サイバー面だけでなく、物理的な脅威も:

2018年に心配される事業継続計画（BCP）のリスクトップ10

http://techtarget.itmedia.co.jp/tt/news/1806/21/news07.html

事業継続と災害復旧に対するリスクは、時代によって変わらないものもあれば、深刻化しているものもある。人々が最も懸念しているリスクとは何だろうか。

2018年06月21日 05時00分 更新

[Paul Kirvan, TechTarget]

関連キーワード

BCP（事業継続計画） | サイバー攻撃 | ディザスタリカバリ

Business Continuity Institute（BCI）は、ここ数年、英国規格協会（BSI：British Standards Institution）のサポートを受け、毎年「BCI Horizon Scan Report」を発行している。この報告書には、事業継続計画（BCP）の重要なトレンドと進展状況が掲載されている。この報告書に記載されるBCPのリスクは一部変わらないものもあるが、テクノロジーの発展やビジネスのグローバル展開が進むにつれて深刻化しているものもある。

近年、サイバー攻撃やデータ侵害などの脅威は、ネットワーク障害などのBCPや災害復旧（DR）への従来の脅威よりも大きな騒ぎを引き起こしている。気象災害は以前から1つの懸念事項ではあったが、地球温暖化の影響でその頻度が高くなった。

2018年度の報告書では、BCIは76カ国でアンケートを行い、657人から詳しい回答を得た。このアンケート調査では、BCP／DRの脅威における現在のトレンドを示すとともに、回答者からの情報を基に脅威の深刻度とそれに対する現状の対策を探っている。

本稿では、この報告書で特定されているBCPのリスクトップ10を紹介する。

併せて読みたいお勧め記事

DR対策製品のトレンド

- どれを買う？　クラウドを活用したバックアップ／DRに役立つ製品を一挙紹介

- 「ディザスタリカバリー」（DR）の注目トレンド　GDPR対策からエージェントレスまで

DRの戦略を考える

- ランサムウェア最悪の大流行に備えるバックアップと災害復旧（DR）戦略
- バックアップ／DRで「システムの切り替え先にクラウドを使用する」8つの方式
- 自然災害からデータを守るIT緊急時対応とは、米国の「反省点」から学ぶ

- サイバー攻撃

BCIが発行したここ数年の年次報告書では、サイバー攻撃とサイバーセキュリティへの脅威をリスクに挙げた調査回答者が最も多かった。調査に参加した多くの回答者は、尽力はしているものの、サイバー攻撃のリスクはいまだ解消されていないと危惧している。主な懸念事項は、サービス拒否攻撃、フィッシング、ウイルスだった。

- データ侵害

サイバー攻撃とほぼ同数の調査回答者が、データやデータベースをはじめ、重要なシステムへの不正アクセスへの懸念を示している。データやシステムの損傷、破損、破壊、データへのアクセス拒否、ランサムウェアが脅威として挙げられた。

- ITシステムと通信の予定外の停止

復旧技術が向上し、クラウドベースシステムが使用されているにもかかわらず、重要なデータや音声システムが損傷する可能性が、依然として調査回答者の大きな懸念になっている。

- 停電

2017年に発生した複数のハリケーンや近年の米国北東部での大雪により、BCPの主なリスクと脅威を示したリストの多くで停電が上位に押し上げられている。停電への基本対策は、バックアップ電源システム（ディーゼルや天然ガスによる発電、バッテリー、無停電電源など）だ。
水道、ガス、廃棄物処理、蒸気などの公共サービスも停止する可能性を考慮する必要がある。

- 悪天候

原因が地球温暖化にあるかどうかはともかく、深刻な悪天候が発生する頻度が高まっているようだ。暴風雨も激しさも増しているように思える。例えば、2017年に発生したハリケーンは、個人資産や公共インフラを合わせて、数十億ドルの損害を引き起こした。

- テロ行為

銃乱射事件、凶器に自動車を用いたテロ、起爆装置を使った爆破テロが連日トップニュースを飾っている。調査回答者は、以前の報告書に比べて、こうしたテロ行為の影響への懸念を強めている。

- セキュリティインシデント

サイバー攻撃とは異なり、BCPへのリスクには、建物への不正侵入、建物や施設の破壊、詐欺行為、民衆による動乱など、セキュリティに関する物理的な脅威も含まれる。

- 火災

どれだけ予防や対策を講じても、火災は起こり得る。調査回答者は最も重要な火災対策の1つに、すぐに使える場所に消化剤を充填（じゅうてん）した消火器を設置し、その場所に適切な目印を付けておくことを挙げる。火災検知、消化システムは、消火器と同様、地域の建築基準で必須要件になっているのが一般的だ。

- サプライチェーンの混乱

上流工程と下流工程のどちらで混乱が生じても、サプライチェーンへの損傷は重大な懸念事項になる。企業に多種多様な影響を及ぼすため、サプライチェーンの継続性は、恐らく、BCP／DR計画チームが対応する最も重要な取り組みの1つだ。インターネットを使ってサービスを提供したり、製造活動を行ったりしていない企業でも、サービスを動かすための機能性の高いインターネットはやはり必要だ。

- 輸送ネットワークの混乱

製品の製造を終えたら、多くの異なる販売経路を利用して、完成した製品を配送する。こうした販売経路が利用できなくなったら、注文に対応できなくなる。出荷／配送の広域ネットワークを持たないAmazon.comのような企業を想像してほしい。こうした企業の活動は完全に停止するだろう。

報告書を詳しく読むと、BCPのリスクや、BCP／DRに影響を及ぼす課題と対策に関する多くの調査と分析が明らかになる。完全な報告書はBCIのWebサイトに掲載されている。

関連記事

どれを買う？　クラウドを活用したバックアップ／DRに役立つ製品を一挙紹介

「ディザスタリカバリー」（DR）の注目トレンド　GDPR対策からエージェントレスまで