くたばれ！！

（みせかけの）PDCA

Agenda

- ちまたにはびこる見せかけのPDCA
- 見せかけ化の原因は？
- 基本から見直そう
- インフラ＆ガバナンスのためにCISSPができること

ちまたにはびこる見せかけの PDCA

事例１：Show Stopperな監査部門

- **現場の実情に合わないポリシーやルール**
- **「ポリシーはこう書いてある」的な内部監査指摘**
  - **形式的なルール違反の指摘**
  - **そもそも実情に合わないルール**

事例２：自動アップデート導入を阻止する社内政治力学

- **社内にWindows Updateの自動化を導入しようとしたシステム部門・・・**
  - **制御用に使ってるPCが影響を受けるかもしれない**
  - **PCで使ってるアプリ（クラサバ？）が影響を受けるかもしれない**
  - **そもそも会社全体でPCの台数・種別・OSが把握しきれていない（部門で独自に購入するものは把握できない）**
- **結局、現場部門の反発に遭って導入計画は頓挫した。**

事例３：２０世紀の遺物のルール

- **添付ファイルはパスワードつけて別メールで送信**
  - **どちらのメールも同じように盗聴されたら無意味**
  - **現在のネットワーク環境では、別のメールだからといって別の経路を転送されていく可能性は低い**
  - **届いた後、受信者側での保護（受信者側社内など）を考えるなら受信者が自ら暗号化すれば良い（パスワードを平文でメールする必然性はない）**

- **ところが「メールに添付するファイルはパスワード付きzipにして、パスワードは別メールで送る」ことが社内ポリシーに書いてあったりする**

事例４：現場が委縮するようなルール

- **ペナルティがあまりに厳しいので現場がビクビクしながら仕事している感じ・・・**
  - **宴会があるときは会社に帰ってPCをしまってから行くのがルール化されている**

- **結果として問題が可視化されてないので、正常にPDCAが回せるはずがない**

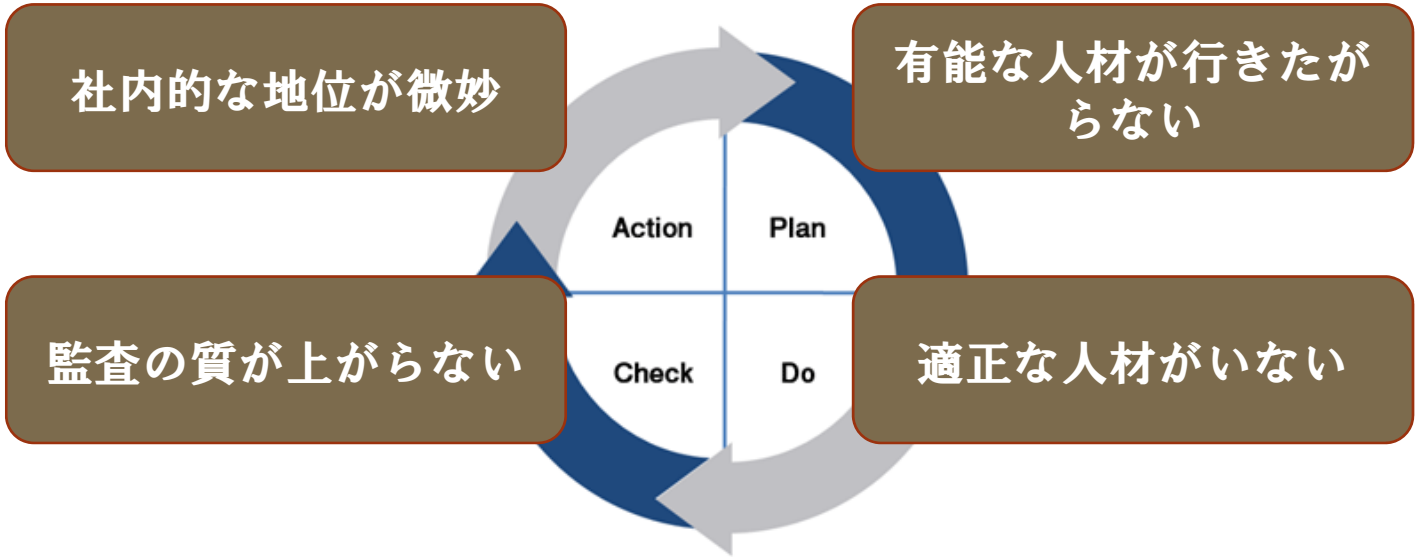
見せかけ化の原因は？

本質を見失った管理部門(1)

- 形式的な内部監査をやりすぎていて、現場からはビジネスを阻害していると思われがち
  - 業務・ビジネスがきちんと理解できていない
  - 対象となるリスクを正しく理解できていない
  - 業務に合わないヘンなルールを作る
- 結局、内部監査部門が現場から信頼されない
  - 「ヤバい情報」が現場から伝わらない、隠される）
  - 社内組織の中での影響力がないので、有効な体制構築ができない
  - 結果としてPDCAは適切に回らない（ISMSは継続審査の前にバタバタと・・・）

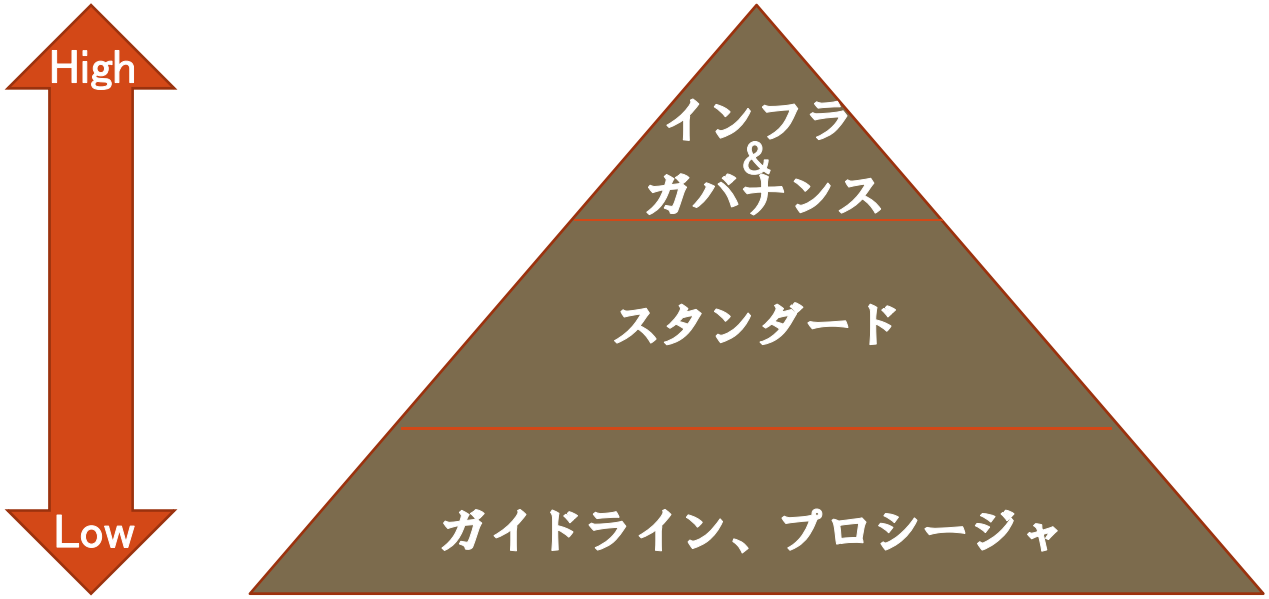
本質を見失った管理部門(2)

- **内部監査部門に適正な人材が配置されているか**
  - **監査やセキュリティのプロはいるか？**
  - **適切なスキル習得や継続教育のしくみはあるか？**
  - **内部監査部門自身にモチベーションはあるか？**
- **負のスパイラルに陥っていないか**



現実に合わない体制

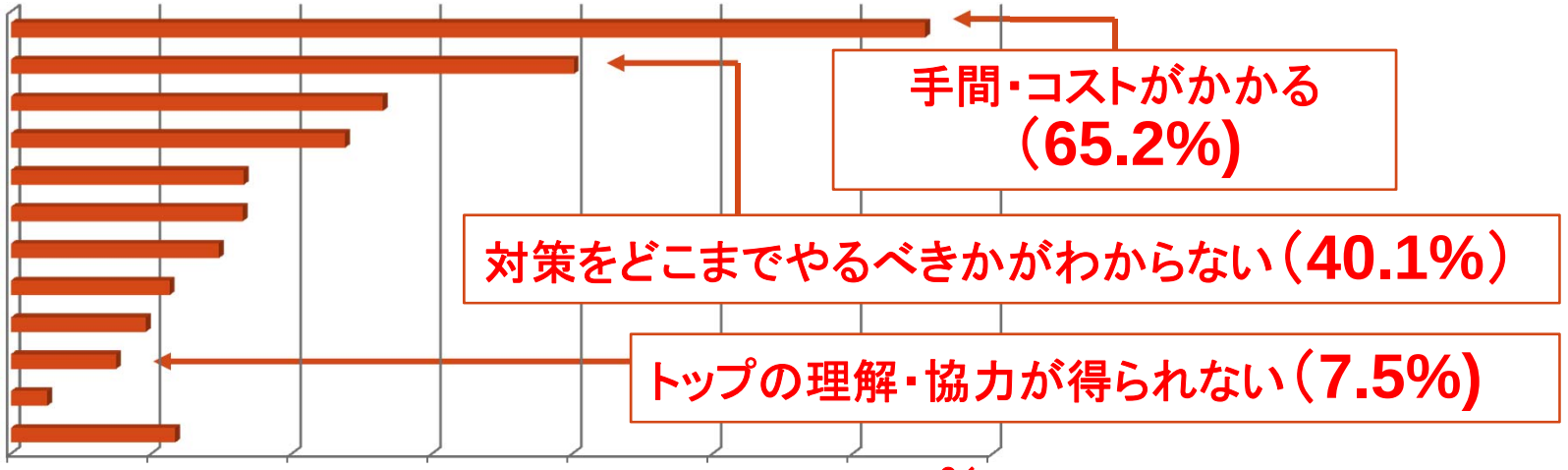
- **指針となるインフラやガバナンスはぐたぐた**
  - **部門独自のワークフローが混在**
  - **定義すべきポリシーがない**
- **現場に即していないガイドライン、プロシージャは存在**



基本から見直そう

結局はガバナンスの問題

- **経営者は内部監査部門や、その部門が支える事業としてのリスクコントロールをどう考えているか**
  - **ITが良くわからない社長「IT担当役員に任せた」**
  - **ひとたび重大な問題が起きれば謝罪するのは社長**
- **でもこんな数字も・・・**



出典：経済産業省・平成22年情報処理実態調査

ガバナンスをインフラとして実装するには・・・？

- **業種・業態などでITに対する依存度が違うので、それに合わせたリスクコントロールとそのためのIT投資を考える・・・のがCISSP？**
- **社長がわかる言葉で、社長が関心を持つアプローチで、リスクを語る・・・のがCISSP？**
- **内部監査体制を改善できる・・・CISSP?**
  - **現場の人も監査期間中、監査チームのメンバーに入れて、「現場のための内部監査」を実行する？**

標準化は大事だけれども・・・

- CISSPであれば、**それぞれのインダストリー・会社に適した提案・アクションができるはず？**

インフラ＆ガバナンスのために CISSPができること

事業会社に出て行こう

たとえ困難に見舞われても・・・

ビジネスに強くなろう

「日々勉強」！？

個性と適性を活かして・・・。

というわけで、まずは第一部 完