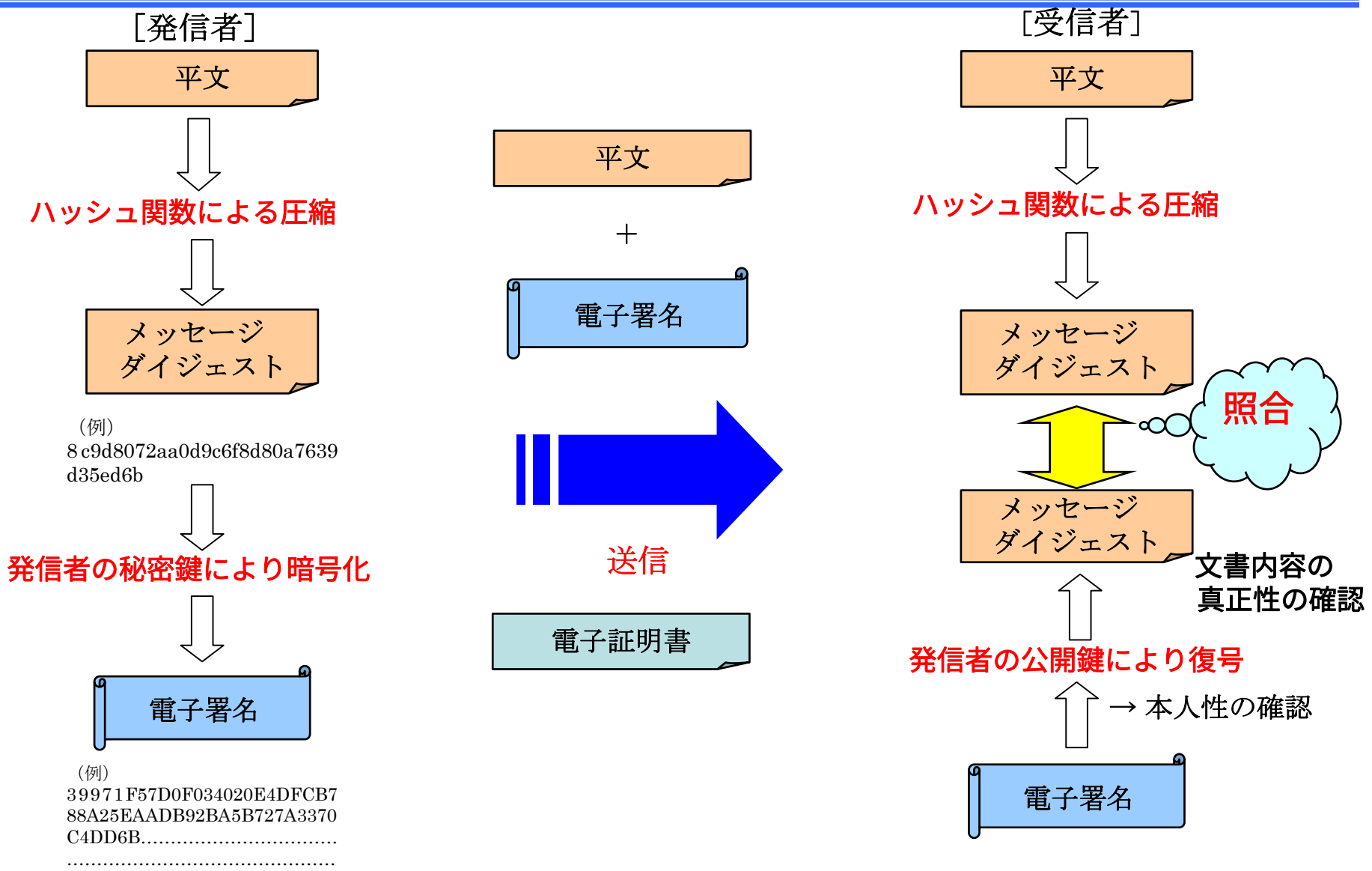
電子署名の仕組み



※（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。