東京工業大学のEntrust効果

Entrust製品により、セキュアで利便性の高いキャンパス共通認証基盤を実現

東京工業大学は、「Entrust IdentityGuard」「Entrust GetAccess」「Entrust Authority」を活用することで、ICカード（PKI）、マトリクスコードにより認証強化されたWebシステムのシングルサインオン及びアクセスコントロールを実現した。

Case study

東京工業大学 講師
飯田 勝吉 氏

Webシステムごとに異なるIDやパスワードの一本化を目指す

1万人の学生と4千人の教職員に利用されている、東京工業大学の学内ポータルサイト（http://portal.titech.ac.jp）は、新しいWebシステムができるたびにIDとパスワードをユーザに告知する必要があった。また従来からのWebシステムについても、セキュリティポリシーに沿って定期的にパスワードを変更しなければならない。これらの通知は今まで学内便（紙による通知）で行っていたが、人数が多く、Webシステムごとのユーザ数も多いため、管理が困難になってきていた。ユーザの立場でも、Webシステムごとに異なるIDやパスワードを管理しなくてはならない上に、アクセスするURLも違う。URLがわからないためにWebシステムを利用しないというユーザも多かったという。

この状況を解決したのが、エントラストジャパンの認証セキュリティソリューションであった。ICカード（PKI）と、IDとパスワードに加えマトリクスコードを併用することで、シングルサインオンによるログインを可能にした。IDやパスワードの管理が容易になりユーザの利便性が向上しただけでなく、同時にセキュリティも高めていることが最大の特徴となっている。

具体的には、Entrust Authorityが発行した証明書をICカードに埋め込み、Entrust Identity-Guardが生成したマトリクスコードをICカード裏に印刷して配付している。利用環境により、各WebシステムにPKI認証もしくはマトリクスコード認証でアクセスが行われ、その際のシングルサインオンとアクセスコントロールがEntrust GetAccessにより実現されている。

Entrust製品を選んだ4つのポイント

サービスの選定は入札によって行われたが、「Entrust製品を選んだ決め手は複数あった」と、東京工業大学学術国際情報センターの飯田勝吉講師は語る。特に重要なポイントは、安全な認証環境を実現するために、IDとパスワードだけの認証から、ICカード（PKI）による認証を導入しようとした際、ICカード用のリーダを持っていない学生も多かったため、この対応としてマトリクスコードを使おうということになったが、Entrustは、これらすべてのソリューションを有し、シームレスな連携が容易だったことである。

2つ目のポイントは権限管理であった。学校は企業と違い、管理、運営がトップダウンではない。教授がたくさんおり、教授をトップとするシステムが複数存在しているため、一括管理が難しいという問題があった。Entrust GetAccessは、5階層までの構成が可能だったため、学術国際情報センターが第一階層を管理し、第二階層以下を学部、学科と振り分けることで、理想的なピラミッドが実現可能であった。

3つ目のポイントは、シングルサインオンの機能である。認証方法には「エージェント型」と「リバースプロキシ型」があり、東京工業大学では両方の認証方式を使用する予定であったが、Entrust GetAccessはこれらすべてに対応していた。

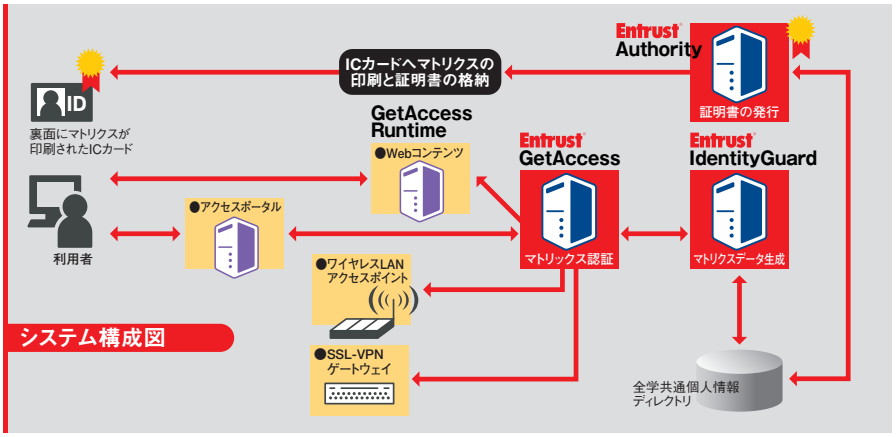
4つ目のポイントは、別の大学との連携認証であった。東京工業大学は、国立情報学研究所および7つの大学と連携しており、大学間での認証を行うプロジェクトに参画している。そこで有力

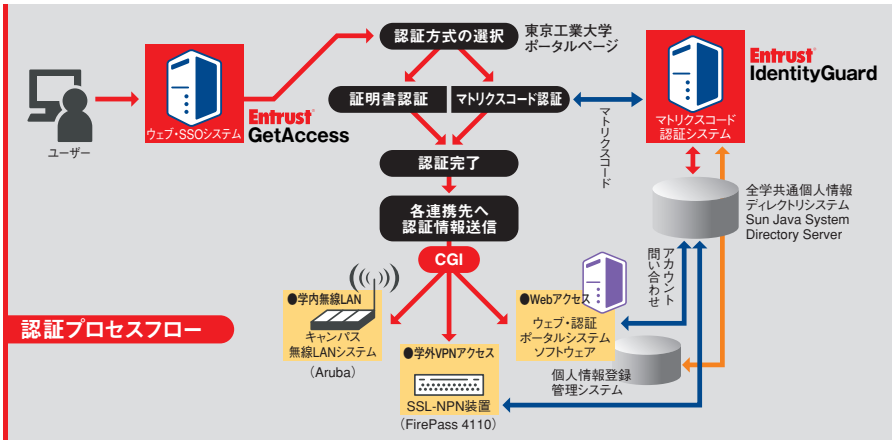
Profile

東京工業大学

1881年（明治14年）に東京職工学校として設立され、1929年（昭和4年）に東京工業大学に昇格。120年を超える伝統と歴史を持ち、現在も科学技術分野をリードする存在である。長期的な目標として“世界最高の理工系総合大学”を実現することを目指し、世界的に通じる人材の育成、世界に誇る知の創造、知の活用による社会貢献を重点的に推進。“21世紀COE（特に優れた研究教育拠点）プログラム”で合計12件のCOEを獲得する等、高い評価を受けている。学部生5,007名、大学院生5,054名（2005年5月現在）。

Entrust®
Securing Digital Identities & Information





な方法の一つが、XML技術の標準化団体であるOASISで定めたSAMLと呼ばれているプロトコルである。SAML 2.0では新たに大学間連携で注目されているID連携の仕様が追加されたが、Entrust GetAccessは最新バージョン2.0をいち早くサポートしていた。

これらの要因によって、エントラストジャパンの認証基盤強化ソリューションが選ばれたのである。しかし、導入の決定がなされたのは2005年の7月であり、エントラストジャパンに決定したのは12月27日であった。しかも2005年度中、つまり3月31日までに納入する必要があった。実質3ヶ月という極端な短期間での導入となったが、エントラストジャパンはこれをパートナーと協力してやってのけた。システム導入のスパンは一般的に短くなる傾向にあるが、3ヶ月というスパンは異例の短さである。これは、Entrust製品がパッケージ製品であるという点と、チューニングなどの手間が不要であることが大きな要因であったという。また、エントラストジャパンでは3万人から5万人規模のシステムをしばしば導入しているため、比較的スムーズに進行できたという。

Entrustの3製品が大学のシステムと柔軟に連携

システムの概要としては、Entrust Authorityによる認証局は学外にあり外部運用されている。学内には、まず認証の要となるLDAPサーバがあり、これに連動したWeb認証基盤としてEntrust GetAccessとマトリクス認証のEntrust IdentityGuardがある。これらはWebサーバとも連携している。

また、学外からのリモートアクセスに利用するSSL-VPN（F5 Networks FirePass）のユーザ認証や、すべての講義室からアクセス可能な無線LAN（Aruba Wireless Networks）のユーザ認証においてもEntrust GetAccessのユーザ認証と連携し、ネットワークアクセスの認証でもシングルサインオンを実現している。このほか、講義支援システムや財務管理システムなどとも連携している。

さらに、東京工業大学は4月3日よりNECやサン・マイクロシステムズなどと構築した、日本最速となるスーパーコンピューティング・グリッドシステム「TSUBAME（Tokyo-tech Supercomputer and UBiquitously Accessible Mass-storage Environment）」の稼動を開始しているが、TSUBAMEが装備する1.1ペタバイトのストレージに接続する際のWeb認証にもEntrust GetAccessと連携させることを検討しているという。

Entrust GetAccessはこのほか、東京工業大学が参画しているオンライン受講のTokyo Tech OCW（Open Course Ware）への採用や、学生の履修申告や成績確認が行える「教務情報システム」との接続も検討されているという。特に後者では、学生がEntrust GetAccessを使ってログインしないと学生生活が成り立たないようになるという。

ユーザの利便性を向上しつつ高いセキュリティを実現

東京工業大学では本システムの導入により、当初の問題をほぼ解消できたという。ユーザにとっては、IDとパスワードは一元化できたものの、マトリクスコードを常に携帯することになる。しかし、それについての不満は少ないという。また、Entrust IdentityGuardはJavaScriptに対応しているため、ブラウザに記憶させたり自動入力ができないようになっている。さらに、キーロガー対策としてマトリクスコードを参照して入力する文字は3つの英字とし、リロードを繰り返してリトライ攻撃が行われた場合には、入力を促すマトリクスコードの組み合わせは1種類に固定される。これにより、キーロガーによって入手したコードによって不正にログインされる危険性は非常に少なくなる。また、学生はしばしば部外者にIDとパスワードを教えてしまうことがあるが、マトリクスコードまで教えるのは心理的に抑制がかかるので、コードが流出する可能性も低いという。

ユーザの利用頻度は好調に伸びており、4月4日から5月17日までの間に64,133回のアクセスがあり、6,136人が利用した。導入以前のデータはないものの、このデータはかなり好調な数字だという。今後はゲストアカウントや携帯電話への対応、ユーザ個人のポータルサイトを動的なものにするといったEntrust GetAccessのリソースメニューのカスタマイズを考えている。エントラストジャパンと共同で開発していく部分も多くなるが、他の外資系ベンダーに比べ要望に対するレスポンスが早く、スムーズな開発が期待できるとしている。

Entrust®
Securing Digital Identities & Information

エントラストジャパン株式会社
〒101-0051 東京都千代田区神田神保町2-23 アセンド神保町ビル3F
Tel: 03-5211-8900（代表）
Fax: 03-5211-7810
URL: http://japan.entrust.com/
E-mail:japan.info@entrust.com