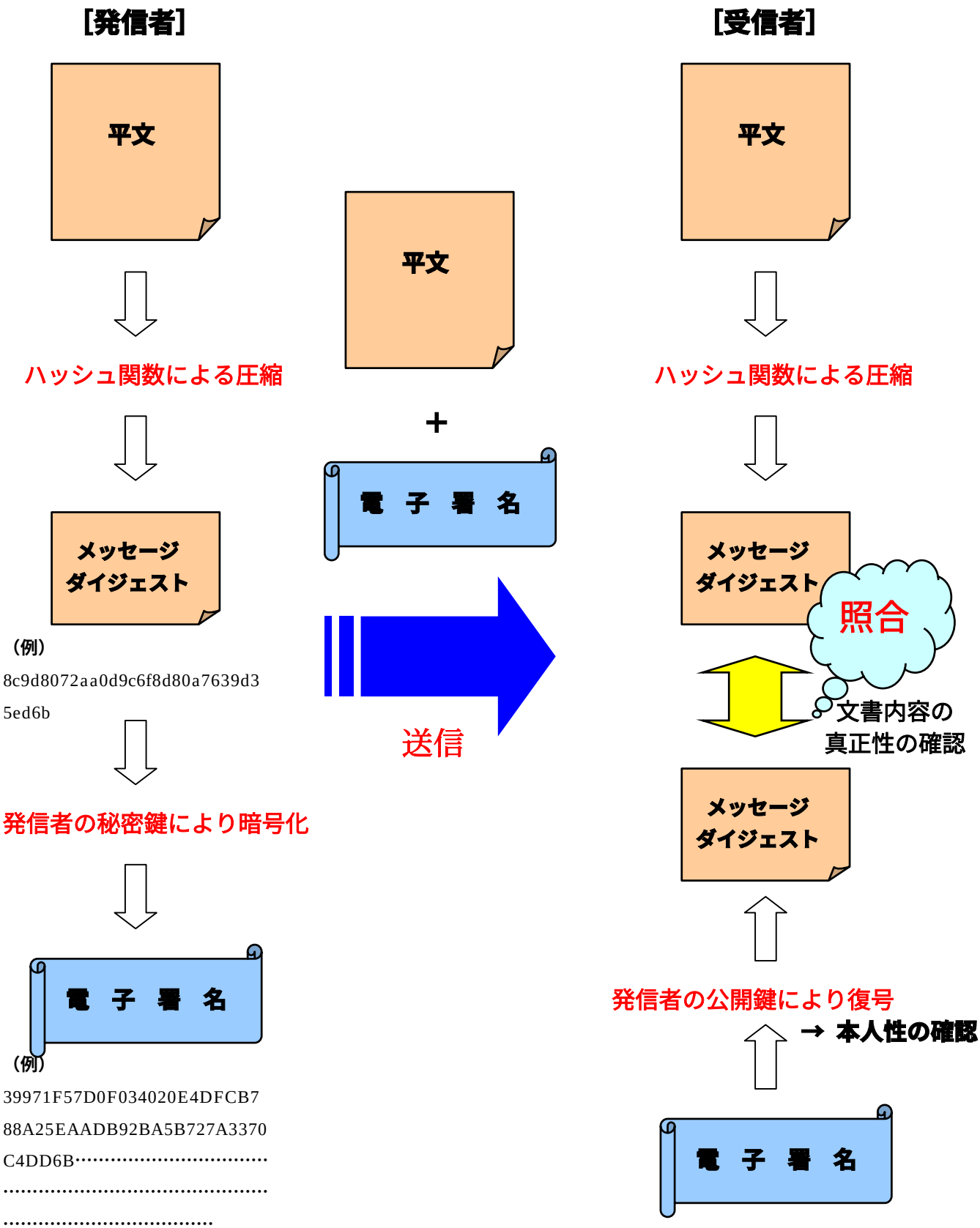
参考４

電子署名(デジタル署名)の概要



※（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。