サイバーセキュリティ経営ガイドライン・概要

１．サイバーセキュリティは経営問題

○ 顧客の個人情報を収集・活用する、営業秘密としての技術情報を活用する、プラントを自動制御する、など様々なビジネスの現場において、IT の利活用は企業の収益性向上に不可欠なものとなっている。

○ 一方、こうしたビジネスを脅かすサイバー攻撃は避けられないリスクとなっている。純利益の半分以上を失うような攻撃を受けた企業も存在するなど、深刻な問題を引き起こすこともある。そして、その防衛策には、セキュリティへの投資が必要となる。つまり、企業戦略として、IT に対する投資をどの程度行うのか、その中で、どの程度、事業継続性の確保やサイバー攻撃に対する防衛力の向上という企業価値のためにセキュリティ投資をすべきか、経営判断が求められる。

○ また、サイバー攻撃により、個人情報や安全保障上の機微な技術の流出、インフラの供給停止など社会に対して損害を与えてしまった場合、社会から経営者のリスク対応の是非、さらには経営責任が問われることもある。

○ 本ガイドラインは、大企業及び中小企業（小規模事業者を除く）のうち、IT に関するシステムやサービス等を供給する企業及び経営戦略上 IT の利活用が不可欠である企業の経営者を対象として、サイバー攻撃から企業を守る観点で、２．経営者が認識する必要がある「３原則」、及び３．経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部(CISO（最高情報セキュリティ責任者：企業内で情報セキュリティを統括する担当役員)等)に指示すべき「重要１０項目」をまとめたものである。

２．経営者が認識する必要がある「３原則」

(1) セキュリティ投資に対するリターンの算出はほぼ不可能であり、セキュリティ投資をしようという話は積極的に上がりにくい。このため、サイバー攻撃のリスクをどの程度受容するのか、セキュリティ投資をどこまでやるのか、経営者がリーダーシップをとって対策を推進しなければ、企業に影響を与えるリスクが見過ごされてしまう。

(2) 子会社で発生した問題はもちろんのこと、自社から生産の委託先などの外部に提供した情報がサイバー攻撃により流出してしまうことも大きなリスク要因となる。このため、自社のみならず、系列企業やサプライチェーンのビジネスパートナー等を含めたセキュリティ対策が必要である。

(3) ステークホルダー（顧客や株主等）の信頼感を高めるとともに、サイバー攻撃を受けた場合の不信感を抑えるため、平時からのセキュリティ対策に関する情報開示など、関係者との適切なコミュニケーションが必要である。

３.情報セキュリティ対策を実施する上での責任者となる担当幹部（CISO 等）に指示すべき「重要１０項目」

指示１：サイバーセキュリティリスクへの対応について、組織の内外に示すための方針（セキュリティポリシー）を策定すること。

指示２：方針に基づく対応策を実装できるよう、経営者とセキュリティ担当者、両者をつなぐ仲介者としての CISO 等からなる適切な管理体制を構築すること。その中で、責任を明確化すること。

指示３：経営戦略を踏まえて守るべき資産を特定し、セキュリティリスクを洗い出すとともに、そのリスクへの対処に向けた計画を策定すること。

指示４：計画が確実に実施され、改善が図られるよう、PDCA を実施すること。また、対策状況については、CISO 等が定期的に経営者に対して報告をするとともに、ステークホルダーからの信頼性を高めるべく適切に開示すること。

指示５：系列企業やサプライチェーンのビジネスパートナーを含め、自社同様に PDCA の運用を含むサイバーセキュリティ対策を行わせること。

指示６：PDCA の運用を含むサイバーセキュリティ対策の着実な実施に備え、必要な予算の確保や人材育成など資源の確保について検討すること。

指示７：IT システムの運用について、自社の技術力や効率性などの観点から自組織で対応する部分と他組織に委託する部分の適切な切り分けをすること。また、他組織に委託する場合においても、委託先への攻撃を想定したサイバーセキュリティの確保を確認すること。

指示８：攻撃側のレベルは常に向上することから、情報共有活動に参加し、最新の状況を自社の対策に反映すること。また、可能な限り、自社への攻撃情報を公的な情報共有活動に提供するなどにより、同様の被害が社会全体に広がることの未然防止に貢献すること。

指示９：サイバー攻撃を受けた場合、迅速な初動対応により被害拡大を防ぐため、CSIRT（サイバー攻撃による情報漏えいや障害など、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）の整備や、初動対応マニュアルの策定など緊急時の対応体制を整備すること。また、定期的かつ実践的な演習を実施すること。

指示１０：サイバー攻撃を受けた場合に備え、被害発覚後の通知先や開示が必要な情報項目の整理をするとともに、組織の内外に対し、経営者がスムーズに必要な説明ができるよう準備しておくこと。