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

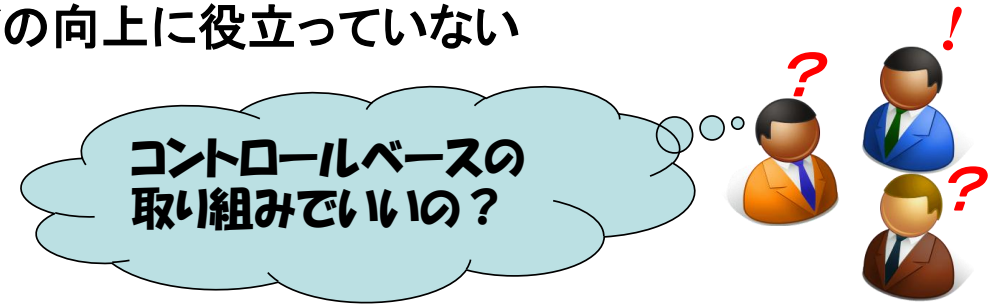
合同報告

発表者：　優成監査法人　鳥越真理子, CISA, CISM

1．情報セキュリティ管理上の現状の問題点

- 必要に迫られた都度個別の対応
- 複数のマネジメントシステムが乱立
- 認証取得が目的化している
- 企業としてのリスクマネジメントのバランスの欠如
- 取組みが企業ブランドの向上に役立っていない

・管理策の有効性に疑問
・現場に過大な負担
・受身的な対策の実施
・業務の効率性低下
・経営目的と不一致



2. 研究会のねらい

- ☑ **有効性と効率性の追求**
  - 情報セキュリティ要求レベルの適正化
  - 事業リスク全体の中で情報セキュリティの位置づけ
  - 費用対効果面から経営としての意思決定
  - 管理の重複排除による業務効率化
- ☑ **ステークホルダの期待を先取りした能動的な対策の実施**
- ☑ **リスクマネジメントと内部統制の強化**
- ☑ **差別化取り組みによる企業ブランド価値の向上**

3. 情報セキュリティ取り組みの現状

よく見られる考え方		・発注者の要求への対応・営業上の優位性の確保 ・情報セキュリティの運用実績づくり
		凡例:「▲」は本来の経営目的に反する状況を示す。
取組み状況	経営者	・発注者の要求に応えた情報セキュリティ対策 ・受注の確保・拡大 ・顧客との信頼関係の維持・取引の継続
	推進者 (事務局)	・コンサルタント等の支援を受けたISMSの短時間での構築 ・ISMS構築・導入における現場負担の軽減 ▲Pマーク個人情報保護、J-SOX財務報告の信頼性、とは非同期 ▲事業の内容・規模や現場の業務に不整合なルールの制定 ・ISMS認証取得による情報セキュリティの実績づくり ・現場の統制・管理による運用の維持
	現業部門	・ISMS推進者の指示に基づく導入 ▲ISMS／Pマーク／J-SOXについて各々個別の運用指示 ▲日常における情報セキュリティ意識の醸成が未達成 ・策定されたISMSの情報セキュリティ手続きの遵守 ▲業務優先によるルール不遵守の発生

4. 統合管理/統合監査への動き

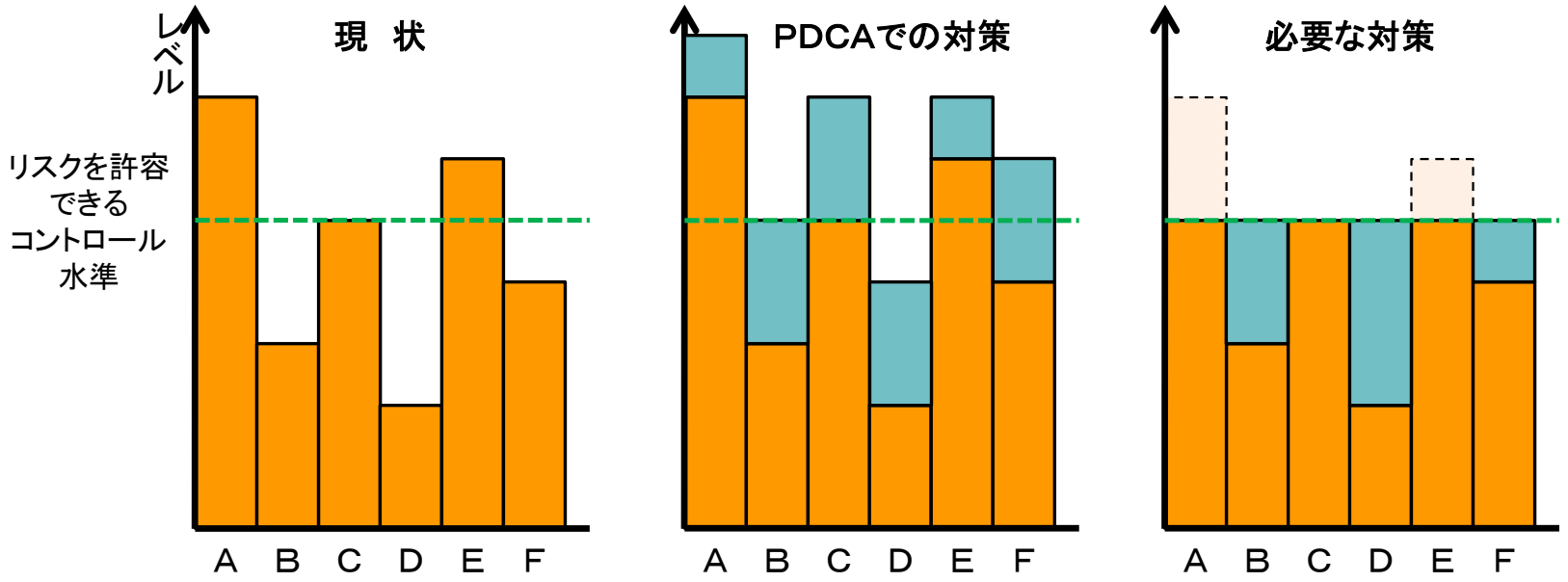
現状取り組まれている改善策		・統合マネジメントシステム化によって一本化を目指す ・現行ISOマネジメントシステムを統合化し効率的に維持
改善策への取組み例	経営者	・ ISO推進組織を統合し、事務局を一部署に集める ・ ISO管理責任者の一元化 ・ 各ISOのマネジメントレビューの統合
	推進者 (事務局)	・各ISOのマネジメントシステムの文書統合 ・各ISOの記録・報告の様式の統合 ・各ISOの方針、目標、定例教育、実施計画、マネジメントレビューの統合 ・各ISOの統合内部監査の実施 ・各ISOの統合(複合)審査の受査
	現業部門	・各ISOの部門の目標、実施計画、進捗管理の一元化 ・各ISOの連絡・報告先の一元化 ・各ISOの改善実施の一元化 ・各ISOの統合内部監査・統合(複合)審査の受査

5. 真に必要な対策の実施

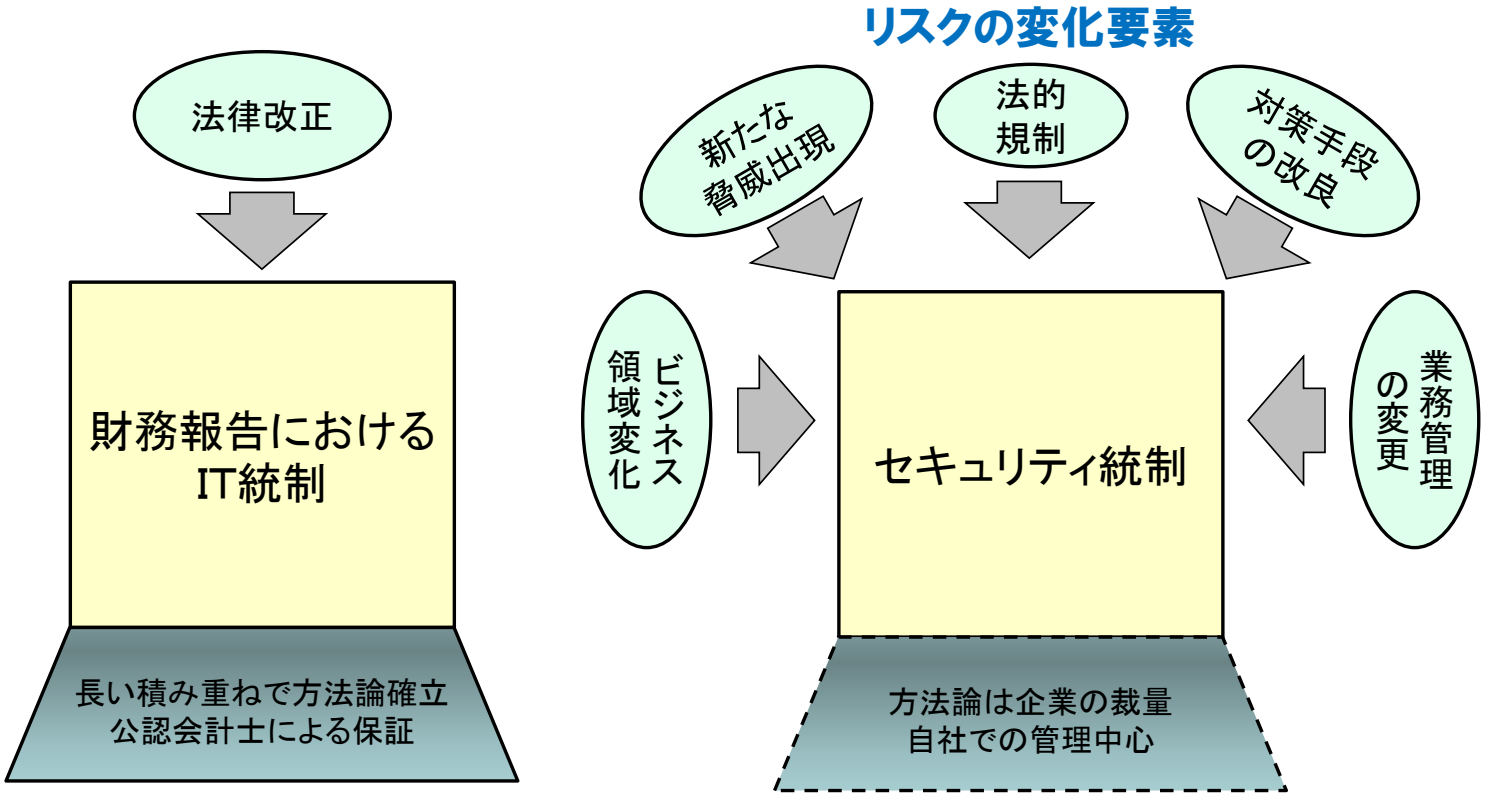
◆「PDCAマネジメントサイクルで管理レベル向上」の旗印の下、
各項目で対策が強化されるが、めざしている姿ではない。

◆「マネジメントレベル向上」が必要以上の対策の実施につながる場合もある。

◆ 自社にとって必要にして妥当な「過不足ない対策」が重要であって、中には緩める対策項目もあってよい。



6. 情報セキュリティに対する環境変化の影響



- ◆ 財務統制のように伝統的な方法論が確立していない
- ◆ 財務統制は、急激な変化を前提としない
- ◆ セキュリティ統制では、影響する環境変化の要素が多い

7. 企業経営を考えた目指すべき取り組み

あるべき考え方		・事業リスクとしての情報セキュリティ事故の重大性の認識 ・日常の業務プロセスの中で情報セキュリティ要求を実現
あるべき取組み例	経営者	・ステークホルダーの期待を先取りする経営 ・事業リスクの提言（情報セキュリティ事故も重大な事業リスクと認識） ・事業継続対策を整備して永続企業（going concern ）へ
	推進者 （事務局）	・認証取得目的でなく、日常業務の中での情報セキュリティ定着を第一に ・トップダウン・リスクアプローチによるバランスよい統制実現の方針 ・事業リスクの一環としての情報セキュリティ／個人情報保護／財務報告の信頼性／その他の各リスクを想定 ・現場主義で情報セキュリティ推進（業務プロセスを重視） ・現場を統制管理するのではなく現場支援を（現場が自らプロセスを改善） ・業務効率を維持向上できる情報セキュリティ技術の導入
	現業部門	・日常における情報セキュリティ意識の維持 ・情報セキュリティを考慮した業務手順の作成と実行 ・業務効率とリスク対応のバランスを考慮した継続的な見直しと改善

8. リスクベースによるマネジメントの実現

目的と目標	・自社の事業リスクに対するリスクマネジメントの枠組みの構築 ・財務報告の信頼性、情報セキュリティ、個人情報保護、製品・サービス品質、事業継続などのリスク統制による企業活動の永続
責任と権限	・経営者によるリスク統制に対する方針策定と責任権限と役割の割当て ・経営者による**内部統制総括責任者の選任** ・内部統制総括責任者による**各種リスクに対して専門性のある責任者の選任** ・内部統制総括責任者による**業務毎の責任者の指名**
役割分担	・内部統制総括責任者によるバランスの取れた内部統制の整備・運用 ・専門性のある責任者によるリスク想定と有効な統制制御の検討 ・業務毎の責任者による業務のリスク分析と統制の実施
業務推進	・業務毎に、リスク分析に基づく業務上の統制制御の検討 ・業務上のリスクに対する統制制御に必要な手続の制定／改訂と実装
運用状況 点検と反映	・業務上のリスクに対する統制制御の手続の運用状況を点検し報告 ・業務遂行の中で把握した課題の報告と改善への反映
統制の 評価と改善	・業務上のリスクに対する統制の整備と運用状況を内部監査で評価 ・検出された不備の是正、改善すべき点の改善への反映 ・外部監査を受け、統制に関する保証を得て、結果を公表

9. 経営者にとってのメリット

- 自社にとって過不足なくミニマムな管理に絞り込める
- J-SOX、情報セキュリティ、個人情報保護、等の間での重複が排除できる
- J-SOX、情報セキュリティ、個人情報保護、等の各種のリスクに対して、対応レベルを合わすのが容易
- ステークホルダーに対し整備・運用状況評価結果を表明できる
- 各部門が自発的に責任を遂行できる
- 「新たな種類のリスク」へ対応するとき、その道の専門家による“リスク想定”以外は、同じアプローチで統制の整備が行える
- 自社のリスクマネジメントを自己宣言し、これについて外部監査を受けて、統制に関する保証を得て結果を公表することで、ステークホルダーの信頼を得ることができる

10. 情報セキュリティで考慮すべきポイント

- ✓ **環境変化によって変わるリスクへの対応**
  - → リスクの増減について都度把握し対策を見直す
- ✓ **情報セキュリティの対策レベルは経営判断**
  - → リスクと対策コストと想定される残存リスクを勘案する
- ✓ **自社の内部統制をどのように外部に示すか**
  - → PマークやISMS認証取得により効果的かつ効率的に外部に示す
  - → 専門監査人による保証型監査を受審する
- ✓ **圧倒的に多い「うっかりミス」による情報セキュリティ事故**
  - → コントロールを業務に組み込む（＝自動化）
  - → ITリテラシィ啓蒙教育で防止を図る

11. 今、経営者がもつべき情報セキュリティ意識

◆ **業務の効率性を下げる管理策は、管理策ではない！！**

◆ 重要なビジネスプロセスの重要なリスクを許容レベルまで低減

◆ リスクに対してマネジメント体制を一元化して対応

◆ トップダウン・リスクアプローチによるバランスある統制の採用

◆ 情報セキュリティ事故も重大な事業リスクと認識

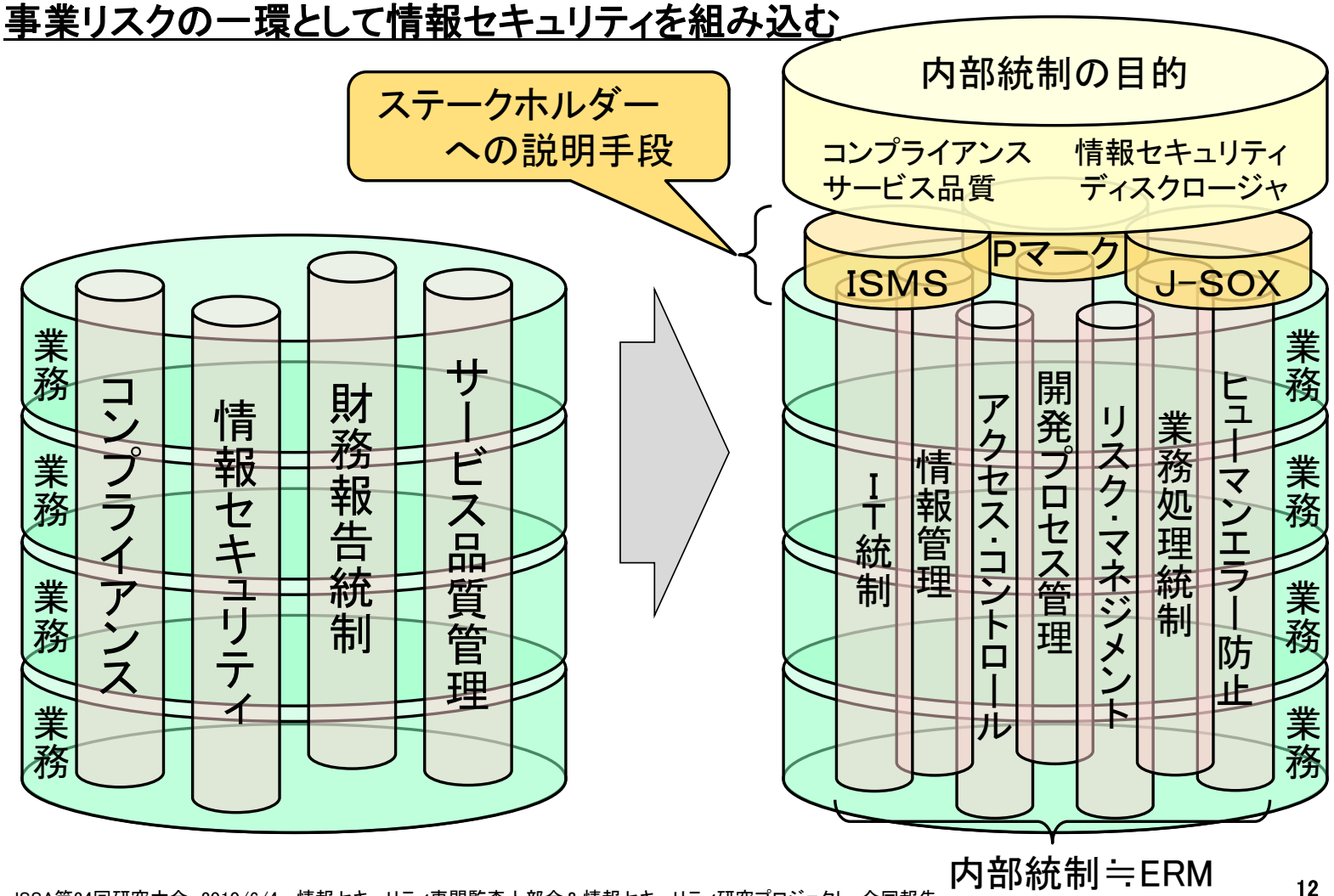
◆ 情報セキュリティを企業の内部統制の一環として統制

◆ 内部統制の整備・運用状況については内部監査にて評価

◆ 内部統制に対する外部監査を受けることで第三者の保証を得る

■　情報セキュリティのあるべき姿

事業リスクの一環として情報セキュリティを組み込む



■　情報セキュリティ合同プロジェクト・メンバ

氏　名	所　属
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ズ
税所哲郎	群馬大学
齋藤 敏雄	日本大学
桜井由美子	ＥｙｅＢｅｙｏｎｄ
鳥越真理子	優成監査法人
内藤 裕之	バルク

氏　名	所　属
永井好和	山口大学
西川征一	西川技術士事務所
西澤 利治	電脳商会
水谷　　穣	水谷情報技術士事務所
安尾勝彦	ヤフー
山本　孟	優成監査法人
芳仲 宏	東京地方裁判所

ご清聴ありがとうございました。
研究会は、さらに、情報セキュリティの管理策の有効性と効率性を「深堀り」します。一緒に研究しましょう。 ***メンバー募集中!!***