

IT全般統制の一つとして注目されるアイデンティティ管理

1999年度にシングルサインオン、 2000年度には統合ID管理環境を既に構築していた清水建設 これは自然の流れであったが...

大手総合建設業の清水建設では、「正当なユーザ」に「正しい権限」で情報システムを快適に利用してもらうために、1999年度にシングルサインオン(SSO)、2000年度にはメタディレクトリによる統合ID管理(IDM:アイデンティティ管理)システムを15,000ユーザに対して導入した。今回、SSO製品をRSA Access Managerへリプレースするとともに、従来は別管理だったSSOとIDMとの完全連携を実現し、人事情報から一元的にID情報の配信・管理を行うことを可能とした。現在、清水建設では、社内のほとんど全てのシステムに対してSSOでの認証を行っており、SSO管理下のサーバは100台以上である。今回のSSOのリプレースとIDMに関する今後の展開などについて、清水建設株式会社 情報システム部 インフラ企画グループ長 伊藤 健司氏と主査 松本 善太氏に詳しく聞いた。

今回、SSOシステムをリプレースされた経緯を教えてください

従来のSSO製品は、OSのプラットフォームが変更になった場合の対応や、製品自体の機能UPを目的としたバージョンアップが遅いなどの問題に加えて、原因不明のトラブルに対する対応なども遅く、メーカーやベンダーへの信頼性が低下したため、ユーザの利便性やセキュリティ対応の観点から、リプレースの検討を行いました。

どのように製品選定をされたのでしょうか

従来の製品が持っていた機能に加えて、今後必要となる機能を盛り込んだ要件定義書を作成しまし

た。一方で、各種セミナーや展示会、インターネットなどから情報収集を行い、プロキシ型2製品とRSA Access Managerを含むエージェント型2製品の4製品に絞って要件定義書を提示し、提案をお願いしました。

各提案は、それぞれの製品の特徴に基づいた提案でしたが、守るべきWEBサーバが支店などに点在しているという要件から、一次評価でエージェント型の製品を選択することにしました。

プロキシ型の製品では、原則としてサーバの集約が必要になること、またエージェント型の機能を混在できる製品もありましたが、現在の環境からの移行性や導入後の運用管理を考慮するとプロキシ型を選択するには至りませんでした。

最終的には、RSA Access Managerを選択されましたが

一次評価で残ったエージェント型の2製品は基本機能全般の評価に関してはほぼ同等でしたが、パフォーマンスと機器構成に注目してRSA Access Managerを選択しました。これは、従来のSSO製品の導入当初にパフォーマンスに関して重大な問題が発生し、苦労した経験があったからです。長期休暇明けの始業時などには、約2,000から3,000名程度が一斉に認証要求を行う場合もあるため、これらの要求に対するパフォーマンスは絶対条件でした。1999年度の導入時には、負荷テストツールなどもなくメーカー・ベンダーの話を信じるしかありませんでしたが、現在では要件定義に負荷要件を盛り込んで製品選定を行うとともに導入時には必ず負荷テストを行っています。

移行期間に8ヶ月掛かったそうですが、苦労された点などをお聞かせください

全社のイントラネットの認証システムであり、アクセス管理とシングルサインオンの機能を提供していますので、移行を失敗すれば日常業務に影響を与えてしまいます。そういう面では、8ヶ月というのは短かったかもしれませんが、エージェント型の製品のために管理対象サーバを一斉に切り替える必要がありました。このため長期休暇でないと切り替え作業を行うことができず、移行

時期が先にありきのスケジュールとなりました。また、既存システムからのリプレースのため、できる限りエンドユーザーの操作性に影響がでないようにする必要がありました。更に、当社の利用環境の特殊性などから、同時に以下のような対応も行いました。

★C/Sシステムへの対応

従来のSSO製品では、当社向けにカスタマイズを行い、一部のC/Sシステムに対しても認証処理を行っていました。RSA Access Managerは基本的にはWEBシステムに対応したSSO製品ですが、同様の機能を実現するために、従来の認証処理を改修し、RSA Access Managerサーバに問い合わせを行えるようにしました。

★冗長構成

従来は、SSO製品のリポジトリはコールドスタンバイ構成でしたが、今回のリプレースを機に、ホットスタンバイとして冗長化したことにより、より信頼性を増すことができました。しかし、Accessサーバの冗長化、リポジトリの冗長化、及びメタディレクトリとの連携部分の冗長化と、冗長化構成の組み合わせが非常に複雑になり、待機系から稼働系への復旧時の切り戻しのタイミングが難しく冗長構成の最終テストには苦労しました。現在は、運用である程度カバーしており安定して稼働しておりますが、リポジトリを含めた二重化の効果は、認証システム全体の信頼性という意味で大きな効果があると感じます。

★IDM(アイデンティティ管理)連携

電子メール、グループウェア、ワークフロー、ポータルなど、SSO製品を除くほとんどのシステムは、Novell Identity Managerをメタディレクトリとして、人事システムと連携して統合的なID管理システムとして運用してきました。しかし、メタディレクトリよりも早期に導入したSSO製品だけは、リポジトリがディレクトリではなくRDBであったこともあり、連携が困難で別管理となっていました。今回のリプレースでは、SSO製品をRSA Access Managerに変更すると同時にリポジトリをディレクトリにしたことにより、Novell Identity Managerとの連携を実現しました。今までは、大規模な組織の変更や従業員の異動時には、Novell Identity Manager(メタディレクトリ)で管理されているシステムと、別管理となっ

清水建設株式会社

情報システム部



インフラ企画グループ長 主査
伊藤 健司氏 松本 善太氏

ユーザプロフィール

清水建設株式会社

http://www.shimz.co.jp/

資本金：743.65億円

従業員数：11,357人

(2007年4月1日現在)

1804年(文化元年)に初代清水喜助が江戸神田で創業。創業200年の歴史を持つ。国立屋内総合競技場を始め歴史的にも多くの名建築を手がける大手総合建設会社である。

ていた SSO 製品との間で、組織の情報やユーザの情報に不整合が発生していないか、常に監視している必要がありました。今回、IDM と連携することにより、組織の変更やユーザの異動、職位や資格の変更などが自動的に反映されることで、今後は ID 管理作業が一段と効率化されると期待しています。

★アクセス権の設定、ロールとルール

RSA Access Manager は、従来利用していた SSO 製品とはアクセス権の設定方法が異なるため、システムの移行には十分注意を払いました。従来製品では、組織を束ねたユーザの集合（グループ）と資格や職種などユーザの属性に基づいたロールを作成し、組織の観点とロールの観点で、コンテンツに対してアクセスを許可する / しないの設定を行っていました。一方、RSA Access Manager では、部署や役職、雇用条件などから構成される個人の属性情報を演算することでアクセス権を付与するルールという考え方でしたので、慣れるまで時間がかかり既存アクセス権の移行設計には苦労しました。

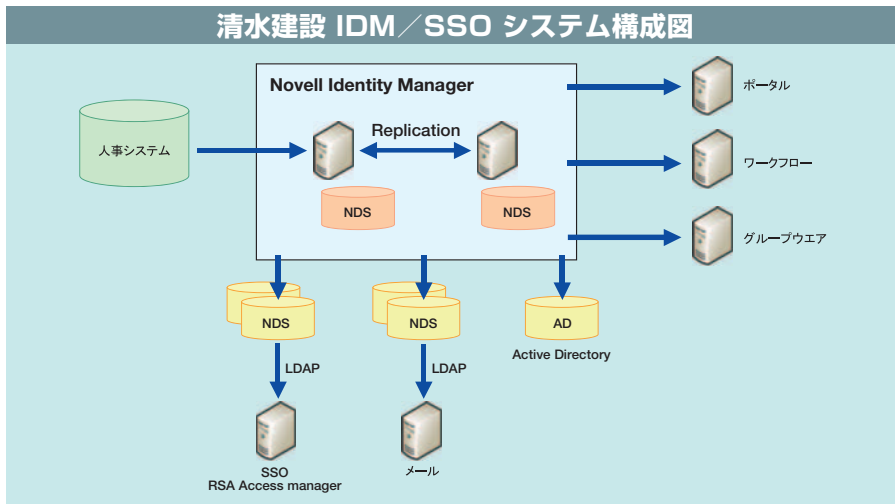
ただ、実際に移行作業を行ってみると、古い組織やロールによるアクセス権の情報が残っていたり、新たな資格や職位のユーザのアクセス権が正確に反映されておらず、本来アクセスできるコンテンツにアクセスできないユーザがいるなど、何点かの不整合も発見でき、移行作業と合わせて整合性を取ることができました。

今回の SSO 製品のリプレイスと IDM 管理による効果を教えてください

2006 年 8 月の運用開始から半年以上が経過しましたが、まず言えることはトラブルが少ないことです。従来の SSO 製品では、トラブルの度にサーバの再起動を余儀なくされたり、サーバのダウンを取得しても解決できないような原因不明のトラブルが発生したりと、運用面で不安がありました。RSA Access Manager は非常に安定した製品であると言えます。これは、要件定義書に基づいて綿密な製品選定を行うとともに、パフォーマンスの評価などにも十分な時間をかけた結果だと思っています。また、IDM との連携を実現し、アイデンティティ管理を完全に一元化できたことで、ID 管理の運用負荷の更なる軽減や権限設定ミス、ID の削除忘れなどの危険性がなくなったことも大きな効果だと思っています。

更に、このアイデンティティ管理の統合により、2007 年 2 月には、再雇用者のアクセス権管理と言う、新たな人事イベントに対する柔軟かつ迅速な対応や、情報漏洩防止を目的とした派遣社員に対する ID 管理制限の見直しにも対応することができました。

清水建設 IDM / SSO システム構成図



内部統制に対する IDM の必要性についてお聞かせください

内部統制における IT 全般統制では、アクセス管理が統制対象となっており、このアクセス管理を支える仕組みとして IDM の重要性は実感しています。システム監査において、人事情報から退職したユーザを無作為に指定され、そのユーザのアカウントが各システムに存在しないこと（正しく ID 管理が行われていること）を証明するという要求に対しても、IDM の管理画面やディレクトリブラウザなどを利用してユーザを検索し、存在しないことを証明することが可能です。逆に言えば、IDM がなければこのような ID 管理やアクセス管理に関する監査に対して、正当性を証明することは難しいのではないのでしょうか。

ただ、当社の場合は、システム監査や内部統制のために 2000 年度に IDM を導入したわけではありません。オープン系の情報系システム群が増加していく中で、純粋に ID 管理の運用負荷の軽減や確実な運用管理を目指し、ID 管理体系の設計を行った結果として IDM を導入しただけです。その結果として、システム監査や内部統制にも対応できる現在のシステムになっただけです。ID 管理の重要性を理解していれば、運用管理面からの IDM の導入とユーザの利便性を維持したセキュリティの維持（アクセス管理）のための SSO 製品の導入は自然の流れでした。

今後の計画について紹介ください

一元化された IDM により、社内の情報システムを利用する全てのユーザ（社員、派遣社員、関係会社社員など）のアカウントを管理できる体制とな

りました。当初は、全てのシステムを IDM 連携すれば良いと思っていましたが、これまでの経験から、IDM と直接連携（密結合）すべきシステムと間接連携（疎結合）させた方が良いシステムがあることがわかりました。パスワードなど、即座に変更を反映したいものに関しては、直接連携が必須となりますが、間接連携で十分なものを直接連携にするとトラブル発生時の影響範囲が大きくなったり、システムの更新が難しくなる場合があります。近い将来、直接連携と間接連携を考慮して、アイデンティティ管理システム全体の再構築も検討したいと考えています。

アクシオに対する期待などをお聞かせください

ID 管理や SSO 製品のリポジトリとして、ディレクトリの活用が一般的になってきていますが、AD (Microsoft 社 Active Directory) を構築できるベンダーは増加しているのに対して、AD 以外のディレクトリの設計や構築ができるベンダーはそれほど多くありません。ましてや、ディレクトリ間の連携設計や連携部分の開発ができるベンダーは非常に限られています。また、ID 管理用の製品も色々と提供されるようになってきましたが、ディレクトリに関する知識やノウハウの無いベンダーから ID 管理製品を導入するのは不安です。やはり、我々がしっかりした要件を定義できれば、その要件を満足するディレクトリ、IDM、SSO 製品などの提案ができるベンダーを選択することが重要なのです。アクシオとは、2000 年度の IDM の初期構築時から付き合いとなりますが、ディレクトリの専門家であるアクシオへの期待は変わっていません。

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。