産業サイバーセキュリティセンター

～サイバーセキュリティ対策の中核機関を設立～

近年、インフラに物理的ダメージを与えるサイバー攻撃のリスクが増大。
テロリストや他国家によるサイバー攻撃は、大規模停電のように生命・財産を脅かす。

事例1 電力網へのサイバー攻撃
（ウクライナ、2015年）

マルウェアの感染により、電力網が遠隔制御。
数万世帯で３～６時間にわたる大停電が発生。

事例2 製鉄所の溶鉱炉損傷
（ドイツ、2014年）

何者かが製鉄所の制御システムに侵入し、
不正操作をしたため、生産設備が損傷。

事例3 原発の制御システム停止
（アメリカ、2003年）

発電所の制御システムがウィルスに感染。
制御システムが約5時間にわたって停止。

国家として、我が国経済・社会を支える重要インフラや産業基盤における
サイバー攻撃に対する防護力の強化が必須です。

2017年4月 産業サイバーセキュリティセンターをIPAに開設

模擬プラントを用いた演習や、攻撃防御の実践経験、最新のサイバー攻撃情報の調査・分析等を通じて、重要インフラ・産業基盤のサイバーセキュリティ対策の根幹を担う人材・技術・ノウハウを生み出していく。最新の技術・ノウハウを学び、他業界のセキュリティ責任者や専門家、海外との人脈を形成した人材が、自社のシステムのリスクを認識しつつ、必要な対策を判断し、自社の総合的なセキュリティ戦略を立案。

人材育成事業のポイント

- 多様な攻撃パターンへの対応訓練
- 海外の大学や機関との交流による知見蓄積
- 演習を自ら企画し、実践
- 最新の攻撃情報を調査し、対策を立案

人材・技術・ノウハウを結集し、重要インフラ・産業基盤の
サイバーセキュリティの抜本的強化へ

IPA 独立行政法人 情報処理推進機構
Information-technology Promotion Agency, Japan