コンピュータ・サイエンス2

第11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

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

今回の内容

- 情報ネットワーク(実習)

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

設問1

- 下記の説明にあてはまる言葉を答えなさい。
  1. セグメントまたはデータグラムに送信元や宛先のデータを付加したもの
  2. 必要な情報をデータに付加すること
  3. ネットワークケーブルの規格を定め、データを電気・光信号の形に変換することを担当する、OSI参照モデルの層

解答:

1. パケット
2. カプセル化
3. 物理層

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

設問2

- 下記について、正しいものと間違っているものを考えなさい。
  a. スマートフォンでLINEをするときはIPアドレスは不要である。
  b. 日本のある1台のコンピュータと、アメリカのある1台のコンピュータに、同じIPアドレス(インターネット通信用)が設定されると、その2台はインターネットに接続できない。
  c. 1台のコンピュータで同時に2つのIPアドレスを使うことができる。
  d. スマートフォンを使ってGoogleで検索をした。このとき、スマートフォンがサーバ、Googleのコンピュータがクライアントである。

解答:

- 正しいもの: b, c
- 間違っているもの: a, d

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

前回の質問の回答

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

前回の復習

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

名前解決(p. 102)

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

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)

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

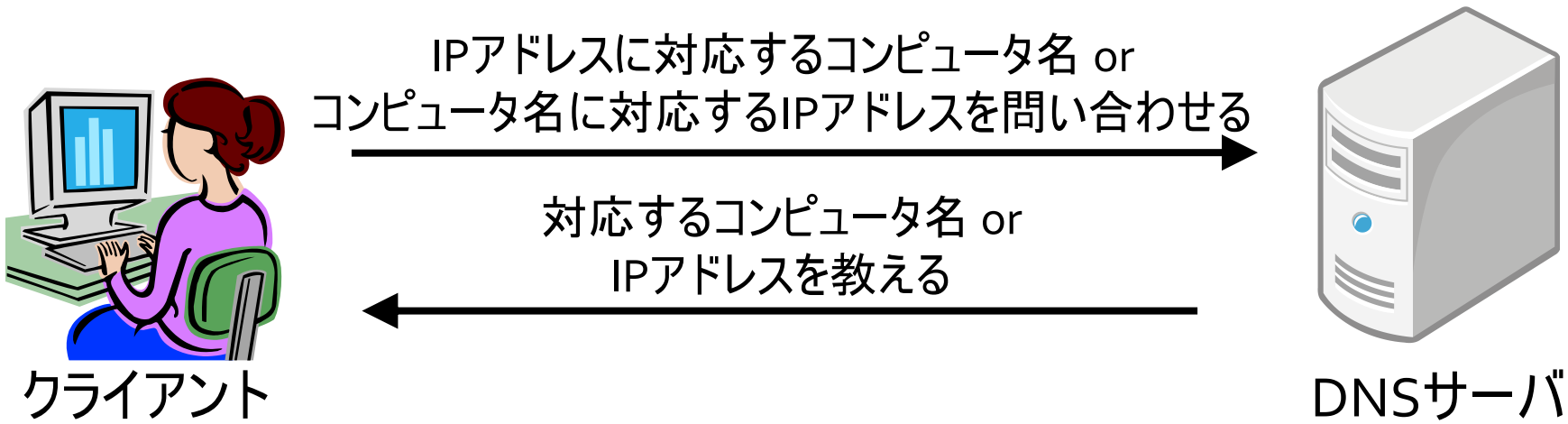
DNS[2](p. 102)

- 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

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

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



Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

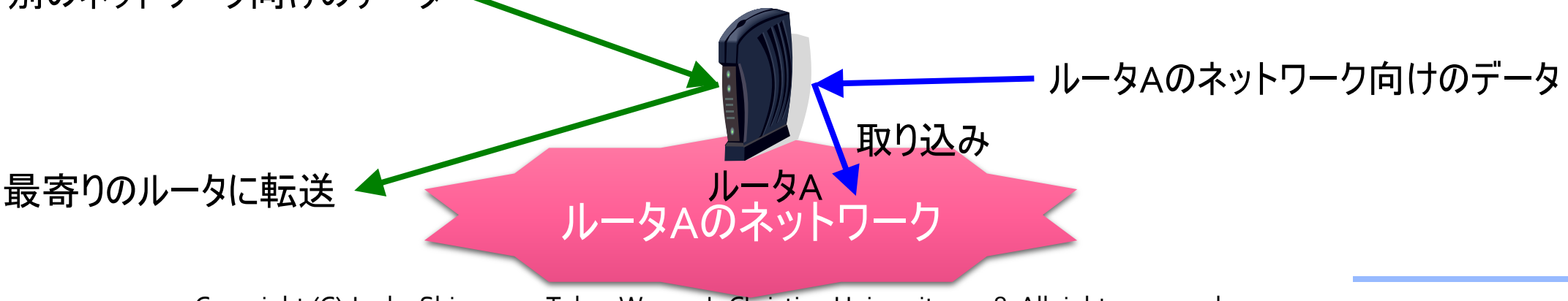
経路制御

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

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

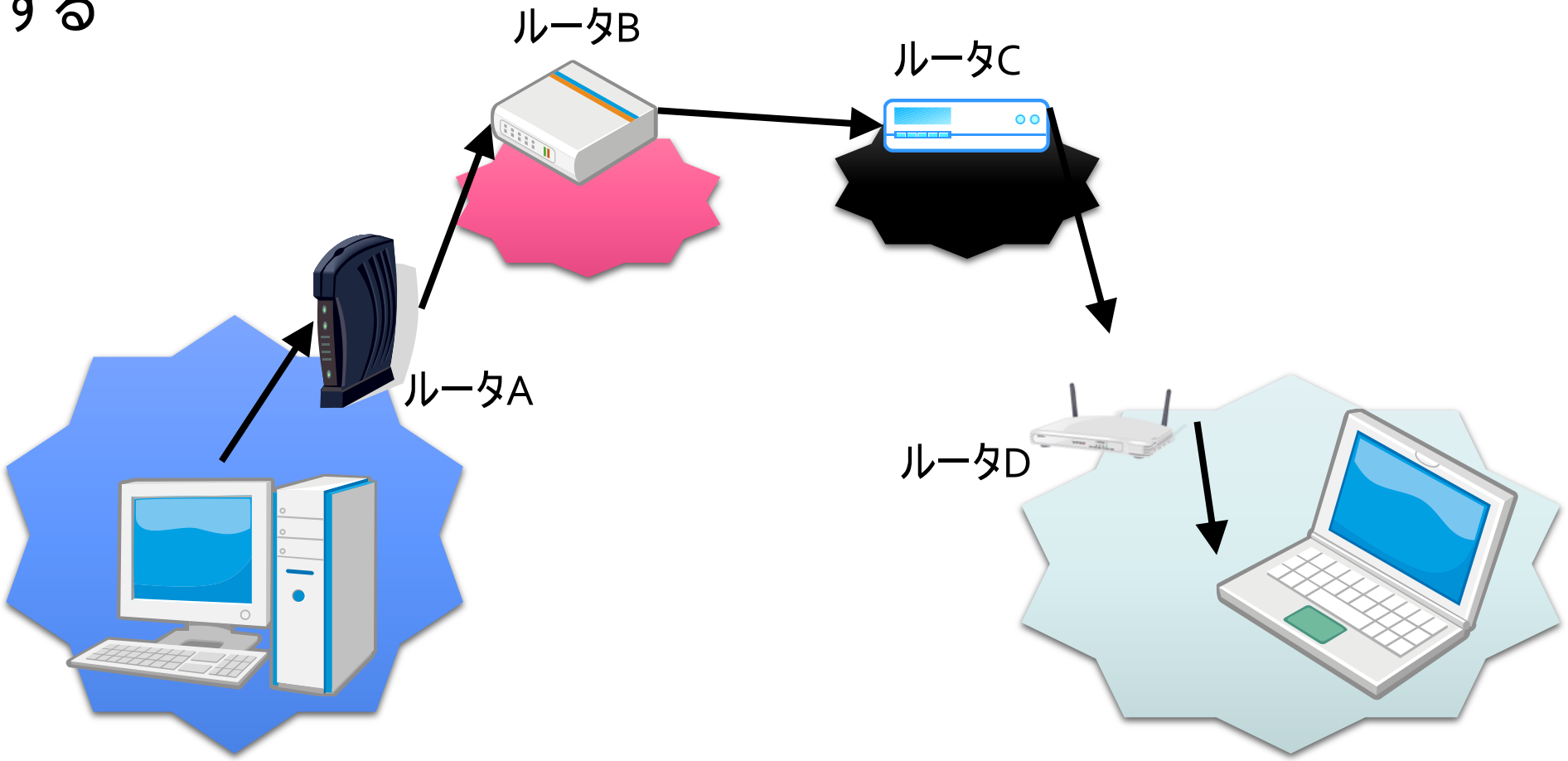
データの宛先のIPアドレスで判断



Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

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



Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

ネットワークセキュリティ

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

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!

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

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

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

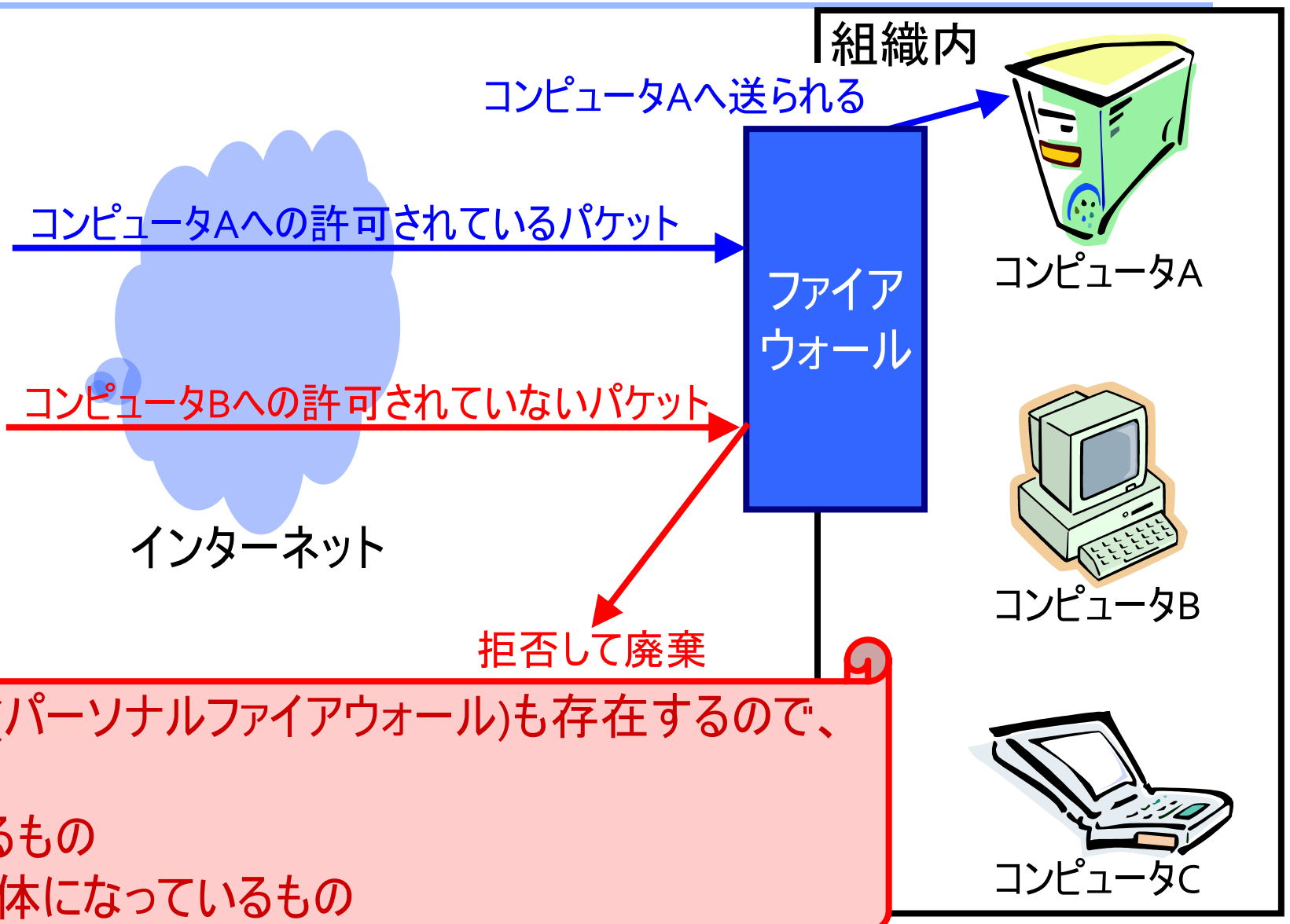
情報の隔離[2](p. 110)

- 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)

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

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

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

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

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

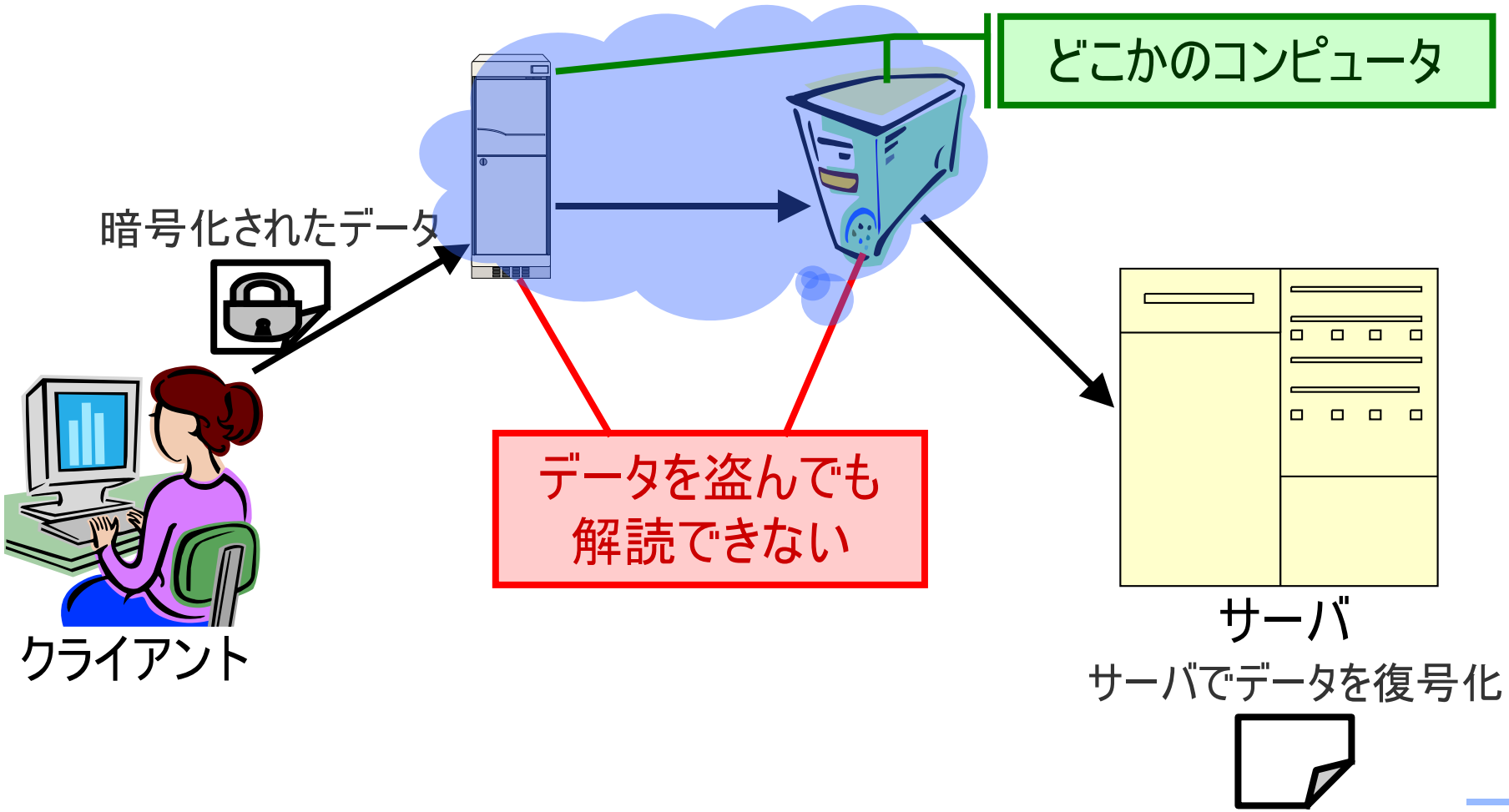
情報の隠蔽[2](p. 111)

- 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

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

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



Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

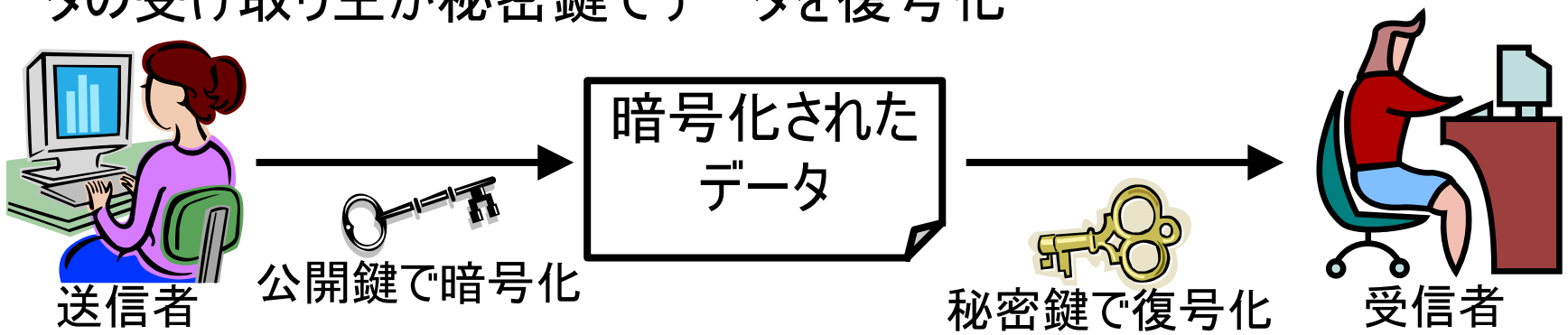
情報の隠蔽[4](p. 111)

- 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

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

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



Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

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

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

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!

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

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

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

Question!

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

実習

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

準備～ターミナル～[1]

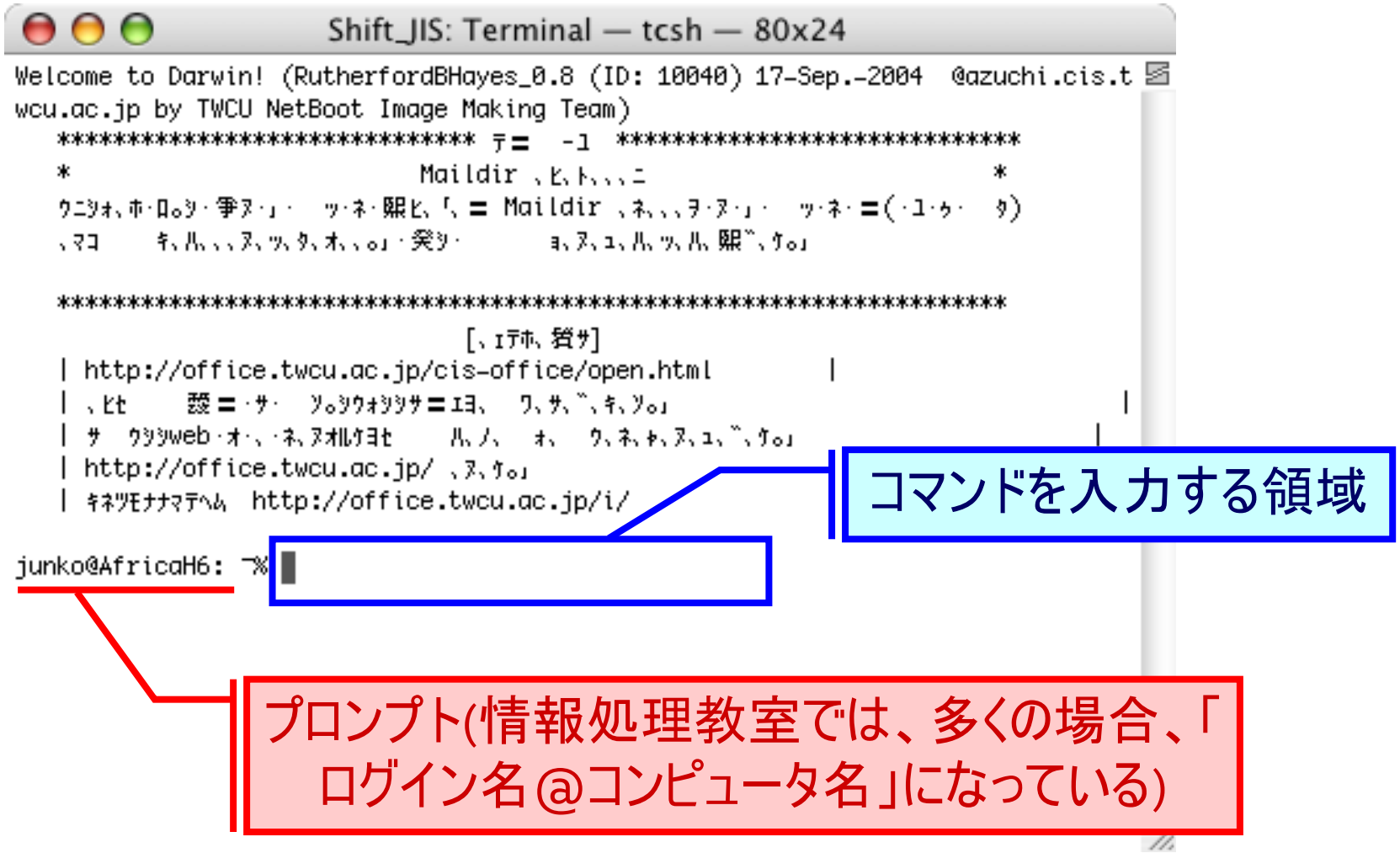
- ソフトウェアの名前(+α)を入力することで、ソフトウェアを使うための道具
  - 普通、ソフトウェアを使うときには、そのソフトウェアのアイコンをダブルクリックすると、ソフトウェアが起動
  - ターミナルでは、ソフトウェアの名前(+α)を入力し、「Return」キーを押すと、ソフトウェアが起動
- 今回の実習で使うターミナル:
  「Finder」→「アプリケーション」→
  「ユーティリティ」フォルダを開き、その中の「ターミナル」をダブルクリック

「コマンド」と呼ぶ

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

コマンド入力の基本(1)

- コマンドは、「プロンプト」の後ろに半角英数で入力



Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

コマンド入力の基本(2)

- コマンドの形

「コマンド名」がソフトウェアの名前に相当

コマンド名　引数

  - 必ず「コマンド名」を最初に入力し、その後に「引数」を入力
  - 「コマンド名」と「引数」の間にはスペースが1つ以上必要
  - 「引数」は1つとは限らない
  - 「引数」が複数ある場合には、引数と引数の間にもスペースが1つ以上必要

例えば、コマンド名「ls」、引数「WWW」の場合:
「ls WWW」と入力

- 入力したコマンドを間違えていても、消すことは不可

間違えた内容を消さなくて良いので、コマンドを入力しなおして実行しなおし

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

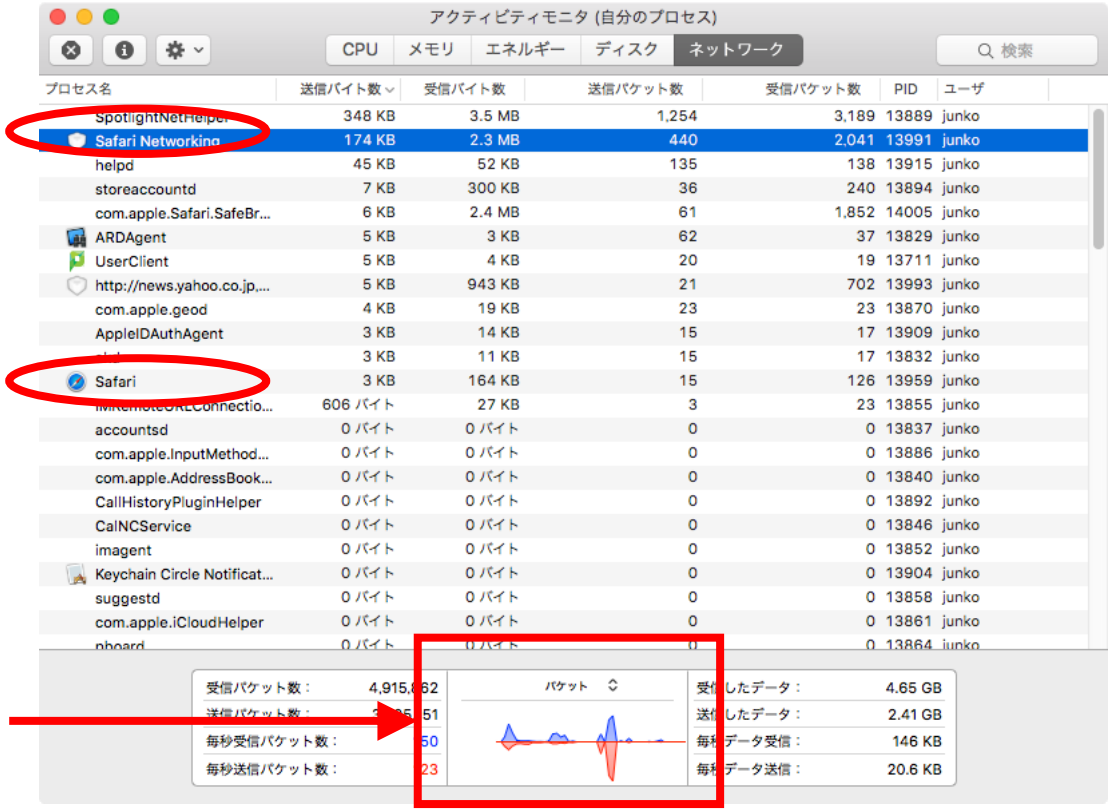
パケットチェック[1]

- Finder→「アプリケーション」→「ユーティリティ」→「アクティビティモニタ」を起動
  - コンピュータの様々な状態をチェックするアプリケーションが起動
- 「ネットワーク」タブを選択
- メニューバーの「表示」→「自分のプロセス」をチェック
  - 自分が使っているアプリケーションでの、ネットワーク通信の状態が表示

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

パケットチェック[2]

- Safariを起動して、送信・受信パケットの量の変化を見てみよう!
  - 様々なWebページへアクセスしてみる
  - 「Safari Networking」や「Safari」の項目でチェックする



送信・受信パケットの量の移り変わり

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

相手先への経路確認

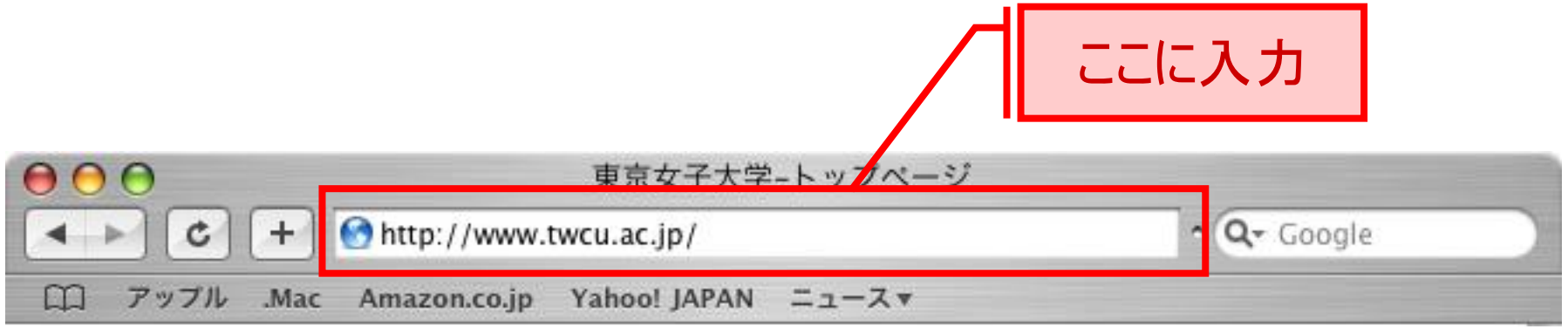
- 様々なコンピュータに、どのような経路をたどってたどり着くかを調べてみよう
  1. ターミナルで
     traceroute　コンピュータ名
     と入力し、「Return」キーを押す
     - コンピュータ名は、「www.twcu.ac.jp」など、様々なWebページの「http://XXX/...」の「XXX」の部分を入力してみる
  2. どのような経路をたどっているか、確認してみる

※表示が止まってしまったら、「Ctrl」キーを押したまま「C」キーを押す

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

IPアドレスの確認

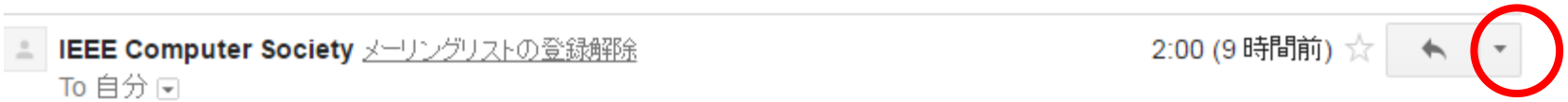
- コンピュータ名→IPアドレスの調査をしてみよう
  - ターミナルで、
    host コンピュータ名
    と入力し、「Return」キーを押す
    - コンピュータ名は、「www.twcu.ac.jp」など、様々なWebページの「http://XXX/...」の「XXX」の部分または、メールアドレスの「@」以下の部分入力してみる
  - IPアドレスでWebページにアクセスしてみる
    - 「http://XXX/...」の「XXX」の部分にIPアドレスを入れて、Webページにアクセスしてみる



Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

メールの経路確認

- 大学のメールで、どのような経路をたどってメールが届いたか、確認してみよう
  - 他の人から届いたメールで、上部の「返信」ボタンの右の「▼」→「メッセージのソースを表示」



    - できるだけ、大学外のメールアドレスからのメールが望ましい
    - 大学外からのものがなければ、携帯メールを送ってみる
  - 表示されたウィンドウで、「Received:」の項目をチェック
    - どのくらいの経路をたどって届いているか?

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

Question!

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

データ構造とアルゴリズム

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

データ構造(p. 116)

- データ構造: データをメインメモリに格納するときの形式
  - コンピュータはデータをメインメモリに記憶させて処理
  - コンピュータが扱いやすい形式で格納する必要
  - データの形式によって、プログラムの効率に大きく影響

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

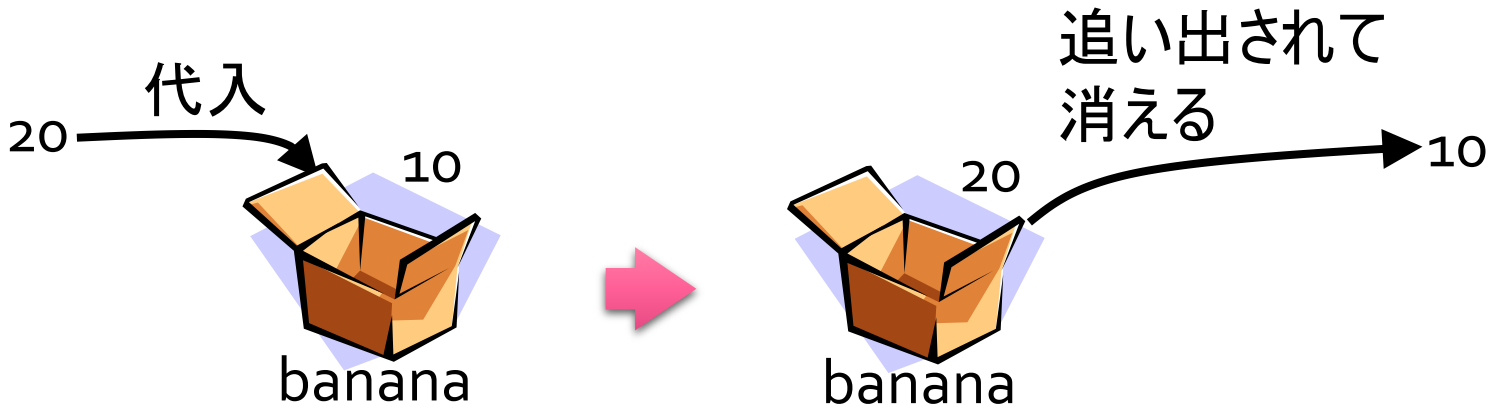
変数(p. 116)

- 変数: 計算の対象や処理結果などのデータを記憶しておくための場所
  - データを入れておく「箱」と言うことができる
  - 変数には名前をつける
  - 変数にデータを入れることを「代入」と呼ぶ
  - 変数に入れられたデータのことを「値」と呼ぶ
  - 変数の名前を指定するとデータを取り出すことができる
  - 変数は扱うデータの個数分だけ用意する

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

変数の特徴[1](p. 116)

- 変数の中のデータを取り出しても、変数の中にデータは残っている
  - 「変数の値を参照する」とは、「箱の中のデータを見る」という意味
- すでにデータが入っている変数に別のデータを入れると、元のデータは消えてしまう
  - 1つの変数に入れておくことができるデータは1つだけ



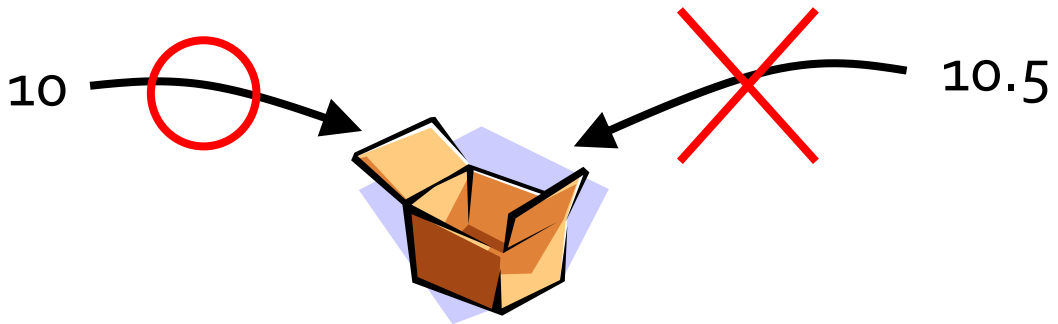
Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

変数の特徴[2](p. 116)

- データの種類によって、違う箱を使う必要がある
  - 整数用の箱
  - 実数用の箱
  - 文字列用の箱
  - etc.

  ➢ 整数用の箱に実数を入れることはできない
  ➢ 文字列用の箱に整数や実数を入れることはできない

あらかじめ、「この名前の箱は整数用の箱」と、決めてコンピュータに知らせた上で箱を使い始める



banana: 整数用の箱

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

「配列」って?[1](p. 116)

- データの種類(整数や小数)が同じで、処理方法も同じ変数をたくさん扱うときに利用する変数
  - たくさんの変数を1度にまとめて利用する方法

例えば…生徒の英語の成績を扱うプログラム(30人分)

出席番号1番の生徒の成績
出席番号2番の生徒の成績
….
出席番号30番の生徒の成績

} 30個の変数が必要!

→ english1, english2, english3, …, english30 のように用意して使うのは大変!

→ 「配列」を利用

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

配列って?[2](p. 116)

- 配列を利用するには…
  - 扱うデータのグループに名前を付ける(配列名)
    - Ex. 生徒の英語の成績: english
  - 配列名に番号(添え字)を「[]」でつけて、個々のデータを扱う
    - Ex. 生徒の英語の成績
      - 出席番号1番の生徒の成績: english[0]
      - 出席番号2番の生徒の成績: english[1]
      - ….
      - 出席番号30番の生徒の成績: english[29]

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

アルゴリズム

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

アルゴリズムとは[1](p. 118)

- アルゴリズム: ある問題を解決するときに必要な処理手順
- プログラムでの処理の方法を記述したもの
  - 何をどのように行うかを記述
  - コンピュータには手順を1つ1つ詳細に指示する必要
    - 人間には一言ですむような処理でも、コンピュータがその処理をこなすには、たくさんの手順が必要

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

アルゴリズムの書き方(p. 119)

- 文章で書く
  - 箇条書きで書くことも多い
- プログラミング言語に自然言語を混ぜて書く(疑似言語)
  - 自然言語: 普段人間が話したり書いたりしている言葉
- 図で描く
  - フローチャート(流れ図)を使うことが多い

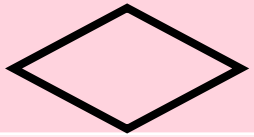
Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

フローチャート[1](p. 119)

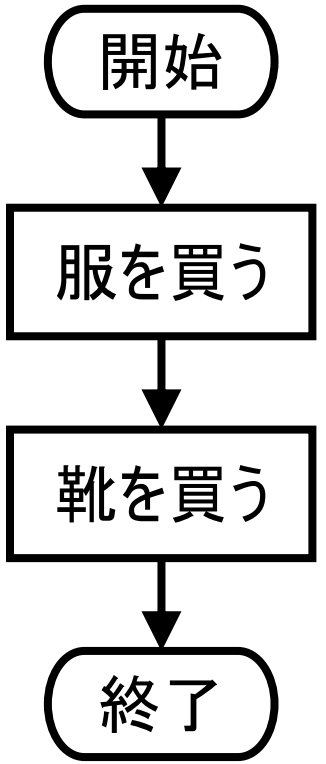
- 記号や矢印などを使って処理の流れを描いた図
- 順次処理、条件分岐、反復処理が基本
  - 順次処理:プログラム中に書いてある命令を、上から順に1つずつ処理すること
  - 条件分岐:ある条件を満たしたときとそうでないときで、処理内容が変わること
  - 反復処理:ある条件が満たされている限り、処理を繰り返すこと

Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

フローチャート[2](p. 119)

記号	意味
	開始と終了
	処理
	条件判断
	処理の流れ

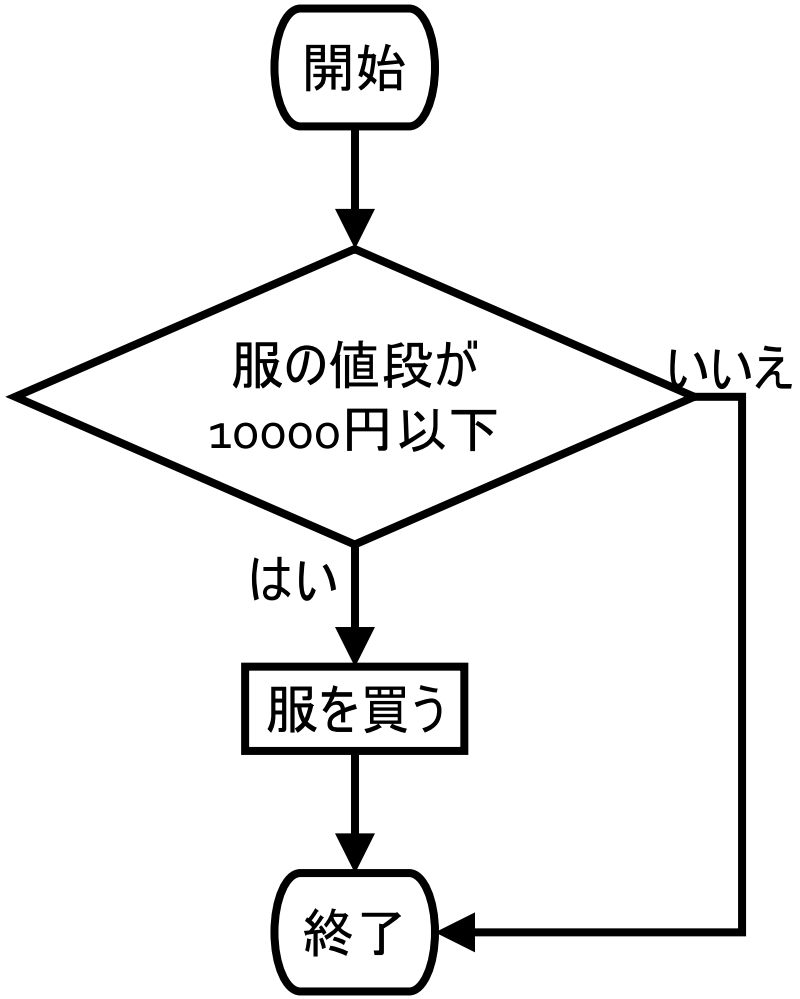
順次処理の例



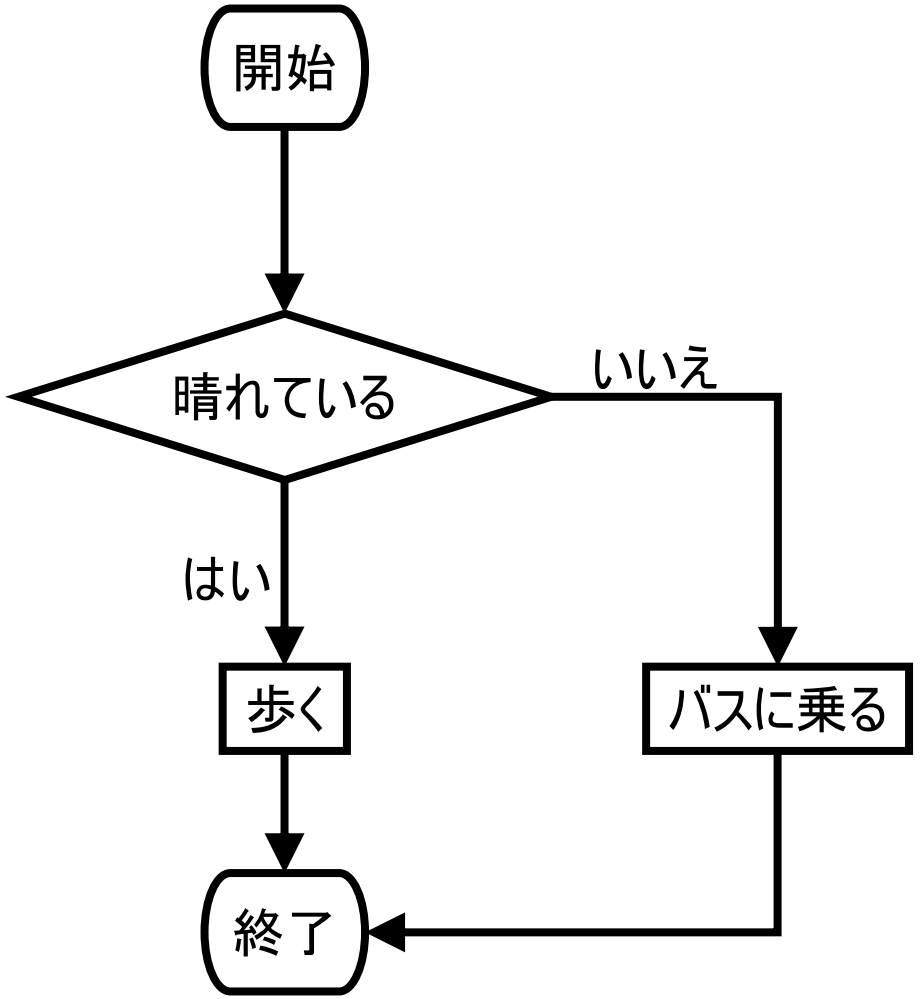
Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

フローチャート[3](p. 119)

条件分岐の例1
(条件判断が「いいえ」の場合何もしない)

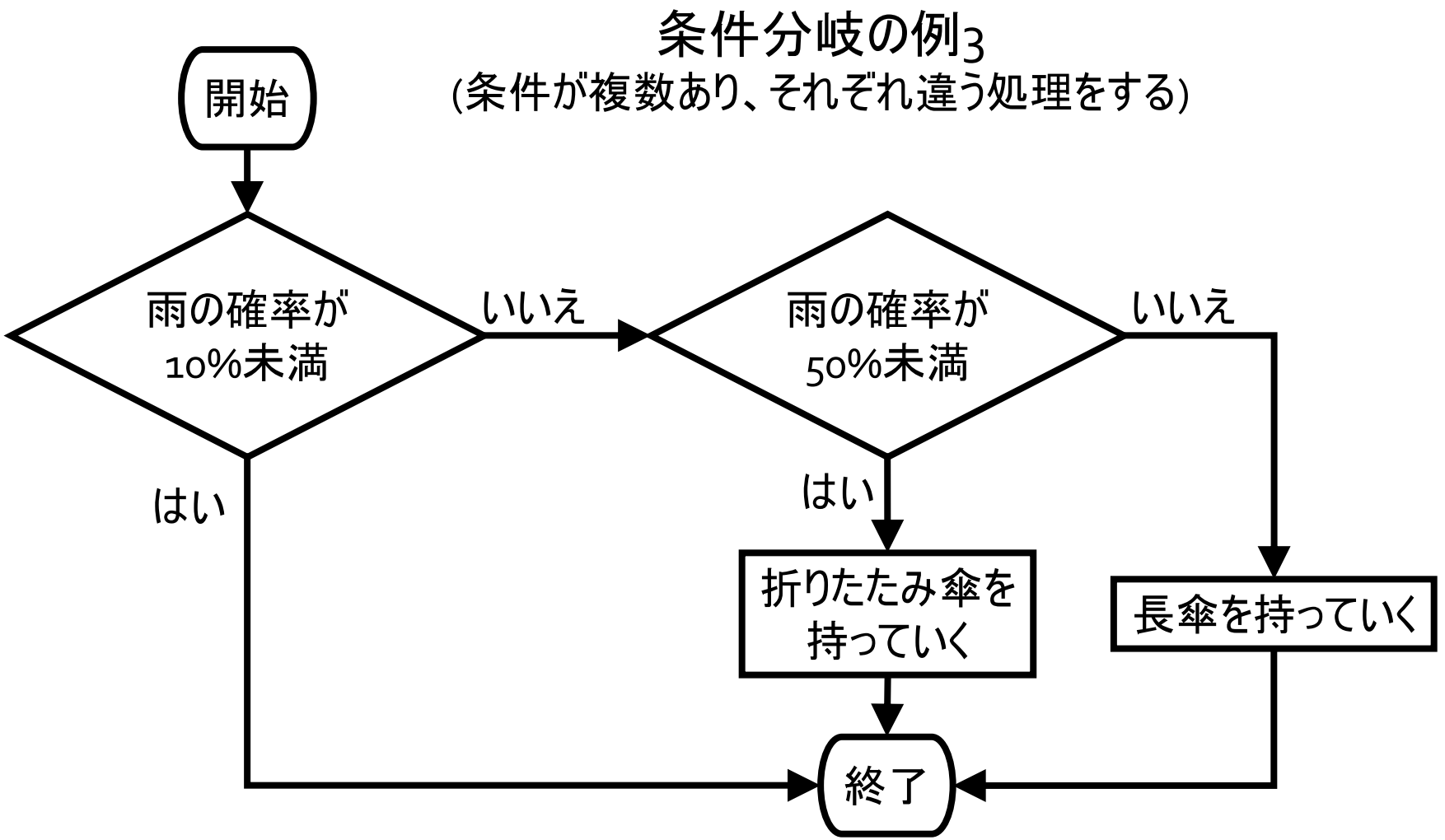


条件分岐の例2
(条件判断が「いいえ」の場合別のことをする)



Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

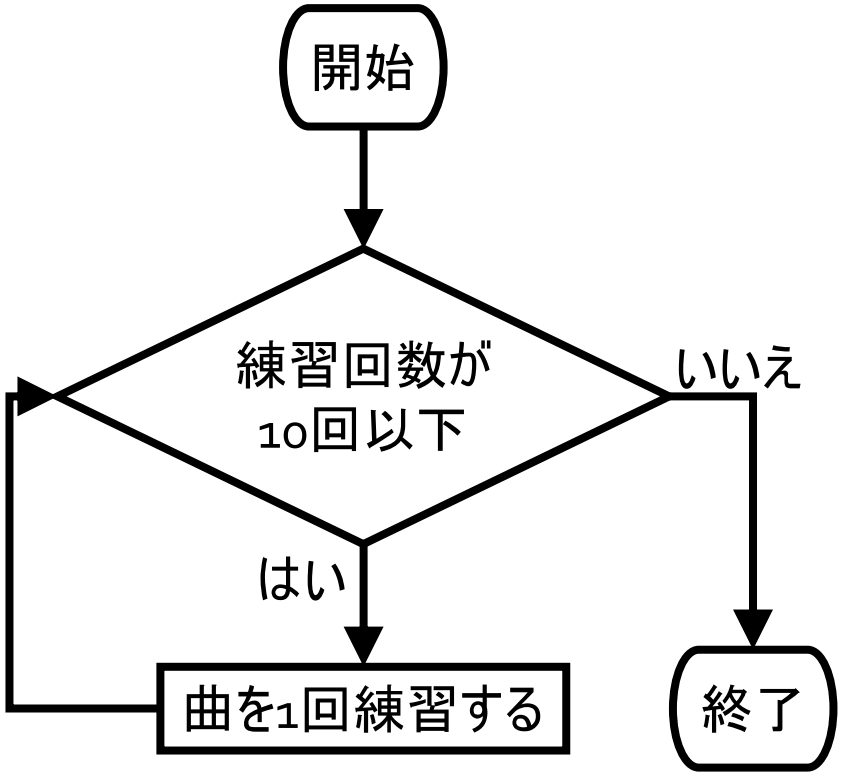
フローチャート[4](p. 119)



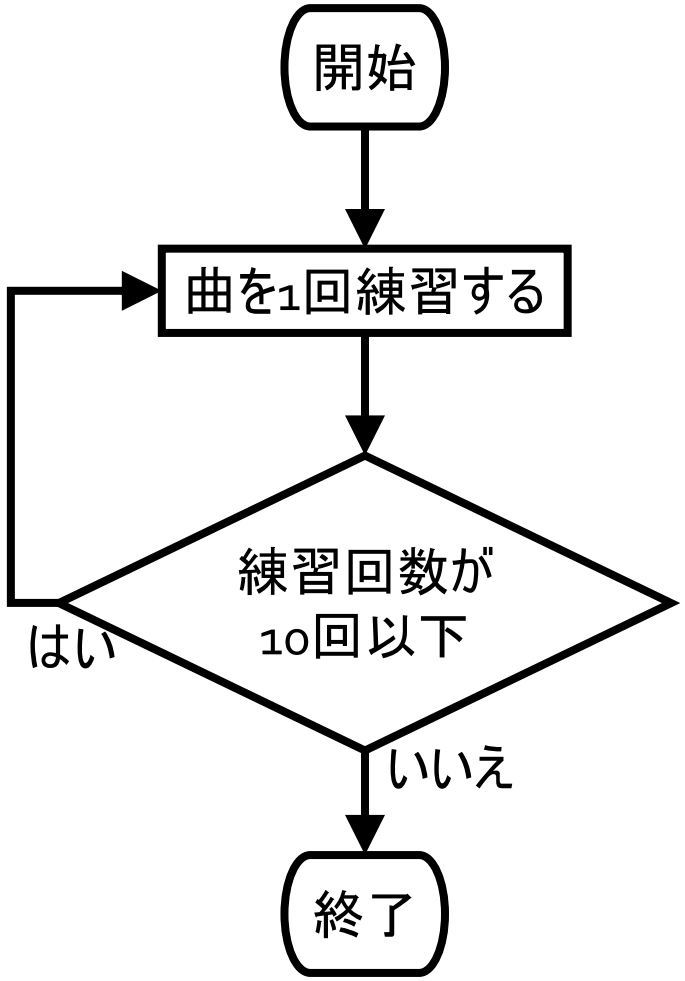
Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.

フローチャート[5](p. 119)

反復処理の例
(最初に条件を判断)



反復処理の例
(最初に処理をしてから条件を判断)



Copyright (C) Junko Shirogane, Tokyo Woman's Christian University 2018, All rights reserved.