コンプライアンスのシステム監査について（中間報告）

－System Auditing of Information System Compliance (interim report)－

2011年6月10日

システム監査学会・システム監査人協会　共同
コンプライアンスのシステム監査研究プロジェクト

雑賀　努（株式会社ニイタカ　監査室）
吉田　博一（大阪府）
松田　貴典（大阪成蹊大学）

研究会メンバー

【主査】
雑賀　努　（株式会社ニイタカ）
【副主査】
吉田　博一（大阪府）
【主要メンバー】
荒牧　裕一（荒牧総合研究所）
伊地知裕貴（株式会社ニイタカ）
木村　安寿（関西学院大学大学院）
中田　和男（株式会社エスシーエイエヌ）
林　　裕正（富士通株式会社）
広瀬　克之（(株)ナレッジ，ヒューマン＆テクノロジーズ）
福本　洋一（弁護士法人　第一法律事務所）
松田　貴典（大阪成蹊大学）

（アイウエオ順）

当研究プロジェクトの活動実績（１／２）

【第一期】

・期間　　２０１０年１月～２０１０年８月（８回開催）

・内容　　コンプライアンス確保のため関連法規を一覧化し、それらの法規に関連する情報システム（ＩＣＴ）のマップを作成。

【第二期】

・期間　　２０１０年９月～２０１１年２月（５回開催）

・内容　　研究活動の参考のため、有識者による情報提供を受け、研究会メンバーと討議を実施。

　その結果を受け、第一期の成果物の見直しを行った。

当研究プロジェクトの活動実績（２／２）

講演テーマ、講演者、及び講演内容は次の通り。

①情報システムに関連するコンプライアンス（松田貴典氏）
　サイバーショッピングをモデルとして情報システムに関連するコンプライアンスの問題点を解説。

②システム監査人に求められるコンプライアンス（山口利昭氏）
　最近の事例に基づいて企業におけるコンプライアンスに係るリスク管理の問題点を解説。

③コンプラアンスとシステム監査　（芳仲宏氏）
　システム監査が情報システムに係るコンプライアンスに対するリスクを低減する重要な手段となることを解説。

目　次

０．報告要旨

１．研究の経緯
　１．①当プロジェクトの前提
　１．②松田の提起するコンプライアンスのシステム監査視点
　１．③Ｊ－ＳＯＸの内部統制の枠組み
　１．④当研究プロジェクトの考え方
　１．⑤当研究プロジェクトの研究方法

２．研究の中間成果物
　２．①「部門・業務別コンプライアンスＭＡＰ」の内容説明
　２．②「部門・業務別コンプライアンスＭＡＰ」の抜粋

３．今後の研究

補足資料①　部門・業務別コンプライアンスＭＡＰ
　　②　システム監査基準及び管理基準のコンプライアンス

０．報告要旨

- 本研究プロジェクトは、システム監査人協会との共同で開始したものである。
- 情報通信技術の進歩により、情報システム（ＩＣＴシステム）と密接に関連する法的問題を、コンプライアンス視点で点検・評価することが、重要な課題となっている。
- 本研究プロジェクトでは一般企業（製造業）を対象とした情報システムを対象に、コンプライアンスのシステム監査基準の策定を目標として研究を行っている。
- 今回は中間報告である。

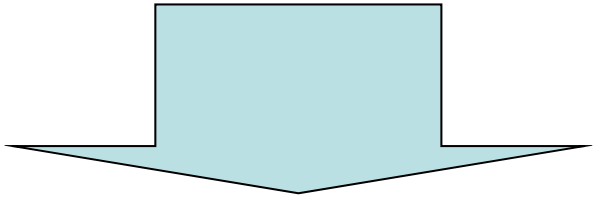
1. ①当プロジェクトの前提

システム監査人協会
２００９年度西日本合同研究会
基調講演
「コンプライアンスのシステム監査」

松田
１．②

「財務報告に係る内部統制の評価及び監査に関する実施基準」
内部統制の枠組み

金融庁
１．③



当研究プロジェクト

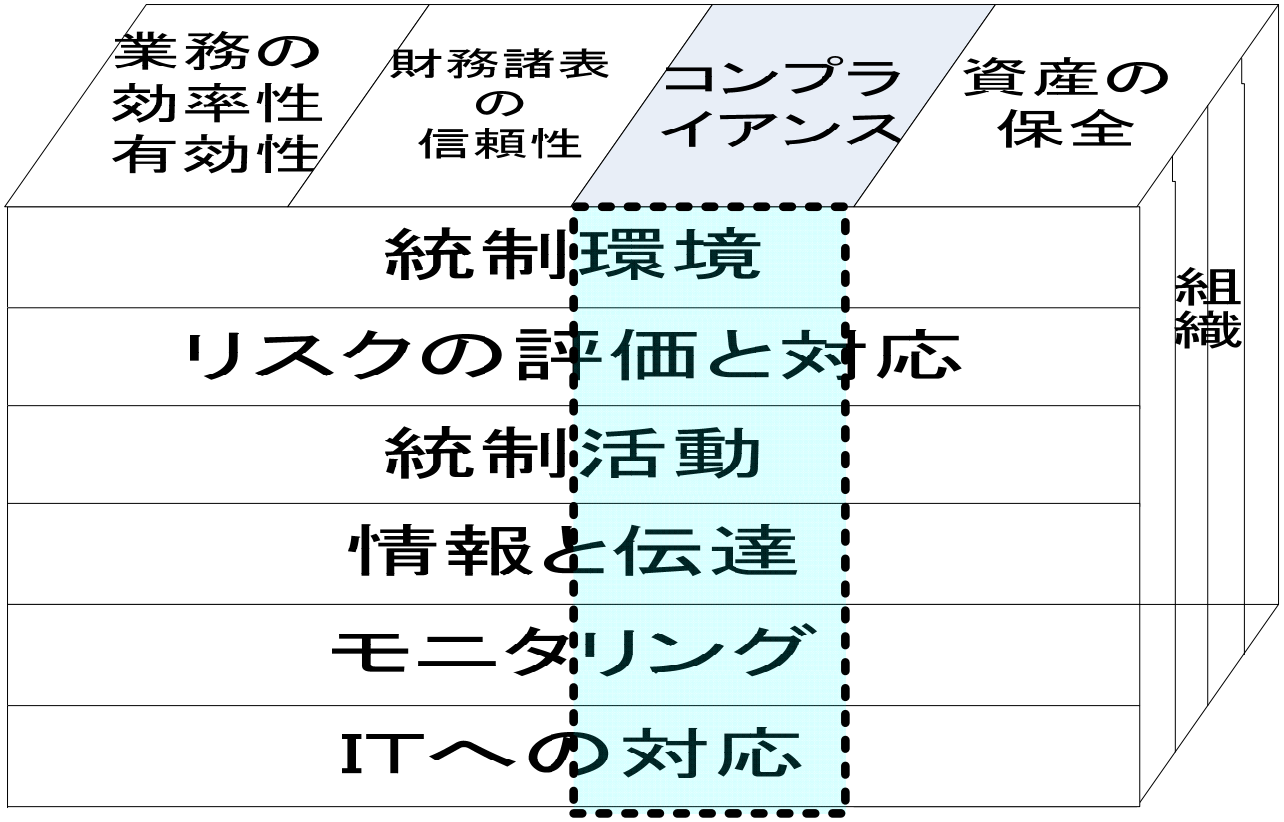
1. ②松田の提唱するコンプライアンスのシステム監査視点

1. 全社的視点でのコンプライアンスの視点

2. 組織における固有の業務で発生する
コンプライアンスの視点

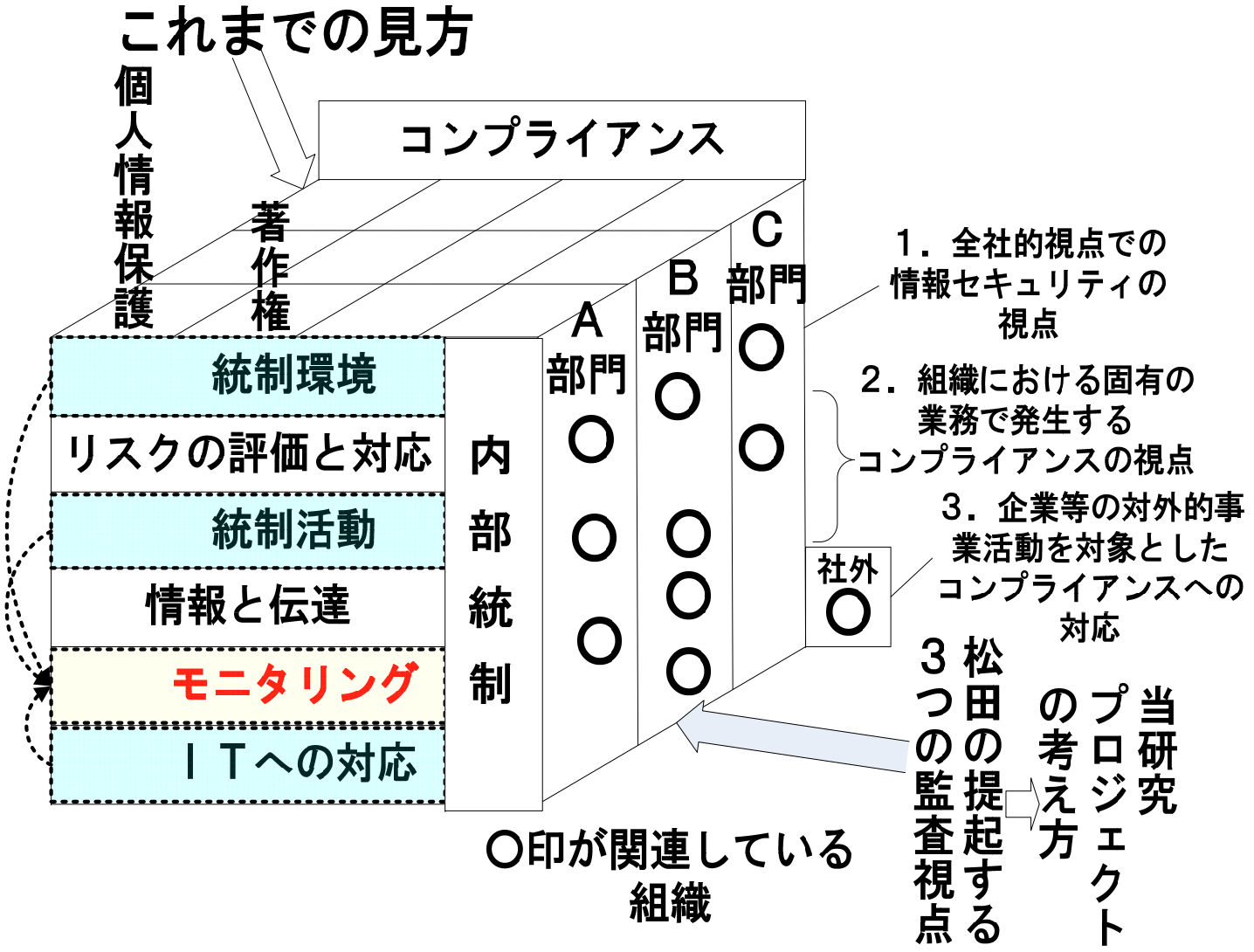
3. 企業等の対外的事業活動を対象とした
コンプライアンスへの対応

1. ③J－SOXの内部統制の枠組み

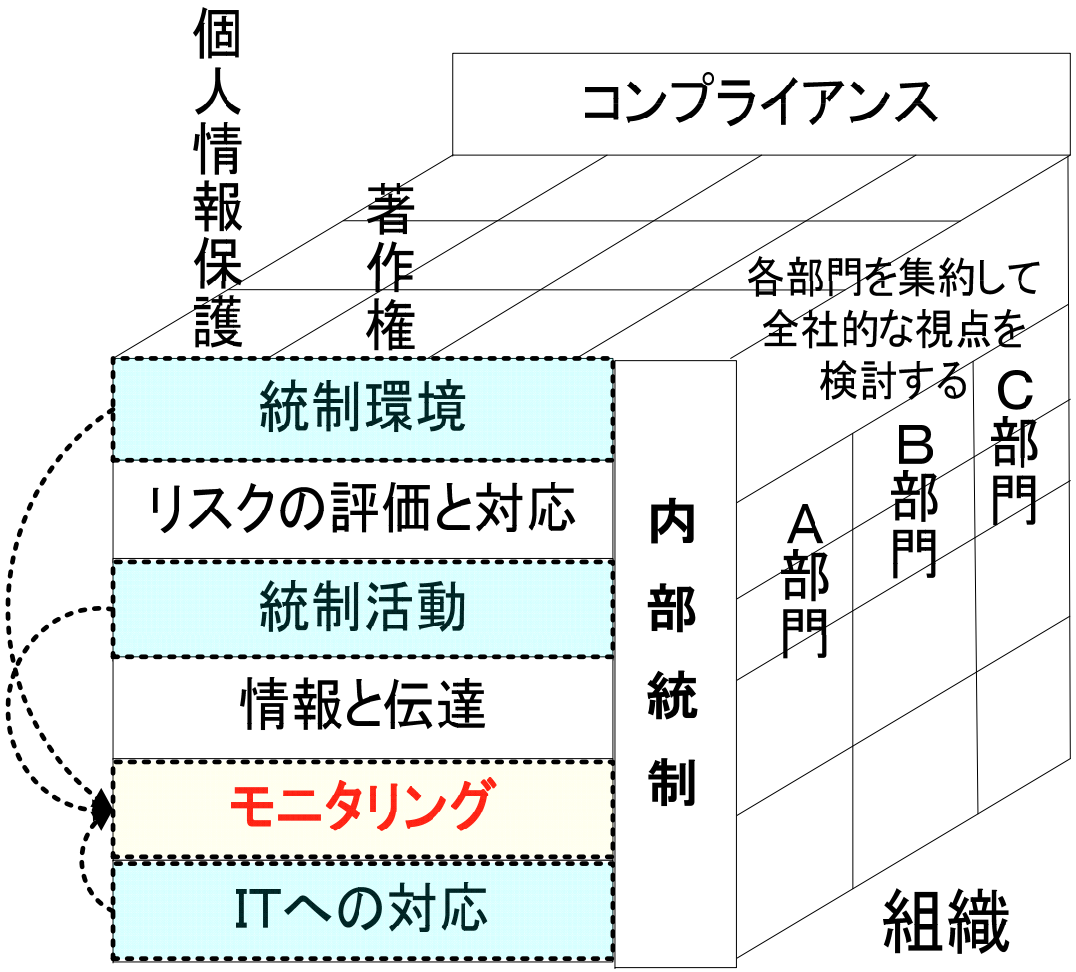


この中で情報システムに関連する部分が
当研究プロジェクトの対象

1. ④当研究プロジェクトの考え方



1. ⑤当研究プロジェクトの研究方法



1. 当研究プロジェクトの目的
　コンプライアンスのシステム監査の要件を明らかにし、できれば個別の監査基準を提案する。

2. 当研究プロジェクトの研究方法
　組織面を入り口に対象となる法令を抽出、分類する。結果を個別の対象に対する検討を深める。ここで外部の発表も考慮する。

3. 前提条件
　情報システムに係るの意味は以下の通り
・ITへの対応は全般統制（IT部門業務）とする。
・業務システムは各組織の手作業も含めた統制活動として考える。
・社内規定、方針等の統制環境も含める。

2. ①「部門・業務別コンプライアンスMAP」の内容説明

今回は参加メンバーの所属を勘案してメーカーを企業モデルとした。

大部門	部署	業務	関連法令	関連情報システム
以下の３つに分類した。 ①本社管理部門（コーポレート部門） ②工場・物流・研究部門 ③営業部門	総務部、人事部等通常企業に存在すると思われる部門を設定した。	実際の業務を内容が分かるレベルで記載した。 （記載例） 総務部：「定款管理」、「役員会・総会関連」、「株式・株主管理」等	関連する法令を情報システムとの関連に係りなく網羅的に記載した。	使用しているまたは関連のあるシステムを網羅的に記載した。

2. ②「部門・業務別コンプライアンスMAP」の抜粋

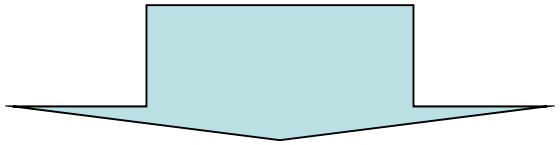
大部門：本社管理部門（コーポレート部門）　　詳細は補足資料

部署	業務	関連法令	関連ICTシステム
総務部	定款管理	会社法	文書管理
	役員会・総会関連	会社法 商業登記法	文書管理 スケジュール管理 総会管理システム（証券代行側）
	株式・株主管理	会社法 金融商品取引法 会社情報適時開示ガイドブック（東証）	電子株式管理 株主優待管理システム
	広報、IR	景品表示法 著作権法	電子媒体 HP
	建物・物品・固定資産管理	法人税法 固定資産税法	会計システム 固定資産管理、リース資産管理 IT資産管理
		建築基準法 消防法 不動産登記法	
	契約管理	民法 商法 電子署名・認証法	EDI
	社内稟議	会社法 刑法	稟議システム
	渉外	民法 商法 著作権法 暴力団対策法 国家公務員倫理法	電子メール
人事部	人事制度・人事企画	公益通報者保護法	人事情報管理システム
	人事評価・考課・昇給	個人情報保護法	人事システム
	採用	労働基準法 障害者雇用促進法 男女雇用機会均等法 個人情報保護法	採用管理システム HP
	労務管理・給与	労働基準法 雇用保険法 厚生年金法	就業管理システム
		職安法 労働者派遣法	
		じん肺法	
		ストーカー行為等の規制等に関する法律	
		育児・介護休業法	
		介護保険法　　健康保険法	
	安全衛生（労働環境の整備）	労働安全衛生法	
		感染症の予防及び感染症患者に対する医療に関する法律	
		建築物における衛生的環境の確保に関する法律（ビル衛生管理法）	
	組合	労働組合法　　労働調整法	
	給与処理	所得税法 各種社会保険法規	給与システム

3. 今後の研究(サブセットとしての基準)

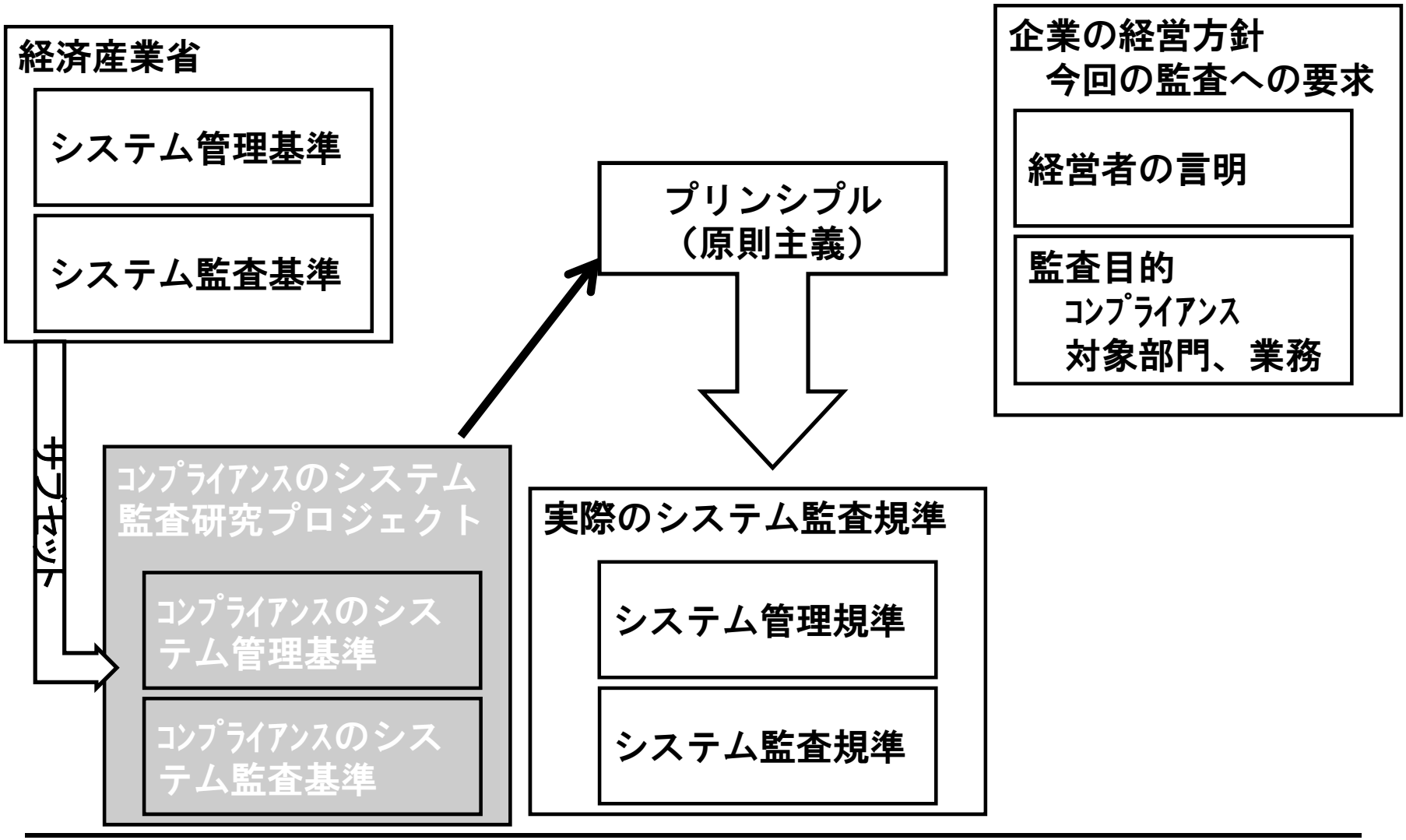
● システム管理基準及び監査基準に記載されているコンプライアンス項目は個別具体的な項目ではない。
● 個別の監査現場で実際に使用できるものとはなっていない。

(詳細は「補足資料② システム監査基準及び管理基準のコンプライアンスに関する松田の主張」を参照



今回の研究プロジェクトでは、監査目的をコンプライアンス・監査対象を企業の部門と業務で絞り込むことによりできるだけ監査現場で使用できる基準をシステム監査基準及び管理基準のサブセットとして設定する。

3. 今後の研究



補足資料①　部門・業務別コンプライアンスＭＡＰ　－１－

大部門：本社管理部門（コーポレート部門）

部署	業務	関連法令	関連ICTシステム
総務部	定款管理	会社法	文書管理
	役員会・総会関連	会社法 商業登記法	文書管理　スケジュール管理 総会管理システム（証券代行側）
	株式・株主管理	会社法 金融商品取引法 会社情報適時開示ガイドブック（東証）	電子株式管理 株主優待管理システム
	広報、IR	景品表示法　著作権法	電子媒体 HP
	建物・物品・固定資産管理	法人税法　固定資産税法	会計システム 固定資産管理、リース資産管理 IT資産管理
		建築基準法　消防法　不動産登記法	
	契約管理	民法　商法　電子署名・認証法	EDI
	社内稟議	会社法　刑法	稟議システム
	渉外	民法　商法　著作権法　暴力団対策法 国家公務員倫理法	電子メール
人事部	人事制度・人事企画	公益通報者保護法	人事情報管理システム
	人事評価・考課・昇給	個人情報保護法	人事システム
	採用	労働基準法　障害者雇用促進法 男女雇用機会均等法　個人情報保護法	採用管理システム　HP
	労務管理・給与	労働基準法　雇用保険法　厚生年金法	就業管理システム
		職安法　労働者派遣法	
		じん肺法	
		ストーカー行為等の規制等に関する法律	
		育児・介護休業法	
		介護保険法　　健康保険法	
	安全衛生（労働環境の整備）	労働安全衛生法	
		感染症の予防及び感染症患者に対する医療に関する法律	
		建築物における衛生的環境の確保に関する法律（ビル衛生管理法）	
	組合	労働組合法　　労働調整法	
	給与処理	所得税法　各種社会保険法規	給与システム

補足資料①　部門・業務別コンプライアンスＭＡＰ　－２－

大部門：本社管理部門（コーポレート部門）

部署	業務	関連法令	関連ICTシステム
人事部	給与処理	地方税法	
	社員教育　　能力開発	著作権法	e－ラーニング　教育管理システム
経理部	予算管理	会社法　金融商品取引法	会計システム
	伝票処理	手形法・小切手法　電子記録債権法	経理システム
	会計監査・税務監査対応	会計基準　電子帳簿保存法 金融商品取引法	会計システム
	環境会計	環境関連法	文書管理システム
	決算処理	会社法　金融商品取引法　法人税法	会計システム
財務部	資金運用・資本調達	金融商品取引法　外為法　金融商品販売法	資金管理システム
	決済・資金繰り	手形法・小切手法　電子記録債権法	資金管理システム
情報システム部	情報化企画（情報化戦略）	情報処理の促進に関する法律 不正競争防止法	
	要求・要件定義・プロジェクト管理	民法　著作権法　不正競争防止法	提案書管理
	システム開発	民法　著作権法	プロジェクト管理システム
	インフラ構築	不正アクセス禁止法	認証システム ログ管理システム
	情報システム保守・運用	情報システム安全対策基準	システム運用管理システム
	ソフトウェア資産管理	著作権法	ソフトウェア管理システム
	メール管理（情報セキュリティー）	個人情報保護法　刑法	メールシステム ウィルス対策ソフト
	データ保存・BCP	e－文書法　電子帳簿保存法	文書管理システム
経営企画部	経営戦略　経営目的　経営計画	個人情報保護法	販売管理、生産管理、物流システム等の個別システム
	組織管理	会社法	
	関係会社管理	会社法　金融商品取引法	連結会計システム
	海外会社管理	外為法、出資法	
	顧客対応・渉外窓口	個人情報保護法	顧客情報管理システム
知財部	特許管理	特許法	ナレッジマネジメントシステム 特許管理システム
	実用新案管理	実用新案法	知財管理システム
	意匠管理	意匠法	知財管理システム
	著作権管理	著作権法	知財管理システム

補足資料①　部門・業務別コンプライアンスＭＡＰ　－３－

大部門：本社管理部門（コーポレート部門）

部署	業務	関連法令	関連ICTシステム
知財部	商標管理	商標法、不正競争防止法	知財管理システム
	営業秘密	不正競争防止法	知財管理システム
CSR・監査部	品質管理	ISO9001等	生産管理システム（一部機能）
	プロセス管理		生産管理、工程管理システム、制御システム
	業務管理		個別業務の管理システム
	環境対応	省エネ法	
		化学物質審査規制法　　騒音規制法	
		土壌汚染対策法	
		大気汚染防止法　水質汚濁防止法	
		廃棄物処理法　　悪臭防止法	
		リサイクル法	
		環境基本法　ISO14001	
		環境配慮促進法	
		循環型社会形成推進基本法	
		温対法	
	内部統制	会社法　金融商品取引法	会計システム

補足資料①　部門・業務別コンプライアンスＭＡＰ　－４－

大部門：工場・物流・研究部門

部署	業務	関連法令	関連ICTシステム
研究開発部	研究開発管理	著作権法、特許法、不正競争防止法	
	企画		
	設計・デザイン	意匠法	CAD／CAM
	試作・テスト	下請法	
	シミュレーション・解析		
製造部	生産計画・統制	不正競争防止法	生産管理システム
	製造	製造物責任法、下請法	生産管理システム
	品質表示	計量法　JIS法、JAS法、食品衛生法、健康増進法、薬事法	生産管理システム
	原材料管理	計量法　JIS法、JAS法、食品衛生法、健康増進法、薬事法	在庫管理システム
	消耗品管理		消耗品管理システム
	原価管理	金融商品取引法	原価管理システム
	廃棄物管理	廃棄物処理法、環境関連法規	
品質保証部	計測、検査	計量法　JIS法、JAS法、食品衛生法、健康増進法、薬事法	品質管理システム
	不具合対策	製造物責任法	
施設部	設備資産管理		設備資産管理システム
	点検・修繕		設備資産管理システム
	衛生・清掃	環境衛生関連法	設備資産管理システム
	保安警備	労働安全衛生法	設備資産管理システム
	防災	消防法	設備資産管理システム
業務（物流）部	在庫管理	食品衛生法、健康増進法、（下請法）	在庫管理システム
	入荷確認	（下請法）	入荷（検品）システム
	配送、出荷	道路交通法 自動車NOx・PM法、排ガス抑制法	配送システム
	輸出	輸出入取引法、関税法、外為法	
購買部	発注手配・購買企画		発注システム
	契約業務・発注	民法、商法	
	未払金管理		
	輸入	輸出入取引法、関税法、外為法	

補足資料①　部門・業務別コンプライアンスＭＡＰ　－５－

大部門：営業部門

部署	業務	関連法令	関連ICTシステム
営業部	直接営業・販売活動	消費者契約法、特定商取引法 個人情報保護法 刑法（詐欺、横領、背任）	営業支援システム
	パートナー営業	独占禁止法、下請法	営業支援システム
	グローバル営業	外為法、関税法、通則法、現地法規制	営業支援システム
	通信販売・コールセンター	個人情報保護法、不正競争防止法、刑法、不正アクセス禁止法、著作権法、特定商取引法、割賦販売法、消費者契約法、民法特例法、特定メール適正化法、景品表示法，食品衛生法　JAS法　薬事法、古物営業法、	ネット販売システム 顧客管理システム HP
営業管理部	営業計画・需要予測・販売計画	不正競争防止法、独占禁止法	営業管理システム
	実績管理・販売予算管理	会社法　金融商品取引法	営業支援システム
	債権管理	民法、金融商品取引法	債権管理システム
	契約管理	民法、会社法、金融商品取引法	契約管理システム
営業企画部	商品企画	知財関連法規、不正競争防止法	特許管理システム
	市場調査、マーケティング	個人情報保護法	
	販売促進、広告宣伝	景品表示法	
CS部	顧客サービス	個人情報保護法	顧客管理システム
	アフターサービス	個人情報保護法、民法（瑕疵担保）、製造物責任法 特定消費生活用品安全法	製品ユーザー管理システム

補足資料② システム監査基準及び管理基準のコンプライアンス

システム監査基準及び管理基準 コンプライアンス規程

システム監査基準及ぶシステム管理基準では，組織体が情報システムにまつわるリスクに対するコントロールを適切に整備・運用する目的の一つに，「**情報システムが，関連法令，契約又は内部規程等に準拠するようにするため**」と規程している。

コンプライアンスに関して，システム管理基準では「情報戦略・全体最適化」の「**全体最適化計画**」で，「全体最適化はコンプライアンスを考慮すること」と記載している。また，システム管理基準の「**情報戦略・コンプライアンス**」で5項目の管理基準を規程している。

出典：平成21年11月21日付　「コンプライアンスのシステム監査」（松田）

補足資料② システム監査基準及び管理基準のコンプライアンス

システム監査基準・管理基準でのコンプライアンス規程

1．情報戦略・組織体制の「コンプライアンス」

①法令及び規範の管理体制を確立するとともに，管理責任者を定めること。
②遵守すべき法令及び規範を識別し，関係者に教育及び周知徹底すること。
③情報倫理規定を定め，関係者に教育及び周知徹底すること。
④個人情報の取扱い，知的財産権の保護，外部へのデータ提供等に関する方針を定めること。
⑤法令，規範及び情報倫理規定の遵守状況を評価し，改善のために必要な方策を講じること。

2．共通業務の「委託・受託」での「契約」

①契約は，委託契約ルール又は受託契約ルールに基づいて締結すること。
②コンプライアンスに関する条項を明確すること。
③知的財産権の帰属を明確化すること。
④特約条項及び免責条項を明らかにすること。
⑤契約締結後の業務内容に追加及び変更が生じた場合、契約内容を再検討すること

以上が，システム監査基準及びシステム管理基準に示されたコンプライアンス関連事項である。システム監査を実施するにあたっては，これらの規程事項から，企業等がそれぞれの情報システムに対応して，コンプライアンスを対象としたシステム監査視点を明らかにする必要がある。

出典：平成21年11月21日付　「コンプライアンスのシステム監査」（松田）