〔論　文〕

持ち込み PC を用いるウェブベース試験における不正行為防止システムについて

山田　貴裕[*1]

Cheat Prevention System in Web-based Test Using Test Taker's Personal Computers

Takahiro YAMADA[*1]

Abstract

A system was developed to prevent cheating in web-based examinations using test taker's personal computers (PCs). The following method was used to prevent cheating: The test taker's PC launches a web browser, where the test web page is displayed in full screen at the front, and the image on the screen is sent to the server every few seconds until the browser is closed; the server records this information. Further, this information can be checked in real-time and subsequently by the examination proctor. The effectiveness of this approach in preventing cheating was verified after practical use.

Key Words：Web-based Test (WBT), Test Taker's PC, Cheat Prevention

1．背　　景

近年，学生に必ず PC を持参させ，その PC を用いて授業を行う必携 PC の制度を導入する大学が増えてきている．久留米工業大学でも2018年度より必携 PC 制度を導入している．また，教育の質の向上や教育者・学習者の利便性の向上等の目的で，多くの大学で Learning Management System（LMS）が利用されている．久留米工業大学でも必携 PC の制度を導入する以前から，Moodle や Google Classroom 等の LMS は利用されて来た．LMS は試験を実施する機能も有しているので，その機能を利用して小テストや期末試験を実施することも可能である．LMS はウェブベースで使用するので，LMS を利用した試験はウェブベース試験である．コンピュータ演習室等のように教室に備え付けられた PC を利用したウェブベース試験であれば，試験の時間帯だけ利用出来るアプリケーションをウェブブラウザだけに限定し，アクセス可能なサイトを LMS だけに限定するといった不正行為を防ぐための対策を実施することが出来る[(1)]．しかし，学生の持込み PC でこのような対策を実施することは現実的ではないため，厳密な試験を実施するためには別の対策が必要になる．必携 PC の制度が導入されて PC を用いた授業が増えれば，学生の持込み PC を用いた小テストや期末試験実施の需要も増えると考えられるので，持込み PC を用いた試験における不正行為防止対策の実現は急務であると言える．

企業の採用試験等では受験者の PC を用いた遠隔でのウェブベース試験が行われることもあるようだが，大学の期末試験等においては遠隔での試験は適切ではないと考える．遠隔で試験を行う場合，例えばウェブカメラで監視していて不正行為が疑われる様子が見られたとしても，不正行為の証拠を確保することは出来ない．そのような状況では不正行為を防止することは出来ないからである．そのため，遠隔での試験については本研究では扱わないことにする．本研究の前提として，試験は大学の教室等において，受験者は各自の PC を用いてウェブベース試験を受験するものとする．また，監督者は紙ベースの試験と同様に時折見回る等して受験者が不正行為を行わないよう監視するものとする．

ところで，一般的にウェブベース試験における問題点としては次の 3 点が挙げられる．

(a)　試験場外において監視されない状態での受験が可能．
(b)　他人のなりすまし或いは身代わりによる受験が可能．

[*1] 情報ネットワーク工学科　兼　学術情報センター
令和 3 年10月29日受理

(c) 容易にカンニング出来る．なお，カンニングとは広義では試験中の不正行為全般のことを指すが，本稿では他人の答案や隠し持ったメモ等を参照する不正行為のことを指すものとする．

(a)と(b)の対策として，試験場において学生証などで本人確認を行えば，(a)のみ及び(b)のみの対策は可能である．しかし，(a)と(b)を同時に行う不正行為，即ち，本人は試験場で受験している振りをして，試験場外の身代わりに受験してもらうという不正行為までは防ぐことは出来ない．これを防ぐためには，受験者には試験のウェブページの URL が分からない状態で受験させる必要がある．

(c)の対策としては，通常の筆記試験と同様に監視することは当然必要である．しかし，PC を利用しているので，PC の画面に参考資料等を表示させれば容易にカンニング出来る．これを防ぐには次の 2 つの方法が考えられる．

(A) 受験者の PC で試験のページを表示している最中には他のウィンドウを表示出来ないようにする．
(B) 試験中の受験者の PC の画面を記録しておき，監督者がリアルタイム及び試験終了後にそれらを確認出来るようにする．

(A)については Windows では有効な手段がない．久留米工業大学では必携 PC の OS は Windows なので，(B)を実現する必要がある．受験者が自身の PC の画面が記録されていることを知っていれば，PC を用いてカンニングを行うとその証拠が残ることになるため，カンニングの抑止力になると考えられる．(B)については WisdomBase の受験者のデスクトップの監視[2]のようなサービスが提供されている．しかし，このサービスでは不正が疑われる行動が検出された際のスクリーンショットを記録するだけなので，確実にカンニングの証拠を記録できるとは限らない．

2．目　　的

PC でカンニングが行われた際に確実にその証拠を記録するには，試験中に十分短い時間間隔で受験者の PC のスクリーンショットを記録する必要がある．ただし，多数の受験者の多様なデスクトップのスクリーンショットを記録していては，不正な資料を表示していることを発見することは困難である．そのため，不正行為の発見を容易にする工夫が必要になるのだが，受験者の PC が試験のウェブページを全画面で表示している状態であれば，受験者の PC の画面はほぼ同様のものになるので，不正行為の発見も容易になるだろう．多数の画面の内，1 台だけが試験以外のウィンドウを表示していれば特に目立つと予想されるためである．

本研究の目的は，受験者の持込み PC を使用したウェブベース試験において，受験者の PC に試験のウェブページを全画面で最前面に表示させ，かつ，その画面を記録しておき，リアルタイムおよび試験終了後にそれらを確認出来るようなシステムを開発し，そのシステムを用いることで不正行為を防止することが可能か検証することである．なお，ウェブベース試験で使用するウェブブラウザとしては Google Chrome や Microsoft Edge，Mozilla Firefox を想定している．これらのウェブブラウザは KIOSK モードをサポートしており，全画面表示には KIOSK モードを使用する．KIOSK モードとは，KIOSK 端末のような特定の目的のみに使用させるためのモードである．KIOSK 端末とは，店舗や公共施設等に設置される自立式の情報端末であり，例えば図書館の蔵書検索や，役所や病院等での受付や支払い処理等がある．KIOSK モードは単なる全画面表示とは異なり，タブバーやアドレスバーが表示されず，右クリックによるメニューも表示されなくなる．KIOSK モードではアドレスバーが表示されないため，受験者には試験のウェブページの URL が分からない状態で受験させることが可能であり，(a)と(b)を同時に行う不正を防ぐ対策となる．

3．不正行為防止システムの構成要素

3・1　システム構成

本研究で開発するシステムの構成要素としては，①受験者の PC で動作する受験者用のソフトウェア，②試験監督者が受験者の PC の画面を監視するためのソフトウェア，③受験者の PC の画面を記録し，監督者が監視できるようにするソフトウェアの 3 要素が考えられる．図 1 に本システムのシステム構成図を示す．

①は受験者の PC 上でウェブブラウザを KIOSK モードで起動して，試験のウェブページを表示させた後は，受験者が試験を終了するまで受験者の PC の画面を③へ送信し続ける．その為①を受験者用クライアントと呼ぶことにする．②は③に送信されてくる受験者達の PC の画面を確認するものなので，②を監督者用クライアントと呼ぶことにする．

③は受験者用クライアントから送信されてくる画像を記録し，その画像を監督者用クライアントに提供するものなので，③を不正防止サーバと呼ぶことにする．

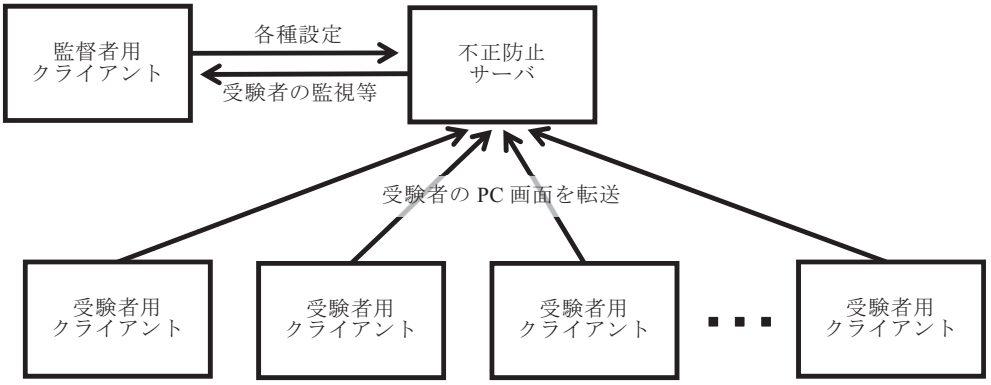

図１．システム構成図

不正防止サーバと受験者用クライアント及び監督者用クライアント間の通信には HTTP を使用する．そうすると，不正防止サーバはウェブサーバとして開発すれば良いし，監督者用クライアントはウェブページとして作成できる．受験者用クライアントもウェブサーバをアクセスするコマンドやライブラリは存在するので他のプロトコルより開発は容易になると思われる．

３・２　受験者用クライアント

受験者用クライアントが送信する PC の画面を動画として送信していては，不正防止サーバが受信するデータ量は膨大になる．その為，受験者用クライアントは画面を PNG 形式の静止画として，ほぼ５秒に１回の時間間隔で送信することにした．解像度が1920×1080の画面で試験のウェブページを全画面で表示した場合，PNG 形式にした画像のファイルサイズは30kByte～100kByte 程度であり，１秒当りのデータ量は受験者１名につき20kByte 程度となる．100名の受験者がいる場合でも１秒当りのデータ量は２MByte 程度となるので，無線 LAN で接続している環境であってもネットワークに過負荷を掛ける事はないと考えられる．ただし，近年の PC では画面解像度が Full HD を大きく上回る機種も珍しくないので，画面解像度によっては縦横を２分の１に小さくする等してデータ量を削減する必要が生じるかも知れない．

受験者用クライアントは受験者を識別するために，不正防止サーバへログインして通信を行う必要がある．ログインが成功して初めて試験のウェブページの URL を取得して，その URL を指定してウェブブラウザを KIOSK モードで起動し，最前面で表示させる．KIOSK モードではアドレスバーが表示されないため，受験者に試験のウェブページの URL を知られることはなく，外部の協力者を利用した不正行為は防ぐことができる．また，KIOSK モードでは全画面で表示されるため，監督者による試験中の監視や試験後の確認作業が容易になる．更に最前面で表示させているので，他のウィンドウを試験のウェブページより前に表示することは Windows キーを使わない限り困難であり，カンニングを抑止することが出来る．なお，Ctrl キーを使えば新しいタブを開いてインターネットを閲覧することも出来るので，試験が終了するまでは Windows キーや Ctrl キーを使用してはならないと受験者に周知しておく必要がある．

２章で述べた通り本システムにおいて受験者が使用するウェブブラウザは Google Chrome，Mozilla Firefox および Microsoft Edge としている．久留米工業大学では必携 PC に Chrome をインストールしておくことになってはいるが，必ずしもインストールされているとは限らない．そのため，受験者用クライアントは Chrome→Firefox→Edge の順に起動を試みるようになっている．ここで Edge が最後になっているのは，バージョン78以前の Edge は KIOSK モードをサポートしていないので，優先順位を最も低くしたためである．これらのブラウザは－kiosk をオプションとして指定して起動すると KIOSK モードで起動する．ただし，既にそのブラウザが起動している場合，－kiosk をオプションとして指定して起動しても KIOSK モードにはならない．そのため，起動しようとしているブラウザが既に起動していないか確認し，起動している場合はそのブラウザを終了させた後に KIOSK モードで起動するようにしている．起動しようとしているブラウザを起動出来なかった場合は，次のブラウザの起動を試みる．全てのブラウザを起動できなかった場合は，使用可能なブラウザの一覧を表示して終了する．しかし，Windows であれば Edge はインストールされているだろうから，ブラウザを起動できないことはないだろう．ただし，Edge のバージョンが78以前だったとしても受

験者用クライアントは関知しないので，監督者はなるべく早い時点で少なくとも一度は全受験者の画面が全画面で試験ページを表示していることを確認する必要がある．

受験者用クライアントはウェブブラウザを起動した後，ウェブブラウザが終了するまで約 5 秒間隔で全画面をキャプチャして PNG 形式に変換し，不正防止サーバへ転送する．なお，受験者用クライアントが不正防止サーバへアクセスする際にはログインに必要な情報や画面のデータだけでなく，PC の現在時刻と IP アドレスも送信するようになっていて，これらの情報は不正防止サーバに記録される．PC の時刻を記録することで，万一不正防止サーバの時刻が著しくずれていた場合でも受験者の受験開始時刻等をほぼ正確に把握することができる．また，IP アドレスを記録することで，万一学外からアクセスされたとしても，そのことを把握することができる．

受験者用クライアントは受験者全員に配布して実行させる必要がある．インストーラによるインストールが不要な方が配布は容易になる．そこで，スクリプトファイルをダウンロードして実行する方法を検討した．スクリプトは前述の機能を実現するため，PowerShell スクリプトで記述した．ただし，PowerShell スクリプトのファイルは直接実行することは出来ないので，BAT ファイルを配布して，その BAT ファイルから PowerShell スクリプトファイルをダウンロードして起動するようにした．試験終了後には PowerShell スクリプトファイルを削除するようにして，スクリプトファイルを解析・改ざんして不正を行うことも難しくしている．また，BAT ファイルの起動後，不正防止サーバの IP アドレスを入力することで PowerShell スクリプトファイルをダウンロードするようにしているので，試験開始直前まで受験者は不正防止サーバにアクセス出来ないようにすることも可能である．また，1 で述べた(a)と(b)を同時に行う不正行為において，協力者が学内の試験教室とは別の場所にいて，不正防止サーバへのログインから始めて身代わり受験しようとしても，不正防止サーバの IP アドレスを監督者が試験開始直前に受験者に伝えるようにすれば，協力者には不正防止サーバの IP アドレスが分からないので身代わり受験は不可能である．

3・3　監督者用クライアント

本不正防止システムを使用するには，監督者は試験の監視だけでなく準備や事後処理を行う必要がある．監督者用クライアントはこれらの機能も提供する．試験の準備としては，①受験者を不正防止サーバのユーザとして登録する，②試験のウェブページの URL を登録する，の 2 つである．それらの操作方法については本論文の主旨ではないので割愛する．なお，本不正防止システムを公開する際には利用方法のページを用意して，監督者用クライアントのページからリンクを張り，その中で操作方法については説明する予定である．なお，試験のウェブページの URL を登録することで，受験者用クライアントへその URL を伝えるスクリプトを生成するようにしていて，そのスクリプトが存在しない場合には受験者用クライアントに一切応答しないようにしている．これにより，監督者が開始の合図をする前に受験を始めることを防ぐことが出来る．

試験中は監視画面で受験者の PC 画面を監視できる．監視画面は複数の受験者の画面を同時に確認出来るように，横幅 2 分割～10分割にして，受験者の PC 画面を並べて表示されるようになっている．図 2 に監視画面を 8 分割で表示している様子を示す．なお，図 2 は試験終了後に監視記録から再現したものであり，試験中に監視画面をキャプチャしたものではない．しかし，図 2 は試験中の監視画面のある時刻をほとんどそのまま再現出来ている．ただし，プライバシーに配慮してユーザ名と氏名等は黒く塗りつぶす加工を施している．

受験者の PC 画面の並びの順序は開始時刻（ログイン時刻），ユーザ名又は更新時刻（新しい画面のデータが届いた時刻）から選択出来る．開始時刻の順に並べると，ある受験者の近傍の受験者は開始時刻が近いので，問題の解答進度も近くなり，およその進度を把握出来るのではないかと考えたが，実際には回答の進度には個人差があり，進度を把握することは難しかった．ユーザ名で並べると，特定の受験者を探し易くなる．受験者が多いと横幅10分割しても監視画面をスクロールしないと全員分を確認することは出来ない．そこで，更新時刻で並べると画面の上部に更新分が集中するので，監視画面をスクロールすることなく更新分を確認出来ると考えた．しかし，実際にはスクロールが必要なこともあった．また，ある受験者の画面に疑問を持って，その受験者に注視しようとしても直ぐに別の場所に並べ替えられてしまい，十分確認することは出来なかった．結果的にはユーザ名で並び替えるのが最も実用的だった．

監視画面では 1 秒おきに不正防止サーバへリクエストを送り，その間に受験者用クライアントから不正防止サーバへ送られてきたデータを取得するようになっている．不正防止サーバは受験者用クライアントから送られてきたデータをリレーショナルデータベースに保存している．ここで使用しているリレーショナルデータベースでは，テーブルの各行に ROWID という疑似カラムがあり，格納された順に通し番号が振られている．監視画面のページからサーバへ送るリクエストには，前回受け取ったデータの ROWID の最大値を含めておき，不正防止サーバはその値より大きな ROWID をもつ行のデータだけを返すようにしている．このようにして監視画面では前回リクエストからの更新分のデータだけ

を受け取るようになっている．監視画面は受け取ったデータの受験者の部分だけ更新すると同時に，その受験者の画面を赤枠で囲むようにしている．これによって一目でどの受験者の画面が更新されたか分かる．

図 2．監視画面（この図ではユーザ名，氏名等は黒く塗りつぶしている）

監視画面が不正防止サーバから受け取る 1 行分のデータは“ROWID，ユーザ名，開始／更新／終了，受験者の PC の時刻，不正防止サーバの時刻，受験者の PC の IP アドレス，不正防止サーバに保存された画像のファイル名，受験者の氏名等”である．開始／更新／終了は受験者用クライアントの状態で，受験者が不正防止サーバにログインした際は開始，受験者用クライアントを終了する際は終了，それ以外は更新である．受験者の PC 画面の画像の上部に表示されている開始時刻は，この状態が開始の際の時刻を表示している．PC 画面の画像の下部に表示している更新時刻は，状態が更新の際の時刻を表示していて，同じ受験者の更新のデータを受信する度に書き換えられる．受験者の PC 画面の画像ファイルは不正防止サーバ内には“ユーザ名－日付－時刻．png”というファイル名で保存されている．監視画面はこのファイル名を指定して画像ファイルをダウンロードして表示している．最後の受験者の氏名等は，監督者が受験者をユーザ登録する際に付加した氏名等の情報である．この部分には任意の文字列を指定できるので，氏名以外の情報が含まれていることもあり得る．

不正防止サーバに記録された監視記録は一括してダウンロードすることが出来る．監視記録をダウンロードする際には，監督者用クライアントは ROWID が 0 より大きい行のデータを要求することで，不正サーバに保存されている全てのデータを取得する．そして，そのデータを CSV 形式に変換して保存し，全ての PC 画面の画像ファイルを逐次ダウンロードする PowerShell スクリプトを生成し，そのスクリプトを保存するためのリンクを生成して表示する．また，この PowerShell スクリプトを実行するための BAT スクリプトも生成して，その BAT ファイルを保存するためのリンクを生成して表示する．監督者は表示されたこれら 2 つのリンクをクリックして保存し，BAT ファイルを実行することで，不正防止サーバに記録された監視記録を全てダウンロードすることが出来る．こうしてダウンロードしたデータには review.html という監視記録を表示するための HTML ファイルが含まれており，このファイルをブラウザで表示し，PowerShell スクリプトにより生成された CSV ファイルを読み込むことで監視記録を確認することが出来る．確認の画面（以降，確認画面と呼ぶ）は監視画面とほぼ同様であるが，表示する時刻を 1 秒単位で進める／戻すボタンや時刻を設定するためのスライダーが画面上部に設置されていて，自由に時刻を進めたり遡ったり出来るようになっている．

ところで本システムは，現状では複数の試験に同時に対応出来るようにはなっておらず，監視記録も複数に分けることは出来ない．その為，1 つの試験の終了後に別の試験に利用するには，終了した試験の監視記録をダウンロードした上でその試験の監視記録を削除しておく必要がある．監視記録は監督者クライアントで一括して削除することが出来るようになっている．

3・4　不正防止サーバ

前述のように本システムは同時に複数の試験に対応出来るようにはなっていない．これは本システムが未だ開発中であることも理由の１つだが，不正防止サーバの運用方法も関係している．不正防止サーバは同時に多数のクライアントから継続的にアクセスされることになる．そのようなサーバを学内ネットワークの何処か１か所に配置して，同時に複数の試験に対応させようとすると，学内ネットワーク全体のトラフィックが増加してしまう．逆に不正防止サーバを，試験を行っている教室毎に配置すれば，殆どのトラフィックは教室内に留まり学内ネットワーク全体には影響しない．これは次の理由による．久留米工業大学では，普通の教室には１教室につき１台の無線 LAN アクセスポイントが設置されているので，同じ教室内の受験者の PC と監督者の PC は同じアクセスポイントに接続する．同じアクセスポイントに接続している端末同士の通信では，パケットはアクセスポイントによって無線 LAN の機能で中継されるのみであり，イーサネットに流れることはない．また，大教室ではアクセスポイント１台では接続可能な端末数が不足するので２台設置されている．そのため，同じ教室であっても異なるアクセスポイントに接続する端末もあることになる．しかし，アクセスポイントが接続しているイーサネットはスイッチングハブに接続していて，スイッチングハブは宛先が接続しているポート以外にパケットを転送することはない．そのためスイッチングハブを経由することにはなるが，大教室であってもトラフィックは教室内に留まることになる．不正防止サーバが必要なのは試験を行う時だけなので，その時だけ監督者の PC でサーバを起動するようにすればトラフィックを教室内に留めることが出来る．その為には監督者の PC に不正防止サーバをインストールする必要があるが，不正防止サーバを仮想マシンとして実現しておけば，仮想化ソフトウェアがインストールされた PC ならば OS 等に依らず不正防止サーバを利用出来る．本不正防止システムを公開した場合，本システムを利用しようとする者は必ずしも不正防止サーバを稼働させるための環境（Apache HTTP Server や PHP，SQLite3 等）を整えるスキルを有しているとは限らない．仮想マシンであれば仮想化ソフトウェアさえインストールしてあれば，仮想化ソフトウェアで仮想マシンを起動するだけで良く，それ以上の設定作業はほとんど必要ない．その為より簡単に利用出来るだろうと考える．そこで今回は，不正防止サーバを仮想マシンとして実装した．仮想化ソフトウェアとしては Oracle VM VirtualBox を使用した．

4．使用評価

本システムを使用しても Ctrl キーや Windows キーを使用すると簡単にカンニングできてしまうため，試験中はそれらの使用を禁じる必要がある．そのため試験開始時に，Ctrl キーや Windows キーは試験が終了するまで使用してはならず，もし使用した場合は不正行為と見做され得ること，また，本システムは受験者のデスクトップ画面を監視していて記録に残していることを周知しておく必要がある．以下に述べる期末試験での使用時には，試験開始時にこれらのアナウンスを行っている．

本システムは2020年度前期の期末試験において初めて使用を試みた．受験者には予め受験者用クライアントの BAT ファイルを配布しておく必要があるので，受験者には試験の前に受験者用クライアントの BAT ファイルをダウンロードさせ，BAT ファイルを起動出来るようにしておくよう指示しておいた．しかし，試験の際に BAT ファイルを起動しても，不正防止サーバをアクセスすることが出来ない受験者が半数程度いたため，急遽本システムの使用を断念し，本システムを介さずに受験するよう指示することになった．不正防止サーバをアクセスすることが出来なかった理由としてはパスワードを覚えていないとか，サーバの IP アドレスを正しく入力出来ないといった受験者の問題が多かったが，それだけでなく，受験者用スクリプトをダウンロードして実行する BAT ファイルにも問題があった．この BAT ファイルの中で PowerShell スクリプトをダウンロードして保存するパスを指定している部分があったのだが，これにはユーザのホームパスが含まれていた．そして，ユーザ名に半角や全角のスペースが含まれていると，ホームパスにスペースが含まれてしまい，パスを正しく解釈出来ず，コマンドを実行することが出来なかった．

その為，BAT ファイルの中でパスを指定しないように変更した．そして，2020年度後期の期末試験では，事前にダミーの不正防止サーバと試験問題の代わりのアンケートを用意して，受験者にダミーの不正防止サーバを介してアンケートをアクセスさせることで，受験者が問題なく使用出来ることを確認するようにした．その結果，実際の試験では大半の受験者は問題なく使用することが出来た．しかし，一部の受験者は BAT ファイルの起動時の作業ディレクトリに問題があり，直ぐに試験を始めることが出来なかった．これは，ファイルを保存するパスを指定しないようにした為，起動時の作業ディレクトリに保存されるようになったのが原因である．BAT ファイルが保存されているフォルダを開いて BAT ファイルのアイコンをダブルクリックすることで起動すれば，作業ディレクトリは BAT ファイルのフォルダと同じになるので問題は起きない．しかし，Windows の検索ボックスで BAT ファイルを検索して実行すると，作

業ディレクトリが“C:¥Windows¥System32”となり，ファイルを保存することが出来ずに，スクリプトを実行できなかった．この時は検索して実行しようとしていた学生には BAT ファイルがあるフォルダを開いて実行するよう指示したことで，直ぐに始められなかった学生も遅れて受験することが出来た．その後，BAT ファイルで最初にホームドライブのホームパスに作業ディレクトリを移動するように改修して2021年度前期の期末試験で使用したところ，本システムの使用については問題なく試験を実施出来た．これまでは期末試験でのみ使用したが，面接授業における小テストで使用しておけば，ダミーの不正防止サーバをアクセスさせるといった準備は不要であり，より簡単に本システムを用いた期末試験を実施出来るだろう．

本システムを用いた試験の監視については，40〜50名程度なら画面の横幅10分割に設定すれば同時に監視することは可能だが，それ以上の人数では画面に入りきらず，スクロールが必要になって同時に監視することは出来なかった．受験者の画面は試験ページを全画面で表示しているため，かなり小さくしても試験画面かそれ以外かは確認出来る．そのため15分割ぐらいも選択出来るようにすると良いだろう．監視画面及び確認画面では１受験者当りの横幅を分割数に合うようにスタイルシートで指定することで分割している．図３にウェブブラウザの開発ツールの機能を使い，一時的に確認画面のスタイルシートを上書きして15分割にしてみた様子を示す．

図３．15分割にした確認画面の様子

2021年度前期の期末試験では２科目で使用したが，１科目目の監視記録を確認したところ，画面の更新が30秒以上空くことがあった．その際の仮想マシンのリソースとしては1CPU，メモリ2GByte を割り当てていたが，クライアントからのリクエストを処理するにはリソースが不足していたのではないかと考えた．しかし，2020年度後期の期末試験では仮想マシンのリソースは同様であったが，そのような現象は発生していない．これは遅れて試験を開始した受験者が半数程度おり，アクセスが分散して同時に処理しなければならないリクエストが受験者の総数に対して少なかったため，結果的に仮想マシンのリソースが不足しなかったのではないかと考えられる．そこで２科目目の試験では仮想マシンのリソースを2CPU，メモリ4GByte を割り当てて本システムを使用した．そして監視記録を確認したところ，ほぼ５秒間隔で画面が更新されていたので，リソースの問題だったと考えて良いだろう．１科目目の受験者は79名で，２科目目の受験者は94名だった．試験中に仮想マシンが実際にどれだけのリソースを使用していたかは確認出来ていないが，受験者の人数が100名を超えるような場合には，より多くのリソースを割り当てる必要があるかも知れない．

確認画面で監視記録を確認した結果，殆どの受験者は不正行為を行うことなく受験していたことを確認できた．本システムが不正行為を防止する上で有効だったものと考えられる．ただし，2021年前期の１科目ではカンニングを行っている学生が１名いた．この学生は点数不足で不合格になったので，不正行為を報告しなかったが，本システムによって不正行為を発見することが可能であり，その証拠が残ることも確認出来た．図４に確認画面で不正行為を行っていることが分かる様子を示す．図４の上部が確認画面であり，図３と同様にして15分割で表示している．下部はカンニング中の PC 画面の画像である．図４では文字がつぶれて分かり難いが，この時の PC 画面の画像を実際の画面サイズで表示

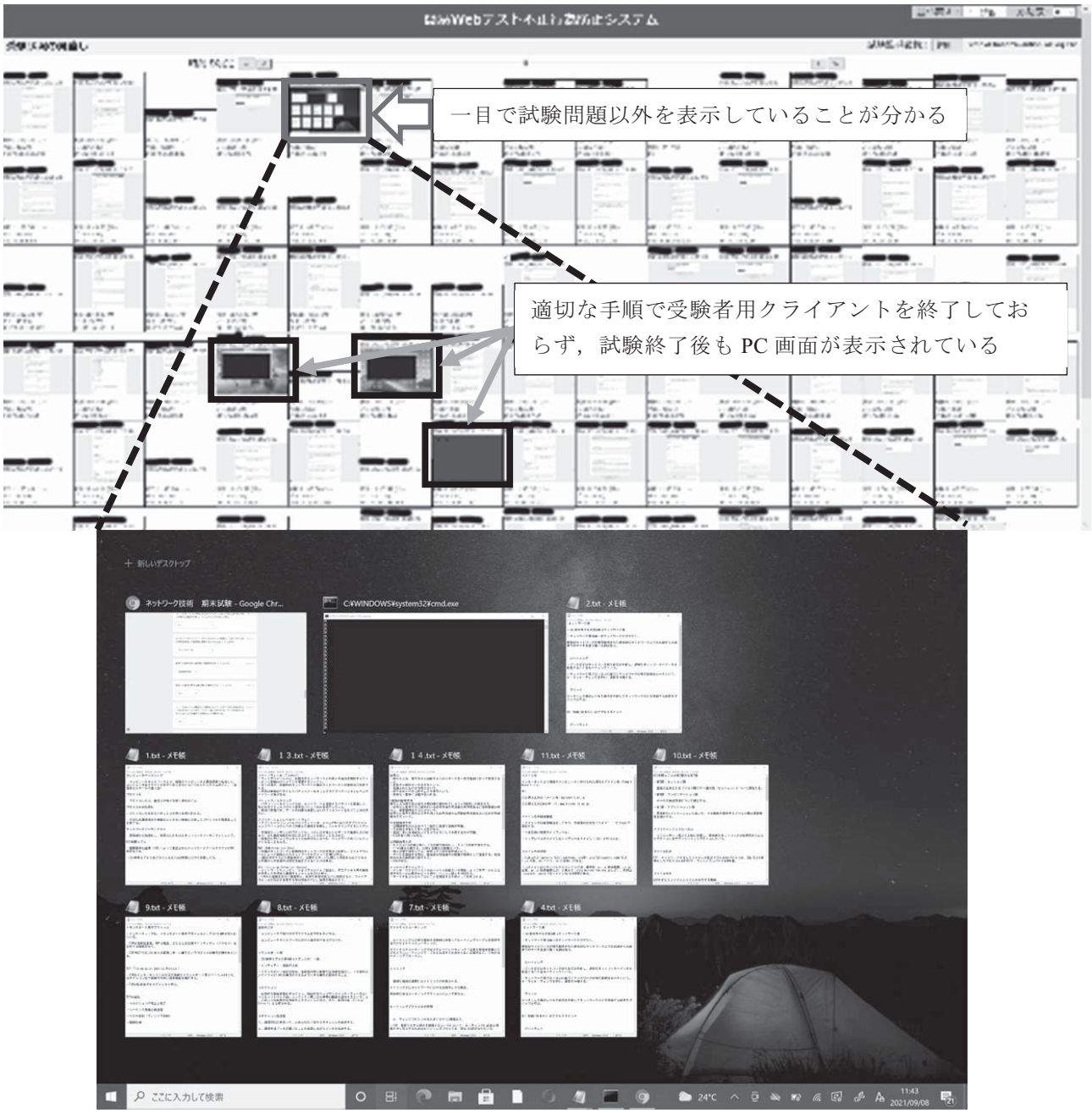

図４．不正行為を行っている様子（確認画面と PC 画面の画像）

したところ，複数のメモ帳を開いてカンニング用のメモを表示していることを確認出来た．この画像も保存されているので，不正行為を行っていた証拠は残っている．また，他に３名の受験者の PC 画面が試験問題以外を表示しているが，これは受験者が適切な手順で受験者用クライアントを終了しておらず，試験終了後も PC 画面が表示されているためである．これらの受験者については，確認画面で表示する時刻を遡って試験を終了していることを確認している．

確認画面で監視記録を確認する際には，表示する時刻を１秒進めるのにボタンを１回クリックする必要がある．10分間の確認を行うには600回クリックする必要があり，この点に関しては不便に感じた．自動的に表示時刻を進める自動化の機能が必要だろう．

５．終わりに

受験者の持込み PC を使用したウェブベース試験において，受験者の PC に試験のウェブページを全画面で最前面に表示させ，かつ，その画面を記録しておき，試験終了後に確認出来るようなシステムを開発し，使用を試みた．最初に

試用した際は, 本システムを使用出来ない受験者が半数程度いたため, 本システムの使用は断念せざるを得なかった．2回目には BAT ファイルを改修し，受験者に予めダミーの不正防止サーバをアクセスさせて，本システムを使用出来ることを確認させておいたことで，本システムを使用して試験を実施することが出来た．しかし，BAT ファイルに問題があり直ぐに始めることが出来ない受験者がいたので，更に BAT ファイルを改修して 3 回目の使用を行ったところ，問題なく試験を実施することが出来た．それらの監視記録を確認した結果，殆どの受験者は不正行為を行うことなく受験していたことから，本システムの有効性を確認できた．また，不正行為を発見できることも確認できた．しかし，監視画面や確認画面の分割数の設定や確認画面の自動化など，改善すべき点が残っている．2021年度後期の期末試験までにはこれらの点を解決して試用したいと考えている．

本システムを利用して試験を行うのに必要となるのは，受験者用クライアントの BAT ファイルと不正防止サーバの仮想マシンのイメージである．前述の改善すべき点が解決出来たら，これらのファイルに加えて簡単な使用説明書となる README.txt を加えて公開したい．なお，より詳しい使用説明書は不正防止サーバに掲載する予定である．公開の際にはこれらのファイルを ZIP でまとめ，ウェブサーバからダウンロード出来るようにしたいと考えているが，URL は未定である．

文　献

⑴ 古川文人，渡辺博芳，佐々木茂，及川芳恵，高井久美子，武井恵雄，“コース管理システムのテスト機能を用いた定期試験の実践”，情報処理学会研究報告．CE,［コンピュータと教育］86（2006-10-21），pp. 51-57
⑵ 株式会社シェアウィズ，“オンライン試験の不正・カンニングをダブルで防止するインカメラ＆デスクトップ監視機能を追加しました”，［online］https://wisdombase.share-wis.com/news/prevention-of-fraudulent-exams/，2021年10月22日アクセス