6H-4

仮想化デスクトップを用いたｅラーニングー認証方法

梅澤 克之[†]
(株)日立製作所[†]
横浜研究所

小泉 大城[‡]
サイバー大学[‡]
IT 総合学部

中澤 真[‡]
サイバー大学[‡]
次世代ｅラーニング研究所

平澤茂一[‡]
サイバー大学[‡]
IT 総合学部

1. はじめに

遠隔学習では，直接，対面で本人確認ができないために，受講時の遠隔での認証を正しく行うことが重要である．認証を正しく行わないと，本当の受講者でない第三者が，代わりに受講するなりすまし受講ができてしまう．

大学の学位やその他資格を与えるような遠隔学習の場合の認証と，通常の認証には，本人の意識の違いがあると考えられる．例えば，クレジットカードなどは，他人に使われることを一番嫌っているのは「本人」である．しかし，第三者が代わりに受講するなりすまし受講の場合，本人自らが他人に使って欲しいと思っている．このような状況に対して，指紋や静脈等の本人の身体的特徴を用いて本人確認を行う生体認証を行うことが考えられる．しかし，この方式であっても受講開始時のみ，本人の生体認証を行い，その後は，第三者に受講を替わってもらう，ということができてしまう．このような課題に対しては，受講開始時だけでなく，不定期に認証をかけるという方法が考えられる．

本研究では，上記遠隔学習の特徴を踏まえて，初回の受講開始時のログイン時だけでなく不定期に認証をかける方法を提案する．ただし，認証の頻度はランダムな時間間隔やあらかじめ決められた時間間隔ではなく，認証にかかった時間，その認証結果の精度，受講者が使っている端末，認証に用いた認証デバイスの種類等から第三者がなりすまして受講していそうな度合い（以降，懐疑度と呼ぶ）を算出し，懐疑度が高い受講者には頻繁に認証を要求し，懐疑度が低い受講者には認証の頻度を下げる認証方法を提案する．

2.従来の遠隔学習時の認証方法

なりすまし受講を防ぐ方法の従来研究として，文献[1]には，受講開始時の初回ログイン以降に1つの教材区分単位が終了する毎に，又は，ランダムに設定される随時認証時間に基づいて，生体認証による再度の本人認証処理を行う方法が示されている．また，文献[2]には，あらかじめ定められた時間ごと当該受講者の生体情報を取得して認証を行う方法が知られている．

また，文献[3]には，サイバー大学における取組として，遠隔教育における 3 つの個人認証方式(携帯電話機を用いる方式，ウェブカメラを用いた顔認証方方式，ウェブカメラを用いた目視認証による方式）が紹介されている．この論文の中では，技術的・運用的な課題の一つとして，ウェブカメラの誤操作や顔への光量不足などが挙げられている．

3.提案方式

3.1 提案方式の概要

本節では，本当の受講者でない第三者が，代わりに受講するなりすまし受講を防ぐための提案方法を示す．文献[1][2]のように，初回の受講開始時のログイン時だけでなく不定期に認証をかける方法を採用する．ただし，ランダムな時間間隔やあらかじめ決められた時間間隔では，正当な利用者に対して認証の負荷がかかってしまう恐れがある．よって提案の方針としては，第三者がなりすまして受講していそうな度合い（懐疑度）によって，認証の頻度を変える方式を提案する．

懐疑度に影響を与えそうな要因を下記に示す．

- 認証にかかった時間：第三者がなり済まして受講していれば，サーバ側から認証要求の際に，本人を呼ぶまでに時間がかかる．
- 認証結果の精度：生体認証などの場合，他人と判断するほどではないが，マッチング率が低い場合に懐疑度が高いと考える．前節の従来技術の課題の一つであった顔への光量不足なども本要因に関連する．
- 受講者が使っている端末：組織内（学内）にある端末なのか，自宅にある端末なのか，あるいは，公共施設にある端末なのかによって，懐疑度が変わってくると考えられる．
- 認証デバイスの種類の種類：認証に用いるデバイスとして，生体情報（と読取デバイス），クレジットカードなどの IC カード，学生証，携帯電話端末などが考えられる．これらのデバイスは受講者にとっては他人に貸したくない度合いが変わってくると想定できる．

e-learning using the virtual desktop - authentication method
†Katsuyuki Umezawa, Yokohama Research Laboratory, Hitachi, Ltd.
‡Daiki Koizumi, Makoto Nakazawa, Shigeichi Hirasawa, Cyber University.

本研究では，これらの懐疑度を総合的に判断し，懐疑度が高い受講者には頻繁に認証を要求し，懐疑度が低い受講者には認証の頻度を下げる認証方法を提案する．

3.3 提案方式の処理フロー

図 1に受講者認証を行うフロー図を示す．

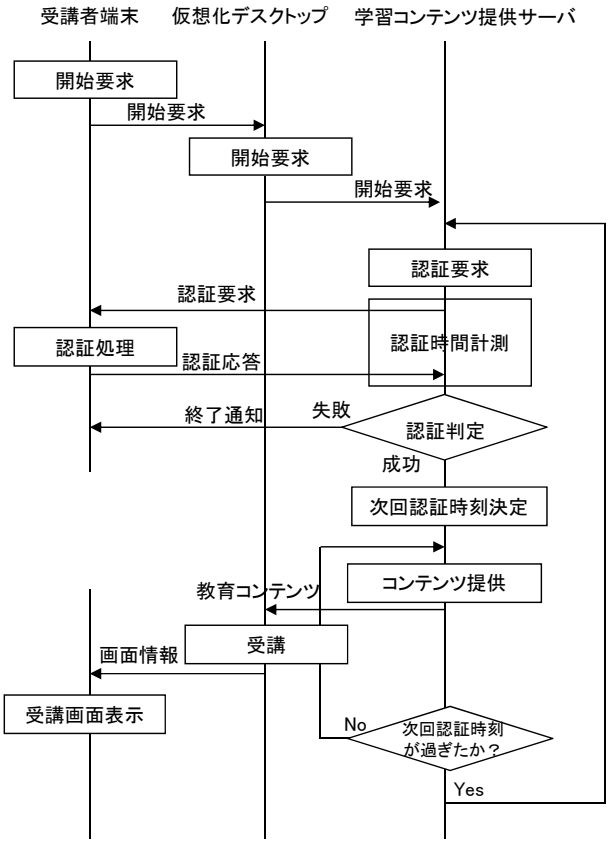

図 1 受講者認証を行うフロー図

受講者端末は，仮想化デスクトップにログインし，仮想化デスクトップがコンテンツ提供サーバから学習コンテンツの配信を受け，受講者端末上には，仮想化デスクトップの画面情報が表示される環境を想定している．学習開始時だけではなく図 1に示したように，学習コンテンツ提供サーバは，次回認証時刻決定処理で決定された時刻を過ぎたか否かを判定し，過ぎていなければ教育コンテンツの提供を継続し，次回認証時刻を過ぎている場合には，認証要求処理から繰り返すことによって認証を強化する．

図 2に，図 1の次回認証時刻の算出処理用のポリシーの例を示す．それぞれのポリシーごとに懐疑度があらかじめ振られている．ただし，認証時間ポリシーに関しては，他受講者のデータを用いて統計処理を行い，標準偏差基準法や，マハラノビス平方距離を用いた方法などで統計的異常値の判定を行い，異常値と判定された場合には懐疑度を 1 に，異常値と判定されなかった場合には懐疑度を 0 にする方法も考えられる．

最後に，次回までの認証時間を，正当な受講者を認証する時間間隔を基準認証時間とし，基準認証時間－(a×認証時間による懐疑度)－(b×認証精度による懐疑度)－(c×端末装置による懐疑度)－(d×認証デバイスによる懐疑度)により算出する．ただし，a，b，c，dは，それぞれの懐疑度に係る重み付け係数とする．

認証時間ポリシー

認証時間	3秒未満	3秒以上
懐疑度	0	1

認証精度ポリシー

認証精度	a/2未満	a/2以上
懐疑度	0	1

注）a=生体認証単体での判定限界

端末装置の種類ポリシー

端末装置	組織内端末	家庭内端末	未登録端末
懐疑度	0	0.2	1

認証デバイスの種類ポリシー

認証デバイス	ICカード	免許証	携帯端末	学生証	生体認証装置
懐疑度	0	0.1	0.1	0.5	0.1

図 2 次回認証時刻の算出処理用のポリシー

4. まとめと今後の課題

本研究では，初回の受講開始時のログイン時だけでなく不定期に認証をかける方法を提案した．具体的には，認証の頻度は，認証にかかった時間，その認証結果の精度，受講者が使っている端末，認証に用いた認証デバイスの種類等から受講者の懐疑度を算出し，懐疑度が高い受講者には頻繁に認証を要求し，懐疑度が低い受講者には認証の頻度を下げる認証方法を提案した．本研究によって，正当な受講者には認証の負担をかけず，なりすまし受講を行う不正な受講を抑制することができる．

今後は，本研究におけるポリシー，および懐疑度算出時の重み付け係数(a, b, c, d)を具体的に設定し，実験による評価を行う必要がある．

参考文献

[1]遠藤正樹,“e ラーニングシステムにおける本人認証システム,” 特開 2011-53969

[2]植松正実,“遠隔試験・講習システム,”特開 2005-258364

[3]川原洋,“遠隔教育における単位認定のための個人認証,”メディア教育研究 Vol.7, No.1, pp.S57−S63, 2010.