セッション5

実事例から学ぶ
～CSIRT構築の悩みどころと構築後の成長の測り方～

経営として何を守るのか

ニュートン・コンサルティング
CISO／プリンシパルコンサルタント
内海 良 氏

あるセキュリティーベンダーのリポートによると、企業の約4割はサイバー攻撃を受けている。そして検知に1日遅れると保障費用なども含めて約4割コストが上昇するとある。つまり初動がポイントだ。こうした状況に対し、いち早く動くのがCSIRTであり、実際に効果を上げている企業も多い。

サイバーセキュリティーの強化は法令で定められ、ガイドラインが示されるなど強化の方向にある。日本企業でも海外のフレームワークに対応し強化する事例もある。

これまではどのように情報を守るかがポイントだった。近年、大規模なセキュリティーインシデントが頻発し、企業ブランドをどのように守るかという視点が重要になった。

CSIRTをどのように構成するかという点で、我々は既存のセキュリティーの仕組みを生かすよう訴えている。

CSIRTは「つくる」ではなく「定義する」に近い。経営理念や方針を踏まえ「何を守るのか」を明確にし、短期集中型の構築を提案している。トップインタビューや当事者を対象にしたワークショップなどを開催し、効率的に合意形成を図る。

CSIRTは設置して終わりではない。対応能力を可視化する演習を実施し、ブレない指標を用いて評価と改善を行う。合意に基づくロードマップに沿って対応力を成長させることも重要だ。