ＣＯＥソフトロー・ディスカッション・ペーパー・シリーズ
COESOFTLAW-2007-11

金融機関における外部委託業務を巡るソフトローの動き

～内部監査（システム監査）における監査基準の視点から～

白崎宏一
トレードウィン株式会社

2007 年 9 月

1. はじめに

最近、わが国金融機関でも、「顧客ニーズの多様化への対応」、「ビジネスのスピード化」、「ビジネス構造の柔軟性確保」、「経営資源の効率的活用」といった目的のもと、自社のサービス提供にあたり、アウトソーシング・業務提携といった形態により外部リソースを活用する「外部委託」の例が多く見受けられる。

リスクマネジメント、コントロールといった観点から、この外部委託業務を捉えた場合、従来、自社業務に存在していたリスクが業務委託先に振り変わるなど、リスク構造が変化することになり、このようなリスクに適切に対処するには、業務委託に適した「リスクマネジメント体制」を自社に整備し、運用していくことが必要である。また、最近、リスクマネジメント体制の確立においては、直接的なマネジメント体制の整備だけではなく、体制の整備・運用状況を客観的に独立な立場から評価し、改善活動へと繋げていく内部監査の重要性が増している。

内部監査など、監査の実施においては、対象システム、対象業務の健全性・有効性に関して評価するための基準が必要になるが、この評価基準（監査基準）のベースとして、パブリックセクター、プライベートセクターの各種団体等から公表されているガイドライン、評価・認証制度・当該制度において規定されている基準、規格などが活用されている。

この場合、各種ガイドライン、基準などは、適切なリスクマネジメント体制確立のための参考とすべきものというが本来の位置付けであるが、例えば、監督当局から公表されているガイドラインなどは、監督当局による検査へ対応するために準拠すべき基準と見なすことができる。また、第三者による評価・認証制度が外部業務委託における選定条件などに課せられていると、当該制度・基準へ準拠しなければビジネスを継続することも困難となる。このような各種ガイドライン、基準などは、法的拘束力がないにも拘わらず、事業体が準拠すべき、所謂「ソフトロー」と呼べるのではないかと考える。

本稿では、金融ビジネスの重要インフラである「情報技術に関わる外部委託業務」を中心に、内部監査（システム監査）における基準策定の観点から、各種ガイドラインや、外部委託業務に関わる各種評価・認証制度と実務との関わり、つまり委託元金融機関、委託先企業におけるガイドラインの捕らえ方、準拠状況などについて見ていくことにする。

2. 金融機関における業務の外部委託の現状

わが国の金融機関を取り巻くビジネス環境は、近年急速に浸透してきたインターネット取引など「取引形態・顧客ニーズの多様化」、異業種企業や外資系金融機関などの「新規参入」などを受けて、ますます厳しい競争環境となっている。このような環境下、各金融機

関は、「顧客ニーズの多様化への対応」、「ビジネスのスピード化」、「ビジネス構造の柔軟性確保」、「経営資源の効率的活用」といった目的のもと、自社のサービス提供にあたり、アウトソーシング・業務提携といった形態により外部リソースを活用する例が多く見受けられる。

例えば、「顧客ニーズの多様化への対応」として、金融機関と顧客との取引チャネルについて見れば、従来からの「対面取引を希望する顧客」に加え、「インターネットなど情報端末による取引を希望する顧客」、「電話など音声端末による取引を希望する顧客」など、さまざまなニーズが存在する。これら取引チャネルの多様化に関しては、情報技術の進歩に依存する部分が大きいため、自社で内製するのではなく、専門業者に外部委託するケースなどが増加している。また、さらなる顧客利便性向上を目的として自社チャネルの拡大のみに留まらず他企業（コンビニエンスストア、他金融機関）のチャネルとの相互乗り入れ、など取引チャネルの拡大は留まるところを知らない。

また、「ビジネスのスピード化」の観点から見れば、規制緩和などにより新規ビジネス分野への進出が可能になった場合、自社で新規ビジネスを一から育てていくのではなく、当ビジネス分野における専門業者と提携し、いち早く当ビジネスに進出するといったケースが見られる。

「経営資源の効率的活用」という観点からは、電話対応業務といった金融ビジネスに直接の関係ない部分を「コールセンター」業務として外部委託を用いたり、「経理」や「決済」などの「勘定系」業務といった、ビジネス上、差別化要因になりにくいバックオフィス業務自体を外部委託する「ビジネスプロセスアウトソーシング」といった外部委託形態も増加している。

このように、各金融機関は、厳しい競争環境を生き残るために、業務をアンバンドリング化させ、金融機関は自社における戦略的分野（コアコンピタンス）を明確にし、自らの経営資源を「コアコンピタンス」分野に集中させ、それ以外の業務は、専門業者に外部委託し、外部業者の専門性を享受するケースが増加している。また、外部リソースを効果的に活用し、ビジネスを効率的・効果的に推進させていくには、情報・データの効率的連携・活用が重要であり、これらの業務を支える情報システム等の整備・マネジメントが企業における重要な課題となってきている。

3. 外部委託業務におけるリスク

リスクマネジメント、コントロールといった観点から、この外部委託業務の現状を捉えた場合、従来、自社業務に存在していたリスクが業務委託先に振り変わるなど、リスク構造が変化することになる。例えば、外部委託先で何らかのトラブル・障害などが発生し、

業務遂行に影響が出た場合、委託元金融機関自身が、その損失を被ることになる。

外部委託に係るリスクとしては、一般的に以下のようなことが言われている。

―外部委託先企業との関係におけるリスク―

- 機密事項などが外部委託先を経由して漏洩するリスク
- 外部委託先におけるトラブルの影響を被るリスク
- 外部委託先における不祥事などによる監督責任を問われるリスク

―自社におけるコントロールに係るリスク―

- ビジネスプロセス・情報技術などのノウハウが社内に蓄積されないリスク
- 自社ビジネス戦略の変更に対する即応性・柔軟性を喪失するリスク
- 自社ビジネス戦略に合致したサービスが受けられないリスク

また、資本・金融市場においては、規制当局としても、この外部委託というビジネス形態の浸透には注意を払っているようである。つまり、外部委託の実施により、規制当局の監督下である金融機関から、リスク管理機能、法令遵守機能などの機能が、規制対象となっていない第三者へ、移転する可能性があり、規制当局の監督下である金融機関が、如何にして規制上の義務を遵守していることを担保できるかといった懸念がある。また、複数の金融機関が同一企業に業務を外部委託している場合など、当委託先企業の不祥事・トラブルが委託元である複数の金融機関の業務に同時に影響を及ぼす可能性がある。このような場合、影響範囲は、当該金融機関内の業務のみに留まらず、金融市場全体に波及するシステミックな問題に発展する可能性といった懸念がある。

4. リスクマネジメントと内部監査

このようなリスクに対して適切に対処するには、金融機関として、単に外部委託先に業務を委託するのではなく、外部委託に係るリスクを整理し、そのリスクを適切に管理するための評価方法、評価基準などを含んだ枠組み、すなわちリスクマネジメント体制を自社に整備し、運用していくことが必要である。また、このリスクマネジメント体制に関しては、直接的なマネジメント体制を整備するだけではなく、独立した立場の専門家である監査人による検証・評価する間接マネジメントの実施により、リスクマネジメントの有効性

をより高めることができる。近年の相次ぐ個人情報の漏洩などの事故、不祥事などを受け、このリスクマネジメント体制の確立に関して、客観的に独立な立場で評価し、問題があれば適切かつタイムリーな改善を図るための施策、監査の重要性が増大している。

内部監査など監査の実施においては、対象業務、対象システムの健全性・有効性に関して評価するための監査基準が必要になるが、この基準のベースとして、パブリックセクター、プライベートセクターの各種団体等から公表されているガイドラインなどが活用されており、そのガイドライン等の多くに「外部委託管理」が取り上げられている。

金融機関において、外部へ委託する業務としては、現金輸送などの運送業務、決済などの業務運営、基幹システムの開発・運用、信託財産の管理事務、外貨建証券の保管・管理など幅広い分野で実施されているが、本稿では、先の例で取り上げた事例においても重要なインフラとして位置づけられる「情報技術」に関わる「外部委託業務」に焦点を絞って、各種ガイドライン、基準などについて見ていくことにする。

金融機関において、データ処理量の増大、多様化、高度化した取引形態の進展などを受けて、今や情報技術はなくてはならない存在となっている。しかし、情報技術が有する「目まぐるしいまでの進歩の速さ」、「技術を取扱う上での専門性の高さ」などといった特徴のため、金融機関が自らの経営資源で情報技術に係る業務を取扱うのは、大きな負担であり、非効率でもある。その結果、情報システムの開発、運用といった業務を外部の専門業者に委託するケースが増加している。

また、情報技術の金融ビジネスへの浸透に伴い、情報技術に係る障害が発生した場合の影響範囲の広さ、影響の大きさは、ビジネス遂行上、深刻なものになる可能性があり、外部業者に委託されている業務も含めて、情報技術に関するリスクを適切に管理する重要性が認識されてきている。この情報技術に係るリスクマネジメント体制の確立のための有効な手段として、情報システムを客観的に独立の立場から評価・検証し、タイムリーな改善へと繋げるための「システム監査」の必要性が認識されてきている。

システム監査の定義としては、経済産業省から公表されている「システム監査基準」に規定されている定義が一般的に用いられている。「システム監査基準」によるとシステム監査とは、「組織体の情報システムにまつわるリスクに対するコントロールがリスクアセスメントに基づいて適切に整備・運用されているかを、独立かつ専門的な立場のシステム監査人が検証又は評価することによって、保証を与えあるいは助言を行い、もって IT ガバナンスの実現に寄与すること」と定義されている。

わが国金融機関における、システム監査実施の際に用いられる基準としては、経済産業省から公表されている「システム監査基準」もさることながら、金融庁から公開されている「金融検査マニュアル（システムリスク管理態勢の確認検査用チェックリスト）」と（財）

金融情報システムセンターから公表されている「金融機関等のコンピュータにかかる安全対策・基準」をベースの拠り所として自社に適応する形でカスタマイズして自社の基準を作成している事例が多く見受けられる。

5. 外部委託業務に係る各種ガイドライン

本節では、この「金融検査マニュアル（システムリスク管理態勢の確認検査用チェックリスト)」と「金融機関等のコンピュータにかかる安全対策・基準」における「外部委託管理」部分と日本銀行から公表されているアウトソーシングに関するペーパーを概観しておくことにする。

（金融検査マニュアル）

（目的）

1999 年に発出された「金融検査マニュアル」は、その前文にて、「金融検査マニュアルはあくまでも検査官が金融機関を検査する際に用いる手引書として位置づけられるものであり、各金融機関においては、自己責任原則の下、このマニュアル等を踏まえ創意・工夫を十分に生かし、それぞれの規模・特性に応じたより詳細なマニュアルを自主的に作成し、金融機関の業務の健全性と適切性の確保に努めることが期待される。また、マニュアルの各チェック項目は検査官が金融機関のリスク管理態勢及び法令等遵守態勢を評価する際の基準であり、これらの基準の達成を金融機関に直ちに法的に義務づけるものではない。」と記載されており、あくまでも、自社リスク管理体制、内部監査体制の整備は自己原則の下、行われるべきものであり、当検査マニュアルは、自社リスク管理体制を整備する際の参考にできるものという位置づけであり、当検査マニュアルに沿うことは法律的な義務でないことも付記されている。

（外部委託業務に関する記述）

1999 年の「金融検査マニュアル(システムリスク管理態勢の確認検査用チェックリスト)」（初版）では、「外部委託業務」に関しての記載は、項目「Ⅳ企画・開発体制のあり方－１．企画・開発体制」と「Ⅴ体制の整備－２．システム運用体制」のそれぞれにおいてチェック項目の一つとして「委託先管理」が記載されていた。2001 年の改定では、項目として「Ⅵ外部委託先管理」が新設（追加）され、内容も充実されたものになった。この改定により、「外部委託業務に関する計画・実行」、「外部委託業務のリスク管理体制」、「問題点の是正」といった観点からのチェック項目が設けられている。

「VI外部委託先管理」における各チェック項目は以下のように定義されている。

「外部委託業務に関する計画・実行」

- ✧ システムにかかる外部委託業務の計画・実行に当たっては、外部委託を行う範囲の決定及びリスク管理の具体策を策定しているか。

「外部委託業務のリスク管理体制」

- ✧ 外部に委託しているシステム及び業務を適切に管理する管理者を設置しているか。
- ✧ 外部に委託している業務についてリスク管理が十分できるような体制（リスクの認識・評価体制、是正等）を契約等によって構築しているか。
- ✧ 委託先と守秘義務契約を締結しているか。
- ✧ 委託先社員等が接することができるデータには、必要に応じて一定の制限を設けているか。
- ✧ 外部委託した業務及び業者について定期的に評価を行っているか。なお、外部委託した業務について、業務の内容等に応じ、第三者機関の評価を受けていることが望ましい。

「問題点の是正」

- ✧ 認識された問題点については、外部委託先と連携して速やかに是正しているか。

このように、「外部委託業務」に関わるチェック項目は、主に委託元金融機関において、業務の外部委託を実施するに当たり、その外部委託業務に係るリスク管理に関して、計画（適切な範囲の選定、適切な契約内容での締結）・実行（リスク管理体制の整備）・モニタリング（定期的な評価）を適切に実施しているかといった観点からの内容となっている。

当検査マニュアルへの準拠に関しては、先に見たように法的義務ではないと記載されているが、金融庁による検査は、法的根拠により実施される検査であり、当検査マニュアルに沿って実施される検査により指摘事項があった場合には、勧告、行政処分等のペナルティが発生する可能性があることを勘案すると、被検査主体である金融機関としては、当検査マニュアルの記載内容に応じた体制を整備することになる。

ただ、「外部委託」に関する記載で見たように、記載レベルとしては、リスク管理に関する枠組みを指摘するにとどまり、具体的な指標・レベルについての記載はほとんど見当たらないため、実務レベルでの評価基準に活用することは難しく、基準の具体的な内容に関しては、各々の金融機関にて策定する必要がある。

（金融機関等コンピュータシステムの安全対策基準・解説書）

（目的）

「金融機関等のコンピュータシステムの安全対策基準・解説書」は、金融機関等におけるコンピュータシステムの安全対策は、第一義的には自己責任の下、各々の金融機関にて講じられるべきものであるが、金融機関等におけるコンピュータシステムが高い公共性および広汎性を有するという特徴を持ち、十分な安全性の確保が社会的に要請されるため、（財）金融情報システムセンターにより、金融機関等の拠り所になるべき共通の安全対策基準として策定された。

また、上記、「金融検査マニュアル（システムリスク管理態勢の確認検査用チェックリスト）」の前文において「検査官は、「リスク管理態勢の確認検査用チェックリスト（共通編）」及び本チェックリストにより、システムリスクの管理態勢の確認検査を行うものとする。しかしながら、管理態勢に問題が見られ、さらに深く業務の具体的検証をすることが必要と認められる場合には、検査官は、「金融機関等コンピュータシステムの安全対策基準」及び「同解説書」（（財）金融情報システムセンター編）等に基づき行うものとする。」と明記され、金融機関においては、検査マニュアルとならんで自社の評価基準策定の拠り所となっている。

（外部委託業務に関する記述）

「外部委託業務」について、当基準では、近年、金融機関等において、外部委託するケースが増加し、またその形態に関しても従来の自社子会社への外部委託から資本関係にとらわれない会社への外部委託、ホストコンピュータ等を共同で運用する「共同センター」など多様化してきたことを前提に、「情報システム戦略等の策定に際し、外部委託に関する事項を十分に検討することの重要性」「個別システムの開発、運用のため、外部委託を計画・実施するに当たっては外部委託を行う目的や範囲を明確に定め、リスク管理のための具体的な方策を実施することの重要性」を認識し、安全対策を実施するべきと述べられている。

具体的には、「運用基準」の一項目として「外部委託管理」が規定されており、その中で、「外部委託に関する計画」と「外部委託業務管理」に分類され、各項目に関してチェック項目が列記されている。

各チェック項目は以下のように定義されている。

「外部委託に関する計画」

- ✧ システムの開発や運用等で外部委託を行う場合は、事前に目的や範囲を明確にすること。
- ✧ 外部委託先の選定手続きを明確にすること。
- ✧ 安全対策に関する項目を盛込んだ委託契約を締結すること。

「外部委託業務管理」

- ✧ 外部委託先の要員にルールを遵守させ、その遵守状況を管理、検証すること。
- ✧ 外部委託における業務組織の整備と業務の管理、検証を行うこと。

当基準においても、金融庁検査マニュアルと同様、外部委託業務管理に関して、委託元金融機関等において、適切に外部業者を管理できるような施策を整備・運用するためのチェックリストとなっている。記載レベルに関しては、管理、指標項目などが「具体例」といった形で記載されており、また、金融庁検査マニュアルにおいて、当「安全・対策基準」がリファレンスされていることもあり、多くの金融機関における内部監査（システム監査）においては、当基準に記載されている「具体例」をもとに自社における委託業務内容、自社管理方針などと整合性をとる形で自社基準を作成していると考えられる。

実質的には、ガイドラインという位置付けではありながら、検査対応として準拠すべき基準として実務上は捉えられていると考える。

（金融機関業務のアウトソーシングに際してのリスク管理）

（目的）

2001 年 4 月に日本銀行より公表された当ペーパーでは、アウトソーシングについて、わが国金融機関においても、近年、顧客ニーズの多様化、経営効率化などを背景に確実に広まってきており、専門的技術の享受、コスト削減などアウトソーシングの活用によるメリットが期待できるが、これに伴う新たなリスクも軽視できないものとなっており、その適切な管理は、今日の金融機関経営にとって重要な課題との認識を示している。この認識のもと、当ペーパーでは、日銀が実施している考査等によって、アウトソーシングのリスク

管理手法、あるいはアウトソーシングに伴うリスクの所在について金融機関内に十分認識・整理されていないケースが少なくない現状を踏まえ、金融機関がアウトソーシングを実施するに当たってのリスク管理上のポイントを整理し公表している。

（外部委託業務に関する記述）

当ペーパーでは、アウトソーシングに係るリスク管理を「アウトソーシング開始段階でのリスク管理の枠組み構築」「アウトソーシング実施後のモニタリング」「事故等が発生した場合の対応」に分類し、各々の項目における留意ポイントを示している。各項目における留意ポイントの概要は以下のとおり。

「アウトソーシング開始段階でのリスク管理の枠組み構築」

アウトソーシング開始に当たっては、「アウトソーシングに伴うリスクの評価」、「適切なアウトソーシング先の選定」、「業務委託契約による権利義務関係の明確化」などを適切に実施することが望ましいとしている。

「アウトソーシング実施後のモニタリング」

金融機関は、「定期的な業務報告」、「アウトソーシング先での内部監査・外部監査結果の入手」などの手段により、アウトソーシング開始後も、継続的にアウトソーシング先の経営状況、サービスレベル、リスク管理態勢などをモニターしていくことが望ましいとしている。

「事故等が発生した場合の対応」

トラブルが発生した際の影響を最小限に食い止めるために、「主要なシナリオ（システムダウン、顧客情報の流出など）を想定した、連絡・協調体制や代替手段の確保、必要な事務フローなどの整備」「定期的な実地訓練の実施による実務担当者の習熟をはかる」など委託元金融機関、アウトソーシング先双方で、緊急時対応計画（コンティンジェンシー・プラン）を整備しておくことが重要としている。

当ペーパーは、日銀が金融機関に対して実施している考査等の実績から、整理されたペーパであるため、日銀の考査を受けない事業者にとっては参考とすべき位置付けであるが、考査を受ける金融機関にとっては、日銀の考えを把握・理解する上では十分に意識しなければならない位置付けのペーパーだと考えられる。

これら以外にも、内部監査（システム監査）における評価基準のベースと成りうるガイドラインは多く公表されているが、各金融機関において策定する評価基準に関して、第一義的に拠り所とするものは、監督当局の考えを示している・反映されている上記示した金

融検査マニュアル等のペーパーだと考えられる。

ただ、これらガイドラインにおいては、外部業務委託に係るリスク管理体制の枠組みに関わる留意点などが抽象的に述べられている部分が多く、また、詳細な記述においても「具体例」といった形で記載されており、実施すべきか否か、実施するとしても、どの項目に関してどのレベルまで実施するべきかを判断する基準が明示されていないケースが多く見られる。また、「外部委託業務に係るリスクマネジメントにどれくらいのコストをかけるべきかの基準が不明確」、「掛けたコストに対してどれほどのメリットがあるのか（費用対効果）測定が困難」、「業務を委託している業者がその業務の専門家である」、「業務を委託している業者とは長年の付合いである」ことなどを理由に、委託先企業に対するチェックする意識が希薄になっているケースも見受けられる。

そのため、外部委託に関する実態調査等によると、外部業務委託契約書に記載する事項、委託先企業から委託元企業への報告内容など具体的な項目になると、金融機関間でその実施状況、内容については、かなり、ばらつきがあるようである。

このように各金融機関では、外部委託業務に係るリスク・リスクマネジメントの重要性についての認識は、監督当局からのペーパー等をはじめ、各種団体からのレポート、各社事例等により、広く浸透してきていると考えられる。また、監督当局としても、事業を継続していく上で認識される多くのリスクの一つとして「外部業務委託」を捕らえ、リスクマネジメント体制の整備の一環として、金融機関へ「外部業務委託」に係るリスクへの対応を求めていると考えられ、また、拠り所とするガイドラインの記載レベルが抽象的であること、外部委託業者との関係維持、リスクマネジメントに係るコスト・メリットの把握の難しさといった点から、外部業務委託に関する管理体制は、形式的な管理に留まっているケースが多いものと思われる。

6. 重要性を増すガイドライン

しかし、最近、外部業務委託を活用する企業が、外部委託先の監督の強化に乗り出す事例が多々見受けられる。これは、2005 年 4 月から全面施行された「個人情報の保護に関する法律」において、「外部委託先の監督」という項目があり、個人情報取扱事業者が個人データの取扱いを外部の組織に委託する場合、その委託先においても個人データの安全管理が図られるよう監督することが義務付けられていることに起因していると考えられる。

以下では、この個人情報保護に係る「外部業務委託」の取扱いについて見ていくことにする。

2004 年 4 月、「個人情報の保護に関する基本方針」が閣議決定された。その中でも「責

任体制の確保」の中で、「外部委託先の監督体制」と定義されており、「個人情報の保護措置が委託先においても確保されるために、業務委託契約において委託元と委託先の責任を明確化すること」と規定されている。

「個人情報の保護に関する法律」では「第二十二条　個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。」と規定されており、委託元事業者は、外部委託先事業者を適切に監督する法的責任が明確に打ち出されている。

また、「個人情報の保護に関するガイドライン」の位置づけについて、基本方針では「2 国が講ずべき個人情報の保護のための措置に関する事項」の「(3) 分野ごとの個人情報の保護の推進に関する方針　① 各省庁が所管する分野において講ずべき施策」において「(略) 各省庁は、法の個人情報の取扱いに関するルールが各分野に共通する必要最小限のものであること等を踏まえ、それぞれの事業等の分野の実情に応じたガイドライン等の策定・見直しを早急に検討するとともに、事業者団体等が主体的に行うガイドラインの策定等に対しても、情報の提供、助言等の支援を行うものとする。」と記載されている。さらに「6　個人情報取扱事業者等が講ずべき個人情報の保護のための措置に関する基本的な事項」の「(1) 個人情報取扱事業者に関する事項」において、「個人情報取扱事業者は、法の規定に従うほか、2 の (3) の①の各省庁のガイドライン等に則し、個人情報の保護について主体的に取り組むことが期待されているところであり、事業者は、法の全面施行に向けて、体制の整備等に積極的に取り組んでいくことが求められている。」と記載されている。

このように基本方針では、「ガイドライン」を「各分野横断的に共通する部分だけを規定した法律をそれぞれの事業分野の実情に応じた内容を規定するもの」と位置づけられている。

「個人情報の保護に関する法律」においても、「第八条　国は、地方公共団体が策定し、又は実施する個人情報の保護に関する施策及び国民又は事業者等が個人情報の適正な取扱いの確保に関して行う活動を支援するため、情報の提供、事業者等が講ずべき措置の適切かつ有効な実施を図るための指針の策定その他の必要な措置を講ずるものとする。」と規定されており、この条文の「指針」がガイドラインに当たると考えられる。実際、経済産業省から発出されているガイドラインの前文においても、ガイドラインの目的の拠り所としてこの第 8 条を明記している。

次に、上記ガイドラインの例として、金融庁から公表されている「金融分野における個人情報の保護に関するガイドライン」を概観する。

当ガイドラインでは、外部委託に関して、「第 12 条 委託先の監督（法第 22 条及び基本

方針関連)」の中で次のような内容が規定されている。

✧ 金融分野における個人情報取扱事業者は、個人データを適正に取扱っていると認められる者を選定し委託するとともに、取扱いを委託した個人データの安全管理措置が図られるよう、個人データの安全管理のための措置を委託先においても確保することが必要である。なお、二段階以上の委託が行われた場合には、委託先の事業者が再委託先等の事業者に対して十分な監督を行っているかについても監督を行わなければならない。具体的には、金融分野における個人情報取扱事業者は、

① 個人データの安全管理のため、委託先における組織体制の整備及び安全管理に係る基本方針・取扱規程の策定等の内容を委託先選定の基準に定め、当該基準に従って委託先を選定するとともに、当該基準を定期的に見直すこと。

② 委託者の監督・監査・報告徴収に関する権限、委託先における個人データの漏えい・盗用・改ざん及び目的外利用の禁止、再委託に関する条件及び漏えい等が発生した場合の委託先の責任を内容とする安全管理措置を委託契約に盛り込むとともに、定期的又は随時に当該委託契約に定める安全管理措置の遵守状況を確認し、当該安全管理措置の見直しを行うこと。

また、金融庁は、当ガイドラインの「第 10 条　安全管理措置」の実施について、「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」（以下　「実務指針」と記載）を別に規定しており、その中でも「外部委託」に関して、以下示すように、かなり具体的に実施しなければならない事項を規定している。

✧ （個人データ保護に関する委託先選定の基準）

5－1 金融分野における個人情報取扱事業者は、個人データの取り扱いを委託する場合には、ガイドライン第 12 条第 3 項①に基づき、次に掲げる事項を委託先選定の基準として定め、当該基準に従って委託先を選定するとともに、当該基準を定期的に見直さなければならない。

① 委託先における個人データの安全管理に係る基本方針・取扱規程等の整備

② 委託先における個人データの安全管理に係る実施体制の整備

③ 実績等に基づく委託先の個人データ安全管理上の信用度

④ 委託先の経営の健全性

5－1－1 委託先選定の基準においては、「委託先における個人データの安全管理に係る基本方針・取扱規程等の整備」として、次に掲げる事項を定めなけ

ればならない。

① 委託先における個人データの安全管理に係る基本方針の整備

② 委託先における個人データの安全管理に係る取扱規程の整備

③ 委託先における個人データの取扱状況の点検及び監査に係る規程の整備

④ 委託先における外部委託に係る規程の整備

5－1－2 （略）

5－2 金融分野における個人情報取扱事業者は、5－3 に基づき、委託契約後に委託先選定の基準に定める事項の委託先における遵守状況を定期的又は随時に確認するとともに、委託先が当該基準を満たしていない場合には、委託先が当該基準を満たすよう監督しなければならない。

✧ （委託契約において盛り込むべき安全管理に関する内容）

5－3 金融分野における個人情報取扱事業者は、委託契約において、次に掲げる安全管理に関する事項を盛り込まなければならない。

① 委託者の監督・監査・報告徴収に関する権限

② 委託先における個人データの漏えい、盗用、改ざん及び目的外利用の禁止

③ 再委託における条件

④ 漏えい事案等が発生した際の委託先の責任

5－4 金融分野における個人情報取扱事業者は、5－3 に基づき、定期的又は随時に委託先における委託契約上の安全管理措置の遵守状況を確認するとともに、当該契約内容が遵守されていない場合には、委託先が当該契約内容を遵守するよう監督しなければならない。また、金融分野における個人情報取扱事業者は、定期的に委託契約に盛り込む安全管理措置を見直さなければならない。

当ガイドライン・実務指針に記載されている「外部委託業務」に係る部分の内容は、「個人情報の保護に関する法律」の第 22 条における「委託を受けた者に対する必要かつ適切な監督を行わなければならない。」との規定を具体化したものであり、努力規定という位置付けではなく、準拠しなければならないもの、つまり義務規定と認識されている。これらの認識は、金融庁がガイドラインに対して寄せられた意見に対する回答からも伺える。

「実務指針」の位置づけ・記載されている内容について、金融庁は、「「個人情報の保護

に関する法律」第 20 条から第 22 条の解釈に係る内容は義務規定であるが、実務指針において事業者の講ずべき措置として定められた事項について、その具体的な対応方法は、各事業者の自主的な取組みを求めるもの」としている。実施するべき事項に関しては、かなり具体的事項まで含んでおり、この実務指針の内容そのものを用いる金融機関が多いのではないかと考える。実務的にも各金融機関は、「個人情報保護に関する法律」の施行を受けて、外部業務委託先に対して、「個人情報に関する覚書」など改めて締結するように動いている。その内容は、「個人情報保護に関する法律」のみではなく当ガイドラインに準拠することも同等の位置付けとされ、覚書の内容が規定されている。

複数の金融機関にサービスを提供している委託先企業では、複数の委託元金融機関と、個人情報の取扱いに係る契約などを個別に締結し、各々の委託元金融機関の定めた条項を遵守しなければならず、各々の金融機関から監督されることになる。その結果、委託先企業における個人情報保護に係るコストが増大し、コスト増分をサービス対価などに転嫁する、といった外部委託による低コストなどメリットが相殺される事象も懸念される。また、委託元金融機関から外部委託先企業に対して、委託先企業における「安全管理に係る基本方針・取扱規定」などの提供を求める場合もあるが、それら規定には、委託先企業としての企業秘密に関わる部分が含まれることも多々あり、契約締結には難航しているケースも見受けられる。

この事例においては、個人情報保護に関するガイドライン（外部委託に係る部分）の内容・観点が、委託元におけるコントロールにフォーカスされているため、このガイドラインに準拠した場合、外部委託先企業における委託元企業との関係マネジメントに係るコストが大きな負担となり、効率的な業務遂行に影響を及ぼすことが懸念される。また、委託元金融機関における内部監査（システム監査）等においても、外部委託業務が増加するに伴い、委託先の監督状況の評価・検証作業の負担が大きくなることが懸念される。

また、前掲した「金融機関等コンピュータシステムの安全対策基準・解説書」に関しても、金融庁からの当ガイドラインの公表を受け、改定が実施された。改定にあたって、(財)金融情報システムセンターでは、「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」に示されている要求事項を分析し、「金融機関等コンピュータシステムの安全対策基準・解説書」と対比させ、対応関係を明確にした上で、追加・訂正が実施された。当安全対策基準は、自主基準との位置づけとしているが、「対応表で対応付けている安全対策基準の具体的な対策は、金融庁の公表している実務指針の各項目の求める措置の概念に該当するものである」ということを（財）金融情報システムセンターは表明しており、さらに「対応表の対策が唯一の対策というわけではなく、対応表に記載された対策の代替策を講じることも可能である。ただし、対応表に記載された対策以外の対策を講じる場合は、検査時にその措置が実務指針の内容と整合的であることの挙証が求められる可能性がある」とも言明しており、当安全対策基準は、自主基準ではありな

がらも、かなり強制力のある（法律の後ろ盾がある）ガイドラインとなったように感じられる。

7. 外部委託業務マネジメントにおける効率化

情報技術に関わる分野では、セキュリティなどに関するリスクマネジメントの重要性の増大などの潮流を受け、上記個人情報保護に関わる部分だけなく、システムの信頼性・安全性の確保という観点からも、委託元企業と委託先企業との関係マネジメントを効率化させる方策が、それぞれの委託元、委託先の企業の立場で検討されている。

この節では、この効率化の方策として活用の方向で検討されている具体例をいくつか概観することにする。

（プライバシーマーク制度）

プライバシーマーク制度は、1998 年から（財）日本情報処理開発協会が個人情報の取扱いについて適切な保護措置を講ずる体制を整備している民間事業者等に対し、その旨を示すマークとしてプライバシーマークを付与（有効期限は 2 年間）し、事業活動に関してプライバシーマークの使用を認容する制度である。

認定に当たっては、JISQ15001「個人情報保護に関するコンプライアンス・プログラムの要求事項」に基づいた審査を行っている。JISQ15001 では、事業者に対して「個人情報保護に関する方針」「個人情報の取扱いに関する管理規程・運用規程」などが整備され、個人情報の取扱いに関して、全社的なマネジメントシステムが確立されており、かつ当マネジメントシステムの実行・維持が適切に実施されているかを内部監査等の実施により改善していくマネジメントシステムの実効性が求められている。この要求事項は、各省庁から公表されている個人情報に係るガイドラインの要求事項を満足しているものと考えられる。

当マークを取得することにより、事業者は個人情報の取扱いに関して適切にマネジメントされていることを第 3 者から評価されることになり、外部委託先業者は、委託元企業に対して、自社の個人情報に関する管理体制が整備されており、その体制が有効に運用されている証になるので、委託元企業は、当認証の有無により、外部委託先の個人情報保護管理体制を評価することが可能になり、外部委託先管理業務が効率化されることが期待される。

当制度の認定事業者数は、平成 17 年 8 月現在で、18,000 社となっており、平成 15 年度からは大きく取得者数が増えている。これは、先に述べた「個人情報の保護に関する法律」

が大きく影響していると考えられる。

また、当制度は、官公庁の入札条件にも加えられるような事例が出てきていることから当制度の認識度、実効性も向上され、ますますの広がりを見せると思われる。

（情報セキュリティマネジメントシステム（ISMS）適合性評価制度）

ISMS 適合性評価制度とは、2002 年より（財）日本情報処理開発協会が定めた情報セキュリティマネジメントシステムの確立に関しての認証基準「ISMS 認証基準」に基づき評価し、認定する制度である。

ISMS とは、（財）日本情報処理開発協会の定義によると「個別の問題毎の技術対策の他に、組織のマネジメントとして、自らのリスク評価により必要なセキュリティレベルを決め、プランを持ち、資源配分して、システムを運用すること」と定義されている。すなわち、情報システムの技術的なセキュリティ対策だけでなく、組織として情報を扱う際の基本方針(セキュリティポリシー)や、それに基づいたセキュリティレベル向上に関する計画、計画の実行・運用、内部監査による評価、その結果等による方針・計画の見直しまで含めたマネジメント体系のことを指す。

この適合性で使用する認証基準「ISMS 認証基準」は、英国規格 BS 7799-2：2002 に基づき作成したもので、当基準で使用する用語、表現については、JIS X 5080：2002（国際規格 ISO/IEC 17799：2000）との互換性を確保されている。

当適合評価制度の認定事業者数は、平成 17 年 8 月現在で約 1,000 社となっており、当制度も国や自治体などでの入札条件等になってきている事例も見受けられる。

前述のプライバシーマーク制度も ISMS 適合性評価制度も企業における情報セキュリティマネジメントに関する認証基準であるが、プライバシーマーク制度が対象範囲を個人情報の取り扱いに主眼を置いているのに対し、ISMS は事業会社における情報資産全てを対象範囲としている。また、プライバシーマーク制度では、個人情報の安全管理策のみならず、個人情報主体の権利の保護や、利用目的の明示・提示などについて規定されており、企業での個人情報の適切な活用も想定に入った認定基準となっている。

（SAS70 報告書）

正式名称は、米国公認会計士協会監査基準（SAS）70 号。外部の委託者に提供される業務における内部統制の整備状況、有効性に関して独立な監査人が意見表明し、委託者等に対して情報提供を行うための指針。日本の制度ではないが、日本でのシステム監査などに

準用されているケースが見受けられる。

当基準の目的は、財務諸表監査で企業の会計処理システムなど会計処理に関係する内部統制の検証過程において、その企業が他企業に財務諸表作成に係る業務の一部を外部の企業に委託している場合などにおいて、外部委託先企業が独立な監査人から SAS70 報告書を受領していれば、委託元企業の監査人は委託先企業への監査を当報告書の検討に代替することができ、委託元企業における内部統制の評価作業の効率化を図ることにある。また、外部委託先企業としても、多くの委託元企業による個々の監査に対応することは大きな負担となるが、SAS70 報告書を受領していると委託元企業の監査人は当報告を検討すればよいため、外部委託先企業における負担は軽減される。

当報告書は、信託銀行、投信投資顧問会社等の資産運用業務・資産管理業務、情報システムのデータセンター、認証局などの運用業務に適用されている例がある。

また、外部委託業務に係る例として、幾つかの欧米金融機関では、外部委託先企業に対して、外部委託先企業の行った監査結果を SAS70 に基づき報告させているケースもある。さらに、米国の公開企業会計監督委員会（PCAOB）が公表している監査基準においても、業務を外部に委託している企業の内部統制の評価には、外部委託先企業の SAS70（タイプⅡ）報告書を利用できるとしている。

（Trust サービス）

Trust サービスは、米国公認会計士協会（AICPA）とカナダ勅許会計士協会（CICA）が開発したシステムに関する保証サービスであり、企業のシステムの内部統制の状況を 4 つの基本原則、「可用性」「安全性」「完全性」「保守性」に関して評価し、システムが信頼可能か否かを公認会計士による第三者評価を提供するサービスである。日本においても日本公認会計士協会が 2003 年 12 月に、AICPA/CICA とライセンス契約を締結し、日本公認会計士協会とサブライセンス契約を締結した監査法人・公認会計士が、企業に対して当サービスを提供できるようになった。Trust サービスは、SysTrust および WebTrust の 2 つのサービスから構成されており、SysTrust がシステム全般を対象とし、WebTrust はオンラインにおける電子商取引にのみ焦点を当てたものとなっている。

例えば、業務の委託を受けている委託先企業（受託企業）が、当サービスにより保証を受けていれば、自社システムの信頼性の水準を委託元企業へ提示でき、委託元企業では、当サービスの保証により、委託先企業のシステムに関する内部統制の状況を判断することが可能となる。

上記示した評価・認証制度等以外にも情報技術に係る様々な評価・認証制度などが運営されているが、各々の制度の目的、カバー範囲（評価範囲）、保証水準、認定に求められる準拠レベル、取得・維持コストなどもそれぞれ異なる。そのため、これらの制度等を外部委託業務に係る関係マネジメントの効率化のために用いる場合、外部委託する業務に最も適切な評価・認証制度が何であるかといった認識が、自社コントロールの評価基準として用いる委託元金融機関と、委託先企業とで認識があっていることが重要である。このような評価・認証制度といったスキームの利用により、委託元金融機関、委託先企業との関係マネジメントを効率化する一助となることが期待され、例えば、委託元金融機関における「外部委託先選定基準」として、これらの評価・認証制度を活用することにより、選定作業に係るコストを減らすことが可能であろう。また、「委託先の監督」に関しても、委託先における管理状況などを保証サービスの報告を活用し、評価作業を当報告内容に依拠することにより、効率化が図れる。また、委託先企業としても、これらの評価・認証制度が普及すれば、個々の委託元金融機関と個別に対応することなく、効率的な関係を築くことが可能と考える。

今後、委託元、委託先にて、ある特定の評価・認証制度の利用が増え、普及すれば、これら評価・認証制度、これら制度にて規定している規格それ自体が該当ビジネス分野におけるデファクト・スタンダードを形成することになる。委託元企業では、この普及した制度・規格を利用しなければ、同一条件で公平な委託先企業の選定・評価が難しくなるため、デファクト・スタンダード化した規格・基準を活用することが考えられる。また、委託先企業においても、先の事例で挙げた「プライバシーマーク取得」が委託先としての条件に課せられたりと、普及した評価・認証制度を取得・維持することなしにビジネスを継続することが困難となる。つまり、これら評価・認証制度、および制度にて規定している規格自体、法的拘束力がないにも関わらず企業が準拠するべき「ソフトロー」として機能すると言えるのではないだろうか。

通常、「デファクト・スタンダード」は、事業体の競争力の中心となるコア領域における「標準」としての議論が多くされ、この議論のうえでは、「デファクト・スタンダード」に準拠しない場合のサンクションは想定されず、如何に自社のコアビジネスでの競争力を増すかという観点から、「デファクト・スタンダード」に準拠するべきか否かを各事業体は決断していくことになる。しかし、今回の例で見たように、公共性を有する事業体である金融機関における「リスク管理体制の整備」、また、「コンプライアンス」、「社会的責任」といった事業会社にとって事業を継続させる上で実施しなければならないこと、といった分野においては、競争力を増すといった観点ではなく、多くは、如何にコストを掛けず効率的に対応するか、といった観点が重要視され、その分野での「デファクト・スタンダード」は、事業継続上、各事業体が準拠するべき「ソフトロー」としての特徴を備えてくると考えられるのではないだろうか。

8. 結びにかえて

先日、2005 年 4 月に国会にて成立した保険業法の改正により、金融庁は保険会社の外部委託先企業に対しての直接検査の権限を入手した。

保険会社等に係る立入検査等

内閣総理大臣は、保険会社等（外国保険会社等、免許特定法人、引受社員及び保険持株会社を含む。以下同じ。）の業務の健全かつ適切な運営を確保し、保険契約者等の保護を図るため特に必要があると認めるときは、その必要の限度において、保険会社等の子法人等又は保険会社等から業務の委託を受けた者に対し、保険会社等の業務等の状況に関し報告若しくは資料の提出を求め、又は、職員にその施設に立ち入らせ、質問等をさせることができることとする。

（保険業法第 128 条、第 129 条、第 200 条、第 201 条、第 226 条、第 227 条、第 271 条の 27、第 271 条の 28 関係）

また、日本銀行においても、「平成 17 年度の考査の実施方針等について」の中で、「オープン系システムの導入やネットワーク化が進展するなかで、外部委託先を含めて、維持管理・運用が適切に行われているかを確認」と記載されており、外部委託先に対して考査を実施することを表明している。

金融機関におけるコンピュータシステムで大規模な障害などが発生した場合の社会的に与える影響の大きさを鑑みると、実質的に金融機関の業務を受託している外部委託先に検査や考査が入る必要性は理解できる。しかし、現状、金融庁や日本銀行が一般事業会社である外部委託先企業に対して、どこまでの範囲を検査・考査を実施し、検査の結果の指摘事項、改善勧告などに関して、どのような強制力を有するのか明確でない。また、複数の金融機関にサービスを提供している外部委託先企業を想定した場合、委託元金融機関への検査の度に当該外部委託先企業へ検査を実施するのかといった頻度の問題、当該外部委託先企業において改善事項などが指摘された場合の対応方法（改善実施に関する責任者が誰になるのか)、当該外部委託先企業のその他のサービス提供先である金融機関への対応方法なども不明な部分が多い。

米国においても、監督当局である OCC が金融機関の基幹業務を受託している外部委託先企業の検査を実施することが法令により定められている。このケースにおいて、複数の金融機関にサービスを提供している外部委託先企業に検査が入った場合は、OCC は当外部委託先企業に関する検査報告書を各委託元金融機関に対して開示されるケースもあり、委託元金融機関と外部委託先企業との関係マネジメントの効率化を図ろうとする動きと捉える

ことができる。

今後も、金融機関における業務（サービス）の複雑化、専門化、グローバル化、競争の激化といった潮流により、監督当局として金融機関の外部業務委託に係るリスクマネジメントへの関心はますます高まると考えられる。また、外部業務委託される事業分野はますます広範囲に及び、また新興国への業務移転なども始まっており、外部業務委託に係るリスクマネジメントは、より高度化、複雑化されることが想像される。

このような流れの中、委託元金融機関においても、委託先事業会社においても、この「外部業務委託」を効率よく、効果的に実施していくためにお互い、関係マネジメントの実施方法について模索していくことが想定され、そのような中で形成された「ガイドライン」、「評価・認証制度」が広く活用されるようになれば、これらは「ソフトロー」を形成し、企業体の行動に規範を与えていく存在になると想像される。

このような「事業体として競争力に直結する分野ではなく、事業継続する上で実施しなければならない分野」における「ソフトロー」に関して、「監督当局との関わり」、「各事業会社のソフトロー形成への関わり」「ソフトロー形成・改定・運営主体の特徴」「強制力の効果」「強制力の掛かり方（直接的か、市場からの圧力か等）などの観点から、より詳細な研究を続けることにより「ソフトロー」の新たな特徴・メカニズムが明らかになる可能性があると考える。

以上

【参考文献】

- （財）金融情報システムセンター,「金融機関等コンピュータシステムの安全対策基準・解説書」，平成 15 年 10 月
- （財）金融情報システムセンター,「アウトソーシングにおけるコントロールと監査」,「金融情報システム」，No.261，平成 15 年 1 月
- （財）金融情報システムセンター,「金融機関等のアウトソーシングにおけるシステム監査の実態調査」,「金融情報システム」，No.265，平成 15 年 7 月
- （財）金融情報システムセンター,「平成 15 年度　金融機関等コンピュータシステムに関する事故・犯罪動向調査報告書」,「金融情報システム」，No. 275，平成 16 年 11 月
- （財）金融情報システムセンター,「『金融機関等コンピュータ・システムの安全対策基準・解説書』の改定について」,「金融情報システム」，平成 17 年 6 月
- （財）日本規格協会,「JISQ15001 個人情報保護に関するコンプライアンス・プログラムの要求事項」，平成 11 年 3 月
- 根来龍之,「競争優位のアウトソーシング:＜資源―活動―差別化＞モデルに基づく考察」,「早稲田大学 IT 戦略研究所ワーキングペーパーシリーズ No.7」，平成 16 年 12 月

【参考 URL】

- 金融庁,「預金等受入金融機関に係る検査マニュアル」, http://www.fsa.go.jp/manual/ manualj/yokin.pdf, 平成 16 年 2 月（改定）
- 金融庁,「金融分野における個人情報の保護に関するガイドライン」, http://www.fsa.go.jp/common/law/kj-hogo/01.pdf, 平成 16 年 12 月
- 金融庁,「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」, http://www.fsa.go.jp/common/law/kj-hogo/04.pdf, 平成 17 年 1 月
- 日本銀行,「金融機関業務のアウトソーシングに際してのリスク管理」, http://www.boj.or.jp/set/01/fsk0104b.htm, 平成 12 年 4 月
- ジョイント･フォーラム,「金融サービスにおけるアウトソーシング」（日本銀行仮訳）, http://www.boj.or.jp/intl/05/data/bis0502b2.pdf, 平成 17 年 2 月
- 経済産業省,「システム監査基準、システム管理基準」, http://www.meti.go.jp/policy/it_policy/press/0005668/0/041008system.pdf, 平成 16 年 10 月
- （財）日本情報処理開発協会,「プライバシーマーク制度」, http://privacymark.jp/
- （財）日本情報処理開発協会,「情報セキュリティマネジメントシステム（ISMS）適合性評価制度」, http://www.isms.jipdec.jp/
- （財）日本情報処理開発協会,「ISMS 認証基準(Ver.2.0)」, http://www.isms.jipdec.jp/doc/JIP-ISMS100-20.pdf, 平成 15 年 4 月
- 日本公認会計士協会,「適合する Trust サービス規準及びその例示」, http://www.jicpa.or.jp/technical_topics_reports/008/008-20030609-01-02.pdf, 平成 15 年 6 月
- 日本銀行,「平成 17 年度の考査の実施方針等について」, http://www.boj.or.jp/set/05/fsk0504a.htm, 平成 17 年 4 月
- 金融庁　http://www.fsa.go.jp/
- 日本銀行　http://www.boj.or.jp/
- （財）金融情報システムセンター　http://www.fisc.or.jp/
- （財）日本情報処理開発協会　http://www.jipdec.jp/
- 日本公認会計士協会　http://www.jicpa.or.jp/
- American Institute of Certified Public Accountants（AICPA）http://www.aicpa.org/
- Public Company Accounting Oversight Board（PCAOB）http://www.pcaobus.org/
- The Office of the Comptroller of the Currency（OCC）http://www.occ.treas.gov/