Management Insight
2022/9 増刊号
経営インサイト
管理部門担当者様にとって注目のテーマに気付きをお届けする

緊急企画 急務!

サイバー攻撃や通信障害に備えたBCPの策定

リスク対策.com編集長／
新建新聞社取締役専務
中澤幸介 氏

サイバー攻撃や通信障害にまつわるニュースがメディアを賑わせています。インターネットが普及し利便性が大幅に向上した一方で、インターネットへの依存性も高まり、サイバー攻撃や通信障害などによって、事業の継続が難しくなるほどの被害を受けるケースが頻発するようになりました。
サイバー攻撃や通信障害などの緊急事態に見舞われたとき、事業を止めないために、私たちはどのような取組みをすればよいのでしょうか?
今回は、事業継続計画のうち、ITに特化して、リスク対策.com編集長 中澤幸介さんに対応策などについてお話を伺いました。

各企業のBCP策定状況と拡大するサイバー攻撃の被害

災害などの緊急事態に陥ったときに被害を最小限にとどめ、事業を途切れさせることなく継続させるための計画が「BCP(Business Continuity Plan／事業継続計画の意)」です。

BCPに関しては、多くの企業がその必要性を認識しており、大企業を筆頭に取組む企業も増えています。内閣府が発表している「企業の事業継続及び防災の取組に関する実態調査」の令和3年度版によれば、調査対象となった大企業の85%以上がBCPを策定済、または策定中と回答しました。中堅企業についてはまだ52%にとどまってはいますが、取組む企業は増えています。

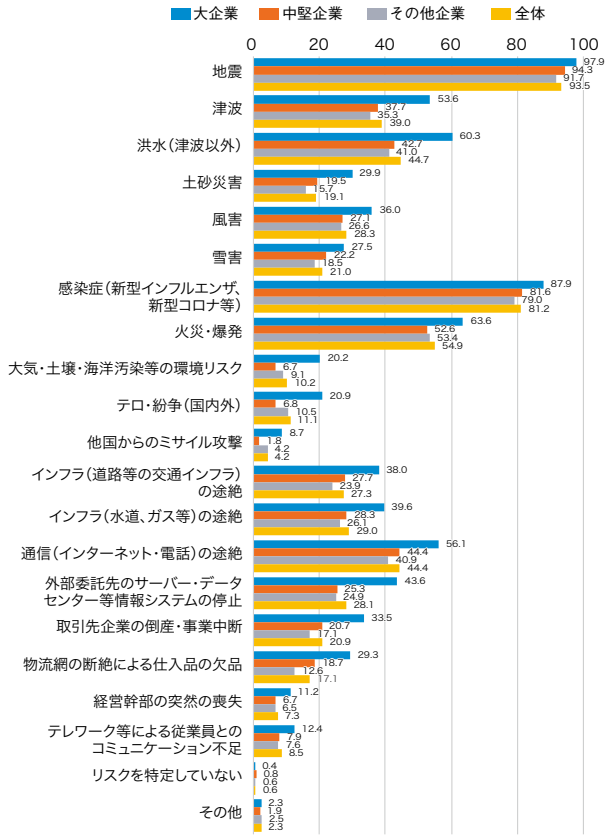
BCPを策定するにあたって80%以上の企業が「地震」や「感染症」についてリスクとして重視していると回答している一方で、「通信の途絶」をリスクと回答した企業は44・4%、「情報システムの停止」においては28・1%にとどまっていました(**図表1**)。目の前に降りかかってきた危機に対応する形でBCPを策定する傾向が強く、サイバー攻撃や通信障害などへの対策をとっている企業は非常に低いのが現状です。

しかし、震災や豪雨などの天災と同じく、サイバー攻撃や通信障害、特にサイバー攻撃は企業に壊滅的な被害をもたらしかねません。

サイバー攻撃の被害は増えている

2020年、大手ゲームソフトウエアメーカーのカプコンがランサムウェアによるサイバー攻撃を受け、35万件にも及ぶ顧客情報と取引先情報などの機密情報が盗まれました。ランサムウェアとは、感染したコンピュータをロックしたり、ファイルを暗号化したりすることによって使用不能に

図表1　重視しているリスク



出典：「令和３年度企業の事業継続及び防災の取組に関する実態調査」（内閣府）

したのち、元に戻すことと引き換えに「身代金」を要求するマルウェアです。

サイバー攻撃の被害に遭っているのはカプコンだけではありません。日立製作所やトヨタ自動車の協力会社である小島プレス工業など、名だたる大企業がサイバー攻撃の影響により被害に遭っています。表に出てくるのはほんの一部で、私たちの知らないところで多くの企業がサイバー攻撃の被害に遭っていることは容易に想像できます。

サイバー攻撃によって、会社が傾くおそれすらある

企業が被る被害は、決して少なくありません。ウイルスに感染したパソコンの復旧または破棄、セキュリティシステムの再構築などのコストのほかにも、考えておかなければならないのが罰金や被害を受けた人への損害賠償です。

２０２０年に個人情報保護法が改正（施行は２０２２年４月）されましたが、不正アクセスなどによって顧客情報などが流出した場合、企業には、個人情報保護委員会と情報を漏洩された個人に対して報告義務が課せられることとなり、こうした義務に違反した場合には、最大１億円の罰金が科されることが定められました。

ウイルス感染による情報流出は、企業としては「自分も被害者であるはずだ」と言いたくなるものです。確かに、企業側に一切の落ち度や過失がないと認められれば、企業が負う責任はかなり軽減されるでしょう。

しかし、企業側に本当に落ち度がなかったのか、過失がなかったのかという評価は年々厳しくなっています。これほどまでにサイバー攻撃の脅威が高まっているにも関わらず、基本的なセキュリティ対策すら講じておらず「まさかこの環境下で漏洩するとは思っていなかった」というような抗弁が認められる可能性は非常に低くなっていると考えられます。

中小企業の課題

大企業のなかにはサイバー攻撃などのＩＴ関連の事象も想定して、ＢＣＰを見直している企業もあります。しかし、中堅企業、中小企業においては、その対策はほとんどできていないと思われます。

ただ、見てきたとおり、万が一何かあったときの被害の大きさを考えれば、企業規模に関わらず、早急にＢＣＰのなかにＩＴに関連した対策を含めなければなりません。

２０２２年３月、経済産業省が、サイバーセキュリティ対策の強化について注意喚起を行うと明言しました。経済産業省がこのような警鐘を鳴らすことは、非常に珍しいことです。裏を返せば、国が見過ごせないほど、サイバー攻撃の被害が甚大なものになっている証ともいえるのです。

ＢＣＰがサイバー攻撃に奏功した例
徳島県つるぎ町立半田病院

このように災害や感染症、あるいはサイバー攻撃なども想定して、さまざまな不測の事態に対応できるＢＣＰを策定していくことが求められていますが、多くの企業がＢＣＰを策定することをゴールにしていると感じます。しかし、ＢＣＰは作って終わりではありません。ＢＣＰに継続的に取組むことが重要なのです。

また、予防については対策を立てられていても、実際に被害に遭ったときの対策については無策な企業も多く見られます。ＢＣＰの本質は、どのような状況になっても事業を途絶させずに継続させることです。だから、「サイバー攻撃の被害に遭わないように注意喚起をする」などの予防対策に加えて、「もしも感染してしまったらどうするか」という、被害を受けたときの対策も必要なはずです。

ここで、サイバー攻撃への備えはできていなかったものの、災害への備えとしてＢＣＰを策定していたために事業を復活させられた例をご紹介します。徳島県つるぎ町立半田病院の事例です。

半田病院では、２０２１年10月末にランサムウエアのサイバー攻撃を受け、電子カルテなどが閲覧できなくなりました。

幸い個人情報の流失は避けられたようですが、通常診療を再開できたのは、サイバー攻撃を受けてから2カ月以上のちの2022年1月でした。

半田病院では、事件が発生してすぐに対策本部を立ち上げるなど、迅速な動きが見られました。いわゆる初動対応の手順を、BCPのなかで決めていたのです。

サイバー攻撃を受けたとき、対応としては復旧作業や原因の特定、全容の解明など、さまざまなタスクが生じます。半田病院は事業継続のための基本方針を、①今いる入院患者を守る、②外来患者は基本的に予約患者のみ、③電子カルテ復旧に努める、④皆で助け合って乗り切ろう！と定め、更に、攻撃者に身代金を支払わないことや、データが完全に復旧する保証がないことを確認し、優先順位を付けて復旧業務に取組みました。

攻撃を受けたのは10月31日の未明です。システムに異常を感知した当直看護師はすぐにシステム担当者に連絡する対応をとっています。半田病院は同日朝10時には災害対策本部を設置しており、BCPに基づく対応を開始しているのです。更にいえば、同日に記者会見まで行っています。

ここまでの迅速な動きは、ただBCPを策定していただけでは不可能です。おそらく、普段から「自分が当事者になるかもしれない」という意識を持って何度も訓練を行っていたおかげで、当日の当直医師を含めた病院関係者の一人一人が、事業継続のために動けたのではないでしょうか。だからこそ、復旧に向けた初動がスムーズに進み出せたといえるでしょう。

重要な事業が依存しているリソースを見つけることも大切

BCPにおけるITや通信対策においては、「緊急事態に陥ったとしても、社内のこの事業だけは止めてはならない」という優先順位付けと、その業務を遂行するために不可欠な経営資源を洗い出し、その経営資源が万が一使えなくなった場合にどう主要事業を継続するのか、という代替策を考えておくことが極めて重要です。

例えば、2022年にKDDIの大規模な通信障害がありました。障害が復旧するまでに3日を要し、最大で3900万件以上の回線に影響を及ぼしましたが、仮に社用携帯の回線が全てKDDIに依存していたとしたら、事業の継続にも大きな影響が出ていたわけです。

経営資源の洗い出しが平時にできていれば、本当に重要な業務に使われている契約回線だけは分散させるなどの予防策をとることができます。この洗い出しと代替策の検討ができてない企業も多いように感じます。

今後、同様の障害が起きないように通信各社は何らかの対策を講じるはずですが、その対策だけでひと安心だと考えるのは早計です。通信各社による対策がとられようがとられまいが、企業は万が一に備えて自ら対策を講じておかなければならないのです。

一人一人の意識を高めることが何よりも重要

実効性のあるBCPを構築するうえで何よりも大切なことは、社員一人一人が危機感を持ち、自主的に動けるようにすることです。そのためには、従業員を育てる体制が必要になります。災害などの被害に遭った際に真っ先に対応にあたるのは現場スタッフです。セキュリティ対策も同じです。

社員に危機感がなければ、厳しいルールを設定しても守られません。仮に「USBメモリーは使用禁止」というルールを定めたとしても、「手間だから」「バレないようにすればいい」というような意識でUSBメモリーを使う人が必ず出てきます。更には、「USBメモリーがダメでもSDカードならいいだろう」と独自の判断で動く社員も出てくるでしょう。

ルールを徹底させるためには、経営者をはじめとした全社員のリテラシーを高めることが不可欠です。

まずは体制を整える

現場の従業員の意識を高めていくには、まず体制をしっかり整えることです。社長が「BCP担当事務局」を設置し、各事業部でもBCP推進役を決めます。もちろん、ITに関してはある程度の能力があったほうがいいですし、BCP担当事務局のITリテラシーが低いなら、ITを管理している担当者をBCP推進役に入れることが肝要です。

そのうえで、毎月のように定期的にBCP委員会を行います。例えば、1月は方針の見直し、2月は重要業務の見直し、3月はリスク分析の見直し、4月はボトルネック資源の見直し…と。2年目以降も、同じ頻度で同じ作業を行いながら、BCPの策定プロセス一つ一つを毎年見直していきます。そして年数回は訓練を行う。その訓練も、災害だけでなく、サイバー攻撃などを取り入れてみる。どのような手順で、誰が、どこに、何を連絡すべきか、システムが使えない期間をどう凌ぐか、情報漏洩に対してどのように謝罪広報をするかなども検討します。大変な作業に思えるかもしれませんが、委員会は、月に1回、30分程度でもいいと思います。重要なのは、継続的に見直しを続けていくことなのです。

これを、「総務部にでもやらせておけ」という程度の考えで押し付けているなら、おそらくBCPは破綻するでしょう。したがって、BCP担当事務局には本当に

社長が信頼できる股肱の臣を充てることが絶対条件です。逆に、それだけ社長の信頼を得ている人なら、IT問題も含め、必ず解決策を見つけられるはずです。そこまでしてBCP対策をする覚悟が社長にあるかが問われているのです。

繰り返しになりますが、BCPは策定して終わりではありませんから、ブラッシュアップのためにもアンテナを張っておきたいところです。私たちが発行している「リスク対策.com」の無料メルマガを購読いただき、BCPやサイバー攻撃に関する記事を拾い読みしていただくのもいいですし、ニュースを購読するのも有益です。

特に同業者の事例については、対応まで含めて追いかけることがポイントです。

BCPは、トレーニングと同じ

BCPとは、企業の生命力を鍛えるためのトレーニングだと私は考えています。BCPは策定して終わりではありません。むしろ大切なのは、策定後の動きです。筋トレをして身体を鍛えるように、継続してBCPに取組んでいただきたいと考えています。

リスク対策.com編集長／
新建新聞社取締役専務
中澤幸介 氏
2007年に危機管理とBCPの専門誌リスク対策.comを創刊。数多くのBCPの事例を取材。内閣府プロジェクト「2013年度事業継続マネジメントを通じた企業防災力の向上に関する調査・検討業務」アドバイザー、「2014年度～2016年度地区防災計画アドバイザリーボード」、2017年熊本地震への対応に係る検証アドバイザー。著書に「被災しても成長できる危機管理『攻めの』5アプローチ」「命を守る教科書 LIFE」などがある。

BCPの策定とその後の定期的な取組みは、自社だけで行うよりも、外部の協力を得たほうがスムーズにいきますし、結果的にコストもかかりません。ここでは、ITに関するBCPを策定するにあたってたたき台となるもの、定期的にチェックを受けられる機関について紹介します。

プライバシーマーク制度

▶https://privacymark.jp/

個人情報について適切な保護措置を講ずる体制を整備している事業者等を評価して、その旨を示すプライバシーマークを付与し、事業活動に関してプライバシーマークの使用を認める制度。2年ごとに更新審査があり、定期的なチェックが可能。

ISO 22301（事業継続）

▶https://www.jqa.jp/service_list/management/service/iso22301/

さまざまな脅威から事業を守り早期の復旧と再開を実現するためのマネジメントシステム規格。ITだけでなく、自然災害や感染症などのリスクも含めた脅威に備えて、効率的かつ効果的な対策を行うための包括的な枠組を示している。1年に1回の維持審査、3年目には更新審査を受ける必要がある。

ISO/IEC 27001（情報セキュリティ）

▶https://www.jqa.jp/service_list/management/service/iso27001/

さまざまな情報資産を守り有効に活用するためのマネジメントシステム規格。1年に1回の維持審査、3年目には更新審査を受ける必要がある。

レジリエンス認証

▶https://www.resilience-jp.biz/certification/

自らの事業継続力を高めることに積極的に取組んでいる団体を認証してその取組みの普及を図ることを目的とした認証制度。中小企業者の方が防災に資する施設等の整備を行う際に、日本政策金融公庫による制度融資「社会環境対応施設整備資金」の利用が可能となり、優遇金利が適用されるなどのメリットがある。

本誌に掲載の記事は2022年8月1日時点での情報を基に作成しております。

発行：株式会社 星和ビジネスリンク
本社：〒108-0014　東京都港区芝 4-1-23　三田NNビル4階
TEL：(03) 5439-2370（大代表）　FAX：(03) 5439-2371

●お届けいたしましたのは

NISSAY
（生 22 - 4271, 法人開拓戦略室）