移転が見込まれる技術に対する流出防止に必要となるリバース・エンジニアリング対策事業について

経済産業省　貿易経済協力局　貿易管理部　安全保障貿易管理政策課　吉野　寛史

1　はじめに

防衛技術と民生技術が相互連関（スピンオフ・スピンオン）する中、安全保障上、管理すべき技術は多様化しています。また、そのような技術の保有主体もスタートアップから大学等まで裾野が拡大している状況です。とりわけ、エマージングテクノロジー（例 .AI、サイバー等）については、そのコアとなる要素技術の特定は容易ではありません。

技術をめぐる国際状況も変化しています。欧米各国だけでなく新興国は、開発・製造工程の国産化、ゲームチェンジャーとなり得る先端技術分野（IoT、ビッグデータ解析、AI 等）の重点的開発を推進するとともに、国内技術開発の推進に留まらず、既存の輸入・技術移転に加え、買収や学術交流（留学生等）、ヘッドハンティング、サイバー攻撃等、技術獲得手法も多様化しています。

また、平成 30 年 6 月 15 日閣議決定された「統合イノベーション戦略 2018」においては、安全保障の観点から、伸ばすべき / 適切に管理すべき技術分野の明確化（＜知る＞）、当該分野の強力な育成（＜育てる＞）、技術情報流出への対応（＜守る＞）をパッケージとして打ち出しています。

このような政府の方針を受け、経済産業省では政策課題として、以下の対応を検討しています。

(1)「知る」：技術動向の把握

効果的・効率的な技術管理を実現するため、国際動向（経済、外交、軍事等）、懸念主体の動向（懸念主体特定、技術獲得手法等）、技術動向（安全保障上重要な技術の動向とその軍事転用可能性等）などの必要な情報を一元的に集約・分析し、知見として蓄積する。

(2)「守る」：エンフォースメント強化

上記、技術動向の把握をもとに、管理制度の強化（最新技術動向等に機動的に対処）、メリハリをつけた法執行（重点管理分野へのリソース配分）、科学技術を活用した技術流出対策の促進（リバース・エンジニアリング対策）、企業・大学の管理能力の底上げ（輸出管理・情報保全の両面からアプローチ）、国際連携（アウトリーチ、懸念情報共有、協調行動）の観点から既存の取り組みを合理的に見直し、強化を図る。

本誌では、この「守る」の一環として、平成 30 年度から取り組んでいる「リバース・エンジニアリング対策」について紹介します。

2　リバース・エンジニアリング対策事業の概要

重要技術の適切な海外移転は、国際的な平和と安全の維持へ寄与するとともに、我が国の産業基盤の維持・強化に資するものですが、これらは、安全保障環境や産業基盤に悪影響を与えないように、適切な技術流出防止策を併せて実施していくことが極めて重要です。しかし、これまで各重要技術にどの水準の技術流出防止策が必要なのか等の調査は十分になされておらず、輸出管理を所管する経済産業省として、それについて調査・分析しておくことが必要です。今後、重要技術の輸出が増加する可能性もあることから、早急に取り組む必要があります。

本事業では、ハードウェア、ソフトウェアの両面

に関するリバース・エンジニアリング対策技術に係る調査・試験研究及び評価を実施することにより、迅速、かつ、厳格な管理下における適切な重要技術の移転に寄与するものです。

平成30年度は、①ソフトウェア無線機、②レーダ、③水中航走体、④電磁パルス防護装置、⑤装軌車両用トランスミッションに係るリバース・エンジニアリング対策技術について調査、試験研究及び評価を実施しています。

	①	②	③	④	⑤
軍事転用例					
	軍用無線機	防空レーダ	魚雷探知機	電磁パルス防護	戦車

図1　我が国の移転・市場流通が見込まれる軍事転用可能な先端技術の例

(1) 調　査

○我が国及び諸外国のリバース・エンジニアリングの状況

○リバース・エンジニアリングの脅威

○各調査対象技術の概要

○我が国及び諸外国の調査対象技術の動向（技術レベル、主要メーカー等）

(2) 試験研究

ア　ソフトウェア無線機

○リバース・エンジニアリング対策を施す装置

単一のハードウェアで、マルチバンド（各周波数帯）に対応でき、ソフトウェアの変更で、様々な通信方式に対応できる軍用の無線機。

○リバース・エンジニアリング対策の概要

・暗号鍵、データ消去等により、外部インターフェースからのアクセス対処等。

・基板の加工等により、内部基板への直接アクセス対処等。

・サイドチャネル攻撃等の外部からの間接アクセス対処等。

イ　レーダ

○リバース・エンジニアリング対策を施す装置

高周波アンプに用いられるディスクリート高周波半導体（ＧａＮ）を用いた回路基板。

○リバース・エンジニアリング対策の概要

・基板の中に固い材料と柔らかい粘性のある材料を混ぜ込み、機械研削によるリバース・エンジニアリング対策等。

・回路の中にヒューズ等を埋め込み、指定条件以外の電圧、電流が流れると不可逆的に破壊する電気的なリバース・エンジニアリング対策等。

ウ　水中航走体

○リバース・エンジニアリング対策を施す装置

魚雷に適用可能な水中航走体。

○　リバース・エンジニアリング対策の概要

・起動時、ＲＯＭに書かれたソフトウェアを読み込み後、ＲＯＭ内のデータを消去等。

・ハードウェアに電装品単体の起動を検出する導通モニタ回路等を追加し、電装品単体の起動を検出したときにＲＯＭ内のデータを消去等。

・計測機器による観察防止及び基板からチップをはずせないよう硬化樹脂等のコーティング材で覆い、コーティング剤をはがした場合、基板パターンやチップを破壊する仕組み等。

・ソフトウェアについて本来の性能を保持したままの難読化・暗号化等。

・起動中のＣＰＵへのログインに失敗した場合、不正アクセスを検出して秘匿性のないダミーソフトウェアの書き換え等。

エ　電磁パルス防護装置

○リバース・エンジニアリング対策を施す装置

ノイズ対策のための堅牢で高価な保護装置

に頼らず、発生した誤動作から迅速に復帰して、正常な動作を継続するためのマイコンに使用可能なソフトウェア。

○リバース・エンジニアリング対策の概要

ソフトウェアについて本来の性能を保持したままの難読化・暗号化等。また、難読化・暗号化されたソフトウェアについては、ＵＳＢメモリ等の２次配布が可能な媒体に格納等。

オ　装軌車両用トランスミッション

○リバース・エンジニアリング対策を施す装置

装軌車両（戦車）用のトランスミッションの構成品である油圧ポンプモータ。

○リバース・エンジニアリング対策の概要

特性、形状、機能等の面から第三者による解体・分解を困難にする対策等。

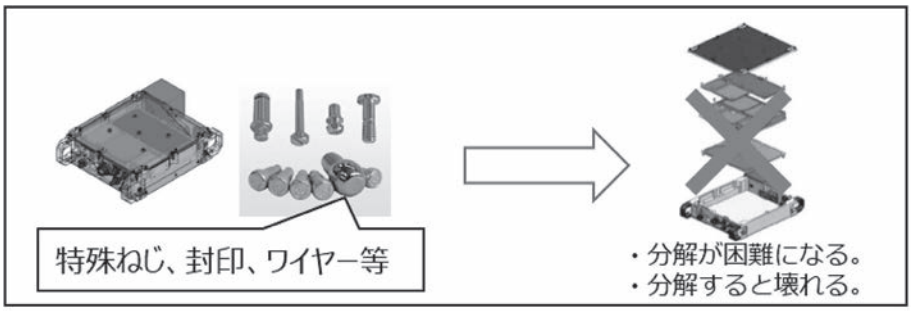

図2　対策技術例（ハードウェア）

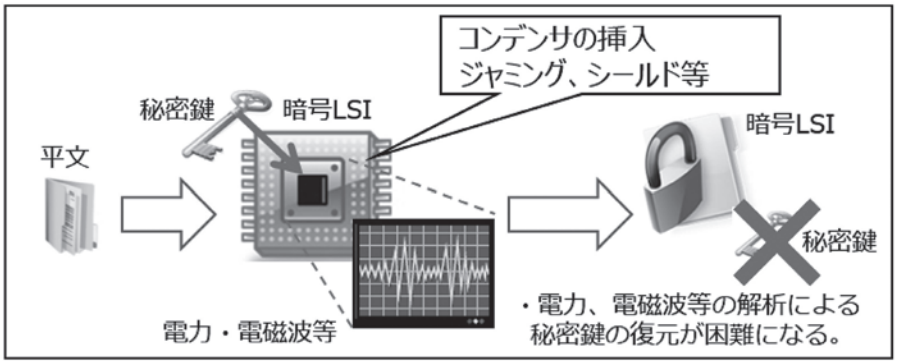

図3　対策技術例（ソフトウェア）

(3) 評　価

各試験研究対象技術について、検証を行うために試作した機器のリバース・エンジニアリング対策について、その性能を以下の通り評価します。

○各リバース・エンジニアリング対策について、その効果を無効とするような解体・分解等の手法を考察し、対策の特性及び問題点を発見するとともに、それぞれの実行の可能度及び処置すべき事項を明確化。

○分析の結果明らかになった比較のための重要な要因を挙げ、これらの軽重を評価・判定し、各要因の対策の優劣を比較。さらに比重の大きい要因を重視して総合的に判断し、有効性を検証するに値する２つ以上の対策を選定。

○選定された対策の有効性の評価を行うための評価項目、評価基準等を作成。

○完成品若しくは模擬部材（完全な構成部品ではないが検証に必要な材質、形状及び構造を模擬した部材）により、リバース・エンジニアリング対策の効果を検証。

○上記により、リバース・エンジニア対策の有効性を明確化。また、必要に応じ特有の課題の抽出及び解決方法等を検討。