ハードウェア・サプライチェーンにおける米国の法政策・標準の動向

―セキュリティと知的財産の観点から―

○氏名　橘　雄介（Yusuke TACHIBANA）

Keywords：ハードウェアセキュリティ、サイバー・サプライチェーン・リスク管理（SCRM）、知的財産、半導体集積回路、米国

１　目的

近時、ハードウェアのサプライチェーンについてセキュリティ上の懸念が強まっている。背後には、サプライチェーンが世界的なものになってきたという事情があり、たとえば、米国では、中国からのものと思われる Cisco ルーターの模造品が米国の政府機関に納品され、異常な電力供給のために火災が生じた。こういった事件を契機に、米国では情報システム及びそのコンポーネントのセキュリティ管理策に加え（NIST・FIPS 200 や SP 800-53）、サイバー・サプライチェーン・リスク管理（SCRM）の管理策も発展してきている（NIST IR 7622 及び SP 800-161）。

また、知的財産及び模造品対策の観点から、サプライチェーンの管理策が設定されることもある。たとえば、米国上院委員会は、模造品と疑われる電子部品が国防総省の機関に納入されている事例があり、部品の総数は 100 万点を超えると報告している。こういった事情を背景に、国防総省の調達基準（DFARS）や民間のガイダンス（たとえば、SAE の定める AS6171A）が策定されている。

このようにハードウェアに関するサプライチェーンの保護策はセキュリティの確保と知的財産の保護という 2 つの目的を持っている。本報告では、この 2 つの目的から米国のサプライチェーン・セキュリティ管理策を分析し、その目的の達成度と欠点を明確にし、今後の標準の在り方を模索する。

２　方法

検討対象分野として、主に知財集約産業である半導体産業を検討する。その上で、まず、米国のハードウェアセキュリティに関する法制度及び主に半導体集積回路に関する知的財産制度を整理し、ハードウェアのサプライチェーン・セキュリティの目的を定める。次に、米国政府のものを中心に、ハードウェアのサプライチェーンの保護策の近時の展開を整理する。最後に、上記目的と保護策を比較し、その達成度と欠点を指摘する。

３　結論

調査の結果、米国では、信頼できる供給者及びオリジナルの製造業者から電子部品を取得するという管理策が強化されている。これはセキュリティ上の効果及び模造品の混入を防ぐ効果がある。また、実際に半導体集積回路について光学的及び電気的に模造品かどうかを検査する標準もある。こういった標準について、知的財産の保護策としての効果は期待できるが、オリジナルの部品などとの比較を要求しており、脆弱性の不存在を証明するものではない。したがって、セキュリティの保護策としては不十分であり、必要な技術開発と改善が望まれる。

【主要参考文献】

Mohammad Tehranipoor & Farinaz Koushanfar, *A survey of hardware trojan taxonomy and detection*, 27.1 IEEE Design Test of Computers 10 (2010)

Ujjwal Guin, Navid Asadizanjani and Mark Tehranipoor, *standards for hardware*, 23-1 GetMobile 5 (2019)