複雑化・多様化する海外でのリスク対策

—— 企業価値向上に向けた危機管理とリスク管理

デジタル時代の新たなリスクと
どう向き合うか。

コントロール・リスクス・グループ株式会社
アソシエイト・ディレクター　**丹羽雅彦**

対策強化 ３つのポイント

企業を取り巻くリスクが複雑化、多様化していく中で、リスク対応強化の究極的な目的は企業価値の向上にあると考えられる。

企業を取り巻く様々なリスクへの対応を強化する上で、近時のポイントとして次の３点が挙げられる。

第１にデジタル上の脅威が引き起こす物理的脅威である。リモートワークの普及とクラウド化の推進により、サイバー脅威の時代が本格的に始まった。経営上の意思決定を支えるための、より迅速で正確なインテリジェンスの収集・分析能力の強化がサイバー空間でも求められる。

第２に持続可能な社会へのコミットメントである。近年、企業のステークホルダーは多様化しており、それぞれのステークホルダーから寄せられる期待は大きなものとなっている。特に海外における ESG（環境、社会、企業統治）リスクへの対応が注目されている。

第３に安全保障である。近年、国家安全保障の観点からサプライチェーンの安定化が重要になっており、ここに民間企業の海外事業も組み込まれるかたちになってきている。特に水面下で続いていた米中デカップリング（分離）の問題が、新型コロナウイルスの感染拡大とともに旧トランプ政権時代に急浮上し、日系企業に影響を与えるケースも見られる。経済安全保障リスクへの対策の実効性が上がれば、海外リスクをより果敢にテイクできる可能性は高まる。

今注目すべき４つのリスク

以上を踏まえて、企業にとって重要と考えられる４つのリスクと、それらの対応について取り上げたい。

１．ランサムウェアによる物理的危機の発生と経済安全保障リスク

標的型ランサムウェアによる攻撃を仕掛けて身代金の要求を行うサイバー恐喝の主な標的となっているのは、政府機関の他、ヘルスケア、金融サービス、IT・通信など幅広い業種の民間企業である。昨今、大手の日系企業が標的とされる事例も増えている。

ランサムウェアによる脅威は増大し続けており、犯罪組織は 2019年後半から恐喝によって利益を得る機会を最大化するために、ランサムウェアとデータ漏洩（ろうえい）攻撃を組み合わせるようになってきた。過去６カ月間に要求された身代金の平均額は 350万ドル（約４億円）に上る。さらに、ランサムウェア攻撃からの復旧にかかる平均コストは推定８万4000ドル（約 966万円）を超えるというデータもある。復旧に向けたダウンタイムのコストは、通常、実際の身代金額の５倍から 10 倍にもなるため、被害を受けた組織の 58% が身代金を支払ってしまっているというデータも確認されている。ただし、犯罪組織に対して身代金を支払えば、米国政府による制裁リスクに直面することになる。金銭的被害の