資料３－４

Keidanren
Policy & Action

セキュリティマインドを持った企業経営ＷＧ（第４回）

経営とサイバーセキュリティに関する経団連の取り組み

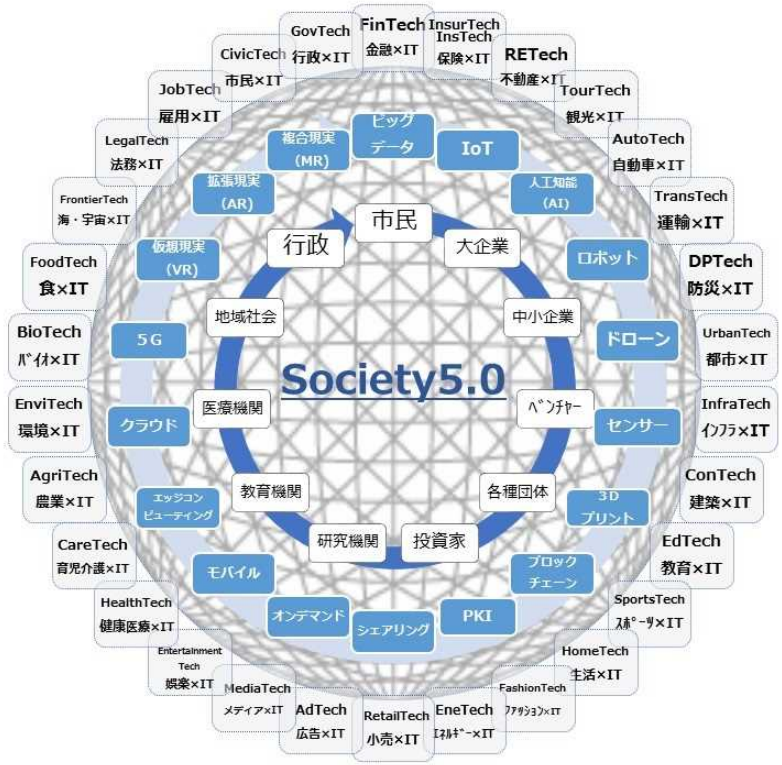
2017年 10月 30日

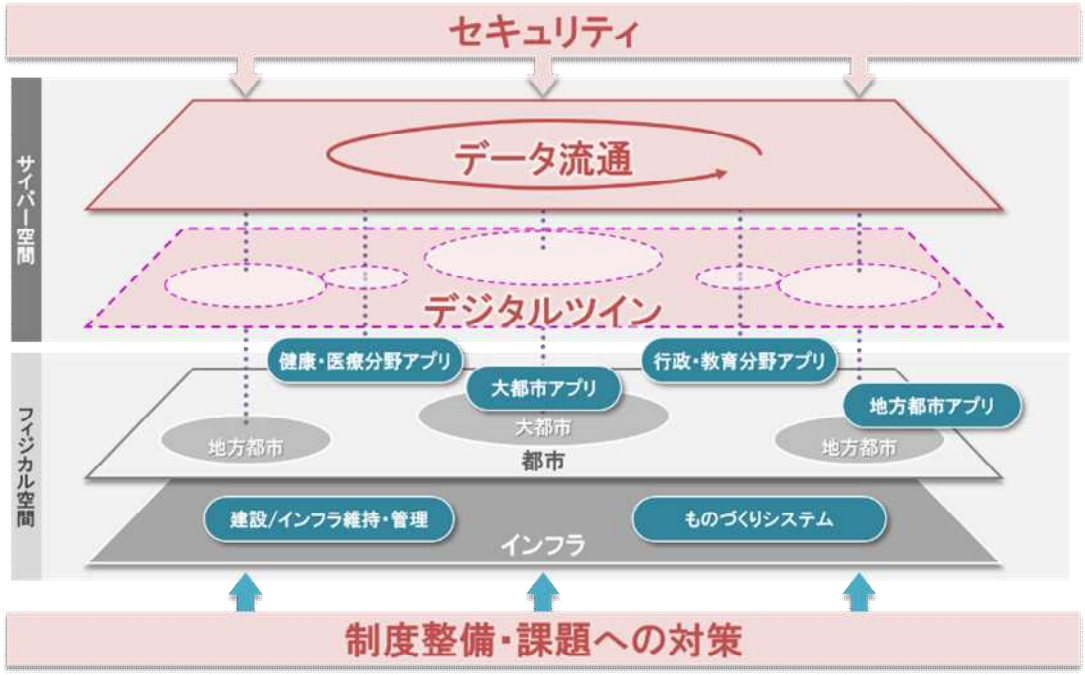
一般社団法人　日本経済団体連合会
情報通信委員会 企画部会長代行
サイバーセキュリティに関する懇談会 座長
（日立製作所　上席研究員）
梶浦　敏範

Society 5.0の実現に向けて

Keidanren
Policy & Action

- 経団連では「Society 5.0」の実現を最重要課題と捉え、日本政府とともに推進。
- Society 5.0では、あらゆる産業のデジタル化が進み、サイバー空間で大量のデータが流通し、イノベーション創出や課題解決に貢献。
- データ流通・活用の前提となるのが、サイバーセキュリティであり、経営課題として取り組むことが必要。





基本的な視点

Keidanren
Policy & Action

①「守り」国家全体の安全を確保する視点

- ✓ 近年、サイバー攻撃の巧妙化により、重要インフラへの攻撃などを通じた物理的な破壊も可能となっている。
- ✓ 業界間・官民間・国際間での連携を強め、リアルタイムに情報共有を行うことが必要である。
- ✓ 重要インフラの多くを担う民間企業が主体的に対策することが求められる。
- ✓ 巧妙化するサイバー攻撃を完璧に防御するのは不可能であり、早期の検知や対応・復旧力を重視した事業継続の観点から対策しなければならない。

②「攻め」サイバー空間で価値を創出する視点

- ✓ Society 5.0では、IoTによりあらゆるモノがインターネットにつながり、そこで生み出されたデータが価値を創出する時代が到来しつつある。
- ✓ 日本の経済社会を支える中小企業も含めて社会全体がサイバー空間につながることで、競争力を高めることができる。
- ✓ グローバル市場でのビジネス環境確保の観点からも、わが国として早急にサイバーセキュリティの強化を図る必要がある。

こうした視点のもと、経団連としてはサイバーセキュリティ確保をSociety 5.0実現に向けた重要課題と捉え、各種役員会等で議論。
特に意識の高い約40社が集い、サイバーセキュリティに関する懇談会を2014年に発足させ、対策強化に向けた提言を行ってきた。

サイバーセキュリティ対策の強化に向けた提言

Keidanren
Policy & Action

■ 経団連では、2015年2月、2016年1月の2度にわたり、サイバーセキュリティ対策の強化に向けた提言を公表するとともに、産業界としての取り組みを提示。

○サイバーセキュリティ対策

(1)情報共有

政府機関と企業による双方向の情報共有。ISAC(情報共有・分析機関）やCSIRT（セキュリティ事案対処チーム）などの業界や企業における設置。機密情報を保全した情報提供。

(2)人材育成

人材の要件の明確化。大学等における人材レベルに応じた教育。
企業における評価や処遇の見直し。産学官による人材育成と維持のシステムの構築。

(3)セキュリティレベルの高いシステムの構築

①社会システム

重要インフラの重点的な防護、範囲の見直し。高度人材が産学官で柔軟に動ける仕組みの構築。

②技術開発とシステム運用

通信検知や攻撃解析などの技術開発。システムの安定的な稼働。
内閣府の戦略的イノベーション創造プログラムやIoT推進コンソーシアムの活動への期待。

(4)国際連携の推進

国際的な議論への積極的な参画。米国、欧州、ASEANなどとの連携。

(5)東京オリンピック・パラリンピックへの対応

大会会場に加えて周辺施設等を含めた総合的な対策の実施。中核となるCSIRTの早期設置。演習・訓練の実施。既存の人材の能力向上。NISC（内閣サイバーセキュリティセンター）を中心とした体制整備や対策のロードマップの策定と実行。

○産業界の取り組み

サイバーセキュリティの確保を経営上の重要項目として位置づけ、経営層の意識を改革。組織・体制の整備、情報共有、人材育成を自主的かつ迅速に推進。ステークホルダーへの自主的な情報開示。セキュリティが確保されたシステム開発や製品提供。サイバーセキュリティ保険の提供。