Vol.2014-DCC-7 No.1
Vol.2014-EIP-64 No.1
2014/5/14

有価証券報告書にみるリスク認識のあり方について
－　金融機関とシステムベンダの認識の差異　－

嶋作泰洋[†1]　　原田要之助[†2]

多くの組織では業務の多様化・複雑化やコストカットなどを理由に、業務の外部委託を行っている。金融機関においても業務の外部委託を行っており、特に情報システムにおいてはシステムの運営・開発なども合わせ、外部委託が幅広く利用されている。有価証券報告書にて、金融機関とシステムベンダのリスク認識の差異について調査した。この調査から、金融機関は外部委託に対するリスク認識が乏しい事がわかった。外部委託先に対して適切な管理方法を確立する事は、企業にとって重要な課題のひとつである。

Study on risk awareness in securities report
－Differences in the recognition of system vendors and financial institutions -

YASUHIRO　SHIMASAKU[†1]　YONOSUKE HARADA[†2]

IT Outsourcing is common for the purpose of diversification, complexity or the cost cut of duties in many organizations. Outsourcing in the financial institution is common, has been widely used in the information system in particular, including the operational administration or the development of the system. Investigation of the differences in the perception of risk between financial institutions and system vendors has performed based on Annual Securities Reports. From this investigation, the risk recognition of the outsourcing in financial institutions has been poor. Establishment of appropriate management methods for IT outsource has become one of the most important tasks for enterprise.

1. はじめに

企業のサービスが多様化・複雑化しており，それに伴い自社内の業務も多様化・複雑化している．自社内の人員だけでは、より良いサービスを作り上げる事は困難になり，多くの企業は業務の一部を外部委託している．

特に情報システムは近年技術進歩が著しく高度な専門性が求められようになっており，多くの企業で戦略的に外部委託を利用するようになっている.金融機関においては，情報システムが事業基盤そのものであり，巨大化複雑化する中で外部委託を広く利用している．

本稿では，外部委託先管理を含めた内部統制を取り上げ調査した．その結果，内部統制の差が，前提となるリスク認識によるのではないかとの仮説を立て，リスク認識と内部統制との関係性について考察を行った．委託側の金融機関とその金融システムの運営を担うシステムベンダのそれぞれの側から調査し，どのようなリスク管理をすべきかについて考察する．

第２章で背景の説明を行い，第３章以降から本論に入る．

†1 情報セキュリティ大学院大学
Institute of Information Security
†2 情報セキュリティ大学院大学
Institute of Information Security

2. 背景について

本稿において調査対象とした「有価証券報告書」及び金融機関の事業基盤となる情報システム「勘定系システム」について，概略を説明する．また，内部統制の広がりについて記載する．

2.1 有価証券報告書について

有価証券を発行している企業が自社の情報を開示するために作成する報告書をいう．上場企業では，事業年度終了後３か月以内に金融庁に提出することが義務付けられている．これらは公認会計士または監査法人の監査証明がされた企業の公的な外部への意見表明である．

有価証券報告書の構成は，「企業情報」と「提出会社の保証会社等の情報」の二部構成となっており，監査証明として「監査報告書」及び「確認書」が記載されている．監査証明の範囲は，業務の内容は当然の事ながら，公開する文章も対象となっており，内容に虚偽があった場合には罰則規定が設けられている．

企業情報には，「企業の概況」，「事業の状況」，「設備の状況」，「提出会社の状況」，「経理の状況」，「提出会社の株式事務の概要」,「提出会社の参考情報」が記載されている．また，「事業の状況」において，「事業等のリスク」「コーポレートガバナンスの状況」が記載されている．

2.2 勘定系システムについて

勘定系システム[1]とは金融機関の情報システムの中で最

も重要な基幹システムであり，預金や融資，為替といった資金移動を行うためのシステムである．この勘定系システムは，各金融機関で共通する業務システムについてコスト削減や新サービスの迅速な対応といった観点から，地方銀行を中心に共同でシステムを構築・運用するようになっている．現在，地方銀行１０８行のうち７７行が勘定系の共同システムを利用している．

2.3 内部統制について

（１）COSO 内部統制フレームワーク

ＣＯＳＯの内部統制フレームワーク[2]には，①会計統制だけでなく，事業活動全般にわたるきわめて広義の内部統制概念を採用していること，②有効な内部統制の構築に資する目的から，その策定および運用に第一義的な責任を負うべき経営者の視点に立脚したものとなっていること，③内部統制とは統制目的を達成するためのプロセスであり，組織に属するあらゆる人間によって遂行されるものであると位置づけていること④内部統制の有効性は，取締役会および経営者が統制目的に関する合理的な保証を得られるかどうかによって判断されること，⑤内部統制に関する経営者報告およびそれに対する監査人の関与を想定し，その基礎となる概念枠組みを形成していること，といった５つの特徴がある．

（２）日本における内部統制構築の取組みについて

日本では，2006 年 5 月に会社法が改正され，会社法第三百六十二条・会社法施行規則第九十八条・会社法施行規則第百十八条において，コンプライアンスやリスクマネジメントを整備することを明文化された. また, 内部統制については，2006 年 6 月には金融商品取引法が国会で成立し，金融商品取引法の中の第二十四条の四の四（財務計算に関する書類その他の情報の適正性を確保するための体制の評価）において定められ, この部分は内部統制報告制度と呼ばれ，企業が財務に関係した内部統制を構築するための基礎となっている．

制度を構成するにあたって，（１）に述べた米国のＣＯＳＯ内部統制フレームワークに対して，目的に「資産の保全」，基本的要素に「ＩＴへの対応」を追加している．内部統制報告制度では，従来の制度監査とは異なり，リスクベースアプローチによりリスク分析を行い，内部統制に係る規則や規定を策定し，それが企業内で有効に行われている事を表明する事，また，内部統制の有効性を担保するために，年一回以上，公認会計士などによる外部監査の実施を求めている．

企業における内部統制を継続するため，外部監査が義務付けられているが，この監査項目が膨大であり，時間・費用が掛かる．そのため，実務では効果的に監査を実施するために，初年度にリスクコントロールマトリックスを満たす内部統制を構築し，次年度以降はリスクの高い部分を重点的に見る方針により，業務などに変更が無ければ，前年度のものを適用できる，すなわちリスクが高くなく変更がない場合には，詳細な監査を省略することができるという運用となっている．

人材・人員不足からリスクに重点を置いた監査を運用することは難しく，このような監査実態が内部統制の構築に対する形骸化の一要因に成っていると考える．

（３）COSO 内部統制フレームワークの改訂について

米国ＣＯＳＯ内部統制フレームワークは 2013 年 5 月に改訂版が公表されている．[3]

内部統制の３つの目的と５つの構成要素という大枠は変更ないが，目的のひとつである「財務報告」が「報告」に変更されている．旧フレームワークは外部向けの「財務報告」に焦点を置いたものであったが，今回の改訂で，外部向け財務報告だけではなく，非財務報告および内部向けの「報告」についても内部統制の中に含まれることとなった．

さらに，今回の改訂で，内部統制の５つの構成要素それぞれを支える概念が『原則』として明示され，それらを「１７の原則」と呼び，１７の原則が機能していることを示す８７の着眼点が明示された．原則や着眼点は，外部委託している業務に当てはめる事ができ，外部委託に対しても従来よりも広い範囲で内部統制を考えなければならず，なおかつ，外部環境の変化も考慮しなければならないというものである. 日本では, これに対応した改訂を検討中である．

3. 有価証券報告書に基づく各金融機関のリスク認識の比較

3.1 リスク認識について

有価証券報告書の「事業等のリスク」の記述内容を分析することで，金融機関がシステムや外部委託に対してどれほどリスクを認識しているかを調査した．金融機関は，メガバンク†3，地方銀行†4，第二地方銀行†5，その他銀行からシステムの運営形態別にそれぞれ経常収益を基準に２５の金融機関を選出した．勘定系システムを共同化している金融機関は，共同システム毎に幹事行†6 または主力行†7 を選出した．選出した金融機関を，勘定系システムの運営を委託しているか否か，勘定系システムの運営を委託しているのであれば共同化しているか否か，の３つに分類し，「システムリスク」，「外部委託に関するリスク」，「インシデントに対するリスク」について整理した．また，本稿ではリスク発生時に自行に与える影響を，０（影響なし）～５（事業継続に影響）の６つにランク付けを行い，図１及び図２

†3 全国規模の業務を展開している普通銀行.
†4 本店所在の都道府県内を主たる営業基盤とする普通銀行.
†5 相互銀行や信用金庫から転換した普通銀行.
†6 勘定系システムの共同化参加行のうち, 共同システム運営の幹事を行っている金融機関.
†7 勘定系システムの共同化参加行のうち, 発言力が大きい（規模が大きい）金融機関.

に示す．図１及び図２中の縦軸及び横軸は，それぞれのリスクの影響度を示し，勘定系システムの運営を自社で行っている金融機関は「自営行」，自社単独で委託している金融機関を「単独行」、委託し共同化している金融機関を「共同行」と表現した．

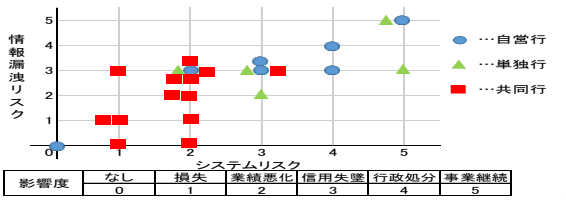

図１：金融機関のシステムリスクとインシデントに対するリスクの影響（有価証券報告書を元に作成，[4]）

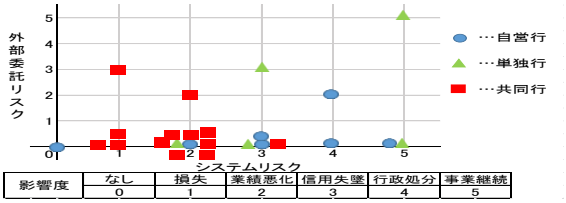

図２：金融機関のシステムリスクと外部委託に関するリスクの影響（有価証券報告書を元に作成，[4]）

図１，図２から金融機関によりリスクの認識が異なり，リスクが顕在化したときの事業への影響度も異なっている事が分かった．勘定系システムの運用を自社で行っている金融機関に比べ，外部委託している金融機関の方がシステムリスク顕在化時の事業への影響は小さいと認識しており，共同システムを利用している金融機関はこの傾向が顕著に見られる．

また，勘定系システムの運営・開発を外部委託している金融機関でも，外部委託に関するリスクを表記していない事が分かった．

3.2 リスク認識の推移

特定の金融機関のシステムリスク及びインシデントに関するリスク認識（影響度０から５）の経年変化について過去１０年間の有価証券報告書をもとに調査した結果を図４及び図５に示す．図４及び図５では，特定の金融機関は，それぞれのカテゴリから経常収益が大きい金融機関のみを選出している．

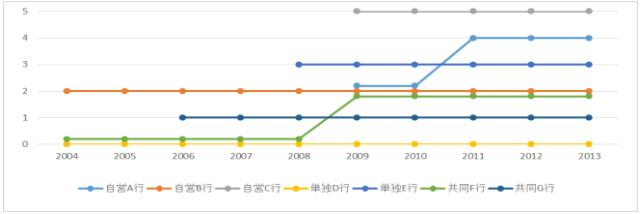

図４：金融機関のシステムリスクの認識推移（有価証券報告書を元に作成，[5]）

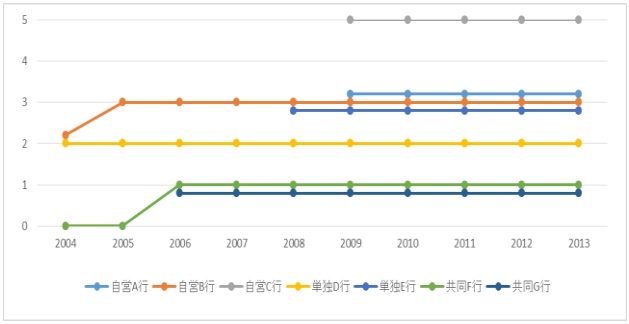

図５：金融機関のインシデントに対するリスクの認識推移（有価証券報告書を元に作成，[5]）

「事業等のリスク」の推移で，文言の変更があったのは，法改正や大きな金融危機，大災害，また，自行内の大きな経営面の変更があった時のみであり，それ以外では文言の変更は無く，ほぼ毎年同様の内容で記載され続けている．

3.3 考察

リスク認識の調査から以下の事が推測される．

今回調査した金融機関に共通して言えることは，外部委託をリスク要因と見なしていないという事である．また，システム運営を外部委託している金融機関は，システムに関するリスク認識が乏しい．また，抽出した全金融機関ともリスク分析の見直しはあまり行われていない．

以上の理由となっているのは各金融機関とも内部統制報告制度に基づく運営をしているためで，システムに大きな変更が無ければリスクは変化していないとしているためと考えられる．また，IS031000：2009「リスクマネジメント」が策定される以前において，外部委託する事はリスク移転であり，自社へのリスクがなくなると考えられてきた事（現在は，リスクの共有と考え，リスクが移転されて無くなるとは考えない）も一因であると考えられる．

内部統制において，管理すべき範囲が広がりつつある中，金融機関では，外部委託について，まだリスクがあることを認識していないことが分かった．

４章以降にて，外部委託先について記載する．

4. 経済産業省のガイドラインについて

経済産業省は，外部委託先管理やコーポレートガバナンス構築の一環として，2009 年 6 月に「アウトソーシングに関する情報セキュリティ対策ガイダンス[6]」及び「情報セキュリティガバナンス導入ガイダンス[7]」といったガイドラインを公表している．その内容について述べる．

4.1 アウトソーシングに関する情報セキュリティ対策ガイダンス

「アウトソーシングに関する情報セキュリティ対策ガイダンス」では，アウトソーシングを，「計画プロセス」，「実行・評価プロセス」，「改善プロセス」の３つのプロセスに分け，

各プロセスのセキュリティ管理について記載している．リスクを検討する際に考えなければならない論点として,「事業戦略」,「リスク管理」,「事業継続」,「情報システムの信頼性」,「サービス品質」,「法令遵守」,「知財管理」,「安全保障」の８つを挙げている．３つのプロセスそれぞれでリスクを検討し，サイクルを回していく事が有用であるとしている．

なお，本書の「アウトソーシングに係る情報セキュリティ管理の考え方」において,『情報セキュリティ上の脅威への対処については，発注元企業がアウトソーシング先の情報セキュリティ対策を直接コントロールすることが一般には難しいため，契約における情報セキュリティ上の要求条項の明確化，発注元企業の判断によるアウトソーシング先に対する監査の実施，といった間接的な手法を検討する必要がある.』と委託先管理の困難さについて述べている．

4.2 情報セキュリティガバナンス導入ガイダンス

「情報セキュリティガバナンス導入ガイダンス」では，『情報資産の管理が経営戦略そのものであり，それを支えるリスク管理の一環としての情報セキュリティ対策こそバリューチェーン・サプライチェーンの高付加価値化を支える重要な要素である』と述べ，情報セキュリティに関わる意識，取組及びそれらに基づく業務活動を組織内に徹底させるための仕組みを構築･運用する必要があるとしている．

本書では，情報セキュリティガバナンスのフレームワークを提示しており,「方向付け」,「モニタリング」,「評価」,「監督」,「報告」,の５つに分けている．経営陣が経営戦略やそれに基づくリスク管理方針を策定し（方向付け），管理者層で情報セキュリティの管理を行う．その戦略に従って適切にリスク管理出来ているかの情報を集め（モニタリング），集めた情報から情報セキュリティ目的･目標が実現出来たかを評価する．目的・目標が未達の場合，原因を分析し，目標・目的を見直す．このサイクルが適切に遂行出来ているかを監督し，経営陣は利害関係者に対し，リスク管理状況について報告する．

外部委託先管理において，委託元が直接コントロールできるのは「方向付け」,「モニタリング」,「評価」の３つであり，この３つで委託先をコントロールする必要がある．

５章では，文献調査（アンケート）による，企業の外部委託先管理方法や従業員の不正防止対策について述べる．

5. 外部委託先に対する管理方法及び従業員の不正防止対策について

文献は,情報セキュリティ大学院大学原田研究室の「2013情報セキュリティアンケート[8]」,日本銀行の「金融機関におけるシステム外部委託の現状について[9]」,独立行政法人情報処理推進機構（以下，IPA と言う）の「組織内部者の不正行為によるインシデント調査[10]」の３つについて比較・調査した.「2013 情報セキュリティアンケート」では ISMS 及び P マーク取得先における外部委託先管理について,「金融機関におけるシステム外部委託の現状について」では地方銀行における外部委託先管理について,「組織内部者の不正行為によるインシデント調査」では従業員及び経営者が不正対策として有効な対策について，それぞれのアンケート結果をまとめた.これを以下に示す.

5.1 2013 情報セキュリティアンケート

（ｉ）概要

情報セキュリティ大学院大学原田研究室では毎年，情報セキュリティに関するアンケートを行っている．2013 年度は，2013 年 7 月から 8 月に ISMS または P マーク取得企業及び大学 4,378 組織に対しアンケートを郵送し，367 組織から有効回答を得ている．有効回答を得た組織は，情報通信業が 45%で，次いで大学が 20%，人材派遣などのサービス業が 11%，売上規模は 50 億円以下の事業体が 75%以上である．設問は，情報セキュリティマネジメントの取組み状況，情報セキュリティへの管理体制と人材育成，情報セキュリティのガバナンス，営業秘密の管理，クラウド・コンピューティング，事業継続計画等となっている．

（ⅱ）委託先に対する情報セキュリティ及び個人情報保護に関する方針

「顧客の立場として，購買方針や調達方針（IT 委託，業務委託を含む）が策定されていますか．策定されている場合，個人情報保護および情報セキュリティに関する項目が含まれていますか.」の設問に対し，IT 業務の委託に対する部分を抜粋し，図６に示す.

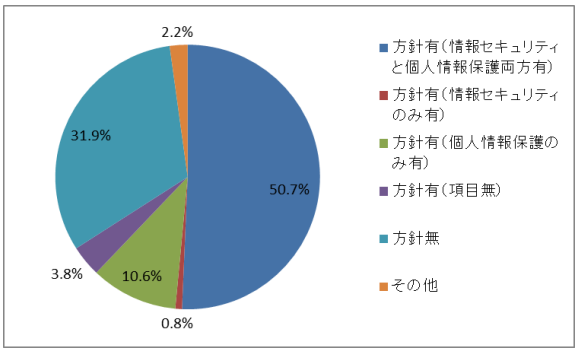

図６：委託先に対する情報セキュリティ及び個人情報保護に関する方針（N=367）

図６から，約７割の組織が，原部材やサービスを調達する際の方針の中で情報セキュリティや個人情報保護について方針を策定している事が分かった.

（ⅲ）情報セキュリティポリシーで委託先に関わる項目

「情報セキュリティポリシーの中で委託先に関する項目はありますか.」の設問の回答を図７に示す.

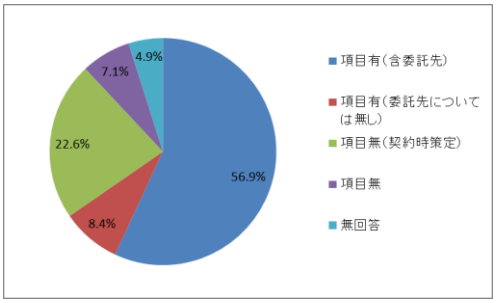

図７：情報セキュリティポリシーの中で委託先に関わる項目（N=367）

図７では，７割弱の組織が情報セキュリティポリシー中で委託先について触れており，契約時に策定も含めれば約９割の組織が委託先に対して何らかの取り決めをしている事が分かった．

（iv）多重委託に対する管理

「顧客の立場として委託先・調達先を選定する際に，下請けになる二次，三次といった委託先・調達先に情報セキュリティ管理(個人情報保護を除く)を要求していますか.」の設問の回答を図８に示す．

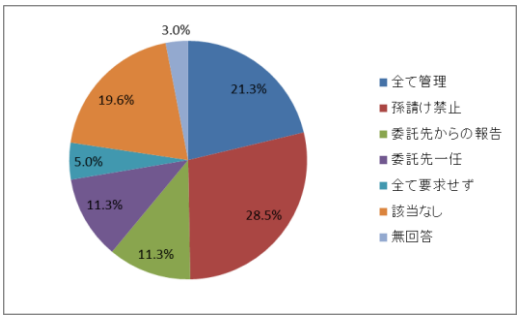

図８：多重委託に対する管理（N=367）

図８では，約半数が「全て管理」及び「孫請け禁止」と多重委託に対し一定の制限を設けている事が分かった．

（v）外部委託先への管理手法

「外部委託している運用中のシステムのセキュリティ管理は，どのような手法を用いていますか（複数選択可)」の設問に対し，有効回答は 367 組織中 354 組織あり，うち「外部委託業務はない」の回答数 119 組織を除き，235 組織の管理手法を図９に示す．

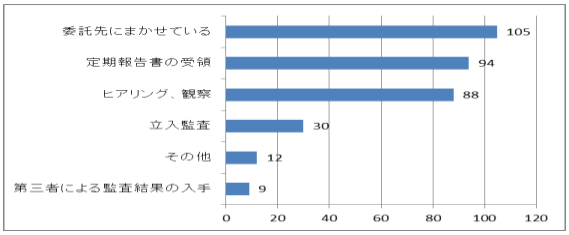

図９：システムの外部委託管理手法（N＝235）

図９から，システムの外部委託のセキュリティ管理では，「委託先任せ」が最も多く，次いで「定期報告書の受領」「ヒアリング，観察」が主流であり，「立入監査」や「第三者による監査結果の入手」が少ない事が分かった．

（vi）考察

以上のアンケート調査から，委託先に対し情報セキュリティの方針作成や多重委託に対する規制のような「方向付け」は行うものの，図９に示すように「モニタリング」は不十分である事が分かった.「モニタリング」が不十分であるため，その「評価」も不十分であることが予想される．

この理由としては，委託元企業は管理策として「定期報告書の受領」「ヒアリング，観察」で十分であると考えている，委託元の管理能力（管理手法）不足，委託元の管理者不足，委託先への管理の丸投げ体制，となっていることなどが推測される．

5.2 金融機関におけるシステム外部委託の現状について

（ｉ）概要

日本銀行は 2008 年 4 月に，地域銀行全 109 行，信用金庫のうち日本銀行取引先 268 信金の 377 行庫に対しアンケート調査を実施している[9]．設問は，外部委託の進展状況，委託先の管理状況，委託先管理の現状認識と今後の方針の構成となっている．本稿では，地方銀行に対する回答のみを抜粋している．

（ii）委託先の情報セキュリティポリシー・スタンダート遵守状況

委託先に対し，「自行庫†8 の情報セキュリティーポリシー・スタンダードの適用範囲が委託先にも及ぶことを，規程上明定」及び「委託先との契約上，委託先に自行庫の情報セキュリティーポリシー・スタンダードに基づくセキュリティ要求事項の遵守義務を課す」の２つの設問への回答を図１０に示す．

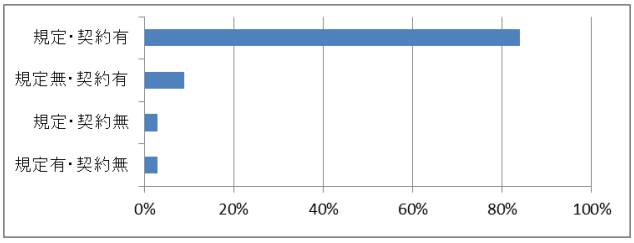

図１０：セキュリティポリシー・スタンダートの規定・契約の有無（出所：日本銀行，N＝109）

図１０から，ほぼ全ての地方銀行が，委託先に対し何らかの取り決めをしている事が分かった．

（iii）再委託の状況

「委託先から第三者への再委託の可否」,「再委託時の事前承認制度の有無」,「再委託先からの再々委託の制限の有無」についての回答を図１１に示す．

†8 銀行、信用金庫において自組織を指す。

Vol.2014-DCC-7 No.1
Vol.2014-EIP-64 No.1
2014/5/14

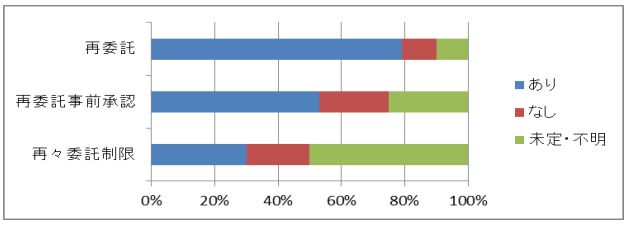

図１１：再委託の状況（出所：日本銀行，N=109）

図１１から，地方銀行の約８割が再委託を認めており，再委託には事前承認を求めていることが分かった．

（iv）外部委託先への管理方法

「定例打合せの実施（以下，打合せと言う）」，「定例報告書の受領（以下，書面受領と言う）」，「委託先への立入監査実施（以下，立入監査と言う）」，「委託先が実施した監査結果の入手（以下，監査結果と言う）」の実施状況についての回答を図１２に示す．

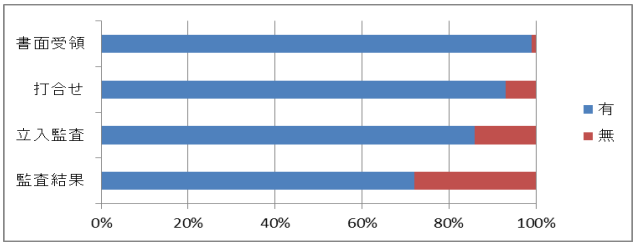

図１２：外部委託先への管理方法（出所：日本銀行，N=109）

図１２から，地方銀行では，打合せや書面受領の実施率が９割を超えているほか，立入監査，監査結果も７割以上の先で実施されていることが分かった．

「金融機関におけるシステム外部委託の現状について[9]」では，さらにそれぞれの管理方法についても設問があり，その内容を述べる．

打ち合せでは約９割が月次以上で実施しており，作業内容や個別障害に対する内容がほとんどであり，障害分析や性能確認についての内容は約８割，SLA の見直しや管理方法の見直しについての内容は約４割止まりで，通常業務に係る内容がほとんどであった．書面受領については，ほぼすべての地方銀行が月次以上で実施しており，作業内容から管理方法の見直しまで網羅されている．立入監査については，年一回の実施が約６割，年複数回の実施が約４割であった．監査担当者は，銀行内部の担当者や外部監査人が７割以上であった．監査結果についても，年一回の実施が約６割，年複数回の実施が約４割であった．入手する監査結果は，「金融庁検査マニュアルや FISC の安全対策基準の充足度評価」のギャップ判定が８割，財務会計監査の監査結果が５割であった．

（v）委託先管理の運用業務における十分性

委託先管理の十分性に対し，「現状で十分」，「強化する必要があると認識しており強化計画がある（以下，強化必要・計画有りと言う）」，「強化する必要があると認識しているが強化計画はない（以下，強化必要・計画無し）」，「管理レベルは低下する方向であるが仕方ない（以下，レベル低下容認と言う）」の回答を，図１３に示す．

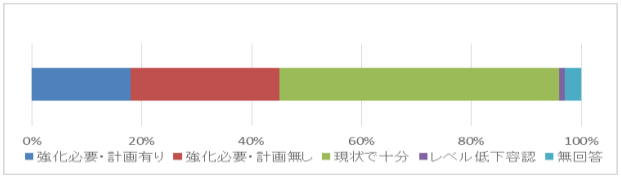

図１３：委託先管理の運用業務における十分性（出所：日本銀行，N=109）

図１３から，運用業務については，「強化必要・計画有り」と「強化必要・計画無し」を合わせた管理強化の必要性を認識している地方銀行と現状で十分と回答した地方銀行はほぼ同じであった．

（vi）考察

図１０～図１３より，地方銀行では，「方向付け」や「モニタリング」についてある程度の実施が認められる．しかしながら，委託先管理の十分性では回答が分かれ，約半数が管理強化の必要性を認識している．調査結果や調査報告からは，地方銀行は，ISMS または P マーク取得先企業における「モニタリング」より管理体制を整えられていることが分かるが，まだ不十分であり管理強化が必要であると述べられている．これからは，外部委託先の管理がいかに困難かが読みとれる．

5.3 組織内部者の不正行為によるインシデント調査

（i）概要

IPA は 2012 年７月に，内部不正対策される側の社員や職員を対象にした 3,000 人の Web アンケートと，内部不正対策をする側の経営者及びシステム管理者を対象とした 110 人アンケートの２つを実施している[10]．アンケートの内容はほぼ同一であり，設問により一部言い回しを変更している．

（ii）不正行為に対して効果的だと考えられる対策

「不正行為に対して効果的だと考えられる対策（複数選択，上位５つ）」の調査結果を，従業員向け及び経営者向けのアンケート結果を合わせて図１４に示す．

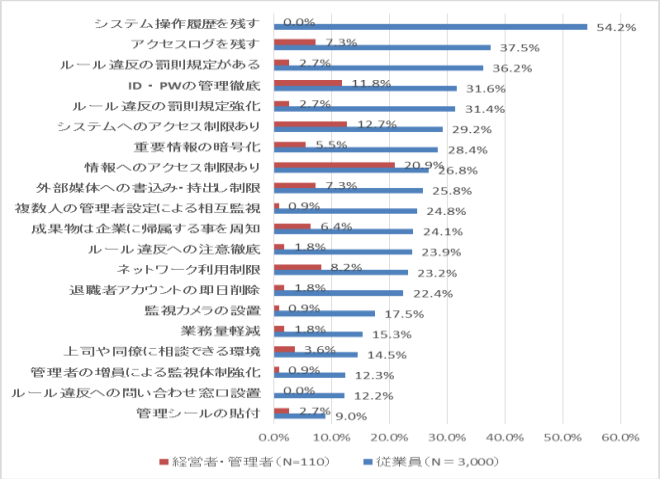

図１４：不正行為に対し効果的な対策（出所：IPA のアンケート調査を元に作成）

図１４から，証拠が残ることが一番の対策であり，ルール違反に対する規定やシステムや情報へのアクセス制限も効果がある対策である事が分かる．

（iii）考察

図１４に示す対策のうち，委託元が直接コントロール出来るものは，ルール違反に対する規定や，情報の暗号化のみであり，ほとんどの対策は委託元が直接コントロール出来ない．大半の対策は，委託元が委託先に対して行う間接的なコントロールであり，中には委託元で全くコントロール出来ないものもある．間接的なコントロールについては，委託先が委託元の満足する対策を実施するとは限らず，実施していない場合，実施していないことを理由にして委託先に対し罰則を与える事は難しい．それは委託先が満足のいく対策を実施していない場合，その対策を実施させる事が難しいと同義である．

委託元が，委託先の対策について十分と感じるのは，委託元と委託先のリスク認識が近しい，または，委託先が委託元と同様のリスク認識を持ち，かつ，委託先のリスク認識の方が高い時のみであると考えられる．

そこで６章にて，金融機関とシステムベンダのリスク認識の違いについて考察する．

6. 金融機関とシステムベンダのリスク認識の違い

本章では，有価証券報告書を用いて，金融機関とシステムベンダのリスク認識と内部統制の構築の違いを調査する．すなわち，有価証券報告書の「事業等のリスク」及び「コーポレート・ガバナンスの状況」について比較する．

調査対象は，共同システムの幹事行または主力行の金融機関，また，その共同システムのメインフレームを作成しているシステムベンダ，システムを自営しているメガバンク，業界大手かつ共同システムを手掛けていないシステムベンダ３社とした．

「事業等のリスク」では，「アウトソーシングに関する情報セキュリティ対策ガイダンス」が述べている，リスクを検討する際に考えなければならない８つの論点を参考に，情報システムの運営・開発を外部委託するといった視点で各企業が掲げているリスクの違いを比較した．

「コーポレート・ガバナンスの状況」では，各企業の内部統制の仕組み/体制の違いを比較した．

6.1 リスク認識の差異

「アウトソーシングに関する情報セキュリティ対策ガイダンス」の８つの論点のうち，「リスク管理」，「情報システムの信頼性」，「法令遵守」から，それぞれに関わるリスクについて比較した．また，合わせて，内部統制構築に関わるリスク，内部不正に関わるリスクが有価証券報告書に記載されているかどうかを調査した．その結果を図１５に示す．縦軸にはそれぞれのリスク，横軸にはそれぞれのリスクを有価証券報告書に記載している企業数を表している．

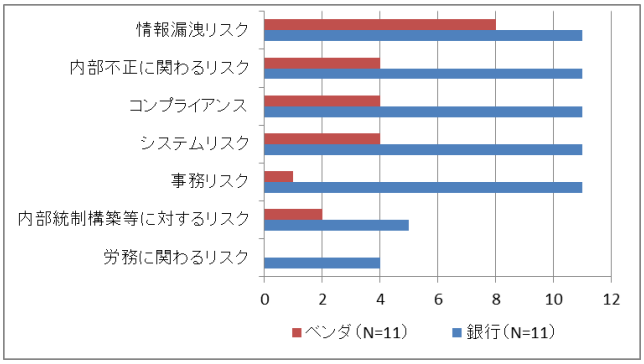

図１５：リスク認識の差（有価証券報告書を元に作成[4]）

図１５から，システムベンダは金融機関に比べ，システムリスクや事務リスク，コンプライアンス，内部不正に関わるリスク等の認識が低い事が分かった．業種による違いとはいえ，リスク認識の差が大きい．情報システムは金融機関において，金融インフラを支える重要なものであるため，金融機関はシステムベンダに対して，リスク管理について多くを求める必要がある．しかしながら，図２から金融機関は外部委託対してリスク認識をしていない事が分かっており，図１５からシステムベンダとの認識の差異が認められた．そのため，金融機関ではリスク認識の差異を理解した上で「情報セキュリティガバナンス導入ガイダンス」にある「方向付け」を適切に行う必要がある．また，リスク認識に大きな差がある以上，「方向付け」は詳細なものが望まれる．また，その「方向付け」が正しく機能しているかどうかを確認する「モニタリング」では，その方法の精度を高くし、適度な頻度で実施する事が求められる．

6.2 内部統制の体制について

次に，金融機関とシステムベンダの内部統制の体制の違

いを，「コーポレート・ガバナンスの状況」にて比較した．内部統制の体制については，大きな違いは見受けられなかった．企業によってはコンプライアンス委員会（部）や内部監査部，オペレーショナルリスク管理委員会（部）など，ある特定の分野のリスクの責任を明確にしている企業が見受けられた．

コーポレートガバナンスの考え方においては，金融機関は「コンプライアンス」や「企業倫理」などを最重要課題とし，「信頼」を第一とするところが多く見受けられた．一方，システムベンダにおいては，「企業価値最大化」や「経営の迅速化」などを最重要課題とし，「成長」を第一とするところが多く見受けられた．

6.3 考察

金融機関とシステムベンダとでは，リスク認識に大きな差があり，一方，内部統制の体制面においては，業種間に大きな差異は見受けられなかった．

体制に大きな差がないため，外部委託を行う場合，共通のリスク認識を持つ事が重要であると思われる．共通のリスク認識を持つためには，リスクコミュニケーションを密にし，意見の摺合せが重要となる．また，業種の違いによる知識の差も双方で埋める必要がある．

7. まとめ

外部委託先での内部不正やインシデントといったリスクがある事は周知の事実である．それに対して，有価証券報告書の調査では，金融機関は外部委託に関するリスク認識は乏しい事が分かった．内部統制報告制度や業界に対するガイドラインもその一因でもあるとも言える．また，外部委託を受けるシステムベンダと金融機関とでは，オペレーショナルリスクや内部不正についての意識の差が見られた．

冒頭述べたとおり、高度化する情報システムを構築、管理するためにすべてを内製化することは経済的なメリットがない，そこで，外部委託の管理については，委託元が直接コントロール出来ない困難さもあり，適切な管理体制の確立が求められる．また，多重委託での外部委託は，さらに困難さが増すため，外部委託においては，リスクオーナーの所在を明確にし，委託元による確実な監督が求められる．

リスクは業務の変更や組織変更，外部環境の変化など様々な要因で変化するものであり，企業は一度確立したリスク管理体制を忠実に運営するだけでなく，絶えずリスク分析を行い，リスク管理体制も変化させていくべきである．

適切な内部統制の構築が，企業の信頼を築き上げる土台となるため，内部統制構築の前提となるリスク認識を確実に行う事が求められる．

8. 今後の研究

本稿では，内部統制構築の前提であるリスク認識の差を調査し，委託元と委託先の認識の違いを明らかにした．今後はリスク認識の違う委託先をどのように管理していくのかを検討し，適切な外部委託管理手法の提案を行いたい．

謝辞

本研究のアンケート調査および開示情報の分析にご協力いただいた，原田研究室の先輩同僚の皆様に謹んで感謝の意を表します．また，アンケートのデータ入力に多大な協力を頂いた神奈川県内特別支援学校の皆様に感謝します．

参考文献

[1]公益財団法人金融情報システムセンター，“金融情報システム白書（平成 25 年版）”，財経詳報社，2012 年 12 月
[2]町田祥弘，内部統制の知識（第２版），日本経済新聞出版社，2007 年 3 月，pp.51-56
[3] 新日本有限責任監査法人，“2013 年改訂版 COSO - 17 の原則と 87 の着眼点-”，http://www.shinnihon.or.jp/services/advisory/risk-management/topics/pdf/2013-09-24-04.pdf，2014 年 3 月 7 日アクセス
[4]2012 年度有価証券報告書
みずほ銀行，三菱東京 UFJ 銀行，三井住友銀行，りそな銀行，群馬銀行，千葉銀行，東京都民銀行，横浜銀行，静岡銀行，八十二銀行，京都銀行，福岡銀行，新生銀行，あおぞら銀行，徳島銀行，愛媛銀行，福岡中央銀行，常陽銀行，東邦銀行，三重銀行，肥後銀行，福島銀行，西日本シティ銀行，中国銀行，伊藤忠テクノソリューションズ，IT ホールディングス，アグレックス，日本電気，NEC フィールディングングス，日立製作所，日本ユニシス，富士通，富士通フロンテック，NTT データ
[5]2002 年度から 2012 年度の有価証券報告書
みずほ銀行，三菱東京 UFJ 銀行，三井住友銀行，千葉銀行，横浜銀行，静岡銀行，京都銀行
[6]経済産業省，“アウトソーシングに関する情報セキュリティ対策ガイダンス”，http://www.meti.go.jp/policy/netsecurity/docs/secgov/2009_OutsourcingJohoSecurityTaisakuGuidance.pdf，2014 年 4 月 2 日アクセス
[7]経済産業省，“情報セキュリティガバナンス導入ガイダンス”，http://www.meti.go.jp/policy/netsecurity/docs/secgov/2009_JohoSecurityGovernanceDonyuGuidance.pdf，2014 年 4 月 2 日アクセス
[8]情報セキュリティ大学院大学，“2013 情報セキュリティアンケート”，http://lab.iisec.ac.jp/~harada_lab/survey/2013/2013_questionnaire_result.pdf，2014 年 4 月 2 日アクセス

[9]日本銀行，“金融機関におけるシステム外部委託の現状について”，https://www.boj.or.jp/research/brp/ron_2008/.../ron0808a.pdf，2014 年 4 月 2 日アクセス
[10] 独立行政法人情報処理推進機構，“組織内部者の不正行為によるインシデント調査”，www.ipa.go.jp/files/000014169.pdf，2014 年 4 月 2 日アクセス