五井　孝

大和総研ビジネス・イノベーション　内部監査部長

情報処理技術者試験委員

公認情報システム監査人（CISA）、システム監査技術者

＜略歴＞

大手システム会社での開発、営業を経て、大和総研入社

内部/外部監査、コンサルティング、情報セキュリティおよびリスクマネジメントの統括部門を経て、現在に至る

# 情報セキュリティにおける内部監査の視点とは？

すべての資産は、明確に識別する。
また、重要な資産すべての目録を、作成し、維持する。
【情報セキュリティ管理基準　Ⅳ. 管理策基準　3.1.1】

目録を閲覧した結果、一部に登録、更新の漏れが見つかったら・・・・

＜指摘事項＞
目録に漏れがないように登録し、更新すること。

この指摘は正しいでしょうか？

# “準拠性”の指摘は「いたちごっこ」

- 業務プロセス上に乗っていないルールは、
  守らなくても困らない

  ＝　後回し

- 業務効率を下げるルールは守られない

  ＝　”絵に描いた餅”

# 内部監査で個別最適に“メス”を入れる！

業務との関わりはどうなっているのか
（業務の中で“孤立”していないか）

ex. ・なぜ、目録に登録や更新漏れがあっても
困らないのか？
・資産のセキュリティを守るために、目録は
具体的に何に使われているのか？
・日常の業務プロセスに目録は登場している
のか？

→ 「情報セキュリティ基準にあるから目録を作成する」
という理由だけなら、“否定”することも必要・・・・