

# 総合研究大学院大学は、 なぜ、100人のユーザ環境において アイデンティティ管理システムを導入したのか・・・

情報システムの利用ユーザ数が100人程度と、一般の大学に比べて極めて少ない総合研究大学院大学(総研大)が、アイデンティティ管理(ID管理)システムを導入した。大学でのID管理システムの導入はこれまでも多くの事例が紹介されているが、その多くはIDの管理負荷軽減が目的である。小規模ユーザの環境においてID管理システムは有効であるのか、そのメリットとID管理のパッケージ製品であるLDAP Managerを導入した背景などを、葉山情報ネットワークセンターの 大田氏、洞田氏に詳細を聞いた。



国立大学法人  
**総合研究大学院大学**  
THE GRADUATE UNIVERSITY FOR ADVANCED STUDIES



葉山高等研究センター  
准教授・  
葉山情報ネットワーク  
センター長  
大田 竜也 氏

葉山情報ネットワーク  
センター  
助教  
洞田 慎一 氏

## ユーザプロフィール



国立大学法人  
**総合研究大学院大学**

<http://www.soken.ac.jp/>

本部 葉山キャンパス

〒240-0193

神奈川県三浦郡葉山町 (湘南国際村)

平成元年に設立された18の大学共同  
利用機関等を基盤とする大学院大学。

文化科学研究科

物理科学研究科

高エネルギー加速器科学研究科

複合科学研究科

生命科学研究所

先端科学研究科

## ユーザ環境を教えてください

総研大は、基礎学術分野の総合的発展と高度な研究的資質を備えた人材の育成を目指して、大学院学生の教育を行なうために1988年に設立されました。現在では、葉山キャンパスを大学本部として、各地に置かれた18の学術研究機関等を基盤として、大学院生を分散配置し、ユニークな博士課程教育を展開しています。その結果、学生を含め、職員、教員は他の機関に分散しており、葉山キャンパスでのネットワークの常時利用は100名程度のユーザとなります。

## ID管理システム導入の目的は？

ユーザ数が100名程度と少なく、人手によるIDの管理も不可能ではありませんでした。しかし、大学のセキュリティポリシーから、IDの的確な付与や確実な管理が必要不可欠なものであることを認識するに至りました。さらに現時点では、IDや台帳の管理がシステムごとに分散してしまった結果、整合性がとりづらくなっており、ID管理により管理負荷が上がってしまうことを危惧していました。

そこで、葉山キャンパスにアカウントDBを保持して、IDを体系的に管理することが必要であると判断しました。現状では連携するシステムも決して多くはない状況ですが、今後システムが増えたら検討するよりもシステム数の限ら

れた今のうちにID管理基盤を構築することで、より柔軟なシステムが構築できると判断したからです。

また、ID管理システムの導入と同時に、ネットワーク利用時の利用申請のプロセスの確立がもう一つの目的でした。これまでは、利用申請は曖昧な運用の基に行っていました。逆に利用者へのサービス提供の遅延や、説明の不足につながっており、かえって管理負荷を上昇させていました。

そこで、利用申請に関するフロー全体を抜本的に再構築する目的で、連携システムの少ない状況で、ID管理システムの構築を開始しようと考えたからです。

## LDAP Managerを選定した理由

製品選定では、基盤システムという位置づけにより自由度が要求されることから、LDAPをベースとする製品とすることにしました。

しかし、LDAPサーバ単体の構築だけではなく、IDの追加や削除、変更に関してどのように管理するのか、そのインターフェースをどのように作り込めばよいのかが重要で、その作り方によっては将来的に使えないものとなってしまいます。

汎用的なLDAPエディターでは、入力者の負荷を軽減できないため、入力インターフェースのカスタマイズや、項目、スキーマの対応関係の整理、項目値へのマクロ機能、データの入力方法といった、LDAPレポジトリの操作や制御の可能な

ものを想定していました。

そこで、LDAP サーバの制御できるパッケージ製品を含め導入することに決め、機能面、価格面から最終的に、国内メーカーであるエクシエン・ネットワークス社の LDAP Manager を採用しました。

### ID 管理システムの構成

現状では、連携先システムとして無線・有線 LAN の認証ネットワークのみを連携させて試験的にスタートしています。LDAP Manager から連携した LDAP サーバは負荷分散装置による冗長構成をとり、Radius サーバは LDAP サーバの VIP (仮想 IP アドレス) 宛に参照を行います。

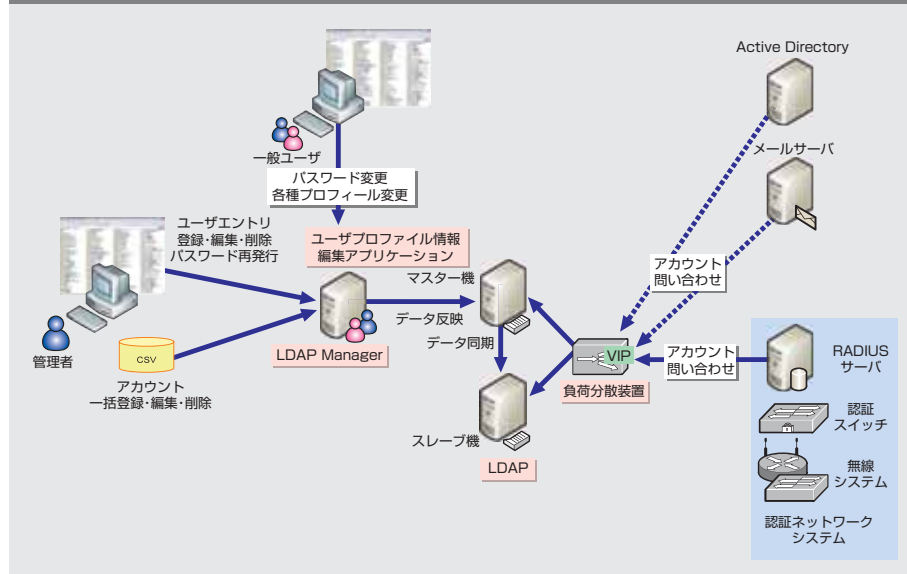
認証ネットワークでは MAC アドレスを組み合わせ、Radius サーバでの認証を行っており、ユーザ数は 100 名ですが利用端末が 300 台程あります。LDAP サーバでは、Radius サーバでの認証に必要な ID やパスワードを格納します。

Radius クライアントの仕様に合わせ、項目値のカスタマイズや、スキーマの追加といったレポジトリ管理、ID の一括登録・編集・削除やパスワード再発行は管理 GUI から容易に行え、各システムの構成変更にも柔軟に対応できます。

### 構築期間は何ヶ月でしょうか

今回の ID 管理システムの導入には 2 ヶ月の期間を要しましたが、ID の利用申請プロセスの確立と認証ネットワークの構築を同時に行ったため、認証ネットワーク側の仕様を確認しながらの作業となりましたので、実質的には 1 ヶ月程度の構築と考えられます。

### 総研大 ID管理システム構成図



### 導入のメリット

導入のメリットとしては、特に ID 管理の基盤を手に入れたことで将来的にシステムが増加したとしてもセキュリティポリシーに合致した管理が可能になったことと ID の申請プロセスが確立できた点が挙げられます。

また、連携先システムとの LDAP のスキーマ (属性情報) の紐付け (マッピング) も GUI から、項目名の関連付けにより容易に設定可能であることもメリットと感じています。更に、LDAP Manager のログによる ID に関する証跡管理も大きなメリットといえます。

### 将来的な拡張

今後は、メールや Active Directory との連携を予定しています。特に、事務局では利用する C/S のアプリケーションが多く財務、学務、図書、e-ラーニングなど複数の

ID を利用しているユーザもおります。これには SSO の導入を検討しており、この SSO システムも ID 管理システムに連携するべきと考えます。更に、将来的には、学生が配置されている研究機関と ID 管理基盤を連携することも視野に入れています。

### アクシオとの付き合い

今回、アクシオとは初めてのお付き合いとなります。「アイデンティティ管理」、「ID 管理」などのキーワードによるインターネット検索を行ったのがきっかけです。リストアップした数社の製品を検討し、その中から最終的にアイデンティティ管理において実績のあるアクシオのソリューションを採用することになりました。今後も認証、ディレクトリ、LDAP などに関する情報提供に期待しています。また、連携システムの拡張時には意見を伺わせて頂きたいと思います。

**貴重なご意見ありがとうございました。**

\*記載された内容は予告なしに変更する場合があります。\*掲載の社名、製品名は一般に各社の商標、登録商標です。