

# 情報学基礎 第9回

## 6章 インターネット2: アプリケーション

管理工学科

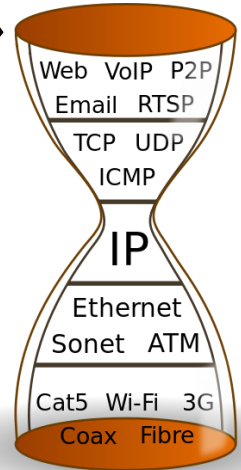
担当: 篠沢佳久

# 本日の内容

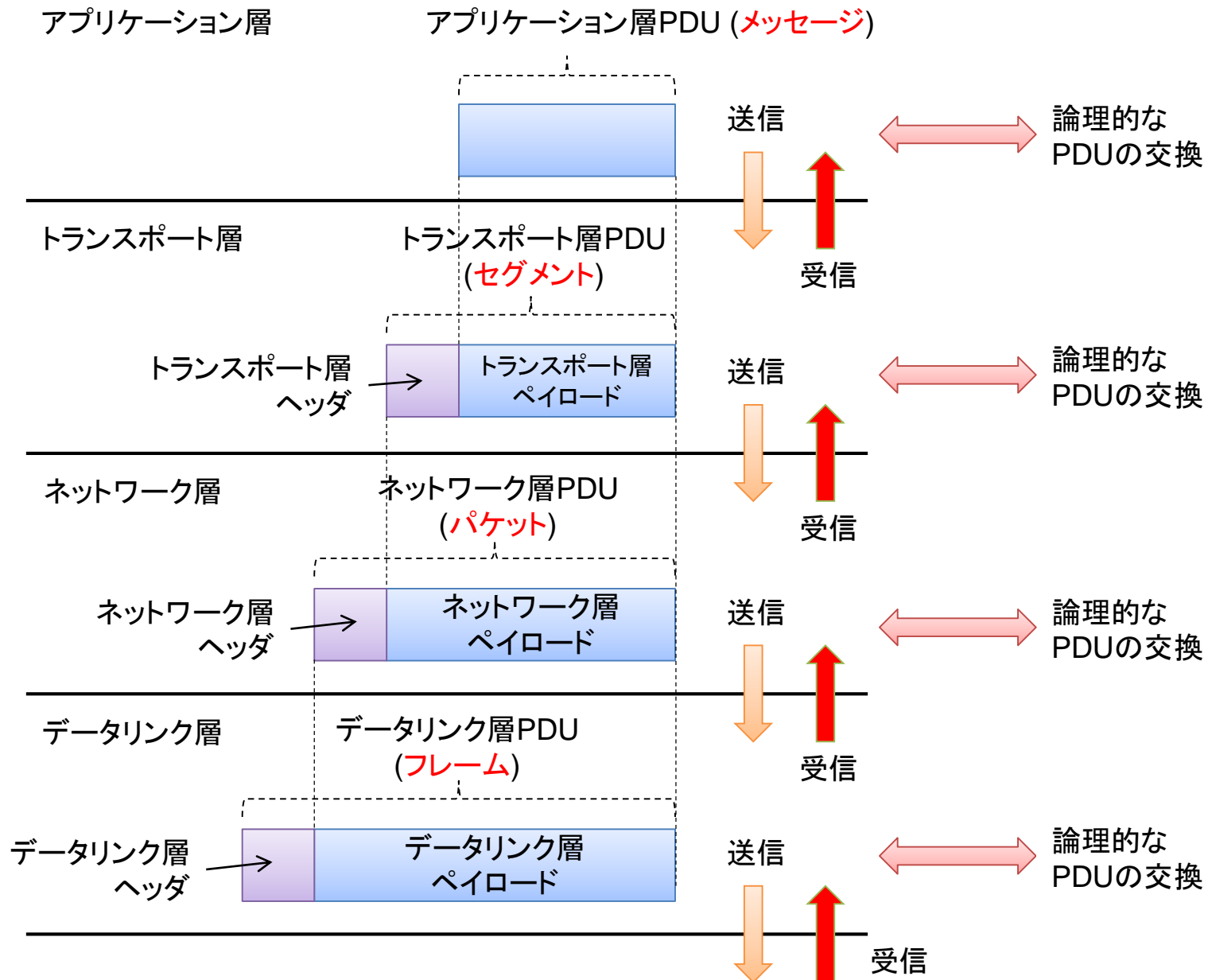
- インターネット2: アプリケーション
  - アプリケーションのサービスモデル(6.1節)
  - ドメインネームシステム(6.2節)
  - メールの仕組み(6.3節)
  - Webの仕組み(6.4節)
  - インターネットにおけるセキュリティ(6.5節)
- 第四回課題
  - 締め切り 6/28(水)23:50
- 第三回課題の締め切りは本日(6/14)です

# インターネットのモデル

- 砂時計モデル
  - IPだけを世界共通の方式に規定
  - 通信方式, アプリケーションの選択に幅
- インターネット普及の一因
  - アプリケーションを限定しないネットワークモデル
  - アプリケーションを限定すると
    - 利点
      - 要求事項が明確化するためネットワークを設計しやすい
      - 要求事項が明確でないと, 新サービスのメリットが分からない
    - 欠点
      - 時代によって変化するアプリケーション要求に対応できない
      - 個人によって異なるアプリケーション要求に対応できない



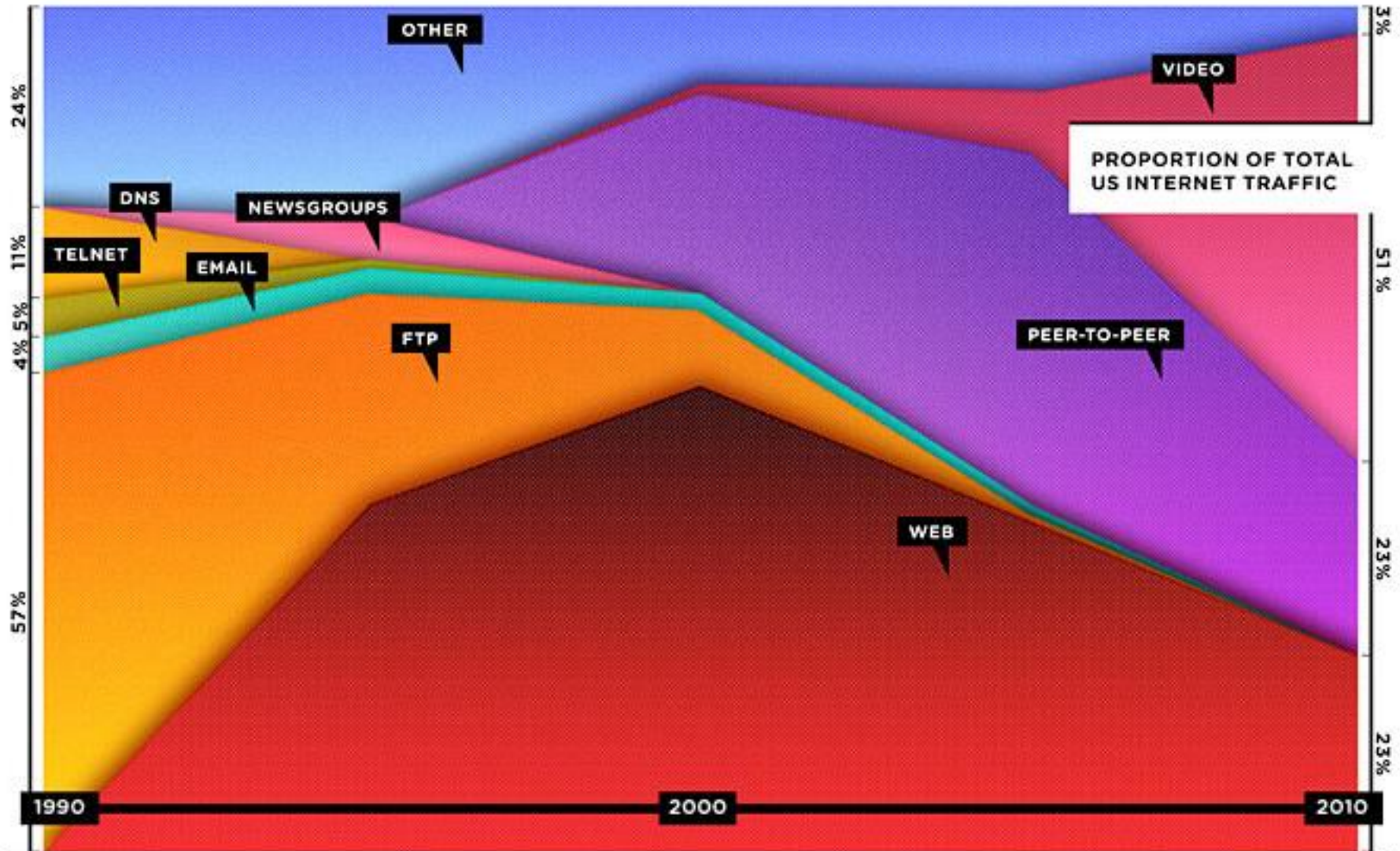
# プロトコルの階層化: 送受信データの流れ



# インターネットにおけるサービス

- ウェブブラウジング (www)
- 電子メール
- ファイル転送 (ftp)
- ソーシャルネットワーキング (facebook, twitter)
- チャット (line, skype, MSN Messenger)
- 電話, テレビ電話 (google voice, skype)
- ショッピング (楽天, amazon)
- ビデオストリーミング (youtube)
- 音楽ストリーミング
- ゲーム
- コンピュータへのログイン (telnet)

# インターネットのトラフィックの変化



Sources: Cisco estimates based on CAIDA publications, Andrew Odlyzko

# 主要なサービス

- 最近はほとんどのサービスがウェブ(標準化された方式)上で動作
  - 基本的なウェブ閲覧(yahoo, Googleの検索画面)
  - ファイル共有, ビデオ閲覧, 音楽ストリーミング(Youtube, radiko)
  - メールサービス(Gmail), ソーシャルネットワーク(facebook, twitter)
  - カレンダー共有
- メール(標準化された方式)
  - Emailの送受信
  - 携帯のメールもemail(SMSを除く)
- P2P(サービス会社によって異なる方式を利用, 標準化されていない)
  - Skype, ファイル共有等
- DNS
  - 直接的なサービスではないが, 多くのインターネットサービスの基盤となるサービス(例: ウェブ, メール)

# インターネットにおける標準化

- IETF (Internet Engineering Task Force) が標準化
  - <http://www.ietf.org/>
  - インターネットのプロトコル等の標準(規格)を決めている
  - 誰でも書ける(オープンなインターネットの象徴)
  - 認められるとRFC (Request for Comments) となる
    - RFCには順番に番号がつく



# アプリケーションのサービスモデル (6.1節)

# アプリケーションのサービスモデル(6.1節)

- インターネット上におけるアプリケーション
  - 複数台のコンピュータ上でアプリケーションプログラムが動作
- サービスモデル
  - クライアントサーバーモデル
  - ピアツーピアモデル

# クライアントサーバモデル

- インターネットのアプリケーションの典型的な構成
  - サーバー：サービスを提供するホスト
  - クライアント：サービス提供を受けるホスト
- リクエスト・レスポンス
  - クライアントはサーバに処理を依頼し，応答を受け取る

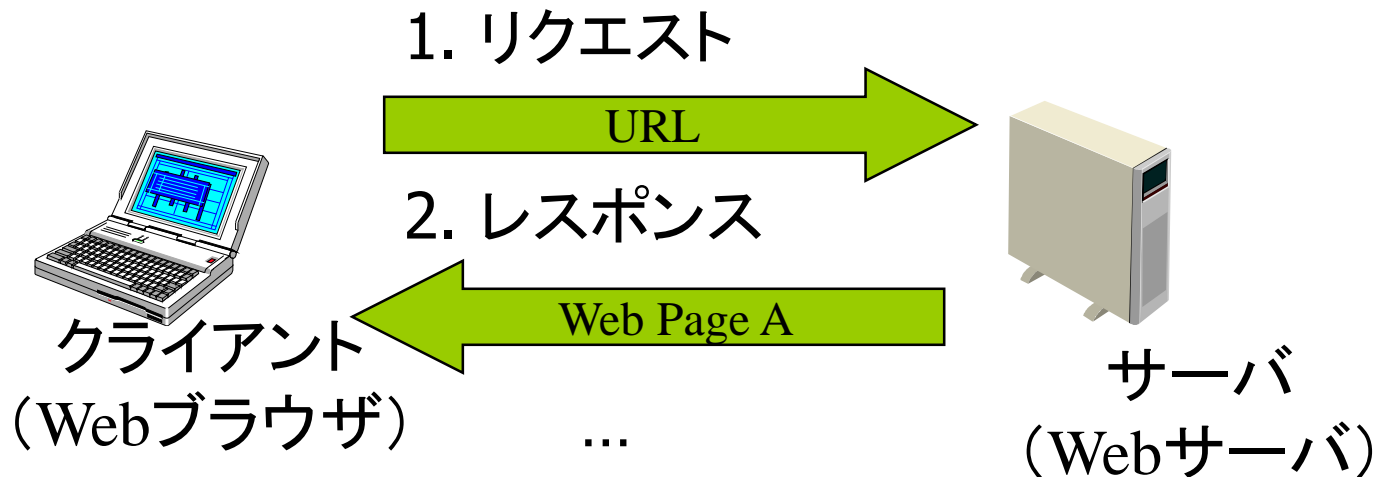
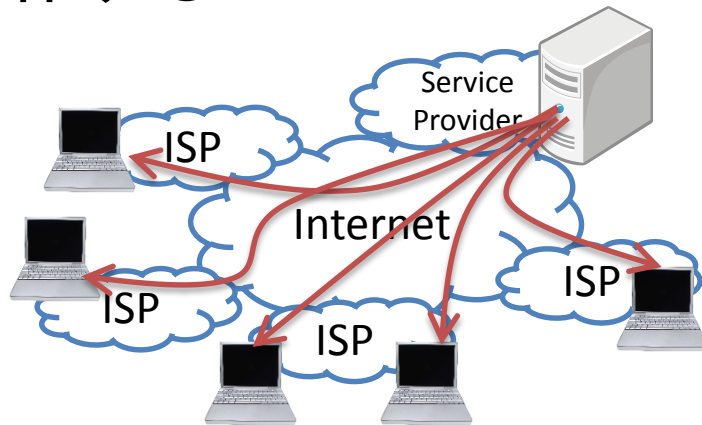


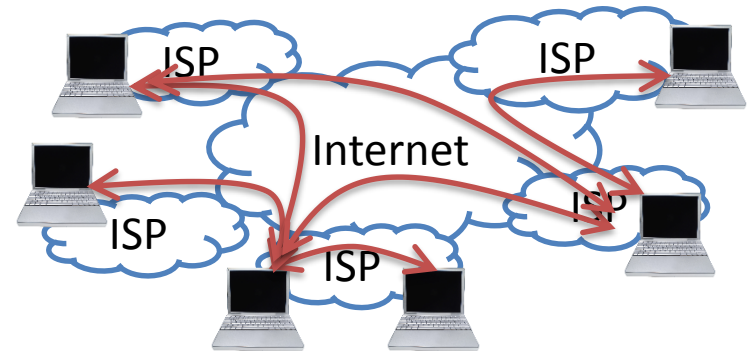
図 クライアントサーバ(Webを例に)

# クライアントサーバ(C/S)と ピアツーピア(P2P)モデル

- ピアツーピアモデルでは、クライアントとサーバの機能が同一のコンピュータに同居し、一体となって動作する



(a) クライアントサーバモデル



(b) ピアツーピアモデル

# ドメインネームシステム (6.2節)

# IP (Internet Protocol) アドレス

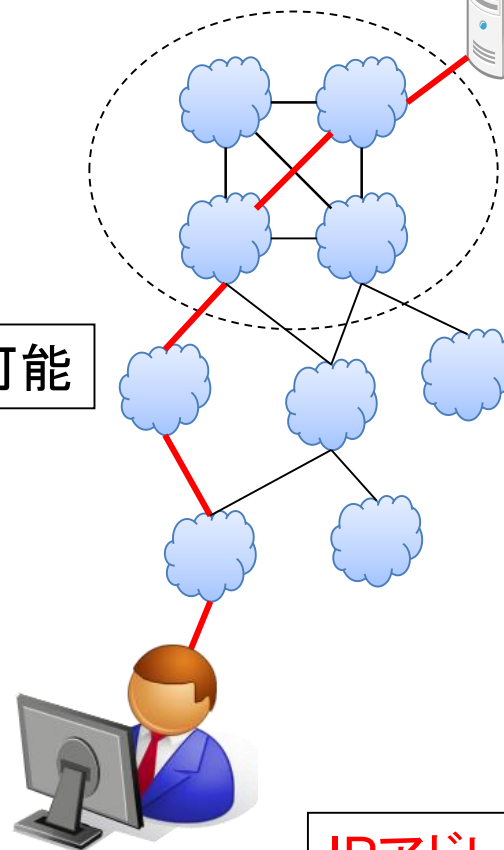
音楽配信用アプリケーション

- インターネット上での通信
  - 通信先のIPアドレス\*が必要

???.???.???.???



通信不可能



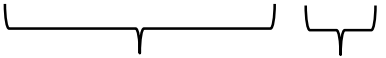
IPアドレス

音楽ダウンロード  
アプリケーション

131.113.10.1

\*資料はIPv4で説明

# IPv4アドレス(復習)

- インターネット上のホストを指定するためのアドレス
- 表記法: 8ビットごとの4つの10進数で表記
  - 例: 131.113.71.3
- IP アドレス = サブネット番号 + ホスト番号
- CIDR (Classless Inter-Domain Routing)
  - サブネット番号のビット長を “/” のあとに明示
  - 例: 131.113.71.3/24 (先頭から24ビットがサブネット番号)  
  
サブネット番号    ホスト番号

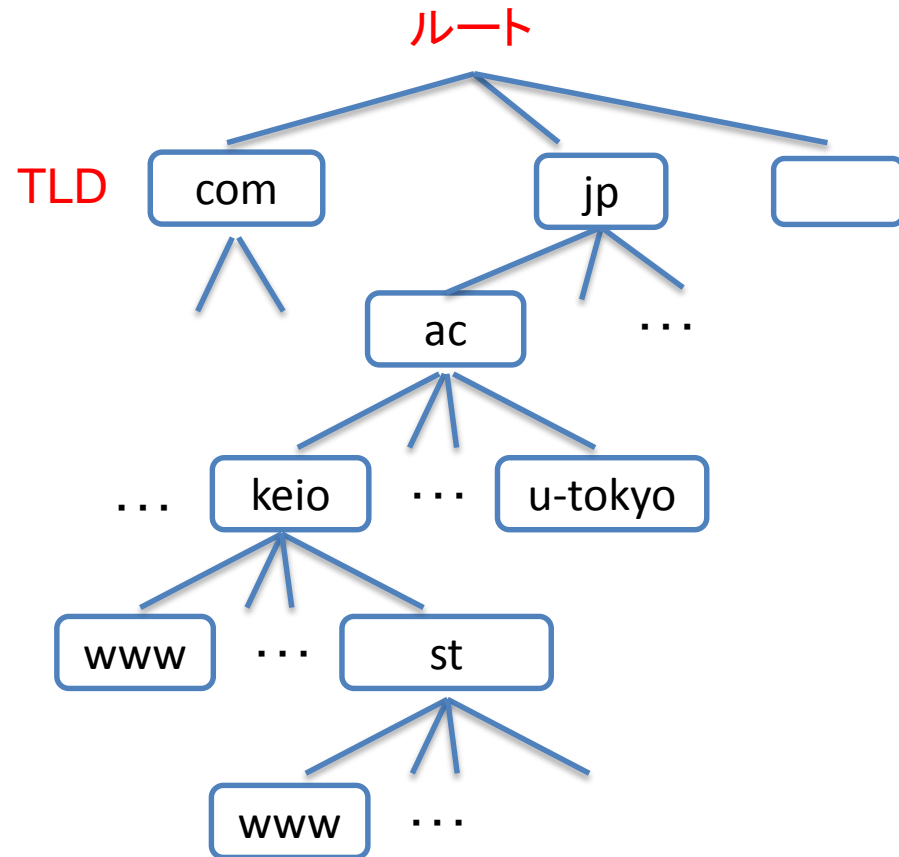
# DNS : Domain Name System

- インターネットのホストを32bitのIPアドレスではなく、人間に分かりやすい名前(ホスト名/ドメインネーム)で呼べるようにする基盤
  - 省略のないホスト名(FQDN) www.st.keio.ac.jp
  - ホスト名をIPアドレスに変換する — アドレス解決
    - www.keio.ac.jp → 131.113.134.20
    - www.kantei.go.jp → 202.232.146.151
- ホスト名とIPアドレスの対応関係を管理する一種の分散データベース
  - ネットワークをドメイン(管理のためのコンピュータの集合)に分割して、情報を管理
  - 各ドメインには管理組織があり、そのドメインに含まれるコンピュータの情報(レコード)を追加・削除・変更
    - レコード: IPv4アドレス(A), ドメイン名(NS), メールサーバ(MX)...



# DNSの仕組み

- 名前空間全体も階層的なドメインに分割して管理
  - 例: www.st.keio.ac.jp
    - 「jpドメインに属するac.jpドメインに属する...wwwというホスト」
  - 最上位: ルートドメイン
- 各ドメインにはDNSサーバ(ネームサーバ: NS)があり, そのドメインに含まれるコンピュータの情報を管理
  - 下位の階層については, 下位のサーバにお任せ
  - 分からなければ, ルートNSから, 下位のNSに順次問い合わせ



# メールの仕組み(6.3節)

# メールアドレス

y-fukuzawa@keio.jp

アカウントの  
ユーザ名

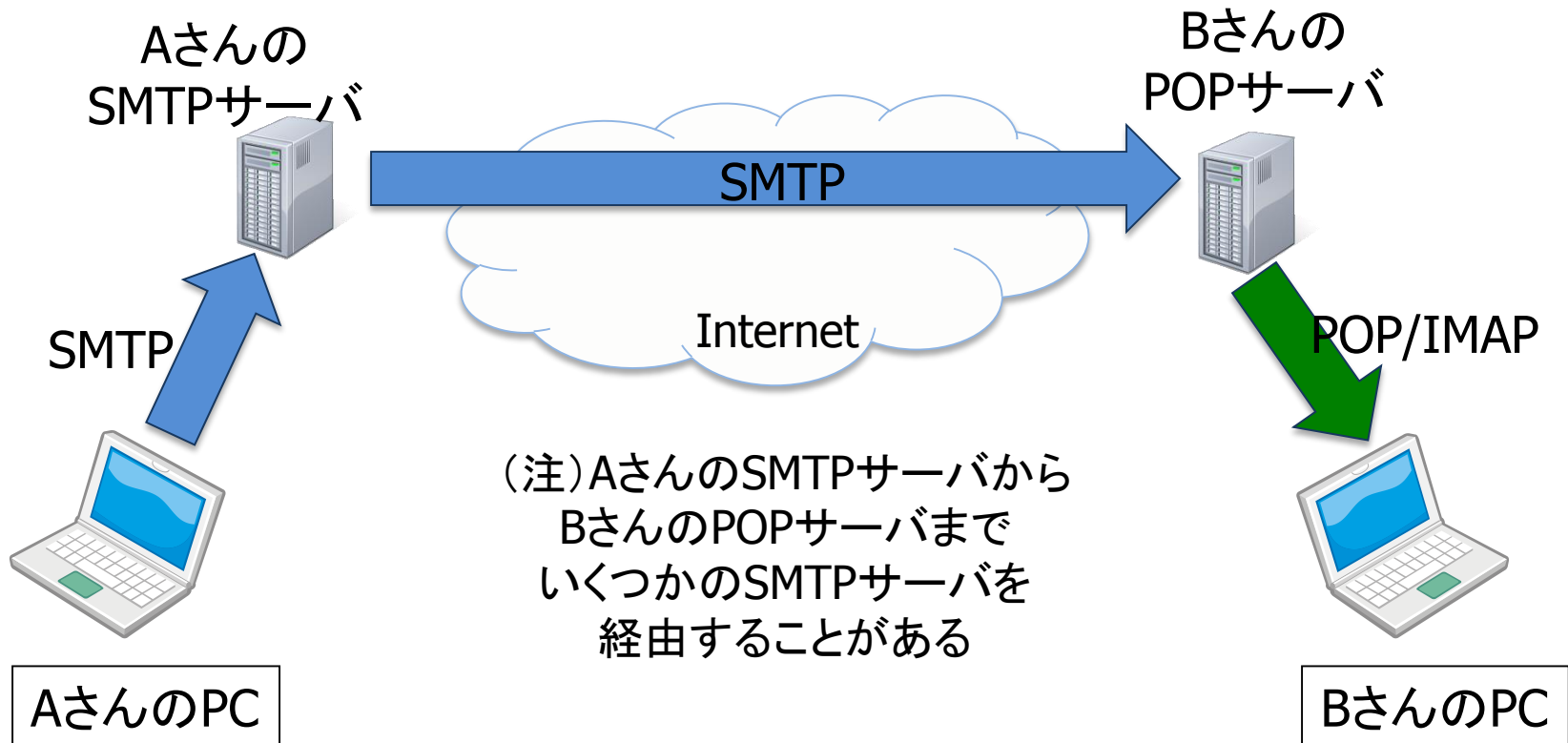
ドメイン部

- ドメイン部 (keio.jp) のメールサーバのIPアドレスをDNSに問い合わせ取得する  
＝「DNSを使って解決」
  - － メールサーバはDNSにおいてMXレコードで記載
- IPアドレスが分かれば、接続してメール転送のプロトコルでやりとり

# メールの仕組み

基本的に平文!!  
(暗号化されて  
いない)

- メールは2種類のプロトコルで成り立っている
  - 送信用プロトコル(SMTP) (送信先を見つけるためにDNSを利用)
  - 受信用プロトコル(POP3, IMAP)



# Webの仕組み(6.4節)

# World Wide Web

- WWWもしくはWebと略される
- ハイパーテキストとインターネットを結びつけた技術
- 1990年スイスのCERN(欧州原子核機構)が開発

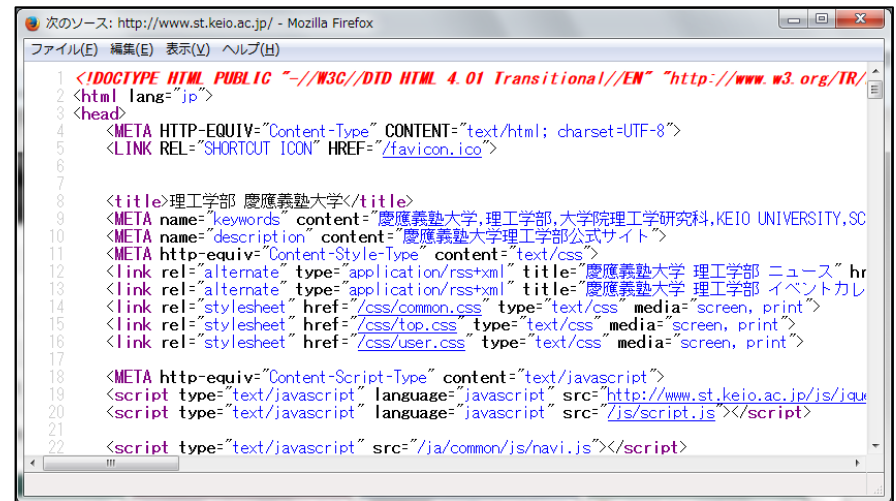
# Web技術

- ハイパーテキスト
  - 情報資源間の関係性, 見やすい表現形式をマークアップランゲージを用いて記述
- TCP/IP
  - 信頼性の高い転送技術の提供
- HTTP
  - Hypertext Transfer Protocol
  - ハイパーテキスト, 情報資源の取得のためのプロトコル
  - アプリケーションレベルのプロトコル
- DNS
  - 情報資源のドメインの名前解決

# ハイパーテキストマークアップランゲージ

ホームページ

ハイパーテキスト  
アップランゲージ





# URI・URL

- URI (Uniform Resource Identifier)
  - インターネット上の情報資源を特定するための書式化 (URLの一般拡張概念)
- URL (Uniform Resource Locator)
  - インターネット上の情報資源の場所の書式化
  - 情報資源を持つホストの場所 + ホスト内での一意な場所による資源特定
- URLの例
  - [http://www.keio.ac.jp/ja/about\\_keio/index.html](http://www.keio.ac.jp/ja/about_keio/index.html)




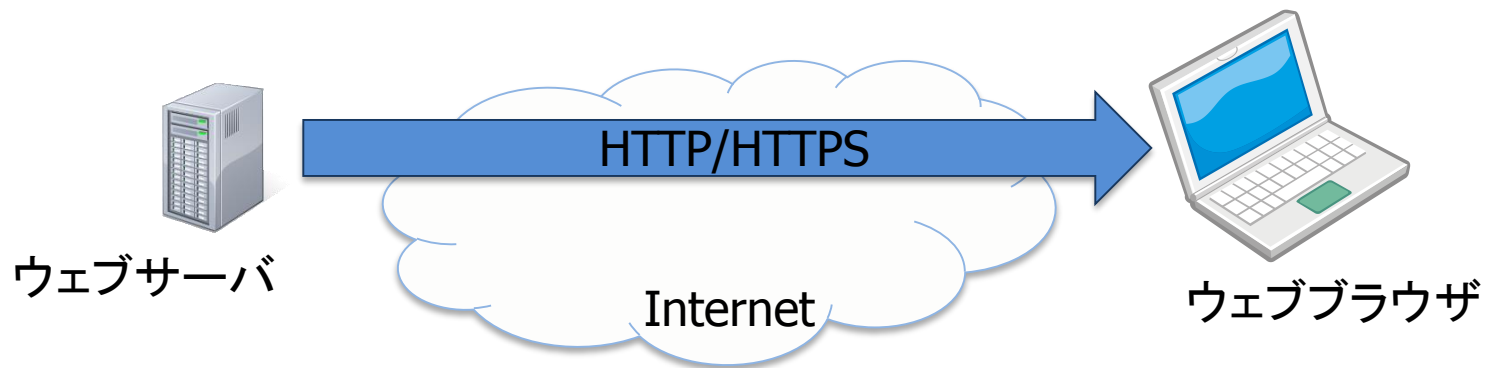
Diagram illustrating the components of the URL `http://www.keio.ac.jp/ja/about_keio/index.html`:

- スキーム** (Scheme): `http`
- オーソリティ** (Authority): `www.keio.ac.jp`
- パス** (Path): `/ja/about_keio/index.html`

- スキーム: アクセスするためのプロトコル (http, https, ftp, etc.)
- オーソリティ: ホスト情報 (ホストにアクセスするための認証情報も含)
- パス: ホスト内でのディレクトリとファイル名による一意な指定

# ウェブの仕組み

- ウェブはHTTP/HTTPSプロトコルを利用
  - HTTP
    - Hyper Text Transfer Protocol
    - ウェブブラウザとウェブサーバ間でのやりとりを決めたプロトコル
  - HTTPS
    - Hyper Text Transfer Protocol over Secure Socket Layer
    - ウェブブラウザとウェブサーバ間でのやりとりを安全性を高めて実現

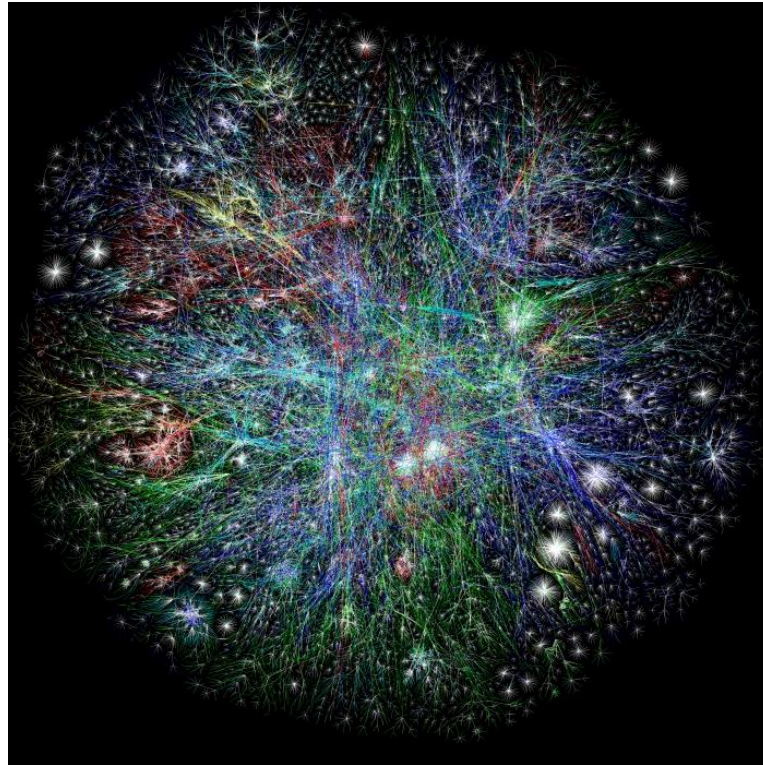


# ウェブを使ったサービス

- URLで指定する情報を多くすることで、複雑な処理を実現
  - 表示ページの指定
  - アカウントの指定
- ソーシャルネットワーキングのサイトでは、ブラウザの画面スクロール状況をサーバに送信して、表示コンテンツ(広告)を変化させている



# インターネットにおけるセキュリティ (6.5節)



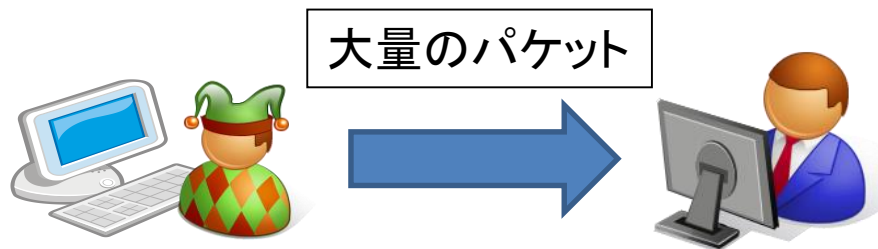
Internet Mapping Project, Bell Labs/Lumeta Corporation

# インターネットの安全性

- インターネットの接続性
  - どこにでも繋がる自由
  - どこからでも繋がる危険
- Ethernetや無線ネットワーク
  - 通信回線を共有(安価)
  - 盗聴が容易
- ファイアウォール(firewall)
  - 防火壁
  - パケットをひとつひとつチェックして不必要と判断したものを遮断
  - パフォーマンスの劣化
  - ファイアウォールのコスト
  - 繋がる自由度の放棄

# セキュリティに関する脅威

- DoS攻撃 (Denial of Service Attack)
  - 大量のパケットを送り、ターゲットのコンピュータの機能を停止させる



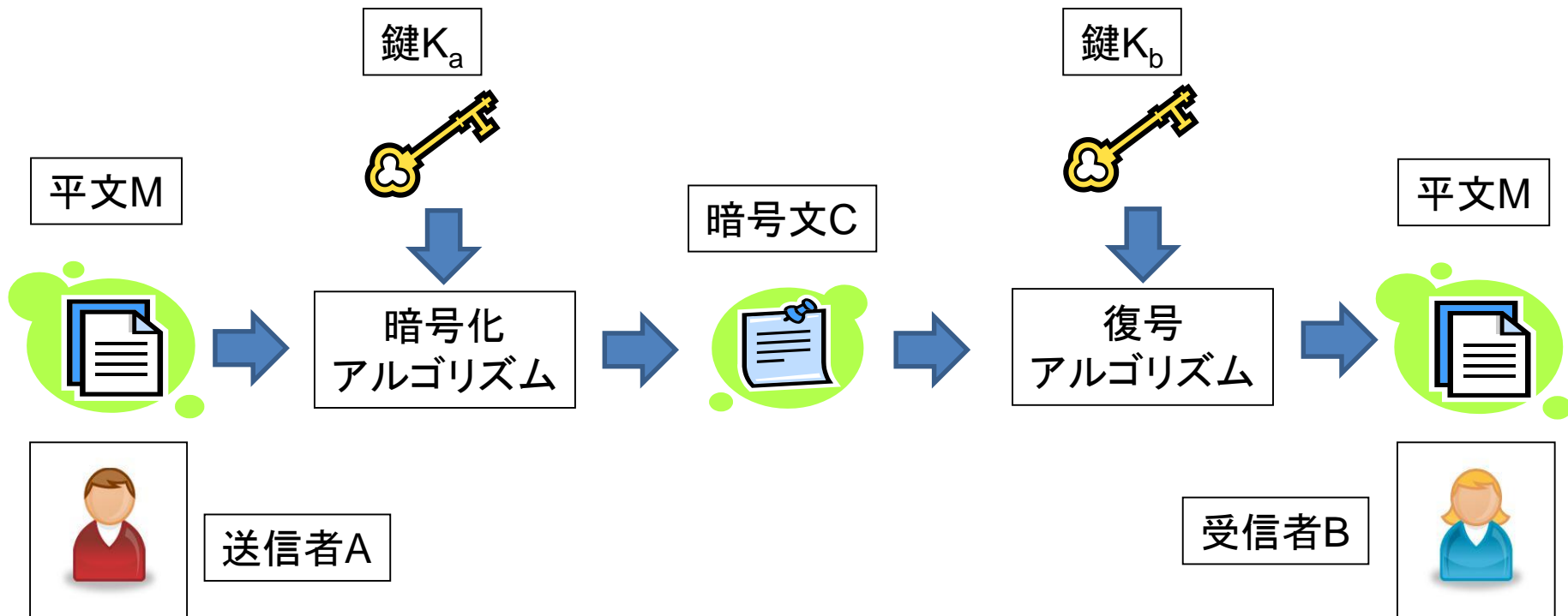
- セキュリティホールからの侵入
- 添付ファイルによるコンピュータウィルスの感染

# 暗号技術の基礎(6.5.1節)

共通鍵(秘密鍵)暗号  
公開鍵暗号

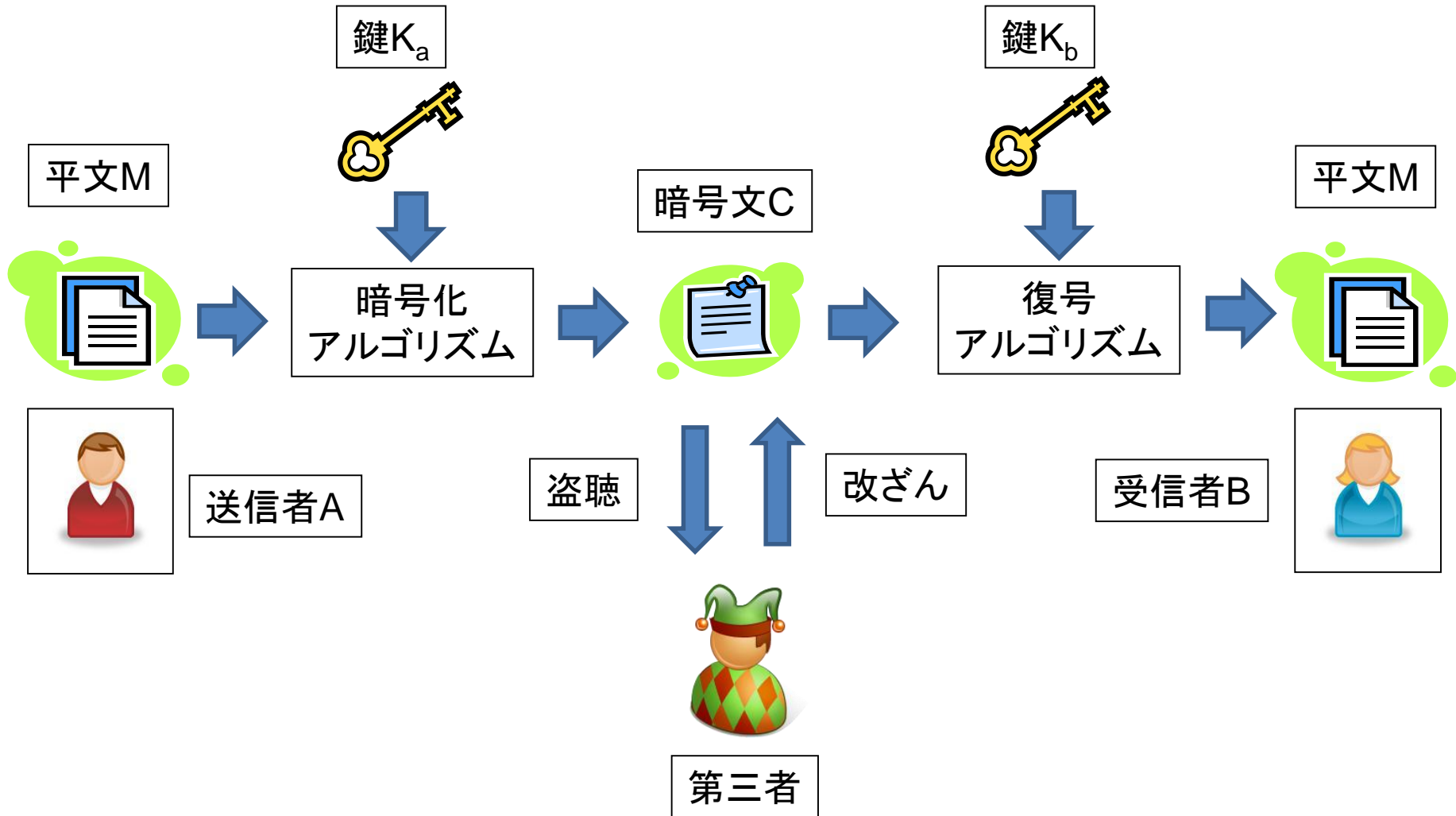
# 暗号①

- 暗号 (cryptograph, cipher)
  - 情報を第三者に理解できない形に変換する技術
  - 情報の機密性を保つ





# 暗号②

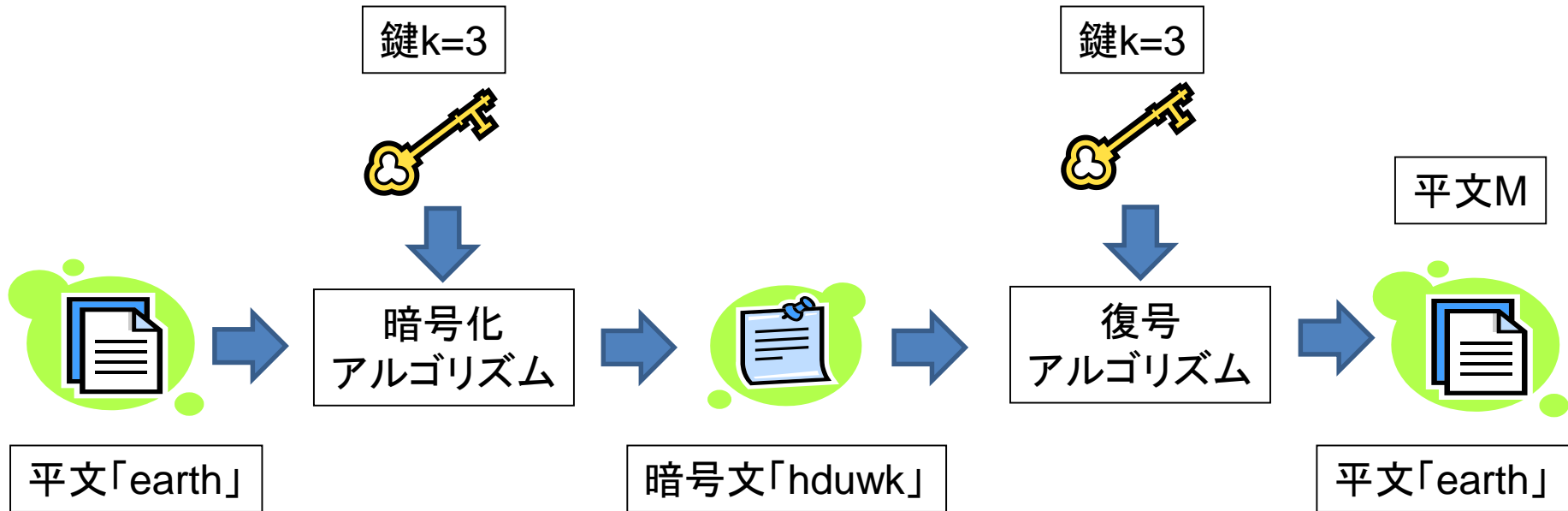


# シーザー暗号①

- 暗号化アルゴリズム
  - 平文の文字をあらかじめ決められた文字数 $k$ だけずらす(シフトする)
- 暗号鍵 $k$ 
  - 平文の文字がアルファベット小文字26文字
  - $k=3$ の場合

平文	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
暗号文	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

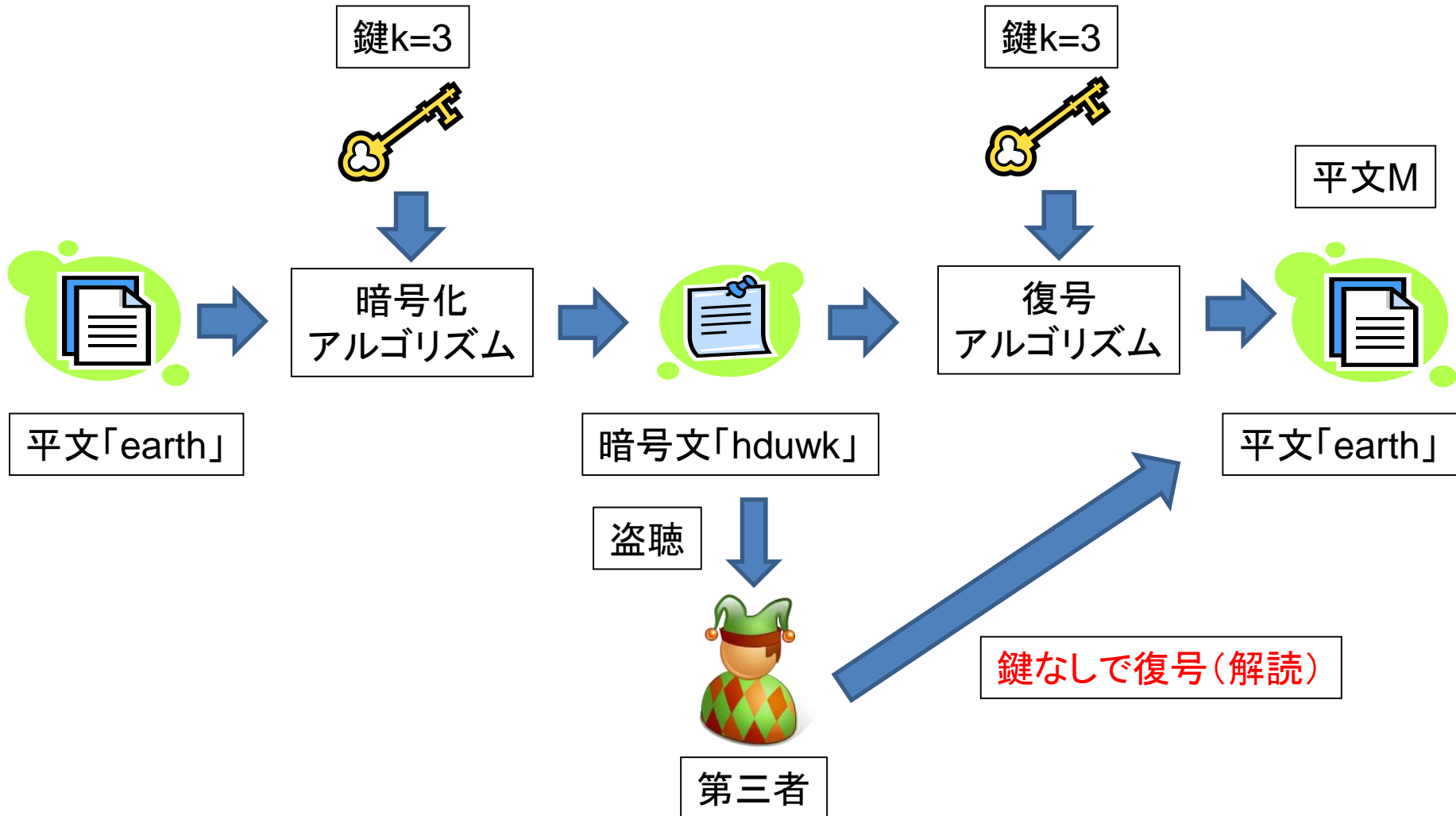
# シーザー暗号②



K=3の場合

平文	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
暗号文	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

# シーザー暗号③



# 暗号強度

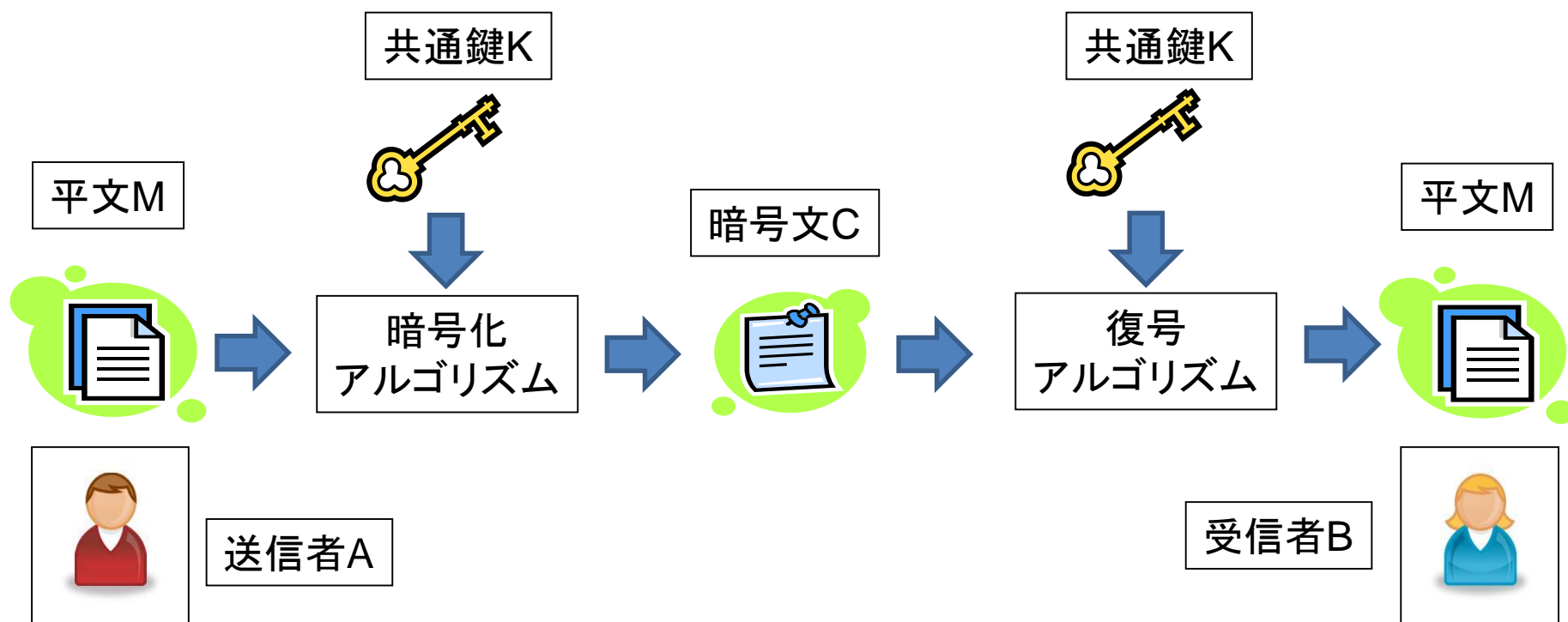
- シーザー暗号
  - 平文がアルファベット小文字26文字の場合
  - 鍵 $k=1\sim 25$ を試すことにより解読可能
- 暗号強度
  - 暗号の解読の難しさを暗号強度と呼ぶ
  - 同じ暗号方式の場合, 鍵の組み合わせの多い方が解読が困難

# コンピュータネットワーク上でのセキュリティ技術

- 計算量的安全性
  - 暗号化された文書をコンピュータを用いて解読するために必要な時間(計算量)
  - 解読に要する時間が大きい程, 暗号化は安全
  - コンピュータ技術の進歩にともない, セキュリティ技術も向上させなければならない

# 共通鍵暗号（秘密鍵暗号）①

- 暗号化と復号化で、同じ鍵を用いる
- 共通鍵は送信者，受信者のみで共有し，第三者には秘密にする（秘密鍵暗号）



# 共通鍵暗号(秘密鍵暗号)②

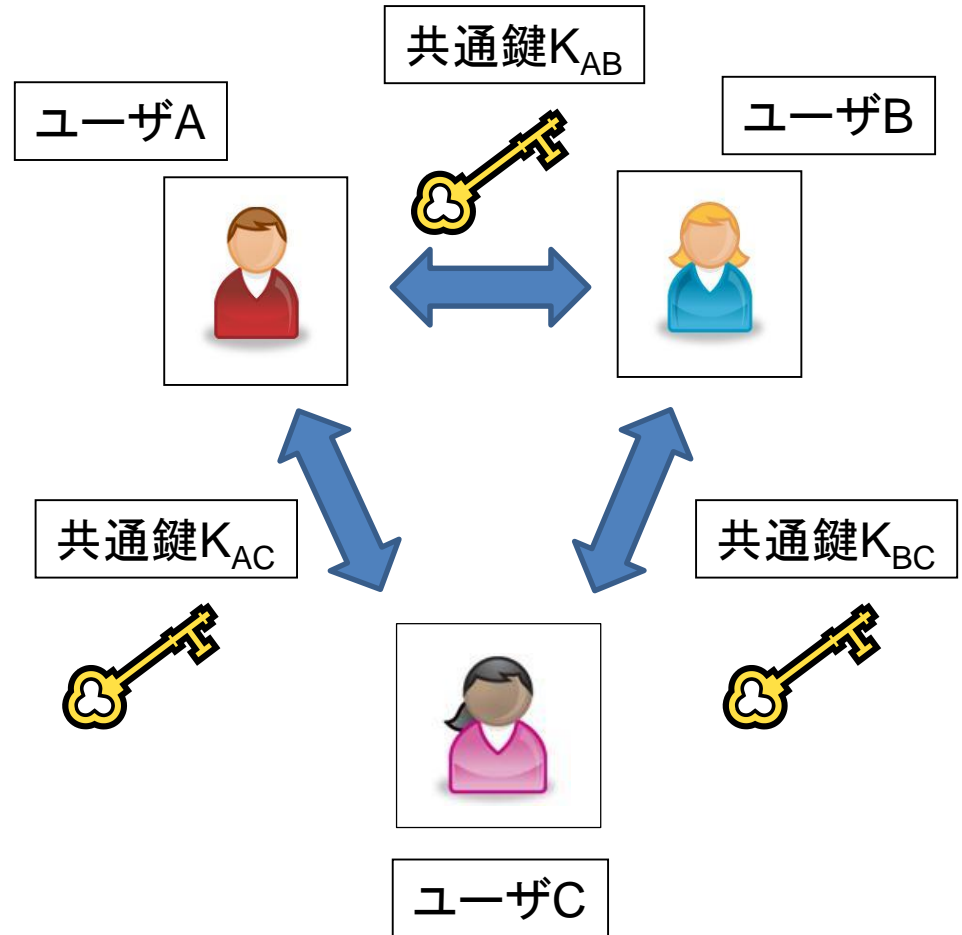
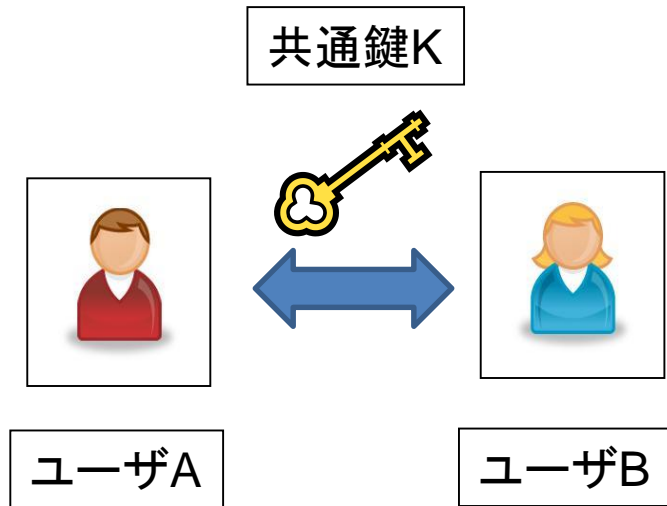
- 長所
  - 高速に大量の情報の暗号化が可能
- 短所
  - 鍵の交換方法
  - 鍵配送問題



# 鍵配送問題

二人の場合

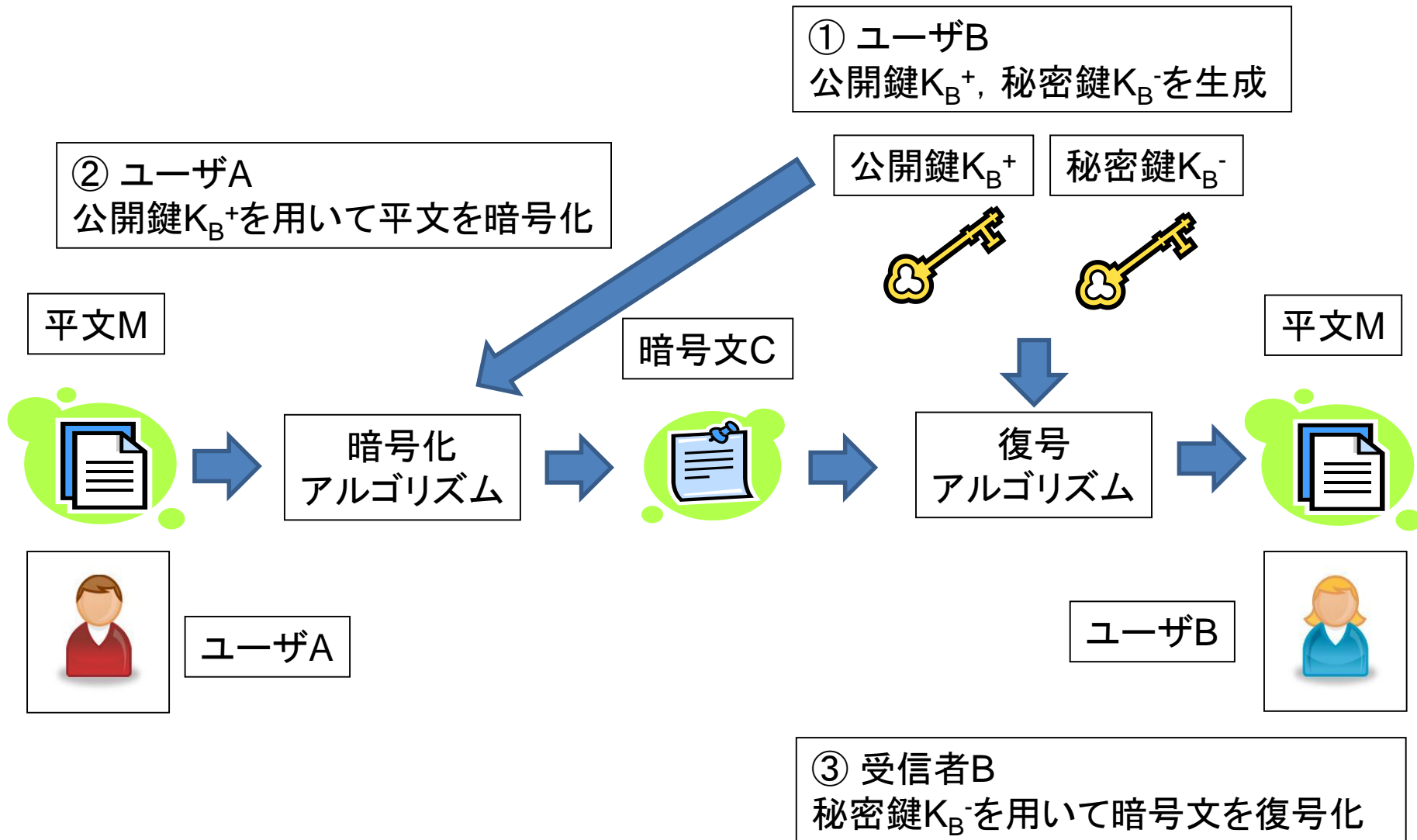
三人の場合



# 公開鍵暗号①

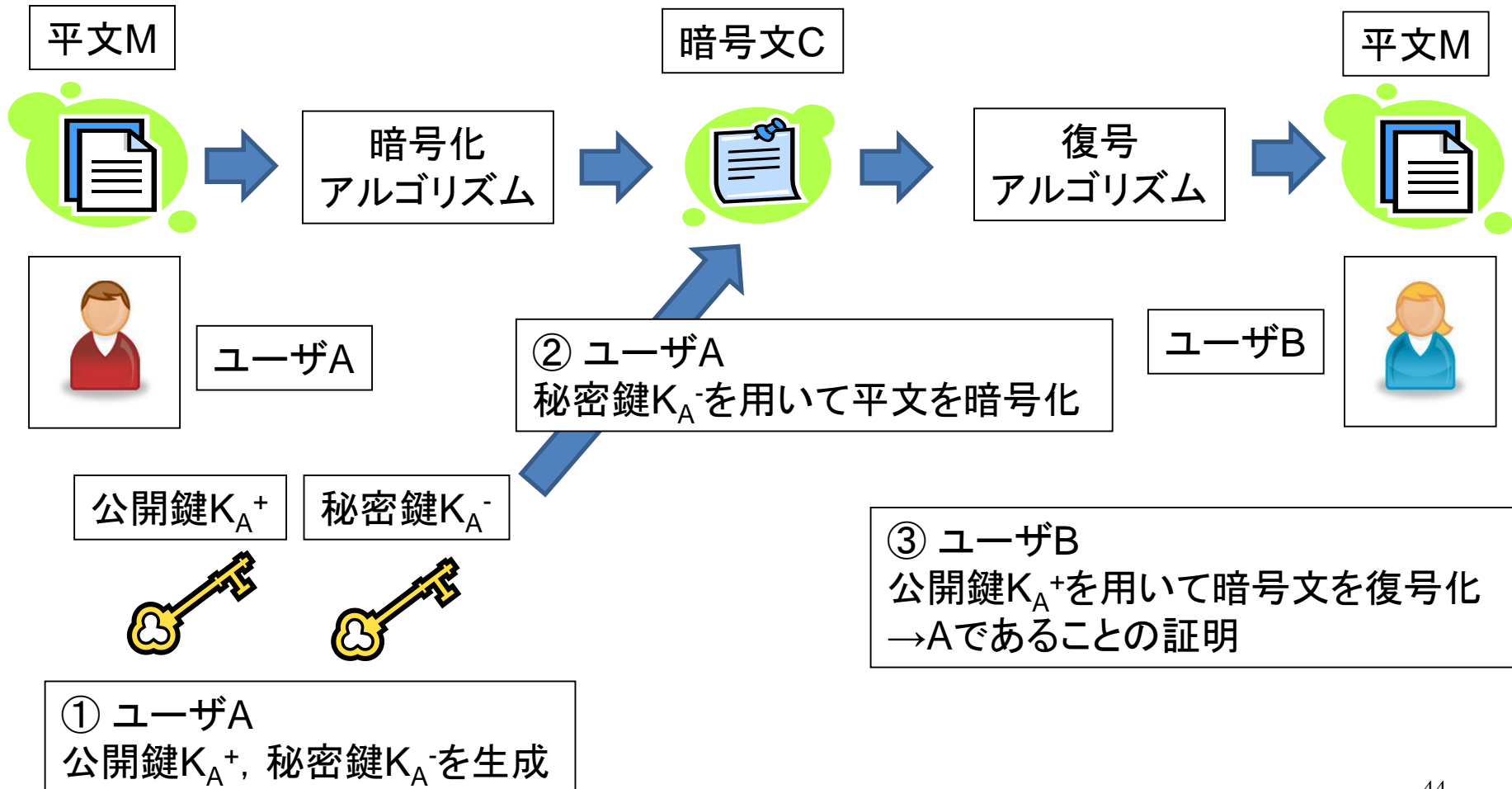
- 公開鍵暗号
  - 二つの鍵の組 $k^+$ ,  $k^-$ を用いる
  - 一方の鍵を用いて生成した暗号文は、他方の鍵を用いて復号できる
  - ただし、一方の鍵から他方の鍵を推測することは困難
  - 二つの鍵の一方を公開(公開鍵 $k^+$ )、他方を秘密(秘密鍵 $k^-$ )とする
  - 暗号化アルゴリズム、復号化アルゴリズムは公開されている

# 公開鍵暗号②



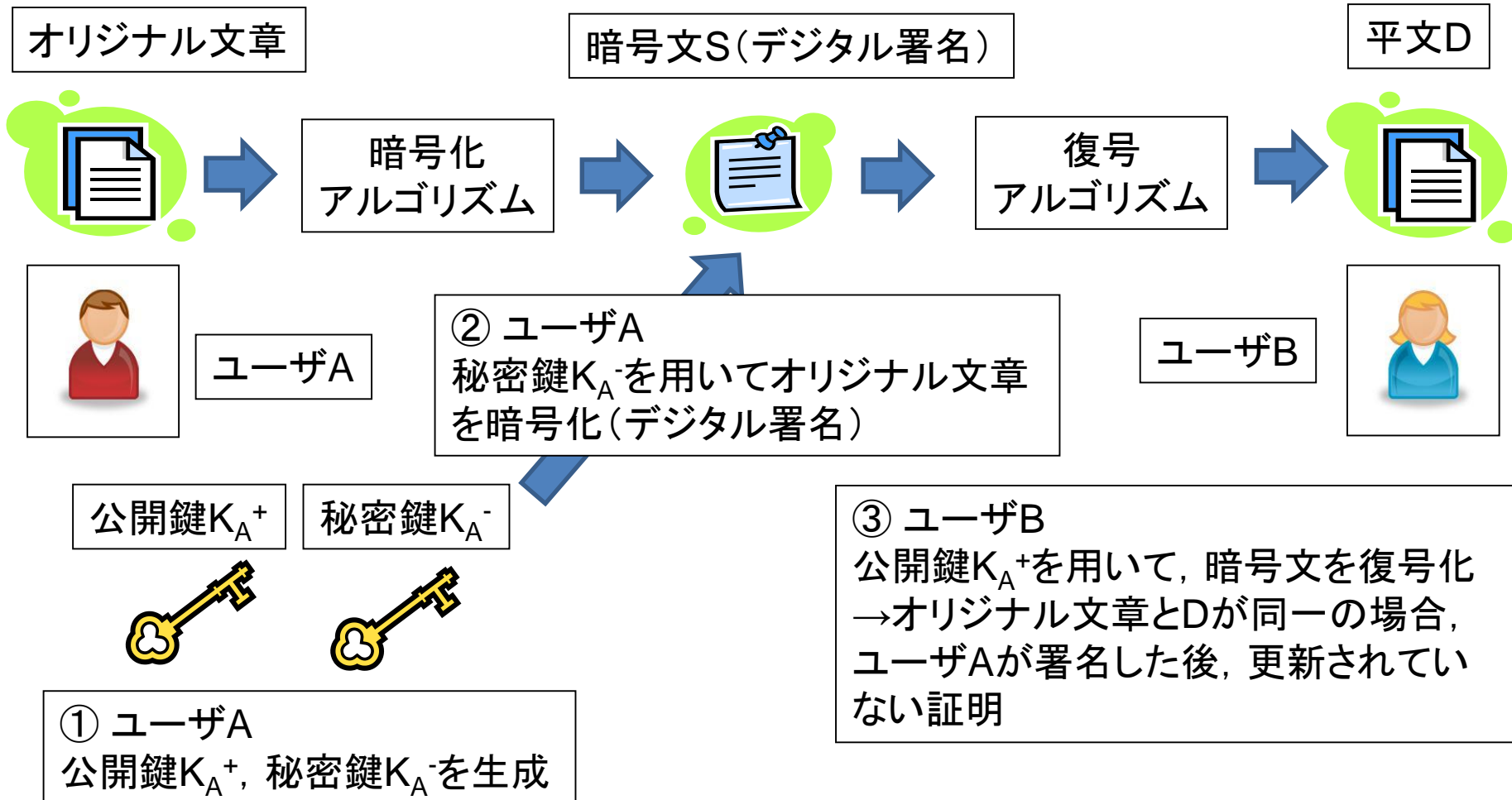
# 応用①(認証)

- ユーザAが自分自身を証明するためには？



# 応用②(デジタル署名)

- オリジナル文章が改ざんされていないことを証明するためには？



# 情報セキュリティ(6.5.2節)

情報システムに関する危険  
情報セキュリティの要素

# 情報セキュリティ

- 現在の情報機器は、一般にオープンなインターネットに接続
  - オープン = 誰もがアクセスでき、厳密にコントロールされていない
- 情報セキュリティ
  - 情報と情報システムを、さまざまな危険から守ること
  - 組織(会社や学校)だけでなく、個人でも重要

# 脆弱性(vulnerability)/セキュリティホール

- 情報システム, ネットワーク, ソフトウェア等の安全性を損なう弱点
  - 脆弱性を悪用することで, システムの安全性を損なうことができる(かも) = セキュリティ上の攻撃
- さまざまな脆弱性
  - 設計上の脆弱性
  - 実装上(作り方)の脆弱性
  - 運用上の脆弱性
    - システムの管理や利用法に起因する弱点



# 脅威(threat)①

- 情報や情報システムの安全性を損なう要因を脅威と呼ぶ
- 盗聴
  - ネットワーク上を流れる情報を第三者が不正に取得する行為
- 情報漏えい:
  - 組織や個人の機密情報が、持ち主の意図に反して、権利のない第三者に渡ること
- なりすまし
  - 他人のID, メールアドレス, ネットワーク上の呼称(ハンドル)などを詐称し, 他人のふりをして, 不正に情報やシステムを使用すること

# 脅威(threat)②

- 改ざん
  - 第三者によって不正に情報が書き換えられること
- 不正アクセス:
  - 本来システムを使用する権利がない第三者が不正にシステムにアクセスすること
  - 情報漏えい, 改ざん, サービス停止, 情報やシステムの破壊などにつながる恐れがある.
- コンピュータウィルス
  - コンピュータ間に伝染し, ある期間潜伏した後, 何らかの問題を引き起こす(発病する)プログラム

# 情報セキュリティの要素

- 情報のCIA
  - 機密性(confidentiality)
  - 完全性(integrity)
  - 可用性(availability)
- 加えて...
  - 真正性(authenticity)
  - 責任追及性(accountability)
  - 否認防止(non-repudiation)
  - 信頼性(reliability)

# 情報のCIA ①(機密性)

- 情報が許可された個人や組織だけで、保持、利用されていること
  - (例) 許可されていない第三者には、開示されない&利用できないように維持されている
  - (例) 個人の医療情報(カルテの情報)
  - 本人、診察する医者は見ることできる
- 機密性を維持するために、情報の暗号化が利用される

# 情報のCIA②(完全性)

- 情報が正確に完全な状態で維持されること
  - 情報の一部がわからないように書き換えられたりしない
- (例) 契約書
  - 契約の関係者が合意した時点の内容が完全に維持される必要がある。合意の後で、一部が書き換えられてはならない
- (例) コンピュータのプログラム
  - 動作や安全性を確認したプログラムが維持されなければならない

# 情報のCIA③(可用性)

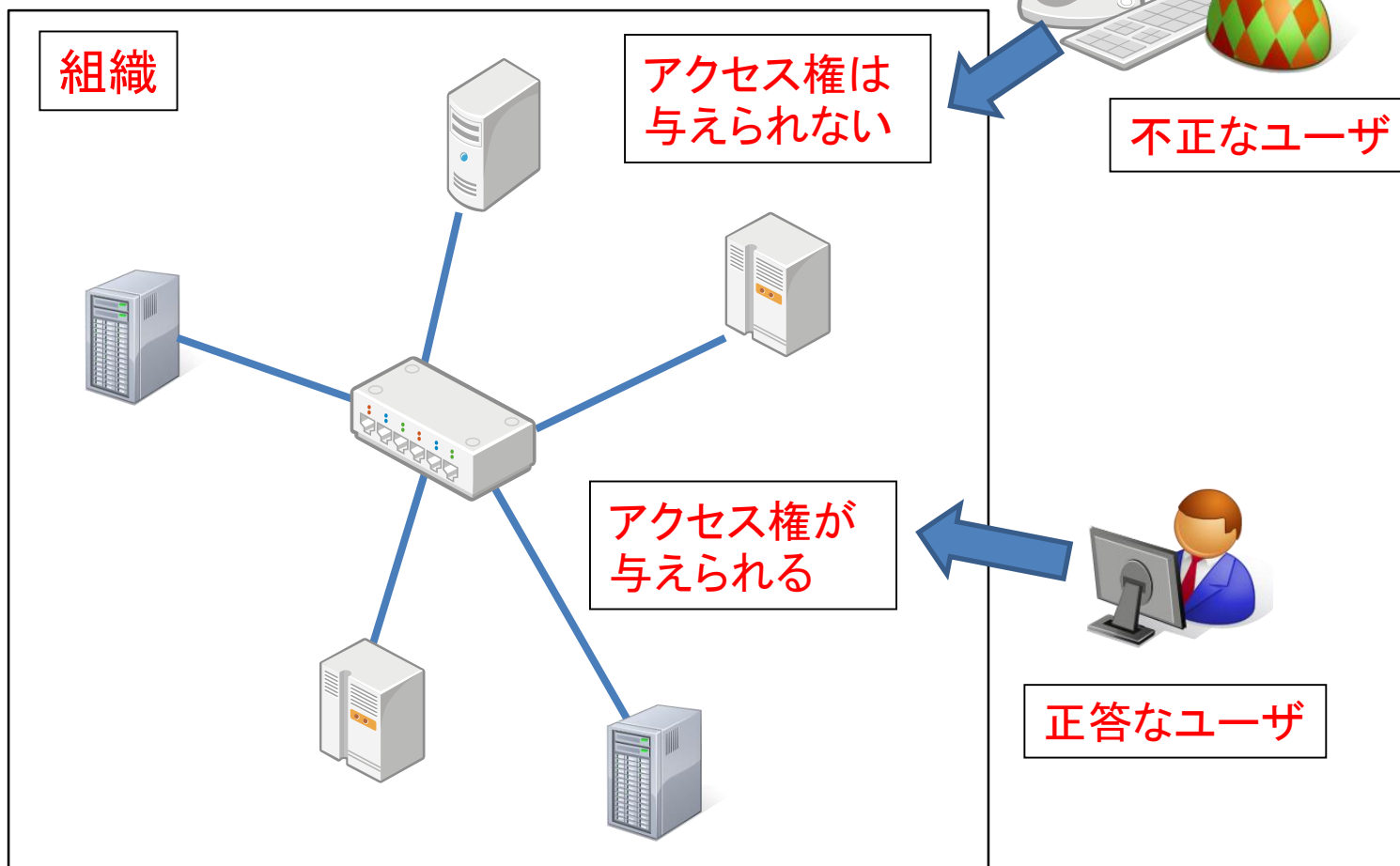
- 許可された個人や組織が望むときは、いつでも利用できること
- 情報システムを脅威から守り、常に正しく動作するように維持する必要がある
  - セキュリティ上の攻撃への対策
  - システム故障への対策, 故障からの迅速な復旧

# その他の情報セキュリティの要素

- 真正性
  - 情報などが主張通りに正しくそのものであること
- 責任追及性
  - 情報処理や発生した事象について、理由や過程を説明できること
    - システムはログと呼ばれ記録を保存している
- 否認防止
  - 後から、行為や情報の内容を不正に否認すること
- 信頼性
  - 情報システムや情報処理の動作、プロセス、結果が意図した通りのものであること

# アクセス権（権限）①

情報システム





# アクセス権(権限)②

- アクセス権の適用
  - ファイル, コンピュータ, ネットワーク, システム
- アクセス権のレベル
  - 作成, 閲覧, 変更
  - (例)成績データ
  - 教師:成績の決定, 変更, 閲覧
  - 学生:閲覧
- 情報システムは, 誰が正当なユーザなのかと, そのユーザに許可される権限を管理している

# 認証①

情報システム

組織

認証  
偽のユーザID, パスワード

アクセス権は  
与えられない

アクセス権が  
与えられる

認証  
ユーザID, パスワード

不正なユーザ

正答なユーザ

# 認証②

- 自分が自分であることを証明するためには？
- 現実の世界
  - 身分証明書
- 情報システム
  - ユーザID, パスワード
  - 生体情報(指紋, 虹彩, 静脈)認証

# デジタル署名

- 文書とプログラムが確かに本物であり, ある時点から変更されていない(改ざんされていない)ことを示すための情報
- (例) デジタル署名をつけた電子メール
  - 送信者や内容が確かに記された通りであることが保証
  - 内容が改ざんされていないことが保証

# 本日のまとめ

- インターネット2: アプリケーション
  - アプリケーションのサービスモデル(6.1節)
  - ドメインネームシステム(6.2節)
  - メールの仕組み(6.3節)
  - Webの仕組み(6.4節)
  - インターネットにおけるセキュリティ(6.5節)
- 次回は8章を読んでください
  - 第三回課題の提出も忘れずに