

中小企業向け サイバーセキュリティ 対策の極意



さいば まもる
冴羽 守

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。

※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？

〇〇さん 決済のことで
△△クレジットから
お電話です

△△クレジット？
何だろう？



はい
〇〇ですが

いつもお世話に
なっております。

御社の顧客情報が
流出しているようなのですが、
調べていただけますか？



カードの不正使用の疑惑が
あり、御社のサイトがハッ
キングされている可能性が
あります



ちょっと待ってください
何かの間違いでは？

教えてください
弊社に登録された個人情報だと
どうして分かるのですか？





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。個人情報を取捨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の、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はいるからといって、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

〇〇社長
あなたの会社との
取引は中止だ

そんな!!

納品した
製品に何か問題が?

君の会社に
△△という社員がいる
だろう。そいつがうち
の設計担当の▲▲に
ウイルスメールを送り
つけてきたんだ

それは何かの間
違いでしょう

△△は開発部
にいる真面目
な人間ですよ

れっきとした証拠がある。
原因が分かるまで
部品の納品は中止
だ

ボクはそんなメール
送っていませんよ。それに
設計担当の▲▲さんとは
つながりがないですし

君がやったと
言っているわけじゃ
ないんだ

まいったな。
会社がつぶれる!



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 万件の攻撃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るけど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ないなどの理由から、手つかずのままにいませんか？

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

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？……………	2
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！……………	4
ケーススタディー 3	取引先企業への踏み台にされた……………	6
はじめに……………		8
目次……………		10
この冊子の使い方……………		16

TOP SECRET

MISSION 1

知っておきたいサイバー攻撃の知識

1・1	標的型攻撃による情報流出……………	18
1・2	ランサムウェアを使った詐欺・恐喝……………	20
1・3	Web サービスからの個人情報の窃取……………	22
1・4	集中アクセスによるサービス停止……………	24
1・5	内部不正による情報漏えいと業務停止……………	26
1・6	Web サイトの改ざん……………	28
1・7	インターネットバンキングの不正送金……………	30
1・8	悪意のあるスマホアプリ……………	32
1・9	巧妙・悪質化するワンクリック詐欺……………	34
1・10	Web サービスへの不正ログイン……………	36
1・11	公開された脆弱性対策情報の悪用……………	38

1・12	IoT 機器を踏み台にした攻撃	40
1・13	中小企業におけるサイバー攻撃被害の例	42
	おさらいクイズ	44

TOP SECRET

MISSION 2

すぐやろう！ 対サイバー攻撃アクション

今やろう！ 5 + 2 の備えと社内使用パソコンへの対策

2・1	サイバー攻撃に対して何ができるか	46
2・2	OS とソフトウェアのアップデート	48
2・3	ウイルス対策ソフト・機器の導入	50
2・4	定期的なバックアップ	52
2・5	パスワードの管理	54
2・6	アクセス管理	56
2・7	紛失や盗難による情報漏えい対策	58
2・8	持ち込み機器対策	60

今やろう！ 電子メールへの備え

2・9	電子メールの安全利用	62
2・10	標的型攻撃メールへの対応	64
2・11	迷惑メール発信への対応	66

今やろう！ インターネット利用への備え

2・12	安全な Web サイト利用	68
2・13	閲覧制限	70

今やろう！

- 2・14 重要情報の洗い出し……………72
- 2・15 重要情報の保管……………74
- おさらいクイズ……………78

TOP SECRET MISSION 3

経営者は事前に何を備えればよいのか？

サイバーセキュリティ対策は、事業継続を脅かすリスクの 1 つ

- 3・1 サイバーセキュリティ対策が経営に与える重大な影響……………80
- 3・2 サイバー攻撃を受けると企業が被る不利益……………82
- 3・3 経営者に問われる責任……………84
- 3・4 投資効果（費用対効果）を認識する……………86

自社の IT 活用・セキュリティ対策状況を自己診断する

- 3・5 IT の活用診断……………88
- 3・6 サイバーセキュリティ投資診断……………90
- 3・7 情報セキュリティ対策診断……………92

ビジネスを継続するために（守りの IT 投資とサイバーセキュリティ対策）

- 3・8 業務の効率化、サービスの維持のために……………94
- 3・9 経営者が認識すべきサイバーセキュリティ経営 3 原則……………96
- 3・10 経営者がやらなければならない
サイバーセキュリティ経営の重要 10 項目……………98

ビジネスを発展させるために（攻めの IT 投資とサイバーセキュリティ対策）

- 3・11 次世代技術を活用したビジネス展開……………110

【コラム】「攻めのIT 経営中小企業百選」	111
3・12 IoT、ビッグデータ、AI、ロボットの活用	112
【コラム】IoT、ビッグデータ、AI、ロボットはつながっている	113
3・13 IoT が果たす役割と効果	114
【コラム】ものづくり企業 IoT 活用事例	115
3・14 人工知能（AI）が果たす役割と効果	116
【コラム】新しい価値を持った業務の創出	117
3・15 IoT を活用する際のサイバーセキュリティ上の留意点	118
3・16 IoT を活用する一般利用者のための基本ルール	120
【コラム】クラウドサービスの活用	122

セキュリティホールを減らす網羅的・体系的な対策の策定方法

3・17 新・5分でできる自社診断シート	124
3・18 情報セキュリティハンドブックひな形（従業員向け）	126
3・19 情報セキュリティポリシーの明文化	128
3・20 情報資産管理台帳の作成	130
おさらいクイズ	132

TOP SECRET

MISSION 4

もしもマニュアル

4・1 緊急時対応用マニュアルの作成	134
4・2 基本事項の決定	136
4・3 漏えい・流出発生時の対応	138
4・4 改ざん・消失・破壊・サービス停止発生時の対応	140

4・5	ウイルス感染時の初期対応	143
4・6	届け出および相談	145
4・7	大規模災害などによる事業中断と事業継続管理	146
	【ワークショップ】 自社でやろう サイバー攻撃への対応アクション	148

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

SCENE 01	サイバー攻撃前夜	150
SCENE 02	攻撃発生その瞬間	151
SCENE 03	サイバー攻撃直後	152
SCENE 04	潜入拡大	153
SCENE 05	顧客への被害の拡大 取引先への被害の拡大	154
SCENE 06	サイバー攻撃の発覚	155
SCENE 07	原因が判明 ウイルス感染が原因	157
SCENE 08	再発防止策の作成	159
SCENE 09	復旧回復	161

TOP SECRET INFORMATION

インフォメーション

6・1	もしかしてサイバー攻撃？ ここに連絡を！	164
-----	----------------------	-----

6・2	やられる前に、しっかり予防を！	166
6・3	情報セキュリティ5カ条	170
6・4	情報セキュリティ用語解説	172
6・5	セキュリティお役立ちリンク	178
6・6	情報セキュリティポリシーサンプル	180
	主な参考文献	185
	用語解説インデックス	187

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、現実には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

すぐやろう



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