

HRO Report

インタビュー調査編

明治大学 経営学部

中西 晶 山下 充

宇田川元一

高木俊雄

星 和樹



2006/05/29

MEIJI UNIVERSITY

目次

1. セキュリティに関して
 - 1-1 人的セキュリティ
 - 1-2 技術的セキュリティ
 - 1-3 組織的セキュリティ
2. 情報共有に関して
 - 2-1 電子媒体などの活用
 - 2-2 文書化
 - 2-3 フェイス・トゥ・フェイス
3. 人材育成に関して
 - 3-1 Off-JTの積極的活用
 - 3-2 現場での学習
4. まとめーインタビュー調査から見る今後の課題ー

2006/05/29

MEIJI UNIVERSITY

1. セキュリティに関して

1-1 人的セキュリティ

- 掌、指紋認証など生態認証方式を採用
 - セキュリティレベルが設定しており、登録されたスタッフ以外の入室不可
- 制服の色分け
 - 担当分野によって色が異なる
 - ⇒このような方法は、空母などでも見られる
- 正社員で運営
 - 非正社員は簡便な業務に限定
 - 正社員採用時には技術的スキルのみならず、倫理的判断力もチェック

1-2 技術的セキュリティ

- 基幹網のみならず末端網まで二重化
- 発生するイベントのフィルタリング
 - 重要なものだけを報告
- セキュリティ監査を導入
 - 外部からの攻撃を依頼
- エスカレーション・ルールを採用
 - 技術的難易度+顧客へのフィードバックで設定

1-3 組織的セキュリティ

- 情報セキュリティ委員会を設置
 - 情報セキュリティ管理責任者(CISO)
 - ISMS適合性評価制度
 - BS7799
- 業務のモニタリング
 - 厳重な入退出管理を行い、業務エリアとは隔離
 - 専任スタッフが24時間365日体制でオペレーターをチェック

2. 情報共有に関して

2-1 電子媒体などの活用

– メール・メーリングリスト

- インシデント情報の共有
- 簡単な問題解決の指示

– 電話・電話会議

- 緊急性が高いもの
- メールでは時間がかかるもの

– チケットシステム

– ホワイトボード

- 当初は用いられていなかったが、物理的な情報共有
⇒ディスプレイ上の情報は技術者にとってもリアリティが薄く、ホワイトボードによる情報共有は依然として有効であるとの認識

2-2 文書化

– 手順書の作成

- 失敗例の重視
 - 業務手順をマニュアル化するだけでなく、失敗例の文書化をおこなう

– 再現試験と報告書の作成

- 問題が生じた件に対する再現試験を実施し、その試験結果をまとめる(場合によっては部門間共有する)

2-3 フェイス・トゥ・フェイス

– 業務時間の重複

- シフト交代時に約30分程度の重複時間をつくる
 - 特に重要事項について口頭による引継ぎが行われる
 - そのほかに関しては電子媒体(メールや社内WEB)などを利用

– システムセキュリティ会議の開催

- 脆弱性情報の共有、解決にかかった時間などの報告

– 部門内・部門間ミーティング

- 品質会議やレビュー会議など

– MBWA (Management By Walking Around)

- マネジャーが他部門に積極的に顔を出す

3. 人材育成に関して

3-1 Off-JTの積極的活用

- 研修
- JANOG等への参加
- 社内設備の活用
 - ・ いつでも自由に使えるPC、仮想システムを設置
 - ⇒ 勤務時間外(休憩時間や休日)に利用することにより、専門性を高める

3-2 現場での学習

- ベテランと新人
 - 高い専門性を持った人と新人を一緒のチームにする
 - ⇒現場での学習を促進
- ローテーション
- 演習(エクササイズ)

4. まとめ

—インタビュー調査から見る今後の課題—

4-1 一極集中

- 専門性が高いため、スキルの差が生ずる
 - ⇒問題に対処するためのキーパーソンが発生
 - ⇒その人がいないと解決までに時間がかかる

4-2 人材育成

- ゼネラリストとスペシャリスト
 - 単一業務のみに秀でた技術者ではなく、様々な業務を遂行できる技術者が必要
 - 他部門間の調整や、全体的把握ができる人材が必要
- 定着率
 - 技術者の定着度が低い
- Off-JTとOJTとの関連
 - Off-JTでの研修とOJTを結びつける
 - ⇒その教育方法を充実させることが必要

4-3 開発と運用の分離

- サービス提供者に顧客からのレスポンスがこない
 - ⇒部門がクローズになりやすい
 - ⇒技術的専門性のみ高まることがある