平成28年11月10日　長崎新聞　ふるさと総合面掲載

県立大・連続セミナー　2

情報セキュリティマネジメント

情報システム学部
情報セキュリティ学科教授
小松　文子

計画的な点検が必要

情報をさまざまな脅威から守るには、技術対策とともに、組織の対策である情報セキュリティーマネジメントが重要です。これは脅威が企業・組織の持続性にいかに影響するかを分析・評価し、対応を検討するリスク管理の一環です。

情報セキュリティー対策は、組織を横断して周知し実施する必要があるため、組織トップの関与が不可欠です。まず、組織全体に適用される原則を文書化し、これを基に具体的な規定や指針・運用規則を作成します。次に、企業・組織に影響を与える脅威や事象を特定。情報システムの脆弱性や起こりやすさ、原因などを分析し、幾つかのリスクのレベルを決めます。

さらに法制度、業界慣習などを考慮して、具体的な影響やリスクを受容できるかなどを評価。最終的にはリスクの重大性や対策の実現性も合わせてリスクへの対応を決めます。対応には「リスク回避」「リスクの最適化」「リスクの移転」「リスク保有」があります。リスク保有は、情報に基づく意思決定によって決めるもので、想定外であってはなりません。

最後に対策を実行しますが、技術の進歩で新たな脅威が出現するので計画的な点検が必要です。2年前に教育関連企業から大規模情報が流出した事件では、組織内のシステムエンジニア（ＳＥ）がデータベースの個人情報をスマートフォンにダウンロード。企業は対応策を実施していましたが、スマホに導入された新技術に対応できず情報が抜き取られていました。

事故発生時の体制整備も大切です。近年多くの組織が「ＣＳＩＲＴ」というチームをつくっています。リスク発生を前提に、被害の広がりを防ぎ再発防止を図るものです。

（随時掲載します）