「技術情報等の流出防止に向けた官民戦略会議」行動宣言ポイント

平成27年1月28日

背景

- 企業独自の製造ノウハウ等（営業秘密）は競争力の源泉。
- その重要性は増大※する一方で、窃取され、価値を喪失する懸念が深刻化（内外での流出事例の増加、手口の高度化）。

※注 特許要件を満たす発明であっても、あえて特許権ではなく、営業秘密として秘匿化を選択する割合が増加（経産省調査では、3割の企業がここ5年～10年の間に増加と回答）。

営業秘密侵害を断固として許さない社会を創出

1．企業情報の防御（予防策の徹底）

- 我が国企業でも技術の秘匿化、情報の電子化、外国人従業員の増加を含む雇用環境の変化が進む中で、必要な対策を講じる必要。
  （参考）米国では、特定国からのサイバー攻撃、従業員への働きかけ等によって、IT、化学、自動車など民生分野の最先端技術が盗取される事例が増加。
- 予防策の実施に当たっては、経営層自身のリーダーシップの下、事業、総務、法務、人事、情報セキュリティ、知財等の各部門にわたる全社的な対策が不可欠。情報セキュリティ対策の強化やスキルのある従業員を能力主義・成果主義に基づき適正に評価する人事制度の構築も重要。

＜政府・各団体の取組の宣言＞
- ○各種団体による啓発活動の加速
- ○営業秘密管理指針の全部改訂、営業秘密保護マニュアルの策定
- ○営業秘密に関する相談窓口の設置
- ○中小企業等に対する普及・啓発
- ○サイバー攻撃の手口情報の共有の促進

2．情報漏えいへの断固とした対処

- 「有事」には被害の拡散防止等の応急処置を迅速に実施するとともに、「一罰百戒」の観点から行為者に対する厳正な措置が必要（民事、刑事）
  （情報漏えいの100%防止は不可能。適切な対応を行った上での情報漏えいを恥じる必要はない）
- 政府は、抑止力向上のための制度整備、被害企業への相談対応、捜査力の充実強化を実施

＜政府・各団体の取組の宣言＞
- ○抑止力向上のための制度整備
- ○営業秘密に関する相談窓口の設置（再掲）
- ○深刻なサイバー攻撃被害への復旧支援の促進

3．継続的な官民連携により攻撃手法の高度化への対応

- サイバー攻撃など情報通信技術の高度化に応じて、手口も高度化・複雑化
  →「営業秘密官民フォーラム」で最新の手口や被害実態について情報交換を実施

＜政府・各団体の取組の宣言＞
- ○実務者による官民での緊密な情報交換の実施
- ○政府による情報収集・提供
- ○各団体の取組の推進