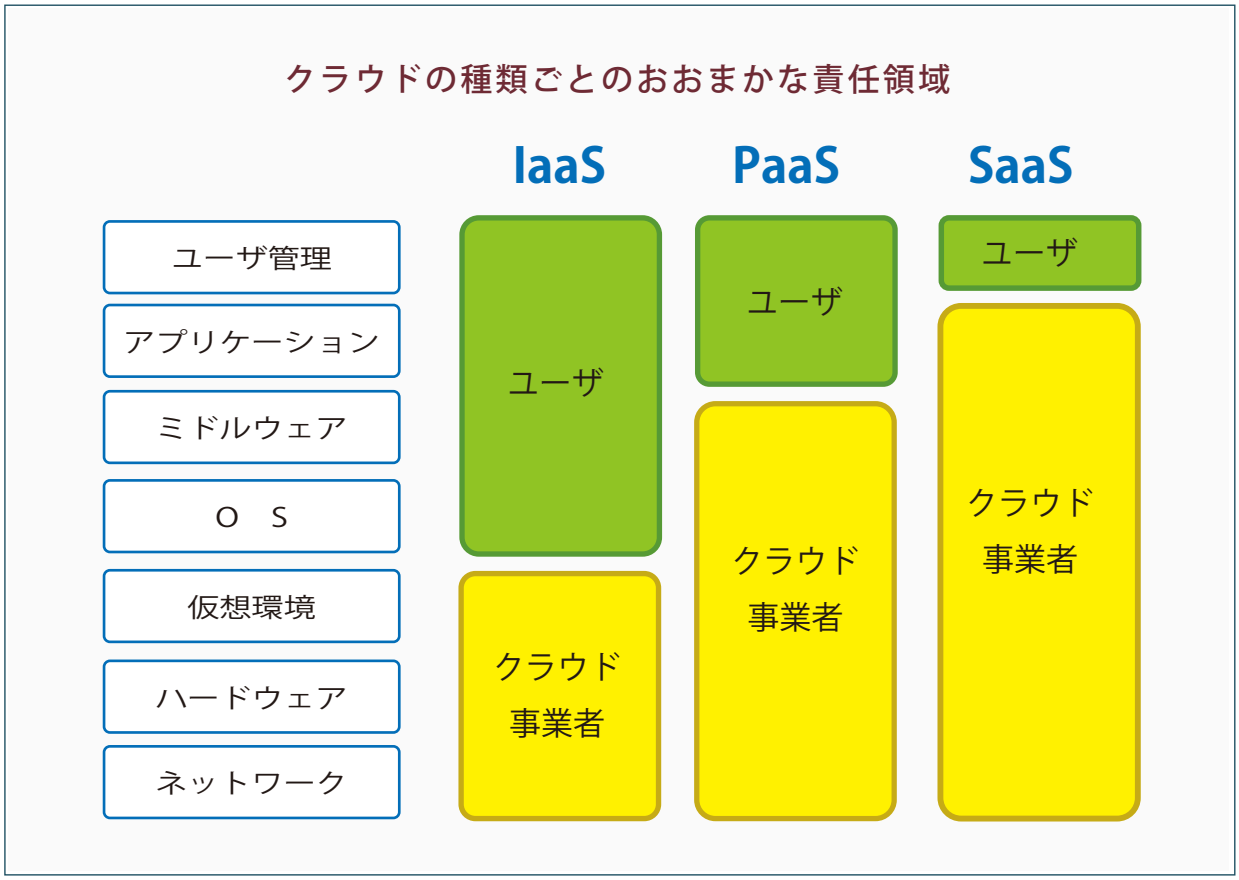
クラウドの責任分界点



クラウドのセキュリティ対策を考える場合、クラウド事業者とユーザの間で「責任分界点」という言葉を使用することがあります。

責任分界点は、電気工事や通信事業などで使われている言葉のようですが、トラブル時などの責任範囲を明確にするためには、クラウドサービスを利用する上でとても重要な観点となります。これは、IaaS、PaaS、SaaS のどの特性でサービスを選ぶかという場合に、ユーザの企業側でも自己責任で行うべきセキュリティ対策が明確になるため、どの部分がクラウド事業者が主体になるのか、それとも企業側が責任を持って管理すべきなのかが具体的に把握できます。

IaaS は、データセンターにあるコンピュータやネットワーク環境を借りて運用するので、基本的にユーザ側の企業が管理主体のイメージですが、仮想サーバ単位に契約が行われることが多く、仮想環境までを含むマシンやネットワーク機器などのインフラがグラウド事業者側の管理となります。ユーザ側は、ファイヤフォールなどのベーシックなセキュリティから、設計、管理が必要です。

PaaS は、インフラ部分に加え、OS やネットワークの設定などはすでにクラウド事業者側の責任で用意されており、サービスとしてのプラットフォームなので、加えて多くのミドルウェアもインストール済みで選択使用が可能です。但し、それらはユーザ側で設定する部分も多いため、ユーザ側での管理も必要になってきます。

SaaS は、サービスとしてのソフトウェアなので、セキュリティ管理についても、アプリケーションまですべてグラウド業者にお任せというイメージに思えますが、ID 管理などはユーザ側の責任なので、考慮は必要です。

どのサービスを利用するにしても、責任分界点はあくまでも選定先の事業者や、サービス内容によって異なり必ず個別で確認が必要です。また、どのタイプのサービスであっても、事業者側では、ユーザ固有の事情は責任範囲外なので、ユーザが責任主体となるのが基本です。

たとえば、予定していたよりアクセスが多く、CPU 使用率も上がりそのために異常終了した場合、クラウドサービスには、契約の前提状況があり、リソースの使用量オーバーは、ユーザ責任となります。また、使用法をよく理解できていなかったために情報漏洩が疑われるような場合、ユーザの自己責任になりかねません。

クラウドサービスを利用する場合は、リスク対応計画のためにも、責任分界点の把握はセキュリティ対策上必須です。