公開鍵方式

原理　受信者の公開鍵で暗号化して
受信者の秘密鍵で復号化
言い換えると
受信者は自分宛の文書を予め自分が配布した公開鍵で暗号化してもらい、暗号文を受け取った後自分が手元に保有する秘密鍵で復号化する。

特徴

(1)秘密鍵は受信者だけが保有するので、共通鍵方式に比べ、鍵が盗まれる機会が少ない。
(2)暗号化、解読に時間がかかる。
(3)公開鍵から秘密鍵を見破られる可能性は極めて低い。
(4)逆に、秘密鍵で暗号化すれば、公開鍵で復号化できる。この性質を署名の認証に利用する。
(5)相手の公開鍵の保有が必要
(6)費用がかかる。

以上により、下の左の犯罪に対し右で対応する

1.盗聴	暗号化(公開鍵と共通鍵)
2.改ざん	電子署名と認証
3.成りすまし	電子署名と認証
4.自己否定	電子署名と認証

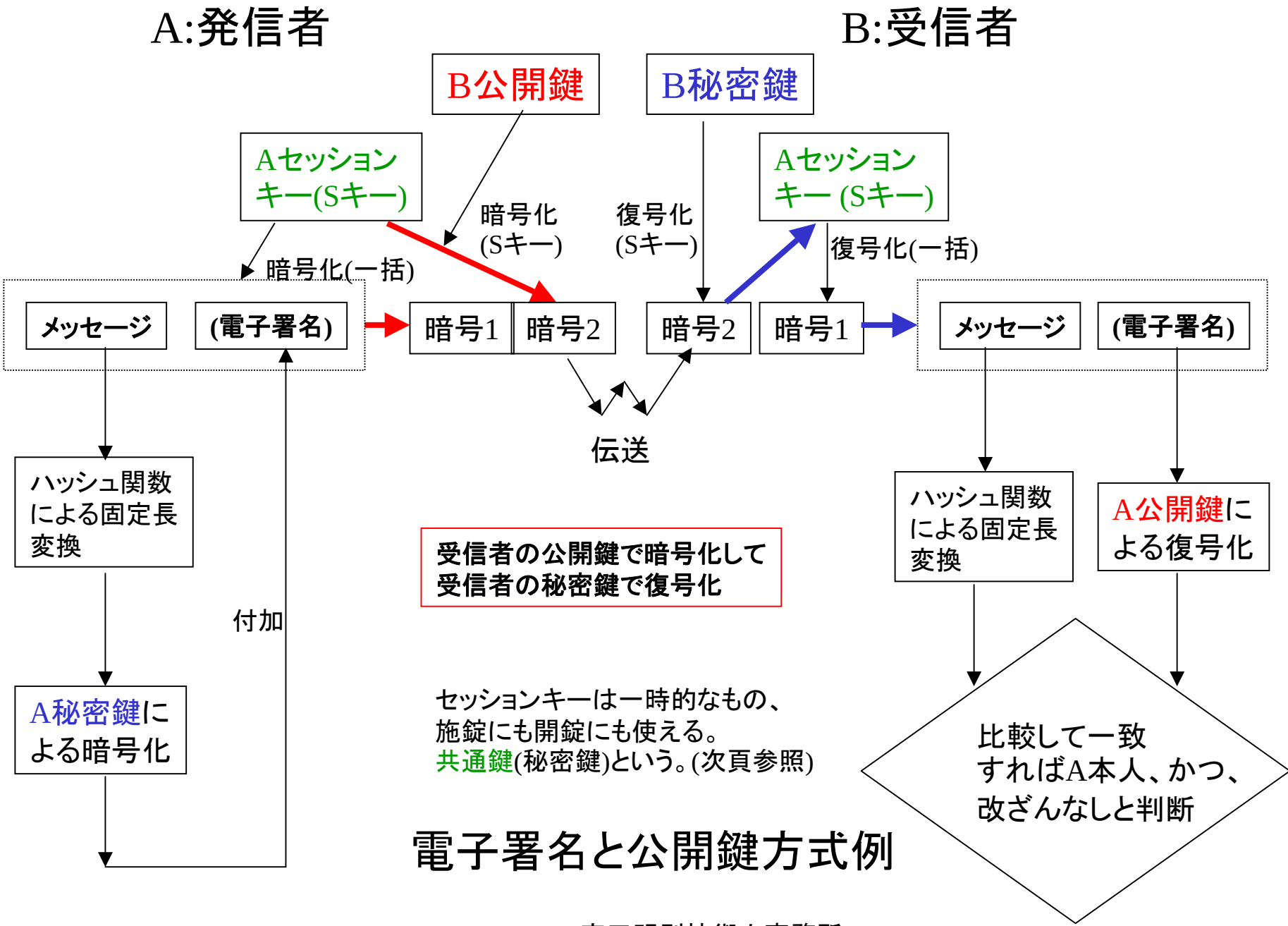
共通鍵(秘密鍵)方式

原理　発信者と受信者は予め共通の秘密鍵を保有しておく。
暗号化と復号化とは同じ鍵で可能である
(可逆性があるという)

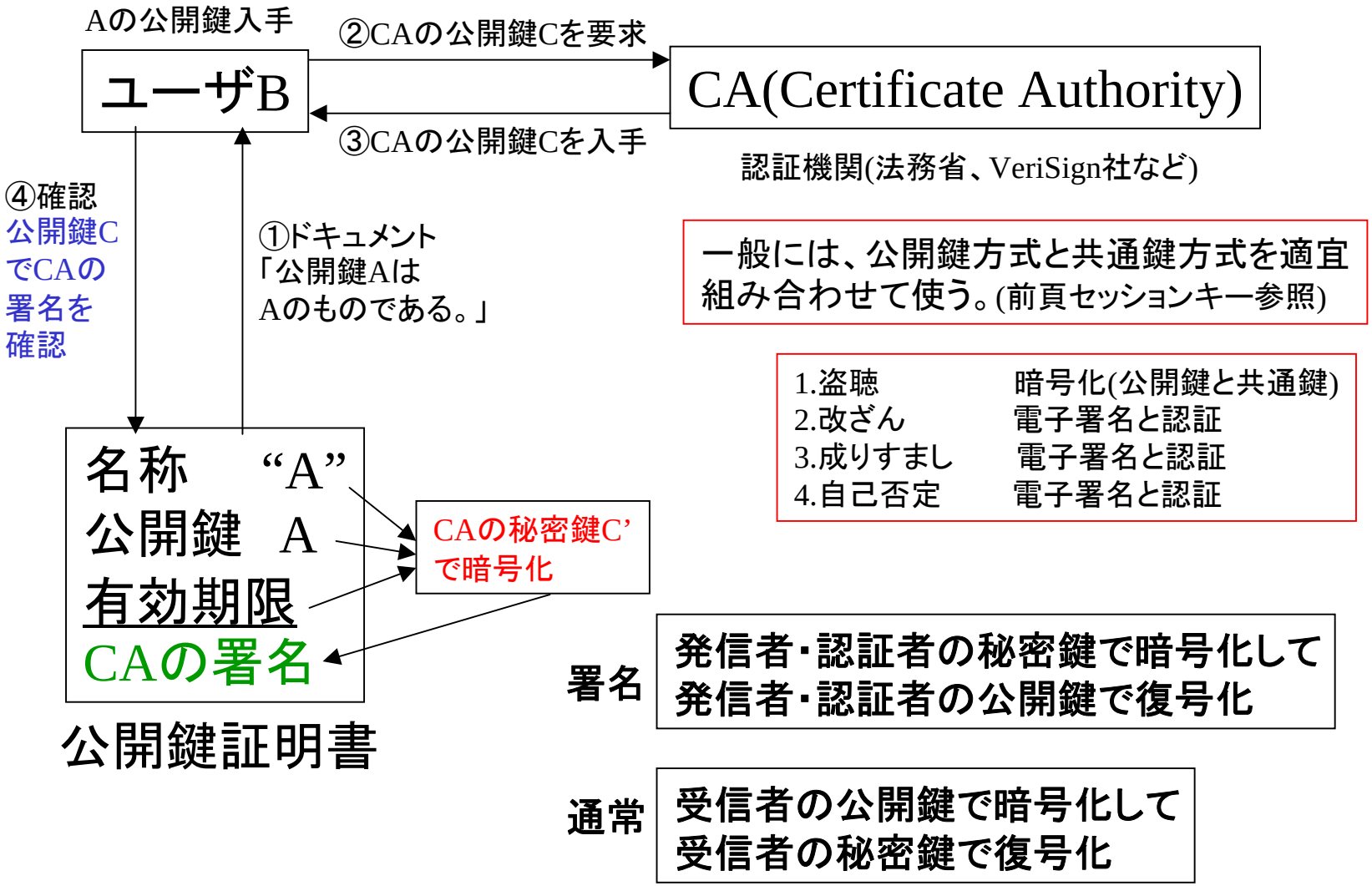
特徴

(1)共通鍵が盗まれると盗聴、改ざん成りすましの可能性がある。
(2)暗号化、解読に時間がかからない。
(3) 鍵が盗まれさえしなければ簡単で便利な方法である。
(4)電子署名には不向き。
(5)費用が安い。

公開鍵方式と共通鍵(秘密鍵)方式のそれぞれの特徴を理解し、適当に組み合わせて使う



電子署名と公開鍵方式例



認証(BがAの公開鍵をCAに確認してもらう方法)