暗号アルゴリズム「ＭＡＲＳ」

詳細評価（攻撃評価）レポートサマリー

ＡＥＳ仕様の（改定後の）ＭＡＲＳについては、理論的なものを含め、鍵の全数探索よりも高速であるようないかなる解読法も発見されていない。その意味では、ＭＡＲＳは現時点では十分安全な暗号アルゴリズムといってよい。しかしながら、暗号理論的あるいは実用的な観点から以下の点に注意すべきである。

（１） ＭＡＲＳのＳｂｏｘは設計者の意図した通りには作られていなかったことが最近になって判明している。この事実に関する詳細な検討はまだあまり行われていない。このことがＭＡＲＳの安全性に大きく影響することは現状考えにくいが、注意しておく必要がある。

（２） ＭＡＲＳは３２ビットプロセッサ上のソフトウエアでは優秀な性能を発揮するが、ＩＣカード向けやハードウエア向けには作られていない。ＭＡＲＳを利用する場合にはその利用環境に関する注意が必要である。

（３） ＭＡＲＳのコンポーネントである、乗算とデータ依存回転シフト演算が、タイミング攻撃や差分電流解析に対してどのように作用するか、すなわちこれらの解読法に対する防御実装にどの程度のコストがかかるかは、いまだ研究途上であるが、その情報はＭＡＲＳを特定の環境で利用する上で重要になる可能性がある。