分散システム

第8回 セキュリティ

双見 京介（FUTAMI Kyosuke）
高田秀志（TAKADA Hideyuki）
2025年11月

情報セキュリティの特性

満たすべき性質

性質	内容
機密性（Confidentiality）	「盗聴」されない
完全性（Integrity）	「改ざん」されない
可用性（Availability）	必要なときに利用できる
真正性（Authenticity）	「なりすまし」されない
責任追跡性（Accountability）	操作者やプロセスを追跡できる
否認防止（Non-repudiation）	「しらばくれ」られない
信頼性（Reliability）	操作や処理結果が正しい

セキュリティの脅威

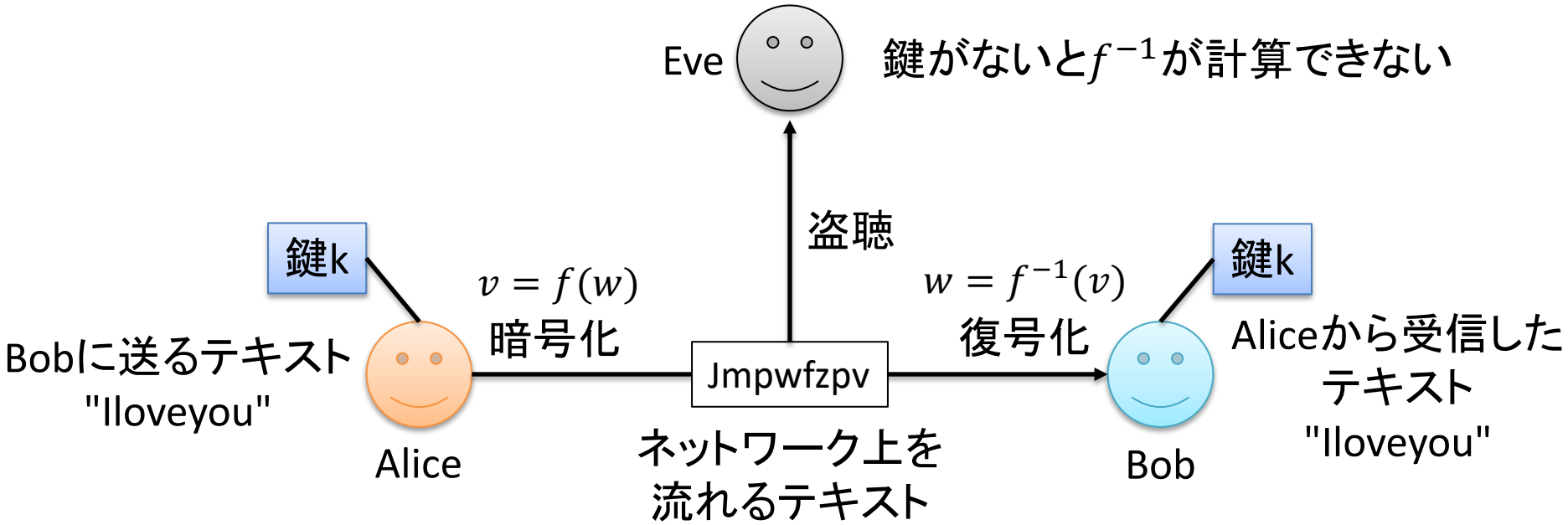
- 通信の傍受・盗聴，データへの不正アクセス
- データの改ざん，通信内容の改変
- サービスの停止・破壊

セキュアなシステムの実現

- セキュリティポリシー
  - セキュリティに関する要求の記述
  - ユーザ，サービス，データ，マシンにどのような動作が許可され，どのような動作が許可されないか
- セキュリティ機構
  - 暗号化（Encryption）
  - 認証（Authentication）
  - 認可（Authorization）
  - 監視・監査（Monitoring and auditing）
- セキュリティポリシーに従って，適切なセキュリティ機構を構築

共通鍵暗号の原理

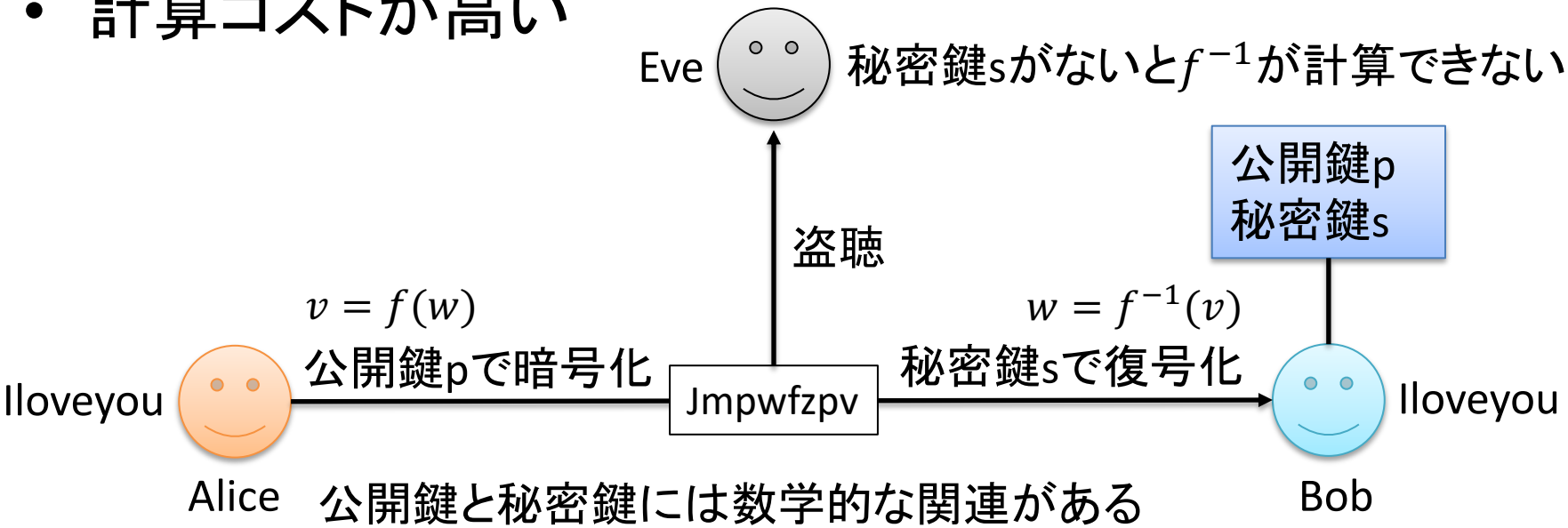
- 送信者と受信者が共通の鍵を所有
- 比較的計算コストが低い



鍵があれば$f \cdot f^{-1}$が容易に計算できる

公開鍵暗号の原理

- 受信者側の公開鍵と秘密鍵の組を利用
- 公開鍵から秘密鍵は計算不能
- 計算コストが高い



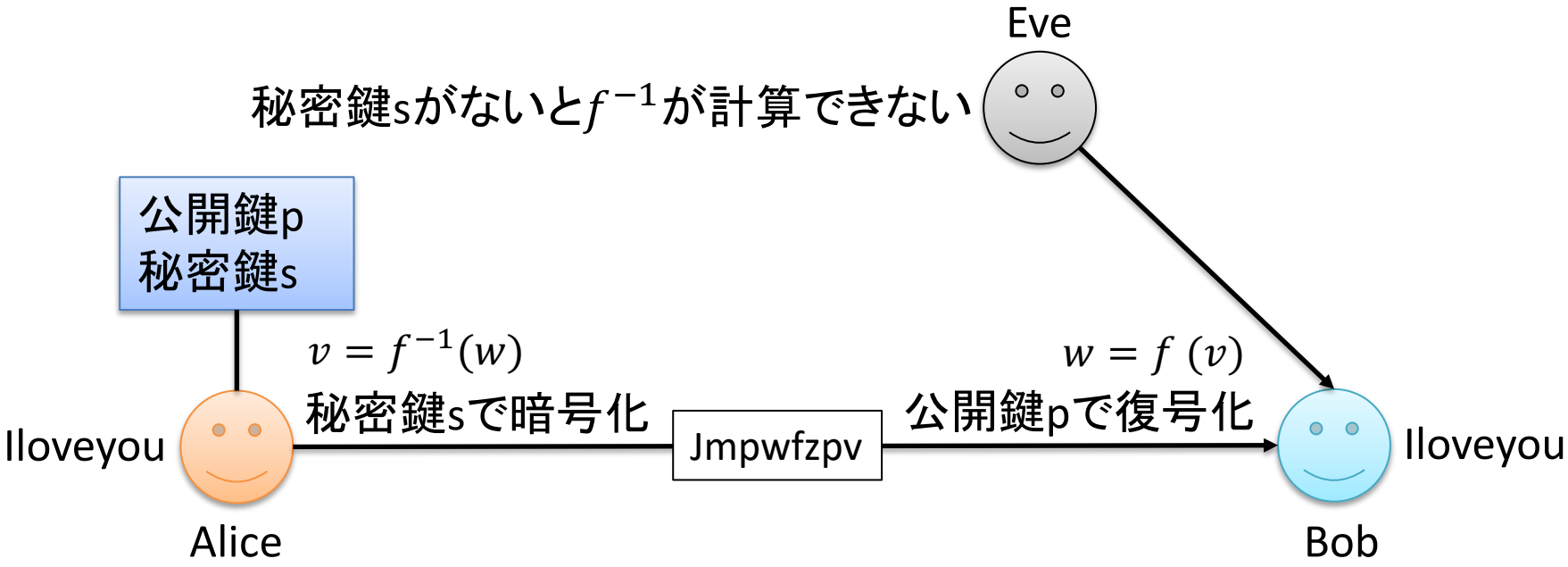
公開鍵と秘密鍵には数学的な関連がある

RSA暗号 : $n = ab$

（非常に大きな素数a, bに対して，nからa, bを求めることは計算量的に見て不可能なことを利用）

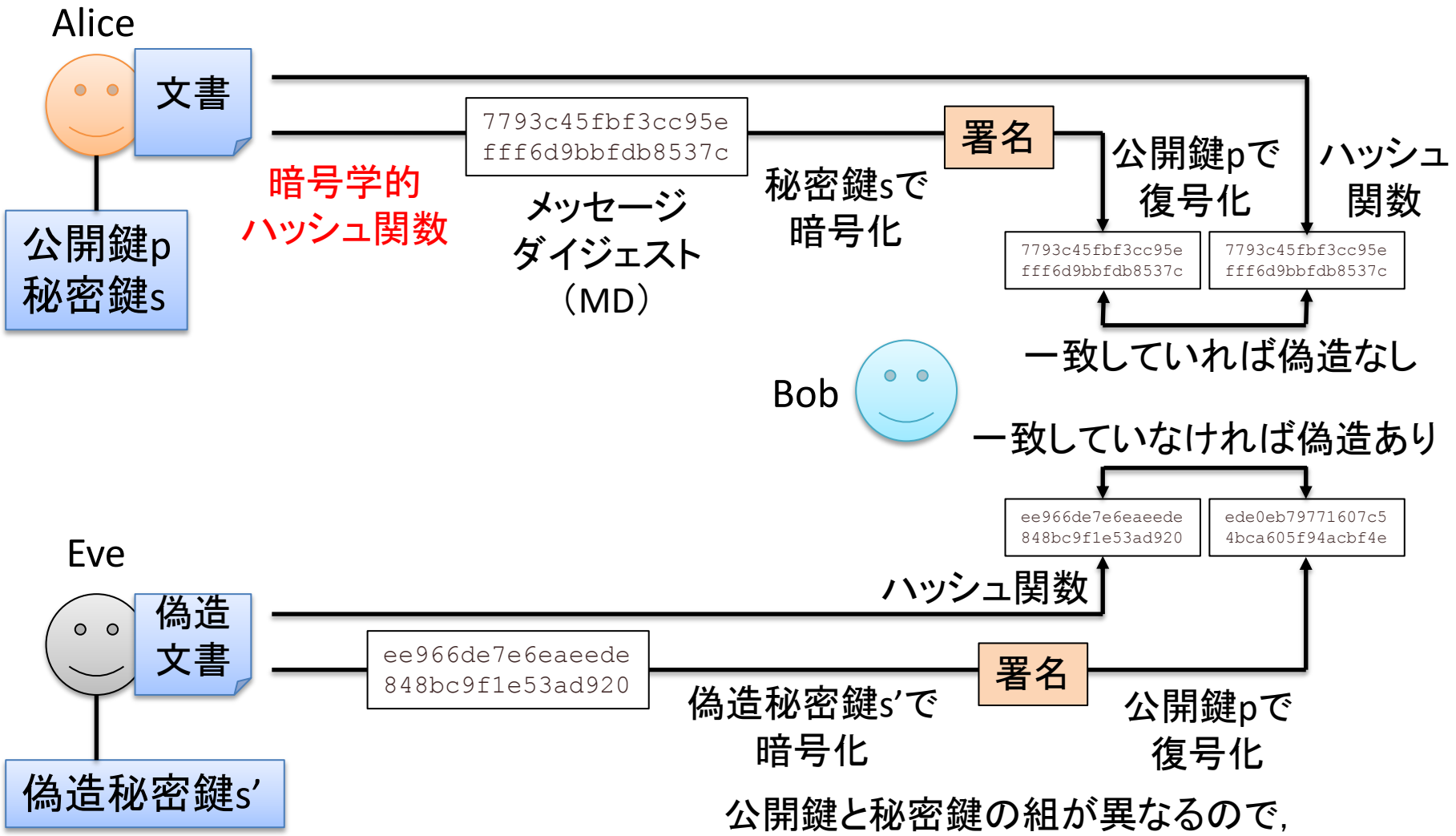
電子署名の原理

- 送信者側の公開鍵と秘密鍵の組を利用
- 否認防止を実現



Aliceの公開鍵pで復号できたということは，Aliceしか知らない秘密鍵sで暗号化（署名）されたことが保証される

暗号学的ハッシュ関数を用いた電子署名

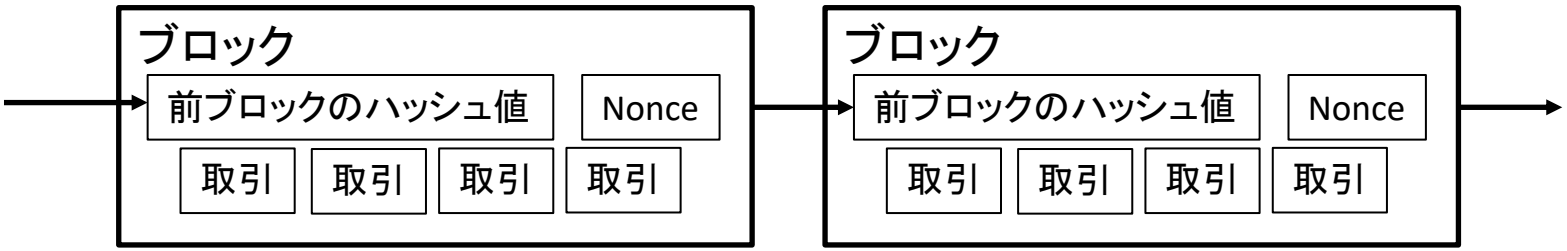


暗号学的ハッシュ関数

- 任意の長さのメッセージから固定長のビット列（ダイジェスト）を生成
- 以下の性質を持つ
  - 原像計算困難性
    - 既知の h に対して，$h = \mathrm{hash}(m)$となるメッセージ m を探すのが困難
  - 第2原像計算困難性
    - 既知の$m1$に対して，$\mathrm{hash}(m1) = \mathrm{hash}(m2)$ となる $m2$ を探すのが困難
  - 衝突困難性
    - $\mathrm{hash}(m1) = \mathrm{hash}(m2)$ となる $m1$ と $m2$ の組を探すのが困難
- 2つのメッセージのダイジェストが同じ場合はメッセージが同一，異なる場合はメッセージが異なる

ブロックチェーン技術

- 暗号学的ハッシュ関数の応用
- P2P型により，「台帳」をブロックの鎖で管理
- ブロックには以下のものが含まれる
  - 多数のトランザクション（取引）
  - ナンス（Nonce）と呼ばれる特別な値
  - 直前のブロックのハッシュ値
- ナンスの値を変えながらブロックに対する特別なハッシュ値を見つけた参加者がブロックを追加できる



秘密分散

- 秘密にしておきたい情報をいくつかの「分散情報」に分ける
- 分散情報を一定数以上集めると秘密情報が復元できるように符号化
- N 個の分散情報に分け，K 個集めると復元できるようにしたものを「(K, N)しきい値法」という
  - K-1次多項式$F(X)$を用意
  - i番目の人に$F(i)$を配布
  - K-1人では秘密情報Sを計算不能，K人で可能

セキュアな通信路

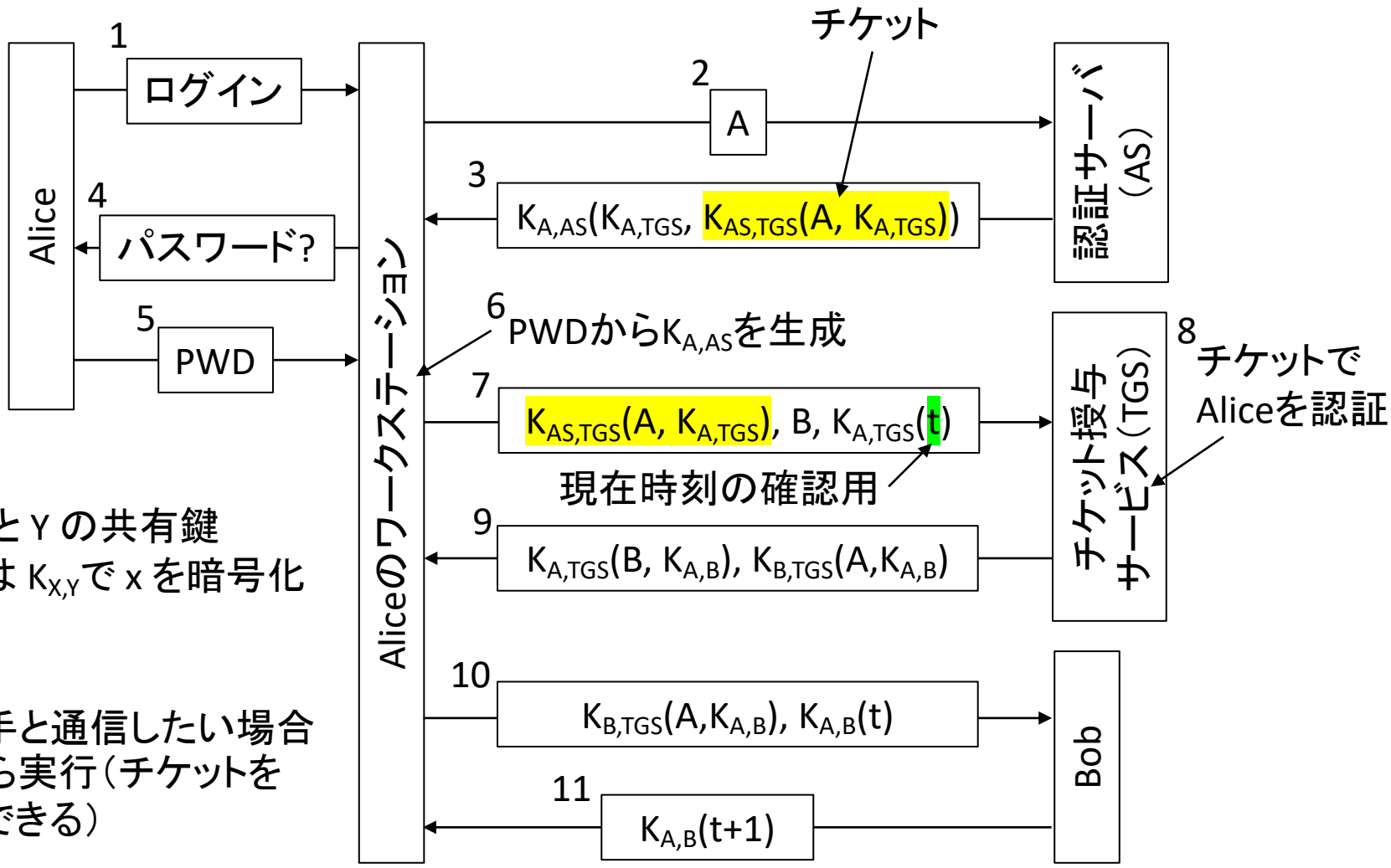
- 通信相手が正当な相手かを確認する「認証」
  - IDとパスワード
  - 指紋や虹彩
  - USBメモリやICカード
  - チャレンジ・レスポンス方式（後述），Kerberosシステム
- メッセージの完全性・機密性
  - メッセージ認証コード（IPSec）
  - セッション鍵の生成（Transport Layer Security, TLS）

チャレンジ・レスポンス認証

AliceとBobは共通鍵（パスワード）を保持

- 共通鍵がネットワーク上を流れない
- 乱数はセッションごとに変化するため，暗号化された乱数を傍受しても，別のセッションに再利用できない（リプレイ攻撃の防止）
- 共通鍵に基づくプロトコルとして，シングルサインオンに使われているKerberosシステムがある

Kerberosにおける認証

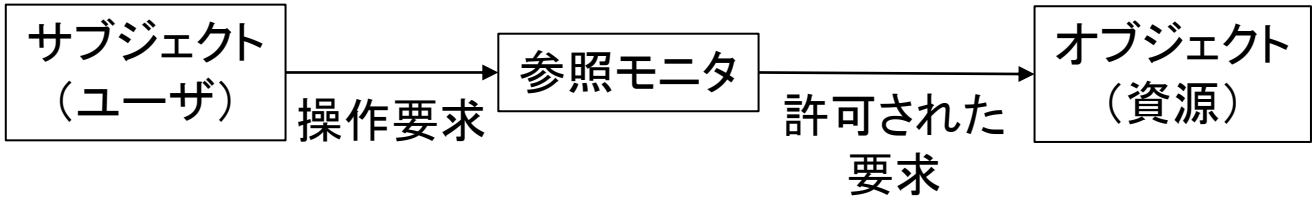


$K_{X,Y}$はXとYの共有鍵
$K_{X,Y}$(x) は $K_{X,Y}$で xを暗号化

別の相手と通信したい場合は，7から実行（チケットを再利用できる）

アクセス制御（認可）

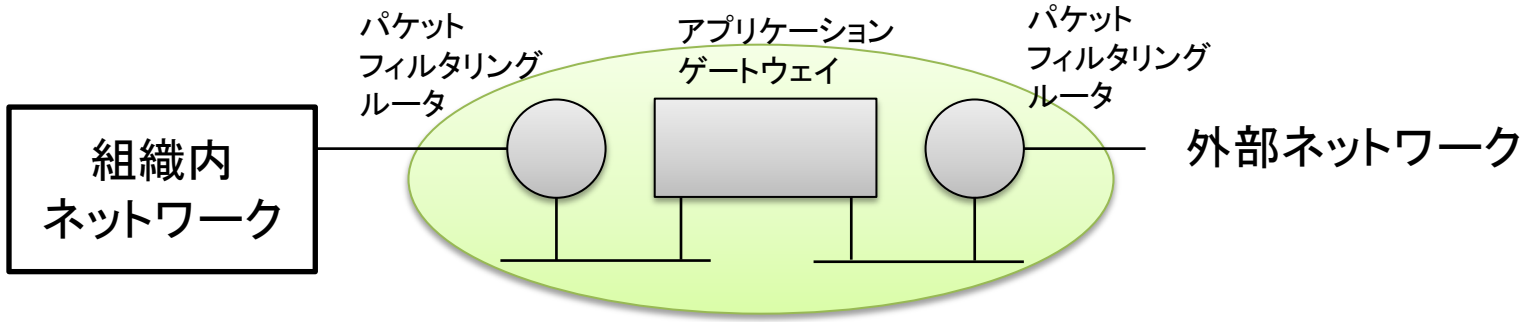
- クライアントがサーバの資源にアクセスできる権限を持つ場合のみ，要求を実行する
- サブジェクト，参照モニタ，オブジェクトでモデル化



- オブジェクトにアクセスできるサブジェクトをアクセス制御リスト（Access Control List, ACL）で管理
- ユーザ毎ではなく，サブジェクトを「役割（role）」とする方法もある

ファイアウォール

- 外部ネットワークと組織内ネットワークの間に設置
- 有害情報，不正プログラム（ウィルス），不正アクセスを遮断
- パケットフィルタリングルータ
  - IPレベル，TCP/UDPレベルでアドレスやポート番号を識別
  - 条件に合わないパケットを捨てる
- アプリケーションゲートウェイ
  - アプリケーション層の情報（メールアドレス等）を識別



モバイルコードのセキュリティ

- ホスト間を移動するプログラムに対する保護
- モバイルコードの情報を保護
  - モバイルコードへの署名
  - 追加専用ログ機能（追加のみ許可，改変・削除不可）
  - 状態の選択的な公開（指定されたサーバのみ閲覧可）
- モバイルコードからホストを保護
  - 保護領域（サンドボックス）内での実行
  - 他のプログラムやデータを操作できないようにする

セキュリティ管理基盤

- 公開鍵基盤（Public Key Infrastructure, PKI）
  - 企業間取引などにおいて安全な通信を確保
  - 認証局（Certification Authority）が「公開鍵が本物であること」を証明する証明書を発行
- 権限管理基盤（Privilege Management Infrastructure, PMI）
  - ホストからアクセス制御リストの管理を独立
  - 属性認証局（Attribute Authority）が所有者の役割や権限などの属性証明書（Attribute Certification）を発行