

2017年3月期 決算説明会 質疑応答の要約

質問者 1

①2017年3月期のクラウド関連ビジネスについての手応えを教えてください。

弊社では、デジタルマーケティング事業、セキュリティソリューション事業、クラウドソリューション事業を注力3事業と位置付けています。昨年度の決算説明会で、これら3つの注力事業をクラウド上に一本化してお客様に提供する方針を発表し、1年間活動してきました。その結果、クラウド関連ビジネスとして注力3事業の合計売上高で年成長率20%の成長を継続しております。

②クラウド関連ビジネスについて、2018年3月期以降の期待もしくは課題を教えてください。

2018年3月期以降も、クラウド関連ビジネスとして注力3事業の合計売上高で20%以上の成長を目指しています。

企業のデジタルマーケティングは、CRM（※1）で顧客データをどう分析するか、営業のコンタクト、あるいは商談の進み方をどう分析するかという方向に、データ解析の主軸が移っていくと考えています。

また弊社のデータアナリティクス事業は、2017年3月期より、Webサイトのアクセス解析からIoTなどのクラウド上に集まったビッグデータの処理へと大きく舵を切っています。今後、クラウド上にCMS（※2）を構築するソリューションの提案も推進していきます。

③クラウドソリューション事業で、2017年3月期第4四半期から2018年3月期第1四半期に期ズレした案件があったのか確認したい。

十数億円規模の官公庁向け農業関連プロジェクトにおいて、一部の納品が4月以降に移った案件もありました。

④前年同期比で2017年3月期第4四半期の限界利益率が低下している背景を確認したい。

今期は、旺盛な需要に対して900名ほどの外部パートナーと共に対応を進めてきました。しかしながら、外部パートナーと協業を行っていくストラクチャーが整備されていませんでした。これが、限界

利益率低下の要因の1つであると考えています。2018年3月期においては、外部パートナーとの協業ストラクチャーについて見直しを行い、パートナー制度を導入する予定です。

⑤パートナー戦略を見直す予定ということだが、従業員数拡大の見通しを教えてください。

2017年4月27日現在、連結従業員数は982名です。2018年度上期中に約30名の採用を予定しています。弊社の社員がやるべきことと、パートナーへ依頼することの区別をしていくことが重要と考えており、そこを整備していく予定です。

質問者2

⑥データアナリティクス事業の減収について、事業環境の変化や戦略見直しについて確認したい。

Webアクセスの解析が、広告を販売するための一つのサービスに移ってきています。弊社では広告を取り扱っておらず、Web解析だけで売れるような状況ではなくなってくると想定しています。既存のお客さまに対してはWeb解析のサービスを継続しますが、新規に成長する分野だと考えていません。

RやPythonといった統計のスキルを身に着けてきた人材を活用し、オリジナルのサービスを開発し、Webのアクセス解析よりも、IoTなどのクラウド上に集まったビッグデータの処理などに活路を見出したいと考えています。

⑦セキュリティソリューション事業の伸長について、2017年3月期が特需だったのか確認したい。

2017年3月期は、自治体情報セキュリティクラウドの案件が各都道府県で発生し、弊社は4県の開発を行いました。2018年3月期からは運用のフェーズになります。また、セキュリティ分野の特性から、継続した改善や追加の対策が求められるのではないかと考えています。

⑧2018年3月期の採用は、どの事業領域の人材が中心になるのか教えてください。

昨年度は、セキュリティ分野ではSOC^(※3) ビジネスの拡大に貢献できる人材、データサイエンスの分野ではツールを使って解析するのではなく、オリジナルサービスを立ち上げるといったことに興味のある人材の採用を進めました。2018年度も引き続き、セキュリティの専門家やデータ解析の人材など、注力事業の分野での人材獲得を計画しています。

※1：CRM (Customer Relationship Management) とは、主に情報システムを用いて、顧客と接する機会のあるすべての部門で顧客情報や商談状況といったコンタクト情報を共有・管理することで、顧客に合わせた細かい対応を行うことができ、長期的に良好な関係を構築する手法です。

※2：CMS (content management system) とは、コンテンツ管理システムとも呼ばれ、ウェブコンテンツを構成するテキストや画像などを体系的に管理し、配信など必要な処理を行うシステムです。専門的な知識がなくとも簡単にウェブサイトを更新・管理することができます。

※3：SOC (Security Operation Center) とは、24時間365日ネットワークやデバイスの監視をし、サイバー攻撃の検出と分析、脅威となるインシデントの発見や特定、連絡を行う組織です。