様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　３０　年　　６　月　　５　日現在

機関番号：　３２６６５
研究種目：　基盤研究(C)（一般）
研究期間：　2015～2017
課題番号：　１５Ｋ０３７８６

研究課題名（和文）情報システムの信頼性に対する外部保証及び内部保証連携モデルの構築

研究課題名（英文）Construction of external assurance and internal assurance cooperation model for reliability of information system

研究代表者

堀江　正之（HORIE, Masayuki）

日本大学・商学部・教授

研究者番号：７０１７３６３０

交付決定額（研究期間全体）：（直接経費）　　1,900,000円

研究成果の概要（和文）：　本研究は、情報システムに関係する外部保証サービスと、内部監査部門によって行われている内部保証としての情報システム監査とを連携させるための概念モデルの構築にある。
　本連携モデルは、次の2つの視点で構築した。第1は、外部保証及び内部保証を通じて検出された情報システムの不備事項を連携させるモデルである。第2は、連続的モニタリングの手法を取り入れた連携モデルである。すなわち、本モデルは、連続的に発生するイベントをモニタリングするモジュール、異常性のあるイベントをリスクカテゴリーにプロットするモジュール、及びリスクに基づくコントロールを連続的にモニタリングするモジュールを組み合わせるものである。

研究成果の概要（英文）：The result of this research is the construction of a conceptual model to link the external assurance services related to the information systems with the information systems audit as the internal assurance services.
In this research, I attempted to construct a cooperative model based on the following two approaches.The first is a model for cooperating defects of the information systems detected through external assurance and internal audit.The second is a cooperative model of external and external assurance that incorporates a continuous monitoring method.This model combines a module that monitors continuously occurring events, a module that plots abnormal events into risk categories, and a module that continuously monitors control based on risk categories.

研究分野：　監査論

キーワード：　保証マーク　認証マーク　保証サービス　内部保証　外部保証　内部監査　情報システム監査　連続的モニタリング

１．研究開始当初の背景

(1) 情報システムの信頼性を対象とした企業等の組織体外部の主体による保証サービスは、認証、証明、評価、審査登録等の名称のもとに提供されており、ゆうに 100 種類を超えている。通例、一定水準にあることの確認をもって保証マークが付与され、「大丈夫です」「確かです」というお墨付きが与えられていることから、保証（assurance）が付与されているとみることができる。

(2) しかしながら、組織体の外部主体によって提供される保証サービスのほとんどは、何を（保証の対象範囲）、どのような方法によって（保証の手続）、どこまで（保証の水準）保証しているかが多様かつ曖昧である。

一方、組織体の内部主体によって行われている保証サービスは内部監査としての情報システム監査であり、情報セキュリティ対策についての改善勧告と保証を行っているのが実情である。

そこで、この2つの保証サービスの連携を図ることができれば、両者の保証サービスをより効果的かつ効率的なものとすることができるのではないかと考えた。

2. 研究の目的

(1) 本研究では、まずもって現状認識を踏まえて、「3 つのディフェンスライン」への着目、及び「連続的モニタリング」の手法を応用することで、組織体の外部主体による保証サービスと内部主体による保証サービスを連携するための概念モデルの構想を目的とした。

(2) このような概念モデルを構想し、実践にも応用できるようにすることによって、外部保証サービスがかかえる課題と内部保証サービスがかかえる課題が解決できるとともに、直接的には、外部保証サービスの中に内部保証サービスを組み込むモデルの実現によって、保証サービスの効率化（同じような保証が重複することによる、いわゆる「アシュアランス疲れ」の解決）にもなると考えた。

３．研究の方法

(1)本研究では、まずもって、提供されている各種認証等の外部主体による保証サービスの種類や内容についての精査を行い、あわせて内部監査として実施されている情報システム監査の特質に焦点を当てた実態把握を行った。この作業は、連携モデルを構築するための基礎となる連携パターンを探る上で不可欠な予備的作業としての位置づけにあった。

(2) 上記の予備的な作業を受けて、第 1 段階として、外部保証の多様性を踏まえた連携のあり方から探り、それを受けて、第 2 段階として、3 つのディフェンスライン・モデルに着目し、組織体内部における統合保証のあり方を究明し、第 3 段階として、連続的モニタリングの手法を外部保証と内部保証との連携に利用するモデル構想を試みた。

さらに、本研究で想定するのは、あくまでも概念的な連携モデルではあるが、実装可能性を無視しては意味がないので、構想した概念モデルについて、外部保証サービスの提供主体及び内部保証サービスの提供主体に対して、その実装可能性についてのヒントを得るべく、インタビューを行った。

なお、本連携モデルは概念モデルとして構想するものであることから、外部保証と内部保証との連携についての理論的な裏付けを固める作業も不可欠なものとなった。

４．研究成果

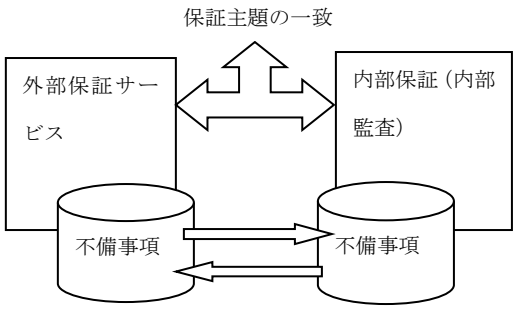
(1) 外部保証と内部保証との連携に関する概念モデルの構想に際して、まずもって外部保証サービス及び内部保証サービスの実態把握を行った。

外部主体による保証サービスは、そのほとんどが保証の範囲及び保証の主題が不明確であることが判明した。各種認証等として実施されている外部保証は、結果的には、保証できるかできないかの二者択一でしかないが、連携モデルを構想する上で、不備等が検出された場合の処理が問題となる。保証プロセスの中で不備等が検出されることのないように、事前のコンサルティング的なサービスが行われた上で保証サービスの提供が行われる事例や、保証サービスのプロセスの中で指導的な機能が発揮されて不備等の修正が行われるケースなど、さまざまな対応が見られたが、発見された不備等を潰すことが優先され、内部保証でみられような、いかなる改善が望ましいかまで進まないことが通例であった。また、不備等が内部監査に適時に伝達されているということも稀であったようである。つまり、保証のプロセスという点では、内部保証（内部監査）との間に本質的な断絶があったのである。

その一方で、内部保証（内部監査）として実施されている情報システム監査は、本来であれば、重大な不備等を原因とする監査報告上の指摘事項が検出されなかった場合には、その旨を保証意見として表明し、指摘事項が発見された場合には当該事項を除いて監査対象に保証を付与し、指摘事項を記載するとともに改善勧告を行う報告スタイルが理想である。しかしながら、実務の多くは、不備等の存在を前提とした評価・検証行為が主であり、指摘事項と改善勧告のみを報告するスタイルが主流であったといえよう。

しかしながら、外部保証と内部保証との連携モデルを想定した場合、下図のように、外部主体による保証サービスのプロセスにおいて検出された不備等が、内部監査部門等に適切かつ適時に伝達され、逆に、情報システム監査としての内部保証における不備等が外部保証の主体に適切かつ適時に伝達されるような仕組みとして構想することが理想である。とりわけ、外部保証の前提として内

部監査が要求されている場合には、このような仕組みが有効かつ効率的なものとなろう。



なお、このようなモデルの前提として、第1に、外部保証サービスを受ける目的が組織体内部の経営管理目的として行われること、及び②外部保証と内部保証の保証の主題を合致させておく必要がある。

(2)　上記のように、外部保証と内部保証との連携を構想する場合、内部保証（内部監査）における保証サービスの特質から、まずもって組織体内における各種保証の統合を想定せざるを得ない。このことは、とりわけ大規模組織においては、内部監査部門における情報システム監査（第3のディフェンスラインにおける保証）、情報システム部門管理者によるマネジメントレビュー（第1のディフェンスラインにおける保証）、情報セキュリティ管理部門等による各部門に対する情報セキュリティ管理状況の検証（第2のディフェンスラインにおける保証）、さらには情報セキュリティ対策等に関するISO認証に係る内部監査等々が重層的になっている現実がある。

そこで、①内部監査部門内における情報セキュリティ監査と業務監査との統合から進め、②情報セキュリティ管理部門等の第2のディフェンスラインが第1のディフェンスラインに対する評価を行っている場合には、第3のディフェンスラインに位置する内部監査部門は、第1のディフェンスラインに対する保証を提供するのではなく、第2のディフェンスラインが行う評価が適切に行われているかどうかの保証を行うものとし、さらに③ISO内部監査のプロセスで検出された不備等について内部監査部門が行っている業務監査の知見を活かして共同で改善事項をまとめるといった段階的な統合を試みた上で、外部保証との統合へと進むというプロセスを踏む必要がある。

また、内部保証と外部保証との統合を目指して、内部監査部門が組織内で保証の対象となるテーマ、保証の主体、保証手続きの計画やその実施方法、さらには保証結果の報告先をあらかじめ仕分けし、全体の調整を行うという機能を持たせることである。

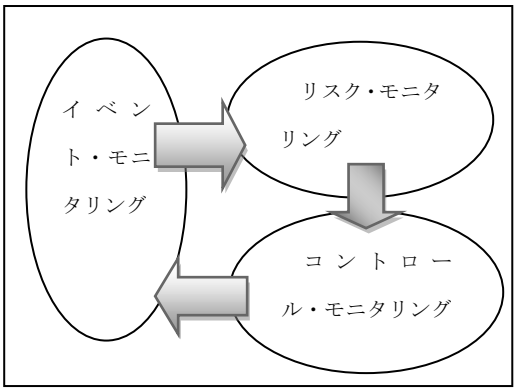
そのための一つのアイデアとして、保証活動の成熟度（高、中、低）を組み込んだ「保証主体と保証対象のマッピング」の考え方を取り込んだ。それは、縦軸に情報セキュリティについての個々のテーマ（サイバーセキュリティ、個人情報保護、外部委託等々）を記載し、横軸には、プロジェクトチーム、マネジメントチームの「第1のディフェンスライン」、情報セキュリティ管理部門、リスク管理部門、コンプライアンス部門、品質管理部門、CSR部門等からなる「第2のディフェンスライン」、そして内部監査部門、ISO内部監査人、外部評価者等からなる「第3のディフェンスライン」をとってマトリックス化し、そこに業務ごとのリスクの大きさ（影響強度と発生可能性）、保証の成熟度、及び現在行われている保証かどうかを重ね合わせてカラーリングするものである。

このように、まずもって組織内において統合的な保証が行われれば、類似の保証サービスが調整・統合されて資源の無駄遣いを避け、最高経営者、統治機関、部門管理者に対してよりよい意思決定を行うための（意思決定のための優先順位づけも含む）保証結果を提供できるのみならず、外部保証との連携をよりスムースに行うことが期待できる。

(3) 連携に関する概念モデルの構想に際して、連続的モニタリングという手法にも着目した。この発想は、かつてカナダ勅許会計士協会とアメリカ公認会計士協会の共同成果として描いた連続的監査（continuous auditing）を元としている。最近では、「データ・アシュアランス」という用語も頻繁に用いられるようになってきているが、トランザクション等の事象の発生と同時に保証を付与する手法である。コンピュータの処理能力の飛躍的な向上によって、事象の発生ごとに保証を付与することが現実味を帯びてきており、くわえて、その際に、ビッグデータやAIを用いることで、保証の精度を飛躍的に向上させることができるようになってきている。

この手法を、外部保証サービス及び内部保証サービスにおいて適用することで、保証の適時性を高めるという目的ではなく、むしろ2つの保証を連携させるための手段として活用することができる。

連続的モニタリングは、下図のように、複数のモニタリングの組み合わせからなっている。



連続的に生ずるイベント（厳密にはトランザクションに限定されない）の発生ごとにそれを記録しつつ、あらかじめ定めたルールから逸脱したイベントが生じた場合にアラームを発し記録する「イベント・モニタリング」の機能がまずもって必要となる。情報セキュリティ対策のためのモニタリング機能に限定すれば、このイベント・モニタリングだけでも意味がある。

しかしながら、本研究では、外部保証と内部保証との連携を想定していることから、図に示すようにイベントから生ずるであろうリスクをあらかじめ想定しておき、とりわけ異常性のあるイベントをその発生ごとに、合致するリスクカテゴリー（リスクの種別、大きさ等）に分類する機能（リスク・モニタリング）を付加し、さらに異常性ありと判定されたイベントの発生ごとにリスクに見合ったコントロールが設定されているかどうか（理想的には、適切に運用されているかどうか）を評価するための機能（コントロール・モニタリング）の組み込みを構想した。

図中、矢印でも示しているように、イベント・モニタリングはリスク・モニタリングのインプットとして機能する。異常性のあるイベントごとに、それに係るリスクがリスクカテゴリーに従ってモニタリングされることこそ重要であるからである。また、リスクが認識された場合には、それにもっとも適合するコントロールが適用されなければならないことから、リスク・モニタリングの結果に基づいてコントロールの状況がモニタリングされなければならないという関係になる。

さらに、リスクに対するコントロールが適切であることが確認されたことをもってイベントの適切性が保証されるというロジックで概念モデルを構想している。したがって、イベント、リスク、コントロールの一連のつながりのなかで、イベントについては、あらかじめ定めたルールから逸脱しなかったものを適切なものとして自動的に保証を付与し、逸脱イベントについてはリスクカテゴリーに基づいてそれに見合った適切なコントロールが設定されているかどうかの検証を通じたコントロールに対する保証を行い（したがって、この場合には一部のコントロールを除いて適切と判断する限定的な保証やコントロールが全体として機能していない旨の否定的な保証ということもあり得る）、最終的にイベントに対してより確証的な保証を提供するという仕組みを想定している。

(4)　このようにリスクとコントロールに対する保証をもモデルの中に組み込むことの理由は、事象に対する保証をより確実にするということ以外に、内部保証（内部監査）の実務にみられる保証のあり方の特性と密接に関連している。

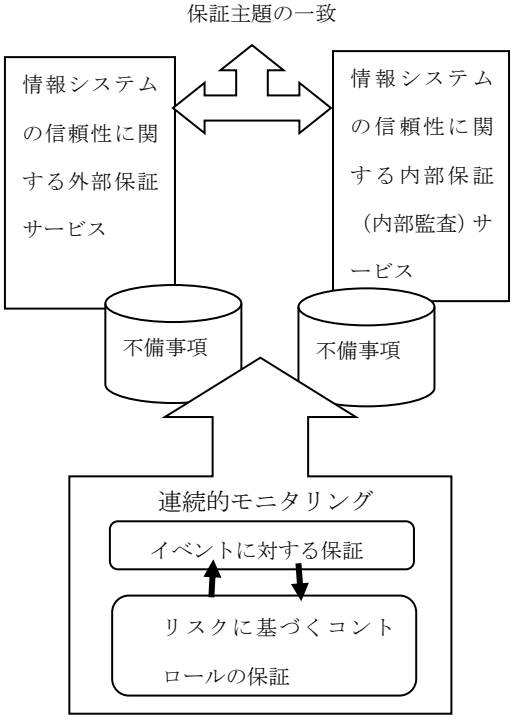
外部保証についてその内容を類型化するとさまざまなタイプがあるが（サイトの実在性証明や開示されているセキュリティ関連の情報の信頼性保証などまさにさまざまである）、そのうち情報システムの信頼性に対する包括的な保証となるサービスでは、情報システムに組み込まれたコントロールに対する保証を付与するものである。

その一方で、内部監査では、すでに（1）で明らかにしたように、情報システムの信頼性（情報セキュリティ監査と言い換えてもよい）に対する監査では、情報システムに対する保証の付与というよりもコントロール上の不備等の検出とそれに対する改善勧告（この改善勧告に力点が置かれている傾向が強いことがインタビュー等を通じて確認されている）に重きが置かれている。

そこで、このような内部保証の実態を踏まえて、外部保証との連携を考える場合、リスクに対するモニタリング機能とそれに対応するコントロール機能を絡ませ、コントロールをリスクとの関係において保証するというモデルが現実的であると考えたからに他ならない。

このように、情報システムの信頼性保証に限定しても、現在提供されている多様性きわまりない外部保証サービスと、改善に重点が置かれた情報システム監査としての内部保証とを連携させると、かなり限定的なモデルとならざるを得ないが、このような限定された領域における統合的な保証モデルを手掛かりとして包括的な連携モデルの構築を試みることが重要であろう。

本研究で想定したモデルの詳細は、逐次公表し、またその実装可能性についても継続してテストも重ねてゆくことになるが、もっともシンプルに本研究で想定したモデルを描けば、下図のようになる。



(5) 最後に、連続的モニタリングに関連して、最新のテクノロジーの活用について言及しておきたい。

第 1 は、ビッグデータ分析の活用である。情報セキュリティに係るイベントのモニタリングをリスクのコントロール評価に効果的に結び付けるためには、単なるシステムログの分析だけではなく、リスクの変化を捕捉するためのデータをはじめ、新たなセキュリティ脅威や組織体を取り巻く環境条件の変化をも捕捉できるデータを取り込む必要がある。とりわけコントロールの有効性評価においては、リスクの変化や、リスクの連鎖・派生現象を捕捉する必要があることから、システムの技術的な側面に限定されたデータ分析のメカニズムを組み込むだけでは不十分であることは言を俟たない。

また、ビッグデータ分析では、相関分析に焦点が当てられることから、単なるシステムログの分析では得られなかった未知の相関が発見されることも期待でき、より深度のあるリスク・コントロールに対する評価が可能となるであろう。

第 2 は、AI 技術の活用である。ビッグデータ分析は「相関分析」にフォーカスするのに対して、AI は「因果分析」にフォーカスする。たとえば、異常性のあるイベントの抽出やリスクカテゴリーへの分類などでは、あらかじめルールをいちいち与えておかなくても、規則性や傾向をコンピュータ自らが獲得するいわゆる機械学習の技術を連続的モニタリングのモジュールとして組み込めれば、より精度の高いモニタリングが可能となるであろう。もちろん、コントロールの有用性評価プロセスにおける推論や判断まで進めるためには、コントロールの有効性評価のロジックを確定しなければならないという難しさがある。また、その場合の特徴量をどのように表現するかといった根本的な問題もある。このように、連続的モニタリングの核心部分への AI の適用については、現実的には乗り越えなければならないさまざまな壁があるものの、外部保証や内部保証のプロセスにおける不備事項の検出や、それらを適切なリスクカテゴリーにプロットする手続への適用であれば、技術的にも十分可能であると思われる。

AI 技術は、監査手続（本研究に即して言えば保証手続）の自動化によるモニタリング業務の効率性の向上といった面のみが注目されるが、ビッグデータ分析とあわせて活用することで、モニタリング精度の向上という視点で考えてゆく必要がある。

本研究では、当初、このような新しいテクノロジーを外部保証と内部保証との連携モデル、とりわけその中核技術となる連続的モニタリングのどの局面にどのように組み込むかまで計画していなかったこともあり、具体的な研究成果まで得られなかったので、今後の研究に反映してゆきたいと考えている。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　７件）

① 堀江正之、内部監査の品質管理・品質保証の考え方、會計、査読無、192 巻、2017、79-93
② 堀江正之、IT の進展による監査業務の深化、会計・監査ジャーナル、査読無、29 巻、2017、124-131
③ 堀江正之、統合アシュアランスのあり方に関する序論的検討、産業経理、査読無、76 巻、2017、4-13
④ 堀江正之、会計監査のシンギュラリティは到来するかービッグデータと人工知能のインパクト、税経通信、査読無、72 巻、2017、8-15
⑤ 堀江正之、監査人の不正摘発力の向上、青山アカウンティング・レビュー、査読無、6 巻、2016、66-72
⑥ 堀江正之、三線ディフェンスモデルの検討、會計、査読無、190 巻、2016、16-29
⑦ 堀江正之、ガバナンス監査へのシフトする内部監査、會計、査読無、188 巻、2015、31-43

〔学会発表〕（計　２件）

① 堀江正之、システム監査の品質と課題、システム監査学会、2017
② 堀江正之、監査規制としてのガバナンスと高品質な監査環境整備、日本監査研究学会、2016

〔図書〕（計　０件）

〔産業財産権〕
○出願状況（計　０件）

○取得状況（計　０件）

〔その他〕
ホームページ等

６．研究組織

(1)研究代表者

堀江　正之（HORIE, Masayuki）
日本大学・商学部・教授
研究者番号：７０１７３６３０