Keidanren
Policy & Action

サイバーセキュリティ対策の強化に向けた提言（概要）

2015年2月17日
一般社団法人 日本経済団体連合会

世界中でサイバー攻撃による被害が深刻化、わが国では対策を強化。国民生活や経済活動に支障が生じるおそれがある重要インフラ等のサイバーセキュリティ対策の強化に向けて提言。

1. 国内外の情勢

(1)国際情勢
2012年にイギリスのロンドンオリンピック、昨年末に米国でサイバー攻撃が発生。
(2)国内情勢
サイバー攻撃の件数は増加傾向。サイバーセキュリティ基本法の成立やサイバーセキュリティ戦略本部の設置。2020年の東京オリンピック・パラリンピックにおける対策が急務。

2. サイバー攻撃の脅威

情報通信、金融、鉄道、電力、ガスなどが停止すれば、国家の機能維持が困難。
(1)サイバー攻撃の特徴　攻撃者の特定が困難。攻撃者が常に優位な立場。
(2)サイバー攻撃への対処　全ての攻撃を防ぐことは困難で、被害の極小化が重要。
(3)攻撃対象の拡大　情報システムに加え制御システム、スマートフォンなども攻撃対象。

3. 重要インフラ等に対するサイバーセキュリティ対策

政府は重要インフラ等をサイバー攻撃から守ることを明確にし、抑止力を向上させる必要。
(1)具体的施策
①情報共有の強化
サイバー攻撃に関する多数の会議体の情報共有体制の強化。
被害、対応、予防等に関する官民の具体的な情報共有方法の検討。
②演習の実施等
大規模なサイバー攻撃に対する判断基準や指針の整備、官民合同の訓練・演習の実施。
③技術開発とシステム運用
事前探知と攻撃の無効化、探知と追跡、情報共有などの技術開発。第5期科学技術基本計画への盛り込み。優れた防御システムの継続的運用と能力向上。
④人材育成の強化
トップ人材やホワイトハッカーなどの育成、産学官連携によるセキュリティ人材の質と量の充足。
⑤国際連携の推進
海外との情報共有。攻撃者を追跡、特定し、対処する国際的な仕組みの検討。国際会議の開催。
⑥重要インフラ分野の見直し
現在の13分野の見直し。スマートシティやITSなど新たなネットワーク系サービスの追加の検討。
⑦インターネットの安全性の向上
インターネットの利用者の知見の向上。
(2)政府の体制整備
内閣官房に情報集約機能を一元化。サイバーセキュリティ戦略本部のリーダーシップの発揮。

4. 産業界の取組み

産業界は、サイバーセキュリティを経営上の重要課題として、経営層の意識改革、組織改革や人材育成、業種間の情報交流や意見交換を促進。大学・大学院のセキュリティ講座を企業が支援。こうした取組みにより国家のサイバーセキュリティが向上。