自組織に最適な情報セキュリティ対策

（中小組織を対象とした情報保護内部統制）

システム監査学会　第25回研究大会2011年6月10日
情報セキュリティ専門監査人＆情報セキュリティ研究プロジェクト
合同報告

報告者　川辺良和（情報セキュリティ専門監査人）
（ISMS主任審査員・システム監査技術者）

内　　容

Ⅰ．中小組織の情報セキュリティ管理体制の問題点

Ⅱ．自組織に最適な情報セキュリティ対策の取り組み

Ⅲ．東日本大震災から教えられること

Ⅰ．中小組織における情報セキュリティ管理の問題点

- 必要に迫られた都度個別の対応
- 複数のマネジメントシステムが乱立
- 認証取得が目的化している。
- 企業としてのリスクマネジメントのバランス欠如
- 情報セキュリティ管理の取り組みが役に立っていない

Ⅱ-1. 自組織に最適な情報セキュリティ対策の必要性

- 要求事項への対応：過剰対応になりがち
- 内部監査、委託元監査、審査などへの対応で手一杯
- 規格・規制・顧客要求等の他律的な活動からの脱却
- 主体的・能動的な情報セキュリティ対策
  →自組織に最適な情報セキュリティ対策へのシフト

Ⅱ-2. 自組織に最適な情報セキュリティ対策の考え方

＜経営者＞

- 事業上のリスクとして情報セキュリティの重大性の認識
- 事業継続の観点からリスク対応計画としての情報セキュリティ

＜推進者＞・・・適切な対策の実施と具体的な説明

- バランスのよい管理策
- 現場の運用を考慮した管理体制の構築
- 認証取得の場合も1つの手段、それを目的としない

＜現場＞

- 日常の業務プロセスの中で情報セキュリティ体制を実現
  （情報保護の内部統制）

Ⅱ-3. 自組織に最適な情報セキュリティ対策の取組み

- 組織全体のリスクマネジメントの中での情報セキュリティ
  - （1）顧客・事業上の要求、組織を取り巻く社会環境
  - （2）事業環境の特性
    - ・保護すべき主要な情報
    - ・情報システム
- （3）組織特性を考慮した情報セキュリティ対策の有効性・効率
  - ・組織目的、公共性、他組織との関係～
  - （4）リスクアセスメントと統制方法決定・統制活動
    - ・重要な情報資産の集中管理
    - ・モニタリングの重要性
  - （5）参考とする管理策のモデル

Ⅱ-4. 自組織に最適な情報セキュリティ対策の取組み

●企業全体のリスクマネジメントの中での情報セキュリティ

・請負業務を主体とした情報保護体制

・現場業務から具体的な事業上のリスクを識別する。
（事業継続への影響の大きさからの優先順位付け）

＜参考＞

（1）個人情報保護マネジメント

（2）情報セキュリティマネジメント

（3）ITサービスマネジメント

（4）事業継続マネジメント　など

Ⅱ-5. 自組織に最適な情報セキュリティ対策の取組み

●重要な推進組織

・事業上のリスクを踏まえた情報セキュリティ対策
→具体的な発生リスクに現実的にどう対応するか
（例：自然災害に対して、バックアップ情報の遠隔地保管）

・現場が実際に継続的に運用できる対策
→一過性ではなく、遺伝子として引継ぐ組織
→過剰で、形式的な対策として終わらせないために）

●重要な推進組織の責任者：

適切な情報セキュリティ対策の実施を具体的に説明する

Ⅱ-6. 自組織に最適な情報セキュリティ対策の取組み

●情報セキュリティ対策の取組みの証明

・発注者サイド、契約者からの要請

→受託者サイドは要請への対応について説明責任を果たす

・例1：定期的モニタリングや内部監査

・例2：各マネジメントシステムの認証取得
（プライバシーマーク、ISMS、ITSMS、BCP～）

→審査員に適切な対策を説明できる・・・双方にとってプラス

・例3：自己宣言（ISO14000、三島市の事例）

・説明責任を果たす：当社は適切な情報セキュリティ対策を講じていますと説明できるかどうか

Ⅲ．東日本大震災から教えられること

- 携帯電話が使用できずタイムリーな情報伝達ができなかった。
- 緊急時対策発生時の行動指針となっていなかった。
  （発生後に考えたのでは抜け、遅れが甚だしい）
- 自家発電等の予備電源や無停電源装置テスト未実施は多い
- 戻せなくなる状態を回避するためにオフサイトバックアップ必須
- 停電：電子媒体のBCPを出力できない。
- 重要なサプライーチェーンシステム：自社だけでない取引先
- 今回の経験を危機管理マニュアルに生かす→経験者の文書化
- リスク対応計画：発生確率が1000年に1度も発生前提の対応
- 想定外への対応こそが緊急時対応計画・・・・