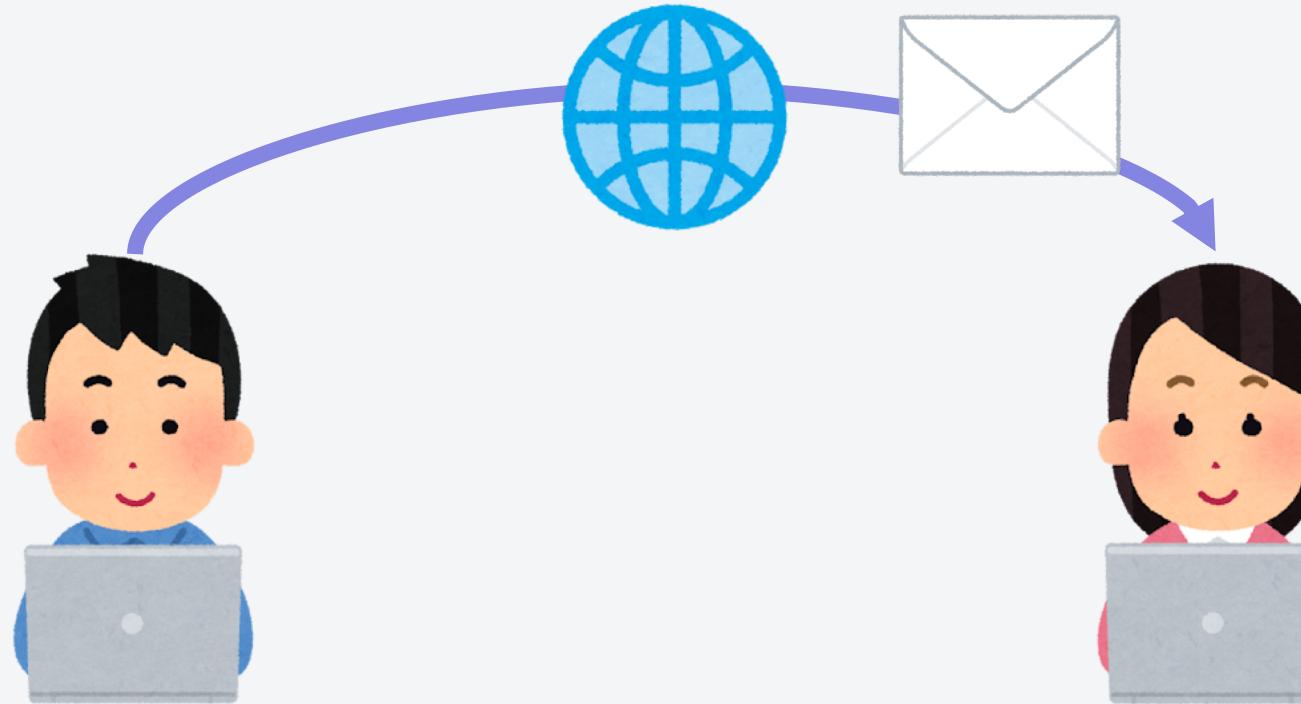


第20回

20_ネットワーク⑤(情報の暗号化)

情報の盗聴とは？

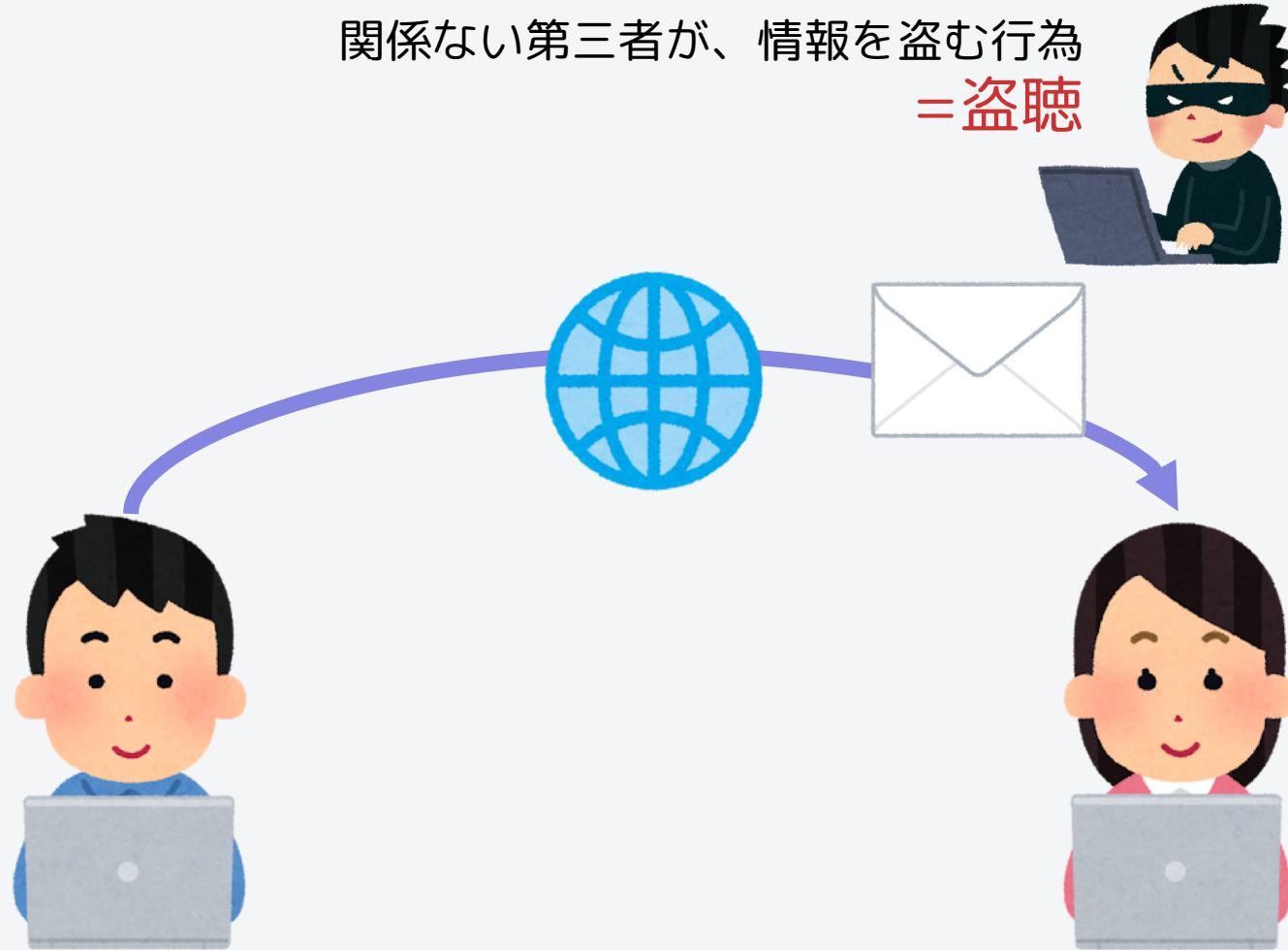
インターネットを通してメールを送る



情報の盗聴とは？

関係ない第三者が、情報を盗む行為

= 盗聴



情報の盗聴とは？

どんなデータを送信したかなどの情報は、簡単に盗聴することが可能



```
[Full request URI: http://192.168.22.  
[HTTP request 1/3]  
[Response in frame: 1792]  
[Next request in frame: 1810]  
File Data: 34 bytes  
▼ HTML Form URL Encoded: application/x-www-form-urlencoded  
  > Form item: "username" = "yoidea"  
  > Form item: "password" = "Rossy0213"
```

<https://youtu.be/FnhD7IjtPhY?si=TEJgjEBBuV5nZKIh> ラムダ技術部：【注意】フリーwifi盗聴ちょろすぎて草

情報の盗聴とは？

データを **暗号化** することで、情報の解読を防いでいる

```
192.168.197.227 192.168.87.20 443 → 61625 [ACK] Seq=5199
 3:bc:65:b0 (b2:2a:43:bc:65:b0), Dst: Apple_94:0e:ba
 4, Src: 216.58.197.227, Dst: 192.168.87.20
 ocol, Src Port: 443, Dst Port: 61625, Seq: 5153, Ack
 5199, Len: 23
  Application Data Protocol: http2
  Application Data (23)
 303: 解読できないようになっている
  Data: 0000000000000000d455381e8891416d622852bff53779
  op_data), 41 bytes
  Packets: 864 · Displayed: 836 (96.8%) · Dropped:
```

<https://youtu.be/FnhD7IjtPhY?si=TEJgjEBBuV5nZKIh> ラムダ技術部：【注意】フリーwifi盗聴ちょろすぎて草

| 身近な暗号化の例

IZOZM ➤➤➤➤ JAPAN

のとき、

GDKKN ➤➤➤➤ ???

| 身近な暗号化の例

IZOZM ➤➤➤➤ JAPAN

のとき、

GDKKN ➤➤➤➤ HELLO

| 身近な暗号化の例

IZOZM ➤➤➤➤ JAPAN

のとき、

GDKKN ➤➤➤➤ HELLO

ルール:1文字ずらす

| 身近な暗号化の例

暗号文

IZOZM



JAPAN

GDKKN



HELLO

ルール:1文字ずらす

| 身近な暗号化の例

暗号文

IZOZM



のとき、



GDKKN

平文

JAPAN

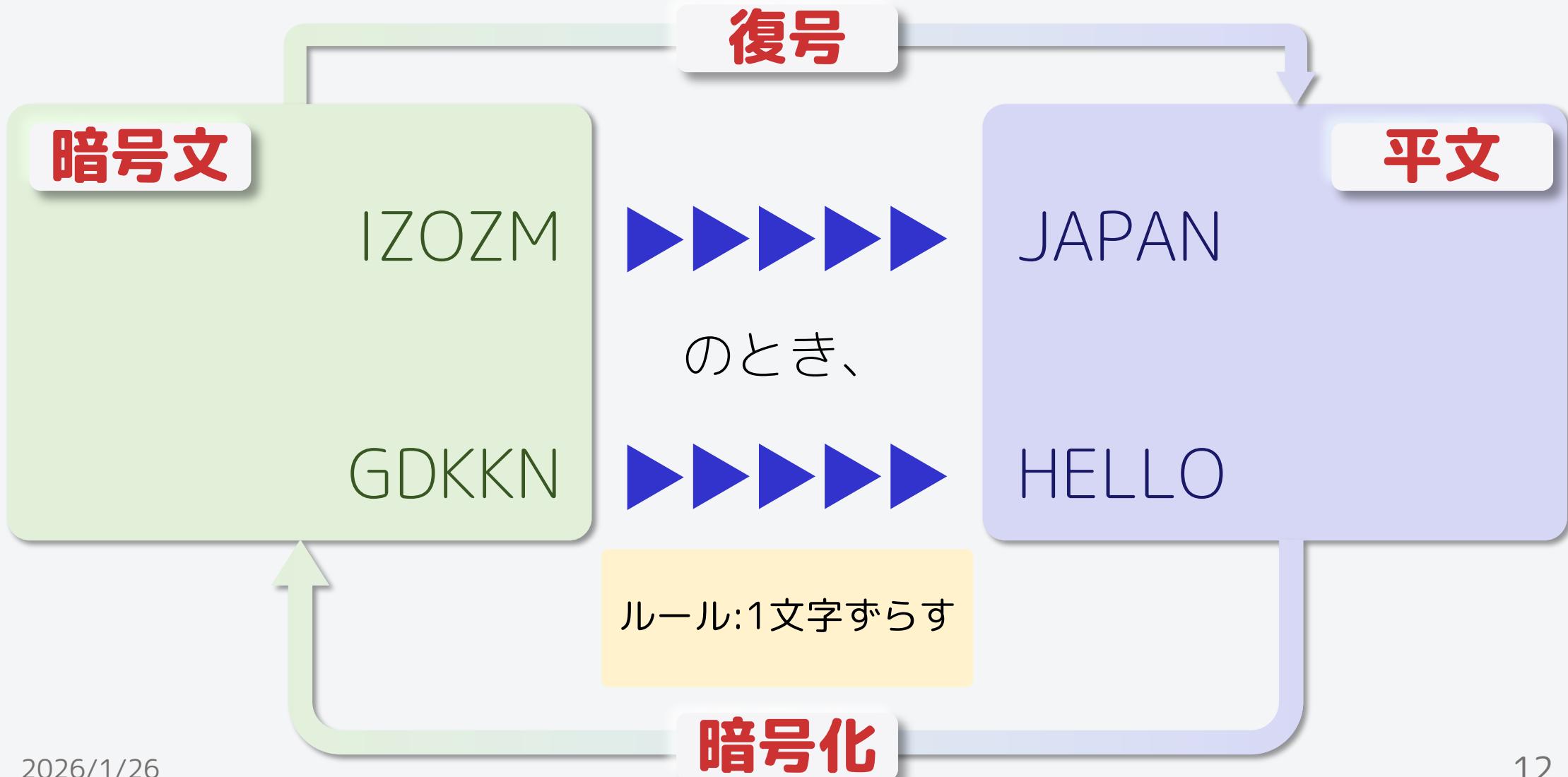
HELLO

ルール:1文字ずらす

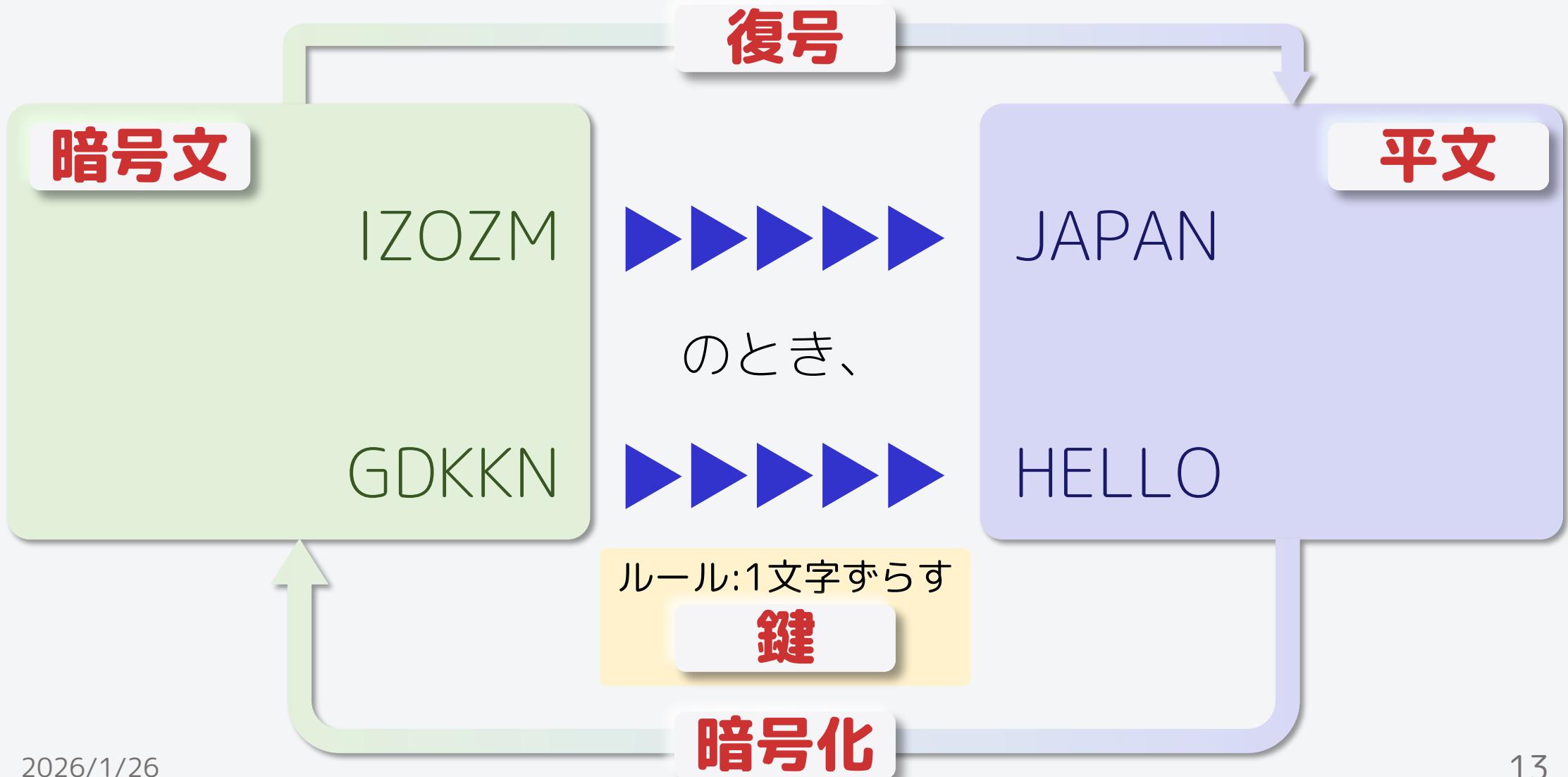
| 身近な暗号化の例



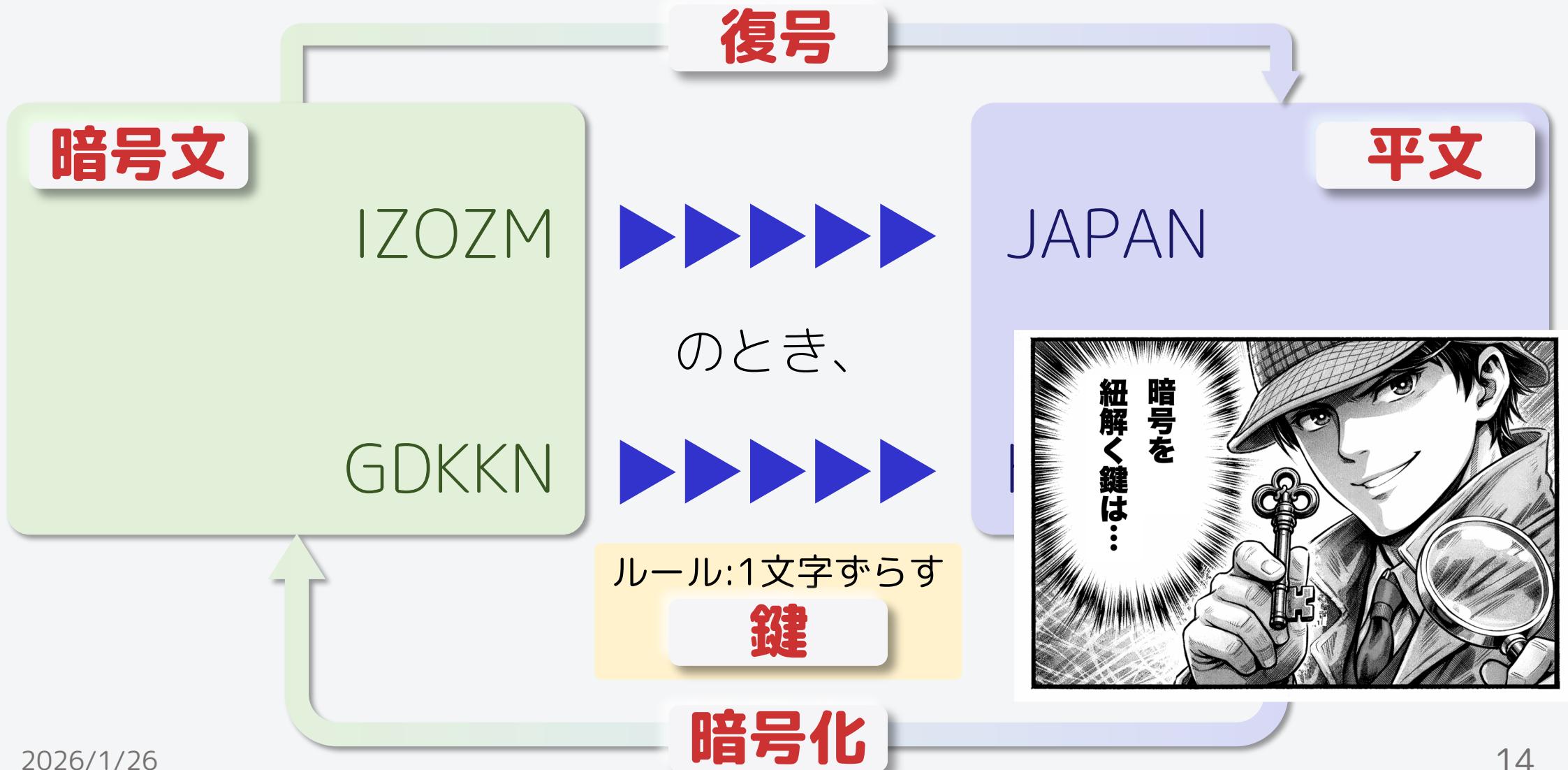
| 身近な暗号化の例



| 身近な暗号化の例



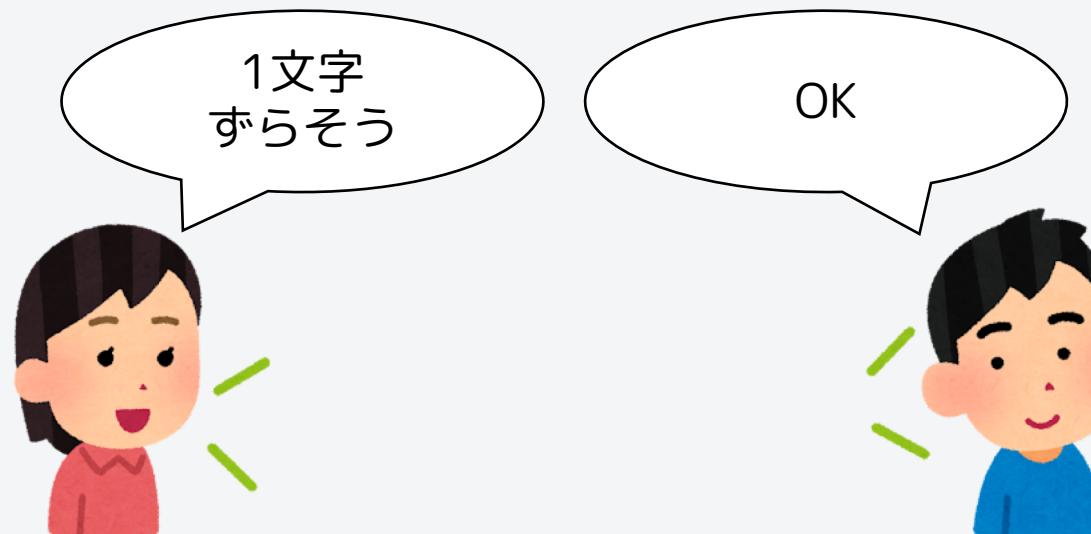
身近な暗号化の例



身近な暗号化の例

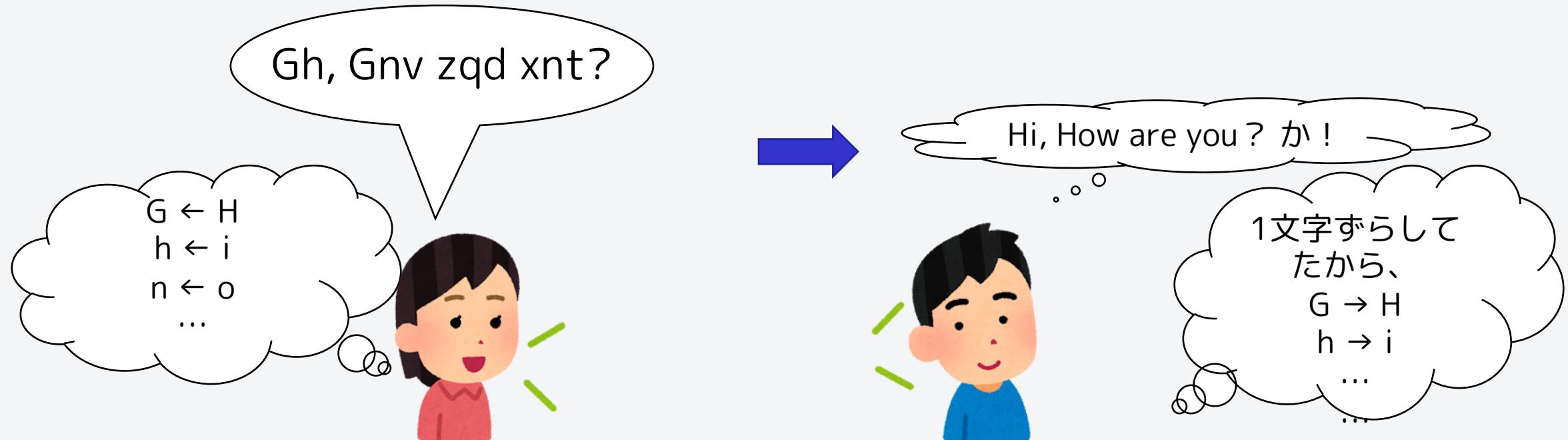
- ・シーザー暗号(アルファベットを一定文字数分ずらす)

①何文字ずらすかを2人だけで約束する



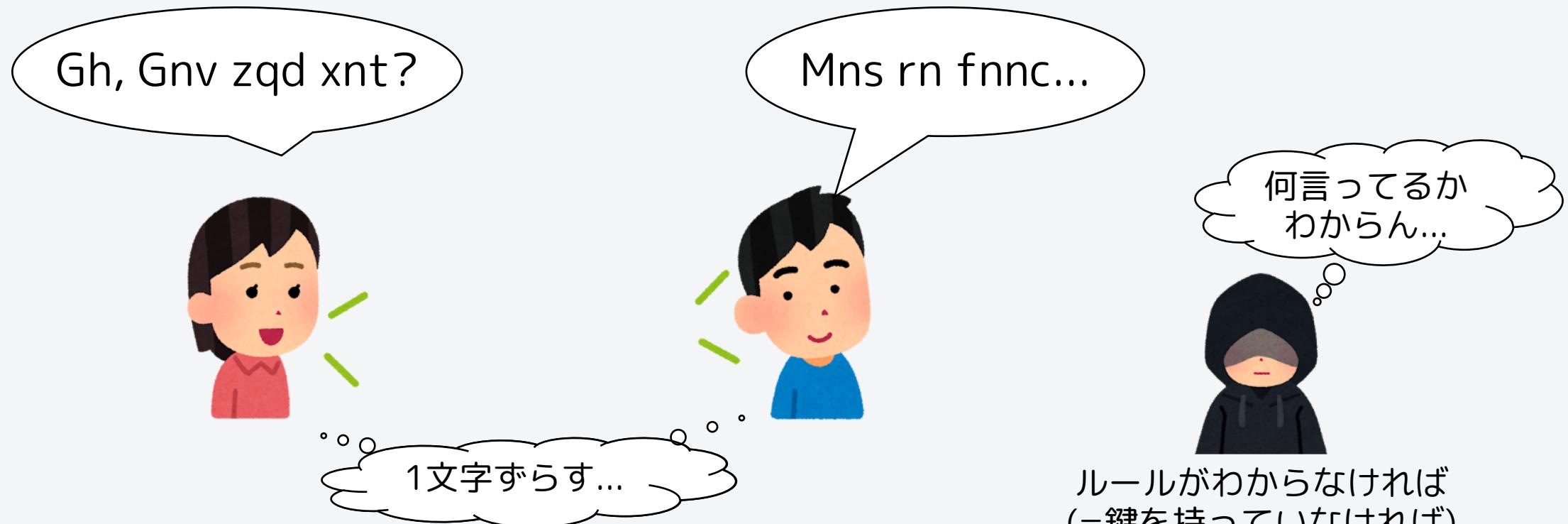
| 身近な暗号化の例

- ・シーザー暗号(アルファベットを一定文字数分ずらす)



| 身近な暗号化の例

- ・シーザー暗号(アルファベットを一定文字数分ずらす)



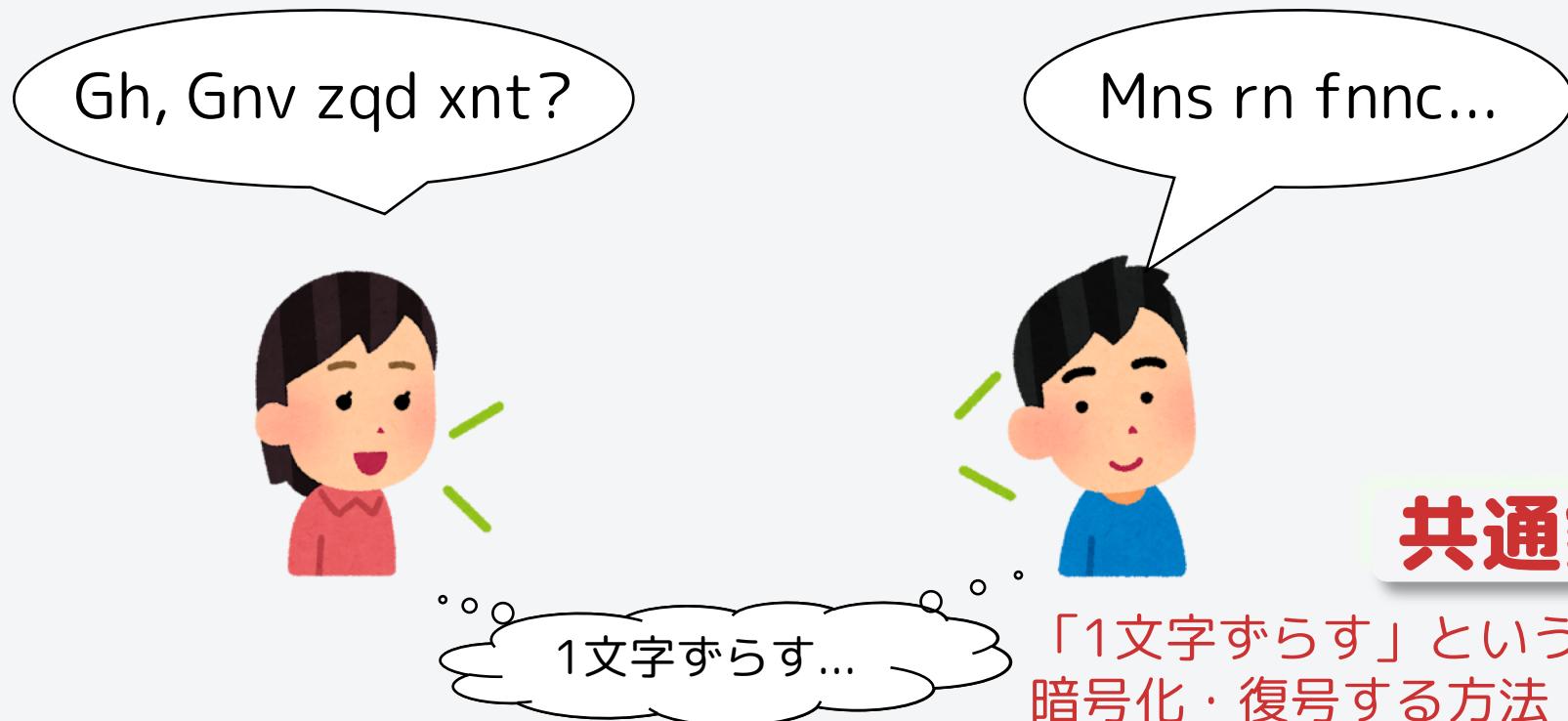
| 身近な暗号化の例

- ・シーザー暗号(アルファベットを一定文字数分ずらす)



| 身近な暗号化の例

- ・シーザー暗号(アルファベットを一定文字数分ずらす)

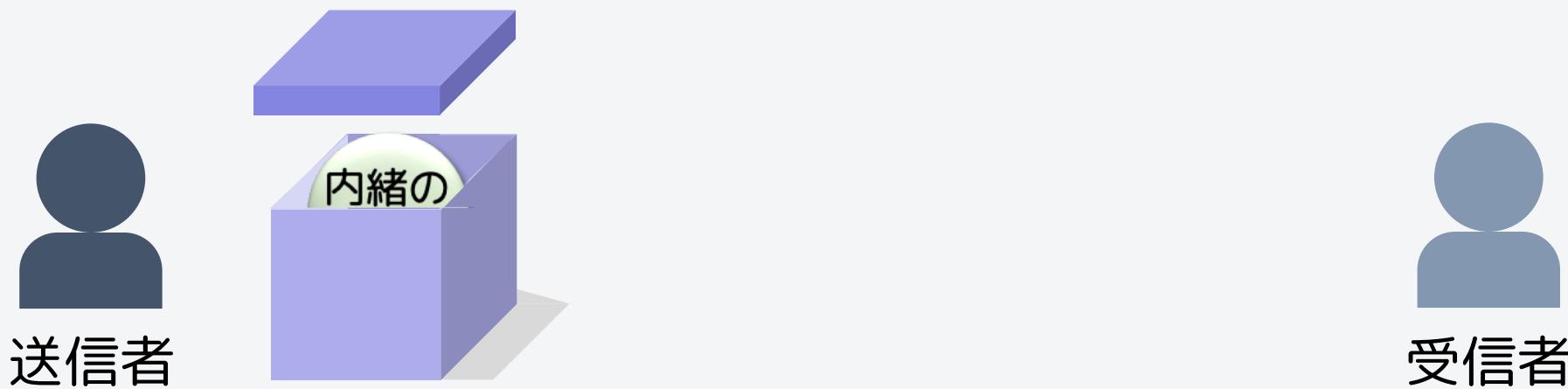


共通鍵暗号方式

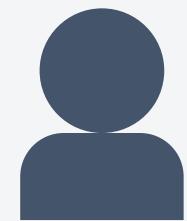
「1文字ずらす」という共通の鍵を使って
暗号化・復号する方法

共通鍵暗号方式

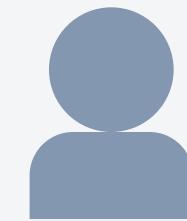
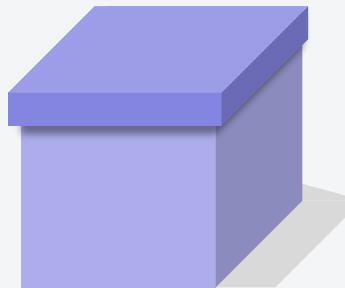
データを送るとは？



データを送るとは？



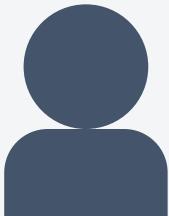
送信者



受信者

そのまま受信者に送る

データを送るとは？



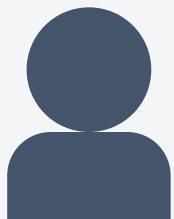
送信者



受信者

データの送信を行うことができます。

データを送るとは？



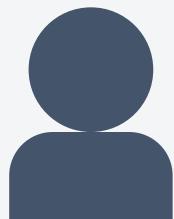
送信者



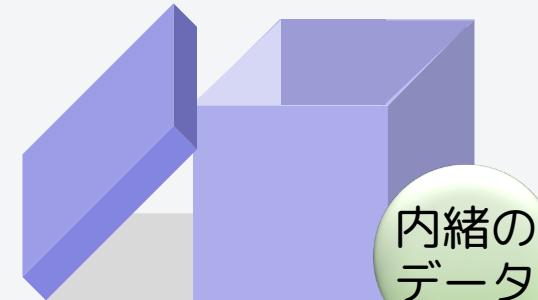
受信者

データの送信を行うことができます。

データを送るとは？



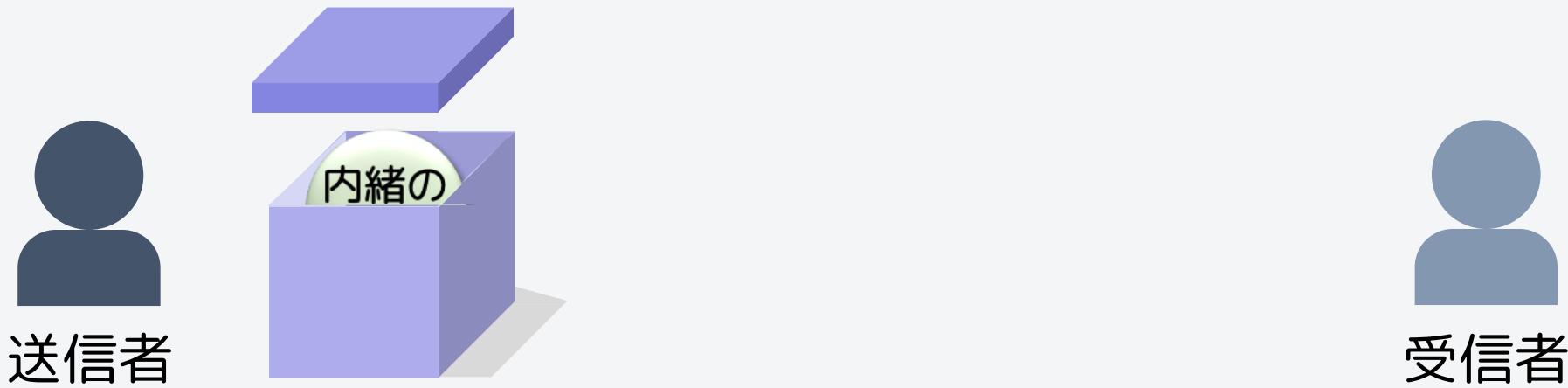
送信者



受信者

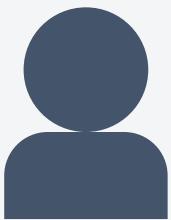
データの送信を行うことができます。

この送り方の問題点

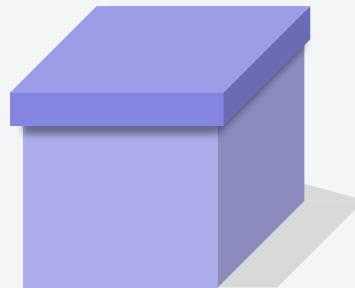


送信者は、箱の中にデータを入れて

この送り方の問題点



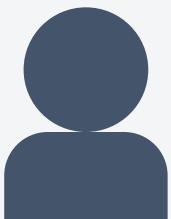
送信者



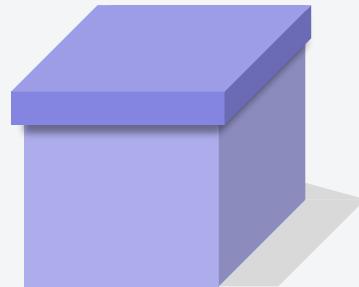
受信者

送信者は、箱の中にデータを入れて

この送り方の問題点



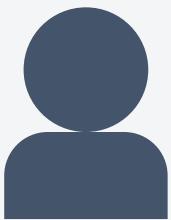
送信者



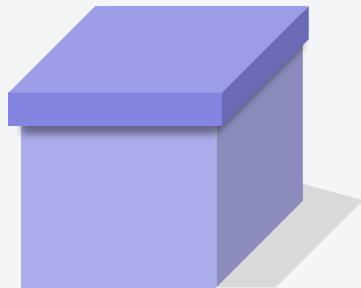
受信者

そのまま受信者に送るとき、

この送り方の問題点



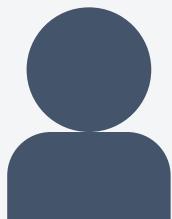
送信者



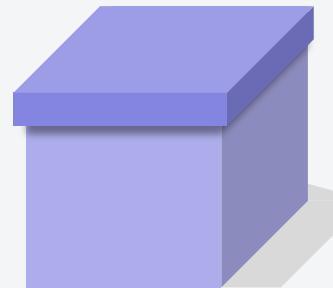
受信者

送っている途中で

この送り方の問題点



送信者



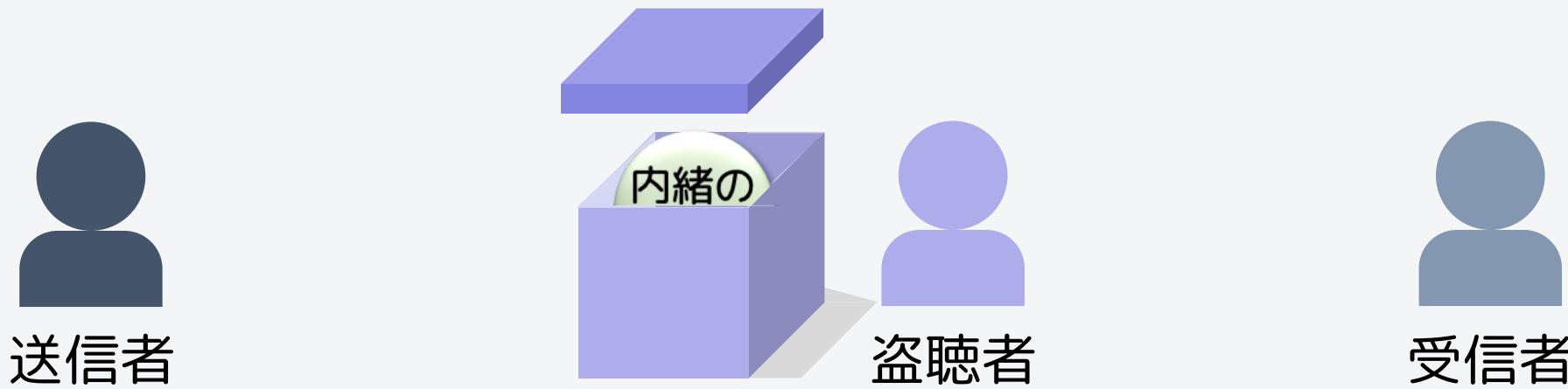
盗聴者



受信者

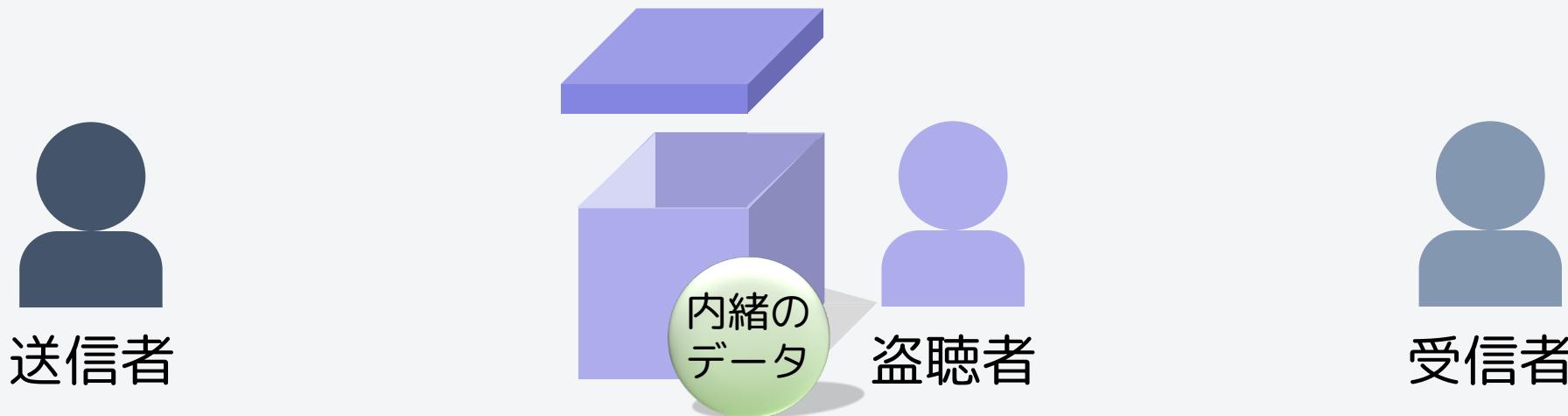
箱の中身(データ)を盗まれる可能性があります。

この送り方の問題点



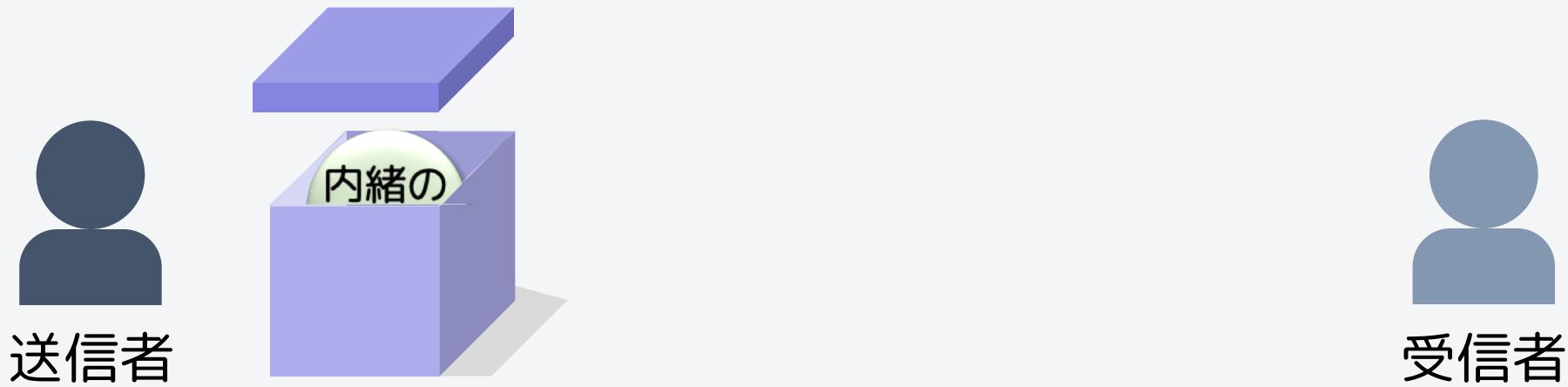
箱の中身(データ)を盗まれる可能性があります。

この送り方の問題点



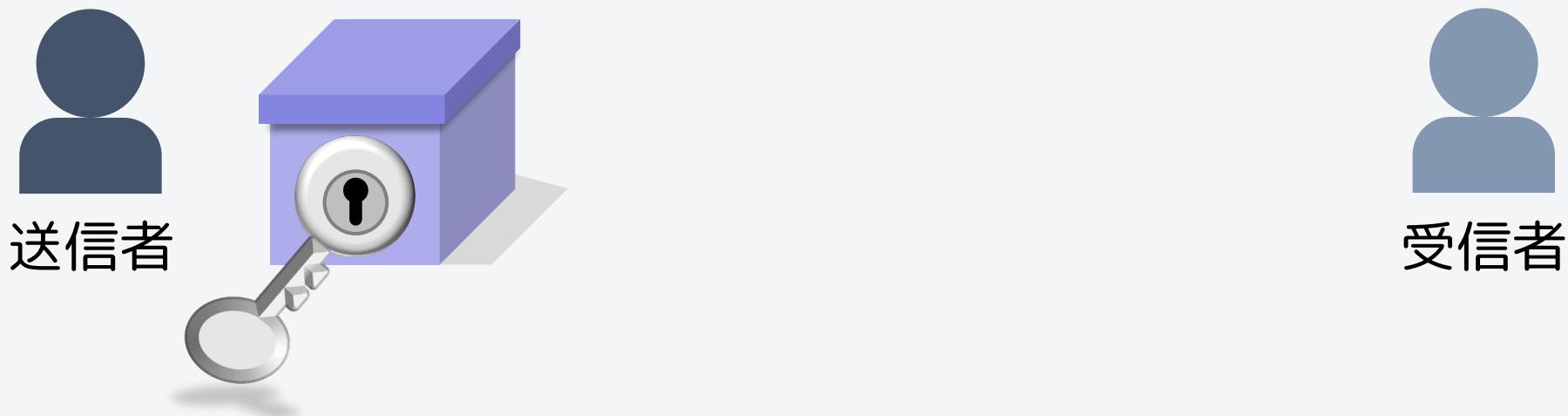
箱の中身(データ)を盗まれる可能性があります。

データが盗まれないようにするには…



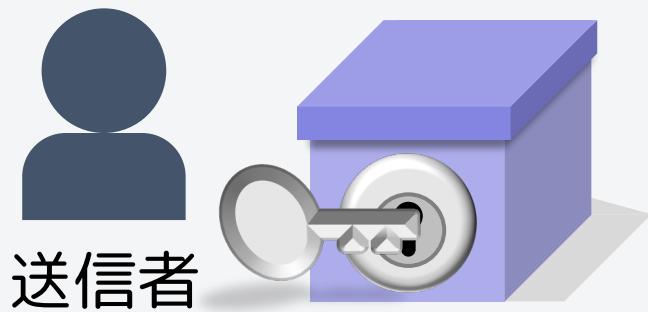
では、これを防ぐためにはどうすればいいでしょうか。

データが盗まれないようにするには…



それは、箱に鍵をかけることです。

データが盗まれないようにするには…



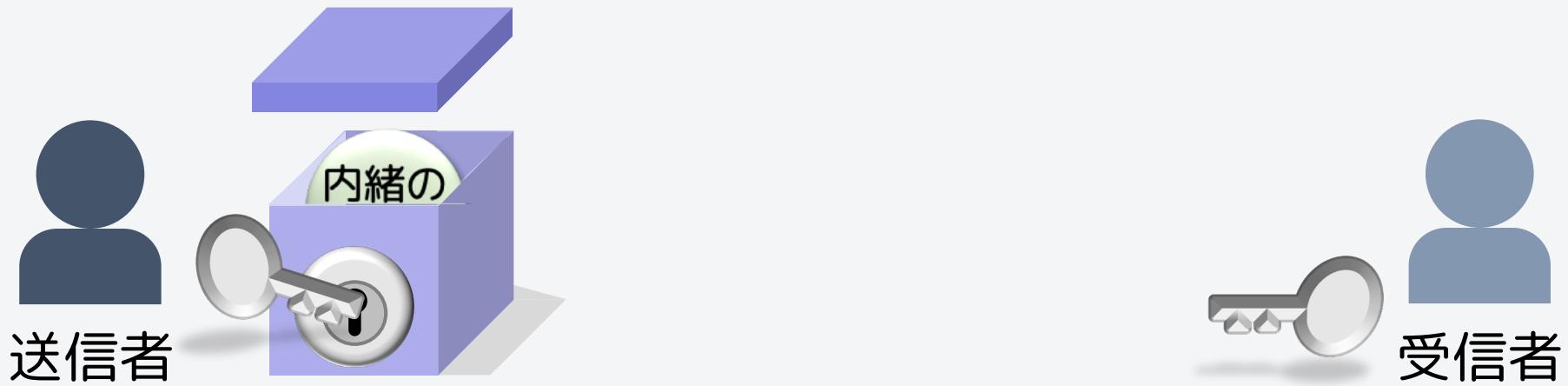
送信者



受信者

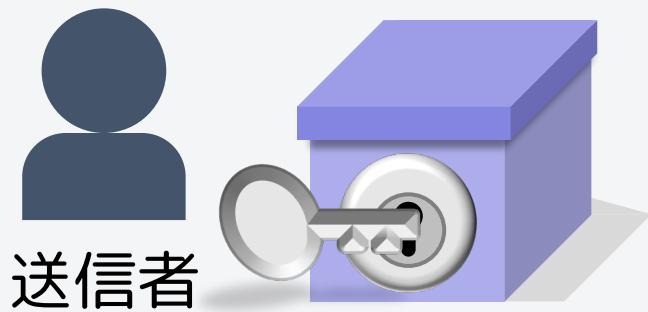
家の鍵のように、開閉可能な鍵を用意しておけば、

データが盗まれないようにするには…



家の鍵のように、開閉可能な鍵を用意しておけば、

データが盗まれないようにするには…



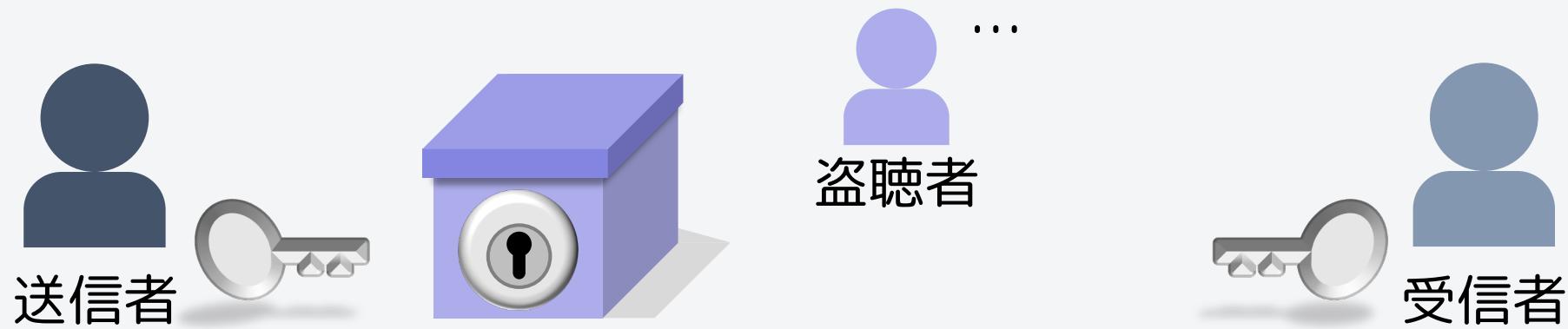
送信者



受信者

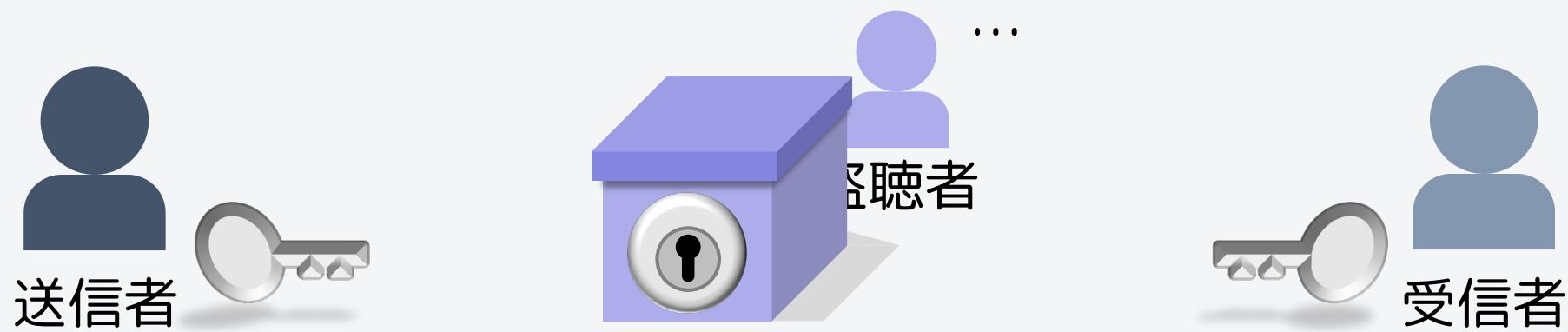
家の鍵のように、開閉可能な鍵を用意しておけば、

データが盗まれないようにするには…



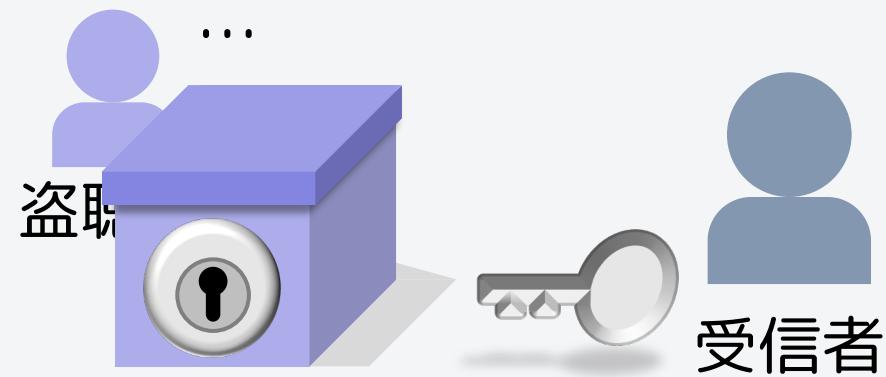
鍵を持っていない人は中を見ることができません。

データが盗まれないようにするには…



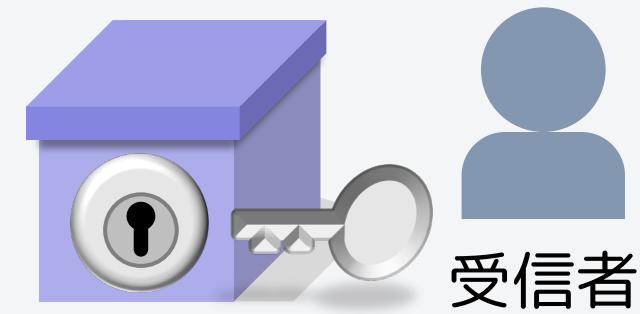
鍵を持っていない人は中を見ることができません。

データが盗まれないようにするには…



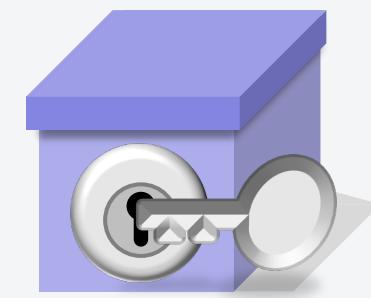
鍵を持っていない人は中を見ることができません。

データが盗まれないようにするには…



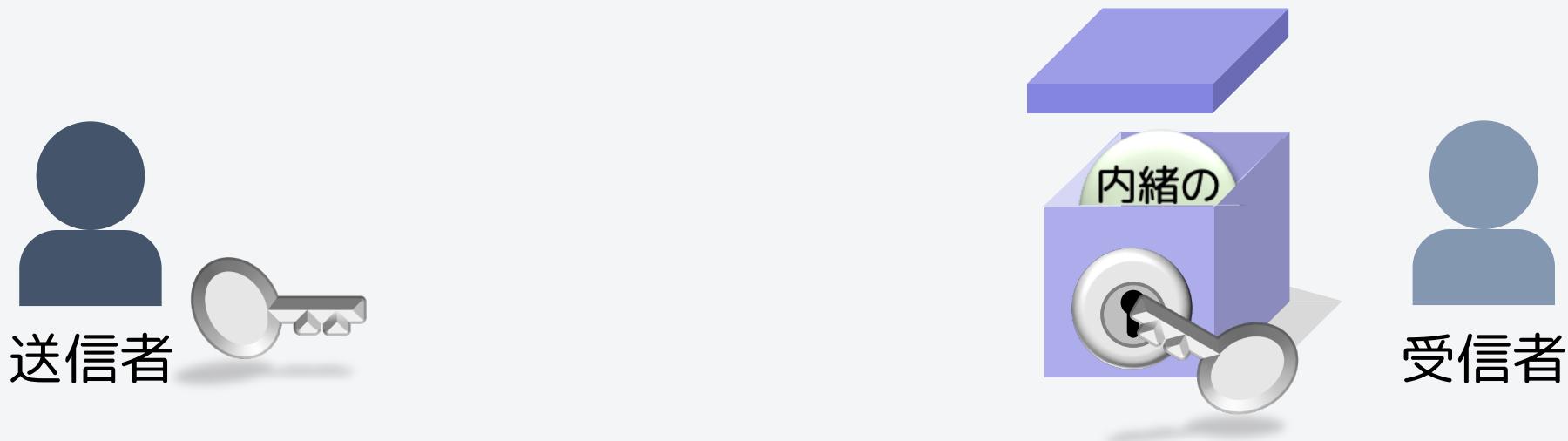
これで安全にデータを送ることができました。

データが盗まれないようにするには…



受信者は、送信者と同じ鍵を使って解錠します。

データが盗まれないようにするには…



受信者は、送信者と同じ鍵を使って解錠します。

データが盗まれないようにするには…



このとき、鍵をかけてデータを守ることを「暗号化」

データが盗まれないようにするには…



このとき、鍵をかけてデータを守ることを「暗号化」

データが盗まれないようにするには…



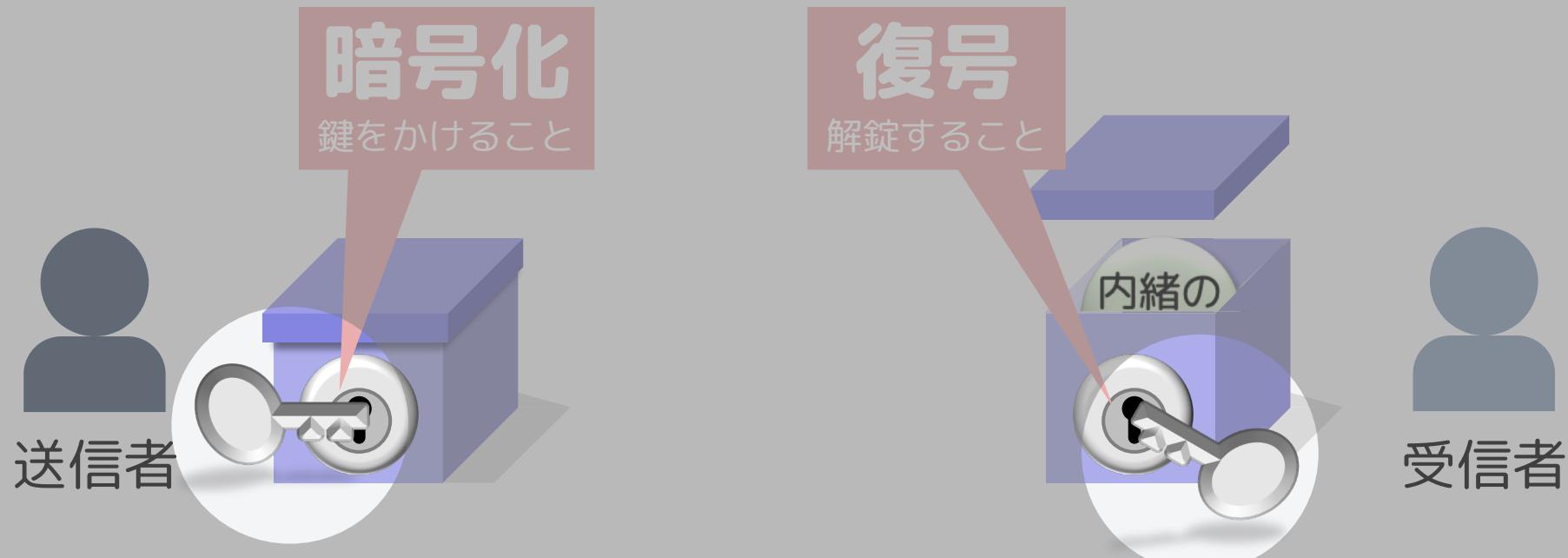
暗号化されたデータを元に戻すことを「復号」といいます。

データが盗まれないようにするには…



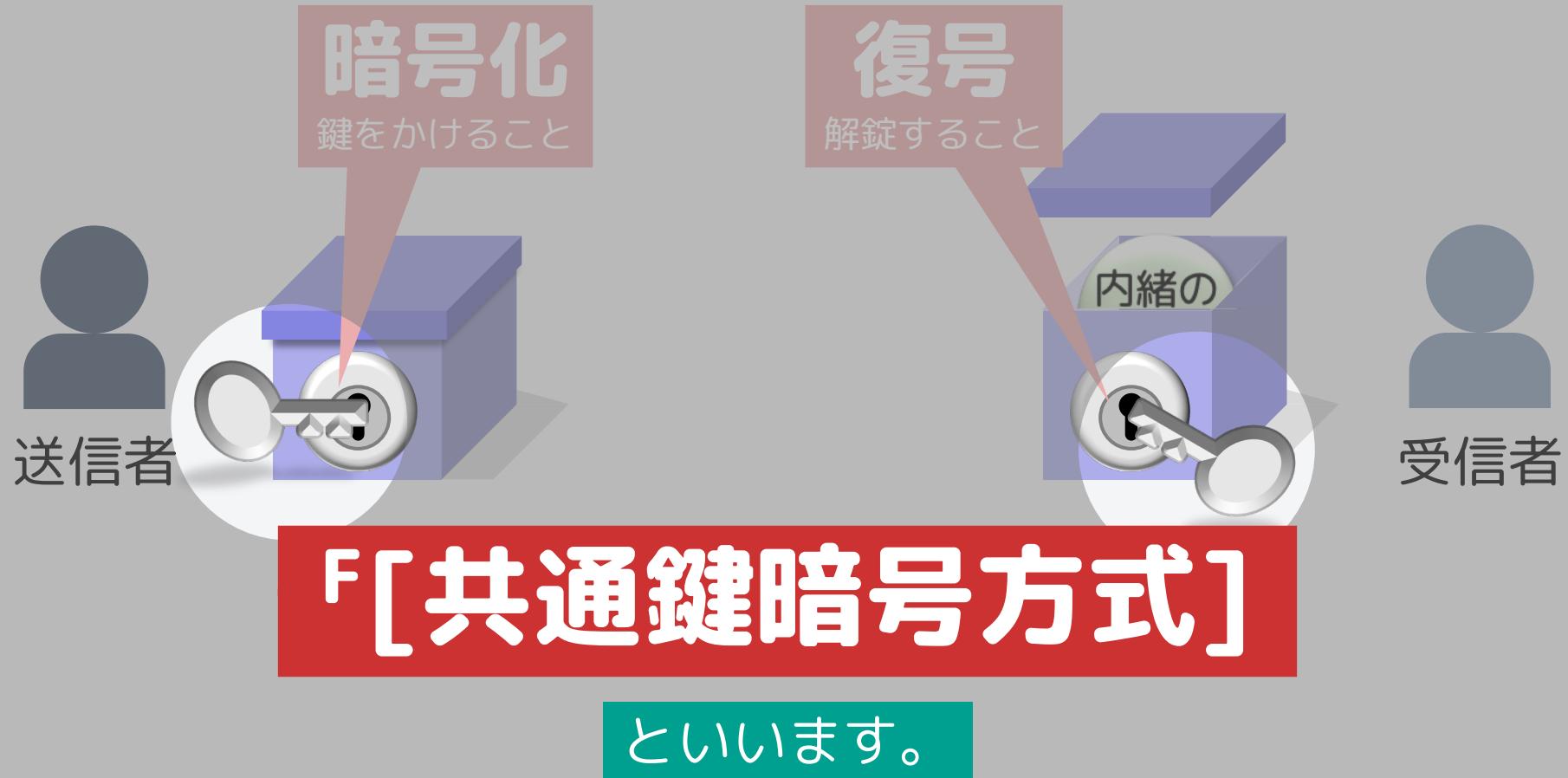
暗号化されたデータを元に戻すことを「復号」といいます。

データが盗まれないようにするには…

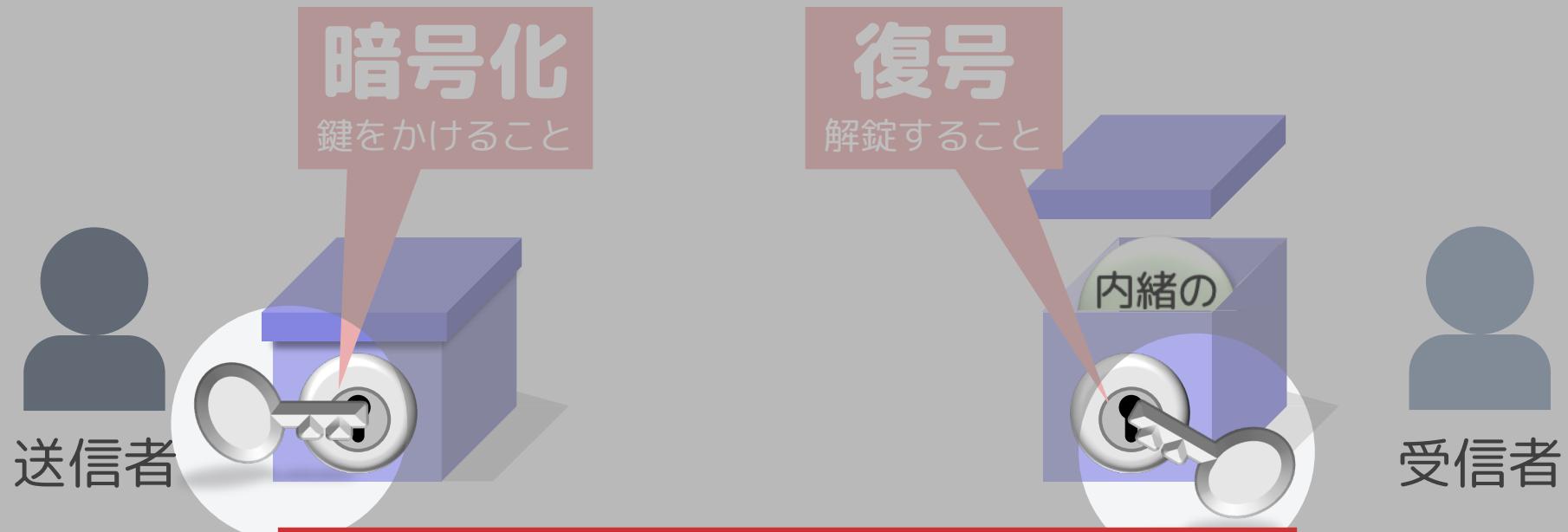


そして、暗号化と復号で同じ鍵を使う暗号方式を、

データが盗まれないようにするには…



データが盗まれないようにするには…

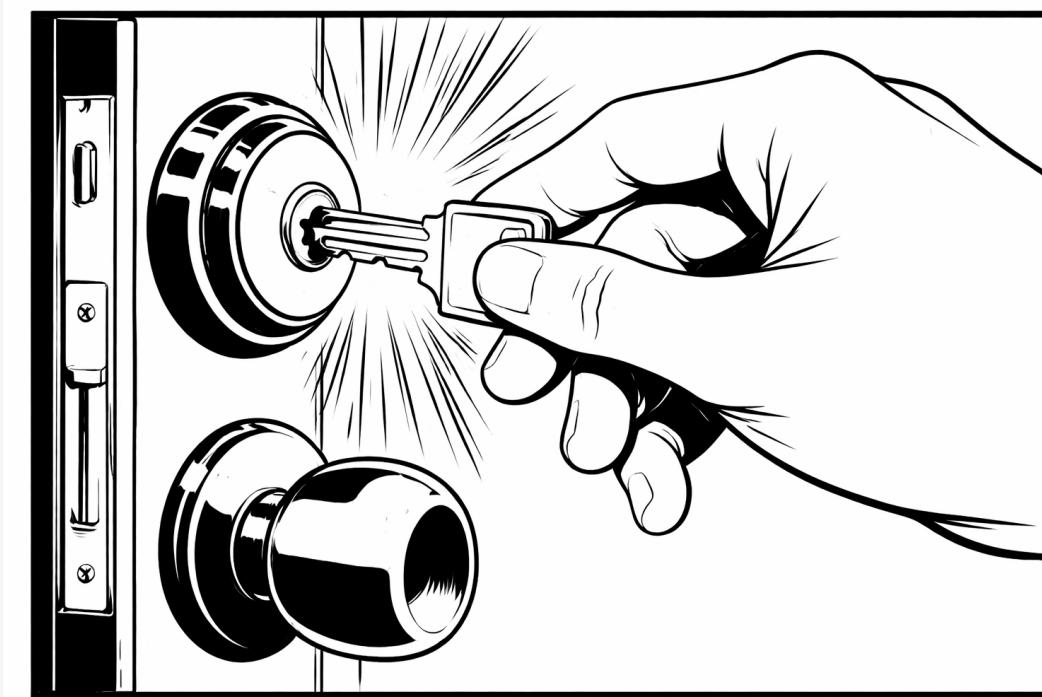


「**共通鍵暗号方式**」

といいます。

イメージは、「**家の鍵**」

共通鍵暗号方式 イメージは家の鍵

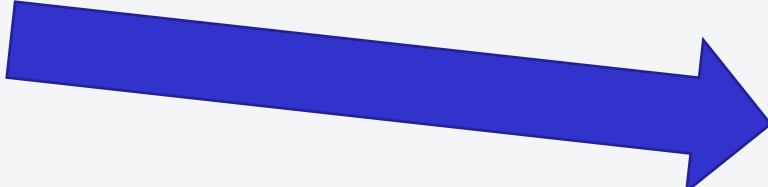
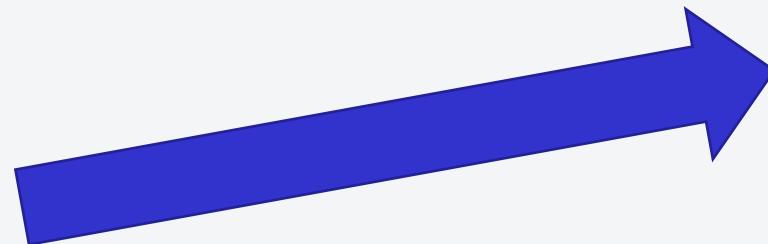


共通鍵暗号方式

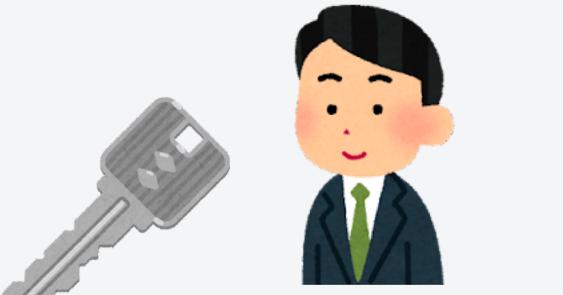
通信相手が増えると、管理する鍵が増える。



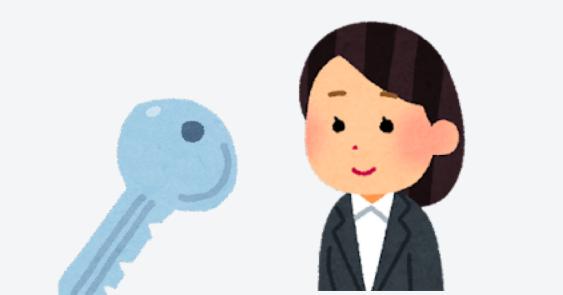
送信者



受信者Aさん



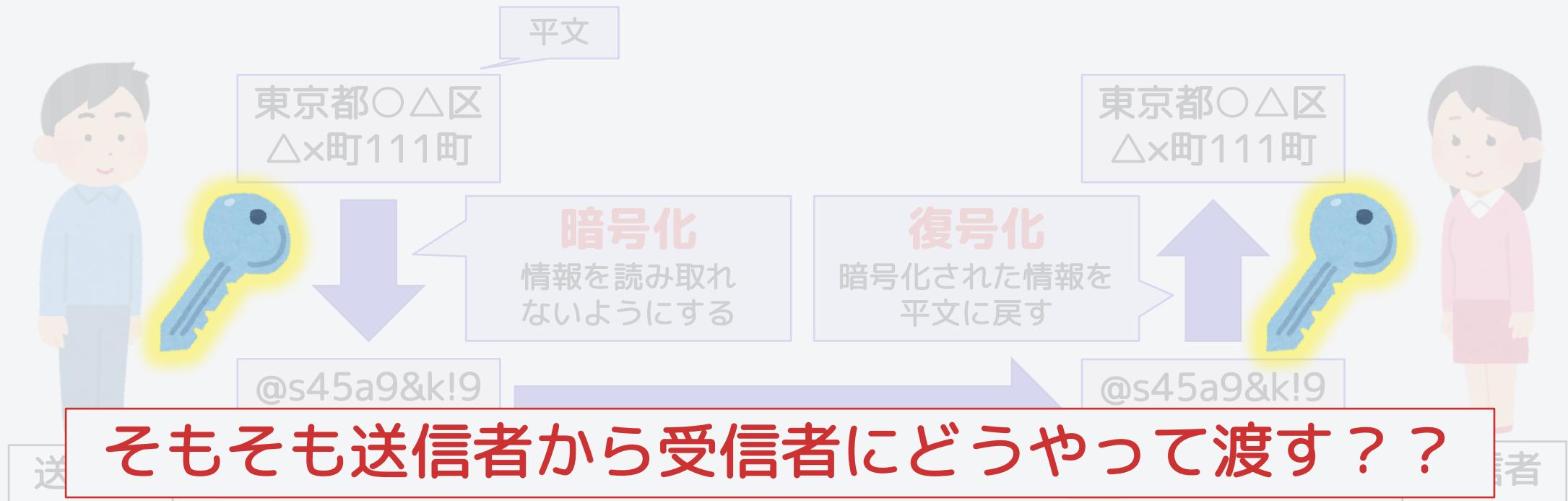
受信者Bさん



受信者Cさん

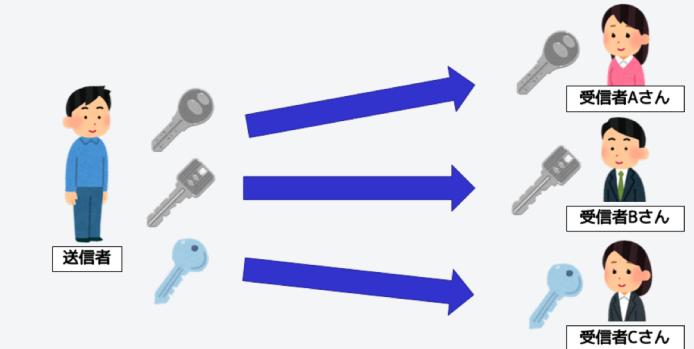
共通鍵暗号方式

暗号化と復号化で同じ鍵を使用する

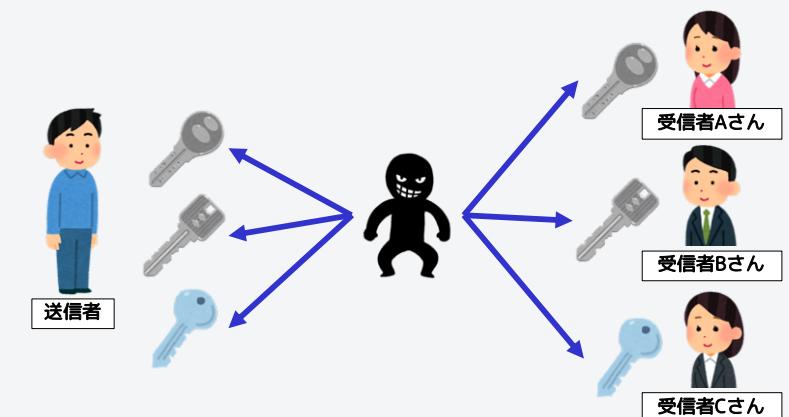


共通鍵暗号方式

- 通信相手が増えると管理する鍵が増える

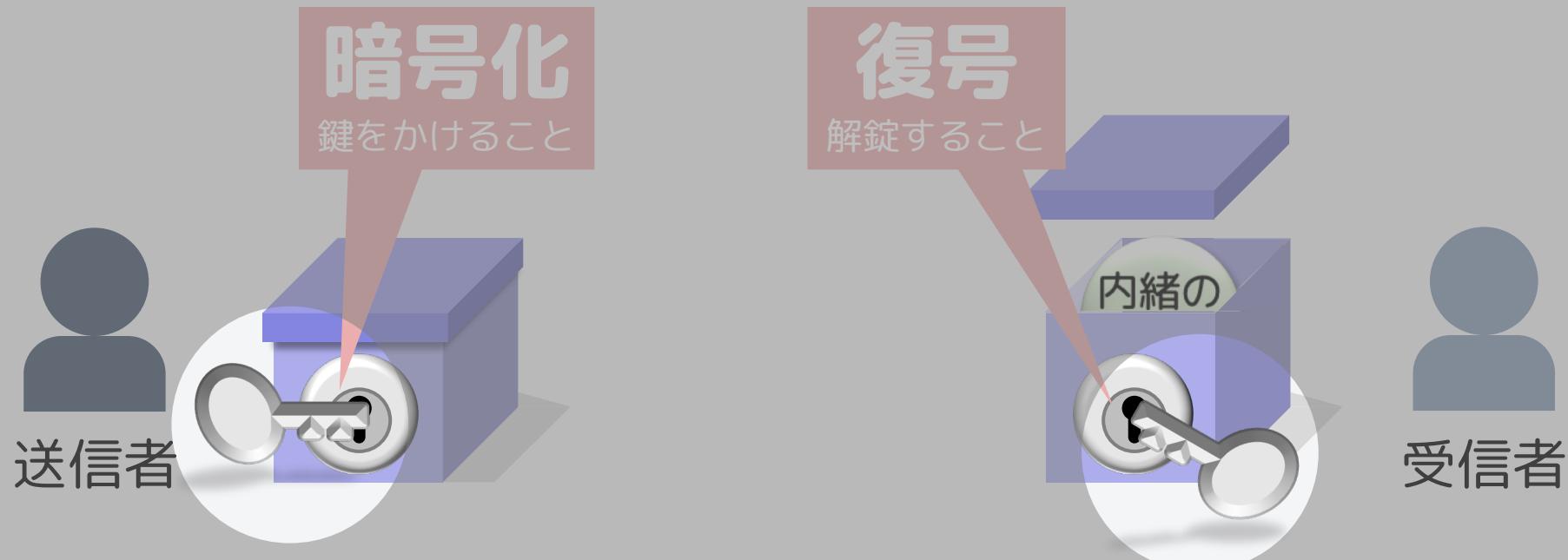


- 共通鍵を渡すときにもリスクがかかる



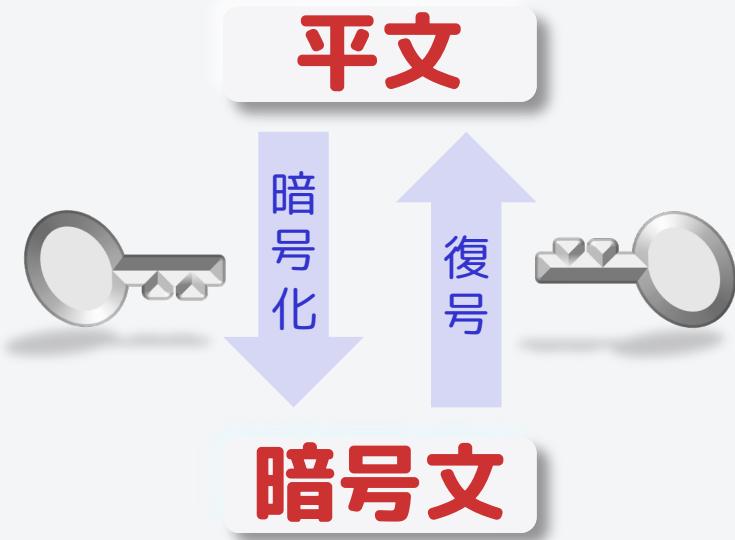
公開鍵暗号方式

データが盗まれないようにするには…



暗号方式には、もう一つ別のものがあります。

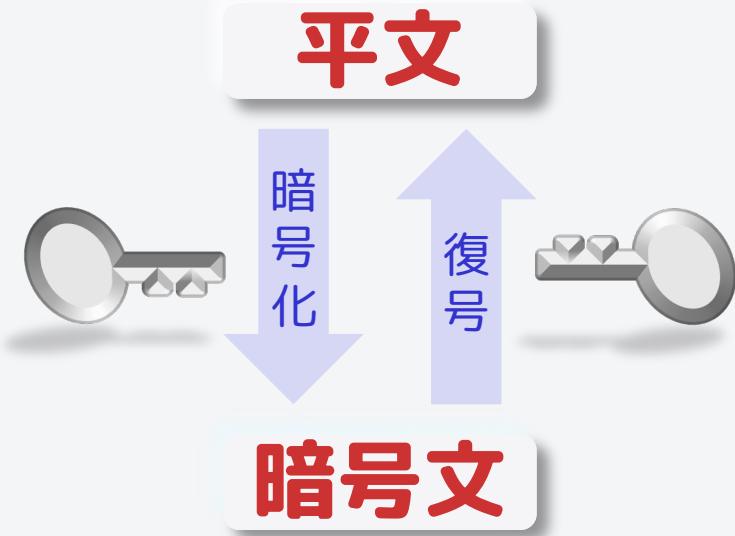
もう一つの暗号方式



共通鍵暗号方式

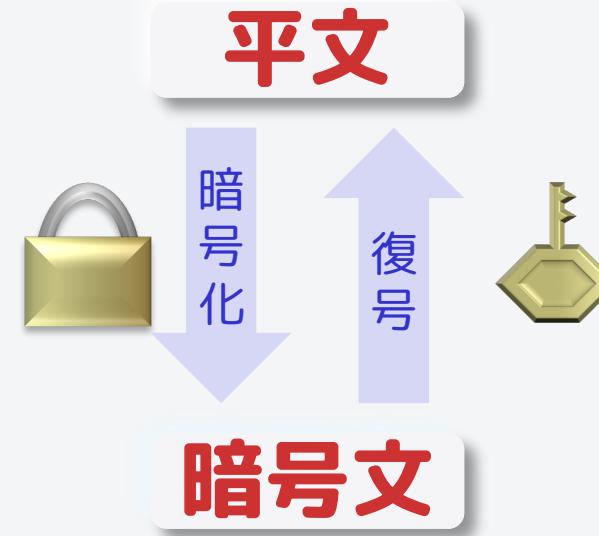
暗号化と復号で同じ鍵を使う

もう一つの暗号方式



共通鍵暗号方式

暗号化と復号で同じ鍵を使う



公開鍵暗号方式

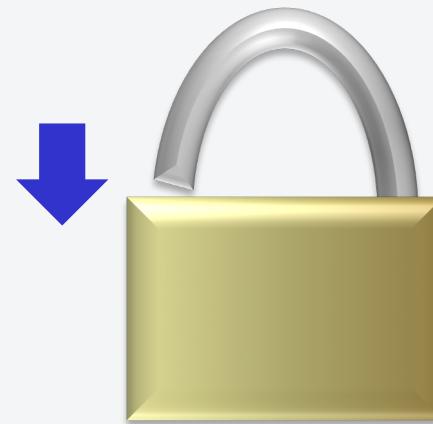
暗号化と復号で違う鍵を使う

もう一つの暗号方式は南京錠をイメージ



南京錠を想像してください。

もう一つの暗号方式は南京錠をイメージ



南京錠は、U字型の金属の部分を手で押すだけで

もう一つの暗号方式は南京錠をイメージ



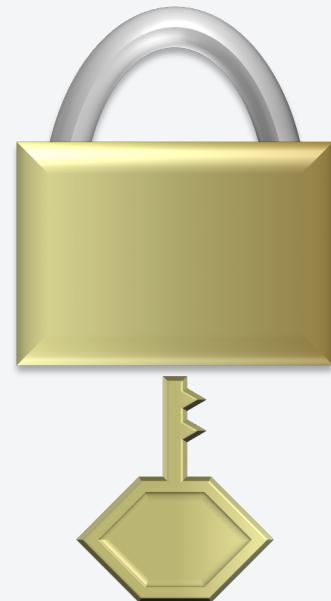
鍵をかけることができます。

もう一つの暗号方式は南京錠をイメージ



鍵を開けるためには、底面の穴に鍵を差し込み

もう一つの暗号方式は南京錠をイメージ



鍵を開けるためには、底面の穴に鍵を差し込み

もう一つの暗号方式は南京錠をイメージ



鍵を開けるためには、底面の穴に鍵を差し込み

もう一つの暗号方式は南京錠をイメージ



ひねることで鍵を開けることができます。

もう一つの暗号方式は南京錠をイメージ



ひねることで鍵を開けることができます。

もう一つの暗号方式は南京錠をイメージ



ひねることで鍵を開けることができます。

もう一つの暗号方式は南京錠をイメージ



ひねることで鍵を開けることができます。

もう一つの暗号方式は南京錠をイメージ



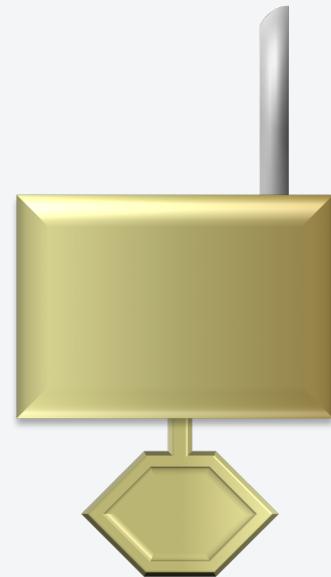
ひねることで鍵を開けることができます。

もう一つの暗号方式は南京錠をイメージ



ひねることで鍵を開けることができます。

もう一つの暗号方式は南京錠をイメージ



ひねることで鍵を開けることができます。

もう一つの暗号方式は南京錠をイメージ



ひねることで鍵を開けることができます。

もう一つの暗号方式は南京錠をイメージ



ひねることで鍵を開けることができます。

南京錠を使った安全な物の渡し方を考えよう

公開鍵



秘密鍵

1 ア は イ に ウ を送る



送信者



受信者

2 イ は、ア の ウ を使って
鍵をかける(=暗号化)



3 その状態でデータを送信する



4 ア は、ア の エ を使って
鍵を開ける(=復号)



南京錠を使った安全な物の渡し方を考えよう

公開鍵



秘密鍵

1 ア は イ に ウ を送る



送信者



受信者

2 イ は、ア の ウ を使って
鍵をかける(=暗号化)



3 その状態でデータを送信する



4 ア は、ア の エ を使って
鍵を開ける(=復号)



南京錠を使った安全な物の渡し方を考えよう

公開鍵
鍵をかける



秘密鍵
鍵を開ける



1 ア は イ に ウ を送る



送信者

2 イ は、ア の ウ を使って
鍵をかける(=暗号化)



3 その状態でデータを送信する



4 ア は、ア の エ を使って
鍵を開ける(=復号)



南京錠を使った安全な物の渡し方を考えよう

公開鍵
鍵をかける



秘密鍵
鍵を開ける



受信者

1 ア は イ に ウ 公開鍵 を送る



送信者

2 イ は、 ア の ウ 公開鍵 を使って
鍵をかける(=暗号化)



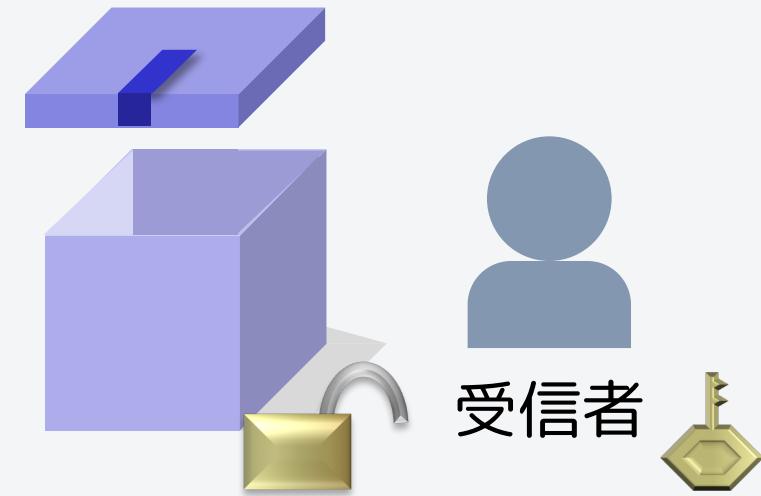
3 その状態でデータを送信する



4 ア は、 ア の エ 秘密鍵 を使って
鍵を開ける(=復号)

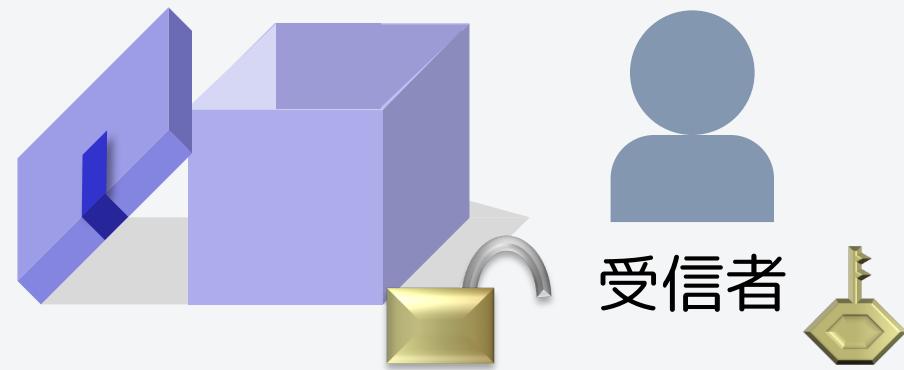


南京錠を使った暗号方式



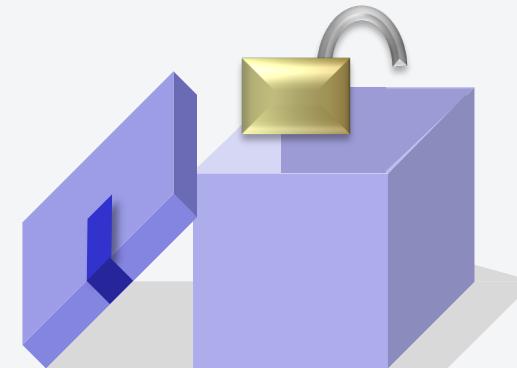
では、南京錠を使ったデータの送り方を説明します。

南京錠を使った暗号方式



まず、受信者が送信者に開いた状態の南京錠を送ります。

南京錠を使った暗号方式

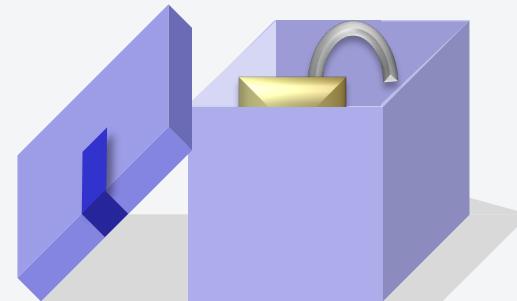


まず、受信者が送信者に開いた状態の南京錠を送ります。

南京錠を使った暗号方式



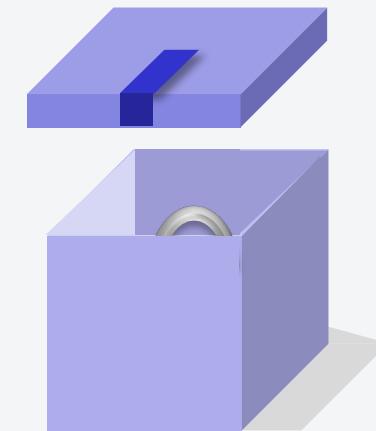
送信者



受信者

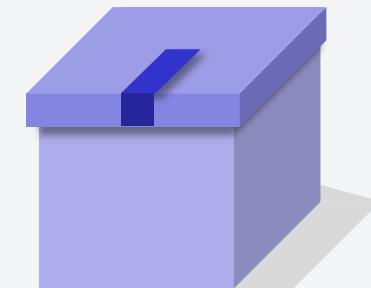
まず、受信者が送信者に開いた状態の南京錠を送ります。

南京錠を使った暗号方式



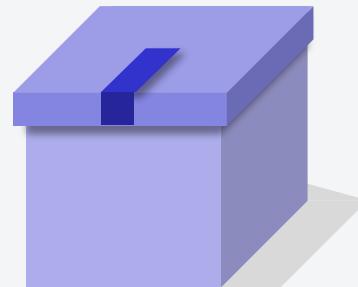
まず、受信者が送信者に開いた状態の南京錠を送ります。

南京錠を使った暗号方式



まず、受信者が送信者に開いた状態の南京錠を送ります。

南京錠を使った暗号方式



まず、受信者が送信者に開いた状態の南京錠を送ります。

南京錠を使った暗号方式



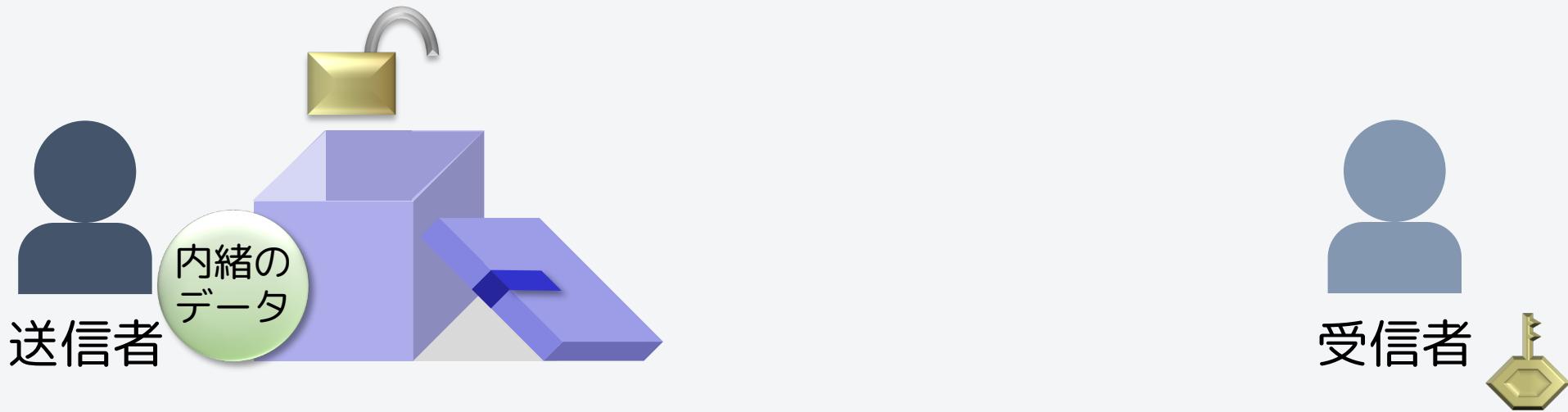
まず、受信者が送信者に開いた状態の南京錠を送ります。

南京錠を使った暗号方式



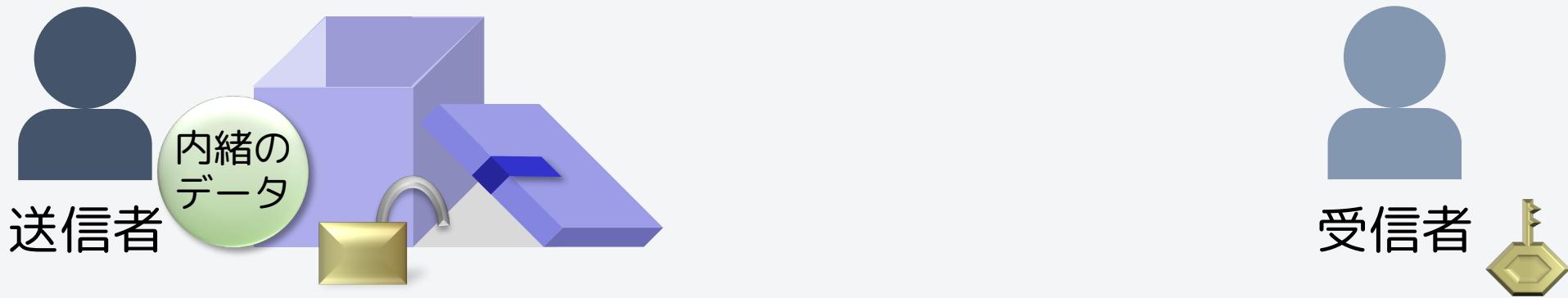
送信者は箱の中にある南京錠を取り出し、

南京錠を使った暗号方式



送信者は箱の中にある南京錠を取り出し、

南京錠を使った暗号方式

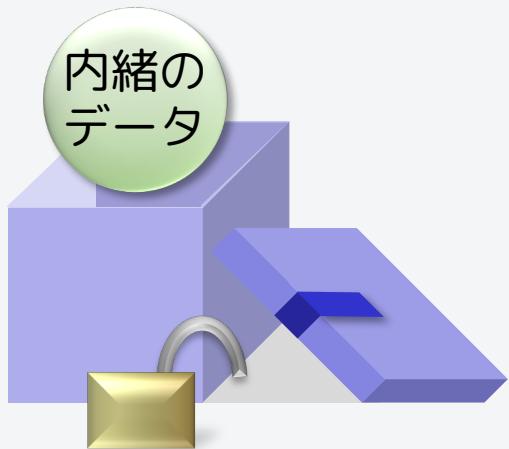


送信者は箱の中にある南京錠を取り出し、

南京錠を使った暗号方式



送信者



受信者



箱の中にデータを入れます。

南京錠を使った暗号方式



送信者

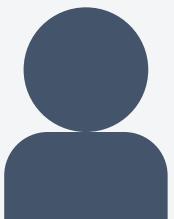


受信者

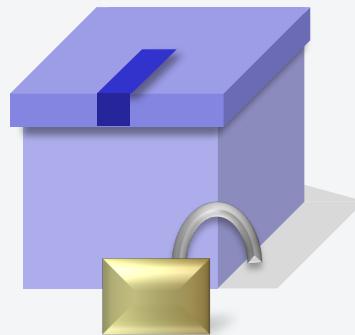


箱の中にデータを入れます。

南京錠を使った暗号方式



送信者



受信者

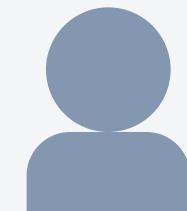
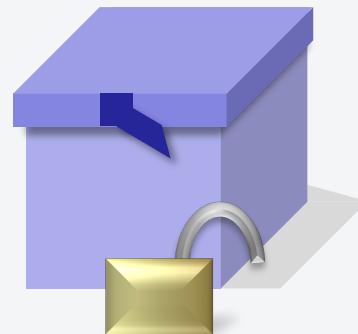


箱の中にデータを入れます。

南京錠を使った暗号方式



送信者



受信者

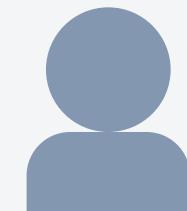
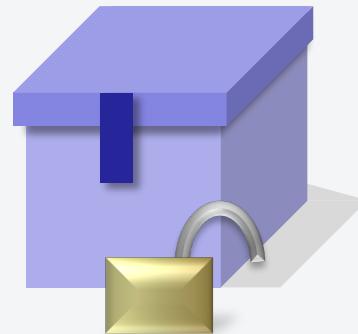


データを入れたら、受け取った南京錠で鍵をかけます。

南京錠を使った暗号方式



送信者

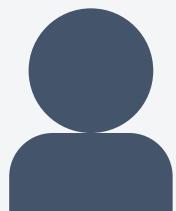


受信者

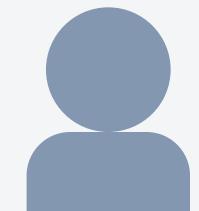
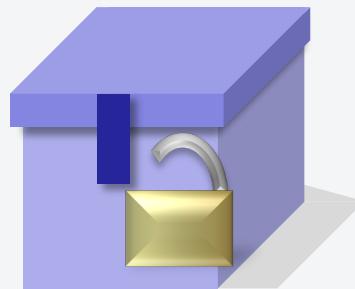


データを入れたら、受け取った南京錠で鍵をかけます。

南京錠を使った暗号方式



送信者

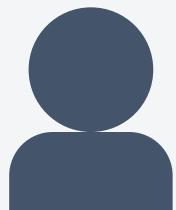


受信者

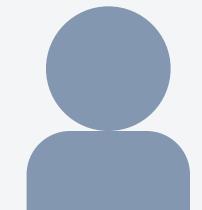
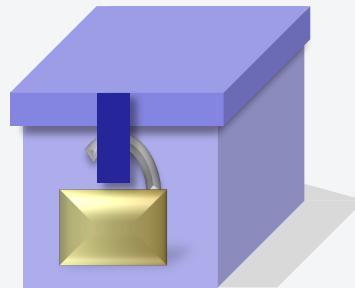


データを入れたら、受け取った南京錠で鍵をかけます。

南京錠を使った暗号方式



送信者

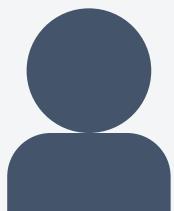


受信者

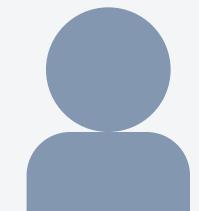
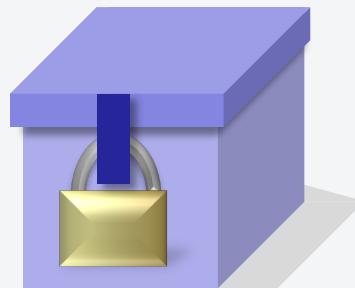


データを入れたら、受け取った南京錠で鍵をかけます。

南京錠を使った暗号方式



送信者

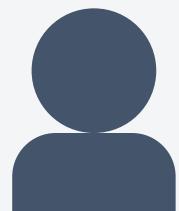


受信者

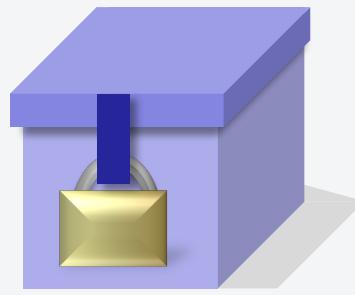


データを入れたら、受け取った南京錠で鍵をかけます。

南京錠を使った暗号方式



送信者



受信者

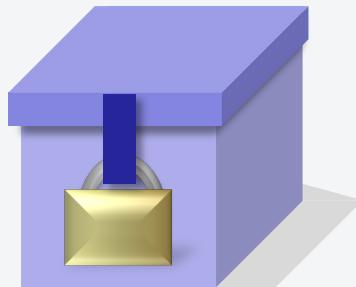


手で押すだけで、鍵をかけることができます。

南京錠を使った暗号方式



送信者



盗聴者



受信者

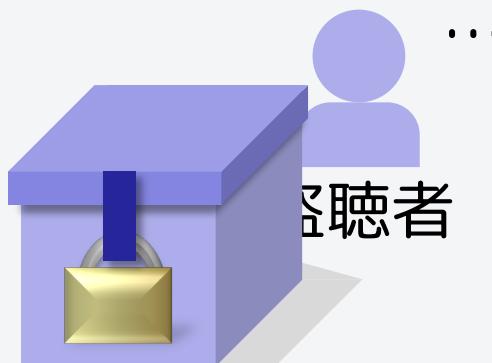


もちろん、鍵を持っていない人は中を見ることができません。

南京錠を使った暗号方式



送信者

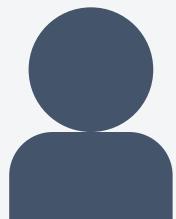


受信者



もちろん、鍵を持っていない人は中を見ることができません。

南京錠を使った暗号方式



送信者

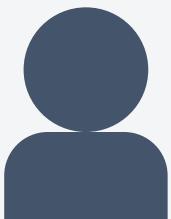


受信者

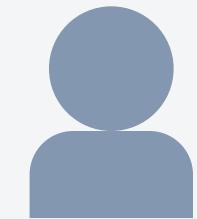
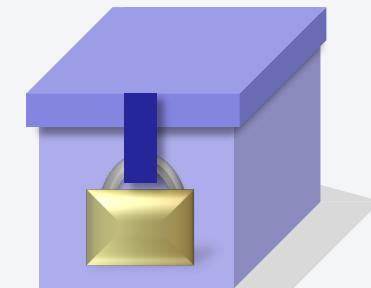


もちろん、鍵を持っていない人は中を見ることができません。

南京錠を使った暗号方式



送信者

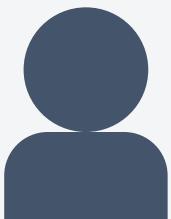


受信者

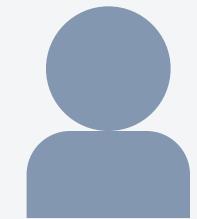
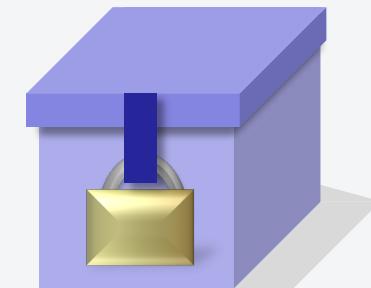


これで安全にデータを送ることができました。

南京錠を使った暗号方式



送信者

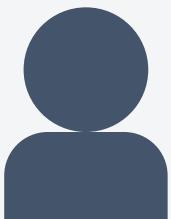


受信者

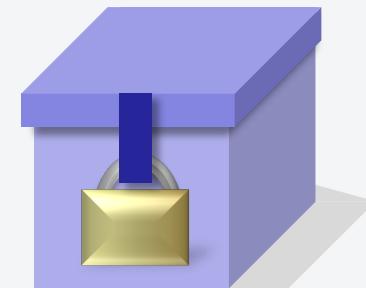


受信者は、持っている鍵を使って錠を開けます。

南京錠を使った暗号方式



送信者

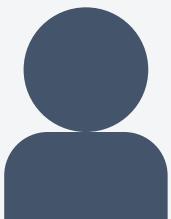


受信者



受信者は、持っている鍵を使って錠を開けます。

南京錠を使った暗号方式



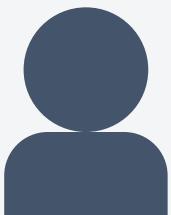
送信者



受信者

受信者は、持っている鍵を使って錠を開けます。

南京錠を使った暗号方式



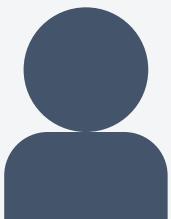
送信者



受信者

受信者は、持っている鍵を使って錠を開けます。

南京錠を使った暗号方式



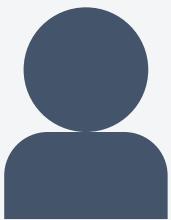
送信者



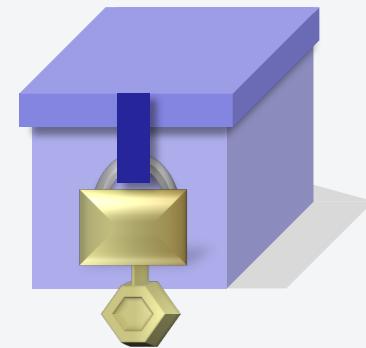
受信者

受信者は、持っている鍵を使って錠を開けます。

南京錠を使った暗号方式



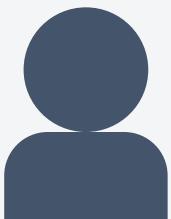
送信者



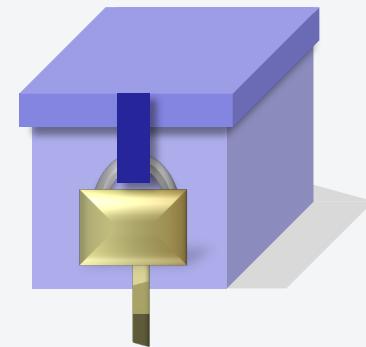
受信者

受信者は、持っている鍵を使って錠を開けます。

南京錠を使った暗号方式



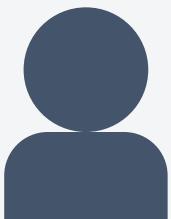
送信者



受信者

受信者は、持っている鍵を使って錠を開けます。

南京錠を使った暗号方式



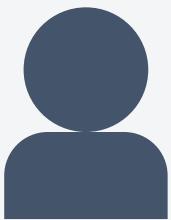
送信者



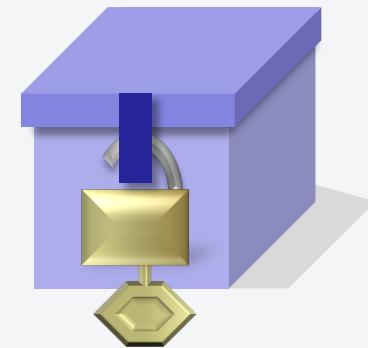
受信者

受信者は、持っている鍵を使って錠を開けます。

南京錠を使った暗号方式



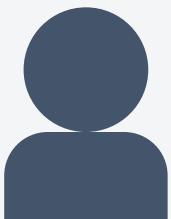
送信者



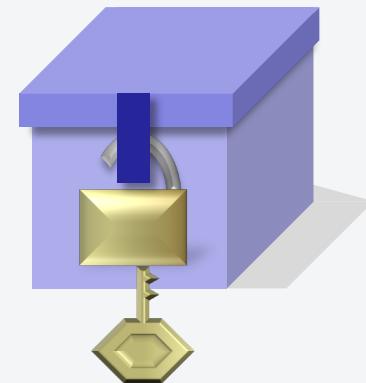
受信者

受信者は、持っている鍵を使って錠を開けます。

南京錠を使った暗号方式



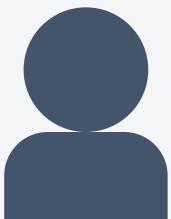
送信者



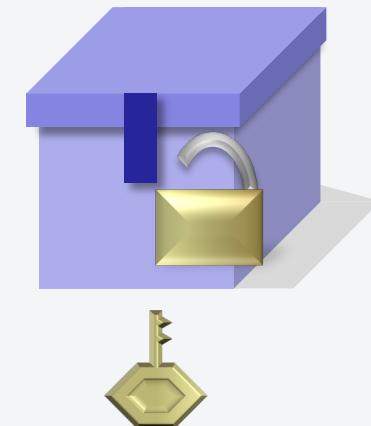
受信者

受信者は、持っている鍵を使って錠を開けます。

南京錠を使った暗号方式



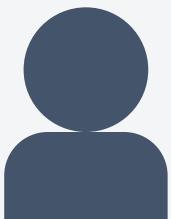
送信者



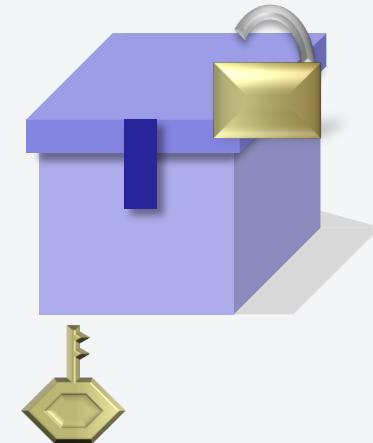
受信者

受信者は、持っている鍵を使って錠を開けます。

南京錠を使った暗号方式



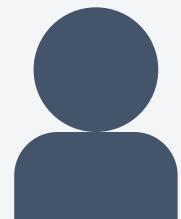
送信者



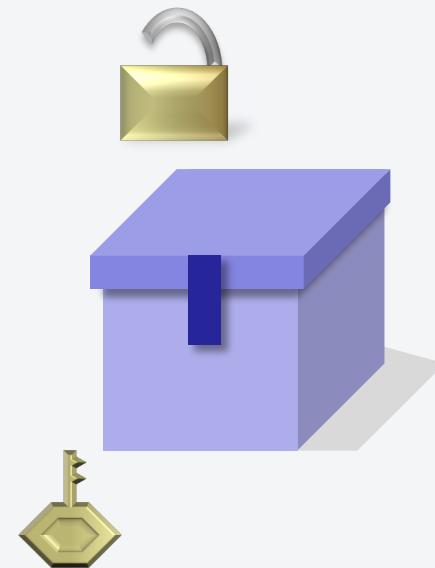
受信者

受信者は、持っている鍵を使って錠を開けます。

南京錠を使った暗号方式



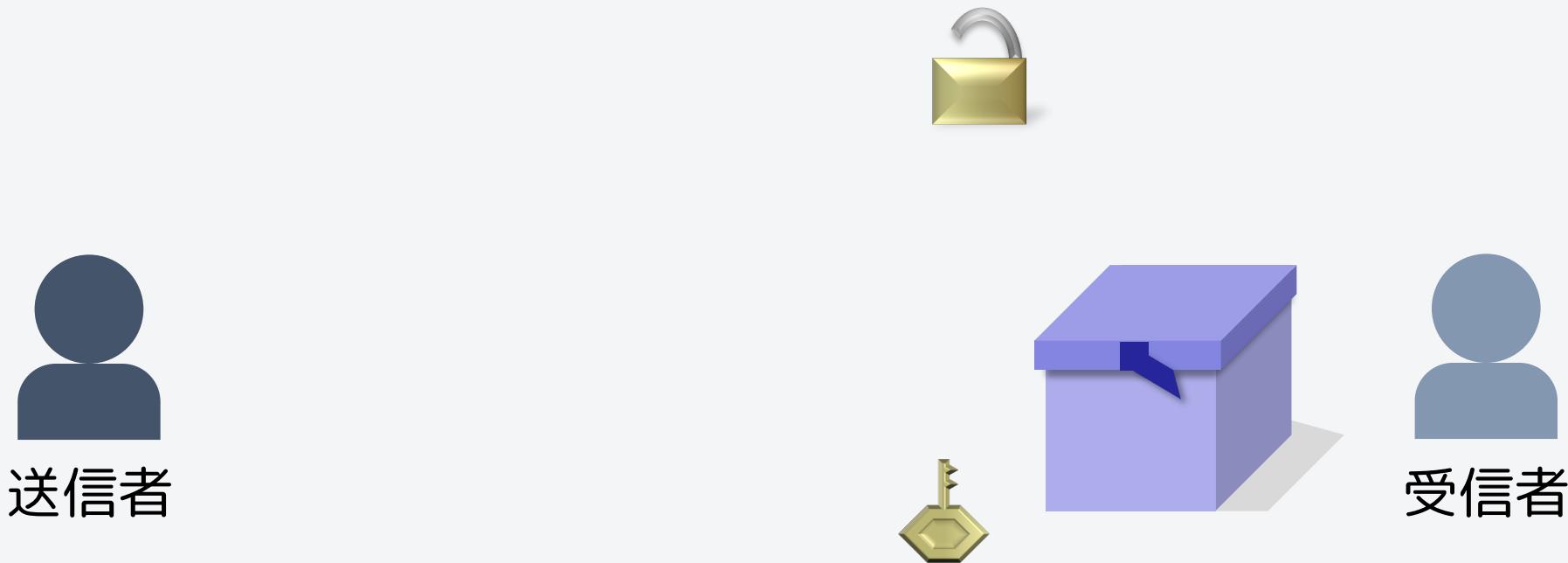
送信者



受信者

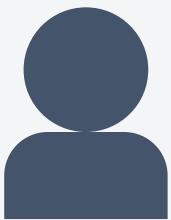
受信者は、持っている鍵を使って錠を開けます。

南京錠を使った暗号方式

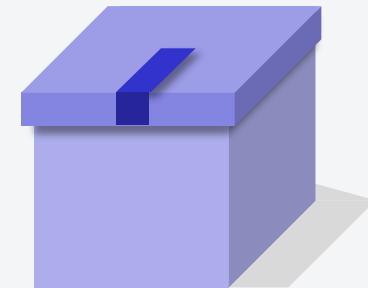


受信者は、持っている鍵を使って錠を開けます。

南京錠を使った暗号方式



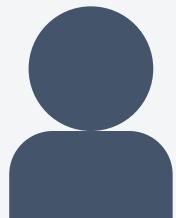
送信者



受信者

受信者は、持っている鍵を使って錠を開けます。

南京錠を使った暗号方式



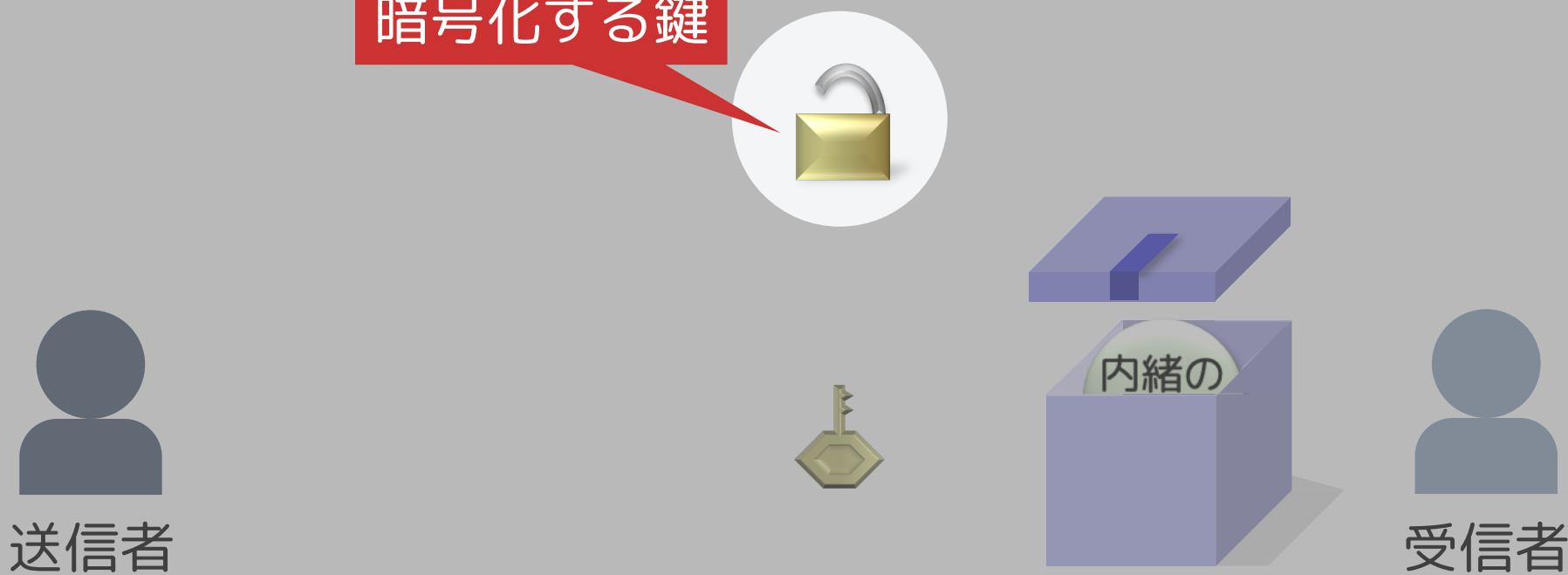
送信者



受信者

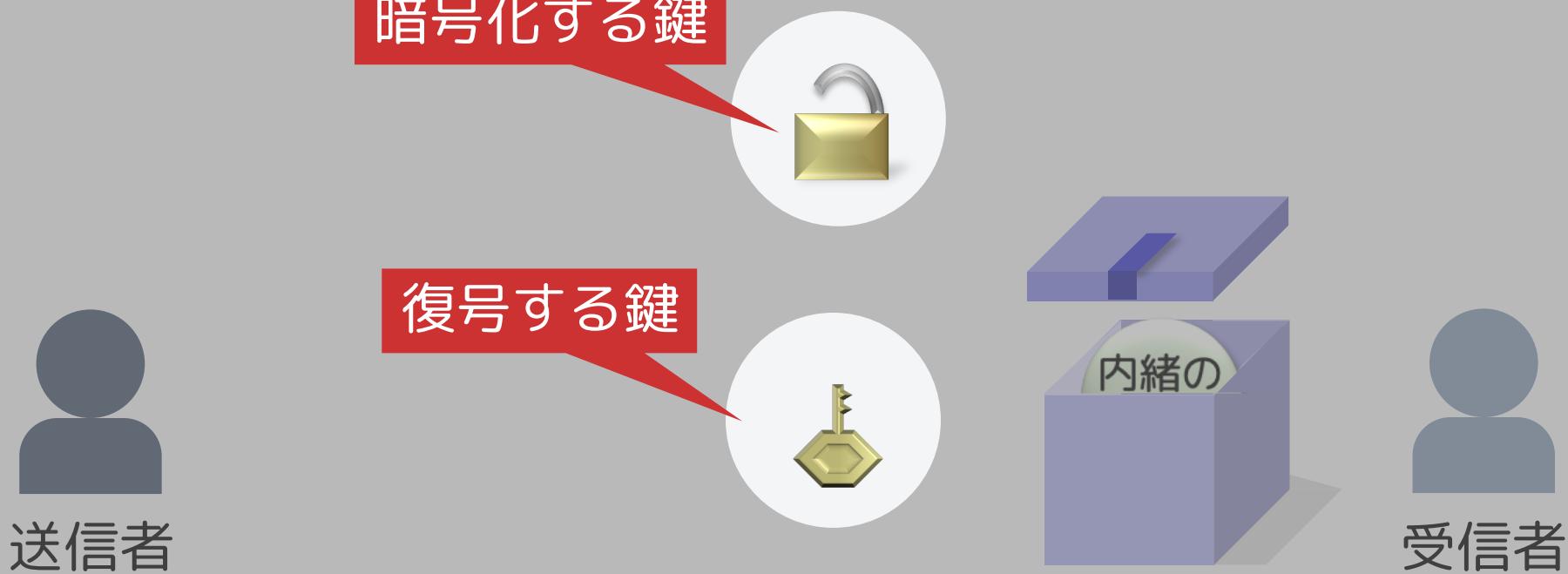
受信者は、持っている鍵を使って錠を開けます。

南京錠を使った暗号方式



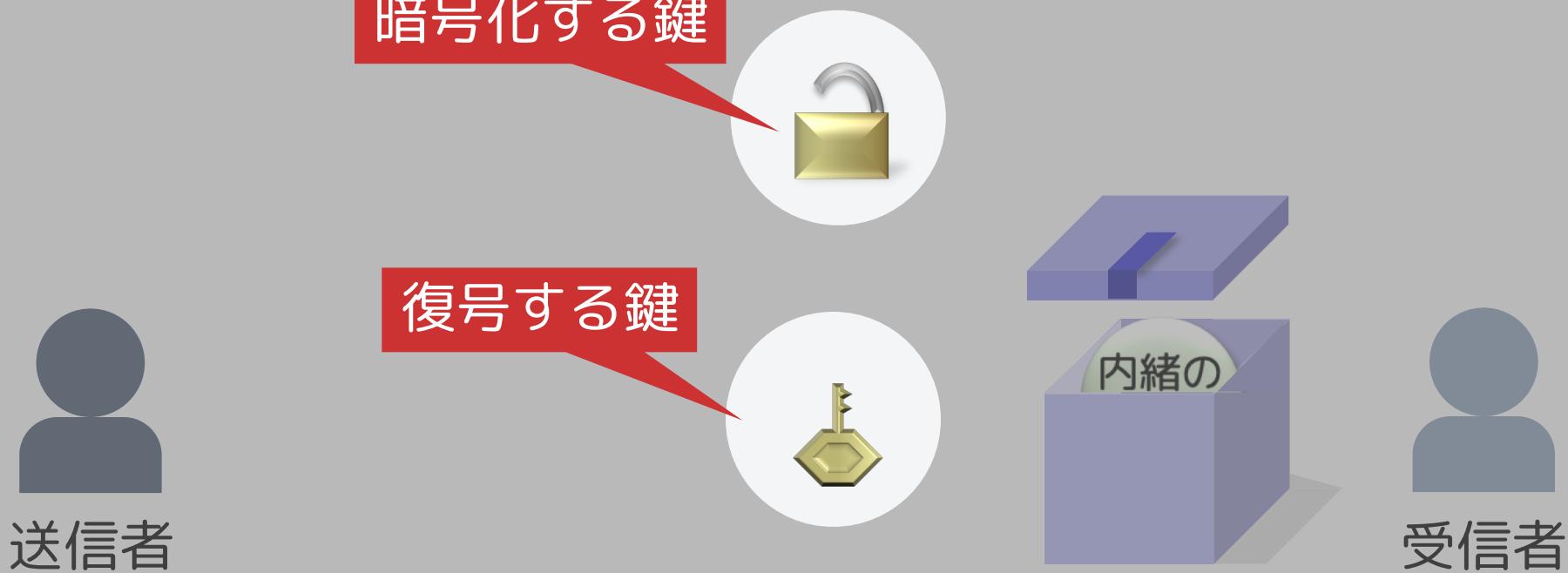
このとき、暗号化と復号で違う鍵を使う暗号方式を、

南京錠を使った暗号方式



このとき、暗号化と復号で違う鍵を使う暗号方式を、

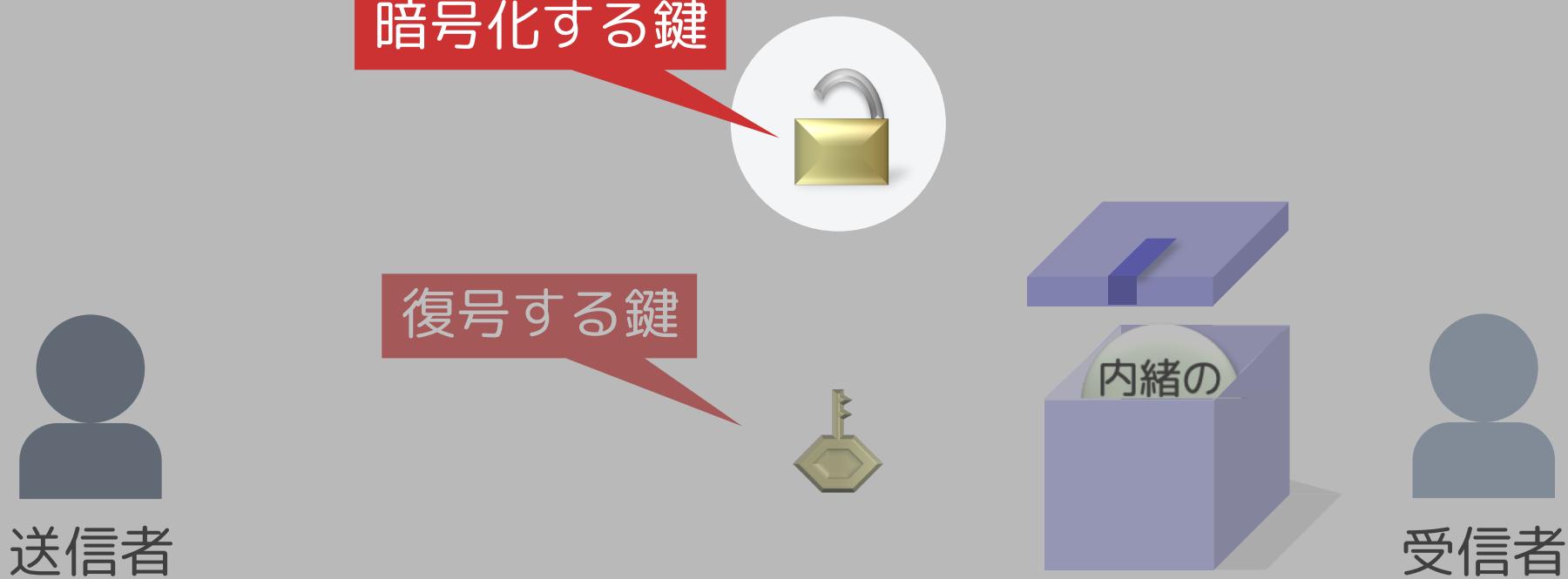
南京錠を使った暗号方式



公開鍵暗号方式

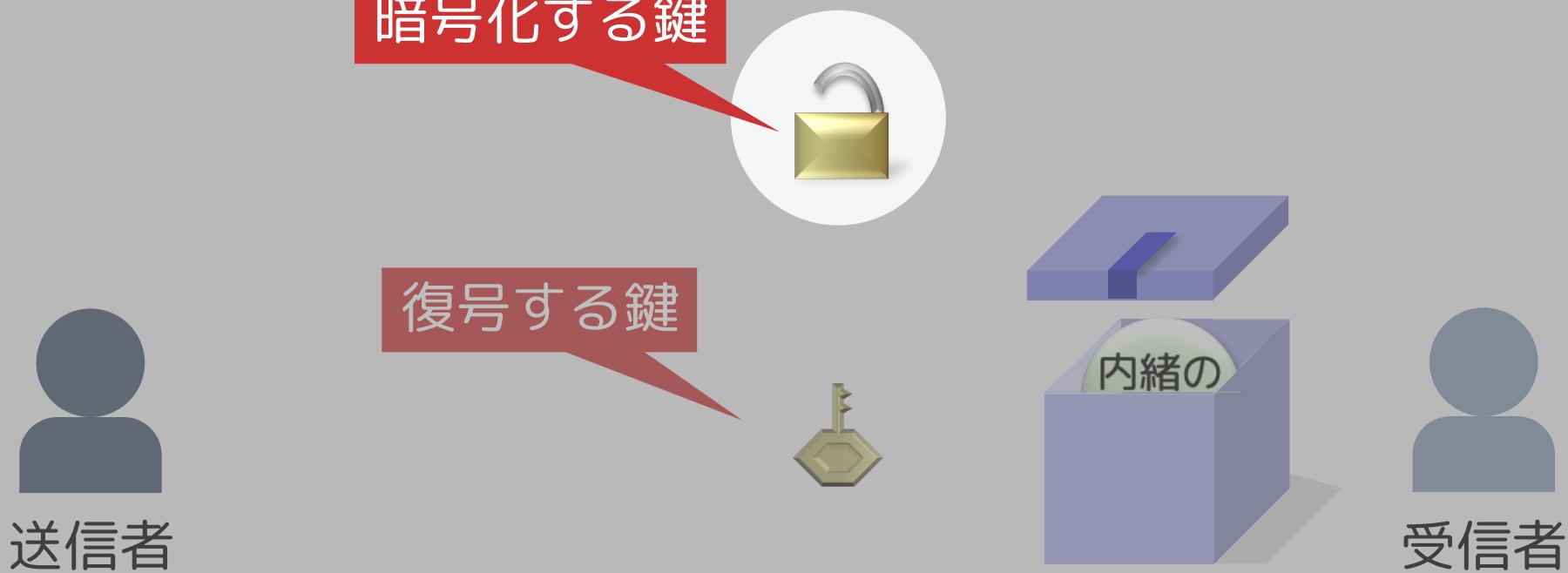
といいます。

公開鍵暗号方式で用いる鍵



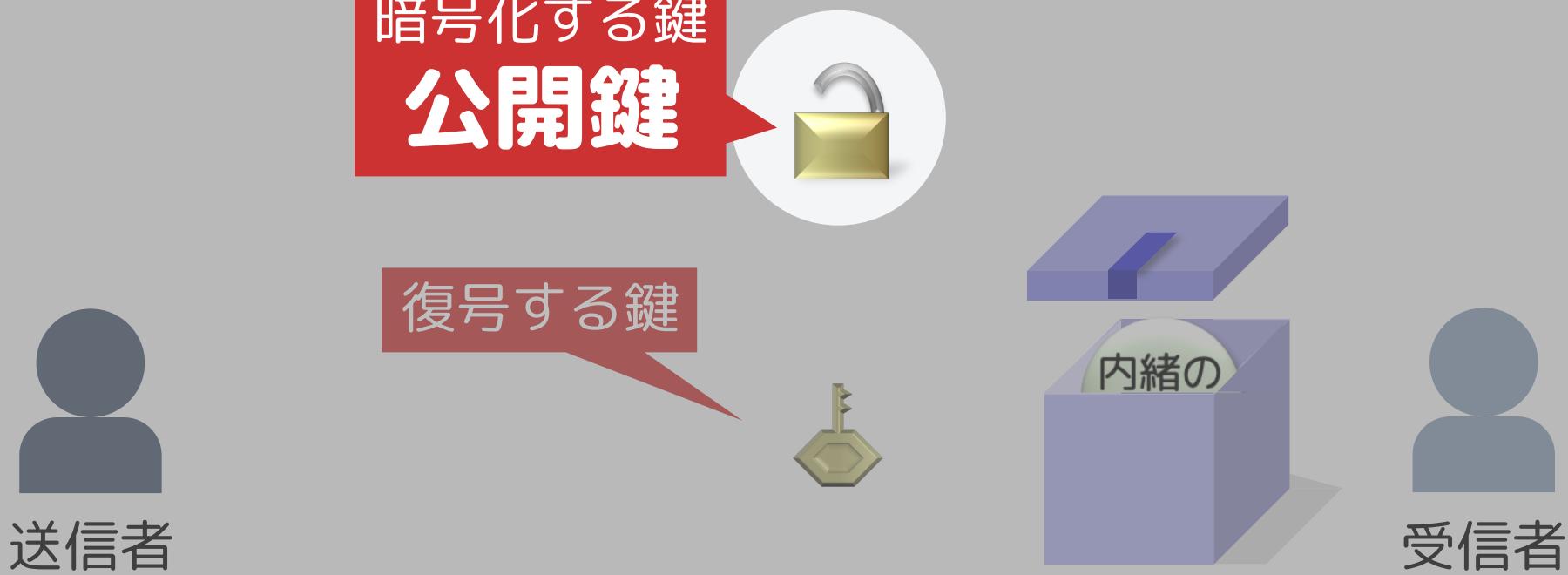
暗号化する鍵は、暗号化する(=鍵をかける)ことしかないので

公開鍵暗号方式で用いる鍵



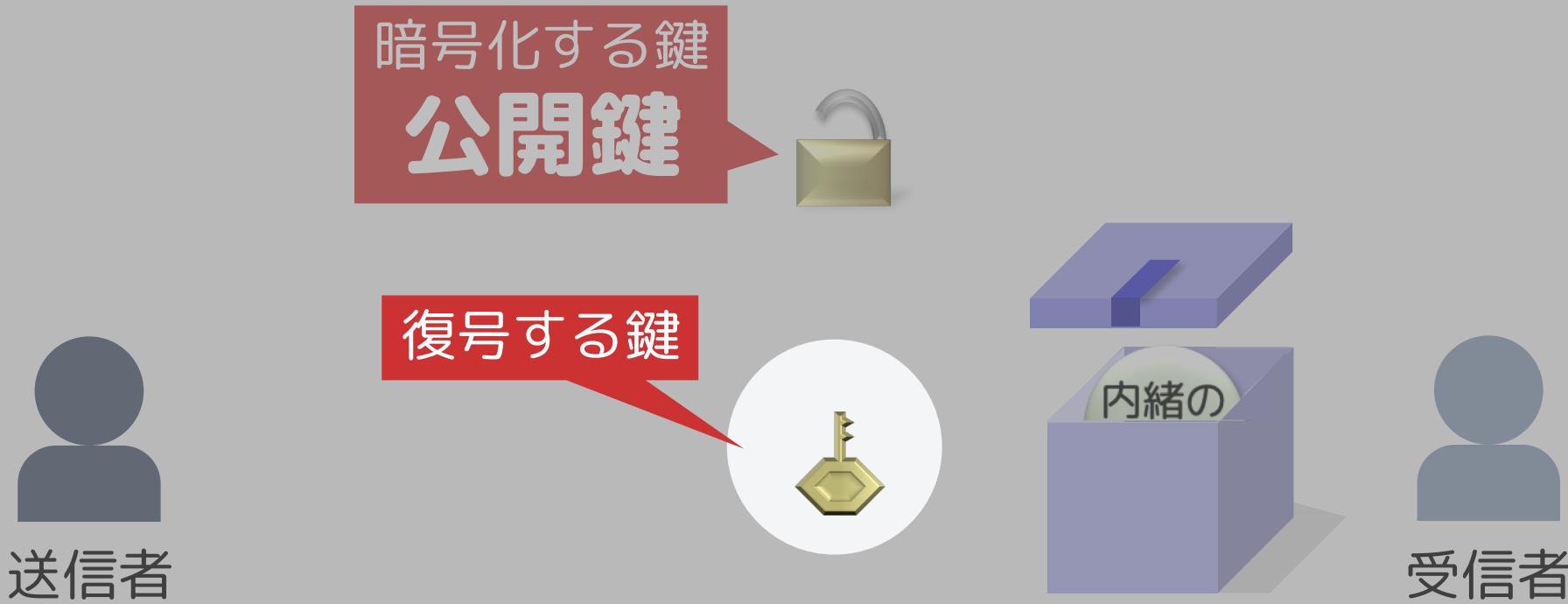
誰でも入手してもいい鍵になります。

公開鍵暗号方式で用いる鍵



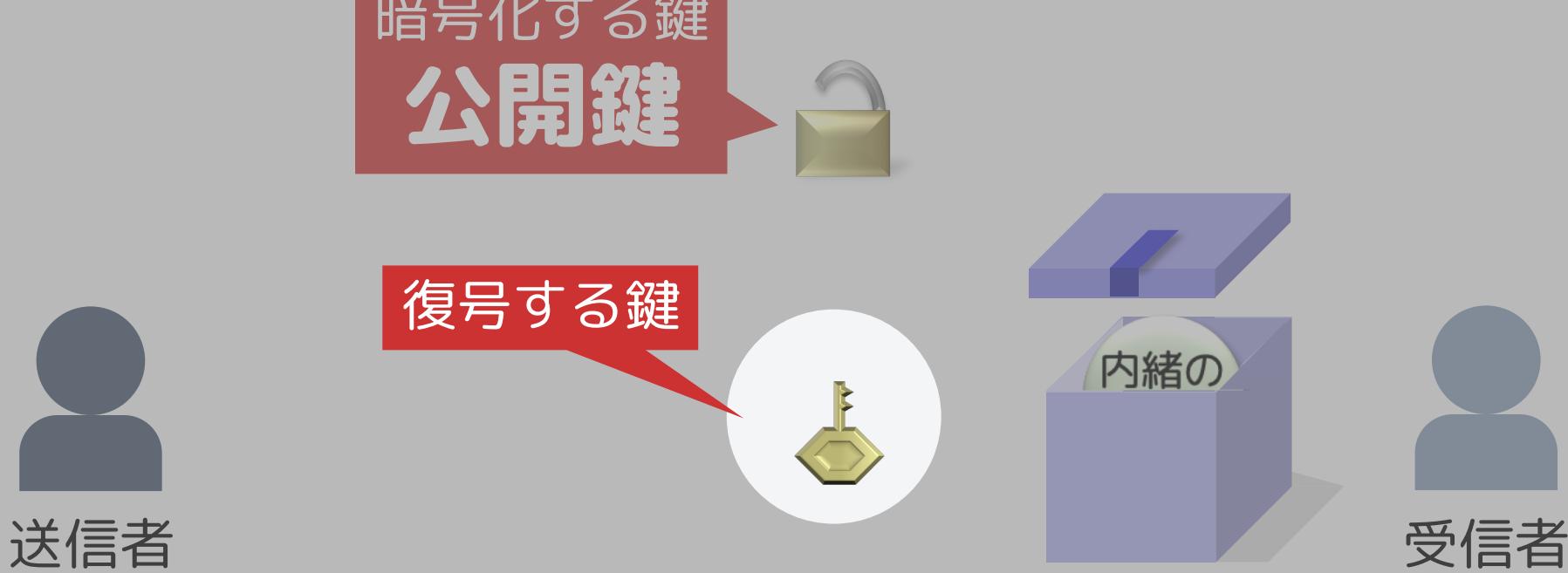
この鍵を、「公開鍵」といいます。

公開鍵暗号方式で用いる鍵



一方で、復号する鍵は暗号化された情報を復号できてしまうので

公開鍵暗号方式で用いる鍵



受信者だけが秘密に持っている必要があります。

公開鍵暗号方式で用いる鍵



送信者

暗号化する鍵

公開鍵



復号する鍵

秘密鍵



受信者

この鍵を、「秘密鍵」といいます。

南京錠を使った安全な物の渡し方を考えよう

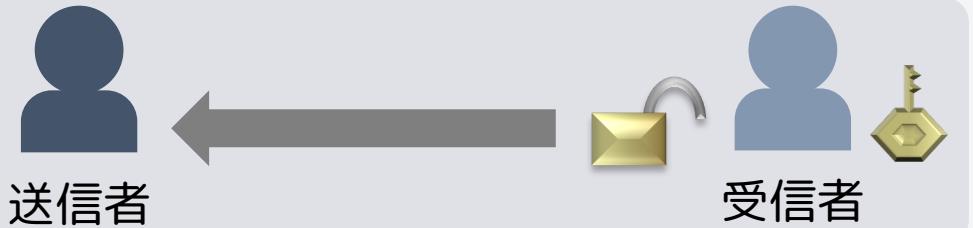
公開鍵
鍵をかける



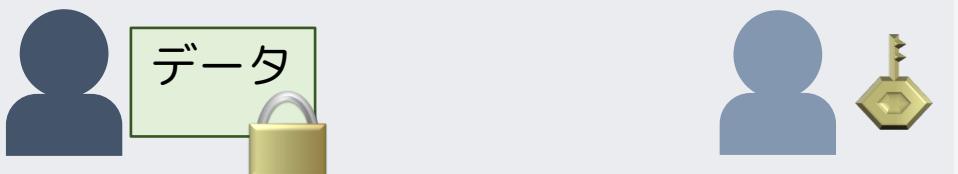
秘密鍵
鍵を開ける



1 ア受信者は イ送信者 に ウ公開鍵 を送る



2 イ送信者は、ア受信者の ウ公開鍵 を使って
鍵をかける(=暗号化)



3 その状態でデータを送信する



4 ア受信者は、ア受信者の エ秘密鍵 を使って
鍵を開ける(=復号)

