ISSN 1343−2885

日 本 大 学 工 学 部 紀 要

第 63 巻 第 1 号

令 和 3 年 9 月

日 本 大 学 工 学 部
工 学 研 究 所

目　　次

工　学　編

工　学　編

遠隔授業実施時の演習サーバへの２要素認証の円滑な導入方法の検討とその評価

杉山 安洋*・中村 和樹**・大山 勝徳***

Smooth Migration to Two Factor Authentication on the Students' Programming Servers Considering Online Courses

Yasuhiro SUGIYAMA*, Kazuki NAKAMURA** and Katsunori OYAMA***

Abstract

This paper reports our process of migration to two factor authentication(2FA) on our students' programming servers while all the programming courses are given online. Our 2FA mechanism adopted is based on smart-phones which most students are familiar with. We built several helper applications to assist the students to setup their smart-phones for 2FA, even if they cannot get face-to-face assistance from the faculty on online courses. As a result, most of the students have successfully completed their migration process to the 2FA without troubles within the expected period of time.

キーワード：２要素認証，ssh，遠隔授業，セキュリティ

１．はじめに

筆者らの学科では，学生が自宅からアクセスしてプログラム演習を行えるようなsshサーバを公開している。大学演習室での演習の時間に終了しなかった課題や，事前学習，事後学習を行うために多くの学生が使用している。特に昨年はコロナウイルスの流行に伴う遠隔授業の実施により，全ての演習の授業をこのサーバを用いて行った。今年度は対面授業の再開にともない一部の科目は演習室を使用するようになったが，依然としてほとんどの科目がこのサーバを用いて演習を行っている。

一方インターネット上での不正アクセスは後を絶たない。このサーバへの不正アクセスも数多く検出されている。侵入されるまでには至っていないが，危険な状況にあることは言うまでもない。しかも，コロナ禍に伴うリモートワークの増加によるネットワークを使用する機会の増加を背景とし，不正アクセスも増えることが様々なところ[1) 2)]で指摘されてきた。

このサーバで検出されている主な不正アクセスの手法は，ブルートフォースアタック（総当たり攻撃）と呼ばれ，存在しそうなユーザ名とパスワードを総当たりで使用して，ログインを試みるものである。この攻撃への防御策として筆者らの学科では以下の対策を行ってきた。

まず，学生が簡単なパスワードや類推されやすいパスワードを使用していると，不正侵入をされることになってしまう。そのため，授業では類推されやすいパスワードは使用しないことを学生へ強く指示している。

さらに，ssh-guard[3)]と呼ばれる不正アクセスを検出するツールも学科のサーバにインストールして使用している。これは，同一の送信元からの認証エラーが連続した場合は，その送信元からのネットワーク接続を一定時間遮断するというものである。しかも，一定時間後には遮断は解除されるが，その後さらに認証エラーが継続すると，より長時間に渡り接続を遮断する機能も持っている。

しかしながら，学生が類推されやすいパスワードを設定する可能性があることは否定しがたい事実である。どうしても覚えやすいパスワードを使用したり，他のサイトのパスワードを使い廻したりしてしまう。多くの不正アクセスの事例の原因が，この理由であることはよく知られている。

この問題への対策の一つに，２要素認証（Two Factor Authentication以後2FA）がある。１つのパスワードのみでユーザ認証を行うのではなく，パスワード以外の情報も用いてユーザ認証を行う方式である。パスワード以外の情報としては，ワンタイムパスワード（使い捨てパスワードあるいは認証コードとも呼ばれる）や生体認証などがある。生体認証を行うためには，顔や指紋の識別ができるハードウェアが必要になり，導入へのハードルが高い。一方，ワンタイムパスワードの導入は，スマートフォンを用いれば手軽に実現できる。

パスワードの安全性チェックツール[4)]を用いて，学生に安全なパスワードへ変更してもらうことも検討した。しかし，いかに複雑なパスワードを使用したとしても，使い捨てでないパスワードを単独で使用している限り，何らかの理由で漏洩すると不正侵入を許してしまう。そこで，筆

令和３年６月30日受理

*日本大学工学部情報工学科演習室管理グループ
**日本大学工学部情報工学科演習室管理グループ
***日本大学工学部情報工学科演習室管理グループ

者らの学科では，ワンタイムパスワードを用いた2FAを導入することとした。

本論文は，遠隔授業実施時というこれまでとは異なる状況で行った演習サーバへの２要素認証の導入の方法や実施状況をまとめ，それを評価したものである。２節で導入した2FAの概要を述べ，３節で導入方式を述べる。４節で導入の実施状況を述べ，５節で導入が円滑に行われたかを検証する。

なお，論文中では，セキュリティ上の理由から，個別のサーバなどの情報が特定できないように架空の名称やモザイク処理を用いている。

２．2FAの概要

今回導入した2FAは，通常のパスワードに加えて，スマホアプリに表示される使い捨てパスワードを使用するものである。使用できるスマホアプリには，Google Authenticator[5]やMicrosoft Authenticator[6]などに加えて，FreeOTP[7]などのようなオープンソースのアプリもある。これらのアプリで生成される認証コードは，同じ初期設定がされていれば全て同一であり，どのアプリでも使い方はほぼ同じであるので，ユーザが自分の好みで使い分けることもできる。また，Google ChromeやApple SafariなどのWebブラウザには2FAのための機能拡張が用意されている。従って，スマートフォンを持たないユーザでも今回導入した2FAを使用できる。

筆者らの学科では，遠隔授業の学内標準ツールとしてGoogle Workspace[8]を使用していたことを考慮し，Google Authenticatorを2FAの標準アプリとしたが，Google Authenticatorが他のスマホアプリと比較して機能的に優れているわけではない。そのため，他のスマホアプリやブラウザの機能拡張版もユーザの希望により使える形とした。

なお，ワンタイムパスワードを電子メールなどでユーザへ通知する2FAの方式も広く採用されている。しかし，この方式ではメールを使用することによって新たなセキュリティ上の問題が発生する可能性がある。また，この方式の実現のためにはメールサーバを準備する必要があるが，大学内でのメールサーバの設置はセキュリティ上の理由から近年難しくなっている。これらのことから，スマホアプリによりワンタイムパスワードを表示する2FAを採用することとした。

本節では，Google Authenticatorアプリを用いた２要素認証の概要を説明する。

まず，ログインの際であるが，サーバへsshコマンドなどで接続すると通常のパスワードに加えて図１に示すようにVerification code（認証コード）の入力を要求される。認証コードはGoogle Authenticatorアプリに図２(a)のように表示されている。この認証コードはユーザごとに異なるだけでなく，30秒ごとに自動で更新されるので，他の人に見られても安心である。Google Authenticatorアプリの右側に欠けた円形の表示があるが，これは現在表示されている認証コードの有効期限の残り期間を示している。この図では20秒程度の残り時間があることが分かる。

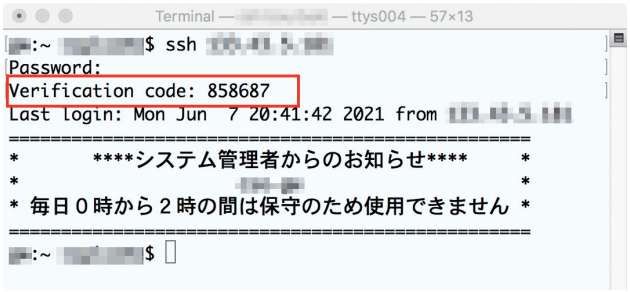

図１　２段階認証を用いた接続

Google Authenticatorアプリを使用するためにはあらかじめユーザごとの設定が必要である。各ユーザはサーバ管理者から送られてくるQRコードをスマホに読み込ませることにより設定を行う。図２(b)はQRコードを読み込んでいる様子を示している。Google Authenticatorアプリからスマホのカメラで読み込むことだけで設定は完了する。QRコードの読み込みは，画面の中央で読まなくても，また多少ピントが合っていなくても大丈夫である。

(a)認証コード表示　　(b)QRコード登録

図２　Google Authenticatorの画面

３．導 入 手 順

2FAの初期導入は昨年（2020年）の前期に実施した。本節ではその際の導入手順について述べる。

2FAを導入する際には円滑に2FAへ移行できることが重要である。突然2FAを導入してしまうと，演習サーバへアクセスできない学生が多く出てしまい授業に支障が出る可能性がある。特に昨年の前期は，遠隔授業が初めて導入された時期であり，遠隔授業に慣れていない学生が多かった。

また，オンデマンド形式の遠隔授業をしている科目も多く，何か問題が発生しても直接学生と接して問題解決の支援をすることができなかった。そのため，以下の方針を設定した。

- 2FAの完全実施までには余裕を持ったスケジュールとする。
- 学生が自分で移行作業を完了できるように簡潔な作業手順とする。
- 何らかの理由で移行の設定に失敗した学生でも演習サーバが全く使用できなくなるような状況は起きないようにする。
- 全学生が同時に2FAへ移行できる可能性は低いので，2FAの設定が完了した学生と，未完了の学生が暫くの間共存することを前提とする。
- 予定している期間内に設定を完了できない学生がいることも考慮する。
- 対象学生数が多いので，対応する教員の負荷も低く抑える。

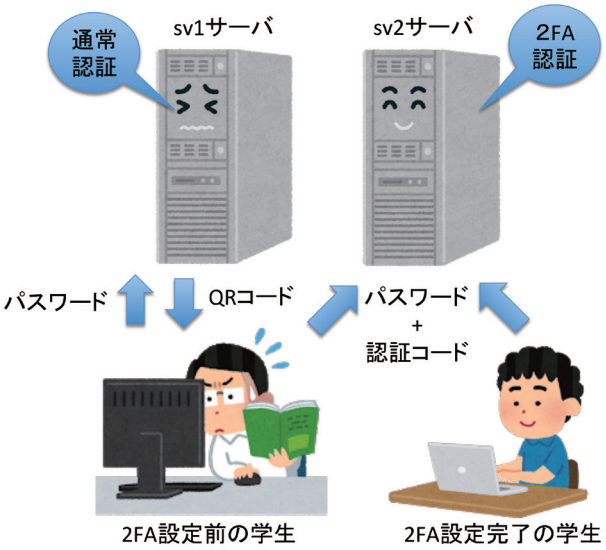

図３　ハードウェア構成

３.１　ハードウェア構成

2FAの導入初期には，2FAの設定が完了した学生と完了していない学生が共存する。そのため，どちらの学生でも演習ができるような環境を作る必要がある。

もともと演習サーバは同じ構成のサーバを２台用いる冗長構成で運用していた。２台ともパスワードのみの認証で運用していたが，それら２台のサーバを別の認証方式で使い分けることにより対応することとした。図３に示すように，１台目は2FA無しで通常のパスワードのみで認証可能なサーバ（以下sv1サーバ）として運用し，２台目は2FAが必須のサーバ（以下sv2サーバ）として運用する。sv1サーバは，2FAの設定が完了していない学生が演習を行う際に使用するサーバであり，2FAの設定が完了した学生は，sv2サーバを使用する。sv1サーバは学生が2FAの設定を行うためにも使用する。多くの学生が2FAの設定を完了した段階で，sv1も2FAを必須とする。これにより，2FAへの移行が完了した段階で冗長構成に戻ることになる。

サーバ側への2FA機能の追加に当たっては，演習サーバの基本ソフトウェア（Apple OS X）のPAM（Pluggable Authentication Module）の機能を用いた。PAMを用いると既存のソフトウェアの認証機能に独自の認証機能を追加することが可能となる。PAMはSun Microsystems社により，Open Software Foundation RFC86.0[9]において提案されたもので，その後，数多くの基本ソフトウェアで採用されている。今回は，学生が演習サーバへリモートアクセスする際に使用するサーバ側のソフトウェアであるsshdの認証機能に，ワンタイムパスワードによる認証を可能とするPAMモジュールを追加した。ワンタイムパスワードに対応したPAMモジュールでオープンソースのものはいくつか存在するが，緊急事態宣言に伴う遠隔授業の即時実施という状況下でApple OS Xで使用できることが短期間で確認できたgoogle-authenticator-libpam[10]を採用した。

３.２　学生の作業

前節で説明した通り，2FAのスマホアプリの設定にはQRコードを用いる。このQRコードは学生ごとに異なるものなので，個別にQRコードを通知する必要がある。

最初は，2FAの設定に必要なQRコードを全学生にメールで配布する手法を検討した。しかし，この方法だと全学生のQRコードの生成と，そのメールでの送付という作業が管理する側の教員に発生する。その負荷を軽減するため，QRコードは学生自身が取得できる方式を採用することとした。

学生側の準備として，自分のスマートフォンへGoogle Authenticatorなどの認証コード生成のためのアプリをインストールしておく。

１．学生は，sv1サーバへパスワードのみでログインする。
２．学生は，そこでotpwコマンドを実行し，自分のQRコードを表示するためのURLを取得する。図４にotpwコマンドの実行の様子を示す。なお，otpwは今回の2FAの導入のために筆者らが開発したツールである。

```
[redacted]:~ [redacted]$ otpw
https://www.google.com/chart?chs=200x200&chld=M|
0&cht=qr&chl=otpauth://totp/[redacted]@[redacted]%3Fsecret
%3DTQ7YFUPG3RZT5WRQYM4JJYJC5E%26issuer
%3D[redacted]
[redacted]:~ [redacted]$
```

図４　otpwコマンドによるURLの取得

３．学生は，そのURLをブラウザで開き，QRコードを表示する。（図５）
４．学生は，スマホにインストールしたアプリで，そのQRコードを読み込むと，アプリの画面にワンタイムパスワードが表示できるようになる。
５．学生は，スマホの設定の検証のために，sv2サーバ

図５　QRコードの表示

へアクセスし，通常のパスワードに加えて，スマホに表示された６桁の数値（認証コード）を入力してログインできれば設定完了である。

なお，スマートフォンの機種変更などにより設定済みの2FAスマホアプリが使えなくなった場合には，svlサーバへパスワードのみでログインし，otpwコマンドでQRコードを再取得すれば新しいスマートフォンで2FAのスマホアプリの設定が行える。

３.３　移行ナビ

学生へは，2FAへの移行の説明を授業で行ったり，Google Classroomで手順書を公開して行うが，手順書だけでは設定を行わない学生がいることが想定される。そのため，設定を支援するナビゲータアプリ（付録A）を開発した。このアプリが表示する手順に従って作業を行えば，2FAへの移行が完了するというものである。また，設定作業が正しく行われたかの確認も行える。このアプリに従えば，手順書などを読む必要はない。

３.４　移行期間終了後の対応

移行期間の終了時点でも何らかの理由で設定を行わない学生がいる可能性は否定できない。そのような学生は演習ができなくなってしまう。そこで，スマホアプリを設定していない学生でも認証コードを取得できる図６のようなWEBサイトを用意した。

図６　認証コードの発行サイト

まず，設定完了していない学生がログインしてきた場合には図７の警告メッセージを出してログインをキャンセルする。その警告メッセージの中で，本WEBサイトのURLが表示されているので，学生は本WEBサイトへアクセスし，そこで自分のユーザIDとパスワードで認証することにより，認証コードを取得できる。この認証コードを用いることにより，学生は演習サーバへログインできる。

図７　ワンタイムパスワードの設定警告

しかし，このようなサイトを公開することは不正アクセス防止の観点からは危険なので，本サイトは，検索エンジンでは検索できないようにすると同時に，同一学生のアクセス回数にも上限を設けることとした。

なお，本WEBサイトにおいて認証コードを表示する機能は，Open SourceのOATH Toolkit[11] を使用して実装した。また，現在でもスマホの機種変更などにより認証コードが得られない学生などのために本サイトは使用可能であるが，学外からのアクセスはできないように設定している。

３.５　学生への対応

全体的な学生への支援として，次の２項目を実施した。

・Google Classroomに演習室関連の部屋を作成し，そこに移行作業の手順書などの資料を集約した。
・学生の質問の窓口であるメールアドレスを用意した。

４．実施の状況

学生への周知は，まず５月の中旬に筆者（杉山）の授業科目の受講学生（約40名）に対して行った。これは一般の学生が移行作業を行う前の予備検証の意味合いを持つ。その後，全学生への連絡を６月初めに行った。周知の内容は，「７月20日以降は2FA認証が必須となるので，それまでにスマホの設定を完了しておくように」というものである。

移行スケジュールの概要を表１に示す。図８は2FAの設定を完了した学生数を日別に集計したグラフである。また，図９は2FAの設定を完了した学生の割合を学年別に集計したグラフである。割合の分母は，５月の学期開始時から移行期間終了までの間にパスワードのみでログインをした学生の人数である。

表１　移行スケジュール

月日	予定	各サーバの認証	
		sv1	sv2
５月	予備検証	パスワード	2FA
６月１日	移行期間開始	パスワード	2FA
６月 30 日	ログイン時アナウンス	パスワード	2FA
７月８日	ナビ自動起動開始	パスワード	2FA
７月 20 日	2FA 完全運用開始	2FA	2FA

図８　日別の2FA新規登録完了者数（全学年）

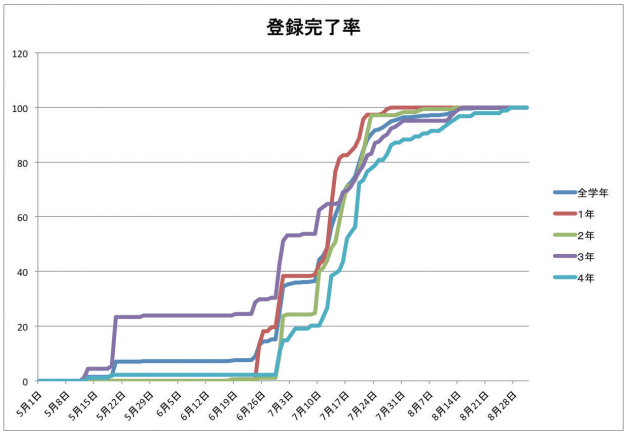

図９　日別の2FA新規登録率（学年別）

４.１　予備検証期間中の状況

筆者の科目の受講学生に対しては，５月12日に2FAへの移行手順書をこの授業のホームページで公開した。その時点では何も説明などは行っていないが，12日に２名，13日に７名，19日に３名の2FAの登録者がいたことが分かる。説明がなくとも設定を行う積極的なグループである。その後，５月20日の演習授業で全受講学生に設定をさせた結果，33名の学生が設定を完了できた。オンライン授業ではあったが双方向の授業であったこともあり，全員の設定が短期間で完了した。また，手順書については，特に問題がないことを確認した。

４.２　移行期間中の状況

筆者の担当科目以外の受講学生の状況は，以下の通りである。６月初めに各演習科目の担当教員を通して学生への周知を依頼した。さらに，その時点で設定ドキュメントをGoogle Classroomに公開した。しかし，それだけでは学生の設定作業は進まなかったことが，図８からは読み取れる。

６月25日に27名の小さなピークがあるが，これは１年生の演習科目の１クラスで設定を行ったためである。しかし，１年生の授業は１クラス50名程度であるので，６割程度の学生しか設定を行わなかったことが見て取れる。このように，授業で指示しても学生はなかなか設定を行わない。

学生の設定作業が進まないことは当初から織り込み済みであった。設定作業を促進させるため，６月30日からは図10に示すような2FAへの移行を知らせるメッセージを，sv1サーバへログインする際に表示することとした。このメッセージは，motd（Message of the day）と呼ばれ，ログインする度に全ユーザへ必ず表示されるので，周知効果が高いと想定した。このメッセージ中に表示されているonetime_naviは，３.３節で述べた移行ナビアプリである。その結果，６月30日に65名，７月１日に60名の学生が設定を完了した。特に学年により偏りがあるわけではなく，全学年で同程度の人数が設定を完了させた。

```
**************************************************
**** 注意！ 注意！注意！ 注意！ 注意！ 注意！ ****
****                                          ****
**** gwサーバは間も無くワンタイムパスワードを ****
**** 使用しないとログインできなくなります。   ****
**** 設定していない人は早めに行ってください。 ****
****                                          ****
****        設定の方法はGoogleClassRoomの     ****
****        「学科共通ソフトウェア案内」の    ****
****        「ワンタイムパスワードの設定」    ****
****              を見てください              ****
****                                          ****
**** 今すぐ設定する場合は                     ****
****  > onetime_navi                          ****
**** と実行してください。                     ****
**** 対話形式で設定できます。                 ****
****                                          ****
**** 質問は，                                 ****
****  [redacted]                              ****
**** まで                                     ****
****                                          ****
**** 注意！ 注意！注意！ 注意！ 注意！ 注意！ ****
**************************************************
****          ワンタイムパスワードへは        ****
****              ７月２０日（月）            ****
****              に移行予定です              ****
**************************************************
```

図10　motdによる一般学生へのアナウンス

さらに，７月８日に３.３節の移行ナビアプリをsv1サーバのログイン時に自動で起動することとした。これにより，全学年の学生の設定作業が同程度の速さで増えていった。

移行期間終了時の７月20日の設定完了率は，１年生が89%（167名），２年生が77%（137名），３年生が76%（141名），４年生が72%（68名），全体で80%（513名）であった。この時点では，かなりの数の未完了者がいることが分かる。理由は今回集計しているサーバ側のデータからのみでは分

からない。

そこで，この日以後は，３.４節で述べたWebサイトを公開した。これにより，順調に設定完了が増え，８月末にはほぼ全員の設定が完了したことが分かる。

４.３　発生した問題点と対策

当初の移行計画の策定時には想定していなかった問題点もいくつか発生した。

(1)　タイプミスの多さ

一つ目は，設定を完了しているにもかかわらずログインできないという学生や教員が複数見られた。原因を解析したところ，パスワードや認証コードのタイプミスがほとんどであった。2FAの導入により，タイプミスによるログイン失敗が増加するのではないかと考えていたが，想定より多い結果となったため，その状況を分析した。学生のログインエラーの状況を集計したグラフが図11である。なお，正規のユーザ名以外によるログインエラーは不正アクセスと思われるので，このグラフには含めていない。このグラフでは，ログインエラーを起こした学生の日別の人数と，その内の何人が認証コードエラーを起こしたかを集計している。

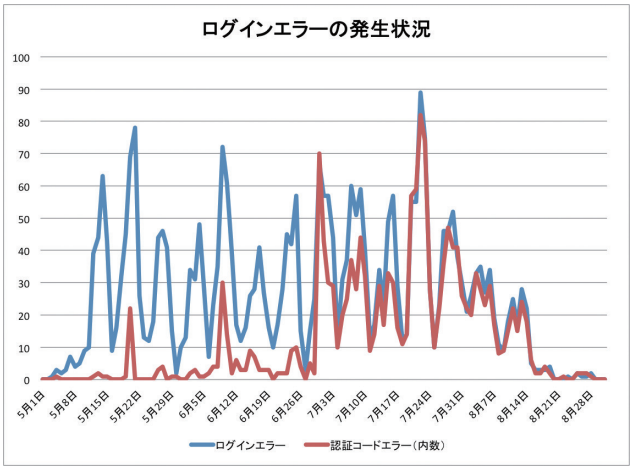

図11　日別のログインエラー人数

また，ログインエラーを起こした学生の人数とログインした学生の人数の関連性を分析した表が表２である。

表２　日別のログインエラー者数の平均値

月	ログイン者数	日別の平均エラー者数	
		総数	認証コードエラー
５月	109.0	22.9(21.0%)	1.2 (1.1%)
６月	173.1	30.0(17.3%)	6.9(4.0%)
７月完了前	166.8	36.7(22.0%)	24.8 (14.9%)
７月完了後	141.2	45.6(32.3%)	43.5 (31.0%)
８月前半	120.4	23.2(19.3%)	20.4 (16.9%)

興味深い事実として，2FAの設定を行う以前の５月でも，単純平均で毎日平均23人程度のパスワードの入力エラーが記録されていることがグラフから見て取れる。これはログイン者数の21%に当たる。かなり想定した値よりも大きな数である。

６月になると毎日平均30人となり絶対数は増えたが，ログイン者数に対する割合は17%で減少した。しかし，これでも想定したより高い数値である。

７月に入っても，移行期間中である７月前半（７月19日以前）までは，ログインエラーの平均人数は37人で，これはログイン者数の22%に当たり５月や６月と大きな変化はなかった。また，８割の学生が2FAの設定を完了した時期ではあるが，認証コードのエラーはログイン者数の15%程度と増えたものの，ログインエラーの総数は増えていない。これは，2FAを導入してもログインエラーが増えるわけではないことを示している。

しかし，移行期間終了直後の７月20日以降は，平均人数が46人へ増え，ログイン者数に対する割合も32%と増加した。３人に１人がパスワードあるいは認証コードの入力を誤っていることになり，これはかなり高い頻度である。

原因として考えられる点は，この期間は2FAの設定を行っていない学生が２割程度残っていた時期であり，それらの学生が無理やりログインしようとして認証エラーが増えたのではないかと言うことである。その証拠として，８月になり設定完了者が増えるに従い，ログインエラー者数は再度減少に転じている。ログインエラーの平均人数は23人で，割合も19%と７月20日より前の水準に戻った。

これらを総括すると，７月20日の2FAへの切り替え直後に一時的にログインエラーを起こす学生は増えたが，それ以外は定常的にログイン者数の２割程度がログインエラーを起こしていることになる。パスワードは毎回同じであるが，認証コードは毎回異なるため，認証コードの入力エラーが頻繁に発生することを想定していたが，実際にはパスワードの入力を間違うユーザが元々多かったという興味深い結果となった。

この問題の対策としては，利用者に注意して入力してもらうしかないので，その状況を説明し，ゆっくり入力することを勧めた。

(2)　ホームディレクトリの空き容量不足

２点目の問題点として，ホームディレクトリの空き容量不足（quota超過）で2FAの設定ができない，あるいは，設定は完了していたが途中からログインできなくなった利用者が数名ではあるが発生した。

まず，2FAの設定ができないという問題であるが，今回用いた2FAのモジュールは，設定情報をユーザのホームディレクトリ中にファイルとして保存する。そのため，容量に余裕がないと2FAの設定を行うことができない。容量不足で設定できない状況が発生するとエラーメッセージが表示されるため，利用者が自分で不要のファイルを削除することで問題を解決できる。ただ，エラーメッ

セージの意味が理解できない利用者からの問い合わせがあったので個別に対応した。

一方，設定完了後ログインできなくなることがあるという問題であるが，今回使用した2FAのモジュールには，空き容量がないユーザのログインを禁止する機能があり，その機能がデフォルトで有効化されていたため，この問題が発生したことが判明した。この問題が発生すると，利用者はログインできなくなるために，不要なファイルを消すこともできなくなる。

本来，容量不足となると，通常の演習のプログラム作成などにも障害が発生するので，利用者は気がつくはずである。しかし，今回の問題の利用者は，そのような状況が発生していることに気がついていなかった。エラーメッセージを見ていない，あるいは，メッセージが英語であるため意味を理解できていない状況であったと考えられる。そのため，問題が発生してしまった利用者については個別に不要ファイルを削除するという対応をした。さらに，この問題の発生を防ぐため，サーバ側のこの機能を無効化することとした。

さらに予防的措置として，ログイン時に空容量を計算し，空容量に合わせて状況を警告するメッセージをmotdに含めて日本語で出すこととした。図12は容量を超過しているユーザへのメッセージである。この警告メッセージを出すようにして以来，ログインできなくなるという利用者は発生していない。

```
**************************************
#緊急事態#
ディスクの空きが-1MBしかありません。
不要なファイルを今すぐ消して下さい。
**************************************
```

図12　容量不足の際の警告メッセージ

4.4　後学期の状況

2FAへの移行期間は前学期で終了したが，前学期には演習科目を履修していないなどの理由で，後学期に初めて2FAの設定をする学生もいることが考えられる。そこで後学期の状況も追跡した。

まず，月別の設定者数の推移を表３に示す。人数は多くはないが毎月一定数の学生が新規設定していることが分かる。また，３年生以上の学生が多いこともこの表から分かる。この表以外にも，スマートフォンを交換したなどの理由で設定を再度行った学生もいたが，それらの学生はこの表には含まれていない。

前学期の段階でログインエラーを起こす学生が多いことが分かっていたが，後学期の状況も追跡して調査した。通年のログインエラーの発生状況を図13に示す。このグラフでは，ログインエラーの日別の発生数と，７日間の移動平均を示している。移動平均のグラフから平均30名程度の学生がログインエラーを時期を問わずに起こしていることが分かる。

表３　後学期の月別新規設定者

月	9 月	10 月	11 月	12 月	1 月
2 年生以下	8	0	0	0	1
3 年生以上	29	18	11	6	5
合計	37	18	11	6	6

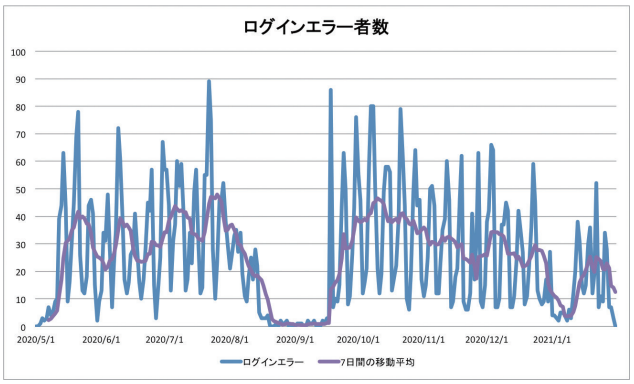

図13　通年のログインエラー者数

4.5　サーバの利用状況

今回は２台のサーバを用い，それらの認証方式を切り替えることにより2FAの導入を行った。この方式では，認証方式の変更に伴い学生の利用するサーバが変わる。そこで，学生がどのように２台のサーバを使っていたかを分析した。その結果を図14に示す。各サーバの日別のログイン者数と，７日間の移動平均を示している。

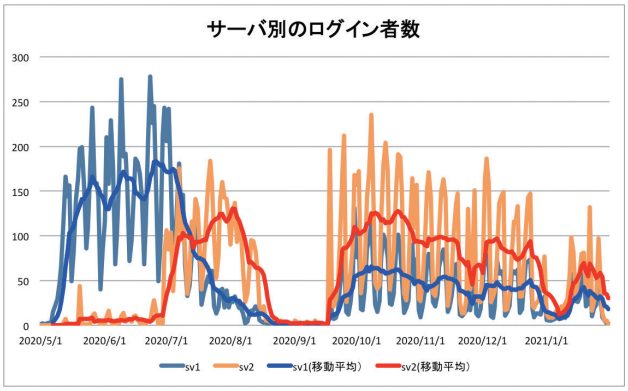

図14　通年のサーバ別のログイン者数

まず，５月初旬の段階では2FAの設定を行っていないため，全ての学生はパスワード認証のみのsv1サーバを使用している。その後，５月中旬の予備検証期間中に2FAの設定作業を行った学生が設定作業のためにsv2サーバを利用したことが見て取れる。しかし，設定完了後はsv2サーバの利用者は再度減少している。これは設定を完了した学生がsv2ではなくsv1サーバを利用していたことを示している。

６月末以降は，2FAの設定のためにsv2サーバを利用する学生が増加したことが分かる。一方で，sv1サーバを利用する学生が減少している。移動平均のグラフでは７月15日を境にして，sv2のユーザ数がsv1のユーザ数より多く

なっている。注目すべき点は，7月20日の2FA移行後は後学期も継続してsv2サーバの利用者がsv1サーバの2倍程度いたことである。これは，5月に2FAの設定を完了した学生がsv2サーバではなくsv1サーバを利用していたこととは異なる状況である。

このような現象が起きた原因として考えられる点は，5月の段階ではsv1サーバは通常のパスワードのみでログインできたため，その手軽さからsv1サーバのユーザ数の減少につながらなかった可能性がある。一方，7月20日の2FA移行後は，サーバは2台とも2FAが必須となったため，sv2サーバで設定を完了した学生がsv1サーバへ戻る理由がなくなり，設定作業を行ったsv2サーバをそのまま継続使用した可能性はある。

5．評　　価

本節では，4節で述べた実施状況を分析して得られた知見をまとめる。

⑴　移行作業について

まず2FAへの移行であるが，目標として設定した7月20日までに学生のほぼ8割の移行が完了した。このことから遠隔授業の実施中という特殊な状況下ではあったが移行作業は順調に完了したと言える。

学生に対しては，手順書の公開などよりも，サーバのログインメッセージ（motd）を通した直接的なアナウンスの方が有効であることが分かった。

さらに，motdによるアナウンスにしても，ただメッセージを表示するだけでなく，移行ナビを直接起動してしまうことの方が有効であった。

motdによる移行アナウンスから3週間で8割の学生が移行を完了させたわけではあるが，motdによる移行アナウンスだけで2割の学生が移行を完了し，さらに移行ナビの自動起動から2週間程度で6割の学生が移行を完了させた。このことから，最初から移行ナビの自動起動を行えば2週間程度で移行が完了した可能性がある。

後学期にも新規設定を行った学生がいたが，こちらも混乱はなかった。

⑵　2FA導入に伴う副作用の有無

2FAの設定がうまくいかずサーバを使用できなくなる利用者が出ることが危惧されたが，サーバを2台用いたことにより，認証方式の切り替えの副作用として演習サーバが使えなくなる学生が出なかった。

2FAを導入することによりログインエラーを起こす利用者が増えることが危惧されたが，設定完了日の直後に一時的にログインエラーの増加が増える状況が確認されたが，その後はそのような状況は発生しなかった。

逆に，2FAの導入とは無関係に，パスワードの入力エラーを起こす学生が定常的に2割程度いることが分かった。これは，キーボード入力への不慣れや，タイプ時のケアレスミスなど，様々な要因が考えられるが，今回の分析ではその理由までは分析できていない。

また，ホームディレクトリの空き容量不足でログインできない学生が数名ではあるが発生したため個別に対応した。また，今後同じ問題が発生しないように，ホームディレクトリの空きが少ない学生については，ログインする度に通知することとした。

このことから，サーバ使用時にサーバが出すメッセージは，学生にうまく届いていないことが分かった。これは，学生がメッセージに注意を払っていない，メッセージの内容を理解できていない，あるいはメッセージを読んでもすぐには対応しないなどの理由が考えられる。

⑶　教員の負荷の軽減

学生が自分で設定に必要な情報（QRコード）の収集や設定作業を完了できる手順を準備したため，教員側の負荷は設定がうまくいかない一部の学生への対応のみで済んだ。また，学生の移行作業を支援するナビゲーションアプリを用意したことにより，学生への個別の説明を省力でき，教員側の負担を大幅に軽減できた。

このことから，教員が直接指導するよりも，学生の支援をするようなアプリケーションを作成することにより，教員側の負担の大幅な軽減を図ることができることが確認できた。

⑷　サーバの利用状況

7月中旬までは，sv1サーバの方がsv2サーバよりユーザ数が多かった。この状況は，2FAの設定を完了した学生がsv2サーバを使ってはいなかったことを示している。パスワードのみで認証可能なsv1サーバを使っていた可能性が高い。

しかし，7月中旬以降はsv1サーバよりもsv2サーバの方が利用者が増えた。特に，7月20日の2FAへの移行後は後学期も継続してsv2サーバの利用者がsv1サーバの2倍程度いた。この理由は，サーバは2台とも2FAが必須となったため，sv2サーバで設定を完了した学生がsv1サーバへ戻る理由がなくなり，設定作業を行ったsv2サーバをそのまま継続使用した可能性はある。筆者らの学科で学生が使用しているsshのクライアントTeraTermでは接続先のサーバを保存できる。設定確認の際にsv2へ接続し，その設定を保存して継続使用した可能性が高い。

このことから，一度使い始めたサーバは継続して使用する学生が多いことが再確認できた。なお，sv1とsv2サーバは1台が停止しても他の1台で十分運用を継続できるような冗長化構成となっているため，この程度のユーザ数の差はサーバの性能上は全く問題にならない。

6．ま　と　め

本論文では，遠隔授業の実施に伴うネットワークセキュリティ上の脅威の増大に備え，学生向けプログラミング演習用サーバにおいて，2要素認証（2FA）を導入した際の手順と，その経過を分析して得られた知見を報告した。今回導入した2FAは，通常の使い捨てでないパスワードに加え，30秒ごとに更新されるワンタイムパスワード（認証コー

ド）での認証を行うものである。

2FAの導入手順の決定に当たっては，遠隔授業という対面での学生指導が難しい状況でも学生が単独で設定作業を行えることを重視した。特に配慮した点は以下の通りである。

⑴　2FAの方式としては，学生が普段から使い慣れているスマートフォンによりワンタイムパスワードを表示する方式を採用した。

⑵　使用するスマホアプリとしては，遠隔授業でGoogle Workspaceを用いていたため，同社のGoogle Authenticatorを標準アプリとした。ただし，他のアプリやブラウザの機能拡張もユーザの希望によって使える方式とした。

⑶　移行期間中は，２台のサーバを，それぞれ，従来認証用および2FA認証用として運用することにより，移行完了した学生と未完了の学生がどちらもログインできるようにした。

⑷　手順書などを読むことが苦手な学生のために，2FAの設定作業を説明・支援するアプリ（移行ナビ）を実装した。

⑸　メッセージなどを読まない学生や，読んでもすぐには対応しない学生のために，ログイン時に移行ナビへ誘導する仕組みを作った。

⑹　移行期間中に設定を完了しなかった学生のために，暫定的に認証コードを発行するWEBサイトを用意し，移行期間終了後でもスマートフォンの設定を行えるようにした。

また，導入経過のログを分析することにより以下の知見が得られた。

⑴　登録者数の推移を解析することで，遠隔授業中の指示や手順書の公開だけでは不十分で，授業中にその場で作業をさせるか，ログイン時に学生を設定作業へ導く移行ナビのようなツールが登録者数の増加に有効であることを明らかにした。

⑵　ログインエラーの発生状況を解析することで，パスワードの入力ミスが非常に高い頻度で起きていることを明らかにした。しかも，その状況は2FAの導入前後で変わらなかったことを明らかにした。

⑶　サーバへのログイン者数を解析することで，最初に登録したサーバを継続して利用する傾向があることを明らかにした。

まとめの最後として，遠隔授業の実施中に限らず，演習用サーバのセキュリティ強化は，いずれの大学においても緊急かつ重要な課題である。今回，学生が普段から使い慣れているスマートフォンを用いることにより，パソコンを使い始めたばかりの１年生を含めて2FAの設定がほぼ順調に完了できた。これは，筆者らの学科のような情報系の学科だけではなく，多様な分野の学生が使う演習サーバのセキュリティ強化の手法としても有効である可能性が高いことを示唆している。また，導入時の設備投資もサーバ側のPAMの追加だけで済み，手軽に導入できたと言える。学生数に応じたサーバ側の設備の増強なども必要ないため，様々な規模の大学でも導入をしやすい方式であると言える。

７．今後の課題

今回，演習サーバに２要素認証を導入した理由は，演習サーバのセキュリティの強化である。学生などの利用者の2FAの設定がほぼ順調に完了し，運用に問題がないことは確認できた。また，不正にサーバに侵入されたことがないことも確認済みである。しかし，2FAを導入したことにより，どの程度のセキュリティ上の効果があったかについてはまだ未検証である。

今後の課題として，2FAの導入によりセキュリティ面でどの程度の効果があったかを検討することがあげられる。2FA導入前のパスワード認証とssh-guardによるネットワークの遮断による運用時と比べて，定量的にどの程度効果が上がったのかの確認ができれば良いと考えている。2FA単独での有効性の評価については既発表の研究[12]もあるので，我々の環境を考慮した2FAとssh-guardを組み合わせた場合の効果などについて検証したいと考えている。

また，今後，ブルートフォースアタック以外の新たな不正アクセス手法が出てくる可能性があるが，そのような場合の対応の方法についてもあらかじめ準備しておくことも今後の課題の一つである。

さらに，今回の実施状況の分析により，２要素認証の導入とは直接の関係はない次の２点が今後の課題として浮き彫りになった。

まず，学生のログインエラーの多さが分かった。タイプミスなどのタイピングスキルの低さが原因と考えられるが，タイプミスはログイン時のみでなく，もっと本質的なプログラムの作成時のエラーの発生に直結する。従って，学生のタイピングスキルの向上も今後の課題の一つである。

また，サーバが出す警告メッセージ（ホームディレクトリの容量不足など）についても学生が注意を十分に払っていないことが明確になった。これは，プログラム作成や実行時に表示されるコンパイルエラーや実行時エラーなどのエラーメッセージを学生が理解していないことと共通である。自分の書いたプログラムが動かないと，エラーメッセージの詳細を確認することなく思いつきでプログラムを変更する学生を目にすることが多い。そのような学生はエラーを修正するというよりも，エラーを増やしてしまい，よりプログラムのデバッグ作業を難しいものとしてしまう。従って，エラーメッセージを正しく理解できるようなスキルを身につけさせることも今後の課題の一つであると考えている。

謝　　辞

本論文に対して貴重なコメントを下さった査読者の方々に感謝いたします。

参 考 文 献

1）総務省，テレワークにおけるセキュリティ確保，https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/
2）IPA，テレワークを行う際のセキュリティ上の注意事項，https://www.ipa.go.jp/security/announce/telework.html
3）ssh GUARD，https://www.sshguard.net/index.html
4）Florencio, D., Herley, C., Oorschot, P.C.v., An Administrator's Guide to Internet Password Research, Proceedings of the 28th USENIX Conference on Large Installation System Administration, pp.35-52, 2014.
5）Google, google-authenticator, https://github.com/google/google-authenticator
6）Microsoft, Microsoft Authenticator, https://www.microsoft.com/en-us/account/authenticator
7）RedHat, FreeOTP, https://freeotp.github.io
8）Google, Google Workspace for Education, https://edu.google.com/intl/ALL_jp/products/workspace-for-education/
9）Samar, V. and Schemers, R., Unified Login with Pluggable Authentication Modules (PAM), Open Software Foundation RFC86.0, October 1995.
10）Google, google-authenticator-libpam, https://github.com/google/google-authenticator-libpam
11）OATH Toolkit One-time password components, https://www.nongnu.org/oath-toolkit/
12）Thomas, K. and Moscicki, A. New research: How effective is basic account hygiene at preventing hijacking. Google Security Blog, 17, https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html, 2019

付録A 移行ナビアプリ

移行ナビアプリは，対話形式のアプリである。アプリの質問に答えながら，表示された通りにスマホを操作することにより，2FAの設定を完了できる。このアプリを実行している画面のスクリーンショットを示す。

```
ワンタイムパスワードの設定作業を行いますか？ (y/n)y

スマホを用意し，AppStoreあるいはPlayStoreから「GoogleAuthenticator」をダウンロードしてください。

ダウンロードは完了しましたか？ (y/n)y

次のURLをPCのブラウザで開いてください。
必ずURL全体をブラウザへコピーして開いてください。

  https://www.google.com/chart?chs=200x200&chld=M|0&cht=qr&chl=otpauth://totp/user@sv1%3Fsecret%3DUZT6SZXHNKOGVSE2KFT4JKHY7A%26issuer%3Dsv1

QRコードが表示されましたか？ (y/n)y

アプリを起動し
(1) 「＋」あるいは「開始」をタップ
(2) Androidの場合は，Googleへのログインは「スキップ」をタップ
(3) 「バーコードスキャン」を選ぶ
(4) カメラが立ち上がるので，PC画面上のQRコードをスマホ画面上の枠内に写す
(5) うまく写るとカメラは消え，ワンタイムパスワードの画面となる

スマホでQRコードを読み込みましたか？２回目の設定の場合でも必ず読み込む必要があります。 (y/n)y

スマホ画面に６桁の数字（ワンタイムパスワード）が表示されましたか？ (y/n)y

スマホ画面に今表示されている６桁の数字をタイプしてリターンキーを押してください(半角数字でスペース入れない)：123456

＊＊＊間違った数字がとどきました＊＊＊
＊＊＊数字は30秒ごとに更新されます＊＊＊

毎分0秒と30秒に更新されますが，時計がずれていると正しく表示されません

＊＊                                ＊＊
＊＊  0秒と30秒の前後5秒程度は避けて  ＊＊
＊＊                                ＊＊
＊＊  スマホの数字を読んでください    ＊＊
＊＊                                ＊＊

もう一度スマホ画面に表示されている【最新】の６桁の数字をタイプしてリターンキーを押してください(半角数字でスペース入れない)：226361

**********
おめでとうございます！
**********
これで設定は完了です
ログアウトして，sv2サーバへログインしログインできるか確認してください。sv1ではなくsv2です。
(1) TeraTermの場合は，キーボードインタラクティブ（あるいはチャレンジレスポンス）を使う
(2) 最初にパスワードを聞かれるので，これまでのパスワードを入力
(3) 次にVerification Codeを聞かれるので，スマホの６桁の数字を入力
(4) 正しいパスワードとCodeの入力でログイン完了！

ログインできない場合はもう一度onetime_naviコマンドを実行するかClassRoomの学科共通ソフトウェアの「ワンタイムパスワードの設定」に従って設定してください
```

日本大学工学部紀要　　第63巻第1号

令和3年9月22日　印刷
令和3年9月25日　発行

非売品

編集兼
発行者　日本大学工学部工学研究所
〒963-8642　福島県郡山市田村町徳定字中河原1
Tel.（024）956-8648
〈e-mail address〉　ceb.kenkyu@nihon-u.ac.jp

印刷者　共栄印刷株式会社
〒963-0724　福島県郡山市田村町上行合字西川原7-5
Tel.（024）943-0001(代)

JOURNAL OF THE COLLEGE OF ENGINEERING
NIHON UNIVERSITY
Vol. LXIII, No. 1, 2021

CONTENTS

ENGINEERING