ITサービス・リスクマネジメントにおけるSLA活用

2007年7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

JEITA
一般社団法人 電子情報技術産業協会

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

↓

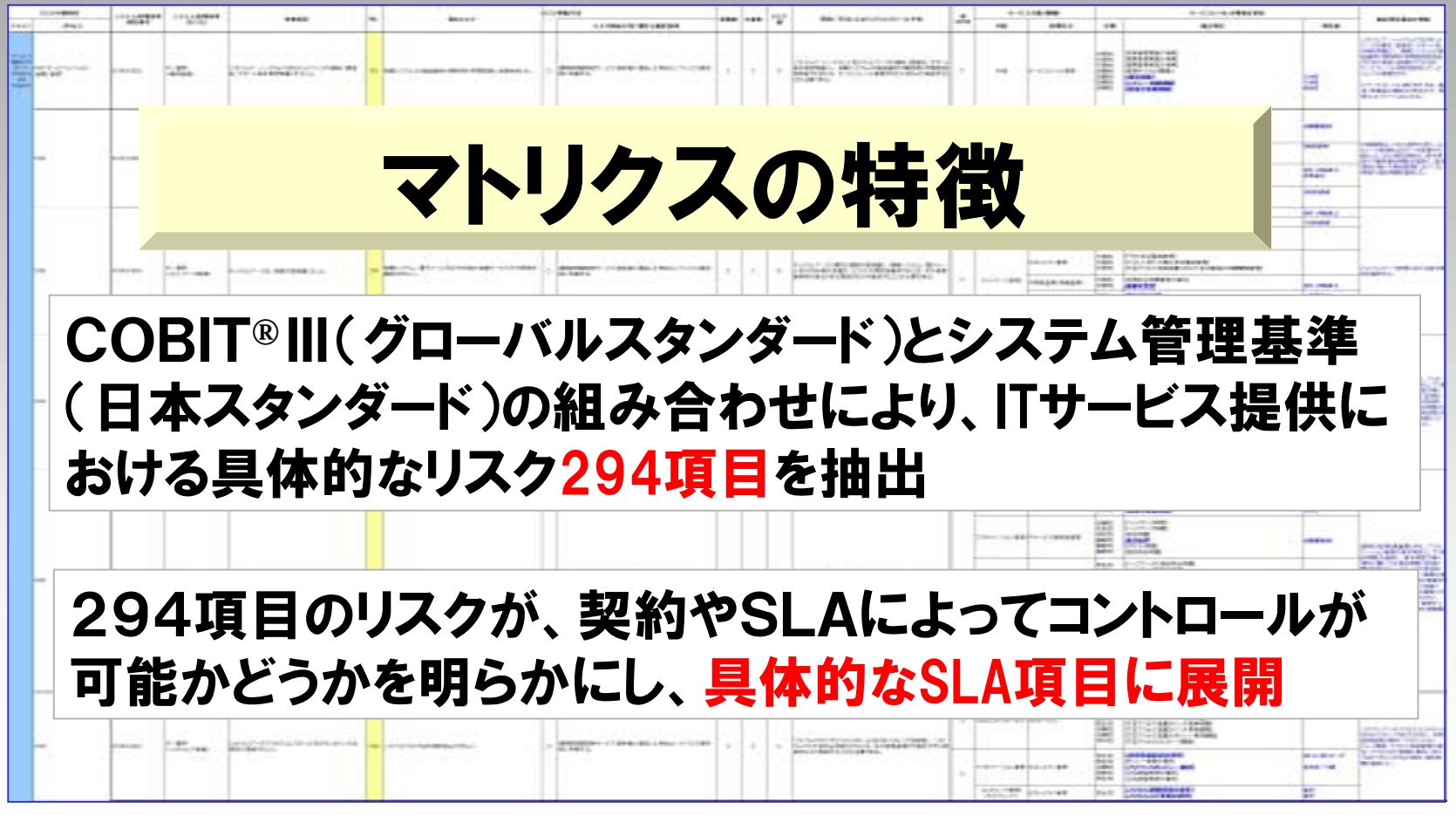
リスクマネジメントの観点から、ITサービス提供者と利用者の関係において、リスクとサービス品質のバランスの取れた適性なITサービスの活用に結びつくガイドラインを提供する必要がある

↓

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

ITサービスリスク／SLAマトリクスの作成



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

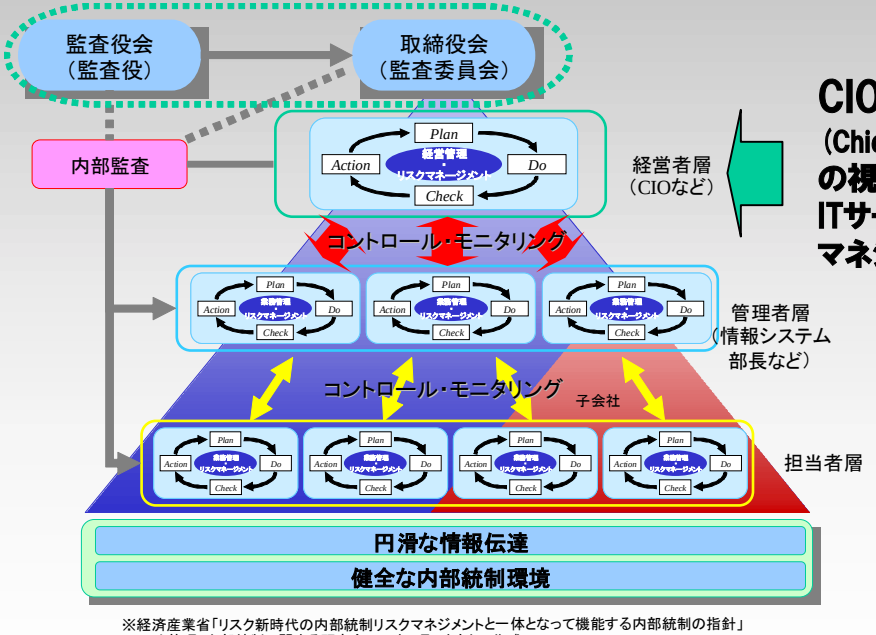
294項目のリスクが、契約やSLAによってコントロールが可能かどうかを明らかにし、**具体的なSLA項目に展開**

JEITA 一般社団法人 電子情報技術産業協会

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

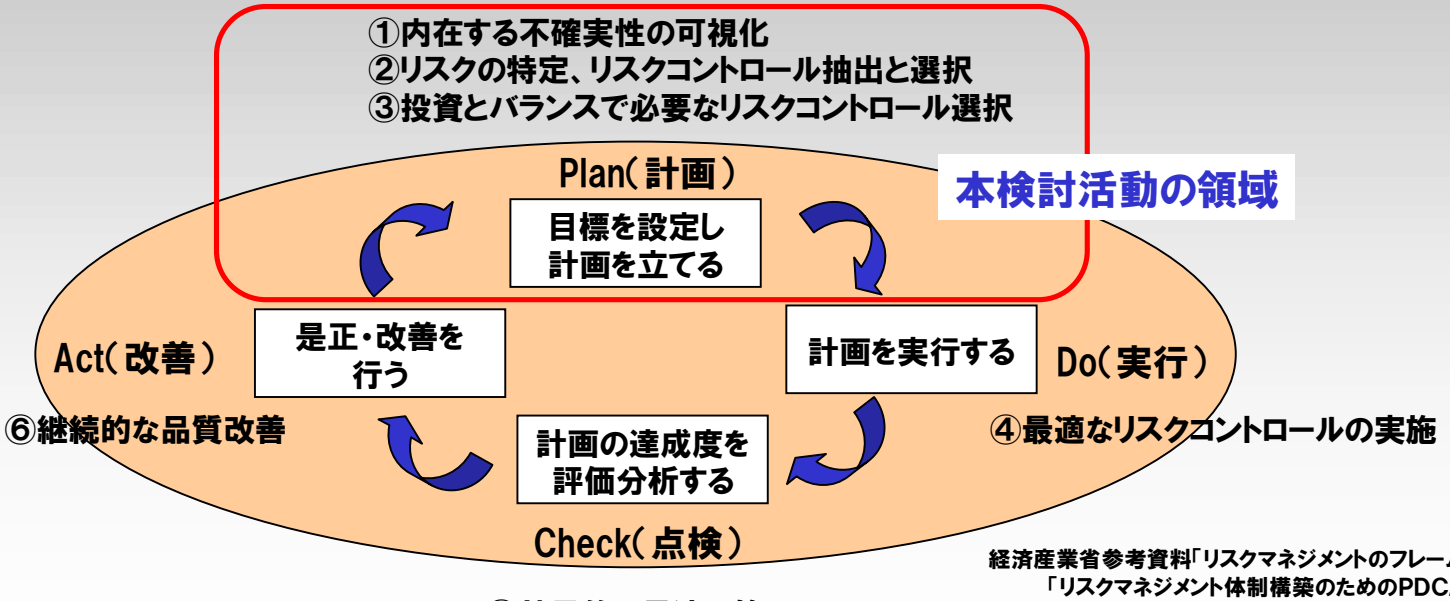


※経済産業省「リスク新時代の内部統制リスクマネジメントと一体となって機能する内部統制の指針」
リスク管理・内部統制に関する研究会2003年6月　をもとに作成

JEITA
一般社団法人 電子情報技術産業協会

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

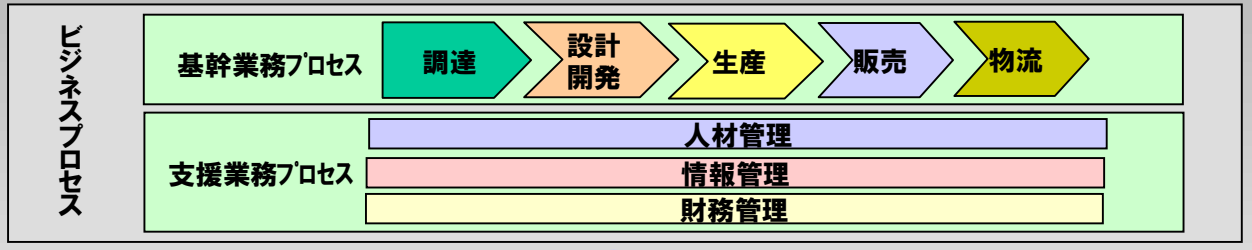


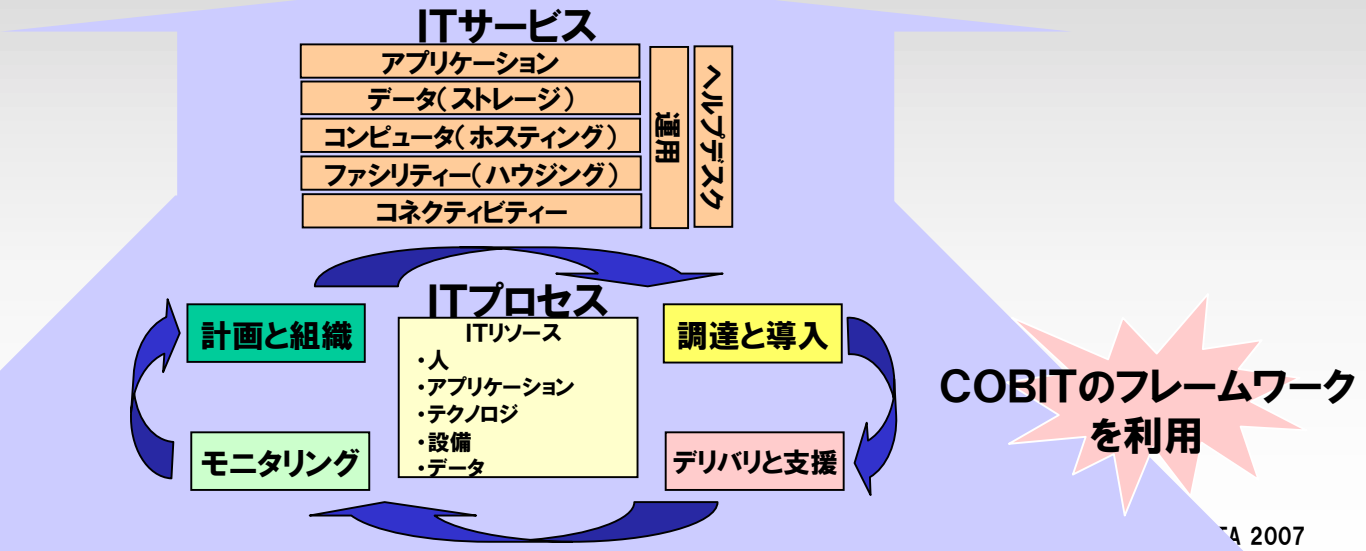
ITサービス・リスクマネジメントのPDCAサイクル

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

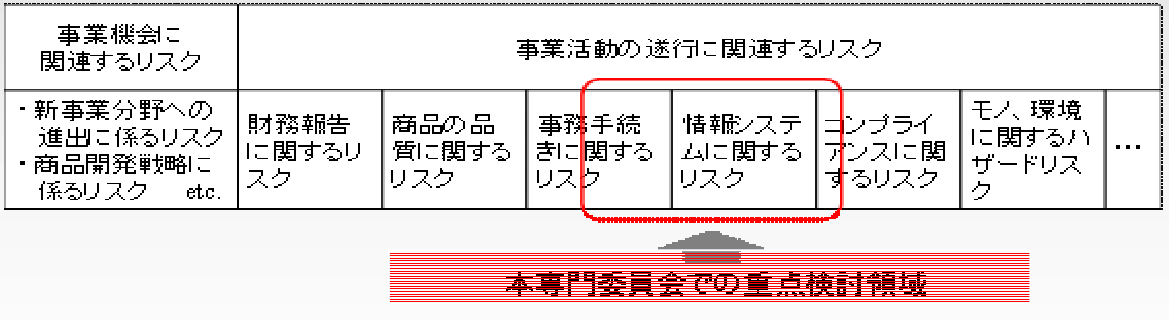
- ITサービスとは、ビジネスプロセスの効率的な遂行を支援するために提供されるITを活用した各種サービス





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）

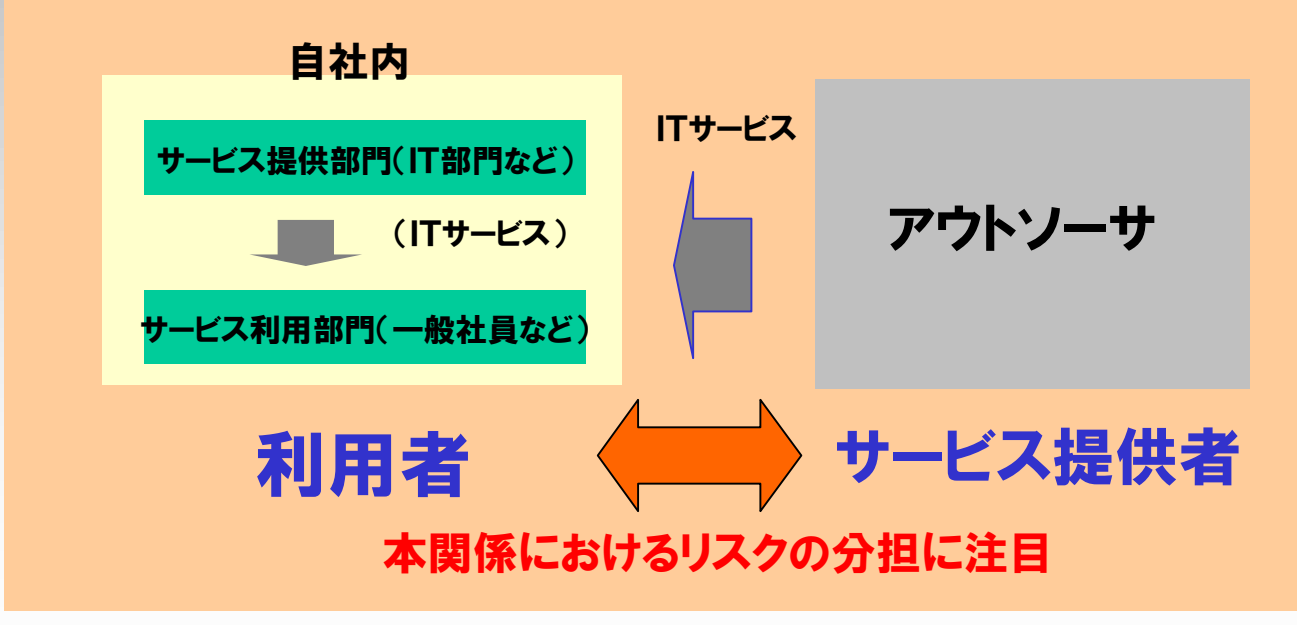


※経済産業省「リスク新時代の内部統制リスクマネジメントと一体となって機能する内部統制の指針」
リスク管理・内部統制に関する研究会2003年6月　をもとに作成
① 事業機会に関連するリスク: 経営上の戦略的意思決定に係るリスク
② 事業活動の遂行に関連するリスク: 適正かつ効率的な業務の遂行に係るリスク

JEITA 一般社団法人 電子情報技術産業協会

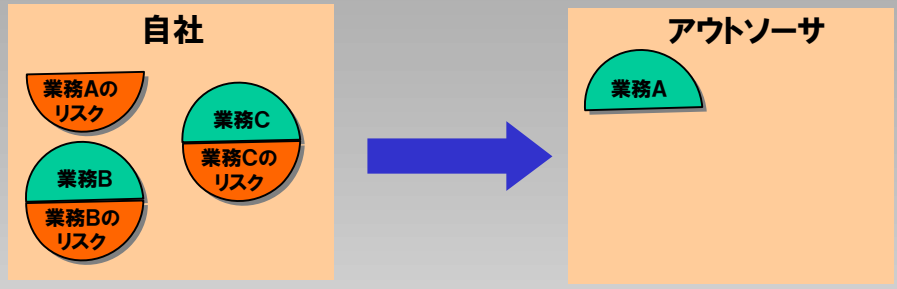
ITサービス提供の考え方とリスクの分担

- 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



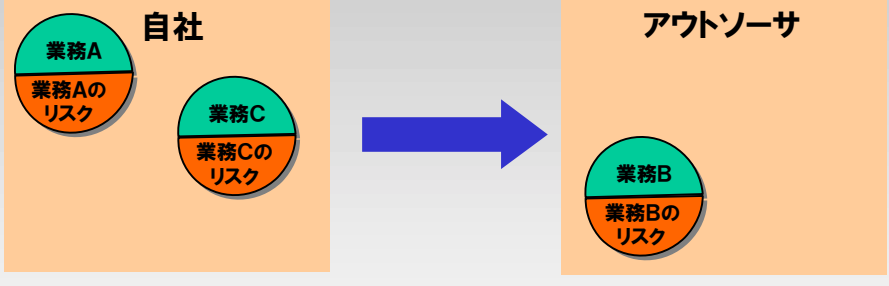
ITサービスリスクの移転の考え方

自社でリスクを**保有**する場合



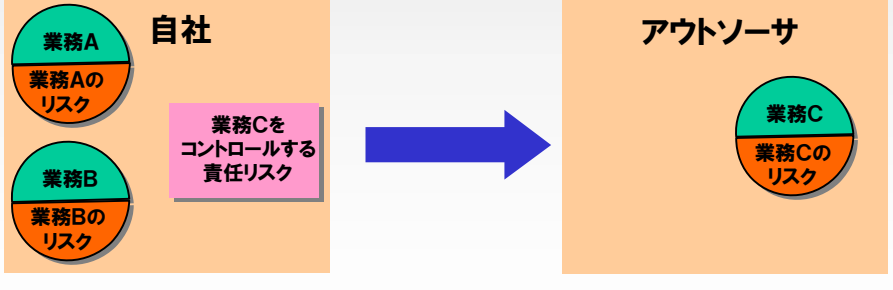
業務Aをアウトソースしても業務Aのリスクは自社内に**留まる**

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

「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

JEITA 一般社団法人 電子情報技術産業協会

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

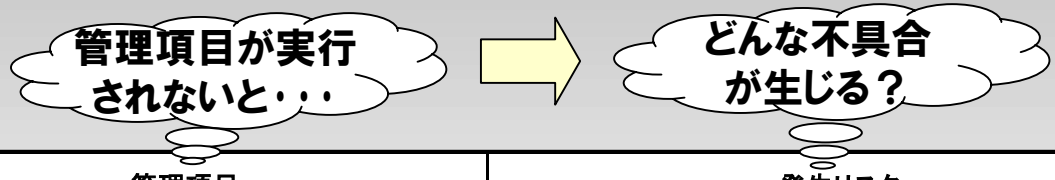
JEITA 一般社団法人 電子情報技術産業協会

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。

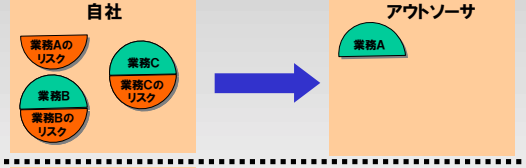
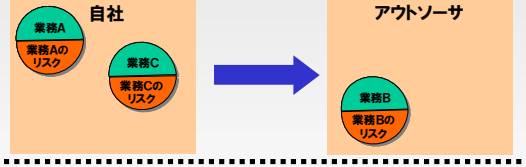
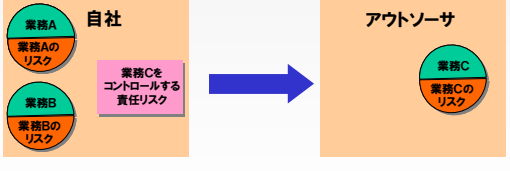
ITサービスリスク／SLAマトリクス（リスク移転可否）

■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**		△

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）

■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。

JEITA 一般社団法人 電子情報技術産業協会

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 ）

■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 ）

■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 ）

■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]

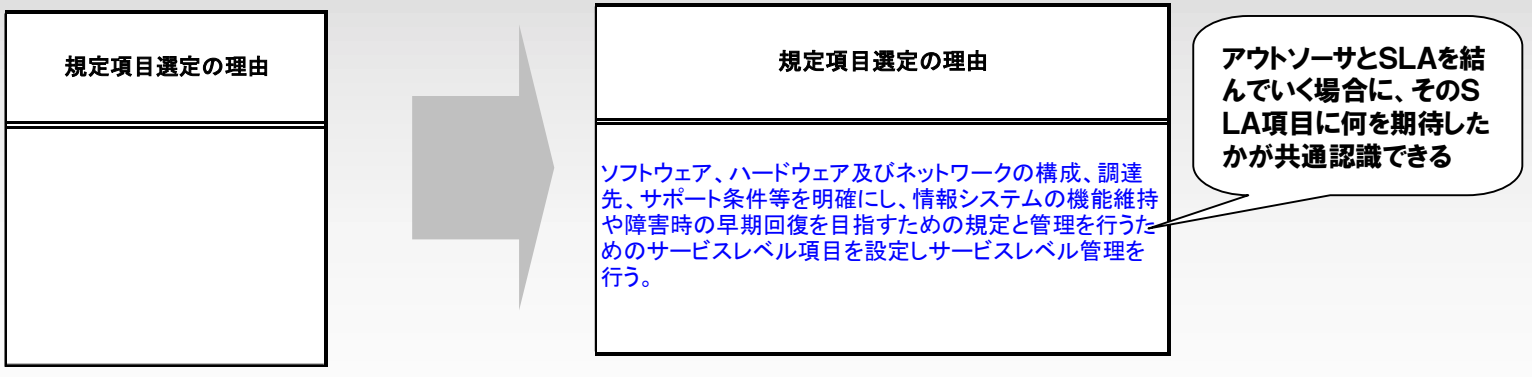
JEITA 一般社団法人 電子情報技術産業協会

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）

■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。



「ITサービスリスク／SLAマトリクス」の活用プロセス

■活用プロセスを7ステップに詳細化し、リスクの絞込みと有効なSLAの選択を効率的に実施可能

自社でコントロールすべきリスクの明確化・SLA項目選択までのプロセスを提示

P1: リスク分類項目の選択

P2: システム管理基準カテゴリ選択

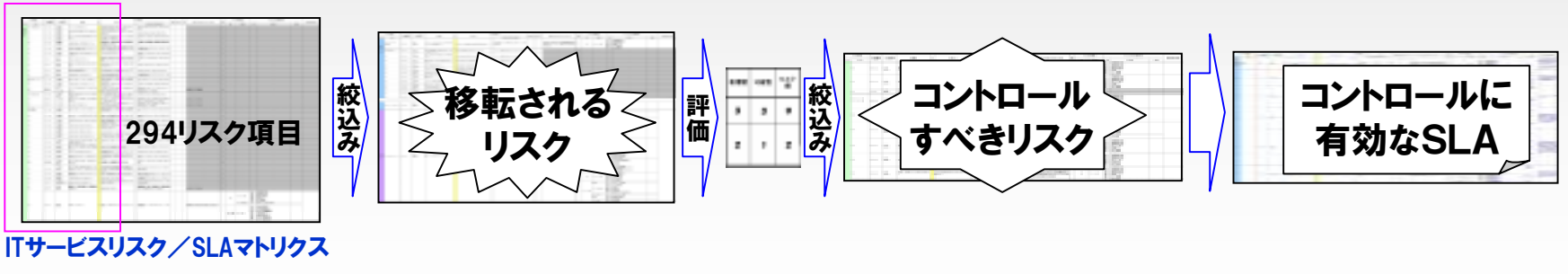
P3: 移転されるリスク項目の洗い出し

P4: リスクの評価

P5: コントロールするリスクを特定

P6: サービスレベル主要規定項目絞込み

P7: SLA項目値設定



ITサービスリスク／SLAマトリクス

活用プロセスの進め方(P1, P2)

P1:リスク分類項目を選択

リスクマネジメントを行なう実際の適用業務の対象領域と過程より「リスク分類項目」からドメインおよびプロセスを選択

P2:システム管理基準カテゴリを選択

対象範囲を「システム管理基準カテゴリ」から選択し絞り込む。

→次にこの項目に対して、適用業務の業務要件による絞込みを行なう

活用プロセスの進め方(P3, P4)

P3:移転されるリスク項目の洗い出し

「リスク移転可否」区分より、適用業務のアウトソーシングの範囲に合わせ、「リスク移転可否」から選択

P4:リスクの評価

実際の適用業務にあわせて、リスクの評価を行う。

活用プロセスの進め方(P5, P6)

P5:コントロールするリスクを特定

リスク評価の結果をもとに、コントロールするリスクを特定する

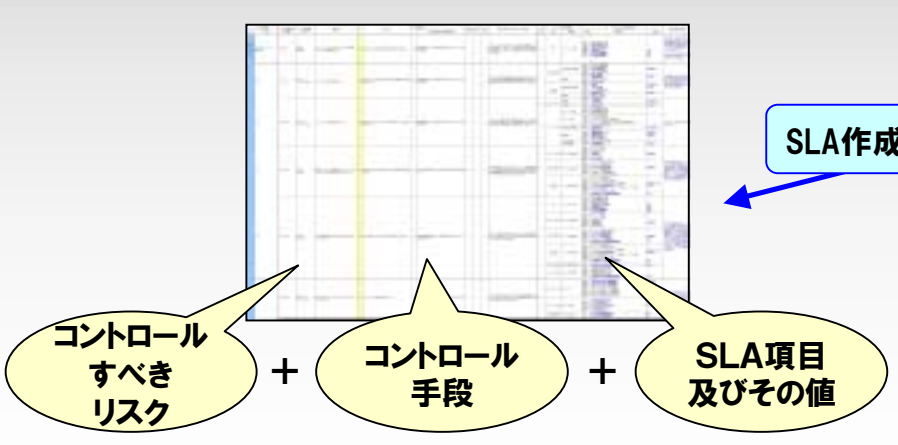
P6:サービスレベル主要規定項目絞り込み

実際の適用業務の内容にあわせて、
「サービスレベル主要規定項目」の中から業務要件にあったものを選択

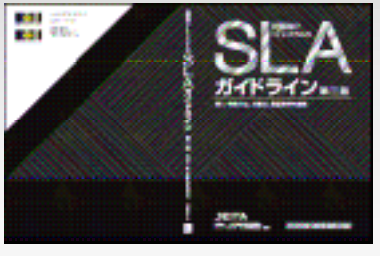
③活用プロセスの進め方(P7)

P7:SLA項目値設定

「サービスレベル主要規定項目」に対して、SLA項目値を設定
→SLA項目値の設定にあたっては、
「SLAガイドライン」の「SLA作成プロセス」を使用



SLA作成プロセス



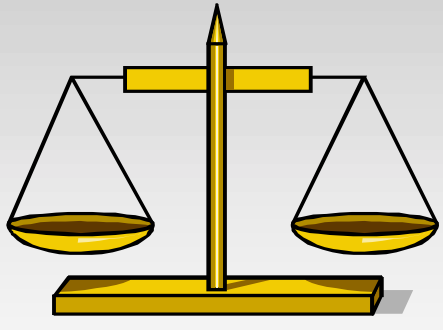
期待効果

「民間向けITシステムのSLAガイドライン　第三版」と組み合わせることにより、コストと品質・リスクのバランスをとることが可能となる。

ITサービスの
品質の可視化

SLA

ITサービスの
リスクの可視化



サービス提供者と利用者の
相互理解に基づく健全な
アウトソーシングサービス

JEITA

2007年度の活動計画

2008年度からの適用が決まった日本版SOX法等、今後の規格・法律整備の動きや市場の変化に対応させた業界標準、ガイドラインを作成すべく、以下の事項について更なる検討を推し進めて行く予定。

1) SLA適用領域の拡大

ITサービスの「見える化」のツールとしてSLAを位置づけ、SLAガイドラインに記載されているSLAの適用範囲を拡大する。

特にSaaS（Software as a Service）の普及を見据えて、SaaS型サービスのSLAガイドラインを検討する。

2) SLM（サービスレベル管理）モデルの検討

ITサービスの継続的な品質維持・向上活動であるSLMのあるべき姿を検討し、SLMモデルを提言する。

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

ご清聴ありがとうございました

（１）今回ご紹介した年度報告書（有償）は下記の問い合わせ先で
お申し込み頂けます。

（２）ガイドラインに関する最新情報は、今後もJEITA情報・産業社会システム部会（ソリューションサービス事業委員会）のホームページに記載しますので参照ください。

- 問合せ先（事務局）：

社団法人 電子情報技術産業協会（JEITA）インダストリ・システム部
〒101-0062　東京都千代田区神田駿河台3丁目11番地三井海上別館ビル
電話：03-3518-6426　　FAX：03-3295-8724
Eメール：itt3@jeita.or.jp
JEITAホームページ　http://www.jeita.or.jp/japanese/index.htm

JEITA
社団法人 電子情報技術産業協会