「CSAJ/JCSSA 情報システムの信頼性向上のための取引慣行・契約に関する検討委員会」

～情報システムの取引慣行・契約に関する実施ガイド～

＜保守・運用に関するガイドライン＞

社団法人コンピュータソフトウェア協会（CSAJ）
社団法人日本コンピュータシステム販売店協会（JCSSA）

目 次

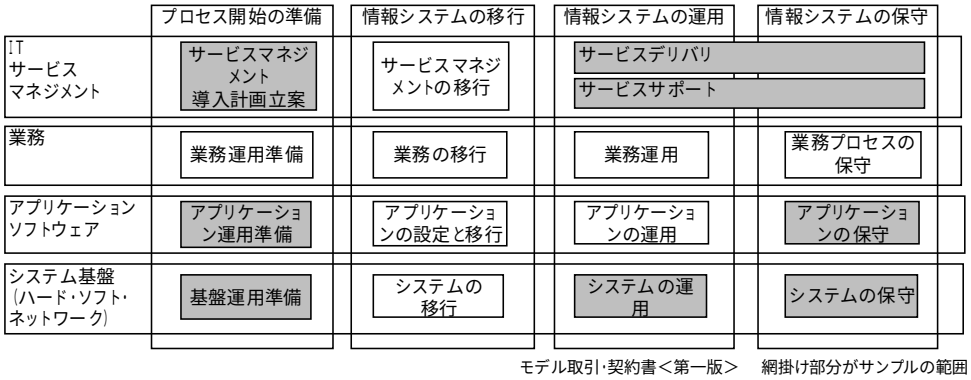
図表 目 次

1　保守･運用サービスの範囲

1.1　モデル取引･契約書＜第一版＞の範囲

「信頼性向上に関するガイドライン[1]」（以降、「信頼性ガイドライン」とする）では、「情報システムを求められる水準で安定的に稼動させていくためには、情報システムの供給者及び利用者が協同して適切な保守･運用を実行しなければならない」と述べている。これを受けて「モデル取引･契約書＜第一版＞[2]」（以下、「第一版」とする）では、検討する保守運用の範囲を、「情報システム運用保守の範囲図[3]」で示し、サンプル事例がその中でどこに位置づけられているかを網掛けで表示している。（図 1 参照）

図 1　情報システム運用保守の範囲図＜第一版＞



モデル取引･契約書＜第一版＞　網掛け部分がサンプルの範囲

また、市場で取引されている多彩な保守･運用サービスの中からサンプル事例として、二つのモデルに関して記述している。

- アプリケーション保守サービス
- オンサイト型アウトソーシングサービス

「アプリケーション保守サービス」では、ITサービスマネージメントレベルまでをカバーしたモデルとなっている。またアウトソーシングサービスを下記の二つのモデルに分類･定義し、オンサイト型のフルアウトソーシングをサンプルとして記述している。（表 1 参照）

表 1　アウトソーシングサービスの分類

データセンター型	保守･運用事業者の施設にユーザの情報システムを設置するサービスを提供する型
オンサイト型	ユーザのデータセンターに保守･運用事業者の要員が常駐してサービスを提供する型

モデル取引･契約書＜第一版＞より

---

1 「情報システムの信頼性向上に関するガイドライン」　経済産業省商務情報政策局情報処理振興課　平成１８年6月１５日

2 「情報システムの信頼性向上のための取引慣行・契約に関する研究会」～情報システム・モデル取引・契約書～（受託開発（一部企画を含む）、保守運用）＜第一版＞　経済産業省商務情報政策局情報処理振興課　平成１９年４月１３日

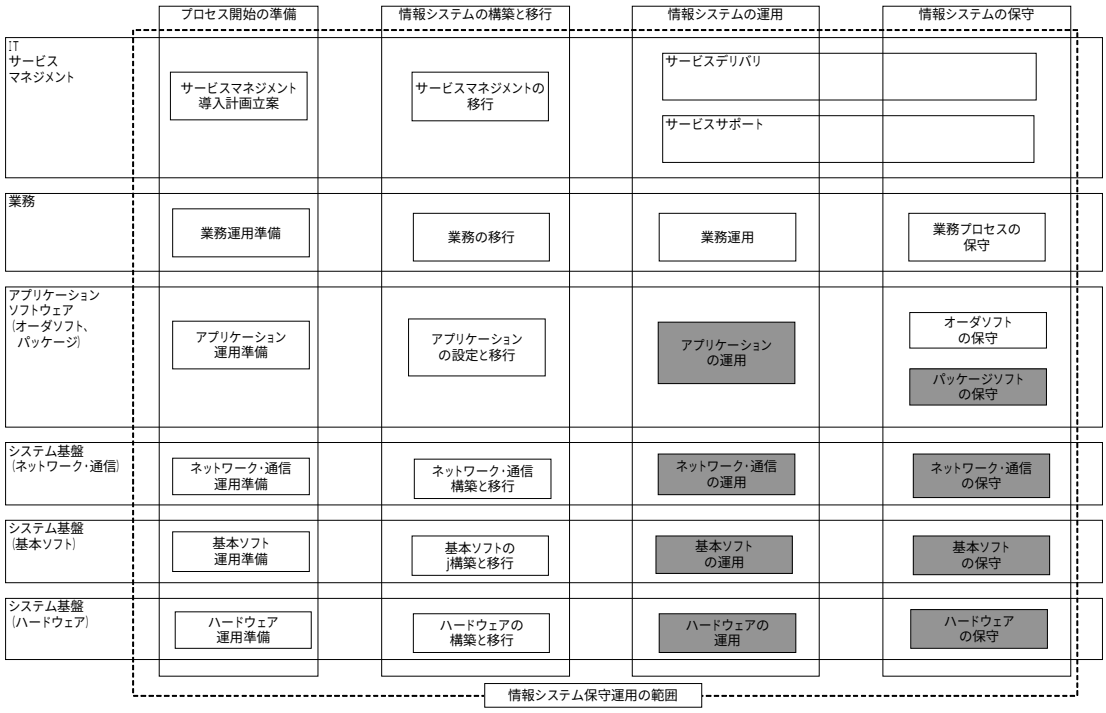
3 モデル取引･契約書＜第一版＞の「(4) 情報システム保守運用委託基本モデル契約書　②保守運用業務の全体構成とサンプル事例の対象」（137頁）

1.2　保守運用ワーキング･グループでの討議範囲

今回の追補版[4]をまとめるに当り、契約検討委員会[5]の下部組織として保守運用ワーキング･グループ（以降、「本 WG」とする）が設置され討議の結果、「保守･運用ガイドライン」（以降、「本ガイドライン」とする）をまとめた。本ガイドラインでは中堅･中小企業ユーザを想定した保守･運用モデルを体系化し、パッケージソフトウェアやＡＳＰ･ＳａａＳモデルを範囲とした。

第一版の「情報システム保守運用の範囲図」を参考に、本ガイドラインの範囲図を一部修正した。（図 2 参照） 修正した部分は、アプリケーションソフトウェアをオーダソフトとパッケージソフトに二分類化し、パッケージソフトウェアを今回の範囲とした。またシステム基盤もハードウェア、基本ソフト、ネットワーク･通信の三階層とし、ハードウェア保守も明確に範囲とした。

図 2　情報システム保守運用の範囲図＜追補版＞



「情報システムの信頼性向上のための取引慣行･契約に関する研究会」～情報システム･モデル取引･契約書～＜第1版＞平成19年4月発行（経済産業省）を参照し一部変更しています。

各階層に含まれる代表的な技術要素を分類化し、本 WG で共通理解を得るようにした。（図 3 参照） 情報システムの技術マップは、各種文献[6]で報告されているが、今回は保守･運用サービスから見た分類をしている。

4 「情報システムの信頼性向上のための取引慣行・契約に関する研究会」～情報システム・モデル取引・契約書～（中小企業、パッケージ活用、保守・運用）＜追補版＞

5 CSAJ/JCSSA 情報システムの信頼性向上のための取引慣行・契約に関する検討委員会（略称：契約検討委員会）

6 参考例：「平成１７年度情報サービス産業における情報技術マップに関する調査報告書」（JISA）

図 3　情報システム･レイア別技術 MAP

				準備	構築	移行	運用	保守タイプ 是正	予防	適応	完全化
ITサービスマネジメント	サービスデリバリ	(ITIL)	サービスレベル管理、ITサービス財務管理、キャパシティ管理、可用性管理、ITサービス継続性管理								
	サービスｻﾎﾟｰﾄ		サービスデスク、インシデント管理、問題管理、構成管理、変更管理、リリース管理								
アプリケーションソフトウェア	オーダソフト	基幹系、情報系など	ユーザー用に独自開発したソフトウェア。(部品としてパッケージソフトを利用する場合はある。)								
	パッケージ	基幹系	ERP系、PDM系、CAD系、業務系 (販売、購買、在庫、生産、財務、会計、人事、給与、など)、ECサイト系、SFA、CRM、青色申告、など				○	○	○	○	○
		情報系	グループウェア、掲示板、Information Portal、情報公開WEB、ブログ、E-Mail、E-learning、ワープロ、表計算、など				○	○	○	○	○
		監視系	ウィルス系、セキュリティ系、運用監視系、障害監視系、トラフィック系				○	○	○	○	○
		部品･ツール系	外部のWebサービス利用、部品･ツール (フォント、OCX、印刷系ソフト、画像処理系ソフト、OLAPツール、検索エンジン、バックアップソフト、など)				○	○	○	○	○
システム基盤	ネットワーク･通信	機器	通信機器 (PBX、ハブ、ルーター、TA、帯域制御装置、FAX、無線、ネットワークカード、通信カード、など)、通信機器付属ソフト (ドライバ、ファームウェア、設定ソフト、(但し、無償サンプルソフトは除く))、ケーブル類				○	○	○	○	○
		通信業者	電気通信業者 (公衆、専用、携帯、PHS)、インターネットプロバイダ				○	○	○	○	○
	基本ソフト	開発支援系	コンパイラ、アセンブラ、リンカ、ローダー、デバッカ、テストツール、CASEツール、文書化ツール								
		ミドルウェア系	シミュレータ、エミュレータ、VMウェア、メタフレームなど				○	○	○	○	○
		OS系	オペレーティングシステム、データーベース管理システム (OLTP系、DWH系、文書系、XML系)				○	○	○	○	○
	ハードウェア		メインフレーム								
			サーバー、クライアント、プリンタ、増設記憶装置、バックアップ装置、その他周辺機器 (通信機器以外)、ハードウェア付随ソフト (ファームフェア、ドライバ、ハードウェア設定ソフト、(但し、無償サンプルソフトは除く))、UPS、など				○	○	○	○	○
ファシリティ		建物･関連設備	建物、電気設備、空調機器、障害対策、監視設備、など								

○印の部分が今回の討議対象 (案)

また検討範囲を網掛けと○印で記した。対象範囲外としては、最上位の階層「ITサービスマネージメント」、及び「オーダーソフト」、「開発系ソフト」、「メインフレーム」とした。また階層に「ファシリティ」を追加し、対象外を明確にした。

横軸のプロセスでの対象範囲外は、プロセス開始の準備および移行とした。共通フレーム2007では保守プロセスに「システム又はソフトウェアの廃棄」が定義されているが、第一版と同様にこのプロセスは対象外とした。しかし、ＡＳＰ･ＳａａＳモデルでは、ユーザ側の事情での解約やＳａａＳベンダ側の事情でのサービス停止や倒産等が発生したとき、特有の問題が発生するため一部言及している。

1.3　保守･運用プロセスの定義

保守･運用のプロセスの定義は「共通フレーム2007」で詳細に定義されている。

1.3.1　運用プロセス

運用プロセスは、「開発プロセスからの資産の引き継ぎ」から始まり、「要員確保」、「上流工程で定義された運用要件の確認」、「運用テスト」、「移行」、「教育」、「評価」などを「共通フレーム2007」で定義している。

2007年度版で変更された部分は、「プロセス開始の準備」アクティビティの中を、「システム運用」と「業務運用」に分けてタスク表記している。また「利用者教育」アクティビティも新たに定義された。

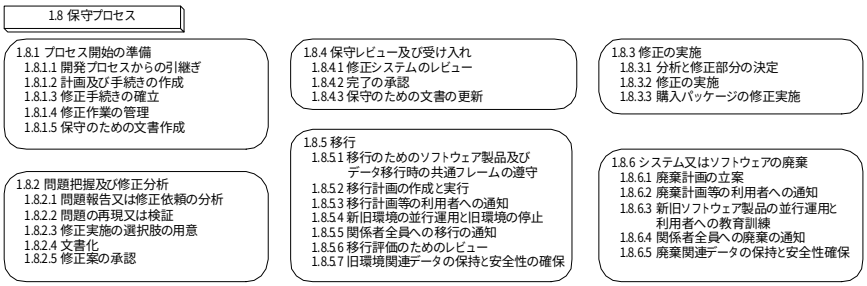
運用プロセスのアクティビティとタスクの一覧を図 4 に示した。2007年度版で変更された部分を太字で、また JIS X 0160 には無い部分を点線の枠で表した。

図 4　共通フレーム2007（運用プロセス）

1.3.2　保守プロセス

「共通フレーム2007」で定義されている保守プロセスを図 5 に示す。

図 5　共通フレーム2007（保守プロセス）



ソフトウェア保守に関しては、JIS X 0161[7]でも定義されている。2008年度版（予定）では緊急保守が是正保守の一部として定義される。（表 2 参照）

表 2　JIS X 0161：2008（ソフトウェア保守）

保守分類	保守のタイプ		説明 〔JIS X 0161:2007〕
訂正保守	是正保守	corrective maintenance	ソフトウェア製品の引渡し後に発見された問題を訂正するために行う受身の修正。 〔注記〕この修正によって、要求事項を満たすようにソフトウェア製品を修復する。
	緊急保守	emergency maintenance	是正保守実施までシステム運用を確保するための、計画外で一時的な修正。 〔注記〕緊急保守は是正保守の一部である。
	予防保守	preventive maintenance	引渡し後のソフトウェア製品の潜在的な障害が運用障害になる前に発見し、是正を行うための修正。
改良保守		maintenance enhancement	新しい要求を満たすために既存のソフトウェア製品への修正 〔注記〕改良保守はソフトウェアの訂正ではない。
	適応保守	adaptive maintenance	引渡し後、変化した又は変化している環境において、ソフトウェア製品を使用できるように保ち続けるために実施するソフトウェア製品の修正。 〔備考〕適応保守は、必ず〔須〕運用ソフトウェア製品の運用環境変化に順応するために必要な改良を提供する。これらの変更は、環境の変化に歩調を合わせて実施する必要がある。
	完全化保守	perfective maintenance	引渡し後のソフトウェア製品の潜在的な障害が、故障として現れる前に、検出し訂正するための修正。 〔注記〕完全化保守は、利用者のための改良、プログラム文書の改善を提供し、ソフトウェアの性能強化、保守性などのソフトウェア属性の改善に向けての記録を提供する。

1.4　IT サービスマネージメント

運用管理を効果的に提供するための規格として、「情報技術－サービスマネージメント」（JIS Q 20000-1 及び-2）が2007年4月に制定された。（表 3 参照）

7 「ソフトウェア保守」JIS X 0161:2008 年度版（予定）

運用サービスのモデルを考慮するに当り、JIS Q 20000 を参考とした。

表 3　情報技術サービスマネージメント(JIS Q 20000-2:2007)

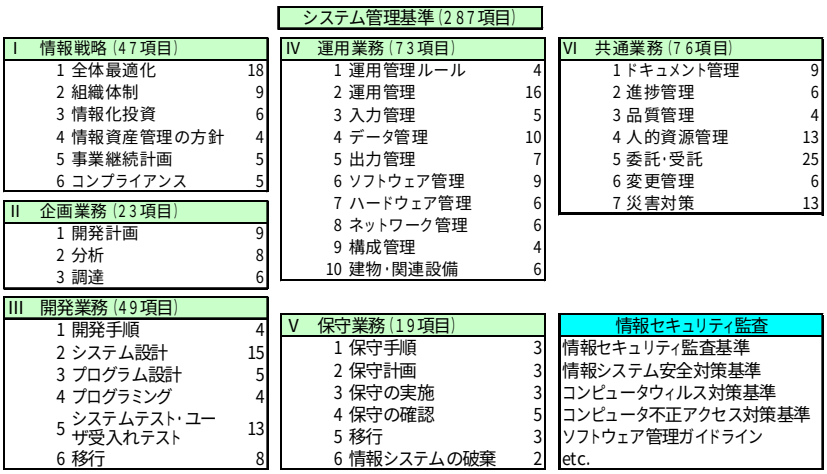
		目的(JIS Q 20000:2007)
6 サービス提供プロセス		
6.1	サービスレベル管理	サービスレベルを定義、合意、記録及び管理するため。
6.2	サービスの報告	十分な情報に基づいた意思決定及び効果的な伝達のための、合意に基づく、適時の、信頼できる、正確な報告書を作成するため。
6.3	サービス継続及び可用性の管理	合意したサービス継続及び可用性についての顧客に対するコミットメントを、あらゆる状況のもとで満たすことを確実にするため。
6.4	サービスの予算業務及び会計業務	サービス提供費用の予算を管理し、かつ、会計を行うため。
6.5	容量･能力管理	顧客の事業において必要な、現在及び将来の合意された需要を満たすために、サービス提供者が十分な容量･能力を常にもっていることを確実にするため。
6.6	情報セキュリティ管理	すべてのサービス活動内で、情報セキュリティを効果的に管理するため。
7 関係プロセス		
7.2	顧客関係管理	顧客及びその事業推進要因に対する理解に基づき、サービス提供者と顧客との間に良好な関係を確立し、かつ、維持するため。
7.3	供給者管理	均質なサービスが確実に提供されるように、供給者を管理するため。
8 解決プロセス		
8.2	インシデント管理	顧客への合意したサービスを可能な限り迅速に回復するため、又はサービス要求に対応するため。
8.3	問題管理	インシデントの原因を事前予防的に識別し、かつ、分析することによって、及び問題の終了まで管理することによって、顧客の事業に対する中断を最小限に抑えるため。
9 統合的制御プロセス		
9.1	構成管理	サービス及びｲﾝﾌﾗｽﾄﾗｸﾁｬのｺﾝﾎﾟｰﾈﾝﾄを定義し、制御し、かつ、正確な構成情報を維持するため。
9.2	変更管理	すべての変更を、制御された方法で、アセスメント、承認、実装及びレビューすることを確実にするため。
10 リリースプロセス		
10.1	リリース管理プロセス	リリースにおける一つ以上の変更を、稼働環境に配送し、配布し、かつ、追跡するため。

1.5　保守･運用の管理基準

システム全体の管理基準は、「システム管理基準解説書[8]」で287項目が定義されている。(図 6 参照)

この中で「Ⅳ. 運用業務」の基準項目として73項目ある。「Ⅴ. 保守業務」はソフトウェア保守を中心に19項目、「Ⅵ. 共通項目」として76項目が、保守･運用に関連する管理基準となっている。ハードウェア保守に関しては運用業務の中の「7. ハードウェア管理」の中にまとめて記述されている。

図 6　システム管理基準



8 「システム監査基準／システム管理基準　解説書」平成１６年基準策定版　監修　経済産業省情報政策局／発行　財団法人日本情報処理開発協会（JIPDEC）

2　保守運用の留意事項

2.1　信頼性ガイドラインでの留意事項

信頼性ガイドラインで保守･運用段階における留意事項が10項目示されている。(表 4及び表 5参照)　これらの留意事項は「システム管理基準」および「システム監査基準」と補完関係にある[9]。

表 4　保守･運用段階における留意事項

留意事項		実施例
1	保守･運用に関する体制等の利用者･供給者間での合意	運用保守体制図及び運用フロー図を作成し、合意する
2	企画･開発･保守･運用の全体を通じたリスク管理	リスクマネジメントのためのチェックリストを作成し、リスクレビュー会議等で定期的にチェックを行う
3	保守･不具合の取扱方針の利用者･供給者間での合意	不具合や保守の重要性を段階的に定め、それぞれのランクに応じた対応内容を文書化しておく(訂正保守と改良保守を峻別し合意)
4	恒常的な運用状況の把握	システムの稼動状況を日･週･月･年単位で取得し、分析を行い、情報システム利用者に対して報告する
5	リリース手順等の整備と訓練	マニュアルに基づくシステムの導入訓練や緊急対応訓練を情報システム関係者間で実施する
6	問題追跡性の確保	構成管理ツールや不具合管理ツール等を活用し、問題追跡性を確保する

表 5　障害対応に関する留意事項

留意事項		実施例
1	緊急時対応の利用者･供給者間での合意	事業継続計画に基づき情報システム障害発生時の対応手順･マニュアルを整備し、定期的な訓練等をしておく
2	原因追求手順等の明確化	情報システム障害に対する原因究明手順書及び様式類を整備し、情報システム利用者及び情報システム供給者間で共有する
3	情報システム障害に関する情報の利用者･供給者間での共有化	情報システム障害管理データベースを整備し、情報システム関係者間で共有化する
4	関連･類似システムの障害情報収集	情報システム障害管理データベースに、関連する情報システム障害を登録する

しかしこの留意事項は、大企業、大規模、重要インフラも範囲とした留意事項であるため、今回の範囲である中堅・中小企業向けには、一部補足説明をする必要がある。また保守・運用に言及するため、より具体的な記述も含めて次節で行う。

2.2　現状の保守運用サービスの問題点と課題

「保守･運用に関する現状の問題点抽出のための調査」[10]を行った。その内容と「信頼性ガイドラインでの留意事項」も合わせて、課題を抽出し留意事項として表 6 にまとめた。

---

9 「情報システムの信頼性向上に関するガイドライン（案）へのパブリックコメント結果表」の項番７より引用

10　本ＷＧで「保守・運用サービスに関するトラブル事例」を平成１９年６月に調査。
調査対象は同ＷＧのメンバー。

表 6　保守運用の留意事項

NO	留意事項	内容	節番
1	組織･体制の明確化	運用責任者の明確化 運用フローの明確化 問題解決手順の明確化、など	2.3
2	曖昧な契約の排除	契約内容の明確化（保守範囲の明確化） コミュニケーション向上（契約担当者と実務担当者など） 情報開示（ハードメーカ、ソフトメーカ）	2.4
3	セキュリティ･可用性の充実	セキュリティの重要性 入退出管理（特に一般人の出入りが多い施設） ID/パスワード管理 バックアップ、事業継続計画の策定、など	2.5
4	ハードウェア保守	保守範囲の明確化、保守対象外部品 製品寿命、部品提供期間などの期間管理 事前停止の考慮、保守機器の管理、など	2.6
5	アプリケーション保守（パッケージソフトウェア）	保守範囲の明確化、カスタマイズの定義、 ＦＯＳＳの保守、保守不能の防止、 変更管理･リリース管理の重要性、 サポート期間の確認 瑕疵基準の合意（訂正保守、改良保守）、など	2.7
6	繰り返し型開発、アジャイル開発の場合	開発モデルに合わせた変更管理、リリース管理	2.8
7	ＡＳＰ･ＳａａＳモデル	通常時の保守運用 ＡＳＰ･ＳａａＳベンダの選定 内部監査実施状況、など	2.9
8	保守タイプと瑕疵との関連	脆弱性対策と瑕疵担保責任 瑕疵調査費用の取扱い 事前確認の重要性、など	2.10

節番：留意事項を説明している本文の節の番号

特に、組織･体制の明確化、契約時の事前確認、契約内容の明確化などが重要となる。

2.3　組織･体制の明確化

信頼性ガイドラインでは、「利用者及び供給者は、保守・運用に係る活動全般について、双方の推進体制及び承認手順を文書化し両者で合意すること」とし、運用保守体制図や運用業務フローを作成し合意することを求めている。「システム監査基準」でも「ユーザ責任者、運用管理責任者、保守責任者などに対して役割と権限を明確に定義する必要がある」と規定している。

企業規模が小さくなるほど運用管理責任者や保守責任者などの責任者を設置していないユーザがあり、保守・運用上のトラブルを正しく対処できなく損失が増大する傾向にある。責任者設置の重要性を認識し、運用フローや問題解決手順などを明確化しておくことが強く望まれる。

2.4　曖昧な契約の排除

保守・運用上のトラブルを分析すると、「契約内容の曖昧さ」や「ユーザとベンダー間での契約時の確認不足」、「利害関係者間のコミュニケーション不足」による問題が多かった。

2.4.1　契約内容の明確化

信頼性ガイドラインでは、契約における重要事項の明確化を求めている。「情報システム利用者と情報システム供給者が明確化・共有すべき事項については、原則として契約において規定する」としている。

保守・運用サービスの範囲、責任、役割分担、体制などの明確化が重要である。中堅・中小企業においても、最大限明確な契約の内容とするよう心掛けることが必要である。

2.4.2　コミュニケーションの向上

契約当事者と実務担当者が異なるときの注意として、契約内容を実務担当者に周知徹底させておく必要がある（ユーザ側、保守側ともに）。特に契約地より遠い出先機関でのトラブルを未然に防ぐためにも必要となる。

2.4.3　情報開示（ハードメーカ、ソフトメーカ）

保守･運用サービスの、より進んだ内容の情報開示が求められる。特にソフトウェアパッケージでは、製品機能に関する情報開示に傾注するのは販売戦略上必要となるが、保守･運用面で考えると実施可能な範囲、注意制限事項など、より進んだ情報の公開が望まれる。（レスポンス、推奨ユーザ数、参照整合性、トランザクション処理、など）

2.5　セキュリティ･可用性の充実

2.5.1　セキュリティの重要性

① 入退出管理

個人情報や機密情報を取り扱う一般人の出入りが多い施設（例：病院や公共施設など）ほど、セキュリティ管理の重要性が望まれる。施設の運用の一部をアウトソーシングするときは、特にセキュリティ管理が重要となる。

② ＩＤ／パスワード管理

パスワードは、あらゆる機器（サーバー、クライアント、ハードディスク、ネットワーク機器、など）やソフトウェア（ＯＳ、データベース、業務アプリケーション、など）に設定されている。セキュリティ面からは、ユーザ個々人のユーザＩＤ、パスワード以外に、あらゆる機器のＩＤとパスワード、ソフトウェアのＩＤとパスワードを運用や保守などの責任者が管理する必要がある。

しかし、責任者が不明確なユーザではパスワードの管理が出来なくなり、保守・運用会社の担当者に安易に依頼する場合がある。担当者レベルでの管理ではなく、第三者に依頼するなど、セキュリティの向上が望

まれる。

2.5.2　バックアップ

データ及び、システムのバックアップは事業継続性の観点からも重要事項となる。バックアップ方針に基づきバックアップ計画を策定し、確実に実行することとともに、リストア計画の策定及びその実行・評価も重要となる。

2.6　ハードウェア保守

「システム管理基準」の「Ⅳ-７-（3）運用業務・ハードウェア管理」で「ハードウェアは定期的に保守を行うこと」と規定されている。また、「想定されるリスクの管理」や「障害対策を講じること」と記述されている。実際のハードウェア保守は、各メーカーによって詳細は異なっており、契約時に事前確認が必要となる。

「問題点抽出のための調査」で寄せられた代表的な意見を解説する。また、この節の最後に確認事項としてまとめている。

2.6.1　データ復旧は別メニュー

① 工場出荷状態に戻すのが一般的

ハードウェア保守は、故障修理が原則であり、工場出荷状態または導入当初の初期状態に戻すのが一般的となっている。ディスク内のデータ復旧や、最新の設定内容にするのは、ユーザ側の責任作業となっている場合が多い。

しかし運用面から見ると、故障発生時直前の状態に戻らないと、運用上の問題が発生する場合が少なくない。保守運用会社に、故障発生直前の状態に戻すことを依頼するためには、「別メニューの契約」や「復旧支援サービス付きのハードウェア保守契約」が必要となる。

② データバックアップはユーザ責任が一般的

データのバックアップはユーザ責任で行うのが一般的である。バックアップも保守運用会社に依頼するときは、「バックアップ運用支援サービス」などを契約する必要がある。これらをパック化したサービス商品も見られる。

③ 交換したディスク内のデータは秘密保持条項で保護

ハードディスク等の外部記憶装置が故障（クラッシュなど）して、部品交換行ったとき、その故障部品の所有権は、保守会社に帰属するのが一般的である。保守料金の設定も、これを前提に設定されている。このとき、故障した部品の中に記憶されているデータ（個人情報や機密情報など）の保護は、保守契約書にある機密保持義務条項で保護される。記憶されている情報の確実な破棄を保守会社に要求するときは、別契約が必要となるのが一般的である。

2.6.2　保守対象外部品

ハードウェア保守契約を締結しているにもかかわらず、部品代の請求が発生するがある。これは保守対象外部品（有寿命交換部品、有償部品、消耗部品などとも言う）が存在するためであり、契約前の事前確認が必要となる。（例：内臓バッテリー、内蔵ハードディスク、インクリボン、トナーなどの消耗品、など）

2.6.3　製品寿命や保証期間などの期間管理

アプリケーションソフトウェアのライフサイクルに合わせて、システム基盤となるハードウェア、ＯＳ、ミドルウェア、ネットワーク機器などの製品寿命や保障期間、部品提供期間などを管理する必要がある。

長期間に渡りアプリケーションソフトウェアを稼動させるためには、システム基盤の各種期間を細かく管理し、期限到達前には代替機種の検討や適用保守などを十分な期間をかけて検討する必要がある。また、費用が発生する場合が殆どなので予算化しておく必要がある。

2.6.4　事前停止の考慮

システムが運用プロセスに入っても、ハードウェアやソフトウェアの保守のために、システムの一部や全体の停止が発生する。企画や要件定義のプロセス時に、製品（ハードウェア、ソフトウェア）の特性や耐久性、安定稼動対策などを考察し、事前停止を考慮しておく必要がある。また、運用時の対応方法（決定ルールや事前通知方法など）も検討しておく必要がある。事前停止には、下記の二つが考えられる。

① 計画停止

1年365日24時間稼動が求められる業務が近年増加している。しかしハードウェアやソフトウェアは定期保守が必要であり、そのための計画停止が必要となる。無停止稼動時間を長くするほど（計画停止時間を短くするほど）、システムの全体価格（導入価格および運用コスト）は上昇する。導入時には費用対効果も検討し、計画停止時間、間隔を決定する必要がある。

② 緊急停止

システムが安定稼動しているときでも、ＯＳの緊急パッチやウィルスチェック強化などのソフトウェア保守が発生する。その時は、システムの一部や全体を、一時的に緊急停止する必要がある。緊急度や影響度などを総合的に判断して、システムの一部又は全体を停止する。

2.6.5　保守機器の管理

保守対象機器の管理は、機種機番、設置場所などの情報がコンピュータ管理され、対象機器には目印となるシールなどが張ってあるのが一般的である。

故障時には、代替機や機器交換などにより、筐体が変更される場合がある。その時は交換された機器に新しいシールの張替えや、機番変更などを行う。これらの処理を正しく行わないと保守対象機器の特定が困難となる。

ハードウェアの設置場所の移設や廃棄をユーザが行った時には、保守会社への連絡が必要となり、ユーザの管理が重要となる。

数多くのクライアントや周辺機器の保守を行う場合は、管理が特に煩雑となる。きめ細かな管理を実施しないと、保守対象機器の特定が出来なくなり支障をきたす。ハードウェアの破棄時、どの保守契約を解約したら良いかの判断も出来なくなり、解約手続きが遅延する。解約するまでは、破棄したハードウェアにも保守料金が発生しているので注意が必要となる。

2.6.6 ハードウェア保守確認事項

アプリケーションソフトウェアを正常に稼動させるには、その構成品目である各種ハードウェア（サーバ、クライアント、プリンター、ルーター、回線、など）の特性、保守状況などを細かく管理することが必要となる。ハードウェア保守での特有の確認事項を表 7 にまとめた。

表 7　ハードウェア保守特有の確認事項

項目名	表示例
ベンダー側	
製品耐久性	印刷20万枚、液晶バックライト時間40,000時間、ハードディスク50,000時間、など
設置環境	動作時温度･湿度、保管時温度･湿度、結露しないこと、設置スペース、など
無償保証期間	半年、1年間、3年間、など
部品提供期間 （部品保有期間）	製造中止後7年、販売終了後5年、ユーザ設置後5年、など
保守対象外部品 （有寿命部品）	内臓ディスク、バッテリー、プリンター･ローラー、消耗品（インク、トナーなど）、など
純正部品のみ保証	リサイクルトナーやリサイクルインクは不可、など
計画停止･緊急停止時期	停止日、期間、サイクル、など
保守機器の管理	保守機器の確認方法、など
ユーザ側	
業界上の制約	法律や業界で規定されている事項 ワイヤレスLAN使用規制、携帯電話使用規制、など
保守機器の管理	アセット管理（設置場所など） 機器別保守会社の把握

2.7 アプリケーション保守（パッケージソフトウェア）

アプリケーションソフトウェアは、オーダソフトとパッケージソフト（基幹系、情報系、監視系、部品・ツール系）に大別される。（図 3 参照）　ここではパッケージソフトに絞った形で言及するが、オーダソフトと共通している部分もある。

ソフトウェア保守をアプリケーション保守と言い換えているのは、基本ソフトを含めてない形を明確にするためである。基本ソフトの保守は、ライセンス

保守として契約されるケースが一般的である。また、パッケージソフトの本体部分はライセンス契約で、カスタマイズした部分はアプリケーション保守契約で行われる場合もある。

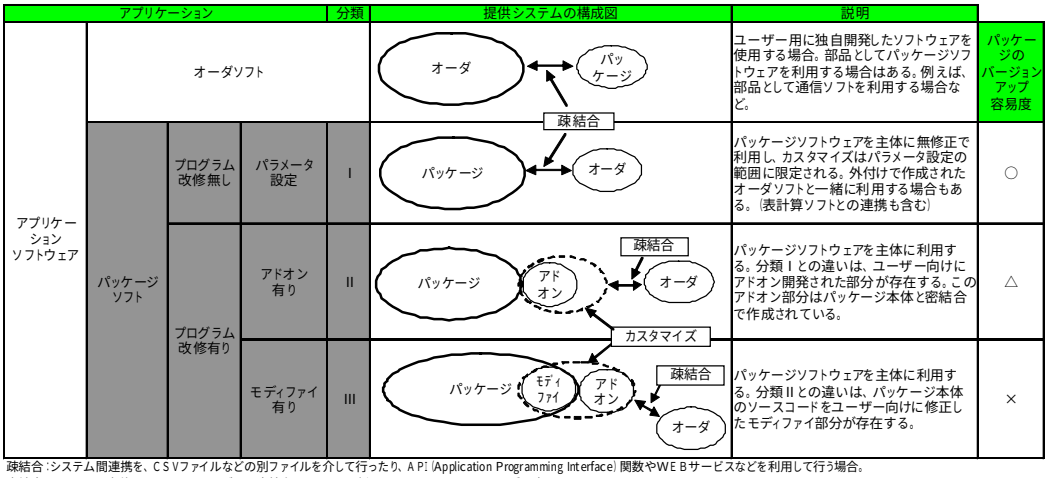
留意事項としては、ハードウェア保守と共通している項目も多い。「契約の曖昧さの排除」や、「サービス内容の範囲を明確化」などである。ソフトウェアの特性としては、瑕疵担保の取扱いが重要となるため、次節（2.10）で詳しく述べる。

2.7.1 カスタマイズの定義

パッケージソフト保守のときは、カスタマイズの有無やカスタマイズの大きさによって保守性が異なる。また保守を担当する会社が、そのパッケージのカスタマイズが出来るかどうかによっても保守性が異なる。

パッケージソフトカスタマイズの一般的な分類をした。（図 7 参照） アプリケーションソフトウェアは、オーダソフトとパッケージソフトに大別される。またパッケージソフトの、カスタマイズを3分類した。カスタマイズは、パラメータ設定部分とアドオン部分、モディファイ部分に分けて考える必要がある。以下に、著作権も含めた一般的な考え方を記した。

図 7 パッケージソフトカスタマイズ分類



疎結合：システム間連携を、ＣＳＶファイルなどの別ファイルを介して行ったり、ＡＰＩ（Application Programming Interface）関数やＷＥＢサービスなどを利用して行う場合。
密結合：パッケージ本体のファイルやテーブルを直接参照したり、更新する。また、ファイルやテーブル変更もありえる。

① 図 7 はアプリケーションソフトウェアをオーダーとパッケージとに大別し、さらにパッケージソフトはプログラム改修有無などで3分類している。

② カスタマイズはユーザ要件により実施され、プログラム改修がともなわない場合とプログラム改修がともなうアドオンとモディファイに分類される。

③ プログラム改修（ソースコードの追加･変更･削除）をしないで、パラメータ設定のみでユーザ要件が満たされる場合を分類Ⅰに区分した。

④ パッケージのソフトウェア保守を行うときは、対象パッケージが分類Ⅰ～Ⅲのいずれかであるかを明確にしておく必要がある。

⑤ 将来、頻繁にバージョンアップが必要なときは、プログラム改修無し（分類Ⅰ）で利用する方が良い。
⑥ カスタマイズが大きくなるほど、バージョンアップが困難になる傾向にある。
⑦ 分類ⅡやⅢで利用しているときにバージョンアップを行うと、別途、開発費用が発生する場合が多い。
⑧ パッケージメーカー以外が、アドオンやモディファイを開発するときには、パッケージ内部の開示や著作権の問題を解決しておく必要がある。
⑨ パッケージ本体及びカスタマイズ部分の著作権は、パッケージメーカーに存在する場合が多い。

2.7.2 フリーソフト及びオープン・ソース・の保守

FOSS[11]の場合の保守は事前の確認や契約が特に重要となる。ベンダが主体で選定する場合や、ユーザが主体で選定する場合によって責任範囲や保守性が異なる。第一版での取扱いを表 8 にまとめた。

表 8 FOSS の場合の責任範囲の取扱い

前提条件	ベンダが瑕疵及び権利侵害の有無を把握することは困難 ベンダが主体で提案した場合でも、ユーザは自らの責任で採用決定をする
ライセンス契約	ユーザがライセンサーと直接、ライセンス契約をする ユーザと第三者間で問題解決を図る
ベンダが主体で選定	ベンダは説明義務を契約上の責任として負う ベンダは故意重過失で説明しなかったときは免責されない
ユーザが主体で選定	ベンダは一定の説明責任を負う ベンダは悪意重過失で説明しなかったときは免責されない。

モデル取引・契約書＜第一版＞より

フリーソフトウェアは低コストで便利に利用できる反面、ウィルスの混入や知的財産権侵害、製品の品質保証などの問題点も多い。採用に当たっては、実績や安全性など十分に検討する必要がある。またシステム管理基準では、「Ⅳ・６・（９）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」と規定している。

2.7.3 保守不能を防止

開発メーカーの倒産等により、パッケージ保守が出来なくなる問題が発生する場合がある。ユーザを保護する制度として、ソフトウェア・エスクロ制度[12]がある。ユーザは利用を含めて検討する必要がある。

---

11 Free and Open Source Software の略。

12 ライセンサー（ソフトメーカ等）が倒産等した場合に、予め設定されている開示条件でソースコード等をライセンシー(利用者等)に開示することにより、ライセンシーの保護を図る制度。この制度は平成９年７月より（財）ソフトウェア情報センター（SOFTIC）が運営している。

オープン・ソース・サポート（OSS[13]）の中で、開発者やコミュニティがしっかりしていて、バージョン管理などが行われている場合は問題が少ない。しかし、オープン・ソース・サーポート・サービスを提供する会社が保守停止する時のことも考慮しておく必要がある。

2.7.4 変更管理の重要性

第一版の「ソフトウェア開発委託基本モデル契約書」第37条に変更管理手続きが記述されており、この手続きによってのみ変更が出来ると規定されている。手続きとは、「変更提案書」に基づき、「変更管理書」を交付し、「連絡協議会」で可否を審議するとなっている。

中堅･中小企業においても、これらの手続きを踏むことが望ましいが、ユーザ･ベンダの体制上や該当アプリケーションパッケージの重要度等の問題で実行困難なときは、別途、簡易手順を事前に取り決めておく必要がある。安易な変更管理は、品質･スケジュール･費用面で問題が発生する可能性が大きくなる。口頭での曖昧な合意は避け、書面による合意が必須となる。

2.7.5 リリース管理の重要性

リリース管理プロセスは「情報技術－サービスマネジメント」（JIS Q 20000）で規定されている。目的は「リリースにおける一つ以上の変更を、稼働環境に配送し、配布し、かつ、追跡するため」としている。また、リリース方針[14]を決め、手順に従って検証、受入れ、文書化、リリース、事後の評価、などを取り決めることが重要と規定している。

本番環境に近いテスト環境で十分な受入れテストを実施し、リスクを最小限にして本番環境に移行させるのが重要となる。しかし、リスクを最小限にするためには、テスト期間やそれなりのコストが必要となる。テスト期間が十分にとれない緊急性のある保守の場合や、本番環境に近いテスト環境がない場合などは、テストが不十分になる可能性がある。これらの時の対応方法やリスクなどを、ユーザ･ベンダ間で事前協議しておく必要がある。

また、リリース直前のバックアップや障害が発生したときの対処方法なども含めたリリース管理方法を双方で確認しておく必要がある。

2.7.6 サポート期間

ハードウェアと同じく、アプリケーション･パッケージソフトにもサポート期間が設定されている場合がある。この期間を超えて利用するためには、バージョンアップやデータ移行作業が発生する場合がある。システム基盤の期間管理と同じく、アプリケーション･パッケージソフトのサポート期間の把握も重要となるが、メーカー

---

[13] Open Source Software の略。ソースコードが公開されているソフトウェアのこと。代表的なものとして、Linux や Apache などがある。

[14] リリース方針：頻度及び種類、役割及び権限、識別及び説明、検証及び受入れ、等

側がバージョンアップするまでなど、期日が明確でないケースも多い。突然のサポート打ち切り通告も存在するため、利用者側の立場に立ったサポート期間の設定が望まれる。

2.8 繰り返し型開発、アジャイル開発の場合

共通フレーム２００７では開発モデルに依存していない。繰り返し型開発モデルやアジャイル型開発モデルは反復型開発モデルに含まれ、ウォーターフォール型開発モデルと区別される。それぞれの開発モデルで開発されたソフトウェアを保守・運用する場合も、開発モデルの特性によって、保守性・運用面で多少の違いがあると考える。

	ウォータフォール型	反復型
開発の最終プロセス	検収（受入れ）	検収（受入れ）
開発期間	長い	短い
保守の発生頻度	少ない	多い
システムの規模	大規模向き	小規模向き

反復型開発モデルの特性として、開発期間の短サイクル化と機能向上のための開発が繰り返されるのが前提となっている。したがって、保守・運用面でも、短サイクル化に対応しなければならない。

2.9 ＡＳＰ･ＳａａＳモデル

2.9.1 通常運用時の保守運用

ソフトウェア･サービスを提供するモデルであるため、システム基盤の内訳（ＯＳやＤＢＭＳの種類など）を、ユーザは詳しく知る必要がない。サービス機能やＳＬＡがどのように実現されるのかを確認する程度にとどまる。保守プロセスはＳａａＳベンダが責任をもって行うため、ユーザは管理コストの低減につながる。

しかし新しいモデルとしてＳａａＳプラットフォームを利用して、業務アプリケーションを構築する場合は、一般の開発手法と同じく、ＳａａＳ用言語[15]での開発となる。

2.9.2 ＳａａＳベンダの選定（保守･運用時）

ＳａａＳベンダの選択基準は、企画･開発プロセスでのチェック項目の他に、保守･運用プロセス面からのチェック項目を示した。

表 9 ＳａａＳベンダ選定時のチェックリスト（保守･運用時）

チェック項目	説明
運用状況の通知機能は？	いつでも閲覧できるか？（平均応答時間、稼動実績、トランザクション処理量、など）
問題発生時の対応は？	問題追跡性の確保、原因追及の手順は？
障害に関する情報公開は？	必要と認められるものは公開

[15] ＳａａＳプラットフォームに特化した言語

メンテナンス通知のタイミングは？	十分な期間をもって事前通知されるか？
定期メンテナンスのタイミングは？	サイクル、時間帯、時間、など
データ保全（保全期間、バックアップ）	いつまで保全されているか？（3年間、など）
データ･ダウンロード機能	レイアウト、項目、などが公開されているか？
改良保守･訂正保守の手順	一般的には公開していない
保険制度に加入しているか？	コンピュータ総合保険、など
内部監査実施状況	どのように確認するか？

2.9.3 内部監査実施状況

利用者はSaaS事業者の内部統制の整備状況をチェックする必要がある。しかし、個々の利用者がSaaS事業者に立ち入り調査することは現実的ではない。第三者による監査報告書で代用することが考えられる。委託業務に関する監査基準には、SAS70[16]や日本版SAS70[17]がある。またSaaS事業者が、ITILの導入や、ISMS、ISO／IEC20000の認証を受けているか、また監査報告書が存在し、利用者から閲覧できる仕組みがあることが望まれる。

2.10 保守タイプと瑕疵との関連

「JIS X 0161 ソフトウェア保守」では、ソフトウェア保守を大きく二つに分類（訂正保守と改良保守）している（表 2 参照）。また保守は修正依頼（Modification Request）[18]から発生すると定義している。しかし、瑕疵担保との関連には言及していない。

保守タイプごとに、修正依頼の起因をユーザとベンダ、第三者に分類し、瑕疵かの判定を示したのが表 10 である。訂正保守時の修正依頼が瑕疵担保期間中に発生し、かつその起因（発生原因元）がベンダのときは瑕疵としているが、改良保守のときは瑕疵ではないとした。

第三者が起因するものとして、システム基盤のバージョンアップ（OSやドライバーなど）に対応するための保守や、セキュリティホール対策などが考えられる。第三者が起因する修正依頼は、契約書などで事前確認が必要と考える。

表 10 保守タイプと瑕疵との関連図

保守分類 / 保守のタイプ		修正依頼の起因		
		ユーザ	ベンダ	第三者
訂正保守				
	是正保守	×	○	△
	予防保守	×	○	△
改良保守				
	適応保守	×	×	×
	完全化保守	×	×	×

○：瑕疵である、×：瑕疵ではない、△：契約によって異なる

16 SAS70(Statement on Auditing Standards) 米国公認会計士協会（AICPA）の監査基準委員会によって定められた監査基準書の第70号

17 日本公認会計士協会が2000年に策定した「監査基準委員会報告書第18号（委託業務に係る内部統制の有効性の評価）」

18 保守対象となるソフトウェア製品への変更提案を識別するために使われる総称用語（JIS X 0161）

現実には起因（発生原因元）が特定できない場合が発生する。これは上流工程（企画・要件定義・開発プロセス）での品質に起因する場合が多い。契約書やドキュメント（ソフトウェアカタログ、提案書、要件定義書や設計書、など）に記述されている機能や性能が、実現されていない時は、「是正保守」となり、起因がベンダであるため、瑕疵と考えられる。

契約書やドキュメントに明示されてないときや、曖昧さがあるときに瑕疵かの特定が困難となる。解決は一般的に話し合いで行われることが多く、交渉のための多大な工数や損失が発生する場合がある。

2.10.1 脆弱性対策と瑕疵担保責任の区別

セキュリティ対策などは「予防保守」に分類され、瑕疵ではない場合が多い。事後のトラブルを防止するためにも、脆弱性対策と瑕疵担保責任の区別の明確化が必要となる。[19]

2.10.2 瑕疵調査費用の取扱い

瑕疵担保期間中の瑕疵調査費用はベンダ側負担で行うのが一般的である。しかしアプリケーション保守契約が締結されていない場合で、かつ調査結果が瑕疵でなかったとき、調査費用の請求が発生する場合がある。特に多額の調査費用を要したときに表面化する。

トラブルを未然に防ぐためにも、事前に取扱いを協議しておくことが望まれる。

2.10.3 事前確認の重要性

トラブルを未然に防ぐためには、ユーザ・ベンダ双方が確認時の注意する項目を列挙した。（表 11 参照） ユーザが正しく判断できないときは、第三者機関[20]の利用も検討する必要がある。

表 11 確認時の注意事項

ユーザが注意すること	・曖昧な要求の排除 ・ユーザ内での同意を得る（TOPと現場、部署間、など） ・ベンダ任せにしない ・第三者機関の利用も検討 ・自己責任による文書チェック ・運用テスト、受入れテストの充実、など
ベンダが注意すること	・確認文書はより詳細に具体的に、分かり易く、誤解のない文書の作成 ・ユーザの業界特性を加味した内容 ・利害関係者に説明し確認を得る ・口答を排除し文書で確認 ・目標品質の確保、など

19 「SI 事業者における脆弱性関連情報取扱に関する 体制と手順整備のためのガイダンス」2005 年 8 月 JISA JEITA

20 ユーザとベンダとの利害関係を有しない第三者機関が、システムの要求品質が保たれているかを監視する。

3　ITサービスの現状

現在、市場には多種多様な IT サービスが存在する。また、その IT サービスの契約形態も多種多様となっている。

3.1　IT サービスの提供方法の現状

市場で IT サービスはさまざまな形で提供されているものを分類しまとめたのを「ITサービス提供形態」で表示している。(表 12 参照)　一般的には、IT サービスの特性や保守･運用会社が採用するビジネスモデルにより、複数の組み合わせで提供される場合が多い。

また技術者を、特定の IT サービスに専任化 (技術者の氏名を特定) させるサービスの提供形態も存在する。(表 13 参照)

表 12　IT サービス提供形態 (保守･運用)

常駐型	保守運用会社の技術者をユーザーに常駐させてITサービスを提供する。
待機型	技術者は保守運用会社に待機しており、必要に応じてユーザーに訪問する。訪問型との違いは、特定の技術者がほぼ１００％当該契約に占有される。
訪問型	イベント発生時 (障害発生や定期点検、監視など) ごとに技術者がユーザーに訪問しITサービスを提供する。
リモート型	イベント発生時 (障害または定期点検、監視、ユーザーの理由など) に、ユーザーの設置環境にリモートで接続しITサービス (リモートメンテやリモート監視など) を提供する。
センドバック型／持込型	ユーザーが故障したハードウェアを保守会社に宅急便などで送り、修理後返送される保守サービス
電話FAX型	障害の対処方法や操作方法などを電話やFAX、E-Mailで回答するITサービス。コールセンターは、このサービス提供形態をとっている。
情報提供型	障害情報や操作･運用方法、パッチ情報などをＷＥＢやメールなどで提供したり、ダウンロードできるITサービス。

運用サービス (帳票デリバリーや計算センター利用など) は除く

表 13　技術者専任･非専任

専任型	ITサービスを提供する技術者の氏名が、事前にユーザーとの間で決められている。イベント発生時は特殊な事情がない限り、その技術者が対応する。特定技術者が複数名割り当てられる場合もある。
非専任型	イベントが発生するたびに別の技術者が割り当てされる場合がある。一般的に保守運用会社ではグループで対応するケースが多い。

3.2　地域企業の求める IT サービス

「地域企業の求める IT サービスの利活用[21]」の調査結果を参照すると、多種多様な IT サービスが存在する。大きくは開発系の IT サービスと保守･運用系の IT サービスに大別される。

表 14　ITサービス業者から受けているサービス (保守･運用系)

[21] 「地域企業の求める IT サービスの利活用と費用対効果調査研究」（社）日本コンピュータシステム販売店協会（JCSSA）平成１９年２月

ITサービス	全体	地域別	
		大都市	地方都市
サンプル数	148	96	51
アプリケーション保守サービス	49%	57%	35%
修理復旧サービス	49%	48%	51%
統合保守サービス	42%	38%	49%
運用支援サービス	38%	42%	31%
メールサーバー管理サービス	35%	38%	31%

保守･運用系の IT サービスの中で最も多く利用されているのは「アプリケーション保守サービス」である。ついで「修理復旧サービス」、「統合保守サービス」「運用支援サービス」と続いている。(表 14 参照)

今回のモデルは、このアンケート調査の内容を踏まえて上位から選別した。しかし、フルアウトソーシングに近いITサービス(例:統合保守サービス)は、第一版の範囲と重複する可能性が高いため、より単純化(サービス範囲が限定)されたITサービスをサンプルモデルとした。(表 15 参照)

表 15 ITサービスのモデル(保守･運用系サンプル)

サービス名称	区分	主なサービス内容	節番
ハードウェア保守	保守	サーバの保守、復旧支援は含まない	4.6
アプリケーション保守	保守	パッケージの保守	4.7
セキュリティ監視	運用支援	ファイアウォールを主体とした監視	4.8
サーバ運用支援	運用支援	障害の自動検知を主体とした監視	4.9
SaaSモデル	SaaS		4.10

節番:サービ内容を説明している本文の節の番号

4 ユーザ･ベンダの共有すべきガイドライン

ベンダが提供しているＩＴサービスは多種多様であり、ユーザとベンダが事前に取り決めるべき事項を一様に定義することは現実的ではない。そこで、当WGは、情報システムの運用保守に関する国際標準となった JIS Q 20000-1:2007（ISO/IEC 20000-1:2005）をベースに、ユーザ・ベンダが共に参照し活用できるガイドラインを提供することを目指す。

4.1 JIS Q 20000 運用保守ガイドライン

当WGでは、JISQ20000-1:2007 が要求する管理プロセスに則って、各プロセスで管理することが想定される項目について検討した。例えば、インシデント管理プロセスにおいて、そもそもインシデントとして取り扱う事象にユーザ・ベンダ間に差異があっては、適切なインシデント管理は実現されない。したがって、まず、ユーザ・ベンダは、当該ＩＴサービスにおけるインシデント及び運用面について取り決めをする必要がある。

4.2 JIS Q 20000 とITサービスの関係

JIS Q 20000-1:2007 で要求される 13 個の管理プロセスから、ＩＴサービスにおいて管理すべきと考えられる主要な項目について抽出した。(表 16 参照) ユ

ーザ・ベンダは、適用する管理プロセスを選択し、そのプロセスにおいて管理していく項目を相互に協議することになる。

また、ＳＬＡ項目も、各種ＩＴサービスの特性やユーザ・ベンダ間の取り決めで異なってくるものと考える。ここでは、代表的なものをサンプルとして列挙した。尚、L1～L4 は他章の管理レベルと同様の設定とする。

表 16　JIS Q 20000 運用保守ガイドライン

JIS Q 20000-1:2007			項目の説明	L1	L2	L3	L4
6	サービス提供プロセス						
	6.1	サービスレベル管理					
		SLAの締結	提供サービスに対する品質を保証するためのSLAを締結しているか	規定なし	部分的に締結	提供サービス毎に締結	
		SLAの監視	SLAの遵守状況を確認するために監視されているか	規定なし	部分的に監視	提供サービス毎に監視	
		SLAの見直し	SLAが引続き妥当かを判断するための見直しが実施されているか	規定なし	部分的に見直し	定期的に見直し	
	6.2	サービスの報告					
		報告会の実施	SLAの遵守状況を確認するための報告会は実施されているか	規定なし	場当たり的に実施	定期的に実施	
		報告内容の定義	報告される内容は定義されているか	規定なし	場当たり的	定義済み	
	6.3	サービス継続及び可用性の管理					
		要求事項の定義	サービス継続及び可用性を担保するための要求事項が定義されているか	規定なし	部分的に定義	提供サービス毎に定義	
		計画策定	サービス継続及び可用性を担保するための計画が策定されているか	規定なし	部分的に策定	統合された計画が策定	
		計画のレビュー	計画の妥当性を確認するためのレビューが実施されているか	規定なし	場当たり的に実施	定期的に実施	
		計画の試験	計画の実効性を確認するための試験が実施されているか	規定なし	場当たり的に実施	定期的に実施	
	6.4	サービスの予算業務及び会計業務					
		予算計画の策定	SLAを維持するために必要となるリソースの予算計画を策定しているか	規定なし	部分的に策定	提供サービス毎に策定	
		予実の管理	策定された予算計画の執行状況を確認するために予実を管理しているか	規定なし	部分的に管理	定期的に管理	
	6.5	容量･能力管理					
		監視対象の定義	SLAを遵守するために監視すべき対象を定義しているか	規定なし	部分的に定義	提供サービス毎に定義	
		容量･能力の監視	SLAを遵守するために定義された対象を監視しているか	規定なし	場当り的に監視	定義された対象を監視	
		需要管理	SLAを遵守するために監視すべき対象の需要を管理しているか	規定なし	部分的に管理	定義された対象を管理	
	6.6	セキュリティ管理					
		基本方針の定義	セキュリティを管理するための基本方針が定義されているか	規定なし	部分的に策定	統一的な基本方針が定義	
		リスクアセスメント	守るべき情報資産に対してリスクアセスメントが実施されているか	規定なし	部分的に実施	全社的に実施	
		変更による評価	変更要求に関わるセキュリティ障害を防止するために変更を評価している	規定なし	部分的に評価	変更諮問会議で変更毎に評価	
7	関係プロセス						
	7.2	顧客関係管理					
		サービスレビュー会議	サービスを改善するためのサービスレビュー会議（対顧客）を実施している	規定なし	不定期に実施	定期的に実施	
		苦情処理	顧客に対して苦情を処理するための方法を定義しているか	規定なし	担当者により実施	責任者により実施	
		顧客満足度の測定	提供サービスに対する顧客満足を把握するための測定を実施しているか	規定なし	担当者により実施	責任者により実施	
	7.3	供給者管理					
		契約管理	提供するサービスの品質を担保するため供給者と契約を締結しているか	規定なし	一部の供給者と締結	関係する全ての供給者と締結	
		監査	供給者との契約が遵守されているかを監査しているか	規定なし	一部の供給者に実施	関係する全ての供給者に実施	
8	解決プロセス						
	8.2	インシデント管理					
		インシデントの定義	記録すべきインシデント（サービス要求含む）が定義されているか	規定なし	インシデントのみ定義	サービス要求まで定義	
		インシデントの検知と記録	定義された全てのインシデントが検知・記録されているか	規定なし	全て手動	一部自動	全て自動
		インシデントの分類	対応の優先順位を判断するために分類しているか	規定なし	事業インパクトで分類	事業インパクト×緊急度で分類	
		インシデントのライフサイクル管理	インシデントはライフサイクルに沿って管理されているか	規定なし	クローズのみ管理	複数のステータスで管理	
	8.3	問題管理					
		問題コントロール	問題の根本原因を追究するための手順が定義されているか	規定なし	場当り的な作業	手順が定義されている	
		エラーコントロール	既知のエラーを取り除くための手順が定義されているか	規定なし	場当り的な作業	手順が定義されている	
		既知のエラーデータベース	既知になったエラー情報を共有するための仕組みはあるか	規定なし	部分的な実施	常に参照可能な状態で管理	
		傾向分析	エラーの傾向を把握するために問題を分析しているか	規定なし	場当り的な作業	定期的に実施	
		プロアクティブな活動	問題を事前予防的に発生させないための仕組みはあるか	規定なし	場当り的な作業	予防処置あり	
9	統合的制御プロセス						
	9.1	構成管理					
		構成識別	管理すべき構成品目が明確にされているか	規定なし	部分的な資産台帳あり	方針が定義されている	
		構成コントロール	構成品目を適切に管理するための手順が定義されているか	規定なし	台帳のみ作成	手順が定義されている	
		履歴管理	構成品目に対する変更を追跡できるよう履歴管理しているか	規定なし	手動管理	一部自動	自動管理
		構成監査	構成品目の完全性を維持するために監査しているか	規定なし	年次監査	部分的な資産棚卸し	月次監査
	9.2	変更管理					
		変更要求の記録	全ての変更要求は証跡を残すために記録されているか	規定なし	部分的な記録がある	全て記録されている	
		変更要求の分類	対応の優先順位を判断するために分類しているか	規定なし	部分的な分類	事業インパクト×緊急度×難易度で分類	
		変更要求の評価	変更によるリスクを低減するために変更要求を評価しているか	規定なし	部分的な評価	変更諮問会議で評価	
		切戻し計画	変更の失敗による障害を低減するために切戻し計画を作成しているか	規定なし	部分的な作成	変更諮問会議で評価	
		傾向分析	変更の傾向を把握するために変更要求を分析しているか	規定なし	部分的な実施	定期的に実施	
		変更要求のレビュー	変更による効果を測定するために変更要求をレビューしているか	規定なし	部分的なレビュー	変更諮問会議でレビュー	
10	リリースプロセス						
	10.1	リリース管理プロセス					
		リリース方針	本番環境を維持するためのリリース方針は定義されているか	規定なし	場当り的な作業	方針が定義されている	
		リリース計画	計画的なリリースを実現するための計画書は作成されているか	規定なし	部分的に作成	リリース毎に計画書が作成されている	
		リリース手順	計画的なリリースを実現するための手順書は作成されているか	規定なし	部分的に作成	リリース毎に手順書が作成されている	
		コミュニケーション	リリース作業に伴う混乱を避けるため、事前連絡を実施しているか	規定なし	部分的に連絡	リリース毎に関係者に連絡している	

※ＳＬＡ（service level agreement）：サービスレベル合意書
※当ガイドラインへの準拠が、JISQ20000-1:2007 の認証取得を保証するものではない。

4.3　サービスの内容に関する項目

ＩＴサービスの内容を特定するにあたり、代表的な項目を下記に列挙した。

項目	説明
サービス名称	
サービス内容	サービス内容を詳細に記載
対象外	対象外の条件や、注意制限事項などを記載
対象環境	システム基盤（ハード、OS、など）、環境
契約年月日	契約の日付
契約期間	サービス開始年月日及び終了年月日
更新･解除条件	自動更新などの更新条件、解約条件、など
料金	月額や年額、など
受付方法及び時間	平日、土日、祝祭日の対応
保守時間	実際の保守作業を行う時間帯
定例協議会	開催の有無やサイクルなど

秘密保持	
再委任	再委任の条件
ITサービス提供形態	常駐、訪問、リモート、電話／FAX、情報提供、など
技術者専任･非専任	技術者を氏名で特定、非特定

4.4 運用面に関する項目

ユーザ･ベンダ双方の運用体制や運用フローを事前に取り決めされていることが望まれる。

ベンダー側	
会社名･部署名	(再委託先名も含む)
責任者	営業･技術者･氏名･連絡先
担当者名	営業･技術者･氏名･連絡先
問い合わせ先	電話/FAX番号、URL、メールアドレス等を記す。サービス提供部署のほか、一般問合せ先がある場合、その連絡先も記す。
役割分担	サポート範囲、責任範囲、など
緊急連絡先	
ユーザ側	
部署名	
責任者･連絡先	
担当者･連絡先	サービス連絡先と一般連絡先が異なる場合、両方を記す。
役割分担	作業範囲、責任範囲、など
緊急連絡先	

4.5 SLA･SLMに関する項目

各種ITサービスごとにSLAやSLMの設定がされることが望まれる。また、アプリケーションパッケージの特性や重要性などにより、ユーザ･ベンダ間の協議の上、SLAのレベルが決定される。下記の項目は、SLA設定時に必要と思われる項目を列挙した。

項目	説明
サービスレベル項目	SLAの項目名
内容	SLAの内容を説明
測定方法	測定の方法を説明
測定単位	分･時･日･週･月･年
目標/保証	目標･保証
値	

尚、以降の章において、具体的なＩＴサービスを対象としたサービスレベル項目をサンプルとして示していく。

4.6 ハードウェア保守

4.6.1 範囲の明確化

ハードウェア保守を契約する場合、契約作業と契約外作業を明確にする必要がある。また、訂正保守（是正・予防）・改良保守（適応・完全化）のどれを含むのかも明確にする必要がある。

ハードウェア保守サービスには、出張修理保守（定期点検付、定期点検なし）、引き取り保守、持込保守がある。また、障害復旧にあたり、データ

復旧、保守対象外部品の交換、データバックアップ、交換したディスク内のデータの消去の各サービスが別メニューとなる場合が一般的であるが、これらのサービスがひとつのサービスメニューとなっている場合もある。そのため、サービスの範囲を明確化する必要がある。

項目	説明
サービス提供形態	出張対応、引き取り対応、持込対応、定期点検の可否を確認
対応範囲	データ復旧、保守対象外部品、データバックアップ、ディスク内のデータの取り扱いなど
期間管理	契約期間、製品寿命、保障期間、部品提供期間
事前停止	定期点検時の計画停止時間、間隔
契約外作業	契約対応範囲外の作業内容と実施した場合の料金
報告	対応実績の報告の有無、報告内容、定例会開催の有無など

4.6.2 SLA･SLM

サービスレベル項目	内容	測定単位	目標保証	レベル1	レベル2	レベル3	レベル4
サービス提供時間	電話受付時間	時間	目標	営業時間内		時間外	365日 24H
サービス提供時間	出動時間	時間	目標	翌日	当日	4H	2H
サービス提供時間	復旧時間	時間	目標	翌日	当日	契約毎個別	
定期点検	実施回数	回数	保証	なし	1回/年	2回/年	3回/年

4.7 アプリケーション保守サービス（パッケージ）

4.7.1 範囲の明確化

パッケージのアプリケーション保守を契約する場合、パッケージ本体とカスタマイズ部分を明確にする必要がある。また、訂正保守（是正･予防）･改良保守（適応･完全化）のどれを含むのか、問題解決プロセスを組み込んでいるのかも明確にする必要がある。

アプリケーション保守サービスには、コールセンター、ライセンス保守、障害対応、カスタマイズ保守、導入教育･指導の各サービスに分かれる場合がある。これらが一つのサービスメニューとなっている場合や、分かれる場合、含まれていないサービスなどが考えられる。いずれにしても、サービスに関しての範囲の明確化が必要となる。

［コールセンター･サービス］

項目	説明
カスタマイズ分類	･パッケージ本体部分の対応か、カスタマイズ部分も含めた対応かを確認
問合せの範囲	機能、操作、不具合、など
ITサービス提供形態	電話FAX型、情報提供型、リモート型
技術者専任区分	専任（技術者氏名特定）対応、 非専任（技術者氏名非特定）対応かの確認

［ライセンス保守サービス］

項目	説明
保守種別（JIS X 0161）	含まれる保守タイプ（是正、予防、適応、完全化）の確認
各種権利の確認	著作権、利用許諾権利、複製権、再許諾権など
バージョンアップ関連	バージョンアップの有無、範囲、サイクル、方法、時間帯、など
法律改正対応	予測可能な法律改正（給与所得税率、消費税率などの変更）⇒一般的には含めている場合が多い。 予測不可能な法律改正（新会社法、など）⇒一般的には含めない場合が多い。
問合せ窓口	コールセンター、部署、電話番号、FAX 番号、など
トラブル発生時	窓口、ＢＵＧ発生時などの対応方法、など

［障害対応サービス］

項目	説明
保守種別（JIS X 0161）	含まれる保守タイプ（是正、予防、適応、完全化）の確認
サービスマネージメント（JIS Q 20000-1、-2）	解決プロセス（インシデント管理、問題管理）
対応範囲	原因調査、原因排除、再インストール（プログラム）、再設定（プログラム）、データリストア（バックアップデータがある場合）
提供形態	常駐型、待機型、訪問型、リモート型、電話ＦＡＸ型、情報提供型

［カスタマイズ保守サービス］（別途、保守開発契約を締結する場合もある）

項目	説明
保守種別（JIS X 0161）	含まれる保守タイプ（是正、予防、適応、完全化）の確認
サービスマネージメント（JIS Q 20000-1、-2）	プロセスは何を含むのか？（サービス提供、関係、解決、統合的制御、リリース）
カスタマイズの範囲	ユーザ要件変更時のカスタマイズの対応方法。 一定条件（人月で設定する場合、など）を設定
カスタマイズの対応	モディファイかアドオンまで対応するのかなど
新しくカスタマイズした成果物の権利の確認	著作権、利用許諾権利、複製権、再許諾権など
ITサービス提供形態	常駐型、待機型、訪問型、リモート型、電話ＦＡＸ型、情報提供型
技術者専任区分	専任、非専任
テスト環境	個別ユーザ環境、一般環境
変更管理プロセス	方針、手順、緊急時、など
リリース管理プロセス	リリース方針、手順、など
コールセンター対応	カスタマイズ部分の対応は？　個別対応？
教育･指導	訪問型、電話･FAX 型、集合教育･個別教育
トラブル発生時	窓口、対応方法、など
精算方法	途中解約や、設定回数未達時の対応、など

［導入教育･指導サービス］

項目	説明
指導タイミング及び回数、場所、規模	初期指導または再指導、個別または集合指導、E-learning、場所、対象人員、レベル、など
カリキュラムの範囲	カスタマイズを含めた教育、または基本部分のみ、など
ITサービス提供形態	常駐型、待機型、訪問型、リモート型、電話ＦＡＸ型、情報提供型
技術者専任区分	専任、非専任
コールセンター	有無
トラブル発生時	窓口、対応方法、など

4.7.2　SLA･SLM

［コールセンター･サービス］（例）

JISQ20000との対応	サービスレベル項目	内容	測定方法	測定単位	目標/保証	レベル1	レベル2	レベル3	レベル4
8.2 インシデント管理	サービス提供時間	電話受付時間	--	時間帯	保証	営業時間内		時間外特約	契約毎個別
8.2 インシデント管理	即応率	電話が鳴ってから基準時間内に応答した率	月	%	目標	規定無し	80%以上	90%以上	95%以上
8.2 インシデント管理	放棄率	着信電話に出られなかった率	月	%	目標	規定無し	20%未満	10%未満	5%未満
8.2 インシデント管理	電話ビジー率	電話がビジー(話中)でつながらなかった率	月	%	目標	規定無し	20%未満	10%未満	5%未満
8.2 インシデント管理	コールバック率	即答できずに折り返しをした率	月	%	目標	規定無し	20%未満	10%未満	5%未満

［ライセンス保守サービス］（例）

JISQ20000との対応	サービスレベル項目	内容	測定方法	測定単位	目標/保証	レベル1	レベル2	レベル3	レベル4
10.1 リリース管理	バージョンアップサイクル	バージョンUP回数を規定	年		目標	未定	1回／数年	1回／年	数回／年
10.1 リリース管理	バージョンUP範囲	バージョンUP対応の範囲			保証	未対応	特定バージョンのみ対応		全てのバージョン
10.1 リリース管理	媒体要求	バージョンUP媒体の要求方法			目標	未対応	ユーザのリクエスト		自動
10.1 リリース管理	提供方法	媒体の提供方法			目標	未対応	郵送	リアルタイム(ダウンロード時)	ダウンロードまたは郵送
10.1 リリース管理	リードタイム	媒体要求が発生してから、ユーザの手元に届くまでの時間	日	時間	目標	未定	数日		

［障害対応サービス］（例）

JISQ20000との対応	サービスレベル項目	内容	測定方法	測定単位	目標/保証	レベル1	レベル2	レベル3	レベル4
8.2 インシデント管理	応答時間	着手有無の決定を回答する時間	月	時間	目標	規定無し	翌日	半日以内	1時間以内
8.2 インシデント管理	復旧時間	障害が発生してから復旧するまでの平均時間	月	時間	目標	規定無し	1週間以内	1日以内	12時間以内

［カスタマイズ保守サービス］（例）

JISQ20000との対応	サービスレベル項目	内容	測定方法	測定単位	目標/保証	レベル1	レベル2	レベル3	レベル4
9.2 変更管理	応答時間	着手有無の決定を回答する時間	月	日	目標	規定無し	1月以内	1週間以内	翌日
9.2 変更管理	着手時間(緊急保守)	作業が着手されるまでの時間	月	日	目標	規定無し	数日	翌日	当日
9.2 変更管理	着手時間(改良保守)	作業が着手されるまでの時間	月	日	目標	規定無し	2ヶ月以内	1ヶ月以内	1週間以内
9.2 変更管理	作業ボリューム	1回当りの最大作業工数	月	日	保証	個別契約で設定			

9.2 変更管理	作業回数	単位期間のリクエスト最大回数	月	日	保証	個別契約で設定

［導入教育･指導サービス］（例）

JISQ20000 との対応	サービス レベル項目	内容	測定 方法	測定 単位	目標 /保証	レベル 1	レベル 2	レベル 3	レベル 4
6.5 能力管理	実施回数					個別契約で設定			
6.5 能力管理	実施間隔					個別契約で設定			
6.5 能力管理	実施場所					個別契約で設定			
6.5 能力管理	対象人数					個別契約で設定			
6.5 能力管理	対象レベル					個別契約で設定			

4.8 運用支援系（セキュリティ監視サービス）

4.8.1 範囲の明確化

セキュリティ監視サービスで最も一般的である、ファイアウォールの管理を代行するファイアウォールマネージメントサービスをサンプルとして例示する。セキュリティ関連のサービスとして、IDS[22]や IPS[23]を利用した不正侵入検知サービス、ウイルス対策やセキュリティパッチを代行するサービス等が考えられるが、適宜サービスレベル項目を定め、予めユーザと合意を取ることが望ましい。

別途、ユーザで不正侵入等緊急を要するセキュリティインシデントが発生した場合に備え、緊急対応サービス(エマージェンシーレスポンスサービス)を提供することが望ましい。

4.8.2 SLA･SLM

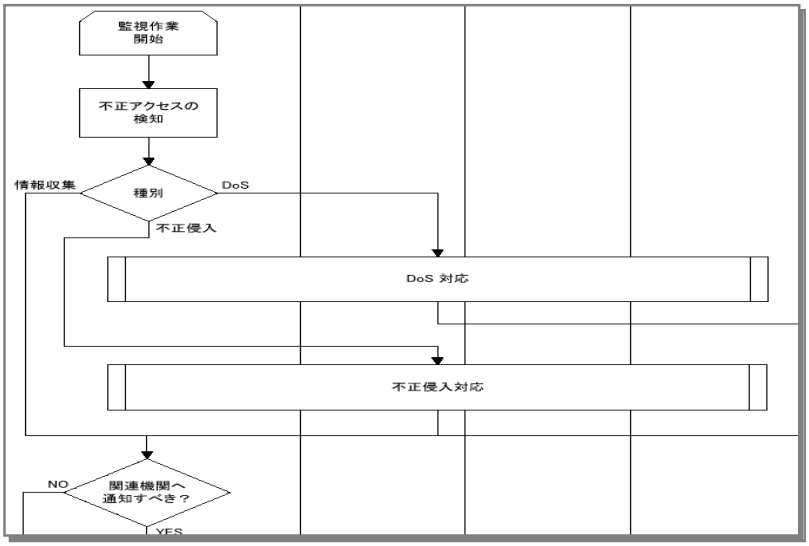
［セキュリティ監視サービス：ファイアウォールマネージメントサービス］（例）

JISQ20000 との対応	サービスレベル項目	内容	測定方法	測定単位	目標 /保証	レベル 1	レベル 3
6.5 容量･能力管理	稼動監視	リモートから定期的に稼動を監視する	稼動停止検知から通報までの時間	分	目標	60 分以内	10 分以内
6.5 容量･能力管理	不正アクセス検知報告	不正アクセスを常時監視し異常発生時に報告する	ファイアウォールがブロックしたしたアクセスを検知する	分	保証	60 分以内	10 分以内
6.6 セキュリティ管理	ログアーカイブ	アクセスログを保管する			保証	(未対応)	過去 3 ヶ月分
6.2 サービスの報告	ログ分析	ログレポートを提出する			保証	(未対応)	翌日
9.2 変更管理	ポリシー変更	ユーザからのポリシー設定変更依頼に対応する	ユーザの変更要求から作業完了までの時間	日	保証	1 週間	翌日
8.2 インシデント管理	ハードウェア保守	機器故障時の交換作業を行う	故障検知から交換までの時間	時	目標	翌営業日	2 時間
6.2 サービスの報告	稼動状況報告	稼動状況について報告する	月次で稼動状況のサマリ報告を行う	月	保証	(未対応)	翌月月初 10 営業日以内

[22]不正侵入検知システム(Intrusion Detection System)：第三者からの攻撃や不正アクセスをリアルタイムで検知するシステム

[23]不正侵入防御システム(Intrusion Prevention System)：第三者からの攻撃や不正アクセスからリアルタイムで検知・遮断し、公開サーバ等を防御するシステム

[運用フロー図:ファイアウォールマネージメントサービス(一部抜粋)]



ファイアウォールマネージメントサービスの運用フロー図(一部抜粋)を例示する。サービス提供に当たっては、運用フローに基づいた対応を確実にするために、予め要員への訓練を実施することが望まれる。

4.9 運用支援系(サーバ運用支援サービス)

4.9.1 範囲の明確化

システム運用支援サービスとして、サーバ運用支援サービスを例示する。近年、エントリサーバの分野にも障害の自動検知機能等、可用性を向上する機能が実装されてきた。サービスベンダもこのような機能を積極的に活用し、ユーザシステムの可用性を高めることや保守効率の向上を図ることが望まれる。

また、システム導入時点において、処理する業務の重要度に応じて、ハードウェア部品の二重化、システムの二重化等、可用性を高める手段を提案することが望ましい。

4.9.2 SLA・SLM

[サーバ運用支援サービス](例)

JISQ20000との対応	サービスレベル項目	内容	測定方法	測定単位	目標/保証	レベル1	レベル3
6.5 容量・能力管理	稼動監視	リモートから定期的に稼動を監視する	稼動停止検知から通報までの時間	分	目標	60分以内	10分以内
6.5 容量・能力管理	障害自動通報	ハードウェア障害を自動検知し、メールや snmp プロトコルを利用して通報する	ベンダ側のサポート部署で、通報メール、snmpトラップ受信を検知するまでの時間	分	目標	60分以内	10分以内
6.5 容量・能力管理	システムリソース監視	ディスク空き容量 CPU 負荷率を監視し、閾値を超えた場合、メールや snmp プロトコルを利用して通報する	ベンダ側のサポート部署で、通報メール、snmpトラップ受信を検知するまでの時間	分	目標	(未対応)	10分以内

8.2 インシデント管理	ハードウェア障害復旧	ハードウェアの故障部位を特定し、復旧する	ユーザからの連絡や監視システムからの通報時点から、復旧するまでの時間	時	目標	24 時間以内(ベンダ側の休日は除く)	4 時間以内
8.2 インシデント管理	サーバ運用問合せ対応	OS レベルハードウェアレベルでの操作方法や設定についての問い合わせ対応を行う	メールや電話等でのユーザの問合せから回答までの時間	日	目標	翌日(ベンダ側の休日は除く)	即日(ベンダ側の休日は除く)
6.2 サービスの報告	稼動状況報告	稼動状況について定期的に報告を行う	月次で稼動状況のサマリ報告を行う	月	保証	(未対応)	翌月月初 10 営業日以内

4.10 ASP･SaaSモデル

4.10.1 範囲の明確化

ASP･SaaSモデルのITサービスを契約する場合、基本サービスとオプションサービス(カスタマイズ等を含む)を明確にする必要がある。また、ベンダとの契約を締結した段階で、提供されるサービスレベルにユーザが同意したことになるので、ユーザは、利用するITサービスを価格だけでなく、サービスレベルの項目･水準によっても判断しなければならない。

4.10.2 SLA･SLM

ここでは汎用的なサンプルを提示するに留め、詳細は総務省や経済産業省からも資料[24]が公開されているので参照されたい。

[ASP･SaaSモデルのSLA](例)

JISQ20000との対応	SLA項目	L1	L2	L3	L4
	信頼性				
6.5 容量・能力管理	稼働率	97.50%	99.00%	99.90%	99.99%
6.5 容量・能力管理	目標復旧時間(RTO)	設定なし	24時間	個別契約で設定	
6.5 容量・能力管理	目標復旧時点時間(RPO)	設定なし	24時間	個別契約で設定	
6.5 容量・能力管理	バックアップ間隔	設定なし	24時間	個別契約で設定	
6.5 容量・能力管理	冗長化	ミラーリング	ミラーリング+ホットスワップ		レプリケーション
6.5 容量・能力管理	障害監視間隔	60秒	30秒	10秒	5秒
	性能				
6.5 容量・能力管理	システム応答時間※1	設定なし	8秒	5秒	1秒
6.5 容量・能力管理	処理時間 (ﾊﾞｯﾁ、ｵﾝﾗｲﾝﾄﾗﾝｻﾞｸｼｮﾝ等)	設定なし	個別契約で設定		
6.5 容量・能力管理	域内回線帯域	個別契約で設定			
	キャパシティ				
6.5 容量・能力管理	ディスク容量	個別契約で設定			
	セキュリティ				
6.6 情報ｾｷｭﾘﾃｨ管理	不正侵入対策※2	FWのみ	FW+NIDS		FW+NIDS+HIDS
6.6 情報ｾｷｭﾘﾃｨ管理	ウイルス対策※3	ホストのみ	GW+ホスト		GW+ﾎｽﾄ+ﾏﾙﾁﾍﾞﾝﾀﾞ
6.5 容量・能力管理	脆弱性診断間隔	1回／年	1回／半年	1回／3ヶ月	毎月
	サポート				
8.2 インシデント管理	受付時間	平日9:00-17:00	平日9:00-20:00	9:00-20:00×7D	24h×7D
8.2 インシデント管理	受付要員	専任者なし	一部専任者あり		完全専任者制

※1:システム応答時間は、ベンダが直接契約等でコントロールできない要因(ユーザ側のアクセス回線等)も含まれるため、SLA項目に設定する場合は、ベンダの責任範囲を明確に定義する必要がある。

※2:不正侵入対策には各種ソリューションがあるが、ここでは、FW(ﾌｧｲｱｳｫｰﾙ)+NIDS(ﾈｯﾄﾜｰｸﾍﾞｰｽの侵入検知ｼｽﾃﾑ)+HIDS(ﾎｽﾄﾍﾞｰｽの侵入検知ｼｽﾃﾑ)の組み合わせをL4の対策と想定した。

※3:ウイルス対策には各種ソリューションがあるが、ここでは、GW(ｹﾞｰﾄｳｪｲ型ｳｲﾙｽ対策)+ﾎｽﾄ(ﾎｽﾄｲﾝｽﾄｰﾙ型ｳｲﾙｽ対策)+ﾏﾙﾁﾍﾞﾝﾀﾞ(複数ベンダのウイルス対策ソリューションを併用)の組み合わせをL4の対策と想定した。

24 「ＡＳＰ・ＳａａＳの情報セキュリティ対策に関する研究会」　総務省　平成１９年１０月１７日
「ＳａａＳ向けＳＬＡガイドライン（案）」経済産業省　（独）情報処理推進機構　平成１９年１１月２１日

略語
FW：Firewall
NIDS：ﾈｯﾄﾜｰｸ型 Intrusion Detection system
HIDS：ﾎｽﾄ型 Intrusion Detection system
GW：Gateway
RTO：Recovery Time Objective
RPO：Recovery Point Objective

5 IT サービス仕様書（サンプル）

5.1 記載すべき事項

記載すべき内容は、IT サービスの種類により異なる。以下は共通に発生する項目を列挙する。

サービス名称	
サービス内容	可能な限り詳細に記述
サービス目標	SLM、SLA
注意事項	注意制限事項、対象外、例外事項、など
受付時間	受付時間、対応時間、時間外対応、など
連絡先	通常時、緊急時

5.2 「サーバ運用支援サービス」サンプル

以下に「サーバ運用支援サービス」のサービス仕様書（サンプル）を記載した。このサービス仕様書の中に書かれている内容は、あくまでもサンプルであり実際にサービス提供するためには、各ベンダのビジネスモデルとユーザ要求に合わせてさらに細かく調整し記述されるべきと考える。

サービス仕様書（サンプル）

サービス名称	サーバ運用支援サービス
サービス内容	① 電話問い合わせサービス ・ ご契約いただいているサーバに関する技術的問合せを、 フリーダイヤル、E-Mail、およびFAXにて対応させていただきます。 ② 障害切り分けサービス ・ ご契約いただいているサーバのトラブル発生時に、 電話または必要に応じて、リモートにより接続して障害の切り分けをおこないます。 ・ 監視ツールでエラーやアラートが検知された場合は、 インターネットメールにて弊社コールセンターに通報します。 ③ オンサイトサービス ・ ②の内容で障害の切り分けが解決しない場合、技術者の訪問により 障害の切り分けを行います。 （注意）障害復旧に関しては、別途契約「障害復旧支援サービス」などが必要となります。
対象サーバーおよび対象ＯＳ	＜対象ＯＳ＞ ・ Windows 2000 Server（SP4以降） ・ WindowsServer2003StandardEdition ・ WindowsServer2003R2Standard Edition、2003EnterpriseEdition ＜対象ハード環境＞　（以下のサーバ管理エージェントが必須） ・ HP Proliantシリーズ　HPマネジメントエージェント ・ NEC Express5800/100シリーズ　NEC ESMPRO/ServerAgent ・ 富士通 PRIMERGY　富士通 Systemwalker
監視・通報項目	① ハードウェア障害監視（サーバ管理エージェントによるハードウェアの監視） ② オペレーティングシステム稼動監視（CPU負荷状況、ディスク、メモリの空き容量監視） ③ アプリケーション障害監視（バックアップソフト、ウィルスソフト、BackOffice製品など）
注意事項	① 1サイト環境に限りの対応範囲といたします。 ② 障害の切り分けまでとし、復旧及びハードウェア修理またはそれらの支援は含みません。 ③ サーバとネットワークインフラ環境との障害は、原因の切り分けまでを対応とします。 ④ サーバ以外のインフラの障害対応は、範囲外となります。 ⑤ サーバパッケージで無償提供されている、以下のサービスサポートは対応範囲とします。 「WINS」、「DHCP」、「RRAS」、「IIS」、「DNS」、「Index」、「ターミナルサービス」 ⑥ ⑤以外のサービスは、対応範囲外とします。 ⑦ 以下の項目は対応範囲外とします。 ・弊社技術者が対応、設定した箇所以外のトラブルおよび技術的問い合わせ ・言語、開発、コンサルティングに関わるトラブルおよび技術的問い合わせ ⑧ ハードウェア保守契約をいただいているハード（サーバ）が対象となります。 ⑨ リモートメンテナンスする場合、事前にお客様のご了承をいただいてから 接続させていただきます。 ⑩ インターネットやお客様ネットワークに通信障害が発生した場合の通報不達 および連絡漏れに対する責任は負いかねます。 ⑪ このサービスではお客様のサーバで障害が発生した場合、障害の原因を 究明するためにお客様のイベントログファイルをいただいております。
ＳＬＡ・ＳＬＭ	別途「ＳＬＡ合意書」に記載
電話受付時間及び対応時間	月～金　9:00～18:00（日曜日・祝祭日・弊社休業日は除く） 土　9:00～12:00　13:00～17:00
オンサイト対応時間	月～金　9:00～17:00（土・日曜日・祝祭日・弊社休業日は除く） ※上記時間外の対応の場合は別途有償作業となります。
連絡先	通常時：弊社コールセンター・フリーダイヤル（電話番号などはご契約時にお知らせします。） 緊急時：弊社営業所　xx-xxxx-xxxx

6　参考資料

6.1　参考文献一覧

1. 『情報システムの信頼性向上のための取引慣行・契約に関する研究会～情報システム・モデル取引・契約書～（受託開発（一部企画を含む）、保守運用＜第1版＞』 経済産業省商務情報政策局情報処理振興課　平成19年4月13日
   http://www.meti.go.jp/policy/it_policy/keiyaku/index.html
2. 『新「システム監査基準」、「システム管理基準」』 経済産業省商務情報政策局　平成16年10月8日
   http://www.meti.go.jp/policy/it_policy/press/0005668/
3. 『情報システムの信頼性向上に関するガイドライン』 経済産業省商務情報政策局　平成18年6月15日
   http://www.meti.go.jp/press/20060615002/20060615002.html
4. 『公共 IT におけるアウトソーシングに関するガイドライン』 総務省　平成15年3月
   http://www.soumu.go.jp/denshijiti/pdf/060213_03.pdf
5. 『 JIS Q 20000-1:2007』 情報技術―サービスマネジメント―第1部：仕様
6. 『 JIS Q 20000-2:2007』 情報技術―サービスマネジメント―第2部：実践のための規範
7. 『共通フレーム2007－ SLCP-JCF2007 －』 （独）情報処理推進機構（IPA） 平成19年10月1日
8. 『JIS X 0161:2008（予定）』 ソフトウェア保守
9. 『サービスレベル契約（SLA）に関する調査報告書』 （財）ソフトウェア情報センター（SOFTIC） 平成17年3月
10. 『民間向けITシステムのSLAガイドライン＜第3版＞』 （社）電子情報技術産業協会（JEITA） 平成18年10月2日
11. 『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』 （社）電子情報技術産業協会（JEITA） 平成19年8月13日
12. 『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－ 』 （社）電子情報技術産業協会（JEITA） 平成19年3月
13. 『地域企業の求めるITサービスの利活用と費用対効果調査研究』 （社）日本コンピュータシステム販売店協会（JCSSA） 平成19年2月
14. 『SI 事業者における脆弱性関連情報取扱に関する 体制と手順整備のためのガイダンス』（社）情報サービス産業協会（JISA） （社）電子情報技術産業協会（JEITA） 2005 年 8 月
    http://www.jisa.or.jp/report/2004/vulhandling_guide.pdf
15. 『ASP・SaaS の情報セキュリティ対策に関する研究会』資料　総務省　平成19年10月17日
16. 『SaaS向けSLAガイドライン（案）』　経済産業省　（独）情報処理推進機構　平成19年11月21日
    http://search.e-gov.go.jp/servlet/Public?Pcm1010&BID=595207044