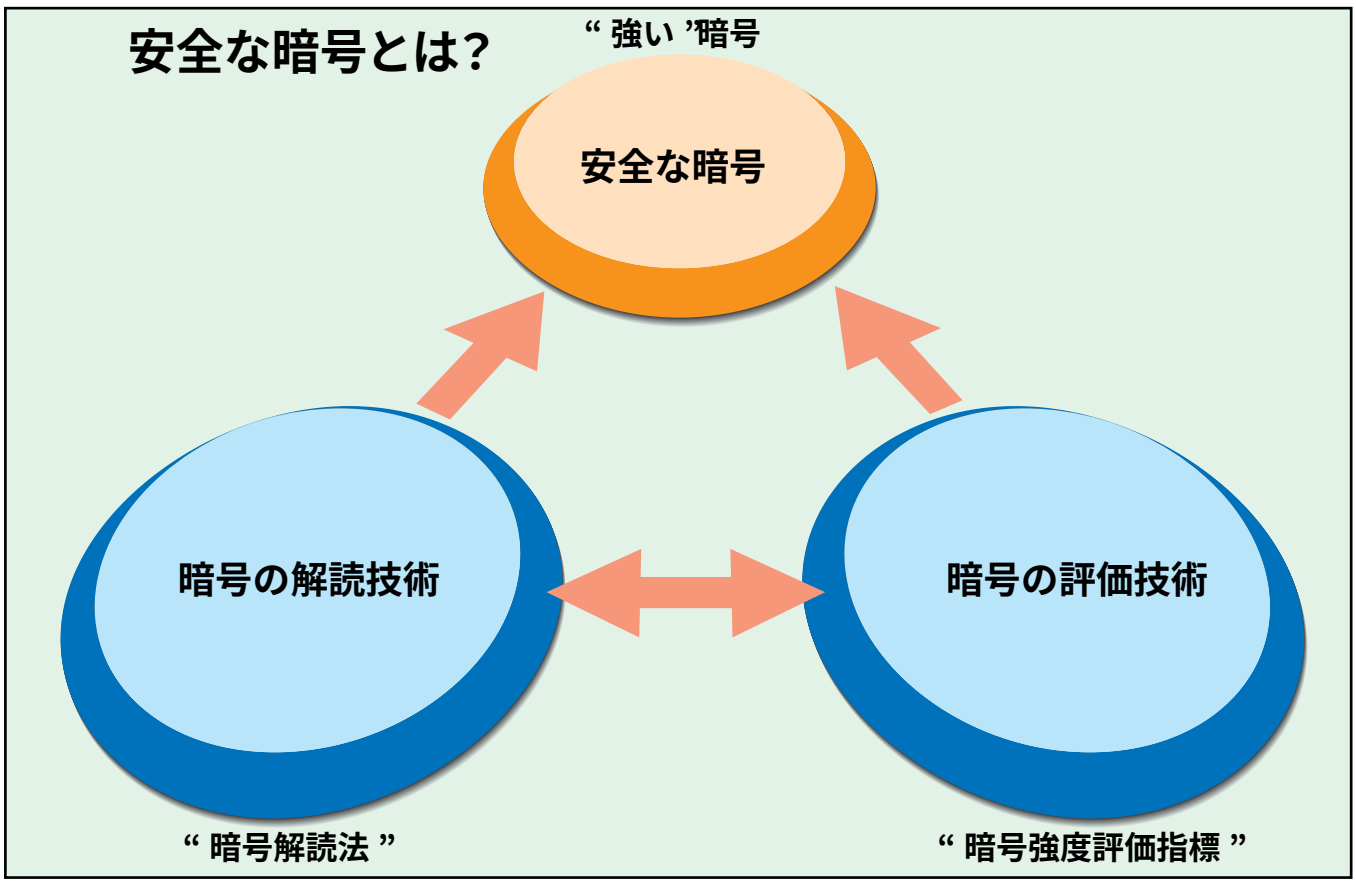
暗号解読・強度評価技術

時田俊雄*
松井　充*
反町　亨*

要　旨

かつて暗号技術が軍事目的を中心として用いられていた時代には，暗号アルゴリズムの詳細は機密であった。しかし，今日のように暗号がオープンネットワークでも利用されるようになると，暗号アルゴリズムは不特定多数の利用者によって共有されることが前提となるため，そのアルゴリズムの詳細は利用者には知られていると考えることが妥当である。このことを暗号強度の立場から見ると，“強い暗号”とは，第三者がそのアルゴリズムの詳細を知っていると仮定しても，暗号化に必要なかぎ(鍵)の情報を推定するのに必要な情報量又は計算量が十分大きいものでなければならない，ということを意味している。この情報量や計算量は実際にその暗号を“解読”すれば明らかとなるが，実際に解読できてしまう暗号は“弱い暗号”であり，私たちが必要とする“強い暗号”は解読できない暗号である。そこで，実際には解読を試みなくても，もし解読を試みるとどれくらいの情報量や計算量が必要となるかを評価できる指標，すなわち強度評価指標を得ることが重要となる。この意味で暗号強度評価技術と暗号解読技術とは表裏をなしていると言える。

また，このような暗号強度評価技術，暗号解読技術があって初めて暗号の性能評価ができるとともに，より強い暗号アルゴリズムの設計が可能となる。今後も暗号研究者にとって暗号解読技術，暗号評価技術の研究は不可欠である。



安全な暗号

安全な暗号とは，様々な暗号解読法に対して強い暗号のことである。したがって，暗号設計者はあらゆる暗号解読技術に精通している必要がある。また，設計した暗号の強度を評価するには，暗号強度評価技術は欠かすことができない。安全な暗号を設計するためには，暗号の解読技術と暗号の評価技術が必要不可欠である。

*情報技術総合研究所