＜研究論文＞

金融情報システムの開発上流工程における システム監査ポイントの提言

A Proposal for Crucial Audit Issues to Implement Upper Processes in Developing Financial Information System

遠藤　正之　Masayuki Endo　　高野　研一　Kenichi Takano

（慶應義塾大学大学院システムデザイン・マネジメント研究科）

概要

我が国金融事業者が保有・運用する情報システム（金融情報システム）の社会インフラとしての重要性が高まり、経営リスクの比重も増しているが、実際には経営者が適切に目配りをできていないケースも多い。本稿では、情報システム開発の上流工程であるプロジェクト計画段階や基本設計段階のリスクマネジメントに資することを目的に、4 種類の代表的なシステム監査に関連する基準を用いて、経営者から見たシステム監査ポイントを抽出し、6 つの視点に集約する試みを行った。更に、システム監査人も、ビジネスリスクが意識された「COBIT4.1 版」と実務的な項目が網羅された「金融機関等のシステム監査指針」を組み合わせ、「システム管理基準」や「金融検査マニュアル」の項目を補完することが妥当であるという示唆を得た。

キーワード：COBIT4.1 版，システム管理基準、金融機関等のシステム監査指針、金融検査マニュアル

1. はじめに

我が国の金融事業者が保有・運用する情報システム（以下金融情報システム）、とりわけ顧客の決済を取り扱うシステムは、その信頼性及び可用性の要求の高さからみて重要な社会インフラであると言える。このような金融情報システムは、他の情報システムとは異なる四つの特異性を有している。第一は、各種の広範囲なネットワークへ接続しており、大量決済データの即時処理を確実に行うことを要請されている点。第二は、顧客の財産情報を取り扱うことからセキュリティに対する要求も高い点。第三は、システム全体が、レガシーなホスト系システムとより新しく構築された分散系システムから構成される大規模かつ複雑なシステムである点。そして第四は、被規制産業として当局の指導や国際的な金融規制の制約を受ける点である。

金融事業者の経営者は、厳しい企業間競争環境での優位性を高めつつ、一方でさまざまな経営リスクを考慮して経営を行わなければならない。インフラとなる金融情報システムの重要性は高まり、経営リスクの比重は増してきており、経営者が、金融情報システムを十分理解する必要性も高まっているにも関わらず、実際は実効性の高い目配りができていないケースも多い。また、これまでの研究では、第一に過去の問題点を指摘するもの（奥田晃司，2005）（富永新，2009）、第二に経営体制の重要性を論じたもの（森俊也，2006）（宮坂美樹、山本秀男，2010）、第三に事故事例から分析するもの（坂東幸一、田中健次，2009a）（坂東幸一、田中健次，2009b）（日本銀行金融機構局，2007）、第四に管理体制構築の提言（大橋利夫，2001）（渡辺研司，2005）、第五にリスク低減手法の提案（益田美貴，高野研一，2010，2011）があるが、経営者[1]視点でのリスクマネジメント項目は十分に整理されていない。一方、内部監査とりわけシステム監査においては、経営者の要請に基づき、かつ金融情報システムの特異性に沿っ

1　CEO（Chief Executive Officer: 経営トップ）及び CIO（Chief　Information Officer：最高情報責任者）を想定

2013/6/28 受付、2013/10/28 受理

た監査を行うことで、経営をサポートすることが求められている。そこで本研究では、既存のシステム監査関連の基準の項目を比較しつつ、我が国の金融業の経営者が金融情報システムの開発上流工程であるプロジェクト計画段階や基本設計段階に注意を払うべき不可欠な視点について検討し、経営者から観た監査ポイントを集約し提言する試みを行う。

2. 金融情報システムのリスク

2.1. 金融事業者のリスク

金融システムを構成する金融事業者のリスクについては、市場リスク、信用リスク、流動性リスク、法務・規制リスク、オペレーショナルリスク、ビジネスリスク、戦略リスク、風評リスクがある（[1]の分類による）。金融情報システムリスクは、従来オペレーショナルリスクに含まれるシステム障害の分野のリスクであると狭く捉えられがちであった。しかし金融情報システムが、経営を左右する力を及ぼすようになってきたので、本稿では、金融情報システムリスクの範囲をより広く捉えて分析する。金融事業者のリスクは、金融情報システムとの関係で、表１に示すように以下の２つのタイプに分類できると筆者は考える。

第一のタイプは、金融情報システムが外部のステークホルダーに利用され、それ自体の可用性や信頼性に関して外部から直接評価されるタイプのリスクである。このタイプのリスクとしては、オペレーショナルリスク、ビジネスリスク、戦略リスク、風評リスク、法務・規制リスクが該当し、システム監査の対象となると考えられ、本稿で詳細に検討する。

第二のタイプは、金融システムの経営上重要なリスクに対し、金融情報システムが経営判断をサポートするタイプのリスクである。金融業はリスクを取り、それを管理することによって収益を得る[2]と言われるが、金融経営の本質は、リスクを評価し、社会全体のリスク低減を行うことである。第二のタイプのリスクには、市場リスク、信用リスク、流動性リスクが該当し、金融情報システムは、リスクの正確な情報をタイムリーに経営に対して提供することが要請されている。

3. 既存のシステム監査関連基準からの経営者関連項目の抽出

この章では、既存のシステム監査関連の基準から金融情報システムの開発において、経営者のリスクマネジメントとして有効な項目を抽出する。既存のシステム監査関連の基準の項目は、過去の様々なプロジェクトに基づいて作成されており、経営者のリスクマネジメントの現実的で重要なポイントがほぼ網羅されていると考えられる。ここで対象とするのは、金融情報システムのリスクマネジメントに活用できる既存の４つのシステム監査関連の基準である。具体的には、「COBIT4.1 版」[3]、「システム管理基準」・「システム監査基準」[4]、「金融機関等のシステム監査指針」[5]、「金融検査マニュアル（預金等受入機関に係る検査マニュアル）」・「システム統合リスク管理態勢の確認検査用チェックリスト」[6][7]、以上４つであり、それぞれの基準から経営者が金融情報システムの開発において、関与すべき項目を抽出する。

表１　金融事業者のリスク

金融情報システムとの関係でのタイプ	リスクカテゴリー	リスク内容
Ⅰ．金融情報システム自体が、外部から直接評価されるタイプ	オペレーショナルリスク	システム障害、情報漏洩、事務ミス、不正
	ビジネスリスク	顧客ニーズとの不適合、提供タイミングを逃す
	戦略リスク	投資途上での中断、利用されないシステム、二重投資の発生
	風評リスク	企業イメージの低下や信用の低下による競合への取引流出
	法務・規制リスク	契約が法律や規制と合致しないことで、損害を受けるリスク
Ⅱ．金融情報システムが経営判断をサポートするタイプ	市場リスク	金融市場における価格・相場の変化で資産の価値が減少する
	信用リスク	カウンターパーティの信用力劣化により資産の価値が減少する
	流動性リスク	市場で市場価格での決済や資金調達取引ができない

3.1.「COBIT4.1 版 」（Control Objective for Information and related Technology）

米国に本部を置く情報システムコントロール協会[2]が設立したＩＴガバナンス協会が、1996 年に初版を発行し、その後 1998 年 2 版、2000 年 3 版、2005 年 12 月 4 版、2007 年 4.1 版と版を重ね、2012 年 4 月に 5 版が発表された。5 版では事業体全体のガバナンス観点の色彩がより強まっているため、本論文では、システム監査に関連する国際的な基準として完成度が高いと考えられる 4.1 版（2008 年 6 月日本語版）で検討する。

4.1 版では IT 業務を、4 つのドメイン（領域）に分類して、ガバナンスの観点で、コントロール目標とアクティビティを整理している。ドメインとは IT ガバナンスを整備・運用する上で欠かせない領域を指す [8]。

第一の PO（計画と組織：Plan and Organise）のドメインは、PO1:IT 戦略計画の策定、PO5：IT 投資の管理、PO8：品質管理、PO9：IT リスクの管理に代表されるシステム開発プロジェクト構築前の 10 プロセスからなっている。第二の AI（調達と導入：Acquire and Implement）のドメインは、AI5：IT 資源の調達、AI6：変更管理に代表されるシステム開発時の 7 プロセスからなっている。第三の DS（サービス提供とサポート：Deliver and Support）のドメインは、DS5：システムセキュリティの保証に代表される運用保守の 13 プロセスからなる。第四の ME（モニタリングと評価：Monitor and Evaluate）のドメインは、PO から DS までのドメインで提示したプロセスが適切に運用されているかをモニタリングするドメインで、ME4：IT ガバナンスの提供を含む 4 プロセスからなる。全体では合計 34 プロセスとなる。各プロセス内に、詳細化したコントロール目標 210 項目と経営者管理者のアクティビティ項目[3]197 項目が示される。

アクティビティ項目については、CEO や CIO 等の経営者や管理者の関与に関し、4 つの類型で分類されている。関与が大きいものから、①実行責任者、②説明責任者、③協議先、④報告先の 4 類型である。アクティビティ項目の 4 類型は、その順に関与度の大きさとなるため、筆者はこの類型に対し、実行責任者を 4 ポイント、説明責任者を 3 ポイント、協議先を 2 ポイント、報告先を 1 ポイントのウェイト付けをして、開発計画に関するアクティビティに関し、プロセス毎に単純集計した。その結果の抜粋は、表 2 の通りであるが、CEO の関与度の集計値が高いプロセスは、1 番目が ME4：IT ガバナンスの提供であり、以下 PO1:IT 戦略計画の策定、PO9:IT リスクの評価と管理、PO5:IT 投資の管理、AI5:IT 資源の調達と続いた。一方、CIO の関与度の集計値が高いプロセスは、PO9:IT リスクの評価と管理、AI1：コンピュータ化対応策の明確化が 1 番目 2 番目でほぼ拮抗しており、以下 PO10: プロジェクト管理、PO8: 品質管理、PO5:IT 投資の管理、PO1:IT 戦略計画の策定が続いた。実施工程別分析でも上流工程で行うものが中心であることが確認できた。

全般に実務に近い CIO のアクティビティ項目の関与度の方が CEO より大きいが、ME4：IT ガバナンスの提供だけは、CEO のアクティビティ項目の関与度が大きくなる。そこで具体的なアク

表 2 「COBIT4.1 版」で CEO,CIO の関与度の集計値が高いプロセス

CEO・CIO の関与度の集計値が高いプロセス	アクティビティ項目数（満点）	CEO	CIO	CEO+CIO 合計	主な実施工程
ME4：IT ガバナンスの提供	5（20）	18	14	32	上流から下流
PO1:IT 戦略計画の策定	5（20）	11	18	29	上流
PO9:IT リスクの評価と管理	10（40）	10	28	38	上流から下流
PO5:IT 投資の管理	5（20）	7	19	26	上流
AI5:IT 資源の調達	5（20）	7	9	16	上流から下流
PO10: プロジェクト管理	7（28）	5	22	27	上流から下流
PO8: 品質管理	5（20）	3	20	23	上流から下流
AI1: コンピュータ化対応策の明確化	8（32）	0	27	27	上流

2　ISACA：Information Systems Audit and Control Association
3　コントロール目標とアクティビティ項目は一対一対応していない。

ティビティ項目を見ると、「経営層と取締役会によるITアクティビティに対する監督と推進の確立」、「IT成果・IT戦略・資源とリスクの管理のビジネス戦略との整合、レビュー、承認、及び周知」「成果及びポリシー、計画、手続へのコンプライアンスに関する独立した定期評価の実施」「独立した評価による検出事項の解決、およびマネジメント層による合意された改善案の確実な実施」の４項目に関して、CEOが実行責任者となっていることが確認できた。IT戦略とビジネス戦略との整合を保ち、監督推進を行い、実施状況を定期評価して改善を確実に実施することが、CEOに期待されていることが読み取れる。CIOについては、ＩＴ戦略計画を策定し、システム化要件を確定させた上で、開発マネジメントに関し主導的な役割を果たす等、より実務的な関与が期待されている。

3.2.「システム管理基準」「システム監査基準」

経済産業省（旧通商産業省）が、情報システム監査を普及振興させるため、1985年に制定した「システム監査基準」を、2004年に大幅改定し「システム監査基準」と「システム管理基準」との二文書構成としたものである。「システム監査基準」が、システム監査人の行為規範であり、「システム管理基準」が、監査上の判断の尺度として用いるべき基準である。「システム管理基準」は、情報システムに係る産業全般を視野に入れ、監査項目を列挙している。金融情報システムに特化したものではないが、我が国の標準的なシステム監査関連の基準であり、検討対象とした。内容は、システム部門の管理に重点が置かれている点が特徴である。6つの章に分かれており、Ⅰ章の情報戦略が6節47項目、Ⅱ章の企画業務が3節23項目、Ⅲ章の開発業務が6節49項目、Ⅳ章の運用業務が10節73項目、Ⅴ章の保守業務が6節19項目、Ⅵ章の共通業務が7節76項目で、合計38節287項目が基準として掲載されている。

CEOとCIOの具体的関与の記載が無いため、筆者が各項を独自に「COBIT4.1版」のアクティビティ項目の４類型に分類、ウェイト付け（①実行責任者４ポイント、②説明責任者３ポイント、③協議先２ポイント、④報告先１ポイント）して、単純集計し、関与度の高い項目を分析した。その結果は、表３の通りで、CEOについては、１番目が全体最適化、２番目が組織体制となり、以下災害対策、委託･受託、情報化投資、事業継続計画、開発計画、コンプライアンスとなった。CIOについては、１番目が全体最適化と組織体制であり、以下委託・受託と人的資源管理が続いた。

「COBIT4.1版」とは異なり、CIOよりCEOの関与度の集計値が高い節は見出せなかった。これは、システム部門向け管理項目が中心であるというこの基準の特徴の帰結であると考える。実施工程別分析では、上流工程から対応が必要な項目が上位を占めた。CEO、CIOの両方で１番目となった全体最適化の詳細項目には、「ITガバナンスの方針を明確にすること」、「情報化投資及び情報化構想の決定における原則を定めること」、「情報システム全体の最適目標を経営戦略に基づいて設定すること」といった経営戦略やガバナンスに関する項目が含まれている。

表３ 「システム管理基準」でのCEO,CIOの関与度の集計値が高い節

CEO・CIOの関与度が高い章、節[4]	内訳数（満点）	CEO	CIO	CEO+CIO合計	主な実施工程
Ⅰ.情報戦略　1．全体最適化	4（16）	7	11	18	上流
Ⅰ.情報戦略　2．組織体制	3（12）	6	11	17	上流
Ⅵ.共通業務　4．災害対策	4（16）	4	5	9	上流から下流
Ⅵ.共通業務　5．委託・受託	5（20）	2	8	10	上流から下流
Ⅰ.情報戦略　3．情報化投資	1（4）	2	4	6	上流から下流
Ⅰ.情報戦略　5．事業継続計画	1（4）	2	4	6	上流から下流
Ⅱ.企画業務　1．開発計画	1（4）	2	3	5	上流から下流
Ⅰ.情報戦略　6．コンプライアンス	1（4）	2	2	4	上流から下流
Ⅵ.共通業務　4．人的資源管理	4（16）	1	8	9	上流から下流

4　Ⅰ.Ⅱ.…が章。１,２，…が節。１.１,１.２…が項。

3.3.「金融機関等のシステム監査指針」

財団法人金融情報システムセンター（FISC[5]）が、1987 年に金融機関向けに制定し、その後、2000 年第２版､2007 年第３版と二回の改訂を経ている。第３版は、個人情報保護法、金融商品取引法等の法制度の変更や、ＩＣＴガバナンスやリスクマネジメントの国際標準である COSO-ERM[6] の考え方を反映した改訂である。

金融機関のシステム監査に焦点を絞って策定されており、本稿の対象である金融情報システムに適合している。情報システムの対象領域を 12 に分類し、その対象領域をシステム監査の要点項目として、169 の小項目に分類し小項目毎にチェックポイントを記載している。要点項目別の小項目内訳は､1. 情報システムの計画と管理 11 項目､2. 情報システムリスクの管理５項目、3. 情報セキュリティ 20 項目、4. システム開発 26 項目、5. システム運用 18 項目､6. システム利用 15 項目､7. 入出力等の処理 22 項目、8. ネットワーク 10 項目、9. システム資産・資源管理７項目、10. 外部委託４項目､11. コンティンジェンシープラン 23 項目、12. ドキュメンテーション８項目である。

CEO や CIO の関与は記載されていないが、小項目毎に監査対象となる部門として情報システム部門、利用部門、本部各部門を明示している。その記載を参考にして､「COBIT4.1 版」のアクティビティ項目の４類型に分類、ウェイト付け（①実行責任者４ポイント、②説明責任者３ポイント、③協議先２ポイント､④報告先１ポイント）して、単純集計し、CEO と CIO の関与度の高い要点項目を分析した。その結果は、表４の通りで、CEO は、１番目が情報システムの計画と管理であり、情報システムリスクの管理、システム開発、情報セキュリティが続いた。CIO は、１番目の情報システムの計画と管理は同じだが、以下はシステム開発、情報セキュリティ、情報システムリスクの管理と続いた。実施工程別分析では、上流工程から対応が必要な項目であることが確認できた。

CEO、CIO とも１番目となった情報システムの計画と管理の小項目には、「経営戦略に沿った情報システム戦略の策定」、「情報システム運営委員会」、「情報システム部門の組織」、「ユーザー部門等の組織体制」、「情報システム中長期計画の策定」、「予算計画の策定」といった項目が含まれており、経営戦略に沿った情報戦略と組織整備への関与が重要であることを示している。

3.4.「金融検査マニュアル（預金等受入機関に係る検査マニュアル)」・「システム統合リスク管理態勢の確認検査用チェックリスト」

「金融検査マニュアル（預金等受入機関に係る検査マニュアル)」は、金融庁の検査用として、1999 年に制定された。その後改訂がなされ、現在は 2013 年８月版である。本マニュアルは、検査官の視点を揃えることを目的とするが、ホームページ上で公開することによって、金融機関の意識をも高め、リスクに対する態勢整備が図られることを意図したものである。その中でシステムリスク管理態勢の整備・確立状況に関し、158 項目の検査チェックポイントを制定している。項目の内訳は、経営陣による整備項目 22 項目（方針の策定６項目、内部規程・組織体制の整備 11 項目、評価改善活動５項目)、管理者による整備項目 21 項目（管理者の役割責任 10 項目、システムリスク管理部門の役割 11 項目)､個別項目 115 項目(情報セキュリティ 27 項目、システム企画・開発・運用管理等 47 項目、防犯・防災・バックアップ・不正利用防止 18 項目、外部委託管理 13 項目、付保預金払戻 10 項目）となっている。

「金融検査マニュアル（預金等受入機関に係る検査マニュアル)」の分冊の位置づけで、「システム統合リスク管理態勢の確認検査用チェックリスト」が 2002 年 12 月に制定されている。これは、

表４　「金融機関等のシステム監査指針」での CEO,CIO の関与度の集計値が高い要点項目

CEO・CIO の関与度が高い要点項目	内訳数（満点）	CEO	CIO	CEO+CIO 合計	主な実施工程
1. 情報システムの計画と管理	8（32）	14	26	40	上流
2. 情報システムリスクの管理	5（20）	7	17	24	上流から下流
3. 情報セキュリティ	8（32）	5	19	24	上流から下流
4. システム開発	14（56）	5	21	26	上流から下流

5　The Center for Financial Industry Information Systems
6　米国のトレッドウェイ委員会組織委員会（COSO）が 2004 年２月に公表したエンタープライズ・リスクマネジメントのためのフレームワークで、８つの統制要素、４つの統制目標からなる。

2002年4月に発生した大手銀行統合時のトラブルにより、金融情報システムの統合のリスク認識が社会的に高まったことを受けて制定されたものであり、システム統合リスク管理態勢に絞って、32項目のチェック項目を示している。内訳は、経営陣のリスク管理に対する協調した取組み10項目、協調したシステム統合リスク管理態勢のあり方16項目、不測の事態への対応3項目、監査及び問題点の是正3項目となっている。

CEOやCIOの関与の分析については、経営陣による整備項目の22項目に絞って、「COBIT4.1版」のアクティビティ項目の4類型に分類、ウェイト付け（①実行責任者4ポイント、②説明責任者3ポイント、③協議先2ポイント、④報告先1ポイント）して、単純集計し、CEOとCIOの関与度の集計値を分析した。その結果は、表5の通りであるが、CEO、CIOとも、内部規程・組織体制の整備が1番目となった。2番目以降は、CEOは方針の策定、評価・改善活動の順となり、CIOは逆に評価・改善活動、方針の策定の順となった。

なお、各項目の素点で見た場合は、方針の策定はCEO平均が3点となっており、内部規程・組織体制の整備の平均2点を1点上回っており、CEOの比重が高い項目であると考えられる。実施工程別分析では上流工程が中心であることが確認できた。

4. 既存の基準の限界と開発リスクマネジメントの視点

4.1. 既存の基準の限界と他の先行文献

システム監査に関する4つの基準（群）は、169から287項目とチェック項目数が多いため、抜けや漏れのない管理を行うのには適しているが、運用には高いスキルが必要となる。ICTの専門家が利用するには意義のある基準であると考えられるが、経営者にとっては、利用しにくいものであることは否定できない。 また適用には、相応のICTガバナンスが確立していることが前提となる。ICTに必ずしも精通しておらず、金融情報システムに関与する時間にも制約のある金融事業の経営者を対象に、金融情報システム開発時に注意を払うべき不可欠なリスクマネジメントの視点を絞り込んで提示することが望ましいと考える。

経営者視点での情報システムのリスクマネジメントのポイントを提示する先行文献として、情報システム一般を対象とした「IT経営ロードマップ改訂版」[9]及び、「重要インフラ情報システムの信頼性向上の取組ハンドブック」（以下「信頼性向上の取組ハンドブック」）[10]がある。

「IT経営ロードマップ」では、従来のIT投資が「守りの投資」が中心であるという問題意識から、「攻めのIT投資」実現に向けた10カ条のIT経営憲章を掲げている。具体的には、①経営とITの融合、②改革のリード、③優先順位の明確化、④見える化、⑤共有化、⑥柔軟化、⑦CIOと高度人材の育成、⑧リスク管理、⑨環境への配慮、⑩国内企業全体の底上げの10項目である。

また「信頼性向上の取組ハンドブック」では、経営者の開発時の役割として8点を挙げている。具体的には、①事業要件レベルでの外部関係者との合意、②情報システムに関係する部分の識別、③事業要件レベルでの信頼性要求のとりまとめ、④情報システムの信頼性提供見込みの承認、⑤個別の開発保守プロジェクトの承認、⑥個別の開発保守プロジェクトへの監視の参画、⑦情報システムの信頼性の評価結果と対策の承認、⑧事業要件レベルでの外部関係者への説明の8点である。

4.2. 成功事例の分析検討と視点の集約

最近の大規模かつ複雑でミッションクリティカルな金融情報システムの開発における成功事例で、報道等でその開発過程が開示されているものについて分析を行った。具体的には、A銀行のシステム統合事例と、B取引所のシステム更改事例

表5 「金融検査マニュアル」でのCEO,CIOの関与度の集計値が高い項目

CEO・CIOの関与度が高い中項目	内訳数（満点）	CEO	CIO	CEO+CIO合計	主な実施工程
1. 方針の策定	4（16）	12	16	28	上流
2. 内部規程・組織体制の整備	7（28）	14	28	42	上流
3. 評価・改善活動	5（20）	10	20	30	上流から下流

を元に検討を行った（表６）。

次に先行文献である「IT 経営ロードマップ」、「信頼性向上の取組ハンドブック」と両事例から、経営者の関与するポイントを図１の６視点に集約した。まず両文献と両事例から視点１の「経営トップのコミットメント」を導出した。次に「IT 経営ロードマップ」と両事例から、視点２の「組織体制と ICT ガバナンス」、視点３の「IT リスクマネジメント」、視点４の「拡張性一貫性確保」を導出した。最後に「信頼性向上の取組ハンドブック」と両事例から視点５の「要件定義最適化」と視点６の「品質重視の仕組構築」を導出した。

視点１：経営トップのコミットメント

経営トップが、経営戦略に沿った形の ICT 戦略の優先順位を把握決定していき、利用部門と開発部門の間の組織体制を整備し、また情報システム開発への直接的な関与により、現場の士気を向上させることで、開発と ICT 投資の成功に繋げている。

視点２：適切な組織体制構築による ICT ガバナンス体制（以下「組織体制と ICT ガバナンス」）

対象となる金融情報システム開発に適した全社的組織体制やプロジェクト体制が構築され、システム部門においても開発における ICT ガバナンス

表６　成功事例の分析

	A 銀行システム統合	B 取引所システム更改
トップの関与	CEO のリーダーシップで体制構築。開発は CIO に委任するも継続して支援	CIO を外部から調達して、その後委任し継続して支援。
体制構築	経営、業務部門、システム部門三位一体のプロジェクト体制構築	体制を整備するとともに、外部要員も投入して強化
重視したポイント	データ量増加に対するキャパシティ面での可用性、信頼性確保	高速取引に対応したレスポンスを重視
グランドデザイン	EA（エンタープライズアーキテクチャー）を適用	EA（エンタープライズアーキテクチャー）を導入
要件定義	計画に６カ月掛け、要件を整理、多様な顧客を背景に要件の優先順位の合意に注力	発注者責任の徹底、レスポンス面の重視に伴う機能を簡素化した要件定義に注力
プロジェクマネジメント	進捗管理「見える化」 各種レビューとテストの充実	開発単位別に進捗品質を管理 早期不具合発見の手法を徹底
ベンダーマネジメント	マルチベンダーをコントロール	ベンダーを巻き込んで開発

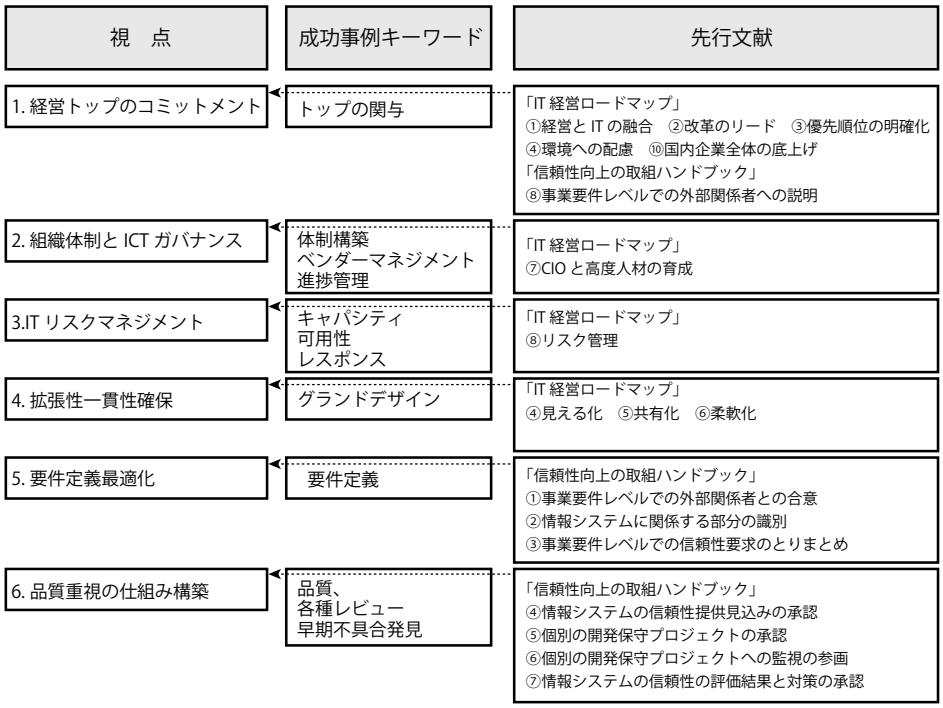

図１　視点の集約

を高めている。
視点３：IT リスクの適切な評価と対策の構築（以下「IT リスクマネジメント」）

金融情報システム開発期間に発生可能性のあるリスクや、リリース後に発生可能性のあるリスクについて、開発開始時に広い視野で全般的に洗い出した上で、リスクの発生確率と影響度合いを分析し、対処の優先順位付けを決めている。その後、適切な対策を立案し実施するとともに、継続的にリスクの状況を管理し続けている。
視点４：業務の拡張性とシステムの拡張性及びシステム間の一貫性の確保による二重投資の排除(以下「拡張性一貫性確保」)

将来の業務の拡張性やシステムの拡張性を確保できるような設計がなされ、更に将来にわたるシステムの二重投資がないように、金融情報システム全体のグランドデザインの上での位置付けが明確になったうえで、開発を行っている。
視点５：経営の要請と ICT のケイパビリティの間をつなぐ要件定義最適化（非機能要件を含む）(以下「要件定義最適化」)

経営及び業務部門から出た要件と、現状のシステムで構築可能な仕組みとの組合せに関し、業務面とシステム面で検討の上、より焦点を絞ってコストパフォーマンス良く、ビジネスに対しタイムリーで効果的な情報システム開発を行っている。
視点６：品質重視の仕組構築

金融情報システム開発では、開発スピードと同時に、可用性や安全性が重視されるため、設計品質や開発品質を向上して、最終的な稼働品質を高めることが必要であり、そのためのルールや手順の制定や、品質向上のための会議体や組織の設置が行われている。

5. 集約した視点での分析

４章の集約が適切であることを確認するため、6 つの視点がそれぞれの基準の詳細記述に、どのように対応しているかを調査分析した。また 2.1 項のリスクカテゴリーについても、主目的として考慮されているオペレーショナルリスク以外のリスクへの言及記載を確認した。

5.1.「COBIT4.1 版」

「COBIT4.1 版」の調査結果は表 7 の通りであるが、組織体制と ICT ガバナンス、IT リスクマネジメント、拡張性一貫性確保、要件定義最適化

表 7 「COBIT4.1 版」と 6 つの視点の対応

6 つの視点	プロセス	CEO の関与アクティビティ項目例
1．経営トップのコミットメント	PO1:IT 戦略計画の策定	ビジネス目標と IT 達成目標の関連付け
2．組織体制と ICT ガバナンス	PO1:IT 戦略計画の策定	IT 戦略計画、IT 実行計画策定
	PO4:IT プロセスと組織及びそのかかわりの定義	IT 戦略委員会の設置、利害関係者及びベンダーとのリレーションシップの確立、IT 組織構造の確立、IT プロセスフレームワークの策定
	PO10: プロジェクト管理	IT 投資のためのプログラム / ポートフォリオ管理フレームワークの定義
	ME4:IT ガバナンスの提供	IT 成果、IT 戦略、資源とリスクの管理のビジネス戦略との整合のレビュー承認周知、経営層による IT アクティビティに対する監督と推進の確立
3．IT リスクマネジメント	PO9:IT リスクの評価と管理	リスクマネジメントの整合性に関する判断 リスク対応実行計画の維持及びモニタリング
	DS5: システムセキュリティの保証	IT セキュリティ計画の定義と維持
4．拡張性一貫性確保	PO1:IT 戦略計画の策定	プログラムポートフォリオの分析とプロジェクトおよびサービスポートフォリオの管理
	PO5:IT 投資の管理	プログラムポートフォリオの維持
5．要件定義最適化	PO1:IT 戦略計画の策定	重要な依存関係及び最近の成果の特定
	PO2 情報アーキテクチャの定義	情報モデル、データディクショナリ、および分類スキームを活用した、最適化されたビジネスシステムの計画策定
6. 品質重視の仕組構築	PO8: 品質管理	品質管理システムの定義 、品質管理システムの確立と維持
6 つの視点以外	ME1：IT 成果のモニタリングと評価	モニタリングアプローチの確立、ビジネス目標をサポートする測定可能な目標の特定と収集

の４視点が複数のプロセスで記述されていることが確認できた。とりわけ組織体制とICTガバナンスの項目は８プロセスに記述されていた。尚、６つの視点以外でCEOが関与するアクティビティ項目として、ME1：IT成果のモニタリングと評価のプロセスの項目が見出された。

リスクカテゴリーに関しては、「戦略計画の策定」「戦略との整合」と言うキーワードで戦略リスクが強く意識され、「ビジネスとITの整合」でビジネスリスク、「コンプライアンス」で法務規制リスクに言及がある一方で、風評リスクに関しては、記載が見当たらなかった。

5.2.「システム管理基準」

「システム管理基準」の調査結果は表８の通りであるが、６つの視点が監査項目として記載されていることが確認できた。また、組織体制とICTガバナンス、ITリスクマネジメント、要件定義最適化に関してはCEO関与の複数の項が確認できた。経営トップのコミットメント、拡張性一貫性の確保、品質重視の仕組構築については、１つの項での記述の確認にとどまった。また６視点以外のCEO関与項目は見出せなかった。

リスクカテゴリーに関しては、「情報戦略」「全体最適化計画との整合性」というキーワードで戦略リスクが強く意識され、「コンプライアンス」の記載で法務規制リスクが意識されていた。一方、風評リスクについては、「障害の報告体制」という関連項目の記載に留まり、ビジネスリスクに関しては記載が見当たらなかった。

表８「システム管理基準」と６つの視点の対応

６つの視点	章、節、項	CEO関与の監査項目例
１．経営トップのコミットメント	Ⅰ.情報戦略　１．全体最適化 １.１全体最適化の方針・目標	ITガバナンスの方針を明確にすること 情報システム全体の最適目標を経営戦略に基づいて設定すること
２．組織体制とICTガバナンス	Ⅰ.情報戦略　２．組織体制 ２.１情報システム化委員会	全体最適化計画に基づき、委員会の使命を明確にし、適切な権限及び責任を与えること
	Ⅰ.情報戦略　２．組織体制 ２.２情報システム部門	情報システム部門の使命を明確にし、適切な権限及び責任を与えること
	Ⅵ.共通業務　２．進捗管理 ２.２評価	業務の工程終了時に、計画に対する実績を分析評価し、責任者が承認すること
	Ⅵ.共通業務　４．人的資源管理 4.１責任・権限	要員の責任及び権限は、業務の特性及び業務遂行上の必要性に応じて定めること
３.ITリスクマネジメント	Ⅰ.情報戦略　５．事業継続計画	情報システムに関連した事業継続の方針を策定すること。
	Ⅰ.情報戦略　６．コンプライアンス	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
	Ⅵ.共通業務　４．災害対策 7.2 災害時対応計画	リスク分析の結果に基づき、事業継続計画と整合をとった災害時対応計画を策定すること
４．拡張性一貫性の確保	Ⅰ.情報戦略　３．情報化投資	情報化投資計画は、経営戦略との整合性を考慮して策定すること
５．要件定義最適化	Ⅰ.情報戦略　４．情報資産管理の方針	情報資産の管理方針及び体制を明確にすること
	Ⅱ.企画業務　１．開発計画	開発計画は、組織体の長が承認すること
６．品質重視の仕組構築	Ⅵ.共通業務　３.品質管理	品質管理計画は、方法、体制等を明確にすること

5.3.「金融機関等のシステム監査指針」

「金融機関等のシステム監査指針」の調査結果は表９の通りであるが、６つの視点に関する記述が確認でき、組織体制と ICT ガバナンス、IT リスクマネジメント、品質重視の仕組構築の３視点が大項目レベルで複数記載されていた。尚、６つの視点以外の CEO 関与小項目は見出せなかった。

リスクカテゴリーに関しては、「情報システム戦略」「法令遵守」という項目で戦略リスク、法務規制リスクが意識されていた。「広報活動の準備」という風評リスクの記述もあったが、ビジネスリスクへの言及は見当たらなかった。

表９「金融機関等のシステム監査指針」と６つの視点の対応

６つの視点	要点項目、大項目[7]	CEO 関与の小項目例
１．経営トップのコミットメント	1. 情報システムの計画と管理 1.1. 情報システム戦略	A. 経営戦略に沿った情報システム戦略の策定 B. 情報システム運営委員会
２．組織体制と ICT ガバナンス	1. 情報システムの計画と管理 1.2. 全社的な情報システム組織	A. 情報システム部門の組織 B. ユーザー部門等の組織体制
	1. 情報システムの計画と管理 1.3. 情報システム計画	A. 情報システム中長期計画の策定 B. 情報システム短期計画の策定と実施
	4. システム開発 4.1. 運営と要員管理	B. システム開発業務の運営管理
	4. システム開発 4.7. プロジェクトマネジメント	A. プロジェクト計画の策定 B. プロジェクト計画の内容 C. プロジェクト要員
３.IT リスクマネジメント	2. 情報システムリスクの管理 2.1. 情報システムリスクの管理	A. 情報システムリスク管理体制 B. 情報システムリスクの識別と評価 C. 情報システムリスク対策 D. 法令・規制の遵守
	3. 情報セキュリティ 3.1. 全社的なセキュリティ管理体制	A. セキュリティポリシー B. セキュリティスタンダード C. セキュリティ管理体制
４．拡張性一貫性の確保	1. 情報システムの計画と管理 1.6. 投資及び予算管理	A. 予算計画の策定
５．要件定義最適化	2. 情報システムリスクの管理 2.3. 情報システムの最新技術及び金融犯罪の動向に関する調査と研究	A. 情報システムの最新技術及び金融犯罪の動向に関する調査と研究
６．品質重視の仕組構築	4. システム開発 4.7. プロジェクトマネジメント	D. 進捗・コスト・品質管理
	9. システム資産・資源管理 9.2. 容量管理	A. キャパシティプランニング

[7] 1.2.…が要点項目、1.1,1.2…が大項目、A,B…が小項目。

5.4.「金融検査マニュアル」

「金融検査マニュアル」の調査結果は表 10 の通りであるが、6 つの視点が監査項目で記述されており、どの視点も複数のチェック内容が CEO 関与項目として、確認できた。大項目レベルでは、組織体制と ICT ガバナンスと IT リスクマネジメントのみが複数の項目で確認できた。また 6 視点以外の CEO 関与項目として、「システム統合リスク管理態勢の確認検査用チェックリスト」から、運営体制の明確化というチェック内容を見出すことができた。

リスクカテゴリーに関しては、「戦略目標の明確化」「マネーローンダリング」という項目で戦略リスク、法務規制リスクが意識され、外部委託管理で「レピュテーション」との風評リスク関連の記載があったが、ビジネスリスクへの言及はなかった。

表 10「金融検査マニュアル」と 6 つの視点の対応

6 つの視点	大項目、中項目[8]	ＣＥＯ関与のチェック内容抜粋
1．経営トップのコミットメント	Ⅰ.1. 方針の策定 Ⅰ.1.2. 戦略目標の明確化	・システム戦略方針を含むか ・システム開発の優先順位 ・情報化推進計画 ・システムに対する投資計画
2．組織体制と ICT ガバナンス	Ⅰ.1. 方針の策定 Ⅰ.1.3. システムリスク管理方針の整備周知	・担当取締役及び取締役会等の役割 ・責任・システムリスク管理に関する部門の設置
	Ⅰ.2. 方針の策定 Ⅰ.2.3. システムリスク管理部門の態勢整備	・業務の遂行に必要な知識と経験を有する人員を適切な規模で配置 ・システムリスク管理部門から各業務部門に対する牽制機能が発揮される態勢を整備しているか
3.IT リスクマネジメント	Ⅰ.3. 評価改善活動 Ⅰ.3．1 システムリスク管理の分析・評価	システムリスク管理の状況を的確に分析し態勢上の弱点や改善すべき点を検討し、原因を検証しているか
	Ⅲ．3．防犯防災バックアップ不正利用防止 Ⅲ．3．コンティンジェンシー・プランの策定	災害等でコンピュータシステムが正常に機能しなくなった場合に備えたコンティンジェンシー・プランを整備しているか。
4．拡張性一貫性の確保	Ⅲ．2．システム企画・開発・運用管理 Ⅲ．2．1 企画・開発態勢	・投資対効果を検討しシステムの重要度及び性格を踏まえ、報告しているか。 ・中長期の開発計画を策定しているか
5．要件定義最適化	Ⅲ．2．システム企画・開発・運用管理 Ⅲ．2．1 企画・開発態勢	・信頼性が高く効率的なシステム導入を図る企画開発のための内部規程・業務細則等の整備 ・横断的な審議機関を設置しているか
6．品質重視の仕組み構築	Ⅲ．2．システム企画・開発・運用管理 Ⅲ．2．1 企画・開発態勢	・テスト計画を作成し、適切かつ十分にテストを行っているか ・テストやレビュー不足が原因で、長期間顧客に影響が及ぶような障害が発生しないようなテスト実施態勢を整備しているか
6 つの視点以外	Ⅱ．協調したシステム統合リスク管理態勢のあり方 Ⅱ．ⅳ協調した業務運営態勢のあり方	・運営体制の明確化（システム統合後のデータ受付、オペレーション、作業結果確認、データやプログラムの保管管理の職務分担を定め統合後の運営体制を明確にしているか。

8　Ⅰ.1.，Ⅰ.2.…が大項目、Ⅰ.1.1.，Ⅰ.1.2.…が中項目。

6. 考察とまとめ

6.1. 考察

既存基準の分析の結果を、6つの視点に関する項目の記載と、2.1項に記載したリスクカテゴリーを意識した記載という切り口で纏めたのが表11である。

既存基準の分析と表11から、筆者は以下の5点を見出した。

第一に、各基準とも、CEOの関与度が特に高い項目として、経営方針の確定、ガバナンスの確立、組織の整備に関する項目を含んでおり、それらを抽出することができた。特にガバナンス関連の項目は各基準とも充実していた。筆者が見出した視点のうち、経営トップのコミットメント及び組織体制とICTガバナンスに集約できるものである。

第二に、リスクの評価と管理の項目については、CIOがCEOよりも関与度が高い項目として、どの基準でも採り上げられていた。筆者が見出したITリスクマネジメントの視点に集約できるものである。基準ごとに重点が異なっていたが、金融事業者向けの基準である「金融機関等のシステム監査指針」で情報セキュリティ項目の関与度の集計値が高かった点が特徴的であった。これは、金融事業が顧客の資産負債に関わる重要情報を取り扱っており、情報漏えいや紛失の事故が大きく報道されるという特質を反映したものと考えられる。

第三に、拡張性一貫性の確保、要件定義最適化、品質重視の仕組構築の各視点については、切り口や記載の濃淡はあるものの、既存の基準の中で採り上げられていることが確認できた。

第四に、筆者が見出した視点以外の項目として、2点を抽出することができた。一つ目は、「COBIT4.1版」に記載されたIT成果のモニタリングと評価の項目であり、稼働開始後のシステムの評価についての経営者の関与の重要性を示唆するものであった。二つ目は、「金融検査マニュアル」の分冊である「システム統合リスク管理態勢の確認検査用チェックリスト」から抽出した、協調した業務運営態勢のあり方の項目であり、システム統合後の業務側の運営体制整備が重要であることを示唆するものである。

表11　既存基準に関する6つの視点とリスクカテゴリー

6つの視点とリスクカテゴリー		COBIT4.1版	システム管理基準	システム監査指針	金融検査マニュアル
視　点	経営トップのコミットメント	○	○	○	○
	組織体制とICTガバナンス	◎	◎	◎	◎
	ITリスクマネジメント	◎	◎	◎	◎
	拡張性一貫性の確保	◎	○	○	○
	要件定義最適化	◎	◎	○	○
	品質重視の仕組構築	○	○	◎	○
リスクカテゴリー	オペレーショナルリスク	◎	◎	◎	◎
	ビジネスリスク	○	−	−	−
	戦略リスク	◎	◎	○	○
	風評リスク	−	△	○	△
	法務・規制リスク	○	○	○	○

注）◎：複数記載あり、○：記載あり、△：関連項目記載あり、−：記載なし

(複数記載は、CEO関与の視点でCOBITのプロセス、システム管理基準の章、システム監査指針・金融検査マニュアルの大項目レベルでカウント)

第五に、リスクに関して、オペレーショナルリスクについては、どの基準も十分意識されていたが、経営者が重視しているビジネスリスクの観点はCOBITだけが意識しており、日本の監査に関連する基準では明確に意識されていなかった。また風評リスクについては、どの基準もやや間接的な記載であった。さらに金融事業者の経営者が本業として関心を持っている市場リスク、信用リスク、流動性リスクについての記載は見出せなかった。経営者が着目するリスクへの記述が不十分であるという点で、経営者のリスクマネジメントに直接活用するには、やや物足りない面があることが伺える。

6.2. まとめ

結論として、筆者が見出した経営者向けの６つの視点に関しては、今回検討した２事例とシステム監査関連の４基準の分析の範囲では、経営者が着目すべきリスクマネジメントの項目を集約するものとして妥当性が示唆された。ただし、CEO中心の関与項目とCIO中心の関与項目があること、金融事業者の経営者が重視するビジネスリスクや、風評リスク等の観点が既存の基準に盛り込まれていないという示唆もあった。金融機関のシステム監査人は、ビジネスリスクが意識された「COBIT4.1版」と実務的な項目が網羅された「金融機関等のシステム監査指針」を組み合わせ、更に「システム管理基準」や「金融検査マニュアル」の要素を補完することが望ましいと考える。

7. おわりに

本稿は、金融事業者の経営戦略が直接反映される情報システム開発の上流工程に関し、リスクマネジメントの観点から重要性を検証するとともに、経営者のリスクマネジメントの着眼点について、既存の国際的監査基準であるCOBITや日本の監査に関連する基準の項目も踏まえながら、不可欠な項目に絞り込んで提言した。この６つの視点をベースとして、今後経営者の利用できるリスクマネジメントのポイントを、情報技術の進展や経済のグローバル化の動向も踏まえて、より具体的に提示する研究を系統的かつ実践的に進めて行きたい。

参考文献

[1] Michel Crouhy、Dan Galai、Robert Mark,『リスクマネジメントの本質』（訳者代表三浦良造）, 共立出版 , 2008, pp. 21-30.
[2] 日本型金融システムと行政の将来ビジョン懇話会 ,「金融システムと行政の将来ビジョン」, 2002.,pp.6
[3] ITガバナンス協会 ,『COBIT4.1版（日本語版）』, ITガバナンス協会 , 2007.
[4] 経済産業省 ,「システム管理基準」「システム監査基準」, 2004.
[5]（財）金融情報システムセンター ,『金融機関等のシステム監査指針第３版』, 財団法人金融情報システムセンター , 2007.
[6] 金融庁 ,「金融検査マニュアル（預金等受入金融機関に係る検査マニュアル）」, 2013.
[7] 金融庁 ,「システム統合リスク管理態勢の確認検査用チェックリスト」, 2002.
[8] 梶本政利、原田要之助 ,「経営を支えるITの実現に ‘COBIT’ を生かす」,『日経コンピュータ 2008年10月15日号』, 2008, pp. 92-98.
[9] 経済産業省 ,「IT経営ロードマップ改訂版」, 2010. http://www.meti.go.jp/policy/it_policy/it_keiei/action/conference/roadmap_main.pdf. [アクセス日 : 2013年6月22日].
[10] 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 ,「重要インフラ情報システムの信頼性向上の取組みガイドブック」, 独立行政法人情報処理推進機構 , 2011.

付　録

別紙１（表２表７の根拠）
別紙２（表３表８の根拠）
別紙３（表４表９の根拠）
別紙４（表５表10の根拠）
別紙５（表10の根拠）

別紙 1

開発リスクマネジメント（RM）の要素…C：経営、Or：組織ガバナンス、R：IT リスク、E：拡張性、Op: 要件定義最適化、Q：品質重視
経営者関与ポイント…4 点（R）：実行責任者、3 点（A）：説明責任者、2 点（C）：協議先、1 点（I）：報告者

COBIT4.1版　コントロール目標	アクティビティ	CEO	CIO	CEO+CIO	開発RMの要素	CFO	企業幹部	ビジネスオーナー	OP責任者	設計責任者	開発責任者	IT管理責任者	PMO	コンプラ・監査・リスク・SEQ担当	導入チーム	研修部門	サービスインシデント構成問題管理担当	取締役会	合計
PO1 IT 戦略計画の策定		11	18	29		7	11	11	10	8	10	8	7	6	0	0	0	0	107
1.1 IT 価値の管理																			
1.2 ビジネスとIT の整合	ビジネス達成目標とIT 達成目標の関連付け	2	4	6	C	1	4	2											13
1.3 現在の能力と成果の評価	重要な依存関係および最近の成果の特定	2	4	6	Op	2	4	2	2	2	2	2		2					24
1.4 IT 戦略計画	IT 戦略計画の策定	3	4	7	Or	2	2	1	2	2	2	2	1	2					23
1.5 IT 実行計画	IT 実行計画の策定	2	3	5	Or	1		2	2	2	2	2	4	1					21
1.6 IT ポートフォリオの管理	プログラムポートフォリオの分析と、プロジェクトおよびサービスポートフォリオの管理	2	3	5	E	1	1	4	4	2	4	2	2	1					26
PO2 情報アーキテクチャの定義		4	11	15		8	8	10	2	16	12	2	0	13	0	0	0	0	86
2.1 企業の情報アーキテクチャモデル	企業情報モデルの構築と保守		3	3	Or	2	1	2		4	2	2		2					18
2.2 企業データディクショナリおよびデータ構文規則	企業データディクショナリの構築と保守		1	1	Op			2		4	4			2					13
2.3 データ分類体系	データ分類体系の確立と保守	1	2	3	Op	2	3	2	1	2	2			4					19
2.4 インテグリティの管理	データオーナに対する情報システム分類手続とツールの提供	1	2	3	Op	2	3	2	1	2	2			4					19
	情報モデル、データディクショナリ、および分類スキームを活用した、最適化されたビジネスシステムの計画策定	2	3	5	Op	2	1	2		4	2			1					17
PO3 技術指針の決定		0	15	15		5	5	0	9	20	9	4	6	8	0	0	0	0	81
3.1 技術指針計画の策定	技術インフラストラクチャ計画の策定と維持		3	3	E	1	1		2	4	2	2		2					17
3.2 技術インフラストラクチャ計画	技術標準の策定と維持		3	3	E				2	4	2	1	1	1					14
3.3 将来の動向および規制のモニタリング	技術標準の公開		3	3	E	1	1		1	4	1	1	1	1					14
3.4 技術標準	技術進歩に関するモニタリング		3	3	Op	1	1		2	4	2		2	2					17
3.5 IT アーキテクチャ委員会	新しい技術の(将来的)(戦略的)使用の定義		3	3	Op	2	2		2	4	2		2	2					19
PO4 ITプロセスと組織及びそのかかわりの定義		4	14	18		8	10	5	11	11	8	14	8	8	0	0	0	0	101
4.1 IT プロセスフレームワーク	委員会の設置、利害関係者およびベンダーとのリレーションシップの確立を含む、IT 組織構造の確立	2	3	5	Or	2	2		2	2	2	4	2	1					22
4.2 IT 戦略委員会	IT プロセスフレームワークの策定	2	3	5	Or	2	2		2	2	2	4	2	2					23
4.3 IT 運営委員会	システムオーナの明確化		3	3	Or	2	2	2	4	1	1	1	1	1					18
4.4 組織におけるIT 部門の配置	データオーナの明確化		2	2	Or	1	3	2	1	4	1	1	1	2					18
4.5 IT 組織の構造	監督業務および職務の分離を踏まえた、IT 担当者の役割および責任の確立と導入		3	3	Or	1	1	1	2	2	2	4	2	2					20
4.6 役割と責任																			
4.7 IT の品質保証の責任																			
4.8 リスク、セキュリティ、およびコンプライアンスに関する責任																			
4.9 データおよびシステムのオーナシップ																			
4.10 監督																			
4.11 職務の分離																			
4.12 IT スタッフの配置																			
4.13 主要IT 担当者																			
4.14 契約社員に関するポリシーおよび手続																			
4.15 リレーションシップ																			
PO5 IT 投資の管理		7	19	26		12	16	6	6	6	6	8	9	5	0	0	0	0	100
5.1 IT セキュリティの管理	プログラムポートフォリオの維持	3	4	7	E	4	4	2					1	1					19
5.2 IT 予算内での優先順位の決定	プロジェクトポートフォリオの維持	1	4	5	E	2	4	2		2	2		2	1					20
5.3 IT 予算編成プロセス	サービスポートフォリオの維持	1	4	5	E	2	4	2	2				2	1					18
5.4 コスト管理	IT 予算編成プロセスの確立と維持	1	3	4	E	2	2		2	2	2	4	2						20
5.5 便益管理	ビジネスにおけるIT 投資、コスト、および価値の特定、周知、およびモニタリング	1	4	5	E	2	2		2	2	2	4	2	2					23
PO6 マネジメントの意図と指針の周知		3	12	15		4	3	1	4	2	4	10	0	6	0	0	0	0	49
6.1 IT ポリシーおよび統制環境	IT 統制環境およびフレームワークの構築と維持	1	4	5	Or	2	1	1	2		2	2		2					17
6.2 企業のIT リスクおよび内部統制のフレームワーク	IT ポリシーの策定および保守	1	4	5	Or	1	1		2	2	2	4		2					19
6.3 IT ポリシーの管理	IT コントロールフレームワークおよびIT 目標と指針の周知	1	4	5	Or	1	1					4		2					13
6.4 ポリシーの展開				0															0
6.5 IT 目標と指針の周知				0															0
PO7 IT 人材の管理		0	6	6		2	0	0	6	6	6	8	6	2	0	0	0	0	42
7.1 要員の募集および保持	IT スキル、職位定義書、給与支払い区分、個人的な業績ベンチマークの特定		3	3	Or	2			2	2	2	4	2						17
7.2 要員の能力	IT 人材に関する人事ポリシーおよび手続の実施(募集、採用、調査、報酬、研修、評価、昇進、および解雇)		3	3	Or				4	4	4	4	4	2					25
7.3 役割に応じた人材配置				0															0
7.4 要員の研修				0															0
7.5 個人に対する依存				0															0
7.6 要員の人事認可手続				0															0
7.7 従業員の業績評価				0															0
7.8 職務の変更および解雇				0															0
PO8 品質管理		3	20	23		2	3	5	9	9	9	9	9	10	0	0	0	0	88
8.1 品質管理システム	品質管理システムの定義	2	4	6	Q		2	1	1	1	1	1	1	2					16
8.2 IT IT 標準および品質の実践基準	品質管理システムの確立と維持	1	4	5	Q	1	1	1	2	2	2	2	2	2					20
8.3 開発および調達標準	品質標準の策定と組織全体への周知		4	4	Q	1		1	2	2	2	2	2	2					18
8.4 顧客中心	継続的改善に向けた品質計画の策定および管理		4	4	Q			1	2	2	2	2	2	2					17
8.5 継続的改善	品質目標へのコンプライアンス状況の測定、モニタリング、およびレビュー		4	4	Q			1	2	2	2	2	2	2					17
8.6 品質の測定、モニタリング、およびレビュー				0															0
PO9 IT リスクの評価と管理		10	28	38		14	14	33	26	19	19	19	2	17	0	0	0	0	201
9.1 IT リスクマネジメントとビジネスリスクマネジメントの整合	リスクマネジメントの整合性に関する判断(リスクの評価など)	3	2	5	R	4	2	4	1					1					17
9.2 リスクをめぐる状況の明確化	関連する戦略的ビジネス目標の理解		4	4	R	2	2	2	2					1					13
9.3 イベントの特定	関連するビジネスプロセス目標の理解		2	2	R			2	4					1					9
9.4 リスク評価	社内のIT 目標の特定とリスク背景の明確化		4	4	R			4		2	2	2		1					15
9.5 リスクへの対応	目標に関連するイベントの特定(イベントの一部はビジネス指向(ビジネスはA)、一部はIT 指向(IT はA、ビジネスはC)	1	3	4	R			3	4	4	4	4		2					25
9.6 リスク対応実行計画の維持およびモニタリング	イベントに関連するリスクの評価		3	3	R			3	4	4	4	4		2					24
	リスク対応策の評価	1	3	4	R	1	3	3	4	4	4	4		2					29
	コントロールに関するアクティビティの優先順位付けおよび計画	2	3	5	R	2	3	4	4	2	2	2		2					26

別紙 1

開発リスクマネジメント（RM）の要素…C：経営、Or：組織ガバナンス、R：IT リスク、E：拡張性、Op: 要件定義最適化、Q：品質重視
経営者関与ポイント…4 点（R）：実行責任者、3 点（A）：説明責任者、2 点（C）：協議先、1 点（I）：報告者

COBIT4.1版　コントロール目標	アクティビティ	CEO	CIO	CEO+CIO	開発RMの要素	CFO	企業幹部	ビジネスオーナー	OP責任者	設計責任者	開発責任者	IT管理責任者	PMO	コンプラ・監査・リスク・SEQ担当	導入チーム	研修部門	サービスインシデント構成問題管理担当	取締役会	合計
	リスク対応実行計画の承認および資金の確保			0	R	3	3	4	1	1	1	1		1					15
	リスク対応実行計画の維持およびモニタリング	3	4	7	R	2	1	4	2	2	2	2	2	4					28
PO10 プロジェクト管理		5	22	27		4	13	5	8	8	9	6	26	14	0	0	0	0	120
10.1 プログラム管理フレームワーク	IT 投資のためのプログラム/ポートフォリオ管理フレームワークの定義	2	4	6	Or	2	3						2	2					15
10.2 プロジェクト管理フレームワーク	IT プロジェクト管理フレームワークの確立と維持	1	4	5	Or	1	1	1	2	2	2	2	4	2					22
10.3 プロジェクト管理のアプローチ	IT プロジェクトのモニタリング、測定および管理システムの確立と維持	1	4	5	Or	1	1		2	2	2	2	4	2					21
10.4 利害関係者の関与	プロジェクト憲章、日程、品質計画、予算、コミュニケーション管理計画、およびリスクマネジメント計画の作成		2	2	Or		2	2	2	2	2	2	4	2					20
10.5 プロジェクト範囲の記述	プロジェクトの利害関係者の協力および関与の確保	1	4	5	Or		3	2					4	2					16
10.6 プロジェクトの各フェーズの開始	プロジェクトおよびプロジェクトに関する変更の効果的なコントロールの保証		2	2	Or		2		2	2	2		4	2					16
10.7 統合プロジェクト計画	プロジェクトの保証およびレビュー方法の定義と導入		2	2	Or		1				1		4	2					10
10.8 プロジェクトの資源				0															0
10.9 プロジェクトのリスクマネジメント				0															0
10.10 プロジェクトの品質計画				0															0
10.11 プロジェクト変更コントロール				0															0
10.12 保証方法に関するプロジェクト計画				0															0
10.13 プロジェクトの成果の測定、報告、およびモニタリング				0															0
10.14 プロジェクトの終了				0															0
AI1 コンピュータ化対応策の明確化		0	27	27		3	24	20	17	15	19	2	32	11	0	0	0	0	170
1.1 ビジネスの機能的および技術的要件の定義と保守	ビジネスの機能的および技術的要件の定義		2	2	Op		2	4	2	4	4		4	1					23
1.2 リスク分析報告	要件のインテグリティ/通用性を目指したプロセスの確立		2	2	Op				2		2		4	2					12
1.3 実現可能性調査および代替対応策の策定	ビジネスプロセスリスクの特定、文書化、および分析		4	4	R		4	4	4	2	4		4	2					28
1.4 要件および実現可能性の決定および承認	提案されたビジネス要件の導入に関する実現可能性調査/影響評価の実施		4	4	Op		4	4	2	2	2		4	2					24
	提案されたソリューションにおけるIT 運用便益の評価		4	4	E	1	4	4	1	1	1		4						20
	提案されたソリューションにおけるビジネス便益の評価		4	4	E		4		2	2	2	1	4						19
	要件承認プロセスの作成		3	3	Op		2		2	2	2		4	2					17
	提案されたソリューションの承認		4	4	Op	2	4	4	2	2	2	1	4	2					27
AI2 アプリケーションソフトウェアの調達と保守		0	3	3		0	0	9	6	8	23	2	24	12	0	0	0	0	87
2.1 概要設計	ビジネス要件の概要設計仕様への変換			0	Op			2		2	4		4	2					14
2.2 詳細設計	詳細設計およびソフトウェアアプリケーションの技術的要件の策定		2	2	Op			2	2	2	4		4	2					18
2.3 業務処理統制および可監査性	設計における業務処理統制の組み込み			0	E			4	2		4		4	4					18
2.4 アプリケーションのセキュリティおよび可用性	調達した自動化機能のカスタマイズおよび導入			0	ー			2	2		4		4	2					14
2.5 調達したアプリケーションソフトウェアの構成および導入	アプリケーション開発プロセスの管理に関する正式化された方法論およびプロセスの策定		1	1	Or				2	2	3	2	4	2					16
2.6 既存システムの大幅なアップグレード	プロジェクトのソフトウェア品質保証計画の策定			0	Q			1		2	4		4	2					13
2.7 アプリケーションソフトウェアの開発	アプリケーション要件の追跡および管理			0	Q						4		4						8
2.8 ソフトウェアの品質保証	ソフトウェアアプリケーションの保守計画の策定		1	1	ー				2		4		2						9
2.9 アプリケーション要件の管理				0															0
2.10 アプリケーションソフトウェアの保守				0															0
AI3 技術インフラストラクチャの調達と保守		0	9	9		4	0	1	10	8	8	10	0	2	0	0	0	0	52
3.1 技術インフラストラクチャの調達計画	調達手続/プロセスの定義		3	3	Or	2			2	2	2	4		1					16
3.2 インフラストラクチャ資源の保護と可用性	インフラストラクチャの要件について承認済みのベンダーと協議		3	3	Or	2		1	4	2	2	4		1					19
3.3 インフラストラクチャの保守	インフラストラクチャの保守に関する戦略および計画の策定		3	3	Or				4	4	4	2							17
3.4 実現可能性テスト環境	インフラストラクチャコンポーネントを構成		3	3	ー				4	2				1					10
AI4 運用と利用の促進		0	5	5		0	0	6	4	0	4	0	0	1	6	6	0	0	32
4.1 運用上のソリューションの計画	ソリューションを運用可能にする戦略の作成		3	3	Op			3	4		4			1	4	2			21
4.2 ビジネス部門の管理者への知識の移転	知識移転の方法論の作成		2	2	E			3							2	4			11
4.3 エンドユーザへの知識の移転	エンドユーザ向けの手続マニュアルの作成			0	ー			4			4			2	2				12
4.4 運用スタッフおよびサポートスタッフへの知識の浸透	運用スタッフおよびサポートスタッフ向けの技術サポート文書の作成			0	ー				4		2			2					8
	研修の整備と実施			0	ー			3	3		4					4			14
	研修結果の評価と必要に応じた文書の改訂			0	ー			3	3						4	4			14
AI5 IT 資源の調達		7	9	16		6	0	0	9	1	9	16	4	6	0	0	0	0	67
5.1 調達のコントロール	会社レベルの調達ポリシーと整合されたIT 調達ポリシーおよび手続の策定	1	3	4	Or	2			1	1	1	4		2					15
5.2 サービスプロバイダとの契約の管理	認可されたサービスプロバイダのリストの作成/保守			0	Or							4							4
5.3 サービスプロバイダの選定	提案依頼(RFP)プロセスを使用したサービスプロバイダの評価および選定	2	3	5	Or	2			4		4	4	4	2					25
5.4IT 資源の調達	組織の利益を保護する契約の策定	4	3	7	Or	2			4		4	4		2					23
	確立された手続を遵守した調達		3	3	ー				4		4	4		2					17
AI6 変更管理		0	3	3		0	0	1	4	2	4	2	2	2	0	0	0	0	20
6.1 変更の標準と手続	変更要求の一貫した記録、評価、優先順位付けのための仕組みの策定および導入		3	3	Or			1	4	2	4	2	2	2					20
6.2 影響評価、優先順位付け、および認可	ビジネス上の必要性に基づく変更の影響評価および優先順位付け		1	1	ー			4	4	2	4	2	4	2					23
6.3 緊急変更	緊急変更や重要な変更の実施における、承認されたプロセスの遵守		1	1	ー			1	4	1	4			2					13
6.4 変更の状況追跡および報告	変更の承認		1	1	ー			2	4		4								11
6.5 変更の終了および文書化	変更の関連情報の管理と周知		3	3	ー			1	4	2	4	1	4	2					21
AI7 ソリューションおよびその変更の導入と認定				0															0
7.1 研修	導入計画の策定とレビュー		3	3	ー		2	1	2	2	4		2	2					18
7.2 テスト計画	テスト戦略(開始基準と終了基準)および運用テストの計画策定方法の確立およびレビュー		3	3	ー		2	2	2	2	4		2	2					19
7.3 導入計画	ビジネス要件および技術的要件のリポジトリと認定されたシステムのテストケースの作成と保守		3	3	ー						4								7
7.4 テスト環境	テスト環境におけるシステムの変換テストと統合テストの実施		1	1	ー		1	4	2	2	4		1	2					17
7.5 システムおよびデータの変換	テスト環境の準備および最終受け入れテストの実施		1	1	ー		1	4	3	2	4		1	2					18
7.6 変更のテスト	合意された認定基準に基づいた本番環境への移行の推奨		4	4	ー		1	3	4	2	4		1	2					21
7.7 最終受け入れテスト				0															0
7.8 本番環境への移行				0															0
7.9 導入後レビュー				0															0
DS1 サービスレベルの定義と管理		0	3	3		0	2	2	2	1	2	2	1	2	0	0	4	0	21

別紙 1

開発リスクマネジメント（RM）の要素…C：経営、Or：組織ガバナンス、R：IT リスク、E：拡張性、Op: 要件定義最適化、Q：品質重視
経営者関与ポイント…4 点（R）：実行責任者、3 点（A）：説明責任者、2 点（C）：協議先、1 点（I）：報告者

COBIT4.1版　コントロール目標	アクティビティ	CEO	CIO	CEO+CIO	開発RMの要素	CFO	企業幹部	ビジネスオーナー	OP責任者	設計責任者	開発責任者	IT管理責任者	PMO	コンプラ・監査・リスク・SEQ担当	導入チーム	研修部門	サービスインシデント構成問題管理担当	取締役会	合計
1.1 サービスレベル管理フレームワーク	IT サービス定義のためのフレームワークの策定		3	3	Or		2	2	2	1	2	2	1	2			4		21
1.2 サービスの定義	IT サービスカタログの作成		3	3	—		1	2	2	1	2	2	1	1			4		19
1.3 サービスレベル・アグリーメント	重要なIT サービスについてのSLA の定義		2	2	—	1	1	2	4	1	4	4	2	2			4		27
1.4 オペレーショナルレベル・アグリーメント	SLA 履行のためのOLA の定義		1	1	—			2	4	1	4	4	2	2			4		24
1.5 サービスレベル達成状況のモニタリングと報告	包括的なサービスレベル成果のモニタリングと報告		1	1	—			1	4		1	1		1			4		13
1.6 サービスレベル・アグリーメントおよび請負契約の見直し	SLA とその請負契約の見直し		1	1	—	1		2	4		4	4		2			4		22
	IT サービスカタログの見直しと更新		3	3	—		1	2	2	1	2	2	1	1			4		19
	サービス改善計画の策定		3	3	—		1	1	4	1	4	2	2	1			4		23
DS2 サードパーティのサービスの管理		0	10	10		5	0	5	14	3	14	15	8	8	0	0	0	0	82
2.1 すべてのサービスプロバイダとのリレーションシップの特定	サードパーティとのサービスのリレーションシップの特定と分類		1	1	Or			2	4	2	4	3	2	2					20
2.2 サービスプロバイダとのリレーションシップの管理	サービスプロバイダの管理プロセスの定義と文書化		3	3	Or	2		1	4	1	4	4	2	2					23
2.3 サービスプロバイダにかかわるリスクの管理	サービスプロバイダの評価および選定に関するポリシーと手続の確立		3	3	Or	2		2	2		2	4	2	2					19
2.4 サービスプロバイダの成果のモニタリング	サービスプロバイダにかかわるリスクの特定、評価および低減		3	3	Or	1			4		4	4	2	2					20
	サービスプロバイダからのサービス提供状況のモニタリング		4	4	—			3	4		4	4	2	2					23
	すべての利害関係者に対するサービスのリレーションシップの長期的達成目標の評価	2	4	6	—	2	2	2	2	2	2	4	2	2					26
DS3 性能とキャパシティの管理		0	11	11		0	0	5	20	4	12	10	9	3	0	0	0	0	74
3.1 性能とキャパシティの計画策定	IT 資源の性能とキャパシティのレビューに関する計画策定プロセスの確立		3	3	Or				4	2	2	2	2						15
3.2 現状の性能とキャパシティ	IT 資源の現行の性能とキャパシティのレビュー		2	2	Op			1	4		2	2	2						13
3.3 将来の性能とキャパシティ	IT 資源の性能とキャパシティの予測		2	2	Op			2	4	2	2	2	2						16
3.4 IT 資源の可用性	IT 資源に関する不適合を特定するギャップ分析の実施		2	2	Op			1	4		4	2	2	1					16
3.5 モニタリングと報告	IT 資源が利用不能になる潜在的リスクに備えた緊急時対応計画の策定		2	2	R			1	4		2	2	1	2					14
	IT 資源の可用性、性能とキャパシティの継続的なモニタリングと報告		1	1	—			1	4		1	1	1	1					10
DS4 継続的なサービスの保証		0	5	5		4	4	4	8	6	6	4	4	6	0	0	0	0	51
4.1 IT 継続フレームワーク	IT 継続フレームワークの作成		3	3	Or	2	2	2	4	4	4	2	2	4					29
4.2 IT 継続計画	事業影響分析とリスク評価の実施		2	2	R	2	2	2	4	2	2	2	2	2					22
4.3 重要なIT 資源	IT 継続計画の策定と保守	1	2	3	—	2	2	1	4		2	2	2	2					20
4.4 IT 継続計画の保守	復旧目標に基づくIT 資源の特定と分類		2	2	—				4		2	1	2	1					12
4.5 IT 継続計画のテスト	IT 継続計画を常に最新の状態で維持するための変更管理手続の策定と実施		1	1	—				4		4	4	4	1					18
4.6 IT 継続計画に関する研修	IT 継続計画の定期的なテスト		1	1	—			1	4		2	2	1	1					12
4.7 IT 継続計画の配付	テスト結果に基づく追加対応計画の作成		2	2	—			1	4	2	4	4	4	1					22
4.8 IT サービスの復旧および再開	IT 継続計画に関する訓練の計画と実施		1	1	—			4	4		2	4	1	1					17
4.9 遠隔地におけるバックアップ保管施設	IT サービスの復旧と再開の計画策定		2	2	—	1	1	2	4	2	4	4	4	2					26
4.10 再開後のレビュー	バックアップの保管と保護に関する計画の策定と実施		1	1	—				4		2	2	1	1					11
	再開後のレビュー実施手続の確立		2	2	—			1	4		2	2		2					13
DS5 システムセキュリティの保証		1	9	10		2	3	5	10	8	5	1	1	10	0	0	0	0	55
5.1 IT 財務管理フレームワーク	IT セキュリティ計画の定義と維持	1	3	4	R	2	2	2	2	2	2	1	1	4					22
5.2 IT セキュリティ計画	ID(アカウント)管理プロセスの定義・作成・運用		3	3	R		1	2	4	4	1			2					17
5.3 ID 管理	潜在的および実際のセキュリティインシデントのモニタリング		3	3	R			1	4	2	2			4					16
5.4 ユーザアカウントの管理	ユーザのアクセス権・特権の定期的見直しと確認		1	1	—			3	2					4					10
5.5 セキュリティのテスト、監視、モニタリング	暗号鍵の保持・保護のための手続作成と改訂		3	3	—				4			1		2					10
5.6 セキュリティインシデントの定義	ネットワーク間の情報フローを保護する技術的・手続的なコントロールの導入・維持		3	3	—			2	2	4	4			2					17
5.7 セキュリティ技術の保護	定期的な脆弱性評価の実施		3	3	—	1		1	2	2	2			4					15
5.8 暗号鍵の管理				0															0
5.9 不正ソフトウェアの阻止、発見、および是正				0															0
5.10 ネットワークのセキュリティ				0															0
5.11 機密データの交換				0															0
DS6 コストの捕捉と配賦		0	12	12		8	6	6	8	8	8	16	8	0	0	0	0	0	80
6.1 サービスの定義	提供サービス/サポートされているビジネスプロセスへのIT インフラストラクチャの対応付け		3	3	E	2	2	2	2	2	2	4	2						21
6.2 IT 財務管理	すべてのIT 費用(要員的費用、技術的費用など)の特定と、これらの費用のIT サービスへの単位原価での対応付け		3	3	E	2			2	2	2	4	2						17
6.3 コストモデルの策定とコスト請求	IT 会計および原価管理のプロセスの確立と保守		3	3	E	2	2	2	2	2	2	4	2						21
6.4 コストモデルの保守	課金に関するポリシーと手続の確立と保守		3	3	E	2	2	2	2	2	2	4	2						21
DS7 利用者の教育と研修		0	3	3		0	2	4	2	2	2	2	2	2	0	4	0	0	25
7.1 教育と研修のニーズの特定	ユーザの研修ニーズの特定とその分析		3	3	Op		2	4	2	2	2	2	2	2		4			25
7.2 教育と研修の実施	研修プログラムの作成		3	3	—		2	4	2	1	2	2	2	1		4			23
7.3 受講研修内容の評価	啓蒙活動と教育研修の実施		3	3	—		1	2	2	1	2	2	2	1		4			20
	研修評価の実施		3	3	—		1	4	2	1	2	2	2	1		4			22
	最良の研修実施方法およびツールの特定と評価		4	4	—		1	4	2	2	2	2	2	2		4			25
DS8 サービスデスクとインシデントの管理				0															0
8.1 サービスデスク	分類(重大度と影響力)とエスカレーション(機能と階層)の手続の作成		2	2	—			2	2	2	2	2		2			4		18
8.2 顧客からの問い合わせの登録	インシデント/サービス要求/情報要求の発見と記録			0	—												4		4
8.3 インシデントエスカレーション	問い合わせの分類、調査、および診断		1	1	—				2	2	2			1			4		12
8.4 インシデントのクローズ	インシデントの解決、回復、およびクローズ			0	—			1	4	4	4			2			4		19
8.5 傾向分析	ユーザへの通知(最新の進行状況など)		1	1	—			1									4		6
	マネジメントレポートの作成	1	1	2	—			1	1			1		1			4		10
DS9 構成管理				0															0
9.1 構成リポジトリとベースライン	構成管理の計画策定手続の作成			0	—			2	3	2	1	2		2			4		16
9.2 構成管理アイテムの特定と管理	初期構成情報の収集とベースラインの確立			0	—				2	2	2			1			4		11
9.3 構成のインテグリティのレビュー	構成情報の検証と監査(未承認ソフトウェアの発見を含む)			0	—	1			3			1		1			4		10
	構成管理用リポジトリの更新			0	—				4	4	4			1			4		17
DS10 問題管理				0															0
10.1 問題の特定と分類	問題の特定と分類		1	1	—		1	2	3	2	2			1			4		16
10.2 問題の追跡と解決	根本原因の分析の実施			0	—				2		2						4		8

別紙 1

開発リスクマネジメント（RM）の要素…C：経営、Or：組織ガバナンス、R：IT リスク、E：拡張性、Op: 要件定義最適化、Q：品質重視
経営者関与ポイント…4 点（R）：実行責任者、3 点（A）：説明責任者、2 点（C）：協議先、1 点（I）：報告者

COBIT4.1版　コントロール目標	アクティビティ	CEO	CIO	CEO+CIO	開発RMの要素	CFO	企業幹部	ビジネスオーナー	OP責任者	設計責任者	開発責任者	IT管理責任者	PMO	コンプラ・監査・リスク・SEC担当	導入チーム	研修部門	サービスインシデント構成問題管理担当	取締役会	合計
10.3 問題のクローズ	問題の解決			0	—			2	3	4	4		4	2			2		21
10.4 変更管理、構成管理、および問題管理の統合	問題の状況の確認		1	1	—		1	2	4	2	2		2	2			4		20
	改善のための提案事項の提示と関連する変更要求の作成			0	—			1	3	1	1		1				4		11
	問題の記録保持			0	—			1	1		1			1			4		8
DS11 データ管理				0															0
11.1 データ管理におけるビジネス要件	データの保管と保持に関する要件を取り入れた手続の定義		3	3	—			1	2	4				2					12
11.2 データの保管および保持の調整	メディアライブラリの管理手続の定義、維持、および導入		3	3	—				4	2	2	1		2					14
11.3 メディアライブラリ管理システム	メディアと機器の安全な廃棄手続の定義、保守、および導入		3	3	—			2	4			1		2					12
11.4 廃棄	計画に基づくデータのバックアップ		3	3	—				4										7
11.5 バックアップと復元	データ復元のための手続の定義、維持、および導入		3	3	—			2	4	2	2			1					14
11.6 データ管理におけるセキュリティ上の要件				0															0
DS12 物理的環境の管理		1	2	3		2	2	2	4	2	0	2	2	2	0	0	0	0	21
12.1 サイトの選定と配置	要求される物理的保護レベルの定義			0	—			2	4	2				2					10
12.2 物理的なセキュリティ対策	サイト(データセンター、オフィスなど)の選定と委託	1	2	3	Or	2	2	2	4	2		2	2	2					21
12.3 物理的アクセス	物理的環境に関する対策の実施			0	—			1	4	1	1			2					9
12.4 環境的要因からの保護	物理的環境の管理(保守、モニタリング、報告を含む)			0	—				4	2									6
12.5 物理的施設の管理	物理的アクセスを許可および維持する手続の定義と導入		2	2	—			1	4	1	1	1		2					12
DS13 オペレーション管理				0															0
13.1 オペレーション手続と指示	オペレーション手続(マニュアル、チェックリスト、シフト交代計画、引き継ぎ文書、エスカレーション手続など)の定義/変更			0	—				4					1					5
13.2 業務のスケジュール策定	作業負荷とバッチジョブのスケジュール策定			0	—			2	4	2	2								10
13.3 IT インフラストラクチャのモニタリング	インフラストラクチャと処理のモニタリングおよび問題の解決			0	—				4					1					5
13.4 機密文書と出力デバイス	物理アウトプット(紙、メディアなど)の管理と保護			0	—				4					2					6
13.5 ハードウェアの予防的保守	スケジュールとインフラストラクチャへの修正または変更の適用			0	—			2	4	2	2			2					12
	認証デバイスを侵害、損失、盗難から保護するためのプロセスの導入/確立		3	3	—				4			1		2					10
	予防的保守のスケジュール策定と実施			0	—				4										4
ME1 IT 成果のモニタリングと評価				0															0
1.1 モニタリングアプローチ	モニタリングアプローチの確立	3	4	7	—	4	2	1	2	1	2	1		2					22
1.2 モニタリングデータの定義と収集	ビジネス目標をサポートする測定可能な目標の特定と収集	2	3	5	—	2	2	4	4		4								21
1.3 モニタリング方法	スコアカードの作成		3	3	—				4	2	4	2							15
1.4 成果評価	成果の評価		3	3	—		1	4	4	2	4	2							20
1.5 取締役会およびマネジメント層への報告	成果の報告	1	3	4	—	1	4	4	4	2	4	2		1					26
1.6 是正措置	成果改善策の明確化とモニタリング		3	3	—			4	4	2	4	2		2					21
ME2 内部統制のモニタリングと評価				0															0
2.1 内部統制フレームワークのモニタリング	IT 内部統制活動のモニタリングとコントロール		3	3	—				4		4	4		4					19
2.2 監督レビュー	セルフ評価プロセスのモニタリング		3	3	—		1		4		4	4		2					18
2.3 コントロール例外事項	独立したレビュー、監査、および検査の成果のモニタリング		3	3	—		1		4		4	4		2					18
2.4 コントロールセルフ評価	サードパーティによるコントロールの確実性を保証するためのプロセスのモニタリング	1	3	4	—	1	1		4		4	4		2					20
2.5 内部統制の保証	コントロールの例外事項を特定し、評価するためのプロセスのモニタリング	1	3	4	—	1	1	1	4		4	4		2					21
2.6 サードパーティにおける内部統制	コントロールの例外事項を特定し、是正するためのプロセスのモニタリング	1	3	4	—	1	1	1	4		4	4		2					21
2.7 是正措置	主要な利害関係者への報告	1	4	5	—	1	1							1					8
ME3 外部要件に対するコンプライアンスの保証		0	4	4		0	0	2	1	1	1	2	1	4	0	0	0	0	16
3.1 外部法規制、および契約のコンプライアンス要件の特定	法律、契約、政策、および規制上の要件を特定するプロセスの策定と実行		4	4	R			2	1	1	1	2	1	4					16
3.2 外部要件への対応の最適化	IT のポリシー、標準、および手続に対するIT アクティビティのコンプライアンスの評価	1	4	5	—	1	1	1	4	4	4	4	4	4				1	33
3.3 外部要件に対するコンプライアンスの評価	IT のポリシー、標準、および手続に対するIT アクティビティのコンプライアンスの積極的な保証に関する報告		4	4	—			2	2	2	2	2	2	4					20
3.4 コンプライアンスの積極的な保証	コンプライアンス要件に応じて、IT のポリシー、計画、および手続を整合するインプットの提供		4	4	—			2	2	2	2	2		4					18
3.5 報告の統合	法的要件に関するIT 部門の報告と、その他のビジネス部門からの類似報告との統合		4	4	—				1	1	1	4	1	4					16
ME4 IT ガバナンスの提供		18	14	32		9	7	2	3	3	3	3	3	14	0	0	0	0	79
4.1 IT ガバナンスフレームワークの確立	経営層と取締役会によるIT アクティビティに対する監督と推進の確立	4	2	6	Or	2	2							2					12
4.2 戦略との整合	IT 成果、IT 戦略、資源とリスクの管理のビジネス戦略との整合、レビュー、承認、および周知	4	4	8	Or	1	1							2					12
4.3 価値の提供	成果、およびポリシー、計画、手続へのコンプライアンスに関する独立した定期評価の実施	4	2	6	Or	2	1		1	1	1	1	1	4					18
4.4 資源の管理	独立した評価による検出事項の解決、およびマネジメント層による合意された改善案の確実な実施	4	2	6	Or	2	1		1	1	1	1	1	4					18
4.5 リスクの管理	IT ガバナンス報告の作成	2	4	6	Or	2	2	2	1	1	1	1	1	2					19
4.6 成果の測定																			0
4.7 独立した保証																			0

別紙２

開発リスクマネジメント（RM）の要素…C：経営、Or：組織ガバナンス、R：IT リスク、E：拡張性、Op: 要件定義最適化、Q：品質重視
経営者関与ポイント…4 点（R）：実行責任者、３点（A）：説明責任者、２点（C）：協議先、１点（I）：報告者

システム管理基準	CEO	CIO	CEO+CIO	CFO	企業幹部	開発RMの要素
Ⅰ. 情報戦略(47)						
1. 全体最適化(18)	7	11	18	6	9	
1.1 全体最適化の方針・目標(6)	4	4	8	2	2	C
(1)ITガバナンスの方針を明確にすること。						
(2)情報化投資及び情報化構想の決定における原則を定めること。						
(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すること。						
(4)組織体全体の情報システムのあるべき姿を明確にすること。						
(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すること。						
(6)情報セキュリティ基本方針を明確にすること。						
1.2 全体最適化計画の承認(3)	2	4	6	2	4	Or
(1)全体最適化計画の立案体制は、組織体の長の承認を得ること。						
(2)全体最適化計画は、組織体の長の承認を得ること。						
(3)全体最適化計画は、利害関係者の合意を得ること。						
1.3 全体最適化計画の策定(7)	1	3	4	2	3	Or
(1)全体最適化計画は、方針及び目標に基づいていること。						
(2)全体最適化計画は、コンプライアンスを考慮すること。						
(3)全体最適化計画は、情報化投資の方針及び確保すべき経営資源を明確にすること。						
(4)全体最適化計画は、投資効果及びリスク算定の方法を明確にすること。						
(5)全体最適化計画は、システム構築及び運用のための標準化及び品質方針を含めたルールを明確にすること。						
(6)全体最適化計画は、個別の開発計画の優先順位及び順位付けのルールを明確にすること。						
(7)全体最適化計画は、外部資源の活用を考慮すること。						
1.4 全体最適化計画の運用(2)	1	3	4	1	1	−
(1)全体最適化計画は、関係者に周知徹底すること。						
(2)全体最適化計画は、定期的及び経営環境等の変化に対応して見直すこと。						
2. 組織体制(9)	6	11	17	4	3	
2.1 情報システム化委員会(5)	2	3	5	2	2	Or
(1)全体最適化計画に基づき、委員会の使命を明確にし、適切な権限及び責任を与えること。						
(2)委員会は、組織体における情報システムに関する活動全般について、モニタリングを実施し、必要に応じて是正措置を講じること。						
(3)委員会は、情報技術の動向に対応するため、技術採用指針を明確にすること。						
(4)委員会は、活動内容を組織体の長に報告すること。						
(5)委員会は、意思決定を支援するための情報を組織体の長に提供すること。						
2.2 情報システム部門(2)	2	4	6	1		Or
(1)情報システム部門の使命を明確にし、適切な権限及び責任を与えること。						
(2)情報システム部門は、組織体規模及び特性に応じて、職務の分離、専門化、権限付与、外部委託等を考慮した体制にすること。						
2.3 人的資源管理の方針(2)	2	4	6	1	1	Or
(1)情報技術に関する人的資源の現状及び必要とされる人材を明確にすること。						
(2)人的資源の調達及び育成の方針を明確にすること。						
3. 情報化投資(6)	2	4	6	4	4	E
(1)情報化投資計画は、経営戦略との整合性を考慮して策定すること。						
(2)情報化投資計画の決定に際して、影響、効果、期間、実現性等の観点から複数の選択肢を検討すること。						
(3)情報化投資に関する予算を適切に執行すること。						
(4)情報化投資に関する投資効果の算出方法を明確にすること。						
(5)情報システムの全体的な業績及び個別のプロジェクトの業績を財務的な観点から評価し、問題点に対して対策を講じること。						
(6)投資した費用が適正に使用されたことを確認すること。						
4. 情報資産管理の方針(4)	1	3	4	2		Op
(1)情報資産の管理方針及び体制を明確にすること。						
(2)情報資産のリスク分析を行い、その対応策を考慮すること。						
(3)情報資産の効率的で有効な活用を考慮すること。						
(4)情報資産の共有化による生産性向上を考慮すること。						
5. 事業継続計画(5)	2	4	6	2	4	R
(1)情報システムに関連した事業継続の方針を策定すること。						
(2)事業継続計画は、利害関係者を含んだ組織的体制で立案し、組織体の長が承認すること。						
(3)事業継続計画は、従業員の教育訓練の方針を明確にすること。						
(4)事業継続計画は、関係各部に周知徹底すること。						
(5)事業継続計画は、必要に応じて見直すこと。						
6. コンプライアンス(5)	2	2	4	2	4	R
(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)情報倫理規程を定め、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程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。						
Ⅱ. 企画業務(23)						
1. 開発計画(9)	2	3	5	2	3	Op
(1)開発計画は、組織体の長が承認すること。						
(2)開発計画は、全体最適化計画との整合性を考慮して策定すること。						
(3)開発計画は、目的、対象業務、費用、スケジュール、開発体制、投資効果等を明確にすること。						
(4)開発計画は、関係者の教育及び訓練計画を明確にすること。						
(5)開発計画は、ユーザ部門及び情報システム部門の役割分担を明確にすること。						
(6)開発計画は、開発、運用及び保守の費用の算出基礎を明確にすること。						
(7)開発計画はシステムライフを設定する条件を明確にすること。						
(8)開発計画の策定に当たっては、システム特性及び開発の規模を考慮して形態及び開発方法を決定すること。						
(9)開発計画の策定に当たっては、情報システムの目的を達成する実現可能な代替案を作成し、検討すること。						
2. 分析(8)	1	3	4		3	Op
(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すること。						
(2)ユーザニーズの調査は、対象、範囲及び方法を明確にすること。						
(3)実務に精通しているユーザ、開発、運用及び保守の担当者が参画して現状分析を行うこと。						
(4)ユーザニーズは文書化し、ユーザ部門が確認すること。						
(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すること。						
(6)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、諸規程等は、見直し等の検討を行うこと。						
(7)情報システムの導入効果の定量的及び定性的評価を行うこと。						
(8)パッケージソフトウェアの使用に当たっては、ユーザニーズとの適合性を検討すること。						

別紙２

開発リスクマネジメント（RM）の要素…C：経営、Or：組織ガバナンス、R：IT リスク、E：拡張性、Op: 要件定義最適化、Q：品質重視
経営者関与ポイント…4 点（R）：実行責任者、3 点（A）：説明責任者、2 点（C）：協議先、1 点（I）：報告者

システム管理基準	CEO	CIO	CEO+CIO	CFO	企業幹部	開発RMの要素
3．調達（6）	1	3	4	2	2	E
(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すること。						
(2)ソフトウェア、ハードウェア及びネットワークは、調達の要求事項を基に選択すること。						
(3)開発を遂行するために必要な要員、予算、設備、期間等を確保すること。						
(4)要員に必要なスキルを明確にすること。						
(5)ソフトウェア、ハードウェア及びネットワークの調達は、ルールに従って実施すること。						
(6)調達した資源は、ルールに従って管理すること。						
Ⅲ．開発業務（49）						
1．開発手順（4）		2	2		1	Op
(1)開発手順は、開発の責任者が承認すること。						
(2)開発手順は、開発方法に基づいて作成すること。						
(3)開発手順は、開発の規模、システム特性等を考慮して決定すること。						
(4)開発時のリスクを評価し、必要な対応策を講じること。						
2．システム設計（15）		2	2		1	Op
(1)システム設計書は、ユーザ、開発、運用及び保守の責任者が承認すること。						
(2)運用及び保守の基本方針を定めて設計すること。						
(3)入出力画面、入出力帳票等はユーザの利便性を考慮して設計すること。						
(4)データベースは、業務の内容及びシステム特性に応じて設計すること。						
(5)データのインテグリティを確保すること。						
(6)ネットワークは、業務の内容及びシステム特性に応じて設計すること。						
(7)情報システムの性能は、要求定義を満たすこと。						
(8)情報システムの運用性及び保守性を考慮して設計すること。						
(9)他の情報システムとの整合性を考慮して設計すること。						
(10)情報システムの障害対策を考慮して設計すること。						
(11)誤謬防止、不正防止、機密保護等を考慮して設計すること。						
(12)テスト計画は、目的、範囲、方法、スケジュール等を明確にすること。						
(13)情報システムの利用に係る教育の方針、スケジュール等を明確にすること。						
(14)モニタリング機能を考慮して設計すること。						
(15)システム設計書をレビューすること。						
3．プログラム設計（5）		1	1			―
(1)プログラム設計書は、開発の責任者が承認すること。						
(2)システム設計書に基づいて、プログラムを設計すること。						
(3)テスト要求事項を定義し、文書化すること。						
(4)プログラム設計書及びテスト要求事項をレビューすること。						
(5)プログラム設計時に発見したシステム設計の矛盾は、システム設計の再検討を行って解決すること。						
4．プログラミング（4）		1	1			―
(1)プログラム設計書に基づいてプログラミングすること。						
(2)プログラムコードはコーディング標準に適合していること。						
(3)プログラムコード及びプログラムテスト結果を評価し、記録及び保管すること。						
(4)重要プログラムは、プログラム作成者以外の者がテストすること。						
5．システムテスト・ユーザ受入れテスト（13）		2	2		2	―
(1)システムテスト計画は、開発及びテストの責任者が承認すること。						
(2)ユーザ受入れテスト計画は、ユーザ及び開発の責任者が承認すること。						
(3)システムテストに当たっては、システム要求事項を網羅してテストケースを設定して行うこと。						
(4)テストデータの作成及びシステムテストは、テスト計画に基づいて行うこと。						
(5)システムテストは、本番環境と隔離された環境で行うこと。						
(6)システムテストは、開発当事者以外の者が参画すること。						
(7) システムテストは、適切なテスト手法及び標準を使用すること。						
(8)ユーザ受入れテストは、本番同様の環境を設定すること。						
(9)ユーザ受入れテストは、ユーザマニュアルに従い、本番運用を想定したテストケースを設定して実施すること。						
(10)ユーザ受入れテストは、ユーザ及び運用の担当者もテストに参画して確認すること。						
(11)システムテスト及びユーザ受入れテストの結果は、ユーザ、開発、運用及び保守の責任者が承認すること。						
(12)システムテスト及びユーザ受入れテストの経過及び結果を記録及び保管すること。						
(13)パッケージソフトウェアを調達する場合、開発元が品質テストを実施したことを確認すること。						
6．移行（8）		2	2		2	―
(1)移行計画を策定し、ユーザ、開発、運用及び保守の責任者が承認すること。						
(2)移行作業は文書に記録し、責任者が承認すること。						
(3)移行完了の検証方法を移行計画で明確にすること。						
(4)移行計画に基づいて、移行に必要な要員、予算、設備等を確保すること。						
(5)移行は手順書を作成し、実施すること。						
(6)移行時のリスク対策を検討すること。						
(7)運用及び保守に必要なドキュメント、各種ツール等は開発の責任者から引き継いでいること。						
(8)移行は関係者に周知徹底すること。						
Ⅳ．運用業務（73）						
1．運用管理ルール（4）		1	1			―
(1)運用管理ルール及び運用手順は、運用の責任者が承認すること。						
(2)運用管理ルールは、運用設計に基づいて作成すること。						
(3)運用手順は、運用設計及び運用管理ルールに基づいて、規模、期間、システム特性等を考慮して作成すること。						
(4)運用設計及び運用管理ルールに基づいて、担当責任者を定めること。						
2．運用管理（16）		1	1		1	―
(1)年間運用計画を策定し、責任者が承認すること。						
(2)年間運用計画に基づいて、月次、日次等の運用計画を策定すること。						
(3)運用管理ルールを遵守すること。						
(4)ジョブスケジュールは、業務処理の優先度を考慮して設定すること。						
(5)オペレーションは、ジョブスケジュール及び指示書に基づいて行うこと。						
(6)例外処理のオペレーションは、運用管理ルールに基づいて行うこと。						
(7)オペレータの交替は、運用管理ルールに基づいて行うこと。						
(8)ジョブスケジュール及びオペレーション実施記録を採り、ジョブスケジュールとの差異分析を行うこと。						
(9)オペレーション実施記録は、運用管理ルールに基づいて一定期間保管すること。						
(10)事故及び障害の影響度に応じた報告体制及び対応手順を明確にすること。						
(11)事故及び障害の内容を記録し、情報システムの運用の責任者に報告すること。						
(12)事故及び障害の原因を究明し、再発防止の措置を講じること。						
(13)情報システムのユーザに対する支援体制を確立すること。						
(14)情報セキュリティに関する教育及び訓練をユーザに対して実施すること。						

別紙２

開発リスクマネジメント（RM）の要素…C：経営、Or：組織ガバナンス、R：IT リスク、E：拡張性、Op: 要件定義最適化、Q：品質重視
経営者関与ポイント…4 点（R）：実行責任者、3 点（A）：説明責任者、2 点（C）：協議先、1 点（I）：報告者

システム管理基準	CEO	CIO	CEO+CIO	CFO	企業幹部	開発RMの要素
(15)情報システムの稼動に関するモニタリング体制を確立すること。						
(16)情報システムの稼動実績を把握し、性能管理及び資源の有効利用を図ること。						
3. 入力管理(5)		1	1			－
(1)入力管理ルールを定め、遵守すること。						
(2)データの入力は、入力管理ルールに基づいて漏れなく、重複なく、正確に行うこと。						
(3)入力データの作成手順、取扱い等は誤謬防止、不正防止、機密保護等の対策を講じること。						
(4)データの入力の誤謬防止、不正防止、機密保護等の対策は有効に機能すること。						
(5)入力データの保管及び廃棄は、入力管理ルールに基づいて行うこと。						
4. データ管理(10)		1	1			－
(1)データ管理ルールを定め、遵守すること。						
(2)データへのアクセスコントロール及びモニタリングは、有効に機能すること。						
(3)データのインテグリティを維持すること。						
(4)データの利用状況を記録し、定期的に分析すること。						
(5)データのバックアップの範囲、方法及びタイミングは、業務内容、処理形態及びリカバリの方法を考慮して決定すること。						
(6)データの授受は、データ管理ルールに基づいて行うこと。						
(7)データの交換は、不正防止及び機密保護の対策を講じること。						
(8)データの保管、複写及び廃棄は、誤謬防止、不正防止及び機密保護の対策を講じること。						
(9)データに対するコンピュータウイルス対策を講じること。						
(10)データの知的財産権を管理すること。						
5. 出力管理(7)		1	1			－
(1)出力管理ルールを定め、遵守すること。						
(2)出力情報は、漏れなく、重複なく、正確であることを確認すること。						
(3)出力情報の作成手順、取扱い等は、誤謬防止、不正防止及び機密保護の対策を講じること。						
(4)出力情報の引渡しは、出力管理ルールに基づいて行うこと。						
(5)出力情報の保管及び廃棄は、出力管理ルールに基づいて行うこと。						
(6)出力情報のエラー状況を記録し、定期的に分析すること。						
(7)出力情報の利用状況を記録し、定期的に分析すること。						
6. ソフトウェア管理(9)		1	1			－
(1)ソフトウェア管理ルールを定め、遵守すること。						
(2)ソフトウェアへのアクセスコントロール及びモニタリングは、有効に機能すること。						
(3)ソフトウェアの利用状況を記録し、定期的に分析すること。						
(4)ソフトウェアのバックアップの範囲、方法及びタイミングは、業務内容及び処理形態を考慮して決定すること。						
(5)ソフトウェアの授受は、ソフトウェア管理ルールに基づいて行うこと。						
(6)ソフトウェアの保管、複写及び廃棄は、不正防止及び機密保護の対策を講じること。						
(7)ソフトウェアに対するコンピュータウイルス対策を講じること。						
(8)ソフトウェアの知的財産権を管理すること。						
(9)フリーソフトウェアの利用に関し、組織体としての方針を明確にすること。						
7. ハードウェア管理(6)		1	1			－
(1)ハードウェア管理ルールを定め、遵守すること。						
(2)ハードウェアは、想定されるリスクに対応できる環境に設置すること。						
(3)ハードウェアは、定期的に保守を行うこと。						
(4)ハードウェアは、障害対策を講じること。						
(5)ハードウェアの利用状況を記録し、定期的に分析すること。						
(6)ハードウェアの保管、移設及び廃棄は、不正防止及び機密保護の対策を講じること。						
8. ネットワーク管理(6)		1	1			－
(1)ネットワーク管理ルールを定め、遵守すること。						
(2)ネットワークへのアクセスコントロール及びモニタリングは、有効に機能すること。						
(3)ネットワーク監視ログを定期的に分析すること。						
(4)ネットワークは、障害対策を講じること。						
(5)ネットワークの利用状況を記録し、定期的に分析すること。						
(6)ネットワークを利用したサービスについて、組織体としての方針を明確にすること。						
9. 構成管理(4)		1	1			－
(1)管理すべきソフトウェア、ハードウェア及びネットワークの対象範囲を明確にし、管理すること。						
(2)ソフトウェア、ハードウェア及びネットワークの構成、調達先、サポート条件等を明確にすること。						
(3)ソフトウェア、ハードウェア及びネットワークの導入並びに変更は、影響を受ける範囲を検討して決定すること。						
(4)ソフトウェア、ハードウェア及びネットワークの導入並びに変更は、計画的に実施すること。						
10. 建物・関連設備管理(6)		1	1			－
(1)建物及び関連設備は、想定されるリスクに対応できる環境に設置すること。						
(2)建物及び室への入退の管理は、不正防止及び機密保護の対策を講じること。						
(3)関連設備は、適切な運用を行うこと。						
(4)関連設備は、定期的に保守を行うこと。						
(5)関連設備は、障害対策を講じること。						
(6)建物及び室への入退の管理を記録し、定期的に分析すること。						
Ⅴ. 保守業務(19)						
1. 保守手順(3)		1	1		1	－
(1)保守ルール及び保守手順は、保守の責任者が承認すること。						
(2)保守手順は、保守の規模、期間、システム特性等を考慮して決定すること。						
(3)保守時のリスクを評価し、必要な対応策を講じること。						
2. 保守計画(3)		2	2		2	－
(1)保守計画はユーザ及び保守の責任者が承認すること。						
(2)変更依頼等に対し、保守の内容及び影響範囲の調査並びに分析を行うこと。						
(3)保守のテスト計画は、目的、範囲、方法、スケジュール等を明確にすること。						
3. 保守の実施(3)		1	1		1	－
(1)システム設計書、プログラム設計書等は、保守計画に基づいて変更し、ユーザ及び保守の責任者が承認すること。						
(2)プログラムの変更は、保守手順に基づき、保守の責任者の承認を得て実施すること。						
(3)変更したプログラム設計書に基づいてプログラミングしていることを検証すること。						
4. 保守の確認(5)		1	1		1	－
(1)変更したプログラムのテストの実施は、保守のテスト計画に基づいて行うこと。						
(2)変更したプログラムは、影響範囲を考慮してテストを行うこと。						
(3)変更したプログラムのテストは、ユーザが参画し、ユーザマニュアルに基づいて実施すること。						
(4)変更したプログラムのテストの結果は、ユーザ、運用及び保守の責任者が承認すること。						
(5)変更したプログラムのテストの結果を記録及び保管すること。						
5. 移行(3)		1	1		1	－
(1)移行手順は、移行の条件を考慮して作成すること。						

別紙２

開発リスクマネジメント（RM）の要素…C：経営、Or：組織ガバナンス、R：IT リスク、E：拡張性、Op: 要件定義最適化、Q：品質重視
経営者関与ポイント…4 点（R）：実行責任者、3 点（A）：説明責任者、2 点（C）：協議先、1 点（I）：報告者

システム管理基準	CEO	CIO	CEO+CIO	CFO	企業幹部	開発RMの要素
(2)変更前のプログラム及びデータのバックアップを行うこと。						
(3)運用及び保守の責任者は、他の情報システムへ影響を与えないことを確認すること。						
6. 情報システムの廃棄(2)		1	1		1	ー
(1)旧情報システムは、リスクを考慮して廃棄計画を策定し、ユーザ、運用及び保守の責任者の承認を得て廃棄すること。						
(2)旧情報システムの廃棄方法及び廃棄時期は、不正防止及び機密保護の対策を考慮して決定すること。						
Ⅵ. 共通業務(76)						
1. ドキュメント管理(9)	0	2	2	0	2	
1.1 作成(5)		1	1		1	Or
(1)ドキュメントは、ユーザ部門及び情報システム部門の責任者が承認すること。						
(2)ドキュメント作成ルールを定め、遵守すること。						
(3)ドキュメントの作成計画を策定すること。						
(4)ドキュメントの種類、目的、作成方法等を明確にすること。						
(5)ドキュメントは、作成計画に基づいて作成すること。						
1.2 管理(4)		1	1		1	Or
(1)ドキュメントの更新内容は、ユーザ部門及び情報システム部門の責任者が承認すること。						
(2)ドキュメント管理ルールを定め、遵守すること。						
(3)情報システムの変更に伴い、ドキュメントの内容を更新し、更新履歴を記録すること。						
(4)ドキュメントの保管、複写及び廃棄は、不正防止及び機密保護の対策を講じること。						
2. 進捗管理(6)	1	3	4	1	2	
2.1 実施(3)						Or
(1)進捗計画に基づいて方法、体制等を定め、ユーザ、企画、開発、運用及び保守の責任者が承認すること。						
(2)ユーザ、企画、開発、運用及び保守の責任者は、進捗状況を把握すること。						
(3)進捗の遅延等の対策を講じること。						
2.2 評価(3)						Or
(1)業務の工程終了時に、計画に対する実績を分析及び評価し、責任者が承認すること。						
(2)評価結果は、次工程の計画に反映すること。						
(3)評価結果は、進捗管理の方法、体制等の改善に反映すること。						
3. 品質管理(4)	1	3	4	1	1	
3.1 計画(2)	1	2	3	1	1	Q
(1)品質目標に基づいて品質管理の計画を定め、ユーザ、企画、開発、運用及び保守の責任者が承認すること。						
(2)品質管理計画は、方法、体制等を明確にすること。						
3.2 実施(2)		1	1			Q
(1)業務の工程終了時に、計画に対する実績を分析及び評価し、責任者が承認すること。						
(2)評価結果は、品質管理の基準、方法、体制等の改善に反映すること。						
4. 人的資源管理(13)	1	8	9	2	2	
4.1 責任・権限(3)	1	3	4	2	2	Or
(1)要員の責任及び権限は、業務の特性及び業務遂行上の必要性に応じて定めること。						
(2)要員の責任及び権限は、業務環境及び情報環境の変化に対応した見直しを行うこと。						
(3)要員の責任及び権限を周知徹底すること。						
4.2 業務遂行(4)		1	1			Or
(1)要員は、権限を遵守すること。						
(2)作業分担及び作業量は、要員の知識、能力等から検討すること。						
(3)要員の交替は、誤謬防止、不正防止及び機密保護を考慮して行うこと。						
(4)不測の事態に備えた代替要員の確保を検討すること。						
4.3 教育・訓練(4)		2	2			Or
(1)教育及び訓練に関する計画及びカリキュラムは、人的資源管理の方針に基づいて作成及び見直しを行うこと。						
(2)教育及び訓練に関する計画及びカリキュラムは、技術力の向上、業務知識の習得、情報システムの情報セキュリティ確保等から検討すること。						
(3)教育及び訓練は、計画及びカリキュラムに基づいて定期的かつ効果的に行うこと。						
(4)要員に対するキャリアパスを確立し、業務環境及び情報環境の変化に対応した見直しを行うこと。						
4.4 健康管理(2)		2	2			Or
(1)健康管理を考慮した作業環境を整えること。						
(2)健康診断及びメンタルヘルスケアを行うこと。						
5. 委託・受託(25)	2	8	10	5	2	
5.1 計画(3)	1	3	4	2	1	Or
(1)委託又は受託の計画は全体最適化計画に基づいて策定し、責任者が承認すること。						
(2)委託又は受託の目的、対象範囲、予算、体制等を明確にすること。						
(3)委託又は受託は、具体的な効果、問題点等を評価して決定すること。						
5.2 委託先選定(3)	1	2	3	2	1	Or
(1)委託先の選定基準を明確にすること。						
(2)委託候補先に必要な要求仕様を提示すること。						
(3)委託候補先が提示した提案書の比較検討を行うこと。						
5.3 契約(8)		1	1	1		Or
(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にすること。						
(3)再委託の可否について明確にすること。						
(4)知的財産権の帰属を明確にすること。						
(5)特約条項及び免責条項を明確にすること。						
(6)業務内容及び責任分担を明確にすること。						
(7)契約締結後の業務内容に追加及び変更が生じた場合、契約内容の再検討を行うこと。						
(8)システム監査に関する方針を明確にすること。						
5.4 委託業務(7)		1	1			Or
(1)委託業務の実施内容は、契約内容と一致すること。						
(2)契約に基づき、必要な要求仕様、データ、資料等を提供すること。						
(3)委託業務の進捗状況を把握し、遅延対策を講じること。						
(4)委託先における誤謬防止、不正防止、機密保護等の対策の実施状況を把握し、必要な措置を講じること。						
(5)成果物の検収は、委託契約に基づいて行うこと。						
(6)業務終了後、委託業務で提供したデータ、資料等の回収及び廃棄の確認を行うこと。						
(7)委託した業務の結果を分析及び評価すること。						
5.5 受託業務(4)		1	1			Or
(1)受託業務の実施内容は、契約内容を遵守すること。						
(2)受託内容の進捗状況を把握し、リスク対策を講じること。						
(3)成果物の品質管理を行うこと。						
(4)契約に基づき、受託業務終了後、提供されたデータ、資料、機材等を返却又は廃棄すること。						
6. 変更管理(6)	0	4	4			

別紙２

開発リスクマネジメント（RM）の要素…C：経営、Or：組織ガバナンス、R：IT リスク、E：拡張性、Op: 要件定義最適化、Q：品質重視
経営者関与ポイント…4 点（R）：実行責任者、3 点（A）：説明責任者、2 点（C）：協議先、1 点（I）：報告者

システム管理基準	CEO	CIO	CEO+CIO	CFO	企業幹部	開発RMの要素
6.1 管理（3）		3	3			Or
(1)変更管理ルールを定め、ユーザ、開発及び保守の責任者が承認すること。						
(2)仕様変更、問題点、ペンディング事項等の変更管理案件が生じた場合、他システムの影響を考慮して決定すること。						
(3)変更管理案件は、提案から完了までの状況を管理し、未完了案件は定期的に分析すること。						
6.2 実施（3）		1	1			Or
(1)変更管理案件は、変更管理ルールに従って実施すること。						
(2)変更管理案件を実施した場合に、関連する情報システムの環境も同時に変更すること。						
(3)変更の結果は、ユーザ、開発、運用及び保守の責任者が承認すること。						
7．災害対策（13）	4	5	9	4	2	
7.1 リスク分析（3）	2	3	5	2	1	R
(1)地震等のリスク及び情報システムに与える影響範囲を明確にすること。						
(2)情報システムの停止等により組織体が被る損失を分析すること。						
(3)業務の回復許容時間及び回復優先順位を定めること。						
7.2 災害時対応計画（6）	2	2	4	2	1	R
(1)リスク分析の結果に基づき、事業継続計画と整合をとった災害時対応計画を策定すること。						
(2)災害時対応計画は、組織体の長が承認すること。						
(3)災害時対応計画の実現可能性を確認すること。						
(4)災害時対応計画は、従業員の教育訓練の方針を明確にすること。						
(5)災害時対応計画は、関係各部に周知徹底すること。						
(6)災害時対応計画は、必要に応じて見直すこと。						
7.3 バックアップ（2）	2	3	5	2	1	−
(1)情報システム、データ及び関連設備のバックアップ方法並びに手順は、業務の回復目標に対応して定めること。						
(2)運用の責任者は、バックアップ方法及び手順を検証すること。						
7.4 代替処理・復旧（2）	2	2	4	2	1	−
(1)ユーザ及び運用の責任者は、復旧までの代替処理手続き及び体制を定め、検証すること。						
(2)ユーザ及び運用の責任者は、復旧手続き及び体制を定め、検証すること。						

別紙３
金融機関等のシステム監査指針：チェックポイント集一覧表

開発リスクマネジメント（RM）の要素…C：経営、Or：組織ガバナンス、R：IT リスク、E：拡張性、Op: 要件定義最適化、Q：品質重視
経営者関与ポイント…4 点（R）：実行責任者、3 点（A）：説明責任者、2 点（C）：協議先、1 点（I）：報告者

要点項目	大項目	小項目	経営者				開発RMの要素	システム監査対象部門					システム監査の着眼点				
			CEO	CIO	CFO	企業幹部（ユーザー部門）		情報システム部門			本部各部門	利用部門	有効性	効率性	信頼性	安全性	遵守性
								企画	開発	運用							
1.情報システムの計画と管理(11)	1.情報システム戦略	A.経営戦略に沿った情報システム戦略の策定	2	4	1	2	C	◎			○		◎				
		B.情報システム運営委員会	2	3	2	2	C	◎	○	○	○	○	◎				
	2.全社的な情報システム組織	A.情報システム部門の組織	2	3	2	2	Or	◎	○	○			◎	○	○	○	○
		B.ユーザー部門等の組織体制	2	3	2	2	Or				◎	◎	◎	○	○	○	○
	3.情報システム計画	A.情報システム中長期計画の策定	3	4	2	2	Or	◎			○		◎	○			
		B.情報システム短期計画の策定と実施	2	3	1	1	Or	◎			○		◎	○			
	4.有効性評価	A.情報システム部門における評価					―	◎	○	○			◎	○	○	○	○
		B.ユーザー部門等における評価					―				◎	◎	◎	○	○	○	○
	5.最新技術の調査と研究	A.最新技術の調査と研究		3	1	1	Op	◎	○	○	○		◎	○	○	○	○
	6.投資及び予算管理	A.予算計画の策定	1	3	2	2	E	◎	○	○			○	◎			
		B.実績管理					―	◎	○	○			○	◎			
	合計		14	26	13	14											
2.情報システムリスクの管理(5)	1.情報システムリスクの管理	A.情報システムリスク管理体制	1	4	2	1	R	◎	○	○	◎		○	○	○	◎	○
		B.情報システムリスクの識別と評価	3	2	4	2	R	◎	○	○	◎		○	○	○	◎	○
		C.情報システムリスク対策	1	4	1	1	R	◎	○	○	◎		○	○	○	◎	○
	2.法令遵守	A.法令・規制の遵守	1	4	1	1	R	◎	○	○	◎	○					◎
	3.情報システムの最新技術及び金融犯罪の動向に関する調査と研究	A.情報システムの最新技術及び金融犯罪の動向に関する調査と研究	1	3			Op	◎	○	○	◎		○	○	○	◎	○
	合計		7	17	8	5											
3.情報セキュリティ(20)	1.全社的なセキュリティ管理体制	A.セキュリティポリシー	1	3	2	2	R	◎	○	○	◎	○				◎	○
		B.セキュリティスタンダード	1	3	2	2	R	◎	○	○	◎	○				◎	○
		C.セキュリティ管理体制	1	3	2	2	R	◎	○	○	◎	○				◎	
		D.セキュリティ教育・研修		3		2	Op	◎	○	○	◎	○				◎	
		E.障害・事故・犯罪等の対応					―	○	○	◎	○	○				◎	
	2.建物・設備等の安全対策	A.建物・設備等の安全対策		1		1	R	○	○	◎	○	○				◎	
		B.入退館(室)管理		1		1	R	○	○	◎	○	○				◎	
	3.パソコン、サーバー等の管理	A.パソコン等の管理					―	◎	◎	◎	◎	◎				◎	
		B.サーバーの管理					―	◎	◎	◎	◎	◎				◎	
	4.機密情報管理	A.機密情報の管理					―		◎	○	○					◎	
		B.機密情報の暗号化					―		◎	○						◎	
		C.暗号鍵の管理					―	○	◎	○	○	○				◎	
	5.アクセスコントロール	A.アクセスコントロールの方針と手続き					―	○	◎							◎	○
		B.アクセスコントロール設計					―		◎							◎	
		C.ユーザーIDの管理					―	◎	◎	◎	◎	◎				◎	○
		D.パスワード管理					―	◎	◎	◎	◎	◎				◎	○
		E.アクセスの監視					―			◎						◎	
	6.コンピュータウイルス等不正プログラム対策	A.コンピュータウイルス等不正プログラム対策	1	3			R	◎	◎	◎	◎	◎				◎	
	7.顧客データ保護	A.顧客データ管理					―	○	○	◎	○	○				◎	○
		B.個人データの取扱方針と管理	1	2		2	R	○	○	◎	○	○				◎	○
	合計		5	19	6	12											
4.システム開発(26)	1.運営と要員管理	A.職務の分離		3	1	1	R		◎							◎	
		B.システム開発業務の運営管理	1	2			Or		◎					◎	○		
		C.システム開発要員の管理					―		◎					◎	○	○	○
		D.開発環境の整備		1			Or		◎							◎	
	2.標準と手続き	A.標準と手続きの制定		1			Op		◎					○	◎		○
		B.標準と手続きの維持管理					―		◎					○	◎		○
	3.システム開発ライフサイクル(SDLC)	A.システム分析		1		1	E		◎	○	○	○	◎	○	○	○	○
		B.開発検討		1		1	E		◎				○	◎	○	○	○
		C.システム設計		1			E		◎				○	○	◎	○	○
		D.プログラム設計					―		◎					○	◎		○
		E.プログラミング					―		◎					○	◎		○

別紙３
金融機関等のシステム監査指針：チェックポイント集一覧表

開発リスクマネジメント（RM）の要素…C：経営、Or：組織ガバナンス、R：IT リスク、E：拡張性、Op: 要件定義最適化、Q：品質重視
経営者関与ポイント…4 点（R）：実行責任者、3 点（A）：説明責任者、2 点（C）：協議先、1 点（I）：報告者

要点項目	大項目	小項目	経営者				開発RMの要素	システム監査対象部門					システム監査の着眼点				
			CEO	CIO	CFO	企業幹部（ユーザー部門）		情報システム部門			本部各部門	利用部門	有効性	効率性	信頼性	安全性	遵守性
								企画	開発	運用							
4.システム開発	3.システム開発ライフサイクル(SDLC)	F.システムテスト					―		◎					○	◎	○	○
		G.移行		1		1	Op		◎	○	○	○		○	◎	○	○
		H.移行後レビュー					―		◎	○	○	○	◎	○	○	○	○
	4.システム変更管理	A.システム変更					―		◎	○	○	○		○	◎	○	○
		B.プログラム変更作業					―		◎					○	◎	○	○
		C.一時的プログラム変更					―		◎					○	◎	○	○
	5.障害対策	A.障害対策		1			R		◎						◎	○	
	6.パッケージソフトウェア取得	A.調査・分析		1			Op		◎				◎	○	○	○	○
		B.導入					―		◎				○	○	◎	○	○
		C.フォローアップ					―		◎				◎	○	○	○	○
	7.プロジェクトマネジメント	A.プロジェクト計画の策定	1	2		1	Or		◎	○	○	○	◎	○	○	○	○
		B.プロジェクト計画の内容	1	2		1	Or		◎					◎	○	○	
		C.プロジェクト要員	1	2			Or		◎					◎	○	○	
		D.進捗・コスト・品質管理	1	2			Q		◎					◎	○	○	
		E.プロジェクトの評価					―		◎				○	◎	○	○	
	合計		5	21	1	6											
5.システム運用(18)	1.運営と要員管理	A.職務の分離		2			R			◎						◎	
		B.システム運用業務の運営管理					―			◎				◎	○		
		C.システム運用要員の管理					―			◎				◎	○	○	○
	2.標準と手続き	A.標準と手続きの制定					―			◎				○	◎		○
		B.標準と手続きの維持管理					―			◎				○	◎		○
	3.運用管理	A.オペレーション管理-スケジュール管理					―			◎				○	◎	○	○
		B.オペレーション管理-作業管理					―			◎				○	○	◎	○
		C.オペレーション管理-管理記録					―			◎				○	○	◎	○
		D.システム運用状況の監視					―			◎					◎	◎	○
		E.ファイル管理					―			◎				○	○	◎	○
		F.プログラム管理					―			◎				○	○	◎	○
		G.機器管理					―			◎					◎	◎	○
		H.外部接続管理					―			◎					◎	◎	○
		I.障害対策-発生管理					―			◎					◎	◎	
		J.障害対策-原因究明・対策					―			◎					◎	◎	○
		K.重要帳票管理					―			◎					◎	◎	○
		L.カード管理					―			◎					◎	◎	○
		M.CD/ATM等及び無人店舗の管理					―			◎					◎	◎	○
	合計		0	2	0	0											
6.システム利用(15)	1.運営と要員管理	A.ユーザー部門等における運営管理					―				○	◎	◎			○	○
		B.ユーザー部門等の要員管理					―				○	◎		◎	○	○	
		C.教育・訓練					―				○	◎		◎	○	○	
		D.防災・防犯					―				○	◎				◎	○
		E.機器の保守					―				○	◎			○	◎	○
	2.ユーザー業務手続きとマニュアル	A.ユーザー業務手続きとマニュアルの維持管理					―				○	◎			○		◎
	3.業務管理	A.端末機等操作の管理					―					◎				◎	○
		B.データファイルの取扱管理					―					◎				◎	○
		C.重要帳票の管理					―					◎				◎	○
		D.顧客の認証媒体やキャッシュカード等の管理					―					◎				◎	○
		E.顧客のパスワードや暗証番号の管理					―					◎				◎	○
		F.CD/ATMの管理					―					◎				◎	○
		G.無人店舗の管理					―					◎				◎	○
		H.その他の店舗形態の管理					―					◎				◎	○
		I.渉外用パソコン等の管理					―					◎				◎	○
	合計		0	0	0	0											
7.入出力等の処理(22)	1.入出力業務管理体制	A.職務の分離					―					◎				◎	
		B.業務管理					―					◎				◎	
	2.入力原票	A.入力原票の作成					―					◎					◎
		B.入力原票の承認					―					◎					◎
		C.入力原票の訂正					―					◎					◎
		D.入力原票の保存					―					◎					◎

別紙３
金融機関等のシステム監査指針：チェックポイント集一覧表

開発リスクマネジメント（RM）の要素…C：経営、Or：組織ガバナンス、R：IT リスク、E：拡張性、Op: 要件定義最適化、Q：品質重視
経営者関与ポイント…4 点（R）：実行責任者、3 点（A）：説明責任者、2 点（C）：協議先、1 点（I）：報告者

要点項目	大項目	小項目	経営者				開発RMの要素	システム監査対象部門					システム監査の着眼点				
			CEO	CIO	CFO	企業幹部（ユーザー部門）		情報システム部門			本部各部門	利用部門	有効性	効率性	信頼性	安全性	遵守性
								企画	開発	運用							
7.入出力等の処理	3.入力処理	A.データ入力					－		◎		○	◎			◎	○	○
		B.外部企業等からの入力データの受入れ					－		◎	○	○	◎			◎	○	○
		C.入力原票がない場合のデータ入力					－		◎		○	◎			◎	○	○
	4.処理の一貫性の制御	A.処理の正確性確保					－		◎	○	○	◎			◎		○
		B.ファイル間の整合性確保					－		◎	○	○	◎			◎		○
		C.複数システム間のインタフェース					－		◎	○		◎			◎		
	5.エラーデータ	A.エラーデータの修正					－		◎		○	◎					◎
		B.エラーデータの分析					－		◎		○	◎			◎		
	6.出力処理	A.出力情報の検証					－				○	◎			◎		
		B.出力情報の訂正					－				○	◎			◎	○	○
		C.出力情報の配布					－			○	○	◎			◎	○	○
		D.外部企業等へのデータ送付					－			○		◎			◎	○	○
		E.出力情報の保存、廃棄					－					◎			○	◎	○
		F.出力情報の有用性					－			○	○	◎	◎	○			
	7.マスターファイル	A.マスターファイルの更新					－			◎					◎	○	
		B.マスターファイルの完全性及び正確性の確保					－			◎					◎	○	
	合計		0	0	0	0											
8.ネットワーク（10）	1.ネットワーク管理	A.ネットワーク管理体制		1			Or			◎	○	○		○	○	◎	
		B.ネットワーク管理に係る手続き					－			◎	○	○		○	○	◎	
		C.ネットワークの構成管理					－			◎	○	○		○	○	◎	
		D.障害対策					－			◎	○	○		○	○	◎	
	2.セキュリティ管理	A.アクセスコントロール					－			◎	○	○		○	○	◎	
	3.インターネットセキュリティ	A.インターネットセキュリティ					－			◎	○	○		○	○	◎	
		B.ホームページ					－			◎	○	○			○	◎	○
	4.電子メール	A.電子メール					－	○	○	◎	○	○		○	○	◎	○
	5.オープンネットワークを利用した金融サービス	A.不正取引を防止する機能					－			◎	○	○			○	◎	○
		B.顧客への対応					－				◎	◎			○	◎	○
	合計		0	1	0	0											
9.システム資産・資源管理(7)	1.資産管理	A.ハードウェア資産管理					－			◎			○	○		◎	
		B.ソフトウェア資産管理					－			◎			○	○			◎
	2.容量管理	A.キャパシティプランニング	1	2			Q			◎			○	◎			
	3.性能管理	A.性能測定とチューニング					－			◎				◎	○		
	4.データベース管理	A.データベース管理					－		○	◎				○	○	◎	
	5.パッチの適用と管理	A.パッチの適用と管理					－			◎				○	○	◎	
	6.構成管理	A.構成管理					－			◎				○	○	◎	
	合計		1	2	0	0											
10.外部委託(4)	1.外部委託計画	A.外部委託計画の策定	1	2			Or	◎			○		○	○	○	◎	
		B.外部委託先の選定		1			E	◎	○	○	○		○	○	○	◎	
		C.外部委託契約の締結					－	◎	○	○				○	○	○	◎
	2.外部委託業務管理	A.外部委託業務の管理					－		◎	◎			○	◎	◎	◎	○
	合計		1	3	0	0											
11.コンティンジェンシープラン(23)	1.情報システムのコンティンジェンシープランの策定と維持管理	A.コンティンジェンシープランの策定		2		2	R	○			◎				○	◎	
		B.コンティンジェンシープラン策定のための体制		2		2	R	○	○	○	◎	○			○	◎	
		C.リスク分析と評価		2		2	R	○			◎				○	◎	
		D.復旧手順の作成					－	○			◎				○	◎	
		E.教育・訓練					－	○	○	○	◎	○	○		○	◎	
		F.コンティンジェンシープランの維持管理					－	○	○	○	◎	○	○		○	◎	
	2.緊急事態に対する準備	A.緊急時対応組織の準備					－	○			◎				○	◎	
		B.人員及び資産の安全確保					－	○			◎				○	◎	
		C.通信手段の確保及び情報収集					－	○			◎				○	◎	
		D.緊急用資源と搬送手段の確保					－	○			◎				○	◎	
		E.緊急時の業務運営の方法					－	○			◎				○	◎	
		F.災害対策システムーバックアップサイト等の対応					－	○	○	○	◎				○	◎	
		G.広報活動の準備					－	○			◎				○	◎	
		H.損害状況評価の方法					－	○			◎				○	◎	

別紙３
金融機関等のシステム監査指針：チェックポイント集一覧表

開発リスクマネジメント（RM）の要素…C：経営、Or：組織ガバナンス、R：IT リスク、E：拡張性、Op: 要件定義最適化、Q：品質重視
経営者関与ポイント…4 点（R）：実行責任者、3 点（A）：説明責任者、2 点（C）：協議先、1 点（I）：報告者

要点項目	大項目	小項目	経営者				開発RMの要素	システム監査対象部門					システム監査の着眼点				
			CEO	CIO	CFO	企業幹部（ユーザー部門）		情報システム部門			本部各部門	利用部門	有効性	効率性	信頼性	安全性	遵守性
								企画	開発	運用							
11.コンティンジェンシープラン	3.対策本部における対応	A.初期対応の手順					－	○			◎				○	◎	
		B.暫定対応の手順					－	○			◎				○	◎	
		C.本格復旧の手順					－	○			◎				○	◎	
	4.コンピュータセンター等における対応	A.初期対応の手順					－	○	○	○	◎				○	◎	
		B.暫定対応の手順					－	○	○	○	◎				○	◎	
		C.本格復旧の手順					－	○	○	○	◎				○	◎	
	5.営業店等における対応	A.初期対応の手順					－				◎	○			○	◎	
		B.暫定対応の手順					－				◎	○			○	◎	
		C.本格復旧の手順					－				◎	○			○	◎	
	合計		0	6	0	6											
12.ドキュメンテーション(8)	1.ドキュメンテーションの標準化	A.ドキュメンテーション標準の制定と管理					－		◎	○	○			○	◎		○
		B.電子媒体によるドキュメンテーションの標準					－		◎	○	○			○	◎	○	○
	2.ドキュメントの作成	A.ドキュメントの作成					－		◎					○	◎		
		B.ドキュメントの作成管理					－		◎					○	◎		
		C.プロトタイプ開発等におけるドキュメントの作成					－		◎					○	◎		
	3.ドキュメントの管理	A.ドキュメント管理手続きの制定					－		◎	○	○	○				◎	○
		B.ドキュメントの内容の更新					－		◎					○	◎		
		C.ドキュメントの機密性					－		◎	○	○	○				◎	
	合計		0	0	0	0											

別紙４

開発リスクマネジメント（RM）の要素…C：経営、Or：組織ガバナンス、R：IT リスク、E：拡張性、Op: 要件定義最適化、Q：品質重視
経営者関与ポイント…4 点（R）：実行責任者、3 点（A）：説明責任者、2 点（C）：協議先、1 点（I）：報告者

金融検査マニュアル（預金等受入機関に係る検査マニュアル）							
大項目	中項目	CEO	CIO	CFO	企業幹部	合計	開発RMの要素
1．方針の策定	①【取締役の役割・責任】	4	4	4	4	16	C
	（ⅰ）取締役						
	（ⅱ）取締役会						
	（ⅲ）システム担当取締役						
	②【戦略目標の明確化】	4	4	2	4	14	C
	③【システムリスク管理方針の整備・周知】	2	4	2	2	10	R
	④【方針策定プロセスの見直し】	2	4	2	2	10	Or
	合計	12	16	10	12	50	
2．内部規程・組織体制の整備	①【内部規程の整備】	2	4	2	2	10	Or
	②【システムリスク管理部門の態勢整備】	2	4	2	2	10	Or
	（ⅰ）設置と役割付与						
	（ⅱ）管理者の配置と権限付与						
	（ⅲ）人員の配置						
	（ⅳ）業務部門への牽制機能						
	③【各業務部門及び営業店等におけるシステムリスク管理態勢の整備】	2	4	2	4	12	Or
	（ⅰ）内部規程等周知遵守態勢の整備						
	（ⅱ）システムリスク管理の実効性確保						
	④【取締役会等への報告・承認態勢の整備】	2	4	2	2	10	Or
	⑤【監査役への報告態勢の整備】	2	4	2	2	10	Or
	⑥【内部監査実施要領及び内部監査計画の策定】	2	4	2	2	10	Or
	⑦【内部規程･組織体制の整備プロセスの見直し】	2	4	2	2	10	Or
	合計	14	28	14	16	72	
3．評価・改善活動							
⑴ 分析・評価	①【システムリスク管理の分析・評価】	2	4	2	2	10	R
	②【分析・評価プロセスの見直し】	2	4	2	2	10	R
⑵ 改善活動	①【改善の実施】	2	4	2	2	10	Or
	②【改善活動の進捗状況】	2	4	2	2	10	Or
	③【改善プロセスの見直し】	2	4	2	2	10	Or

別紙５
「システム統合リスク管理態勢の確認検査用チェックリスト」

開発リスクマネジメント（RM）の要素…C：経営、Or：組織ガバナンス、R：IT リスク、E：拡張性、Op: 要件定義最適化、Q：品質重視
経営者関与ポイント…4 点（R）：実行責任者、３点（A）：説明責任者、２点（C）：協議先、１点（I）：報告者

項目		リスク管理態勢のチェック項目	CEO	CIO	CFO	企業幹部	合計	開発RMの要素
Ⅰ．経営陣のリスク管理に対する協調した取組み	ⅰ．経営統合に係るリスク管理態勢のあり方	1．経営統合に係るリスクに対する認識	4	2	2	2	10	R
		2．協調体制の整備	4	2	2	2	10	Or
		3．顧客対応の重要性に対する認識等	4	2	2	2	10	Or
		4．統合方針の確立	4	2	2	2	10	C
		5．ビジネスモデルの確立	4	2	2	2	10	C
		6．統合計画及び実行計画の策定	4	2	2	2	10	C
		7．統合プロジェクトの管理	4	2	2	2	10	Or
		8．統合プロジェクトの移行判定	4	2	2	2	10	Q
	ⅱ．システム統合に係るリスク管理態勢のあり方	1．システム統合に係るリスク管理体制の整備	3	4	2	2	11	Or
		2．システムの移行判定	3	4	2	2	11	Q
	合計		38	24	20	20	102	
Ⅱ．協調したシステム統合リスク管理態勢のあり方	ⅰ．セキュリティ管理体制の整備	セキュリティ管理体制の整備	4	2	1	2	9	R
	ⅱ．協調した事務リスク管理態勢のあり方	1．管理者の役割	2	2	1	4	9	R
		2．事務部門の組織整備	2	2	1	4	9	Or
		3．用語の統一と事務規定の整備	2	2	1	4	9	Op
		4．金融商品・サービス体系の整備	2	2	1	4	9	Op
		5．営業部店網の整備	2	2	1	4	9	Or
		6．顧客データの整備	2	2	1	4	9	Op
		7．営業部店における対応	2	2	1	4	9	Or
	ⅲ．協調したシステムリスク管理態勢のあり方	1．管理者の役割	2	4	1	2	9	R
		2．企画・開発・移行の体制	2	4	1	2	9	Or
		3．システム開発の管理	2	4	1	2	9	Or
		4．規定・マニュアルの整備		4		4	8	−
		5．テスト等	2	4	1	2	9	Q
	ⅳ．協調した業務運営態勢のあり方	1．運営体制の明確化	2	2	1	4	9	−
		2．業務運営の検証	2	2	1	4	9	Q
	ⅴ．外部委託業務管理態勢のあり方	外部委託業務管理	2	4	1	4	11	−
	合計		32	44	15	54	145	
Ⅲ．不測の事態への対応		1．統合計画遅延時の対応	4	3	1	3	11	R
		2．コンティンジェンシープランの整備	4	3	1	3	11	R
		3．統合日前後における不測の事態への対応	4	3	1	3	11	R
	合計		12	9	3	9	33	
Ⅳ．監査及び問題点の是正	ⅰ．内部監査	1．内部監査体制の整備	4	2	1	3	10	Or
		2．内部監査の手法及び内容	4	2	1	3	10	Or
	ⅱ．第三者機関による評価	第三者機関による評価の活用	4	2	1	3	10	Or
	合計		12	6	3	9	30	