様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２７ 年　 ５ 月 ２０ 日現在

機関番号：３２６６５
研究種目：基盤研究(C)
研究期間：2012～2014
課題番号：２４５３０５７６

研究課題名（和文）クラウド・コンピューティングに対するオフサイト型連続監査モデルの構築

研究課題名（英文）Development of the offsite audit model for continuous monitoring in the cloud computing environment

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）　　2,000,000円

研究成果の概要（和文）：　本研究は、ユーザ企業が、クラウド事業者のセキュリティ・リスクと内部統制を効果的にモニタリングするための概念モデルの構築を行うものである。システムとして自動化された形式でリスク・プロファイルを連続的にモニタリングできる技術を導入することで、リスクと統制に関する情報を効果的に分析できる。ユーザ企業は、クラウド事業者の開示用モニタリングデータベースにアクセスするか、又は内部監査人によるアシュアランス報告書からオンデマンドで必要な情報を入手することになる。

研究成果の概要（英文）：　The research project involves development of a conceptual model that user entities effectively monitor security risk and control in a cloud vendor. Using continuous monitoring techniques of risk profiles in systemized form provides an effective means of analyzing risk and control information in a cloud vendor.　User entities can gather useful information through on-demand access the monitoring database or the internal auditor’s assurance report in a cloud vendor.

研究分野：監査論

キーワード：クラウド・コンピューティング　オフサイト監査　連続的モニタリング　連続的アシュアランス　マチュリティ・モデル　自己評価　リスク評価　外部委託管理

１．研究開始当初の背景

(1) 企業等が自前でシステムをもつことなく、外部のコンピュータ資源をオンデマンドで利用するクラウド・コンピューティングは、今後、着実に増加することが予想される。

クラウド環境では、データがインターネットを介して国内外で分散処理・保管される。それゆえ、ユーザ企業（又はその監査人）は、特定のデータセンターに出向いて、当該センターの内部統制の状況を確かめることが現実的ではなくなる。

そこで、ユーザ企業が、Web を介して、クラウド事業者側におけるセキュリティ管理（内部統制）の状況を必要に応じてモニタリングできる仕組みの構築が必要となるのである。

２．研究の目的

(1) 本研究の目的は、ユーザ企業が、Web を介して、クラウド事業者側でどのようなセキュリティリスクを認識し、それに対してどのような内部統制を構築・運用しているかについての情報を直接入手したり、リスク変化に応じた内部監査結果を適時にモニタリングできるオンデマンド型のモニタリング手法の概念モデルを構築することにある。

クラウド事業者側における情報開示で重要な点は、リスクと内部統制のセット開示という考え方である。そこで、本概念モデルでは、クラウド事業者におけるリスクと内部統制との関連を視覚的に理解できる手法を応用する。

(2) また、将来的には、クラウド事業者側のモニタリング・モジュールとユーザ企業側のモニタリング・モジュールとを接続できれば、ユーザ企業側の監査人等はオンデマンドで情報を入手し監査データとして加工することができる。

３．研究の方法

本研究は、大まかに、予備的調査、全体的なモデルの構想、リスク・プロファイリング・モデルの構築、モニタリング・モデルの構築というフェーズに分かれる。

(1) 予備的調査では、ユーザ企業がクラウド事業者の内部統制の有効性を評価・確認するための方法としての、質問書法（確認書法との併用を含む）、直接監査法、内部統制に関する証明書や認証を利用する方法の課題について、ユーザ企業、クラウド事業者、及び監査法人等に対するヒアリング調査によって情報を収集し整理した。

(2) 全体的なモデルの構想では、リスク・プロファイリング・モデルとモニタリング・モデルの接合が必要となることから、両者のシステム的な連携メカニズムについてとりわけ注意を払った。

(3) リスク・プロファイリング・モデルの構築フェーズでは、リスクを特定し、対応する統制手段と統制強度が視覚的に理解できるような設計とした。また、モニタリング・モデルは、クラウド事業者及びユーザ企業が、オンデマンドで、リスク変化に基づく内部統制の変更情報を入手できるような仕組みとし、クラウド事業者の内部監査人によるアシュアランス報告書への Web を介したユーザ企業からのアクセスも可能とする設計とした。

なお、本研究では、当初より、概念モデルの構築を目的としており、実装可能性についての簡単なテストは含めたが、実際にプログラミングを行って情報システムとして開発することまで目的とはしていない。

４．研究成果

(1) 予備的調査から得られた知見

予備的調査の結果、ユーザ企業は、クラウド事業者がどのようなリスクを認識し評価しているかではなく、むしろデータセンターにおける内部統制が有効に設定され運用されているかどうかについての情報を入手し

たがる傾向がある。その一方で、クラウド事業者は、内部統制に関する「包括的な情報開示」にはそれほど大きな抵抗を示してはいないが、リスク評価結果に関する情報開示に難色を示す傾向が確認された。

そのようなことから、ユーザ企業が用意した内部統制質問書にクラウド事業者からの回答を求める質問書法や、クラウド事業者が自社の内部統制の有効性に関する外部監査人の証明や認証を受けてその結果を開示するといった実務が主流であったと推定される。一定時点又は一定期間における内部統制の全般的な有効性が重視されており、リスク変化を原因とする内部統制の変更を細かくフォローする仕組みについては、その重要性すらほとんど認識されていなかったといってよい。

しかしながら、内部統制はリスクの種類と大きさ（発生可能性×インパクト）によって設定・運用されるべきものである。したがって、内部統制はリスクと関連づけられてはじめて意味をもち、クラウド事業者側にとっても、リスク変化を適時・適切に反映できる仕組みがあればより望ましいことは言うまでもない。

また、このような仕組みをユーザ企業側への情報開示に援用すれば、リスク変化に基づく統制の変更についての情報（逆に、リスク変化がないにもかかわらず統制の変更があったという情報も含まれることになる）の適時な提供が可能となる。

ユーザ企業側では、内部統制が適切に「運用されているかどうか」につよい関心を有し、その確証を希望していることから、「リスク―内部統制」の関連性の変化を適時に知ることができるモニタリング手法があればその利用ニーズが高いことも明らかになった。

(2) 概念モデル構築の概要

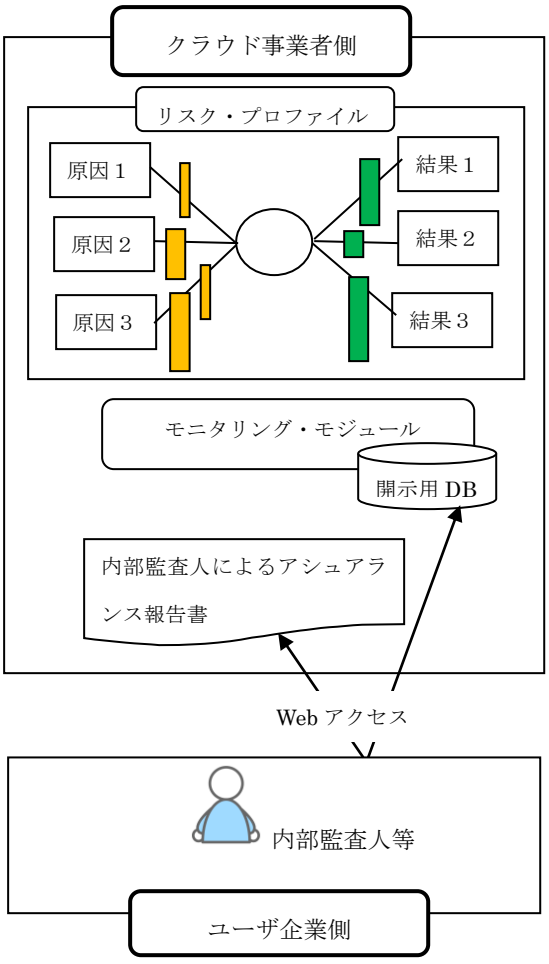
① 概念モデルの仕組み

以上のような予備的調査の結果からも、リスクに応じた内部統制が実際に有効に運用されているかどうかを、ユーザ企業側で、Web を介して連続的にモニタリングできたり、クラウド事業者の内部監査人によるアシュアランス報告書にアクセスしてオンデマンドで必要な情報が入手できる仕組みの構築が求められる。

概念モデルの構築に際しては、JIS Q 31000:2012 の附属書にみられる「蝶ネクタイ図」を援用することとした。

蝶ネクタイ図を援用することで、リスクの原因と結果を対応づけて表すことでき、そこに重ねるようにリスクに対応する事前の「予防策」と事後の「緩和策・復旧策」とに分けて統制手段を描くことができ、しかも相対的な統制強度もあわせてイメージできるように、リスクをプロファイルリングできる。

当該概念モデルは、おおよそ次のような仕組みとなる。



* 図中、「原因」側の縦棒は予防策、「結果」側の縦棒は緩和策・復旧策を表し、棒の大きさが統制強度を示す。

② ユーザ企業側にとってのメリット

このモデルでは、リスクの原因と結果、リスクと統制手段とを関連づけてプロファイリングできることから、ユーザ企業側では、これまで入手できなかったリスクと内部統制との結びつきをオンデマンドでかつ視覚的に知ることができるというメリットがある。

また、リスクと統制との関連性を描くことができるので、クラウド事業者のリスクの原因事象が変化したときに、それに対応する統制手段が適切に変更されているかどうかといった情報も知ることができる。蝶ネクタイ図に変更があったときに、それをユーザ企業に自動的に知らせるアラームを組み込むことで、ユーザ企業では適時なモニタリングを行うことが可能となる。

このように、ユーザ企業は、クラウド事業者が用意した開示用のリスク・プロファイル・データベースや、クラウド事業者側の内部監査人による連続的なアシュアランス報告書にアクセスすることで、必要な情報を適時に入手することができる。

③ クラウド事業者側にとってのメリット

一方、クラウド事業者側からみたときに、リスク変化に応じた内部統制の変更が適切に行われているかどうかを内部監査人が適時にモニタリングすることができる。このような変化・変更のプロセスを電子データとして処理・共有・活用することで、機敏なリスク管理手段として活用することができる。

このように、蝶ネクタイ図を援用したモデルは、クラウド事業者側におけるリスク管理の一自動化手段としての活用が第一義的に考えられる。とりわけ、リスク事象の変化によって、「事前防止策」が変更になった場合、「事後緩和策（復旧策を含む）」をどのように変更すべきかの検討材料を得ることができる。

また、クラウド事業者は、内部統制に関する証明書や認証を入手・取得する方法のように、外部の監査人の立ち入り調査を受ける必要もないことから、事務手続きの軽減にもなる。

④ オンデマンド・アシュアランス・モデルへの展開

以上に述べてきた概念モデルは、基本的に、クラウド事業者による自己評価をベースとしたものである。したがって、その信頼性をいかに担保するかは、別の問題として残る。

本概念モデルを前提とした自己評価の信頼性をいかに担保するかについては、クラウド事業者側における内部監査を通じたアシュアランス機能の発揮が考えられる。

クラウド事業者側に内部監査機能が存在する場合、その内部監査人は、モニタリング・モジュールを通じて、リスクに対して適切な種類と強度をもった内部統制が設定されているか、またリスク変化によって内部統制が適切に変更されているかについてのアシュアランスを付与するための情報を自動的かつ適時に入手することができる。

従来、本モデルで提案しているような Web を介した内部監査によるアシュアランス結果の外部開示という発想はみられなかった。今後、内部監査でなければできない連続的な監査機能を生かして、リスク変化ないしは内部統制の変更があった場合の適時なアシュアランスをオンデマンドで開示できるような仕組みへの展開が考慮されるべきである。

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６件）

① 堀江正之、「再委託先の内部統制評価を巡る課題」、『會計』、査読無、第 186

巻第 5 号、2014 年、pp.29-41。

② 堀江正之、「地方自治体の情報セキュリティ監査にみる『内部監査の外部化』」、『會計』、査読無、第 184 巻第 5 号、2013 年、pp.15-28。

③ 堀江正之、「情報セキュリティガバナンス：規制の情報セキュリティから戦略の情報セキュリティへ」『Nextcom』、査読無、第 10 号、2012 年、pp.22-29。

④ 堀江正之、「外部委託に係る監査・保証：最近の基準改訂と理論的課題」、『会計・監査ジャーナル』、査読無、第 24 巻第 8 号、2012 年、pp.91-96。

〔図書〕（計２件）

① 内藤文雄編著、宮本京子、児嶋隆、松本祥尚、吉見宏、伊藤公一、林隆俊、那須伸裕、正司素子、堀江正之、越智信仁、『監査・保証業務の総合研究』、中央経済社、2014 年、pp.143-153。

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