情報セキュリティ／サイバーセキュリティに関する情報開示では何が求められているのか

JCIC 主任研究員　青木優美
2020 年 5 月 15 日

企業・組織のサイバーセキュリティの取り組み状況をひろく一般に開示することが議論されている[1]。本稿では、サイバーセキュリティへの取り組みの可視化に関する国内の議論を振り返り、情報を開示する/あるいは開示を求める際の考え方を整理する。情報開示の目的と効果は 3 つの観点から議論されてきた。

１.情報セキュリティ対策水準向上の内的観点から

過去の取り組みとしては、経済産業省で 2005 年 3 月期の「企業における情報セキュリティガバナンスのあり方に関する研究会」から派生した「情報セキュリティガバナンス確立促進事業」において、情報セキュリティガバナンス施策ツールのひとつとして「情報セキュリティ報告書モデル」が提示された[2]。このひな形は、情報セキュリティガバナンス確立のための経営者の取り組みを支援する目的で作成された。

同様に組織の取り組みを支援するツールとして、「情報セキュリティガバナンス導入ガイダンス」「情報セキュリティ関連法令の要求事項集」「ISMS」「情報セキュリティ対策ベンチマーク」「事業継続計画策定ガイドライン」「情報セキュリティ格付」「情報セキュリティ監査」などが示されている。

日本経済団体連合会が 2018 年 3 月に著した「経団連サイバーセキュリティ経営宣言[3]」もこれと同様に、組織内の取り組み方針を宣言したものだ。「いまやすべての企業にとって価値創造とリスクマネジメントの両面からサイバーセキュリティ対策に努めることが経営の重要課題となっている」との認識の下、サイバーセキュリティを経営課題と認識し、実施事項としてセキュリティ方針の策定や社内外におよぶ体制の構築、対策の実施などを掲げている。これを受け、複数の企業グループがサイバーセキュリティ経営宣言を策定、公表している。2020 年 3 月には「経団連サイバーセキュリティ経営宣言に関する取組み[4]」が公開された。企業に対し、自社の取り組みの成熟度を測り、対策方針を社外に示し、サイバーセキュリティ人材のスキルの可視化とトレーニングを進めるよう促している。

---

[1] 一例として、日本サイバーセキュリティイノベーション委員会「サイバーセキュリティ情報公開のポイント ～経営者の取組み姿勢が重要～」https://www.j-cic.com/pdf/report/Disclosure-Report.pdf

[2] 経済産業省、関連報告書・ガイドライン類一覧、http://www.meti.go.jp/policy/netsecurity/secgov-documents.html

[3] 日本経済団体連合会「経団連サイバーセキュリティ経営宣言」2018 年 3 月 16 日、https://www.keidanren.or.jp/policy/2018/018.html

[4] 日本経済団体連合会「経団連サイバーセキュリティ経営宣言に関する取組み」2020 年 3 月 17 日、https://www.keidanren.or.jp/policy/2020/025_honbun.pdf

2.外的観点：投資判断材料を求める観点から

上場企業等に対しては、金融商品取引法等でリスク情報の開示が規定されている。公益と投資者を保護する観点から一定の情報開示を求める趣旨で、事業特性に応じたリスクの整理と管理策の取り組み状況を有価証券報告書で開示するよう求められている。

該当する企業は、金融庁が定める「企業内容等の開示に関する留意事項について（企業内容等開示ガイドライン）」と市場が定める規則を参照して開示事項を選択する。金融庁は企業に対し、投資判断に誤解を生じさせないという観点から、重要と考えられる情報を、正確、迅速、明瞭に、かつ客観的に記載するよう求めている。同時に、他の規則等に抵触しないように開示する必要があるとも指摘している。開示ガイドライン等に沿ったリスク情報の記述に関しては、金融庁が好事例集を公開、適宜更新している[5]。企業は、好事例とされた報告書の発行主体の業種や規模を考慮して参考情報を得ることができる。

また、国内証券取引所に上場する企業に対しては、東京証券取引所の場合は新規上場時にコーポレートガバナンス報告書を提出することが新規上場申請者施行規則で定められている。他の国内市場においても、総会後速やかにコーポレートガバナンス報告書を提出するよう求める[6]など、情報開示が求められる。多くの企業においては、開示事項のうち情報セキュリティに関係するのは「IV 内部統制システム等に関する事項」だろう。

情報開示を求める/求められることを、企業側はどうとらえているのだろうか。これについて、数年前の資料にはなるが、内閣サイバーセキュリティセンターが 2015 年 3 月期に実施した「企業の情報セキュリティリスク開示に関する調査[7]」が参考になる。調査対象とされたのは、その時点で日経平均に採用されていた東京証券取引所の上場企業 225 社だ。その結果を見ると、国内上場企業の有価証券報告書におけるサイバーリスク記載状況等が調査されており、業種ごとにリスクの分布や比重等が異なる点に改めて注意が促される。また、21 社を対象としたヒアリング調査では、情報開示に関するガイドラインを求める声が複数の企業から上がったとされる。

2018 年 3 月期には、総務省の「IoT セキュリティ総合対策[8]」において「セキュリティ対策に係る情報開示の促進」の施策に「セキュリティ対策に係る情報開示の促進」が盛り込まれた。サイバーセキュリティ対策を講じている企業が第三者から評価される仕組みが必要だとの認識の下、任意の情報開

---

[5] 金融庁、企業内容等開示ガイドライン等、https://www.fsa.go.jp/common/law/kaiji/index.html、同「記述情報の開示の好事例集」の更新について、2019 年 12 月 20 日、https://www.fsa.go.jp/news/r1/singi/20191220.html

[6] 一例として福岡証券取引所「提出書類の概要」、2019 年 5 月 27 日、https://www.fse.or.jp/files/lis_fmt/teisyutsugaiyo20190527.pdf

[7] 平成 26 年度内閣サイバーセキュリティセンター委託調査「企業の情報セキュリティリスク開示に関する調査 調査報告書」（受託者：ニュートン・コンサルティング株式会社）、https://www.nisc.go.jp/inquiry/pdf/kaiji_honbun.pdf

[8] 総務省「IoT セキュリティ総合対策」、2017 年 10 月 3 日、https://www.soumu.go.jp/main_content/000510701.pdf

示を促進するためのガイドラインを策定する必要があると結論づけられた。米国上場企業の情報開示において、セキュリティ対策に関する記載推奨（拘束力を有しない）事項が定められていることを参考にしたという[9]。

その後 2019 年 6 月には総務省が「サイバーセキュリティ対策情報開示の手引き」（以下「手引き」）を公表した[10]。手引きでは、情報開示の目的を 6 点に整理している（下図）。この段階では、グループ企業や委託先のサイバーセキュリティ対策の意識向上に資するといった企業内の視点も盛り込まれている。他と比較して記載要求事項の説明が具体的であることから、ここでは手引きの内容を紹介する。

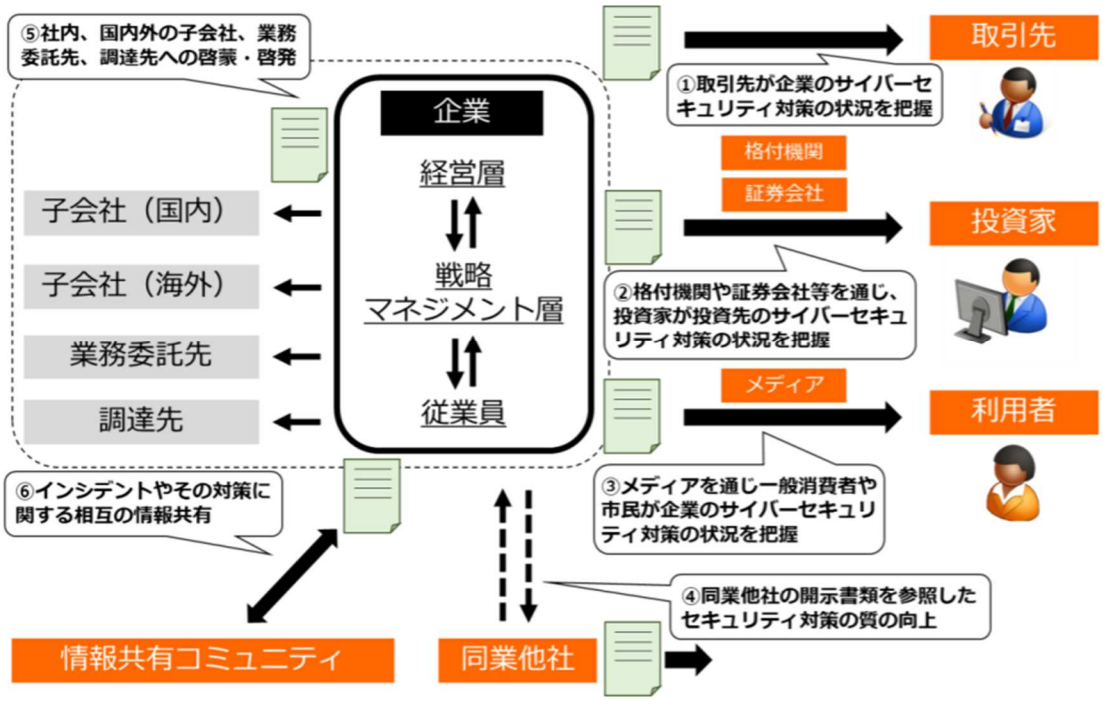

図　企業をとりまくステークホルダとサイバーセキュリティ対策の情報開示

（出典：総務省 サイバーセキュリティ統括官「サイバーセキュリティ対策情報開示の手引き」、p.9）

手引きでは、一般に企業において実施されるのが望ましい 10 種類のサイバーセキュリティ対策と情報開示のポイント、記載例が紹介されている。実施が望ましいサイバーセキュリティ対策として挙げ

---

[9] Form 10-K の Item 1A - “Risk Factors”を指すと思われる。詳しくは U.S. Securities and Exchange Commission, How to Read a 10-K, https://www.sec.gov/fast-answers/answersreada10khtm.html を参照のこと。また、SEC は上場企業向けにサイバーセキュリティに関するリスクとインシデントを開示する際のガイダンス文書（拘束力を有しない）を発行しており、2018 年 2 月 26 日に発効済み。

[10] 総務省「サイバーセキュリティ対策情報開示の手引き」、2019 年 6 月 28 日、https://www.soumu.go.jp/main_content/000630516.pdf

られているのは「サイバーセキュリティ経営ガイドライン Ver2.0[11]」において「サイバーセキュリティ経営の重要 10 項目」の指示項目で、下記のとおり。なお、太字で記した事項の記載においては、具体的に開示することでサイバー攻撃等を誘発するリスクもある点に考慮を要するとして、手引きでは「特に④、⑤、⑦、⑧、⑨などについては開示する内容について留意が必要な場合があり、全体として経営層の責任の上で開示のメリットとデメリットを判断の上で開示の内容を考えていく必要がある」と指摘されている。

実施が望ましいとされるサイバーセキュリティ対策

① サイバーセキュリティ対応方針策定
② 経営層によるリスク管理体制の構築
③ 資源（予算、人員等）の確保
④ リスクの把握と対応計画策定
⑤ 保護対策（防御・検知・分析）の実施
⑥ PDCA の実施
⑦ 緊急対応体制の整備
⑧ 復旧体制の整備
⑨ 取引先・委託先やグループ単位のサイバーセキュリティ対策
⑩ 情報共有活動への参加

また、ステークホルダへの情報開示が目的であるため、同業他社、同規模企業との対比、1 社の取り組みの推移把握を可能にする配慮が求められている[12]。

3.外的：取引先選定の観点から

企業・組織が自らのリスク管理に取り組む過程で、いわゆるサードパーティリスク（業務委託先等、自組織外に起因するリスク）を認識する必要がある。組織によっては、こうした問題意識から、サプライチェーン管理のなかで個々の取引先のリスク評価項目として情報セキュリティ対策／サイバーセキュリティ対策の状況を考慮する。前述の手引きにおいても、情報開示により、必要な対策が取られていることを取引先が把握でき、企業への信頼感が増すことを期待している。

ある組織のサイバーセキュリティ対策状況を組織の外から理解することは通常困難だ。そこで、公知情報を収集する、サードパーティリスク評価サービスを利用する（公知情報のみに基づく／公知情報に加えて聴取等を含む詳細調査を実施し、評価する）、認証取得状況を検索する、特に高リスク分野

---

[11] 経済産業省、情報処理推進機構「サイバーセキュリティ経営ガイドライン Ver2.0」2017 年 11 月 16 日、https://www.meti.go.jp/press/2017/11/20171116003/20171116003-1.pdf

[12] 自社の取り組みを開示する際に、基準なくして不特定者による比較を考慮することは困難であるため、手引きの観点から「記載が望ましい」とされた事項を本稿付録にまとめた。

に関して取り組み状況を定期的に照会する、遵守事項を契約書面に反映させる、誓約書の提出を求める、相手方の協力を得て現地調査を実施する等、さまざまな手段を組み合わせて必要な情報を収集する。調査対象項目や調査手法は、サイバーリスクの比重と必要な情報の粒度を考慮して選択することになる。いずれの手段においても、情報セキュリティガバナンスの観点から、評価基準を組織自らが十分把握し、調査の有効性を確保する必要がある。場合によっては、脅威動向やサイバーリスクの位置づけの変化を調査・評価枠組に反映させることが可能でなければならない。

いずれの観点からも、従来企業・組織内で情報セキュリティ対策として進められてきた施策を適時見直してサイバーリスクに備えることができているかどうかが問われる。

付録

表：情報開示が求められるサイバーセキュリティ対策事項の例

項番	企業において実施が望まれるサイバーセキュリティ対策*	開示内容のイメージ	手引きで紹介された記載例			
1	サイバーセキュリティ対応方針策定	経営陣のメッセージ 組織におけるサイバーリスクの位置づけ	リスク認識（例：「サイバーセキュリティを重大リスクと定義している」）	情報セキュリティ基本方針、個人情報保護方針の開示状況	参照・準拠するフレームワーク	取得済認証の名称と取得件数
2	経営層によるリスク管理体制の構築	責任者設置状況 体制の構造 活動内容	情報管理の責任者（例：社長、CIO、CISO）、CIO等の設置状況（とその任命者）	企業グループを包含する会議体の設置	リスク管理体制の概要	アセスメントの実施
3	資源（予算、人員等）の確保	従業員等の教育（定量表現） セキュリティ対策予算	従業員教育の概要（例：全従業員に毎年実施、節目研修時に実施、職務別実施）	社内認定制度の存在と目的	当該年度に開示したセキュリティインシデントへの事後対応費用総額	
4	リスクの把握と対応計画策定	守るべき情報とリスク 対策計画 すでに実施済の対策	情報保護施策の例示	個人情報委託先選定基準の策定・運用状況		
5	保護対策（防御・検知・分析）の実施	防御策 ログ監視・検知等の取り組み状況 SOC整備状況	企業グループを包含する予防・検知システムの導入	常時監視の実施	ログ取得・集約・分析体制の構築	
6	PDCA の実施	リスク管理KPIと実績の対比 改善施策 認証取得状況	ルールに該当する事象への対応率	システム展開計画と達成率	情報セキュリティに関する習熟度テストの合格率	外部への発表を要するインシデントの発生状況、再発防止策
7	緊急対応体制の整備	CSIRTなどのインシデント対応体制 インシデント発生時対応演習の実施状況	CSIRTの設置	情報収集の実施	訓練・演習の実施（自社開催でないものを含む）	社外の情報共有活動への参加
8	復旧体制の整備	事業継続計画	CSIRTの設置			
9	取引先・委託先やグループ単位のサイバーセキュリティ対策	取引先等のサイバーセキュリティ対策把握方法 子会社の対策強化状況	調達ガイドラインの策定と取り組み状況	説明会の実施	啓発資料・トレーニングコンテンツの提供	現地訪問調査と改善申し入れの実施
10	情報共有活動への参加	ISAC等への参加状況 IPA、JPCERT/CC等の情報の活用状況	参加している団体	参加している分野横断演習		

*各項目について、詳しくは「サイバーセキュリティ対策情報開示の手引き」pp.15-16ならびに経済産業省、情報処理推進機構「サイバーセキュリティ経営ガイドライン Ver2.0」を参照のこと。

出典：「サイバーセキュリティ対策情報開示の手引き」をもとにJCIC作成

https://www.soumu.go.jp/main_content/000630516.pdf