

日産ディーゼル工業 ID管理／SSO認証基盤で セキュリティの向上とコスト削減を両立

日産ディーゼル工業は、新しい部品表システムの導入とともに、ユーザー情報管理の足固めとなる基盤構築の第一ステップとして、アイデンティティ管理とSSO（シングルサインオン）システムによる自社のIT環境を整備。このID管理基盤に対しては、セキュリティの向上とともにJ-SOX法をにらんだ内部統制強化としての重要な礎となることが期待される。更に、アカウントメンテナンスにかかるコストが将来的には1人／月分程度削減されると試算する。

UD 日産ディーゼル

日産ディーゼル工業株式会社
情報システム企画部



課長
須藤 眞彦 氏

株式会社システムプレーン
アウトソーシング事業部



白井 直樹 氏

ユーザプロフィール

日産ディーゼル工業株式会社

<http://www.nissandiesel.co.jp/>



【所在地】 埼玉県上尾市

【創業】 1935年

【資本金】 385億9712万円

【従業員数】 2858名

【事業内容】 大型／中型／小型トラック、バス、ディーゼルエンジン、自動車用部品の製造・販売など

新しい部品表システムの開発と ID管理／SSO認証基盤の構築

日産ディーゼル工業は、50社以上のグループ会社を有し、トラック・バスや、ディーゼルエンジン、自動車部品などの製造・販売を中心として、ワールドワイドな展開を図る自動車メーカーである。同社は「Ultimate Dependability」(UD：究極の信頼)という長期ビジョンを掲げ、経営や技術の革新に日夜努力を続けてきた。製造部門から技術・開発部門まで、ITテクノロジーを積極的に取り入れ、これらのノウハウを製品開発や製造技術に織り込んでいる。

同社では、従来からホストコンピュータ/UNIX/Windows系のプラットフォーム上で、人事・経理といった一般的な業務から、製造業として必要な設計、生産、販売に至る様々なアプリケーションを稼働させていた。しかし、その一方で、これらアプリケーションのユーザー情報がシステムごとに個別に管理されていたため、ID管理のメンテナンスに掛かる工数やコストが大きな課題として残されていた。退職時のアカウント処理や、共有アカウントなども含め、これらの問題を解決するために新しいID管理や認証基盤の導入検討を2003年より着手した。日産ディーゼル工業 情報システム企画部の須藤眞彦氏は、新基盤構築の経緯について次のように述べる。

「新しい部品表システムを構築するために、社内プロジェクトが立ち上がったことが大きな契機となりました。関係会社である日産自動車が開発していた部品表システムをベースに、トラック用の新システムを導入することになったのですが、そのシステムを使う際に“利用者認証”が必須の要件となっていました。そのため、ID管理の整備やSSO環境の基盤構築が新部品表プロジェクトと同時に始まりました」

新基盤の構築は、ディレクトリまわりの技術に強いという理由からアクシオが担当することとなり、システムの開発・運用・保守については、日産ディーゼル工業の情報システム部

門の一部が分社・独立したシステムプレーンが担当することになった。システムプレーンの白井直樹氏は、構築前の要件定義や基盤構築への準備に関して次のように説明する。「今回のケースでは、新部品表システムについてお手本となる日産自動車の先例がありました。そのため、個々に持っているユーザー情報を統合するためのノウハウがあり、比較的スムーズに導入の準備ができたと思います」

2004年9月には本件の導入が終了し、利用者認証基盤として運用が開始された。

基盤構築の第一ステップとして、 低価格なLDAP Managerを導入

同社のID管理・認証基盤システムの構成を図1に示す。「ユーザー情報管理サーバ」「LDAPサーバ」「認証サーバ」「リバースプロキシサーバ」という4システムから構成される。現在のところ利用できるWebシステムは、前述の新品表システムのほかに、新車の原価管理システム、開発時に必要な法規情報の参照システム、サプライヤーに対する生産・購買などの情報提供システム（現在開発中）である。

ID管理のキーポイントとなるユーザー情報管理サーバは、人事マスターからの人事情報を取り込み、認証に利用するユーザー情報を整形した形で一元的にデータを管理している。新品表などのWebシステムは、社内だけでなく、外部のサプライヤーや関連会社でも利用される。外部情報は人事マスター側で管理していないため、現状ではマニュアルで登録・変更・削除が行われている。

これらのデータをLDAPサーバ側に蓄積し、認証サーバと連携することで、各種Webシステムをユーザーごとの権限に応じて利用できる仕組みだ。また、セキュリティの観点から、サプライヤーや関連会社からの外部アクセスについては、リバースプロキシサーバを介して中継する方式を採用している。

中核となる具体的な製品を見てみよう。ID管理を行うユーザー情報管理サーバ側には、

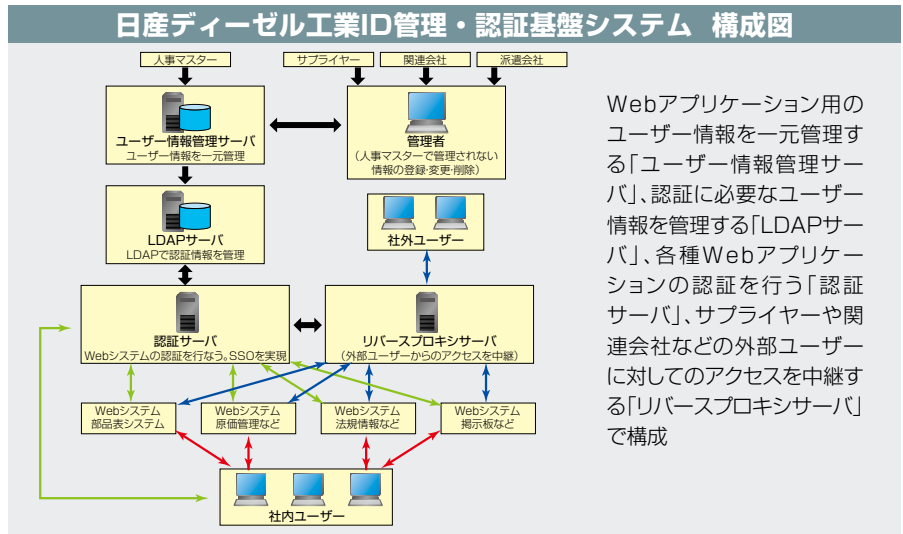
エクスジェネットワークスの「LDAP Manager」が採用されている。LDAP ManagerをID管理製品として選定した理由について、須藤氏は次のように語る。「ID管理の第一ステップにおいて、まずユーザー情報を一元管理できるシステムを低コストで構築できる点に着目しました。そこから必要であれば、LDAPや、Notes、Active Directoryなどに連携させようと考えました。そして、まずLDAPを手始めに連携させることになり、データソースを投入する手段として、このLDAP Managerを採用することになったわけです。したがって現状では、CSV形式のファイルからLDAPに連携させる機能のみを利用しています」

LDAP Managerは、CSV形式のファイルを介し、ユーザー情報データベース (Oracle) とLDAPサーバ側 (SUN ONE Directory Server) のユーザー/グループ情報を直接連携させながら、タイムリーなメンテナンスを実現する。必要に応じて連携先のモジュールをプラグインとして追加購入できるため、システム構築要件によっては他社製品と比べて、低コストでID管理基盤を構築できるメリットがある。

また、認証サーバ側には、ブランドの信頼感や実績を考慮して、RSAの「ClearTrust」を導入し、煩雑なパスワード管理を解消するSSO (シングルサインオン) の基盤づくりに一役買っている。ClearTrustは、「スマートルール」といった先進的な機能を備えている。静的または動的なユーザープロファイルに基づいて、Webへのアクセス/ユーザー権限に関するポリシーを組織や属性単位で定義でき、大きな組織変更や人事異動に伴う対応も容易に行える。

将来的には LDAP 未対応の様々な既存システムについても適用を拡大

新しい基盤が導入されてから、2年弱が経過した日産ディーゼルだが、実際にどのような効果もたらされたのだろうか。須藤氏は「社内のユーザー情報に関しては、人事マスターとの連携が可能になったため、最新データを



Webアプリケーション用のユーザー情報を一元管理する「ユーザー情報管理サーバ」、認証に必要なユーザー情報を管理する「LDAPサーバ」、各種Webアプリケーションの認証を行う「認証サーバ」、サプライヤーや関連会社などの外部ユーザーに対するアクセスを中継する「リバースプロキシサーバ」で構成

常に更新できる環境が整い、退職者が出てデータ削除の取りこぼしがなくなりました。データの精度が上がり、その結果としてセキュリティも向上しています。またメンテナンスに掛かっていたコストも下がりました」と、導入の効果について説明する。

「とはいえ、今後さらに大きな効果を得るためには、まだ実現できていないLotus Notes/DominoやWindowsアカウントの連携まで行う必要があると感じています」(須藤氏)

LDAP Managerには、Lotus Notes/DominoやActive Directoryなどの連携モジュールもオプションとして用意されている。システムブレーンの臼井氏は、「これらの連携も実現できれば、人事異動などの改変時期に、1人/月分程度のコスト削減が期待できる」と試算する。

今後は、このようなLDAP未対応システムについての連携も進めていく予定だという。ただし現時点では、具体的なスケジュールについては見えない部分もある。Notesは独自にカスタマイズされた部分もあり、ID連携をするためには、まずその整備を行う必要があるからだ。現在すでに稼働しているシステムをすぐに改変するのではなく、次のシステム更改のタイミングに合わせて、これらを認証基盤に集約していく予定だ。また、社員以外の外部サプライヤーなどのユーザー情報をサプライヤーが直接登録・変更できるようにしたり、

各アプリケーションシステムの権限付与を自動化できるようなワークフローの仕組みなども考えていきたいという。

従来、ID管理といえば、業務管理の効率やコストに対する効果について論じられることが多かった。しかし、最近ではセキュリティやJ-SOX法をいらんだ内部統制の強化のために、まず始めに整えておくべき重要な礎としてフォーカスが当てられている。この点について、須藤氏は次のような感想を述べる。

「セキュリティ面でいうと、ID管理は然るべき人が正当な権限で利用していることを保証する最もベーシックで重要な技術だと考えます。誰がどんなことをしているのかログとして残していても、それが本当に本人であるのかわからなければ意味のないものになってしまうからです。J-SOX法への対応を考えた場合も、ID管理は大変重要であると考えています」

礎がしっかりしていなければ、その上にいくらセキュリティ対策を積み上げたとしても、それは「砂上の楼閣」になってしまう恐れがある。同社では、まずID管理基盤の構築によって、しっかりと足元を固めていき、さらに1つひとつの技術を積み上げていくことで、将来にわたり万全なIT環境を整備していく方針だ。

*本内容は、2006年6月20日にITmedia エンタープライズオンラインムック (<http://www.itmedia.co.jp/enterprise/>)に掲載された内容です。

*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。