中小企業向け
サイバーセキュリティ対策の極意

Ver 2.2

日本で初めてサイバー探偵事務所を開く。ソフト帽とトレンチコートがトレードマーク。日夜懸命に頑張る中小企業の経営者に対して、客観的な態度と視点を持って依頼人に真に役立つ情報を端的に明言する。「東京をサイバー攻撃から守る」という正義感だけが、今日も彼を突き動かす。

今回、その資質を見込まれ、東京都からの依頼でサイバーセキュリティ対策のコンサルタントとして本冊子のガイド役に任命された。

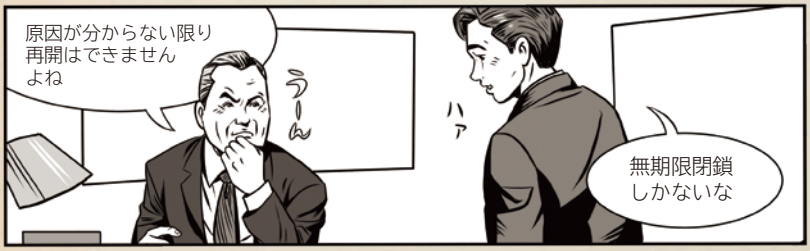
冴羽（さいば） 守（まもる）

※本キャラクターはフィクションです

ケーススタディー　1

なぜ、こんな小さな会社が狙われたの？

1カ月後　会社での会議



これは実際に起きたケースを基に脚色したものだ。この会社は社員10人ほどの小さな会社で、再開時期が未定のままサイトは閉鎖された。個人情報を窃取するサイバー攻撃の対象は、決して大企業や有名な通販サイトだけでなく、顧客情報の収集などインターネットを何らかの形でビジネスに利用している会社は全て標的になっている。サイバー攻撃による被害によって、事業に致命的なダメージを受ける可能性がある。備えあれば憂いなしだ。

ケーススタディー　2

ある日突然、銀行口座の預金残高が消えた！

数日後、銀行の支店長室で

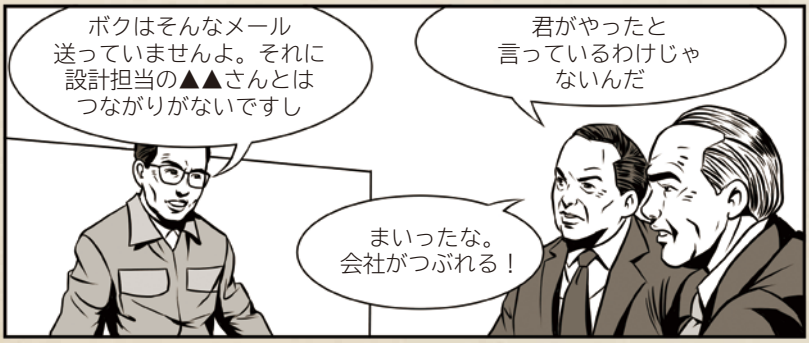
人員不足に悩む中小企業にとって、インターネットバンキングは経理業務の効率化に不可欠なものだが、サイバー攻撃の対象にもなっている。

2019 年は、9 月から被害が急増し、発生件数は 1872 件に上った。年間被害総額も 25 億円超の被害が報告されている。

ケーススタディーにもある通り、インターネットバンキングを利用しているからといって、銀行が代弁してくれるとは限らない。基本的には自己防衛だ。

ケーススタディー　3

取引先企業への踏み台にされた



サイバー攻撃は大企業だけを狙っているわけではない。
このケースでは、標的とされた大企業のセキュリティが堅固だったため、攻撃者はその取引先の中小企業を狙ったのだ。なぜなら、中小企業のセキュリティは大企業に比べて甘く、中小企業のセキュリティを突破すれば、取引のメールなどを介して、大企業のシステム内部へ侵入しやすいからだ。こうして踏み台にされた企業にとっては、ビジネスに与える影響は甚大だ。

ケーススタディー　4

企業データが人質に！日常に潜むサイバー攻撃の魔手

ランサムウェアを使ってパソコンを使用不全にし、身代金要求をするサイバー攻撃が目立つ。そこで中心的役割を果たしたマルウェアの１つに「Emotet（エモテット）」が挙げられる。Emotetは、冒頭のようなやり取りからパソコンや社内システムに忍び込む。そして、感染したパソコンからメール情報やアドレス帳の情報を窃取するほか、ランサムウェアをはじめとする別のマルウェアを呼び込む機能もあり、非常に厄介かつ危険な存在だ。

ケーススタディー　5

メールで届いた入金指示に従ったら詐欺の被害者に！

経営幹部や取引先になりすましたメールを送信し、従業員をだまして不正な口座に入金させることで金銭的な被害をもたらすサイバー攻撃が「ビジネスメール詐欺（Business E-mail Compromise ／ BEC）」だ。攻撃者は、標的となる企業の従業員が業務でやり取りしているメールを、何らかの方法で盗み見したり、ネット上の企業情報などを参考にしたりして、標的となる企業のプロジェクトや人間関係を事前に把握することで、送信メールの信憑性を高める。

ケーススタディー　6

セキュリティは サプライチェーン 全体の責任

中小企業はセキュリティ対策予算や人員が不足しがちで、対策も遅れがちだ。サイバー犯罪者はそこを突く。中小企業を取引のある大企業に攻撃する「入り口」として狙うケースも存在する。そうなれば、被害者であると同時にサイバー犯罪の一端を担ってしまう。取引停止だけでなく、損害賠償を請求されることもあるだろう。「中小企業だから狙われない」という甘い考えは通じない。セキュリティはサプライチェーン全体の問題という点を肝に銘じてほしい。

ケーススタディー　7

サイバー保険に入っていれば……

日々進化するサイバー攻撃の脅威。いつ、どのようなタイミングで狙われるかは分からない。もし攻撃の標的になったら？
そのリスクヘッジに備えるのが「サイバー保険」だ。サイバー事故によって生じた第三者に対する「損害賠償責任」や事故の際に必要となる争訟費用等の損害が補償される。ぜひチェックしてほしい。

はじめに

狙われるのは中小企業

サイバー攻撃の標的は政府・自治体や重要インフラだけではありません。
こうした大規模なサイバー攻撃には、数十万台の端末から一斉攻撃をかける手口があり、それに使用される端末は攻撃者に乗っ取られた端末です。そして比較的セキュリティの甘い中小企業の端末が狙われています。
最近では、大企業は防御が厳重なため、防御の甘い取引先の中小企業を狙い、そこから大企業のシステム内部へ侵入するケースも増えています。

セキュリティ対策はなぜ必要なのか？

インターネットが社会生活の隅々まで普及している今、サイバー攻撃は社会機能や国民生活を脅かす大きな問題となっています。個人も企業もセキュリティに関する正しい知識を身に付け、必要な対策を実践していくことがとても重要になっています。
いったんサイバー攻撃を受けて被害を受けると、金銭の損失はもとより、顧客の喪失、業務の喪失など、経営に直結する重大なリスクが発生します。経営者が責任を問われたり、場合によっては株主代表訴訟の対象にもなったりします。

すぐやろう！　サイバーセキュリティ対策

セキュリティ対策は必要だと分かっていても直接利益を生み出すものではない、難しくてよく分からない、社内に IT のことが分かる人材がいないなどの理由から、手つかずのままにしていませんか？
最優先で実施すべき対策はそんなに難しいものではありません。基本的な対策を実施することで多くの攻撃を防ぐことができます。

備えあれば憂いなし

本書は、サイバー攻撃の最新の手口から、中小企業でも実施できる基本的な対策まで分かりやすくまとめました。

INDEX 目次

中小企業向け　サイバーセキュリティ対策の極意 Ver2.2

TOP SECRET
MISSION 1

知っておきたいサイバー攻撃の知識

TOP SECRET MISSION 2　すぐやろう！　対サイバー攻撃アクション

TOP SECRET MISSION 3　経営者は事前に何を備えればよいのか？

TOP SECRET MISSION 5 やってみよう！サイバー攻撃対策シミュレーション

TOP SECRET INFORMATION インフォメーション

本書の用語表記について

本冊子では、日ごろ、サイバー攻撃や情報技術（IT）に接することの少ない方々にもご理解いただくために、できる限り専門用語を使わず、分かりやすい用語に統一しています。

① コンピューターに潜り込んで正常な利用を妨げる不正･有害なプログラムは、近年「マルウェア」(malware) と呼ぶようになっていますが、本冊子では主にウイルスと表現しています。
② ネットワークを通じて他のコンピューターへの感染を広める不正なプログラムが「ワーム」(worm)、利用者に気付かれないように有害な動作を行うプログラムが「トロイの木馬」(Trojan horse) と名付けられていますが、本冊子では全てウイルスと表現しています。
③ 集中アクセスによるサービス停止についても、手口としてはボットネットウイルス、DoS 攻撃、DDoS 攻撃など多様ですが、本冊子では主として「集中攻撃」という形で総称しています。
④ ウイルスを発見し駆除するプログラムについても、ウイルス対策ソフトによって定義ファイルやパターンファイルなど呼び方が異なりますが、本冊子では全て定義ファイルと表現しています。
⑤ 本冊子では「サイバーセキュリティ」と「情報セキュリティ」という 2 つの言葉を使っています。「サイバーセキュリティ」は、コンピューターやインターネットの中に広がる仮想空間に関するセキュリティという意味で使用しています。一方、現実に存在する紙媒体に記載された情報などを含むセキュリティの場合は「情報セキュリティ」を使用しています。
⑥ 本冊子で参照した多くの資料では、セキュリティを脅かす事件や事故を総称して「セキュリティインシデント」と表現していますが、本冊子では「サイバー攻撃被害」と表現しています。

詳しくは巻末の「用語解説インデックス」を参照してください。

この冊子の使い方

どんなサイバー攻撃があるのかを知る
→ [01] 知っておきたいサイバー攻撃の知識

被害を予防するための対策を行う
→ [02] すぐやろう！対サイバー攻撃アクション

経営者が備えるべきことを知る
→ [03] 経営者は事前に何を備えればよいのか？

会社としての対応計画を準備する
→ [04] もしもマニュアル

攻撃シーンを想定して実際に行動する
→ [05] やってみよう！サイバー攻撃対策シミュレーション

本書では、これだけは必ず実践してほしい項目に「すぐやろう」マークを付けました。このマークが付いている項目は優先的に確認し、必ず実施しましょう。

今すぐチェックしておくべきこと

攻撃について知っておくべきこと

対策のために行動するべきこと