暗号技術入門

第1章「暗号世界ひとめぐり」

暗号技術入門

出版：SB Creative

著者：結城 浩

第三版は2015年発行。暗号化技術の基礎から丁寧に解説されており、各所で初心者にお勧めされている。改訂版ではビットコインなど最新の情報も記載。

基本用語

平文

こんにちは！

嶋村です！！

眠いです！！！

暗号化

復号化

暗号文

gaebetgs

lrgeafbvk

Apfs;ihgwa

送信者

Sender

受信者

Receiver

対称暗号

暗号化と復号化で同じ鍵を使う方式

公開鍵暗号

暗号化と復号化で異なる鍵を使う方式

非対称暗号とも

1970年代に開発

現代セキュリティは
これに大きく依存

一方向ハッシュ関数

- 暗号学的ハッシュ関数のこと
- 入力のハッシュ値を計算する。逆は不可能。
- これが提供するのは機密性ではなく **正真性（完全性）**。

メッセージ認証コード

・メッセージが期待した相手から来たものであるかどうかを確かめる。

・ **正真性**と**認証**を提供。

デジタル署名

・「いや？そんなん送ってないけど？」を防ぐ。

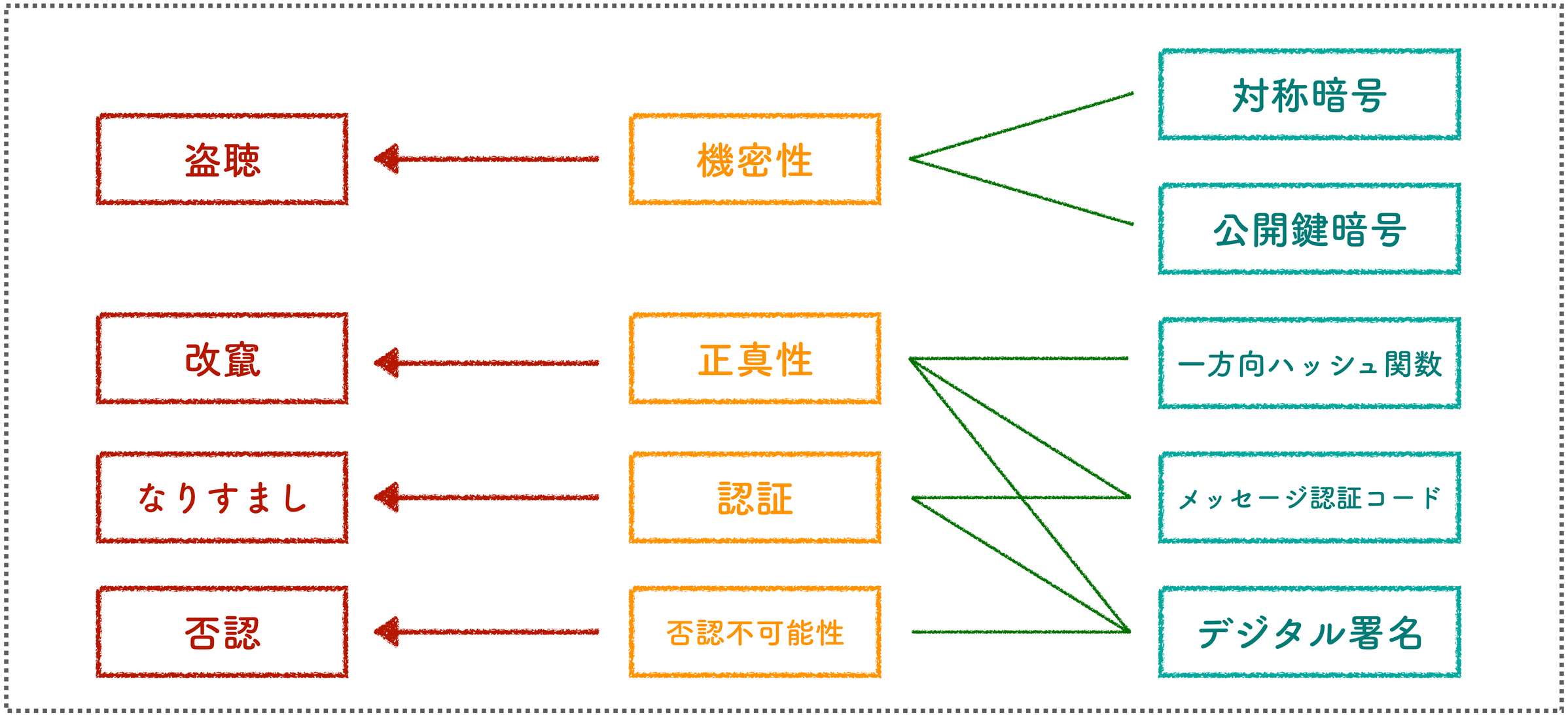
　→**否認不可能性**

・なりすましも防ぐ。

・受信者は送信者の署名を**検証**する。

・**正真性**、**認証**、**否認不可能性**を提供する。

暗号学者の道具箱


盗聴
改竄
なりすまし
否認
機密性
正真性
認証
否認不可能性
対称暗号
公開鍵暗号
一方向ハッシュ関数
メッセージ認証コード
デジタル署名

ステガノグラフィ

・メッセージの存在を隠す。

・縦読み。

・もっと発展させると**電子透かし**とかの技術に。

・暗号は内容を隠し、ステガノグラフィは存在を隠す。

暗号とセキュリティの常識

秘密の暗号アルゴリズムを使うな

・暗号化のアルゴリズムを秘密にすれば最強じゃね？は幻想

秘密はいつか必ず暴かれる

暴かれなかった例などない。

強いアルゴリズムを生み出すことは困難

専門家にかかれば一発で解読される。

・**隠すことによるセキュリティ**は危険で、かつ愚かとみなされる。

「強い暗号」

・専門家に暗号アルゴリズムを教え、ソースコードも渡し、平文と暗号文のサンプルを大量に渡したとしても、それでもなお暴かれない暗号が「**強い暗号**」。

・**タネも仕掛けも明かしてもなお解けない暗号、それが強い暗号。**

弱い暗号は暗号化しないよりも危険

・「暗号」による「誤った安心感」を抱いてしまう。

・「暗号化されている」という事実そのものに安心してしまい、過度な期待と虚空の信頼をおいてしまう。

・結果として機密情報の扱いがぞんざいになる危険性がある。

どんな暗号もいつかは解読される

・全てしらみ潰しに試せばいつかは解読される。有限時間内に。

・ひいては技術の進歩によっても解読可能性は上がる。

ex)ムーアの法則による性能上昇、量子コンピューティング

・使い捨てパッドなど解読が絶対不可能なものもあるが実用的ではない。

暗号はセキュリティのほんの一部である

- 「セキュリティ」は暗号だけでは成り立たない。
- 悪意ある第三者がなりすました「パスワード教えて」メールに返信でもされたら暗号もなにもなくなる。