

The background features a series of vertical, slightly curved light streaks in shades of orange, yellow, green, and blue, creating a sense of depth and movement against a dark backdrop.

暗号化について

1年 情報

次の暗号を解いてみよう

2

Ucjj Zcgle

正解は・・・

Well being

昔の暗号は？

3

シーザー暗号

非常に簡単な換字法の1つ
アルファベットの文字を一定の文字数分だけずらす

転置法

平文の文字を一定の規則で並べかえる方式

E N C R Y P T I O N

↓ 1字ずらす

F O D S Z Q U J P O

「暗号化」を意味する「ENCRYPTION」のそれぞれのアルファベットを1字分ずらすと、「FODSZQUJPO」と暗号化される。

E N C R Y

↓ ↗ ↓ ↗ ↓ ↗ ↓ ↗ ↓

P T I O N

「ENCRYPTION」を2つに分けて、上のように並べ、縦に文字を拾っていくと、「EPNTCIROYN」と暗号化される。

図28 換字法（シーザー暗号）の例

①暗号化

データの内容を第三者にわからなくする技術または手法

こんにちは

暗号化

gejg23ga2g

②平文(ひらぶん)

暗号化されていないデータのこと



③復号

暗号化されたデータをもとのデータに復元すること。

gejg23ga2g

復号

こんにちは



🔑 共通鍵暗号方式

5

暗号化と復号に使う鍵が同じ方式

平文

こんにちは。お久しぶり
です。お元気ですか？

暗号化後

Gapaw3r2023`*#(“fwdk#
” *~” ff4ikuy#!” `>MVE



さくら



ゆうじーん

🔑 共通鍵暗号方式

6

暗号化と復号に使う鍵が同じ方式



さくら



こんにちは。お久しぶり
です。お元気ですか？



ゆうじーん







共通鍵暗号方式 必要な鍵の数は？

7

- 暗号化、復号に同じ鍵を用いるため2人でやりとりする時は1本でやりとりできる。
- 3人の場合はお互いに1本ずつ必要なので3本



人数	2人	3人	4人	5人
鍵数	 1	 3	 6	 10



- 上のような図を書くか $n(n-1)/2$ で求めることができる



公開鍵暗号方式

8

暗号化と復号に使う鍵が異なる方式
鍵ペア→秘密鍵 公開鍵



- ①受信者が秘密鍵と公開鍵を作成
- ②送信者は受信者より公開鍵を得る
- ③送信者は公開鍵で平文を暗号化
- ④受信者は自分の秘密鍵で復号



さくら



ゆうじーん



公開鍵暗号方式

9

暗号化と復号に使う鍵が異なる方式
鍵ペア → 秘密鍵



公開鍵



さくら



ゆうじーん

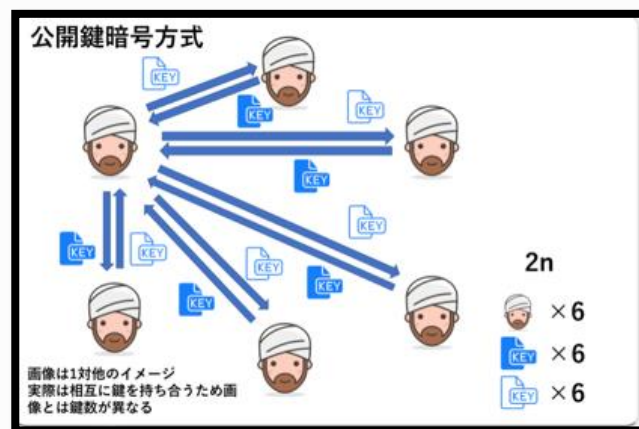
- ① 受信者が秘密鍵と公開鍵を作成
- ② 送信者は受信者より公開鍵を得る
- ③ 送信者は公開鍵で平文を暗号化
- ④ 受信者は自分の秘密鍵で復号



公開鍵鍵暗号方式 必要な鍵の数は？

10

- 暗号化、復号に違う鍵を用いるため2人でやりとりする時は**2本必要**。
- 3人の場合はお互いに2本ずつ必要なので6本必要



- 図を書くよりは $2n$ で求めるほうが早い

共通鍵暗号方式と公開鍵暗号方式の違い

11

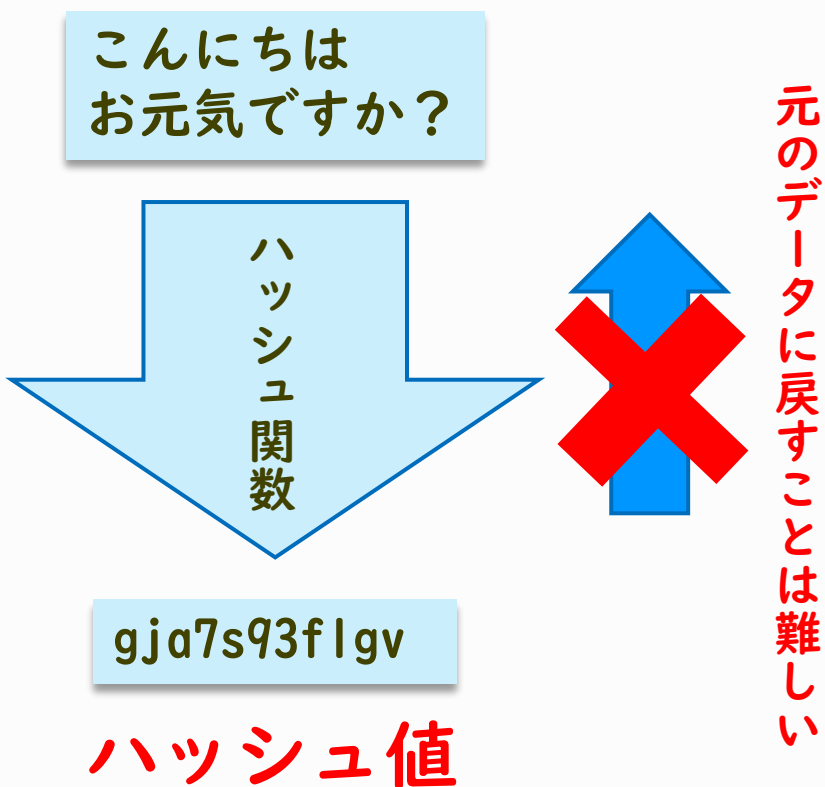
	共通鍵暗号方式	公開鍵暗号方式
メリット	公開鍵暗号方式に比べて暗号化と復合が (① 速い (高速))	(② 公開鍵の方は公開情報なので漏洩しても問題がない)
デメリット	人数分の異なる共通鍵を準備し、これを安全に共有し使い分ける必要があるので、鍵の管理が大変	共通鍵暗号方式に比べて暗号化と復号に (③ 時間がかかる)

ハッシュ値について

12

ハッシュ値の特徴

- 入力値が同じ内容なら、必ず同じハッシュ値となる
- 入力文字を少しでも変えると全く違うハッシュ値となる



公開鍵暗号方式とハッシュ値の技術を応用することで、「誰が送信したのか」と「途中で改ざんされていないか」を確認できるようにした

⇒①デジタル署名（電子署名）

デジタル署名流れ

14



さくら

ゆうじんの
の公開鍵



こんにちは
お元気ですか？

ハッシュ
関数

gja7s93flgv

自分の秘密鍵
で暗号化



ゆうじん

ゆうじんの
秘密鍵

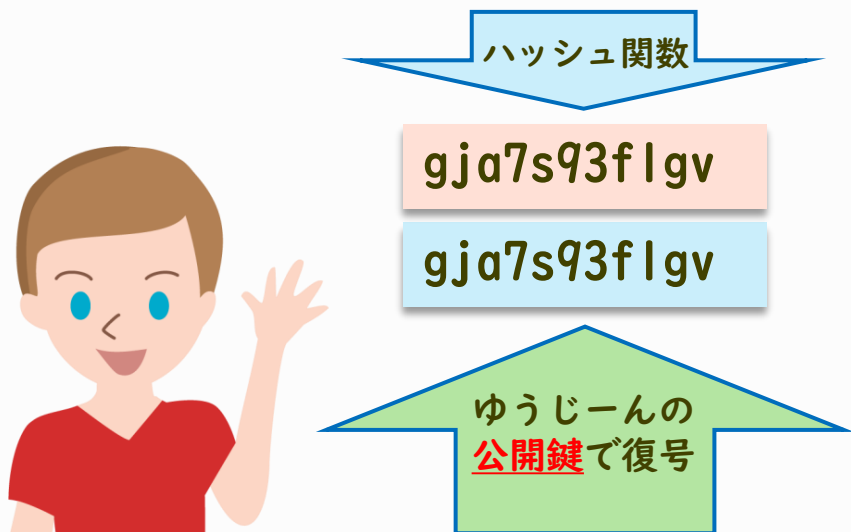


デジタル署名

ハッシュ値を秘密鍵で暗号化したもの

デジタル署名流れ

15



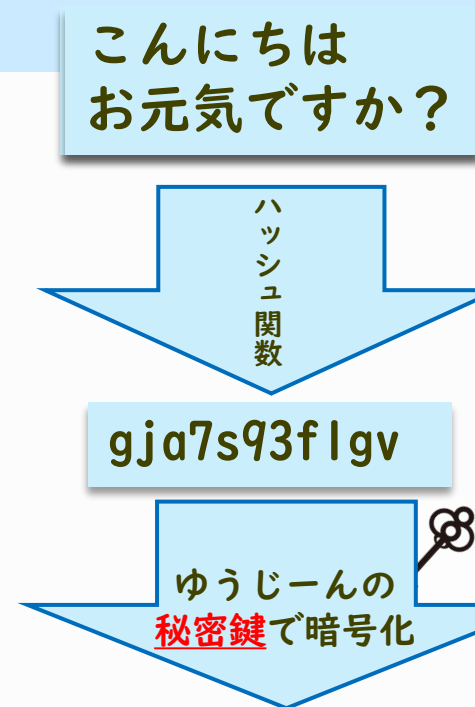
さくら

ゆうじんの
公開鍵



一致した！！
(改ざんされていない)
⇒完全性確認

復号できた！！
⇒真正性確認



ゆうじん

ゆうじんの
秘密鍵



デジタル署名

ハッシュ値を秘密鍵で暗号化したもの

デジタル証明書

16

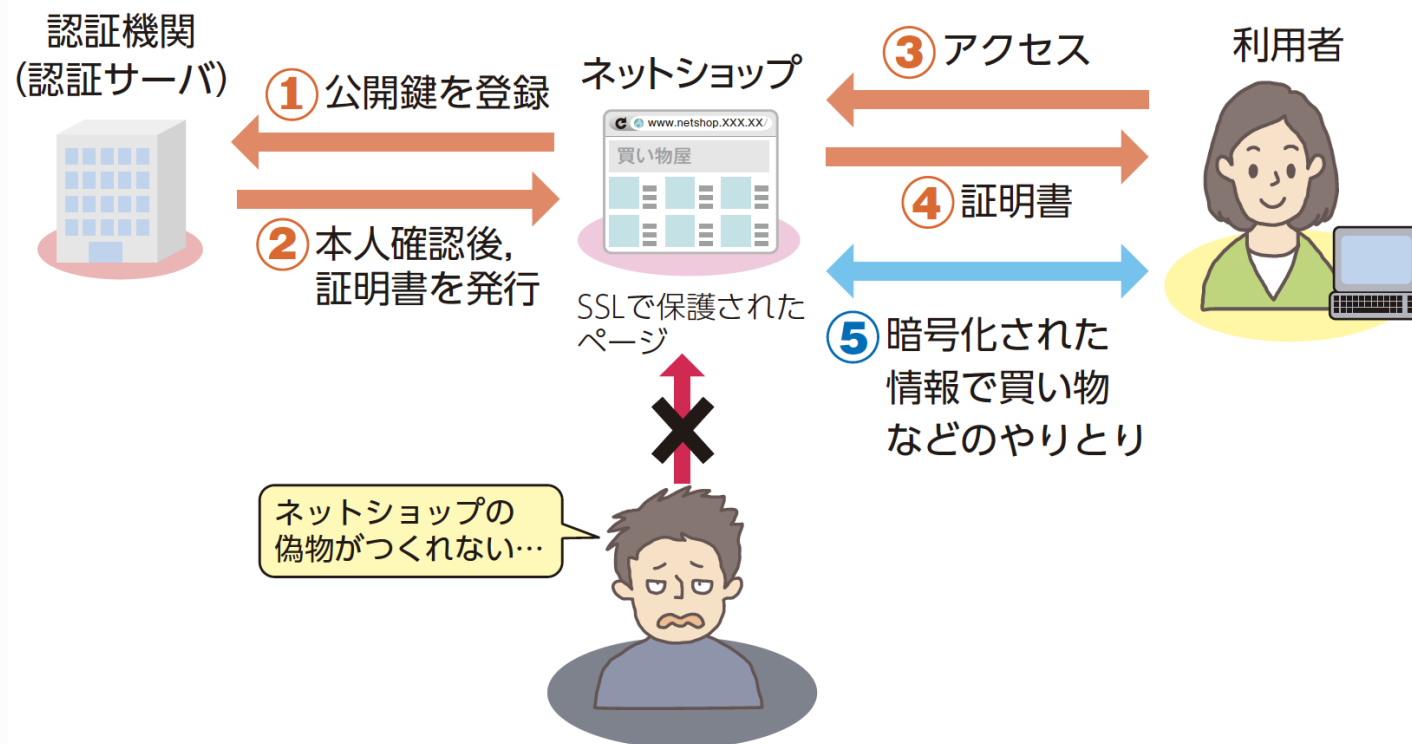
- 公開鍵（デジタル署名）が確かに本人のものであることを、

認証機関（認証サーバ）とよばれる信用できる第三者が証明するしくみがある

- デジタル署名を使いたい人は、認証機関に登録して、

③デジタル証明書

（電子証明書）の発行を受ける



インターネットの暗号技術

17

①SSL

インターネット上で情報を暗号化して送受信する手順の決まり

- SSLを使用していないウェブページのURLは「http://」ではじまるが、SSLを利用したページは「http**s**://」となる
- 近年後継である（②TLS）に置き換わってきているため（③SSL/TLS）と表記されることが多い



図34 SSLとデジタル証明書