システム監査の多様性研究プロジェクト報告
ー組織保護の新たな観点ー

Report by "Diversity in System Audit" Research Project
- A new perspective of the organization protection -

2016年6月3日

システム監査の多様性研究プロジェクト

主　査：荒牧　裕一（京都聖母女学院短期大学）
副主査：雜賀　努　（株式会社ニイタカ　監査室）

研究会メンバー（アイウエオ順）

【主　査】　荒牧　裕一（京都聖母女学院短期大学）
【副主査】　雑賀　努　（株式会社ニイタカ）
【メンバー】
伊地知裕貴（株式会社ニイタカ）
浦上　豊蔵（NPO 情報システム監査普及機構）
片岡　学　（大阪市 行政委員会事務局）
栗山　孝祐（株式会社富士通システムズ・ウエスト）
黒川　信弘（黒川技術士・行政書士事務所）
林　　裕正（富士通株式会社）
深瀬　仁　（パナソニック溶接システム株式会社）
福永　栄一（大阪成蹊短期大学）
福本　洋一（弁護士法人 第一法律事務所）
松田　貴典（大阪成蹊大学名誉教授）
山本　全　（日本アイ・ビー・エム・サービス株式会社）
吉田　博一（大阪府）

本研究プロジェクトについて

- ICTを利用した情報システムが高度化し適用範囲が広がるに従って、情報システム関連 の評価に対する要求も多様化し、システム監査においても従来から異なる対象・視点・手法が求められている。
- 本研究会では、このように多様化する情報システムについて、システム監査の対象・視点・手法からの検討・討議を行い、知識の整理と相互研鑽の場としている。
- 今回は、３年目の活動の報告として、経営計画との不整合、個人情報流出問題、マイナンバー対応、不採算ＰＪ撲滅にむけた対策、経営と連動した監査管理等、組織保護の新たな視点に関するテーマと、システム監査実務への影響についての研究結果を報告する。

当研究プロジェクトの活動実績（１／５）

【第１５回（発表担当：雜賀　努）】
・日 時： 2015年4月3日
・テーマ：**「システム監査とERMと経営計画」**
・内 容：中堅メーカにおけるプロジェクトの事例を基に、リスク管理と経営計画の連動の重要性について意見交換した。

【第１６回（合同研究）】
・日 時： 2015年5月11日
・テーマ：**「最終報告について」**
・内 容：６月５日の報告の内容について討議した。

当研究プロジェクトの活動実績（２／５）

【第１７回（合同研究）】
・日 時： 2015年７月１０日
・テーマ：**「年金機構の個人情報流出問題について」**
・内 容：年金機構の個人情報流出問題を取り上げ、事件の原因の
の分析と再発防止策等について意見交換した。

【第１８回（栗山 孝祐）】
・日 時： 2015年８月１８日
・テーマ：**「不採算プロジェクト撲滅にむけたプロジェクト状況の
数値化と予兆検知」**
・内 容：勤務先で実施しているリスク分析の事例としてプロジェクト状況の
数値化による不採算化の予兆検知への取り組みを紹介し、その
有効性等について討議した。

当研究プロジェクトの活動実績（３／５）

【第１９回（松田　貴典）】
・日 時：　2015年１０月２１日
・テーマ：**「マイナンバーとシステム監査について（その１）」**
・内 容：マイナンバー制度の導入に伴って必要となる対応について、
システム監査の観点から整理し、意見交換した。

【第２０回（吉田　博一）】
・日 時：　2015年１２月２日
・テーマ：**「マイナンバー制度の今日的課題」**
・内 容：マイナンバー制度の導入に関するシステムやネットワークについて、
地方公共団体の対応を紹介し、その問題点やリスクについて
討議した。

当研究プロジェクトの活動実績（４／５）

【第２１回（雑賀　努、伊地知 裕貴）】
・日 時： 2016年１月１３日
・テーマ：**「SAP Audit Managementについて（その１）」**
・内 容：勤務先（ニイタカ）で導入を検討した、監査支援ツールの特徴や導入目的等について紹介し、その導入による効果について意見交換した。

【第２２回（伊地知 裕貴）】
・日 時： 2016年３月２４日
・テーマ：**「SAP Audit Managementについて（その２）」**
・内 容：前回に引き続き、監査ツールの導入について意見交換を行った。

当研究プロジェクトの活動実績（５／５）

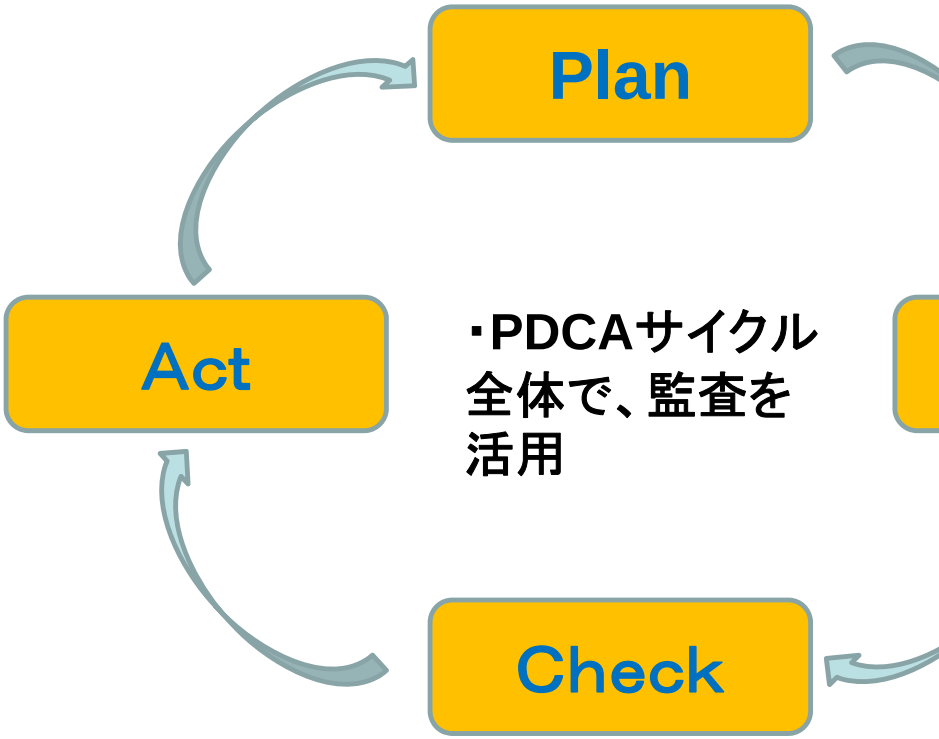
【第２３回（合同研究）】
・日 時： 2016年４月１９日
・テーマ：**「最終報告について」**
「３０周年記念誌の原稿執筆担当について」
・内 容： ６月３日の最終報告の内容について討議した。
３０周年記念誌の原稿執筆の役割分担について検討をした。

【第２４回（ 合同研究）】
・日 時： 2016年５月１２日
・テーマ：**「最終報告について」**
「30周年記念事業への応募テーマについて」
・内 容：前回に続き、６月３日の最終報告の内容について討議した。
30周年記念事業の松田賞・学会賞の対象論文・発表について、各メンバーの応募テーマについて検討をした。

活動から得られたシステム監査の新たなアプローチ（各論）

システム監査のアプローチ（プロセスの評価）

PDCAサイクルとの同期化

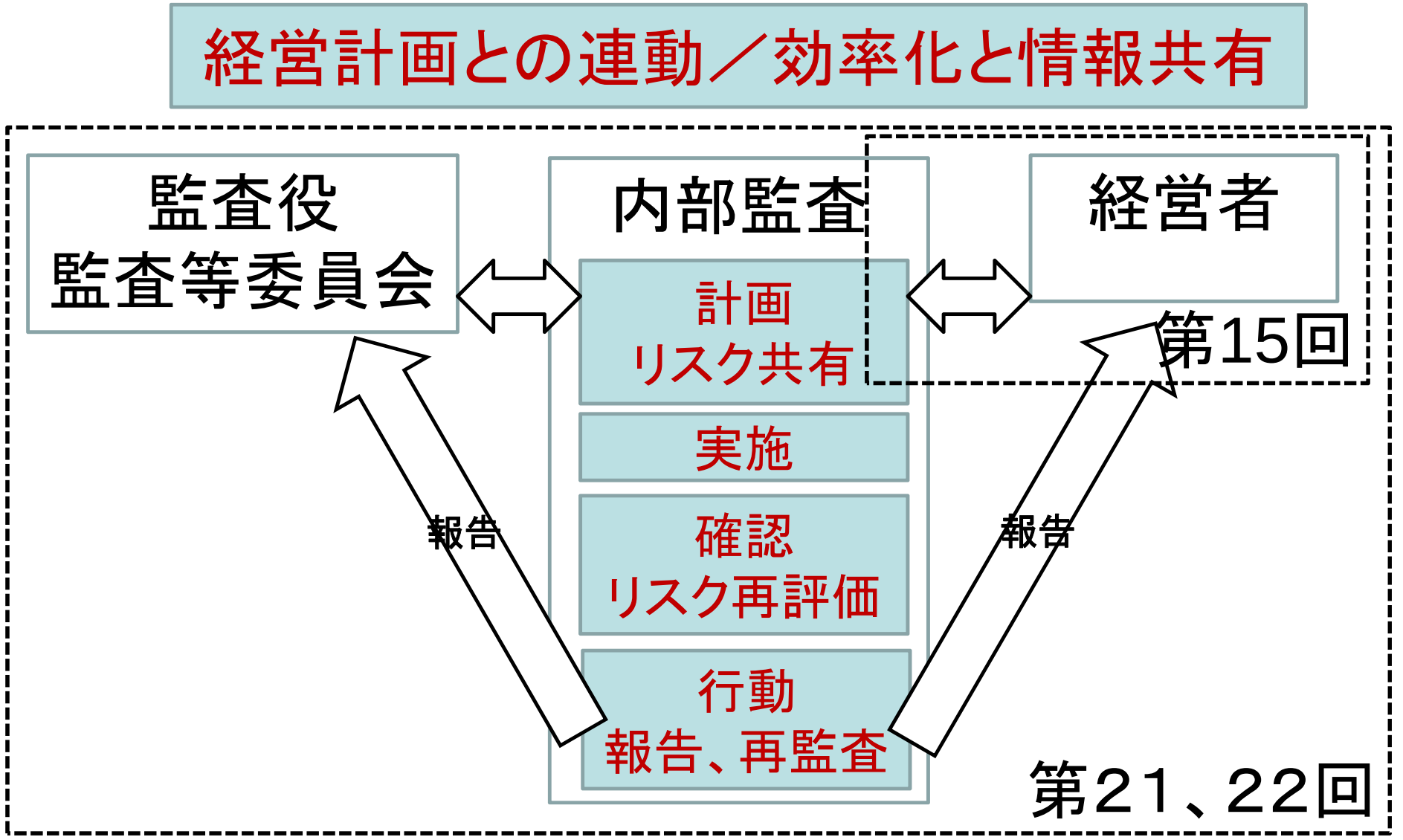


・PDCAサイクル全体で、監査を活用

監査はチェックのひとつではなく、プロセスの評価に変わっている。
本来的な監査へと進化

基本的には、
PDCAサイクルは現場、管理部門の仕事
監査はPDCAの各ステップまたは全体の有効性を評価する。

システム監査のアプローチ（管理手法）



システム監査の視点（リスク評価・対策）

組織存亡のリスク

情報漏えいリスク → 組織の存亡

- 組織全体の意識改革
- 経営トップの理解
- 内部監査の位置づけ

システム監査のアプローチ（セキュリティ対策）

新たなセキュリティ脅威
（標的型メール攻撃）への全社的対策

技術的対策

規定の整備

＋

周知徹底・研修の実施

継続的な対策（模擬攻撃等）の実施

システム監査のアプローチ（プロジェクト管理）

リスク分析のシステム化

プロジェクト数値の見える化

リスク分析の
有効性

契約上の対応
（金額変更･撤退条件）

不採算プロジェクトの早期発見

プロジェクトの暴走の抑止

システム監査のアプローチ（新たな法制度）

自治体等でのマイナンバー制度での
特定個人情報保護評価の監査

新たな制度でのリスク対策の監査の実施

助言型監査ではなく、
保証型監査の実施の動き

一定の手続の実施が必要
（法定監査に近づく）

特定個人情報取扱いプロセスにおけるリスク例（１）

１．特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く）

①目的外の入手が行われるリスク
②不適切な方法で入手が行われるリスク
③入手した特定個人情報が不正確であるリスク
④入手の際に特定個人情報が漏えい・紛失するリスク他

２．特定個人情報の使用

①目的を超えた紐付け、事務に必要ない情報との紐付け
②権限のない（元職員、アクセス権限のない職員等）によって不正に使用されるリスク
③特定個人情報ファイルが不正に複製されるリスク他

３．特定個人情報ファイルの取扱いの委託

①委託先による特定個人情報の不正入手・不正な使用に関するリスク
②委託先による特定個人情報の不正な提供に関するリスク
③委託先による特定個人情報の保管・消去に関するリスク
④委託契約終了後の不正な使用に関するリスク他

特定個人情報取扱いプロセスにおけるリスク例（２）

4. 特定個人情報の提供・移転（情報提供ネットワークシステムを通じた提供を除く）

①不正な提供・移転が行われるリスク
②不適切な方法で提供・移転が行われるリスク
③誤った情報を提供・移転してしまうリスク

5. 情報提供ネットネットワークシステムとの接続

①目的外の入手がおこなわれるリスク
②安全が保たれない方法によって入手が行われるリスク
③入手した特定個人情報が不正確であるリスク
④入手の際に特定個人情報が漏えい・紛失するリスク
⑤不正な提供が行われるリスク他

6. 特定個人情報の保管・消去

①特定個人情報の漏えい・滅失・毀損のリスク
②特定個人情報が古いまま保管されるリスク
③特定個人情報が消去されずにいつまでも存在するリスク他

マイナンバー制度での監査はどうあるべきか

自治体等で先行する特定個人情報保護評価でのリスク対策の監査及び自己点検は、「マイナンバー制度でのリスク対策と監査」における最適な制度設計として作られた

■特定個人情報保護のシステム監査の法定化
特定個人情報保護評価では、厳格な個人情報保護を求めており、自己点検を含めた監査の実施を義務化
■個人のプライバシー等の権利利益を保護する取組みを「宣言」し、その運用が適正に実施されていることを保証する「保証型監査」を実施
■年に一度は、外部監査人による監査を実施

マイナンバー制度の監査の今後の展開

■マイナンバーカードの活用がビッグデータへの活用増大リスクに繋がり
その対応への新たな監査視点とアプローチが求めれる
■マイナンバーの金融分野、医療分野等への利用範囲の拡充対応

■マイナンバーカードに実装される**アプリケーションの信頼性、安全性及び効率性**における監査の活用
ICチップ空き領域搭載アプリに対するシステム監査＝国、地方自治体
公的個人認証サービスの民間事業者に対するシステム監査＝銀行、生保等事業者及びネットモール等ポータル事業者（総務大臣が定める認定基準の準拠性監査）
■地方自治体情報システム**セキュリティ対策の実効性**における監査の活用
ネットワーク強靭化対策、インターネットに対するセキュリティクラウドに対するシステム監査＝地方自治体

今後の活動について

・引き続き、多様性のテーマについて発表と討議を行う。
（マイナンバー制度、フィンテック、知的財産権、IoT 等）

・2016年度の成果をまとめ、6月の研究大会で報告する。

・併行して、参加メンバー有志による個別の研究も進め、
その成果の発表と討議の場としても活用する。

・「松田武彦賞・学会賞」「研究発表奨励賞」の受賞を目指す。