法とシステム監査研究プロジェクト

独立研究者　多和田肇

研究プロジェクトの概要

- 主査 稲垣 隆一、副主査 黒澤 兵夫
- 概要 システム監査は、情報システムの企画、開発、運用、保守に関する現実的な課題の予防、解決に、いかに役立つのか？ レピュテーションリスク、クラウドコンピューティング、ソーシャルネットワーク、ビッグデータの取扱い、マイナンバー制度、IOT/IOEシステム、サイバーアタックなど現下の課題、判決例に表れた紛争事例を素材に検討し、その成果を生み出すシステム監査の技法の開発、管理基準の改訂の提案などに結びつける。

２０１８年度参加メンバー

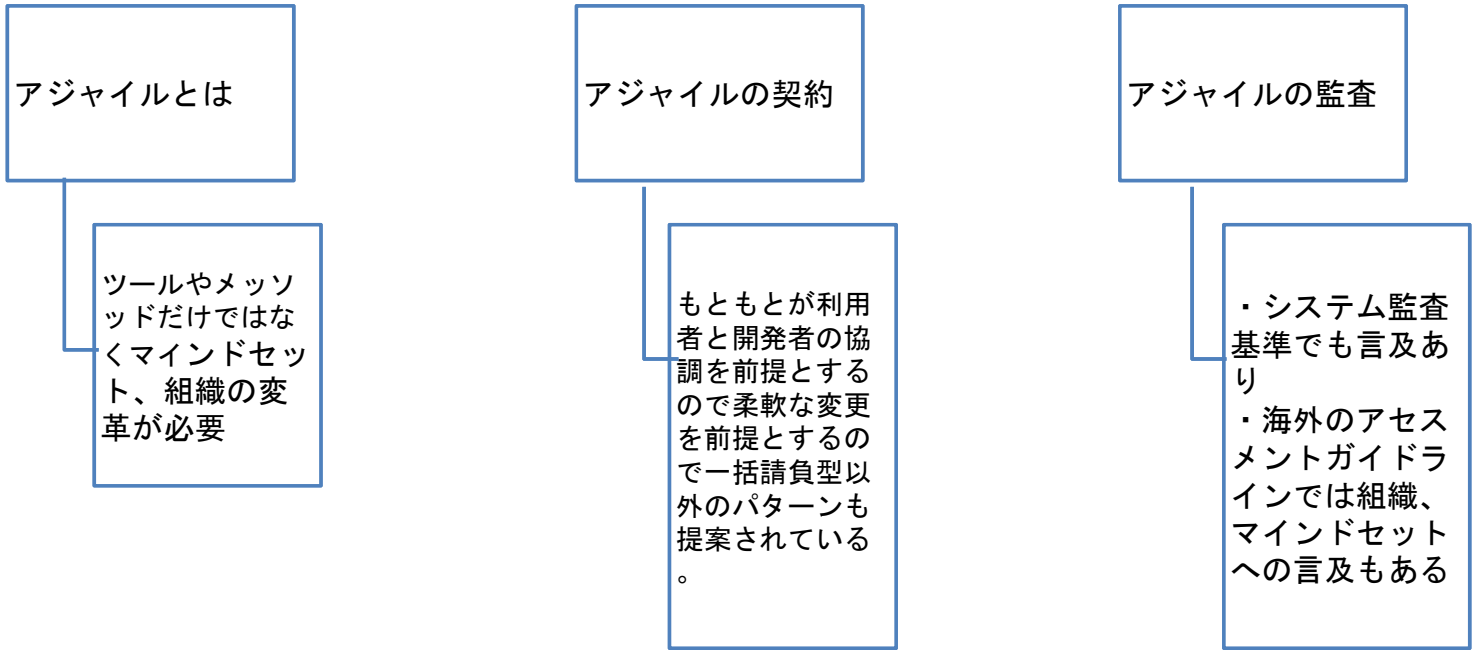
荒木 哲郎	弁護士・システム監査技術者
稲垣 隆一（主査）	稲垣隆一法律事務所・弁護士
黒澤 兵夫（副主査）	TAKE国際技術士研究所
成田 和弘	システム監査技術者,CIA,CISA
芳仲 宏	システム監査技術者
多和田 肇（発表者）	システム監査技術者,CIA,CISA

１．本日の報告の概要と目的

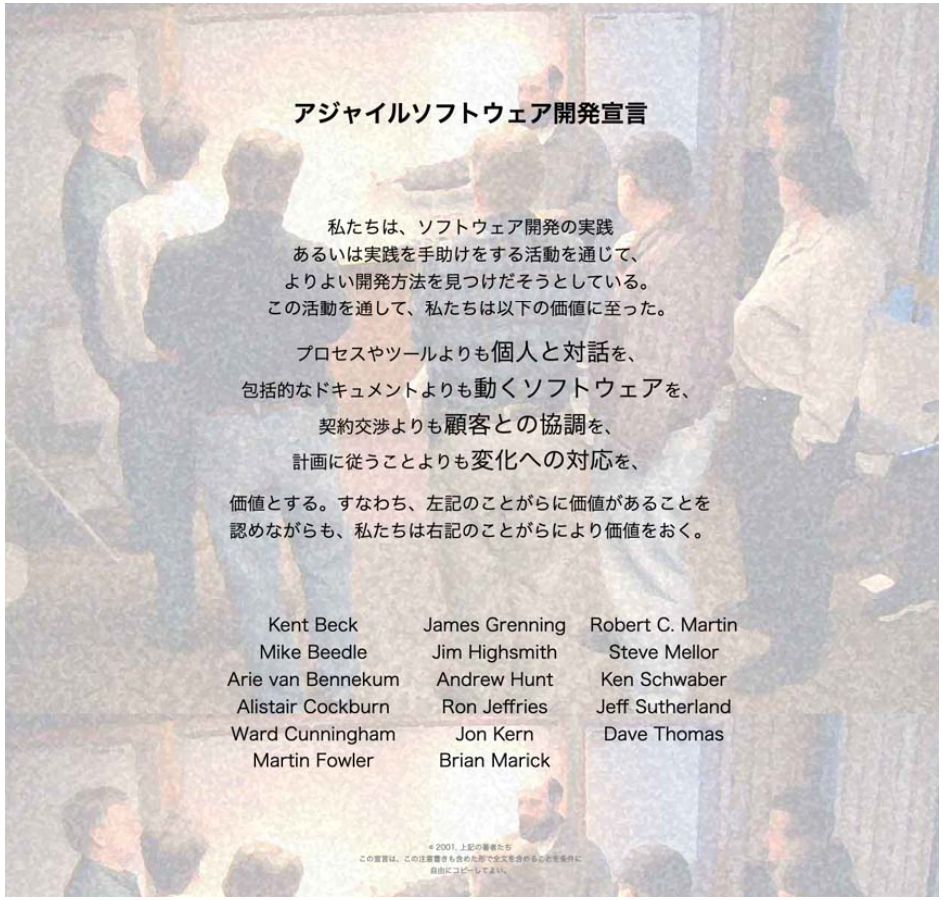
今年度の研究プロジェクトではアジャイル開発について、手法、契約、監査について研究した。その内容について、紹介するとともに、実際にプロジェクトを監査する上での参考情報を提供する。

研究会での実施内容
・アジャイル開発について（アジャイル宣言等）
・アジャイル開発の実例（雑誌記事等の紹介）
・アジャイル開発の契約（論文紹介等）
・監査について（システム管理基準および外国のガイドラインの紹介）
など

ご説明の構成図

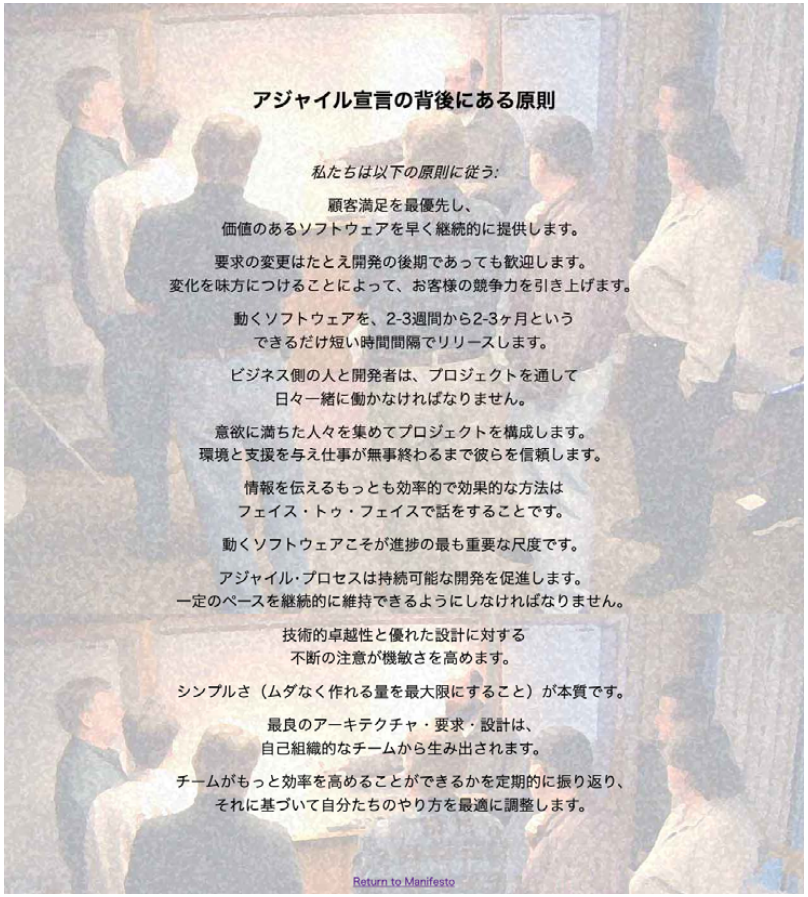


２．アジャイル開発の概念



https://agilemanifesto.org/iso/ja/manifesto.html（２０１９年５月６日閲覧）

２．アジャイル開発の概念（続き）



https://agilemanifesto.org/iso/ja/principles.html（２０１９年５月６日閲覧）

３．アジャイル開発が求められている背景

アジャイル開発が求められている背景について（システム監査学会の定例研究会（２０１２年９月２１日開催）から）

・ウォーターフォール型開発プロセスの問題点

「要件定義」は要求を定義しきれない

など

・情報システムサイクルとソフトウエアサイクル

施主は「原要求」を提出し、設計者は要求の設計を行う。それを受けて施工者は製造すべきであるが、現在は施工者中心のソフトウエアサイクルしか回っていない。施工者は個別の要求があれば作ってしまうことに問題がある。

・システムを例えば2年後の予想のもとに開発して、マーケットが予想通りということはまずない。そのため追加変更がでてくる。大切なのはマーケットの状況に応じてリリースできること。それができるのがアジャイル開発である。

.

３．アジャイル開発が求められている背景（続き）

アジャイル開発とは

「少しずつ作って大きく育てる」戦略をとり、要求変更に柔軟に応える。また、要求設計の段階で、システムの中核部分を間違いなく実装できることを確認する。

課題

・発注側の問題

請負の意識が払拭できない。瑕疵担保責任に拘る。協調よりも交渉を重視。要件定義が曖昧でも何とかしてもらえると考えてる、会社としてシステム要件を決定する仕組みができていない。業務上の課題をシステム問題と認識してしまう。最終的にシステム開発リスクを負うのは発注側との基本認識がない。

・受注側の問題

請負の意識が払拭できない。原則を逸脱する要求を拒否できず、営業対応に頼ろうとする。顧客のビジネスで成功のために必要となる、真のシステム要求に関心がない。システム要求に柔軟に対応できるだけの技術力や対応力がなく、個別開発要求に振り回されてしまう。アジャイルに計画は不要と勘違いしている。

.

３．アジャイル開発が求められている背景（続き）

本日の発表の中でアジャイル開発というときは、必ずしも特定の手法を前提とするわけではなく、”いわゆる”アジャイルと考えられるものを含めている。したがってそもそもそれはアジャイル開発と呼ぶべきか、という議論ではなく、”アジャイル”と呼ばれるものについて、そのプロジェクトが問題を起こさないこと、また起こった際にシステム監査が役立つように、という観点からの発表であることをご理解いただきたい。

.

４．アジャイル開発の例

・チタンメーカーのA社の例
要件を固めきれないが納期は厳守という難題プロジェ クトをアジャイル開発手法を使って乗り切った。同社にとって初めて挑む新しい開発手法だった が、ユーザー部門のキーマンをプロジェクトに固定させたり、プロジェクトの途中でもアジャイル開発向きでない開発者を交代させるなどして完遂した。<日経コンピュータ2009年1月15日号掲載>
２年間で３億円規模の新工場向けの生産管理システムの開発

特に重要と感じた内容
・アジャイルだけのコンサルタントを開発ベンダーとは別に起用した
・発注側がシステム開発に理解があり、１担当者ではなく、工程をよく知るGMをプロジェクトルームに常駐させた
・１回めのイテレーションを終わり、アジャイル向きでないメンバーを２名（全８人のチーム中）交代させた＊
・（最後のA社常務のコメント）

「優秀でアジャイル開発に合った人材をどこまで集められるか が成功のカギ。アジャイル開発はすべてには適用できない」

＊アジャイル向きでないことがプログラマー、SEとしてのスキル全ての評価という意味ではない。
プロジェクトについても向いていないものがあるのと同様である（発表者）

４．アジャイル開発の例（続き）

・ＩＴ企業B社の例
B社はインターネット通販基盤からスタートして現在ではさまざまなインターネットサービス（金融含む）を提供する会社

特に重要と感じた内容
・変化が激しい環境に置かれているので、アジャイルで素早く開発しリリースすることことが事業の利益と密接に結びついている。そのため経営としてもアジャイル開発を受け入れる必要性の認識が強いと思われる
・開発の基盤が整備されていてＩＴ化されている。プロジェクト管理にもツールが導入されている。そのため、アジャイルを使って開発するメリットを開発者自身が実感できる
・インハウスの開発者の育成にも力をいれている

・自社のサービスとアプリが密接につながっているので、フィードバックも早期に得て修正する

ことができる

４．アジャイル開発の例（続き）

・うまくいかない事例
日経システム２０１０年１２月１０日付（
https://tech.nikkeibp.co.jp/it/article/COLUMN/20101215/355244/（２０１９年５月６日閲覧）（「覆面座談会」はびこる失敗アジャイルでの話題から）
・イテレーションの失敗
要求通りのものが最初のイテレーションでできあがらないことにユーザ側のメンバーが怒り出してしまい、２回目でも設計が思ったように進まず、頓挫
・ドキュメントについて
必要以上のドキュメントの作成を行い、ユーザー側が負荷の多さに頓挫
・ペアプログラミング
全く知らない人が組み、お互いが批判をしあってトラブル
・プロジェクトマネジメント
従来のガントチャートやWBSがないことによるPMの不慣れ
・契約の問題
一括請負開発する場合、受注側はリスクを見込むのでウォーターフォール型の開発より高い見積もり金額になってしまう

５．アジャイル開発と契約

・米国の契約パターンは次の通りとのこと（今回の報告は吉田知加（筑波大学大学院ビジネス科学研究科 企業科学専攻（執筆当時）「アジャイル開発の見積りと契約モデルに関する研究」（２０１５年、審査学位論文（博士））によっている（一部改変）。この分類は独立行政法人情報処理推進機構ソフトウェア・エンジニアリング・センター「非ウォーターフォール型開発 WG 活動報告書」（２０１１年）１１４ページと同じ）

	契約種類	特徴	リスク（受注者）	リスク（発注者）
定額型契約	完全定額契約	標準的定額。定義された作業を定額で実施		○
	経済価格調整を含む定額契約	賃金の変動などの価格調整を含む定額契約		○
	際調整可能な定額契約	受注者の現在の業績で今後の価格調整可能		○
	インセンティブ付き定額契約	コスト超過の場合は受注者負担、未満の場合は発注者と受注者が契約で定められた比率で配分		○
	報奨付き定額契約	性能品質により追加報奨を受け取る		○
実費償還型契約	確定報酬付き実費償還契約	契約価格＝確定報酬＋受注者のコスト	○	
	報酬付き実費償還契約	予定コストと実際のコストの差分を分配負担	○	△
	成功報酬付き実費償還契約	定められた条件で成功報酬を（確定報酬＋受注者側コスト）に加えて受け取る	○	
	CostCntract	受注者は報酬はなく、コストだけを受け取る	○	
	CostShareing	受注者のコストの一部を発注者が負担する	○	
間接作業型契約（完遂は前提としない）	Time and Material Level of Effort Term)	プロジェクトの構成要員に必要なスキルと必要時間が定義され、時間当たりのスキルごとの金額を掛け合わせた金額を受け取る	○	
	Fixed Price Level of Term(FFP-LET)	小規模な開発プロジェクトで一定期間、一定作業に対して最初から決まった金額を受け取るだけ	○	
	Cost Plus Fee Term	FFP-LETに報酬が加わる	○	

５．アジャイル開発と契約（続き）

・日本における最近の契約の整理について（富士通社の整理による。
https://www.fujitsu.com/jp/services/knowledge-integration/insights/201805-05/（２０１９年５月５日閲覧））

アジャイル開発に多い契約形態の例

契約形態例	概要	利点	留意点
準委任契約 ・タイム&マテリアル（T&M）	事前に単金、期間、上限金額などを決め、実際にベンダー側が稼働した分だけ支払う	・チームの一体感を醸成しやすい。 ・事業価値、ユーザー価値にフォーカスしやすい ・仮説の改善、変更を素早くできる	・成果を出すためには同じ場所で共に働くことが重要となるため、企業の負担は大きい ・成果物の完成責任は発注者(企業)側が負う必要がある準委任契約 ・善管注意義務に違反するかどうかの判断が難しい
準委任契約 ・定額	1~3カ月単位で定額の準委任契約を繰り返し、双方のリスクを低減していく	T&Mは、見積もりよりも実稼働は少ないケースも多く、コストを抑えやすい反面、稼働の予実管理などの対応も必要。定額の場合、予算と期間を固定できるので予算申請などの社内調整がしやすい。企業の予算管理制度への対応など、社内調整のしやすさなどで使い分けるケースが多い	
準委任と請負のハイブリッド ・請負→準委任	初期仮説の検証のために最小限作ってほしい機能を請負契約に、以降、試行錯誤を繰り返すフェーズを準委任契約に切り替える	・初期フェーズの成果物の完成責任はベンダーが負う ・初期フェーズでベンダーの実力を測れるため、準委任への切り替えは比較的やりやすい	・初期フェーズの仕様があいまいなケースには向かない ・必要最小限の機能の見極めを慎重に行わなければ、作りこみ過ぎて無駄な機能を作ってしまうことになりかねない
準委任と請負のハイブリッド ・準委任→請負	初期フェーズを準委任、作るべきものがある程度見えてきた段階から、イテレーション毎やサブ機能毎に請負契約に切り替える	・請負契約の範囲に入る成果物の完成責任はベンダーが負う ・従来型の契約形態に近いため、社内関係者の合意を得やすい	・請負契約時は、仮説の改善、変更のスピードが落ちるため、試行錯誤を多く繰り返すケースには向かない。期間やサブ機能を小さな単位に分割することが難しいケースでは、変動要素が大きくなるためコストが積み上がる可能性がある ・契約手続きが煩雑にならないように工夫する必要がある

５．アジャイル開発と契約（続き）

・日本における最近の契約の整理について（富士通社の整理による。
https://www.fujitsu.com/jp/services/knowledge-integration/insights/201805-05/（２０１９年５月５日閲覧））

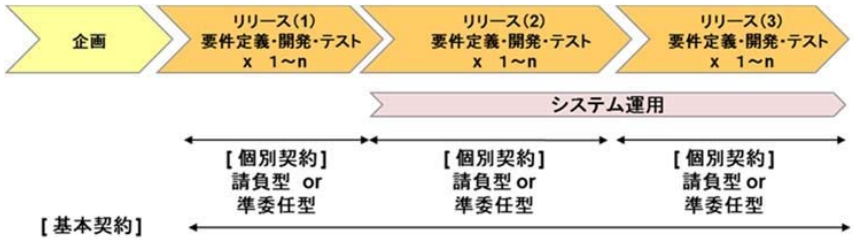
リスクと利益を共有するレベニューシェア型の契約形態の例

契約形態例	概要	利点	留意点
従量課金（SaaS、API等）モデル	プロダクト部分をベンダーが初期費用ゼロで構築し、本稼働の際に企業の利用量などに応じて課金される	・事業価値、ユーザー価値にフォーカスしやすい ・初期投資を抑えることができる（小さく始めることが容易） ・同社の分担などを比較的容易に決められる	・仕様変更の受け入れ判断がベンダー側にある場合も多く、必ずしも企業の要求が全て通るとは限らない ・ソフトウェア資産はベンダーの所有物となるケースも多い
成果報酬モデル	事前に定めた獲得ユーザー数や会員、アクティベーション率の指標に応じて、支払が発生する	・チームの一体感が醸成され、事業価値、ユーザー価値にフォーカスできる ・仮説の改善、変更を素早くできる ・初期投資を抑えることができる（小さく始めることが容易）	・売上に対する報酬の算出方法や分配率、知的財産権の取り決めなど、同社の役割分担や貢献度の測定が難しいケースも多い ・企業はベンダーに経営数値（獲得ユーザー数や会員、アクティベーション率など）を開示し、また監査を受け入れる必要がある
ジョイントベンチャーモデル	企業とベンダーが共同でジョイントベンチャーを作り、成果から得られた収益（株価）を分配する	・連合共同体としてチームの一体感が醸成され、事業価値、ユーザー価値にフォーカスできる ・仮説の改善、変更を素早くでき、短期間で成果につながりやすい ・新しいこと、前例のないことに挑戦しやすい	・制度設計、同社の分担など、合弁会社設立の準備が必要になる ・参加企業それぞれの意向を確認しながら進めていく場合は、意思決定のスピードが遅くなるケースもある

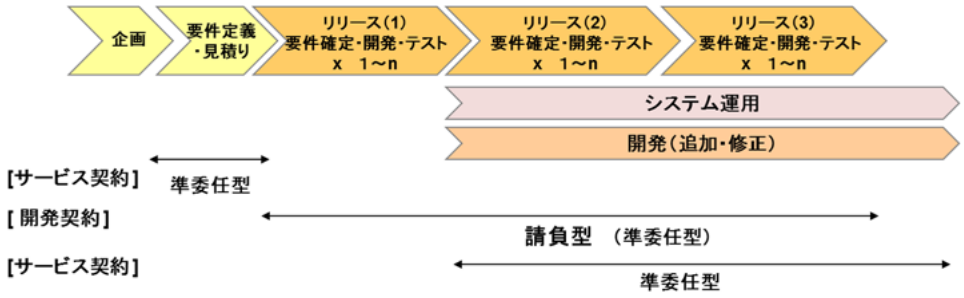
５．アジャイル開発と契約（続き）

・吉田氏の論文では、アジャイルの見積もりの精度をあげることでの解決。および、前ページのイテレーションごとの請負契約にサービス契約を追加して、イテレーションごとの見積もり負担を軽減するモデルを提案している。
・「実務家からのフォードバックを得ることは次の課題」、と論文で述べているので、実際にこのようなモデルを適用したことはない。

IPAのモデル



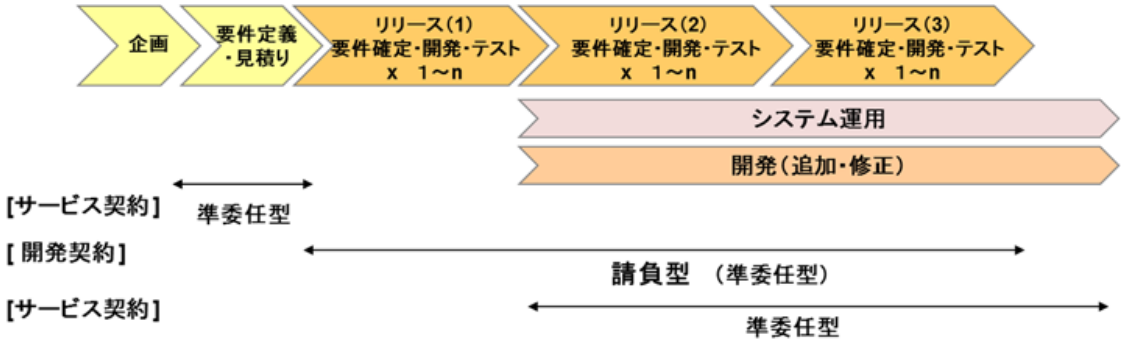
吉田氏のモデル



５．アジャイル開発と契約（続き）

吉田氏のモデルはサービス契約であるが、近年パッケージソフトなどで行われているサブスクリプション契約もアジャル開発には適合するアプリケーションもあるのではないかと考えている。

吉田氏のモデル



アジャイル開発アプリケーション

開発者側：開発後も権利を保有

利用者側：利用価値に見合った金額でサブスクリプションにより利用

６．アジャイル開発と監査

・アジャイル開発においてはドキュメントがないので監査ができない、ということがいわれることがある。これは日本だけではなく米国などでも同様であるようである。これについてシステム監査基準は次のように述べている。

【基準３】システム監査に対するニーズの把握と品質の確保
《解釈指針》２．システム監査のニーズに応じて、公表されている各種基準・ガイドライン等を適切に選択し、必要に応じて組み合わせて、判断尺度とすることが望ましい。システム監査上の判断尺度を確定する際の客観的な参照基準として、「システム管理基準」及び「情報セキュリティ管理基準」が推奨される。

６．アジャイル開発と監査（続き）

III．システム監査計画策定に係る基準【基準６】監査計画策定の全般的留意事項

《解釈指針》１．(4) アジャイル開発手法は、開発部門と利用部門の協調によって迅速かつ柔軟な反復的･継続的開発をすることが本来の意義である。（中略）アジャイル開発手法の本来の意義を損なわないように留意しつつ、監査実施のタイミング、サイクル、作業負荷、及び監査証拠の範囲･種類などを特定して計画を立案する。

６．アジャイル開発と監査（続き）

Ⅳ．システム監査実施に係る基準【基準８】監査証拠の入手と評価システム

４．アジャイル手法を用いたシステム開発プロジェクトなど、精緻な管理ドキュメントの作成に重きが置かれない場合は、監査証拠の入手において、以下のような事項を考慮することが望ましい。（以下抜粋）

（１）自動化ツールを用いて、監査証拠を入手したりするなど、アジャイル手法を用いる開発現場に、監査対応のためだけのドキュメント作成に追加的な負荷をかけないような考慮が望ましい。

（２）（自動化されたツールからの証拠を得るときのツールについての注意点）

（３）必ずしも管理用ドキュメントとしての体裁が整っていなくとも監査証拠として利用できる場合があることに留意する。例えばホワイトボードに記載されたスケッチの画像データや開発現場で作成された付箋紙などが挙げられる。

（４）必要となる監査証拠を適時に入手するためには、開発の関係者間の意思疎通を図る情報共有、コミュニケーションの仕組み、ルールが公式化され、常に適切に実践されていることを確認することが重要である

６．アジャイルと監査（海外）（続き）

海外の事例としてUnited States Government Accountability Officeの”SOFTWARE DEVELOPMENT Effective Practices and Federal Challenges in Applying Agile Methods”(2012)(https://www.gao.gov/assets/600/593091.pdf)から引用（私訳）。

評価

評価はプロジェクトおよび組織レベルで行われます。 たとえば、プロジェクトレベルでは、イテレーションは完了時にふりかえりとして見直されます。 組織レベルでは、アプローチを改善する機会についてプロセスがレビューされます。次の7つのプラクティスは評価としてあげられます。

•ステークホルダー/顧客からのフィードバックを頻繁かつ綿密に入手する。 このプラクティスは、リスクの軽減、顧客のコミットメントの向上、および技術スタッフのモチベーションの向上につながりました。

•プロジェクトレベルと組織レベルの両方でアジャイル採用を継続的に改善する。 このプラクティスは、継続的な改善の原則を呼び起こします。つまり、常に改善する方法を探しています。

•組織およびプロジェクトの双方のレベルが問題を識別して対処するよう努める。

•顧客が意識する価値と投資収益率(ROI)に基づいてプロジェクトの価値を決定する。このプラクティスでは、プロジェクトの開始前に設定されたコストまたはスケジュールの基準に対してのみ進捗をトラッキングすると、たとえばスコープに大きな変更が生じた場合に進捗の不正確な測定につながる可能性があります。 代わりに、アジャイルは進捗の一つの尺度として顧客からのフィードバックを奨励します。 ソリューションの価値をソリューションのコストと比較することもプロジェクトの成功度合いの基準です。

•各イテレーションの最後に価値をデモンストレーションすることで信頼を得ます。

•ツールと計測指標を使用して進捗状況を追跡します。自動化できるバーンダウンチャートやベロシティ（ユーザーストーリーを動くプログラムに変換する速度）などのツールと計測指標を使用して、また「顧客満足」などの成功指標とスタッフのストレスや時間外勤務の削減によって進捗を追跡できます。

６．アジャイルと監査（海外）（続き）

英国の例（National Audit Office(英国の独立した議会機関で、中央政府部門、政府機関、および部門以外の公的機関の監査を担当)”Governance for Agile delivery”(2012)(https://www.nao.org.uk/wp-content/uploads/2012/07/governance_agile_delivery.pdf（２０１９年５月５日閲覧）（私訳）

ガバナンスの原則

アジャイルデリバリーの外部評価またはレビューは、プロセスや文書化だけではなく、チームの行動に焦点を合わせるべきです。評価者が技術やアジャイルデリバリーの経験など、ハイエンドのスキルを持っている場合、重大な課題を解決する上でより効果的です。さらに、「観察」を主要な証拠収集の方法として、チームがどのようにふるまっているかを継続的にレビューするならば、評価はより価値のあるものになります。評価者が質問する鍵となるものは以下のような項目です。

oチームのスキルと経験

oチームの力 – デリバリーチームの内外のコミュニケーションの頻度と質。そして、ビジネス側からデリバリーチームへのインプットのレベル

o組織の文化 – コミットメントのレベルと開かれた組織かどうかのレベル

oデリバリーチームによる品質管理のタイミングと質- テストとリリースのフレームワーク。

oチームがタスクに取り組んだ順序 - アクションと成果物の優先順位付け、バックログリスト内のアクションの量。

o各イテレーションで達成された結果に応じてチームが活動を変更する方法。

oアウトプットがビズネスに対してもたらす価値

６．アジャイルと監査（比較）

日本のシステム管理基準、システム監査基準と海外の２例を比べると、下記の点で大きく異なる点が見受けられた。

・アジャイルを受け入れる組織であるかどうか
・組織およびプロジェクトのマインドセットがアジャイル開発を行う上で十分か
・自律的に品質を保てるチームであるかどうか
・（UK）評価者がプロジェクトの様子をレビューする

７．まとめ

- アジャイル開発を行うためにはまずはアジャイル開発で何を価値として得ようとしているのかが開発主体となるユーザー企業で認識されていないとうまくいかないことが多いように見受けられる。（マインドセット）

- 契約については、アジャイルは開発者の継続的なコミットメントがないと、第３者（全く開発に関与していないメンバー）がコードをみて運用することは難しいのではないかという懸念もある。
  その点紹介した吉田氏の提案はメリットがあるように思うが、それとは違う観点で、サブスクリプションモデルにより、継続的にコミットしていく、というような契約形態もあるのではないかと考える。

- 監査人もシステム管理基準、システム監査基準に書かれている内容を背景まで知るため、アジャイル開発についての認識をもって監査する必要がある。

おききいただきありがとうございました

- 本日の発表の内容は発表者の所属する企業の意見等ではありません。