情報セキュリティガバナンス：

近年、大規模な個人情報漏えい事故が多発しており、企業における情報セキュリティ対策が社会的な関心事項となっている。一方で、2015年6月1日、東京証券取引所が上場企業に対して、コーポレートガバナンスの実現に向けた主要原則となる「コーポレートガバナンス・コード」の適用を開始した。デロイト トーマツ リスクサービス マネジャーの森島直人氏は、個人情報管理のさらなる強化を前提とした上で、「情報セキュリティについても、コーポレートガバナンスの向上が社会的に求められるようになってきている」と指摘、「現在の企業には利害関係者に対する情報開示を意識した情報セキュリティ態勢を構築し、運用していくことが求められている」と強調する。

【ガバナンスの中心となるのは“外部統制(＝モニタリング)】：

デロイト トーマツ リスクサービスマネジャー　森島 直人 氏

まず森島氏は、「ガバナンスは3つの構成要素から成っている」と説明する。1つめがコントロール、2つめがマネジメント、3つめがモニタリングだ。1つめのコントロールは管理策と呼ばれるもので、業務上してはいけないこと、あるいはしなければならないことを定めた具体的なルールのことだ。次にマネジメントは、たとえばリスクを評価して、ルールの維持管理をしていく仕組みのこと、そしてモニタリングは、組織外の利害関係者が、企業のルール及びその維持管理体制を継続して監視する仕組みのことだ。情報セキュリティの係るガバナンスでは、株主、法人顧客、個人顧客の3者が利害関係者の中心となる。「ここでいうモニタリングとは、2つめのマネジメントのフェーズにおいて企業内で回すPDCAサイクルのチェックに相当するものではなく、社外の利害関係者が企業をモニタリングしていく、あるいは企業の情報セキュリティ体制に対する要請を発信し、企業がそれをキャッチする関係性のことを指す。ガバナンスにおいては、この“外部統制”が重要な機能で、実は最近ではこのモニタリングの部分を指して、ガバナンスということが多くなってきている」。現在では経営者が結果責任を問われやすい環境にあり、攻めの経営判断を下すことが非常に難しい状況だ。たとえば収益拡大のために新しい個人情報の収集を伴う事業を開始する場合や、コスト削減のためにクラウドサービスやBYODの導入を検討する場合、情報漏えい時の結果責任追及を想定してやっぱり止めようという話にもなりかねない。「そこで普段から利害関係者と積極的なリレーションを構築しておくことで、自分たちの情報セキュリティに対する考え方を伝えると同時に、それに対してフィードバックをもらってセキュリティ対策に反映していくことも可能となる。それが企業価値の向上と、有事における企業価値の毀損を低減していくことになり、ひいては経営者を結果責任から守ることにも繋がる。そのためにも利害関係者を巻き込んでいく必要がある」

【情報セキュリティにおけるガバナンスの仕組みは、3つの軸で整理する】

企業と利害関係者とのリレーションにおいては、企業には、自社の「状況を伝える」ことと、利害関係者からの「要請を把握する」ことの2つの取り組みが求められることになる。「伝えることについては、特に経営戦略や経営課題、あるいはリスクやガバナンスに関わる情報などの“非財務情報”について積極的、主体的に開示していくべきだとコーポレートガバナンス・コードに記されている。一方、要請を把握していく内容については明記されていないが、基本的には利害関係者の要望に応えていくことになる」。まず企業側が開示する情報について、株主が注目しているのは株価や企業価値に影響を与える情報で、たとえば平時なら情報セキュリティ事故が起きない体制が構築されているか、有事なら株価がどうなるのかなどに関心がある。また法人顧客は、平時なら業務委託時に提供した自社の情報が適切に取り扱われているか、事故が発生したらどう対応してくれるのかが大きな関心事で、有事における自社の情報に対する影響についても非常に注意を払っている。そして個人顧客は、平時は情報セキュリティに関心がない顧客と非常に関心を持っている顧客の大きく2つのパターンに分かれるが、有事の際には、いずれも感情的に反応し、もうこの会社の製品やサービスは使わないといった言動を取ることが少なくない。「情報セキュリティにおけるガバナンスのあり方を考えるためには、利害関係者とのリレーションを、状況を伝える／要請を把握するという軸、平時か／有事かという軸、利害関係者の種類という3つの軸から整理していくことが重要だ。特に社内体制は、状況を伝える／要請を把握する、有事か／平時か、の2軸で考えることで整理することができる(情報セキュリティガバナンスの仕組みは3軸から整理する」

【ISMSでは、利害関係者の要請を把握することを求めている】

企業が行う情報セキュリティ対策のフレームワークとして、ISMS(情報セキュリティマネジメントシステム)がある。リスクとコストのバランスを取りながらセキュリティレベルを最適化していくための仕組みで、ISMS適合性評価制度の要求仕様であるISO/IEC 27001:2013や、ISMSに関するベストプラクティス集であるISO/IEC 27002:2013といった標準規格がある。ISMSでは基本的にPDCAサイクルを回していくことになる。P(=Plan、計画)のところでは、まず、守るべき情報資産とそれに対する脅威を把握し、具体的にどれぐらいのリスクがあるかを明らかにする。次に、それにどう対応するかの経営判断を行い、リスク対応計画を策定する。続くD(=Do、実践)では、リスク対応計画に基づいてリスク対応策を実施する。C(=Check、チェック)では対応策の実施状況やリスクの軽減状況を社内的にモニタリングし、不備が見つかればA(=Act、是正措置)で改善を行う。「ISO/IEC 27001:2013では、Planのフェーズでリスクの把握と対応策の策定を実施する際、利害関係者の情報セキュリティに関する要求事項をインプットとして把握するよう求めている。また、Checkのフェーズでも、マネジメントレビューにおいて利害関係者からのフィードバックを考慮するよう求めている。つまりISMSの規格の中にも、ガバナンスに関する要求事項が入っているということ」。こうしたISMSの要求も考慮して、企業には利害関係者の要請を一元的に把握する仕組みを構築することが求められる。たとえば株主なら経営企画部、個人顧客ならコールセンタなど、企業内には各利害関係者からのフィードバックを受ける様々な部署があるが、それらに集まる情報を一元的に集約し、情報セキュリティ部や品質管理部など関係各所に伝えていく体制が必要だ。「一方ISMSの中では、企業から状況を伝える方法については明確に決められていないため、その仕組みについては別途、設計、構築していく必要がある。ただし、ISMSを構築している、あるいはリスク管理を行う体制を構築しているということ自体が、利害関係者に対して伝えていくべきコンテンツになる」。

【CSIRTの活動では、情報開示の仕組みを作っていくことが大事】

現在、発生したインシデントによる影響を最小限に抑えるために、CSIRT(Computer Security Incident Response Team)の設置を検討する企業が増えている。CSIRTでは、被害を受けることを前提として、インシデントの発見直後から終息までの損害額を最小化することを主なミッションとする。ISMSのような標準規格はないが、一般的に日常的活動、インシデント対応、事後活動という3つの機能を提供する。このうち中心となるのがインシデント対応だ。検出と報告→トリアージ(=対処すべきインシデントの優先順位付け)→意思決定と対処という3つのステップで行い、状況に応じてトリアージ、意思決定と対処の2つのフェーズを繰り返す。そのインシデント対応の前段階として日常的活動があり、何か起きた時にすぐに動けるようなルールや体制作りなどを行う。そして事後活動では、原因究明やインシデント対応時の手順の見直しなどを行い、日常的活動やインシデント対応にフィードバックしていく。「CSIRTのガイドラインとしては、ISO/IEC 27035:2011やNIST SP800-61 Rev.2、RFC2350などの文書があるが、内容はバラバラだ。それというのも、どのようにインシデントを抑えていくか、どの範囲まで対応するかは企業のポリシーによって異なるからだ。しかしいずれの文書も、情報開示が非常に重要だという点を指摘している。その意味で、CSIRTの活動の中では、情報開示の仕組みを作っていくことが非常に重要となる」。具体的には、インシデント対応における意思決定と対処のフェーズで情報開示を行うことになり、ここでは被害の抑制、問題の除去、サービスの回復という段階を踏むが、この段階ごとで開示する情報は異なってくる。そのため、広報担当者をCSIRTのメンバーに入れておくことが非常に重要」。一方、利害関係者からの要請を把握する点については、CSIRTのどの文書でも触れられていないが、インシデント自体が終息したように見えても、その後の世間のレピュテーション(=評判)によっては、ブランド価値の低下が起こり得る。自社が開示した情報に対して世の中がどんな反応を示しているかを迅速に掴み、適切に対応する、あるいはインシデント対応に反映していくという取り組みも重要だ。「ISMSは、平時に利害関係者からの要請を把握する機能を持っている。一方、CSIRTは有事の際に、自社の対応状況を伝える役割と、利害関係者からの反応をキャッチする役割も果たすものだ。情報セキュリティにおけるガバナンスを強化していく上では、こうした仕組みを機能の一部として認識し、有機的に取り込んで全体的な構成を設計することが重要だ」。