クラウドコンピューティング環境下でのコントロール

日本セキュリティ・マネジメント学会
IT統制研究会
主査　澤田栄浩

研究会参加メンバー

石崎 靖敏、一瀬 智司、伊東 寛、大井 正浩
川口 元、河本 高文、斎賀 宣昭、鮫島 吉喜
宍道 洋、清水 惠子、田場 和弘、田吹 隆明
中本 雅寛、橋本 真智子、橋本 純生、
長谷川 誠志、和田 康、澤田 栄浩
（あいうえお順）

研究会活動状況

「クラウドコンピューティングにおける
コントロールに関する調査・研究」

- 第1回　平成21年8月5日（水）
- 第2回　平成21年9月2日（水）
- 第3回　平成21年10月7日（水）
- 第4回　平成21年11月4日（水）
- 第5回　平成21年12月2日（水）
- 第6回　平成22年1月12日（水）
- 第7回　平成22年2月3日（水）

当研究会が考えるクラウドコンピューティングの特性・定義

- クラウドコンピューティング環境とは
  - オンデマンドかつセルフサービス方式で利用されるようになっており、
  - ネットワーク経由でさまざまな場所からアクセスでき、
  - 共有コンピューティング・リソース・プールからリソースが提供され、
  - 必要に応じて利用規模を迅速に拡大、縮小でき、
  - 何らかの方法で使用量が測定される

NIST（National Institute of Standards and Technology）
CSA（Cloud Security Alliance)などを参考とした

なぜクラウドか？

- 既に該当するサービスは大量にあるのになぜクラウドか？
  - アマゾンなどは物を購入するが、今話題のクラウドサービスはネットの向こう側にデータを置き、同じくネットの向こう側にあるCPUを使って処理している。
  - つまりサービスを購入しているのであって、物の売り買いはしていない。
  - 例えばエキスパートのネット版などは典型的なクラウドではないだろうか。

パブリックとプライベートの利用シーン

- パブリッククラウドは中小企業、プライベートクラウドは大企業といわれている。
- しかし、外資系の企業などは大企業でもクラウドサービスを積極的に活用し、情シスを縮小するなどのコスト圧縮を図る動きが見える。

クラウドはワールドワイドに活動をしている
企業ほど大きなメリットがでるのかもしれない

ビジネスチャンスなのか？

- 日本にある外資系企業は、おなじく外資系企業が提供するクラウドのサービスを積極的に使うことになるかもしれない。
- 例えば、外資系の某社はクラウドサービスを積極的に活用して、情報システム部の縮小にまで踏み切るような動きさえある。
- 海外に支社支店をもつ日系企業にむけて、日本企業がサービスを展開すれば、言語の問題もなく、ひとつのビジネスチャンスかもしれない。

問題は何か

- クラウドに預けてはいけないデータ
- ネット犯罪の可能性
- 法や協約など
- その他、監査の視点など

サービスを利用する前に

- そもそもクラウド側に預けても良いデータとそうでないデータがあるのではないか。
  - 過去の同様の事例から推測すると、時間経過と共に、なし崩し的にデータがクラウド側に行ってしまう可能性がある。

例）個人情報
- 個人情報保護法では、日本国外へのデータ移転に関する明示的な規制は定められておらず、各業界で個別に実施されているガイドラインで提示されている。
- EUでは「データ保護指令」で第三国が充分なデータ保護レベル水準にない場合、EU域内から第三国へ個人データを移転してはならないことを定めている。
- 米国商務省は個人情報保護に関するセーフハーバー原則を策定し、EUから「適切な保護レベル」を確保しているとして2000年に承認をうけている。

クラウドサービスの拡大後は

- 企業の預けるデータが増えれば増えるほど、サービス提供会社側で情報を盗んだり、売りさばいたりといったことが出てくるかもしれない。
- 騙す対象が個人から企業になるため被害額は相当大きなものになる可能性ある。

ネット犯罪の可能性①

- リアル社会で実在する犯罪は、ネット社会でも当たり前のように実在する。
- リアル社会にない犯罪もネット社会では発生している。
- 大量のデータを預けてしまえば、人質ならぬ「データ質」のようなものも発生するかもしれない。

ネット犯罪の可能性②

- 信頼の悪用

  （クラウドサービス業者の中にいる業者）

  - 例えば、アマゾンやyahooのサイトで商品を販売している業者は信頼していないが、アマゾンやyahooは信頼している。
  - このような心理をうまく悪用すれば、詐欺行為は簡単かもしれない。
    - 例えばヤフオクで小物で信頼をつみあげて、大きな商品で大量に詐欺を行えば、かなり儲かるか・・・・。

ネット犯罪の可能性③

- 暗号化通信の悪用
  - 企業の出口部分でVPN化するのは良いが、手元のPCからVPNを張ってしまった場合は監査が不可能になる。
  - この環境を利用して機密情報の持ち出しをされても、通信の中身が見えないので分らない。

ネット犯罪の可能性④

- 詐称と詐欺
  - 提供ベンダーから利用料請求をしたら偽装ユーザだったということもあるかもしれない。
  - クラウド側に情報を入れていたら偽装サイトだったということもあるかもしれない。

パブリッククラウド・サービスの提供環境として一般的である「マルチテナント」も課題が多数指摘されるようになってきた

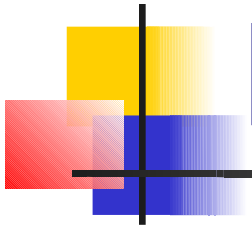
ネット犯罪の可能性⑤

- 社内システムのデータへのアクセス
  - クラウド側から企業の内部システムにアクセスすることがないか？
    - LDAPなどへのアクセスはありうる。ただし、VPNを使うなど縛りが入ると思われる。

法や協約などの問題

- 愛国法（パトリオット法）
  - サーバの設置場所が米国であった場合、有事の時にサーバが差し押さえられてサービスがとまる可能性がある。
- ワッセナー協約
  - 暗号技術など、知らないうちに協約に抵触する可能性がある。

ワッセナー協約とは、通常兵器及びその転用が可能な部品・技術について、特定地域に対する輸出を制限する国際協約及びその管理体制のこと。1996年7月、共産圏の崩壊に伴い、旧共産圏を対象とした輸出規制であったココムから発展する形で成立。主に、イラン、イラク、リビア、北朝鮮への輸出が対象。



問題をまとめてみる‥

大きく問題は6つ捉えられた

- データという資産を使った脅迫などが発生する可能性がある。
- 信頼を悪用した大規模な詐欺が発生する可能性がある。
- 暗号化通信は監査を阻害しうる。
- 提供側、利用者側双方で詐欺が発生する可能性がある。
- 社内システム侵入の可能性がある。
- サーバの設置場所によっては、その国の法や国際協定などにより問題が発生する可能性がある。

監査の視点からは

- SAS70が新基準（米国SSAE　No16）に変わることになっている。
  - 新基準は、2011年6月15日に適用開始。
  - 日本の18号も国際監査保証基準審議会ISAE3402により変更される予定。
- クラウド事業者の関連する項目は、
  - 従来は「統制の記述」を提供した。
  - 新基準では、「設計し、適用しているシステムについての記述」を提供する必要がある。

当研究会では、現在議論の最中であり、結論にまで到達していません。

引き続き議論を重ねて参りますので、御興味のある方は是非会合に御参加ください。

ご静聴ありがとうございました!!　＜IT統制研究会＞