第26講　ネットワークセキュリティ2

暗号化、秘密鍵、公開鍵　電子認証

第26講　ネットワークセキュリティ 2

- 暗号化　平文、暗号文　暗号化・復号
- 秘密鍵暗号方式
- 公開鍵暗号方式
- 電子認証

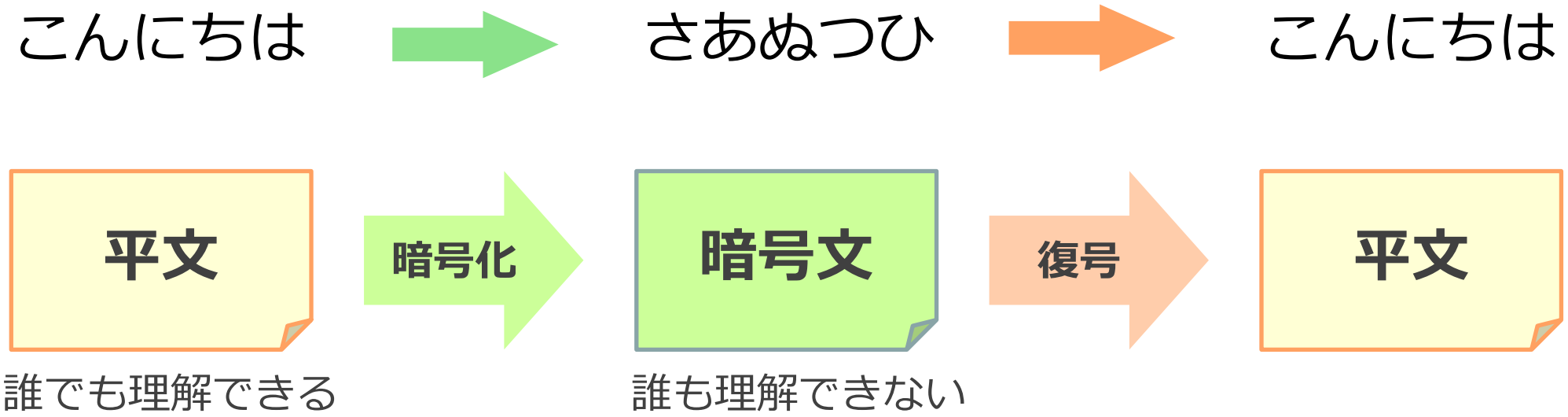
- セキュリティの要「暗号化」

暗号化とは

第三者読み取られないように

データに変換処理を施すこと

セキュリティの要「暗号化」



暗号化に必要なもの

暗号化アルゴリズム　＋　鍵

「暗号化」の簡単な例

暗号化アルゴリズム

文字をずらす

鍵

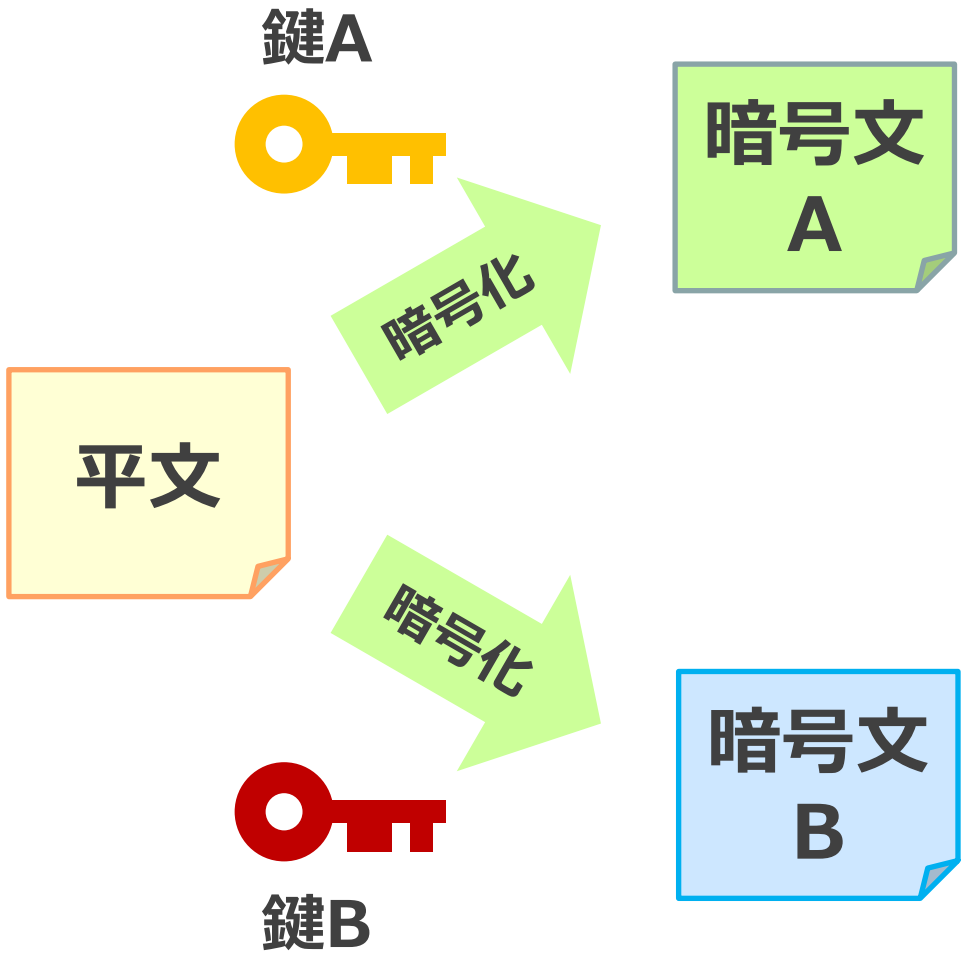
ずらす文字数

平文：こんにちは

鍵＝１の場合　暗号文：**さあぬつひ**

鍵＝３の場合　暗号文：**すうのとへ**

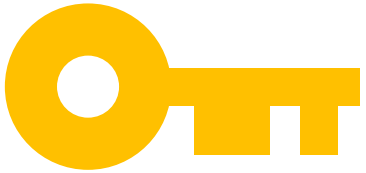
セキュリティの要「暗号化」



鍵が変わると
暗号文も変わる

暗号化した鍵に
対応する鍵でなければ
復号できない

セキュリティの要「暗号化」



共通鍵、公開鍵、秘密鍵

共通鍵：送信側・受信側で共通

公開鍵：秘密鍵をもつ人が作って公開

秘密鍵：公開鍵・秘密鍵は**ペア**になっている

セキュリティの要「暗号化」

2種類の暗号方式

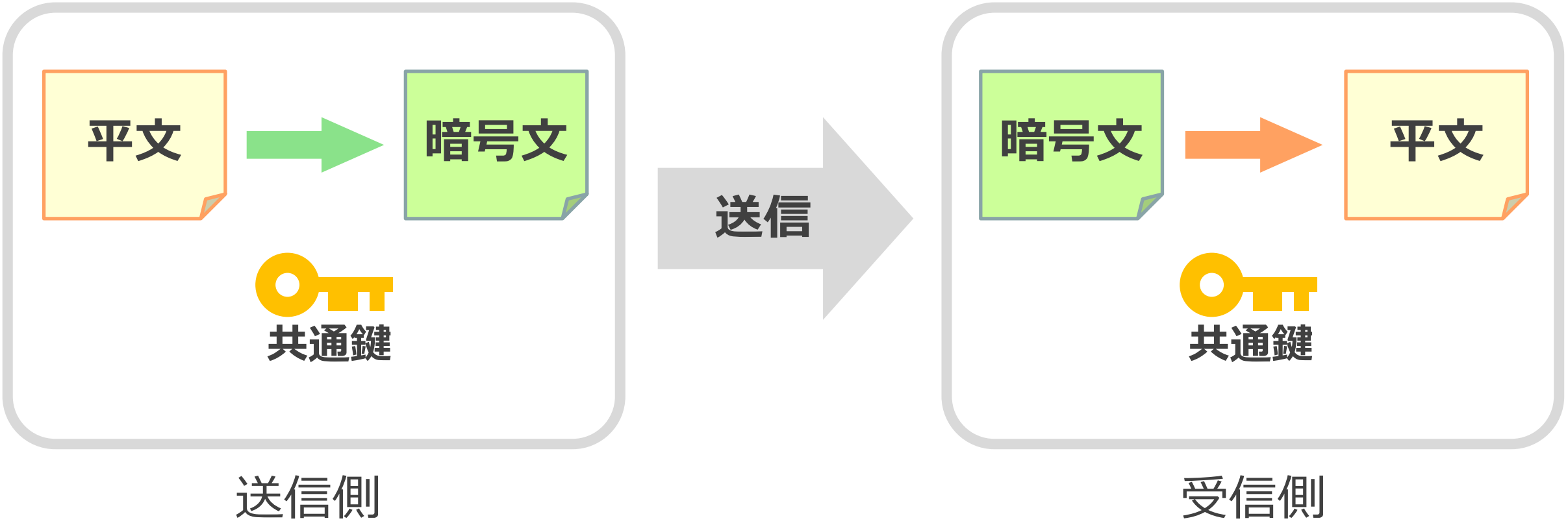
①共通鍵暗号方式

１つの共通鍵で暗号化・復号

②公開鍵暗号方式

1組の公開鍵・秘密鍵で暗号化・復号

共通鍵暗号方式



共通鍵暗号方式

①メリット

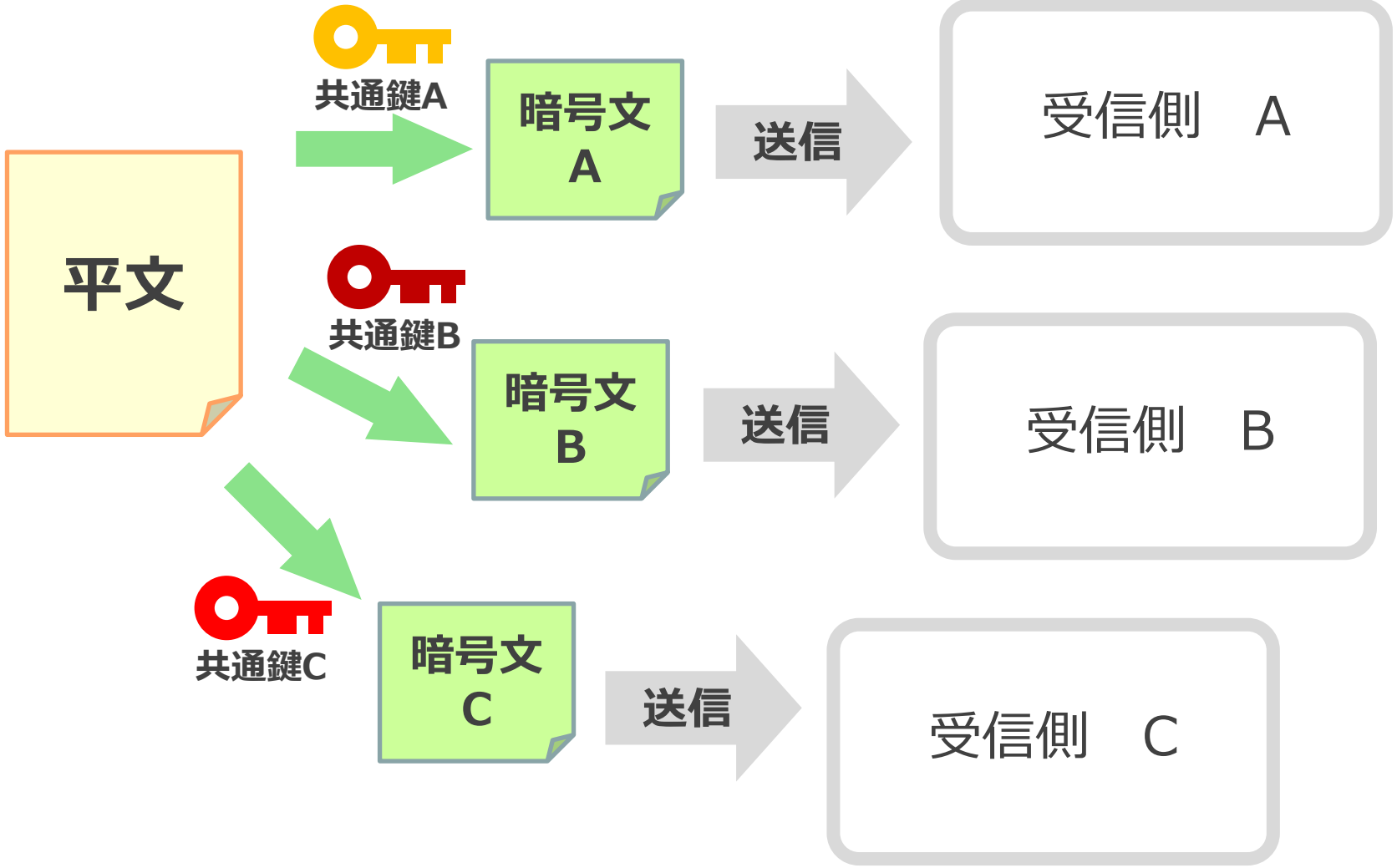
アルゴリズムが単純、処理が速い

②デメリット

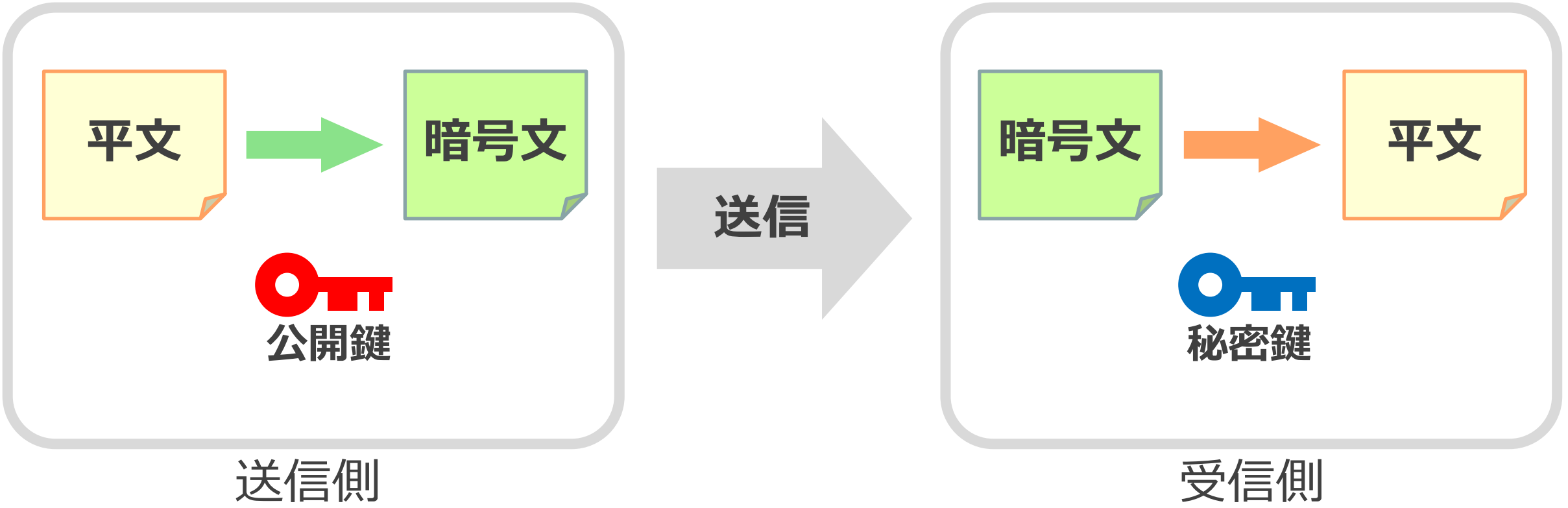
鍵の受け渡しが困難

受信側の数だけ鍵の種類が必要

共通鍵暗号方式



公開鍵暗号方式



送信側

受信側

公開鍵は受信側が作成

公開鍵とペアの秘密鍵でなければ
復号できない

公開鍵暗号方式

①メリット

鍵の種類は１つでOK

②デメリット

アルゴリズムが複雑なので処理が遅い

暗号方式のポイント

①鍵の管理

特に復号鍵の管理が重要

②送信者、公開鍵の認証

送信者が本人かどうか

公開鍵の素性は大丈夫か

- データ改ざんをチェックするには

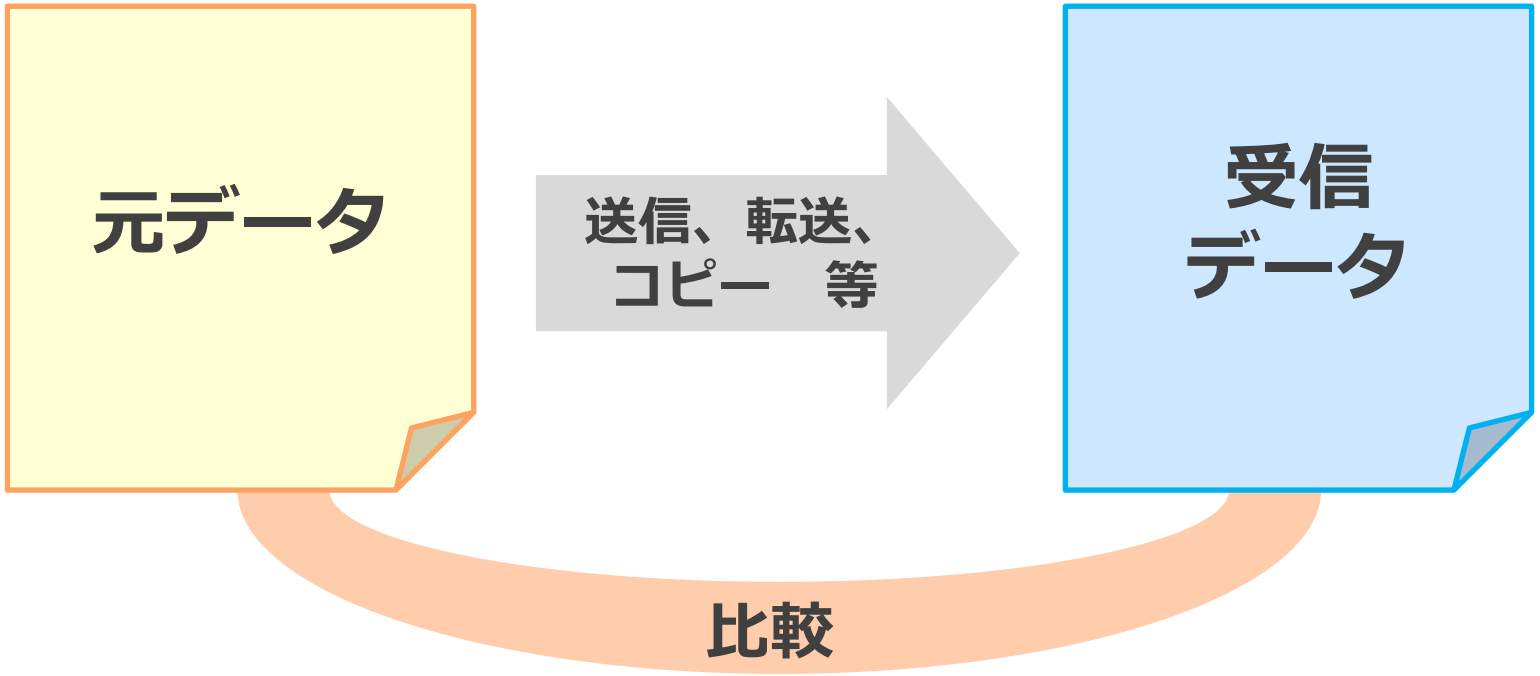
データ改ざんとは

データ改ざんとは

悪意ある第三者がデータを書き換えること

データ改ざんを防ぐには

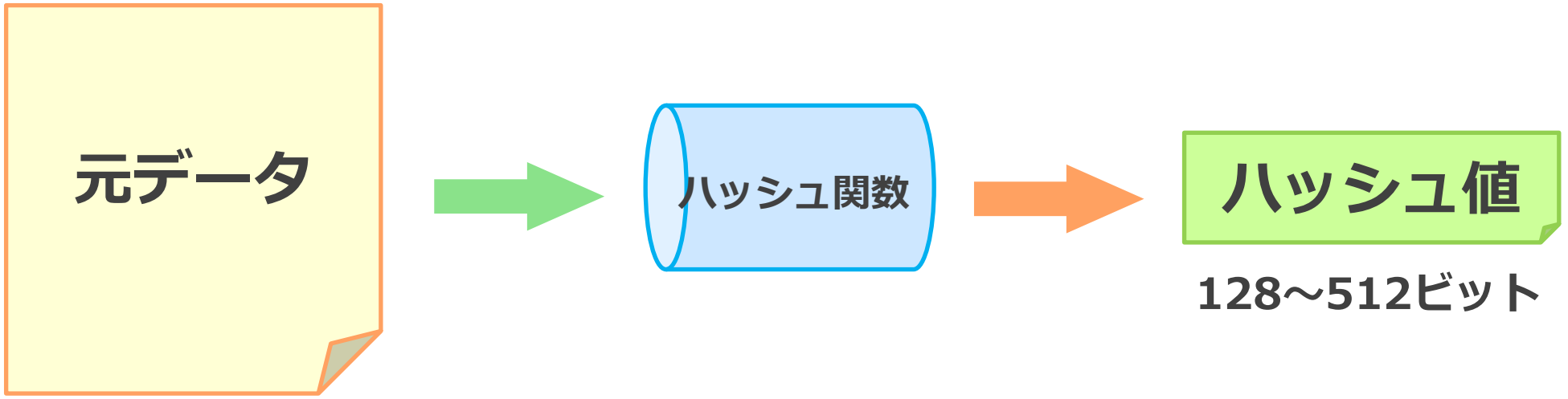
元データと受信データの比較が必要



でも、どうやって？？？

データ改ざんを見つける

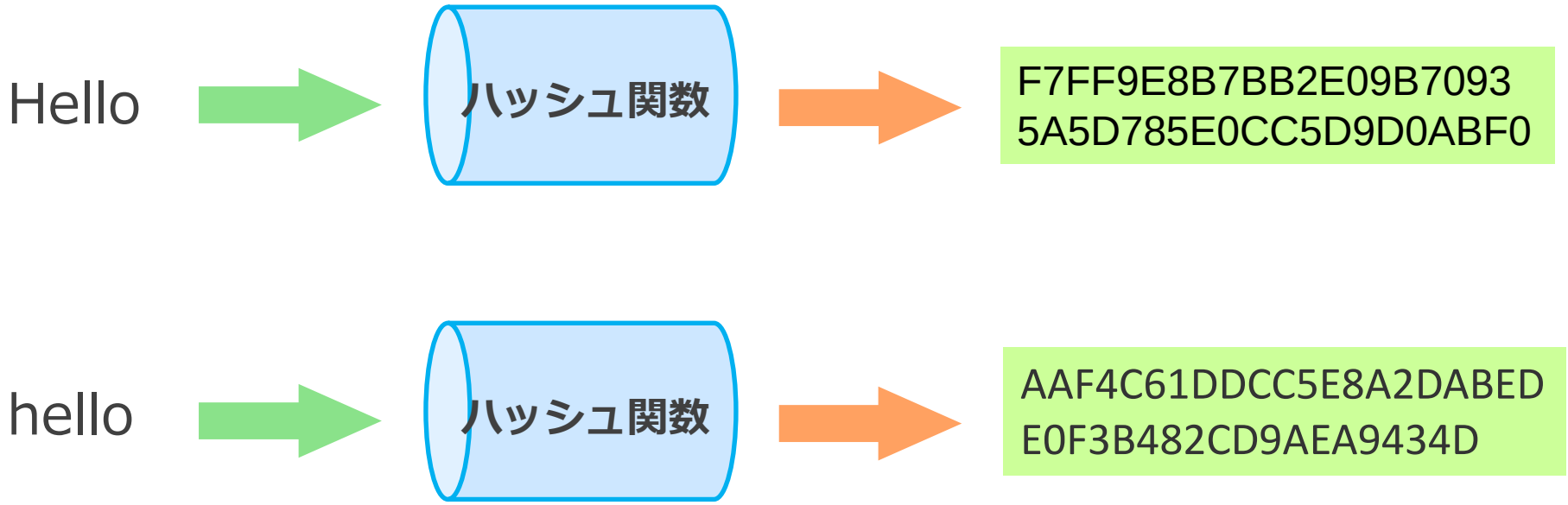
改ざんの有無をチェックするために
ハッシュ値を使う



元データの大きさにかかわらず
同じ長さのハッシュ値を得る

ハッシュ値の特徴

元データが1ビットでも変わると
ハッシュ値は大きく変化する



ハッシュ値の特徴

ハッシュ値が異なれば、
改ざんされていることが分かる

F7FF9E8B7BB2E09B7093
5A5D785E0CC5D9D0ABF0

≠

AAF4C61DDCC5E8A2DABED
E0F3B482CD9AEA9434D

**改ざん
された！**

ハッシュ値を使う

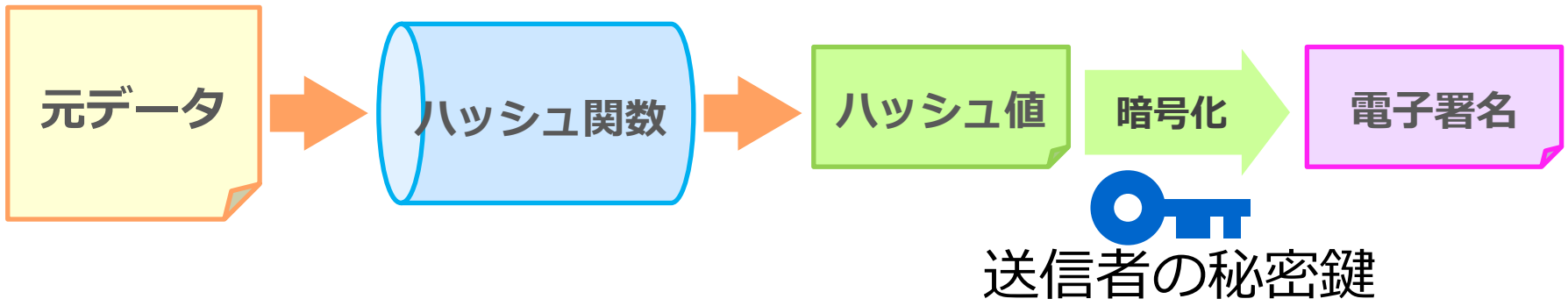
ハッシュ値を利用して**「電子署名」**

本人かどうか確認できるしくみ

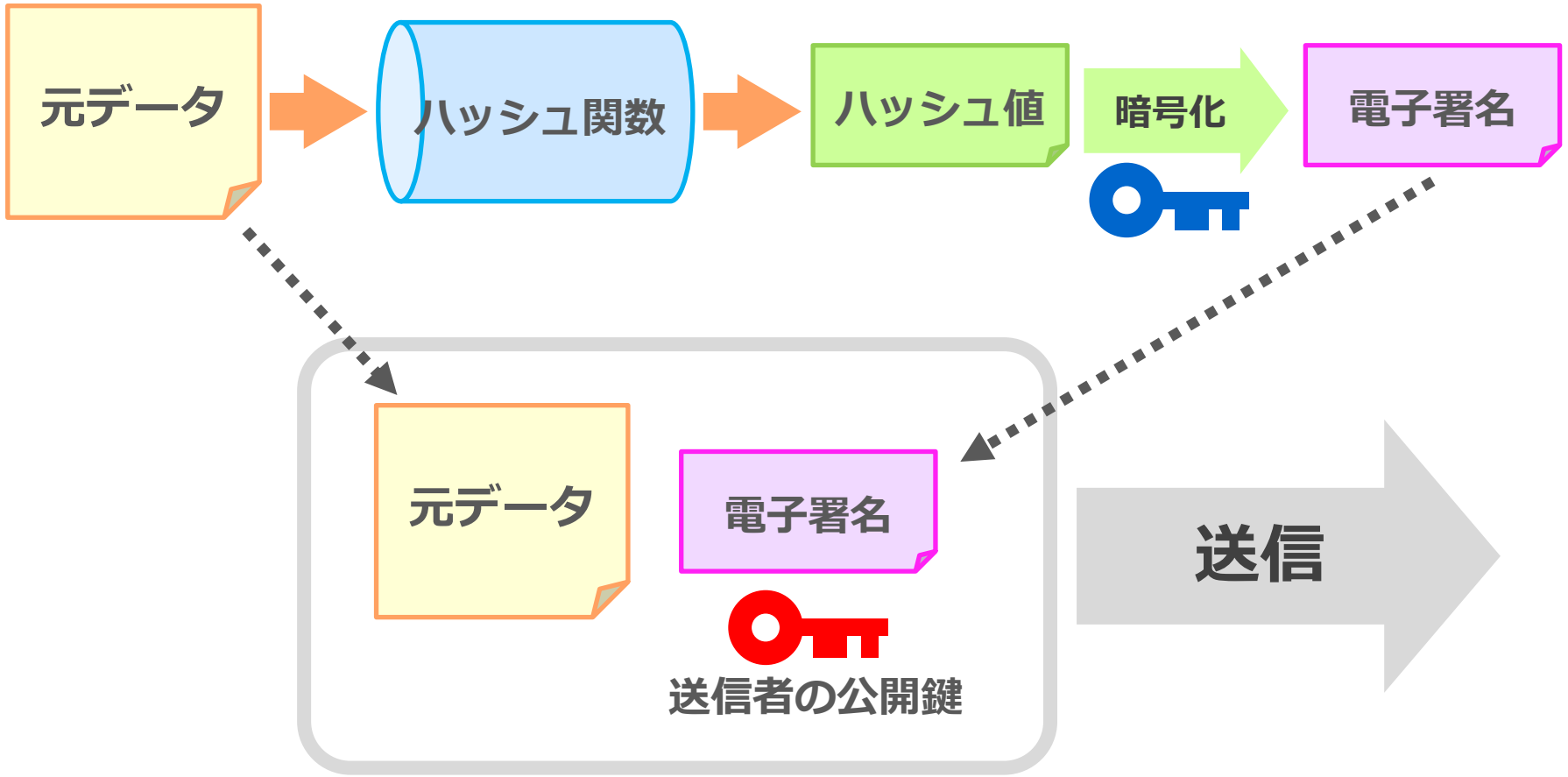
秘密鍵で暗号化したものは
対応する**公開鍵だけで復号できる**
ことを利用

電子署名

送信側が電子署名を作るまで

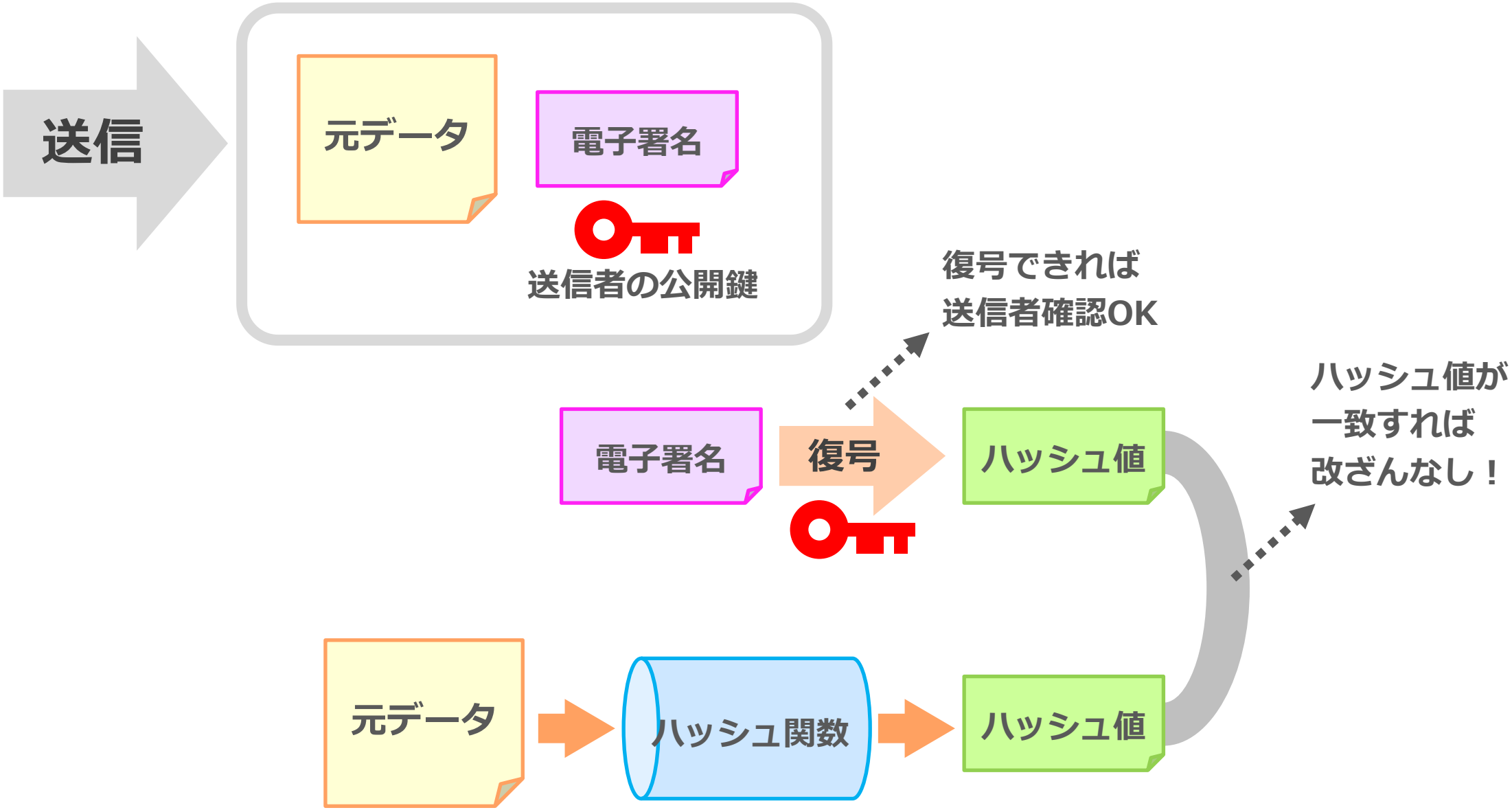


電子署名付きで送信



元データ、電子署名、公開鍵を
セットで送信

受信側でチェック


送信
元データ
電子署名
送信者の公開鍵
復号できれば
送信者確認OK
電子署名
復号
ハッシュ値
ハッシュ値が
一致すれば
改ざんなし！
元データ
ハッシュ関数
ハッシュ値

まだ安心できません

その公開鍵、信用できますか？

悪意ある第三者の公開鍵かも…

公開鍵は **「認証局」** が保証

Certification Authority

まだまだ安心できません

その認証局、信用できますか？

悪意ある第三者の認証局かも…

「認証局」の認証は

「上位レベルの認証局」が保証

認証局は階層構造になっている

第26講　ネットワークセキュリティ２

- 暗号化　平文、暗号文　暗号化・復号
- 秘密鍵暗号方式
- 公開鍵暗号方式
- 電子認証

第25講はここまで