# IT統制の限界

## The Limit of IT Controle

システム監査学会
ITを利用したガバナンス研究会

2013.06.07

第27回研究大会

発表者：清水恵子
（公認会計士　、システム監査技術者）

# アジェンダ

1. 2012年活動状況
2. システム管理者の限界
3. 他社のインシデントの影響
4. リスク要因
5. 企業の防衛策
6. リスクを前提とする経営
7. 今後の活動予定

# 1. 2012年活動報告

メール等を使ったコミュニケーションの活用

* 会合

  日時：2012年12月7日（金）　18:30～20:30

* 場所：機械振興会館　6－60号室（活動内容確認）

* 日時：2013年3月26日（火）　19:00～21:00

* 場所：機械振興会館B3-7号室（発表内容確認）

# 2. システム管理者の限界

- システム管理者は本来は自社のシステムを管理
- システム管理者権限はオールマイティ？（何でもできるは、もう神話）
- 企業の利用するサービスは他人が支配する
- 障害が発生しても原因は解明できない
- なにをまもるべきか
- アンドロイドを利用したら、ディバイス管理はMDM（提供は他社を経由する）

# 3. 他社のインシデントの影響

* 他社のインシデントの発生により、自社のシステムが利用できなくなる
* 自社の営業データが喪失する
* ウィルスが他社のシステムから侵入し、PWが盗まれる
* 安価で便利はリスクがある

# 4. リスク要因

* サービス提供業者の資格や免許は？
  * クラウドサービスは認可事業ではない
* 認証は保証ではない（ISMS、ISO9000）
* 事故を起こすと認証は停止になるケースもあるが事故が起こったら、もう、遅い
  * 絶対の保証がないことを前提とする
  * リスクを認識する

# 5企業の防衛策

* 他社に依存するリスクの低減、受容、回避
  * 古典的だがバックアップデータは確保
    * ネットワーク回線は？（スマートホン営業がストップ）
    * アプリは？
    * 著作権は？
  * ITに依存しない？まさか（電車の事故対応）
    * インシデント対応は考えているか
* 企業がリスクを認識しないこと自体がリスク

# 6. リスクを前提とする経営

- 企業は何を統制できないかを知り、対策を考える
- 格安航空のサービスは限定されている
  - 何が無いサービスなのか（データは保証されているか）
  - 代替はあるか
- 日本は、まだ、安全神話？
  - 契約の内容を理解しているか
  - 全てを依存できない
  - 自分で守るべきものは守る
- 古くて新しいが・・・・
  - 統制はコストとベネフィットのバランス

# 7. 今後の活動予定

* ITを利用するリガバナンスをどう認識するか
  * ITのパフォーマンスは何か
  * IT統制は
* 社会の変化に対応する
* 常にリスクを認識しているか
  * リスクを低減できるか
  * 業界自主規制による安全なITとは
  * リスクに対する説明は十分か
* システム監査と内部統制
* 経営者にも一言（経営者の不正）