

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

背景

- Society 5.0 の実現には、データの流通・利活用によるイノベーションの創出と社会課題の解決が必要。
- データの流通・利活用は、**サイバーセキュリティ確保が前提**。
- 経団連は2015年2月、2016年1月、2017年12月に、サイバーセキュリティ対策の強化を提言。
- 2018年3月には「**経団連サイバーセキュリティ経営宣言**」を
発表し、経済界の全員参加により安心・安全なサイバー空間の構築に貢献することを表明。



サイバーセキュリティ対策に関する**経営者の意識が向上**する一方、**具体的な行動に至る段階で悩みを抱える**企業も存在。

サイバーセキュリティ対策に関する取組みの停滞



サイバーセキュリティ人材に関する不十分な実態把握

1 成熟度の可視化

具体的取組み

- 🎯 フレームワークを使用した**成熟度(※)のセルフアセスメント**
(※)成熟度:サイバーセキュリティ対策の取組みレベル
- 🎯 コンサルティングファーム等、**第三者からの成熟度評価**
- 🎯 **品質管理プロセスへのサイバーセキュリティ組み込み**
- 🎯 **成熟度の経営陣への報告、成熟度向上のための取組み**



効果

- ✓ 望ましい水準と自社の取組み状況のギャップを把握
⇒ **目標設定が容易になり、具体的対策の実施につながる**
- ✓ 取締役会等での報告における**理解の得やすさ**
- ✓ サイバーリスクについてリスク管理全般の枠組みで検討可能
⇒ **リソース配分の上積みが可能**
- ✓ 企業の戦略や計画への**サイバーセキュリティ対策の反映**
- ✓ 現場の業務プロセスにおける**サイバーセキュリティ対策の浸透、社内のサイバーセキュリティ意識醸成**

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における**サイバーセキュリティ対策方針の発信**



効果

- ✓ 他社との比較による、自社のサイバーセキュリティ対策の強化
- ✓ 社会全体のサイバーセキュリティ対策の底上げ
- ✓ 取引先や投資先選定時の参考情報
- ✓ 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
- ✓ 企業価値の向上

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 人材スキルの評価ツールを使って、**サイバーセキュリティ人材のスキルを評価**
 - ② 自社人材のスキルと、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**
- 
- ③ 不足する知識や資格等に関する**教育の実施**
 - ④ 不足人材獲得のために**外部委託と並行して、人事異動や新規採用を検討**
- 

効果

- ✓ 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【企業】
- ✓ キャリアパスの設計【サイバーセキュリティ人材】
- ✓ (仮に企業が、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〉×量〈人数〉でサイバーセキュリティ耐力を推量可能

おわりに

- Society 5.0の実現のために、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。
- 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。
- こうした取組みが進展するためには、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。
- 経団連はこれまで、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予定。

今後の課題として、

- 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つそう容易になり、自らの取組みも向上。
- 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。