★Active Directory の導入と活用★

企業で 1 人 1 台パソコンがあるのは当たり前となり、場合によっては担当業務別に 1 人が複数の端末やアカウントを持つことも珍しくありません。しかし社員数が増え、会社の規模が大きくなると、パスワードを忘れたなどのログイン情報の確認作業や、新規ユーザー追加の際の権限管理など煩雑な業務も増えていきます。

このような場合に役立つものが Active Directory です。Active Directory にはシステム管理の負荷を軽減してくれるさまざまな機能があり、システム管理者の強い味方になってくれます。

ここでは Active Directory とは何なのか、
またメリットやデメリット、使用上の注意点などについてご紹介します。

◯Active Directory とは

Active Directory は Windows 2000 から導入されているサービスの一つで、システム管理者が組織のリソースを管理するのに有用なサービスです。Windows Server に標準搭載されているので、特別なソフトのインストールが不要で、サービス利用料のような形でコストが増えることもありません。

・ユーザー認証とアクセス制御を行う

ドメインとドメインコントローラー

Active Directory は、会社や組織に属している「人」、PC やサーバーなどの「モノ」、ファイルやフォルダなどの「データ」といったネットワーク上に存在するリソースを階層的に管理します。これらのリソースを管理する範囲を「ドメイン」と呼びます。

「ドメインコントローラー」は、ユーザーID とパスワードを使ってユーザー認証を行います。また、どの部署がどの共有データにアクセスして良いのか、その部署には誰が所属しているのか、誰がどの PC を利用しているのか、といったリソース間の関係性を管理します。データ閲覧のみ、データ削除可能といった細かい権限まで決めることもできます。

部署や役職ごとに管理単位を作っておけば、同じ属性を持った人に一括で権限適用することができるため、ミスの少ない簡単な権限管理を実現できます。

・ドメインツリーとフォレスト

組織が大きくなってくると保有するリソース（人・モノ・データ）が膨大になってくるため、上部組織・下部組織と、ドメインを分けて管理することが合理的になってきます。

ですが組織全体で共有リソースにアクセスしたい場合はどうすればよいのでしょうか？

例えば、下部組織に所属するユーザーが、上部組織のドメイン内にあるリソースにアクセスしたい場合、当該ユーザーは上部組織のドメインに所属していないためアクセスできませ

ん。上部組織のドメイン内で新たにアカウントを作ってもらうのは手間です。
そこで上部組織・下部組織のドメイン間で信頼関係を構築し、アクセスができるようポリシー設定します。これを「ドメインツリー」といいます。
また、会社の吸収合併など、もともと別の組織が 1 つの組織になる場合なども、別ドメインへのアクセスが必要になってきます。その場合でも、ドメイン間で信頼関係を構築することで、別ドメインへのアクセスが可能になります。これを「フォレスト」といいます。

・シングルサインオン

ユーザー自身が所属するドメイン内のリソース（ファイルサーバーなど）にアクセスしようとするとき、ドメインコントローラーから ID・パスワードで認証を受ける必要がありますが、次に同じドメイン内の他リソース（プリンターなど）にアクセスする際には、認証は必要ありません。これは、最初にファイルサーバーへアクセスしたときの認証が、当該ドメインコントローラーが管理しているドメイン内では有効なためです。
これを、信頼関係を結んだドメインツリーやフォレストにも適用するのがシングルサインオンです。ユーザー自身が所属するドメインに一度ログインするだけで、信頼関係を結んだほかのドメインのリソースにもアクセスできるようになります。

◯ドメイン内のソフトウェアや接続機器・メディアを管理する

ユーザーが利用するソフトウェアを管理者がまとめて設定することが可能です。端末上に業務に必要なソフトウェアをリモートから自動でインストールできるので、1 台ずつ設定していく必要がありません。 Windows Update も一括で行えるため、システム管理者の負担を減らせるとともに、ユーザーは個別の端末のメンテナンスを気にすることなく使い続けることができます。
また、Active Directory サーバーにプリンタドライバーを予めインストールしておくと、ユーザーがプリンターを利用時にプリンタドライバーが自動配信されますので、ユーザー自身がプリンターをインストールする必要がありません。Windows のグループポリシー機能と組み合わせることで、USB メモリなどのメディアへのアクセスを拒否する設定も可能になります。

◎なぜ Active Directory を利用するのか

利用する大きな目的は認証権限の一元管理であることが多いですが、その範囲は社内サーバーだけにとどまらず、クラウドシステムのサービスへもつなげることができます。

・Active Directory が必要な理由

ユーザー目線ではシングルサインオンが実現され、システムごとの ID、パスワードの入力が不要となります。さまざまな社内システムにそれぞれの ID、パスワードでログインしていると、パスワードを忘れてログインができなくなるリスクがあります。

かといってセキュリティ上同じパスワードばかり設定するわけにもいきません。複数のシステムで ID やパスワードを一括管理できる Active Directory を活用すれば、パスワード忘れが減り、パスワード忘れが発生するたびに対応が必要だった管理者の負担も軽減されます。

また、管理者目線では、Active Directory 内にあるパソコンの管理者権限をまとめて持つことができます。権限設定が細かくなればなるほど、1 台 1 台設定していく作業は、間違いが起きやすくなります。一括で設定ができることで、間違いを起こさず迅速に設定が行えます。

・Active Directory の利用例

Active Directory が多く利用されるのは、ドメインごとの権限設定時です。
具体的には、部署ごとや役職ごとでアクセスできるサービスや見られるフォルダを制御する際に多く利用されます。人事異動や役職変更があった際も、該当ユーザーのドメインを変更するだけで設定が完了します。シングルサインオンのため、先に会社のポータルサイトにログインしてしまい、その後ポータルサイト経由でさまざまなシステムにアクセスしていく際、すべてログインを省略するといった構成を作ることも可能です。

◯Active Directory を利用するメリット・デメリット

Active Directory を導入するメリットとデメリットは、

管理するパソコンの台数やユーザー数、担当者の習熟度など左右される要素がいくつかあります。自社の状況に当てはめながら検討すると現実的なシミュレーションができるでしょう。

・Active Directory のメリット

最大のメリットは、主に管理者の負荷削減です。
ユーザー属性ごとに権限付与できるためユーザー個々について設定しないでよいことや、シングルサインオンができるのでパスワード忘れへの対応工数も削減できます。またユーザーの利用端末を一括管理でき、設定ミスも抑えることができます。

ユーザー側もシステムごとの ID、パスワードを管理する必要がなくなるのはもちろん、

端末アップデートを手動で行う必要がなくなったり、ネットワーク上のプリンターなどの機器が使いやすくなったりとオフィスでの煩わしい作業が軽減されます。

・Active Directory のデメリット

Active Directory を利用するのに初期設定に多少手間がかかるのがデメリットです。ドメインごとの権限を決めてしまえば、あとはユーザーを追加して運用するだけですが、どこまでどの権限を持たせるか、どの範囲までシングルサインオンを許すか等の設計が、運用上またセキュリティ上、非常に重要になってきます。

一度決めたポリシーを変更するのは影響が大きくなりますので、慎重に検討しましょう。ユーザーはドメインの権限から逸脱することはできません。そのため、ソフトを一つインストールするだけだとしても、管理者の承認が必要となります。状況によっては業務を煩雑化してしまう可能性もあるのです。セキュリティ上権限制御は必要ですが、厳しすぎても円滑な業務を妨げるため、自社の環境に応じてバランスがとれるポイントを探す必要があります。また、Active Directory サーバーがダウンすると、リソースにアクセスできなくなるため、サーバーを冗長化する、定期的にバックアップを取る、サーバー障害時の復旧手順を予め決めておく、などの対策も必要です。

◯Active Directory の使用上の注意点

初めに設定したものをあとから変えようとすると、大幅な変更となってしまうケースが多いため、各設定に関しては変更する必要がないよう慎重に決定することをおすすめします。例えば、ドメイン名は多くの場合、自社名のアルファベット表記の省略系や、部署名などを使う傾向にあります。このドメイン名を変更しようとすると、ドメインへの参加がすべてやり直しとなり、ユーザー数が多ければ多いほど複雑な作業が発生してしまいます。

また、システム自体は定期的にバージョンアップする必要がありますが、バージョンアップの難易度が少し高くなっています。セキュリティ対策を万全にするにはバージョンアップが必須なので、実際にアップデートを行う前に手順を準備しておくとよいでしょう。

◯セキュリティ強化策としての Active Directory

Active Directory がきちんと運用されていれば、共有アカウントを使って、複数人が、同じアカウントでログインする状況は作られません。あくまでも同じ権限を持った個々のユーザーでログインするので、ログでそれぞれのユーザーの操作を追いかけることができるのです。(ただし対象となるログは、ログオン時の認証やファイルサーバーに対する操作ログなど、Active Directory に関連したサーバーに対するログのみとなります。)。

ログが残ることがユーザー側からするとプレッシャーになることもありますが、

操作をある程度トレースできる状態にしておくことはセキュリティ上必要でしょう。
また、最新のセキュリティソフトやセキュリティパッチをユーザー端末へ一括配信できたり、USB メモリなどポリシーに反するメディアへの接続を拒否できるなど、マルウェア感染などのセキュリティリスクを一定程度抑えることができます。

ただし、管理サーバー自体への攻撃に厳重に注意する必要があります。Active Directory はアカウントやリソース情報を集中管理する仕組みのため、ドメインコントローラーが攻撃され管理者権限を乗っ取られると、被害も甚大になります。

Windows Server の脆弱性をついて、ドメイン管理者権限を搾取する攻撃例も実際にあり、
「ドメイン管理者やサーバー管理者権限を持つアカウントは最小限にする」
「ドメイン管理者アカウントを、クライアント PC で利用しない」
「Active Directory サーバーには常に最新のセキュリティパッチを適用する」など最低限の対策は必須となります。

◯全体として、

システム管理者の稼働削減やユーザーの利便性向上が狙える Active Directory は、
管理する対象が増えれば増えるほどその効果を発揮します。
ただしセキュリティ対策が甘いまま安易に使うと組織に甚大な被害を与えかねません。
Active Directory を使いこなして、メリットを最大限享受できるようにしましょう。