

アクセス権限管理の新しい考え方 「アイデンティティマネジメント」

情報漏洩対策は経営者の義務である。その対策が不十分なために機密情報を流出させてしまった場合、企業経営を揺るがしかねない事態となることは言うまでもない。その情報漏洩対策の第一歩となるのはアクセス権限管理である。本稿では、アクセス権限管理のための新しい概念である「アイデンティティマネジメント」について解説する。

リスクマネジメントとアクセス権限管理

2005年4月に全面施行された個人情報保護法や、米国のサーベンス・オクスリー法（いわゆる企業改革法）を待つまでもなく、情報管理を適切に行い、また企業経営の透明性を確保することは企業の責務である。情報漏洩対策に関しても、その仕組みを構築し、それを定期的に検討・評価し、顧客や株主に対してその有効性を証明し報告することが企業には求められている。

もちろん、企業でもその必要性の認識からそれなりの対策を行ってきたはずである。しかしそれにもかかわらず、最近でも情報漏洩事件はなくなっていない。そのような事例をみると、アクセス権限情報が的確に更新されていなかったことが原因となったケースが少なくない。これは、パート従業員を含めた退職者のアクセス権限を速やかに停止していなかったなどの人為的ミスである。

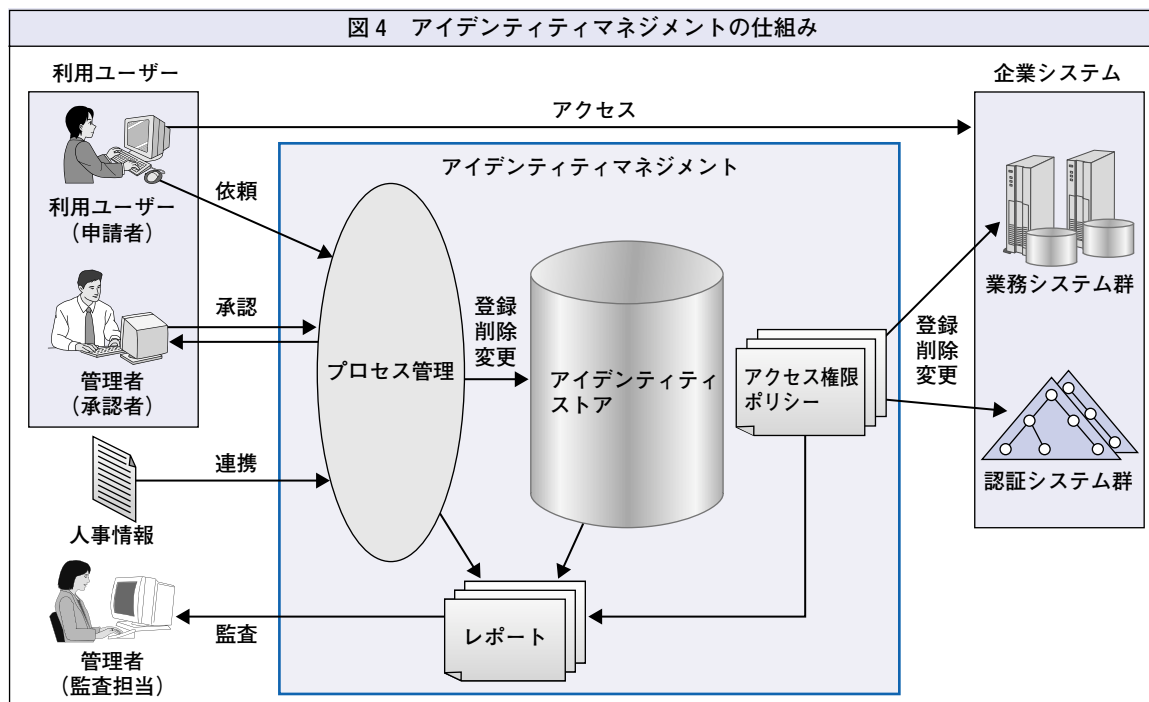
こうした問題は、入社・異動・昇進・休職・退職など、従業員のステータスが変更になったときに即座にアクセス権限を付与または停止するELC（従業員ライフサイクル）管理の仕組みを設けることで解決できる。

アクセス権限管理の問題点

しかし、実際にこのような仕組みを構築することは簡単ではない。それには運用面からみて2つの大きな理由がある。1つは、利用効率向上と運用負荷軽減を目的にアクセスIDを共有するため、ELCをシステムへ反映する手段がないことである。もう1つは、利用ユーザーとシステムの関係性を管理できるような集中管理方式をとっていないことである。すなわち、オープン系企業システムの場合、現状では個別のシステムからみた利用ユーザーの管理、すなわち各システム担当者に依存した分散管理方式となっているのである。これでは、情報漏洩対策の重要な要素であるアクセス権限ポリシーを、企業システム全般にわたり矛盾なく包括的に適用できていることを評価し、証明・報告することは困難である。

アイデンティティマネジメントの考え方

そこで企業がまず取り組む必要があるのは、「誰」（どのような属性をもつユーザー）が「何」（どのシステム）にアクセスできるのか、アクセス権限が付与または停止されるまでのプロセスはどうなっているのかを明確



化することである。これがアイデンティティマネジメントの基本的な考え方である。

図1にアイデンティティマネジメントの仕組みを示す。アイデンティティとは、単にそのユーザーが何者であることを示したものではない。それは、組織におけるそのユーザーの役割は何か、そのユーザーがアクセスする必要のあるリソースや情報は何か、そのリソースや情報に対してそのユーザーは何ができて何ができないのかという、利用ユーザーと企業システムとの関係を定義したものである。このアイデンティティマネジメントの仕組みを集中管理方式でシステム化することにより、ELC管理と、アクセスポリシーの包括的な適用が可能となり、また、それを定期的に評価

し、株主や顧客に対して評価結果を証明・報告することができるようになる。

グローバル企業の標準として

いまや、自動車や金融をはじめ、さまざまな業種で国境を越えた企業提携や合併が増え、半導体・電子部品・化学・鉄鋼などの分野では世界的な電子取引市場が形成される状況にある。適切な情報漏洩対策はいまや国際的なビジネスの枠組みという観点からもきわめて重要である。その一環としてのアイデンティティマネジメントは、コンプライアンス（法令順守）やセキュリティの面にとどまらず、サービスの面でもグローバル企業の標準となる可能性をもつものである。