横浜銀行

日本銀行金融機構局金融高度化センター

金融高度化セミナー資料

システムリスク管理体制の構築

株式会社　横浜銀行

執行役員　IT統括部長　米田誠一

＜目次＞

はじめに（背景）

１．バーゼルⅡに向けた対応

- バーゼルⅡ対応では、オペリスクを含めた自己資本比率算定のほか、金融機関自ら内在するリスクを発見し、把握・評価して、対策を行うPDCAの仕組み作りを行うことが必要であった。

- メリハリのある適正なリスク管理を行うため、システムと情報の重要度や形態に応じ、あるべきセキュリティレベルを設定し、実現を目指すためアセスメント（ＣＳＡ）に取り組んできた。

２．目白押しであった大型開発案件

- 平成１８年度は、開発すべき大型プロジェクトが数多く存在した。

- 並行するプロジェクトをトータルで管理し、計画どおり遂行するためには、問題点の早期発見と対策が必須であるが、銀行経営陣・主管部からアウトソーサーに至るまで進捗状況を可視化・共有することにより可能となる。

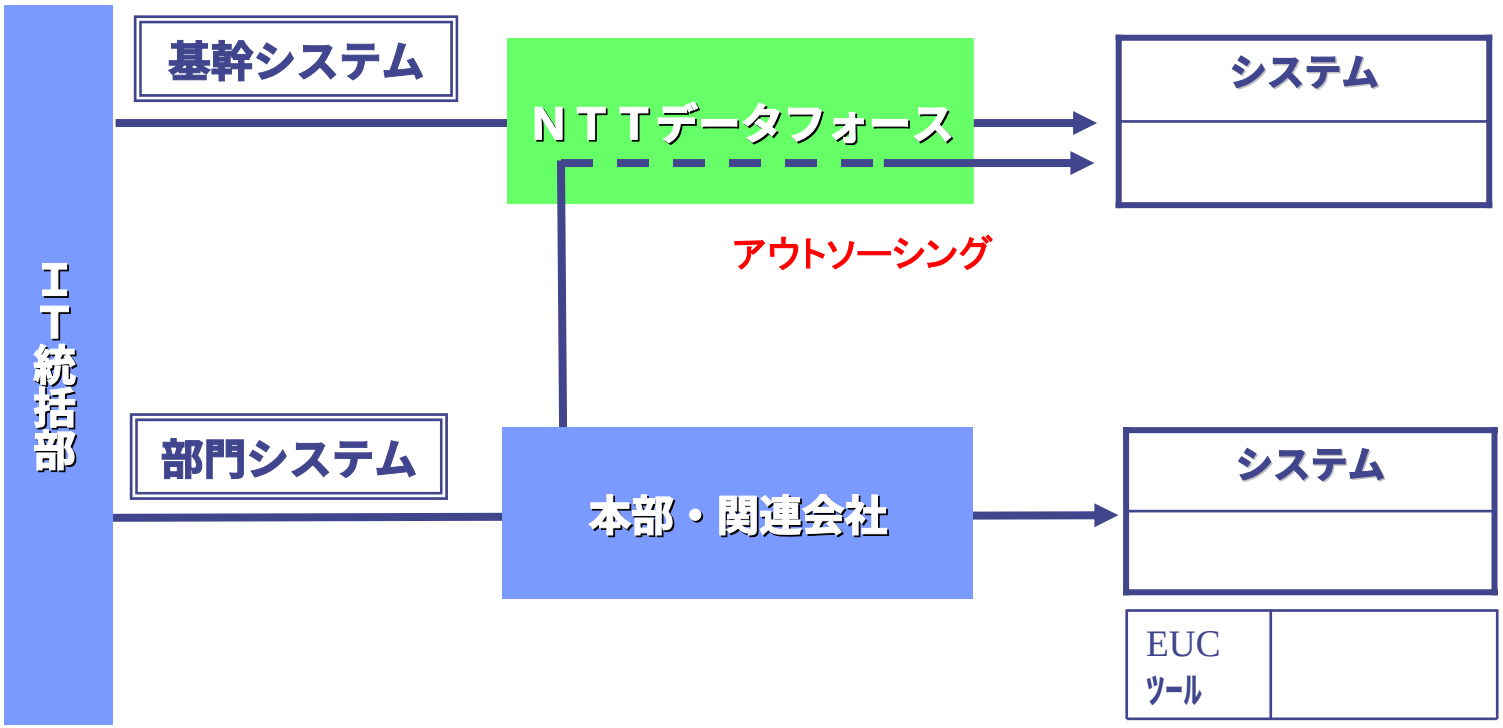
- このため、進捗状況を定量・定性両面から評価し、内在するリスクを共有・コントロールする仕組み作りに取り組んできた。

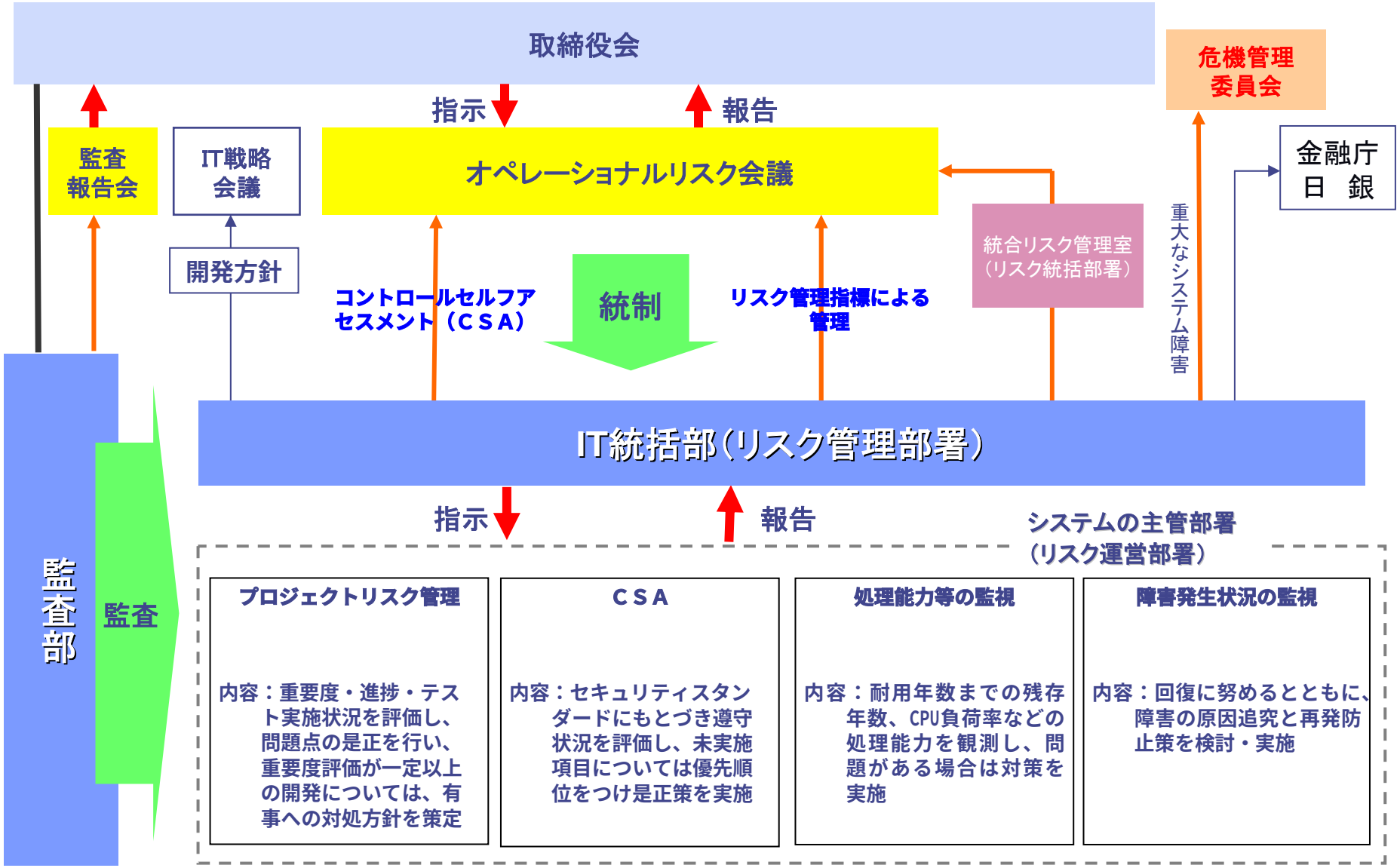
本日は、当行がこれまで行ってきたリスク管理の枠組みとともに、今後の課題について紹介する。

１．システムの管理体制

（１）組織体制

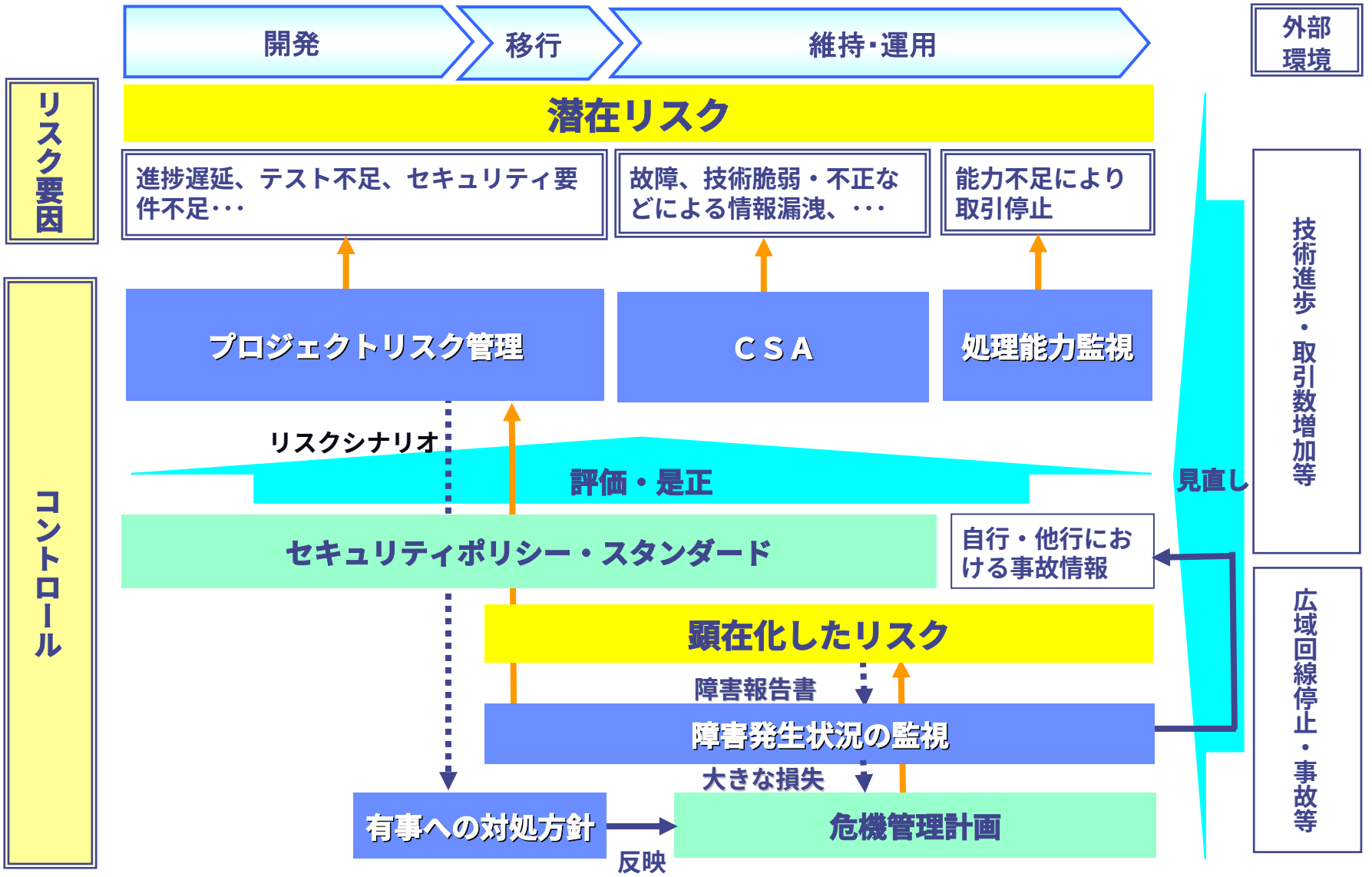
ＩＴ統括部	主な役割	本部・関連会社
システム企画室 （１５名）	・ＩＴ戦略、中長期計画、企画 ・共同利用システム ・プロジェクト統括	ITマネージャー （各組織１名以上）
管理グループ （４名）	・リスク管理、ＳＯＸ法対応 ・ＩＴ投資経費	セキュリティ責任者・管理者　等 （各組織１名以上）





※金融検査マニュアルの改訂を受けて見直しをしている

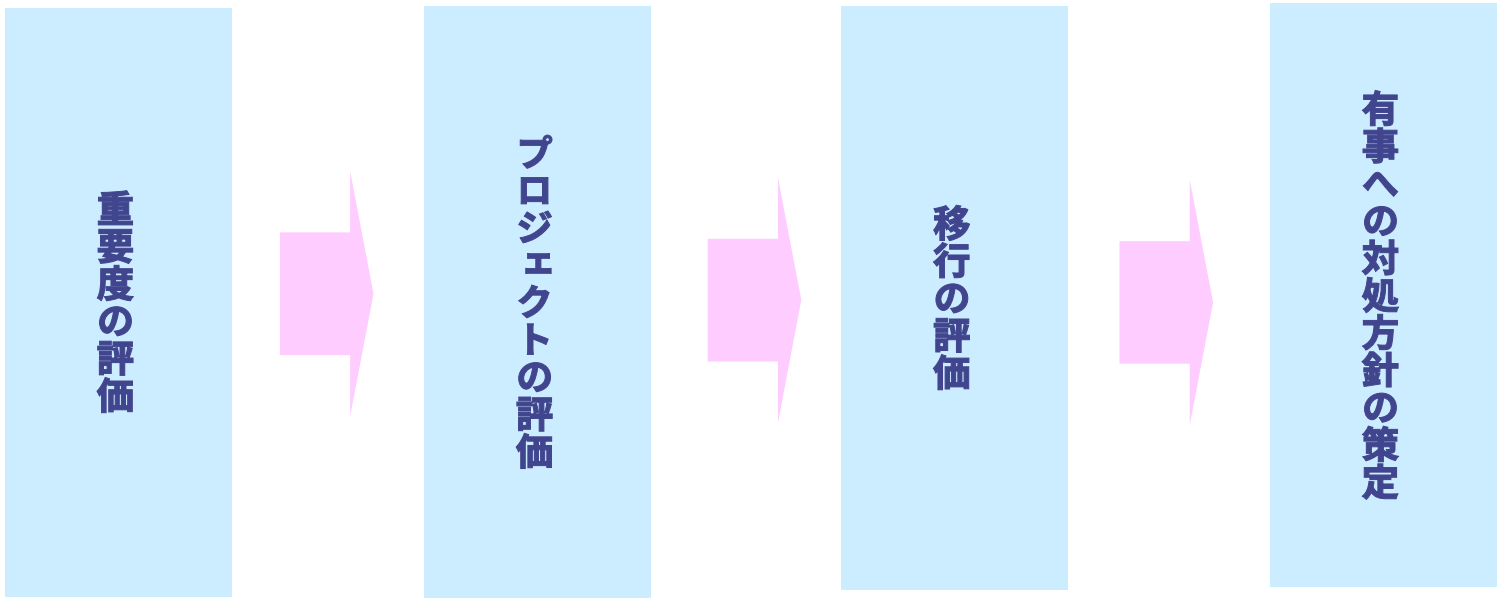
（2）ライフサイクルからみた全体像



２．プロジェクトリスク管理

（1）概要

プロジェクトの「重要度」と「進捗」の両方を可視化・評価し、外部委託先から銀行経営者まで情報を共有し、早期に問題点を発見し是正する。



（2）重要度・進捗の評価

大規模な開発（人月が一定以上）に対して、障害時の影響範囲等からプロジェクトの重要度を評価し、定量・定性の両面から進捗状況を詳細に管理する。

重要度

障害時影響範囲 × **資金決済影響有無** × **リスク度合** = **重要度(1～18段階)**

障害時影響範囲	
顧客・外部	
営業店・本部	
システム部門	

資金決済影響有無	
有	
無	

リスク度合	
経営に報告	
行内関係者の対応	
システム担当対応	

	a	b	c
A			
B			
C			

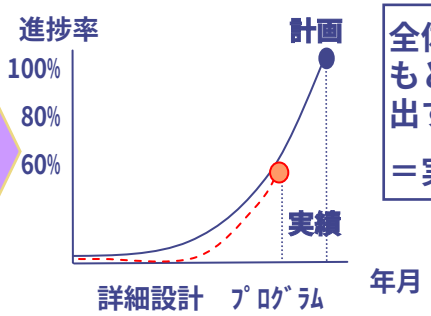
( )は資金決済影響なしの点数

進捗

定量評価（進捗率） : **定性評価（3段階）**

工程	成果物
基本設計	・・・・
詳細設計	・・・・
ﾌﾟﾛｸﾞﾗﾑ	
結合試験	
総合試験	

計画策定



全体計画・実績をもとに進捗率を算出する。

＝実績値／計画値

委託/受託双方からみた業務・体制面の課題等を、IT統括部が総合評価する。

問題なし	
課題あるが進捗に及ぼす影響は少ない	
進捗大いに懸念あり	

（3）プロジェクトの評価

並行する大型案件について「開発人月」と「重要度」によりプロジェクトの「重さ」を表し、進捗・問題点等を明確にする。

案件名	開発責任者	開発人月	重要度	進捗		有事への対処方針	開発進捗（18年度）											
				定量評価	定性評価		上期						下期					
							4	5	6	7	8	9	10	11	12	1	2	3
○○システム開発				100%		要・済												
							定性評価コメント欄											
□□システム導入				90%		要・未済												
							定性評価コメント欄											
△△システム更改				80%		要・未済												
							定性評価コメント欄											

開発人月×重要度の大きさでプロジェクトの「重さ」を表す。

（4）移行の評価

移行段階の高いリスクに備えより慎重を期すため、テストの詳細で網羅的な実施状況を外部委託先と確認する。（一定以上の重要度ランク）

主な評価項目	具体的な内容	評価数	達成数
懸案事項	・懸案事項について、未結末の有無	5	5
プログラム品質	・テストする項目の消化状況 ・バグ（プログラムの誤り）の発見状況	7	6
性能品質	・システムを利用した操作等が想定時間内かの確認	5	4
運用品質	・正常運用、障害、異例時における手順書の準備	5	3
・・・	・・・	数値は例示	
移行品質	・本番移行にあたっての移行日の体制・手順の準備 ・本番移行が正しく行われなかった場合、移行前のシステムを引続き稼働させる手順	4	2

（５）有事への対処

事前に「有事への対処方針」を作成し、万が一の対応について本部内・委託先と情報共有し、初動動作を素早く行える体制を準備する。（一定以上の重要度ランク）

～１シナリオで１枚程度～

○○系システム編

１．リスクシナリオ

システムダウン

２．復旧方法

３．影響（再立上げまでの時間帯で下記処理が取引不可とな

影響内容を共有する

（１）想定損失額

（２）事前準備資料

（３）対応内容

関連部署		顧客への影響	最大影響先数
営業店			
事務センター			
本店			

影響範囲を認識する

行内指示・対応

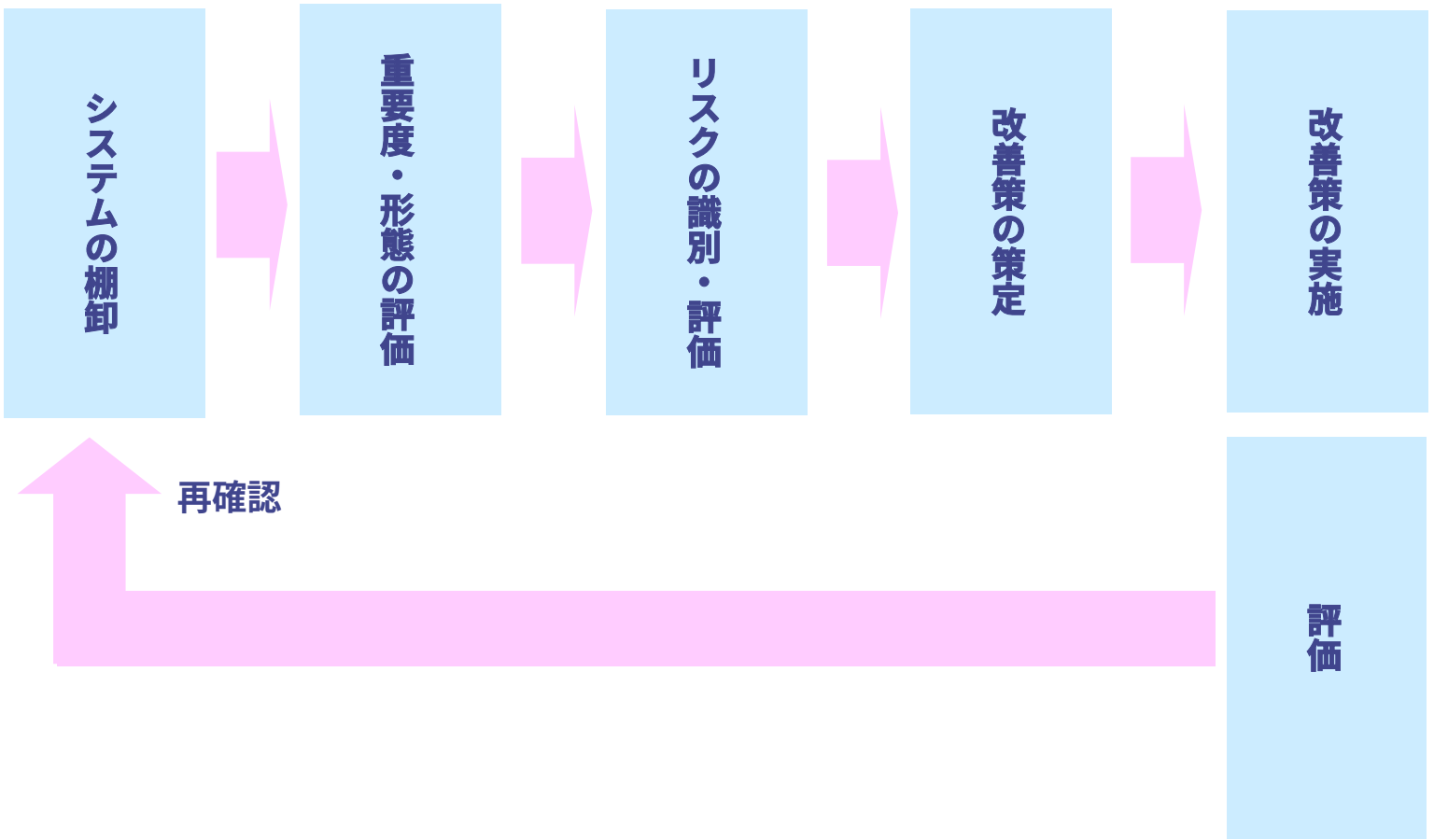
指示する内容を共有する

顧客への対応

３．ＣＳＡ

（１）概要

リスク対策の優先順位を策定し、実行に移すため管理体制や安全対策の遵守状況をシステムごとに識別・評価する。



（2）重要度・形態の評価

システム・情報のそれぞれの重要度および、形態を判断し、適正に沿った効率的なセキュリティレベルを実装しているかの判断根拠とする。

重要度

システムの重要度と判断基準

名称	重要度
最重要	
重要	
一般	

項目	最重要	重要	一般
障害時影響範囲			
ﾘｶﾊﾞﾘｰ許容時間			
取引件数（ﾋﾟｰｸ）			
取引金額（ﾋﾟｰｸ）			
ｼｽﾃﾑ接続先			

情報の重要度

名称	重要度
最重要	
重要	
一般	

（例）最重要の判定：最重要項目のうち３項目以上該当する場合
など一定の基準を作成。

形態

名称	内容
自行構築型	自行構築あるいはパッケージ導入
共同センター利用	ホストやサーバを外部の共同センター等に設置し、システムを構築
端末設置（ASP方式含む）	外部システムの端末のみを設置し、業務上の取引を行う

（３）リスクの識別・評価

セキュリティスタンダードを評価基準として設定し、システム毎に脆弱性を評価する。個々の評価基準については、重要性およびシステム形態から、まもるべき項目を明確にする。

Ａ．評価基準の設定（セキュリティスタンダード）

１．本人確認機能の整備

（１）基本事項（区分Ｂ）

正当な権限を有する本人であることを、確認するための機能（本人確認機能）を保有する。

本基準の対象となる情報・システム分類および形態

情報＼ｼｽﾃﾑ	最重要	重要	一般
最重要			
重要			
一般			

自行構築	外部システム利用	
	共同ｾﾝﾀｰ	端末設置

（２）詳細事項（区分Ｃ）

✓**本人確認機能を保有する。（以下のいずれか）**

Ａ．パスワード等
- （ａ）暗証番号
- （ｂ）ＩＤ・パスワード
- （ｃ）ワンタイムパスワード（アクセスの都度、パスワードを変更する機能）
- ・

※具体的な評価基準

技術面
ID、パスワード等のアクセス管理や、暗号化などの情報漏えい対策など、各リスクに対する備えを検証する項目を設定。

組織、体制面
セキュリティ管理体制や、事務センター、コンピュータ室等への入退館（室）管理など、日常の管理体制などについて、検証する項目を設定。

両方合わせて約１８０項目程度。

B．評価方法

システム名称		○○システム
重要度	システム	重要
	情報	重要
形態		端末設置

評価項目 ※ｾｷｭﾘﾃｨｽﾀﾝﾀﾞｰﾄﾞと連動	評価対象	未実施・十分ではない場合のリスク	状況評価	リスク顕在化した場合の大きさ
本人確認機能の保有 Ａ．パスワード等 （ａ）暗証番号 （ｂ）ＩＤ・パスワード ・・・・	必要	本人確認機能を保有しないことによりシステムが不正使用され情報が漏洩する。	実施有無	システム重要度×情報重要度×・・・ ×脆弱性 ⇒点数化
・・・・	必要			
・・・・	不要			

顕在化した場合のリスク

情報漏洩
外部からの不正
ハードウエアの故障
ソフトウエアの故障
オペレーションミス

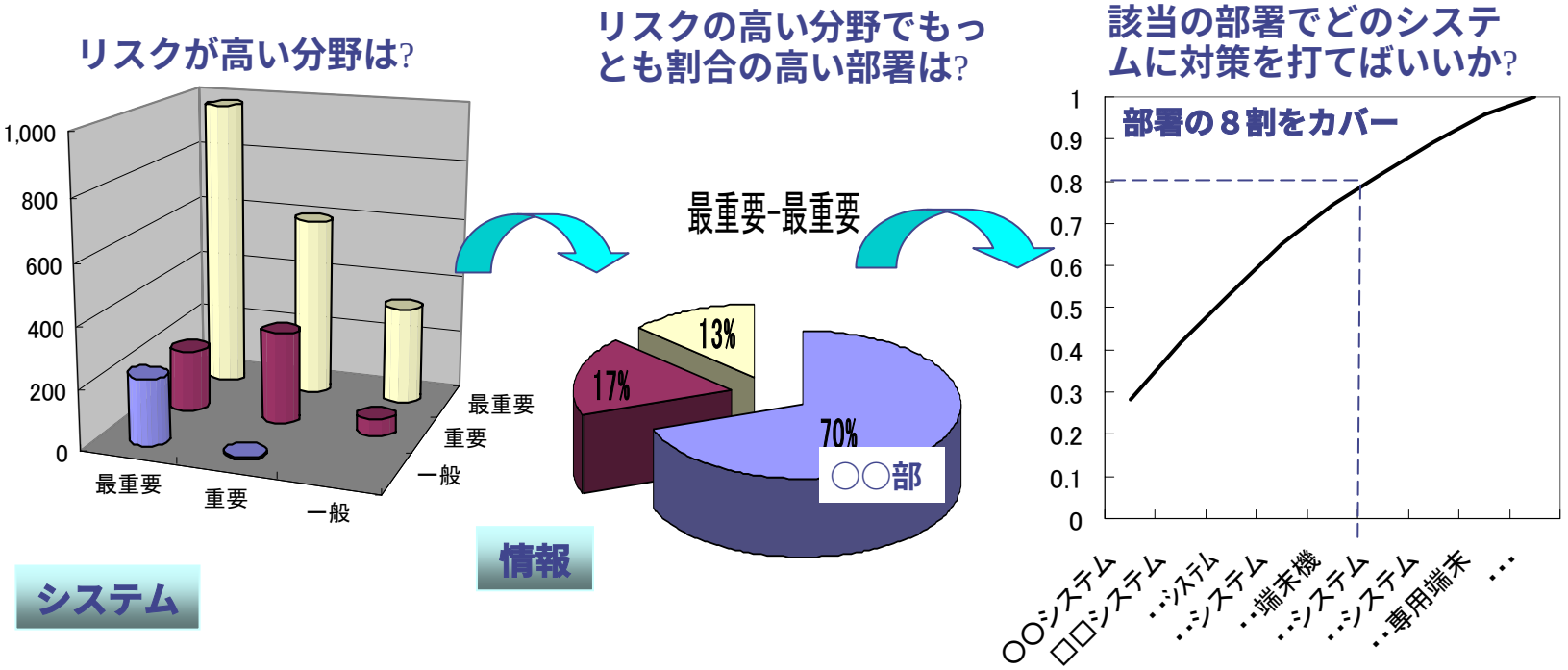
などあらかじめリスクを９種類にパターン化

（4）対策優先順位の策定

点数化したリスクを集計し、対策をとるべきシステム・項目を主管部署と相談のうえ選定し、全体の方針を策定する。（予算の確保も一元的に）

①リスクの高い（前項の点数化）システム・項目はなにか？
②特定のシステムで脆弱性が高い項目はなにか？
③平均して脆弱的な項目はないか？　　など

＜①のアプローチ例＞



（５）その他リスク改善にむけたアプローチ

全体のリスク量からみたアプローチ

・さまざまなシステムを開発するなか、全体のリスク量を把握

（良くなっているか、悪くなっているか）

・増減している要因と要因を踏まえた、今後の対策。

システムの更改期からみたアプローチ

・個々の脆弱点の是正と合わせ、システムの更改期を捉えた一括した改善策を実施。

・更改期等を捉えた、類似機能をもつシステムの統廃合など管理対象システムの削減。

など

（6）実施タイミング

翌年度の予算策定時期にあわせリスク評価し、対策について全体の優先項目を決め実行に移す。

４．処理能力等の監視

能力以上の処理による突然のシステムダウンを防ぐため、処理件数などを定期的に監視・評価する。

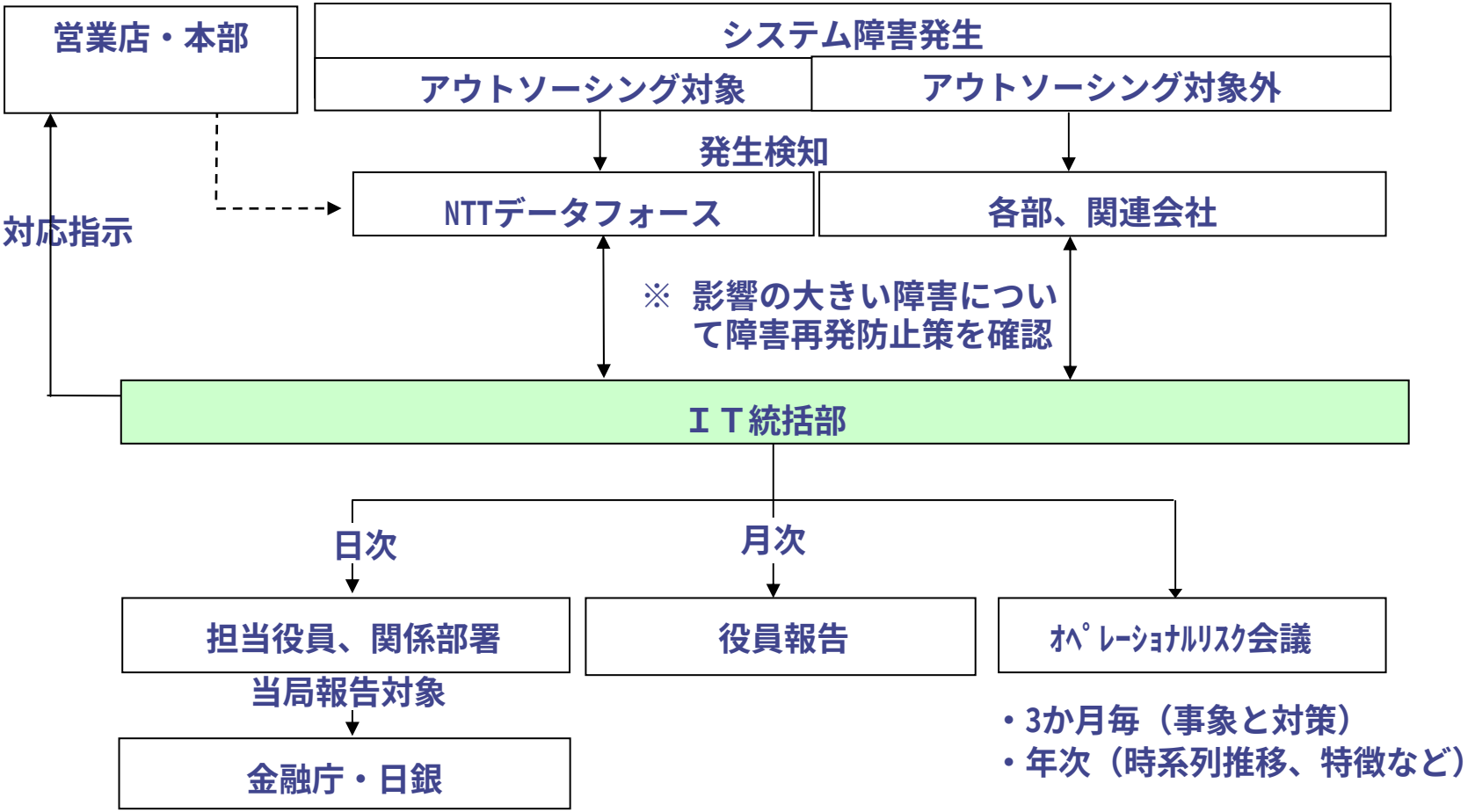
システム	能力	管理値	現状値	耐用年数	管理値	現状値	現状・課題	方　針
○○系					○年	○年 ○月		
□□系					○年	○年 ○月		
・・・					○年	○年 ○月		
・・・					○年	○年 ○月		
・・・					○年	○年 ○月		
・・・					○年	○年 ○月		
・・・					○年	○年 ○月		

耐用年数までどのくらい残っているか？

処理能力１００に対してどのくらい使用しているか？
■例えば想定処理件数での比較

５．障害発生状況の監視

（１）報告ルート



（２）障害管理

件数、利用時間、保守到着時間などシステムの形態にあったＳＬＡ項目・水準を設定し管理する。

月次・年次で件数推移を把握し、問題がある場合は是正する。

６．規程の体系