# パスワード管理のアイデア

現在の問題は、どれほど個人で用心しても相手サイトから漏れる場合があること
（https://haveibeenpwned.com でチェックしてみよう）
→ パスワードを共用しない。一つ漏れれば、別のサイトでも悪用される
→ とりあえず安全といえるパスワードの長さは15文字以上
→ **記憶できるわけがない**

対策1: ブラウザのパスワード保存機能を信頼する
→ 共用PCでは使えない
対策2: LastPass, Dashlane, 1Passwordなどのパスワード管理ソフトを使う
→ ここから漏れることはないと信じる必要がある
対策3: 紙のリストを使う　→ 紛失・盗難・押収に備える必要がある

IJF2019（欧州ジャーナリズム会議）では、紙に書き、財布に入れておくことを勧めています
二段階認証は必要に応じて使います（もちろん携帯電話番号を相手に提供してしまいます）

| パスワード | 用途 |
|---|---|
| パスフレーズ（キャッチフレーズくらい長い、大文字or小文字だけ） | PGPパスフレーズ |
| パスフレーズの最初の__文字分 | 自分のPCのログイン |
| **重要アカウント（決済を伴うもの）** | |
| __文字分 + jc26173 | 社内ネットワーク |
| __文字分 + B_2019 | 銀行 |
| __文字分 + g@2019 | Google（二段階認証） |
| __文字分 + apT19 | Appleアカウント |
| __文字分 + amazon2019 | Amazon |
| **発信を伴うもの** | |
| __文字分 + Gh3I | Twitter（二段階認証） |
| __文字分 + MW9 | Yahooアカウント |
| __文字分 + MW9 | ニュースサイト |

追加部分に@yahooなどのようにサービス名を使わない（簡単に類推される）
**パスフレーズだけを記憶し、使い方は紙という物体に頼る**ことに意味がある。絶対にパソコンには保存しないこと