2018.03.01

CSR・ERM トピックス ＜2017 年度第 12 号＞

本誌は、CSR（企業の社会的責任）および ERM（統合リスクマネジメント）に関連する諸テーマについて、国内・海外の最近の動向や企業の抱える疑問などについて紹介・コメントした情報誌です。「コーポレート・ガバナンス」「リスクマネジメント」「コンプライアンス」「人権」「労働慣行」「環境」「品質」「CS（顧客満足）」「社会貢献」「CSR 調達」「情報セキュリティ」等、関連する様々なテーマを取り上げます。

国内トピックス：2017 年 12 月～2018 年 1 月に公開された国内の CSR・ERM 等に関する主な動向をご紹介します。

＜労働慣行＞

○厚生労働省、「柔軟な働き方に関する検討会」報告書を公表。テレワーク、副業・兼業について方針示す

（参考情報： 2017 年 12 月 25 日付　厚生労働省 HP）

12 月 25 日、厚生労働省の「柔軟な働き方に関する検討会」は検討結果をまとめた報告書を公表し、雇用型テレワーク、自営型テレワーク、副業・兼業等についての指針を示した。今後、同省は、これらのテーマに関するガイドライン等の策定・改定を実施する。

1.「柔軟な働き方に関する検討会」

安倍首相の私的諮問機関「働き方改革実行計画」が、2017 年 3 月 28 日に策定した「働き方改革実行計画」を踏まえ、具体的な法整備を行うために厚生労働省に設置されたもの（座長：松村茂　東北芸術工科大学教授、日本テレワーク学会会長）。2017 年 10 月から計 6 回開催された。

2. 同報告書の提言

（1）テレワーク

柔軟な働き方に資する一方、労働時間の長時間化等につながる可能性を指摘した。

雇用型テレワークについては、労働時間管理を企業が適切に行うことが重視されており、業務の開始時間や終了時間の報告、移動時間の労働管理上の取り扱い、フレックスタイム制、事業場外みなし労働時間制、裁量労働制におけるテレワークの扱いについても考え方を示した。また、これに関連して「情報通信技術を利用した事業場外勤務の適切な導入および実施のためのガイドライン」の原案が示された。

自営型テレワークについては、トラブルを未然に防止するため、契約の段階で詳細を決めておくこと等の対策を示した。また、「自営型テレワークの適正な実施のためのガイドライン」の原案を提示した。

（2）副業・兼業

副業・兼業を認めていない企業が多い現状を踏まえ、労働者が主体的に自らの働き方を選択できるよう、副業・兼業を促進することが重要とした。その上で、厚生労働省で示しているモデル就業規則の規定を副業・兼業を認める内容に改めることを表明した（ただし、労務提供上の支障や企業秘密の漏洩が生じる場合等は除く）。副業・兼業の懸念事項としては、主業務および副業務双方の企業が実施する労働時間・健康管理、労災保険、雇用保険等の適用基準や、長時間労働などが挙げられている。

＜SDGs＞

〇SDGs 推進本部が、第１回「ジャパン SDGs アワード」の結果を公表

（参考情報：2017 年 12 月 26 日付　同推進本部 HP）

SDGs 推進本部*は、第１回「ジャパン SDGs アワード」（以下、本アワード）の受賞企業・団体を公表した。

本アワードは、SDGs 達成に向けた優れた取り組みを行う企業・団体を選定し表彰する制度で、今年度新たに創設されたもの。評価項目は、「普遍性」「包摂性」「参画型」「統合性」「透明性と説明責任」の 5 項目で構成され、280 を超える応募者の中から、12 企業・団体が第１回受賞者として選定された。

大賞にあたる「SDGs 推進本部長（内閣総理大臣）賞」は北海道下川町が受賞（取り組み概要は以下参照）。また、「SDGs 推進副本部長（内閣官房長官）賞」は、特定非営利法人しんせい、パルシステム生活協同組合連合会、金沢工業大学が、「SDGs 推進副本部長（外務大臣）賞」はサラヤ株式会社、住友化学株式会社が受賞した。

◇内閣総理大臣賞受賞者である北海道下川町の取り組み

【活動概要】

- 下川町は人口 3,400 人、高齢化率約 39%の小規模過疎地域かつ少子高齢化が顕著な「課題先進地域」。
- 町の憲法とも言われる「下川町自治基本条例」に「持続可能な地域社会の実現」を位置づけ、①森林総合産業の構築（経済）、②地域エネルギー自給と低炭素化（環境）、③超高齢化対応社会の創造（社会）に、統合的に取り組んでいる。
- 具体的には、持続可能な森林経営を中心に、適正な木材、木製品の生産と供給、森林の健康や教育への活用、未利用森林資源の再エネ利用、再エネ熱供給システムを核としたコンパクトタウン等を推進。
- これら取組を通じて、「誰もが活躍の場を持ちながら良質な生活を送ることのできる持続可能な地域社会の実現」を目指している。

SDGs 実施指針における実施原則（本アワード評価基準）	
普遍性	小規模自治体や国内における地方創生モデルになり得る。
包摂性	既住民のみならず、女性を始め多様な人々が移住。
参画型	バイオマスボイラ導入による燃料費削減効果額を基金に積み立て、社会的立場の弱い人への支援を実施。
統合性	バイオマス原料製造による熱供給システムを核としたコンパクトタウン化などにより統合的に解決。
透明性と説明責任	進捗管理機関及び内閣府設置の評価委員会から評価を受けるとともに、評価を踏まえた取組の軌道修正。

（同推進本部 HP「受賞団体の取組紹介」より引用）

◇全受賞団体の取り組み紹介（特別賞受賞の 6 企業・団体等を含む）

https://www.kantei.go.jp/jp/singi/sdgs/japan_sdgs_award_dai1/siryou2.pdf

（同推進本部 HP より）

*　SDGs 推進本部

持続可能な開発目標（SDGs）に係る施策実施について、関係する行政機関が連携し効果的な推進を図る

ため、内閣総理大臣を本部長、全国務大臣を構成員として設置した組織。現在までに計 4 回の会合が開催されており、平成 29 年 6 月の第 3 回会合にて、「ジャパン SDGs アワード」の創設が決定された。

＜CSR＞

〇花王が被災時を想定した清潔情報サイト「そなえーる」を開設

（参考情報：2018 年 1 月 12 日付 同社 HP）

花王は 1 月 12 日、災害時を想定した普段からの備えや、災害時に役立つ知識、心がけたい清潔情報などを紹介する自社の公式ウェブサイト「そなえーる」を開設した旨を発表した。

同社グループは、これまでの被災地支援活動を通じて、地震や異常気象などの災害時に、家族や生活等を守るためには、「日ごろから備える防災」が重要であるとの認識の下、社内プロジェクトを組成。同プロジェクトを通じて、有識者へのヒアリングや被災した同社グループ社員へのアンケートなど、様々な調査と検討を重ねてきた。今般、その結果を踏まえて、同社グループの事業活動の原点である「清潔」をテーマに、防災対策に役立つ物品や工夫などの有用な情報を提供することを決定した。

2018 年 1 月時点の「そなえーる」への掲載情報概要は以下の通り。今後も継続的に更新される予定。

区分	「そなえーる」への掲載情報の概要
普段からの備え	すぐに持ち出せるように予め準備しておきたい非常用持ち出し品、家庭内での備蓄（食品以外の備蓄品、食品の備蓄方法）、実際の災害時に特に役立った物品とその活用事例を紹介
災害時の過ごし方	清潔を保つために推奨する励行事項を、手洗い、トイレ、からだの清潔、歯みがき、居住スペースの 5 項目で紹介
災害時にも役立つ花王製品	清潔を保つために推奨する自社製品と使用事例を、水が使えない時、水が使えたら、肩こり・腰痛に、スキンケア、気分リラックス、居住スペースの 6 項目で紹介
災害支援団体からのメッセージ	同ウェブサイトを監修した、JVOAD（特定非営利活動法人 全国災害ボランティア支援団体ネットワーク）による災害に備えたメッセージを掲載

（同ウェブサイトの掲載情報を基にインターリスク総研にて作成）

＜情報セキュリティ＞

〇独立行政法人情報処理推進機構（IPA）が「情報セキュリティ 10 大脅威 2018」を発表

（参考情報：2018 年 1 月 30 日付　同機構 HP）

独立行政法人情報処理推進機構（IPA）は 1 月 30 日、情報セキュリティにおける脅威のうち、2017 年に社会的影響の大きかったトピックなどを選出し、順位付けした「情報セキュリティ 10 大脅威 2018」を公表した。

「個人」「組織」あわせて 20 の脅威のうち、16 の脅威が昨年に引き続きランクインした一方、「個人」では「偽警告」が、「組織」では「ビジネスメール詐欺」「セキュリティ人材の不足」が初めてランクインした。

「偽警告」は PC の画面に突然「ウイルスに感染した」などの警告メッセージが表示され、サポート窓口と表示された電話番号に連絡するよう仕向ける手口であり、IT に詳しくない PC 利用者が騙されやすいことが特徴である。

「ビジネスメール詐欺」は巧妙に細工したメールのやりとりを通じて企業の担当者を騙し、攻撃者の用意した口座へ入金させる詐欺の手口である。また、「セキュリティ人材の不足」は他の脅威とは観点がやや異なるが、組織として取り組むべき課題である。人材育成は長期的な課題であり、数年先を見据えて計画的に進める必要があるとしている。

IPA は、3 月下旬に「情報セキュリティ 10 大脅威 2018」の詳しい解説をウェブサイトで公開する予定である。

昨年順位	「個人」の 10 大脅威	順位	「組織」の 10 大脅威	昨年順位
1 位	インターネットバンキングやクレジットカード情報の不正利用	1 位	標的型攻撃による情報流出	1 位
2 位	ランサムウェアによる被害	2 位	ランサムウェアによる被害	2 位
7 位	ネット上の誹謗・中傷	3 位	ビジネスメール詐欺 NEW	ランク外
3 位	スマートフォンやスマートフォンアプリを狙った攻撃の可能性	4 位	脆弱性対策情報の公開に伴い公知となる脆弱性の悪用増加	ランク外
4 位	ウェブサービスへの不正ログイン	5 位	セキュリティ人材の不足 NEW	ランク外
6 位	ウェブサービスからの個人情報の窃取	6 位	ウェブサービスからの個人情報の窃取	3 位
8 位	情報モラル欠如に伴う犯罪の低年齢化	7 位	IoT 機器の脆弱性の顕在化	8 位
5 位	ワンクリック請求等の不当請求	8 位	内部不正による情報漏えい	5 位
10 位	IoT 機器の不適切な管理	9 位	サービス妨害攻撃によるサービスの停止	4 位
ランク外	偽警告 NEW	10 位	犯罪のビジネス化（アンダーグラウンドサービス）	9 位

■の色づけは、ランク外から 10 位以内にランクインした脅威

（出典：IPA HP）

海外トピックス：2018 年 1 月に公開された海外の CSR・ERM 等に関する主な動向をご紹介します。

＜ESG 投資＞

○国連責任投資原則（UNPRI）が署名機関の最低要件を 2020 年までに導入すると発表

（参考情報：2018 年 1 月 4 日　国連責任投資原則 HPなど）

国連責任投資原則（United Nations Principles for Responsible Investment、以下 UNPRI*）は、運用資産総額の半分以上を ESG 投資に割り当てることなどを求める最低要件を 2020 年までに導入すると発表した。同原則に従った運用の実践を表明する署名機関のうち「invest manager」（投資顧問）と「asset owner」（機関投資家）が適用の対象となる。

最低要件は全 3 項目で、上記のほかに責任投資の実践の担当者（専任でなくても可）の設置とその実践に経営レベルが関与し責任を担う体制の確立が求められる。

2018 年 3 月時点で最低要件に達しない署名機関は、2 年間の猶予が与えられ、その間 UNPRI が個別に協議・支援する。要件に達しない場合、最終的に除名の可能性もある。

* UNPRI
機関投資家が環境・社会・ガバナンス（ESG）の課題を投資の意思決定プロセスに取り込み、受益者のための長期的な投資成果の向上を目的として、2006 年 4 月に当時の国連事務総長であったアナン氏によって提唱された原則。2018 年 2 月時点で、世界の約 1800 の投資顧問会社や機関投資家が参加している。

＜リスクマネジメント＞

○世界経済フォーラムが「グローバルリスク報告書 2018」を公表

（参考情報：2018 年 1 月 17 日付　同 HP）

世界経済フォーラムは 1 月 17 日、グローバルリスク*に関する影響度と発生可能性を分析した「グローバルリスク報告書 2018」を発表した。世界経済フォーラムは毎年、ダボス会議に合わせて同報告書を発表しており、今回が 13 回目となる。

同報告書では、世界の約 1000 名の専門家および政策決定者に対して実施されたアンケート調査の結果が示されている。アンケートは、30 種類のグローバルリスクが提示されたうえで、各リスクの発生可能性および影響度について回答するものである。

報告書によれば、2018 年の発生可能性および影響度が高いグローバルリスクの上位 5 項目は以下のとおり。前回の報告書に引き続き「異常気象」「気候変動の緩和・適応の失敗」「水危機」といった環境関連のリスクが上位に多く挙がっているほか、「サイバー攻撃」「データの詐欺・盗難」といった情報セキュリティ関連のリスクも注目されるようになっている。

	影響度		発生可能性
1 位	大量破壊兵器	1 位	異常気象
2 位	異常気象	2 位	自然災害
3 位	自然災害	3 位	サイバー攻撃
4 位	気候変動の緩和・適応の失敗	4 位	データの詐欺・盗難
5 位	水危機	5 位	気候変動の緩和・適応の失敗

また、同報告書においては各リスクの関係性や長期的なリスクのトレンドについても分析され

ており、重要なトレンドとしては「気候変動」「所得や富の格差の拡大」「サイバー依存の高まり」「社会対立の増加」が挙げられている。

*グローバルリスク

世界経済フォーラムはグローバルリスクを「今後 10 年間のうち発生した場合に、複数の国や個人にネガティブな影響を及ぼす可能性のある事象や状況」と定義している。グローバルリスク報告書における 30 種類のグローバルリスクは以下のとおり。

経済リスク	主要経済圏における資産価値の極端な変動	環境リスク	極端な気象現象（洪水や暴風等）
	主要経済圏におけるデフレーション		気候変動の緩和・適応の失敗
	主要な財政機構・財政メカニズムの失敗		主要な生物多様性の喪失、生態系の崩壊
	致命的な社会インフラの失敗や不足		甚大な自然災害（地震、津波、噴火、磁気嵐等）
	主要経済圏における金融危機		人為的な環境汚染、環境災害（石油流出、放射性物質による汚染等）
	構造的な失業または不完全就業	社会リスク	都市計画の失敗
	不正取引		食糧危機
	極端なエネルギー価格の変動		大規模な非自発的移民
	極端なインフレーション		深刻な社会不安
地政学的リスク	国家統治の失敗		急速かつ大規模な感染症の拡大
	地域的またはグローバルな統治の失敗		水危機
	国家間紛争	科学技術リスク	科学技術の進歩による悪影響
	大規模なテロ行為		情報インフラやネットワークの致命的な障害
	国家の崩壊や危機（暴動、予期しない軍事行動、国家破綻等）		大規模なサイバー攻撃
	大量破壊兵器		大規模なデータ詐欺・盗難

（インターリスク総研訳）

＜リスクマネジメント＞

〇米トレッドウェイ委員会組織委員会と持続可能な開発のための世界経済人会議が ESG リスクを ERM フレームワークに統合させるための手法を公表

（参考情報：2018 年 1 月 23 日付　WBCSD ホームページより）

米トレッドウェイ委員会組織委員会（以下、COSO）と持続可能な開発のための世界経済人会議（以下、WBCSD）は 1 月 23 日、ESG リスクを COSO の提唱する ERM フレームワークに統合させるための手法を公表した。

世界経済フォーラムが発表した「グローバルリスク報告書 2018」によると、企業を取り巻くリスクはこの 10 年で様変わりし、ESG に関連するリスク（特に環境リスク）が上位を占めるようになった。同リスクにどのように対処するかが企業にとって重要なテーマとなっている。また、ESG 関連リスクは、機関投資家などの注目度も高まっており、対処しないことが企業の時価総額にも大きな影響を及ぼすようになっている。ところが、現在の組織ではリスクマネジメントを所管する部署と ESG 課題へ対処する部署が別々で、一体的な管理がなされていない。

こうした非効率な状況を打開するために、本手法が公開された。

COSO は昨年 9 月に、ERM フレームワークを改訂し、20 の原則でリスクマネジメントを実践

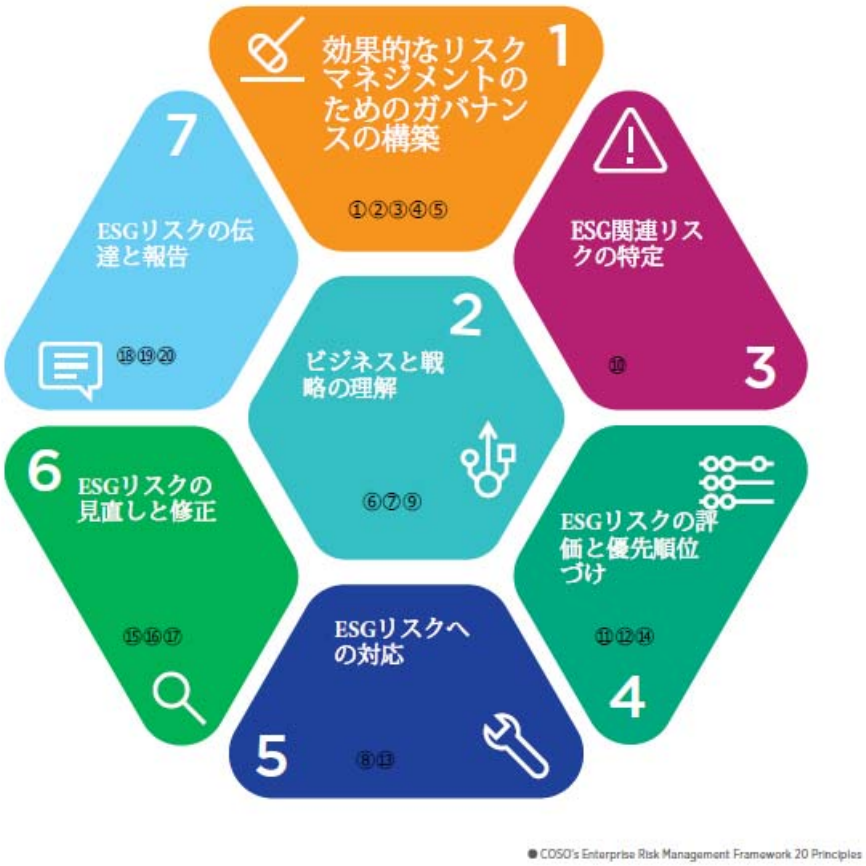
するモデルを提唱している【表１】。一方で WBCSD は、ESG リスクに対処するためのマネジメント手法を 7 つのモジュールで示している。この度公表された手法は、COSO の 20 の原則と WBCSD の 7 つのモジュールの対照関係・相関関係を示し、それぞれを統合的にマネジメントしていくための在り方を示している【図１】。

【表 1】COSO の ERM フレームワーク

ガバナンス &カルチャー	戦略＆目標設定	パフォーマンス	レビューと見直し	情報、伝達、報告
①取締役による監督機能の実施	⑥ビジネスの分析	⑩リスクの特定	⑮大きな変化をとらえる	⑱情報テクノロジーの活用
②オペレーションモデルの構築	⑦リスク選好の定義	⑪リスクの重要度の評価	⑯リスクとパフォーマンスのレビュー	⑲リスク情報のコミュニケーション
③要求される企業文化の定義	⑧代替戦略案の評価	⑫リスクの優先順位の決定	⑰リスクマネジメントの取り組みの改善	⑳リスク、文化パフォーマンスのレポート
④コアバリューの徹底	⑨ビジネス目標の設定	⑬リスク対策の浸透		
⑤優秀な人材の開発・育成・保持		⑭ポートフォリオビューの発展		

（出展：COSO’s Enterprise Risk Management Framework 20 Principles を基に、インターリスク総研訳）

【図 1】WBCSD のガイダンス



（出展 : Guidance for applying ERM to ESG-related risks を基に、インターリスク総研訳）

Q&A：CSR・ERM 等に関するさまざまなご質問についての解説を行うコーナーです。

Question

2017 年 11 月に改訂されたサイバーセキュリティ経営ガイドライン Ver.2.0*において、復旧対応に関する記載が設けられました。当社では地震を想定して事業継続計画（BCP）**を策定していますが、サイバー攻撃を想定した場合でも準用できるのでしょうか。

Answer

1. BCPにおいて日本企業が想定しているリスク

「平成27年度　企業の事業継続及び防災の取組に関する実態調査（内閣府防災担当）」によると、リスクを想定した経営を行っている（もしくは計画中、その予定がある）大企業の98.3%が「地震・台風等の自然災害」、70.6%が「新型インフルエンザ等の感染症」を想定していると回答しています。「外部委託先のサーバー・データセンター等情報システムの停止」を想定している大企業は66.8%で、3番目に多い結果となっています。

2. サイバーセキュリティ経営ガイドラインが求める「復旧対応」

同ガイドラインでは、セキュリティ対策の責任者に指示すべき事項として「サイバーセキュリティ経営の重要10項目」を定めており、そのうち指示8において「BCPとの連携等」が求められています。

> **指示8「インシデントによる被害に備えた復旧体制の整備」**
> インシデントにより業務停止等に至った場合、企業経営への影響を考慮していつまでに復旧すべきかを特定し、復旧に向けた手順書策定や、復旧対応体制の整備をさせる。BCP との連携等、組織全体として整合のとれた復旧目標計画を定めさせる。また、業務停止等からの復旧対応について、適宜実践的な演習を実施させる。

（経済産業省「サイバーセキュリティ経営ガイドライン Ver.2.0」から引用）

また、同ガイドラインの「付録A サイバーセキュリティ経営チェックシート」で、指示8に係るチェック項目が示されています。

> **指示8「インシデントによる被害に備えた復旧体制の整備」 対策例**
> ・被害が発生した場合に備えた業務の復旧計画を策定している
> ・復旧作業の課題を踏まえて、復旧計画を見直している
> ・組織の内外における緊急連絡先・伝達ルートを整備している
> ・定期的に復旧対応訓練や演習を行っている

（経済産業省「サイバーセキュリティ経営ガイドラインVer.2.0」から引用）

3. 「復旧対応」の検討について

（1）地震 BCP の準用

では、同ガイドラインが求める「復旧対応」を検討する上で、地震BCPを準用することはできるのでしょうか。

まず、BCPで復旧対応を検討する主なプロセスは、以下のとおりです。

①自社の事業から中核事業を選定し、緊急時においても継続すべき重要業務を選定するプロセス
②選定した重要業務に関わるリソースを整理し、そのリソースが毀損した場合における課題（ボトルネック）を洗い出すプロセス

③復旧対応を戦略的に行うため、方針や目標を検討・決定するプロセス
④復旧対応について具体的な手順に落とし込むプロセス

上記プロセスのうち、①については地震BCPでの検討結果を準用することが可能です。事業中断の原因事象が自然災害であるにせよサイバー攻撃であるにせよ、企業にとって中核となる事業や重要な業務が変わるものではなく、地震BCP等で重要と選定された事業や業務に関わるITサービスを速やかに復旧（もしくは継続）させるための体制、手順等が求められます。

一方、②～④のプロセスについては、原因事象によって検討内容が変わることがあります。たとえばサイバー攻撃の場合、組織内の機器やネットワークにマルウェア***が残存している間はITサービスを再開できないため、再開にあたって以下事項についても確認が不可欠となり、地震BCPの場合よりも対応事項が増える可能性があります。

- サーバ等に脆弱性がないかの確認を行う
- バックアップデータを復元する前に、復元先やバックアップデータにマルウェアが残存していないか等の確認を行った上でデータの復元を行う
- 不正な通信がないかの確認を行う

よって、既に地震BCPにおいて復旧対応を検討している場合でも、上記の脆弱性有無の確認などについて、対応手順に組み込まれているかの確認が望まれます。また、目標値（RTO（目標復旧期間）、RPO（目標復旧時点）、RLO（目標復旧レベル）、など）についても、サイバー攻撃を想定した場合においても現実的であるか確認が望まれます。検討の結果、現行のBCPに定められた復旧体制・手順や経営資源だけで重要業務の復旧や継続が目標を満足しない場合には、対応手順などのソフト的な対応だけでなく、一定の投資が必要なハード面からの検討も視野に入れることが必要になります。

（2）重要業務に関わるデータ等の保護対策

復旧対応に関わる記述は前述のとおり主に指示8に規定されていますが、BCPでいう「重要業務」の表記は、指示5「サイバーセキュリティリスクに対応するための仕組みの構築」の対策例にも見られます。同ガイドラインVer.2.0では復旧対応についての記載が新たに設けられましたが、インシデント発生時における対応だけでなく、平時から防御・検知・分析に関する対策も求められていることには留意が必要です。

指示5「サイバーセキュリティリスクに対応するための仕組みの構築」 対策例
重要業務を行う端末、ネットワーク、システム又はサービス（クラウドサービスを含む）には、多層防御を実施する。
－必要に応じてスイッチやファイアウォールなどでネットワークセグメントを分離し、別のポリシーで運用する。
－脆弱性診断等の検査を実施して、システム等の脆弱性の検出、及び対処を行う。
－営業秘密や機微性の高い技術情報、個人情報などの重要な情報については暗号化やバックアップなど、情報を保護する仕組みや、改ざん検知の仕組みを導入する。

（経済産業省「サイバーセキュリティ経営ガイドライン Ver.2.0」から引用）

4. 緊急時対応体制について

復旧対応を適切に行うには、その前段階で実施する「緊急時対応****」を適切に行うことも重要です。地震BCPにおける緊急時対応では、甚大な人的・物的被害が想定されるため、発災直後から物的な被害の確認だけでなく避難誘導や安否確認、応急救護といった対応を組織的に行うことが求められます。

これに対し、サイバー攻撃に対する緊急時対応については、同ガイドラインの指示7に以下の通り記載されています。

指示7 インシデント発生時の緊急対応体制の整備
影響範囲や損害の特定、被害拡大防止を図るための初動対応、再発防止策の検討を速やかに実施するための組織内の対応体制（CSIRT 等）を整備させる。被害発覚後の通知先や開示が必要な情報を把握させるとともに、情報開示の際に経営者が組織の内外へ説明ができる体制を整備させる。また、インシデント発生時の対応について、適宜実践的な演習を実施させる。

（経済産業省「サイバーセキュリティ経営ガイドライン Ver.2.0」から引用）

指示 7 には、影響範囲や損害の特定、被害拡大防止を図るための初動対応等が定められており、例えば情報漏えいの場合、漏えい原因の調査やステークホルダーへの情報開示、被害者へのお詫び対応といった対応が求められます。これらの対応の出来が後の復旧活動を左右するため、計画策定だけでなく実効性を高めるための演習実施も求められています。

また、関連資料として「付録 C　インシデント発生時に組織内で整理しておくべき事項」が掲載されています。同資料は、調査すべき事項がインシデントごとに整理されており、原因調査の確認事項や手順の検討に活用することも有効です。

基本項目　全てのインシデントで共通して調査すべき項目
初動対応/第一報
インシデントの分類、事業分類…など
原因調査/第二報以降
システムの運用状況、システム構成
情報漏えいに係る項目　情報漏えいが発生した際に調査すべき項目
原因調査/第二報以降
発覚の経緯、原因及び経路、情報漏えいの有無、漏えいしたデータの項目及び件数…など
原因調査/第二報以降　事後対策/最終報
事業者による対応（再発防止策を含む）、報告先…など
ウイルス感染に係る項目　ウイルス感染が発生した際に調査すべき項目
（省略）
不正アクセスに係る項目　不正アクセスを受けた際に調査すべき項目
（省略）
（D）DoS に係る項目　（D）DoS 攻撃を受けた際に調査すべき項目
（省略）

（経済産業省「サイバーセキュリティ経営ガイドライン Ver.2.0　付録 C」を参考にインターリスク総研にて作成）

地震をはじめとする自然災害の初期対応においては、総務部門や人事部門が対応の中心となることが一般的ですが、上記の調査対応は情報システム部門や法務部門などを中心とする CSIRT*****が対応の中心となるのが一般的です。

このように、緊急時対応においても、実施内容、組織体制とも、地震 BCP と異なるものが多く、サイバー攻撃に備えた検討を進めておくことが望まれます。

5.　おわりに

上述の通り、サイバー攻撃における緊急時対応や復旧対応では、地震BCPを準用するだけでは不十分であり、投資を伴うハード面の対策、技術的対応を念頭に置いた体制、平時からの重要業務に関するシステムの多層防御など、サイバー攻撃固有の様々な検討が必要になります。

自社のみでの検討が困難な場合には、普段から取引のあるシステムベンダーやセキュリティベンダーなどに予め相談し、いざというときにこれらベンダーの支援を受けられるようにしておくことも望まれます。

* サイバーセキュリティ経営ガイドライン Ver.2.0
Ver.1.1 と Ver.2.0 との比較は CSR・ERM トピックス 2017 年度第 10 号を参照ください。

** 事業継続計画（BCP:Business Continuity Plan）
企業が自然災害、テロ攻撃、サイバー攻撃などによる被害が発生した場合において、中核となる事業の継続、早期復旧を実現するために、平時及び緊急時における事業継続のため手段等を取り決めておく計画のこと。（経済産業省「サイバーセキュリティ経営ガイドライン Ver.2.0」から引用）

*** マルウェア
悪意のあるソフトウェアの総称。

**** 緊急対応
標準的な手順は、CSR・ERM トピックス 2016 年度第 2 号を参照ください。

***** CSIRT：シーサート (CSIRT: Computer Security Incident Response Team)
コンピュータセキュリティにかかるインシデントに対処するための組織の総称です。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動をします。（日本シーサート協議会 HP から引用）

以上

株式会社インターリスク総研は、MS&AD インシュアランスグループに属するリスクマネジメント専門のコンサルティング会社です。CSR（企業の社会的責任）・ERM（全社的リスク管理）等に関するコンサルティング・セミナー等のサービスを提供しています。
弊社サービスに関するお問い合わせ・お申込み等は、下記のお問い合わせ先、または、お近くの三井住友海上、あいおいニッセイ同和損保の各社営業担当までお気軽にお寄せ下さい。

お問い合せ先
㈱インターリスク総研　リスクマネジメント第三部
TEL.03-5296-8912（危機管理・コンプライアンスグループ）
TEL.03-5296-8913（環境・CSRグループ）
TEL.03-5296-8914（統合リスクマネジメントグループ）
http://www.irric.co.jp/

主な担当領域は以下の通りです。

＜危機管理・コンプライアンスグループ＞
- ◆ 危機管理・海外危機管理
- ◆ コンプライアンス（法令遵守）
- ◆ 役員賠償責任（D&O）
- ◆ CS・苦情対応
- ◆ 製品安全・食品安全

＜環境・CSRグループ＞
- ◆ 環境経営（環境リスク・ブランディング）
- ◆ 環境マネジメントシステム（ISO14001等）
- ◆ 生物多様性
- ◆ エネルギー（再エネ・省エネ）
- ◆ 社会リスク（環境デューデリジェンス・人権リスク等）

＜統合リスクマネジメントグループ＞
- ◆ ERM（全社的リスク管理）
  - ・リスクマネジメント体制構築
  - ・企業リスク分析・評価（リスクアセスメント）
- ◆ 情報漏洩リスク