事前の対策と環境づくりが重要

情報を漏洩させない経理アウトソーシングの心得

給与計算や月次決算、経費支払や旅費精算、年次決算と財務開示等の経理アウトソーシングを進めるに際しては、アウトソーサーの選定から業務遂行、成果物の受領にわたるすべての局面で有効な内部統制を敷くことにより、情報漏洩のリスクを大幅に削減することができる。一方、内部統制の強化だけでは防ぎきれない情報漏洩リスクも存在する。本稿では経理アウトソーシングの実務から現実的で効果的な情報漏洩防止体制について考えてみたい。

APアウトソーシング㈱
公認会計士・税理士
千葉　和彦

中央経済社『旬刊経理情報』2014 年 11 月 1 日号(No.1395) 寄稿記事

■はじめに

近年、諸経費の支払や従業員立替精算、請求書作成や回収入金の消込み、給与計算や社会保険届出といった経理・人事業務や、月次決算・年次決算と財務開示資料作成（英文開示を含む）といった財務報告業務を、会計事務所等にアウトソースする事例が多くなってきている。現代のネットワーク化された情報社会では、これらの経理・人事業務を比較優位の経済原則に基づいて戦略的に外部の専門家にアウトソースするほうが、自社の競争力を高めることが可能となるため、ますます経理・人事業務のアウトソーシング化は進むと考えられる。

一方で、クライアントのさまざまな経理情報・人事情報等の機密情報が、アウトソーシングの過程のなかで会計事務所等の業務受託者（以下、「アウトソーサー」という）に伝達されるために、それらの機密情報が外部に漏洩するのではないかというリスクも増大する。したがって、経理アウトソーシングにおいては、いかに情報の機密性を確保し、漏洩を防止するかが重要な課題となる。本稿では、経理アウトソーシングの実務の観点から情報漏洩防止のあり方を考えてみたい。

■アウトソーサーの選定における留意点

(1) 見積提案依頼書の作成

情報漏洩防止のためには信頼性の高いアウトソーサーを選定することが肝要である。

経理・人事業務のアウトソーシングの大きな目的の1つに、コスト削減があることはいうまでもない。しかしながら、単に経済的な理由だけでアウトソーサーを選ぶのは大きな誤りである。契約期間が長期に及び、しかも自社の経理・人事業務のかなりの部分を任せることを考えると、アウトソーサーの選択は重要な業務アライアンスのパートナー選びそのものだからである。

アウトソーサーの選定にあたっては、経済面のみならず、種々の要素を取り入れて多面的に分析・検討しなければならず、それらの要素を「見積提案依頼書」（RequestFor Proposal, RFP）のなかに記載し、アウトソーサーに対して提示することになる。もちろん、まったくRFPが提示されずに、「100人の給与計算と社会保険業務のフルアウトソーシングはいくらか」というような非常に乱暴な依頼の場合もあるが、アウトソーサーの選定にあたっては多面的な内容をRFPに盛り込み、アウトソーサーの内部統制の整備状況、情報セキュリティ方針、漏洩防止対策や事業継続計画等を評価すべきであろう。

（図表 1）アウトソーサーの選定

選定のステップ	選定のポイント
①RFP の作成	過去の実績
	情報セキュリティの概要
	情報システム部門や外部コンサルの活用
②NDA の締結	秘密情報の定義
	個人情報の取扱い
	第三者開示義務の要件　など
③内部統制の事前調査	書類審査
	プレゼンテーション
	実地調査　など
④業務委託契約書の締結	秘密保持条項
	インサイダー取引防止条項
	再委任禁止条項
	監査権限　　など

(2) 見積提案依頼書の内容

以下では、どのような事項がRFPに盛り込まれているかを簡単に紹介する。

1. アウトソーサーとしての経営方針、規模、過去の実績といった一般的情報
2. 依頼する業務の具体的範囲
3. 期待する最低限のサービスレベル
4. アウトソーサーの使用する情報システムの状況（ハードやソフトに関する基本事項）
5. アウトソーサーの情報セキュリティの概要（アクセス制限等の情報漏洩対策）
6. アウトソーサーの事業継続計画
7. インサイダー取引の防止に関する事項
8. 内部監査および外部監査の実施状況及びそれらの受け入れ体制

弊社が受け取るRFPも数頁前後のものから50頁を超えるものまでさまざまである。アウトソーサーに対しRFPを作成・提示することはかなり専門的な業務であり、経営者に直結した経営企画部などが主体となり、かつ社内の情報システム部門、外部のコンサルタント等も活用して、漏れのない精緻なRFPを作成すべきであろう。

(3) 秘密保持契約の締結

アウトソーサーがRFPへの回答を作成するにあたっては、クライアント企業の種々の機密情報や個人情報に触れる場合も多いため、秘密保持契約（Non-DisclosureAgreement，NDA）を締結する。NDAでは、秘密情報の定義、秘密保持義務、従業員や第三者への開示の条件、個人情報の取扱い、情報の返還、損害賠償等の条項が記載される(1)。クライアント企業のなかにはNDAを結ばずに見積提案依頼をするところもあるが、やはり、法的な情報漏洩防止策として、NDAの締結は重要である。

(4) アウトソーサーの内部統制の事前評価

RFPへの回答を候補アウトソーサーから入手後は、それらを評価し最終的に決定することになる。その際に、RFPへの回答の書類審査だけでなく、候補アウトソーサーを招いてプレゼンテーションを行わせることが重要である。

アウトソーシングは器官の移植手術のようなもので、経営者から従業員レベルのどの各階層においても拒絶反応を起こすようなものであってはならない。情報漏洩に対するアウトソーサーの経営姿勢が極めて真摯であり、職業専門家としての正当な注意義務を持って高いレベルで業務が遂行され、クライアント企業の情報セキュリティ方針や経営文化となじむものであるかどうか、プレゼンテーションやその後の質疑応答等を通じて十分に吟味すべきである。大変時間を要するため候補者数が多い場合、書類審査で絞り込み最終候補となる数社にプレゼンテーションを行わせるほうが効率的である。

また、実際にアウトソーサーの業務遂行場所（ファシリティ）を訪問し、RFPの回答やプレゼンテーションで知り得た情報を実地見聞することも可能な限り行うべきである。その結果、書面では知り得なかった事項等が明らかになり、最終候補数社との質疑応答を繰り返しながら1社を決定していく。このプロセスは、まさに重要な幹部人材を採用する手続と同じである。

(1) ＡＰアウトソーシング編『実例でわかる経理アウトソーシングの実務』（ 中央経済社、２０１３年）参照。

■アウトソーサーの管理における留意点

(1) 情報漏洩の要因と内部統制

一般に情報漏洩等の不正行為や不祥事が発生する原因には、個人的・主観的な事情（動機や正当化）と客観的事情（機会）があるといわれている。

前者は、個人的な借金の返済のために機密情報を意図的に外部に提供する場合であるとか、この程度の不正・漏洩ならば問題が起きないだろうと正当化するような場合である。これは人の心情・倫理の問題であるため、内部統制による制度的な防止策は大変難しい。特に経営者レベルでの不正は内部統制の限界を超え、社外取締役や社外監査役機能の強化により経営者を厳しく監視、監督する以外はない（いわゆる企業統治の強化）。

アウトソーサーの経営者に対しても、同様な監視・監督体制を採る以外にないと思われる。従業員レベルにおいては、職業倫理や不正のリスクが及ぼす影響に関する継続的な教育と研修を通じて、そのような主観的事情（動機や正当化）が起きないような環境や文化をつくり出すことが重要である。

一方、後者は情報漏洩の機会を許す客観的事情である。たとえば上長の承認が形骸化している、ダブルチェックの体制が弱い、ITシステムが脆弱で内部・外部から攻撃の対象にされやすい等により不正や情報漏洩が起こる制度的な環境要因であり、然るべき内部統制を強化することで相当程度防止が可能である。以下では、その対応策について紹介する。

（図表２）情報漏洩の要因と内部統制

情報漏洩の要因/ 内部統制の有功性	内部統制による効果	具体例
動機や正当化など個人的・主観的事情	大きな効果は期待できない	・各種誓約書、職業倫理誓約書、退社誓約書等への署名
		・定期的情報セキュリティ研修
		・トップからの真摯なメッセージ発信
情報漏洩を許す客観的事情	有効に機能させることが可能	・社内 PC では、DVD、CD-R、USB メモリなどの記憶媒体についてアクセスを制限
		・外部ストレージのアクセスは禁止。SNS についても全面的に禁止
		・許可されていない記憶媒体の接続やサイトへアクセスをした場合、操作は中断され、アラートメールを発信。管理ソフトの導入

(2) 法的拘束

アウトソーサーが最終決定されると、まず行わなければならない情報漏洩防止策は、法的拘束である。業務委託契約書のなかに、秘密保持条項、個人情報保護条項、インサイダー取引防止条項、事故対応条項、再委託禁止条項、損害賠償条項等を記載する。また、アウトソーサーの業務提供場所で、クライアント企業による実地調査や監査の権限を記載することも有用である。[(2)]

(3) 内部統制に関する質問書

クライアント企業は、業務委託先であるアウトソーサーの内部統制がどのように整備され、運用されているか、常に監視し評価する必要がある。そのため、アウトソーサーに対して定期的に「内部統制に関する質問書」を作成・送付して回答を入手し、整備状況に不備がある場合には然るべき対策を講ずるように勧告する。また、必要に応じアウトソーサーへの実地調査や監査も行う。弊社でも多くのクライアント企業から「内部統制に関する質問書」を受け取るが、その内容を以下に簡単に紹介する。

① 全般的リスクマネジメント

経営陣によって承認された全社的リスクマネジメント・プログラムがあり、適切に構成員に通知されているかどうか。そのプログラムを維持・評価する責任者の有無。

② 情報セキュリティ方針

セキュリティの認識についての研修と教育。方針を遵守しない場合の取扱い。アクセスコントロール、アプリケーションセキュリティ、暗号化、モバイルコンピューティング、リモートアクセス、ソーシャルメディア・ソーシャルネットワーク、脆弱性管理等の方針などを定めた情報セキュリティ方針の有無。

③ 組織のセキュリティ

組織内にセキュリティの取組みを担当する情報セキュリティ機能の有無。部外者によるシステムやデータ・処理施設へのアクセス防止策の有無。

④ ＩＴ資産管理

経営陣によって承認されたＩＴ資産（ハードウェアとソフトウェア資産）の管理方針やプログラムが、適切に構成員に通知されているかどうか。その方針やプログラムを維持・評価する責任者の有無。業務の中断や一般的なサービスの中断をカバーする保険の有無。

⑤ 人材のセキュリティ

行動規範、倫理規範、秘密保持契約、施設利用規程等への入社時署名義務。セキュリティへの認識を高める研修プログラムの有無。退職等の場合のアクセス権の剥奪プロセス。貸与したＰＣ、携帯電話、鍵等の資産返却義務と時期。

⑥ 物理面および環境面のセキュリティ

アクセス制限とすべてのアクセス記録の保存。アクセスをコントロールする電子システム（キーカード、トークン、生体認証装置など）の有無。施設内または施設へのアクセスをコントロールする暗号ロック。外部者の入館時と退館時の記録。

⑦ 通信および業務管理

対象となるシステムやデータのバックアップ。対外ネットワークとの接続の有無。リムーバブルメディアに関する方針。電子メール送信の暗号化。メール添付ファイルのパスワード設定および暗号化。無効なログインによるアカウントロック。アクセス権の付与とアクセス承認権限の分離。社内標準外オペレーティング機器購入時の情報セキュリティチェックと承認。

⑧ アクセスコントロール

パスワードポリシーの有無（記録の禁止、情報漏洩の場合のパスワード変更、定期的な変更、ユーザーパスワードの共有の禁止等）。リモートアクセスの方針。

⑨ 情報システムの取得、開発、メンテナンス

文書化されたセキュリティ要件の有無。アプリケーション開発の場合、独立した組織によるセキュリティ評価の実施。すべてのアプリケーションに対する脆弱性テストの実施方法。対象となるデータについての暗号化ツールの維持管理方法。

⑩ インシデントイベントと通信管理

正式なインシデント対応プラン（報告手順、懲戒プロセス、ウイルス防止、ワーム等のマルウェア対策等）。サービスの中断方針。

⑪ 事業の継続と災害からの復旧

文書化された事業の継続と災害からの復旧に関する方針とプログラムの有無。パンデミックプランの有無。

⑫ コンプライアンス

情報システムがセキュリティ実施基準を遵守しているかどうかのチェック。ネットワーク侵入テストの実施。組織内の独立した監査機能の有無。

⑬ メディアの輸送

保証付きの配達業者の使用。追跡エレメントの記録。万全を期した輸送方針やプログラムの有無。

⑭ 個人情報保護

正式に文書化された個人情報に関する方針の有無。個人情報に関する定期的なリスク評価実施。情報セキュリティプログラムにおいて、他の情報と個人情報の保護は別々の対策を講じているかどうか。従業員等に対する個人情報保護に関する研修の有無。

(2) ＡＰアウトソーシング編『実例でわかる経理アウトソーシングの実務』（ 中央経済社、２０１３年）参照。

■アウトソーサーにおける内部統制の実践

弊社ではクライアント企業からの「内部統制に関する質問書」の要請になるべく近づけるように努力をしているが、「内部統制に関する質問書」の全部について100点満点の回答をすることは困難な場合が多い。内部統制を強化すればするほどコストがかかり、アウトソーサーとしての業務効率や市場での価格競争力を阻害するからである。そこで、費用対効果の見地から、弊社で行われている事務的対応例を図表3にていくつか紹介する。

（図表３） 内部統制に関わる事務的対応例

個人的・主観的事情の抑制	
①	入社誓約書、守秘義務誓約書、インサイダー取引等に係る誓約書、身元保証書（以上、入社時）、職業倫理誓約書（本採用時）、退社誓約書への署名。
②	入社直後の情報セキュリティ研修の実施。
③	社員に対する情報漏洩対策についての注意喚起や、情報の取扱いルールの整備や遵守、適切な管理を徹底する定期的な情報セキュリティ研修を実施。
④	違反者に対し、監視をしていることを知らしめるための厳重注意。
⑤	経営者による情報セキュリティメッセージの直接発信（四半期全体ミーティング時）。

客観的事情の抑制（内部統制の具体例）	
①	社内 PC では、DVD、CD-R、USB メモリなどの記憶媒体についてアクセスを制限。
②	IT 資産へのアクセス状況について操作ログなどを収集。ログの定期的、継続的なモニタリングを実施。
③	送信メールは全件コピー。携帯アドレスやフリーアドレス宛メールは原則禁止。業務上の必要性を確認するためにモニタリングを実施。
④	外部ストレージのアクセスは禁止。SNS も全面的に禁止。
⑤	許可されていない記憶媒体の接続やサイトへアクセスをした場合、操作は中断され、アラートメールを発信。管理ソフトの導入により少ない工数でより多くの細かいコントロールを実施。
⑥	健全な懐疑心でログなどを監視。
⑦	情報セキュリティに関する国際認証規格（ISMS/ISO27001）の取得と維持。
⑧	携帯電話やスマートフォンの社内執務室への持ち込み禁止（入室前に専用ロッカーに預け施錠）。
⑨	外部の専門家(公認会計士・公認システム監査人)による内部監査の実施とフォローアップ(年 2 回)。
⑩	IT 資産購入時のセキュリティチェックとリスク評価の義務づけ。
⑪	クライアント企業による内部統制監査の受入れ。
⑫	レストラン等「公の場」ではクライアントに関する会話を禁止。やむを得ない場合は隠語使用を徹底。
⑬	成果物の送付時における宛先、宛名、内容物のダブルチェックの徹底。
⑭	業務再委託の禁止。やむを得ず再委託をする場合は厳密な第三者評価を実施。業務委託契約書に基本契約書と同等以上の責任を明記。
⑮	クリーンデスク、クリアデスクの徹底。
⑯	施錠された専用の文書廃棄箱の使用。
⑰	情報資産の廃棄は専門業者に委託し、溶解を確認。
⑱	キーカードによる外部者の入室制限および監視カメラによる監視。
⑲	施錠されたロッカーへの文書保管。

■経営者のリーダーシップ

(1) 内部統制の重要性の認識

クライアント企業では情報漏洩防止のためにさまざまな内部統制を制度として整備・運用しているが、アウトソーシングを利用する場合に、アウトソーサーに対しても同様の内部統制が必須であることは前述のとおりである。アウトソーサーは会社の外にいる者であるが、社内リソースと同様に重要な経営機能の担い手であり、内部統制を怠ると単に「問題点の外出し」となってしまう。すなわち、情報漏洩等レピュテーションリスクを含む重大な経営リスクを生じさせることになりかねないのである。

情報漏洩等の不正行為や不祥事が発生する原因には、個人的・主観的な事情（動機や正当化）と客観的事情（機会）があることを述べたが、経営者は、後者、すなわち「情報漏洩の機会を許す客観的事情」を最小化するように内部統制を強化することで相当程度防止することができると肝に銘ずるべきである。そのような内部統制の強化は、アウトソーサーの選定から、契約締結、処理の実務、結果の受領に至るすべての局面で、人任せにせず、経営者がリーダーシップを持って行わなければならない。

(2) 当事者意識

「内部統制に関する質問書」がマニアックなまでに精緻に作られているにもかかわらず、その回答のフォローアップに関しては、クライアント企業により必ずしも実務上適切になされているとは限らない。必要以上に精緻な質問書を作り回答を求めたにもかかわらず、その後の音信がまったくない場合もあるのは、質問書を作る部署、回答をフォローアップする部署がまったく別々であり、経営者も現場任せで当事者意識が薄いのではないかと思ってしまう。

経営者が内部統制や情報セキュリティの専門家である必要は毛頭ないが、アウトソーサーでの情報漏洩防止のためには、「内部統制に関する質問書」の回答を踏まえ、不備があると考えられる点に関しては適時に追加質問を投げかけ、対応策を講ずるように強い態度で臨むべきである。その勧告に対する対応策もアウトソーサーから適時に入手し、納得のいくまでフォローアップが必要である。

また、内部統制の運用状況については回答だけではわからないことが多いため、回答をうのみにせずに、現場を視察し、組織的な監査を実施すべきである。そのことで、クライアント企業とアウトソーサーの間に適度な緊張が生まれ、情報漏洩防止に対する共通認識と協働意欲を形成できる。

アウトソーシングは、自社(クライアント企業)の業務の一部であり、その部分だけを精緻にしても、全体業務の視点での統制や最適性において意味をなさない。アウトソーサーに求める内部統制の精度は、自社でも実現できるものでなければならない、という強い当事者意識が経営者に望まれる。

(3) 研修の重要性

残された問題は、前者、すなわち、個人的・主観的な事情(動機や正当化)の抑制をいかにするかである。人間は不正の機会があり露見しにくい状況があれば弱い心が働き、つい出来心で善が悪に変化し自制できなくなるという「性弱説」に立脚することが重要であろう。すなわち、経営幹部や従業員に対しては、トップの経営者より情報漏洩等の不正行為に対して厳しい態度で臨むという強いメッセージを発信し続けることが不可欠である。それは、単にお飾り的メッセージであってはならず、経営者自身が生の声で経営幹部や従業員、アウトソーサーにひしひしと語りかけるものでなくてはならない。

情報セキュリティに関する定期的な社内研修は、万全ではないにしても個人的・主観的な事情の抑制に貢献する。「性弱説」という認識のもと、1回だけでなく定期的・継続的に行っていくことが重要である。単にITリタラシーをつける研修ではなく、ケーススタディやワークショップを取り入れ、各階層の参加者自身が問題意識を持って参加し、実践的な判断力を養成する場にすべきである。参加者が内容を理解し、自分のものとなってこそ意味ある研修になる。情報セキュリティに対する経営者の意思を直接的に伝えるよい機会として、経営者は可能な限り研修のなかで「情報セキュリティの重要性」を力説すべきであろう。決して他人任せにしない経営者のコンプライアンスに対するそのような「真摯な姿勢」こそが、最後の砦であると思う。

千葉　和彦（ちば・かずひこ）
APアウトソーシング㈱　代表取締役
APO-税理士法人　代表社員。公認会計士・税理士
1982年アーサーアンダーセン東京事務所入社。
1989年より同シカゴ事務所に5年間勤務。
2004年有限責任あずさ監査法人の会計アウトソーシング部門をMBOし、APアウトソーシング㈱を設立。
福島大学経済学部卒。
著書に『実例でわかる経理アウトソーシングの実務』（中央経済社、2013年）がある。