ITサービスリスクマネジメントとSLAについて

2007年11月29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

JEITA

目　次

JEITA

1.　取り組みの主旨と狙い

取り組みの主旨と狙い

- アウトソーシングサービスの活用が広まっている環境下で、サービス提供者と利用者でのリスクマネジメントの要求が高まっている
- 日本版SOX法では外部委託におけるSLAの重要性を指摘しているが、具体的な項目が提示されておらず、有効な対策を講じ難い

↓

リスクマネジメントの観点から、ITサービス提供者と利用者の関係において、リスクとサービス品質のバランスの取れた適性なITサービスの活用に結びつくガイドラインを提供する必要がある

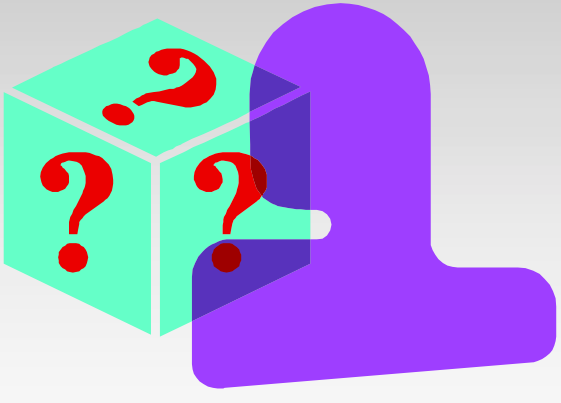
↓

アウトソーシングにおけるリスクを明確化し、サービス提供者と利用者の協調による統制活動に対するSLAの活用方法を具体化する

JEITA

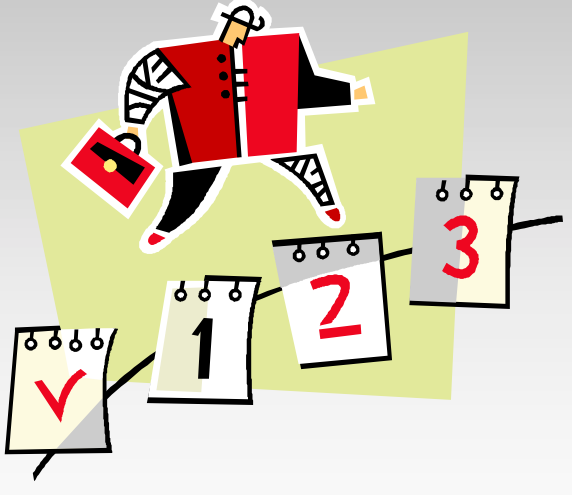
SLAの基本的な考え方

SLAとは、ITサービスの利用者と提供者が合意した目標を達成するための、コミュニケーション手段である。



- ITサービスの機能や範囲、品質、性能などが不明確

可視化



- ITサービスの達成目標をSLAとして明確化

SLA：Service Level Agreement

SLAガイドライン

①SLA策定の具体的な方法を手順化

①対象業種・業務分類
②ITサービス項目の決定
③ITサービスレベルの決定
④SLAの締結

②標準SLA項目表、サービスレベル基準表の提供

③SLA契約書雛型の提供

④SLMの中でのSLA活用方法の定義

⑤SLAを活用した企業の取組み事例

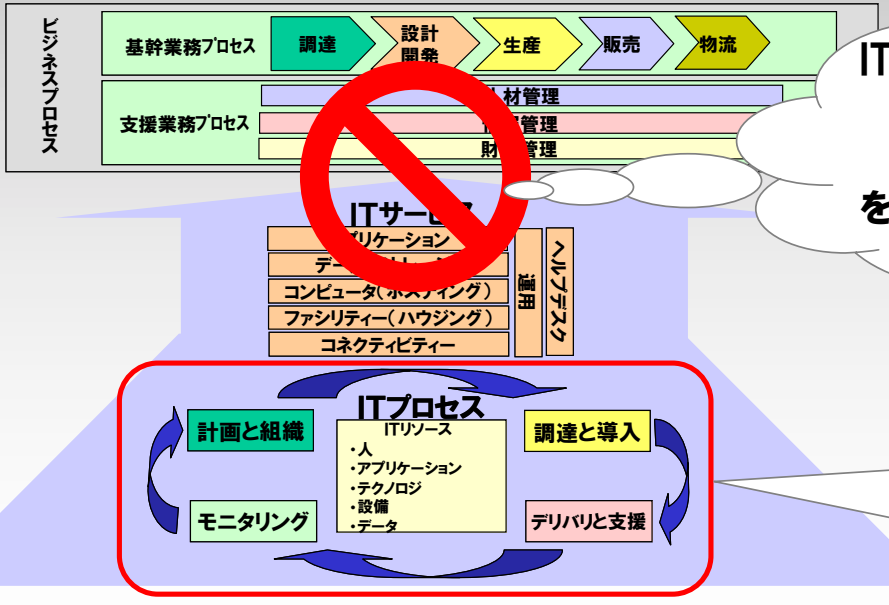
JEITA

2.　ITサービスリスクについて

JEITA

ITサービスリスクの考え方

- ITサービスが以下のような状況に陥ること
  - ・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

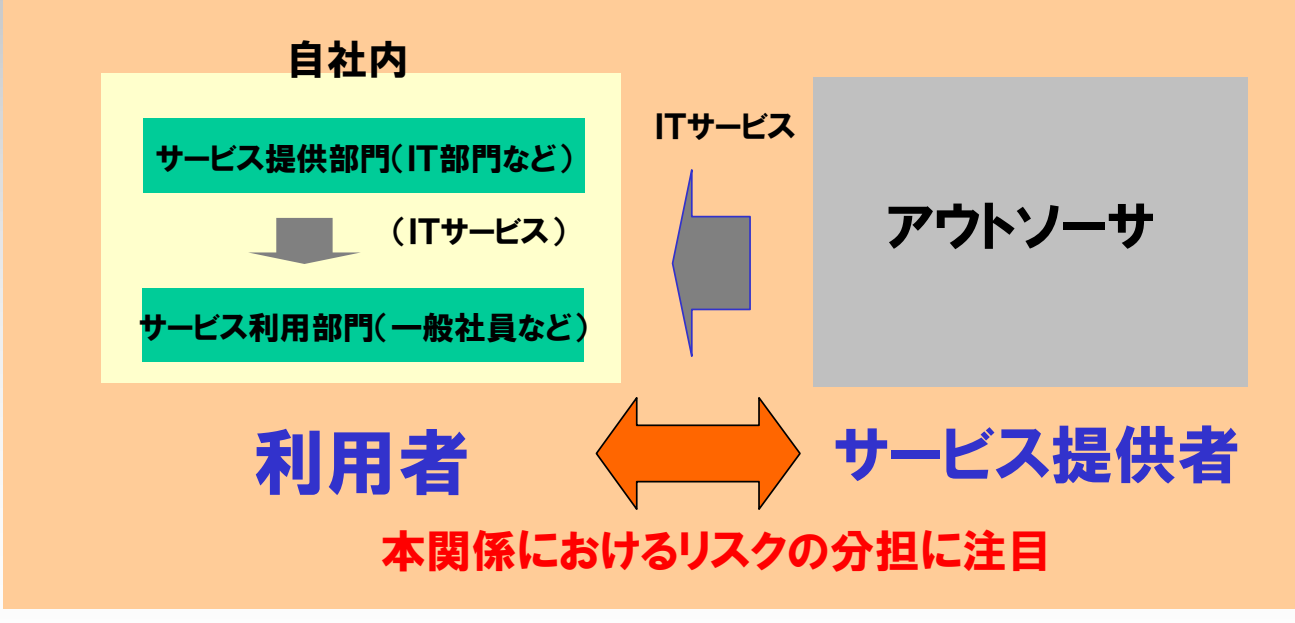


ITサービスリスクの顕在化により、
サービス提供コストの増加
事業上の損害(売り上げ減少、機会損失)
をもたらすことになる。

ITサービスリスクとして、
ITプロセスが予定通りに機能
しないケースに重点を置いて
検討

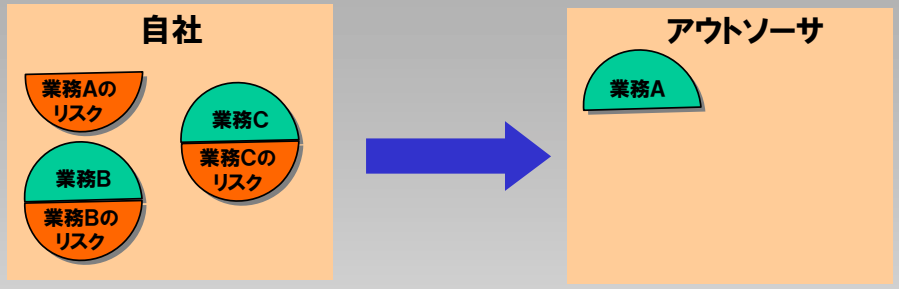
ITサービス提供の考え方とリスクの分担

- 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



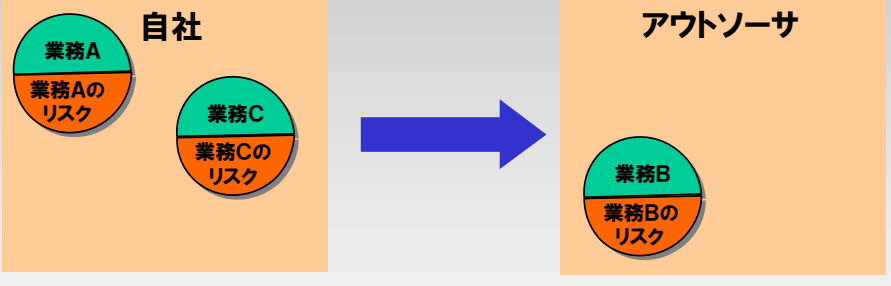
ITサービスリスクの移転の考え方

自社でリスクを**保有**する場合



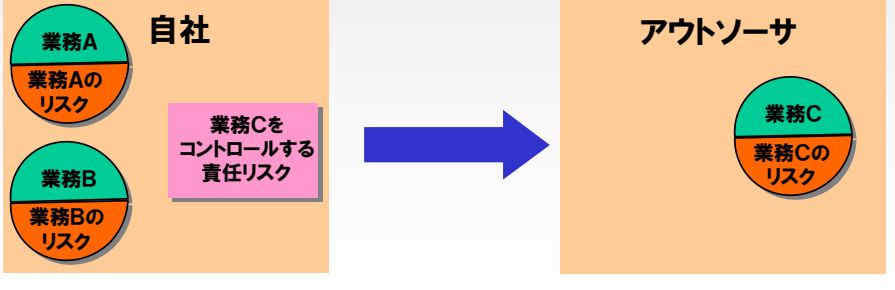
業務Aをアウトソースしても業務Aのリスクは自社内に**留まる**

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

JEITA

3.　ITアウトソーシングで失敗しない SLAチェックポイント294

ITアウトソーシングで失敗しない SLAチェックポイント294

（１）ITサービスリスク項目（294項目）の提示

（２）リスクコントロールに有効なサービスレベル項目の例示

（３）「IT内部統制の為の統制項目表」の提供

JEITA

本書の構成

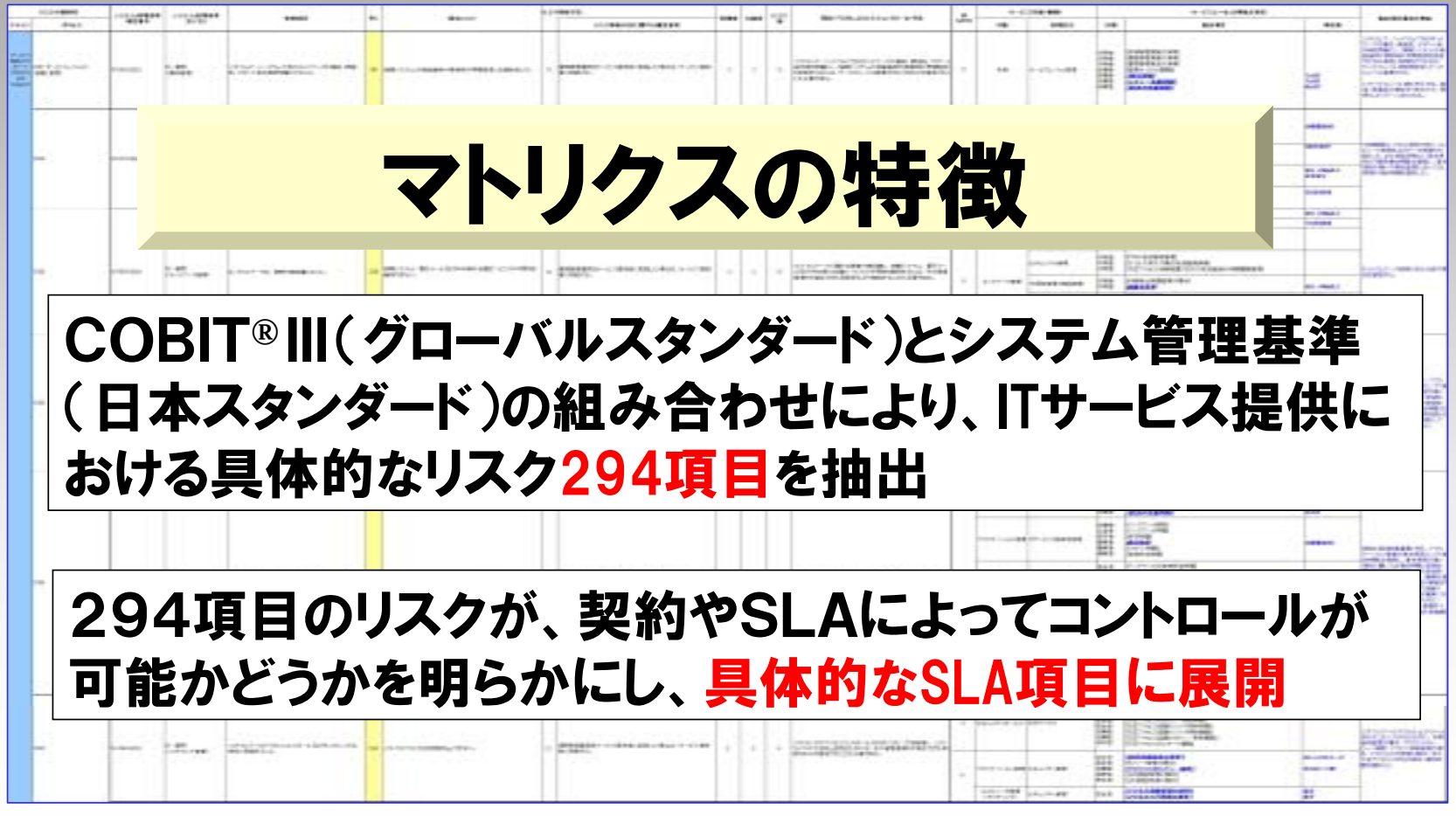
ITアウトソーシングで失敗しない
SLAチェックポイント294

- **ITサービス・リスクマネジメントとSLA**
  ITサービス・リスクマネジメントがなぜ必要か、SLAはなぜ必要かを内部統制の観点も含めて解説。ITサービスのアウトソーシングとリスク移転についても整理。
  - **ITサービスリスク／SLAマトリクス**
    利用者がアウトソーシングサービスを受ける場合のSLAによるリスクコントロールを規定したツール
  - **ITサービスにおける管理項目と発生リスク**
    ITサービスのアウトソーシングによるリスクコントロールの実行時、どのような管理項目と発生リスクがあるか、その移転の可否について解説
- **ITサービス・リスクマネジメントに関する調査報告**
  上場企業353社を対象とした取り組み状況の調査結果と解説
- **内部統制におけるIT統制**
  内部統制の動向とITにかかわる内部統制についての解説
  - **IT内部統制の為の統制項目表**
    ITサービスのリスクを統制するITプロセスに対応した統制方法を体系化した「IT内部統制の為の統制項目表」とその活用方法
- **内部統制に関わる市場動向調査**
  上場企業151社を対象とした、内部統制に関するアンケート調査結果

JEITA

4.　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



マトリクスの特徴

COBIT®Ⅲ（グローバルスタンダード）とシステム管理基準（日本スタンダード）の組み合わせにより、ITサービス提供における具体的なリスク**294項目**を抽出

294項目のリスクが、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、**具体的なSLA項目に展開**

JEITA

「ITサービスリスク／SLAマトリクス」の期待効果

- 「ITサービスリスク／SLAマトリクス」は実践的な活用を前提に作成されており、以下の効果が期待できる。

①リスク可視化のためのアセスメント項目やコントロール項目として活用できる。

②適切なリスク分担の指針として活用できる。

③リスクコントロール手段の例として活用できる。

④SLAでリスクコントロールする際の、項目として活用できる。

「ITサービスリスク／SLAマトリクス」の構成

リスク分類項目・システム管理基準

発生リスク

リスク移転可否

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		影響度	可能性	リスク値
ドメイン	プロセス							リスク移転可否に関する補足事項			
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。			

コントロール手段、サービスレベル主要規定項目

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]***		

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）

✓COBIT®IIIの各プロセスを円滑に遂行する上で管理すべき事項を、システム管理基準に記載されている管理項目からリストアップ。
✓COBIT®IIIのフレームワークにより検討の網羅性を高め、システム管理基準により具体性のある管理項目を設定。

■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）

■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

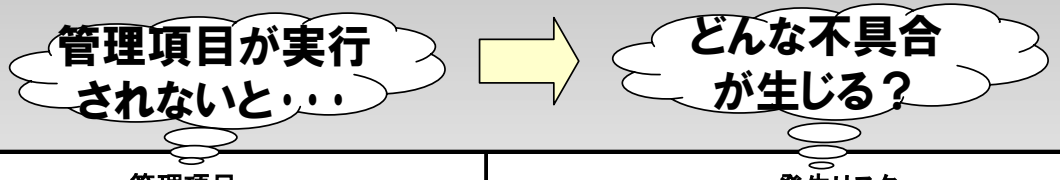
※「日本情報処理開発協会（JIPDEC）「新版 システム監査基準/管理基準解説書 平成16年基準改訂版）システム管理基準とCOBITーIII比較表」に基づいて検討

ITサービスリスク／SLAマトリクス（発生リスク）

■発生リスク

- **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。



プロセス	管理項目	発生リスク
AI2　アプリケーションソフトウェアの調達	ユーザニーズは文書化し、ユーザ部門が確認すること。	ユーザニーズの調査結果を的確に開発計画の策定、開発業務に反映することができない。
	パッケージソフトウェアの使用に当っては、ユーザニーズとの適合性を検討すること。	情報システムが、期待された機能、効果を得られたことを確認することができない。
	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。	構築する情報システムの機能、性能、品質等の要求が、計画とおりに達成することができない。
	開発手順は、開発の責任者が承認すること。	開発手順が、システム分析及び要求定義で定めた要員、予算、期間などを満たしているか確認できない。

ITサービスリスク／SLAマトリクス（リスク移転可否）

■リスク移転の考え方

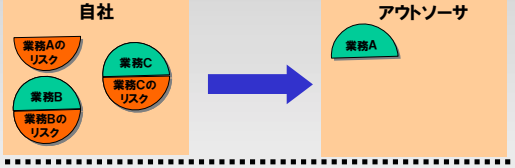
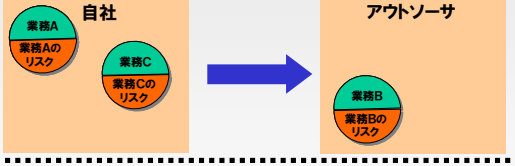
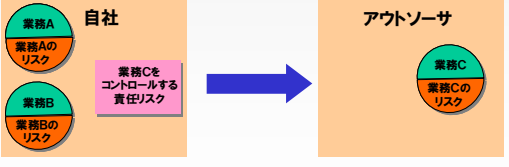
業務をアウトソーシングする場合、発生リスクについて利用者からサービス提供者への移転の可能性を提示

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は移転されず利用者にすべて残る

		表記記号
自社でリスクを**保有**		×
業務Bをアウトソースすることでリスクを**移転**		○
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**		△

JEITA

ITサービスリスク／SLAマトリクス（コントロール手段、サービスレベル主要規定項目 ）

■契約／SLAによるコントロール手段、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項目は、「SLAガイドライン」の「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。

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]

本説明のご参考資料

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

JEITA