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
一般社団法人 日本経済団体連合会

１．経団連の取組み

Society 5.0 の実現には、多種多様な大量のデータを流通・利活用することによって、イノベーションを創出するとともに、社会的課題の解決を図ることが求められる。一方、データの流通・利活用にあたっては、サイバーセキュリティの確保が前提となる。

経団連は、サイバーセキュリティ強化のために、政府への提言として「サイバーセキュリティ対策の強化に向けた提言」(2015 年２月)、「サイバーセキュリティ対策の強化に向けた第二次提言」(2016 年１月)、「Society 5.0 実現に向けたサイバーセキュリティの強化を求める」(2017 年 12 月）を発表した。

また、2018 年 3 月に公表した「経団連サイバーセキュリティ経営宣言」(以下「経営宣言」という）では、経済界が全員参加でサイバーセキュリティ対策を推進することで安心・安全なサイバー空間の構築に貢献することを表明し、サイバーセキュリティ対策についていっそうの啓発・推進を図った[1]。

２．現状の課題

以上のような取組みの成果もあり、サイバーセキュリティ対策に関する経営者の意識は高まってきている[2]一方、具体的な行動に至る段階で悩みを抱えているという声も聞く。

（１）サイバーセキュリティ対策に関する取組みの停滞

経営層はサイバーセキュリティを経営上のリスクとして認識しつつある一方、現場レベルでは、サイバーセキュリティは自身の業務とは関係ない、情報システム部門の仕事であるという意識が未だに存在しているという声が聞かれるな

[1] その他、経営者のサイバーセキュリティ対策の推進のため、米国 Internet Security Alliance と共同で、サイバーリスク管理のために取締役が具体的に取り組むべき事項をまとめた「サイバーリスクハンドブック　取締役向けハンドブック日本版」(2019 年 10 月）を発行した。

[2] トレンドマイクロ株式会社の「法人組織におけるセキュリティ実態調査 2019 年版」〈 https://resources.trendmicro.com/jp-docdownload-form-m164-web-sor2019.html 〉によれば、経営層・上層部が「セキュリティを事業継続上あるいは組織運営上のリスクとして十分認識している」または「セキュリティを事業継続上あるいは組織運営上のリスクとしてある程度認識している」と回答した割合は 70%以上に及ぶ。

ど、サイバーリスクに関する取組みが全社的な規模で進んでいない現状がある。こうした問題の原因の一つとして、サイバーセキュリティ対策の客観的な把握が困難であることが考えられる。この課題を解決するために、客観的な評価指標を使って、サイバーセキュリティ対策の実施状況を可視化させることが必要である。可視化により、経営層は、自社のサイバーセキュリティ対策の状況を具体的に把握できるようになり、全社的な取組みの実施を促すことにつながる。

（２）サイバーセキュリティ人材に関する不十分な実態把握

現在、日本全体でサイバーセキュリティ人材が不足していると言われている[3]。しかし、サイバーセキュリティに携わる人材は、いわゆるホワイトハッカーのような専門人材から、ユーザー企業でサイバーセキュリティ業務に従事する人材、サイバーセキュリティの理解をもって経営判断を補佐するような人材まで様々であり、具体的にどういった人材が、どのくらい不足しているのかを把握できていない。サイバーセキュリティ人材といっても多様であり、その不足の実態を正確に把握するためには、組織内で担うべき業務や役割に応じて、スキルや経験を客観的な指標によって可視化させることが必要である。

３．サイバーセキュリティ経営のいっそうの強化にあたり

本章では、前章で指摘した課題の解決策を中心に、経営宣言について経済界の対策をさらに推進するうえで必要と思われる取組みを提示する。経団連の各会員においては、各項目を参考に、具体的な行動のあり方を工夫するとともに自主的に実践していくことを期待する。

（１）成熟度の可視化

【具体的取組み】

① 自社の業種や業界に応じて適切なフレームワークを選択し、自社のサイバーセキュリティ対策の取組みレベル(以下、「成熟度」という)についてセルフアセスメントを行う。参考までに、成熟度評価のフレームワークの一部を紹介する。

- ✓ 独立行政法人 情報処理推進機構『情報セキュリティ対策ベンチマーク』
- ✓ Federal Financial Institutions Examination Council（米国連邦金融機関検査協議会）『Cyber Security Assessment Tool』
- ✓ The Center for Responsible Enterprise And Trade（CREATe.org）『Leading Practice for Cybersecurity』

[3] 経済産業省「IT 人材の最新動向と将来推計に関する調査結果」<https://www.meti.go.jp/policy/it_policy/jinzai/27FY/ITjinzai_report_summary.pdf>〔参照 2020-01-14〕

- ✓ The Information Systems Audit and Control Association (ISACA)『Cybermaturity Platform』
- ✓ The Information Security Forum『The ISF Maturity Model－Accelerator Tool』
- ✓ The U.S. Department of Defense (DoD)『Cybersecurity Maturity Model Certification (CMMC) Version 1.0』

② 自社の事業規模、予算、事業の IT 依存度等に応じて、コンサルティングファーム等、第三者からの成熟度評価を受けることも検討する。

③ サイバーセキュリティを製品・サービスの品質管理の一要素とし、成熟度の向上を品質向上と捉える。

④ 成熟度を取締役会や経営会議等にて経営陣に報告する。そのうえで、成熟度向上のために、サイバーセキュリティ対策の目標設定を行うとともに、戦略・対策・投資計画などを見直し、再構築する。

【効果】

① 成熟度の可視化により、望ましい水準と自社の取組み状況のギャップが把握できるようになるため、サイバーセキュリティ対策の目標設定が容易になり、具体的対策の実施につなげることができる。

② サイバーセキュリティ対策が成熟度として目に見える形で提示できるため、取締役会や経営会議等、サイバーセキュリティ専門部署以外での報告でも理解を得やすい。それに伴い、自社のリスク管理全般の枠組みにおいてサイバーリスクを検討することが可能となり、投資等リソースの配分の上積みも期待できる。また、経営層や上層部の理解が得られることで、経営方針や中長期計画等、企業の戦略や計画にサイバーセキュリティ対策が反映される可能性も高まる。

③ サイバーセキュリティを製品・サービスの品質管理の一要素と捉えることで、現場の業務プロセスにおいてもサイバーセキュリティ対策が浸透し、社内のサイバーセキュリティ意識醸成を図ることができる。

（２）サイバーセキュリティ対策の方針に関する情報発信

【具体的取組み】

アニュアルレポート、統合報告書、CSR 報告書/サステナビリティ報告書等、任意の媒体において、自社のサイバーセキュリティ対策の方針を発信する。

【効果】

① 同業他社等、事業規模や事業領域が似ている会社と自社の対策方針を比較することで、自社のサイバーセキュリティ対策強化の契機となり、社会全体のサイバーセキュリティ対策の底上げにつながることが期待される。

② 取引先や投資先候補が適切なサイバーセキュリティ対策方針を講じているかどうかを把握することで、選定時の参考にすることができる。

③ 対外的にサイバーセキュリティ対策方針の情報発信を行うことで、外部委託先などサプライチェーン上でつながる企業のサイバーセキュリティ対策の意識向上につながることが期待される。

④ 透明性の確保に取り組む姿勢や、サイバーセキュリティ対策方針の適切性が投資家や社会から評価され、企業価値が向上する可能性がある。

（３）サイバーセキュリティ人材スキルの可視化

【具体的取組み】

① サイバーセキュリティ人材のスキルを評価し、自社の人材が持っているスキルと、業務や役割において必要なスキルを比較し、自社に不足するスキルや人材を可視化する。参考までに、人材スキルの評価ツールを紹介する。

- ✓ 一般社団法人サイバーリスク情報センター　産業横断サイバーセキュリティ人材育成検討会(CRIC CSF)『人材定義リファレンス』『OT セキュリティ人材スキル定義リファレンス』
- ✓ 情報セキュリティ教育事業者連絡会（ISEPA)『セキュリティ業務を担う人材のスキル可視化ガイドライン（β版)』

② 自社のサイバーセキュリティ人材に不足する知識や資格等に関する教育を実施する。現在の人員では足りない場合、外部委託と並行して、必要なスキルを持った人材を獲得すべく、人事異動や新規採用を検討する。

【効果】

① 役割・業務に必要なスキルと個人の有するスキルが可視化されることで、企業にとって、組織の透明化・外部リソースおよび社内人材の適切な配置が可能となる。

② サイバーセキュリティ人材にとって、自身のスキルが可視化されることで、目標とする将来像とのギャップが把握でき、キャリアパス設計が容易になる。

③ 仮に企業が自社のサイバーセキュリティの組織体制や人材構成について公表した場合、取引先や投資家が、人材の質(スキル)と量(人数)から当該企業のサイバーセキュリティ耐力を推量することができる。

４．おわりに

Society 5.0 の実現のために、わが国においても社会全体が一丸となってサイバーセキュリティの確保に取り組むことが必要となっている。取組みの一翼を担う企業には、サイバーセキュリティの確保が価値創出や事業継続の前提であることを認識しつつ、主体性を持った対応を行うことが求められる。そういった対応の一つとして、今回、サイバーセキュリティ対策の情報発信を取り挙げた。企業が自主的に公開した情報を市場が評価し、それを受けて企業が取組みを強化するというサイクルが構築されれば、サイバーセキュリティのさらなる強化に寄与することとなる。しかしながら、こうした取組みが進むためには、企業の全経営者・従業員のセキュリティリテラシー向上を含めた、サイバーセキュリティに関する社会全体の理解促進が不可欠である。経団連としてはこれまで、セミナーの開催等の情報発信に努めており、今後ともこうした活動を継続する予定である。

また、今後の課題として、成熟度の公表がある。企業のサイバーセキュリティ対策を定量的に評価できる成熟度の積極的な公表が進めば、他社の取組みとの比較がいっそう容易になることにより、自らの取組みの向上が達成可能となる。その際、成熟度評価のフレームワークの妥当性についての検証および、それを踏まえた不断の見直しが不可欠である。

以　上