システム監査学会第29回研究大会
法とシステム監査研究プロジェクト成果報告

情報漏えい発生時の
レピュテーショナルリスクと危機管理
～システム監査の視点から

株式会社ラック／東京電機大学
久山真宏

「法とシステム監査」研究プロジェクト

- **主査：稲垣隆一　　副主査：黒澤兵夫**
- **概要**

**　システム監査は、情報システムの企画、開発、運用、保守に関する現実的な課題の予防、解決に、いかに役立つのか？　クラウドコンピューティング、ソーシャルネットワーク、ビッグデータの取扱い、マイナンバー制度など現下の課題、判決例に表れた紛争事例、現下のシステム上の課題を素材に検討し、その成果を生み出すシステム監査の技法の開発、管理基準の改訂の提案などに結びつける。**

プロジェクトメンバー

指名	所属	備考
荒木哲郎	弁護士・システム監査技術者	
稲垣隆一	稲垣隆一法律事務所・弁護士	主査
植野俊雄	ISU	
黒澤兵夫	TAKE国際技術士研究所	副主査
瀧澤和子	早稲田大学	
成田和弘	システム監査技術者，CIA，CISA	
芳仲宏	東京地方裁判所	
久山真宏	株式会社ラック，東京電機大学	発表

主に五十音順

発表テーマ

情報漏えい発生時のレピテーショナルリスクと危機管理 ～ システム監査の視点から

- **セキュリティインシデントにおける企業の情報漏えいが多発している。それに伴い、情報漏えいが発生した際に起こる問題が顕在化してきている。発生しえる問題の中でも、当該企業への信頼度低下（悪評）による企業への影響（被害）は、利益の低下、最悪の場合は企業が倒産になる危険性がある。そこで、事例を基に情報漏えい発生時における企業の危機管理とリピテーショナルリスクマネジメントについてシステム監査の視点から考察する。**

Agenda

- レピュテーショナルリスク
- 要因と事例
- システム監査の視点
- まとめ

レピュテーショナルリスク

様々な事業リスク

- 市場リスク
- 信用リスク
- 財務リスク
- 不動産リスク
- 自然要因リスク
- 人的要因リスク
- 制度的リスク
- 情報システムリス
- 業務リスク
- 技術・製品要因リスク
- レピュテーショナルリスク

レピュテーショナルリスク

レピュテーション

- **企業に関する肯定的・否定的な評価・評判**

レピュテーショナルリスク(レピュテーションリスク)

- **企業に関する否定的な評価・評判が世間に周知されることで企業の信用やブランド価値等が悪化し、結果的に損失を被るリスク**

出典：先進企業から学ぶ事業リスクマネジメント実践テキスト
http://www.meti.go.jp/policy/economic_industrial/report/downloadfiles/g50331i00j.pdf

要因と事例

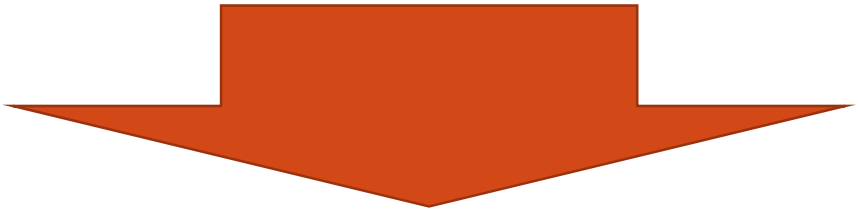
要因

- セキュリティインシデント
  - 情報漏えい
  - マルウェア感染
- 企業や製品に対する口コミや噂話
  - 製品の不具合
  - 食品偽装
- 経営者・従業員の行動
  - 社会道徳上不適切な行動
  - 法律・法令・規則違反

要因と事例

経営へのダメージ

- **賠償金**
- **裁判コスト**
- **株価の低下**
- **顧客離れ**



インシデント後の対応によって増幅
（レピュテーショナルリスク）

要因と事例

事例

- **情報漏えい**
  →内部不正による情報漏えい
- **食品偽装**
  →賞味期限や産地の偽装
  →調理日時の改ざん
- **データ改ざん**
  →性能評価基準を満たさないデータ改ざん

要因と事例

危機事態に対する対応の失敗

- **不誠実な経営体制**
  - **記者会見を開くも詳細が不明確**
  - **再発防止策や反省が見られない**

- **隠ぺい体質**
  - **事実と異なる情報やデータの公表**

システム監査の視点

危機管理に対応する準備が出来ているのか？

✓ **要点**

- **倫理綱領や行動指針の策定と周知徹底**
  （－経営トップの率先垂範）
- **オープンなコミュニケーションの確立**
- **正しい行動が正当に評価される評価制度**

システム監査の視点

危機管理対応の実施

- NIST「重要インフラのサイバーセキュリティを向上させるためのフレームワーク」の視点を追加
  - 企業に関する評判等の情報を収集
  - エスカレーションルールを整備
  - リスクの兆候となる情報を早い段階

➡ レピュテーショナルリスクマネジメント

システム監査の視点

DE.DP-1: **説明責任を果たせるよう、検知に関する役割と責任を明確に定義している。**

RS.CO-1: **対応が必要になった時の自身の役割と行動の順番を従業員は認識している。**

RS.CO-2: **定められた基準に沿って、イベントを報告している。**

RS.CO-3: **対応計画に従って情報を共有している。**

RS.CO-4: **対応計画に従って、利害関係者との間で調整を行っている。**

RS.CO-5: **サイバーセキュリティに関する状況認識を深めるために、外部利害関係者との間で任意の情報共有を行っている。**

RC.CO-1: **広報活動を管理している。**

RC.CO-2: **イベント発生後に評判を回復している。**

RC.CO-3: **復旧活動について内部利害関係者と役員、そして経営陣に伝達している。**

出典：重要インフラのサイバーセキュリティを向上させるためのフレームワーク

https://www.ipa.go.jp/files/000038957.pdf

まとめ

危機管理対応の実施を提案

- **エスカレーションルールの策定**
  →経営者が事実把握
- NIST**「重要インフラのサイバーセキュリティを向上させるためのフレームワーク」の視点を追加**
  →悪評（不誠実な経営体制、隠ぺい体質）に対するレピュテーショナルリスクマネジメント

ご清聴ありがとうございました

