

東京大学 情報基盤センター

MISSION

- 文献の閲覧など学内の充実したWebシステムのオフキャンパスでの利用
- 多種多様なOSや使い手が混在する環境でのシームレスな稼動と導入の手間の削減

SOLUTION

- セキュリティをPKI認証で強化し、リモートアクセスの利便性を最大限に活用
- マルチプラットフォーム対応でユーザー環境を問わず、かつクライアントレスで管理の手間も大幅削減

IDとパスワードだけでは情報は守れない 東京大学のネットワークを支える情報基盤センターは FirePassとPKIの連携によるシステムを選択した

東京大学情報基盤センターは、大学内におけるネットワーク整備の支援や、共同利用PCのサービスなどを提供している。大学内のネットワークではプライバシーに関わる情報を多く取り扱うため学外からの利用は制限されていたが、長期出張なども多い大学教職員の間にはリモートアクセスの需要が高まっていた。そんな中、学内システムの強固なセキュリティ基盤構築のため、USBトークンを使ったPKI認証の導入が決まった。そこで、同センターでは次に、学生や全教職員が利用できるシステムへと展開することも視野に入れた情報共有のためのリモートアクセス環境の構築を視野に入れ、既存PKI製品との連携実績を持つF5ネットワークスのSSL VPN製品FirePassを選択した。



東京大学
情報基盤センター
助教授 理博
佐藤 周行氏



東京大学
情報基盤センター
図書館電子化研究部門 中川研究室
助手 博士(情報学)
清田 陽司氏



東京大学
情報基盤センター
特任助手
西村 健氏

学校プロフィール

東京大学 情報基盤センター

〒113-8658 東京都文京区弥生2-11-16
Tel:03-5841-2710

URL:<http://www.itc.u-tokyo.ac.jp/>

大型計算機センター、教育用計算機センターおよび図書館の一部を改組して誕生したのが、現在の東京大学情報基盤センターだ。教育のための大学内のコンピュータ、ネットワーク整備を行っており、研究部門とそれに付随する業務支援部門から成っている。すでに提供されているサービスの運営、管理だけではなく、さらなる利便性向上のための研究も行なわれている。

Pentio PKI Private CAとFirePassの連携により、 安全性の高い個人認証が実現 リモートアクセスに求められる課題をクリア

PKI導入により打破された セキュリティの壁

東京大学情報基盤センターでは、学内システム利用者の個人認証を強化するため、PKIを導入している。USBトークンタイプのもので、個人が所有するトークンを接続しなくてはネットワークにログインできない仕組みになっている。こうした個人認証の基盤が整ったことを受け、学内向けのWebサービスをオフキャンパスで利用するための仕組みづくりがスタートした。「IDとパスワードによる認証は、みなさんが思っているほど安全ではありません。リモートアクセスを考えた場合にも、既存のPKIと連携できることがまず最初の条件でした」

PKIの導入にも当たった佐藤助教は、そう述べた。情報基盤センター内では情報共有や施設予約などのためにサイボウズが利用され、図書館では過去のジャーナルをPDF化し、オンラインで閲覧できる電子ジャーナルも実現されている。研究に必要な資料確保から学生の成績管理、物品の購入にいたるまでがWebサービス化されていく一方、それらのサービスはセキュリティ上の配慮から、IPアドレスによるアクセス制限に守られ続けていた。FirePass導入以前には職員が活用できるようリモートアクセスの環境は存在しなかった。大学の教職員には長期出張なども多く、もともとオフキャンパスでの学内システム利用には需要があったが、予算や成績などのプライバシーに関わる情報を扱うため、外部への開放には慎重にならざるを得なかった。

2005年春、リモートアクセス環境を構築すべく機器選定が始められた。大学内ではMacintoshやLinuxも多く利用されているため、佐藤助教らはマルチプラットフォームに対応することを条件として機種種を選び、実際に試用して詳細な比較検討を

行なった。その結果、FirePassの優れたセキュリティ機能と実行速度の高さが認められ、採用されることとなった。特に使用感においては、もっとも快適なパフォーマンスを得られたという。また佐藤教授とともに導入にあたった清田氏は、FirePassに対するサポート体制の厚さにも安心感を覚えたという。「検討した機種の中には、試用段階では一切サポートを受けられない機種もあり、苦労しましたが、FirePassはドキュメントが充実している上、販売店によるサポートも手厚く、使用段階での操作や設定でも迷いませんでした」

GUIの完成度の高さも、ドキュメントの整備と並んで評価の対象となった。比較、検討した機器の中でGUIが日本語化されていたのはFirePassだけだったのだ。また、「既に導入を決めていたペンティオさんのPKI製品との連携部分についてもFirePassとの連携実績があったので安心して選択することができました」と西村氏は語ってくれた。

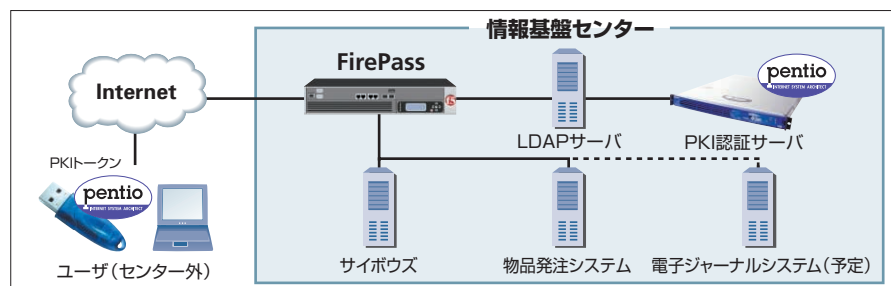
アカウントごとのアクセス権限管理など 機能面の課題はクリア

導入に際しては、まずは情報基盤センターの中で実際に運用をスタートさせつつシステムの拡大に向けて試験運用を進めているという。経費清算などを行う職員向けのWebページやサイボウズをオフキャンパスで利用できるようになり、実際に利用している職員からは好評だという。長期出張中の教職員も、随時必要な情報にアクセスできるようになり、Webシステムの利用価値自体が向上しているという。現在はポータルアクセス機能を使って接続できる学内システムを順次増やし、今後学内全体に利用範囲を広げ、システムの利便性と教職員の生産性向上を目指していく予定だ。

大学内にはもともと各部署がおのの開発し、個別に管理しているWebサイト、アプリケーションが数十はあると見られており、これらを統一して管理できるID基盤が求められている。実際、ハード面での準備として2005年4月から学生証、職員証がICカード内蔵のものに刷新されており、ソフトウェアや学内の仕組みの対応を待つばかりとなっている。FirePassにはIDをグループごとに管理し、個別にアクセス可能な範囲を設定できる強力なグループ管理機能がある。管理権限を部分的に委譲することもできるため、現在の仕組みに近い分権型の管理も可能であり、複数部署をまたいだシステムを運用するための機能は整っている。アクセス権を失ったIDについても、OCSPプロトコルによりPKIの認証局から失効情報を即時に反映できる。「試験運用は非常に順調で、機能面でも安定稼働という観点でも満足しています」と語ったのは西村氏。その後、佐藤助教は学内の各サービスを運用しているシステム環境に差があり、クライアントとして利用される端末もWindows以外のものが多数あることを説明してくれながら、次のように語った。「マルチプラットフォームに対応しているので、教職員が使うすべての端末から利用できるのは安心です。システムの機能としての課題はすべてクリアになったので、後は制度面での調整ですね」

エンドポイントセキュリティ機能を活用し 今後は学内環境の認証も

オフキャンパスでの学内システム利用が定着したのちは、FirePassを活用し、セキュアな情報アクセス環境を学内においても構築していきたいと、助教たちは今後の展望を語ってくれた。特に興味を持っているのはエンドポイントセキュリティの機能のようだ。学内の共有スペースにキオスク端末を設置したいという要望があるが、そうした端末はいたずらや想定外の利用によってネットワークへのセキュリティリスクとなりがねない。そこで、誰もが利用できる端末からはFirePass経由でのみネットワークへの接続を許すようにし、エンドポイントセキュリティ機能によりログイン時に厳格なチェックを行ないたいのだという。大学という場でネットワークシステムの先駆者たちが選択したFirePassは、学内のあらゆる場所で活躍することになりそうだ。



F5製品に関するお問い合わせは F5 Networks Certified Partner

PKI製品に関するお問い合わせは

TechMatrix

テクマトリックス株式会社
ネットワークセキュリティ営業本部
ネットワークインテグレーション営業部
インターネットシステム営業課
TEL: 03-5792-8613 FAX: 03-5792-8713
E-mail: f5-info@techmatrix.co.jp
URL: http://www.techmatrix.co.jp



ペンティオ 株式会社
PKIソリューション事業部
〒160-0004 東京都新宿区四谷2-4 久保ビル3階
TEL: 03-5919-0971 FAX: 03-5919-0980
E-mail: sales@pentio.com
URL: http://www.pentio.com/