



中小企業を狙う

「サイバー攻撃」への備えと 万が一の際の対処法

大企業へのシステム攻撃の踏み台として、セキュリティが脆弱な中小企業が狙われるケースが増えています。ここでは、セキュリティ対策、侵入された際の対処法等を紹介します。

ベルケンシステムズ代表取締役
IT導入コンサルタント

鈴木 純二

中小企業を狙う 犯行の増加

企業をターゲットとしたサイバー攻撃が、近年、増加の一途をたどっています。少し前までは、攻撃の対象は行政機関であったり大企業であったりと、中小企業とは少し遠いところで起きているものでした。ところが、IPA（独立行政法人情報処理推進機構）が毎年公表している「情報セキュリティ10大脅威」2022年版を見ても、サプライチェーンの弱点を悪用した攻撃が3位に入るなど、大企業の取引先である中小企業が狙われる傾向が強まっています（図表1）。

犯人は、大企業のように防衛を固めているところを避け、「狙いやすいところから攻める」という極めて悪質な手段をとるようになってきているのです。もはや企業の規模を問わず、サイバー攻撃への備えは待ったなしの状況と言えるでしょう。

ところが、この分野の情報には非常に難解な技術用語が多用されることが多く、なかなか素人が理解するにはハードルが高いのが実

情です。本記事では、そのような技術面での話題はなるべく避け、企業経営者や実務責任者が、その立場を全うするために知るべき知識ととるべき行動を解説していきます。

(1) 犯人の狙いは？

攻撃に対して備えるためには、まず犯人の意図や攻撃の手法を知ることが肝要です。

企業をターゲットとした犯行の狙いは、大きく分類して「金銭要求型」と「いやがらせ型」となりますが、最近は金銭が犯行動機になることが増えています。金銭目的なので、通常であれば他者への直接転売がしにくい図面や部品表などの技術情報、営業情報のデータも犯行のターゲットとなります。たとえば、

- ・データを使えなくして金銭を要求する
- ・「データを公開する」と脅して金銭を要求する

といったものです。

これが、最近話題の「ランサムウェア」と呼ばれる身代金要求型攻撃となります。

(2) 攻撃を受けるとどうなる？

一度犯行の被害に遭ってしまえば、パソコンが使えなくなるだけで

**図表1 2021年度に発生した情報セキュリティの脅威
(上位10)**

順位	脅威の内容	(昨年順位)
1位	ランサムウェアによる被害	(1位)
2位	標的型攻撃による機密情報の窃取	(2位)
3位	サプライチェーンの弱点を悪用した攻撃	(4位)
4位	テレワーク等のニューノーマルな働き方を狙った攻撃	(3位)
5位	内部不正による情報漏えい	(6位)
6位	脆弱性対策情報の公開に伴う悪用増加	(10位)
7位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	(初)
8位	ビジネスメール詐欺による金銭被害	(5位)
9位	予期せぬIT基盤の障害に伴う業務停止	(7位)
10位	不注意による情報漏えい等の被害	(9位)

出典：IPA「情報セキュリティ10大脅威2022」を基に作成
(<https://www.ipa.go.jp/security/vuln/10threats2022.html>)

「武器」ウイルスなどの悪意のあるソフトウェアに、「運搬手段」メール・インターネット・USBメモリ・メッセージ等」と読み替えることとなります。複数の武器とその

「武器」ウイルスなどの悪意のあるソフトウェアに、「運搬手段」メール・インターネット・USBメモリ・メッセージ等」と読み替えることとなります。複数の武器とその

ではなく、要求された金額を支払っても元に戻してもらえない保証はなく、しかも何度も金銭を要求される、といった様々な嫌がらせが続きます。

また、データを盗まれた場合、そのデータは犯人の手元に永続的に残る可能性がありますので、さらにそこから他人の手に渡ってしまう可能性もあります。

つまり、いったん攻撃の被害に遭ってしまったと、元の状態に完全

に戻することは難しい、と言えるのです。

(3) 防衛は「敵の攻め方を理解することから」

では、犯人はどのようにして犯行に及ぶのでしょうか？ テロ事件を思い浮かべてみてください。犯人には「武器」が必要となります。たとえば爆弾などです。

しかし、爆弾を持っているだけでは、危害を及ぼすことはできません。「運搬手段」がないといけ

運搬手段がありますので、それらを巧みに組み合わせることで、高度な攻撃も可能となります。

前述のランサムウェアも、最初に使われる武器は「ウイルス」で、その運搬手段として多用されているのが「メール」です。メールでウイルスが送り込まれ、それに感染するとパソコン内のデータを勝手に暗号化し、さらにインターネット経由でデータを外に運び出そうとします。

多くの人が頼りにしているウイルスチェックプログラムは、既知のウイルスおよびその派生種を検出する能力はありますが、新しくつくられたウイルスを100%検出することはできません。ウイルスチェックプログラムをすり抜けてしまうウイルスが日々開発され、バリエーションが豊富になってきています。

これらの武器と運搬手段を複雑に組み合わせ、犯行の口をどんなに巧妙なものに改良することが可能なので、サイバー攻撃は日々進化・多様化し、根絶が難しい犯罪となってしまうわけです。

サイバー攻撃への備えを考えるためには、この「武器と運搬手段」の組合せの原理をよく理解し

ておくことが何よりも肝要です。

中小企業に求められる備えとは

さて、犯行の動機と手段を理解したところで、どうやって自社を防御すればよいのか考えてみましょう。

あちこちのセキュリティセミナーで語られている定番の対策をひと言で言えば、「技術的な対応と人的な対応の2つをバランスよく進める」ということになります。

しかし、日進月歩で技術革新が進んでいるなか、それら対策の内容は難解な専門用語が並ぶばかりで、専門外の人が理解できるものではありません。

でも、ご安心ください。これらの高度な技術がわからなくても、中小企業にできる対策はたくさんあります。具体的には、「技術的防衛については世間的にごく当たり前のことを地道に実行しつつ、人が対処すべき防御に重点を置いて進める」という発想で、自社の攻撃耐性を高めるのです。

(1) 「技術面でのごく当たり前の備え」とは？

前述したとおり、犯人が用意す

る武器はウイルスなどのソフトウェアがメインとなります。したがって技術面での対応は、悪意あるソフトウェアを作動しないようにする、万が一持ち込まれてしまった場合は早期に見つけられるようにする、などとなります。

たとえば、

① ウィンドウズ等のパソコンのOSは最新のものに更新し続ける(サポートの切れたOSは決して使わない、配信された更新をもれなく適用させる等)

② ウイルスチェックプログラムをもれなく導入し、更新を怠らないようにする

③ 社員が使っているソフトウェアについて、配信された更新をもれなく適用させる

④ ルーターなどのネットワーク機器のソフトウェアを最新のものに続ける

といった対応となります。

要するに「古いものは使わず、メンテナンスをこまめに行なう」ということに尽きます。これらが疎かになると、古いソフトウェアが持つ弱点を悪用するタイプの武器を持ち込まれてしまったり、持ち込まれた武器を検出できなくなったりするわけです。

(2) 重要な「企業組織としての備え」

ここからが、企業経営者と管理者の重要な出番です。

冒頭でも触れたサプライチェーンを狙う攻撃の場合、発注元である大手企業の情報を狙うために取引先企業を標的にする場合が多発していますし、仕事を下請けに出している場合はそちらも狙われる危険性があります。

したがって、以後説明する備えは、社内および取引先(下請けや外注先)にも範囲を広げて解釈してください。実行には、経営者のリーダーシップと調整力が問われるところです。

① 情報資産を棚卸し、リスクを分析する

まず「どこに、どんな情報を誰の責任下で保有していて、それが滅失や漏洩した場合にどうなってしまうのか」を洗い出します。要するに、「情報資産の棚卸しとリスク分析」をします。

このとき、取引先から預かっている情報、他社に貸し出している情報、クラウドに保管されている情報まで含めて洗い出すことが重要です。大変手間がかかる仕事ですので、経営層の強い意思とリー

ダーシップがないと現場はついてきません。

とても地道な作業ですが、これを行なうことによって、これらの情報の防御策や管理方法を考え出すことができます。

なお、最初から完璧な作業ができなくてもかまいません。できることから少しずつ継続的に作業を続けるのがコツです。

その結果、超重要と判断されたファイルは、オフラインでメディアなどに保管するといった物理的防御をする必要があるかもしれません。そこまですななくとも、ある特定の人しかアクセスできないストレージに保管するという対策になるかもしれません。許可された人だけがパソコンに保管できるように取り決めることで守る情報もあるでしょう。

防御態勢を確立するために必要な作業ですが、これをするにによって、仮に攻撃を受けて破損または漏洩した場合に、どのような対処をすればよいかが明確になります。

② 自社の防御力を客観的に評価する

情報資産の洗い出しとともに、セキュリティに関する自己診断を

行ない、自社の防御力を客観的に評価することも必要です。IPAが発行している「5分でできる! 情報セキュリティ自社診断」などを使えば、簡易的に自社チェックを行なうことができます(図表2)。また、同時に下請けや外注先にもチェックを行なってもらうことを忘れてはいけません。

③ 情報セキュリティ方針を定め、関連規定を策定する

これらの作業を通じて得られた結果や課題を踏まえ、会社としての情報セキュリティ方針や関連規定をつくりまします。これもIPAで各種テンプレートを提供しているので、それを自社向けにアレンジすることで比較的簡単につくることができまします。

特に規定には、「社員を継続的に教育し続ける定め」を盛り込むことが重要です。いくら防御対策を充実させても、社員が犯人に騙されて無意識に武器を持ち込んでしまうケースが後を絶ちません。社員1人ひとりのセキュリティ意識の強化が、会社としての最後の砦となります。

④ 情報セキュリティ対策委員会をつくる

完成した方針や規定を使って社

図表2 情報セキュリティの自社診断表

診断項目	No	診断内容	チェック			
			実施している	一部実施している	実施していない	わからない
Part 1 基本的対策	1	パソコンやスマホなど情報機器のOSやソフトウェアは常に最新の状態にしていますか？	4	2	0	－1
	2	パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル（※1）は最新の状態にしていますか？	4	2	0	－1
	3	パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？	4	2	0	－1
	4	重要情報（※2）に対する適切なアクセス制限を行なっていますか？	4	2	0	－1
	5	新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？	4	2	0	－1
Part 2 従業員としての対策	6	電子メールの添付ファイルや本文中のURLリンクを介したウイルス感染に気をつけていますか？	4	2	0	－1
	7	電子メールやFAXの宛先の送信ミスを防ぐ取組みを実施していますか？	4	2	0	－1
	8	重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか？	4	2	0	－1
	9	無線LANを安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？	4	2	0	－1
	10	インターネットを介したウイルス感染やSNSへの書き込みなどのトラブルへの対策をしていますか？	4	2	0	－1
	11	パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？	4	2	0	－1
	12	紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫などに安全に保管していますか？	4	2	0	－1
	13	重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？	4	2	0	－1
	14	離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？	4	2	0	－1
	15	関係者以外の事務所への立ち入りを制限していますか？	4	2	0	－1
	16	退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていますか？	4	2	0	－1
	17	事務所が無人になる時の施錠忘れ対策を実施していますか？	4	2	0	－1
	18	重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにしていますか？	4	2	0	－1
Part 3 組織としての対策	19	従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか？	4	2	0	－1
	20	従業員にセキュリティに関する教育や注意喚起を行なっていますか？	4	2	0	－1
	21	個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？	4	2	0	－1
	22	重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？	4	2	0	－1
	23	クラウドサービスやウェブサイトの運用等で利用する外部サービスは、安全・信頼性を把握して選定していますか？	4	2	0	－1
	24	セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備していますか？	4	2	0	－1
	25	情報セキュリティ対策（上記1～24など）をルール化し、従業員に明示していますか？	4	2	0	－1
合計点			A	B	C	
A+B+C 合計点						

※1 コンピュータウイルスを検出するためのデータベースファイル「パターンファイル」とも呼ばれる。

※2 重要情報とは営業秘密など事業に必要で組織にとって価値のある情報や顧客や、従業員の個人情報など管理責任を伴う情報のこと。

（診断結果）

100点満点	入門レベルのセキュリティ対策は達成です。ステップアップを検討しましょう。
70～99点	ほぼ、できていますが、部分的に対策が不十分な点があるようです。
50～69点	対策が行き届いていないところが目立ちます。
49点以下	いつ情報流出などの事故が起きても不思議ではありません。

出典：IPA「5分でできる！情報セキュリティ自社診断」より一部を抜粋

(<https://www.ipa.go.jp/security/keihatsu/sme/guideline/5minutes.html>)

員教育の徹底を図るため、社内各部署からメンバーを選出して情報セキュリティ対策委員会をつくります。そこで社員教育や方針・規定の徹底、継続的な改善活動を展開させます。

また、この委員会は、実際に攻撃を受けてしまった場合の初動対策班としても、有効に機能させることができます。

なお、委員会をつくるときに「パソコンに詳しい社員を選ぶ」ことにこだわる必要はありません。技術的な知識や技量よりも、現場業務を熟知している中間管理職のほうが、この役割にふさわしい場合が多いものです。

万が一の際の対処法とは？

様々な防御策を凝らしても、攻撃の被害に遭う確率を下げられるだけで、ゼロにはできません。では、不幸にして攻撃を受けてしまったときは、どのように行動すればよいのでしょうか。

(1) 異変に気付いたとき

まず、社員が何かおかしいことに気がついた場合、たとえばパソコンのデータが使えなくな

った
・そもそもパソコンが立ち上がらない
・何やら脅迫めいた文言が画面に表示されている

・パソコンの動作がいつもよりもずっと遅い
・会社のホームページが改ざんされている

といった、攻撃による被害に気がついた場合、その社員がとるべき第一の行動は「ネットワークを切断すること」です。

パソコンの電源を切ってしまうと、攻撃の証拠が消える、再起動の時にさらに悪さをされる等の可能性があるので、あまりおすすめはできません。ネットワークを切断することによって、証拠を保全しつつ周囲のパソコンへの被害拡散を防止・軽減できる可能性が高まります。

第二の行動は、周囲の同僚や上司、そして情報セキュリティ委員会の窓口直ちに事実を伝えることです。最近のサイバー攻撃では同じ部署の複数の社員に同時に攻撃を仕掛けるケースが見られますので、周囲に注意を促すことはとても大切な行為となります。防火訓練では、火災に気がつい

た人は大声で周囲に火災を知らせ、初期の消火活動を組織的に行なうように訓練します。サイバー攻撃に対する初動は、それとまったく同じ考え方で行なうことが重要なのです。

(2) 被害の報告を受けたとき

サイバー攻撃による被害が社内でも報告された後、経営者や管理者がとるべき行動は、発生している事象の把握と被害調査です。この段階では技術的な知識が必要な場合もありますので、外部のセキュリティ専門家に対応を依頼することも選択肢となります。

「何が起きたかわからないから何もしない」という対応は絶対に避けるべきですし、憶測で動いてしまうことも禁物です。犯人の仕掛けた武器は社内はまだ存在しているかもしれない、密かに重要なデータを社外に送信している可能性もあるのです。

調査の結果によつては、社外や取引先への連絡・サイバー攻撃を受けた事実の公開が必要かもしれません。なかなか勇気が必要なことです。が、犯行は時々刻々と進行している可能性もありますので、先送りすることは事態の悪化を招くだけです。

なお、身代金を要求されるランサムウェアの場合には、お金を支払つても元に戻してくれるとは限りません。要求に応じることは避けるべき行動と言えるでしょう。

(3) 再発の防止

データやパソコンを復旧させ、いったん対策を実行して業務を再開できたとしても、必ず再発の防止をしなければなりません。技術的な検討については専門家の力も借りましょう。

社内の体制に弱点があったのであれば、体制や規定・各種ルールの見直しを行ない、再発防止に努めます。再発防止策は取引先からも求められますので、業務が再開できたからといって、気を抜いてはいられません。

サイバー攻撃を仕掛けてくるのは人間なので、犯人の攻撃意図を把握すれば、防御できることも多くなります。社員が一人となつて社内外の情報を守る。それができると、中小企業の経営者や管理者に求められます。

ぜひ一度、社内の見直しをするところから始めることをおすすめします。

すずき じゅんじ ベルケンシステムズ代表取締役。大手OA機器メーカーでハードウェアエンジニアを経験後、情報システム部、ネット経営戦略責任者等を歴任。独立後、製造業、サービス関係の企業のIT導入を支援する事業を展開する。