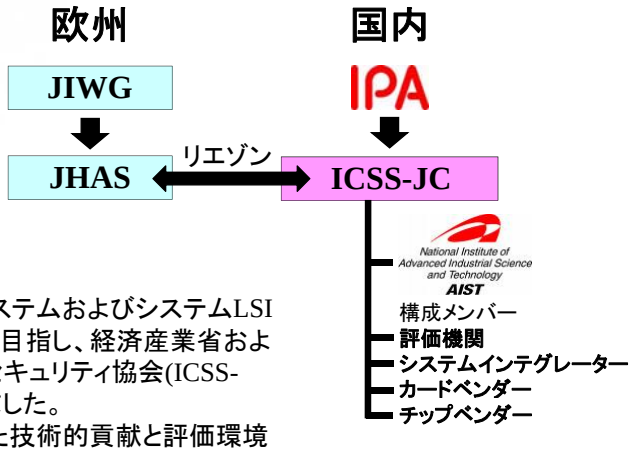
組込システムに対するセキュリティ評価技術の研究開発
－ICシステムセキュリティ協会への貢献－

産業技術総合研究所　情報セキュリティ研究センター

研究の背景と目的

組込システムの心臓部であるシステムLSIチップは日本の大きな産業のひとつです。国際的なシステムLSIチップのセキュリティ評価はISO/IEC 15408 (Common Criteria認証: CC認証)に基づいて行われています。システムLSIや組込システムのセキュリティ評価は、欧州における評価技術開発の長い歴史から、現在欧州の独占状態にあります。また、LSIチップの評価基準は、欧州の評価制度の協議体であるJIWG(European Joint Interpretation Working Group) で決められており、日本企業にとって大きな障壁が発生しています。



そこで、わが国では国際的な競争力を確保するため、国産の組込システムおよびシステムLSIチップについて国際市場で信頼されるセキュリティ評価制度の確立を目指し、経済産業省および独立行政法人情報処理推進機構(IPA)が中心となり、ICシステムセキュリティ協会(ICSS-RT)および、その部会としてCC認証評価部会(ICSS-JC) が組織されました。
本計画において産総研は、セキュリティ評価制度の立ち上げに向けた技術的貢献と評価環境の整備を求められており、システムLSIチップ評価技術の開発を行います。

システムLSIのセキュリティ評価基準

システムLSIのセキュリティ評価基準はJHAS(JIL Hardware Attack Subgroup)によって提案され、JIWGによって承認され、ドキュメントにまとめられています。これは、”Application of Attack Potential to Smartcards”として一般に公開されています。ここで評価対象とされている攻撃としては、「物理攻撃」「摂動攻撃」「サイドチャネル攻撃」等があります。
こうした攻撃に対して、脆弱性の探索および攻撃を実行する観点から、「実行時間」「攻撃者のスキル」「攻撃対象の知識」「攻撃必要サンプル数」「解析ツールの容易性」といった視点で評価が点数にまとめられ、合格可能な点数か否か判断されます。

Joint Interpretation Library:　“Application of Attack Potential to Smartcards”
https://www.bsi.bund.de/cae/servlet/contentblob/478142/publicationFile/30249/JIL-Application-of-Attack-Potential-to-Smartcards_pdf.pdf
等

研究対象としている評価技術

産総研では”Application of Attack Potential to Smartcards”に記載される、
■「物理攻撃」:エッチング、FIB(Focused Ion Beam)加工、プロービング等
■「摂動攻撃」:電源ノイズ注入、レーザーエネルギー注入等による誤動作を利用した、データ解析技術、
■「サイドチャネル攻撃」:LSIからリークする電流、あるいは電磁波等を解析しデータを読み取る技術、
等の攻撃耐性を評価する技術を導入した上、CCの評価基準に影響を及ぼすパラメータである、
・実行時間に着目し、短縮が可能かどうか
・解析ツールに着目し、特殊でない汎用ツールでの実施が可能かどうか
　また、低コスト化が可能かどうか
といったポイントについて研究を行っていきます。
また、これまでに発表されていないような攻撃事例についても研究開発に取り組み、世界に発信して行くと同時に、世界に先駆けてツール化してゆきます。
その一方で、システムLSIを開発するベンダも産総研において研究に参加できる環境を整備し、対策技術の向上を目指す目的の研究も行います。


レーザー装置

お問い合わせ先

(独)産業技術総合研究所 情報セキュリティ研究センター ICSS技術チーム
http://www.rcis.aist.go.jp/index-ja.html