システム監査学会2014年度第28回研究大会

共通フレームをベースとした システム管理基準検討 研究プロジェクト の報告

2014年6月6日

城西国際大学
本田実

目次

1．研究プロジェクトメンバ

氏名	所属	備考
朝倉　俊道	エムビーケーメタルソリューション株式会社	
大島　誠	みずほ情報総研株式会社	
高野　美久	NECソリューションイノベータ株式会社	
本田　実	城西国際大学	研究プロジェクト主査

2. 活動状況

- 平成26年8月2日より平成27年5月26日まで11回開催
  時間は18時半から20時半
- 場所は城西国際大学紀尾井町キャンパス
- メンバは現状4名
- 活動は月1～2回開催予定

3. 研究プロジェクトの背景

- システム管理基準が作成されてから9年経っていて、必ずしも最近の情報システムの監査のための管理基準としては十分とは言えなくなってきている。
- 平成16年作成のシステム管理基準を参考にした共通フレーム(「共通フレーム2007」)が平成25年3月に改訂された(「共通フレーム2013」)。
- 現在、システム監査のISO化が検討されているが、JIS化には若干時間がかかるものと思われる。

4. 研究プロジェクトの目的

- 「共通フレーム2013」をベースとしたシステム管理基準の改定版の作成

■システム監査学会のHPへの掲載
⇒システム監査学会のHPのアクセス回数の増加

■システム監査技術者試験シラバスの見直し提案
⇒システム監査技術者育成に寄与

■システム管理基準改定案の提案
⇒システム監査業務のより実践的な判断基準に寄与

５．研究プロジェクトの作業範囲

- システム管理基準の項目すべてに対して、共通フレーム2013のタスクを対応
- 共通フレーム2013のタスクを参考に、システム管理基準の項目の見直し（範囲は「Ⅱ．企画業務」）

6. 研究プロジェクトの作業項目（1）

- 作業手順は以下の通り

① システム管理基準の各項目（コントロール）と、内容的に同等の共通フレーム2013のタスクに対応付ける。
   a. システム管理基準の各項目に共通フレーム2013のタスクが対応しないこともある。
   b. 同一の共通フレーム2013のタスクが、システム管理基準の別の複数の項目に対応することもある。
② 共通フレーム2013のタスク番号順に並び替える。
③ 共通フレーム2013のタスクでシステム管理基準の各項目に対応していないタスクを追加する。

6. 研究プロジェクトの作業項目（2）

① システム管理基準の各項目（コントロール）と、内容的に同等の共通フレーム2013のタスクに対応付ける。

システム管理基準 基準項目		共通フレーム アクティビティ タスク	
1.0.0.0	Ⅰ．情報戦略		
1.1.0.0	1・全体最適化		
1.1.1.0	1.1 全体最適化の方針・目標		
1.1.1.1	(1)ITガバナンスの方針を明確にしているか。		―
1.1.1.1	(2)情報化投資や情報化構想の決定における原則を定めているか。	2.1.1.1.3 企画環境の準備	企画者は、本プロセス及び支援ライフサイクルプロセスを実施するために、文書化されていて適切で、その組織で確立された標準、方法論、手順から適切なものを選択、テーラリング（修整）し、それらを使用する。
1.1.1.1	(3)情報システム全体の最適化目標を経営戦略に基づいて設定しているか。	2.1.1.2.1 経営上のニーズ、課題の確認	経営・事業戦略、経営・事業目標、中長期構想、これらと連動した企業の情報戦略（ITによる経営・事業戦略の実現プラン）などの事業要件に沿って、経営上のニーズ、あるいはシステム化、システム改善を必要とする業務上の課題などについて、その目的、求められる成果（目標）を確認する。企業の情報戦略には、運用の概念を含む。運用の概念では、開発されるシステム、現行のシステム及び将来開発される可能性のあるシステムを使ってビジネスの運用全体あるいは、一連の運用に関する組織の前提条件や目的を説明する。この概念にはしばしば長期の戦略的な契約や年間運用計画を含む。
1.1.1.1	(4)組織体全体の情報システムのあるべき姿を明確にしているか。	2.1.1.2.6 業務の新全体像の作成	企画者は、対象となる業務の明確化（2.1.1.2.5）に基づき、企業で将来的に必要となる最上位の業務機能と業務組織のモデルを検討する。この検討の結果、目標とする業務の新しい全体像を描く。加えて新システムの全体イメージも作成し、業務機能と組織モデル、新システムとが整合しているかを、検証プロセス（4.3参照）に従って検証及び妥当性確認を行う。
1.1.1.1	(5)システム化によって生ずる組織及び業務の変更の方針を明確にしているか。	2.1.1.2.7 対象の選定と投資目標の策定	企画者は、現行業務、システムの調査分析（2.1.1.2.3）、業務の新全体像の作成（2.1.1.2.6）との差異を確認する。それらから得られる効果、必要な想定開発期間と開発体制、他に必要となる経営資源、経営上のニーズ、課題の確認（2.1.1.2.1）との整合性、費用の概算、考えられるリスクなどを分析する。これらの分析結果、経営への寄与、法的な対応等から実施の優先順位付けを行い、順位ごとにプロジェクトの規模、必要資源などを検討し、システム投資対象の選定と目標の策定を行う。
1.1.1.1	(6)情報セキュリティ基本方針を明確にしているか。		―

6．研究プロジェクトの作業項目（3）

② 共通フレーム2013のタスク番号順に並び替える。
③ 共通フレーム2013のタスクでシステム管理基準の各項目に対応していないタスクを追加する。

システム管理基準　基準項目		共通フレーム　アクティビティ　タスク	
		1.1.1.01 構想またはニーズの記述	
2.3.0.1	(2)ソフトウェア、ハードウェア、ネットワークは、調達の要求事項を基に選択しているか。	1.1.1.02 システム要件、ソフトウェア要件の定義と分析	取得者は、システム又はソフトウェア要件を定義し、分析する。システム又はソフトウェア要件は、関連する設計、テスト、適合する規格及び手順と一緒に、事業、組織及び利用者の要求に加えて、安全性、セキュリティ及び他の重大要件を含むことが望ましい。
2.3.0.1	(2)ソフトウェア、ハードウェア、ネットワークは、調達の要求事項を基に選択しているか。	1.1.1.03 システム要件、ソフトウェア要件の定義と分析の委託	取得者は、自分自身でシステム又はソフトウェア要件の定義及び分析を行ってもよいし、このタスクを実行するために供給者を雇っておいてもよい。
6.5.1.1	(1)委託または受託の計画は全体最適化計画に基づいて策定し、責任者が承認しているか。	1.1.1.03 システム要件、ソフトウェア要件の定義と分析の委託	取得者は、自分自身でシステム又はソフトウェア要件の定義及び分析を行ってもよいし、このタスクを実行するために供給者を雇っておいてもよい。
2.3.0.1	(1)調達の要求事項は、開発計画及びユーザニーズに基づき作成し、ユーザ、開発、運用及び保守の責任者が承認しているか。	1.1.1.04 システム要件、ソフトウェア要件の承認権限	取得者がシステム又はソフトウェア要件の分析を供給者に委託したとしても、要件の分析結果を承認する権限は取得者が持っている。
6.5.1.1	(1)委託または受託の計画は全体最適化計画に基づいて策定し、責任者が承認しているか。	1.1.1.04 システム要件、ソフトウェア要件の承認権限	取得者がシステム又はソフトウェア要件の分析を供給者に委託したとしても、要件の分析結果を承認する権限は取得者がもっている。
		1.1.1.05 テクニカルプロセスの使用	
2.2.0.1	(8)パッケージソフトウェアを使用にあたっては、ユーザニーズとの適合性を検討しているか。	1.1.1.06 選択肢の検討	取得者は、各選択肢に対するリスク、費用及び利点を含めるために、適切な基準に照らして分析することで、取得のための選択肢を検討する。選択肢は、次を含む。 a)要件を満たす市販のシステム、ソフトウェア製品又はサービスを購入する。 b)内部的にシステム又はソフトウェア製品を開発するか、又はソフトウェアサービスを得る。 c)契約してシステム又はソフトウェア製品を開発するか、又はソフトウェアサービスを得る。 d)上記のa)、b)及びc)を組み合わせる。 e)既存のシステム、ソフトウェア製品又はソフトウェアサービスを強化する。

6．研究プロジェクトの作業手順（4）

④ システム管理基準の項目を、共通フレーム2013のタスクの内容に応じて見直す。

例えば、システム管理基準が「情報システムの導入によって影響を受ける業務、管理体制、諸規定等は、見直し等の検討を行うこと」（Ⅱ．企画業務　2．分析　（6））は、共通フレーム2013の「要件定義者は、健康、安全、セキュリティ、環境及び他の利害関係者の要件並びに重大な品質に関係する機能を指定し、人間の健康及び安全に対する、システムの使用が及ぼす悪影響の可能性に対処する」（2.2.3.5　要件の抽出）が対応する。これにより、システム管理基準を見直して次の通りとする。

「情報システムの導入によって影響を受ける業務、健康、安全、セキュリティ、環境、管理体制、諸規定等は、見直し等の検討を行うこと」

６．研究プロジェクトの作業手順（５）

⑤ システム管理基準に対応する項目がない場合、共通フレーム2013のタスクの内容より、そのタスクのリスクを考慮してコントロールを作成する。

⑥ システム管理基準の項目が、複数の共通フレーム2013のタスクに対応している場合は、共通フレーム2013のタスクのリスクを考慮してコントロールを作成する。

6．研究プロジェクトの作業手順（6）

⑤ システム管理基準に対応する項目がない場合、共通フレーム2013のタスクの内容より、そのタスクのリスクを考慮してコントロールを作成する。

2.2.0.1	(4)ユーザニーズは文書化し、ユーザ部門が確認しているか。	2.2.4.1　導出要件の分析	要件定義者は、導出された要件の全集合を分析する。
2.2.0.1	(5)情報システムの導入に伴って発生する可能性のあるリスク分析を実施しているか。	2.2.5.1　要件の問題解決	要件定義者は、要件に関する問題を解決する。
2.3.0.1	(1)調達の要求事項は、開発計画及びユーザニーズに基づき作成し、ユーザ開発、運用及び保守の責任者が承認しているか。	2.2.5.2　利害関係者へのフィードバック	要件定義者は、ニーズ及び期待が適切に把握され、表現されていることを確実にするために、分析された要件を該当する利害関係者へフィードバックする。
2.2.0.1	(4)ユーザニーズは文書化し、ユーザ部門が確認しているか。	2.2.5.2　李義関係者へのフィードバック	要件定義者は、ニーズ及び期待が適切に把握され、表現されていることを確実にするために、分析された要件を該当する利害関係者へフィードバックする。
2.2.0.1	(1)開発計画に基づいた要求定義は、ユーザ、開発、運用及び保守の責任者が承認しているか。	2.2.5.3　要件の確立	要件定義者は、利害関係者要件が正確に表現されていることを、利害関係者とともに確立する。
2.2.0.1	(4)ユーザニーズは文書化し、ユーザ部門が確認しているか。	2.2.5.3　要件の確立	要件定義者は、利害関係者要件が正確に表現されていることを、利害関係者とともに確立する。
	(xx)ユーザニーズは要件管理に適した形式で記録すること	2.2.6.1　要件の記録	要件定義者は、ライフサイクルを通して及びその後も、要件管理に適した形式で、利害関係者要件を記録する。
	(xx)ユーザニーズはその源への追跡可能性を維持すること	2.2.6.2　要件の追跡可能性維持	要件定義者は、利害関係者のニーズの源への要件の追跡可能性を維持する。

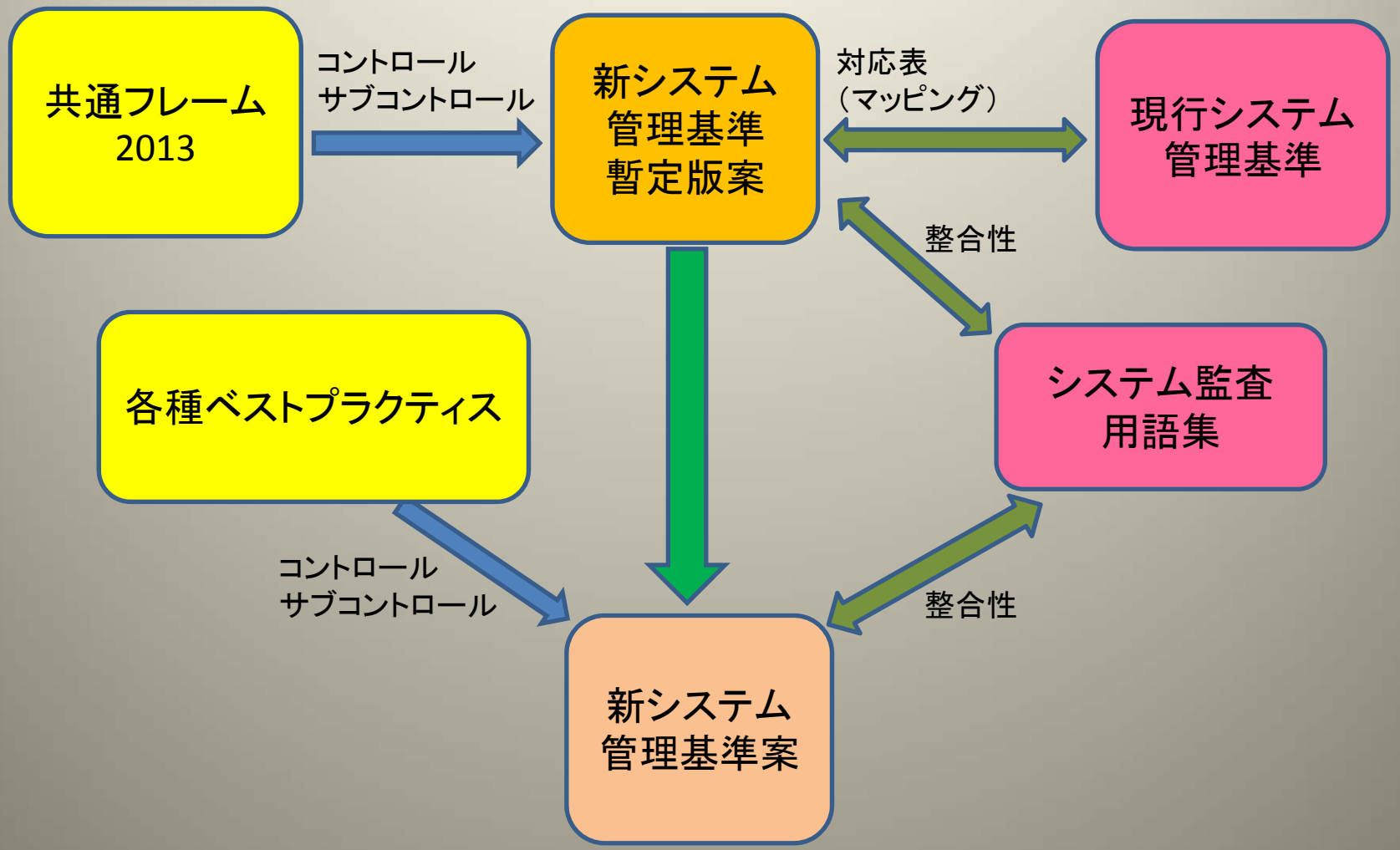
7. やり残した作業項目

- 共通フレーム2013をベースとしたシステム管理基準の項目の見直しを、「Ⅱ. 企画業務」以外も行う。
- システム管理基準と共通フレーム2013との用語の対応表
- システム管理基準の項目の見直しに、共通フレーム以外にもISMS、ITIL、PMBOK等も利用する。

8. 今後の方向(1)

- 本研究プロジェクトは、平成26年度活動予定。
- 平成26年度は、新システム管理基準暫定版の作成予定。
- プロジェクトの成果物として、システム監査学会のHP等に掲載予定。
- システム監査学会のシステム監査コンテンツ委員会で審議し、システム監査学会としてHP等に掲載予定。

8. 今後の方向(2)



最後に

- ご清聴ありがとうございました。

- 本研究プロジェクトは、実質始まったばかりの状況ですので、ご関心のある方は是非参加して頂ければと思います。