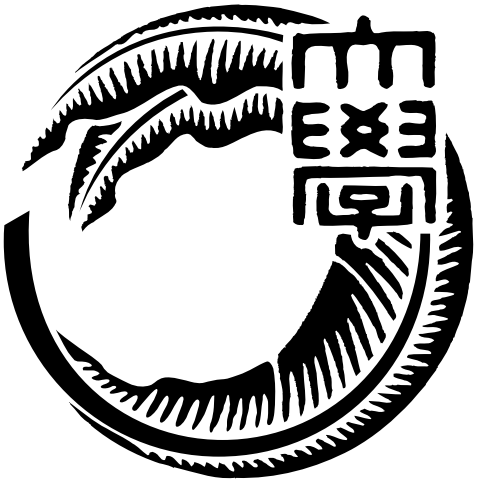
令和元年度 卒業論文

公開暗号方式を用いたSSH認証による アカウント作成の簡略化

Simplify Creating Account by SSH Authentication using Public-key Cryptography



琉球大学工学部情報工学科

165714D 与那嶺東

指導教員 長田智和,谷口祐治

目 次

図 目 次

表 目 次

第1章　はじめに

1.1　背景と目的

1.2　論文の構成

第2章　基礎概念

2.1

2.2

第3章　提案手法

3.1　ボツ案

3.1.1　ログイン状態のセッション橋渡し

実装したいこと
公開鍵暗号方式による ssh 認証を成功した際に，WEB サービスでログイン状態になる．ここでいう，ログイン状態は，セッションを用いて，ステートフルな通信をする (HTTP 通信はステートレスな通信).

実装するための手段案
ログイン状態のセッション情報を橋渡しすることにより，実現しようと考案した。以下の図 3.1 を用いながら説明する。

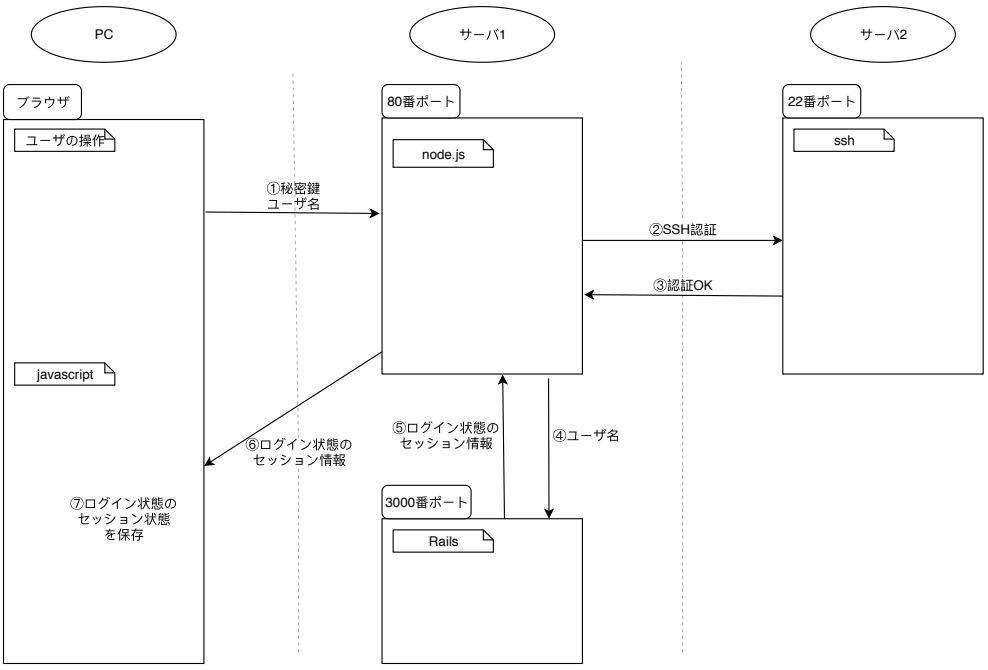


図 3.1: ログイン状態のセッション橋渡し案

図 3.1 の① 〜 ③では，エンドユーザはブラウザを用いて，公開鍵暗号方式による ssh をしている。図 3.1 の④では，HTTP リクエストの POST をしている。図 3.1 の⑤では，HTTP レスポンスが来て，そのヘッダ情報に「セッション情報を Cookie に保存する」という情報が付与されている (のちのち, アクセス制限で,localhost からしかアクセスできないようにする). 図 3.1 の⑥では，図 3.1 の⑤の情報を, ブラウザの javascript 側に socket 通信で渡す. 最後に，図 3.1 の⑦で，ログイン状態のセッション情報を Cookie に保存する.

ブラウザを用いての検証
ログイン中のセッション情報を, ブラウザの Cookie に保存することで，ログインすることが可能かを検証する。
検証環境
- 機器
  - MacBook Pro (Retina, 13-inch, Early 2015)
  - macOS High Sierra(バージョン 10.13.6)
- サーバ側
  - Ruby on Rails(6.0.2.1)
  - localhost:3000
- ユーザ側
  - 2っのブラウザ
    - Google Chrome
    - Google Chrome Canary

Crome の開発環境 (デベロッパーツール) を用いて以下の検証を行った。
まず，ログインした際の動きとして，HTTP レスポンスのヘッダ情報に,set-cookie がある.Crome のデベロッパーツールでは，以下の図 3.2 と表示される.

図 3.2: ログイン成功した際の,HTTP レスポンスの抜粋

次に，図 3.2 の HTTP レスポンスを元に，ブラウザの Cookie にセッション情報を保存する。Crome のデベロッパーツールでは，以下の図 3.3 と表示される.
上記の 3.2,3.3 は,HTTP レスポンスのヘッダ情報で, ブラウザの Cookie に値を保存して

図 3.3: ブラウザの Cookie のセッション情報

いる. その後,HTTP リクエストで,Cookie 情報を付与 [1] することにより, ステートレスな

プロトコルである HTTP 上で，状態管理ができる [2](ログイン状態の維持).
現状で以下の図 3.4 のように，ログインしているブラウザ，ログインしていないブラウザがある.

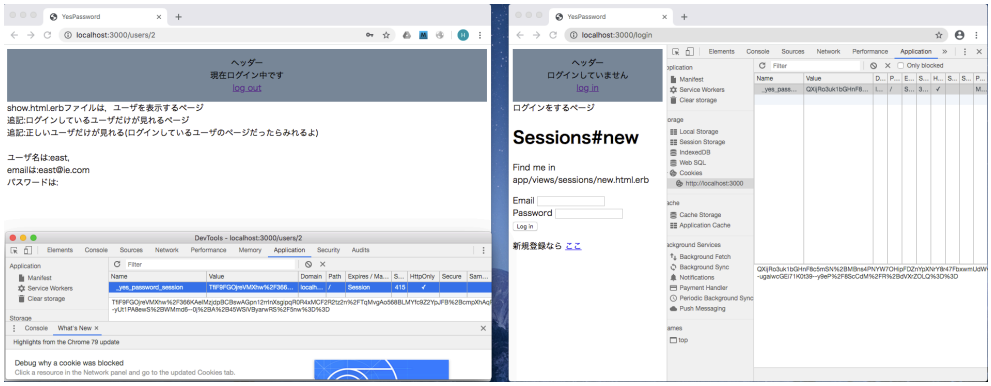


図 3.4: 2っのブラウザ (ログイン状態, ログインしていない状態)

上記の図 3.4 の状態から次の操作を行う. デベロッパーツールを用いて，ログインしているブラウザから，ログインしていないブラウザに，Cookie 情報の, コピーアンドペーストを行い. リロードする. その際の，状態が以下の図 3.5 になり, ログイン状態のセッションを橋渡し (Cookie に保存) することにより, ログインすることができることがわかる.

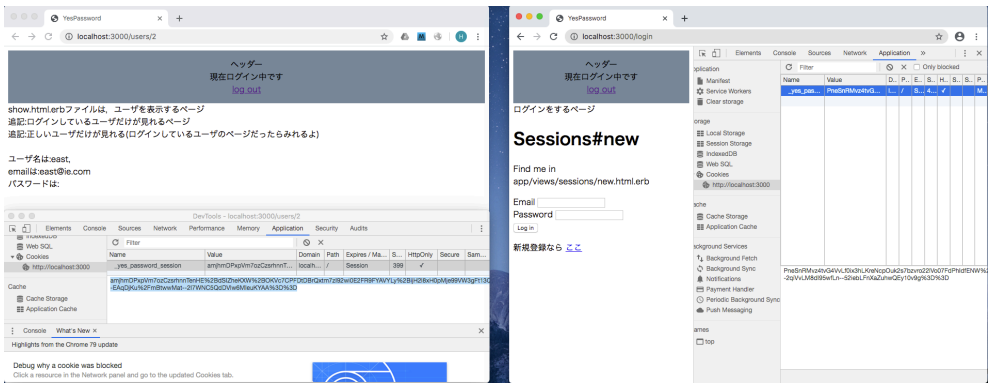


図 3.5: 2っのブラウザ (ログイン状態, ログイン状態)

図 3.5 の補足.
HTTP リクエストをする際に, 新しい Cookie 情報が付与されることが確認できた. そのことにより, ログイン中の 2っのブラウザが別のセッションになっている.

実際に実装
実際に実装を進めて，図 3.1 の① ～ ⑥までできた. しかしながら，図 3.1 の⑦ができなかった. その理由を以下の図 3.6 を元に説明する.
図 3.6 の⑤ で,rails ではセッションを発行する際に,http-only 属性を付与している [3]. その

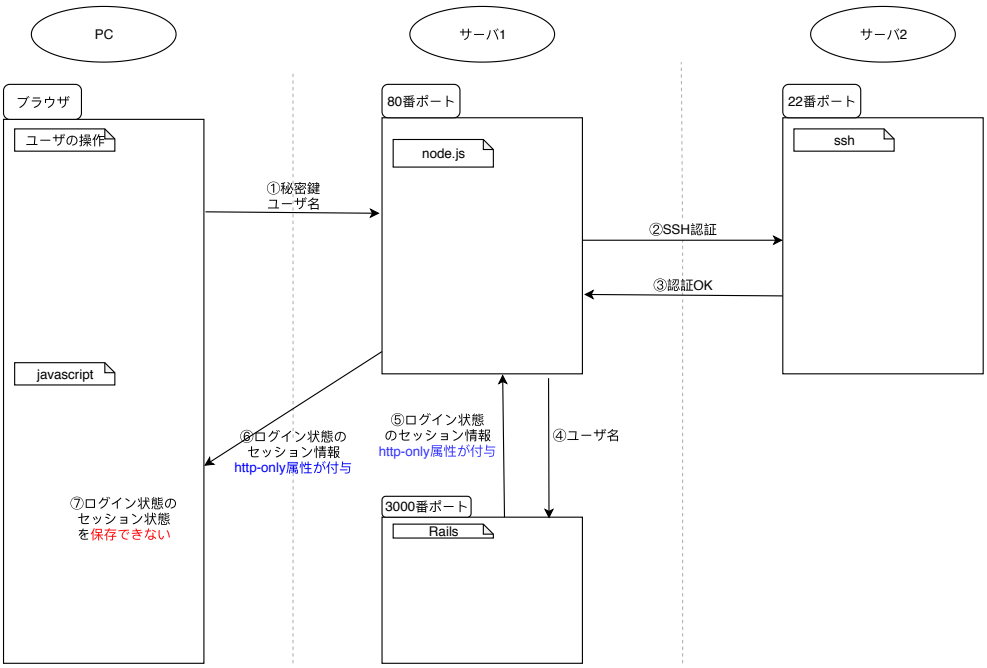


図 3.6: ログイン状態のセッション橋渡し案がボツになった

ことは，ログイン時の HTTP レスポンスである図 3.2 でも現れている．http-only 属性がついた Cookie は,javascript で扱うことができなくなり，セッションハイジャックの対策を行っている [4]．そのため, 図 3.6 の⑦のように, セッション状態を保存することができなかったため,「ログイン状態のセッション橋渡し」の案はボツになった.

第4章　検証

4.1　検証1

4.1.1　検証背景

検証目的

password 認証方式の，新規登録・認証の面倒さを解決するために，第 3 章の提案手法で password 認証方式に変わる，公開鍵暗号方式による ssh 認証を用いた,WEB サービス認証の提案を行った。
しかしながら，提案だけだと，新規登録・認証の面倒さを解決していることの根拠に乏しい。よって，検証を行い，第 3 章の提案手法は”面倒さの軽減”に効果的に繋がっているかの確認をする。

検証手段

検証の手段としては，実際に, 以下の 2っの認証方式の登録・認証を被験者に体験してもらう。

- パスワード方式認証 (以後 ”パスワード認証”と記述する)
- 公開鍵暗号暗号方式による ssh 認証 (以後 ”鍵認証 ”と記述する)

その後，2っの観点から，”面倒さ”を数値化する。
1っ目の観点は「時間」である。”面倒さ”をアカウント登録・認証にかかる時間と推測し，計測化する。詳しい詳細については，検証環境のマニュアルに記述する。
2っ目の観点は「アンケート」である。アンケートには，点数で答える方式, 文字で記入する欄 の 2っがあり，点数で答える方式により”面倒さ ”を数値化する。アンケートの細かい内容は，4.1.3 の検証画面に記述する。
また，アンケートには”面倒さ”を数値化する以外にも，以下の 2っの意味を込める。1っ目の意味は次の通りである。アカウント登録・認証にかかる時間 を，”面倒さ”と予想して検証しているが，その予想を確かめる必要がある。アンケートを取ることにより,「アカウント登録・認証にかかる時間」と,「アンケートによる面倒さ」が比例していることを確認することで，予想を確かめることができる。また，被験者の状態も確認することで，面倒と感じるのが，検証自体に対しての面倒さと関係があるのかを確認する。2っ目の意味は次のとおりである。記入欄で，改善点や感じたことの意見をもらうことで，今後の研究に生きるようなアンケートをもらう。

4.1.2 検証環境

検証場所

第 3 章で記述したとおり，検証場所は学科の VM を用いているため，学科のネットワーク内 (有線 LAN,wifi アクセスポイント ie-ryukyu) から検証を行う。

検証画面

検証マニュアル

4.1.3 検証結果

4.1.4 考察

4.2 検証 2

第5章　今後の課題

参考文献

[1] https://tools.ietf.org/html/rfc6265#section-1
最終閲覧日:2020/1/20

[2] https://qiita.com/mogulla3/items/189c99c87a0fc827520e
最終閲覧日:2020/1/20

[3] https://qiita.com/yasu/items/8ae3077bdbee606681f6#cookiestore%E3%81%8C%E5%95%8F%E9%A1%8C%E3%81%AA%E3%81%AE%E3%81%8B
最終閲覧日:2020/1/21

[4] https://developer.mozilla.org/ja/docs/Web/HTTP/Cookies
最終閲覧日:2020/1/21

謝辞

本研究の遂行，また本論文の作成にあたり、御多忙にも関わらず終始懇切なる御指導と御教授を賜わりました hoge 助教授に深く感謝したします。

また、本研究の遂行及び本論文の作成にあたり、日頃より終始懇切なる御教授と御指導を賜わりました hoge 教授に心より深く感謝致します。

数々の貴重な御助言と細かな御配慮を戴いた hoge 研究室の hoge 氏に深く感謝致します。

また一年間共に研究を行い、暖かな気遣いと励ましをもって支えてくれた hoge 研究室の hoge 君、hoge 君、hoge さん並びに hoge 研究室の hoge、hoge 君、hoge 君、hoge 君、hoge 君に感謝致します。

最後に、有意義な時間を共に過ごした情報工学科の学友、並びに物心両面で支えてくれた両親に深く感謝致します。

2010 年 3 月

hoge