JSSM　ITリスク研究会

ITリスクの落とし穴
- ある企業の事故事例からの反省 -

2008年10月4日

中村　達

JSSM
ITリスク研究会

今日の話の内容

- A社の事故事例
  - 事業概要
  - 情報セキュリティ対策への取組
  - 事故の概要
  - 事故の初期対応
  - 事故の影響
- まとめ(私の研究課題)

JSSM　ITリスク研究会

A社の事業概要と
情報セキュリティ対策への取組

JSSM
ITリスク研究会

A社の事業概要

名　称	株式会社　A社
業　種	SI、ソフトウェア開発 情報システム運用
社員数	約1500名
協力会社員数	約1500名
事業所	非公開
センター	非公開

JSSM
ITリスク研究会

A社提供サービス内容

- 情報処理
  - ✓情報の入力、処理、印刷、加工
  - ✓ホスティング
  - ✓ハウズイング
- SI、システム開発
  - ✓自治体
  - ✓民間
- 情報セキュリティ・サービス
  - ✓ISMS取得コンサル
  - ✓監査コンサル

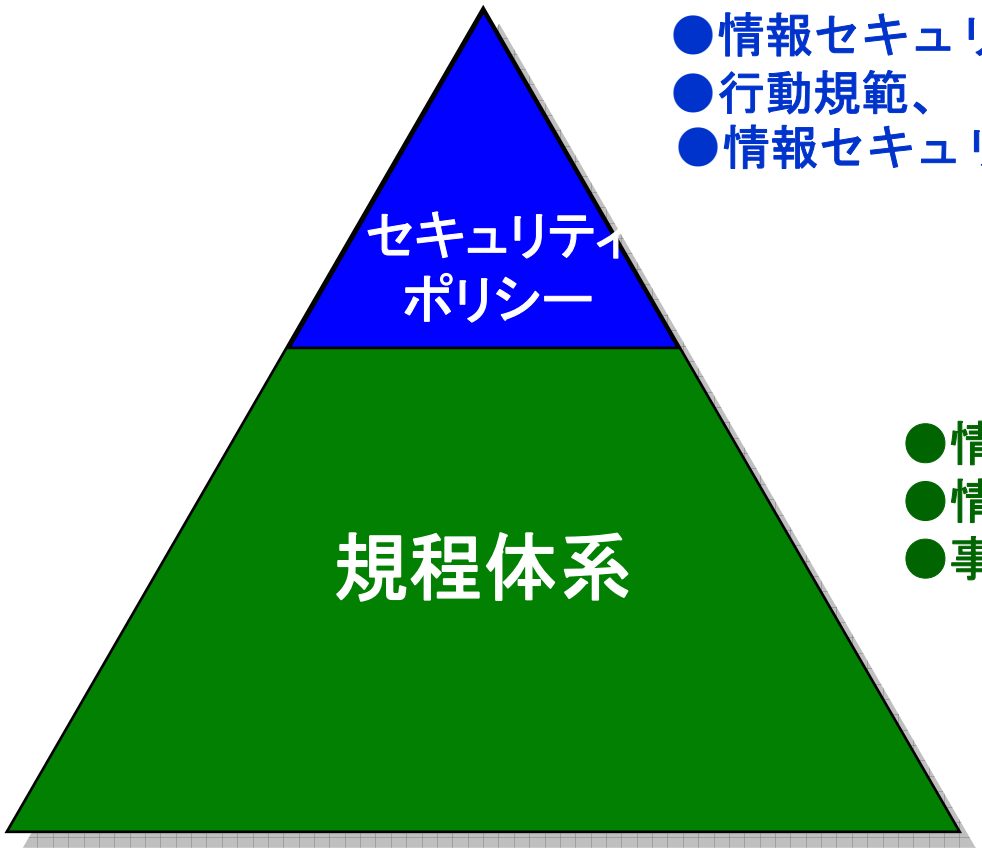
JSSM
ITリスク研究会

A社のセキュリティ関連公的資格

- 情報セキュリティ・マネジメント
  適合性評価制度(ISMS)
- プライバシー・マーク
  適合性評価制度(PM)

JSSM
ITリスク研究会

情報セキュリティポリシー体系



●情報セキュリティ基本方針
●行動規範、
●情報セキュリティ対策基準

公開

●情報セキュリティ実施規程、
●情報セキュリティ実施手順書
●事業所・部門固有手順

JSSM
ITリスク研究会

リスク管理統括委員会の設置

社長を委員長とするリスク管理統括委員会を設置、その配下で3委員会を運営

JSSM
ITリスク研究会

委員会活動

JSSM
ITリスク研究会

教育研修・監査

- 社外講師による集合研修、部門別集合研修、eラーニングによる全員教育等を実施
- 監査室が年１回以上、部門監査を実施

教育	・ISMS、PM　集合教育 ・ISMS、PM　eラーニング ・部門別社内研修会（事業所・部門固有手順等の周知徹底） ・外部講師による研修会（年複数回開催) ・事故事件ニュース（世の中の事故事件を随時発行）
監査	・ISMS、PMの情報セキュリティ監査 ・特命監査（テーマを決めた監査）

JSSM　ITリスク研究会

事故の概要と初期対応

JSSM
ITリスク研究会

事故の概要

事故、事件発生

日付：〇〇〇〇年9月〇日
時間：15時30分頃
場所：関東地区のX市内
　　ごみ集積所

　関東地区のX市の家庭ゴミ集積所でX市の個人情報が含まれた書類が見つかった。

JSSM
ITリスク研究会

当面の関心ごと

事故か、事件か
誰が

２次被害は発生するか

JSSM
ITリスク研究会

初期対応

非公開とさせていただきます。

事故の影響

JSSM
ITリスク研究会

事業に及ぼす影響

非公開とさせていただきます。

JSSM
ITリスク研究会

社内への影響

非公開とさせていただきます。

まとめ(私の研究課題)

JSSM
ITリスク研究会

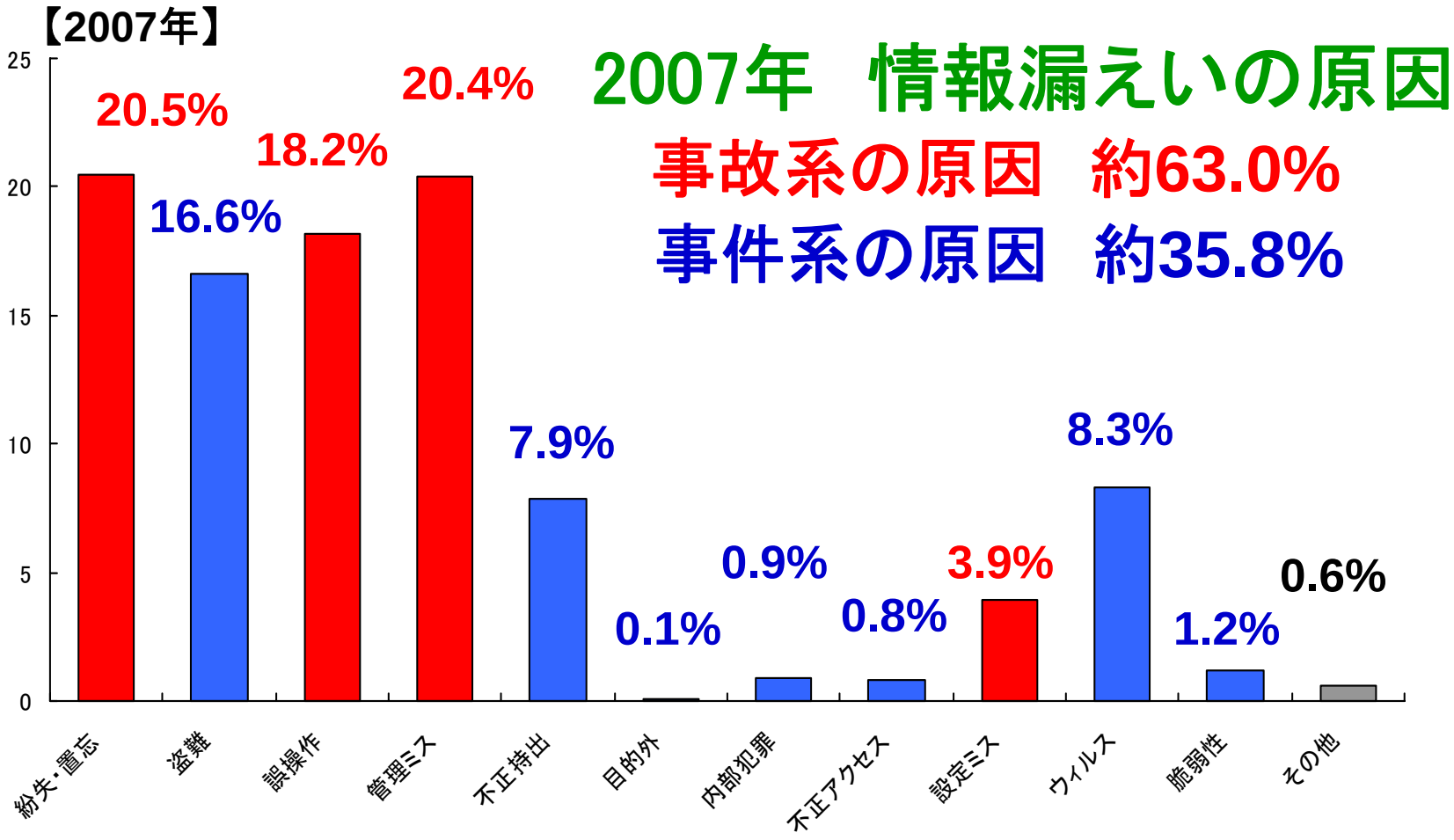
研究課題･その１

■セキュリティ事故を起こさないためには、何をすればよいか

ISMSを取得することだけが、セキュリティ事故を防止するための対策になっていないか。本来は何をしなければいけないか。

JSSM
ITリスク研究会

情報漏えいの原因



日本ネットワークセキュリティ協会「個人情報漏えいインシデントに関する調査報告」より
http://www.jnsa.org/result/index.html

研究課題･その２

■事故系の情報漏えい対策は、何をすればよいか

情報セキュリティ対策というと「ハイテク」のハッカー等が起こす事件系の対策に注目してしまうが、大半は一般従業員の「ケレスミス」が原因である。こちらへの対策が、あまり研究されていない。

研究課題･その3

■事故による影響は、社外、社内の両方に出る

一番の被害者は、個人情報が漏えいした当事者であるが、事故を起こした従業員も被害者である。ITリスク事故･事件が発生したときの被害者救済の方法について、更なる研究が必要である。