国際銀行協会　情報フォーラム

検査官の視点で見た

システムリスク管理態勢のポイント

～検査マニュアルに沿って～

平成23年10月11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

- はじめに
- 検査マニュアルについて
- 検査官の視点で見たシステムリスク管理態勢のポイント
- まとめ

(注) 本日の講演内容は藤田個人の見解です。

はじめに

- 検査官は検査の中で検査マニュアルに基づき被検査先のシステムリスク管理態勢に関する事実を確認している。
- 本日は、検査官から見たシステムリスク管理態勢のポイントを、検査マニュアルに沿って述べていく。
- 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。

検査マニュアルについて

(注) 正式名称

「金融商品取引業者等検査マニュアル」

検査マニュアルの位置づけ

「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。

↓

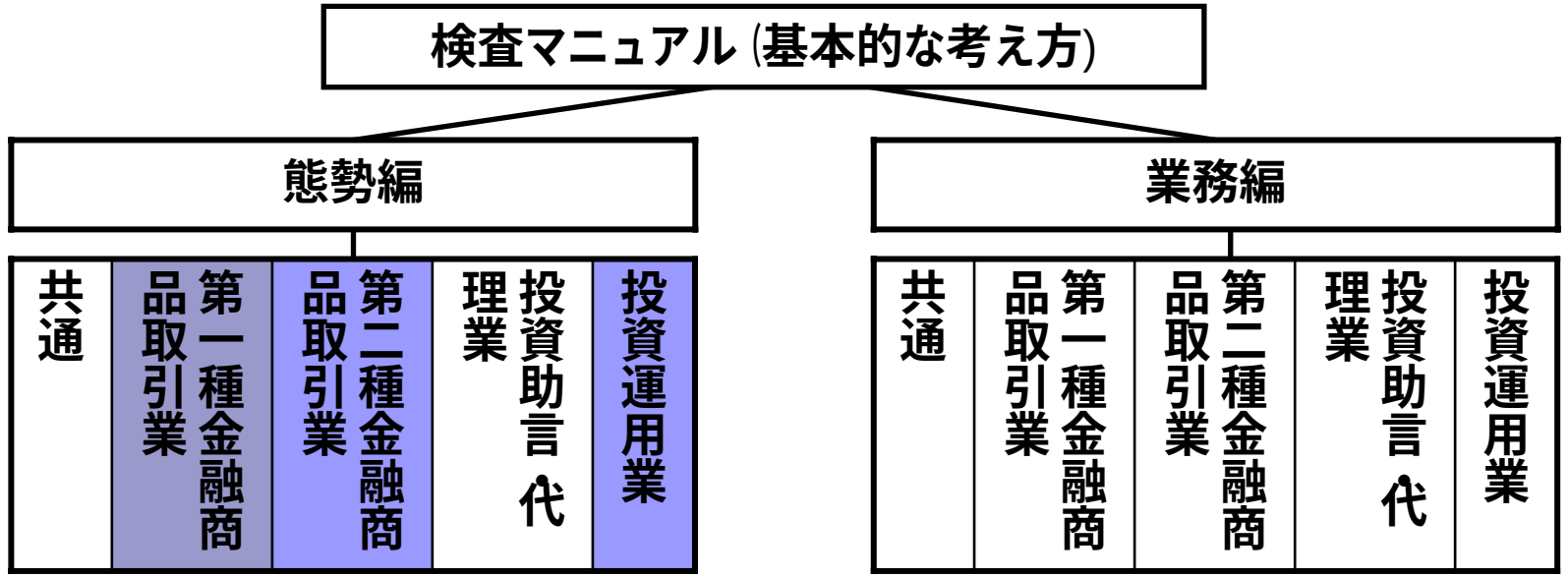
「金融商品取引業者等向けの総合的な監督指針」
　Ⅲ－２－８　システムリスク管理態勢
　Ⅳ－３－２－１(3) 証券会社等の電子情報処理組織の管理に係る留意事項

↓

「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

検査マニュアルの構成

経営管理態勢			
内部管理態勢･法令遵守態勢			
リスク管理態勢（財務の健全性等）			
自己資本規制関連リスク	事務リスク	システムリスク	その他リスク(運用リスク)(資金繰りリスク)等
内部(外部)監査態勢			
危機管理態勢			



検査マニュアルの構成

＜「システムリスク管理態勢」の項の構成＞

(1)システムリスクに対する認識等 — 経営者のリスク認識と管理方針の決定

(2)適切なシステムリスク管理態勢の確立 — システムリスク管理方針の決定と体制の整備

(3)安全対策の整備 — 上記(2)に基づく管理手順と担当部署の整備

(4)システム統合

(5)障害発生時の対応

(6)コンティンジェンシープラン

(7)外部委託管理

（(4)～(7)：特に重要な事項）

(8)システム監査 — システム監査態勢の整備

検査マニュアルの構成

検査マニュアルの項目をリスク･マネジメントの観点から整理

リスクマネジメント（広義）

リスクマネジメント（狭義）

リスク顕在化

クライシスマネジメント

(1)システムリスクに対する認識等

(2)適切なシステムリスク管理態勢の確立

(3)安全対策の整備

①情報セキュリティ管理態勢の整備

②システムの運用及び保守管理態勢の整備

③システムの企画及び開発管理態勢の整備

(5)障害発生時の対応

(6)コンティンジェンシープラン

(7)外部委託管理

(4)システム統合

(8)システム監査

検査マニュアルの改訂

平成２３年４月１日「金融商品取引業等検査マニュアル」の改正項目

1．「適切なシステムリスク管理態勢の確立」にシステムリスク管理方針の記述を追加。

2．「安全対策の整備」に「情報セキュリティ管理態勢の整備」の項を追加。

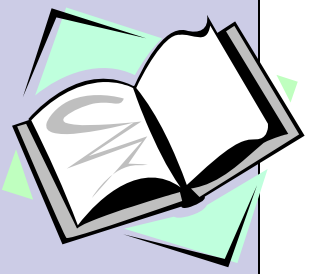
　特に、サイバー攻撃への対応を記載。

3．「安全対策の整備」に以下を追加。

・開発担当と運用担当の相互牽制体制構築。

・容量や処理能力等の点検と発生した問題点の管理手順。

・システム本番移行時の移行判定。



4．「障害発生時の対応」に障害の全体的な発生状況・原因等についての分析と再発防止策を追加。

5．「コンティンジェンシープラン」にサイバー攻撃時の対応手順を追加。

6．「外部委託先管理」を「外部委託管理」に変更し、注釈を追加。

7．「システム監査」に問題点の改善フォローを追加。

8．「大規模かつ複雑な業務をグループとして行う証券会社グループのリスク管理態勢等」の「システムリスク管理態勢」を追加。

検査マニュアルの視点で見たシステムリスク管理態勢のポイント

(注) 次ページ以降の凡例

管理上のポイント

検査で見られる問題点

(1)システムリスクに対する認識等

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」

システムリスクには情報セキュリティやリスクが顕在化した時の対応態勢（クライシスマネジメント）を含んでいること。

検査官に対して「自社のシステムリスクはシステム障害と認識しており、障害時の対応は十分実施している。」と説明する等、リスクマネジメントとクライシスマネジメントの違いを十分認識していない経営者がいる。

(2)適切なシステムリスク管理態勢の確立

自社のリスクに見合ったシステムリスク管理方針を策定すること。

同管理方針には、情報セキュリティポリシーと外部委託管理方針を含むこと。

どこが見たような「システムリスク管理方針」だが、本当に自社のリスクを適切に認識できているのか？

グローバルの「システムリスク管理方針」に沿う必要はあるが、それだけで本当に十分か？　日本独自のリスクはないのか？

(参考)「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

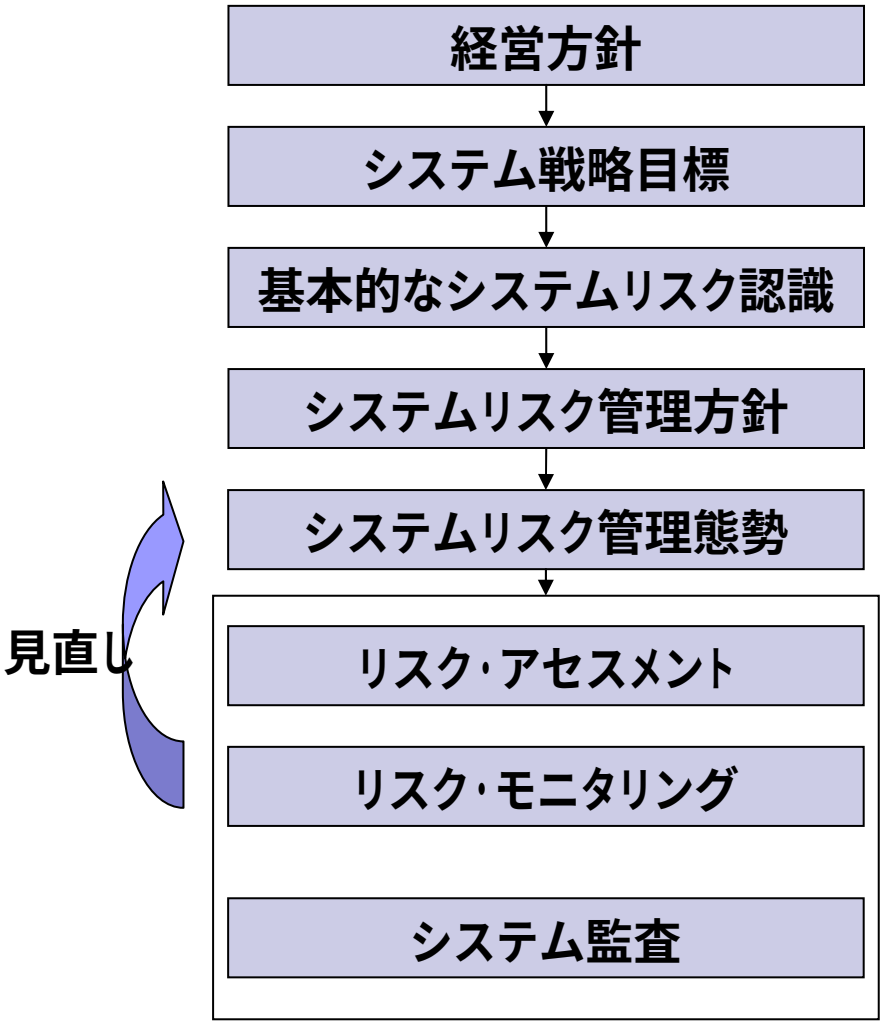
登山において、山頂に向けて選択したルートによって遭難リスクが異なるように、経営目標実現に向けて選択したIT戦略により「システムリスク」が異なる。

現在のシステム管理状況のみで「システムリスク」を判断できない。

(2)適切なシステムリスク管理態勢の確立

システムリスク管理のプロセスを確立すること。

＜システムリスク管理プロセスの例＞



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。

(2)適切なシステムリスク管理態勢の確立

システムリスク管理の実効性を確保すること。

リスク・アセスメントに現場の問題がフィードバックされていないケース。

システム障害分析結果		システムリスク分析結果
・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。	→ 見直しが必要	・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

リスクと課題を適切に管理していないケース。

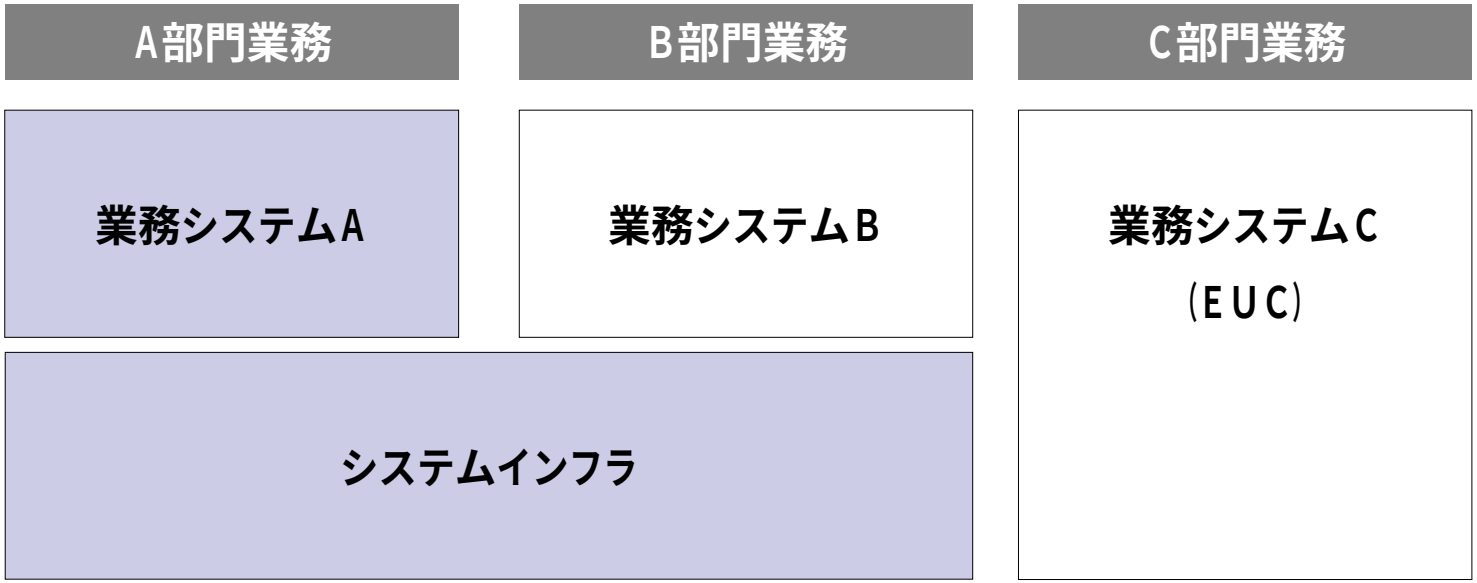
リスク管理		課題（問題）管理
顕在化していない不利になる可能性を、顕在化しないように又は顕在化しても影響を小さくするよう事前に対応する。	顕在化 → 管理目的の違いを認識	リスクが顕在化して、具体的な問題（課題）となった場合、その影響を小さくすると同時に、解決に向けて対応する。

（注）リスクを潜在課題と呼ぶこともある。

(2)適切なシステムリスク管理態勢の確立

管理すべきシステムリスクを適切にカバーしていないケース。

＜事例＞



システム部門がシステムリスク管理

他部門がシステムリスク管理又は管理対象外

→ システムリスク管理の不整合や管理漏れが発生

(3)安全対策の整備
①情報セキュリティ管理態勢の整備

管理すべき情報資産を特定、分類していること。

物理的･論理的な対策に加え人的な対策も重要。

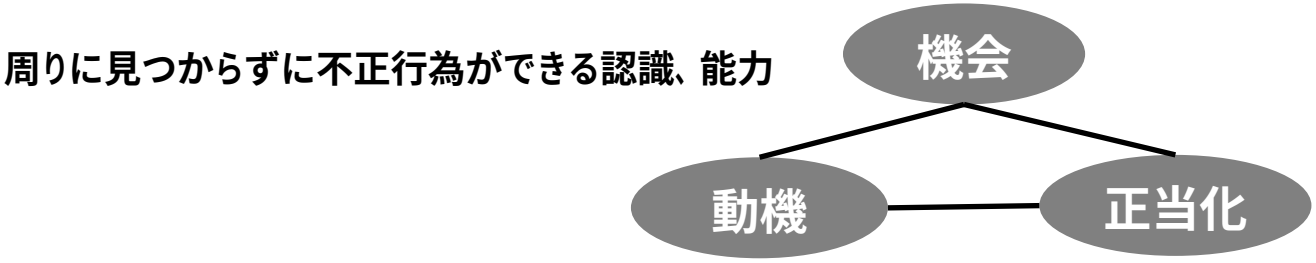
アカウント管理･ログ管理を含むアクセス管理が重要。

サイバー攻撃への対策も追加すること。

人的なリスク認識が不十分なケース。

サイバー攻撃のリスク対策が不十分なケース。

(参考) 不正のトライアングル　～ この3つが揃うと不正が発生しやすくなる ～



周りに見つからずに不正行為ができる認識、能力

他人に打ち明けられない問題、過度のプレッシャー

自分がしようとしている行為を正当化する理由付け

(3)安全対策の整備

①情報セキュリティ管理態勢の整備

＜情報セキュリティ管理の例＞

外部委託先

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

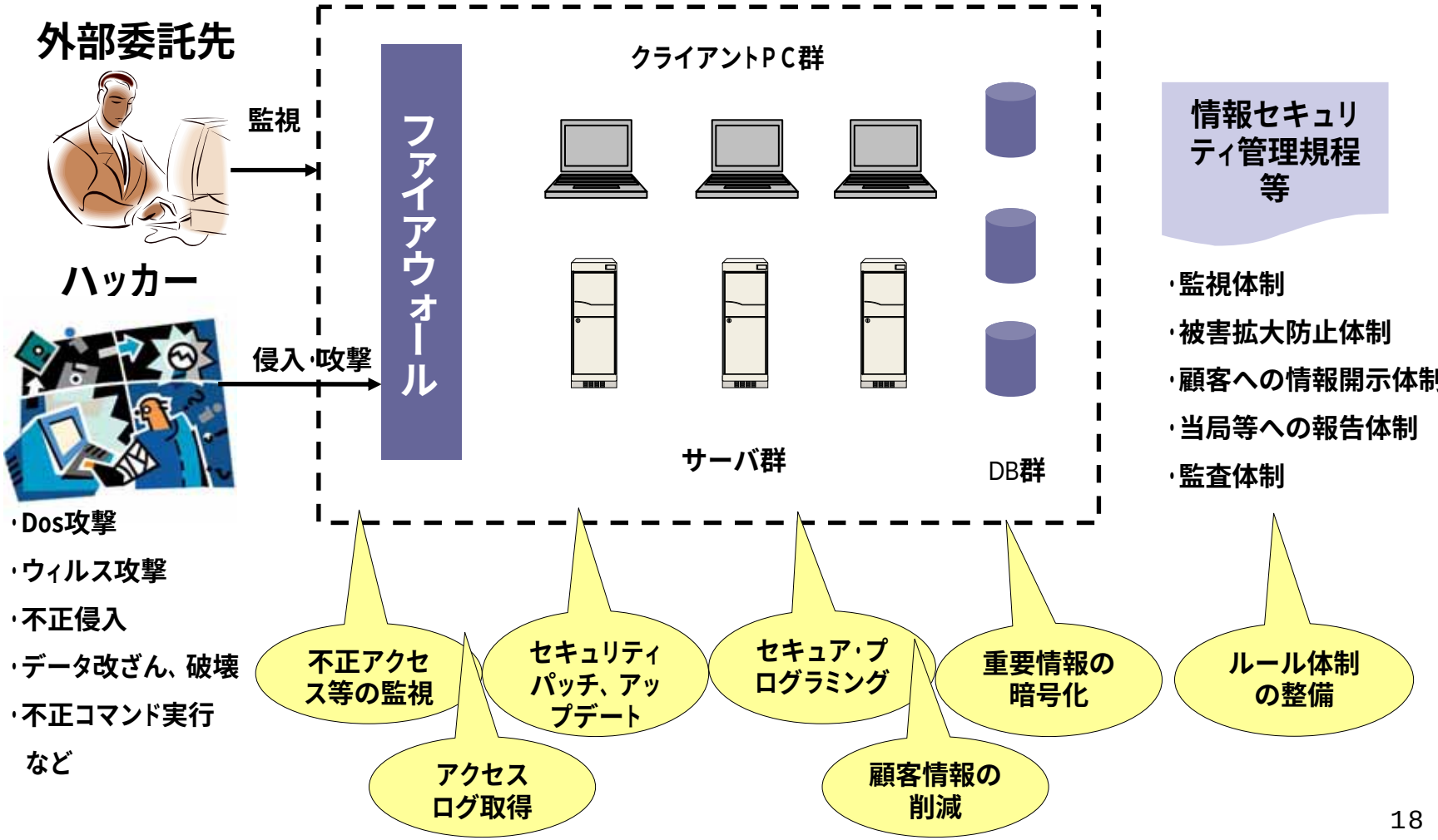
取締役会等報告

情報セキュリティ研修記録

情報セキュリティ管理のベースとなる資料

(3)安全対策の整備
①情報セキュリティ管理態勢の整備

＜サイバー攻撃対策の例＞



(3)安全対策の整備
②システムの運用及び保守管理態勢の整備

運用･保守に関する管理方針を定め、役割と責任を明確にすること。特に開発と運用の相互牽制体制を構築すること。

容量･処理能力等を含めたシステム稼動環境の点検項目･手順、発生した問題点の管理手順等を定めること。

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、安全対策の整備がシステムリスク管理の肝。

システム運用を外部委託等している場合、点検結果の確認や問題管理を任せきりにしたため、問題が再発したケース。
データ処理時限等のあるコーポレートアクション関連作業において、データ量予測に業務部門が関与していなかったため、正確なデータ量を予測できず、処理時限に間に合わなかったケース。

(3)安全対策の整備
③システムの企画及び開発管理態勢の整備

開発標準、品質管理基準など開発に関する適切なルールを制定すること。特に、進捗管理と品質管理が重要。

利用部門の役割と責任を明確にすること。

重要プロジェクトにおいては、適切な移行判定を行うこと。

開発標準

障害の未然防止のためには、開発における進捗管理と品質管理が重要で、それらの管理のベースとなるのが、開発工程、成果物などを定めた開発標準。

利用部門の役割

要件定義、業務フロー策定、受入確認テスト等が利用部門の基本的な役割。

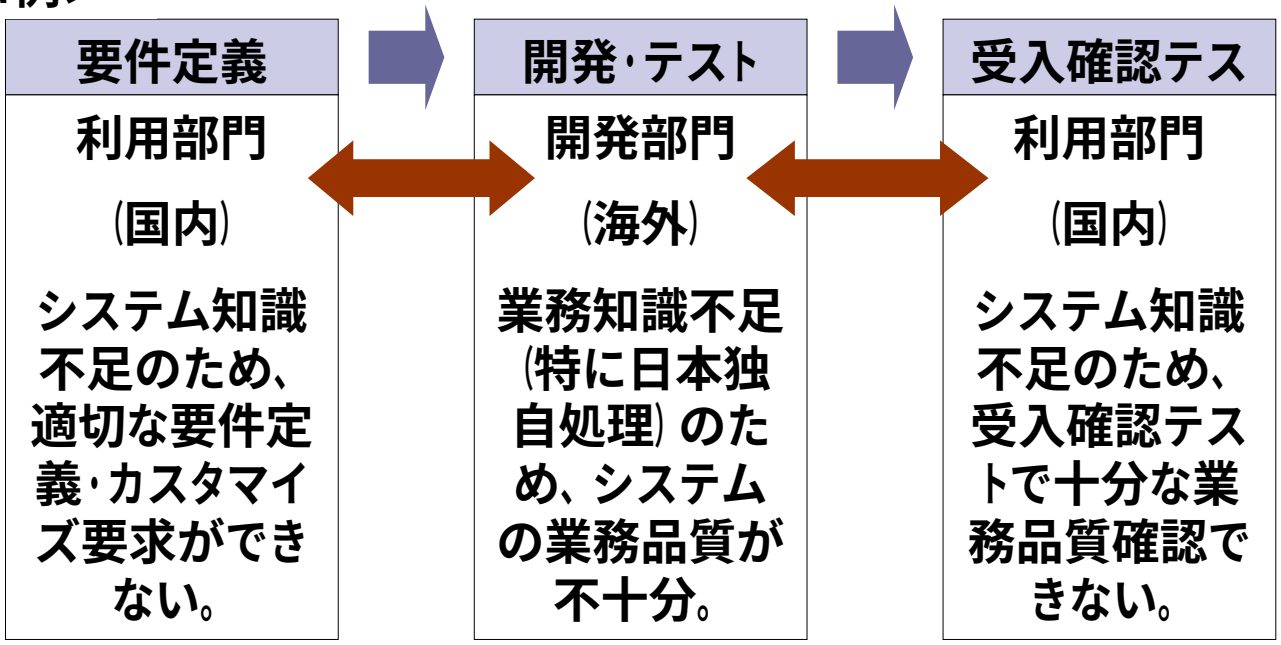
移行判定（稼動判定）

極力、定量的･客観的な移行判定基準を策定。業務事務を含む網羅性も重要。
さらに、移行判定に向けたスケジュール･体制などの移行判定計画を策定。

(3)安全対策の整備
③システムの企画及び開発管理態勢の整備

開発プロセス間･部門間の連携が不十分なため障害が発生しているケース。

＜事例＞



利用部門と開発部門の適切な連携を図ること、
また連携を図れる体制を構築することが重要。

(3)安全対策の整備
③システムの企画及び開発管理態勢の整備

不適切な開発管理に起因したアルゴリズム取引、コロケーションサーバ等の発注に関連する障害が増加している。

・発注機能に関する障害は、自社の顧客だけでなく、取引所システムや市場に影響を与えるリスクがある。

・特にアルゴリズム取引はデータ量が多く、誤動作時の影響が大きい。

発注機能に係るシステム変更時には、重要な開発事案であることを認識し、利用部門と開発部門の適切な連携を図った上で、利用部門の受入テストを含む十分な確認を実施すること。

発注機能に、例えば発注回数・発注量の上限を設定する等、誤発注防止機能を組み込むこと。

(4)システム統合

最も重要なことは、経営の関与と統合へ向けた糊代のある協調体制。

システム開発だけでなく、業務対応、移行判定、不測の事態（注）への対応なども重要。

「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」のフレーム	
Ⅰ．経営陣のリスク管理に対する協調した取組み	Ⅲ．不測の事態への対応
ⅰ．経営統合に係るリスク管理態勢のあり方	Ⅳ．監査及び問題点の是正
ⅱ．システム統合に係るリスク管理態勢のあり方	ⅰ．内部監査
Ⅱ．協調したシステム統合リスクの管理体制のあり方	ⅱ．第三者機関による評価
ⅰ．セキュリティ管理体制の整備	
ⅱ．協調した事務リスク管理態勢のあり方	
ⅲ．協調したシステムリスク管理態勢のあり方	
ⅳ．協調した業務運営態勢のあり方	
ⅴ．外部委託業務管理態勢のあり方	

（注）「不測の事態」とは？

①プロジェクトの不測の事態

②移行作業における不測の事態

③稼動直後の不測の事態

(5)障害発生時の対応

障害発生時の対応手順、対応体制を整備し、訓練や実際の対応を評価するなどして、実効性を確保すること。

社内対応だけでなく、顧客への広報、自主規制機関、当局への報告など外部にも適切に対応すること。

＜「障害発生時の対応」の位置づけ＞

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」ことであれば、「障害発生時の対応はリスク管理の失敗の後始末」とも言える。

「障害発生時の対応」が重要であることは言うまでもないが、「システムリスク管理」という意味では、障害を発生させないようにするための対応、例えば安全対策の整備等が、「システムリスク管理」の本質と言える。

(5)障害発生時の対応

障害管理のベースとなる「障害記録」を適切（注）に作成し、管理すること。

＜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	

（注）「適切」とは？

・網羅性

・管理可能性

・分析可能性

(5)障害発生時の対応

個別障害の再発防止策だけでなく、障害の全体的な発生状況・原因等についての分析を通じた再発防止策を行うこと。

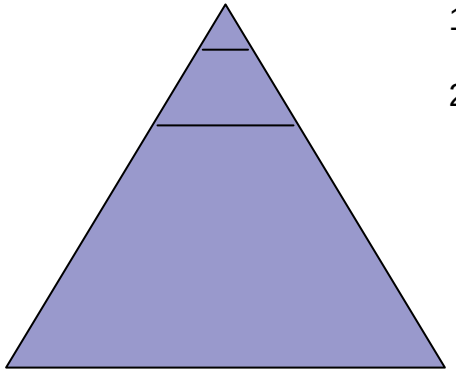
軽微障害も含めた障害を定期的に集計・分析して傾向を把握し、プロセスを改善することで、重大障害の防止を目指す。

重大障害として顧客等の外部に影響をあえたる障害は氷山の一角で、実際には、バグ、ミス等による軽微障害は多数発生している。

(参考)「ハインリッヒの法則」

重大事故の背景には、軽微な事故が29件発生しており、さらに危うく事故になるような「ヒヤリ」「ハッと」するような出来事が300件あるという法則。

重大障害は、決して偶発的な産物ではない、ということを教えてくれている。



(5)障害発生時の対応

障害の再発防止策を未実施のまま稼動し、再発したケース。

障害対応が遅延したケース。

顧客影響のあった障害が適切に管理されていないケース。

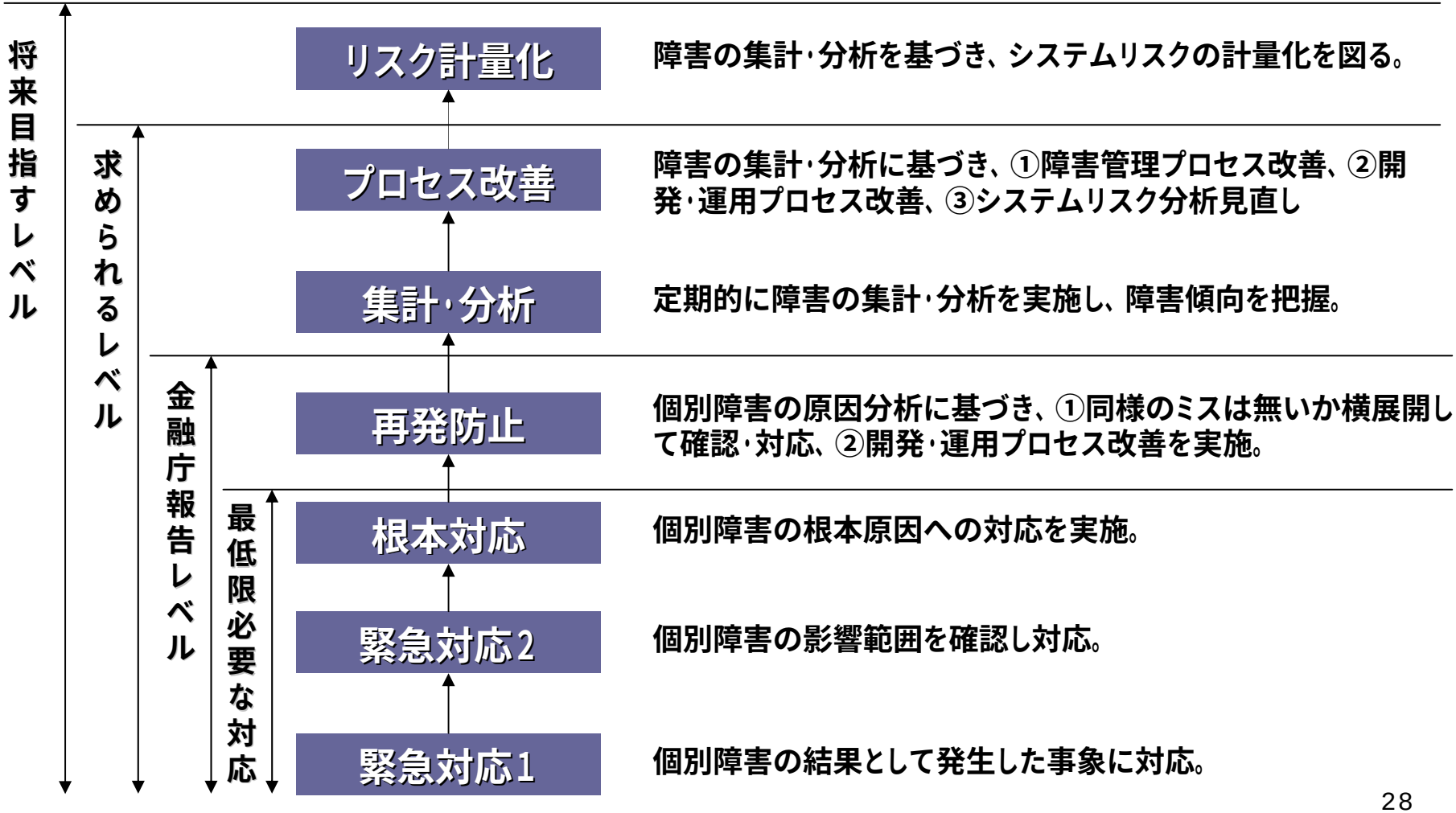
再発防止策が、他システムに横展開されず、同じ原因で再発したケース。

障害の発生状況の分析･原因等の分析を、部署･システム単位のみで実施しているケース。

経営レベルでは全社又はグループ全体を鳥瞰したシステムリスク管理態勢の不足、部門レベルでは部門間のコミュニケーション及び連携の不足に起因した問題が多い。

(5)障害発生時の対応

求められている障害管理とは？



(6)コンティンジェンシープラン

実効性を確保すること。特に訓練は重要。

サイバー攻撃等についても追加すること。

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。

脅威、シナリオや発動基準が不明確なケース。

データ保管等の業務継続計画の前提が適切に整備されていないケース。

新システム稼動等、環境が変わっても見直していないケース。

訓練を一度も実施していないケース。

＜東日本大震災で頻発した「想定外」への対応＞

当面、東日本大震災の教訓を参考に、想定する脅威、シナリオを見直す。

今後、ＢＳ２５９９９（事業継続マネジメント）等を参考に、ＢＣＰの策定方法を見直す。例えば、脅威・シナリオベースから経営資源(注)ベースアプローチに変更。

(注) People, Premises, Technology, Information, Supplies **等**

(6)コンティンジェンシープラン

＜東日本大震災を教訓にして＞

1．想定する脅威、シナリオの見直し

(1)広域型地震、津波

(2)長期間にわたる電気、ガス、水道、交通など社会インフラの停止

(3)上記(2)の結果として通信障害、燃料不足（特に自家発電装設備）

→　安否確認システム、燃料業者との緊急供給契約等の実効性？

(4)計画停電

(5)原発事故　など

2．実効性の確認

(1)訓練の重要性を再認識

3．事業継続とともに求められるもの

(1)生命の安全確保

(2)二次災害の防止

(3)地域貢献･地域との共生

(7)外部委託管理

外部委託のリスク認識に基づく管理体制を構築すること。

適切な選定基準、評価基準の定めて、評価すること。

機密保持、再委託条項、監査権限、ＳＬＡなど契約に明確に定めること。

運用の場合のＳＬＡ遵守状況、開発の場合の進捗･品質状況を把握と検収等、委託元としての適切な管理を実施すること。

グループ会社で開発、運用を実施している場合、「安全対策の整備」と位置付け管理するか又は「外部委託管理」として位置づけ管理するか明確になっておらず、また適切な管理ができていないケース。

(注) 検査マニュアルへの注記追加

「外部委託管理」の対象には、契約の形態や種類を問わず、金融商品取引業者がシステムリスクを認識すべきシステムに係る企画･開発･運用等の全部又は一部を他の者に行わせることを内容とする契約の一切を含む（明示的な契約が締結されていない場合も含む。）

(8)システム監査

システム部門から独立した専門家が、定期的に実施すること。

監査範囲は重要なシステムリスクをカバーすること。

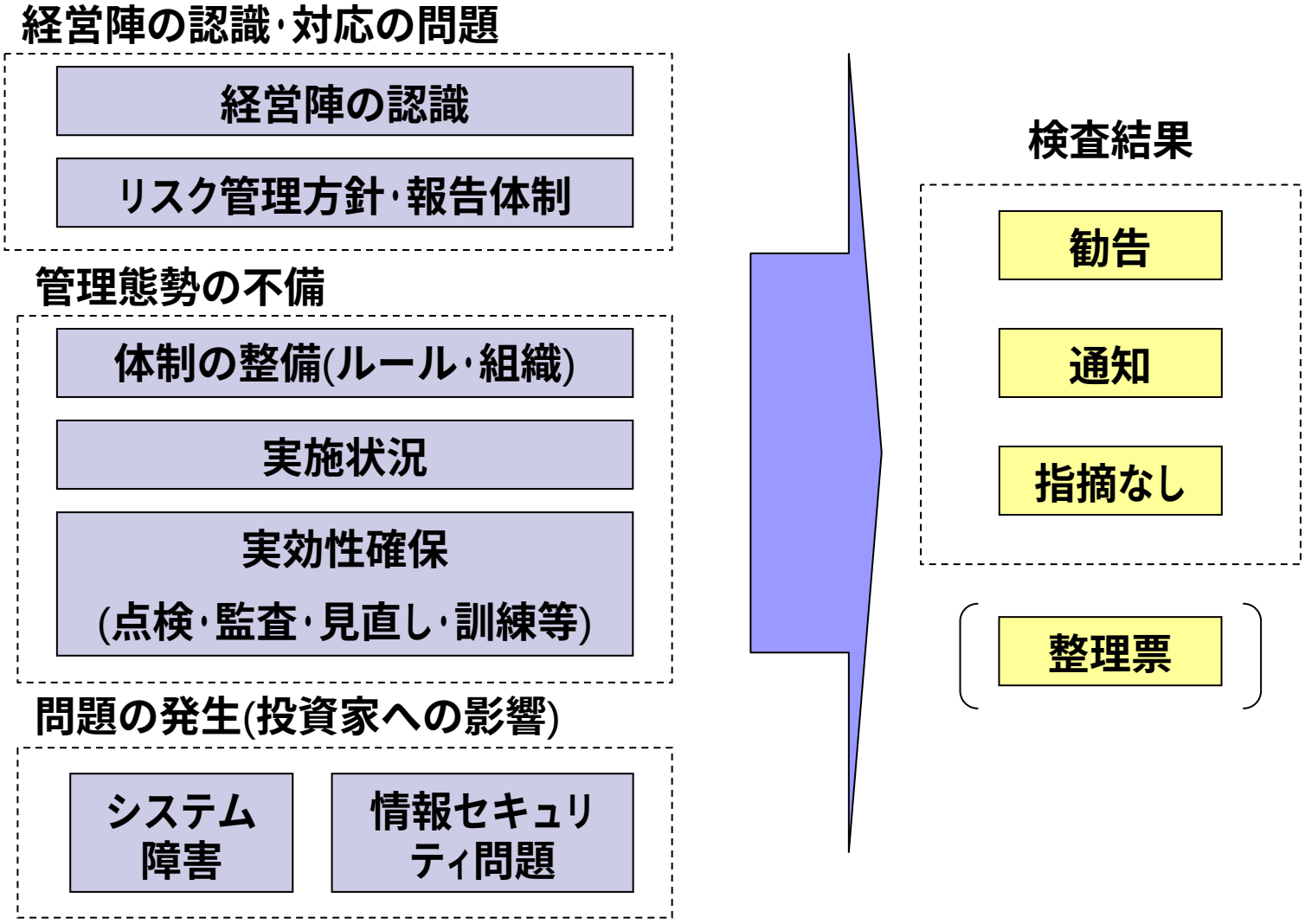
監査指摘事項をフォローすること。

システム監査プロセスの例

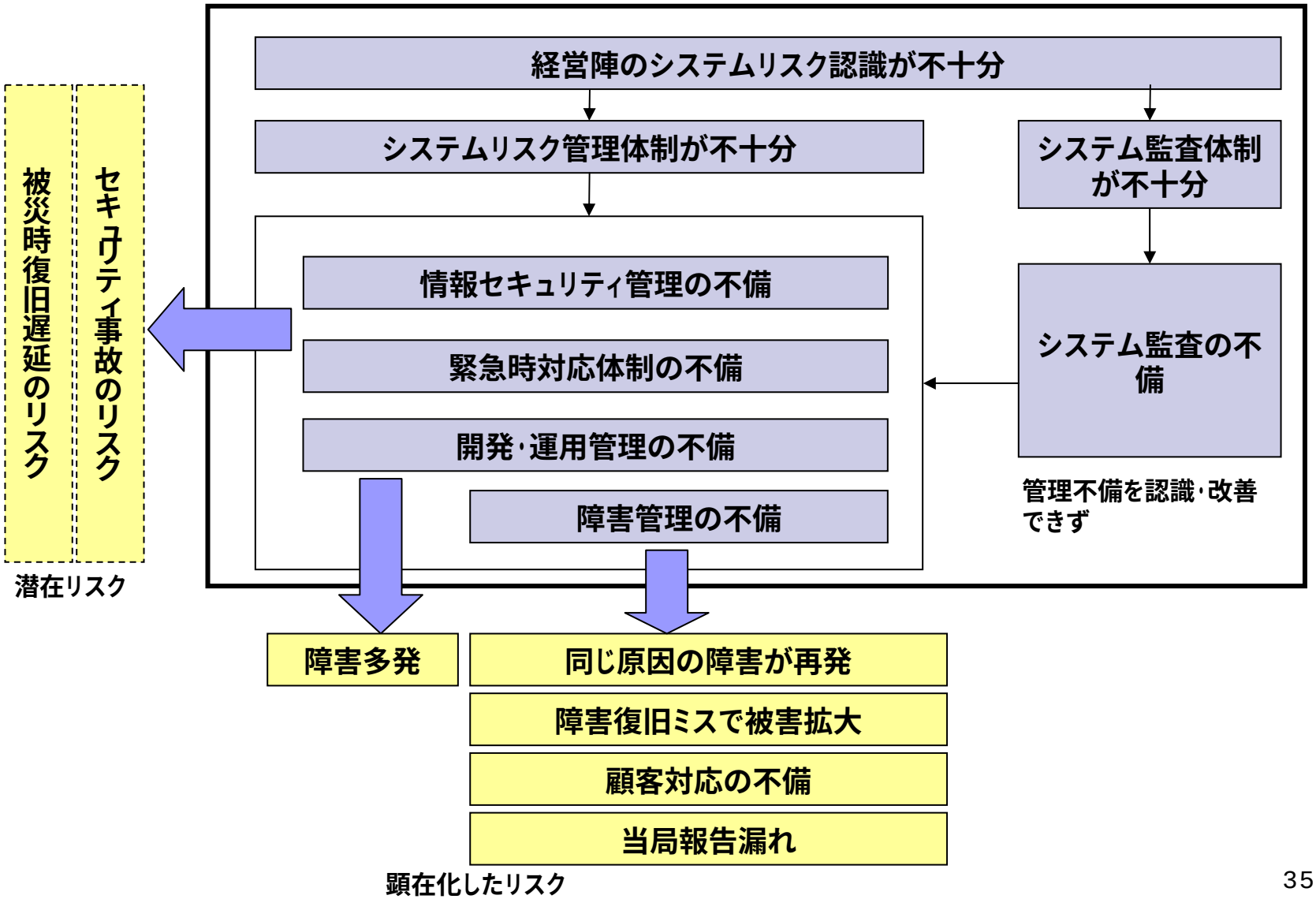
リスク分析・前年度実績	○システム監査の前提としてのシステムリスク分析 前年度システム監査実績、システムリスク分析結果の活用。
↓	
年度計画	○リスクベースをベースとしてシステム監査計画 リスクに応じたシステム監査の頻度、深度を基にした計画。
↓	
個別計画	○重点思考の個別システム監査計画 監査目的と重点項目を明確化した個別計画。
↓	
監査実施	○専門家のよる実施 社内に専門家がいなければ外部専門家に依頼。
↓	
報告	○重要性・緊急性を明確化した報告書の経営あて報告 指摘事項の重要性・緊急性を評価した報告書を取締役会等へ報告。
↓	
フォロー	○指摘事項のフォロー体制整備 指摘事項のフォローおよびフォロー監査の実施。
↓	
年度報告	○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。

まとめ

検査官から見た検査の枠組み



(参考) 検査官の視点で検査結果を整理した例 (よく見かけるパターン)

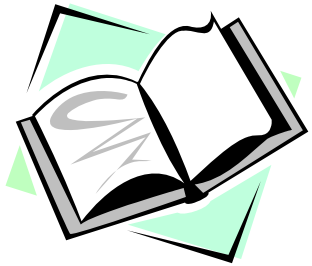


システムリスク管理態勢のポイント

- 経営のシステムリスクに対する理解
- 自社のリスクの見合った基本方針策定
- 態勢整備
- 実施状況把握
- 実効性確保
- 問題発生時の適切な対応

今日の話を踏まえて、

検査マニュアルの再確認を！



検査官の視点で見た

システムリスク管理態勢のポイント

ご清聴ありがとうございました。

ご質問がありましたら