

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。

さいば まもる
冴羽 守

※本キャラクターはフィクションです



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。個人情報や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はいるからといって、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

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!

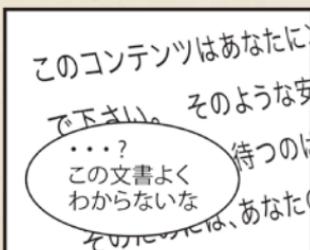


サイバー攻撃は大企業だけを狙っているわけではない。このケースでは、標的とされた大企業のセキュリティが堅固だったため、攻撃者はその取引先の中小企業を狙ったのだ。なぜなら、中小企業のセキュリティは大企業に比べて甘く、中小企業のセキュリティを突破すれば、取引のメールなどを介して、大企業のシステム内部へ侵入しやすいからだ。こうして踏み台にされた企業にとっては、ビジネスに与える影響は甚大だ。



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





どうしよう
大事なメールが
来るはずなのに



警告!

うわっ!

あなたの大切なファイルが暗号化により
直ちに修復をするためには、仮想通貨
を支払う必要があります



大切なファイルを
暗号化ですって?

これウィルス
じゃないですか?



主任! 「仮想通貨で
金をよこせ」と言っ
ています



主任! ファイルが
このままの状態だと
取引停止に
なっちゃいます

う〜む.....

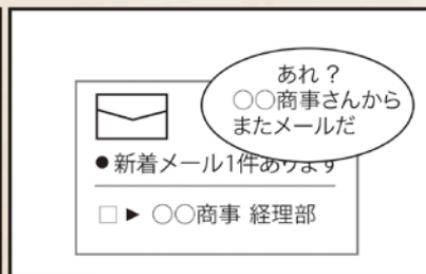
払うしかないのか?

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！





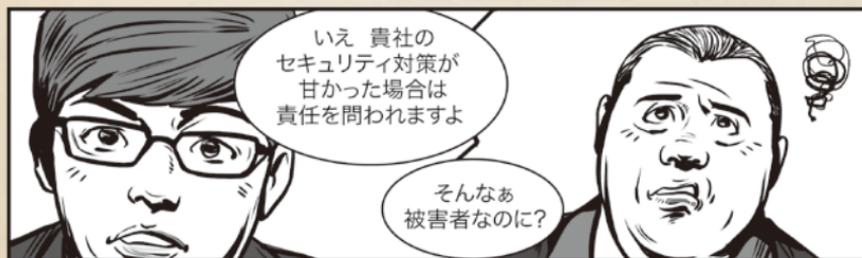
経営幹部や取引先になりすましたメールを送信し、従業員をだまして不正な口座に入金させることで金銭的な被害をもたらすサイバー攻撃が「ビジネスメール詐欺 (Business E-mail Compromise / BEC)」だ。攻撃者は、標的となる企業の従業員が業務でやり取りしているメールを、何らかの方法で盗み見したり、ネット上の企業情報などを参考にしたりして、標的となる企業のプロジェクトや人間関係を事前に把握することで、送信メールの信憑性を高める。



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」や事故の際に必要な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 Ver2.2

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
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	8
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！	10
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	12
ケーススタディー 7	サイバー保険に入っていれば	14
	はじめに	15
	目次	16
	この冊子の使い方	22

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	24
1・2	ランサムウェアを使った詐欺・恐喝	26
1・3	Web サービスからの個人情報の窃取	28
1・4	集中アクセスによるサービス停止	30
1・5	内部不正による情報漏えいと業務停止	32
1・6	Web サイトの改ざん	34
1・7	インターネットバンキングの不正送金	36
1・8	悪意のあるスマホアプリ	38

1・9	巧妙・悪質化するワンクリック詐欺	40
1・10	Web サービスへの不正ログイン	42
1・11	公開された脆弱性対策情報の悪用	44
1・12	IoT 機器を踏み台にした攻撃	46
1・13	中小企業におけるサイバー攻撃被害の例	48
1・14	なりすまし EC サイトの被害と回避策	50
1・15	ビジネスメール詐欺 (BEC) にご注意!	52

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	54
2・2	OS とソフトウェアのアップデート	56
2・3	ウイルス対策ソフト・機器の導入	58
2・4	定期的なバックアップ	60
2・5	パスワードの管理	62
2・6	アクセス管理	64
2・7	紛失や盗難による情報漏えい対策	66
2・8	テレワーク等での持ち出し・持ち込み機器対策	68

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	70
2・10	標的型攻撃メールへの対応	72

2・11	迷惑メール発信への対応	74
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	76
2・13	閲覧制限	78
今やろう！		
2・14	重要情報の洗い出し	80
2・15	重要情報の保管	82

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	88
3・2	サイバー攻撃を受けると企業が被る不利益	90
3・3	経営者に問われる責任	92
3・4	投資効果（費用対効果）を認識する	94

【コラム】セキュリティ対策は経営上の「投資」と位置付ける！ ……95

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	96
3・6	サイバーセキュリティ投資診断	98

【コラム】「IT ガバナンス」と6つの原則 ……99

3・7	情報セキュリティ対策診断	100
-----	--------------	-----

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	102
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	104

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	106
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	118
	【コラム】DX 推進はビジネス飛躍のチャンス	119
3・12	IoT、ビッグデータ、AI、ロボットの活用	120
	【コラム】IoT、ビッグデータ、AI、ロボットはつながっている	121
3・13	IoT が果たす役割と効果	122
	【コラム】中堅・中小企業の IoT 活用事例	123
3・14	人工知能 (AI) が果たす役割と効果	124
	【コラム】新しい価値を持った業務の創出	125
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	126
3・16	IoT を活用するための基本ルール	128

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

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	148
SCENE 02	攻撃発生その瞬間	149
SCENE 03	サイバー攻撃直後	150
SCENE 04	潜入拡大	151
SCENE 05	顧客への被害の拡大 取引先への被害の拡大	152
SCENE 06	サイバー攻撃の発覚	153
SCENE 07	原因が判明 ウイルス感染が原因	155
SCENE 08	再発防止策の作成	157
SCENE 09	復旧回復	159
Attention	大切なのは社内意識の向上！感染を狙うメールに注意	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	その他の主な報告・連絡・相談窓口等	166
6・3	セキュリティお役立ちリンク	168
6・4	中小企業の情報セキュリティ対策ガイドライン	170
6・5	中小企業のためのクラウドサービス安全利用手引き	178
6・6	IT 活用に不可欠な IT 人材の確保と育成	180

6・7	情報セキュリティ関連法令	182
6・8	情報管理が不適切な場合の処罰など	183
	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