日本証券業協会　システムリスク管理講座

システムリスク管理態勢について

～　検査官の視点で　～

平成23年2月17日

証券取引等監視委員会
事務局　証券検査課
特別検査官　藤田正浩

アジェンダ

- システムリスクとは？
- 「金融商品取引業者等向けの総合的な監督指針」及び「金融商品取引業者等検査マニュアル」の考え方
- システムリスク管理態勢検査でよく見かける問題点
- システムリスク管理態勢の事例
- その他考慮すべき事項

（注）本日の講演内容は藤田個人の見解です。

はじめに

- 日常のシステムリスク管理態勢検査の中で認められた問題点や管理の事例を提示することにより、参加者企業のシステムリスク管理態勢改善の一助としたい。
- 提示する事例はベスト・プラクティスや標準型等ではなく、検査官としてポイントになると考えている箇所のいくつかをピックアップしたものなので、雛形ではなく、参加企業が管理態勢を検討する際のヒントとして活用いただきたい。
- 当たり前の話も多いが、当たり前のことを当たり前に行うことが重要。

システムリスクとは？

2009年11月「システムリスク管理講座」の復習を兼ねて

システムリスクとは？

「リスク」の語源をたどれば…

ラテン語　’risicare’　＝　勇気を持って試みる

「JIS　Q　2001（リスクマネジメントシステム構築のための指針）」では…

事態の確からしさとその結果の組み合わせ、又は
事態の発生確率とその結果の組み合わせ

「COSO　ERM（全社的リスク管理に関するフレームワーク）」では…

組織にとって不利な影響を与え得る事象

（注）プラスの影響については「機会（opportunities）」としている。

本日の話ではマイナスの影響として定義

システムリスクとは？

システムリスクの定義

「金融商品取引業者等向けの総合的な監督指針」によれば…

「コンピュータシステムのダウン又は誤動作等、システムの不備等に伴い顧客や金融商品取引業者が損失を被るリスクやコンピュータが不正に使用されることにより顧客や金融商品取引業者が損失を被るリスク」

・情報セキュリティも含む。
・リスクが顕在化した場合の対応態勢も含む。

本日の話でも同じ定義で使用

システムリスクとは？

リスクマネジメントの範囲

リスクマネジメント
(狭義)

リスクの顕在化

危機発生

危機管理
(クライシスマネジメント)

リスクマネジメント
(広義)

本日の話ではリスクマネジメント(広義)

「金融商品取引業者等向けの総合的な監督指針」及び「金融商品取引業者等検査マニュアル」の考え方

監督指針・検査マニュアルの考え方

「金融商品取引法」第40条第2号　(適合性の原則)
業務の運営の状況が公益に反し、または投資家の保護に支障を生ずるおそれがあるものとして内閣府令で定められる状況にあること。

↓

「金融商品取引業者などに関する内閣府令」第123条第14号
金融商品取引業に係る電子情報処理組織の管理が十分でないと認められる状況。

↓

「金融商品取引業者等向けの総合的な監督指針」
　Ⅲ－２－８　システムリスク管理態勢
　Ⅳ－３－２－１(3) 証券会社等の電子情報処理組織の管理に係る留意事項
　その他

↓

「金融商品取引業者等検査マニュアル」
　システムリスク管理態勢、その他

監督指針・検査マニュアルの考え方

「金融商品取引業者など向けの総合的な監督指針」

Ⅳ－３－２－１　証券会社の電子情報処理組織に係る留意事項

(3) 証券会社等の電子情報処理組織の管理について、次に掲げる場合に該当する事実が認められる場合は、金商業等府令第123条第14号「電子情報処理組織の管理が十分でないと認められる状況」に該当するものとする。

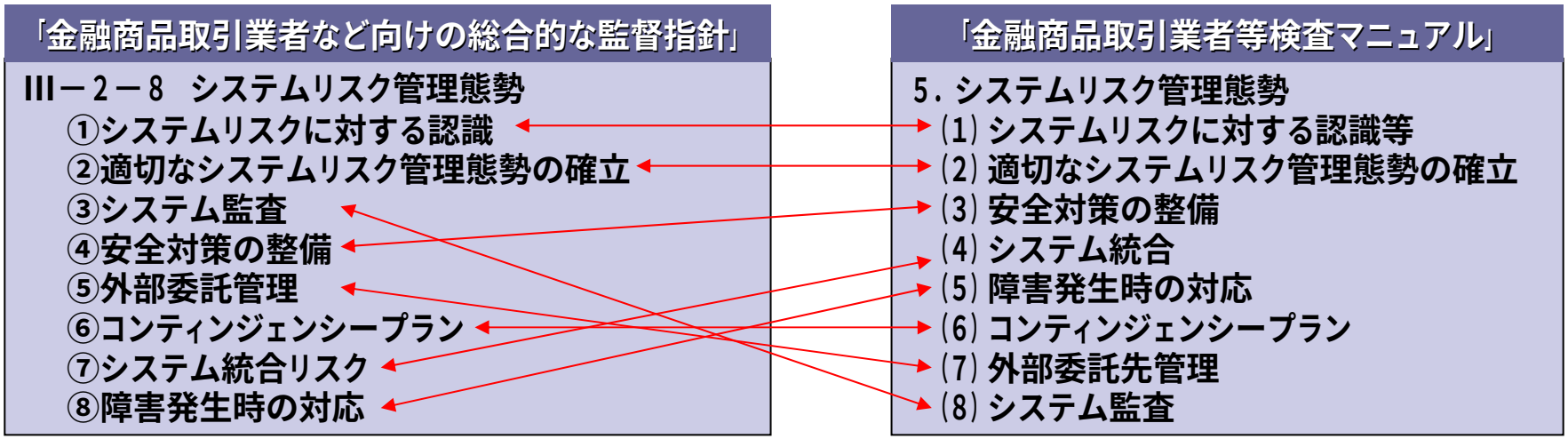
①電子情報処理組織の専門家によるシステム監査など、適切な専門家によるチェックを定期的に行っていない場合

②売買発注に関するハードリミット・ソフトリミットの設定を含む注文制限の設定をシステムに組み込んでいないなど、誤発注防止のためのシステム対応が十分に果たされていない場合

③Ⅲ-2-8に掲げる事項等に照らし、適切な態勢が整備されていないと認められる場合

監督指針･検査マニュアルの考え方

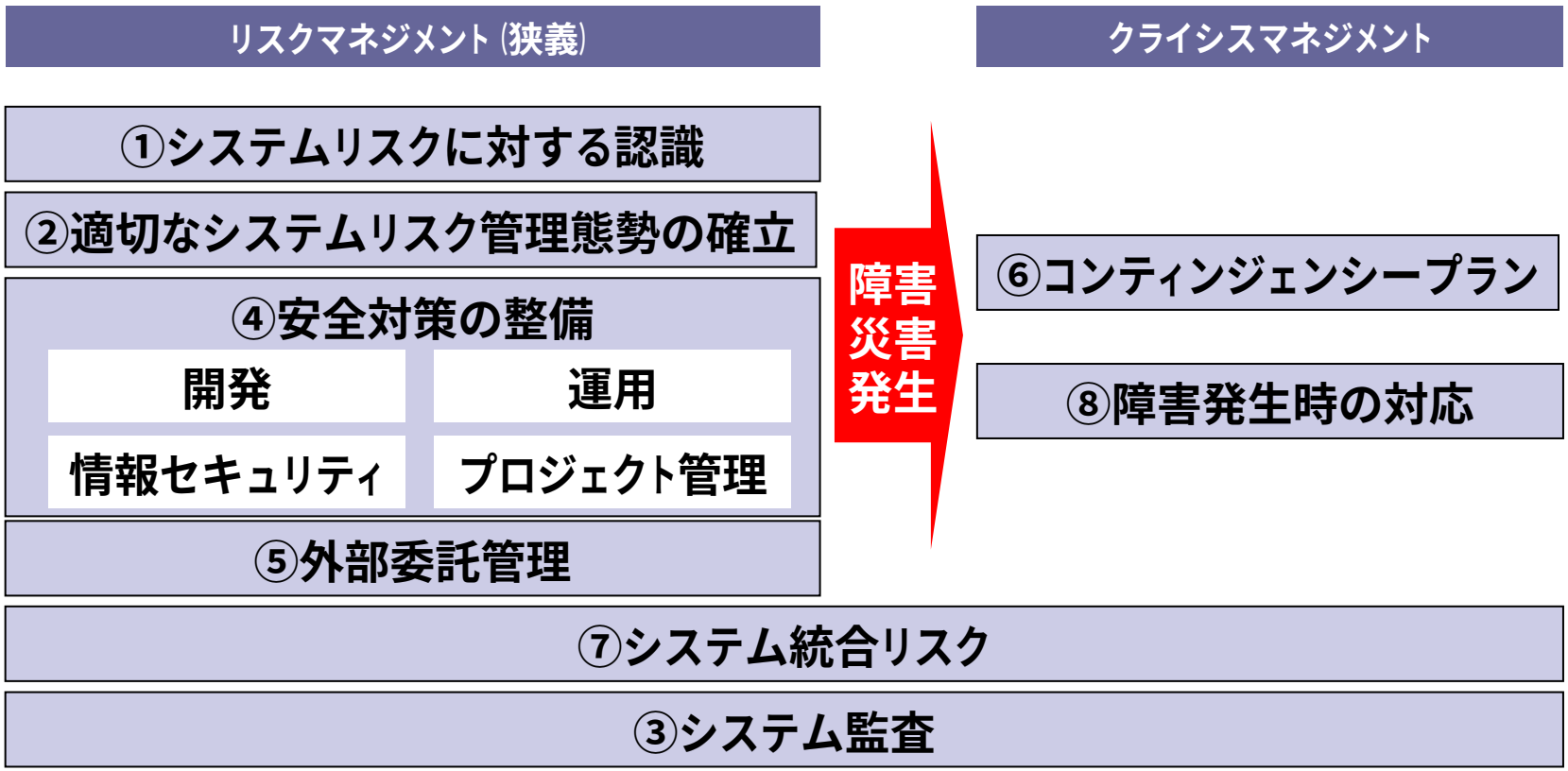
監督指針と検査マニュアルの対比



○監督指針は枠組みを優先し、検査マニュアルは検査実務を優先した順序。

監督指針・検査マニュアルの考え方

監督指針の項目をリスク・マネジメントの観点から整理



監督指針・検査マニュアルの考え方

システムリスク検査に関連する検査マニュアルの項目

Ⅱ－１－１　態勢編・共通項目
- ３．内部管理態勢
  - (6) 顧客情報の保護
  - (10) 外部委託業務の管理
- ４．監査態勢
- ５．危機管理態勢

Ⅱ－１－２　態勢編・第一種金融商品取扱業者
- １.内部管理態勢
  - (9) 電子取引（ＰＴＳ業務を含む）
  - (10) 情報管理

Ⅱ－２－２　業務編・第一種金融商品取引業者
- ７．ＰＴＳ業務
- ８．電子金融商品取引業務　　等

監督指針・検査マニュアルの考え方

検査マニュアルの改訂案

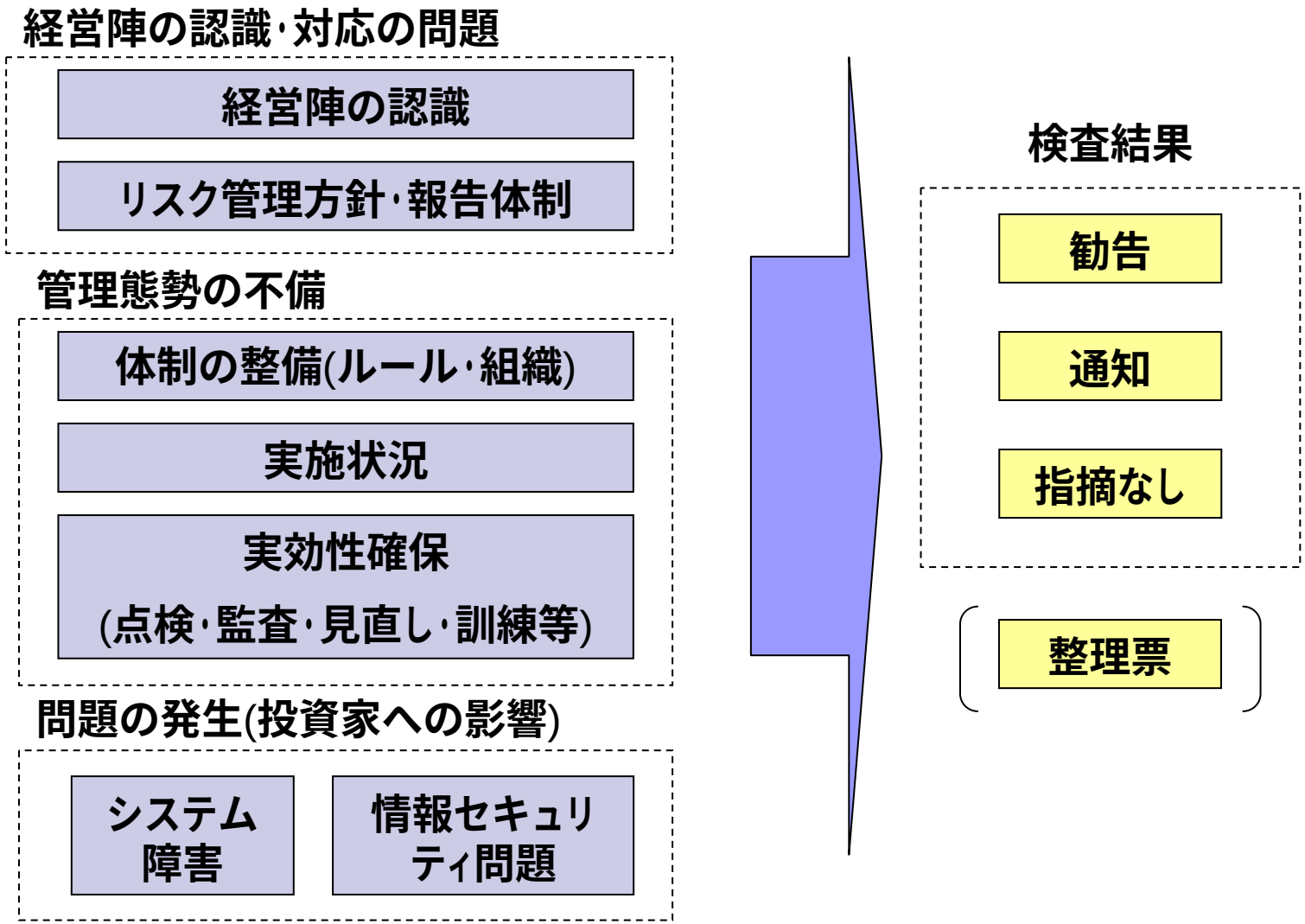
1．「情報セキュリティ管理態勢の整備」の項を追加。

2．その他、重要な検査項目を追加・修正。

- 「外部委託先管理」を「外部委託管理」に変更し、注釈を追加。
- 開発と運用の相互牽制体制を追加。
- 「サイバー攻撃」対策を追加。　　等

監督指針･検査マニュアルの考え方

～ 検査官の視点で見ると ～



システムリスク管理態勢検査でよく見かける問題点

～　検査官として感じた問題点　～

(注意)

問題点として記載した事項は、特定の会社の問題点ではなく、各社の共通的な問題点や複数の会社の問題点を寄せ集めたもの。

システムリスク管理態勢検査でよく見かける問題点

監督指針より抜粋

①システムリスクに対する認識等
イ．取締役会等において、システムリスクが十分認識され、全社的なリスク管理の基本方針が策定されているか。

ロ．システムリスクに関する情報が、適切に経営者に報告される体制となっているか。

②適切なリスク管理態勢の確立
イ．システムリスク管理の基本方針が定められ、管理態勢が構築されているか。

ロ．具体的基準に従い管理すべきリスクの所在や種類を特定しているか。

ハ．システムリスク管理態勢は、自社の業務の実態やシステム障害等を把握･分析し、システム環境等に応じて、その障害の発生件数･規模をできる限り低下させて適切な品質を維持するような、実効性ある態勢となっているか。

システムリスク管理態勢検査でよく見かける問題点

①システムリスクに対する認識

経営者が「リスク」や「リスク管理」に関して認識が不足している、または誤解している会社をよく見かける。

(1)「システムリスク管理方針」「システム管理規程」等が制定されていない、または自社のリスク認識に基づいて策定されているとは考えらないケース。

検査官から見ると、経営者は次のように考えていたのでは？と思える。

「リスク管理に意味があるのか疑問だが、当局から求められているからルール・体制等の形だけは作っておこう。」

「システムリスク管理方針を作るには時間がかかるから、他社のものをコピーして使おう。」

「システムリスク管理は専門家であるシステム部門の役割で、私はよく分からないのであまり関与しない。」

システムリスク管理態勢検査でよく見かける問題点

①システムリスクに対する認識

(2) リスクマネジメント(狭義)とクライシスマネジメントを混同し、本来必要なシステム障害を発生させないための対策が不十分なケース。

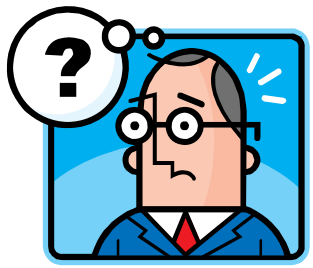
経営者は検査官に「当社のシステムリスクはシステム障害であり、システム障害の対応体制は十分整備している。」と説明するのだが…。

(3) 重大なシステム障害は発生の都度、取締役会に報告しているものの、障害件数の推移、原因・再発防止策、システム稼動・点検状況等定期的なシステムリスク情報を報告していないケース。

・リスク管理では、問題が発生する可能性に対して、実際に発生しないように、または発生しても影響が少なく、また早く回復できるように対策を行うことが重要。

・一般論ではなく、自社のリスク認識を踏まえて基本方針を策定することが重要。

・経営者のシステムリスク認識に関する問題は、検査結果においてシステムリスク管理態勢不備の原因として整理することが多い。



システムリスク管理態勢検査でよく見かける問題点

監督指針より抜粋

①システムリスクに対する認識等
イ．取締役会等において、システムリスクが十分認識され、全社的なリスク管理の基本方針が策定されているか。

ロ．システムリスクに関する情報が、適切に経営者に報告される体制となっているか。

②適切なリスク管理態勢の確立
イ．システムリスク管理の基本方針が定められ、管理態勢が構築されているか。

ロ．具体的基準に従い管理すべきリスクの所在や種類を特定しているか。

ハ．システムリスク管理態勢は、自社の業務の実態やシステム障害等を把握･分析し、システム環境等に応じて、その障害の発生件数･規模をできる限り低下させて適切な品質を維持するような、実効性ある態勢となっているか。

システムリスク管理態勢検査でよく見かける問題点

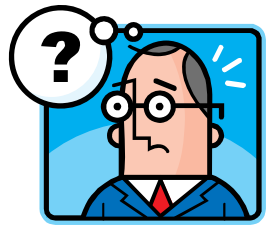
②適切なシステムリスク管理態勢の確立

(1) 形式的なリスク管理

「リスク管理規程」は制定しているが、規程で定めたリスク分析を実施していない会社、リスク分析を実施していても、形式的であったり、その後のモニタリングを実施していない会社をよく見かける。

システムリスクが顕在化したものが、システム障害であるという観点に立てば、リスク分析結果と、実際に発生したシステム障害の状況が差異があれば、リスク分析結果を見直す必要があるはず。

システムリスク分析結果		システム障害分析結果
・プログラムバグによるシステム障害のリスクが高い ・Aシステムが古いのでシステム障害のリスクが高い	← 見直しが必要	・作業ミスに起因するシステム障害の比率が高かった。 ・顧客影響あるシステム障害はBシステムが多かった。



システムリスク管理態勢検査でよく見かける問題点

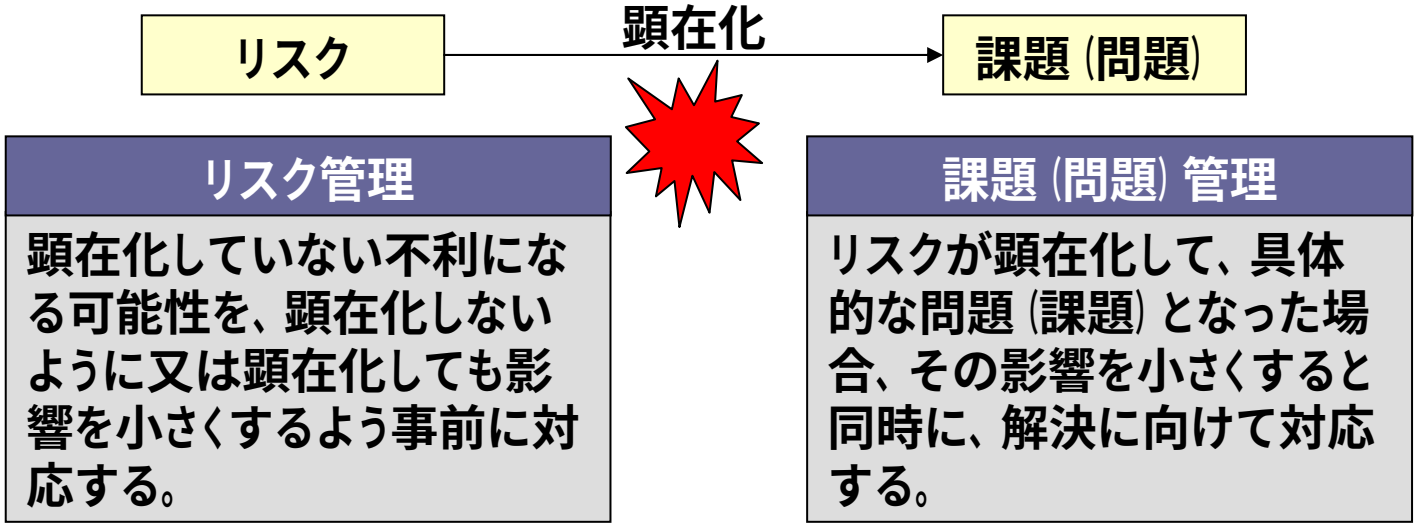
②適切なシステムリスク管理態勢の確立

(2) 実効性の無いリスク管理

システムリスクに関する規程は策定しているが、その趣旨を十分理解しておらず、実効性あるリスク管理を実施していないケースをよく見かける。

例えば、「リスク管理」と「課題管理」の違いを十分認識せず、リスク管理台帳に課題を掲載しているケースをよく見かける。

まだ問題が顕在化していない「リスク」と、実際に問題が顕在化している「課題」とでは、重要性・対応期限など管理方法が異なるはず。



（注）リスクを潜在課題と呼ぶこともある。

システムリスク管理態勢検査でよく見かける問題点

③システム監査

システム監査の実施体制を整備し、形式は整えているが、実効性の伴っていない会社をよく見かける。

(1) 専門家が実施していないケース

(2) 自己点検と監査の違い (監査の独立性) を認識していないケース

(3) 自社の重要なシステムリスクをカバーしていないケース

→ 基幹システム刷新のような重要プロジェクトに関するリスク等

(4) 指摘事項のフォローが実施されていないケース

(5) 定期的に実施していないケース

監督指針より抜粋

③システム監査
イ．システム部門から独立した内部監査部門において、システムに精通した監査要員による定期的なシステム監査が行われているか。
ロ．監査の対象はシステムリスクに関する業務全体をカバーしているか。

(参考) システム監査の定義 (経済産業省「システム監査基準」より)

「監査対象から独立かつ客観的立場のシステム監査人が情報システムを総合的に点検及び評価し、組織体の長に助言及び勧告するとともにフォローアップする一連の活動」

システムリスク管理態勢検査でよく見かける問題点

④安全対策の整備

(1) 企画・開発において、自社の開発標準を制定していない会社、制定していても工程の完了規準、品質基準など重要な事項を明確化していない会社をよく見かける。

・完了基準を明確にしていないため、結合テストが十分完了していない（当初計画したテストケースは終了したが、不具合が収束していない）にも関わらず、次工程であるシステムテストに入ったため、システムテストにおいて、結合テスト工程以前で抽出すべき不具合が多発しているケース。

・特に、テスト工程における品質基準が不明確で、当初計画したテストの完了でもってテスト完了としているケース。

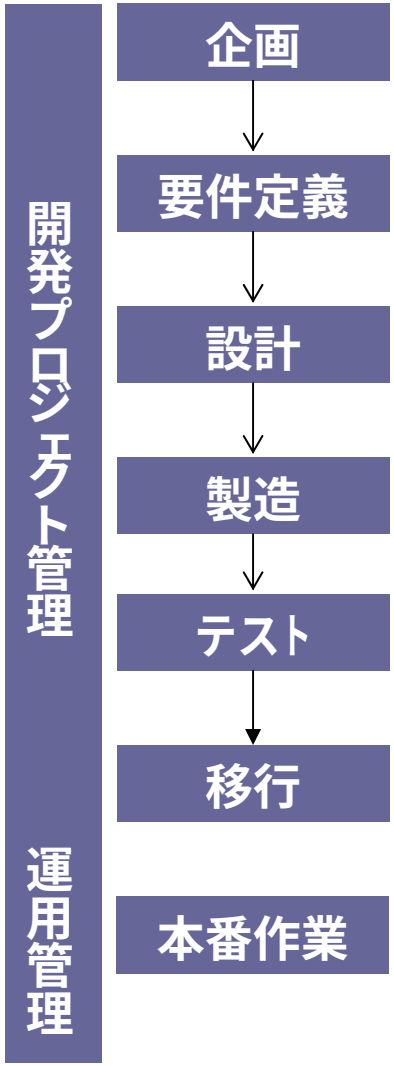
・システムリスク管理の本質が「システムの安全かつ安定的な稼動を図る」ことであるなら、安全対策がシステムリスク対策の肝であり、障害の未然防止のために品質管理が必要。

・品質管理のベースとなるのが開発標準。

システムリスク管理態勢検査でよく見かける問題点

④安全対策の整備

(2) 企画・開発・運用プロセス



・プロジェクト計画書を整備していない、または整備していても、工程・成果物・完了基準、特に品質基準を明確化していない。
・リスク管理計画を策定していない。

・ユーザ部門が業務要件を承認していない。
・システム部門が性能・容量目標を確認していない。

・設計レビュー、プログラムレビュー等、品質管理に関わるプロセスを確認していない。
・定期的に作業の進捗状況を確認していない。

・テスト計画、テスト結果レビュー等のテスト状況を確認していない。
・品質報告書が無い、または確認していない。
・受入テスト(検収テスト)を実施していない。

・稼動判定を実施していない、または判定項目が不足。
・不測の事態への対応計画を策定していない、または考慮が不十分。

・開発担当者が本番作業を実施しているなど、開発担当と運用担当の相互牽制体制が確立されていない。

システムリスク管理態勢検査でよく見かける問題点

④安全対策の整備

(3) 情報セキュリティ管理における重要な事項でアカウント管理、ログ管理において、右記のように

「不要な特権アカウントの付与」

「アカウントの変更管理の遅延」

「共有アカウントの存在」

「定期的なアカウント棚卸未実施」

「アクセスログ取得・保管未実施」
「ログの定期的なモニタリング未実施」

など、管理態勢の不十分な状況をよく見かける。

× 管理不十分な項目

システム名 / 管理項目	Xシステム	
	件数	内委託先貸与
業務アカウント数	80	20
内特権アカウント	×50	5
内共有アカウント	×10	× 5
システムアカウント数	20	15
内特権アカウント	5	5
内共有アカウント	× 5	× 5
アカウント削除時期	× 3カ月毎	
アカウント台帳棚卸サイクル	× 未実施	
パスワード変更管理	× 未実施	
ログ保管期間	1年	
ログ種類	× ログインログのみ	
ログ・モニタリング	× 必要時のみ	

・アカウント管理は、情報セキュリティ管理のベースのひとつ。退職直後の不正アクセスが多いと言われている。

・ログ管理は、問題発生時の証跡としてだけでなく、けん制機能としても有効。

システムリスク管理態勢検査でよく見かける問題点

⑤外部委託管理

外部委託管理について、以下のような管理態勢上の問題をよく見かける。

(1) 共通管理

・委託先の監査などで業務の実態や問題が無いか等の把握をしていないケース。

・情報セキュリティ管理、特にアカウント管理やログ管理が不十分なケース。

(2) 開発委託

・進捗管理、品質管理、受入検収テスト等、開発に関するリスク管理が不十分なケース。

(2) 運用委託

・障害管理を任せきりにしているケース。

・システム性能、容量等の点検結果を確認していないケース。

・本番作業結果の検証、確認を実施していないケース。

システム障害や情報セキュリティ等の問題が発生するリスクがあり、
発生した問題の原因と認定されれば検査指摘となる可能性あり。

システムリスク管理態勢検査でよく見かける問題点

⑥コンティンジェンシープラン

(1) 全体の枠組みを明確にしないまま、個別の計画を策定しているケース、

(2) 業務継続計画が取締役会等で承認されていないケース、

(3) 前提となるシナリオや発動基準が不明確なケース、

(4) 業務継続計画の前提が適切に整備されていないケース、

(5) その他実効性が維持されていないケース、

等をよく見かける。

基本的な業務継続計画
・業務優先度
・目標復旧時間
・想定するシナリオ
・連絡体制、安否確認
・発動基準
・意思決定者、代替者
・情報開示手順、手段

シナリオ毎の計画
・想定する非常事態
・体制、手順
前提の整備
・バックアップシステム
・バックアップデータ等
・バックアップオフィス
・切り替え手順　等

実効性の維持
・計画の見直し
・訓練
・研修

○ 不十分なケースが多い事項

システムリスク管理態勢検査でよく見かける問題点

⑧システム障害発生時の対応

(1) 基本的な障害管理の不備

障害発生時の対応手順が未整備、障害発生から対応完了までの継続管理、消しこみ管理の未実施。

(2) 障害記録等の不備

障害記録洩れ、一元管理未実施、管理項目が不十分、集計･分析未実施。

(3) 再発防止策の不備

再発防止策を未策定、再発防止策の未実施（含む当局報告分）。

(4) 顧客対応の不備

顧客影響の把握不十分、顧客による対応の差異、顧客への損失補てん未実施。

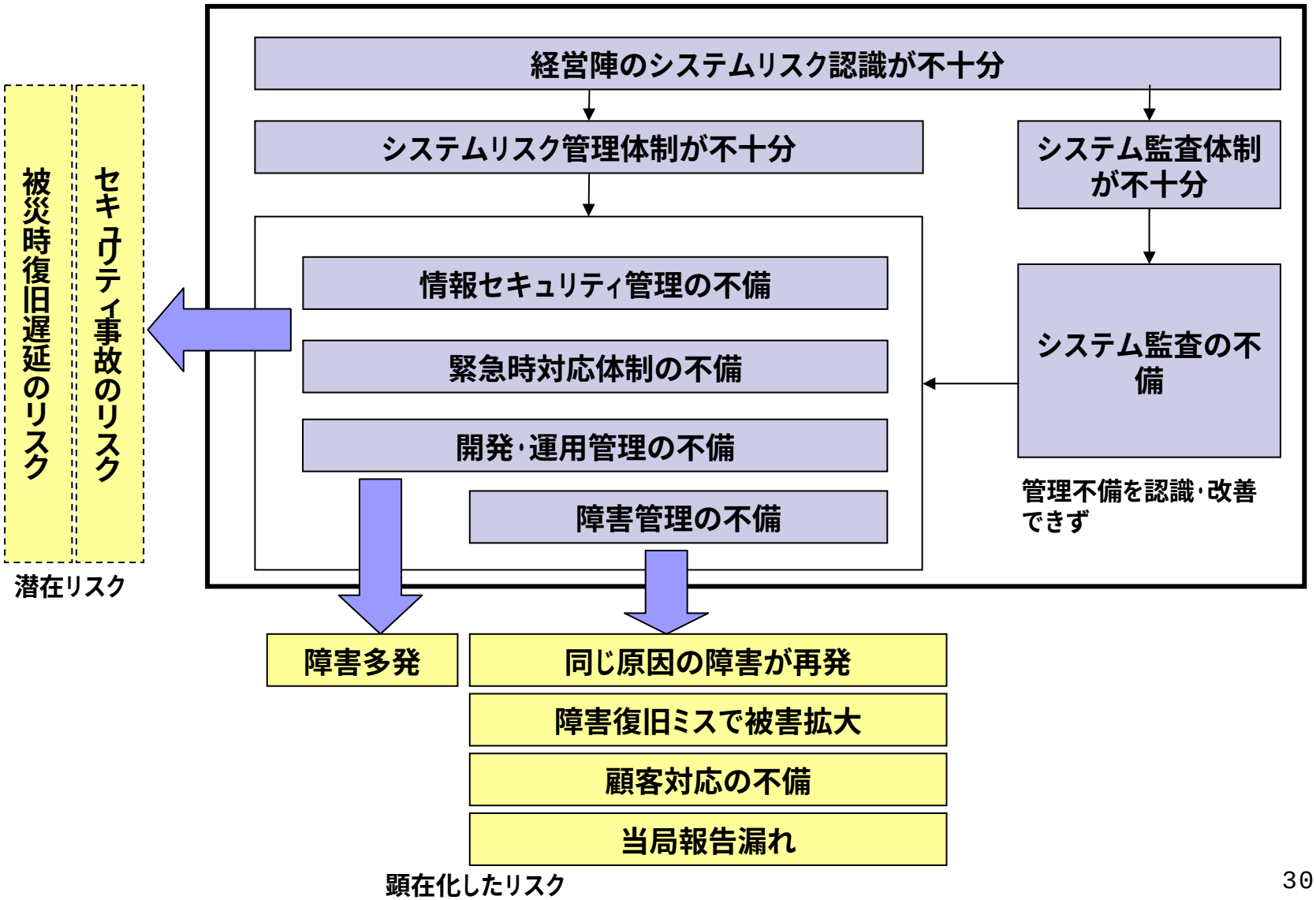
(5) 外部委託先管理の不備

障害管理を外部委託先に任せきり。

(6) 当局報告の不備

当局報告基準の未統一、顧客影響ある障害の報告洩れ。

(参考) 検査官の視点で検査結果を整理した事例 (よく見かけるパターン)



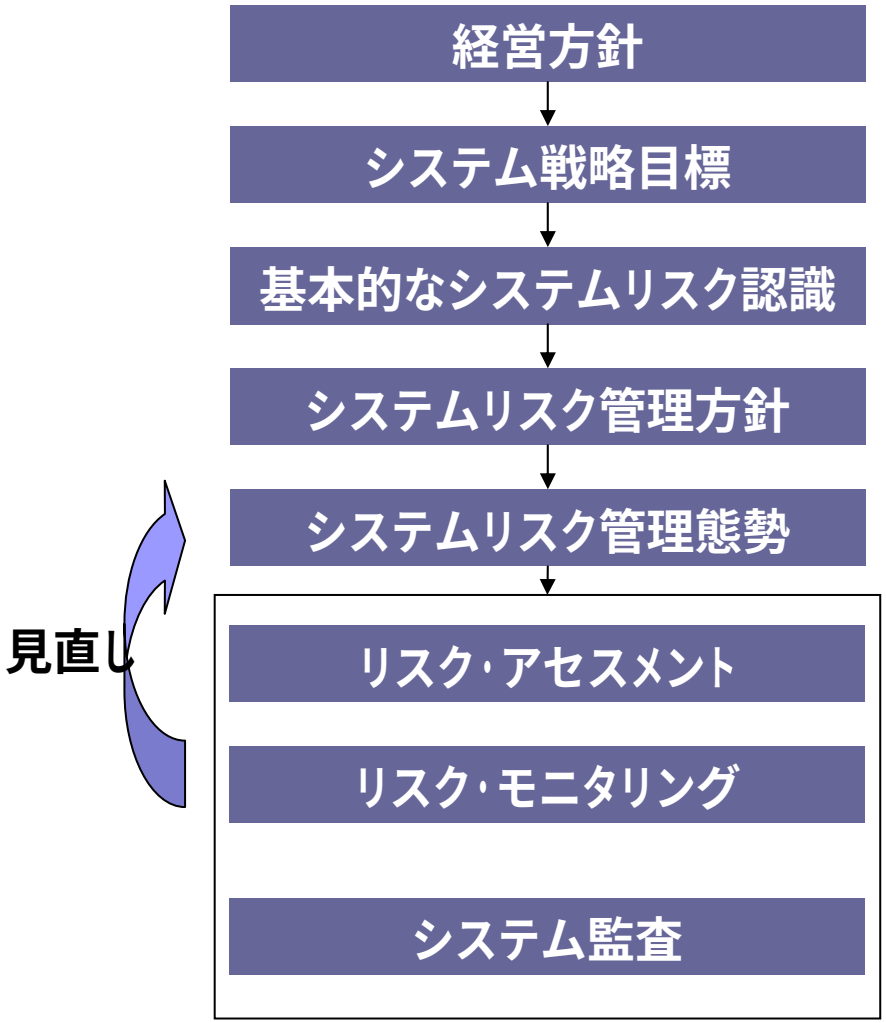
システムリスク管理態勢の事例

（注意）

事例に記載した事項が整備されているだけで管理態勢が十分というわけではない。また会社の状況により、記載した事項が整備されてなくともリスクがそれほど大きく無いケースもありうる。会社の実態、リスク状況に合わせた管理態勢整備が重要である。

また、記載した事例は、特定の会社の事例ではなく、複数の会社の事例を参考にとりまとめたものである。

システムリスク管理プロセス



取締役会等で経営方針に基づいた情報戦略を策定。

取締役会等でリスク認識に基づいたシステムリスク管理方針を策定。

システムリスク管理方針に基づき、システムリスク管理規程等、管理基準・手順・体制等を制定。

システムリスク洗い出し・評価・対策。

定期的なシステムリスクモニタリングと取締役会等への報告。

専門家によるシステム監査と経営者への報告。

「○社のシステムリスク管理態勢概要」

システムリスク管理プロセス

リスク･アセスメントの事例

リスク洗い出し

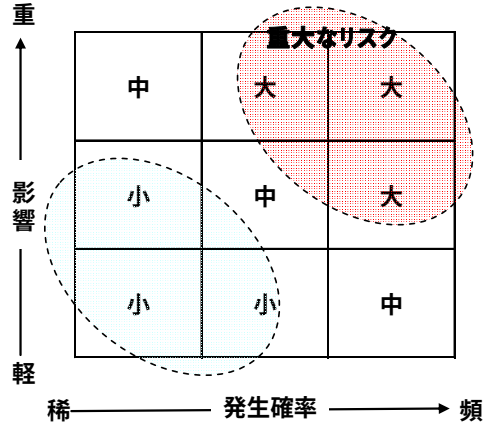
･情報資産、プロセス等をベースに洗い出し。

･偶発的（災害･故障）と自発的（過失･故意）に分けて洗い出し。

･機密性、完全性、可用性に分けて洗い出し。

リスク評価

「発生確率×影響度」で評価。
発生確率、影響度とも3段階での評価をよく見かけるが、GIMITS「ITセキュリティマネジメントのための手法」では発生頻度として5段階評価（0～4）を採用している。



リスク対策

「回避」
リスクを回避するために業務を廃止したり、情報資産を廃棄すること。
「低減」
適切な管理策を採用して、リスクを軽減すること。
「移転（転嫁）」
保険などの契約等により、リスクを他社(他者)に移転すること。
「保有」
リスクが顕在化した場合の損失負担を受容すること。

システム監査

システム監査

リスク分析・前年度実績

年度計画

個別計画

監査実施

報告

フォロー

年度報告

○システム監査の前提としてのシステムリスク分析
前年度システム監査実績、システムリスク分析結果の活用。

○リスクベースをベースとしてシステム監査計画
リスクに応じたシステム監査の頻度、深度を基にした計画。

○重点思考の個別システム監査計画
監査目的と重点項目を明確化した個別計画。

○専門家のよる実施
社内に専門家がいなければ外部専門家に依頼。

○重要性・緊急性を明確化した報告書の経営あて報告
指摘事項の重要性・緊急性を評価した報告書を取締役会等へ報告。

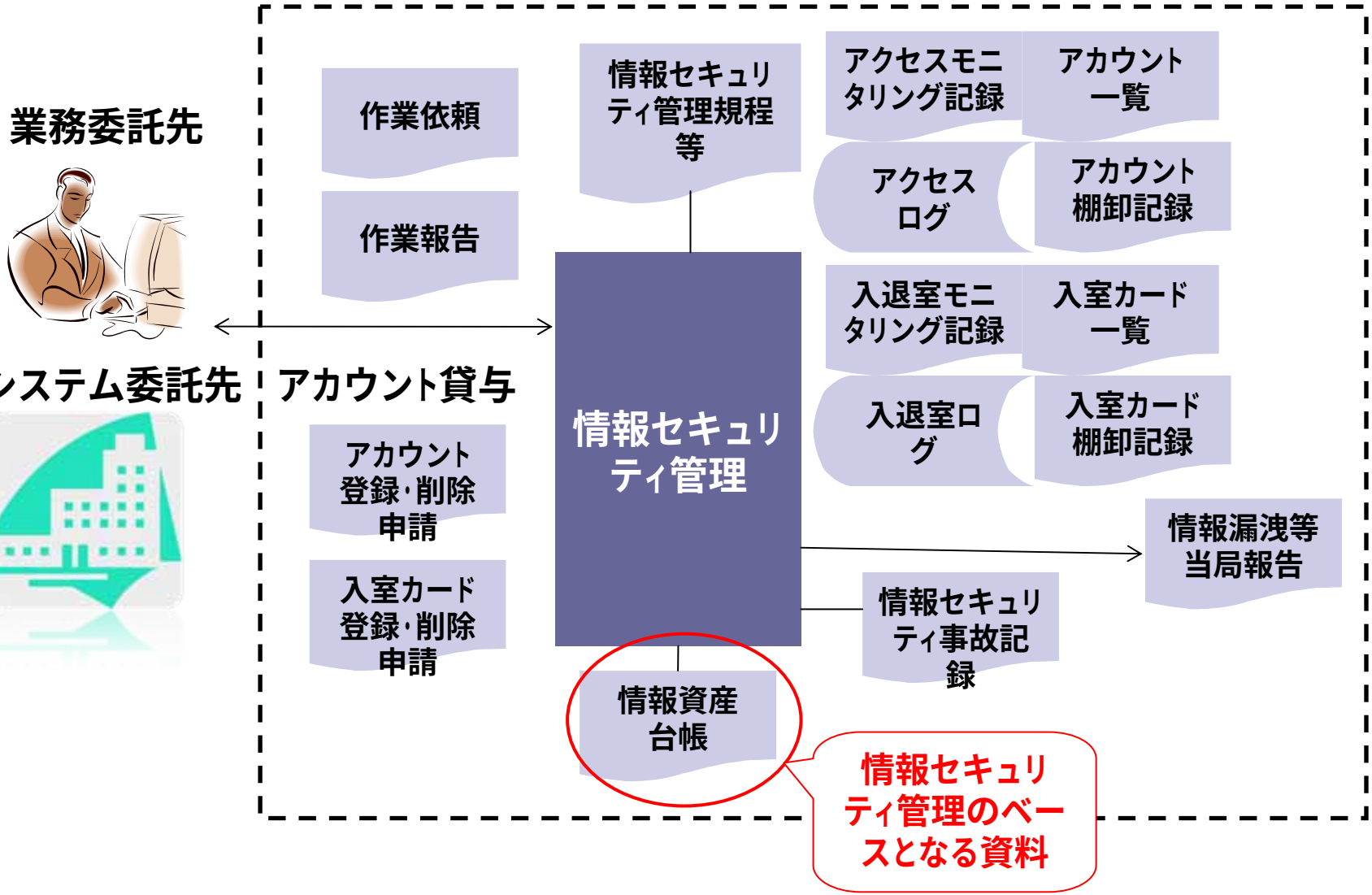
○指摘事項のフォロー体制整備
指摘事項のフォローおよびフォロー監査の実施。

○年度実績からみた全体評価
年度実績全てを再度見直して、全体としてどこが弱いか評価したうえで年度報告。

○「システム監査規程」「チェックリスト」等のシステム監査に関するルールを制定。

○システム監査そのものの品質評価により、システム監査品質を向上。

情報セキュリティ管理


業務委託先
システム委託先
作業依頼
作業報告
アカウント貸与
アカウント登録･削除申請
入室カード登録･削除申請
情報セキュリティ管理規程等
情報セキュリティ管理
情報資産台帳
アクセスモニタリング記録
アカウント一覧
アクセスログ
アカウント棚卸記録
入退室モニタリング記録
入室カード一覧
入退室ログ
入室カード棚卸記録
情報漏洩等当局報告
情報セキュリティ事故記録
情報セキュリティ管理のベースとなる資料

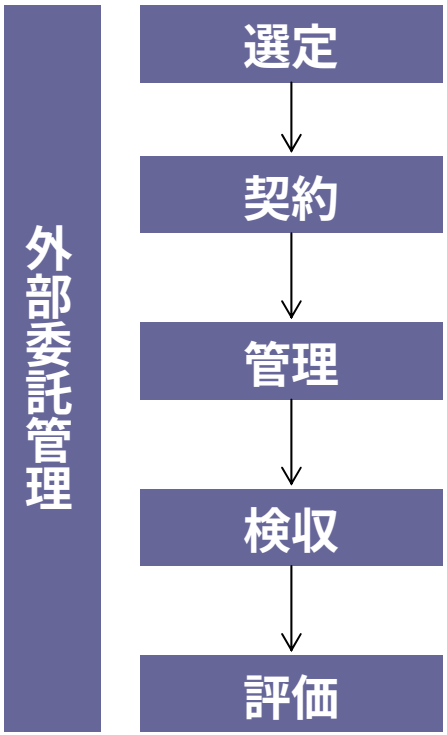
情報セキュリティ管理

アカウント管理･アクセスログ管理の事例

システム名 / 管理項目	○システム		
	件数	内委託先貸与	
業務アカウント数	80	20	委託先へ貸与する場合のルールを制定し、ルールに基づき適切に管理している。
内特権アカウント	5	3	
内共有アカウント	0	0	共有アカウントを使用していない。
システムアカウント数	20	15	
内特権アカウント	5	3	特権アカウント、システムアカウントの管理は、一般アカウントの区別し、リスクに応じて管理している。
内共有アカウント	0	0	
アカウント削除時期	毎日		適切なタイミングで削除している。
アカウント台帳棚卸サイクル	毎月末		適切なタイミングで点検している。
パスワード変更管理	3ヵ月毎自動		パスワード変更が確認されている。
ログ保管期間	1年		アクセスログを適切な期間保管し、確認できる体制を整備している。
ログ種類	全アクセスログ		
ログ･モニタリング	毎月		定期的にログをモニタリングしている。

外部委託管理

外部委託管理体制、外部委託管理規程等の整備



制定した選定基準･手続きに基づき選定

管理規程に定められた事項を盛り込んだ契約書･ＳＬＡの締結

定期的な報告、会議等でのモニタリング、委託先の監査による委託業務実施態勢の確認

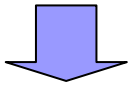
受入テスト、品質評価報告書、運用監視実績等、契約に基づく成果物等による委託結果の検収確認

制定した評価基準に基づき評価し、契約･ＳＬＡ等を見直し

外部委託管理

選定基準の事例

選定基準項目
経営の健全性、安定度
委託業務に関する実績
担当要員の技術力
会社全体としての業務完遂能力
継続保守体制
損害賠償能力
情報セキュリティ体制
提供業務内容とコストの妥当性
(注) 複数先を比較検討すること



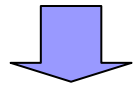
各項目の具体的な
判定基準を策定

契約項目の事例

必須契約事項
契約の始期、終期、更新
委託業務内容と責任範囲
成果物定義
検収手続き
委託費用支払い条件
委託業務実施状況の定期報告
機密保持契約
情報の取り扱い
再委託手続き
監査権限
著作権の取り扱い
損害賠償責任
所轄裁所
ＳＬＡ
個人情報取扱に関する覚書

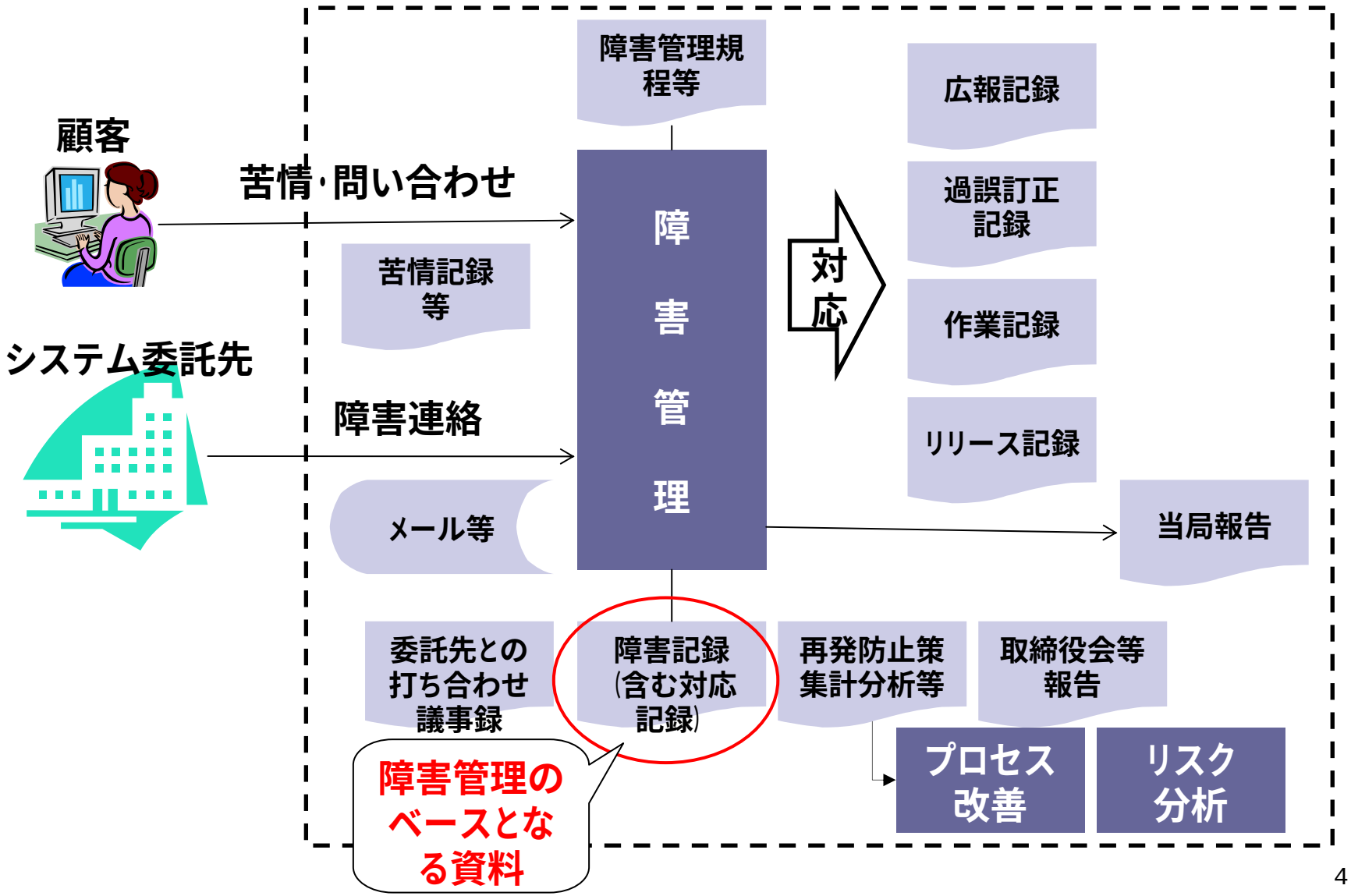
評価項目の事例

評価基準項目
業務実施状況
SLA達成状況
コスト
工程管理状況
技術力
業務管理体制
情報セキュリティ体制
会社としての支援体制
(注)提案と比較すること



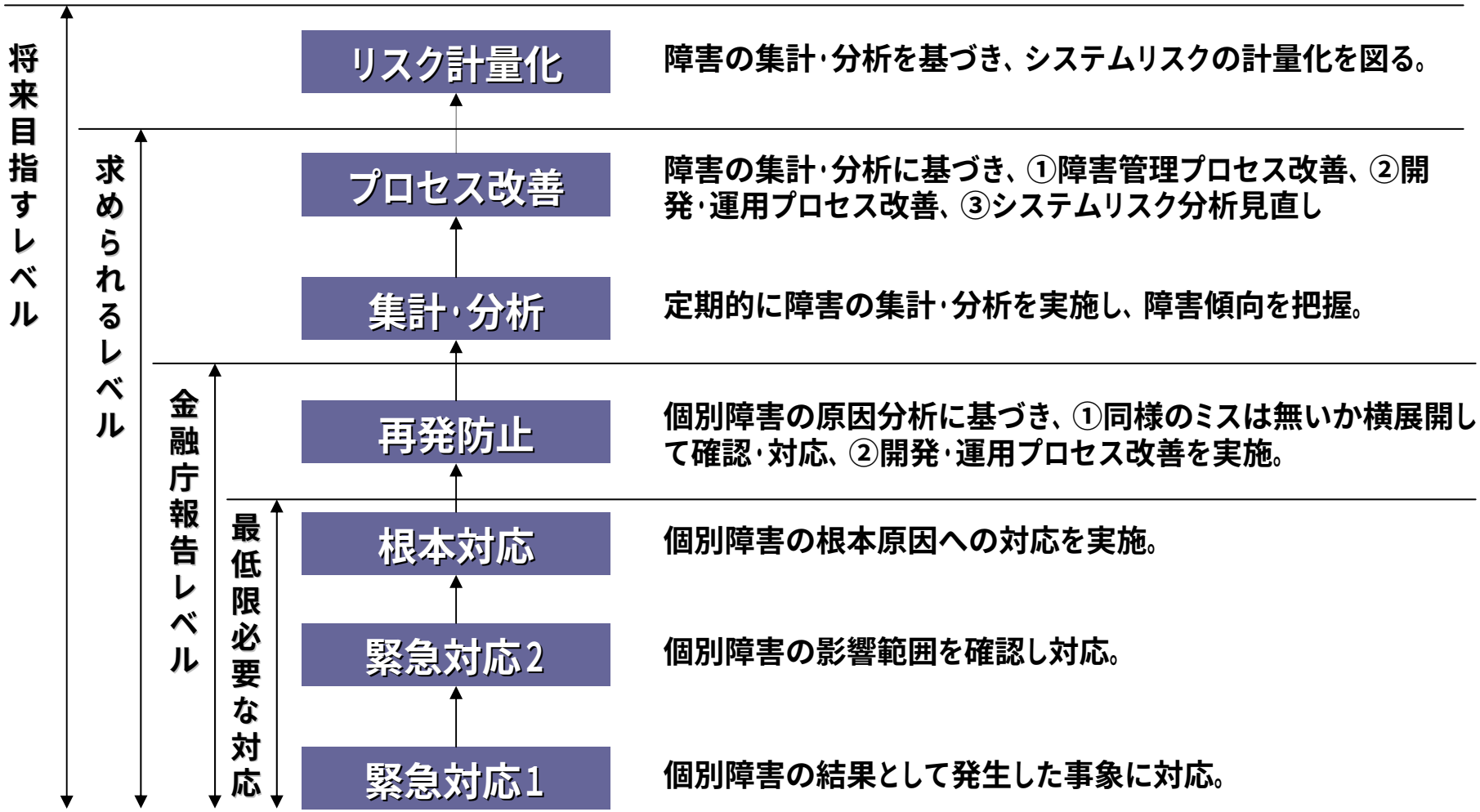
各項目の具体的な
判定基準を策定

障害管理


障害管理規程等
広報記録
顧客
苦情・問い合わせ
過誤訂正記録
苦情記録等
障害管理
対応
作業記録
システム委託先
障害連絡
リリース記録
メール等
当局報告
委託先との打ち合わせ議事録
障害記録(含む対応記録)
再発防止策集計分析等
取締役会等報告
プロセス改善
リスク分析
障害管理のベースとなる資料

障害管理

求められている障害管理とは？



障害管理

障害管理表（障害記録）管理項目の事例

共通項目	対応のための項目	分析のための項目
判明日時	影響	原因分類
発生日時	原因	プログラム稼動期間
復旧日時	根本原因	原因工程
システム名	緊急対応	システム停止時間
サブシステム名	緊急対応完了日	損害額
内容	根本対応	
担当者	根本対応完了日	
委託先会社	再発防止策	
委託先担当者	再発防止策完了日	
重要度	当局報告要否	
顧客影響有無	当局報告日	
	約定訂正実績	

障害管理

障害集計の事例

原因分類 / システム名	ハード	ネットワーク	インフラソフト	システム負荷	アプリ	作業・ペミス	相場配信元カバー先等	その他	計	内当局報告
Aシステム	18	0	10	15	45	1	0	20	109	0
Bシステム	1	0	0	0	85	2	0	3	91	8
Cシステム	0	2	2	0	12	25	0	8	49	2
Dシステム	3	1	3	1	28	9	12	1	58	0
計	22	3	15	16	170	37	12	32	307	10

原因工程 / システム名	要件定義	設計	製造	テスト	移行	その他	計
Aシステム	1	18	15	10	0	1	45
Bシステム	35	21	12	15	1	1	85
Cシステム	0	2	4	6	0	0	12
Dシステム	2	4	7	12	2	1	28
計	38	45	38	43	3	3	170

障害管理

障害管理において障害件数は重要な指標であるが、例えば大規模システムの新規稼動、システム改修の多い場合などは障害件数は多くなるので、一概に障害件数だけで評価できない。例えばリリース後一定期間に発生した障害を初期障害として別管理している会社もある。

(参考) 障害に関する指標の事例

区分	指標名	用途／目的	計算式
オンラインシステム	オンラインシステムの稼働率	品質基準の設定時などで当初稼動させると計画した時間に対する、オンラインシステムが実際に稼動した時間の割合。	オンラインシステムが実際に稼動した時間数／当初稼動させると計画した時間数。
全般	稼動品質率	利用者に、障害発生による迷惑をかけていないことの確認。総資産規模に対する、障害で利用者に迷惑をかけた回数の割合。	利用者に迷惑をかけた回数／ソフトウエアの量。 ソフトウエアの量には、ファンクションポイント数、あるいは総ステートメント数などがある。
全体	規定時間以上のシステム停止回数	システム障害の中、あらかじめ定めた上限の時間以内では回復はできなかった障害の割合。	－
オンラインシステム	お客様迷惑度指数	オンラインシステムでトラブルが発生した時に、そのトラブルによるお客様への影響を数値化して、客観的に把握しようとするもの。	(迷惑を与えた対象＋業務の重要度) ×量×(再発、反復性) 「量」は影響件数を使用するが、これが不明な場合には (影響時間×影響割合×ピーク性) で算出する。
全般	年間の運用費用1億円当たりの事業を中断した障害件数	事業の実施に支障が出た障害の年間の発生回数を、年間の運用費用の総額(億円単位)で割ったもの。	事業の実施に支障が出た障害の年間の発生回数／年間の運用費用の総額 (億円単位)

2009年4月 IPA「重要インフラ情報システム信頼性研究会報告」より抜粋

その他考慮すべき事項

根本的な課題

- **経営戦略とIT戦略のギャップ**
  経営環境の変化に対応するための業務改革とそれらを効果的に実現するための情報システムの見直しが十分行われていない。
- **空洞化**
  企業規模が大きくなるについて、IS機能のアウトソーシング比率が高まっている。
- **ITガバナンス機能の不在**
  実質的なCIOの不在、または、その機能が欠如している。
- **要件定義能力の低下**
  実現したいシステムの使用が明確になっていないままISの構築に着手している。
- **IT投資戦略の不在**
  実現したい機能をベースにシステムコストを積算せず、予算ありきでIS費用を決定している。
- **利活用の未熟**
  IS機能の整備による効果を、組織力向上に結びつけることがなかなかできにない。

日本情報システム・ユーザ協会（JUAS）による「企業IT動向調査」より

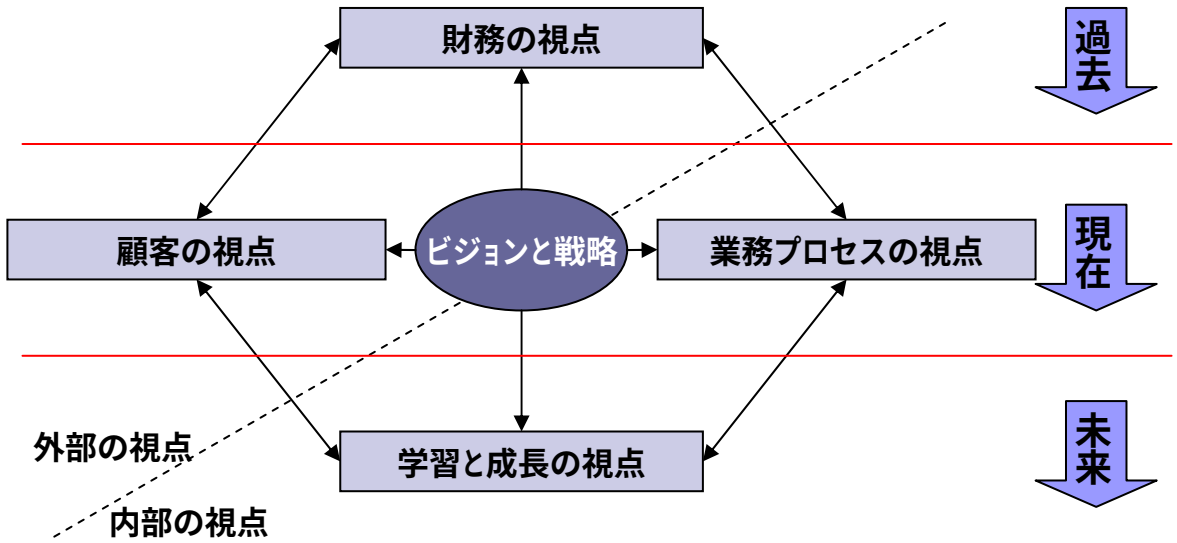
検討する上での参考事項
「バランススコアカード」

企業のビジョンと戦略を4つの視点かに具体的なアクションに繋いで計画・管理するための経営戦略立案・実行評価のフレームワーク。

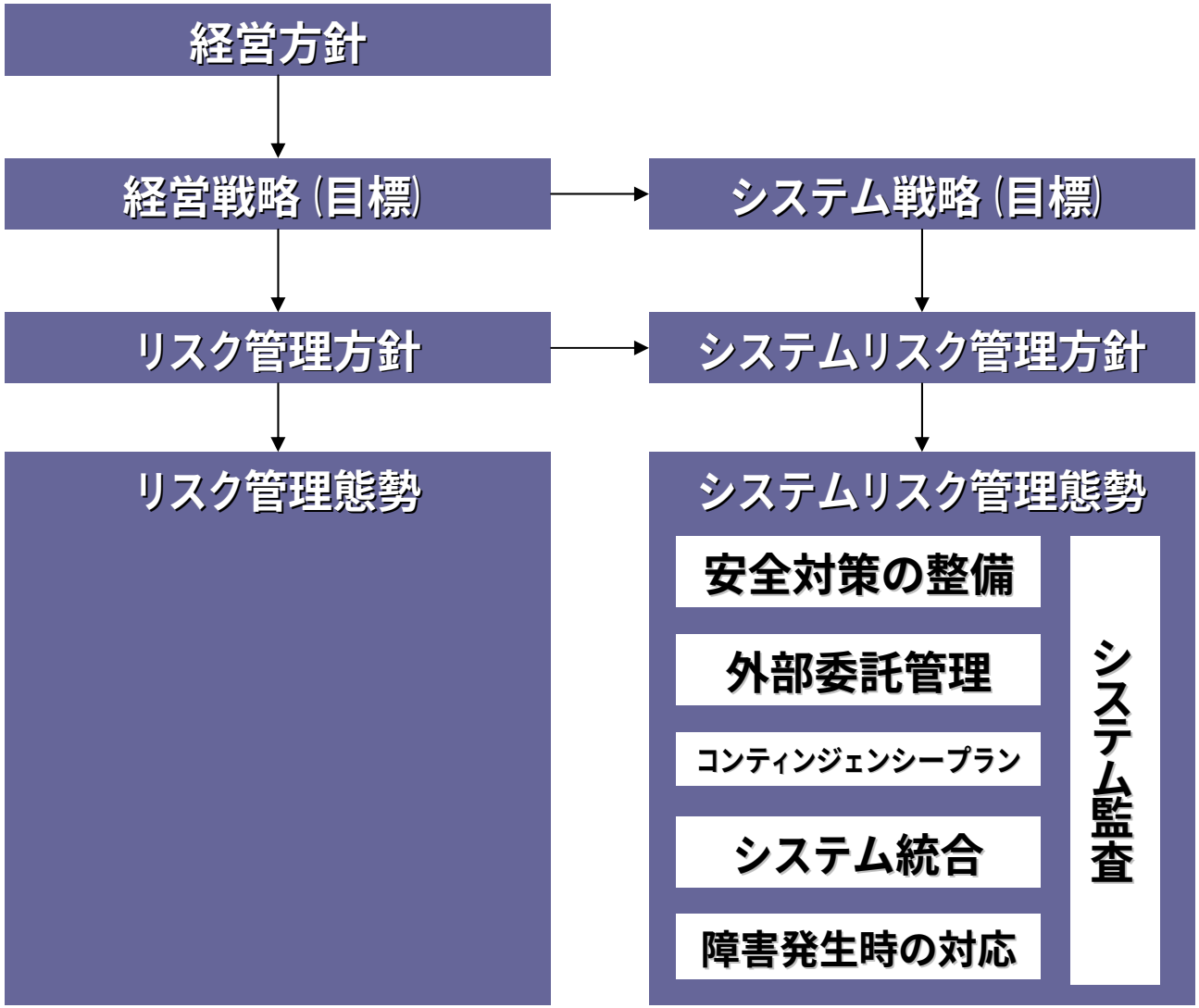
4つの視点

財務の視点:
株主や従業員などの利害関係者の期待に応えるため、財務の視点から目標の達成を目指す。
顧客の視点:
財務の視点を実現するために、顧客（外部）の視点から目標の達成を目指す。
業務プロセスの視点:
財務目標の達成や顧客満足度を向上させるために、どのように業務プロセスを改善するか、業務改善に関する目標達成を目指す。
学習と成長の視点:
業務プロセスを改善し、顧客満足度を向上させ、財務目標を達成するためには、どのように従業員の能力を高めるか、能力開発に関する目標達成を目指す。

基本コンセプト



経営戦略とシステム戦略



CIOの役割

システム部門管理者の疑問
「情報システム／システム部門に対する経営者の理解が足りないのでは?」
「CIOがいない、又はCIOはいるが役割を果たしていないのでは？」

CIOの役職ではなく機能・役割として捉えて考えては…

＜CIOの主な役割＞

「経営・事業戦略の計画・立案」「ITとビジネスニーズの連携実現」

「情報システム戦略の立案・執行」「ITに関わる前者最適の実現」

「IT投資・コストの適切な管理」「ITリスクの適切な管理」

＜CIOに求められる主なスキル＞

「プロセス＆プロジェクトマネジメントスキル」

「コミュニケーションスキル」

「モニタリング＆コントロールスキル」

「情報リテラシー」

(参考)「CIO育成テキスト」(IPA)

2010年4月28日日経コンピュータ
「CIOオフィスを創る」より

従来の情報システム部門でもなく経営企画部門でもない新しい情報化推進部門が続々と登場している。名称は千差万別だが、米国では一般的な**「CIOオフィス」**そのものだ。経営戦略と情報化戦略を同期させるために、システム開発・運用部門やITベンダーと連携しながらに、経営改革や業務改革を推進することを専門とする。

人材育成

まず、自社で必要な人材を明確化すること。

＜必要な人材を考えるために重要なこと＞

①「システム開発・運用の知識・経験≠システムリスク管理の知識・経験」を認識し、開発・運用力と管理力のバランスをとることが重要。

②開発・運用力、管理力とも外部委託で補えるプロセスと補えないプロセスがあることを認識し、補えないプロセスを実行できる人材の育成が重要。また、「補えないプロセス」は会社の状況によって異なるが、少なくとも要件定義、受入検収、委託先評価等のプロセスを実行できる人材が必要。

③システムは業種・業務によって求められる品質が異なり、特に金融システムは高い品質を求められているという認識が重要。単にシステム開発・運用経験が豊富ということで採用して任せきりにしては、管理が不十分になる可能性がある。

（注）「人材育成」とは、社内人材のレベルアップだけでなく、中途採用等の外部調達を含む。

人材育成

システムのライフサイクルと役割分担の事例

システム開発工程		開発						運用
		企画		設計	製造		導入	
担当 ＼ ライフサイクル		企画	要件定義	設計	プログラミング	テスト	導入	運用・保守
自社	業務部門	要件提示	要件定義 RFP作成 委託先選定			業務対応 テスト確認 受入テスト	訓練 移行手続	業務運用
	システム部門	システム化企画	要件定義 RFP作成 委託先選定	進捗管理 設計確認	進捗確認	進捗管理 受入テスト	進捗確認 移行作業	管理
委託先	開発業者	資料提供	提案	設計	プログラミング	テスト	移行作業	保守
	運用業者			運用設計	導入準備	運用テスト	導入	運用

外部委託しているからシステム関連のスキルは必要ない。」は、大きな誤り！

＜主な必要スキル＞

①システムリスク管理のスキル

②企画のスキル（含む業務知識）

③プロジェクト・マネジメントのスキル

さらにシステム開発、運用のスキルがあればベター。

人材育成

☆UISSの活用

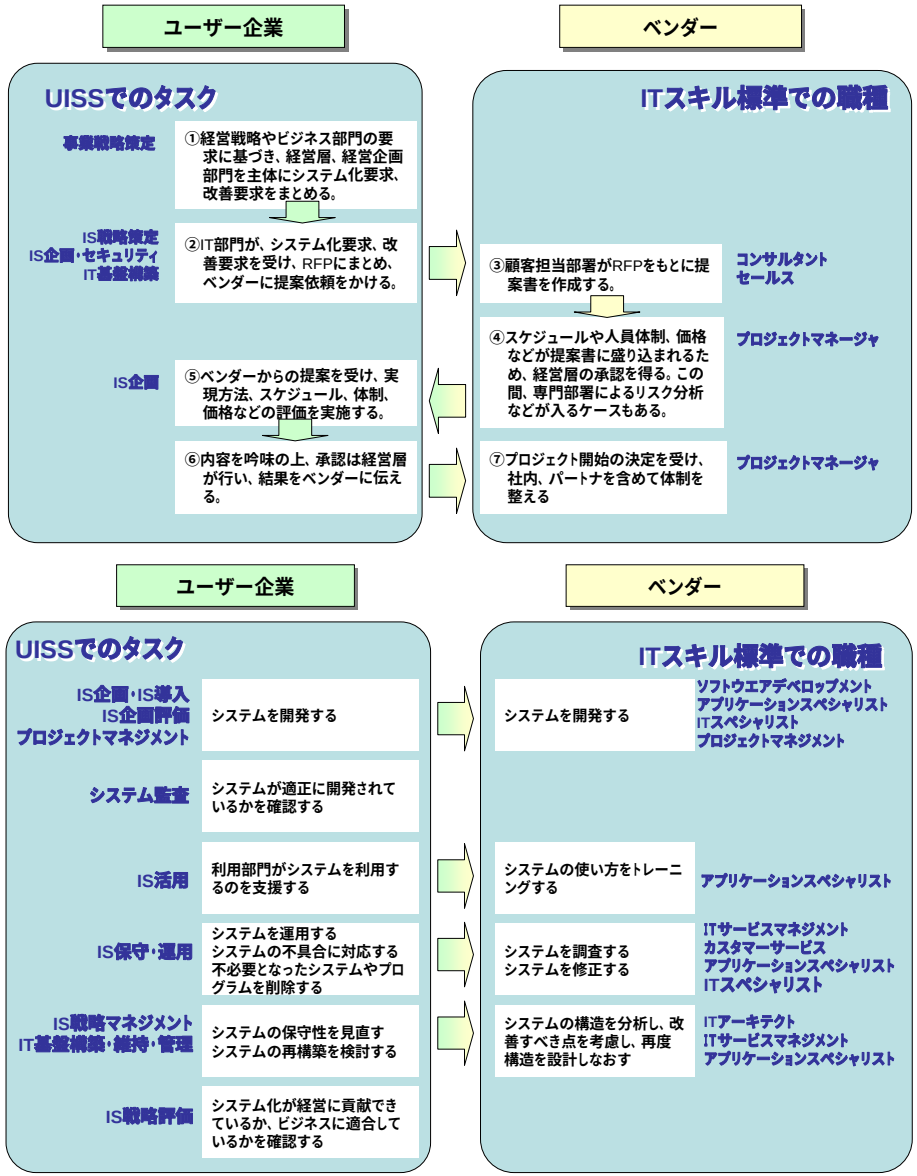
UISSを参考にして、必要なスキルを整理してみることも有効。

「情報システムユーザースキル標準」

～ UISS ～

情報システムユーザー企業における情報システムにかかわる組織や人に必要となる知識を、網羅的かつ体系的に整理・一覧化したもの。

IPA「UISS有効活用ガイド」より



人財育成　~~人材育成~~

人材から人財へ

「人・物・金」
は経営資源。

人を
「材料から財産へ」

参考）UISSの人材像とタスクの関連

IPA「UISS有効活用ガイド」より

タスク ＼ 人材像	ビジネスストラテジスト	ISストラテジスト	プログラムマネージャ	プロジェクトマネージャ	ISアナリスト	アプリケーションデザイナー	システムデザイナー	ISオペレーション	ISアドミニストレータ	ISアーキテクト
事業戦略策定	■	▨								
IS戦略策定	▨	■	▨							▨
IS戦略実行マネジメント		▨	■							
プロジェクトマネジメント				■	▨					
IS企画				▨	■	▨	▨		▨	
IS導入(ｱﾌﾟﾘｹｰｼｮﾝｺﾝﾎﾟｰﾈﾝﾄ)				▨	▨	■	▨	▨	▨	
IS導入(ｼｽﾃﾑｺﾝﾎﾟｰﾈﾝﾄ)				▨	▨	▨	■	▨	▨	
IS企画評価				▨	■	▨	▨		▨	
IS保守(ｱﾌﾟﾘｹｰｼｮﾝｺﾝﾎﾟｰﾈﾝﾄ)						■	▨	▨	▨	
IS保守(ｼｽﾃﾑｺﾝﾎﾟｰﾈﾝﾄ)						▨	■	▨	▨	
IS運用						▨	▨	■		
IS活用						▨			■	
IS戦略評価	▨	■	▨							▨
事業戦略評価	■	▨								
IT基盤構築・維持・管理							▨			■

凡例　■ 主たる領域　▨ 従たる領域

＜UISS人材像の事例＞

ISストラテジスト…事業戦略実現に向けたIS戦略を策定・評価する。

プロジェクトマネージャ…IS戦略実現に向けて、個別案件をマネジメントする。

システムデザイナー…IS戦略実現に向けた、個別案件のアプリケーションコンポーネントの導入・保守を実施する。

システムリスク管理態勢について
～　検査官の視点で　～

ご清聴ありがとうございました。

ご質問がありましたら