**暗号化**

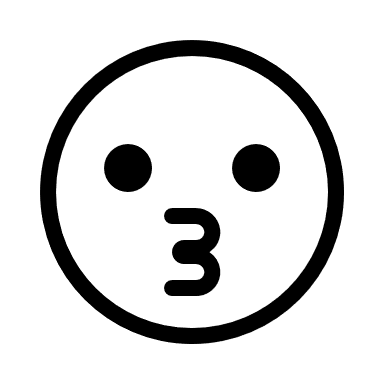
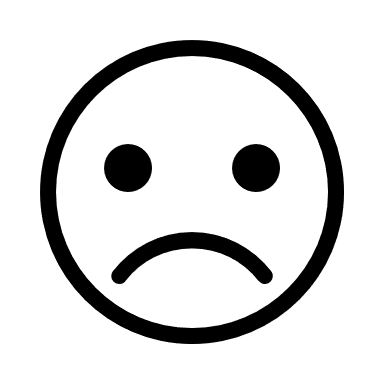
**暗号化とは**

元のデータ(平文)を暗号化アルゴリズムで第三者が読み取れない文章(暗号文)にすること

受け取った暗号文を平文に戻すことを復号と呼ぶ

ユーザとのやりとりの際、通信経路自体を暗号化しておくことで第三者に通信を盗聴されても内容が読みとられず、盗聴が成功した場合でも被害を出さないようにすることができる

○HTTP通信の場合



平文でやりとりすると、盗聴が成功した場合内容が読みとれる

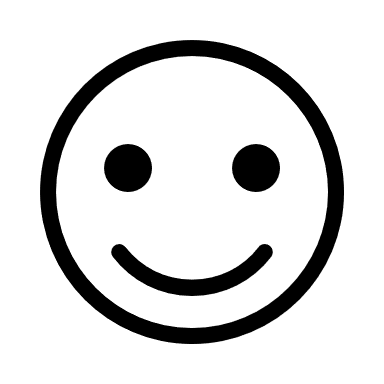
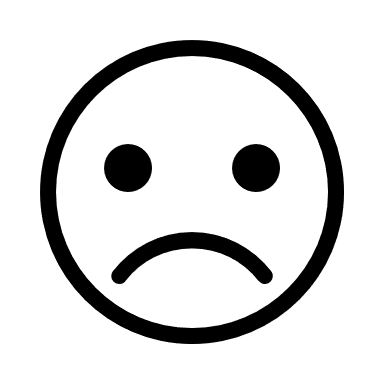
ユーザID

パスワード



Webサーバ

○HTTPS通信の場合



通信が暗号化されていると、盗聴が成功しても内容が読みとれない

暗号化されたデータはサーバ内で複合

Aqg4h8vF7

mdr@9jd35



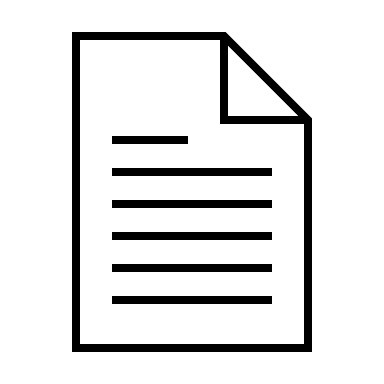
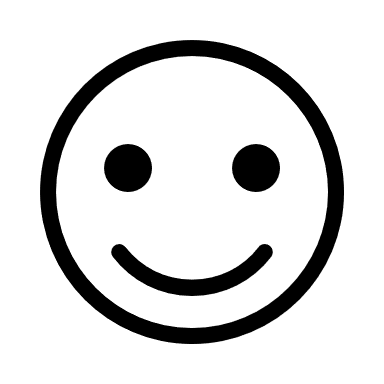
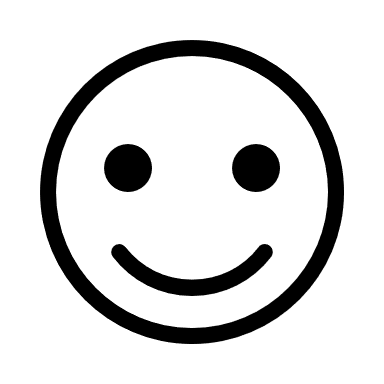
Webサーバ

**保存データの暗号化**

機密性の高いデータはWebアプリケーションがデータを保存するときに暗号化しておき、使うときはデータを復号して利用したり、ハッシュ化して保存することで攻撃への対策となる

・スクランブル化…暗号鍵に相当する秘密の情報を用いずにデータを一定の手順で乱雑化する。送信時とは逆の変換処理を受信側で行い復号する必要があり、暗号を用いて専用の機器や秘密鍵などがなければ復号できない方式と簡単に逆変換できない方式がある

・ハッシュ化…ハッシュ関数によって任意の文字列を固定長の文字列(ハッシュ値)に変換すること、ハッシュ値の長さはハッシュ関数の種類によって異なり、同じハッシュ値を持つ別のデータを生成するのは難しいため認証の際は、送信されてきたパスワードのハッシュ値と保存されているハッシュ値を比較することでパスワードが正しいか判定する



違っていたら改ざんされている

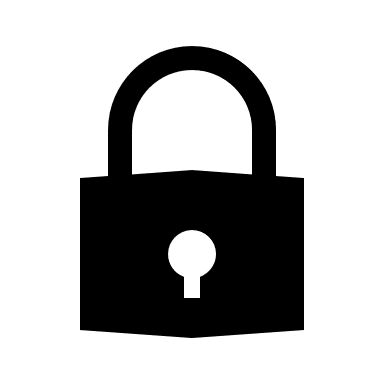


秘密鍵を渡す



元データと一緒にハッシュ値を暗号化したものも送信

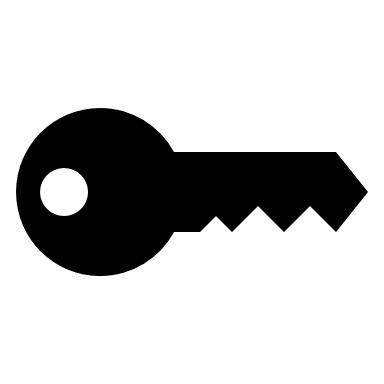
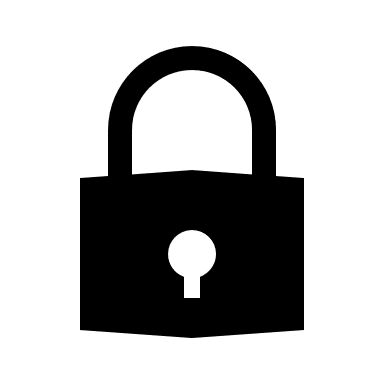
63p



63p

データをハッシュ値に変換

63p



共通鍵

63p

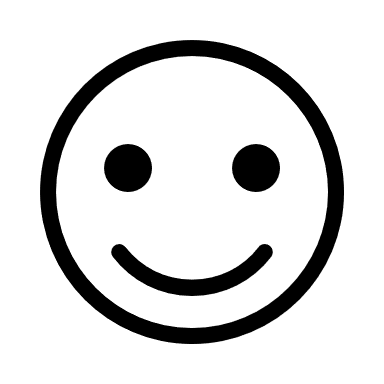
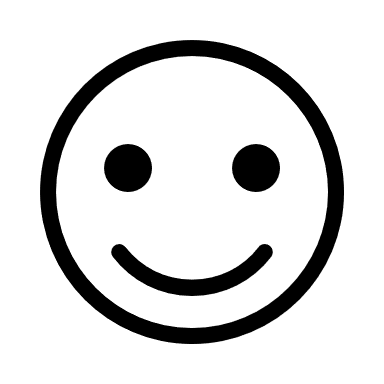
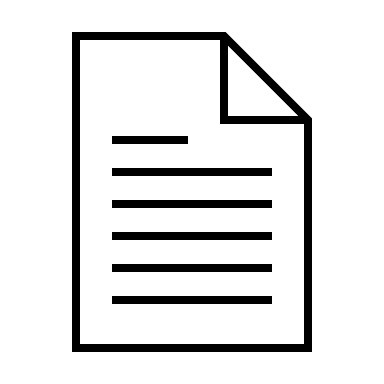
送られてきたデータをハッシュ化したものと暗号化されたハッシュ値を比較

**共通鍵暗号方式**

暗号化と復号化に同じ鍵を使う方式

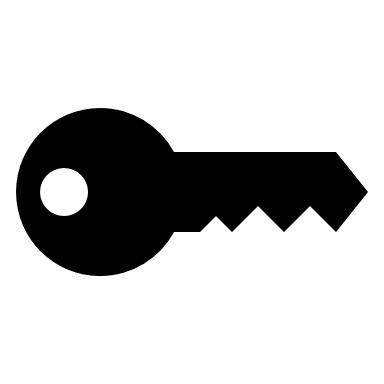
受信側で暗号化・復号化用の鍵を作成し、同じ鍵のうちの１つの鍵を送信者側に送信しておき自分宛てにデータを送信する場合はあらかじめ渡した鍵で暗号化して送信してほしいと依頼する。そして受け取ったデータを自分が持っている鍵を使って復号化する

鍵の受け渡しは、インターネット経由では第三者に見られてしまうため郵送といった手段で行う必要がある

また、複数の相手から暗号化したデータを受け取る場合、相手ごとに鍵を別に用意しなければならない

同じ鍵なので、盗聴されると改ざんされてしまう

持っている共通鍵で復号化



共通鍵

共通鍵で暗号化したデータを渡す

共通鍵を渡す

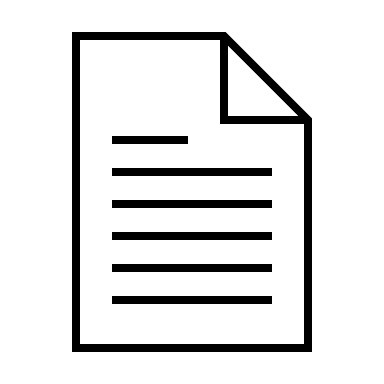
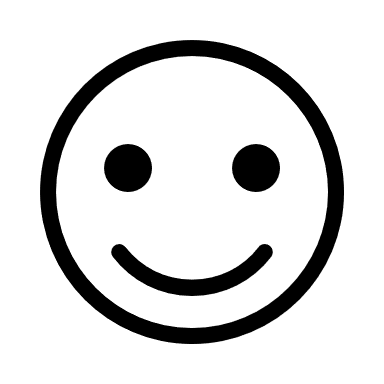
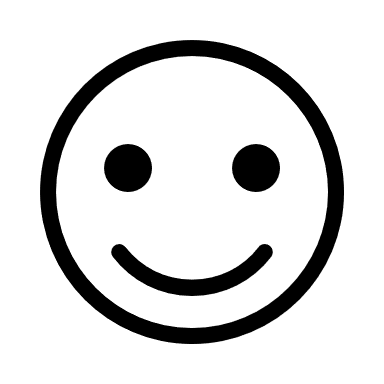
**公開鍵暗号方式**

公開鍵と秘密鍵の2つの鍵を使って暗号化と復号化を行う、どちらの鍵も暗号化・復号化に使用する

公開鍵で暗号化したデータは秘密鍵でしか復号できない、秘密鍵で暗号化したデータは公開鍵でしか復号できないという特徴があるため、第三者に盗聴されても復号化することができない

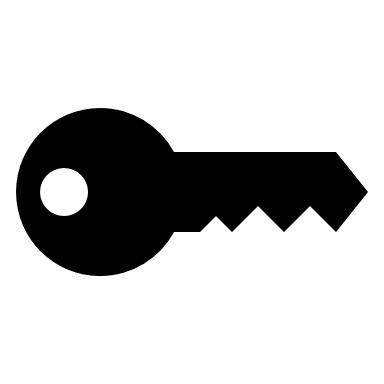
また、送信側が複数になっても公開鍵は1つでいい

ただし、共通鍵暗号方式と比べて処理が複雑になるため処理速度が遅くなる傾向がある





秘密鍵



公開鍵

持っている秘密鍵で復号化

公開されている公開鍵を取得

公開鍵で暗号化したデータを渡す

盗聴されても秘密鍵でないと復号化できない

**公開鍵証明書(SSL証明書)**

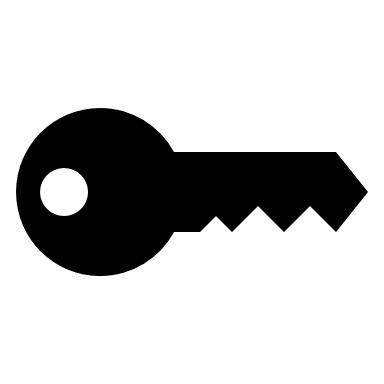
HTTPS通信に使うための公開鍵の持ち主がだれなのか証明し、公開鍵の持ち主が実在することを証明する(実在証明する)もの

認証局と呼ばれる第三者機関から発行され、その認証局を信頼するユーザ全員から信頼されることになる

公開鍵証明書には有効期限があり、Webサイトの停止などで証明が不要になった場合は有効期限内であっても認証局が証明書を失効させることができる

偽造に強く、偽造されてもそれを検知できるつくりになっている

  
  
  
  
  
  
  
  
  
  
  
・自己証明書…認証局から公開鍵証明書を発行してもらうためには発行費用と審査のための時間が必要なため、身内で試験的に公開鍵証明書が必要な場合は自らを認証局とした公開鍵証明書を作成することができるが、一般的に信頼される認証局ではないため限られた用途にしか使えない



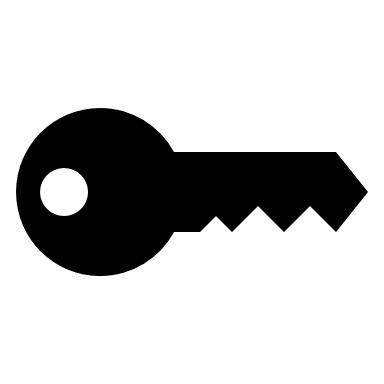
公開鍵証明書

サイトの実在証明をする

Webブラウザ

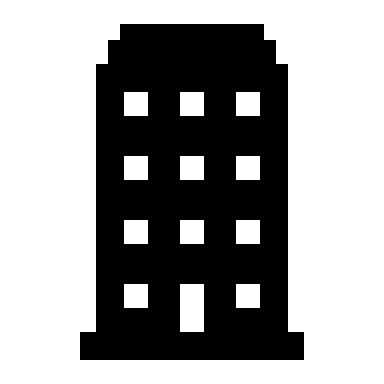
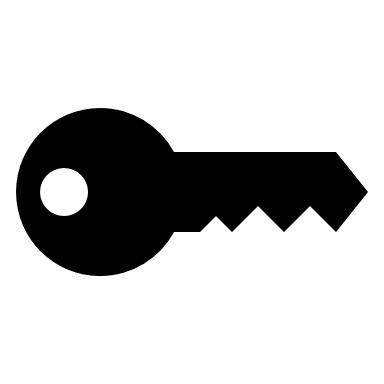
証明された公開鍵を使って暗号化を行う

暗号化通信



公開鍵証明書

クレジットカード情報



認証局



ショッピングサイト