

サイバーセキュリティ戦略で示された課題

- 情報セキュリティに係るリスクの深刻化に対応するためには、
- 人材の量的不足の解消に向け 積極的な取組が必要であるとともに、教育だけでは得られない突出した能力を有する人材の確保も大きな課題。
 - そのためには、社会全体で育成し活用するための仕組みが必要。

人材の量的・質的不足

情報セキュリティ従事者 約26.5万人

うち質的不足 約16万人

さらに量的不足 約8万人

⇒これら人材の雇用の受け皿も不可欠

取組の方針

我が国の情報セキュリティの水準を高めるため、人材の「需要」と「供給」の好循環を形成する。

【需要】経営層の意識改革

○組織の経営層

- ・経営層の意識改革を促し、情報セキュリティを経営戦略として認識させるための取組を推進。
- ・製品・サービス調達における情報セキュリティの要件化等を通じ、投資意欲を喚起して、人材の需要を創出。

○実務者層のリーダー層

- ・経営戦略の視点から情報セキュリティの課題や方向性を考え、経営層と実務者層の橋渡しができる能力を育成。

【供給】人材の「量的拡大」と「質的向上」

- IT技術者等に、情報セキュリティを必須能力として位置付け、訓練・演習教材等の作成や能力評価基準・資格のあり方の検討を進める。
- 高度な専門性及び突出した能力を有する人材の発掘・育成を推進するとともに、実社会での活躍を促進。
- グローバル水準の人材の育成に向け、国際的な体験や情報共有を通じて人材が研鑽を積む環境を構築。
- 政府機関は自ら率先して、情報セキュリティ上のリスクに対応できる職員の採用・育成や研修・訓練等を強化。
- 教育機関(初等中等教育機関含む)の実践的なIT教育を充実させるとともに、情報セキュリティに関する教員養成を推進。