IoT eラーニング

IoTと暗号技術・認証技術

（暗号技術・認証技術の最新動向、IoTにおける活用）

国立大学法人　琉球大学

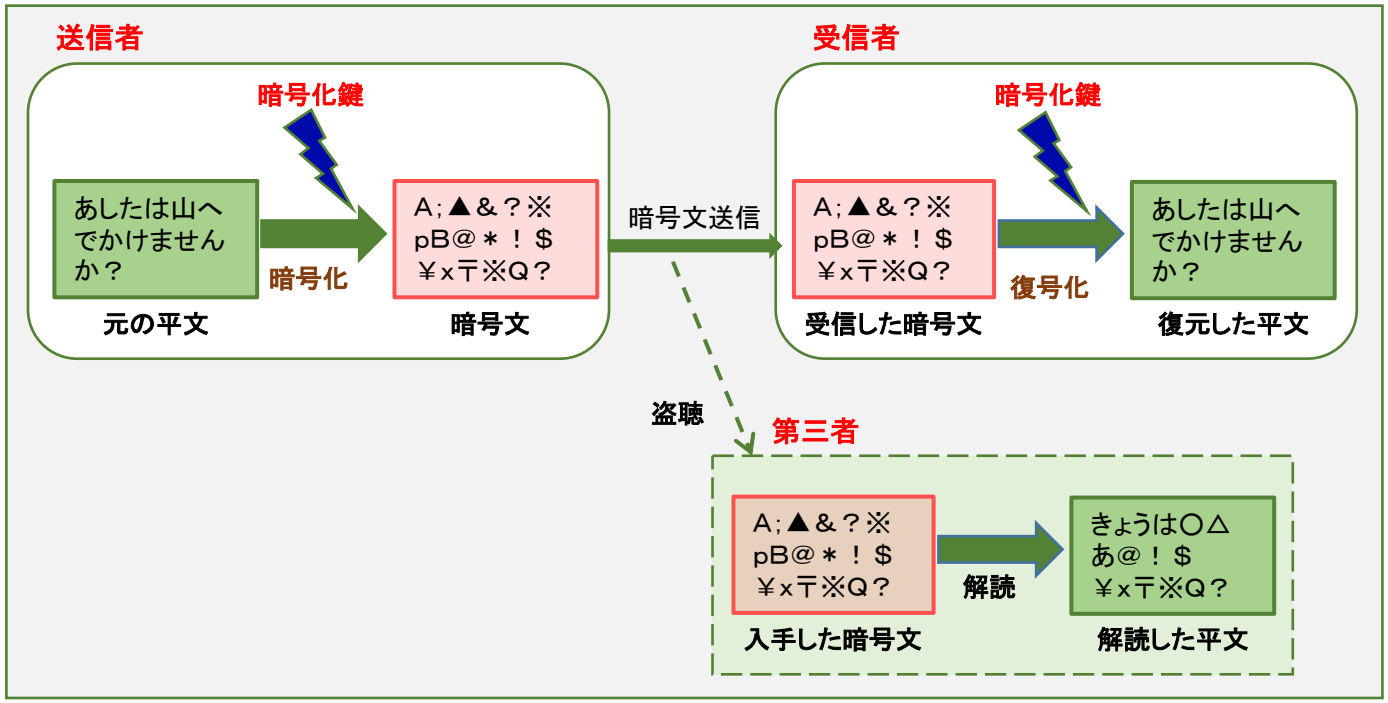
目次

暗号

● 暗号とは

暗号とは、データを任意の方法で変換し、容易に内容を解析できないようにすることである。第三者が暗号化されたデータを入手してもそのままでは意味をなさず、解除するにも情報（暗号化手法や鍵等）が分からないと利用することができない。

暗号を構成する要素としては次のようになる。



● 暗号の流れ（暗号と復号）

前頁の図の中で出てきた言葉として、「平文（ひらぶん）」、「暗号文」、「復号」と「鍵」がある。

- 送信者が暗号化したいデータのことを「平文」と呼び、「鍵」を使って暗号化し「暗号文」を作り出している。
- 受信者が暗号化された「暗号文」を「鍵」を使って復元することを「復号」と呼んでいる。
- 第三者が通信の途中で通信内容を摂取することを「盗聴」と呼び、暗号文だけから元の「平文」を求めることを「解読」と呼んでいる。

「平文」から「暗号文」を作り出す方法を「暗号アルゴリズム」と呼ばれている。
「暗号アルゴリズム」には様々な方式があり、利用者はその中から暗号文の解読され難さを表す安全性／強度とそれを実現するコストをもとに最善な方法を採用している。

共通鍵と公開鍵

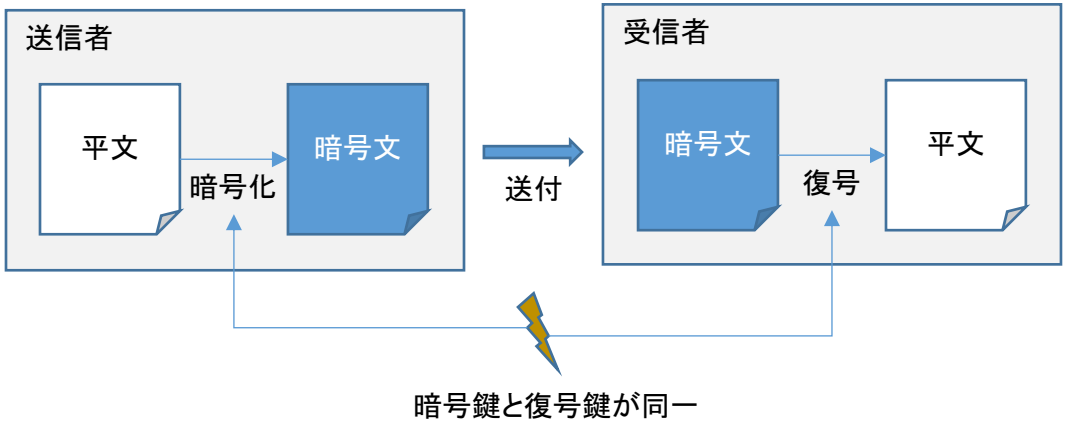
● 共通鍵

共通鍵暗号は同じ鍵（鍵は１つ）で暗号化と復号を行う方式である。

- ドアの鍵のように施錠するときに使う鍵と開錠するときの鍵が同じ鍵であるなど、一般的な鍵から連想する方式はこれにあたると思われる。

- この方式は簡単な原理なため実装しやすく広く使われているが、この鍵をどのようにして受信者へ安全に届けるかが問題になってくる。

鍵がなければ復号できず、鍵が受信者以外に漏れてしまえば第三者が元に復号されてしまう恐れがあり、共通鍵暗号を利用する際に、鍵をどのようにして受信者へ届けるかが課題となってくる。



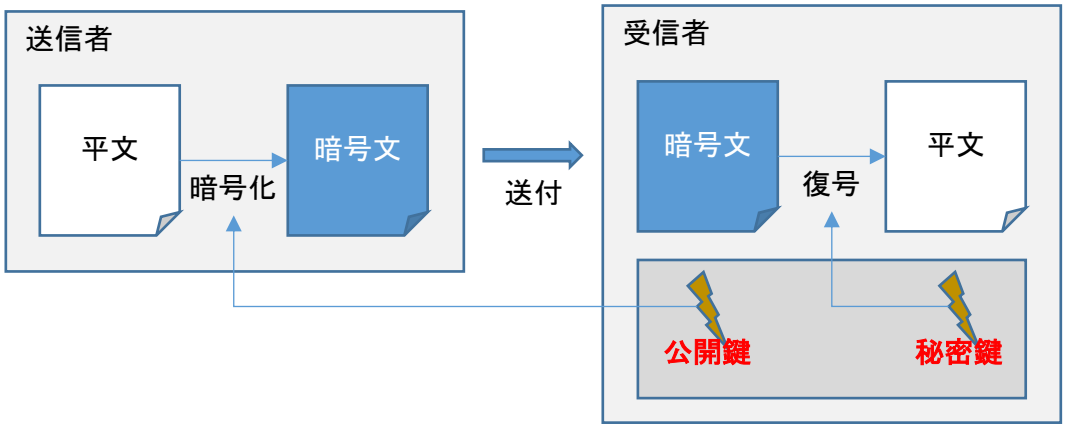
共通鍵と公開鍵

● 公開鍵

公開鍵暗号では２つの異なる鍵（暗号化用と復号用）を用意し、１つ（暗号化用）を公開しても良い点が特徴である。この方式で使用する鍵はそれぞれ「秘密鍵」「公開鍵」と呼ばれている。

- 暗号化に使用する「公開鍵」は広く公開し、復号に使用する「秘密鍵」は秘匿しておく。
- 送信者が受信者に暗号化してデータを送りたい場合は、受信者の「公開鍵」で暗号化した暗号文を受信者に送信する。受信者は送られてきた暗号文を「秘密鍵」で復号する。

共通鍵暗号では鍵情報を相手に伝える必要があり、受け取った側も厳重に保管しておく必要があったが、この公開鍵暗号では相手が公開している鍵を利用するためこのような管理が不要となってくる。

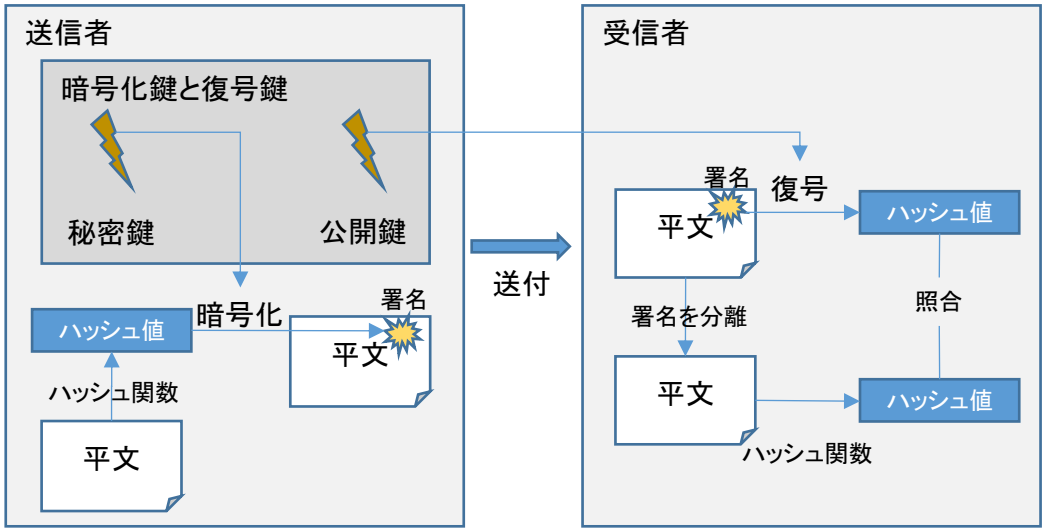


デジタル署名

● デジタル署名とは

デジタル署名は、
◆ 受信したデータが改ざんされていないか
◆ 送信元が間違っていないか
を確認する技術である。

デジタル署名では、公開鍵暗号化方式を使い「誰から送られてきたか」の確認に、ハッシュ関数を使い「改ざんされていないか」の確認に使用している。



デジタル署名

● デジタル署名の流れ

デジタル署名の流れは次のようになる。

- 送信者は送信するデータからハッシュ値を求め、そのハッシュ値を送信者の「秘密鍵」で暗号化する。
- 送信者は暗号化されたハッシュ値とデータをペアで受信者へ送付する。
- 受信者は受信したハッシュ値の暗号文を送信者の「公開鍵」でハッシュ値を復号する。
- 受信したデータからハッシュ値を求め、復号したハッシュ値と一致するかを確認する。

一致していれば、受信したデータは送信者から改ざんされることなく送られてきたと判断できる。

セキュリティプロトコル

● セキュリティプロトコルとは

あるデータを送信する際に、データそのものを暗号化して送信してもセキュリティが確保されるとは限らない。

通信に使用するプロトコルによっては、悪意を持つ第三者が送信者になりすましデータを送り付けるなどが発生する場合がある。

WebサーバとWebブラウザ間での通信に、HTTPプロトコルとHTTPSプロトコルがあり、次のような違いがある。

- HTTPはデータを平文で送信する
- HTTPSはSSL証明書を用いた暗号化を行って送信する

セキュリティの確保をする上でも、通信時に利用するプロトコルの選択も重要となってくる。

- **認証とは**

  あるコンピュータを操作しても良いか、保存されている情報を閲覧しても良いか等、あらかじめ決められた人またはモノに許可を与える行為である。

  認証方式には様々な方式があり以降で説明する。

● パスワード認証

パスワード認証は多くのシステムでされている。IDとパスワードによる認証のため実装が容易なためである。

パスワードを盗まれたり推測される等して破られる場合があるため、定期的にパスワードを更新する、パスワードの使いまわしは不可、複雑なパスワードを使用する等の仕組みを用いる必要がある。

IoTではデバイスによりパスワードを入力することができない場合がある。

- **ICチップ認証**

ICチップ認証は、ICチップが埋め込まれたカード等を携行し読み取り機でICチップの内容を読み取ることにより認証をあたえる仕組みであり、ICチップのデータ保管領域に強固なパスワードを保管することができる。

ただし紛失や盗難などの危険性があり、そのような事態が発生した場合のために運用体制を築く必要がある。（利用者からの相談窓口や問題となったデバイスの無効化手続き等）

携帯電話等のSIMカードや交通機関の乗車カードのFeliCa等で利用されている。

● 生体認証

生体認証とは、人間の指紋や虹彩等の身体的特徴や筆跡やまばたき等の行動的特徴の情報を事前に登録しておき、認証時にそれを確認することで認証を与える仕組みである。

身体的特徴には、指紋、網膜、虹彩、掌等の血管・形、音声などがあり、行動的特徴には筆跡、まばたき、歩行等がある。

この方式ではパスワードを覚えたり、ICチップのカード等を携帯しておく必要がないため、手軽な認証手段、あるいは第三者を防止できる手段として建物などの入口やキャッシュディスペンサー等で利用されている。

しかし、年をとることで特徴が変わり認証できなくなる場合や、けがや先天性の欠損などで生体認証を利用できない人への対応が必要となる。

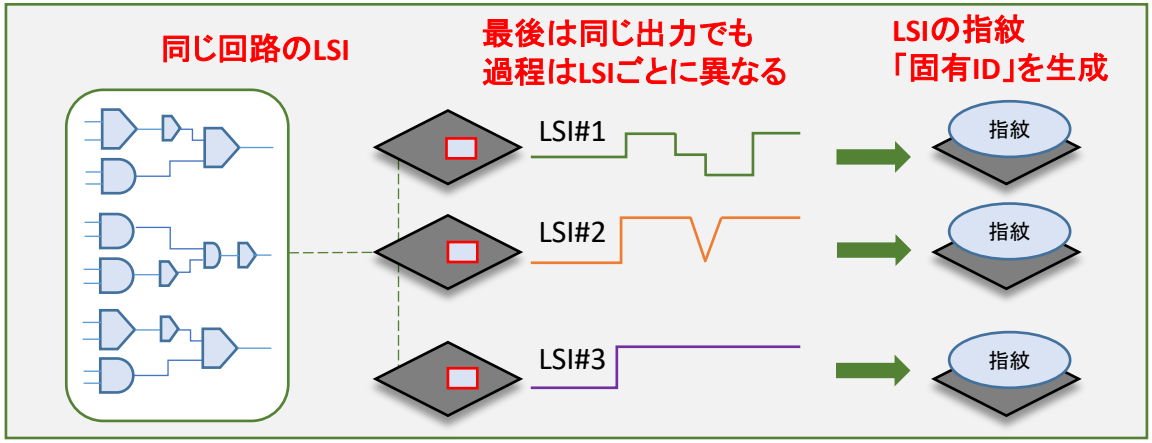
また、複製によって破られてしまった場合は同一の認証方法では安全性を回復できなくなる。

● LSIの指紋「固有ID」

三菱電機は、同じ回路を持つLSIでも信号を出力する過程で個別に異なることを利用してセキュリティの向上を図る仕組みを研究中であると発表した。

- LSIは同じ回路であっても個体差があり、同じ出力でも個体ごとに出力の上昇パターンが異なる。これをLSIの指紋と捉え、固有IDを生成する。
- LSIから出力される上昇パターンを固有IDとして利用するため、分解・解析してもIDを盗み見ることができず、また複製してもパターンが変わるため同じIDを求めることができない。

この技術で「見えないID・複製できないID」という安全性を証明する条件をクリアした。



● SIMを活用したIoTセキュリティ

KDDI株式会社と株式会社KDDI総合研究所は、SIMを活用したIoTセキュリティ技術を開発したと発表した。発表された技術は、IoTデバイスの通信にSIMの高いセキュリティ耐性を持たせることで、不正遠隔操作やなりすましを防止する技術である。また、SIMの特徴を生かした遠隔保守も可能となる。

- 高いセキュリティ耐性と遠隔保守が可能なSIMの中に、IoTデバイス向けの暗号鍵を発行するアプリを組み込み、IoTデバイスへ共通鍵や公開鍵証明書を安全に発行する。

- OTA（Over The Air：無線通信で行う）による遠隔操作でIoTデバイスへ暗号鍵を発行するアプリの設定や解除の実証実験に成功したと発表した。

これにより、IoTデバイスの認証や暗号通信等の保守を遠隔で行うことが可能となった。この技術を応用することで、IoTデバイスのソフトウェアを安全にアップデートできるなど、IoTデバイスへの利便性の向上等が期待される。

● スマートフォンで指静脈認証

日立製作所は、スマートフォンに搭載されているカメラで高精度な指静脈認証を実現する技術を開発したと発表した。この技術は指の静脈を利用した生体認証でオンラインショッピングなどの際に本人認証が可能となる。

これにより、パスワードの漏洩や本人のなりすましによる不正を防ぎスマートフォンで安全な本人認証を実現する。
静脈認証は特徴を示すパターンが体内にあり、偽造やなりすましが困難であるが、静脈パターンを読み取るため専用のセンサーを必要としていた。今回の技術ではスマートフォンに標準搭載されているカメラでも読み取ることを実現した。

具体的には、撮影された複数の指のカラー画像からそれぞれの指を検出し、静脈パターンを安定的に抽出するとともに、それぞれの指の静脈パターンを組み合わせることで認証精度を高めている。これにより、偽造やなりすましが困難な指静脈による生体認証がスマートフォンで利用できるようになる。