情報セキュリティとシステム監査に対する経営者の認識の現状と課題

システム監査学会　第26回研究大会　2012年6月8日

情報セキュリティ専門監査人＆

情報セキュリティ研究プロジェクト合同研究会

報告者：NECソフト株式会社　ソフトサービスセンター

高野　美久（システム監査技術者）

（ISMS主任審査員・ITコーディネータ）

システム監査学会 第26回研究大会 情報セキュリティ専門監査人＆情報セキュリティ研究プロジェクト 合同報告

はじめに

我々は、過去2年「経営者」に対して、「自組織に最適化したリスクベースによる情報セキュリティ対策の実践」について提言してきた。

企業活動とリスクマジメント
～リスクベースによる情報セキュリティの実践～

“Business Operations and Risk Management ”
-Implement Risk Based Information Security-

システム監査学会　第24回研究大会　2010年6月4日

情報セキュリティ専門監査人部会＆情報セキュリティ研究プロジェクト
合同報告

発表者：　優成監査法人　鳥越真理子, CISA, CISM

自組織に最適な情報セキュリティ対策

（中小組織を対象とした情報保護内部統制）

システム監査学会　第25回研究大会2011年6月10日
情報セキュリティ専門監査人＆情報セキュリティ研究プロジェクト
合同報告

報告者　川辺良和（情報セキュリティ専門監査人）
（ISMS主任審査員・システム監査技術者）

2011年度は、当合同研究会では、以下の内容を検討。
①「事業継続と情報セキュリティ」
②「情報セキュリティとシステム監査」
今回「情報セキュリティとシステム監査」について研究成果を報告する。

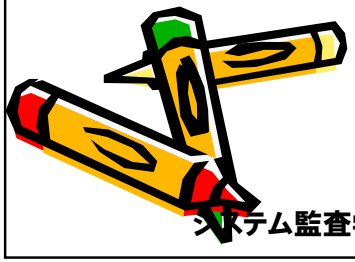
アジェンダ

1. システム監査の現状

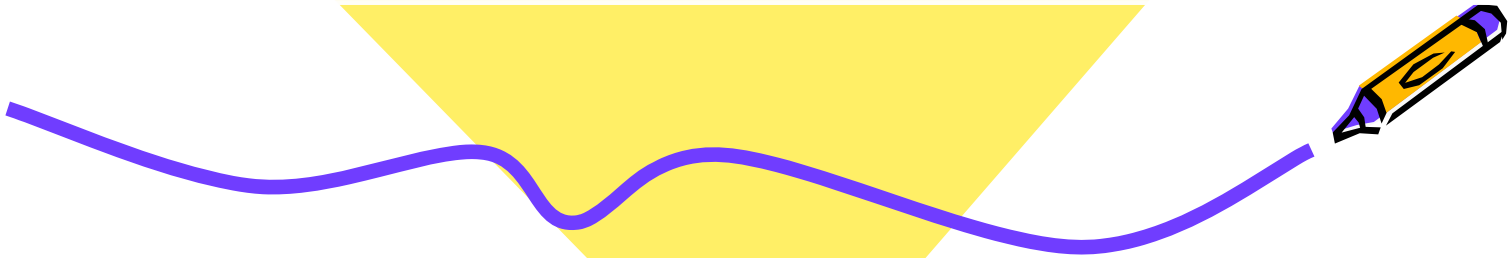
2. システム監査に対する経営者の認識

3. 経営者の心理分析

4. システム監査人の役割



1. システム監査の現状



システム監査の現状

① 「J－SOX内部統制に伴う状況評価」、「情報セキュリティ監査」、「ISMS監査」等を実施した組織は耳にしたことがあるが、金融機関を除き、***「システム監査」を実施したという組織は聞いたことはない***

② 書店に行っても、「情報処理技術者試験のシステム監査技術者試験」対策本以外、***「システム監査」に関連する本が、置いていない。***

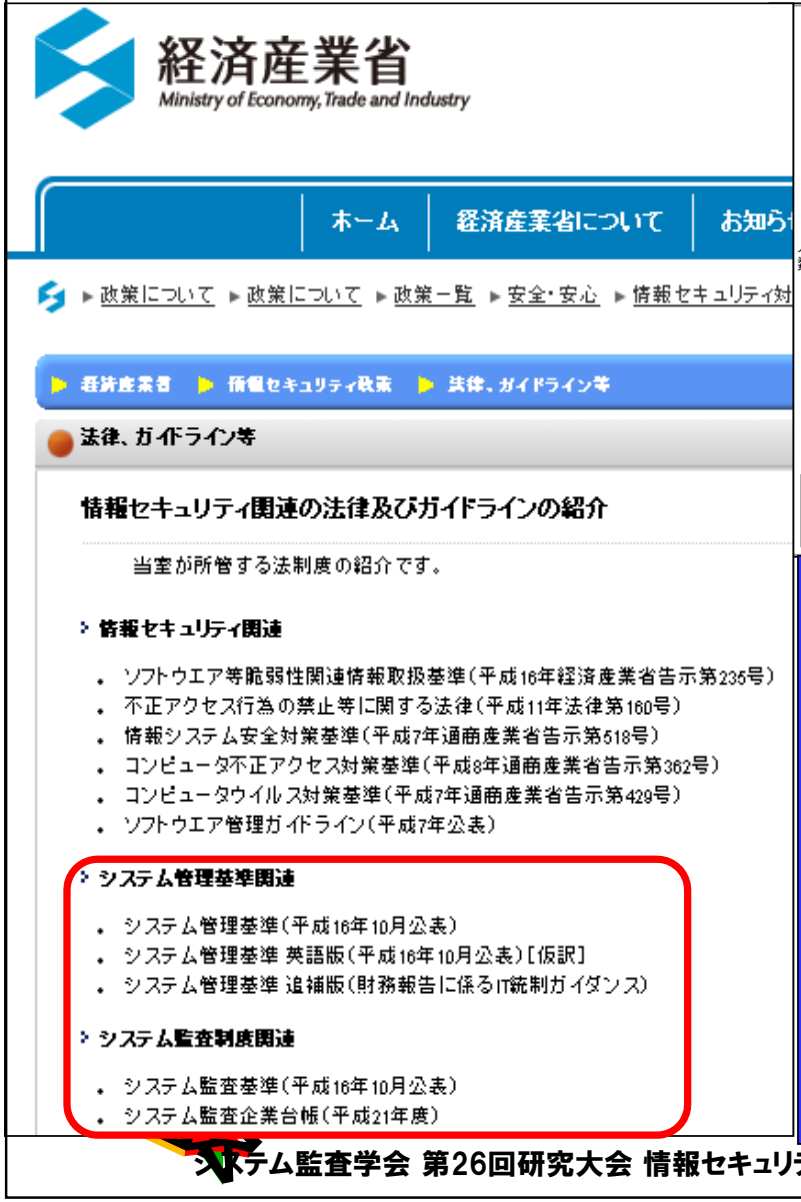
③ インターネットで「システム監査」で検索したら、企業広告と試験対策広告以外、***2010年以降の関連情報が見当たらない。***

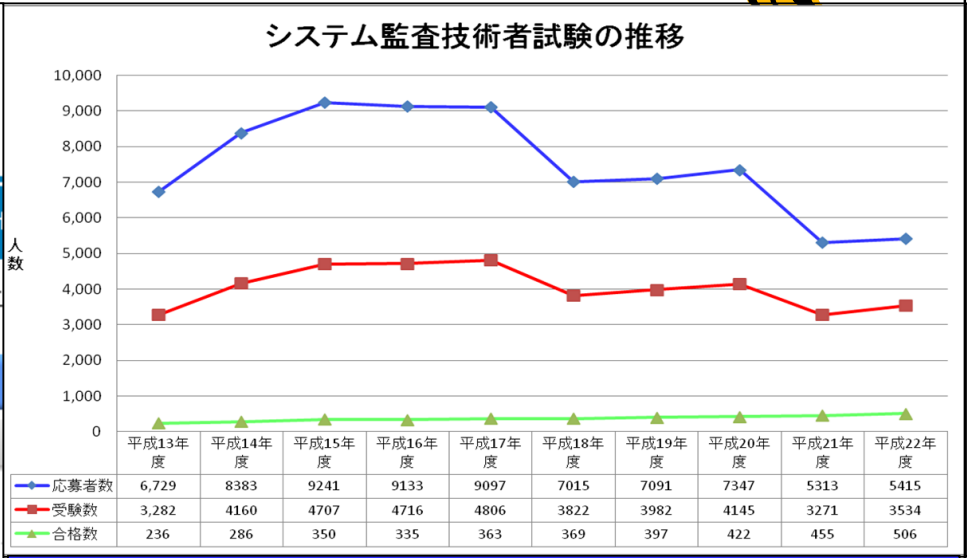
④ 次頁の「経済産業省のホームページ」を見ると、***「情報セキュリティ関連の法律及びガイドラインの紹介」の一部として「システム監査」のガイドラインが掲載***されている。

⑤ ***「システム監査技術者試験」受験数は、減少傾向***である。（次頁グラフ参照）

・ 情報セキュリティ合同研究会としては、***「システム監査」の重要性が社会で認知されない理由は何故か***と危惧しており、なぜこのような状況にあるのかを調査分析することにした。

システム監査活動の現状





	平成13年度	平成14年度	平成15年度	平成16年度	平成17年度	平成18年度	平成19年度	平成20年度	平成21年度	平成22年度
応募者数	6,729	8383	9241	9133	9097	7015	7091	7347	5313	5415
受験数	3,282	4160	4707	4716	4806	3822	3982	4145	3271	3534
合格数	236	286	350	335	363	369	397	422	455	506

当研究会では、「情報セキュリティとシステム監査に対する経営者の認識」を調査することにした。
理由：「システム監査」は、経営者からの依頼で実施する活動
「経営者の『システム監査』に対する認識が低いので、『システム監査』の影が薄くなってきた」と仮説を立て調査を開始した。

なぜ経営者は、「システム監査」に取り組まないのか？

想定した仮説

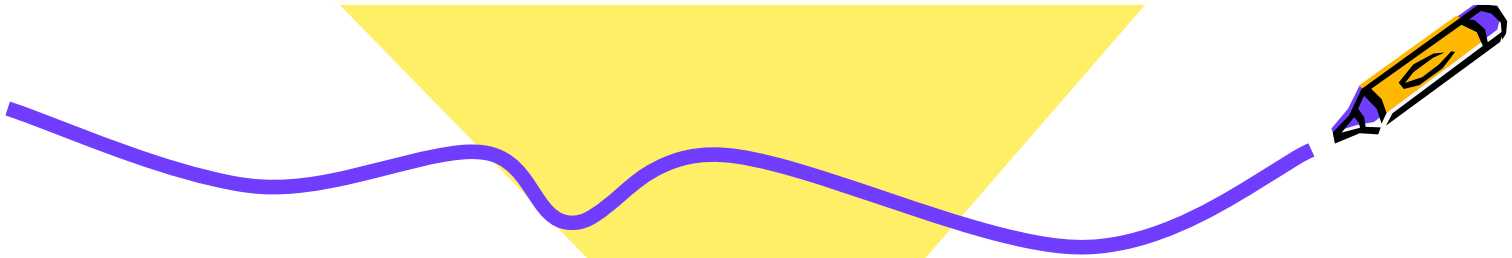
① 経営者が、「システム監査」の意義を十分理解していないのではないのか？

② 経営者は、「顧客の要求に基づき『ISMS』・『Pマーク』の認証を取得した。自社ではセキュリティインシデントは発生しないから、認証取得できていれば、これで十分。」と思っているのではないのか？

③ 経営者は、「J－SOX・IT全般統制における監査」は、法令で定められている対象法人だけがやればいいと思っているのではないのか？（J－SOX法は、非上場企業及び行政機関・特別行政法人は、対象外）

仮説を検証するため、経済産業省発表の「平成22年情報処理実態調査」を分析した。

2. システム監査に対する経営者の認識

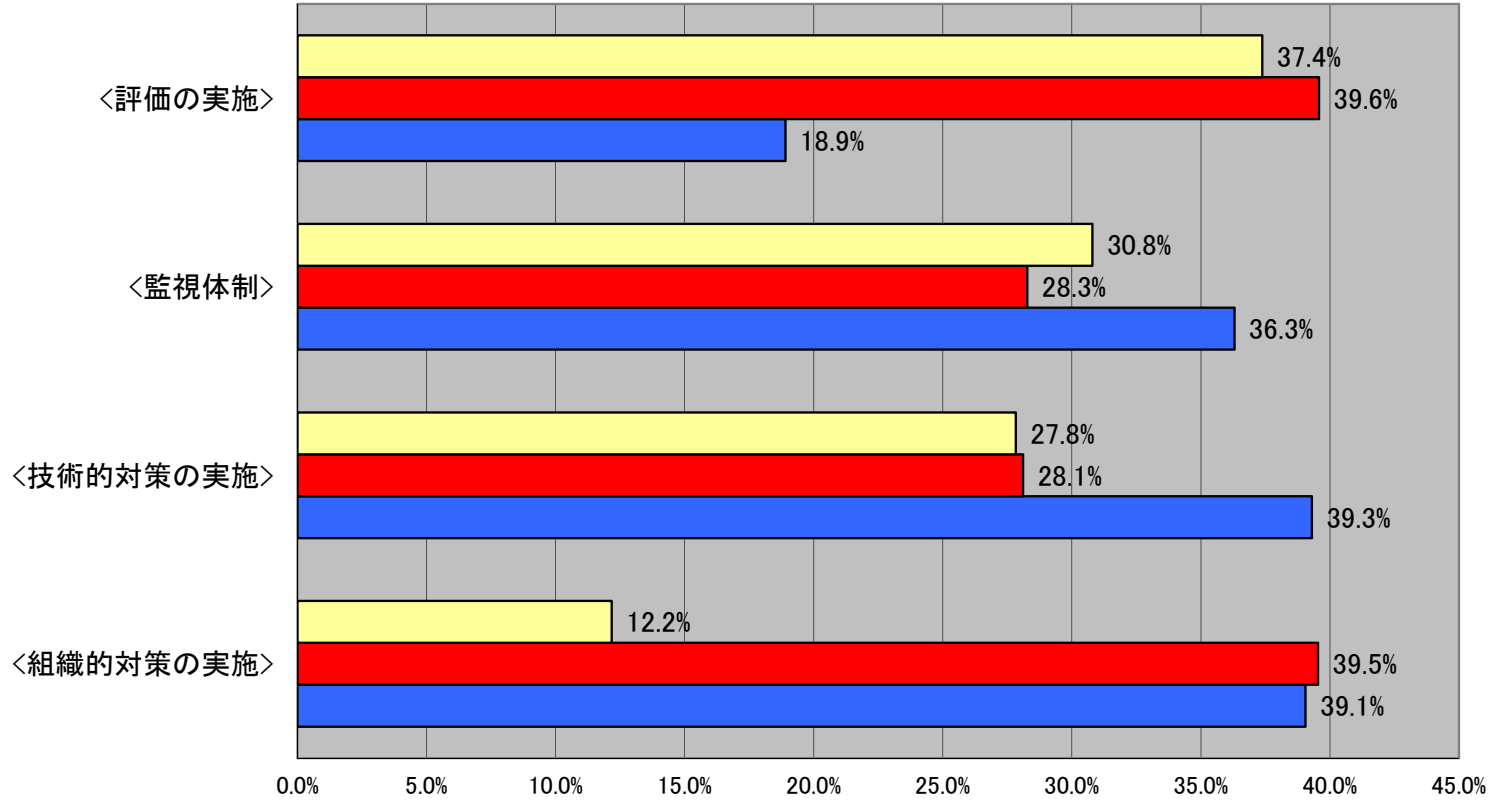


「平成22年情報処理実態調査」の概略

- 調査の対象
  - 【実施機関】経済産業省 【地域】全国 【単位】企業
  - 【属性】日本標準産業分類の分類を活用して情報処理実態調査における調査業種26業種
    - 調査業種対応表（調査対象業種－日本標準産業分類：平成20年調査以降）
  - 【調査対象数】9,500
  - 【回収率】約5割（※回収率＝回収数／調査対象数）
  - 【調査期日】3月31日時点
  - 【実施期間】1ヶ月間
- 抽出方法：標本調査
  - 【選定】無作為抽出
  - 【抽出率】9,500／42,387
  - 【抽出方法】
    - 資本金3,000万円以上かつ従業員50人以上のすべての企業に対して調査が行われている企業活動基本調査の調査対象及び帝国データバンクのデータベースに登録されている企業を母集団として、平成13年事業所・企業統計における製造業及び卸・小売業の占める割合（製造業29.9％、卸・小売業 24.3％）から、製造業を約2,800社、卸・小売業を約2,200社抽出し、残りのその他業種を約4,500社抽出
    - 抽出に際しては、これらの業種分類のほか、従業員規模を層化基準とする。
    - 階層ごとのサンプル数の割当についてはネイマン配分するが、1,000人以上の区分については全数調査とする。

「平成22年情報処理実態調査」からの対策の状況

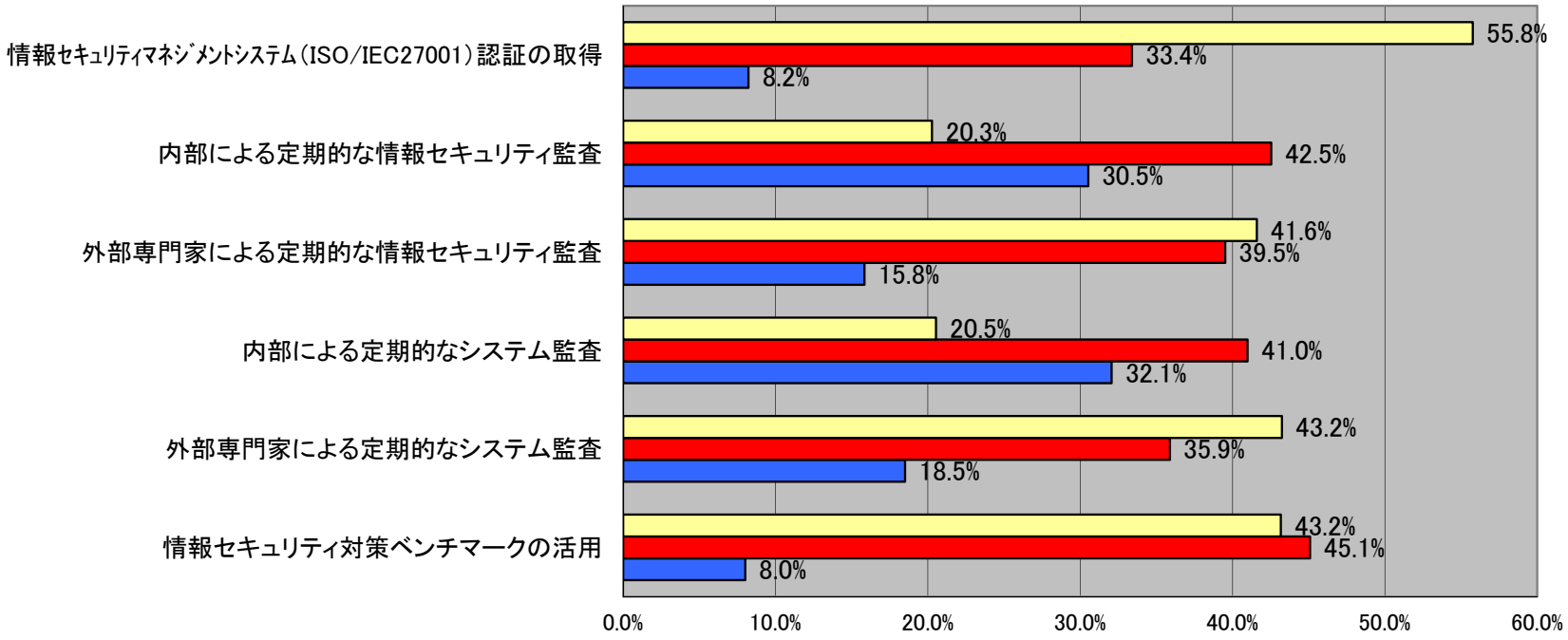
図1：情報セキュリティ対策の実施状況



	〈組織的対策の実施〉	〈技術的対策の実施〉	〈監視体制〉	〈評価の実施〉
必要性を感じず、未実施	12.2%	27.8%	30.8%	37.4%
必要性を感じるが、未実施	39.5%	28.1%	28.3%	39.6%
既に実施している	39.1%	39.3%	36.3%	18.9%

「平成22年情報処理実態調査」からの評価の内容

図2：＜評価の実施＞の詳細



	情報セキュリティ対策ベンチマークの活用	外部専門家による定期的なシステム監査	内部による定期的なシステム監査	外部専門家による定期的な情報セキュリティ監査	内部による定期的な情報セキュリティ監査	情報セキュリティマネジメントシステム（ISO/IEC27001）認証の取得
□必要性を感じず、未実施	43.2%	43.2%	20.5%	41.6%	20.3%	55.8%
■必要性を感じるが、未実施	45.1%	35.9%	41.0%	39.5%	42.5%	33.4%
■既に実施している	8.0%	18.5%	32.1%	15.8%	30.5%	8.2%

「平成22年情報処理実態調査」からの考察

- 全体として「対策の実施済」は、4割未満！！（図1参照）
  - セキュリティ対策は遅れていることが判明
  - 個別に見ると「対策」と「監視」は、35%以上、「評価」は、18．9%
- 図1より、「評価の実施」は低いが、必要であると認識はしている
  - 「必要と感じるが未実施」と「実施済」と合わせると　58．5%
- 図2では、システム監査は「外部」より「内部」が重要と認識
  - 内部による、「システム監査」の「必要と感じるが未実施」と「実施済」と合わせると73%以上であった
  - 「情報セキュリティ監査」も同様であった
  - しかし、ISMS認証は「実施済」8．2%、「必要と感じるが未実施」と合わせても41．6%で、半数以上は必要なしと判断していた

【分析結果】

① 「評価（システム監査）」、特に内部監査は、「必要」と感じている経営者は、半数以上で、「システム監査の意義を十分理解していない」の仮説は、誤りであった。

② しかし、「実施済み」が18．9%で、「システム監査」に対して、経営者は、躊躇している状況であると推測できた。

なぜ「評価（システム監査）」に対して躊躇しているのか？

【さらなる仮説】

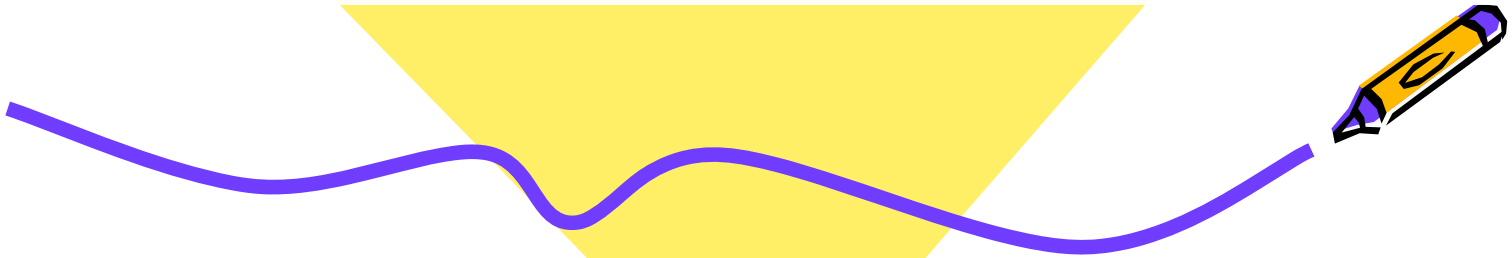
① 経営者は、専門家・情報システム部門・外部委託先等に任せた業務は適切に実施しており、**自社では「情報セキュリティインシデント」は、発生しない**と思っているのではないのか？

② 経営者は、「システム監査」をシステム管理基準の「開発業務」「運用業務」、「保守業務」及び「共通業務」の部分の監査と認識。**経営者は関わらなくてもよい**と思っているのではないのか？

- 「システム管理基準」の「情報戦略」「企画業務」は、経営者関与事項と知らないのではないのか？
- 情報システム部門出身の経営者がほとんどいないのも一因

ここからは、①項の「『情報セキュリティインシデント』は、発生しない」の仮説に対して、経営者の心理を推測してみた。

3. 経営者の心理分析

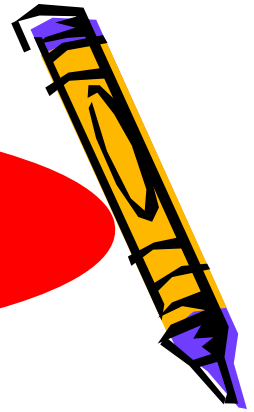


経営者の心理の推測

- 情報セキュリティインシデントに対して経営者の考え方の推測
  - 「関わらなくても構築システムは、品質良く、問題なく稼働するはず」
  - 「当社は、情報セキュリティインシデントは絶対発生しないはず」
  - 「当社は地震・津波があっても、対策を打たなくても被害はないから大丈夫なはず」
- なぜ、根拠がなく、「自分のところは大丈夫なはず」と思ってしまうのか？　⇒【根拠なき否定】
  - 「起きて欲しくないことは、起きない」と信じている経営者は、「『起きて欲しくないこと』を予防する『システム監査』」は、重要だが、すぐに発生しないので今は不要と思っているのではないのか？
  - だが、インシデントが発生すると、経営者は、「ヒステリック」状態になり、部下に責任転嫁したり（某製肉会社経営者）、『どうして対策を講じていなかったのか！』と逆ギレする経営者もいる。

この根拠もなく「自分のところは大丈夫」と思う
社会的心理は、何なのか？
これは、「正常性バイアス（正常性の偏り）」ではないのか？

正常性バイアスによる経営者心理の説明



認めたくない情報

①自分の所には個人情報がある
「個人情報漏洩事故に遭うかも！！」

②コスト・労力等が足りず対応ができない

不愉快

居心地が悪い

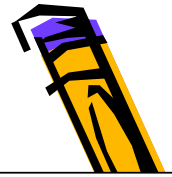
←認知的不協和

認めやすい事実に変える

③個人情報漏洩は必ず起きるとは限らない
「当社は大丈夫」

正常性バイアスは心の自動防御装置

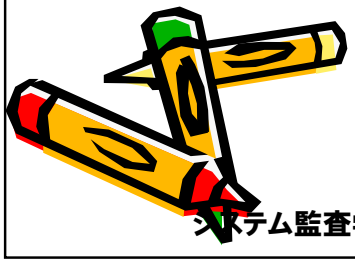
【参考】情報セキュリティと正常性バイアス



情報セキュリティ対策においても、この正常性バイアスが大きな壁となる場合があります。

これだけ頻繁にファイル共有ソフトの暴露ウイルスによる情報漏洩事件が報道され、多くの組織が業務情報や個人情報を私用パソコンで使うことを禁止しているにもかかわらず、情報漏洩は一向に減りません。

漏洩を起こした当事者からは、「自分だけは大丈夫だと思っていた」、「パソコンが普段と違う動作をしたような気がしたが、問題はないと思っていた」という証言が多く聞かれ、正常性バイアスの悪影響が強く疑われます。



NISCNEWS第10号　2007年4月25日発行（内閣官房情報セキュリティセンター）
http://www.nisc.go.jp/nisc-news/0010/news0010.pdfより引用

”正常性バイアス”を更に強化してしまう他のバイアス

正常性バイアス
（異常を正常の範囲内のことと捉えてしまう錯覚）

異常に気付かない

行動が鈍くなる

同化性バイアス
（異常を背景の中に埋没させてしまう錯覚）

同調性バイアス
（他社が行動するまで行動しない錯覚）

- **同化性バイアス**
  - ヒヤリハットが発生しても「まぁそんなことはあるだろう」と軽く見ていたら、実は重大なインシデントの兆候であり、適切に初動対応しておればよかったのにと後悔する。**【ヒヤリハットの無視】**
- **同調性バイアス**
  - 多くの同業他社が実施すれば、実行するが、多くの同業他社が実施しなければ、同調して実行しない。**【横並び】**

【参考】同調性バイアスと正常性バイアスの事例

2003年2月18日、韓国で地下鉄火災が発生し、200人の命が奪われる大惨事がありました。
事件後に発表された報道写真に奇妙な行動が見られます。
火災が始まり煙が充満してきた車内に平然と人々が座っているのです。
普通なら窓を割って逃げるのが最善の策でしょう。
これについて、防災システム研究所所長の山村武彦氏は「同調性バイアス」と「正常性バイアス」が支配した結果であると言っています

http://psychological-jp.com/column/p9.htmlより引用

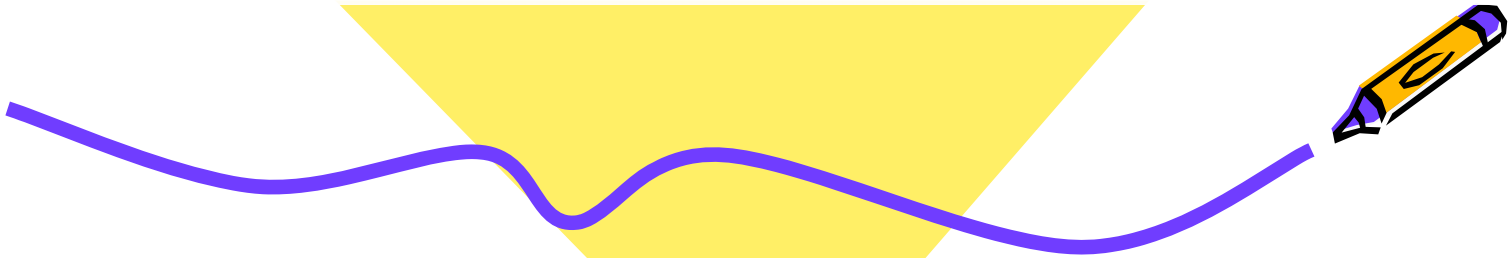
”正常性バイアス”に陥ると

- 正常性バイアスになるとリスクに鈍感になる。
  - 近づいてくるリスクに気づかなくなり、無思慮にリスク要因に近づき、インシデントに巻込まれることが多い。
- 経営者の安心を得ようとする心（正常性バイアス）は、リスク対応を阻害する。
  - その結果、油断が生じ、インシデントの被害を受けてしまう

以上から、システム監査は必要であると認識しているが、他方、実施に対しては躊躇してしまう経営者の姿勢を、正常性バイアスを用いて説明できる。

- 正常性バイアスに陥らないためには
  - 心の働きには、「正常性バイアス」が存在する事実を認めること
  - 「正常性バイアス」のワナに陥らないためには、リスクを見据えていくこと
  - リスクに対する恐れを持ち続けること

4. システム監査人の役割



「経営者」と「システム監査人」の考え方のギャップを理解する

- **システム監査人の考え方は、「改善指向（問題解決）型」**
  - 「経営者が情報セキュリティインシデントに備えないのは、『非合理』である」とシステム監査人は考える。
  - 「だから、システム監査をなんとか実施させなければならない」という専門家の立場で議論し提言する。

- **経営者の考え方は、正常性バイアスの呪縛の下での合理的な判断**
  - 経営者は情報セキュリティインシデントに対して、監査人の尺度（専門家の尺度）と別の尺度（正常性バイアスの尺度）を持っており、それが合理的であると判断している。

経営者を「正常性バイアス」の間違った安心感から解放し、
「評価実施」による安心感へ切り替えさせることが重要

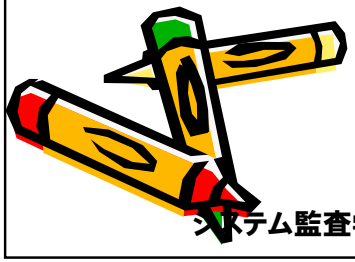
システム監査人が経営者に対して行うべきこと（１）

- 経営者とリスクを共有する（経営者の気持に寄り添う）
  - 目的は、経営者を「正常性バイアス」による間違った安心感から解放し、「評価（監査）実施」による安心感へ切り替えさせること
    - 「自分のところは、大丈夫！」と思うのは、「希望」「願望」であって、決して「正しい判断」ではないこと強く訴える
    - 「インシデントは、発生する確率は高いので、システム監査は必要だ。」しかし、「当社は何もしていない」。この受け入れがたい矛盾を気付かせる
    - 経営者へ『日常』から『非日常』、『尋常』から『非常』、『通常』から『異常』は、必ず起きるという事実を認識させるのがシステム監査人の役割！

システム監査人が経営者に対して行うべきこと（２）

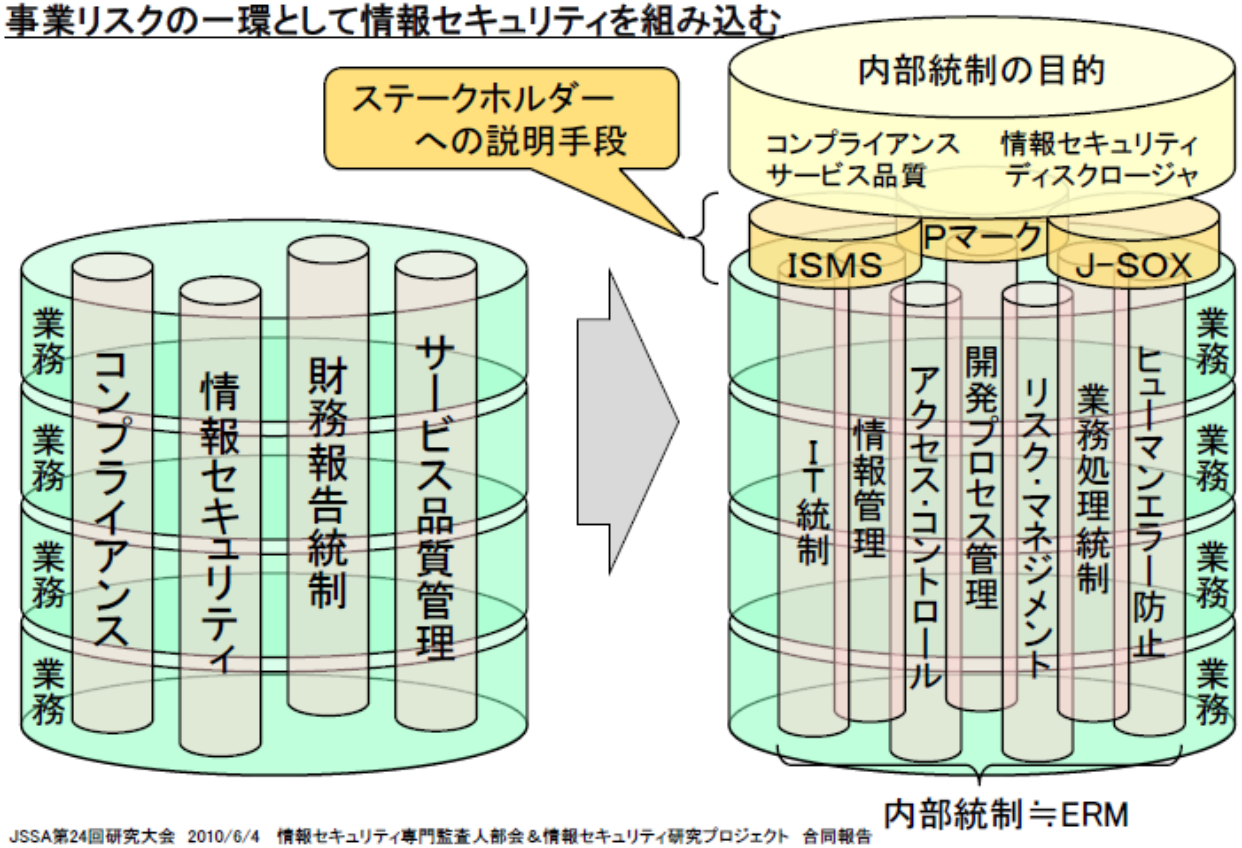
- 「システム監査人」は、システムに対する信頼できる情報源になる。
  - 経営者に、情報システムが持つリスクをきちんと見据えさせ、リスクに対する恐れを持ち続けさせること

- 「システム監査の視点の整理、特に有効性」を経営者へ継続的に訴え続ける必要がある。
  - ここで、「情報戦略策定から企画に至る上流工程」のシステム監査をどのようにすればよいかが、今後の検討課題となる



究極の使命は
「情報セキュリティのあるべき姿」を経営者へ理解してもらう！！

事業リスクの一環として情報セキュリティを組み込む



JSSA第24回研究大会　2010/6/4　情報セキュリティ専門監査人部会＆情報セキュリティ研究プロジェクト　合同報告

我々は、「事業リスク軽減の一環としてシステム監査に取り組む」ことの重要性を今後も経営者に提言していくつもりである。

情報セキュリティ合同研究会メンバー

研究会メンバー	研究会メンバー
齋藤 敏雄【日本大学】:主査	山本 孟【優成監査法人】
桜井 由美子【EyeBeyond】	芳仲 宏【東京地方裁判所】
川辺 良和【㈲インターギデオン】	内藤 裕之【ﾌﾞﾘｰｽﾞ・ｺﾝｻﾙﾃｨﾝｸﾞｵﾌｨｽ】
植野 俊雄【ISU】	黒川 信弘【パナソニック㈱】
小谷野 幸夫【㈱さいたまソリューションス】	足立 憲昭【㈱光洋】
長野 加代子【㈱ピーアンドアイ】	高橋 孝治【CRC】
鳥越 真理子【優成監査法人】	西澤 利治【㈱電脳商会】
西川 征一【㈱西川技術士事務所】	水谷 穣【水谷情報技術士事務所】
桂 由紀子【国際ﾋﾞｼﾞﾈｽｺﾐｭﾆｹｰｼｮﾝ協会】	中田 猛【古河インフォメーション・テクノロジー㈱】
永井好和【山口大学】	高野 美久【NECソフト㈱】:発表者

ご清聴ありがとうございました。
研究会は、さらに情報セキュリティとシステム監査の有効性と効率性を「深堀り」します。これからもよろしくお願いします。