GMO CLOUD

クラウド事業者からみた実態とジレンマ

GMOクラウド株式会社
技術部開発セクション セクションチーフ
岩間 和彦

自己紹介&略歴

岩間　和彦

GMOクラウド株式会社
技術部開発セクション　セクションチーフ

- ✓ 山口出身、宇部工業高等専門学校卒業
- ✓ 日本TI、@YMCを経て、GMOクラウドに
- ✓ 讃岐うどんとヱビスをこよなく愛する何でも屋

略歴（クラウドっぽいもの）

1998/9 … Webringの日本語化を担当
- (株)兼松コンピュータシステムが日本語版を提供

2006/4 … Xenを採用したVPSサービスの開発
- (株)アット・ワイエムシー

2011/6 … パブリッククラウド(IaaS)サービスの開発
- グループ会社横断での共同開発

2012/4 … クラウド基盤を利用したVPSサービスの開発

現在 … GMOクラウドに転籍し、各種サービス開発を行う

クラウドサービスとは(1)

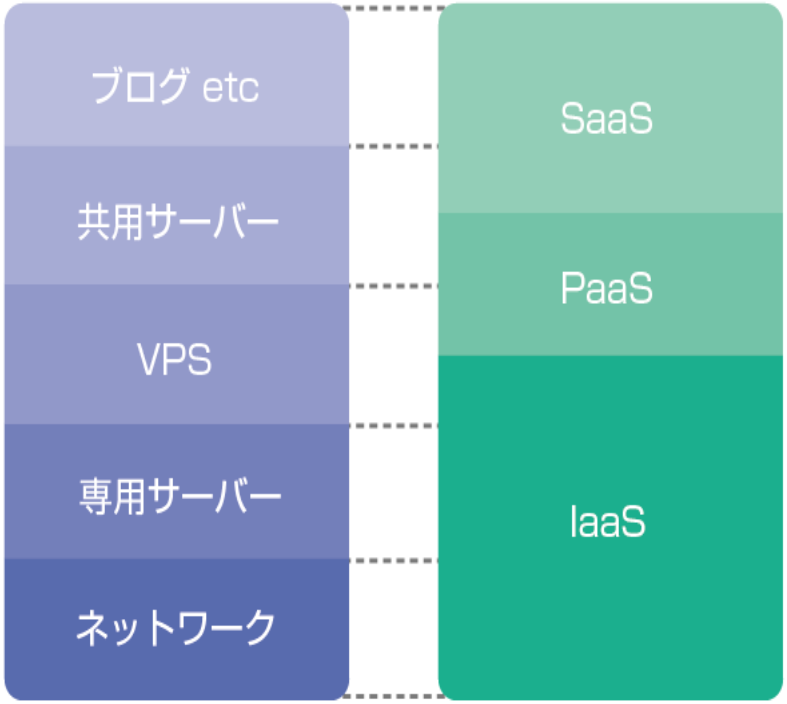
- ネットワーク、サーバー、ストレージ、アプリケーションなどのリソースを、オンデマンドで利用できるサービス
- SaaS, PaaS, IaaSなどを初め、用途毎に様々なカテゴリーのサービスが展開されている
- そのため、「クラウド」という言葉だけでは、何をさすのか分からず、混乱の素になっている

クラウドサービスとは(2)

- クラウドの一番の特徴は「オンデマンド」
  - ✓必要なリソースを
  - ✓必要なときに
  - ✓必要なだけ利用できる
- 仮想化技術の普及により、従来はサービス化の難しかったネットワークやストレージも利用できる
- 自由度が高い反面、利用者の責任範囲も増大している

各種サービスの特徴と違い

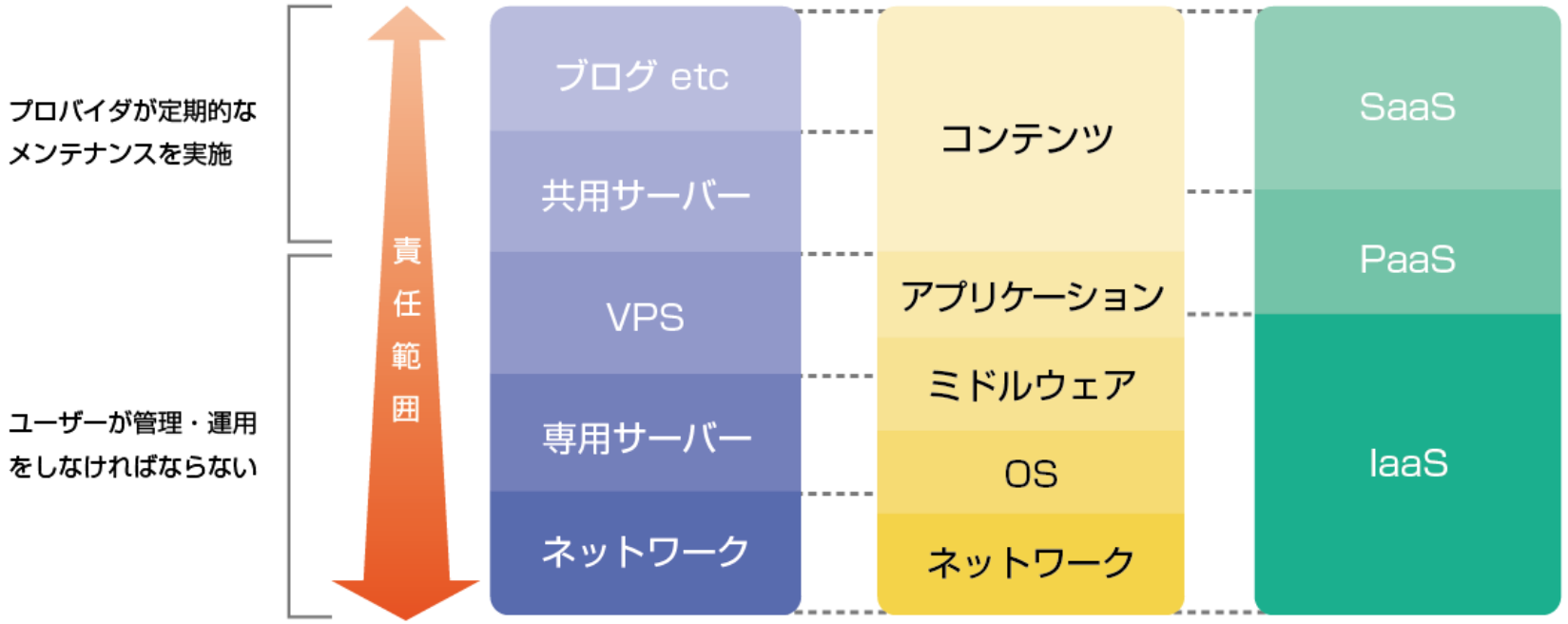
- ✓ SaaS/PaaSは、ブログサービスや共用サーバー、VPSに相当するサービスで、より特定の分野に特化されている
- ✓ IaaSの自由度は従来のVPS・専サバ以上で、より複雑な構成も可能
- ✓ SaaS→PaaS→IaaSと段階的に専門的な知識が必要になる



従来のサービスとの対応

管理しなければならない範囲

- PaaS/SaaSに関しては、従来のブログサービスや共用サービスと大きく変わらないため、コンテンツ作成に集中できる
- IaaSはOSやネットワークまで含めて管理・運用しなければならない



何が起こるのか(1)

今までは「コンテンツ」だけを
考えていれば良かった

IaaSサービスではサーバー(OS)設定、
ミドルウェア、アプリケーションの設定まで
責任を持たなければならない

初期状態のままで使い続けていませんか?

何が起こるのか(2)

- ✓コンテンツの改ざん
- ✓フィッシングサイトの設置
- ✓マルウェアの設置
- ✓データの漏洩
- ✓不正プログラムの設置
  - →外部への攻撃
- ✓バックドアの設置
  - →最新版にしても対策できない

WordPress

WordPressは非常に人気のあるCMSのため、利用ユーザーも多く、また攻撃対象となる事も多い

- WordPress本体のみでなく、プラグインにも注意が必要

Plesk

多くのプロバイダで利用されているサーバー管理ツール

- 特に古いバージョンを狙った攻撃が多い
- 複数のサイトを運用している場合、サーバー内の全てのサイトが改ざんされることも!!

対策

WordPressやPleskのようなアプリケーション、ミドルウェアに関しては、最新版へのバージョンアップを怠らない事が重要

また、サーバー設定の不備が原因のことが上位を占め、特にVPSやIaaSを利用している場合には、初期状態のまま利用していることも多く、注意が必要

SSH/FTP

SSHやFTPへの攻撃は、ブルートフォースあたっく(総当たり攻撃)によるパスワードの取得が原因の場合が多い

- 不特定多数への攻撃では辞書を使った攻撃が多い
- パスワードが解読されてしまったサイトが、攻撃サイトとして使われる場合も

対策

- 不要なアカウントの削除
- 安易なパスワードを使わないように
- 接続元を限定したり、利用ポートを変更するのも有効

メールサーバ/DNS

インターネットになくてはならないものだが、適切な設定・運用が難しく、また、外部に対してオープンにしておかなければならない為、攻撃の対象となりやすい

- 不用意にメールサーバーを動かすことでスパムの踏み台にされてしまうことが多い
- DNSへはサービス不能状態(DoS)となる攻撃がたびたび行われている

対策

- 最新版に保つだけでなく、安全な設定を行うことが重要

✓メールに関しては、外部のメールサービスを利用できないか検討する

✓DNS自体を自分で立ち上げなければならない場合は多くないので、本当に必要か考える

何をするべきか

- OS・サーバーの設定をみなそう
  - 初期設定の状態で使っていてはダメ
  - 不要なアカウント、アプリケーションの削除を
- とにかくアップデート
  - 最新版になっていない時点で対策が難しくなる
- ファイヤーウォールの設定
  - IaaSでは無料でファイヤーウォールが利用できる場合が多いので、必要なところ以外は閉じる
- 継続的な監視と見直し
  - システムに異常がないか、普段と違うことがおこっていないか、継続して監視することが重要
  - バージョンアップや、不要な設定の削除などを継続して行う