東京海上日動リスクコンサルティング株式会社
ビジネスリスク本部　兼　Ｒ＆Ｄ本部（サイバー）
主任研究員　川口　貴久

サイバーリスクと危機管理・事業継続：訓練・演習から得られた課題と教訓

Cyber Risks and Crisis Management/Business Continuity:
Lessons Learned from Our Drills and Exercises

はじめに

サイバー攻撃は企業・組織から機密情報を窃取し、データやシステムを改竄し、事業や社会に不可欠な機能やサービスを停止に追い込むものである。実際、サイバーリスクは多くの企業にとって最重要なリスクの 1 つとして認識されつつある。例えば、世界経済フォーラムが毎年発行する『グローバルリスク報告（Global Risks Report）』では、サイバーリスクはここ数年、上位リスクにランクインし、日本企業へのアンケート調査からも同様の結果が確認されている[1]。

その結果、多くの企業はサイバーリスクに関する評価やインシデント発生時の対応体制を整備しつつある。本稿は、トップマネジメント層や経営管理・リスク管理・危機管理統括部門が認識すべき、サイバーリスク関連の課題を提示したい。

なお、本稿において提示する課題は、実際のインシデントからではないが、実際の危機管理・事業継続訓練・演習から観察・推察されたものである。訓練・演習のサンプル数が十分ではないため、定量的な議論は難しいが[2]、企業・組織におけるサイバーリスク対応を考える上でのヒントになるかもしれない。

危機管理・事業継続という観点からは以下の 4 点が大きな課題であると考える。本稿はまず、サイバーリスクの概要と特徴を整理し、その上で下記の 4 つの課題について検討する。

サイバーリスクに関する危機管理・事業継続訓練・演習から得られた課題・教訓

1. サイバーリスクは危機に転化する瞬間・閾値が明確ではないことが多いため、危機発生時の初動対応（危機レベルの判定や関係部門連携等）が難しい
2. サイバーリスクの物理的側面（データセンターの対策等）は認識されていないケースがある
3. 危機発生時、システム停止措置は被害拡大防止に有効だが、事前に検討すべきことは多い
4. サイバーリスクは専門性が高い分野のため、社内のリスクコミュニケーションは限定的である

[1] 弊社による調査（企業へのアンケート調査（n=265）、2015 年実施）では、回答企業の約 53%が情報・システムリスクを「重視している」と回答し、「コンプライアンス違反・ガバナンス問題」「地震・津波」」に次ぐ、第 3 番目のリスクとランキングされている。詳細は、「リスクマネジメント動向調査 2015：事業継続の取組みの進化と新たなリスクへの挑戦」東京海上日動リスクコンサルティング㈱（2016 年 1 月発行）

[2] 本稿は実証研究、現状分析・評価・見通し、分析・評価手法に関する科学的研究ではなく、コンサルティング実務・経験に基づく試論である。したがって本稿の課題抽出のプロセスや結果に反証可能性はない。

１．サイバーリスクの概要

（１）サイバーセキュリティとサイバーリスク

サイバーセキュリティの定義は難しいが、2015 年 12 月に公表された経済産業省の『サイバーセキュリティ経営ガイドライン』（2016 年 12 月改定）によれば、サイバーセキュリティとは「サイバー攻撃により、情報の漏えいや、期待されていた IT システムの機能が果たされない等の不具合が生じないようにすること」と定義される。サイバーリスクとはこうした漏えいや不具合を生じさせる不確実性を指す。

このように考えると、サイバーセキュリティは情報セキュリティの定義をサイバー空間に拡大したものと理解しても問題はない。情報セキュリティとは「情報の機密性（Confidentiality: C）、完全性（Integrity: I）、可用性（Availability: A）を維持すること」（ISO/IEC27001）である。企業にとってサイバーセキュリティとは、サイバー攻撃から重要な情報やデータを守り、システムやサービスを期待するとおりに維持することに他ならない。したがって、サイバーリスクとは、電磁的空間上の、あるいは電磁的空間を通じて、情報の C.I.A.を阻害する不確実性を指す[3]。

（２）危機管理･事業継続からみたサイバーリスクの特徴

危機管理・事業継続の観点からみると、サイバーリスクは他のリスクと比較していくつかの特徴がある。第一に、サイバーリスクとその他リスクでは利用可能な経営リソース[4]が異なる【図表１】。多くの企業・組織が「オールリスク」「オールハザード」でのリスクマネジメントを推進しながら、実態としては地震やパンデミックを念頭においていることが少なくない。しかし、サイバーリスクとその他リスクでは、利用可能な経営リソースは異なるため、地震・パンデミックとは異なる危機管理・事業継続の手順や留意点が求められる。

第二に、サイバーリスクはその他リスクに比べて、危機に転じる瞬間・閾値が明確ではないことが多い（平時と有事の曖昧性）。サイバーリスクは目に見えず、リスクや危機の進行に気づきにくい。自社への不正アクセスを認知したとしても、実際に社内のデータやプログラムに影響がでているのか、情報の漏えいが生じているのかを確定させるには一定の時間やリソースがかかる（2 章（1）参照）。

第三に、サイバーリスクは事業にもたらす結果が多様である（結果の多様性）。サイバーリスクが顕在化した場合の影響は、情報の漏えい（個人情報、営業秘密等）、データやプログラムの消去・改竄、機能やサービスの停止等、多岐にわたる。

第四に、サイバーリスクは競争上の劣後環境をつくりだす。ゼロデイ（未知の脆弱性）を利用した攻撃や重要インフラ・特定業界に対する攻撃を除いて、サイバーリスクの多くは自社・自組織のみで顕在化する。地震であれば、同業他社や取引先も含めて、損害や事業中断が発生しているが、サイバーリスクの場合、自社・自組織のみが被災することがあり得る。これは競合者に対して自社が明らかに劣後する形となる。

図表１：リスクごとの利用可能な経営リソースの比較

		利用可能な経営リソース			
		ヒト	モノ	情報	外部*
リスク	地震等の自然災害リスク	×	×	×	×
	パンデミック・感染症リスク	×	○	○	×
	供給・サプライチェーンリスク	○	○	○	×
	サイバーリスク・システムリスク	○	○	×	○

* 外部とは、委託先・調達先・仕入れ先等の事業に不可欠な社外リソースを指す。　出典：筆者作成

[3] 当然ながら、サイバーセキュリティ基本法も同じような考え方を示している。サイバーセキュリティ基本法（第二条）によれば、サイバーセキュリティは「電子的方式、磁気的方式その他人の知覚によっては認識することができない方式により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置が講じられ、その状態が適切に維持管理されていること」（補足等は引用者が割愛）と定義され、実質的に情報の C.I.A.の維持に言及していると解釈できる。

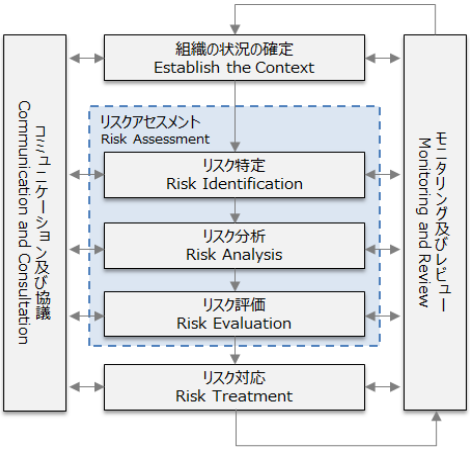
[4] 経営リソースとは、企業の運営に欠かせない資産（例：ヒト、モノ、金、情報、時間 等）のこと。

２．サイバーリスク対応訓練･演習から得られた課題と教訓

上記のようなサイバーリスクの定義・範囲と特徴を踏まえて、弊社では 2015 年 4 月以降、複数のサイバーリスクに関する危機管理・事業継続訓練・演習を実施した。訓練・演習の目的は様々で、①組織の意思決定・判断を検討するもの、②現状の組織・対応手順の課題を検討・改善するもの、③インシデント発生後の対応手順（マニュアル等）を検証するもの 等である。それゆえ対象者も様々で、トップマネジメントから、経営管理・リスク統括・危機管理部門、ICT 担当部門、事業部門と多岐にわたる。ただし、訓練・演習の範囲は CSIRT（Computer Security Incident Response Team）や関係部門向けのインシデント・ハンドリングではなく、あくまでも会社・組織全体の危機管理・事業継続である。

こうした訓練・演習で観察された課題、あるいは推察された課題はいくつかあるが、複数の企業・組織に共通する課題として冒頭の 4 つを抽出した。これら 4 つの課題がリスクマネジメントのプロセス（図表２）のどこに該当しているのかを明らかにした結果が図表３である。次頁以降、課題が大きいと考えられるものから詳細を述べていく。

図表２：リスクマネジメントの一般的なプロセス



1. 「組織の状況の確定」は、目指すべき姿や現状の課題、適応範囲等のリスクマネジメントの前提にあたる部分である。組織外部や組織内部（責任と役割、経営リソース、ルール等）を確認し、リスク基準等を検討するステップである。
2. 「リスクアセスメント」は、リスクを特定し、影響度や頻度を分析し、リスクマネジメントの中での優先順位を評価するものである。
3. 「リスク対応」の選択肢としては、①リスクの回避、②リスクの増加、③リスク源の除去、④起こり易さの変更、⑤結果の変更、⑥リスクの共有（契約や保険等）、⑦リスクの保有 に分類される（従来は「回避」「低減」「移転」「保有」と分類）。
4. 「モニタリング及びレビュー」はリスクマネジメントのプロセスやリスクそのものを把握・監視・検証し、これまでのプロセスにフィードバックを与えるものである。
5. 「コミュニケーション及び協議」は、リスクマネジメントプロセス全体を支えるもので、ステークホルダーとの情報共有等を指す。

出典：ISO31000: Risk management - Principles and guidelines(2009)から筆者作成

図表３：危機管理・事業継続訓練・演習から推察された課題

プロセス		概要	課題の大きさ
組織の状況の確定		サイバーリスクは危機に転化する瞬間･閾値が明確ではないことが多いため、危機発生時の初動対応（危機レベルの判定や関係部門連携等）が難しい	大
リスクアセスメント（特定・分析・評価）		サイバーリスクの物理的側面（データセンターの対策等）は認識されていないケースがある	中
リスク対応	事前予防	（訓練・演習からは観察・推察できず）	―
	発生時対応	危機発生時、システム停止措置は被害拡大防止に有効だが、事前に検討すべきことは多い	大
モニタリング及びレビュー		（訓練・演習からは観察・推察できず）	―
コミュニケーション及び協議		サイバーリスクは専門性が高い分野のため、社内のリスクコミュニケーションは限定的である	中

出典：筆者作成

（１）システム停止は被害拡大防止に有効だが、事前に検討すべきことは多い

サイバーリスクの顕在化時、システム停止措置（自らの判断に基づく積極的な停止措置）は被害拡大防止に有効な手段である。システム停止の判断・完了が遅れたため、被害が拡大したケースとしては、2016 年 5 月に発生した大手旅行事業者の個人情報漏えい事案がある。報道によれば、システム停止の判断が遅れたことが被害拡大に繋がった。この事案では、外部との通信遮断作業を開始してから完了までに 6 日かかっている。ところが、実際に個人情報が流出した可能性あるデータは遮断作業 2 日目（完全遮断完了の 4 日前）に複製されている。ただちに外部との通信遮断が完了しなかった理由について、当該企業の経営者は「情報流出の可能性の認識が十分ではなく、事業を停止させてまでの判断ができなかった」と述べている[5]。

被害拡大防止として迅速なシステム停止は有効である。しかし、外部との通信遮断等のシステム停止は影響が大きいことも事実である。それゆえ、有事の際には、迅速に現状を評価して経営が決断することが必要である。その際に必要なポイントとしては以下のようなものある。

システム停止措置の選択肢

第一に、**システム停止は、all or nothing ではない**。つまり、システム停止措置は正常稼働か完全停止の二者択一ではなく、その中間領域が（多くの場合）存在する。

図表 4 は架空の企業における「システム停止の段階的オプション」とその際の「社内にあるシステムやアプリケーションの利用可否」を例示したものである。最も低いレベルでのシステム停止措置は外部ネットワークの遮断である。この措置がとられた場合、社外とのメールの受発信やインターネットブラウジングが不可能となり、社内からの公開ホームページや EC（Electronic Commerce）サイトの管理もできなくなる。他方で、マルウェア感染等による情報漏えいや外部からの不正アクセスのリスクは極小化される。最も厳しい措置は端末自体を全面使用禁止とすることである。これ自体は、システム面での措置というよりも管理運営上の指示に近い。自社・自組織のネットワーク構成やシステムの特性を踏まえて、段階的なシステム停止措置を検討しておくことが望ましい。

図表４：架空企業におけるシステム停止措置の段階的オプション

システム停止の段階的オプション	社内のシステムやアプリケーションの利用可否（例）				
	オフラインでの端末利用（基本的なオフィスソフトの操作等）	社内ネットワークにある共有フォルダ・データへのアクセス	社内ネットワーク内にある経理・プロジェクト管理システム	公開 HP や電子商取引サイトの社内からのメンテナンス	メールやインターネットブラウジング
Level 1 通常稼働	○	○	○	○	○
Level 2 外部ネットワークの遮断（メール、インターネットブラウジングの禁止）	○	○	○	×	×
Level 3 外部ネットワーク・基幹システムＡ（社内人事・プロジェクト管理システム）の停止	○	○	×	×	×
Level 4 外部ネットワーク・基幹システムＡ・Ｂ（ファイルシステム）の停止	○	×	×	×	×
Level 5 端末の全面使用禁止	×	×	×	×	×

出典：筆者作成

[5] 「JTB 情報流出 遅れた外部接続遮断」毎日新聞（2016 年 6 月 14 日）;「JTB 不審な通信確認も直ちに対応せず」NHK ニュース（2016 年 6 月 15 日）。

システム停止に関する迅速な判断･実行

第二に、システム停止判断から実行はスピード勝負であり、**システム停止の判断・手続きと実行手順は事前に準備する**必要がある。停止判断はインシデントを検知してから時間との闘いであり、適切な停止判断の権限、基準、運用手順、チェックリスト等が不可欠である。

システム停止による影響が大きいほど上位者の権限が必要となる。（業態・マネジメント体制・ネットワーク構成にもよるが）単に外部との通信遮断であれば、SOC（Security Operation Center）や ICT 部門による通常業務の監視下で異常を検知した場合、即座に判断・実行しても問題ないことが多い。他方で、重要インフラ事業者における業務基幹システムの中断（例えば、航空業界における運行システム、銀行業界の勘定系システム等）は、国家・社会レベルでの損失・被害の可能性もあるため、高度な判断が求められる。

オフラインでの事業継続

第三に、**システム停止時のオフラインでの事業継続態勢は不可欠**である。

弊社で実施したあるサイバーリスク危機管理・事業継続訓練では、システム停止を判断するかどうかの判断基準で最も多い回答は「機密情報漏えいの恐れの有無」で、次に多い回答は「システム停止時の事業継続計画に実効性があるか否か」であった。つまり、オフラインでの重要業務継続の可能性は、システム停止の判断そのものに影響を与える重要要素の 1 つである。

しかし多くの企業では、インシデント発生時の CSIRT 向けのインシデントハンドリングマニュアルは整備されつつあるが、事業全社としての危機管理･事業継続計画･手順は策定されていないことも多い。

サイバーリスクを念頭におく事業継続計画（BCP）策定は不可欠である。最近は、リスク事象や特定シナリオに依存しない「結果ベースの BCP」「オールハザード・オールリスク対応型の BCP」の策定が推奨されている。しかし、蓋然性や影響度が高く、特徴的なリスクについては一定のシナリオを前提とする BCP が必要である。多くの企業で地震リスク、台風・洪水リスク、パンデミックリスクに対応した個別 BCP を策定しているように、サイバーリスクに特化した BCP は不可欠である。その理由は、サイバーリスクは地震やパンデミックとは異なり、利用可能な経営リソースが異なるからである（前述の図表 1 参照）。また「自社のみ劣後環境」といった自責の念にかられることからも、被害を受けた際の自社の相対的ダメージは自然災害より大きく、準備の必要性は高い。

＜被害拡大防止としてのシステム停止措置＞

- □ 被害拡大防止のためのシステム停止措置の権限・手続きは明確か？
- □ システム停止措置は複数の段階的オプションがあるか？
- □ システム停止を決定した後の社内外への連絡体制は整備されているか？
- □ システム停止を決定した後の事業継続計画（サイバーリスク版）はあるか？

（２）危機発生時の初動対応が難しい

サイバーリスク（潜在的状態）は、クライシス（顕在的）に変わる閾値が明確でないため、危機初動段階の危機レベルの判定や部門間の連携が難しい。

地震や火災・爆発等のリスクに比べ、セキュリティインシデントはクライシスに変わる瞬間（crisis point）が明確でないことが少なくない。というのは、サイバー攻撃等のインシデントは可視化され、誰の目にもわかるものではなく、サイバー攻撃の発生に気づくことが難しい。サイバー攻撃の認知は、外部機関（JPCERT/CC 等）からの連絡であったり、社内の異常の検知であったり、ベンダーとのコミュニケーション等から始まる。サイバー攻撃および被害を確定するには、一定の時間やリソースが必要である。一般的な企業であれば、不正アクセス等を認知したとしても、実際の被害が生じているかどうかは専門事業者の力を借りなければ明らかにならないケースも多い。

その結果、企業・組織として危機レベルを判断し、組織活動を平時モードから有事モード（危機管理・事業継続態勢）に切り替えることが困難となっている。少なくとも、平時から有事への切替モードに明確な線引きや閾値があるわけではない（図表５）。

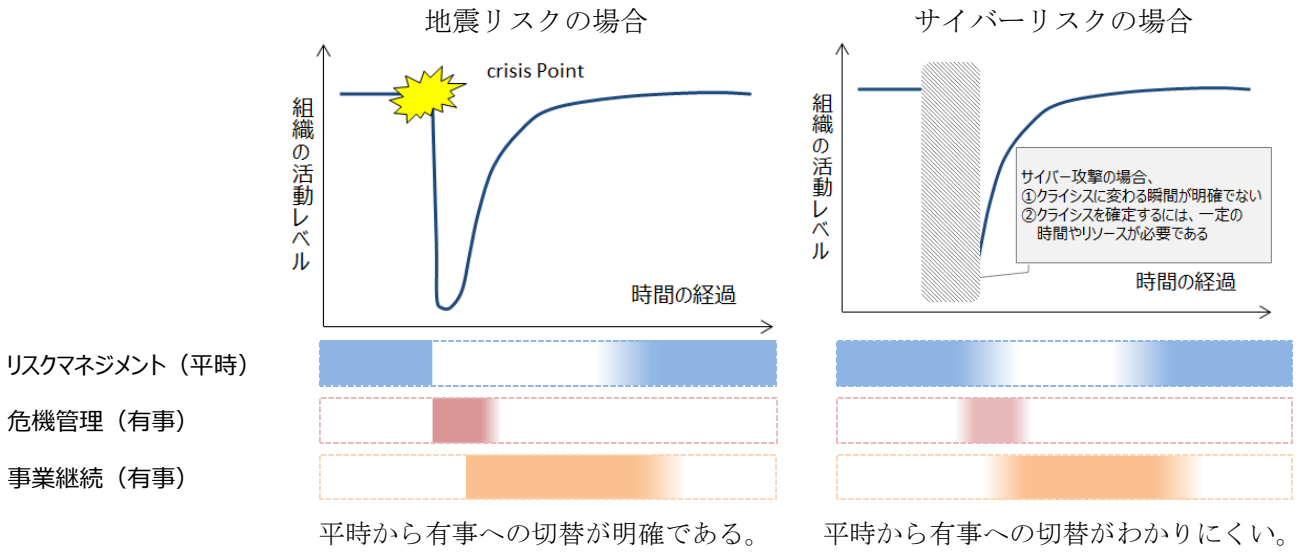
図表６のとおり、サイバーリスクに関係する危機管理・事業継続に関係する組織・部門として、①リスク統括部門、②危機管理統括部門、③事業継続統括部門（②③は「対策本部」として組織される場合もある）、④サイバーリスクのオーナー部門、⑤サイバーリスクの危機対処部門 等、多岐にわたる。①②③はリスク・クライシス全般を扱い、④⑤はサイバーリスクに特化した組織である。

サイバーリスクの場合、サイバーリスク担当部門である④と⑤の連携は比較的良好な場合が多いが、全社のリスク・クライシスを扱う①②③と④⑤の連携がうまくいかないことが多い。サイバーリスクの担当部門（④⑤）は、インシデントが情報インフラやシステムに及ぼす影響・危機レベルを判断することはできるが、それがビジネスサイドに及ぼす影響を図ることは必ずしも所与のものではない。ビジネスサイドへの影響評価は④⑤が行うことが一般的であり、初動における危機レベルの判断が難しくなっている場合がある。例えば、会社としての危機の認定基準として、「機密情報漏えいの恐れの発生」を掲げていたとしても、システムサイドとビジネスサイドの評価基準や具体例は必ずしも一致しない。

＜初動段階における危機認定と部門間連携＞

- □ サイバーリスクに関する全社的な「危機」の基準や閾値はあるか？
- □ インシデントを認知してから、経営層や経営管理部門にエスカレーションする際の基準・内容・方法は整備されているか？
- □ サイバーリスクに関して、システムサイドだけでなく、ビジネスサイドの影響を評価する仕組みは整備されているか？

図表５：地震とサイバーインシデント時の組織対応の比較（イメージ）



出典：筆者作成

図表６：サイバーリスクに関係する危機管理・事業継続に関係する組織・部門

分類	概要	担当組織・部門
①リスク統括部門	平時における全社のリスクマネジメントを統括する部門	経営企画部、リスク統括部、総務部等 *単一の部署が担うこともあれば、複数の部署で分担することもある。または委員会や対策本部が組織されることもある。
②危機管理統括部門	有事における全社の危機対応を統括する部門	
③事業継続統括部門	平時または有事における全社の事業継続を担当する部門	
④サイバーリスクのオーナー部門	平時におけるサイバーリスク、情報・システムリスクのマネジメントを統括する部門 IT・システムベンダーとの連携窓口部門	ICT 部門
⑤サイバーリスクの危機対処部門	有事におけるサイバーリスク、情報・システムリスクの危機対応を統括する部門 IT・システムベンダーとの連携窓口部門	セキュリティ部門、CSIRT 等

出典：筆者作成

（３）サイバーリスクの物理的側面が忘れられがち

企業・組織におけるリスクマネジメントの中で、情報リソースが重視されていることは言うまでもない。しかし、こうした情報リソースの物理的側面や物理的脆弱性は見過ごされることが少なくない。

話は大きくなるが、わかりやすいのはインターネットである。インターネットは物理を超えた空間であると思われがちだが、完全に真実ではない。インターネットの基幹インフラは地理と密接に関連している。国際トラフィックの約 95%（日本ではそれ以上）が海底ケーブルを経由しているが、世界で約 200 本の海底ケーブルとその陸揚げ拠点は地理的に偏在している[6]。日本の陸揚げ拠点は、丸山や千倉等の千葉県房総半島南端、茨城県阿字ヶ浦や北茨城、三重県志摩に無防備な状態で集中している【図表７】。海底ケーブルは自然災害や事故といったリスクだけでなく作為的リスク（攻撃）にもさらされている[7]。

政府や企業のデータセンターの所在地も特定の場所に集中する傾向にある。そうした所在地の地震・浸水や火災・爆発といった物理的リスクの評価が十分でないこともある。また、こうした基幹インフラは公開情報や合法的な調査で特定することが可能である。例えば、慶應義塾大学の土屋大洋教授は公開情報のみを用いて、ニューヨーク州にあるデータセンターの所在地を特定している[8]。

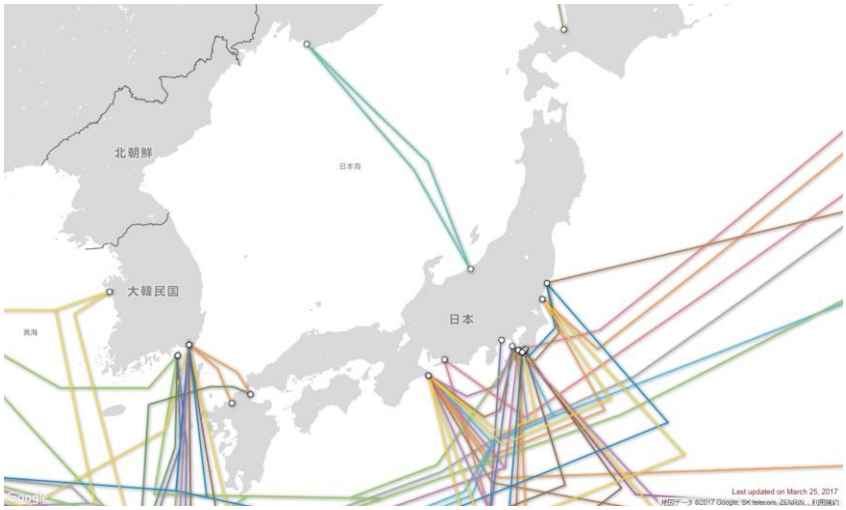
たしかにインターネットやデータセンターを始めとする情報インフラは冗長性のある仕組みではあるものの、その基幹インフラは地理的には偏在し、特定可能であり、物理的なリスクに脆弱であると言える。こうした事実を経営層や経営管理部門が十分に理解していないケースがある。

とはいえ、あらゆるインフラを二重化する等の対策は現実的ではない。リスクマネジメントとは許容できるリスク量を合意するプロセスでもあり、費用対効果を踏まえたものである必要がある。物理的対策は、事前に脅威評価や優先順位付けを行った上で講じる必要がある。企業や組織は少なくとも以下の点で、自社のリスクをアセスメントしておくことが望ましい。

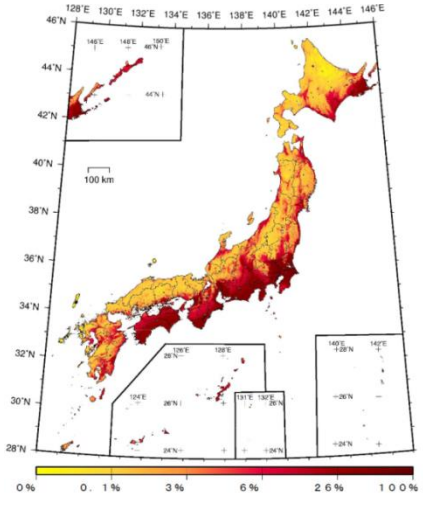
＜サイバーリスクの物理的側面＞

- □ 自社・自組織のデータセンター／サーバはどこにあるのか？（所在地）
- □ 所在地は第三者が公開情報を用いて特定可能か？
- □ 所在地の地震・火災・テロ等の物理的リスクはどの程度あるか？【図表８】
- □ 代替データセンター／サーバは存在するか？　有事の切替判断・手順は明確か？

図表７：日本近郊の海底ケーブル図（Submarine Cable Map）



図表８：日本の地震発生確率※



※　発生確率（%）は、今後 30 年以内に震度 6 弱以上の揺れに見舞われる確率を指す。なお、今後、30 年以内に交通事故で負傷する確率は約 24%と評価されているため、震度 6 弱以上の揺れに見舞われる確率は交通事故と比較しても同程度かそれ以上と言える。

出典：（図表 7）TeleGeography［http://www.submarinecablemap.com/］より抜粋（2016 年 8 月 12 日取得）
（図表 8）全国地震動予測地図 2016 年版より抜粋

[6] Robert Martinage, “Under the Sea: The Vulnerability of the Commons,” *Foreign Affairs*, Vol.94, No.1(January/February 2015), pp.117-126.
[7] 例えば元 NATO 最高司令官のスタヴリディス海軍提督（Admiral Jim Stavridis）はロシアが海底ケーブルの脆弱性を探っていると評価する。Admiral Jim Stavridis (Ret.), “A New Cold War Deep Under the Sea?,” The Huffington Post (October 28, 2015)
[8] 土屋大洋『暴露の世紀：国家を揺るがすサイバーテロリズム』（角川新書、2016 年）、167-172 頁。

（４）リスクコミュニケーションは限定的である

サイバーリスクに関する社内のリスクコミュニケーションは現時点では十分とは言い難い状態にあると思われる。例えば、第一に業務執行と経営（取締役会等）、第二にサイバーリスクのオーナー部門（ICT 部門等）とリスク統括部門（経営管理部門等）で問題となる[9]。

コミュニケーションギャップが発生する大きな理由は、サイバーリスクをとりまく専門性の有無によるものと考えられるが、リスクコミュニケーションに個別リスクに関する高度な専門性は必ずしも必要ではない。多くの企業で、地震・パンデミック・コンプライアンス違反といったリスクについては、経営と執行の間で、またリスク統括部門と個別リスクオーナー部門の間でコミュニケーションがとられている。地震リスクのコミュニケーションに高度な地質学・工学の知識は不要であり、パンデミックのリスクコミュニケーションは疫学・病理学の専門家である必要はなく、コンプライアンスに関するコミュニケーションも法的な専門性までは不要である。同様に、サイバーリスクに関するコミュニケーションの際にも高度な専門性は不要である。

もちろん、執行・取締双方の経営層やリスク統括部門はサイバーリスクに関する基本的な知識は踏まえる必要があるし、リスクオーナー部門もそうした情報や知識を発信していく必要がある。サイバーリスクは、影響度の大きいリスクだが、リスクマネジメント・危機管理・事業継続のプロセスの中で決して特殊なものではない。

＜リスクコミュニケーション＞

- □ 経営者や経営管理部門はサイバーリスクに関する基本的な知識を有しているか？
- □ 社内外のセキュリティインシデント等、サイバーリスクに関する基本的な情報が経営層を含む会社全体に共有されているか？

おわりに

本稿では実際のサイバー攻撃等に起因する危機管理・事業継続の訓練・演習で観察された課題、推察される課題について詳述した。限られたコンサルティングの実務と経験から抽出した課題であり、課題抽出のプロセスや結果は科学的ではないが、企業・組織におけるリスクマネジメント・危機管理・事業継続態勢を整備する上でのヒントになれば幸いである。

（2017 年 4 月 10 日脱稿）

[9] こうしたリスクコミュニケーションの少なさは、それぞれの要員の価値観・文化に起因するという見方もある。しばしば指摘されるのは「ギーク（geek）」と「スーツ（suits）」のコミュニケーションギャップである。「ギーク」は元々「オタク」「変人」の意味であり、情報技術の専門家を指す。「スーツ」とは官僚や軍人などの政策形成者を指し、転じて企業の経営管理部門を指すと考えて良いだろう。ジョン・カッツ（松田和也訳）『ギークス GEEKS：ビル・ゲイツの子供たち』（飛鳥新社、2001 年）；土屋大洋『情報による安全保障：ネットワーク時代のインテリジェンス・コミュニティ』（慶應義塾大学出版会、2007 年）、3-13 頁。