｜第5回｜ クライシスの要因ごとに3つの「R」を考える（その1）

デロイト トーマツ
パートナー 麻生裕貴 CBCP, CISSP 尾嶋博之　シニアマネジャー 白濱直哉

Ⅰ はじめに

本連載の前半（第１～４回）では，クライシスマネジメントの要点を「Readiness（計画・準備プロセス）」，「Response（対処プロセス）」，「Recovery（回復プロセス）」の３つのRの観点から解説した。後半の４回では，クライシスのきっかけとなるインシデントの種類ごと，また，国・地域ごとの特性をふまえて３つの「R」を考える。本稿では，自然災害，サイバー攻撃，不正・不祥事，という３種類のインシデントを対象とする。

Ⅱ 自然災害

地震大国の日本では「クライシス」といってまず思い浮かぶのが自然災害ではないだろうか。ここでは，自然災害の特徴を整理し，その対処について述べる。

1　自然災害の特徴

自然災害とは，地震，津波，噴火，暴風，豪雨，豪雪，洪水，高潮等，さまざまな自然現象が原因となり，人命をはじめ各種施設・設備等に影響を及ぼす被害のことで，時として企業経営や社会活動に甚大な影響を与えうる脅威となる。その主な特徴は，原因となる自然現象の内容により多少異なるが，おおむね次のとおりである。

⑴　自然現象はコントロール困難である

気象の操作など，自然現象をコントロールしようという試みは研究レベルで検討されてはいるものの，現在のところ現実的なものはない。ましてや一企業でどうにかなるようなものでもない。自然災害の発生自体を防ぐことは困難であることの認識が必要である。

⑵　被害が広域に及ぶ

一般的に自然災害の被害は広域に及ぶため，社会全体に甚大な影響を与えるケースが少なくない。社会システムや経済システムの広範囲に影響が及ぶため，一企業の努力だけでは太刀打ちが難しいことも多いが，企業としてできること，すべきことを明確にし，対応を検討することが必要である。

⑶　突発的に発生するものと徐々に発生するものがある

突然発生する地震や長期の降雨による洪水のように，発生の仕方や被害の出方は，自然現象の内容によってさまざまである。徐々に被害が出る災害であれば，状況を見ながら身構え，備えを施していくこともできるが，突発的に発生する災害は，被害を少しでも減らすべく発生前から一定の準備をしておくことが必要である。

⑷　地域により異なる

自然現象は地域に依存する。日本では地震が多いが，フランスのように地震がほとんどない国もある。タイでは毎年のように洪水が発生する。北米では東海岸においてはハリケ

ーンを想定する一方で，西海岸では地震を想定する，というように同じ国内であっても地域によりそれは異なる。日本では情報が少ない，現地の肌感覚に欠ける等により海外の自然災害を想定しづらい場合もあるので，海外拠点を有する企業や海外企業との取引が多い企業は注意が必要である。

2　自然災害への対処

自然災害への対処は，本連載前半で解説したクライシスマネジメントの３つの「R」が基本になるが，中でも最初のReadinessが特に重要となる。自然災害では前述のような特徴から，クライシス発生後の企業への被害の範囲や程度が想定しづらく，発生後に対応するのでは「時すでに遅し」ということになる。できる限り事前にクライシスを想定し，クライシス発生後の迅速な対応や各種判断を容易にすることで，その影響を低減するReadinessが必要である。Readinessでは，クライシスに備えた「計画」を立て，その「計画」に基づくシミュレーションをすることは本連載第２回で述べたとおりである。

また，自社への対処だけを考えれば良いというものではないことを付け加えておきたい。自然災害は被害が広域に及ぶことから，地域連携や社会貢献といった観点での取組みも重要となる。災害発生時に地域社会に迷惑をかけないため，火災防止や化学薬品漏えい防止等の安全対策を実施する必要があるし，自社の復旧においては資機材の搬入や工事の騒音など，周辺地域の理解や協力が必要になる。また，企業にとって，顧客や従業員が地域の人々である場合も多く，自社だけでなく地域全体の復旧を考えなくてはならない。つまり，地域を構成する一員として，企業にも地域や社会への積極的な貢献が求められているのである。災害対応となると総務等の特定の部門に任せる企業も多く見受けられるが，クライシスマネジメントは経営陣が中心となり積極的に取り組むべき事項であるといえるのではないだろうか。

Ⅲ　サイバー攻撃

筆者は20年近くサイバーセキュリティ業界に身を置くが，不幸なことに，昨今ではサイバー攻撃を発端としたインシデントの話題に欠くことがなくなってしまった。近年においてはサイバーインシデントによる被害が大きくなる傾向にあり，金銭的被害だけではなく責任者が辞任するケースも増えている。サイバークライシスと聞いて思い浮かぶ事例のひとつに，数年前に発生した教育大手の情報漏えい事件があるが，本インシデントでは取締役が２名引責辞任している。

本稿執筆中にも世界規模のサイバーインシデント[1]が発生した。英国の病院をはじめとした世界中の多くの組織でシステムが利用できなくなり，事業継続が困難になったケースが報道された。遠隔医療システムや自動運転車，スマートホーム等，生活をより便利にするためのITの進化は，人命をも脅しかねないサイバークライシスの発生と表裏一体であると言っても過言ではないだろう。

1　サイバー攻撃の特徴

前述した自然災害と大きく異なるのは，サイバー攻撃は悪意のある者が人為的に起こしているということと，攻撃そのものやインシデントを目で見ることが困難ということ，イ

[1] WannaCryと呼ばれるランサムウェアによるインシデント。ランサムウェアとは，コンピュータのデータを暗号化する等によりシステムの利用を制限し，その解除のために身代金（Ransom）を要求するマルウェア（悪意のあるソフトウェア）である。

ンターネットに国境はなく地域による差はないということである。これらの特徴から，攻撃の予兆はおろか，巧妙化した攻撃や発生したインシデントの発見も困難なものとなっている。また，インシデントの原因となるシステムの脆弱点を事前に把握し対策することで，サイバー攻撃による被害を未然に防ぐことが可能であることも特徴と言える。

2　サイバー攻撃への対処

サイバーインシデントを未然に防ぎ，発生したインシデントがクライシスに発展しないよう対処する組織として，CSIRT（Computer Security Incident Response Team）がある。クライシスマネジメントを行うための３つの「Ｒ」を担当する組織であり，大手企業を中心に構築が盛んになっている。

それぞれの「R」のサイバー特有の事項について述べると，まずはReadinessでは，攻撃が多様化しシステムが複雑化していることから，情報漏えいというひとつのインシデントでも複数の計画や準備が必要となる。情報を分散し保管していることが多く，攻撃の手法や経路がさまざまであるためである。可能な限りのインシデントシナリオを想定したシミュレーション（サイバー演習）を行い，対処手続の実効性を向上させる必要がある。

次にResponseだが，多くの場合で，原因や影響範囲を確認するためにデジタル・フォレンジックという高度な技術スキルが必要な調査が発生する。自組織で対応するのは困難であり，Readinessの段階で複数の専門業者を選定しておくことが求められる。組織において必要となるのは，高度な調査が必要な事象か判断する能力と，専門業者が実施した調査が適切なものか判断する能力である。

最後のRecoveryで，システム復旧と再発防止を行い終息宣言をするのだが，インシデントの直接原因を対策するだけではなく，他のシステムでの同様の問題や，他に似たような問題で同様のインシデントが発生するリスクがないか調査し，対策することも必要となる。

サイバー攻撃は目に見えないため，誰が何をもってどう判断するのかが難しい。判断に必要な情報を適時に収集し，時にはクリティカルなシステムの停止をも決定し実行するトップダウンでの対応が重要となる。

Ⅳ　不正・不祥事

粉飾決算やデータの改ざん・偽造等，不正への対処についても十分な不正リスク管理体制を構築し不正防止，早期発見に努め，また端緒を発見したらその潜在的影響を過小評価せずに迅速かつ適切に対応することの重要性は，他のインシデントと同様である。

1　まずは実態の把握から

Responseで重要なのは，まずは事件の全容解明で，それは事件の５Ｗ１Ｈをすべて明らかにすることである。これが後にとるべきあらゆるアクションの基礎となる。何が起こり，影響額はいくらかという無機質な調査ではなく，誰が，誰と，なぜ，などを含めて明らかにしなければならない。

不正実行者のみならず組織のどの層から指示があったのか，明確な指示はなくとも不正の認識はどの層まであったのか等，トカゲのしっぽ切りで良しとしないためには，遠慮なく徹底してこれらを追求できる調査体制を敷くことが肝要だ。そのためには調査主体の設計がカギとなる。調査主体と調査対象者（なんらかの関与の可能性のある潜在的な対象者を含む）の厳密な区分をしない，混然とした社内調査体制を見かけることがある。このような体制で調査に臨むのは論外である。

次に，発覚した事件以外に同様の事象がな

いか徹底的に膿を出し切ることが重要だが，発覚事象の全容解明がこの「膿出し」のための基礎となることは言うまでもない。

2　真の原因追及と是正の徹底

Responseの最終段階で調査委員会などが報告書をまとめ，原因分析と是正の提言などを行うことが一般的な実務になっているが調査の大部分の時間は事件の実態解明にあてられ，原因分析と是正提言は，実態解明の過程で把握できた事実や事象の範囲で行わざるをえないのが実情である。十分に真因までたどり着いていない，この段階での原因分析と是正提言を基にした是正策は，表面的なものとなりがちである。

よって，次のRecoveryでは，調査報告書等で分析された原因と提言された是正策に脊髄反応するのではなく，それらを十分に吟味しつつも，事件発生の真の原因を徹底して追求し，その根本原因を除去する対策を取らなければ再発のリスクは低減できない。

データ偽装や粉飾決算等の事件でも，根本原因として事業自体に課題を抱えていることも多い。たとえば，創業の事業であるとの理由で事業の実態を把握するためのメスが入れられることもなく長期間粉飾が重ねられた事例や，新規事業の目玉としての期待からデータ偽装に走ってしまった例など，事業の本当の姿から目を逸らせていたこと，あるいは実態が見える仕組みをもっていなかったことが重大な原因であった例も多々ある。その場合，事業ポートフォリオの見直し，事業戦略・計画の見直し，およびその実行が答えとなることもある。こういった場合，不正防止のためのガバナンスやコンプライアンスの強化，教育などによる企業風土改善といった対策だけでは十分ではないのである。

事件そのものの影響に加え，事業計画の見直し等も資金計画に大きく影響を及ぼすことがある。損害賠償等の費用の影響はもちろんだが，問題製品の製造停止と工場の長期閉鎖や広範囲の製品回収などといった意思決定においても，企業体力を勘案した資金繰りを見据えた舵取りが必要になる。

最後に，これら一連の方針や施策についての積極的な開示やステークホルダーとのコミュニケーション戦略は必須である。Recoveryステージでは，徹底した是正と安全宣言を前提として，レピュテーション回復，ブランド再構築という視点は欠かすことができない。

＊　　＊　　＊

麻生裕貴（あそう　ゆうき）
米国公認会計士。デロイトのニューヨーク事務所にてグローバル企業の監査業務を経験後，事業会社のCFO職などを経て，現在はデロイト トーマツファイナンシャルアドバイザリーのクライシスマネジメント事業部パートナー。国内外の企業への係争支援，不正調査などフォレンジックアカウンティング業務全般に精通している。

尾嶋博之（おじま　ひろゆき）
通信事業者，通信機器メーカーを経て，2005年にデロイト トーマツに入社。さまざまな業種・業界の企業・組織に対する，BCM/BCPやクライシスマネジメント/リスクマネジメント関連のコンサルティングに従事。BCP策定やBCM構築・導入支援をはじめ，BCP訓練支援，グローバルリスクマネジメント体制構築・導入支援，危機管理態勢強化支援などの案件を多数手掛ける。

白濱直哉（しらはま　なおや）
公認情報システム監査人。大手情報セキュリティ会社を経て，デロイト トーマツに入社。一貫してサイバーセキュリティ関連のコンサルティング業務に携わる。技術的なセキュリティ対策やインシデント対応，不正調査を中心に，近年ではサイバー人材に関するコンサルティングやサイバービジネス立ち上げ支援も手がけている。東京電機大学国際化サイバーセキュリティ学特別コース外部講師も勤める。