「ITサービス・リスクマネジメントとSLA」

― ITサービスリスクのコントロール手段としてのSLA活用 ―

2007年 4月20日

ソリューションサービス事業委員会
SLA/SLM専門委員会 委員長

株式会社富士通総研
斎藤 弘志

目　次

1.民間企業におけるSLAの活用実態調査

①調査概要

(1) 調査対象

- 民間企業353社 (一部上場企業を中心に選定)

(2) 調査時期

- 2006年11月 ～ 2006年12月

(3) 調査方法

- 書面アンケート、ヒアリングにより、SLAの利用状況、契約状況を調査
- アンケート回収ができなかった企業にも、可能な限りSLA導入状況のヒアリングを実施

(4) 調査対象項目

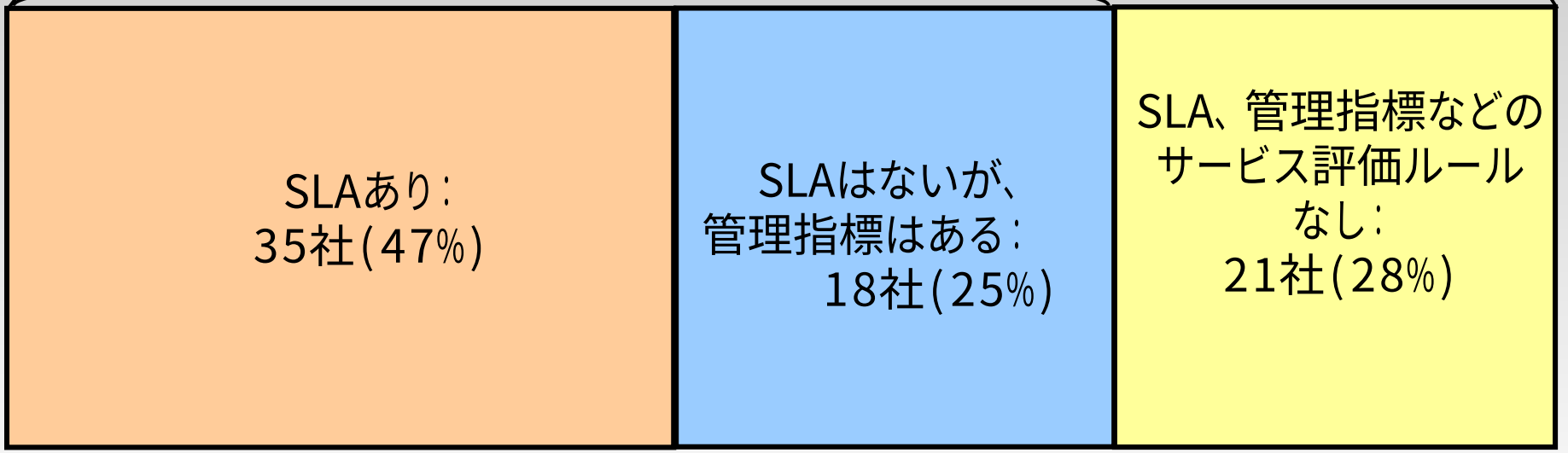
- 企業プロフィール：業種・企業規模、IT投資額、認証の取得状況など
- システム環境：利用システムと規模、利用形態、運用形態など
- ITサービス利用やシステム運用に対する考え方：問題・課題の認識、内容など
- 管理指標やSLAに対する評価：PDCAサイクル管理の状況、管理指標設定の効果など
- SLAガイドラインについて：認知度、利用・活用した内容、SLA/SLM取り組み事例など

②回答状況

353社：調査アプローチ先

74社：アンケート回答

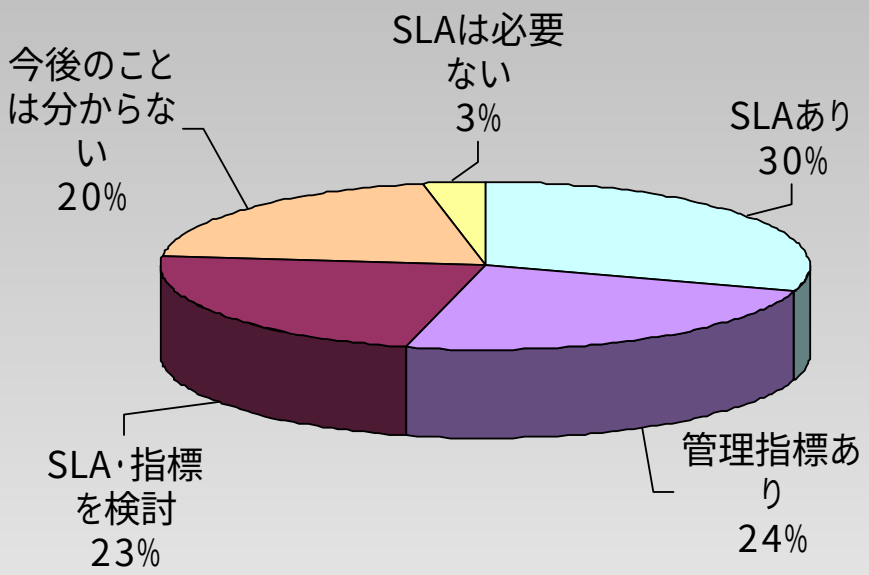
サービス評価での取り決めがあるケース：　53社
（内、SLAがあるケース　35社）



③SLAの全体導入状況

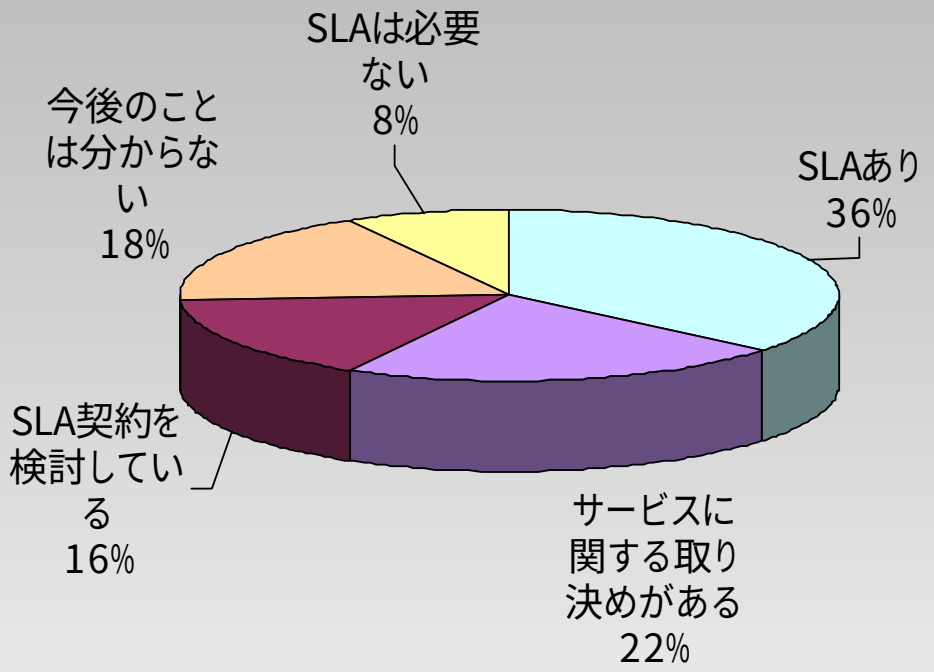
●2005年度

N＝376



●2006年度

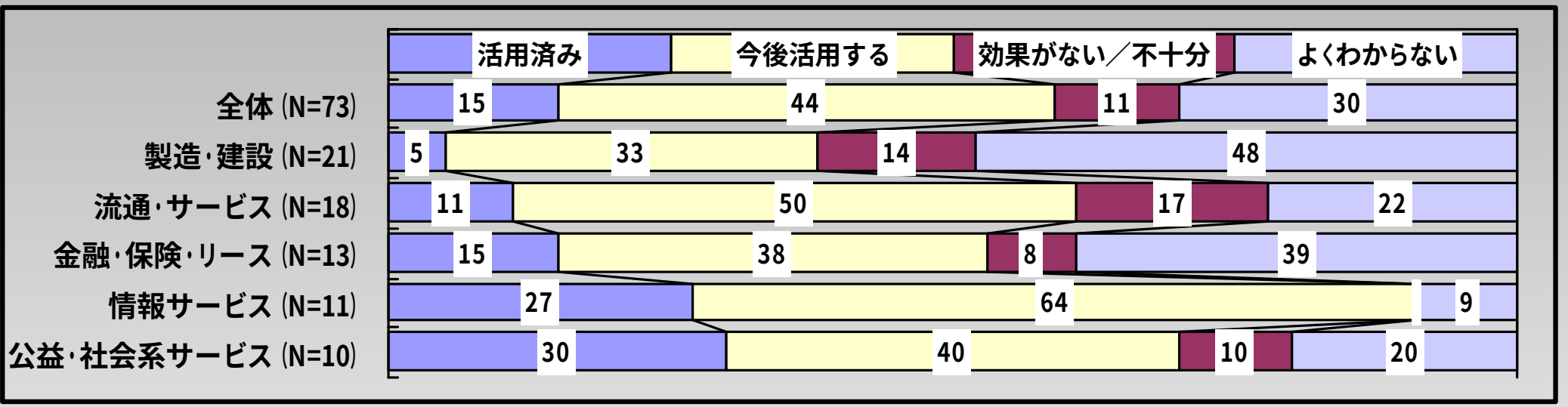
N＝353



- ✓「SLAあり」、「管理指標あり」、「SLA･指標を検討」の3項目を合わせると74％。
- ✓「SLAは必要なし」は5%から8％に増加。
  ⇒サービス提供者とサービス利用者との間でSLAというものが、認知･理解され、SLAを必要とする企業、必要としない企業が明確化してきている

④リスク対策におけるSLAの活用状況

リスク対策におけるSLAの活用実態（%）

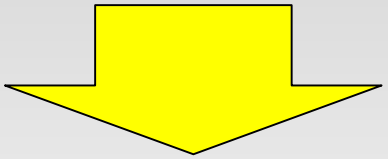


✓現状ではITサービス・リスクマネジメントにSLAを活用しているケースは15%。
✓一方で、今後活用したいと考えている企業が44%に上る。
　⇒リスク対策の領域においてもSLAの認知が高まっていると考えられる。

2.民間向けITシステムのSLAガイドライン第三版の概要

①ガイドライン改版のねらい

- SLAは、「認知期間」から「導入・普及期」に変わった。
- SLA導入事例調査を行い、実際にSLAを導入・活用している7社の取り組み状況がわかった。
- 日本版SOX法が2009年3月期以降の決算期から適用が予定されており、内部統制の観点からもSLAがより重要視されている。



「民間向けITシステムのSLAガイドライン」の実用性を高め、ITサービスの質的向上をめざす

②ガイドラインの特徴

(1) SLA策定の具体的な方法を手順化
- 現システムの課題と問題点の洗い出し
- ITサービス項目、ITサービスレベルの決定
- SLAの締結

(2) 標準SLA項目表、サービスレベル基準表の提供

(3) SLA導入チェックシートの提供

(4) SLA契約書雛型の提供

(5) SLMの中でのSLA活用方法の定義

(6) SLAを活用した企業の取組み事例

③第二版と第三版の違いについて

- 第2章1節「SLAに対する認識」に2005年度の市場調査の結果を反映させた。
- 第2章2節「SLA導入の目的」の内容を、1節の変更に合わせて修正した。
- 第2章3節のタイトルを、「SLA導入のフレームワーク」に変更した。
- 第2章4節として、「SLA活用事例の調査概要」を新たに収録した。
- 付録10として、「SLA導入事例」を7例収録した。
- 付録11として、2004～2005年度に通算5回開催した本ガイドラインの説明会で出たQ&Aの主なものを収録した。
- ITサービス、ITプロセスマネジメント、ITリソースの評価項目の名称を統一した。

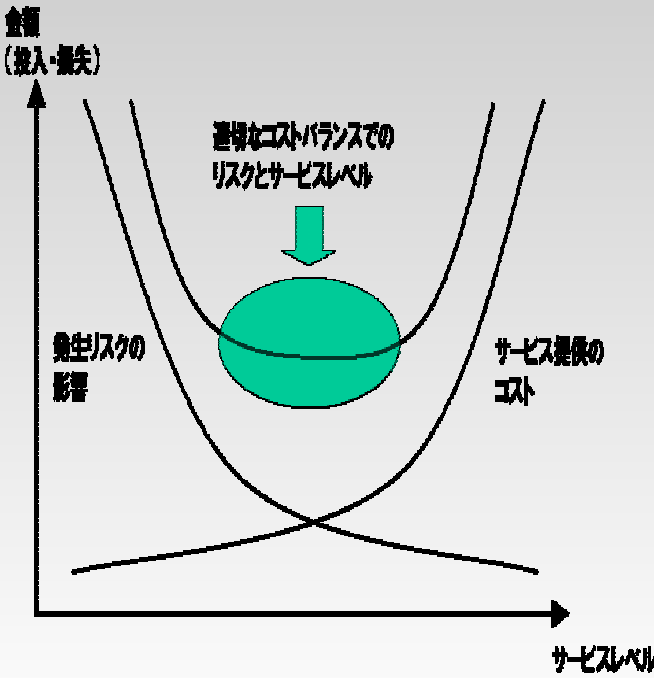
3.ITサービス・リスクマネジメントとSLA

取り組みの主旨と狙い

- 日本版SOX法に代表されるように企業活動での内部統制、リスクマネジメントの重要性が高まっている
- ITが内部統制の目的を達成する重要な手段として位置づけられている

業務遂行に必要なITサービスリスクを定義し、
リスクマネジメントとSLAの関係を明らかにする

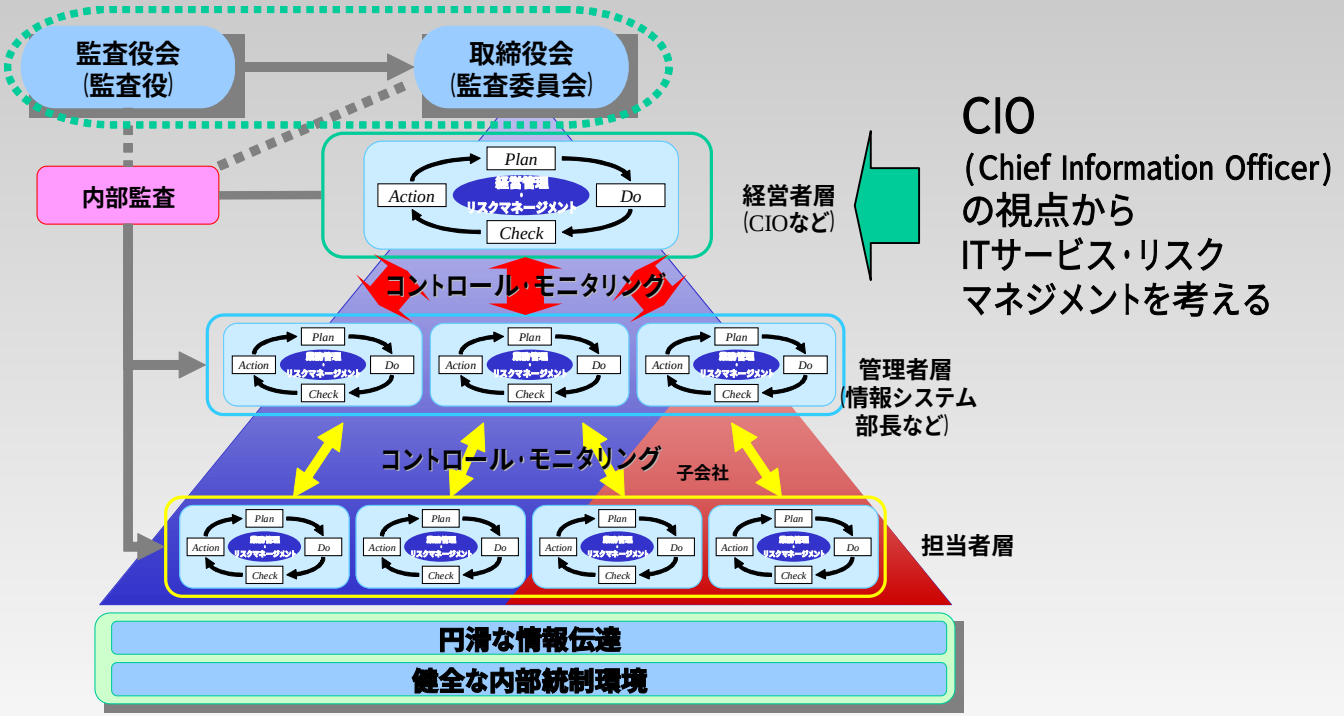
ITサービス提供者と利用者の関係において、
リスクとサービス価値のバランスの取れた
適性なITサービスの提供につながる



検討の視点

- COSO-ERMと経済産業省「リスク新時代の内部統制」を利用
- リスクとリターンの管理を、組織としての視点から行う立場で検討

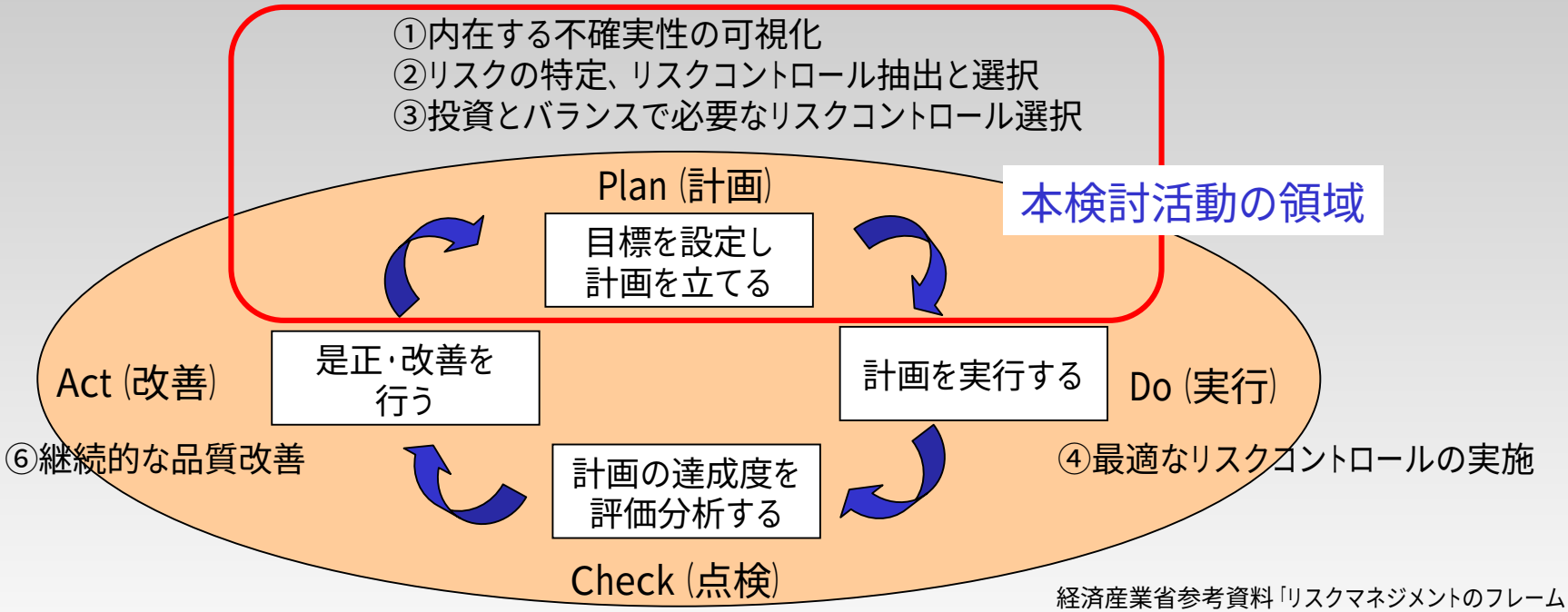
COSO ERMの構造を示すキューブ
「Enterprise Risk Management ― Integrated Framework Executive Summary」より



※経済産業省「リスク新時代の内部統制リスクマネジメントと一体となって機能する内部統制の指針」
リスク管理・内部統制に関する研究会2003年6月 をもとに作成

ITサービス・リスクマネジメントの目的と期待効果

- 目的　リスクマネジメントのＰＤＣＡをまわすことで、組織としてITサービスを適性に提供し、ビジネスプロセスの効率的な支援をすること
- 期待効果　ITサービスリスクの発生と損失を回避し、事業の安定性と効率性を高め、ひいては企業価値を向上すること

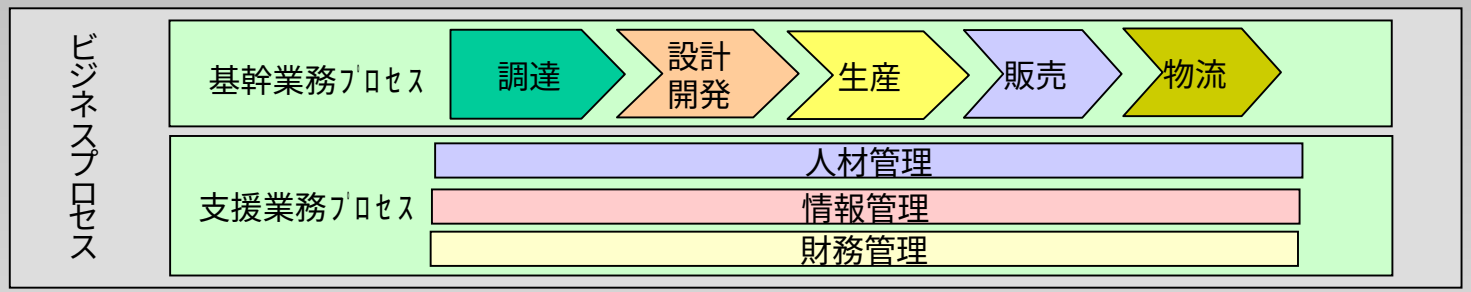


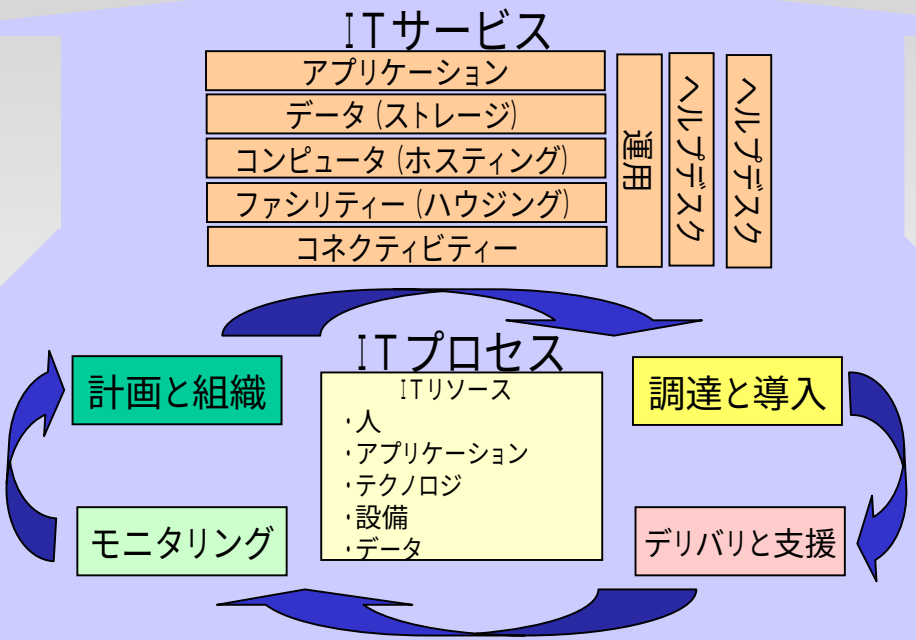
ITサービス・リスクマネジメントのＰＤＣＡサイクル

経済産業省参考資料「リスクマネジメントのフレームワーク」
「リスクマネジメント体制構築のためのＰＤＣＡサイクル」に追記

ITサービスの定義

- ITサービスとは、ビジネスプロセスの効率的な遂行を支援するために提供されるITを活用した各種サービス

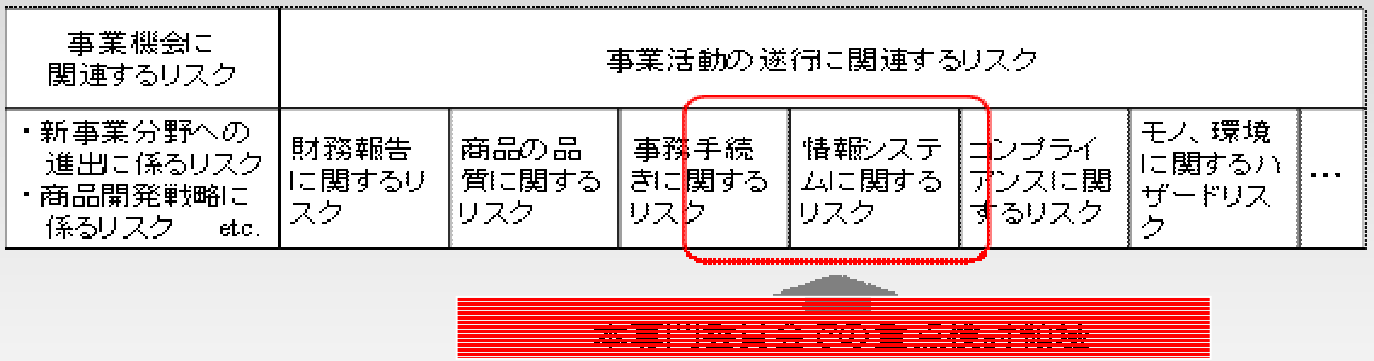




COBITのフレームワークを利用

ITサービスリスクの定義

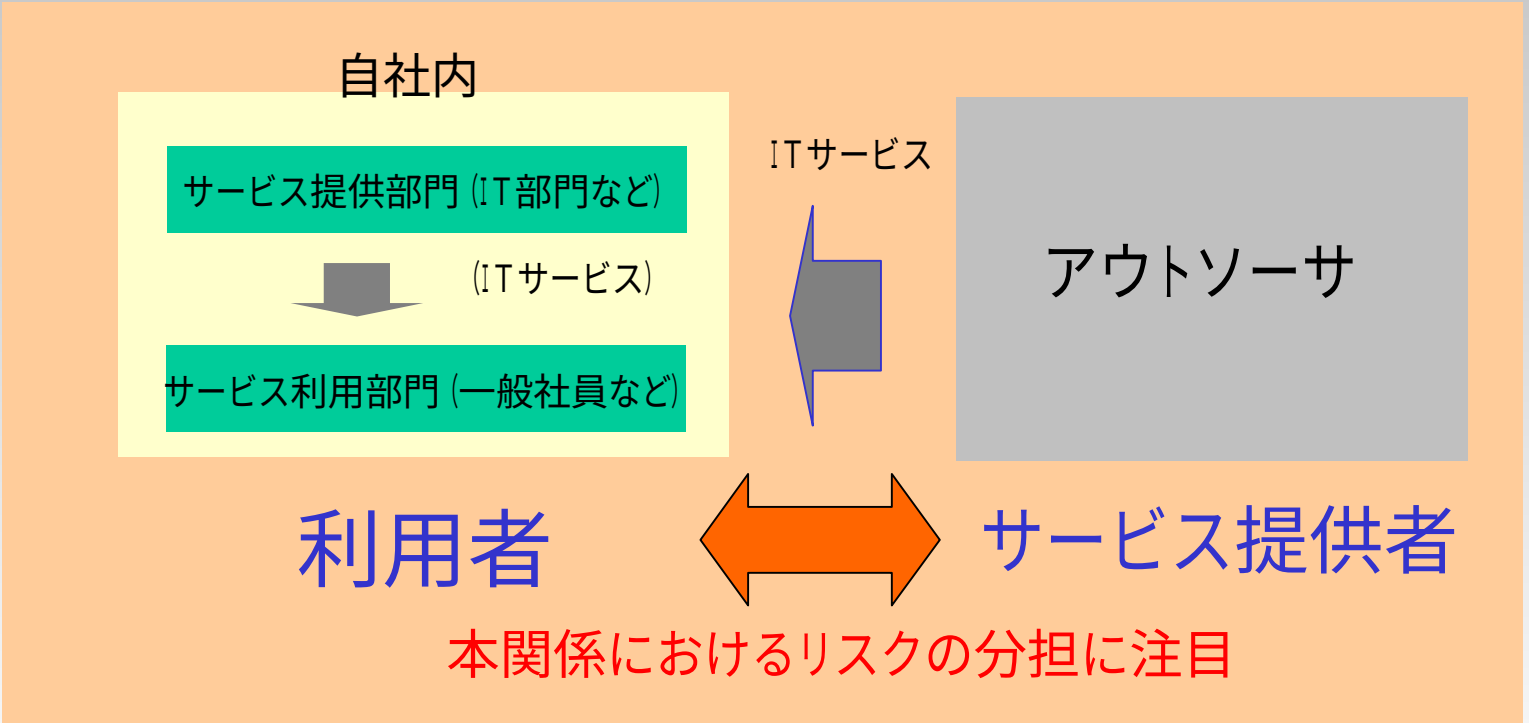
- ITサービスが　当初予定どおりに提供できなくなる
  ビジネスの要求に対応できなくなる
  業務遂行に支障をきたす
- 結果として　サービス提供コストの増加
  事業上の損害（売り上げ減少、機会損失）



※経済産業省「リスク新時代の内部統制リスクマネジメントと一体となって機能する内部統制の指針」
リスク管理・内部統制に関する研究会2003年6月　をもとに作成
①事業機会に関連するリスク：経営上の戦略的意思決定に係るリスク
②事業活動の遂行に関連するリスク：適正かつ効率的な業務の遂行に係るリスク

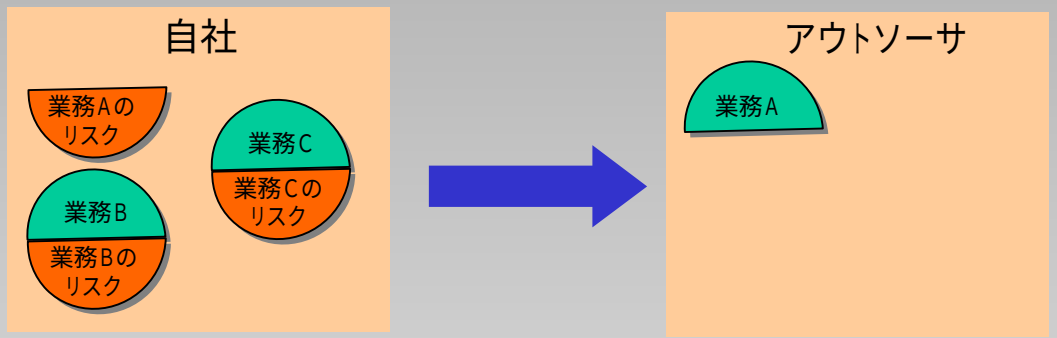
ITサービス提供の考え方とリスクの分担

- 利用者（利用企業）⇔サービス提供者（アウトソーサ）との関係にフォーカスしてリスクの分担を検討



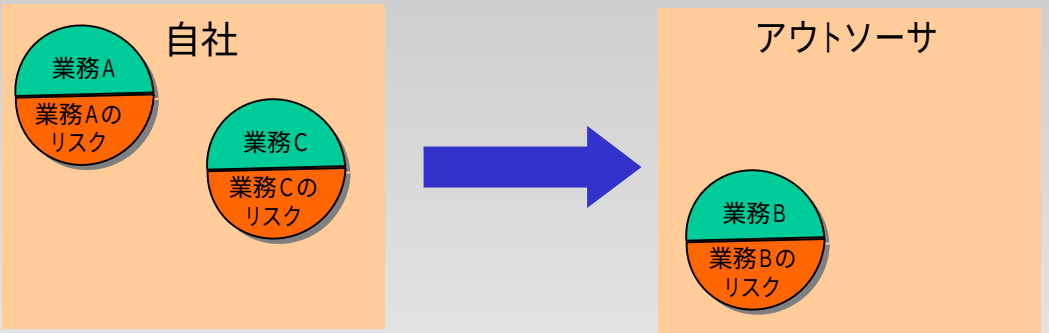
ITサービスリスクの移転の考え方

自社でリスクを
保有する場合



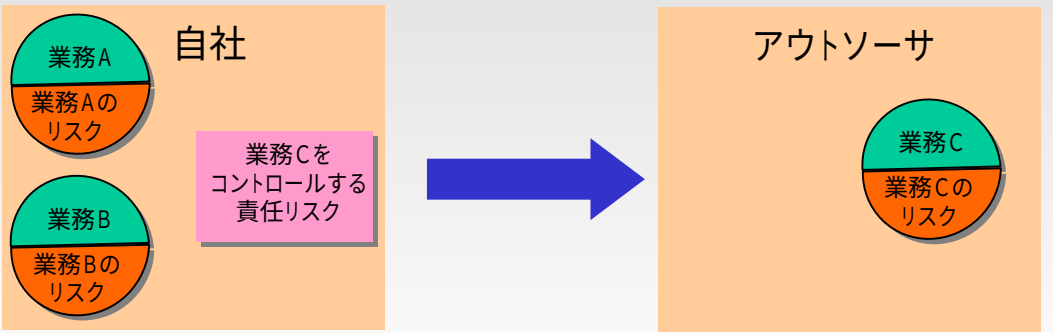
業務Aをアウトソースしても
業務Aのリスクは自社内に
留まる

業務Bをアウトソース
することで
リスクを移転する場合



業務Bをアウトソース
することで
業務Bに係わるリスクも
すべて移転する

業務Cをアウトソース
して業務リスクは
移転するが
新たにコントロールする
責任リスクが発生する
場合

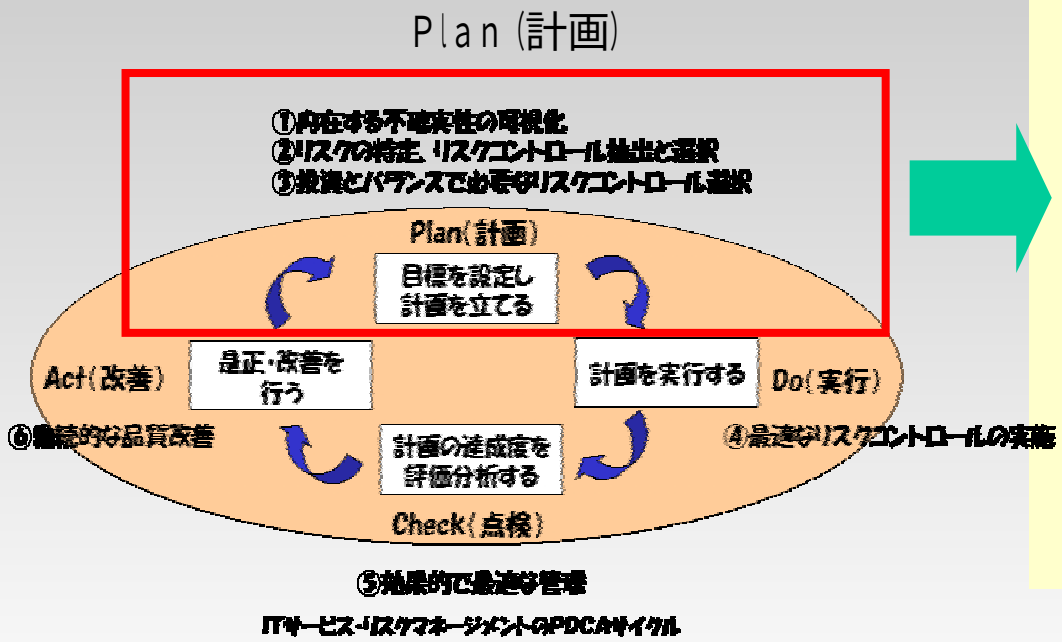


業務Cをアウトソース
することで
業務Cのリスクは移転するが
新たに業務をコントロールする
責任リスクが発生する

4.「ITサービスリスク／SLAマトリクス」の概要

「ITサービスリスク／SLAマトリクス」の作成

- ITサービス・リスクマネジメントのPlan（計画）フェーズを支援するツール（洗い出し、特定、コントロールの抽出）ツールとして作成



①リスクアセスメント
リスクの洗い出し・評価

②リスクの特定、リスクコントロール
方法の抽出と選択

②最適な意思決定
可能な投資で
必要なリスクコントロールを選択

ツールとして利用可能

ITサービス リスク／ SLA マトリクス

「ITサービスリスク／SLAマトリクス」の特長

① リスク区分をCOBIT―III（グローバルスタンダード）のフレームワークを用いて4つのドメインと34のプロセスに分類することで網羅性を高めている

② システム管理基準（日本スタンダード）を組み合わせることで、具体的なリスク項目（294項目）を抽出している

③ ITサービスをアウトソーシングする際の、サービス利用者と提供者とのリスク分担の考え方を明確にしている

④ サービス利用者と提供者とのリスクの移転について、契約やSLAによってコントロールが可能かどうかを明らかにしている

⑤ サービス提供者にすべてもしくは一部が移転されるITサービスリスクに対して、SLAによってリスクコントロールを行うためのサービスレベル主要規定項目を明らかにしている

「ITサービスリスク／SLAマトリクス」の構成

リスク分類項目（ドメイン・プロセス）

リスク移転可否

影響度・可能性・リスク値

発生リスク

システム管理基準（項目番号、カテゴリ、管理項目）

リスク移転可否に関する補足事項

リスク分類項目		システム管理基準 項目番号	システム管理基準 カテゴリ	管理項目	No.	発生リスク	リスク移転可否	リスク移転可否に関する補足事項	影響度	可能性	リスク値
ドメイン	プロセス										
サービス提供とサポート Delivery and Support	DS1 サービスレベルの定義と管理	IV-09-0-(02)	IV- 運用（構成管理）	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。	181	情報システムの機能維持や障害時の早期回復に支障を来たす。	○	運用管理業務をサービス提供者に委託した場合は、サービス提供者に移転する。			

契約またはSLAによるコントロール手段

サービス対象範囲

サービスレベル主要規定項目

サービスレベル項目値

契約／SLAによるリスクコントロール手段	表 S/P/R	サービス対象（範囲）		サービスレベル主要規定項目			規定項目選定の理由
		対象	管理区分	分類	規定項目	項目値	
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し、情報システムの機能維持や障害時の早期回復を目指すためには、サービスレベル管理プロセスをSLAで規定することが必要である。	P	共通	サービスレベル管理	可用性 可用性 可用性 信頼性 信頼性 信頼性 信頼性	[体制管理実施の有無] [運営管理実施の有無] [運用管理規定の有無] [管理サイクル(間隔)] *[報告間隔]* *[レビュー実施間隔]* *[監査の実施間隔]*		サービスレベル規定項目選定理由

ITサービスリスク／SLAマトリクス (リスク分類項目、システム管理基準)

①リスク分類項目 (ドメイン・プロセス)

COBIT－IIIのフレームワークを適用 (4ドメイン・34プロセス)

- 計画と組織 (PO: Planning and Organization)
- 調達と実施 (AI: Acquisition and Implementation)
- デリバリーとサポート (DS: Delivery and Support)
- モニタリング (M: Monitoring)

②システム管理基準 (項目番号、カテゴリ及び管理項目)

プロセス毎の具体的な管理項目を定義するため、システム管理基準を利用

日本情報処理開発協会 (JIPDEC) 発行の「新版 システム監査基準/管理基準解説書 平成16年基準改訂版) の参考資料である システム管理基準とCOBIT－III対比表を使用

システム管理基準とCOBIT－IIIの対比表

大項目	中項目	小項目	管理項目	COBIT－III					
				PO 1 戦略的IT計画の定義	PO 2 情報アーキテクチャーの定義	PO 3 技術指針の決定	PO 4 ITの組織とそのかかわりの定義	PO 5 IT投資の管理	PO 6 マネジメントの意図と指針の周知
I.情報戦略	01.全体最適化	1.1全体最適化の方針・目標	01.ITガバナンスの方針を明確化する	●					
			02.情報化投資及び情報化構築の決定における原則を定めること	●					
			03.情報化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	●					
			04.組織全体の情報システムのあるべき姿を明確にすること		●		●		
			05.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				●		
			06.情報セキュリティー基本方針を明確にすること						●

システム管理基準

【出典:「日本情報処理開発協会 (JIPDEC) 「新版 システム監査基準/管理基準解説書 平成16年基準改訂版) システム管理基準とCOBIT－III比較表より抜粋」】

ITサービスリスク／SLAマトリクス (発生リスク)

③発生リスクの定義

- 管理項目の内容が、未実行だった場合に発生するリスクを想定

  管理項目の未実行を起因として発生の可能性があるインシデントや不具合、実行課題や問題などを発生リスクとして抽出している。

- 管理項目に対して、発生リスクは1つまたは2つ程度に集約

  情報システムに関するリスク、情報システムによって支援される事務手続きに関するリスク、情報システムに関連したコンプライアンスリスクを中心に、CIOの視点に立った経営的な観点でのリスクに集約を行っている。

- リスクの記載においては、断定表現に統一

  発生リスクの語尾の表現を統一化することで、同じ視点からリスク内容を評価でき、アセスメント項目などに利用する際に変換し易いように考慮している。

ITサービスリスク／SLAマトリクス (リスク移転可否)

④リスク移転の考え方

業務をアウトソーシングサービスの導入によって、利用者からサービス提供者に移転する

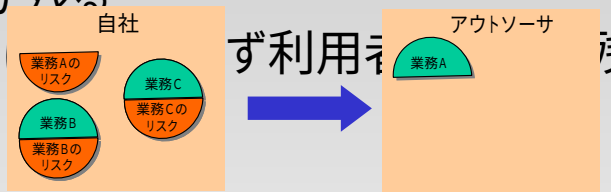
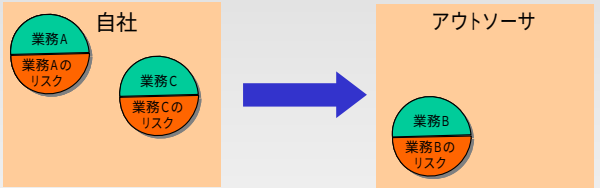
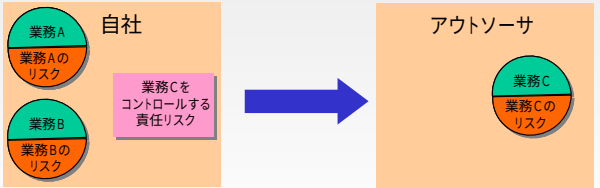
場合、発生リスクについても利用者からサービス提供者への移転の可能性を提示

移転区分

○:利用者からサービス提供者にリスクがすべて移転する

△:利用者に一部のリスクが残る

×:サービス提供者にリスク[illegible]ず利用者[illegible]残る

		表記記号
自社でリスクを保有する場合		×
業務Bをアウトソースすることでリスクを移転する場合		○
業務Cをアウトソースして業務リスクは移転するが、新たに業務をコントロールする責任リスクが発生する場合		△

ITサービスリスク／SLAマトリクス (リスク移転可否に関する補足事項)

⑤リスク移転可否に関する補足事項

利用者からサービス提供者に発生リスクが移転可能となるための補足事項や条件を説明

リスク移転可否	リスク移転可否に関する補足事項
△	災害対策業務を委託する場合、代替処理･復旧の責任はサービス提供者に移転するが、「業務を継続できない」というリスクは利用者にも残る。
○	災害対策業務を委託する場合、代替処理･復旧の責任はサービス提供者に移転する。
×	運用管理業務をサービス提供者に委託した場合でも、知的財産権に関するリスクは移転できない。

リスク移転の可否判断に至った考え方や、補足事項を記載。

ITサービスリスク／SLAマトリクス（リスクの影響度、可能性、リスク値）

⑥影響度(脆弱性)と可能性(脅威)及びリスク値欄の使用方法

「ITサービスリスク/SLAマトリクス」の利用者が、自らのケースによる影響度、可能性からリスク値を算出することで発生リスクの優先順位付けを行えるよう空欄を設定

・リスクの評価は、一般にリスク発生の影響度(脆弱性)や可能性(脅威)またその他のリスク要素を数値化や記号化を行い、算定式によりリスク値として算出する。
・算出したリスク値に基づいて対象リスクの絞込みを行う。

影響度	可能性	リスク値

影響度	可能性	リスク値	
3	3	9	優先度高
2	1	2	優先度低

ITサービスリスク／SLAマトリクス（契約/SLAによるリスクコントロール手段）

⑦契約/SLAによるリスクコントロール手段の考え方

利用者からサービス提供者へ移転するリスクを、契約またはSLAによってコントロールするための手段や条件について記載

・管理項目の内容を実現する、又は発生リスクを低減するなどのリスクコントロール手段を記載している。
・本項目に基づいてサービスレベル主要規定項目が選定される。

ITサービスリスク／SLAマトリクス（サービス対象範囲、サービスレベル主要規定項目）

⑧サービス対象範囲、サービスレベル主要規定項目

リスクコントロール手段として最も有効と考えられるSLA項目を、基本項目を中心に記載

・「SLAガイドライン」の付録2　標準SLA項目詳細表における「サービス対象（範囲）」、「サービスレベル主要規定項目（分類、規定項目）」から抽出している。

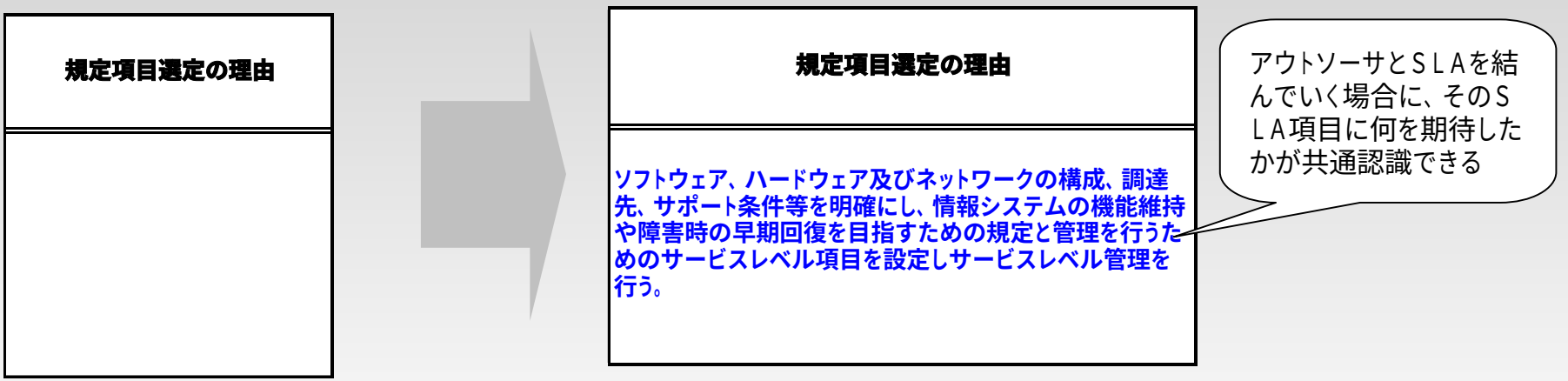
契約／SLAによるリスクコントロール手段	表 S/P/R	サービス対象（範囲）		サービスレベル主要規定項目	
		対象	管理区分	分類	規定項目
ユーザ及び運用の責任者が、復旧までの代替処理手続き及び体制を定め、検証し、停止した情報システムを復旧するまで間、業務を継続できるようにするためには、それらの達成度を把握するための評価プロセスが利用者で必要となる。また、それらを実現するためには、管理基準を可視化できる項目をSLAで規定することが必要である。	P	コンピュータ管理（ホスティング）	サービスレベル管理	可用性 可用性 可用性 信頼性 信頼性 信頼性 信頼性	[体制管理実施の有無] [運営管理実施の有無] [運用管理規定の有無] [管理サイクル（間隔）] [報告間隔] [レビュー実施間隔] [監査の実施間隔]
			ITサービス継続性管理	信頼性	[要員教育、および訓練の実施間隔]
定められた災害復旧手続き及び体制によって、円滑かつ確実に情報システムを復旧するためには、その管理基準を可視化できる項目をSLAで規定することが必要である。	P	共通	サービスレベル管理	可用性 可用性 可用性 信頼性 信頼性 信頼性 信頼性	[体制管理実施の有無] [運営管理実施の有無] [運用管理規定の有無] [管理サイクル（間隔）] [報告間隔] [レビュー実施間隔] [監査の実施間隔]

ITサービスリスク／SLAマトリクス（サービスレベル主要規定項目選定の理由）

⑧サービスレベル主要規定項目選定の理由欄の使用方法

サービスレベル主要規定項目の中から、自らのケースに最も妥当と考えられる規定項目を選択する際の選定理由を記述するための空白欄を設定

・自らのケースに照らして、最適なサービスレベル主要規定項目を絞り込む際に、選定理由を記述することを想定している。



本講演のご参考資料

① 社団法人 電子情報技術産業協会（ＪＥＩＴＡ）発行
平成１７年度 ソリューションサービスに関する調査報告書III
「ＩＴサービスリスクマネジメントとＳＬＡ」
－利用者と提供者のための「ＩＴサービスリスクマネジメント」－

②日本情報処理開発協会（ＪＩＰＤＥＣ）発行
「新版 システム監査基準/管理基準解説書 平成１６年基準改訂版）

③情報システムコントロール協会（ＩＳＡＣＡ）東京支部 ホームページ
ＣＯＢＩＴ 第３版マネジメントガイドライン 日本語版 無償ダウンロード
http://www.isaca.gr.jp/standard/cobit_ver3_MG.html

④ 経済産業省ホームページ 「リスク新時代の内部統制」
http://www.meti.go.jp/kohosys/press/0004205/1/030627risk-hokokusyo.pdf

上記をご参照ください