平成18年度事後評価結果（平成18年11月）

［研究開発課題名］　**高度情報セキュリティに向けた真性乱数生成用集積回路の研究開発**
［委 託 機 関 名］　**株式会社 東芝**

項目	評価	総　合　所　見
総合所見	A	（技術関係） ①乱数の質向上：熱雑音（またはショット雑音）から生成された物理乱数のレベルを上回ることを達成。 ②回路の小型化：100ゲート程度で真性乱数を生成するデジタル回路の開発に成功。 ③乱数の統計評価：大量データを評価する方法を確立し、また、サイドチャネル攻撃に対する耐性を評価。 　以上の成果から、量産化と低コスト化を念頭に置いたデバイス製造の基盤技術が確立され、初期の目標は達成されていると判断できる。 　また、研究論文等とともに、国内特許６件、国外特許３件を出願している。特に論文については、３件の受賞があり優れていると評価できる。 　なお、故障時、経年変化による乱数の特性に関する評価とともに、現在マルチバイブレータ型で実現している乱数変換回路の周波数特性の改善などが将来的な課題として残される。 （事業化関係） 　超小型の乱数生成回路を同社の情報セキュリティ機能付きシステムLSIに搭載する事業化計画であり、今後、現行の擬似乱数生成回路よりも本研究開発成果である真性乱数生成回路の方が乱数の質、省回路面積性、低消費電力性で大幅に優れていることから、当該製品の販売以後は擬似乱数生成回路からの置き換えが発生すると考えられる。 　情報セキュリティ機能付きシステムLSIについては、[redacted]、複数の製品への搭載が計画されており、同社の半導体事業の実績も含めて、一定の収益納付が期待される。

（注）総合所見の公表にあたっては、企業秘密等に配慮しています。