BCAO 関西支部 2015 年 9 月度勉強会 （第 104 回）議事録

日時：2015 年 9 月 16 日、18：40～20：30
場所：大阪市中央公会堂　第 6 会議室
出席者：細坪、萩原、速水、野原（司会）、伊藤（高）、飯田、伊藤（聖）、山口、中村（和）、増穂、櫻本、山本、鷲山、柳父（書記）

テーマ：クラウドサービスの概要とその注意点～クラウドサービスは安全という神話的な誤解を正して、利用者はサービス内容を確認し、正しく利活用しましょう
話題提供者：山口孝一氏（株式会社インターネットイニシアティブ）

会社紹介、担当業務紹介に続き、クラウドの神話について

- 出席者のクラウドに対する理解を確認し、Gmail もＬＩＮＥもクラウドサービスの一つであることを指摘
- クラウドサービスの実態を紹介するが、利用者の期待値とあっているかを理解してもらい利用していただきたい
- 皆使っているから大丈夫と思っているかもしれないが、何を求めているかが問題
- そもそもクラウドという言葉は実体のない Buzz ワードのようなもの
- クラウドサービスのメリットとして一般的に言われているのは、「個別ソフト開発不要でスピードアップでき、維持管理もお任せで安い」
- 「サービスが止まらず、データは冗長化され消えず、天変地異でもサービスを継続でき、SLA 契約があるので大丈夫」という神話がある
- そもそも初期のクラウドサービス（Google など）は、自社システムの余剰リソースを提供してはじめられた
- その後、各社から多種多様なサービスが提供され爆発的に利用されたので、各社とも需要に応えようとしてサービスを充実させている
- サービス停止もあれば、データの冗長性も一部のメールサービスぐらいで、個別システムやアプリは冗長ではない
- 冗長性を確保するにはサーバの追加が必要
- 「3.11 でも使えた」ことで、クラウドサービスに対して「天災に強い」期待は高いが、そもそも約款では（“不可抗力”にあたる）自然災害時などは免責になっている

C：アメリカでは天変地異のためのクラウドサービスがある
A：ニーズがあれば対応するだろうが、日本では一般的ではない

- 免責契約の実態は、利用料の返金で、機会損失の補償はない
  クラウドサービスの停止例：
  ウェブアリーナ（NTTPC コミュニケーションズ子会社）は事故復旧できずにサービスを終了（2011.5）

ファーストサーバ（ヤフー子会社）は、データ消失し復旧時に情報漏洩を起こした

- 2013 年は障害が 1388 件発生し､925 万人が被災し､補償が 2.7 万円／人の場合もあり、最初のヤフーの 500 円／人より上昇した
- BCP へ対応手段として利用する場合は、目的に合っているかが問題で、選択肢の一つと考えるのがよく、クラウドだから安心ということはない
- クラウドに対する過剰な期待が多いので、あえて否定的な話をした。

C：他のインフラと同じでクラウドも大きな災害により被災した場合はダメになる

C：クラウドは「(災害があっても）大丈夫」というサービス提供者がいるので、誤解を招く

Q：天災時のリスクを減らすためのテクニックは契約によってできるのか？

A：クラウドサービスにはパブリック（共用）とプライベート（専用）があるが、プライベートサービスでニーズに合わせた冗長構成をとることは可能。

Q：(クラウドサービス会社は）トラブルを起こしても生き残れるか（倒産しないか）

A：(資産提供可能な）親会社が大きかったりすれば、すぐに倒産などということはないだろう

- 基幹システム等、重要なシステムはクラウド業者に何でもお任せではなく、契約内容を理解したうえで利用すべきである。企業情報など Web に公開するシステムで利用するのがよいのではないか
- 米国の愛国法や中国等、カントリーリスクに対する懸念を受けて、実際にサービス提供を行っている場所情報は公開されるケースが増えている

ベンダーロックインについて

- あるシステムを構築した際に、その後他のベンダーへの乗り換えが難しくなるようなシステム構築がなされることをベンダーロックインという
- システムは階層構造的に作られているが、ハードウエア（物理層）よりもユーザに近いほど（アプリケーション層）ロックインされやすくなる
- またクラウドサービスにおいて、利用している下の階層のサービス障害は、その上の階層のサービス障害にもつながり、サービスを利用できなくなる（道連れになる）という連鎖問題もある
- メールなど、アプリに近いほど他のクラウドでは使えず、データを預け増やしてサービスが止まっても、データを移転できないことがある
- 買う側はちゃんとサービス内容を見る必要があり、使い勝手を深く確認する
- 気になったことは質問すること。ちゃんと答えられない業者は理解せずに提案していると思ってよい。発注者は勉強しないと業者の回答が核心からずれていても見破れない。重要なデータを預ける場合は、勉強する必要がある

Q：クラウドサービスを選ぶときのコツは？

A：何が必要かを整理するところから手掛けるべきで、そもそも何をしたいのか（What）よりなぜそれを使わなければならないか（Why）で考えるのが良いのではないか。ビジネス上の背景、目標は何かを意識すればよいと思われる

- 利用者側担当者は勉強し、リスクとメリットを認識すべきである
- 一般ユーザがフリーに使っているメールが攻撃されることはめったにない
- タダに多くを求めてもダメ
- 基本は何がしたいか

Q：中小企業が小さなサーバーを持つよりクラウドを利用した方がよいのか？

A：各企業の環境により異なる。雑居ビルのフロアにサーバーを置くより、クラウドを利用したほうが、安全な場合もある。どこに安心を求めるかにより異なる。リスクとコストを考えた判断はあるだろうが、ちゃんと考えているかどうかが問題

Q：病院でまだ WindowsXP を使っているところがたくさんあり、OS サポート切れでもアプリが入れ替えられない

A：一般的には OS サポート切れに合わせて作り替える。一番危ないのはネット接続の PC。ネットから物理的に切り離すことを勧める

Q：インターネットバンキングはクラウドサービスか？

A：銀行自身が提供している Web サービスである。その銀行がどこかのクラウドサービスを使うということはあり得るが、ここではわからない

Q：クラウドでデータを蓄積するのはまずいのか？

A：データをダウンロードするときに課金するシステムなら、バックアップ用に使うと安い

Q：ファーストサーバのデータ消失は元に戻せなかったのか？

A：一部は戻った。経緯の詳細は http://support.fsv.jp/urgent/参照。

ことの発端は技術的に上位にいる者がマニュアルと異なる方法でメンテナンスを行ったが、上位者ゆえ誰もそのイレギュラー対応を止めることができなかった。さらにはプログラム不具合などが重なってデータロストという障害を引き起こした。(一次障害)

その後データ復元に当たっては、復元できたデータもあったのだが、その公開にあたってアクセス権限の確認ができておらず、他利用者、さらには消去したはずのデータ（サービス利用をやめたユーザのデータ）まで公開してしまった。(二次障害)

このこともあり、現在利用者がサービス提供者に対してデータ消去証明書を求めることもある。

Q：過去のインシデントを踏まえて、クラウドは進化し続けているか？
A：ニーズに合わせて進化している

- 「BCP に対する投資は直接、利益に結びつかない。災害対応のためのシステム二重化はコストが合わない。」と言われてきたが、最近は仮想化、データ重複排除技術等により安価に DR（デザスタリカバリ）できるようになってきた。（DR は個々に要件が異なるため）個別のシステム構築（SI 案件）で取り扱うべきである。
- クラウドなら防災に有効と考える人が多いが使い方次第

Q：メールの乗っ取りは？
A：特定の個人を狙う攻撃がある。メールは暗号化できるが、通常は平文で送受信される
フィッシングメール等、メールに返信するだけで情報を取られることもある。（社保庁の年金通知の成り済ましメール等）
同じユーザ ID とパスワードをあちこちで使いまわしするのは良くない
Q：ISP と契約している有料メールと gmail 等の無料メールのどちらが安全か？
A：広くシェアのあるところは狙われやすく、これなら大丈夫というサービスはない。
OS でいえば Windows と Linux と比較し、Linux が強いということは言えない。たまたま Windows のシェアが多いだけ。
Q：情報が持つ価値により狙われる度合いが決まると考えてよいか？
A：一般的にはそう考えられている。ソーシャルハッキング対策として、タバコ部屋を正社員と派遣社員で分けるところもある。セキュリティに対する教育、リテラシィ向上が必要。

Q：スマホをビジネスで使うときの注意点は？
A：スマホも PC と中身は同じ。PC と同じセキュリティ対策が必要。スマホは落としやすいので、紛失したらリモートでデータ消去する（リモートワイプ）機能を使うことも検討するとよい
インターネット経由で資料を参照する場合は、実データではなく画像データとして送るとセキュリティが高くなる
個人スマホの業務利用（BYOD）は社内外での使い方のルール作りが必要
どういう使い方をしたいかが基本。何がやりたいかが明確になっていないと、導入後に不満が出る。
重要なことの判断で、他人がやるからやるという話はない

Bot 機能を持ったメッセンジャーソフト（IIJ 商品紹介）

- 安否確認なら、中にいる Bot（小人のようなもの、自動応答ロ**ボット**）が総務部の担当者に替わり安否確認メッセージの送信を代行できる
- LINE と違い未読者が分かるので、無回答でもある程度の状況が把握でき、記録集計に

便利

Q：気象庁がリツイートによる救助要請を認めず、助けての声が消えたのでは？
A：気象庁については分からない。3.11 では Google などの情報発信が有効であった。(地図と道路が通れるかどうか。Finder で行方不明者のリスト作りなど)。善意の内のベストエフォート。信用できるかどうかはそれぞれの判断だが、こういった活動が行われた。
上手く回れば成功で、回らなければ失敗

Q：BitCoin は儲かるか？
A：それはわからない。個人的には儲からないと思うし、手を出す気はない。
Q:ねずみ講と同じか？
A:ねずみ講ではないので、仕組み自身で儲かることはない。
またインセンティブ（手数料収入のようなもの）を得るには、(計算能力の高い）ハイパワーなマシンが必要となる。

Q：SLA とは何か
A：サービスレベルアグリーメント。サービス品質を保証する契約条項のこと。サービスが止まらないと言っているわけではない。止まった場合は、返金するという契約。
C：アメリカでは非常時の SLA をうたったものもある

以上