採用会社、所属部署、職階などに基づき シングルサインオンとアクセス制御を実現

旭化成工業では全社共通情報システムに、日本エンコマースの「getAccess」を認証システムとして導入し、シングルサインオンを実現した。同社と関連会社の従業員約3万人が、各人の電子メールIDでログインするだけで、アクセスを許可されたすべてのWebサーバーを利用できる。アクセス制御は人事データベースを基に作られた役割(ロール)リストによって、一元的に運用管理される非常に効率的なシステムである。

旭化成情報システム株式会社技術企画室主査
常盤 正樹 氏

旭化成情報システム株式会社技術企画室主査
天沼 宏幸 氏

旭化成工業では、1994年頃から各部門ごとにITソリューションの導入が進められ、さまざまな情報システムが使われるようになった。同社と関連会社あわせて3万人の従業員に対してPCもほぼ1人1台という体制を実現し、これによって、部門ごとでの生産性の向上は進んだ。しかし、複数システムを併用する際のIDとパスワードの管理が大きな問題となってきた。エンドユーザーにとっては、接続ごとにいちいちIDとパスワードを入力するのは非常に煩雑な作業になる。管理者にとっては、組織改編や人事異動のたびに、複数のシステムに対して行わなければならないアクセス権の変更作業や、IDとパスワードの管理が大きな負担になっていた。

そこで、同社では、グループ全体としての情報システム基盤の整備を行ない、そこにシングルサインオンの環境を実現することを決定した。そして、一元管理されるユーザー情報をもとにシングルサインオンを実現するために導入されたのが日本エンコマースの「getAccess」である。

旭化成グループの情報システムの企画・支援を担当している旭化成情報システム技術企画室主査の常盤正樹氏は「クライアント・サーバー・システムからブラウザをベースとしたシンクライアント・システムへと切り替え、ユーザー環境の統一、管理の集中とともに、IDやパスワードなどの共通利用可能なデータの一元管理を狙いました」とその背景を語る。

従業員の役割をベースに「getAccess」でアクセス権限を制御

旭化成工業では旭化成工業本体の社員だけでなく、関連会社の社員も同じシステムを使用する。そこで、採用会社、所属部署、職階、地区などによって従業員の役割(ロール)を決め、このロールを使ってシステムへのアクセス権限を管理しようと考えた。人事や総務部門と協力して調べたところ、このロールはあわせて数万種類に登ることが分かった。そこで、このような複雑なアクセス権のコントロールを行える製品の調査を行ったところ、もっとも同社に適しているソリューションとして浮上してきたのが「getAccess」だった。

製品選定の要件として、1.URLに基づいたアクセス制御を行っており、Webブラウザを用いたシンクライアント・システムと適合性が良いこと、2.クライアントには何もインストールする必要がないこと、3.サーバーOSやWebサーバー・プログラムに柔軟に対応すること、などを同社は考えていたが、「getAccess」はこれらの条件を満たしており、またコスト的にもリーズナブルな製品だったのである。

旭化成情報システム技術企画室主査の天沼宏幸氏は「proxyサーバーを設けるようなものは負荷の集中の問題があり、クライアントにソフトが必要なものはその管理の手間とコストが大変になってしまいます。その点、getAccessはアクセス・サーバーと認証サーバーを使ったシンプルな構造で、合理的にアクセス管理が実現できると思いました」とその事情を説明する。

電子メールIDを基にユーザーを判別 Cookieでユーザーのマシンに渡す

旭化成工業では、約3ヶ月で「getAccess」の導入を決定したのち、社員のロールの洗い出し、アクセス権限のモデリングなどシステムのデザインに半年をかけて、細部を詰めた。そして、99年5月から「getAccess」によるシングルサインオン・システムの運用を開始した(図1)。「システムの設計に十分な時間をかけたおかげで、トラブルもなく、順調に稼動しました」(常盤氏)という。

同社の認証システムは、図1に示すような手順で認証を行なう。まず、ユーザーは社員それぞれの持つユーザーIDとパスワードでアクセスサーバーにログインする。旭化成工業の場合、このユーザーIDとしては既に全社員が持っている電子メールのIDを利用している。アクセスサーバーは認証サーバーに問い合わせ、そのIDの持つロールに対応したアクセス可能なURLリストを受け取り、これを暗号化されたCookieとして、ユーザーのブラウザに送る。これによって、アクセス可能なWebサーバーが自動的に区別できるようになるわけである。

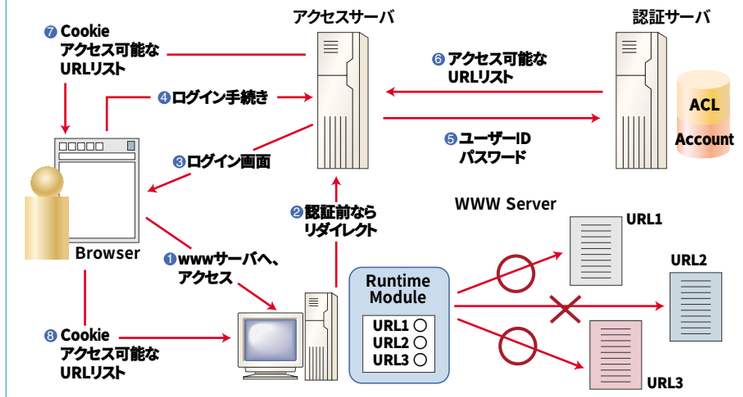
人事データベースから 30分以内にアクセス制御データへ

認証サーバーの持つ「getAccess」用のロール・データは、関連社員も含めた3万人分の人事データベースを基に中間データベースを作成し、そこから毎月新規のロール・データを作成する。中間データベースを作るのは、人事データベースや「getAccess」側にシステム変更があっても柔軟に対応できるようにするためである。

同社では毎月16日づけで異動が実施されるので、このときが更新のタイミングであるが、現在のところ業務引き継ぎなどのための移行期間として異動前のロールも1ヵ月間は有効になっている。電子メールIDとパスワードは、電子メール・サーバーから認証サーバーに引き渡され、毎日更新される。

人事データから「getAccess」用データへの変換は、1回の作業あたり30分以内で終了、IDの更新も自動的に行える。したがって、IDとパスワードの管理のコストと時間、管理者の負担は、シングルサインオン実現以前に比較して大きく減らすことができた。

図1　旭化成工業の「getAccess」によるユーザー認証のしくみ



認証用インフラとしては一段落 今後は“草の根”Webなどへの対応を

99年5月の認証システム利用開始当初は、「getAccess」によってアクセス制御を行っているWebサーバーは1つだけだった。しかし、現在では旭化成グループのシステム内で、大小とりまぜて約60のWebサーバーのアクセス制御を行っている。このため、アクセス可能なサーバーを示すURLのリストが大きくなり、最近ではCookieの容量が2kバイトを超えるようになってきたという。このため規格に沿ったCookie対応をしていないWebアプリケーションでは、認証がされないという珍しいトラブルも発生したが、送付する暗号化されたCookieに処理を加えることで現在では問題なく運用されている。

現在、旭化成工業では、シングルサインオン環境が当然のものとして一般社員に使われている状況である。「全社規模の主要なWebサーバーへの対応はほとんど完了しました。今後は新規システムや、“草の根”Webサーバーなどへの対応が多くなるでしょう」と常盤氏は語る。“草の根”Webサーバーとは、部門や新規計画などのプロジェクトごとに個別に作られるWebサーバーのことで、NTサーバーが簡単に立てられることから、こうしたWebサーバーが増えている」という。「日常的にシングルサインオンの便利さを実感しているので、こうした独自サーバーもgetAccessでアクセス制御したいというニーズが増えている」(常盤氏)のである。

旭化成工業としては、今後は「ディレクトリ・サービス技術の進展を見ながら、認証システムにこれを取り入れた形へと進化させていきたいと考えている」(天沼氏)という。また、ECやEIP(Enterprise Information Portal)などについても「getAccess」のアクセス制御機能を利用して実現していけないか、さまざまな検討を始めており、日本エンコマースにも引き続きサポートや情報提供を期待しているという。

お問い合わせ

日本エンコマース株式会社
〒102-0093 東京都千代田区平河町2-10-10
ハイックス平河町2階
TEL 03-3556-8041 FAX 03-3556-8334
URL http://www.encommerce-jp.com

会社プロフィール

旭化成工業株式会社

代表取締役社長：山本　一元
本　社：〒530-8205大阪市北区堂島浜1-2-6
資本金：1033億円
従業員：1万2808名
主な業務：化成品・樹脂、繊維、住宅、医薬品、電子材料など化学技術をベースにした製品を市場に提供している。2001年1月からは社名を「旭化成」に変更し、ネットビジネスなど新たな事業展開を行っていく方針である。