ITの利用の拡大と統制

Expansion use of IT and expand control by governing body to achieve its governance of IT

システム監査学会
ITを利用したガバナンス研究会
2012.06.08
第26回研究大会

アジェンダ

1. 2011年活動状況
2. 企業はどこまで統制すべきか
3. 企業のリスクと統制
4. リスク要因
5. 企業のIT利用の統制
6. 企業の従業員の統制
7. 今後のITの統制

1. 2011年活動報告

* プロジェクト名の変更
  内部統制研究会⇒ITを利用したガバナンス研究会

* 隔月ペースの会合
  11月10日／12月13日／3月26日
* メール等を使ったコミュニケーションの活用

* 登録メンバー　11名

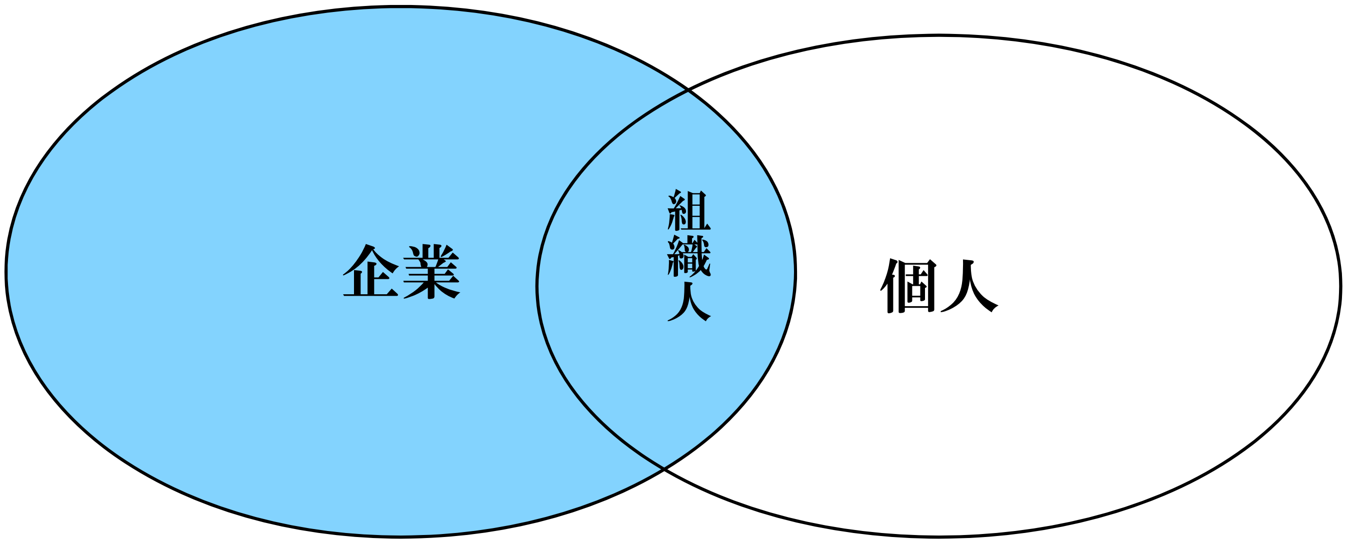
2. 企業はどこまで統制すべきか

- 企業はネットワークを通じて、外部と繋がっているが、自社の従業員や外注先の従業員のSNSによる情報提供により企業が守るべき情報の漏えいが起きる(アルバイトが有名人来店情報をTwitterに投稿etc.)
- 企業の主要な業務が依存している他社システム(含むネットワーク)がダウンすることにより、自社業務が停止する(クラウド環境が利用できなくなるという障害が12時間にわたって発生)

3. 企業のリスクと統制

* 自分だけでは生きられない
* 社会インフラ（ITは社会インフラ）への依存
* 従来の内部統制だけでは統制が及ばない領域に影響がでる（内部とは何か）
* 他社のシステム復旧を待つしかない
* 通信の遮断の損害賠償は通品費の範囲内（SLAの成り立ち：通信事業者を守る目的）

3. 企業のリスクと統制



4. リスク要因

- 社会的な要因が大
  - 社会基盤の変化
    - 所有ではなく利用することによる利益、ただ、支配できない
  - 情報拡散（ここだけの話はここだけではない）
    - SNSにより、社会に向けて個人情報、企業情報を発信（Twitterを営業に活用する企業もあるが、その反面、簡単に企業の機密情報や顧客個人情報が漏えい）
    - SNSの利用の心得が必須？（全世界に繋がっている認識が薄い）

4. リスク要因

* IT提供者の意識と倫理観

  * Googleプライバシーポリシーの波紋
  * Privacy Policy - Policies & Principles – Google Last modified: March 1, 2012
  * http://www.google.com/policies/privacy/

  * 総務省の通知
  * http://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000117.htm

  * 経済産業省の注意喚起文書

  * http://www.meti.go.jp/press/2011/02/20120229011/20120229011.html

  * 「個人情報の保護に関する法律(平成15年法律第57号)」「電気通信事業法(昭和59年法律第86号)における通信の秘密の保護等に関する規定」をそれぞれ順守することが重要|
  * 利用者にわかりやすい説明を

  * 自分の個人情報だけではなく、通話相手の情報も収集される?

5. 企業のIT利用の統制

* 他社に依存するリスクの低減,受容、回避
  * 他社への依存度合は気がつかないうちに拡大？
    * サプライチェーン（東日本大震災）
    * 通信網の遮断
  * ITは社会インフラ（言いふらされていること？）
    * どこにリスクがあるか
* 企業最大のリスクはリスクを認識できないこと

5. 企業のIT利用の統制

* 正確な情報は提供されるか
  * 多くの提案は利益のみ
  * 技術の進化
  * 統制のコスト
* ITの提供業者の価値観・倫理観は
  * アンドロイドの課題
  * 新技術は統制を入れているか
* もともとITはブラックボックスだが
  * 技術革新の速度が加速する

6. 企業の従業員の統制

* 企業はどこまで、個人を統制できるか
  * 会社内部では制御できても個人の生活まで制御できるか
  * どこまでが、社外秘か
* どこまでが個人の意見でどこからが企業の意見か
  * 個人のHP記事が就職先企業への攻撃材料に
  * 会社人としての姿勢が個人にも問われる？
* 古くて新しいが・・・・
  * 情報の拡散の範囲と速度は大幅に拡大
  * 意図しない情報漏えい

7. 今後のITの統制

- ITを利用するリスクをどう認識するか
  - ITはわからないではなく、知る努力が大切
  - リスクとベネフィットのバランス
- 社会の価値観、倫理観をどうとらえるか
  - いままでの経験だけでは判断ができない情報の提供（公的機関の広報：教育）が重要
- 社会の流れは止められない
  - リスクを受容、削減して利用
- 業界自主規制による安全なIT
  - わかりやすい説明が大切