IT成熟度をどのように向上させるか

ＫＰＭＧビジネスアシュアランス株式会社
シニアコンサルタント
吉川 正弘

はじめに

ここでは、IT成熟度（※1）をどのように向上させていくか、つまりどのようにITリスクを認識し、予防／発見的なコントロールを設定／実施し、強化していくか、をテーマとする。筆者は、年間35社以上のクライアントに対してシステム監査を行っており、その経験から、どうすればスムーズかつ着実にIT成熟度を向上させられるかを、できるだけ具体例を交えながら解説していきたい。

1．IT成熟度を高めていくことの必要性

ITリスクには次のように多種多様なものが存在する。
（図－1参照）

・経営戦略に沿わないIT投資
・基幹システムダウン
・不正アクセスや顧客情報漏洩
・システムの開発遅れやコストオーバー
・プログラムバグ
・運用ミス

これらの事態が発生した場合、ビジネスに多大な影響を及ぼすものも少なくない。

例えば、経営戦略に沿わないIT投資を行ったことによる投資回収期間の長期化、基幹システムのダウンによる取引先への迷惑、顧客情報漏洩による顧客離れ、等が挙げられる。

自社で起こり得るITリスクとは何かを、全く把握していなければ、問題が表面化してから対応を行わざるを得ず、常に対応は後手に回ることになる。つまりどこに地雷が埋まっているか分からずに地雷原を歩いているようなもので、非常に危険な状況だと言える。

逆に、ITリスクの状況（どのようなことが起こり得るか、発生可能性、発生した場合のビジネスへの影響）を把握し、それぞれのリスクに対するコントロール（予防／発見等の措置）を構築しておけば、必要以上に恐れることはない。

コントロールの構築に関しては、成熟度の概念が非常に参考になる。

コントロール成熟度の例として、ここでは、COBIT（※2）の6段階（レベル5～0）の成熟度を挙げる。

・レベル5：最適化されている
　標準プロセスを改善･改良し、常に最適化された状態を維持している
・レベル4：管理されている
　定義された標準プロセスに従って業務が進められているかモニタリングしている（また、その体制がある）
・レベル3：定義されている
　標準プロセスがきちんと定義され、組織としてそれを認証している
・レベル2：反復可能
　標準プロセスがあり、ほとんどがそのプロセスに従って業務をこなしているが、遵守は個人に依存している
・レベル1：初歩的
　場当たり的な対処
・レベル0：存在しない
　ルールや問題についての認識がない

ここで留意すべき概念として、「IT成熟度の広がり」が挙げられる。IT成熟度の広がりには、縦の広がり、横の広がりがあり、それぞれ次のようになる。

縦の広がり：ITにとどまらない全社的なコントロールの向上（経営の成熟度の向上）、更には、社会のIT成熟度の向上（高度IT活用社会の実現）に繋がっていくこと。

横の広がり：自社単独ではなく、ソフトハウスや社外データ／運用センターといった、IT開発･運用の委託先、グループ企業等との協働に繋がっていくこと。

従って、IT成熟度の向上を検討する際には、ITコントロール、もしくは自社の問題、としてだけ捉えるのではなく、IT以外、自社以外への影響を検討する必要がある。

それでは、IT成熟度を如何に向上させていくべきなのであろうか。

2．IT成熟度向上の手順

IT成熟度向上のための手順は、次のサイクルを回していくことである。（図－2参照）

①現状の把握、②ITリスクの洗い出しと評価、
③改善策の策定、④改善策実施、
⑤フォローアップ（改善策の評価）

確実にこれらの手順を進めていくためにも、①～⑤のステップごとに責任者および実施期限を定め、それぞれのステップ終了時には、成果物をきちんと文書で残しておく必要がある。

それぞれのステップ終了時の成果物としては、例えば次のようなものが挙げられる。

①あるべきコントロールと現状の対比表
②ITリスク一覧表（緊急性、重要度等により評価を行ったも

の）
③改善策の実施計画書
④関係者への実施説明資料、整備した規程類
⑤改善策の評価報告書

次に、これらステップについて、留意点を解説する。実施にあたっては、必要に応じて専門家の助力を仰ぐのが望ましいことが多い。

（1）現状の把握

現状を把握するには、例えば情報システム部門の体制や、システムの開発手順といったITプロセスに関する何らかのフレームワークを使用するのが望ましい。フレームワークを使用することにより、検討漏れや、偏りを防止し、また、自社の全体状況を一覧できる、というメリットがある。

フレームワークの中には、コントロール目標（あるべき姿）が設定されており、コントロール目標と比べて現状がどうなっているかを確認できるようになっているものもあり、ITライフサイクル全般を網羅的に捉えているものを利用すべきである。例えば先出のCOBITでは、4つの管理プロセスの中で34のITプロセスを評価するフレームワークとなっている。

現状の把握は通常、組織図や開発手順、資産管理規程等の文書類の査閲、関係者（主にシステム部門）への質問表の送付やヒアリング、ハードウェアの設置場所や利用部門への視察等を通じて実施する。

（2）ITリスクの洗い出しと評価

現状を把握した後で、コントロール目標とのギャップを整理し、ITリスクの洗い出しを行う。ここで留意すべきは、ギャップが即、ITリスクとならない点である。ギャップは原因であり、ギャップから発生するITリスク（問題、結果）を把握することが重要になる。

例えば、採用したフレームワークで、システム部門の体制についてのコントロール目標の1つが、「システム部門は利用部門から独立していること」となっており、現状では、システム部門はなく、システム課が経理部門の下にあったとする。

ここでの問題を、「システム部門（課）が利用部門から独立していないこと」、としてしまうと、改善策は「システム部門を独立させること」となる。通常、組織改編はシステム部門だけではなく、全社的なバランスの基に実施されるものであり、組織戦略、人事戦略に係るため、すぐに何らかの手を打つのは難しい場合が多く、このままでは有効なコントロールの設定が難しい。

ここで重要なことは、「システム部門が利用部門から独立していないこと」自体は問題ではなく、現状（あるべき姿とのギャップ）であって、それによりどのような問題（ITリスク）が引き起こされるかを検討する必要があることである。

「システム部門が利用部門から独立していないこと」による問題点は、会社によって異なってくるものと思われるが、例えば次のようなものが挙げられる。

①利用部門の指示により、直接データの（不正）操作を行ったり、データ修正を行うプログラムの提供を行ったりしてしまう。
②システム部門直属の利用部門に便宜を図るようなシステム開発やシステム変更を行う（システムの全体最適化が図られない）。

このように、現状からどのような問題点が引き起こされる可能性があるかを検討することが必要である。

ITリスクの洗い出しについて、もう一つ例を挙げる。

採用したフレームワークで、システム運用のコントロール目標の1つが「利用部門の業務運用マニュアルを整備すること」となっているが、現状では業務運用マニュアルがなく、運用が担当者に依存していたとする。

ここでの問題は、やはり業務運用マニュアルが整備されていないことそれ自体ではない。「業務運用マニュアルが整備されていないこと」としてしまうと、改善策は、「業務マニュアルを整備すること」となる。しかし、現状では問題なく運用が行われている、とシステム部門が認識していれば、業務運用マニュアルの整備への着手には抵抗感が強い。

「業務運用マニュアルが整備されていないこと」が引き起こすと考えられる問題点には、例えば次のようなものが挙げられる。

①オペレーションが利用部門のオペレータに依拠されることで、処理の均一化がしづらい（継続性の保持が困難）こと（特にデータ修正等のイレギュラー処理において、この傾向は顕著である）。
②急な要員交代時の引継ぎが困難なこと

①について例を挙げる。例えば、会計システムであれば、先月入力･確定したデータに誤りが見つかった際のデータ修正の対応時には、次のような事項を判断する必要がある。

・誤った伝票取消のために、金額をマイナスした仕訳を入力するのか
・誤った伝票取消のために、貸借逆の仕訳を入力するのか
・それらの仕訳を入力する際に、また修正した伝票を同時に（セットで）登録するのか
・修正時の伝票番号をどのように採番するか
・修正時の伝票の摘要欄に何を記載するか

これらの事項に関して、オペレータごとに処理が異なっていては、処理の妥当性の検証がしづらく、処理が誤っていても検出されない可能性がある。

このように、あるべき姿とのギャップから、具体的にどのような問題が発生するかを把握するのがITリスクの洗い出しである。

具体的なITリスクの洗い出しの後、各ITリスクを発生可能性（頻度）、発生した場合のインパクト（影響度）で評価し、取り組むべきITリスクの優先順位付けを行う。

（3）改善策の策定

（2）のITリスクの洗い出しにより、具体的な問題点が明確になっていれば、改善策の策定はそれほど難しくはない。

例えば（2）の「システム部門が利用部門から独立していないこと」で挙げた問題点①や②に対して、やはりもっとも望ま

しい改善策は、「システム部門（課）の独立」となる。しかし、それが難しいとなれば、次善の策として次のようなものが考えられる。

・利用部門からシステム課に対して、データ操作の指示が行われていないかどうかを、独立した部門（内部監査部門等）が定期的に確認する
・システム変更の意思決定がシステム課の直属の利用部門により影響を受けていないかの調査を行う
・運用規程、開発規程等に、他部門の指示による（不正）データ操作の禁止や、特定の利用部門に便宜を図ったシステム開発を禁止するといった条項を盛り込み、周知する。

これらの手続を設定することで、不正の予防、発見可能性を高め、さらにシステム課とその直属の利用部門に対する牽制機能を持たせることができる。

また、(2) で挙げた「利用部門の業務運用マニュアルが整備されていないこと」については、オペレータが処理方法を迷ったり、実際に処理方法が異なったりしているようなイレギュラーケースを中心に、重要性の高いシステムから、対応を文書化（最初はメモ書き程度でも良い）していくのが現実的である。最初から全体を作成するのではなく、重要度の高い部分から文書化を進め、徐々に完成度を高めていけば良い。

このように問題点が明確であれば、改善策も現実的かつ具体的に設定することが可能となる。

新たなコントロール（改善策）を策定する際には、次の3点に留意すると良い。

1点目は、改善策の実施には、人／時間／費用といった経営資源を投入する必要があるため、効果的かつ効率的なものを選択する必要があることである。

コントロールには、予防的コントロール、発見的コントロールがあり、一般的に予防的コントロールのほうがコスト高となる。

上記の例でいえば、システム部門を独立させたり（つまり組織上、不正データ操作を行う指示そのものを出せなくする）、規程類を整備したりすることが予防的コントロールであり、他部門により不正が行われていないかどうかを確認するのが発見的コントロールである。

なお、コントロールは、効果的で、ITリスクに緊急性があるものから設定すべきであるため、(2) で洗い出したリスクの重要性もしくは発生頻度が低い場合やコントロールの設定に多大なコストがかかる場合は、リスクの最適化という観点からは、「何もしない」という選択もあり得る（例えば、火災や地震対策として、重要性の低いシステムに対しては、システムの二重化といった施策を行わない、等）。

2点目は、改善策の策定の際には、教科書的なものではなく、実現可能なものを選択していくことである。最初から満点を目指すのではなく、徐々にコントロールを強化（成熟度の向上）を図っていけば良い。

(2) で具体的な問題点が明らかになっており、問題点が発生した場合の影響を説明できれば、比較的現場の抵抗も少なくなり、協力を取り付けやすくなる。また、説明の際には、ITリスク発生の原因を特定部門の責任としないよう、表現に注意を払うことも重要である。

3点目は、関係者ごとのITに関する責任を考慮した上で、どの関係者にコントロールを設定するのかを検討することである。（図－3参照）

(1)～(3) をより深く理解していただくために、現状、問題点、改善策をまとめた他の例を用意したので、参考にされたい。（図―4参照）

（4）改善策実施

改善策の実施にあたっては、責任者と期限を定め、必要があれば関連部署（場合によっては委託先や関係会社等、社外も含む）と協働しながら実施することが重要である。

実施の際には、実施が適切に行われたか、効果的かを確認するために、フォローアップの周期を定めることが望ましい。

また関連部署と一緒に検討する際には、実施メリットと、実施しない場合のリスクをよく吟味、理解しながら、合意を形成しつつ進めていくことが必要となる。

例えば、システムアクセスに関して、次のような検討を行い、改善策を決定したとする。

コントロール目標：利用部門で不要なユーザ、及び権限の定期的な確認は行うこと

現状：利用部門で不要なユーザ、及び権限の定期的な確認を行っていない

問題点：①退職者や異動者のユーザIDが不正使用される可能性がある、②適切な権限ではなく、以前の権限のままでの使用が行われる可能性がある

改善策：ユーザIDおよびユーザIDごとの権限一覧を各利用部門に配布し、適切な権限設定となっていることを定期的に（半期に一度程度）確認させ、利用部門長の承認の上で、システム管理部門に提出させる

改善策のスムーズな実施のために、関連部門に対しては、現状と問題点を説明し、なぜそのような取組を行う必要があるかを理解してもらう必要がある。上記の例では、システム部門だけではユーザIDとそれぞれの権限の把握は難しいこと、ユーザIDが不正使用された場合、被害が甚大だと予想されること、を訴えると良い。このように問題点が具体的に整理されていれば、比較的関連部門の協力は得やすい。

（5）フォローアップ（改善策の評価）

(4) で決定したタイミングで、フォローアップ（改善策の評価）を行う。

実際には設定したコントロールが有効に機能し、運用されているかを、関係者へのヒアリングや関連資料のサンプリングチェック等を行い、確認する。予定通りの成果をあげていない場合は、コントロールの改善を行っていくこととなる。

おわりに

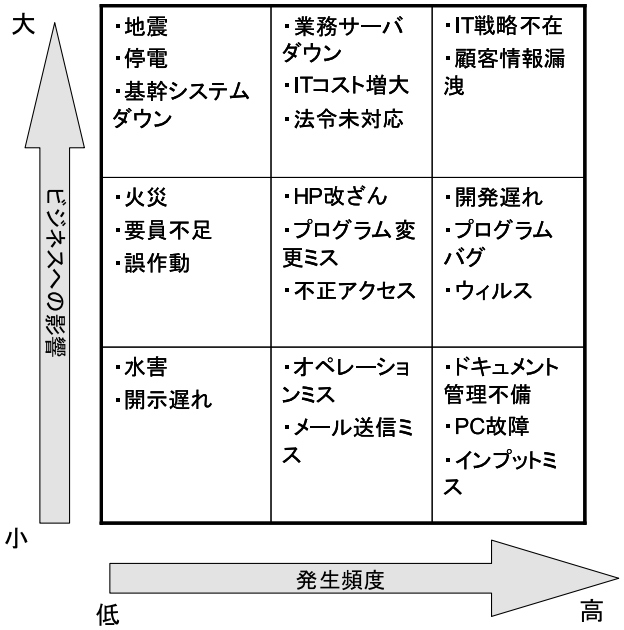
ここまで、IT成熟度をどのように向上させていくか、その際の留意点は何かを、筆者の経験を交えて解説してきた。

最も大切なことは、まず起こり得るITリスク自体を認識すること、そして、限られた経営資源の中で、無理なく（徐々に）IT成熟度を高めていくよう、常に改善を行っていく姿勢である。

（注1）：IT技術の利用度合、ネットビジネスの浸透度、ブロードバンドの普及率、等を意味する場合もあるが、ここで言う「IT成熟度」は、「ITリスク管理の成熟度（ITコントロールの進展度合）」のことである。

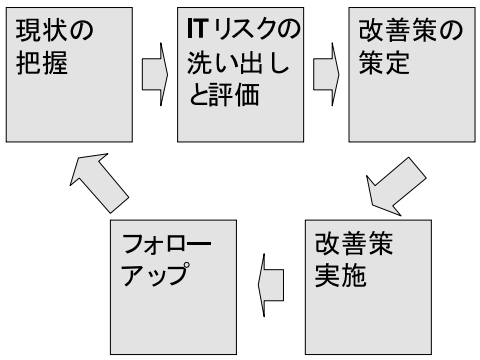
（注2）：Control Objectives for Information and related Technology。米国の情報システムコントロール協会（ISACA：Information Systems Audit and Control Association）が提唱するITガバナンスの成熟度を測るフレームワーク。

図－1. ITリスクの例



出典：「ITリスクと会計情報―ビジネスインパクトアナリシス 中央青山監査法人」の抜粋を一部改訂

図－2. IT成熟度向上のための手順



上記サイクルを回していくことが必要

図－3. 関係者ごとのIT責任とコントロールへの取組

関係者	IT責任	コントロールへの取組
経営者	投資家への情報信頼性の説明、投資妥当性判断	投資判断、モニタリング
IT担当役員（CIO）	IT戦略 計画立案、戦略適合性判断	設計、モニタリング
IT部門（情報部門）	システム開発、システムの可用性保証、サポート	設計、機能組込、教育
利用部門管理者	業務遂行の監督、承認	教育、監督、モニタリング
利用部門担当者	業務の正確な遂行	実施
監査人	信頼性の確認	評価、指導

図－4. 現状、問題点、改善策例①

プロセス	現状	問題点	改善策
システム開発全体	・システム開発の規約等は、作成していない。 ・プログラミングのコーディングルールに関しても、特に文書化してはいない。	・開発が属人的になり、システムの品質にばらつきが出る。また、コーディングが担当者によって様々であるため、後でメンテナンスする際の効率悪化にも繋がる可能性がある。	・開発、コーディング規約を作成することが望ましい。まずは、判断に迷うような箇所、クリティカルなポイントだけでも最低限文書化し、徐々に充実させていくのが良いと思われる。
システム開発・テスト	・システム開発の各段階において、管理者もしくはユーザによるレビューを実施しているが、承認／確認結果を文書化して残してはいない。	・テスト結果を文書化していないので、テスト実施の有無／問題の有無の結果が残らない。 ・テストの効果／効率を分析できず、次回以降のテストにフィードバックができない。	・まずは、テスト結果および進捗状況を記載／管理（承認）するシートを作成してテスト時に利用する等、なるべく負荷のかからない方法で、文書を残していくのが良いと思われる。

図－4. 現状、問題点、改善策例②

プロセス	現状	問題点	改善策
システム運用アクセス管理（権限管理）	・会社には、販売、人事給与、会計システムがあり、システム課員はサポートやメンテナンスのため、全システムの照会／操作ができる。操作履歴は取っており、誰がどの操作をしたかは分かる。	・システム課では、非常に秘匿性の高い、人事給与情報の照会／操作ができる状況である。 （注意：操作履歴を取っており、誰がどの操作をしたかが分かるので、不正操作の可能性は低い。）	・サポートやメンテナンスの利便性を損ねないようにする必要はあるが、システム課でも、職務権限に応じたアクセス制限を行うべきである。（例：人事給与は、テスト環境のみアクセス可能とし、本番データを見る際は人事部内で行う等）
システム保守障害管理	・オペレーション中に発生したトラブルは、「システム運用管理簿」（一年間保管）に記載するが、ユーザから報告されるトラブルや回線エラーなどのトラブルについては、特に管理簿を作成していない。	・ユーザから報告されるトラブルの記録を取っておらず、対応の漏れが生じたり、同じトラブルを別トラブルとして対応する可能性がある。また、トラブル発生の傾向が分析できず、報告が改善に役立てられない。	・簡単な記録が取れるよう、フォーマットを作成し、全報告に対して残すようにするのが望ましい。（記載するのは、発生日時、発生部署、内容、対応者、結末、上長の確認、程度）