CTC の統合 ID 管理の事例紹介

市川順之
伊藤忠テクノソリューションズ株式会社
ネットワークシステム推進部　セキュリティ推進課

概要：昨今のセキュリティに対する責任の高まりや、内部統制への対応のために、アカウントの統合管理が注目されております。CTC でもいち早く総合 ID 管理のシステムを取り入れました。実際の大学での導入事例の紹介をしながら、IDM 構築にあたってのポイントをご紹介します。

キーワード：IDM、シングルサインオン、監査

1.　IDM とは?

アイデンティティ・マネジメント（IDM）という言葉の中には、たくさん要素が含まれます。しかし、その中でも 4 つの要素（アクセス制御、プロビジョニング、ワークフロー、監査）が重要ではないかと考えています。（図 1）

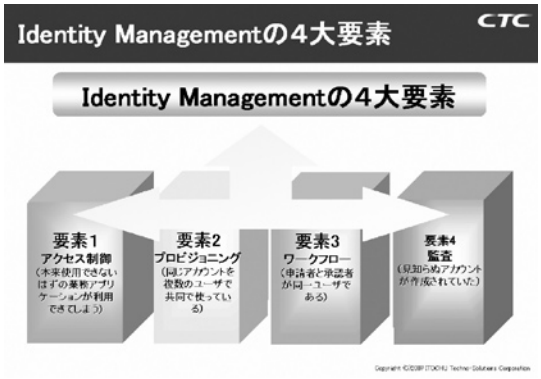

図 1.　Identity Management の 4 大要素

例をあげると、使用を許可されていない業務アプリケーションを利用できる ID が、間違えて付与されたり（アクセス制御）、同じアカウントを複数ユーザで共同利用できてしまう（プロビジョニング）こと、また、申請者、承認者が同一のユーザである（ワークフロー）、知らないアカウントがいつの間にか作られている（監査）ということがあります。

これらを管理・制限するために 4 つの要素があります。これらを統合的に、うまく使うことによって IDM を適切に管理、構築することができます。

アクセス制御では、ユーザの役割、基本属性を適切にコントロールすることが必要です。一般社員や営業部長、所属部署により、扱えるシステムは違います。例えば、一般社員は、顧客管理のシステムや人事システムにはアクセスさせないなどです。

2 つ目の要素、プロビジョニングは、ID のマスターになるシステムからそれぞれのシステムに対して、ユーザの ID、属性を連携していくことです。まず、人事データベースでアカウントの作成や変更、削除を行います。通常のやり方では、各システムに対しても同じことをやらなければなりません。さらに、システムごとの属性についても手入力が必要ですが、このプロビジョニングの機能を使うことによって、マスターを変更するだけですべてのシステムを連携させることができます。

3 つ目はワークフローです。これは重要です。申請されたアカウントをチェックもなしでやってしまったり、口頭の依頼で受けたりすると、不適切な登録や変更漏れなどの問題も多くなります。そこで、申請、登録などの運用をシステム化すれば、人によるミスはなくなります。

そして最後は監査です。特に監査の記録の観点で、ID そのものが適切なものであるかと、もう一つは、誰が、いつ、どこで利用したかというアクセスログを取得することです。これは、内部統制の観点からも重要です。

IDM といって、必ず出てくるのは、シングルサインオンという言葉です。1 回の認証で、すべてのシステムと連携して、何度も ID とパスワードを入れ直す必要がないということです。利用者がログインをすると、シングルサインオンサーバにログインの情報が行き、そこから認証情報をディレクトリサーバに情報を参照しにいきます。そして、そこから必要な属性だけを引っ張ってきて、各システムにアクセスした際、シングルサインオンサーバに問い合わせ、利用の可否を判断します。これについては、利用者の利用効率を上げる点でも有効です。

2. CTC が IDM を導入した理由

なぜ、CTC が IDM を入れたのかですが、導入前は、ID 管理が複雑化していて、情報システムの人間が管理しきれなくなってしまったということがありました。そして、あるシステムに入ろうとすると、以前の ID でも、今付与されている ID でも入れるという状態もありました。また、パスワードを何度も入力するのも面倒なので、システムをなるべく利用しないなど、システムの利用率の低下という課題もありました。これらの問題点を解決するために、IDM のプロジェクトが始まりました。

3. IDM のメリット

どのような機能要件で進めていったかについてですが、言い方を変えると、IDM をやることによって得られるメリットになります。

まず、散在する ID の管理リソースを統合できることです。次に、複雑かつ運用コストがかかる ID 管理のコスト削減、そして、ID の消し忘れや重複、間違った ID の付与を防ぐためのセキュリティレベルでの改善。

アクセスログやデータの配信のログについての監査レポートの機能も必要です。最後は、内部統制の点から、監査レポートを自動化して、何かあったときに見られるようにしておきました。

導入後のイメージ（図 2）ですが、左側が利用者、右側が社員の ID とパスワードを管理している人事のシステムです。右側の人事のシステムから、IDM のシステムを通じて各ディレクトリや、ディレクトリに対応していないシステムには直接 ID を送り込み、連携させます。初めに、利用者はアクセスマネジャーという、シングルサインオンの機能を持つシステムに ID、パスワードを入力し、ログインします。その際、裏でディレクトリサーバに LDAP のプロトコルで ID・パスワードの確認に行き、セッションを持ちます。それにより、グループウエアやポータル、会計系、販売系などさまざまなシステムを使えるようになります。

製品選定の基準としては、標準プロトコルに対応しているなど、既存のリソースとの連携手段があること、IDM 側からパスワードの変更ができることは当然ですが、リソース側からの変更や、パスワードポリシーが設定できるなど、パスワードの同期方法が複雑ではないことを考慮しました。

そして、将来的な拡張性があることも重要です。コンプライアンス対応として、ワークフローの機能、監査の機能。最後に、製品自体の導入事例が豊富であるというところを考えて決めました。

4. 導入事例

ここからは、大学向けにに提案・構築した事例を紹介します。

1 つ目は、某国立大学の例です。学生と教職員のアカウント情報を一元管理したいという要望がありました。一般ユーザは自分でパスワードの変更ができました。

このときの要件としては、アイデンティティ管理に関する運用コストを削減したいということ、学内のセキュリティポリシーの順守、シングルサインオン化、ディレクトリサービスや既存のアプリケーションと統合できることがありました。

このときはサン・マイクロシステムズ社の Sun Java System を使って、ユーザ情報の取り込みを行い、シングルサインオン対象のシステムに関しては、システム内にエージェントを組み込み、ID とアクセス情報の連携を

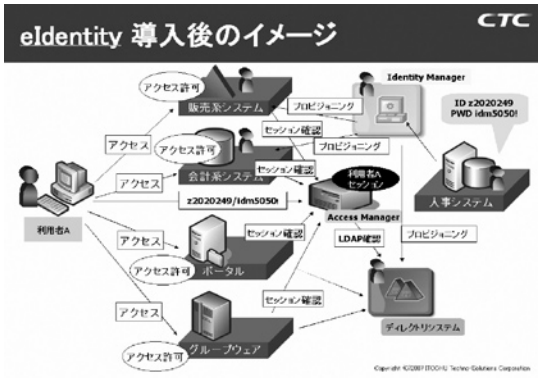

図 2. eIdentity 導入後のイメージ

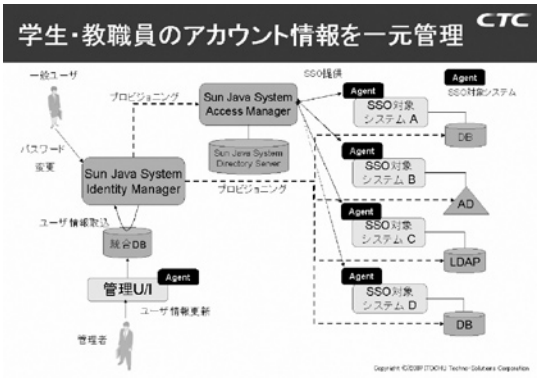

図 3. 大学導入事例 1

行いました。(図 3)

2つ目の導入事例としては、これも国立大学です。ここでも、各システムの ID 管理コストの削減、ID 管理漏れの防止、シングルサインオンが要望としてあがりました。また、教育研究系と事務系のネットワークがばらばらになっていて、それぞれが ID 管理をしているので、それを統合しながらも、管理としては分散管理したいという要望もありました。そして、ウインドウズのログインもきちんと統合管理したいということでした。

そこで、統一された ID のアクセス権限を教育研究系と事務系のネットワークで、それぞれ従来どおり管理者を立てていただき運用していただいています。(図 4)

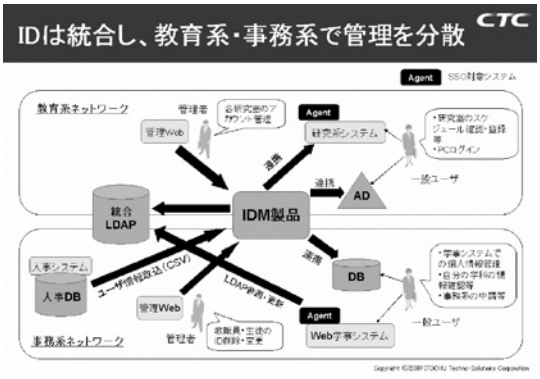

図 4.　大学導入事例 2

5.　IDM の現状

IDM 市場では海外製品、国内製品を含めて乱立しています。いろいろな製品が出ていて、単純に型、スペックでは比較できません。流れとしては、機能をたくさん持っている製品と、むしろ機能を限定している製品に二極化しているように思います。

我々に相談されるお客様は、IDM が必要だという認識はもちろん持たれています。やはり ID をきちんと管理しないで問題が起こると困る。ただ、投資のプライオリティとしてはもっと他にもやらなければならないことがたくさんあり、一番ではないと聞きます。導入に躊躇する理由として一番よく聞くのが、高価な割に利益に直結しない為、上層部への理由付けに苦慮するということです。ID を適切に管理できますという話をしたら、そもそも管理できていなかったのか、どういう運用・管理をやっていたんだと、その管理者の方が怒られてしまうということをよく聞きます。

そのときに、IDM に対してよく誤解されるところとしては 2 つあります。1 つは、ID 管理は、製品を導入するだけで簡単にできてしまうのかということです。実態としては、製品を入れるだけでは、実現できません。設計が 8 割なので、製品的に何にこだわるかより、まずは IDM の基本設計をしていきながら、製品を選定していく方法がいいのではとおすすめしています。

もう一つは、ID 管理はシステムを入れたからといって便利になるとは限らないし、結局、運用コストもかかるのではということです。短期的に設計・構築・導入と考えると、確かにシステム的には複雑になるので、手離れが悪いように見えます。しかし、一度導入して運用が波に乗れば、かなりのコスト軽減や、システムそのものの利用率が上がるなどのメリットも多いのです。

6.　製品選定のポイント

カタログに載っていない部分での製品の設定のポイントとしては、基本システムの連携手段として、よくカタログには、何に対応と書いてあるのですが、実際にどのように連携するか、カスタマイズは必要なのかということは、まずカタログには載っていません。ここは確実に一つ一つ確認していくしかないというのが現状です。

次に、パスワードの同期方法ですが、IDM からのパスワード変更ももちろん、リソース側からの変更ができ、パスワードポリシーの設定もできることが重要です。

そして、将来的な拡張性としては、現状のＤＢに合わせて、導入時に必要なデータベースを考えていく必要があります。また、連携先のシステムを追加する際に、単純にＡＰＩを入れるだけで使えるのか、それともカスタマイズが必要かまでを確認する必要があると思います。

また、導入事例を参考に、どのようなメリットがあったかを確認することも重要だと考えます。

7.　まとめ

IDM を構築にあたってのプロセスをまとめたいと思います。

Step1 は、IDM の構成要素を理解し、組織の中でどのような要件が必要とされているかを確認し、統合させるシステムの範囲を決定する必要があります。いきなりすべてに導入しようとすると、大概のケースで失敗するのが実情です。まずはクリティカルなシステムから統合していくことが重要です。

Step2 としては、現状の ID 管理の実情を洗い出していくことです。各システムでどのような ID、パスワードの命名規則があって、誰が、どのように追加・削除・変更等の管理をしているのかを洗い出すことです。ここが設計にかかわる肝になるので、ここで手を抜くと、また後で設計し直すことになってしまいます。

そして、Step3 として、ルールの確定と設計です。洗い出した情報から、マスター ID の命名規則や、連携先の ID との連携方式について決めていきます。

ここで大事なのは、もし IDM のシステムが壊れたときに、誰もシステムにログインできないという状況を避けるための逃げ道を考えておく必要があります。各システムへ個別ログインできる方法を用意しておくことが重要です。

Step4 では、システムの構築です。これについては、弊社にお任せください。

Step5 としては、実際の運用の確立と、ID の適用範囲の見直しです。そして、Step1 に戻ることの繰り返しにより、組織の中のすべての ID を統合管理できる形をつくっていくことをご提案します。