キャンパス共通認証認可システムの構築と運用

飯田　勝吉[†a)]　新里　卓史[††]　伊東　利哉[†]　渡辺　治[†††,†]

Construction and Operation of Campus-Wide Authentication and Authorization System

Katsuyoshi IIDA[†a)], Takushi SHINZATO[††], Toshiya ITOH[†], and Osamu WATANABE[†††,†]

あらまし　東京工業大学及び多くの大学において，様々なアプリケーションで認証が必要となり，各部局の担当者がこれまで個別に各アプリケーションごとに認証システムを構築されることが多かった．一方，今後多数の認証が必要なウェブアプリケーションの導入が期待されており，大学で共通の認証システムの構築が極めて重要となる．本論文では東京工業大学において平成 18 年 3 月に導入したキャンパス共通認証認可システムの構築と運用について述べる．キャンパス共通認証認可システムは，大学の重要な ICT (Information Communication Technology) 基盤として設計された．主な特徴としては，すべての学内ユーザに対し基本情報環境権という考え方で IC カード身分証と連動してアカウントを発行すること，PKI (Public Key Infrastructure) 技術などを用いた高いセキュリティを提供すること，ウェブシングルサインオンの導入によりユーザに対し高い利便性を提供すること，学術国際情報センターと事務組織等の作業分担による高い運用管理性を提供することが挙げられる．要求仕様，設計，構築などを述べた後に東京工業大学の経験によって得られた技術的及び運用体制構築の知見を明らかにする．

キーワード　キャンパス共通認証認可システム，PKI，ウェブシングルサインオン，運用管理性

1. まえがき

大学におけるウェブアプリケーションの発展が目覚ましい．学生の履修申告や成績の確認を行う教務システム，研究者それぞれが科学研究費補助金などの研究費ごとの会計支出の登録を行う財務会計システム，図書館における図書の貸し出し状況を調査する図書館システムなど多岐にわたり，更に今後多数の新規ウェブアプリケーションの導入が予想される．これらのシステムの特徴は，ウェブ上で利用者の認証が必要で，利用者の種別などに応じて異なる権限の付与が必要なことである．また，研究用のスーパコンピュータ，学生用の計算機演習室，キャンパス無線 LAN，電子メールなどのアプリケーションにおいて利用者の認証が必要とされている．このように，大学内にはウェブアプリケーションを始めとする多数の認証が必要なアプリケーションが存在する．

しかし，これまでは個々のアプリケーションの管理組織が個別に情報アカウントの管理を行ってきた．例えば，教育担当部署が行っていた講義情報配信システムの Open Course Ware [1] 及び英語教育システム，契約担当部署が行っていた財務会計システムなどがある．また，学術国際情報センターの中においても，電子メールのサービスを研究用コンピュータ（スパコン）のユーザ，教育用コンピュータ（コンピュータ演習室）のユーザ，それ以外の一般のユーザと 3 種類のシステムの運用をセンター内の異なる部署が行っていた．そのため，個々の部署による個別の情報アカウント管理の負荷が大きく問題となっていた．個々のアプリケーションの管理部局が情報アカウント管理に必要な情報を収集し，発行した情報アカウントを個別に配布して

† 東京工業大学学術国際情報センター，東京都
Global Scientific Information and Computing Center, Tokyo Institute of Technology, 2–12–1 Ookayama, Meguro-ku, Tokyo, 152–8550 Japan
†† 東京工業大学技術部情報基盤支援センター，東京都
Division of Technical Staffs, Tokyo Institute of Technology, 2–12–1 Ookayama, Meguro-ku, Tokyo, 152–8550 Japan
††† 東京工業大学大学院情報理工学研究科数理・計算科学専攻，東京都
Graduate School of Information Science and Engineering, Tokyo Institute of Technology, 2–12–1 Ookayama, Meguro-ku, Tokyo, 152–8550 Japan
a) E-mail: iida@gsic.titech.ac.jp

いた．例えば，教職員向けのアプリケーションの場合は学内便という郵便システムを用いてユーザ名，パスワードなどの情報を記載した用紙を配布していた．そのためアプリケーション数が増えるたびに教職員の机の中にユーザ名とパスワードが書かれた用紙の数が増え，利便性が低下するだけでなくセキュリティも低下していた．

また，大学の事務においては，一般に教職員及び学生のアイデンティティ情報を異なる組織が管理している．ここで，アイデンティティ情報とは，職員番号，学籍番号などの個人を識別する番号と，その個人の属性情報（氏名，性別，生年月日，所属）を含む情報で，認証システムの管理に必須の情報である．そのため，教職員だけ，または学生だけが利用するアプリケーションの場合であれば実現は比較的容易であるが，教職員と学生の双方が利用するアプリケーションにおいては，多数の事務組織とのやり取りが必要となり，大学全体での情報システムの管理負荷が増加しがちとなる．東京工業大学（以下，東工大）においては，キャンパス無線 LAN システムを構築する際に，大学内のすべての利用者を含めている認証システムが存在しなかったことにより，学術国際情報センター(注1)の管理負荷が増加し問題となった．

このように，利用者から見た場合はアプリケーションの利便性やセキュリティ，管理者から見た場合は管理負荷を低減するために，共通の情報アカウント管理システムの導入が求められていた．

このような目的のため，東京工業大学（以下，東工大）では平成 17 年度末にキャンパス共通認証認可システム [2], [3] を導入し，平成 18 年当初より運用を開始した．キャンパス共通認証認可システムは，IC カード身分証，LDAP などのアイデンティティ情報ディレクトリシステム，ウェブシングルサインオンシステム，アイデンティティ情報管理システムなどを統合したシステムである．キャンパス共通認証認可システムの特徴は，

（1） 大学内のすべての在籍者（教職員，学生）に対して PKI 対応の IC カード身分証を発行．

（2） 身分証（職員証，学生証）に付随して情報アカウントを発行し，身分証保持者に対して基本情報環境権を提供．

（3） 身分証を発行できないが大学の業務に深くかかわっている者に関しては，例外として「アクセスカード」(注2)という IC カードとそれに付随する情報アカウントを発行．

（4） ウェブシングルサインオンと全学ポータルを導入．

（5） 学術国際情報センターの作業範囲を情報システムの運用管理に限定し，情報アカウント発行作業は他の事務組織が実施．

などがある．

本論文では東京工業大学で導入したキャンパス共通認証認可システムの技術的な特徴と実運用を可能とする制度設計等について述べる．以下 **2.** では，その要求仕様を，**3.** ではその設計，構築及び統計情報について述べる．**4.** では，構築及び実運用により明らかになった知見を述べ，**5.** で関連研究を紹介し，**6.** でまとめる．

2. 要求仕様

東工大のキャンパス共通認証認可システムには様々な要求仕様が存在する．本章ではその要求仕様について述べる．本章で述べる要求仕様を表 1 にまとめる．ここで述べる要求仕様は東工大における要求仕様であるが，東工大だけに通用する特別な要求仕様は特に含まれていないので，多くの大学でも参考になると考えられる．

本システムの第一の目的は，東工大に在籍するすべての個人に対して「基本情報環境権」という権利を付与することである．基本情報環境権とは，利用者が何らかのアプリケーションを利用したくなったときに書面などによる利用申請の必要がなく，東工大に在籍しているだけで事前に付与されている権利のことである．

そのような権利を実現するためには，在籍した初日から情報アカウントを発行する必要があるが，その事務の負荷を低減させ，運用管理性を高めることも大きな要求仕様であった．具体的には，大学内の各部署の人的リソースは限られており，限られた人的リソースの中で効率的な学内の作業分担体制を確立することが重要である．また，大学内で実施することでコストアップの要因となる部分については，外部アウトソース業者に運用してもらうこととし，そのための作業分

(注1)：本論文では，研究用コンピュータ，教育用コンピュータ，キャンパスネットワークなどを管理する大学一般の情報センターのことを「情報センター」と記す．東京工業大学の情報センターを指す場合には，明示的に「学術国際情報センター」と記す．

(注2)：アクセスカードは，部局長等が学長に対して発行申請する IC カードで，科学技術振興機構等の博士研究員であるが東工大の籍をもたない者などに対して発行するものである．

表 1　キャンパス共通認証認可システムの要求仕様
Table 1　Requirements of campus-wide authentication and authorization system.

種別	要求仕様
基本情報環境権	(R0-0) 在籍する個人すべてに対し在籍初日に情報アカウントを付与
運用管理性	(R1-1) 大学全体での運用管理負荷を平滑化する学内での作業分担体制の確立
	(R1-2) 外部アウトソース業者との作業分担体制の確立
	(R1-3) 認可権限の分散管理
セキュリティ	(R2-1) 複数人での情報アカウントの共有を防ぐ認証方式の提供
	(R2-2) 財務会計などのアプリケーションのために耐タンパデバイスを用いた強固な認証方式の提供
	(R2-3) 大学法人と利用者個人の責任の切り分け
利便性	(R3-1) 事前の申請なしにアプリケーションの利用ができること
	(R3-2) ウェブシングルサインオンとウェブポータルサイトの導入
	(R3-3) 特別なハードウェア等を必要としない認証方式を可能とすること
	(R3-4) 柔軟な有効期限の設定を可能とすること
相互接続性	(R4-1) UPKI に参加する他大学との相互接続を可能にすること
性能	(R5-1) 東工大の全構成員の人数（最大約 15,000 人）に登録可能であること
	(R5-2) 大学の基盤として，アクセスが集中した場合でも十分な性能を提供できること

担体制の確立も重要となる．

更に，学術国際情報センターの運用管理負荷を上昇させる要因として，認可権限の管理負荷がある．キャンパス共通認証認可システムに接続するウェブアプリケーションが増えたときに，個々のアプリケーションのための認可権限管理(注3)が必要となり，その設定管理の負荷が問題となる．例えば，財務会計システムであれば，教職員が利用できるが，学生は利用できない．また，学外から電子ジャーナルにアクセスする VPN 機能は，常勤職員と学生であれば利用できるが，出版社との契約の関係上，非常勤職員は利用できない．そこで，認可権限の管理が情報センターに集中せず，学内の個々のウェブアプリケーションの管理者が行えるようにする必要がある．

次に，セキュリティについての要求仕様について述べる．従来，ユーザ名及びパスワードを用いた認証方式による情報アカウント配布の運用を行ってきた．しかし，この方式では過去に複数名で単一の情報アカウントを使い回す事例が報告されていたので，パスワードよりも強固な情報アカウントの発行方法が求められた．更に，高度なセキュリティを必要とする一部のアプリケーションにおいては耐タンパデバイスを用いた偽造が極めて困難な認証方式提供の必要があり，以前から財務会計のウェブアプリケーションにおいては IC カード身分証による認証が採用されていた．そのため，新システムにおいても同様のレベルの認証方式の導入が必要とされた．

また，法人組織と利用者個人の責任の切分けの必要がある．例えば，キャンパス無線 LAN に接続した端末から学外に対する迷惑行為を行う個人の存在を仮定し，法人組織としてはそのような迷惑行為の発生を抑制し，仮にそのような行為が行われた場合に，法人として重過失が問われない制度やシステムを構築する必要がある．そのほか，キャンパスネットワークセキュリティに関する要求条件については, [6] を参考にすること．

次に，利便性についての要求条件について述べる．本システムの最大の目的である基本情報環境権の提供を実現するために，それぞれのウェブアプリケーションは事前の申請なしに利用可能とすべきである．また，今後ウェブアプリケーションの数が増えたときに，それぞれログインするのではなく，一度のログインで複数のウェブアプリケーションの利用を可能とするウェブシングルサインオンの導入が必要である [7]〜[9]．更に，利用者がそれぞれのウェブアプリケーションに効率的にたどり着くために，ウェブポータルサイトの構築が必要である．ウェブシングルサインオンとウェブポータルサイトを構築することにより，ユーザは一度ウェブポータルサイトにログインするだけで，様々なウェブアプリケーションをシングルサインオンで利用可能となる．

また，例えば IC カードによる認証方式のみを提供したとすると，IC カードリーダのない環境でのウェブアプリケーションの利用が不可能となり，多くの学生や教職員が不便になると考えられる．そのため，IC カードリーダなどの特別なハードウェアを必要としな

(注3)：認証と認可の違いについて説明する．認証 (Authenticaiton) とは，アクセスしてきた利用者が利用者本人かどうかを特定することを指す．一方，認可 (Authorization) とは，認証された利用者の権限でどのようなサービスが利用可能かを管理する機能である．例えば [4], [5] が詳しい．

い認証方式の提供が必要である．

更に，有効期限を柔軟に設定することも必要となる．民間企業においては，退職した翌日からすべてのシステムの利用ができなくなる．同様のことを大学で実施した場合は，大きな混乱が生じると考えられる．例えば学生が卒業し，就職先などで新しい電子メールアドレスを取得し，電子メールアドレスの切換が終わるまでは，ある程度柔軟な有効期限の設定が有効と考えられる．

次に，相互接続性についての要求条件について述べる．複数の大学が認証システムを導入した際に，大学間の認証システムの相互接続が検討されている．例えば，学術コンテンツを出版社から購入する際に大学と出版社の間の認証システムの接続方式を統一したりすること，また，大学が E-learning の教材を提供する場合に単位互換制度を用いている他大学の利用者もその教材にアクセス可能とすることである．そのような目的のため，UPKI イニシアティブ [10] という団体と共通仕様 [11] が作られた．UPKI 共通仕様に従い，相互接続性を確保することも要求仕様である．

最後に，性能についての要求条件について述べる．東工大の在籍者全員に対してサービスするものであるので，在籍者全員が登録できる必要があり，また，アクセスが集中した場合の十分な性能を提供で繰る必要がある．

以上で述べたように，基本情報環境権を提供するために，運用管理性，セキュリティ，利便性に関する要求仕様が存在する．また，他大学の認証システムとの間での相互接続性を提供することも要求仕様である．

3. 設計・構築・統計情報

本章では，前節で述べた要求条件を満たすための設計と構築について述べ，現在までの統計情報を記す．なお，前節の表 1 の要求仕様の番号に基づいて説明する．

本章は，東工大のキャンパス共通認証認可システムの設計・構築等ついて述べる．設計・構築においては，学内組織間での役割分担と連携が重要になる．東工大の事例を他大学等でも参考にしやすいように，東工大における学内組織及び各組織の所掌範囲の簡単なモデルを記す．

- 学術国際情報センター（一般には情報センター）

教員・学生が利用する情報通信システムを所掌する．具体的には，研究用コンピュータシステム，教育用コンピュータシステム，キャンパスネットワーク，全学共用電子メールサーバなどである．

- 事務情報担当部署

事務職員が利用する情報通信システムを所掌する．具体的には，事務情報システム及び事務用ネットワークなどである．本論文では事務情報担当部署についての記述は登場しないが，分類上異なるため明示する．

- 人事担当部署

教員・事務職員などの教職員のアイデンティティ情報の管理などを所掌する．

- 教務担当部署

学生のアイデンティティ情報の管理などを所掌する．

- 部局情報システム担当部署

部局で独自に導入した情報システムを所掌する．本論文では，ログイン用 ID・パスワードなどによる個人認証が必要な情報システムについて対象とする．

上記の「アイデンティティ情報」とは，職員番号，学籍番号，氏名，性別，所属，役職，学年などのキャンパス情報システムを構成する際にアイデンティティ情報ディレクトリシステムに含めるべき情報を指す．

3.1 設　　計

要求仕様 R1（運用管理性）に関する設計について説明する．従来，学術国際情報センターなどの情報システム管理部署が情報アカウントの発行までを行っていた．しかし，氏名生年月日などのアイデンティティ情報の源泉情報は人事及び教務担当部署が所掌している．学術国際情報センターが情報アカウントの発行すべてを行うことは，現実的ではない．そこで，情報アカウントの発行は人事及び教務担当部署で行うこととし，学内の業務の効率的な分担を実現した (R1-1)．

しかし，情報アカウントの発行業務は，従来，人事及び教務担当部署の所掌範囲でなかったため，新たな作業負荷が発生する．そこで，従来から行っていた IC カード身分証発行業務を実施すると自動的に付随する情報アカウントが発行されることとした．

また，従来，人事及び教務担当部署は内製により IC カード身分証を発行しており，そのための作業負荷が大きかった．特に，教務担当部署においては，後期入

試該当者の身分証発行情報が入試担当部署より届いてから，入学式までの間に大量の IC カード身分証を発行しなければならず，担当者に大きな負担がかかっていた．

そこで，IC カード身分証発行を外注委託することにより，その部分の負荷を軽減させた (R1-2)．更に，後で説明するセキュリティに関する要求仕様を満たすため，PKI (Public Key Infrastucture) 認証局の運用と PKI クライアント証明書の発行及び IC カード身分証への PKI クライアント証明書の封入作業が必要となる．特に，PKI 認証局は Webtrust for Certification Authorities (CA) [12] などの厳格な基準に基づいて運用する必要があるとされており，内製運用にかかるコストが大きくなる．そのため，IC カード身分証の発行だけでなく，PKI 認証局の運用，PKI クライアント証明書の発行及び IC カードへの PKI クライアント証明書の封入作業をまとめて外注委託することとした．

また，ウェブアプリケーションの認可権限設定の管理負荷を分散させるため，認可権限の分散管理が可能なシステムを導入した．これにより，中央の認証システムは第 1 階層のみを管理し，すなわち第 2 階層の管理者に対して権限を付与する権限を付与し，同様な階層管理により大学全体での業務負荷の平滑化を目指した．階層数をどのように設定するかは，アプリケーションの種別やその運用によって変わってくると考えられる．実際には 5 階層までの認可権限管理を可能なシステムを導入した (R1-3)．

次に，セキュリティに関する要求仕様 (R2) に関する設計について説明する．従来の認証システムでは，通常ユーザ名とパスワードを用いたパスワード認証方式を用いていた．しかし，パスワード認証方式の場合，複数人で情報アカウントを共有する事例が見受けられ，問題となっていた．具体的には，事務組織において，係内のある情報アカウントを共有の情報アカウントとし，複数人が同一の情報アカウントを用いて事務作業を行う例が見受けられた．これにより，仮に何らかのインシデントが発生した際に，責任が不明確になることが問題だったといえる．新システムでは，そのような問題を解決するため，情報アカウントの共有が困難な認証方式の提供が必要となった．

そこで，二要素認証と呼ばれる [5], [13] 認証方式を導入した．二要素認証とは，二つの要素によって認証する方式で，例えばパスワードなどの秘密の情報を知っていることを一要素とし，唯一の存在，または，あまり流通していない物品を所持していることをもう一つの要素とする認証方式である．仮に秘密情報であるパスワードが漏れたとしても，認証に利用する物品が同一人物に渡らない限り，その人物による認証は成功しない．

二要素認証において本人の唯一性を確保するために配布するのが (R2-2) で説明する PKI 対応の IC カードである．IC カードで認証を行う場合，IC カードという物品を所持していることの認証と，事前に設定された本人だけが知っている PIN コードという秘密情報に関する認証を行う．

しかし，PKI 認証方式だけでは後に説明する (R3-3) を満たすことができない．そこで，PKI 対応の IC カードによる認証方式のほかに身分証券面裏に印刷したマトリックスコード表を用いたマトリックスコード認証と呼ばれる方式を用い，その認証方式とパスワード認証の併用方式(注4)を導入した．

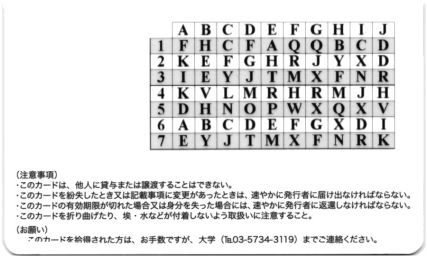
マトリックスコード認証は，マトリックス認証またはグリッドカード認証とも呼ばれる認証方式で，銀行のオンラインバンキングなどで利用されている [14]〜[16]．図 1 にサンプル IC カード身分証を示す．図 1 (b) に裏面のサンプル画像を示しているが，このように個人ごとに異なる表を印刷し，この表のあるマスにある文字に対する質問によって認証することで，パスワード認証を単独で行う場合に比べて複数人での情報アカウントの共有を抑制した (R2-1)．

もちろん，マトリックスコード表をコピーして第三者に渡すことで，原理的には情報アカウントの共有は可能であるが，個人ごとに異なる情報アカウントを用いて情報システムの利用を行う文化が醸成されたこともあり，パスワード認証単独の場合と比べて複数人での情報アカウントの共有が減少したと考えられる．この方式は，二要素認証においてユーザごとに個別の物品を最も安価に配布可能な方式と考えられる．

マトリックスコード認証を採用することのもう一つのメリットとして，キーロガーなどの攻撃に対する対策となることが挙げられる．インターネットカフェなどで，仮にキーロガーがしかけられた端末からアクセスし，パスワードが盗難された場合においても，マトリックスコード表のすべてが盗まれるわけではないの

(注4)：ウェブポータル上では，IC カード認証のログインボタンとマトリックスコード認証のログインボタンを異なるボタンとした．マトリックスコード認証のログインボタンを押すと，ユーザ名とパスワードの問合せが行われ，その後にマトリックスコード認証の問合せが行われる．

(a) 表面



(b) 裏面

図 1　サンプル IC カード学生証
Fig. 1　Sample IC card as student ID.

で，情報アカウントの盗難のリスクが提言すると考えられる．

また，財務会計アプリケーションなどのためのより強固な認証方式の提供を図った．耐タンパ性のあるデバイスに PKI 認証局によるクライアント証明書発行の際に利用したプライベート鍵を封入し，そのデバイスを保持し，なおかつそのデバイスに結び付けられた PIN コードが照合できたときのみ，本人認証することとした (R2-2)．

そのようなデバイスの候補として，IC カード身分証のほかに USB キーなどの提供も検討した．しかし，人事及び教務担当部署は IC カードの発行業務は行っていたが，USB キーの発行業務は行っておらず，新たな作業負荷が発生するため，運用負荷の観点から，IC カード身分証を採用した．

更に，例えば利用者個人がキャンパス無線 LAN に接続して学内外への迷惑行為発生を抑制するなどの目的で，法人（大学）と利用者個人の責任の切分けが必要となった．そのため，IC カード身分証及び情報アカウントの発行に先立ち,「情報基盤利用に関する誓約書」を制定し，利用者個人から誓約書を提出してもらうこととした（図 2）(R2-3)．更に，ログインするたびに「東京工業大学情報基盤利用承諾」に同意ボタンを押してもらうこととし，利用者個人の責任を明確化

情報基盤利用に関する誓約書

国立大学法人
東京工業大学長　殿

私は，このたび，国立大学法人東京工業大学の情報基盤を利用するにあたって，東京工業大学情報倫理ポリシー，東京工業大学情報セキュリティポリシー，及び東京工業大学共通認証・認可カード利用の注意を遵守するとともに，学内外への情報の受発信には社会的責任が伴うことを十分理解し，情報環境を乱すことのないよう良識に基づいた節度ある利用を行うことを誓います．

図 2　情報基盤利用に関する誓約書
Fig. 2　Information infrastructure use agreement.

東京工業大学情報基盤利用承諾

東京工業大学の情報基盤を利用するにあたり，本学の「情報セキュリティのためのガイド」に記載の本学情報倫理ポリシー及び情報セキュリティポリシーならびに下記の「東工大情報基盤利用ガイドライン」,「通信記録の取り扱い」をよく理解し，情報環境を乱すことないよう良識に基づいた節度ある利用を行うことに同意します．

図 3　東京工業大学情報基盤利用承諾
Fig. 3　Agreements on Tokyo Tech information and comunication infrastructure.

した（図 3）．

次に，利便性 (R3) に関する設計について述べる．(R3-1)=事前の申請なしにアプリケーションの利用ができること，に関しては (R1-1) で述べた IC カード身分証発行に付随して情報アカウントを発行することで可能とした．

ユーザの利便性において重要な要素に，ウェブシングルサインオンとウェブポータルサイト（図 4）の導入がある (R3-2)．ウェブシングルサインオンの導入により，一度のログインで複数のアプリケーションをシームレスに利用することが可能となり，ウェブポータルサイトの導入により，ウェブアプリケーションが増えた際に利用者を効率的に各アプリケーションに誘導することが可能となる．

ウェブシングルサインオンには，一般に，リバースプロキシ型とエージェント型の 2 種類の方式が存在する（シングルサインオンの 2 種類の方式の詳細については，例えば [17] を参照のこと）．本システムでは両方の方式を採用した (R3-2)．リバースプロキシ型は，ウェブアプリケーションのサーバの配置場所をネットワーク的にウェブシングルサインオンサーバの内側に

図 4　東工大ポータル [18]
Fig. 4　Tokyo Tech portal.

おき，ウェブシングルサインオンが認証済みかどうかを調べて内部のアプリケーションに接続する方式である．一方，エージェント型は Apache，IIS などのウェブサーバソフトウェアに専用のモジュールを組み込み，モジュールを通してユーザが認証済みかどうかを確認する方式である．エージェント型のメリットはネットワーク的に柔軟に配置できることがメリットである．そのため，ほとんどのウェブアプリケーションは原則としてエージェント型で導入することとした．しかし，アプリケーションによっては専用のモジュールソフトウェアを組み込みことができない．実際，学内ネットワークアクセスのための SSL-VPN というウェブアプリケーションを接続する際に，SSL-VPN はアプライアンスであり専用の OS を用いることによりエージェントモジュールを組み込むことができなかったため，この場合にのみリバースプロキシ型を利用することとなった．

また，(R3-3)=特別なハードウェア等を必要としない認証方式を提供すること，に関しては，R2-1 で説明したマトリックスコード認証方式を利用することにより対応した．マトリックスコード認証方式は特別なハードウェアを必要とせず，また，Internet Explorer や Firefox などの標準ブラウザで利用できるため，利便性が高いといえる．

(R3-4)=柔軟な有効期限の設定を可能とすること，に関しては，有効期限が切れたのちに 2 種類の猶予期限を設けることとした．IC カード身分証は非接触 IC カード機能を用いた入館証としても機能する．例えば，3 月末で卒業した学部生が 4 月から大学院生に進学した場合，新カードが付与されるまでのあいだに旧カードが期限切れになると業務に支障がでる．この目的のため，IC カードの機能は身分証の有効期限が切れたのちに 15 日間猶予期間を設けた．更に，電子メールのアプリケーションに関しては，更に長い猶予期間が必要と考えられる．そこで，マトリックスコード認証に限定し，更にアプリケーションを電子メールに限定し，有効期限が切れた後に 90 日間の猶予期間を設けることとした．

次に，相互接続性に関して説明する．平成 17 年当時，7 大学情報基盤センター会議・認証研究会にて議論されていた．そこでは，SAML (Security Assertion Markup Language) 2.0 [19] という方式でウェブ認証を導入し，SAML の技術で相互接続すると議論されていた（SAML については [9] が詳しい）．そのため，SAML2.0 対応のシングルサインオンソフトウェアを導入した (R4-1)．しかし，現在は，SAML の拡張方式である Shibboleth [20] が標準とされている [21]．Shibboleth も SAML を拡張した方式であるので，Shibboleth との相互接続は比較的容易と考えられる．

また，[11] によると，UPKI のアーキテクチャは学内認証基盤，オープンドメイン認証基盤，グリッド認証基盤の 3 層構造で構成されるとされており，学内認証基盤は利用者を学内在籍者に限定した認証基盤とするとされている．つまり，学内在籍者のためにクライアント証明書を発行する学内認証基盤の PKI 認証局は，いわゆるプライベート認証局とし，学内に閉じた認証局としてよいことを意味している．もし，認証局証明書が幅広く普及しているウェブブラウザ等にインストール済みであるオープンドメイン認証局(注5)によって発行したとすると，その認証局は東工大以外の顧客のクライアント証明書も発行することになる．結果として，その認証局が発行するクライアント証明書は東工大在籍者のものだけではなくなり，つまりキャンパス共通認証認可システムに接続するアプリケーションを実装する際において，正しいクライアント証明書を検証するだけでは東工大在籍者かどうかの区別ができなくなり，その結果として構成が複雑になる．そのため，キャンパス共通認証認可システムにおいて外注運用している認証局は，プライベート認証局とし

(注5)：パブリック認証局と呼ばれることもあるが，政府認証基盤などの公的機関の PKI との混同を避けるためにオープンドメイン認証局と呼ぶ．

表 2　キャンパス共通認証認可システムの主なソフトウェア一覧
Table 2　List of installed softwared in campus-wide authentication and authorization system.

種別	ソフトウェア名
LDAP サーバ	Sun JAVA Directory Server
シングルサインオンサーバ	Entrust GetAccess
マトリックス認証サーバ	Entrust IdentityGuard
PKI IC カード及び認証ソフトウェア	NTT communications eLWISE Security Keeper
アイデンティティ情報管理メタディレクトリミドルウェア	Exgen LDAP Manager
IC カード及び情報アカウント発行システム	新規開発

た．なお，オープンドメイン認証基盤はウェブブラウザや S/MIME 対応メールソフトなど主要な PKI アプリケーションがその認証局を信頼できる認証局として事前に登録している基盤であり，学内の利用者が正当かどうかを判定する学内認証基盤とは目的が異なるため，別の基盤となっている．

最後に，表 2 にキャンパス共通認証認可システムを構成する主なソフトウェアを示す．ほとんどのソフトウェアは商用のソフトウェアを利用し，ただし，IC カード及び情報アカウント発行システムに関しては東工大の事情に合わせて新規開発した．

3.2 構　　築

本節ではキャンパス共通認証認可システムの構築について説明する．平成 17 年当時，IC カード身分証を利用していたが，IC カードが陳腐化及び高コスト化し，一刻も早い身分証の更新が求められていた．当初は単に身分証だけの更新をする案もあったが，大学の ICT (Information Communication Technology) の重要基盤とするべくウェブシングルサインオン等も導入することが大学執行部により決定された．

決定された時期は，平成 17 年 7 月であり，同年 11 月 27 日応札期限，同年 12 月 27 日開札，平成 18 年 3 月 31 日納入期限というスケジュールで納入された．このようなスケジュールであったため，仕様書作成及び制度設計などを急ピッチで進める必要があった．

中心となって活動したのは，学術国際情報センター運営委員会の下に設置された，情報基盤検討専門委員会であった．同委員会は，当時学術国際情報センターの副センター長であった渡辺治を委員長とし，センター教員 5 名，センター外教員 4 名から構成された（その後，センター教員 12 名，センター外教員 6 名に増員された）．平成 17 年 10 月 31 日に同委員会設置前の予備会合を開き，その後，平成 18 年 3 月 8 回の第 7 回委員会までの間に計 8 回の会合をもった．

表 3　キャンパス共通認証認可システムのアプリケーション
Table 3　List of applications connected to campus-wide authencation and authorization system.

種別	名称
研究	東工大リサーチリポジトリ (T2R2)
教育	TOKYO TECH OCW 教務 Web システム 講義支援システム
共通・事務	共通メール（ウェブメール） 学内ネットワークアクセス (SSL-VPN) 無線 LAN アクセス 物品等請求システム 図書館オンラインリクエスト 人事給与 Web システム ソフトウェア配布システム
管理・設定	パスワード変更 姓名読み登録 タイムアウト設定 共通メール設定（管理者用） キャンパスネットワークサービス（管理者用） 業務 ID 管理サービス（事務システム利用者専用）

同委員会は，七つの作業班（総括班，新入生班，在校生班，職員班，入館システム班，認証システム班，メール班）を構成し，教員以外に事務職員及び技術職員計 20 名とともに導入等の作業にあたった．

平成 18 年 3 月末の検収の後，同年 4 月 3 日から本学所属の常勤職員，非常勤職員，学生の全員にカード配布を開始し，システムの利用を開始した．ただし，接続するアプリケーションがほとんどなかったため，開始当初のアクセス数は比較的低調であった．

表 3 に平成 21 年 4 月現在のウェブアプリケーションの一覧を示す．特に共通・事務というカテゴリーのアプリケーションが充実しており，今では東工大の在籍者にとってなくてはならない ICT システムとして機能している．なお，ソフトウェア配布システムについては [22] を参考にされたい．

また，前節で述べたとおり，PKI 認証局はプライベート認証局としてアウトソース運用することとしたが，その運用基準である認証局証明書ポリシー・認証運用規定（いわゆる CP/CPS）を規定し，どのレベルでの運用基準にするかを検討する必要があった．運用基準としては，東工大のセキュリティポリシーに従って満たすべきレベルを検討し，そのレベルにて規定する案もあったが，今後 UPKI において認証局の大学間連携するときのことを考慮し，最大限高い基準とし

表 4　キャンパス共通認証認可システムの登録者数
Table 4　Number of registered people in campus-wide authencation and authorization system.

種別	人数
常勤職員	1,765
非常勤職員	1,568
アクセスカード	302
学部学生	4,688
修士学生	3,390
博士学生	1,440
研究生（その他）	133
計	13,286

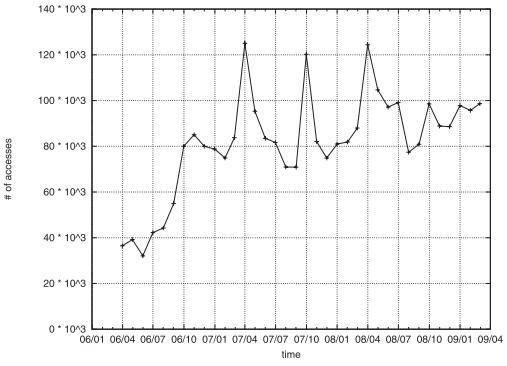


図 5　東工大ポータルトップページアクセス数の遷移
Fig. 5　Transition of number of accesses of Tokyo Tech portal.

て，Webtrust for CA [12] の基準に従うこととした．CP/CPS は，運用開始後の平成 19 年 3 月 12 日に制定された [23]．

3.3 統 計 情 報

本節ではキャンパス共通認証認可システムの統計情報を記す．表 4 に平成 21 年 4 月現在の登録者数を示す．ここで，アクセスカードとは，東工大に在籍していないが，東工大の業務に深くかかわっているため，部局長から学長に対して IC カードの発行申請があったものである．そのため，東工大の学内で生活し，IC カードの取得が必要な人はほぼ全員取得している状況といえる．

次に，平成 18 年（西暦 2006 年）4 月から平成 21 年（西暦 2009 年）3 月までの 3 年間における，1 か月単位での東工大ポータルトップページのアクセス数の遷移を示す（図 5）．月単位でのアクセス数の変化は激しいが，全体として，増加傾向にあることが見て取れる．また，4 月と 10 月のアクセス数が多いことが分かる．これは，入学等による新たな在籍者が多数生じる時期が 4 月と 10 月だからであると考えられる．

4. 構築・運用によって明らかとなった知見

本章では，システムの構築及び 3 年間の運用によって明らかになった知見を述べる．大規模な大学において PKI 対応の IC カード身分証の全構成員への配布を伴う全学認証システムを導入・運用した過去の事例はなく，設計・構築及び運用を始める際は手探り状態であった．そのため，設計・構築の際には気がつかなかった多数の問題が運用することにより明らかになった．その中でも，今後導入する大学にとって意義があると思われる知見を紹介する．

4.1 一時停止機能

東京工業大学のキャンパス共通認証認可システムには，情報アカウントの一時停止機能を設けなかった．一時停止機能とは，電話等で身分証の紛失の連絡があった際に，身分証の再発行を行わずに，情報アカウントの機能を一時的に停止する機能である．一時停止機能を設けなかったために，確実に本人確認がとれない場合（電話など）において，身分証の再発行をする必要があり，無駄が生じてしまう．運用を考慮すると，一時停止機能は必須の機能と考えられる．

4.2 氏名の漢字コード

LDAP サーバソフトウェアは，通常，氏名のフィールドに UTF-8 でエンコードする．しかし，東京工業大学のキャンパス共通認証認可システムの場合，メタディレクトリミドルウェアが SJIS で受け取ったデータを変換して UTF-8 でエンコードする．そこで，SJIS で記録する印刷用氏名のスキーマを作り，第 2 水準以上の難しい漢字の印刷に対応した．氏名の漢字は難しい漢字が多いため，仕様策定の際には漢字コードについて十分注意すべきと考える．

4.3 新入生の氏名のデータ

新入生の氏名のデータは，大学入試センターから入試担当部署を経由して入手される．ところが，そのデータ中の氏名のデータに関しては，カナ文字のデータだけしか含まれていないため，留学生などを除くとアルファベット氏名が含まれていない．東京工業大学では，基本情報環境権の重要な要素として電子メールの情報アカウントを配布し，そのアドレスの決定方法に氏名を使うのだが，アルファベット氏名のデータがないため，事前に電子メールアドレスを決定することができない．そのため，自分でログインし，半角アルファベット氏名のデータを登録した後に，電子メールを利用可能とする方式を採用した．入学時にメールア

ドレスが発行されていることが学内の様々な事務の観点から便利であるが，学生が入学後に自分でログインしアルファベット氏名のデータを自分で登録する方式にも一定の合理性があると考えられる．

4.4 ユーザ問合せ対応部署と情報システム運用管理・開発部署の分離

学術国際情報センター内で，キャンパス共通認証認可システムの運用を行うため，新設の部署を設けた．東工大ポータルは，すべてのウェブアプリケーションの入口であるため，各ウェブアプリケーションを管理する部局情報システム担当部署ではなく，東工大ポータルの運用管理部署に様々な問合せが寄せられることとなった．その結果として，一義的に行うべき，情報システム運用管理の力がそがれることとなった．特に，様々な要望に対応するため情報システムの改良や新機能の開発を絶えず行っているが，そのための能力がそがれることが問題といえる．認証システムの導入を検討する大学に対しては，可能であればユーザ問合せ対応部署と情報システム運用管理・開発部署の分離を検討することをお勧めする．

4.5 アプリケーション収容のポリシーと運用体制の確立

要求仕様 (R1-3) において，認可権限の分散管理が運用上必要になると述べた．しかし，システムを導入して実運用を始めたところ，実際には分散管理の利用が困難であった．そもそも，東工大では現在のところ全学的なサービスのみを収容しており，各部局等が個別に行うアプリケーションの接続ができていない．実際に接続するためには，そのためのポリシーを作る必要がある．更に，部局等に対してどのような運用体制を求めるかの検討も必要となる．

5. 関 連 研 究

キャンパスネットワークにおける無線 LAN やオープン端末の認証に，Opengate がある [24], [25]．また，大学向けのオープンソースのシングルサインオンサーバソフトウェアに CAS (Central Authentication System) [26] 及び CAS^2 (Central Authetication and Authorization Service) がある [27].

また，他大学における共通認証システムの導入事例として, [7], [8], [28] 等がある．名古屋大学は平成 16 年（西暦 2004 年）に CAS^2 を導入し，成績入力及び履修登録などに利用している [7]．大阪大学は学務情報システムなどを対象とした全学 IT 認証基盤を構築し，平成 19 年（西暦 2007 年）1 月より運用を開始している [29]．慶応義塾大学は keio.jp というドメインにおいて共通認証システムを運用している [28]．いずれも大学の共通の認証システムであるが，東工大のキャンパス共通認証認可システムと異なり，全構成員に IC カード化された身分証を配布したものではない．

6. む す び

本論文は，東京工業大学のキャンパス共通認証認可システムを紹介した．基本情報環境権という新しい権利を全学在籍者に IC カード身分証に付随する情報アカウントの形式で配布した．システムの重要な要求仕様としては，運用管理性，セキュリティ，利便性，相互接続性があった．それらの要求仕様を満たすべく，システムの設計について延べ，実際にシステムを構築と運用によって明らかになった知見を示した．

今後は，運用管理性の更なる向上と認証システムの普及が求められる．現在のところ，キャンパス共通認証認可システムに接続するウェブアプリケーションの数は限定的で，特に各部局による部局専用のアプリケーションの導入を行っていない．今後そのような利用の拡大を実現するためには，部局情報システム担当部署に対する接続方法などの運用管理のフローを確立し，認証システム側の運用管理負荷を減らす必要がある．また，大学における認証システムや IC カード身分証は幅広く普及しているとはいえない．そのため，このような論文により本学での知見を明らかにし，またセミナー [30] を開いて多くの大学の方々に紹介している．今後もこれらの活動を続け，認証システムにおける先導的役割を続けたいと考えている．

謝辞 キャンパス共通認証認可システムの導入，運用にあたっては，多数の方々のお世話になりました．本学関係者と致しましては，情報基盤検討専門委員会の委員の皆様，関連する技術職員・事務職員の皆様，何より同システムの導入を決めた執行部の皆様に感謝致します．また，学外におきましては，システム導入を実施して頂きました多数の業者の関係者の皆様に，仕様策定等に多くの御意見を頂いた認証研究会の皆様に厚く御礼申し上げます．最後になりましたが，招待論文のお招きを頂き，私どもに本論文の発表の機会を頂きました特集号編集委員会の皆様に深く感謝申し上げます．

文　　献

[1] 植松友彦，“Tokyo Tech OCW の公開について,” 東工大

クロニクル，no.401, pp.14–15, July 2005.
http://www.titech.ac.jp/about/introduction/pdf_chronicle/401.pdf
[2] 飯田勝吉，“招待講演：キャンパス共通認証・認可システムが拓く高度な研究・教育のための情報通信基盤，”信学技報，IA2006-22, Oct. 2006.
[3] 新里卓史，飯田勝吉，岸本幸一，太刀川博之，昆野長典，山崎孝治，伊東利哉，渡辺　治，“大学内の業務・システムと連携するキャンパス共通認証認可システムの構築と運用，”信学技報，NS2006-197, March 2007.
[4] Microsoft, “It’s me, and here’s my proof: Why identity and authentication must remain distinct,” Feb. 2006. http://technet.microsoft.com/en-us/library/cc512578.aspx
[5] D. Todorov, Mechanics of user identification and authentication: Fundamentals of identity management, Auerbach Publications, 2007.
[6] 飯田勝吉，“招待講演：キャンパスネットワークにおけるセキュリティ運用の実態と技術動向，”信学技報，IN2008-125, Feb. 2009.
[7] 内藤久資，梶田将司，小尻智子，平野　靖，間瀬健二，“大学における統一認証基盤としての CAS とその拡張，”情処学論，vol.47, no.4, pp.1127–1135, April 2006.
[8] 秋山豊和，寺西裕一，岡村真吾，坂根栄作，長谷川剛，馬場健一，中野博隆，下條真司，長岡　亨，“大阪大学における全学 IT 認証基盤の構築，”情処学論，vol.49, no.3, pp.1249–1264, March 2008.
[9] 高橋健司，“アイデンティティ管理の現状と今後，”信学誌，vol.92, no.4, pp.287–294, April 2009.
[10] 国立情報学研究所，“UPKI イニシアティブ.”
https://upki-portal.nii.ac.jp
[11] 島岡政基，谷本茂明，片岡俊幸，峯尾真一，曽根原登，寺西裕一，飯田勝吉，岡部寿男，“大学間連携のための全国共同電子認証基盤 UPKI における認証連携方式の検討，”信学技報，IA2006-3, May 2006.
[12] American Institute of Certified Public Accountants, Inc. and Canadian Institute of Chartered Accountants, “WebTrust for certification authorities.”
http://www.webtrust.org/
[13] S. Randy, “Two-factor authentication for online banking: Here are some key things to consider when trying to satisfy new federal banking guidelines to protect online account access,” Aug. 2007.
http://www.entrepreneur.com/tradejournals/article/168180769_1.html
[14] Wisdom, “マトリクス認証.”
http://www.blwisdom.com/word/key/000464.html
[15] G.D. Williamson, “Enhanced authentication in online banking,” J. of Economic Crime Management, vol.4, no.2, Fall 2006.
[16] Entrust, “IdentityGuard.” http://japan.entrust.com/products/identityguard/enterprise.html
[17] 松永　功，“アイデンティティ管理の実現に関する一考察，”INTEC TECHNICAL JOURNAL, no.2, pp.58–63, Oct. 2003.
[18] 東京工業大学学術国際情報センター，“東工大ポータル.”
http://portal.titech.ac.jp/
[19] OASIS, “SAML specifications v2.0,” March 2005.
http://saml.xml.org/saml-specifications
[20] Internet2, “Shibboleth.”
http://shibboleth.internet2.edu
[21] 国立情報学研究所，“UPKI シングルサインオン実証実験〜Shibboleth を利用した大学間認証連携の実現.”
https://upki-portal.nii.ac.jp/SSO
[22] 新里卓史，飯田勝吉，植松友彦，渡辺　治，“東京工業大学におけるキャンパス共通認証認可システムを用いた安全なソフトウェア配布機構の設計と実装，”信学技報，IA2007-48, Jan. 2008.
[23] 東京工業大学，“認証局証明書ポリシー (CP)・認証運用実施規定 (CPS)，”March 2007. http://portal.titech.ac.jp/info/titech_cps_4.pdf
[24] 渡辺義明，渡辺健次，江藤博文，只木進一，“利用と管理が容易で適用範囲が広い利用者認証ゲートウェイシステムの開発，”情処学論，vol.42, no.12, pp.2802–2809, Dec. 2001.
[25] 只木進一，江藤博文，渡辺健次，渡辺義明，“利用者移動端末に対応した大規模ネットワークの Opengate による構築と運用，”情処学論，vol.46, no.4, pp.922–929, April 2005.
[26] JA-SIG, “The central authentication service project.”
http://ww.jasig.org/cas
[27] H. Naito, S. Kajita, Y. Hirano, and K. Mase, “Multiple-tiered security hierarchy for web applications using central authentication and authorization system,” Proc. IEEE/IPSJ 2007 Intn’l Symposium on Applications and the Internet Workshops (SAINTW’07), CDROM, no.27, Jan. 2007.
[28] 慶応義塾大学，“keio.jp — はじめに.”
http://keiojp.itc.keio.ac.jp/manual/
[29] 秋山豊和，寺西裕一，岡村真吾，坂根栄作，長谷川剛，馬場健一，中野博隆，下條真司，“キャンパス IT 認証基盤の構築—大阪大学における導入事例と課題，”信学技報，IA2007-9, May 2007.
[30] 東京工業大学学術国際情報センター (GSIC)，“2008 年度 GSIC セミナー，”April 2008.
http://portal.titech.ac.jp/seminar/

（平成 21 年 4 月 7 日受付，6 月 8 日再受付）

飯田　勝吉　（正員）

平 8 九工大・情報工・電子情報卒．平 10 奈良先端大・情報科学・博士前期課程了．平 12 九工大・情報工・博士後期課程中退．同年奈良先端大・情報科学・助手．平 13 米国カリフォルニア大学アーバイン校計算機科学科客員研究員．平 16 東工大・学術国際情報センター講師．平 19 東工大・学術国際情報センター准教授．ネットワークシステム工学，ネットワークシステムの性能解析に関する研究に従事．平 15 テレコムシステム技術賞，平 17 本会通信ソサイエティ活動功労賞，平 19 本会ネットワークシステム研究賞．博士（情報工学）．IEEE 会員．

新里　卓史

平 12 埼玉大・工・応用化学卒．平 14 東工大・技術職員．平 17 よりキャンパス共通認証認可システムの構築，運用などに従事．

伊東　利哉　（正員）

昭 57 東工大・工・電気電子卒．昭 59 同大大学院工学研究科博士前期課程了．昭 59 日立製作所入社．昭 60 東工大・工・助手．平 2 東工大・総合理工・講師．平 4 同助教授．平 13 東工大・学術国際情報センター教授．理論計算機科学，応用離散数学などの研究に従事．工博．ACM，情報処理学会各会員．

渡辺　　治　（正員）

昭 57 東京工業大学大学院理学研究科情報科学専攻博士後期課程中退．同年，理・助手．平 9 より東工大・情報理工・数理・計算科学専攻教授．平 17 より東工大・学術国際情報センター副センター長兼務，平 19 より同センター長兼務，計算の理論，特にアルゴリズムの設計と解析，計算の複雑さの理論の研究に従事．平 4 日本 IBM 科学賞．工博．EATCS，LA，情報処理学会各会員．