Keidanren
Policy & Action

サイバーセキュリティ対策の強化に向けた第二次提言（概要）

2016年1月19日
一般社団法人　日本経済団体連合会

1. はじめに

■わが国では、昨年1月にサイバーセキュリティ基本法の施行やサイバーセキュリティ戦略本部の発足など政府の推進体制が強化。
■一方、政府機関や企業に対するサイバー攻撃が増加。昨年5月に日本年金機構から個人情報が流出。
■サイバー空間はイノベーション創出により成長戦略を実現する重要な場。2020年の東京オリンピック・パラリンピック に向け重大な局面。昨年9月に政府はサイバーセキュリティ戦略を閣議決定。
■産学官の連携強化と経済界の具体的な取り組みについて、経団連として第二次提言をとりまとめ。

2. サイバーセキュリティの意義

■公的機関（中央省庁、独立行政法人、特殊法人等）における総合的な対策の強化。マイナンバー制度の導入により、地方公共団体を含めた対策の充実。
■インターネットに接続するIoT（Internet of Things）の安全な利用。
■サイバー攻撃により企業の事業活動への支障や、情報漏洩による信用の毀損等のリスクへの対応。
■サイバー空間における国際的に自由な情報の流通の確保。

3. 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。

4. 産業界の取組み

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の開発や製品の提供。サイバーセキュリティ保険の提供。