諸外国並みの技術安全保障体制の構築を

～技術保護とサイバーセキュリティが急務～

2018 年 10 月 10 日

技術安全保障研究会

技術安全保障研究会

座長	玉井克哉	東京大学教授・信州大学教授
委員	荒井寿光	知財評論家（元通商産業審議官）
	國分俊史	多摩大学大学院教授　ルール形成戦略研究所所長
	坂本吉弘	安全保障貿易情報センター理事長（元通商産業審議官）
	長瀬正人	株式会社グローバルインサイト 代表取締役社長（元三菱商事（株)）
	西　正典	元防衛事務次官
	西山淳一	未来工学研究所　研究参与（元三菱重工（株)）
	頓宮裕貴	サイバーセキュリティ有識者（元（独）情報処理推進機構理事)
	森口泰孝	JAEA シニアアドバイザー（元文部科学事務次官）
	渡辺秀明	SBI ホールディングス株式会社顧問(元防衛装備庁長官)
幹事役	利光　尚	安全保障貿易情報センター　参与（元三菱商事（株)）

事務局長

國分俊史	多摩大学大学院教授　ルール形成戦略研究所所長

背景

我が国は、戦後、技術立国を目指し、優れた技術を研究開発し、それにより国を豊かにすべく、官民共に知恵を絞ってきた。ところが、バブル崩壊後は、徐々に日本の技術力が衰え、２１世紀に入ってからは、テレビ、パソコン、携帯電話、更に半導体までも、台湾、韓国、中国に追いつかれ、事業規模の大幅な縮小・撤退に直面している。その背景には、我が国が技術者と技術の流出に関してあまりにも無頓着であり、制度的にも無防備であったことが指摘されている。

これまで、我が国は主に特許によって研究開発成果を保護することとしてきたが、特許制度においては技術の内容は公開される。国家的見地からそれを避ける必要のある対象について、各国には非公開特許制度があるが、日本では、未だ整備されていない。

今日、先端技術の多くは、デュアルユース技術として安全保障技術と一体化している。好むと好まざるとに関わらず、この傾向は今後も強まり、各国による技術情報保護の対象となる。特に米国は、安全保障にかかわる先端技術の無秩序な国外流出を防止するため、対外投資等の制限を含む対策を講じてきている。とりわけ、研究実施者のセキュリティ・クリアランス（秘密取扱者適格性）に関しては、民間企業同士の研究協力であっても技術情報保護の措置を執るよう要求を強めており、個人単位のセキュリティ・クリアランス制度を整備しなければ、今後、日米間の産業協力に支障が生じることが想定される。

また今日では、すべての情報、データ等はデジタル化され、サイバー攻撃の対象となる。我が国におけるサイバーセキュリティについて、米国の識者から、日本は無防備すぎるとの指摘がある。その代表的な例として、サイバーインテリジェンス（サイバー空間で行われる諜報活動）が挙げられる。諸外国では各種のサイバー情報を収集し、自国への攻撃を未然に防止しているが、日本ではこのような制度が確立していないため、各種の対策を講じることが形式的には違法行為となってしまう。また、サイバー攻撃防御の演習も実際のインターネット環境を利用して行うことが禁じられているなど、制約が多い。

我が国においては、サイバー攻撃を受け、データが流出したことが明瞭な案件であっても「実質的被害は確認されなかった」といった趣旨の発表がなされることが多い。このように国内で被害を小さく見せようとし、結果的にサイバー攻撃に対する認識が低いことを露呈している。

我が国のサイバー防衛の司令塔は内閣官房の内閣サイバーセキュリティセンターであり、インシデント（コンピュータやネットワークのセキュリティを脅かす事象）発生時も各省庁と連携を取りながら我が国全体のサイバー防衛態勢を万全なものとすることとして推進しているが、国民への理解を含めさらに強化すべき時期に来ている。

なお、この分野における日本の体制は、米欧などの先進国のみならず、中国、ロシア、韓国、北朝鮮を始め多くの国に比べて遅れているのが、残念ながら現実である。このため表題を「先進国並み」ではなく「諸外国並みの技術安全保障体制の構築を」とした。

このような事態を憂い、我々は以下のような提言をまとめた。

提言のねらい

１　工業化時代からデジタル時代に移行しつつある現在、IT 技術をはじめとする国の技術力が、産業の国際競争力のみならず、一国の安全保障に直結している。技術保護政策も二つの保護法益を一体として目指すべきである（技術安全保障）。

２　技術力が産業競争力と安全保障を不可分一体として支えるとの観点から、国の政策立案や法執行についても、一体としての取り組みを強化すべきである。

３　既に同様の観点から重要技術の流出防止について包括的な法制度を整備している欧米各国や韓国との制度間競争に生き残り、安全保障に関する各国の信頼を得るためには、我が国も、技術保護の保護水準の同等化を目指す必要がある。

１０の提言

「国」「企業」「個人」における多角的なセキュリティ・レベルの向上

１．国のサイバーセキュリティ機能の抜本的充実

・日本に対する無秩序なサイバー攻撃を減らすためサイバー攻撃コストを増大させるアトリビューション（サイバー攻撃の実行者の特定）を同盟国と連携して実施する体制を整備する。

・日本に対するサイバー攻撃は、今そこにある危機であり、それへの的確な対応は自衛隊の任務でもあることを明確にする。従って、諸外国と同様に日本への攻撃の予知等のためにもサイバーインテリジェンスを実施できるようにすると共に、自衛隊が行う演習についても実際のインターネット環境を利用した演習環境を実現すべきでる。
・自衛隊のサイバー防衛隊が、自衛隊自身のサイバー防衛だけでなく、日本全体のサイバー防衛をできるように抜本的な体制整備を図る。

２．企業レベルのサイバーセキュリティ・レベルの向上
・自衛隊と民間の間の技術移転を促進し、産学官が共同歩調を取ってサイバー空間における国家安全保障を推進する体制を構築する。
・特に重要インフラ（電力、通信、ガス、水道、交通など）へのサイバー攻撃は国家の安全を脅かすため、自衛隊のサイバー部隊は重要インフラに対してもサイバーインテリジェンスを駆使し、民間企業および他の政府機関と連携して被害の発生を未然に防ぐ、または被害を最小化する防衛範囲の拡大を行う。

３．セキュリティ・クリアランス制度の導入
・米国に倣った個人レベルのクリアランス制度を導入し、安全保障上機微に触れる技術の製品の開発にあたっては政府として技術者の適格性保証を行う。特に、非公開特許（後述）に指定された技術情報を活用して製品化や研究開発に従事する個人及び組織に対し、セキュリティ・クリアランスの取得を義務付けると共に、防衛省等各府省が実施している現行の秘密取扱者適格性確認制度に組み入れることを検討する。

技術流出防止体制の整備

４．防諜活動を強化するため、国に専門の情報機関を設置し、「脅威インテリジェンス機能」を持たせる。特に防衛省・自衛隊に関しては、米国 DTSA（国防技術保全局）や DSS（国防保全局）に倣った機関を設置する。

５．技術窃取に関する警察機能を抜本的に強化し、従前の都道府県警の枠組みを超えて、国レベルで法執行を行う体制を整える。また、特許取得段階で強いられる技術情報の公開時に他国に技術情報が流出のリスクを回避する制度（非公開特許制度）を創設することとする。

６．サイバーセキュリティ人材の発掘と育成については、産学官が一体となって

抜本的に強化する。また、サイバーセキュリティのために不可欠な技術については、従前の通念にとらわれず、安全保障の見地からの研究開発に大学を含む公的研究機関が自衛隊と連携して積極的に取り組むこととする。

技術保護を実現する体系的な法整備

７.安全保障及び産業の競争力の確保を同時に目的とした「重要技術流出防止法」（仮称）を制定し、技術分野ごとに特許等の知財及び技術論文等の公開又は非公開の取り扱いを整理し、国家としての技術管理を徹底するとともに、諸外国等への技術流出を防止する。その際、非公開となった特許等知財の発案者及び論文の著者の権利を保障し、金銭的な補償と学術的価値の認定を行うこととする。

８．安全保障の見地から国が重要と認める核心的技術については、外部からの不審な接近があった場合などの国への報告義務を導入するほか、流出防止のための特別な措置を個別に執りうることとする。

９.「重要技術」の指定のほか、中長期的な産業安全保障計画の策定を含む政策の立案、その前提となる内外の情報収集の把握、分析、対策立案等を行うため、「国家技術安全保障会議」を内閣に設置する。

１０．営業秘密の窃取防止法制は不正競争防止法から抜き出して「営業秘密保護法」として一括する。特に重要技術の外国への流出に関しては、前記５．の国家レベルの警察組織が担当するものとする。対外的に秘匿すべきその種の対象につき、特許権設定登録に代えて保護するための制度を導入する。