NetIQ Active Directory管理ツール

「Directory and Resource Administrator(DRA)」導入事例

スミセイ情報システム株式会社

DRAによりActive Directoryの本格的な管理、運用を実現
権限委任と監査ログ、バッチ処理による効率化がポイントに

内部統制のさらなる強化が求められる中、Active Directoryの本格的な管理、運用への関心が高まっている。住友生命グループの情報システム会社、スミセイ情報システムでも同様の問題意識を持っていた。金融分野を中心に、さまざまな企業にトータルなITソリューションを提供する同社では、3年前、セキュリティの視点からITインフラの抜本的な見直しを実施。その一環として懸案となっていた権限委任と統制強化の両立を図るべく、NetIQのActive Directory管理ツール「Directory and Resource Administrator(DRA)」を導入した。Active Directoryの一元的な管理、運用を可能にし、案件別の権限委任や監査ログの記録、バッチ処理による効率化を実現。同社の信頼を支えるセキュリティ基盤の強化に大いに貢献している。

権限委任と統制強化という矛盾の解決へ

企業における情報漏洩のトラブルが後を絶たない。ハッキングやコンピュータウイルスなど社外からの攻撃よりも社内の人間による不正行為や操作ミスといった内部に起因するケースが増えている点が近年の傾向だ。情報活用を促進する一方で、統制の強化を図らなければならないという矛盾が根本的な問題として横たわっている。「市場が大きく変化する中、競争力を高めるために現場での迅速な情報活用は不可欠です。権限設定の自由度をある程度、現場に持たせるために権限委任をしないと、仕事はスムーズに動きません。しかし、一方で統制もしなければならない。非常にジレンマがありました」と、スミセイ情報システムの総務部担当部長 藤田尚孝氏は語る。

スミセイ情報システムは、住友生命グループの情報システム会社だ。金融分野で培った技術とノウハウをベースにさまざまな業種の企業に対し、システムコンサルティングから設計、開発、保守、運用管理までトータルソリューションを提供。IT技術を通じて企業の経営課題を解決していくプロ集団としての実力は、売上高比率の50%近くが住友生命以外という数字が証明している。

同社の強みは何といっても高度な技術が求められる金融分野で蓄積してきた豊富な経験と実績だ。金融系に企業としてのアイデンティティを持つ同社にとって、個人情報保護などセキュリティへの取り組みは最優先課題となる。3年前、1年間をかけてセキュリティの視点からITインフラを抜本的に見直したのも、そうした同社の企業姿勢の表れだ。その中で、重要なテーマの1つとなったのが権限委任と統制強化の問題だ。解決へのポイントは、Windowsネットワークのディレクトリサービス Active Directoryをいかに管理、運用していくか。

Active Directoryを上手く活用することでセキュリティのさらなる向上が図れる。

Active Directoryの一元的な管理、運用を実現するDRA

「従来、Active Directoryの管理は開発案件ごとに対応する必要もあって本部単位で行っていました。全社での一元管理はずっと実現したいと考えていましたが、膨大な手間と時間がかかることから運用がついていけない。断念せざるを得ない状況でした」(藤田氏)。

本部単位でActive Directoryを管理していると、どうしてもバラツキがでてくる。全社的にセキュリティのレベルを上げるためには、Active Directoryの一元的な管理、運用が不可欠だった。また、部門間を横串で連携する案件も増えてきており、Active Directoryの管理も複雑化していた。

こうした課題を解決しようとするとActive Directoryの限界に突き当たる。たとえば、OU(Organization Unit、組織単位)レベルではなく、案件単位で横断的にチームをつくったり、役職ではなく案件上のリーダーに権限を与えたり、ある一定期間だけ兼務するケースなど、対象範囲と委任先を柔軟に定義することはActive Directoryでは困難だ。

インターネットでNetIQのActive Directory管理ツール「Directory and Resource Administrator(DRA)」の記事を見たとき、藤田氏は「これなら使えるかもしれない」と直感した。同じ頃、偶然にも同社インフラソリューション本部のメンバーもDRAの存在を知り、同様の思いを抱いていたという。

DRAを導入した理由について、インフラソリューション本部インフラソリューション部 部長 前川義信氏はこう話す。「大きく3つのポイントがありました。1つは、権限委任が容易かつ柔軟にできること。一般部門とは



総務部
担当部長
藤田 尚孝 氏

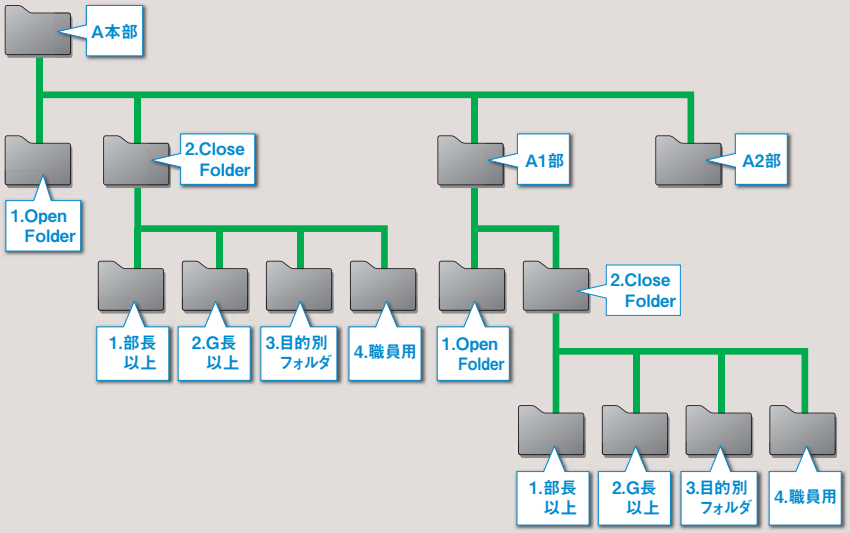


インフラソリューション本部
インフラソリューション部 部長
前川 義信 氏



総務部
河原 由美香 氏

全社ファイルサーバのフォルダ構成



「1.OpenFolder」は、該当本部、または部の所属グループのみに所属しているメンバ（他組織者グループには所属してない）にアクセス/更新可能な権限を付与しています。

「2.CloseFolder」は、該当本部、または部の所属グループ配下のメンバに読み取り権限のみ付与しています。

「1.部長以上」フォルダは、該当本部、または部の部長以上グループ配下のメンバにのみアクセス/更新可能な権限を付与しています。

「2.G長以上」フォルダは、該当部のG（＝グループ）長以上グループ配下のメンバにのみアクセス/更新可能な権限を付与しています。

「3.目的別フォルダ」は、該当本部、または部の所属グループ配下のメンバに読み取り権限のみ付与し、部長以上グループ配下のメンバにはアクセス/更新可能な権限を付与しています。管理者グループ配下のメンバにはフルコントロールを付与しており、個別に作成したセキュリティグループによるフォルダ単位でのアクセス管理を可能としています。（例えば案件別など）

「4.職員用」は、該当本部、または部の所属グループ配下のメンバに読み取り権限のみ付与し、部長以上グループ/職員グループ配下のメンバにアクセス/更新可能な権限を付与しています。管理者グループ配下のメンバにはフルコントロールを付与しており、個別に作成したセキュリティグループによるフォルダ単位でのアクセス管理を可能としています。

異なり、一律な権限委任ができない開発案件などに対応するためです。2つは、権限委任はするけれど、「誰が、いつ、何を行ったのか」、監査ログをしっかりと記録できること。監査ログは不正行為をしていないという証明にもなり、社員を守ることにもつながります。権限委任と監査ログは表裏一体として捉えるべきでしょう。そして最後のポイントは、そうした処理が効率的かつ確実にできるということです」。

組織変更の際もバッチ処理で対応、運用の大幅な効率化を実現

導入は2008年の春。運用でポイントになったのは、最初の設計でどういう単位でActive Directoryを管理していくかということだ。同社では組織図に合わせ、部門単位で、また本部で運営しているケースでは本部単位で管理者をつくり権限委任を行っている。基本的な考え方としてオープンとクローズという概念をつくっているという。

「オープンは部門の誰でも見ることができます。クローズは、部長以上、グループ長、案件別、社員全員と、4つに分かれています。ポイントとなるのは案件別です。部門の管理者は必要に応じて案件別にセキュリティグループをつくり個別管理が行えます。各案件のデータは、管理者により委任を受けているメンバーしか見ることができません。DRAは権限委任の単位を絞り込んでいけるため、権限が必要な単位から無暗に広がることなく、一元的な管理のもとで個別対応を可能にします」（前川氏）。

個別対応は運用の柔軟性につながる。実際にDRAの運用に携わっている総務部 河原由美香氏はこう語る。「個別対応は、協力会社の方が案件に参加した際の対応や、営業から開発、保守と、案件のライフサイクルに伴って主管部門が移動していくケースでも非常に有効です」。

管理者による権限委任と担当者による権限の行使は監査ログとして記録。また、他部門のメンバーを追加することも可能だが、部門を超えた権限に関しては申請によりインフラソリューション本部が追加作業を行っている。従来と比べ、Active Directoryの運用管理の大幅な効率化も図れた。「組織変更のときに、これまではセキュリティグループの付け替えに、1つの本部単位でも発令日の前の休日に出社して一日がかりで処理していました。それが今はコマンドベースでできてしまうので、全社レベルの対応が発令日の朝にバッチを流すだけです。事前に準備した上でバッチ処理ができるのでミスもなくなります。またDRAサーバのOSのバージョンが混在しても対応できるため、今後のバージョンアップも容易に行える点もメリットですね」（河原氏）。

障害対応面も向上した。DRAはプライマリとセカンダリという構成になっており、プライマリの機能を簡単にセカンダリに移すことができるため、万一の障害発生時も運用を止めることなく継続できる。

DRAの導入について藤田氏は率直にこう語った。「DRAがなければActive Directoryの本格的な運用はできなかったというのが実感です。今や当社の信頼を支えるセキュリティの重要な要素の1つです。これからも安定したサポートをお願いしたいし、また運用していく中で生じてくる改善点についてもいろいろとアドバイスをいただければと思います」。

“With your NEXT”、常にお客様企業とともに歩み続けるスミセイ情報システム。同社の信頼の基盤をこれからもNetIQはDRAの提供を通じてしっかりと支えていく。

スミセイ情報システム株式会社

PROFILE

スミセイ情報システム株式会社

本社所在地 ： 本社/大阪市淀川区宮原4-1-4 新大阪センタービル
東京本社/東京都新宿区西新宿6-14-1 新宿グリーンタワービル
設　　立 ： 1971年5月
資 本 金 ： 3億円
従業員数 ： 1,320名（2009年3月現在）
事業内容 ： システムコンサルティング/システム開発、運用管理/SI事業/ERP事業/ネットワーク設計、運用/アウトソーシング/セキュリティサービス

ネットアイキュー株式会社　URL：http://www.netiq.co.jp
〒162-0845　東京都新宿区市谷本村町1-1 住友市ヶ谷ビル12階
TEL：03-5206-9500　FAX：03-5206-9501　e-mail：info-japan@netiq.com

※NetIQ、Directory and Resource Administrator及びNetIQのロゴは、米国NetIQ Corporationの商標です。
※この文書で使用されているその他の企業名または商品名はあくまでも指摘を行うことを目的としており、それらは一般にそれぞれの所有者に帰属する商標及び登録商標です。
©2012 NetIQ Corporation, all rights reserved.