# 中小企業のための
# 情報セキュリティ
# ハンドブック


株式会社GatewayLink

# 目　次

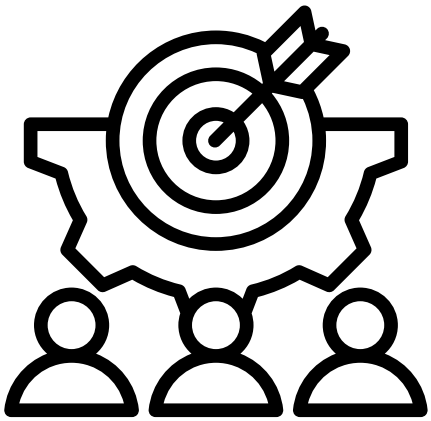
# はじめに

## 情報せキュリティ対策は、とても重要な経営課題です

近年、日本の企業や団体、医療機関などに対するサイバー攻撃による被害が、かつてないほど多く発生しています。
その手口は様々ですが、個人情報の搾取や、データやWebページの改ざんなどの被害が多く、それをもとに金銭を要求してくるランサムウェア（身代金要求型）攻撃も流行しています。
そのような被害に遭ってしまうと、復旧までに非常に多くの時間とお金がかかり、最悪の場合は事業継続不能な状態に陥ってしまうケースもございます。
また、情報セキュリティ対策が不十分な状態でサイバー攻撃を受け第三者に経済的損失を与えてしまった場合の経営者の責任は非常に重く、取締役が個人で賠償責任を負わなければならないリスクが、民法や会社法に定められています。
こうした事を踏まえ、サイバー攻撃による被害を極力抑えるための情報セキュリティ対策は、会社の規模や個人情報の有無にかかわらず、とても重要な経営課題といえます。

## 本ハンドブックの目的

中小企業の経営者の中には、「うちみたいな小さな会社は狙われない」「個人情報が無いから大丈夫」などと安穏とした考えをお持ちの方も少なくありません。
しかし警察庁のデータによると、令和5年に実際に発生したランサムウェア被害（身代金要求型の攻撃）では、被害全体の52%が中小企業となっています。
本ハンドブックの目的は、一人でも多くの経営者に日本に対するサイバー攻撃の現状を知っていただいた上で情報セキュリティ対策をすることの重要性を認識していただき、実際に対策をしていただく事で中小企業のサイバー攻撃による被害を1件でも多く減らすことにあります。
実際に情報セキュリティ対策をする場合、決して安くはない費用がかかることも事実です。また投資と違って新たな収益を生むものでもありません。しかし、サイバー攻撃による被害額に比べればほんのわずかな費用ですし、情報セキュリティ対策をしっかり取り組んでることで企業価値の向上も期待できます。
本ハンドブックをぜひ最後までご覧いただき、情報セキュリティ対策についてご参考にしていただければ幸いです。



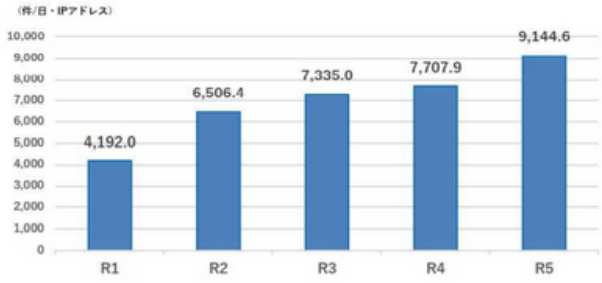
# 第一部　サイバー攻撃の現状

「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）より

## 脆弱性探索の攻撃は、9.4秒に１回！

攻撃者は、インターネット上の脆弱性のある機器を探索するために、不特定多数のIPアドレスに対し無差別に通信パケットを送信しています。このような脆弱性探索攻撃の件数は、1日１IPアドレスあたり、令和4年では7,707.9件（約11.2秒に１回）、令和５年では9,144.6件（約9.4秒に１回）と、脅威的な件数となっており、平成23年以降増加の一途をたどっています。
わかりやすく例えると、ドロボーが空き巣を狙ってドアノブをガチャガチャして回っているイメージで、鍵が空いていると侵入されてしまいます。9.4秒に一度の頻度でドアノブをガチャガチャされたら、気持ち悪いですよね。
増加の要員としてはIoT機器の普及などで攻撃対象が増加していることなどが挙げられます。
パソコンやIoT機器のアップデート情報が公開された際は、なるべく早くアップデートをすることをお勧めします。これを怠ると、公開されている脆弱性を突いて攻撃を受けてしまうことにつながります。

警察庁ではインターネット上に空っぽのサーバーを設置し、そこに対して送信される脆弱性探索のパケットを観測しています。（空っぽなので、本来であれば誰もアクセスしてくるはずのないサーバーでの観測です。）
こうして検知したアクセス件数の推移は、右のグラフの通りです。

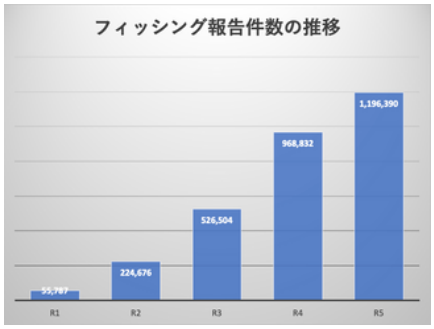



## 増え続けるフィッシング行為

フィッシングとは、実在する企業や団体を装って、メールやSNS、ショートメッセージなどから偽サイトへ誘導し、IDやパスワード、クレジットカード情報を入力させて搾取する行為をいいます。


フィッシング対策協議会（https://www.antiphishing.jp/）に寄せられたフィッシング件数は年々増加傾向にあり、令和4年では968,832件、令和5年では1,196,390件でした。
この数字はあくまでもフィッシング対策協議会に情報が寄せられた件数であり、情報提供されない件数を想像すると、少なく見積もっても上記数字の100倍以上はあるのではないかと推察します。

最近では、金融機関を装ったパスワードの再確認要請や、レンタルサーバー会社を装ったドメインの期限切れに伴うクレジットカード情報の入力要請、宅配業者になりすましたクレジットカード情報の入力要請などの手口が増えています。



# フィッシングサイトの具体例

下記は、実際にメールで送られてきたフィッシングの例です。
さくらサーバーを装ったもので、「お客様のサービスは2日後に期限切れとなります」と記載があり、受信者を焦らせる意図が伺えます。
送信元メールアドレスのドメインを見ると、さくらサーバーとは全く関係のなさそうなドメインだったため、このメールの受信者は偽物ではないかと疑ったようです。


さらに「コントロールパネルにログインする」をクリックしたところ、下記ページに飛んだそうです。
ロゴマークや企業情報へのリンクなどは本物と同じなので巧妙に作られてはいますが、ログインID/パスワードの画面が無く、いきなりクレジット情報の入力画面だったので、偽物だと確信したようです。

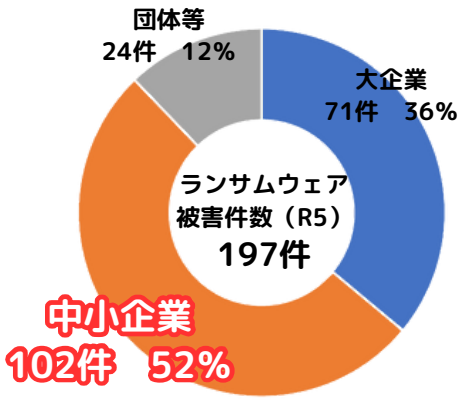

このケースは、単純にクレジット情報を盗み取る目的のフィッシングです。
少しでも「あやしい」と感じたら、情報を入力する前に、メールアドレスやURLのドメイン（今回の場合はメール送信元のドメインは「workiz.com」です）をよく見てみましょう。ドメインの持ち主が誰なのかは、Whois検索で確認できる場合があります。
ブラウザの検索画面に「Whois」と入力すると、複数のWhois検索サイトが出てきますので、試してみてください。

# ランサムウェアの被害状況

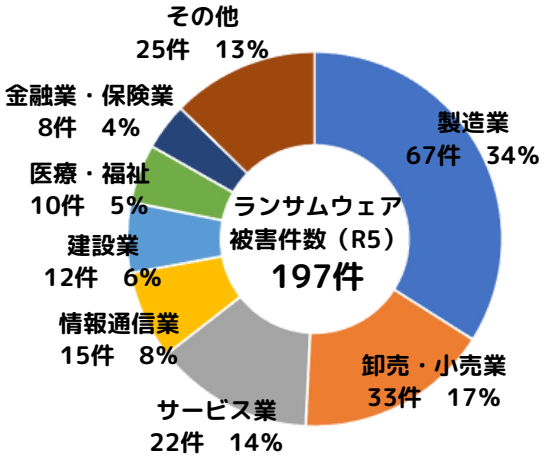
令和5年に警察庁で把握したランサムウェア（身代金要求型の攻撃）による被害件数は、197件でした。この数字は少ないように感じるかもしれませんが、恐らく警察庁で把握していない事案が相当数あるものと推察されます。

また197件のうち52%にあたる102件が中小企業でした。
サイバー攻撃というと、大企業が標的にされているイメージをお持ちの方が多いかと存じますが、決してそんな事はなく、攻撃者は対象企業の事業規模の大小や業種に関わらず攻撃を仕掛けてきています。

＜規模別＞

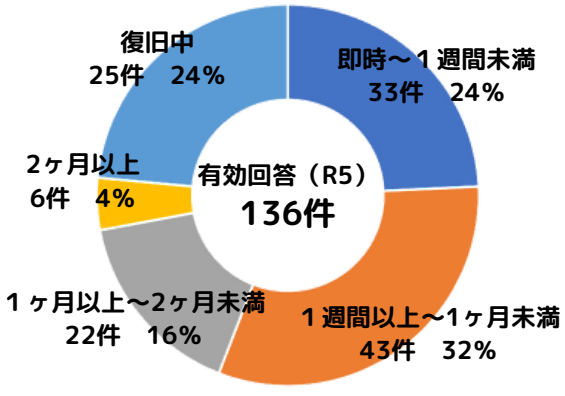



＜業種別＞

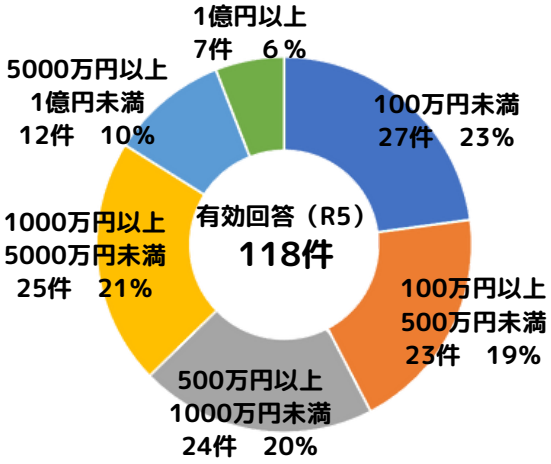



また、被害にあってから復旧に至るまでに要した費用は、全体の57%で500万円以上、47%で1000万円以上となっており、経済損失の大きさが伺えます。
また、復旧までの期間も、１週間以内で復旧できたのはわずか24%しかおらず、44%で1ヶ月以上を要しています。この間はほぼ通常業務が出来ていなかったものと思われ、取引先からの信用失墜や従業員の精神的ダメージにつながってしまったケースもあるのではないかと推察いたします。

＜復旧に要した期間＞




＜復旧に要した費用＞

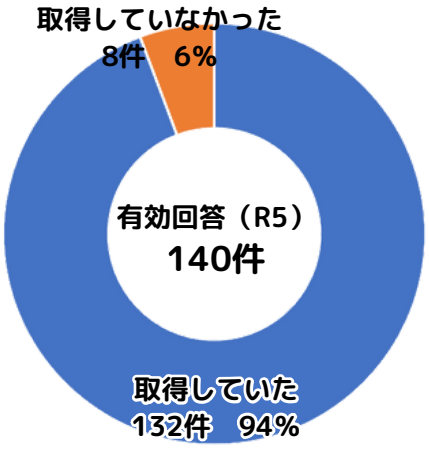


# バックアップから復旧できない！

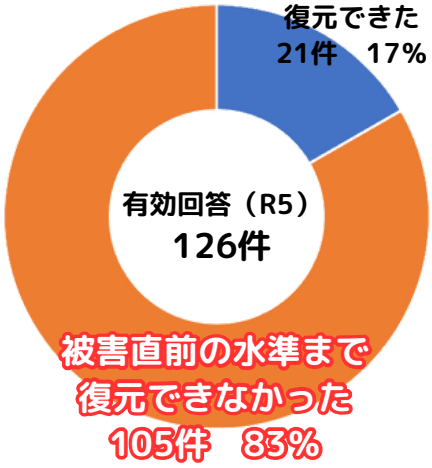
令和5年にランサムウェア（身代金要求型の攻撃）被害を受けた企業・団体へのデータのバックアップに関するアンケートでは、94%でバックアップを取得していたと回答していますが、そのバックアップからデータを復旧できたと回答したのは、わずか17%でした。
バックアップを取得していたにも関わらず、83%で完全には復旧ができなかったと回答しています。

パソコンや社内にあるファイルサーバーのバックアップというと、HDD（ハードディスクドライブ）の故障に対応するため、というイメージが強いかと存じます。HDDは磁気ディスクが高速回転している記録装置で、いつか必ず故障しますので、この考えは正しいと言えます。
しかし、上記のようなアンケート結果からも分かる通り、想定するリスクはHDDの故障だけでは不十分で、サイバー攻撃によるデータの改ざんや暗号化にも対応できるバックアップでなければならないことを示しています。

＜バックアップの有無＞




＜バックアップからの復元状況＞




大切なデータが失われると、どうなるでしょう？
請求データ、納品予定のデータ、顧客情報、これらの情報が失われてしまうと、営業活動ができなくなる恐れがある事は容易に想像できるでしょう。

また、大切なデータはクラウド上のストレージに保存しているから大丈夫だ、と考えている方も多くいらっしゃいますが、これは大きな間違いです。
もちろん、クラウドサーバーを運営している企業は、サーバー自体への直接攻撃にはしっかり備えをしていると思われますが、クラウドサーバーにアクセスしている社内のPCが乗っ取られてしまったとしたらどうでしょう？
クラウドサーバーにアクセスするためのID/パスワードの文字列は、簡単に盗まれてしまうであろう事はご理解いただけるかと存じます。そしてクラウド上のデータの改ざんや暗号化、搾取などにつながってしまう恐れがあるのです。

大切なデータがどこに保存してあるのかに関わらず、サイバー攻撃を意識したバックアップ対策は必須であると言えます。

# 第二部　経営者の責任

## サイバー攻撃により被る不利益

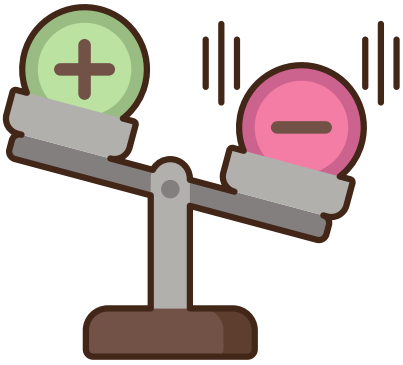
AI技術の発展により、IT分野の発展はさらに加速感が出てきましたが、これらを利用したり依存したりする範囲もどんどん広がっています。
こうした中で情報セキュリティ対策が十分ではなく、サイバー攻撃を受けてしまった場合、大きく分けて下記のような不利益が考えられます。

- **経済的不利益**
  （調査復旧費用、顧客対応費用、裁判費用、弁護士費用、逸失利益、など）

- **信用失墜**
  （顧客へ損害を与えてしまう、今後の取引継続が危うくなる、訴訟に発展）

- **従業員への悪影響**
  （職場環境の悪化、離職リスク、内部不正リスク）

- **事業継続不能**
  （長期にわたる業務停滞、資金ショート）



こうした不利益を被るリスクを極力減らすために、経営者は社内の情報セキュリティ対策について担当部署や外部ベンダーに任せるだけでなく、率先して取り組むリーダーでなければなりません。

## 内部不正リスク

社内で保有している重要な情報（顧客情報、機密情報）の取り扱いに関するルールを定めていますか？
システム的にこうした情報を簡単に外部に持ち出せる状態で、且つルールも策定されていない環境だとしたら、従業員のモラル低下などによる情報漏洩リスクを考えなければならないでしょう。
どんなに善良そうに見える人でも「魔が刺す」ということもありますので、「この人なら大丈夫」「うちの社員はみんな真面目だから」は危険です。
経営者が先頭に立ち、重要情報の取り扱いルールを定めて従業員に根付かせることは、不正をしようという気持ちを起こさせない抑止効果が期待できます。
サイバー攻撃だけではなく内部不正リスクの低減に努めるのも、経営者の重要な役割です。

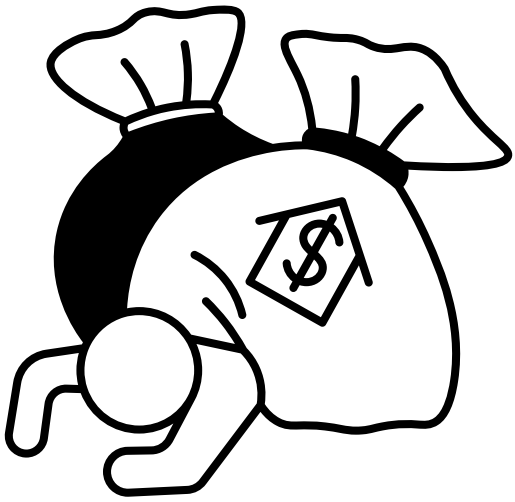
# 取締役の法的責任

独立行政法人情報処理推進機構セキュリティセンターが公開している「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」（https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf）には下記のような表が掲載されています。

| 法令 | 条項 | 要約 |
|---|---|---|
| 民法 | 第415条 債務不履行による損害賠償責任 | サイバー攻撃により仕事が停滞した場合、会社及び第三者に対する、契約違反による賠償責任を負う。 |
| | 第644条 取締役の善管注意義務違反 | 企業のセキュリティ体制が規模や業務内容に鑑みて適切ではなく、サイバー攻撃により企業や第三者に損害が発生した場合、**取締役は**会社に対して、善管注意義務違反による賠償義務を負う。 |
| | 第562条 契約不適合責任 | 請負契約の仕事の奥的物（開発システムなど）について、その種類や品質が契約内容に適合しないことが仕事の完成後に判明した場合、会社及び第三者に対する契約不適合となる。 |
| | 第709条 不法行為による賠償責任<br>第715条 使用者等の責任 | 故意または過失によって他人の権利又は法律上保護される利益を侵害した者は、これによって生じた損害を賠償する義務を負う。 |
| 会社法 | 第330条 取締役の善管注意義務違反<br>第423条第1項 任務懈怠による損害賠償責任<br>第429条第1項 第三者に対する注意義務違反 | 企業のセキュリティ体制が規模や業務内容に鑑みて適切ではなく、サイバー攻撃により企業や第三者に損害が発生した場合、**取締役は**会社に対して、善管注意義務違反による任務懈怠（けたい）に基づく損害賠償義務を負う。 |

※ 上記表を掲載している資料は2023年4月26日改訂が最新版ですが、民法は2024年4月1日施行が最新、会社法は2024年5月22日施行が最新のため、一部条項番号が異なっている場合があります。（2024年10月1日現在）

赤の色付けは本ハンドブックによるものですが、これによると、情報セキュリティ対策が不十分な状態でサイバー攻撃により第三者に損害が発生した場合、取締役（会社法の423条第1項には「取締役、会計参与、監査役、執行役又は会計監査人（以下この節において「役員等」という。）」と記載されています）が会社に対して、個人で賠償責任を負うことが定められているようです。
また、損害保険業界からの情報によると、この賠償責任は相続対象になるとのことです。これは会社役員等にとっては非常に重い責任といえます。
つまり、会社の規模や業務内容に鑑みて適切な情報セキュリティ対策を講じることは避けて通れない課題であると言えるでしょう。



# 第三部　情報セキュリティ対策（ネットワーク編）

## ネットワークセキュリティの重要性

ここまで読み進めていただいた経営者の方であれば、情報セキュリティ対策の必要性と重要性はご理解いただけたかと思います。

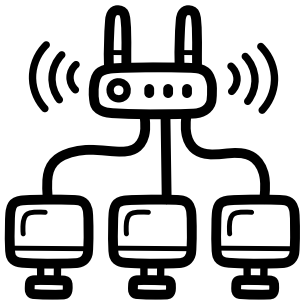
情報セキュリティ対策には大きく分けて下記の２つがあります。

**１、システムセキュリティ**
**２、ネットワークセキュリティ**

システムセキュリティは特定の業務に使用するシステムにセキュリティ機能を組み込んで動作を監視するものですが、ネットワークセキュリティは社内ネットワーク全体を監視し異常を検知する物になります。

**＜システムセキュリティ＞**
**特定のシステムの中を監視**

**＜ネットワークセキュリティ＞**
**ネットワーク全体を監視**



例えば、医療機関が使う電子カルテシステムなどでは、情報漏洩を防止するセキュリティ機能が組み込まれているのが一般的ですが、ネットワーク全体を監視する物ではないため、電子カルテを使用しない端末（PC以外にも様々なIoT機器があります）は監視の対象外となります。

大阪急性期・総合医療センターで令和4年10月31日早朝に発生したサイバー攻撃では、まず給食事業者が情報基盤構築事業者と結んでいたVPNの脆弱性を用いて侵入され、給食事業者の端末から搾取した病院のサーバーの認証情報（ID/パスワード）から病院給食サーバーに侵入されています。各サーバーのID/パスワードが同じ文字列だったこともあり、他のサーバーや電子カルテシステム、基幹システムなどに容易に侵入されてしまい、最終的に各サーバーをランサムウェアに感染させ院内端末が正常動作しない状態に陥らせてから身代金を要求しています。（大阪急性期・総合医療センター「情報セキュリティインシデント調査委員会報告書」より）

このケースの場合、電子カルテ端末のセキュリティシステムだけでは防ぎようが無く、給食事業者と情報基盤構築事業者との間のVPNの脆弱性への対策ができていなかった事が大元の原因となっています。
情報基盤事業者、給食事業者、病院の３者がそれぞれがネットワークへの不正侵入などを検知するためのネットワークセキュリティ対策をしっかり行っていたら、もっと早い段階で異常を検知して対策ができたかもしれません。

特定の端末や特定のシステムを保護する情報セキュリティ対策ももちろん重要ですが、ネットワーク全体を考えたネットワークセキュリティは、とても重要な対策です。

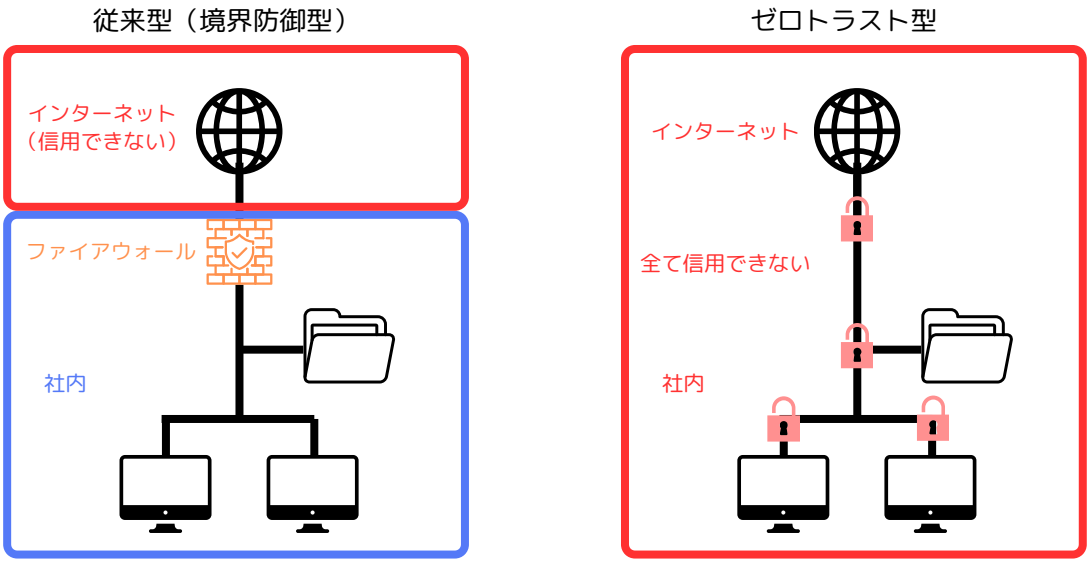
# 従来型（境界型）とゼロトラスト型

ネットワークセキュリティ対策は、「従来型（境界型）」と「ゼロトラスト型」の二つに大別されます。

従来型（境界型）のネットワークセキュリティとは、社内ネットワークと外部ネットワークとの境界を明確にして、社内ネットワークを保護する手法です。具体的にはネットワークの出入り口部分にファイアウォールなどのセキュリティ機器を設置するなどです。

一方、ゼロトラスト型とは、内部か外部かに関わらず全ての機器を信用しない、という考えに基づいた対策になります。具体的にはEDRなどを用いて全ての端末を監視、不正な動きを検知し管理者に通知、不正ファイルを封じ込めて復旧させる、といった対応です。

従来型とゼロトラスト型の大きな違いは、従来型は不正侵入やマルウェア感染を予防することに重点を置いているのに対し、ゼロトラスト型は不正侵入やマルウェア感染がある前提でその後の封じ込めや感染拡大に重点をおいている点です。
また従来型にくらべてゼロトラスト型は費用面で高額になるケースが多く、中小企業向けには従来型のほうが導入しやすい傾向にあります。



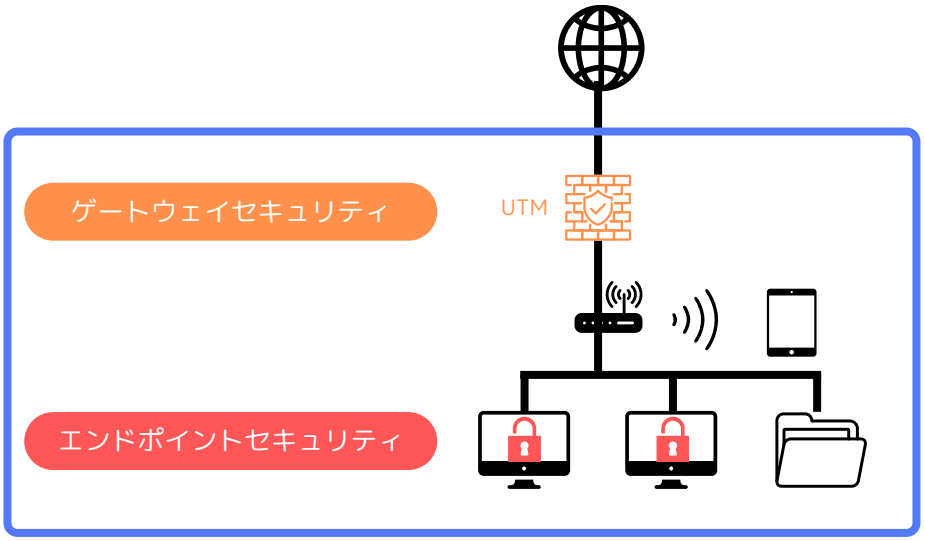

| | 従来型（境界防御型） | ゼロトラスト型 |
|---|---|---|
| 主な考え方 | 不正侵入やマルウェア感染を予防する。 | 不正侵入やマルウェア感染後の被害拡大を予防する。 |
| コスト | 比較的安価で道入しやすい（中小企業向け） | 比較的高額になりやすい（中堅以上の企業向け） |
| 機能面 | 運用面までサポートしてくれるベンダーがいれば、管理はしやすい。 | 運用面は基本的に自社で管理だが、サポートをするベンダーもあり。 |

# ゲートウェイセキュリティとエンドポイントセキュリティ

コスト面や運用のしやすさなどから、中小企業向けの具体的な対策としては、「ゲートウェイセキュリティ」と「エンドポイントセキュリティ」があります。

**＜ゲートウェイセキュリティ＞**
ネットワークの出入り口（ゲートウェイ）をしっかり固めてネットワーク全体をガードする手法。
ルーターのファイアウォール機能だけでは不十分なため、UTMを設置するのが望ましいです。
UTMとは、Unified Threat Managementの略で、日本語では統合型脅威管理と訳されます。一つのUTM端末に複数のセキュリティ機能が搭載された機器で、不正アクセスやフィッシングなど、様々な脅威に対応することができます。

**＜エンドポイントセキュリティ＞**
いわゆるアンチウィルスソフトのことで、EPP（End Point Platform）とも呼ばれます。
エンドポイントセキュリティの役割は、インストールし端末への不正アクセスの防御、マルウェア感染の予防、感染したマルウェアの駆除になります。




| | **ゲートウェイセキュリティ**<br>（UTM） | **エンドポイントセキュリティ**<br>（アンチウィルスソフト） |
|---|---|---|
| 主な役割 | **配下のネットワーク全体を保護**<br><br>外部からの不正侵入をガード<br>情報の不正持ち出しをブロック<br>フィッシングサイトをブロック<br>配下の端末を監視<br>配下端末のマルウェア感染を検知 | **インストールした端末だけを保護**<br><br>不正侵入の予防<br>マルウェア感染の予防<br>マルウェアの感染を検知<br>感染したマルウェアを無害化 |

**【重要】**
**ゲートウェイセキュリティ（UTM）とエンドポイントセキュリティ（アンチウィルスソフト）は、いずれか一方だけでは不十分で、両方を導入して初めて強固な情報セキュリティ対策となります。**
**また、しっかりした運用、特にSOC対応が非常に重要になります。事項でSOC対応について詳しく紹介いたします。**

## SOC対応の重要性

SOCとは、Security Operation Centerの略で、情報セキュリティ対策を専門的に扱う組織や部門のことで、ネットワーク全体の監視や、サイバーインシデントの予防・早期発見・速やかな対応などが主な役割となります。
専門的な知識や技術、経験が必要なため、中小企業が専門の人員を雇用することは難しく、アウトソースすることが賢明であるといえます。

**そしてこのSOCこそが、情報セキュリティ対策で最も重要な部分です。**
どれだけ高価な機器やソフトウェアを導入しても、有事の際にそれを適切に運用できなければ意味がありません。

## SOC対応がなかったら・・・

例えばランサムウェア被害の場合、最初の感染から身代金要求まで、約４～６ヶ月のリードタイムがあると言われています。
この間に攻撃者は、大量の個人情報や機密文書などお金になりそうな情報はあるか？、ID/パスワードの文字列は何か？売上や利益の規模はどれくらいか？などを徹底的に調べた上で、適切な身代金の要求金額の上限（相手が支払ってくれそうな金額の上限）はいくらなのか？を算定しているとされています。
（身代金は、米ドルやビットコインなどの仮想通貨で要求されるケースがほとんどです。）

しかし、SOC対応により感染初期の段階で対処することができれば、重大インシデントに発展するリスクを大幅に低減できるのです。


**UTMなどのセキュリティ機器を導入する際は、アラート機能を活用したSOC対応をしてくれるベンダーなのかどうかをしっかり確認することがとても重要です。**

（大変残念なことに、納品後のサポートや保守は一切しないというベンダーが多く存在していますので注意が必要です。）

# 情報セキュリティ製品を選ぶポイント

ここでは主にUTMを選ぶ際のポイントをご紹介します。また、失敗例も記載しますので、ぜひご参考にしてみてください。

**・必要十分なスペックか？**
UTMには各メーカーごとに機種のラインナップがいくつかあります。例えばパソコン端末数30台まで、50台まで、100台まで、といった感じです。
社員が20名程度しかいないのに、パソコン100台まで対応可能な機種を購入させられた例などもありますので、カタログなどを良く見て確認する必要があります。

**・セキュリティレポートは定期的にもらえるか？**
定期的なLog情報のレポートをもらえないベンダーは、そもそも納品後の保守をする気が無い、または保守が出来ないケースがあります。メーカーによっては、高度な専門知識がある人が見ないとわからないLogデータしか出てこないものもあり、技術者がいないベンダーでは保守は難しいでしょう。最低でも月に1度のレポートを出してくれるかどうか、その内容について説明を受けられるかどうか、確認をしたほうがい良いでしょう。

**・エンドポイントのセキュリティのライセンスは管理してくれるか？**
アンチウィルスソフトは、パソコンごとの導入時期によってライセンスが切れるタイミングがバラバラになりがちです。中小企業の場合、これを自社で一元管理している会社は少なく、ライセンス切れに気づかすに感染してしまうケースが多発しています。販売ベンダー側で一元的にライセンス管理をしてくれるとかなり安心ですね。

**失敗例１　ライセンスが揃っていなかった**
UTMを購入する際、A社の見積もりは80万円だったが、B社は30万円以下だった。A社は暴利だと思いB社と契約をしたが、のちにC社の営業担当に確認をしてもらったところ、７種類あるセキュリティライセンスのうち、ファイアウォールのみが有効で、残り６種類はライセンス料未払いで機能無効になっていた。
→ **このケースは、極端に安いB社の見積もりが、そもそもファイアウォールのセキュリティライセンスしか入っていなかった例です。UTMは一般的に5年間のセキュリティライセンス付きで、安いものでも50万円程はします。ファイアウォールのみ有効では、一般的なルーターのファイアウォール機能を使っているのと何ら代わりはありませんおで、全く無駄な買い物だったと言えます。契約者に専門知識が無いことに漬け込んだ、かなり悪質な例です。**

**失敗例２　保守をしてくれない**
UTMを購入してからしばらくの間は何事もなかったのですが、ある時パソコンのアンチウィルスソフトがアラートを表示したことで、ウィルス感染に気づきました。UTMで検知しなかったのか？と疑問に思い、販売業社に保守を依頼したところ、保守は契約に含まれていないと断られてしまった。メーカーに問い合わせて見てもらったところ、検知はしていた様だがアラートメールを送信する設定が空欄になっていたとのことだった。
→ **このケースは、最初から保守をする気が無いのに販売をしている例です。UTMの保守にはそれなりの技術や経験が必要なため、このような保守をしないベンダーが少なくありません。契約の際に有事の際の保守対応の有無やアラート機能の有効化について、よく確認をする必要があります。見積もりや契約書類に「SOC対応あり」が明記されていると、より安心だと思います。**

**失敗例１　ポップアップ表示をOFFにしてしまって感染した**
アンチウィルスソフトが有料オプションの加入を勧めるポップアップを頻繁に表示するのが邪魔だったので、ポップアップ機能をOFFにして使っていたら、セキュリティライセンス更新のポップアップも出なかったためセキュリティライセンスが切れていることに気づかずに使っていたら、ウィルスに感染してしまっていた。
→ **この例は、たまたま弊社のセキュリティ診断を受けて頂いたことで判明し、すぐに対処したので重大なインシデントにはなっていませんが、、そのまま気づかずに使い続けていたら危険だった可能性があります。**

# 第四部　情報セキュリティ対策（組織運用編）

## 現実を知ろう

情報セキュリティ対策においてまず重要なのは、「リスクがある」ことをきちんと認識するための現実を知ることです。正しい情報を知らないと、「うちみたいな小さな会社は狙われない」「うちは個人情報がないから大丈夫」などの誤った考えになってしまい、適切な情報セキュリティ対策ができなくなってしまいます。
以下に、目を疑いたくなる様な現実情報をいくつか紹介します。

**情報１　高度な組織化**
数年前までのサイバー攻撃は、卓越した技術を持ったごくわずかなハッカーが行っていたが、近年は高度に組織化されたチームによる波状攻撃が主流になりつつあり、APT攻撃（持続的標的型攻撃）とも呼ばれている。
彼らは細かな分業制を敷いて組織としての攻撃を可能にしており、各現場では人事評価までしていると言われている。

**情報２　攻撃用ソフトウェアの開発**
最近では、専門知識や技術がなくても容易にサイバー攻撃を仕掛けることができるソフトウェアを開発して世界中に販売していると言われている。警視庁のある警部補は「これからは中学生でもサイバー攻撃ができる時代になるかもしれない」と漏らしていた。

**情報３　攻撃対象の変化**
かつてのサイバー攻撃は、政府機関や防衛関連企業を狙って行われることが多かったが、近年では経済界全体がターゲットになっており、あらゆる企業・団体が攻撃対象となっている。

**情報４　目的の変化**
かつてのサイバー攻撃は、自らの技術力を誇示するためのイタズラが多かったが、近年は経済界を狙った身代金要求型の攻撃（ランサムウェア攻撃）が増えている。サイバー攻撃の目的がお金を稼ぐこと、つまりビジネスになっている。

**情報５　侵入経路の急増**
OA機器や防犯カメラ、ゲーム機などネットワークに接続されるIoT端末が急速に増えている。これはサイバー攻撃を仕掛ける対象や侵入経路が増えていることに他ならない。2016年には、DDoS攻撃によりX（旧Twitter）やNetflixなど1,000社以上の企業ウェブサイトへ のアクセスが著しく阻害された。この攻撃はハッカーたちによって数十万台にもおよびぶ家庭用IoT機器悪用して行われたものだった。

**情報６　外部にもリスクが**
紙からPDFへ、FAXからメールへ、情報交換手段がどんどん電子化されていくなか、もはや自社のネットワークのセキュリティだけでは十分ではなく、顧客やベンダー、サプライヤーなどネットワークで接続された相手先が潜在的な脆弱ポイントとなりうる。

**情報７　攻撃頻度**
2024年第1四半期に世界で検知されたWebアプリケーションへのサイバー攻撃の総攻撃数は、計2億912万623件で、1日平均約220万回だった。

**情報８　相談件数**
令和5年における警察へのサイバー攻撃関連の相談件数は、2,596,188件（1日あたり7,112.8件）だった。

# 組織としての取り組み

前項では、個人や各社員がチェックすべき行動を記載しましたが、ここからは中小企業の経営者の目線で組織としての取り組みについて紹介していきます。
あくまでも中小企業が対象ですので、必要最低限の内容としています。

1、「情報セキュリティ基本方針」の作成
2、「情報セキュリティ基本方針」の周知
3、情報セキュリティ対策の実施
4、契約書類の見直し

# 「情報セキュリティ基本方針」の作成

まずは「情報セキュリティ基本方針」を作成しましょう。
決まった雛形はありませんので、自由に作成していただいて結構ですが、いくつかポイントがありますので自社に合った内容にしていきましょう。

**ポイント**

・専門用語はなるべく避けて、社員全員が理解しやすい平易な言葉で記述しましょう。
・従業員が情報セキュリティの重要性を理解して、協力しやすい内容にしましょう。
・抽象的な表現ではなく、具体的な対策を盛り込みましょう。
・事業の特徴や顧客の期待などを考慮して、自社の業務にあった内容にしましょう。
・すでに実施している情報セキュリティ対策があれば方針に盛り込みましょう。

**「情報セキュリティ基本方針」に盛り込むことの例**

1、はじめに
　・目的：情報資産を保護し、情報セキュリティ事故の発生を防止すること。
　・適用範囲：自社で取り扱うすべての情報資産および情報システムに適用する。
　・定義：情報資産、情報セキュリティ事故などの用語を定義する。
2、情報セキュリティに関する基本的な考え方
　・経営者の責任：情報セキュリティは経営者の責任であることを明記する。
　・従業員の役割：全従業員が情報セキュリティの重要性を認識し、責任ある行動をすることを求める。
　・情報資産の重要性：自社にとって重要な情報資産を明確にする。
3、情報セキュリティに関する項目
　・情報漏洩の防止：個人情報、その他機密性の高い情報の漏洩を防止する。
　・不正アクセス防止：外部からの不正アクセスを防止し、情報システムの安全稼働を確保する。
4、情報瀬キィリティに関する対策
　・組織体制：情報セキュリティに関する責任者を定め、組織体制を整備する。
　・教育・啓発：従業員への情報セキュリティに関する教育・啓発を定期的に実施する。
　・アクセス管理：情報システムへのアクセス権限を厳格に管理する。
　・パスワード管理：強固なパスワードを設定し、定期的な変更を義務付ける。
　・端末管理：端末の持ち出しルールを定め、紛失、盗難対策を実施する。
　・バックアップ：重要なデータのバックアップを定期的に実施する。
5、監査と見直し
　・定期的なチェック：情報セキュリティ対策の実施状況を定期的にチェックする。
　・継続的な改善：チェックの結果に基づき、情報セキュリティ対策を改善する。

# 「情報セキュリティ基本方針」の周知

「情報セキュリティ基本方針」が完成したら、全従業員に周知および実施をしていきましょう。

「情報セキュリティ基本方針」の内容を従業員に周知して理解を深めることは、組織全体のセキュリティレベルの向上に不可欠です。単に文書を配布するだけではなく、多角的なアプローチが重要です。
以下に周知および意識向上につながる具体的な方法を紹介しますので、自社に合った取り組みをしてみてください。

**1、入社時に研修を行う**
新しく入社する社員には、入社時に情報セキュリティの基本的な知識と、会社の情報セキュリティ方針を理解してもらうための研修を行いましょう。

**2、全社説明会**
全従業員を対象とした説明会を開催して、方針の目的や重要性について理解を深めてもらいましょう。

**3、メール配信**
方針をまとめた文書を全社員にメールで配布して、より深い理解を促しましょう。

**4、イントラネットへの掲載**
社内イントラネットや社員同士のコミュニケーションツールがある場合にはそこに掲載し、何時でも参照できるようにしておきましょう。

**5、定期的な配信**
全国で発生している情報セキュリティインシデント情報や新サービスなど、関連する情報を定期的にメール等で配信しましょう。

**6、情報セキュリティ月間**
年に2度ほど、情報セキュリティ月間を設け、クイズ大会やポスターコンクールなどを実施して楽しみながら学べる機会を提供しましょう。

**7、部門別勉強会**
部門ごとに情報セキュリティ関する勉強会を開催し、業務に関連する具体的な事例を交えるなどして説明しましょう。

**8、フィッシング対策訓練**
フィッシングメールの見分け方や不審なメールへの対応方法を学ぶ訓練を実施しましょう。

**9、アンケート調査**
従業員のセキュリティに対する意識や、改善点などを把握するためのアンケートを実施しましょう。

# 情報セキュリティ対策の実施

「情報セキュリティ基本方針」の周知と同時に、実際の対策を実施してきましょう。
情報セキュリティ対策には、会社としてコストをかけて取り組むものと、基本方針に沿って全従業員が主体的に取り組むべきものの２つがあります。

## １、会社としてコストをかけて取り組むもの

１１ページで紹介した、ゲートウェイセキュリティ対策と、エンドポイントセキュリティ対策、この２つは必須であるとお考えください。
そしてベンダー選びの際に重要なのが１２ページで紹介をしたSOC対応の有無です。
１３ページのポイントと失敗例も、ぜひ併せてご参考にしてみて下さい。

## ２、基本方針に沿って従業員が主体的に取り組むべきもの

具体的な取り組みの内容については、各社それぞれ「情報セキュリティ基本方針」に定めた内容、ということになりますが、下記にいくつか例を挙げますのでご参考にしてください。

**・常に最新の状態に**
パソコンやスマホ・タブレットのOSや各種ソフトウェアは、常に最新の状態にアップデートして使いましょう。月に一度程度、最新のものになっているか部署ごとにチェックなどをしても良いでしょう。

**・パスワードは複雑に**
パスワードは、極力複雑なものにしましょう。パスワードの強度を測定するサイトがいくつもありますので、解読までの年数が数百年～千年以上が望ましいでしょう。また同じパスワードを複数のサイトで使いまわないこと、3～6ヶ月に1度程度でパスワードを変更することもお勧めします。

**・パスワード管理ソフトを活用**
パスワードを複雑にすると、記憶しておくのが困難ですので、パスワード管理ソフトを活用してみてください。ほとんどのパスワード管理ソフトにあるコピペ機能で入力することで情報漏洩の予防になります。

**・怪しい情報は社内で共有**
メールやSMSなどで怪しいメッセージを受け取ったら、すぐに削除せずに社内で情報共有をして注意喚起をしましょう。日常的に行うことで、社内全員の意識が向上して、不用意な開封などによる感染を予防することができます。

**・重要な情報はパスワードで保護**
取引先や顧客に重要な情報をメールで送る際は、メール本文に記載するのではなく、パスワードで保護した添付ファイルで送信しましょう。またそのパスワードは、SMSなどメール以外の手段で送信するとより安全です。

**・パソコンはパスワードでロック**
業務に使用するパソコンやスマホなどは、パスワードが無いと起動やスリープからの解除ができない様にしておきましょう。指紋や顔などの生体認証機能があるものは、積極的にその機能を使って下さい。

**・覗き見帽子フィルム**
外出先でスマホやパソコンを使う機会の多い社員には、覗き見防止フィルムの利用を徹底させましょう。
また混雑した電車内でスマホで仕事のメールをするのNGです。後ろの人が見ています。

**これらの施策は、基本方針で定めた通りに運用されているか、定期的にチェックをしましょう。また実際の現場スタッフの働き方に合わない施策があれば、基本方針の見直しをして改善することも重要です。**

# 契約書類の見直し

国内へのサイバー攻撃の脅威は拡大しており、サプライチェーン（企業間の取引関係）を通じて深刻な被害に発展する例も増えています。被害をめぐって企業間でのトラブルが起これば、思わぬ二次災害になりかねませんので、具体的なリスクを想定した契約書の整備は、有効な情報セキュリティ対策のひとつと言えるでしょう。ぜひ今後のご参考にしてください。

主なポイントは以下の通りです。

・それぞれが自社の事業規模に鑑みて適切な情報セキュリティ対策を実施すること。
・サイバー攻撃を受けた場合、速やかに相手方にその事実を報告する義務を負うこと。
・サイバー攻撃にり相手方に損害を与えた場合
　→ 損害賠償の上限額をあらかじめ定めておく。
　→ 調査に必要な費用は損害を与えた側が負担をすること。
・不可抗力条項にサイバー攻撃を明記する。
・相手方にサイバーセキュリティ保険の加入を要請すること。

上記をすべて盛り込む必要はなく、業務内容などにあせて必要と思われる整備をしてください。

※ 具体的な整備をする際の内容については、企業法務が得意な弁護士などにご確認されることをお勧めします。

# 第五部　その他

## 参考資料

本ハンドブックを作成するにあたり、参考とした資料は以下の通りです。本ハンドブックに記載し切れなかった情報も多数掲載されていますので、ぜひご参照いただければと存じます。

・IPA独立行政法人情報処理推進機構セキュリティセンター
「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」（2023年4月26日）
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf

・一般社団法人 日本経済団体連合会
「サイバーリスクハンドブック　取締役向けハンドブック　日本語版」（2019年10月31日）
https://www.keidanren.or.jp/policy/cybersecurity/CyberRiskHandbook.pdf#page=3

・警察庁　サイバー企画課
「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」（2024年年3月14日）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf

# 用語解説

本ハンドブックで使用した用語について解説します。主に通信事業関連で使われる用語をピックアップしており、汎用的な意味ではなく、情報セキュリティに関連づけた解説内容としています。
尚、情報セキュリティ関連用語で本ハンドブックで使用していない用語については、解説を割愛いたします。

| 用語 | 解説 |
|---|---|
| APT攻撃 | Advanced Persistent Threatの略で、日本語では高度標的型攻撃と呼ばれます。<br>最新の技術や高度な手法を用いて行われる高度なサイバー攻撃で、長期間にわたって標的を監視し、隙をついて攻撃を仕掛けてきます。特定の組織や個人を標的にし、その組織の持つ機密情報を盗み出すことを目的とします。 |
| DDoS攻撃 | Distributed Denial of Serviceの略で、日本語では分散型サービス拒否攻撃といいます。<br>複数のコンピュータから同時に大量のアクセスを仕掛けることで、標的となるサーバーに過度の負荷をかけます。サーバーは正常に動作できなくなり、ウェブサイトやオンラインサービスが利用できなくなる状態に陥ります。<br>多くの場合、攻撃者は、マルウェアに感染した多数のコンピュータを「ボットネット」と呼ばれるネットワークに組み込み、これを利用して攻撃を行います。 |
| EDR | Endpoint Detection and Responseの略で、日本語ではエンドポイント検知・対応と訳されます。<br>端末上で常に監視を行い、ファイルの変更、ネットワーク通信など、様々な活動について記録、収集されたデータを基に、異常な挙動や既知の攻撃パターンと一致する動きを検知します。<br>また、検知された異常な挙動について、詳細な調査を行い、それが本当に攻撃であるかどうかを判断します。<br>攻撃と判断された場合は、感染したファイルを隔離したり、攻撃者の活動を阻止したりするなどの対応を行います。 |
| EPP | Endpoint Protection Platformの略で、日本語ではエンドポイント保護プラットフォームと訳されます。（エンドポイントセキュリティ、アンチウィルスソフト、ウィルス対策ソフト、などと同義）<br>PCやサーバーなどのエンドポイントと呼ばれるデバイスを、マルウェアなどのサイバー攻撃から未然に防ぐことを目的としたセキュリティソリューションです。<br>EDRが侵入したマルウェアの動きを検知・分析し、被害を最小限に抑えることに重点を置いているのに対し、EPPはマルウェアの侵入を未然に防ぐことに重点を置いています。 |

| 用語 | 解説 |
| --- | --- |
| HDD | Hard Disk Driveの略で、日本語ではハードディスクドライブと呼ばれます。パソコンやサーバーなどで、データを保存するための記録装置です。<br>磁気ディスクと呼ばれる円盤を高速回転させ、その表面にデータを磁気的に記録・読み出す仕組みになっていて、複数のディスクが積み重ねられている場合もあります。<br>比較的安価で大容量のデータを記録できますが、衝撃に弱く故障しやすいという側面もあります。 |
| IoT | 「Internet of Things」の略で、日本語では「モノのインターネット」と訳されます。<br>従来のインターネットがコンピュータ同士を繋ぐものであったのに対し、IoTは、あらゆるモノ（家電製品、自動車、センサーなど）をインターネットに繋ぐことで、より高度な情報化社会を実現しようとする考え方です。<br>生産性向上やコスト削減効果、遠隔操作や自動化などの便利さ、パーソナライズされた新サービスの提供などのメリットがある一方、大量のデバイスがインターネットに接続されるため、通信トラフィックの増大や個人情報漏洩のリスクがあります。 |
| IPアドレス | Internet Protocol Addressの略で、インターネットに接続された全ての機器に割り当てられる、いわばインターネット上の「住所」のようなものです。<br>インターネット上では、このIPアドレスを頼りに、データを送りたい相手を特定して、スムーズな通信を実現しています。 |
| Log情報 | コンピュータやネットワークシステムなどが、何らかの処理を行った際に記録される情報のことです。いわば、そのシステムの「日記」のようなもので、いつ、誰が、何を、どのように行ったかといった詳細な記録が保存されています。<br>システムに異常が発生した場合、ログを分析することで、その原因を特定し、迅速な対応が可能になり、不正アクセスやデータ漏洩などのセキュリティインシデントが発生した場合には、ログを分析することで、犯人の特定や被害状況の把握に役立ちます。<br>またシステムの利用状況を把握し、より効率的な運用に繋げることができます。 |
| OS | Operating System の略で、日本語では オペレーティングシステムと呼ばれます。コンピュータを動かすための基本的なソフトウェアであり、いわばコンピュータの「脳」のようなものです。<br>＜OSの例＞<br>Windows: マイクロソフトが開発したOSです。<br>macOS: アップルが開発したOSです。<br>Linux: オープンソースのOSで、様々な種類があります。 |

| 用語 | 解説 |
| --- | --- |
| SMS | Short Message Service の略で、日本語ではショートメッセージサービスと呼ばれます。携帯電話やスマートフォン同士で、短いテキストメッセージを送受信するサービスのことです。 |
| SOC | Security Operation Center の略で、日本語ではセキュリティオペレーションセンターと呼ばれます。<br>企業や組織のITシステムを監視し、サイバー攻撃から守り、安全性を確保するための専門組織や部門です。<br>情報セキュリティ対策においては非常に重要な役割を果たします。 |
| UTM | Unified Threat Management の略で、日本語では統合脅威管理と呼ばれます。<br>インターネット上の様々な脅威に対し、多段階の防御策を実現することができるネットワークセキュリティ製品の総称です。<br>不正な通信を社内と外部の境界で遮断することにより、安全なネットワーク環境を実現します。 |
| VPN | Virtual Private Network の略で、日本語では仮想私設網と呼ばれます。<br>VPNは、インターネットのような不特定多数が利用するネットワーク上に、仮想的な専用線を構築します。この仮想のトンネル内では、データが暗号化されるため、たとえ途中で通信内容が傍受されても、第三者に内容が漏れる心配が少なくなります。<br>多拠点展開をしている企業やテレワーク環境には欠かせない技術ですが、近年ではVPN機器の脆弱性をついた不正侵入などのサイバー攻撃が増加傾向にあり、適切に管理する必要があります。 |
| Whois検索 | インターネット上のドメイン名やIPアドレスに関する情報を、誰でも無料で検索できるサービスです。まるで電話帳で電話番号を調べるように、Whois検索でドメイン名を入力すると、そのドメインを所有している個人や企業の情報、ドメインの登録日、更新日などの詳細な情報が得られます。<br>しかし近年はWhois情報をもとにした営業活動の抑止や個人情報保護の観点から、個人や企業を特定できる情報は隠されている場合が増えています。 |
| アンチウィルスソフト | サイバー攻撃やマルウェアなどの悪意のあるプログラムからパソコンやスマートフォンを守るソフトウェアです。<br>アンチウィルスソフトのインストールは、最も基本的な情報セキュリティ対策です。 |

| 用語 | 解説 |
| --- | --- |
| インシデント | インシデント とは、一般的には「出来事」「事件」などを意味する言葉ですが、情報セキュリティ分野においては、サイバー攻撃による不正侵入や個人情報漏洩、データやWebの改ざん、システム障害などのトラブルを指します。 |
| エンドポイントセキュリティ | パソコン、スマートフォン、タブレットなどの、ネットワークの末端に位置するデバイス（エンドポイント）を、マルウェアやサイバー攻撃から保護するためのセキュリティ対策の総称で、EDRやアンチウィルスソフトがこれに当たります。 |
| クラウド | クラウドは、インターネットを通じて提供されるコンピューティングサービスの総称です。従来は、企業が自社内にサーバーを設置してソフトウェアやデータを管理していましたが、クラウドサービスを利用することで、インターネットに接続できるデバイスがあれば、いつでもどこからでもデータにアクセスしたり、ソフトウェアを利用できます。<br>とても便利な反面、セキュリティ上の問題やベンダーロックイン（特手のベンダーに依存しすぎて乗り換えが困難になること）などの課題があり、企業における道入には慎重な検討が必要です。 |
| ゲートウェイセキュリティ | ネットワークの入り口にあたる「ゲートウェイ」という部分で、外部からの不正なアクセスや攻撃からネットワークを保護するためのセキュリティ対策のことです。<br>ゲートウェイセキュリティは、ネットワークの入り口を守るための重要なセキュリティ対策です。ファイアウォールなどの技術を活用し、外部からの攻撃や内部からの情報漏洩を防ぐことで、ネットワーク全体の安全性を高めることができます。 |
| サプライチェーン | 製品が原材料の段階から、製造、流通、消費、リサイクルに至るまでの一連の企業や組織のネットワークを指します。<br>またサプライチェーンの脆弱性を悪用した攻撃をサプライチェーン攻撃といい、近年増加傾向にあります。<br>サプライチェーン攻撃は、多くの企業が影響をうけ、広範囲にわたる流情報漏洩やシステム障害につながる恐れがあり、気づくのが遅れるというような特徴があり、大企業だけではなく中小企業においてもサプライチェーンを意識した情報セキュリティ対策が重要になっています。 |
| システムセキュリティ | 広義では情報セキュリティ全般を指しますが、本マニュアルではネットワークセキュリティと区別する観点から、電子カルテシステムのような特定のシステム内のデータを保護するために組み込まれたものと位置付けています。 |

| 用語 | 解説 |
| --- | --- |
| ストレージ | データを保存しておく場所。<br>PC内であれば内部ストレージ、外付けのHDDやUSBメモリなどは外部ストレージ、インターネット上にデータを保存するGoogleDriveやDropboxなどはクラウドストレージ、と呼ばれます。 |
| セキュリティライセンス | セキュリティソフトやサービスを利用するために必要な許可証のようなものです。<br>セキュリティソフトは、開発元の知的財産です。これを利用するためには、ライセンスを購入し、その権利を持つ必要があります。 |
| ゼロトラスト | ネットワーク上のすべてのデバイスやユーザーを信頼せず、常に認証と認可を行うことでセキュリティを確保する考え方です。従来の「社内ネットワークは安全、外部ネットワークは危険」という境界型の考え方ではなく、あらゆるアクセスに対して慎重な検証を行うことが特徴です。<br>現状では大企業向けのサービスが多く、中小企業にとっては経済的なハードルが高い傾向にあります。 |
| ドメイン | ネットワーク上の端末は、数字の羅列であるIPアドレスで識別されますが、これを人が覚えるのは困難なため、人が認識しやすい文字にしたものがドメインです。 |
| ネットワークセキュリティ | 広義では情報セキュリティ全般を指しますが、本ハンドブックでは、個別のシステムに組み込まれてシステム内のデータを保護するシステムセキュリティと、ネットワーク全体を監視するネットワークセキュリティを分けて解説しています。 |
| ハッカー | コンピューターやネットワークに関する高度な知識と技術を持ち、それを利用して様々な活動を行う人のことを指します。<br>中でも、その技術力を活かして国や企業のセキュリティレベル向上に貢献している人をホワイトハッカー、悪意を持ってサイバー攻撃を仕掛ける人をブラックハッカーといいます。 |
| バックアップ | コンピュータやスマートフォンなどに保存されている大切なデータや設定などを、別の場所にコピーして保存しておくことをいいます。<br>バックアップの目的は、ハードウェアの故障や誤作動、サイバー攻撃などで失われた場合に、元の状態に復元するためです。近年では特にサイバー攻撃による改ざんや暗号化から素早く復旧できる機能やサービスが重要視されています。 |

| 用語 | 解説 |
| --- | --- |
| ファイアウォール | コンピューターネットワークにおいて、不正なアクセスや不要な通信を遮断し、ネットワーク内の情報を保護するためのセキュリティシステムのことで、ネットワークの出入り口であるゲートウェイに設置されます。<br>ファイアウォールは通過する通信を全てチェックし、あらかじめ設定されたルールに基づいて、許可された通信のみを通過させ、それ以外の通信は遮断します。 |
| ファイルサーバー | ネットワーク上に設置され、複数のユーザーが共通してファイルにアクセスし、共有することを目的としたサーバーのことです。<br>NAS（Network Attached Storage）もファイルサーバーの一種ですが、一般的にNASは、ファイルの保存と共有に特化したシンプルな装置であるのに対し、ファイルサーバーは、より高度な機能（バックアップ、アクセス権限管理など）を搭載しています。 |
| フィッシング行為 | 信頼できる企業やサービスと見せかけたメールやSMSメッセージなどから偽のウェブサイトへ誘導し、ID・パスワードやクレジットカード情報などを搾取行為です。<br>近年その手口は巧妙になってきており、本物との見分けが難しいものもあり、注意が必要です。 |
| フィッシング対策訓練 | 社員がフィッシングメールを識別し、巧妙な攻撃に騙されないよう、知識と意識を高めるためのトレーニングです。<br>社員に模擬フィッシングメールを送信し、リンクや添付ファイルを開いてしまう人がどれくらいいるかをチェックし、その後勉強会などをおこなうのが一般的です。 |
| マルウェア | サイバー攻撃に利用される悪意のあるソフトウェアやプログラム（ウィルス、ワーム、トロイの木馬、ランサムウェア、スパイウェア、ボットなど）の総称です。 |
| ランサムウェア攻撃 | フィッシングメール、不正なウェブサイト、USBメモリなどを通じて、コンピューターに侵入し、コンピューター内のファイルを暗号化して利用不能な状態にしておいて、復号の代わりに金銭を要求する、いわゆる身代金要求型の攻撃手法です。<br>近年は特にこの被害が増加傾向にあります。 |
| 暗号化 | データを元の状態から別の形に変換し、第三者が内容を解読できないようにする技術のことです。<br>暗号化には、鍵と呼ばれる特別な情報が使われます。この鍵を使ってデータを暗号化し、同じ鍵か別の鍵を使って復号します。 |

| 用語 | 解説 |
| --- | --- |
| 情報資産 | 企業や組織が保有する、「ヒト・モノ・カネ」に関する情報の総称で、企業の活動によって生み出され、蓄積されたあらゆるデータや知識のことを指します。<br>情報資産は、一旦漏洩すると企業に大きな損害を与える可能性があります。そのため、情報資産を適切に管理することは、企業にとって非常に重要な経営課題といえます。 |
| 脆弱性 | コンピュータシステムやソフトウェアに存在する、不正なアクセスや攻撃に対して弱い状態、つまりセキュリティ上の欠陥のことを指します。<br>脆弱性が見つかるとメーカー側から修正プログラムが提供されるので、その様な情報をキャッチした場合は、速やかに修正プログラムを適用する（アップデートする）必要があります。 |
| 通信パケット | インターネットなどのネットワーク上を流れるデータの最小単位のことです。<br>インターネットでは、様々な種類のデータ（メール、画像、動画など）が同時に送受信されています。これらのデータをそのまま送ると、大きなデータがネットワークを占有し、他の通信を妨げてしまう可能性があります。<br>そこで、大きなデータを小さなブロック（パケット）に分割して送信することで、複数の通信を効率的に行えるようにしています。 |

# さいごに

本ハンドブックを最後までご覧くださいまして、誠にありがとうございました。
内容はご満足のいくものでしたでしょうか？

本ハンドブックは、特にITリテラシーのあまり高くない中小企業の経営者向けに編纂いたしました。
しかし、どうしても専門用語を使わざるを得ない部分が多々ありましたので、用語解説ではなるべくわかりやすい表現を心がけたつもりです。
それでもやはり難しい、よく話分からない、という部分もあろうかと存じますので、気になる方はどうぞお気軽にお問い合わせ下さい。

また、業界のあまり良くない情報や失敗例（お客様の失敗というより、販売ベンダー側の問題が大きい）なども一部記載をさせて頂きました。この様な情報は、サイバー攻撃の現状と同じくらい、お客様の耳には届きにくい情報かと思います。こうした情報をあえて記載したのは、注意喚起の意味合いもありますが、少しでもクリーンな業界になってほしいという願いも込められております。同業者の方々には、どうかご理解を賜りたくお願い申し上げます。

さて、本編では触れておりませんが、情報セキュリティ対策をしっかり行い、それを対外的にアピールすることで企業価値の向上も期待できます。実際「客単価をアップできた」とのお声をいただいたこともございます。
大手企業では、取引先企業に対し、大企業側が求める情報セキュリティ対策の実施要件を満たすことを取引開始の条件にするような動きも広がっていますので、今後の会社の発展という観点においても、情報セキュリティ対策が不可欠であるとご理解いただければ幸いです。

また、中小企業の皆様がサイバー攻撃の被害にあってしまうことは、国益を損ねることに他ならないと考えられます。つまり、情報セキュリティ対策をしっかり行うことは、安心して取引のできる市場づくりに寄与する社会貢献の一つであると考えることもできるでしょう。

最後となりましたが、本ハンドブックが、皆様の会社の情報セキュリティ対策を強化するための一助となりましたら幸いです。

発行：2024年10月1日

一般社団法人 中小企業を守る会　代表理事
株式会社GatewayLink　代表取締役
野呂　公平