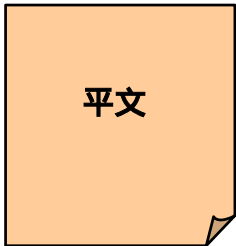


# 電子署名(デジタル署名)の概要

[ 発信者 ]



ハッシュ関数による圧縮

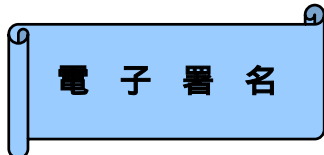


(例)

8c9d8072aa0d9c6f8d80a7639d3  
5ed6b

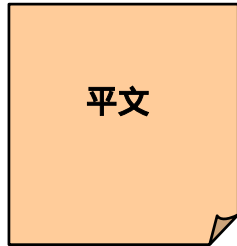


発信者の秘密鍵により暗号化

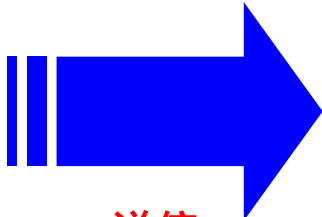


(例)

39971F57D0F034020E4DFCB7  
88A25EAADB92BA5B727A3370  
C4DD6B.....  
.....

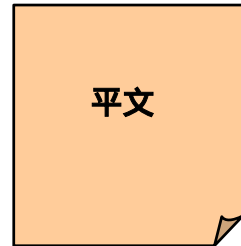


+



送信

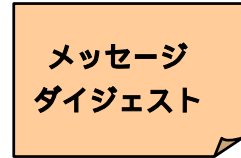
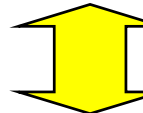
[ 受信者 ]



ハッシュ関数による圧縮



文書内容の  
真正性の確認



発信者の公開鍵により復号

本人性の確認



(注) 1 この他、文書内容の秘匿性を確保するための暗号化に鍵ペアが使用されることもある。

2 ハッシュ関数： $y=f(x)$ において、 $x$  (平文) から  $y$  (メッセージ・ダイジェスト) を求めるのは簡単であるが、 $y$  から  $x$  を求めるのは事実上困難であり、かつ異なる  $x$  から同一の  $y$  を生成するのが計算上不可能であるような関数をいう。