中小企業向け
サイバーセキュリティ対策の極意

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も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。
平成 27 年度には、1 件当たり 9,100 万円という被害も発生し、全体で 30 億円余り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、銀行が弁償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。

はじめに

約400倍

情報通信研究機構（NICT）サイバーセキュリティ研究所サイバーセキュリティ研究室が2016年の1年間で観測したサイバー攻撃に関連する通信量は約1,281億パケット※でした。観測を始めた2005年は約3.1億パケットでしたから、11年間で413倍に増加しています。

※通信の伝送単位

2020年東京が狙われている

2020年には東京2020オリンピック・パラリンピックが開催されます。
2016年に開催されたリオデジャネイロオリンピックでは、テロと同様にサイバー攻撃が大きなリスクとして懸念され、2,300万件のアタックをブロックしたと報告されています。また、オリンピックの中核施設に隣接した変電所を運営している電力会社Light社が期間中に受けた攻撃は、1,300万件に達しました。
東京2020大会でも同様のサイバー攻撃が予想されます。

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ります。

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

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 4 もしもマニュアル

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、本冊子では全て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「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