

暗号技術について

暗号技術は、必要な人以外には内容がわからないようにしてデータ通信あるいはデータ保存を行う技術です。最近はこの鍵のペアで暗号化・復号化を行う特別な暗号技術を使って電子署名、証明書といったICT（情報通信技術）社会に必要なインフラを実現する公開鍵暗号もあります。

- ・共通鍵暗号：一つの鍵でデータや通信が第三者にわからないように暗号・復号する
- ・公開鍵暗号：公開鍵・秘密鍵のペア（二つ）の異なる鍵を持ち、電子署名等に使用する。

暗号技術に基づいた仕掛けが安全であることは、暗号解読に要する計算時間が膨大であるために、現実のコンピュータでは実質的に解読不能であることを安全性の拠り所としています。しかしながら暗号の研究により、特別な解読方法で現実的な解読時間で解読することが出来ることが発見されて、ある暗号アルゴリズムが安全でなくなることが発生します。

現在のICT社会では、「安全な通信」や「個人や機器の特定」のために暗号技術が用いられており、その安全性を評価する公的機関CRYPTRECがあります。CRYPTRECでは、推奨暗号をとして安全な暗号のリストを公開しています。

無線LANの暗号

無線LANで使用されている暗号として次のものがあります。

- ・WEP：従来使用されてきた暗号。解読手法が発見されて現在は安全ではないとされる
- ・TKIP：WEPを用いて暗号鍵を定期的に変更するが、基本的にWEPと同等
- ・AES：米国および日本の公的機関が現在安全として推奨する暗号

昨今メディアでも報道されているように、WEPは高速な解読手法が発見されて「安全でない」とされています。AESは暗号の安全性評価の公的機関で評価されて推奨されています。

@CELL LANと暗号

@CELL LANでは、PC側にも専用のアダプタを用いて電波飛散を抑えた場合、原理的には暗号の必要はありません。PCに専用のアダプタを用いない場合は暗号化が必要であり、安全なAESの使用を推奨します。

※仕様は予告無く変更されることがあります。

※株式会社セルクロス、CELLCROSS Co., Ltd.、CELLCROSSロゴ、@CELL LAN は株式会社セルクロスの登録商標または商標です。

株式会社セルクロス

連絡先 TEL : 03-5, ' #z%\$#*
FAX : 03-5, ' #z%\$#+
所在地 〒11z##\$% 東京都文京区 (z\$z\$*
SOビル 201
ホームページ <http://www.cellcross.co.jp>