情報セキュリティーと“例外”

Exception Measures as an Information Security Policy

村﨑康博・法制倫理研究部会・情報セキュリティ大学院大学

Whether information security policy includes exception measures〃 decide the response time for incident in the organization is true.
The exception measure is one of the barometer measuring the organization governance situation.

情報セキュリティポリシーへの満足度 約“80%”は安心か

（仮定）

背景

- 情報セキュリティに関する規定の策定・実施は，組織（企業や官庁等）では必須施策
- 規定から逸脱する事象にも“例外規定”を事前に設定してリスク回避・対処を実施

- 具体的な事象において、どの程度まで例外措置を規定するか？
- 例外規定の策定・措置の実施を適正に評価できるか？

アンケート紙面上での主観評価実験を実施、評価数値・定量化を試算

NISC：政府機関の情報セキュリティ対策のための統一基準群

- 情報セキュリティに関わる内部規定に例外措置の手順と担当者を含めるよう記載
- 重要インフラ指定機関・金融関連機関等一部の民間組織でも参考・導入

ISMS：ISO/IEC27002 12.1運用の手順及び責任

- 例外措置を認めた場合は、例外規定として明確に規定。
- 運用変更においては変更管理を徹底

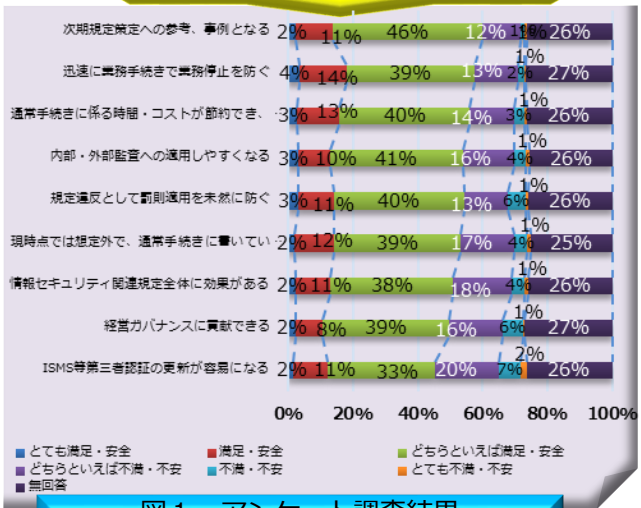

図１　アンケート調査結果
【設問23】：例外措置の主観評価

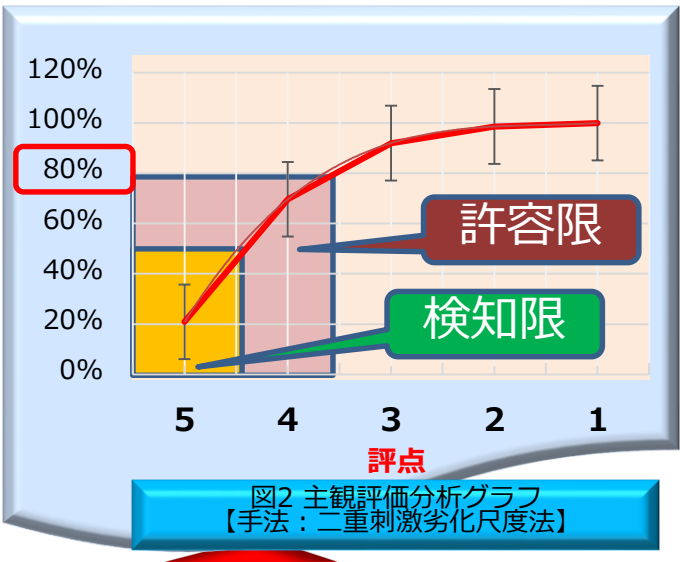

図2 主観評価分析グラフ
【手法：二重刺激劣化尺度法】

評点	5	4	3	2	1
アンケート回答選択肢	とても満足・安全／満足・安全	どちらといえば満足・安全	どちらといえば不満・不安	不満・不安	とても不満・不安
二重刺激劣化尺度法回答選択肢	気にならない	どちらかといえば気にならない	どちらかといえば気になる	気になる	とても気になる