

# 6000ユーザに30以上のシステムを提供するには ひとつ上のID管理を目指す必要があった

システム毎に分散管理されていたIDのセキュリティ対策が課題となっていた総合化学メーカーの東ソー。同社では、その課題に対してIDを統合的に管理するID管理システムを2007年10月に導入した。これにより、ID管理に対するセキュリティの向上と業務効率の改善が図られ、今後の東ソーグループにおける新たなIT戦略の推進が可能となった。

## 東ソー情報システム株式会社

システムサービス事業部



ネットワークグループリーダー  
岡 幸一氏



内田 和哉氏

### ユーザプロフィール



東ソー株式会社 南陽事業所



## 東ソー株式会社

TOSOH

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

本社所在地 東京都港区芝三丁目8番2号

設立 1935年2月11日

資本金 406億円 (2008年3月末現在)

従業員数 [連結] 11,088人

(2008年3月末現在)

事業内容

単一工場としては日本最大規模となる南陽事業所を有する総合化学メーカー

[基礎原料事業] 化学品、セメント

[石油化学事業] オレフィン、ポリマー

[機能商品事業] 有機化成品、バイオサイエンス、機能材料、電子材料

## 東ソー情報システム株式会社

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

本社所在地 東京都港区芝2丁目5番10号

芝公園NDビル

設立 2000年1月11日

事業内容

東ソー株式会社およびグループ会社に対して情報システムサービスを提供する

・ビジネスソリューションサービス

・システムマネジメントサービス

・システムコンサルティングサービス

・プロダクト提供サービス

### ID管理に係る脆弱性

本システムの導入を担当した東ソー情報システムのシステムサービス事業部では、国内の東ソーグループ26社、6000ユーザに対して、ASPサービス、ネットワークサービスと運用管理サービスをワンストップソリューションとして提供している。

提供する30以上のシステムで利用されるIDは、東京、南陽、四日市の各事業所のシステム担当者により管理されていた。申請情報により手作業で行うID管理は管理負荷が大きいためだけでなく、IDの登録・変更・削除における作業ミスの危険性が考えられた。また、システム単位で存在するIDを覚えられず、メモ書きして運用するユーザもあり、これら管理者とユーザにおけるIDの煩雑な管理に起因するセキュリティが以前から危惧されていた。そこで、東ソー情報システムでは、人事情報に基づいたポリシーを動的に各システムのIDに反映する統合ID管理システムとシングルサインオン (SSO) の導入を決定した。

### ひとつ上のID管理に対応した製品を選択

ID管理を実現するための製品の選定に関して、本システム導入の責任者である東ソー情報システム ネットワーク・グループリーダー 岡 幸一氏は次のように紹介する。「ユーザが追加や削除された場合に、ユーザ情報を配信するだけの安価なパッケージ製品も存在した。しかし、ID管理に係るセキュリティの向上を目的としたため、単純なID情報の連携だけでは満足できなかった。一元管理したポリシーをいかに柔軟に各システムのID情報として反映できるのかという点に重点をおいて、ひとつ上のID管理を目指した製品選定を行いました。」

「例えば、新入社員が入社した場合に、配属部署などの情報は人事システムから反映することができませんが、IDに関してその人のWindowsログインスクリプトの設定や権限が自動的に反映されないのであれば、結局手作

業で設定することとなり作業ミスを招く恐れがあるのです。」とシステムサービス事業部 内田 和哉氏は続けた。

そこで、最終的に国内での導入実績も考慮した結果、Novell Identity Manager (NIM) とSSOとしてRSA Access Managerを採用した。

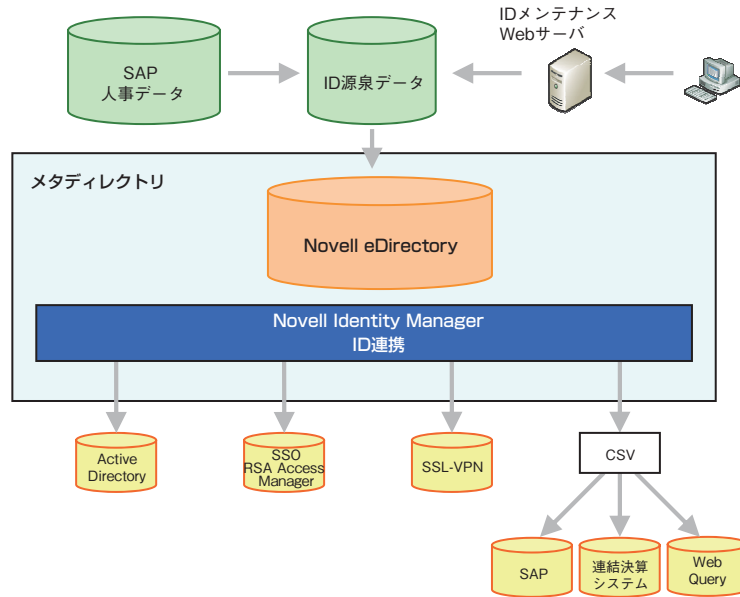
### 設計・構築に2年を要した。その理由は…SAPの導入

「導入には連携する人事システムやActiveDirectory (AD)の導入の影響もあり、これらシステムとの調整に苦労した。」と岡氏は振り返る。ID管理システムの導入計画の直後に、人事システムとしてSAPの導入が決定したのだ。

これが今回のID管理システムの導入に大きな影響を与えることとなった。ID管理システムでは、人事情報を源泉として他システムへポリティシーに基づいたID情報を配信する。源泉データとなるSAPのインターフェース部分の仕様が決定するまで設計に入ることができず、運用開始まで2年の期間を必要とした。

また、Windows NT4.0からAD統合化によりPCのプロファイルの移行作業を行ったばかりであったが、ID管理システムから新たなID情報をADに連携すると、再度プロファイルの変更が必要となるという問題が生じた。再度のプロファイル変更作業の実施は許されなため、AD管理者によるこのID情報のギャップを埋めるためのコンバート作業が必要となった。

「更に、東ソー社員である4200名の情報は、ID管理システムに対して自動入力されるが、関連会社の2000ユーザの情報は、紙データからの手作業による入力を与儀なくされた。これには、ID管理チームを編成して入力対応したが、一時的ではあったが大変だった。」と内田氏は運用開始までの苦労を紹介する。現在は、WebベースのID申請用のワークフローを作成しこのような対応は不要となっている。

**東ソー「ID管理システム」構成図**

**ID管理システムが他システムの基盤となる**

図のように源泉とする人事情報からID管理システムに対して、異動や退職といった人事イベントの情報を投入し、その情報を基に各システムにID情報が連携される構成である。ここでNIMの前端にID源泉情報の精査と連携のタイミング調整を目的としたDBが配置される。管理者によるIDのメンテナンスもこのDBを通して行われることとなる。

連携システムとしては、AD、SSL-VPN、SSOが直接連携し、連結決算システムにはCSV連携する構成とした。

「今後もサービスしているシステムをこのID管理システムへ連携していく方向で考えている。」(岡氏)とのことで、将来的にもこのID管理システムが各システムの基盤として運用されていく予定である。

**SAPの権限付与や内部統制対応にも**

これまで各システム管理者に任せていたID管理は、ユーザ毎の人事イベントに連携してタイムリーに反映できることとなり、人為的な作業もなくなったことでセキュリティは確実に向上し、管理負荷も大幅に軽減された。

特に、SAPでの細かな権限付与に関しても、本システムに連携することで容易に行うことが可能であった。

導入計画時には、日本版SOX法に対してどこまで対応する必要があるのか判断できない状況であったが、セキュリティ対策として管理者の特権IDも含めたIDの一元管理を可能としたことで、現在では内部統制対応に大きく貢献している。監査時に各システムへのアクセス権の正確性を証明することも容易となった。

**アクシオの対応について**

「特に今回のシステム導入では、並行してSAP導入などの大きな外的要因に対して、自分達と同じ立場に立って対応してもらうことで乗り越えることができたと感じています。最後まで対応してもらい非常に助かりました。」(岡氏)と笑顔でお答えいただき、アクシオのスローガンである“Standing on your Viewpoint”を実感した。

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。

# 株式会社アクシオ

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

- 本 社 / 〒105-0001 東京都港区虎ノ門1-1-18 東京虎ノ門ビル5F  
TEL:03-5501-0940 FAX:03-5501-0954
- 大阪営業所 / 〒530-0004 大阪府大阪市北区堂島浜1-4-16 アクア堂島西館6F  
TEL:06-6341-0940 FAX:06-6341-0965
- 東海村営業所 / 〒311-0103 茨城県那珂市横堀851-12  
TEL:029-353-0940 FAX:029-353-0941
- データセンター / 神奈川県川崎市、相模原市