Keidanren
Policy & Action

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

一般社団法人　日本経済団体連合会

<背景>
- サイバー攻撃による被害が世界中で拡大するなか、2020年の東京オリパラに向けて対策強化は喫緊の課題。
- サイバーセキュリティの強化は「Society 5.0」の基盤となりうる成長のための最重要分野でもある。
- 経団連は、2015年・2016年に提言を公表し、ある程度の対策は進んだが、まだ道半ばである。
- 2017年11月には経団連「企業行動憲章」を改定し、社会的責任としてサイバー対策に取り組むことを打ち出した。
- あらゆるステークホルダーの連携のもとでより具体的な対策を進めるために、改めて提言を行う。

サイバーセキュリティに関する基本的な視点

①価値創造
- Society 5.0時代には、IoTによりあらゆるモノがサイバー空間と結びつく。サイバーセキュリティ確保が競争力の源となる。
- 中小企業も含めたサプライチェーン全体のサイバーセキュリティ確保が重要。

②危機管理
- サイバー攻撃による情報漏えいやサービス停止など被害が拡大中。IoTなど攻撃の対象も増加。
- 対策を怠れば、関係者から信頼を失いかねない。
- 企業としては、事業継続を重視し、自主的に対策を行うことが必要。

具体的に取り組むべき事項　～自助・共助・公助・国際連携の視点で取り組み推進を～

①意識改革
- 社会全体での意識向上、協調領域としての認識
- セキュリティ・バイ・デザインの実装
- 経営の最重要課題としての認識
- 被害を受けた企業を過度に責めない社会風土醸成

②リソース確保　～ヒト・情報・技術・カネの好循環～

人材育成
- 国民全体のリテラシー向上
- 経営者の理解増進
- 人材育成・維持のエコシステム
- キャリアパス構築、見える化
- 高度人材の厚遇
- 資格普及
- 人材発掘

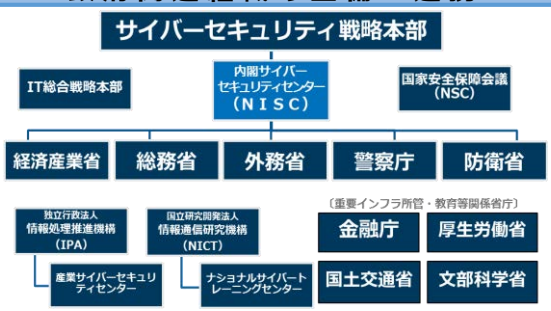
情報共有
- 情報の類型等の整理
- ISAC・ISAOの設立
- 政府支援・情報提供
- アクセス権限管理
- 活用・対応の仕組み
- 国際連携

投資促進
- 官民での積極投資
- サイバー保険の活用
- 共済や全国的組織、シンクタンクの設置
- 対策費への税制・補助金等の公的支援
- 政府予算の大幅拡充

技術対策
- OS等のアップデート
- 中小企業クラウド化
- 商品・サービスのセキュリティ強化
- OTとIT連携への対策
- 研究開発の推進
- 国際標準の先導

③推進体制の整備

政府関連組織の整備・連携



- 関係省庁の役割分担の明確化、施策の一体化、優先順位の共有
- NISCの総合調整機能の強化、予算・人員拡大
- 将来的には情報関連政策を一元的に所管する機関の創設
- 政治のリーダーシップへの期待

企業内外の体制整備
- CISOやCSIRTの設置及びスタッフの充実
- 従業員への継続的な研修や演習
- BCP(事業継続計画）の策定及び訓練
- サプライチェーン全体のサイバーセキュリティ管理
- SOCレポート、各種報告書の活用

④法制度・規範の整備
- 技術進歩に法制度が追いついていないことへの対応
- 不正アクセス禁止法や電気通信事業法の見直し
- 技術標準や対策ガイドラインの整備
- 国際規範の策定に向けた官民の協力・積極参加

経団連アクションプラン　～経団連自らも具体的な取り組みを推進～

①経営層の理解促進
- 「サイバーセキュリティ経営宣言」策定
- 経営者向けセミナー、研修、合宿

②広報・周知活動
- 実態調査、事例集の公開
- 機関紙や説明会を通じた周知

③国際連携
- 国際会合への参加
- 世界経済フォーラムとの連携