CASB は企業に必要なのか？

CASB（Cloud Access Security Broker）

- 2012 年にガートナーが提唱
- クラウド利用を可視化・制御を可能にする
- 4 つの実装形態 (API、3 種のプロキシのモード）
- セキュリティベンダーが様々な製品やサービスを提供

4 つの機能

可視化・分析
コンプライアンス
データ保護
脅威からの防御

クラウドサービスの利用が高まるにつれ、CASB（Cloud Access Security Broker：キャズビィ）に対する需要が高まっています。
CASB は、ガートナーが提唱した言葉ですが、企業や組織が利用するクラウドサービスについて、基本的には、サービスを使用するユーザとクラウドの間に単一のコントロールポイントとして CASB を設置して、可視化し、データを保護して、不正な通信についてはアクセス不可とするような集中管理をするような製品やサービスを指します。
それを実現する仕組みとして、クラウドが提供している API を利用してアクセスなどの可視化をする API モード、使用する端末側にプロキシを配置するフォワード・モード、クラウド側に配置するリバースプロキシ・モード、既存のプロキシからログ情報を得るエグジスティングプロキシ・モードの 4 つのモードに大別されます。
製品やサービスによって提供されるモードや特徴が違うため、どういった手法を使うかは、使用するユーザの環境やセキュリティポリシーによって、どれが適しているかを十分注意して調査する必要があります。
ここで分かりづらいのは、企業の多くは既に様々なセキュリティ対策を実施しており、クラウドサービス提供側のシステムでも、セキュリティ対策は提供しているので、それでもまだ何が必要なのかという点です。
従来、情報漏洩の対策としては、ファイアウォールやプロキシを監視し、不正な通信は遮断するなどの対策が取られていましたが、その際は、守るべきデータが企業内にありました。クラウドサービスの利用が広がり、情報漏洩させていけない重要なデータもクラウド上に保管される可能性が出てきました。しかも、利用するサービスは多岐に渡り、複数のクラウドをまたがって利用することも珍しくありません。グラウドの種類によってもセキュリティ対策の方法や、レベルが違ってきます。このあたりで、自社のセキュリティポリシーに従い、統一した管理を望むのも当然の流れでした。
しかも、働き方改革でテレワークの需要が拡大し、個人所有の PC やモバイル端末を使用して、企業で利用実態が把握できない「シャドー IT] の脅威も増大してきました。こればかりは、いくら運用ルールを作っても、ID パスワードで Web ブラウザから利用できてしまうサービス等は、利用状況を把握し統一的な管理をすることが難しいのが現状です。
CASB については、今後クラウドサービスへの移行が進めば進むほど、増大する脅威やリスクを回避するために、まだまだセキュリティ対策としての投資が必要となりそうです。