メディア教育研究　第７巻　第１号
Journal of Multimedia Education Research 2010, Vol.7, No.1, S57－S63

特集（招待論文）

遠隔教育における単位認定のための個人認証

川原　洋[1)]

サイバー大学ではすべての授業と履修評価をウェブ上で行うために，授業コンテンツへのアクセスや定期試験において，適切な認証システムを複合的に利用し，単位認定に伴う履修者の本人確認の信頼度を高めている。3G携帯電話機をワンタイムパスワード出力端末として使う認証システムは稼動も安定していることから，高い利用率が報告されている。一方より厳格な個人認証が必要とされる定期試験等では，一律にウェブカメラをつかった顔認証による試験サイトへのアクセス制御がおこなわれ，そのまま試験中の監視カメラとして機能している。これらの認証システムが円滑に運用されているうえで，授業活動における学生とのマルチメディアを利用した双方向コミュニケーションが，最も信頼性の高い本人確認となっている。

キーワード
遠隔教育，e-Learning，メディア教育，本人確認，人体認証

1. はじめに

サイバー大学は，福岡市における構造改革特区を活用し，2007年に開学された全ての授業をウェブによる遠隔教育で行い，単位認定に伴うスクーリング（対面授業）が一切不要な我が国初の４年制大学である。サイバー大学の授業は，すべてオンデマンド形式で提供されるため，ネットワークに接続しているPCがあれば，時と場所を選ばず，授業を受け，試験を受験することができる。従って，サイバー大学における遠隔教育による履修認定や試験時の本人確認方法であるセキュリティシステムの信頼性は重要である。

しかし，開学時点での受講時における本人確認は，ID・パスワードによるものだけで運用されており，簡単に成りすまし履修が可能であった。その後，文部科学省による「平成21年度 設置計画履行状況等調査 留意事項」への対応として改善を行い，2008年度春学期において，すべての受講時・試験時において，成りすましによる授業出席や，ログイン後の成り代わりによる定期試験受験を未然に防ぐことをシステム機能として実装した。その後も継続的にシステム機能の更新や運用改善に取り組んでいる。

本稿では，まず遠隔教育における３つの個人認証方式，

① 携帯電話機を用いる方式（シンクロック）
② ウェブカメラを用いた人体認証による方式（顔認証）
③ ウェブカメラを用いた目視認証による方式（スナップショット）

を紹介する。次に100%オンライン教育における本人確認に関し，サイバー大学の取り組みをもとに課題の確認と認証技術の適用および運用の実態について報告する。

2. 個人認証システムの概要と適用

2.1 サイバー大学の遠隔教育におけるセキュリティ要件

セキュリティを構成する要素は秘密性，認証性などが含まれると言われている。秘密性とは特定の利用者だけに情報へのアクセスを許すことで，それ以外の者がアクセスできないことを保証する事である。認証とは，情報や情報主体の正当性を確保するための技術であり，ユーザ認証とは，認証者が正当な利用者であり，かつその人本人であることを認証することである（佐藤，2001）。遠隔教育により単位認定を行うためには，それぞれの認定プロセスにおいて適切な「本人確認」を行うことが必須である。

サイバー大学における本人確認は，学生ごとに以下の場合に行うことが求められている（表１参照）。

表１　個人認証の必要性

認証場面	認証目的
入学時	本人と入学合格者との照合
授業履修時	授業出席管理
単位認定時	定期試験等の成績評価
卒業時	本人と学位授与対象者の確認

[1)] ㈱日本サイバー教育研究所　サイバー大学IT総合学部　教授

入学式や学位授与式（卒業式）には，直接面談と写真入り身分証明書の照合によって，本人の確認を行う対面的な認証行為であるので，通学制の大学の場合と相違はない。入学時にどうしても入学式会場に出席できず，対面による本人確認が取れない場合は入学許可前に必ずウェブカメラによるビデオ会議や携帯電話機のテレビ電話機能による本人確認を行う。学位授与においても卒業式等の会場で対面による本人確認を行っている。入学時と卒業時における本人確認は基本的に対面式である。なお，授業の履修および単位認定を行う評価や試験の実施では，一切のスクーリングが必要ないことから，入学から卒業まで本人と全く直接面談する機会がない可能性もある。

教育や学生指導の観点から，学生の在学中に少なくとも一度は直接面談の機会を設けるため，担任制を設け，年に数回全国の拠点で公開授業などの講習会や研究会を開催して，できるだけ多くの学生と対面できる機会を設けている。それでも本人の都合で，在学中どうしても面談に応じられない学生も少なくない。特に海外在住の学生で，在学期間中に一度も帰国しない可能性もある。また，重度の身体障害から，医療施設から容易に外出できる状況にない学生も，教員が自ら出向いていって面談しない限り，必ずしも容易ではない。

これらの場面における本人確認はその頻度も努力範囲で済むが，日常的に本人確認が頻繁に，従って日常的に学生の負荷が少なく実践的なシステムが求められるのは，上記で示した項目(2)の授業履修時（授業コンテンツの視聴やディスカッションなどへの参加）と(3)の定期試験等の単位認定時である。しかし，前者が授業コンテンツへのアクセスを制御するなど，サイトへのログイン時の認証が求められているシステムと，後者のオンラインでの定期試験など，試験サイトへのログイン時の認証と試験開始後のいわゆる替え玉受験などの不正を防ぐ受験監視では，求められる認証要件は技術的に異なるものとなる。

そこでサイバー大学では，学習管理システム（以下LMS）へのログイン時における個人認証と定期試験など，ログイン後の受験監視を継続的に実施できるシステムを複合的に併用することで，すべての個人認証の要件を満足することとした。認証機器そのものは，操作が簡単で入手可能な汎用的な機器であることが望ましい。次にこれらのシステム機能と適用について解説する。

2.2　3G携帯電話機を認証端末とする本人確認システム（シンクロック）

サイバー大学設置認可時における本人確認の手段は，ICチップが埋め込まれているカード式学生証をPCに接続されているカード認証機器に読み取らせ，ログイン画面に入力するパスワードとの一致で学生サイトへログインさせる方法であった。しかし，この手法は他人に学生証を預け，パスワードを知らせることで成りすましによる履修が容易に行われることが想定される。従って，ICチップを埋め込むなど学生証等の認証媒体のセキュリティレベルをいくら向上しても，本人の意思により第三者にその認証媒体が委ねられ，学習システムへのアクセスと履修活動そのものが委託されれば，成りすましの実行者がICカードの保持者に限定されるだけで，通常のIDとパスワードによるセキュリティレベルと何ら変わるところがない。

PCやLANへのログイン認証方法として，ログインの都度，専用端末機のディスプレイに乱数を表示させ，それをパスコード（パスワード）としてシステムへのログイン時にPC画面に入力させる方法（ワンタイムパスワ

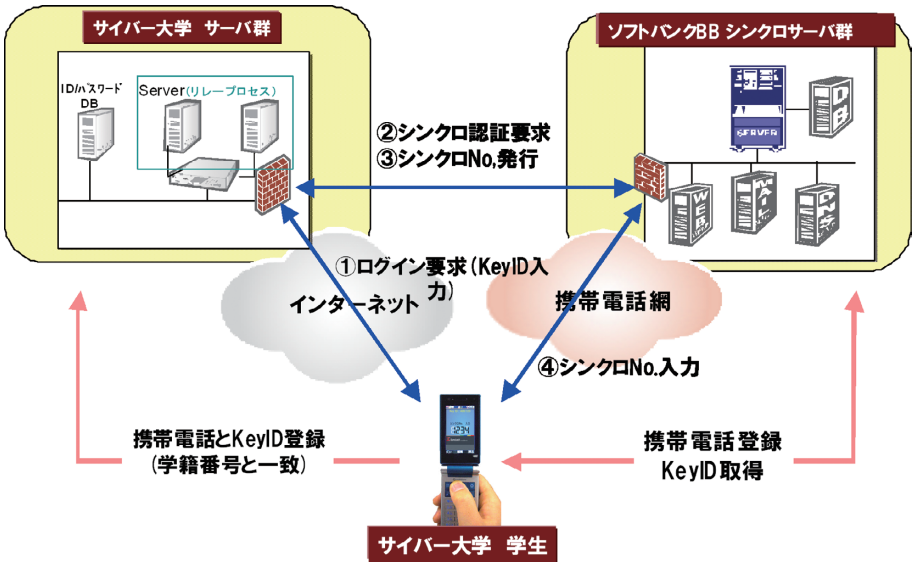

図１　シンクロックによるシステムログイン時の個人認証の流れ

ード方式）は，専用端末を保持しなければシステムにアクセスできないことから，通常のIDとパスワードによるログインよりもセキュリティレベルが高いとして商用化され，特に金融業などの企業において広く使われている。この専用端末機をデータ通信機能をもつ携帯電話機で置き換えた認証システムがソフトバンクBB㈱社のSyncLock™（以下シンクロック）（http://www.synclock.jp/）である。

ここで外部資料を引用するまでもなく，18歳以上の国内人口における携帯電話の普及率は高い水準で推移している。今や個人に特定電話番号が付与されているがごとく個人を特定する手段として，また文字通り個人が常に携帯する機器として，人体以外の認証媒体として位置づけるには最も適した認証システムといえる。また，データ通信機能を保有するいわゆる第３世代携帯電話（3G）の普及は，各携帯通信会社の第２世代携帯電話のサービス停止とあいまって，その利用者数が伸びている。

基本的なシンクロックによる認証のプロセスを図１に示す。

学生はシンクロサーバに携帯電話機を事前に登録してキーIDを取得する。取得されたキーIDはサイバー大学の専用サーバに学籍番号と連携する形で登録されると，該当する携帯電話機はサイバー大学LMSへの専用認証端末機となる。

この携帯電話機を使ったLMSへのアクセスは以下の手順で行われる：

(1)　登録した携帯電話機からサイバー大学サイトへのログインを要求する。
(2)　サイバー大学サーバからシンクロ認証要求がシンクロサーバへ送信される。
(3)　シンクロサーバは４桁「シンクロ番号」を発行する。
(4)　学生はこの「シンクロ番号」を携帯電話に入力して，シンクロサーバへ送信し，「開始」をクリックするとLMSへのログインが完了する（図２参照）。

携帯電話機を用いた認証方式のメリットとして，経済性，安全性，簡便性の３つがある。経済性として，市販の携帯電話機を本人認証キーとして活用できるため，新たな認証専用のデバイスを購入する必要がない。安全性として，パソコンと携帯電話機をインターネットを介して同期させることで，ワンタイムパスワードによるログインと同等のセキュリティレベルが確保されている。また，通常のワンタイムパスワード・システムと異なり，登録されている携帯電話機によって大学サイトへアクセスをしたのが果たして本人なのか，大学から任意に電話やTV電話をかけて確認もできる。簡便性として，学生にとって使い慣れた携帯電話機を用いるので，携帯電話機の電波が届いている場所であれば，いつでもどこでも本人認証が行える点や，パスワードを記憶して定期的に変更する必要がない点が挙げられる。

2.3　ウェブカメラによる人体認証システム（顔認証）

シンクロックによる個人認証が，簡単かつ信頼度の高い手順であっても，シンクロックに対応した携帯電話機が利用できない国・地域に在住している学生には利用することができない。このような学生向けに，シンクロックの代替手段を提供する必要がある。しかも，シンクロックと同等あるいはそれ以上の認証機能であることが求められる。

人体（バイオメトリック）認証方式は個人に固有の身体的な特徴を用いて機械が個人の認証を行う技術である。パスワードのように記憶する必要がなく，紛失の危険の少ないきわめてセキュリティレベルの高い方式であるとされているが，コストが高いことが欠点として指摘されている（松本，2006）。学生が保有しているPCとの接続や設定，および障害対応を遠隔で行う時間とコストを考慮すると，システムの導入の選択肢は限られている。そこで授業でも利用していたウェブカメラで顔を撮影して行う人体認証システム（以下「顔認証」）を採用することとした。また，後述するが，映像や画像データの人間の目視による事後確認が実践的な本人確認の手段とも

図２　シンクロックによるLMSへのログイン画面

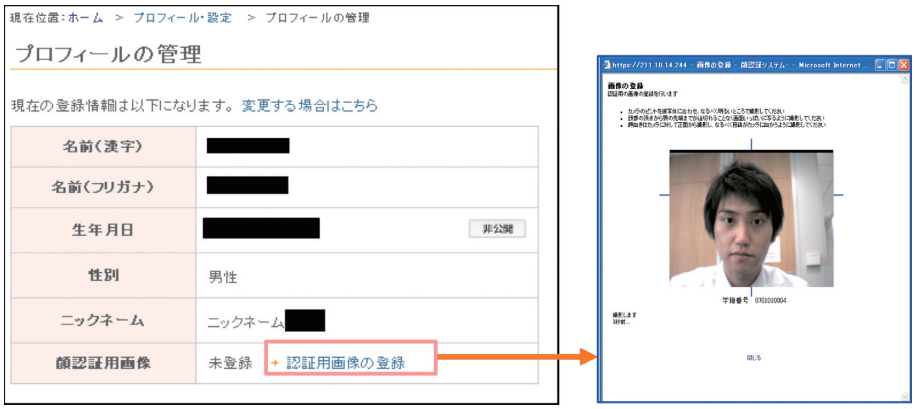

図３　学生のプロフィール管理画面で実施する顔認証画像のマスター登録

なる。顔認証による個人認証の流れは以下の通りである：

(1)　学生はPCにウェブカメラを接続し，学生専用サイトに用意されている，認証用の画像を登録する（図３参照）。登録画像は，これ以降行われる顔認証のマスターとして利用される。

(2)　サイバー大学の事務局は，学生が自ら登録した画像を目視により，入学時の顔写真と比較し，随時マスター画像としての精度を確認する。

(3)　時間が経つに従い，学生の顔映像も撮影環境も変化するので，必要に応じてマスター映像の再設定を以上の手順によって都度実施する。

すべての顔認証プロセスはサーバ上で処理される。LMSへのログイン時に学生のPCに接続されているウェブカメラで撮影された顔の画像はサーバへ送信され，サーバ上で稼動している認証エンジンがマスター登録されている画像との一致を瞬時に判定する。判定結果後，両者の一致が認められると，LMSへのログインが許可される。顔認証の高い信頼性から，本システムはシンクロックを使用しないLMSへのログイン時の認証システムだけでなく，単位認定のため，より厳密な本人確認が求められるオンライン試験サイトへのログイン時や定期試験として評価されるレポート提出時の本人確認として運用されている。

2.4　LMSへのログイン手順

サイバー大学の学生専用サイトからLMSへはシンクロックないし顔認証によってログインすることができる。当初，学生にはどちらかの認証システムを選択するよう勧めていたが，少なからぬ学生からの要望で，どちらでも都度選択してログインできるように仕様変更をおこなった。

一度LMSへログインすると，履修登録した科目の一覧が提示され，受講可能な回の授業コンテンツを視聴することができる。（図４参照）

2.5　ウェブカメラによる試験監視（スナップショット）

システムが正常に稼動している限り，顔認証による本人確認手法が最も有効とされる。しかし，単にLMSへのログイン時において本人確認ができても，例えばオンライン試験など，一度顔認証でログインできても，受験中に本人以外の人間が替え玉受験を行うことも可能である。従って，LMSへのログイン後も，少なくとも成績

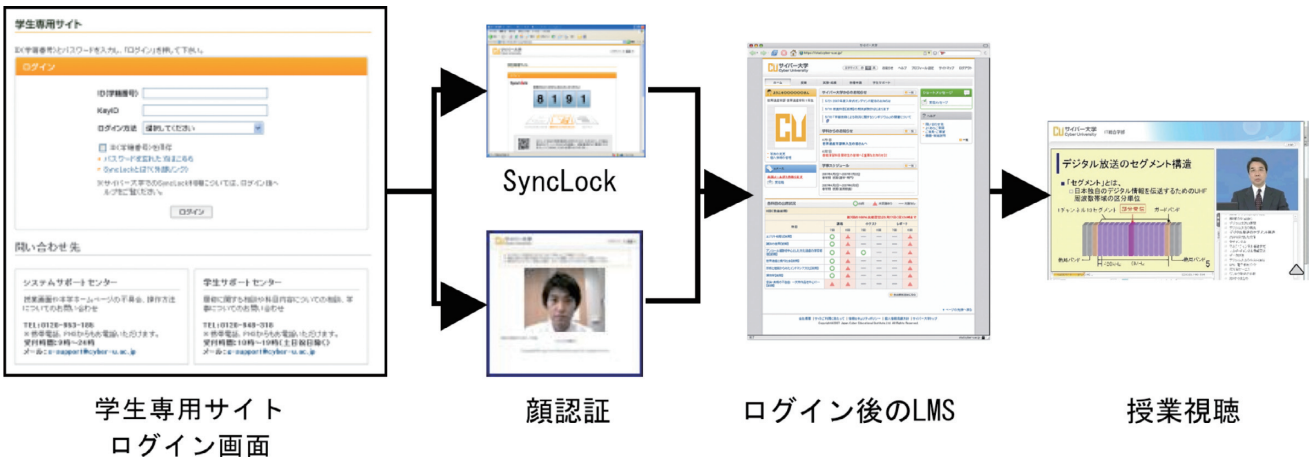

図４　シンクロックないし顔認証によるLMSへのログイン

評価に直接かかわる定期試験の受験中の監視が必要である。この目的のためにオンライン試験サイトへのログイン時の顔認証で利用しているウェブカメラをそのまま監視カメラとして活用することは，極めて実践的な成り代わり防止策である。

サイバー大学ではシンクロックないし顔認証によってLMSへログインした後，定期試験の受験やそれに順ずるレポートの提出画面では顔認証による個人認証を行っている。さらにオンライン試験の場合は，ウェブカメラをそのまま利用して，学生の受験中にある一定間隔で受験者の顔（顔認証時に確定されたウェブカメラのアングルが維持されていることを想定して）のスナップショットを収録し，サーバへ都度送信している。

本システムに適用しているオンライン試験形態には，制限を設けている。受験者の成りすましを未然に，またログイン後の成り代わりを事後に精査する機能を充足しているが，ウェブカメラの限られた視角内の監視なので，資料の持込など，いわゆるカンニングによる不正受験まで監視することはできない。従って，本監視システムでは，制限時間で定められた資料持込可能な試験にのみ適用している。

3. 認証システムの運用と学習機会への影響

3.1 学生の遠隔学習環境と認証システムへの要望

遠隔教育における優位性のひとつに，履修者が任意に受講時間を選べることが挙げられる。また，ブロードバンドのインターネットサービスに接続しているPCさえあれば，設置場所にかかわらず，いつでも学習が可能である。しかし，個人認証機器がPCに接続されて利用できる状態になければ，せっかく確保した学習時間からの授業出席は認められず，提出したレポートも無効となってしまう。従って，本人確認が円滑にできなければ，学習環境を制限することとなり，それに伴って学習時間も削減される。

遠隔教育のメリットである学習環境の柔軟性と単位認定のための本人確認の厳格性は相反する要件である。仮に学生自身が固定的な学習端末で，定常的に履修を行っているのであれば，安定して稼動する単一の個人認証システムを提供すれば良いこととなる。そこで学生の学習環境の多様性について実態を把握する必要があった。

サイバー大学では，学生の履修形態を把握するため，2009年５月にアンケート調査を行った。その結果，有効回答数282に対し，63.8%にあたる180名が「利用するPCは１台のみ」と回答したが，残りの36.2%は複数のPCで履修していると回答した。また別の設問で，複数種の個人認証システムの利用のニーズについて尋ねたところ，80%以上の学生が複数の認証システムの必要性を示唆した（図４参照）。

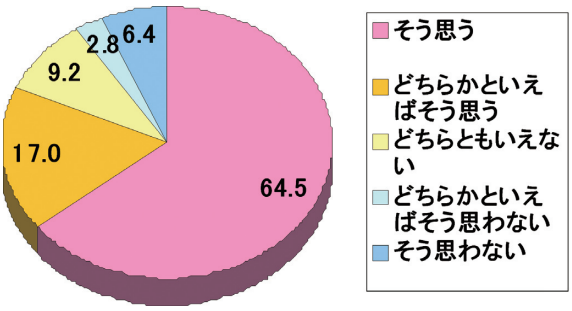

図４　複数の個人認証方式のニーズ調査結果

3.2 シンクロックの導入率

シンクロックは安定して稼動し，かつ操作が容易な認証システムであることから，単位認定時の本人確認に関する留意事項を解消するため，2008年春学期からその導入を推進した。導入開始時には，学生からのクレームが多く寄せられたが，一切のスクーリングをなくすための条件であることを粘り強く説得してきた。過去３年間の在校生（履修者）によるシンクロック利用者登録率は，表２に示すように，全年次に渡って７割強に至っている。シンクロック未登録の学生は，顔認証のみの認証システムを利用しているが，日本国内の携帯電話会社３社（NTTドコモ，ソフトバンク，au）の3G携帯端末を利用できない環境にある学生や携帯電話の操作そのものが困難な学生を除くと少数である。

2007年度入学生については，個人認証プロセスの指導を入学後に行ったにもかかわらず，2009年４月時点で，同年度入学者のシンクロック登録率は他の年度の入学者と同レベルの水準となっており，本人確認に対する学生への動機付けの違いは，2009年度において解消されたと判断している。

表２　入学年度別シンクロック登録率
（2009年４月現在）

入学年度	シンクロック登録率
2007年度入学者	73.00%
2008年度入学者	72.30%
2009年度入学者	74.80%

3.3 認証システム別にみるLMSへのログイン頻度

先に述べたように，シンクロックによるLMSへのログイン手順が簡便であることから，一人当りのシンクロックによるLMSへの平均ログイン回数と顔認証による平均ログイン回数の比較を行った。その結果，2007年度入学者（初年度）にみえる顕著な顔認証によるアクセス回数については，さらに詳細な分析が必要であるが，2009年春学期間における全学年の学生一人当りのLMSへの平均アクセス回数をみると，総じてシンクロックに

よるアクセス回数が顔認証によるアクセス回数を大きく上回っていることがわかった（表３参照）。

表３　入学年次別学生一人当りのLMSへのアクセス回数（2009年春学期）

入学年度	シンクロック(A)	顔認証(B)	A/B
2007年度入学	235.2	231.8	1.01
2008年度入学	268.4	138.2	1.94
2009年度入学	276.3	159.9	1.73

（注）顔認証が必須のオンライン試験やレポート提出時を除く

この結果から，認証システムの操作性や使い勝手が，学習サイトへのアクセスを簡便にし，従ってアクセス回数も増える傾向にあるといえる。

3.4　顔認証システムの運用課題と対策

LMSへのログイン時に在校生の70%以上の学生が利用しているシンクロックが極めて安定的に運用されているなか，顔認証の運用障害は断続的に発生している。これらの障害の主な理由はウェブカメラの誤操作や被写体（顔）への光量不足などがあげられる。顔認証導入当初は，かなりの障害件数が報告されていたが，学生に障害事例集の提示や操作上のヘルプデスクを設置して，各々の障害対応とシステムの改善を行ってきた結果，事務局に報告される障害報告は学期期間中に数件，期末試験期間中でも十数の報告に止まっている。また，マスター映像の再登録の手順も簡単にできるため，学生自身が自ら問題の解決ができるようになっているのも障害の報告件数の減少に貢献している。なお，学生によるマスター画像の再登録は，その更新後，大学職員によって目視確認されている。

従って，最も信頼性の高い人体認証のひとつである顔認証ではあるが，すべて自動化されているレベルに至っておらず，人的支援と品質管理によって運用されている。

3.5　オンライン試験の監視

オンライン試験サイトへのログイン時に顔認証による本人確認を行っても，ログイン後に別の者が受験することは可能である。したがって，サイバー大学では顔認証で使ったウェブカメラを試験開始後は監視カメラとして利用するシステムを開発し，運用している。

通信データ量を大幅に削減するため，監視カメラは，成り代わりを十分把握できる間隔でスナップショット（連続映像データ）を試験時間中撮り続け，直ちに大学サーバへ送信する。担当教員あるいは担当教員の監督下にある学習支援者（メンター）により，すべてのスナップショットは目視により確認され，試験中の本人確認を行う。通常60分間行われる期末試験で，すべてのスナップショットを確認するのは，膨大な量の時間を要するかに思われるが，スナップショットの連続性を確認する作業は学生一人当たり十数秒で完了する。

顔認証やシンクロックが本人確認を事前に行うシステムであるのに対し，ウェブカメラによる試験監視は，防犯カメラのごとく，事後の本人確認システムである。しかし，単位認定や成績評価は，不正後において十分その評価をやり直すことができるので，事前の認証システムと同等の信頼性が期待できるし，かつビデオや画像データは，事後に何度でも確認することができるので，複数の人間が容易に目視できる証拠としても有効である。

3.6　双方向学習における本人確認

サイバー大学は，いわゆる高度マルチメディア教育といわれている，教員と学生の双方向コミュニケーションにより授業を行っている。専門分野の多くの演習科目や卒業研究の論文発表などでは，学生はオーサリングツールを駆使して，スライドと自分の映像から構成されているプレゼンテーションコンテンツを制作している。発表を行う学生のコンテンツは，教員を含む科目学生全員が視聴するところとなる。

また，専任教員は，Skypeなどのビデオ会議システムによる個別相談時間（オフィスアワー）を設け，学生指導に充てている。このライブビデオによる学生面談は，単位認定の対象とはならないが，普段から学生と顔が見えるコミュニケーションをとることができる。つまり，教員は認証システムに頼らず，ライブ映像やビデオによる学生との交流により，特別意識することもなく，おのずとお互いが本人同士であることを了解しながら，学生と接している。

4. むすび

本稿では，サイバー大学が授業等で運用している個人認証システムの機能概要とその適用について解説した。認証システムは，学生の利用環境や本人確認の厳格性と利便性のバランスにより，複数のシステムが複合的に活用されている実態を報告した。シンクロックのような簡便な認証システムを導入することで学生のLMSへのログイン回数が伸びている。一方，顔認証などの人体認証システムは，まだ運用上の課題はあるものの，正常に稼動した際の信頼性は高いので，技術的なサポート体制を充実させて，運用している。従って，現実的な本人確認の運用は，これらのシステムを統合的に活用することで成立している。

学生の成績評価や単位認定におけるシンクロックとウェブカメラによる個人認証システムの全貌を認証目的別に表４に整理した。表中，○印は実施中であることを示す。

表４　単位認定場面における本人確認方式

認証場面	認証目的	ウェブカメラ		シンクロック
		顔認証	ビデオ/スナップショット	
授業出席	授業コンテンツ視聴	○		○
	演習やゼミでの学生発表		○	
定期試験	レポート提出	○		
	オンライン試験ログイン	○		
	オンライン試験受験監視		○	

オンライン試験システムの監視のように，成りかわりによる不正行為は，事後の監視データの分析によって，成績評価や単位認定前に未然に防ぐことができるため，有効である。この監視データによる本人確認の考え方は，モバイルによる遠隔教育のように，ダウンロード型のコンテンツをオフラインで視聴する際の本人確認の手段としても有効と思われる。

また，本人確認は認証システムだけに頼らず，日常的な授業における学生間，あるいは学生と教員の間の映像を媒体としたコミュニケーションも加わって，学生の本人確認の信頼性が担保されていることも合わせて報告した。

実施中の個人認証における第１種の過誤（本人であるのに本人と認識しない）と第２種の過誤（他人であるのに本人と認識する）の確率の定量的評価，コストを考慮した顔認証の改善は，今後の課題である。

参考文献

［１］ 松本勉（2006）．バイオメトリック認証システムのセキュリティとその評価，映像情報メディア学会誌，Vol. 60, No. 10, pp. 1547-1550
［２］ 佐藤修（2001）．ネットラーニング－事例に学ぶ21世紀の教育，中央経済社

川原（かわはら）　洋（ひろし）
1984年Massachusetts Institute of Technology, School of Engineering, Department of Naval Architecture and Ocean Engineering 博士課程卒。Sc. D.（工学博士）
Schlumberger Wireline，新日鉄ソリューションズ㈱，日本アイ・ビー・エム㈱を経て，2000年ソフトバンクBB㈱入社。
以来，数々のネットビジネスの起業にCTOとして参画。2007年，ソフトバンク100%出資によるサイバー大学IT総合学部教授就任，現在に至る。
情報処理学会会員。
日本MITエンタープライズ・フォーラム理事。

Student Authentication for Course Credit in Distance Learning

Hiroshi Kawahara[1)]

In order to provide school credit for class attendance and course work, Cyber University utilizes fully integrated student authentication systems when students access their course content and online examinations. The results of using 3G mobile phones, which are used as one-time password devices, provide stable security measures, and have high utilization is reported. A web camera is used as a biometric authentication monitor to capture the image of the student's face when the student has access to the on-line examination system. The face image is crosschecked with the student's pre-registered photo ID. The same web camera is continuously used to monitor the student's activities during the on-line exams. Besides those authentication systems performing flawlessly, the most reliable identification of the students is achieved during the bilateral communication by means of multimedia.

Keywords
distance learning, e-Learning, multimedia education, student authentication, biometric authentication

[1)] Professor, Faculty of Information Technology and Business, Cyber University operated by Japan Cyber Educational Institute, Ltd.