２０１５年1月２８日
日本機械工業連合会

技術流出防止政策に関する提言

提言１　総合相談窓口機関等の早期設置と効果的な運用の確保

工業所有権・研修館（ＩＮＰＩＴ）における営業秘密管理、知財戦略に関する相談窓口の設置及び官民連携による取組み強化のための「営業秘密官民フォーラム」の設置が検討されているが、いずれも営業秘密侵害行為に対する対抗力を強化する上で有意義な対策であり、その効果的な運用を期待するなかで、次の諸点に留意を求めたい。

（１）検討されている工業所有権情報・研修館（ＩＮＰＩＴ）における営業秘密・知財戦略相談窓口（営業秘密１１０番）と同じく検討されている「営業秘密官民フォーラム」の両者間での連携及び情報の共有が十分確保されるように対応いただきたい。
また、中小企業のみならず、大企業を含めて関係省庁を横断した円滑なワンストップ相談機能がこの両者の連携のなかで図られるよう、配意願いたい。

（２）「営業秘密官民フォーラム」にあっては、こうした場を通じて官民のより一層包括的な連携とともに関係省庁間の連携とコミュニケーションの深化が期待されるところであり、そのためにも関係する省庁の参画が部分的なものとなることのないよう、構成メンバーの適性を期待する。

（３）日本機械工業連合会（以下「日機連」という）では、2年間に亘る会員間の意見交換や米国での調査等をもとに、近く「機械工業等における技術流出防止のためにガイド」を公表し、シンポジウムの開催等を通じて防止策の普及に努める予定であるが、官民連携フォーラム等を通じてより広くこうした情報が共有されるとともに、政府において予定している「営業秘密保護マニュアル」の策定にも参考となることを期待したい。

（４）米国や韓国の取組みを引き続きフォローするなかで、窓口機関等の組織体制のあり方については今後の運用状況を踏まえつつ、より一層の実効性の確保に向けて不断の見直しが行われることを期待する。

＜参考＞

米国には、特許商標庁、国土安全保障省の入国・税関における捜査担当部署、警察等の主要連邦政府機関に加えて、周辺国のカナダやメキシコ、さらにはインターポール、ユーロポール等の海外の警察とも連携して知的財産侵害に対して包括的に対応する「National Intellectual Property Rights Coordination Center (National IPR Center)（国立知的財産コーディネーション・センター（略称：国立知財センター）[1)]」があり、企業等の提供した情報に基づいて、米国連邦捜査局（FBI）他の警察組織が自律的に捜査を行い、技術流出や模倣品の国内流入を未然に阻止している。

韓国でも、特許庁と特許情報院により設立された「営業秘密保護センター」があり、公正取引委員会、中小企業庁、警察等と連携し、営業秘密原本証明サービスをはじめとした営業秘密の保護に関するワンストップサービスを提供して、営業秘密の保護と管理活動を全般的に支援している。我が国では、模倣品に対しては、「政府模倣品・海賊版対策総合窓口」があり、経済産業省、財務省 税関、総務省、警察等が連携しているが、技術流出に対しても、企業等からの相談にワンストップで対応する窓口組織の整備と関係省庁間のより一層の連携が強く期待される。

提言２　営業秘密侵害行為への法的責任追及のための法制の強化

営業秘密侵害行為が適切かつ迅速に処罰され、結果として侵害行為の発生そのものを抑制する抑止効果を持つような、法制面での充実を図るべく、営業秘密侵害罪の非親告罪化、未遂行為の処罰、国外犯の処罰範囲の拡大、罰則の厳罰化、民事における立証負担の軽減、水際措置の導入等の早期実現を求める。また、司法のルール・メーカーとしての実効性のある適切な判断に資するべく、より一層適切なガイドラインとなるよう「営業秘密管理指針」が早期に改定されることを歓迎する。

＜参考＞

諸外国の例で見ると、例えば韓国では、営業秘密侵害は、非親告罪であるため、警察の捜査が先行し、立件に至る例は相当数にのぼっている。米国においても同様である。他方、我が国では親告罪の制度のもとで、最近で見ても営業秘密侵害で起訴に至った例は数件を数えるのみとなっている。情報漏洩件数自体は相当数にのぼると推定されるなかで、このような状況は「伝家の宝刀は抜かれない」という加害者側への安心のメッセージともなり、抑止力を減退させている。

「知的財産計画２０１４」にも記載されているとおり、我が国における技術流出の実態と課題に照らし、実効的な抑止力を持つ刑事規定の整備、実効的な救済（損害賠償・差止）を実現できる民事規定の整備を実現すべく、上述のとおりの具体的な法制の整備が今通常国会での法案審議を通じて実現することが強く期待される。

提言３　製造業における生産技術等のパラダイムシフトへの対応

ドイツにおける「ＩＮＤＵＳＴＲＩＥ４．０」や米国における「ＩＮＤＵＳＴＲＩＡＬ　ＩＮＴＥＲＮＥＴ」に見られる生産技術等のパラダイムシフトの動きは、技術流出防止のあり方に対しても今後大きな与件の変化として影を投げかけるものである。これまでいわば「自動化の孤島」であった工場や通信機器以外の製品が通信を介在して外の世界と繋がり、インテグレート化するなかで、生産現場の技術データや顧客の活動にかかるデータがビッグデータとしてサイバーセキュリティ上のリスクに晒されることとなる。技術流出防止政策の今後一層重要になる課題として官民双方での対応策の検討が求められる。

＜参考＞

「インダストリー４．０」（第４次産業革命）の旗印のもとで検討が進められている取組みは、工場内外のネットワーク化や３Ｄデジタル化の推進、スマートファクトリーの実現等をめざしているが、そのための８つの優先課題分野として、ネットワーク化等の標準化などとともに、「ネットワーク上のセキュリティ」が取り上げられている。「つながる工場」のメリットをデメリットにさせない工夫が求められている。

こうした課題に取組む上で、機械のハード技術に関する知見とＩＣＴに関す

る知見の双方が関係者に求められるが、例えば情報処理技術者試験の応募者数の勤務先業種別のデータについて、情報セキュリティやネットワーク科目でみると、ソフトウェア業及び情報処理・提供サービス業では毎回 1 万人を超える応募者があるのに対して、製造業全体で千人を満たないといった 10 対 1 以上のアンバランスがあり、ネットワークや情報セキュリティの知見をもつ人材の偏在が気になるところである。諸外国と比べて極端にアウトソーシングの体制になっているのではないか、そうしたなかで今後のものづくりにおけるサイバーセキュリティの問題にどう対処するのかが課題となる。