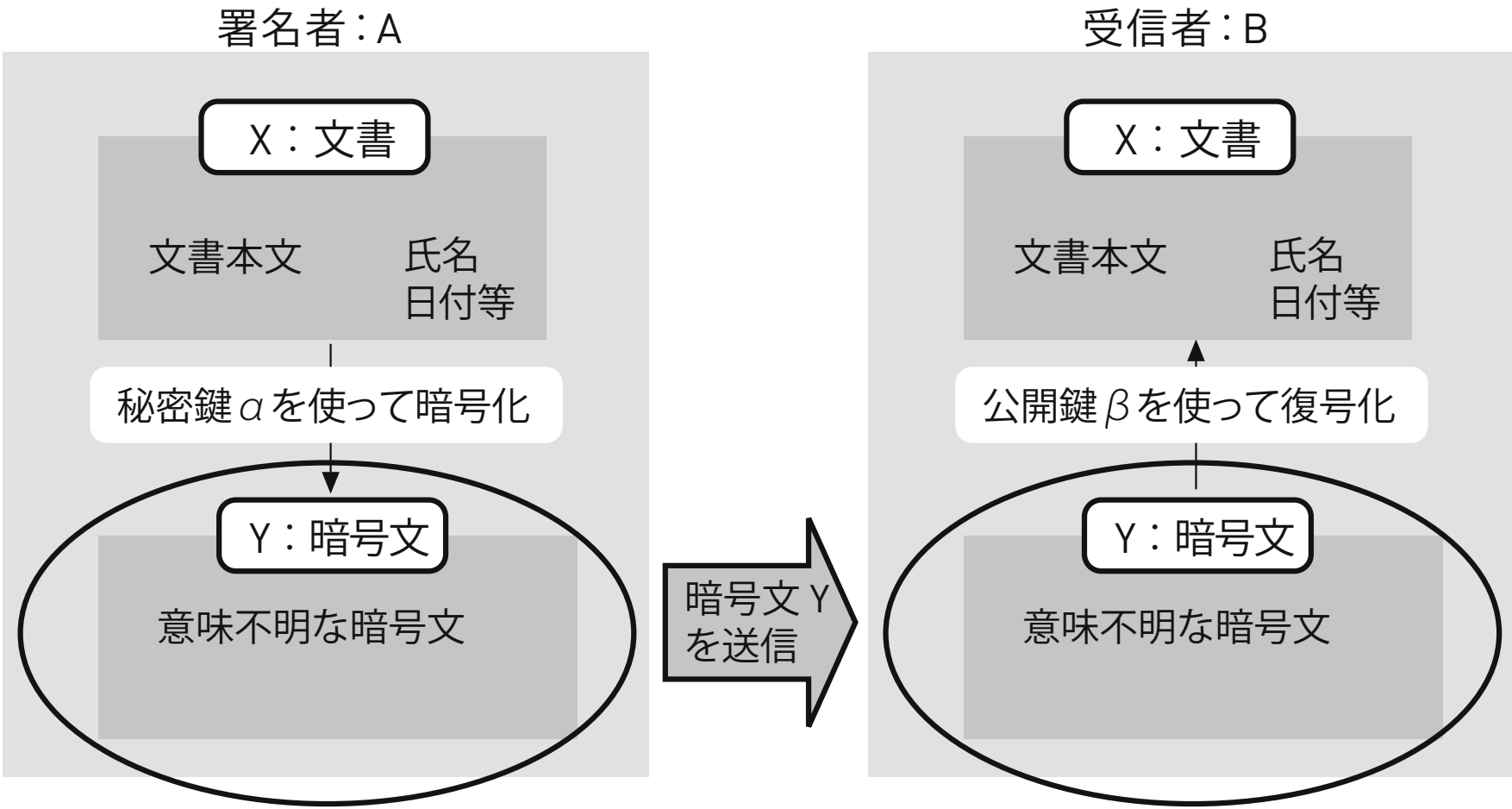
図表2-2｜電子署名のイメージ



- 公開されている公開鍵 β を利用すれば，Y→X と文書を復号化することができる．
- 公開鍵 β と暗号文からは，秘密鍵 α を知ることができない．したがって，Y という暗号文を作成できるのは，秘密鍵 α を保有している署名者 A だけである．
- 受信者 B は，公開鍵 β で暗号文 Y を復号化できれば，文書が署名者 A によって作成された真正なものであると確認できる．