

**第二回 ITトレンド研究会 議事録**

日時: 2011/12/14(水)14:00~17:00

会場: 丸紅ビル B1F A 会議室

テーマ: 待ったなしの自然災害への備えは万全か?  
~3.11 後の BCP にクラウドサービスは有用か? 徹底検証~

講演者: NTT コミュニケーションズ株式会社  
クラウドサービス部 ホスティング&プラットフォームサービス部門  
サービスマネジメント担当課長 馬場 登志郎 氏

司会・進行: ITトレンド研究会座長  
京都 IT 相談室  
林 道彦 氏

当研究会の運営方針により、個人/会社名を特定できる発言、および発表者から公開の許可を得られなかった内容は 議事録より削除されています。あらかじめご了承ください。

◆第1部

馬場様のご講演

◆第二部

【自己紹介】

<座長>: BCP について困っていることあれば、それも含めてご紹介して下さい。

<A 社>: お客様に提案する立場です。BCP もキーワードになっていて、今回参加しました。金融業界等の大企業お金をかけているのですが、逆に小さい企業の場合、どうすれば BCP 対策に対応できるか聞きたいです。

<B 社>: 運用メインの仕事です。BCP 対策に興味があり、参加しました

<C 社>: 最近、総務に移動になったのですが、総務も BCP 対策を検討する必要があると思ひ、参加しました。帰宅難民や、ネットワークがなくなってしまった場合、どうなるのか聞きたいです。

<D 社>: BCP に関して非常に意識しております。運用ベースの中でどういう形でコストをかけずにできるか? という観点に立って聞きたいです。

<E 社>: 大阪にも拠点があり、奈良に拠点があります。災害が起こったらどうなるか不安です。大阪と奈良は近いですが、2つ拠点間で BCP を実施しております。ただ、拠点側が台風時に水没の恐れになり、もう少しで、水害に。次は水害のことを考えた BCP も必要。

<F 社>: BCP に関して、迫りくる東海地震等に対策をとっておかなければなりません、タイ洪水で部品調達が怠ってしまっております。そのような面での、事業継続に関しても考えていかなければなりません。

<M 社>: 電話が使えなかった場合の衛星電話の管理とかを担当しております。データセンターが山奥にあり、震災発生時にインフラが断られた場合、どうするのかという議論がでています。ここは社内でも、再検討課題になっています。

タイ洪水で、PC の部品供給切れがあるのですが 皆さんの会社は、影響はないか聞いてみたいです。

<G 社>: データセンター等の 2 拠点を利用して BCP 対策を実行しようとしていたところですが、次に考えておかないといけないのは、データ量の増加に関する事です。データをテープにとっていたのですが、それだと追いつけない状態に陥ってきました。この部分は改善策を打っていく必要があります。

また社員の安否確認をどうするのかというところを検討中です。

<I 社>: ハウジングで十数台所持していましたが、トップから、マスタ・請求・グループウェアをクラウドに変更せ

よと指示があり、2台の仮想化に移行しました。保守が切れていたサーバがありました。12月決算にいくまそ  
うとしていました。保守だとまたお金かかるだろうと思うのですが、社長は、クラウドにすれば安くなるだろうとい  
頭しかないです。

平準化したコストが果たして企業としてよいのでしょうか。キャッシュフローの観点からするとリスクがあるような  
気がします。

→座長: レンタル? リース? 購入の議論は、以前にも PCNW のテーマ「PC 購入するとき」にありましたよね。その  
時期の経済状況によっては購入を我慢しなければならないとかありましたよね。そういうのと同じなのでしょう  
ね。

<J 社>: 個人的に 3.11 の震災で感じたことですが、役場が流されたところで、住民の確認等が大変困難でし  
た。公共の施設の状況どうなっているのでしょうか?

Q<K 社>: 石川県と大阪の2拠点で BCP を行なっております。NTT の安否確認システムを導入しましたが、訓  
練の仕方がどうなっているのか不安です。そこが未だに検証できておりません。大規模災害の後は、パンデミック  
のような衛生面も崩れていくはずだと思います。そういったところまで考えている企業があるのでしょうか?

→<講師>: 弊社では災害前、災害時、災害後と3つのフェーズでBCPを定義しています。BCPは事業継続計  
画なので災害前の対策から復旧までの一連のリスク対策を定義する必要があります。データ容量が多いときの  
DR に関しては、悩んでいるお客様も沢山いらっしゃいますが、クラウドやホスティングはコネクティビティも含まれ  
た、一体型の DR/BCP ソリューションとして提供されている例が増えてきています。また企業の脅威の定義によ  
って BCP も、DR サイトの距離も変わってきます。

ネットワークがなくなればどうなるのかというご質問もありましたが、弊社は全国 73 拠点の DC があり、デー  
タセンターは複数ルートを持っています。また DR のプラットフォームはそのうち大都市中心に設置されています  
ので、更に迂回ルートが充実しており、また人が多いのでライフラインもしっかりしています。ひごろの災害訓練に基  
づき復旧は全精力をあげていますので復旧スピードも速いです。したがって、ネットワーク全断のリスクは少ないで  
す。

→<座長>: 箱さえしっかりしていたら大丈夫という時代がありました。

→<講師>:

クラウドのお得感に関しては、企業の中でも考え方はいろいろあります。SI 的な構築も場合によってはアリです。  
ただし、ビックデータの時代(経営資源を守る)になっていくと、SI 構築は 100 の容量を構築し、更新時は 200 に増  
大する可能性もありますので、そうなるコスト高となり、システムのライフサイクルを鑑み検討する必要もあり  
ます。使った分だけ使用料を支払うクラウドと比較して分析が必要です。また、検討するときは高熱費等周辺の環  
境コストも含めて考える必要があります。

Q<座長>: タイ洪水で、PC 部品調達で困っている人はいますか?

→<H 社>: ⑩日本で古い技術は、タイに機械が移りました。なので、現場、今は作れないですし、修理もでき  
ません。

→<G 社>: ⑨あるハードディスクを発注したのですが、テラステーションはありますが、予備 HD が危ういです。

→<K 社>: ⑭スキャナ部品が社内で影響がありました。

→<座長>: 東日本大震災やタイ洪水の影響で、部品がないから作れない、ということが発生してしまいました。  
当初は、その他サプライ系で対応できるだろうと予測していたのですが、大手企業が買占めてしまい、在庫がな

い状態になってしまいました。なので、しばらくは厳しい状況が続くと聞いています。

→<D 社>:メーカー系は部品もっているだろうけど、商社系はもっていないでしょう。3~4月になれば元に戻るだろうという話を聞いています。

→<講師>:地震発生時は、まず電源の確保が必要になってきます。弊社のグループとしては、東日本から 35 台、西日本から 25 台を現地に調達しました。燃料補給基地があります。北日本まわりで、ラインも迂回しました。輻輳する可能性もあるので、仮設等で構築する場合があります。弊社は災害時様々な対策を考慮して備えています。常日頃備えをしておき、そこへのネットワークをつなげさえすればビジネス継続(BC)は確保できます。

Q<A 社>:電柱が立てられない場所に、移動アンテナと電柱の復旧の重要度はどのくらいですか？

→<講師>:設備による重要度は関係ないです。中に誰が利用しているかでネットワークの重要度を計られます。

Q<座長>:衛星通信は？

→<講師>:東日本大震災の災害時はワイドスターの問い合わせが多かったです。

<C 社>:保険会社は意思決定のため、全役員に衛星電話を配布したと聞きました。

<座長>:どこかの役所は衛星電話配備していましたが、結局、災害時は使い方がわからず NTT のライン復旧の方が早かったですね。このように、東日本大震災で大騒ぎになったが、この時期に総括しておくべきことがあるとおもいます。

Q<座長>:電源対策がすでに終わっているという企業はありますか？

→<講師>:電話の交換機は、自社の電源で電気容量が大きなものが必要になります。

→<C 社>:あきらめてとめてもいいとは思いますが、その代わり安全に止める必要があります。それが一番大事ではないのかと思います。

→<K 社>:3.11 の時、営業拠点は停電してオーダーエントリーができなくなってしまいました。サーバ本体・ネットワーク・クライアント PC をどれかひとつでもなくなれば BCP はできなくなってしまいます。

→<座長>:絶対止められないものは、考えておく必要があります。そのためには、トップに理解してもらい、常時共有しておく必要があります。逆に、止める場合でもアナウンスしてから行う事が大事です。

Q<座長>:製造業にとって、品質・モノの作りこみは 4M※っていられています。

※4M =Man(人)・Machine(作るもの)・Method(方法)・Material(材料)

人をどう確保していくか、災害が起きたときに 誰が音頭をとるのか、またサブは誰なのか、ということの Man の観点も必要。たとえば連絡網とかも、そこに含まれます。そういうのが決まっている企業はありますか？有事の際に連絡が来る事はありますか？また、社員同士の安否確認できていますか？

→<講師>:そのような導入はしていますが、とても苦労しています。電話をかけてみて、つながらなかつたらメールで連絡をとりました。ただ、じわじわと回復していきましたが、大きな災害時は想定外の事象が発生します。

→<H 社>:震災後、安否確認システムが導入されました。地域レベルで設定、つまり、社員が現在住んでいる所で設定しているので、本人が出張していたら、機能しなくなってしまいます。それから、緊急時だと慌ててしまっており、安否確認の電話ができなくなってしまっております。なので、ひとつの方法だけでなく 複数確保しておく必要があります。

→<L社> 部署ごとに、Gメールを使っているところがありました。本社とのやりとりはめっちゃめっちゃでした。その後、危機管理委員会を受けて、電話やキャリアメールは止め、インターネットメールを利用しようという方針になりました。iPhoneを所持したり、私物のものを利用できるようにしたりしていく予定です。

→<F社> 安否確認システムは、完全でなくても一覧で見れる事が必要というのが、総務の意見です。

→ 一斉メール配信もできるので活躍します。

→<K社> 普段のメンテナンスが必要ですね。総務から定期的に、メールを送っているの、その精度を保つ必要があります。そうすれば、ひとつのチャネルとして有効利用できるのではないのでしょうか。

→<F社> メンテナンスはしています。ただ、当初3ヶ月に1回していたのが、現在は半年に一回にしています。安否確認は、プッシュでくるのがいいのかと思います。

<C社> グーグルドックスを使用して、安否確認システムを構築中です。そこに災害時に社員が情報を書き込む形式です。ユーザー入力簡易化を考えアンケート形式。もちろん、個々の情報は、管理者のみが閲覧可能というシステムになっています。

弊社では、総務側から社員に確認をするのではなく、「企業人なのだから この連絡先(方法)で安否確認を下さい」と言っておけば出来る。という考えで安否確認システムを作っています。

Q<F社> 災害のときにそれができるのでしょうか？

→<C社> 防災カードにマニュアルが記載してありますので、問題ないかと思います。

<座長> Material(材料)の部分、Method(方法)、ネットワーク切れたらどうするのでしょうか。

「情報漏えいが怖いのでPC持ち歩くな。家に帰ったらPCなし。」という体制ですと、帰宅時に災害起きた時はどうすればいいのでしょうか。そのような事を避けるためには、方法論も複数考えておく必要があります。

企業はひとつの方法を2重化するというやり方が好きなかもしれませんが、災害時は、複数の方法を作っておくことも大事かと思います。個人のインターネットも利用に関しても考える必要があります。個人のクラウドを広げ、個人のiPhoneやiPadでも利用できる方法もありかと思います。個人利用のデバイスを会社インフラとの親和性をつなげていきたいです。

災害対策はいろいろ関わり・観点があるので、第3部では、その議論を続けていきたいです。