

システム監査学会 第37回研究大会

システム監査の方向性・在り方の調査研究

Research on the direction and ideal state of systems audits

「監査の適合性チェックとコンサルティング機能の実効性・有効性の達成」

研究プロジェクト(2022年度継続)

木村 裕一

赤尾 嘉治

稲留 和紀

尾崎 孝章

目次

1. プロジェクト発足の経緯
2. 企業でのシステム監査の導入と実績
3. 企業におけるシステム監査活動の課題抽出
4. システム監査の方向性を検討するに当たっての考慮事項
5. 企業におけるシステム監査活動の改善の方向性
6. システム監査を支援(サポート)する関連団体への要望
7. おわりに

1. プロジェクト発足の経緯

1. 1 研究の経緯

- ▶ 情報システムの持つ役割・責任の重要性は高まってきている。
- ▶ サービス停止の障害、またサイバー攻撃による被害が継続的に発生している。システム監査の必要性が増加している状況である。
- ▶ システム監査実践企業は減少していると言われるが、本当か、その要因について調査研究した。

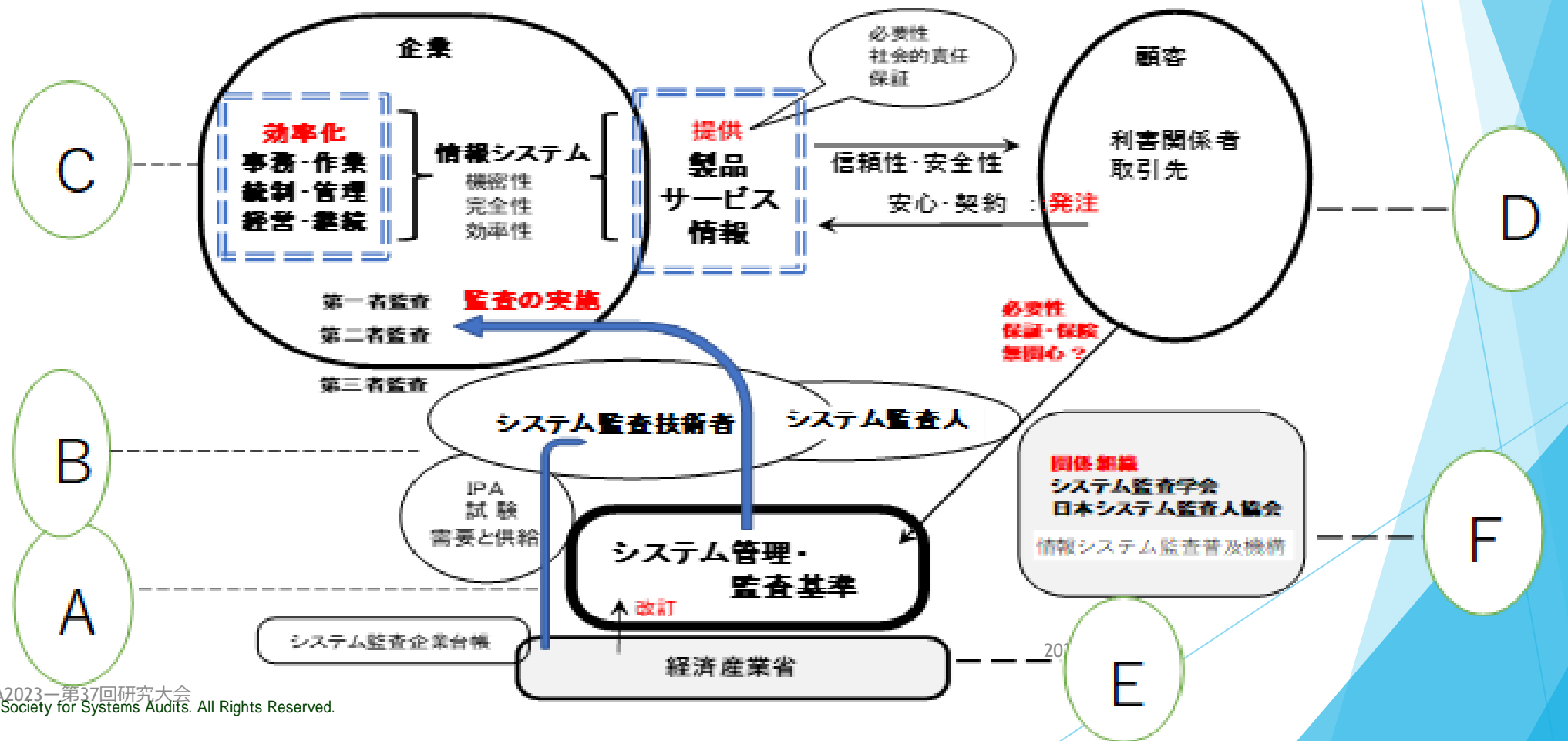
1. 2 研究のアプローチ

- ▶ ・企業におけるシステム監査の実施が増えること
- ▶ ・実施が増えれば監査人への需要が増える
- ▶ ・システム監査人を目指す者、試験受験者が増える
・学会が監査人をサポートすれば会員も増える
- ▶ 企業がシステム監査の実施者である。
図表 1. 2 - 1 (企業におけるシステム監査活動の関係図)
システム監査の促進に関して、**©** : 企業との関りを検討対象とした。

1. プロジェクト発足の経緯

1.2 研究のアプローチ

図表1. 2-1 企業におけるシステム監査活動の関係図



1. プロジェクト発足の経緯

1.2 研究のアプローチ(つづき)

▶ 図表1.2-2 システム監査の実施に関わる要因

区分	内容	主体
A: システム管理・監査基準	システム監査実施のための基準文書	METI
B: システム監査実施者	企業内で任命された者 システム監査技術者試験合格者、 関連団体のシステム監査の個人資格(*1)認証者	社員 個人事業主 委託先など
C: 情報システムの利用企業 (原則: システム監査実施企業)	社内業務のデジタル化で、①事務、②管理、③経営、の情報処理 情報システムにより顧客に、①製品、②サービス、③情報を提供する	経営者
D: ステークホルダー	Cのサービスの提供先 顧客、利害関係者、取引先(提供される商品の利用者)	企業・組織 個人
E: 経済産業省	システム管理・監査基準の策定 システム監査技術者試験の実施 システム監査企業台帳制度	行政官庁
F: 関連団体	システム監査の研究、研修を目的する活動 システム監査の促進支援 システム監査人の情報交換など	システム監査学会、日 本システム監査人協 会、FISC 等

2. 企業でのシステム監査の導入と実績

2.1. 企業におけるシステム監査の状況

システム監査: 経営者自身の判断でシステム監査基準に基づき実施する、**第一者監査**

- ▶ Web上で企業のシステム監査活動の統計的収集データは発見できなかった。
- ▶ システム監査企業台帳 システム監査実施企業の台帳を整備、利用促進を図る制度
2022年度の登録企業数は62社である(1996年は64社)。
システム監査学会の賛助会員組織は62社中、1社であった

1) 登録企業によるシステム監査のデータ 前年度実施数

- ・組織体で実施するシステム監査 ⇒ 企業内監査が延べ**343回**実施
- ・企業の委託により実施するシステム監査 ⇒ 企業外監査が延べ**7524回**実施

2) 企業台帳に記載のシステム監査(印象)

- ・様々なレベルのシステム監査があるようだ
- ・7500件も監査委託がある一方、1件も受託していない企業も19社(約3割)ある

2. 企業でのシステム監査の導入と実績

2.2 企業におけるシステム監査活動

(1) 企業におけるシステム監査実施の推奨・要請

- ▶ システム監査実施は、金融・保険関係企業において監査の一環で推奨。
- ▶ 他の業種においては取り組みを推奨する活動はない。
システム監査制度にも、実施推奨など働きかけの仕組みはない。
- ▶ 企業におけるシステム監査活動の現状を調べ始めると、下記のような疑問が生じてくる。
 - ・情報システムに関する障害・事故が発生し、影響も大きくシステム監査の必要性が増していると思われる。
 - ・その状況の割りには企業内でシステム監査が盛んに実施されていない。
 - ・なぜシステム監査が盛んに実施されないか／・企業がもっとシステム監査を実施するようになるためにはどうすればよいか
 - ・金融・保険等での法的規制が監査の実践を要求しているような外圧がないからか

2. 企業でのシステム監査の導入と実績

2.3. 情報システムの企業における役割

▶ 企業での情報システムの役割

(1) ビジネス活動では契約上の要因が各種存在する

図表1.2-1では、情報システムが果たすべき役割を監査を通して示している。

(2) 企業が情報システムを使う経営活動の仕組みは二つ

★ 業務システム: 社内業務のデジタル化における管理テーマ

① 事務、② 管理、③ 経営、などの情報処理

★ 提供システム: 企業の生業。顧客に提供する商品における管理テーマ

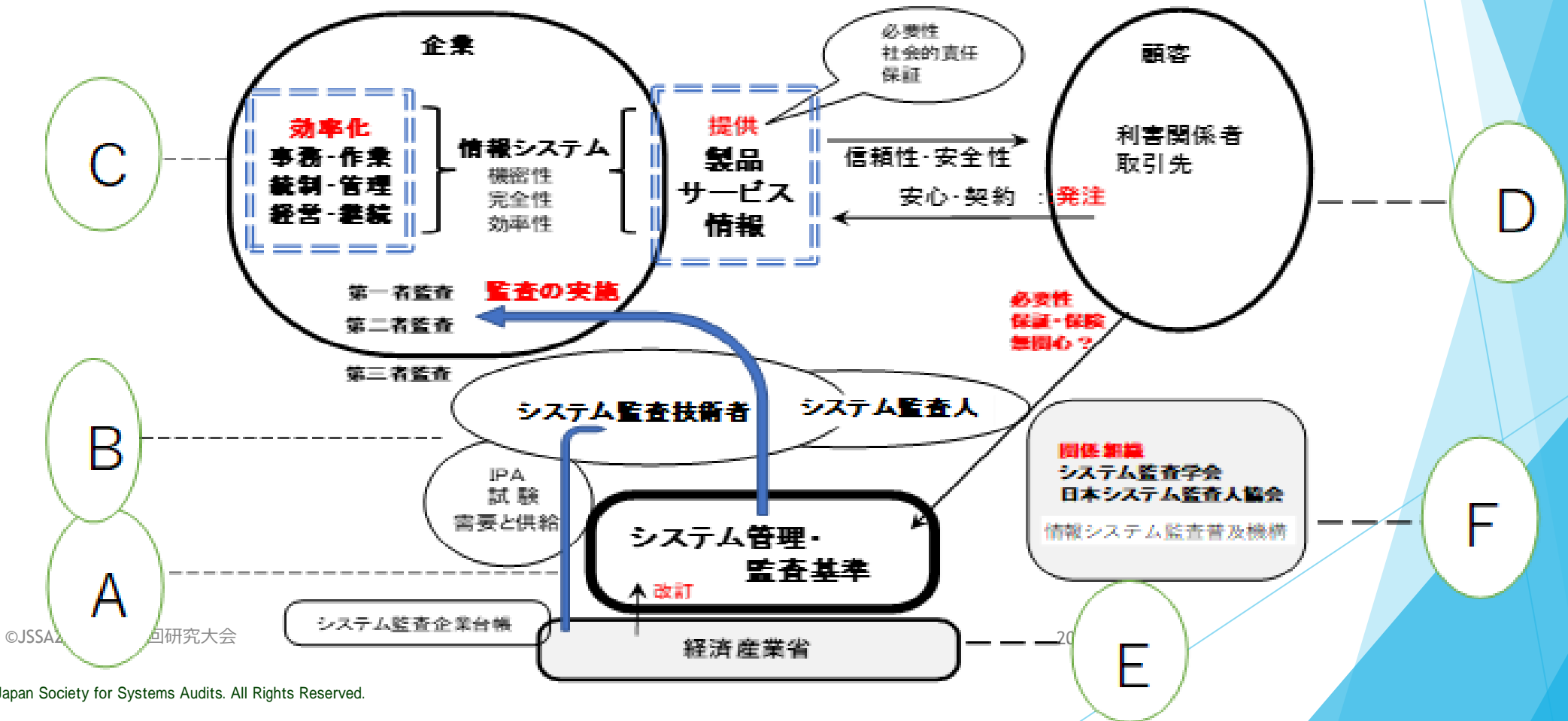
① 製品、② サービス、③ 情報、④ 個人、の商品情報

1. プロジェクト発足の経緯

1.2 研究のアプローチ

図表1. 2-1企業におけるシステム監査活動の関係図

スライド4再掲



3. 企業におけるシステム監査活動の課題抽出

3.1. システム管理・監査基準の持つ課題

(1) 情報システムにおけるシステム監査のカバーする範囲と、要求事項

図表3. 1-1 情報システムの構築フェーズとシステム監査のカバー範囲

フェーズ(局面)	信頼性	安全性	効率性	有効
システム企画	ガバナンス	力量・技術	コスト・効果	×
システム開発	体制・手順、SIer 選定	セキュリティ対策	仕様変更	×
システム運用	可用性	監視、インシデント対応	省力化	◎
システム保守・更新	市場対応、ライフサイクル	更新漏れ	タイムリー	◎
外部サービス管理	SIer 評価、実績	受け入れ試験	コスト	○
システム支援・インフラ	力量・技術	最新技術	コスト・効果	△
システム人材	人材不足	内部犯行	人件費適正	○
事業継続管理	可用性	セキュリティ	訓練・見直し	△

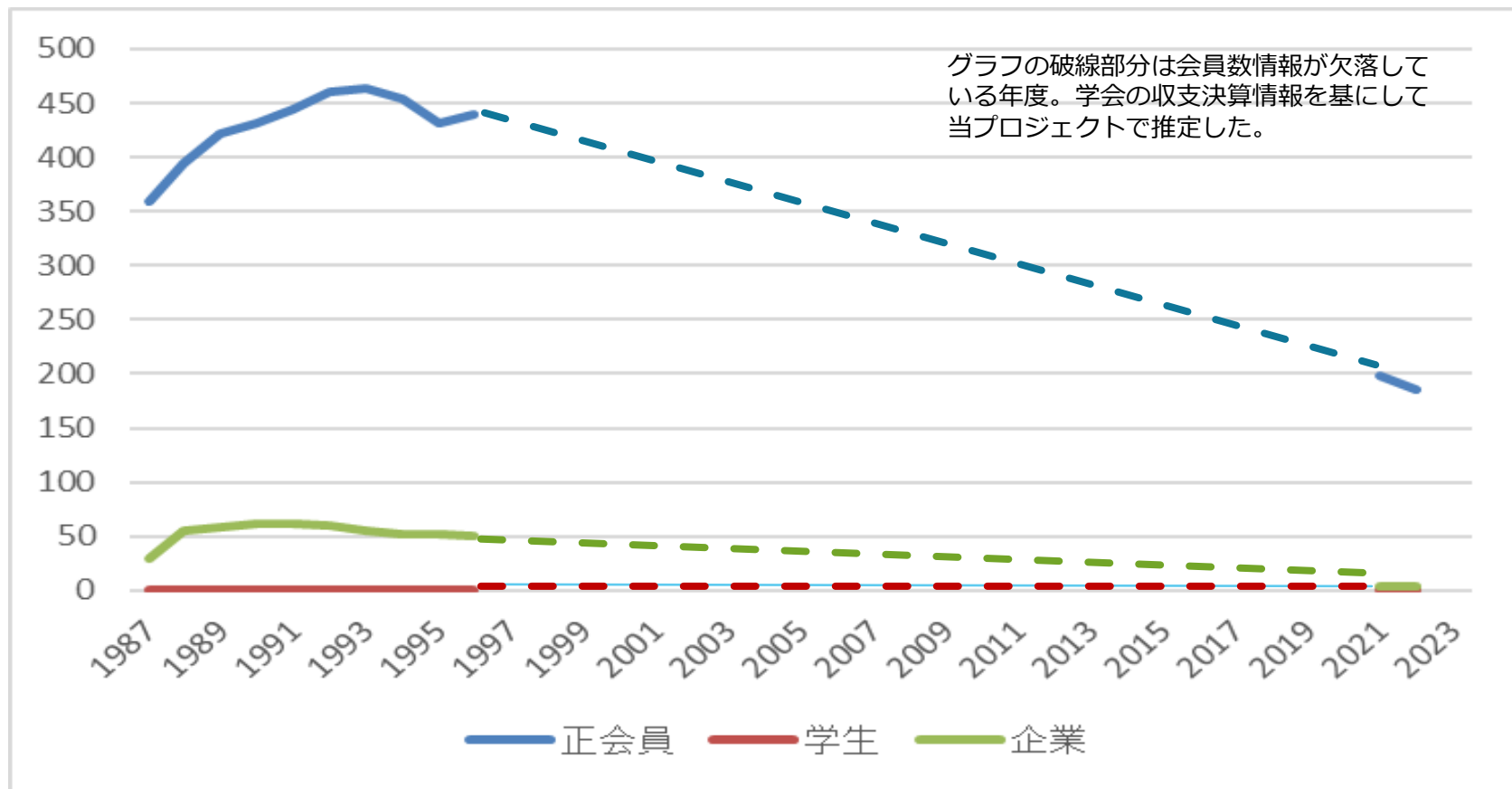
これを見ても分かるように、あまりにも範囲が広すぎて全てを網羅する対策や実践には多くの困難な状況が想定される。システム開発関連に各種の標準・規格がある。システム監査が選択されない結果になる。

3. 企業におけるシステム監査活動の課題抽出

3. 1. システム管理・監査の持つ課題

図表3. 1-1 システム監査学会 会員推移

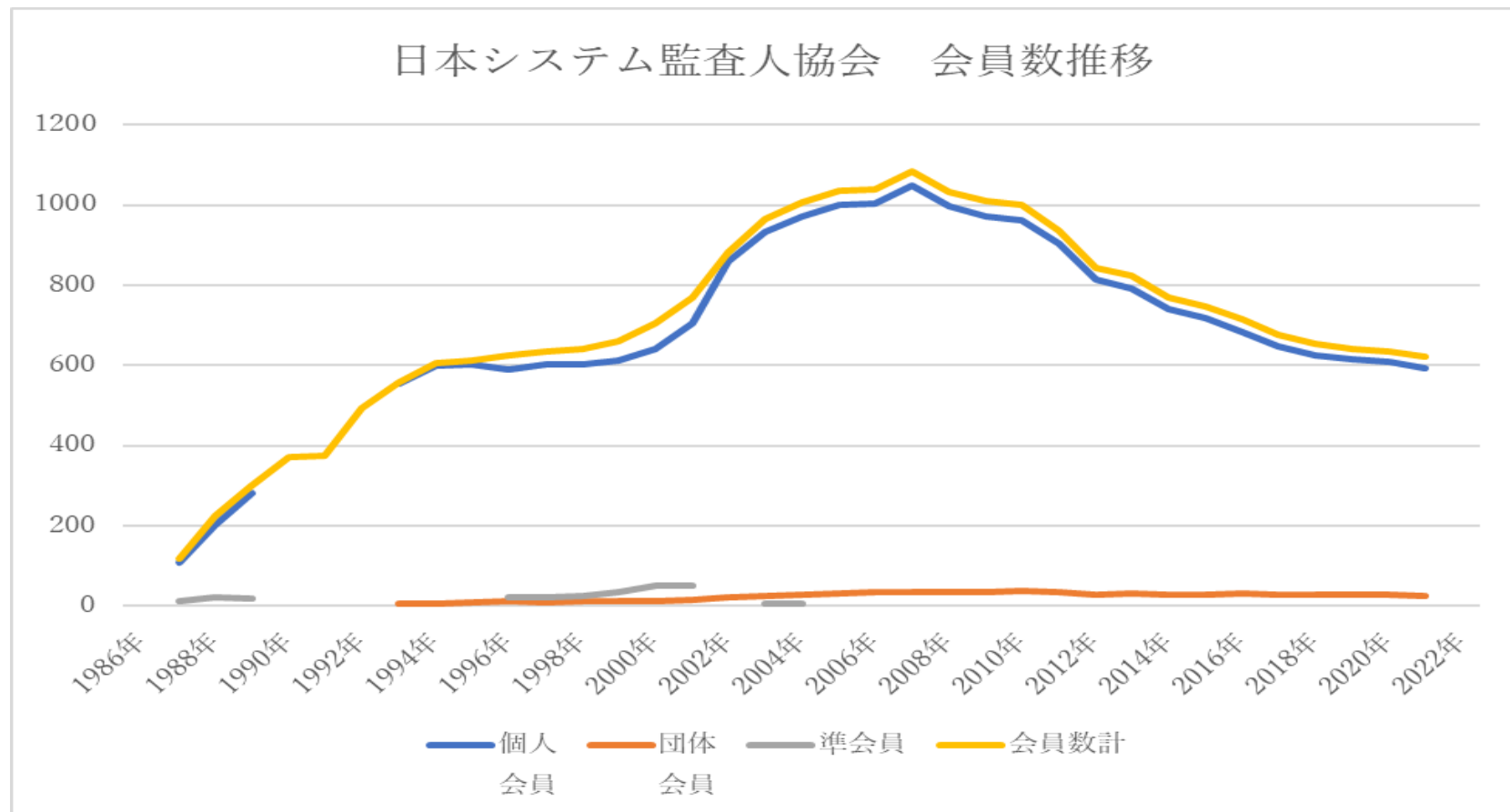
参考資料[14]



3. 企業におけるシステム監査活動の課題抽出

3. 1. システム管理・監査の持つ課題

図表3. 1-2 日本システム監査人協会の会員数 推移 参考資料[15]

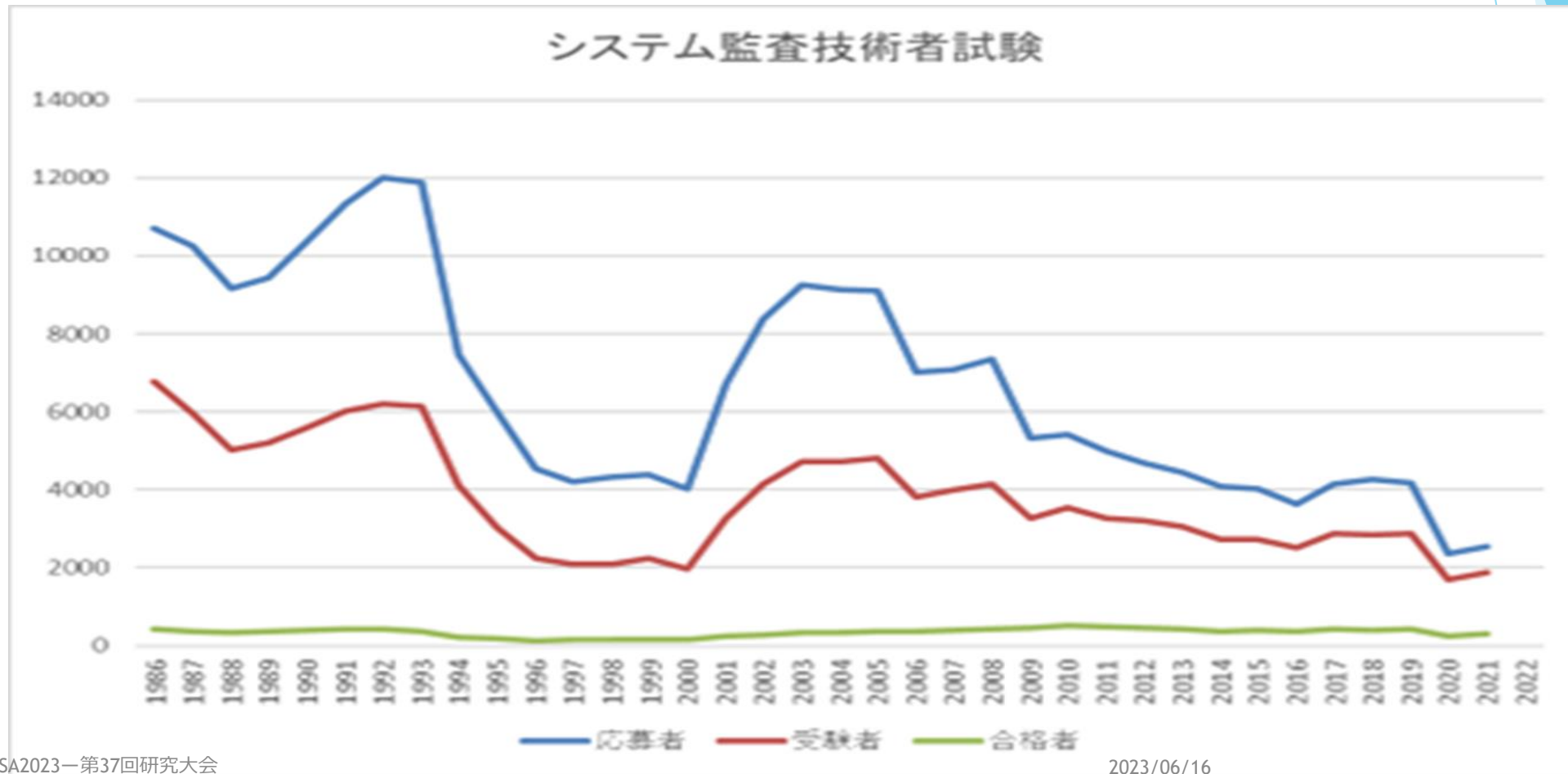


3. 企業におけるシステム監査活動の課題抽出

3. 1. システム管理・監査の持つ課題

図表3. 1-3 システム監査の受験者数の推移

参考資料[13]



©JSSA2023—第37回研究大会

2023/06/16

3. 企業におけるシステム監査活動の課題抽出

3.2. 企業の経営者が持つ課題

(1) 企業の課題

求めるメリット	期待される内容
コストカット	<ul style="list-style-type: none">・コストパフォーマンスが悪いシステムの可視化と対応・無駄な機能を明確化し、システムの再構築・開発作業に活用・自社に必要な機能だけを搭載しているシステムを選定し、無駄な費用の発生を回避
顧客満足度向上	<ul style="list-style-type: none">・メンテナンス頻度増加に伴うシステム障害のリスク最小化・商品やサービスの供給停止の機会を最小化し、スムーズな取引を実現・トラブルが起きた場合もすぐに復旧が望めるため取引先へ安心感を付与
BCP 対策強化	<ul style="list-style-type: none">・サイバー攻撃や内部漏洩に気を配った強力なセキュリティ対策を構築・自社に必要なセキュリティツールに関する助言を獲得・サイバー攻撃や自然災害に伴う被害から最短での復旧を実現
システムライフサイクルの最適化	<ul style="list-style-type: none">・システム開発に関する進捗状況を可視化・開発プロジェクトの妥当性に関する客観的な評価を獲得・遅延が発生している場合は、遅延原因や課題を明確化

(2)このような期待がある中で、経営者からシステム監査実施のニーズが出てこないのが不思議である。

3. 企業におけるシステム監査活動の課題抽出

3.2. 企業の経営者が持つ課題(つづき)

(3) システム監査と改善コンサル機能の連携

システム監査を実施した結果、問題点の指摘をされても、問題の改善方法は示されないということがある。

指摘事項の緊急性、重要性などの助言の他に改善勧告を受けるが、問題解決の助言提案が欲しい。

“改善のための助言を行う”ことはシステム監査実施効果を高める。

システム監査人は監査について独立性・客観性などの要件を満たしたうえで当該分野に対しての見識・能力と技術を持ち、十分な検討の下でそれに応える必要がある。さもないと解決には2度手間となる。

3. 企業におけるシステム監査活動の課題抽出

3. 3. 情報システムに関わる課題

・企業における情報システムの役割で、その機能・範囲は限りなく広範囲に広がっている。システム管理基準で一元的にその信頼性、安全性、効率性を担保できる状況とはなっていないと推察される。現に、情報セキュリティに関連する項目は、「情報セキュリティ管理基準（平成28年改正版）」（経済産業省）を参照することになっている。

- (1) 具体的には、企業が情報システムを使って経営活動を行っている。「3. 4. 利害関係者に関わる課題」の内容が重要です。（契約上の役割を監査を通して保証する）
- (2) 対象情報システムは、クラウド、リモートワークの普及、携帯・端末利用の拡大など、業務形態などが多様化している。
- (3) AI、アンドロイド、メタバース、アバター、アジャイル、などの技術を駆使した情報システムの構築、進展に対して、その取扱い、運用に対するシステム管理基準が必要である。充分とは推測しがたい状況。
- (4) システム監査は、多様化したシステムの監査に対応できていない？
多様化したシステムの監査は複雑で手間暇がかかる。

3. 企業におけるシステム監査活動の課題抽出

3. 4. 利害関係者に関わる課題

- (1) システム監査を実施しても、実施するメリットが明確でない。
顧客等利害関係者に客観的なアピールが弱い、説明根拠が十分でないなど
- (2) しかし、現実のビジネス活動は行われているので、保証への根拠となる構図は、「4. 3. 保証への根拠となる客観的な評価尺度」、「図表4. 3 企業におけるシステム監査の構図」(1)、によって間接的に行われていると考えられる。しかし明確な根拠とは言えない
- (3) システム監査基準【基準3】(システム監査に対するニーズの把握と品質の確保)では監査結果が利害関係者に対する信頼性の保証となる枠組みが経営者による言明書の範囲内である。客観性を持った保証となりうるかの解釈がなされていない
- (4) ここに顧客に対する情報システムの保証のニーズが発生する。従って、ここでシステム監査が保証への根拠となるには保証に関して客観性(第三者的視点)確保に何らかの工夫が必要と考えられる

3. 企業におけるシステム監査活動の課題抽出

3. 5. システム監査の範囲でのリスクとインシデントに関する課題

(1) 障害への対応をどうしているかの情報（社会的に情報共有が少ない）

社会的に影響が大きなインシデントでは対応内容が公表される。それ以外では公になることは少ない。システム監査の実施がインシデント予防に有効であった場合も、その情報共有は少ない

(2) 公表されたトラブル事例から学ぶこと

トラブル、事故発生後は再発防止に真剣に取り組む。課題は事前の取り組みである。

企業はインシデントの予防のため、ルールを整備し判断していると考えが十分でない事例がある。このフェーズに、システム監査を導入する意味は大きいと考える。

▶ システム監査実施は企業の資源が必要。ここで抑止効果を費用対効果に反映するべきか。費用対効果“問題が起きない”メリットを認識し、納得する、見せかたがない。

(3) システム監査をまじめに実施していれば、防げたのでないか リスクアセスメントと基本事項への実直な対応がポイントであり、発生防止、再発防止ができたか、検討する。

(4) 障害対応とトラブルの防止に有効な対処がある。(トラブルの公表事例を参照)

(4) 障害への対応とトラブルの防止に有効な対処

図表3. 5—1 企業におけるインシデントの事例

事件・事故	原因	システム管理基準の要求事項
2020年10月1日に株式売買システムで発生した障害 東京証券取引所	マニュアルの不備により正しい仕様が把握できませんでした。	X.ドキュメント管理、2.ドキュメントの管理 (2) 利用部門及び情報システム部門の管理者は、利用する情報システムや情報サービスの変更に伴い、ドキュメントの内容を更新し、更新履歴を記録すること。
株式会社みずほ銀行におけるシステム障害	月末はシステムに負荷がかかる時期で、45万件＋通常月末処理25万件のデータ更新処理に失敗	Ⅲ. 開発フェーズ、7.移行の管理 (1) PMは、移行計画を作成し、文書化すること <主旨>円滑な移行を実現するために、予め必要な資源、リスク、対策を明確にする必要がある。 Ⅴ. 運用・利用フェーズ、2.運用管理 (4) 運用管理者は、ジョブスケジュールを、業務処理の優先度を考慮して設定すること。
地方公共団体情報システム機構(J-LIS)発注のマイナンバー事業で、2015～20年に少なくとも9件のシステム障害が発生し、再発防止のためのシステム増強などで計約30億3000万円の追加負担が生じていたことが機構への取材で分かった。	再発防止策の11件、計約30億3000万円は機構の負担で追加発注。うち10件をNTTコミュニケーションズが受注(共同受注を含む)するなど、トラブルを起こした業者に依存する状況が浮き彫りになった	Ⅶ. 外部サービス管理、4.サービスレベル管理(SLM) (3) 外部委託元管理者は、外部委託業務がSLAを満たしているかを定期的に確認し、その結果を外部委託元部門長に報告すること。 (4) 外部委託元管理者は、サービスレベル未達成の場合に備え、リソース増強や代替手段の適用など具体的な対応方法を検討していること。

出典 日経新聞 システム障害 トピック一覧 <https://www.nikkei.com/theme/?dw=21071202>

4. システム監査の方向性検討の考慮事項

4. 1. 企業環境の変化

(1) 経営課題・環境の変化

- ▶ 会社が抱えている問題が多すぎて、システム監査まで気が回らない。
- ▶ 余裕がないのでシステム監査を実施する優先順位を上げられない、後回しにされる。

(2) システム監査が他の形態で実施されて検証されているので良しとしている

- 会計システムや顧客管理システムの各種監査等を信頼。システム監査の必要性を検討せず。

(3) 安価で導入しやすい仕組みづくりが難しく、取り組めない

- 費用が掛かり導入しにくいいためか、企業の状況を分析し、検討する必要があるがあっても、費用対効果でお金がかかる、効果が見えないなどを理由に推進されない状況が推測される。

(4) 経営陣の危機意識の内容

- ▶ システムへのセキュリティ意識は高く、ウイルス対策やハッキング対策は実施。一方で、信頼性、効率性などへの対応はなおざりが感じられる。効果的な啓蒙や現実的なトラブル事例で危機意識を理解させる工夫が必要である。
- ▶ また、情報システムの保証に関する課題があり、後述(4.3項)する。

4. システム監査の方向性検討の考慮事項

4.2. 第一者監査の目標と評価

(1) 内部監査の持つ役割

- ▶ 内部監査発生の枠組み → 上図
- ▶ システム監査が実施されない要因と結果 → 下図

(2) 第一者監査の内容を顧客等に信用・信頼してもらうためには、第一者監査の在り方、実施内容等の実施基準の提示が最低限必要と考える。

(3) システム監査の目的であった、信頼性・安全性・効率性について多様な対応策がうまれている。実施に当たって監査目的の見直しが必要でないか。

- ▶ 企業におけるシステム監査の目標
 - ・信頼性 → 開発工程での確認
 - ・安全性 → 情報セキュリティ監査
 - ・効率性 → システム監査での的確な手法でない
 - ・ガバナンス → 経営陣へ指摘できる監査人いるか

監査要求	監査種類	第X者監査
法規制	会計監査 等	第三者
ISO・JIS規格	ISOの監査	第三者
告示等	システム監査	第二者
契約上の要求	取引先監査	第二者
自社の監査要求	社内規程	第一者

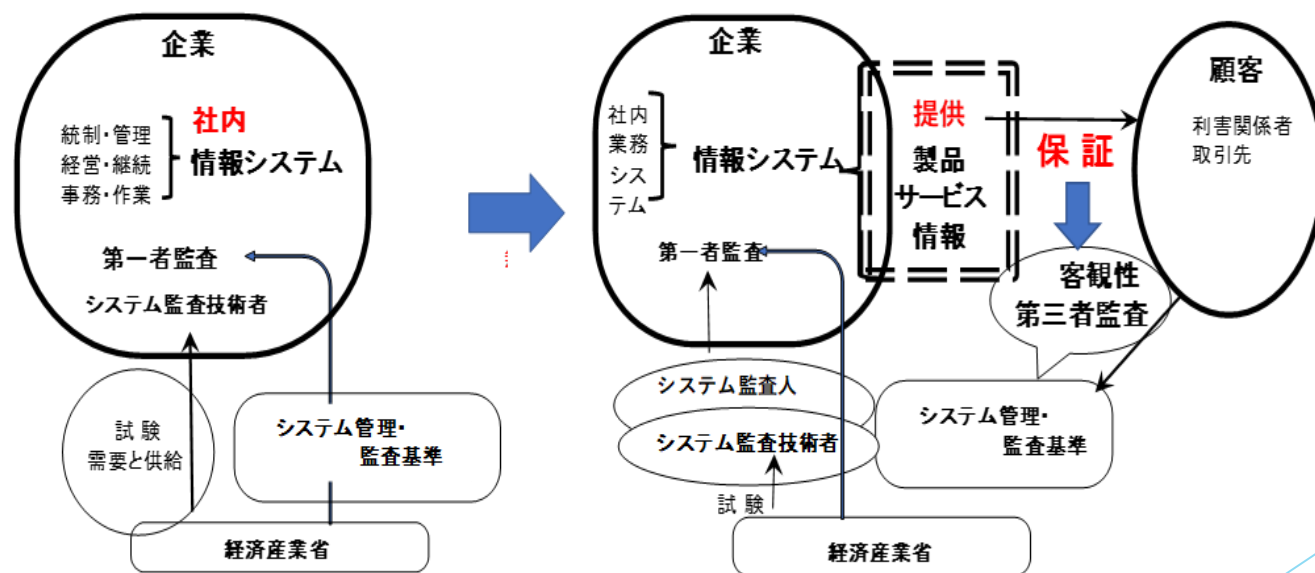
システム監査が実施されない要因	その原因
経営者に知られていない	該当しなければ無関心
経営者の期待・メリットが不明確	顧客アピールが不明確
実施評価できる監査人がいない	社内での意向次第
情報セキュリティ監査が中心	左記以外の余裕なし

4. システム監査の方向性検討の考慮事項

4. 3. 保証への根拠となる客観的な評価尺度

- ▶ システム監査は助言型から保証型への変革が期待されている。
- ▶ 3. 4項(利害関係者に関わる課題): システム監査制度の評価も、数字がないと絵に描いた餅での議論となる。経営者が納得する客観的な評価尺度が必要であり、経営者はシステム監査による評価尺度を得て、それを保証の根拠としてステークホルダー(顧客等)に呈示したい。しかし評価尺度がないのが現状である。

▶ 図表4. 3 企業におけるシステム監査の構図 助言型【当初】⇒保証型【現在】



4. システム監査の方向性検討の考慮事項

4. 3. 保証への根拠となる客観的な評価尺度(つづき)

企業と顧客の取引関係の中で、保証への根拠となる項目を列挙。

(1) 対外的構図

- ・社会的知名度、・上場企業、・長年の取引関係、・信用調査結果、・経営者の信用、
- ・各種第三者認証の取得

(2) 提供しているビジネスへの保証となるテーマ

- ・情報システムの効果検証の枠組みを保証、・信頼性、安全性の保証(保障)、・ステークホルダーの要求事項(納得)を保証、・ITガバナンスの執行を保証

(3) 対内的構図

- ▶ 社内的活動:社内規程の整備、周知徹底、サークル活動、提案制度、社内教育、報償制度、切磋琢磨、ルール化標準化、チャレンジ、トライアンドゴー、進取の気性、システム監査を実施 など

(4) 社内向けに監査がチェックするテーマ

- ・システム開発・運用で手順通りに実施された結果か、・手順は最新、最適な内容に保持されているか
- ・監査での指摘事項の改善がなされているか、・情報システムが現在のニーズを反映しているか

(5) 認証制度であれば、代表的なISOのISMS・ITSMS、ISACAが提供するCOBIT、・アメリカ公認会計士協会(AICPA)が提供するSOC (System and Organization Controls)など。

利害関係者の要求や、認証取得した企業数等で制度の認知度・信頼性の状態が推量可能

4. システム監査の方向性検討の考慮事項

4. 3. 保証への根拠となる客観的な評価尺度(つづき)

(6) 保証型システム監査(システム監査学会の公開シンポジウム(2022年11月26日)で報告)

- ①保証型システム監査は、情報システムの管理者が作成する言明書に対してその内容をシステム監査により保証する。信頼性を付与することを目的にシステム監査を実施する。ニーズから4分類(経営者、委託者、受託者、社会)の主導方式に分けて、夫々の視点で作成された言明書を基に、その内容を当事者間で契約したシステム監査により保証する。企業と顧客(企業)、あるいはユーザには、この言明書が公開の文書になり、信頼を提示する根拠になる仕組みである。
- ②社会一般の企業や個人が利用するには、“社会主導方式”が考えられる。ただ現在は法定化された基準がなく、このシステム監査を誰が実施するか、この結果をどのように管理するか、システム監査実施者の信頼度をどう確認するかなどが課題である。しかし、言明書、監査報告書の公表により監査内容、監査結果を明確に確定できることは、システム監査の実施普及の大きな改革方法になるといえる。 参考資料[11]

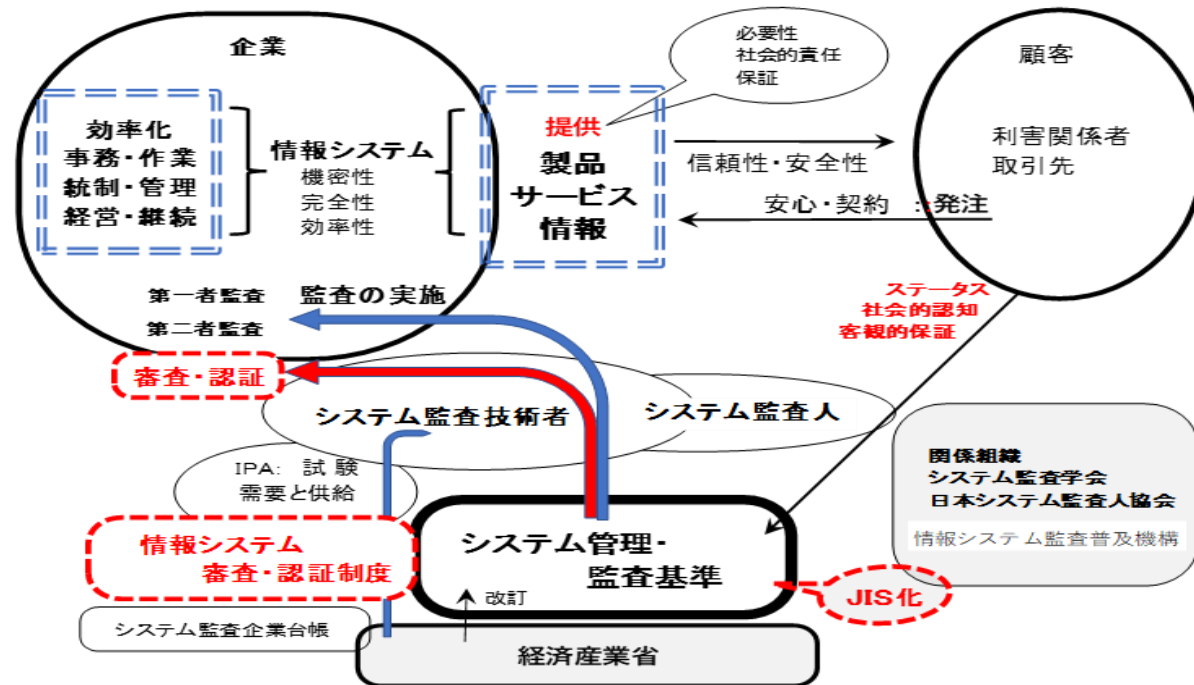
(7) システム監査実施水準の評価

システム監査基準に基づききちんと実施されたシステム監査であることを検証し保証する仕組みは評価尺度に該当する。情報システムが信頼性・安全性の基本を満たすことを数値化して検証する、公開基準に基づき自己評価し公表することで一定の水準を満たしていると認定する仕組みが作れないか。認証が数値化されればそれでも当然良い。

▶ただ、上記全体で 現在根拠となるものは希薄である

5. 企業におけるシステム監査活動の改善の方向性

- ▶ 企業におけるシステム監査活動の実施促進の方向性検討のため下図表5. 1を用いる。特に保証型監査への期待を具体化するための方策が必要となる。
- ▶ 図5. 1 企業におけるシステム監査活動の方向性



5. 企業におけるシステム監査活動の改善の方向性

5.1. 経営における監査の目的と方向性

(1) 企業(経営者に)はシステム監査実施を必要とする要因がありながら実施のニーズが出てこない。
経営陣の意思決定行動に関する期待・要望の①、②を参考資料[4].で分析している

- ① 監査への期待・要望とは？ 情報システム部門、担当者から「当社の業務システムが適正であるか、監査により確認したい」との要望はあるか
- ② 監査の効果がなければ、被監査部署に嫌われる。効果のあるシステム監査、監査体制の在り方は、監査人の力量、教育はどう行われるか

(2) 実施形態のアンマッチの改善 システム監査が情報システムの多様性に十分対応しているか

- ・AI活用による自動化・効率化の工夫、
- ・対面監査とオンライン監査の併用、など方法・技法を検討する
- ・年に一度ではなく、リアルタイムで監査することは可能であるか
- ・サプライチェーンの有効性を確認する連結監査などの有効性の検討

▶ なおシステム監査基準、システム管理基準の2022年度の見直しによりガイドライン部分を民間に移行し、多様性対応についてタイムリーな改訂を可能にされたことにより、今後の改善が期待できる

5. 企業におけるシステム監査活動の改善の方向性

5. 2. 利害関係者との方向性

(1) システム監査実施メリットの評価尺度による標示

顧客等利害関係者に客観的なアピールが弱い。しかし、現実のビジネス活動は行われているので、4.3項(保証への根拠・・・)(1)(対外的構図)の項目とシステム監査実施の結果を結びつけて表示出来れば望ましい。

(2) 顧客・取引先での情報システムの信頼性確認維持の仕組みの確立

▶ 取引でかかわってくる、①製品、②サービス、③情報、についての信頼性の仕組み

★製品では製品の持つ属性が測定可能であれば信頼性が表示される

★サービスでは情報の正確さが重要。特にデータの改竄によってサービス品質が左右される

★情報そのものはフェイクニュースで論じられているように、その信頼性は担保する方法が難しい

(3) 委託元、委託先間での情報システムの信頼性確認維持の仕組みの確立

▶ 企業の業務委託契約に守秘義務、情報管理条項がある。その実行は当事者企業に任される。時には委託元が委託先に監査に出向く等の対応が行なわれるが、委託先が自主的にシステム監査を実施してそれにより契約事項の遵守を担保するような使い方が考えられる。

5. 企業におけるシステム監査活動の改善の方向性

5.3. システム監査及びシステム監査基準・管理基準の方向性

(1) 法制度化への方向性

- ▶ 学会のプロジェクトの検討範囲を超えるが、法制度化への期待がある。
- ▶ システム監査実施状況の評価：システム監査基準に基づき、きちんと実施されているシステム監査であることを検定し、何らかの方法で保証する・認証するような仕組みがあればこれに該当するが、現在これはない。システム監査を実施して基本事項を満たすことを検定する、公開基準に基づく自己評価を公表するような仕組み、一定水準のシステム監査実施の認証が考えられればそれでも当然良い。

(2) JIS Q 19011 (マネジメントシステム監査のための指針) をシステム監査基準として運用
代表的な監査規定 JIS Q 19011 と比較を試みた。監査に当たって、システム監査固有の技法はあるのか、に関して特に顕著な事象はなかった。JIS Q 19011 をシステム監査基準として運用することが考えられる。JIS化された監査基準を使うことで、監査の信頼性を高め、結果を比較しやすくなる。

(3) システム監査基準と改善コンサル機能の連携強化

システム監査結果で指摘事項の改善が必要な場合、システム監査に加えて(コンサルの立場で)適切な助言をすることが有効と考える。監査の独立性・客観性などを確保の上、特に内部監査などにおいて、柔軟な対応を行ってよい場合があると考える。

5. 企業におけるシステム監査活動の改善の方向性

5.4 人材に関する対応の方向性

(1) システム監査に関わる人材の位置づけ

① システム監査基準におけるシステム監査人の要件

システム監査人の要件はシステム監査技術者試験合格者であることが限定ではない。今後様々な経緯を経てシステム監査人になる者(*3)に企業はこれまで以上に留意し、システム監査人としての要件を満たす育成環境・手段の提供に考慮する。

*(*3) 認証取得の監査人：例えばプライバシーマーク、環境14001認証、品質9000認証などの認証取得企業が、認証活動として情報システムの内部監査を実施する(試験合格者以外の)担当者*

② 監査実務の実践・習得

- ▶ システム監査技術者試験の合格者は合格時点では大部分は監査が未経験であると想定される。また別の経緯の者(*3)も同様と言える。監査は個人では経験することが困難な場合が多い。合格・任命後に企業として実践の場を提供する必要がある。

③ システム監査試験合格者の企業における評価

- ▶ システム監査技術者試験合格者の評価は所属企業における必要性かつ有用度によると考える。企業として必要である資格であれば、試験合格者を資格取得手当、あるいは受験料補助、合格時の一時金などで評価する方法がある。

5. 企業におけるシステム監査活動の改善の方向性

5.5 リスクとインシデントに関する対応

▶ システム監査をまじめに実施していれば、事故・障害の発生が防げたのでないか。再発防止への有効性が認められる例もある。対応として次を考える。

(1) 予防型の監査の実施

情報システムの最大のリスクはインシデントの発生である。その対応のために3.5項に記載した内容を含め事故発生防止、対策のチェックに的を絞った予防型監査を手順として規定して行うべきではないか。

1) 各種規定事項を実直に実施しているか

- ・開発・運用・保守・廃棄の各工程のルールの実施確認
- ・運用マニュアルの作成とその周知・徹底確認

2) トラブル発生を誘発する原因の発見

- ・手順を都合よく変更して実施している(ルール違反)
- ・結果のデータを改変(改竄)している
- ・現状に合わない手順のまま放置されている
- ・手順の変更に伴う、改定(規程見直し)を行っていない
- ・手順が最適になるよう改善されていない

しかし、この分野でのシステム監査の実施方法には検討・研究の余地がまだあるのではないか。システム監査の実施、費用対効果の算定、事例の洗い出し、対策のチェックなどにAIを利用するなど。

6. システム監査を支援(サポート)する関連団体への要望

(1) システム監査学会

会員数は3.1項に記載した減少状況。本研究に関しては次の事項への対応を望みたい。

① システム監査学会の中期経営計画(3か年)・年度計画[12]の達成

計画は会員減少などの課題に対して策定され、A.戦略・戦術業務群、G.広報、コミュニケーション業務群などの目標を設定しHPに掲載している。計画達成への取り組みはシステム監査の認知を高め、また普及、促進に寄与すると考える。ただ策定から時間がたっており、組織の変化、更なる会員の減少もあり、情報システム環境等の変化が大きくシステム監査学会への期待、役割も変わってきていると考える。現在の状況を踏まえたものに見直し、計画の達成を図ってほしい。

② システム監査に関する技術、能力を持つ人材の位置づけを、IT人材の技術、能力マップにおいて明確にする。継続的な研鑽目標になるスキルマップの策定・提示を望みたい。チームでのシステム監査実施を考慮したスキルマップが必要と考える。

③ 法規制等の整備への促進対応(5.3項参照)

6. システム監査を支援(サポート)する関連団体への要望

(2) 特定非営利活動法人 日本システム監査人協会

システム監査技術者試験の合格者の団体として発足した。システム監査に携わる実践的な立場の会員が主体の団体でそれが強みである。システム監査に関するCSA個人認証制度とあわせて、啓発・広報活動として幅広くシステム監査実践に関わる出版、研究、教育研修活動を展開している。

2023年度にシステム監査基準、管理基準の改訂に伴い、監査・管理ガイドライン改訂に中心組織として担当する。これにより情報システムの多様化にタイムリーな対応がなされることに期待する。更に次の活動を期待したい。

①幅広くシステム監査人を会員としての取りこみに注力し、システム監査の需要と供給の動向が協会の会員数に表れるように推進する。

(3) 日本内部監査協会

▶ 内部監査及び関連する諸分野の理論及び実務の研究、内部監査人の能力向上、内部監査知識を広く一般に普及する目的で設立された。内部監査基準・内部監査基準実践要綱の策定・公表、情報システム監査専門内部監査士の制定、運用、システム監査を含んだ内部監査に関する研究成果の発表、各種研修会等の開催等の活動を行っている。本報告でシステム監査の実施状況調査の研究成果を参考にした。

(4) 行政等における支援活動

① ISMAP(セキュリティ評価制度)

評価の考え方が民間での制度に活用される期待がある

② デジタルガバメント標準ガイドライン

官公庁でのシステム監査実施を契機に民間への広がりを期待

(5) 情報システム・ユーザー会連盟

システム監査講演会(2022年度第42回)の実施

2023/06/16

7. おわりに

7.1 研究成果

▶ 今回は下記のとおり検討テーマを展開した。

- ① 企業に於けるシステム監査の状況は「2. 企業でのシステム監査の導入と実績」で監査の状況、システム監査活動、役割について論じた。
- ② 企業経営者からの視点は「3. 企業におけるシステム監査活動の課題抽出」として、基準の持つ課題、経営者が持つ課題、情報システムに関わる課題、利害関係者に関わる課題、リスク・インシデントに関する課題について検討した。
- ③ 企業におけるシステム監査活用の方向性に関しては「4. システム監査の方向性検討の考慮事項」において、企業環境の変化、第一者監査、客観的な評価尺度について検討し、更に5項で「経営における監査の目的、利害関係者、システム監査及び管理・監査基準」について方向性の検討を行った。
- ④ システム監査関連団体については「6. システム監査を支援(サポート)する関連団体への要望」で検討した。

7. おわりに

7.2 結論

- ▶ 今回の調査研究を総括して結論を導き出すとすれば以下のとおり
- ① 企業環境の変化に伴い情報システムがビジネスに直接的な役割を担うことにより、システム監査の役割が大きく変わろうとしている変革期であるとの認識が明確になった
- ② 生産性や収益性のみならず、信頼性、保証といったカテゴリーが顧客等の利害関係者から上がってきている。これに応えられるシステム監査の新機軸の形態を模索する必要がある
- ③ 情報システムの企画、開発、運用、保全等の局面で要求される要件はかなり異質なものになりつつある、このため、この要求に対応できる手立てはシステム監査だけにこだわっていても困難を伴うだけで、複合的な検証の制度を構築することが望まれる
- ④ 結局は、経営者がシステム監査に対する価値を認識し実施するか否かが、システム監査の需要喚起のカギとなり、システム監査の社会的な位置づけが明確なる必要要件といえる
- ▶ この調査研究のきっかけとなった、システム監査学会や日本システム監査人協会の会員の減少傾向に対する対策の一助となり、システム監査の振興に役立てば幸いである

7. おわりに

7.3 今後の課題

(1) 情報システムの多様化対応

- ▶ 情報システムの技術、運用、利用関係者の拡大、変化に対応すること
システム監査基準改定により監査・管理ガイドラインが分離され改訂される。適時・適宜の改訂に期待する

(2) 情報システムへの信頼性の保証への対応

- ▶ 保証として、客観的な評価尺度を求める声があることを伺い知ることができた。この対応で、情報システムの安定、監査人の需要と充実が確保され、監査をサポートする組織・仕組みも明確になっていくものと考え

(3) 人材(監査人)

- ▶ ①情報システムの多様化に対応して、様々な分野の専門知識・技能を保持すること(一個人に限定せず)
- ▶ ②監査上のヒアリング、問題発見、レポート等のスキルアップを継続的に蓄積していく手段、場を整えていくこと

(4) 監査実施体制

- ▶ ①監査チーム全体として必要なスキルを満たせるように体制を編成をする必要がある
- ▶ ②IT技術者の参加が不可欠となり、システム開発部門、運用・保守部門から参加を可能にする仕組みが大切
- ▶ ③これらのメンバーを統括してシステム監査を実施できるリーダーの確保が課題となる。社内で育成が充分でない、適任者がいない場合、リーダーを社外に委託することが可能となるよう、関連団体の協力が不可欠である
- ▶ ④システム監査人のスキルマップも監査チームでのマネジメントを考慮した内容が必要

参考資料

- ▶ [4] 赤尾嘉治「サイバーセキュリティ対応を躊躇する経営陣の意思決定行動に関する考察」経営情報学会全国研究発表大会，2016秋.

https://doi.org/10.11497/jasmin.2016f.0_1

- ▶ [11]「保証型システム監査の実践」NPO法人情報システム監査普及機構編 同文館出版（2022年）

- ▶ [12]システム監査学会 <https://www.sysaudit.gr.jp/>

- ▶ [13]IPA HP 試験情報、統計情報

- ▶ [14]システム監査学会 収支決算情報（事務局から入手）

- ▶ [15]日本システム監査人協会 会員情報（事務局から入手）

- ▶ なお、当報告は次の報告書による。

「システム監査の方向性・在り方の調査研究」 2023年6月

（システム監査学会 「監査の適合性チェックとコンサルティング機能の実効性・有効性の達成」
研究プロジェクト）

ご清聴ありがとうございました

- ▶ 研究プロジェクトの内容を、ここでは十分に報告できませんでした。詳細については、当研究の報告書をご覧ください。
- ▶ 報告書：「システム監査の方向性・在り方の調査研究」をご希望の方、及び当報告についての問い合わせは、以下にへご連絡ください。
(kimura-yuu1@jg8.so-net.ne.jp、akao.y@canvas.ocn.ne.jp)
なお、報告書は別途学会誌に投稿予定です。
- ▶ 当研究プロジェクトは月1-2回、オンラインまたは対面で実施しております。
- ▶ 2023年度計画は下記の研究テーマ予定しております。
 - ISO27001の改訂への考察
 - J-SOXの改訂への考察
 - 身の回りにあるミニマムなシステム監査の検討

以上