# 7.セキュリティ要求

1. **主体認証**

* システムでは、各ユーザを認証のために、ユーザにusernameとパースワード（主体認証情報）を融通します。それでは、各ユーザはアカウントがあります。
* 各アカウントは先生と学生とシステム管理者の区別情報を追加します。
* ユーザが特別な機能を利用するとき、ログインしなければなりません。例えば勉強の機能、アップロードの機能、システム管理の画面。。。パブリックの情報をアクセス時ログインしないでもいいです。
* ログイン機能の要求：
* システム管理者（Admin）に対して、IP情報をチェックします。予め決められたIP アドレスだけログインできます。
* username とパースワードを５回間違う場合、一時的にロックし、verifycode を送って一回確認する。
* ２４時間でログインすると、自動ログアウトします。
* ユーザはパースワードを覚えない場合、パースワードを引き取る機能があります。

1. 機能を限る

* ログインしたアカウントは先生か学生か管理者かによる各機能をアクセスできるか決定します。
* アップロード機能に対して、以前使用したIP アドレスとは違うIP アドレスでアクセスするとverifycode を送って一回確認します。

1. 脅威

* データベースに不正アクセスの脅威

対策：

* データベースにアクセスのために、usernameとpasswordを必要です。
* ユーザ情報のテーブルにはパスワードを暗号化しなければなりません。データベースにアクセスできる場合、ユーザのアカウントを取れません。
* アカウントが亡くなる脅威　：　ログインして、ログアウトしないで、他の人はアカウントを取ります。

対策：

* ２４時間でログインすると、自動ログアウトします。
* 盗み聞き：データをクライアントからサーバに送信するとき、データを盗み聞き脅威があります。

対策：

* クライアントでデータを暗号化して、送信します。

1. **バックアップ／リストア**

* 定期的にデータベースをバックアップします。
* データベースは事故があれば、リストアします。
* コードもバックアップします。