

一般カードを用いた仮想 PC 教室環境の設計

Design of virtual PC rooms utilizing widely-used smart cards

清水 さや子[†], 関根 卓史[†], 吉田 次郎[‡], 戸田 勝善[†]
Sayako SHIMIZU[†], Takuji SEKINE[†], Jiro YOSHIDA[‡], Masayoshi TODA[†]

smz@kaiyodai.ac.jp, tsekin0@kaiyodai.ac.jp, jiroy@kaiyodai.ac.jp, toda@kaiyodai.ac.jp

[†] 東京海洋大学情報処理センター

[‡] 東京海洋大学大学院海洋科学技術研究科

[†] Information Processing Center, Tokyo University of Marine Science and Technology

[‡] The Graduate School of Marine Science and Technology, Tokyo University of Marine Science and Technology

概要

近年、授業や自習で利用する PC 教室の教育システムにおいて、利用者数は増加傾向にあるが、運用コストは削減傾向にあることより、PC 教室の増設や利用時間の拡張が難しい。そのため、PC 教室を授業で利用したい場合や、PC 教室で自習したい際、空き教室がないことが頻繁に発生している。この問題回避のために、本研究では、PC 教室以外の研究室や自宅等からでも個人 PC を使って教育システムが利用出来る仮想 PC 教室環境の設計を行う。東京海洋大学の教育システムは、ログイン時に本人認証として IC カードを使った認証を用いている。そのため、PC 教室以外の研究室や自宅等から利用する際においても、PC 教室で利用する認証方式と同等以上の認証方式が求められる。そこで、仮想 PC 教室の利用の際においても、カード認証を併用する。併用するカード認証は、IC カードが導入されていない教職員でも利用できるよう、大学が発行する IC カードだけでなく、個人が保有する携帯電話や定期等のカード（以下、一般カードとする）でも認証が行える仕組みとする。一般カードを使った認証方法は、著者らが先行研究として行っている PIN コード生成方式を応用して実現する。

キーワード

教育システム, 仮想 PC 教室, PIN コード, 一般カード認証システム

1. はじめに

近年、市場にはノート PC やタブレットが普及し 1), 大学においても、保持者は年々増加している。一方、授業で PC 教室の使用を希望する人や自習で利用する PC 教室の利用者数は、一定、もしくは増加傾向にある。授業では、同じデスクトップ環境で授業をしたいという要望や、個人購入には高額な教育システム上のソフトを使用したいという要望があるためである。しかし、要望とは逆に、依然として、運用コストが削減傾向にあり、PC や PC 教室の増設や利用時間の拡張は難しく、検討課題となっている。

PC 教室は授業で利用したい場合、既に別の授業で教室が埋まっていることや、授業で使用される際以外は自習室として開放しているが、授業の使用が多く開放できる自習室が少ない場合、利用できる PC も少なくなり、利用者に対して効率良い学習環境の提供ができないことが頻繁に発生している。

本研究では、これらの問題回避のために、PC 教室以外の研究室や自宅等からでも、個人 PC を使って PC 教室の教育システムが利用出来る仮想 PC 教室環境の設計を行う。その際、仮想 PC 教室から教育システムへログイン際の認証方法は、PC 教室における教育システムのログイン時と同等もしくは同等以上の安全性が保つことができる認証方法とする。

なお、東京海洋大学では、PC 教室の教育システムへのログイン時には、本人認証強化のために IC カードを使った認証方式を用いている。そのため、本研究において、仮想 PC 教室から教育システムにログインする際にも、IC カードを使った認証方式とし、教室 PC から教育システムへログイン際と同等もしくは同等以上の安全性を確保する認証方式を検討する。また、現在、東京海洋大学では、IC カードが発行されているのは学生のみであるが、本研究では、組織内で IC カードが発行されている人も IC カードが発行されていない人も利用できるよう、組織が発行する IC カードだけでなく、個人が保有する携帯電話や定期券等のカード（以下、一般カードとする）でも認証が可能となる仕組みを提案する。

本提案を実現することにより、PC 教室が満室で利用できない場合や、省電力化のため利用時間が短縮された場合でも、PC 教室以外から教育システムの利用が可能になる。さらに、PC 教室で授業を行いたい際に、利用出来る PC 教室や PC が不足していたとしても、持ち込み PC により、同じデスクトップ環境で授業することができるようになる。さらに、万が一、通学が困難な事態が起こっても自宅等から仮想 PC 教室の利用ができることで、教育システムが利用できるようになる。

2 章では、既に PC 教室で稼働中の教育システムと、仮想 PC 教室の構築の為の検討について述べ、3 章では、仮想 PC 教室の設計、4 章では、仮想 PC 教室における教育システム使用時に必要とするカードによる認証方式について述べる。5 章では、提案するシステムに対する評価を述べ、最後にまとめを述べる。

2. 稼働中の教育システム

東京海洋大学の教育システムは、2006 年よりネットブート方式を採用している。2006 年より、全学的に IC カード学生証が導入されることになり、教育システムのログイン時の認証においては、IC カードを使った認証方式を採用している。なお、品川地区においては、2000 年度より IC カードを使った認証方式を採用している 2)。

2.1 PC 教室の教育システム構成

現教育システムは、Citrix 社の Citrix XenDesktop Provisioning Services (PVS) サーバで構成している。教育用 PC のログイン時に、まず、ActiveDirectory サーバ上の DHCP サーバに対して、DHCP 要求を行い、IP アドレスおよびブートサーバ、ブートファイル情報を取得する。次に、PVS サーバに対して、ロ

グインサービスやストリームサービス等を要求し、情報を取得後、イメージ化された仮想ディスクである vDisk をダウンロードする (図 1)。

教育用システムの起動時は、IC カード利用ツールにより、IC カード内に格納されている PIN コード情報と利用者が入力した PIN コードを照合する。照合が合致すれば、IC カード内からユーザ ID とパスワード情報を読み出し、ActiveDirectory に送信する。ActiveDirectory 上でユーザ ID とパスワードの認証に成功すれば、ログイン可となる。IC カードを IC カードリーダから抜くことで、シャットダウンする。

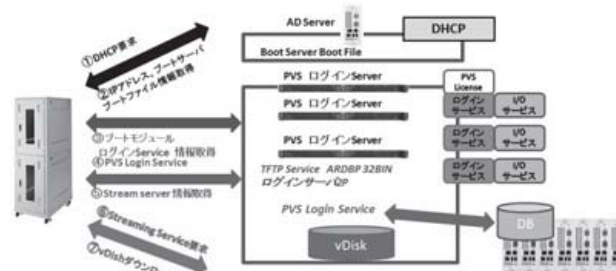


図 1 PVS サーバを使った教育システム

2.2 IC カード学生証

東京海洋大学では、2006 年より学生に対してのみ IC カード学生証を導入し、教育システムのログイン時に IC カードを使った認証方式を採用している。それまでにおいても、品川地区 (旧東京水産大学) の教育システム利用時には、2000 年より IC カードによる認証方式を採用している。IC カード導入の経緯は、なりすましと思われる学外への不適切なアクセスがあったことより、アカウントとパスワードともう一つ個人認証を加えることになり、IC カードが採用された 3)。

カードタイプは接触型・非接触型を組み合わせた FeliCa ハイブリッドカードである。教育システムログイン時の認証は接触チップを使用し、図書館貸出システムや証明書発行システムなどでは、非接触チップを使用している。

2.3 仮想 PC 教室の設計に向けて

仮想 PC 教室を実現する際、PC 教室で既に稼働している教育システムと同じ方式が使えるとよいが、PVS サーバは、使用する端末と物理的に接続しておく必要があることより、離れた場所からアクセスする際に使用するのは難しい。そこで、VDI (Virtual Desktop Infrastructure) 環境を検討する。VDI 環境を実現するためには、既に他大学で実現されている VMware 社 VMwareView や Citrix 社の XenDesktop

Desktop Delivery Controller (DDC) が候補に挙がる 4)5).

両製品について、構築方法や、運用方法の比較を行った 6). VMwareView を使った実現は、既存の教育システムと連動させることができないが、構築時に既存のシステムに対しての変更やシステムの停止を伴わずに、構築ができるというメリットがある。ただし、既存システムとは別のコンソールにて管理することになり、運用・管理におけるコストが増える可能性がある。XenDesktop DDC は、既存の教育システムと連動させることができるが、構築時に既存システムに対して変更を加えることや、既存システムの停止が伴うことがある。しかし、構成管理を既存の PVS サーバへ集約することができることより、運用・管理においてのコストは、現状とほとんど変わらない。運用・管理のコスト削減を求められていることより、VDI の実現は XenDesktop DDC で行うこととした。

3. 仮想 PC 教室へのカード認証方法の検討

次に、仮想 PC 教室における教育システムのログイン時のカードによる認証方法を検討する。東京海洋大学では、IC カードが発行されているのは学生のみであるが、IC カードが導入されていない教職員でも利用できるよう検討を行う。

3.1 先行研究 7)8)

著者らは、大学や大学共同利用機関等の組織において、IC カードを全学導入する際、IC カードが発行されない一時利用者に対して、管理運用の煩雑さやカード発行に関するコストを最低限に抑えるため、一時利用者には IC カードを発行せず、本人が日常利用している交通系 IC カードなどの共通規格に基づいて発行されている IC カード（一般カードと呼ぶ）を使い、IC カードを使ったサービスが利用できるよう提案している。

提案では、システムの重要性に応じて要求されるセキュリティレベルの格付けを行い、中程度以上のセキュリティレベルが要求されるシステムに対しては、本人のみ知りうるキー情報（以下、PIN コードとする）による認証を併用する。

PIN コード認証を行う際、一般カード内には容易に情報を追加できないため、PIN コード情報を認証システム側に格納しておく必要がある。しかし、運用上の観点から、一時利用者の認証に関する認証システムの負荷が一般利用者と同程度以下であることや、一時利用者の登録・抹消に伴う人的コストが十分小

さいことが求められる。また、一時利用者は様々な部局に在籍していることより、一時利用者に対する PIN コードの発行は、中央ではなく、それぞれの部局で行えるようにする。その際、部局の管理者に対しても、PIN コードの管理に対する人的コストが小さいことが求められることより、システム側には、PIN コード情報は格納せず、PIN コードを生成する式だけを格納する。PIN コード生成式は、カード内情報のカードごとに異なる値を利用し、SALT や HASH を用いて生成する。これらを PIN コード生成方式と呼び、これによって、部局の管理者は PIN コードを管理することなく、一時利用者が保持する一般カードに対して、PIN コードを発行すれば、一時利用者はシステムが利用可能になる（図 2）。

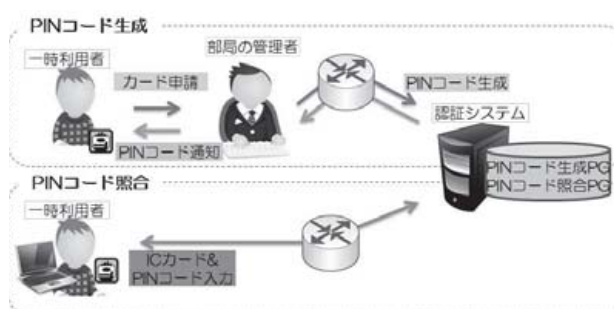


図 2 一時利用者における認証システム

カードやPIN コードを使った認証システムを使用する際、カードの紛失や偽装、PIN コードの紛失や漏えい、カードとPIN コードを書いた紙の両方同時に紛失など、様々なインシデントに対する対応が必要になる。本研究におけるPIN コードは、基本的には、IP アドレスによる制限や共通鍵のようなものとし、学内にいけば誰でも使用できるようなものとする。そのため、PIN コード認証だけでは不足する場合、必要に応じて、個人認証としてID とパスワード認証を加える。ただし、卒業者や退職者がいつまでもPIN コード認証を行えることを避けるため、PIN コードに有効期限を設け、定期的に変更を行う。PIN コード生成式にはSALT を付加し、PIN コードの有効期限ごとに、SALT を変更することで対応する。

3.2 一般カードの使用

一般カードの使用に関しては、先行研究より東京海洋大学の一建屋において、一般カードを用いた入退館システムの試験運用を継続的に行っている。非常用に防犯カメラを設置しているため、カードの複製に対しては意識しなくてよいということより、認証には一般カード内情報からカードIDのみを使用した比較的セキュリティレベルが低いシステムとし

ている。約 200 名の学生と 100 名の教職員が登録しており、学生は IC カード学生証、教職員は Suica や PASMO (パスモ) 等のカードを使用している。IC カードが発行されていない教職員の中で、一般カードを保持していない人や、一般カードを使用することに抵抗を感じる人はほとんどおらず、一般カードが使えることにより、保持するカードが増えないことより、好評の声も多く寄せられている。また、運用においても大きな問題は発生していない。

これらより、東京海洋大学では、学生と一部の教職員以外には IC カードが発行されていないため、本研究においては、先行研究で提案する一般カードによる認証方法の応用を検討する。

3.3 先行研究を応用した一般カード認証システムの検討

本研究における仮想 PC 教室の利用対象者は、一時利用者だけではなく、教職員や学生を含む全ての構成員を対象とする。なお、本研究で定義する一般カードには、大学が発行する IC カード学生証や、FeliCa や NFC (Near Field Communication) 機能搭載の携帯端末等も対象とする。

一般カードによる認証において、セキュリティレベルが比較的低いシステムでは、偽装の恐れ等は考慮しないことより IDm (製造 ID) 等のカード内の読取可能情報を使った認証方法とする。しかし、仮想 PC 教室利用時の認証は、セキュリティレベルが中程度以上のシステムとして、偽装等の恐れを考慮することより、カードと本人のみ知る PIN コードを併用する。この PIN コードを併用する認証は個人認証ではなく、PC 教室につけている IP アドレスによる制限のようなものとする。そのため、PIN コードによる認証後、さらに個人認証 ID とパスワード認証を行う必要があると考える。

3.1 節の先行研究における PIN コード生成の手法は、それぞれの一時利用者がそれぞれの部局で管理するシステムを利用したい場合、それぞれの部局のシステム管理者に PIN コードの発行申請を行う。しかし、本研究で想定している利用者は、大学に所属する全構成員であることより、申請の度に PIN コードの発行を行うことは、非常に負担となるため行わない。そこで、本研究においては、それぞれの利用者が Web 上から PIN コードを発行できる仕組みを構築する。なお、仮想 PC 教室で利用するソフトのライセンス上の関係より、PIN コードを発行可能な人は大学の構成員に限定し、学内ネットワークから ID とパスワードによる認証を行うこととする。

また、先行研究で生成する PIN コードは、一般カ

ードの読み取り可能領域から、カードごとに異なる値を抽出し、少し工夫を加えた値とする。システム側には PIN コードを生成する式のみを格納し、PIN コードは格納しない。部局ごとの管理者が一時利用者に対して、PIN コードを発行する際、管理が複雑にならないことや、ネットワークが離れた研究所等でも容易に利用できるためである。本研究においても、PIN コードを管理する際の人的負担やコストを極力抑えたいことより、システム側には PIN コードは格納せず、PIN コード生成式だけを格納する (図 3)。

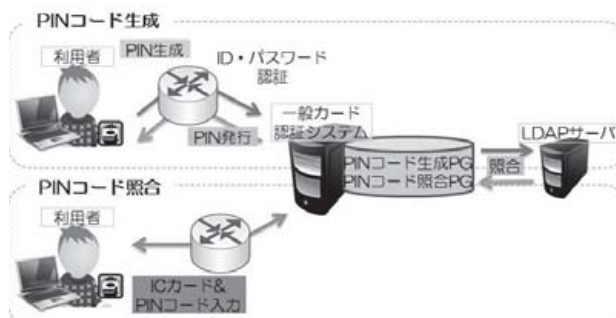


図 3 提案する一般カード認証システムの概略

4. 一般カードを用いた仮想 PC 教室

本章では、2 章と 3 章により検討した上で、提案する仮想 PC 教室について述べる。

実現にあたっては、仮想 PC 教室の教育システムと一般カード認証システムを分けて試験環境の構築を行う。仮想 PC 教室用の教育システムは、XenDesktop DDC を使って実現する。教育システムのログインには、別途、一般カード認証システムを構築し、リバースプロキシを用いて実現する。一般カード認証システムには、PIN コード生成式も格納する (図 4)。

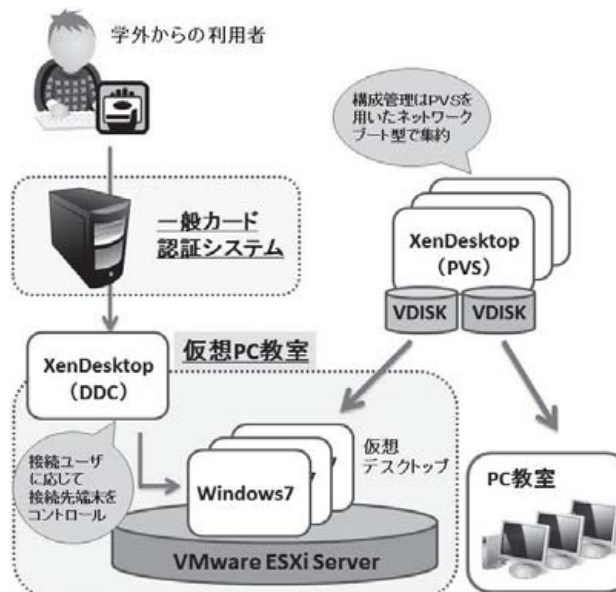


図 4 教育システム

4.1 仮想 PC 教室の教育システムの構成

仮想 PC 教室の実現には、VMware ESXi Server を構築する。そして、その上に、DDC の構築と仮想 PC の新規構築が必要となる。

さらに、本来であれば、東京海洋大学で既に稼働しているシステムと組み合わせるため、Xen Desktop PVS サーバに vDisk を作成するため、既存システムの修正が必要となる。しかし、本研究においては、まず、試験稼働を必要とすることより、既存システムにほぼ影響が及ばないよう、既存システムと同じ構成の PVS サーバを新たに構築し、既存の教育システムとほぼ同様の vDisk も作成する。PVS サーバにより、VMware ESXi Server 上の仮想 PC に vDisk を配信し、DDC により利用者に仮想デスクトップ環境を提供する 9)。

仮想 PC 教室の教育システムの認証には、一般カードと PIN コードによる認証を行い、照合が成功すれば、個人照合のための ID とパスワードによる認証を行う。前者の認証は、一般カード認証システムで行い、後者の認証は、DDC サーバ上の Web インターフェースで行うものとする。

4.2 PIN コード発行

PIN コード利用にあたり、先に、PIN コードの発行が必要となる。PIN コードの発行は、一般カード認証システム上に格納する PIN コード生成式により行う。

4.2.1 PIN コード生成方法

一般カードの読取り可能領域には、カードごとに異なる値が格納されている。PIN コード生成には、これらの異なる値を含めた読取り可能な値から任意の値を抽出したものを組み合わせ、ハッシュ関数によりハッシュ化し、生成された値より任意の桁数を抜き出す。PIN コード生成には、カード内の読取り可能な値だけで、PIN コードが生成できることを防ぐため、一方向関数であるハッシュを組み合わせる。また、一度発行した PIN コードがいつまでも使える状態になることを防ぐため、SALT を付加し、SALT を変更することにより、新しい PIN コード体系に移行する。SALT を変更する際、利用者の混乱を避けるため、移行期間を設定し、移行期間は旧 PIN コードも新 PIN コードも利用できることとする。

4.2.2 PIN コード発行方法

利用者による PIN コード発行時は、まず、学内ネ

ットワークに接続された PC から、PIN コード発行用の専用 Web ページにアクセスし、既に発行済の ID とパスワードでログインする。ログイン後、PIN コード発行画面が表示されるとカードリーダーに一般カードをかざし、カード判別を行う。カード判別に成功すれば、カード内から PIN コード生成に必要な情報を抽出し、一般カード認証システムに送る。認証システム側では送られてきた情報に対して PIN コード生成式により PIN コードを生成し、PIN コード情報を返す (図 5)。



図 5 PIN コード発行フロー

4.3 一般カード認証システムを使った仮想 PC 教室の利用

一般カード認証システムには、PIN コード生成式と PIN コード照合式を格納し、それぞれの照合が成功すれば、リバースプロキシの機能により、仮想 PC 教室に入るための ID とパスワード認証の画面に移行する 10) (図 6)。

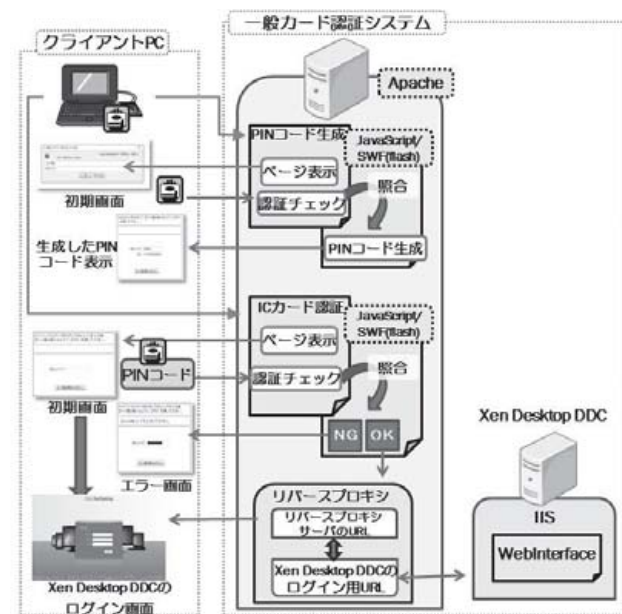


図 6 一般カード認証システム

利用者は、仮想 PC 教室の教育システムを使用す

る際、個人 PC から専用の URL にアクセスする。PIN コード照合を行うための画面が表示されれば、カードリーダーに一般カードをかざす。カード判別に成功すれば、先に生成した PIN コードを入力し、PIN コードの照合を行う。PIN コード照合プログラムでは、入力された PIN コードとカード内から抽出した PIN コード認証に必要な情報を、照合する。PIN コードが合致すれば、仮想 PC 教室の教育システムにログインするための個人照合用 Web ページが表示される。そこで、ID とパスワードを入力し、認証が成功すると、仮想 PC 教室の教育システムにログインできる。

4.4 一般カードを使った PIN コードによる認証方式の評価

本研究における仮想 PC 教室の利用者は、教職員や学生を含む全構成員とすることより、申請の都度、管理者が PIN コード発行を行うと、管理者に非常に負担となる。よって、利用者は申請を行わず、Web インターフェース上から PIN コードの取得を可能とする。PIN コード発行の際の本人確認は、既に発行されている ID とパスワードによる認証を行い、認証に成功すれば、PIN コードが発行可能となる仕組みとしている。PIN コード発行における ID とパスワード認証は、Web インターフェースによるものとし、アクセス制限は学内限定としている。

PIN コードは、SALT やハッシュ関数を組み合わせ生成することにより、自身の PIN コードが漏えいした場合でも、他の利用者の PIN コードは推測できないため、当該利用者以外への影響を防ぐことができる。しかし、PIN コードは、カード内の読み取り可能情報を元に生成するため、カード内の電子証明書等を使用する認証に比べると、安全性が優れているとは言い難い。そのため、一般カードと PIN コードを併用する認証方式は、IP アドレスや共通パスワードによる制限のようなものと考え、PIN コードによる認証後、さらに ID とパスワードによる認証を行う。また、本研究における PIN コードは、利用者個人に対してではなく、一般カード内の情報に対して生成することより、利用者が卒業や退職した後も、いつまでも使える状態になる。これらを防ぐため、利用者の入れ替わりが激しい 4 月か 10 月頃に SALT を変更する必要があると考える。

4.5 提案システムの試験稼働の評価

本研究における提案システムの試験稼働を、数名の学生と教職員により行った。試験稼働のため、ラ

イセンスは 10 ライセンスとし、同時接続数がライセンス数を超えない範囲で、一般カードを使って仮想 PC 教室の利用を行った。学生は既に発行済の IC カード学生証を使用し、教職員は、一般カードを使用した。初めてリーダーを接続する時や仮想 PC 教室への接続時に、3 名失敗することがあったが、以降の試験稼働期間中の利用において問題は発生していない。

個人 PC から一般カードを使用する際、PaSoRi 等のカードリーダーを使用することになるが、PaSoRi リーダーを初めて PC に接続する際、自動的にドライバーをダウンロードする仕組みであるため、ネットワーク環境が不安定な場合、正常に動作しない。また、仮想 PC 教室の実現に DDC を使う場合、利用者が初回利用時に Web ブラウザのプラグインとして Desktop Receiver (Citrix Receiver) をインストールする必要がある。このプラグインは、カード認証後に、ダウンロードを促すダイアログが表示され、各自インストールする必要があるが、ダウンロード時にネットワーク環境が不安定な場合は正常に動作しない。これらについては、運用でカバーできる範囲であると考ええる。

PIN コードは大小英数字含む 6 桁で運用していたが、利用者のほとんどが手書きメモや携帯に記憶させていた。途中で桁数を 4 桁に変更しても、同様であった。カードと同時に PIN コードを紛失しないよう運用でカバーを行うが、同時に紛失した場合でも、一般カードと PIN コードによる認証の後、既に発行されている ID とパスワードによる認証が必要となるため、ただちに悪用される可能性は低いと考える。ただし、ブルートフォース等の悪用の可能性も考えられることより、該当カードや該当 IP アドレスの利用停止方法について、今後、検討が必要である。

本研究で提案するシステムは、利用者にとっては、安定したネットワーク環境があれば、難しい操作を必要とせず利用出来ることより、今後、実運用化に向けて、さらなる検討を行っていく予定である。実運用化に向けては、VDI 環境実現のためのライセンス体系や管理方法についての検討が必要になる。さらに、利用者の個人 PC にカードリーダーが付属していない場合の取り扱いについて、貸出か各自購入か、貸出する場合は、管理方法についても検討が必要になると考える。

5. まとめ

近年、大学等においては、PC 教室を授業で利用したい場合に空き教室がないことや、授業で使用される際以外は自習室として開放しているが、利用でき

る PC の空きがないことが度々発生している。しかし、運用コストが削減傾向にあるため、PC や PC 教室の増設や利用時間の拡張が難しいという問題があった。

そこで、本研究では、PC 教室以外の研究室や自宅等からでも、個人 PC を使って PC 教室の教育システムが利用出来る仮想 PC 教室環境の設計を行った。既に稼働している PC 教室では、本人認証強化のために IC カードを使った認証を用いていることより、仮想 PC 教室のログイン時にも、教室 PC のログイン時と同等もしくは同等以上の本人認証を強化する認証方法が求められる。東京海洋大学では、IC カードが発行されているのは学生と一部の教職員のみであるが、仮想 PC 教室の利用には、IC カードが導入されていない教職員でも利用できるように、大学が発行する IC カードだけでなく、一般カードでも認証が行える仕組みとした。

仮想 PC 教室の実現には、既存の教育システムが Citrix XenDesktopPVS サーバを使用していることより、XenDesktop DDC を用いることで、管理・運用のコストは、これまでとほぼ変わらず運用可能となる。また、一般カードによる認証は、カード複製の対策として、PIN コードを使って認証を行う。一般カードと PIN コードによる認証後、個人を照合する ID とパスワードによる認証を行う。

本提案を実現することにより、PC 教室が満室で利用できない場合や、省電力化のため利用時間が短縮された場合でも、PC 演習教室以外から利用可能になる。さらに、PC 教室で授業を行いたい際に、利用出来る PC 教室や PC が不足していたとしても、持ち込み PC により、同じデスクトップ環境で授業することができるようになる。さらに、万が一、通学が困難な事態が起こっても自宅等から仮想 PC 教室の利用ができることで、教育システムが利用できるようになることが期待される。

参考文献

- 1) 森 博, 田近 一郎, 杉江 晶子: タブレット PC を活用したマルチメディア教育, 名古屋文理大学紀要 12, 97-104, 2012
- 2) 清水さや子, 鈴木直樹, 戸田勝善: IC カードを用いたシンクライアント教育システム, 大学情報システム環境研究, vol.13, 37-46, 2010
- 3) 清水さや子, 横田賢史, 戸田勝善, 吉田次郎: 東京海洋大学における IC カード学生証の運用・評価および今後の展開, 学術情報処理研究, Vol.13, 64-73, 2009
- 4) 櫻田武嗣, 萩原洋一: シンクライアントと持ち込みノート PC による端末室デスクトップ環境の設計, 情報処理学会研究報告, インターネットと運用技術 (IOT) Vol.2011-IOT-13 No.18, 2011.
- 5) 上田浩, 喜多一, 森幹彦, 石井良和, 外村孝一郎, 植木徹, 上原哲太郎, 梶田将司: ネットブートとデスクトップ仮想化を採用した京都大学の教育用端末系の構築: TCO 削減を目指して, 情報処理学会 インターネットと運用技術シンポジウム 2012 論文集, 46-54, 2012
- 6) REPORT A PRINCIPLED TECHNOLOGIES TEST : http://deliver.citrix.com/rs/citrixsandbox4/images/JP_Xendesktop_View_UX_bandwidth_06-21-12v5.pdf
- 7) 清水さや子, 岡部寿男, 吉田次郎: 一般カードを使った一時利用者向け認証システムの設計と実装, 情報処理学会論文誌コンシューマ・デバイス & システム Vol.3, No.1, 34-45, 2013
- 8) 清水さや子, 岡部寿男, 吉田次郎, 戸田勝善: 一般カードを用いた認証システムにおけるハッシュ関数を用いた PIN コード生成方式, インターネットと運用技術シンポジウム 2012 論文集, 70-77, 2012
- 9) Citrix XenDesktop : <http://www.citrix.co.jp/products/xendesktop/overview.html>
- 10) Apache モジュール mod_proxy : http://httpd.apache.org/docs/2.2/ja/mod/mod_proxy.html