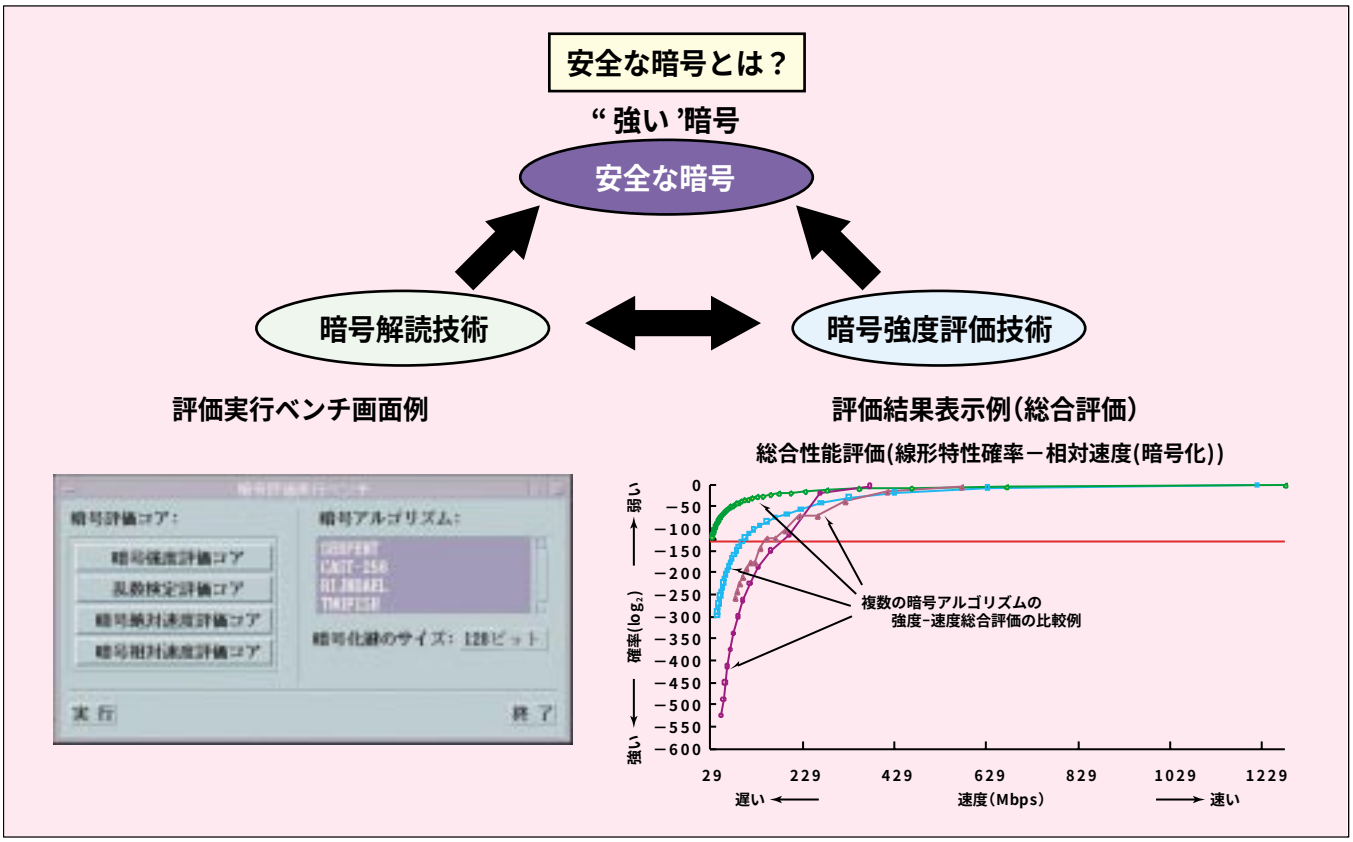
暗号強度評価技術

時田俊雄*
酒井康行*
高島克幸*

要　旨

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状況で‘安全な(＝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，通信路から得られる情報を基に暗号化に必要な情報(＝暗号化鍵。パスワードをイメージすると分かりやすい)を推定(解読)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。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，解読に必要な情報量や計算量を“評価”でき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おり，これらがあって初めて暗号の性能評価が可能となり，より強い暗号の設計が可能となる。

これを実現するために三菱電機が開発したのが本稿で示す“暗号性能評価ソフトウェア”であり，共通鍵ブロック暗号と公開鍵暗号の強度評価を実現する。例えば共通鍵ブロック暗号では，評価者は“評価実行ベンチ”と呼ばれるGUIを通して評価項目(コア)と評価対象暗号を選択し，さらに，必要な各種パラメータを入力／実行することによって様々な強度評価結果を得て，その結果はパソコン上で各種グラフの形で表示される。その特長は，評価者があらかじめ規定されたインタフェースに従って評価項目(コア)及び評価対象暗号を作成／追加することが可能であり，拡張性が高い点が挙げられる。



安全な暗号と暗号性能評価ソフトウェア

安全な暗号を設計するためには暗号解読技術と暗号強度評価技術が必要不可欠である。当社の暗号性能評価ソフトウェアは，共通鍵ブロック暗号と公開鍵暗号に関して，各種暗号解読法に対する強度評価結果を客観的な数値データとして示すことを目標に開発された。特に共通鍵ブロック暗号では，暗号強度とソフトウェア実装上の性能を総合的に評価可能である。

*情報技術総合研究所