第2章 シーザー暗号/XOR pad/AESの仕組みからひもとく

メカニズムから見る暗号鍵の役割

大坂 幸治

表1 暗号に関する基礎的な用語

用　語	意　味	シーザー暗号における例
暗号化	平文を暗号文に置き換えること	−
復　号	暗号文を平文に戻すこと	−
平　文	暗号化されていない(元の)メッセージ	図1では「Caesar Shift」
暗号文	暗号化されたメッセージ	図1では「Fdhvdu Vkliw」
暗号アルゴリズム	暗号処理の規則	平文の各文字について，決まった量だけずらした文字と置き換える
暗号鍵	同じ暗号アルゴリズムで違う結果を得るための要素	ずらす文字の量．図1では「3」

暗号とは，情報を第三者に読み取られないようにするために，元の値を別の値に置き換えることです．暗号で重要な要素が暗号鍵と暗号アルゴリズムです．本稿では，暗号鍵に注目して，その重要性を，シーザー暗号，XOR pad(排他的論理和を利用した暗号)の仕組みとそれぞれの暗号鍵の弱点，そして，その弱点をクリアしたAESの仕組みを解説します．

暗号技術の基本…暗号鍵と処理内容

まずは歴史的に有名な暗号であるシーザー暗号を例に，暗号鍵をはじめとする基本的な用語(**表1**)を説明します．

シーザー暗号はローマ帝国のカエサル(英語読みでシーザー)が，秘密にしたい文書を作る際に使用したとされています．シーザー暗号はアルファベットを3文字だけずらした文字と置き換える(**図1**)という単純なものですが，紀元前には既に暗号は存在していたことになります．ずらす文字の量が「暗号鍵」，ずらした文字と置き換えるという規則が「暗号アルゴリズム」です(**図2**)．

図1を詳しく説明します．アルファベットで「C」の3つ後は「F」ですので，「C」は「F」に置き換えます．同様に，「a」は「d」に，「e」は「h」に置き換えます．結果として「Caesar Shift」という単語は，ぱっと見ただけでは意味の通らない文字列「Fdhvdu Vkliw」に変換されます．

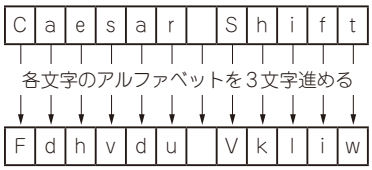

図1 シーザー暗号による暗号化

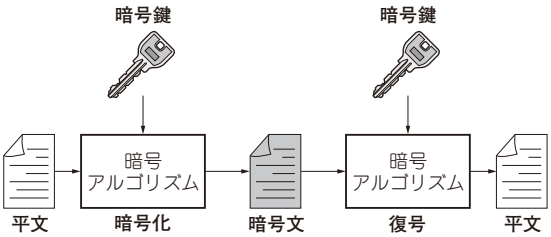

図2 暗号に関する基礎的な用語の関係
暗号化と復号で異なるアルゴリズムを使用する場合もある

暗号文を元に(平文に)戻すことを復号と呼びます．シーザー暗号では暗号化とは逆に，各文字のアルファベットを3文字戻すことで復号できます．

カエサルは3を使っていましたが，暗号鍵(ずらす文字の量)は変更可能な要素です．3のときに暗号文は「Fdhvdu Vkliw」になりましたが，4ならば「Geiwev Wlmjx」になりますし，10ならば「Mkockb Crspd」になります．暗号鍵を変更することによって，同じ暗号アルゴリズムでも違う結果を得られます．

シーザー暗号の弱点から暗号鍵の役割を考える

● シーザー暗号の仕組み

シーザー暗号における，暗号鍵の役割をより詳しく見るために，**リスト1**にシーザー暗号のPythonコードを示します．`caesarshift`関数が暗号処理の本体です．`key`は暗号鍵(ずらす文字の量)です．アルファベットはA ～ Zの26種類ですので26文字ずらす