。

用語	範囲	実施主体	特徴
監査	組織全体または特定部門	監査担当者や外部専門家	独立性・客観性を重視
点検	特定の業務や設備	業務や設備の担当者	問題の早期発見・予防を重視

監査は対象業務に従事していない他部署や取引先など、独立した立場の監査担当者によって実施されるものに対し、点検は担当者自身が実施します。
従って、客観的かつ専門的な確認を行う場合には監査が適しており、適時簡易に確認する場合には点検が適しています。
状況に応じて使い分けることで効果的なセキュリティ対策が可能となります。

※1 経済産業省「情報セキュリティ監査基準」では次のように説明しています。
情報セキュリティ監査は、独立かつ専門的な立場から、組織体の情報セキュリティの状況を検証又は評価して、情報セキュリティの適切性を保証し、情報セキュリティの改善に役立つ的確な助言を与えるもの

３．効果的な情報セキュリティ監査・点検の実施方法

情報セキュリティの監査と点検を効果的に進めるためには、以下の事柄を確認します。

- セキュリティルールの徹底
  一般に必要とされる情報セキュリティ対策を基準として、組織内で策定されたセキュリティルールがしっかりと周知・実行されているか確認します。
- 潜在的なリスクの特定
  現行のシステムやプロセスにおける見落としや潜在的なリスクはないか確認します。不十分な点があれば、必要な改善策を講じます。
- 事故防止対策の検証

現行の対策の有効性やセキュリティ事故の防止に役に立っているかを検証し、必要に応じて改善策や新たな対策の導入を検討します。

監査・点検には、以下の方法があります。

質問（インタビュー）	従業員や委託先の管理者などに直接質問して回答してもらう
閲覧（レビュー）	関連する文書や記録、パソコンの設定画面など対策を実行した証拠となるものを確認する
観察（視察）	点検の対象となる職場に出向き、従業員が規程や標準規格などに従った行動をしていることを確認する
技術診断	専用ソフトウェアなどを使ってコンピュータやネットワークのセキュリティ対策が実行されているかを確認する
チェックリスト	チェックリストや質問書を配付して回答してもらう

ここでは例として、監査・点検の基準に独立行政法人情報処理推進機構（IPA）の公表資料「情報セキュリティ５か条※2」を用いた進め方を解説します。

※2「情報セキュリティ５か条」
https://www.ipa.go.jp/security/sme/f55m8k0000001wb3-att/000055516.pdf

４．監査・点検の進め方の例

「情報セキュリティ５か条」を監査・点検の基準に用いて「質問（インタビュー）」「閲覧（レビュー）」を行う場合、以下のステップに沿って進めていきます。

（１）「情報セキュリティ５か条」を基準にする。

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！

（２）5 か条のうち「1. OS やソフトウェアは常に最新の状態にしよう！ 」に示された対策例の実施状況を確認する。

1．OS やソフトウェアは常に最新の状態にしよう！	
対策例	• **WindowsUpdate（WindowsOS の場合）、ソフトウェア・アップデート（macOS の場合）などベンダの提供するサービスを実行する。** • Adobe Reader、ブラウザなど利用中のソフトウェアを最新版にする。 • テレワークで利用するパソコン等のソフトウェアやルーター等のファームウェアを最新版にする。 • 利用中のソフトウェアに脆弱性が存在しないか、MyJVN バージョンチェッカ※で確認する。 ※パソコンにインストールされているソフトウェア製品が最新かどうかを簡単な操作で確認できるツール https://jvndb.jvn.jp/apis/myjvn/

【手順１】従業員に、パソコンの WindowsUpdate 画面を開いてもらい、以下を確認する。

・「最新の状態です」または「更新プログラムを利用できます」「利用可能な更新があります」のいずれが表示されているか。

・その他のオプション「利用可能になったらすぐに最新の更新プログラムを入手する」がオンになっているか。

【手順２】「更新プログラムを利用できます」「利用可能な更新があります」と表示された場合、または「利用可能になったらすぐに最新の更新プログラムを入手する」がオフの場合は、最新の状態にしていない理由を訊ねる。

【手順３】回答から「セキュリティ事故防止のために役に立っているか？」を判断し、必要に応じて、助言や改善を依頼する。

回答例	改善依頼・助言例
• アップデートが始まると、完了するまでパソコンが使えなくなることがあるので更新プログラムの入手をオフにした。 • アップデートのリリース時に、たまたまネットワークに接続していなかったのでアップデートを後回しにしてパソコンを使っていた。	• 更新プログラムの入手をオンにしてアップデートを業務時間外に設定してもらう。 • アップデートしてからパソコンを使うようにしてもらう。
• OS をアップデートすると利用している業務システムの動作が保証されないので更新プログラムの入手をオフにしている。	• 業務システムが最新版の OS に対応しているかメーカーに問い合せてもらう。 • 対応している場合は業務システムもアップデートし

• サポートが終了した OS で動く業務システムを使っているため、アップデートすることができない。	てもらう。 • 対応していない場合は以下を遵守してもらう。 ① インターネットに接続しない。 ② 外付け HDD や USB メモリ等の外部メディアに接続する時には場合には必ずパターンファイルを更新したウイルス検知ソフトでスキャンしてから接続する。

５．情報セキュリティ監査・点検の基準

情報セキュリティの監査・点検を実施するには、判断の根拠となる基準が必要です。
情報セキュリティ監査・点検の基準として利用できる資料は、公的機関が無償で提供しているものがあります。
社内の環境や取り組みレベルに合わせて、活用してください。

＜IPA＞
『情報セキュリティ 5 か条』
https://www.ipa.go.jp/security/sme/f55m8k0000001wb3-att/000055516.pdf
『5 分でできる！情報セキュリティ自社診断』
https://www.ipa.go.jp/security/sme/f55m8k0000001waj-att/000055848.pdf

＜東京都＞
『中小企業向けサイバーセキュリティ対策の極意』MISSION2 すぐやろう！対サイバー攻撃アクション
https://www.cybersecurity.metro.tokyo.lg.jp/security/docs/CyberSecurity.Ver.2.2a.pdf

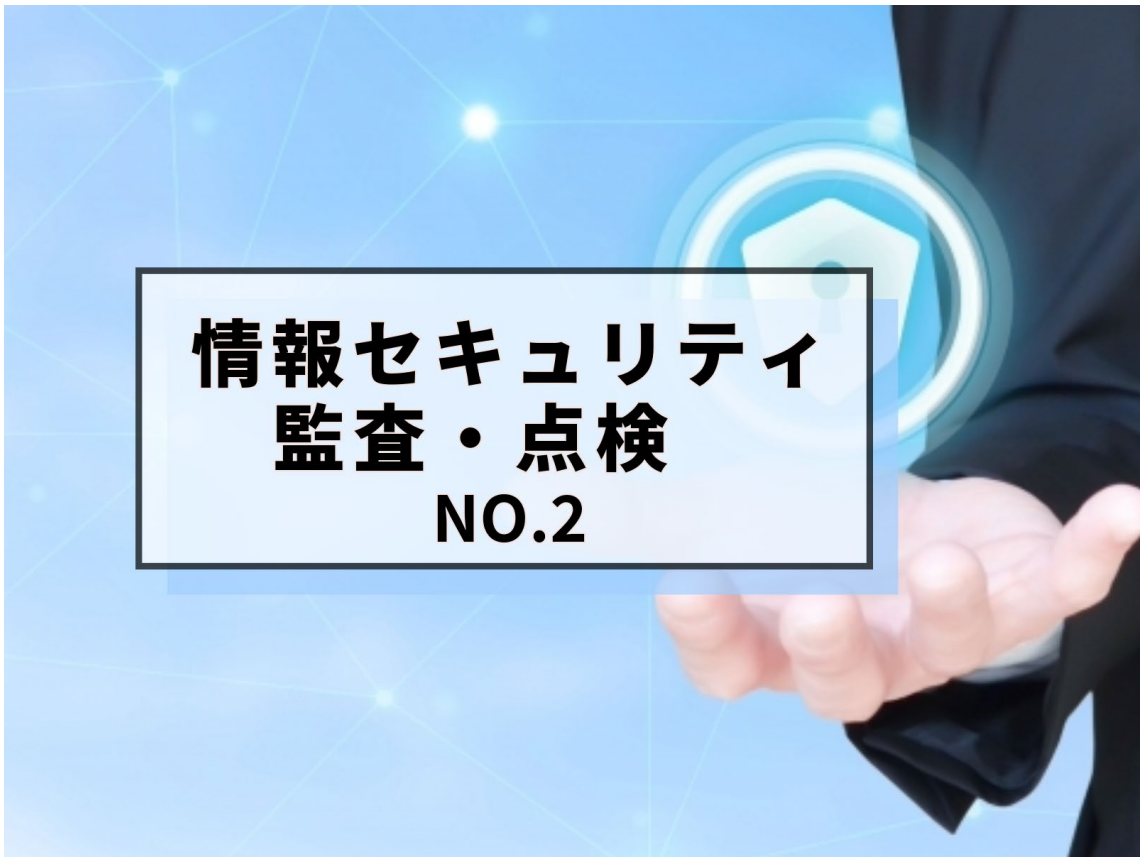
＜経済産業省＞
『情報セキュリティ管理基準』
https://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Management_Standard_H28.pdf

＜内閣サイバーセキュリティセンター＞
『政府機関等のサイバーセキュリティ対策のための統一基準』（令和 5 年度版）
https://www.nisc.go.jp/pdf/policy/general/kijyunr5.pdf

なお、本稿は、IPA が発行している「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」を参考に解説しています。

次回は、「監査・点検結果をどのように活かすか？」について解説します。

レベル 3_#12_情報セキュリティの見直しと強化（監査と点検）（2/3）
掲載日：2024/11/28



中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。
本記事では、組織における情報セキュリティへの取り組みを評価して、さらなる改善へと導くための監査・点検の重要性とその実施方法について説明します。

全 3 回にわたってお伝えするこのシリーズ。2 回目となる今回は、実施した監査と点検の結果をどのように活かすかに焦点を当てます。

前回の記事はこちら：「情報セキュリティの見直しと強化（監査と点検）（1/3）」

１．監査・点検における経営者の役割

品質管理や業務改善においてよく使われる経営管理手法に PDCA サイクルがあります。
PDCA サイクルとは、計画（Plan）→ 実行（Do）→ 確認（Check）→ 改善（Act）の 4 段階で構成され、多くの企業で使用されています。

監査・点検は、この PDCA サイクルの「確認（Check）」に該当します。

現代では、企業の競争力を維持・強化するためのデジタルトランスフォーメーション（DX：Digital Transformation）の推進が重要な経営課題として挙げられています。この DX を推進するうえで、情報セキュリティへの対策が必要不可欠です。
経営者は情報セキュリティ監査および点検の結果を適切に活かし、組織全体のセキュリティ水準を高めることが求められます。

２．経営者が実行すべき「重要７項目の取組」

中小企業で情報セキュリティを確保するために、経営者は以下の「重要７項目の取組」を推進する必要があります。これには情報セキュリティポリシーの策定や、実際に情報セキュリティ対策を実践するうえでの責任者・担当者に明確な指示を出すことが含まれます。
場合によっては、情報セキュリティの責任者として経営者自らが実行することも必要になると考えられます。

取組１	**情報セキュリティに関する組織全体の対応方針を定める**
情報セキュリティ対策を組織的に実施する意思を、従業員や関係者に明確に示すために、どのような情報をどのように守るかなどについて、自社に適した情報セキュリティに関する基本方針を定め、宣言します。 自社の経営において最も懸念される事態は何かを明確にすることで具体的な対策を促し、組織としての方針を立てやすくなります。	
取組２	**情報セキュリティ対策のための予算や人材などを確保する**
情報セキュリティ対策を実施するために、必要な予算と担当者を確保します。 これには事故の発生防止だけでなく、万が一事故が起きてしまった場合の被害の拡大防止や、復旧対応も含みます。 情報セキュリティ対策には高度な技術が必要なため、専門的な外部サービスの利用も検討します。	
取組３	**必要と考えられる対策を検討させて実行を指示する**
懸念される事態に関連する情報や業務を整理し、損害を受ける可能性（リスク）を把握したうえで、責任者・担当者に対策を検討させます。 必要とされる対策には予算を与え、実行を指示します。 実施する対策は、社内ルールとして文書にまとめておけば、従業員も実行しやすくなり、取引先などにも取り組みを説明する際に役に立つので、併せて指示します。 実行を指示した情報セキュリティ対策がどのように現場で実施されているかにつき、月次や四半期ごとなど適切な機会をとらえて報告させ、進捗や効果を把握します。	
取組４	**情報セキュリティ対策に関する適宜の見直しを指示する**
取組３で指示した情報セキュリティ対策について、実施状況を点検させ、取組１で定めた方針に沿って進んで	

いるかどうかの評価をします。 また業務や顧客の期待の変化なども踏まえて基本方針なども適宜見直しを行い、致命的な被害につながらないよう、対策の追加や改善などを行うように、責任者・担当者に指示します。
取組５　緊急時の対応や復旧のための体制を整備する
万が一に備えて、緊急時の対応体制を整備します。被害原因を速やかに追究して被害の拡大を防ぐ体制を作るとともに、的確な復旧手順をあらかじめ作成しておくことにより、緊急時に適切な指示を出すことができます。 整備後には予定どおりに機能するかを確認するため、被害発生を想定した模擬訓練を行うと、意識づけや適切な対応のために効果的です。 経営者のふるまいについても、あらかじめ想定しておけば、冷静で的確な対応が可能になります。
取組６　委託や外部サービス利用の際にはセキュリティに関する責任を明確にする
業務の一部を外部に委託する場合は、委託先でも少なくとも自社と同等の対策が行われるようにしなければなりません。 そのためには契約書に情報セキュリティに関する委託先の責任や実施すべき対策を明記し、合意する必要があります。 IT システム（電子メール、ウェブサーバー、ファイルサーバー、業務アプリケーションなど）に関する技術に詳しい人材がいない場合、自社でシステムを構築・運用するよりも、外部サービスを利用したほうが、コスト面から有利な場合がありますが、安易に利用することなく、利用規約や付随する情報セキュリティ対策などを十分に検討するよう担当者に指示する必要があります。
取組７　情報セキュリティに関する最新動向を収集する
情報技術の進化の早さから、実施を検討するべき対策は目まぐるしく変化します。 自社だけで把握することは困難なため、情報セキュリティに関する最新動向を発信している公的機関などを把握しておき、常時参照することで備えるように情報セキュリティ担当者に指示します。 また、知り合いやコミュニティへの参加で情報交換を積極的に行い、得られた情報について、業界団体、委託先などと共有します。

３．監査・点検結果を経営管理に活かす

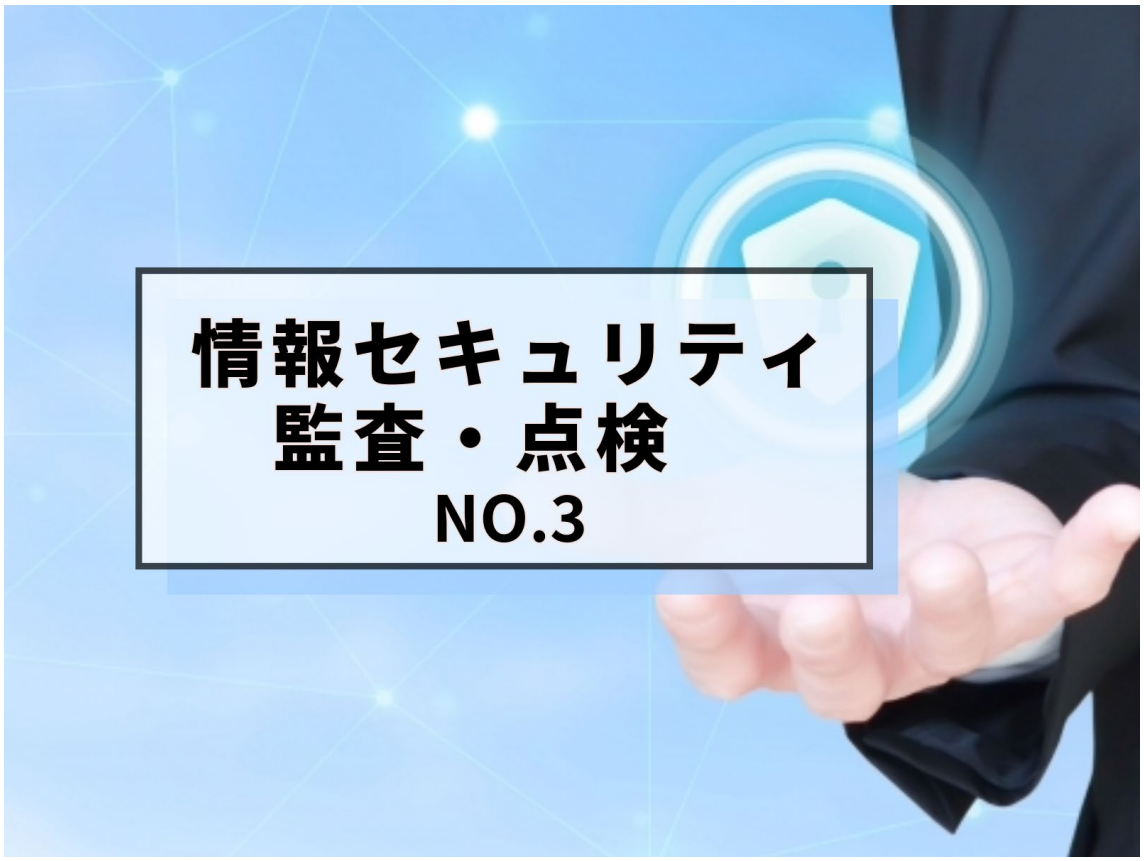
経営者にとって、前述の「重要７項目の取組」を通じて、情報セキュリティの確保が会社にとって不可欠であることは理解できても、社内の実施状況を正確に把握し、適切な対策を講じることはなかなか難しい課題です。
経営者が状況を把握できていないと、的確な意思決定や指示、命令が疎かになり、事故発生のリスクが大きくなってしまいます。

そこで、監査や点検の結果を経営者に報告し、経営者が意図するセキュリティ対策が実現できているか

評価することが極めて重要です。
これにより、経営者は社内の情報セキュリティの状況を適宜把握することができ、精緻にリスク管理と改善を図ることが可能になります。
このような取り組みによって、企業全体のセキュリティ水準を向上させることが期待できます。その結果、経営管理の一環として監査・点検の結果を最大限に活用することができるのです。

なお、本稿は、独立行政法人情報処理推進機構（IPA）が発行している「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」を参考に解説しています。
次回は、「内部環境・外部環境の変化を監査・点検で見逃すな！」について解説します。

レベル 3_#13_情報セキュリティの見直しと強化（監査と点検）（3/3）
掲載日：2024/12/12



中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。
本記事では、組織における情報セキュリティへの取り組みを監査・点検する方法について全 3 回にわたって紹介しています。今回はシリーズの最終回として、常に進化し続ける IT 環境に合わせた監査・点検のあり方を詳しく解説します。
前回の記事はこちら：情報セキュリティの見直しと強化（監査と点検）（2/3）

１．サイバーセキュリティの背景

今さらですが、本記事の主題である「サイバーセキュリティ」に関する法律があることをご存じでしょうか。

2014 年に施行された「サイバーセキュリティ基本法」には、以下の条文があります。

> （目的）
> 第一条　この法律は、インターネットその他の高度情報通信ネットワークの整備及びデジタル社会形成基本法第二条に規定する情報通信技術の活用の進展に伴って世界的規模で生じているサイバーセキュリティに対する脅威の深刻化その他の内外の諸情勢の変化に伴い、
> （中略）
> サイバーセキュリティに関する施策を総合的かつ効果的に推進し、もって経済社会の活力の向上及び持続的発展並びに国民が安全で安心して暮らせる社会の実現を図るとともに、国際社会の平和及び安全の確保並びに我が国の安全保障に寄与することを目的とする。
>
> （定義）
> 第二条　この法律において「サイバーセキュリティ」とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置が講じられ、その状態が適切に維持管理されていることをいう。

簡潔にいうと「インターネット活用が進展する中、世界的規模でサイバーセキュリティに対する脅威が深刻化し、その他の内外の諸情勢が変化している。そこで、セキュリティ対策を積極的に行わなければならない。」ということです。

この法律からは、インターネットの普及に伴うサイバー脅威の深刻化を背景に、適切な対策を講じることが求められていることが読み取れます。例えば、インターネットがもたらす急速な IT 環境の変化に最新のセキュリティ対策で応えていくことが、現代社会では不可欠であることが理解できます。

では、IT 環境の急速な変化・進展に応じたセキュリティ対策を実行するには、どうしたらよいのでしょうか。ここでは、定期的に実施される監査・点検を通じて、日々変化・進展する IT 環境に適したセキュリティ対策を「見つける」ための観点について解説します。

２．IT 環境の変化・進展に応じた監査・点検の必要性

こちらの記事「情報セキュリティの見直しと強化（監査と点検）(1/3)」では、「情報セキュリティの監査・点検とは、社内のセキュリティのルールや、一般に必要とされる情報セキュリティ対策を基準として」と述べました。
監査や点検の基準となるセキュリティポリシーやガイドラインは、その策定時点では有効であっても、IT 技

術の急速な変化により陳腐化してしまうことがあります。
このため、監査・点検は社内外の IT 環境の変化を踏まえ、柔軟にその時勢に合った基準や観点で実施する必要があります。特に IT 分野は「ドッグイヤー（Dog Year）」と呼ばれるほど技術革新や進歩が速く、常に最新の状況に対応した監査基準が求められます。

３．IT インフラの変化・進展による新たなセキュリティモデル

従来のサイバーセキュリティ対策は、境界型防御※といって組織のネットワークの境界、つまり外部ネットワークと内部ネットワークの境目で防御を行うことに重点を置いていました。
※ファイアウォール、IDS/IPS（侵入検知・防止システム）、ウイルス検知、Web フィルタリング、スパムメール対策や、それらを統合した UTM（Unified Threat Management、統合脅威管理）を境界に設置して、外部からの不正なアクセスや攻撃から防御する手法。

ところが、ここ数年、テレワークの普及もありクラウドサービスの利用が急増しました。
クラウド環境では、データやアプリケーションが組織のネットワークの外部に存在し、従来の境界を意識することが難しくなります。
このため、セキュリティ対策として「ゼロトラスト」モデルが注目されるようになりました。このモデルでは、外部・内部を問わず、すべてのアクセスを検証します。
具体的には、ユーザーの認証、デバイスのセキュリティ状態の確認、アクセス権限の厳格な管理などを行います。これにより、内部からの脅威や、不正アクセスに対する防御を強化します。

例えば、基幹システムを自社内に設置したサーバーやネットワーク機器、ソフトウェアで運用し、境界型防御をセキュリティ管理の基準としていた組織が、基幹システムをクラウドサービスに移行した場合、監査・点検で自社のファイアウォールやウイルス検知についてチェックしても意味がありません。
このようなときは、従来の境界型防御の運用状況ではなく、クラウドサービスの選定要件や、サービス提供者のセキュリティ対策などを基準、観点にして監査・点検を行う必要があります。

４．情報機器の変化への対応

総務省の「通信利用動向調査」によるとスマートフォンの世帯保有率は、2010 年に 9.7%だったものが、2021 年には 88.6%に増加し、既にパソコンの 69.8%、固定電話の 66.5%を超え、最も普及した情報通信機器になりました。
もはや、スマートフォンを持っていない人は、ほとんどいない、といってもいいでしょう。

スマートフォン普及以前の 2003 年頃、ファイル交換ソフト Winny が流行りました。
当時は私物パソコンの業務利用は珍しくなく、企業データが Winny を通じて外部に漏えいする事故が相次ぎました。
そのため、多くの企業では私物パソコンの持ち込みや業務利用が禁止されるようになりました。
今でも社内ルールで私物パソコンの持ち込み、業務利用を禁止している企業は多いと思います。

一方スマートフォンはメールやチャット、SNS での取引先とのメッセージ交換など、私物を業務に利用する「BYOD（Bring Your Own Device）」として活用が広がっています。

パソコンとスマートフォンは名称や形は違いますが、どちらも小型のコンピュータです。特にスマートフォンはインターネット接続を前提とした多機能、高性能コンピュータであり、サイバー攻撃の対象にもなります。
つまり、私物スマートフォンの業務利用には新たなセキュリティリスクが伴うのです。実際、私物スマートフォンを社内 Wi-Fi に接続したことで、社内システムがウイルスに感染してしまった事例も発生しています。

社内ルールで私物パソコンの持ち込みおよび業務利用を禁止しても、私物スマートフォンは対象外としている場合、会社貸与機器を基準とした監査・点検を行っても、セキュリティ対策としては不十分になってしまいます。
しかし、スマートフォンの持ち込みや業務利用を禁止すると、業務に支障が出ることも考えられます。

このような状況に対応するため、私物スマートフォンにはモバイルデバイス管理（MDM）を導入するなど、現代のビジネス環境に合った柔軟なセキュリティ対策の導入と監査・点検の基準の見直しが求められます。

皆さんの会社や組織では正しい監査・点検が行われていますか？この機会に定期的な監査・点検のあり方や重要性を考えてみてください。

次回は、セキュリティ対策に関わる費用と効果について解説します。

レベル 3_＃14_コスト意識から投資意識へ　～セキュリティ対策に関わる費用と効果～
掲載日：2024/12/19

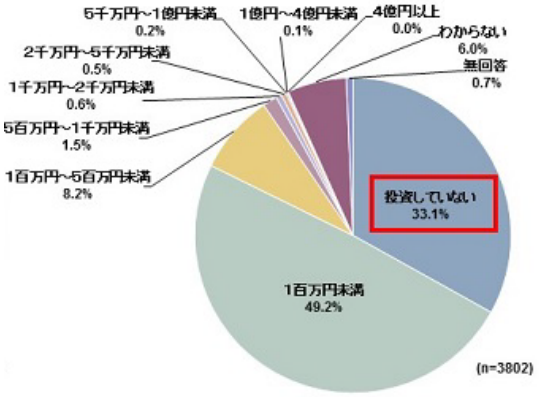


中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。
本記事では、セキュリティ対策に関わる費用とその効果について、データを交えながら包括的に考察します。

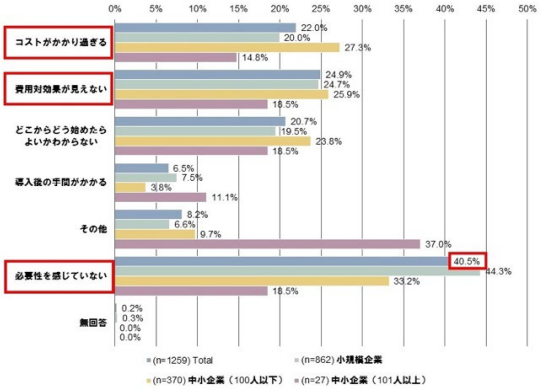
１．中小企業のセキュリティ対策の現状

独立行政法人情報処理推進機構（IPA）が中小企業を対象に行った「中小企業における情報セキュリティ対策の実態調査」によると、多くの中小企業がセキュリティ対策にあまり投資していない実態が明らかになっています。
直近過去 3 期の情報セキュリティ対策投資額について「100 万円未満」の割合が約半数を占める一方で、33.1%の企業は全く「投資していない」と回答しています。

情報セキュリティ対策投資を行わなかった理由として、企業規模に関わらず「必要性を感じていない」という回答が最も多く、特に小規模企業や中小企業（100 人以下）においてその割合が高くなっています。



直近過去 3 期の情報セキュリティ対策投資額

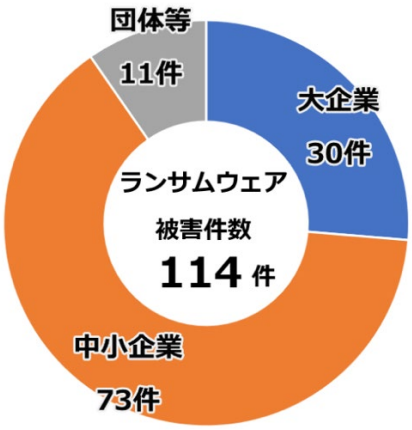


情報セキュリティ対策投資を行わなかった理由（企業規模別）

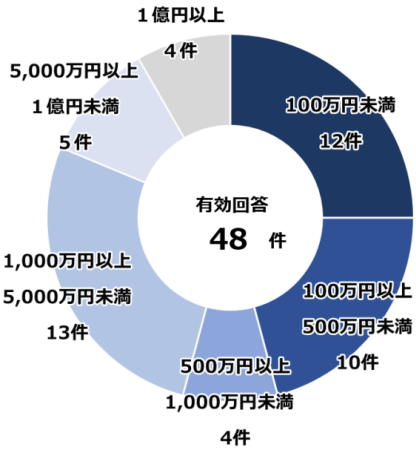
「2021 年度 中小企業における情報セキュリティ対策に関する実態調査」報告書について より

しかし、警察庁の資料「令和 6 年上半期におけるサイバー空間をめぐる脅威の情勢等について」によると、近年増加しているランサムウェアの被害は中小企業が最も多く、被害件数 114 件中 73 件（64%）を占めています。

さらに、復旧に要した費用は「1,000 万円以上 5,000 万円未満」が最も多い（28%）という結果でした。



被害企業・団体等の規模別



復旧等に要した調査費用の総額

「令和 6 年上半期におけるサイバー空間をめぐる脅威の情勢等について」資料編より

これらのデータから、中小企業では情報セキュリティ事故が多発しており、対策に費用をかけなければ多額の損失が発生するリスクがあることが分かります。

「わが社では情報セキュリティ事故は起きないから、コストをかける必要はない」という意識のままでは危険です。

２．セキュリティ対策の費用対効果

一般的に費用対効果とは、ビジネスやプロジェクトの実施に伴う費用と得られる効果や利益を比較評価することです。
中小企業の多くが情報セキュリティ対策投資に「必要性を感じていない」のは、得られる効果が目に見えにくく、経済的利益が感じられないからでしょう。

ところで、自動車の任意保険に加入する理由を考えてみてください。自動車保険の加入率は、毎年増加を続け、現在では対人賠償の普及率は 90%弱あるそうです。
加入が義務付けられている自賠責保険だけでなく、毎年保険料を支払って、目に見える効果も経済的利益もない自動車保険に大半の人が加入するのはなぜでしょうか？
答えは明白で、万が一事故を起こした場合、自賠責保険や個人の資産だけでは負担しきれないほどの賠償責任を負うリスクがあることを、誰もが理解できるからです。
交通事故は表面化するため、事故を起こした時の負担を容易に想定することができます。

しかし、情報セキュリティ事故は必ずしも表面化するとは限らず、事故が起きた、あるいは知らないうちに起きていたときの損害や負担を想定することが難しい側面があります。
このため「対策は必要ない」という意識につながりやすいのです。

そこで、セキュリティ対策の費用対効果を評価するには、予期せぬ事故による損害を金額に換算し、財務上どの程度の影響があるかを明確にします。
セキュリティ対策の費用は、企業の支払能力を超える負担を避けるためのものであり、それ自体が効果的であると考えるべきです。

３．セキュリティ事故の損害額の試算

IPA が提供する便利なツールに「NANBOK」があります。
『企業のセキュリティ担当者がセキュリティ対策を遂行するために経営陣に対して予算取りを行う際に利用してもらう』ために開発されたツールで、ランサムウェア被害が発生した際の損害額を簡単に試算することができます。
サイバー攻撃のリスクを被害想定金額で表現できるため、より具体的な説明が可能です。経営陣への対

策費用の根拠や必要性の説明に苦慮している方は、是非活用してください。

参考：IPA「セキュリティ関連費用の可視化」
https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2022/visualization-costs.html

４． 優先的・重点的に対策が必要な情報資産の把握

セキュリティ対策は、組織にとって価値があり重要な「情報資産」を脅威から守るために行います。
「情報資産」は業種や事業によって様々です。そのため、全ての情報資産に対策を講じると無制限に費用がかかってしまいます。
そこで、優先的・重点的に対策が必要な情報資産を把握するために、「情報資産の洗い出し」を行います。以下にその手順をご紹介します。

なお、情報資産の洗い出しには次の IPA 資料を使用します。（無償でダウンロード可能）
・中小企業の情報セキュリティ対策ガイドライン
　https://www.ipa.go.jp/security/guide/sme/about.html
・リスク分析シート
　https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055518.xlsx
今回は、作業手順の一部をご紹介しますが、「リスク分析シート」の最初のシート(利用方法タブ)に作業手順の詳細が記載されています。皆さんの会社で活用される際は、まずはこちらのシートをご確認ください。

また、当事業のセキュリティセミナーでもリスク分析について解説しています。
こちらの動画も是非ご覧ください。

・第 4 回セミナー「効果的なリスク分析方法」
　https://youtu.be/5NTrzcNZxaE?t=3

【情報資産の洗い出し手順】

※今回は、「リスク分析シート」作業手順の⑧をご紹介します。

（１）情報資産管理台帳の作成

リスク分析シートの「情報資産管理台帳」の重要度欄（M 列）を使用します。
日頃どのような電子データや書類を利用して業務を行っているかを考えて洗い出すと、作成しやすくなります。

（２）情報資産ごとの機密性・完全性・可用性の評価

機密性、完全性、可用性が損なわれた場合の事業への影響や、法律で安全管理が義務づけられているなど、【表 1】の評価基準を参考に評価値３～１を記入します。
情報セキュリティの ３ 要素「機密性」「完全性」「可用性」については、こちらの記事でも詳しく解説しています。こちらもあわせてご覧ください。
https://follow-up.metro.tokyo.lg.jp/glossary/yogokaisetu5/

【表 1】情報資産の機密性・完全性・可用性に基づく重要度の定義

評価値		評価基準	該当する情報の例
機密性 アクセスを許可された者だけが情報にアクセスできる	3	法律で安全管理（漏えい、滅失又はき損防止）が義務付けられている	●個人情報（個人情報保護法で定義） ●特定個人情報（マイナンバーを含む個人情報）
		守秘義務の対象や限定提供データ※ として指定されている 漏えいすると取引先や顧客に大きな影響がある	●取引先から秘密として提供された情報 ●取引先の製品・サービスに関わる非公開情報
		自社の営業秘密として管理すべき（不正競争防止法による保護を受けるため） 漏えいすると自社に深刻な影響がある	●自社の独自技術・ノウハウ ●取引先リスト ●特許出願前の発明情報
	2	漏えいすると事業に大きな影響がある	●見積書、仕入価格など顧客（取引先）との商取引に関する情報
	1	漏えいしても事業にほとんど影響はない	●自社製品カタログ ●ホームページ掲載情報

引用元：IPA リスク分析シート

【表 12】情報資産の機密性・完全性・可用性に基づく重要度の定義（一部変更）

※限定提供データとは、不正競争防止法で次のように定義されています。
「第二条…７…この法律において「限定提供データ」とは、業として特定の者に提供する情報として電磁的方法（電子的方法、磁気的方法その他人の知覚によっては認識することができない方法をいう。次項において同じ。）により相当量蓄積され、及び管理されている技術上又は営業上の情報（秘密として管理されているものを除く。）をいう。」

評価値		評価基準	該当する情報の例
完全性 情報や情報の処理方法が正確で完全である	3	法律で安全管理（漏えい、滅失又はき損防止）が義務付けられている	●個人情報（個人情報保護法で定義） ●特定個人情報（マイナンバーを含む個人情報）
		改ざんされると自社に深刻な影響または取引先や顧客に大きな影響がある	●取引先から処理を委託された会計情報 ●取引先の口座情報 ●顧客から製造を委託された設計図
	2	改ざんされると事業に大きな影響がある	●自社の会計情報 ●受発注・決済・契約情報 ●ホームページ掲載情報
	1	改ざんされても事業にほとんど影響はない	●廃版製品カタログデータ

評価値		評価基準	該当する情報の例
可用性 許可された者が必要な時に情報資産にアクセスできる	3	利用できなくなると自社に深刻な影響または取引先や顧客に大きな影響がある	●顧客に提供しているEC サイト ●顧客に提供しているクラウドサービス
	2	利用できなくなると事業に大きな影響がある	●製品の設計図 ●商品・サービスに関するコンテンツ（インターネット向け事業の場合）
	1	利用できなくなっても事業にほとんど影響はない	●廃版製品カタログ

引用元：IPA リスク分析シート

【表 12】情報資産の機密性・完全性・可用性に基づく重要度の定義

（３）情報資産の重要度評価

「情報資産管理台帳」に情報資産ごとの機密性・完全性・可用性の評価値を記入すると、【表 2】の基準に従って「重要度」欄に重要度３～１が自動で表示されます。ここで重要度の値が大きい情報資産が、優先的・重点的に対策が必要な情報資産です。この重要情報資産が漏えいや改ざん、あるいは利用できなかった場合に、被害が大きくなる可能性があります。重要度が高い情報資産に対して、セキュリティ対策の費用を投じることがで、リスクを最小限に留められる可能性が高まります。

【表 2】情報資産の重要度判断基準

判断基準	重要度
機密性・完全性・可用性評価値のうち最大値が「3」の情報資産	3
機密性・完全性・可用性評価値のうち最大値が「2」の情報資産	2
機密性・完全性・可用性評価値すべてが「1」の情報資産	1

引用元：IPA リスク分析シート

【表 13】情報資産の重要度判断基準

５．セキュリティ対策は未来への投資

情報セキュリティ対策に関わる費用を単なる支出としてではなく、企業の長期的な安定と成長を支える重要な投資と捉えることが必要です。投資によって得られる効果を定量評価し事業への影響を把握することで、組織の実態に見合った対策を講じることができます。そして、将来的な大規模損害を回避し、企業の信頼性と安全性を高めることが可能になるのです。

次回は、セキュリティ関連サービスの導入について解説します。

レベル 3_#15_情報セキュリティサービスの特徴・導入のメリットとは
掲載日：2025/1/9



中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。

昨今、ビジネス成長を支えるカギとして、DX 推進の重要性が認識されています。
その背景にあるのが、IT 技術の目覚ましい進化です。しかし、一方でその複雑さや高度化も加速しています。
IT の進歩は確かに便利ですが、その利便性の裏には隠されたリスクが存在し、特にセキュリティ問題を軽視することはできません。

そのため、企業が全てのセキュリティ対策を自社で実施するには、専門知識と人材が必要です。しかし、それを整えるには限界があります。そこで検討すべきは、専門的な知識と技術を持つ外部サービスの活用です。

本記事では、情報セキュリティサービスの特徴と導入のメリットについて説明します。

１．情報セキュリティサービスの概要

情報セキュリティサービスは、企業のデータを保護し、サイバー攻撃のリスクを削減するために提供される専門的なサポートと技術支援を指します。サービスの内容は多岐にわたりますが、デジタル環境で安全に業務を推進するための基盤づくりに役立つこれらのサービスを利用することで、より強固で有効なセキュリティ対策を実施できます。

中小企業が抱える課題

中小企業は、大企業と比べて IT リソースが限られており、セキュリティの専門知識や専任の IT 担当者不足など、自社での対応が難しいといった課題があります。
そのため、中小企業にとっては外部の専門的なサポートを活用することが、効率的かつ経済的に情報セキュリティを強化する手段になります。

導入のメリット
情報セキュリティサービスを導入することで、専門知識を持った外部の専門家から支援を受けられます。これにより、日常業務における情報の保護が強化され、万が一の事態への備えと迅速に対応できる体制が整います。また、外部機関の支援を受けることで、最新のセキュリティ技術やトレンドを取り入れやすくなり、効率的にリスクをコントロールすることが可能になります。

２．情報セキュリティサービスの種類と導入効果

（１）情報セキュリティコンサルテーション

企業の情報セキュリティ管理体制や対策を強化するための支援を行うサービスです。セキュリティ対策の現状を診断し、最適な改善策を提案することで、企業のセキュリティレベルの向上を図ります。また、セキュリティ関連の適合性評価制度等における認証・認定を支援するサービスも行っており、取引先等外部からの信頼性を高めるサポートをします。

（２）情報セキュリティ教育サービス

従業員の情報セキュリティ意識を高め、セキュリティ知識や対応スキルを習得するための教育を行うサービスです。セキュリティへの理解を深めることで、日常業務でのセキュリティリスクを軽減することが

期待できます。

（３）情報セキュリティ監査サービス

このサービスでは、企業が保有する情報資産を守るためのセキュリティ管理体制やリスク対策が正しく実施されているかどうかを、第三者の立場から評価します。国際的に整合性のとれた基準に従って検証または評価し、保証や助言を行うサービスです。
監査サービスを受けることで、自社のセキュリティ対策が十分なのかが確認でき、不十分な点の洗い出しや対処が可能になります。また、取引先などにセキュリティ対策を適切に行っていることをアピールできます。

（４）脆弱性診断サービス

システムやソフトウェアなどに潜むセキュリティ上の脆弱性の有無を専門家がチェックし、セキュリティ状態を診断するサービスです。システムに脆弱性があると、サイバー攻撃や情報漏えいのリスクが高まり、企業の信頼を損ねるおそれがあります。診断を受けることで、安心してシステムを運用することができます。
診断には以下のような種類があります。

ア　ウェブアプリケーション脆弱性診断
　Web サイトや Web アプリケーションに潜む脆弱性を発見してリスクを診断します。システム停止や情報漏えい、データ改ざん・不正アクセスなどにつながる脆弱性を洗い出します。
イ　プラットフォーム脆弱性診断
　サーバーやネットワーク機器などのシステムに脆弱性がないか、設定に問題はないか検査します。
ウ　スマートフォンアプリケーション脆弱性診断
　スマートフォンやタブレット端末内のアプリケーションに内在する脆弱性を診断します。主にアプリケーションを提供する企業が利用します。

（５）デジタルフォレンジックサービス

システムやソフトウェア等の不正利用、サービスの妨害、データの破壊、誤った情報の漏えいなどの問題を扱うための専門的な支援を提供するサービスです。これらの問題が法的な争いや訴訟に発展した場合、電子情報を証拠として保全し、詳細な調査と分析を行います。また、電磁記録の改ざんや

毀損等に対する対策として、以下のような分析及び情報収集を実施します。

ア　機器や記録デバイスの徹底調査
　　デジタルフォレンジックの手法を用いて、コンピューターやスマートフォン、その他のデジタルデバイスに保存されたデータの調査を実施。これにより、問題の原因や証拠を見つけ出すことが可能です。
イ　訴訟サポートと電子情報開示
　　デジタルフォレンジックによる調査の一環として、訴訟を進めるための支援や電子証拠の開示手続き（ｅディスカバリ）に対応するサービス。これにより、法的手続きで必要となる証拠を効果的に管理できます。

（６）セキュリティ監視・運用サービス

企業のシステムやソフトウェアなどをセキュリティに精通した専門家が監視および適切な運用を行うサービスです。次に掲げるいずれか、あるいは全てのサービスを指します。

ア　マネージドセキュリティサービス（セキュリティインシデントまたはその予兆の検知、防御を目的とするものをいいます。）
イ　セキュリティ監視サービス（セキュリティ製品が出力するログの分析、通知、レポート提供を継続的に提供するものをいいます。）
ウ　マネージドセキュリティサービスやセキュリティ監視サービスを包含する複合的なサービス

このサービスを活用し、セキュリティ監視・運用を外部委託することで、セキュリティ人材確保の必要性がなくなりコスト削減につながります。また、情報漏えいなどのリスク軽減やセキュリティ対策強化のメリットがあります。

３．情報セキュリティサービス活用の注意点

情報セキュリティの分野では、信頼性のある企業を選択することが極めて重要です。
多くの中小企業では、専門的な知識が不足しているため、提供されるサービスの質を見極めることが困難です。

近年、情報セキュリティサービスを提供する企業の数が増加し、提供されるサービスの種類も多様化しています。したがって、どの企業にサービスを依頼すべきか、また、そのサービスの評価方法について

迷う企業は多いかもしれません。

信頼できる業者選びのポイント

信頼できる情報セキュリティサービスの提供企業を選ぶためには、具体的な基準を参考にすることが大切です。
専門知識のない中小企業がサービスを選ぶ際、その品質を判断できるようにするための基準として、第三者がサービス提供企業を客観的に評価する認定制度があります。
次に挙げる認定制度や公開されている情報を参考にして、信頼できる業者を選びましょう。

（１）情報セキュリティサービス基準審査登録制度

経済産業省による、情報セキュリティサービスに関する品質の維持や向上に努めているサービスを明らかにするために設定された「情報セキュリティサービス基準」。
「情報セキュリティサービス基準審査登録制度」は、この基準を満たすサービスをリスト化し公開することで、利用者が安心してサービスを選定することを目的としています。

独立行政法人情報処理推進機構（IPA） では、この情報セキュリティサービス基準に合致している情報セキュリティサービスについて調査を行い、その結果を「情報セキュリティサービス基準適合サービスリスト」として公開しています。
これにより、サービスの利用を検討している企業は、信頼できる情報源に基づいて選択することが可能となります。

情報セキュリティサービス基準適合サービスリストは、５つのサービス分野を対象としています。
先述の２．情報セキュリティサービスの種類と導入効果の（３）～（６）で説明したサービスを検討する際、業者選定の一助として利用してください。

【情報セキュリティサービス基準適合サービスリスト】
https://www.ipa.go.jp/security/service_list.html

（サービス分野）
- 情報セキュリティ監査サービス
- 脆弱性診断サービス
- デジタルフォレンジックサービス

- セキュリティ監視・運用サービス
- 機器検証サービス

（２）認定情報処理支援機関（スマート SME サポーター）制度※

中小企業に IT ツールを提供する IT ベンダーなどを「情報処理支援機関（スマート SME サポーター）」として認定する制度。
この制度は、IT ベンダーが中小企業向けに使いやすい IT ツールを提供し、その普及を支援することを目的としています。この制度を利用することで、中小企業は信頼できる IT ベンダーから生産性を向上させるための有用な IT ツールを入手することが可能になります。

※ https://www.smartsme.go.jp/SSS_OverviewPage （中小企業庁）

４．もっと簡単にサービスを活用するなら

情報セキュリティサービスを活用するにあたって、もっと手軽に利用開始するためのパッケージ化されたサービスもあります。

サイバーセキュリティお助け隊サービス制度

「サイバーセキュリティお助け隊サービス」は、中小企業に対するサイバー攻撃への対処として不可欠な以下のサービスをワンパッケージにまとめた、民間事業者から提供されるサービスです。

＜ワンパッケージで安価に！＞

1	**見守り**	24 時間 365 日監視 挙動や問題のある攻撃を検知し、あなたの PC とネットワークを守ります。
2	**駆付け**	問題が発生したときに地域の IT 事業者等が駆付け対応します。（リモート支援の場合あり）
3	**保険**	簡易サイバー保険で駆付け支援等のサイバー攻撃による被害対応時に突発的に発生する各種コストが補償されます。

IPA では、基準を満たしているサービスに「お助け隊マーク」を付与しています。
また、このサービスを利用する際、IT 導入補助金が利用できる『サイバーセキュリティお助け隊サービ

ス』の導入支援制度を活用し、実際にかかる費用を軽減することも可能です。

・制度の概要はこちら：https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/

５．経費削減のための制度

情報セキュリティサービスの導入に際し、「IT 導入補助金」を活用することで、費用を抑えつつ効果的なセキュリティ対策を実現できます。
IT 導入補助金は、中小企業や小規模事業者等が生産性向上を目的として、業務効率化や DX 推進に向けた IT ツールの導入を支援するための補助金制度です。
この制度を活用することで費用を軽減でき、より多くの企業が情報セキュリティ強化を図ることができます。

・制度の概要はこちら：https://it-shien.smrj.go.jp/

６．まとめ

情報セキュリティリスクが高度化し、それに対応するためには高い専門スキルが必要となっています。このような状況下で、企業が独自に対策を講じるのはますます困難になっています。
情報セキュリティサービスは多様化しており、そのため、公的機関によって、企業が安心して利用できるようサービス基準の策定や、補助金などの制度が整備されています。

人材不足や知識不足でセキュリティ対策が思うように進まない企業は、こうした情報セキュリティサービスの利用を検討してみてはいかがでしょうか。

なお、本稿は、IPA が発行している「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」を参考に解説しています。

次回は、セキュリティ教育の必要性について解説します。

レベル３_#16_より深く学ぶ　セキュリティ教育の重要性
掲載日：2025/1/23



中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。

情報化社会が進む中で、日常生活やビジネスにおける IT の利活用がますます広がっています。しかし、その一方で情報漏えいやサイバー攻撃といったリスクも顕在化しています。こうしたリスクに対処するために欠かせないのが「セキュリティ教育」です。

本記事では、セキュリティ教育の重要性、その背景や事例、そして効果的な教育手法について詳しく説明します。

１．セキュリティは常識？

今では当たり前のように使われる「サイバーセキュリティ」という言葉が一般的に使われるようになったのはいつ頃でしょうか。
1990 年代初頭、インターネットの普及が本格化する前に、コンピュータネットワークと情報システムのグローバル化が進みました。この時期に、企業や政府の情報システムが普及し、セキュリティの重要性が認識され始めました。

例えば、1992 年に OECD（経済協力開発機構）が情報システムのセキュリティに関する国際原則「情報セキュリティに関するガイドライン」を発表しました。
このガイドラインには、信頼性、データの完全性、アクセスの適切性など、サイバーセキュリティの基本的な考え方が明記されています。

そして、1990 年代後半以降、急速なインターネットの普及に伴い、個人も企業もネットワークを日

常的に利用する時代が始まりました。それと同時にハッキングやウイルス感染などの新たなリスクが登場し、「サイバーセキュリティ」という言葉が使われるようになり、セキュリティの概念はますます重要になりました。

今日では、「情報セキュリティ」や「サイバーセキュリティ」という言葉を、ニュースなどでよく耳にするようになりました。
しかし、実際のところ学校教育や職場研修でセキュリティについて教えられることは少なく、日常生活での具体的な対策方法を学ぶ機会が限られています。
また、セキュリティに関する知識は専門的である場合が多く、一般の人々にとっては理解しづらい点が、セキュリティに関する理解の普及を妨げています。

２．セキュリティ教育が求められる理由：過去の事例に学ぶ

セキュリティ教育の必要性を考える上で、実際の事例から多くのことを学ぶことができます。
代表的な例として、日本年金機構で発生した大規模な個人情報漏えい事件（2015 年）が挙げられます。この事件では、職員のパソコンから約 125 万件の個人情報が流出し、事故の要因は職員へのセキュリティ教育が不十分であった点にあると結論付けられました。

公表資料には「電子メールのウイルスが入った添付ファイルを開封したことにより、不正アクセスが行われ、情報が流出したものと認められます。」とあり、原因は標的型攻撃メールにより職員５名のパソコンがウイルスに感染したことにあることが分かりました。
また、調査結果報告には、「毎年、全職員を対象に情報セキュリティに関する研修を実施していたが、研修教材の中で標的型メール攻撃に関する記載内容が不十分であった。」「標的型メール攻撃に関する内容を周知したこともあったが、実際に必要とする対応方法に即したものになっておらず、職員への十分な周知・徹底には至っていなかった。」（原文ママ）という記述があり、職員への教育が不十分であったことがわかります。
この事故は、セキュリティ教育の重要性を再認識させるものとなりました。

３．セキュリティは専任者の仕事という誤解

組織の中には多くの専門分野と部門があり、それぞれ業務遂行には専門知識が必要となります。
経理部門では会計の知識が、人事部門では労務管理の知識が必要とされ、誰でも配属後に研修や OJT を通じて、専門知識を身に付けていきます。

ところがセキュリティとなると、特定の部門や担当者にだけ任せればよいと考えるケースが少なくありませ

ん。
しかし、サイバー攻撃や情報漏えいのリスクは特定の部門だけで防ぐことはできません。むしろ、業務で IT を利用する従業員一人ひとりが情報セキュリティに対する意識を持ち、組織全体で対応する必要があります。

実際、情報漏えいなどの事故は、その原因の多くが従業員の不注意や誤操作に起因しています。たった一人の従業員の不注意が、企業全体の信頼や事業環境に深刻な打撃をもたらす可能性があるのです。

４．セキュリティ教育の進め方

セキュリティに関する知識やスキルは非常に幅広く多岐に渡るため、従業員に短時間で多くの内容を伝えても、全てを理解し実行するのは困難です。

従業員の理解を深めるためには、業務上特に求められるスキルやポイントを絞り、計画的にセキュリティ教育の機会を設ける必要があります。
例えば、テレワークやクラウド環境などの新しい働き方や技術を導入する際は、その特性に応じた教育が必要になります。
以下にセキュリティ教育を計画的に進めるためのポイントを説明します。

（１）目的を明確にする

受講者の職種や役職、利用する情報システムに応じて、必要となる知識やスキルを具体的に設定します。例えば、全従業員向けにはセキュリティ関連規程の周知を行い、経理部門には会計システムのランサムウェア対策やバックアップの必要性を重点的に教育します。

（２）教育テーマを絞る

短時間で多くを伝えることは困難なため、現場で直面しやすいテーマを選び、1 回の教育で学ぶ焦点を絞ります。例としては、「テレワーク時の Wi-Fi セキュリティリスクと対策」などです。

（３） ５Ｗ１Ｈを決める

教育内容を計画する際、５Ｗ１Ｈの視点を取り入れると良いでしょう。これにより、具体的で実行可能な教育プログラムが設計できます。

Who（対象者）	全従業員、管理職、パート、新入社員など
When（実施時期）	年度初め、半期ごと、入社時、システム導入時など
Where（場所）	会議室、在宅、外部研修会場など
What（内容）	社内ルール、標的型攻撃対策、パスワード強化など
Why（理由）	テレワーク導入、不審メールの増加など
How（方法）	集合教育、e ラーニング、Web 会議など

（４）教育効果を検証する

教育後、アンケートやテストを実施して、理解度を確認しましょう。また、教育内容が職場でどの程度実践されているのか、教育効果を評価することも大切です。

５．無料教材を賢く活用する

セキュリティ教育にはテーマに沿った教材が必要です。
教材を独自に作成することが難しい場合には、既存の教材を利用しましょう。無償で提供されている教材も多数あります。
ここでは、無料で利用できる教材をご紹介します。

（１）『5 分でできる！情報セキュリティポイント学習』（IPA）

https://www.ipa.go.jp/security/sec-tools/5mins_point.html

主に中小企業の方を対象とした、1 テーマ 5 分で情報セキュリティについて学べるコンテンツです。
職場の日常的なシーンを取り入れた親しみやすい学習テーマが特徴で、セキュリティに関する様々な事例を疑似体験しながら、正しい対処法を学ぶことができます。
各テーマの最後には確認テストがあり、理解度を把握することができます。

（２）『5 分でできる！情報セキュリティ自社診断』（IPA）

https://www.ipa.go.jp/security/guide/sme/5minutes.html

情報セキュリティ対策のレベルを数値化し、自社の問題点を把握するために役立ちます。

（３）『映像で知る情報セキュリティ』（IPA）

https://www.ipa.go.jp/security/videos/

情報セキュリティに関する脅威や対策などを学べる映像コンテンツです。「IPA Channel」（YouTube）で公開されています。

（４）『中小企業向けサイバーセキュリティ対策の極意』（東京都）

https://www.cybersecurity.metro.tokyo.lg.jp/security/guidebook/#page1

サイバー攻撃の現状と必須のサイバーセキュリティ対策を、できるだけわかりやすく解説しています。組織として対策を検討する際の参考資料として活用できます。

６．教育の進め方に関する動画紹介

東京都では中小企業向けに様々な支援を行っており、当事業でもセキュリティ専門家によるセミナーを開催しました。
初回のセミナーでは、セキュリティ規定の作り方に加え、効果的な社内講習会の組み立て方や講習用コンテンツの入手方法、解説のポイントなども紹介されています。セキュリティ教育に悩みを抱えている方には有益です。

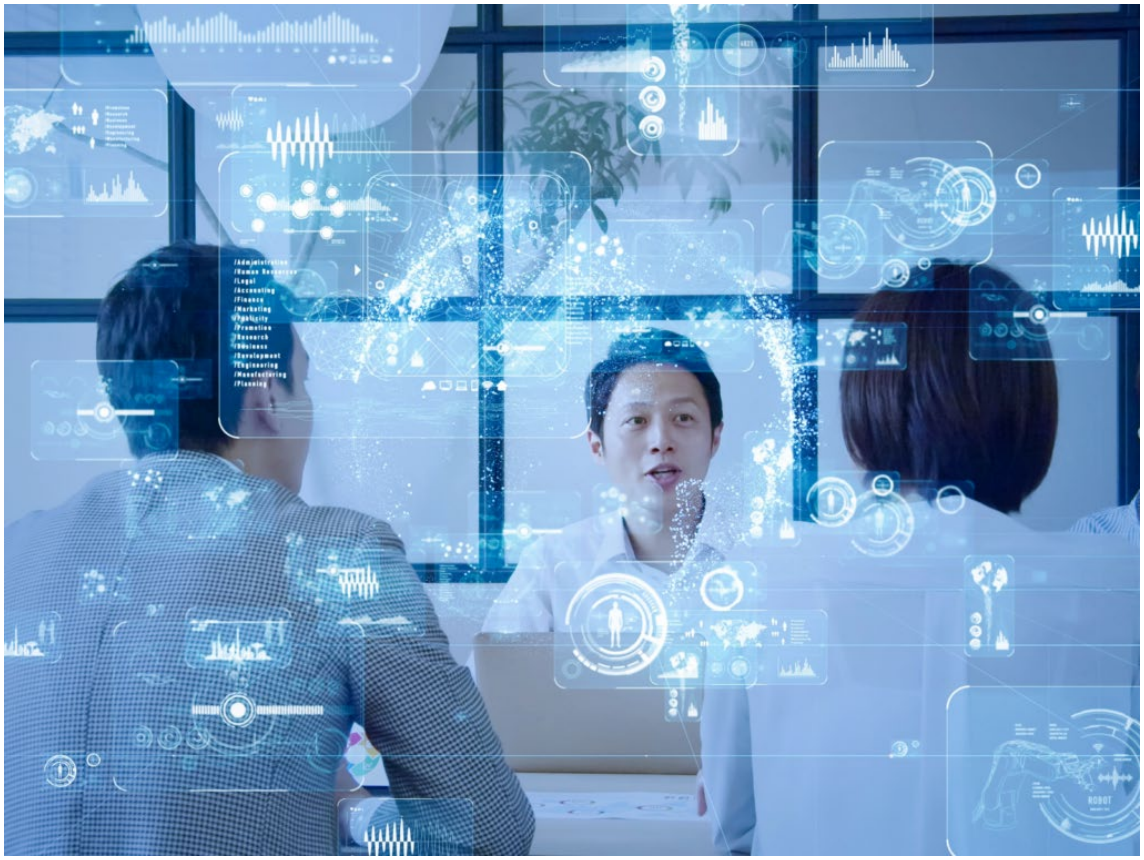
・第 1 回セミナー「社内へのサイバーセキュリティ対策の浸透」
https://follow-up.metro.tokyo.lg.jp/seminar/seminar1/

独立行政法人情報処理推進機構（IPA）のサイトでも効果的な講習会の組み立て方や、講習用コンテンツの入手方法、解説のポイントなどを説明するオンラインセミナーのアーカイブ動画が公開されています。
こちらも社内のセキュリティ教育に役立つ内容です。
https://www.ipa.go.jp/security/seminar/sme/seminar.html

なお、本稿は、IPA が発行している「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」を参考に解説しています。

次回は、組織的なセキュリティ向上に必要なことについて解説します。

レベル 3_＃17_組織全体でセキュリティを向上させるために必要な視点と取り組み
掲載日：2025/1/30



中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。

現代のビジネス環境において、情報セキュリティの重要性は年々高まっています。対策を怠れば、大きな損害や信頼の損失につながる可能性もあります。
そこで本記事では、会社全体で組織的にセキュリティを強化・向上させるために必要な手法や心構えを詳しく解説します。

とても大事なことですので、すでに日頃から基本的対策を実施している企業も、ぜひ一度読み進めて確認・再考する機会として活用してください。

１．経営者や管理者の積極的な関与が鍵を握る

情報セキュリティの問題は、専門の部門や特定の従業員だけが担うべきものではありません。特に情報漏えいやサイバー攻撃が発生すれば、企業全体が大きな損害を被る可能性があります。企業全体の経営方針や体制に深く結びついているため、経営課題として捉えることが不可欠です。

そのため、セキュリティ強化を推進するためには、経営層が主導的に関与し、必要な意思決定を行うことが必須です。セキュリティは、組織全体に関わる重要課題です。経営層が情報セキュリティ対策を組織運営の最優先事項として位置づけることが大切です。

そして、対策にはシステム導入や教育実施などが必要で、時間や資金、人材も必要です。
しかし、これらのリソースは限られており、経営層が情報セキュリティ対策の必要性を理解しなければ、十分な対応ができません。

こうした意思決定を行うのが経営層の役割であり、それをトップダウンで示すことで、従業員の意識改革が進み、組織全体のセキュリティ向上につながります。

このように、経営者や管理者が支援することで、組織は効果的にセキュリティリスクを管理し、体制を構築することができるようになります。

情報セキュリティは技術的な対策だけでは十分ではありません。
従業員一人ひとりの意識や行動も重要な要素です。従業員が日常的なセキュリティ行動を怠れば意味がありません。
次のような基本的な行動を全員が徹底して行うことでリスクを大幅に軽減できます。
・強固なパスワードの使用と定期的な変更
・標的型攻撃メールに注意を払う

中小企業の場合、少人数である強みを活かし、少しの努力で組織全体の意識をまとめ上げることができる可能性があります。

このような取り組みを通じて、経営者や管理者が情報セキュリティの重要性を強調し、模範的な姿勢を示すことで、従業員は情報セキュリティを「他人事」ではなく「自分事」として捉えるようになります。
前回解説した「セキュリティ教育」においても、従業員が情報セキュリティを「自分事」として捉えることが重要です。
前回の記事はこちら：より深く学ぶ　セキュリティ教育の重要性

２．顧客や取引先から信頼されるために

経営層が明確なセキュリティ体制を打ち出し、積極的に関与することで、顧客や取引先に対して情

報セキュリティに真剣に取り組んでいる姿勢を示すことになります。
このことは、ビジネスの競争力を維持し、信頼を得る上で重要です。

近年はサプライチェーン全体でのセキュリティ対策が求められており、顧客や取引先に「この会社はセキュリティ対策がしっかりしていて安全だ」と感じさせるセキュリティレベルを維持することが、ビジネス拡大に繋がります。

さらに、経営層自らが率先してセキュリティに対する積極的な姿勢を示せば、社内外に「安全・安心を重視する企業である」とのイメージを効果的に伝えられるでしょう。それは信頼にとどまらず、ブランド価値そのものも向上させる原動力となるはずです。

３．現代における脅威インテリジェンスの重要性

サイバー攻撃が日々巧妙化し、世界中で新しい脅威が次々と発生する現代において、セキュリティ強化の柱として「脅威インテリジェンス」が注目を集めています。
この概念は、サイバー攻撃に関する情報を収集・分析し、その結果をもとにセキュリティリスクを可視化し、攻撃に備えるための対応を決定するプロセスを指します。
*インテリジェンスとは、収集した脅威情報をベースに自組織に活用可能なコンテキスト（付帯情報）を追加したもの。

近年、脅威インテリジェンスの重要性が注目されていますが、その背景にはサイバー攻撃の高度化や増加、そして組織の IT 環境の複雑化が挙げられます。

独立行政法人情報処理推進機構（IPA）が公表している「脅威インテリジェンス導入・運用ガイドライン」には、次のように述べられています。

「日本国内では海外と比較して、脅威インテリジェンスの活用は成熟していない現状にあり、概念そのものの認知度や、導入しているが有効活用できていない組織も多く存在する。日本という単位でも「National Cyber Power Index 2020」（Harvard Kennedy School Belfer Center）によれば、調査対象となった 30 カ国の中で、日本はサイバーセキュリティの総合指標において、9 位であったのに対し、インテリジェンス部門については能力で 16 位、意識で 22 位という結果となっており、脅威インテリジェンスの未発展が日本の課題となっている。」

ここでは、日本では脅威インテリジェンスが海外に比べて遅れており、課題であることがうかがえます。

	監視	インテリジェンス	商業および産業成長	サイバー防衛	情報操作	サイバー攻撃	国際規範および標準化
能力	22位	16位	6位	13位	13位	14位	11位
意識	25位	22位	17位	6位	17位	15位	15位

【日本におけるセキュリティ指標の総合評価 2020】（Harvard Kennedy School Belfer Center）

しかし今後、脅威インテリジェンスの導入は、企業規模を問わず重要なリスクを回避するための鍵となるでしょう。

４． 脅威インテリジェンスの分類

脅威インテリジェンスには、次のような種類があります。

・戦略的インテリジェンス

会社全体の方針を決めるための情報のこと。

サイバー攻撃に関する脅威動向や外部環境の分析などによりリスクを明確化し、経営層によるセキュリティに関する意思決定、投資判断を支援します。

・運用インテリジェンス

自社のセキュリティ改善に役立てる情報のこと。

サイバー攻撃の手法を分析して脅威を理解し、ペネトレーションテストなどの短～中期的なセキュリティ改善を行います。

・戦術的インテリジェンス

具体的な攻撃の兆候を見つけて、すぐに対策を取るための情報のこと。

組織内部で検知した、または外部組織から共有される攻撃や脆弱性に関する情報をもとに短期的にインシデントの予防・検知・対応を行います。

５． 脅威インテリジェンス活用のプロセス

脅威インテリジェンスを活用するには、以下のプロセスを整理して実行することが効果的です。

*説明の（）内に脅威インテリジェンスで用いられる言葉を示しておきます。

（１）目的を明確にする（方針策定フェーズ）

組織の課題に応じたインテリジェンスの目的を明確にします。

目的に沿って、求めるインテリジェンスに必要なデータの収集方法や収集計画を定めます。

（２）情報を収集する（収集・加工フェーズ）
必要なデータを収集し、分析しやすいように整理・加工します。

（３）分析する（分析フェーズ）
集めたデータを分析し、その結果からリスクを予測し、意思決定に必要なインテリジェンスにまとめます。

（４）共有する（配布フェーズ）
部門や役職に応じた適切な形で、インテリジェンスを必要とする人に共有します。

（５）評価する（評価フェーズ）
脅威インテリジェンスプロセスが適切だったのか振り返り、評価します。

６．最後に

情報セキュリティは技術的対策だけではなく、組織全体の文化として根付かせる必要があります。そのためには、経営層の積極的関与や時にはトップダウンによる意思決定が必要となります。
適切な経営支援のもと、情報セキュリティを強化することで顧客や取引先からの信頼を獲得し、自社の競争力を強化していきましょう。
この記事をきっかけに、身近なセキュリティ対策を考えてみてください。

※情報セキュリティに関する最新動向は次の公的機関から発信されています。

- **独立行政法人情報処理推進機構（IPA）情報セキュリティ**
  https://www.ipa.go.jp/security/
- **内閣サイバーセキュリティセンター（NISC）自由、公正かつ安全なサイバー空間を確保するために。**
  https://www.nisc.go.jp/
- **総務省 国民のためのサイバーセキュリティサイト**
  https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/
- **警察庁 サイバー警察局**
  https://www.npa.go.jp/bureau/cyber/
- **警察庁 サイバー空間をめぐる脅威の情勢等について**
  https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf

なお、本稿は、IPA が発行している「脅威インテリジェンス導入・運用ガイドライン」を参考に解説しています。

次回は、中小企業におけるセキュリティ対策の取組事例について解説します。

レベル 3_#18_中小企業におけるセキュリティ対策取組事例
掲載日：2025/2/6



中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。
本記事では、中小企業がどのようにセキュリティ対策に取り組んでいるのか、実際の取組事例をご紹介します。

１．中小企業の役割とその重要性

日本における中小企業の存在は、経済の基盤を支える重要な要素として位置付けられています。
中小企業庁の統計によると、2021 年 6 月時点で日本国内には以下の企業が存在しています。
（※以下、原文ママ）

- 中小企業　336.5 万者（構成比　99.7%）
- 大企業　　1.0 万者（構成比　0.3%）
  中小企業と大企業の合計　337.5 万者

国内企業の大部分を中小企業が占めている一方、大企業はわずか全体の 0.３%にとどまっており、この数値から中小企業が国内経済の重要な柱であることがわかります。

中小企業の比率が高い傾向は日本に限ったことではなく、OECD 加盟国でも企業全体の占有割合は約 99%と、主要先進国共通の傾向です。つまり、中小企業は国を問わず経済活動の中核的な存在であり、その役割の重要性が認識されています。

こうしたことからも、デジタル化と国際化が進む現代社会では、中小企業の情報セキュリティ対策への取組は、各企業の存続や成長という次元を超え、安全で安心なデジタル社会の実現に不可欠であることがわかります。

２．業種別にみる取組事例

一口に中小企業といっても業種や経営形態は非常に多岐にわたります。
また、同じ業種であっても企業ごとに業務プロセスは異なり、デジタル化の進展状況も様々で、直面する課題も変わってきます。
しかし、企業規模や業種に関係なく、共通する課題も存在します。その一つがパソコンやインターネットの利用、オフィスソフトや業務アプリケーションなどの業務効率化を目的としたデジタルツールの活用です。これらは多くの企業で共通しているため、他社の取組事例はとても参考になります。

今回は、独立行政法人情報処理推進機構（IPA）の公表資料「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―事例集―」の中から、特に企業数が多い２業種「卸売業・小売業」と「製造業」に注目し、実際に被害が発生し、再発防止のために取り組んだセキュリティ対策の事例をご紹介します。
同じ中小企業において、セキュリティの問題に直面した際、どのように対策を講じたのかを知ることは、自社のセキュリティ対策を考える上で、参考になるのではないでしょうか。

（１）卸売業・小売業 の取組事例

「元従業員による機密情報の持ち出しの疑いから、対策を拡充」

【対策・投資多】・【被害有】

所在地	**東京都**
従業員数	**6～20 名以下**
業種	**卸売業・小売業**
実施している対策	**・社内の機密情報に関する社内規定を策定** **・情報資産管理やログ管理、デバイス管理を行うシステムを導入**

【概要】
（取組背景と実施事項）
海外から素材を輸入して国内のメーカーに販売している卸売業を営む都内中小企業。
情報セキュリティ強化の背景には、元従業員が退職前に大量のファイルをダウンロードし、その PC から完全に履歴を消去していたことが挙げられる。機密情報の漏えいの証拠は得られなかったが、社内からの脅威への対策が不十分であることを認識。
そのため、社内規定の策定や情報資産管理システム、デバイス管理システムを導入し、機密情報の取り扱い方法を改善した。
費用面の負担は中小企業庁の「IT 導入補助金」を活用することで、軽減化に成功。
また、従業員向けに研修を実施し、情報資産の重要性やキャリアへの影響について共通認識を持つことができた。

（見込まれる効果）
・情報セキュリティ対策を行うことで、経営者も従業員も安心できる。
・小規模企業でも社内規定を作り、システムを導入することで、従業員は自分が疑われていると感じることなく安心して働ける。
・トラブル発生時に大きな心理的負担となった膨大なデータチェックや作業の必要がなくなる。
・セキュリティ対策が進むことで、クライアントからの信頼を得ることができる。
例えば、機密情報を専用の鍵付きケースで管理・持ち運ぶことで、万が一の対策が取れ、クライアントから好感を持たれるなど。
・被害の予防効果。

この事例の詳しい内容は下記からご確認ください。
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―事例集― （P31）

（２）製造業の取組事例

「小規模な製造業でも社内の技術情報・機密情報管理は大切」

【被害有】

所在地	**徳島県**
従業員数	**５名以下**
業種	**製造業**
実施している対策	**・当社のサーバから情報が漏えいする被害を受けたことを踏まえ、開発に関わる技術情報等の重要情報をスタンドアローン環境で管理。**

【概要】
（取組背景と実施事項）
徳島県で製造業を営んでおり、以前は別の地域で事業を展開していたが、現在の事業への転換を図るため、従業員数を縮小した経緯がある。
現在は少人数で運営しており、情報セキュリティ対策は経営者が直接対応している。
過去に内部不正による情報漏えいが疑われる事案があった。
当時、外国人従業員を含む複数の従業員が在籍し、海外市場向けの製品開発を行っていた。
しかし、製品開発は安全対策が進まず、途中で断念。事業縮小に伴い、研究開発や情報セキュリティ担当の従業員が退職。
情報セキュリティは社内規定を整備し、それに基づいて運営していたが、退職後にサーバ移管作業を行った際に大量のアクセスログが発覚。顧客や外部委託先への影響はなかったが、アクセスが退職した従業員によるもので、経理情報や技術情報などがダウンロードされていたことが確認された。

現在は少人数で運営し、重要な情報はスタンドアローン環境で管理。
サーバにはファイルを保存せず、技術情報はローカルや外付けハードディスクに、経理情報はローカルなソフトウェアで管理。
今後、事業の成長に伴い、従業員増加や工場設置が必要になるため、IT 環境への投資が課題。
新たにサーバを準備し、情報セキュリティ対策をさらに強化する必要がある。

事業は常に上り調子であるとは限らず、下り調子の時にはトラブルが大きくなることが予想されるため、情報セキュリティ対策は積極的に取り組むべきであると考えられている。

この事例の詳しい内容は下記からご確認ください。
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―事例集― （P17）

３．まとめ

１つ目の事例では、社内からの情報漏えい疑惑を機に社内規定を整備し、情報資産管理などのシステムを導入して技術的な対策を進めました。この事例からは、組織のルール作りを第一に行い、その後技術的な対策を導入することで、効果的なセキュリティ対策を推進できたことがわかります。まだ規定を作っていない企業は、まずは社内規定を作成するところから始めるとよいでしょう。

２つ目の事例では、ファイルの保管場所を変更するなど会社の事業規模や状況の変化に応じて対策を見直しています。状況の変化を捉えて、業務効率を維持しながら柔軟に適切な対策に見直していくことが必要であると言えます。

今回ご紹介した事例集には、全国各地の様々な業種の事例が 61 社分掲載されています。皆さんの企業に似た事例を見つけ、参考にしていただくことで、一つでも取り組みを開始していただけることを期待しています。

次回は、ISMS やプライバシーマークなどの認証制度について解説します。

レベル 3_#19_情報セキュリティ関連認証とは？その制度、メリット・デメリットを解説
掲載日：2025/2/13



中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。
本記事では、情報セキュリティや個人情報保護の取り組みに関する認証制度について説明します。

１． 認証制度とは？

認証制度とは、正確には「第三者認証制度」「第三者適合性評価制度」などと言います。
ある製品やサービス、または組織が特定の基準や規格を満たしていることを、独立した第三者機関が評価し、認証を付与する仕組みです。第三者が審査を通じて評価することで、公平性や信頼性が担保されます。

例えば、情報セキュリティ分野では ISO/IEC 27001 に基づく ISMS（情報セキュリティマネジメントシステム：Information Security Management System）や、JIS Q 15001 に基づくプライバシーマーク（P マーク）、さらには技術情報管理認証制度（TICS）などが存在します。これらの制度は、企業が情報を適切に管理し、保護するための枠組みを提供し、外部のステークホルダーに対して信頼性を示す手段として重要な役割を果たします。

【第三者認証制度の代表例】

	ISMS	プライバシーマーク（Pマーク）	TICS
正式名称	情報セキュリティマネジメントシステム Information Security Management System	個人情報保護マネジメントシステム Personal information protection Management System（PMS）	技術情報管理認証制度 Technology Information Control System
基準等	ISO/IEC 27001　国際規格	JISQ15001　日本産業規格	産業競争力強化法
評価対象	組織が情報セキュリティを確保するための仕組みをもち、その仕組みを維持し継続的に改善していることを評価	個人情報について適切な保護措置を講ずる体制を整備している事業者等を評価	技術に関する事業活動に有用な情報について組織の情報セキュリティ体制を審査・認証
目的	組織の重要情報を脅威から保護	個人の権利利益を侵害から保護	組織の「強み」となる技術等情報の漏えいを防止

２．認証制度のメリット

情報セキュリティ認証を受けることには多くのメリットがあります。
まず第一に、認証を取得することにより、企業は情報管理の枠組みを整備し、システム全体の安全性を高めることができます。

また、企業が情報セキュリティに取り組むときの共通の悩み事として、以下のようなものが挙げられます。

「何から始めたらよいか分からない。」
「どのような対策が必要なのか分からない。」
「何が成果なのか分からない。」

このような悩みの解決策として、認証の取得は、情報セキュリティ対策の進め方の手引きとして非常に役立ちます。それぞれの制度は目的に応じた規格、基準に基づいており、組織の重要情報や個人情報を適切に管理・保護するための枠組みを提供します。
これにより、リスクアセスメントを通じた脅威や脆弱性の特定、対策の計画・実施、さらに定期的な評価と改善のプロセスを体系的に行うことができるようになります。

また、認証を取得することで企業の信頼性が向上し、取引先や顧客に対してセキュリティ対策が整備されていることを証明できます。
特に中長期的な組織の持続可能性や法規制への対応を意識する場合、認証制度の枠組みは効率的かつ効果的なガイドラインとなります。

さらに、定期的に第三者機関による審査を受けることで、新たな気付きを得ることができ、取り組みへのモチベーションの維持につながります。

３．デメリットや注意点は？

一方で、情報セキュリティ認証を受けることにはデメリットもあります。
初期導入および維持にかかるコストや、認証取得および更新に必要な時間と手間が挙げられます。
特に中小企業にとっては、これらのコスト負担が大きく感じられることがあります。
また、認証を受けたからといって完全に安全が保証されるわけではなく、継続的に内部のセキュリティを見直す努力が求められます。
したがって、認証の取得はあくまでセキュリティ対策の一環であることを理解し、組織全体での意識改革と日々の運用が欠かせません。

４．各認証制度の概要

情報セキュリティ認証には、業界や分野に応じて様々な種類が存在します。ここでは特に代表的な３つの制度について触れていきます。これらはそれぞれ異なる基準や目的を持ち、企業の情報セキュリティレベルを向上させるための有効な手段となります。企業は自社のニーズやリスクに応じた認証を選択し、適切な対策を講じることが求められます。

（１）ISMS の概要

制度の概要	この認証の保護対象は企業の情報資産全般にわたります。 組織にとって価値がある情報の「機密性」、「完全性」、「可用性」※を保護するための管理システムです。 ※機密性…情報が漏えいしないようにする 完全性…改ざんや誤りがないようにする 可用性→必要なときに必要な人が利用できるようにする 技術的な対策だけでなく、従業員の教育や組織体制の整備を含めた包括的なアプローチが特徴です。 この認証を取得することは、企業間の契約や取引の際に情報資産の管理体制が明確にされていることを示すものとなり、顧客への対外的なアピールに活用できます。 国際規格であるため、グローバルな取引にも有効的です。
認証基準の概要	ISO/IEC 27001に基づいて運用されます。これは2部構成になっています。 企業が情報セキュリティを組織的に管理し、計画・実行・評価・改善（PDCAサイクル）を繰り返すことで、継続的なセキュリティの向上を目指します。
審査等の頻度	有効期限は3年 【取得時】初回認証審査を受けます。 【年1回】取得後、維持するためのサーベイランス審査を受けます。 【3年ごと】更新のための再認証審査を受けなければなりません。

参考：ISMS とは（一般社団法人情報マネジメントシステム認定センター）
ISMS パンフレット（一般社団法人情報マネジメントシステム認定センター）
※参照記事：「情報セキュリティ 3 要素（機密性、完全性、可用性）」

（２）Ｐマークの概要

制度の概要	日本産業規格「JIS Q 15001 個人情報保護マネジメントシステム－要求事項」に基づき、個人情報の適切な管理を評価する制度です。保護対象は個人情報全般にわたります。 付与対象は、国内に活動拠点を持つ事業者で、法人単位での付与となります。 認証を取得することで、消費者や取引先に対し、個人情報の取り扱いにおける信頼性を高めることができます。 また、2年ごとの更新により、継続的な改善と意識向上が図られ、企業の製品などにPマークをつけることで、消費者へのイメージアップが図れます。
認証基準の概要	個人情報保護に関する法律への適合性だけではなく、社内体制の整備や従業者の意識向上、事故の予防や発生時のリスク低減といった、より高い保護レベルの個人情報管理を自主的に確立することが求められます。
審査等の頻度	有効期間は2年間で、以降は2年ごとに更新が可能です。

参考：プライバシーマークとは（プライバシーマーク制度）：一般財団法人日本情報経済社会推進協会

（３）TICS の概要

制度の概要	法律に基づく認証制度であり、国が策定した基準に基づき、組織が情報セキュリティ対策を行い、その管理体制を第三者機関が審査・認証します。 認証を取得することで、取引先からの信頼を得ると同時に、一部の補助金などでの優遇や低利融資といった各種支援を受けられる可能性があります。
認証基準の概要	産業競争力強化法に基づいており、企業の技術情報管理体制を評価するものです。 情報が外部に漏れないようにするための具体的な対策を実施し、その有効性を専門家に審査してもらうことが求められます。
審査等の頻度	有効期限は3年 【年1回】取得後、1年ごとに定期報告を行う必要があります。 【3年ごと】更新のための審査を受けなければなりません。

参考：技術情報管理認証制度（経済産業省）

これまでの記事で参考にしてきた独立行政法人情報処理推進機構（IPA）の「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」に従ったサイバーセキュリティ対策ができていれば、いずれの認証制度にも共通する次の考え方は実施できています。

・対象にする情報資産を特定し、リスクを分析し、対策を計画する
・PDCA サイクルで継続的に改善する

それぞれの認証基準に沿うように見直しは必要ですが、全く新しい取り組みではありません。

取引先や顧客からセキュリティ対策が整備されていることを求められている場合だけでなく、継続したサイバーセキュリティ対策への取り組みを確実なものにしたい企業は、認証取得を検討してみてください。

５．まとめ

情報セキュリティ認証は、企業のセキュリティ意識を高め、対策を組織的に進める上で重要な役割を果たします。ISMS、P マーク、TICS など、それぞれの制度には独自の基準や目的があり、企業は自社のニーズに応じて導入を検討することが推奨されます。
ただし、認証取得そのものが目的化することなく、日々の業務の中で継続的にセキュリティ対策を見直し、改善する意識が求められます。適切な認証を選び、実践することで、企業の信頼性と競争力を高めていきましょう。

次回は最終回です。これまでのおさらいとして、情報セキュリティの重要ポイントを振り返ります。

レベル 3_#20_情報セキュリティ対策の重要ポイント（まとめ）
掲載日：2025/2/20



中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。
本記事も今回が今年度最終回となります。
最終回ではこれまでに取り上げた情報セキュリティ対策の要点を振り返り、その重要ポイントを整理します。

１． クラウドサービスの情報セキュリティ

クラウドサービスは今後ますます重要になっていくと考えられます。利用者としてはセキュリティを確保するための対策が欠かせません。ここでは『クラウドサービスを安全に利用するためのポイント』15 項目の中から、サービス利用者が見落としがちだが、必ず実施する必要のある対策 5 項目を再確認します。

No.3	**取り扱う情報の重要度を確認する**	クラウドサービスで取り扱う情報が漏えいしたり、改ざんされたり、消失、サービスが停止したときの影響を確認しましょう。
No.9	**利用者の認証を厳**	パスワードなどの認証機能を適切に設定・管理しましょう。

	格に行う	
No.10	**バックアップに責任を持つ**	サービス停止やデータの消失・改ざん等に備えて、重要情報を手元に確保して、必要なときに使えるようにしましょう。
No.11	**付帯するセキュリティ対策を確認する**	クラウドサービスにおけるセキュリティ対策が具体的に公開されているか確認しましょう。
No.13	**利用終了時のデータを確保する**	サービスの利用が終了したときの、データの取り扱い条件について確認しましょう。

※詳しくは「クラウドサービスを安全に利用するポイントとは（1/3～3/3）」をご参照ください。
・クラウドサービスを安全に利用するポイントとは（1/3）
・クラウドサービスを安全に利用するポイントとは（2/3）
・クラウドサービスを安全に利用するポイントとは（3/3）

２．ウェブサイトのセキュリティ

インターネットの普及に伴い、ウェブサイトは個人や企業が簡単に情報を発信するための主要な手段となりました。
しかし、これに伴いサイバー攻撃のリスクも増加しています。不正アクセスやデータ漏えい、フィッシング詐欺などの手口が巧妙化しており、これらの攻撃は利用者と運営者の信頼関係を崩壊させかねません。
こうした状況を踏まえて、安全なウェブサイト運営のためには、包括的で段階的なセキュリティ対策が欠かせません。

ここでは、ウェブサイトの運営形態の検討から構築、実際に運営するまでの３つの段階で、それぞれ取るべき安全対策について解説します。
ウェブサイトに適したセキュリティ対策を実施することで、安心できるオンライン環境の構築を目指しましょう。

ウェブサイト運営形態の検討	ウェブサイトの運営形態によってセキュリティ対策が異なるため、自社の状態に見合った運営形態を検討しましょう。 （運営形態） ・サーバー自社設置（オンプレミス） ・レンタルサーバー・クラウドサービス（PaaS） ・ショッピングモール・ASP

ウェブサイトの構築	ウェブサイトの技術的な脆弱性を認識したうえで、必要なセキュリティ対策を設計・開発の段階から検討しましょう。
ウェブサイトの運営	運用開始後に発覚した情報セキュリティ上の問題にも適切に対応し、ウェブサイトの安全性を維持向上しましょう。

※詳しくは「ウェブサイトのセキュリティ対策（1/3～3/3）」をご参照ください。
・ウェブサイトのセキュリティ対策（1/3）
・ウェブサイトのセキュリティ対策（2/3）
・ウェブサイトのセキュリティ対策（3/3）

３．技術的セキュリティ対策

情報セキュリティ対策において、技術的対策は不可欠です。
不正アクセスやマルウェア感染、機密データの漏えいといったリスクを軽減するには、ファイアウォールの設置やウイルス対策ソフトの導入が基本です。また、暗号化技術を活用することで、データの保護を強化することが求められます。

さらに、システムやソフトウェアを常に最新バージョンに更新することで、脆弱性を悪用した攻撃を未然に防ぐことができます。また、多要素認証やアクセス制御を用いて、不正な操作を防止することも有効です。

このように多岐にわたる技術的セキュリティ対策の中から特に重要なものとして、優先して実装すべき対策を以下に挙げます。

（１）ネットワーク脅威・端末対策

ネットワークの境界付近に配置して通信の処理や監視を行い、不正な通信の制御と管理を行うことで対策を実施します。

●UTM（Unified Threat Management：統合脅威管理）
ファイアウォールや IDS・IPS、メールフィルタリング、URL フィルタリングなど複数の異なるセキュリティ機能を一つのハードウェアに統合して、社内ネットワークとインターネットの脅威であるウイルスの侵入や不正アクセス、サイバー攻撃などを検知し、防御するツールです。

●WAF（Web Application Firewall）

ウェブアプリケーションの脆弱性を悪用した攻撃からウェブアプリケーションを保護する技術。例えばファイアウォールや IDS/IPS とウェブサーバーの間に設置することで、ウェブアプリケーションがやり取りするデータを監視して攻撃を検出できます。

●VPN（Virtual Private Network）

インターネットのような公衆ネットワーク上で、保護された仮想的な専用線環境を構築する技術。例えば、テレワーク勤務者が職場との間で機密性の高い電子データをやり取りする際に、VPN を利用することで暗号化による安全な通信ができます。

（２）コンテンツセキュリティ対策

プログラム実行や電子メール送受信、ウェブ閲覧などを、その内容（コンテンツ）によって制御することで対策を実施します。

●ウイルス対策

ウイルスを検知・駆除することで、ウイルスに感染するのを防ぐための対策。例えば、利用するパソコンにウイルス対策ソフトをインストールしてウイルス定義ファイルを最新の状態にすることで、既知のウイルスを検知できます。

（３）アクセス管理

情報システムの利用者を、認可及び制限する機能を提供します。

●アクセス制御

利用者や情報機器がデータなどにアクセスすることができる権限や認可を制御する技術。例えば、業務で使用するクラウドサービスなどを事務所のみで利用可能とするアクセス制御を行うことで、事務所外からデータへの不正アクセスのリスクを軽減できます。

（４）システムセキュリティ管理

組織が保有する IT 資産について、一元的な管理や脆弱性を検出する機能を提供します。

●ログ管理

サーバーなどに誰がログインしたか、どのデータに対してアクセスがあったかは、サーバー上にログファイルとして記録されます。

サイバー攻撃があった場合、このログファイルに書かれている内容をもとに、情報漏えいが生じたかどうかを分析するので、ログファイルをどのように管理するかの方針を、組織として定めておくことは重要です。
一方で、ログファイルの内容を十分に理解するには専門的な知識が必要となるため、こうした管理を容易にするためのツール類も提供されています。

※詳しくは「技術的セキュリティ対策（1/2～2/2）」をご参照ください。
・技術的セキュリティ対策（1/2）
・技術的セキュリティ対策（2/2）

４． セキュリティインシデント対応

サイバー攻撃の手法がますます巧妙化する中で、セキュリティインシデント（情報漏えいや改ざん、破壊・消失、情報システムの機能停止、またはこれらにつながる可能性のある事象など）が増加しています。

昨今の状況を踏まえると、予防策を講じるだけではなく、インシデント発生をあらかじめ想定し、被害を最小化する手順を整備しておく必要があります。これを実現するためには、インシデント対応を３つのフェーズに分け、それぞれで効果的な対応策を想定しておくことが求められます。

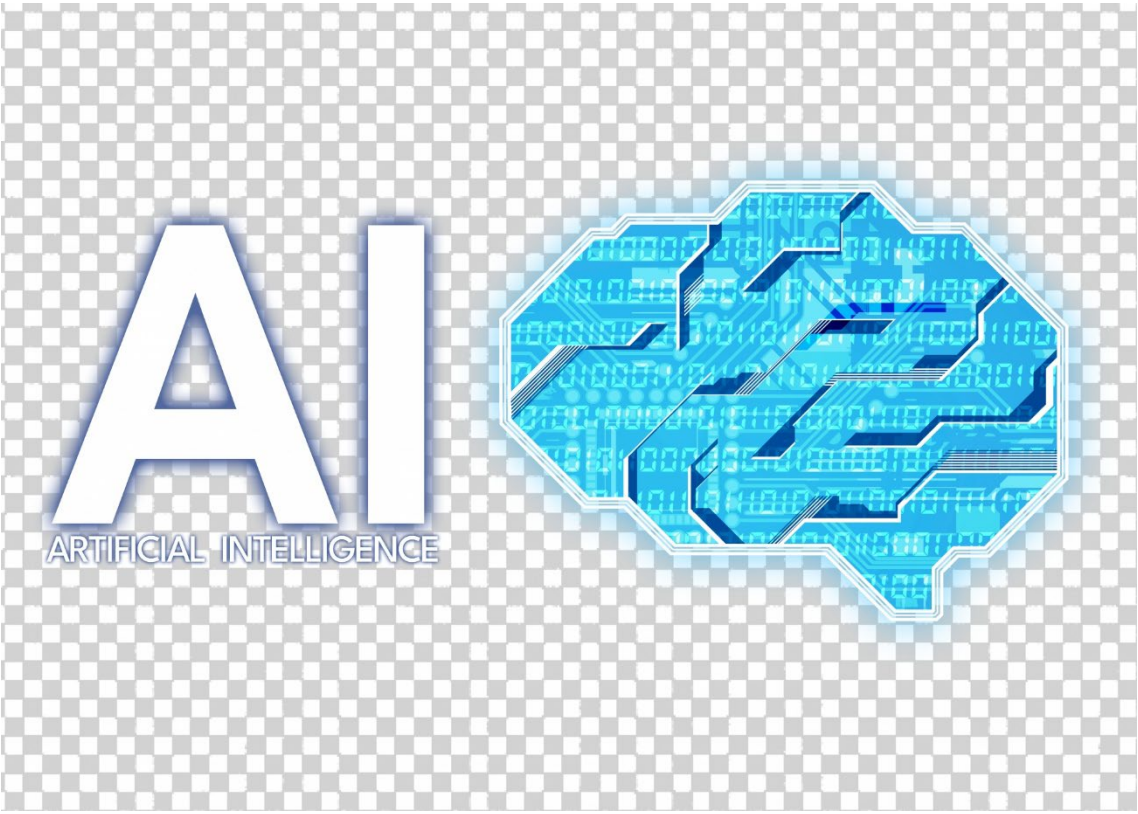
①検知・初動対応	インシデントを検知した場合、速やかに情報セキュリティ責任者に連絡し、被害を拡大させないための初動対応を行いましょう。
②報告・公表	顧客や関係者、行政機関、一般・メディア等に対して、必要に応じてタイムリーに公表や情報の開示を行いましょう。
③復旧・再発防止策	システム管理者や外部専門組織と協力して、迅速な復旧作業や根本的な再発防止策を検討しましょう。

※詳しくは「セキュリティインシデント対応（1/2～2/2）」をご参照ください。
・セキュリティインシデント対応（1/2）
・セキュリティインシデント対応（2/2）

全 20 回にわたり「もっと知りたい！セキュリティ」を配信してきました。
本記事が、お読みいただいた皆さまの情報セキュリティに関する知識向上のお役に立てることを願っています。

※この記事は、独立行政法人情報処理推進機構（IPA）作成の中小企業の情報セキュリティ対策ガイドライン第 3.1 版に基づいて作成しています。

一般向け 1_＃1_AI とサイバーセキュリティ
掲載日：2024/7/1



皆さんは日々の業務や生活の中で、AI を活用していますか？特に最近では、生成 AI の進化が著しく、様々な分野でその活用が進んでいます。しかしその一方で、AI の利用によるセキュリティリスクも増大していることをご存知でしょうか。

AI 利用時の注意点

生成 AI のサービス（ツール）を使う時には、個人情報や機密情報を含めないようにと言われています。この注意点は、実は生成 AI に限ったことではありません。
利用時に入力した情報をサービス提供者が利活用できる規約がある場合、その情報は漏えいしてしまう危険があります。特に生成 AI では、サービス提供者に加えて、他の利用者もあなたが入力した情報を利用できてしまうのです。プレゼン資料などを作成するツールやサービスは便利ですが、なおさら利用規約を詳細に確認することが重要です。

そして、規約を守っているとはいえ、サービスを提供している事業者にも注意を払う必要があります。

AI を使う時の注意事項はこれくらいにしておいて、ここからは、AI 技術がサイバーセキュリティにもたらす脅威についてお話しします。

サイバーセキュリティへの AI の影響

皆さんは、翻訳サービスを使ったことはありますか？少し前までは翻訳サービスを使って翻訳された日本語はかなり不自然でした。しかし最近は技術の進化により、以前よりも自然な日本語が生成されるようになりました。生成 AI を使って作成された文章もそうですよね。これは今まで、不審なメールを見分けるのに「不自然な日本語かどうか」で判断するようにと言われていましたが、こういった判断ができなくなることを意味しています。

さらに標的型メール攻撃の場合、攻撃者は普段のメールのやり取りから、その人の癖に合わせた、より自然な文章を生成し、メールを送ってくるようになるでしょう。そうすると、メールの文面だけでは見分けがつかなくなる可能性が高まります。

コード生成 AI とマルウェアのリスク

最近では、「コード生成 AI」という言葉も耳にするようになりました。コード生成 AI というのは、プログラムを作るときにこんなふうに作ればいいよと教えてくれるとても便利な機能です。
この技術を使えば、プログラムの作成が容易になり便利ですが、同時に攻撃者もマルウェア（※マルウェアとは、悪意あるプログラムの総称で、コンピュータウイルスなどのことです。）と呼ばれる悪意のあるプログラムを容易に作成できてしまうのです。2024 年 5 月には、全国で初とみられる生成 AI によるウイルス作成容疑での摘発が実際に起きています。（出典：生成ＡＩでウイルス作成容疑　男逮捕「楽に稼ぎたかった」―遠回しの質問で回答引き出す・警視庁：時事ドットコム（jiji.com））

また、有名人の声や画像を悪用したフェイクニュースも話題となっていますが、これらの技術を使えば、社内や取引先の人になりすますことだって可能です。音声のみのオンライン会議では、攻撃者がなりすましていても見抜くのは難しいでしょう。将来的には、画像や動画でもなりすますことができるようになるでしょう。

サイバー攻撃の低コスト化と中小企業の脆弱性

AI の進化により、サイバー攻撃のハードルが下がったとも言えるでしょう。言い換えると、攻撃を低コストで行えるようになってきたということです。

身代金を要求するランサムウェア攻撃を仕掛ける際、少額の要求でも割に合うようになりますし、情報搾取を目的とした攻撃では、少量の情報で目的を達成できるようになってしまいます。このような状況は、中小企業がより狙われやすくなるということだと考えられます。

最後に、今回の話でサイバーセキュリティへの取り組みが以前にも増して重要であることをご理解いただけましたでしょうか。東京都では、中小企業向けにサイバーセキュリティに関する様々な支援策を実施しています。
東京都の取り組み：(https://www.cybersecurity.metro.tokyo.lg.jp/torikumi/#page1）
ぜひ、これらの施策を有効に活用して、安心・安全な事業環境を構築してください。

一般向け 1_#2_同報メール送信での個人情報漏えいの事例に学ぶ、身近なセキュリティ対策
掲載日：2024/7/22



皆さんはメールを送信するとき、送信先をどのように指定していますか。
宛先（TO）、CC、BCC を使い分けていますか。
また使い分けるよう社内に徹底、確認していますか。

ニュースの報道でご覧になった方もいらっしゃると思いますが、2024 年 6 月 3 日に最高裁判所が、送信先の指定方法を誤り、個人情報を漏えいさせる事故（修習資金の被貸与者に対する不要な個人情報の送信について）を起こしました。
この事故の原因は、送信先のメールアドレスを BCC に入力すべきところを誤って宛先（TO）欄に入力してメールを送信してしまったことです。

事故を防ぐには、宛先、CC、BCC の違いを確認することです。

- **宛先（TO）**：メールを読んでほしい相手のメールアドレスを指定する欄です。
- **CC：**Carbon Copy の略で、書類では「ご参考」として配布する先を指定します。
- **BCC：**Black Carbon Copy の略で、Black は見えないことを意味します。

BCC に指定したメールアドレスは、受信者側からは見えません。逆に宛先や CC に指定したメールアドレスは、全てのメール受信者に公開されます。

独立行政法人情報処理推進機構（IPA）が発行している「中小企業の情報セキュリティ対策ガイドラ

イン 第 3.1 版」の「付録 5：情報セキュリティ関連規程（サンプル）」によれば、＜メールアドレス漏えい防止＞として次のように記されています。

> 同報メール（外部の多数相手に同時に送信するとき）を送信する場合は、宛先（TO）に自分自身のアドレスを入力し、BCC で複数相手のアドレスを指定する。

上記、最高裁判所の事例では、同報メールを送信する場合は相手のメールアドレスを BCC に指定するルールがあったにも関わらず守られていなかったようです。

メールアドレスの漏えいを防ぐためのステップは、以下のとおりです。

１．同報メールを送信する場合は、宛先に自分自身のアドレスを入力し、BCC で複数の送信先アドレスを指定する。このルールを定めて、社内に徹底することが同報メールでメールアドレスの漏えいを起こさない第一歩です。
また、ルールを繰り返し周知することと、それが守られているか現場の状況を普段から確認することが大切です。

２．周知する際には、なぜ BCC に指定するのか、指定しなかった場合メールアドレスが知られたくない相手に知られてしまうリスクや、メールの内容によっては事故や事件になることを伝えてください。

３．状況を確認する際は、同報メールの送信先を BCC に指定しているかだけでなく、誤って宛先や CC に指定しそうになったヒヤリハットが無いか聞き出し、改善策を検討してください。

ヒヤリハットが繰り返し発生している場合は、ルールの周知徹底だけでは防げず、人手に頼らない仕掛けが必要かもしれません。
例えば、同報メールを手作業で送信するのをやめて、送信先を登録した一覧とあらかじめ用意した本文の情報を使って自動的にメールを送信するといった仕掛けなども検討してみてください。

なお、メールアドレスについて個人情報保護委員会は次の見解を出しています。

> メールアドレスのユーザー名及びドメイン名から特定の個人を識別することができる場合（例：kojin_ichiro@example.com）、当該メールアドレスは、それ自体が単独で、個人情報に該当します。
> これ以外の場合、個別の事例ごとに判断することになりますが、他の情報と容易に照合することにより特定の個人を識別することができる場合、当該情報とあわせて全体として個人情報に該当することがあります。

同報メールで送信先アドレスが 1,000 件を超えることは稀だと思いますが、送信内容によっては、要配慮個人情報（本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報）と関連づけられる、または不正に利用されることにより財産的被害が生じるおそれがある場合は、個人情報保護委員会への報告が必要となります。

日常的に行なっている同報メールによる情報漏えいの危険性は、身近なセキュリティ対策と意識で低減させることが可能です。
皆さんの会社で同報メールに起因した個人情報漏えいの事故が起きないことを願っています。

一般向け 1_#3_「サイバーセキュリティアワード 2023」の紹介
掲載日：2024/7/29



皆さんは、サイバーセキュリティアワードという賞をご存知でしょうか？

サイバーセキュリティアワードは、デジタル政策フォーラムが主催する賞で、サイバーセキュリティだけでなくプライバシーなどに関する知識や分析を、一般の人にもわかりやすく伝えるために行われています。
書籍や Web、フィクションなどの優秀な作品を選定し表彰することで、サイバーセキュリティやプライバシー、信用・信頼などに関する理解や認識を促進させることを目指しています。

この賞は、「サイバーセキュリティ」をより身近に感じてもらい、日本におけるサイバーセキュリティ・リテラシーの向上と、イノベーションの活性化に寄与することを目的としています。

サイバーセキュリティアワード 2023 の書籍部門で最優秀賞を受賞したのが、『**「サイバーセキュリティ、マジわからん」と思った時に読む本**』（大久保 孝雄 著、オーム社 刊、ISBN：978-4-274-23103-2）です。

サイバーセキュリティアワード 2023 の表彰式開催レポートに掲載された「審査委員長講評より抜粋」によれば、この書籍は次のように紹介されています。

「「サイバーセキュリティ、マジわからん」と思ったときに読む本」は思わず手に取ってみたくなる書籍タイトル

で、サイバーセキュリティの基礎から技術的な事項まで網羅されています。また日常的なテーマからの視点や、イラストを活用したわかりやすい内容になっている点が高く評価されました。

「サイバーセキュリティアワード 2023　表彰式開催レポート」より転載

この本で紹介されている対策内容は、一般社員が実施する一般的なものです。従って、セキュリティポリシーなどの組織的な対策の内容は含まれていません。

一方、「サイバー攻撃のしくみを知ろう」という章では、パスワードがどのように破られるのか、それにどれくらい時間がかかるのかといったことがわかりやすく解説されているので、なぜ対策が必要なのかが理解でき、社員一人一人が意識をもってサイバーセキュリティに取り組むようになる内容となっています。

多くの項目が見開きで解説されているので、少しずつ読み進められる点も良いのではないでしょうか。IT やサイバーセキュリティに詳しい人がいないという企業では、社員のサイバーセキュリティへの意識を高めるために活用されてはいかがでしょうか。

専門知識がない社員でも、サイバーセキュリティの基礎知識を身につけることができる本となっています。

一般向け 1_#4_狙われやすい Web サイト（脆弱性の脅威と対策）　～IPA NEWS vol.67 より～
掲載日：2024/8/5



皆さんは、独立行政法人情報処理推進機構（IPA）が隔月で発行している「IPA NEWS」をご存知でしょうか？

IPA NEWS は、IPA の日々の活動内容や成果を紹介し、IPA の活動への理解および事業成果の普及推進等を図ることを目的とした広報誌です。IPA NEWS は IPA のホームページで公開されています。最新号は 2024 年 7 月号（Vol.67）です。

中でも注目すべきは、「セキュリティのすゝめ」というコーナーです。毎号、セキュリティに関する重要な情報が掲載されています。

今回は最新号の「セキュリティのすゝめ 16―ウェブサイトの脆弱性の脅威と対策」から最新情報をご紹介します。大見出しは「サイトのセキュリティの弱点 「脆弱性」に今すぐ対応を！」となっています。さらには、「放置しておくとサイバー攻撃を招く恐れも…」となんともおっかなびっくりの言葉が続いています。

多くの企業が Web サイトを運営していることを考えると、今回のお話は非常に重要です。ぜひ最後まで読

んでください。

「セキュリティのすゝめ 16」は、以下の３つのトピックスで構成されています。
（１）CMS の脆弱性を突き、サイトを乗っ取る事件も
（２）情報セキュリティ５か条で被害軽減を図る
（３）脆弱性対策は経営課題という認識を

CMS の脆弱性とは

最初の項目でいきなり CMS と出てきて、面食らった方が多いと思います。

CMS とは「コンテンツ・マネジメント・システム」の略称で、専門的な知識がなくてもブログのように Web ページの作成や公開、更新が誰にでも簡単にできるシステムのことです。代表的なものに WordPress や Wix が挙げられます。

CMS にはブラウザの拡張機能のように、Web サイトの管理・更新をしやすくするためのプラグインという追加機能があります。お問い合わせフォームなどはプラグインで設置される代表例です。

これらの CMS やプラグインには、脆弱性が見つかることがあります。

脆弱性とは、システムの不具合や設計ミスなどが原因で発生する、セキュリティ上の欠陥を指し、セキュリティホールとも呼ばれるものです。このセキュリティホールは、サイバー攻撃に狙われやすく、悪用されるとウイルス感染や情報漏えいなどの被害を受けるリスクがあります。実際、CMS の脆弱性を第三者が突き、管理者パスワードが盗まれることによって、Web サイトが改ざんされる事件も発生していると書かれています。
事例：CMS の脆弱性突かれ、サイトが改ざん被害

脆弱性への対策

そして、脆弱性への基本の対策として挙げられるのが、２つ目の項目「情報セキュリティ５か条」です。これは IPA が策定しているもので、実践して被害軽減を図りましょうというものです。

「情報セキュリティ５か条」は次の５つです。

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！

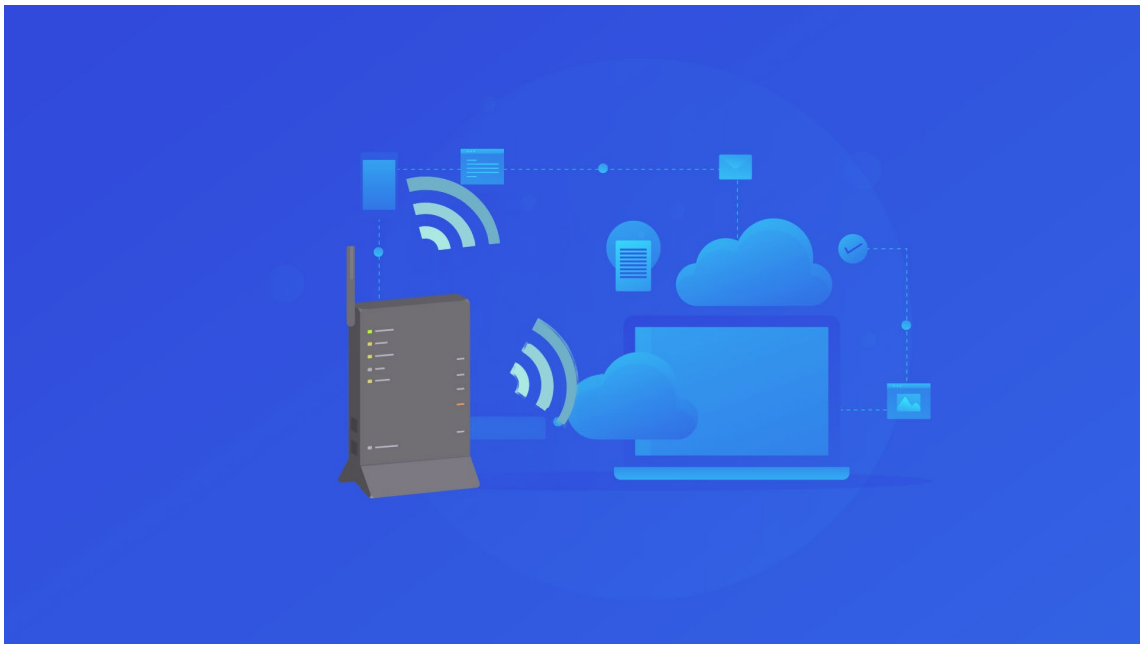
CMS の脆弱性対策はこのうちの「①ソフトウェアは常に最新の状態に」することが該当します。「情報セキュリティ 5 か条」は普段使っているパソコンやスマホなどだけではなく、Web サイトのシステムやプラグインなどにも実践することが大切です。

さらに、Web サイトの管理者情報については、「③パスワードを強化」も実践してください。多要素認証などパスワード以外の認証が用意されている場合は、そちらも利用しましょう。管理者になりすましてログインされ、画面を改ざんされたり情報が漏えいすることを防ぎましょう。

皆さんの会社では Web サイトの運用はどのようにされていますか？
外部へ委託している場合でも、万が一事故が起きれば皆さんの会社が責任を負うことになります。脆弱性を放置したままでは Web サイト運営、ひいては事業継続に悪影響が生じかねません。脆弱性対策をシステム管理者や委託先任せにしないで、経営課題として認識してくださいというのが３つ目の項目です。

この機会にシステム管理者あるいは委託先と、脆弱性対策の状況を話し合ってみてください。そして定期的にサイトの状況を経営者自らが確認することをお勧めいたします。

一般向け 1_#5_無線 LAN ルーターに潜む危険性
掲載日：2024/8/19



今回は、多くの家庭で使われていて、職場でも使われることがある無線 LAN（Wi-Fi）ルーターに潜む危険性について説明します。

無線 LAN ルーターは、様々な機器をインターネットに接続する装置です。
この無線 LAN ルーターが、悪意を持った第三者に外部から操作されてしまうことがあります。第三者は、無線 LAN ルーターのセキュリティに弱い面（脆弱性）を見つけ、ルーターに接続する機器の通信を覗き見したり、不正サイトへ誘導したりします。
このため、無線 LAN ルーターの脆弱性対策が必要になってきます。

万が一、脆弱性をそのままにしておくとどのような被害に遭う可能性があるのでしょうか。
具体的な被害事例をご紹介します。

事例：通信が傍受され、銀行口座の認証情報が漏えい
被害者は、脆弱性のある無線 LAN ルーターを使っていたところ、第三者に悪用されてルーターの設定を変えられてしまいました。
攻撃者は、被害者の通信を盗み見し、ネットバンキングや様々なシステムのログイン ID とパスワードを搾取。

盗まれたログイン ID とパスワードで銀行の不正送金の被害に遭ってしまいました。

参考サイト：トレンドマイクロ社
https://www.trendmicro.com/ja_jp/research/17/b/attacks-on-routers-what-kind-of-damage-do-they-cause-and-what-can-you-do-about-them.html

上記の被害事例ではネットバンキングのログイン ID とパスワードが漏えいしましたが、業務で利用する情報システムのログイン ID とパスワードが同じように漏えいすれば、会社や顧客の機密情報が第三者によって不正に取得されることに繋がります。

テレワークを行なっている企業では、従業員の自宅の無線 LAN ルーターの脆弱性を突かれ、業務システムのログイン ID とパスワードが搾取されるケースも考えられます。

このほかにも、不正サイトへ誘導されたり、マルウェアを送り込まれたりする危険性もあります。

ルーターのメーカーは脆弱性がないように細心の注意を払っていますが、製造時に脆弱性を見逃したまま出荷してしまうことがあります。
出荷後に脆弱性が見つかった場合、メーカーは対策情報を出すようにしています。

皆さんは、無線 LAN ルーターの脆弱性対策を行っていますか。

国内で使用されているソフトウェアなどの脆弱性関連情報と、その対策方法を提供している**脆弱性対策情報ポータルサイト(JVN)**があります。
ここには、無線 LAN ルーターの脆弱性情報が 2024 年に公表されたものだけでも、下表のように多く登録されています。

ID	タイトル
JVNDB-2024-003249 (JVNVU#97214223)	エレコム製無線 LAN ルーターにおける OS コマンドインジェクションの脆弱性
JVNDB-2024-003025 (JVNVU#95381465)	エレコム製無線 LAN ルーターにおける複数の脆弱性
JVNDB-2024-002831 (JVNVU#99444194)	エレコム製無線 LAN ルーターにおける OS コマンドインジェクションの脆弱性

JVNDB-2024-001061 (JVNVU#90908488)	エレコム製無線 LAN ルーターにおける OS コマンドインジェクションの脆弱性
JVNDB-2024-000040 (JVN#58236836)	バッファロー製無線 LAN ルーターにおける複数の脆弱性
JVNDB-2024-000020 (JVN#44166658)	エレコム製無線 LAN ルーターおよび無線 LAN 中継器における複数の脆弱性

（JVN iPedia で、検索キーワード：無線 LAN ルーター、公表日：2024 年 01 月～で検索し、無線 LAN ルーターに該当するタイトルだけを掲載）

総務省は、「無線 LAN（Wi-Fi）の安全な利用（セキュリティ確保）について」という Web サイトを公開しており、そこにはルーター利用時の注意点（「自宅 Wi-Fi 利用者向け 簡易マニュアル（令和 6 年 3 月版）」）が掲載されています。
マニュアルのタイトルは「自宅 Wi-Fi」となっていますが、職場で利用する無線 LAN ルーターにおいてもこのマニュアルを適用できます。

ここでは、このマニュアルの中から、特に重要な 2 点についてご紹介します。

（1）パスワードを第三者に推測されにくいものにする

パスワードには、インターネットに接続する際に必要なパスワード(SSID のパスワード)と、無線 LAN ルーターの設定画面にログインするためのパスワードの 2 つがあります。
これらのパスワードは初期設定時のパスワードから、推測されにくいものに変更しましょう。

（2）ファームウェアを最新にする

無線 LAN ルーターのファームウェア(ソフトウェア)に脆弱性が見つかった場合は、JVN に登録される※とともに、製造元メーカーから修正版のファームウェアが提供されます。
無線 LAN ルーターを購入した時は、メーカーサイトでユーザ登録をしてメールアドレスも登録しましょう。
メーカー側から脆弱性情報が配信されることもあります。
また、JVN サイトにも登録をしておくことで、最新の脆弱性情報をメールで受け取ることができます。
※海外メーカーの場合は JVN ではなく、各国・地域の同様の情報に登録されることがあります。

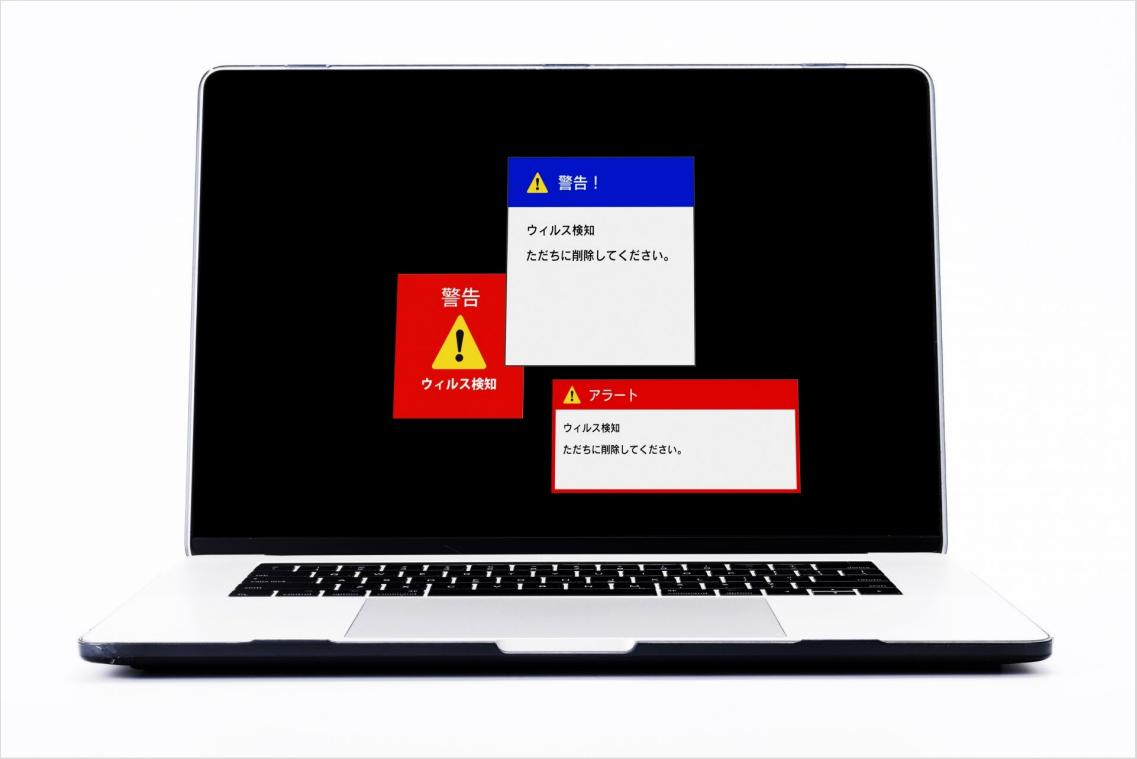
上記以外の対策や詳しい内容は、「無線 LAN（Wi-Fi）の安全な利用（セキュリティ確保）について」をご参照ください。

※このサイトでは、わかりやすい解説動画も公開しています。

職場で無線 LAN ルーターを利用している場合は、上記のガイドラインとルーター機器のマニュアルを見ながら設定を見直してみてください。
自宅でテレワークを行う従業員がいる場合は、対策について従業員へも周知徹底し、安心してテレワークができる環境を構築してください。

一般向け 1_#6_サポート詐欺の脅威

掲載日：2024/9/2



皆さんは、パソコンで作業中に以下のようなウイルス感染やパソコンの不具合を知らせる画面が表示されたらどのようにしますか？



出典：警察庁サポート詐欺対策

https://www.npa.go.jp/bureau/cyber/countermeasures/support-fraud.html

突然のことでびっくりしますね。画面上に表示されている電話番号に電話をしたら、ヘルプデスクに繋がって助けてくれると思うかもしれません。または、表示されているボタンをクリックしてみるかもしれません。

しかし、これは数年前から被害が多発している「サポート詐欺」の可能性があります。今回はサポート詐欺について説明します。

サポート詐欺とは

サポート詐欺は、インターネットを閲覧中に画面に突然表示される「ウイルス感染」などの嘘の警告を利用して、被害者を騙す手口です。
まずは、具体的な事例を紹介し、その脅威と対策について説明します。

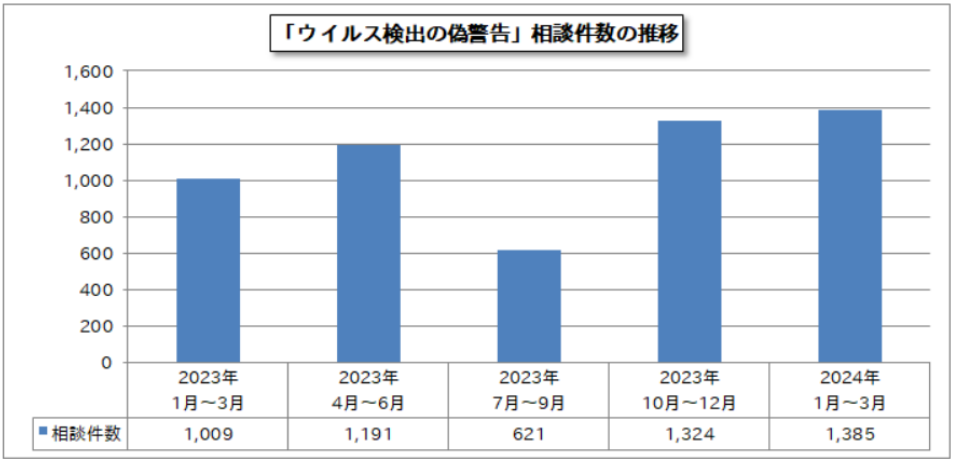
【事例：笛吹市商工会の被害】

笛吹市商工会が 1000 万円詐欺被害　パソコンにうその警告
引用元：NHK（https://www3.nhk.or.jp/lnews/kofu/20240318/1040022800.html
　2024 年 3 月 18 日掲載記事から一部抜粋）

笛吹市商工会によりますと、先月 27 日、職員の業務用パソコンの画面にコンピューターウイルスとして知られている「トロイの木馬に感染した」という嘘の警告が出ました。
あわてた職員が表示された「サポート窓口」に電話をかけると、大手ソフトウェア会社の職員を名乗る人物から、「インターネットバンキングにもウイルスが侵入している可能性がある」などと伝えられました。
それを信じた職員がパソコンで管理していた４つの金融機関のインターネットバンキングのパスワードなどを伝えたほか、パソコンを遠隔操作できるような情報も伝えてしまったということです。
そして、その日の夜にパソコンを遠隔操作され、一つの口座からあわせて 1,000 万円が不正に送金されたということです。
不審に思った別の職員が同じような詐欺の手口があることに気付き、調べた結果だまされたことがわかったということです。
笛吹市商工会は警察に被害届けを出すとともに、個人情報が流出していないかどうか調べています。

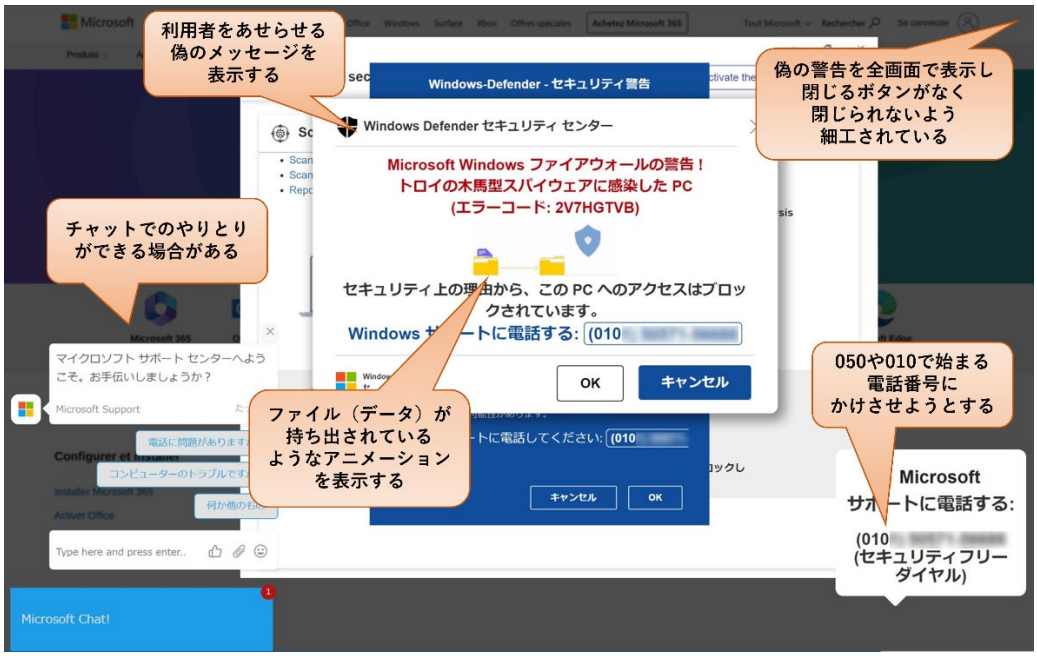
増加するサポート詐欺の被害

このようなサポート詐欺は、近年非常に増えており、独立行政法人情報処理推進機構（IPA）には、2024 年 1 月から 3 月の間だけでも 1,385 件の相談が寄せられています。



出典：IPA 情報セキュリティ安心相談窓口の相談状況［2024 年第 4 四半期（1 月～3 月）］
https://www.ipa.go.jp/security/anshin/reports/2024q1outline.html

【偽のセキュリティ警告画面】



出典：偽セキュリティ警告（サポート詐欺）対策特集ページ
https://www.ipa.go.jp/security/anshin/measures/fakealert.html

サポート詐欺に使われる偽のセキュリティ警告画面（上記画面参照）は、インターネットを閲覧中に突然表示されます。

あわてて画面をクリックすると、ディスプレイいっぱいに表示されてしまい、マウス操作で閉じることができなくなってしまいます。
このとき、表示されているサポート電話番号に電話をしてしまうと、思わぬ被害に遭います。

では、このような被害に遭わないためには、どのようにしたら良いのでしょうか。

サポート詐欺への対策

まずは、パソコン操作中に普段見慣れない警告画面が出た場合、あわてずに社内の IT 担当者や信頼のおける情報システム関係の取引先に相談することが大切です。自身の判断で表示された電話番号に電話したり、不明なリンクをクリックすることは避けましょう。

パソコンを操作していた本人は、「私が問題を起こしてしまったのではないか」、「自分が何とかしなければ」と考え、不審な電話番号に電話をし、騙されてしまいます。誰かに相談をすれば「それは怪しくないか。解決方法を自分たちで調べてみよう」など、他の対応案が出てくるかもしれません。

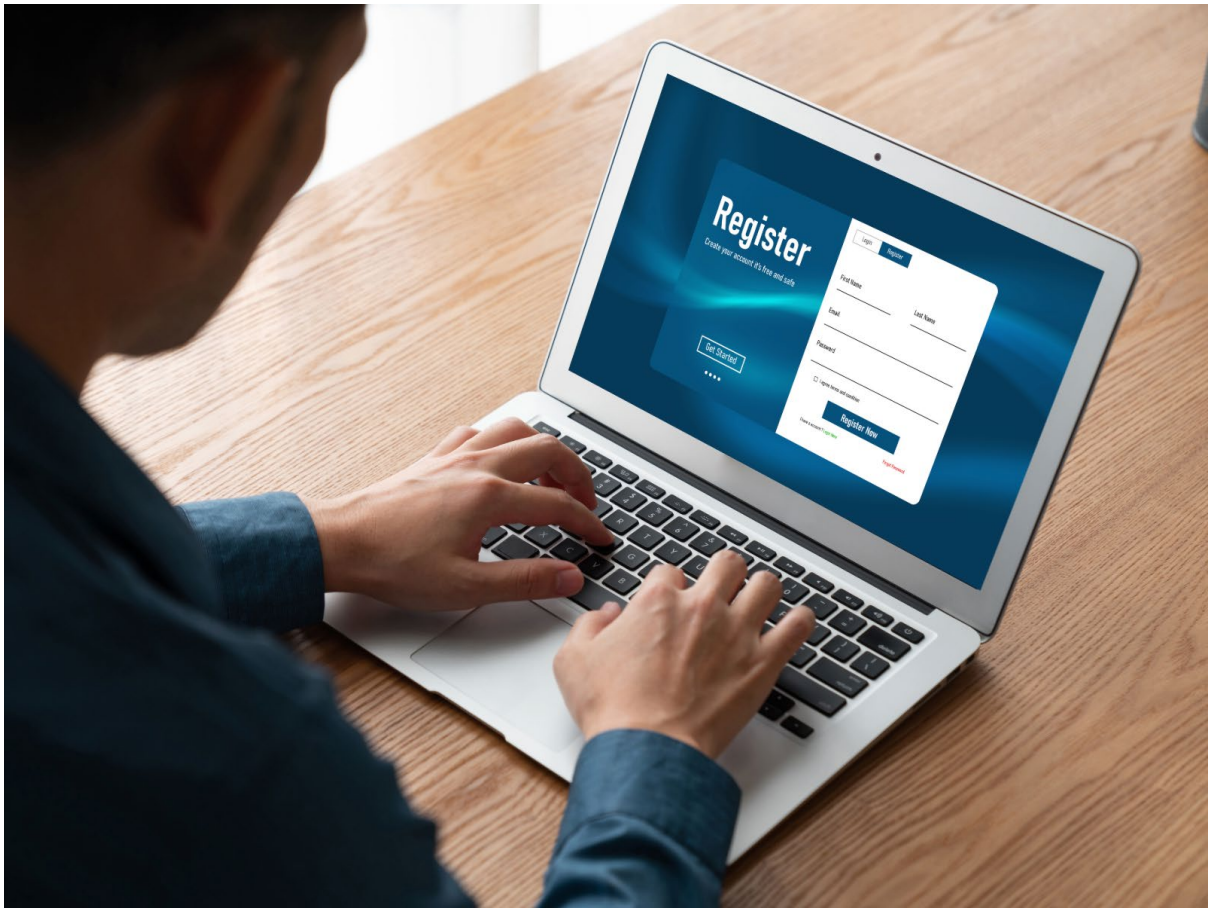
また、サポート詐欺では、被害者のパソコンを遠隔操作するために不正なプログラムをインターネット上からダウンロードしてインストールするように促してくることもあります。パソコンの OS やセキュリティ対策ソフトの定期的なアップデートを行っておくことで、そのような不正なソフトウェアのインストールを防ぐことも可能です。

IPA では、サポート詐欺に遭わないための予防策として、「偽セキュリティ警告画面」を疑似体験できる Web サイトを提供しています。
https://www.ipa.go.jp/security/anshin/measures/fakealert.html

このサイトを活用して、従業員向けの情報セキュリティ研修を行うことを推奨します。

避難訓練と一緒で、日頃からの訓練が大切です。実際に疑似体験をしておくことで、突然の偽の警告画面に冷静に対応できるようになり、サポート詐欺の被害を回避するための意識を高めることができます。

一般向け１_#7_Web 入力画面（申し込みフォーム）などの設定ミスによる情報漏えい
掲載日：2024/9/16



今回は、Web アンケートやイベントなどの申し込みフォーム、会員登録画面などの危険性について説明します。

皆さんはセミナーへの参加申し込みや会員登録を行う際に、Web ページの案内に従って、フォームに個人情報を入力したことはありませんか？
現代社会において、インターネットから様々な申し込みや登録を行うことは日常的なこととなっています。

Web フォームの作成と利用状況

下記画像は、実在する申し込みフォームではなく、本記事の為に作成したサンプルです。



このようなインターネット上で利用できる Web フォームは、無償または低コストで簡単に作成できるため、多くの企業をはじめ様々な組織が利用しています。代表的なものに Google フォームが挙げられます。
皆さんの会社でも、利用したことがあるかもしれません。
しかし、その使いやすさが裏目に出ることもあります。簡単な作成方法ゆえに、設定ミスが発生しやすいのです。

利用者と管理者の役割

Web フォームには情報を登録する利用者と、その情報を管理する管理者（フォームを設置する側）が存在します。

（１）利用者（情報を登録する人）：自分の情報のみを入力。本来、他の利用者が登録した情報は見られない
（２）管理者(主催者)：登録者全員の情報を見ることができる

しかし設定を間違えると、利用者に他の利用者の登録情報が見えてしまうことがあります。

近年発生している個人情報漏えい事件の中には、この Web フォームに起因するものが多数あります。
実際に発生した事例を 1 つご紹介します。

【事例：イベント申し込みフォームでの情報漏えい】

公益社団法人自動車技術会は、イベントへの参加登録を行う登録画面(Web フォーム)において、アクセス権限に設定ミスがあり、本来イベント事務局しか見ることができない登録者に関する個人情報を誰もが閲覧できる状態にしてしまったことを明らかにしました。
同会によれば、申し込み登録者の個人情報(氏名、メールアドレス、所属する組織名など)をインターネット経由で閲覧できる状態となっていたとのことです。参加申込みに「Google フォーム」を利用した際、共同編集者が「URL リンクを知っている全員」に設定されていたため、URL がわかれば誰でも個人情報を閲覧できる状態になっていたようです。
引用元サイト：Security Next
https://www.security-next.com/159389

Web フォームの危険性

ここでは、Web フォームの権限設定ミスがもたらす主な危険性について解説します。

（１）情報漏えいのリスク

権限設定ミスにより、第三者が機密情報にアクセスできる状態になると、個人情報や企業の重要情報が漏えいする危険性があります。

（２）企業の信頼失墜

顧客情報が漏えいすると、企業の信頼が損なわれる可能性があります。これは、顧客からの信頼を失うだけでなく、ブランドイメージの低下にもつながります。

（３）法的リスク

個人情報保護法や GDPR※など、各国のデータ保護規制に違反する可能性があり、罰金や訴訟リスクを抱えることになります。
※GDPR：一般データ保護規則。EU 加盟国及び欧州経済領域の一部であるアイスランド、ノルウェー、リヒテンシュタインの個人データ保護を規定する法。

正しい権限設定のためのポイント

権限設定を正しく行うためには、以下のポイントに注意することが重要です。

（１）正しい手順の確認

Web フォームは、誰でも簡単に利用できるように操作説明書を読まなくても直感的に操作・作成できるようになっています。
しかし、正しい手順を理解しないまま「何となく」で操作してしまうと、設定を誤り情報漏えいに繋がる可能性があります。必ず公式のマニュアルやヘルプ情報を確認しながら作業を行いましょう。

（２）複数人でのチェックを行う

作成したフォームは必ず複数人でチェックを行いましょう。また、実際の情報を登録してみて、正しく画面が動くか、他人の登録情報などが閲覧できないか等、チェックを行います。
「自分はシステムに詳しくないから、若い人に任せよう」で組織として確認を行わないことは最も危険な行為です。

（３）最小権限の原則

必要最低限の権限のみを付与することで、アクセス制御を厳格に行います。例えば、データ入力者にはデータ閲覧権限を与えず、管理者だけが全てのデータにアクセスできるようにします。

（４）定期的な権限確認

定期的に権限設定を見直し、不必要な権限が付与されていないか確認します。

情報漏えいは企業にとって重大な問題です。しかし、適切な権限設定とセキュリティ対策を講じることで、そのリスクを大幅に低減することが可能です。
常に最新のセキュリティ情報を把握し、適切な対策を継続的に実施することが重要です。
企業の信頼を保ち、法的リスクを避けるためにも、これらの対策は欠かせないものになります。

一般向け 1_#8_Zoom の脆弱性
掲載日：2024/9/30



コロナ禍以降、オンライン会議を利用する機会が増えましたが、皆さんの組織ではオンライン会議にどのようなツールを利用していますか？
Zoom を使っている組織も多いと思います。
Zoom は非常に便利なツールですが、一方でセキュリティの脆弱性も存在します。
本日は、Zoom の脆弱性に関する最新情報や対策について詳しく解説します。

１．Zoom の新たな脆弱性

2024 年 7 月、Zoom は 8 件の脆弱性を対処したことを公式に発表しました。
そのうちの 1 件は、重要度「高」と評価された脆弱性であり、即座にアップデートを行うことが強く推奨されています。多くの組織がリモートワークを導入している現代において、オンライン会議ツールのセキュリティ強化は非常に重要です。

２．脆弱性とは？

まず、脆弱性という概念を理解することが重要です。「狙われやすいWebサイト（脆弱性の脅威と対策）～IPA NEWS vol.67 より～」【ホットトピックス#4】の記事でも説明しましたが、脆弱性とは、システムの

不具合や設計ミスなどに起因するセキュリティ上の欠陥を指し、セキュリティホールとも呼ばれるものです。
セキュリティホールは、攻撃者に悪用される可能性があり、不正アクセスやデータ漏えい、システムの機能停止など深刻な被害をもたらすリスクがあります。

３．脆弱性の対処法

脆弱性は、攻撃者に悪用される危険性があるため、発見されたら迅速な対応が求められます。
開発ベンダーは早急に脆弱性を修正したプログラム（セキュリティパッチ）を開発・配布します。
利用者は、ベンダーが配布するセキュリティパッチを速やかに適用する必要があります。
以下に、脆弱性が公表された際に取るべき基本的な対処法を説明します。

（１）公式情報の確認

まずは、ソフトウェア会社やセキュリティ機関の公式発表を確認してください。公式発表は、公式 HP や信頼できるニュースサイトで確認できます。
脆弱性の具体的な内容や影響範囲、対策方法などを信頼できる情報元で確認することが重要です。

（２）迅速なアップデート

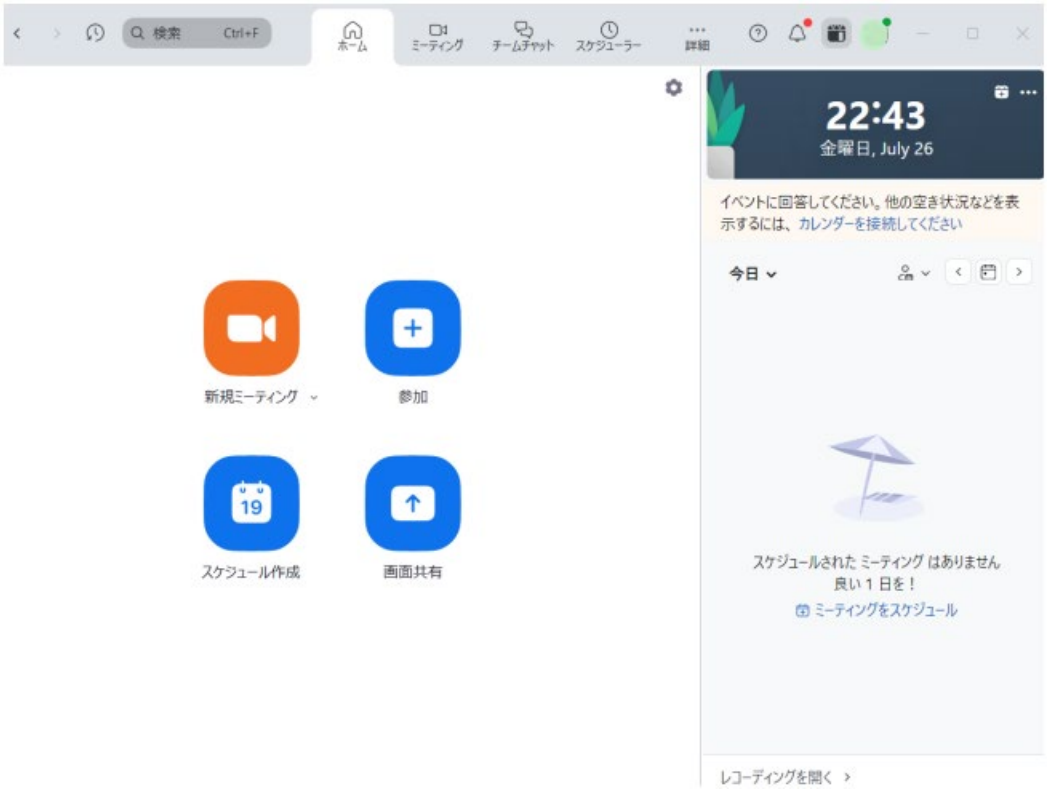
ソフトウェア会社が提供するセキュリティパッチを速やかに適用(アップデート)します。これにより脆弱性を修正し、攻撃のリスクを低減することができます。

４．Zoom のアップデート

Windows は標準的な利用環境では、最新の更新プログラムがないか定期的にチェックを行い、自動的に最新のものにアップデートされます。
しかし、Zoom の場合は、自動アップデートが行われません。
このため、利用者自身が定期的にアップデートを行う必要があります。
以下に、Zoom の具体的なアップデート方法を説明します。

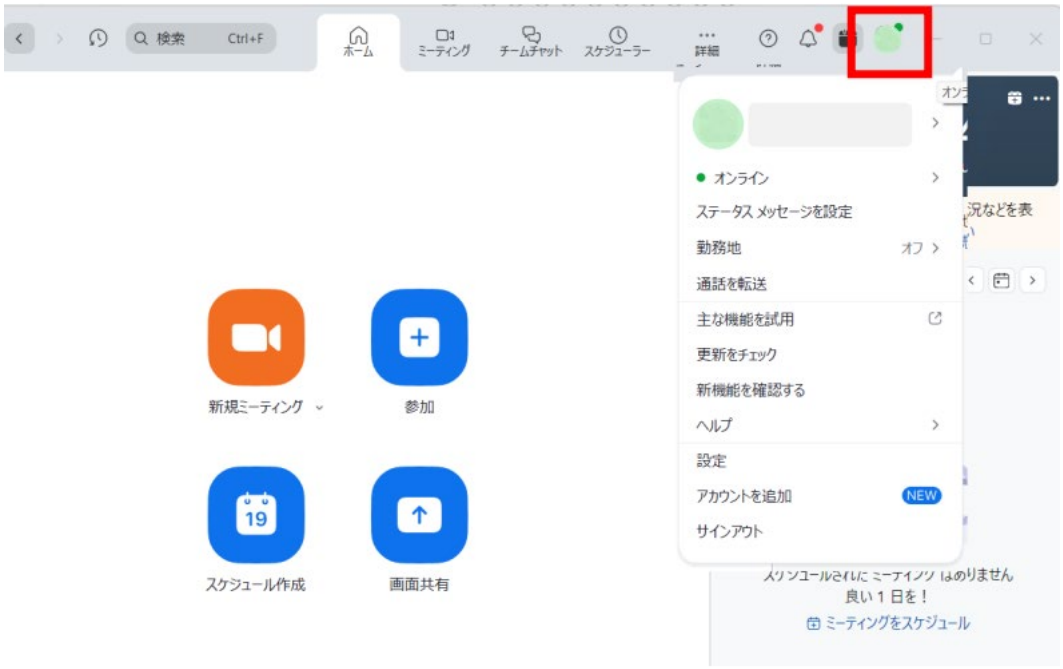
（１）Zoom アプリを開く

まず、使用中の PC で Zoom アプリケーションを開きます。



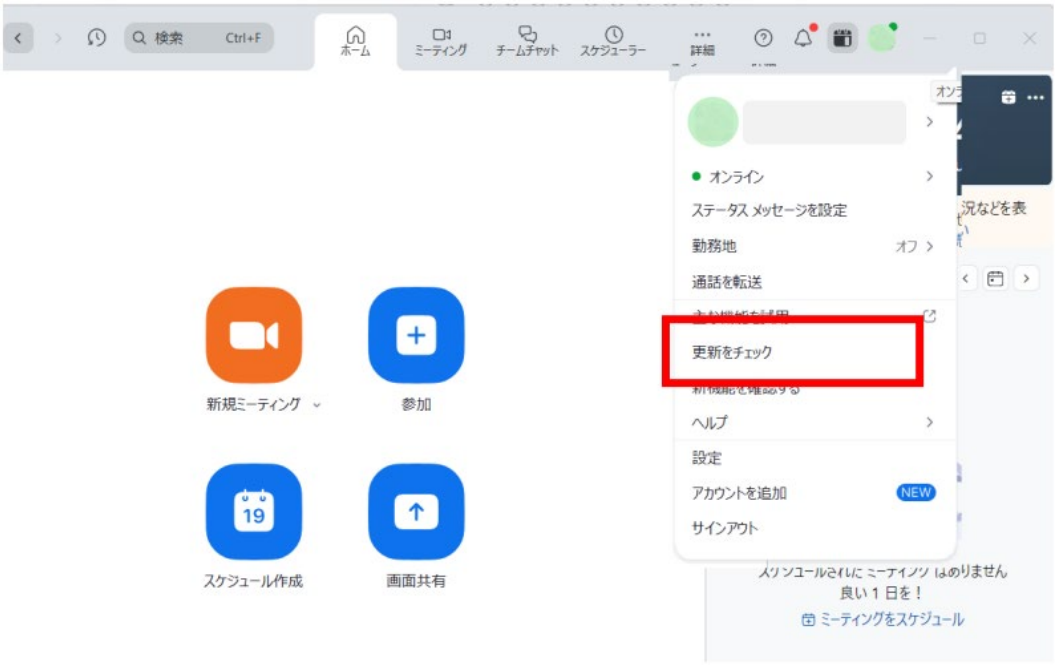
（２）プロフィールアイコンをクリック

画面右上にあるプロフィールアイコンをクリックします。このアイコンは、あなたの名前やプロフィール画像が表示されている部分です。



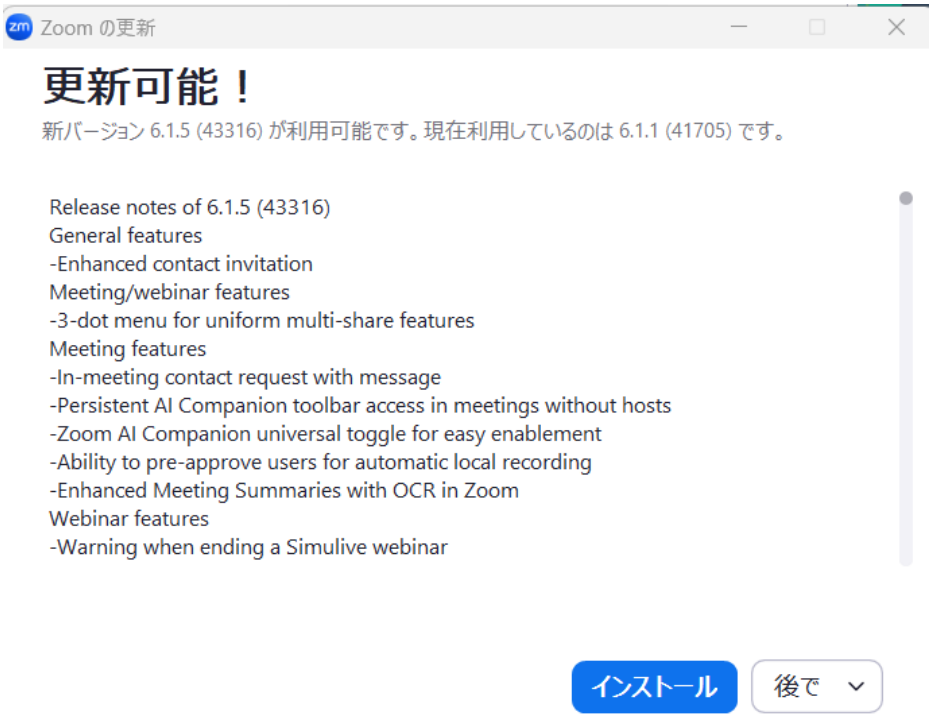
（３）アップデートを確認

ドロップダウンメニューから「更新をチェック」を選択します。このオプションを選ぶと、Zoom は自動的に最新のバージョンをチェックし、利用可能なアップデートがある場合は通知します。



（４）更新プログラムの有無を自動でチェック

最新のバージョンをチェックし、利用可能なアップデートがある場合は通知します。



（５）アップデートを実行

新しいバージョンが利用可能な場合、画面の指示に従ってアップデートを実行します。これには、最新バージョンのファイルをダウンロードし、インストールするプロセスが含まれます。



詳細な手順については、以下のリンクをご参照ください。
https://support.zoom.com/hc/ja/article?id=zm_kb&sysparm_article=KB0060729

ソフトウェアは、Windows のように定期的に自動アップデートが行われるものと、Zoom のように利用者が自主的に操作してアップデートを行う必要があるものとに分かれます。

オンライン会議のツールは Zoom の他にも、Microsoft Teams や Google Meet、Slack、Chatwork などがあります。
自社の業務でどのようなソフトウェアを使っているのか・アップデートを手動で行う必要があるのかどうか、把握するようにしてください。

さらに、いずれも最新バージョンへのアップデートが随時実施されているか、日ごろから確認することをお勧めします。

そのためには、従業員への教育も非常に大切です。

脆弱性に関する情報を社内や関係者に共有し、適切な対処方法を教育します。従業員が脆弱性の存在やリスクを理解し、必要な対策を講じることができるようにしておくことが重要です。

一般向け 1_#9_迷惑メール
掲載日：2024/10/14



皆さんは毎日、どのくらいの数のメールを受信していますか？
メールはビジネスやプライベートにおいて欠かせないツールですが、その便利さの裏に潜む危険性を忘れてはなりません。
メール利用時の困りごとの 1 つに、迷惑メールがありますね。
今回は、迷惑メールの危険性とその対策について説明します。

迷惑メールは、単に煩わしいものだと思っていませんか。
実は企業の情報セキュリティに大きなリスクをもたらす存在です。
このリスクに対処するためには、具体的な事例を理解し、適切な対応策を講じることが不可欠です。

一般的に迷惑メールとは、受信者の意図に反して一方的に送られてくるメールのことを指し、スパムメールとも呼ばれます。

主なスパムメールには、
・受信者が希望していない宣伝広告メール
・コンピュータウイルスを含んだメール

・フィッシングメール
・標的型攻撃メール
・ビジネスメール詐欺
・なりすましメール
などがあります。

【参考情報】
日本では「特定電子メールの送信の適正化等に関する法律」と「特定商取引に関する法律」で、送信してはいけない広告宣伝メールの基準が定められています。メールを送信する立場になった際には下記に注意しましょう。
・広告、宣伝メールを送信することに対して同意した受信者以外に送信してはならない（オプトイン）
・広告、宣伝メールの受信拒否を通知した者に対して送信してはならない（オプトアウト）
・広告、宣伝メールには取扱業者の所在地などの連絡先を明示しなければならない
（「特定電子メールの送信の適正化等に関する法律」「特定商取引に関する法律」より）
参照資料：トレンドマイクロ　ウイルスバスタートピックス

最近の迷惑メールはますます巧妙化しています。
よくある迷惑メールの一例に、「フィッシング攻撃」が挙げられます。

「あなたのアカウントが不正に利用されています」という内容のメールが従業員に届きました。
このメールは、一見すると銀行や IT システム会社からの公式な通知のように見えますが、リンクをクリックすると偽の WEB サイトに誘導され、そこでログインすることが求められます。

ここで偽サイトであることに気づかず自身の ID とパスワードを入力してしまうと・・・偽サイトを作った犯人に、皆さんの ID やパスワードが盗まれてしまいます。

このようなメールは、日常的に不特定多数の人に送られており、攻撃者は企業の従業員を狙い、組織全体に大きな損害を与えることを目的としています。

また、「未払い請求書」という件名の添付ファイル付きメールも注意が必要です。
人の心理として、「未払い」と書かれたら、慌てて「あ、すぐに確認して払わなきゃ」と思いますね。
メールに添付されたファイルを開くことでウィルスなどの不正プログラムに感染することは皆さん聞いたことがあり、「怪しいメールの添付ファイルは開かない」と気を付けているはずです。
しかし、上記のように「未払い」などと書かれると、慌てて開いてしまうこともあり、攻撃者はその心理を突いてくるのです。

不正プログラムに感染すると、ネットワーク全体が感染し、社内で共有しているファイルやサーバなどにあるデータが暗号化されてしまいす。
これにより業務が停止し、さらには身代金を要求される事態に発展したケースもあります。

では、迷惑メールを受信した場合、どのように対応すればよいのでしょうか？
以下の対応を徹底することが推奨されています。

（１）開封しない、添付ファイルを開かない
迷惑メールは、最初から開かないことが最善です。メールをクリックしてプレビューするだけで、不正プログラムに感染することがあります。また、メールに添付されたファイルも開かないでください。
思い当たる内容でなければ、即削除を心がけましょう。

（２）リンクをクリックしない
メールに含まれるリンクをクリックすると、フィッシングサイトやマルウェアが仕込まれたページに誘導されるリスクがあります。
メール文中のリンクを不用意にクリックせず、公式サイトに直接アクセスして確認する習慣をつけましょう。

（３）スパム報告を徹底する
総務省では、「特定電子メールの送信の適正化等に関する法律」に違反していると思われるメールの情報収集・分析を行って、違反送信者への措置を行っています。



引用元：総務省　迷惑メール情報提供用プラグインダウンロードサイト

総務省のサイトには、受信した迷惑メールの情報を送ることができるツールが用意されています。
迷惑メールを受信した際には、「迷惑メール情報提供用プラグイン」を使用して、これを報告しましょう。

利用手順などは上の図の引用元リンクに記載されていますので、一読したうえでダウンロードしてご活用ください。迷惑メールを報告することで社会全体のセキュリティが向上します。しかし、これはあくまで報告用のツールです。迷惑メール対策ツールではないため、注意が必要です。

ここまでに解説したように、不審なメールは開かない・文中リンクはクリックしないなどの対策を日常的に実行することで、企業全体のセキュリティレベルを高め、従業員が不用意にリスクにさらされる可能性を大幅に減らすことができます。

迷惑メールは企業にとって脅威となる可能性がありますが、適切な対策を講じることで、そのリスクを大幅に低減することができます。

社員全員がセキュリティ意識を持ち、常に最新の対策を実行することが、企業全体の安全を守るために不可欠です。

「フィッシング攻撃」については、「フィッシングと SNS 乗っ取り」【3 分でわかる！用語解説＃ 7】、「ビジネスメール詐欺」については、「ビジネスメール詐欺とは？事例から対策を学ぶ」【基礎から学ぶ！セキュリティ＃ 5】で解説しています。まだご覧になっていない方はこちらの情報もご覧ください。

一般向け 1_#10_情報セキュリティ白書
掲載日：2024/10/28



今回は、独立行政法人情報処理推進機構（IPA）から 7 月 30 日に発行された「情報セキュリティ白書 2024」について紹介します。

「情報セキュリティ白書」は毎年発行されており、国内外で起きているサイバー攻撃や、それに対する対策がわかりやすくまとめられています。
この白書を読めば、どんなサイバー攻撃が流行しているのか、どうやって守ればいいのかを知ることができます。

主な対象者は企業のセキュリティ担当者や経営層、IT 部門の方々で、中小企業の経営者や、サイバーセキュリティに関心があるすべての方にとって有益な内容が盛り込まれています。
日常的にサイバーセキュリティに関わる方には、業務のガイドとして非常に役立つので、ぜひ読んでほしい資料です。
ただし、200 ページ以上もあるので、すべてを読み切ろうとするのは大変です。資料は販売されていますが、IPA の WEB サイトから PDF 版をダウンロードできるので、PDF 版で興味のある部分を読むだけでも十分有益な資料となっています。

「情報セキュリティ白書 2024」の役割

この白書を読むことで得られるメリットは、次のようなものがあります。

（１）最新の脅威と対策を把握

2024 年に注目すべきサイバーセキュリティのトレンドや脅威について、詳しく知ることができます。

（２）セキュリティ戦略の強化

白書に掲載されている具体的な事例や対策を参考にして、自社のセキュリティポリシーを見直すことができます。

（３）法令順守の確認
国内外のセキュリティ政策の最新情報を把握し、法令順守に役立てることができます。

（４）社内教育資料としての利用
従業員教育に使える実例や防御策が豊富に含まれており、社内研修の質を向上させることができます。

2024 年版の構成と内容

次に、2024 年版の構成と内容を、章ごとにご紹介します。

序章 2023 年度の情報セキュリティの概況

2023 年に発生した主なセキュリティインシデントや、国内外のセキュリティ政策の変化についてまとめています。
これを読むことで、昨年のセキュリティ動向を振り返り、今後の対策に役立てることができます。

第 1 章 情報セキュリティインシデント・脆弱性の現状と対策

ランサムウェアや標的型攻撃、ビジネスメール詐欺（BEC）など、2023 年に観測された主なサイバー攻撃の手口とその対策が詳しく解説されています。
具体的な事例を通じて、どのような対策を取るべきかがよくわかります。

第 2 章 情報セキュリティを支える基盤の動向

国内外のセキュリティ政策や標準化の動向について解説されています。

また、サイバーセキュリティリスクに対応するためのフレームワーク（CSF）の改訂が紹介されています。サプライチェーンの上流の企業が改訂された CSF を取り入れると、中小企業にも影響が及びます。
今後のセキュリティ施策を考えるうえで、最新の政策や標準化の動向を知っておくことは大切です。

第 3 章　情報セキュリティ対策強化や取り組みの動向

クラウドや IoT などの最新技術に対応したセキュリティ対策の動向がまとめられています。
新技術を導入する際に注意すべきポイントが示されており、組織のセキュリティ強化に役立つ情報が掲載されています。

第 4 章　注目のトピック

注目トピックとして、虚偽情報の拡散の脅威とその対策の動向、AI のセキュリティが紹介されています。
AI のセキュリティでは、「AI を悪用したセキュリティ脅威」と「AI　に対するセキュリティ脅威」について解説されています。
生成　AI　のリスクが高まる中、これらの最新情報を把握することで、組織としての対応力を高めることができます。

気になった章はあったでしょうか。
この白書を読めば、国外のサイバーセキュリティに関するトレンドや動向も知ることができます。
また、資料中にあるコラムはサイバーセキュリティに詳しくない人でも難しくなく、抵抗感なく読める内容になっているので、ぜひ下に記した IPA の WEB サイトから PDF 版の白書をダウンロードして、まずは気になったところから読んでみてください。

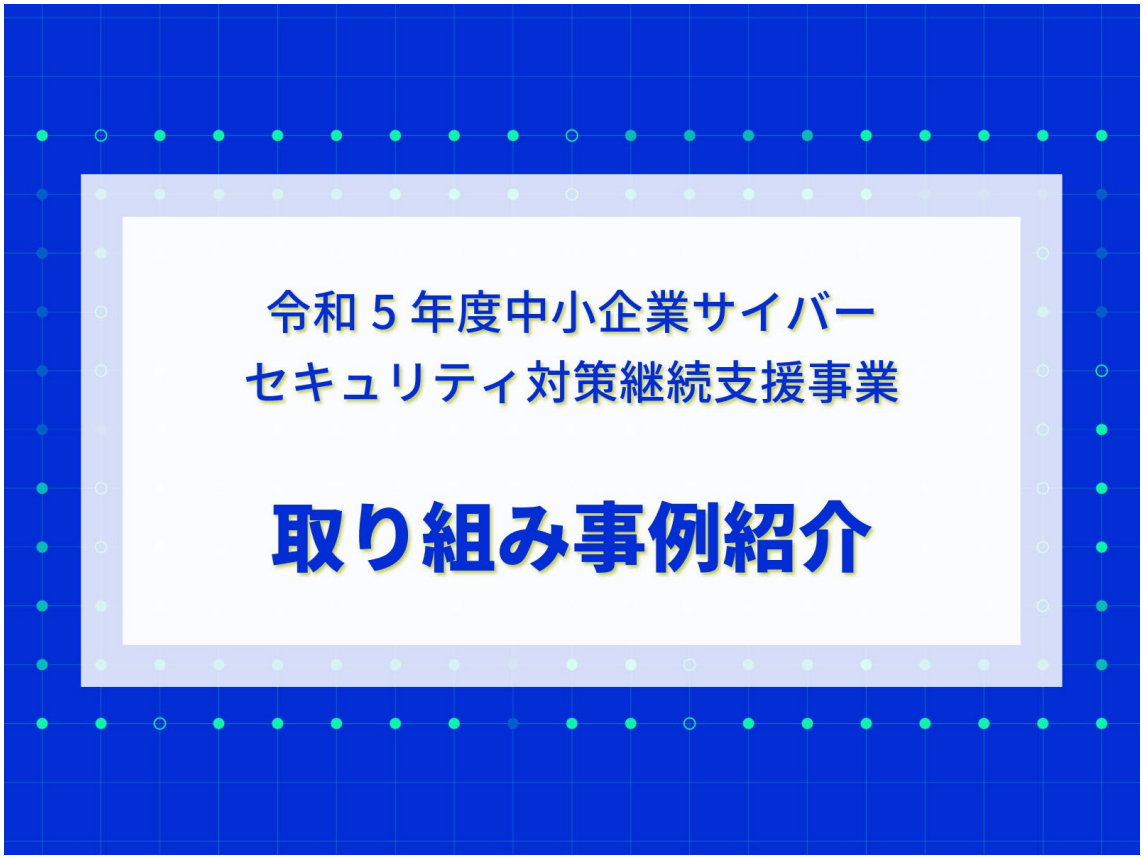
IPA　情報セキュリティ白書 2024 のサイト

https://www.ipa.go.jp/publish/wp-security/2024.html

情報セキュリティ白書は、企業が直面するサイバーリスクに対応するための重要なガイドです。
最新の動向を把握し、効果的なセキュリティ対策を講じることで、貴社の安全を確保してください。
この白書が、皆さんのセキュリティ強化にお役立ちできることを願っています。

一般向け 1_#11_セキュリティ対策取り組み事例の紹介　～令和 5 年度中小企業サイバーセキュリティ対策継続支援事業より～

掲載日：2024/11/11



はじめに

「セキュリティ対策を考えているものの、他社がどのように実施しているのかが気になる」
「自社に合った事例を参考にしたい」といったお悩みを抱えていませんか？
今回ご紹介するのは、東京都が提供するサイバーセキュリティ対策セミナーを受講して、セキュリティ対応を行なった企業の事例です。

東京都では、昨年、「令和 5 年度中小企業サイバーセキュリティ対策継続支援事業」として、多くの中小企業が抱えるセキュリティの課題解決をサポートしました。この事業のウェブサイトでは、実際に支援を受けた企業の具体的なセキュリティ対策事例が数多く掲載されています。今回はその事例の中からいくつかピックアップしてご紹介します。

事例を読めば、各企業が持つ課題に対して、セキュリティ対策をどのように実施したのかがよくわかります。
情報セキュリティ対策で必要な、**「自社の問題点の明確化と現状把握を行なったうえで具体的な対策を実施する」「従業員への意識啓蒙」「継続的な取り組み」**について参考になる事例ですので、是非ご覧ください。

事例１：印刷業

デザイン制作から印刷、製本・加工までのサービスを提供する印刷業社(従業員 20 名未満)
こちらの企業では、セキュリティ機器の導入や、自社に必要な対策の明確化が課題となっていました。
また、従業員のセキュリティ知識不足や、ログ取得・監視体制の整備が不十分なことが問題でした。その他、情報漏えい以外のインシデント対応手順も未策定でした。

そこで、以下の対策を実施しました。
（１）セキュリティ機器の見直しから着手し、ベンダーと協力して最適な 24 時間監視サービス付きの EDR※1 製品を導入。
（２）独立行政法人情報処理推進機構(IPA)の「5 分でできる！情報セキュリティ自社診断」を全従業員に実施し、従業員のセキュリティ知識向上を図る。
（３）担当者が習得した知識を基に、今後は定期的な情報発信や研修を実施。情報漏えい以外のインシデント対応の手順も整理。

こちらの企業では、現在も継続的なセキュリティ強化を検討されています。

※1：EDR とは、PC やスマホで不審な動作を検知し、未知のマルウェアにも対応し、脅威に対して即座に対処するシステムのことです。
「ＥＤＲ」【３分でわかる！用語解説＃２】の記事で詳しく解説しています。

事例２：金属製品製造業

通信基地局の建設部材の設計から、製造・施工を行う企業（従業員は約 100 名規模）
自社のセキュリティ対策を客観的に評価できておらず、従業員のセキュリティ意識のレベルがどの程度なのか分からない、PC のパスワード設定がなされていないことなどが問題でした。
さらに、セキュリティルールの不明確さや UTM※2 のログ管理も不十分でした。

そのため、以下の対策を行いました。
（１）セキュリティ状況を確認し、課題の洗い出し。
（２）PC の認証パスワード設定と、ウェブサイトのセキュリティ設定を確認。
（３）セキュリティ対策ガイドラインを社内に展開し、インシデント管理体制を整備。

こういった取り組みを実施したことにより、従業員のセキュリティリテラシーが向上し、セキュリティ対策への意識が高まりました。
今後も定期的な教育や EDR 導入を計画し、継続的なセキュリティ対策を行う予定です。

※2：UTM とは、ファイアウォールや侵入検知、ウイルス対策などを 1 台にまとめ、ネットワーク全体のトラフィックを監視・管理するシステムのことです。
「ＵＴＭ」【３分でわかる！用語解説＃３】の記事でも詳しく解説しています。

事例３：労務コンサルタント業

社会保険労務士法人と連携し、人事労務コンサルティングサービスを提供する企業（従業員は 50 名規模）
セキュリティ対策に関する従業員教育が不足しており、ネットワークセキュリティの管理体制の強化が必要でした。また、セキュリティ機器の運用がベンダー任せで、データのバックアップ運用も課題でした。

そこで、こちらの企業では以下の対策を行いました。
（１）ウェブサービスに関するパスワード管理体制を見直し、定期的な更新ルールを策定。
（２）UTM のネットワークログ管理体制の整備と、重要データのバックアップ運用の強化。
（３）リモートワークに対応するための VPN 利用に関するルールを策定し、運用を開始。

これらの取り組みにより、担当者のセキュリティ知識が向上し、取引先からの信頼向上につながりました。
今後も継続的に自社の業務に合わせたセキュリティ対策の強化を図り、取引先の監査や対応に備える体制を整えることを検討しています。

おわりに

今回ご紹介した事例からわかるように、企業ごとに抱えるセキュリティ課題は異なります。
自社の課題に近い他社の成功事例を参考にすることで、自社に合ったセキュリティ対策を効果的に進めることが可能になります。

冒頭でご紹介したウェブサイトには、ここで取り上げた事例以外にも、様々な業種や規模の企業が実施した事例が紹介されています。同じ悩みを抱えている企業の取り組みや解決方法は皆さんの役に立つのではないでしょうか。
こちらをご覧いただき、自社のセキュリティ対策の参考にしてください。

※この記事は、令和 5 年度中小企業サイバーセキュリティ対策継続支援事業*の情報に基づいて作成しています。

*昨年度の事業名は「サイバーセキュリティ対策継続支援事業」でした。今年度は「サイバーセキュリティ社内体制整備事業」として実施しています。

また、今年度の事業詳細は下記のサイトで確認していただけます。セミナーで使用した資料なども順次公開しているので、是非こちらもご覧ください。

令和 6 年度 中小企業サイバーセキュリティ社内体制整備事業

一般向け 1_#12_情報セキュリティセミナーのご紹介
掲載日：2024/11/25



サイバーセキュリティの重要性を実感しながらも、具体的な対策方法がわからないという悩みを抱えている方も多いのではないでしょうか。
そんな皆さんに、今回は、独立行政法人情報処理推進機構(IPA)が主催し、近隣で開催される無料の情報セキュリティセミナーを２つご紹介します。

どちらのセミナーも千葉県地域 SECUNITY 連絡会が IPA とともに主催していますが、東京都内の方も参加していただけます。

１． オンラインセミナー

１つ目は「かっこつけない、お金をかけないセキュリティ対策」と題し、中小企業の経営者や管理職を対象に、実践的な情報セキュリティ対策を紹介するものです。
オンライン開催ですので、職場や自宅から参加することができます。

【開催概要】
開催日時: 2025 年 1 月 28 日（火）13：30～15：30
配信方法：オンライン配信（13：00 から入室開始）
参加費　：　無料（事前申込みが必要）
定　員　：100 名程度
申込 URL：https://info.ipa.go.jp/form/pub/application/semi-reg
申込締切：2025 年 1 月 23 日（木）23：59

■セミナー詳細はこちら
https://www.ipa.go.jp/security/seminar/sme/t6hhco000000h903-att/20250128chiba.pdf

このセミナーでは、千葉県警察本部 生活安全部 サイバー犯罪対策課の情報セキュリティアドバイザーが、日本におけるサイバー犯罪や多発するランサムウェアへの感染、フィッシング詐欺等の現状に加え、これらの被害に遭わないために管理者としてなすべきことを説明します。
「ランサムウェア」の手口や感染事例、サイバー空間における犯罪者側の探索行為、フィッシング詐欺やサポート詐欺などの実態と危険性を学ぶことができます。

また、2 つ目の講演「費用をできるだけ抑えて、効果があがるサイバーセキュリティ対策のポイント」では、費用を極力抑えて自社にとって効果のある対策を選択するための手順を説明します。
当事業のメルマガ「基礎から学ぶ！　セキュリティ」で解説している内容と重なるところはありますが、30 分で概要を押さえることができる内容となっています。

そのほか、国の支援策（サイバーセキュリティお助け隊サービス、IT 導入補助金等）やセキュリティ対策の費用が軽減できる方法など、利用するとお得な情報も紹介されます。

２．対面ワークショップ（同内容で２回開催）

２つ目は、ワークショップ型の「セキュリティ・インシデント（事故）対応机上演習」です。

本事業のメールマガジンや第２回セミナーでご紹介した、セキュリティインシデント対応の**「検知・初動対応」**と**「報告・公表」**の一連の流れを、ランサムウェアに感染した想定で、演習を通して体感していただく内容になっています。

集合形式で実施されるので、他社の経営者や管理職との交流を通じた情報交換やベストプラクティスの共有も可能です。

このセミナーは、千葉県内で２回実施され、両日とも同一の内容での実施となりますので、ご都合の良い日程や会場をご検討ください。

【開催概要・1 回目】
開催日時： 2024 年 12 月 2 日（月）14：00～17：00（受付 13：30～）
会　場　：ペリエホール　RoomA（JR 千葉駅直結）
千葉県千葉市中央区中央１丁目１－１　ペリエ千葉７階
参加費　：無料(各社２名まで参加可能)
対象・定員：中小企業経営者層およびシステム責任者など定員 20 名。
情報セキュリティに関する知識レベルは問いません。
申込 URL：https://info.ipa.go.jp/form/pub/application/semi-reg
申込締切：2024 年 11 月 27 日（水）23：59
（※締切日が迫っているのでお急ぎください。）
【開催概要・2 回目】
開催日時: 2025 年 2 月 5 日（水）14：00～17：00（受付 13：30～）
会場：柏市民交流センター（パレット柏）　多目的スペース A
柏市柏１丁目７番 1-301 号　Dayone タワー３階
参加費: 無料(各社２名まで参加可能)
対象・定員：中小企業経営者層およびシステム責任者など定員 20 名。
情報セキュリティに関する知識レベルは問いません。
申込 URL：https://info.ipa.go.jp/form/pub/application/semi-reg
申込締切：2025 年 1 月 31 日（金）23：59

■ 1 回目の詳細はこちら

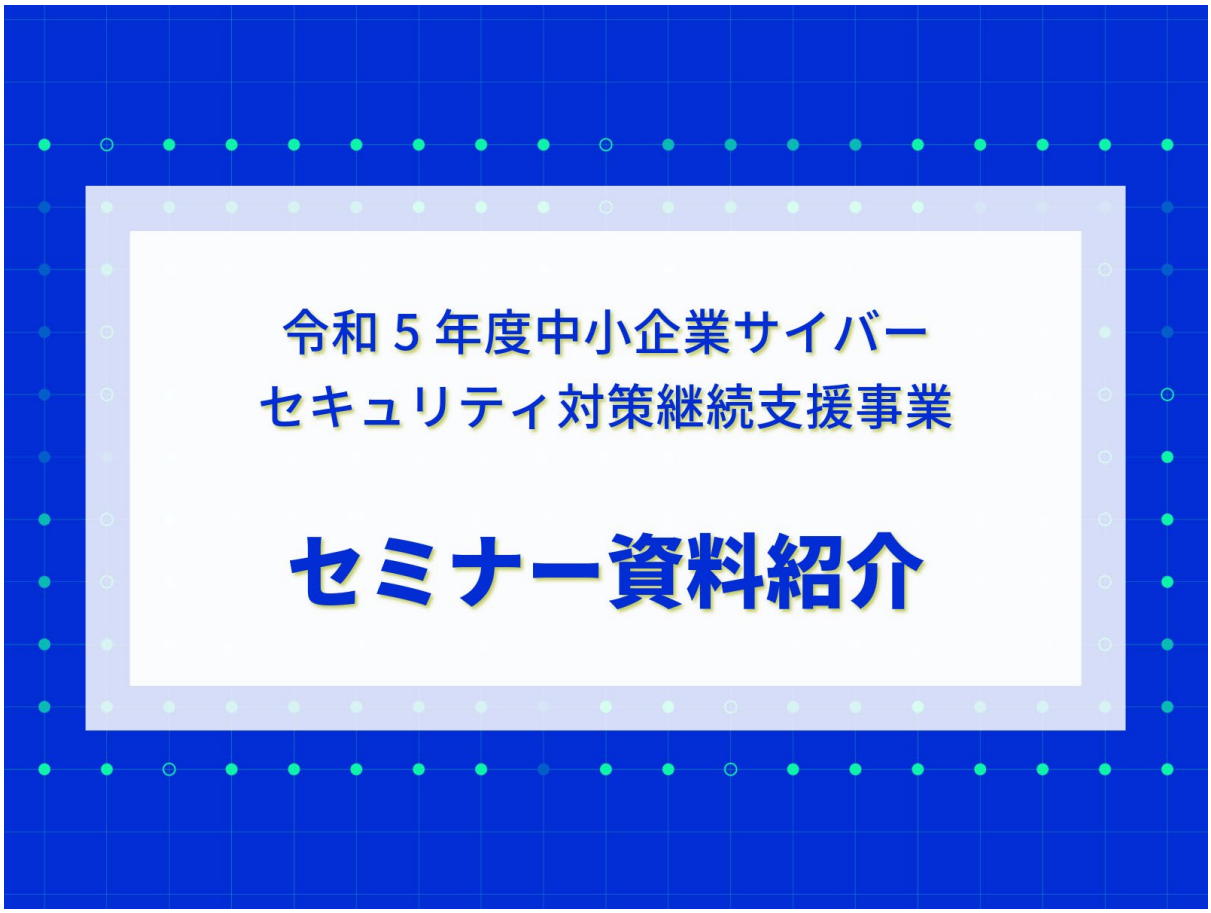
https://www.ipa.go.jp/security/seminar/sme/t6hhco000000h903-att/20241202chiba.pdf

■2 回目の詳細はこちら
https://www.ipa.go.jp/security/seminar/sme/t6hhco000000h903-att/20250205kashiwa.pdf
※セミナー内容は 1 回目、2 回目ともに同様です。

セキュリティ対策を効果的に実施するためには、経営者や管理職の方々が率先して情報セキュリティに関する意識を高め、自社のセキュリティ体制を強化することが重要です。
今回紹介した 2 つのセミナーは、その第一歩を踏み出すための絶好のチャンスです。
是非、こういった機会をご活用ください。

一般向け 1_#13_セキュリティ対策セミナー資料の紹介 ～令和 5 年度中小企業サイバーセキュリティ対策継続支援事業より～

掲載日：2024/12/9



「セキュリティリスクが増大している今、どこから手をつければ良いのかわからず困っている」、「最新のサイバー攻撃の傾向や、それに対する効果的な対策を具体的に検討したい」。

このようなお悩みを持つ中小企業の IT 担当者や経営者の方は少なくないでしょう。今回は東京都が実施したサイバーセキュリティ対策セミナーの資料を紹介します。このセミナーは、忙しいビジネス環境の中でどのようにセキュリティ対策を強化していくのか、具体的な指針を示すものです。

セミナー資料は、最新のセキュリティリスクと対策方法を詳細に説明しており、ウェブサイト上で閲覧することができるだけでなく、様々な形式でダウンロードが可能です。
PDF、PPT、EPUB などが用意されており、非常に利便性に優れています。

セミナー内容の概要

全 10 回にわたるセミナーの内容は、中小企業が取り組むべきセキュリティ対策について包括的に解説しています。各回 2 時間のセミナーテーマは以下のとおりです。

1 日目：サイバーセキュリティを取り巻く環境と求められる対策

情報セキュリティ白書や 10 大脅威、ランサムウェアやサプライチェーン攻撃の深刻さが紹介されています。
特に中小企業向けに推奨される「情報セキュリティ 5 か条」が、初めに実践すべき対策として取り上げられています。
続いてセキュリティ診断や基本方針の策定方法が示されています。

2 日目：企業経営における IT 活用とサイバーセキュリティ対策

IT 活用を通じた守りと攻めの投資について、企業経営との関連性が解説されています。
守りの IT 投資（業務効率化・コスト削減）と攻めの IT 投資（DX 推進）の違いや、実施手順および主要デジタル技術の選定方法の紹介とともに、経営者主導でのセキュリティ対策の重要性が説明されています。

3 日目：サイバーセキュリティに対する国の方針と脅威動向

政府のデジタル政策とサイバーセキュリティの重要性について解説されています。
コロナ禍を背景に、デジタルトランスフォーメーション（DX）が進む中で、デジタルリテラシー及びセキュリティ対策の重要性がますます高まっています。DX 推進が進められている中で、特にデジタルリテラシーとセキュリティ対策が不可欠であることが述べられています。
このセッションでは、企業の IT 活用と人材育成の重要性も説明されています。

4 日目：サイバーセキュリティ対策におけるフレームワークの体系

セキュリティ対策に役立つフレームワークの特徴や概要が解説されています。
企業が自社の課題に合ったフレームワークを選ぶ重要性が述べられ、ISMS や CSF、NIST SP 800、CPSF などが紹介されています。
特に ISMS は網羅性が高く、他のフレームワークとも共通する概念を持つため、基盤として推奨されています。

5 日目：組織に必要となるセキュリティポリシーの立案

セキュリティポリシーの構成やサイバーセキュリティ対策のアプローチ、ISMS の管理策、リスクマネジメントの用語について解説されています。
セキュリティポリシーの「基本方針」「対策基準」「実施手順」の概要が紹介され、クイック、ベースライン、網羅的アプローチが説明されています。

6 日目：リスクマネジメントの基本と対策

リスクマネジメントプロセスの各段階（リスク基準の確立、リスクアセスメント、リスク対応）について解説されています。
リスクマネジメントがセキュリティ対策に不可欠であり、適切な手法を用いてリスクを特定し、分析、対応することの重要性が述べられています。

7 日目：組織として実施すべき具体的な対策事項・手順

セキュリティ対策の手順が 3 つのアプローチ（クイック、ベースライン、網羅的）に分けて説明されています。
特に網羅的アプローチでは、ISMS を活用した PDCA サイクルを用いた継続的な改善の必要性について述べられています。

8 日目：組織的対策と人的対策

ISMS の管理策を参考に、対策基準と実施手順の策定方法について解説されています。
ISO/IEC 27002 の基準を参考にしながら、自社に合った基準を策定する重要性が述べられています。

9 日目：対策および状況の有効性評価手法

ISMS に基づく物理的・技術的管理策の対策基準と実施手順について解説されています。
物理的管理策の具体例や、技術的管理策としてゼロトラストやネットワーク制御が取り上げられ、内部・外部監査による有効性評価の重要性も説明されています。

10 日目：総括

全体の総括のため概要は省略します。

このセミナーでの学びは、中小企業のセキュリティ対策にとって重要なものばかりです。
これを機に、自社に相応しい対策を選定し、積極的に取り入れることでセキュリティ強化の一歩を踏み出しましょう。

セキュリティ対策は一朝一夕で完成するものではありません。
常に変化する脅威に対応するため、継続的な取り組みが求められます。それが将来的なリスク軽減につながります。
セミナー資料を折に触れて参考にし、セキュリティ対策を継続して見直すことでより安全なビジネス環境を構築していきましょう。

なお、今回ご紹介したセミナー資料は令和 5 年度の事業のものですが、大変参考になるものです。
今年度のセミナー資料も順次公開される予定です。こちらも是非ご参照ください。
令和 6 年度　中小企業サイバーセキュリティ社内体制整備事業

※この記事は、令和 5 年度中小企業サイバーセキュリティ対策継続支援事業*の情報に基づいて作成しています。

*昨年度の正式事業名は「サイバーセキュリティ対策継続支援事業」でした。今年度は「サイバーセキュリティ社内体制整備事業」として実施しています。

一般向け 1_#14_メールセキュリティ強化の必要性と対応策　～メールアドレスの不正利用事故を防ぐには～

掲載日：2024/12/16



メール普及とそのリスク

皆さんは、1 日に何通くらいメールを受け取っていますか？
現代社会におけるメールは、電話と並び重要な通信インフラとなっています。

皆さんが当たり前のように日々利用しているメール。しかし、メールにはセキュリティリスクが存在しており、これを悪用したインシデントも増加しています。

以前の記事で「迷惑メール」の危険性とその対策について解説していますので、こちらもご覧ください。
（「迷惑メール」：https://follow-up.metro.tokyo.lg.jp/topics/hottopic9/）

本記事では、最近の事例として兵庫県姫路市の神姫バス株式会社で発生したメールアドレス不正利用事件をもとに、メールの送信の仕組みやメールセキュリティの対策について解説します。

神姫バスの事例：インシデント発生の背景とその影響

皆さんは 2024 年 10 月 3 日に公表されたこちらのニュースをご存知ですか。

【注意喚起】第三者による弊社メールアドレスの不正利用およびメール送信について（神姫バス株式会社）
https://www.shinkibus.co.jp/sys/frames/view/2085

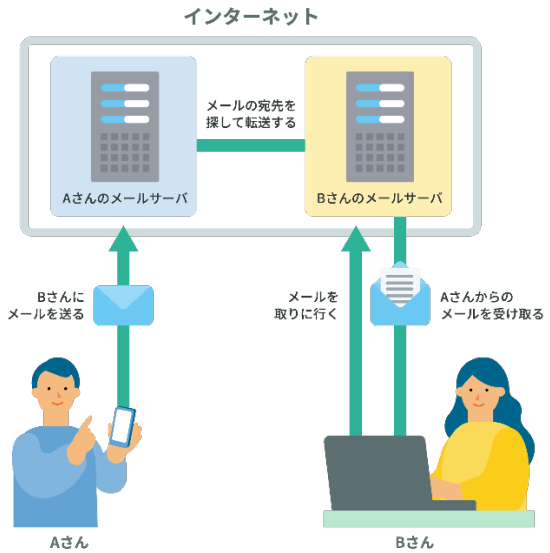
この事例は、会社のメールアドレスが第三者に不正に利用され、大量の迷惑メールが送信されるというものでした。
事件が発覚したのは、採用担当者が「自分が送信していないにもかかわらず、『送信不可』という通知が届いている」という報告を社内の情報システム課に行ったことがきっかけでした。
この通知は、迷惑メールが送信先に届かなかった際に返されるもので、担当者がすぐに異変を察知したことが早期対応につながりました。

会社ではその後、パスワードの再設定や調査が進められ、システムへの侵害や情報漏えいは確認されていないと報告されています。

しかし、このような事件が発生すること自体が企業にとって大きな信用失墜につながります。万が一このメールを介して受信者が不正プログラムに感染した場合、企業は法的責任を負わなければならない可能性もあります。

そもそも、なぜ会社のメールアドレスが第三者に不正利用されたのでしょうか。
それには、メールが送られる仕組みを理解することが必要です。

メール送信の仕組みとセキュリティ上の問題



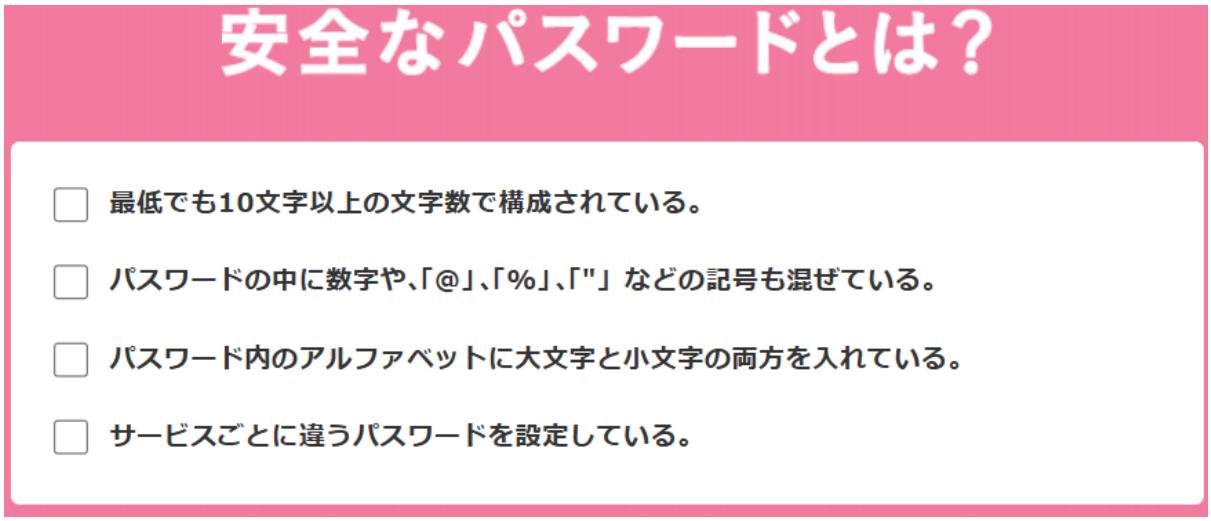
出典：国民のためのサイバーセキュリティサイト（総務省）
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/basic/service/04/

メールは、普段私たちが見えない部分で複雑な仕組みを経て送信されます。
初めに送信者がメールクライアント（Gmail や Outlook など）でメールを作成し、送信ボタンを押すと、メールは SMTP サーバ※（上図 A さんのメールサーバ）に送られ、そのサーバから受信者のメールサーバに届く仕組みです。
その後、受信者のデバイス上のメールクライアントにメールが配信されます。
※SMTP サーバ：Simple Mail Transfer Protocol（SMTP）と呼ばれる通信プロトコルを使用してメールを送信・転送するためのサーバ。SMTP はメール送信者がメールサーバに送信し、そのメッセージが受信者のメールサーバに届くまでの通信規約を指します。

ここで重要なのは、SMTP サーバでメールを送信する際パスワードが必要になるという点です。一般的には、送信者が利用しているメールクライアントにパスワードを登録します。
このパスワードが漏えいすると、第三者によるなりすましが可能となり、不正なメール送信が行われてしまうのです。

メールセキュリティ向上のための具体的対策

メールの仕組みを理解することは、なぜこうした事件が起こるのか、そしてどのように防げるのかを考える第一歩となります。
このような被害を防ぐためには、下図にあるように、安全なパスワードを SMTP サーバに設定する必要があります。



引用元： ちょこっとぷらすパスワード（独立行政法人情報処理推進機構（IPA））
https://www.ipa.go.jp/security/chocotto/

おわりに

メールは日常的に使用するツールですが、その背後には様々なリスクが潜んでいます。
今回の神姫バスの事例を通じて、メールセキュリティの重要性が再認識されました。

企業は、パスワード管理の強化や外部セキュリティ会社との連携を行い、万が一の際にも迅速に対応できる体制を整えることが必要です。
また、利用者自身も不審なメールに対するリテラシーを高め、セキュリティ意識を持ってメールを使用することが求められます。

サイバーセキュリティのリスクに対して常に油断することなく、継続的な対策を講じることが、企業の信頼と安全を守るためには不可欠です。

一般向け 1_#15_2024 年上半期のサイバー犯罪動向

掲載日：2025/1/6



昨今、サイバー犯罪が急増し、その手口もますます複雑化・高度化していることをご存知でしょうか？
これらの攻撃を受けた場合、企業の信頼を失墜させるだけでなく、経済的損失をもたらすため、企業にとって無視できない問題となります。企業がこうしたリスクに備えるためには、基本的な情報セキュリティの知識を持つことが非常に重要です。

今回は、2024 年上半期に報告されたサイバー犯罪の動向について解説します。

１．サイバー犯罪の主要な手口

2024 年上半期は、政府機関や大手企業を狙ったサイバー攻撃が多発しました。
特に、企業のデータや業務に直接影響を及ぼす「DDoS（ディードス）攻撃」や「ランサムウェア（身代金ウイルス）攻撃」が増え、深刻な被害が報告されています。

DDoS 攻撃は、大量のデータを送り込むことでネットワークを麻痺させ、システムを一時的に停止させる攻撃手法です。
自社のネットワークが不正アクセスされないよう、パスワードの強化やシステムを最新状況に保つことが重要です。

この対策により、情報が盗まれたり、業務が停止したりするリスクを大幅に減らすことができます。

ランサムウェア攻撃は、システムをロックしてしまう、あるいはデータを暗号化し、解決のための金銭を要求する手法が特徴です。
さらに、「二重恐喝型・データ公開脅迫型」という新たな手口も増加傾向にあります。この手法では、搾取した暗号化していないデータを公表すると脅し、身代金を要求します。
2024 年上半期におけるランサムウェアの被害報告件数は 114 件にのぼり、高水準を保っています。

ランサムウェアの詳細な解説は以下をご確認ください。
「セキュリティ 10 大脅威」のトップ　身代金を要求する「ランサムウェア」とその対策とは
https://follow-up.metro.tokyo.lg.jp/tip/business6/

そのほか、不正送金や SNS を使った詐欺、特に投資詐欺やロマンス詐欺が増加しています。
上半期に報告されたインターネットバンキングによる不正送金被害額は約 24 億円に達し、深刻な被害が広がっています。
特に、銀行口座のパスワードが脆弱であると不正アクセスの危険性が高まります。
安全性を確保するために、強固なパスワードを設定し、定期的に変更することを推奨します。
また、二段階認証機能なども積極的に利用し、不正アクセス防止を徹底しましょう。

今年は生成 AI を悪用した不正プログラム作成の事件も注目されました。
従来、生成 AI の悪用事例は詐欺や偽情報拡散が中心でしたが、2024 年 5 月には、生成 AI を利用してランサムウェアを作成した事件が報告されました。
この事件では、一般的な生成 AI サービスを使用して不正プログラムを作成しようとした容疑者が逮捕されています。

AI 技術は便利である反面、犯罪者にとっても強力なツールとなり得ます。生成 AI を利用することで、攻撃がより精密かつ効率的になってきています。
これに対抗するためには、AI を活用した防御手段も検討し、日々情報を収集して最新の手口を把握することが重要です。
また、生成 AI の利用にはセキュリティ対策とあわせ、利用する社員の教育も実施しましょう。AI とサイバー犯罪については、過去の記事でも詳細に解説していますので、是非ご覧ください。

AI とサイバーセキュリティ
https://follow-up.metro.tokyo.lg.jp/topics/01/

２．セキュリティ対策の必要性

最後に、セキュリティ対策は企業の経営課題でもあり、自ら対策を講じることが重要です。
専門的な技術を持たない企業の場合、外部のセキュリティ企業の力を活用することが効果的です。
例えば、サイバー攻撃対策の監視サービスを利用することや、定期的なセキュリティ診断を業者に依頼するのもひとつの手段です。
社内に IT 部門がある場合は、担当者とのコミュニケーションを強化し、必要な支援や予算確保を進めていきましょう。
小さな対策でも、セキュリティ事故を未然に防ぐために大きな役割を果たします。

サイバー犯罪の手口が年々高度化する中、企業側はセキュリティ対策を怠るわけにはいきません。
セキュリティ対策の向上のため、まずは自発的に基本的な対策を行い、可能であれば専門家の支援を受けることを検討してみてください。
長期的な視点でのセキュリティ計画を立て、安全なビジネス環境を構築していくことが重要です。
そのためには、日々のセキュリティ意識を高め、情報資産を守る取り組みを始めましょう。

なお、東京都では、中小企業の皆様に向けて様々な支援を行っています。
あまり情報を持ち合わせていないという方は、まずはこちらの動画をご覧ください。
・「知らないでは済まされない！　今すぐ始めるサイバーセキュリティ（アーカイブ）」
　https://follow-up.metro.tokyo.lg.jp/seminar/seminar0/

マルウェアとコンピュータウィルス、ランサムウェアの違いと関係性といった基礎知識から、どのようにしてサイバー攻撃が行われ、どのような対策が有効なのかを、具体的な事例を交えながら、クイズ形式で分かりやすく解説しています。サイバーセキュリティの基本から最新の脅威までを学べる動画ですので、社内教育用の最初のツールとしてもお勧めです。

参考資料
「令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について」（警察庁）
「警察庁「2024 年上半期サイバー犯罪レポート」で押さえておくべきポイントは？～ランサムウェアと脆弱性～」
（トレンドマイクロ株式会社）

一般向け 1_#16_フリーソフトと無料 Web サービスに潜むリスク
掲載日：2025/1/20



今回は、皆さまからいただいた「フリーソフトに潜むリスクや、利用時の注意点について教えてほしい」という質問にお答えします。

私たちの生活や仕事を支えるツールには、無料で利用できるソフトウェアや Web サービスが数多く存在します。これらはコストを抑えつつも、十分な機能を提供してくれるありがたい存在です。

しかし、**「無料」**という魅力の背後には、注意しなければならないリスクが潜んでいることをご存知でしょうか。今回の記事では、そのリスクを様々な視点から探り、安心して利用するための方法を考えてみたいと思います。

１． 無料サービスに潜むリスク

無料で提供されるソフトウェアや Web サービスの中には、ユーザーにとって重要な役割を担っているツールもあります。
たとえば無料サービスには、次のようなものがあげられます。

・無料で利用できるウイルス対策ソフト
・動画や写真など大容量のファイルを一時的に保存・共有できるファイル共有サービス

・ソフトウェアをインストールせずにブラウザで利用できる、オンライン画像編集ツール

これらのサービスは大変便利なものですが、「無料」の背後にはユーザーにとって予期せぬリスクが潜んでいることがあります。
運営者が無料で提供する理由の一つに、ユーザーのデータを活用して収益を得る仕組みが隠れていることがあり、この仕組みが場合によってはユーザーに不利益をもたらすことがあるのです。

２．フリーソフトをインストールする際のリスク

まず、パソコンにインストールして使用するフリーソフトに潜むリスクを見てみましょう。
フリーソフトには、次のようなリスクが存在します。

（１）悪意のあるソフトウェアやマルウェアのリスク

無料で提供されるフリーソフトには、意図しないプログラムが仕込まれている場合があります。ダウンロードし、インストールする過程で、不正なプログラムがこっそりと紛れ込み、ユーザーが気づかないうちにマルウェアや不正プログラムに感染する危険性があります。これらのプログラムによって、インストール後に自動的に個人情報などのデータが搾取されたり、パソコンが乗っ取られたりすることがあります。

（２）セキュリティ更新の遅延

最新の脅威に対応するためには、定期的なソフトウェアアップデートが必要不可欠です。
しかし、有料のソフトウェアに比べて、無料のソフトウェアはセキュリティ更新が遅れることがあり、最悪の場合、更新が全く行われないこともあります。

３．無料 Web サービスのリスク

次に、パソコンにソフトウェアをインストールしなくても使える無料 Web サービスに潜むリスクについて考えましょう。
これらのサービスの多くは、利用者の個人情報やデータを扱うため、以下のようなリスクがあります。

（１）個人情報やデータの漏えいのリスク

無料 Web サービスは、広告やユーザー情報を収益源とすることが一般的です。

このため、ユーザーの個人情報やデータ、利用履歴が悪用されるリスクがあります。
サービスを利用する前に、利用規約でどのようにデータが取り扱われるのかをしっかりと確認しておくことが重要です。

（２）サービス終了時のデータ消失のリスク

無料 Web サービスは、運営者の都合でサービスが突然終了する可能性があります。
サービス終了と共に、アップロードして保存していたデータが永久に失われるリスクがあるため、データのバックアップを取るなど、十分な注意が必要です。

４．安全に利用するための対策

どのようにすればこれらのリスクを回避しながら、フリーソフトや無料の Web サービスを活用できるのでしょうか。
以下のポイントに注意しましょう。

（１）インストール前のチェック

フリーソフトをインストールする前に、提供元やダウンロード先が信頼できるものか必ず確認しましょう。
公式サイトからダウンロードすることが基本です。
また、インストール時には、不要なオプションやツールバーが追加されないように確認することも大切です。
パソコンやスマホ内でどのような情報と連携するのかを確認することも忘れないようにしましょう。

（２）利用時のセキュリティ対策強化

無料サービスに限らず、Web サービスを利用する際は、強力なパスワードを設定し、二段階認証を有効にしましょう。しっかりとした対策を取ることで、不正アクセスを未然に防ぐことができます。
また、サービスのセキュリティ設定を十分に理解し、個人情報やデータの取り扱いについて確認しておくことも重要です。

（３）定期的なバックアップと代替サービスの検討

大切なデータは、定期的にバックアップを取りましょう。
また、万が一のサービス終了に備えて、あらかじめ代替サービスの検討をしておくと安心です。特に、重要なデータをクラウド上に保管する場合は、複数のサービスを利用してリスクを分散させることが大切です。

無料のソフトウェアや Web サービスは非常に便利ですが、その利用にはリスクが伴います。これらを安全に活用するためには、背後に潜むリスクを理解した上で、慎重に対応することが求められます。

無料で利用できるからこそ、リスクを十分に理解し、日々の生活の中で上手に活用していきましょう。

一般向け 1_#17_知らないうちに業務が止まる？新たなサイバー攻撃　～マイニングマルウェアの脅威～
掲載日：2025/1/27



近年、企業のシステムを狙う新しいタイプのサイバー攻撃「暗号資産マイニングマルウェア」が注目されています。

この攻撃は、従来の情報漏えいを目的とした攻撃とは異なり、企業のシステムリソースを不正利用して暗号資産（仮想通貨）の採掘（マイニング）を行うことを目的としています。表面上は被害が目立ちにくいものの、その影響は計り知れないものがあり、気づかないうちに企業活動に深刻なダメージを与える可能性があります。

2024 年 10 月、大手デリバリーサービス「出前館」が、このマイニングマルウェアに感染し、サービスが 3 日間停止する事態が発生しました。
この間、顧客の注文処理ができなくなり、売上が大幅に減少するなど、深刻な影響を受けました。
この被害を引き起こしたのは「RedTail」と呼ばれるマイニングマルウェアです。
今回は、この新種のサイバー攻撃「マイニングマルウェア」について解説いたします。

１．マイニングマルウェアとは？

マイニングマルウェアとは企業や個人のコンピュータをハッキングし、システムリソースを悪用して、暗号資産（仮想通貨）を作り出す不正プログラムです。暗号資産（仮想通貨）を作る作業を採掘（マイニング）と呼びます。このマルウェアは、感染させたコンピュータの計算能力を限界まで使用するため、サーバーやクラウドシステムが重くなり、正常な業務が行えなくなる可能性があります。攻撃者は性能の高い企業のサーバーやクラウドシステムを狙う傾向があります。

最近確認されている「RedTail」というマルウェアは、ルーターや VPN などの脆弱性を悪用して感染を拡大させる特徴があります。

２．企業が受ける影響

マイニングマルウェアは、他のサイバー攻撃（ランサムウェアや情報漏えいを狙った攻撃など）とは異なり、感染後行われる暗号資産のマイニング自体は直接的なデータ損失や情報漏えい、金銭的な請求行為を伴いません。

そのため、多くの企業はこの攻撃を軽視しやすい傾向にあります。
しかし、企業がマイニングマルウェアの攻撃を受けると、次のような問題が起こります。

（１）システムの動作が遅くなる

暗号資産のマイニングには大量の計算能力が必要となります。企業のサーバーやシステムがこれらに利用されることで、システムのパフォーマンスが著しく低下し、業務に時間がかかるようになります。最悪の場合、業務全体が停止する可能性もあります。

（２）予想外のコスト増加

クラウドサービスを利用する企業の場合、リソース（計算に使う能力）が大量に消費され、費用が急に高額になることがあります。

（３）事業停止のリスク

出前館の事例では、感染によりサーバーの負荷が急激に高まったため、一度サービスを停止しました。その後、当該サーバーからシステムを切り離してサービスを再開したものの、翌日には前日とは異なるサーバーが高負荷となり、再びサービスを停止する事態となりました。
このサービス停止は３日間続き、その間に売上の減少や顧客離れといったリスクが生じました。

（４）他社への攻撃の起点となる

攻撃者はより多くの利益を得ようとするため、感染させた企業や組織を踏み台としてさらに別の企業への攻撃に利用する場合があります。自社のシステムが他企業への攻撃に利用され、責任を問われる事態を引き起こす可能性もあります。

３．企業がとるべき対策

企業がマイニングマルウェアから自社を守るためには、攻撃者の進化する手口に対抗するための総合的なセキュリティ対策が必要です。

（１）脆弱性管理とシステムの防御

- **不要な通信ポートの閉鎖**
  インターネットにつながる通信ポート（通信口）は必要なものだけ開いて、それ以外の必要のない通信ポートを閉じ、外部からの不正アクセスを防ぐ。
- **ソフトウェアアップデート**

OS やアプリケーションを常に最新の状態に保ち、脆弱性を悪用されるリスクを削減する。

•定期的な機器の確認・整理

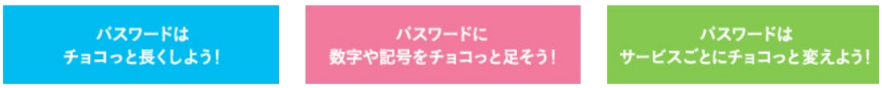
長期間使用していないルーターや機器が潜在的なリスク要因となる可能性があるため、定期的な棚卸しを実施し、不必要なものを排除する。

（２）アクセス管理の強化

•強固なパスワードポリシーを設定

他人に推測されにくい複雑なパスワードを使用する。

＜パスワード設定のポイント＞



詳細は下記サイトでご確認ください。

チョコっとプラスパスワード（IPA 独立行政法人 情報処理推進機構）

•多要素認証を導入

パスワードだけでなく、他の認証方法を追加して安全性を高める。

スマートフォンを使った認証や、指紋認証などの他の認証方法を追加することで、安全性がさらに向上します。

•アクセス権限を管理

業務上必要な最低限の人にだけにアクセス権限を付与する。

不要になった人のアクセス権限をすぐに削除する。

（３）監視体制を整備

•ネットワークのモニタリング

ネットワークを常に監視して、不審な通信や異常なトラフィックに注意を払い、マイニングマルウェアの兆候を見逃さない。

•監視ツール EDR や XDR※の導入

高度なセキュリティツールである EDR（Endpoint Detection and Response）や XDR（Extended Detection and Response）で、異常な通信やリソース消費の兆候を検知し、攻撃を早期に発見して対応する。

※ XDR(Extended Detection and Response)とは、EDR（詳細はこちらの記事「EDR」を参照）とは異なり、エンドポイント（パソコン、サーバー、スマートフォンなど）だけでなく、ネットワークやサーバー、メールなど複数の情報の関連性を分析して、サイバー攻撃の全体像を可視化して対処できるようにする仕組みです。

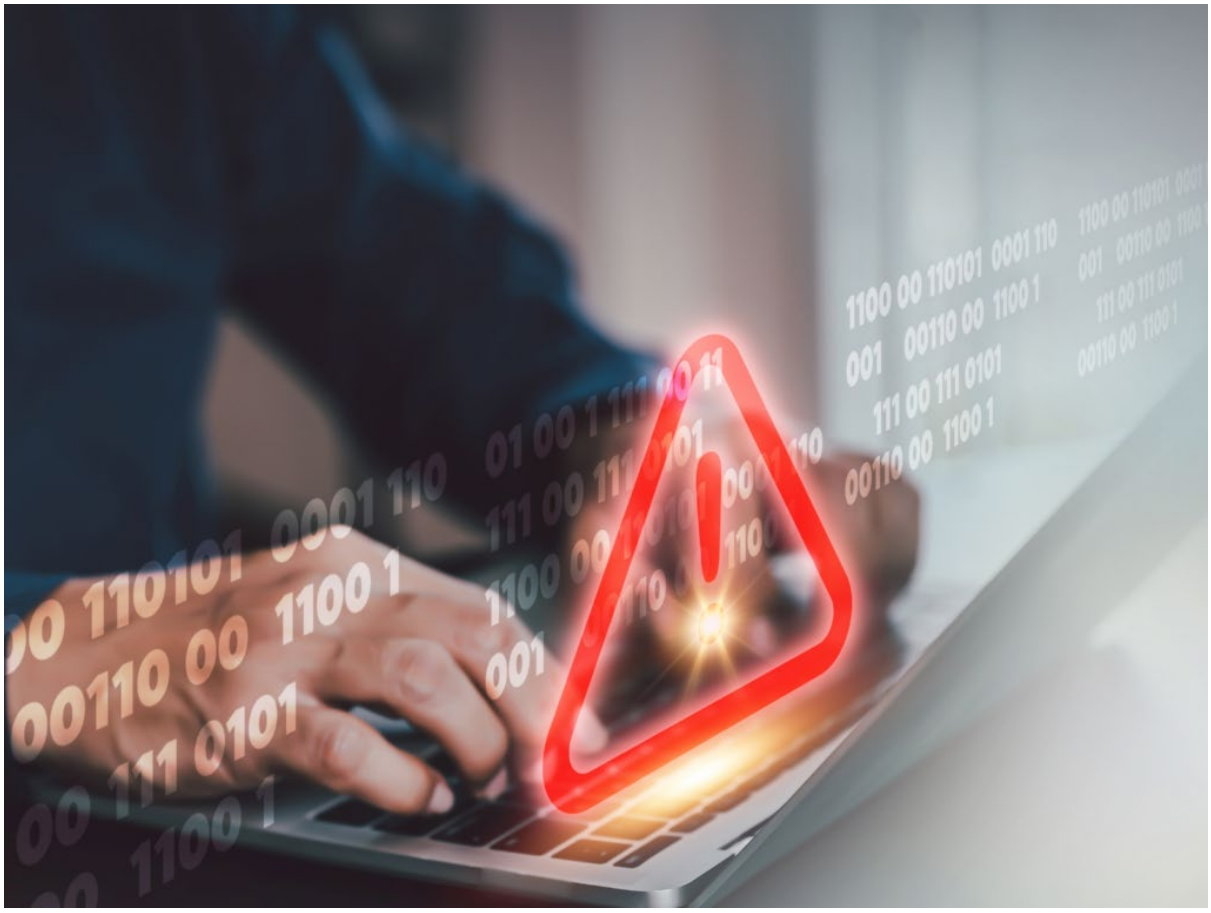
４．終わりに

マイニングマルウェアは、見えにくい被害で企業を蝕むサイバー攻撃の新たな形態です。

一度感染すると、事業継続を脅かす危険性があります。

「RedTail」のような進化型のマルウェアは今後も増加が予想されます。
サイバー攻撃は見えにくいですが、早めに対策をとることで大きな被害を防ぐことができます。企業の重要な資産であるシステムリソースを守るため、適切な対策を講じていきましょう。

一般向け 1_#18_会社の Web サイトに仕掛けられた「罠」にご用心！
掲載日：2025/2/3



今回は、会社のホームページ(以下、Web サイト)が危険な目に遭うかもしれない、という話を紹介します。

デジタル技術の進化により、最近では専門的な知識がなくても自社の Web サイトを作ることがとても容易になりました。便利なテンプレートや、不慣れな人でも直感的に操作できるツールが普及したことで、多くの中小企業でも低コストで Web サイトを持てるようになっています。

しかし、多くの企業が見落としがちなのが「管理や運用」の重要性です。
『Web サイトを作ったらそれで終わり』ではいけません。
管理が不十分な場合、どんなに素敵な Web サイトであってもサイバー攻撃者のターゲットとなり、時には悪意のあるプログラム（マルウェア）が仕込まれる可能性があるのです。最悪の場合、サイトを訪問した多くの人に迷惑をかけてしまうことが起こり得ます。

例えば、

・Web サイトを訪れた人のパソコンにこっそりとマルウェア(不正プログラム)が送り込まれ、ウイルスに感染する。
・個人情報や訪問者が閲覧していたサイトの情報が盗まれる。

などの被害が考えられます。

上記のような状況は、Web サイトを運営する企業にとって重大な危機です。
悪意をもった攻撃者は、皆さんの会社の Web サイトに「罠」を仕掛けることがあります。そして、訪問者は気づかないうちにその罠にかかってしまいます。これを「クロスサイトスクリプティング攻撃(XSS 攻撃)」と言います。

XSS 攻撃とはどのような攻撃か

XSS 攻撃とは、攻撃者が Web サイトに「不正なプログラム(罠)」を仕掛ける攻撃のことです。
攻撃者は、Web サイトの脆弱性を利用して悪意のあるコードをサイトに埋め込み、その Web ページを閲覧した不特定多数のサイト訪問者に不正プログラムを実行させます。Web サイトを訪れた人がその罠に引っかかると、個人情報が盗まれたり、パソコンがウイルスに感染したりする危険性があります。
また、罠はこっそりと仕掛けられるため、企業側が自社の Web サイトに罠が仕掛けられたことに気づくのが遅れがちです。

XSS 攻撃を受けるとどのような影響があるか

もし会社の Web サイトが XSS 攻撃を受けると、以下のような深刻な影響が生じる可能性があります。

（１）ブランドイメージの損傷

「あの会社の Web サイトを見ると、変なサイトに飛ばされて危険だ」「ウイルス感染の原因になった」などの噂が広がれば、企業の信頼性は一気に損なわれます。
その結果、顧客離れはもちろん、取引先からの取引停止などの可能性があります。

（２）顧客情報の漏えい

Web サイトに「お問い合わせ」ページを作っている会社も多いと思います。しかし、このお問い合わせフォームやクレジット決済ページを通じて集めたお客様の情報が、攻撃によって盗まれる恐れがあります。そうなった場合、顧客対応や法的責任など多大なコストが生じることとなります。

【XSS 攻撃の事例】
2024 年 10 月、タリーズコーヒーの公式サイトが 3 年間にわたり XSS 攻撃を受けていたことが報じられました。
同社の会員登録ページが XSS 攻撃の対象となり、攻撃者によって不正なプログラムが仕込まれた状態が続いていました。この攻撃は 3 年間発覚せず、長期間にわたり顧客の個人情報（氏名や住所、クレ

ジットカード番号など）が盗み取られていました。

XSS 攻撃は、不正プログラムが仕掛けられても企業側が気づかないことが多く、大企業であっても被害を受ける可能性が高いことを示しています。実際に、数年間にわたり情報が抜き取られていた事例が頻繁に起きています。

XSS 攻撃への対策

では、どのようにして XSS 攻撃から Web サイトを守ればいいのでしょうか。
企業側は適切な予防と継続的な管理が欠かせません。以下に推奨される対策をまとめました。

（１）セキュリティに配慮したサイト構築

Web サイトを構築する段階でセキュリティ対策を組み込むことが重要です。
例えば、独立行政法人情報処理推進機構（IPA）では、「安全なウェブサイトの作り方」という Web ページを公開しており、その中に、XSS 攻撃に遭いにくくする Web サイトの作り方という項目が掲載されています。
Web サイト構築を業者に依頼する場合、上記のページを見せて「ここに書かれている対策はやってほしい」と伝えることが有効です。あるいは、こうした情報を参考に具体的な対策や要望を伝え、安全な設計を目指しましょう。

（２）保守契約の締結

『Web サイトを作ったらそれで終わり』ではなく、作成後も、サイトを安全に保ち、常に最新のセキュリティ対策を行うことが重要です。そのためにも Web サイトを作成した業者と保守契約を結び、脅威に対応し続ける体制を整えましょう。

（３）ログ管理とアクセス監視

攻撃者は、Web サイトを自由自在に書き換えられるように、管理者になりすましてこっそり Web サイトにログインしようとします。
誰がいつ Web サイトの管理システムにログインしたのかを定期的にチェックし、不審な挙動を見逃さないことが大切です。
「この日にログインした記録があるけど、誰もログインしてないはずなのに…？」という時は、要注意です。

Web サイトは今や企業の顔であり、デジタル時代におけるビジネスの重要な資産です。
しかし、適切な管理や防御の仕組みがなければ、それは大きなリスクを内包する存在にもなり得ます。

XSS 攻撃は、あなたの Web サイトにとって深刻な脅威ですが、適切な対策を講じることで、そのリスクを大幅に軽減することができます。
セキュリティは一度設定して終わりではなく、継続的な努力が必要です。
この機会にセキュリティ対策を見直し、しっかりとした防御を築きましょう。

一般向け 1_#19_気づかぬうちに被害者に！？　ASM と脆弱性診断活用のすすめ

掲載日：2025/2/10



みなさん、インターネットを安全に使うために何をすべきか悩んだことはありませんか？

デジタル社会が進む中、インターネットは私たちの生活に欠かせない存在となっています。しかし、その一方でサイバー攻撃はますます身近な脅威になっています。

私たちの大切な個人情報や企業の資産を守るために、最近よく耳にする「ASM（アタックサーフェスマネジメント）」と「脆弱性診断」についてご紹介し、どのようにセキュリティを強化できるかをお伝えします。

最新動向とサイバーセキュリティの重要性

年末年始に、国内企業がサイバー攻撃のターゲットになったニュースをご覧になった方も多いと思います。

世界中で進化し続けるサイバー攻撃は、従来の防御法だけでは対抗しきれないほど複雑になっています。特に、注目すべき点は「アタックサーフェス」の拡大です。

アタックサーフェスとは、サイバー攻撃の対象となりうる IT 資産や攻撃点および攻撃経路を指し、攻撃対象領域とも呼ばれます。その範囲が広がると、それだけ攻撃されるリスクも増えてしまいます。

近年増加しているランサムウェアインシデントの多くは、インターネット上に公開された管理不十分なサーバやネットワーク機器からの侵入が主な原因となっています。
このような背景から、2023 年に経済産業省から、「ASM（Attack Surface Management）導入ガイダンス」が公表されました。

ASM（アタックサーフェスマネジメント）とは

ASM とは、企業や個人が持つデジタル資産、例えば Web サイトやサーバ、ネットワーク機器、クラウドサービスなどを特定し、どこに攻撃リスク（アタックサーフェス）が潜んでいるのかを明確にする方法です。
これらのデジタル資産は、ビジネスや日常生活でとても重要な役割を果たしています。しかし、もしこれらが適切に管理されていないと、サイバー攻撃の標的になってしまう恐れがあります。
ASM を活用することで、まだ気づいていないリスクを早めに見つけて対策を取ることができます。
具体的には、資産を自動で見つけ出し、リスクを評価して、どの対策を優先すべきか対策の優先順位付けを行います。また、常に監視することで最新の脅威にも備えられます。

ASM が必要な背景

近年のクラウド化やテレワークの普及、モバイルデバイスの利用拡大により、IT 環境が広がっています。また、働き方の変化により、シャドーIT（参考記事：「BYOD とシャドーIT」）と呼ばれる企業の管理外で使用される IT 資産が増えており、アタックサーフェスの拡大が進んでいます。

セキュリティチームが存在を把握できていない IT 資産は、セキュリティ対策が不十分なことも多く、サイバー攻撃のリスクが高くなっています。このような背景から ASM の必要性が高まっています。

脆弱性診断とは

脆弱性診断は、特定のシステムやアプリケーションに存在する問題や弱点を見つけ出し、その部分を修正するプロセスを指します。
例えば、Web サイトやネットワークにあるセキュリティホール（攻撃されやすい穴）を発見し、悪用されないように対策を講じます。

脆弱性診断は、主に以下の 5 つのステップで進みます。

1．調べる対象をはっきりさせる

2．スキャンツールという特別なソフトを使って問題を探す
3．見つかった問題を詳しく分析する
4．分析結果をもとに、どうやって直すかを報告する
5．報告に基づいて具体的な対策を行う

脆弱性診断には、自動スキャンによる広範囲な診断、専門家による手動診断など、様々な種類があります。

ASM と脆弱性診断の違い

どちらもサイバーセキュリティにとって大切な手法ですが、それぞれ目的が異なります。
ASM は、デジタル資産全体を把握して、どの部分にリスクがあるか明らかにすることが目的です。攻撃者がどのようにシステムに侵入しようとするかを見える化し、管理します。
対して、脆弱性診断は、特定のシステムやアプリケーションの弱点を見つけ出し、修正などの具体的な対策を施すことが目的です。攻撃者が悪用できるセキュリティホールを事前に発見し、対策を行います。

ASM と脆弱性診断のシナジー効果

ASM と脆弱性診断を組み合わせることで、企業のセキュリティ対策は一層強化されます。
ASM でデジタル資産を広く管理し、脆弱性診断によってその資産を詳しく調べることで、悪用されるリスクのある弱点（セキュリティホール）を最小限に抑えることができるのです。
新たに発見された資産に対しては、迅速に診断を行い、先手を打って対策を施すことが重要です。
さらに、定期的に脆弱性診断を実施することで、把握済みの資産のセキュリティ対策の継続的な改善を図ることができます。

具体的な対策の大切さ

セキュリティ対策は一度設定すれば終わりではなく、常に最新の状態を保つことが重要です。
サイバー攻撃は日々進化しており、過去に有効だった対策が今では通用しないこともあります。
そのため、企業や組織は常に最新の脅威情報を収集し、セキュリティ対策を更新し続ける必要があります。

また、技術的対策だけではなく、組織全体や周りの人たちのセキュリティ意識を高めることも大切です。
社員全員でセキュリティ教育やトレーニングを受け、全員がセキュリティリスクに敏感になるように促すことで、組織の防御力を向上させましょう。

一般向け 1_#20_あなたの企業の被害額は？サイバー攻撃の現実とその対策
掲載日：2025/2/17



昨今のニュースでしばしば耳にするサイバー攻撃の話題を見聞きして、「もし自分の会社が攻撃されたら、どれくらいの被害になるのだろう？」と考えたことはありませんか？

もしかすると、実際に企業が受ける被害額は想像以上に大きいかもしれません。
今回は、実際に起きた事例を通じて、サイバー攻撃がもたらす被害額について考察してみましょう。

日本企業のサイバー攻撃被害額

日本の企業でも、サイバー攻撃による大きな被害が出ています。
例えば、大手出版社である株式会社 KADOKAWA は、サイバー攻撃によって約 23 億円の損失を計上しました。この金額は、攻撃により被害を受けたシステムの修復や顧客対応のために必要な費用として使用されました。

また、スーパーマーケットを運営する株式会社イズミも約 10 億円の損失を計上しています。攻撃によるシステム停止期間の売上減少や、システム復旧のための高額な修復費用が主な内訳とされています。

さらに、建設コンサルタント企業の株式会社オリエンタルコンサルタンツホールディングスも、サイバー攻撃被害からの復旧に向けた調査や対応などのために約 7.5 億円の損失を受けました。
（参考記事：サイバー攻撃の被害額から考えるセキュリティ ｜ トレンドマイクロ（JP） ※2024 年 11 月 29 日更新記事より）

サイバー攻撃による金銭的損失には、以下の項目が含まれます。

- ・被害状況の調査費用
- ・システムの修復/修理費用
- ・顧客対応費用
- ・売上の減少
- ・売掛金の回収不能

これらの直接的な金銭の損失に加えて、企業の評判が大きく損なわれ、顧客からの信頼を失う可能性もあります。
特に顧客の個人情報が漏えいした場合、企業はそれに対する社会的責任を問われるだけでなく、長期的な信頼の損失に繋がりかねません。

こういった被害を未然に防ぐためには、企業はサイバー攻撃被害に遭った際の損害額を把握した上で、サイバーセキュリティ対策を強化する必要があります。

サイバー攻撃の見えないリスクを「見える化」する必要性

サイバー攻撃への対策を効果的に行うためには、まずリスクを明確にする「見える化」が欠かせません。
「見える化」とは、目に見えないものをデータや情報でわかりやすく可視化するプロセスです。これにより経営者は、どれくらいの資金をセキュリティ対策に投入すべきかを具体的に検討し、判断できるようになります。

「見える化」は、組織内のどの部分が脆弱で、どのようなリスクが存在するのかを詳細に把握するための手法です。
例えば、どのセキュリティソフトを使うべきか、従業員にどんな訓練が必要なのかを検討する際、具体的な数値データがあれば意思決定が容易になります。

また、「見える化」は社内外の関係者と情報を共有するのにも役立ちます。
全員が同じ情報を持つことで、セキュリティ対策の重要性が理解されやすくなり、組織全体で協力して対策を進めることが可能になります。

効果的なリスク管理ツールのご紹介：「NANBOK」

セキュリティコストを「見える化」するツールとして、独立行政法人情報処理推進機構（IPA）が提供する

「NANBOK」があります。
このツールは、サイバー攻撃が発生した場合の被害予測や、必要な対策を検討する上で非常に役立ちます。

「NANBOK」には以下のような機能があります。
・業界ごとのリスクに応じたシナリオ選択
企業は自社の業界に関連するシナリオを選択することができます。
・企業規模に応じた損害額の試算
自社の規模に応じた被害の予測を行うことができます。
・必要な対策費用の見積もり
セキュリティ対策にかかる費用を具体的に見積もることで、適切な予算立案に役立ちます。

「NANBOK」を活用することで、企業は自社のセキュリティ状況を詳細に分析し、適切な対策を講じることができます。
特に中小企業にとっては、限られた予算をどのように効果的に使用するかは重要な課題です。
このツールを使用すれば、費用対効果の高いセキュリティ対策が実現できます。

サイバーセキュリティの未来と企業が取るべき次のステップ

サイバー攻撃の脅威は日々進化し、これからも一層巧妙化していくと考えられます。
そのため、企業は常に新しい脅威に対応できる体制を整えていく必要があります。
まず、定期的なセキュリティリスクの評価を行い、最新の脅威に対して準備をすることが求められます。

また、従業員の教育や訓練も欠かせません。サイバー攻撃の多くは、人的ミスを狙っています。
したがって、従業員のセキュリティ意識を高め、適切な行動を取れるようにするための定期的な研修が重要です。

最後に、セキュリティ関連の最新情報を常に把握し、柔軟に対応できる体制を構築することが求められています。技術の進化により、新しい脅威が次々と現れるため、企業は常に最新の情報を収集し、適切な対策を行うことが必要です。

サイバーセキュリティは、企業の存続に直結する極めて重要な課題です。
適切な対策を講じることによって、サイバー攻撃から自らを守ることができます。
今すぐ行動を起こし、企業の未来を守るために必要なセキュリティ対策を講じていきましょう。

一般向け 2_#1_「3-2-1 ルール」
掲載日：2024/7/1



サイバーセキュリティの基本を理解するためには、いくつか重要なセキュリティ用語を知っておくことが必要です。これらの言葉や概念を正確に理解することで、企業が直面するリスクを最小限に抑え、適切な対策を講じることができます。本記事では、中小企業が特に知っておくべきセキュリティ用語について解説していきます。

今回のテーマは、データを守るために大切な「3-2-1 ルール」です。

「3-2-1 ルール」とは

「3-2-1 ルール」は、データのバックアップを取る際に推奨されている方法の一つです。このルールは、常に**３つのデータコピーを作成**して、それを**２つの異なるメディアで保存**し、**１つは別の場所に保管**することを指します。

例えば、企業の重要なデータをクラウドストレージと外付けハードドライブにバックアップするとともに、もう一つのバックアップコピーを別の物理的な場所に保管します。これにより、自然災害やランサムウェア（マルウェアの一種で後述にて説明あり）攻撃など、さまざまなリスクからデータを守ることができます。

万が一データが消失した場合でも、複数のバックアップから迅速にデータを復旧できるため、事業の中断を最小限に抑えることが可能です。このバックアップを取る対象は、電子データだけでなく紙の文書（契約書など）も含まれます。紙媒体による情報は、スキャナで読み取ってデータ化する、随時更新される情報は、Excel 等の電子データ化をして保管すると良いでしょう。

また、バックアップデータの定期的な更新も重要です。古いデータでは、最新の業務状況に適さないことがあるため、定期的にバックアップが正確に行われているか確認し、必要に応じて更新することが求められます。これにより、常に最新の状態でデータを保護し、緊急時にも確実に事業継続ができる体制を整えることができるのです。

サイバー攻撃に対する備えの一環として

日々の業務に欠かせない情報やデータは、企業活動を継続する上で欠かすことのできない大切な資産です。DX の本格化に伴い、規模や業種を問わずデータの重要性は高まっています。

また、その大切なデータを狙ったサイバー攻撃も増加し続けています。特に近年ニュースで取り上げられることが多い「ランサムウェア攻撃」は、攻撃者側が企業のネットワークに侵入しマルウェア(コンピューターやその利用者に被害をもたらすことを目的とした、悪意のあるソフトウェア)に感染させることで、データを暗号化して利用不可能な状態にし、そのデータを元に戻すことと引き換えに金銭（身代金）を要求してくる攻

撃手法です。

このランサムウェアには個人商店等の小規模事業者も被害に遭っており、どの企業がいつ被害に遭ってもおかしくありません。

データのバックアップが複数あれば、このような攻撃に遭った場合でも、迅速なデータ復旧が可能になります。特に中小企業にとっては、限られたリソースの中でのセキュリティ対策が求められます。

そのために、まずは基本の対策として大切なデータを保護する「3-2-1 ルール」を導入・実践することから始めることをお勧めします。

一般向け 2_#2_「EDR」

掲載日：2024/7/26



サイバーセキュリティの基本を理解するためには、いくつか重要なセキュリティ用語を知っておくことが必要です。

これらの言葉や概念を正確に理解することで、企業が直面するリスクを最小限に抑え、適切な対策を講じることができます。

本記事では、中小企業が特に知っておくべきセキュリティ用語について解説しています。

今回のテーマは、「EDR」です。

１．「EDR」とは

「EDR」は Endpoint Detection and Response の頭文字をとった言葉です。

「Endpoint(エンドポイント)」は、ネットワーク上の 1 台 1 台のパソコン、スマホ、タブレット、サーバーを総称する言葉です。

皆さんの会社では、複数台のパソコンやスマホ、タブレット、サーバーが無線あるいは有線でネットワークに接続されていますね。

これらすべてのことを表しています。

EDR は、それぞれのエンドポイント端末において不審な挙動がないか監視（Detection）し、検知した場合、サイバー攻撃への迅速な対応（Response）を支援するためのセキュリティソリューションのことです。具体的には、次の 3 つのサービスで構成されています。

- **監視ソフト**：エンドポイントにインストールする監視ソフト。ウイルスやマルウェアの活動、不審なファイル、外部との不適切な通信などを監視します。
- **制御サーバー**：監視ソフトを制御し、異常を検出した場合、監視者に通知します。エンドポイントからのアラートを受信し、適切な対応を行うためのサーバーまたはサービス提供事業者のクラウドサービスです。
- **サポートサービス**：監視者（多くはシステム担当者）に必要な情報を提供。EDR の運用や対応に関するサポートを行います。

２． EDR の機能

皆さんのパソコンがコンピュータウイルス(以下ウイルスと略します)に感染したとします。

本来ならウイルス対策ソフトが働いてウイルスを隔離・駆除といったことが行われますが、これまでに見つかっていないウイルスなどの場合には検知できずにすり抜けることがあります。

こういった場合に活躍するのが EDR です。

ウイルスに感染したパソコンでは、様々な意図しない処理が始まります。

- ウイルスが検知されないようにシステムの一部を書き換えます。

・　ほかのパソコンに自分のコピーを配布しようとします。

・　インターネットのサイトにアクセスして不正なソフトをダウンロードし、インストールしようとします。

・　パソコンにある情報を外部のサイトにアップロードする、などです。

EDR はこれらに対処するため、以下の動作をします。

1. 監視ソフトによるウイルス等によるパソコンファイルの変更、外部との不適切な通信などを検知し、制御サーバーへ通知
2. 制御サーバーによる監視者への通知、EDR として可能な範囲での異常事態への対応（例えば、該当パソコンの通信の遮断、ウイルスの除去など）
3. 監視ソフト、制御サーバーだけではできない状況の監視者・エンドポイント利用者への通知、契約によっては人手による復旧

同じようなことがインターネットを通じた不正侵入などの場合でも行われます。

３．EDR の導入に当たっての注意点

EDR だけを導入したからと言って、そのほかのセキュリティ対策が不要になるわけではありません。

ウイルス対策ソフト、ネットワーク監視のための仕組みなどについては必ず何らかの対策が必要です。

また、EDR はサービス事業者により提供される機能の範囲が異なります。

自社に適合する、EDR を選定する必要があります。

EDR から通知されたセキュリティの異常に対しては、導入した企業側での対応が原則です。

したがって、導入した企業側にも何らかの体制を準備することが必要です。

４．最後に

注意点で述べたように導入が難しい部分もあります。

ただ、現在のウイルス対策ソフトだけでは、侵入された後の対応が難しくなっているのも現状です。

内部に侵入されてしまった場合の迅速な対応による被害の拡大を防ぐための有効なソリューションとして EDR は注目されています。

最近は、AI を使ってランサムウェアを作ったとの事件も報道されています。

また、企業情報を狙うために特別なウイルスが作成されることもあります。

EDR は企業のセキュリティレベルを上げるための有効な一つの手段なのです。

参考資料

1. EDR とは｜機能や効果、従来のウイルス対策ソフト（EPP）との違い
   https://www.ntt.com/business/lp/edr.html
2. エンドポイントでの検知と対応（EDR）とは
   https://www.crowdstrike.jp/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/
3. EDR とは？　概要から主なセキュリティ機能、EPP やアンチウイルスとの違いをわかりやすく解説
   https://frontier.networld.co.jp/useful-security/edr-overview/

５．事業紹介

今回はEDRについて解説しました。
そのソフトウェアが無償で3か月程度体験できる機会を、東京都が提供しています。

事業名：中小企業サイバーセキュリティ基本対策事業

セキュリティ機器（UTM）またはソフトウェア（EDR）を無料で3か月程度体験していただけます。
東京都内の中小企業様対象です。

基本対策事業内容はこちら

一般向け 2_#3_「UTM」

掲載日：2024/8/2



サイバーセキュリティの基本を理解するためには、いくつか重要なセキュリティ用語を知っておくことが必要です。これらの言葉や概念を正確に理解することで、企業が直面するリスクを最小限に抑え、適切な対策を講じることができます。本記事では、中小企業が特に知っておくべきセキュリティ用語について解説します。

今回のテーマは、外部との通信を監視する「UTM」です。

前回の EDR に引き続き、情報産業にありがちな 3 文字略語となっていますが、ご容赦ください。

１．「UTM」とは

「UTM」は Unified Threat Management の頭文字をとった言葉です。

コンピュータウイルスや不正アクセスなどの脅威に対して、複数のセキュリティ機能を一つの機器に集約して運用することで包括的に保護するソリューションのことです。

日本語では「統合脅威管理」あるいは「統合型脅威管理」と呼ばれます。

２．UTM導入のメリット

1995 年 Windows95 発売以降急速にインターネットが普及しました。その後、徐々に増えてきたホームページ改ざん、ネットワークを通じた攻撃などの事案に対応するネットワーク防御の方法が構築・導入されてきました。

例えば、ネットワーク環境を社内と社外に分けて、相互の不正なアクセスを防止するファイアウォール、ネットワークを流れる信号を監視し、悪意のある活動や脅威を検出・防止する侵入検知/侵入防止システム（IDS/IPS）、社内から危険なウェブコンテンツへのアクセス等を制限するコンテンツフィルタリングシステムなどです。

この結果、発生したのが複数のネットワーク監視装置が連なるという事態です。導入するシステムの数分の管理・運用が必要でコストが膨らんできました。

これを解決するために開発されたのが、UTM です。一つの機器に複数のネットワークセキュリティを守る機能を搭載することにより、システムの機器数や運用コストを抑えることが可能となっています。

３．UTMに搭載されている機能

UTM は各社それぞれに開発しており、搭載されている機能は少しずつ異なっています。多くの UTM は以下の機能を搭載しています。

- ファイアウォール：ウイルスやマルウェア、フィッシング攻撃など外部からの悪意ある通信を遮断します。
- IPS/IDS：不正な通信や異常な通信があった場合に管理者へ通知、もしくは不正／異常な通信をブロックします。
- Web フィルタリング：社内ネットワークから外部の不正・有害なサイトへのアクセス制限をします。
- アンチウイルス：エンドポイント端末（※ネットワークに接続されたパソコンやタブレット、スマートフォンなどの機器）に侵入を試みるコンピュータウイルスを検知・除去する機能。
- アンチスパム：スパムメールを防止する機能。

４．UTM導入に当たっての注意点

UTM を選択する際には注意が必要です。提供会社ごとに機能は少しずつ異なります。例えば、テレワークを実現するための仮想プライベートネットワーク（VPN：インターネット上に専用ネットワーク実現するための暗号化通信技術）を提供する UTM も存在します。

各製品の特長と自社に必要な機能を比較し、自社にとって有効性の高いセキュリティを実現することが必要です。

また、最低限の運用・管理（ログの確認等）は必要です。自社で実施できる範囲か、もしくは UTM の提供会社よるサポートを受けた方が良いのか、相談しやすいサポート体制なのかどうかも確認すると良いでしょう。

５．最後に

中小企業にとって、最低限のネットワークセキュリティを担保する上で UTM は有効な手段です。すでに実施しているセキュリティ対策と適合する製品を選ぶことにより、皆さんの会社のセキュリティレベルを上げることが可能となります。

参考文献

1. UTM とは何かをわかりやすく解説　クラウド型のメリットも紹介
   https://www.ntt.com/business/services/network/internet-connect/ocn-business/bocn/knowledge/archive_07.html
2. 【2024 年】UTM のおすすめ 10 製品（全 17 製品）を徹底比較！満足度や機能での絞り込みも
   https://www.itreview.jp/categories/utm

６．事業紹介

今回はUTMについて解説しました。
そのソフトウェアが無償で3か月程度体験できる機会を、東京都が提供しています。

事業名：中小企業サイバーセキュリティ基本対策事業

セキュリティ機器（UTM）またはソフトウェア（EDR）を無料で3か月程度体験していただけます。
東京都内の中小企業様対象です。

基本対策事業内容はこちら

一般向け 2_#4_「VPN とゼロトラスト」

掲載日：2024/8/9



サイバーセキュリティの基本を理解するためには、いくつか重要なセキュリティ用語を知っておくことが必要です。

これらの言葉や概念を正確に理解することで、企業が直面するリスクを最小限に抑え、適切な対策を講じることができます。

本記事では、中小企業が特に知っておくべきセキュリティ用語について解説しています。

今回のテーマは、社内ネットワークに外部からアクセスを可能とする仕組みである「VPN」と「ゼロトラスト」に焦点を当ててみましょう。

VPNとは

VPN とは Virtual Private Network の頭文字をとった言葉です。その名の通り、仮想的なプライベートネットワークを構築する技術です。日本語では「仮想プライベートネットワーク」などと呼ばれます。

1990 年代前半までは、建屋を越えたコンピュータ間の通信は専用線と呼ばれる専用回線を使用していました。専用線は文字通り、企業ごとに専用の回線を持つことで、セキュリティが高く、安定した通信を実現していました。ただ、価格が高いことと、2 地点間の通信しかできないことが欠点となっていました。

この課題を解決したのが、VPN です。

VPN は、2 地点間の通信を暗号化することで、インターネット回線などの安価な通信網をあたかも専用線のように安全に利用できるようにする技術です。もともとは小規模拠点との安全な通信を確保するために使われていましたが、近年ではテレワークを導入する多くの企業で活用されています。

テレワークを行う際、最初に自分の PC を会社のネットワークにつなぐ操作が必要ですが、その際に使われるのが VPN です。

VPN は社内ネットワークとインターネットの両方に接続された VPN サーバによって実現しています。PC 上の専用接続用のソフトウェアを使って、PC と社内ネットワーク間で暗号化された通信が確立されます。利用者は、あたかも社内で作業しているかのように安全に通信できるようになります。

VPNの問題点とゼロトラスト

一方で VPN にはいつくかの課題があります。暗号化やテレワークによる接続 PC 数の増加による通信速度の低下、VPN サーバやクライアントコストの増加などが挙げられます。

しかし、最も重大な問題は、社内ネットワークに接続さえできれば、社内のすべてのシステムを利用できてしまうことです。

この問題を解決するために、ゼロトラストという考え方が生まれました。

ゼロトラストは、システムに接続する利用者や外部システムは信頼できないという前提のもと、接続を認証・検証します。また、接続後も必要な範囲に限ってアクセスを許可し、不審な動きがあった場合にはアクセス権を取り消します。

なお、近年広く使われているクラウドサービスを利用するシステムにおいても、同じゼロトラストの考えを適用し、正しい利用者が使っているかを認証・検証することが可能となります。

ただし、ゼロトラストを導入するためには、大きく 3 つの課題があります。

- 既存のシステムやネットワークの大幅な変更
- 利用者の利便性低下
- 継続的な監視と分析

これらの課題に対応するためには、クラウドベースのゼロトラストソリューションの活用や段階的な導入が有効です。

最後に

テレワークを進めるためには、VPN の導入が必要不可欠です。しかし、現状では VPN だけでは社内ネットワークを守り切れなくなっており、あわせてゼロトラストの導入も検討することでより安全な環境を実現できるようになります。

参考文献

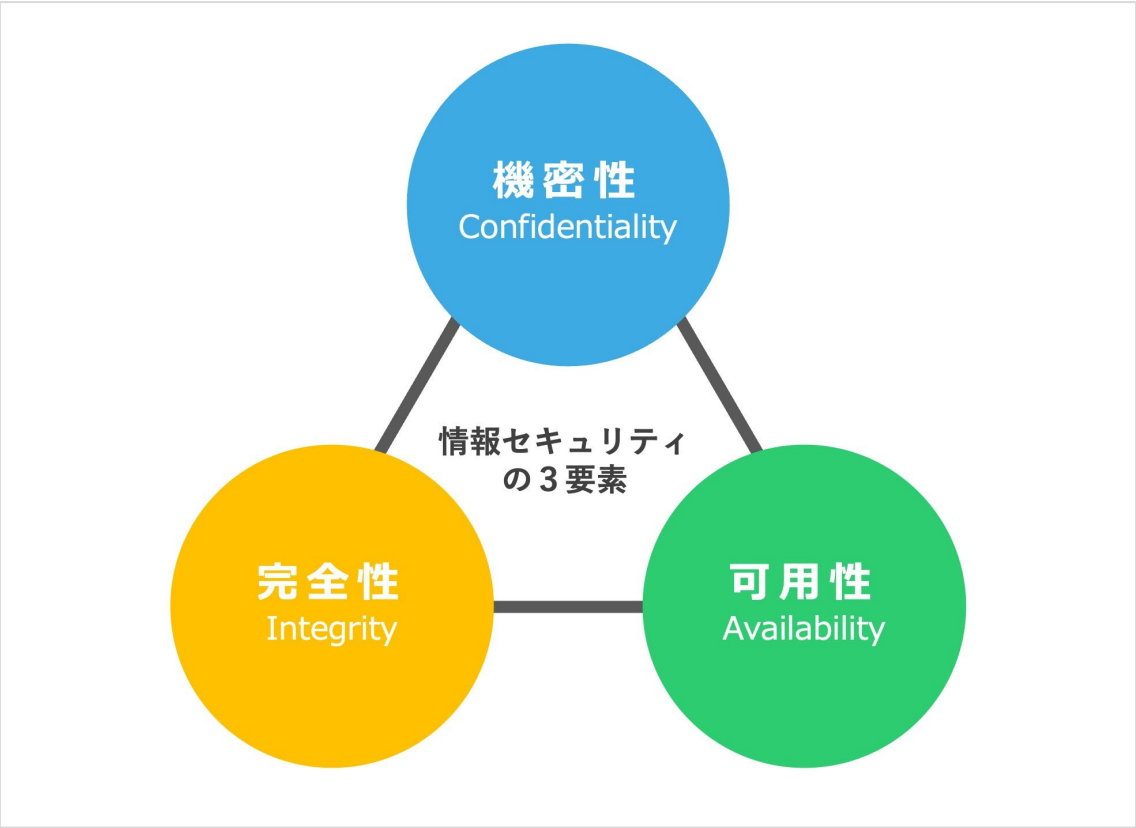
1. VPN とは何か、2024 年に必要なのか？[完全解説]
   https://ja.safetydetectives.com/blog/vpn とは何か/
2. 信頼していた VPN が悪用された場合に何が起きるのか

https://www.fujitsu.com/jp/solutions/business-technology/security/secure/column/202002-1/

3. ゼロトラストとは？基本的な概念から、定義・仕組みまで徹底解説
https://cybersecurity-jp.com/column/94300

一般向け 2_#5_「情報セキュリティ 3 要素（機密性、完全性、可用性）」

掲載日：2024/8/23



サイバーセキュリティの基本を理解するためには、いくつか重要なセキュリティ用語を知っておくことが必要です。これらの言葉や概念を正確に理解することで、企業が直面するリスクを最小限に抑え、適切な対策を講じることができます。本記事では、中小企業が特に知っておくべきセキュリティ用語について解説していきます。

今回のテーマは、システムの情報セキュリティを考える上で重要な 3 つの要素（機密性、完全性、可用性）です。

サイバーセキュリティもしくは情報セキュリティと聞いたときに、すぐに思い浮かぶのは「漏えい」あるいは「不正持ち出し」ではないでしょうか。そのようなことから、「うちの会社にはそんな重要な情報はないからサイバー

セキュリティは関係ないよ」という声を聞くことがあります。

しかしサイバーセキュリティには「漏えい」や「不正持ち出し」以外にも考えなければならないことがあります。今回はさまざまな脅威から組織の情報資産を守るための大切な３つの要素と、適切な対策方法を解説します。

情報セキュリティ

情報セキュリティとは、組織や個人の情報を守ることを意味します。

具体的には、企業活動に必要な情報資産に加えて、そのデータが保管されている媒体やシステムを守ったりすることです。

情報セキュリティマネジメントシステム（ISMS）における情報セキュリティの管理・リスク・制御に関するベストプラクティスがまとめられている JIS Q 27000:2019 では、情報セキュリティを「情報の機密性、完全性及び可用性を維持すること」と定義しています。

この「機密性」「完全性」「可用性」の３つを一般的に**情報セキュリティの 3 要素**と言います。また、「機密性(Confidentiality)」、「完全性(Integrity)」、「可用性(Availability)」の頭文字をあわせて「CIA」とも呼ばれます。

機密性(Confidentiality)

機密性は、アクセスを許可されたユーザだけが情報にアクセスできる状態にしておくことを指します。

独立行政法人情報処理推進機構（IPA）の「中小企業の情報セキュリティ対策ガイドライン 第3.1版」では、「アクセスを許可された者だけが情報にアクセスできる」と説明されています（※１）。「者」は人だけではなくシステムも含まれます。逆に言い換えると、許可されていない者には情報を使用させないということです。

一例として、皆さんの会社における個人の評価へのアクセス権を思い描いてください。対象者と上司、人

事部門しか閲覧できないように設定してあるはずです。異なる部門の人や同じ部門であっても、上司ではない同僚などのメンバーはアクセスできないことが「機密性」です。

機密性が保たれていない場合、個人情報や機密の漏えい・悪用により、信頼の喪失や法的な責任を負うリスクが生じます。このことから、機密性の確保は極めて重要とされています。

機密性はシステム的には「アクセス権限の設定」「パスワードの付与」「データの暗号化」などによって実現します。

※1「中小企業の情報セキュリティ対策ガイドライン 第 3.1 版」
P55「【表 12】情報資産の機密性・完全性・可用性に基づく重要度の定義 」より

完全性（Integrity）

完全性は、保有する情報が正確かつ完全な状態に保たれていることを指します。

「中小企業の情報セキュリティ対策ガイドライン 第 3.1 版」では、「情報や情報の処理方法が正確で完全であること」と説明されています。

システムにデータを要求したときに、「要求したすべてのデータが提供され、過不足がないこと」、「提供されたデータが最新であり、間違いがないこと」です。また、データが破損・改ざんされにくいことを示します。

完全性が低いと、正しいデータが提供されません。

完全性を高めるためには、少なくともアクセス履歴や変更履歴のバージョン管理とバックアップの確実な実施が必要です。

バージョン管理により、ファイル変更者や変更内容が確認できるようになります。また、バックアップがあれば、データの損失時や改ざん時に復元が可能になります。

可用性（Availability）

可用性は、いつでも情報を利用可能な状態にしておくことを指します。

「中小企業の情報セキュリティ対策ガイドライン 第3.1版」では、「許可された者が必要な時に情報資産

にアクセスできる」と説明されています。

可用性を低下させるものとして、「ハードウェアの故障」「サイバー攻撃」などがあります。

ハードウェアの故障に対して「ハードウェアを複数用意して、１つが故障してももう１つで運用できるようにする」、サイバー攻撃に対しては「オフラインバックアップ」などが有効な対策となります。

オフラインバックアップについては、【3 分でわかる！セキュリティ用語解説】「3-2-1 ルール」で解説しています。

3要素の維持はバランスが重要

情報セキュリティを高めるためには、これら 3 要素の 1 つのみを高めるのではなく、バランスよく高めることが必要です。

機密性をどんなに高めても、格納されている情報が正しくない（完全性が低い）と、その情報は使えないデータとなってしまいます。また、可用性が低ければ、情報の完全性が高くてもデータを利用できないため業務に影響が出ます。

このようにどれか一つの要素だけを高めてしまうと、業務の利便性や生産性が低下したり、情報漏えいのリスクが高まったりしてしまいます。

情報セキュリティには、「機密性」「完全性」「可用性」の３つの要素をバランスよく高め・維持することが重要です。

参考文献

1．JISQ27000:2019 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語 (kikakurui.com) の3.28（情報セキュリティ）
https://kikakurui.com/q/Q27000-2019-01.html
2．中小企業の情報セキュリティ対策ガイドライン 第3.1版-情報処理推進機構（IPA）

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf

一般向け 2_#6_「マルウェア・ランサムウェア」

掲載日：2024/9/6



サイバーセキュリティの基本を理解するためには、いくつか重要なセキュリティ用語を知っておくことが必要です。これらの言葉や概念を正確に理解することで、企業が直面するリスクを最小限に抑え、適切な対策を講じることができます。

本記事では、中小企業が特に知っておくべきセキュリティ用語について解説しています。

今回のテーマは、情報セキュリティの脅威である「マルウェア」と、マルウェアの中でも近年被害が増している「ランサムウェア」を解説します。

マルウェアとは

マルウェアは、英語の「malicious」（悪意のある）と「software」（ソフトウェア）の 2 つの単語を組み合わせた造語です。

これはパソコンやスマホなどのデバイスに対して、悪意を持って不利益をもたらすプログラムやソフトウェアの

総称となっています。

マルウェアの分類（NTTコミュニケーションズ ホームページから抜粋）

マルウェアに含まれる代表的なものは、以下の 4 つです。

1. **コンピュータウイルス**: プログラムの一部を書き換え、自己増殖します。ウイルスは他のプログラムを必要とし、感染したプログラムの一部を改ざんして増殖します。
2. **ワーム**: ウイルスと同じように自己複製して感染させていきます。ただし、ウイルスとは異なり、他のプログラムを必要とせず、単独で存在できます。
3. **トロイの木馬**: 一見問題のないファイルやアプリに偽装してデバイスに侵入し、外部からの指令によってデバイスを操るマルウェアです。
4. **スパイウェア**: 利用者の個人情報やアクセス履歴などを収集するマルウェアで、データ流出の原因となります。

マルウェアへの感染により、社内情報の抜き取り、ファイルの改ざん、PC・スマホのロック、外部との通信、サイバー攻撃の踏み台として使われるなどの被害が発生します。

マルウェアの感染経路と予防方法

マルウェアの感染経路はいくつかあります。感染経路を知り、適切な対策を取りましょう。

1. メールの添付ファイル
   不審なメール、添付ファイルは開かない
2. ネットワーク経由での侵入
   ウイルス対策ソフトを常に最新版にする
3. 不正サイトへのアクセス
   怪しい URL は開かない
4. 不正なソフト・アプリのインストール
   怪しいソフト・アプリはインストールしない

5. ソフトウェア脆弱性をついた侵入
   OS、ソフトウェアの最新版へのアップデート

さらに、サイバー攻撃にいち早く気づき対応するために EDR による監視を導入することも有効です。EDR については、【3 分でわかる！セキュリティ用語解説】「EDR」で解説しています。

ランサムウェア

マルウェアの中でも最近猛威を振るっているのが、ランサムウェアです。

ランサムウェアとは、「ransom（身代金）」と「software（ソフトウェア）」を組み合わせた造語です。

ランサムウェアは、マルウェアの一種です。感染すると、次の症状が引き起こされます。

- ＰＣ内のファイルの暗号化
- 操作画面のロック
- ユーザアカウント・パスワード変更
- 身代金の要求
- 機密情報の漏えい（窃取）

データが暗号化されることから、業務の中断が発生します。復旧するまでに 2・3 か月以上かかることもあり、その間業務が再開できないこともあります。

このため、実際にランサムウェア攻撃の被害を受けた組織では、攻撃者に対して身代金を支払ってしまうケースも一定数存在します[*1]。

*1 なぜ被害者は身代金を支払ってしまうのか？ランサムウェアの狡猾な脅迫手法

直近では、出版業界大手の KADOKAWA が大規模なサイバー攻撃を受け、ランサムウェアによって業務に大きな影響が出ている報道がなされています[*2]。

* 2 KADOKAWA がランサム攻撃で「ニコニコ」停止、身代金を支払うもデータ復旧できず

被害にあったとしても身代金を支払う行為は絶対にやめましょう。身代金を支払ったとしても、必ずしも暗号化の解除や窃取した情報の公開を中止するとは限りません。また、攻撃者に対して身代金を支払う企業だと、社会から認識されるリスクもあります。

ランサムウェアの対策方法は、セキュリティソフトの導入、OS・ソフトウェアのセキュリティ更新とパッチ適用、不審なメールを開かないなどマルウェアの対策方法と同じです。

異なる点は、感染後に備えた定期的なオフラインバックアップの取得だけです。オフラインバックアップについては、【3 分でわかる！セキュリティ用語解説】「3-2-1 ルール」で解説しています。

ランサムウェアにはいくつかの種類があり、中には特定の企業を狙ったものもあります。特定の企業として狙われた場合、感染を防ぐことは大変難しいのが現状です。

万が一ランサムウェアに感染してしまったら、次の手順で対処します。

1. 初動対応（ネットワークからの切断、証拠保全のため PC の電源を入れたままにする、感染していない PC からメールアドレス、パスワードを変更する）
2. ランサムウェアの種類を特定
3. 詳細な状況をセキュリティ担当者に報告
4. サイバーセキュリティ専門家・警察に相談
5. ランサムウェアの駆除・解除・復旧
6. データの復元について専門家に相談
7. 今後の感染予防策の策定

ランサムウェア被害からの復旧には、オフラインバックアップを取っておくことが重要となります。日頃のセキュリティ対策の中でぜひ心掛けてください。

参考文献

1. マルウェアとは？ウイルスとの違いは？ | NTT コミュニケーションズ

https://www.ntt.com/business/services/network/internet-connect/ocn-business/bocn/knowledge/archive_19.html

2. マルウェア「ランサムウェア」の脅威と対策（脅威編） | 警視庁
   https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/joho/ransomware_threat.html
3. マルウェア「ランサムウェア」の脅威と対策（対策編） | 警視庁
   https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/joho/ransomware_taisaku.html
4. 侵入型ランサムウェア攻撃を受けたら読む FAQ |JPCERT/CC
   https://www.jpcert.or.jp/magazine/security/ransom-faq.html

最後に

2024 年 7 月 17 日（水）に開催したトークショーでもマルウェアについて取り上げました。こちらのアーカイブ動画もあわせてご視聴ください。

URL：https://www.youtube.com/watch?v=99LnluHbb4Q（約 1 時間）

一般向け 2_#7_「フィッシングと SNS 乗っ取り」

掲載日：2024/9/20



サイバーセキュリティの基本を理解するためには、いくつか重要なセキュリティ用語を知っておくことが必要です。これらの言葉や概念を正確に理解することで、企業が直面するリスクを最小限に抑え、適切な対策を講じることができます。本メールマガジンでは、中小企業が特に知っておくべきセキュリティ用語について解説していきます。

今回のテーマは、「フィッシング」と「SNS 乗っ取り」です。

フィッシング

フィッシング(phishing)とは、正規のサービス事業者を装って利用者を騙して、個人情報や決済情報などの様々な情報を盗み取るサイバー攻撃です。魚釣り(fishing)の“f”を“ph”に置き換えた造語で、主に個人情報を盗み出すために行われるインターネット上の詐欺の一種です。

※参考情報：“f”を“ph”で置き換えている理由については複数の説があり、洗練された(so**ph**isticated)、1970 年代のアメリカにおける無慮電話をする電話ハッキング(phone **ph**reak)に加えて、パスワード収集釣り(**p**assword **h**arvesting f**ishing**)の略といったものがあります。

フィッシング攻撃は、実在する企業やサービス（例えば、銀行やクレジットカード会社など）を装ったメールやSMSを送り、攻撃者が用意した偽のウェブサイトに誘導するのが一般的な手法です。

誘導された偽のリンク先のWebページは、一見すると本物のページと見分けがつかないように作られています。このため、利用者は案内に従ってアカウントIDやパスワード、クレジットカード情報、銀行口座情報などの個人情報を入力してしまいます。そして、その入力された情報は攻撃者に送信される仕組みになっています。

攻撃者は、盗み取った情報を利用して、クレジットカードの不正利用、Web サービスなどへの不正アクセスを行います。また、盗み出した個人情報はダークサイト（違法または不正な活動を行うために設計されたウェブサイト）で売買されることもあります。

【フィッシングの事例】

警察庁ウェブサイトでは、フィッシングの注意喚起と対策方法を紹介しています。
そちらで紹介されている、フィッシングのよくある相談事例を一部抜粋して掲載します。
よくある相談（警察庁ウェブサイトより）

＜相談事例１＞
ネット口座を開設している銀行から「重要なお知らせ」という件名のメールが届いたので、記載されたＵＲＬにアクセスし、口座番号、暗証番号等を入力した。その後、知らない口座に対して、身に覚えのない多額の送金をされていることが分かった。

＜相談事例２＞
クレジットカード会社から「クレジットカード情報の確認」という件名のＳＭＳが届いたので、記載されたＵＲＬにアクセスし、カード情報を入力した。後日、クレジットカードの支払い明細を見ると、身に覚えのない支払いがあった。

SNS乗っ取り

フィッシングにより盗み出した情報を使って、様々な攻撃が行われます。その一つに「SNS 乗っ取り」があります。

SNS アカウントが乗っ取られることにより、次のような被害が発生します。

- 個人情報の悪用：架空請求・不正オンラインショッピング、個人情報のダークサイトでの販売、乗っ取ったアカウント ID によるフィッシング行為
- なりすまし：誹謗中傷の書き込み、不適切な投稿や発言による人間関係トラブル、信用被害の発生　など

最も深刻なのが、「乗っ取られた ID によるフィッシング」です。

普段信用している友達からのフィッシングとなるため、被害発生の確率が高くなります。また、乗っ取られてしまった上に自身の信用が大きく傷つくことにもなります。

被害に遭わないために

フィッシングのメール本文や誘導されるリンク先は、少し前までは一見しておかしいと感じられるものがほとんどでした。しかし、近年届いているフィッシングメールは非常に精巧になっており、まったく本物と区別ができないものも出てきています。

信頼できる企業や個人からのメールや SNS の投稿であっても、本文のリンクではなく、いつもの公式ウェブサイトやアプリ、ブックマークなどから該当のサイトにアクセスして確認してください。

個人情報を要求するメールやウェブサイトには、特に注意が必要です。

また、フィッシング対策協議会のホームページには、**「思い込んでいる時、急いでいる時、疲れている時に『ついうっかり』は起こりやすくなります。」**との記載があります。

疲れている時にフィッシングメールが来ると、いつものブックマークではなくメール内のリンクをクリックしてしまいがちです。

メール内のリンクのクリックは、必ずいったん立ち止まって、確認する習慣を身に着けてください。

フィッシングは、インターネットを利用する全ての人々が直面しているリスクです。

自身の情報を守るために、常に警戒心を持って対応してください。

フィッシング詐欺の被害に遭ってしまった場合の対策については、参考文献 2、3 を参考にしてください。

警視庁ウェブサイトでは、フィッシング被害に関する情報提供を求めています（警視庁ウェブサイト：フィッシング 110 番）。もし、フィッシング被害に遭ってしまったら、次の被害を減らすための情報提供にご協力ください。

参考文献

1. フィッシングとは ｜ フィッシング対策協議会
   https://www.antiphishing.jp/consumer/abt_phishing.html
2. 利用者向けフィッシング詐欺対策ガイドライン｜ フィッシング対策協議会
   https://www.antiphishing.jp/report/consumer_antiphishing_guideline_2024.pdf
3. フィッシング対策｜警察庁 Web サイト
   https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html

一般向け 2_#8_「不正アクセス」と「踏み台」

掲載日：2024/10/4



サイバーセキュリティの基本を理解するためには、いくつか重要なセキュリティ用語を知っておくことが必要です。これらの言葉や概念を正確に理解することで、企業が直面するリスクを最小限に抑え、適切な対策を講じることができます。本メールマガジンでは、中小企業が特に知っておくべきセキュリティ用語について解説しています。

今回のテーマは、「不正アクセス」と「踏み台」です。

不正アクセスとは

総務省の「国民のためのサイバーセキュリティサイト」では、不正アクセスについて「本来はアクセス権限を持たないものが、サーバや情報システムの内部へ侵入する行為」と説明しています。

簡単に言えば、**本来アクセスを許可されていない者が、他人の ID やパスワードを盗んで不正にログインし、サーバや情報システムの内部へ侵入してシステムを勝手に操作すること**です。

不正アクセスに使う他人の ID やパスワードは、「フィッシングと SNS 乗っ取り」【3 分でわかる用語解説 #7】で解説したフィッシング行為や、知り得た ID に対する総あたり攻撃などで悪意を持った第三者に盗まれています。

不正アクセスにより、機密情報・個人情報・重要ファイルの盗み出しや消去、不正なプログラムのインストール、システムの乗っ取りなどが行われ、近年多くの企業が、不正アクセスによる深刻な被害を受けています。

企業の機密情報が流出したり、サーバやシステムの停止・ホームページの改ざんなどです。

他にも発生する被害として、次のようなものも考えられます。

- 盗まれた個人情報による銀行口座、クレジットカードの不正利用による金銭的被害
- 取引先や機密情報の漏えいおよびシステム停止等による機会損失、信用失墜
- 自社サーバなどから他社攻撃が行われることによる、攻撃された企業からの復旧対応要求や損害賠償請求、取引停止等

不正アクセス禁止法とその影響

不正アクセスは単なる悪意ある行為に留まらず、法律としても厳しく禁止されています。

それが「不正アクセス禁止法」（不正アクセス行為の禁止等に関する法律）です。

不正アクセス禁止法では、不正アクセスそのものだけでなく、不正アクセスに関与するための他人の ID やパスワードの取得、提供、保管も違法としています。違反者には最大で 3 年以下の懲役または 100 万円以下の罰金が科される可能性があります。

この法律は企業に対するサイバー攻撃に限らず、個人の SNS アカウントへの不正ログインなども対象となります。

「あいつの ID とパスワードがわかったから、ちょっと覗いてやろう」「ネットにさらしておこう」も犯罪となります。

参考記事：不正アクセス禁止法をわかりやすく解説［組織が取るべき対策を紹介］（Securify Web サイト）

踏み台攻撃とは

踏み台攻撃とは、攻撃者が最初に、標的とは別の不正アクセスで侵入したサーバ等を乗っ取って、最終標的への攻撃に利用する手法です。この攻撃に使われたサーバ等を「踏み台」と呼びます。

踏み台を使うことで、攻撃者は自身の正体を隠しつつ、攻撃を行うことができます。また、恐ろしいことに、乗っ取られたサーバやコンピュータは、攻撃者に利用され攻撃に加担することになるため、不正アクセスを受けた被害者から加害者になってしまうのです。

この踏み台を使って大規模な攻撃が行われることがあります。DDoS（Distributed Deny of Service）攻撃と標的型攻撃です。

DDoS 攻撃は、攻撃者が複数のサーバ等を乗っ取ることから始まります。攻撃者は乗っ取ったサーバ等を使って、攻撃対象のサイトに一斉に大量のデータを送り、過負荷にして、対象サイトをシステムダウンさせます。最近では、家庭用のネットワーク機器（ルータなど）が乗っ取られて、攻撃に利用されたという事例もあります。

標的型攻撃は、攻撃者が乗っ取ったサーバや PC 等から関連のある企業（サプライチェーン上の企業など）にマルウェア付きのメールを送り、乗っ取りを図るものです。一見、「知人」からの「それらしいメール」となっているため、非常に防ぎにくい攻撃となっています。

中小企業における対策の重要性

攻撃者が最終的な標的とする大手企業のシステムへ侵入する踏み台として、中小企業が狙われることが多くあります。理由は、大手企業に比べセキュリティ対策が十分でないと考えられているからです。

そのような攻撃者から自社を守るため、中小企業も積極的に対策を講じる必要があります。不正アクセスへの対策は、これまでのセキュリティ対策と同じです。強固なパスワードを設定し、多重認証の導入が基本の対策になります。

また、最新のセキュリティ機器やソフトウェアを導入し、定期的なシステム更新とパッチ適用を行うこと（OSやソフトウェアの脆弱性を修正するために、ベンダーが配布する修正プログラムを適用すること）も重要です。

この時、特に注意すべきは、**ネットワーク機器などにも強固なパスワードを設定し、適宜パッチを適用すること**です。

常日頃の地道な基本的なセキュリティ対策が肝要です。このような取り組みが、企業の信頼性を高めることにつながります。

参考文献

1. 不正アクセスとは？ | 国民のためのサイバーセキュリティサイト (soumu.go.jp)
   https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/basic/risk/07/
2. 不正アクセス行為の禁止等に関する法律 | e-Gov 法令検索
   https://elaws.e-gov.go.jp/document?lawid=411AC0000000128

最後に

東京都では、セキュリティ機器（UTM）の３か月程度の無償体験や、企業のセキュリティ環境を調査し、今後の対策に向けて指導・助言する情報セキュリティマネジメント指導支援を行っています。それぞれ定員がございますので、詳しくはこちらをご覧の上、お早めにお申し込みください。

https://kihontaisaku.metro.tokyo.lg.jp/

一般向け 2_#9_「フリーWi-Fi」と「野良 Wi-Fi」
掲載日：2024/10/18



サイバーセキュリティの基本を理解するためには、いくつか重要なセキュリティ用語を知っておくことが必要です。これらの言葉や概念を正確に理解することで、企業が直面するリスクを最小限に抑え、適切な対策を講じることができます。本メールマガジンでは、中小企業が特に知っておくべきセキュリティ用語について解説していきます。

今回のテーマは、「フリーWi-Fi」と「野良 Wi-Fi」です。

Wi-Fiとは

そもそも Wi-Fi とはなんでしょうか。
無線 LAN＝Wi-Fi と認識されていることが多いのですが、厳密には少し異なります。無線 LAN ができた当初はその規格がバラバラだったため、規格を統一することを目的としてできたのが Wi-Fi です。このため、Wi-Fi は無線 LAN の規格のひとつです。
最近ではスマートフォンやタブレット・パソコン・家電などで Wi-Fi 利用が一般的になっており、Wi-Fi が無線 LAN の規格の主流となっています。

Wi-Fi にはいくつか種類があり、外出先で利用できるものとして「公衆 Wi-Fi（有料）」「フリーWi-Fi」「野良 Wi-Fi」と大きく３つに分けることができます。
中でも特に「フリーWi-Fi」と「野良 Wi-Fi」には危険が潜んでいるため、注意が必要です。

フリーWi-Fiとは

フリーWi-Fi とは、誰でも無料で自由に接続できる Wi-Fi を指します。飲食店や公共の場に設置されていることが多く、より多くの人が利用できるようになっています。
例えば携帯キャリア（ドコモ、au、ソフトバンク）、FREESPOT 協議会のように日本の複数の地域・施設で提供されているものや、交通機関、公共施設、商業施設(コンビニ、レストラン、ホテル)などの特定の地域・建物、チェーン店内だけで提供されているものがあります。
また、訪日外国人向けに用意されているフリーWi-Fi(FREE Wi-Fi PASSPORT、Japan Connected-free Wi-Fi、TRAVEL JAPAN Wi-Fi)もあります。
そのほか、東京や大阪では、自治体が主要な場所にフリーWi-Fi を設置しています。

【全国的に展開されているフリーWi-Fi】

提供元	フリーWi-Fi 名	SSID*	注意事項
FREESPOT 協議会	FREESPOT	‘freespot’ =SecurityPassword（AES）	接続後にポータルサイトでメール認証
NTT ドコモ	d Wi-Fi	「0001docomo」 「0000docomo」	d アカウントが必要
au	au Wi-Fi アクセス		スマートフォンのみ au ID と専用アプリが必要
ソフトバンク	ソフトバンク Wi-Fi	「0000softbank」 「0002softbank」	フラット型パケット定額サービス加入が必要

*SSID：Wi-Fi において、利用するネットワークを識別する名前。PC やスマートフォンにおいて Wi-Fi 接続しようとするときに「接続可能なネットワーク一覧」で表示される名前。

いずれのフリーWi-Fi も提供元がはっきりしており、無料で使え、携帯等の通信量に算定されないという観点からは「お得な」ものです。
しかし、誰でも使えるからこそ、セキュリティに注意する必要があります。

野良Wi-Fi

野良 Wi-Fi とは、主にパスワードも設定されていなくて、誰が何の目的で設置しているのか分からない正体不明の Wi-Fi の総称です。
野良 Wi-Fi には、「設定が面倒」「忘れた」といった理由で、特に悪意もなくパスワードをかけていないものもあります。
しかし、接続した人の個人情報を狙っている悪意を持った Wi-Fi もあります。
接続した携帯等の通信の盗聴、乗っ取りツールなどの送り込みにより、端末情報・個人情報を盗むものです。
そもそも、パスワードがかかっていないということは、通信が暗号化されておらず、ほかの人が無線を受信すれば、内容が理解できてしまうということです。
よく、テレビのドラマなどで警察無線を聞いているシーンが出てきます。それと同じ状態が、野良 Wi-Fi では起きていることになります。

「なりすましWi-Fi」と「悪魔の双子」

明らかな悪意を持った Wi-Fi として、「なりすまし Wi-Fi」と「悪魔の双子」があります。
「なりすまし Wi-Fi」は、本来の SSID に似た SSID のアクセスポイントを作ることにより、利用者に誤認させて、接続させることにより、端末情報・個人情報を盗むものです。
「悪魔の双子」は、対象のフリーWi-Fi と同じ SSID のアクセスポイントをつくることで、一部の利用者を誘導します。

例えば、dWi-Fi の SSID の一つは 0001docomo ですが、0001docomo**01** のようになっている SSID の Wi-Fi が「なりすまし Wi-Fi」です。
一方、0001docomo と全く同じ SSID でユーザを騙そうとするのが「悪魔の双子」と呼ばれるものです。

なりすまし Wi-Fi については、SSID に注意すれば避けることは可能です。
しかし、「悪魔の双子」については、区別できません。一度つないだことがある Wi-Fi には自動的に再接続される設定になっている端末は多く、「悪魔の双子」に遭遇した場合残念ながら悪意のある Wi-Fi に接続してしまうことになります。

フリーWi-Fiを安全に使うためには

フリーWi-Fi は非常に便利なサービスです。しかし、100%安全とは言えません。
できる限り安全に使うために、次のことを心掛けてください。

⑴ 野良 Wi-Fi に接続しない

野良 Wi-Fi にはなりすましや悪魔の双子など、悪意を持った Wi-Fi があります。接続してしまうとクレジットカード情報などが盗まれたり、マルウェアなどのウイルスに感染してしまう危険性があります。勝手に接続しないよう、Wi-Fi の自動接続を OFF にするか、使わないときは Wi-Fi 接続自体を切っておきましょう。

⑵ 接続するフリーWi-Fi を確認する

フリーWi-Fi に接続する前に、その場に掲載されているステッカー等でそのネットワークの提供元やサービス内容を確認します。その上で記載されている SSID を選んで手動で接続しましょう。

⑶ Wi-Fi で使われている暗号化方式をチェック

Wi-Fi に接続する際、SSID の横に表示される「鍵マーク」をチェックしましょう。
鍵マークがある場合、その Wi-Fi が暗号化によりセキュリティ対策を実施していることを意味します。
鍵マークのあるフリーWi-Fi を選ぶことで、安全性がある程度高まります。

⑷ ホームページにアクセスする場合は、「https」から始まるサイトだけ見る

「https://」から始まるサイトは、インターネットへの通信を暗号化します。この HTTPS 通信は、端末とサーバ間の通信を暗号化したプロトコルで行うことを指しており、通信内容が保護されているので、ホームページにアクセスする場合は「https://」から始まるサイトに限定しましょう。
一方「S」のない「http://」から始まるサイトは、通信が暗号化されていないため、通信内容を第三者に盗み見されてしまう可能性があります。
しかし、「https://」から始まるサイトであっても情報が盗まれる可能性はゼロではないので、フリーWi-Fi を使っているときはサイトへのログインは控える、個人情報などはできる限り入力しないようにしましょう。

⑸ 使っていて違和感がある、おかしいと感じた場合は通信を切断する。

これらのほかに、普段から安全な環境になるように PC やスマートフォンを設定しておくことも有効です。

個人向けの VPN*接続サービスの導入、メールソフトに暗号化通信を設定することなどは、通信の盗聴による個人情報の流出を防止します。
*VPN については「VPN とゼロトラスト」【3 分でわかる！用語解説＃4】の記事で解説しています。

また、自宅の Wi-Fi 環境をフリーWi-Fi にしないように暗号化キー（パスワード）を設定しましょう。暗号化キーを設定しないと勝手に接続されて、第三者に悪用される危険性があります。
自宅や会社で使用する無線 LAN ルーター利用時の注意点は「無線 LAN ルーターに潜む危険性」【ホットトピックス＃5】で確認することができます。

フリーWi-Fi を使うときには、事前の準備をしたうえで、前述の安全に使うための心掛けを守って使うようにしてください。

一般向け 2_#10_「多要素認証」と「パスキー」

掲載日：2024/11/1



サイバーセキュリティの基本を理解するためには、いくつか重要なセキュリティ用語を知っておくことが必要です。これらの言葉や概念を正確に理解することで、企業が直面するリスクを最小限に抑え、適切な対策を講じることができます。本記事では、中小企業が特に知っておくべきセキュリティ用語について解説しています。

近年、サイバーセキュリティへの重要性がますます高まっています。
増加するサイバー攻撃や不正アクセスへの対応として、従来の ID とパスワードだけによる認証では不十分と感じる方も多いでしょう。この ID とパスワードによる認証に代わり、さらに簡便さとセキュリティ強度を高める技術が、今回のテーマの「多要素認証」と「パスキー」です。

多要素認証（MFA）

「多要素認証」は、MFA（Multi-Factor Authentication）とも呼ばれる認証方法です。
セキュリティを強化するために、2 つ以上の異なる要素を同時に使用して、ユーザを認証する方法です。
ここでいう要素「要素」とは知識情報、所持情報、生体情報の 3 つです。

1.　知識情報（SYK：Something You Know）
自分だけが知っている情報。例えば、暗証番号、パスワード、PIN、秘密の質問とその答えなどが該当します。

2.　所持情報（SYH：Something You Have）
自分だけが持っているモノ。例えば、社員証、スマートフォン、キャッシュカード、PC などが該当します。

3.　生体情報（SYA：Something You Are）
自分自身。例えば、指紋、顔、静脈、虹彩などが該当します。

多要素認証では、これらの 3 つの要素の 2 つ以上を同時に使うことで、セキュリティを強化します。

皆さんがよく使われている実際の例として、銀行のキャッシュカード認証があります。
キャッシュカード自体は所持情報、入力する暗証番号は知識情報となります。
また、スマートフォンでは、端末の所有（所持情報）に加えて、PIN や指紋認証（知識情報、生体情報）を利用することが一般的です。

多要素認証導入のメリット

多要素認証の導入により、セキュリティを飛躍的に強化できます。
特にネット銀行では、ID・パスワードの入力後、登録したメールアドレスや電話番号にワンタイムパスコードを送信し、さらに確認を行う方式が一般的です。厳密にはこれを多段階認証と呼ぶことが多いですが、多要素認証の一種として捉えられることもあります。

パスキー

パスキーとは、パスワードを使わずにセキュリティと使いやすさを実現させた認証方式です。公開鍵暗号方式*[1]を使った FIDO2（Fast Identity Online 2）という FIDO アライアンス*[2]が定めた国際規格に基づいています。

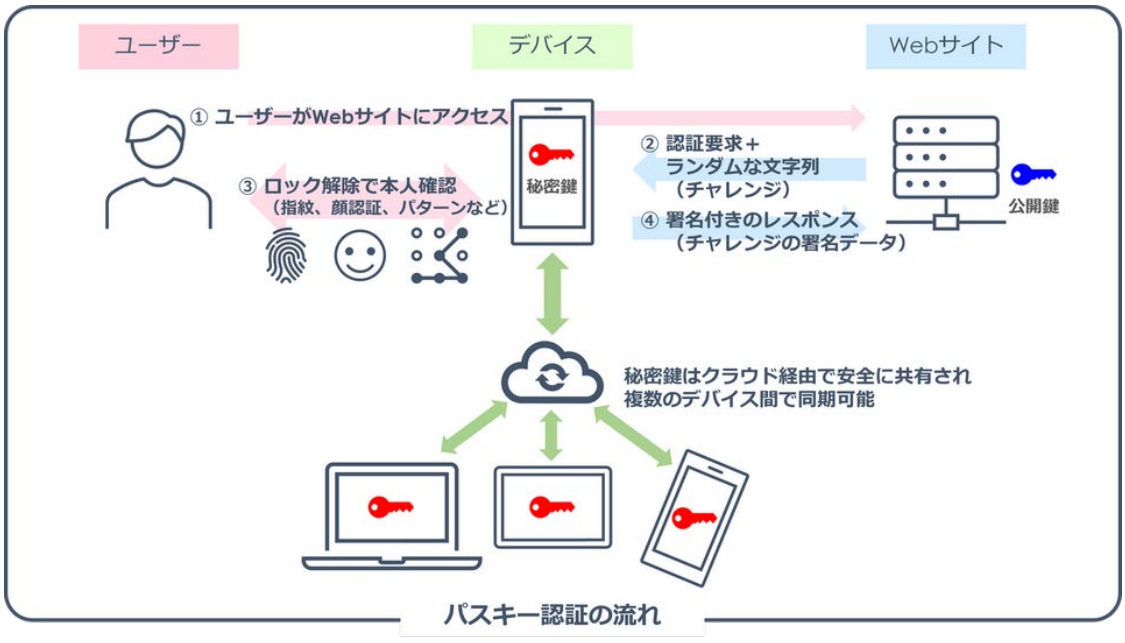
*[1]公開鍵暗号方式：データを暗号にする鍵と異なる鍵で、もとに戻す（復号化する）暗号方式。2 つの鍵は暗号化にも復号化にも使用できるが、一方の鍵で暗号化した情報はもう片方の鍵でしか復号化できない。

＊2FIDO アライアンス：パスワードへの過度の依存を減らすための認証標準を定める業界団体。

多くの Web サイトで利用されている ID・パスワード認証は、Web サイトで事前に登録した ID とパスワードを使ってログインする仕組みです。
しかし、推測されやすいパスワードや、複数のサイトで同じ ID・パスワードを使い回すといった問題が起こりがちです。

一方、パスキー認証では、利用者のデバイス（PC やスマートフォン）で Web サイトごとに秘密鍵と公開鍵のペアを作成し、事前に対象の Web サイトに ID と公開鍵を登録します。

パスキーを使用する際の流れは下記の通りです。
①利用者がサイトにアクセスし、ログイン ID を入力すると、
②Web サイト側は認証のために、利用者のデバイスにチャレンジと呼ばれるランダムな文字列を送ります。
③利用者は送られたランダムな文字列を確認するために、デバイスのロック解除をすることで本人確認を行い、
④送られてきたランダムな文字列を秘密鍵で暗号化し、Web サイトに送信します。
Web サイト側は送られてきたランダムな文字列を公開鍵で復元し、②で送った文字列と一致している場合にシステムの使用を許可します。



出典：NTT テクノクロス㈱　クラウドセキュリティ情報局「パスキーってなに？パスワードの代わりになる最新の技術を解説 」から

ID・パスワード認証では、ID とパスワードがインターネット上を通過します。これに対して、パスキー認証では ID とチャレンジと呼ばれるランダムな文字列のみがインターネット上を流れるため、ID やパスワードが盗まれるリスクが最小化されます。

パスキー導入のメリット

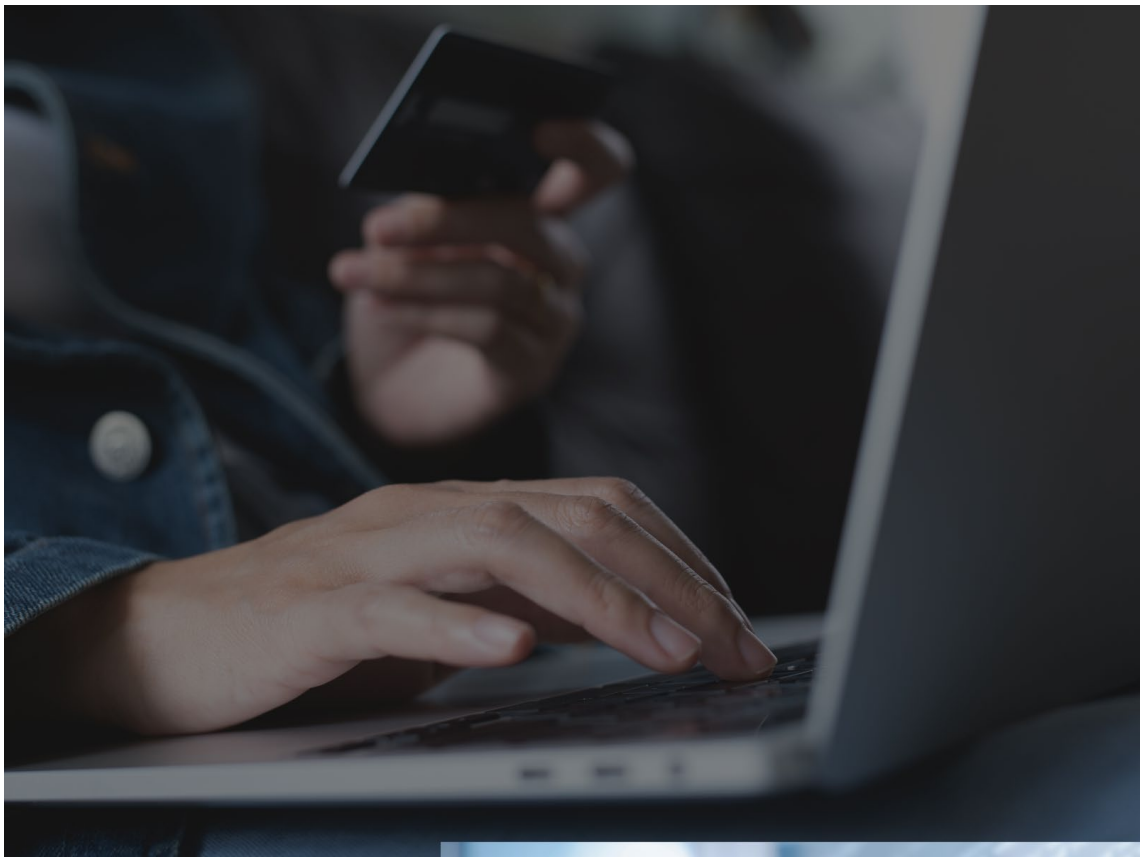
従来の ID・パスワード認証は、予測されやすいパスワードや使い回しによるセキュリティリスクが問題視されています。それに対し、パスキー認証では、複合的なセキュリティ層を提供し、不正アクセスを防ぎやすくします。企業や組織がこれらの新しい認証方法を導入するメリットは大きく、ユーザの安全性を確保しつつ、利便性を損なうことがありません。

今後、ますます多くの企業やサービスがこの 2 つの認証技術を採用し、より安全で便利なユーザ体験を提供していくことでしょう。技術の進歩により、これらの認証方法は新しいセキュリティの標準となる可能性があります。

参考文献

1. 【初心者向け】多要素認証とは? 二段階認証との違いや具体例を紹介｜ICT Digital Column https://www.nttpc.co.jp/column/security/whats_multi-factor-authentication.html
2. パスキーってなに？パスワードの代わりになる最新の技術を解説 https://www.trustbind.jp/column/passkeys-20240314.html

一般向け 2_#11_「不正送金」
掲載日：2024/11/15



サイバーセキュリティの基本を理解するためには、いくつか重要なセキュリティ用語を知っておくことが必要です。
これらの言葉や概念を正確に理解することで、企業が直面するリスクを最小限に抑え、適切な対策を講じることができます。
本記事では、中小企業が特に知っておくべきセキュリティ用語について解説しています。

今回のテーマは、「不正送金」です。

不正送金とは

「不正送金」とは、本人の意思に反して、銀行口座から資金が不正に引き出される行為を指します。
昔からある犯罪であり、高齢者を狙った電話での詐欺（いわゆる「オレオレ詐欺」）で銀行から特定口座に振り込ませるものや、経理担当者が自分の口座に会社の資金を振り込む内部不正のケースも「不正送金」に当たります。

今回はサイバーセキュリティに関するものとして、インターネットバンキングとビジネスメール詐欺について詳しく解説します。

インターネットバンキングでの不正送金

インターネットバンキングでの不正送金は、利用者の ID とパスワード等を窃取、もしくは乗っ取ること(以下アカウント乗っ取りと略す)により実行されます。

アカウント乗っ取りの主な手段は、フィッシング（本記事＃7「フィッシングと SNS 乗っ取り」で解説）が多くなっています。
そのほかにも、次のような手口もあり、組み合わせて使われる場合もあります。

【手口１】専用マルウェア（本記事#6「マルウェア・ランサムウェア」で解説）：アカウント情報を盗み出す、ユーザーのキー入力を送信するなどアカウント乗っ取り専用のマルウェア
【手口２】標的型メール：相手を特定して送るフィッシングメール

インターネットバンキングでの不正送金は急増しています。
警察庁報告書「令和５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」では、令和 5 年の状況について次のようにまとめています。

・ 被害件数・金額は 5,578 件・87.3 億円と過去最多で、令和 4 年（被害 1,136 件・15.2 億円）に比べて件数で 4.9 倍、金額で 5.7 倍と急速に増大。
【図表９：インターネットバンキングに係る不正送金事犯の発生件数及び被害額の推移】



出典：令和５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(警察庁)

- 被害者の 97.9%が個人。全体の 60%が 40 代~60 代。
- フィッシングの手口としては、電子メールが 53%、SMS が 21%。
- 不正送金先は暗号資産交換業者の金融口座が金額の 51%。

インターネットバンキングでの不正送金は、フィッシング、マルウェア等を通じて発生します。このような被害を防ぐためには、対策をしっかりと行うことが重要です。

ビジネスメール詐欺（BEC）での不正送金

ビジネスメール詐欺（Business E-mail Compromise：BEC）とは、取引口座番号の変更や急な支払い要求などの偽の電子メールを組織や企業に送り付け、従業員を騙して攻撃者の用意した口座へ送金させるもので、標的型メール攻撃の一種です。
インターネットバンクでの不正送金に比べて、1 件当たりの被害金額が大きいのが特徴です。

独立行政法人情報処理推進機構（IPA）の分類では、BEC には 2 つのタイプがあります。
一つは取引先を装うもので、もう一つは経営者を装うものです。
攻撃者はこれらのメールを使って、従業員に偽の口座に送金させるのがその手口です。

【手口１】取引先を装うもの

攻撃者が取引先になりすますものです。取引先との請求書等のやり取りをメールなどで行っている場合に利用されます。攻撃先企業の取引にかかわるメール内容を事前に入手することで、攻撃先企業担当者に偽の請求書等を取引先からの本物の請求書メールと誤認させます。

【手口２】経営者を装うもの
攻撃者が攻撃先企業の経営者や役員などになりすますものです。財務・経理・会計担当者に攻撃者の用意した口座に振り込ませる手口です。
攻撃先企業の経営者や役員などの情報を事前に入手することで、攻撃先企業の財務・経理・会計担当者に経営者や役員などからの指示のメールと誤認させます。

BEC は単独の企業だけでは対策が完結できません。
偽の電子メールは、取引先や経営陣を装って送られてきます。
マルウェア等を使って乗っ取った本来の取引先や経営陣の PC を使って送っていることもあり得ます。

各企業には基本的セキュリティ対策を確実に実施することが求められます。
その上で、BEC 対策の要となる「財務・経理・会計担当者」への教育や、取引先口座の変更はメール以外で確認するなどのルール整備が重要です。

最後に

不正送金を防ぐためには、フィッシング対策やウイルス対策などのセキュリティ対策をすべての企業が確実に実施することが必要です。
今回、参考文献として下記に掲載した資料は、皆さんに確認していただきたい資料です。

中小企業だからと言ってセキュリティ対策を怠ると、サプライチェーンの別企業を攻撃するための踏み台に利用され、被害を受けた企業からの損害賠償請求や取引停止となる場合もあります。
各企業が十分にセキュリティ対策を行うことが、不正送金防止の第一歩です。

参考文献

1. 令和５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(警察庁)
   https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf
2. ビジネスメール詐欺に注意！(警察庁)
   https://www.npa.go.jp/bureau/cyber/countermeasures/bec.html
3. ビジネスメール詐欺（BEC）対策

https://www.ipa.go.jp/security/bec/index.html

一般向け 2_#12_「内部不正」
掲載日：2024/11/29



サイバーセキュリティの基本を理解するためには、いくつか重要なセキュリティ用語を知っておくことが必要です。
これらの言葉や概念を正確に理解することで、企業が直面するリスクを最小限に抑え、適切な対策を講じることができます。
本メールマガジンでは、中小企業が特に知っておくべきセキュリティ用語について解説しています。

今回のテーマは、「内部不正」です。
セキュリティインシデントと聞くと、外部からのサイバー攻撃などの脅威を連想しがちです。しかし、情報漏えいといったインシデントは、内部関係者の不正行為によって発生するケースもあるのです。独立行政法人情報処理推進機構（IPA）が毎年発行している「情報セキュリティ 10 大脅威 2024（組織編）」では、**内部不正による情報漏えい等の被害**が第 3 位にランクインしています。
内部不正による情報漏えいは、具体的な被害に遭うだけでなく企業イメージの損失に繋がりかねないため、組織は内部不正が起きないよう対策を施す必要があります。

内部不正とは

「内部不正」とは、従業員や委託先など組織の関係者が自己の利益等を目的に、企業の機密情報や資産を不正に持ち出したり、不正に利用したりする行為です。
例えば、顧客情報の無断持ち出しや漏えい、情報システムの破壊などが挙げられます。故意に不正をはたらくケースはもちろん、従業員が意図せず誤って情報漏えいを引き起こしてしまうケースも内部不正の一種になります。

内部不正の事例

実際にあった事例には、次のようなものがあります。いずれの事例も、内部不正をはたらいた個人の利益を目的に引き起こされました。

事例	企業	時期	実施者	漏えい情報とその使い道
1	NTT 西日本	‘23 年 10 月	業務委託先 グループ企業に勤務していた派遣社員	900 万件の顧客情報を名簿業者に売却
2	兼松	‘23 年 9 月	従業員	新製品情報等の営業秘密を転職時に持ち出し
3	平塚市	‘19 年 8 月	市議会に立候補した元職員	市民 3 万人分の個人情報を持ち出し、有権者にハガキを送付
4	ベネッセ	‘14 年 6 月	業務委託先グループ企業に勤務していた派遣社員	3500 万人の会員情報を名簿業者に販売
5	東芝	‘14 年 3 月	提携先企業の従業員	研究データ(営業秘密)を持ち出し、転職先に提供

事例 4 において、株式会社ベネッセコーポレーション(ベネッセ)は自社の会員に対し、1 人当たり 500 円(単純計算で 175 億円)を支払いました。
また事例 5 では、情報を持ち出された株式会社東芝（東芝）は元従業員の転職先の企業に対して損害賠償を請求する訴訟（損害額 1 千億円以上）を起こしています。

内部不正が起こる要因

内部不正の多くは、システムへのアクセス権等もともと正当な権限を持っている人が業務の中で行う行為のため、不正行為を防ぐことが非常に難しくなっています。

人が不正をしてしまう仕組みをモデル化した「不正のトライアングル」理論では、内部不正は「機会」「動

機・プレッシャー」「正当化」の 3 つの要素が組み合わさることで発生するとされています。

要素	内容	具体的状況の例
機会	不正ができてしまう環境・制度があること	・長期間、個人の専任業務になっている ・一人で簡単に情報が入手できる
動機・プレッシャー	やむなく不正をしなければならない理由があること	・多額の借金がある ・達成困難な目標がある ・その情報が転職後に優位にはたらく
正当化	不正行為を行う本人が、その行為を正当化する理由を持っていること	・自分は適切に評価されていない ・周りも同じことをやっている ・影響は小さい

上記からわかるように、人の心理がきっかけとなりやすい内部不正は、サイバー攻撃への対策とは別のアプローチによる対策が必要となります。

内部不正を防ぐために

内部不正を防ぐ鍵は、上記の表の「具体的状況の例」にあるような状況を作りださないような仕組みづくりにあります。具体的な対策として、以下のようなものがあります。

【不正を行わせないシステム】

特定の従業員がすべてのプロセスを長期間担当することを避け、**一定の期間ごとに担当者を変更する・業務を分割する・複数人で分担する**ことが有効です。また、重要な情報へのアクセスや持ち出しを伴う作業は、**申請・承認のワークフローを必須化するなど、不正を行いにくくするルールの策定**も効果的です。

【労働環境の整備】

組織として個人と十分なコミュニケーションをとり、過度なストレスや組織の不満に対する策を講じます。定期的な個別面談（1on1 など）により、業務過多になっていないかや、個人的な困りごとであっても組織として把握し、手助けできるような**良好な関係性や組織風土・職場環境を築く**必要があります。
良好な関係性であっても、組織に不利益をもたらすようなことへの処罰を明確化し、厳罰に処する**毅然とした組織風土を醸成する**ことも重要です。

職場環境が悪い・風通しが悪い企業では個人の不満が増幅し、内部不正を引き起こす要因を作り出してしまいます。
組織に関わる**個々人の業務に対する満足度を上げていくこと**が「内部不正」対策への重要な施策と考えられています。

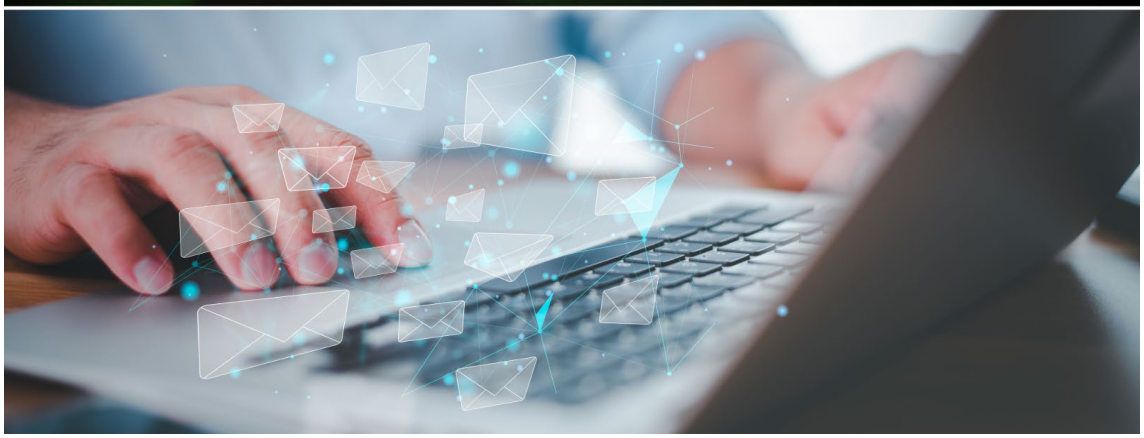
※内部不正については、こちらの記事でもご紹介しています。こちらもご覧ください。
中小企業におけるセキュリティ脅威への対策強化 ～内部不正による情報漏えい等の被害 から対策を学ぶ～【基礎から学ぶセキュリティ#10】

参考文献

１．（事例１）お客さま情報の不正流出に関するお詫びとお知らせ（西日本電信電話株式会社）
https://www.ntt-west.co.jp/news/2310/231017a.html
お客さま情報の不正持ち出しを踏まえた NTT 西日本グループの情報セキュリティ強化に向けた取組みについて（西日本電信電話株式会社）
https://www.ntt-west.co.jp/news/2402/240229a.html
２．（事例２）大手商社「双日」元社員を逮捕　前職「兼松」から機密情報を不正に持ち出した容疑（ITmedia NEWS）
https://www.itmedia.co.jp/news/articles/2309/28/news139.html
３．（事例３）元職員による個人情報等の持ち出しについて（平塚市）
https://www.city.hiratsuka.kanagawa.jp/joho/page06_00025.html
４．（事例４）事故の概要　（ベネッセお客様本部）
https://www.benesse.co.jp/customer/bcinfo/01.html
５．（事例５）東芝技術流出事件と営業秘密管理　（デルタエッジコンサルタント株式会社）
https://deltaedge.co.jp/2014/04/01/%E6%9D%B1%E8%8A%9D%E6%8A%80%E8%A1%93%E6%B5%81%E5%87%BA%E4%BA%8B%E4%BB%B6%E3%81%A8%E5%96%B6%E6%A5%AD%E7%A7%98%E5%AF%86%E7%AE%A1%E7%90%86/
６．「不正のトライアングル」を理解して、組織の不正を未然に防ぐ方法とは（ UPGRADE）
https://www.corner-inc.co.jp/media/c0200/

一般向け 2_#13_「標的型攻撃メール」
掲載日：2024/12/13





サイバーセキュリティの基本を理解するためには、いくつか重要なセキュリティ用語を知っておくことが必要です。
これらの言葉や概念を正確に理解することで、企業が直面するリスクを最小限に抑え、適切な対策を講じることができます。
本記事では、中小企業が特に知っておくべきセキュリティ用語について解説しています。

今回のテーマは、「標的型攻撃メール」です。

標的型攻撃メールとは

「標的型攻撃メール」とは、特定の企業や組織に属する従業員をターゲットとしたフィッシングメールの一種です。
一般的なフィッシングメールでは、不特定多数に同じ内容のメールが送信され、主に個人の財産や情報が狙われます。
これに対して、標的型攻撃メールでは、特定の対象者宛に個別メールを送信し、企業や組織の資産や

重要情報を狙うという相違点があります。

フィッシングメールについては、こちらの記事＃7「フィッシングと SNS 乗っ取り」で詳しく解説しているので、ご参照ください。

標的型攻撃メールとフィッシングメール攻撃の違い

標的型攻撃メールとフィッシングメールの比較を次の表にまとめました。

	標的型攻撃メール	フィッシングメール
受信者 （標的）	特定の企業や組織に属する個人やグループ	不特定多数の個人
送信者 (攻撃者がなりすます相手)	対象企業の取引先や上司など関係者、社内関連部署等	クレジットカードやネットサービスの管理者等
メール内容	仕事上の指示や依頼に関するもの	ID の不正使用や切替えへの対応依頼等
攻撃の目的	企業や組織の資産、PC や ID の乗っ取り、他企業攻撃の足掛かりの作成	個人の財産、PC や ID の乗っ取り

次からは、受信者、送信者とメール内容、攻撃の目的の 3 つに分けて、標的型攻撃メールで行われていることを順に説明します。

（１）受信者（標的）

標的型攻撃メールでは、攻撃者は初めに攻撃対象となる企業や組織に属する従業員のメールアドレスを様々な方法で取得し、ターゲットを絞ってメールを送信してきます。
受信者（標的）を特定するための方法には、次のようなものがあります。

- インターネットサイトやダークウェブ(闇サイト)での取得
- すでに乗っ取った関連企業・組織(対象企業・組織含む)の PC や ID 等の利用
- 取引先等を詐称して該当企業に電話するなど、人間の心理的な隙へのつけ込みによる取得

（２）送信者（攻撃者がなりすます相手）とメール内容

メールの送信者名や送信元アドレスは容易に偽装されます。
フィッシングメールでも標的型攻撃メールでも、送信者が偽装される点は同じです。
しかし、偽装された送信者が全く異なります。
標的型攻撃メールでは、取引先や上司・経営者、社内関連部署などになりすまし、メールの内容も偽装した送信者に合わせたものになっているのが特徴です。
例えば、取引先からの請求書差し替えのメールや上司からの指示メールなど、日頃の業務に関わる内容になっています。このため、受信者はあたかも通常の業務の一環として対応し、疑うことなく文中のリンクをクリックしたり、添付ファイルを開いたりしてしまうことがあります。

標的型攻撃メールでは、狙われた人の関係者が送信者となっていることから、攻撃メールとは気づかずに本物のメールと信じてしまう確率が非常に高くなっています。
特に、乗っ取られた PC や ID を使った標的型攻撃メールは、偽装部分がメール内容だけのため、防ぐのは非常に困難です。

（３）攻撃の目的

標的型攻撃メールの最終的な狙いは様々で、企業の機密情報や内部情報の搾取や金銭の取得です。
標的型攻撃メールで金銭を取得する方法は、ビジネスメール詐欺（こちらの記事 ＃11「不正送金」で解説）による直接の金銭詐取、マルウェアから企業内部へ侵入し機密情報を盗み売却するもの、ランサムウェアを感染させ身代金を要求するものなど、多岐に渡ります。

標的型攻撃メールへの対策

前述したとおり、標的型攻撃メールは受信者が不審を抱かないように、あたかも業務に関係したメールのように偽装されるため、防ぐことは非常に困難です。
自企業内に攻撃者に乗っ取られた PC や ID が存在すると、その PC や ID を使って取引先へ攻撃ができることになります。

このため、**すべての企業が「基本的なセキュリティ対策を確実に実施すること」が最も重要な防止策**となります。
たとえ信頼できる送信者からのメールであっても、内容に違和感を持ったときには、電話などメール以外の方法で、必ず相手に確認するようにしてください。

また、EDR や UTM などのセキュリティソリューションを導入することで、標的型攻撃メールによるマルウェア感染時の早期検知が可能となり、被害の拡大を抑えることが期待できます。
完全な防護策ではありませんが、EDR、UTM をまだ導入されていない方は、早期の導入を検討してみることも対策の一つとして有効です。

EDR や UTM については、下記で詳しく解説しているので、あわせて参照ください。
・#2「EDR」
・#3「UTM」

参考文献
１．「国民のためのサイバーセキュリティサイト（標的型攻撃への対策）」総務省
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/security/business/staff/04/

一般向け 2_#14_「クラウドセキュリティ」

掲載日：2024/12/20



サイバーセキュリティの基本を理解するためには、いくつか重要なセキュリティ用語を知っておくことが必要です。

これらの言葉や概念を正確に理解することで、企業が直面するリスクを最小限に抑え、適切な対策を講じることができます。

本記事では、中小企業が特に知っておくべきセキュリティ用語について解説しています。

近年テレワークの導入が進み、クラウドサービスを利用する企業が増加しています。

今回のテーマは、クラウドを利用する際に気を付けなければならない「クラウドセキュリティ」です。

クラウド利用のリスク

企業のあらゆる規模や業種において、クラウドは今や欠かすことのできない社会インフラとなっています。

スマートフォンを使っていれば、iCloud や Google ドライブといったクラウドサービスは日常的に使用するツールとなってきています。

また、企業環境においても Word、Excel、PowerPoint などの Microsoft365 や各種会計ソフトのようなクラウドベースのアプリケーションが広く利用されています。

しかし、これらの利便性の背後には、いくつかの重大なリスクが潜んでいます。

（１）自由なアクセスに伴うセキュリティリスク

ID とパスワードによる認証のみで、だれでもどこからでもアクセスができること。これこそがクラウドの最も便利なところですが、企業にとってはリスクもあります。
従業員が業務時間外に不適切な利用を行う、サイバー攻撃者に認証情報の不正取得をされるリスクがあります。一度**攻撃者に認証情報が漏れると、クラウドに格納されている情報は窃取**されます。

（２）導入の容易さと潜在リスク

簡単に利用を開始できることがクラウドの良いところです。
しかし、それゆえに部門ごとに個別の契約がなされるケースもあり、企業の財務に**隠れた負債**が生じる可能性があります。
これが**企業の隠れ債務**となる可能性があるのです。

（３）セキュリティ対策の不備

クラウドサービスの中には、セキュリティ対策や可用性が不十分なものもあります。
過去には、個人情報の漏えい、システムの長期間の停止やデータの消失が発生したクラウドもありました。
契約したクラウドサービスでインシデントが発生した場合、**自社の機密情報漏えいや業務停止が起こります**。
また、一部の国や地域では、公権力へのデータ開示が義務づけられています。クラウドを構成するサーバーは、存在する国・地域の法律が適用されるので注意が必要です。

クラウドを安全に使うには

クラウドの持つメリットを最大限に活用しつつ、安全に利用するためには、提供されるサービスや機能、利用条件を確認することが最も重要です。確認する項目は次の通りです。

（１）機能適合性の確認

まず、選定するクラウドサービスが**自社の業務要件に合っているか**を確認することが重要です。
多くのクラウドサービスはお試し期間を設けているので、**事前に試してみるこ**とをお勧めします。
クラウド契約のなかには、**部門単位の契約を認めておらず、全社員分の契約を要求する**ものもあります。必ず契約内容を確認してください。

（２）セキュリティレベルの確認

次に、クラウドサービスが取り扱う情報の重要性に応じたセキュリティ対策が講じられているかを確認します。クラウドのセキュリティレベルは様々です。
ID とパスワードによる認証のみに依存しない、**二要素認証や二段階承認などの追加セキュリティが実装されていること**が望ましいです。
また、サービスを**海外で展開する場合には、該当のクラウドが GDPR**（General Data Protection Regulation：EU 一般データ保護規則）に準拠しているか、サーバー所在地の国や地域の法律の確認も必要になります。

（３）信頼できる提供者の選定

どんなに機能的に優れたサービスであっても、信頼できない企業が運営しているクラウドに自社のデータを預けませんよね。
セキュリティ対策はもちろんのこと、クラウドサービスの提供者がどれほど信頼できるかという点も重要なポイントです。
提供者が十分な資金力を持ち、セキュリティ更新やデータのバックアップなどが堅実に行えるかどうかを確認することで、リスクを軽減できます。

クラウドサービス利用時のルール整備

最後に、自社内でのクラウドサービス利用に関するルールの策定が欠かせません。
申請方法、利用権限、データの配置方法など、セキュリティを考慮した**利用方法が決められていないと、**

本来安全に使えるクラウドでの情報漏えい事故が発生する可能性が高まります。ルールを策定し、安全にクラウドを利用できる環境を整えましょう。
クラウドを使う目的を明確にし、自社にあったルールを制定してから、利用することが重要です。

まとめ

クラウドサービスは、正しく利用すれば非常に便利で安全なサービスです。
しかし、利用にあたっての適切な対策を怠った場合、大きな問題を引き起こすリスクがあります。各機関が発行しているガイドラインや資料を参考にすることで、さらに効果的な対策の構築が期待できます。
サービスの特徴を十分理解し、安全に利用するための準備を整えましょう。

参考文献

1. 「中小企業のためのクラウドサービス安全利用の手引き」（独立行政法人情報処理推進機構（IPA））
   https://www.ipa.go.jp/security/sme/f55m8k0000001wpl-att/outline_guidance_cloud.pdf
2. 中小企業の情報セキュリティ対策ガイドライン 付録 6：中小企業のためのクラウドサービス安全利用の手引き （IPA）
   https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000072150.pdf
3. クラウドサービス提供における情報セキュリティガイドライン（第 3 版） 総務省
   https://www.soumu.go.jp/main_content/000771515.pdf
4. クラウドセキュリティガイドライン 活用ガイドブック（2013 年度版） 経済産業省
   https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudseckatsuyou2013fy.pdf

一般向け 2_#15_「サプライチェーン」
掲載日：2025/1/10



サイバーセキュリティの基本を理解するためには、いくつか重要なセキュリティ用語を知っておくことが必要です。
これらの言葉や概念を正確に理解することで、企業が直面するリスクを最小限に抑え、適切な対策を講じることができます。
本記事では、中小企業が特に知っておくべきセキュリティ用語について解説しています。

今回のテーマは、これまでたびたび触れてきた「サプライチェーン」です。

サプライチェーンとは

サプライチェーンは簡単に言うと、『取引先を含めた供給ネットワーク』です。
もう少し詳しく言うと、サプライチェーンは製品やサービスの提供者、原材料の供給元、さらには物流業者や販売パートナーなど、多岐にわたる要素で構成されています。

一つの製品が消費者に届くまでには、さまざまな企業が連携し、それぞれが異なる役割を果たしています。

例えば、皆さんが勤めている企業を中心に考えてみましょう。下図を参照してください。

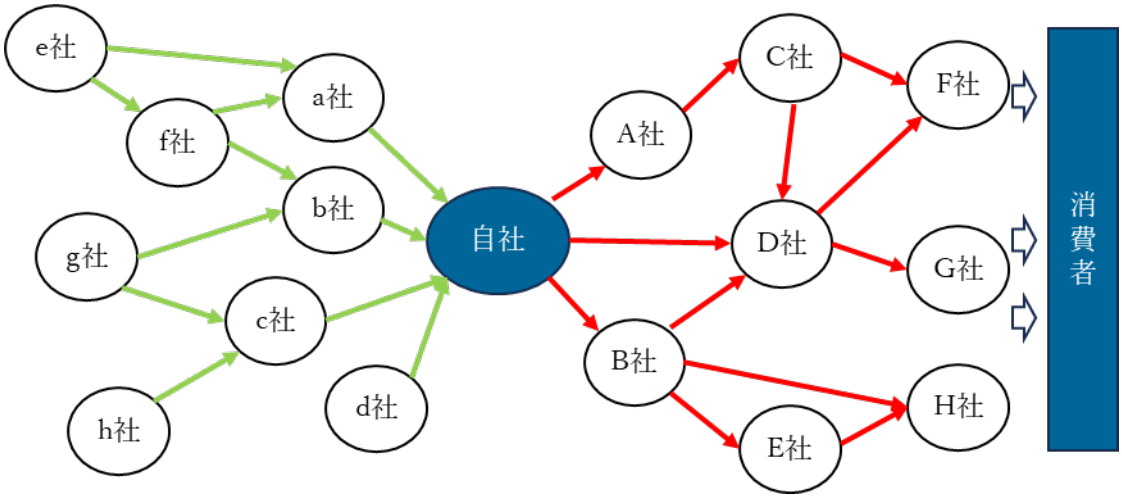


図.サプライチェーン

この図の白い丸で示されているのが各取引先であり、それを結ぶ網のようなネットワークがサプライチェーンです。

このサプライチェーンの中には、自社や各取引先が利用しているクラウドサービスの提供事業者や、社内の IT 機器を保守している IT ベンダーなども含まれています。

サプライチェーンリスクとは

サプライチェーンリスクとは、取引先を経由して自社のセキュリティが破られてしまうこと、または取引先のセキュリティ事故などにより自社が被害を受ける危険性があることを指します。

サプライチェーン内で起きるサイバー攻撃の具体例を挙げると、以下のような状況が考えられます。

〈ステージ１〉サプライチェーンの中にセキュリティ体制が脆弱な企業がある場合、
その企業が最初に攻撃を受けセキュリティが破られます。
〈ステージ２〉攻撃に成功した企業を足掛かりにその企業の取引先へと攻撃が波及し、
時間とともに被害が拡大します。
〈ステージ３〉攻撃被害の拡大の中で自社の取引先が侵害されることで、自社も攻撃対
象となる危険性が高まります。

攻撃方法としては、以前ご紹介した「標的型攻撃メール」に加え、取引先からの物理的な納品物

（USB メモリ、CD-ROM、電子媒体など）にマルウェアが混入されるケースなどがあります。

また、取引先がサイバー攻撃を受けた場合、自社が受ける影響には次のようなものがあります。

- 取引先が攻撃を受け業務が停止した場合、必要な部品等の供給がストップし、自社の生産が停止する。
- 取引先のマルウェア感染などにより、自社から委託していた個人情報や秘密情報が漏えいする。

サプライチェーンリスクの重要な点は、「自社だけでは対応できない」ということです。
これまで何度も、「自分事としてセキュリティに気を付けてください」というメッセージを伝えてきました。
しかし、自社のセキュリティをどれだけ高めても十分に対応できないリスクの一つが「サプライチェーンリスク」です。

サプライチェーンリスクへの対応策

自社だけで、サプライチェーンリスクを完全に回避することは非常に困難です。
しかし、取引先と協力し、セキュリティを共に強化することにより、リスクの低減を図ることが可能になります。

重要なのは自社のセキュリティを強化するだけではなく、取引先に対しても同じレベルのセキュリティの強化を要求することです。

例えば、次のようなことが考えられます。

- 同等の品質や価格で同じ製品やサービスを提供する企業が複数ある場合、セキュリティ状況を比較し、セキュリティレベルが高い企業と取引を行う。
- 取引の契約書にセキュリティの条項を設け、一定レベル以上のセキュリティ水準を達成することを取引条件とする。
- 取引先からのセキュリティ強化の相談に応じる。または、共同でセキュリティ確保の施策を検討し、実施する。

最後に

今後、取引先からのセキュリティに対する取り組みの要求はますます高まると予想されます。
これまで、一部の経営者の中には「中小企業だから狙われない」「セキュリティはコストで利益を生まない」という認識がありました。
しかし、このような認識は自らのビジネスを狭める要因となります。セキュリティ対策が不十分な企業は、今後、取引先から選ばれにくくなり、ビジネスチャンスを逃すことにもなりかねません。

もう一度、自社のセキュリティ状況を確認し、対応が不十分な項目を一つ一つ改善していくことが重要です。セキュリティ対策を継続的に強化し、自社のビジネスを守っていきましょう。

サプライチェーンに関する攻撃例や具体的な対策について、こちらの記事で詳しく紹介しています。ぜひ自社のセキュリティ対策に活かしてください。

・中小企業におけるセキュリティ脅威への対策強化～サプライチェーンの弱点を悪用した攻撃から対策を学ぶ～

参考文献

1. 実務者のためのサプライチェーンセキュリティ手引書　IPA
   https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2024/f55m8k0000003vf5-att/f55m8k0000003vp7.pdf
2. SC3 サプライチェーン・サイバーセキュリティ・コンソーシアム
   https://www.ipa.go.jp/security/sc3/

一般向け 2_#16_「脆弱性とゼロデイ攻撃」
掲載日：2025/1/24



サイバーセキュリティの基本を理解するためには、いくつか重要なセキュリティ用語を知っておくことが必要です。
これらの言葉や概念を正確に理解することで、企業が直面するリスクを最小限に抑え、適切な対策を講じることができます。
本記事では、中小企業が特に知っておくべきセキュリティ用語について解説しています。

今回のテーマは、「脆弱性とゼロデイ攻撃」です。
いずれもあまり聞きなれない言葉かもしれませんが、サイバーセキュリティでは非常に重要な用語ですので、ぜひ覚えておきましょう。

脆弱性とは

もともと「脆（もろ）くて弱い性質または性格」（「デジタル大辞泉」より）という意味ですが、IT の世界では「システムやネットワークのセキュリティ上の欠陥または、設定ミスによる欠陥のこと」(「情報セキュリティ用語辞典」より)という意味で使われます。

簡単に言えば、**ハードウェアやソフトウェアに存在するセキュリティ上の弱点**のことです。
プログラムの不具合や設計上のミスが原因となって発生するセキュリティ上の欠陥を意味し、セキュリティホールとも呼ばれます。

攻撃者は脆弱性を悪用して攻撃を仕掛けてきます。例えば、システムの情報を窃取したり、システムそのものを停止または乗っ取ったり、偽のシステムに誘導して個人情報を盗み出すなど様々です。

では、なぜ脆弱性が生まれるのでしょうか。
いろいろな原因がありますが、**いずれもシステムの不具合や設定ミス**に起因します。
プログラムやシステムは、予測される様々な使用状況を想定して作られています。
しかし、**想定外の入力に対する予測が不十分な場合、誤った処理が行われたり、システムが停止したりすること**があります。これが脆弱性の原因となります。

代表的な例として、SQL インジェクションという攻撃手法があります。
これは Web サイトのデータ入力欄にデータベースを操作するコマンドを入力することで、データベースを不正に操作したり、データを不正に入手するものです。このような攻撃は、入力内容を厳密にチェックしていない Web サイトの設計ミスを巧みに利用しています。

脆弱性への対応方法

繰り返しになりますが、脆弱性は想定外のデータが入力されたり、想定外の環境で使用されたりすることで発生します。

また、よくできたプログラムであるほど長期間使用され、別の環境で利活用されることもあります。脆弱性はどんなシステムにも存在し得ます。プログラムである以上、100%バグがないということは非常に難しいことです。

このような状況が進むと、時間の経過やシステム設定の変更によって新たなバグが発生することになります。
例えば、商品コードの体系を数字 6 桁から英数字 6 桁に変更したり、使用しているデータベース製品のバージョンアップにより、新たな環境設定が必要になったりすることです。

また、長年安全だと思って使用していたシステムに脆弱性が潜んでいたという事例もあります。
例えば、Web などのインターネット通信を行う際に、安全にデータをやり取りするための暗号化通信方式として使用されてきた SSL 3.0 は広く使用されていましたが、2014 年に重大な脆弱性が発見されたため、TLS という別の暗号化通信方式に移行されました。

これらのことから、脆弱性に対応するためには、以下の 2 つの取り組みを継続的に行うことが必要です。

（１）セキュリティアップデートの適用
　使用しているシステムの脆弱性が発見された場合、開発者等から配布されるセキュリティパッチやアップデートを早期に適用する。
（２）老朽システムの置き換え

保守が行われなくなった古いシステムは、新しい技術やシステムに移行する。

ゼロデイ攻撃

ゼロデイ攻撃とは、**脆弱性に対応するアップデートやセキュリティパッチが提供される前に、その脆弱性を悪用したサイバー攻撃**です。
対応するアップデートやセキュリティパッチを適用する前に攻撃が行われるため、防ぐことは非常に困難です。

攻撃手法は大きく分けて「標的型攻撃」と「ばらまき型攻撃」の 2 つがあります。特にメールを利用した標的型攻撃の場合、悪意あるメールが送付されていても、攻撃を受けたことがわからないままとなる場合があります。
標的型攻撃メールについては前回解説しています。こちらも是非ご覧ください。
「標的型攻撃メール」

では、どうしたらよいのでしょうか。
標的型攻撃メールへの対応策として以前ご紹介したセキュリティソリューションである UTM や EDR は、ゼロデイ攻撃に対しても有効です。
UTM、EDR は PC やサーバーの不審な動きを検出するツールです。ゼロデイ攻撃を 100%防ぐことはできませんが、攻撃を受けた際の早期検知と迅速な対応が可能になります。

最後に

脆弱性はどんなシステムにも存在します。
また、新たな脆弱性が発見されると、それを利用したゼロデイ攻撃が行われます。
UTM や EDR を導入しても、ゼロデイ攻撃を 100%防ぐことはできません。

では、どのような対策が有効でしょうか。
ゼロデイ攻撃も含めたサイバーセキュリティ事故が発生した場合の対応を事前に定め、訓練することによって、被害を軽減することができます。
このように、サイバーセキュリティ事故の発生を常に想定し、準備を整えておくことが重要です。

参考文献

1. ゼロデイ攻撃とは? 仕組みや手段から被害、対策まで基本を広く解説｜ICT Digital Column 【公式】NTTPC コミュニケーションズ

https://www.nttpc.co.jp/column/security/whats_0day-attack.html

一般向け 2_#17_「BYOD とシャドーIT」
掲載日：2025/1/31



サイバーセキュリティの基本を理解するためには、いくつか重要なセキュリティ用語を知っておくことが必要です。
これらの言葉や概念を正確に理解することで、企業が直面するリスクを最小限に抑え、適切な対策を講じることができます。
本記事では、中小企業が特に知っておくべきセキュリティ用語について解説しています。

今回のテーマは、「BYOD とシャドーIT」です。
近年の企業活動や働き方改革において注目を集める概念のひとつに「BYOD（Bring Your Own Device）」があります。これと表裏一体で課題となるのが「シャドーIT」です。
企業の許可を得た「BYOD」に対し、無許可で利用される「シャドーIT」は、企業にとって大きなリスクとなります。
今回は、利便性や生産性向上を期待して導入される「BYOD」と、その導入が引き起こすリスクである「シャドーIT」について説明します。

１．BYODとは

BYOD とは、「自分のデバイスを持ち込む」という意味で、従業員が私物のパソコンやスマートフォン、タブレット端末など（以下、「デバイス」と記載）を業務用として利用する仕組みを指します。

２．BYODの利点とリスク

BYOD の運用は、従業員側・企業側の双方にメリットをもたらします。しかし、その裏にはいくつかの課題も隠れています。

（１）BYOD の利点

BYOD には、以下の利点があります。

- **・生産性の向上**
  従業員が使い慣れた自身のデバイスを使用することで、熟知した操作性や機能性を活用でき、生産性や業務効率が向上する。
- **・コスト削減**
  企業が全従業員分の PC やスマートフォンを購入・貸与するには多額のコストがかかるが、BYOD を活用することで購入や維持に関する投資を抑えることができる。

さらに、企業には特別な投資を抑えながら柔軟な働き方を提供できるメリットもあります。一見、良さそうな施策ですが、最大の課題はセキュリティリスクになります。

（２）BYOD のリスク

私物デバイスはセキュリティ上の統制（使用禁止アプリ・サイトの規制など）が個人任せになります。
そのため、企業のポリシーやセキュリティ基準に沿っていない場合が多く、BYOD を採用すると、従業員が自己管理するデバイスを企業のネットワークに接続することになり、以下のようなリスクが生じます。

- **・マルウェア感染のリスク**
  危険なアプリや不正なソフトウェアのインストール、個人のメールなどからマルウェアに感染し、**企業のシステム全体へ感染が広がる。**
- **・データ漏えいのリスク**
  従業員が個人のメールアドレスで業務データを扱った場合や、フィッシングメールに遭遇した場合、**企業の重要な情報が外部に流出する危険性が高まる。**
  セキュリティパッチの未実施や、OS やソフトウェアの脆弱性が放置されることも重大なリスクとなる。

３． BYODを安全に使うには

安全性を考えると、デバイスは BYOD を避け、企業が用意する方が望ましいです。
しかし、やむを得ず BYOD を許可する場合は、次のような対策を実施してください。

（１）明確な利用ルールの策定と従業員教育

BYOD を利用するときに守るべきこと、注意すべきことを取り決め、セキュリティポリシーを文書化し、従業員に明確に共有します。
たとえば、「危険なアプリを入れない」「データ取り扱い範囲を制限する」などです。
BYOD を利用する従業員には、ルールとその理由を分かりやすく説明し、決められたルールを守れるよう支援します。

（２）デバイス管理ツールの導入

BYOD 端末も企業側で適切に管理する必要があります。デバイス管理ツールを BYOD 端末に導入し、従業員の私用デバイスも管理できるようにします。
企業は BYOD 端末の状態を遠隔で確認し、必要に応じてリモートでデータ消去を行うことが可能になります。データ漏えいやウイルス感染対策が効果的に行えます。

（３）ネットワークセキュリティの強化

BYOD によるウイルス感染やハッキング被害を防ぐため、VPN（仮想専用ネットワーク）を使用してネットワークにアクセスさせることで、外部からの不正アクセスを防ぐことができます。

（４）データの確実な消去

BYOD で利用したデバイスの会社情報は、利用終了時に完全に削除します。
データは利用者が意図しない場所にも残ることがあり、データ漏えいを防ぐため、BYOD 終了時にデバイスを初期化し、データを確実に消去してください。

そのほか、デバイスの紛失・盗難にも注意を払うことを徹底しましょう。また、退職者のデバイスに、顧客データや業務の機密情報が残るリスクにも注意しましょう。

BYOD 導入のメリットは、会社が定めた適切なルールのもとで利用した場合に限ります。デメリットもあるので、導入する際はリスクコントロールをしっかりした上で運用するようにしましょう。

４．シャドーITとは

BYOD におけるセキュリティリスクの一つにシャドーIT があります。
シャドーIT とは、会社が正式に許可していないデバイスや機器、アプリケーションを従業員が個人的に使用することを指します。従業員が独自に導入したツールやサービスの使用は、企業のセキュリティポリシー外で運用されるため、リスク管理が非常に難しくなります。BYOD の利用が進むと、このシャドーIT のリスクが高まります。

よくあるシャドーIT の事例とリスクには以下のようなものがあります。

種類	使用例	起こりうる問題
クラウドサービス	個人アカウントのGoogle DriveやDropboxを利用した業務データの保存	・業務データの漏えい
ストレージデバイス	許可されていないUSBドライブの使用	・機密情報の持ち出し ・ウイルス感染
ソフトウェアアプリケーション	勝手にインストールしたアプリの利用	・ウイルス感染 ・ライセンス違反
ネットワークデバイス	個人用ルーターを使用した社内ネットワークへの接続	・外部からの企業ネットワークへの侵入

５．シャドーITに対する具体的な対策

シャドーIT は、それぞれの事例ごとに対応することが可能です。
しかし、継続的にかつ網羅的に実施するためには、**仕組み（ハードウェア/ソフトウェアの導入と継続的な監視）の構築**が必要です。
シャドーIT のリスク認識も含めた**従業員向けセキュリティ教育を継続**して実施すること、**IT に関して相談できる部門や人を設置**することなども有効です。
シャドーIT のリスクを減らすためには、以下のような対策を講じることが重要です。

（１）シャドーIT の可視化と監視

企業ネットワークに接続される全てのデバイスやアプリケーションを管理し、従業員が使用する非公式なツールを監視します。これにはネットワーク監視ツールの導入が有効です。

（２）セキュリティ教育と啓発活動

シャドーIT のリスクを従業員にしっかりと伝え、セキュリティに関する意識を高める教育を行います。また、従業員が新しいツールの導入を希望する場合は、会社の許可を得るよう促すことが重要です。

（３）公式の IT ツールやサービスの導入

企業が公式に認めたツールやサービスを導入し、従業員がそれを使用するよう、ガイドラインを設けます。

６．最後に

BYOD は、従業員の利便性や業務効率化など、柔軟な働き方を促進し、生産性を向上させるメリットがあります。しかし、企業が正式に認めていないハードウェアやソフトウェアを従業員が無断で使用するシャドーIT の存在は、重大なセキュリティリスクをもたらします。
BYOD は適切な管理体制を整えることでリスクを抑えて運用することが可能ですが、シャドーIT は安全性の問題が大きいため、企業として根絶すべきものです。

もしシャドーIT が見つかったら、従業員に「なぜ使っているのか」「何に困っているのか」を聞いてみましょう。
その答えから、仕事をもっと効率よく進めるためのヒントが見つかることもあります。

従業員と企業が協力し合い、情報セキュリティに対する意識を共有することが成功の鍵となります。

参考文献

1. WeWork（ウィーワーク）公式サイト｜シャドーIT とは？BYOD との違いや、セキュリティリスクへの対策を解説
   https://wework.co.jp/contents/knowledge/case200
2. シャドーIT と BYOD との違いは？具体例からリスク、原因・対策まで分かりやすく解説
   https://product.sct.co.jp/blog/security/the-difference-between-shadow-it-and-byod

一般向け 2_#18_「BCP（事業継続計画）」
掲載日：2025/2/7



~~こんにちは。「サイバーセキュリティフォローアップ事務局」です。~~

サイバーセキュリティの基本を理解するためには、いくつか重要なセキュリティ用語を知っておくことが必要です。
これらの言葉や概念を正確に理解することで、企業が直面するリスクを最小限に抑え、適切な対策を講じることができます。
本記事では、中小企業が特に知っておくべきセキュリティ用語について解説しています。

今回取り上げるテーマは、「BCP（事業継続計画）」です。
緊急事態への対応として BCP はご存知だと思いますが、サイバーセキュリティとは関係がないとお考えではないでしょうか。
実は、サイバー攻撃リスクへの対策にも深く関わる重要な考え方です。
皆さんのビジネスを守るため、ぜひ一緒に深掘りしていきましょう。

BCPとは

BCP、正式名称「Business Continuity Plan（事業継続計画）」とは、自然災害、大規模火災、テロ攻撃などの予測不可能な緊急事態が発生したときでも、会社の重要な事業を滞りなく継続させるた

め、あるいは可能な限り速やかに復旧させるための対策や手段などをまとめた計画のことです。
緊急事態が発生しても、事業資産の損害を最小限にとどめるため、平常時から準備を行い、危機発生時にどのように行動すべきかを定めたものです。

この概念は、1970 年代にアメリカやイギリスで提唱され始めました。
そして、2001 年 9 月のアメリカ同時多発テロがきっかけとなり、BCP の重要性が世界的に認識されるようになったのです。

企業は BCP を事前に準備しておくことで、不測の緊急事態が起きた際に、迅速かつ適切な対応が可能になります。
当初は、自然災害やテロ、感染症によるパンデミック等を想定した事業継続の計画を意味していましたが、最近では、サイバー攻撃（サイバーテロ）等のサイバーセキュリティリスクに対応する事業継続計画(以下、サイバーセキュリティ対応の BCP と記載)が必要となっています。

サイバーセキュリティとBCP

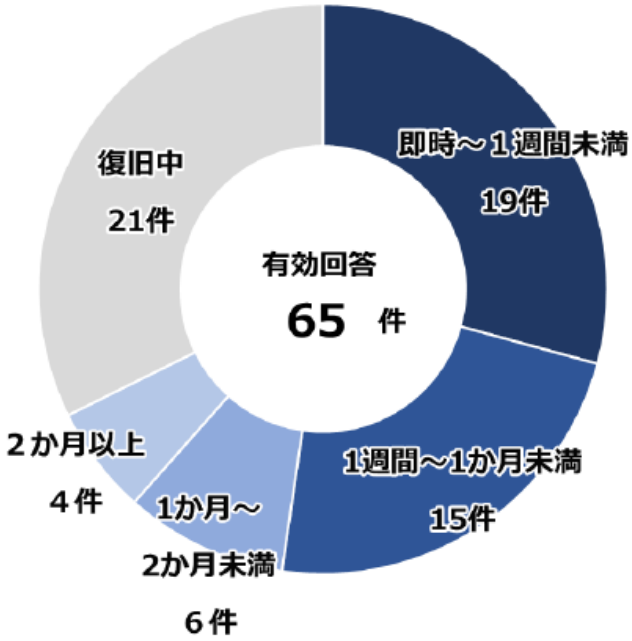
情報化が進む現在、多くの企業で、電子メールやビジネスチャット（LINE Works や Chatwork など）でコミュニケーションを取り、ファイルサーバーやクラウドサービス（Google Drive や OneDrive など）でデータを管理しています。

普段の業務を振り返って見てください。
皆さんの会社でも、業務効率化とデータ管理を目的に、これらの仕組みを活用している場合が多いと思います。
でも、もしそれらが突然使えなくなったとしたら、事業を継続することができるでしょうか？例えば、データファイルにアクセスできなくなったり、取引先との連絡が一切取れなくなるような状況を想像してみてください。
事業継続は非常に困難になるはずです。

従来の BCP は、地震や台風などの自然災害やテロ行為、あるいはパンデミックのような事業継続が困難な緊急事態を想定して策定されることが一般的でした。
一方、サイバーセキュリティ対応の BCP は、近年企業にとって大きな脅威となっているサイバー攻撃により、事業継続が困難になる事態を想定して策定されます。

これらの脅威の中で最もわかりやすい例は、ランサムウェアに感染することです。
以前、「マルウェア・ランサムウェア」の記事でも解説したとおり、ランサムウェアは、ファイルの暗号化により、データの喪失や PC 等が起動しなくなるという状況を引き起こします。
その結果、業務を停止せざるを得ない状況になることも少なくありません。

下記は「令和６年上半期における脅威の情勢等について」(警察庁発表)に掲載されているランサムウェア被害の「復旧等に要した期間」のグラフです。



出典：「令和６年上半期における脅威の情勢等について」(警察庁)

このグラフによると、ランサムウェア被害を受けた企業のうち、１週間以内に復旧できた企業は 19 件（29%）に過ぎません。復旧までの間、業務が完全に停止した企業も少なくなかったと推測されます。このようなサイバー攻撃リスクに備えるために、サイバーセキュリティ対応を定めた BCP が必要となるのです。

サイバーセキュリティ対応のBCPを策定する際のポイント

サイバーセキュリティ対応の BCP の基本的な策定方法は、通常のものと同じです。
ランサムウェア感染等のサイバー攻撃被害を受けた状況を想定し、その状況が発生した時の計画を作っていきます。

なお、作成する際、以下の３つのポイントに注意してください。

（１）オフラインバックアップの確保

ランサムウェア攻撃では、オンラインのバックアップも暗号化され、利用できなくなる可能性があります。
そのため、必ず定期的に重要なデータをオフライン環境（外付け HDD など）に保存するようにしましょう。
参考記事：「3-2-1 ルール」【3 分でわかる！用語解説】

（２）守るべき情報資産の最適化

管理するシステムやデータ量は必要最低限に絞りましょう。保護すべきデータを厳選し、最適化することで、守りやすく、復旧しやすくなり、リスク軽減にもつながります。
例えば、小容量データ（4GB 以下）であれば、DVD へのバックアップも可能です。この機会に情報資産を整理し、不要なデータの削除を検討しましょう。

（３）作成した BCP の実現性の確認と見直し

どれだけ優れた BCP を作成しても、実際に行動できなければ意味がありません。
実現性を確保するために定期的な訓練やシミュレーションを行い、計画に無理がないことを確認しましょう。また、訓練の結果を基に問題があれば改善することも大切です。

最後に

BCP は企業を守るためのものですが、それだけではありません。BCP の存在により、取引先や顧客を守り、ひいては社会全体への影響を最小限に抑えることにもつながります。
しかし、日本国内の中小企業における BCP 策定率は、まだ 15%程度にとどまっており、多くの企業が未対策となっているのが現状です。
皆さんの会社、お客様を守るためにも、ぜひ BCP の策定を考えてみてください。

中小企業サイバーセキュリティ特別支援事業の紹介

今年度、東京都ではインシデント対応に特化した中小企業向けの支援を行っています。
この事業では、基本的なセキュリティ対策を実施済みの企業を対象に、インシデント対応体制の強化を目的として、IT-BCP の策定または CSIRT の構築を支援します。

今後、本事業参加企業の取組内容をホームページ上で公開する予定です。
皆様と同業種、同規模、同じお悩みを抱えた企業の取組事例は、参考になるのではないかと思います。
2 月下旬公開予定ですので、事業内容とともにぜひご覧ください。



事業 URL：令和 6 年度 中小企業サイバーセキュリティ特別支援事業

参考文献

1. 中小企業 BCP 策定運用指針　（中小企業庁）
   https://www.chusho.meti.go.jp/bcp/index.html
2. サイバー空間をめぐる脅威の情勢等　（警察庁 Web サイト）
   https://www.npa.go.jp/publications/statistics/cybersecurity/index.html
3. プロが教える！中小企業のための BCP 対策（BCPP）
   https://www.bcp-perfect.com/

一般向け 2_#19_「サポート詐欺」
掲載日：2025/2/14



サイバーセキュリティの基本を理解するためには、いくつか重要なセキュリティ用語を知っておくことが必要です。
これらの言葉や概念を正確に理解することで、企業が直面するリスクを最小限に抑え、適切な対策を講じることができます。
本記事では、中小企業が特に知っておくべきセキュリティ用語について解説しています。

今回のテーマは、「サポート詐欺」です。

サポート詐欺とは

サポート詐欺とは、パソコンやスマートフォンを使用している時に、突如表示される「ウイルスに感染しました」という内容の偽の警告画面を通じて恐怖心を煽り、サポート窓口を装い金銭を搾取しようとする悪質な詐欺の手口です。
以前はパソコンユーザーが主な標的とされていましたが、最近ではスマートフォンの普及に伴い、スマホユー

ザーも標的とされ、被害に遭うケースが増えています。

サポート詐欺の手口

サポート詐欺には、いくつかの手口があります。
どの手口も、利用者を不安にさせ、サポートの名目で金銭をだまし取ろうとする点は変わりません。
サポート詐欺に引っかからないためには、手口を知っておくことが重要です。

警告画面等に表示されている電話番号に電話をかけること、記載されているリンクをクリックすることは絶対にしないようにしてください。

（１）Web ページを使った手口

Web ページにポップアップなどを仕込む手法があります。これにより、あたかも「ウイルス感染」したように見せかけ、ユーザーを偽のサポート窓口へ誘導したり、遠隔操作ソフトをインストールさせたりするものです。

【手口１：偽のポップアップ】
ページを開くと、「あなたの PC はウイルスに感染しました」「個人情報が漏えいしています」などのポップアップ画面が表示されます。警告音が鳴る場合もあります。
このポップアップ画面には、偽のサポート窓口の電話・メールアドレス、偽アプリのリンクなどが記載されています。

【手口２：　操作不能の偽メッセージ】
ページを開くとポップアップ画面が最大化され、通常の操作ができなくなります。表示される画面には、偽のサポート窓口の電話・メールアドレスなどが記載されています。
操作不能を解除する方法は、過去の手口では単純に ESC キーの長押しなど、簡単なものでしたが、最近では電源の再起動が必要となる場合もあります。
解除手順は独立行政法人情報処理推進機構(IPA)のホームページの「サポート詐欺で表示される偽のセキュリティ警告画面の閉じ方」で確認できます。

（２）偽の企業 Web サイトへ誘導する手口

Microsoft や Apple など、実在する企業の Web サイトに似せた偽の Web サイトを作成し、そこに偽

のサポート窓口の情報を掲載します。
この偽サイトへの広告を検索エンジンに表示させ、ユーザーを騙し、偽のサポート窓口へ誘導する手口です。

（３）フィッシングメールや SMS を使う手口

フィッシングメールや SMS を使った手口も一般的です。偽のメールや SMS を送り、その中に記載されたリンクをクリックさせることによって、偽のサポートサイトに誘導する手口です。
この手口では、「ウイルス感染」や「ID の乗っ取り」といった内容に加え、「Windows の更新が必要です」「ドライバーの更新が必要です」などのソフトやアプリの更新通知を装うこともあります。

サポート詐欺の被害に遭った事例や実際の警告画面をこちらの記事で紹介しています。
あわせてご参照ください。
・参考記事：サポート詐欺の脅威

サポート詐欺への対応方法

ウイルス感染した際の通知は、自身が導入したウイルス対策ソフトや OS（Windows や Android/iOS など）からしか来ません。
それ以外からのウイルス感染の通知は、すべて偽物です。無視することが基本的対策になります。

ただし、フィッシングメールや SMS などで「ID の乗っ取り」が示唆されたり、気になる場合は、使用しているサービスの公式の連絡先に直接問い合わせてください。
その際、メールに記載された連絡先ではなく、公式アプリや公式サイトから確認した正しい連絡先を利用してください。
もし不安が続くような場合には、一人で悩まず、消費生活センターや警察、あるいは専門の相談窓口に相談することも検討してください。

まとめ

サポート詐欺は、セキュリティ知識や IT リテラシーが不足している人々を狙った犯罪です。
これらを防ぐには、個々がセキュリティ知識や IT リテラシーを高めることが不可欠であり、その結果、そのほかのサイバーセキュリティの脅威も回避することが可能となります。
ぜひ、本記事や下記の動画を活用して、知識を深める一助としてください。

・手口検証動画シリーズ ： 独立行政法人 情報処理推進機構（IPA）
・髭男爵さんによるサイバーセキュリティ啓発漫才　（警視庁）（2025/2/14 時点）

参考文献

1. サポート詐欺対策｜警察庁 Web サイト
   https://www.npa.go.jp/bureau/cyber/countermeasures/support-fraud.html
2. サポート詐欺とは？ | 国民のためのサイバーセキュリティサイト（総務省）
   https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/basic/risk/06/
3. パソコンに偽のウイルス感染警告を表示させるサポート詐欺に注意 | 情報セキュリティ | 独立行政法人 情報処理推進機構（IPA）
   https://www.ipa.go.jp/security/anshin/attention/2024/mgdayori20241119.html
4. そのセキュリティ警告画面・警告音は偽物です！「サポート詐欺」にご注意！！－電話をかけない！電子マネーやクレジットカードで料金を支払わない！－(発表情報)_国民生活センター
   https://www.kokusen.go.jp/news/data/n-20220224_2.html
5. パソコンで警告が出たらサポート詐欺に注意！－70 歳以上で大幅に増加－(発表情報)_国民生活センター
   https://www.kokusen.go.jp/news/data/n-20240327_1.html

一般向け 2_#20_「多層防御」
掲載日：2025/2/21



サイバーセキュリティの基本を理解するためには、いくつか重要なセキュリティ用語を知っておくことが必要です。
これらの言葉や概念を正確に理解することで、企業が直面するリスクを最小限に抑え、適切な対策を講じることができます。
本記事では、中小企業が特に知っておくべきセキュリティ用語について解説しています。

本年度の用語解説の記事は今回が最終回です。最終回となる今回は、新しいセキュリティ対策の考え方である「多層防御」を紹介します。

多層防御とは

多層防御は、多様化するサイバー攻撃に対して、企業や組織のシステムを「入口」「内部」「出口」の３つの主要な領域に分け、それぞれに対策を講じる考え方です。

従来のサイバーセキュリティ対策の基本は、境界防御と呼ばれるものでした。
境界防御は、社内ネットワークを安全な領域、社外インターネット空間を危険な領域とし、危険な領域からの脅威を防ぐために、ウイルス対策ソフトやファイアウォールなどを利用してネットワークの境界線上で脅威を遮断することに焦点を当てていました。

しかしながら、この考え方には課題がありました。
ウイルスなどの脅威が一度社内ネットワーク内部に侵入してしまうと、その後の対策に乏しく、これが大きな弱点となっていました。
さらに、近年のサイバー攻撃は、「ゼロデイ攻撃」や「標的型攻撃メール」など、従来の境界線防御モデルでは侵入を防ぐことが困難なものが増えています。

この課題を解決する方法として、「ゼロトラスト」や「多層防御」という新しい考え方が打ち出されています。

ゼロトラストは、従来のネットワーク環境の境界の概念を捨て去り、大切な情報資産にアクセスするものはすべて信用できないものとして捉え、すべてのアクセスを検証するという考え方です。
ゼロトラストに対応するシステムは、入口でそのアクセスの可否を検証します。

一方、多層防御は企業システムやネットワークに複数の防御層を設ける考え方で、様々な階層（レイヤー）でセキュリティ対策を行います。
例えば、「社内に入る通信」「内部での活動」「社外へ出てゆく通信」をそれぞれ確認することにより、たとえ入口が突破されても、「内部」や「出口」で追加のセキュリティチェックを行うことで、多層的にシステムを守ることが可能になります。

多層防御における主な対策

多層防御では、主に、「入口」「内部」「出口」の３つの領域それぞれに特化した対策を行います。

（１）入口対策

社内ネットワークへの脅威の侵入を防ぐことに重点を置く対策です。
ファイアウォールまたは UTM（Unified Threat Management）、ウイルス対策ソフトなどの導入が該当します。

（２）内部対策

脅威が侵入してしまった場合に、その拡大を阻止することを目的とした対策です。
アクセス制御（ID 等によるデータやシステムの使用を制限する仕組み）の導入・設定、ログの監視もしくは監視ツールの実装、EDR（Endpoint Detection and Response）や暗号化ツールの導入等が該当します。

（３）出口対策

企業の重要情報や個人情報が外部に漏えいするのを防ぐための対策です。
プロキシサーバー(インターネット接続を中継する装置。不適切な接続の遮断、ユーザーの IP アドレスの隠蔽を行う)の導入や、WAF（Web Application Firewall：Web サイト向けのファイアウォール）の設置等が該当します。

多層防御のメリットとデメリット

多層防御では、防御する階層に合わせて様々なセキュリティ対策ツールを導入します。
複数のツールで防御することにより、企業にとって様々なメリットが見込めますが、デメリットもあるので注意が必要です。

（１）メリット

システムおよびネットワーク全体を様々なツールで監視するため、次のようなセキュリティリスクを低減するメリットがあります。

・マルウェア感染リスクの低減
・不正アクセスの早期検知と確度の向上
・被害の最小化

（２）デメリット

一方で、導入には次のようなデメリットになりうる部分もあります。

・複数の導入ツール、機器によるコスト増大
・管理の複雑化
・運用負荷の増大

まとめ

多層防御は、現在のサイバー環境におけるリスクの軽減と、被害を最小限に抑えるための最も有効的な対策の一つです。
しかし、実装や運用のコストが大きいという課題もあります。
「守るべきもの」と「どのように守るか」を明確に定めてから、仕組みを構築することが重要です。

なお、基本的なセキュリティ対策（ウイルス対策ソフトの導入、セキュリティパッチ等の即時適用、従業員への教育など）は、多層防御の土台となります。
土台となる基本のセキュリティ対策に、企業独自の対策を加えることによって、もう一段高いセキュリティレベルを実現してください。

参考文献

1. 多層防御とは？特徴や多重防御との違い、セキュリティ攻撃対策として有効な BDAP を解説！ | ドコモビジネス | NTT コミュニケーションズ 法人のお客さま
   https://www.ntt.com/business/services/xmanaged/lp/column/defense-in-depth.html
2. ICS-CERT：多層防御による制御システムセキュリティの強化 概要 （IPA 訳） 独立行政法人情報処理推進機構（IPA）
   https://www.ipa.go.jp/security/controlsystem/ssf7ph0000004ej5-att/000055601.pdf