タイトル：IT の外部委託と海外委託：リスク評価と管理

著者: Arthur D. Perez, PhD and Glenn Morton
(Pharmaceutical engineering, 2010, vol .30, No6, 1-9)

翻訳：　高林　信能（Nobuyoshi Takabayashi）
監修：　川上　浩司（Koji Kawakami）

はじめに

ハードウェアは汎用されているものの値段は高くはない。インターネットのパワーは第三者によるデータセンターを増やし、そのデータセンターは利用者に設備やスタッフがもはや企業の建物の地下にないことを多くのクライアントに気付かせることなく、サービスを提供することが可能となっている。

ソフトウェアはさらに強力で、我々はより依存している。ソフトウェアサプライヤはヘルスケア企業のニーズを取り入れてきており、かつては選択肢がなく利用会社がソフトウェアを独自に開発しなければならなかったが、今や機能を実行するための複合的な商用のアプリケーションが存在している。結果的に、ヘルスケア企業はソフトウェア開発のために小数のスタッフを雇う程度で済むようになっているかもしれない。同時にこのことは、ヘルスケア企業はユニークなニーズに合わせるため、または市場での優越性を得るためのソフトウェアを臨時で開発するリソースを有していないことを意味している。

このような状況はインフラストラクチャ管理やソフトウェア開発の両方の面で、ヘルスケア企業と外部委託される IT サプライヤ間の契約を急増させた。本稿では、そのようなパートナー企業と連携する時に考慮しなければならない多くのリスクや緩和戦略について検討する。これらのリスクのいくつかは我々の産業に特化したものであり、ほかのいくつかは IT サービスのパートナーを探すどのような企業にも共通するものである。GAMP®5 は外部委託上のいくつかの問題点を付録に記載しているが、本稿は実施前から業務中にかけて管理しなければならないリスクに焦点をあてる。

なぜ、外部委託するのか？

最大の要因は、IT 業務を管理、実行できる専門性を有したスタッフに投資し、維持することの難しさであろう。これは小さな企業であるほど当てはまる。何百という IT スタッフを有する大企業でさえ、大規模な IT サービス企業によって達成され得るスケールメリットと対抗することはできない。そのようなプロバイダーはコンピューター関連のリソースとスタッフ機能をヘルスケア企業では真似できない程に強化することができ、大規模な製薬企業がかけている費用の 2 倍程度で 10 倍以上のデータセンターを管理できるかもしれない。

さらに、大規模なグローバル IT サービス企業は、労働賃金が安い国で業務をおこなうと

いう費用上の利点を有しており、欧州や北米に位置するデータセンターの企業を利用しないという選択ができる。例えば、インドではより大きく、より教育された IT 専門家の労働市場があり、欧州や北アメリカの労働者の一部分の労働費用でまかなうことができる。理論的に、これらの経済的な優位性は、いずれサービスの改善につながるであろう。

外部委託はヘルスケア企業にプロジェクト実行のための柔軟性を大いにもたらす。例えば、大規模なグローバル SAP の更新を実施しているか？それなら、一年間に 50 人の ABAP プログラマーを加えることができる。製造現場を閉鎖しているか？それなら、適切な水準にサポートを減らすことができる。

IT サービスの外部委託/海外委託で生じる不利益

外部委託されたどのような業務も、監督権は引き渡される。業務がどのように実行されているか透明性の点でも相当な縮小になる。これらの要因には、ある程度の信頼性が必要であり、いくつかの組織化された企業では認めがたいことかもしれない。

契約交渉で適正なサービス水準を見つけることには注意を要する。要求が大きすぎれば節約効果は減るだろうし、要求が小さすぎれば IT 部門が利用者の憤怒にさらされるリスクが生じる。これは、おそらくコストを増やし更なるリソースを必要とさせ、結果的に不満のあるユーザーや節約効果の減少へとつながる。外部委託先が内部のビジネス習慣を変えることを決めるなら、これは組織化された企業にとって大きな効果をもたらすかもしれないが、リスクの増加や予期せぬ費用が発生するかもしれない。

最終的な留意点は、外部委託を準備している者にとって明らかにより低い費用は、とても魅力的に見えることである。クライアントの要望に対して契約した企業の能力を完全に理解せず見誤ることは、見込んでいた費用削減効果を容易に失うことになるだろう。

すべてはデータのために

15 年ほど前、きわめて独立していたという長所によって電子データは合理的にただ安全なものであった。製造や品質管理の結果、臨床試験や多様なその他の重大な情報からのデータは一般的に企業のデータセンターのハードディスクにあり、企業のネットワーク外から非従業員やその他の者がアクセスすることはできなかった。今や明らかにこのような状況ではない。

今日では、情報は多様なサイトを介して企業内で共有され、そのうちいくつかは公共のインフラストラクチャを通して伝送される（多くの企業の WAN はインターネットを活用している）。契約社員は彼/彼女らの PC を介して企業内ネットワークにアクセスしているかもしれない。USB フラッシュのようなメディアの拡がりは、直接的なアクセスをしていなくても、不正な方法で情報共有を行っている正社員を介して間接的なアクセスをしているかもしれない。結論を言えば、企業のデータが請負業者のノートパソコンにある経路は数多くあり、企業がそれを効果的にコントロールする方法はない。

企業はサービスを供給する他の企業と情報供給するかもしれない。例えば、配送データを必要とする宅配企業や臨床研究受託機関（CRO）といった企業が該当する。外部委託されたIT サービスのプロバイダーは自身のサーバーに企業データを有しているかもしれない。このことは自国のパートナーに対してでさえ複雑なものであるのに、異なった国の法令によって縛られている海外委託では更に複雑なものになる。国の法令の違いの点で、個人情報（PII）保護ほど激しく批判され、際立って問題となっているものはない。これは臨床試験の記録や従業員記録等を扱わなければならないヘルスケア企業に間違いなく影響を与える。

最後は、パートナー企業の提携先に関するものである。上記で言及した宅配企業はIT サービスを下請けにだしているかもしれず、軽率なヘルスケア企業のデータが聞いたこともないような企業の機器に存在するかもしれない。

データに関する主要な3つのリスク

外部委託のパートナーと提携を考えたときに、保護されなければならないデータに関連した3つの懸案事項がある。

1. 完全性：データは何であるか、そして、データはあるがままである必要がある。例えば、監査の経過は完全なものでなければならないし、精度や確度は失われないようにしなければならない。そして、もちろん、それらの保存期間が終わるまで、記録が失われることや、削除されることがあってはいけない。
2. 可用性：データは必要時に必要とされる場所で、合理的な必要性があるときにのみ使用できる必要がある。
3. 機密性：例外的に慎重に扱うべきいくつかのデータがあり、保証されていない環境から守られることが不可欠となる。このような情報にはIP（知的所有権）、PII、特権を与えられた弁護士・依頼者間のコミュニケーションやさまざまな他のビジネス情報が含まれる。

5つのリスク領域

論点のポイントを理解するために、評価しなければならない5つのリスク領域がある。

- ガバナンス
- 国
- 企業
- 契約
- 契約業務の性質

本稿の残り部分を用いてこれらのリスク領域を詳細に分析する。

リスク#1: ガバナンス

契約しているヘルスケア企業は、全ての活動や関連するリスク、契約内容の順守、そしてビジネスの要求に応じたサービスの変化を特定することに、ある程度の見通しを確保しておくことがガバナンスには必要不可欠である。それを達成するためには緻密な管理や報

告から監査によるものといった多様なアプローチがある。そのアプローチは当事者間の信頼の程度に大きく依存する。理想的には、重大な出来事が生じたときのクライアントへの報告を含め、パートナーが標準的なプロセスを順守している、利用可能なリソースや手段を最適に利用している、リスクを適切に管理しているといったことに、契約している企業が自信をもっている状況である。効果的なガバナンスは、ほかの 4 つの領域におけるリスクの同定、緩和、管理にも大きな役割を果たす。

ガバナンスの範囲は全ての部門や地理的な位置を含めなければならないし、IT、情報保護、事業単位で開始した関連活動も対象にしなければならない。ガバナンスの実施には、全ての関連する/利害関係のある企業からの参画、活動の証拠書類や結果の報告を必要とする（図 2）。効果的であるために、ガバナンスのチームは影響する全ての管轄下の法律と規制を十分に理解しておく必要がある。

リスク#2: 国

法律/規制

国内法令が外部委託のパートナーを雇用するのに取り組んでいる方法にどのように影響するか理解することは重要である。一般的に、図 3 で描かれたように、企業情報を保護する強力な国内法令がない場合、契約しているヘルスケア企業はおそらく、いくつかのリスク緩和策を導入しなければならないだろう。より強力な法律は一般的に、より大きな保護をもたらし、緩和策は必要なくなる方に働く。

考慮を要する独特の法律や規制にはもちろん GxP 規制も含まれるが、GxP は幸運にも世界中でかなりそろっている。一方で、知的所有権（IP）の保護はそろっていない。いくつかの国家では IP は特許を取得できない。もし、情報に欠陥があるなら企業に何百万、もしくは何十億という費用が発生しかねない。別の考慮すべき事項は強制実施権に関連する。データが存在する国家の政府は現地の低賃金の製造業者の利用のために、ビジネスパートナーに情報譲渡を強制させることができるだろうか？

データのプライバシー法は国家間で大きく異なっている。欧州の法律は一般的に米国の法律より保護的である一方でインドは米国より保護的でない。米国の中でさえ、データプライバシーに関連する州法の要求はかなり異なっている。何のデータが含まれているか、データが保管またはコントロールされている両方の国で、そして、関係している人々が居住する管轄域の全てでデータが何の法律に関連するかを企業が理解しておくことは必須である。もし、適切な管理を確立できないなら、関連する法律に従うために管理を外部委託するよりも、ヘルスケア企業内に PII を伴ったデータベースを保管する必要があるかもしれない。

米国の Sarbanes-Oxley 法のように、財務に関する規制は新たなリスクとなるかもしれない。例えば、管理するのにデータへ制限されたアクセス環境を必要とし、IT サービスのサプライヤが 70 名の UNIX サポート員全体に財務アプリケーションを有するサーバーへの管理権

を望むなら、断固とした米国の法律に応じるために必要な管理への理解について明らかにずれがある。

最後に、訴訟の電子的開示手続きに関連したルールを理解する必要がある。例えば、米国の法律は弁護士と依頼者間の秘匿特権に該当する情報に関連した保護について、かなり明快である。この権利は他の国では存在していないかもしれない。そういうわけで、企業の法務部は外部委託との契約構築時に関与するべきである。

慎重に扱うべきデータの暗号化や、いくつかの国で、あるデータを保管または使用しないという方針といった緩和対策に上記の要因は影響し得るだろう。

他国でのリスク

海外のパートナーを評価するとき、データとは異なった他の要因が考慮されるべきである：

- 法律体系は一般的に効果的であり、政治から独立しているとみなせるか？
- 税の方策が明快または契約している企業が巨額で予期しない増税に襲われることがあるか？パートナーは突然消えるかもしれない優遇税制措置を考慮しているか、高額で予期せぬ経費を契約している企業に預けているか、または、もはや操業さえ危ういパートナーであるか？
- マクロ経済上危険な要因があるか？現地通貨が不安定であるか、またはその国は持続性のない他国の援助に依存しているか？支払いのバランスは政治の安定性に脅威となっていないか？
- 戦争、暴動、テロ、暴力的な犯罪の可能性により治安に危険はあるか？
- 政府は政治的に安定しているか？それは友好的でなくなる可能性はあるか？
- 政府が友好的であり安定しているなら、それは効果的か？既得権利との汚職または衝突の問題があるか？
- 国は、ビジネスで必要な会議ができる、しっかりとした社会基盤（電力、電話、インターネット、道路など）を有しているか？著しく災害に脆弱であるか？
- 労働市場はビジネスの要望に沿っているか？必要とされる技術を擁する労働者の十分な供給量があるか？労働者は一般的に幸福か不幸か？一時解雇を妨げる国内の法律があるか？国の法基盤は、効果的な雇用前の素性調査を可能にしているか？

カントリーリスクの緩和

その国の独特なリスクに取り組む過程では、最初に、適正な評価のところでかなりの労力を要する。海外のパートナーを評価するとき、ヘルスケア企業の戦略的業務配分を担う部門が関わらなければならない。問題になっている国の知識を有する外部弁護士を含め、法務部が関わることも強く勧められる。このようなリスクを評価するのに特化したコンサルティング企業があり、そのような企業との提携は有益であろう。産業調査の情報源や報道の注意深い精読も、方針決定の過程に役立つ。契約を交渉するとき、カントリーリスクを緩和するために設定された、いくつかの保護策を盛り込むことが可能である。例えば、

別の国の契約社員によるデータアクセスを許可する前に承認を必要とすることは、新しい国の IP やデータプライバシーの法が適切であるか評価できる能力があることを示すことになる。たとえそうでなくても、抑止することにはなる。

カントリーリスクを評価するときの最終的な決断は、”我々はここでビジネスをしたいか？”ということに要約されることもある。しかしながら、その業務が認められる程度の他の緩和策があるかもしれない。例えば、特定の地域で行なわれる仕事の内容を制限することや、暗号化のようなデータ保護対策を追加するといったようなことである。

リスク#3: 企業

すべての潜在的なパートナーが等しく作られているわけではない。より上手に経営している企業や、より安定している企業、また、ハングリーに仕事を獲るため契約に目を光らせているたいへん優秀な企業などがある。不幸にも、経営がうまくいっていない企業やまじめにコンプライアンスに取り組んでいない企業、もしくは共に満たす企業もある。

外部委託先のパートナーを評価するとき、その企業が安定しているかどうか知ることは重要で最初に行なうことになる。企業がデータセンターの実務を外部委託先へ移すことについて真剣に考えているなら、その計画を実施するには、パートナーが破産宣言をしていない、従業員を解雇していない、すべてのサーバーを売却していないといったことを確実にしておくのが望ましい。これは契約締結の前にかなりの労力を要するだろう。加えて、その企業の財務上の安定性を継続的にモニタリングすることになる。パートナーのリーダーは安定面や効率面でも評価されるべきである。2 年間以上 3 人の CEO を有していた企業はおそらく、根本的ないくつかの問題があるのだろう。

多くの大規模な IT サービス企業は複数の場所（いくつかは海外）に事業所を有している。パートナーの企業は実務上カントリーリスクをもたらすような、より低賃金の海外リソースの利用を最大化したいということになるだろう。その場合、データプライバシーが主な懸念事項となる。一般的に、それには許可なく異なった場所へのデータ移動を禁止させる契約を交わすことが望ましく、またそのような移動に関する全てのリスクを最初に評価することなく承諾されるべきでない。

ひとつの国の中でさえ、サービス供給企業が異なった場所で同じプロセスに従わない可能性がある。別の論点としては、場所に関連するかもしれない。その場所は自然災害に脆弱だろうか？ヘルスケア企業は活火山のふもとや毎春洪水をおこす川の土手に主要なデータセンターは置かないようにしているだろう。

特に GxP、他の規制、またデータのプライバシーの要件に応じる必要性を考慮すると、パートナー企業の経験値が関連してくる。コントロールされた環境下で作業したことがない企業は、彼らが必要としていることをしていると主張し、コンプライアンスは論点とならないだろう。しかし、これまでの経験では、期待される書類の量や厳密さは、不慣れなパートナーをほぼ必ず驚かせてきた。彼らが要件を受け入れ処理するためには数年を要す

るものであり、これはヘルスケア企業の場合、GxP SMEs の監視下で活動をしていないという事実により、さらに事態は悪化する。この観点で、ヘルスケア企業は破格の安い価格を提供しているようにみえる未熟な企業に対し慎重になる必要がある。彼らは悪い方へと巻き込まれていることに気付いていないだろうし、直接対応して失敗した責任をとらされていないので、まじめにその要件に取り組まないかもしれない。

パートナー企業の社員に関連したいくつかのリスクがある。契約しているヘルスケア企業は慎重に扱うべきデータがリスクにさらされており、パートナーの従業員は自身の従業員と同様に最低限の基準は合わせるべきであることを認知しておく必要がある。バックグランドの確認は少なくとも国家インフラストラクチャの能力内で繰り返されるべきである。従業員の離職率は重要な留意事項である。発展途上の経済下での離職率は、技術を要する職業でさえかなり高く、30%程度である。これは、職員がいつも学習曲線の急峻な位置におり、労働効率が低いことを意味している。継続性の欠落の結果として、コンプライアンスの資料の質にもよくない影響を与えることになり得る。最後に、職員は必要とされる規制について訓練され、契約している企業のビジネス要件を理解すべきである。この訓練はパートナーによって提供されることになるだろう。

外部委託を魅力的なものにする同程度の経済規模は新しいリスクを発生させる：役割分担。もし隣のキュービクルで競争相手のために仕事が行なわれていたら問題だろうか？もし、同じ人が競争相手の仕事も請け負っていれば問題だろうか？

もし外部委託したパートナーが失敗し、その失敗がヘルスケア企業に巨額の費用を生じさせたなら契約は賠償を求めることができるだろう。しかし、1000 万ドルの価値のパートナーが 1 億ドルの価値がある知的財産を失うようなデータ盗難のために支払いができるとは思えない。これは、そのような企業に任せる業務内容に影響するかもしれない。

企業リスクの緩和

企業に関連したリスクを認め、回避し、緩和するのに重要なことは、再度になるが、適正な評価をすることである。宿題にしよう。できる限りその企業について調査する。施設に行き、監査をする。できるなら、満足感を得ている顧客と不満をつのらせている顧客の両方をみつけ、話してみる。

たとえ、最も低い費用の企業と取り組む、または単に”終わらせる”という相当なプレッシャーがあっても、将来的に不十分であろうパートナーと契約しないことである。*Caveat emptor* : 取引が良すぎて真実であるはずがないように思えるか（それはおそらく真実ではないが）自覚する。最後に契約書を注意深く書く。パートナーが契約したサービス外の部分で欠落しているとき、説明した業務をパートナーが行なうことが何と難しいことか、大変さは相当なものである（次章参照)。

リスク #4： 契約リスク

費用節減の最大の敵のひとつ（つまり十分な財務リスクといえる）として、契約したサ

ービスレベルについての具体性のなさや、望まれるサービスレベルを達成するために整えられているはずの評価基準のすべてに不明確な表現があるといったものがある。前もっての適性評価は、結果的により確固たる、現実的な値段となり、後の”ささいな”費用を減らすこととなる。全体費用のかなりの割合になる過剰なささいなことは脆弱な契約の表れである。

いくつかの特異的なリスクのシナリオは契約内で直接、対処しなければならない。これらのシナリオが生じたときに期待される行動を詳細に記載するべきであり、期待されるものが満たされていない又はヘルスケア企業が損害を被った際のペナルティーの項を含むのも賢明である。もちろん将来のパートナーが契約上のペナルティー用語に抵抗することは十分ありそうなことであるし、どのくらいの信頼が見込まれているか理解することが責務となる。いくつかの場合、ペナルティーの項の受け入れの拒絶がサプライヤを不適格とみなすのに十分であるかもしれない。

対処すべきいくつかのリスクは以下に記載するが、その他のリスクもあり得る

- **知的財産（IP）保護**：ほかのデータから分離されているかも含めて、どのように安全に保たれているか評価基準を決めておく必要がある。アクセスできる者、何の環境下、そしてそれがどのように許可され管理されるかも契約で特定しておくのが望ましい。
- **違反通知**：発覚した事象または情報の喪失において、ヘルスケア企業はすぐに知る必要がある。契約は何が違反であるか、それがどのように迅速に報告されなければならないか規定すべきである。追求や軽減活動のために両方の組織の責任も決めておくべきである。
- **補償金：**データ破棄やほかの重大な出来事に対し、ヘルスケア企業は損失の負担を軽減するために金銭上の補償を求めるだろう。そしてパートナーの企業は支払い能力を有していなければならない。
- **監査する権利：**契約しているヘルスケア企業は契約の遵守を検証するためにパートナーの企業を監査する権利を保持しておかなければならない。”正当な理由による”監査ガイドラインや、通常の監査の頻度、報告の要件を契約に特記しておくことができる。
- **継続性/災害からの復帰：**契約のビジネスの継続性に関する項はヘルスケア企業の継続性を確保する必要がある。この観点から、パートナーのビジネスの継続性は二次的なものである。ヘルスケア企業はシステムに再接続するために、二つの銀行、小売店、ネイルサロンの行列で待ちたくはない。対策として、一時的にデータ転送や他のどこかでの作業を要するなら、そのことは特記しておくべきである。見落とすかもしれない一つの側面は、DR test のために IT サプライヤとヘルスケア企業のシステム所有者との協調である。サービス供給者は型にはまった業務よりも、DR test のために違った仕事の実例を必要とするかもしれない。しかしながら、災害は型にはまった業務とは程遠いことは認識しておく必要がある。契約に記載しておくことは、この極めて重大な活動に伴う問題を避けることになるだろう。

- **背景確認：**ヘルスケア企業が雇用前の素性調査を必要とする場合、パートナーの従業員にそのような予防措置を求めることが妥当な場合のみ実施する。これは条件に明記されるべきであり、特に日常的に行なわれない習慣なら、なおさらである。
- **分離：**IP の点をクリアしたとしても、ヘルスケア企業は他の企業とは分けてデータを保有したがるかもしれない。例えば、企業が ERP アプリケーションを外部委託する場合、その他の企業と共にプールされたデータを保有するのを受け入れることができるだろうか？それとも独立したデータベースを要するだろうか？別の点では人員配置がある。同時にそのヘルスケア企業とは別の顧客とも働いている従業員を受け入れることができないなら、契約書に明記するべきである。
- **安定性：**パートナーが廃業したなら、データ、アプリケーションそして従業員でさえ、どうなるか考えてみることである。アプリケーションがパートナー企業のハードウェアで起動しているなら、その企業が破綻したとき何がおこるだろうか？ヘルスケア企業が頼りにしている多くの主要な専門家はパートナー企業に雇用されていると推測されるので、彼らの運命は関心事となる。契約で破綻に対し保護対策をしておくことは難しいが、パートナー企業が不安定な場にいることにアラートがでるよう財務報告の項を含むことはできるかもしれない。経費削減の指標としてパートナー企業が人員を切りつめる場合、ビジネスに不当に影響しないようにするためにヘルスケア企業はどんな予防を考えるだろうか？
- **出口戦略：**必要に応じてパートナーシップを合理的に問題なく解約できるようにヘルスケア企業は確保しておく必要がある。同様に、パートナー企業が関係を解消することを決めた場合、その企業または異なったサプライヤに滞りなく移行する手助けを行なう条項があるようにしておく必要がある。別の組織へのサービス移行を補助することを含め、解約通知のタイムラインは契約にあるべきである。

契約に関連したリスク緩和

サプライヤにおけるある組織や活動は最も都合のよい契約になるようにとても支援的である。調達部門や法務部門は確実に参加するべきである。彼らは契約交渉や大部分の人にはひどくわかり難い契約用語に最も経験を有している。コンサルタントもサプライヤの能力を理解するのに大変役立つ可能性がある。また、内部の主要な専門家には深く関わってもらう必要がある。これらの SMEs は内部の IT 顧客に加え、QA のようなほかの部局も含めた十分な範囲から成るべきである。小チームで運営することは簡単であるが、重大なビジネス上の必要要件も忘れやすい。サービスのサプライヤは追加の支払いなしで契約外と感じる仕事をするのは拒絶できるよう明示しておくことができる。契約の必要要件一覧にこのことを加えているなら、そのような仕事に驚くことはないだろう。

その他のクライアントからの推薦、産業調査や効果的な見積り依頼書（RFP）のプロセスは、適正なサプライヤを選ぶことや契約条項のいくつかを選ぶのに強力なツールとなる。直接の監査を含め、サプライヤの評価は契約に記載しておくべきサプライヤの欠点を強調

するのにも役立つ。

リスク#5: 業務の性質

扱っているデータの種類やデータになされていることはリスクに対し決定的なインパクトをもつ。個人情報の盗難の流行やその事項への立法者の注目の具合から、PII の取扱いは主要なリスクとなり得る。このカテゴリーに含まれているものとして、人事記録やソーシャルセキュリティーナンバー、連絡先、患者情報といった記録がある。後者は病状、薬剤、誕生日等といったデータも含む。異なった司法権は個人を特定できるものの解釈も異なる。ゆえに、そのような記録がパートナーによって扱われるべきかどうか、どのようなコントロールが必要かを決めるときにデータが保管されている、かつ／または、扱われている場所だけでなく個人が居住している司法権の要求を理解しておくことが必要不可欠である。

他の機密情報も同様に考慮される必要がある。もし破られたなら、企業に甚大な被害を起こし得る類のビジネス上の情報がある。例えば合併と買収のデータや弁護士依頼者間の秘匿特権下で保護された書類といったようなものである。おそらく直接的な被害は少ないかもしれないが、販売キャンペーン、売上高、銀行取引、そして当然であるが知的財産に関する情報は競争上の強みに重要なものである。

業務の性質によるリスクの緩和

どの業務を外部委託することができるか決める際に、内部の主要な利害関係者は数名含まれるべきである。このグループには、法務部、情報セキュリティー、個人情報保護管理オフィス、GxP 適用のための QA、そして事業主が含まれる。リスク分析や緩和のためにとられる手段は委託中の期間にわたって変化するかもしれないことを認識しておくことは重要である。

データの種類について事前に基準を取り決め、データのそれぞれの種類に戦略を決めておくことは、よい考えである。例えば、ある慎重に扱うべきデータに対し、パートナーの従業員の一部のみにそのようなデータへのアクセスを制限することや暗号化のような技術的な管理によってリスクは減るかもしれない。

リスクの平均化

与えられたアプリケーションやデータセットに対する全体のリスクは、リスクの 4 要因の合計として”定量化する”ことができ、すべては効果的なガバナンスというレンズを通して見ることができる。

国のリスク
企業のリスク
契約リスク
＋業務とデータの性質

＝全体のリスク

これらのすべてが考慮されるとき、可能性のある 4 通りの対応がある。図 4 で示すように、これはちょうどリスクインパクトと可能性をプロットした 2x2 表にあてはまる。これらへの可能性のある対応は：

- （法的責任や説明責任を外部委託することはできないと理解しながら）サービスのサプライヤがリスク管理することを許しリスクを無視する。
- リスクを受け入れ、サプライヤに緩和策を委任する。リスク緩和の努力はモニターされ報告されるようにする。
- リスクを受け入れ、ヘルスケア企業内で緩和策を管理する。この場合は、リスク緩和の責務がとても重大でサプライヤに任せることができない場合と考えられ、解決策はクライアントから生じる。
- リスクを全体的に回避する。典型的には、これはデータを内部で保有し管理することとなる。リスクプロファイルが高インパクト／高確率から高インパクト／低確率または、低インパクト／高確率にシフトしているなら、リスクが低いと思われる代替のサプライヤを使用するという別のルートもあるだろう。

学んだ教訓

IT を外部委託するという業務をしっかり進めるために、いくつかの教訓を肝に銘じておくべきである：

責任や説明義務は放棄することはできない。コンサルタントはサプライヤの選択過程やサプライヤを評価するのに、かなり価値のあるものを付加するが、結局、ビジネスは現地の IT から同じサービス、信頼性、リスクレベルを期待する。そして、IT は不十分な点に対し責任をもつことになる。

詳細な調査は実施されなければならない。サプライヤは、契約前と契約期間中の両方で監査される必要がある。効率を証明するために指標や報告書を要求する。サービスサプライヤの財務健全度に注意する。リスクレベルがまだ受け入れ可能であることを保証するために、重大な変更がクライアント側かまたはプロバイダーも含めて生じるときには、確認のためにも決められた変更管理プロセスを使う。

トレーニングやガバナンスによって、アウェアネスを確かなものにしておく必要がある。すべての現地の IT スタッフを削減できると仮定することは過ちである。実際には幾人かのスタッフ削減は可能であるが、外部委託に取り組むガバナンスやサプライヤも含めたプロジェクトの現地管理は、現地 IT の新しい責務になっているだろう。現地の IT スタッフを削減しすぎることは、結局、ヘルスケア業界内でのサービスサプライヤと不満足な顧客間に不仲な関係を生じさせる。

ヘルスケア企業は管理可能なリスクを減らす全ての機会を活用すべきである。同時に、効果的にまたは効率的にコントロールできないリスクがいくつかあることを理解しておく必要がある。これらの種々のリスクは、サプライヤによって経営管理者に委任されておく方が良いかもしれない。

外部委託で考えられる業務の本質は明確に理解され、分類され、記録される必要がある。リスクの許容範囲によっては、単純に他国に海外委託すべきでなく、場合によっては全く外部委託すべきでないといった物事があるかもしれない。どのような場合でもアクセスは仕事で必要とされるデータのみにすべきである。

要求や見込みは十分に記録されるべきである。ある活動が重要であるなら、契約書内にあった方がいいかもしれない。とはいっても、大規模な外部委託では、すべての必要事項が事前に同定されていることはありそうもないので、契約書内にある程度の柔軟性をもたせておくことを覚えておくことである。契約書の記載上、最大限の努力を求めているなら、サプライヤが必要とされる追加の努力ができないように網羅されていない何かが見つかったときには、よい機会となるだろう。

解決にむけてサプライヤと協力する。彼らは提供しているサービスの専門家であることを受容する。関係の価値を最大化するために、言われたことしかしない人ではなく、方向性を示せる指導者であることを期待する。

完了と移行時の留意事項を含める。すべての良い仕事には終わりがあり、定義された終了計画がなければ、関係が終わるときに大きな不安を引き起こすことになる。

内部のリスク

本稿では主に外部委託のパートナーを雇うことに関するリスクを取り扱ったが、外部委託する IT モデルを移行する際に企業が取り組まなければならない内部リスクも存在する。外部委託で追跡可能な内部リスクについて 3 例ここで挙げる。

- 外部のリソースを管理することは常に時間を浪費する。これはプロジェクトの経営資源の調節を要することになりかねない影響があるだろう。いくつかの場合にはサプライヤを訪問しなければならないかもしれない。さらに、IT が”古参の”スタッフを削減するなら顧客と IT サービスサプライヤ間の橋渡しを管理するために新しい役職が必要となるかもしれない。この新しい役職は IT の技術的な側面を基盤にもち、ビジネスの優先順位や必要性を理解しておかなければならない。
- スタッフの削減は結果的に現地の専門知識を失うこととなる。現地で一度取り組まれた出来事は今や外部のリソースとなる。特にサポートスタッフが異なった時間帯にいる場合にいえることだが、お役所的な仕事が増えそうである。問題を解決するために必要とされる余分な時間や労力の量は顧客の欲求不満というリスクになり、”shadow IT”の台頭を促し得る。

- ”shadow IT”は十分な脅威である。IT 部門によって実施されたプロジェクトが外部委託/海外委託により難航し始めたら、ビジネス管理者のところで中間業者を削減することや自身で解決する衝動が生じるだろう。これは、基準外の基盤、認知されていないサポートの要求、サポートされていないシステムへと先導していく可能性があり、データの完全性／機密性／可用性／アクセスのしやすさの点で更なるリスクを導く可能性がある。

結語

ありふれた IT 業務を外部委託または海外委託することによって実感する潜在的な有益さがある。そうだけれども、監視され、ある場合には緩和されなければならないリスクもつきまとう。もし、あなたがこのマントラを覚えておくなら、それほど間違えることはないだろう。

すべてはデータである。

肝心なことは製薬企業やバイオテクノロジー企業の最も大事な資産は情報であるということである。第三者のサービス供給者の手に情報を置くということは自動的にリスクのレベルを想定することとなる。そのリスクがどの程度のものかは、法律や政治的な要因に関連する国の問題、企業の問題、契約の問題、データやサプライヤによってされる仕事の性質によって決まる。

最後に、我々が規制当局側から常に思い出させられるように、ヘルスケア企業の名前を用いてなされるどのようなことも、つまるところ、クライアント企業の責任である。これは、5 つのリスク要因のうちの 1 つである、外部委託／海外委託プログラムのガバナンスにつながることである。

本文以上

＜図表の説明＞

図 1　すべてはデータである：だれがそれを有し、アクセスでき、どのように保護されているか？

図 2　ガバナンスは広範囲の責務を含んでいる

図 3　一般的にデータを保護している法律はリスクを緩和するものとなっている

図 4　リスクのシナリオと可能性のある対応

水色の枠内の訳

IT サービスは過去 10 年を経て便利なものとして見なされてきている。企業はビジネスのエネルギーとリソースを中核となる活動に集中させる方法を探しており、中核とならない活動の費用や労力を減らす方法として、しばしば国内や海外の外部のパートナーに頼ることとなる。ヘルスケアのように規制化された産業の重荷は、正しさを入手することに課題が増えていることである。