ITサービスリスク/SLAマトリクスの活用方法

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　副委員長

日本ユニシス株式会社
銅玄 智昭

JEITA

1．　ITサービスリスク/SLAマトリクスの活用プロセス

「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

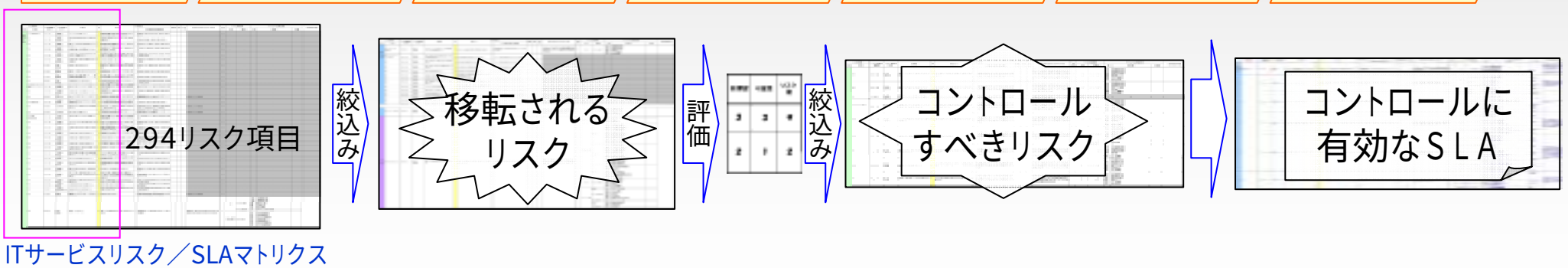
P3: 移転されるリスク項目の洗い出し

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

リスク分類、管理基準カテゴリの選択

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
ドメイン	プロセス						
計画と組織 Planning and Organisation	PO1 IT戦略計画の策定	I -01-1.1-(01)	I -情報戦略 (全体最適化)	ITガバナンスの方針を明確にすること。	1	情報化戦略や情報化投資の決定等について、最終的な判断を下す機関や役職が明確に定義されず、意思決定が遅れる。	×
	PO1	I -01-1.1-(02)	I -情報戦略 (全体最適化)	情報化投資及び情報化構想の決定における原則を定めること。	2	短期計画と中長期計画が矛盾するなど、首尾一貫した全体最適化計画ができない。	×
	PO1	I -01-1.1-(03)	I -情報戦略 (全体最適化)	情報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。	3	最適化目標の達成が経営戦略に結びつかないなど、経営目的を実現する情報システムを企画できない。	×
	PO1	I -01-1.3-(01)	I -情報戦略 (全体最適化)	全体最適化計画は、方針及び目標に基づいていること。	4	経営戦略に基づいた、組織体全体の整合かつ一貫性を確保した情報化を推進することができない。	×
	PO1	I -01-1.3-(06)	I -情報戦略 (全体最適化)	全体最適化計画は、個別の開発計画の優先順位及び順位付けのルールを明確にすること。	5	個別計画の着手の順序、資源配分、開発の期間が、業務との整合性がないままに検討されてしまい、経営課題の重要性および緊急性を反映した、有効な開発投資が行えない。	×
	PO1	I -01-1.4-(02)	I -情報戦略 (全体最適化)	全体最適化計画は、定期的及び経営環境等の変化に対応して見直すこと。	6	全体最適化計画が硬直化・陳腐化してしまう。	×
	PO1	II -01-0-(01)	II -企画 (開発計画)	開発計画は、組織体の長が承認すること。	7	開発計画が全体最適化計画に基づかないまま、部門独自の判断で開発されてしまい、同様なシステムの部門間での統一した開発ができない。	×
	PO1	II -01-0-(02)	II - 企画 (開発計画)	開発計画は、全体最適化計画と整合性を考慮して策定すること。	8	経営戦略に基づいた、組織全体で整合かつ一貫性を確保した開発を行うことができない。	×
	PO1	II -01-0-(03)	II - 企画 (開発計画)	開発計画は、目的・対象業務、費用、スケジュール、開発体制、投資効果等を明確にすること。	9	関係者間で、情報システムの目的や機能などについての共通認識がなく、投資効果があいまいなまま開発が行われてしまう。	×
	PO1	IV-02-0-(01)	IV- 運用 (運用管理)	年間運用計画を策定し、責任者が承認すること。	10	運用計画が責任者や関係者に周知されず、イベントなどスケジュールどおりに円滑な運用が遂行されない。	×
	PO2 情報アーキテクチャーの定義	I -01-1.1-(04)	I - 情報戦略 (全体最適化)	組織体全体の情報システムのあるべき姿を明確にすること。	11	組織体全体の情報システムが、個別の情報システムとの相互整合性を保たずに構築されてしまい、効率性や目的とする効果を達成することができない。	×
	PO2	I -01-1.3-(01)	I - 情報戦略 (全体最適化)	全体最適化計画は、方針及び目標に基づいていること。	12	経営戦略に基づいた、組織体全体の整合かつ一貫性を確保した情報化が推進できなくなる。	×
	PO2	III-02-0-(04)	III- 開発 (システム設計)	データベースは、業務の内容及びシステム特性に応じて設計すること。	13	大量・多種のデータが効率的に格納できず、必要な情報が要求定義を満たす性能で検索・更新できない。	○

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。

移転されるリスク項目の例

システム管理基準項目番号	システム管理基準カテゴリ	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
I -01-1.3-(01)	I - 情報戦略 (全体最適化)	12	経営戦略に基づいた、組織体全体の整合かつ一貫性を確保した情報化が推進できなくなる。	×	全体統制がとれた情報化推進は、利用者側での管理が必要である。
III-02-0-(04)	III- 開発 (システム設計)	13	大量・多種のデータが効率的に格納できず、必要な情報が要求定義を満たす性能で検索・更新できない。	○	開発業務を委託した場合、データベースの設計に関してはサービス提供者側の責任となり、リスクも移転する。
I -02-2.1-(03)	I - 情報戦略 (組織体制)	14	変化する情報技術動向に適切かつ迅速に対応できず、組織体全体としての整合性のとれた情報技術基盤を確立することができない。	×	技術採用方針は、最終的には利用者の判断が必要である。
II -03-0-(03)	II - 企画 (調達)	15	開発に必要なリソースの確保ができず、開始直前や途中で頓挫するなど、計画通りの開発ができない。	○	開発業務を委託した場合には、開発要員・費用・設備・期間の計画策定はサービス提供者の責任となり、リスクも移転する。
II -03-0-(04)	II - 企画 (調達)	16	開発内容に適合したスキルを持った開発要員が確保できず、システムの機能、性能、品質の実現ができない。	○	開発業務を委託した場合には、開発要員のスキル定義はサービス提供者の責任となり、リスクも移転する。
I -01-1.1-(04)	I - 情報戦略 (全体最適化)	17	組織体全体の情報システムが、個別の情報システムとの相互整合性を保たずに構築されてしまい、効率性や目的とする効果を達成することができない。	×	あるべき姿を明確にすることは、最終的には利用者の判断が必要である。
I -01-1.1-(05)	I - 情報戦略 (全体最適化)	18	情報システムの (再) 構築と同期して行われるべき組織および業務の新設、改変および廃止が正しく行われない。	×	組織や業務の新設、改定・廃止は、最終的には利用者の判断が必要である。
I -01-1.2-(01)	I - 情報戦略 (全体最適化)	19	参画者の役割 (統括役員、リーダ、メンバ) が不明確で、能力、経験等を考慮して参画者を選定することができないなど、計画的な立案体制を確立することが難しくなる。	×	経営戦略に基づいた中長期計画の策定判断は、利用者側での管理が必要である。
I -01-1.2-(02)	I - 情報戦略 (全体最適化)	20	経営戦略に基づいた、組織全体で整合かつ一貫性を確保した情報化を推進することが難しくなる。	×	経営戦略の全体整合や一貫性確保は、最終的には利用者判断が必要である。
I -01-1.2-(03)	I - 情報戦略 (全体最適化)	21	全体最適化計画を定めても、それを円滑に運用することができない。	×	利害関係者の調整および合意は、全体判断する利用者側による調整が必要である。
I -01-1.3-(07)	I - 情報戦略 (全体最適化)	22	内部資源の量、質及びコストが外部資源と比較して適性であるかを正しく判断できず、品質低下・コスト増加を招く。	×	資源面での調整および活用は、最終的には利用者判断が必要である。
I -02-2.1-(01)	I - 情報戦略 (組織体制)	23	経営戦略に基づいた情報システムの全体最適化を実現できなくなる。	×	経営戦略を決定する執行機関は、利用者主導であることが必要である。

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

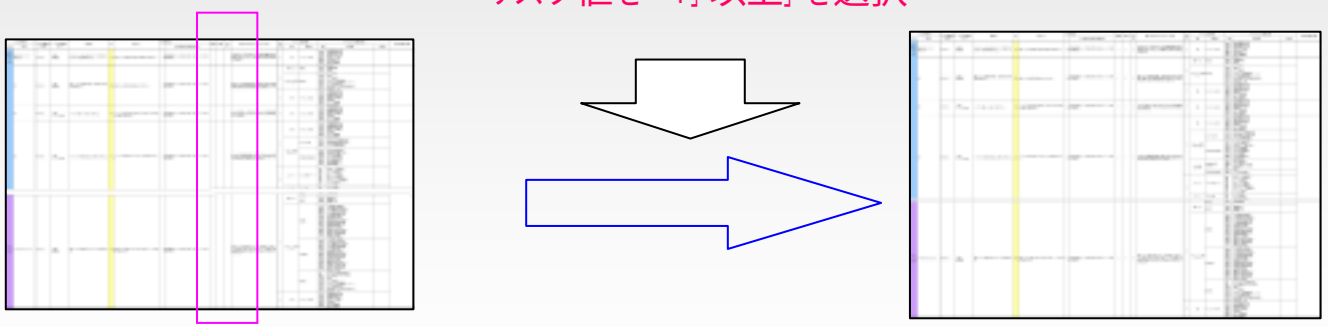
実際の適用業務の内容にあわせて、
「サービスレベル主要規定項目」の中から業務要件にあったものを選択

リスクの特定例

リスク値が一定値以上（例えば「4」以上など）のものを、ITサービス・リスクとしてコントロールする

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
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。	3	3	9

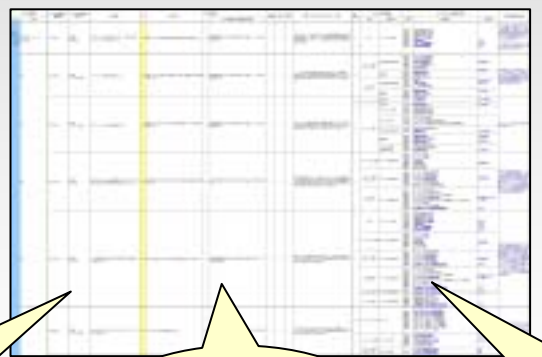
「リスク値を「4」以上」を選択



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

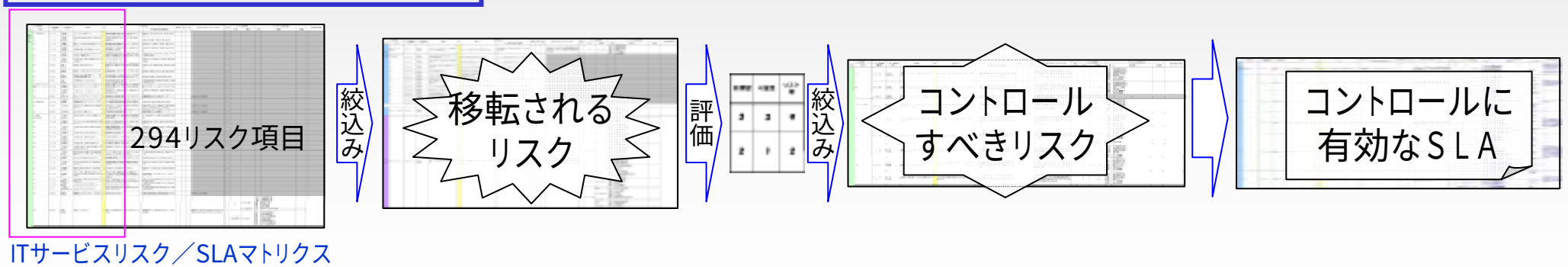
コントロール
すべき
リスク
＋
コントロール
手段
＋
ＳＬＡ項目
及びその値

2．活用プロセスのポイント

【ポイント①】活用プロセスのポイント

実際の活用におけるプロセスのポイントをご紹介

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

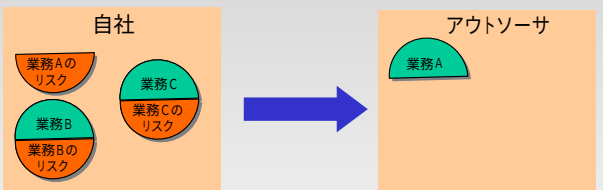
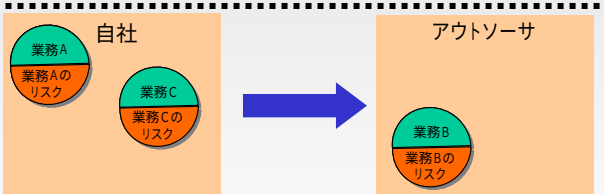
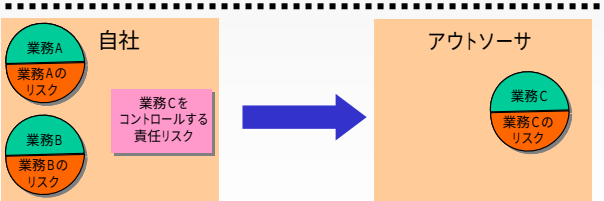
【ポイント②】移転されるリスク項目①

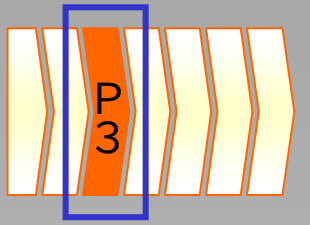
リスク移転の考え方

アウトソーシングサービスの導入によって、業務を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する可能性を提示

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（責任リスクが発生する場合）
×：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		△



【ポイント②】移転されるリスク項目②

リスク移転の考え方整理

「○：移転」と「△：一部移転」の垣根にあいまいさが残らないように整理した。

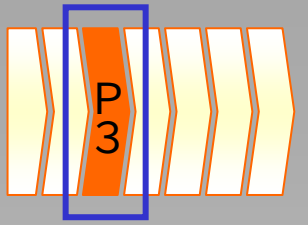
(例)「運用」を全て委託先に業務移転した場合には、「○」となるが、業務に関する最終責任は、利用者に残るので、業務をコントロールするリスクは利用者に残るのでは？
→これでは全て「△」と整理されることになる。

関与度の観点を追加

【関与度が浅い】：開始時に契約でコントロールするリスク管理を明記しヘッジされるもの
(基本的には頻繁に、管理する必要の無いもの)
【関与度が深い】：開始後も定期的に管理作業が発生するもの。

関与度の深さに基づき整理

「○」	リスクを移転可能なもの。【関与度が浅い】ものを含む。
「△」	一部リスクが残るもの、または責任リスクも含む。【関与度が深い】ものを含む。



【ポイント②】移転されるリスク項目③

項目例

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
IV-06-0-(04)	IV- 運用 (ソフトウェア管理)	ソフトウェアのバックアップの範囲、方法及びタイミングは、業務内容及び処理形態を考慮して決定すること。	218	ソフトウェアの記録媒体の障害、誤操作、コンピュータウィルス等による影響を最小化できない。	○	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。

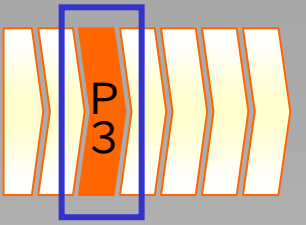
リスクを移転可能なもの。
【関与度が浅い】ものを含む

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
IV-02-0-(14)	IV- 運用 (運用管理)	情報セキュリティに関する教育及び訓練をユーザに対して実施すること。	247	ユーザの情報セキュリティに関する意識が向上しないことに起因するセキュリティ事故が発生する。	△	運用管理業務をサービス提供者に委託した場合は、教育及び訓練を行なう責任はサービス提供者に移転する。ただし教育、訓練を受けた利用者部門のセキュリティ事故に対する責任は残る。

一部リスクが残るもの、または責任リスクも含む。
【関与度が深い】ものを含む。

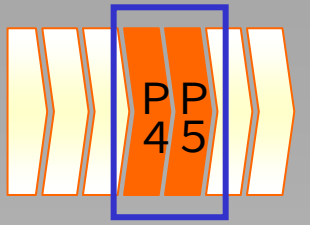
JEITA

【ポイント②】移転されるリスク項目④



移転されるリスク項目の洗い出し

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
IV-08-0-(03)	IV- 運用 (ネットワーク管理)	ネットワーク監視ログを定期的に分析すること。	243	進入及び不正利用を検出して必要な対策を講じられない。	○	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。
IV-02-0-(14)	IV- 運用 (運用管理)	情報セキュリティに関する教育及び訓練をユーザに対して実施すること。	247	ユーザの情報セキュリティに関する意識が向上しないことに起因するセキュリティ事故が発生する。	△	運用管理業務をサービス提供者に委託した場合は、教育及び訓練を行なう責任はサービス提供者に移転する。ただし教育、訓練を受けた利用者部門のセキュリティ事故に対する責任は残る。
IV-06-0-(09)	IV- 運用 (ソフトウェア管理)	フリーソフトウェアの利用に関し、組織体としての方針を明確にすること。	249	処理結果の無保証、コンピュータウイルス混入の危険性、知的財産権侵害等のリスクが内在している。	×	利用者組織体の方針策定は、利用者の責任である。
IV-06-0-(01)	IV- 運用 (ソフトウェア管理)	ソフトウェア管理ルールを定め、遵守すること。	250	ソフトウェアを適切に利用できず、不正を防止できない。	○	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。
IV-02-0-(10)	IV- 運用 (運用管理)	事故及び障害の影響度に応じた報告体制及び対応手順を明確にすること。	252	事故及び障害の発生時に、適切な処置を取れず、影響の拡大を抑制することができない。	○	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。



【ポイント③】リスクの評価と特定①

【影響度】：利用者として、発生した場合の業務にかかるインパクトの大きさ、
もしくは重要性を評価する。重み付けは以下の3段階とする。
「3」：発生した場合に、業務への影響が深刻かつ重大である。もしくは重要である。
「2」：発生した場合に、提供者（アウトソーサ）だけでなく利用者へも影響するが、
業務への影響は低い。
「1」：発生した場合に、提供者（アウトソーサ）内部で閉じて、影響が利用者へ及ばない。

【可能性】：アウトソーシングで発生する可能性を評価する。
重み付けは以下の3段階とする。
「3」：アウトソーシングで発生する可能性が高まるもの。
「2」：アウトソーシングしても、利用者が行なっても発生する可能性が変わらないもの。
「1」：アウトソーシングで発生する可能性が低くなるもの。

【リスク値】：「影響度」と「可能性」をもとにリスク値を評価する。
ISMS（ISO 27001）の考え方に準じ、リスク値は、「影響度」と「可能性」を乗じて求めることとする。

【ポイント③】リスクの評価と特定②

P４：リスクの評価例

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
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。	3	3	9

P５：リスクの特定例

ITサービスリスク／SLAマトリクス

【ポイント④】SL項目絞込みと項目値設定

■P6：サービスレベル主要規定項目絞込み

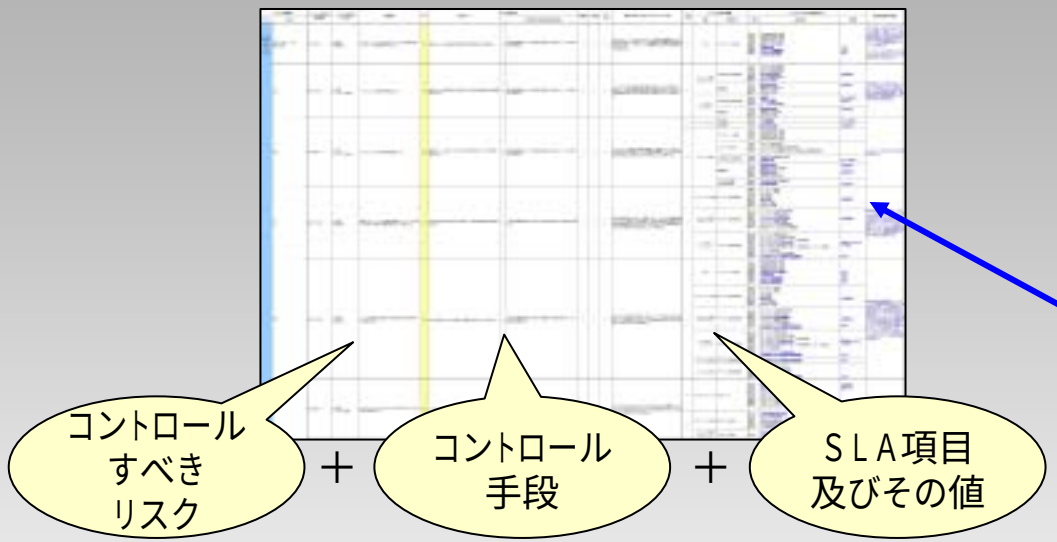
業務内容にもとづき、「サービスレベル主要規定項目」を選択する。

No.	発生リスク	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	
219	情報システムの稼動停止・機能低下の防止や障害発生時の早期復旧ができない。	P	コンピュータ管理（ホスティング）	可用性管理（稼動管理）	信頼性 応答性 応答性 確実性 信頼性	[HWの死活監視間隔] [HWの死活通知時間] ***[HW の復旧時間]*** [HWの定期監視回数] [閾値監視間隔]		対象範囲は、HWの提供であり、コンピュータ管理およびデータ管理を対象とした、また規定項目は、基本項目の「障害通知時間」を選択し、基本項目の無い可用性管理においては、同様の復旧時間を選択した。
				問題管理	応答性 応答性 確実性	***障害通知時間*** [障害切り分け時間] [復旧通知時間]		
			データ管理（ストレージ）	可用性管理（稼動管理）	信頼性 保守性 信頼性	***故障率*** ***サポート期間*** [ハード監視通知間隔]		
				問題管理	応答性 応答性 確実性	***障害通知時間*** [障害切り分け時間] [復旧通知時間]		

ITサービスリスク／SLAマトリクス

【ポイント④】SL項目絞込みと項目値設定

■ITサービスリスク／SLAマトリクス



SLA作成プロセス

SLAガイドライン　付録2　標準SLA項目詳細表

サービス対象（範囲）		サービスレベル主要規定項目（サービスレベル評価項目）			評価および測定方法	測定単位	区分キー		項目選択キー	選択基準	サー				SLAパターン別の目標SLA値								
		分類	項目	内容			要件：required、指標：SL項目		基本・個別	（重要度1→3）	レベル3（上位レベル）	レベル2（			C	D	E	F	G	H	I	J
アプリケーション	サービスレベル管理	信頼性	報告間隔	サービス管理の実施状況を報告する時間間隔が運用ルールに規定されていること	報告間隔＝実施状況を報告する時間間隔	時間（日）	指標		個別	1	数週間以内	1ヶ月			2	2	2	2	2	2	2	2
アプリケーション	サービスレベル管理	信頼性	レビュー実施間隔	定期的にサービスレベル状態をレビューする実施間隔を運用ルールに規定していること	レビュー実施間隔＝サービスレベルの状態が適切に維持されているかどうかを定期的にレビューする実施間隔	時間（日）	指標		個別	1	数週間以内	1ヶ月			1	1	1	1	1	1	1	1
アプリケーション	サービスレベル管理	信頼性	監査の実施間隔	PDCAサイクルが運用ルールに従って適切に実施されているかを監査するサイクルを運用ルールに規定していること	監査実施間隔＝定期的な監査を実施するサイクル	時間（月）	指標		個別	1	3ヶ月	6ヶ月	12ヶ月	規程無し	2	2	2	2	2	2	2	2

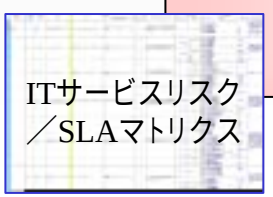
ITサービスリスク/SLAマトリクスの活用の期待効果

「ITサービスリスク／SLAマトリクス」を活用することにより、
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