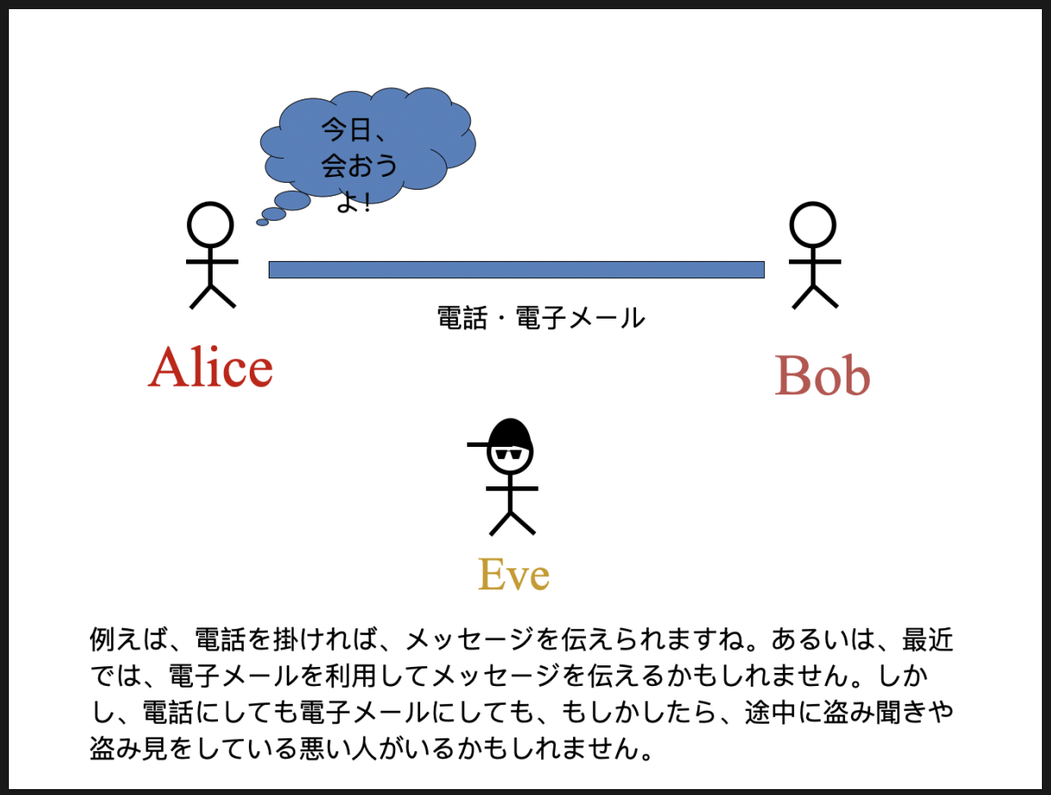
(再掲)秘密通信はどう実現できる

- Alice と Bob は遠くに離れているところに住んでいて、Alice さんは Bob さんにメッセージを伝えたいとしましょう。
- ただし、メッセージの内容を他の人に知られたくありません。



- 事前に秘密を共有すれば解決できそうだが、その秘密はどう共有するの?

公開鍵暗号方式

- 公開鍵と秘密鍵のキーペアを生成する
  - 公開鍵：暗号化する（全世界に公開しても良い）
  - 秘密鍵：復号化するのに使う（誰にも公開しない）
- 安全性
  - 公開鍵や暗号文から秘密鍵へ推測困難
  - 原理：素因数分解問題の計算困難性（計算量的安全性）

【ハンズオン】SSH で GITHUB を利用する

- 新しい SSH キーを生成する
- GitHub アカウントに新 SSH キーを追加する
- 接続可能かを検証する

JAVASCRIPT 、その他

- 分割代入 (Destructuring assignment)
- 残余引数 (Rest parameters)
- JSON 操作
  - JSON.parse()
  - JSON.stringify()