コンピュータ・サイエンス2

第9回
情報ネットワーク(続き)

人間科学科コミュニケーション専攻
白銀 純子

今回の内容

- 情報ネットワーク(続き)
  - LAN
  - IPアドレス
  - DNS
  - 経路制御
  - インターネット上のアプリケーション
  - セキュリティ

設問1

- 下記の文章のを埋めなさい。

人間が作るプログラムを(ア)と呼ぶ。(ア)をコンパイルすると、(イ)ができる。
(イ)は(ウ)語に翻訳されたプログラムである。

解答:

(ア) ソースコード
(イ) 実行可能プログラム
(ウ) 機械

設問2

- オープンソースのアプリケーションについて、どんなメリット・デメリットがありそうか、考えなさい
  - 不具合の修正の早さ以外で

解答例(メリット):

- 無料で使えるものが多い
- プログラミングができる人であれば、自分でカスタマイズができる
- 様々な人が見るので、比較的品質が良い

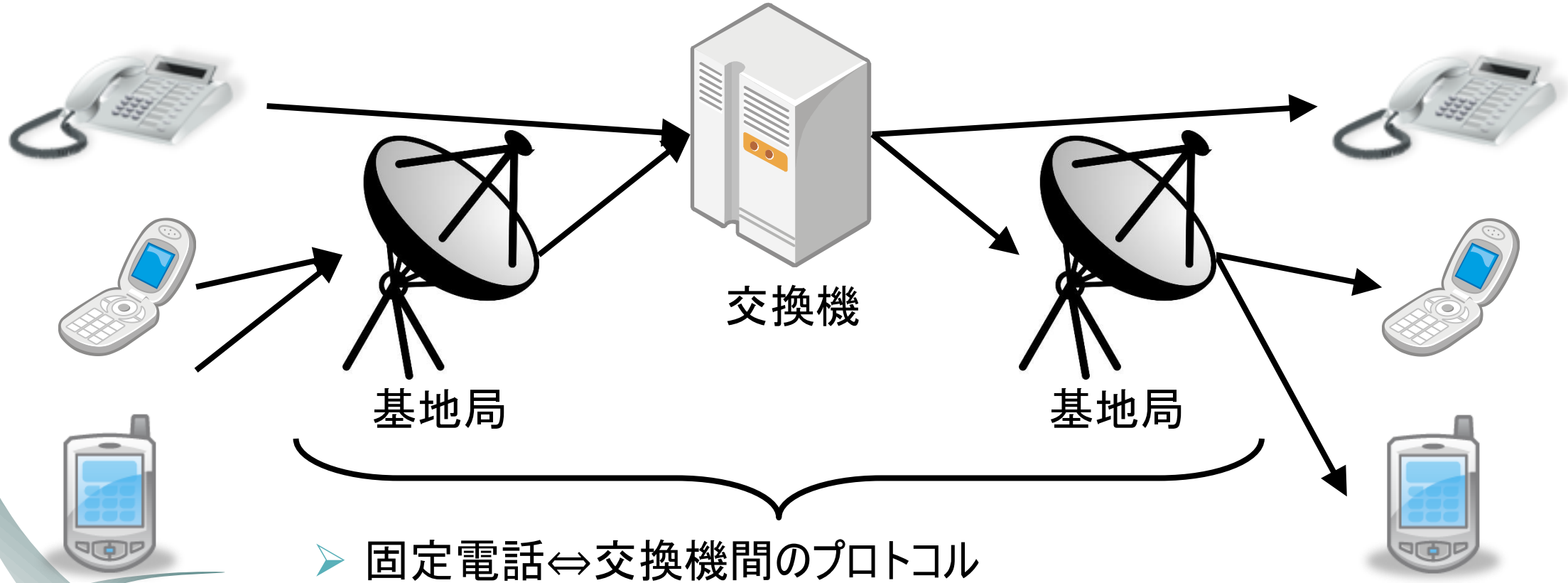
解答例(デメリット):

- トラブルが起こったときに責任を取ってもらえない
- マニュアルなどが整備されていないことが多い
- メンテナンスをきちんとしてもらえないことがある(特にマイナーなソフトウェアの場合)

前回の質問の回答

仮想化～電話を例にして考えると…～[1]

- 相手先に声が届くまでに、様々なプロトコルが使われている

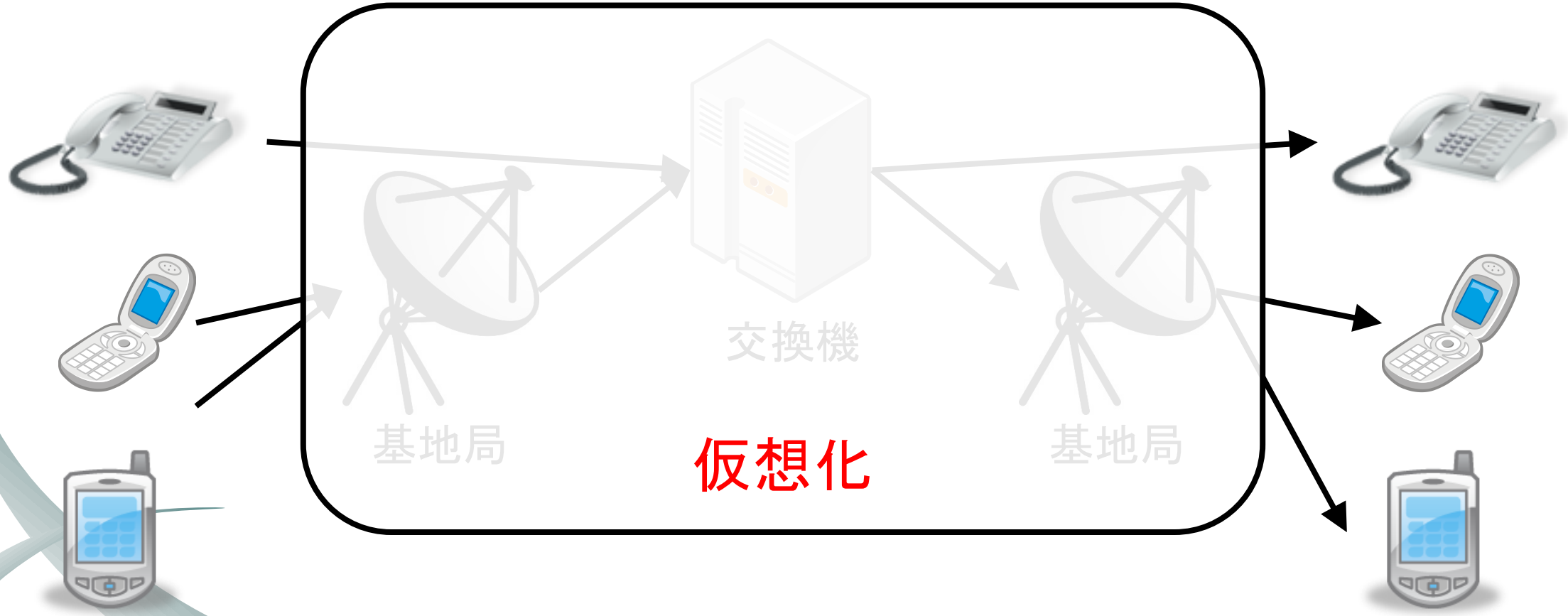


- 固定電話⇔交換機間のプロトコル
- 携帯電話・スマートフォン⇔基地局間のプロトコル
- 基地局⇔交換機間のプロトコル, etc.

仮想化～電話を例にして考えると…～[2]

- 実際は、どのようなプロトコルが使われているかを意識することはない

利用者には見えなくしている(利用者が意識しなくても良いようにしている)



Question!

前回の復習

情報ネットワーク

現代の情報ネットワーク[1](p. 89)

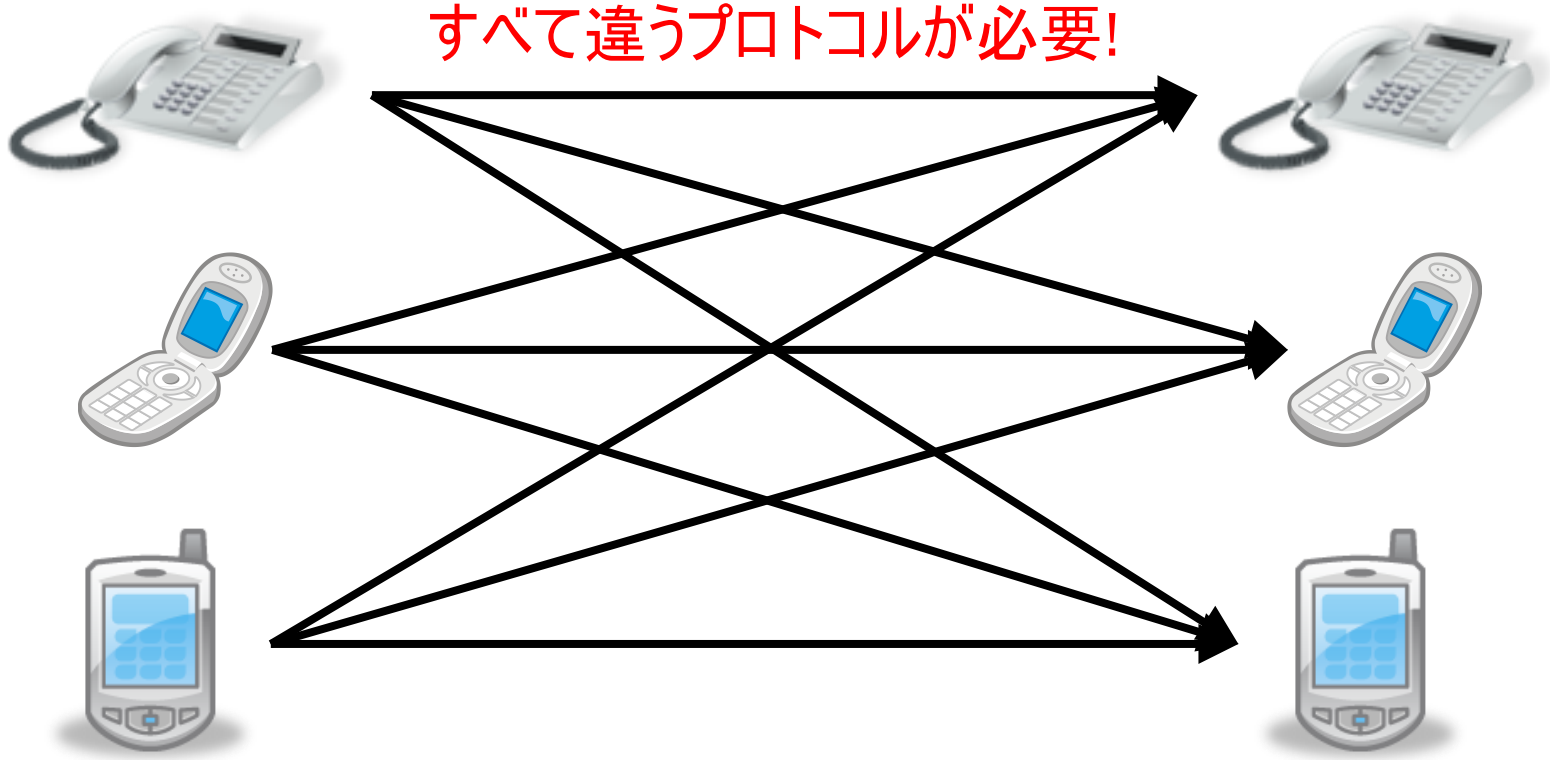
- 電気通信技術とデジタル化技術の組み合わせ
  - 文字・音声・画像などの情報をデジタル情報として扱い
  - 高速性・信頼性・経済性・利便性など、多くの利点
- 通信路(伝送路)によって、情報を伝達
  - 伝送媒体や通信機器などで構成
  - 多数の約束事(通信プロトコル)が必要
    - 通信路に正しく情報をのせ、届いた情報の意味を正確に理解するため
  - 多種多様な情報を、情報ごとに目的の場所に届けるための交換機能も必要
    - どこに届けるかを識別し、選択するための仕組み

現代の情報ネットワーク[2](p. 90)

- 通信路
  - 銅線・光ファイバ・電波などの伝送媒体を適材適所で組み合わせ
  - 伝送媒体同士をつなぐ通信機器
- 交換機能
  - 複数の利用者が共通の通信路を共有し、伝送先に対応した通信路を選び、信号を通過させる仕組み
    - あらゆる通信相手との間に専用の通信路を設けるのは不可能なため
- 通信プロトコル(通信をするためのルール)
  - 電気信号を伝えるためのケーブルの材質やコネクタの形状
  - 信号の種類や大きさ、意味, etc.

仮想化[1](p. 91)

- 利用者側として、利用する通信に必要なプロトコルをすべて使うのは面倒
  - Ex. 固定電話から固定電話へのプロトコル, 携帯電話から固定電話へのプロトコル, etc.



仮想化[2](p. 91)

- 自分の身近な部分だけ扱い方を知っていればOK
  - Ex. 電話のかけかた(電話番号のボタンを押す)
- それ以外の部分は、利用者からは隠して、統一化しているように見せかけ(仮想化)

階層化(p. 91)

- 正常に利用できているときには仮想化は便利
- 問題が起こった時や別の使い方を考えるときなどにはプロトコルの深い理解が必要

階層化

- ネットワークを機能別に分割し、それぞれを独立して扱えるようにする
  - ✓ プロトコルも機能ごとに分類する
- 各機能を順番に実行すれば、通信できるようにする

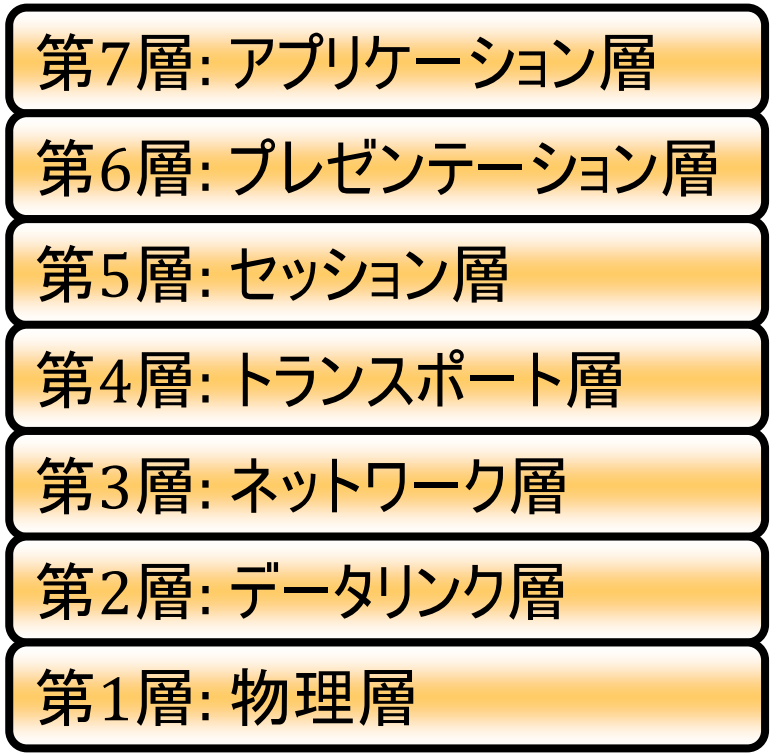
階層化により…

- 故障した時の機器の入れ替えなどがしやすくなる
- 機能の変更をする時に、その機能の前後の機能のみ注意すれば良い
  - ✓ 変更の影響を少なくできる

OSI参照モデル

OSI参照モデル(p. 94)

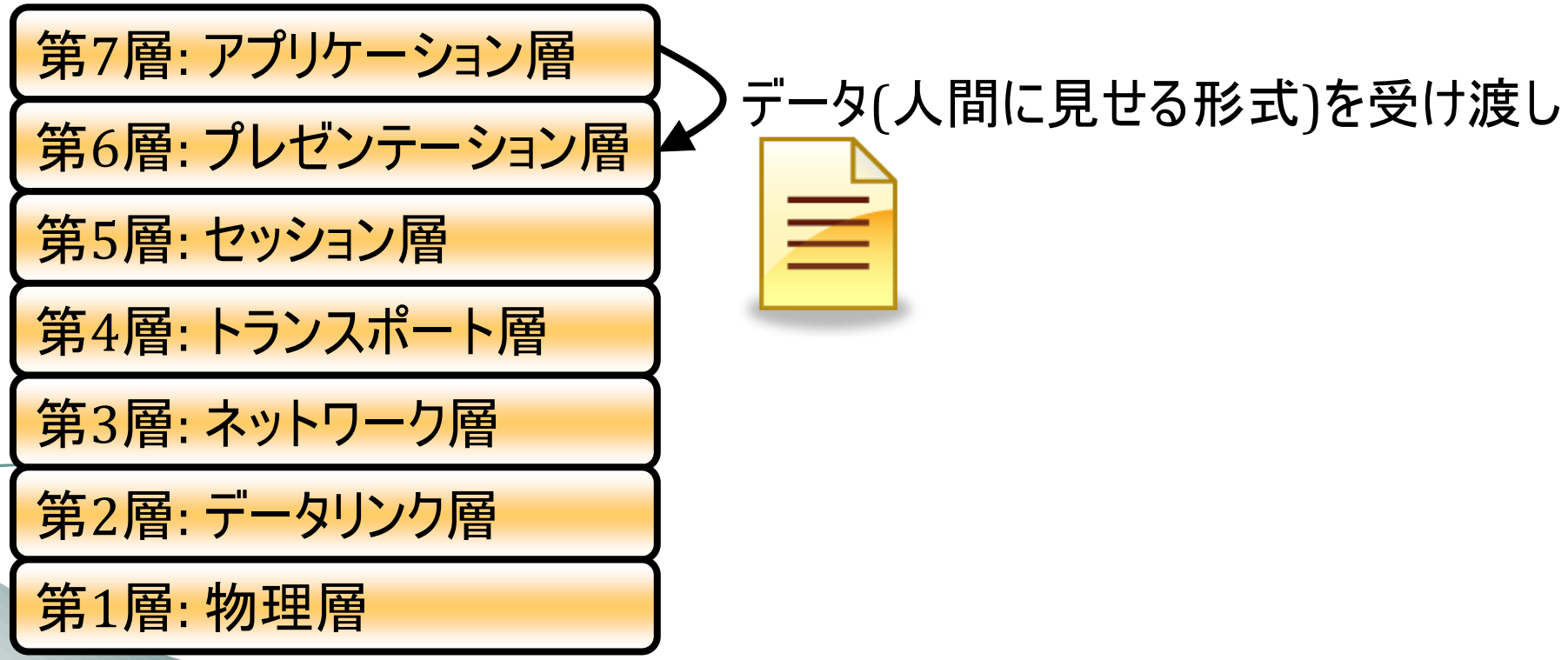
- コンピュータの通信機能を7つの階層に分割したモデル
  - 各階層ごとに必要なプロトコルを定義
  - 実際に使われるモデルは、OSI参照モデルをもとに規定



データの送信(p. 94)

データ送信[1](p. 94)

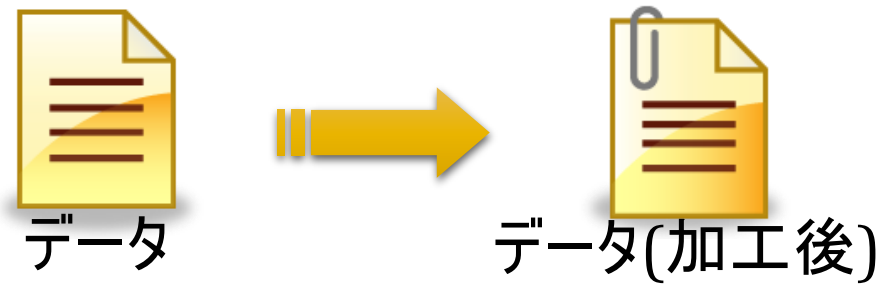
- アプリケーション層の役割: 人間が直接接するアプリケーション部分の規定
  - 具体的な通信サービスの提供(メールやWebなど)



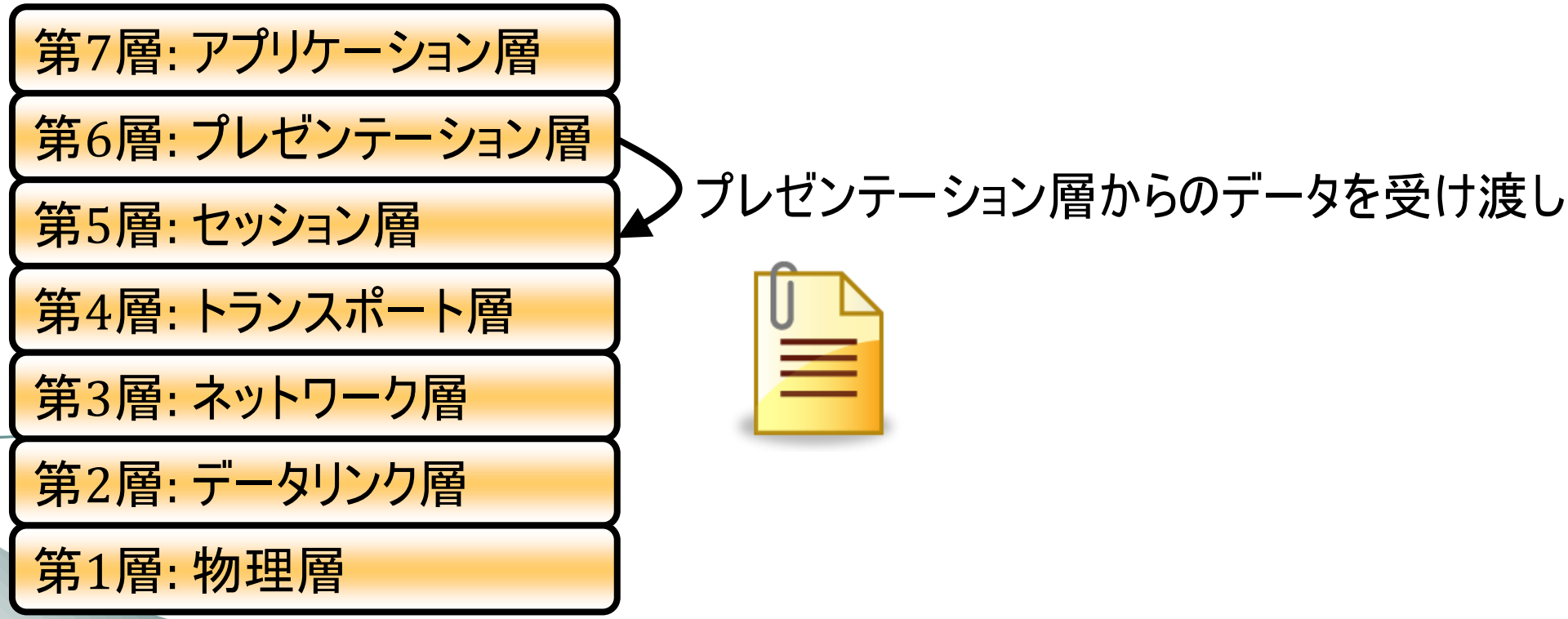
データ送信[2](p. 94)

- プレゼンテーション層の役割: データの表現形式の規定
  - データの圧縮・暗号形式や画像の形式、文字コード等に関する規定
  - データをネットワークで送信できる形式に変換
  - ネットワークから受信したデータをソフトウェアが理解できる形式に変換

第7層: アプリケーション層
第6層: プレゼンテーション層 → 暗号化や圧縮など、データを必要な形に加工
第5層: セッション層
第4層: トランスポート層
第3層: ネットワーク層
第2層: データリンク層
第1層: 物理層

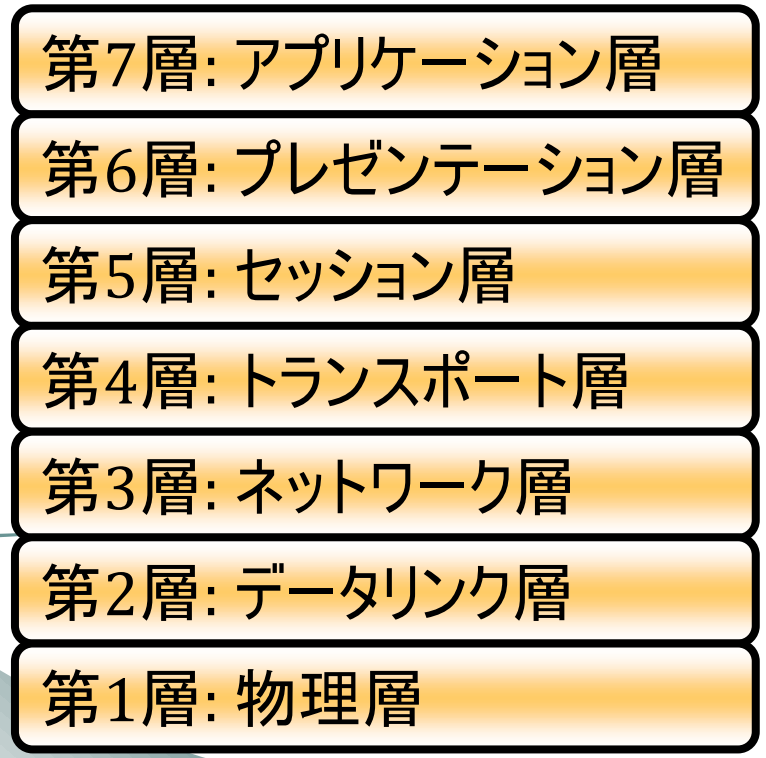


データ送信[3](p. 94)



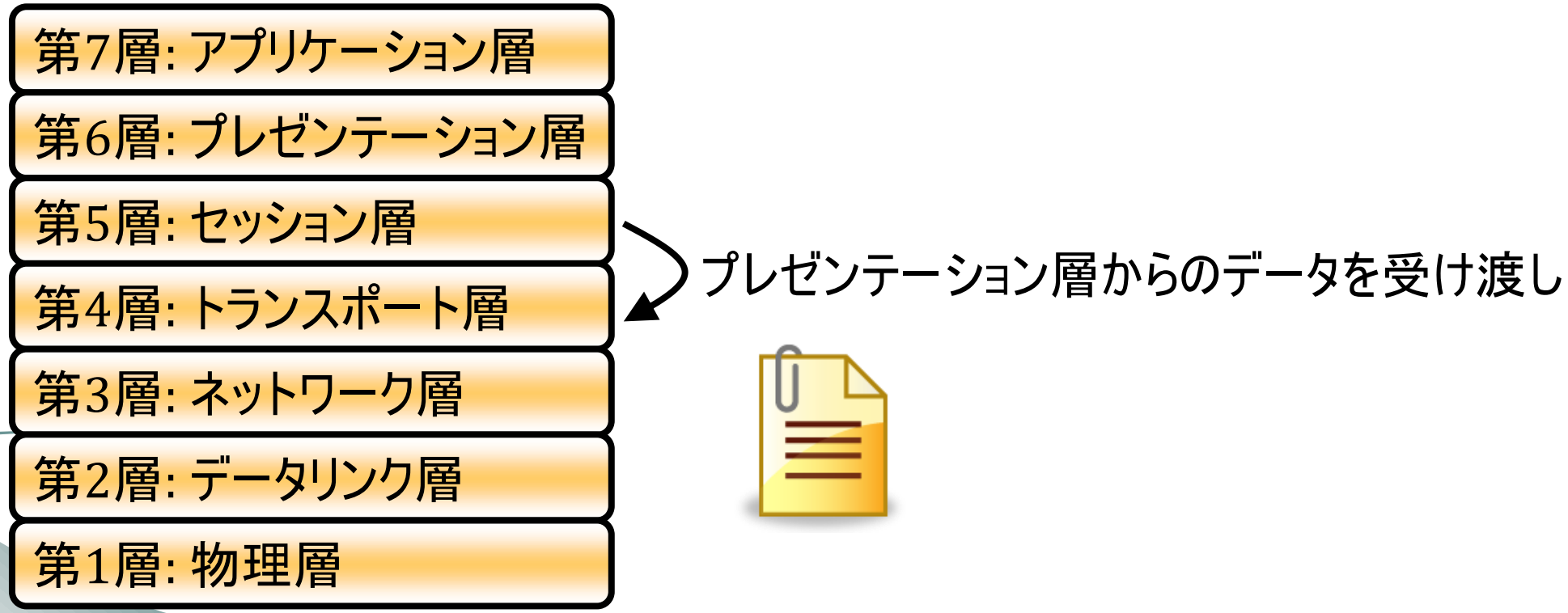
データ送信[4](p. 94)

- セッション層の役割: 通信の開始時・終了時の合図を規定
  - 通信の開始から終了までの手順
  - データ送受信のための経路の確保



→ 送信の開始と終了の合図を決定

データ送信[5](p. 94)



データ送信[6](p. 94)

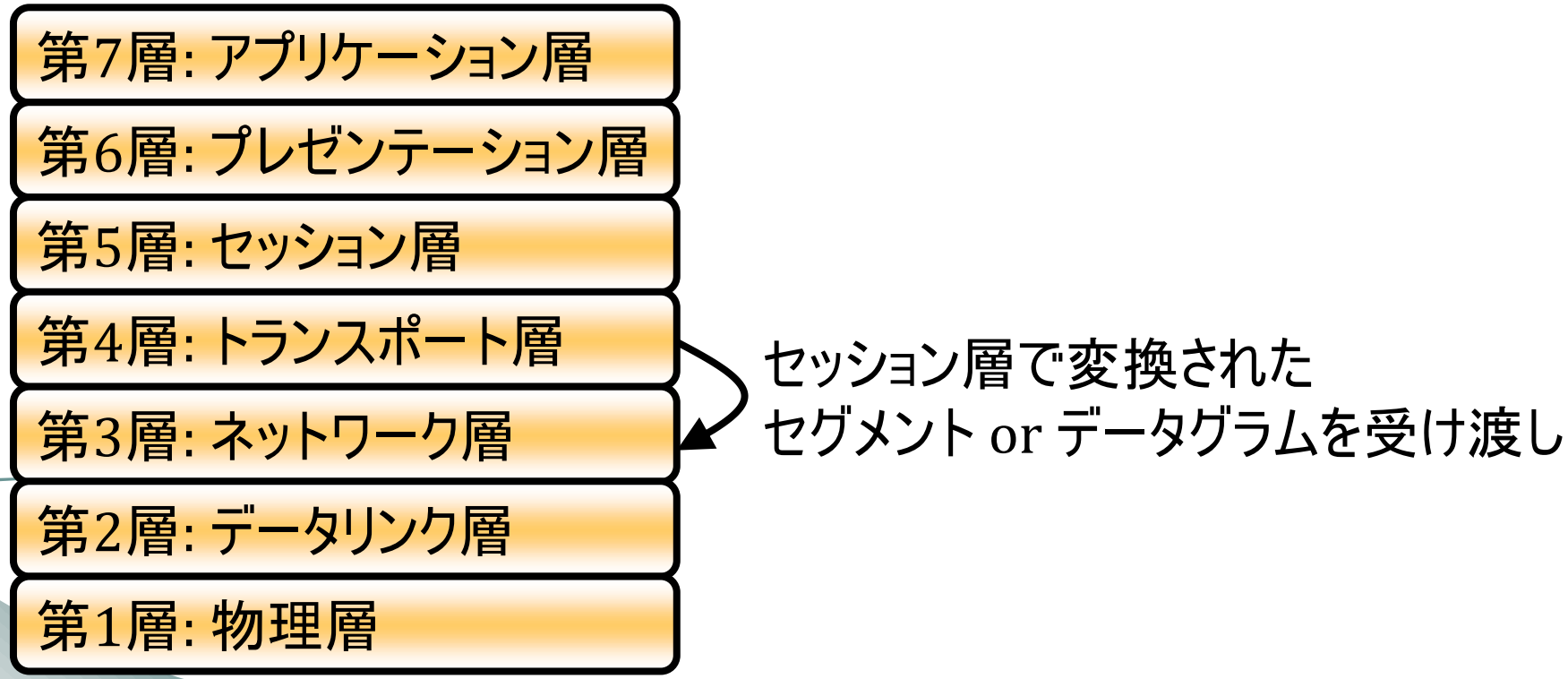
- トランスポート層の役割
  - データ送受信の信頼性を確保
    - データ内容にエラーがないかをチェックし、あれば是正や再送
  - データをネットワークで送信できる大きさに分割

- 第7層: アプリケーション層
- 第6層: プレゼンテーション層
- 第5層: セッション層
- 第4層: トランスポート層
- 第3層: ネットワーク層
- 第2層: データリンク層
- 第1層: 物理層

→ セッション層からのデータをネットワークで送信できる大きさに分割

分割された1つ1つのデータ: セグメント or データグラム
- セグメント: 高信頼の通信の時
- データグラム: 低信頼の通信の時

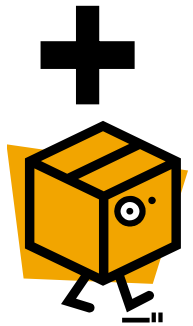
データ送信[7](p. 94)

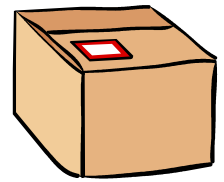


データ送信[8](p. 94)

- ネットワーク層の役割
  - データの宛先を特定して送受信
    - データに宛先の情報を付加し、送る経路の選択
  - ルータ(経路選択のための機器)などの規格を規定

送信元・あて先





パケット

セグメント or データグラム

セグメント or データグラムに送信元やあて先の住所を付加

- 第7層: アプリケーション層
- 第6層: プレゼンテーション層
- 第5層: セッション層
- 第4層: トランスポート層
- 第3層: ネットワーク層
- 第2層: データリンク層
- 第1層: 物理層

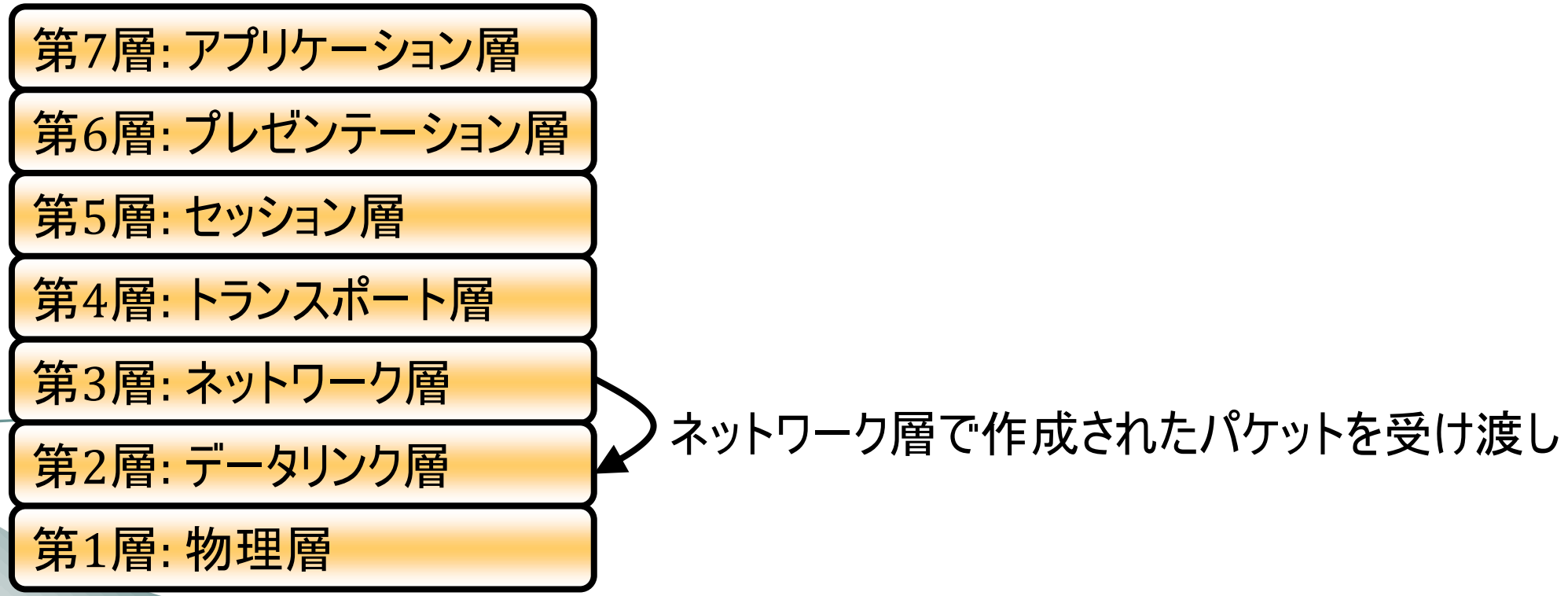
付加されたセグメント or データグラム: パケット

カプセル化(p. 93)

- 送受信するデータには、送受信のために必要な情報がつけられていない
  - 送信する宛先
  - 正しく届いたかどうかのチェック情報, etc.

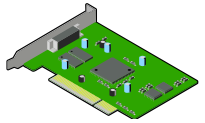
必要な情報をデータに付加すること: カプセル化

データ送信[9](p. 94)

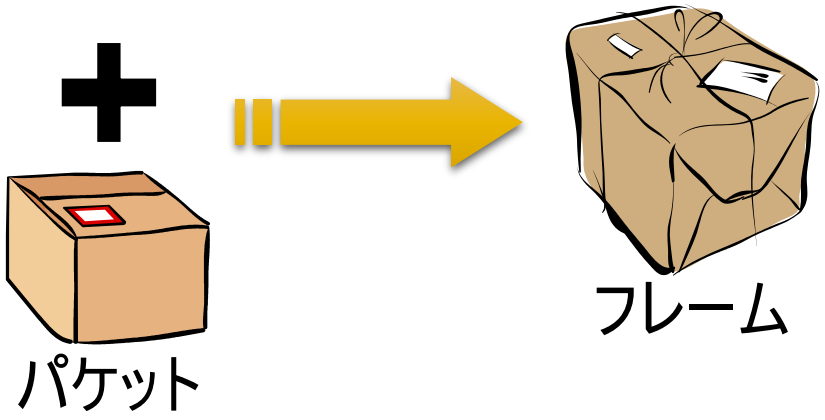


データ送信[10](p. 94)

- データリンク層の役割
  - 物理層での通信に誤りがないかをチェックし、誤りがあれば、再送信を要求
  - スイッチングハブ(コンピュータ同士を接続するための機器)などの規格を規定



MACアドレス
(ネットワークカードの固有の番号)

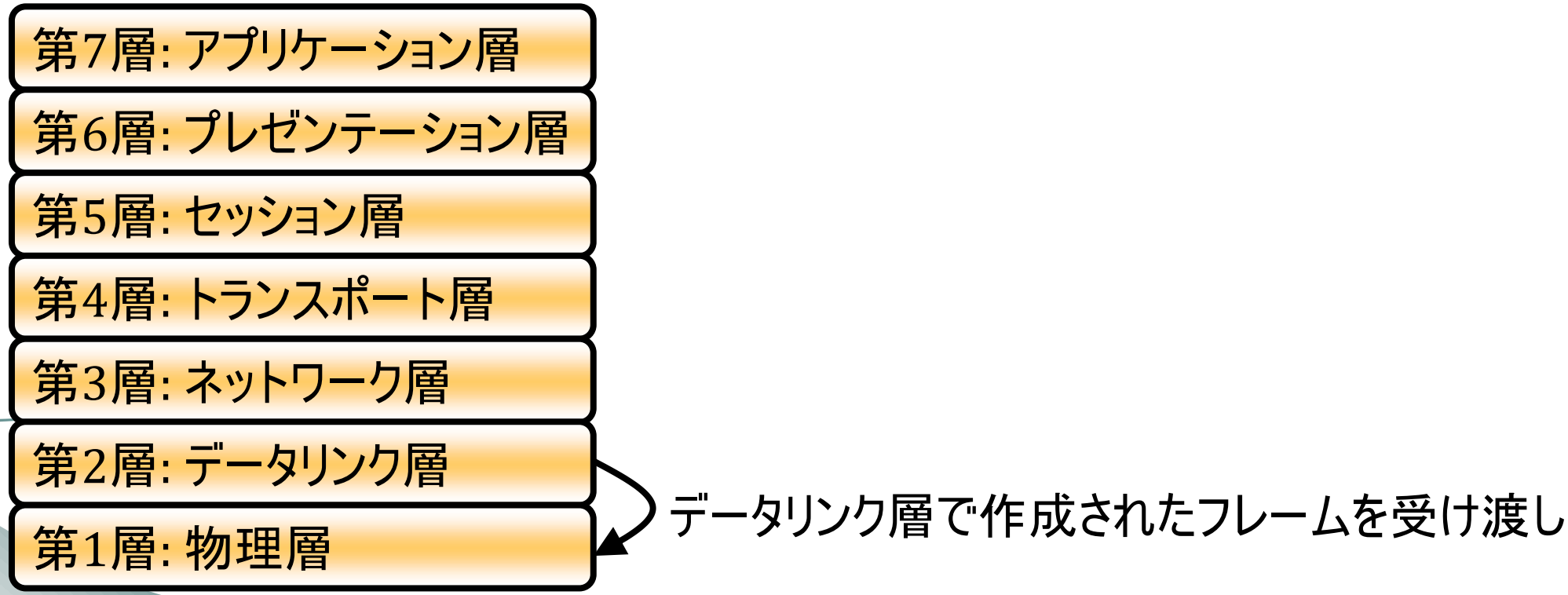


第7層: アプリケーション層
第6層: プレゼンテーション層
第5層: セッション層
第4層: トランスポート層
第3層: ネットワーク層
第2層: データリンク層
第1層: 物理層

→パケットに送信先のMACアドレスの情報を付加

付加されたパケット: フレーム

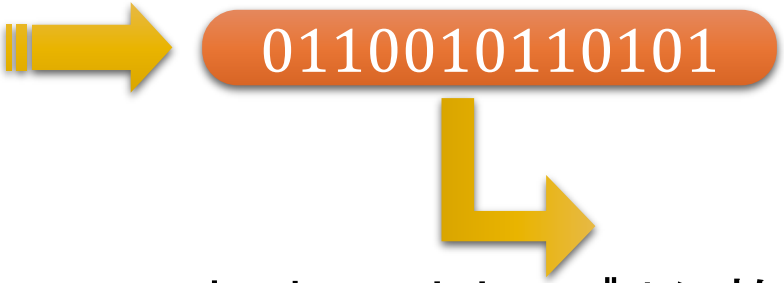
データ送信[11](p. 94)



データ送信[12](p. 94)

- 物理層の役割
  - ケーブルの規格を定め、やデータを電気・光信号の形で送受信
    - データと電気信号との間の変換
    - ケーブルに関する様々な規格(材質, コネクタの形状, etc.)

フレーム



ネットワークケーブルに放出

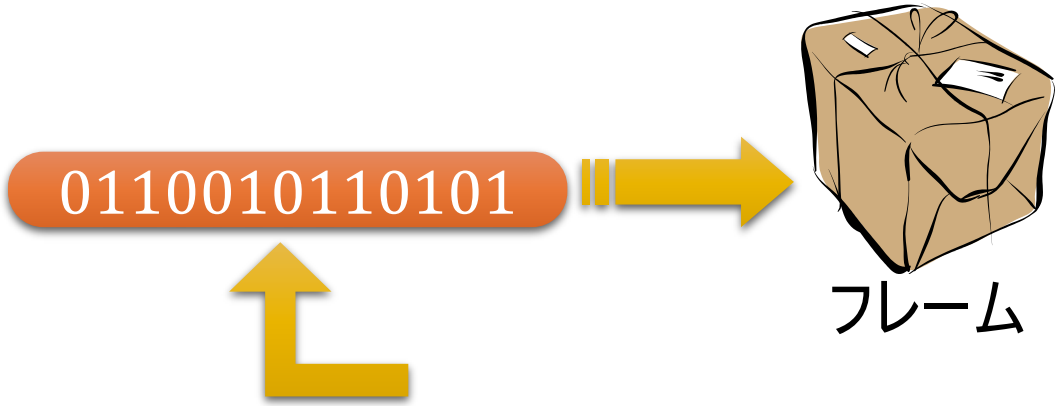
- 第7層: アプリケーション層
- 第6層: プレゼンテーション層
- 第5層: セッション層
- 第4層: トランスポート層
- 第3層: ネットワーク層
- 第2層: データリンク層
- 第1層: 物理層

→フレームを信号(電気や光)に変換

データの受信

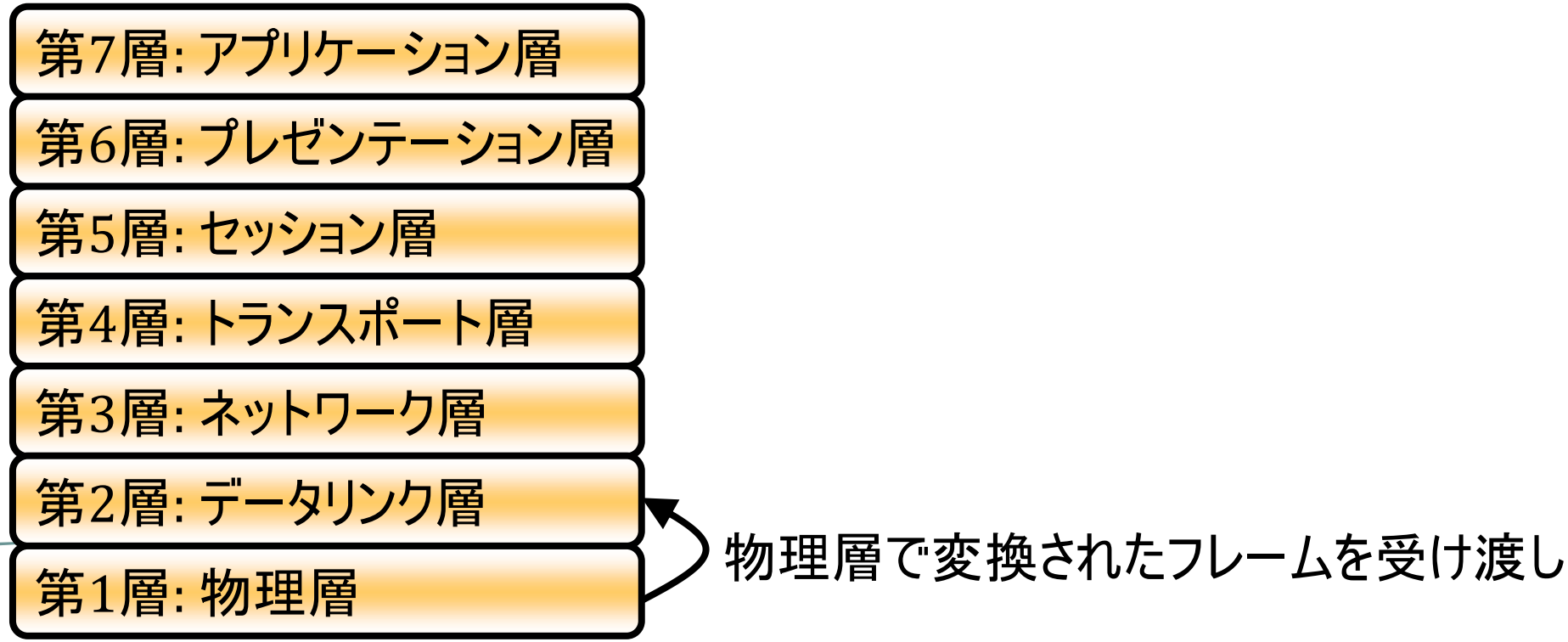
データ受信[1](p. 94)

第7層: アプリケーション層
第6層: プレゼンテーション層
第5層: セッション層
第4層: トランスポート層
第3層: ネットワーク層
第2層: データリンク層
第1層: 物理層



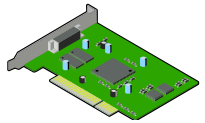
→信号(電気や光)をフレームに変換

データ受信[2](p. 94)



データ受信[3](p. 94)

フレーム



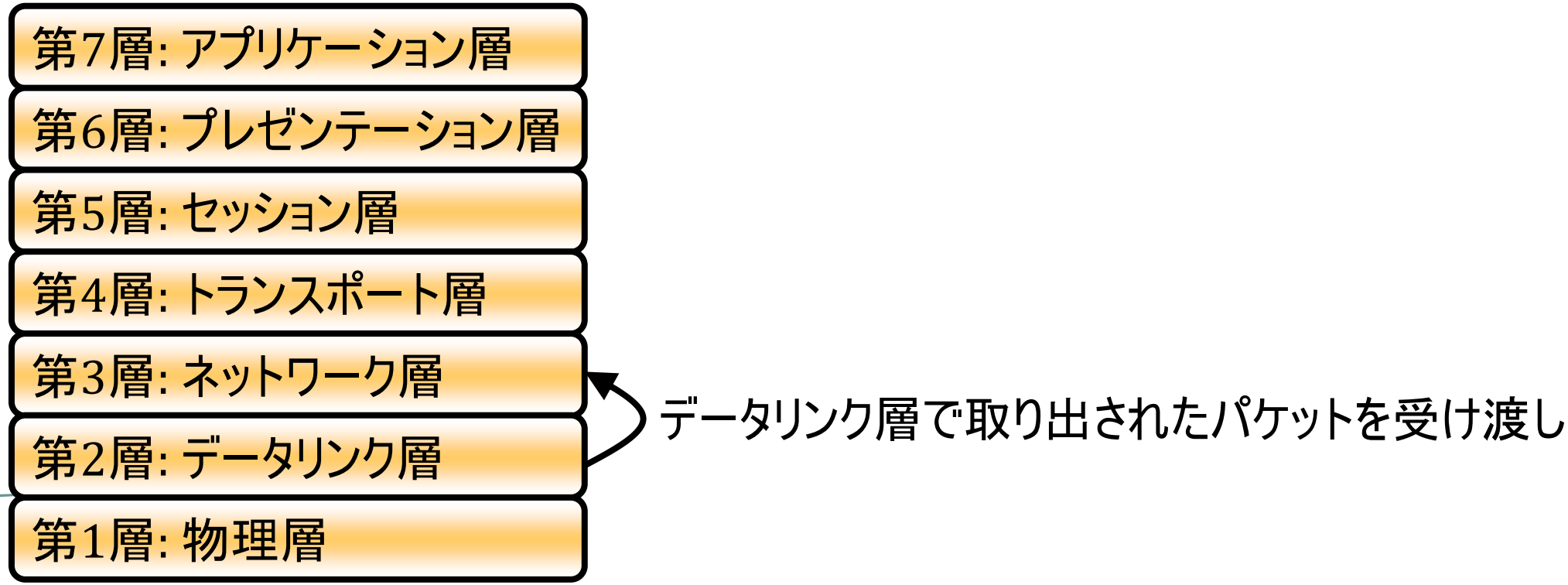
MACアドレス
(ネットワークカードに固有の番号)

パケット

- 第7層: アプリケーション層
- 第6層: プレゼンテーション層
- 第5層: セッション層
- 第4層: トランスポート層
- 第3層: ネットワーク層
- 第2層: データリンク層
- 第1層: 物理層

→ フレームから送信先のMACアドレスの情報を削除してパケットを取り出し

データ受信[4](p. 94)



データ受信[5](p. 94)

パケット

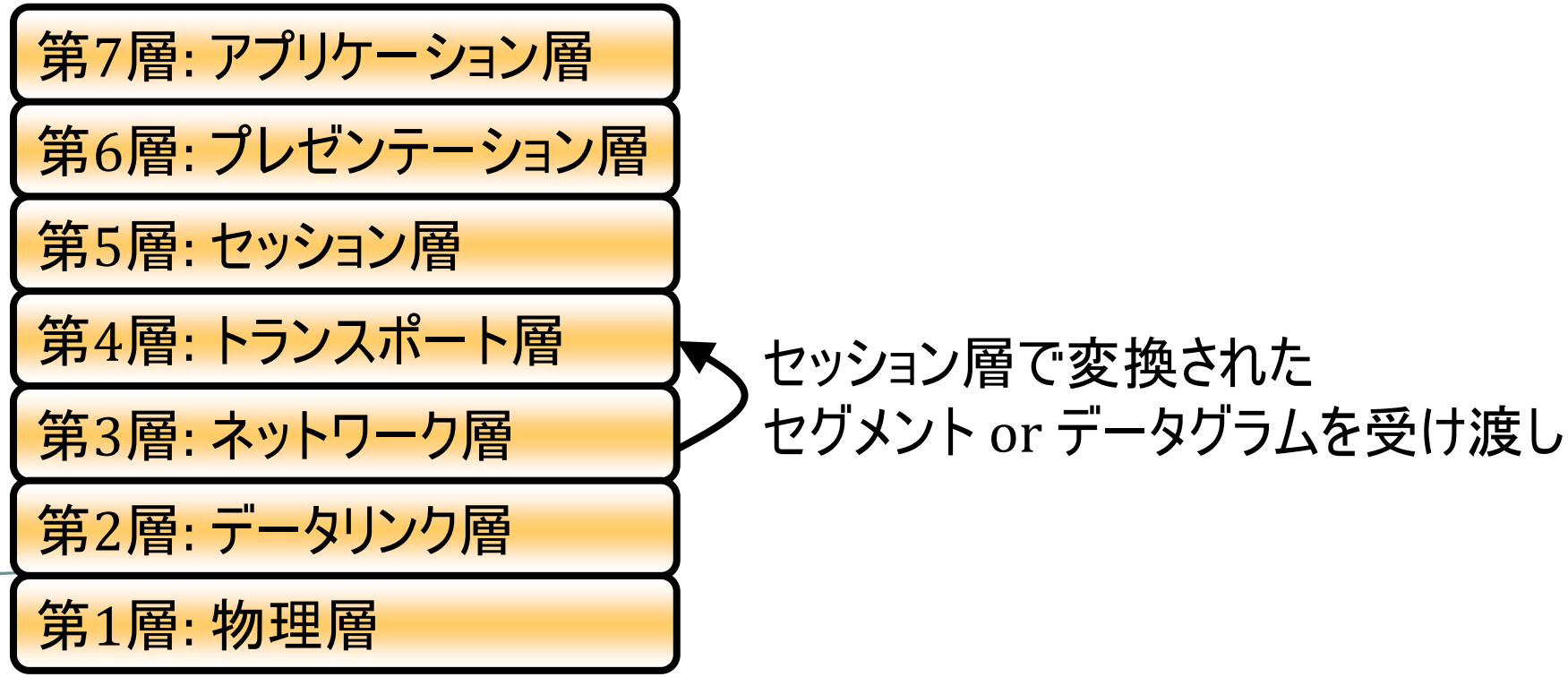
送信元・あて先

セグメント or データグラム

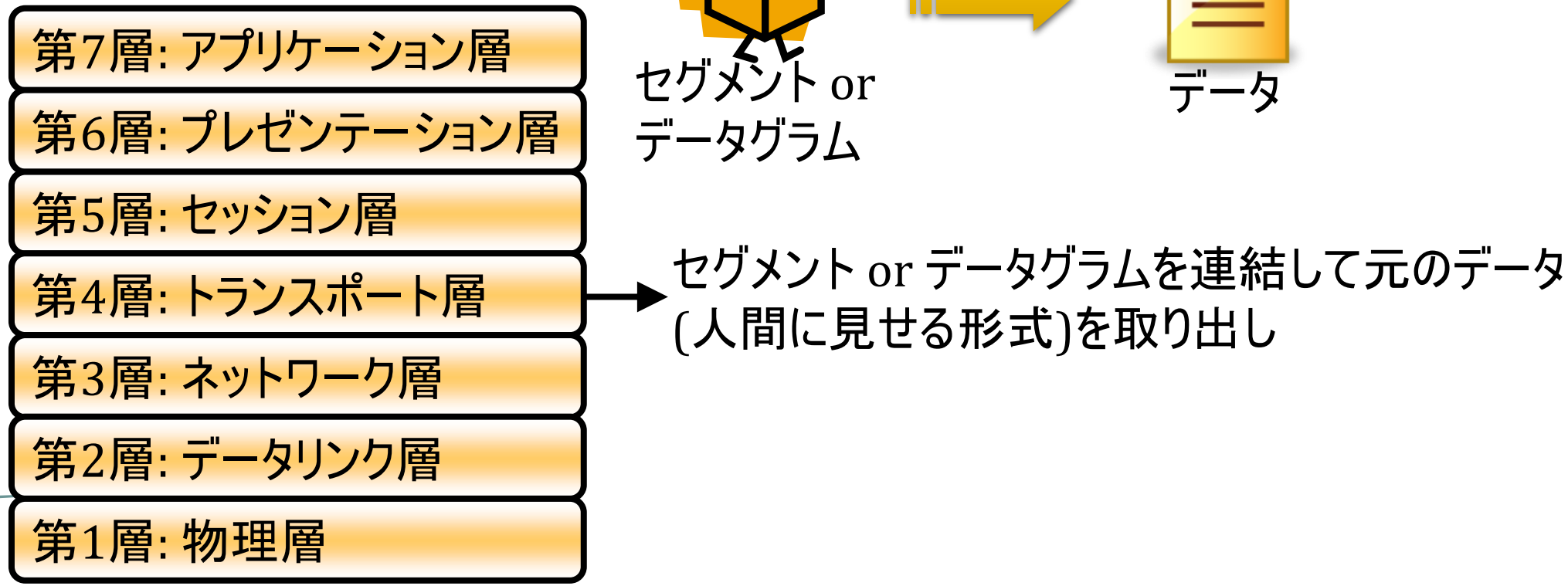
- 第7層: アプリケーション層
- 第6層: プレゼンテーション層
- 第5層: セッション層
- 第4層: トランスポート層
- 第3層: ネットワーク層
- 第2層: データリンク層
- 第1層: 物理層

→ パケットから送信元やあて先の住所を削除して
セグメント or データグラムを取り出し

データ受信[6](p. 94)

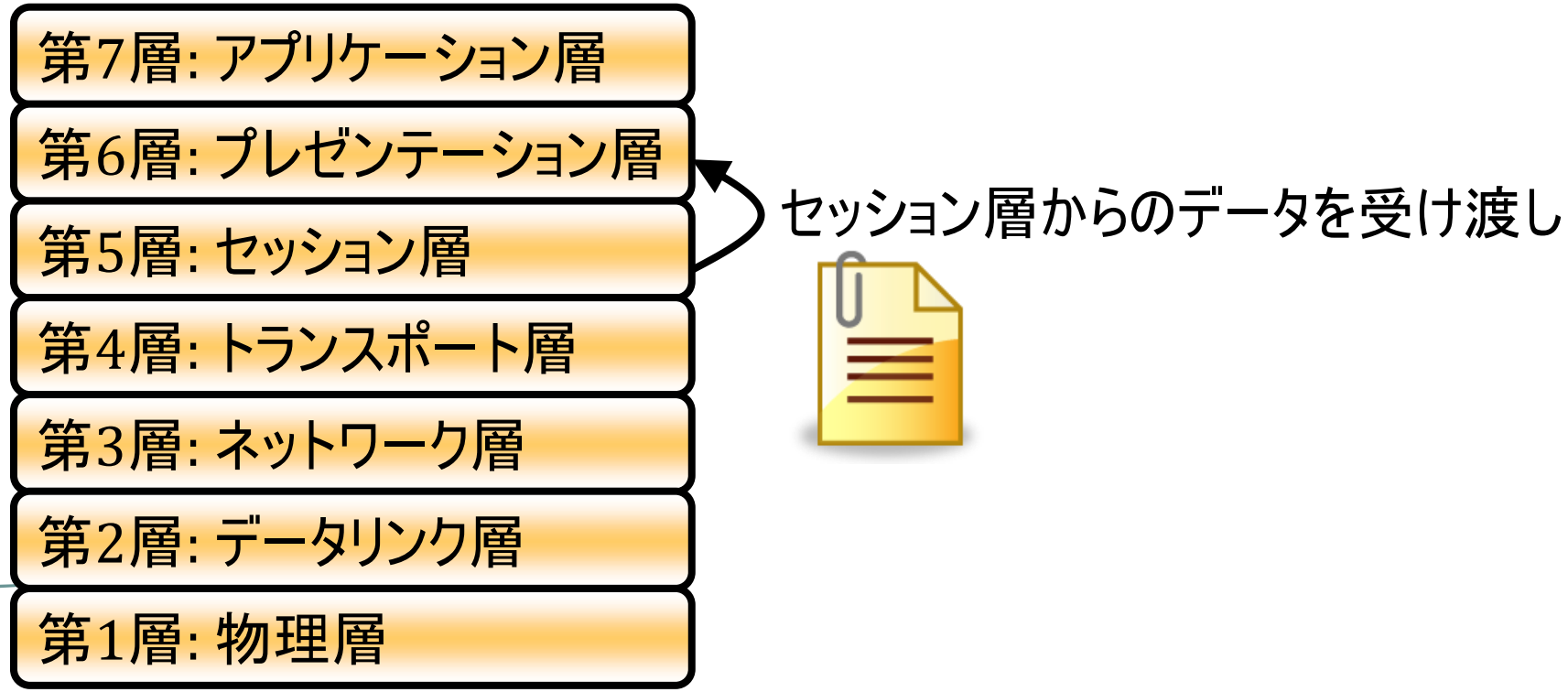


データ受信[7](p. 94)



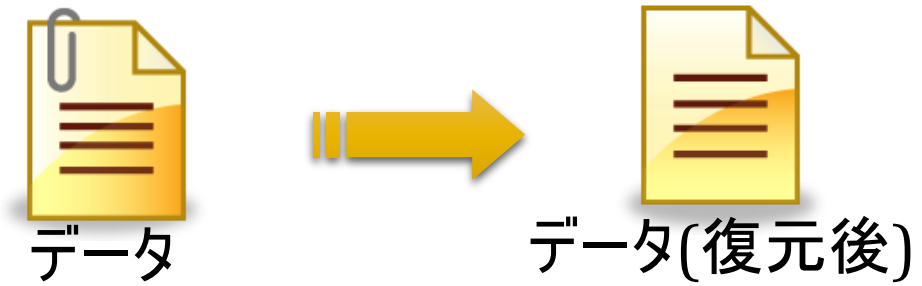
データ受信[8](p. 94)

データ受信[9](p. 94)

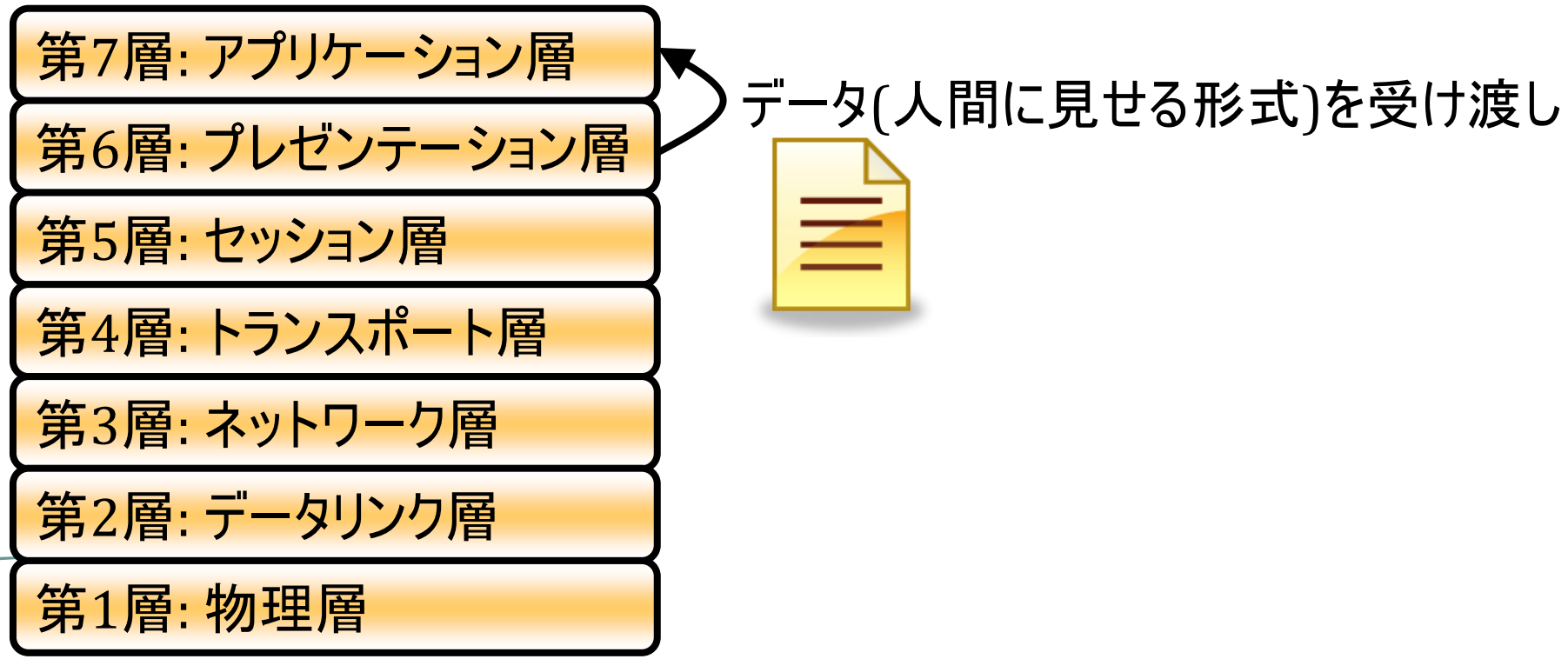


データ受信[10](p. 94)

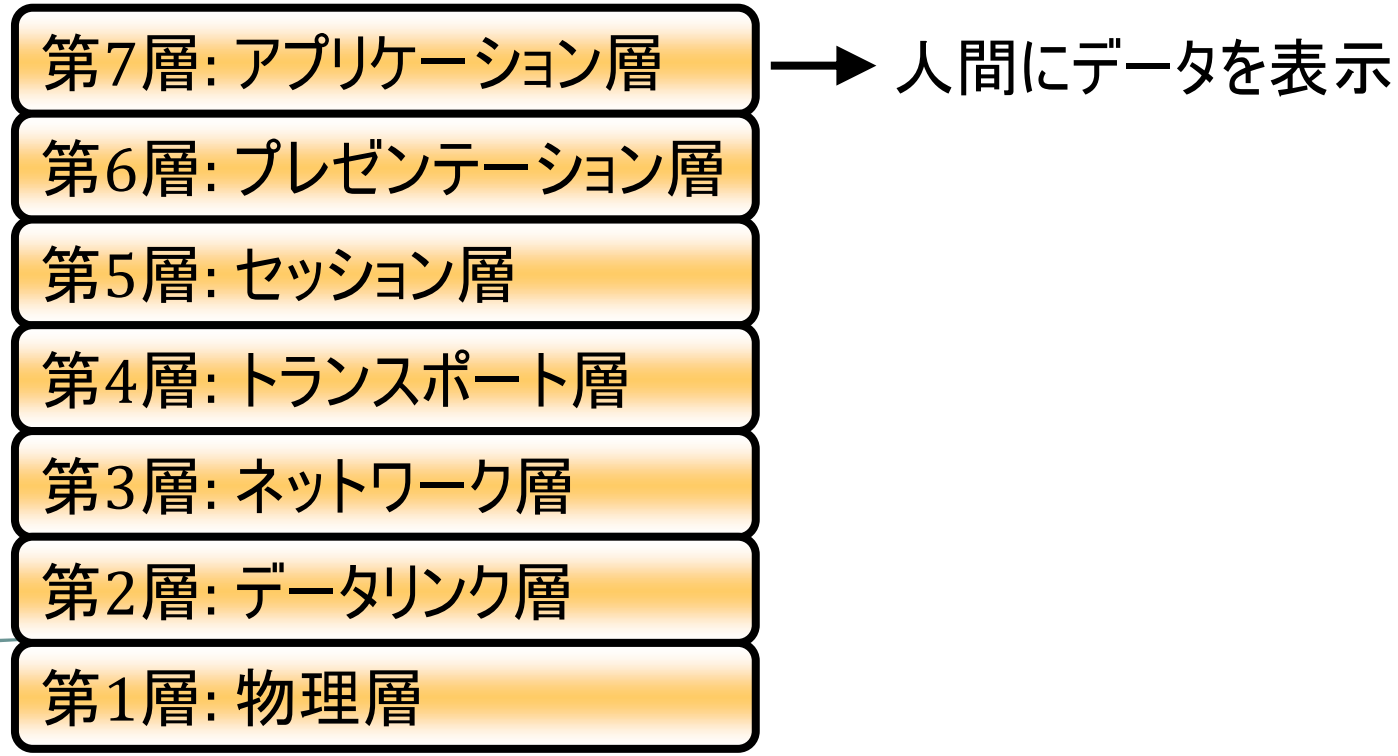
第7層: アプリケーション層
第6層: プレゼンテーション層 → 暗号化や圧縮などを解除し、元のデータを取り出し
第5層: セッション層
第4層: トランスポート層
第3層: ネットワーク層
第2層: データリンク層
第1層: 物理層



データ受信[11](p. 94)



データ受信[12](p. 94)



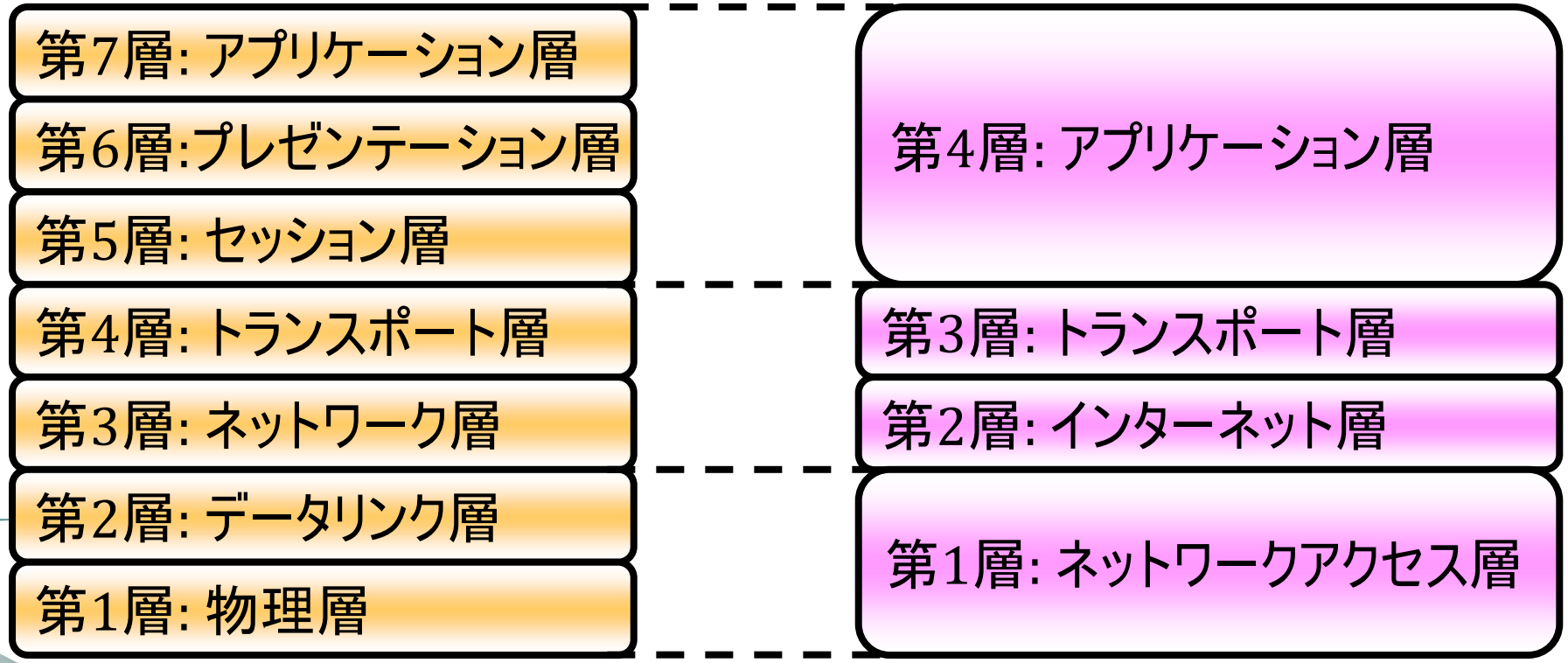
TCP/IPモデル

TCP/IPモデルとは?(p. 96)

- TCP/IP: データがインターネットを通るためのプロトコル
  - Transmission Control Protocol/Internet Protocol
  - インターネットでの標準規格
- コンピュータの通信機能を4つの階層に分割したモデル
  - 各階層ごとに必要な機能(プロトコル)を定義
  - 現在最もよく使われているモデル
    ※OSI参照モデルは、実際に利用するモデルの基礎

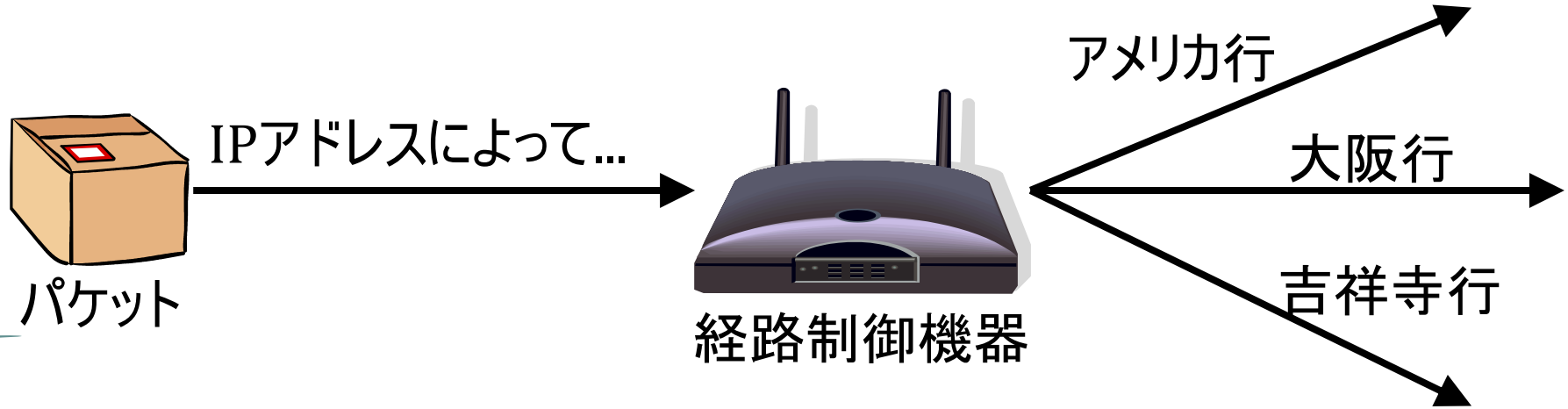
OSIとTCP/IPモデル(p. 96)

- OSIの7層とTCP/IPの4層との対応関係
  - OSI参照モデルと同じ名前の層があるが、必ずしも同じ役割をするわけではない



インターネット層のプロトコル(p. 96)

- IP
  - インターネットの世界でのコンピュータの住所(IPアドレス)を扱うためのプロトコル
    - 通信の宛先として指定される住所
  - IPアドレスに基づいて、送り先を決める経路制御機器で利用



トランスポート層のプロトコル(p. 96)

- TCPとUDP
  - TCP (Transmission Control Protocol)
    - データの通信前に、通信先との道筋を確保し、その上で送受信

コネクション型

  - UDP (User Datagram Protocol)
    - 道筋を確保することなく、いきなりデータを通信

コネクションレス型

TCPとUDP[データの受け渡し](p. 96)

- 上位の層からのデータの受け渡し
  - TCP: データを分割して受け渡し
    - 分割したデータを「セグメント」
  - UDP: データのかたまりをそのまま受け渡し
    - データのかたまりを「UDPデータグラム」
    - データのサイズがある一定以上を超える場合、さらに下位のネットワーク層で分割(IPフラグメンテーション)

TCPとUDP[信頼性](p. 96)

- TCP
  - 通信中にデータの紛失がないかを確認し、紛失があれば送りなおし
    - セグメントに番号をつけ、正しい番号のセグメントが届かなければ再送
    - タイムアウトすれば再送
    - 同じ番号のセグメントが届けば、重複を除去
    - セグメントの番号が順番どおりに届かなければ、順番どおりに並べ替え
- UDP
  - 通信中のデータの紛失については、何もサポートなし

TCPとUDP[シンプルさと軽さ](p. 96)

- TCP
  - 様々な処理をする必要があるので、複雑で遅い(重い)
- UDP
  - データの送受信以外のことをほとんどしないので、シンプルで速い(軽い)

TCPとUDP[使いどころ](p. 96)

- TCP
  - 大きなファイルの送信
    - 第7層か第3層あたりでデータを分割する必要があるが、送信確認をしないと、一部が紛失する可能性
- UDP
  - 小さなメッセージの送信
    - TCPを使うと、小さいデータに様々なものが付加されることになり、非効率
  - 実況中継
    - TCPを使うと、再送などがあってリアルタイム性が問題
  - ブロードキャスト
    - TCPを使うと、再送が起こったときに複数個所に再送が困難

Question!

デファクトスタンダード

デファクトスタンダード(p. 97)

- TCP/IPモデル
  - 階層化が不十分で厳密性が不足
  - but 最も広く使われていて、ネットワークの事実上の標準

デファクトスタンダード

デファクトスタンダード

- 市場で広く使われるようになったために、標準となること
  - ✓ 国際機関などが公的標準として定めたものではない
- 一度標準になると、関連する企画や商品が出て、さらに標準が地位を強化

標準化の流れ(p. 97)

- インターネット関連のプロトコル
  - RFC(Request For Comments)という文書により実現
    - IETF(Internet Engineering Task Force)という技術者組織の技術者が、新しい技術を提案(提案文書: RFC文書)
    - 提案に対して様々ン意見が出され、改良や修正
    - 最終的に、実証実験や正式な会議により、標準化が決定

議論の過程や標準化された規格は広く公開され、誰でも利用可能

➡ 自由で開放的な開発スタイルがインターネットの発展に寄与

but...自由で開放的なために、様々な問題も

- 知的財産の侵害
- コンピュータウィルス
- 不正アクセス

LANとインターネット

LAN(p. 98)

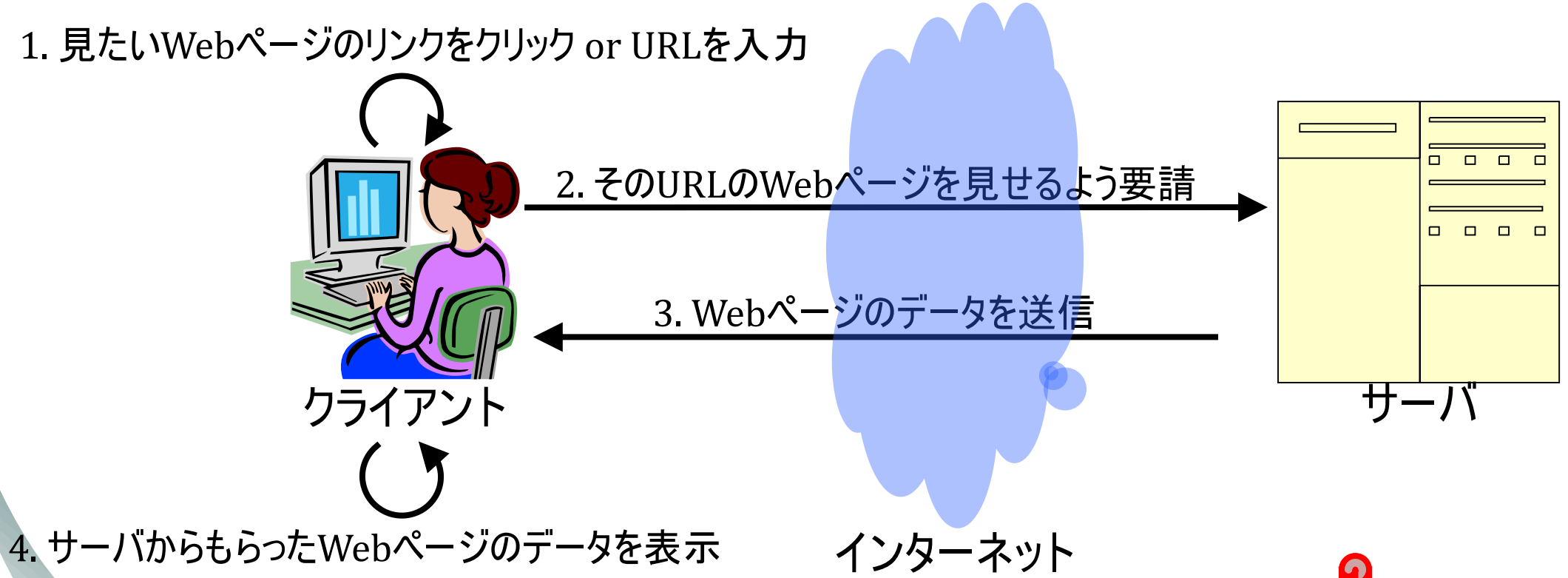
- LAN: Local Area Network
  - 地理的にも限られた狭い範囲のネットワーク
- WAN: Wide Area Network
  - LAN同士を接続したりした、広い範囲のネットワーク
  - インターネットは世界規模のWAN

クライアントサーバ方式[1](p. 99)

- インターネットの世界で広く使われている、様々な処理を行うための方式
  - クライアント
    - サーバに要請をして、様々な処理をしてもらうコンピュータ
    - Ex. Webページを見せてもらう, 届いているメールを見せてもらう, etc.
  - サーバ
    - クライアントからの要請を受けて、様々な処理をするコンピュータ
    - Ex. Webサーバ, メールサーバ, etc.
  - インターネット
    - クライアントからの要請やデータをサーバに届けたり、サーバの返事やデータをクライアントに届けるための道路

クライアントサーバ方式[2](p. 99)

- Ex. Webページの閲覧



Webページの管理をするサーバ:
Webサーバ

IPアドレスとドメイン

IPアドレスとは?(p. 99)

- インターネットの世界で通信を行うために、コンピュータの住所が必要
  - IPアドレス: 原則として世界中で一意(他のコンピュータと重ならない)住所
- 現在広く使われているIPアドレス:「.」で区切られた3桁の10進数を4つ並べた形
  - 1つ1つの10進数は、0～255(2進数で8桁)の間

IPアドレスの例

192.168.20.1 (11000000.10101000.00010100.00000001)

- 国際的な組織ICANN(The Internet Corporation for Assigned Names and Numbers)が管理
  - 各地の支部で実際の管理
  - IPアドレスを使いたい企業・組織は、ICANN(の自分の地域の支部)に申請

IPアドレスが足りない!!(p. 101)

- 現在の形式のIPアドレス: IPv4(Internet Protocol version 4)
  - 2^{32}個(約43億個)存在
- 現在の利用形態
  - IPアドレスを、世界中の人が分け合って利用
    - 世界の人口約70億人(使っていない人も多いが、使う人がどんどん増えている)
    - 1人で複数台の端末を利用(PC, スマートフォン, ゲーム機, etc.)

➡ いろいろな対処方法が考案・実践されたが、もう限界

IPアドレスの枯渇問題

現実に...(p. 101)

- IPアドレスの残り状況
  - 2011年4月15日に、アジア太平洋地域の在庫がなくなった
- IPアドレスの在庫がなくなると...
  - 企業や組織: 新しいネットワークの作成が不可能
  - 一般の利用者: スマートフォンなど、新しい形態の利用に影響がでる...かも?
    - 最近は冷蔵庫とかの家電でもネットワーク接続が利用(=IPアドレスが利用)されているし...

抜本的な解決方法は??(p. 101)

- IPv6(Internet Protocol version 6)の形式のIPアドレス
  - 0011:2233:4455:6677:8899:aabb:ccdd:eeff
    という形式
    - 4桁の数(16進数)を「:」で区切って8つ並べて表現
  - 2^{128}個(約340澗(340×10^{36})個)のIPアドレスを利用可能
    - 数に限りはあるが、世界の人口などを考えても十分に足りる数
      (世界の人口が70億人として、1人あたり約5×10^{28}個)
    - 世界中のすべての端末(PC, スマートフォン, ゲーム機, 家電, etc.)に、重複なくIPアドレスを割り当てることが可能

IPv6への移行が必要!!(p. 101)

- IPv6へ移行しようとすると...(IPv4と扱い方が全く違う)
  - 古い機器ではIPv6に対応していない
    - 新しい機器の導入、新しいソフトウェアの開発や導入が必要
  - 一般利用者には、移行のメリットがわかりにくい
    - ネットワークが劇的に早くなったりするわけでなし
    - 機器やソフトウェアの導入が求められてデメリットに感じる人も...
  - 世界中での移行が必要
    - IPv4とIPv6が混在できるような仕組みもあるが、最終的には完全移行すべき

移行は急務だが、進んでいない

名前解決(p. 102)

DNS[1](p. 102)

- IPアドレス
  - インターネット上の住所を数値で表したもの
    コンピュータにとってはわかりやすい
    but 人間にとっては、数値の住所はわかりにくい!

Ex. 1: 電子メールアドレス

「利用者の名前@コンピュータの住所」の形になっている
→コンピュータは電子メールアドレスを
「利用者の名前@192.168.1.1」のように考えている

Ex. 2: WebページのURL

「http://コンピュータの住所/」の形になっている
→コンピュータはWebページのURLを
「http:// 192.168.1.1/」のように考えている

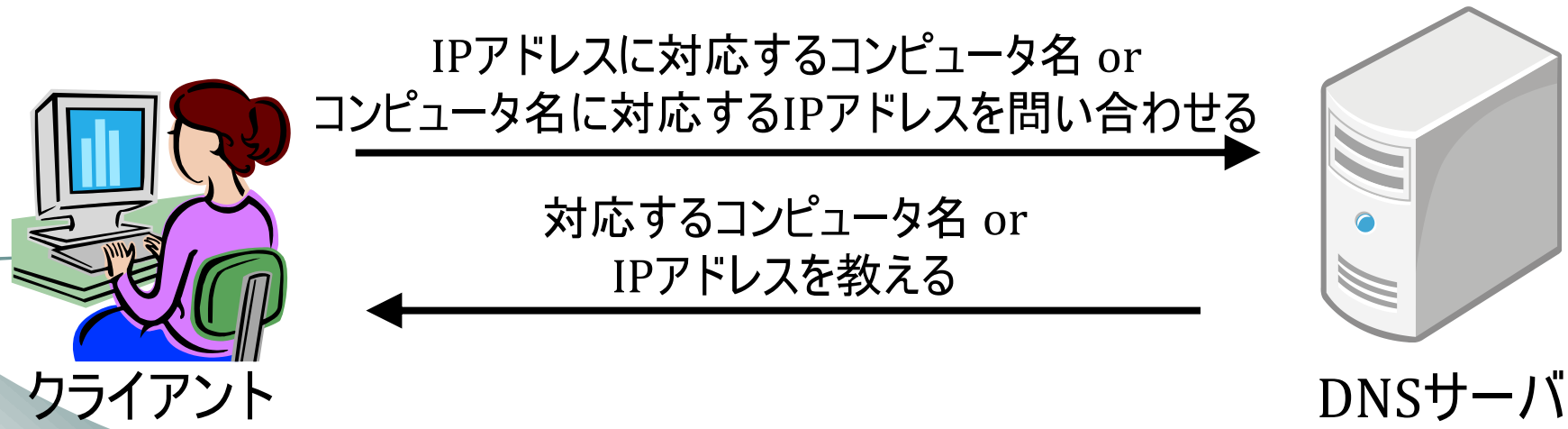
➡ DNS(Domain Name Service)

DNS[2](p. 102)

- DNS: コンピュータの名前とIPアドレスの対応を管理するシステム
- コンピュータの名前を「ドメイン」と呼ばれる単位で管理
  - ドメイン: インターネット上での地域
- コンピュータの名前は、ドメインの前に追加
  - コンピュータ名+ドメインで、インターネット上でのコンピュータのフルネーム(IPアドレスに対応する住所)
  - コンピュータのフルネームにドメインがついているので、世界中で一意の名前
    - それぞれのドメイン内で、コンピュータ名が重ならないようにすればOK
- Ex. コンピュータの名前: www.twcu.ac.jp
  - 「twcu.ac.jp」で、東京女子大学のドメイン
  - 東京女子大学の中の「www」という名前のコンピュータ、という意味

DNSサーバ(p. 102)

- IPアドレス⇔コンピュータ名の対応関係の管理:
  DNSサーバ(ネームサーバとも)
  - IPアドレスとコンピュータ名の対応関係の表の管理
  - クライアントからの問い合わせに応じて、対応するIPアドレス・コンピュータ名を返信

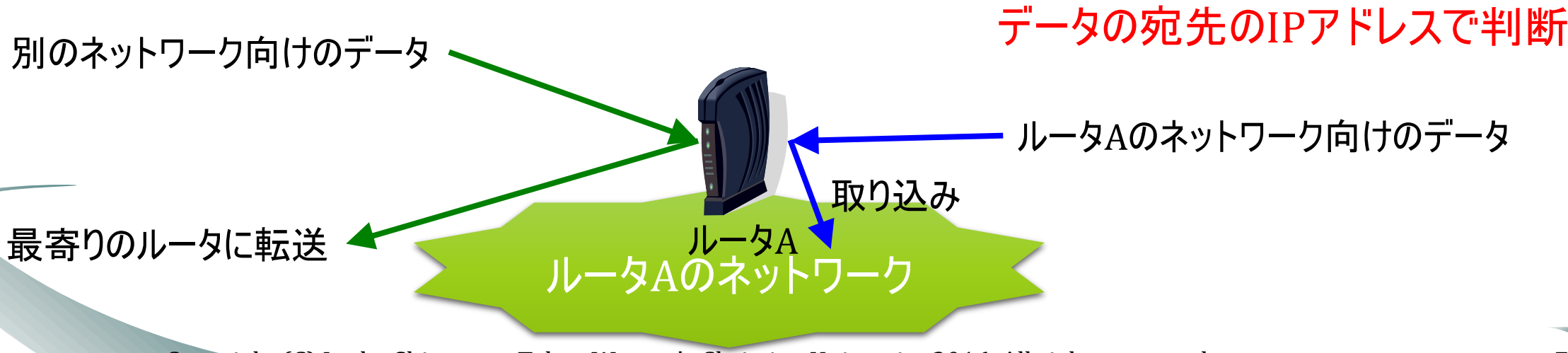


Question!

経路制御

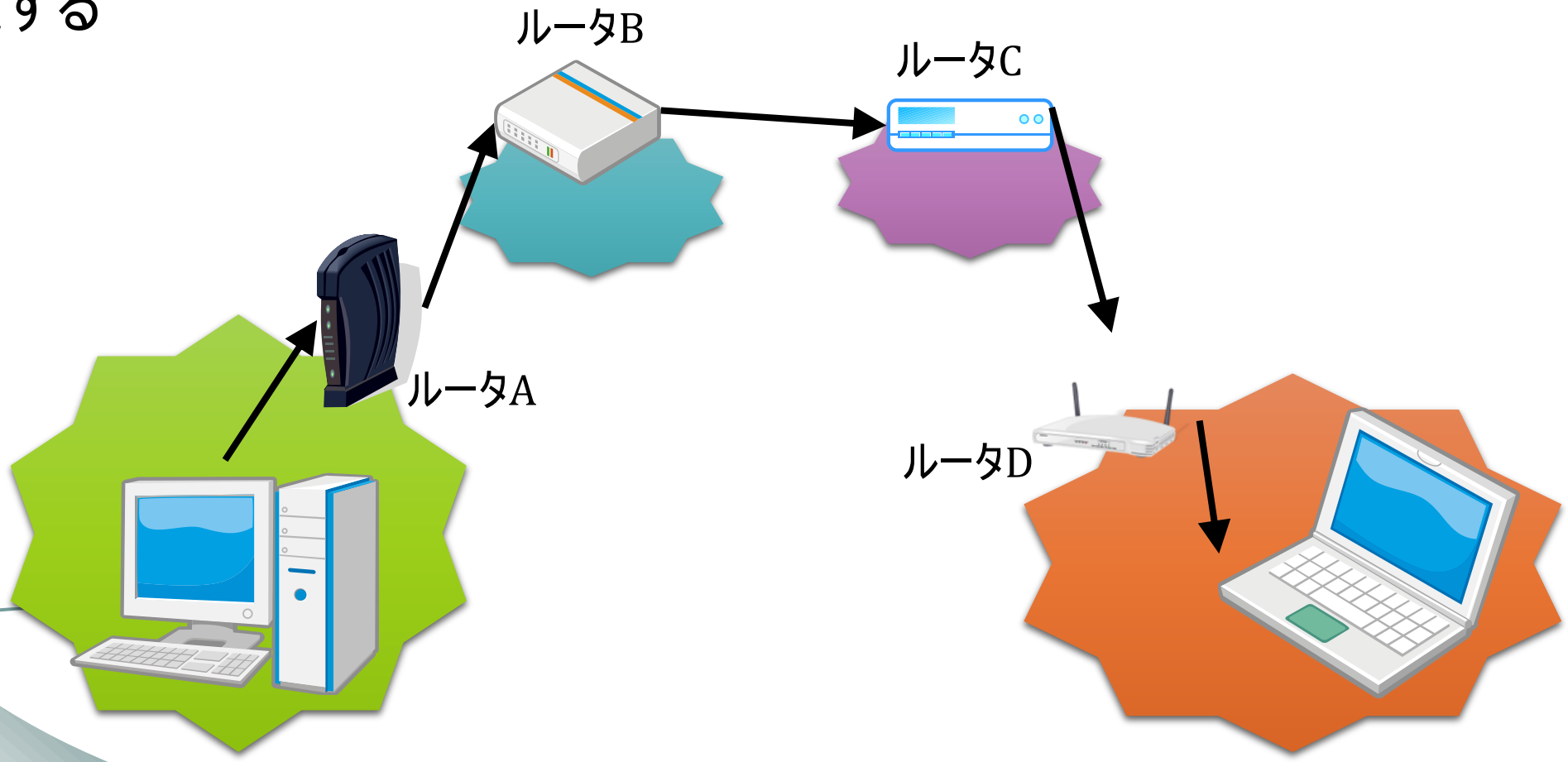
経路制御(p. 104)

- 経路制御(ルーティング): データが相手先に届くために行われる、データがたどる道筋の制御
- ルータが担当
  - ルータ: LANの玄関口として異なるネットワーク同士を接続
    - 届いたデータが自分のネットワーク向けのデータであれば取り込む
    - 届いたデータが自分のネットワーク向けのデータでなければ、最寄のルータ(できるだけ適切そうなルータ)に向かって転送する



データがたどる経路(p. 104)

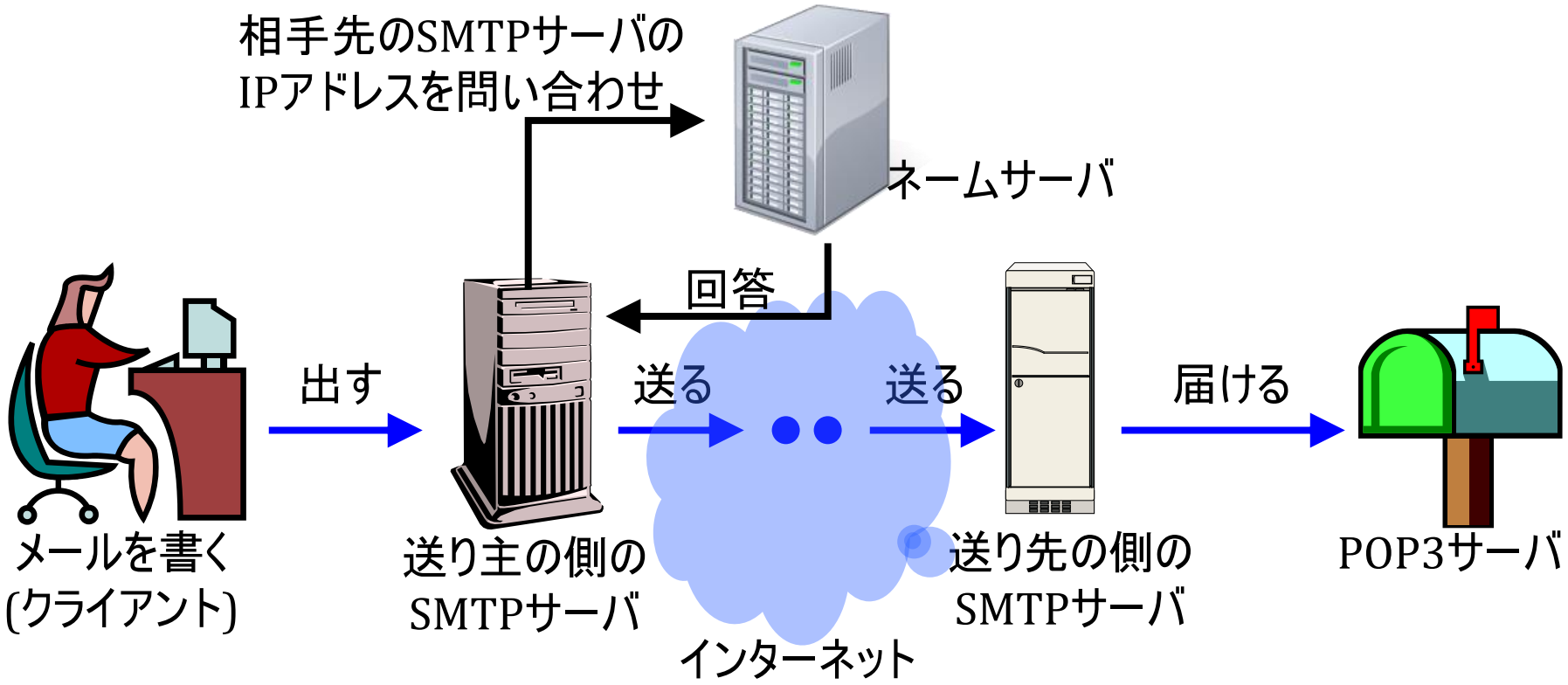
- データは、様々なルータを通って相手先に届く
  - ルータは、データの宛先のIPアドレスをもとに、より適切そうなルータにデータを転送する



インターネット上のアプリケーション

電子メー[送信](p. 105)

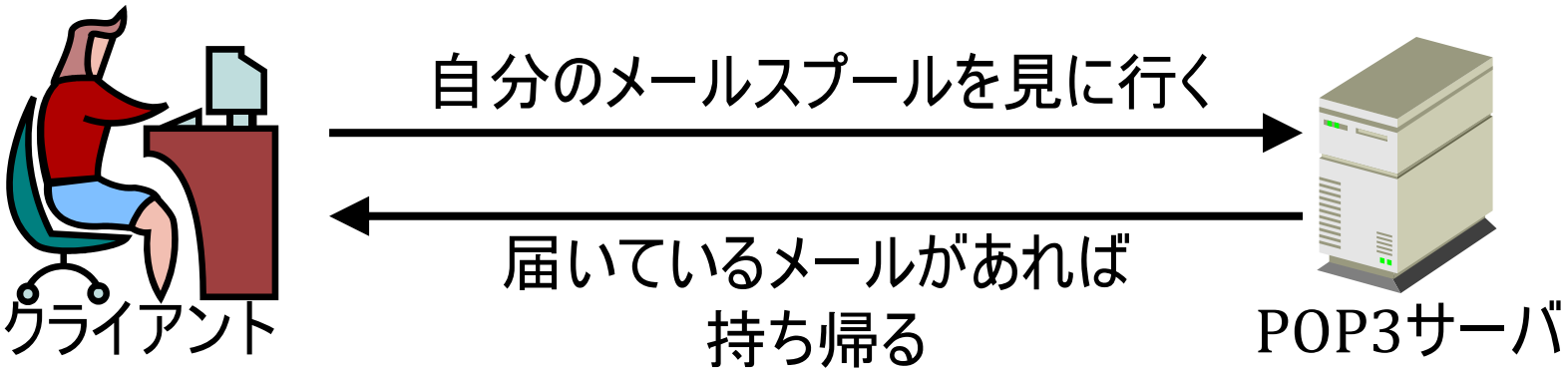
- 電子メール: コンピュータ上での文字でやりとりするメッセージ



SMTP: Simple Mail Transfer Protocol
(メール送信のためのプロトコル)

電子メール[受信](p. 105)

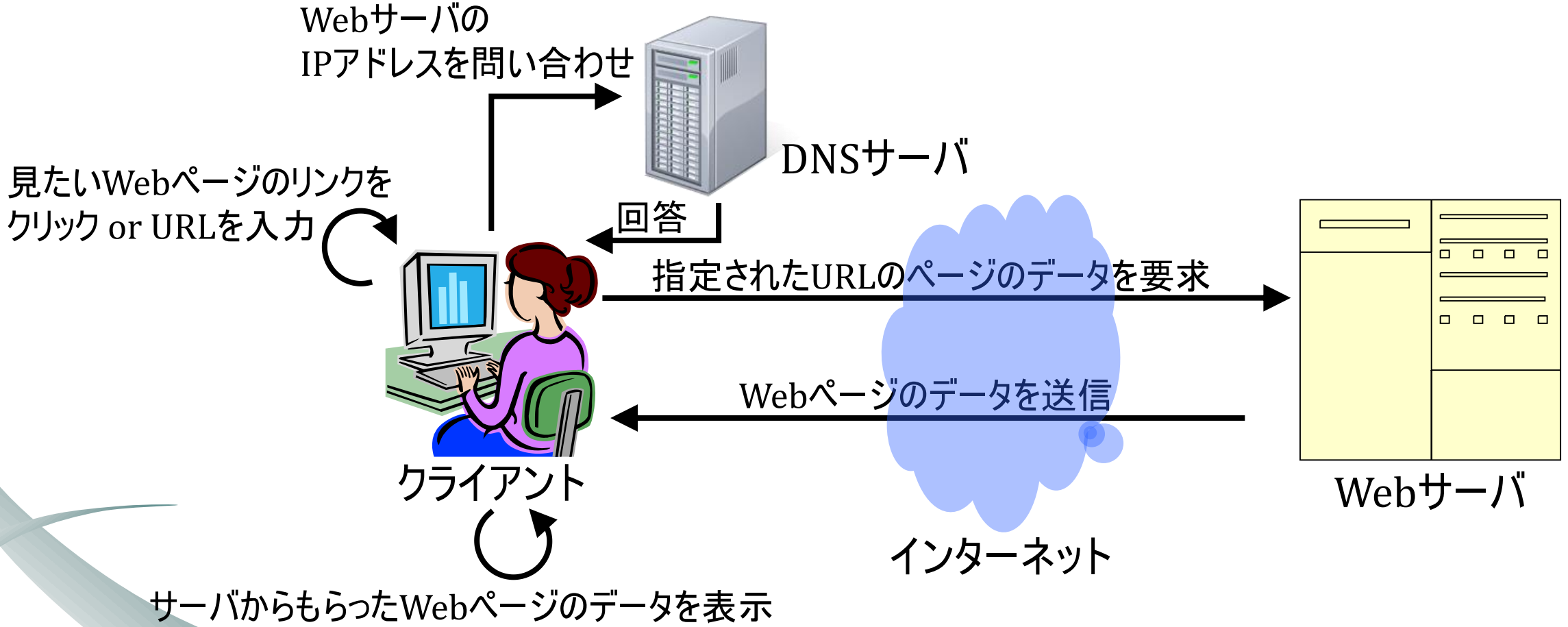
- メールソフトを使った読み書きでは、POP3サーバを利用
  - POP3サーバ中のメールスプール(メールボックス, 個人のメールの保管場所)
- 携帯メールなどでは異なる方式



POP3: Post Office Protocol Version 3
(メール受信のためのプロトコル)

WWW(p. 107)

- WWW: World Wide Web
  - 様々な情報を相互に参照しあえるようにした仕組み



URL(p. 109)

- Uniform Resource Locator
- Webページのありかを示す情報
- URLの形式: http://Webサーバ名/ファイルのパス

http - HyperText Transfer Protocolの略
(WebサーバとWebクライアントとのやり取りをするためのプロトコル)

Webサーバ名 - Webサーバのフルネーム(名前+ドメイン)

ファイルのパス - Webページの内容が書き込まれているファイルのパス(相対パス)

Ex: http://www.cis.twcu.ac.jp/~junko/Science/abc.html
- 東女のWebサーバの中の「~junko」というフォルダの中の「Science」というフォルダの中の「abc.html」というファイル

ネットワークセキュリティ

セキュリティの原則(p. 109)

- 不具合や設定ミスをなくした安全な情報機器を使うこと
- 重要な情報を、扱う権限がない者から隔離すること
- 権限がない者が情報を見てもわからないように隠ぺいすること

安全な情報機器(p. 109)

- 情報機器の機能: プログラムによって実現
  - 人間が作るものなので、不具合(バグ)やセキュリティホールをなくしきれない
    - セキュリティホール: 不正アクセスやウィルス侵入のもとになる不具合
- 初期状態で多数の機能が起動
  - 利用者が意識せずに機能が動いていて、不正アクセスの原因にも

- ソフトウェアのアップデートによるセキュリティホールやバグつぶし
- ウィルス対策
- 初期設定に頼らず、機能の要・不要を考えて利用

を心がけよう!

情報の隔離[1](p. 110)

- 重要な情報を守るために…
  - 守るべきものを隔離する
  - 必要最低限の人や機器だけが利用可能にする
    - 安全性と利便性は常に対立関係
      - ✓ 安全性を上げれば利便性が下がり、利便性を上げれば安全性が下がり…という関係

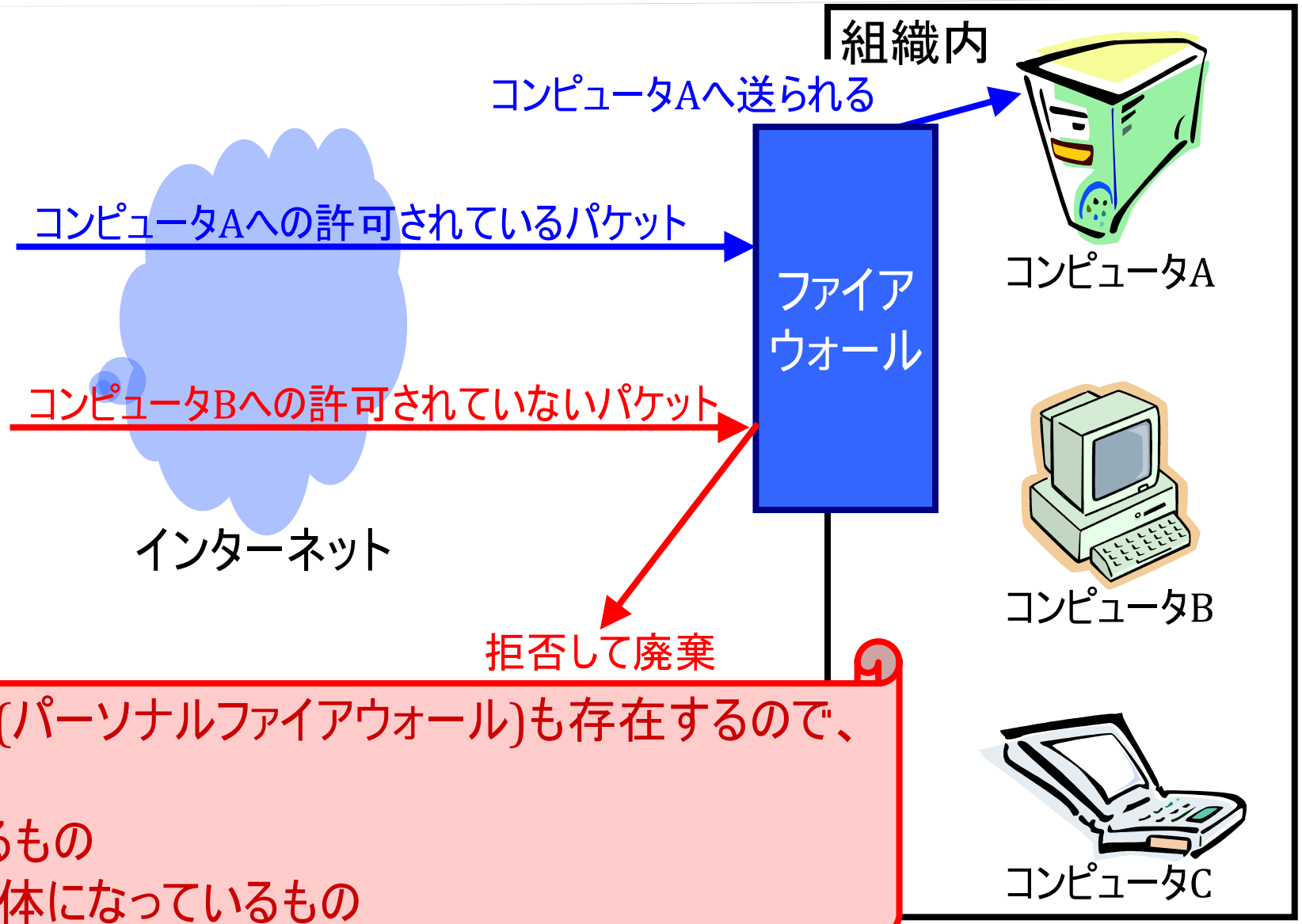
安全性と利便性のバランスを考慮してセキュリティポリシーで情報保護の方針を決定

情報の隔離[2](p. 110)

- ファイアウォールの設置
  - ファイアウォール: 組織内と外部との間に設置して組織内に不正にアクセスされないように監視するコンピュータ
  - 外部からのパケットの監視(アクセス制御)
    - 許可されていないIPアドレス(インターネット上の住所)からパケットが送信されていないか?
    - 許可されていないポート(データの出入り口)にパケットが送信されてきていないか?

許可されていないアクセスを遮断(フィルタリングと呼ぶ)

情報の隔離[3](p. 110)



個人用のファイアウォール(パーソナルファイアウォール)も存在するので、利用して情報を守ろう!

- OSに付属しているもの
- ウィルスソフトと一体になっているもの

情報の隠蔽[1](p. 111)

- インターネット上での通信(メール, Web, etc.)
  - データがそのままの形で送受信される
    = パスワードなどの個人情報がそのままインターネット上に流される

    = 途中で盗聴されてデータが盗まれる可能性もある

    ➡ インターネット上での盗聴は、仕組み上防ぐことは難しい

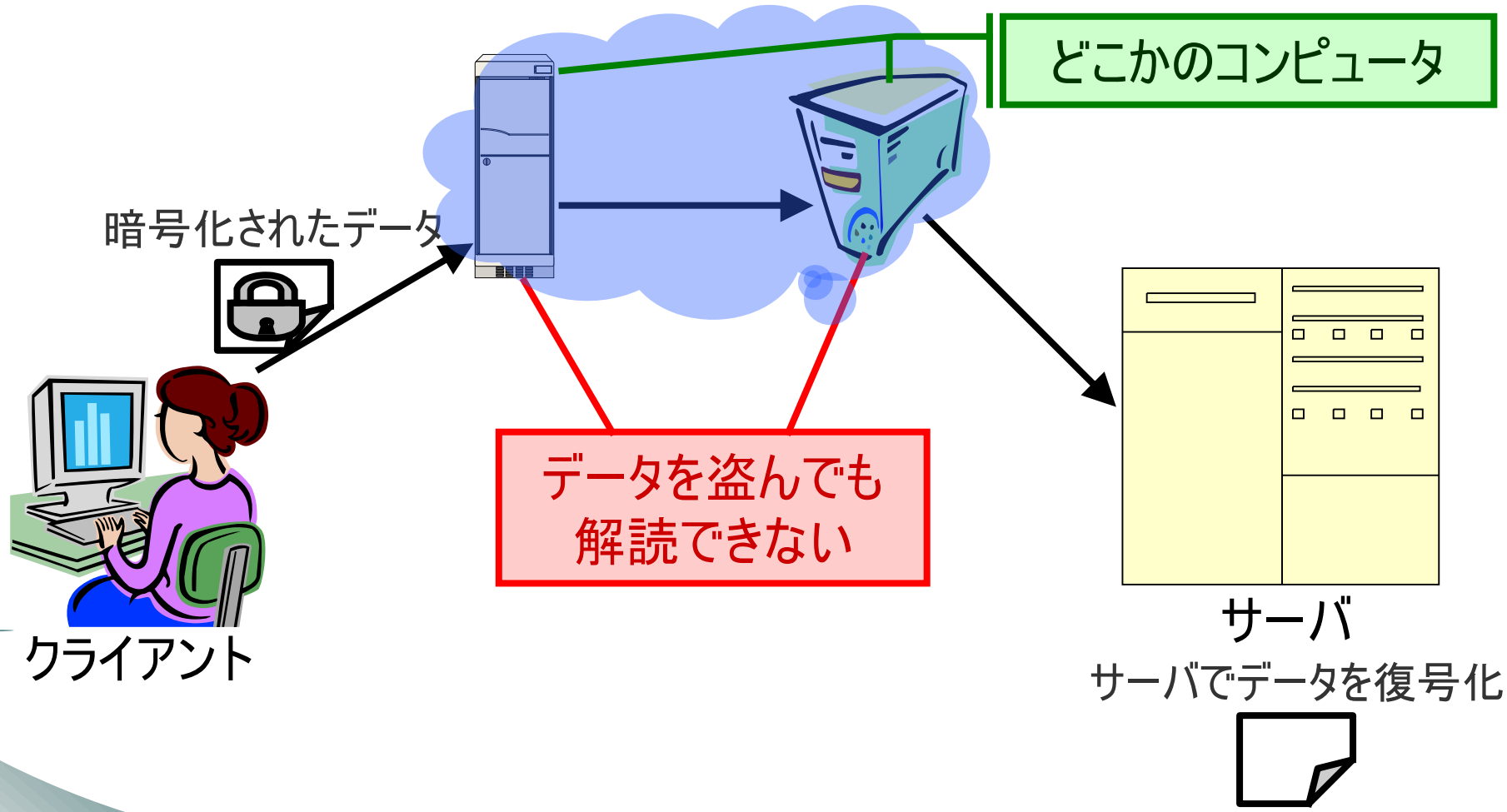
    - データを暗号化し、盗まれても中身を理解不能にする
    - ➡ 正当な受け取り主は、暗号を解読して本来のデータを見ることができるようにする

情報の隠蔽[2](p. 111)

- 暗号化: データを別の形に加工すること
  - データが元の形と違っているので、データを見ても内容がわからない
  - Ex. This is a pen. → Uijt jt b qfo.
    - 暗号化の方法: アルファベットを1文字後ろにずらす
- 復号化: 暗号化されたデータをもとの形に戻すこと
  - 復号化する方法を知らなければ、もとのデータの内容がわからない
  - Ex. Uijt jt b qfo. → This is a pen.
    - 復号化の方法: アルファベットを1文字前にずらす

情報の隠蔽[3](p. 111)

- **暗号化通信**: 利用者の使っているコンピュータで暗号化をして送り、サーバ側で復号化する通信方法

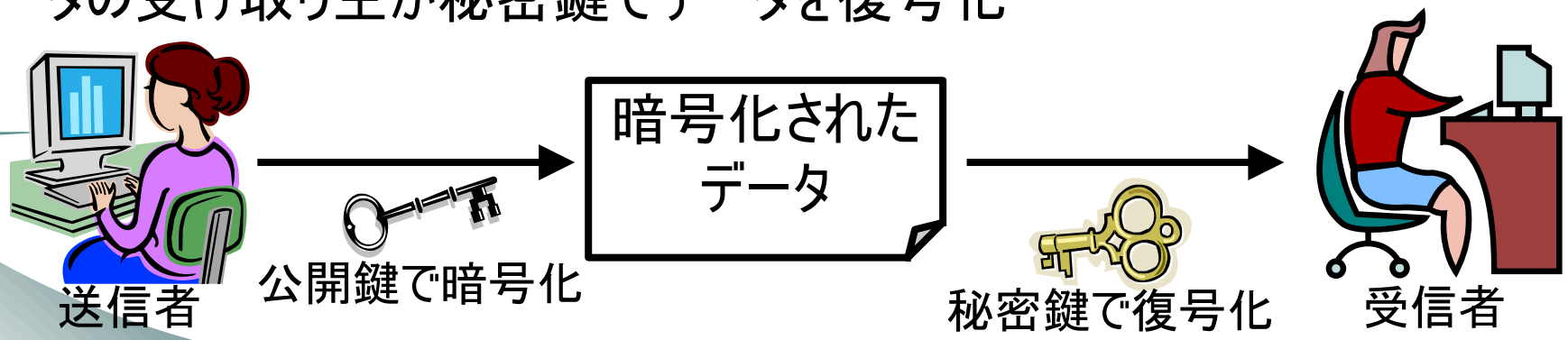


情報の隠蔽[4](p. 111)

- 共通鍵暗号方式(秘密鍵暗号方式とも呼ぶ)
  - データを暗号化するために「暗号鍵」を使う
    - 暗号鍵: データを暗号化するために使うキーワード(キーワードが長ければ長いほど、暗号が解読されにくい)
  - データを暗号化するときと復号化するときで、同じ暗号鍵を使う
  - 欠点1: データを送る側と受け取る側で暗号鍵を受け渡しする方法が難しい
    - 下手な方法では、途中で盗まれてしまう
  - 欠点2: 相手ごとに暗号鍵を用意する必要がある

情報の隠蔽[5](p. 111)

- 公開鍵暗号方式
  - 「公開鍵」と「秘密鍵」という2種類の暗号鍵を使う方法
    - 公開鍵: データを暗号化するための暗号鍵
    - 秘密鍵: データを復号化するための暗号鍵
  - データのやりとりの方法
    1. データの受け取り主が公開鍵と秘密鍵を作成
    2. データの受け取り主が公開鍵をデータの送信者に受け渡し
    3. データの送信者がデータを公開鍵で暗号化し、送信
    4. データの受け取り主が秘密鍵でデータを復号化



情報の隠蔽[6](p. 111)

- 公開鍵方式
  - 秘密鍵を知らなければ、データを復号化できない仕組み
  - 公開鍵と秘密鍵は対
  - 秘密鍵は、データを受け取る側しか知らない暗号鍵
    - 他の人に知られてはならない暗号鍵
  - 公開鍵は、他人に知られても良い暗号鍵
  - 利点: 秘密鍵を割り出そうとすると、膨大な時間がかかるので、事実上不可能
  - 欠点: 共通鍵暗号方式に比べて、復号化処理に時間がかかる

情報の隠蔽[7](p. 111)

- WWWでは、公開鍵暗号方式を利用
  - SSL(Secure Socket Layer)と呼ばれている
- Webの場合、URLが「https://」で始まっていれば、SSLでの通信
  - https: HTTP over SSL
  - 「http://」の場合は、普通の暗号化しない通信

Webでの個人情報の入力時には、URLがhttpsで始まっているかどうかを確認しよう!

認証(p. 113)

- 認証: 正しい権限を持った人かどうかを確認すること
- 認証の手段
  - パスワード: 最も一般的な方法
    - 手軽で広く用いられているが、推測や漏洩の危険性大
  - バイオメトリクス: 人体の身体的特徴を利用する方法
    - 指紋や虹彩、顔などの固有情報を利用
  - 電子署名: 文書を、作成者本人が作ったこと(改ざんされていないこと)を証明する方法
    - 秘密鍵で文書を暗号化
    - 公開鍵で文章を復号化

} うまく復号化できれば、改ざんされていない