Computer Software Association of Japan

平成 19 年度

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

活動報告書

平成 20 年 3 月

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

別添資料

1　経済産業省「情報システムの信頼性向上のためのモデル取引・契約に関する研究会」報告書（平成 20 年 4 月／経済産業省より公表）

1)報告書本編
2)別紙 1.2（全体像）
3)パッケージソフトウェア利用コンピュータシステム構築委託モデル
契約書（システム基本契約書）
4)重要事項説明書
5)セキュリティチェックシート解説（別紙）

2　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検討結果資料（平成 20 年 4 月／CSAJ より公表）

1)情報システムの取引慣行・契約に関する実施ガイド
～企画・開発ガイドライン～
2)情報システムの取引慣行・契約に関する実施ガイド
～保守・運用ガイドライン～
3)セキュリティチェックシート（詳細項目版）
4)システム取引におけるトラブル事例

Ⅰ．経緯

経済産業省が平成 18 年 6 月に公表した「情報システムの信頼性向上に関するガイドライン」は、産業構造審議会情報経済分科会情報サービス・ソフトウェア小委員会（委員長：株式会社 野村総合研究所 村上輝康 理事長）によって審議され、ガイドラインの実効性を担保する措置として、業界団体、利用者団体によるモデル契約書の策定を求められ、昨年 6 月に同省情報処理振興課主管の「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（以下、「METI 研究会」という）」が発足した。METI 研究会では、社会インフラおよび大企業基幹系システムの構築に資するモデル契約および関連ドキュメントが作成され、平成 19 年 4 月に最終報告書＜第 1 版＞（※1）として発表された。

このモデル契約は、(1)対等の交渉能力のある利用者と IT ベンダが対象、(2)独自ソフトウェアをゼロから構築する、(3)利用者がすべて要求仕様を策定する、(4)IT ベンダは要求仕様に基づきソフトを請負作成する、(5)企画、設計、開発、保守において異なる IT ベンダーを想定した多段階契約、などが骨子となっており、初めての画期的なモデル契約となった。

しかしながら、本モデル契約は、IT に関する専門知識を有しない中小・中堅企業ユーザや、パッケージソフトウェアを利用した契約を想定しておらず、本報告書の総論においては「これらに対応したモデル契約については、業界団体における議論が望まれる」とされている。

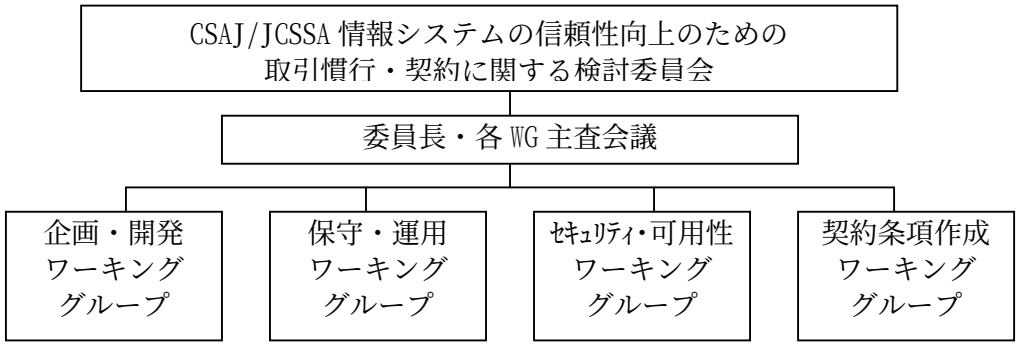
そこで、社団法人コンピュータソフトウェア協会（CSAJ）では、中小・中堅企業における情報システムの円滑な導入、運用を確保するための新たなモデル契約の策定が重要であるとの判断から、中小・中堅企業に向けた情報システムを提供する IT ベンダ業界団体である社団法人日本コンピュータシステム販売店協会（JCSSA）と合同で、平成 19 年 4 月から「情報システムの信頼性向上のための取引慣行・契約に関する検討委員会（以下、「CSAJ/JCSSA 契約検討委員会」という）を発足し、パッケージソフトウェア、ASP/SaaS を利用し情報システムを構築する中小・中堅企業と、ソフトウェアメーカ、システムインテグレータの取引慣行・契約に関する調査・研究を行い、モデル取引・契約およびガイドライン等を作成することとした。

また、本調査・研究を進める中で、平成 19 年 9 月には、経済産業省の「情報システムの信頼性向上のためのモデル取引・契約普及に関する環境整備事業」の一環である「中小企業ユーザ、保守運用サービス等を想定したモデル取引・契約書の整備事業」の委託を請け、CSAJ/JCSSA 契約検討委員会において、IT に関する専門知識を有しない中小・中堅企業ユーザのパッケージソフトウェアを利用した情報システム取引を前提とした「モデル取引・モデル契約および各種ドキュメント」の策定を行うこととなった。あわせて、本モデル取引・契約の普及策のひとつとして「e-Learning コンテンツ」を作成することとなった。

(※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）報告書＜第 1 版＞
http://www.meti.go.jp/policy/it_policy/keiyaku/index.html

Ⅱ．運営体制とメンバー

委員会および委員会の下部組織として詳細な課題を検討するワーキンググループ（WG）を設置し、それぞれ具体的な検討を行った。



（以下、メンバー敬称略、所属は平成 20 年 3 月現在）

●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

ワーキンググループで策定したガイドライン、契約書等を検討し、METI 研究会、CSAJ、JCSSA 等に答申と提言を行った。メンバーは、以下の通り。

顧　問 淺田　隆治　フューチャーアーキテクト㈱　顧問(CSAJ 副会長)
委員長 板東　直樹　アップデートテクノロジー㈱　代表取締役社長(CSAJ 常任理事)
委　員 江口　英則　㈱内田洋行　執行役員　情報システム事業部　事業部長
委　員 宮内　伸一　㈱エム・エスコーポレーション　代表取締役
委　員 田中　邦信　㈱大塚商会　システムサポート部　参事（保守・運用 WG 主査）
委　員 高橋　知久　㈱オービックビジネスコンサルタント　管理本部次長
委　員 中根　弓佳　サイボウズ㈱　経営管理本部　知財法務部マネジャー
委　員 浅野　正樹　㈱ＣＳＫホールディングス　法務部　知的財産管理課　課長
委　員 桐栄　誠一　ソフトバンク・テクノロジー㈱　取締役執行役員
　　最高情報セキュリティ責任者
委　員 高田　和幸　トレンドマイクロ㈱　コーポレートマーケティンググループ
　　ディレクター（セキュリティ・可用性 WG 主査）
委　員 加藤　栄　日経ＢＰ社　パソコン・ビズライフ局長
委　員 宮野　弘幸　日本事務器㈱　経営企画部　部長
委　員 田村　俊一　日本ビジネスコンピューター㈱　ＳＩ事業部ＳＩ本部　本部長
委　員 水谷　学　ピー・シー・エー㈱　代表取締役社長（公認会計士）
委　員 谷畑　良胤　㈱ＢＣＮ　メディアユニット　週刊ＢＣＮ編集長
委　員 脇坂　隆則　日立ソフトウェアエンジニアリング㈱ソリューション開発本部
　　セキュリティソリューション部　部長
委　員 五十嵐邦夫　㈱富士通エフサス　サービスビジネス本部システム運用コンサルタント
委　員 平本　健二　㈱フューリッジ　代表取締役（企画・開発 WG 主査）
委　員 中山　泰宏　マイクロソフト㈱　パートナービジネス統括本部　チャネル開発本部長
委　員 山岸　耕二　㈱豆蔵　代表取締役副社長
委　員 小西　理　㈱豆蔵　ｅ－Ｊａｐａｎ戦略室長
委　員 藤原　宏高　ひかり総合法律事務所　弁護士(METI 研究会委員)
委　員 平野　高志　ブレークモア法律事務所　弁護士(CSAJ 理事/契約条項作成 WG 主査)

委　員 吉田　正夫　三木・吉田法律特許事務所　弁護士(METI 研究会委員長)
委　員 上山　浩　　日比谷パーク法律事務所　弁護士(METI 研究会委員/TF リーダー)
委　員 前川　徹　　サイバー大学　ＩＴ総合学部　教授（CSAJ 常任理事）
委　員 山内　晨弘　㈱クリアテック　取締役
委　員 宮崎　一紀　(有)情報経営ブレインズ　代表取締役（中小企業診断協会東京支部）
委　員 久保寺良之　特定非営利活動法人ＩＴコーディネータ協会　常務理事　事務局長
委　員 小林陽二郎　独立行政法人情報処理推進機構
　　エンタプライズ系プロジェクト（開発プロセス共有化）研究員
オブザーバ　夏目　健夫　　経済産業省　商務情報政策局　情報化人材室長
オブザーバ　石川　浩　　経済産業省　商務情報政策局　情報処理振興課　課長補佐
オブザーバ　長谷川徳慶　　経済産業省　商務情報政策局　情報処理振興課　係長
オブザーバ　原田　俊彦　　社団法人日本情報システム・ユーザ協会　常務理事
オブザーバ　一條　倫子　　社団法人電子情報技術産業協会　インダストリ・システム部
オブザーバ　高部美紀子　　社団法人コンピュータソフトウェア協会　理事・事務局長
オブザーバ　松波　道廣　　社団法人日本コンピュータシステム販売店協会　専務理事
事務局　井上　星子　　社団法人コンピュータソフトウェア協会
事務局　鈴木　啓紹　　社団法人コンピュータソフトウェア協会
事務局　古田　正武　　社団法人日本コンピュータシステム販売店協会

●企画・開発 WG

パッケージソフトウェアの採用プロセスの研究、アドオン、カスタマイズにおける仕様策定の研究、受託における注意事項の研究ならびにガイドラインを策定した。メンバーは以下の通り。

主査　平本　健二㈱フューリッジ　代表取締役
ﾒﾝﾊﾞｰ　浅野　正樹㈱ＣＳＫホールディングス　法務部　知的財産管理課　課長
伊藤　孝洋㈱オービックビジネスコンサルタント　管理部
川手　真史㈱内田洋行　情報システム事業部企画部企画課課長
倉石　英一IT マネジメント・サポート協同組合（ERP 研究推進フォーラム）
小西　理　㈱豆蔵　ｅ－Ｊａｐａｎ戦略室長
小林陽二郎独立行政法人情報処理推進機構
佐藤　裕子ピー・シー・エー㈱　総務部法務担当
瀬戸口静美マイクロソフト㈱　業務執行役員テクニカルソリューション推進統括本部長
高橋　雄大㈱エルム　ASP 事業推進部　主任
中根　弓佳サイボウズ㈱　経営管理本部　知財法務部マネジャー
前川　徹　サイバー大学　ＩＴ総合学部　教授（CSAJ 常任理事）
　　エンタプライズ系プロジェクト（開発プロセス共有化）研究員
水谷　学　ピー・シー・エー㈱　代表取締役社長（公認会計士）
宮内　伸一㈱エム・エスコーポレーション　代表取締役
宮崎　一紀(有)情報経営ブレインズ　代表取締役（中小企業診断協会東京支部）

●保守・運用 WG

パッケージソフトウェアを中心としたシステム（ハード、ソフト、ネットワーク）の保守、運用の研究ならびにガイドラインを策定した。メンバーは以下の通り。

主査　　田中　邦信㈱大塚商会　システムサポート部　参事
ﾒﾝﾊﾞｰ　五十嵐邦夫㈱富士通エフサス　サービスビジネス本部システム運用コンサルタント
岩崎　悦夫ＮＥＣフィールディング㈱　保守事業推進本部　本部長
田村　俊一日本ビジネスコンピューター㈱　ＳＩ事業部ＳＩ本部　本部長
塚原　雅宏ＮＥＣフィールディング㈱　保守事業推進本部 販売店パーソナル保守推進部　部長
宮野　弘幸日本事務器㈱　経営企画部　部長
米山　忠志東芝情報機器㈱　カスタマサポート事業部　フィールドサポート推進部　ＦＳ企画部　部長
ｵﾌﾞｻﾞｰﾊﾞ 板東委員長アップデートテクノロジー㈱　代表取締役社長(CSAJ 常任理事)

●セキュリティ・可用性 WG

パッケージソフトウェアを中心としたシステム（ハード、ソフト、ネットワーク、Web 等）のセキュリティ、信頼性確保、可用性の研究ならびにガイドラインの策定した。メンバーは以下の通り。

主査　　高田　和幸トレンドマイクロ㈱ コーポレートマーケティンググループシニアマネージャー
ﾒﾝﾊﾞｰ　永来　真治アップデートテクノロジー㈱　取締役　営業担当
奥天　陽司マイクロソフト㈱　チーフ　セキュリティ　アドバイザ　早稲田大学非常勤講師
小野寺　匠マイクロソフト㈱　セキュリティレスポンスチーム　チームマネージャ
近藤　伸明㈱神戸デジタル・ラボ　R&D システム部マネージャ
千葉　貴志トレンドマイクロ㈱　コーポレートマーケティンググループコーポレートコミュニケーション課マーケティングスペシャリスト
中塚　勝　ソフトバンク・テクノロジー㈱　情報セキュリティ推進室　マネージャー　情報セキュリティ教育責任者
脇坂　隆則日立ソフトウェアエンジニアリング㈱ソリューション開発本部セキュリティソリューション部　部長
ｵﾌﾞｻﾞｰﾊﾞ 板東委員長アップデートテクノロジー㈱代表取締役社長(CSAJ 常任理事)

●契約条項作成 WG

パッケージソフトウェアを中心としたシステム（ハード、ソフト、ネットワーク）の取引におけるモデル契約書および重要事項説明書の作成と、METI 研究会報告書との整合性の確認を行った。メンバーは以下の通り。

主査　　平野　高志ブレークモア法律事務所　弁護士（CSAJ 理事）
ﾒﾝﾊﾞｰ　上山　浩　日比谷パーク法律事務所　弁護士(METI 研究会委員/TF リーダー)
切貫　総子ブレークモア法律事務所　弁護士
藤井　晋哉ブレークモア法律事務所　弁護士
藤原　宏高ひかり総合法律事務所　弁護士(METI 研究会委員)
吉田　正夫三木・吉田法律特許事務所　弁護士(METI 研究会委員長)
ｵﾌﾞｻﾞｰﾊﾞ 板東直樹　委員長
平本健二　企画・開発ワーキンググループ主査
田中邦信　保守・運用ワーキンググループ主査
高田和幸　セキュリティ・可用性ワーキンググループ主査

Ⅲ. 活動実績

CSAJ/JCSSA 契約検討委員会および各ワーキンググループにおける活動の成果として、「情報システム・モデル取引・契約書（パッケージソフトウェア、ASP/SaaS 活用、保守・運用）＜追補版＞報告書案」を作成し、平成 20 年 1 月に METI 研究会に提出した。さらに、METI 研究会の意見を受け、CSAJ/JCSSA 契約検討委員会でその内容を精査し、最終報告書としては、平成 20 年 4 月 15 日に経済産業省より「報告書－モデル取引・契約書＜追補版＞(別添資料 1 参照)」として公表された。

◆経済産業省／情報システムの信頼性向上のための研究会
http://www.meti.go.jp/policy/it_policy/softseibi/index.html#02

◆報告書－モデル取引・契約書＜追補版＞の概要

特徴

中小企業をITの専門知識を有しないユーザと定義
パッケージソフトウェア利活用の取引モデルを新たに策定
保守を前提とした取引・契約モデルを策定

1

	モデル取引・契約書<第一版＞ 2007年4月公表	重要事項説明書活用型モデル取引・契約書 ＜追補版＞ 2008年4月公表
契約当事者	対等に交渉力のあるユーザとベンダ	ITの専門知識を有しないユーザと業として情報サービスを提供するベンダ
対象モデル	ウォータフォールモデル	パッケージ、SaaS、ASP
対象システム	重要インフラ・社会基幹システムの受託開発（一部企画を含む）、保守・運用	一般業務システム
特徴	初めてユーザ・ベンダ双方が議論の上、策定 フェーズごとのユーザ・ベンダ間の責任の明確化（準委任・請負） 共通フレーム2007準拠 仕様の変更管理手続きの明確化 マルチベンダ・工程分割発注への対応	重要事項説明書を用いた契約合意 ITコーディネータや中小企業診断士を始めとする外部専門家やコンサルタントの参画を前提 システム構築後のプロセスを重視（保守、運用等） パッケージソフトウェアの取り扱いについてのベンダの責任明確化 著作権のベンダへの帰属 上記以外の点について第一版の特徴は原則、追補版でも踏襲

契約のポイント

パッケージ保守はパッケージメーカーの使用許諾契約による
ベンダに善管注意義務を課し、専門家としての責任を明記

2

- 協働
  - ユーザのベンダ丸投げの防止
  - システムの内容の確定についてはユーザが権限と責任を持っている
  - ユーザ、ベンダの共同作業であり役割分担を明確化
- 連絡協議会
  - 口頭での変更を防止
  - 変更規定、議事録、承認プロセスを義務化
- 再委託
  - 原則自由
  - 但し、ユーザ要求に基づき、再委託先を開示
  - 情報漏洩については、秘密保持契約で対応
  - 品質については、瑕疵担保で対応
- パッケージ選定における善管注意義務
  - 業界において一般的に要求される注意義務を課す
  - パッケージ選定は、仕様、制限事項の決定であり、開発、保守、運用全般に重要な影響を与えることを明確化
- 瑕疵担保
  - 帰責事由のある場合に限定
  - 逸失利益や間接損害は負わず、現実に被った通常の損害に限定
  - 損害賠償額は個別契約ごとに上限を設定
  - 仕様書、マニュアルとプログラムの不一致を瑕疵と認定
  - ユーザの資料等が誤っていることに起因した場合は瑕疵とはならないが、不適切を知りつつ指摘しない場合は担保責任を免れない

契約のポイント

著作権はベンダ帰属
保守範囲を限定し明確化、老朽装置等の交換請求権

3

- ベンダの善管注意義務
  - 業界一般的に要求される専門知識・ノウハウに基づく注意義務を課す
  - 準委任契約には専門家としての責任を規定
- 著作権
  - ベンダ帰属
  - プログラムの再利用による生産性向上、パッケージ利用のコスト低減、普及に資する
  - 著作権移転の対価は含まれないことから
  - プログラムの営業上の秘密は秘密保持契約で保護
- 知財侵害
  - 申し立ての際はベンダに対応指揮権
  - 確定判決に従い、損害賠償を負担
  - 使用不可能になった場合は、交換、変更、権利取得
  - 但し、ユーザ指示やハード等に起因する場合は免責
- 保守
  - 不良、不具合の修正（是正保守）のみ対応
  - 環境適応、性能改善、潜在的な不具合対応については範囲外とする
  - 遠隔地サポートの規定
  - 製造打ち切り、補修用部品提供打ち切りの場合、ユーザに対して対象製品の交換請求権を規定
  - 老朽化装置に対しても交換請求権を規定
  - ソフトウェアサポート中止の際の保守契約見直しを既定
  - 交換部品の所有権の移転
  - 設置場所整備はユーザによる
  - 不具合調査で他のシステムが起因する場合は、調査費用を請求

また、1)パッケージソフトウェアの採用プロセスを含む「企画・開発に関するガイドライン」、2)パッケージソフトウェアを中心としたシステム（ハード、ソフト、ネットワーク）の「保守、運用に関するガイドライン」、パッケージを中心としたシステム（ハード、ソフト、ネットワーク、Web 等）の「セキュリティチェックシート（詳細項目版）」をそれぞれ作成し、CSAJ の Web ページで公表した。

◆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
http://www.csaj.jp/committee/keiyaku/index.html

さらには、その普及の一環として e-Learning コンテンツを作成し、経済産業省に提出した。

なお、CSAJ/JCSSA 契約検討委員会および各ワーキンググループの開催および説明会等の開催実績は以下の通り。

■CSAJ/JCSSA 契約検討委員会

第 1 回　平成 19 年 4 月 25 日（水）10:30～12:00
1.契約検討委員会の組織案について
2.「情報システム信頼性向上のための取引慣行・契約等に関する研究会」最終報告書に関する説明
3.契約検討委員会の今後のすすめ方について

第 2 回　平成 19 年 5 月 29 日（火）10:00～12:00
1.トラブル事例紹介
2.各 WG 進捗報告
3.意見交換

第 3 回　平成 19 年 6 月 26 日（火）10:00～12:00
1. 日経 BP 社「動かないコンピュータ」等からの事例紹介
2. 各 WG の進捗報告
3. 意見交換

第 4 回　平成 19 年 7 月 24 日（火）10:00～12:00
1.企画・開発 WG より進捗報告
2.保守・運用 WG より進捗報告
3.セキュリティ・可用性 WG より進捗報告
4.重要事項説明書（案）について
5.意見交換

第 5 回　平成 19 年 8 月 28 日（火）10:00～12:00
1.企画・開発 WG より進捗報告
2.保守・運用 WG より進捗報告
3.セキュリティ・可用性 WG より進捗報告
4.契約条項 WG より進捗報告
5.意見交換

第 6 回　平成 19 年 9 月 25 日（火）16:00～18:00
1.中小企業、パッケージ取引・契約モデルの全体像について
2.各ＷＧにおける進捗報告
　1）企画・開発ガイドライン（案）
　2）保守・運用ガイドライン（案）
　3）セキュリティ・可用性ＷＧ
　4）契約条項作成ＷＧ
3.主要論点について

第 7 回　平成 19 年 10 月 23 日（火）10:00～12:00
1.各WGにおけるガイドライン（案）について
1）企画・開発ガイドライン（案）
2）保守・運用ガイドライン（案）
3）セキュリティ・可用性WGの進捗報告
4）契約条項作成WGの進捗報告
5）その他
2.主要論点について
第 8 回　平成 19 年 11 月 27 日（火）10:00～12:00
1.各 WG から進捗報告
2.主要論点について
3.その他
第 9 回　平成 19 年 12 月 25 日（火）10:00～12:00
1.報告書（案）について
2.その他
第 10 回　平成 20 年 3 月 17 日（月）16:00～17:30
1.経済産業省より公表された報告書＜追補版＞について
2.経済産業省の今後の展開について
3.平成 20 年度の CSAJ/JCSSA 契約検討委員会について
4.その他

■委員長・各WG主査会議
・第 1 回　平成 19 年 5 月 17 日
・第 2 回　平成 19 年 7 月 6 日
・第 3 回　平成 19 年 7 月 31 日
・第 4 回　平成 19 年 9 月 20 日
・第 5 回　平成 19 年 10 月 19 日
・第 6 回　平成 19 年 11 月 22 日
・第 7 回　平成 19 年 12 月 21 日
・第 8 回　平成 20 年 1 月 7 日
・第 9 回　平成 20 年 2 月 14 日

■企画・開発WG
・第 1 回　平成 19 年 6 月 7 日
・第 2 回　平成 19 年 7 月 10 日
・第 3 回　平成 19 年 8 月 21 日
・第 4 回　平成 19 年 9 月 11 日
・第 5 回　平成 19 年 10 月 4 日

■保守・運用WG
・第 1 回　平成 19 年 5 月 21 日
・第 2 回　平成 19 年 6 月 21 日
・第 3 回　平成 19 年 7 月 11 日
・第 4 回　平成 19 年 8 月 6 日
・第 5 回　平成 19 年 9 月 14 日
・第 6 回　平成 19 年 10 月 12 日

■セキュリティ・可用性WG
・第 1 回　平成 19 年 6 月 21 日
・第 2 回　平成 19 年 7 月 19 日
・第 3 回　平成 19 年 8 月 23 日
・第 4 回　平成 19 年 9 月 20 日
・第 5 回　平成 19 年 10 月 4 日
・第 6 回　平成 19 年 10 月 12 日
・第 7 回　平成 19 年 10 月 18 日
・第 8 回　平成 19 年 11 月 9 日
・第 9 回　平成 19 年 11 月 15 日
・第 10 回　平成 19 年 12 月 20 日

■契約条項作成WG
・第 1 回　平成 19 年 9 月 21 日
・第 2 回　平成 19 年 10 月 25 日
・第 3 回　平成 19 年 11 月 1 日
・第 4 回　平成 19 年 11 月 14 日
・第 5 回　平成 19 年 11 月 21 日
・第 6 回　平成 19 年 12 月 4 日

・第 7 回　平成 19 年 12 月 11 日　　・第 9 回　平成 20 年 2 月 6 日
・第 8 回　平成 19 年 12 月 18 日

■説明会の開催
○平成 19 年 11 月 27 日(火)　於：クオリティ㈱
・「情報システムの信頼性向上のための政策」
石川　浩氏　経済産業省商務情報政策局情報処理振興課　課長補佐
・「共通フレーム 2007」の概要とシステム取引における効果的な利用方法について
小林　陽二郎氏　独立行政法人情報処理推進機構(IPA)
エンタプライズ系プロジェクト（開発プロセス共有化）研究員
・「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の進捗報告」
板東　直樹氏　アップデートテクノロジー㈱　代表取締役社長
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委員長／CSAJ 常任理事

○平成 20 年 3 月 12 日（水）　於：大塚商会
・「経済産業省における情報システムの取引可視化に向けた取組」
長谷川　徳慶氏　経済産業省商務情報政策局情報処理振興課　課長補佐
・「システム設計、開発、保守・運用のモデル取引について」
板東　直樹氏　アップデートテクノロジー㈱　代表取締役社長
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委員長／CSAJ 常任理事

○平成 20 年 3 月 19 日（金）　於：大塚商会
・「経済産業省における情報システムの取引可視化に向けた取組」
石川　浩氏　経済産業省商務情報政策局情報処理振興課　課長補佐
・「システム設計、開発、保守・運用のモデル取引について」
板東　直樹氏　アップデートテクノロジー㈱　代表取締役社長
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委員長／CSAJ 常任理事

※経済産業省主催「情報システムの信頼性向上のためのモデル取引・契約に関するセミナー」への協力
日時：平成 20 年 3 月 14 日（金）　於：住友ホール（東京・新宿区）
共催：（社）コンピュータソフトウェア協会、（社）日本コンピュータシステム販売店協会、（社）日本情報システム・ユーザー協会、（財）ソフトウェア情報センター、（社）情報サービス産業協会、（社）電子情報技術産業協会

Ⅳ．添付資料について

1.経済産業省「情報システムの信頼性向上のためのモデル取引・契約に関する研究会」報告書（平成 20 年 4 月 15 日公表版）
1)報告書本編
2)別紙 1.2（全体像）
3)パッケージソフトウェア利用コンピュータシステム構築委託モデル契約書
（システム基本契約書）
4)重要事項説明書

5)セキュリティチェックシート解説（別紙）
2.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
1)情報システムの取引慣行・契約に関する実施ガイド～企画・開発ガイドライン
2)情報システムの取引慣行・契約に関する実施ガイド～保守・運用ガイドライン
3)セキュリティチェックシート（詳細項目版）
4)システム取引におけるトラブル事例

Ⅴ．最後に

本委員会および各ワーキンググループの度重なる議論の結果が、「情報システム・モデル取引・契約書（パッケージ、SaaS/ASP 活用、保守・運用）＜追補版＞」として経済産業省より公表されたこと、また、各種ガイドライン等を CSAJ Web サイトで公表できたことは、情報システム取引の可視化、信頼性の向上等に大きく貢献できたことと、多大なるご協力・ご支援をいただきました関係各位にこの場をお借りして深く感謝を申し上げます。

今後は、本モデル取引・契約書等が広く活用されることを期待しつつさらなる内容の精査及び普及活動等により、信頼性の高い情報システムの取引を実現するための取り組みを行って参りますので、引き続き皆様のご支援・ご協力をお願い申し上げます。

添付資料 1

経済産業省「情報システムの信頼性向上のためのモデル取引・契約に関する研究会」報告書（平成 20 年 4 月 15 日公表版）

1)報告書本編
2)別紙 1.2（全体像）
3)パッケージソフトウェア利用コンピュータシステム構築委託モデル契約書（システム基本契約書）
4)重要事項説明書
5)セキュリティチェックシート解説（別紙）

※本資料は、経済産業省「情報システムの信頼性向上のためのモデル取引・契約に関する研究会」が公表した報告書から引用
http://www.meti.go.jp/policy/it_policy/softseibi/index.html#02

「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～
（パッケージ、SaaS/ASP 活用、保守・運用）＜追補版＞

2008 年 4 月

（報告書）

〈目　　次〉

総論

経緯

平成18年6月に経済産業省より「情報システムの信頼性向上のためのガイドライン」[1](以下、「信頼性ガイドライン」という。）が公表された。信頼性ガイドラインは、我が国の情報システムの障害による社会的影響は日々、深刻化していると位置づけ、「システムの信頼性・安全性向上は喫緊の課題」との認識を示した上で、信頼性確保のためにはユーザ、ベンダの円滑な協力が必要なことから、「最大限明瞭な契約」、「契約における重要事項の明確化」、「情報システム構築の分業時の役割分担及び責任関係の明確化」の重要性を指摘した。さらに信頼性ガイドラインは、信頼性確保の実効性を担保するため、情報システムの利用者団体と情報システムの供給者団体による具体的な検討を求めた。

経済産業省は信頼性ガイドラインの指摘を受けて「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」(以下、「本研究会」という。)を設置し、ユーザ、弁護士、有識者と各団体による検討を重ね、パブリックコメントを経て ～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〉[2]（以下、「モデル取引・契約書第一版」という。）をとりまとめ平成19年4月に公表している。

このモデル取引・契約書第一版の特色は、「対等に交渉力のあるユーザ・ベンダ」、「重要インフラ・企業基幹システムの受託開発」を前提に、ソフトウェアの企画、開発、保守、運用をカバーし、共通フレーム2007[3]に準拠したユーザ、ベンダの詳細な役割分担を条文化したことにある。特に、仕様変更などにおける「口頭での合意による曖昧さ」を排除するための詳細な変更管理手続や、大幅な仕様変更に対応するための再見積規定、フェーズごとに異なるベンダの参画を想定したマルチベンダ・多段階契約などを規定した。さらに、機能要件[4]のみならず従来不明確であった非機能要件[5]の明確化を求めるとともにセキュリティに関連する条項を設け、ユーザ、ベンダ双方にとって見落としがちであった項目を条項化し、公平かつ透明性の高い合意が得られるよう工夫がなされている。

---

[1] http://www.meti.go.jp/policy/it_policy/softseibi/index.html#1

[2] http://www.meti.go.jp/policy/it_policy/softseibi/index.html#2

[3] 「共通フレーム2007～経営者、業務部門が参画するシステム開発および取引のために～」 独立行政法人 情報処理推進機構ソフトウェア・エンジニアリング・センター編、オーム社刊。ソフトウェア開発とその取引の適正化に向けて、ソフトウェアライフサイクルプロセス規格（ISO/IEC 12207）を基盤に、システム企画、要件定義、開発、運用、保守の作業項目を定義し、標準化したもの。

[4] ユーザの要求を満足するために、ソフトウェアが実現しなければならない機能に係る要件。システム機能及びデータにより定義される。〈例〉システム機能：業務フロー、業務処理定義、システム機能（階層、体系等）等。データ：データ構造（階層、関係等）、データ項目定義等。

[5] 機能要件以外のすべての要素に係る要件。業務内容及びソフトウェアの機能と直接的な関連性を有さない品質要件、技術要件、移行要件、運用要件、操作性及び付帯作業等からなり、それぞれに対する目標値及び具体的事項により定義される。(例) 品質要件：効率性（平均レスポンスタイム、ピーク時性能等）、信頼性（平均故障間隔、平均復旧時間等）、保守性（解析、変更等）、操作性（処理時間、処理容易性、操作理解性など）、セキュリティ要件等。技術要件：実現方式（処理方式、通信プロトコル等）、システム構成（ネットワーク構成、ソフトウェア構成、ハードウェア構成等）、開発方式（開発言語等）等。移行要件：移行対象業務、移行対象データ、移行時期、移行体制等。運用要件：運用体制、運用形態、運用スケジュール、運用管理方式（監視、バックアップ等）、災害対策等。付帯作業：ハードウェア展開、ソフトウェア展開、ユーザ教育等。

一方で、今後の検討課題として「パッケージを中心としたシステム導入の場合や反復繰り返し型の開発の場合、中小企業等ユーザにおける活用の場合等」について議論を深めるべきとの指摘があり、この指摘が本書における中核的なテーマとなった。本書は、モデル取引・契約書第一版を元に、「中小企業等におけるパッケージソフト等の活用と保守、運用」を含めた情報システム構築のためのモデル取引と契約のあり方を集約したものである。

目的

本書策定の目的は以下のとおりである。

（中小企業等におけるパッケージ、SaaS/ASP を活用したモデル取引・契約書の策定）
モデル取引・契約書第一版同様に、信頼性ガイドラインの遵守、取引関係・役割分担の可視化、オープン化への対応等を踏まえ、新たに IT・法務の専門家がいない中小企業等への配慮、パッケージソフトウェアの活用、共通フレーム 2007 の活用等を基本的な視点とし、情報システムの信頼性向上、取引可視化に資する理想的な取引・契約モデルを目指す。併せてモデル取引・契約書第一版で示された取引慣行、契約条項との整合性を確保する。

最終成果物として、①パッケージ、SaaS/ASP 取引を活用したシステム構築取引・契約モデル、②モデル契約書（システム基本契約書及び企画、開発、移行、教育、運用、保守の各フェーズの個別契約に関するシステム基本契約書の別紙に相当する重要事項説明書）、③モデルドキュメントを策定する（以下総称して、「モデル取引・契約書追補版」という。）。

モデル取引・契約書追補版の活用にあたっては、以下の点に留意をする必要がある。

① 本研究会においては、一定の前提条件をもとに議論を重ね、ユーザとベンダの理想的かつ実践的なモデルを提示したものである。パッケージソフトウェアを活用した情報システムのライフサイクルにおいて、ユーザとベンダ相互が参照し、円滑な取引のためのガイドラインとしての機能提供を狙っている。実際の取引においては、多様な取引形態や状況に応じ、モデル取引・契約書追補版上のモデル取引の全部又は一部及び共通フレーム 2007 を検討して活用することが望まれる。また、主要論点はモデル取引・契約書第一版を踏襲していることから、契約書の修正にあたっては適宜モデル取引・契約書第一版[6]を参照されたい。

② モデル取引・契約書追補版においては「中小企業等」を従業員数、資本金の大小などではなく「ベンダと対等の交渉力を有しない」[7]、IT や情報システム取引、法務の専門家、専従者を設置することが困難な団体、法人、企業等とした。こうした観点から、企業規模を問わず、IT、法務の専門家以外でも、情報システム取引の内容を正確に理解でき使いやすい契約書・重要事項説明書等を用意した。

③ 「パッケージソフトウェア」「SaaS/ASP」[8]については、特定の業種又は業務を想定し、そのなかで汎用的に使用されることを前提とした市販ソフトウェアとした。従って、ユーザとパッケージソフトウェア製造会社との間で使用許諾契約、保守契約が個別に締結されることを前提としている。また、SaaS/ASP を利用する場合、ユーザは SaaS/ASP アプリケーション事業者と、場合によっては SaaS/ASP プラットフォーム事業者の間において、個別にサービス契約が締結される事を前提としている。

---

6 http://www.meti.go.jp/policy/it_policy/keiyaku/index.html

7 第一版では「対等の交渉力のあるユーザ・ベンダ」、「ウォータフォールモデル」、「重要インフラ・企業基幹システムの受託開発」を想定している。

8 SaaS：サースもしくはサーズ読む。経済産業省 SaaS 向けガイドラインでは、「インターネット経由でアプリケーション機能を提供するサービスの形態」を指す。最も一般的な SaaS の形態は、SaaS 提供者が提供するウェブアプリケーションを利用者がウェブブラウザを通じて利用する形態である。」と定義されている。ASP：Application Service Provider。アプリケーションソフトをインターネットを介してユーザに提供するサービス形態。またはサービス提供事業者を指す場合もある。

SaaS/ASP 事業者のビジネスモデルについては、後述を参照されたい。

④ これらを踏まえ、モデル取引・契約書追補版で示したモデル取引・契約書は、信頼性確保の観点から、業務要件定義に基づくパッケージソフトウェア、補完製品の選定、パッケージソフトウェアのパラメータ設定、モディファイ・アドオン[9]などの開発、構築・設定業務、保守、運用支援といった役務や財を提供するベンダとユーザの一連の取引[10]に対応するためのものである。

⑤ 信頼性の高い情報システムの確保は、ユーザとベンダのたゆまない緊密な協働によってのみ得られるとの立場から、取引全般においては、ユーザ自身が役割を理解しベンダとの緊密な協働を行うことを前提とし、その上でユーザの理解を促しギャップを埋めるためのチェックリスト等を用意した。取引にあたってはこれらドキュメントの積極的な活用を前提としている。

⑥ ベンダにおいては、情報システムの知識を有しない企業に対して、業として情報サービスを提供する専門家としての十分な配慮と注意を払う必要と一定の責任があり、この点についてはモデル取引・契約書第一版と同様である。ベンダは、専門家として、コンサルティング能力、エンジニアリング能力を保有していることは当然のこと、善良な管理者の注意義務をもって、ユーザ業務に精通する努力、最新テクノロジーや将来動向を平易に説明する能力、さらにはプロジェクトマネジメントや品質管理能力の強化に日々留意を払っていることを取引の前提としている。

モデル取引・契約書第一版が示した、デューデリジェンス、契約締結、変更管理手続に至る一連の取引ルールと国際取引慣行との整合性、多段階契約、再見積りの考え方を踏襲した。情報システム取引に多くみられる「ベンダ丸投げ」を排除するため、上流工程から保守、運用に至るまで、取引の透明性の確保に留意した。

モデル取引・契約書第一版で示されたパッケージソフトウェア活用モデルを拡張・改良し、要件定義、パッケージソフトウェアの選定、カスタマイズ開発の有無、データ移行、運用、保守、要員教育を含めた、パッケージソフトウェア活用のシステム構築プロセスを改めて構想し、モデル取引・契約書第一版同様にユーザ、ベンダ双方にとって使いやすく、共通理解が促進される取引の目安として機能するように構成した。

各フェーズのタスクは共通フレーム 2007 を準用しており、必要に応じて共通フレーム 2007 を参照することによって、目的や相互の役割などを共有、確認することを前提にしている。チェックリストはこれらの解説に努め、取引の節目において何をするべきかの理解が促進されるように構成した。

SaaS/ASP は昨今、新しいソフトウェアの利用形態として注目を浴びており、モデル・契約書追補版においても、一般的なパッケージソフトウェアだけでなく、SaaS/ASP モデルでの活用も想定し全体を構成している。本年 1 月に経済産業省から「SaaS **向け** SLA **ガイドライン**」[11]が発表されたところであり、同ガイドラインにおいて「インターネット等を

---

[9] モディファイ：パッケージソフトウェアのソースコードの変更を伴うカスタマイズ。
アドオン：パッケージソフトウェアのソースコードの変更を伴わず、API（Application Program Interface）、外部 I/F、ファイル交換等を利用した外部プログラム。単独で動作するものと、パッケージソフトウェア本体とともに動作するものがある。

[10] パッケージソフトウェアの取引モデルについては、15 ページを参照。

[11] 経済産業省「SaaS 向け SLA ガイドライン」公表について
http://www.meti.go.jp/press/20080121004/20080121004.html を参照のこと。

経由するサービスであり、また、自社の財務データや顧客データなどをサービス提供者に預けることとなるため、企業が安心して利用するためには、利用者とサービス提供者間で、サービスレベルに関する取り決めが重要である。」との指摘がなされている。このような指摘を踏まえ、同ガイドラインの SLA モデルケースを掲載し、また、保守、運用における SLA については SLA 合意書の記入例を例示した。

また、SaaS/ASP のベンダは運用形態によって、①アプリケーション、認証、利用制限、課金、サーバ管理、データセンタまでを一体として提供するベンダ、②SaaS/ASP のアプリケーションソフトウェアを提供するベンダ、③SaaS/ASP の認証、利用制限、課金、サーバ管理等を提供する SaaS/ASP プラットフォームベンダなどに分かれる。③のプラットフォームベンダがデータセンタと契約し一体として管理する場合もあれば、②のアプリケーションベンダが③のプラットフォームベンダのソフトウェアだけを導入し、データセンタと契約するケースもあり、新たな市場を開拓すべく様々なビジネスモデルが競い合っている状況にある。一方で、利用するユーザにとっては、企業内のサーバ等で動作するパッケージソフトウェアと大きく異なることなく、一体の Web アプリケーションとしてサービスが提供されていることから、ユーザはこれら運用形態の違いや評価が異なる点を見落としがちであるので注意が必要である。そこで、機能、サービス評価の対象として②SaaS/ASP のアプリケーションベンダ、③SaaS/ASP のプラットフォームベンダを対象とした SaaS/ASP 選定のためのチェックリストを用意した。また、カスタマイズのための API やツールを整備している SaaS/ASP のベンダもいるが、上流工程の重要性、ベンダのユーザに対する説明責任、ユーザとベンダの協働等、パッケージソフトウェアを利用する場合と異なる事はない。また、SLA についてはユーザが見落とす可能性が高いため、重要事項説明書での SaaS/ASP 候補選定、SaaS/ASP 選定の際に SLA の評価を行うこととしている。

（パッケージソフトウェアをベースとしたシステム開発、導入の問題点）

パッケージソフトウェアをベースとしたシステム開発には、様々なメリットがある反面、ユーザの誤解や問題点の指摘も少なくない。

■ユーザが想定するメリット

① パッケージソフトウェアの持つ機能や業務の流れを利活用する事で、自社の業務改革を実施する事ができる。

② 導入期間とコストを削減することができる。

③ 導入のための専門要員を確保しなくても、システムを導入する事ができる。

④ 導入後、即座にシステムを稼働する事ができる。

■現実の問題

① パッケージソフトウェア自体は完成しているが、ユーザの目的を達成するシステムとしての導入及び開発期間は短いとは限らない。

② 要件にそぐわないパッケージソフトウェアの導入を図ったり、カスタマイズを実施した場合、予想を上回るコスト増大を招く場合がある。

③ パッケージソフトウェア本来の設計意図に反するカスタマイズを実施した場合、大幅なパフォーマンスの低下や制限事項の増加を招く場合がある。

④ 既存システムの置き換えまたは刷新において、従来は実現可能だった機能が実現できるとは限らない。場合によっては、機能実現のためにコストの増大や、使い勝手の悪化を招く場合がある。

⑤ 既設のシステムとの連携、データ交換は可能であるが、システムの OS や基本構造が

異なる場合は、膨大な費用がかかることがあり、また、意図するタイミングで想定する出力が得られるとは限らず、既設システムの大幅な改造が必要となるケースも散見される。

⑥ パッケージソフトウェアにカスタマイズを実施した場合、パッケージソフトウェア本体のバージョンアップが困難になる場合や、不具合改修などの保守サポートが受けられない、もしくは、割高のコストを負担しなければならない場合がある。

パッケージソフトウェアをベースに開発したとしても、しっかりとした要件定義が重要であることは、受託開発と何ら変わる事がない。反面、パッケージソフトウェアとして完成しているが故に、要件との適合性評価は、ユーザの要件と評価するパッケージソフトウェアをいかに知悉しているかにかかってくる。また、評価の範囲はパッケージソフトウェアの機能、カスタマイズの実現性と難易度の評価、開発会社のサポート体制、使用許諾契約の内容、将来のバージョンアップの動向など、個々に専門性が高く、幅が広い。このような点を踏まえた実効性のあるモデル契約の策定の必要性が指摘された。

（モデル契約書の策定・逐条解説）

モデル取引・契約書第一版で併記となった主要論点については、引き続き両論を尊重し逐条解説において併記し、注意を促すように努めている。ただし、モデル契約書本文においては分かりやすさを優先して選択条項は併記していない。主要論点においてかかる部分については注意を促すように努めている。

モデル取引・契約書第一版は、対等の交渉力を有するユーザ（民間大手企業等）とベンダ（情報サービス企業）を想定しているが、これは、情報システムに対する十分な知識を有している専門家の存在を前提としている。さらに、契約の実態として準委任契約、請負契約という契約類型が多段階に渡り選択されるため、法務及び契約実務の知識も併せて必要としている。

モデル取引・契約書追補版では、これらの情報システム及び法務の専門家がいない中小企業等のユーザと、業として情報システム関連のサービスを提供するベンダとの契約を前提に、パッケージソフトウェアをベースとしたシステム開発、導入の問題点等も踏まえ、現状の取引実態に配慮した構成をとっている。主要論点については後述を参照されたい。

① 上流工程における多様性の確保

上流工程は、企業の規模、システムの大小を問わず最も重要な工程であり、その品質は情報システムの成果、信頼性に多大な影響を及ぼす。ところが、中小企業等は社内に情報システムの専門家を配置することができないため、ベンダの行う業務分析に依存せざるを得ない上に、要件定義書、RFP[12]など成果物の正否の評価が困難であり、結果として信頼性の低下や情報化投資の失敗の原因となるという指摘があった。

そこで上流工程においては、共通フレーム 2007 をベースに、IT コーディネータや中小企業診断士をはじめとする外部専門家やコンサルタントの参画を考慮したモデルを構想した。システムインテグレータ（SIer）やソフト会社だけでなく、さまざまな視点から要件定義を行うことで、システム構築の質を高め信頼性の向上を図る重要なポイントであるといえる。また、パッケージソフトウェアの持つ機能や知見の比較を得て、業務の見直しを図るといったことも多く、上流工程が

[12] RFP：Request for Proposal、「提案依頼書」、「提案要望書」、「見積依頼書」などと言う。情報システム調達の際に、ベンダに詳細なシステム提案を行うよう要求すること、またはその調達要件をまとめた仕様書等をいう。第一版、25p 参照。

手戻りを前提としてスパイラル的に進むことも想定しなければならない。このように、パッケージソフトウェアのカスタマイズの有無や、導入する業務の特性によって、上流工程の作業が大きく異なってくることから、多様な導入モデルに対応できるよう配慮した。

② システム構築後のプロセスの重視（保守、運用等）

企業における情報システムの安定稼働、信頼性の確保は、事業継続性にも大きく関わることであり、特に運用に携わる要員のリテラシの確保や、保守体制の重要性は論をまたない。ところが、情報システム構築においては、業務のシステム化や高度化に関心が集中し、運用や保守からの仕様検討がなされず、あるいは構築費用の確保を優先することから先送りが多く、これらが業務との不一致や運用上の障害解消を困難とする原因となり信頼性を大きく損なっているとの指摘がなされた。本来、情報システムは一定期間、安定稼働することによって企業の業績に寄与するのであって、運用と保守体制が要件として確立されなければならない点に着目し、要員教育、保守、運用支援といったシステム構築後のプロセスも配慮した。また、保守、運用支援については、ハードウェア、OS、ミドルウェア等の構成要素別に保守契約を締結するのではなく、一次的なサポートの窓口が設定されることを前提に、障害の切り分けや問題のエスカレーションがなされることとしている。ユーザ自身が障害切り分けを行なうことができないことから、一次的な窓口は、ソフトウェア設計・制作業務及び構築・設定業務を行ったベンダ、またはその再委託先とし、下流工程からの一貫性を維持することで、信頼性、安定性を確保するものとしている。

③ 重要事項説明書を用いた契約合意

IT の専門知識を有しない中小企業等のユーザにおいては、ベンダの提案するシステムの内容が世の趨勢に従っているか、自社の目的に適合した正しい仕様であるかということを客観的に評価することが難しい。その結果、契約締結後の開発工程において、契約で定められた仕様が望むものでなかったことが判明し、工程の手戻りや、コストの増大、さらにはコスト負担ができずに不完全で信頼性の低いシステムでの稼働、あるいはベンダ側のかかるコストの負担による採算割れなど、様々な問題が発生してきた。体力のない中小企業等が、信頼性が高くかつ目的と合致するシステムを構築するためには、契約の透明性を高める合意プロセスの確保が重要であるとの指摘があった。さらに、大企業であっても情報システム部門や法務部門が関与しない情報システム取引においては、同様のプロセスが必要との指摘があった。

そこで、システムの目的、セキュリティを含む仕様、開発、保守、運用といったシステムライフサイクルと、双方の権利、義務について詳細内容を記述し、これらをもとに確認と合意を得るために、重要事項説明書を用いた合意プロセスを策定した。

また、重要事項説明書は、個別の業務に関する取引内容をユーザに説明するためのものであると同時に、個別の業務に関する契約条件を定めるものとして基本契約と一体となって契約を構成するものとなり、契約類型、個別の業務に必要となる契約条文を表すとともに、ベンダの作業内容を詳細に明示する役割を担っている。重要事項説明書によって、法的知識が十分でないユーザ企業にとっても契約内容の理解が促進され、開発着手に至る前での仕様の再検討と合意、厳密な変更管理の実施など、モデル取引・契約の実効性が高まることを期待している。また、これによりユーザが外部の弁護士に契約書の確認・アドバイスを依頼する場

合も、その効率化・容易化が図れることを期待されている。[13]
　一方、重要事項説明書を外形的に整えユーザに強要することで、ベンダが一方的に免責されるなどの懸念が指摘された。そこで、重要事項説明書には告知事項を設け、その内容の理解については、ユーザに対して十分な注意を喚起するよう配慮した。実際の運用においては、理解できた旨を文書で確認するなどによって、より実効性を高めることも考えられる。

④ パッケージソフトウェア
パッケージ活用によるシステム構築におけるパッケージソフトウェアの選定ミス（これにより、重大な瑕疵、モディファイ、アドオン開発上のトラブルがしばしば発生する。）は、即システム導入の失敗につながる。モデル取引・契約書第一版は第 48 条、第 49 条の第三者ソフトウェア（パッケージソフトウェア等）・FOSS[14]の利用について、「ベンダは当該ソフトの選定（利用方法、機能上・利用上の制限、保証期間等）について、専門家としての情報提供義務を契約上の責任として負う」として、ベンダに対して善管注意義務を課し慎重な業務遂行を求めている。他方で、ベンダはパッケージソフトウェアの作成に関与していないので、パッケージソフトウェアの保証をすることができないことから、パッケージソフトウェアの採否の最終的な決定はユーザ責任で行うこととし、パッケージソフトウェア自体については、ユーザとパッケージソフトウェア製造会社との間でライセンス契約を締結し、問題を解決することにしている。
　モデル取引・契約書追補版では、ベンダはパッケージソフトウェアの瑕疵、バグの対応、使用上の制限等については、重要事項説明書での説明事項として位置づけるとともに、パッケージソフトウェアの選定に関しては、ベンダは善良なる管理者としての責任をもってパッケージソフトウェアに関する情報提供等の業務にあたるとしてベンダの責任を明確化した。

（モデルドキュメント）
　ユーザは IT や情報システムに精通していないし、他方ベンダは必ずしもユーザの業務に精通していないことから、取引の初期において相互の情報の偏りが著しい。さらにユーザ、ベンダ双方に異なる「当然の常識」や「取引慣行」が存在すると、後々に大幅な仕様変更などが起こりやすい。実態として、ユーザはベンダの選定やドキュメントの内容の正確性、正当性を評価する体制に欠け、ベンダは、ユーザからの情報入手の漏れや、作業都合上による課題や工程の先送りが生じやすく、それらが原因で齟齬が発生する。これらの点に着目し、ユーザ自身が各フェーズの成果を評価ができるようなチェックリスト、さらには具体的なイメージをつかむための詳細サンプルドキュメントを例示した。

---

[13] ただし、法務の専門家が関与しないでよいということではない。むしろ、法務の専門スタッフを内部に抱える大企業よりも、そのような人材がいない企業の方が外部の弁護士の支援を受けるべき必要性は高い。モデル取引・契約書第一版のような詳細な契約書に基づく取引の場合と比較すれば、本報告書のモデル契約書・重要事項説明書は簡潔かつ平易な内容となっているので、弁護士との間の検討の効率化も期待される。

[14] FOSS：Free and Open Source Software の略称。「オープンソース」「オープンソースソフトウェア」「フリーソフトウェア」などとも言う。

モデル取引・契約書追補版の全体像とポイント

（モデル取引・契約書追補版の対象範囲）

本研究会におけるモデル取引・契約書追補版の策定にあたっては、以下のような前提条件をおいている。

- 契約当事者：IT の専門知識を有しないユーザと業として情報サービスを提供するベンダを想定。
  (例) 委託者（ユーザ）：民間中小・中堅企業、地方自治体、独立行政法人等、
  受託者（ベンダ）：情報サービス企業（SIer、ソフト会社、IT コーディネータ等）。
- パッケージソフトウェアについては、ユーザとパッケージソフトウェア製造会社で使用許諾契約、保守契約を別途締結。
- 開発モデル：パッケージ＋カスタマイズ型、パッケージ＋オプション型。
  ＊モデル取引・契約書第一版「2.(7)パッケージ活用、反復繰り返し型の開発、中小企業等ユーザにおける活用の留意点」を基に、新たに策定したモデル。
- 対象システム：財務会計システム、販売管理システム、電子メール、グループウェア、Web システム等の導入、構築・設定、カスタマイズ開発、移行、教育、保守、運用支援。
- 対象モデル：パッケージソフトウェアモデル、SaaS/ASP モデル。
- プロセス：共通フレーム 2007 に準拠したシステムの企画、要件定義段階、開発段階、運用段階、保守段階の定義及びその修正。
- 一括発注の場合に加え、マルチベンダ形態、工程分割発注に対応。

（パッケージソフトウェアを利用したシステム構築の特殊性、導入戦略による多様性）

パッケージソフトウェアを選択決定することで、大半のソフトウェア要件が決定されるという特色がある。要件を積み上げ、必要な機能を定め開発するのではなく、あらかじめ存在している機能を選択採用することで要件が確定されるともいえる。

パッケージソフトウェアの導入戦略は、(a)自社の業務に適合するようにパッケージソフトウェアをカスタマイズする、(b)自社の業務をパッケージソフトウェアに適合させる、という 2 つの対極が想定できる。コストという観点からそれぞれを評価すると、(a)はパッケージソフトウェアを開発工数削減のためのツールとして位置づけ、(b)は業務改善の知見や機能を得るツールとしての位置づけとなる。また、導入戦略によってベンダの選択も変化する。

実際には、(a)と(b)の中間に位置しつつ、業務の汎用性、特殊性に基づき取捨選択を行っており、その時点での社会的背景を含むビジネスモデルに大きな影響を受けていると言える。従って、モデル取引・契約書の策定にあたっては、パッケージソフトウェアの利用の目的を(a)と(b)の中間におき、上記導入戦略に左右されない全体像を追求した。

（モデル取引・契約書追補版の全体像）

基本的な考え方や信頼性確保のための手続はモデル取引・契約書第一版を踏襲した。

基本契約書は、パッケージソフトウェア利用コンピュータシステム構築委託契約書とし

て基本的な 14 条を策定した。必要と思われる相互の権利と義務を明示するようにしてあり、基本契約書が長大となることで、債権債務が不明瞭になることを避けるとともに、契約に不慣れなユーザが後日「読んでなかった」「知らなかった」といった事態を招かないようにし、契約の実効性を高めることを目的としている。

■パッケージソフトウェア利用コンピュータシステム構築委託モデル契約書（システム基本契約書）

第 1 条　本契約の構造
第 2 条　契約内容の変更
第 3 条　協働と役割分担
第 4 条　連絡協議会
第 5 条　ユーザがベンダに提供する資料等及びその返還
第 6 条　再委託
第 7 条　秘密情報の取扱い
第 8 条　個人情報
第 9 条　報告書の著作権
第 10 条　損害賠償
第 11 条　解除
第 12 条　権利義務譲渡の禁止
第 13 条　協議
第 14 条　合意管轄

個別契約書の役割をはたす重要事項説明書は、プロセスに応じて上流工程から保守、運用までの 11 契約を策定した。重要事項説明書はシステム基本契約書の別紙となり、それぞれに記名押印して一体の契約として機能する。契約当事者が表紙等の基本部分と業務に応じた必要な個別契約を選択し重要事項説明書を構成することで、多段階契約、マルチベンダ契約に対応できる。また、システム基本契約書の第 2 条（契約内容の確定、変更等）、第 4 条（連絡協議会）に基づいて仕様の変更に伴う再見積にも対応している。

■重要事項説明書（個別契約書）

（鑑部分）
表紙（契約の表示、受託者、重要事項を説明する契約担当責任者、委託者、告知事項）
契約の一覧（契約名称、受託金額、支払条件、特約条項）
その他本件業務に必要な事項
添付図書（図書名、版、日付）

（要件定義：準委任）
A　要件定義支援及びパッケージソフトウェア候補選定支援業務契約（カスタマイズモデル）
B　パッケージソフトウェア選定支援及び要件定義支援業務契約（カスタマイズモデル）
C　パッケージソフトウェア選定支援及び要件定義支援業務契約(オプションモデル)

（外部設計：準委任）
D　外部設計支援業務契約

（内部設計、システム構築・設定：請負）
E　ソフトウェア設計・制作業務契約
F　構築・設定業務契約

（移行・運用準備：準委任）
G　データ移行支援業務契約

H　運用テスト支援業務契約
I　 導入教育支援業務契約

（保守・運用：準委任）
J　保守業務契約
K　運用支援業務契約

例えば、保守と運用支援を受託するベンダは、重要事項説明書の「表紙」「契約の一覧」「その他本件業務に必要な事項」「添付図書」に加え、該当する「J　保守業務契約」「K　運用支援業務契約」の契約条項と具体的内容を記述し、システム基本契約書と重要事項説明書の記載事項をすべて説明し合意の上、それぞれに記名押印して契約とする。同一のベンダが複数業務を受託する場合は、各業務開始時に重要事項説明書の内容を確定し説明する。後工程の重要事項の条項は空白とするか、確定していない条項については「予約」として記載し、改めて業務開始に内容を確定し説明する。

重要事項説明書の表紙には、システム基本契約書との関係、契約の表示、契約の類型、重要事項の説明、受託者、重要事項を説明する契約担当責任者、告知事項、受領書及び契約条件の承認、委託者が記載されている。そして、ベンダ側の重要事項を説明する契約担当責任者が、重要事項説明書と関連図書を交付及び重要事項を説明し、委託者は、重要事項説明書を受領し告知事項と契約の条件を承認した旨の記載がされており、受託者からの契約全般の詳細説明を受けて合意の上契約の締結がなされる様式となっている。このように、契約合意をシステム基本契約書と重要事項説明書を分離し、情報システム取引での個別難解な事項を条文としてではなく、具体的作業内容として説明し、さらに重要と思われる部分については告知事項とすることで、ユーザ、ベンダ双方の契約の可視化を図るものである。

ベンダ側で契約締結にあたる責任者である上記の「重要事項を説明する契約担当責任者」とは別に、重要事項説明書の鑑部分及び各契約項目に、ユーザ側とベンダ側のプロジェクトの管理遂行について責任を有するプロジェクトマネージャとしての「責任者」及びプロジェクトの遂行について円滑な意思疎通を図るための連絡窓口としての「主任担当者」を明記するようにした。ベンダの組織体制、プロジェクトの規模、進め方によって、契約担当責任者とプロジェクトの管理遂行に関する「責任者」が同一の場合もあれば、営業担当者が契約担当責任者となり、技術担当者がプロジェクトの管理遂行に関する「責任者」としてなる場合がある。同様にユーザにおいても、代表者など契約締結に当たる責任者とプロジェクトの管理遂行について責任を有する「責任者」が同一の場合も異なる場合もあり得る。

さらに、各個別契約の具体的作業内容については、できる限り対応する共通フレーム 2007 該当事項を記述してある。共通フレーム 2007 をリファレンスとすることで、ベンダと再委託業者間や、マルチベンダ契約での解釈の相違を少なくするためである。[15]

さらに、表紙の告知事項では、情報システム取引におけるユーザとベンダの役割とともに協働の重要性を告知し、ユーザによる重要事項説明書の精査を促している。ユーザ、ベンダのコミュニケーション不足や協働がなされないことによるシステム構築のリスクを告知した上で、契約条件の確定と承認を得ることで、ユーザの詳細な検討と業務着手前の修正の余地を確保している。また個別業務ごとに、作業の概要、契約類型、契約条項と作業

[15] これによってすべての取引が JIS、ISO に対応するものではない。「共通フレーム 2007」26 ページを参照。

内容（範囲、仕様等）、納期又はサービスの期間、業務の完了、代金、損害賠償の上限、及びその支払方法を明確にしている。また、上流工程では、未決事項の記述欄を設け、ユーザの注意を促すように配慮した。

重要事項説明書の鑑部分の添付図書一覧は、構築システムに関わるすべての記録原簿としての機能を果たすようにし、提案書や見積書等のドキュメントをそのまま重要事項として採用し、重要事項説明書作成の負担を軽減することも可能としている。

上流工程の契約はカスタマイズを前提とした「A　要件定義支援及びパッケージソフトウェア候補選定支援業務契約（カスタマイズモデル）」、「B　パッケージソフトウェア選定支援及び要件定義支援業務契約（カスタマイズモデル）」と、パッケージソフトウェアのパラメータ設定や補完製品等での対応を前提とした、「C　パッケージソフトウェア選定支援及び要件定義支援業務契約(オプションモデル)」を策定し、それぞれに該当する 2 つのモデル取引を策定した。

■カスタマイズモデルとオプションモデルの特徴

	モデル取引	カスタマイズモデル(別紙 1)	オプションモデル(別紙 2)
業務	対象システムの例	生産管理、管理会計等	制度会計、青色申告等
	対象業務の汎用性	低い	高い
	業務、システムの移行	ある	ある
カスタマイズ	検討範囲	比較的広い	比較的狭い
	パッケージ本体のモディファイ	ありうる	ない （補完製品の選定､パラメータ設定、外部プログラムで対応）
	関連ソフトウェアとの結合	密結合、疎結合	疎結合
	既存ソフトウェア側の変更	小	小もしくはない
	既存システムとの結合工数	小	軽微もしくはない

■モデルと契約の関係

<table>
<tr><td></td><td colspan="2">モデル取引</td><td>カスタマイズモデル(別紙 1)</td><td>オプションモデル(別紙 2)</td></tr>
<tr><td rowspan="5">契約</td><td colspan="2">基本契約</td><td colspan="2">パッケージソフトウェア利用コンピュータシステム構築委託契約書</td></tr>
<tr><td rowspan="4">個別契約</td><td rowspan="2">準委任</td><td>A　要件定義支援及びパッケージソフトウェア候補選定支援業務契約（カスタマイズモデル）
B　パッケージソフトウェア選定支援及び要件定義支援業務契約（カスタマイズモデル）</td><td rowspan="2">C　パッケージソフトウェア選定支援及び要件定義支援業務契約(オプションモデル)</td></tr>
<tr><td>D 外部設計支援業務契約</td></tr>
<tr><td>請負</td><td colspan="2">E ソフトウェア設計・制作業務契約
F 構築・設定業務契約</td></tr>
<tr><td rowspan="2">準委任</td><td colspan="2">G データ移行支援業務契約
H 運用テスト支援業務契約
I 導入教育支業務援契約</td></tr>
<tr><td colspan="2">J 保守業務契約
K 運用支援業務契約</td></tr>
</table>

ある程度のプログラム開発が見込まれる場合は、カスタマイズモデルを選択し、プログラム開発が伴わない、または軽微であると見込まれれば、業務要件定義支援業務とシステム要件定義支援業務を分離することなく要件定義支援業務として、一定の手戻りを許容しつつパッケージの選定が行われる方がコスト的にも有利となる。これらの判断に苦しむ場合は、ユーザ、ベンダともに「取引・契約モデルの全体像（別紙 1、別紙 2)」を利用し、必要と思われるプロセスについて検討し、一定期間での成果とその後の契約内容の見直し特約を合意した上で、いずれかの契約を締結すればよい。

情報システムの信頼性・安全性を確保するためには、機能要件及び非機能要件の文書化

が重要であり、こうした考え方もモデル取引・契約書第一版を踏襲している。特に中小企業等ユーザに対しては、非機能要件としてのセキュリティ仕様をユーザの IT リテラシに沿った形で策定、提示されることが望ましいが、ユーザにとってはセキュリティ対策の重要性が理解しづらく、また、個別仕様が難解である。そのため、パッケージソフトウェア選定支援及び要件定義支援業務契約（カスタマイズモデル及びオプションモデル）の重要事項説明書において、告知事項としてセキュリティ対策を明示し、策定した仕様を提示するようにした。併せて JIS Q 27001[16] に基づいたセキュリティチェックシート解説を策定し、個別仕様についてユーザの理解が促進されるよう配慮した。具体的には、セキュリティチェックシート解説で、技術的セキュリティ対策と相当する脅威の内容を具体的に例示し、脅威に対する対策を何も対策していない～高度な対策の実施までを 4 段階で示した。物理的なセキュリティなどユーザ自身が実施すべき内容を含めて、項目を例示してある。これによって、ユーザは詳細な技術内容を知悉しなくても、セキュリティに対する仕様の脅威に対する強度や、堅牢さを把握することができ、コストや状況に応じたシステム仕様をベンダに求め、また、自社のセキュリティ対策を施すことが可能となる。ベンダは業務要件定義の策定段階で、セキュリティチェックシート解説に基づくセキュリティ対策の仕様をユーザに提出し、承認を受けて業務要件に組み込みセキュリティ仕様が策定されることとなる。また、データ移行支援業務と運用テスト支援業務においても、ユーザ自身の正誤又は可否判定を求める場合についての、ユーザの確認、精査、最終判断の必要性を告知し、相互の役割を正しく認識するよう配慮している。

モデル取引は、ソフトウェア設計・制作業務及び構築・設定業務を請け負ったベンダが、保守業務契約、運用支援業務契約を締結することを前提としている。一次切り分け窓口を一本化し、IT の専門知識のないユーザの負担を最小限にするとともに、ベンダ同士の責任回避を防ぎ、保守、運用支援プロセスの処置の明確化を確保するためである。さらに、具体的なサービス品質を確保するため、SLA[17]合意書の添付の有無を重要事項説明書に設けた。SLA 合意書では個別具体的な数値目標を明示し、また、SLM[18]の規定も明確化している。その上で、ハードウェア保守など、ベンダ自身がサービスを提供できない場合に対応するため、「再委託先の表示」を項目として設けた。

ハードウェアの販売契約についての重要事項は、個々のベンダによって内容が大きく異なることから重要事項説明書に組み込んでいない。ただし、業務要件定義や外部設計にあたって、カスタマイズの可否の検討や調査のために、ハードウェア、ソフトウェアの導入が必要となるケースがあるため、重要事項として機器、ソフトウェアの一覧を記述するようにしてある。この中では、ハードウェアの無償保証の条件や、補修用有償部品の保有期限等を明示するようにし、ハードウェアの保守の限界期限を相互に確認できるようにしてある。これは近年、ハードディスクやメモリなどの主要部品の規格が多岐にわたり、かつ、製品として入手可能な期間が短くなっているためである。一般的な電気製品や機械装置に比べ、著しく短い期間で規格の世代交代が進むことに理解を求めるとともに、システムライフサイクルに応じた情報投資を確保するためである。

---

[16] JIS Q 27001：情報技術―セキュリティ技術―情報セキュリティマネジメントシステム―要求事項、あらゆる形態の組織（例えば，営利企業，政府機関，非営利団体）を対象にする。その組織の事業リスク全般に対する考慮のもとで、文書化した ISMS（Information Security Management System）を確立、導入、運用、監視、レビュー、維持及び改善するための要求事項について規定。

[17] SLA：Service Level Agreement、サービスレベルに関する合意書、サービス品質契約書。

[18] SLM：Service Level Management、サービスレベル管理、サービスレベルの維持向上を目的とした管理活動。

モデル取引・契約書追補版におけるモデル契約のタスクは、ユーザ、業界関係者、情報システム取引契約に精通した弁護士による議論を経た配置をとっているが、業務要件定義に至るタスクでは、プロジェクト体制によって順序が異なる場合もある。また、パッケージソフトウェアによっては、評価のためであっても有償で使用許諾契約の締結を求められる場合もあり、ユーザの一般的な商習慣と大きくかけ離れる場合もある。いずれも、ユーザへの事前説明と議事録等での合意をもってプロジェクトを推進することが望まれる。

モデル取引・契約書追補版の主要条項の論点整理

（パッケージソフトウェア（候補）の選定支援における善管注意義務）

モデル取引・契約書追補版の検討においては、いわゆる上流工程（業務要件定義支援及びシステム要件定義支援）におけるあるべきビジネスプラクティス及びそれを反映した契約文言の検討に時間をかけた。

まず、モデル取引・契約書追補版が想定するビジネスの特色がパッケージソフトウェア（システムの構築に利用する第三者が権利を有するソフトウェア、SaaS/ASP）の利用にあること、パッケージソフトウェアはモデル取引・契約書追補版における成果物となるシステムの技術的中核となるものであり、また、システムの利用に関連し、パッケージソフトウェアに関してはその固有の条件が適用されることからシステムの全体の利用条件にも大きな影響を与え、瑕疵担保等の法的問題の分野においても重要な意味をもつこと、そしてそれが下流工程である設計、構築・設定、保守、運用の契約条件に対しても大きな影響を与えるものであることを認識した。さらに、IT コーディネータや中小企業診断士などの専門家の参画による、上流工程のモデルの多様性を勘案した。

このことに鑑み、上流工程を「業務要件定義」「外部設計」などとするのではなく、過程でパッケージソフトウェアがどのような意味を持つかを検討し、その結果、「業務要件」に基づきパッケージソフトウェア候補の選定が、パッケージソフトウェア候補の詳細なシステム要件の評価に基づく最終選定によって、業務要件とパッケージソフトウェアのシステム要件などの「要件定義」が行われるものと認識し、それぞれの業務の名称をそれぞれ「要件定義支援及びパッケージソフトウェア候補選定支援業務」「パッケージソフトウェア選定及び要件定義支援業務」とした。そして、それぞれにおいてパッケージソフトウェア（候補）の選定業務について対応する条項を入れるべきとの判断を行った。次に、モデル取引・契約書追補版が想定する中小企業等ユーザは、パッケージソフトウェア等に関する専門的知識を有するベンダに比べ、そのようなパッケージソフトウェアに関する知見に欠け、ベンダと対等な交渉能力がないものであること、しかしながらユーザの業務内容及びプロジェクトゴールを熟知しているのはユーザ自身であり、また上流過程における役割分担においてユーザがベンダに頼りきりいわば丸投げ状態を認めることはユーザとベンダのシステム契約についての理解の不一致を招き、こうした契約における契約条件の透明性・明確性の妨げとなることを認識した。

そこでモデル・取引契約書追補版では、最終的にパッケージの選定を行う者をユーザとし、ベンダはユーザに対し、パッケージソフトウェアに関する情報提供をしつつ、採用すべきパッケージソフトウェア候補をユーザに提案する位置づけとしている。そして前述したモデル取引・契約書追補版が想定する中小企業等ユーザのパッケージソフトウェアについての知見の不足に対応するために、当該推奨に係るパッケージの提案に関して、ベンダは業界で一般的に認められる専門知識とノウハウに基づく善良な管理者としての注意義務を負わせるものとした。また、これらの専門知識とノウハウに基づき、ベンダが適切と判断したときは、パッケージソフトウェア候補が存在しない、または、最適なパッケージソ

フトウェアが存在しない、ことをユーザに進言しなければならない、とした。「善良なる管理者の注意義務を果たした」かどうかは、情報処理技術に関する業界で一般的に要求される専門知識・ノウハウにもとづく注意義務を果たしたかどうかによって決定されるとした。すなわち、ここでの注意義務とは、自らの能力に応じた注意義務の程度という主観的な意味ではなく、業界において一般的・客観的に要求される注意義務を意味し、このような注意義務を欠くときは過失が認められることとした。ここで規定される善管注意義務は準委任契約におけるベンダの善管注意義務に重なるものであるが、上記したとおりパッケージソフトウェア候補の選定支援作業の重要性に鑑み、特に重複して記載している。

（瑕疵担保）

構築されるべきシステムは、パッケージソフトウェア、機器等のハードウェア、OS 等の本件パッケージソフトウェア以外のシステム構成物から構成されるシステムである。かかるシステムについて稼働不良などの問題が起きたときに誰が責任を負うべきかの問題は、問題の切り分け自体ができるかの技術的問題、切り分けができたとして誰がどの部分について責任を負うべきかの法的問題を含め難しい問題である。

モデル取引・契約書追補版では、パッケージソフトウェアについて、ベンダはその固有の瑕疵については責任を負わないものとした。パッケージソフトウェアはベンダ以外のものが制作、販売することが多く、瑕疵等の問題はそうした供給者とユーザとの間で解決すべき問題とし、ベンダはユーザがそうした問題を事前に知ること、分析、判断することの支援をするものとした。その結果、モデル取引・契約書第一版と同様に、ベンダはパッケージソフトウェアの固有の瑕疵について知っていたか、重大な過失により知らなかったことでユーザに告げなかった場合にのみ責任を負うものとした。

次に機器等のハードウェア、OS 等のソフトウェアについても、ベンダは責任を負わず、これらの問題についてもユーザと供給者との間で締結される別契約によって処理されるものとした。

（著作権の帰属）

新たに作成されたソフトウェアの著作権をベンダ、ユーザのいずれに帰属させるべきかについては、ベンダは作成したソフトウェアの再利用のために自己のものとして留保したいと考え、ユーザは自己の機密情報が含まれる場合の保護の観点などからベンダから譲り受けて、自己のものとしたいと考えている。モデル取引・契約書第一版においては、社会的な生産効率の向上の観点などから、汎用性のあるプログラムについてはベンダに帰属させると共に、そのようなプログラムに関してベンダ帰属案、ユーザ帰属案、共有案が記載されている。モデル取引・契約書追補版が前提とする取引は、パッケージソフトウェアを利用することとユーザが中小企業等であることなどに特色がある。

この観点より本論点を検討すると、まず、アドオン等のカスタマイズで新たに作成されるソフトウェアは前提となるパッケージソフトウェアの関連で作成されるものであり、当該パッケージソフトウェアの一般的機能となるべきものが、カスタマイズという形で先行して開発されることも多い。それゆえ、係る部分が将来的には他のユーザにも共通に利用できる部分となるケースもしばしばある。なお、ユーザがベンダから著作権の譲渡を受ける場合には、別途譲渡の対価を支払うことが要請されるため、そのような場合にはユーザの費用負担が増大する。他方、かかる部分にユーザの機密情報が含まれている場合にノウハウの流出防止など当該機密情報の保護をユーザが求めることは当然のことであるが、機密情報の保護のためには、著作権を取得しなくとも別途用意される秘密保持条項で対応できるものと考えられる。

以上のように、カスタマイズ等により作成されたソフトウェアの権利をベンダに帰属さ

せベンダが他のビジネスにおいても再利用できる環境を整えていた方が、総体としては価格を低く抑えることができ、中小企業等が利用するシステムとして比較的合理的な価格で広く普及することに資する結果となると考えられるため、カスタマイズ等により新たに作成されたソフトウェアの権利は原則ベンダに帰属させることとした。

（再委託）

モデル取引・契約書追補版においては、パッケージソフトウェアを利用したシステム開発の取引実態により適合するものとして、モデル取引・契約書第一版第 7 条[19]【B 案】を採用している。再委託の可否については、①再委託先の技術力についての保証がなくまた機密保持の観点からも原則禁止とし委託者の承諾を要するとすべき（原則禁止、【A 案】）との考えと、②再委託を原則禁止としてしまうことによって業務の遂行における柔軟性が失われ結局提供される技術の質も効率も損なわれてしまうので原則自由とすべき（原則自由、【B 案】）との考えの対立があり、モデル取引・契約書第一版においても、両論が併記されている。

モデル取引・契約書追補版が前提とする取引は、パッケージソフトウェアを利用すること、ユーザが中小企業等であることなどに特色がある。この観点より本論点を検討すると、そもそも多くの場合、第三者製品であるパッケージソフトウェアをシステムのコアの部分に据えるのであるから、再委託を厳しく制限することは現実的ではないこと、また原則再委託自由としてもユーザが要求するときは再委託先を開示させることとし、かかる再委託先を使うことを止めさせることに合理的な理由があるときはかかる再委託を止めさせることができるとすれば弊害も少ないものと考えられる。従って、再委託は原則自由としユーザが要求するときには再委託先を開示し、ユーザは合理的な理由があるときには再委託を中止できることとした。なお、かかる再委託中止に関連して委託料、納期に影響が出る場合には契約変更手続に基づいて行うことが必要となる。

今後の検討課題及びモデル取引・契約書追補版の活用について

（E-Learning 等を活用した普及）

経済産業省及び関係業界団体は、E-Learning のトレーニングプログラムの整備、セミナーの開催等を通じてモデル取引・契約書追補版に基づく取引慣行の普及に努める。

（IT 取引の適正性を担保するための資格制度の検討）

IT の専門知識を有しないユーザと業として情報サービスを提供するベンダの間では、モデル取引・契約書追補版に基づき契約事項・取引内容について真に合意に至ることが重要である。他方で、モデル取引・契約書追補版を形式的にしか利用せず、IT の専門知識を有さないユーザが実質的に合意していないにも関わらず、合意しているとの外観を整え、ベンダ側の免責の材料として使われる恐れもある。そうした慣行を防止する観点から、経済産業省及び関係業界団体はユーザの視点からのモデル取引・契約書追補版の活用のガイドの整備や、十分な IT と法務の知識を有し第三者としてモデル取引・契約書追補版に基づき取引を適正に行われることを担保する専門家を認定する資格制度の創設を含めた総合的な環境整備・制度設計の検討を進める。

---

[19] モデル取引・契約書第一版 59～60p。A 案：再委託先におけるユーザの事前承諾を設ける場合、B 案：再委託先の選定について原則としてベンダの裁量（但し、ユーザの中止請求が可能）とする場合。

（ユーザ・ベンダ間の役割・責任分担の明確化）

情報システムの信頼性の向上のためには、契約等によるユーザ・ベンダ間の役割・責任分担の明確化が重要である。他方で、IT を巡る紛争については、裁判例及び判例が十分に蓄積されておらず、契約上の文言の個別事例への適用についての予見可能性が小さいとの指摘がある。このような状況を改善するために、経済産業省及び業界団体は指針や準則の策定等も含めた取組について検討する。

（再委託先を含めた品質保証体制の確立）

我が国のソフトウェア産業の生産性については、欧米と比較して高くないといわれており、その原因として「労働集約的な受注ソフトウェア比率が高いこと」「中小企業等が中心で重層的な下請け構造」との指摘[20]がある。モデル取引・契約書追補版においては、パッケージソフトウェアでの開発であることから、再委託先についてはベンダの裁量を認めることで、柔軟なプロジェクトの推進を確保した。他方、ユーザは、開発形式を問わずプロジェクトに参画する情報サービス企業の品質保証、個人情報保護、情報セキュリティ等の管理体制について、重大な関心があるところであるが、再委託に関する開示情報は一律でなく、品質保証基準も定めがない。今後、業界団体を中心とした元請けと再委託先の品質保証体制の確立及び情報開示について議論が望まれる。

（システム性能の適正性及びシステムライフサイクルを担保するための情報開示）

システムの応答や処理速度などのシステム性能を確保するためには、ハードウェアの適正な選択が重要である。一方、OS、ミドルウェア、パッケージソフトウェア、デスクトップアプリケーションがそれぞれ、CPU 速度、必要メモリ、ディスク容量などの動作環境を提示しているところであるが、これらは、ベンダの独自裁定によるものであって、一定基準に沿った応答性能を保証するものなのか、最低限の動作を保証するものなのかは明らかでない。さらに近年、OS、ミドルウェアの様々なバージョンが混在する状況であり、アプリケーションソフトウェアの動作に適切なハードウェアを選択する方法論は確立されていない。

他方、システム構築からシステムの廃棄に至る期間は、ユーザの企画するビジネスモデルなどに深く影響する。激しい市場競争によって、高機能化、多機能化を重ねる情報システム製品、OS、ソフトウェアは、短期間で世代が交代する場合もあり、その結果、補修用部品の提供やサポート期間が、ユーザが想定する償却期間よりも短い期間で打ち切られ、システムの維持が困難となるケースが見受けられる。

今後、メーカーや業界団体等において、ソフトウェアの適正な動作基準の策定とそれに基づくハードウェア要件の開示、また、サポート期間等を考慮したうえで適切にシステムの企画・構築ができるよう、サポート・保守に関する情報の開示等の検討が望まれる。

[20] 峰滝・元橋、2007。http://www.rieti.go.jp/jp/publications/dp/07j018.pdf

モデル取引・契約プロセス

概要

企業の規模を問わず、経営の情報システムに対する依存度が高まることにより、システムの信頼性の低下が経営に打撃を与える可能性は比例する。信用や取引環境、財務的な安定度を考慮すると、中小企業等の情報システムの構築から運用、保守に至る信頼性確保は、企業存続のための重要な要件の一つと言える。

システム構築の核となるパッケージソフトウェアは、パッケージソフトウェア製造会社が利用状況と環境を想定し、一定の目的を達成するためのプログラムの体系であることから、構築稼働に至る時間を大幅に節約できるメリットがあるが、ユーザの目的やそれに沿った機能評価に失敗すると、信頼性のみならず適合性をも損ない、経済的な損失を招くことになる。

信頼性を確保し、業務に適合した情報システムを構築するためには、ユーザ自身が自社の事業、業務システムを分析し、パッケージの選定にあたることが重要である。反面、中小企業等ユーザにとっては、自社の業務分析や、パッケージに対する知識、機能評価を自ら自己完結することは困難な場合があり、それに代わる能力を外部に委託する場合がある。また、多くは情報システム構築の経験が少ない、もしくは前回の情報システム構築から年月が経過しているなどにより、近年の IT 関連情報に詳しくなく、情報システム取引に関わる法的知識に乏しいことが想定される。

これらを背景として、パッケージ選択に至る上流工程での、ユーザとベンダの役割、責任、義務を明確にするとともに、ベンダ以外の IT コーディネータを始めとする外部専門家やコンサルタントが上流工程を担うことを想定する必要がある。

一方で、完成した情報システムの操作運用はユーザが担い、保守については、アプリケーション部分がパッケージソフトウェア製造会社と、モディファイ、アドオンを開発したベンダに分かれ、場合によっては OS 製造会社、データベースエンジン製造会社からの保守を受ける必要があり、ハードウェアは各製造会社又は製造会社と契約している保守会社が提供することになる。さらに、通信インフラが加わることになると、一旦、障害が発生した場合には、ベンダ同士ですら障害切り分けや原因の究明が困難となる。

情報システムの取引、構築、維持はこのような複雑かつ多岐に渡る知識と契約実務を、専門的な知識を有しないユーザに要求するため、システムの提供側であるベンダは情報の非対称性に十分に配慮しなければならない。中小企業等における情報システムの信頼性確保のために、これら情報の非対称性の解消を観点として、モデル取引・契約書追補版でのモデル契約プロセスの全体構成、共通フレーム 2007 とモデル契約の関係を論じる。

モデル契約プロセスの全体構成

（前提とする中小企業等ユーザ像）
対等な交渉力を有しない中小企業等を以下のように想定する。

■LAN＋Internet への接続はできており、日常的に電子メール、財務会計、販売管理等のパッケージソフトウェアを利用している。

■最新の情報システム関連動向、パッケージソフトウェア関連動向は把握しておらず、システムの価格や妥当性を正確に評価することができる人材を有していない。

■情報システム資産の管理はなされておらず、情報システムに関連するドキュメントは整備されていない。

■取引上、相手先の機密情報や個人情報を取り扱う場合があるが、セキュリティ確保のための措置はとれていない。

■競争優位のための情報システムの役割を自ら構想することは困難である。

■バックアップや保守体制の確立、システムライフサイクルの認識などが事業継続に多大な影響があるとは承知していない。

■システム構築の検討に入る場合の多くは、システムの老朽化や処理能力への不満である。

■法務に精通した担当者が不在である。

■IT 精通した担当者が不在である。

ユーザは業務及び情報システムの課題や問題点に対する説明能力に欠ける。一方で、ベンダが限られた時間と予算の中で、最適な情報システムを提案することに心がけたとしても、ユーザの業務の特性や、現行システムへの不満、業務上の課題をすべて知悉することは困難である。このように、初期段階ではユーザとベンダのシステムに対する情報量と質ともに大きなギャップがあることを前提に、契約締結に至る必要がある。

システム構築の検討に入ったユーザは、ベンダに対して現状と保守、運用を含めた全体予算や人員、リテラシについて早期から可能な限り情報開示する事が望ましい。また、ベンダはユーザに対して、情報システム取引の全体の流れやプロセスの留意点、自社の管理体制を説明することが望ましく、ベンダの選定は、コンサルティング会社選定のためのチェックリスト等を参考に、予算、実績、技術力、経営安定度、委託を含めた業務管理能力、秘密及び個人情報保護の管理体制等を総合的に判断すべきである。

これらを前提に取引モデルを解説する。

（別紙 1 パッケージカスタマイズ 取引・契約モデル）
A　要件定義支援及びパッケージソフトウェア候補選定支援業務契約（カスタマイズモデル）

企画、業務要件定義、パッケージソフトウェア候補選定が本契約の具体的作業内容である。情報取引に不慣れなユーザは費用対効果を判断できないため、コストに対して不釣り

合いな要求を行う場合がある。このプロセスでは適宜 RFI[21]に基づく価格調査や保守・運用を含めた他社事例を取得することが重要である。パッケージの機能・制限事項の比較や、複数のパッケージを想定し導入後の運用シミュレーションを重ねることで、費用対効果や実現すべき要件の優先順位付けが可能となる。

企画においては、業務の新全体像、業務モデル、システム方式等の策定を求めている。ここでいうシステム方式の策定は、開発内容とアーキテクチャ、データベース、サーバ、ネットワーク構成概要を明確にすることがゴールである。企画段階で具体的な画面イメージや処理の流れを共有し、業務の流れとシステムの動きを策定し、要件の漏れや先送りを防止することを期待している。

業務要件定義については、機能要件とセキュリティを含む非機能要件の定義を行うものとし、さらに、パッケージ候補選定にあたっては、業務要件に対する機能適合評価のみならず、使用許諾契約の内容及び制限事項、SaaS/ASP においては SLA の内容及び制限事項、保守性（バージョンアップポリシー、OS のバージョンアップへの対応等）についての評価を求めている。ここで注意が必要なのは、パッケージ候補の選定だけでなく、適合しない又は適合性が低くパッケージソフトウェア利用の合理性がないと判断される場合である。前述の通り「A　要件定義支援及びパッケージソフトウェア候補選定支援業務契約（カスタマイズモデル）」、「B　パッケージソフトウェア選定支援及び要件定義支援業務契約（カスタマイズモデル）」では、適切なパッケージソフトウェアがない場合に備え、パッケージ候補、又はパッケージが存在しないことをユーザに進言することも、ベンダの善管注意義務としている。ベンダは、適切なパッケージソフトウェアが存在しない理由または回避策や代替案を提示し、ユーザが最終的に判断するに十分な情報の提供が必須となる。

「A　要件定義支援及びパッケージソフトウェア候補選定支援業務契約（カスタマイズモデル）」でのセキュリティに関する要件定義は、セキュリティチェックシート等を活用し、ユーザに対して具体的な脅威とあるべき対策を提示し、業務や規程で対応するものと技術で対応するものを検討し、業務要件定義で承認を受け次工程で具体的なシステム仕様が策定されるものとしている。従って、「B　パッケージソフトウェア選定支援及び要件定義支援業務契約（カスタマイズモデル）」の契約締結の際に重要事項説明書の＜告知事項＞として「要件定義におけるセキュリティ仕様」をユーザに確認し、これを基に具体的なシステム要件等の検討に入ることを前提としている。

最終報告書となる業務要件定義書は次の工程であるパッケージ選定及び要件定義支援契約での利用を前提に、その内容をユーザが評価しなければならない。特に、ユーザは経営層のみならず現場のオペレータを含め、機能要件並びに非機能要件について十分な検討をが必要である。セキュリティ要件については、システム要件定義支援業務の＜告知事項＞として次の工程で確認事項とされるため、十分な討議と合意が求められる。

業務要件定義書の評価にあたって、ユーザは IT コーディネータ、中小企業診断士、システム監査人等の専門家の助言を得ることが望ましい。その際は、共通フレーム 2007 を用いて相当する業務を示し、用語や業務内容の違いによる誤解を起こさない等の配慮が望まれる。

「A　要件定義支援及びパッケージソフトウェア候補選定支援業務契約（カスタマイズモデル）」を担当するベンダと、次工程を担当するベンダが異なる場合は、変更管理手続を用い、特約条項として最終報告書提出後も期間を定めてユーザとそれぞれのベンダの連絡協

[21] RFI：Request For Information、情報提供依頼書。第一版 24p 参照。

議会を設け、疑義の解消にあたるべきである。また、業務要件の未決事項はシステム化することが不可能となるため、その取扱いについて合意し、以降での対応方法を決定しなければならない。ベンダが異なる場合は、最終報告書に未決引き継ぎ事項を明示する。

B　パッケージソフトウェア選定支援及び要件定義支援業務契約（カスタマイズモデル）

要件定義支援業務は、業務要件定義書に基づき実施されるため、パッケージソフトウェア選定及び要件定義支援契約の重要事項説明(2) 具体的作業内容で、該当する文書を明示する。契約締結にあたっては、業務要件に対するベンダの疑義や不明点が解消されていることが望ましい。業務要件定義を行ったベンダが同一ベンダであっても担当者が異なる事は一般的であるので、連絡体制、疑義に関する解消方法等について、特約条項で定めるのが良い。

パッケージソフトウェア選定支援の各作業は、以降のあらゆる作業、業務に重大な影響を与えるため、重要事項説明書では各作業単位で報告書提出期限を定め、文書化を求めている。将来の保守性向上や信頼性確保に配慮し、さらに詳細な説明を加えることが望ましい。特に移行がある場合、現行システムから新システムへの移行のために、想定以上のコストが発生する場合もあるため、システム要件評価には移行要件を含むとした。前述の通り、最適なパッケージソフトウェアが存在しない場合のベンダの善管注意義務はユーザの十分な理解が必要である。

パッケージソフトウェアのモディファイの範囲を検討や、外部設計をするために、パッケージソフトウェアの使用許諾契約を締結しなければならない場合がある。業務要件定義でパッケージ候補が絞り込まれており、あらかじめ使用許諾契約締結が必要とわかっている場合は本件契約時に、「パッケージソフトウェア選定及び要件定義支援業務契約の重要事項(3)ソフトウェア、機器、ドキュメントの明細及び納入場所」を記載し、実務にあたることとなる。また、パッケージ候補が複数あり、本件契約で最終候補が絞り込まれた後、使用許諾契約締結が必要となった場合は、同様に「パッケージソフトウェア選定及び要件定義支援業務契約の重要事項(3)ソフトウェア、機器、ドキュメントの明細及び納入場所」を用い、変更管理規定に則って必要なソフトウェア、機器の納入、販売等を行うことになる。

前述のように、要件定義の重要説明の一環として、「＜告知事項＞要件定義におけるセキュリィ仕様」の記述を設けている。業務要件定義支援業務でユーザが合意されたセキュリティ要件を詳述し、それに基づいたシステム要件を定めるとともに、ユーザの注意喚起を図るためである。なお、データのバックアップについては、日常のデータバックアップ作業実施はユーザの責任とし、ベンダは機能の実装を担当するものとしているので、留意されたい。

パッケージ選定では、後述のデータ移行支援業務の重要事項を参照し、データ移行について仕様を定めることが望ましい。移行要件は、移行するデータによって見積と運用準備、システム稼働に関するスケジュールに多大な影響を与えるためである。

業務要件定義において選出されたパッケージソフトウェア候補が、すべての要件を満たさない場合に、予算を超さずにモディファイやアドオンによって要件を実現できれば、ユーザの満足度は高まるが、反面、システムの保守性、信頼性は低くなる。また、モディファイにあたっては、パッケージソフトウェア製造会社のサポートや保守体制、将来に渡るバージョンアップ時の対応、経営状況などを十分に考慮する必要がある。

本件契約の具体的成果としてパッケージソフトウェアが選定され、推奨ハードウェア構

成等が決定される。さらに、既存システムとの接続等がある場合、その範囲や既存システム側の変更のための仕様をどうするか、なども重要な決定事項となる。次工程である外部設計では、要件の追加や変更が頻発しない完成度を期待している。一連の成果はユーザが最終的な判断をするものとされるが、ベンダの作業は「情報処理技術に関する業界の一般的な専門知識及びノウハウに基づき善良な管理者の注意を持って行うもの」とされている。最適なパッケージソフトウェアが存在しない場合を含め、ベンダの慎重かつ的確な作業と説明責任が求められていることに留意されたい。

（別紙 2 パッケージオプション取引・契約モデル）

C　パッケージソフトウェア選定支援及び要件定義支援業務契約(オプションモデル)

この契約は財務会計ソフトウェア等で、不足する帳票を表計算ソフトウェア等で補うような、パッケージソフトウェアのモディファイやアドオンがない場合を想定している。パッケージソフトウェア本体のパラメータ設定および補完製品として販売されている補完製品の適合性をもっとも重視し、作り込みは最小限にすることが主眼であるといえる。小規模企業の財務、販売、人事管理などが相当するであろう。他方、いかに企業規模が小規模であろうとも、何らかの外部プログラムを作成するとなれば、一定の分析と文書化は必須である。従って、プロセスが一部省略されていても、主要な項目については、「A 要件定義支援及びパッケージソフトウェア候補選定支援業務契約（カスタマイズモデル）」、「B　パッケージソフトウェア選定支援及び要件定義支援業務契約（カスタマイズモデル）」と変わることはない。プロセスの途中で、＜告知事項＞要件定義におけるセキュリティ仕様がユーザに提示され、承認されることに留意する必要がある。

主要なポイントは前述の契約と変わることなく、それを一つの契約で実施しているところにある。外部設計は含んでいないが、外部プログラムの要件策定に当たっては表計算ソフトウェア等を実施に使用し、画面をその場で作り込んで、全体の流れやイメージをユーザにつかんでもらうことが重要である。

また、パッケージソフトウェアの補完製品選定においては、カタログ等でのスペックでは実現可能となっていても、実際には複数の手順を重ねて実現されるといった場合も散見される。補完製品や外部プログラムで構築が困難となった場合は、変更規定を利用し、契約の範囲を拡大し「B　パッケージソフトウェア選定支援及び要件定義支援業務契約（カスタマイズモデル）」への変更もあり得よう。

情報システムの信頼性確保は選定するパッケージソフトウェア、補完製品の適合性と使用許諾契約、保守契約の内容に依存することになる。パッケージソフトウェア候補の業務への適合性が低い場合、プロジェクトの中止以外に、コスト制限を解除できれば以下の選択肢が考えられる。

(1) 契約を検討し直し、モディファイ、アドオン開発に切り替える
(2) 外部プログラムの作成を行う
(3) 業務をパッケージソフトウェアにあわせシステム化する
(4) 優先順位を下げシステム化をしない

業務システムの信頼性や業務全般の見直しという視点からはどれも正しい選択とは言い難い。さらに、ユーザのリテラシやモラルも大きく関与するところであり、パッケージソフトウェアの適合性が低い場合の戦略は、ベンダだけでなく、ユーザの自立的な判断が重要であるといえる。実際の業務要件の決定にあたっては、ベンダがユーザの環境を総合的

に勘案するとともに、パッケージソフトウェアの導入事例を中心に、パッケージソフトウェアの特色を活かした利活用の実例をユーザ、ベンダと協働で分析し、ユーザが自主的にシステム化の優先順位を決定することが望ましい。スパイラル的な検討を重ねることによって、プロジェクトゴールの大幅な修正もありえることを契約時点で確認するとともに、いたずらに期間が費やされることのないように、進捗管理の方法を具体的に合意することが重要である。

RFP について

上流工程の契約終了時点で、外部設計支援業務、ソフトウェア設計・制作業務、構築・設定業務を異なるベンダに委託する場合は、最終報告書もしくは RFP を提示し、詳細見積を取得することとなる。RFP 作成を依頼した場合は RFP に対する疑義解消のための特約を結び、本件契約の業務を受託したベンダによる RFP 説明会を開催するのが望ましい。個別に RFP を説明するのではなく、後工程を受託しようとするすべてのベンダの参加を得て、十分な質疑応答を実施することで内容の共有がはかれ、疑義や用語定義の相違などを解消することができ、より精度の高い見積を得ることができるようになる。特約が無くとも複数のベンダから多数の疑義が生じ、または見積作成が困難とされた場合は、業界の一般的な善管注意義務を果たしていない事となり、最終報告書を作成したベンダの債務不履行となる可能性がある。

既存システムとの連携がある場合は、既存システム側の変更を含むのか、他のベンダがそれを担う場合は、最終的にどのベンダが接続、連携部分の責任を負うのかなど、ベンダ間での調整が必要となる。複数のベンダが参加する場合は、ユーザを含めた参加者全員の役割と責任、指揮命令系統を明らかにし、接続部分の成果や品質に対して無責任体制とならないようなプロジェクト体制の確立が求められる。RFP を提示されたベンダのプロジェクトでの役割と責任が明瞭となることが求められる。

システムの大きさ、範囲によって RFP 提示から見積提出までの必要な期間は様々であるが、あまりに期間が短いと当然のことながら見積精度は劣ってくる。問い合わせの対応を含め、一定期間を見積作業のために確保することも信頼性確保につながることに留意されたい。

運用手順書、利用者文書について

要件定義書で定義された機能要件はこれ以降ソフトウェアに実装されるが、利用者のための運用手順をどのように規定するか、運用マニュアルをどのように作成するかなど、実運用にかかる作業を最終的に取り決める必要がある。外部設計、ソフトウェア設計・制作業務で実装されたソフトウェアと実際の業務とのすり合わせのプロセスは、H 運用テスト支援業務契約で(35)運用にかかわる作業手順の確立として定義されているが、本来はソフトウェア制作と並行して検討、策定されるべき重要プロセスである。要件定義業務から開発プロセス移行にあたっては、これら運用手順の確立について、ユーザの業務規模、運用の複雑さに応じて、しかるべき方策を定めることが望まれる。特に、バックアップ作業については、その範囲、手順、世代管理等について、ユーザの能力に応じたベンダの十分な配慮が必要である。また、開発プロセス以降での各プロセスにおいて、利用者向け文書の作成のための作業や役割について、検討されることが望まれる。

小規模システムへの適用について

これらパッケージソフトウェアを活用した契約モデルは、共通フレーム 2007 に則りプロ

セスと契約を分離したモデルであるが、小規模システムで帳票の追加でユーザの要望に対応できるケースや少額取引では、上流工程において要件定義と外部設計を一つの契約で行うことも考えられる。また、業務要件定義の一部がベンダの営業提案で無償で実施され、パッケージソフトウェアとベンダが絞り込まれた状態で、(16)「API の実現性の確認」(17)「パッケージソフトウェアの選定と要件定義」(22)モディファイ、アドオンの範囲の確定、及びそれに伴うユーザ I/F・他システム I/F 設計」を契約し、その後、確定見積を取得し、システム構築・設定とソフトウェア開発をする場合も想定される。このように契約モデルに適合しない取引においても、信頼性確保の観点から、重要事項説明書を活用しベンダの十分な説明責任と善管注意義務が果たされ、正しい要件定義がなされることが望まれる。

D　外部設計支援業務契約、E　ソフトウェア設計・制作業務契約、F　構築・設定業務契約

開発工程は、外部設計支援業務と、内部設計にあたるソフトウェア設計・制作業務である。ここでの外部設計支援業務は、画面設計というプロセスの名の下に要件を抽出するということは想定していない。画面のイメージや画面遷移は十分に検討され、要件定義書を基にすれば、改めてユーザの業務分析を行わなくても外部設計ができる完成度の要件定義書が存在していることを期待している。ユーザがシステムと業務の動きをフローチャートや画面のデザインだけで理解できず、外部設計で要件を定義することも想定されるが、外部設計支援業務での要件の多大な追加や変更の多発は前工程の失敗を意味する。

RFP に基づき詳細見積が得られた段階で、以降の業務を担うベンダの選定が行われる。モディファイ、アドオンが伴う場合は、ソフトウェア設計・制作を実施したベンダに保守を依存することとなる。また、サーバ、クライアント、ネットワークの設定等の構築・設定業務契約と既存システムからのデータ移行支援業務、保守業務、運用支援業務は、運用を含めた信頼性の観点から分離することなく同一のベンダと一貫して契約することが望ましい。それぞれの業務を担当するベンダが異なる場合は、いずれかのベンダを主担当としてプロジェクトの推進調整、進捗管理を担わす必要がある。

RFP 又は要件定義書等で示された推奨ハードウェア構成については、外部設計段階で、十分な検討と確認が必要である。万一、性能等を確保できないと判断された場合は、ユーザ及び RFP を担当したベンダへの確認と疑義の解消が必須である。将来の処理増大に伴うスケールアップ、スケールアウトの拡張構成など柔軟性の確保と、稼働時点で過少・過剰設備とならないよう細心の注意をもってハードウェア構成がなされるように、ユーザとプロジェクトに参加しているベンダの検討、合意が望まれる。

ベンダの選定においては、コストだけでなくプロジェクトの管理体制、保守体制を評価すべきである。仕様書に基づいてプログラムを制作する技術と、制作されたプログラムを将来に渡ってメンテナンスするための技術はいずれも別のものである。極端にコストが安い場合は、十分に管理面の評価を行うべきである。

外部設計支援業務は重要事項(2)具体的作業内容で、要件定義書、作業体制、外部設計検討会、委託先等を記述する。(3)パッケージソフトウェアの表示で、バージョン、リビジョン、保守やサポート体制について詳述し、その時点で判明している不具合等があれば記載しておく。(4)設計書、付属文書の一覧で、作成する業務フロー、システム構成、実態関連図などの作成する文書を記述する。特に、外部設計検討会は作成文書に基づきインターフェースや基本設計等をユーザ、ベンダが合同で検討評価するものであり、業務の中核をなすものである。ベンダは、作成する文書の内容を詳しく説明するとともに、どのような作

業をもとに外部設計検討会で何を決定するかを契約時点で明らかにし、外部設計検討会の成果と品質について十分に合意すべきである。準委任契約であるため、ベンダの善管注意義務が課せられていることに留意する。また、成果物の瑕疵については、パッケージソフトウェア固有の瑕疵はパッケージソフトウェア製造会社とユーザの間で解決されるものとし、モディファイ、アドオン部分の瑕疵は、要件定義書、関連文書との不一致の場合、修正責任を負うこととなっている。この場合、ユーザが要件定義書、外部設計書に記述されていない操作を行った場合の不具合が問題となる。契約にあたってベンダは要件定義書に基づく外部設計上の不明点を十分に解消し、設計にあたるとともに、表記にない場合に備え、操作規約[22]、開発標準規約[23]等をユーザと合意することが望まれる。

ソフトウェア設計・制作業務は、重要事項(2)具体的作業内容で要件定義書、外部設計書、開発体制、委託先等を記述する。特に、ベンダの出荷テストである適格性テストについては、テスト体制、合格基準、ユーザデータの仕様の有無についてユーザ、ベンダが合意する必要がある。テスト体制の環境が異なる場合、ベンダ出荷では合格、ユーザ環境では不合格となるケースが想定されるためである。定められたテスト期間で、ユーザが適格性テストを実施し、検収が行われる。期間については、ユーザの受入体制を考慮し決定する。(3)パッケージソフトウェアの表示で、バージョン、リビジョン、保守やサポート体制について詳述し、その時点で判明している不具合等があれば記載しておく。(4)納入物の明細で、納入されるプログラムのほか、物理データ設計書、入出力詳細設計書などの作成する文書を記述する。また、納品形体についてはハードウェアとともに納品するか、個別に承認事項や検収がある場合はその条件を明示する。

構築・設定業務は最終的な納品、現地調整作業と、場合によっては既設のシステムとのシステム結合等がなされる。従って、作業によってはネットワーク設定変更で電子メールや Web へのアクセスが一時的に制限される場合や、電源の関係上、既設の機器を一旦停止するなどの場合がある。構築・設定業務契約の重要事項(2)具体的作業内容で、「関連するシステムの停止等の条件」を明記し、ユーザの業務への影響をあらかじめ合意することが望ましい。さらに、他システムの結合がある場合、ソフトウェア設計・制作業務でシステム結合を実施するか、構築・設定業務で実施するか、結合される側の設定等を含むか、システム結合の際の障害切り分けを含むかなど、業務の範囲と責任体制が明らかになるように(2)具体的作業内容で記述する。構築・設定に関する仕様書、テスト仕様書がある場合は、その仕様書を付属文書として添付し、実施内容を説明しなければならない。構築・設定に関する仕様書と実作業の乖離があった場合、保守、運用に備え、また、運用マニュアルや利用者文書作成においてそれらが反映できるよう、構築・設定業務設定報告書において実際の設定内容が記載され、ユーザに承認されなければならない。仕様との不一致は「瑕疵」となり修正請求を受けることとなるので留意する。

G データ移行支援業務契約

データ移行支援業務は、重要事項「パッケージ候補のシステム要件評価」において移行要件を含むとしてあり評価済みであることから、要件定義に基づく仕様に基づき作業が実施される。データ移行支援業務の重要事項(2)及び(3)具体的作業内容で「移行するデータの

[22] 操作で割り当てられていないキーボードを無効にしておく、画面遷移の定義が無い場合は直前の画面にのみ戻る等の措置。

[23] ファイルの命名法、コーディングにおける変数の制限・使用法、コメントの規約など、開発上の作法をまとめたもの。

範囲」、「移行のための抽出作業」、「移行のための変換作業」、「新システムへの移行」を詳述するが、仕様が記述できない場合は、相当するシステム要件定義書等を指定する。作業に伴うデータのバックアップ等は付帯事項として、移行に伴う現行システムの停止などは特約条項として記述する。

プログラムの納品は、ベンダ側で仕様書に基づく適格性テストを実施した後に納品し、ユーザ側でも同様の適格性テストを実施することを想定している。オープンシステムでの開発は開発環境を全く同一にすることが困難な状況があるためである。構築・設定業務においては、システム結合に備え、仕様書に定めたテストを実施することを想定している。また、業務要件、システム要件に定められたセキュリティ設定は十分な配慮が必要であり、運用において多大な影響を及ぼすため、現場での設定の修正や変更があった場合の変更承認や文書化のルール作りが重要となる。適格性テスト及び構築・設定業務設定報告書でのセキュリティ設定の確認は、ユーザの検収プロセスを含めたチェック体制を検討すべきである。

H 運用テスト支援業務契約、I 導入教育支援業務契約締結

運用テスト支援業務は、直接実運用に供する実運用環境での実施を想定しており、実際の利用者が実施することを想定し、準委任契約としている。実際の利用者がテストを実施することで、利用者文書の改訂や問題の発見につながるためである。テスト実施にあたっては、運用にかかわる作業手順が確立されている必要がある。要件定義書、外部設計書、構築・設定業務報告書等の文書を検討し、実際に運用に資する文書を作成し、その文書を基に、テスト仕様書の策定がなされるべきである。

運用にかかわる作業手順の確立では、日次業務開始から終了、月次、年次など期間特有の処理、停電や異常終了した際の対処方法、記憶領域が不足した場合の対処、バックアップ及び復旧の手順、OS やアプリケーションの修正プログラムの適用がなされた場合など多岐にわたる。併せて、顧客データの一括出力やマスタデータの登録変更など、業務上の権限管理や個人情報、セキュリティに関わる事項についての運用手順、利用者文書は、情報管理規定等の社内規則との整合性も確認されなければならない。また、ウイルスが発見された場合の対応手順や運用にかかる問い合わせなど、運用支援業務との関わりを含めて総合的に検討、策定されることが望ましい。

導入教育支援業務は、個別の操作指導、集合教育、E-learning などさまざまな提供方法が想定される。また、ユーザのリテラシによって内容が大きく異なることが予想されるため、ユーザリテラシについての事前の合意が重要である。

J 保守業務契約、K 運用支援業務契約

保守業務契約については、外部設計段階やソフトウェア設計・制作段階でパッケージソフトウェアを導入した場合にはすでに開始されている場合がある。いずれも、SLA に基づく保守業務内容の事前合意が重要である。また、ネットワークを含むシステム全体の障害切り分けを委託する場合は、保守業務契約の重要事項(1) において、保守業務の範囲とともに不具合の調査費用についての取り決めが必要となる。ネットワークによって導入したシステムの設定がそれ以外のシステムに影響を及ぼす場合があり、またその逆の例もあり、ユーザとベンダの争いの原因となる。

保守業務で交換された故障部品は製造会社に戻され、原因の究明や保守用部品として修理、再生されるのが一般的である。このため、交換された故障部品はベンダに無償で譲渡される規定としている。この際、個人情報を含んだハードディスクが故障した場合、個人情報の漏洩につながるおそれがあるとして、ユーザが故障部品の譲渡を拒むケースがある。プライバシーマーク等を取得しているユーザにおいては、個人情報保護規定と保守業務契約の事前の合意との関係に留意する必要がある。

契約条項、告知事項において、日常のデータのバックアップ作業はユーザ責任としており、ベンダはバックアップがないことによって生じる損害賠償等の責めに応じないとしている。データはユーザ資産であり、ユーザが正しく資産を保管することは当然のことであり、また、ベンダは、データの正当性、正確性について、最終的な判断ができないためである。ベンダはバックアップの重要性について、詳しく説明を行い、ユーザの注意喚起をはかる必要がある。

運用支援業務は、操作、運用に関わるヘルプデスク業務や、機器の動作監視、ウイルス除去といった、直接運用に関わる業務ではなく、周辺の支援業務を想定している。当該業務についても保守契約同様に SLA を締結し、支援業務のサービス提供の具体的な内容を取り決める必要がある。

共通フレーム 2007 とモデル契約の関係

共通フレーム 2007 とモデル契約の関係を以下の表にまとめた。

別紙 1 パッケージカスタマイズ 取引・契約モデル

<table>
<tr><th rowspan="2">共通フレーム 2007</th><th rowspan="2">取引・契約モデルのフェーズ</th><th colspan="2">契約</th></tr>
<tr><th>基本</th><th>重要事項説明書</th></tr>
<tr><td>1.4 企画プロセス
システム化の方向性
システム化計画</td><td>(1)事業要件定義
(2)プロジェクトゴールの策定
(3)要求品質の明確化
(4)パッケージソフトウェアを利用し実現する業務の新全体像の作成（1.4.2.6～1.4.3.7 該当）
(5)パッケージソフトウェアベンダに対してシステム、パッケージソフトウェア等の情報提供要求、試算見積依頼（RFI）
(6)ユーザに対し RFI に基づくシステム、パッケージソフトウェア等の情報の提供、試算見積の提示</td><td rowspan="8">パッケージソフトウェア利用コンピュータシステム構築支援契約書</td><td rowspan="2">A 要件定義支援及びパッケージソフトウェア候補選定支援業務契約（カスタマイズモデル）</td></tr>
<tr><td rowspan="2">1.5 要件定義プロセス
要件定義</td><td>(7)業務要件定義（1.5.2.4 機能要件、1.5.2.5 非機能要件を含む）
(8)ベンダに対しパッケージソフトウェア候補選定のための情報提供依頼（RFI）
(9)ユーザに対し RFI に基づくパッケージソフトウェア関連情報の提供、概算見積の提示
(10)パッケージソフトウェアの機能要件、非機能要件、使用許諾契約(利用条件、保守等) 、SaaS/ASP においては SLA の検討
(11)パッケージソフトウェア候補の選定
(12)業務要件及び適合するパッケージソフトウェア候補の報告書の提出
(13)受入れ</td></tr>
<tr><td>(14)使用許諾によってはパッケージ、OS、ハードの導入及び保守の開始
(15)パッケージ候補のシステム要件評価
(16)API の実現性の確認（候補パッケージの API、既存システムとの接続性等の評価）
(17)パッケージソフトウェアの選定と要件定義、システム要件定義と評価</td><td>B パッケージソフトウェア選定支援及び要件定義支援業務契約（カスタマイズモデル）</td></tr>
<tr><td>1.6 開発プロセス
システム要件定義
システム方式設計
ソフトウェア要件定義
ソフトウェア方式設計</td><td>(21)使用許諾によってはパッケージソフトウェア、OS、ハードウェアの導入及び保守の開始
(22)モディファイの範囲、アドオン等の外部設計範囲の確定、及びそれに伴うユーザ I/F・他システム I/F 設計
(23)外部設計書の承認(受入れ)</td><td>D 外部設計支援業務契約</td></tr>
<tr><td rowspan="2">1.6 開発プロセス
ソフトウェア詳細設計、ソフトウェアコード作成及びテスト、ソフトウェア結合、システム結合、システム適格性確認テスト、ソフトウェア導入、受け入れ支援</td><td>(25)ソフトウェア設計
(26)モディファイ、アドオンの設計、プログラミング、ソフトウェアテスト
(27)適格性確認テスト、監査、ソフトウェア導入
(28)納品
(29)検収（受入れ）</td><td>E ソフトウェア設計・制作業務契約</td></tr>
<tr><td>(30)構築・設定業務（機器・OS 等の設定、納品）
(31)システム結合、テスト
(32)検収（受入れ）</td><td>F 構築・設定業務契約</td></tr>
<tr><td>1.7 運用プロセス
業務及びシステムの移行</td><td>(33)データ移行
(34)完了報告(受け入れ)</td><td>G データ移行支援業務契約</td></tr>
</table>

運用テスト 利用者教育	(35)運用に関わる作業手順の確立 (36)運用テスト (37)完了報告(受け入れ)		H 運用テスト支援業務契約
	(38)利用者導入教育 (39)完了報告（受け入れ）		I 導入教育支援契約
1.8 保守 問題把握及び修正分析、修正の実施、保守レビュー及び受入れ	(41)ハードウェア保守、カスタマイズ部分保守開始		J 保守業務契約
1.7 運用プロセス 業務運用と利用者支援	(42)運用支援		K 運用支援業務契約

別紙 2 パッケージオプション 取引・契約モデル

共通フレーム 2007	取引・契約モデルのフェーズ	契約	
		基本	重要事項説明書
1.4 企画プロセス システム化の方向性 システム化計画	(1)事業要件定義 (2)プロジェクトゴールの策定 (3)要求品質の明確化 (4)パッケージソフトウェアを利用し実現する業務の新全体像の作成（1.4.2.6～1.4.3.7 該当） (5)パッケージベンダに対してシステム、パッケージソフトウェア等の情報提供要求、試算見積依頼（RFI） (6)ユーザに対し RFI に基づくシステム、パッケージソフトウェア等の情報の提供、試算見積の提示	パッケージソフトウェア利用コンピュータシステム構築支援契約書	C　パッケージソフトウェア選定支援及び要件定義支援業務契約(オプションモデル)
1.5 要件定義プロセス 要件定義	(7)業務要件定義 (10)パッケージソフトウェアの機能要件、非機能要件、使用許諾契約(利用条件、保守等) 、SaaS/ASP においては SLA の検討 (11)パッケージソフトウェア候補の選定		
	(14)使用許諾によってはパッケージソフトウェア、OS、ハードウェアの導入及び保守の開始 (15)パッケージ候補のシステム要件評価 (16)API 実現性の確認（候補パッケージの API、既存システムとの接続性等の評価） (17)パッケージソフトウェアの選定と要件定義、システム要件定義と評価		
1.6 開発プロセス システム要件定義 システム方式設計 ソフトウェア要件定義 ソフトウェア方式設計	(21)使用許諾によってはパッケージソフトウェア、OS、ハードウェアの導入及び保守の開始 (22)外部プログラムの機能の確定、及びそれに伴うユーザ I/F・他システム I/F 設計 (23)外部設計書の承認(受入れ)		D 外部設計支援業務契約
1.6 開発プロセス ソフトウェア詳細設計、ソフトウェアコード作成及びテスト、ソフトウェア結合、システム結合、システム適格性確認テスト、ソフトウェア導入、受け入れ支援	(25)ソフトウェア設計 (26)外部プログラムの設計、プログラミング、ソフトウェアテスト (27)適格性確認テスト、監査、ソフトウェア導入 (28)納品 (29)検収（受入れ）		E ソフトウェア設計・制作業務契約

1.7 運用プロセス 業務及びシステムの移行 運用テスト 利用者教育	(30)構築・設定業務（機器・OS 等の設定、納品） (31)システム結合、テスト (32)検収（受入れ）		F 構築・設定業務契約
1.7 運用プロセス 業務及びシステムの移行 運用テスト 利用者教育	(33)データ移行 (34)完了報告(受け入れ)		G データ移行支援業務契約
	(35)運用に関わる作業手順の確立 (36)運用テスト (37)完了報告（受け入れ）		H 運用テスト支援業務契約
1.8 保守 問題把握及び修正分析､修正の実施､保守レビュー及び受入れ	(38)利用者導入教育 (39)完了報告（受け入れ）		I 導入教育支援契約
1.8 保守 問題把握及び修正分析､修正の実施､保守レビュー及び受入れ	(41)ハードウェア保守、外部プログラム等保守開始		J 保守業務契約
1.7 運用プロセス 業務運用と利用者支援	(42)運用支援		K 運用支援業務契約

以下、別紙 1 パッケージカスタマイズ取引・契約モデルと共通フレームのポイントを解説する。別紙 2 については、各ポイントを参考し準用されたい。

最初のプロセスである「業務要件定義プロセス」の目的は、共通フレーム 2007 における「1.4 企画プロセス」と「1.5 要件定義プロセス」の成果を得ることにある。

■1.4　企画プロセスの成果：
(1)経営層及び各部門からシステムに関係する要求事項が集められ、かつ、合意される。(2)要求事項に基づいたシステム化の範囲及びシステム構成、基本的なアーキテクチャが定義される。(3)システムを実現する実施計画が策定され、かつ、合意する。

■1.5　要件定義プロセスの成果：
ユーザの利害関係者間で
(1)対象システムを含む業務、組織に関する要件が定義され、かつ合意される。(2)システムに対する要件及び制約事項が定義され、かつ合意される。(3)定義された要件と、プロセスの入力となった要求事項との整合性が保たれる。

■契約の開始：
調査手法、分析手法、範囲とともに場所や設備などの付帯事項が確定しており、途中報告書、最終報告書の様式、量、日程などの全体計画が立案されユーザと合意している状態にある。

■契約の終了：
業務要件定義に基づき、システム化する機能が精査決定され、パッケージソフトウェアが選定され、モディファイやアドオン部分の外部設計が可能な状態にある。RFP を提示することで、開発、保守、運用の費用を含めた全体的な見積が得られる状態にある。

プロセス開始に当たっては、以下のドキュメントを参照するとよい。

■参考ドキュメント：
1.コンサルティング会社選定のためのチェックリスト
3.業務システム仕様書の記述レベル
4.ユーザ IT 成熟度チェックリスト
9.セキュリティチェックシート 一般版（上位概念）
10.セキュリティチェックシート Web アプリケーション版

(2)「プロジェクトゴールの策定」から(6)「ユーザに対し RFI に基づくシステム、パッケージソフトウェア等の情報の提供、試算見積の提示」は、共通フレーム 2007「1.4.2 システム化構想の立案」、「1.4.3 システム化計画の立案」に相当する。特に、「1.4.2.6 業務の新全体像の作成」から、「1.4.3.6 業務モデルの策定」「1.4.3.7 システム化機能の整理とシステム化方式の策定」「1.4.3.8 システム化に必要な付帯機能、付帯設備に対する基本方針の明確化」がスパイラル的に検討されることを想定している。プロセス初期はユーザに知見が乏しいことから、他社動向やパッケージソフトウェアの機能や知見を得ることで、プロジェクトゴールが随時変更されることを前提としている。ただし、プロジェクトゴールはコストと制約条件でコントロールされるべきで、闇雲な拡大を狙うものではない。結果としてシステム化が実現可能な業務の絞り込みがなされることを期待している。

(3)「要求品質の明確化」はユーザが顧客に提供する業務の品質が上位にあり、それを支えるための情報システムの品質としてとらえるべきである。とはいえ、情報システム構築の経験が少ないユーザは、業務品質を特段に意識していることが少ないといえるので、早期に共通フレーム 2007「1.4.3.9 サービスレベルと品質に対する基本方針の明確化」[24] 等で要件を明確化するように努める。これらによって非機能要件の先送りを防止することが可能となる。信頼性の観点から、システムの停止が業務に与える影響の評価、セキュリティの観点から個人情報や企業情報の漏洩の影響の評価、保守性の観点から誤操作や障害発生時のユーザの対応できる範囲を具体的に議論することが望まれる。

(4)「パッケージソフトウェアを利用し実現する業務の新全体像の作成」は、最終的に共通フレーム 2007「1.4.2.6 業務の新全体像の作成」に相当する。(4)を作成した後の、(6)「ユーザに対し RFI に基づくシステム、パッケージ等の情報の提供、試算見積の提示」でコスト評価を行い費用対効果についての意識を持つことは、ユーザの過大な要求を適正化することにも寄与し、かつ信頼性向上にも大きく関与する。口頭による曖昧な合意の排除、要件の先送りを防止するため、変更管理手続による未決定事項の管理を実施し、議事録の採番、記述様式、手交の方法を取り決めることが必要である。

ユーザは利用者からの幅広い聞き取りを実施し、操作性の向上や要求漏れによる手戻りの防止に努めるべきである。その際、ベンダは、具体的な画面イメージや画面遷移などのシステムの流れの説明に努め、業務の流れとシステムの流れをユーザに理解される工夫が必要である。この段階での要件の先送りを極力減らすことは、信頼性確保の重要なポイントとなる。機能比較が行われることで、新たに開発し実装すべき不足部分が明確となっている。また、既存システムとの接続や移行があり得る場合は、既存システムの調査や、接続性、移行性の難易度についても検討を加えておく。「1.4.3.8 システム化に必要な付帯機能、

[24] 共通フレームは工程や時間に依存して定義されたものではない。共通フレームの項番は順序や時間関係を規定していないことに留意する。（共通フレーム 2007、23p を参照）

付帯設備に対する基本方針の明確化」は、プロジェクトの範囲、全体の工数に多大な影響を及ぼし、コスト、期間、構築の難易度を左右する。

(7)「業務要件定義」以降のフェーズは、費用対効果に基づく優先順位付けの検討に留意したい。ユーザの業種、業務の特殊性や独自性が高い場合、パッケージソフトウェアの評価段階で、パッケージソフトウェアの機能不足に着目し、モディファイやアドオンの範囲が過大になりがちとなる。一般的にコストをかければパッケージソフトウェアの適合性は高まるが、反面、パッケージソフトウェアを導入する経済合理性が失われてしまう可能性も高くなる。また、過大な要求は、次のフェーズにおいてパッケージソフトウェアの変更費用の増加となって現れる可能性が高くなる。さらには、パッケージソフトウェア本体の根本的改造といった信頼性、経済性を大きく損なう要因になる。業種、業務の特殊性に関わらず、状況が許す限り極力モディファイ、アドオンの作成を避けるという方針の維持が重要である。

(8)「ベンダに対しパッケージソフトウェア候補選定のための情報提供依頼（RFI)」、(9)「RFI に基づくパッケージソフトウェア関連情報、見積の提供」は、パッケージソフトウェアに実装されている機能情報、価格情報をもとに、(10)「パッケージソフトウェアの機能要件、非機能要件、使用許諾契約の検討」[25]、(11)「パッケージソフトウェア候補の選定」の実施に重大な影響を及ぼす。業務要件定義支援契約全般における品質に関与する事と環境適合を念頭に、必要に応じて繰り返し実行してもよい。共通フレーム 2007「1.4.3.5 適用技術の調査」及び「1.4.3.14 費用とシステム投資効果の予測」が該当する。

(12)「業務要件及び適合するパッケージソフトウェア候補の報告書の提出」は、ユーザの要望を基に、新しい業務のあり方や要員などの運用要件、導入方針やスケジュール、機能要件、セキュリティを含む非機能要件を確定する。さらに、これらの要件を実現すると思われるパッケージソフトウェア候補は、使用許諾契約、バージョンアップ、保守性なども考慮されて選定されることを期待している。運用にあたっての問い合わせ窓口の情報、サポート契約などは、運用コストに直結するため、十分な情報提供が望まれる。

(15)「パッケージ候補のシステム要件評価」以降ではパッケージソフトウェアが要求するシステムの機能及び能力、設計条件、開発環境などの技術的要素だけでなく、利用者の要件やインターフェース、操作及び保守要件など、運用や保守についても詳細な評価がなされることが重要である。SaaS/ASP においては、経済産業省 SaaS 向け SLA ガイドラインの別表 SaaS 向け SLA におけるサービスレベル項目のモデルケースを参考に、事業者が提供している SLA について評価する。この際、可用性、信頼性はもとより、クライアント端末での性能確保について評価が必要である。共通フレーム 2007「1.5.2.3 機能要件定義」、「「1.5.2.4 非機能要件定義」」が該当する。これ以降、口頭による曖昧な合意を排除するため、変更管理手続による未決定事項の管理、議事録の手交を取り決めることが望ましい。なお、この時点でバックアップや、サーバーの構成などすべてのシステム全体の構成を決定するのではないことから「1.6.2 システム要件定義」とは異なることに留意する。

(16)「API の実現性の確認」は、モディファイやアドオンの実現性の評価となるため、個別具体的な技術的検討が必要である。また、既存システムとの接続がある場合、その接続性の評価、既存システムの改造等の評価も含まれる。ここで、プロジェクト全体の範囲、要素が抽出されるため、既存システム、パッケージソフトウェアに精通したエンジニアの

[25] SaaS/ASP においては、SLA の詳細な検討、回線の冗長化等の信頼性確保の検討等が含まれることに留意する。

参画、もしくはパッケージソフトウェア製造会社の協力が必要となる。

（17)「パッケージソフトウェアの選定と要件定義、システム要件と評価」では、パッケージソフトウェア候補に対する機能要件、非機能要件の過不足評価だけで終わることなく、コストを前提とした利用者要件、環境適合、セキュリティ、運用、保守、移行、使用許諾契約、SLA なども要件として定義される。特に、使用許諾契約はパッケージソフトウェア製造会社とユーザの個別契約であり、かつ、パッケージソフトウェア本体の使用上の権利や瑕疵の扱いなどが決定されるため、細部にわたる慎重な評価が求められる。パッケージソフトウェアの選定によって手作業部分とシステム要件（機能要件、非機能要件[26]）のほとんどが決定されるため、様々な視点からの評価が重要となるため、直接的な利用者や利害関係者のレビューが重要である。各評価のポイントは、ユーザとベンダにおいて合意された重み付けがなされていることが望ましい。場合によっては(15)〜(17)が繰り返される。(17)「パッケージソフトウェアの選定と要件定義、システム要件と評価」以降の要件の未決事項は実装が困難となるため、変更管理手続に則り処理を決定する必要がある。外部設計以降に要件の追加や範囲の拡大などが発生しないよう、ユーザ、ベンダの慎重な検討と合意を図るべきである。

この後、(19)「ベンダへの見積要求」によってベンダから見積を得ることとなるが、その際、ベンダにどこまでの業務を依頼するかによって、コスト及び精度が異なってくる。パッケージに関わる開発行為なのか、接続すべき既存システムがある場合や移行を伴うかなどの範囲を明確にし、RFP の内容精度の向上に努めるべきである。RFP の内容が不明確、不明朗であることで、受託後の調査工数が上乗せされ本来不要なコストが発生したり、見積に失敗する大きな原因になることを留意する。

「設計・制作・テスト・移行プロセス」では、共通フレーム 2007 の「1.6.2 ソフトウェア詳細設計」から「1.6.13 ソフトウェア受け入れ支援」と、「1.7.2 運用テスト」、「1.7.3 業務及びシステムの移行」、「1.7.5 利用者教育」を想定しており、「1.6 開発プロセス」と「1.7 運用プロセス」の成果の一部を得ることにある。

■1.6 開発プロセスの成果：
(1)ソフトウェア開発の要件が収集され、合意されている。(2)ソフトウェア製品及び／又はソフトウェアを中心とするシステムが開発されている。(3)最終製品が要件に基づくことを示す中間作業成果が開発されている。(4)開発プロセスでの製品間で一貫性が確立されている。(5)システム品質要因がシステム要件（例えば、速度、開発費用、使用性など）に照らして最適化されている。(6)最終製品が要求事項を満たすことを示す証拠（例えばテストの証拠）が存在している。(7)最終製品が合意した要求事項に従って導入されている。

■1.7 運用プロセスの成果：
(1)ソフトウェアの正しい運用の条件が、意図された環境下で識別され、評価されている。(2)ソフトウェア及び業務が、意図された環境下で運用されている。(3)ソフトウェア製品の顧客に援助及び相談が、契約に従って提供されている。

■契約の開始：
要件定義書、外部設計書の実現可能性を含めた総合的な評価が完了し、す

---

[26] SaaS/ASP においては SLA も含む。

べての利害関係者の中で、用語、要求の定義等について疑義が無い状況であることが確認されており、詳細工程の日程を含む全体計画が立案され評価がすんでいる状態にある。

■契約の終了：

要件に従って選択されたパッケージソフトウェア（モディファイ部分を含む)、もしくはアドオンプログラムが、ソフトウェア設計・制作業務で示された適格性テストを合格し稼働する状態でユーザに納品され、既存のシステムからのデータ移行がある場合は、データ移行が完了している状態にある。サーバ、クライアント、ネットワークの構築、設定、システム結合がある場合、これらが完了している状態にある。

プロセス開始に当たっては、以下のドキュメントを参照するとよい。

■参考ドキュメント：

3.業務システム仕様書の記述レベル
7.検収事前チェックリスト
8.検収チェックリスト
9.セキュリティチェックシート 一般版（上位概念）
10.セキュリティチェックシート Web アプリケーション版

---

(17) までの要件定義を行ったベンダと、(21)以降の外部設計支援を行うベンダが異なる場合については留意が必要である。(17)までの要件定義を担当したベンダは、(21)以降の外部設計支援を行うベンダが全体計画を策定し作業着手できるまでは、必要な打ち合わせ、問い合わせの対応を業務の責任範囲とし、合理的な範囲で疑義解消を業務範囲とすべきである。また、いずれの契約類型も準委任契約であることから、ユーザはベンダ同士の解決に頼らず自らも疑義解消に努め要件の精度向上を担うべきである。

(21)「使用許諾によってはパッケージソフトウェア、OS、ハードウェアの導入及び保守の開始」は、(22)「モディファイ、アドオンの範囲の確定、及びそれに伴うユーザ I/F・他システム I/F 設計」を実行する際に、パッケージソフトウェアそのものの導入が必要なケースを想定している。モディファイの範囲決定のためにソースコードの調査が必要で、パッケージソフトウェア製造会社が無償で調査を実施しないケースがこれに該当する。この時点でパッケージソフトウェアと調査のための動作環境を購入しなければならない。この場合、(30)「構築・設定業務」、(31)「システム結合、テスト」、(32)「検収」の一部が発生する。

(22)「モディファイ、アドオンの範囲の確定、及びそれに伴うユーザ I/F・他システム I/F 設計」[27]では、パッケージソフトウェア本体へのモディファイを実施する場合の詳細範囲の決定や、不足している入出力機能、画面・帳票のデザイン、画面遷移、操作性、他システムとの接続がある場合は、そのインターフェースなどが要件定義書に基づき設計される。ユーザに対して画面遷移を含むデザインレビューは手戻りを防止する上で重要である。[28]

---

[27] 別紙 2 パッケージオプション 取引・契約モデルでは、「(22)外部プログラムの範囲の確定、及びそれに伴うユーザ I/F・他システム I/F 設計」となる。

[28] モデル取引・契約書第一版においても、外部設計から内部設計にかけての仕様の「深化」「詳

この時点で未決定事項の最終的な処理決定が必要となる。共通フレーム 2007「1.6.4 ソフトウェア要件定義」が該当する。また、併せて「1.6.5.4 利用者文書(暫定版)の作成」を実施し、ユーザの理解を深めることが望ましい。運用マニュアル作成、運用テストの重要な関連ドキュメントとなる。モディファイが伴う場合は、範囲を最小限にするとともに、不具合対応、信頼性、保守性の観点からパッケージソフトウェア製造会社との協業もしくは、サポート契約の締結を検討すべきである。また、将来にわたってのパッケージソフトウェア本体のバージョンアップが困難になる可能性があること、将来にわたって保守のためにソースコードに変更を加える場合の管理方法とコストを慎重に検討し、ユーザと文書で合意すべきである。

重要な留意点として、(22)「モディファイ、アドオンの範囲確定、及びそれに伴うユーザ I/F・他システム I/F 設計」において、パッケージソフトウェアによる要件の達成が困難又は大幅なコスト超過が判断された場合の手戻り対応が想定される。かかる事態は事実上のプロジェクトの破綻であり、要件定義プロセスの失敗を意味する。そのため要件定義業務とソフトウェア設計・制作業務が異なるベンダで契約される場合は、ソフトウェア設計・制作契約の停止条件や、業務要件定義の見直しなどの手戻りによって発生する費用の負担などの取り決めが重要となる。

(23)外部設計書の承認（受入れ）で、ユーザの画面等の承認を得た後、(25)「ソフトウェア設計」で、要件定義書、外部設計書に基づき、それ以降の開発全体のプロジェクト計画が立案され、各コンポーネント、インターフェース、データベースの詳細設計がなされ、併せて利用者向けのマニュアルの作成とコンポーネントのテスト、結合テストの要求事項がまとめられる。共通フレーム 2007「1.6.6 ソフトウェア詳細設計」が該当する。

(26)「モディファイ、アドオンの設計、プログラミング、ソフトウェアテスト」[29]は、いわゆるコンポーネントのプログラミング、コンポーネントの結合、テストとシステム結合（ハードウェアへの導入、他システムとの接続等）の一部である。共通フレーム 2007「1.6.7 ソフトウェアコード作成及びテスト」、「1.6.8 ソフトウェア結合」、「1.6.9 ソフトウェア適格性確認テスト」、「1.6.10 システム結合」までが該当する。ここでシステム結合の一部と限定したのは、ソフトウェアテストを実現するための環境構築及びシステム結合であり、他システムとの連携を含めた全体のシステム結合は(30)「構築・設定業務（機器・OS 等の設定、納品）」～(32)「検収（受入れ）」でなされることを想定しているためである。

それぞれの工程で、業務要件定義書、外部設計書、全体計画が常に参照され、利用者文書のアップデートがなされるとともに、最終的にはシステム適格性テストのテストケースとテストデータまでが準備される。モディファイにあたっては、将来にわたっての保守性を維持することを目的としたソースコード、変更履歴が保存され、履歴と目的がまとめられた変更状況報告書が文書化されることを期待している。

(27)「適格性確認テスト、監査、ソフトウェア導入」では、要件定義書に定められたテスト方法、テストデータを基にシステム要件が実現され納品可能な状態になる。テストは納品実機で実施されることが望ましいが、困難な場合は、実機相当品を準備し、OS 等の環境を同一にすることが必要であり、(29)「検収（受入れ）」でも(27)の適格性確認テストの仕様に基づくテストを実施する必要がある。共通フレーム 2007「1.6.11 システム適格性確認

細化」に伴う前提条件の変動が指摘されている。

[29] 別紙 2 パッケージオプション 取引・契約モデルでは、「(26)外部プログラムの設計、プログラミング、ソフトウェアテスト」となる。

テスト」が該当する。

(30)「構築・設定業務（機器・OS 等の設定、納品）」～(32)「検収（受入れ）」は外部設計、ソフトウェア設計・制作に並ぶ重要なプロセスである。このプロセスによってサーバ、機器、ネットワーク等の設定、構築並びにシステム結合が実施され、運用の一歩手前の状態となる。(30)「構築・設定業務（機器・OS 等の設定、納品）」～(31)「システム結合、テスト」では、サーバ、クライアントの OS、ネットワーク、セキュリティの設定、個別の機器の設定、他システムとの結合などが実施される。既設のシステムがある場合は、事前の調査に基づいて、業務の中断や処理の停止等を考慮し、設置計画を立案、承認されることが求められる。また、電源、空調等の環境も併せて考慮されることを期待している。ユーザ、ベンダは合意の上、(29)「検収（受入れ）」、(31)「システム結合、テスト」、(32)「検収（受入れ）」を一つのプロセスとし、システム適格性確認テストを再現し、要件定義書に基づいた条件で検収を受けてもよい。「E ソフトウェア設計・制作契約」の納期とテスト期間、「F 構築・設定業務契約」の構築・設定業務報告書提出期限とテスト期間を同一にすればよい。構築・設定業務契約で留意が必要なのは、構築・設定に関する仕様書通りに設置調整ができなかった場合である。運用マニュアルの作成や、セキュリティに多大な影響を及ぼす可能性もあることから、構築・設定に関する仕様書と異なる設定を行う際の承認方法や、構築・設定業務設定報告書の作成、記述については注意が必要である。共通フレーム 2007「1.6.12 ソフトウェア導入」、「1.6.13 ソフトウェア受入れ支援」が該当する。

(33) 「データ移行」では、データ移行支援契約に基づき、顧客のシステム現況から移行対象となるデータが確定され、抽出、変換、移行の作業が支援される。移行対象のデータについては、十分に事前の打ち合わせを行い、マスタのみとするか、トランザクションも含めるか、慎重な検討がなされるべきである。あわせて、コード体系、外字、異体字の取扱い、半角、全角等の取扱いを定める必要がある。変換のためのプログラミングが必要な場合は、要件定義書を策定し、(25)ソフトウェア設計以降の手順を踏まなければならない。また、トランザクションを含むとすれば、どの時点までのデータとするかが詳細に検討されなければならない。現行システムの停止や保全のためのバックアップ、移行に至る実施手順シミュレーションが必要となる。共通フレーム 2007「1.7.3 業務及びシステムの移行」が該当する。

(35)「運用に関わる作業手順の確立」 は共通フレーム 2007「1.7.1.3 運用時の問題管理手続きの確立」「1.7.1.4 システム運用に関わる事前調整」「1.7.1.5 システム運用に関わる作業手順の確立」を想定している。運用手順が確立されていないと、運用テスト計画の策定が困難なためである。

(36)「運用テスト」では、一般的な運用状況と例外処理、エラー処理を想定した運用テスト計画書を策定し評価する。運用テスト計画書においては、実際の業務シナリオに基づき、確認項目、実施方法、確認内容、テストデータが定義されなければならない。運用テスト計画書が承認されたら、要件通りの動作（入出力、画面遷移等）がなされることを、運用テスト計画書に基づいて確認する。業務ピークや、月次や年次における特有の処理などがある場合は実際のデータが用意され、実態に即して実行されなければならない。印刷時のエラー処理や通常業務で想定されない処理についても、運用テスト計画書において想定する必要がある。共通フレーム 2007「1.7.1.10 運用テスト計画の作成」「1.7.2 運用テスト」が該当する。

(38) 「利用者導入教育」では、実際の環境もしくは同等の環境での操作の習得、障害発生時の対応等の教育である。利用者の IT リテラシを考慮し、利用者文書に基づき、日常の操作と、月次・年次処理や障害時の操作、対応、措置、連絡等を習得し、単独で操作が遂

行されることを期待している。共通フレーム 2007「1.7.5 利用者教育」が該当する。なお、この段階で利用者文書の改訂や見直しを図る場合もあるため、その場合は、教育計画において事前の合意を得ておく。

（別紙 1、別紙 2 共通：「1.7 運用プロセス」「1.8 保守プロセス」のポイント）

「1.7 運用プロセス」「1.8 保守プロセス」では、共通フレーム 2007 の「1.7.4 システム運用」、「1.7.6 業務運用と利用者支援」、「1.8.2 問題把握及び修正分析」、「1.8.3 修正の実施」、「1.8.4 保守レビュー及び受入れ」 を想定しており、「1.7 運用プロセス」と「1.8 保守プロセス」の成果の一部を得ることにある。

■1.7　運用プロセスの成果：

(1)ソフトウェアの正しい運用の条件が、意図した環境下で識別され、評価されている。(2)ソフトウェア及び業務が、意図された環境下で運用されている。(3)ソフトウェア製品の顧客に援助及び相談が、契約に従って提供されている。

■1.8 保守プロセスの成果：

(1)リリース戦略に従って製品の修正、移行及び廃棄を管理するために、保守の戦略が、作成されている。(2)現行システムへの組織上、運用上又はインターフェース上の変更の影響が、識別されている。(3)影響されたシステム／ソフトウェアの文書は、必要に応じて更新されている。(4)修正された製品が、要件を損ねていないことを示すテストを重ねた上で作成されている。 (5)製品のアップグレードが、顧客の環境へ移行されている。(6)要求に応じて、製品が、顧客の混乱を最小限にする管理された方法で廃棄されている。(7)システム／ソフトウェアの修正が影響を受けるすべての関係者に伝達されている。

■契約の開始：

運用テストが終了し、ソフトウェア要件、システム要件がすべて決定され、瑕疵がない、もしくは解決される状態にある。ただし、これ以前に保守開始となった場合や、個別の判断で開始となった場合はこれに限らない。

■プロセスの終了：

すべてのソフトウェア、システムは適切に運用、保守され正常に動作しており、廃棄のプロセスに移行する直前の段階の状態にある。

---

(41)「ハード保守、カスタマイズ部分保守開始」では、指定されたハードウェア、アドオン、モディファイされたパッケージソフトウェアの保守が開始される。パッケージソフトウェア本体の保守は、パッケージソフトウェア製造会社との契約でなされるため、必要に応じて個別契約を締結する。保守の範囲、期間、金額とともに SLA 合意書で受付時間、応答時間、復旧時間等を定義し、測定可能なサービス内容として合意する。共通フレーム 2007「1.8.2 問題把握及び修正分析」、「1.8.3 修正の実施」、「1.8.4 保守レビュー及び受入れ」が該当する。保守を受けた場合の変更履歴は、ベンダ、ユーザともに保管されなければならない。SLA 締結において文書様式をあらかじめ合意しておくことが重要である。

(42)「運用支援」では、サーバやネットワーク機器の遠隔監視、ログ取得、ウイルスやセキュリティ関連のサービス提供が想定される。保守同様に SLA を締結し、具体的に測定可能なサービス内容として合意することを期待している。共通フレーム 2007 の「1.7.6 業務運用と利用者支援」が該当する。

パッケージソフトウェア利用コンピュータシステム構築委託契約書

【対象・前提】

- 契約当事者：IT の専門知識を有しないユーザと、業として情報サービスを提供するベンダを想定

  (例) 委託者（ユーザ）：民間中小・中堅企業、地方自治体、独立行政法人等

  受託者（ベンダ）：情報サービス企業（SIer、ソフト会社、IT コーディネータ等）

  ※対等に交渉力のあるユーザ・ベンダについてはモデル取引・契約書第一版を参照。

- 開発モデル：パッケージ＋カスタマイズ型、パッケージ＋オプション型

  ※モデル取引・契約書第一版「2.(7)パッケージ活用、反復繰り返し型の開発、中小企業等ユーザにおける活用の留意点」を基に、新たに策定したモデル

- 対象システム：財務会計システム、販売管理システム、電子メール、グループウェア、Web システム等の導入、構築・設定、カスタマイズ開発、移行、教育、保守、運用支援

- 対象モデル：パッケージモデル、SaaS/ASP モデル

  ※大規模受託開発についてはモデル取引・契約書第一版を参照。

- プロセス：共通フレーム 2007 に準拠したシステムの企画、要件定義段階、開発段階、運用段階、保守段階の定義による。

- 一括発注の場合に加え、マルチベンダ形態、工程分割発注に対応。

- システム基本契約書はプロジェクトごと、ベンダごとに締結。個別契約はシステム基本契約書の別紙である重要事項説明書をもって締結。

パッケージソフトウェア利用コンピュータシステム構築委託モデル契約書
（システム基本契約書）

委託者＿＿＿＿＿＿＿＿＿＿（以下「ユーザ」という。）と受託者＿＿＿＿＿＿＿＿＿＿（以下「ベンダ」という。）とは、パッケージソフトウェア、SaaS および／もしくは ASP を利用して構築するユーザ向けのコンピュータシステム（以下「本件システム」という。）に係る業務の委託に関して、次のとおり契約（以下「システム基本契約書」という。）を締結する。

（本契約の構造）

第１条　本契約は、システム基本契約書及び以下の業務のうち左欄に☑が記された業務（以下「本件業務」という。）に関する各個別契約書によって構成される。

A　要件定義支援及びパッケージソフトウェア要件定義支援業務契約（カスタマイズモデル）
B　パッケージソフトウェア選定支援及び要件定義支援業務契約（カスタマイズモデル）
C　パッケージソフトウェア選定支援及び要件定義支援業務契約（オプションモデル）
D　外部設計支援業務契約
E　ソフトウェア設計・制作業務契約
F　構築・設定業務契約
G　データ移行支援業務契約
H　運用テスト支援業務契約
I　導入教育支援業務契約
J　保守業務契約
K　運用支援業務契約

2)　前項の各個別契約書は、システム基本契約書と一体となる本件業務に関するそれぞれの別紙重要事項説明書へのユーザ及びベンダによる記名押印をもって締結する。

本モデル契約書は、企画フェーズから保守運用フェーズまでに共通して適用されることを想定しており、本契約書（わかりやすい記載にするため個別契約書を含まない本契約書だけに記載された事項についての契約を「システム基本契約書」と定義している。）は、本件業務の種類に関係なく、すべてに適用される契約条項を定めるものであり、全体の基本契約の役割をはたす。それぞれの本件業務を受託するベンダが異なる場合には、システム基本契約書はベンダごとに作成、締結される。

別紙重要事項説明書は各本件業務についての業務の内容及び個別の契約条項を定めるものであって、各本件業務についての個別契約書の役割をはたすものである。別紙重要事項説明書（個別契約書）は、それぞれの本件業務を担当するベンダごとに作成、締結される。

（契約内容の確定及び変更等）

第２条　本契約（システム契約並びに選択された本件業務についての別紙重要事項説明書によって構成される契約全体を指す）の内容は、以下のとおり確定し、以下の条件に従って変更することができる。

①　ベンダ及びユーザが記名押印した、システム契約並びに別紙重要事項説明書に記載された内容は、ひとつの契約を構成し、そのタイトルの部分に「予約」と記載されていない限り、ベンダ及びユーザを法的に拘束する。

②　別紙重要事項説明書には、確定した契約条件のほかにまだ確定していない契約条件が記載されていることがあり、このうち確定していない契約条件については、そのタイトルの部分に「予約」と記載される。予約と記載された事項についての記載はベンダ及びユーザを法的に拘束するものではない。

③　ベンダが複数の本件業務を担当する場合、ユーザ及びベンダは、最初に遂行すべき本件業務に係る部分については、すべての契約内容を確定させるものとする。

④　ベンダが複数の本件業務を担当する場合で当初複数の重要事項説明書を作成している場合は、ユーザ及びベンダは、最初に遂行すべき本件業務以外に係る重要事項説明書について、それぞれの本件業務の開始時に、具体的業務内容、個別契約条項等の条項の再確認を行い、その時点までにで確定していなかった条項を確定し、また必要に応じて確定されていた条項についての変更を行った上で、当該本件業務に関する契約条件を確定する。この場合における契約条件の確定は、新たに重要事項説明書（以下「改訂版重要事項説明書」という。）を作成しこれにユーザ及びベンダが記名押印することによって行う。

⑤　改訂版重要事項説明書は、これが作成され記名押印されたときから、本契約と一体をなすものとして本契約の内容を規定する効力を生じる。

⑥　④所定の契約条件変更のほか、ユーザ及びベンダの協議により、別紙重要事項説明書（改訂版重要事項説明書を含む。以下同じ。）に記載された条項の変更を行う場合は、ユーザ及びベンダが記名押印した書面によって行うものとする。なお、かかる変更の際には価格及び納期の変更の有無、変更の内容についても協議・合意されるものとする。

⑦　ベンダは、ユーザが前号の変更規定に基づかずに契約条件の変更を行った場合、この変更により生じたことについて、一切の責任を負わない。

同一のベンダが複数の本件業務を受託する場合であっても、システム基本契約書は１通のみを作成することになる。一方、重要事項説明書については、同一のベンダが複数の本件業務を受託する場合は、各本件業務の開始時に、それぞれの本件業務についての内容を確定して作成する。これは、同一のベンダが複数の本件業務を一括して受託する場合であっても、各本件業務の内容は、前工程となる本件業務が実施された結果を反映して決定すべきものであるから、本件業務の区切りごとにその内容を確認する機会を設ける必要があるからである。このような建付けとすることにより多段階契約方式を実現している。

同一のベンダが複数の本件業務を受託する場合に複数の本件業務についての重要事項説明書を当初から作成してしまう場合も考えられる。その際、最初に遂行すべき本件業務に

ついての重要事項説明書にはすべて確定された条項が記載されることになるが、後工程の本件業務についてのいくつかの条項は、暫定見積りを行うためのものであって、これらの条項は確定条項として当事者を拘束するものではない。こうした確定していない条項について暫定的な記載をする場合はかかる条項について「予約」と記載する。、ベンダがこのように予約として記載された条項も、そうした条項が含まれる本件業務が始まる前には前項で説明したようにユーザとベンダがその内容を確認し改訂版重要事項説明書を作成、記名押印することによって確定されていく。

上記のとおり本件業務を開始する時点で、当該本件業務に関する条件はすべて確定しているが、これを当該本件業務の途中で変更する場合は、本条⑥に規定する契約内容変更の手続によることになる。

（協働と役割分担）

第 3 条　ユーザ及びベンダは、双方による共同作業及び各自の分担作業を誠実に実施するとともに、相手方の分担作業の実施に対して誠意をもって協力するものとする。

2)　ユーザ及びベンダ双方による共同作業及び各自の分担作業は、別紙重要事項説明書においてその詳細を定めるものとする。

3)　ユーザ及びベンダは、共同作業及び各自の実施すべき分担作業を遅延し又は実施しない場合若しくは不完全な実施であった場合、それにより相手方に生じた損害の賠償も含め、かかる遅延又は不実施若しくは不完全な実施について相手方に対して責任を負うものとする。

「信頼性ガイドライン」において、「商慣行・契約・法的要素に関する事項」として、「情報システム構築の分業時の役割分担及び責任関係の明確化」が重要である旨指摘されているが、これは、情報システム構築取引の特徴を反映したものである。ソフトウェア開発は、ユーザの業務をコンピュータで処理可能にするものであるところ、その業務はユーザ毎に異なり、ユーザこそがその内容の確定についての権限と責任を負っている。但し、「ユーザの業務」といっても、システム開発業務の着手段階ではユーザの責任者自身も完成形をイメージできていないこともしばしばである。この点で、よくたとえられる建物の建築とは大きな違いがある。ソフトウェア開発業務は建物の建築とは似て非なるものであることを十分理解しておく必要がある。

こうした理由から、ソフトウェア開発は、ユーザとベンダが意思の疎通を図りつつ共同作業及び分担作業を適切に行うことが重要である。しかし、その対象となる業務の範囲は広範で多様なため、しばしば作業項目自体の漏れが生じるし、ユーザ・ベンダ間で互いに「この業務は相手方の責任範囲である」という思惑違いも生じる。これがシステム開発におけるトラブルの原因となる場合も多い。そのため、本モデル契約には、ユーザ・ベンダの役割分担を別紙重要事項説明書において具体的に文書化することとしている。

第 1 項は、システム開発は、ユーザとベンダの共同作業であるという基本認識を確認している。ソフトウェア開発に関する紛争は、このような基本認識の欠如に起因するところが大きい。

第 2 項は、詳細な役割分担については、ユーザ・ベンダ間の個別の状況に応じて、別紙重要事項説明書において定めることとしている。

第 3 項は、各当事者が実施すべき共同作業又は分担作業を怠った場合には、それぞれ責任を負うことになることを確認している。例えば、ユーザが実施すべき共同作業又は分担

作業に関して債務不履行があった場合には、結果としてソフトウェアが完成しなかったとしてもベンダは債務不履行責任を負わないことや、ベンダの債務不履行責任に関する損害賠償請求においてユーザ側の過失相殺事由として勘案すること、さらに場合によってはベンダよりユーザに対する損害賠償請求を行うことなどが考えられる。

（連絡協議会の設置）

第 4 条　ユーザ及びベンダは、本件業務が終了するまでの間、その進捗状況、リスクの管理及び報告、ユーザ及びベンダ双方による共同作業及び各自の分担作業の実施状況、システム仕様書に盛り込むべき内容の確認、問題点の協議及び解決その他本件業務が円滑に遂行できるよう必要な事項を協議するため、連絡協議会を開催するものとする。但し、システム基本契約及び別紙重要事項説明書の内容の変更は第 2 条（契約内容の確定及び変更等）に従ってのみ行うことができるものとする。

2)　連絡協議会は、原則として、別紙重要事項説明書で定める頻度で定期的に開催するものとし、それに加えて、ユーザ又はベンダが必要と認める場合に随時開催するものとする。

3）　連絡協議会には、ユーザ及びベンダ双方の責任者、主任担当者及び責任者が適当と認める者が出席する。また、ユーザ及びベンダは、連絡協議会における協議に必要となる者の出席を相手方に求めることができ、相手方は合理的な理由がある場合を除き、これに応じるものとする。

4）　ベンダは、連絡協議会において、別途ユーザ・ベンダ間にて取り決めた様式による進捗管理報告を作成して提出し、当該進捗管理報告に基づいて進捗状況を確認するとともに、遅延事項の有無、遅延事項があるときはその理由と対応策、推進体制の変更（人員の交代、増減、再委託先の変更など）の要否、セキュリティ対策の履行状況、別紙重要事項説明書の変更を必要とする事由の有無、別紙重要事項説明書の変更を必要とする事由があるときはその内容などの事項を必要に応じて協議し、決定された事項、継続検討とされた事項並びに継続検討事項がある場合は検討スケジュール及び検討を行う当事者等を確認するものとする。

5)　ユーザ及びベンダは、本件業務の遂行に関し連絡協議会で決定された事項について、システム基本契約及び別紙重要事項説明書に反しない限り、これに従わなければならない。

6)　ベンダは、連絡協議会の議事内容及び結果について、書面により議事録を作成し、これをユーザに提出し、その承認を得た後に、ユーザ及びベンダ双方の責任者がこれに記名押印の上、それぞれ 1 部保有するものとする。ベンダは、議事録の原案を原則として連絡協議会の開催日から○日以内に作成して、これをユーザに提出し、ユーザは、これを受領した日から○日以内にその点検を行うこととし、当該期間内に書面により具体的な理由を明示して異議を述べない場合には、ベンダが作成した議事録を承認したものとみなすものとする。

7)　前項の議事録は、少なくとも当該連絡協議会において決定された事項、継続検討とされた事項及び継続検討事項がある場合は、検討スケジュール及び検討を行う当事者の記載を含むものとする。

本条は、ユーザ及びベンダによる連絡協議会の開催を定期的に開催することを定める。

連絡協議会は、プロジェクトの重要事項を検討し、決定していく重要な場であり、ほとんどのソフトウェア開発プロジェクトで設けられている。こうした会議体の運営で重要な

ことは、その場で議論された内容を明確に記録に残しておくことである。具体的には議事録を作成し、それに必要な事項を明確に記載することが求められる。しかし、上手くいかないプロジェクトでは、こうした運用が適切になされていない場合がしばしばある。

第 1 項は、協議会で協議すべき事項について定めた。本モデル契約書では、進捗状況・リスクの管理及び報告、ユーザ及びベンダによる共同作業及び各自の分担作業の実施状況、問題点の協議・解決その他本件業務が円滑に遂行できるよう必要な事項について協議会を開催することとした。

第 2 項は、連絡協議会の開催頻度について、別紙重要事項説明書に基づくことを定める。

第 3 項は、ユーザ及びベンダの責任者及び主任担当者[30]以外の者、例えば、開発担当者やユーザ内の従業員等の出席を認め、相手方の出席要請に応じる義務も明記している。

第 4 項は、ベンダの責任者が、連絡協議会の席上、「進捗管理報告」に基づいて報告を定期的に行う進捗管理を義務づけている。

第 5 項は、連絡協議会で決定した事項が当事者により遵守されなければ無意味であるので、これに従うことを義務づけている。

第 6 項は、協議会の議事録の作成をベンダに義務づけるとともに、ユーザが記名押印を怠る場合に備えてみなし承認規定を設けている。

第 7 項は、議事録の必要的記載事項として、連絡協議会において決定された事項、継続検討とされた事項、継続検討事項がある場合は検討スケジュールと検討を行う当事者の記載を義務づける。

（ユーザがベンダに提供する資料等及びその返還）

第 5 条　ユーザは、ベンダに対し、本件業務に必要な資料、機器、設備等（以下「資料等」という。）の開示、貸与等を行うものとする。

2)　ユーザが前項に基づきベンダに提供した資料等の内容に誤りがあった場合又はユーザが提供すべき資料等の提供を遅延した場合、これらの誤り又は遅延によって生じた費用の増大、完成時期の遅延、瑕疵などの結果について、ベンダは責任を負わない。

3)　ベンダは、ユーザから提供を受けた資料等を善良なる管理者の注意義務をもって管理し、双方が合意した返還日又はユーザから請求があったときに、これらを返還する。

4)　資料等の提供及び返還にかかる費用は、ユーザが負担する。

システム開発においては、ユーザからベンダへの情報提供が不可欠であり、ユーザはベンダにさまざまな資料等を提供することになる。また、ベンダは、ユーザに対し、必要な資料等の提供を要求できることを明確に規定しておく必要がある。

本条では、ユーザからベンダに提供される資料等の提供、保管、使用、返還について定める。

---

[30] 責任者とは、個別契約におけるユーザ及びベンダ双方のプロジェクトの管理遂行責任者をいう。ユーザにおいては、中間資料等の承認、仕様・設計等の確定、検収、変更管理書の交付などの権限と責任を負う。ベンダにおいては、個別業務の遂行、ユーザからの要請・請求に対する対応、変更管理書の交付などの権限と責任を負う。主任担当者とは、各責任者の下に、窓口として円滑な意思疎通を図るため、連絡確認及び必要な調整を行う者をいう。（第一版第 9 条 63 ページ、第 10 条 65 ページ参照）

第 1 項は、ユーザは、ベンダに対し、受託業務遂行に必要な資料等の開示、貸与等を行うことを定める。
第 2 項は、資料等の提供について、ユーザが一定の役割を負担することを明確にするために、ユーザが提供する資料等の内容の誤りがあった場合又はユーザが資料等の提供を遅延した場合は、それによって生じた開発費用の増大、完成時期の遅延、瑕疵などの結果について、ベンダは責任を負わないものと定める。
第 3 項は、ベンダの資料等の保管義務及び返還義務について定める。
第 4 項は、資料等の提供がユーザの責務であることから、返還にかかる費用がユーザの負担となることを定め、これにより、返還費用に関するトラブル予防を図ることとした。

（再委託）

第 6 条　ベンダは、ベンダの責任において、本件業務の一部を第三者に再委託することができる。但し、ベンダは、ユーザから請求があった場合には、再委託先の名称及び住所等、再委託先を特定しうるだけの情報をユーザに通知しなければならない。当該第三者に再委託することが不適切となる合理的な理由が存する場合、ユーザは、その理由を書面によりベンダに通知することにより、当該第三者に対する再委託の中止を請求することができる。なお、ユーザから再委託の中止の請求をベンダが受けた場合は、作業期間、納期または委託料等の内容の変更について、第 2 条⑥に準じて協議を行い、合理的な範囲で合意するものとする。

2)　ベンダは、再委託先との間で、再委託に係る業務を行わせる場合、本契約に基づいてベンダがユーザに対して負担するのと同様の義務を、再委託先に負わせる契約を締結するものとする。

3)　ベンダは、再委託先の履行についてユーザに帰責事由がある場合を除き、自ら業務を遂行した場合と同様の責任を負うものとする。

本モデル契約書においては、パッケージを利用したシステム開発の取引実態により適合するものとして、モデル取引・契約書第一版第 7 条[31]【B 案】を採用している。再委託の可否については、①再委託先の技術力についての保証がなく、また機密保持の観点からも原則禁止とし委託者の承諾を要するとすべき（原則禁止【A案】）との考えと②再委託を原則禁止としてしまうことによって業務の遂行における柔軟性が失われ結局提供される技術の質も効率も損なわれてしまうので原則自由とすべき（原則自由【B案】）との考えの対立があり、モデル取引・契約書第一版においても、両論が併記されている。

本モデル契約書が前提とする取引は、パッケージソフトウェアを利用すること、ユーザが中小企業等であることなどに特色がある。この観点より本論点を検討すると、そもそも多くの場合第三者製品（パッケージソフトウェア）をシステムのコアの部分に据えるのであるから、再委託を厳しく制限することは現実的ではないこと、また原則再委託自由としてもユーザが要求するときは再委託先を開示させることとし、かかる再委託先を使うことを止めさせることに合理的な理由があるときはかかる再委託を止めさせることができるとすれば弊害も少ないものと考えられる。

---

31 モデル取引・契約書第一版 59～60p。A 案：再委託先におけるユーザの事前承諾を設ける場合、B 案：再委託先の選定について原則としてベンダの裁量（但し、ユーザの中止請求が可能）とする場合。

従って、第 1 項においては、再委託は原則自由とし、ユーザが要求するときには再委託先を開示し、ユーザは合理的な理由があるときには再委託を中止できることとした。ここで、「合理的な理由」とは、例えば、現に再委託先がユーザと競合する企業のソフトウェア開発業務に関与し、ユーザ独自の業務ノウハウが競合先に流出しかねない危険があること、再委託先の情報セキュリティ確保の措置が不十分であること、以前に当該再委託先に業務を委託したが適切に業務が遂行されなかった実績があること、再委託先の経営権に関する紛争の存在、再委託先の業務内容が不健全であること、ユーザにおいて制定している委託先選定基準への不適合等の状況が想定される。

ユーザからのかかる再委託の中止請求については、特に再委託先での作業が既に進んでいるときなど、作業期間、委託料、納期等に影響が出ることが予想されるので、そのような場合には、契約変更手続（システム基本契約書第 2 条⑥）に準じて契約条件の変更に係る協議を行い、ユーザ及びベンダは、合理的な範囲での変更合意を行う義務を負うこととしてある。例えば、ユーザがベンダからの合理的な委託料増額案に対して応じないときは、ベンダに対して債務不履行責任を負うことになり、増額分について損害賠償責任を負うこともあり得る。なお、ユーザは合理的な範囲の契約変更を受け容れられない場合には、各本件業務にかかる契約の解約を選択することもできる。この場合、ユーザは、原則としてベンダに対し、既になされた業務の対価を支払い、発生した損害を賠償しなければならないものと考えられる。

第 2 項は、ユーザとベンダ間の本契約に基づくベンダの義務を、再委託先にも負わせることを義務づけている。

第 3 項は、ユーザが再委託について承諾したとはいっても、ベンダは自らが業務を遂行した場合と同様の責任を負うものとする。この場合においても、再委託先の履行に関し、ユーザに帰責事由がある場合についてまでベンダに責任を負わせることは酷なのでベンダの責任の範疇から除かれている。

（秘密情報の取扱い）

第 7 条　ユーザ及びベンダは、本件業務の遂行のため、相手方より提供を受けた技術上又は営業上その他業務上の情報のうち、相手方が書面により秘密である旨指定して開示した情報、又は口頭により秘密である旨を示して開示した情報で開示後○日以内に書面により内容を特定した情報（以下あわせて「秘密情報」という。）を第三者に漏洩してはならない。但し、次の各号のいずれか一つに該当する情報についてはこの限りではない。また、ユーザ及びベンダは秘密情報のうち法令の定めに基づき開示すべき情報を、当該法令の定めに基づく開示先に対し開示することができるものとする。

① 秘密保持義務を負うことなくすでに保有している情報

② 秘密保持義務を負うことなく第三者から正当に入手した情報

③ 相手方から提供を受けた情報によらず、独自に開発した情報

④ 本契約に違反することなく、かつ、受領の前後を問わず公知となった情報

2) 秘密情報の提供を受けた当事者は、当該秘密情報の管理に必要な措置を講ずるものとする。

3) ユーザ及びベンダは、秘密情報について、本契約の目的の範囲内でのみ使用し、本契約の目的の範囲を超える複製、改変が必要なときは、事前に相手方から書面による承諾を受けるものとする。

4) ユーザ及びベンダは、秘密情報を、本契約の目的のために知る必要のある各自（本契約に基づきベンダが再委託する場合の再委託先を含む。）の役員及び従業員に限り開示するものとし、本契約に基づきユーザ及びベンダが負担する秘密保持義務と同等の義務を、秘密情報の開示を受けた当該役員及び従業員に退職後も含め課すものとする。

5) 秘密情報の提供及び返還等については、第 5 条（ユーザがベンダに提供する資料等及びその返還）に準じる。

6) 秘密情報のうち、個人情報に該当する情報については、第 8 条が本条の規定に優先して適用されるものとする。

7) 本条の規定は、本契約終了後、○年間存続する。

ソフトウェア開発においては、ユーザ、ベンダが互いに相手方の秘密情報に接することが想定されることから、本条では、それぞれの秘密保持義務を定める。

第 1 項では、秘密保持義務の対象となる情報を特定している。本項では、対象となる情報を明確にするため、相手方が書面により秘密である旨指定して開示した情報であるか、または口頭により秘密である旨通知して開示した情報は、開示後○日以内に書面により内容を特定することを必要としている。第 1 号から第 4 号は、秘密情報の例外規定である。

第 2 項は、秘密情報の提供を受けた当事者は、秘密情報の管理に必要な措置を講ずることとしている。秘密情報の秘密管理性及び非公知性を維持するためには、提供を受けた当事者に秘密情報を適正に保護する体制の構築を義務づけておく必要がある。秘密情報の管理については、物理的、技術的、人的、組織的管理措置を実効的に構築しなければならない。

第 3 項は、秘密情報の目的外使用を禁止し、複製、改変については相手方の承諾を要件としている。

第 4 項は、システム基本契約書及び個別契約に基づき乙が再委託する場合の再委託先も含め、秘密情報の開示を受けた役員、従業員、退職者へも秘密保持義務を負わせるよう求めている。開示を受けた者が退職してしまった場合に、第三者に秘密情報が出て行くことのないよう退職者についても秘密保持義務を課すことを義務づけている。秘密情報の開示を受ける担当者等に秘密保持の誓約書を義務づけるなど、より具体的な方策を定めておくことも考えられる。退職者に対して秘密保持義務を課す場合には、一般的に秘密保持契約を締結する必要がある。特に、現職の従業者等及び退職者と秘密保持契約を締結する際には、秘密保持義務が必要性や合理性の点で公序良俗違反（民法第 90 条）とならないよう、その立場の違いに配慮しながら、両者がコンセンサスを形成できるようにすることが重要である（「営業秘密管理指針」（平成 15 年 1 月 30 日、平成 17 年 10 月 12 日改訂、経済産業省）参照）。

本条で定める秘密情報と次条で定める個人情報は、公知情報でない個人情報について適用が重複する場合もありうるので、第 6 項でその優先関係について取り決めている。

第 7 項は、秘密保持義務は通常契約期間より長期の存続が必要であるため、本契約終了後一定期間（秘密情報の性質から鑑みて合理的な期間）、存続させるものとしている。

（個人情報）

第 8 条　ベンダは、個人情報の保護に関する法律（本条において、以下「法」という。）に定める個人情報のうち、本件業務遂行に際してユーザより取扱いを委託された個人データ（法第 2 条第 4 項に規定する個人データをいう。以下同じ。）及び本件業務遂行のため、ユーザ･ベンダ間で個人データと同等の安全管理措置（法第 20 条に規定する安全管理措置をいう。）を講ずることについて、別紙重要事項説明書その他の契約において合意した個人情報（以下あわせて「個人情報」という。）を第三者に漏洩してはならない。なお、ユーザは、個人情報をベンダに提示する際にはその旨明示するものとする。また、ユーザは、ユーザの有する個人情報をベンダに提供する場合には、個人が特定できないよう加工した上で、ベンダに提供するよう努めるものとする。

2)　ベンダは、個人情報の管理に必要な措置を講ずるものとする。

3)　ベンダは、個人情報について、本契約の目的の範囲内でのみ使用し、本契約の目的の範囲を超える複製、改変が必要なときは、事前にユーザから書面による承諾を受けるものとする。

4)　個人情報の提供及び返還等については、第 5 条（資料等の提供及び返還）を準用する。

5）　第 6 条第 1 項の規定にかかわらず、ベンダはユーザより委託を受けた個人情報の取扱いを再委託してはならない。但し、当該再委託につき、ユーザの事前の承諾を受けた場合はこの限りではない。

個人情報保護法第 22 条に基づいて委託者は、委託先に対する監督の責任を負うことから、ソフトウェア開発委託契約においても、委託先の監督について取り決めておく必要がある（個人データの取扱いを委託する場合に契約に盛り込むことが望まれる事項については、「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン[32]」（以下、「個人情報ガイドライン」という。）等を参照）。また、個人情報は、秘密保持義務の対象となる秘密情報とは対象、契約で定めることが望まれる事項が異なるので、個人情報保護に関する条項を秘密保持とは別途規定してある。

第 1 項は、ベンダに個人情報保護を義務づける。「その他の契約」とは、システム基本契約書及び別紙重要事項説明書以外に、個人情報の取扱いに関する委託契約を別途締結するケースを想定している。また、ユーザ保有の個人情報については、当該個人に対し責任を持っているユーザ自身がより安全な取扱いにつき配慮すべきである。例えば、テスト時に使用するデータをユーザ側がダミー化する等してベンダに渡す等の配慮を行う必要がある。

第 2 項は、ベンダに必要な安全管理措置を義務づける。

第 3 項は、ベンダに個人情報の目的外の使用を禁止し、複製、改変についてはユーザの

---

[32] 個人データの取扱いを委託する場合に契約書への記載が望まれる事項について、「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」（平成 16 年 6 月、経済産業省）（以下、「個人情報ガイドライン」という。）において、委託者及び受託者の責任の明確化、個人データの安全管理に関する事項、再委託に関する事項、個人データの取扱状況に関する委託者への報告の内容及び頻度、契約内容が遵守されていることの確認、契約内容が遵守されなかった場合の措置、セキュリティ事件・事故が発生した場合の報告・連絡に関する事項が挙げられている。

承諾を要件としている。
　第 4 項は、個人データの提供、返還・消去・廃棄に関する事項については、第 5 条（資料等の提供及び返還）を準用する。
　第 5 項は、再委託がベンダの裁量で可能な場合にも、個人情報の取扱いの再委託についてはユーザの事前承諾を要するものとしている。個人情報ガイドラインに、再委託を行う際に委託者への文書による報告を契約上規定すべきとされている趣旨に対応する[33]。

　個人情報をどのように取り扱うのかについては、ユーザの事業分野に関するガイドライン等を踏まえた上で、事前に具体的内容について十分協議して、委託者と受託者の責任分担を明確にしておく必要がある。

（報告書の著作権）

第 9 条　ベンダがユーザに対して提出する報告書に関する著作権（著作権法第 27 条及び第 28 条の権利を含む。）は、ユーザ又は第三者が従前から保有していた著作物の著作権を除き、ベンダに帰属するものとする。

2)　ユーザは、前項の報告書又はその複製物を、本件システムを利用するために必要な範囲で、複製、翻案することができるものとする。

　本条は、全ての各本件業務に共通して問題となりうる報告書に関する著作権の帰属について規定する。

　なお、本契約における成果物となるべきソフトウェア等に関する著作権については、ソフトウェア設計･制作業務に関する別紙重要事項説明書で定める。

（損害賠償）

第 10 条　ユーザ及びベンダは、本契約の履行に関し、相手方の責めに帰すべき事由により損害を被った場合、相手方に対して、法令に基づく損害賠償を請求することができる。但し、別紙重要事項説明書に請求期間が定められている場合は、法令に基づく請求期間にかかわらず重要事項説明書に定める期間の経過後は請求を行うことができない。

2)　前項の損害賠償の累計総額は、債務不履行、法律上の瑕疵担保責任、不当利得、不法行為その他請求原因の如何にかかわらず、帰責事由の原因となった業務に係る別紙重要事項説明書に定める損害賠償限度額を限度とする。

3)　前項は、損害が損害賠償義務者の故意又は重大な過失に基づくものである場合には適用しないものとする。

---

[33] 委託者が受託者について「必要かつ適切な監督」を行っていない場合で、受託者が再委託した際に、再委託先が適切とはいえない取扱いを行ったことにより、何らかの問題が生じた場合は、元の委託者がその責めを負うことがあり得るので、再委託する場合は注意を要する。（「個人情報ガイドライン」参照）

本条は、瑕疵担保責任、債務不履行責任、不法行為責任等に基づく損害賠償責任の制限について規定する。情報システム開発の特殊性を考慮して、損害賠償責任の範囲・金額・請求期間について、これらを制限する規定をおくべきかどうか、またその内容をどのようにすべきかについては、ユーザ・ベンダ間で対立するところであるが、本モデル契約書では、具体的な損害賠償の上限額、損害の範囲・請求期間の制限については、個々の情報システムの特性等に応じて、個別に決定できるように記述している。

第 1 項では、損害賠償責任の成立を、帰責事由のある場合に限定している。本項は瑕疵担保責任としての損害賠償請求についても適用されるが、ソフトウェア開発に関連して生じる損害額は多額に上るおそれがあるので、本件システムの瑕疵を修正する責任について無過失責任とすること（別紙重要事項説明書「E　ソフトウェア設計・制作業務契約の重要事項（1)」第 6 項等を参照されたい。）と同様に無過失責任とすることはベンダに過重な負担を課するとの考え方による。なお、損害の範囲について制限を設ける場合には、通常損害のみについて責任を負い、特別事情による損害、逸失利益についての損害や間接損害を負わないとする趣旨から、直接の結果として現実に被った通常の損害に限定して損害賠償を負う旨規定することが考えられる。
また、本項では損害賠償請求を行う場合一般について請求期間を重要事項説明書で定めることができると定めている。当該期間をどのように設定するかは、個別具体的な事情を勘案して定められるべきである。

第 2 項は、損害賠償の累積総額の上限額を設定する規定で、請求原因の構成如何に関わらず上限が設定されている。なお、解除に伴う原状回復としての委託料の返還は、損害賠償とは異なることに注意が必要である。例えばベンダ側に重大な債務不履行があり、ユーザから本件業務にかかる契約を解除され、原状回復として委託料全額を返還したとしても、委託料の返還は損害賠償の支払いではないので、損害賠償の上限を決める累計総額には加算されないことになる。すなわち、委託料 250 万円が上限となる規定があり、委託料が支払い済みである場合でベンダの債務不履行で解除となったとき、ベンダは 250 万円の委託料の返還に加え、250 万円を上限とする損害賠償を請求される可能性が出てくることになる。

第 3 項は、第 2 項の免責は、損害賠償義務者に故意重過失ある場合には適用されないことを明記する場合の規定である。損害発生の原因が故意による場合には、判例では免責・責任制限に関する条項は無効となるものと考えられているし、重過失の場合にも同様に無効とするのが、支配的な考え方になっていることから設けられた規定である。

なお、遅延損害金についてシステム基本契約書では定めをおいていない。商事法定利率である年 6 分を超える割合の遅延損害金を定める場合は、別紙重要事項説明書上の各本件業務における「特約条項」欄に記載されたい。

（解除）

第 11 条　ユーザ又はベンダは、相手方に次の各号のいずれかに該当する事由が生じた場合には、何らの催告なしに直ちに本契約の全部又は一部を解除することができる。

①　重大な過失又は背信行為があった場合

②　支払いの停止があった場合、又は仮差押、差押、競売、破産手続開始、民事再生手続開始、会社更生手続開始、特別清算開始の申立があった場合

③　手形交換所の取引停止処分を受けた場合

④　公租公課の滞納処分を受けた場合

⑤　その他前各号に準ずるような本契約を継続し難い重大な事由が発生した場合

2)　ユーザ又はベンダは、相手方が本契約のいずれかの条項に違反し、相当期間を定めてなした催告後も、相手方の債務不履行が是正されない場合は、本契約の全部又は一部を解除することができる。

3)　ユーザ又はベンダは、第 1 項各号のいずれかに該当する場合又は前項に定める解除がなされた場合、相手方に対し負担する一切の金銭債務につき相手方から通知催告がなくとも当然に期限の利益を喪失し、直ちに弁済しなければならない。

本条は、本契約の解除に関する条項である。本契約は、システム基本契約書と重要事項説明書から構成されるが、本条はその全部又は一部について解除する場合の要件を定めている。

第 1 項は、取引上の重大な事由について、無催告解除事由として規定する。
第 2 項は、個別の契約違反の催告解除について定める。
第 3 項は、期限の利益喪失に関する特約である。民法にも期限の利益の喪失自由（民法第 137 条）が規定されているが、その他の信用不安事由等も加えたものである。事由の軽重により、当然に期限の利益を喪失する第 1 項所定の場合と解除により期限の利益を喪失する第 2 項の場合とに分けた。

（権利義務譲渡の禁止）

第 12 条　ユーザ及びベンダは、互いに相手方の事前の書面による同意なくして、本契約上の地位を第三者に承継させ、又は本契約から生じる権利義務の全部若しくは一部を第三者に譲渡し、引き受けさせ若しくは担保に供してはならない。

本条は、契約上の地位の移転、債権譲渡、担保化の禁止に関する規定である。

（協議）

第 13 条　本契約に定めのない事項又は疑義が生じた事項については、信義誠実の原則に従いユーザ及びベンダが協議し、円満な解決を図る努力をするものとする。

本条は、一般の取引基本契約に定められているのと同様の協議解決条項である。

（和解による紛争解決・合意管轄）

第 14 条　本契約に関し、ユーザ及びベンダに紛争が生じた場合、ユーザ及びベンダは、次

項の手続をとる前に、紛争解決のため第 4 条に定める連絡協議会を開催し協議を充分に行うとともに、次項及び 3 項に定める措置をとらなければならない。

2） 前項所定の連絡協議会における協議でユーザ・ベンダ間の紛争を解決することができない場合、本条第 4 項に定める紛争解決手続をとろうとする当事者は、相手方に対し紛争解決のための権限を有する代表者又は代理権を有する役員その他の者との間の協議を申し入れ、相手方が当該通知を受領してから○日以内に（都市名）において、本条第 4 項に定める紛争解決手続以外の裁判外紛争解決手続（以下「ADR」という。）などの利用も含め誠実に協議を行うことにより紛争解決を図るものとする。

3）前項による協議又は ADR によって和解が成立する見込みがないことを理由に当該協議又は ADR が終了した場合、ユーザ及びベンダは、法的救済手段を講じることができる。

4） 本契約に関し、訴訟の必要が生じた場合には、○○地方裁判所を第一審の専属的合意管轄裁判所とする。

本条第 1 項、第 2 項は、本契約に関し、紛争が生じた場合、法的救済手段を講じる前段階として、当事者間でまず十分協議し、解決に尽力すべきことを規定している。

第 3 項は、当事者間による解決が不可能な場合、当事者は、法的救済手段（仲裁又は訴訟）による解決を求めることができることを規定している。

第 4 項は、裁判所に訴訟提起する場合を前提に、専属的な合意管轄（民事訴訟法第 11 条）について規定する。なお、特許権、実用新案権、回路配置利用権又はプログラムの著作物についての著作者の権利に関する訴えについては、東京高等裁判所、名古屋高等裁判所、仙台高等裁判所又は札幌高等裁判所の管轄区域内に所在する地方裁判所については東京地方裁判所の管轄、大阪高等裁判所、広島高等裁判所、福岡高等裁判所又は高松高等裁判所の管轄区域内に所在する地方裁判所については大阪地方裁判所の管轄とされる（民事訴訟法第 6 条第 1 項）が、合意管轄も認められている（民事訴訟法第 13 条第 2 項）ので、本条の適用範囲に含まれる。

○○○○年○○月○○日

ユーザ： ベンダ：

重要事項説明書

重要事項説明書は、契約によって構成が異なるため、別冊に代表的なパターンを掲載してある。ここでは、重要事項説明書記載の契約条項について解説する。

要件定義～導入教育支援業務までの契約約定一覧は以下の通りである。

A　要件定義支援及びパッケージソフトウェア候補選定支援業務契約（カスタマイズモデル）
B　パッケージソフトウェア選定支援及び要件定義支援業務契約（カスタマイズモデル）
C　パッケージソフトウェア選定支援及び要件定義支援業務契約(オプションモデル)
D　外部設計支援業務契約
E　ソフトウェア設計・制作業務契約
F　構築・設定業務契約
G　データ移行支援業務契約
H　運用テスト支援業務契約
I　導入教育支援業務契約
J　保守業務契約
K　運用支援業務契約

契約条項の一覧	A	B	C	D	E	F	G	H	I
契約の成立	○	○	○	○	○	○	○	○	○
パッケージソフトウェア候補の選定支援における善管注意義務	○								
パッケージソフトウェアの選定支援における善管注意義務		○	○						
ベンダの善管注意義務	○	○	○	○			○	○	○
業務終了の確認	○	○	○	○			○	○	○
機器の売買等		○	○	○	○	○	○	○	○
本件システムの納入					○	○			
本件システムの検収					○	○			
本件パッケージ固有の瑕疵					○	○			
本件システムについての瑕疵担保					○	○			
危険負担					○	○			
特許権等の帰属					○	○			
著作権の帰属					○	○			
知的財産侵害の責任					○	○			

保守業務～運用支援業務までの契約約定一覧は以下の通りである。

Ｊ　保守業務契約
Ｋ　運用支援業務契約

契約条項一覧	J	K
契約の成立	○	○
機器等の売買等	○	○
保守業務の範囲	○	
運用支援業務の範囲		○
サービスの範囲（サービス仕様書による）	○	○
設置場所への立ち入り等	○	○
遠隔操作によるサービス	○	○
製造打ち切り、保守部品提供の中止の際の取扱い	○	
老朽化装置の取扱い	○	
交換部品の所有権	○	
秘密保持	○	
設置場所の変更	○	○
設置場所の整備	○	○
不具合の調査費用	○	
使用地域の制限	○	○
パッケージ本体の瑕疵担保責任	○	
有効期間	○	○
支払い遅延	○	○

A　要件定義支援及びパッケージソフトウェア候補選定支援業務契約（カスタマイズモデル）

別紙１のパッケージカスタマイズ取引契約モデルの上流工程前半に対応する規定である。

第 1 条は契約の成立についての規定である。

第 2 条はパッケージソフトウェアの候補選定支援における善管注意義務についての規定である。

本モデル契約書のいわゆる上流工程における最も重要な作業は、パッケージソフトウェア（本件システムの構築に利用する第三者が権利を有するソフトウェア、SaaS/ASP。以下「本件パッケージ」という。）の選定である。本モデル契約書においては「A　要件定義支援及びパッケージソフトウェア候補選定支援業務契約（カスタマイズモデル）」において本件パッケージ候補の選定が、「B　パッケージソフトウェア選定支援及び要件定義支援業務

契約（カスタマイズモデル）」、「C　パッケージソフトウェア選定支援及び要件定義支援業務契約(オプションモデル)」において本件パッケージの選定がユーザによって行われ、ベンダはその支援業務を行う。本件パッケージは本モデル契約の成果物となる本件システムの技術的中核となるものであり、また、利用・瑕疵担保等の法的問題の分野においても広い範囲にわたってその固有の条件が適用されることにより重要な意味をもつ。そして下流過程である設計、構築・設定、保守、運用の契約条件に対しても大きな影響を与えるものである。

本モデル契約書が想定する中小企業等ユーザは、パッケージソフトウェア等に関する専門的知識を有するベンダに比べ、そのようなパッケージソフトウェアに関する知見に欠けている。しかしながらユーザの業務内容及びプロジェクトゴールを熟知しているのはユーザ自身である。また上流過程における役割分担においてユーザがベンダに頼りきり、いわば丸投げ状態を認めることはユーザとベンダのシステム契約についての理解の不一致を招き、こうした契約における契約条件の透明性・明確性の妨げとなる。

そこで本モデル契約書では、最終的に本件パッケージの選定を行う者をユーザとし、ベンダはユーザに対し、パッケージソフトウェアに関する情報提供をしつつ、推奨するパッケージをユーザに提案する建付けとしている。そして前述した本モデル契約が想定する中小企業等ユーザのパッケージソフトウェアについての知見の不足に対応するために、当該推奨に係るパッケージの提案に関してベンダは、業界で一般的に認められる専門知識とノウハウにもとづく善良な管理者としての注意義務を負わせるものとした。また、これらの専門知識とノウハウに基づき、ベンダが適切と判断したときは、本件パッケージ候補が存在しないことをユーザに進言しなければならないとした。

「善良なる管理者の注意義務を果たした」かどうかは、情報処理技術に関する業界で一般的に要求される専門知識・ノウハウにもとづく注意義務を果たしたかどうかによって決定される。すなわち、ここでの注意義務とは、自らの能力に応じた注意義務の程度という主観的な意味ではなく業界において一般的・客観的に要求される注意義務を意味し、このような注意義務を欠くときは過失が認められる。ここで規定される善管注意義務は第３条のベンダの善管注意義務に重なるものであるが、上記したとおり本件パッケージの候補の選定支援作業の重要性に鑑み、再度確認して記載している。

第 3 条はベンダの善管注意義務一般についての規定である。ベンダは、ユーザに対し、各本件業務（請負契約であるソフトウェア設計・制作及び構築・設定業務を除く。）の履行に関し、準委任契約上の善良なる管理者の注意義務を負うことを確認する（民法第 656 条、第 644 条）。前述したとおり「善良なる管理者の注意義務を果たした」かどうかは、情報処理技術に関する業界で一般的に要求される専門知識・ノウハウにもとづく注意義務を果たしたかどうかによって決定される。すなわち、ここでの注意義務とは、自らの能力に応じた注意義務の程度という主観的な意味ではなく業界において一般的・客観的に要求される注意義務を意味し、このような注意義務を欠くときは過失が認められる。

逆に言うと、ベンダは、ユーザに対し、善良な管理者の注意義務をもって本件業務を履行している限り、各業務の内容、結果等について責任を負わない。

第 4 条は業務終了の確認についての規定である。
本条では、準委任としてベンダが善管注意義務に基づき業務を適切に行ったかどうかの確認を行う手続を定める。

第 1 項は、ベンダはユーザに対し、業務終了後所定の期間内に業務完了報告書を提出することとする。業務完了報告書兼検収依頼書の例については、別添のドキュメントモデルを参照のこと。

第 2 項は、点検期間を明確にした上で、ユーザが業務完了報告書の確認を行うことを定める。

第 3 項の業務完了確認書兼検収書の例については、別添ドキュメントモデルを参照のこと。
第 4 項は、ユーザが業務完了確認を怠った場合のみなし確認を定める。

B　パッケージソフトウェア選定支援及び要件定義支援業務契約（カスタマイズモデル）

別紙１のパッケージカスタマイズ取引契約モデルの上流工程後半に対応する規定である。

第 1 条、3 条、4 条、5 条は、基本的に A パッケージソフトウェア選定・要件定義支援業務契約のものと変わらない。

第 2 条は機器等の売買等についての規定である。本件業務においては機器等の販売が行われる場合があり、その際ユーザは、本件システムを構成する機器等（ハードウェア機器、電子媒体、OS）をベンダ又は第三者から購入し、またはリースすることとなるが、ベンダ又は第三者は、ユーザとの間において別途売買等に関する契約を締結することが多い。そうした契約が存在するときは、契約の対象となる当該機器等に関しては、本契約に優先して適用される旨を定める。

C　パッケージソフトウェア選定支援及び要件定義支援業務契約(オプションモデル)

別紙 2 のパッケージオプション取引契約モデルの上流工程に対応する規定である。条項は別紙 1 のパッケージカスタマイズ取引契約モデルに対応する「A　要件定義支援及びパッケージソフトウェア候補選定支援業務契約（カスタマイズモデル)」、「B　パッケージソフトウェア選定支援及び要件定義支援業務契約（カスタマイズモデル)」のものと同じである。

D　外部設計支援業務契約

契約の成立、機器等の売買等、ベンダの善管注意義務、業務終了の確認の 4 条項から成り、各条項の説明は前述のとおりである。

E ソフトウェア設計・制作業務契約、F　構築・設定業務契約

第 1 条は請負契約の成立に関する規定である。

第 2 条は本件システムの納入および出荷テストについての規定で、基本的にモデル取引・契約書第一版の規定と同じである。ソフトウェア設計・制作業務の場合はベンダによる適格性（出荷）テストの実施を定めている。

第 3 条では本件システムに関する検収を行う手続について定める。
第 1 項については、本件パッケージについて検査期間内に適格性（出荷）テスト条件（構築・設定の場合は「受入れテスト条件」）に基づき検査し、システム要件定義書、関連する文書と本件システムとが合致することを点検することを規定する。構築・設定業務の場合、現地調整の都合上、仕様書通りとならない場合があるため、構築・設定業務報告書が加わっている。

第 2 項は、本件パッケージがシステム要件定義書、関連する文書と本件システムに適合しないことが判明した場合、ベンダがこれを修正して修正版をユーザに納入することを義務付けている。検査合格通知書兼検収書の例は、別添のドキュメントモデルを参照のこと。
第 3 項は、みなし検査合格に関する規定を定めることにより、ユーザの都合により検収が引き延ばされることを防ぐものである。
第 4 項は、検査合格をもって本件ソフトウェアの検収完了とすることを明記する。

第 4 条は機器等の売買等がある場合の規定であり、文言は、他の業務における規定と同じである。
機器等の売買について別契約が存在する場合はかかる契約が本契約に優先して適用されるので、当然瑕疵担保についても優先される。本件パッケージについても通常は本契約とは別の使用許諾契約書等が存在し、当該契約書に瑕疵担保の規定が存在することが多いと考えられるので本条と本件パッケージ固有の瑕疵の規定は重複する点もあるが、本モデル契約書における本件パッケージの役割の重要性に鑑み個別の条項において権利関係を明確にすることが重要であることから重複して規定してある。

第 5 条は、本件パッケージの固有の瑕疵に関する規定である。
第 1 項は、ソフトウェア設計・制作業務においてベンダが、ユーザに対し、本件パッケージに固有の瑕疵（本件パッケージそのものについての瑕疵）について原則として責任を負わないことを規定する。
第 2 項は、ベンダが例外として責任を負う場合を規定するものであって、ベンダが本件パッケージの固有の瑕疵（不具合、権利侵害等）の存在を知り、または重大な過失によりこれを知らず結果としてユーザにこれを告げなかった場合にのみ、民法第 415 条によって責任を負うことを定める。これは請負契約そのものから導き出される責任ではなく、本件パッケージの重要性に鑑みソフトウェア設計・制作業務に付随して発生する契約責任である。
第 3 項は、第 1 項によって責任を負う場合であっても、本体の請負契約の瑕疵担保の瑕疵が軽微であっても、納入物の修正に過分の費用を要する場合に無償での修正をベンダに求めるのは酷であるとの考え方から、民法第 634 条第 1 項但書に準じた規定を設けていることからこれに準じ損害が軽微な場合の免責を定めたものである。

第 6 条は、本件システム（ただし、本件パッケージソフトウェア及びハードウェア機器部分を除く。）に関する瑕疵担保責任について定める。履行がなされていない（仕事が完成されていない）場面での債務不履行責任と履行が一応完了した（仕事が完成した）後の場面での瑕疵担保責任の境界は、実務上判断が難しいところがある。システム開発についてシステムを完成させたと認められるか否かは、仕事が当初の請負契約で予約していた最後の工程まで終えているか否かを基準にすべきであるとする裁判例がある（東京地判平成 14 年 4 月 22 日）。具体的には、当初仕様書にて予約されている業務の最後の工程まで終えて納品及び検査合格後、瑕疵が発見された場合には、原則として瑕疵担保責任が適用されることになると考えられる。
前述したように本件システムを構成するものであっても、本件パッケージソフトウェアについてはベンダは当該パッケージの固有の瑕疵（不具合、権利侵害等）の存在を知り、または重大な過失によりこれを知らず結果としてユーザにこれを告げなかった場合にのみ責任を負うものであって、本件パッケージソフトウェアについての本条の適用はない。さらに本件システムを構成する機器等であっても、係る機器等について別の契約が存在する場合はやはり本条の瑕疵担保の規定の適用はない。

第 1 項は、パッケージシステム利用コンピュータソフトウェア開発業務において生じた「本件システムについてシステム要件定義書及び／もしくは関連する文書等の仕様との不

一致（バグを含む。）」を瑕疵とする。本件システムに関するセキュリティ対策についてはシステム仕様書等に含まれているのであればその仕様書との不一致があれば、「瑕疵」に該当する。瑕疵担保期間は、情報システムの規模や対価等を考慮してケースバイケースにより、当事者間で決めるべきことであるから、ここでは具体的な期間は明示しない。

第 2 項では、瑕疵が軽微であっても、納入物の修正に過分の費用を要する場合に無償での修正をベンダに求めるのは酷であるので、民法第 634 条第 1 項但書に準じた規定を設けている。

第 3 項は、民法第 634 条第 1 項但書に準じ、瑕疵がユーザの指示や提供した資料等に起因する場合にはベンダは担保責任を負わないが、ベンダがかかる資料等又はユーザの指示が不適当であることを知って指摘しない場合には担保責任を免れないとする規定である。

第 4 項は、瑕疵担保責任の範囲を定める。実務上、瑕疵担保責任による修補と保守業務とが区別されずにいたため、本来であれば、ベンダがユーザに対して有償で提供する保守サービスが瑕疵担保責任の名の下に無償にて提供されている場合がよくある。このような現状を整理するため、本項では瑕疵担保責任の対象は、本契約のもとでテストが行われた本件システムのみであって、当該システムがアップグレードされたことに起因する問題等については、ベンダは、有償による保守サービスによってこれに対応するものとする。

担保責任に関する損害賠償については、本契約書第 10 条を参照のこと。

第 7 条は有体物の納入がある場合の危険負担について定めたものである。

第 8 条は特許権の帰属についての規定である。ベンダが開発したソフトウェア等の納入物に関しては、特許権、著作権、ノウハウ等の知的財産権が発生する場合がある。知的財産権の帰属については、ユーザ、ベンダ双方の利害が対立することから、契約で明確に規定しておくべきである。本条は、ソフトウェア設計・製作業務及び構築・設定業務の遂行過程で生じる特許権等に関する権利の帰属及び実施権について定める。

第 1 項は、発明者主義に従い、当事者のいずれか一方の発明者が単独で発明考案した場合には、特許権等は当該当事者に帰属するものとする。なお、モデル取引・契約書第一版におけるモデル契約書第 44 条第 2 項のようにベンダ及びユーザが共同発明を行うことは、本件システムがパッケージソフトウェアを前提としているものである以上、考えにくく、ベンダのみが発明者となる場合が圧倒的に多いであろう。

第 2 項は、ベンダが特許権等を保有する場合においても、ユーザが開発されたソフトウェアを使用するのに必要な範囲では、特許権等を使用する必要があるため、通常実施権を許諾するものとしている。また、一定の第三者に使用せしめる旨を個別契約の目的として特掲した上で開発された特定ソフトウェアについては、当該第三者に対しても許諾するものとする。なお、かかる許諾についての対価は委託料に含まれることを明記すべきである。

第 9 条では、納入物の著作権の権利帰属及び利用について規定する。
新たに作成されたソフトウェアの著作権をベンダ、ユーザのいずれに帰属させるべきかについては、ベンダは作成したソフトウェアの再利用のために自己のものとして留保したいと考え、ユーザは自己の機密情報が含まれる場合の保護の観点などからベンダから譲り受けて、自己のものとしたいと考えている。モデル取引・契約書第一版においては、社会的な生産効率の向上の観点などから、汎用性のあるプログラムについてはベンダに帰属させると共に、その余のプログラムに関してベンダ帰属案（A 案）、ユーザ帰属案（B 案）、共有案（C 案）が記載されている。

本研究会が前提とする取引は、パッケージソフトウェアを利用すること、ユーザが中小企業等であることなどに特色がある。この観点より本論点を検討すると、まず、アドオン等のカスタマイズで新たに作成されるソフトウェアは前提となるパッケージソフトウェアの関連で作成されるものであり、当該パッケージソフトウェアの一般的機能となるべきものが、カスタマイズという形で先行して開発されることも多い。それゆえ、かかる部分が

将来的には他のユーザにも共通に利用できる部分となるケースもしばしばある。なお、ユーザがベンダから著作権の譲渡を受ける場合には、別途譲渡の対価を支払うことが要請されるため、そのような場合にはユーザの費用負担が増大する。他方、かかる部分にユーザの機密情報が含まれている場合にノウハウの流出防止など当該機密情報の保護をユーザが求めることは当然のことであるが、機密情報の保護のためには、著作権を取得しなくとも別途用意される秘密保持条項で対応できるものと考えられる。

以上の次第で、カスタマイズ等により作成されたソフトウェアの権利をベンダに帰属させベンダが他のビジネスにおいても再利用できる環境を整えていた方が、総体としては価格を低く抑えることができ、中小企業等が利用するシステムとして比較的合理的な価格で広く普及することに資する結果となると考えられるため、カスタマイズ等により新たに作成されたソフトウェアの権利は原則ベンダに帰属させることとした。

勿論、当事者の合意により、B 案又は C 案を採用することも可能である。第 1 項は、納入物に関する著作物の著作権については、ユーザ又は第三者が従前から保有していた著作権を除き、ベンダに全ての著作権を帰属させる。

第 2 項は、本件ソフトウェアに関して、ユーザが行う自己使用のための複製又は翻案について定める。また、一定の第三者に使用せしめる旨を個別契約の目的として特掲した上で、開発された特定ソフトウェアについては、当該第三者に対しても利用許諾できるものとし、ベンダは、著作者人格権（著作権法第 59 条）を行使しないことを定める。なお、一定の第三者に使用せしめる旨を個別契約の目的として特掲した上で開発された特定ソフトウェアについては、当該第三者に対しても許諾するものとする。なお、かかる許諾についての対価は委託料に含まれることを明記すべきである。

第 10 条では、納入物が、著作権及び特許権その他の知的財産権を侵害した場合のベンダの責任について規定する。著作権侵害についてはクリーンルーム手法等による回避の可能性もあるが、特許権は未公開中のものもあるし、公開済みの出願であっても、ベンダにおいて侵害の有無をすべてを完全に調査検証することは事実上困難であるし、海外も含め調査検証にかなりの費用を要することもある。また、ベンダが、第三者の知的財産権に関する納入物の非侵害を保証することは現実的ではないため、侵害時の責任分担を定めておくことも必要となる。個別取引の実情にあわせて規定を設けることになるが、本契約では、以下の案を提示する。

本条では、パッケージソフトウェア等の選定についてベンダがユーザに提案することから、ユーザが権利者に対して支払うこととなった損害賠償額等をベンダが負担することとしている。但し、ベンダがかかる責任を負う前提として、ベンダに必要な情報が提供され、防御に関する適切な権限が与えられることが必要である。そこで、ベンダが責任を負う要件として、①申立ての事実及び内容のすみやかな通知、②ベンダが交渉又は訴訟の決定権限を有すること、③ユーザの敗訴判決確定又は和解成立などによる確定的解決で損害賠償の支払義務が確定することを規定する。ユーザに生じた損害賠償額及び合理的な弁護士費用の上限は、システム基本契約書第 10 条に従う。[34] 第 1 項但書は、侵害の申立がユーザの帰責事由による場合、本件パッケージソフトウェア及びシステム基本契約書に優先する契約の対象となる機器等を原因とする場合には、ベンダが免責される旨規定する。例えば、特許権侵害等がユーザの指示した仕様に関する部分である場合、納入した本件ソフトウェアをユーザが他のソフトウェアと組み合わせるなどして第三者の特許権を侵害した場合、ユーザが本件ソフトウェアをベンダとの事前の合意に反して本邦外で使用し本邦外の特許権を侵害した場合、ユーザが本件ソフトウェアをベンダとの事前の合意なく変更した場合、ユーザが本件ソフトウェアを自己利用の範囲又は第三者に使用せしめる旨を特掲した特定

[34] モデル取引・契約書第一版では上限は規定されていない。

ソフトウェアの範囲を超えて配布した場合などが想定されている。
第 2 項は、ベンダは、本条に基づく責任を主体的に負うことになるので、ユーザは、防御方法等の一切をベンダに委ねなければならない旨を定める。
第 3 項は、ベンダの帰責事由により納入物の使用が不可能となるおそれがあるような場合には、ベンダの判断と費用負担で、ユーザが第三者の知的財産権を侵害することなく情報システムを継続使用できるように措置を講じることができる旨を規定する。第三者の知的財産権を侵害するものとして損害賠償額が拡大し、プログラムの継続使用ができなくなる事態を考慮したものである。

G データ移行支援業務契約、H 運用テスト支援業務契約、I 導入教育支援業務契約

契約の成立、機器等の売買等、ベンダの善管注意義務、業務終了の確認の 4 条項から成り、各条項の説明は前述のとおりである。

J 保守業務契約

第 1 条は、準委任契約の成立に関する規定である。

第 2 条は、保守業務の範囲についての規定である。本件システムに対する保守業務には、ハードウェア保守及びアプリケーション保守（パッケージソフトウェアに関する保守を除く。）があり、本条はこの双方について定めるものである。共通フレーム 2007 によれば、保守業務には、(1)不良や不具合を修正する業務（是正保守）、(2)あらゆる環境の変化に対応させる業務（適応保守）、(3)本件システムの性能又は保守性を改善する業務（完全化保守）及び(4)引渡後潜在的な不具合が顕在化する前に発見し修復する業務（予防保守）が挙げられる。本条にてベンダが行う保守とは、(1)のみであり、(2)、(3)及び(4)の業務は、既に本件システムの変更でありこれを通常の保守業務としてベンダに行わせるのは酷との考えから、対象外であるとした。

第 3 条は、サービスの範囲についての規定であり、保守サービスの内容は、別途ベンダとユーザとの間で取り交わされるサービス仕様書による旨を定めた。

第 4 条は設置場所への立ち入り等についての規定であり、保守業務の便宜のために、ベンダによる本件システムの設置場所への立ち入り、ユーザによる作業場所及び消耗品の提供について定めた。

第 5 条は、遠隔操作によるサービスについての規定である。事前の合意がある場合、ベンダが遠隔地からユーザのサーバにログインして保守サービスが実行できる。遠隔保守を実行する都度、ユーザの個別承認を得るかは、個別に重要事項説明書の付帯事項で定める。

第 6 条は、製造打ち切り、保守部品提供の中止の際の取扱いについての規定であり、本件システムを構成するハードウェアの製造会社の都合によってハードウェアの製造が中止された場合、又は保守部品の提供を中止した場合、ベンダは、ユーザに対し、ハードウェア保守を行うことは不可能である。そこで、ベンダは、ユーザに対し、ハードウェア自体を有償にて交換することを請求することができる。当該請求に応じなかったユーザについては、当該ハードウェアを保守業務の対象から外すことができる。この場合の保守料金は、当該保守料金体系に従って処理されるものとする。

第 7 条は、老朽化装置の取扱いについての規定である。前条と同様の趣旨から、本件システムを構成するハードウェアの保守部品がハードウェア製造会社の定める耐用年数（設計標準使用期間）を超えた場合、当該保守部品が老朽化し、保守業務が適切に行われなくなる可能性が高いので、ベンダは、ユーザに対し、当該保守部品を有償にて交換することを請求することができる。当該請求に応じなかったユーザについては、当該保守部品を保守業務の対象から外すことができる。この場合、ユーザがベンダに対して支払う保守料金については変更しない。

第 8 条は、ソフトウェアのサポート中止がなされた際の取扱いの規定である。ソフトウェアの製造会社がサポートを中止した後、機能の不具合やセキュリティ等の欠陥が発見された場合、ベンダはそれを改修することが不可能である。また、ソフトの製造会社が不具合を修正しないことで、ソフトウェアの安定稼働を維持することが困難になり、それによって、カスタマイズ部分に影響が及び、保守業務が適切に行われなくなる等の場合がある。ベンダはこのような場合、保守の継続について検討し、その内容をユーザに提示した上で、保守内容の変更交渉を開始することができる。この場合、ユーザはベンダと保守契約の見直し交渉に応じなくてはならない。

第 9 条は、交換部品の所有権についての規定である。交換された保守部品については、従来はユーザに所有権がある。ただ、本条は、保守業務の履行の際の実務上の慣行に基づき、交換された保守部品の所有権が交換によってベンダに帰属する旨を定める。

第 10 条は、秘密保持についての保守契約独自の規定である。契約書の秘密保持義務の規定と矛盾せず、その前提での規定である。前条により、交換された保守部品についてはベンダの所有となるが、ユーザの使用により、当該保守部品にはユーザの情報が記憶されている。本条は、ベンダが当該ユーザ情報を本契約第 7 条に定める秘密情報として取扱い、保護する旨を定めた。

第 11 条は、設置場所の変更についての規定である。ユーザが本件システムの設置場所を変更した際、ベンダがこれを知らなければ円滑な保守業務が行われることはないので、ユーザに対し、ベンダに変更の 30 日前までにこれを通知することを求めた規定である。仮に、ユーザがこれを怠った場合、ベンダによる保守業務を受けられなくてもこれをベンダの債務不履行であると主張することはできない。

第 12 条は、設置場所の整備についての規定である。ユーザが本件システムを所有及び管理しているので、ユーザが本件システムの設置場所を整備しておかなければベンダによる適切な保守が受けられない。そこで、ユーザは、ハードウェア製造会社が定める数々の使用環境条件に適合するよう本件システムの設置場所を整備しなければならないことを定める。

第 13 条は、不具合の調査費用についての規定である。本件システムのハードウェア、ソフトウェアの不具合については、原則としてシステム保守の専門家であるベンダがその費用負担にてこれを調査する。しかしながら、調査の結果、当該不具合がユーザの重過失により発生したことが判明した場合、調査の費用をベンダに負わせることは公平ではない。また、保守業務の対象に含まれないハードウェア、ソフトウェアが原因になって保守業務の対象であるハードウェア、ソフトウェアに不具合が発生した場合、調査の費用をベンダに負わせることは公平ではないことから、本件システムの不具合の際の調査費用について定めた。

第 14 条は、使用地域の制限についての規定である。本件システムは、もともと日本国内においてのみ使用することが予約されており、仮にユーザがこれを一回でも日本国外にて

使用した場合本件システムに何らかの影響が発生する可能性が大きく、ベンダは、当該システムについては適切な保守業務を行うことはできないため、本件システムの使用地域の制限について定めた。

第 15 条は、パッケージ本体の不具合についての規定である。ベンダは、パッケージソフトウェアの固有の不具合について、適切な保守業務を行うことは不可能であるから、これは保守業務の対象外であることを定めた。パッケージソフトウェアの固有の不具合については、パッケージソフトウェアの使用許諾書に従うものとする。

第 16 条は、有効期間についての規定であり、保守業務の期間を 1 年間とし、当事者から申し出がなく、また保守業務の対象機器であるハードウェアの部品が市場において供給される限り、自動更新されることを定める。

第 17 条は、支払遅延についての規定である。保守業務は、継続的な保守サービスを供給することをその内容とするため、仮にユーザが代金債務の支払を怠った場合においてもベンダにサービスの提供を要求することは酷であるため、このような場合、ベンダは、ユーザに対し、支払遅延日以後の保守サービスを行う必要がない旨を定めた。

K 運用支援業務契約

保守業務契約の規定とほぼ同様であるのでそちらを参照されたい。

ドキュメントモデル

本契約書、重要事項説明書、モデル取引のプロセスに合致するサンプルドキュメントを準備した。適宜、全部または一部を参考し活用されたい。

また、チェックシートは、取引の端緒にあたって、ベンダからユーザに配布し、プロセスの理解を深めるための資料として活用されることを期待している。

業務関連サンプルドキュメント

1.プロジェクト連絡協議会議事録
2.設定等合意書
3.業務完了報告書兼検収依頼書
4.業務完了確認書兼検収書
5.業務完了報告書兼外部設計書承認依頼書
6.業務完了確認書兼外部設計書承認書
7.システム構築・設定業務完了報告書兼検収依頼書
8.検査合格通知書兼検収書（構築・設定業務契約）
9.納品書兼検収依頼書
10.検査合格通知書兼検収書（ソフトウェア設計・制作業務契約）

チェックリスト

1.コンサルティング会社選定のためのチェックリスト
2.提案依頼書(RFP)のチェックリスト
3.業務システム仕様書の記述レベル
4.ユーザ IT 成熟度チェックリスト
5.パッケージソフトウェア選定のためのチェックリスト
6.SaaS/ASP 選定のためのチェックリスト
7.検収事前チェックリスト
8.検収チェックリスト
9.セキュリティチェックシート 一般版（上位概念）
10.セキュリティチェックシート Web アプリケーション版
11.SaaS 向け SLA におけるサービスレベル項目のモデルケース

提出日：〇〇〇〇年〇〇月〇〇日

本紙を含む全〇枚

1.第〇回　〇〇〇〇プロジェクト連絡協議会議事録（記入例）

（委託者）株式会社〇〇商事 御中

（受託者）△△システム株式会社
〇〇事業部
作成者 〇〇〇〇 印

パッケージソフトウェア利用コンピュータシステム構築委託モデル契約書第 4 条 6 項に基づき、議事録を提出いたします。精査の上、ご承認をお願い申し上げます。

開催日時：	〇〇〇〇年〇〇月〇〇日　〇〇時〇〇分～〇〇時〇〇分
開催場所：	株式会社〇〇〇〇〇〇〇 本社会議室
出席者：	株式会社〇〇〇〇〇〇〇
	責任者〇〇、〇〇、〇〇
	〇〇〇〇〇株式会社
	責任者〇〇、〇〇、〇〇

議事：（契約書第 4 条 7 項により、決定事項、継続検討事項がある場合は検討スケジュール及び検討当事者を記載の事。）

以上、議事の内容に相違ないことを確認し、本議事録を承認いたします。

（委託者）株式会社〇〇商事　　責任者　〇〇〇〇　印

（受託者）△△システム株式会社　　責任者　〇〇〇〇　印

2.設定等合意書（記入例）

〇〇〇〇年〇〇月〇〇日付けパッケージソフトウェア利用コンピュータシステム構築委託契約書第 2 条⑥に基づき、下記の通り別紙重要事項説明書記載の設定等及びもしくは条件の変更について合意し決定しました。

■　　合意した設定等（設定の変更、仕様の修正、追加事項、未決定事項等）の内容：

■　　必要な措置、付帯事項、特約条項：

■　　条件の変更（委託料金、納期等）：

■　　添付資料（議事録、提案書、見積書等）：

以上の合意に相違ありません。　　〇〇〇〇年〇〇月〇〇日

（委託者）株式会社〇〇商事　　責任者　〇〇〇〇　印

（受託者）△△システム株式会社　　責任者　〇〇〇〇　印

○○○○年○○月○○日

3.業務完了報告書兼検収依頼書（記入例）

（委託者）株式会社○○商事　御中

（受託者）△△システム株式会社
○○事業部

○○○○年○○月○○日付けパッケージソフトウェア選定支援及び要件定義支援業務契約（カスタマイズモデル）の業務が完了いたしましたので、下記の通り報告書をご提出申し上げます。
つきましては、○○○○年○○月○○日までにご精査頂き、ご検収をお願い申し上げます。

記

件名：　○○○○システム

期間：　○○○○年○○月○○日～○○月○○日

報告書：　○○○○年○○月○○日付け
○○○○システム　要件定義書 第○○版 一式
（文書明細は別添の通り）

提出場所：　東京都千代田区○○○○○○○○
株式会社○○商事営業本部

作成責任者：　△△システム株式会社○○事業部 ○○○○
〒○○○-○○○○ 東京都千代田区霞が関○○-○○
TEL. 03-○○○○-○○○○

契約金額：　○○○○円

以上

〇〇〇〇年〇〇月〇〇日

4.業務完了確認書兼検収書（記入例）

（受託者）△△システム株式会社　御中

（委託者）株式会社〇〇商事

〇〇〇〇年〇〇月〇〇日付けパッケージソフトウェア選定支援及び要件定義支援業務契約（カスタマイズモデル）の業務完了を確認し、報告書を検収いたしました。

記

件名：　〇〇〇〇システム

期間：　〇〇〇〇年〇〇月〇〇日～〇〇月〇〇日

報告書：　〇〇〇〇年〇〇月〇〇日付け
〇〇〇〇システム　要件定義書 第〇〇版 一式
（文書明細は別添の通り）

提出場所：　東京都千代田区〇〇〇〇〇〇〇〇
株式会社〇〇商事営業本部

作成責任者：　△△システム株式会社〇〇事業部 〇〇〇〇
〒〇〇〇-〇〇〇〇 東京都千代田区霞が関〇〇-〇〇
TEL. 03-〇〇〇〇-〇〇〇〇

契約金額：　〇〇〇〇円

以上

○○○○年○○月○○日

5.業務完了報告書兼外部設計書承認依頼書（記入例）

（委託者）株式会社○○商事　御中

（受託者）△△システム株式会社

○○○○年○○月○○日付け外部設計支援業務契約の業務が完了いたしましたので、下記の通り報告書をご提出申し上げます。
つきましては、○○○○年○○月○○日までにご精査頂き、ご承認をお願い申し上げます。

件名：　○○○○システム

期間：　○○○○年○○月○○日～○○月○○日

報告書：　○○○○年○○月○○日付け
○○○○システム　外部設計書 第○○版 一式
○○○○システム　外部設計支援作業実績一覧表 一式
（文書明細は別添の通り）

提出場所：　東京都千代田区○○○○○○○○
株式会社○○商事営業本部

作成責任者：　△△システム株式会社○○事業部 ○○○○
〒○○○-○○○○ 東京都千代田区霞が関○○-○○
TEL. 03-○○○○-○○○○

契約金額：　○○○○円

以上

○○○○年○○月○○日

6.業務完了確認書兼外部設計書承認書（記入例）

（受託者）△△システム株式会社　御中

（委託者）株式会社○○商事

○○○○年○○月○○日付け外部設計支援業務契約の業務完了を確認し、報告書を承認いたしました。

件名：　　○○○○システム

期間：　　○○○○年○○月○○日～○○月○○日

報告書：　　○○○○年○○月○○日付け
○○○○システム　外部設計書 第○○版 一式
○○○○システム　外部設計支援作業実績一覧表 一式
（文書明細は別添の通り）

提出場所：　東京都千代田区○○○○○○○○
株式会社○○商事営業本部

作成責任者：　△△システム株式会社○○事業部 ○○○○
〒○○○-○○○○ 東京都千代田区霞が関○○-○○
TEL. 03-○○○○-○○○○

契約金額：　　○○○○円

以上

〇〇〇〇年〇〇月〇〇日

7.〇〇〇〇システム構築・設定業務完了報告書兼検収依頼書（記入例）

（委託者）株式会社〇〇商事　御中

（受託者）△△システム株式会社
〇〇事業部

〇〇〇〇年〇〇月〇〇日付け構築・設定業務契約に基づく作業が完了いたしましたので、下記の通り構築・設定業務報告書及び納品書をご提出申し上げます。
つきましては、〇〇〇〇年〇〇月〇〇日までに検査の上、ご検収をお願い申し上げます。

記

件名：　〇〇〇〇システム

期間：　〇〇〇〇年〇〇月〇〇日～〇〇月〇〇日

作業内容：　〇〇〇〇年〇〇月〇〇日付け構築・設定業務契約に基づく 一式

報告書：　〇〇〇〇年〇〇月〇〇日付け
〇〇〇〇システム　構築・設定業務設定報告書 第〇〇版 一式
（文書明細は別添の通り）

納品書：　別添の通り

提出場所：　東京都千代田区〇〇〇〇〇〇〇〇
株式会社〇〇商事営業本部

担当責任者：　△△システム株式会社〇〇事業部 〇〇〇〇
〒〇〇〇-〇〇〇〇 東京都千代田区霞が関〇〇-〇〇
TEL. 03-〇〇〇〇-〇〇〇〇

契約金額：　〇〇〇〇円

以上

〇〇〇〇年〇〇月〇〇日

8.検査合格通知書兼検収書（記入例）

（受託者）△△システム株式会社　御中

（委託者）株式会社〇〇商事

〇〇〇〇年〇〇月〇〇日付け構築・設定業務契約の受け入れ検査に合格し、報告書を検収いたしました。

記

件名：　〇〇〇〇システム

期間：　〇〇〇〇年〇〇月〇〇日～〇〇月〇〇日

作業内容：　〇〇〇〇年〇〇月〇〇日付け構築・設定業務契約に基づく 一式

報告書：　〇〇〇〇年〇〇月〇〇日付け
〇〇〇〇システム　構築・設定業務報告書 第〇〇版 一式
（文書明細は別添の通り）

提出場所：　東京都千代田区〇〇〇〇〇〇〇〇
株式会社〇〇商事営業本部

担当責任者：　△△システム株式会社〇〇事業部 〇〇〇〇
〒〇〇〇-〇〇〇〇 東京都千代田区霞が関〇〇-〇〇
TEL. 03-〇〇〇〇-〇〇〇〇

契約金額：　〇〇〇〇円

以上

○○○○年○○月○○日

9.納品書兼検収依頼書（記入例）

（委託者）株式会社○○商事　御中

（受託者）△△システム株式会社
○○事業部

○○○○年○○月○○日付けソフトウェア設計・制作業務契約に基づくソフトウェア設計・制作作業が完了いたしましたので、下記の通り納品申し上げます。
つきましては、○○○○年○○月○○日までに検査の上、ご検収をお願い申し上げます。

記

件名：　○○○○システム

期間：　○○○○年○○月○○日～○○月○○日

作業内容：　○○○○年○○月○○日付け○○○○システム要件定義書に基づく
ソフトウェア設計・制作、適格性テスト実施、ドキュメント作成 一式

納品物：

システム設計書	印刷物 2 部
適格性テスト仕様書及び報告書	印刷物 2 部
運用マニュアル	印刷物 2 部
ユーザマニュアル	印刷物 2 部
オブジェクト及びソースコード、ドキュメント一式	CD-ROM2 部

（上記ファイル明細は別添通り）

納品場所：　東京都千代田区○○○○○○○○
株式会社○○商事本社ビル 3F　サーバールーム内
○○社製 型番○○○○○○○ サーバ（IP アドレス：192.168.○○.○○）

担当責任者：△△システム株式会社○○事業部 ○○○○
〒○○○-○○○○ 東京都千代田区霞が関○○-○○
TEL. 03-○○○○-○○○○

契約金額：　○○○○円

以上

○○○○年○○月○○日

（委託者）株式会社○○商事　御中

（受託者）△△システム株式会社
○○事業部

納品ファイル明細書

媒体ボリューム名：					
ディレクトリ名	ファイル名	形式	バージョン	日付	サイズ

※○○○○年○○月○○日付けソフトウェア設計・制作業務契約に基づくソフトウェア設計・制作作業の納品明細書です。

○○○○年○○月○○日

10.検査合格通知書兼検収書（記入例）

（受託者）△△システム株式会社　御中

（委託者）株式会社○○商事

○○○○年○○月○○日付けソフトウェア設計・制作業務契約に基づくソフトウェア設計・制作作業の受け入れ検査に合格し、報告書を検収いたしました。

記

件名：　○○○○システム

期間：　○○○○年○○月○○日～○○月○○日

作業内容：　○○○○年○○月○○日付け○○○○システム要件定義書に基づく
ソフトウェア設計・制作、適格性テスト実施、ドキュメント作成 一式

納品物：

システム設計書	印刷物 2 部
適格性テスト仕様書及び報告書	印刷物 2 部
運用マニュアル	印刷物 2 部
ユーザマニュアル	印刷物 2 部
オブジェクト及びソースコード、ドキュメント一式	CD-ROM2 部
（上記ファイル明細は別添通り）	

納品場所：　東京都千代田区○○○○○○○○
株式会社○○商事本社ビル 3F　サーバールーム内
○○社製 型番○○○○○○○ サーバ（IP アドレス：192.168.○○.○○）

担当責任者：△△システム株式会社○○事業部 ○○○○
〒○○○-○○○○ 東京都千代田区霞が関○○-○○
TEL. 03-○○○○-○○○○

契約金額：　○○○○円

以上

1.コンサルティング会社選定のためのチェックリスト

コンサルティングを導入するには、コンサルティング会社もしくはコンサルタントのポリシーや信頼性について評価を行う必要がある。コンサルタント選定にあたって、解説を参考に、以下の評価軸で評価を行う。

◎：期待以上である　○：十分なレベルである　△：不十分なレベルである　×：記述レベルが明らかに不足もしくは記述がない　ＮＡ：該当しない、不明

コンサルティング会社

記述項目	解説	評価
経営安定性	コンサルティング会社の経営は安定しているか	
コンサルティングポリシー	どのようなコンサルティングを目指しているのかを確認。堅実な解答、積極的な解答	
実績	類似コンサルティング業務の実績（最近 1 年間のコンサルティング内容、期間、フェーズ、業種、企業規模などを記述する）	
品質失敗実績	最近 3 年間の品質が損なわれた失敗実績を説明してもらう	
得意分野	得意の業務分野を記述してもらう	
コンサルタントの人数	所属するコンサルタントの人数、資格保持者の数	
コンサルタントの入れ替え	所属するコンサルタントの平均滞在年数	

担当コンサルタント

記述項目	解説	評価
担当コンサルタント	担当コンサルタントの略歴	
担当コンサルタントのスキルレベル	IT スキル標準、情報システムユーザスキル標準、情報処理技術者試験などによる証明	
チームバランス	チーム内のスキルの充足度	
コミュニケーション力	提案などに来たときに、きちんと質疑応答ができている、一方的に話していないか	
業務分野提案力	提案内容に筋が通っていて、依頼内容に沿っている	
論理性	提案や説明の内容が論理的である	
人柄	会話をしていて不快感を与えないか、高圧的ではないか	

他ユーザからのコンサルティング会社に対する評価

記述項目	解説	評価
満足度	使い勝手、投資効果について悪い評価はないか	

提案書

記述項目	解説	評価
背景	説明した背景などを理解して記述している	
	業界の環境などを理解して記述している	
目的	説明された目的を理解し記述している	
方針	説明された目的を踏まえた上で検討方針を明確に提示している	
アプローチ	企画作成、提案依頼書（RFP）作成、プロジェクト・マネジメント・オフィス（PMO）支援などの目的を達成するための方法論を提示している	
	企画作成、RFP 作成、PMO 支援などの目的を達成するためのタスクを提示している	
アウトプットイメージ	成果物の構成や記述レベル、分量、サンプルなどを提示する	
スケジュール	全体のスケジュールが詳細化され、報告方法やマイルストンが明示されている	
体制	プロジェクトの意思決定体制、チーム構成などを記述している	
	プロジェクトメンバのスキル、実績などを記述している	
実績	類似プロジェクトの概要を記述する。	

2.提案依頼書(RFP)のチェックリスト

当該システム構築の前提として、「ユーザ企業の現況及び環境」を示す必要がある。ユーザ企業が有する EA、IT ガバナンスの方針、情報セキュリティ基本方針、情報資産管理の方針、事業継続計画、コンプライアンス方針等の中から、当該システム構築の前提として、必要と思われる部分をベンダに開示する必要がある。作成した RFP を、解説を参考に、以下の評価軸で評価を行う。

◎：内容は期待以上のレベルで記述されている　○：十分なレベルで記述されている　△：記述が曖昧もしくは不足　×：レベルが低いもしくは記述がない　NA：該当しない、不明

システムの概要(基本方針)

記述項目	解説	評価
システム化の目標・方針	提案依頼に関し、システム化規模が企業の全体・部分・改造なのか、システム形態が集中型・分散型・ネットワーク型なのか、システム構築が新しい生産環境の構築や技術の大規模な再編成なのか、既存ソフトウェア資産の継続なのか、切り換えなのか、業務の効率化・生産性向上・高付加価値サービスの開発なのか、国内外のネットワークの拡大や情報化ニーズの高度化・複雑化の解消なのか等、今回のシステム化の目的・方針等を具体的に明示する。これらの明示のためには、ユーザ内において、システム化構想にかかわるステークホルダの意思統一を図り、経営層が明確な意思決定を行った上で、明示しなければならない。	
狙いとする効果	企業の戦略等機密事項も含まれるので、抽象的表現にならざるを得ないが、ユーザのシステム化の狙い、例えば、ダウンサイジング化や低価格化、事務や業務の効率化や生産性向上、情報処理の迅速化によるサービスの向上、システム資源の集約化や再利用化等、システム化の狙いと効果の特徴を明示する。	
運用対象者	システムを運用管理する人やシステムを日常的に利用し操作する人が専任なのか、不慣れな人なのか、また同時に何人がこのシステムを利用するのか等を明示する。	
既存システムとの関連	現在稼働中のシステム機器類の構成、取り扱うデータの種類や量や処理サイクル等、既存システムと今回依頼システムとの情報処理の関連を明示する。また、既存システムと接続する場合の実環境の技術的制約事項があればそれを明示する。	

提案依頼手続

記述項目	解説	評価
説明会の日程	提案依頼の具体的スケジュール、例えば、システム導入時期、導入説明会の場所や日時、提案書提出期限、提案システムのヒアリング日時、入札日、ベンダ決定時期等を明示する。	
対応窓口	ベンダ決定までの対応窓口組織や責任者等の氏名・職制・電話番号・FAX 番号等を明確にし、質問や問い合わせに関する対応方法について明示する。	
提供する資料	提案依頼に際して提供する会社案内書、システム関連資料、提案依頼の日程等の案内のほか、各種提供した資料の機密性の有無、返還の必要性等を明示する。	
参加資格条件	提案や入札に参加できる条件、例えば、ISO 9000 や IS014000 シリーズ認証、プライバシーマーク認定、ISMS 認証等の取得の有無 117、企業規模、業務知識や専門技術の有無、開発実績の有無、情報処理技術に関わる試験合格・資格者の人数や、支社店や支援組織体制が近くにある等、独占禁止法に抵触しない範囲での各種参加資格要件を明示する。	
提案手続	提案依頼に対応して、今回の提案書や見積書の提出によって、即刻業者選定を実施するのか、最初は提案書提出の意志や技術の確認等を第 1 次審査で行い、提案要求をさらに詳細に明確にして、再度、提案依頼を出し、これに対応する提案書や見積書によって業者選定を行うのか等の業者決定の手順を明示する。	
ベンダ選定方法	ベンダ選定を行う組織・決定機関等、決定までのプロセス等をわかる範囲で明示する。	

依頼事項

記述項目	解説	評価
システム化の依	システム化依頼の業務や機能の範囲を明確にする。具体的には、システム全体の構造	

記述項目	解説	評価
頼範囲	や、既存システムや今後の開発計画と今回開発予約部分との関連を明確にする。特に、範囲外の部分については詳細を明示する。 明示に当たっては、機能要件（インターフェース）を示すシステム間関連図、システム間インターフェース定義書等のドキュメントが有効である。	
依頼内容・業務の詳細 機能要件①プロセス	機能情報関連図：業務機能間の情報（データ）の流れを明確にする。 業務流れ図：業務がどのような組織、手段、手順で処理されるかを明確にする。 業務処理定義書：業務流れ図の各業務処理機能の内容を明確にする。 システム機能関連図：業務機能を実現する情報システムの機能を明確にする。	
依頼内容・業務の詳細 機能要件②データ	概念 ER 図：情報システムにおける概念レベルのデータ構造を明確にする。 データ項目定義書：データ項目の要件を明確にする。	
依頼内容・業務の詳細 機能要件③インターフェース	システム間関連図：検討対象システムと既存システム又は周辺システムとのデータの流れを明確にする。 システム間インターフェース定義書：検討対象システムと既存システム又は周辺システムとのデータのやりとりを明確にする。 画面、帳票一覧表：検討対象のビジネス機能で必要となる画面・帳票を業務フローごとに洗い出し、画面・帳票一覧として整理し、基本的なビジネスデータの所在を明確にする。 画面、帳票レイアウト：各画面、帳票のレイアウトサンプルを集め、整理し、基本的なビジネスデータを収集することで、画面・帳票を処理する業務設計条件を明確にする。	
システム構成	システムに必要なソフトウェアの機能を明示する。また、国内外の流通ソフト等があれば例示して、具体的な業務機能を明示する。さらにシステムに必要なハードウェア及び周辺装置及びネットワーク等の概念図や構成事例を例示する。また、必要な容量、機能、性能、ネットワークの接続性については、特記すべき事項を明示する。	
納期	ソフトウェア、ハードウェア等の導入時期、試運転時期、テスト時期、並行処理時期、運用時期等それぞれの納期を明示する。	
必要な技術・技術者の資格	提案依頼に伴って、システムの開発、運用、データベースの取扱いに関し、必要な技術や技術者の資格要件があれば明示する。	
成果物・納入物	今回のシステム依頼に関する成果物、納入物を明示する。特に文書類は、記述方法、記述の詳細さ、印刷等で作業工程が大きく変わる場合があるので、所定の書式なのか、ベンダ側の書式で可なのか、記述事例等をつけて明示する。	
開発標準類の確認	提案依頼するシステム開発の開発標準類をベンダと確認し、開発標準類の変更が必要な場合には、共通フレームの修整プロセスを適用するので、ベンダの参加の有無及び方法を明示する。	
共同レビュー	提案依頼するシステム開発における節目を定義し、ユーザとベンダの双方が参加する共同レビューの進め方を明示する。また、契約レビューの有無と方法についても明示する。	
工程計画	提案依頼物件の作業スケジュールの概要(ユーザ側のチェックポイント時期)を明示する。また工程を管理する上で必要となる会議や報告の周期や方法についても明示する。	
開発推進体制	システムを推進するユーザ側の組織体制の概要を提示する。例えば、調査段階、開発段階、運用段階等それぞれの段階で協力・管理・監査・検収する部門の支援体制を、必要に応じて明示する。	
非機能要件 ①品質要件	システムに対する品質に関する要件 ・品質、性能条件 システムの品質、性能に関し、相互に確認をするための保証、例えば、納入時の品質、テストの方法、テストツールの例示等の品質・性能保証に関する要求を明示する。	
非機能要件	ソフトウェアの開発、維持管理（保守管理）、支援及び実行のための技術・環境に関	

記述項目	解説	評価
②技術要件	連した要件 ・開発モデル・開発言語：システム開発に必要な開発モデル、開発標準や開発ツール等の指定がある場合はそれを明示する。また、開発に必要な言語や特定用途向け言語等があれば、これを明示する。 ・支援ツール：ユーザが持つ支援ツールやベンダに求める支援ツール等について、ツール機能の仕様や性能について明示する。 ・ソフトウェア製品の使用：ユーザが使っているソフトウェア製品、ベンダに新規に求めるソフトウェア製品等について、類似するソフトウェア製品名称、使用条件、個数等の要求を一覧の形で例示する。 ・保守条件：ソフトウェアの保守体制の有無、無償保守期間、ハードウェア保守の体制や組織、夜間休日保守の可能性、時間外保守の単価や条件リモート保守等の条件を明示する。	
③セキュリティ要件	セキュリティに関する要件 ・セキュリティチェックシートに基づく条件：セキュリティチェックシートをもとに具体的に明示する。	
非機能要件 ④運用・操作要件	安定したシステム運用を行うための検討対象のビジネス機能を実行するシステムについての運用要件（含む、SLA、BCP）と操作要件（エンドユーザ操作方法等） ・運用条件：システムの稼働時間や稼働環境に関する運用条件を明示する。例えば、情報システム部門の稼働体制や稼働時間、利用者部門の利用時間や利用方法等を明示する。	
非機能要件 ⑤移行要件	現行システムから新システムへの移行対象、移行方法などの移行に関する要件 ・移行条件：移行対象業務・プログラム・ハードウェア、移行手順、移行時期等を明示する。	
非機能要件 ⑥付帯作業	システム構築に付帯する作業に関する要件	
非機能要件 ⑦その他	上記に該当しない要件（導入教育等）	

開発体制・開発環境

記述項目	解説	評価
役割分担	ユーザとベンダ双方の作業進捗や費用負担の責任を明確にするため、作業推進の工程毎に発生する各種作業のそれぞれの役割や完了時期を明示する。役割分担の表示に際しては、責任者の明示と共に、機能要件（インターフェース、プロセス、データ）、非機能要件（品質要件、技術要件、その他の要件）の担当者名も明示する。	
作業場所	システム開発に伴い、工程別に必要となる作業場所、例えば、作業室、会議室、開発用計算機や端末や通信装置等の設置場所の提供が可能か否か、これらはユーザ、ベンダのいずれが準備すべき事項なのかを明示する。	
開発機器・使用材料費の負担	システム開発に必要な資材、例えば、開発用電子計算機費用の負担方法、端末や周辺装置の導入時期や負担方法、また、備品や消耗品類の有償・無償等の提供条件を明示する。	
貸与物件・資料	システム開発に必要な資料・伝票・書類・機器類等の貸与の条件や、機密保持条件、返還の必要性、持ち出し禁止条件等について明示する。	

保証要件

記述項目	解説	評価
システム	ソフトウェアのバグ等に関する保証期間、ハードウェア装置の機能・性能に関する保証要件や限界性能、ネットワークの機能や接続台数等に関するシステムとしての保証要件を明示する。	
品質保証基準	ソフトウェア・ハードウェア・ネットワークの機能や性能の保証基準を明示する。また、文書類の記述方法の基準や標準等があれば、それら基準を具体的に明示する。	
記述項目	解説	評価
システムの性能	ソフトウェア機能、性能に関する安全性、ハードウェア装置の機能・性能、容量等に関する信頼性や、ネットワークの機能・性能に関する応答性、その他システム全体の信頼性、安全性・応答性等の保証に関する要求を明示する。	
セキュリティ	計算機や端末に関する可用性の確保、利用者に関する個人情報の安全管理、業務システムの利用に関する機密性の確保等、システムに必要なセキュリティ上の対策（機密性、可用性及び完全性の確保）や障害発生に対する状況別対応策の必要性を明示する。また、「情報システムの構築等におけるセキュリティ要件及びセキュリティ機能の検討に関する解説書」（内閣官房情報セキュリティセンター）を参考にすること。	
デモ・テスト計画	システムモデルの提示やシステム機能確認のためのデモの必要性、その他テストの時期等について明示する。	

契約事項

記述項目	解説	評価
発注形態	システム開発の発注形態が、例えば、基本契約と個別サービス契約、SI 包括契約、部分請負契約、ソフトウェアのみの契約等、発注に関する形態を明示する。	
その他、契約書中に盛り込むべき重要事項	契約類型（準委任／請負）、再委託、損害賠償責任（範囲・限度額・期間）、知的財産権の帰属、第三者ソフトウェアの利用、検収・支払い条件等について、これらの条件、あるいは要求について予め明らかにしておく。	

その他

記述項目	解説	評価
用語	提案依頼書に使用している用語の定義を明示する。共通フレーム 2007 の用語を使用することが望ましい。また、ベンダに対し提案書で使用する用語と共通フレーム 2007 の用語との読み替え表が必要ならその旨明示する。	
外部委託に関する管理	ベンダが、システム、ソフトウェア製品の開発又はソフトウェアサービスを外部委託しようとする場合の外部委託の管理方法（事前通知の要否等）を明示する。	
リスクに対する相互認識	システムの開発に関しユーザとベンダの双方が、新技術適用のリスクや詳細仕様決定の遅れあるいは開発作業の遅れ等のリスクの予測や費用増大に対する原価意識を持ち、双方の立場を尊重し合いながら、予測されるリスクの抑制を徹底して管理していく必要があることを明示し、相互認識とする。	
仕様変更・機能追加等の条件	大きなシステム開発に関しては、開発契約締結後にシステム仕様の補正(機能追加)や仕様変更等が生じるので、これを管理する変更管理プロセスを契約書において明示する。	

3.業務システム仕様書の記述レベル

システム発注にあたっては、業務システム仕様書を作成する必要がある。そのときの記述レベルを明確にすることで、合意レベルも明確になり、トラブルを防止することができる。以下は日本情報システム・ユーザ協会「ビジネスシステム定義研究 2004」で作成したレベルである。A-D のドキュメントはユーザ部門には必要であるが、見積もり時に必ずしも添付する必要はない業務システム仕様書であり、ドキュメント 1-10 が見積要求仕様書となる。

仕様の責任と記述項目			レベル 1 ビジネス機能提示	レベル 2 ビジネスプロセス提示	レベル 3 業務フロー提示	レベル 4 業務処理提示	レベル 5 業務処理/データ項目提示
責任分担	1	ユーザ側責任	RFP レベルでベンダ提案書をベースに要求仕様書を明確にしシステム構築	既存システム再構築ではビジネスプロセス定義と既存システム仕様提示で発注	As-Is ベース機能拡張で業務フローを通常業務/例外業務処理につき提示	To-Be ベースの業務処理方法の提示による効果的な発注	To-Be ベースのシステム構築の発注によるシステム構築効率追及
			要求仕様承認の責任	基本設計承認の責任	詳細設計/機能性能の承認	納品仕様/成果物の仕様承認	システム設計の効率化推進
	2	ベンダ側責任	RFP のビジネス機能から To-Be のあるべき姿のシステム機能を提案	提示ビジネスプロセスの改革を実現するシステム構築を実現	更なる To-Be 機能への展開とシステム設計と納品物の QCD 追求	To-Be ベースの IT 処理方式からの改善改革と構造的で明快なシステム構築	To-Be ベースのシステム機能強化と最適化の追求
			納入/契約仕様の実現	設計、納入品の瑕疵責任	システム設計開発の合理化/コスト低減	きれいな構造設計/コスト低減	システム設計開発の合理化/コスト低減
A	ビジネス機能関連図				IS 部門で企業/事業全体機能定義	IS 部門で企業/事業全体機能定義	IS 部門で企業/事業全体機能定義
B	ビジネス連携図				業務と対外系/他部門間との連携	業務と対外系/他部門間との連携	業務と対外系/他部門間との連携
C	ビジネスルール定義書				企業/業務上の戦略ルール	企業/業務上の戦略ルール	企業/業務上の戦略ルール
D	システム化目標定義書		業務システム化の目標設定	業務システム化の目標設定	業務システム化の目標設定	業務システムの IT 効果定義	業務システムの IT 効果定義
1	ビジネス機能構成表		ビジネス機能の大分類定義	ビジネス機能の中小分類定義	ビジネス機能の細分類定義	ビジネス機能の細分類定義	ビジネス機能の細分類定義
2	ビジネスプロセス関連図			ビジネスプロセス間の関連定義	ビジネスプロセス間の関連定義	ビジネスプロセス間の関連定義	ビジネスプロセス間の関連定義
3	業務流れ図				業務処理フロー指示 （含む例外処理）	業務処理フロー指示 （含む例外処理）	業務処理フロー指示 （含む例外処理）
4	業務機能関連図					DFD 方式での 上位 DFD として作成	DFD 方式での 上位 DFD として作成
5	業務ルール定義書					業務処理上の社内ルールを定義	業務処理上の社内ルールを定義
6	業務処理手順書					個別の業務処理手順を定義	個別の業務処理手順を定義
7	画面／帳票一覧				基本的に必要な画面/帳票一覧	基本的に必要な画面/帳票一覧	基本的に必要な画面/帳票一覧
8	画面／帳票レイアウト				画面/帳票レイアウトを定義	画面/帳票レイアウトを定義	画面/帳票レイアウトを定義
9	データ項目定義書						データ項目の属性を定義
10	運用・操作要件所				業務システムの 運用・操作の条件設定	業務システムの 運用・操作の条件設定	業務システムの 運用・操作の条件設定
該当仕様書評価							

上記評価欄にチェックとコメントを記載

4.ユーザ IT 成熟度チェックリスト

IT を導入するときに、ユーザの IT に対する準備状況（成熟度）が結果に大きな影響を与えることがあり、ベンダにとって重要な情報である。よって、ＲＦＰを出すときなどにユーザ十進が自分のレベルについて評価を行うことが望ましい。また、ＲＦＰに第三者評価を行う場合にも公正なチェックリストがあることが望ましい。ここでは、経済産業省 IT 経営力指標を活用する。IT 導入にあたってのユーザ成熟度を、以下の評価軸で評価を行う。

◎：期待以上である　　○：十分なレベルである　△：不十分なレベルである　×：できていない

ＮＡ：該当しない、不明

ユーザ評価チェックシート　Ⅰ．経営戦略と IT 戦略の融合

	ステージ 1	ステージ 2	ステージ 3	ステージ 4
評価項目	◆経営層は解決すべき自社の経営課題を把握していない。	◆不十分なところはあるが経営層は解決すべき自社の経営課題を把握している。	◆経営層は解決すべき自社の経営課題を十分把握している。	◆経営層は解決すべき自社の経営課題を十分把握している。
評価				
評価項目	◆経営戦略が策定されていない。あるいは経営戦略は策定されているが実行不可能な非現実的なものである。	◆策定された経営戦略が、経営層のみの周知に留まっており全社的に浸透していない。 ◆経営戦略の想定対象期間が比較的短期（概ね 1 年程度の将来）である。 ◆経営戦略としての全社的な視点に欠ける部分はあるものの、事業部門、機能別組織単位では効率化の促進や付加価値を創造している。	◆策定された経営戦略が、全従業員に周知されている。あるいは経営層及び管理者層に周知され、管理者層の指揮命令の下に従業員が業務を遂行している。 ◆経営戦略の想定対象期間が比較的中長期（概ね３年以上）を見据えている。 ◆経営戦略は、業務改革の実行が中心である。 ◆経営戦略が、企業全体あるいは企業グループ全体の視点から、事業部門、機能別組織の部門戦略に横串を刺した形で策定されている。この結果、企業全体あるいは企業グループ全体での効率化の促進や付加価値を促進するかどうかが経営戦略の具体的な実行にあたっての判断基準となっている。	◆策定された経営戦略が、全従業員に周知されている。あるいは経営層及び管理者層に周知され、管理者層の指揮命令の下に従業員が業務を遂行している。 ◆経営戦略の想定対象期間が比較的中長期（概ね３年以上）を見据えている。 ◆経営戦略には、ビジネス環境の変化を見極め、業務改革の実行及び新しいビジネスモデルの展開を織り込んでいる。 ◆垂直型の企業間連携（調達先から販売先に至るまでの連携）や、水平型の企業間連携（同一産業内での連携）での実現可能性を考慮に入れた上で、企業全体、あるいは企業グループ全体の視点から経営戦略が策定されている。この結果、企業間連携全体で最適な効果を得られるかどうかが経営戦略の具体的な実行にあたっての判断基準になっている。
評価				
評価項目	◆IT 戦略が策定されていない。あるいは IT 戦略は策定されているが実行不可能な非現実的なものである。	◆IT 戦略は経営戦略と整合性が取れている。 ◆IT 戦略の決定プロセスには、経営層が参画している。 ◆IT 戦略が事業部門、機能別組織の単純合計となっている。あるいは全社的な視点から IT 戦略は策定されているが、企業内部での周知が十分ではない。 ◆全社的な視点からの IT の活用や IT 投資判断を下すまでには至っていないが、事業部門、機能別組織単位では効率化の促進や付加価値を創造するような IT 活用、IT 投資を行っている。	◆IT 戦略は経営戦略と整合性が取れている。 ◆IT 戦略の決定プロセスには、経営層が参画している。 ◆IT 戦略が企業全体あるいは企業グループ全体の視点から事業部門、機能別組織の IT 活用方針に横串を刺した形で策定されている。この結果 IT の活用や IT 投資の判断を下すにあたり、企業全体あるいは企業グループ全体での効率化の促進や付加価値を促進するような IT 活用、IT 投資を行っている。	◆IT 戦略は経営戦略と整合性が取れている。 ◆IT 戦略の決定プロセスには、経営層が参画している。 ◆IT 戦略の策定にあたり、IT を活用した垂直型の企業間連携（調達先から販売先に至るまでの連携）や、水平型の企業間連携（同一産業内での連携）の実現可能性を考慮に入れた上で、企業全体、あるいは企業グループ全体の視点から事業部門、機能別組織の IT 活用方針に横串を刺した形で策定されている。この結果、企業間連携全体で最適な効果を得られるかどうかが IT の活用、投資の判断基準になっている。
評価				
評価項目	◆IT 導入の目的が不明確であり、効果が得られていない。	◆事業部門、機能別組織内部の効率化や付加価値の創造、あるいは事業部門、機能別組織が直接的に接する外部組織との取引関係、情報共有などが IT 戦略の中心となっている。	◆企業、企業グループにおける情報の共有化や取引プロセスの効率化、あるいは顧客の視点に立った付加価値の創造などが IT 戦略の中心となっている。	◆垂直型企業間連携、水平型企業間連携における情報の共有化や取引プロセスの効率化、あるいは顧客の視点に立った付加価値の創造などが IT 戦略の中心となっている。

	ステージ 1	ステージ 2	ステージ 3	ステージ 4
評価				

基礎的事項	評価
◆自社の社風、企業規模、業種、製品やサービスなどと、IT との親和性を経営者が理解している。	
◆IT を適材適所に導入し活用することによって、新価値創造、競争優位性獲得をより効率的、効果的に実現できる可能性を経営者は理解している。	
◆IT 戦略の策定においては、IT に関する新規技術や新規のソリューション動向を随時把握し、それらを適切に活用する視点が織り込まれている	
◆経営層は、CIO や CIO の機能を有する者と定期的・継続的に IT の活用に関する意見交換を実施している。	

Ⅱ．現状の可視化による業務改革の推進と IT の活用による新ビジネスモデルの創出、ビジネス領域の拡大

	ステージ 1	ステージ 2	ステージ 3	ステージ 4
評価項目	◆社内の業務プロセスの可視化が行われていない。◆無駄・重複・非効率・属人性がどの部分から生じているのか把握していない。	◆社内の業務プロセスが全従業員に理解できるほどに可視化(フローチャートによる“ 見える化 ”や業務の文書化）されており、事業部門､機能別組織単位で無駄・重複・非効率・属人性の排除に取り組むための業務改革が行われている。	◆社内の業務プロセスが全従業員に理解できるほどに可視化(フローチャートによる“ 見える化 ”や業務の文書化）されており、無駄・重複・非効率・属人性の排除に取り組むために、事業部門、機能別組織単位だけではなく､各組織、部門間にまたがる企業全体、企業グループ全体での業務改革が行われている。 ◆可視化によって作成された文書は文書管理システムの導入などによって、更新履歴管理も行われている。	◆連携先企業とのやりとりを含め、業務プロセスが全従業員に理解できるほどに可視化（フローチャートによる“ 見える化 ”や業務の文書化）されており、無駄・重複・非効率・属人性の排除に取り組むために、企業全体、企業グループ全体だけではなく、連携範囲全体にまたがった業務改革が行われている。 ◆可視化によって作成された文書は文書管理システムの導入などによって、更新履歴管理も行われている。
評価				
評価項目	◆業務改革を行っていない。	◆業務改革の主たる要素が無駄の排除や効率化であり､IT の活用も省力化、自動化が中心であって､情報共有という観点からの IT 活用は事業部門、機能別組織単位に限られている。	◆業務改革の主たる要素が無駄の排除や効率化から情報の共有に移っており､IT の活用も省力化、自動化だけにとどまらず情報共有による新しい価値の創造が中心となっている。	◆業務改革の範囲が企業全体、あるいは企業グループ全体での無駄の排除や効率化、情報の共有に移っており、IT の活用も垂直型、水平型企業間での省力化、自動化、情報共有による新しい価値の創造が中心となっている。
評価				
評価項目	◆IT の導入による効果が得られていない。	◆事業部門､機能別組織内部の情報共有が IT を活用することによって促進された結果､新規顧客の開拓や新たなサービスの創出など収益の向上につながった。	◆企業全体、あるいは企業グループ全体での情報共有が IT を活用することによって促進された結果、新たな業務プロセスを生み出すようなビジネスモデルやサービスが生まれ、顧客満足度の向上につながった。	◆取引先、同業他社も含めた企業間連携内での情報共有が IT の活用によって促進された結果、既存の企業間連携を深化させる、あるいは新たな企業間連携を生み出すようなビジネスモデルやサービスが生まれ、顧客満足度の向上につながった。
評価				
評価項目	◆自社にとっての脅威を把握できていない。	◆自社にとっての脅威を把握している。	◆自社にとっての脅威を把握し、発生可能性、発生した場合の損害の程度などをもとに優先順位を付けた上で、損害を発生させないための仕組みを構築する。 ◆IT の活用によって、損害の実現を防止、発見するための機能を効率的に対応策に組み	◆自社にとっての脅威を把握し、発生可能性、発生した場合の損害の程度などをもとに優先順位を付けた上で、同業他社、取引先等との連携によって損害の発生を防ぐとともに、そのためのコストシェアなどを実現する。 ◆IT の活用によって、損害の実現を防止、発見するための機能を効率的に対応策に組み込む。

	ステージ 1	ステージ 2	ステージ 3	ステージ 4
			込む。	
評価				
評価項目	◆職務権限や職務分掌が明確に定められていない。 ◆業務が属人的になっている。	◆職務権限と職務分掌が定められており、定期的に見直されている。	◆職務権限と職務分掌が定められ、定期的に見直されている上に、システム化された業務部分については、職務権限、職務分掌を超えた権利行使ができないよう、IT を利用したアクセス制限やログ管理といった予防的な措置が施されている。	◆情報へのアクセスや利用・活用に関する連携企業相互間での契約や覚書などが取り交わされており、かつシステム化された業務部分については、契約で取り決めた範囲や権限を逸脱しないよう、IT を利用したアクセス制限やログ管理といった予防的な措置が施されている。
評価				
評価項目	◆業務プロセスの中の不正や誤りを防止、発見するため手続が仕組みとして定められていない。	◆業務プロセスの中の不正や誤りを防止、発見できるような相互チェックの仕組みを取り入れている。	◆業務プロセスの中に不正や誤りを防止、発見できるような相互チェックの仕組みを取り入れ、内部監査部門など直接的に業務と関連しない部門や担当者が継続してモニタリングしている。	◆業務プロセスの中に不正や誤りを防止、発見できるような相互チェックの仕組みを取り入れた上で、各企業の業務範囲を内部監査部門など直接的に業務と関連しない部門や担当者が継続してモニタリングしているとともに、システムが企業間の連携の中心にある場合にはシステム全体のシステム監査などを実施している。
評価				

III. 標準化された安定的な*IT 基盤の構築

*ハードウェア、ネットワーク設備、基本ソフトウェアなど、アプリケーションに左右されにくい汎用性の高い部分

	ステージ 1	ステージ 2	ステージ 3	ステージ 4
評価項目			◆エンタープライズ・アーキテクチャの概念を導入し、経営資産のポートフォリオを分析し、業務プロセスの標準化を推進する。	◆エンタープライズ・アーキテクチャの概念を導入し、経営資産のポートフォリオを分析し、業務プロセスの標準化を推進する。
評価				
評価項目	◆自社のシステム構成をよく理解していない	◆個別のアプリケーションごとに、ネットワーク、サーバー、ストレージ、ミドルウェア、データベース、認証フレームワークなど（以下、システム基盤）を構築している。	◆自社内に多数存在するアプリケーションに共通して求められる、システム基盤の要件を抽出し、集中、統合化すべきコンポーネントを見極め、共通的なシステム基盤として標準化を実施することで、開発・運用の生産性を向上させ、堅牢で安価なシステム基盤を構築するとともに、ビジネス環境の変化にも容易に対応できている。	◆企業間、産業内で共通化、標準化されたシステム基盤を導入し、開発・運用の生産性を向上させ、堅牢で安価なシステム基盤を構築し、ビジネス環境の変化にも容易に対応できる。
評価				
評価項目	◆全社横断的なシステム基盤の構築ポリシーが作成されていない。あるいは作成されていても遵守がなされていない。	◆全社横断的なシステム基盤の構築ポリシーが作成されていない。あるいは作成されていても遵守がなされていない。	◆全社横断的なシステム基盤の構築ポリシーを定め、システム基盤の中で共通化すべき部分と差別化すべき部分を明確にする。	◆企業間、あるいは産業内でのシステム基盤の構築ポリシーが作成され、企業横断的、産業横断的システムの構築にあたっては構築ポリシーが遵守されている。
評価				
評価項目	◆社内の利害調整を行うことができ	◆社内の利害調整を行うことができず、システ	◆全社横断的な統制管理組織を編成するなど、設計思想・ポ	◆企業横断的に統制管理組織を編成して IT 構造（アーキテクチャ）の安

	ず、システム基盤の標準化が行われていない	ム基盤の標準化が行われていない	リシーに沿った IT 基盤の構築を行うために、社内の利害調整を行い、全社的な観点からの IT 投資計画の推進が行われている。安定化を図ることで、ビジネス環境の変化に安定的に柔軟に対応できる。	定化を図ることで、取引先も含めて、ビジネス環境の変化に安定的に柔軟に対応できる。
評価				

基礎的事項	評価
◆自社の経営資産と経営環境を把握し、将来を見越した情報化モデルを構築する。	
◆導入済みのシステムを定期的に棚卸しし、利用状況やトータルコストを把握し、ソフトウェア資産としての価値を評価する。	

Ⅳ．IT マネジメント体制の確立

	ステージ 1	ステージ 2	ステージ 3	ステージ 4
評価項目	◆IT 戦略を策定していない	◆ 自社の IT 戦略の立案にあたっては、経営層及び IT 利用部門のトップが参画している。	◆経営層及び IT 利用部門のトップが参加する企業全体の IT 戦略の立案・管理に関する協議機関、会議体を有しており、経営の観点から IT 投資の判断をしている。	◆経営層及び IT 利用部門のトップが参加する企業全体の IT 戦略の立案・管理に関する協議機関、会議体を有しており、購買・調達先の情報を社内で共有し、経営の観点から IT 投資の判断をしている。
評価				
評価項目	◆IT の導入や活用について理解しておらず、コンサルタントやベンダーに結果的に丸投げとなっている。	◆CIO、もしくは CIO の機能を有する担当者、担当部門を有しており、自社の IT 投資、IT 資産管理に関する方向性を定め、IT の活用によって自社の業務改革に貢献している。 ◆CIO 機能を有する担当者はいないが、外部のコンサルタント等の助言を受けた上で、経営層が自社の IT 投資、IT 資産管理に関する方向性を定め、IT の活用によって自社の業務改革を推進している。	◆CIO、もしくは CIO の機能を有する担当者、担当部門を有しており、自社の IT 投資、IT 資産管理に関する方向性を定め、IT の活用によって自社の業務改革に貢献している。 ◆グループ CIO・グループ IT 部門を設置し、あるいは同様の機能を有する担当者、担当部門を有しており、企業グループ全体での IT 投資、IT 資産管理に関する方向性を定め、IT の活用によって企業グループ全体の業務改革に貢献している。 ◆CIO 機能を有する担当者はいないが、外部のコンサルタント等の助言を受けた上で、経営層が自社の IT 投資、IT 資産管理に関する方向性を定め、IT の活用によって自社の業務改革を推進している。	◆グループ CIO･グループ IT 部門を設置し、あるいは同様の機能を有する担当者、担当部門を有しており、企業間連携の可能性を視野に入れながら、企業グループ全体での IT 投資、IT 資産管理に関する方向性を定め、IT の活用によって企業グループ全体の業務改革に貢献している。 ◆CIO 機能を有する担当者はいないが、外部のコンサルタント等の助言を受けた上で、経営層が自社の IT 投資、IT 資産管理に関する方向性を定め、IT の活用によって自社の業務改革を推進している。
評価				
評価項目	◆アウトソーサー･ベンダーの評価は行っていない。	◆評価基準は定めていないが、アウトソーサー･ベンダーの評価を行っている。	◆アウトソーサー・ベンダーの定量的な評価基準（SLA など）を定めている。	◆アウトソーサー・ベンダーの定量的な評価基準（SLA など）を定めており、評価結果に対する賞罰を実行している。
評価				

基礎的事項	評価
◆CIO（CIO の機能を担う人材）のミッションは明確に定められている	
◆CIO（CIO の機能を担う人材）は経営層と頻繁に情報交換を行っている。	
◆CIO（CIO の機能を担う人材）は IT に関する新技術、価格動向、将来動向を定期的に把握している	
◆CIO（CIO の機能を担う人材）は自社に必要な IT は何か、またその IT の利用・活用のタイミングを常に意識している	

	ステージ 1	ステージ 2	ステージ 3	ステージ 4	
◆自社 IT 部門（情報システム部門等）、子会社 IT 部門、IT 子会社（情報システム子会社等）、外部ベンダー・アウトソーサーなどのそれぞれの役割や機能、責任などが明確になっている。					
◆自社 IT 部門（情報システム部門等）、子会社 IT 部門、IT 子会社（情報システム子会社等）、外部ベンダー・アウトソーサーなど、それぞれの役割や機能、責任分担に従った行動によって、適正な価格でシステム導入の高い効果を実現している。（CIO のみを置いて、自前での IT 部門を持たず全てアウトソースするという選択もあり得る）。					
◆CEO は自社の経営戦略の実現に向けた IT 戦略の位置づけと IT 活用の有効性についてよく理解し、対外的に説明ができる。					
◆プロジェクトごとにアウトソーサー・ベンダーに求める水準を定めて選定している。					
◆重要なアウトソーシング契約については、弁護士、法務部など法的知識を有している者によってチェックされている。					

Ⅴ．IT 投資評価の仕組みと実践 *1（コンピュータシステムの導入、維持・管理などにかかる総経費を表す指標）

	ステージ 1	ステージ 2	ステージ 3	ステージ 4
評価項目	◆IT 投資によって得られる効果を明確に理解しないまま投資を決断している。	◆プロジェクトごとの IT 投資の効果を投資前に定量（指標を含む）的に予測している	◆プロジェクトごとの IT 投資の効果を投資前に定量（指標を含む）的に予測している	◆プロジェクトごとの IT 投資の効果を投資前に定量（指標を含む）的に予測している
評価				
評価項目	◆IT 投資の効果を感じていない。あるいは導入した IT を使いこなしていない。	◆IT 投資後の投資効果測定を行っていない。	◆プロジェクトごとの IT 投資の効果を投資後に定量（指標を含む）的に測定し、投資前の評価と比較した上で内容の改善やシステムの続行の是非などを判断し、PDCA サイクルを確立している。	◆プロジェクトごとの IT 投資の効果を投資後に定量（指標を含む）的に測定し、投資前の評価と比較した上で内容の改善やシステムの続行の是非などを判断し、PDCA サイクルを確立している。
評価				
評価項目	◆IT 資産の導入コスト、維持･管理コストなどを把握していない。あるいは把握しているが、それが適当であるかどうか検討していない。	◆IT 資産の導入コスト、維持･管理コストなどは次年度の予算ベースでは把握しているが、システムの使用期間トータルでは把握していない。	◆IT 資産の TCO（コンピュータシステムの導入、維持・管理などにかかる総経費を表す指標）を分析し、自社のコスト構造を把握している	◆定期的に IT 資産の TCO*1 を分析し、自社のコスト構造を把握した上で、常に最適なポートフォリオの管理を行っている。
評価				

基礎的事項	評価
◆ IT 投資に対する考え方や判断基準が定められており、経営課題の優先度・緊急度・期待される効果・リスクを整理して、総合的に判断している	
◆ IT 投資実施においては、考え方や判断基準を提示した上で経営層・IT 利用部門の合意を得ている	
◆ IT 投資の評価には、定量的な評価とともに定性的な効果も重視している	
◆CIO と CFO（最高財務責任者）が定期的に IT 投資の効果について意見交換しており、その結果が他の経営層に報告されている	

Ⅵ．IT 活用に関する人材の育成

	ステージ 1	ステージ 2	ステージ 3	ステージ 4
評価項目	◆経営層や社員の IT スキル向上につながるような取り組みは特段行っていない。あるいは行っている場合であっても不定期であり、次回の開催予定は定	◆経営層や社員の IT 活用能力を向上させるために、マニュアルを整備している。 ◆経営層や社員の IT 活用能力を向上させるための研修会や啓蒙活動を定期的に行っている。	◆経営層や社員の IT 活用能力を向上させるために、マニュアルを整備している。 ◆経営層や社員の IT 活用能力を向上させるための研修会や啓蒙活動を定期的に行っている。 ◆経営層や社員の IT 活用能力を向上させるために、ヘルプデスクの設置など、社内外を問わず疑問点についての問い合わせ窓口を用意している。	◆経営層や社員の IT 活用能力を向上させるために、マニュアルを整備している。 ◆経営層や社員の IT 活用能力を向上させるための研修会や啓蒙活動を定期的に行っている。 ◆経営層や社員の IT 活用能力を向上させるために、ヘルプデスクの設置など、社内外を問わず疑問点についての問い合わせ窓口を用意している。 ◆調達先や販売先など連携先企業との間で共通システムを使いこなすための研修

	ステージ 1	ステージ 2	ステージ 3	ステージ 4
	まっていない。			会（共同開催も含む）を定期的に行っている。
評価				

基礎的事項	評価
◆CIO（CIO の機能を担う人材）に求められる要素と水準が明確になっている	
◆CIO（CIO の機能を担う人材）の育成プログラムがある。あるいは、将来の CIO 候補をある程度絞ってキャリアを積ませている。	
◆社内 IT 部門のミッション・職務機能・スキルミックス・責任分界を明確にしている	
◆IT スキル標準などを活用して、社内 IT 部門の社員の技術力・スキルを客観的・数量的に把握する仕組みを持っている	
◆社内 IT 部門の社員のスキルを外部の評価基準（第三者など）を参照して評価している	
◆社内 IT 部門の社員のスキル獲得は、人事評価やキャリアパスとリンクされている	
◆社内 IT 部門の社員に対して、経営戦略と IT 戦略の関係について、CIO 自らが定期的に説明している	
◆経営戦略及び IT 戦略に沿って、自社 IT 部門の社員の採用計画（人数、スキル等を考慮)、採用方針を設定している	
◆自社 IT 部門の社員が、一定期間、IT 利用部門に異動する仕組みがあり、IT 利用部門の求めるニーズを把握したうえで IT の活用方策を検討している。	
◆社内 IT 部門の社員のスキル獲得のための教育プログラムを整備している	
◆自社 IT 部門の社員が新技術や不足するスキルを獲得するために、定期的に、社外のプログラムに参加したり、先進企業で研修を受けたりさせている	

Ⅶ. IT に起因するリスクへの対応

	ステージ 1	ステージ 2	ステージ 3	ステージ 4
評価項目	◆ 経営層は IT に関連・起因するリスク（情報漏洩・ウィルス・不正アクセス等）の脅威について理解していない。	◆ 経営層は IT に関連・起因するリスク（情報漏洩・ウィルス・不正アクセス等）の脅威を認識している。	◆ 経営層は IT に関連・起因するリスク（情報漏洩・ウィルス・不正アクセス等）の脅威を認識している。 ◆ IT に関連・起因するリスクの潜在・顕在要因を網羅的に把握し、発生の可能性、発生した場合の影響などを予測し、対応策について検討を行っている。	◆ 経営層は IT に関連・起因するリスク（情報漏洩・ウィルス・不正アクセス等）の脅威を認識している。 ◆ IT に関連・起因するリスクの潜在・顕在要因を網羅的に把握し、発生の可能性、発生した場合の影響などを予測し、対応策について検討を行っている。
評価				
評価項目	◆従業員に対して IT に関連・起因するリスクについて説明を行っていない。	◆従業員に対して IT に関連・起因するリスクについての情報を提供している。 ◆従業員に対して適切な情報セキュリティ対策や情報管理についての教育・研修・訓練を実施している。	◆従業員（パートタイマー・アルバイト、派遣社員を含む）に対して IT に関連・起因するリスクについての情報を提供している。 ◆従業員（パートタイマー・アルバイト、派遣社員を含む）に対して適切な情報セキュリティ対策や情報管理についての教育・研修・訓練を実施している。	◆従業員（パートタイマー・アルバイト、派遣社員を含む）及び調達先や販売先など連携先企業に対して IT に関連・起因するリスクについての情報を提供している。 ◆従業員（パートタイマー・アルバイト、派遣社員を含む）に対してに対して適切な情報セキュリティ対策や情報管理についての教育・研修・訓練を実施している。
評価				
評価項目	◆システムの改ざん・不正アクセスを防ぐ仕組みは特にない。	◆アクセス権限やプログラムの登録管理の設定などにより、事前にシステムの改ざんや不正アクセスを防ぐ仕組みがある。	◆アクセス権限やプログラムの登録管理の設定などにより、事前にシステムの改ざんや不正アクセスを防ぐ仕組みがある。 ◆アクセスログをとってモニ	◆アクセス権限やプログラムの登録管理の設定などにより、事前にシステムの改ざんや不正アクセスを防ぐ仕組みがある。 ◆アクセスログをとってモニタリングするなど、システムの改ざ

			タリングするなど、システムの改ざんや不正アクセスの発生を発見できる仕組みがある。	んや不正アクセスの発生を発見できる仕組みがある。
評価				

基礎的事項	評価
◆ 情報セキュリティの推進体制を整備している	
◆ 情報セキュリティポリシーや情報セキュリティ管理規定を定めている	
◆ 機密情報・重要情報が外部に漏洩した際の対応マニュアルが整備されており、従業員は常時閲覧できる	
◆ システム停止などに伴う事業継続計画を策定し、災害をはじめとする物理的リスクに対応できる体制・システムとなっている	
◆ 内部統制が良好に整備され運用されている	
◆ CISO（情報セキュリティ統括専任担当）を設置している	
◆保管データの改ざん防止策として、電子署名とタイムスタンプ（時刻認証）を活用している	

Ⅷ.「IT 経営力指標」ステージの考え方

	ステージ 1	ステージ 2	ステージ 3	ステージ 4
評価項目	○システムによる在庫管理は行っていない。過剰在庫となるリスクはあるものの、材料や製品を多めに在庫しておき、いつでも対応できるようにしている。	○製造工程毎に在庫情報をリアルタイムに把握して、在庫圧縮によるコスト削減を実現している。	○製品に関して部品の調達から営業･販売に直接関わる一連の業務プロセスにおいて在庫情報等を共有し、これを基に業務改革を通じてコスト削減･売上高増大を図っている☆あらゆるサービスにおいて顧客情報を共有することで、重複業務の排除によるコスト削減、利便性の高いサービス提供による売上高増大を図っている。	○調達先・販売先など複数企業とともに、サプライチェーン全体で在庫情報等の製品の生産・販売に係る情報を共有し、企業横断的に在庫圧縮によるコスト削減を図っている。☆提携先など複数企業とともに、企業横断的に顧客に対するサービス提供状況等の情報を共有し、重複業務の排除等によるコスト削減を図っている。
評価				
評価項目	☆情報は各個人が属人的に保有しており、ナレッジの共有が図られていない。	☆サービス毎・顧客毎の情報管理により、サービス提供を円滑化している。	○製品の調達から営業･販売に関わる責任者（経営層も含む）が、担当部門以外の部門の情報（在庫情報、販売状況、購買先・販売先等）を必要なときに迅速に共有でき、担当部門以外での現状をみながら担当部門の業務改善を図っている☆あらゆるサービスの責任者は、担当部門以外の部門の情報（どの顧客が、いつどんなサービスを受けているか等）を必要なときに迅速に共有でき、担当部門以外での現状をみながら担当部門の業務改善を図っている。	○調達先・販売先などのサプライチェーンと自社のサプライチェーンの両者の最適化に向けて、定期的に関係企業と共同で検討する機会を設け、業務改善を図っている☆提携先などのサービス提供に係る複数企業の最適化に向けて、定期的に関係企業と共同で検討する機会を設け、業務改善を図っている。
評価				
評価項目	◆各製品・サービスの責任者に適時的確な情報が上がってこない。このため何らかの問題が発生した後でなければ何を改善すべきか把握できない。	◆各製品・サービスの責任者は、必要なときに迅速に担当部門の情報を得ることで、担当部門の業務改善を図っている。	○製品の販売動向を必要なときに全社で共有し、商品企画・開発等の担当者が新製品の開発にあたって迅速に対応している☆サービスの利用動向を、必要なときに全社で共有し、商品企画・開発等の担当者が新サービスの企画にあたって迅速に対応している。	○CEO あるいは CIO は、販売先・調達先の CEO、CIO と定期的に自社・販売先・調達先全体のサプライチェーンの最適化に向けた情報交換を行っている☆CEO あるいは CIO は、販売先・調達先の CEO、CIO と定期的にサービス提供に係る複数企業の最適化に向けた情報交換を行っている。
評価				

	ステージ 1	ステージ 2	ステージ 3	ステージ 4
評価項目	◆購買先・販売先に関する必要な情報を、経営者が把握することができない。	◆購買先・販売先に関する必要な情報は、各部門ごとに取りまとめられた上で、定期的に経営者に伝達され、経営判断の材料として活用されている。	◆IT を活用したシステムにより、購買先・販売先に関する必要な情報を、必要なときに（迅速に）経営者が共有し、経営判断の材料として活用している。	◆顧客などから得られる自社にとってのネガティブ情報が、顧客と接する社員・従業員によって共有され、解決に至るまで状況がフォローされるとともに、業務や製品・サービスの改善に繋がっている。 ◆自社が調達した製品や部品・サービスに対するネガティブ情報・課題点は、調達先に迅速に伝え、自社と調達先が共同で改善・高度化している。
評価				
評価項目	◆職務分掌や職務権限が不明確で業務が属人的になっているため、担当者が不在だと業務が滞ってしまう。 ◆業務の不正や間違いを防止し、発見する仕組みが不十分であり、従業員による不正や大きなミスがたびたび発生する。	◆職務権限と職務分掌が定期的に見直されている。 ◆業務の不正や間違いを防止し、発見する仕組みを取り入れているが、部門によって取り組みに温度差があるなど、不正や大きなミスの撲滅には至っていない。	◆職務権限と職務分掌が定期的に見直されている。 ◆各業務領域におけるデータが適切に収集、処理され、財務報告に反映されている。 ◆業務の不正や間違いを防止し、発見する仕組みを全社的に取り入れ、経営層から従業員に至るまでに徹底されている。	◆職務権限と職務分掌が定期的に見直されている。 ◆各業務領域におけるデータが適切に収集、処理され、財務報告に反映されている。 ◆業務の不正や間違いを防止し、発見する仕組みを全社的に取り入れ、経営層から従業員に至るまでに徹底されている。 ◆連携先企業との間での取り決めに従って、適正な取引を行っている。
評価				

5.パッケージソフトウェア選定のためのチェックリスト

パッケージソフトウェアを導入するには、パッケージ製造企業、流通企業、導入支援企業などがかかわるが、それぞれのポリシーや信頼性について評価を行う必要がある。合わせて、パッケージソフトウェアを導入する側の企業の状況やスタンスについて調べ、導入可能か確認する必要がある。パッケージソフトウェア検討にあたって、解説を参考に、以下の評価軸で評価を行う。

◎：期待以上である　○：十分なレベルである　△：不十分なレベルである　×：記述レベルが明らかに不足もしくは記述がない　ＮＡ：該当しない、不明

パッケージソフトウェアベンダ

記述項目	解説	評価	備考
経営安定性	パッケージソフトウェアベンダの経営は安定しているか		
出荷履歴	当該製品の初期バージョンとバージョンアップの出荷時期の履歴		海外製品の場合は国内外を分けて提示
出荷累計	初版から累計と提供バージョンの双方の出荷累計		
導入企業	当該パッケージソフトウェアを導入している企業の実績を提示		バージョンの明示が必要
導入規模	利用人数や端末数などの導入の規模を提示		
海外製品の日本語化	設計時から Unicode 対応していたか、表示機能のみ改造か		
カスタマイズポリシー	カスタマイズの可否、アドオンへの対応		
サービス・保守支援能力	コールセンター・サービス・保守支援拠点があるか		
日本語サポート	サポートが日本語で行われているか		
パフォーマンス	対応可能台数など		
性能	トランザクションの処理スピードなど		
バージョンアップの影響	基盤ソフトのバージョンアップの影響を受けやすいか		
バージョンアップポリシー	下位互換、上位互換を図る方針か、料金方針はどうか、保守・サポート停止に関する方針		

販売店

記述項目	解説	評価
役割分担	パッケージソフトウェアベンダとの役割分担は明確か。	
経営安定性	経営は安定しているか	
サポート安定性	サポートに長期展望を持っているか	

システムインテグレータ

記述項目	解説	評価
経営安定性	経営は安定しているか	
該当パッケージソフトウェア使用経験	そのパッケージや関連製品に関する経験を持っているか	
該当パッケージソフトウェア使用経験者の確保	今回のプロジェクトに専門家を配置できるのか	
パッケージソフトウェアベンダのサポート	SIer はベンダとパートナー契約などをしているのか	
代替ソリューションへの対応力	当該パッケージソフトウェア以外にもサービスを提供できるのか	

他ユーザからのパッケージソフトウェアに対する評価

記述項目	解説	評価
満足度	使い勝手、投資効果について悪い評価はないか	
サポート評価	サポートについて悪い評価はないか	

発注者

記述項目	解説	評価
該当パッケージソフトウェアの使用経験	そのパッケージソフトウェアや関連製品に関する経験を持っているか	
該当パッケージソフトウェア使用経験者の確保	今回のプロジェクトに専門家を配置できるのか	
カスタマイズ交渉経験	投資対効果などを考えて交渉できる担当者がいるか	

今回の導入に関する評価

記述項目	解説	評価
業務適合性	パッケージソフトウェアの業務に、現状の業務を合わせることができるか	
	パッケージソフトウェアをそのまま使うのではなくパラメータの設定が必要か	
	パッケージソフトウェアに追加開発を実現するアドオン機能があるのか	
	パッケージソフトウェア本体の機能を改造するカスタマイズができるか	
既存システムとの整合	データ連携があるか	
	インターフェース連携があるか	
	現行システムとの不整合が発生する可能性は確認したか	
	データ連携があるか	
規模適合性	実績のある規模か	
	規模の柔軟性はあるか	
機器適合性	予定された機器構成で稼動するか	

6.SaaS/ASP 選定のためのチェックリスト

SaaS/ASP を導入するには、SaaS/ASP 提供企業、SaaS/ASP プラットフォーム提供企業などがかかわるが、それぞれのポリシーや信頼性について評価を行う必要がある。合わせて、SaaS/ASP を導入する側の企業の状況やスタンスについて調べ、導入可能か確認する必要がある。SaaS/ASP 検討にあたって、解説を参考に、以下の評価軸で評価を行う。

◎：期待以上である　○：十分なレベルである　△：不十分なレベルである　×：記述レベルが明らかに不足もしくは記述がない　ＮＡ：該当しない、不明

SaaS/ASP ベンダ

記述項目		解説	評価
利用の継続性	経営安定性	SaaS/ASP ベンダの経営は安定しているか。	
	サービス提供時間帯	サービスの提供時間は十分か。	
	定期メンテナンス	定期メンテナンス等による停止時間、停止時期、告知方法等は明確か、停止による業務への影響は軽微か。	
	災害・障害時対応	災害、障害時の対応方法（告知方法、説明方法等）は明確か、システム復旧体制は十分か、停止時間に対する課金方針は妥当か。	
	サービス廃止時の対応（倒産・廃止等）	サービスが廃止となった場合であっても代替ソフトの提供、ソースコードの開示等、継続の手段があるか。計画的廃止の場合、告知は何ヶ月前か、何年間使用可能か。データは保全されるか、データの対応はどうなるか。	
実績	サービス履歴	当該製品の初期バージョンとバージョンアップの出荷時期の履歴（海外サービスの場合は国内外を分けて提示）	
	ユーザ累計	初版から累計と提供バージョンの双方の出荷累計（海外サービスの場合は国内外を分けて提示）	
	導入企業	当該 SaaS/ASP を導入している企業の実績を提示（導入企業規模ではなく、導入の規模を提示）	
	導入規模	利用人数や端末数などの導入規模を提示	
ライセンス	業務スケール	ライセンスの増減などが自由にできるか。増減した場合の価格の扱いはどうなるか	
	価格改定	価格改定のポリシーは開示されているか	
	途中解約	解約した場合の料金の扱いはどうなるか データの対応はどうなるか	
	機能変更（バージョンアップ）	バージョンアップポリシーは明確か。（強制的に適用されるか、任意か。移行の猶予期間はどの程度か）。下位互換か、上位互換を図る方針か バージョンアップの際の価格はどうなるか。	
機能・パフォーマンス	機能	機能は十分か。クライアント側の推奨環境は提示されているか（推奨環境に合致するか）。実使用環境での試用は可能か（試用期間は十分か）	
	カスタマイズポリシー	カスタマイズの可否、アドオンへの対応	
	パフォーマンス	推奨環境下で使用した場合のパフォーマンスは十分か（応答速度、同時接続数、転送量等）。保証はあるか	
	稼働率	稼働時間が開示されるもしくは稼動目標を示しているか	
	基盤ソフトの影響	基盤ソフトのバージョンアップの影響を受けやすいか	
データの取扱い	データの機密性	ユーザのデータにアクセスできる場合、できる人間が限定されているか	
	データの権利	データの権利はユーザになっているか（サービスを終了した場合、データの取り出し等が可能か）	
	データの移行	（必要な場合）データ移行ツールは用意されているか	
	データのダウンロード	（必要な場合）データのダウンロードは可能か	

SaaS/ASP ベンダ（続き）

記述項目		解説	評価
セキュリティ	セキュリティ	セキュリティ内容は開示されており十分なレベルか （暗号強度、サーバの防犯設備、入退室管理、災害対応、ポート監視等）	
	アプリケーションのセキュリティ	アプリケーションのセキュリティは十分か。（使用 DB の種類およびそのバージョン、セキュリティパッチの適用ポリシー等）	
	アカウント設定	利用者ごとに ID が付与できるか	
	アクセス権設定	利用者ごとにアクセス権限を設定できるか	
	ログ管理	ログの保管期間、種類は十分か	
バックアップ	バックアップ	バックアップのポリシーと方法は十分か （世代、復旧方法、保持期間、解約後の対応等）	
	データ多重化	サービス中のデータは多重化して管理されているか	
	複数サイトによるバックアップ	災害対策などのため、複数拠点でデータを管理しているか	
	ローカルバックアップ	ユーザ企業側にローカルバックアップは可能か	
サポート	コスト	別途費用がかかるか	
	サポート時間	サポート時間はユーザの業務時間と合致しているか	
	サポート方法	サポートの方法は十分か（電話か、メールか等）	
	その他	応答時間（特にメールの場合、2 営業日以内に返答されるか等）は十分か。日本語サポートが受けられるか	

SaaS/ASP プラットフォームベンダ

記述項目		解説	評価
利用の継続性	（経営安定性）	SaaS/ASP ベンダの経営は安定しているか	
	サービス提供時間帯	サービスの提供時間は十分か	
	定期メンテナンス	定期メンテナンス等による停止時間、停止時期、告知方法等は明確か 停止による業務への影響は軽微か	
	災害・障害時対応	災害、障害時の対応方法（告知方法、説明方法等）は明確か システム復旧体制は十分か 停止時間に対する課金方針は妥当か	
実績	サービス履歴	当該製品の初期バージョンとバージョンアップの出荷時期の履歴（海外サービスの場合は国内外を分けて提示）	
	ユーザ累計	初版から累計と提供バージョンの双方の出荷累計（海外サービスの場合は国内外を分けて提示）	
	導入企業	当該 SaaS/ASP を導入している企業の実績を提示	
	導入規模	利用人数や端末数などの導入規模を提示（導入企業規模ではなく、導入の規模を提示）	
パフォーマンス	パフォーマンス	推奨環境下で使用した場合のパフォーマンスは十分か（応答速度、同時接続数、転送量等） 保証はあるか	
	稼働率	稼働時間が開示されるもしくは稼動目標を示しているか	
セキュリティバックアップ	セキュリティ	セキュリティ内容は開示されており十分なレベルか（暗号強度、サーバの防犯設備、入退室管理、災害対応、ポート監視等）	
	バックアップ	バックアップのポリシーと方法は十分か（世代、復旧方法、保持期間、解約後の対応等）	
	データ多重化	サービス中のデータは多重化して管理されているか	
	複数サイトによるバックアップ	災害対策などのため、複数拠点でデータを管理しているか	
	ローカルバックアップ	ユーザ企業側にローカルバックアップは可能か	
サポート	コスト	別途費用がかかるか	
	サポート時間	サポート時間はユーザの業務時間と合致しているか	
	サポート方法	サポートの方法は十分か（電話か、メールか等）	

記述項目		解説	評価
	その他	応答時間（特にメールの場合、2 営業日以内に返答されるか等）は十分か 日本語サポートが受けられるか	

他ユーザからの SaaS/ASP に対する評価

記述項目	解説	評価
満足度	使い勝手、投資効果について悪い評価はないか	
サポート評価	サポートについて悪い評価はないか	

発注者

記述項目	解説	評価
該当 SaaS/ASP の使用経験	その SaaS/ASP や関連製品に関する経験を持っているか	
該当 SaaS/ASP 使用経験者の確保	今回のプロジェクトに専門家を配置できるのか	

今回の導入に関する評価

記述項目	解説	評価
導入目的意識	導入に当たっての目的意識は明確になっているか	
業務適合性	SaaS/ASP の業務に、現状の業務を合わせることができるか	
	SaaS/ASP をそのまま使うのではなくパラメータの設定が必要か	
	SaaS/ASP に追加開発を実現するアドオン機能があるのか	
	SaaS/ASP 本体の機能を改造するカスタマイズの必要があるのか	
既存システムとの整合	データ連携があるか	
	インタフェース連携があるか	
	現行システムとの不整合が発生する可能性は確認したか	
	データ連携があるか	
規模適合性	実績のある規模か	
	規模の柔軟性はあるか	

7.検収事前チェックリスト

検収を確実に行うために、事前に検収準備状況について確認しておく必要がある。以下の項目の確認を行う。

チェック項目	結果
検収計画は、プロジェクト責任者の承認を得ていますか？	
システム関連資料は既に運用スタッフに渡されていますか？	
品質（バグ、ユーザビリティ、開発基準適合）に関するテストは終了していますか？	
セキュリティ項目に関するテストは終了していますか？	
検収にあたっての評価基準は決まっていますか？（ミッションを達成していればよい等）	
事業継続計画は考えられていますか？	
サポートスタッフは既に決まっていますか？	
サポートと業務の関係は整理されていますか？（業務時間とサポート時間の関係等）	
検収計画が要求仕様を元にしているか確認していますか？	
検収計画は、構成管理されていますか？	
運用書類や検収書類は、検収チームに配布されていますか？	
検収チームは、検収に関する知識や経験はありますか？	
ベンダ側総合テストは終わっていますか	

8.検収チェックリスト

ベンダが開発したシステムを受け入れるかどうかのチェックポイントである。以下の項目をチェックする必要がある。

チェック項目	結果
ユーザ教育は終わっていますか？	
既存システムがある場合、データ移行は終わっていますか？	
支所等、各導入場所の準備はできていますか？	
システム導入に関して、関係者全体の同意はできていますか？	
ハードウェアの納品と基本動作の確認はできていますか？	
初期データの導入は終わっていますか？	
必要なソフトウェアのインストールは全て終わっていますか？	
問題点や是正処置は書面で管理されていますか？	
テスト後に修正したソフトウェアなどは再テストされていますか？	
総合運転テストの結果はファイルされていますか？	
教育資料は承認され、構成管理されていますか？	
テスト環境は全体の試験をする上で十分なものでしたか？	
検収テストで行う項目は、関係者の間で調整されていましたか？	
検収計画に従って試験は行われましたか？	
全てのテストは正確に実行されましたか？	
問題のあった部分は記録され、修正の上、再テストしましたか？	
検収報告書はできていますか？	
検収テストの結果はファイリングされていますか？	
運用準備のレビューが行われましたか？	
もしもシステムの拡張や変更が必要であったならば、運用に対する必要な対策は打たれていますか？	
検収後に全てのドキュメントがアップデートされていますか？	
完成した運用関連ドキュメントが各部門に配布されていますか？	
正式な検収完了ドキュメントを書面で作成していますか？	
負荷試験は終わっていますか？	
教育や資格や認定が必要な場合の処置はできていますか？	
保守計画はできていますか？	
移行期間と役割が明確にされていますか？	
アクセスルールは適用されていますか？	
将来の拡張計画が、サポート要員に伝えられていますか？	
最終プログラムがライブラリ化し、テストプログラムなどが消されていますか？	
プロジェクト関連資料が、メンテナンス可能な形で運用要員に渡されていますか？	
運用コストや性能予測など各種データはプロジェクト計画に反映されていますか？	
今後に向けてプロジェクト計画がウォークスルーされていますか？	

9.セキュリティチェックシート　一般版（上位概念）

■技術的セキュリティ対策

技術的 セキュリティ対策	脅威の内容	参考情報（上位レベルは下位レベルの内容を含む）				役割		本件業務での対応	
		レベル 1	レベル 2	レベル 3	レベル 4	ユーザ	ベンダ	対応レベル	仕様又は 候補製品等
■認証 情報を参照している人が本人なのかを証明をする。	情報を参照している人が、本人なのかを管理していないと、他人に重要な情報を見られる可能性がある。	■何も決められていない 情報を誰が参照しているか特定できない状態。	■個人を認識できるパスワードを利用して、個人を認識できるようにする。	■本人認証の強化 特定のカードやログインの二重化などで、本人認証を強化する。	■絶対的な本人認証 生体認証等を組み合わせ、定期的なポリシー変更を実施する。				
■アクセス権 個人情報、企業情報によって、アクセスできる人を制限･管理する。	誰でも情報アクセスできるようになっていると、削除、改ざん、複製、持ち出しされたりする。	■何も決められていない 情報に誰でもアクセスできてしまう。	■コンピュータ単位で設定できる サーバ単位、フォルダ単位で、個人･グループが情報単位にアクセスできように設定する。	■認証情報に基づき資源単位でアクセス権が設定できる ファイル単位で、個人･グループが情報単位にアクセスできるように設定する。	■資源単位でアクセスした内容の収集、分析ができる アクセスされた情報（ログ）を収集･分析できる。				
■暗号化 情報を暗号化して、紛失･盗難･盗聴の対策を施す。	情報機器（コンピュータや USB メモリなど）が盗難又は紛失することにより、情報が漏えいするおそれがある。	■何も対策されていない 社外に持ち出すデータ、社内のコンピュータのデータに暗号化が実施されていない。	■モバイルコンピュータや USB メモリ単位で暗号化で持ち出す 社外に持ち出すコンピュータ、USB メモリなどの中に入っているデータを暗号して持ちだす。	■全てのコンピュータについて、データを暗号化する 社内のコンピュータ、社外に持ち出すコンピュータ、業務で使用する USB メモリ、外付け HDD、CD/DVD など情報を書き込めるものに対して暗号化をする。	■暗号化されたものを復号する都度、認証をおこなう 暗号化されたデータを復号するたびに、認証を行い履歴を取得する。				
■ウイルス等の悪意あるプログラムの取り扱い及び検出する機能の導入 悪意あるプログラムから情報資産を守る。	コンピュータに誤動作を起こさせる悪意のあるプログラムにより、システムが利用できなくなる、データが消去される、情報が外部に漏えいしてしまう、などのおそれがある。	■何も決められていない ウイルス対策を実施していない。	■ウイルス等を検出し侵入を停止･警告できるコンピュータ上で悪意のあるプログラムを検出して削除し、警告できる。	■全システムに対するウイルス対策と集中管理 ネットワーク機器やコンピュータなど複数の対象に対して、悪意のあるプログラムを検出、削除するための機能を導入し、被害状況の収集や定義ファイルの更新を集中的に管理できる。	■不審な通信やコンピュータをシステムから隔離できる 悪意のあるプログラムが検出されたコンピュータをネットワークから遮断する。				

技術的 セキュリティ対策	脅威の内容	参考情報（上位レベルは下位レベルの内容を含む）				役割		本件業務での対応	
		レベル 1	レベル 2	レベル 3	レベル 4	ユーザ	ベンダ	対応レベル	仕様又は 候補製品等
■ネットワークの運用 ネットワークを流れるデータ量の管理をする。	ネットワーク障害や大量のデータ転送により、ネットワークが正常に利用できなくなるおそれがある。	■何も決められていない ネットワーク管理ツールもしくはサービスを導入していない。	■管理ツールを導入する 障害検知やネットワーク負荷を検知するツール、サービスを導入する。	■冗長化する、使用状況を監視して記録できるようになる ネットワーク機器を冗長化して大量データに備えたり、ネットワーク障害時にネットワークが利用できなくなるのを回避したりする。	■トラフィックに応じた柔軟な制御ができる ネットワークの使用状況に応じて、機器の設定を容易に変更できる。				
■保守 OSやアプリケーション、ハードの保守を行なう。	ハードウェア保守がされていないと、不具合の発生や、故障が発生するおそれがある。	■何も決められていない メンテナンス作業をやっていない。	■障害発生時に対応する 障害が発生した時点で、保守作業を実施する。	■定期保守を実施する 定期的に機器の点検、整備を行い、耐用期間を過ぎた部品は交換する。	■予防的に対応する 定期的に機器の点検、整備を行い、耐用期間を過ぎる前に部品を交換する。				
	OS、ミドルウェアの保守がされていないと、不具合の発生や、セキュリティホールによって情報が漏洩するおそれがある。	■何も決められていない メンテナンス作業をやっていない。	■障害発生時に対応する 障害が発生した時点で、不具合修正版の適用を実施する。	■定期保守を実施する 定期的に不具合修正版を取得し、予備機でテストをおこない、適用する。	■予防的に対応する 計画的に不具合修正版を取得し、不具合の発生を検討の上、予備機でテストを行い適用する。				
	アプリケーション保守がされていないと、不具合や期待する正しい結果が得られないおそれがある。	■何も決められていない メンテナンス作業をやっていない。	■障害発生時に対応する 障害が発生した時点で、修正版の適用を実施する。	■定期保守を実施する 定期的に修正版を取得し、予備機でテストをおこない、適用する。	■予防的に対応する 計画的に修正版を取得し、不具合や運用変更などの発生を検討の上、予備機でテストを行い適用する。				
■機器運用監視 サーバ、ネットワーク機器の稼働監視を行う。	システムの状況を把握できないことにより、障害の対応が遅れて情報システムへのアクセスが長時間停止するおそれがある。	■何も決められていない サーバ、ネットワーク機器の稼働状況を監視していない。	■運用状況を遠隔で、手動で把握できる 遠隔で稼働状況を手動で確認する。	■運用状況を自動で把握、記録ができる 稼働状況を常時把握し、異常があれば通知する。	■運用状況に異常があれば、自動的に設定された状態に切替わる 異常を通知するとともに、代替手段に自動的に切替わる。				
■障害発生時の対応 障害時の対応マニュアルの整備をする。	システム障害時の対応手順が決められていないと、適切に対応できず、復旧が遅延するお	■何も決められていない システム障害時の対応を決めていない。	■障害発生時は代替機を手配する 代替機を手配し、到着後交換する。データは	■障害発生時は予備システムに手動で切り替える 障害が発生した場合	■障害発生時は予備システムに自動的に切り替わる 障害を通知するとともに、				

技術的 セキュリティ対策	脅威の内容	参考情報（上位レベルは下位レベルの内容を含む）				役割		本件業務での対応	
		レベル 1	レベル 2	レベル 3	レベル 4	ユーザ	ベンダ	対応レベル	仕様又は 候補製品等
	それがある。		バックアップを利用する。	は、予備機に手動で切替える。データはバックアップを利用する。	自動的に切替る。データは自動的に保持される。				
■データの保護 データが改ざんされないように防御する。	データが保護されていないと、データが改ざんされたり、漏えいしたりするなどの恐れがある。	■何も決められていない データの改ざんや、漏えいの対策を施さない。	■特定のデータ、情報が保護されている データ･情報をパスワードや暗号で保護する。	■すべてのデータ、情報が保護されている すべてのデータを暗号化やアクセス権で保護する。	■第三者が利用できないようになっている データに対して、アクセス権と暗号の両方で保護している。				
■ログ管理 情報の持ち出し履歴をとって監査の証跡資料として管理する。	情報システムの適切な監査ログが管理されていないと不正な出来事に気づく事ができない恐れがある。	■何も決められていない ログを取得していない。	■ログの取得のみ ログを保存する。	■ログを取得し、定期的なレポートを行う ログを保存し、内容を分析し報告する。	■取得ログのレポートに加え、常時監視を行う 自動的にログを分析し、異常があれば通知する。				

■物理的セキュリティ対策

物理的 セキュリティ対策	脅威の内容	参考情報（上位レベルは下位レベルの内容を含む）				役割		本件業務での対応	
		レベル 1	レベル 2	レベル 3	レベル 4	ユーザ	ベンダ	対応レベル	仕様又は 候補製品等
■作業領域（場所） マシンルームやコンピュータを置いておく環境を管理する。	部外者が、簡単に会社や部屋に入れてしまうと、情報を盗まれる恐れがある。	■何も決められていない 施錠管理、入退室管理されていない。	■隔離する マシンルームは施錠する。第三者のオフィスへの入退出を制限する。	■立ち入りを制限する 常時、暗証番号、IC カード、生体認証等により、部屋の入退室を制限する。	■立ち入りを監視して記録する 防犯カメラを設置し、部屋の入退室を記録する。				
■データの保管 データのバックアップを行なう。	システムの緊急停止や不慮の災害の発生時に、システムを業務可能な状態に復旧できなくなる。	■何も決められていない データをバックアップしていない。	■複製を保管するための機能を持つ 日次で複製する。障害発生時には、前日までのデータが復旧できる。	■複製を世代管理する 一定期間、遡って復旧できるように複製する。	■離れた拠点で複製が保管されている 世代管理された複製が遠隔地で保管され、被災してもデータを復旧できる。				
■作業環境管理（空調等） 適切な温度、湿度を保つ。	高温、多湿になると、コンピュータが正確に作動しなくなるおそれがある。	■何も決められていない 空調設備がない、又は、管理していない。	■手動で適切な環境を維持する 人が判断して、空調を調節する。	■自動で適切な環境を維持する 自動的に適切な温度、湿度に調節される。	■停電でも適切な環境が維持される 非常用発電装置で作業環境が適切に維持される。				
■停電時の機器運用 停電時の稼動性を確保する。	停電などにより、コンピュータが稼動せずに業務が中断される、データ	■何も決められていない 停電時には利用できな	■停電発生時に安全に停止できる 無停電電源装置によ	■障害発生時にも一定時間稼動できる設備がある	■システムを常に稼動し続けられる設備が整っている				

物理的 セキュリティ対策	脅威の内容	参考情報（上位レベルは下位レベルの内容を含む）				役割		本件業務での対応	
		レベル 1	レベル 2	レベル 3	レベル 4	ユーザ	ベンダ	対応レベル	仕様又は 候補製品等
	を喪失するおそれがある。	い。データが失われることがある。	り、停電を検知し、自動的に機器を停止する。	無停電電源装置により、一定時間稼働し、データを保護の上、機器を停止する。	非常用発電装置により、停電中もシステムを安定稼働する。				
■資産の管理 資産台帳を作成し、資産を管理する。	資産（情報機器・電子媒体・紙）の資産管理がされていないと紛失・盗難の検知ができない。	■何も決められていない 資産管理されていない。	■紙面上で管理している 人が資産を確認し、管理台帳を作成して管理する。	■ツール等によりコンピュータ上で管理している 資産管理ソフトを使い、機器情報を取得し資産台帳を作成、管理する。	■定期的に見直しがかけられている 資産管理ソフトを使い、定期的に実査監査をおこなう。				

■管理的セキュリティ対策

管理的 セキュリティ対策	脅威の内容	参考情報（上位レベルは下位レベルの内容を含む）				役割		本件業務での対応	
		レベル 1	レベル 2	レベル 3	レベル 4	ユーザ	ベンダ	対応レベル	仕様又は 候補製品等
■資産分類 資産を重要度に応じて分類し、取扱いを定め管理する。	情報資産が取扱い基準（極秘・社外秘など）によって分類されていないと、権限のない者から情報が漏えいする可能性がある。	■何も決められていない 分類基準がない。	■分類基準がある 情報資産の分類基準によって分類し、取扱いが定められている。	■分類基準ごとに管理されている 情報資産の所在が管理されている。	■分類基準ごとにアクセスできる人が決まっていて、履歴がとられている 情報を参照した際は、記録が残る。				
■システム受入れ管理 コンピュータシステムの受入れ基準を定め管理する。	受け入れたシステムの不備に気づかず稼動したり、ネットワークに接続すると、不具合が発生する可能性がある。	■何も決められていない 受入れ方法がない。	■ベンダのテスト基準に従う ベンダが作成したデータとテスト方法でテストする。	■自社のデータを使用しテストを行う 自社の実際に使用するデータと、ベンダが作成したテスト方法でテストする。	■自社で受入れ検査基準を定め、システムを網羅するテストを行う 自社でテストデータ、テスト方法を定め、テストする。				
■運用体制 社員または社員以外の組織に運用させる場合の管理方法を定める。	情報システムの運営を部外者に行わせる場合、管理基準がないと、情報が漏えいする。	■何も決められていない 管理基準がない。	■運用契約、SLA を締結する、運用操作や機器、情報の操作履歴を記録する操作や情報持ち出しを記録する。	■運用契約、SLA を締結する、SLM を実施する、操作ログを取得する誤操作や情報持ち出しを監視する。	■運用契約、SLA を締結する、操作ログを取得して、定期的に外部組織で監査する 規定違反者へは、警告が自動的に送られる。				

		参考情報（上位レベルは下位レベルの内容を含む）				役割		本件業務での対応	
■情報漏えい時の対策体制 情報漏えいが発生した場合の手順、組織を定める。	漏えい事故などが発生した場合の管理体制が決まっていないと、対応がおくれ被害が大きくなるおそれがある。	■何も決められていない 情報漏えい時の対策がない。	■体制は決められている 責任者、外部対応窓口など対策実施組織を定める。	■漏えい事故のレベルによって対策体制が決められてる 漏えいした情報の内容に応じて、対策実施組織を定め、想定訓練を行なう。	■漏えい事故のレベルを判断し、全社に指揮命令をする組織体制がある 漏えいした情報の内容に応じて、対策実施組織を定め、想定訓練を行なう。				

10. セキュリティチェックシート Web アプリケーション版

■技術的セキュリティ対策

技術的 セキュリティ対策	脅威の内容	参考情報（上位レベルは下位レベルの内容を含む）				役割		本件業務での対応	
		レベル 1	レベル 2	レベル 3	レベル 4	ユーザ	ベンダ	対応レベル	仕様又は 候補製品等
■認証 情報を参照している人が本人なのかを証明をする。	情報を参照している人が、本人なのかを管理していないと、他人に重要な情報を見られる可能性がある。	■何も決められていない 情報を誰が参照しているか特定できない状態。	■個人を認識できるパスワードを利用して、個人を認識できるようにする。	■本人認証の強化 特定のカードやログインの二重化などで、本人認証を強化する。	■絶対的な本人認証 生体認証等を組み合わせ、定期的なポリシー変更を実施する。				
■アクセス権 情報よって、アクセスできる人を制限･管理する。	誰でも情報アクセスできるようになっていると、削除、改ざん、複製、持ち出しされたりする。	■何も決められていない 情報に誰でもアクセスできてしまう。	■利用者と管理者のアクセス権限の設定 利用者がアクセスできる情報と、管理者だけがアクセスできる情報を区別し、管理する。ログを取得する。	■グループ単位のアクセス権限の設定 利用者が所属するグループごとにアクセスできる情報を区別し、管理する。ログを取得する。	■アクセス権の集中管理機能を有する 利用者･グループ毎のアクセス権限を管理する機能を使って、最新のアクセス権を維持することができる。ログを収集し、問題発生時に参照できる				
■暗号化 情報を暗号化して、紛失･盗聴･改ざんの対策をする。	通信経路やパスワードが暗号化されていない場合は、紛失･盗聴･改ざんや成りすましの可能性がある。	■何も決められていない 通信経路やシステムで保存するパスワードが暗号化されていない。	■パスワードの暗号化を実装する パスワードを暗号化し、容易に第三者にパスワードが漏えいしないようにする。	■個人、決済等に関わる情報の暗号化を実装する 個人情報、決済情報をすべて暗号化し、漏えい、改ざん、紛失しても悪用されないようにする。	■全ての情報について高度な暗号化を実装する あらゆる情報を暗号化し、第三者に悪用されないようにする。				

技術的 セキュリティ対策	脅威の内容	参考情報（上位レベルは下位レベルの内容を含む）				役割		本件業務での対応	
		レベル 1	レベル 2	レベル 3	レベル 4	ユーザ	ベンダ	対応レベル	仕様又は 候補製品等
■ページ間のデータ授受 Web のページをまたがってデータのやり取りをする際の対策をする。	ページ間のデータ授受が正しくなされない場合は、情報が漏えいしたり、成りすましされたりする可能性がある。	■何も決められていない ページ間のデータ授受について、何もルール化されていない。	■データの取り扱いがルール化されている データの有効期限や取り扱い方法が部分的にルール化されている。	■データの取り扱いルールの強化 データの有効期限や取り扱い方法が規定されている。	■ページ間でやり取りするデータの種類を規制する 個人を特定できる情報、決済に関わる情報をページ間でやり取りをしないなどを規定する。				
■悪意のあるコードの侵入阻止 悪意のあるコードが Web サーバに埋め込まれるのを阻止する。	悪意のあるコードが Web サーバ上で実行されると、フィッシング詐欺やユーザの成りすまし、パスワード漏えい等の可能性がある。	■何も決められていない 悪意のあるコードに対して、なにも対策がない。	■悪意のあるコードの対策 悪意のあるコードを排除する仕組みがある。必要最少限のアクセス権限設定をする。不要なファイルを公開しない。	■悪意のあるコードの対策の強化 悪意のあるコードを排除する仕組みがあり、対策方法、管理権限がシステム全体で規定されている。	■Web アプリケーション以外の対策の併用 Web アプリケーション内の悪意のあるコード対策に併せて、WAF（Web Application Firewall）等を使用した対策を実施する。				
■システム連携 他のシステムや他のアプリケーションとの連携を行う際に連携の仕組みを悪用されるのを阻止する。	連携の仕組みを悪用されると、フィッシング詐欺やユーザの成りすまし、パスワード漏えい等の可能性がある。	■何も決められていない 連携の仕組みを悪用されるのを阻止する対策がない。	■システム連携悪用の対策 システム連携悪用を排除する仕組みがある。	■システム連携悪用の対策の強化 システム連携悪用を排除する仕組みがあり、対策方法がシステム全体で規定されている。	■Web アプリケーション以外の対策の併用 Web アプリケーション内のシステム連携悪用の対策に併せて、WAF 等を使用した対策を実施する。				
■Web サーバの設定 Web サーバの設定内容について、最適な設定がされているか。	Web サーバの設定が正しく設定されていない場合、攻撃のために必要とするシステム情報が漏えいする。	■何も決められていない セキュリティ基準が決められていない。	■セキュアな設定 Web サーバの設定が外部からの攻撃などを防ぐセキュリティを意識した設定になっている。	■セキュアな設定の強化 Web サーバの設定がセキュリティを意識した設定になっており、設定内容が規定されている。	■侵入検知 Web サーバの設定に対する侵入・攻撃の際に、検知し、管理者へ通知する				
■内因的な情報漏えい 運用ミスなど内部側の原因で情報が漏えいする。	重要な情報が漏えいしたり、攻撃のために必要とする情報が漏えいする。	■何も決められていない Web サーバの運用について規定が何も設けられていない。	■Web サーバの運用規約 Web サーバの運用について一部の規定だけが設定する。（アクセス、メンテナンス等）	■Web サーバの運用規約を強化 網羅的に Web サーバの運用（アクセス、メンテナンス、ログイン等）について規定が設定されている。	■情報表示の制限 個人情報等の重要情報は、一覧表示を禁止する、一括して CSV ファイル出力を禁止する、などを規定する。				

技術的 セキュリティ対策	脅威の内容	参考情報（上位レベルは下位レベルの内容を含む）				役割		本件業務での対応	
		レベル 1	レベル 2	レベル 3	レベル 4	ユーザ	ベンダ	対応レベル	仕様又は 候補製品等
■アプリケーションへの攻撃対策 機能の悪用、負荷攻撃、多重登録等のアプリケーションに対する攻撃対策。	アプリケーションに対する攻撃により、サービスの停止や情報漏えい、改ざん、踏み台化などの可能性がある。	■何も決められていない 攻撃の対策は特に用意されていない。	■暫定的な攻撃の対策 アプリケーションへの攻撃に対する暫定的な対策が施されている。	■根本的な攻撃の対策 アプリケーションへの攻撃に対する根本的な対策が施されている。	■重複した攻撃の対策 根本的対策に加え、異なる方法を使用して、複数の攻撃対策を施す。				
■ネットワーク構成 ネットワークの構成により、攻撃されやすさが変わる。	不適切な構成の場合、サーバの乗っ取りの可能性がある。	■何も決められていない サーバに乗っ取り対策がなされていない。	■簡易なネットワーク構成 サーバが乗っ取られない為の最低限の対策が講じられている。	■基本的なネットワーク構成 サーバが乗っ取られない為の対策が講じられている。	■セキュアなネットワーク構成 サーバが乗っ取られない為のセキュアな対策が講じられている。				
■電子商取引 電子商取引におけるセキュリティ対策の実施。	取引に関係する情報が漏えい、改ざんされる可能性がある。	■何も決められていない 電子商取引におけるセキュリティ対策はなにもしない。	■取引データに対する最低限の保全性 取引関連情報に誤りが無いことを保証する為の、最低限の保全機能を実装する。	■取引データの保全性 取引関連情報に誤りが無いことを保証する為の、保全機能を実装する。	■取引データの保全性の強化 複数の手段を講じて保全性の強化を図る。				
■ログ管理 情報の持ち出し履歴を取得し監査の証跡資料として管理する。	情報システムの監査ログが適切に管理されていないと不正な出来事に気づく事ができない恐れがある。	■何も決められていない ログを取得していない。	■ログの取得のみ ログを保存する。	■ログを取得し、定期的なレポートを行う ログを保存し、内容を分析し報告する。	■取得ログのレポートに加え、常時監視を行う 自動的にログを分析し、異常があれば通知する。				
■Web アプリケーション開発 導入したパッケージをカスタマイズする業者を選定する基準。	セキュリティに対する対策を考慮しない業者に開発を委託すると、多くのセキュリティホールを作り込まれてしまう可能性がある。	■何も決められていない セキュリティ対策基準なしに開発を行う。	■セキュリティテストの実施 セキュリティに関するテストを実施する。	■開発ルールの規定 開発標準、セッション管理など決められた規定に従って開発を行う。	■セキュリティ対策機能の使用と専門部門の品質管理 実績あるセキュリティ対策機能を使用し開発する。 専任者が品質管理を行う。				

11.SaaS 向け SLA におけるサービスレベル項目のモデルケース　http://www.meti.go.jp/press/20080121004/20080121004.html 参照。
※ 本モデルケースでは、基幹系業務の場合と販売管理やグループウェアなどそれ以外の業務の場合に分けて、サービスレベル設定例を示している。
※ 実際の設定値は、以下の設定例を参考として、業務内容など個々の状況に応じて決定されるべきものである点に留意されたい。

◆アプリケーション運用

種別	サービスレベル項目例	規定内容	測定単位	設定例	備考
可用性	サービス時間	サービスを提供する時間帯（設備やネットワーク等の点検／保守のための計画停止時間の記述を含む）	時間帯	24 時間 365 日 （計画停止／定期保守を除く）	計画停止時間は提供者が個々に設定。
	計画停止予定通知	定期的な保守停止に関する事前連絡確認（事前通知のタイミング／方法の記述を含む）	有無	30 日前にメール／ホームページで通知	
	サービス稼働率	サービスを利用できる確率（(計画サービス時間－停止時間）÷計画サービス時間）	稼働率 （%）	99.9%以上（基幹業務） 99%以上（上記以外）	対象業務の重大性を考慮しつつサービス内容／特性／品質に応じて個々に検討。
	ディザスタリカバリ	災害発生時のシステム復旧／サポート体制	有無	遠隔地のバックアップ用データセンタで保管している日次バックアップデータと予備システムへの切り替え	データセンタ構成、復旧までのプロセス／時間、費用負担についても明示されていることが望ましい。また、適用する業務の重要性に応じた「ディザスタリカバリ」のレベルにより設定内容は変わる。
	重大障害時の代替手段	早期復旧が不可能な場合の代替措置	有無	バックアップデータの取得が可能なホームページを用意	
	代替措置で提供するデータ形式	代替措置で提供されるデータ形式の定義を記述	有無（ファイル形式）	CSV あるいは Excel ファイルで提供	
	アップグレード方針	バージョンアップ／変更管理／パッチ管理の方針	有無	年 2 回の定期バージョンアップを実施	頻度、事前通知方法、履歴管理／公開、利用者の負担についても明示されていることが望ましい。
信頼性	平均復旧時間	障害発生から修理完了までの平均時間（修理時間の和÷故障回数）	時間	1 時間以内（基幹業務） 12 時間以内（上記以外）	対象業務の重大性を考慮しつつサービス内容／特性／品質に応じて個々に検討。
	システム監視基準	システム監視基準（監視内容／監視・通知基準）の設定に基づく監視	有無	1 日 4 回のハードウェア／ネットワーク／パフォーマンス監視	詳細な監視項目は提供者が個々に設定。
	障害通知プロセス	障害発生時の連絡プロセス（通知先／方法／経路）	有無	指定された緊急連絡先にメール／電話で連絡し、併せてホームページで通知	初期対応後の経過報告の方法・タイミングについても明示されていることが望ましい。
	障害通知時間	異常検出後に指定された連絡先に通知するまでの時間	時間	15 分以内（基幹業務） 2 時間以内（上記以外）	営業時間内／外で異なる設定を行う場合がある。
	障害監視間隔	障害インシデントを収集／集計する時間間隔	時間 （分）	1 分以内（基幹業務） 15 分（上記以外）	営業時間内／外で異なる設定を行う場合がある。
	サービス提供状況の報告方法／間隔	サービス提供状況を報告する方法／時間間隔	時間	月に一度ホームページ上で公開	報告内容／タイミング／方法は提供者が個々に設定。

種別	サービスレベル項目例	規定内容	測定単位	設定例	備考
	ログの取得	利用者に提供可能なログの種類（アクセスログ、操作ログ、エラーログ等）	有無	セキュリティ（不正アクセス）ログ／バックアップ取得結果ログを利用者の要望に応じて提供	提供内容／方法は提供者が個々に設定。
性能	オンライン応答時間	オンライン処理の応答時間	時間（秒）	データセンタ内の平均応答時間 3 秒以内	対象業務の重大性を考慮しつつサービス内容／特性／品質に応じて個々に検討。
	バッチ処理時間	バッチ処理（一括処理）の応答時間	時間（分）	4 時間以下	対象業務の重大性を考慮しつつサービス内容／特性／品質に応じて個々に検討。
拡張性	カスタマイズ性	カスタマイズ（変更）が可能な事項／範囲／仕様等の条件とカスタマイズに必要な情報	有無	利用画面上の項目配置変更や新規項目の追加が設定画面より可能	サービス仕様（機能仕様）として契約書／利用マニュアルに記載されている場合は必ずしも SLA で定義される必要はない。
	外部接続性	既存システムや他の SaaS 等の外部のシステムとの接続仕様（API、開発言語等）	有無	API（プログラム機能を外部から利用するための手続）を公開	API がインターネットの標準技術で構成され、仕様が公開されており、API の利用期限や将来の変更可能性が明記されていることが望ましい。
	同時接続利用者数	オンラインの利用者が同時に接続してサービスを利用可能なユーザ数	有無（制約条件）	50 ユーザ（保証型）	同時接続の条件（保証型かベストエフォート（最善努力）型か）、最大接続時の性能について明示されていることが望ましい。

◆サポート

サービスレベル項目例	規定内容	測定単位	設定例	備考
サービス提供時間帯（障害対応）	障害対応時の問合せ受付業務を実施する時間帯	時間帯	24 時間 365 日（電話）	受付方法（電話／メール）や営業時間外の対応は対象業務の重大性およびサービス内容／特性／品質に応じて状況が異なる。
サービス提供時間帯（一般問合せ）	一般問合せ時の問合せ受付業務を実施する時間帯	時間帯	営業時間内（電話）（年末年始・土日・祝祭日を除く） 24 時間 365 日（メール）	受付方法（電話／メール）や営業時間外の対応は対象業務の重大性およびサービス内容／特性／品質に応じて状況が異なる。

◆データ管理

サービスレベル項目例	規定内容	測定単位	設定例	備考
バックアップの方法	バックアップ内容（回数、復旧方法など）、データ保管場所／形式、利用者のデータへのアクセス権など、利用者に所有権のあるデータの取扱方法	有無／内容	有 （日次でフルバックアップ。遠隔地のデータセンタにテープ形式保管。アクセス権はシステム管理者のみに制限。復旧／利用者への公開の方法は別途規定）	保証要件を設定している場合は、具体的に明示。バックアップ内容は対象業務の重大性およびサービス内容／特性／品質に応じて状況が異なる。 また、SaaS ベンダの民事再生、破産等によりサービス継続が出来ない場合についても明示されていることが望ましい。

サービスレベル項目例	規定内容	測定単位	設定例	備考
バックアップデータの保存期間	データをバックアップした媒体を保管する期限	時間	5 年以上（基幹業務） 3 ヶ月以上（上記以外）	対象業務の重大性を考慮しつつサービス内容／特性／品質に応じて個々に検討。
データ消去の要件	サービス解約後の、データ消去の実施有無／タイミング、保管媒体の破棄の実施有無／タイミング、およびデータ移行など、利用者に所有権のあるデータの消去方法	有無	サービス解約後 1 ヶ月以内にデータおよび保管媒体を破棄。	解約時には、CSV などの一般的なフォーマットでデータ出力ができることが望ましい。

◆セキュリティ

サービスレベル項目例	規定内容	測定単位	設定例	備考
公的認証取得の要件	JIPDEC や JQA 等で認定している情報処理管理に関する公的認証（ISMS、プライバシーマーク等）が取得されていること。	有無	ISMS 認証取得 プライバシーマーク取得	IT サービスマネジメントのベストプラクティスである ITIL や JIS Q20000 等の取得状況も確認することが望ましい。
アプリケーションに関する第三者評価	不正な侵入、操作、データ取得等への対策について、第三者の客観的な評価を得ていること。	有無／実施状況	有（年 1 回、外部機関によりサービスの脆弱性に関する評価を受け、速やかに指摘事項に対して対策を講じる。）	セキュリティ監査、システム監査、ペネトレーションテスト等ネットワークからの攻撃に対する検証試験、ウェブアプリケーションの脆弱性検査、データベースセキュリティ監査などを想定。
情報取扱者の制限	利用者のデータにアクセスできる利用者が限定されていること。	有無／設定状況	有（利用者のデータにアクセスできる社員等はセキュリティ管理者の許可を得た者に限る。）	
情報取扱い環境	提供者側でのデータ取扱環境が適切に確保されていること。	有無	有 （オフィスは IC カードによる運用で執務室に入室可能な社員等を最小限に制限しており、PC はすべてシンクライアントである）	
通信の暗号化レベル	システムとやりとりされる通信の暗号化強度。	有無	SSL、あるいは VPN	SSL の場合は、SSL3.0/TLS1.0（暗号強度 128 ビット）以上に限定。

「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」

＜別紙 1・2（全体像）＞

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）

〔パッケージ、SaaS/ASP活用、保守・運用〕＜追補版＞

※数字は共通フレーム2007該当項番

パッケージカスタマイズ 取引・契約モデルの全体像

別紙1

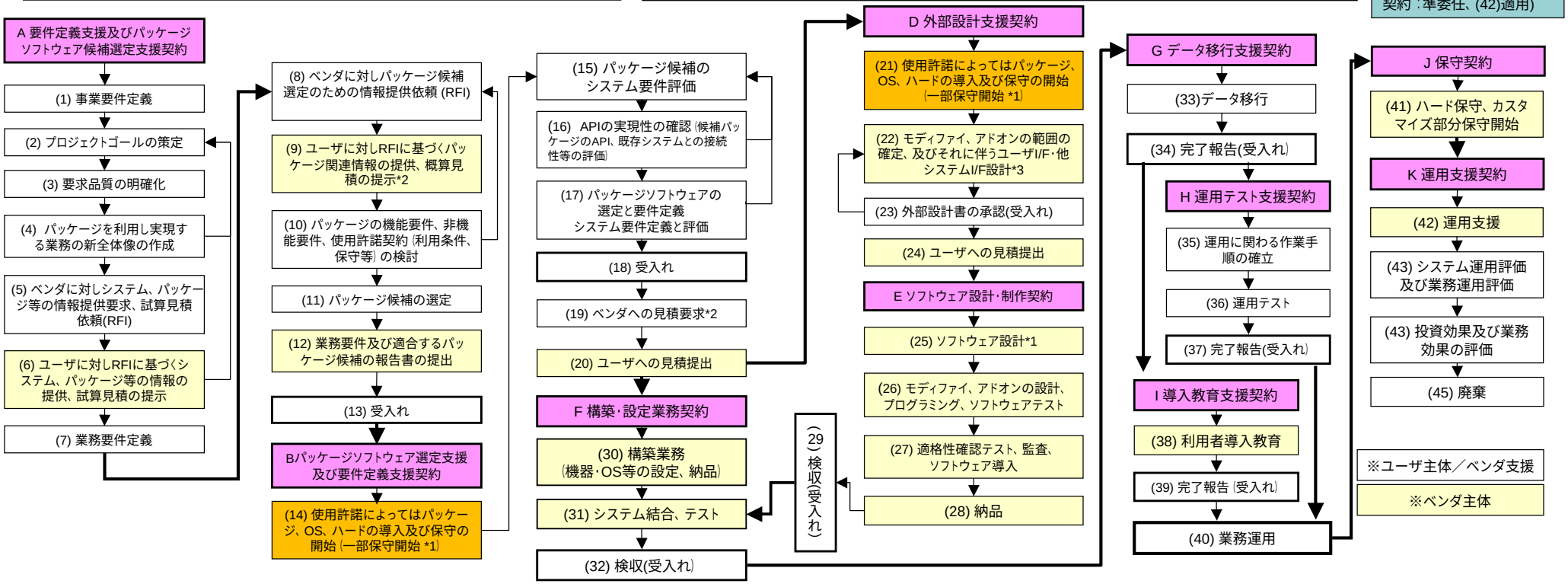
1.4 企画　1.5 要件定義　1.6 開発　設計・制作・テスト・移行　運用準備　1.7 運用　1.8 保守

パッケージソフトウェア利用コンピュータシステム構築委託契約書

重要事項説明書 A要件定義支援及びパッケージソフトウェア候補選定支援業務契約(カスタマイズモデル):準委任、(1)～(13)適用、Bパッケージソフトウェア選定支援及び要件定義支援業務契約(カスタマイズモデル):準委任、(14)～(18)適用

重要事項説明書 D外部設計支援業務契約:準委任・(21)～(23)適用、Eソフトウェア設計・制作契約:請負・(25)～(29)適用、F構築・設定業務契約:請負・(30)～(32)適用、Gデータ移行支援契約:準委任・(33)～(34)適用、H運用テスト支援契約:準委任・(35)～(37)適用、I導入教育支援契約:準委任・(38)～(39)適用

重要事項説明書 J保守契約:準委任・(14)(21)(25)(41)適用、K運用支援契約:準委任、(42)適用)



パッケージソフト、OS、第三者ソフトの使用許諾契約の検討〔制限事項、保守、バージョンアップ等〕

選定したパッケージソフト、OS、第三者ソフトの使用許諾契約の締結及び必要に応じて保守契約の締結*1

選定したパッケージソフト、OS、第三者ソフトの使用許諾契約の締結及び必要に応じて保守契約の締結

パッケージソフトウェア、OS、第三者ソフトウェアの使用許諾契約

*1 パッケージソフトウェアの使用許諾契約及び保守は、開発に入る段階で締結するのが一般的であるが、APIの実現性の確認、又は外部設計で、使用許諾契約、保守契約を締結しなければならない製品がある。使用許諾契約、保守契約の開始については(10)で事前に検討が必要である。
*2 システム規模と要件によって見積は概算もしくは詳細になる。

■参照すべき規格:共通フレーム2007「1.4 企画プロセス」・「1.5 要件定義プロセス」、JIS Q 20000 情報技術ーサービスマネジメント、JIS Q 27001 情報技術ーセキュリティ技術、JIS X 0129-1 ソフトウェア製品の品質

■チェックリスト:コンサルタントチェックリスト、セキュリティチェックリスト

■参照すべき規格:共通フレーム2007「1.5.3 利害関係者要件の確認」・「1.6 開発プロセス」・「2.7 監査プロセス」、JIS Q 27001情報技術ーセキュリティ技術、JIS X 0129-1 6.品質モデル・A.1.21内部測定法・A1.3外部測定法・A3測定法の選択及び測定基準

■チェックリスト:RFPチェックリスト、パッケージ選定チェックリスト、SaaS/ASP選定チェックリスト

■参照すべき規格:共通フレーム2007「1.7運用プロセス」・「1.8 保守プロセス」、JIS X 0129-1 7.1 利用時の品質、JIS X 0161 ソフトウェア保守

■チェックリスト:検収チェックリスト

〔パッケージ、SaaS/ASP活用、保守・運用〕＜追補版＞

※数字は共通フレーム2007該当項番

パッケージオプション 取引・契約モデルの全体像

別紙2

1.4 企画　1.5 要件定義　1.6 開発　設計・制作・テスト・移行　運用準備　1.7 運用　1.8 保守

パッケージソフトウェア利用コンピュータシステム構築委託契約書

重要事項説明書 Cパッケージソフトウェア選定支援及び要件定義支援業務契約(オプションモデル)：準委任、(1)～(18)適用

重要事項説明書 D外部設計支援業務契約：準委任・(21)～(23)適用、Eソフトウェア設計・制作契約：請負・(25)～(29)適用、F構築・設定業務契約：請負・(30)～(32)適用、Gデータ移行支援契約：準委任・(33)～(34)適用、H運用テスト支援契約：準委任・(35)～(37)適用、I導入教育支援契約：準委任・(38)～(39)適用

重要事項説明書 J保守契約：準委任・(14)(21)(25)(41)適用、K運用支援契約：準委任、(42)適用)

Cパッケージソフトウェア選定支援及び要件定義支援契約
(1) 事業要件定義
(2) プロジェクトゴールの策定
(3) 要求品質の明確化
(4) パッケージを利用し実現する業務の新全体像の作成
(5) ベンダに対しシステム、パッケージ等の情報提供要求、試算見積依頼(RFI)
(6) ユーザに対しRFIに基づくシステム、パッケージ等の情報の提供、試算見積の提示
(7) 業務要件定義

パッケージオプションモデルでは、(8)～(9)、(12)～(13)は省略されている。必要に応じて、別紙1を参照すること。(2)～(14)では、必要に応じて(5)情報提供要求～(6)情報の提供タスクを繰り返してよい。

(10) パッケージの機能要件、非機能要件、使用許諾契約(利用条件、保守等)の検討*1
(11) パッケージ候補の選定
(14) 使用許諾によってはパッケージ、OS、ハードの導入及び保守の開始(一部保守開始 *2)

(15) パッケージ候補のシステム要件評価
(16) APIの実現性の確認(候補パッケージのAPI、既存システムとの接続性等の評価)
(17) パッケージソフトウェアの選定と要件定義 システム要件定義と評価*2
(18) 受入れ
(19) ベンダへの見積要求*3
(20) ユーザへの見積提出

F 構築・設定業務契約
(30) 構築業務(機器・OS等の設定、納品)
(31) システム結合、テスト
(32) 検収(受入れ)

(29) 検収(受入れ)

D 外部設計支援契約
(21) 使用許諾によってはパッケージ、OS、ハードの導入及び保守の開始(一部保守開始 *2)
(22) 外部プログラムの範囲の確定、及びそれに伴うユーザI/F・他システムI/F設計*3
(23) 外部設計書の承認(受入れ)
(24) ユーザへの見積提出

E ソフトウェア設計・制作契約
(25) ソフトウェア設計(一部保守開始 *2)
(26)外部プログラムの設計、プログラミング、ソフトウェアテスト
(27) 適格性確認テスト、監査、ソフトウェア導入
(28) 納品

G データ移行支援契約
(33)データ移行
(34) 完了報告(受入れ)

H 運用テスト支援契約
(35) 運用に関わる作業手順の確立
(36) 運用テスト
(37) 完了報告(受入れ)

I 導入教育支援契約
(38) 利用者導入教育
(39) 完了報告(受入れ)

(40) 業務運用

J 保守契約
(41) ハード保守、外部プログラム等保守開始

K 運用支援契約
(42) 運用支援
(43) システム運用評価及び業務運用評価
(43) 投資効果及び業務効果の評価
(45) 廃棄

※ユーザ主体／ベンダ支援
※ベンダ主体

パッケージソフトウェア、OS、第三者ソフトウェアの使用許諾契約

パッケージソフト、OS、第三者ソフトの使用許諾契約の検討(制限事項、保守、バージョンアップ等)
選定したパッケージソフト、OS、第三者ソフトの使用許諾契約の締結及び必要に応じて保守契約の締結*2
選定したパッケージソフト、OS、第三者ソフトの使用許諾契約の締結及び必要に応じて保守契約の締結

*1 パッケージソフトウェアのオプション製品も候補選定、評価する。
*2 パッケージソフトウェアの使用許諾契約及び保守は、開発に入る段階で締結するのが一般的であるが、APIの実現性の確認、又は外部設計で、使用許諾契約、保守契約を締結しなければならない製品がある。使用許諾契約、保守契約の開始については(10)で事前に検討が必要である。
*3 システム規模と要件によって見積は概算もしくは詳細になる。

■参照すべき規格：共通フレーム2007「1.4 企画プロセス」・「1.5 要件定義プロセス」、JIS Q 20000 情報技術－サービスマネジメント、JIS Q 27001 情報技術－セキュリティ技術、JIS X 0129-1 ソフトウェア製品の品質

■チェックリスト：コンサルタントチェックリスト、セキュリティチェックリスト

■参照すべき規格：共通フレーム2007「1.5.3 利害関係者要件の確認」・「1.6 開発プロセス」・「2.7 監査プロセス」、JIS Q 27001情報技術－セキュリティ技術、JIS X 0129-1 6.品質モデル・A.1.21内部測定法・A1.3外部測定法・A3測定法の選択及び測定基準

■チェックリスト：RFPチェックリスト、パッケージ選定チェックリスト、SaaS/ASP選定チェックリスト

■参照すべき規格：共通フレーム2007「1.7運用プロセス」・「1.8 保守プロセス」、JIS X 0129-1 7.1 利用時の品質、JIS X 0161 ソフトウェア保守

■チェックリスト：検収チェックリスト

「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」

パッケージソフトウェア利用コンピュータシステム構築委託モデル契約書
（システム基本契約書）

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）

パッケージソフトウェア利用コンピュータシステム構築委託モデル契約書
（システム基本契約書）

委託者＿＿＿＿＿＿＿＿＿＿（以下「ユーザ」という。）と受託者＿＿＿＿＿＿＿＿＿＿（以下「ベンダ」という。）とは、パッケージソフトウェア、SaaS および／もしくは ASP を利用して構築するユーザ向けのコンピュータシステム（以下「本件システム」という。）に係る業務の委託に関して、次のとおり契約（以下「システム基本契約書」という。）を締結する。

（本契約の構造）

第 1 条　本契約は、システム基本契約書及び以下の業務のうち左欄に☑が記された業務（以下「本件業務」という。）に関する各個別契約書によって構成される。

A　要件定義支援及びパッケージソフトウェア要件定義支援業務契約（カスタマイズモデル）
B　パッケージソフトウェア選定支援及び要件定義支援業務契約（カスタマイズモデル）
C　パッケージソフトウェア選定支援及び要件定義支援業務契約（オプションモデル）
D　外部設計支援業務契約
E　ソフトウェア設計・制作業務契約
F　構築・設定業務契約
G　データ移行支援業務契約
H　運用テスト支援業務契約
I　導入教育支援業務契約
J　保守業務契約
K　運用支援業務契約

2)　前項の各個別契約書は、システム基本契約書と一体となる本件業務に関するそれぞれの別紙重要事項説明書へのユーザ及びベンダによる記名押印をもって締結する。

（契約内容の確定及び変更等）

第 2 条　本契約（システム契約並びに選択された本件業務についての別紙重要事項説明書によって構成される契約全体を指す）の内容は、以下のとおり確定し、以下の条件に従って変更することができる。

①　ベンダ及びユーザが記名押印した、システム契約並びに別紙重要事項説明書に記載された内容は、ひとつの契約を構成し、そのタイトルの部分に「予約」と記載されていない限り、ベンダ及びユーザを法的に拘束する。

②　別紙重要事項説明書には、確定した契約条件のほかにまだ確定していない契約条件が記載されていることがあり、このうち確定していない契約条件については、そのタイトルの部分に「予約」と記載される。予約と記載された事項についての記載はベンダ及びユーザを法的に拘束するものではな

い。

③　ベンダが複数の本件業務を担当する場合、ユーザ及びベンダは、最初に遂行すべき本件業務に係る部分については、すべての契約内容を確定させるものとする。

④　ベンダが複数の本件業務を担当する場合で当初複数の重要事項説明書を作成している場合は、ユーザ及びベンダは、最初に遂行すべき本件業務以外に係る重要事項説明書について、それぞれの本件業務の開始時に、具体的業務内容、個別契約条項等の条項の再確認を行い、その時点までにで確定していなかった条項を確定し、また必要に応じて確定されていた条項についての変更を行った上で、当該本件業務に関する契約条件を確定する。この場合における契約条件の確定は、新たに重要事項説明書（以下「改訂版重要事項説明書」という。）を作成しこれにユーザ及びベンダが記名押印することによって行う。

⑤　改訂版重要事項説明書は、これが作成され記名押印されたときから、本契約と一体をなすものとして本契約の内容を規定する効力を生じる。

⑥　④所定の契約条件変更のほか、ユーザ及びベンダの協議により、別紙重要事項説明書（改訂版重要事項説明書を含む。以下同じ。）に記載された条項の変更を行う場合は、ユーザ及びベンダが記名押印した書面によって行うものとする。なお、かかる変更の際には価格及び納期の変更の有無、変更の内容についても協議・合意されるものとする。

⑦　ベンダは、ユーザが前号の変更規定に基づかずに契約条件の変更を行った場合、この変更により生じたことについて、一切の責任を負わない。

（協働と役割分担）

第 3 条　ユーザ及びベンダは、双方による共同作業及び各自の分担作業を誠実に実施するとともに、相手方の分担作業の実施に対して誠意をもって協力するものとする。

2)　ユーザ及びベンダ双方による共同作業及び各自の分担作業は、別紙重要事項説明書においてその詳細を定めるものとする。

3)　ユーザ及びベンダは、共同作業及び各自の実施すべき分担作業を遅延し又は実施しない場合若しくは不完全な実施であった場合、それにより相手方に生じた損害の賠償も含め、かかる遅延又は不実施若しくは不完全な実施について相手方に対して責任を負うものとする。

（連絡協議会の設置）

第 4 条　ユーザ及びベンダは、本件業務が終了するまでの間、その進捗状況、リスクの管理及び報告、ユーザ及びベンダ双方による共同作業及び各自の分担作業の実施状況、システム仕様書に盛り込むべき内容の確認、問題点の協議及び解決その他本件業務が円滑に遂行できるよう必要な事項を協議するため、連絡協議会を開催するものとする。但し、システム基本契約及び別紙重要事項説明書の内容の変更は第 2 条（契約内容の確定及び変更等）に従ってのみ行うことができるものとする。

2)　連絡協議会は、原則として、別紙重要事項説明書で定める頻度で定期的に開催するものとし、それに加えて、ユーザ又はベンダが必要と認める場合に随時開催するも

のとする。

3) 連絡協議会には、ユーザ及びベンダ双方の責任者、主任担当者及び責任者が適当と認める者が出席する。また、ユーザ及びベンダは、連絡協議会における協議に必要となる者の出席を相手方に求めることができ、相手方は合理的な理由がある場合を除き、これに応じるものとする。

4) ベンダは、連絡協議会において、別途ユーザ・ベンダ間にて取り決めた様式による進捗管理報告を作成して提出し、当該進捗管理報告に基づいて進捗状況を確認するとともに、遅延事項の有無、遅延事項があるときはその理由と対応策、推進体制の変更（人員の交代、増減、再委託先の変更など）の要否、セキュリティ対策の履行状況、別紙重要事項説明書の変更を必要とする事由の有無、別紙重要事項説明書の変更を必要とする事由があるときはその内容などの事項を必要に応じて協議し、決定された事項、継続検討とされた事項並びに継続検討事項がある場合は検討スケジュール及び検討を行う当事者等を確認するものとする。

5) ユーザ及びベンダは、本件業務の遂行に関し連絡協議会で決定された事項について、システム基本契約及び別紙重要事項説明書に反しない限り、これに従わなければならない。

6) ベンダは、連絡協議会の議事内容及び結果について、書面により議事録を作成し、これをユーザに提出し、その承認を得た後に、ユーザ及びベンダ双方の責任者がこれに記名押印の上、それぞれ 1 部保有するものとする。ベンダは、議事録の原案を原則として連絡協議会の開催日から○日以内に作成して、これをユーザに提出し、ユーザは、これを受領した日から○日以内にその点検を行うこととし、当該期間内に書面により具体的な理由を明示して異議を述べない場合には、ベンダが作成した議事録を承認したものとみなすものとする。

7) 前項の議事録は、少なくとも当該連絡協議会において決定された事項、継続検討とされた事項及び継続検討事項がある場合は、検討スケジュール及び検討を行う当事者の記載を含むものとする。

（ユーザがベンダに提供する資料等及びその返還）

第 5 条 ユーザは、ベンダに対し、本件業務に必要な資料、機器、設備等（以下「資料等」という。）の開示、貸与等を行うものとする。

2) ユーザが前項に基づきベンダに提供した資料等の内容に誤りがあった場合又はユーザが提供すべき資料等の提供を遅延した場合、これらの誤り又は遅延によって生じた費用の増大、完成時期の遅延、瑕疵などの結果について、ベンダは責任を負わない。

3) ベンダは、ユーザから提供を受けた資料等を善良なる管理者の注意義務をもって管理し、双方が合意した返還日又はユーザから請求があったときに、これらを返還する。

4) 資料等の提供及び返還にかかる費用は、ユーザが負担する。

（再委託）

第 6 条 ベンダは、ベンダの責任において、本件業務の一部を第三者に再委託することができる。但し、ベンダは、ユーザから請求があった場合には、再委託先の名称及び住所等、再委託先を特定しうるだけの情報をユーザに通知しなければならない。当該

第三者に再委託することが不適切となる合理的な理由が存する場合、ユーザは、その理由を書面によりベンダに通知することにより、当該第三者に対する再委託の中止を請求することができる。なお、ユーザから再委託の中止の請求をベンダが受けた場合は、作業期間、納期または委託料等の内容の変更について、第 2 条⑥に準じて協議を行い、合理的な範囲で合意するものとする。

2) ベンダは、再委託先との間で、再委託に係る業務を行わせる場合、本契約に基づいてベンダがユーザに対して負担するのと同様の義務を、再委託先に負わせる契約を締結するものとする。

3) ベンダは、再委託先の履行についてユーザに帰責事由がある場合を除き、自ら業務を遂行した場合と同様の責任を負うものとする。

（秘密情報の取扱い）

第 7 条 ユーザ及びベンダは、本件業務の遂行のため、相手方より提供を受けた技術上又は営業上その他業務上の情報のうち、相手方が書面により秘密である旨指定して開示した情報、又は口頭により秘密である旨を示して開示した情報で開示後○日以内に書面により内容を特定した情報（以下あわせて「秘密情報」という。）を第三者に漏洩してはならない。但し、次の各号のいずれか一つに該当する情報についてはこの限りではない。また、ユーザ及びベンダは秘密情報のうち法令の定めに基づき開示すべき情報を、当該法令の定めに基づく開示先に対し開示することができるものとする。

① 秘密保持義務を負うことなくすでに保有している情報

② 秘密保持義務を負うことなく第三者から正当に入手した情報

③ 相手方から提供を受けた情報によらず、独自に開発した情報

④ 本契約に違反することなく、かつ、受領の前後を問わず公知となった情報

2) 秘密情報の提供を受けた当事者は、当該秘密情報の管理に必要な措置を講ずるものとする。

3) ユーザ及びベンダは、秘密情報について、本契約の目的の範囲内でのみ使用し、本契約の目的の範囲を超える複製、改変が必要なときは、事前に相手方から書面による承諾を受けるものとする。

4) ユーザ及びベンダは、秘密情報を、本契約の目的のために知る必要のある各自（本契約に基づきベンダが再委託する場合の再委託先を含む。）の役員及び従業員に限り開示するものとし、本契約に基づきユーザ及びベンダが負担する秘密保持義務と同等の義務を、秘密情報の開示を受けた当該役員及び従業員に退職後も含め課すものとする。

5) 秘密情報の提供及び返還等については、第 5 条（ユーザがベンダに提供する資料等及びその返還）に準じる。

6) 秘密情報のうち、個人情報に該当する情報については、第 8 条が本条の規定に優先して適用されるものとする。

7) 本条の規定は、本契約終了後、○年間存続する。

（個人情報）

第 8 条　ベンダは、個人情報の保護に関する法律（本条において、以下「法」という。）に定める個人情報のうち、本件業務遂行に際してユーザより取扱いを委託された個人データ（法第 2 条第 4 項に規定する個人データをいう。以下同じ。）及び本件業務遂行のため、ユーザ･ベンダ間で個人データと同等の安全管理措置（法第 20 条に規定する安全管理措置をいう。）を講ずることについて、別紙重要事項説明書その他の契約において合意した個人情報（以下あわせて「個人情報」という。）を第三者に漏洩してはならない。なお、ユーザは、個人情報をベンダに提示する際にはその旨明示するものとする。また、ユーザは、ユーザの有する個人情報をベンダに提供する場合には、個人が特定できないよう加工した上で、ベンダに提供するよう努めるものとする。

2)　ベンダは、個人情報の管理に必要な措置を講ずるものとする。

3)　ベンダは、個人情報について、本契約の目的の範囲内でのみ使用し、本契約の目的の範囲を超える複製、改変が必要なときは、事前にユーザから書面による承諾を受けるものとする。

4)　個人情報の提供及び返還等については、第 5 条（資料等の提供及び返還）を準用する。

5）　第 6 条第 1 項の規定にかかわらず、ベンダはユーザより委託を受けた個人情報の取扱いを再委託してはならない。但し、当該再委託につき、ユーザの事前の承諾を受けた場合はこの限りではない。

（報告書の著作権）

第 9 条　ベンダがユーザに対して提出する報告書に関する著作権（著作権法第 27 条及び第 28 条の権利を含む。）は、ユーザ又は第三者が従前から保有していた著作物の著作権を除き、ベンダに帰属するものとする。

2)　ユーザは、前項の報告書又はその複製物を、本件システムを利用するために必要な範囲で、複製、翻案することができるものとする。

（損害賠償）

第 10 条　ユーザ及びベンダは、本契約の履行に関し、相手方の責めに帰すべき事由により損害を被った場合、相手方に対して、法令に基づく損害賠償を請求することができる。但し、別紙重要事項説明書に請求期間が定められている場合は、法令に基づく請求期間にかかわらず重要事項説明書に定める期間の経過後は請求を行うことができない。

2)　前項の損害賠償の累計総額は、債務不履行、法律上の瑕疵担保責任、不当利得、不法行為その他請求原因の如何にかかわらず、帰責事由の原因となった業務に係る別紙重要事項説明書に定める損害賠償限度額を限度とする。

3)　前項は、損害が損害賠償義務者の故意又は重大な過失に基づくものである場合には適用しないものとする。

（解除）

第 11 条　ユーザ又はベンダは、相手方に次の各号のいずれかに該当する事由が生じた場合には、何らの催告なしに直ちに本契約の全部又は一部を解除することができる。

① 重大な過失又は背信行為があった場合

② 支払いの停止があった場合、又は仮差押、差押、競売、破産手続開始、民事再生手続開始、会社更生手続開始、特別清算開始の申立があった場合

③ 手形交換所の取引停止処分を受けた場合

④ 公租公課の滞納処分を受けた場合

⑤ その他前各号に準ずるような本契約を継続し難い重大な事由が発生した場合

2) ユーザ又はベンダは、相手方が本契約のいずれかの条項に違反し、相当期間を定めてなした催告後も、相手方の債務不履行が是正されない場合は、本契約の全部又は一部を解除することができる。

3) ユーザ又はベンダは、第 1 項各号のいずれかに該当する場合又は前項に定める解除がなされた場合、相手方に対し負担する一切の金銭債務につき相手方から通知催告がなくとも当然に期限の利益を喪失し、直ちに弁済しなければならない。

（権利義務譲渡の禁止）

第 12 条　ユーザ及びベンダは、互いに相手方の事前の書面による同意なくして、本契約上の地位を第三者に承継させ、又は本契約から生じる権利義務の全部若しくは一部を第三者に譲渡し、引き受けさせ若しくは担保に供してはならない。

（協議）

第 13 条　本契約に定めのない事項又は疑義が生じた事項については、信義誠実の原則に従いユーザ及びベンダが協議し、円満な解決を図る努力をするものとする。

（和解による紛争解決・合意管轄）

第 14 条　本契約に関し、ユーザ及びベンダに紛争が生じた場合、ユーザ及びベンダは、次項の手続をとる前に、紛争解決のため第 4 条に定める連絡協議会を開催し協議を充分に行うとともに、次項及び 3 項に定める措置をとらなければならない。

2）　前項所定の連絡協議会における協議でユーザ・ベンダ間の紛争を解決することができない場合、本条第 4 項に定める紛争解決手続をとろうとする当事者は、相手方に対し紛争解決のための権限を有する代表者又は代理権を有する役員その他の者との間の協議を申し入れ、相手方が当該通知を受領してから◯日以内に（都市名）において、本条第 4 項に定める紛争解決手続以外の裁判外紛争解決手続（以下「ADR」という。）などの利用も含め誠実に協議を行うことにより紛争解決を図るものとする。

3）　前項による協議又は ADR によって和解が成立する見込みがないことを理由に当該協議又は ADR が終了した場合、ユーザ及びベンダは、法的救済手段を講じることができる。

4）　本契約に関し、訴訟の必要が生じた場合には、◯◯地方裁判所を第一審の専属的合意管轄裁判所とする。

◯◯◯◯年◯◯月◯◯日

ユーザ：　　ベンダ：

「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」

重要事項説明書

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）

重要事項説明書

契約の表示	本件システムの名称	○○○○○○○○		
	本重要事項説明書は以下の委託者と受託者における○○○○年○月○日付の**パッケージソフトウェア利用コンピュータシステム構築委託モデル契約書**（以下「システム基本契約書」といいます。）に係る以下の業務の契約に関するものです。			
	契約の名称		該当	契約の類型
	A　要件定義支援及びパッケージソフトウェア候補選定支援業務契約（カスタマイズモデル）		あり・なし	準　委　任
	B　パッケージソフトウェア選定支援及び要件定義支援業務契約（カスタマイズモデル）		あり・なし	準　委　任
	C　パッケージソフトウェア選定支援及び要件定義支援業務契約(オプションモデル)		あり・なし	準　委　任
	D　外部設計支援業務契約		あり・なし	準　委　任
	E　ソフトウェア設計・制作業務契約		あり・なし	請　　負
	F　構築・設定業務契約		あり・なし	請　　負
	G　データ移行支援業務契約		あり・なし	準　委　任
	H　運用テスト支援業務契約		あり・なし	準　委　任
	I　導入教育支援業務契約		あり・なし	準　委　任
	J　保守業務契約		あり・なし	準　委　任
	K　運用支援業務契約		あり・なし	準　委　任

○○○○○○○○○○○○○　　御中（ユーザ）　　日付：○○○○年○○月○○日

標記取引について、本重要事項説明書及び末尾記載の添付図書の原本もしくは写しを交付し、重要事項の説明を致します。**本書の内容は個別契約として本契約の一部を構成する条項の詳細な内容であり大変重要です。用語や内容がご不明の場合は、いつでもご質問頂き、十分理解されるようお願い致します。**

受託者（ベンダ）	会　社　名			
	主たる事務所	〒		
	代表者氏名			
	重要事項を説明する契約担当責任者			
	所属部門名			
	氏　名	記名　　印	電話番号	（　　）
	業務に従事する事務所	〒		

■告知事項

情報システムの機能適合性や品質（応答性能、信頼性、安定性、セキュリティ等）の確保には委託者と受託者の綿密なコミュニケーションと協働が必要です。情報システムの仕様や目的の不適合、運用上の不都合の発生は、事前のコミュニケーションやテストの不足、協働の失敗などが原因であり、これらが原因による情報システムの改修や修復には多大な費用と時間が費やされる場合があります。また、場合によってはこれらの改修費用などをご負担いただくこともあります。情報システムの構築に関わる各業務の性質をご理解頂いた上で、本重要事項説明書を精査の上、ご承認をお願い申し上げます。

受領書および契約条件の承認

△△△△△△△△△△△　　御中(ベンダ)　　日付：○○○○年○○月○○日

標記取引について、本重要事項説明書および末尾一覧に記載された添付図書の原本もしくは写しを受領し、告知事項、重要事項の説明を受け、本契約の条件について承認しました。

委託者（ユーザ）	会　社　名			
	住　所	〒		
	代表者氏名	記名　　印	電話番号	（　　）
	担当者氏名	記名　　印	電話番号	（　　）

（鑑部分）

契約及び費用の一覧

契約名称	受託金額（税抜）	支払条件	システム基本契約書第４条に基づく責任者、主任担当者名				特記事項
			ユーザ側		ベンダ側		
			責任者	主任担当者	責任者	主任担当者	
特約条項：							

プロジェクト体制図（組織図）

（鑑部分）

A　要件定義支援及びパッケージソフトウェア候補選定支援業務契約（カスタマイズモデル）の重要事項　(1)

■要件定義支援及びパッケージソフトウェア候補選定支援業務契約（カスタマイズモデル）の概要（契約の内容となる具体的作業は次頁以降に記載されています。これらの作業実施には、ベンダの担当する作業とお客様に作業をお願いするものがあります。）
【記載例】お客様の業務の調査・分析に基づき、業務の新全体像、業務モデル、システム方式、付帯機能の方針、サービスレベルと品質に対する方針の策定支援、システム機能の実現範囲（機能要件）と品質・性能・運用操作、セキュリティ等（非機能要件）を含む業務要件の定義、これに基づく適切なパッケージソフトウェア候補の選定（使用許諾契約の内容、保守性、SaaS/ASP においては SLA の評価などの検討を含みます。）等の支援を行います。

■契約類型：準委任契約

■個別契約条項

1．個別契約の成立

ユーザは、ベンダに対し、本重要事項説明書の具体的作業内容に記載された業務（以下「本件業務」といいます。）の提供を依頼し、ベンダは、これを引き受けました。本件業務の内容、日程、代金（代金の支払い方法を含みます。）、各当事者の具体的な義務等の取引条件は、システム基本契約書、本重要事項説明書の具体的作業内容及び本個別契約条項の記載に従います。

2．パッケージソフトウェア候補の選定支援における善管注意義務

1)　本契約（システム基本契約書と個別契約書としての本重要事項説明書から構成されます。以下同じ。）及びこれに関連する契約に基づきユーザに納入されるソフトウェア、ハードウェア等のシステムの構築のためには、その中核を構成するものとして第三者が権利を有するソフトウェア、SaaS 及びもしくは ASP（以下あわせて「本件パッケージ」といいます。）が利用されます。その候補の選定はユーザが行うものとします。

2)　ベンダは、本重要事項説明書に定めるところにより、本件パッケージの候補の選定を支援するときには、情報処理技術に関する業界の一般的な専門知識及びノウハウに基づき、善良な管理者の注意をもって行うものとします。ベンダは適切と判断するときは、本件パッケージの候補が存在しないことをユーザに進言しなければなりません。

3．ベンダの善管注意義務

ベンダは、情報処理技術に関する業界の一般的な専門知識及びノウハウに基づき、ユーザの作業が円滑かつ適切に行われるよう、善良な管理者の注意をもって、本契約に基づく調査、分析、整理、提案及び助言などの支援業務を行うものとします。

4．業務終了の確認

1)　ベンダは、本重要事項説明書に記載された期限までに、業務完了報告書兼検収依頼書を作成し、ユーザに提出します。

2)　ユーザは、本重要事項説明書に定める期間（以下「点検期間」といいます。）内に、前項の業務報告書の点検を行うものとします。

3)　ユーザは、第１項の業務報告書の内容に異議がない場合には、業務完了確認書兼検収書に記名押印してベンダに交付することで、本件業務の終了を確認するものとします。

4)　ユーザが、業務完了確認書兼検収書に記名押印をしない場合であっても、点検期間内に書面で具体的な理由を明示して異議を述べないときは、点検期間の満了をもって本件業務の終了を確認したものとみなします。

■告知事項

内容や専門用語でご不明の点は随時ご質問頂き、十分にご精査ください。

<table>
<tr><td colspan="3">A　要件定義支援及びパッケージソフトウェア候補選定支援業務契約（カスタマイズモデル）の重要事項　(2)具体的作業内容</td></tr>
<tr><td>作業項目</td><td colspan="2">作業内容及び作業実施担当</td></tr>
<tr><td>企画（業務の新全体像、業務モデル、システム方式、付帯機能の方針、サービスレベルと品質に対する方針の策定支援）</td><td>ユーザ</td><td>ベンダ</td></tr>
<tr><td colspan="3">以上に関わる報告書の作成：提出予定期限〇〇〇〇年〇〇月〇〇日</td></tr>
<tr><td>業務要件定義（機能要件、非機能要件、セキュリティを含む）</td><td>ユーザ</td><td>ベンダ</td></tr>
<tr><td colspan="3">以上に関わる報告書の作成：提出予定期限〇〇〇〇年〇〇月〇〇日</td></tr>
<tr><td>パッケージソフトウェア候補の選定支援（使用許諾契約、保守性、業務要件に対する機能適合評価、SaaS/ASP においては SLA の評価を含みます）</td><td>ユーザ</td><td>ベンダ</td></tr>
<tr><td colspan="3">以上に関わる報告書の作成：提出予定期限〇〇〇〇年〇〇月〇〇日</td></tr>
<tr><td colspan="3">連絡協議会の実施要項及びユーザ・ベンダの責任者、主任担当者：</td></tr>
<tr><td colspan="3">未決事項：</td></tr>
<tr><td colspan="3">付帯事項（作業を実施する場合の場所・期限等、要件の合意、承認ルールを含みます。）：</td></tr>
<tr><td colspan="3">特約条項：

業務完了報告書の提出期限：〇〇〇〇年〇〇月〇〇日</td></tr>
<tr><td colspan="3">上記各報告書に係る点検期間：提出日から〇日間</td></tr>
<tr><td colspan="2">受託金額(税抜)もしくは受託金額の決定基準：</td><td>損害賠償限度額：</td></tr>
<tr><td colspan="2">支払期限：〇〇〇〇年〇〇月〇〇日</td><td>支払方法：　現金・口座振込</td></tr>
</table>

B　パッケージソフトウェア選定支援及び要件定義支援業務契約（カスタマイズモデル）の重要事項　(1)

■パッケージソフトウェア選定支援及びシステム要件定義支援業務の概要（契約の内容となる具体的作業は、次頁以降に記載されています。これらの作業には、ベンダの担当する作業とお客様にお願いする作業があります。）
【記載例】業務要件定義に基づき、システムの機能・能力等の決定、パッケージソフトウェア候補の機能の比較、不足部分（アドオン、外部プログラム）・変更（モディファイ）を要する部分の明確化・使用許諾契約の内容・将来にわたる保守性、機能、能力、動作環境、セキュリティ等とコストを勘案し、使用するパッケージソフトウェアを決定することを支援します。さらに必要とされる能力を満たすハードウェア等の選定、パッケージソフトウェアのモディファイ、アドオン作成のための API（アプリケーションプログラムインターフェース）、SaaS/ASP においては SLA の評価や、既存システムとの接続性等の評価を支援します。また、API 等の評価にあたりパッケージソフトウェア、ハードウェア等の導入が必要な場合、その明細及び金額を提示します。お客様との取決めによって、システム全体のテスト仕様書の作成及び提案要望書（RFP）の作成を含む場合があります。

■契約類型：準委任契約

■個別契約条項

1. 個別契約の成立
ユーザは、ベンダに対し、本重要事項説明書の具体的作業内容に記載された業務（以下「本件業務」といいます。）の提供を依頼し、ベンダは、これを引き受けました。本件業務の内容、日程、代金（代金の支払方法を含みます。）、各当事者の具体的な義務等の取引条件は、システム基本契約書、本重要事項説明書の具体的作業内容及び本個別契約条項の記載に従います。

2. 機器等の売買等
ユーザは、本契約（システム基本契約書と個別契約書としての本重要事項説明書から構成されます。以下同じ。）に基づきユーザに納入される本件システム（ソフトウェア、ハードウェアを含みます。）に関し、本件業務の提供を受けるにあたり、ベンダ又は第三者からソフトウェア、ハードウェア等(以下「機器等」といいます。)を購入し、又は借り入れる場合があります。当該購入又は借入れの契約条件については、本契約とは別個に締結される契約が本契約に優先して適用されるものとし、ベンダは、ベンダが契約当事者となる当該別契約に別段の定めのない限り、機器等の固有の瑕疵について責任を負いません。

3. パッケージソフトウェアの選定支援における善管注意義務
1)　本契約及びこれに関連する契約に基づきユーザに納入されるソフトウェア、ハードウェア等のシステムの構築のためには、その中核を構成するものとして第三者が権利を有するソフトウェア、SaaS 及びもしくは ASP（以下あわせて「本件パッケージ」といいます。）が利用されます。その選定はユーザが行うものとします。
2)　ベンダは、本重要事項説明書に定めるところにより、本件パッケージを提案しその選定を支援するときには、情報処理技術に関する業界の一般的な専門知識及びノウハウに基づき、善良な管理者の注意をもって行うものとします。ベンダは適切と判断するときは、本件パッケージとして最適なソフトウェア等が存在しないことをユーザに進言しなければなりません。

4. ベンダの善管注意義務
ベンダは、情報処理技術に関する業界の一般的な専門知識及びノウハウに基づき、ユーザの作業が円滑かつ適切に行われるよう、善良な管理者の注意をもって、本契約に基づく調査、分析、整理、提案及び助言などの支援業務を行うものとします。

5. 業務終了の確認
1)　ベンダは、本重要事項説明書に記載された期限までに、業務完了報告書兼検収依頼書を作成し、ユーザに提出します。
2)　ユーザは、本重要事項説明書に定める期間（以下「点検期間」といいます。）内に、前項の業務報告書の点検を行うものとします。
3)　ユーザは、第１項の業務報告書の内容に異議がない場合には、業務完了確認書兼検収書に記名押印してベンダに交付することで、本件業務の終了を確認するものとします。
4)　ユーザが、業務完了確認書兼検収書に記名押印をしない場合であっても、点検期間内に書面で具体的な理由を明示して異議を述べないときは、点検期間の満了をもって本件業務の終了を確認したものとみなします。

■告知事項
内容や専門用語でご不明の点は随時ご質問頂き、十分にご精査ください。

B　パッケージソフトウェア選定支援及び要件定義支援業務契約（カスタマイズモデル）の重要事項　(2)具体的作業内容		
本件業務にあたって使用する業務要件定義書：		
作業項目	作業内容及び作業実施担当	
パッケージ候補のシステム要件評価（移行要件を含みます。）	ユーザ	ベンダ
以上に関わる報告書の作成：提出予定期限○○○○年○○月○○日		
API の実現性の確認（候補パッケージの API、既存システムとの接続性等の評価、SaaS/ASP においては SLA の評価）	ユーザ	ベンダ
以上に関わる報告書の作成：提出予定期限○○○○年○○月○○日		
パッケージソフトウェアの選定（ソフトウェア要件定義と評価）	ユーザ	ベンダ
以上に関わる報告書の作成：提出予定期限○○○○年○○月○○日		
推奨ハードウェア構成の概要	ユーザ	ベンダ
以上に関わる報告書の作成：提出予定期限○○○○年○○月○○日		
システム全体のテスト仕様書作成（実施する・実施しない）	ユーザ	ベンダ
実施する場合、以上に関わる報告書の作成：提出予定期限○○○○年○○月○○日		
連絡協議会の実施要項及びユーザ・ベンダの責任者、主任担当者：		
未決事項		
付帯事項（作業を実施する場合の場所・期限等、要件の合意、承認ルールを含みます。）：		
特約条項：		
業務完了報告書の提出期限：○○○○年○○月○○日（RFP 作成を含む・含まない）		
上記各報告書に係る点検期間：提出日から○日間		
受託金額(税抜)もしくは受託金額の決定基準：	損害賠償限度額：	
支払条件　支払期限：	支払方法：　現金・口座振込	

B パッケージソフトウェア選定支援及び要件定義支援業務契約(カスタマイズモデル)の重要事項　(3)ソフトウェア、機器、ドキュメントの明細及び納入場所及び別途締結する契約の表示

ソフトウェア、機器、ドキュメントの明細一覧

項番	名称・型番・仕様・製造・開発元・提供会社等	単価	数量	価格（税抜）	納入日	納入先 稼働場所	無償保証の条件等*1		補修用性能部品（有償）の最低保有期間*1	取引・決済の形態、方法（リース・レンタル・売買）	別途締結する契約（売買契約、使用許諾契約等）
							無償保証期間	無償保守の条件等			
					○○年○○月○○日						
	合計金額（税抜）										

付帯事項：

特約条項：*1　○○○○年○○月○○日時点での内容であり、将来に向かって予告なく変更される場合があります。

C　パッケージソフトウェア選定支援及び要件定義支援業務契約(オプションモデル)の重要事項　(1)

■パッケージソフトウェア選定支援及び要件定義支援業務の概要（契約の内容となる具体的作業は、次頁以降に記載されています。これらの作業には、ベンダの担当する作業とお客様にお願いする作業があります。）
【記載例】お客様の業務の調査・分析に基づき、システム化の方針、業務内容の整理、システム機能の実現範囲（機能要件）と品質・性能・運用操作、セキュリティ等（非機能要件）などの業務要件の定義、これに基づく適切なパッケージソフトウェア候補の選定（使用許諾契約の内容、保守性、SaaS/ASP においては SLA の評価）などの検討を含みます）等の支援を行います。さらに、業務要件定義に基づき、システムの機能・能力等の決定、パッケージソフトウェア候補の機能の比較、使用許諾契約の内容・将来にわたる保守性、機能、能力、動作環境、セキュリティ等とコストを勘案し、使用するパッケージソフトウェアの決定を支援します。さらに必要とされる能力を満たすハードウェア等の選定等を支援します。パッケージソフトウェアの外部プログラム作成のための API（アプリケーションプログラムインターフェース）、SaaS/ASP においては SLA の評価や、既存システムとの接続性等の評価を支援します。また、API 等の評価にあたりパッケージソフトウェア、ハードウェア等の導入が必要な場合、その明細及び金額を提示します。お客様との取り決めによって、システム全体のテスト仕様書の作成及び提案要望書（RFP）の作成を含む場合があります。

■契約類型：準委任契約

■個別契約条項

1. 個別契約の成立
ユーザは、ベンダに対し、本重要事項説明書の具体的作業内容に記載された業務の提供を依頼し、ベンダは、これを引き受けました。業務の内容、日程、代金（代金の支払方法を含みます。）、各当事者の具体的な義務等の取引条件は、システム基本契約書、本重要事項説明書の具体的作業内容及び本個別契約条項の記載に従います。

2. 機器等の売買等
ユーザは、本契約（システム基本契約書と個別契約書としての本重要事項説明書から構成されます。以下同じ。）に基づきユーザに納入される本件システム（ソフトウェア、ハードウェア等を含みます。）に関し、本件業務の提供を受けるにあたり、ベンダ又は第三者からソフトウェア、ハードウェア等(以下「機器等」といいます。)を購入し、又は借り入れる場合があります。当該購入又は借入れの契約条件については、本契約とは別個に締結される契約が本契約に優先して適用されるものとし、ベンダは、ベンダが契約当事者となる当該別契約に別段の定めのない限り、機器等の固有の瑕疵について責任を負いません。

3. パッケージソフトウェアの選定支援における善管注意義務
1)　本契約及びこれに関連する契約に基づきユーザに納入されるソフトウェア、ハードウェア等のシステムの構築のためには、その中核を構成するものとして第三者が権利を有するソフトウェア、SaaS 及びもしくは ASP（以下あわせて「本件パッケージ」といいます。）が利用されます。その選定はユーザが行うものとします。
2)　ベンダは、本重要事項説明書に定めるところにより、本件パッケージを提案しその選定を支援するときには、情報処理技術に関する業界の一般的な専門知識及びノウハウに基づき、善良な管理者の注意をもって行うものとします。ベンダは適切と判断するときは、本件パッケージとして最適なソフトウェア等が存在しないことをユーザに進言しなければなりません。

4. ベンダの善管注意義務
ベンダは、情報処理技術に関する業界の一般的な専門知識及びノウハウに基づき、ユーザの作業が円滑かつ適切に行われるよう、善良な管理者の注意をもって、本契約に基づく調査、分析、整理、提案及び助言などの支援業務を行うものとします。

5. 業務終了の確認
1)　ベンダは、本重要事項説明書に記載された期限までに、業務完了報告書兼検収依頼書を作成し、ユーザに提出します。
2)　ユーザは、本重要事項説明書に定める期間（以下「点検期間」といいます。）内に、前項の業務報告書の点検を行うものとします。
3)　ユーザは、第１項の業務報告書の内容に異議がない場合には、業務完了確認書兼検収書に記名押印してベンダに交付することで、本件業務の終了を確認するものとします。
4)　ユーザが、業務完了確認書兼検収書に記名押印をしない場合であっても、点検期間内に書面で具体的な理由を明示して異議を述べないときは、点検期間の満了をもって本件業務の終了を確認したものとみなします。

■告知事項
内容や専門用語でご不明の点は随時ご質問頂き、十分にご精査ください。

C パッケージソフトウェア選定支援及び要件定義支援業務契約(オプションモデル)の重要事項　(2)具体的作業内容		
作業項目	作業内容及び作業実施担当	
企画（業務の新全体像、業務モデル、システム方式、付帯機能の方針、サービスレベルと品質に対する方針の明確化）	ユーザ	ベンダ
業務要件定義（機能要件、非機能要件、セキュリティを含む）	ユーザ	ベンダ
パッケージソフトウェア候補選定支援（使用許諾契約、保守性、業務要件に対する機能適合評価、SaaS/ASP においては SAL の評価を含みます。）	ユーザ	ベンダ
パッケージ候補のシステム要件評価	ユーザ	ベンダ
API の実現性の確認（候補パッケージの API、既存システムとの接続性等の評価、SaaS/ASP においては SAL の評価）	ユーザ	ベンダ
パッケージソフトウェアの選定（ソフトウェア要件定義と評価）	ユーザ	ベンダ
推奨ハードウェア構成の概要	ユーザ	ベンダ
システム全体のテスト仕様書作成（実施する・実施しない）	ユーザ	ベンダ
連絡協議会の実施要項：		
未決事項		
付帯事項（作業を実施する場合の場所・期限等、要件の合意、承認ルールを含みます。）：		
特約条項：		
業務完了報告書および要件定義書の提出期限：○○○○年○○月○○日（RFP 作成を含む・含まない）		
上記報告書及び要件定義書に係る点検期間：提出日から○日間		
受託金額(税抜)もしくは受託金額の決定基準	損害賠償限度額：	
支払期限：	支払方法：　現金・口座振込	

C　パッケージソフトウェア選定支援及び要件定義支援業務契約(オプションモデル)の重要事項　(3)ソフトウェア、機器、ドキュメントの明細及び納入場所及び別途締結する契約の表示

ソフトウェア、機器、ドキュメントの明細一覧

項番	名称・型番・仕様・製造・開発元・提供会社等	単価	数量	価格（税抜）	納入日	納入先 稼働場所	無償保証の条件等*1		補修用性能部品（有償）の最低保有期間*1	取引・決済の形態、方法（リース・レンタル・売買）	別途締結する契約（売買契約、使用許諾契約等）
							無償保証期間	無償保守の条件等			
					○○年○○月○○日						
	合計金額（税抜）										

付帯事項：

特約条項：*1　○○○○年○○月○○日時点での内容であり、将来に向かって予告なく変更される場合があります。

＜告知事項＞要件定義におけるセキュリィ仕様　(1)（記載例：B 又は C の業務要件定義に添付する）

	項番	対策内容	脅威の内容	実施担当		本件業務での対応	
				ユーザ	ベンダ	対応レベル*	仕様もしくは候補製品等
技術的セキュリティ対策(例)	1	■認証 情報を参照している人が本人なのかを証明をする。	情報を参照している人が、本人なのかを管理していないと、他人に重要な情報を見られる可能性がある。		○	2	ID、パスワードを利用して、個人を認識する。
	2	■アクセス権 情報よって、アクセスできる人を制限・管理する。	誰でも情報アクセスできるようになっていると、削除、改ざん、複製、持ち出しされたりする。		○	2	サーバ単位、フォルダ単位で、個人・グループがアクセスできるように設定する。
	3	■暗号化 情報を暗号化して、紛失・盗難・盗聴の対策を施す。	情報機器（コンピュータや USB メモリなど）が盗難又は紛失することにより、情報が漏えいするおそれがある。		○	3	社内の PC、社外に持ち出す PC、業務で使用する USB メモリ・外付け HDD、CD/DVD など情報を書き込めるものに対して暗号化をする。
	4	■ウイルス等の悪意あるプログラムの取り扱い及び検出する機能の導入 悪意あるプログラムから情報資産を守る。	コンピュータに誤動作を起こさせる悪意のあるプログラムにより、システムが利用できなくなる、データが消去される、情報が外部に漏えいする、などのおそれがある。		○	2	PC 上で悪意のあるプログラムを検出して削除し、警告する。
	5	■ネットワークの運用 ネットワークを流れるデータ量の管理をする。	ネットワーク障害や大量のデータ転送により、ネットワークが正常に利用できなくなるおそれがある。		○	2	障害検知やネットワーク負荷を検知するツールを導入する。
	6	■保守 OS やアプリケーション、ハードの保守を行なう。	保守がされていないと、不具合の発生や、セキュリティホールによって情報が漏えいするおそれがある。	○	△	3	保守対象となる不具合修正版の発行時に、ユーザが予備機にてテストを行い、適用する手順を文書化する。ベンダは、不具合修正版の発行を伝える。
	7	■機器運用監視 サーバ、ネットワーク機器の稼働監視を行う。	システムの状況を把握できないことにより、障害の対応が遅れて情報システムへのアクセスが長時間停止するおそれがある。		○	3	運用状況の把握や記録を自動的に行う。障害発生時にはユーザに通知する。
	8	■障害発生時の対応 障害時の対応マニュアルの整備をする。	システム障害時の対応手順が決められていないと、適切に対応できず、復旧が遅延するおそれがある。	○		3	障害発生時に手動で切り替える手順を定め文書化する。
	9	■データの保護 データが改ざんされないように防御する。	データが保護されていないと、データが改ざんされたり、漏えいしたりするなどのおそれがある。		○	2	すべてのデータを暗号化もしくはアクセス権での保護を実装する。
	10	■ログ管理 情報の持ち出し履歴をとって監査の証跡資料として管理する。	情報システムの監査ログが適切に管理されていないと不正な出来事に気付く事ができないおそれがある。		○	3	ログを取得し、定期的なレポートを行う。
物理的セキュリティ対策(例)	11	■作業領域（場所） コンピュータを設置する環境を管理する。	部外者が、簡単に会社や部屋に入れてしまうと、情報を盗まれる恐れがある。	○		2	マシンルームやオフィスを鍵で施錠して隔離する。
	12	■データの保管 データのバックアップをとる。	システムの緊急停止や不慮の災害の発生時に、システムを業務可能な状態に復旧できなくなる。	○	○	2	ベンダは日次、定時に複製を保管するための機能を実装する。ユーザは日常のバックアップ作業を実施する。**
	13	■作業環境管理（空調等） 適切な温度、湿度を保つ。	高温、多湿になると、コンピュータが正確に作動しなくなるおそれがある。	○		2	人が判断して、空調を調節する。
	14	■停電時の機器運用 停電時の稼動性を確保する。	停電などにより、コンピュータが稼動せずに業務が中断される、データを喪失するなどのおそれがある。		○	2	停電発生時に安全に停止できるように補助電源装置及び自動停止機能を実装する。
	15	■資産の管理 資産台帳を作成し、資産を管理する。	資産（情報機器･電子媒体･紙）の資産管理がされていないと紛失･盗難の検知ができない。	○		2	管理手順を文書化し、人が確認し、管理台帳を作成して管理する。
管理的セキュリティ対策(例)	16	■資産分類 資産を重要度に応じて分類し、取扱いを定め管理する。	情報資産が取扱い基準（極秘･社外秘など）によって分類されていないと、権限のない者から情報が漏えいする可能性がある。	○		3	情報の所在を管理する手順を定め、文書化し実行する。
	17	■システム受入れ管理 コンピュータシステムの受入れ基準を定め管理する。	受入れたシステムの不備に気付かず稼動し、又はネットワークに接続すると、不具合が発生する可能性がある。	○		3	テスト仕様書を作成し、実際に使用するデータによってテストを行う。
	18	■運用体制 社員または社員以外の組織に運用させる場合の管理方法を定める。	情報システムの運営を部外者に行わせる場合、管理基準がないと、情報が漏えいする。	○		2	運用操作ログや機器、情報の操作履歴を記録、保管する手順を定め、文書化し実行する。
	19	■情報漏えい時の対策体制 情報漏えいが発生した場合の手順、組織を定める。	漏えい事故などが発生した場合の管理体制が決まっていないと、対応が遅れ被害が大きくなるおそれがある。	○		2	漏えい事故のレベルを想定し対策体制を文書化する。

特約条項：本告知事項は、業務要件定義書（○○○○年○○月○○日、第△版）に基づき、お客様が合意した内容であり、かかる合意の範囲外の脅威に対応するものではありません。

告知事項：*対応レベルは、経済産業省情報システム・モデル取引・契約書追補版セキュリティチェックシートに基づく、該当レベルを表示しています。**データのバックアップ作業はユーザの責任とします。バックアップがないことにより生じる損害についてベンダは負いませんので、十分ご注意ください。

＜告知事項＞要件定義によるセキュリィ仕様　(2)（記載例：B 又は C の業務要件定義に添付する）

	項番	対策内容	脅威の内容	実施担当			本件業務での対応
				ユーザ	ベンダ	対応レベル*	仕様もしくは候補製品等
Web システム 技術的セキュリティ対策(例)	20	■認証 情報を参照している人が本人なのかを証明をする。	情報を参照している人が、本人なのかを管理していないと、他人に重要な情報を見られる可能性がある。		○	2	利用者と管理者のアクセス権限の設定を実装する。
	21	■アクセス権 情報よって、アクセスできる人を制限・管理する。	誰でも情報アクセスできるようになっていると、削除、改ざん、複製、持ち出しされたりする。		○	3	個人情報に関わるものの暗号化を実装する。
	22	■暗号化 情報を暗号化して、紛失・盗聴・改ざんの対策をする。	通信経路やパスワードが暗号化されていない場合は、紛失･盗聴･改ざんや成りすましの可能性がある。	○		2	データの有効期限や取扱方法を部分的に定め文書化する。
	23	■ページ間のデータ授受 Web のページをまたがってデータのやり取りをする際の対策をする。	ページ間のデータ授受が正しくなされない場合は、情報が漏えいしたり、成りすましされたりする可能性がある。		○	2	悪意のあるコードを排除する仕組みを実装する。
	24	■悪意のあるコードの侵入阻止 悪意のあるコードが Web サーバに埋め込まれるのを阻止する。	悪意のあるコードが Web サーバ上で実行されると、フィッシング詐欺やユーザの成りすまし、パスワード漏えい等の可能性がある。		○	2	システム連携悪用を排除する仕組みを実装する。
	25	■システム連携 他のシステムや他のアプリケーションとの連携を行う際に連携の仕組みを悪用されるのを阻止する。	連携の仕組みを悪用されると、フィッシング詐欺やユーザの成りすまし、パスワードの漏えい等の可能性がある。		○	3	Web サーバの設定がセキュリティを意識した設定にし、設定内容を文書化する。
	26	■Web サーバの設定 Web サーバの設定内容について、最適な設定がされているか。	Web サーバの設定が正しく設定されていない場合、攻撃のために必要とするシステム情報が漏えいする。	○		2	運用手順を文書化し、条件付で Web サーバの運用について規約を設定する。
	27	■内因的な情報漏えい 運用ミスなど内部側の原因で情報が漏えいする。	重要な情報が漏えいし、又は攻撃のために必要とする情報が漏えいする可能性がある。		○	2	アプリケーションへの攻撃に対する暫定的な対策を施す。
	28	■アプリケーションへの攻撃対策 機能の悪用、負荷攻撃、多重登録等のアプリケーションに対する攻撃対策。	アプリケーションに対する攻撃により、サービスの停止や情報漏えい、改ざん、踏み台化などの可能性がある。		○	3	サーバが乗っ取られない為の対策を実装する。
	29	■ネットワーク構成 ネットワークの構成により、攻撃されやすさが変わる。	不適切な構成の場合、サーバの乗っ取りの可能性がある。		○	2	取引に関わる情報に誤りがないことを保証するための最低限の保全機能を実装する。
	30	■電子商取引 電子商取引におけるセキュリティ対策の実施。	取引に関係する情報が漏えい、改ざんされる可能性がある。		○	3	ログを取得し、定期的なレポートを行う。
	31	■ログ管理 情報の持ち出し履歴を取得し監査の証跡資料として管理する。	情報システムの監査ログが適切に管理されていないと不正な出来事に気付く事ができないおそれがある。		○	2	セキュリティに関するテストを文書化し定期的に実施する。

特約条項：本告知事項は、業務要件定義書（○○○○年○○月○○日、第△版）に基づき、お客様が合意した内容であり、かかる合意の範囲外の脅威に対応するものではありません。
告知事項：*対応レベルは、経済産業省情報システム・モデル取引・契約書追補版セキュリティチェックシートに基づく、該当レベルを表示しています。

D　外部設計支援業務契約の重要事項　(1)

■外部設計支援業務の概要（契約の内容となる具体的作業は、次頁以降に記載されています。）

【記載例】要件定義書、関連する文書等の仕様及び表記の体制に基づき、画面・帳票、インターフェース等に関わる外部設計書の作成支援を行います。これには、ユーザインターフェースや他のシステムと取り交わすデータ種類やフォーマットの設計が含まれる場合があります。外部設計に必要となる事項の明確化又は内容の確認等を行うため、お客様と合同で外部設計検討会を開催し、外部設計書の作成支援業務を実施します。外部設計書の作成を完了した場合、お客様によって決定事項に適合するか点検・承認を頂きます。

■契約類型：準委任契約

■個別契約条項

1．個別契約の成立

ユーザは、ベンダに対し、本重要事項説明書の具体的作業内容に記載された業務（以下「本件業務」といいます。）の提供を依頼し、ベンダは、これを引き受けました。本件業務の内容、日程、代金（代金の支払方法を含みます。）、各当事者の具体的な義務等の取引条件については、システム基本契約書、本重要事項説明書の具体的作業内容及び本個別契約条項の記載に従います。

2．機器等の売買等

ユーザは、本契約（システム基本契約書と個別契約書としての本重要事項説明書から構成されます。以下同じ。）に基づきユーザに納入される本件システム（ソフトウェア、ハードウェア等を含みます。）に関し、本件業務の提供を受けるにあたり、ベンダ又は第三者からソフトウェア、ハードウェア等(以下「機器等」といいます。)を購入し、又は借り入れる場合があります。当該購入又は借入れの契約条件については、本契約とは別個に締結される契約が本契約に優先して適用されるものとし、ベンダは、ベンダが契約当事者となる当該別契約に別段の定めのない限り、機器等の固有の瑕疵について責任を負いません。

3．ベンダの善管注意義務

ベンダは、情報処理技術に関する業界の一般的な専門知識及びノウハウに基づき、ユーザの作業が円滑かつ適切に行われるよう、善良な管理者の注意をもって、本契約に基づく調査、分析、整理、提案及び助言などの支援業務を行うものとします。

4．業務終了の確認

1)　ベンダは、本重要事項説明書に記載された期限までに、業務完了報告書兼外部設計書承認依頼書を作成し、ユーザに提出します。

2)　ユーザは、本重要事項説明書に定める期間（以下「点検期間」といいます。）内に、前項の業務報告書の点検を行うものとします。

3)　ユーザは、第１項の業務報告書の内容に異議がない場合には、業務完了確認書兼外部設計書承認書に記名押印してベンダに交付することで、本件業務の終了を確認するものとします。

4)　ユーザが、業務完了確認書兼外部設計書承認書に記名押印をしない場合であっても、点検期間内に書面で具体的な理由を明示して異議を述べないときは、点検期間の満了をもって本件業務の終了を確認したものとみなします。

■告知事項

1．内容や専門用語でご不明の点は随時ご質問頂き、十分にご精査ください。

2．システム基本契約書第 6 条に基づき、お客様から再委託の中止の請求を受けた場合は、作業期間、納期または委託料等の内容の変更がなされますので、ご注意ください。

D　外部設計支援業務契約の重要事項　(2)具体的作業内容	
1.要件定義 ○○○○年○○月○○日付け「△△△△システム」要件定義書第×版に基づく	
2．設計作業の体制及び方法 (1) 作業体制（受託者の体制、責任者、主任担当者、連絡窓口等） (2) 設計方法（設計工程、進捗管理及び報告、設計環境の貸与もしくは借用等） (3) 外部設計検討会（日程、場所、参加者、内容、変更管理手続等） (4) 委託先（委託先の概要、管理体制等） (5)期間：○○○○年○○月○○日～○○○○年○○月○○日	
5．未決事項	
6．付帯事項（作業を実施する場合の場所・期限等、要件の合意、承認ルールを含む）：	
7．特約条項：	
業務完了報告書及び外部設計書の提出期限：○○○○年○○月○○日	
上記報告書及び外部設計書に係る点検期間：提出日から○日間	
受託金額(税抜)もしくは受託金額の決定基準	損害賠償限度額：
支払期限：○○○○年○○月○○日	支払い方法：　現金・口座振込

D　外部設計支援業務契約の重要事項　(3)パッケージソフトウェアの表示（記入例）

項番	開発元・名称・型番・ バージョン・リビジョン等	保守及びサポート体制、使用許諾契約の内容	添付図書

D　外部設計支援業務契約の重要事項　(4)設計書、付属文書の一覧

項番	工程	設計書、文書名、概要	納期	承認方法

D　外部設計支援業務契約の重要事項の重要事項　(5)ソフトウェア、機器の明細及び納入場所及び別途締結する契約の表示

ソフトウェア、機器の明細一覧

項番	名称・型番・仕様・製造・開発元・提供会社等	単価	数量	価格（税抜）	納入日	納入先 稼働場所	無償保証の条件等*1		補修用性能部品（有償）の最低保有期間*1	取引・決済の形態、方法（リース・レンタル・売買）	別途締結する契約（売買契約、使用許諾契約等）
							無償保証期間	無償保守の条件等			
	合計金額（税抜）										

付帯事項：

特約条項：*1　○○○○年○○月○○日時点での内容であり、将来に向かって予告無く変更される場合があります。

E　ソフトウェア設計・制作業務契約の重要事項　(1)

■ソフトウェア設計・制作業務の概要（契約の内容となる具体的作業は、次頁以降に記載されています。）

【記載例】要件定義書及び外部設計書に基づくソフトウェアの開発（モディファイ、アドオン等のカスタマイズを含みます。）を行い、ソフトウェアをユーザに納入します。ベンダ出荷の際のテスト体制、テスト内容、テストで使用するデータの詳細を定めます。あせてお客様のデータをベンダ出荷テストで使用するかを定めます。

■契約類型：請負契約

■個別契約条項

1．個別契約の成立

ユーザは、ベンダに対し、本重要事項説明書の具体的作業内容に記載された業務（以下「本件業務」といいます。）の提供を依頼し、ベンダは、これを引き受けました。本件業務の内容、日程、代金（代金の支払方法を含みます。）、各当事者の具体的な義務等の取引条件については、システム基本契約書、本重要事項説明書の具体的作業内容及び本個別契約条項の記載に従います。

2．本件ソフトウェアの納入

1)　ベンダは、本重要事項説明書で定める期日までに、要件定義書及び外部設計書に基づきモディファイ、アドオン等のカスタマイズがなされたソフトウェア（以下「本件ソフトウェア」といいます。）を開発した上、本重要事項説明書で定める納入物（以下「納入物」といいます。）をユーザに対し納品書兼検収依頼書とともに納入します。

2)　ベンダは、納入物のユーザに対する納入に先立ち、本重要事項説明書で定める適格性（出荷）テスト条件に基づき、検査を行い、出荷合格を確認するものとします。

3)　ベンダは、納入物の適格性（出荷）テスト条件に基づく検査及び納入に際し、ユーザに対して必要な協力を要請できるものとし、ユーザは、ベンダから協力を要請された場合には、すみやかにこれに応じるものとします。

3．本件ソフトウェアの検収

1)　ユーザは、納入物を本重要事項説明書に定める期間（以下「テスト期間」といいます。）内に前条第 2 項の適格性（出荷）テスト条件に基づき検査し、要件定義書及び外部設計書及びこれらに関連する文書と本件ソフトウェアが合致するか否かを検査しなければなりません。

2)　ユーザは、納入物が前項の検査に合格する場合、検査合格通知書兼検収書に記名押印の上、ベンダに交付するものとします。納入物が前項の検査に合格しない場合、ユーザはベンダに対し不合格となった具体的な理由を明示した書面を速やかに交付し、修正又は追完を求めるものとし、不合格理由が認められるときには、ベンダは、協議の上定めた期限内に無償で修正してユーザに納入し、ユーザは必要となる範囲で、前項所定の検査を再度行うものとします。

3)　検査合格通知書兼検収書が交付されない場合であっても、テスト期間内にユーザが書面で具体的な理由を明示して異議を述べない場合は、納入物は、テスト期間の満了日に本条所定の検査に合格したものとみなされます。

4)　本条所定の検査の合格をもって、本件ソフトウェアの検収完了とします。

4．機器等の売買等

ユーザは、本契約（システム基本契約書と個別契約書としての本重要事項説明書から構成されます。以下同じ。）に基づきユーザに納入される本件システム（ソフトウェア、ハードウェア等を含みます。）に関し、本件業務の提供を受けるにあたり、ベンダ又は第三者からソフトウェア、ハードウェア等(以下「機器等」といいます。)を購入し、又は借り入れる場合があります。当該購入又は借入れの契約条件については、本契約とは別個に締結される契約が本契約に優先して適用されるものとし、ベンダは、ベンダが契約当事者となる当該別契約に別段の定めのない限り、機器等の固有の瑕疵について責任を負いません。

5．本件パッケージ固有の瑕疵

本契約及びこれに関連する契約に基づきユーザに納入されるソフトウェア、ハードウェア等のシステムの構築のためには、その中核を構成するものとして第三者が権利を有するソフトウェア、SaaS 及びもしくは ASP（以下あわせて「本件パッケージ」といいます。）が利用されます。ベンダは本件パッケージに関して、著作権その他の権利の侵害がないこと及び瑕疵のないことを保証するものではなく、何らの責任を負わないものとします。

6．本件ソフトウェアについての瑕疵担保

1)　第 4 条及び第 5 条が適用されることを前提に、本件ソフトウェアのテスト合格後、納入物について要件定義書及び外部設計書の仕様との不一致（バグを含みます。以下本条において「瑕疵」といいます。）が発見された場合、ユーザは、ベンダに対して当該瑕疵の修正を請求することができ、ベンダは、当該瑕疵を修正する

ものとします。但し、ベンダがかかる修正責任を負うのは、本重要事項説明書記載の瑕疵担保期間以内にユーザから請求された場合に限るものとします。

2) 前項にかかわらず、瑕疵が軽微であって、納入物の修正に過分の費用を要する場合、ベンダは前項所定の修正責任を負わないものとします。

3) 第 1 項の規定は、瑕疵がユーザの提供した資料等又はユーザの与えた指示によって生じたときは適用しません。但し、ユーザがその資料等又は指示が不適当であることを知りながら告げなかったときはこの限りではありません。

4) ベンダは、本契約のもとでテストが行われた時点における本件ソフトウェアに関してのみ、ユーザに対し、第 1 項本文に定める瑕疵担保責任を負うものとし、テスト時以降における本件ソフトウェアに関する問題（本件システムの構成要素がアップグレードされたことに起因する問題等を含みます。）については、保守業務にてその契約条件にした従って対応するものとします。

7. 危険負担

本契約の他に別段の定めがある場合を除き、納入物の滅失、毀損等の危険負担は、納入前についてはベンダが、納入後についてはユーザが、それぞれこれを負担するものとします。

8. 特許権等の帰属

1) 本件業務遂行の過程で生じた発明その他の知的財産又はノウハウ等（以下、あわせて「発明等」といいます。）に係る特許権その他の知的財産権（特許その他の知的財産権を受ける権利を含みます。但し、著作権は除きます。）、ノウハウ等に関する権利（以下、特許権その他の知的財産権、ノウハウ等に関する権利を総称して「特許権等」といいます。）は、当該発明等を行った者が属する当事者に帰属するものとします。

2) ベンダは、第 1 項に基づき特許権等を保有することとなる場合、ユーザに対し、ユーザが本契約に基づき本件ソフトウェアを本件システムにおいて使用するのに必要な範囲について、当該特許権等の通常実施権を許諾するものとします。なお、本件ソフトウェアに、本重要事項説明書において一定の第三者に使用せしめる旨を本重要事項説明書に特掲されたソフトウェア（以下「特定ソフトウェア」といいます。）が含まれている場合は、かかる掲載に従った第三者による当該ソフトウェアの使用についても同様とします。なお、かかる許諾の対価は、受託金額に含まれるものとします。

9. 著作権の帰属

1) 本件業務遂行の過程で生じた著作権(著作権法第 27 条及び第 28 条の権利を含みます。)は、ユーザ又は第三者が従前から保有していた著作物の著作権を除き、ベンダに帰属するものとします。

2) ベンダは、本件ソフトウェアに係る著作物のうち自己が著作権を持つもの及び前項に従って自己に帰属するものについて、ユーザに対し、ユーザが本件ソフトウェアを本件システムにおいて利用できるように利用許諾し、これについて著作者人格権を行使しません。なお、本件システムに、特定ソフトウェアが含まれている場合は、かかる掲載に従った第三者による当該ソフトウェアの利用についても同様とします。なお、かかる許諾の対価は、受託金額に含まれるものとします。

3) 本件ソフトウェアに係る著作物のうち第三者が著作権を持つもの（本件パッケージを含みますがこれに限りません。）の権利関係については、当該権利者とユーザとの間の契約条件に従います。

10. 知的財産権侵害の責任

1) 第 4 条及び第 5 条が適用されることを前提に、ユーザが本件ソフトウェアに関し第三者から著作権、特許権その他の産業財産権（以下、本条においてあわせて「知的財産権」といいます。）の侵害の申立てを受けた場合、ベンダは、システム基本契約書第 10 条の規定にかかわらず、当該申立てに関してユーザが第 2 項の措置をとった上で確定した判決又はベンダの同意のもとになされた和解によってユーザが支払うべきとされた損害賠償額及び合理的な弁護士費用を負担するものとします。但し、第三者からの申立てがユーザの帰責事由による場合、本件パッケージの固有の瑕疵による場合、本契約に優先する他の契約の対象となる機器等を原因とする場合はこの限りではなく、ベンダは一切責任を負わないものとします。

2) 前項所定の申立てがなされたときは、ユーザは、すみやかにベンダに書面による通知をなし、弁護士の選任、申立てに係る防御活動のすべてについての決定権限をベンダに与えなければなりません。

3) ベンダの責に帰すべき事由による知的財産権の侵害を理由として本件システムの将来に向けての使用が不可能となるおそれがある場合、ベンダは、ベンダの判断及び費用負担により、(ⅰ)権利侵害のない他の成果物との交換、(ⅱ)権利侵害している部分の変更、(ⅲ)継続使用のための権利取得のいずれかの措置を講じることができるものとします。

4) ベンダが本条第 1 項に基づき損害賠償額及び合理的な弁護士費用を負担するときは、システム基本契約書第 10 条は適用されないものとする。

■告知事項

1. 内容や専門用語でご不明の点は随時ご質問頂き、十分にご精査ください。
2. システム基本契約書第 6 条に基づき、お客様から再委託の中止の請求を受けた場合は、作業期間、納期または委託料等の内容の変更がなされますので、ご注意ください。

E　ソフトウェア設計・制作業務契約の重要事項　(2)具体的作業内容	
1．システム要件、プログラム仕様 ○○○○年○○月○○日付け「△△△△システム」システム要件定義書第×版及び○○○○年○○月○○日付け「△△△△システム」外部設計書第×版に基づきます。	
2．開発作業の体制及び方法 (1) 作業体制（受託者の体制、責任者、主任担当者、連絡窓口、変更管理体制等） (2) 開発方法（開発工程、進捗管理及び報告、開発環境の貸与又は借用等） (3) 委託先（委託先の概要、管理体制等） (4)期間：○○○○年○○月○○日～○○○○年○○月○○日	
3．ベンダにおける適格性（出荷）テスト条件 (1) テスト体制（出荷合格の体制（テスト実施主体、環境、責任者等）） (2) テスト内容、方式（出荷合格とする条件） (3) テストデータ（テストで使用するデータの詳細および作成主体、ユーザデータの使用の有無） (4)期間：○○○○年○○月○○日～○○○○年○○月○○日	
4．運用テスト仕様書（運用テスト計画、運用テスト仕様）の作成	
5．連絡協議会の実施要項及びユーザ・ベンダの責任者、主任担当者：	
6．未決事項	
7．付帯事項（作業を実施する場合の場所・期限等、要件の合意、承認ルールを含みます。）：	
8．特約条項：	
納期：○○○○年○○月○○日	テスト期間：○○○○年○○月○○日～○○○○年○○月○○日
瑕疵担保期間：	
受託金額(税抜) ：	損害賠償限度額：
支払期限：○○○○年○○月○○日	支払い方法：　現金・銀行口座振込

E　ソフトウェア設計・制作業務契約の重要事項　(3)パッケージソフトウェアの表示（記入例）			
項番	開発元・名称・型番・バージョン・リビジョン等	保守及びサポート体制、使用許諾契約、既知の不具合の内容	添付図書

E　ソフトウェア設計・制作業務契約の重要事項 (4)納入物の明細					
項番	工程	納入物（プログラム、設計書、文書名等）	納入形態・媒体	納期	個別承認事項がある場合の条件等

F　構築・設定業務契約の重要事項　(1)

■構築・設定業務の概要（契約の内容となる具体的作業は次頁以降に記載されています。）

【記載例】要件定義書、外部設計書、関連仕様書等に基づき指定された機器、ソフトウェア、ネットワークが要求どおり動作するよう設定を行います。お客様との取り決めによって、既設のシステムとのシステム結合の実施を業務に含む場合があり、また、システム結合の実施をした際に、他のシステムに障害が発生した場合の障害の切り分け（障害原因の調査と特定）を業務に含む場合があります。また、費用がＥソフトウェア設計・制作業務契約に含まれる場合は、構築・設定業務契約の重要事項(2)具体的作業内容で示します。現地調整において構築・設定に関わる仕様書と異なる設定に至った場合を含め、実際の設定を構築・設定業務設定報告書で報告します。

■契約類型：請負契約

■個別契約条項

1. 個別契約の成立

ユーザは、ベンダに対し、本重要事項説明書の具体的作業内容に記載された業務（以下「本件業務」といいます。）の提供を依頼し、ベンダは、これを引き受けました。本件業務の内容、日程、代金（代金の支払方法を含みます。）、各当事者の具体的な義務等の条件については、システム基本契約書、本重要事項説明書の具体的作業内容及び本個別契約条項の記載に従います。

2. 本件システムの納入

1)　ベンダは、本重要事項説明書で定める期日までに、本件システム（ソフトウェア、ハードウェア等を含み、詳細は本重要事項説明書で定めるとおりとします。）を構築・設定して、ユーザに対して構築・設定業務完了報告書兼検収依頼書（構築・設定業務報告書を含みます）及び納品書とともに納入します。

2)　ベンダは、本件システムの納入に際し、ユーザに対して必要な協力を要請できるものとし、ユーザは、ベンダから協力を要請された場合には、すみやかにこれに応じるものとします。

3. 本件システムの構築・設定についての検収

1)　ユーザは、納入された本件システムを本重要事項説明書に定める期間（以下「テスト期間」といいます。）内に本重要事項説明書で定める受入れテスト条件に基づき検査し、要件定義書、外部設計書、構築・設定業務設定報告書、関連する文書と本件システムが合致するか否かを検査しなければなりません。
2)　ユーザは、本件システムが前項の検査に合格する場合、検査合格通知書兼検収書に記名押印の上、ベンダに交付するものとします。また、ユーザは、本件システムが前項の検査に合格しない場合、ベンダに対し不合格となった具体的な理由を明示した書面を速やかに交付し、修正又は追完を求めるものとし、不合格理由が認められるときには、ベンダは、協議の上定めた期限内に無償で修正してユーザに納入し、ユーザは必要となる範囲で、前項所定の検査を再度行うものとします。
3)　検査合格通知書兼検収書が交付されない場合であっても、テスト期間内にユーザが書面で具体的な理由を明示して異議を述べない場合は、本件システムは、テスト期間の満了日に本条所定の検査に合格したものとみなされます。
4)　本条所定の検査の合格をもって、本件システムの検収完了とします。

4. 機器等の売買等

ユーザは、本契約（システム基本契約書と個別契約書としての本重要事項説明書から構成されます。以下同じ。）に基づきユーザに納入される本件システム（ソフトウェア、ハードウェア等を含みます。）に関し、本件業務の提供を受けるにあたり、ベンダ又は第三者からソフトウェア、ハードウェア等(以下「機器等」といいます。)を購入し、又は借り入れる場合があります。この場合、当該購入又は借入れの契約条件については、本契約とは別個に締結される契約が本契約に優先して適用されるものとし、ベンダは、ベンダが契約当事者となる当該別契約に別段の定めのない限り、機器等の固有の瑕疵について責任を負いません。

5. 本件パッケージ固有の瑕疵

本契約及びこれに関連する契約に基づきユーザに納入されるソフトウェア、ハードウェア等のシステムの構築のためには、その中核を構成するものとして第三者が権利を有するソフトウェア、SaaS 及びもしくは ASP（以下あわせて「本件パッケージ」といいます。）が利用されます。ベンダは本件パッケージに関して、著作権その他の権利の侵害がないこと及び瑕疵のないことを保証するものではなく、何らの責任を負わないものとします。

6. 本件システムについての瑕疵担保

1)　第 4 条及び第 5 条が適用されることを前提に、本件システムのテスト合格後、本件システムについて要件定義書、外部設計書又はこれに関連する文書等の仕様との不一致（バグを含みます。以下本条において「瑕疵」といいます。）が発見された場合、ユーザは、ベンダに対して当該瑕疵の修正を請求することができ、ベンダ

は、当該瑕疵を修正するものとします。但し、ベンダがかかる修正責任を負うのは、本重要事項説明書記載の瑕疵担保期間内にユーザから請求された場合に限るものとします。

2) 前項にかかわらず、瑕疵が軽微であって、納入物の修正に過分の費用を要する場合、ベンダは前項所定の修正責任を負わないものとします。

3) 第１項の規定は、瑕疵がユーザの提供した資料等又はユーザの与えた指示によって生じたときは適用しません。但し、ユーザがその資料等又は指示が不適当であることを知りながら告げなかったときはこの限りではありません。

4) ベンダは、本契約のもとでテストが行われた時点における本件システムに関してのみ、ユーザに対し、第１項本文に定める瑕疵担保責任を負うものとし、テスト時以降における本件システムに関する問題（本件システムの構成要素がアップグレードされたことに起因する問題等）については、保守業務にてその契約条件に従って対応するものとします。

7. 危険負担

本契約の他に別段の定めがある場合を除き、納入物の滅失、毀損等の危険負担は、納入前についてはベンダが、納入後についてはユーザが、それぞれこれを負担するものとします。

8. 特許権等の帰属

1) 本件業務遂行の過程で生じた発明その他の知的財産又はノウハウ等（以下、あわせて「発明等」といいます。）に係る特許権その他の知的財産権（特許その他の知的財産権を受ける権利を含みます。但し、著作権は除きます。）、ノウハウ等に関する権利（以下、特許権その他の知的財産権、ノウハウ等に関する権利を総称して「特許権等」といいます。）は、当該発明等を行った者が属する当事者に帰属するものとします。

2) ベンダは、第１項に基づき特許権等を保有することとなる場合、ユーザに対し、ユーザが本契約に基づき本件システムを使用するのに必要な範囲について、当該特許権等の通常実施権を許諾するものとします。なお、本件システムに、本重要事項説明書において一定の第三者に使用せしめる旨を本重要事項説明書に特掲されたソフトウェア（以下「特定ソフトウェア」といいます。）が含まれている場合は、かかる掲載に従った第三者による当該ソフトウェアの使用についても同様とします。なお、かかる許諾の対価は、受託金額に含まれるものとします。

9. 著作権の帰属

1) 本件業務遂行の過程で生じた著作権(著作権法第 27 条及び第 28 条の権利を含みます。)は、ユーザ又は第三者が従前から保有していた著作物の著作権を除き、ベンダに帰属するものとします。

2) ベンダは、本件システムに係る著作物のうち自己が著作権を持つもの及び前条に従って自己に帰属するものについて、ユーザに対し、ユーザが本件システムを本契約の条件に従って利用できるように利用許諾し、これについて著作者人格権を行使しません。なお、本件システムに、特定ソフトウェアが含まれている場合は、かかる掲載に従った第三者による当該ソフトウェアの利用についても同様とします。なお、かかる許諾の対価は、受託金額に含まれるものとします。

3) 本件システムに係る著作物のうち第三者が著作権を持つもの（本件パッケージを含みますがこれに限りません。）の権利関係については、当該権利者とユーザとの間の契約条件に従います。

10. 知的財産権侵害の責任

1) 第 4 条及び第 5 条が適用されることを前提に、ユーザが本件システムに関し第三者から著作権、特許権その他の産業財産権（以下、本条においてあわせて「知的財産権」といいます。）の侵害の申立を受けた場合、ベンダは、システム基本契約書第 10 条の規定にかかわらず、当該申立てに関してユーザが第２項の措置をとった上で確定した判決又はベンダの同意のもとになされた和解によってユーザが支払うべきとされた損害賠償額及び合理的な弁護士費用を負担するものとします。但し、第三者からの申立てがユーザの帰責事由による場合、本件パッケージの固有の瑕疵による場合、本契約に優先する他の契約の対象となる機器等を原因とする場合はこの限りではなく、ベンダは一切責任を負わないものとします。

2) 前項所定の申立てがなされたときは、ユーザはすみやかにベンダに書面による通知をなし、弁護士の選任、申立てに係る防御活動のすべてについての決定権限をベンダに与えなければなりません。

3) ベンダの責に帰すべき事由による知的財産権の侵害を理由として本件システムの将来に向けての使用が不可能となるおそれがある場合、ベンダは、ベンダの判断及び費用負担により、(ⅰ)権利侵害のない他の成果物との交換、(ⅱ)権利侵害している部分の変更、(iii)継続使用のための権利取得のいずれかの措置を講じることができるものとします。

4) ベンダが本条第１項に基づき損害賠償額及び合理的な弁護士費用を負担するときは、システム基本契約書第 10 条は適用されないものとする。

■告知事項

1. 内容や専門用語でご不明の点は随時ご質問頂き、十分にご精査ください。
2. システム基本契約書第 6 条に基づき、お客様から再委託の中止の請求を受けた場合は、作業期間、納期または委託料等の内容の変更がなされますので、ご注意ください。

F　構築・設定業務契約の重要事項　(2)具体的作業内容

項番	名称・型番	設置場所	仕様もしくは仕様書名 （設定内容、他システムとの結合の有無、障害発生時の切り分け作業、受入テスト条件等）	期間

関連するシステム、ネットワークの停止等の条件：

連絡協議会の実施要項及びユーザ・ベンダの責任者、主任担当者：	委託先（委託先の概要、管理体制等）

付帯事項：

特約条項：

構築･設定業務完了報告書（構築･設定業務報告書を含む）提出期限：〇〇〇〇年〇〇月〇〇日	テスト期間：〇〇〇〇年〇〇月〇〇日～〇〇〇〇年〇〇月〇〇日

受託金額：￥〇〇〇〇〇(税抜)　受託金額はソフトウェア設計・制作業務の受託金額に（含んでいます・含んでいません）	瑕疵担保期間：

支払期限：〇〇〇〇年〇〇月〇〇日	支払い方法：現金・銀行口座振込	損害賠償限度額：

F　構築・設定業務契約の重要事項　(3)本件システム構成図

（既存システム、既設機器及び本件システムの機器・ソフトウェア・ネットワーク構成等を含む）

F　構築・設定業務契約の重要事項　(4)ソフトウェア、機器の明細及び納入場所及び別途締結する契約の表示

ソフトウェア、機器の明細一覧

項番	名称・型番・仕様・製造・開発元・提供会社等	単価	数量	価格	納入日	納入先 稼働場所	無償保証の条件等*1		補修用性能部品（有償）の最低保有期間*1	取引・決済の形態、方法（リース・レンタル・売買）	別途締結する契約（売買契約、使用許諾契約等）
							無償保証期間	無償保守の条件等			
	合計金額（税抜）										

付帯事項：

特約条項：*1　○○○○年○○月○○日時点での内容であり、将来に向かって予告無く変更される場合があります。

G　データ移行支援業務契約の重要事項　(1)

■データ移行支援業務の概要（契約の内容となる具体的作業は次頁以降に記載されています。これらの作業には、ベンダの担当する作業とお客様にお願いする作業があります。）
【記載例】既存、既設のコンピュータシステムのデータを、新規に導入するコンピュータシステムに移行する業務を支援します。

■契約類型：準委任契約

■個別契約条項

1. 個別契約の成立
ユーザは、ベンダに対し、本重要事項説明書の具体的作業内容に記載された業務（以下「本件業務」といいます。）の提供を依頼し、ベンダは、これを引き受けました。本件業務の内容、日程、代金（代金の支払方法を含みます。）、各当事者の具体的な義務等の取引条件については、システム基本契約書、本重要事項説明書の具体的作業内容及び本個別契約条項の記載に従います。

2. 機器等の売買等
ユーザは、本契約（システム基本契約書と個別契約書としての本重要事項説明書から構成されます。以下同じ。）に基づきユーザに納入される本件システム（ソフトウェア、ハードウェア等を含みます。）に関し、本件業務の提供を受けるにあたり、ベンダ又は第三者からソフトウェア、ハードウェア等(以下「機器等」といいます。)を購入し、又は借り入れる場合があります。当該購入又は借入れの契約条件については、本契約とは別個に締結される契約が本契約に優先して適用されるものとし、ベンダは、ベンダが契約当事者となる当該別契約に別段の定めのない限り、機器等の固有の瑕疵について責任を負いません。

3. ベンダの善管注意義務
ベンダは、情報処理技術に関する業界の一般的な専門知識及びノウハウに基づき、ユーザによる本件システムへのデータ移行が円滑かつ適切に行われるよう、善良な管理者の注意をもって、ユーザによるデータ移行について支援業務を行うものとします。

4. 業務終了の確認
1)　ベンダは、本重要事項説明書に記載された期限までに、業務完了報告書兼検収依頼書を作成し、ユーザに提出します。
2)　ユーザは、本重要事項説明書に定める期間（以下「点検期間」といいます。）内に、前項の業務報告書の点検を行うものとします。
3)　ユーザは、第１項の業務報告書の内容に異議がない場合には、業務完了確認書兼検収書に記名押印してベンダに交付することで、本件業務の終了を確認するものとします。
4)　ユーザが、業務完了確認書兼検収書に記名押印をしない場合であっても、第 1 項の業務終了報告書提出から〇日以内に書面で具体的な理由を明示して異議を述べないときは、点検期間の満了をもって本件業務の終了を確認したものとみなします。

■ 告知事項

1. データ移行においては、ユーザとベンダの協働が必須であり、各実施作業においてお客様による作業が必須となります。お客様とベンダの作業の分担、内容、期間、費用については十分精査の上、ご承認をお願い申し上げます。

2. 移行するデータの範囲の決定、データ抽出においては、現行システムの十分な事前調査と、作業に応じたデータのバックアップ、システムの停止等が必要となる場合があります。データのバックアップ作業は原則としてお客様に実施をお願い申し上げます。また、場合によっては、新たに機器、ソフトウェアの設定、変更、設計、制作、導入が伴います。

3. 移行のためのデータの変換、新システムへの移行においては、お客様自身によるデータの正誤判定や精査が必要となる場合があります。場合によっては、新たに機器、ソフトウェアの設定、変更、設計、制作、導入が伴います。

4. 内容や専門用語でご不明の点は随時ご質問頂き、十分にご精査ください。

G　データ移行支援業務の重要事項　(2)具体的作業内容

移行するデータの範囲	ユーザ管理者	会社名				現況システム詳細	
		所属					
		氏名					
		連絡先					
	設置場所、保存形態	項番	設置場所	Server 名/媒体	フォーマット/データ形式/文字コード	ボリューム名/ファイル名	内容/アクセス制御等

連絡協議会の実施要項及びユーザ・ベンダの責任者、主任担当者：

付帯事項（作業を実施する場合の場所・期限等、要件の合意、承認ルールを含みます。）：

特記事項：

移行のための抽出作業	ユーザ管理者	会社名		ベンダ担当者	会社名	
		所属			所属	
		氏名			氏名	
		連絡先			連絡先	
	期間	○○○○年○○月○○日～○○月○○日	業務完了報告書提出日並びにその点検期間：			
	項番	作業内容（ユーザ、ベンダの役割分担を含みます。）			作業仕様書名、実施詳細	

連絡協議会の実施要項及びユーザ・ベンダの責任者、主任担当者：

付帯事項：（作業を実施する場合の場所・期限等、要件の合意、承認ルールを含みます。）：

特約条項：

受託金額(税抜)もしくは受託金額の決定基準	損害賠償限度額：
支払期限：	支払い方法：現金・銀行口座振込

G データ移行支援業務の重要事項　(3)具体的作業内容

移行のための変換作業	ユーザ管理者	会社名		ベンダ担当者	会社名	
		所属			所属	
		氏名			氏名	
		連絡先			連絡先	
	期間	○○○○年○○月○○日～○○月○○日	業務完了報告書提出日並びにその点検期間：			
	項番	作業内容作業内容（ユーザ、ベンダの役割分担を含みます。）			作業仕様書名、実施詳細	

連絡協議会の実施要項及びユーザ・ベンダの責任者、主任担当者：
付帯事項：（作業を実施する場合の場所・期限等、要件の合意、承認ルールを含みます。）：
特約条項：

受託金額(税抜)もしくは受託金額の決定基準	損害賠償限度額：
支払期限：	支払い方法：現金・銀行口座振込

新システムへの移行	ユーザ管理者	会社名		ベンダ担当者	会社名	
		所属			所属	
		氏名			氏名	
		連絡先			連絡先	
	期間	○○○○年○○月○○日～○○月○○日	業務完了報告書提出日並びにその点検期間：			
	項番	作業内容作業内容（ユーザ、ベンダの役割分担を含みます。）			作業仕様書名、実施詳細	

連絡協議会の実施要項及びユーザ・ベンダの責任者、主任担当者：
付帯事項：（作業を実施する場合の場所・期限等、要件の合意、承認ルールを含みます。）：
特約条項：

受託金額(税抜)もしくは受託金額の決定基準	損害賠償限度額：
支払期限：	支払い方法：現金・銀行口座振込

H 運用テスト支援業務契約の重要事項　(1)

■運用テスト支援業務の概要（契約の内容となる具体的作業は次頁以降に記載されています。これらの作業には、ベンダの担当する作業とお客様にお願いする作業があります。）
【記載例】運用にかかわる作業手順の策定及び作業手順に基づくテスト仕様書の策定を支援します。テスト仕様書に基づき、プログラムが正常に動作しているかの合否判定作業を支援します。

■契約類型：準委任契約

■個別契約条項

1. 契約の成立
ユーザは、ベンダに対し、本重要事項説明書の具体的作業内容に記載された業務（以下「本件業務」といいます。）の提供を依頼し、ベンダは、これを引き受けました。本件業務の内容、日程、代金（代金の支払方法を含みます。）、各当事者の具体的な義務等の取引条件については、システム基本契約書、本重要事項説明書の具体的作業内容及び本個別契約条項の記載に従います。

2. 機器等の売買等
ユーザは、本契約（システム基本契約書と個別契約書としての本重要事項説明書から構成されます。以下同じ。）に基づきユーザに納入される本件システム（ソフトウェア、ハードウェア等を含みます。）に関し、本件業務の提供を受けるにあたり、ベンダ又は第三者からソフトウェア、ハードウェア等(以下「機器等」といいます。)を購入し、又は借り入れる場合があります。当該購入又は借入れの契約条件については、本契約とは別個に締結される契約が本契約に優先して適用されるものとし、ベンダは、ベンダが契約当事者となる当該別契約に別段の定めのない限り、機器等の固有の瑕疵について責任を負いません。

3. ベンダの善管注意義務
ベンダは、情報処理技術に関する業界の一般的な専門知識及びノウハウに基づき、ユーザによるテストが円滑かつ適切に行われるよう、善良な管理者の注意をもって、ユーザによるテストの実施について支援業務を行うものとします。

4. 業務終了の確認
1)　ベンダは、本重要事項説明書に記載された期限までに、業務完了報告書兼検収依頼書を作成し、ユーザに提出します。
2)　ユーザは、本重要事項説明書に定める期間（以下「点検期間」といいます。）内に、前項の業務報告書の点検を行うものとします。
3)　ユーザは、第１項の業務報告書の内容に異議がない場合には、業務完了確認書兼検収書に記名押印してベンダに交付することで、本件業務の終了を確認するものとします。
4)　ユーザが、業務完了確認書兼検収書に記名押印をしない場合であっても、第 1 項の業務終了報告書提出から〇日以内に書面で具体的な理由を明示して異議を述べないときは、点検期間の満了をもって本件業務の終了を確認したものとみなします。

■ 告知事項

1. 運用テスト支援業務遂行においては、ユーザとベンダの協働が必須であり、各実施作業においてお客様による作業が必須となります。お客様とベンダの作業の分担、内容、期間、費用については十分精査の上、ご承認をお願い申し上げます。

2. テスト仕様策定、実施にあたっては、お客様自身によるテストシナリオの検証、テストデータの入力と出力結果の合否判定、画面遷移や出力帳票等の確認、精査等が必要です。最終結果についてはお客様ご自身で合否判定くださるようお願い申し上げます。

3. 内容や専門用語でご不明の点は随時ご質問頂き、十分にご精査ください。

H 運用テスト支援業務契約の重要事項　(2)具体的作業内容

ユーザ管理者	会社名		ベンダ担当者	会社名	
	所　属			所　属	
	氏　名			氏　名	
	連絡先			連絡先	

■運用にかかわる作業手順の策定（作業内容及びユーザとベンダの役割分担）

報告書の提出期限並びに報告書の点検期間：

■テスト仕様書の策定（作業内容及びユーザとベンダの役割分担）

報告書の提出期限並びに報告書の点検期間：

■運用テスト支援概要	項番	システム名称	作業場所	期間	支援内容 （ユーザとベンダの役割分担）	テスト仕様書 （日付、作成者、版等）

連絡協議会の実施要項及びユーザ・ベンダの責任者、主任担当者：

付帯事項：（作業を実施する場合の場所・期限等、要件の合意、承認ルールを含みます。）：

特約条項：

業務完了報告書提出期限：〇〇〇〇年〇〇月〇〇日	左記報告書の点検期間：提出日から〇日間	損害賠償限度額：

受託金額(税抜もしくは受託金額の決定基準：	支払期限：	支払方法：現金・銀行口座振込

Ⅰ 導入教育支援業務契約の重要事項 (1)

■導入教育支援業務の概要（契約の内容となる具体的作業は次頁以降に記載されています。これらの作業には、ベンダの担当する作業とお客様にお願いする作業があります。）
【記載例】実施内容に基づき操作、運用方法等の教育を実施します。

■契約類型：準委任契約

■個別契約条項

1. 個別契約の成立
ユーザは、ベンダに対し、本重要事項説明書の具体的作業内容に記載された業務（以下「本件業務」といいます。）の提供を依頼し、ベンダは、これを引き受けました。本件業務の内容、日程、代金（代金の支払方法を含みます。）、各当事者の具体的な義務等の取引条件については、システム基本契約書、本重要事項説明書の具体的作業内容及び本個別契約条項の記載に従います。

2. 機器等の売買等
ユーザは、本契約（システム基本契約書と個別契約書としての本重要事項説明書から構成されます。以下同じ。）に基づきユーザに納入される本件システム（ソフトウェア、ハードウェア等を含みます。）に関し、本件業務の提供を受けるにあたり、ベンダ又は第三者からソフトウェア、ハードウェア等(以下「機器等」といいます。)を購入し、又は借り入れる場合があります。当該購入又は借入れの契約条件については、本契約とは別個に締結される契約が本契約に優先して適用されるものとし、ベンダは、当該別契約に別段の定めのない限り、機器等の固有の瑕疵について責任を負いません。

3. ベンダの善管注意義務
ベンダは、情報処理技術に関する業界の一般的な専門知識及びノウハウに基づき、本件システム導入に関するユーザによる利用者に対する教育が円滑かつ適切に行われるよう、善良な管理者の注意をもって、ユーザによる導入教育について支援業務を行うものとします。

4. 業務終了の確認
1) ベンダは、本重要事項説明書に記載された期限までに、業務完了報告書兼検収依頼書を作成し、ユーザに提出します。
2) ユーザは、本重要事項説明書に定める期間（以下「点検期間」といいます。）内に、前項の業務報告書の点検を行うものとします。
3) ユーザは、第１項の業務報告書の内容に異議がない場合には、業務完了確認書兼検収書に記名押印してベンダに交付することで、本件業務の終了を確認するものとします。
4) ユーザが、業務完了確認書兼検収書に記名押印をしない場合であっても、第 1 項の業務終了報告書提出から〇日以内に書面で具体的な理由を明示して異議を述べないときは、点検期間の満了をもって本件業務の終了を確認したものとみなします。

■告知事項
内容や専門用語でご不明の点は随時ご質問頂き、十分にご精査ください。

Ⅰ　導入教育支援業務契約の重要事項　(2)具体的作業内容	
概要	
日程	○○○○年○○月○○日○○時○○分　～　○○○○年○○月○○日○○時○○分
実施場所	
実施対象人員	
実施方法及び実施内容	（集合、個別、E-learning）
目指すべき水準	

付帯事項：（実施場所の立入・提供・貸与・期限等、要件の合意、承認ルール、作業実施にあたりユーザが担当する作業等）
連絡協議会の実施要項及びユーザ・ベンダの責任者、主任担当者：
特約条項：

業務完了報告書提出期限：○○○○年○○月○○日	左記報告書の点検期間：提出日から○日間
受託金額(税抜)もしくは受託金額の決定基準	損害賠償限度額：
支払期限：○○○○年○○月○○日	支払方法：現金・銀行口座振込

J　保守業務契約の重要事項　(1)

■保守業務の概要（契約の内容となる具体的作業は次頁以降に記載されています。これらの作業には、ベンダの担当する作業とお客様にお願いする作業があります。）
【記載例】お客様との合意に基づき障害の訂正、性能等の改善を行うため納入後のシステム、ソフトウェア製品の修正等を実施します。

■契約類型：準委任契約

■個別契約条項

1. 個別契約の成立
ユーザは、ベンダに対し、保守業務として本重要事項説明書の具体的作業内容に記載された業務（以下「本件業務」といいます。）の提供を依頼し、ベンダは、これを引き受けました。本件業務の内容、日程、代金（代金の支払方法を含みます。）、各当事者の具体的な義務等の取引条件については、システム基本契約書、本重要事項説明書の具体的作業内容及び本個別契約条項の記載に従います。

2. 本件業務（保守業務）の範囲
1)　本契約に別段の定めがない限り、本件業務とは、本件システムの引渡し後に発見された本件システム（但し、本件システムを構築するために利用されたパッケージソフトウェア、SaaS および／もしくは ASP、他者との別個の契約に基づく購入もしくはリースされたソフトウェア･ハードウェアを除きます。）の不良や不具合を修正する業務（是正保守）で本重要事項書に記載されたものをいいます。
2)　データのバックアップ作業はユーザの責任とします。バックアップがない事により生じる損害について、ベンダは責任を負いません。
3)　本契約に別段の定めがない限り、本件システムをあらゆる環境の変化に対応させる業務（適応保守）、本件システムの性能又は保守性を改善する業務（完全化保守）及び引渡後本件システムに潜在的な不具合が顕在化する前に発見し修復する業務（予防保守）は、本件業務に含まれません。

3. サービスの範囲
ベンダは、ユーザに対し、別途定めるサービス仕様書に基づき保守業務に係るサービスの内容を定めるものとします。

4. 設置場所への立ち入り等
ユーザは、ベンダに対し、保守業務を行うためにベンダが本件システムの設置場所に立ち入ることを認めます。また、ユーザは、ベンダに対し、ベンダが保守業務を行うために必要となる作業場所及び消耗品を無償にて提供するものとします。

5. 遠隔操作によるサービス
本重要事項説明書でベンダとユーザが合意するときは、ベンダは、ユーザに対し、遠隔操作による保守業務を行います。

6. 製造打切り、保守部品提供の中止の際の取扱い
1)　ベンダは、本件システムを構成するハードウェアの製造会社（以下「ハードウェアメーカー」といいます。）が以下の行為を行った場合、ユーザに対し、当該ハードウェア自体をユーザの費用負担にて交換することを請求することができます。(1)ハードウェアメーカーが本件システムを構成するハードウェアの製造を打ち切り、その後 5 年が経過した場合、又は(2)ハードウェアメーカーが本件システムを構成する保守部品の提供を中止した場合
2)　ユーザがベンダの請求後 90 日以内に前項のハードウェア自体の交換を行わない場合、ベンダは、当該ハードウェアを保守業務の対象から外すことができます。

7. 老朽化装置の取扱い
ベンダは、本件システムを構成するハードウェアの保守部品がハードウェアメーカーの定める耐久期間を超えたことにより本件システムの正常な運用の維持が不可能であると判断した場合、ユーザに対し、当該保守部品をユーザの費用負担にて交換することを請求することができます。ユーザが当該要求後 90 日以内に交換を行わない場合、ベンダは、当該保守部品をハードウェア保守業務の対象から外すことができます。

8. ソフトウェアのサポート打ち切り等の取り扱い
１）ベンダは、本件システムを構成するソフトウェアの製造会社が、本件システムを構成するソフトウェアのサポートを中止した場合、当該ソフトウェア自体の安定稼働及び保守の継続について検討の上、保守の継続が困難になるおそれがある場合、ユーザに対しその内容を提示の上、保守契約の見直しをユーザと交渉することができます。
2) ユーザは、ベンダの請求に応じて、30 日以内に契約条件の見直し交渉に応じるものとします。

9. 交換部品の所有権
ユーザは、保守業務の履行に伴い交換された部品の権利をベンダに無償で譲渡します。

10. 秘密保持
ベンダは、保守業務の履行に伴い、前条の交換された部品に記憶されているユーザの情報をシステム構築契約書第７条に定める秘密情報として取り扱うものとします。

11. 設置場所の変更
ユーザは、予め通知した本件システムの設置場所を変更する場合、ベンダに対し、変更後の設置場所及び変更日を変更の 30 日前までに書面により通知するものとします。

12. 設置場所の整備
ユーザは、保守業務の対象となる本件システムを構成するハードウェアのハードウェアメーカーが定める使用環境条件（入力電源、温湿度、塵埃、振動、電界及び磁界、接地条件、対象製品に有害な塩基及び有酸ガス、メンテナンスエリア等）を本件システムの設置場所において常に整備し、維持するものとします。

13. 不具合の調査費用
1) 保守業務の対象となる本件システムを構成するハードウェア、ソフトウェアに不具合が生じた場合、当該不具合に対する調査費用は、原則として保守サービス料金に含まれるものとします。
2) 前項にかかわらず、当該不具合がユーザの帰責事由により発生したことが判明した場合、又は保守業務の対象となる本件システムを構成しないハードウェア、ソフトウェアが原因で保守業務の対象となる本件システムを構成するハードウェア、ソフトウェアに不具合が生じた場合の調査費用は、別途ユーザが負担します。

14. 使用地域の制限
ユーザは、本件システムを日本国内においてのみ使用するものとします。

15. 本件パッケージ固有の瑕疵担保責任
ベンダは、本件パッケージの固有の瑕疵については保守業務を行いません。ユーザは、本件パッケージの固有の瑕疵及び保守については、本件パッケージの使用許諾書に従うものとします。

16. 有効期間
本契約の有効期間は、契約締結の時から 1 年間とします。但し、期間満了１ヶ月前までにベンダ及びユーザのいずれからも書面による申出がない場合には、保守業務の対象となる本件システムを構成するハードウェアの部品が市場において供給される限り、更に１年間延長するものとし、その後も同様とします。

17. 支払い遅延
ユーザが代金債務の支払を怠った場合、ベンダは、ユーザに対し、当該遅延日以降の保守業務を行う義務はありません。

■告知事項

1. 内容や専門用語でご不明の点は随時ご質問頂き、十分にご精査ください。

2. データのバックアップ作業はお客様の責任であり、特別の定めがない限りバックアップがない事により生じる損害について、ベンダは責任を負いませんので、十分にご注意ください。

J　保守業務契約の重要事項　(2)ハードウェア保守＜記入例＞

項番	保守サービス名称 業務内容	設置場所	サービス料金 （円／年、税抜）	請求方法及び 支払方法	請求開始 年月日	サービス期間		遠隔操作保守の有無	添付図書名	SLA 合意書有無
						開始日	終了日			
1	ハードウェア保守サービス （サーバ保守）	東京都千代田区 ○○-○○	¥○○○,○○○	年額一括 銀行口座自動引落	○○○○年 ○○月○○日	○○○○年 ○○月○○日	○○○○年 ○○月○○日	有り	保守対象機器明細一覧表	有り
2	ハードウェア保守サービス （クライアント PC 及び周辺機器保守）	東京都千代田区 ○○-○○	¥○○○,○○○	年額一括 銀行口座自動引落	○○○○年 ○○月○○日	○○○○年 ○○月○○日	○○○○年 ○○月○○日	無し	保守対象機器明細一覧表	有り
3	ハードウェア保守サービス （ネットワーク機器保守）	東京都千代田区 ○○-○○	¥○○○,○○○	年額一括 銀行口座自動引落	○○○○年 ○○月○○日	○○○○年 ○○月○○日	○○○○年 ○○月○○日	有り	保守対象機器明細一覧表	有り
4	ハードウェア保守サービス （プリンタ保守）	東京都千代田区 ○○-○○	¥○○○,○○○	年額一括 銀行口座自動引落	○○○○年 ○○月○○日	○○○○年 ○○月○○日	○○○○年 ○○月○○日	無し	保守対象機器明細一覧表	有り

受託金額合計（税抜）	損害賠償限度額：（項番ごとに記載）
付帯事項：（作業実施にあたりユーザが担当する作業）	遠隔操作保守の内容：（項番ごとに記載） 項番 1：遠隔操作保守は原則、接続毎にお客様の許可を得て実施します。夜間等で緊急の措置が必要な場合の対応については、SLA 合意書で定めます。 項番 3：ルーター、ファイアウォールの状態監視は 1 時間毎とし、異常発生時は、お客様の事前の許可無く外部接続で、障害範囲及び原因の特定、復旧などの 1 次保守を実施します。遠隔操作保守で対応できない場合は、SLA 合意書に基づきオンサイト保守を実施します。
連絡協議会の実施要項及びユーザ・ベンダの責任者、主任担当者：	
特約条項：	再委託先の表示：

J　保守業務契約の重要事項　(3)アプリケーションソフト保守＜記入例＞

項番	保守サービス名称 業務内容	設置場所	サービス料金 （円／年、税抜）	請求方法及び 支払方法	請求開始 年月日	サービス期間		遠隔操作保守の有無	添付図書名	SLA 合意書有無
						開始日	終了日			
1	アプリケーションソフト保守サービス （XX 社販売管理システム保守）	東京都千代田区 ○○-○○	¥○○○,○○○	年額一括 銀行口座自動引落	○○○○年 ○○月○○日	○○○○年 ○○月○○日	○○○○年 ○○月○○日	有り	ｘｘ社販売管理システム保守仕様書	有り

受託金額合計（税抜）	損害賠償限度額：（項番ごとに記載）
付帯事項：（作業実施にあたりユーザが担当する作業）	遠隔操作保守の内容：（項番ごとに記載） 項番 1：遠隔操作保守は、原則、接続毎にお客様の許可を得て、作業内容についてご承認の上、実施します。マスタおよびデータファイルについては、お客様の責任によるバックアップをお願い申し上げます。夜間及び緊急時の対応については、SLA 合意書で定めます。リモート保守で対応できない場合は、SLA 合意書に基づきオンサイト保守を実施します。
連絡協議会の実施要項及びユーザ・ベンダの責任者、主任担当者：	
特約条項：	再委託先の表示：

保守対象機器明細一覧表 （サーバ・クライアント・周辺機器・ネットワーク機器・プリンタ）＜記入例＞

項番	型番・仕様・製造・開発元・提供会社等	設置場所	数量	保守料金（円／年）		請求開始年月日	サービス期間		保守部品提供期限	保守の範囲及び条件	無償保証の条件等（例：設置環境）	製品特性・耐久性等の特記事項・他
				単価(税抜)	金額（税抜）		開始年月日	終了年月日				
1		東京都千代田区○○-○○		￥○○○,○○○	￥○○○,○○○	○○○○年○○月○○日	○○○○年○○月○○日	○○○○年○○月○○日				
2												
3												
4												
5												
6												
7												
8												
9												
10												
11												
12												

付帯事項：（作業実施にあたりユーザが担当する作業）
遠隔操作保守の内容：（項番ごとに記載）
特約条項：

SLA 合意書（記入例）

項番	保守・運用サービス名称	SLA/SLM 項目名	項目の説明	測定条件又は方法	測定単位	目標／保証	値	保守対象機器明細項番
1	ハードウェア保守サービス（サーバ・ルータ：製品名）	サービス提供時間	電話受付時間	コールセンターでの電話受付時間	時間	目標	平日：9 時～19 時、土：9 時～17 時、日・祝日：休み	
2			平均出動時間	電話を受けてから技術者が現地に到着するまでの時間（遠隔地は除く。）	月平均	目標	2 時間	
3			平均復旧時間	技術者が訪問してからハードウェアが工場出荷状態に戻るまでの四半期平均時間	四半期平均時間	目標	12 時間	
4			定期点検	定期点検月に障害が発生し訪問したときは、同時に定期点検を行うことがある。	回数	保証	年 2 回	
5	ハードウェア保守サービス（クライアント・プリンタ：製品名）	サービス提供時間	電話受付時間	コールセンターでの電話受付時間	時間	目標	平日：9 時～17 時、土日・祝日：休み	
6			出動時間	電話を受けてから技術者が現地に到着するまでの時間（遠隔地は除く。）	四半期平均時間	目標	24 時間	
7			平均復旧時間	技術者が訪問してからハードウェアが工場出荷状態に戻るまでの平均時間	四半期平均時間	目標	48 時間	
8			定期点検	定期点検月に障害が発生し訪問したときは、同時に定期点検を行うことがあります。	回数	保証	なし	
9	アプリケーション保守サービス（製品名）	コールセンター	電話受付時間	コールセンターでの電話受付時間	時間	目標	平日：9 時～17 時、土日・祝日：休み	
10			即応率	電話が鳴ってから基準時間内に応答した率	月平均	目標	90%以上	
11			放棄率	着信電話に出られなかった率	月平均	目標	10%未満	
12			電話ビジー率	電話がビジー（話中）でつながらなかった率	月平均	目標	10%未満	
13			コールバック率	即答できずに折り返しをした率	月平均	目標	20%未満	
14		ライセンス保守	バージョンアップサイクル	バージョンアップ回数を規定	年	目標	1 回／年	
15			バージョンアップ範囲	当該アプリケーション保守範囲でのバージョンアップ		保証	マイナーバージョンアップ	
16			媒体要求	バージョンアップ媒体の要求方法		目標	ユーザからのリクエスト	
17			着手時間(瑕疵時)	障害の報告を受けてからメーカーに報告するまでの時間	月平均時間	目標	3 時間以内	
18			復旧時間	障害報告を受けてから障害が回復するまでの時間。（データ復旧は含まない）			メーカーとの保守契約による	
19		カスタマイズ保守	応答時間	障害報告を受けてから着手するかの有無を決定し回答するまでの時間	月平均時間	目標	24 時間以内	
20			復旧時間	障害報告を受けてから障害が回復するまでの時間。（データ復旧は含まない）	月平均時間	目標	3 営業日以内	
21			着手時間(瑕疵時)	障害の報告を受けてから作業を開始するまでの時間	月平均時間	目標	3 時間以内	
22			着手時間(追加要望時)	連絡協議会で対応を決定する				
23	SLM	連絡協議会	開催サイクル	連絡協議会を開催するサイクルを規定	四半期単位回数	目標	1 回／四半期	
24			開催時間	1 回当りの開催時間	平均時間	目標	2 時間以内	
25			参加人数	ユーザとベンダの最大参加人数を規定	1 回平均	目標	ユーザ：5 名ベンダ：5 名	
		SLA	ＳＬＡ報告サイクル	SLA 報告書の作成サイクルを規定	四半期	目標	1 回／四半期	
26			ＳＬＡ見直しサイクル	SLA の見直しのサイクルを規定	年	目標	1 回／年	
27			承認方法	SLA 実績、見直しなどをどの機関で承認するかを規定			連絡協議会	

K　運用支援業務契約の重要事項　(1)

■運用支援業務の概要（契約の内容となる具体的作業は次頁以降に記載されています。これらの作業には、ベンダの担当する作業とお客様にお願いする作業があります。）

【記載例】お客様との合意に基づきお客様のシステムの運用を支援するための業務を提供します。

■契約類型：準委任契約

■個別契約条項

1. 個別契約の成立
   ユーザは、ベンダに対し、本重要事項説明書の具体的作業内容に記載された業務（以下「本件業務」といいます。）の提供を依頼し、ベンダは、これを引き受けました。本件業務の内容、日程、代金（代金の支払方法を含みます。）、各当事者の具体的な義務等の取引条件については、システム基本契約書、本重要事項説明書の具体的作業内容及び本個別契約条項の記載に従います。
2. 機器等の売買等
   ユーザは、本契約（システム基本契約書と個別契約書としての本重要事項説明書から構成されます。以下同じ。）に基づきユーザに納入されるソフトウェア、ハードウェア等のシステム（以下「本件システム」といいます。）に関し、本件業務の提供を受けるにあたり、ベンダ又は第三者からソフトウェア、ハードウェア等（以下「機器等」といいます。）を購入し、又は借り入れる場合があります。なお、ベンダからの当該購入又は借入れの契約条件については、本契約とは別個に締結される契約が本契約に優先して適用されるものとし、ベンダは、当該別契約に別段の定めのない限り、機器等の固有の瑕疵について責任を負いません。
3. 本件業務（運用支援業務）の範囲
   1)　運用支援業務とは、本件システムの検収時以降における本件システムの運用に関する業務を支援するために行う業務をいい、ユーザの新たな要求を満たすことを目的とする本件システム及びユーザの業務の改良又は変更を含みません。

   2)　データのバックアップ作業はユーザの責任とします。バックアップがない事により生じる損害について、ベンダは責任を負いません。
4. サービスの範囲
   ベンダは、ユーザに対し、別途定めるサービス仕様書に基づき運用支援業務に係るサービス内容を定めるものとします。
5. 設置場所への立ち入り等
   ユーザは、運用支援業務を行うためにベンダが本件システムの設置場所に立ち入ることを認めます。ユーザは、ベンダが運用支援業務を行うために必要となる作業場所及び消耗品を無償にて提供するものとします。
6. 遠隔接続または遠隔操作によるサービス
   本重要事項説明書でベンダとユーザが合意するときは、ベンダは、ユーザに対し、遠隔接続または遠隔操作による業務を行います。
7. 設置場所の変更
   ユーザは、ベンダに対して予め通知した本件システムの設置場所を変更する場合、ベンダに対し、変更後の設置場所及び変更日を変更の 30 日前までに書面により通知するものとします。
8. 設置場所の整備
   ユーザは、運用支援業務の対象となるハードウェアの製造会社が定める使用環境条件（入力電源、温湿度、塵埃、振動、電界及び磁界、接地条件、対象製品に有害な塩基及び有酸ガス、メンテナンスエリア等）を本件システムの設置場所において常に整備し、維持するものとします。
9. 使用地域の制限
   ユーザは、本件システムを日本国内においてのみ使用するものとします。
10. 有効期間
    本契約の有効期間は、契約締結の時から 1 年間とします。但し、期間満了１ヶ月前までにベンダ及びユーザのいずれからも書面による申出がない場合には、更に１年間延長するものとし、その後も同様とします。
11. 支払い遅延
    ユーザが代金債務の支払を怠った場合、ベンダは、ユーザに対し、当該遅延日以降の運用支援業務を行う義務はありません。

■告知事項

1. 内容や専門用語でご不明の点は随時ご質問頂き、十分にご精査ください。
2. データのバックアップ作業はお客様の責任であり、特別の定めがない限りバックアップがない事により生じる損害について、ベンダは責任を負いませんので、十分にご注意ください。

K　運用支援業務契約の重要事項　(2)明細＜記入例＞

項番	運用支援サービス名称 業務内容	設置場所	サービス料金 （円／年、税抜）	請求方法 支払方法	請求開始 年月日	サービス期間		遠隔接続・操作サービスの有無	添付図書名	SLA 合意書有無
						開始日	終了日			
1	サーバ稼動監視サービス	東京都千代田区ｘｘｘ	○○○,○○○円	年額一括 銀行口座自動引落	○○○○年 ○○月○○日	○○○○年 ○○月○○日	○○○○年 ○○月○○日	あり	稼動監視サービス仕様書	有り
2	ウィルス監視サービス	東京都千代田区ｘｘｘ	○○○,○○○円	年額一括 銀行口座自動引落	○○○○年 ○○月○○日	○○○○年 ○○月○○日	○○○○年 ○○月○○日	あり	ウィルス監視サービス仕様書	有り
3	ウィルス駆除サービス	東京都千代田区ｘｘｘ	○○○,○○○円	年額一括 銀行口座自動引落	○○○○年 ○○月○○日	○○○○年 ○○月○○日	○○○○年 ○○月○○日	あり	ウィルス駆除サービス仕様書	有り

受託金額合計（税抜）	損害賠償限度額：（項番ごとに記載）
付帯事項：（ユーザが担当する業務等） 連絡協議会の実施要項及びユーザ・ベンダの責任者、主任担当者：	遠隔接続・操作サービスの内容：（項番ごとに記載） 項番 1：稼働監視サービス仕様書に基づく遠隔接続によって、指定のサーバの稼働状態を常時監視します。異常発生時には、SLA 合意書に基づきお客様に状態通報を実施します。 項番 2：ウィルス監視サービス仕様書に基づく遠隔接続によって、アンチウイルスソフトの稼働状況、ウィルス感染を常時監視します。異常発生時には、SLA 合意書に基づく状態通報を実施します。 項番 3：遠隔操作による駆除サービスは原則、接続毎にお客様の許可を得て実施します。遠隔操作で対応できない場合は、SLA 合意書に基づきオンサイトサービスを実施します。
特約条項：	再委託先の表示

その他本件業務遂行に必要な事項

（法令・規制・規程等の遵守事項、その他の事項）

（鑑部分）

(付録) 添付図書

項番	図書名	版	日付

(鑑部分)

「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～

＜セキュリティチェックシート解説（別紙）＞

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　はじめに

「セキュリティチェックシート解説」は、中堅・中小事業規模ユーザにおいてパッケージ取引・契約モデルに基づき、システム設計導入、更新時における契約活動を支援するためのものである。セキュリティについてユーザの仕様要求書（Request For Proposal、以下：RFP）の作成の支援、ならびに契約プロセスにおける重要事項説明書の理解促進を目的に作成を行なった。

具体的には、自社の IT システムの状況を把握し、自社の事業モデルにおいて必要とされるセキュリティ・可用性の要件定義について、補足資料にある「セキュリティ・可用性チェックシート」の活用を促進するものである。これにより、IT 専任担当者の配置が困難な企業ユーザにおいても適切な仕様要求が行なえることを目指している。

本解説を通じて上述のチェックシートの使用方法を理解し、より安全なシステム運用、事業計画の維持が中堅・中小事業規模の企業においても行なわれることを期待したい。

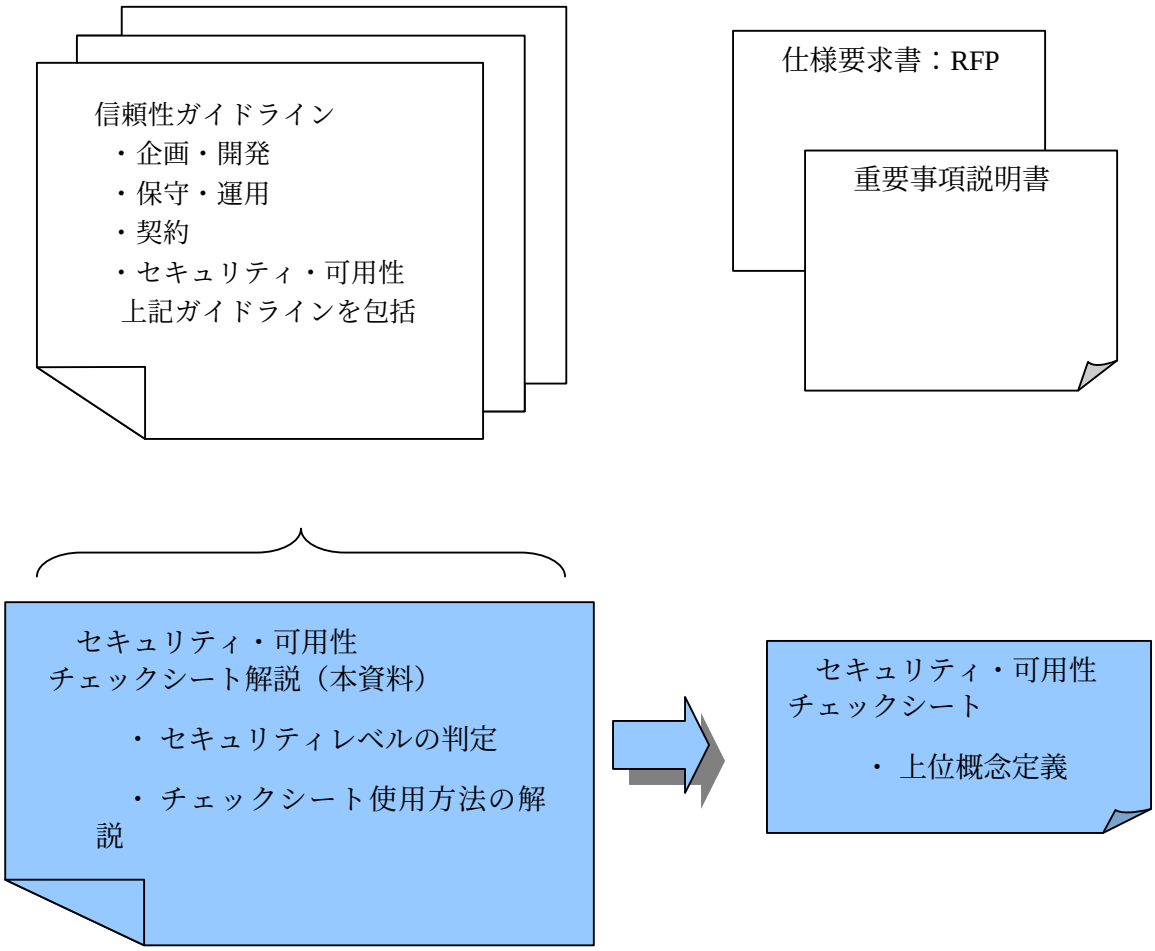


図 1　ガイドライン・チェックシート相関図

2　概要

2.1　　セキュリティチェックシート解説作成の背景

現在、IT は基幹システムのみならず、中堅、中小事業規模の企業においても事業継続において不可欠なツールとなってきている。反面、IT の進歩に従い、法令遵守の観点から取り扱う情報の保護ならびに防衛策の徹底、また、IT インフラを活用しての事業継続性の維持が事業規模に関わらず求められる。[1]

ただし、該当事業規模においては自社システムの導入・運用フェーズにおいて基幹システムと同等の開発を行うことは困難であり、概ね欧米を中心とする諸外国での実装モデルであり、汎用用途を目的に開発された「パッケージソフト」の導入を想定したシステムの構築を行うのが現状である。

本解説においては、このような認識から、平成 19 年 4 月に経済産業省商務情報政策局情報処理振興課より公表された「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＞」（以降、「モデル契約書」）[2]　及び「追補版報告案」にベースに、中堅・中小事業規模の企業における IT セキュリティの確保のための指針に加え、事業継続性の観点より求められる要件定義、非導入リスクについて議論し取りまとめを行った。

2.2　　セキュリティチェックシート解説の目的

本解説の目的は、モデル契約書に基づき、これに準じた中堅・中小事業規模の企業を対象としたセキュリティチェックシート解説を提供することにある。本解説においては以下の点を留意されたい。

- 一般的なシステム導入時におけるセキュリティ対策、可用性設計の要素検討に加え、同一事業規模を対象とした指標・ガイドライン（例：経済産業省「企業における情報セキュリティガバナンスのあり方に関する研究会「情報セキュリティ対策ベンチマーク」、「事業継続計画（BCP)」など）を参照の上、検討を行なった。
- 「パッケージソフトウェア」、「中小事業規模ユーザ」における契約慣行に配慮する。
- 4 レベル（モデル例：大企業連結型、特定事業請負型、独立事業型など）を定義し、汎用パッケージにおけるシステム設計の簡素化を提案する。
- システム運用時における可用性についての定義付け、要求仕様について提言する。
- チェックシート解説に規定した項目を未実装とした場合の事業リスクについて定義を行い、情報システム取引契約時にシステム固有のリスクの可視化の促進を図る。

2.3　　基準とする標準規格

[1] 事業リスクについては「参考資料４．２ セキュリティ事故に従う被害額シミュレーション」を参照

[2] 公示内容は<http://www.meti.go.jp/press/20070116001/20070116001.html>を参照

現在、情報セキュリティ・事業継続計画については、国内外を問わず、多くの検討が行なわれている[3]が、ISO（International Organization for Standardization、国際標準化機構）と共通要件定義が進んでいる段階であり、日本においても今後国際規格に準じた対応を行っていくものと予想される。そのため、本解説作成においても以下の国際基準に基づいた要件定義の検討を行った。

(1) 情報セキュリティ

日本における情報セキュリティガイドラインについては英国規格 BS7799 をベースに JIS X：5080 としての規格化が進み、現在では JIS Q：27001 規格が基準となっている。そのため、セキュリティ要件項目の検討においては本規格に基づく検討を行った。

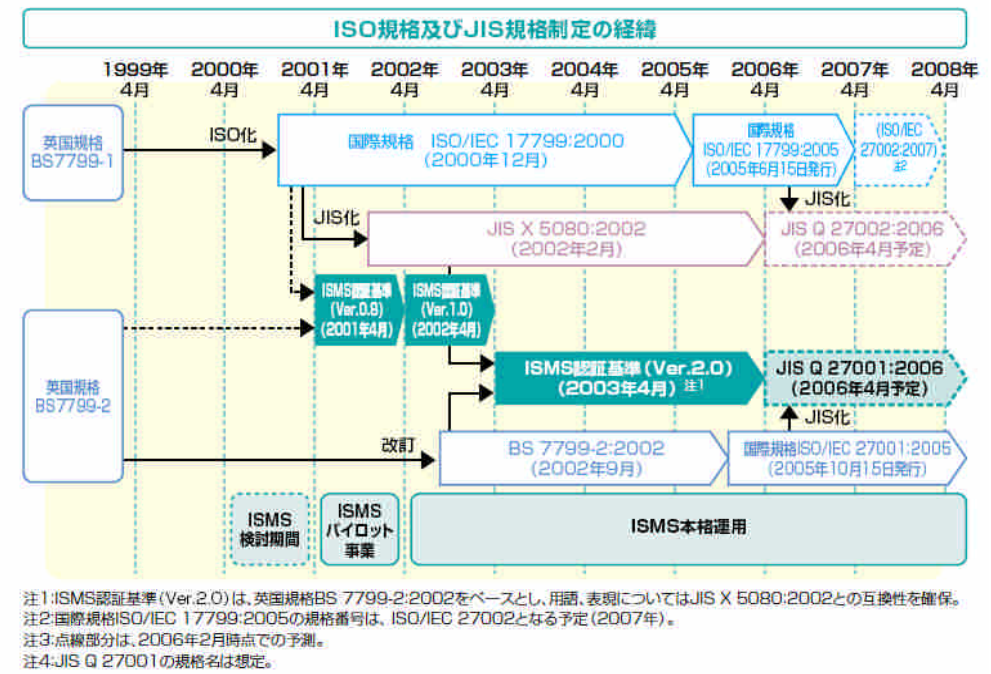


表 1　ISO 規格及び JIS 規格制定の経緯[4]

(2) 可用性

可用性についてはシステム運用の観点から ITIL（Information Technology Infrastructure Library）に基づき規定された IT サービスマネージメントの英国基準 BS15000 をベースに国際基準に発展した JIS Q：20000、また、事業モデルに応じて事業継続性の観点から制定された環境マネジメントシステム(EMS：Environmental Management Systems)の国際基準である JIS Q：14001 を参照したシステム実装が行われている。現在、事業継続計画（BCP：Business Continuity Planning）については事業計画管理（BCM：Business Continuity Management）としての国際基準化に向けた活動が活発化しており、英国規格協会（BSI：British Standards Institution）による PASS56、米国標準協会（ANSI：American National

[3]補足資料４．１　参考資料を参照

[4]出展：情報セキュリティマネジメントシステム 適合性評価制度の概要（ISO/IEC 27001:2005 対応版）（財）日本情報処理開発協会

Standard Institute）による NFPA-1600 の規定、日本においても経済産業省の企業における情報セキュリティガバナンスのあり方に関する研究会の報告書で示された「事業継続計画策定ガイドライン」、中央防災会議専門調査会（内閣府）「事業継続ガイドライン 第一版」などに基づいた提案活動を日本規格協会（JSA：Japan Standard Association）を通じて行われている[5]。ただし規格検討段階（規格提案国は 6 カ国：日本、英国、米国、カナダ、オーストラリア、イスラエル）であることを踏まえ、当検討委員会においては上述ガイドラインならびに ANSI 規定内容などを参照の上、今後の動向を見据えたガイドライン検討を行った。

2.4 セキュリティチェックシート解説で使用される用語定義について

本解説において使用される用語については共通フレーム 2007 を準用した。ただし、セキュリティチェックシートなどの表記については中堅・中小事業規模のユーザにも理解しやすい内容とすることを目的に簡易表記を行なっている。

3 セキュリティチェックシート解説

モデル契約書において、セキュリティ・可用性に関する要件定義については広く議論がなされ、仕様要求書（RFP）作成における方針ならびにサンプルドキュメントの掲載が行なわれている。ただし、中堅・中小事業規模の企業においては専任のシステム管理者の配置が困難である場合も多く、システム導入についての明確なセキュリティ・可用性要件定義を行なうことが困難であるものと推測される。

本解説は、これら企業ユーザを対象に自社のシステム状況の把握、求められるシステム要件定義書作成における支援、ならびにベンダからの説明項目の標準化を目指し、策定を行なった。

3.1 セキュリティ・可用性レベル設定について

(1) 想定される事業モデル

RFP を作成するための知識、人的資源が十分に確保することが困難である中堅・中小事業規模の企業において、具体的な対策についての計画設計を行なうには今までベンダに依存する構造となっていた。今回、以下のようにセキュリティ・可用性対策の観点から事業モデルケースの考察ならびに求められるシステム要件のとりまとめを行なった。

ユーザには自社の事業モデルに基づき、まずはどのレベル達成が求められるのかを本表に基づき考察を進めることを希望する。

[5] 本議論の進捗については JSA の Web サイト<http://www.jsa.or.jp/stdz/mngment/mngment.asp>を参照

	想定される業務モデル	情報セキュリティ要件	可用性要件	SWベンダー要件
レベル 4 (推奨)	行政機関、大企業向けの業務支援活動を中心に行う コンプライアンス対策などについて発注元と同等のものが求められる	・各クライアント対策に加え、ゲートウェイでのセキュリティ対策、コンテンツセキュリティの実装を行う ・管理する専任者を配置	・24×7システムの実装 ・システムダウンタイム 数時間/年間レベルの維持などを 専任管理者の下運用する	・J-SOX対応、P-mark対応などコンプライアンス対策への対応 ・日本国内での障害対応部門の設置 など
レベル 3 (標準)	基本的に委託業務型であり、受注案件に応じて他企業・機関との情報の流通が行われる	・上記同様のセキュリティレベルを維持する。 ・専任管理者の配置が困難な場合には遠隔監視モデルの採用を検討する	・24×7システムの実装 ・システムダウンタイム 数時間/年間レベルの維持など遠隔モデルなどを活用し維持する	・J-SOX対応、P-mark対応などコンプライアンス対策への対応 ・日本国内での障害対応部門の設置 など
レベル 2 (低)	独自事業展開により、他企業との情報の流通はほとんど無い	・クライアント対策など基本的な対応を行う ・導入に対しては企業単位にて管理ツールにて品質維持できる環境を構築	・データバックアップ方法の確立 ・システム障害発生時のリカバリー手段の確保	・管理ツールが実装可能など
レベル 1 (非推奨)	情報閲覧などのみITを活用 事業継続性への影響が全くない	・基本ソフト標準の機能を活用する	・特に行わない	・対策未実装のリスク提示など

表 2　事業モデルにおけるセキュリティ・可用性レベル設定[6]

(2) セキュリティ・可用性　上位概念定義

上述の「2.1.1 想定される事業モデル」ではユーザが自社として実装すべきセキュリティ・可用性レベルについて定義を行なったが、中堅・中小事業規模の企業における実際のシステム運用においては具体的にパッケージソフトウェア製品ならびハードウェア機器を基本としたセキュリティ・可用性対策が求められる。本ワーキンググループの討議においては JIS Q：27001 規格に基づきセキュリティ・可用性対策についてレベルに応じた対策ならびに未実装の場合のリスクについての検討を進めた。ただし、中堅・中小事業規模の企業において、上記 JIS 規格に基づく仕様設計の検討を行なうことは容易なことではないため、上位概念についての検討を行い、取りまとめた。ユーザにはまずこのセキュリティ・可用性対策に関する上位概念定義を参照し、自社のシステムにおいて必要とされる要件定義を把握し、ベンダと対等に契約交渉を行なえるように配慮した。全体は、～情報システム・モデル取引・契約書～（パッケージ、SaaS/ASP 活用、保守、運用）＜追補版＞を参照されたい。

[6] 平成 19 年 4 月交付の信頼性ガイドラインとは異なり、レベル 4 を最高レベルとして定義を行った。これは、将来、より高度なセキュリティ強度が求められる場合に柔軟に対応するためのものである。

対策項目	リスクの詳細	参考情報			
		レベル1	レベル2	レベル3	レベル4
■認証 情報を参照している人が本人であることを証明する。	情報を参照している人が、本人であるかを管理していないと、他人に重要な情報を見られる可能性がある。	**■何も決められていない** 情報を誰が参照しているか特定できない状態。	**■個人を認識できる** パスワードを利用して、個人を認識できるようにする。	**■本人認証の強化** 特定のカードやログインの二重化などで、本人認証を強化する。	**■絶対的な本人認証** 生体認証等を組み合わせ、定期的なポリシー変更を実施する。
■アクセス権 情報よって、アクセスできる人を制限･管理する。	誰でも情報アクセスできるようになっていると、削除、改ざん、複製、持ち出しされたりする。	**■何も決められていない** 情報に誰でもアクセスできてしまう。	**■コンピュータ単位で設定できる** サーバ単位、フォルダ単位で、個人･グループがアクセスできように設定する。	**■認証情報に基づき資源単位でアクセス権が設定できる** ファイル単位で、個人･グループがアクセスできるように設定する。	**■資源単位でアクセスした内容の収集、分析ができる** アクセスされた情報（ログ）を収集･分析できる。
■暗号化 情報を暗号化して、紛失･盗難･盗聴の対策を施す。	情報機器（コンピュータやUSBメモリなど）が盗難又は紛失することにより、情報が漏えいするおそれがある。	**■何も対策されていない** 社外に持ち出すデータ、社内のコンピュータのデータに暗号化が実施されていない。	**■モバイルコンピュータやUSBメモリ単位で暗号化して持ち出す** 社外に持ち出すコンピュータ、USBメモリなどの中に入っているデータを暗号して持ちだす。	**■全てのコンピュータについて、データを暗号化する** 社内のコンピュータ、社外に持ち出すコンピュータ、業務で使用するUSBメモリ、外付けHDD、CD/DVDなど情報を書き込めるものに対して暗号化をする。	**■暗号されたものを復号する都度、認証をおこなう** 暗号化されたデータを復号するたびに認証を実施して、履歴を取得する。
■悪意あるプログラムの検出 悪意あるプログラムから情報資産を守る。	コンピュータに誤動作を起こさせる悪意あるプログラム（ウイルスやスパイウェア等）により、システムが利用できなくなる、データが消去される、情報が外部に漏えいしてしまう、などのおそれがある。	**■何も決められていない** ウイルス対策を実施していない。	**■ウイルス等を検出し侵入を停止･警告できる** コンピュータ上で悪意あるプログラムを検出して削除し、警告できる。	**■全システムに対するウイルス対策と集中管理** ネットワーク機器やコンピュータなど複数の対象に対して、悪意あるプログラムを検出、削除するための機能を導入し、被害状況の収集や定義ファイルの更新を集中的に管理できる。	**■不審な通信やコンピュータをシステムから隔離できる** 悪意あるプログラムが検出されたコンピュータをネットワークから遮断する。
■ネットワークの運用 ネットワークを流れるデータ量の管理をする。	ネットワーク障害や大量のデータ転送により、ネットワークが正常に利用できなくなるおそれがある。	**■何も決められていない** ネットワーク管理ツールもしくはサービスを導入していない。	**■管理ツールを導入する** 障害検知やネットワーク負荷を検知するツール、サービスを導入する。	**■冗長化する、使用状況を監視して記録できるようになる** ネットワーク機器を冗長化して大量データに備えたり、ネットワーク障害時にネットワークが利用できなくなるのを回避したりする。	**■トラフィックに応じた柔軟な制御ができる** ネットワークの使用状況に応じて、機器の設定を容易に変更できる。
■保守 OSやアプリケーション、ハードの保守を行なう。	保守がされていないと、不具合の発生や、セキュリティホールによって情報が漏えいするおそれがある。	**■何も決められていない** メンテナンス作業をやっていない。	**■障害発生時に対応する** 障害が発生した時点で、保守作業を実施する。	**■修正版発行時に対応する** 保守対象となる不具合修正版の発行時に、予備機でテストをおこない、適用する。	**■予防的に対応する** 定期的、計画的に、不具合修正版の取り込みを行う。
■機器運用監視 サーバ、ネットワーク機器の稼働監視を行う。	システムの状況を把握できないことにより、障害の対応が遅れて情報システムへのアクセスが長時間停止するおそれがある。	**■何も決められていない** サーバ、ネットワーク機器の稼働状況を監視していない。	**■運用状況を遠隔で、手動で把握できる** 遠隔で稼働状況を手動で確認する。	**■運用状況を自動で把握、記録ができる** 稼働状況を常時把握し、異常があれば通知する。	**■運用状況に異常があれば、自動的に設定された状態に切替わる** 異常を通知するとともに、代替手段に自動的に切替わる。

表 3　セキュリティ上位概念定義(抜粋)

(3) セキュリティ・可用性チェックシート（詳細項目版）

セキュリティ・可用性チェックシート（詳細項目版）は JIS Q：27001 規格を基準とし[7]、ユーザが実装すべきセキュリティ・可用性対策についてレベル別に定義を行なうものである。今回、対策を行なわなかった場合のリスク要素についても議論を進め、とりまとめを行っており、2008 年 4 月をめどに発表の予定である。

また、現段階では標準規格化に向けた準備段階である Web サイト、Web アプリケーションによるシステム導入時におけるセキュリティ・可用性についても議論を進め、定義付けの検討を行なっている。本チェックシートは上記した上位概念定義に基づくセキュリティ・可用性の仕様選定においての活用、重要事項説明書におけるリスク説明などの際にユーザ側のみならず、ベンダ側での活用を強く望むものである。

[7] 「参考文献（JIS Q 27002：2006 以外）」として、項目によっては他に参照したガイドラインの記載を行った。

	技術的セキュリティ対策 要素	分類	対策項目	リスクの詳細	レベル1	推奨レベル レベル2	レベル3	レベル4
1	情報を他人から守る（機密性保護）	認証	パスワードを利用する	パスワードが推測可能な容易な物になっていると、第三者がシステムに不正アクセスし、情報を漏えいしてしまうおそれがある。	・パスワードを利用しない。	・初期パスワードをすみやかに変更する。 ・定期的（六ヶ月毎）に、パスワードを変更する。 ・パスワードは、複雑なもの（八桁以上）を設定する。 ・パスワードは、管理者を含め誰にも教えない。 ・パスワードを書き留めたり、コンピュータ上のファイルに保管したり、メールで送信したりしない。やむを得ず紙片等にパスワードを記載する必要がある場合には、そのパスワードが容易に第三者に見られることがないように保管する。 ・自分のパスワードが他人に漏えいした可能性や疑いがある場合は、パスワードを変更する。	・定期的（三ヶ月毎）に、パスワードを変更する。 ・パスワードは、複雑なもの（八桁以上、パスワード世代管理、三種類以上の文字種の使用）を設定する。	・同一利用者が複数のアカウントをもつ場合は、それぞれ異なるパスワードを設定する。また、一つのパスワードから他方が推測しやすいパスワードを設定しない。 ・機密性が高い部署では、生体認証を使用する。
2			ネットワーク上の機器を識別する	不正な情報機器がネットワークに接続されると、情報が漏えいするおそれがある。	・未登録や不正なコンピュータの接続を検出できない。	・未登録や不正なコンピュータの社内ネットワークへの接続を、検出して警報をあげる。 ・接続コンピュータのログを取得する。	・未登録や不正なコンピュータの社内ネットワークへの接続を、検出し、警告して、接続を防止する。 ・接続コンピュータのログを取得する。	・未登録や不正なコンピュータの社内ネットワークへの接続を検出・警告し、接続を防止する。 ・正常な未登録のコンピュータを、自動的に登録する。
3			利用者が本人であることを証明し承認する	利用者の身分が証明できないと、権限がない利用者が情報を不正に取得して社外へ漏えいさせるおそれがある。	・一台のコンピュータを一つのアカウントで、複数の利用者が使用する。 ・認証ログは取得しない。	・Windowsのアカウント、パスワードを利用して、利用者を識別する。 ・一台のコンピュータを複数の利用者では使用させない。 ・認証ログを取得する。	・一台のコンピュータに対して、一人しか使用させない。 ・特定のカードやログインの二重化などで、本人認証を実施する。 ・認証ログを取得する。	・生体認証（静脈・指紋認証など）を利用して、利用者の本人認証を実施する。 ・二要素認証を実施し、認証強度を上げる。 ・認証ログを取得する。
4			業務ソフトウェアや機器認証で使うパスワードを管理する	パスワードの管理がされていないと、不正な活動や情報漏えいが確認できないおそれがある。	・パスワードを管理しない。	・認証機能を使用して、コンピュータを利用する。	・認証機能を使用して、コンピュータと業務ソフトウェアを利用する。	・生体認証を利用してパスワードを使わない。
5			業務ソフトウェアの起動時間を監視する	業務ソフトウェアが終了されずに放置されていると、情報が盗まれるおそれがある。	・業務ソフトウェアの未使用時間を監視しない。	・業務ソフトウェアの未使用時間を監視する。 ・一定時間以上利用されないセッションを監視する。	・業務ソフトウェアの未使用時間を監視し、警告する。	・業務ソフトウェアの未使用時間を監視し、警告して、遮断する。
6			情報へのアクセスを管理する	誰もが情報を閲覧できるようになっていると、情報の改ざんや漏えいのおそれがある。	・サーバ上の情報に誰でもアクセスできる。 ・情報を機密レベルに分類しない。 ・情報にアクセスした履歴を取得しない。	・サーバ上の情報にアクセス権をつけて、権限のない利用者は使用できないようにする。 ・情報にアクセスした履歴を取得しない。	・情報を重要度別（「秘」「社外秘」「関係者外秘」など）に分類して、重要度別に利用者やグループ単位でアクセス権をつけて管理する。 ・情報にアクセスした履歴を取得する。 ・印刷物を減らすことにより、管理する対象を減らし、情報漏えいのリスクを減らす。 ・印刷物に対して、誰がいつ印刷したものか、わかるように「すかし」などを挿入する。	・アクセスの履歴を定期的に監査して、情報の持ち出しに問題があれば是正する。
7		暗号化	コンピュータや電子媒体を暗号化する	情報機器が盗難又は紛失されると、情報が漏えいするおそれがある。	・データを暗号化しない。	・社外に持ち出すコンピュータ、電子媒体（USBメモリ、外付けHDD、CD/DVDなど）の中のデータを暗号化する。	・社内のコンピュータ、社外に持ち出すコンピュータ、電子媒体（USBメモリ、外付けHDD、CD/DVDなど）に対して暗号化をする。	・社内のコンピュータ、社外に持ち出すコンピュータ、電子媒体（USBメモリ、外付けHDD、CD/DVDなど）に対して暗号化をする。 ・復号時には認証が毎回必要となる。
8			ネットワークを流れる情報を暗号化する	ネットワーク上のデータが盗聴されると、情報が漏えいするおそれがある。	・社外に送るデータは平文で送信する。 ・Webの通信は暗号化（SSL通信）しない。	・Webの通信を暗号化（SSL通信など）する。	・社外に出る情報を、事前に社内で暗号化して送信する。 ・Webの通信を暗号化（SSL通信など）する。	・コンピュータから発信する情報（メールの添付データなど）を、社内、社外にかかわらず、すべて事前に暗号化して送信する。 ・Webの通信を暗号化（SSL通信など）する。
9			暗号鍵の強度を上げる	暗号の複雑さが低いと、簡単に復号化されて情報が漏えいするおそれがある。	・暗号化しない。	・公に認知されているアルゴリズムで暗号化する。 ・鍵長が64ビット以上の暗号化を使用する（AES 64ビット以上など）。	・公に認知されているアルゴリズムで暗号化する。 ・鍵長が128ビット以上の暗号化を使用する（AES 128ビット以上など）。	---> 前レベルと同様
10			暗号鍵を管理する	暗号鍵が外部に流出すると、暗号化したデータを復号されて、情報が漏えいするおそれがある。	・暗号化しない。	・暗号鍵を、平文（通常の文字列）のままソフトウェア上で管理する。	・暗号鍵を、暗号化してソフトウェア上で管理する。 ・サーバ上で、暗号鍵の保管場所を誰にでもわかるようにする。	・暗号鍵を暗号化して、独自のパスワード等で保護する。 ・暗号鍵の所在については、システム的に管理者以外は閲覧できなくする。

表 4　セキュリティチェックシート（詳細項目版：一部抜粋）

(4)　本チェックシート使用の際の留意事項

- 推奨レベル（網掛け部分）とは、中堅・中小事業規模のユーザにおいても実装することが望まれるセキュリティ対策について定義づけがなされている。
- 必要とされるレベル定義の判断については、網掛けがされている項目に特に留意し、これらの項目が満たされているかを中心に点検を行なう。
- 本チェックシートは業務要件定義でレベルを決定しユーザ、ベンダが仕様について合意する。パッケージ選定の際には、業務要件としてのセキュリティ要件を確認し、システム要件にあわせて具体的な仕様を決定する。
- セキュリティ要件は、技術的、システム的に解決するだけでなく、運用、保守、教育を含めた継続的な措置が重要であることをユーザ、ベンダともに合意する。

3.2　セキュリティ対策

今日では、情報システムがビジネスに密接に関係する比率は高くなっている。たとえば、10 年前に多くの企業で業務の遂行や連絡に、紙の文書、電話、郵便などの情報システムに直接依存しない方法を使用していた。今日では、電子メール、イントラネット、経理システムや Web サイトなどの情報システムを活用している。電子商取引に携わっている企業では、企業顧客間取引(B2C)、企業間取引(B2B)、企業従業員間取引(B2E)等の安定した運用がビジネスの成否に大きな影響を与えている。この様に、ビジネスが情報システムに依存する比率が高くなっており、情報システムの問題はビジネスへのリスクとなる。

環境内のサーバーに深刻な攻撃が行われた場合、組織全体に甚大な被害が及ぶ。例として、攻撃によって組織の Web サイトがダウンした場合、売上や顧客からの信頼を失い、組織の収益にも影響することも考えられる。また、個人情報を漏えいした場合、信頼を失い取引関係が消失し、漏えい後の顧客への対応に多くの費用を必要することが容易に予測できる。

このような問題は、大規模な組織のみでおこるものではなく、中堅・中小事業規模の企

業を含め、どのような規模や環境でも起こり、セキュリティ問題をリスクとして真剣に考える必要がある。リスクは恐れるべき対象ではなく、管理すべき対象であり、情報システムの企画・開発・運用等の各段階において、不確実性を認識して最小化し、確認した各リスクに予防保全的に取り組むことによって管理できる。実際にセキュリティ問題が発生した場合、IT への依存度や問題の程度によっては、ビジネスの存続自体を不可能にし、この可能性はビジネスの規模が小さい程顕著となる。セキュリティ対策に投資することはネガティブにとらえられがちであるが、IT 依存度に比例したセキュリティ対策を導入することが、ビジネスの継続の基盤となる。

事業の内容や規模にあった適切なコストをかけたセキュリティ対策を行うことは、将来のビジネスを保護し不確定なリスクを排除する。セキュリティ問題が発生した場合でも、適切な対策を行っている事で顧客の理解を得られる場合も考えられる。また、適切なセキュリティ対策を行っていることが、取引の条件となる事が今後も増加すると考えられる。

本解説は、主として中小規模の事業者が、パッケージ製品、開発製品、Web サイトの構築を提供または導入する担当者双方が共通の認識で検討するべき事項を提供する。

推奨されるセキュリティ対策を ISO/IEC27001(JIS Q27001)による用語の定義「情報の機密性，完全性及び可用性を維持すること」に基づきセキュリティの重要な 3 要素である、「機密性保護 (個人情報、営業機密などの情報を守る)」「完全性保護 (改ざんやなりすましの様な不正な変更から情報を守る)」「可用性保護 (情報システムや情報が必要な時に利用できるように維持する)」を軸に対策と発生しうるリスクをコストに合わせて選択できるようにまとめを行った。

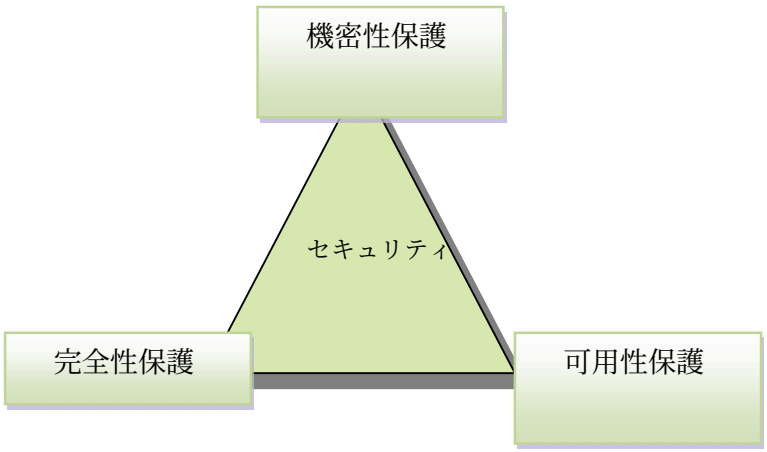


図 2　情報セキュリティに求められる 3 要素

3.3　　可用性対策

可用性とは国際標準化機構（ISO）が定める標準用語（Availability：アベイラビリィティ）に基づくものであり、その定義としては「認可された利用者が、必要なときに情報にアクセスできることを確実にすること」[8]を示すものである。すでに小規模事業企業におい

[8] 総務省 国民のためのセキュリティサイト　用語辞典

ても諸取引の電子化が進んでおり、業務の受託元企業との相互情報伝達の維持、自社のデジタル資産のバックアップが不可欠になってきている。システム導入期（企画・開発フェーズ）においては、システムの安定稼働についての議論がベンダ・ユーザ間で行なわれるが、反面、運用開始後の可用性（事業継続計画に基づく IT システムの安定稼動）については十分な対策が講じられていないのが現状である。そこで想定レベルに応じて、実運用時に起きるトラブル事例に基づいた対策案について議論を進めてきた。

コンピュータが機器である以上、連続使用による経年劣化、温度変化、結露などがもたらす障害発生は起こりえるものと想定し、それに対応するシステムの運用・保守体制が必要である。

(1) 起こりえるシステムトラブル・事業中断内容について
中小規模事業企業においても今日では会計システムに代表とする業務の IT 化が進んでおり、事業継続性の観点からコンピュータの障害・停止などに従うダウンタイムの原因と処置について取りまとめを行なった。

ダウンタイムの原因	例	処置	回避のための予防措置	
			導入（企画段階）	運用・保守
点検（計画保守）による停止、起動	ハードウェア 機器、OS、ソフトウェア	アップグレード、交換、清掃	クラスタリングによる冗長化	ログの監視
機器の障害	コンピュータ（メモリ、冷却ファン、システム ボード、電源装置、ドライブ、ドライブコントローラ、NIC）	交換、清掃	クラスタリングまたはフェイルオーバーによる冗長化 ホットプラグ、RAID構成、SNA構成	定期点検及び交換、清掃、設置環境の維持、必要に応じてファームウェアのアップグレード
	ルーター、ハブ	アップグレード、交換	クラスタリングまたはフェイルオーバーによる冗長化、ホットプラグ	定期点検、清掃、設置環境の維持、必要に応じてファームウェアのアップグレード
	ネットワーク ケーブル	交換	床上げ、無線化	ワイヤリングの見直し、定期点検及び交換
ソフトウェアの不具合	OSの応答停止、アプリケーションの応答停止、異常出力、ファイルの破損	アップグレード、再構築	クラスタリングによる冗長化、仕様の再検討、テスト体制の見直し	計画保守によるアップグレード、テスト及び再起動
悪意あるソフトウェア	外部攻撃、ウイルス、スパイウェアによるファイルの破損、書き換え	認証の強化、通信ポートの制限、OSのアップグレード、アンチウイルスによる駆除	複雑なパスワードの採用、認証システムの強化、必要な通信ポート以外の通信制限、アンチウイルスでの検索・駆除設定、バックアップ	定期的なアンチウイルスによるウイルスの検索及び駆除、定期的なパスワードの変更、パスワード履歴管理
操作員のミス	データの削除、書き換え、誤入力	UIの変更、権限の設定、操作の教育	管理権限と運用ルールの見直し、コード体系の設定、入力ルールの設定、バックアップ、操作員の現況把握と適切な教育	コード体系の見直し、GUIの見直し、ロールバックの設定
悪意のあるユーザー	データの持ち出し、外部漏洩、改ざん	アップグレード、再構築、暗号化、持ち出し制御	セキュリティポリシの策定、出力・複写の制御及び監視、ログ管理、バックアップ、従業員の現況把握と適切な教育	運用ルールの強化、定期的なログの分析、ロールバックの設定、セキュリティポリシの見直し、教育
災害による機器の損傷	火事、水濡れ、地震、台風、洪水、停電、高温障害	交換、再構築	データセンターでのハウジング、バックアップ	清掃、設置環境の維持

表 5　可用性の側面からみたトラブル事例および予防・処置対策

(2) 事業モデルに基づく可用性対策のレベル設定について
また、事業モデルに応じた可用性対策について検討を行なった。実際には事業形態に応じた考察が必要であるがモデルケースとして参照されたい。

	単独 スタンドアロン	LAN1 Internet共有･スタンドアロン	LAN2 ドメイン･2-Tier	LAN3 ドメイン･3-Tier	Saas Web, 3-Tier
管理者	オペレータが兼務	オペレータもしくは兼務の管理担当者	兼務の管理担当者もしくは管理者	管理者	←スタンドアロン以外
外部ネットワーク接続形態	なし	PPTPによるInternet接続	PPTPによるInternet接続	ルータによる固定IP接続	←スタンドアロン以外
内部ネットワーク接続形態	なし	ディスク共有、Workgroup	File-Server, Printer-Server	File-Server, Printer-Server, Apps-Server	←スタンドアロン以外
認証	ローカルパスワード	ローカルパスワード	ドメインパスワード	ドメインパスワード	←すべての形態
オペレーター以外のPC共有	あり	あり	なし	なし	←すべての形態
第三者とのデータのやりとり	リムーバブルメディア、DISK共有	リムーバブルメディア、DISK共有、電子メール	リムーバブルメディア、DISK共有、Server共有、電子メール		←すべての形態
プリンタ	ローカル	ローカル、共有			←すべての形態
主たるデータの場所	ローカル、内蔵、外付HDD	ローカル、内蔵、外付HDD	ローカル、内蔵、外付HDD、Server	DB-Server	Appsに依存、ローカル、Server、外部Server
主たるアプリの場所	ローカル、内蔵、外付HDD	PC、内蔵、外付HDD	PC、内蔵、外付HDD	PC、内蔵、外付HDD、Apps-Server	外部Server
主たるLANの用途	該当なし	電子メール、Web閲覧	電子メール、Web閲覧、基幹業務		
求められるセキュリティ･可用性レベル	レベル2	レベル2	レベル3	レベル4	レベル3 〔社内システムはレベル2〕

表 6　可用性対策におけるレベル別モデルケース

4　Web サイト、Web アプリケーションにおけるセキュリティ対策について

インターネットに接続された Web サイト（企業のポータルサイトや EC サイト等）は、そのシステム構築にパッケージソフトウェアを利用したとしても、技術者によるスクリプト・プログラム（Java、JSP、JavaScript、PHP、Perl….等）の開発作業割合が非常に多い。従って、Web サイトのセキュリティレベルも Web アプリケーションの開発者や開発ベンダの技術レベルに強く依存する。さらに、アンケート機能、E-Commerce 機能等の活用により、個人情報を含む重要な情報が格納されている。そのような特性にもかかわらず、インターネットに直接接続されているため、不正アクセス等の攻撃を受けやすい環境にあり、企業内ネットワークに構築されている各種のシステムと比較すると、より強固なレベルのセキュリティ対策が必要であるといえる。

そこで、本章では、インターネットに直接接続された Web サイトおよび Web アプリケーションのセキュリティ対策について解説する。

4.1　Web アプリケーションのセキュリティ対策の現状と課題

Web アプリケーションにおいて、脆弱性が存在した場合、以下のような被害が発生する可能性がある。

(1) 社内情報の漏洩・改ざん・破壊等
Web サイト（アンケートや会員登録機能）で管理している個人情報や社内の重要な情報が漏洩したり、Web を利用するシステムが破壊されたりする。また、課金情報など重要な情報の改ざん、漏洩の可能性がある。

(2) 会員や管理者への成りすまし
Web サイトの会員に成りすましてオンライン上での購入が行われたり、誹謗中傷

のメッセージを書き込まれたりする可能性がある。また、管理者権限で Web サイト内の情報を搾取・改ざんが行われる可能性もある。

(3) フィッシング詐欺や攻撃の踏み台などに悪用
Web サイトにフィッシング詐欺の勧誘記事を掲載されたり、攻撃者のサイトに誘導されたりする。また、Web サイトを踏み台（経由）して、他の Web サイトの攻撃に利用される可能性がある。

IPA/ISEC（独立行政法人 情報処理推進機構 セキュリティセンター）に届出のあった不正アクセスの被害・相談状況によると、OS の脆弱性に対する修正プログラムが長らく適用されていなかった、といった事例が見受けられる。また、古い脆弱性を攻撃対象としたアクセスも非常に多く、ボットに感染しているコンピュータが日本にもまだまだ多い、ということが推測されている。

これらの不正アクセスや攻撃の方法は、決して目新しいものではない。しかし、Web アプリケーションの開発者や運用を行う管理者の、脆弱性やセキュリティ対策に関する認識レベルには差がある。そのため、Web サイトを安全に運用するためには、開発者や管理者の能力に依存しないよう Web アプリケーションの開発ベンダの選定や、「予防保守」を含めた保守・運用の体制とルールの策定が重要である。

4.2 レベル設定について

(1) 想定される Web サイトモデル
Web サイトの役割、格納するデータの重要度によって、必要とされるセキュリティ対策は異なる。
本チェックシートでは、想定される Web サイトのモデルを以下の４段階に区別し、各 Web サイトに要求するセキュリティのレベルと、ソフトウェアベンダ要件について以下のように分類した。

	想定される Web サイトモデル	Web サイトのセキュリティレベル	ソフトウェアベンダ要件
レベル４（推奨）	EC サイト[9]等商取引を実行する Web サイト、企業の機密情報を取り扱う Web サイト	ハッキング[10]には非常に高度な知識が必要	実績の豊富なフレームワーク等を使用してセキュリティ対策を行っている。専任の品質管理部門がセキュリティ監査を行っている
レベル３（標準）	個人情報、企業の重要情報を取り扱う Web サイト、Web サイトの管理者サイト	知識のある人がハッキング可能	セキュリティ開発ルールが定められ、ルールに従った開発・テストを実施している
レベル２（低）	インターネットに接続された Web サイト	知識の無い人が、ツールを入手すればハッキング可能	セキュリティを意識した開発が実施され、セキュリティに関するテストを実施している
レベル１（非推奨）	インターネットに未接続の Web サイト	知識の無い人も、方法が判ればツール無しでハッキング可能	セキュリティに関する対策を何も行っていない

表 7 事業モデルにおけるセキュリティ・可用性レベル設定（Web サイトモデル）

(2) 上位概念定義

[9] インターネット上で商品やサービスの販売を行っているサイト。
[10] 本来はシステムの解析などの意味。ここではクラッキング（他人のコンピュータへ不正に侵入する）の意味で、使用している。

本チェックシートの上位概念として、セキュリティ対策概要・脅威をまとめ、各項目について、その対策レベルを以下のとおり定義する。全体は、～情報システム・モデル取引・契約書～（パッケージ、SaaS/ASP 活用、保守、運用）＜追補版＞を参照されたい。

対策項目	リスクの詳細	参考情報			
		レベル1	レベル2	レベル3	レベル4
■認証 情報を参照している人が本人であることを証明する。	情報を参照している人が、本人であることを管理していないと、他人に重要な情報を見られる可能性がある。	**■何も決められていない** 情報を誰が参照しているか特定できない状態。	**■個人を認識できる** パスワードを利用して、個人を認識できるようにする。	**■本人認証の強化** 特定のカードやログインの二重化などで、本人認証を強化する。	**■絶対的な本人認証** 生体認証等を組み合わせ、定期的なポリシー変更を実施する。
■アクセス権 情報よって、アクセスできる人を制限･管理する。	誰でも情報アクセスできるようになっていると、削除、改ざん、複製、持ち出しされたりする。	**■何も決められていない** 情報に誰でもアクセスできてしまう。	**■利用者と管理者のアクセス権限の設定** 利用者がアクセスできる情報と、管理者だけがアクセスできる情報を区別し、管理する。ログを取得する。	**■グループ単位のアクセス権限の設定** 利用者が所属するグループごとにアクセスできる情報を区別し、管理する。ログを取得する。	**■アクセス権の集中管理機能を有する** 利用者･グループ毎のアクセス権限を管理する機能を使って、最新のアクセス権を維持することができる。ログを収集し、問題発生時に参照できる。
■暗号化 情報を暗号化して、紛失･盗聴･改ざんの対策をする。	通信経路やパスワードが暗号化されていない場合は、紛失･盗聴･改ざんや成りすましの可能性がある。	**■何も決められていない** 通信経路やシステムで保存するパスワードが暗号化されていない。	**■パスワードの暗号化を実装する** パスワードを暗号化し、容易に第三者にパスワードが漏えいしないようにする。	**■個人、決済等に関わる情報の暗号化を実装する** 個人情報、決済情報をすべて暗号化し、漏えい、改ざん、紛失しても悪用されないようにする。	**■全ての情報について高度な暗号化を実装する** あらゆる情報を暗号化し、第三者に悪用されないようにする。
■ページ間のデータ授受 Webのページをまたがってデータのやり取りをする際の対策をする。	ページ間のデータ授受が正しくなされない場合は、情報が漏えいしたり、成りすましされたりする可能性がある。	**■何も決められていない** ページ間のデータ授受について、何もルール化されていない。	**■データの取り扱いがルール化されている** データの有効期限や取り扱い方法が部分的にルール化されている。	**■データの取り扱いルールの強化** データの有効期限や取り扱い方法が規定されている。	**■ページ間でやり取りするデータの種類を規制する** 個人を特定できる情報、決済に関わる情報をページ間でやり取りをしないなどを規定する。
■悪意のあるコードの侵入阻止 悪意のあるコードがWebサーバに埋め込まれるのを阻止する。	悪意のあるコードがWebサーバ上で実行されると、フィッシング詐欺やユーザの成りすまし、パスワード漏えい等の可能性がある。	**■何も決められていない** 悪意のあるコードに対して、なにも対策がない。	**■悪意のあるコードの対策** 悪意のあるコードを排除する仕組みがある。必要最小限のアクセス権限設定をする。不要なファイルを公開しない。	**■悪意のあるコードの対策の強化** 悪意のあるコードを排除する仕組みがあり、対策方法、管理権限がシステム全体で規定されている。	**■Webアプリケーション以外の対策の併用** Webアプリケーション内の悪意のあるコード対策に併せて、WAF（Web Application Firewall）等を使用した対策を実施する。
■システム連携 他のシステムや他のアプリケーションとの連携を行う際に連携の仕組みを悪用されるのを阻止する。	連携の仕組みを悪用されると、フィッシング詐欺やユーザの成りすまし、パスワード漏えい等の可能性がある。	**■何も決められていない** 連携の仕組みを悪用されるのを阻止する対策がない。	**■システム連携悪用の対策** システム連携悪用を排除する仕組みがある。	**■システム連携悪用の対策の強化** システム連携悪用を排除する仕組みがあり、対策方法がシステム全体で規定されている。	**■Webアプリケーション以外の対策の併用** Webアプリケーション内のシステム連携悪用の対策に併せて、WAF等を使用した対策を実施する。
■Webサーバの設定 Webサーバの設定内容について、最適な設定がされているか。	Webサーバの設定が正しく設定されていない場合、サーバ攻撃に必要となるシステム情報が漏えいする。	**■何も決められていない** セキュリティ基準が決められていない。	**■セキュアな設定** Webサーバの設定が外部からの攻撃などを防ぐセキュリティを意識した設定になっている。	**■セキュアな設定の強化** Webサーバの設定がセキュリティを意識した設定になっており、設定内容が規定されている。	**■侵入検知** Webサーバの設定に対する侵入･攻撃の際に、検知し、管理者へ通知する
■内因的な情報漏えい 運用ミスなど内部側の原因で情報が漏えいする。	重要な情報が漏えいしたり、サーバ攻撃に必要となる情報が漏えいしたりする。	**■何も決められていない** Webサーバの運用について規定が何も設けられていない。	**■Webサーバの運用規約** 条件付でWebサーバの運用について規定が設定する。	**■Webサーバの運用規約を強化** 漏れなくWebサーバの運用について規定が設定されている。	**■情報表示の制限** 個人情報等の重要情報は、一覧表示を禁止する、一括してCSVファイル出力を禁止する、などを規定する。

表 8　Web サイト・アプリケーションにおけるセキュリティ・可用性 上位概念定義（一部抜粋）

4.3　チェックシートの活用法について

(1)　チェックシート活用について

最初に、前項の表「3.2　(1)想定される Web サイトモデル」に従って、構築・運用の対象となる Web サイトが担う役割に従って基準となるレベルを設定する。ただし、あくまでも基準であり、チェックシートの全ての項目を基準レベルに設定する必要は無い。構築・運用計画として、常に上位のレベルを目標に設定したセキュリティ対策を組み入れ、PDCA サイクル[11] に基づく運用を実現することが重要である。

(2)　セキュリティ・可用性チェックシート（Web アプリケーション）

「3.2　(2)上位概念定義」の不明な点については、補足資料「セキュリティ・可用性チェックシート(詳細版）)」を確認すること。

(3)　チェックシートの活用ポイント

・　Web アプリケーションの脆弱性

[11]管理業務などを計画通りに実施する為の管理サイクル。PDCA は計画(Plan)、実施(Do)、評価（Check)、改善（Act）を表す。

チェックシートの「機密性保護」の「ユーザ認証」から「アプリケーションの欠陥」については Web アプリケーションの脆弱性について述べている。
これらの対策を怠ると「5.1　Web アプリケーションのセキュリティ対策の現状と課題」に示した問題が発生し社会的責任問題に発展し、ひいては会社存続の危機に陥る可能性があるので、対応レベルの相違はあっても、可能な限り対応する必要がある。

・　特に重要なチェック項目
Web アプリケーションの脆弱性について特に重要な項目について以下に述べる。

■SQL インジェクションとクロス・サイト・スクリプティング
IPA/ISEC（独立行政法人 情報処理推進機構 セキュリティセンター）によると、Web アプリケーションの脆弱性の内訳では、「SQL インジェクション 」と「クロス・サイト・スクリプティング 」の２つの脆弱性が全体の 60%以上を占める。[12]
このことから、「SQL インジェクション」を含む「他システム・アプリケーションとの連携」の「外部プログラムによる脆弱性」と「アプリケーション対策」の「第三者 Web サイトへの情報の送信」について優先的に対策を行う必要がある。これら最低限の対策すら出来ない開発業者への Web システムの発注は、他の Web 診断業者と連携を取るなど、慎重な対応が必要となる。

・　その他のチェック項目について
Web アプリケーションの脆弱性以外のチェック項目については、社内システムとほぼ同様のセキュリティ項目となるが、インターネットに直接接続されるという性質上、社内システムより１ランク上のセキュリティレベルを設定する必要がある。

・　WEF と電子証明書について
「WAF（web application firewall）の製品および対応業者の選定基準」、「電子署名の製品および対応業者の選定基準」については、次年度での本解説策定の課題とする。

5　【補足資料】

5.1　参考資料一覧

セキュリティ・可用性に関する参照ガイドライン一覧

•経済産業省：情報システムの信頼性向上に関する評価指標 （試行版：平成 19 年 4 月）
＜http://www.meti.go.jp/press/20070413003/20070413003.html ＞

• 経済産業省：情報セキュリティガバナンス研究会報告書 （平成 19 年３月）
<http://search.e-gov.go.jp/servlet/Public?CLASSNAME=Pcm1030&btnDownload=yes&hdnSeqno=0000025559 ＞

[12] http://www.ipa.go.jp/security/fy18/reports/contents/enterprise/html/614.html を参照

• 経済産業省：企業における情報セキュリティガバナンスのあり方に関する研究会（平成 17 年 3 月）
＜http://www.meti.go.jp/policy/netsecurity/sec_gov-TopPage.html ＞

• 経済産業省：個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン（平成 16 年 10 月）

•IPA ：情報セキュリティ対策ベンチマーク
＜http://www.ipa.go.jp/security/benchmark/ ＞

•IPA ：セキュリティ要件の検討支援ツール
＜http://www.ipa.go.jp/security/fy18/development/localgov/lg_secstdy_top.html ＞

•「政府機関の情報セキュリティ対策のための統一基準」（2005 年 12 月版）
＜http://www.nisc.go.jp/active/general/kijun01.html ＞

• 総務省：次世代ＩＰインフラ研究会 第二次報告書
＜http://www.soumu.go.jp/s-news/2005/pdf/050707_2_2.pdf ＞

•IPA ：地方公共団体システム調達におけるセキュリティ要件の検討支援ツール
＜http://www.ipa.go.jp/security/fy18/development/localgov/lg_secstdy_top.html ＞

•IPA ：情報セキュリティ読本（2006 年 11 月 改訂版）
＜http://www.ipa.go.jp/security/awareness/management/management.html ＞

•IPA ：大企業・中堅企業の情報システムのセキュリティ対策～脅威と対策～

＜http://www.ipa.go.jp/security/fy18/reports/contents/enterprise/html/index.html＞

•IT セキュリティ評価及び認証制度（JISEC）
＜http://www.ipa.go.jp/security/jisec/index.html ＞

•JIPDEC 情報マネジメントシステム推進センター
＜http://www.isms.jipdec.jp/ ＞

•WASC ：Web Application Security Consortium
＜http://www.webappsec.org/ ＞

5.2 セキュリティ事故に従う被害額シミュレーション

(1) コンピュータウイルスによる被害額算出

独立行政法人 情報処理推進機構 セキュリティセンター（IPA/ISEC）の調査により、2003 年のコンピュータウイルスによる被害額の推計がおこなわれた。ウイルス被害額は、以下に挙げる金額の累積による、ウイルス被害算出モデルで算出されている。

表面化被害＝逸失利益＋システム復旧コスト
潜在化被害＝システム停止中の業務効率低下コスト＋復旧作業に関わる一般業務コスト
ウイルス被害額＝表面化被害＋潜在化被害

ウイルス被害額算出モデルに 115 事業所からのアンケート結果によるデータを基に算出された、事業所 1 社あたりの被害額は、約 28 万円となった。また、このサンプルに基づき推定された、2003 年１月～12 月の国内セキュリティインシデントの被害総額は、約 3,025 億円に達した。

なお、このウイルス被害額算出モデルには、各種補償や謝罪広告費、風評被害による利益源、等は含まれていないため、実質的なウイルス被害額はこれらを上回ることになる。

（出典：IPA/ISEC「国内・海外におけるコンピュータウイルス被害状況調査」）[13]

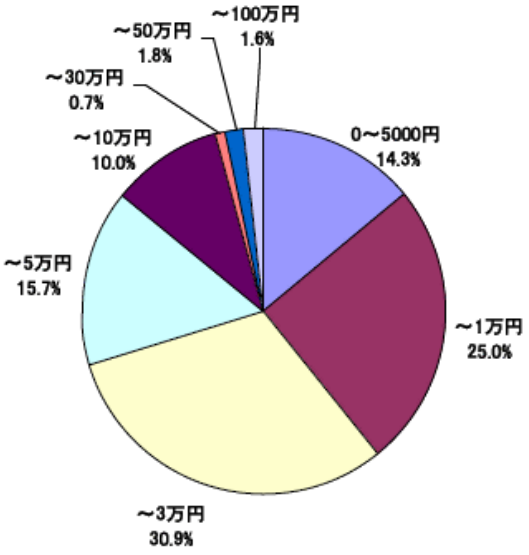
(2) 個人情報漏えいインシデントによる被害額算出

日本ネットワークセキュリティ協会（JNSA）の調査により、2006 年の個人情報漏えいインシデントに関する報告がおこなわれた。2006 年に発生した個人情報漏えいインシデント件数は 993 件で、個人情報が漏えいした合計人数は、約 2,224 万人に達する。この報告書では、「もし被害者全員が賠償請求したら」という仮定に基づく想定被害賠償額も算出されている。賠償額の計算には、以下の算出式が用いられている。

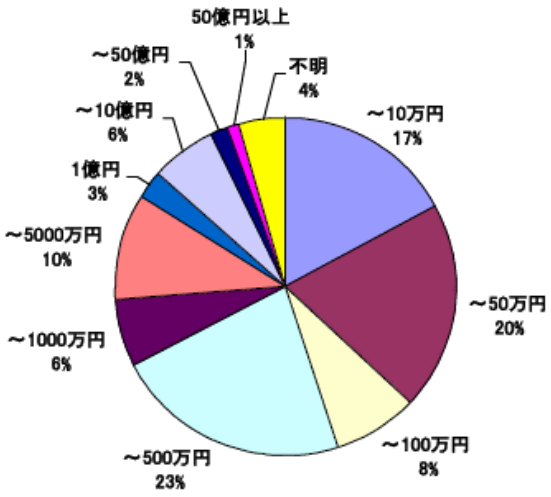
想定損害賠償額
＝漏えい個人情報価値×情報漏えい元組織の社会的責任度×事後対応評価

この算出式と、2006 年 1 年間に報道された個人情報漏えいインシデントに基づき計算された分布図が以下になる。

[13] http://www.ipa.go.jp/security/fy15/reports/virus-survey/index.html



図：一人当たりの想定損害賠償額



図：一件あたりの想定損害賠償総額

インシデント一件あたりの平均想定損害賠償額は 4 億 8,156 円であり、想定損害賠償総額は約 4,570 億円となった。
（出典：JNSA 「2006 年度 情報セキュリティインシデントに関する調査報告書[14]」））

[14] http://www.jnsa.org/result/2006/pol/insident/070720/

セキュリティガイドライン　ワーキンググループ委員名簿

【主査】
高田　和幸
トレンドマイクロ株式会社　コーポレートマーケティンググループ　シニアマネージャー

【委員】
脇坂　隆則
日立ソフトウェアエンジニアリング株式会社　ソリューション開発本部 セキュリティーソリューション部　部長

小野寺　匠
マイクロソフト株式会社　セキュリティレスポンスチーム　チームマネージャ

千葉　貴志
トレンドマイクロ株式会社　コーポレートマーケティンググループ　情報セキュリティマーケティング課マーケティングスペシャリスト

永来　真治
アップデートテクノロジー株式会社　取締役

中塚　勝
ソフトバンク・テクノロジー株式会社　情報セキュリティ推進室　マネージャー　情報セキュリティ教育責任者

奥天　陽司
マイクロソフト株式会社　チーフ　セキュリティ　アドバイザ、早稲田大学　非常勤講師

近藤　伸明
株式会社 神戸デジタル・ラボ　R&D システム部マネージャー

【事務局】
井上　星子　社団法人コンピュータソフトウェア協会　業務課　課長
鈴木　啓紹　社団法人コンピュータソフトウェア協会　業務課

添付資料 2

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

1)情報システムの取引慣行・契約に関する実施ガイド
　〜企画・開発ガイドライン〜
2)情報システムの取引慣行・契約に関する実施ガイド
　〜保守・運用ガイドライン〜
3)セキュリティチェックシート（詳細項目版）
4)システム取引におけるトラブル事例

「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～

＜企画・開発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

※以下のチェックリストについては、本書の「添付資料１　(1)報告書本編」に添付していますのでそちらを参考にして下さい

・提案依頼書(RFP)のチェックリスト
・業務システム仕様書の記述レベル
・ユーザ IT 成熟度チェックリスト
・パッケージ選定のためのチェックリスト
・SaaS 選定のためのチェックリスト
・検収事前チェックリスト

1. 総論

1.1. 経緯

2007 年 4 月 13 日に経済産業省から「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」最終報告書 ”情報システム・モデル取引・契約書 ” が発表された。その中で、パッケージを中心としたシステム導入の場合、反復繰り返し型の開発の場合、中小企業ユーザにおける活用の場合等、モデル取引・契約書で十分カバーできていない論点について、業界団体を中心としてさらに議論が深めることが必要であると指摘されている。特に今後ますます広がると考えられる中堅、中小企業でのパッケージ活用、SaaS、ASP 活用などに対する検討が重要と考え、CSAJ/JCSSA では、2006 年に実施してきた共同作業部会を発展させ、情報システム・モデル取引・契約書に関する検討委員会で検討を進めることとなった。

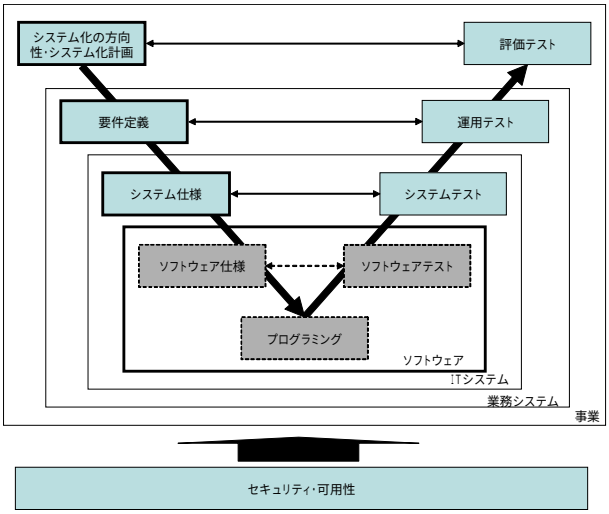
1.2. 目的

「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」最終報告書を踏まえ、パッケージソフトウェア、SaaS、ASP を利用し情報システムの構築、サービスの利用を行う中小・中堅企業と、ソフトメーカー、システムインテグレータ、外部専門家との間の取引慣行・契約に関し課題を明確化し、パッケージソフトウェア、SaaS、ASP の企画、設計、構築、運用、保守にかかわる関係者（ユーザ、システムインテグレータ、メーカー、外部専門家等）の権利と義務、責任の明確化及び信頼性向上に資するガイドライン、モデル契約の策定、政策、普及策の提言を行うこととした。

1.3. ガイドの全体像

1）位置づけ

本ガイドは、平成 19 年 4 月に経済産業省が発表した「情報システム・モデル取引・契約書」を参考にしながら整備しているが、特に、パッケージソフトウェアや SaaS、ASP のシステムライフサイクルの中での企画、設計・開発の工程を対象としている。右図の V 字開発モデルの全体を対象としている。



保守、運用及びセキュリティ・可用性については、それぞれの分冊を参照されたい。

パッケージソフトウェアや SaaS、ASP ではないプログラミング主体の開発を行う場合には、本ガイドを見ながら不足している部分は、経済産業省 ”情報システム・モデル取引・契約書 ” を参照していただきたい。

2）対象とする内容

本ガイドは、パッケージソフトウェアを主体としたプロセスを対象としている。このプロセスは共通フレーム 2007 に準拠する。特に以下の３種類の契約を想定している。

① 企画支援業務、業務要件定義等のパッケージソフトウェア選定及び要件定義支援契約（以下、「業務要件定義支援契約」と記載）

② システム要件定義、カスタマイズ、アドオン、テスト等のソフトウェア設計・制作業務（以下、「システム要件定義支援契約」と記載）

③ システムの開発・実装を行う構築業務契約

④ 上記の一貫契約

特に、ベンダの取引慣行とユーザの予算に起因する齟齬などからトラブルが多数発生している、提案書、見積書等での確認事項などを重点に以下の項目を検討する。

⑤ 仕様、性能、信頼性に関する説明事項、手順

⑥ 保証内容、保証期間（プロダクツライフサイクル）、トラブル発生時の対応窓口、保証対象とならない場合の説明事項、手順

⑦ 最終的に双方が確認する重要事項説明書等の合意プロセスの組み込み

ここで、パッケージソフトウェアを主体といっても様々な導入形態があることから、以下のパターンを検討対象とする。

⑧ 単体パッケージソフトウェアによる開発

- ✓ 概要

  システム導入を１つのパッケージソフトウェア製品により導入する形態

- ✓ 例

  ERP による全社システム
  人事システムのための人事パッケージソフトウェア

⑨ パッケージソフトウェア・インテグレーション

- ✓ 概要

  複数の機能別パッケージソフトウェアを組み合わせて総合的な機能の実現を図るパッケージソフトウェア・インテグレーション

- ✓ 例

  販売管理パッケージソフトウェアと会計パッケージソフトウェアの連携

⑩ SaaS、ASP 等のサービス利用

✓ 概要

システムを自社で持たず、インターネット経由でサービス提供を受ける。

✓ 例

会計ネットワークサービス
CRM ネットワークサービス

また、ユーザが利用するアプリケーションにはパッケージソフトウェアを使わないが、システムの中核機能としてパッケージソフトウェアを使うミドルウェア・インフラパッケージソフトウェアを使用したシステムは、プログラミングをベースとしたシステムと同列の扱いとし、今回対象外とする。

3）前提条件

本ガイドで記述する内容は、以下の条件を前提としている。

パッケージソフトウェアの範囲

対象とするソフトウェアは、一般化された業務フロー、処理、機能を持ち、主にパラメータの設定などで適用できる所謂「プロダクト・パッケージソフトウェア」とする。中核の機能だけ提供し、業務はカスタマイズでプログラムを組み構築するようなソフトウェアは対象としない。また、特定企業で作成したテンプレートしか持たず、汎用的な業務モデルになっていない製品も対象としない。

契約当事者

専門知識を有しないユーザ

専門知識を有する IT ベンダ、システムインテグレータ、外部専門家

例　委託者（ユーザ）： 民間中小・中堅企業、市町村地方自治体　等
　　受託者（ベンダ）： IT ベンダ、システムインテグレータ　等
　　外部専門家　　： コンサルタント　等

開発モデル

経済産業省「情報システム・モデル取引・契約書」パッケージソフトウェア選定モデルに準じる。また、パッケージソフトウェアのカスタマイズ等はウォータフォール型、アジャイル型、反復繰り返し型を想定する

対象システム

企業基幹系、情報系システム

プロセス

共通フレーム 2007 による標準化されたシステム企画・開発・運用・保守プロセスによる

マルチベンダ契約

工程分割発注により、工程毎にベンダを変えることを可能とする。

留意事項

ユーザの IT リテラシーが高いとは限らないため、ユーザ側契約担当者が十分に契約内容を理解できない場合も想定される。契約交渉・締結時には、契約当事者間の情報の質と量、理解に差があることを理解し十分な配慮を行うことが必要である。特に、契約合意に至る交渉プロセスでは、お互いの理解内容を確認しながら進めるなど配慮を行う必要がある。

1.4. 用語

主要な用語は以下に記述する。下記以外の用語は、共通フレーム 2007 の用語解説を参照する。

・モディファイ

パッケージソフトウェアのソースコードの変更を伴うカスタマイズ。

・アドオン

パッケージソフトウェアのソースコードの変更を伴わず、API（Application Program Interface)、外部 I/F、ファイル交換等を利用した外部プログラム。単独で動作するものと、パッケージソフトウェア本体とともに動作する場合がある。

・RFI

Request For Information、情報提供依頼書。

・RFP

Request for Proposal、「提案依頼書」、「提案要望書」、「見積依頼書」などと言う。情報システム調達の際に、ベンダに詳細なシステム提案を行うよう要求すること、またはその調達要件をまとめた仕様書等をいう。

・SaaS

Software as a service、サースもしくはサーズと読む。ユーザが必要とする機能だけを選択し利用可能にしたソフトウェアの形態。もしくは、それを実現するための提供形態・方法（デリバリモデル）を指す場合もある。

・ASP

Application Service Provider。アプリケーションソフトをインターネットを介してユーザに提供するサービス形態。もしくはサービス提供事業者を指す場合もある。

2. パッケージソフトウェアベース開発

2.1. 概要

単体アプリケーションによる開発

必要とする情報システムを 1 つのパッケージソフトウェアにより構築する方式である。全社パッケージソフトウェアを ERP で導入する場合や、人事システムを人事機能専門の総合パッケージソフトウェアで開発する場合がこの方式である。

1）メリット

１つのパッケージソフトウェアをベースにシステム開発をするため、システム開発が容易である。また、パッケージソフトウェアを商品とする時点に、ベンダ内でシステム全体での検証が終わっているため信頼性が高い。

2）デメリット

パッケージソフトウェアは、機能を汎用化するとともに経済性などで取捨選択するので、機能が不十分なことがある。また、パッケージソフトウェア全体のフレームは既に確立されているため、追加機能の付加などのモディファイ（改造）を行うときに制約がある場合がある。

パッケージソフトウェア・インテグレーション

必要とする情報システムを複数のパッケージソフトウェアを組み合わせて構築する方式である。販売や会計など業務分野ごとに最適なパッケージソフトウェアを選定し、一体として運用できるようにする場合がこの方式である。

1）メリット

業務ごとに自社に合った最適のパッケージソフトウェアを選定するので、業務の専門性を高めたり、高度なサービスの実現が可能になる。また、機能に過不足のあるパッケージソフトウェアを無理して使ったりすることがなく、必要な機能を組み合わせられることから、システムを合理的に構成することができる。

2）デメリット

パッケージソフトウェア間のデータの受け渡しなどに問題が生じることがある。また、パッケージソフトウェアごとに操作方法が違うなど、ユーザ・インタフェースが揃わない場合も多い。

ミドルウェア･インフラパッケージソフトウェアの使用（本ガイド対象外）

システムを構成する要素として、パッケージソフトウェアを導入することがある。ユーザの目には触れにくいが、重要な、データ管理、出力などの機能を担うことも多い。

1）メリット

専門性の高い部位、機能に、安定した高度なサービスを求めることができる。

2）デメリット

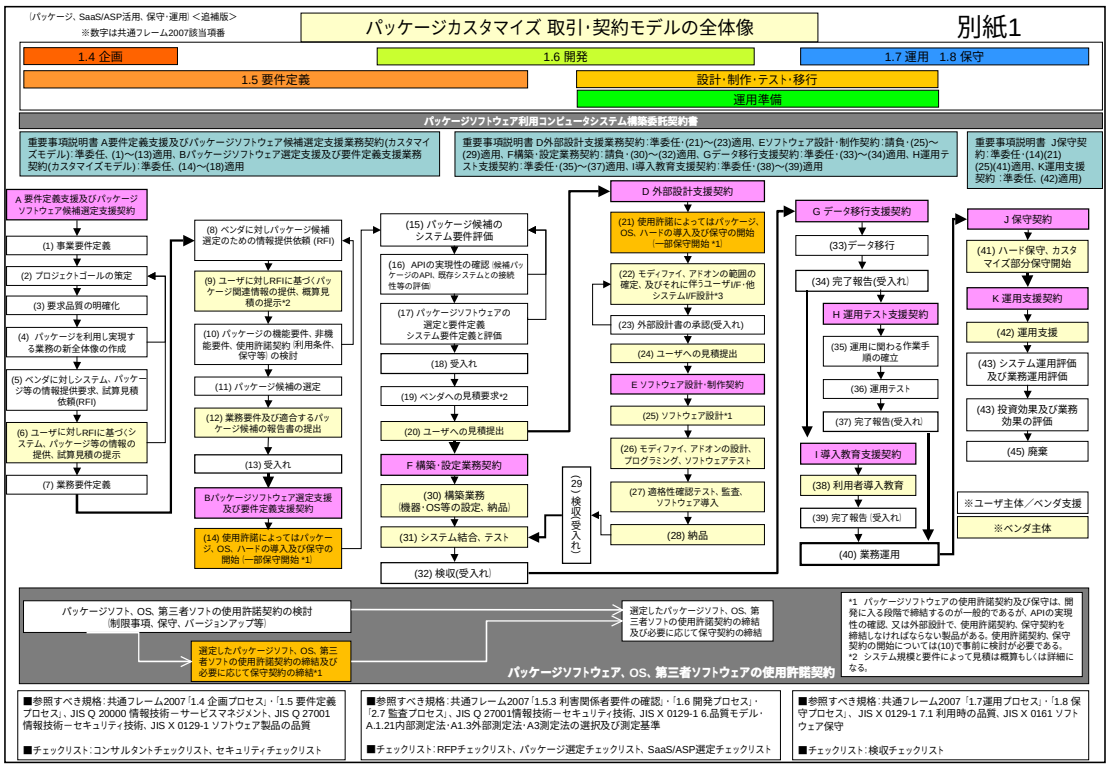
システム内に組み込まれているため、障害の解析などが難しい。

2.2. 主要プロセス

プロジェクトのゴールにむけて企画・開発を行っていく。「業務要件定義」、「開発（システム要件定義）」においては、準委任契約によりコンサルティング契約を外部と結び、その作業を委任することも多い。また、「開発（設計・制作・構築）」では、請負契約が一般的で、テストや教育を準委任契約で契約する場合が多い。契約は、中小規模の契約では一括して行われる場合も多いが、リスクを軽減する意味から、工程ごとに契約を行う多段階契約を行うことを検討する必要がある。

この業務要件定義からシステム要件定義までの過程において、パッケージソフトウェアの持つ設計思想や機能を理解することになるが、その途中で当初考えていたゴール（実現目標）が変更になることもある。また、この過程において、ゴール達成のための必要な機能をパッケージソフトウェアで実現できるのかどうかの検証を行うフィット＆ギャップ分析が重要である。

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報告書で、パッケージソフトウェア活用の場合のモデル契約プロセスが記述されているが、本ガイドでは共通フレーム 2007 との整合を取りながら、以下のように再整理を行っている。



また本モデル契約では、契約書を補完する意味で、重要事項説明書を活用することとしている。建設業界の重要事項説明書と同様に、契約書本体ではないが、この説明をベンダがユーザに行い、設計・開発の基本となる重要事項に関して役割と責任を明確にするとともにユーザの理解を求めることとする。重要事項説明書の説明においては、ユーザの理解に合わせて丁寧に説明を行う必要がある。

2.2.1. 業務要件定義プロセス

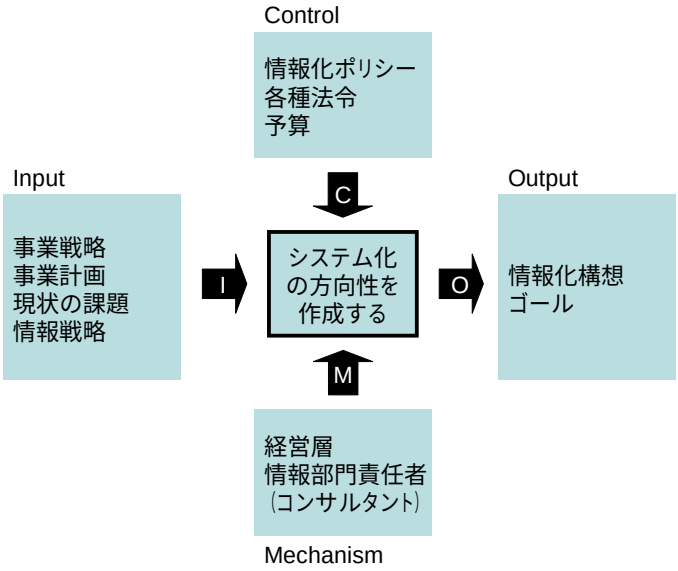
A．システム化の方向性（事業要件定義、プロジェクトゴールの策定、要求品質の明確化）

このプロセスで、業務改革の責任者やシステム責任者は、システム導入を通じて実現したいことを明確にする。

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報告書では、以下のように記述している。

> 「システム化の方向性」、業務部門が、システム開発の前に、経営層が定めた経営方針、全体最適化計画に従い、事業上の目的、システム化の対象業務、システム化のニーズと課題、予算、事業環境を分析し、利害関係者からの要請やその数や役割に応じた規模などに配慮しつつ、システム化するビジネスモデルにつき十分な検討を繰り返し、取締役会等経営層による承認を受けてシステム化の方向性を決定するフェーズである。
>
> ユーザは、ベンダに対し、このフェーズの成果を生かして RFP を発し、ベンダ等から「仮試算見積レベル」の見積提案を受け、これに検討評価を加えて、システム化計画に移行する。
>
> ユーザは、必要に応じて、ベンダ、ＩＴ技術者、ＩＴコーディネータ、システム監査人、情報セキュリティ監査人、公認会計士、弁護士等の専門家との間で支援業務を内容とする準委任契約としてのコンサルティング契約を締結し、これらの作業のための支援を受ける。
>
> （共通フレームのアクティビティ）概ね「システム化構想の立案」に相当する。

業務上のゴールの策定においては、在庫の削減など、構想開始時に考えた視点はもちろんのこと、コストの削減、業務の高度化などの様々な視点から検討をしていく必要がある。パッケージソフトウェアを用いた開発を行う場合には、パッケージソフトウェアの持つ知見やアイデアを調査し、その内容を参照しながら現状の業務体系を見直す。ウォータフォールモデルのようにゴールを達成するための自社専用のシステムを一から作るのではないので、選定したパッケージソフトウェアの思想や機能によってゴールが変わることがあるが、仮のプロジェクトゴール（システム導入の成果）を検討、策定するフェーズである。



日本情報システム・ユーザー協会「ビジネスシステム定義研究 2004」で作成した業務システム仕様書の記述レベルのレベル１が求められる。

仕様の責任と記述項目		レベル 1 ビジネス機能提示	レベル 2 ビジネスプロセス提示	レベル 3 業務フロー提示	レベル 4 業務処理提示	レベル 5 業務処理/データ項目提示
A	ﾋﾞｼﾞﾈｽ機能関連図			IS 部門で企業/事業全体機能定義	IS 部門で企業/事業全体機能定義	IS 部門で企業/事業全体機能定義
B	ﾋﾞｼﾞﾈｽ連携図			業務と対外系/他部門間との連携	業務と対外系/他部門間との連携	業務と対外系/他部門間との連携
C	ﾋﾞｼﾞﾈｽﾙｰﾙ定義書			企業/業務上の戦略ルール	企業/業務上の戦略ルール	企業/業務上の戦略ルール
D	ｼｽﾃﾑ化目標定義書	業務システム化の目標設定	業務システム化の目標設定	業務システム化の目標設定	業務システムの IT 効果定義	業務システムの IT 効果定義
1	ﾋﾞｼﾞﾈｽ機能構成表	ビジネス機能の大分類定義	ビジネス機能の中小分類定義	ビジネス機能の細分類定義	ビジネス機能の細分類定義	ビジネス機能の細分類定義
2	ﾋﾞｼﾞﾈｽﾌﾟﾛｾｽ関連図		ビジネスプロセス間の関連定義	ビジネスプロセス間の関連定義	ビジネスプロセス間の関連定義	ビジネスプロセス間の関連定義
3	業務流れ図			業務処理フロー指示（含む例外処理）	業務処理フロー指示（含む例外処理）	業務処理フロー指示（含む例外処理）
4	業務機能関連図				DFD 方式での上位 DFD として作成	DFD 方式での上位 DFD として作成
5	業務ﾙｰﾙ定義書				業務処理上の社内ルールを定義	業務処理上の社内ルールを定義
6	業務処理手順書				個別の業務処理手順を定義	個別の業務処理手順を定義
7	画面／帳票一覧			基本的に必要な画面/帳票一覧	基本的に必要な画面/帳票一覧	基本的に必要な画面/帳票一覧
8	画面／帳票ﾚｲｱｳﾄ			画面/帳票レイアウトを定義	画面/帳票レイアウトを定義	画面/帳票レイアウトを定義
9	ﾃﾞｰﾀ項目定義書					データ項目の属性を定義
10	運用・操作要件所			業務システムの運用・操作の条件設定	業務システムの運用・操作の条件設定	業務システムの運用・操作の条件設定

B．システム化計画（パッケージソフトウェアを利用し実現する業務の新全体像（BPR） の作成、ベンダに対し情報提供要求、概算見積要求(RFI)、ユーザに対し RFI に基づく情報の提供、ガイドライン適用状況の説明、概算見積の提示）

このプロセスで、ユーザ担当者は、インターネット、書籍、雑誌などを通じて導入できる製品やサービスの情報を収集（カタログ収集等）するとともに、ゴールを達成するための基本方針を検討し、概要の計画を作成する。

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報告書では、以下のように記述している。

「システム化計画」は、業務部門が、システム化の方向性を具体化するために、開発体制、予算、スケジュール、システム化する事業上の要求（例えば、システム化すべき新規事業、社外連携、組織改編、部門間業務分掌変更、法令・契約等のコンプライアンス要件、セキュリティ、個人情報保護、環境など）や対象業務上の要求（例えば、業務内容、業務形態、業務品質、性能目標、運用、移行要件、法令・契約等のコンプライアンス要件、セキュリティ、個人情報保護、事業継続性、環境など）を考慮して、業務範囲や業務分掌、関係者の教育及び訓練計画を定めたシステム化計画書を作成し、ステークホルダの合意を得てから経営層の方針稟議を求め、経営層による承認を受けて、業務部門及び情報システム部門における要件定義に進むフェーズである。

ユーザは、部門間の検討の後、システム化計画を作成して、レビューを繰り返して検討を加え、ベンダに対して RFP を発し、ベンダ等から「試算見積レベル」の見積提案を受ける。これを検討評価して要件定義フェーズに移行する。

ユーザは、システム化の方向性決定フェーズ同様、必要に応じて、ベンダ、ＩＴ技術者、ＩＴコーディネータ、システム監査人、情報セキュリティ監査人、公認会計士、弁護士等の専門家との間で支援業務を内容とする準委任契約としてのコンサルティング契約を締結し、作業のための支援を受ける。

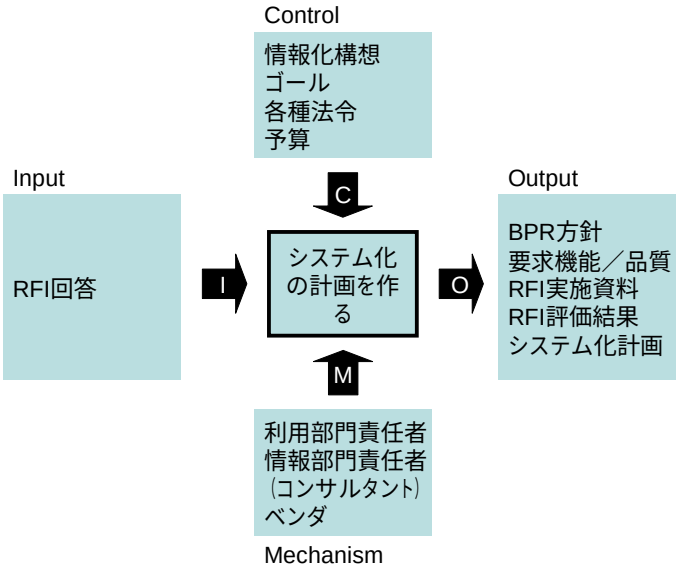
（共通フレームのアクティビティ）概ね「システム化計画の立案」に相当する。

ブラッシュアップした詳細なプロジェクトゴールや要求機能、BPR 方針を作成した後に、RFI によりベンダからの情報提供受ける。それを踏まえ、システムの全体方向性、BPR が検討されるフェーズである。

パッケージソフトウェアは業務の知見を集積しソフトウェアとして提供するものであるので、自社の既存の業務にとらわれることなく、必要に応じてゴールの変更や業務方針の変更を図っていく必要がある。

この工程で作成した成果物にシステムのスケジュールや体制など、システムの具体的な内容を付加して、システム計画書として整理することが望まれる。この概要は、重要事項説明書の前半部分を記載し始めることにより、整理をすることができる。

ここで、(1)～(6)におけるプロセスは、仮説設定、検証を実施していくが、それぞれが独立したプロセスではなく、同時並行的、一体的に推移する場合もあり、大幅な手戻りや見直しが許容される。この時点から外部専門家（コンサルタント等）やベンダの参画を得る場合もある。



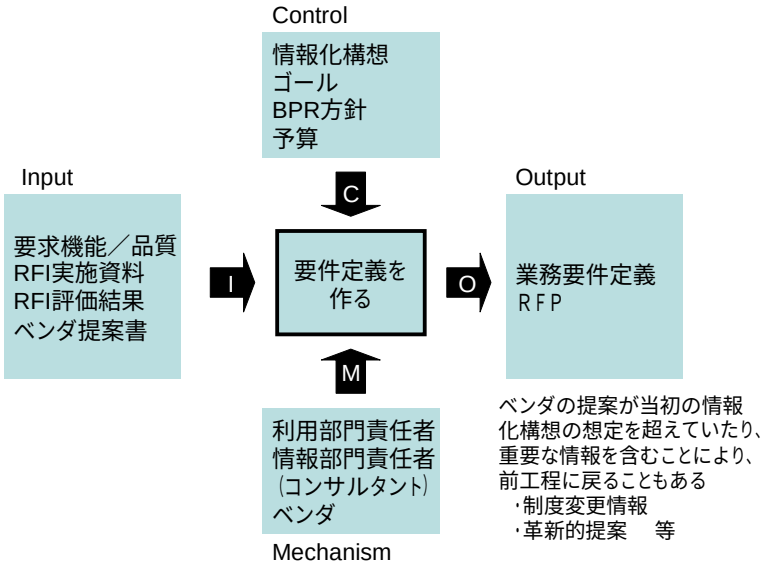
C．業務要件定義プロセス

このプロセスで、ユーザ担当者は、業務で必要な機能を明確にするとともに、現状の業務量や業務の流れを示して、ベンダに対して提案を依頼する。

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報告書では、業務要件定義とシステム要件定義をあわせて、以下のように記述している。

> 「要件定義」は、事業要件を反映したシステム化計画を受けて、業務部門が、業務上の要求を業務要件に、情報システム部門が、システムに実装すべきシステムの機能要件・非機能要件を定義し、経営層による実行稟議、承認を受けるフェーズである。
>
> ここでは、ユーザは、業務要件及びシステム要件を検討して、要件定義書にまとめ、ベンダに RFP を発して「概算見積レベル」の見積提案を受け、これに点検評価を加えて、システム設計に移行する。
>
> そのために、ユーザは必要に応じて、ベンダ、ＩＴ技術者、ＩＴコーディネータ、システム監査人、情報セキュリティ監査人、公認会計士、弁護士等の専門家との間で、準委任契約を内容とする要件定義支援契約、仕様書作成支援契約を締結し、作業のための支援を受ける。
>
> このフェーズの内容の妥当性の検証が、「⑨運用テストフェーズ」である。
>
> （共通フレームのアクティビティ）共通フレーム 2007 で新設される「利害関係者要件の定義」、「利害関係者要件の確認」に相当する。

プロジェクトゴールや要求品質、BPR 方針、業務要求などとシステム化計画をもとに、それを実現するための要件仕様書を含んだ RFP を作成する。前工程でベンダから集めたパッケージソフトウェア情報などを参考にしながら、今回整備するシステムの業務の要件や使用許諾条件等を整備していく。詳細な検討を行うために再度ベンダに問い合わせることもあり、その場合には、再び RFI を実施することとなる。やはり、この工程は専門性も高いため外部専門家（コンサルタント等）やベンダの参画を得る場合も多い。



業務要件定義で作成される要件は、日本情報システム・ユーザー協会「ビジネスシステム定義研究 2004」で作成した業務システム仕様書の記述レベルのレベル２が最低限求められる。本来は業務フローを含むレベル３が必要であるが、それができない場合には次工程以降のフィット＆ギャッププロセスと行き来することによって、後から再定義することとなる。

仕様の責任と記述項目		レベル 1 ビジネス機能提示	レベル 2 ビジネスプロセス提示	レベル 3 業務フロー提示	レベル 4 業務処理提示	レベル 5 業務処理/データ項目提示
A	ﾋﾞｼﾞﾈｽ機能関連図			IS 部門で企業/事業全体機能定義	IS 部門で企業/事業全体機能定義	IS 部門で企業/事業全体機能定義
B	ﾋﾞｼﾞﾈｽ連携図			業務と対外系/他部門間との連携	業務と対外系/他部門間との連携	業務と対外系/他部門間との連携
C	ﾋﾞｼﾞﾈｽﾙｰﾙ定義書			企業/業務上の戦略ルール	企業/業務上の戦略ルール	企業/業務上の戦略ルール
D	ｼｽﾃﾑ化目標定義書	業務システム化の目標設定	業務システム化の目標設定	業務システム化の目標設定	業務システムの IT 効果定義	業務システムの IT 効果定義
1	ﾋﾞｼﾞﾈｽ機能構成表	ビジネス機能の大分類定義	ビジネス機能の中小分類定義	ビジネス機能の細分類定義	ビジネス機能の細分類定義	ビジネス機能の細分類定義
2	ﾋﾞｼﾞﾈｽﾌﾟﾛｾｽ関連図		ビジネスプロセス間の関連定義	ビジネスプロセス間の関連定義	ビジネスプロセス間の関連定義	ビジネスプロセス間の関連定義
3	業務流れ図			業務処理フロー指示（含む例外処理）	業務処理フロー指示（含む例外処理）	業務処理フロー指示（含む例外処理）
4	業務機能関連図				DFD 方式での上位 DFD として作成	DFD 方式での上位 DFD として作成
5	業務ﾙｰﾙ定義書				業務処理上の社内ルールを定義	業務処理上の社内ルールを定義
6	業務処理手順書				個別の業務処理手順を定義	個別の業務処理手順を定義
7	画面／帳票一覧			基本的に必要な画面/帳票一覧	基本的に必要な画面/帳票一覧	基本的に必要な画面/帳票一覧
8	画面／帳票ﾚｲｱｳﾄ			画面/帳票レイアウトを定義	画面/帳票レイアウトを定義	画面/帳票レイアウトを定義
9	ﾃﾞｰﾀ項目定義書					データ項目の属性を定義
10	運用・操作要件所			業務システムの運用・操作の条件設定	業務システムの運用・操作の条件設定	業務システムの運用・操作の条件設定

2.2.2. 開発プロセス

開発は、要件定義に従って設計を行い、実際にシステムを構築していくフェーズである。

A．システム要件定義

このプロセスで、ユーザ担当者は、ベンダからの提案を比較検討し、パッケージソフトウェアを選定するとともに、選定したベンダとともに、画面イメージなどシステムを構築するために必要な詳細機能を明文化していき、構築するシステムを詳細レベルまで定義する。

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報告書では、「要件定義」と「開発」に含まれる。「要件定義」は前項で引用しているのでここでは引用を省略する。「開発」の中では、以下のように記述されている。

> 企画・要件定義段階を経て、ベンダが、ユーザとの間でソフトウェア開発契約に基づいて情報システム開発を展開する段階である。システム設計（システム外部設計）、システム方式設計（システム内部設計）、ソフトウェア設計、プログラミング、ソフトウェアテスト、システム結合、システムテスト、導入・受入支援を経てシステム開発は終了する。
>
> ウォーターフォール型の開発モデルでは、要件定義、外部設計、内部設計、プログラミング等の各工程を明確に区切り、順次実行される。
>
> 他方、反復型では、開発対象を小さな機能単位に分割、機能ごとに各フェーズを繰り返し適用して開発される。プロトタイプモデルでは、工程を区分せずに、ユーザの要望から試作品を作成・提示・評価していくことで開発される。パッケージソフトウェア導入の場合は、要件定義はフィット＆ギャップ評価、システム設計・プログラミングはカスタマイズ（いわゆるアドオンも含む。）に置き換えられる。
>
> しかしながら、どのような開発モデルにおいても、要件定義がそのシステムの挙動を定めること、要件定義にはユーザの参画が不可欠であることに変わりはない。

パッケージソフトウェアを使った開発を行う場合の特徴として、業務要件とパッケージソフトウェアが提供可能な機能の充足度の確認を行うフィット＆ギャップ評価を行うことが重要である。

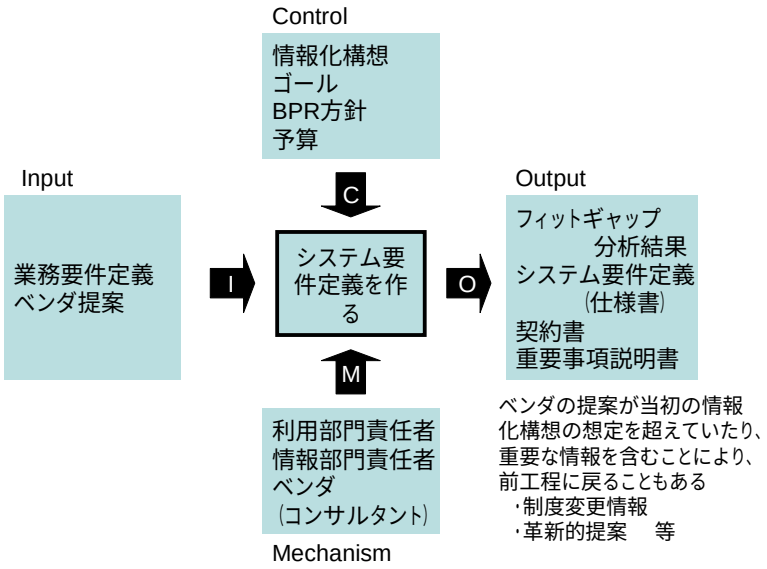
ベンダからの提案を基にしたフィット＆ギャップ評価では、パッケージソフトウェアの適合性、カスタマイズ（モディファイ）やアドオンの必要性、外部インタフェース、既存システムからの移行、要員教育、将来にわたる仕様の拡張性などとともに、運用・保守体制、償却期間におけるトータルコストと得られる効果を、パッケージソフトウェアごとに検証する。

フィット＆ギャップ評価の中で、今回の開発の基本事項に関する矛盾や新たな提案が発見される場合がある。その場合には、フィット＆ギャップ評価に基づき、プロジェクトゴールや BPR の見直しなど、上流工程にさかのぼった変更が許容される。

フィット＆ギャップ評価を得て、パッケージソフトウェアを選定した後に、必要なアドオン、カスタマイズ（モディファイ）、システム構成等を整理し要件定義として取りまとめる。機能の詳細レベルで再度フィット＆ギャップ評価を行うこ

ともある。実機での検証などが必要な場合には、この段階でパッケージソフトウェアやＯＳの導入及び保守を開始する。

ここで、パッケージソフトウェアにない機能をカスタマイズ（モディファイ）で追加することもできるが、パッケージソフトウェアは一定の開発思想と経済合理性をもって設計されているため、ユーザ仕様に適合しない部分を無理にモディファイすることで、一部性能の大幅な低下や、将来の拡張に制限を招く場合がある。モディファイを行う場合には、モディファイによる制限事項やライフサイクルに対する影響に関して留意する必要がある。



パッケージソフトウェアの適合性フィットギャップ評価では、日本情報システム・ユーザー協会「ビジネスシステム定義研究 2004」で作成した業務システム仕様書の記述レベルのレベル３が求められる。業務フローレベルでの評価が求められる。

仕様の責任と記述項目		レベル 1 ビジネス機能提示	レベル 2 ビジネスプロセス提示	レベル 3 業務フロー提示	レベル 4 業務処理提示	レベル 5 業務処理/データ項目提示
A	ﾋﾞｼﾞﾈｽ機能関連図			IS 部門で企業/事業全体機能定義	IS 部門で企業/事業全体機能定義	IS 部門で企業/事業全体機能定義
B	ﾋﾞｼﾞﾈｽ連携図			業務と対外系/他部門間との連携	業務と対外系/他部門間との連携	業務と対外系/他部門間との連携
C	ﾋﾞｼﾞﾈｽﾙｰﾙ定義書			企業/業務上の戦略ルール	企業/業務上の戦略ルール	企業/業務上の戦略ルール
D	ｼｽﾃﾑ化目標定義書	業務システム化の目標設定	業務システム化の目標設定	業務システム化の目標設定	業務システムの IT 効果定義	業務システムの IT 効果定義
1	ﾋﾞｼﾞﾈｽ機能構成表	ビジネス機能の大分類定義	ビジネス機能の中小分類定義	ビジネス機能の細分類定義	ビジネス機能の細分類定義	ビジネス機能の細分類定義
2	ﾋﾞｼﾞﾈｽﾌﾟﾛｾｽ関連図		ビジネスプロセス間の関連定義	ビジネスプロセス間の関連定義	ビジネスプロセス間の関連定義	ビジネスプロセス間の関連定義
3	業務流れ図			業務処理フロー指示（含む例外処理）	業務処理フロー指示（含む例外処理）	業務処理フロー指示（含む例外処理）
4	業務機能関連図				DFD 方式での上位 DFD として作成	DFD 方式での上位 DFD として作成
5	業務ﾙｰﾙ定義書				業務処理上の社内ルールを定義	業務処理上の社内ルールを定義
6	業務処理手順書				個別の業務処理手順を定義	個別の業務処理手順を定義
7	画面／帳票一覧			基本的に必要な画面/帳票一覧	基本的に必要な画面/帳票一覧	基本的に必要な画面/帳票一覧
8	画面／帳票ﾚｲｱｳﾄ			画面/帳票レイアウトを定義	画面/帳票レイアウトを定義	画面/帳票レイアウトを定義
9	ﾃﾞｰﾀ項目定義書					データ項目の属性を定義
10	運用・操作要件所			業務システムの運用・操作の条件設定	業務システムの運用・操作の条件設定	業務システムの運用・操作の条件設定

システム要件定義では、日本情報システム・ユーザー協会「ビジネスシステム定義研究 2004」で作成した業務システム仕様書の記述レベルのレベル４が求められる。レベル５の内容は、次工程の設計以降で達成される。

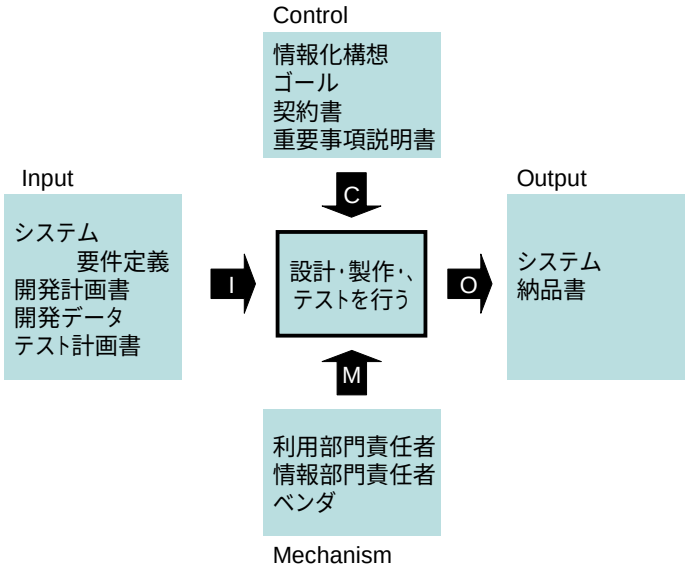
仕様の責任と記述項目		レベル 1 ビジネス機能提示	レベル 2 ビジネスプロセス提示	レベル 3 業務フロー提示	レベル 4 業務処理提示	レベル 5 業務処理/データ項目提示
A	ﾋﾞｼﾞﾈｽ機能関連図			IS 部門で企業/事業全体機能定義	IS 部門で企業/事業全体機能定義	IS 部門で企業/事業全体機能定義
B	ﾋﾞｼﾞﾈｽ連携図			業務と対外系/他部門間との連携	業務と対外系/他部門間との連携	業務と対外系/他部門間との連携
C	ﾋﾞｼﾞﾈｽﾙｰﾙ定義書			企業/業務上の戦略ルール	企業/業務上の戦略ルール	企業/業務上の戦略ルール
D	ｼｽﾃﾑ化目標定義書	業務システム化の目標設定	業務システム化の目標設定	業務システム化の目標設定	業務システムの IT 効果定義	業務システムの IT 効果定義
1	ﾋﾞｼﾞﾈｽ機能構成表	ビジネス機能の大分類定義	ビジネス機能の中小分類定義	ビジネス機能の細分類定義	ビジネス機能の細分類定義	ビジネス機能の細分類定義
2	ﾋﾞｼﾞﾈｽﾌﾟﾛｾｽ関連図		ビジネスプロセス間の関連定義	ビジネスプロセス間の関連定義	ビジネスプロセス間の関連定義	ビジネスプロセス間の関連定義
3	業務流れ図			業務処理フロー指示（含む例外処理）	業務処理フロー指示（含む例外処理）	業務処理フロー指示（含む例外処理）
4	業務機能関連図				DFD 方式での上位 DFD として作成	DFD 方式での上位 DFD として作成
5	業務ﾙｰﾙ定義書				業務処理上の社内ルールを定義	業務処理上の社内ルールを定義
6	業務処理手順書				個別の業務処理手順を定義	個別の業務処理手順を定義
7	画面／帳票一覧			基本的に必要な画面/帳票一覧	基本的に必要な画面/帳票一覧	基本的に必要な画面/帳票一覧
8	画面／帳票ﾚｲｱｳﾄ			画面/帳票レイアウトを定義	画面/帳票レイアウトを定義	画面/帳票レイアウトを定義
9	ﾃﾞｰﾀ項目定義書					データ項目の属性を定義
10	運用・操作要件所			業務システムの運用・操作の条件設定	業務システムの運用・操作の条件設定	業務システムの運用・操作の条件設定

B．設計・製作・テスト

このプロセスで、ユーザ担当者は、開発の進捗についてベンダから報告を受けるとともに、実装機能の問い合わせなど、必要に応じてシステム実装に関する調整を実施する。

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報告書では、「開発」に含まれる。前項で引用しているのでここでは引用を省略する。

開発プロセスは、パッケージソフトウェアベンダによるもの、パッケージソフトウェアそのものの開発者ではないが導入のみ行うシステムインテグレータによるもの、それぞれの再委託によるものと多岐に渡ってさまざまなケースが想定される。守秘義務と品質保証、受入テスト、検収に至る一連のフェーズについて、役割の明確化と十分な事前合意が必要である。



2.2.3. 移行・運用準備プロセス

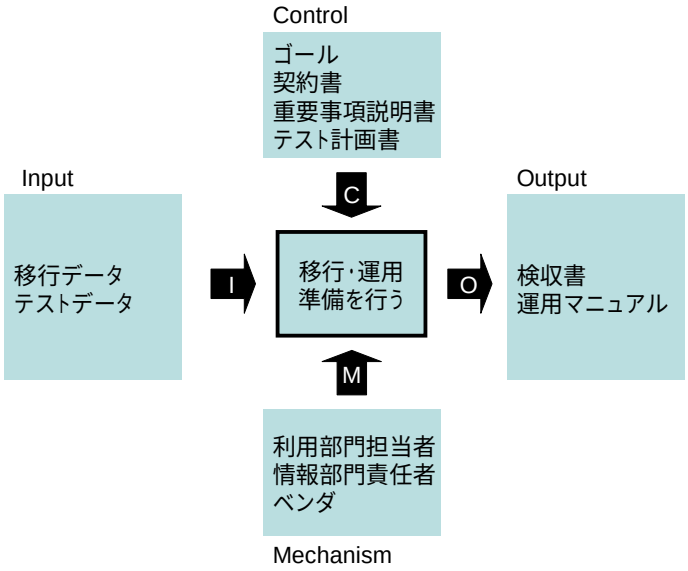
このプロセスで、ユーザ担当者は完成したシステムを実業務として実施してみて、納品物の検収を行うとともに、利用部門の習熟を図る。

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報告書では、「開発」の中で「導入・受入支援」、「保守運用」の中で運用テストのみが以下のように記述されている。

> 「導入・受入支援」は、疑似環境又は実環境にソフトウェアを導入し、ユーザのソフトウェア受入れレビュー及びテストを支援するフェーズである。
>
> （共通フレームのアクティビティ）概ね「ソフトウェア導入」「ソフトウェア受け入れ支援」に相当する。

> 「運用テスト」は、疑似運用環境等での運用テストの実施と実運用環境に移行を実施するフェーズである。
>
> （共通フレームのアクティビティ）概ね「運用テスト」「業務及びシステムの移行」に相当する。

パッケージソフトウェアの移行・受入準備では、パッケージソフトウェアの持つデータ移行機能の確認を行う必要がある。また、利用者の教育には、ベンダが開催するパッケージソフトウェア操作に関する基礎的な研修が用意されている場合も多い。研修開催スケジュールの確認やモディファイした部分の研修などを調整する必要がある。


Control
ゴール
契約書
重要事項説明書
テスト計画書
Input
移行データ
テストデータ
C
I
移行･運用
準備を行う
O
Output
検収書
運用マニュアル
M
利用部門担当者
情報部門責任者
ベンダ
Mechanism

2.3. 関係者の役割分担

システム開発ではユーザの利用部門の責任者が責任を負うが、情報システム部門は技術面から支援をする必要がある。また、トラブルの多発する RFP や要件の確定においては、現場とベンダが協力して行い、情報システム部門は調整を行う必要がある。

項目	ユーザ (現場)	ユーザ (ｼｽﾃﾑ)	ベンダ	備考
プロジェクトゴールの策定	◎	○	―	
要求品質の明確化	◎	○		
BPR 方針の策定	◎	○		
システム化の方向性	◎	○		
RFI	◎	○		
ベンダ情報評価	◎	○		
システム化計画	◎	○		
RFP	◎	○		
RFP の内容確認	○	△ 調整役	○	
ベンダ提案受付	◎	○		
フィット＆ギャップ分析	◎	○	△ 支援	ベンダは必要な情報提供を行う
パッケージソフトウェア選定	◎	○		
要件定義	◎	○		
要件の詳細項目確認	○	△ 調整役	○	
モディファイ・アドオンの設計、開発	◎	○		

外部専門家が作業に参加するときには、ユーザのシステム部門と同じ立場になる。

ユーザ企業にシステム部門がいない場合

ユーザ部門の現場が責任を持つが、実質的には外部専門家が作業を行い、ユーザ部門は確認のみ行う場合が多い。

項目	ユーザ (現場)	専門家	ベンダ	備考
プロジェクトゴールの策定	◎（確認）	◎（実質）	―	
要求品質の明確化	◎（確認）	◎（実質）		
BPR 方針の策定	◎（確認）	◎（実質）		
システム化の方向性	◎（確認）	◎（実質）		
RFI	◎（確認）	◎（実質）		
ベンダ情報評価	◎（確認）	◎（実質）		
システム化計画	◎（確認）	◎（実質）		
RFP	◎（確認）	◎（実質）		
RFP の内容確認	◎（確認）	◎（実質）	○	
ベンダ提案受付	◎（確認）	◎（実質）		
フィット＆ギャップ分析	◎（確認）	◎（実質）	△ 支援	ベンダは必要な情報提供を行う
パッケージソフトウェア選定	◎（確認）	◎（実質）		
要件定義	◎（確認）	◎（実質）		
要件の詳細項目確認	◎（確認）	◎（実質）	○	
モディファイ・アドオンの設計、開発	◎（確認）	◎（実質）		

2.4.　ベンダの説明事項と手順

2.4.1.　業務要件定義プロセス

a．システム化の方向性

このフェーズで契約する場合の成果物は、情報化構想やシステム化の方向性に関する報告である。報告には、今後システム化を進めていく上での方針や要求すべき機能や品質の概要が記述される。

外部支援を受けたときに起こる契約上のトラブルは以下の事項である。

1）システム方針が経営者の満足する内容になっていない。

この工程におけるベンダの説明事項と手順、確認ポイントを以下に整理する

説明事項

・システム方針（情報化構想）

システム全体の基本方針と将来構想を記述したもの。

・ゴール

業務やシステムを通じて実現したいゴールを記述したもの。

保証内容、保証期間（プロダクツライフサイクル）、トラブル発生時の対応窓口、保証対象とならない場合に関する説明事項

ここで決める内容はあくまでも概要であり、保証の対象外とする

成果物イメージ等

① 専門家選定時の説明事項、手順

この工程から外部専門家を活用する場合には、付録のチェックリストによる確認を実施し、当該外部専門家が実施プロジェクトに適しているか評価する必要がある。

② 時の説明事項、手順

提案時には、ユーザの要望をヒアリングしたベンダが、ユーザの行いたいことを提案書として整理し、書面により確認を行う。
確認項目は以下の内容である。付録の外部専門家のチェックリストで評価する。

・背景
・目的
・実施したいこと
・目標指標
・実施手順

・成果物イメージ
・予算とその範囲
・体制と役割分担

また、契約時までに経営層の確認を受ける。

2） 程終了時の説明事項、手順

① 報告書（説明資料のみの場合もある）を基に、提案で記述された内容について説明していく。
② 途中の合意を持って、提案内容を変えた場合には、その変更内容も含めて確認を行う。
③ チェックリスト（フェーズ０）による確認
④ 上記を確認後、経営層の承認を受けることで終了する。

3） 終的に双方が確認するための合意プロセス

契約形態に依存するが、基本的には、業務部門が作成したものを情報システム部門がレビューし、最終的に、経営層が承認を与えることが必要である。
① 担当者レベルで内容確認
② 利用部門責任者による内容確認
③ 合意文書で承認

運用・保守との連携に関する留意事項

このフェーズで運用・保守の詳細までは記述しないが、運用・保守が問題なく行える体制について検討をしていく必要がある。

セキュリティ・可用性に関する留意事項

最低限維持すべきセキュリティ・可用性の要件を明確化する。「停止時間は８時間以内のこと」などのように具体的に記述する。詳細レベルまでは記述する必要はない。

別冊付録のセキュリティチェックリストで必要なセキュリティレベルの確認を行う。

その他留意事項

なし

B．システム化計画

このフェーズで契約する場合の成果物は、システム化計画書である。システム計画書には、システム化方式、機能の概要が記述されるとともに、具体的な実現方法、スケジュールなどが記述される。

外部支援を受けたときに起こる契約上のトラブルは以下の事項である。

1）システム計画書に具体性が無く、システム設計に詳細化していくことができない。

2）システム計画書が、技術や期間などの面から実現不可能であり、システム設計に進めない

この工程におけるベンダの説明事項と手順、確認ポイントを以下に整理する

説明事項

・BPR 方針

業務改革を行う基本的な視点や方針を記述したもの。

・要求機能・品質

このプロジェクトで実現すべき機能の定義や要求品質を記述したもの。

・システム計画書

システムの具体的な計画が記述されたもの。

保証内容、保証期間（プロダクツライフサイクル)、トラブル発生時の対応窓口、保証対象とならない場合に関する説明事項

ここで決める内容はあくまでも概要であり、保証の対象外とする

成果物イメージ等

① 部専門家選定時の説明事項、手順

この工程から外部専門家を活用する場合には、付録の外部専門家チェックリストによる確認を実施し、外部専門家はそのチェック項目の内容をユーザに説明しなければならない。その情報をもとにユーザは、実施プロジェクトに適しているか評価する必要がある。

② 案時の説明事項、手順

提案時には、ユーザの要望をヒアリングしたベンダが、提案書として、ユーザの行いたいことを整理し、資料により確認を行う。
確認項目は以下の内容である。付録の外部専門家のチェックリストで評価する。

・目的
・目標指標
・実施手順

・成果物イメージ
・予算とその範囲
・体制と役割分担

また、契約時までに経営層の確認を受ける。

3） 工程終了時の説明事項、手順

① 報告書（説明資料のみの場合もある）を基に、提案で記述された内容について説明していく。
② 途中の合意を持って、提案内容を変えた場合には、その変更内容も含めて確認を行う。
主な説明項目は以下の通りである。
・システム計画により初期目的が達成する根拠
・システム計画が実施可能な根拠
③ チェックリスト（フェーズ１）で確認する。
④ 確認後、経営層の承認を受けることで終了する。

4） 最終的に双方が確認するための合意プロセス

契約形態に依存するが、基本的には、外部ベンダもしくは業務部門が作成したものを情報システム部門がレビューし、最終的に、経営層が承認を与えることが必要である。

運用・保守との連携に関する留意事項

このフェーズで要求機能や品質において、運用時間や必要な運用体制など、必ず留意しなければならない運用・保守の要件を記述する。この段階では、実行方法の詳細は不要としても、大まかなレベルの指定、設定は必要である。要件として定義できる程度に、要求が明確になっていなければならない。ベンダも技術的に実現可能かどうかの判断が求められる場合がある。

セキュリティ・可用性に関する留意事項

このフェーズで、セキュリティ・可用性の要件を記述する。扱う情報の重要度や２４時間運用など、構想時点で留意しなければならない項目を必ず記入する。

その他留意事項

なし。

C．要件定義プロセス

業務要件を整理したうえで RFP による提案依頼が実施され、ベンダの提案を受け付ける。このフェーズで契約する場合の成果物は、業務要件定義書、提案依頼書（RFP）である。この作業により、今回構築するシステムが実装すべき業務機能や開発方法などが明確に規定される。

外部支援を受けたときに起こる契約上のトラブルは以下の事項である。

1）業務要件定義に具体性が無く、システム要件定義に詳細化していくことができない。

2）業務要件定義が、制度、技術や期間などの面から実現不可能であり、システム要件定義に進めない

3）実施した RFP の記述内容が不十分であり、後工程でトラブルが発生する

この工程におけるベンダの説明事項と手順、確認ポイントを以下に整理する

説明事項

・業務要件定義書

業務（システムではない）の要求機能、品質などを規定するもの。

- ✓ 最低限確保されるべき応答時間や処理時間などの操作性に代表される品質要件は BPR に密接に関連し、技術要件にも大きな影響を及ぼすため、早期に優先度と重要度を明確にすることが望ましい。また、セキュリティ、既存システムからの移行、運用・要員教育、保守等において特段に配慮すべき項目もあわせて抽出しておくことが望ましい。特に、(7)業務要件定義は、現場で運用に携わるオペレータや、利害関係者とプロジェクトゴールの共有や、システム化計画の周知と同意を得ておくことが重要で、プロジェクトチームと BPR に直面する現場の調整に留意すべきである。

・RFP

業務要件とともに各種提案条件を記述するもの。ベンダに提示を行う。

保証内容、保証期間（プロダクツライフサイクル）、トラブル発生時の対応窓口、保証対象とならない場合に関する説明事項

RFP の記述内容の不備という問題が後工程で見つかった場合には、当該作業を実施した外部専門家は善管注意義務に問われることもあることを説明していく必要がある。ユーザ事由により要件未確定であったものの問題を問うことはできないが、常識的に必要な検討が行われていないことによる問題は外部専門家が責任を負う必要がある。

要件未確定部分がある場合には、そのことを書面によって明記することが重要である。

成果物イメージ等

1）業務要件定義時の説明事項、手順

業務要件を後工程で変更すると、予算、スケジュール、品質などに大きな影響が生じることを説明する必要がある。業務要件定義書のテンプレートを基に、記述内容にぬけがないか、記述内容は十分か確認を行う必要がある。

2）RFP 実施時の説明事項、手順

RFP の意味、責任範囲、RFP で記述される要件の詳細、RFP の配布対象について説明を行う。特に、契約時に正式仕様を決定するが、そのもとになるのが RFP であり、RFP がユーザの責任において作成される公式文書であることの理解を得ることが重要である。
RFP の記載内容を、チェックリストを使いながら確認を行う。

3）FP での第三者評価の実施

RFP によるトラブルを防ぐために RFP の確認（監査）サービスを使うことが考えられる。その場合には、RFP のチェックリストのチェック内容を再確認するとともに、ユーザＩＴ成熟度チェックリストにより、ユーザのＩＴに関するレベルも測定し、ユーザにも正しい処置を求める必要がある。

4）パッケージソフトウェア選定時の説明事項、手順

パッケージソフトウェア選定時の評価項目をユーザに説明する必要がある。また、選定の対象とするパッケージソフトウェアの選定理由を明確に説明する。

5）工程終了時の説明事項、手順

① 報告書を基に、提案で記述された内容について説明していく。
途中の合意を持って、契約開始時の提案内容を変えた場合には、その変更内容も含めて確認を行う。
主な説明項目は以下の通りである。
・業務要件定義書 RFP の記載内容
・パッケージソフトウェア選定と判断根拠
・システム計画により初期目的が達成する根拠
・システム計画が実施可能な根拠
② チェックリスト（フェーズ２）で確認する。
③ これらの確認を行った上で、重要事項説明書の作成を行い、確認後、経営層の承認を受けることで終了する。

6）最終的に双方が確認するための合意プロセス

契約形態に依存するが、基本的には、ベンダもしくは業務部門が作成したものを情報システム部門がレビューし、最終的に、経営層が承認を与えることが必要である。各種成果物と重要事項説明書による確認を行った後、業務完了確認書兼検収書により双方の最終確認を持って合意する。

運用・保守との連携に関する留意事項

このフェーズで業務要件定義書の非機能要件の定義において、運用時間や必要な運用体制など、運用・保守の要件を明確に記述する。

セキュリティ・可用性に関する留意事項

このフェーズで業務要件定義書において、セキュリティ・可用性の要件を明確に記述する。要件は見積もりに影響するので、二重化などのシステム構成に影響する内容、バックアップに対する対応やアクセスログなどの機能を付加するなど、一般的な機能よりも多くの機能を要する場合には必ず記入する。

その他留意事項

なし

2.4.2. 開発プロセス

A．システム要件定義

このフェーズで契約する場合の成果物は、システム要件定義書、重要事項説明書である。この作業により、今回構築するシステムの実装すべき機能や実際に適用される開発方法などが明確に規定される。

この工程で外部支援を受けたときに起こる契約上のトラブルは以下の事項である。

1）システム要件定義に具体性が無く、システム設計に詳細化していくことができない。

2）システム要件定義が、技術や期間などの面から実現不可能であり、システム設計に進めない

この工程におけるベンダの説明事項と手順、確認ポイントを以下に整理する

説明事項

・フィット＆ギャップ分析結果

ベンダからの提案内容の要求への整合状況、パッケージソフトウェア選定の考え方について説明を行うもの。

- ✓ パッケージソフトウェアに対するモディファイについては、そもそもパッケージソフトウェアが想定していない運用を求めることによって、パッケージソフトウェアの構造そのものの変更などがありえる。そのため、モディファイやアドオン機能の工数と実現性について詳しく評価を行うべきである。
- ✓ フィット＆ギャップ評価においてベンダの参加を求める場合、当該作業の内容と責任の所在を決めることが重要である。また、複数ベンダからの提案書およびフィット＆ギャップ評価を求める場合は、書式の統一、用語の定義等に配慮し、相互理解に十分な時間をかけることが信頼性確保につながることに留意すべきである。

・システム要件定義書

システムの要求機能、品質などを規定するもの。

- ✓ パッケージソフトウェアの保守期間は、前提となる OS やハードウェアの世代交代、保守打ち切りに影響される場合がある。パッケージソフトウェアの保守期間、ハードウェアの保守期間とともに OS の動向、保守打ち切りの際の移行、費用についても事前に調査、想定することが望まれる。
- ✓ 最終仕様の決定においては、画面の遷移や帳票の形式、運用手順等を、現場オペレータの参画と承認を得るとともに、導入に備えた教育計画が必須である。導入後の手直しや変更を最低限に留めることは、信頼性向上とコストに重大な影響を及ぼすため、十分に留意す

る。

- ✓ パッケージソフトウェアに対するカスタマイズによって、基本機能に制限が加わるなどの他の機能に及ぼす影響と、非機能要件に及ぼす影響について確認し、要件定義とする。
- ✓ ハードウェア、ネットワークの高性能化、低価格化に伴い、データ量の増大とデータの分散が顕著である。信頼性要件、セキュリティ要件の観点から、要件定義の最終評価を行うとともに、これらが付随的要件でないことに留意し信頼性を確保されたい。
- ✓ 対象となるパッケージソフトウェアのプログラムは、(1)パッケージソフトウェアの基本機能部分、 (2)画面、帳票などの何らかの設定を前提としている部分、(3)新たに開発されるアドオン部分に分類される。プログラム変更、改修が(1)に係る場合は、信頼性に多大な影響を及ぼすとともに、将来に渡る保守が得られない場合もある。パッケージソフトウェアベンダと開発ベンダ、ユーザとの十分な相互理解と承認を得た上で、プログラム変更、改修を実施されたい。

・重要事項説明書

ベンダがユーザに説明し、同意を取るべき重要事項が記述された文書であり、契約書の付帯文書である。

保証内容、保証期間（プロダクツライフサイクル)、トラブル発生時の対応窓口、保証対象とならない場合に関する説明事項

システム要件定義書の記述内容や記述レベルはトラブルの最大の原因となる。要件定義書に関する内容の保証は契約上難しいので、十分な確認を行うことが重要である

成果物イメージ等

1）パッケージソフトウェアのフィット＆ギャップ分析実施時の外部専門家契約時の説明事項、手順

フィット＆ギャップ分析を行うときに、製品ベンダにフィット＆ギャップの契約を別途行うことがある。このときに確認のみおこなう、追加費用の算定までおこなうなど、作業範囲を明確に示す必要がある。

2）提案時の説明事項、手順

提案時には、提案書として、ユーザの行いたいことを整理し、資料により確認を行う。
確認項目は以下の内容である。
・実施手順
・成果物イメージ
・予算とその範囲
・体制と役割分担
また、契約時までに経営層の確認を受ける。

3）システム要件定義書確定時の説明事項、手順

システム要件を説明する前提として、フィット＆ギャップ分析の結果を解説し、今回のパッケージソフトウェアが選定された検討プロセスとその結果を明確に説明する。また、システム要件の中で、パッケージソフトウェアから提供される機能、設定が必要な機能、カスタマイズを行う機能を明確に説明する必要がある。
付録のパッケージソフトウェア選定チェックリストも活用し、パッケージソフトウェア全体の確認をすることが望まれる。
パッケージソフトウェアの設定について合意した場合には、この時点で、設定等合意書の作成を行う。

4）契約書確定時の説明事項、手順

契約金額、期間等の契約基本事項を説明するとともに、モデル契約書との差異を説明する。特に、瑕疵担保期間など利害関係として大きく取り上げられる案件についてはユーザがわかるまで十分な説明をする必要がある。さらに、付帯文書である重要事項説明書を使って、ユーザとベンダの責任境界を明確にするとともに、両者がサインすることにより、基本事項について合意をしなければならない。

5） 工程終了時の説明事項、手順

① チェックリスト（フェーズ３）により確認を行う。
② システム要件定義書、重要事項説明書の説明をもって工程を終了する。

6） 最終的に双方が確認するための合意プロセス

契約形態に依存するが、基本的には、外部ベンダもしくは業務部門が作成したものを情報システム部門がレビューし、最終的に、経営層が承認を与えることが必要である。
契約がこの時点で終了する場合には、重要事項説明書で確認を行い、業務完了確認書兼検収書を作成する。また設定の合意をした場合には、設定等合意書も合わせて確認を行う。

運用・保守との連携に関する留意事項

このフェーズで作るシステム要件定義書において、運用・保守のシステム的な要件を具体的に記述する。運用については、運用サポート機能など機能的な内容だけではなく、必要な運用体制などについても言及をする必要がある。

セキュリティ・可用性に関する留意事項

このフェーズで作るシステム要件定義書において、セキュリティ・可用性の要件を記述する。実装すべき技術標準やリカバリー手順など運用に必要な各種条件まで言及を行う。別冊付録のセキュリティ詳細チェックリストを活用する。

その他留意事項

パッケージソフトウェアベンダとシステムインテグレーションベンダが異な

る場合、システムインテグレーションベンダで解決できない不具合や仕様変更が想定される。ベンダ間の協力体制、パッケージソフトウェアベンダとユーザにおける保守契約も合わせて選定評価の基準とすることが望まれる。大規模なカスタマイズなどの場合、進捗の報告について、時期、内容、終了の判断基準、進展の条件などの合意を事前に行うことも必要である。

B．設計・製作・テスト

このフェーズで契約する場合の成果物は、システム本体及び設計書、運用マニュアルなど付帯ドキュメントである。

この工程で外部支援を受けたときに起こる契約上のトラブルは以下の事項である。

1）システム要件定義に記述されていない追加要件などの扱い

2）システム要件定義に記述されていない、非機能要件の実装

設計、製造、テストでの、進捗の報告について、時期、内容、終了の判断基準、進展の条件などの合意を事前に行うことも必要である。同様に終了時での判断基準、終了条件を事前に行うことが必要である。

この工程におけるベンダの説明事項と手順、確認ポイントを以下に整理する

説明事項

・システム開発関連ドキュメント

システム開発に関連して生成されたドキュメント。

保証内容、保証期間（プロダクツライフサイクル）、トラブル発生時の対応窓口、保証対象とならない場合に関する説明事項

システムは瑕疵担保責任の範囲内で不具合の修正が行われる。ただし、システムの不具合は、瑕疵なのか仕様なのか、また誰の責任範囲で起こった問題なのか切り分けることは非常に難しい。障害分析などの初期作業を円滑に行うためにも、開発ベンダと保守契約しておくことが望ましい。保守契約を結ぶことにより保守窓口も明確になる。

成果物イメージ等

1）提案時の説明事項、手順

提案時には、業務要件定義書で示されない項目の扱いを明確にするとともに、仕様変更発生時の手続きや費用の扱いなどについて説明を行う。

2）工程終了時の説明事項、手順

設計書および付帯文書、重要事項説明書の説明をもって工程を終了する。

3）最終的に双方が確認するための合意プロセス

契約形態に依存するが、基本的には、外部ベンダもしくは業務部門が作成したものを情報システム部門がレビューし、最終的に、業務責任者が承認を与えることが必要である。ベンダは作業完了報告書を作成し、ユーザは検査をした上で検査合格通知書兼検収書を作成する。

運用・保守との連携に関する留意事項

このフェーズでは、早い段階から運用・保守担当者との調整を行っておくことが望ましい。テストフェーズにおいて、運用上の問題を明確にする。

セキュリティ・可用性に関する留意事項

このフェーズで作るシステム要件定義が実現されているかの確認を行う。

その他留意事項

受入テスト、検収については、実際の運用を想定したシナリオテストをベンダとユーザにおいて事前検討するとともに、シナリオテストに使用するデータによってテストの信頼性が大きく異なることから、使用データについてはベンダと十分な協議が望まれる。大規模なカスタマイズなどの場合、進捗の報告について、時期、内容、終了の判断基準、進展の条件などの合意を事前に行うことも必要である。

2.4.3. 移行･運用準備プロセス

このフェーズで契約する場合の成果物は、修正済みの設計書、運用マニュアルなど付帯ドキュメントである。ここで要件の実装状況が確認される。

1）移行運用ドキュメントの不備。

2）プロジェクトゴールや業務要件と納品物のギャップ

この工程におけるベンダの説明事項と手順、確認ポイントを以下に整理する

説明事項（報告書に下記項目を記載もしくは別添）

・システム要件定義書

各システム要件が実装されていることを確認する。

・運用マニュアル

ベンダからの提案内容の要求への整合状況、パッケージソフトウェア選定の考え方について説明を行うもの。

・各種設計ドキュメント

保守が可能なレベルで記述された設計ドキュメント。

・重要事項説明書

各重要項目が実現されていることを確認する。

保証内容、保証期間（プロダクツライフサイクル）、トラブル発生時の対応窓口、保証対象とならない場合に関する説明事項

移行や運用の保証は、通常は開発の保証に含まれる。

成果物イメージ等

1）工程終了時の説明事項、手順

テスト結果の報告書及び教育訓練の報告をもって工程を終了する。成果指標を設定していた場合には、その検証も実施する。
検収のチェックリストを活用する。

2）最終的に双方が確認するための合意プロセス

契約形態に依存するが、基本的には、外部ベンダもしくは業務部門が作成したものを情報システム部門がレビューし、最終的に、業務責任者が承認を与えることが必要である。

運用・保守との連携に関する留意事項

実現されているか確認を行う。

セキュリティ・可用性に関する留意事項

実現されているか確認を行う。

その他留意事項

受入テスト、検収については、実際の運用を想定したシナリオテストをベンダとユーザにおいて事前検討するとともに、シナリオテストに使用するデータによってテストの信頼性が大きく異なることから、使用データについてはベンダと十分な協議が望まれる。

3. サービス調達（SaaS、ASP）

3.1. 概要

ユーザが自己保有するシステムにアプリケーションを導入し、自社もしくは委託先に運用を委託する従来の情報システム購入モデルがある。それに対しネットワークを通じてベンダが所有するシステムの上でサービスを利用し業務を行う情報サービス利用モデルがある。

また、SaaS はネットワークを通じて情報システムによるサービスを受けるが、システム開発と同様の特徴がある部分と差異がある部分がある。その特徴を整理する。

	SaaS	システム開発	備考
導入	低価格ですぐに導入できる	SaaS などに比べて導入までの時間がかかる	
サービス変更	月次等一定期間を区切りにして変更できるところと、できないところがある	一旦開発したら変更することはできない	システム開発の場合、サービスの変更は保守または変更になる。
途中解約	可能なところと、一定期間は不可なところがある	一旦開発したら、使うしかない（または廃棄）	
サービス停止時の対応	回復を待つしかない	自社での対応が可能（体制や能力のある場合）	
データバックアップ	オプションサービスの有無による	自由に設定できる	
セキュリティ	ベンダの示した情報で判断	自由に設定できる	
民事再生時の対応	サービス停止	事前調整可能	
天災時の対応	回復を待つしかない	自社での対応が可能（体制や能力のある場合）	
ベンダの瑕疵	ベンダにより対応が分かれる	責任を問える	

1）メリット

サービス導入が短期間にでき、高信頼なサービスが利用できる。また常に最新のバージョンを使い続けることが可能である。

2）デメリット

個別対応ではなく共同で利用する仕組みなので、自社独自などの機能追加要望などに対して対応できない場合がある。インフラなどの信頼性は高いが、障害発生時に自分でコントロールをすることができない。

従来からも ASP といわれるネットワーク型のサービスは提供されていたが、SaaS では、

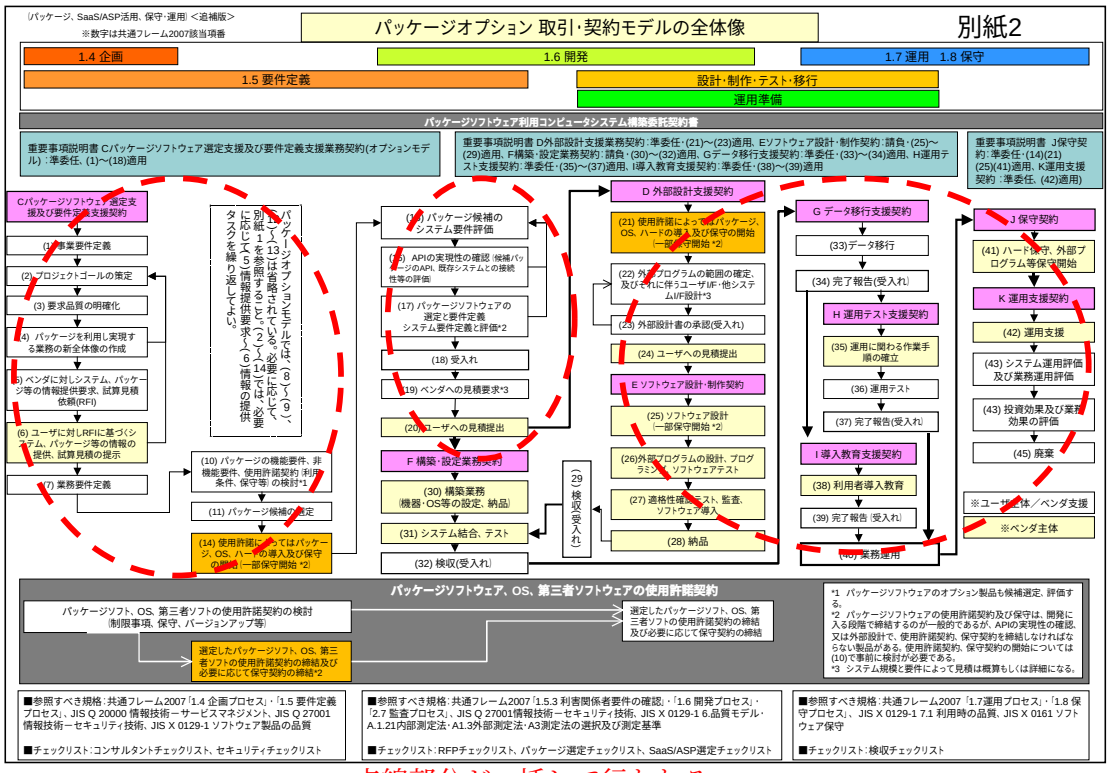
複数企業に同じプラットフォームを使ったサービスを行うマルチテナント方式を使うとともに、Three-Tier と呼ばれる。ユーザの画面、処理のプロセス、データベースが分離され、ユーザは画面表示のブラウザしか持たないモデルが一般的である。

実現形態	システムアーキテクチャ	ユーザ・インタフェース	業務ロジック	データベース
		画面表示、イベント発生	画面遷移、データ処理、DB アクセス	DB 管理
自社システム	Stand-Alone	Client	Client	Client
ASP	Two-Tier	Client	Client	Server
SaaS	Three-Tier	Client	Server	Server

システムの導入ではなくサービスの利用になるので費用の構造もこれまでと変わってくる。サービス利用契約を行っている期間に定額料金を支払う定額料金型とユーザ数やデータ量によって費用を変動させる従量型の課金が一般的に導入されている。

3.2. 主要プロセス

SaaS では、開発ではなくあらかじめ提供されている機能を利用するという形態をとるためパッケージソフトウェア開発のように方針などの検討や機能の検討は短期間で一括して行われることが多い。また、開発がなく、各種設定と移行作業などが行われ導入される。一般的なプロセスを記述する。

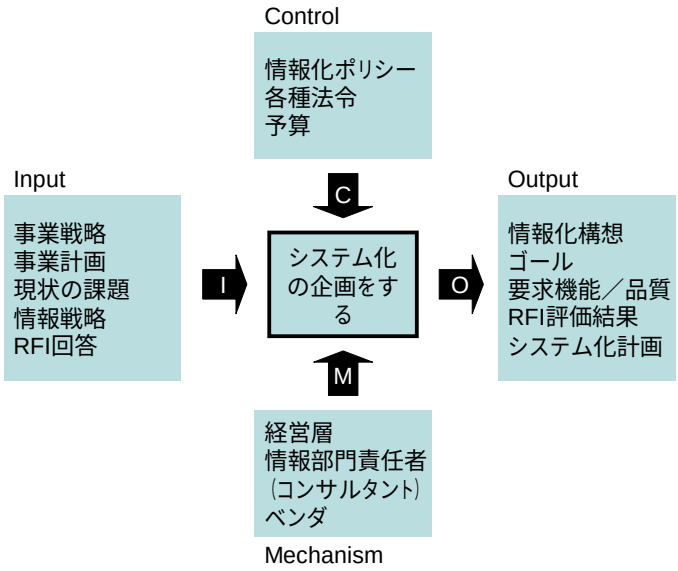


点線部分が一括して行われる。

3.2.1. 企画プロセス

このプロセスで、業務改革の責任者やシステム責任者は、システムを通じて実現したいことを明確にする。また、ユーザ担当者は、インターネット、書籍、雑誌などを通じて導入できる製品やサービスの情報を収集（カタログ収集等）するとともに、ゴールを達成するための基本方針を検討し、概要の計画を作成する。

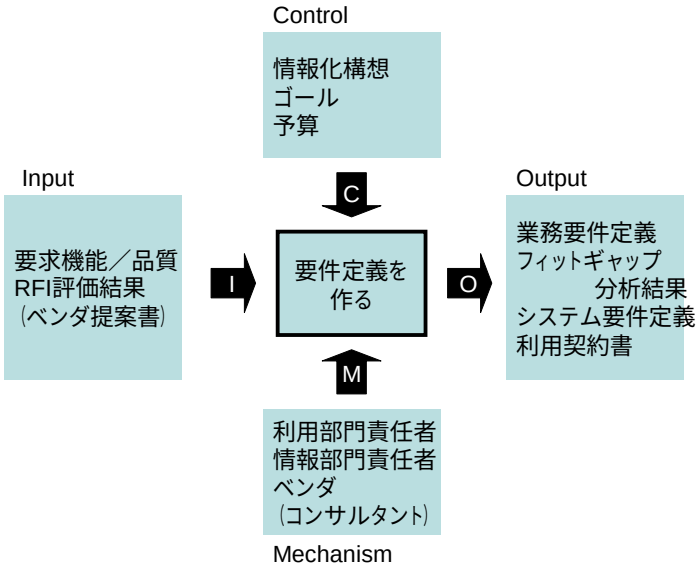
このプロセスの流れは、パッケージソフトウェア開発と同じであるので記述を省略する。(2.2.1 参照)



3.2.2. 要件定義、開発 (システム要件定義) プロセス

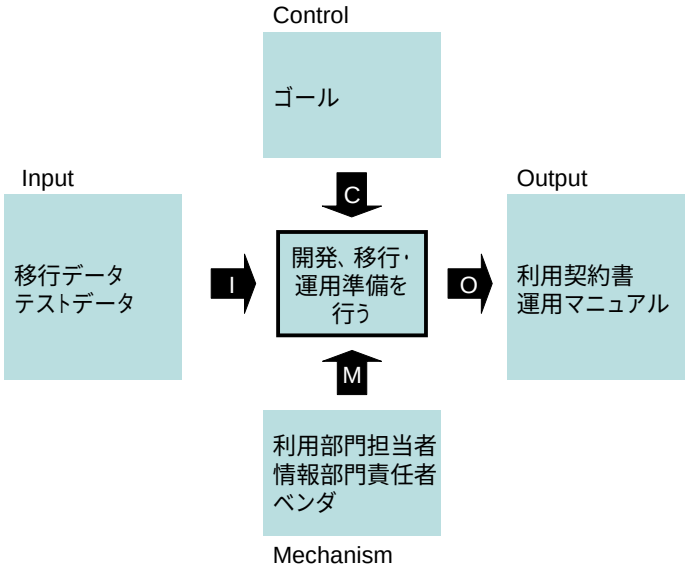
このプロセスで、ユーザ担当者は、業務で必要な機能を明確にするとともに、現状の業務量や業務の流れを示して、ベンダに対して対応可否などの提案を依頼する。(グループウェアなどのカスタマイズを要しないシステムでは、必ずしも提案を求めない）また、ユーザ担当者は、仕様（ベンダから提案があるときは提案）を比較検討し、サービスを選定する、このとき、多くの SaaS ベンダでは試行利用を可能としているので、試行の中で機能を確認する。

また利用するオプションや、社内の他システムとの連携方法を定義していく。



3.2.3. 開発(設計・製作・テスト)、移行・運用準備プロセス

利用契約を結んだ上で、ユーザ担当者はオプションなどの機能の設定を行うとともに、他システムの連携などがある場合にはその確認をする。また、研修を行い利用部門の習熟を図る。



3.3. SaaS での課題と必要な対応

これまでの ASP の導入、SaaS 導入を通じて、ユーザの不満や要求はあるものの契約上のトラブルはほとんど報告されていない。システムのようにこれから未知のものを構築するのではなく、既にあるサービスを納得して使うというのが SaaS のポイントであり、そのため契約上のトラブルまでは発展していない。しかし、利用者にまったく不満や不安がないわけではなく以下のような注意点に配慮する必要がある。

1）機能不足

サービスの機能をユーザが理解していない、もしくは誤解が生じる場合がある。ユーザ側の「こういう機能を期待していた」「標準的な機能かと思っていた」などの期待値がそのままクレームへと発展する場合があるため、ベンダは、サービスの機能について詳細にユーザ側に説明する必要がある。ユーザも試行利用期間等を通じて検証を十分に行う必要がある。

2）サービスの停止（ベンダ都合）

ベンダ側の都合（サーバメンテナンス、プログラム修正、バックアップ作業など）で一時的にサービスを停止する際に、「事前に聞いていなかった」「その時間帯はサービスをどうしても使いたい」といったユーザのクレームが起こる場合がある。ベンダは、契約時にその旨をしっかりと伝え、さらに停止の際にはユーザに事前に承諾もしくは通知する必要がある。ユーザも停止があることを理解し、業務を停止したり、社内にローカルバックアップしたデータで代用するなど、必要に応じて対策を講じる必要がある。

3）サービスの停止（故障など）

災害時や通常環境でのハードウェアの故障、ソフトウェアの不具合などでサービスが停止してしまう場合がある。ベンダ側は停止しないよう最大限の努力を行う必要があるが、発生してしまった場合は速やかに復旧の作業を行うとともに、回復予測などの情報公開を行う。また、ベンダは復旧にかかる時間（保証時間）、その場合の課金の扱いを利用契約などであらかじめ明示しておく必要がある。

4）サービスの中止

サービス提供会社の倒産などでサービスの維持が難しくなった場合、サービスそのものが中止される場合がある。事前に倒産時のサービス維持についての契約事項を盛り込むことが必要である。

5）レスポンスの遅延

サービスレベル自体が通信環境に左右されるという特性を持っているため、ユーザ側の通信環境によっては満足いくレスポンス速度が得られないという場合がある。事前に実環境での運用テストを行う必要がある。また、ベンダは利用規約、場合によっては契約書にサービスの実行環境についての条件を明示する必要がある。

6）個別環境（ハードウェア、ソフトウェア）での不具合

ユーザ側の個別の環境（ハードウェア、ソフトウェア）ではそれぞれソフトウェアやハードウェアの組み合わせによる競合によってサービスがうまく動かない場合がある。ユーザは、事前に実環境でのテストを行う必要がある。また、ベンダはあらかじめサービスの実行環境について詳しい条件を明示する必要がある。

7）途中解約とスケールダウン

ユーザ側の都合により途中解約やユーザ数の減少などのスケールダウンをする場合がある。この場合の契約条件や手続きが明示されていないと、ユーザに予想外の違約金などが発生することがある。契約前に確認をする必要がある。

8）データの保全

ベンダがデータの流出、誤消去などを行ったときの補償範囲を明確にしておかないと事故発生時に問題が発生することとなる。契約等で確認をする必要がある。

9）データ移行

ユーザの都合で他者サービスや自社システムへの変更などを行うときには、これまでのデータを移行することを求められる場合が多い。データ移行のためのデータの変換または、移行ツールの提供をしているかを、ベンダはユーザに明示する必要がある。

10）マッシュアップサービスでの不整合

複数のサービスを組み合わせて使うマッシュアップサービスでの不整合は標準化されたインタフェースを使う SaaS では通常おきないが、これまでに事例などがある場合には、ユーザに開示する必要がある。

11）SaaS プラットフォームにおける障害

SaaS 提供企業が他社のプラットフォーム上でサービスを提供する場合、プラットフォーム停止時の責任を明示する必要がある。

12）価格改定

サービス利用途中での価格改定が行われると、ユーザにとっては受諾せざるを得ない場合も多い。価格改定の方針、猶予期間などの有無等についてユーザに明示する必要がある。

3.4. 関係者の役割分担

システムの検討から導入まで一貫してユーザ責任によって作業を実施する。外部専門家が導入を支援する場合でも、基本的にユーザ業務の実装だけが業務であり、また、利用開始後にユーザがサービス内容を変更することも可能なことからユーザの責任によって作業を行う。

SaaS ベンダの責任範囲は利用規約に記述されている範囲内であり、その内容を十分に説明する義務を負っている。このためユーザは利用時でのリスクに関して十分かつ詳細な確認事項を準備してあたる必要がある。

3.5. ベンダの説明事項と手順

SaaS 導入時の説明は、ホームページによる説明と書面の利用規約（利用契約）のみで行われる場合も多い。また、小規模での試行導入からスタートするユーザも多いことから、トラブル以前にサービスをすぐに中止するユーザもいる。前項で記述された課題を回避するために、ベンダは以下の説明事項をユーザに明示していく必要がある。

説明事項

・サービス機能の詳細説明

提供する機能について記述したもの。

・利用時の規約（制限事項など）

停止予定など利用時に制限事項があることなどを記述したもの。

・安全性

安全性についてどのような対策を採っているか記述したもの。

・データ保全方法

データのバックアップ方法や管理方法について記述したもの

・運用保証

どのくらいの稼働率を保証するのか、または、実績を公開するのかを記述したもの

・運用体制の説明

ユーザ側に必要な運用体制について記述したもの

・移行・導入作業の流れ

移行と運用の流れについて記述したもの

保証内容、保障期間（プロダクトライフサイクル）、トラブル発生時の対応窓口、保証対象となる免責事項に関する説明事項

サービスは利用契約に記述された範囲で保証されるが、一般に、インターネットプロバイダなどの SaaS ベンダに起因しない基盤に関する障害に関しては保証されない。

手順

ベンダからの情報が書面などによる場合には、付録のチェックリストにより確認を行っていく。不明な点に関してはベンダに問い合わせを行う。ベンダはチェックリストに提示されている事項について情報開示していくことが望まれる。

その後納得したら、利用契約を締結する。

運用・保守との連携に関する留意事項

サービス停止時での業務継続方法については、ユーザ側で考慮が必要。

セキュリティ・可用性に関する留意事項

ユーザから見えないところでシステムが稼動しているので、データのバックアップ体制などに関する確認を念入りに行う必要がある。各種認証の有無、ディスクの多重化、データ拠点の多重化、アクセス管理方法などを確認する。特にデータが国外にある場合には、国内法が適用されない場合があるので留意が必要である。

その他留意事項

なし

4. アジャイル開発･プロトタイピング

4.1. 概要

情報システムが企業内の業務で使われるだけではなく、インターネットを経由して一般の利用者にも直接利用されるようになって久しい。今では非常に多くの人がオンラインショッピング、オンラインゲーム、株などの金融取引や行政手続までをインターネットを経由して利用している。情報技術は日進月歩し、利用者の数は急激に増加した。新しいサービスも次から次に生み出されている。言い換えると日々進化する情報システム、新しい価値を提供できるシステム、予測できない事態に早急に対応できるようなシステムが求められるような情況になったといえる。また、オープンソフトウェアに代表されるように、実現する技術についても取捨選択していく時代になった。このような情況を考えると、従来のように結果をしっかりと予測し一から順番に積み上げていくウォータフォール型の開発では予期せぬ事態に即座に対応できない、もしくはもっと別な方法のほうがより適切であるというようなケースも生まれてくる。そこで採用されることになったのがアジャイル型開発という考え方である。

アジャイル開発はまず目的と、その目的を果たすための主要な機能を実現し（プロトタイプ作成)、必要に応じて適宜修正を加えていく考え方である。常に利用者に対しては稼動する完成品の形を成している。当然、計画的に機能を追加していく（反復開発的要素）ようなケースもある。重要なことは目的につながるシステムの価値が常に提供され続けることである。アジャイル型開発における反復は、その結果として何らかの価値が提供されなければならない。

1）メリット

変化の激しい環境において、ゴールに向けて短期間に臨機応変にサービスが提できるので、業務に対する価値を提供しやすくシステム開発リスクが小さい。

2）デメリット

ゴールに向かってとはいえ、予算の全体像を立てにくい。また、ユーザとベンダとの強固な信頼関係が重要である。

アジャイル型開発や反復繰り返し型と呼ばれる開発手法は、実際に機能するソフトウェアの提供に重点を置く手法である。実際に機能するという意味で、そのソフトウェアの実用度を早期に確認できるという特徴がある。

ウォータフォールモデルは上流から下流にむけて企画→要件定義→基本設計→詳細設計→運用テスト→運用というプロセスを踏むことから、万一、要件定義そのものに誤りがあった場合、その誤りはリリースまで判明しないという構造的欠陥が指摘されている。言い換えれば、ウォータフォールモデルでは、要件定義、外部設計でのレビューにおいて、設計書段階でのシミュレーションと確認を重ねることによって、手戻りを防止するモデルである。さらに、要件定義確定後の業務の変更や拡大が少なく、変更があっても予想可能な範囲にとどまるビジネスモデルであるとともに、発注者側が業務全般の説明能力に長けていることが信頼性確保の前提である。

アジャイル型開発は要件定義そのものを、ユーザとともにプロトタイプの開発を通

じて行ってしまおうという考え方にたつ。いわば、対話型のプログラムやユーザ・インタフェースを実環境で実際に構築し、使い勝手やレスポンスの評価を得て、要件そのものを定義していくアプローチである。ユーザ自身で要件定義が困難であったり、ビジネスの範囲が成長、拡大している際に有効なアプローチである。反復繰り返し型異なるのは、オンサイト（ユーザのオフィスや実際のシステムの使用場所）開発、一定期間の間に顧客が選択した機能を作りこむなどの、独特のプラクティスに従う点にある。

機能要件を決定し、非機能要件を満たすリソースを求めるという意味で、銀行の ATM システムの開発においては、ウォータフォールモデルが明らかに優位である。あらかじめ、ATM で提供される機能は要件として定義が可能であり、画面のレスポンス等の非機能要件もユーザがビジネス上の重要な要件として定義することができる。こうした機能要件、非機能要件を実装できるハードウェア、通信環境、システム環境を選択し、必要なリソースを確保して開発にかかることで、運用テストにおける諸問題がどこにあるのかを追求するのも容易であると言える。

反面、ユーザ自身が機能要件を決定できない場合や、応答性や画面遷移といったユーザビリティが顧客満足度や生産性に影響を与えるシステム構築では、ウォータフォールモデルのシミュレーションでは限界がある。反復繰り返し型開発やアジャイル型開発は、このような状況において適用が可能な開発モデルである。

4.2. 主要プロセス

アジャイル開発手法のプロセスを図示すると次のようになる。一旦完成したシステムは、さらに要求分析を繰り返し、改良を続けていくような形となる。ある意味では完成することはないとも言える。

システムに求められる価値は常に提供され続ける。結果として時間をかければかけるほど価値のあるシステムとなることが求められる。一方で価値にならない機能を提供することがあってはならない。そのため、価値のある機能の検討精度を上げるためにも、リリース後の効果測定を行いながら要求を検討することも必要である。

4.3. 企画･開発時の要点

主要な参加メンバーが実現するサービスや業務について熟知していることが前提に

なる。さらに実装をするメンバーを含むメンバー間のコミュニケーションが重要になる。結果としてプロジェクトメンバーの数には制約が出る、参加できるメンバー個々の能力もそれなりに要求されることになる。

アジャイル開発手法を採用する場合には何を実現しようとしているのか、開発しようとしているシステムの目的はどこにあるのかというような点を十分に検討して採用すべきである。明確な目的が設定されていないと、要求を判断する際の指標が無いため、正しい判断が行えないためである。目的が明確でなければ、検討の方向性が曖昧になり、結果として出来上がるシステムも曖昧な形になることが多く、結果として無駄な投資がかさむことが証明されている。目的が複数設定されている場合は、目的に優先順位を設定することが求められる。実際のプロジェクトでは複数の目的が設定されていることも珍しくない。

目的に繋がる価値の検討において、しばしば議論になるのは、価値に繋がる要求の大きさである。ビジネスの価値とその要求の大きさは直交する関係にあるため、要求の大きさは大小まちまちである。また、この要求の大きさは開発計画に密接に関係する。

あらかじめ達成すべき目的が予測可能な時、つまり誰がいつ、どうような使い方をして、どれくらいのトラフィックがあるのかなどがわかっているとき、また将来変動するような可能性が無いような場合にはアジャイル開発手法を採用するメリットは生まれてこない。

以下、アジャイル開発手法の代表的なものとされるエクストリームプログラミング（以下 XP）について重要とされる点は以下のようなものである（参考：エクストリームプログラミング入門、wikipedia）

（XP における基本的事項）

XP では次の「４つを価値」が必要なものとして挙げられている。

1)　コミュニケーション

顧客、管理者、プログラマがそれぞれに対し即時に率直に質問できること。

2)　シンプルであること

動作させるために必要な最低限のところから始めて必要なものを付け加えている戦略をとること。

3)　フィードバックが常になされること

常にテストによって確認し、評価し、計画を修正し、結果を見せていくこと。

4)　勇気を持つこと

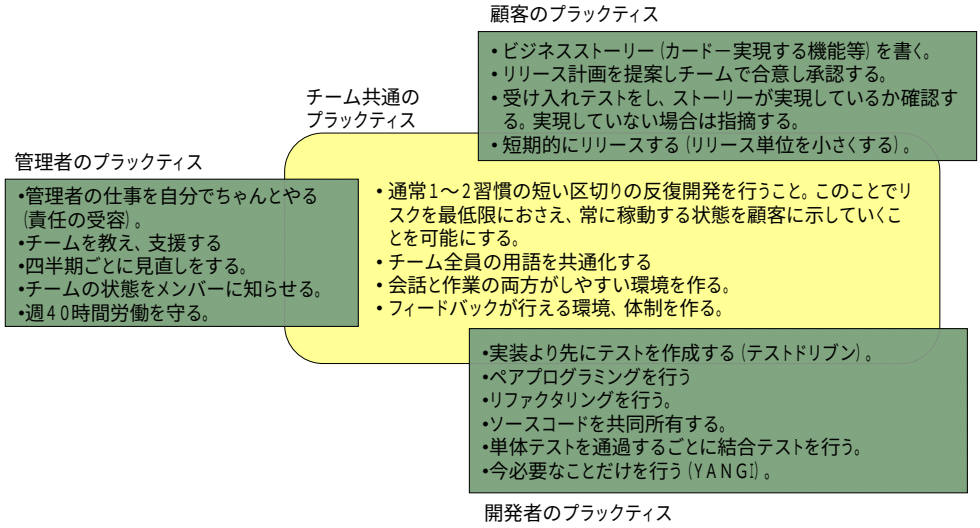
上記の３つを前提にして、大胆な取捨選択、改善、後退、挑戦を行う勇気を持つこと。

4.4.　関係者の役割分担

従来、ウォータフォール型開発では、開発依頼者が開発者に対してシステム構築を丸投げするような形を取ることがあった。開発依頼者はどういうものが出来上がるかということ、どういう機能を実現したいかということに対して常に決断と決断の責任を負う。開発者も要求される要件に対してその実現の可否の判断を速やかに行い、採用できる技術に基づき合意できる決着点を示す必要がある。したがってシステム化の

対象となるビジネスを深く理解している人間が深く関与することは、アジャイル開発には特に欠かせないものである。

同様に、アジャイル開発手法の代表的なものとされるエクストリームプログラミングについての関係者のプラクティスは以下のようなものである（参考：エクストリームプログラミング入門、wikipedia）



これらの中には単独でも機能するものを多く、部分的な採用も多く行われている。

但し、実装の部分に関連しているものが多く、要求定義の部分はビジネスストーリーとして与えられるという点には注意を要する。

4.5. ベンダの説明責任事項

開発依頼者に対して、採用する開発手法の選択に当たって十分な説明を行いその合意を得なければならない。さらに採用するにあたっては、開発依頼者とベンダー（開発者）側はお互いの役割分担とコミュニケーションの確立に当たってお互いに十分な理解を得なければならない。特に開発依頼者がアジャイル開発手法に対する理解、開発への参加の度合いが非常に濃密なものになることを理解することは不可欠である。

4.6. 留意事項

アジャイル型は、反復繰り返し型をもとに発展的にさまざまなプラクティスや原則を定義したもので、さまざまなモデルが存在している。モデルによっては大規模開発に向かないと言われているものもあるため、留意点が異なってくる。

アジャイル型では、開発手法によってさまざまなプラクティスが提唱されており、ユーザとベンダがそのプラクティスを正しく理解することが信頼性確保においては重要である。代表的な手法であるエクストリーム・プログラミング(XP)では、オンサイト開発や、テスト手順を定めてから実装を行うテスト駆動型開発、反復ごとにユーザによる受け入れテストを行うなどのプラクティスが定められており、従来のソフトウェア開発の慣行とは大きくかけ離れた特徴がある。開発者にとっても高い技術力と従来にない管理を要求することから、反復繰り返し型の留意点を踏まえ、ユーザ、ベンダの双方のプラクティスの実現方法、管理方法を契約書に明記する必要がある。

動作するシステムから得られる効果を検証しながら要件定義が確定し、プログラムが完成した段階で設計が完成するため、ソースコードの保守性、可読性を高めるためのリファクタリングと呼ばれる作業が、信頼性向上においては大きく影響を及ぼす。リファクタリングの実現方法について、ユーザ、ベンダでの詳細な取り決めは、将来の保守性を高めるために有用である。

反復繰り返し型、アジャイル型を含め、プラクティスにドキュメントが定められていないことを理由にドキュメントを作成しないことは誤りである。可読性の高いコードの創出とともにユーザにおける信頼性、保守性を確保するためのドキュメントの作成は重要である。XP においてもテクニカルライタの重要性が指摘されており 、プロジェクトの特徴と優先順位を鑑みたドキュメントのあり方を、ユーザ、ベンダで合意することに留意されたい。特に取扱説明書のようなプログラムで表現できないドキュメントについては、それ以外のドキュメントが事前に作成されない関係上、より精緻なものが要求されることとなる。

5. 繰り返し型開発

5.1. 概要

システム開発を行うとき、さまざまな事情から、最初にすべて実現すべき内容が決定できるとは限らない。そのような場合、すでに内容が決定している主要な機能から順次、開発、実現していくような形が考えられる。実際のシステム開発は現状ではウォータフォール型の開発といえども何らかの意味で繰り返し型開発的な要素を持っているといえる。大きな違いは、開発されるユニットを 1 つの価値としてそれごとに確立していくという点である（契約単位にすること）。

5.2. 主要プロセス

次に図示するようなプロセスである。

5.3. 企画･開発で起こるﾄﾗﾌﾞﾙ

どういうシステムが求められているのか明確に開発依頼者と開発者が合意しなければならないことなどウォーターフォール型開発と基本的にまったく同様である。利用者に対してリリースできるレベルでテストまでを含むプロセス単位を小分けにするので、プロジェクトとしてのリスクを軽減することが出来る。

反復繰り返し型の場合は、上流から下流にむけての流れを繰り返すことによって、「統合・テストがすんで安定している『部分として』完成したシステムをリリースすることである。」 とされている。言い換えれば、初期に仕様を完全に定義するのではなく、開発構想書や概要レベルの要求一覧表などをもとに、数週間単位で イテレーション（要求分析、設計、実装、テスト）を繰り返し、段階的に詳細化して仕様の完成度を高めていく開発手法である。イテレーションの流れはウォータフォールモデルに準じており、企画、要件定義の不備は運用テストで明らかになることから、これらの不備に対しては次のイテレーションの企画、要件定義で反映されることになる。同様にイテレーションにおける実装段階では、要件の変更は行わず、次のイテレーションでの課題として引き継がれていく。こうすることで、定められた期間での進捗と完成度を求め、全体の工数見積に反映させていく。

・反復繰り返し型の場合でも、要件定義が信頼性に大きく影響を及ぼすことは同様である。開発構想書や概要レベルの要求一覧表で想定していなかった課題を要求事項として反映するための企画、要件定義プロセスをおろそかにすると、無用なイテレーションを繰り返すこととなる。また、次のイテレーションへのフィードバックを得る

ためのテストにおけるユーザの関与（評価）方法とテスト計画の変更管理、新たなイテレーションでの企画、要件定義の変更管理が必要である。一連の管理が不十分なままイテレーションが繰り返されると信頼性が大幅に損なわれることに留意する。

・要件定義の先送りなどによる無用なイテレーションを防ぐため、実現が必要な機能の優先順位の設定と、量的制限 を契約書に明記しておく必要がある。ユーザとベンダで、見積における積算根拠と作業結果の評価方法を事前に合意しておき、あらかじめ定めた反復回数で作業の見直しを行うことを契約に定めておくことが重要である。場合によっては、期間を定めた数回のイテレーションを見積のために契約し、その後、詳細見積、契約を締結するなどを検討すべきである。

5.4. 関係者の役割分担

ウォータフォール型の開発と基本的に同様である。

5.5. ベンダの説明責任事項

ウォータフォール型の開発と基本的に同様である。

6. 付録

6.1. 付録１ パッケージソフトウェア開発でのトラブル例と必要な対応

企画設計に起こるトラブルは、RFP に起因する内容とその後の要件仕様確定によって起こることが多い。以下が多くの場合で指摘される主な課題である。

（1）不十分なＲＦＰ（要求仕様書）

（2）過大なモディファイ、アドオン

（3）パッケージソフトウェアの機能・サービスレベル不足

（4）仕様外の要求

（5）検収時点での要求不一致

（6）既存、追加ソフトウェアとの不整合

（7）優越的地位の利用

（8）知的財産の帰属

（9）開発中止時の精算

（10）パッケージソフトウェア間インターフェースに起因する問題

（11）システム内で障害が切り分けられない場合

（12）パッケージソフトウェアのバージョンアップに起因する問題

（13）パッケージソフトウェアのサポート切れの問題

(1) 不十分な RFP（提案要求書）

ユーザの作成した RFP の内容が不十分であり、提案内容が絞りきれない場合がある。そのため提案内容に過不足が発生し、その後の要件定義の段階で詳細化しないまま進めると、設計途上や検収において、どちらの責任か問題となることがある。ユーザ側の意見として「プロならば RFP や仕様の不十分さを専門知識で補完せよ」、ベンダ側の意見として「仕様の確認はユーザとベンダとの間で書面で交わしているので、記述されていないことは対象外」といった議論が起こることが多い。

ユーザ側は、業務の暗黙知を仕様で表現できていないことも多く、また、ベンダの技術的な提案を理解できていない場合が多い。ベンダも、説明や要件を聞きだす努力が不足していることも見られるため。十分な留意をする必要がある。

また、RFP の作成に外部専門家を活用する場合もあるが、外部専門家が必要十分な仕様を作成できていない場合もある。コンサルティングを依頼するときには成果物イメージと記述レベルを契約前に十分に打ち合わせする必要がある。

	ユーザ	ベンダ	外部専門家
原因	RFP の記述方法を知らない。 RFP を作る時間が取れない	不十分な RFP を容認している RFP の内容を勝手に解釈している	RFP 作成支援において、十分な RFP を作っていない場合がある
主な対策	ユーザの業界に精通する第三者による RFP 評価・監査的なものを入れる	要件定義にする段階で十分な詳細化を図る	ユーザの業界に精通する第三者による RFP 評価・監査的なものを入れる
契約での留意点	RFP に記載されていない追加変更事項の扱いを契約書に記載する	同左	RFP に必要な項目が記載されない等、明確な不備があった場合の善管注意義務があることを契約締結時に確認する。

(2) 過大なモディファイとアドオン

フィット＆ギャップ分析後にパッケージソフトウェア選定を行うが、この後の詳細要件を定義していく中で、各種パラメータの設定、パッケージソフトウェア本体に改造を加える「モディファイ」、パッケージソフトウェアに機能を加える「アドオン」を実施することとなる。このときにユーザが過大な要求をすることにより、システム全体のオリジナルのパッケージソフトウェアの占める割合が低くなり、システムの信頼性、安全性、性能が低下する要因となるとともに想定外の費用が発生することがある。また、モディファイの影響でバージョンアップが受けられなくなるトラブルも散見する。パッケージソフトウェア選定後であっても、大規模改修が必要とわかった場合には、ＢＰＲ方針の見直しやパッケージソフトウェア選定のやり直しなど、思い切った対策が必要な場合も出てくる点に留意が必要である。

	ユーザ	ベンダ	外部専門家
原因	パッケージソフトウェア導入のポイントを理解していない。 現場が既存の機能などに固執する	パッケージソフトウェアが提示する業務の優位性を十分に説明していない モディファイ・アドオンの増加が売り上げ増加につながる場合、容易にモディファイ・アドオンを受けてしまう	モディファイ・アドオンの必要性、投資対効果が説明できていない
主な対策	パッケージソフトウェア導入時には、パッケージソフトウェア側の業務パターンにあわせることも重要であることを利用現場に啓発する。	企画段階でシステム化方針としてモディファイ・アドオンを少なくする方策を決定する 設計着手前に、十分なユーザ教育を行う	モディファイ・アドオンに対する実施可否の評価基準やチェックリストを提示する
契約での留意点	契約上の留意点はない。	システムのバージョンアップに制限が入ること等を契約書に明記する。 パフォーマンス低下の可能性を示唆する。	契約上の留意点はない。

(3) パッケージソフトウェアの機能・サービスレベル不足

フィットギャップ分析時に、当該機能有りと判断された機能について、設計段階においてユーザのイメージと大幅に異なることが判明し、モディファイの要否、その費用の負担などが問題になる場合がある。応答時間や使い勝手といった非機能要件、ユーザビリティにおいて問題が発生することが多い。

特に、あるユーザ企業用に作ったシステムをそのままパッケージソフトウェアと称して販売する「流用品」では機能の整備が十分ではないケースが見受けられる。システム構築の企画段階からパッケージソフトウェアを視野に入れて開発しシステム完成後に、パッケージ化を図る商品も、初期ユーザの仕様に依存していることが多く汎用的になっていない場合があり注意が必要である

	ユーザ	ベンダ	外部専門家
原因	パッケージソフトウェア選定時の検討が不足している	パッケージソフトウェアの機能や制約を正確に説明していない	パッケージソフトウェアの精査が十分でない
主な対策	パッケージソフトウェア導入時には、パッケージソフトウェア側の業務パターンにあわせることが重要であることを利用現場に啓発する。	重要事項説明を実施する。 流用パッケージの場合には特に注意をする 性能などの非機能要件は早めの確認を行う	パッケージソフトウェア選択の評価基準やチェックリストを提示する
契約での留意点	仕様に記述した機能が、既存機能より低下するときや一般常識的に用意されるべき機能が不足している場合の対応を明記する。	パッケージソフトウェアとして提供されるべき基本機能の不足等、紛争対応を明記する。	同左

(4) 仕様外の要求

システム開発途上で、仕様に書いていなかったことが要求されることがある。それは、ユーザが仕様に書き忘れていた場合や、事業環境が変化したことに起因することも多い。ベンダとユーザの力関係で作業を押し切られてしまうことも多く、手順の明確化が必要である。

	ユーザ	ベンダ	外部専門家
原因	仕様の書き方や位置づけが理解できていない。 仕様確定後の利用部門からの要望をコントロールできない。	仕様確定時に十分な情報提供を行っていない	パッケージソフトウェアの精査が十分でない
主な対策	仕様を基にチェックを行う。(日本情報システム・ユーザ協会「要求仕様定義ガイドライン」等) 仕様の意味付けを利用現場に啓発する。	企画段階でシステム化方針としてモディファイを少なくする方策を決定する。 設計着手前に、十分なユーザ教育を行う。 仕様書に記述がない項目は、仕様変更にあたるという事を啓発する。	パッケージソフトウェア選択の評価基準やチェックリストを提示する
契約での留意点	仕様変更の費用分担判断基準や判断プロセスを明確にする	仕様に明記されていない部分での意識のすれ違いに関する判断基準を明確化しておく	同左

(5) 検収時点での要求不一致

システム検収時点で現場の利用者が来て、これでは使えないなどの指摘をすることも多い。企画、設計などを情報システム部門にまかせっきりなユーザにおいて多発するトラブルであり、フローのあり方や操作性などの指摘を受けることも多い。仕様では明確に記述されていないことも多く、トラブルに発生することが多い。

	ユーザ	ベンダ	外部専門家
原因	システム部門がユーザ部門と十分な確認を取っていない。 完成イメージを勝手に思い込み、ベンダに伝えていない。	完成イメージを勝手に思い込み、ユーザに伝えていない	―
主な対策	プロトタイプやシナリオモデルによるレビューを行う。	プロトタイプやシナリオモデルによるレビューを行う。	嗜好や感覚に属する部分が大きい事、現物（プロトタイプなど）での確認の重要性を説明する。
契約での留意点	契約上の留意点はない。	明文化されている仕様を実現していない場合はベンダの責に帰すべき要求不一致であり、明文化されていない仕様についてはベンダに帰すべき責でない旨を記載する。	―

(6) 既存・追加ソフトウェアとの不整合

システムの開発環境では問題なく稼動していたが、実運用機で動かしてみると既存システムと新システムで使用しているドライバが不整合を起こすなどで正常に稼動しないことがある。逆に、追加システムを入れたことにより納入済のシステムが動かなくなることもある。また、セキュリティ対策などによるＯＳなどの変更もシステム障害を引き起こす可能性がある。

	ユーザ	ベンダ	外部専門家
原因	稼働環境をベンダに事前に連絡していない。 テスト環境を提供しない。	事前に環境確認を行っていない。	―
主な対策	事前に稼働環境をベンダに開示する。	事前環境調査を実施する。	ソフトウェアはその稼働環境の設定が繊細である事を十分に説明する。
契約での留意点	事前環境の確認を仕様に記述しておく。	システム開発終了後の別システム追加によるシステム障害は免責事項として記述する。	―

(7) 優越的地位の利用

ユーザとベンダは、本来は対等なパートナー関係を築く必要があるが、発注側であるユーザが相対的に優越的地位になることが多い。そのため、価格や仕様変更のリスクに備えフェージング契約をしていたとしても、後工程での金額の交渉ができない場合も多い。そのため、初期の概算見積もりのまま、開発をせざるを得なくなりトラブルになることがある。

また、グループ経営をしている企業の情報システムを構築するときに、企画まではグループの中核会社が実施し、その後、グループ会社と個別契約をすることもあるが、責任主体が明確でなくトラブルに発展することがある。

	ユーザ	ベンダ	外部専門家
原因	当初合意していた事項を変更する。	契約条項などに記載していても、強く主張していない	―
主な対策	合意内容を変更しない。	トラブルになりそうな項目は、契約書や議事録で確認を行う。仕様書に明記されていない項目は、追加または変更にあたるという事を啓発する。	仕様書に明記されていない項目は、追加または変更にあたるという事を事前に啓発する。
契約での留意点	次フェーズで合意に至らない場合の解約条項を入れておく。 また、関連契約が影響を及ぼす場合は明記しておく。 「仕様変更・追加が契約に影響する場合は、契約の変更管理プロセスを用いて対応することを合意する。」ように契約に明記し、関係者に啓発、喚起する。	次フェーズで合意に至らない場合の解約条項を入れておく。 また、関連契約が影響を及ぼす場合は明記しておく。 「仕様変更・追加が契約に影響する場合は、契約の変更管理プロセスを用いて対応することを合意する。」ように契約に明記し、関係者に啓発、喚起する。	―

(8) 知的財産の帰属

著作権は開発者に帰属することが基本であるが、ユーザの知識不足による著作権保持の主張や、複数社が関わっての仕様検討等により、業務フローなどのビジネスモデルについてユーザが権利を主張する場合もある。特にビジネスモデルについては、特異なモデルではなく汎用的モデルについての権利を主張される場合、ベンダにとっては応じかねることがある。

	ユーザ	ベンダ	外部専門家
原因	必要以上に著作権を主張する	業務秘密をパッケージソフトウェアなどで流用することがある	業務秘密を他社へのコンサルティングなどで流用することがある
主な対策	著作権と秘密保持契約の関係を啓発する	モラル啓発を行う。 パッケージソフトウェア化を前提とした契約を行う（利益の先渡しは行わない)。	モラル啓発を行う。
契約での留意点	モデル契約を使って、常識的な契約を行う。必要であれば秘密保持契約を締結する。	業務秘密がユーザ固有の物である場合、汎用的で有る場合、業務秘密を流用した場合の扱いを契約書に明記する。	業務秘密を流用した場合の扱いを契約書に明記する。

(9) 開発中止時の精算

開発中にユーザ、ベンダそれとも双方の何らかの事由により開発を中止にせざる得ない場合がある。そのときに、かかった費用の負担や中止に伴う損害に対して問題化することがある。

	ユーザ	ベンダ	外部専門家
原因	仕様決定の遅れや頻繁な仕様変更など、ベンダが対応できない状況になってしまう。	技術力の不足などでプロジェクトが遂行できない。	左記両原因
主な対策	プロジェクト管理を強化する。ベンダ選定を強化する。	プロジェクト管理を強化する。	プロジェクト管理を強化する。
契約での留意点	開発中止時の解約条件を明記する。	同左	同左

（10）パッケージソフトウェア間のインタフェースに起因する問題

システム構築の際に各パッケージソフトウェアの持つ詳細仕様の整合性が取れないことが明確になり、業務要件やシステム要件を満たさなくなることがある。メッセージの連携ができずに統合運用ができない場合や、システム基本ソフトのバージョンに制約があり、同じハードウェア上では同居できないなどの場合もある。そのため、運用が当初想定していたものより手間がかかるようになったり、ハードの重複投資が必要になったり、最悪、システム実現ができない場合がある。

	ユーザ	ベンダ	外部専門家
原因	―	組み合わせに関する十分な調査を行っていない	機能面だけでパッケージソフトウェア選定をしてしまう
主な対策	複数社のパッケージソフトウェアを使う場合には、システムインテグレータなど、その分野の知見を持つ企業に委託するか、パッケージソフトウェアベンダの１社にシステムインテグレーション契約を行う	先行事例の調査を行う。事例がない場合には事前検証を行う。	各社に対して実績などの調査を行う
契約での留意点	障害発生時に対応ができる条項を入れておく。（解約条項など）	―	―

（11）システム内の障害が切り分けられない場合

障害発生時に傷害の原因がわからない場合には、ベンダからテクニカルサポート料などの調査費用を要求されることも多い。１パッケージソフトウェアしか搭載されていない場合でもＯＳとの相性などを理由に自社パッケージソフトウェアの非を認めないベンダも多いが、パッケージソフトウェア・インテグレーションで構築されたシステムにおいては、特に、組み合わせ先パッケージソフトウェアの問題として迅速に対応してくれない場合が多い。

特に、原因が最後まで明確にならない障害については修正ができないままユーザが一方的に不利な状況になることがある。

	ユーザ	ベンダ	外部専門家
原因	―	責任回避をしようとする体質	―
主な対策	複雑なシステムにはシステムインテグレータを活用する 迅速な対応を促すため保守契約を結ぶ	障害履歴を蓄積することによる、対応の高度化 サービス姿勢の改革	―
契約での留意点	障害発生時に対応ができる条項を入れておく。	―	―

（12）パッケージソフトウェアのバージョンアップに起因する問題

ミドルウェアのバージョンアップによって、システムのサポートの継続性が得られないこともあるし、機能拡張時に新しいバージョンのミドルウェアに切り替えたいと言う要求が出るときもある。そのときに、バージョンアップを行った影響が既存の機能に出る場合もある。最近のソフトウェアは自動バージョンアップを行うものも提供されており、注意が必要である。

	ユーザ	ベンダ	外部専門家
原因	―	設計時にバージョンアップを考慮していないことがある	―
主な対策	バージョンアップの可能性やその対処方法を開発初期の段階で確認しておく	バージョンアップの影響を受けにくい設計にする。	―
契約での留意点	―	―	―

（13）サポート切れ

システム内で利用しているミドルウェアなどのパッケージソフトウェアソフトが、サポート切れで、メーカーから今後の対応が受けられなくなることがある。システム自体の寿命がまだ長い場合には、ミドルウェアの入れ替え、システムそのものの入れ替えを求められる場合もある。

	ユーザ	ベンダ	外部専門家
原因	―	設計時にサポート期限を考慮していないことがある	―
主な対策	サポート切れの可能性やその対処方法を開発初期の段階で確認しておく	当該パッケージソフトウェアの影響を受けにくい設計にする。	―
契約での留意点	―	―	―

フェーズレビュー　チェックシート

6.2.　付録 2 フェーズチェックリスト

フェーズレビュー０（システム化の方向性）
評価者：

分類	質問	評価	備考
事業	事業の目的は明確になっていますか？		
事業	ゴールは明確に定めていますか？		
事業	予算の実施により事業・業務目的は達成されますか？		
事業	緊急性、必要性はあるか？		
事業	自社で実施すべき妥当性はありますか？（他社サービスで代替できませんか）		
効果	利便性向上などの価値を生み出す効果は明確に記述されていますか？		
効果	業務改革効果は明確に記述されていますか？		
効果	投資対効果を評価していますか？		
効果	必要な要求品質は検討され明記されていますか？		
予算	予算額は妥当ですか？		
内容	代替案、システムの依存性、類似性は検討されていますか？		
リスク	リスクは許容できるレベルですか？		
ポートフォリオ	戦略性と実現性を勘案して、適当な事業ですか？		
体制	予算執行に必要な体制は発注側、受注側にありますか？		

評価 A：質問を満たしている
評価 B：不十分な部分もあるが概ね満たしている（要備考記述）
評価 C：質問内容を満たしていない
－　　：質問事項に該当しない

フェーズレビュー　チェックシート

フェーズレビュー１（システム化計画）
評価者：

分類	質問	評価	備考
事業	事業目標を実現するための主要成功要因が明確化されていますか？		
事業	要求内容は、関係者全体から収集されていますか？		
事業	システム化計画は整備されていますか？		
改革	BPR の方針は明確ですか？ 納期短縮、コスト削減等		
改革	RFI は適正な対象（ベンダ）に依頼されていますか？		
改革	RFI により、各社のパッケージソフトウェアの特徴など、必要な情報は収集されていますか？		
現状評価	既存の業務・システムがある場合、そのまま継続するのでは駄目ですか？		

評価 A：質問を満たしている
評価 B：不十分な部分もあるが概ね満たしている（要備考記述）
評価 C：質問内容を満たしていない
－　　：質問事項に該当しない

フェーズレビュー　チェックシート

フェーズレビュー２（業務要件定義）
評価者：

分類	質問	評価	備考
事業	主要成功要因が業務機能に展開されていますか？		
事業	事業や業務上の仮説に変化はないですか？		
ＥＡ	機能分析は、設計に引き継げるレベルで行われていますか？		
ＥＡ	情報分析は、設計に引き継げるレベルで行われていますか？		
ＥＡ	業務プロセス分析は、設計に引き継げるレベルで行われていますか？		
ＥＡ	インタフェース分析は、設計に引き継げるレベルで行われていますか？		
ＥＡ	ハード、ソフト、ネットワークは、設計に引き継げるレベルで整理されていますか？		
改革	他者事例の調査はしましたか？		
成果物	RFP はきちんと整備されていますか？		
成果物	外部専門家を使う場合、外部専門家は善管注意義務について理解していますか？		
効果	当初見込んだ効果が得られそうですか？		
予算	当初見込んだ予算内に収まりそうですか？		
引き継ぎ	基本設計に引き継げますか？		

評価 A：質問を満たしている
評価 B：不十分な部分もあるが概ね満たしている（要備考記述）
評価 C：質問内容を満たしていない
－　　：質問事項に該当しない

フェーズレビュー　チェックシート

フェーズレビュー３（システム要件定義）
評価者：

分類	質問	評価	備考
事業	事業や業務上の仮説に変化はないですか？		
外部仕様	関係者は明確になっていますか？		
外部仕様	機能は明確になっていますか？		
外部仕様	インタフェースは明確になっていますか？		
外部仕様	開発モデルについての合意を得ていますか？		
パッケージソフトウェア	フィット＆ギャップ分析は適正な評価項目で行われましたか？		
効果	当初見込んだ効果が得られそうですか？		
予算	当初見込んだ予算内に収まりそうですか？		
リスク	システムに不測の事態が発生した場合の対策が検討されていますか？		
成果物	システム要件定義書が整備されていますか		
引き継ぎ	詳細設計に引き継げますか？		

評価Ａ：質問を満たしている
評価Ｂ：不十分な部分もあるが概ね満たしている（要備考記述）
評価Ｃ：質問内容を満たしていない
－　　：質問事項に該当しない

フェーズレビュー　チェックシート

フェーズレビュー４（サービス開始時、移行・運用準備プロセス）
評価者：

分類	質問	評価	備考
事業	事業や業務上の仮説に変化はないですか？		
品質	品質は許容できるレベルまで収束していますか？		
品質	機能として致命的な問題はないですか？		
品質	過負荷に対する試験をしましたか？		
効果	当初見込んだ効果が得られそうか？		
予算	当初見込んだ予算内に収まりそうか？		
リスク	システムに不測の事態が発生した場合の対策ができていますか？		
引き継ぎ	関係者は操作に習熟していますか		
引き継ぎ	保守体制は明確になっていますか？		
引き継ぎ	サービスレベルの指標は明確になっていますか		

評価Ａ：質問を満たしている
評価Ｂ：不十分な部分もあるが概ね満たしている（要備考記述）
評価Ｃ：質問内容を満たしていない
－　　：質問事項に該当しない

6.3. 付録 3 アジャイル開発適用のチェックリスト

	分類	チェック項目	評価
1	開発側	関係者全員がアジャイル開発を理解し、それを採用することに同意していること	
2	開発側	サーバー管理やマニュアル作成等の担当を除く全員がコーディングできること	
3	相互条件	開発に使うソフトウェアを開発者が選べること	
4	相互条件	タスクをチーム内で決定できること	
5	相互条件	実際に作業する人が顧客と話せること	
6	相互条件	無駄な決まりごとを作らないこと	
7	相互条件	チーム全員が自由に発言できること	
8	相互条件	質疑応答が迅速に出来る環境が整備されていること	
9	相互条件	ソフトウェアの設計を書かなくても良いこと	
10	顧客側	ステークホルダーが 5 人以下であること	
11	顧客側	開発者の要請に応じて時間が取れること	

「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

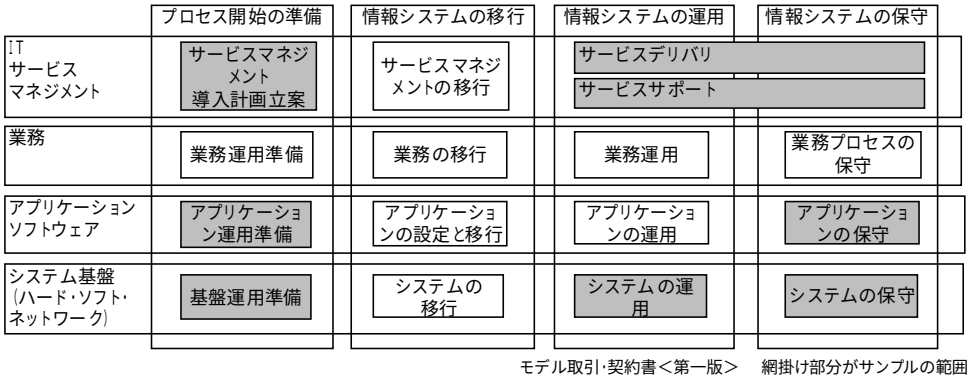
図表 目 次

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

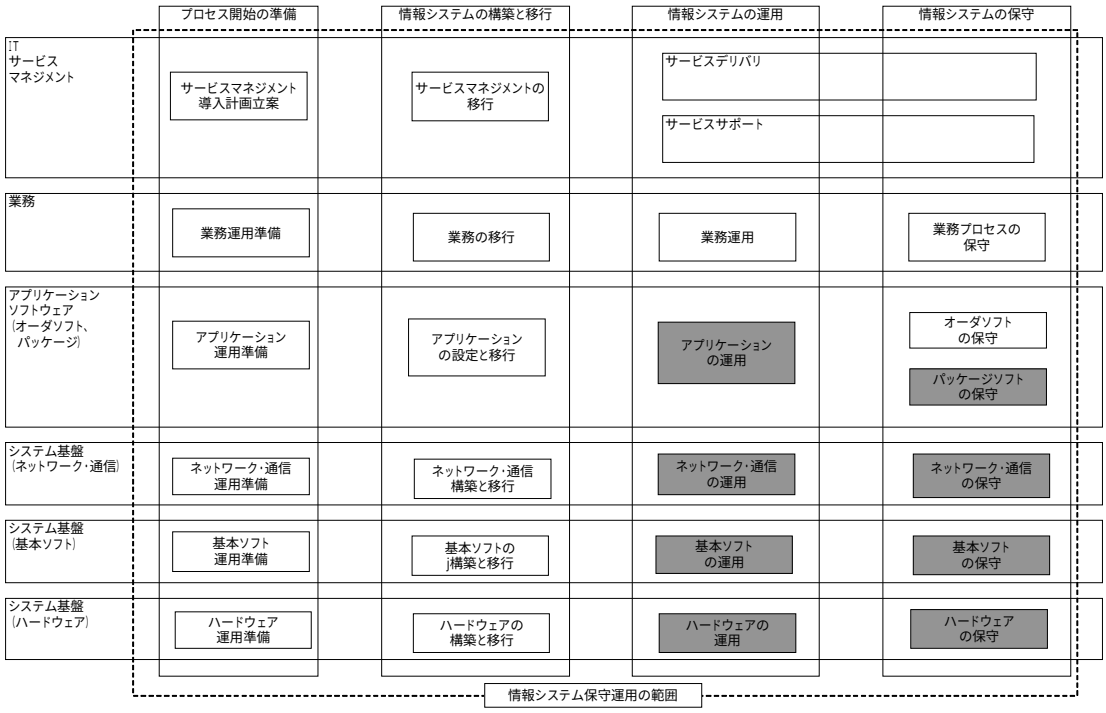
3 モデル取引･契約書＜第一版＞の「(4) 情報システム保守運用委託基本モデル契約書　②保守運用業務の全体構成とサンプル事例の対象」（137頁）

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。

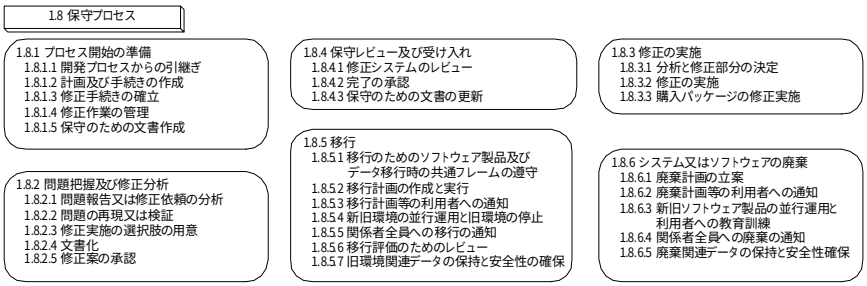
運用プロセスのアクティビティとタスクの一覧を図 4 に示した。2007年度版で変更された部分を太字で、また JIS X 0160 には無い部分を点線の枠で表した。

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)

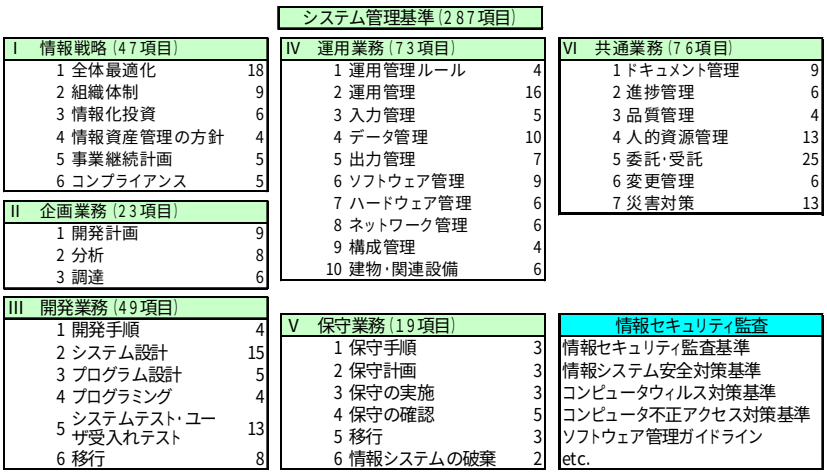
		目的(JIS Q 20000:2007)
6 サービス提供プロセス		
6.1	サービスレベル管理	サービスレベルを定義、合意、記録及び管理するため。
6.2	サービスの報告	十分な情報に基づいた意思決定及び効果的な伝達のための、合意に基づく、適時の、信頼できる、正確な報告書を作成するため。
6.3	サービス継続及び可用性の管理	合意したサービス継続及び可用性についての顧客に対するコミットメントを、あらゆる状況のもとで満たすことを確実にするため。
6.4	サービスの予算業務及び会計業務	サービス提供費用の予算を管理し、かつ、会計を行うため。
6.5	容量･能力管理	顧客の事業において必要な、現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。

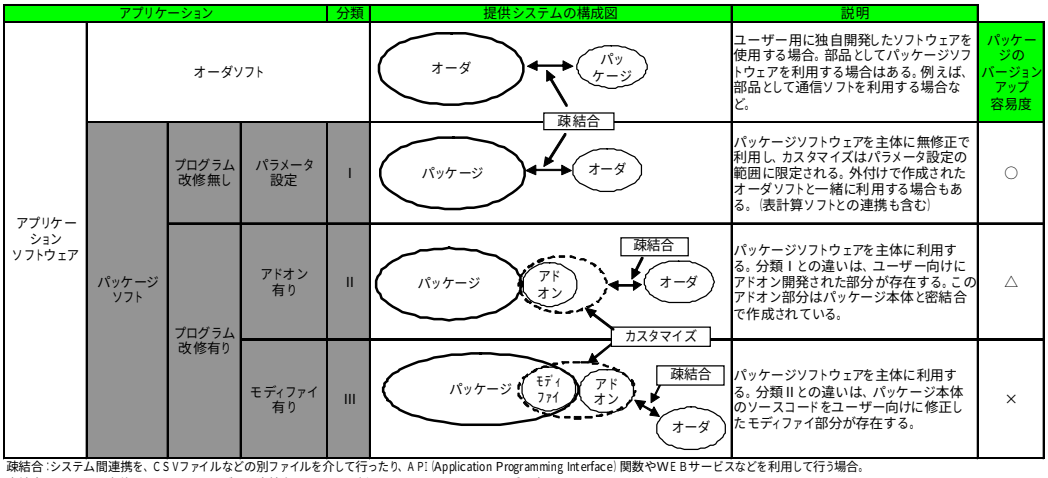
留意事項としては、ハードウェア保守と共通している項目も多い。「契約の曖昧さの排除」や、「サービス内容の範囲を明確化」などである。ソフトウェアの特性としては、瑕疵担保の取扱いが重要となるため、次節（2.10）で詳しく述べる。

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

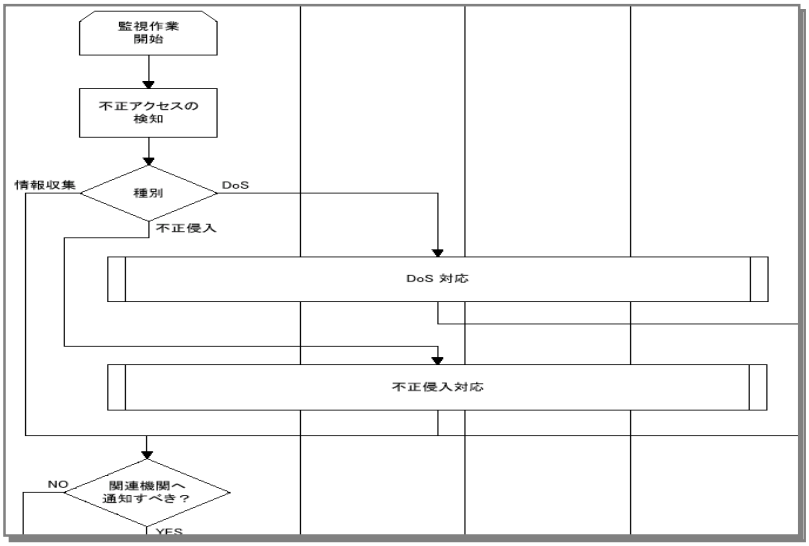
［セキュリティ監視サービス：ファイアウォールマネージメントサービス］（例）

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	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	分	目標	(未対応)	10分以内

		利用して通報する	までの時間				
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

「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～

＜セキュリティチェックシート（詳細項目版）＞

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）

セキュリティ・可用性チェックシート（詳細項目版）

	技術的セキュリティ対策					推奨レベル				本件業務のセキュリティ仕様			
	要素	分類	対策項目	リスクの詳細	レベル1	レベル2	レベル3	レベル4	該当レベル	対策仕様	JISQ項番	参考文献（JIS Q 27002：2006以外）
1	情報を他人から守る（機密性保護）	認証	パスワードを利用する	パスワードが推測可能な容易な物になっていると、第三者がシステムに不正アクセスし、情報を漏えいしてしまうおそれがある。	・パスワードを利用しない。	・初期パスワードをすみやかに変更する。 ・定期的（六ヶ月毎）に、パスワードを変更する。 ・パスワードは、複雑なもの（八桁以上）を設定する。 ・パスワードは、管理者を含め誰にも教えない。 ・パスワードを書き留めたり、コンピュータ上のファイルに保管したり、メールで送信したりしない。やむを得ず紙片等にパスワードを記載する必要がある場合には、そのパスワードが容易に第三者に見られることがないように保管する。 ・自分のパスワードが他人に漏えいした可能性や疑いがある場合は、パスワードを変更する。	・定期的（三ヶ月毎）に、パスワードを変更する。 ・パスワードは、複雑なもの（八桁以上、パスワード世代管理、三種類以上の文字種の使用）を設定する。	・同一利用者が複数のアカウントをもつ場合は、それぞれ異なるパスワードを設定する。また、一つのパスワードから他方が推測しやすいパスワードを設定しない。 ・機密性が高い部署では、生体認証を使用する。			A.11.3.1	・政府機関統一基準適用個別マニュアル群 庁舎内におけるPC利用手順 PCの取扱編 端末利用者パート 2.3 識別コードの日常の取扱い(2), (3)
2			ネットワーク上の機器を識別する	不正な情報機器がネットワークに接続されると、情報が漏えいするおそれがある。	・未登録や不正なコンピュータの接続を検出できない。	・未登録や不正なコンピュータの社内ネットワークへの接続を、検出して警報をあげる。 ・接続コンピュータのログを取得する。	・未登録や不正なコンピュータの社内ネットワークへの接続を、検出し、警告して、接続を防止する。 ・接続コンピュータのログを取得する。	・未登録や不正なコンピュータの社内ネットワークへの接続を検出・警告し、接続を防止する。 ・正常な未登録のコンピュータを、自動的に登録する。			A.11.4.3	
3			利用者が本人であることを証明し承認する	利用者の身分が証明できないと、権限がない利用者が情報を不正に取得して社外へ漏えいさせるおそれがある。	・一台のコンピュータを一つのアカウントで、複数の利用者が使用する。 ・認証ログは取得しない。	・Windowsのアカウント、パスワードを利用して、利用者を識別する。 ・一台のコンピュータを複数の利用者では使用させない。 ・認証ログを取得する。	・一台のコンピュータに対して、一人しか使用させない。 ・特定のカードやログインの二重化などで、本人認証を実施する。 ・認証ログを取得する。	・生体認証（静脈・指紋認証など）を利用して、利用者の本人認証を実施する。 ・二要素認証を実施し、認証強度を上げる。 ・認証ログを取得する。			A.11.5.2	
4			業務ソフトウェアや機器認証で使うパスワードを管理する	パスワードの管理がされていないと、不正な活動や情報漏えいが確認できないおそれがある。	・パスワードを管理しない。	・認証機能を使用して、コンピュータを利用する。	・認証機能を使用して、コンピュータと業務ソフトウェアを利用する。	・生体認証を利用してパスワードを使わない。			A.11.5.3	・政府機関の情報セキュリティ対策のための統一基準（第2版） 4.1.1 主体認証機能(1)
5			業務ソフトウェアの起動時間を監視する	業務ソフトウェアが終了されずに放置されていると、情報が盗まれるおそれがある。	・業務ソフトウェアの未使用時間を監視しない。	・業務ソフトウェアの未使用時間を監視する。 ・一定時間以上利用されないセッションを監視する。	・業務ソフトウェアの未使用時間を監視し、警告する。	・業務ソフトウェアの未使用時間を監視し、警告して、遮断する。			A.11.5.5	
6			情報へのアクセスを管理する	誰もが情報を閲覧できるようになっていると、情報の改ざんや漏えいのおそれがある。	・サーバ上の情報に誰でもアクセスできる。 ・情報を機密レベルに分類しない。 ・情報にアクセスした履歴を取得しない。	・サーバ上の情報にアクセス権をつけて、権限のない利用者は使用できないようにする。 ・情報にアクセスした履歴を取得しない。	・情報を重要度別（（秘）（社外秘）（関係者外秘）など）に分類して、重要度別に利用者やグループ単位でアクセス権をつけて管理する。 ・情報にアクセスした履歴を取得する。 ・印刷物を減らすことにより、管理する対象を減らし、情報漏えいのリスクを減らす。 ・印刷物に対して、誰がいつ印刷したものか、わかるように「すかし」などを挿入する。	・アクセスの履歴を定期的に監査して、情報の持ち出しに問題があれば是正する。			A.11.6.1	
7		暗号化	コンピュータや電子媒体を暗号化する	情報機器が盗難又は紛失されると、情報が漏えいするおそれがある。	・データを暗号化しない。	・社外に持ち出すコンピュータ、電子媒体（USBメモリ、外付けHDD、CD/DVDなど）の中のデータを暗号化する。	・社内のコンピュータ、社外に持ち出すコンピュータ、電子媒体（USBメモリ、外付けHDD、CD/DVDなど）に対して暗号化をする。	・社内のコンピュータ、社外に持ち出すコンピュータ、電子媒体（USBメモリ、外付けHDD、CD/DVDなど）に対して暗号化をする。 ・復号時には認証が毎回必要となる。			A.12.3.1	
8			ネットワークを流れる情報を暗号化する	ネットワーク上のデータが盗聴されると、情報が漏えいするおそれがある。	・社外に送るデータは平文で送信する。 ・Webの通信は暗号化（SSL通信）しない。	・Webの通信を暗号化（SSL通信など）する。	・社外に出る情報を、事前に社内で暗号化して送信する。 ・Webの通信を暗号化（SSL通信など）する。	・コンピュータから発信する情報(メールの添付データなど）を、社内、社外にかかわらず、すべて事前に暗号化して送信する。 ・Webの通信を暗号化（SSL通信など）する。			A.12.3.1	
9			暗号鍵の強度を上げる	暗号の複雑さが低いと、簡単に復号化されて情報が漏えいするおそれがある。	・暗号化しない。	・公に認知されているアルゴリズムで暗号化する。 ・鍵長が64ビット以上の暗号化を使用する（AES 64ビット以上など）。	・公に認知されているアルゴリズムで暗号化する。 ・鍵長が128ビット以上の暗号化を使用する（AES 128ビット以上など）。	---> 前レベルと同様				
10			暗号鍵を管理する	暗号鍵が外部に流出すると、暗号化したデータを復号されて、情報が漏えいするおそれがある。	・暗号化しない。	・暗号鍵を、平文（通常の文字列）のままソフトウェア上で管理する。	・暗号鍵を、暗号化してソフトウェア上で管理する。 ・サーバ上で、暗号鍵の保管場所を誰にでもわかるようにする。	・暗号鍵を暗号化して、独自のパスワード等で保護する。 ・暗号鍵の所在については、システム的に管理者以外は閲覧できなくする。			A.12.3.2	
11		侵入検出（IDS/IPS）	社外ネットワークからの攻撃や不正侵入を防御する	サーバやネットワーク機器に対する侵入行為や攻撃を受けると、データが改ざんされたり、情報が漏えいしたり、システムが停止したりするおそれがある。	・不正アクセスは考慮しない。	・外部からの不正アクセスを検討・考慮する。 ・外部からの攻撃を検出・防御する仕組み（IDSなど）を導入する。	・外部からの不正アクセスを検討・考慮する。 ・外部からの攻撃を検出・防御する仕組み（IDSなど）を導入する。 ・外部からのアクセスログを取得して、定期的にレポートする。	・外部からの不正アクセスを検討・考慮する。 ・外部からの攻撃を検出・防御する仕組み（IDSなど）を導入する。 ・不正アクセス検出した場合、自動的に遮断する仕組みを導入する。 ・外部からのアクセスログを取得して、定期的にレポートする。			A.10.4.1	
12		ウイルス対策	悪意あるプログラムを検出する	コンピュータに誤動作を起こさせる悪意あるプログラム（ウイルスやスパイウェア等）により、システムが利用できなくなる、データが消去される、情報が外部に漏えいしてしまう、などのおそれがある。	・ウイルス対策を実施しない。	・悪意あるプログラム（ウイルス・スパイウェア）が、コンピュータ上のデータに付着していないか、検出する機能を導入する。 ・社内の全コンピュータのウイルス対策状況を把握する仕組みを導入する。 ・悪意あるプログラムを検出した場合、システム管理者に通報する。	・悪意あるプログラム（ウイルス・スパイウェア）が、コンピュータ上のデータに付着していないか、検出して駆除する。 ・システムの変更された部分を自動的に修復できる機能を導入する。 ・社内の全コンピュータのウイルス対策状況を把握する仕組みを導入する。 ・悪意あるプログラムを検出・駆除及びシステムを修復した場合、システム管理者に通報する。	・悪意あるプログラム（ウイルス・スパイウェア）が、コンピュータ上のデータに付着していないか、検出して駆除する。 ・システムの変更された部分を自動的に修復できる機能を導入する。 ・悪意あるプログラムによるネットワーク通信を自動的に遮断する。 ・社内の全コンピュータのウイルス対策状況を把握する仕組みを導入する。 ・悪意あるプログラムを検出・駆除及びシステムを修復した場合、システム管理者に通報する。			A.10.4.1	
13			メールに添付した悪意あるプログラムを検出する	コンピュータに誤動作を起こさせる悪意あるプログラム（ウイルスやスパイウェア等）がメールから侵入すると、システムが利用できなくなる、データが消去される、情報が外部に漏えいしてしまう、などのおそれがある。	・メールのウイルス対策を実施しない。	・悪意あるプログラム（ウイルス）が、メールに添付していないか、検出する。 ・ウイルスを検出した場合、システム管理者に通報する。	・悪意あるプログラム（ウイルス・スパイウェア）が、メールに添付していないか、検出する。 ・メールに添付している悪意あるプログラムを駆除する。 ・ウイルスの可能性があるものを検出する。 ・ウイルスを検出した場合、システム管理者に通報する。	・悪意あるプログラム（ウイルス・スパイウェア）が、メールに添付していないか、検出する。 ・メールに添付している悪意あるプログラムを駆除する。 ・ウイルスの可能性があるものを検出する。 ・ウイルスを検出した場合、システム管理者に通報する。			A.10.4.1	
14			迷惑メールを遮断する	迷惑メールが侵入すると、トラフィック増加、システム負荷の増加、悪意あるプログラムの侵入、悪意あるWebサイトへの転送、などのおそれがある。	・迷惑メールを対策しない。	・迷惑メールの判別をおこない、印をつける。	・迷惑メールの判別をおこない、隔離領域に振り分ける。	・迷惑メールの判別をおこない、悪質な送信元からの受信を拒否する。			A.10.4.1	
15			不要なWebサイト閲覧を管理する	業務に不必要なWebサイト閲覧を許可していると、業務効率の悪化、トラフィック増加、悪意あるプログラムの侵入、外部への情報漏えい、などのおそれがある。	・Webサイトの閲覧に制限をかけない。	・指定されたURLをブロックする。	・指定されたURLをブロックする。 ・提供されるデータベースを使用して、カテゴリ単位でWebサイトをブロックする。	・指定されたURLをブロックする。 ・提供されるデータベースを使用して、カテゴリ単位でWebサイトをブロックする。 ・信頼度の低いWebサイト、危険度が高いWebサイトを、設定したセキュリティレベルでブロックする。			A.10.4.1	・政府機関の情報セキュリティ対策のための統一基準（第2版） 4.2.1 セキュリティホール対策(2), 4.2.2 不正プログラム対策(1)(2)
16			全社のセキュリティ対策製品を集中的に運用管理する	社内のセキュリティ対策製品が管理できていないと、緊急時対応の遅れ、ポリシー漏れ、管理状況の把握が困難、などのおそれがある。	・各製品を個別に運用する。	・利用者のコンピュータに導入されたウイルス対策製品を集中的に管理運用する。 - アップデート状況 - ウイルス検出状況	・社内のすべてのセキュリティ対策製品を集中的に管理運用する。 - アップデート状況 - ウイルス検出状況	・社内のすべてのセキュリティ対策製品を集中的に管理運用する。 - アップデート状況 - ウイルス検出状況 - 自動的なレポート生成機能			A.10.4.1	

セキュリティ・可用性チェックシート（詳細項目版）

	技術的セキュリティ対策					推奨レベル			本件業務のセキュリティ仕様			
	要素	分類	対策項目	リスクの詳細	レベル1	レベル2	レベル3	レベル4	該当レベル	対策仕様	JISQ項番	参考文献（JIS Q 27002：2006以外）
17			Webサイト閲覧時に悪意あるプログラムを検出する	Webサイトから悪意あるプログラムが侵入すると、システムが利用できなくなる、データが消去される、情報が漏えいしてしまう、などのおそれがある。	・Webサイトからの悪意あるプログラムを検出しない。	・Webサイトからのウイルスを検出、自動処理する。 ・処理内容を管理者等に報告する。	・Webサイトからのウイルスを検出、自動処理する。 ・Webサイトからのスパイウェアを検出、自動処理する。 ・処理内容を管理者等に報告する。 ・パターンファイルに対応していない悪意あるプログラムを検出するための機能を導入する。	・Webサイトからのウイルスを検出、自動処理する。 ・Webサイトからのスパイウェアを検出、自動処理する。 ・処理内容を管理者等に報告する。 ・パターンファイルに対応していない悪意あるプログラムを検出するための機能を導入する。 ・利用者グループ毎に異なるポリシー設定する。			A.10.4.1	
18			ブラウザ上で動作する悪意あるプログラムを検出する	ブラウザ上で自動実行されるプログラム（ActiveXスクリプト、Javaアプレット等）が不正に実行されると、ウイルスに感染してしまう、情報が外部に漏えいする、などのおそれがある。	・ブラウザ上ではすべてのプログラムを実行する。	・署名済みのプラグインもしくは管理者の承認済みのスクリプトのみを実行する。	・未署名なActiveXや有効ではないJAVAアプレットの動作を制限する。	・未署名なActiveXや有効ではないJAVAアプレットの動作を制限する。 ・利用者グループ毎に異なるポリシー設定する。			A.10.4.2	
19		ファイアウォール	ネットワークサービスの利用を管理する	ネットワークへのアクセスを適切に制御しないと、社内外から不正なアクセスが発生し情報が漏えいするおそれがある。	・ネットワークサービス利用に関する方針を策定しない。	・ネットワークサービス利用に関する方針を策定する。 ・社外からの通信を遮断する。	・ネットワークサービス利用に関する方針を策定する。 ・社外からの通信は必要なもののみ許可する。 ・社外への通信は必要なもののみに制限する。 ・ネットワークサービス利用に対するログを監視し、必要に応じて警告する。	・ネットワークサービス利用に関する方針を策定する。 ・社外からの通信は必要なもののみ許可する。 ・社外への通信は必要なもののみに制限する。 ・ネットワークサービス利用に対するログを監視し、必要に応じて警告する。 ・必要に応じて、通信を自動的に遮断する。			A.11.4.1	
20			ネットワーク上の装置を識別する	ネットワークを通過・拒否される装置が適切に識別できないと、不正アクセスなどの発生時に対応が長期化するおそれがある。	・各システムに適切なホスト名などを設定しない。 ・DNSやLDAPによりホスト名などを確認できる設定をしない。	・各システムに適切なホスト名などを設定する。 ・DNSやLDAPなどによりホスト名などを容易に確認できる。 ・装置の接続状況をログに残す。	・装置管理のための情報を一箇所に統合する。 ・装置の追加・削除を適切に管理する。 ・装置の接続状況を定期的にレポートする。	・装置の認識がシステムで自動化し管理する。 ・不正な装置接続を自動的に遮断する。			A.11.4.3	
21			遠隔診断用及び環境設定用ポートを保護する	診断・管理用ポートへ不正アクセスを受けると、システムが不正に変更されたり情報が漏えいしたりするおそれがある。	・診断、管理用ポートへ誰でもアクセスできる。	・診断、管理用ポートに適切なアクセス権を設定する。	・診断、管理用ポートに適切なアクセス権を設定する。 ・管理用ネットワークは通常のネットワークとは別に用意し、一般利用者からは物理的・論理的にアクセス不可能にする。	・診断、管理用ポートに適切なアクセス権を設定する。 ・管理用ネットワークは通常のネットワークとは別に用意し、一般利用者からは物理的、論理的にアクセス不可能にする。 ・管理用ネットワークへのアクセスログを監視し、不正なアクセスを警告する。			A.11.4.4	
22			ネットワーク領域を分割する	ネットワークを適切に分割しないと、不正にアクセスされるおそれがある。	・社内ネットワークに社外からアクセスできる。	・社内ネットワークへは社外からのアクセスを禁止する。	・社内ネットワークの一部資源のみ、社外からのアクセスを許可する。	・社外に公開されたネットワーク（DMZ）と社外からはアクセスできない社内ネットワークを完全に分離する。			A.11.4.5	
23			ネットワーク接続を制御する	ネットワークへの接続制御を実施しないと、不正アクセスや情報漏えいが発生するおそれがある。	・誰でもネットワークが自由に使用できる。	・端末毎に接続制限をかける。	・利用者毎にネットワーク使用をコントロールする。 ・アクセス違反に対する適切なモニタリングを実施して、異常時には自動的に警告する。	・利用者毎にネットワーク使用をコントロールする。 ・アクセス違反に対する適切なモニタリングを実施して、異常時には自動的に警告する。 ・不正なネットワーク使用を強制的に切断する。			A.11.4.6	
24			ネットワークルーティングを制御する	内部、外部からの不正なルーティング情報が流入すると、既存のネットワーク情報が不正に変更されたり、情報システムが利用できなくなったりするおそれがある。	・対策しない。	・NATを使用し、外部に対して内部ネットワークを不可視にする。 ・静的ルーティングなど、固定的なルーティングを制御する。	・NATを使用し、外部に対して内部ネットワークを不可視にする。 ・管理下以外のネットワーク機器に対して、ルーティング情報のフィルタを実施する。	・ルーティング情報更新に認証情報(パスワードなど)を追加する。			A.11.4.7	
25		VPN装置	ネットワークサービスの利用を管理する	ネットワークの利用が適切に定義されていないと、不正アクセスが行われたり、情報漏えいしたりするおそれがある。	・適切なネットワークサービス利用に関する方針を策定しない。	・外部からのネットワークサービス利用に関する方針を策定する。	・外部からのネットワークサービス利用に関する方針を策定する。 ・利用者に対して定期的に周知、徹底する。	・外部からのネットワークサービス利用に関する方針を策定する。 ・利用者に対して定期的に周知、徹底する。 ・定期的な内部監査を行い、方針の運用状況を確認			A.11.4.1	
26			外部から接続する利用者を認証する	外部利用者を正しく認証できないと、外部からの不正アクセスで、情報漏えいしたり情報システムが停止したりするおそれがある。	・認証なしに誰でもアクセスできる。	・ユーザ名、パスワードによる利用者の認証をする。	・パスワードの複雑化や定期的な強制変更を実施する。 ・定期的なレポートを作成する。	・ワンタイムパスワードや生体認証など、より高度な利用者の認証を併用する。			A.11.4.2	
27			ネットワーク上の装置を識別する	ネットワークを通過・拒否される装置を適切に識別できないと、不正アクセスなどの発生時に対応が長期化するおそれがある。	・すべての装置がネットワークに接続できる。	・ネットワークにアクセスする装置種別(機種名、OS種別、バージョンなど)を判定する機器を導入する。	・ネットワークにアクセスする装置種別(機種名、OSバージョンなど)を判定する機器を導入する。 ・事前に設定した方針に従ってアクセス可否を自動的に制御する。	---> 前レベルと同様			A.11.4.3	
28			通信を暗号化する	通信を暗号化していないと、不正アクセスが行われたり、情報漏えいしたりするおそれがある。	・通信を暗号化しない。	・外部への通信を暗号化する。	---> 前レベルと同様	・より強力な暗号化方式（AES 128ビット以上など）を利用する。			A.11.7.1	
29			在宅勤務で使用するコンピュータを管理する	会社で許可していないコンピュータが在宅勤務で利用されると、情報が漏えいするおそれがある。	・個人所有コンピュータを使用する。	・会社支給のコンピュータで作業する。 ・すべてのデータがサーバ上にあり、コンピュータには一時保管するが、コンピュータにはデータが保存できなくする。 ・ファイルのアクセスログを取得する。	・会社支給のコンピュータで作業をする。 ・すべてのデータがサーバ上にあり、コンピュータには一時保管するが、コンピュータにはデータが保存できなくする。 ・一時保管したデータは、一定時間で自動的に消去する。	・会社支給のコンピュータで作業をする。 ・すべてのデータがサーバ上にあり、コンピュータには保管できない仕組みにする。 ・ファイルのアクセスログを取得する。 ・コンピュータ間の通信データを暗号化する。			A.11.7.2	
30		オペレーティングシステム（OS）	オペレーティングシステム（OS）の利用者を管理する	認可されない利用者がOSを利用できると、権限以上の操作ができることによる情報漏えいのおそれがある。	・利用者によるアクセス権限の変更をしない	・利用者を識別し、利用者毎にアクセス制御可能な機能、およびファイルシステムを区別する。	・利用者毎の情報システムへのアクセスを統合管理する。	・アクセスログを取得して、範囲外のアクセスについては自動的に警告する。			A.11.5	
31			利用者の成りすましを防ぐ	利用者のログオン情報が悪用されると、成りすましにより第三者がログオンしたり、情報漏えいしたりするおそれがある。	・対策しない。	・Secure Attention Sequence (SAS) などの、認証画面を不正なソフトウェアで模倣されない機能を導入する。 ・パスワードなどの認証情報を暗号化して、複合化できない状態で保存する。 ・パスワードの有効期間が切れた場合、アカウントを無効化する。	・過去にログオンしたユーザ名などのログオンに必要な情報の一部または全てを表示しない。 ・一定回数以上のログオン失敗に対して、一定時間のログオンを禁止する(失敗のしきい値：50回、ロックアウト期間：15分) ・辞書攻撃を防ぐために、一定時間内に連続したログオンを制限する。 ・ログオン時間(利用可能時間帯)を経過した場合は利用者を強制的にログオフする。 ・ログオン時間(利用可能時間帯)の有効期間が切れた場合はコンピュータを切断する。	・一定回数以上のログオン失敗が発生した場合に、管理者に通知する。 ・一定回数以上のログオン失敗に対して、一定時間のログオンを禁止する。(失敗のしきい値：15回、ロックアウト期間：15分)			A11.5.1	
32			オペレーティングシステム変更時に業務ソフトウェアの動作を検証する	オペレーティングシステム変更時に業務ソフトウェアを十分に検証しないと、不具合の発生、新たなぜい弱性の発生、問題の長期化、などのおそれがある。	・検証しない。	・オペレーティングシステムに変更があった場合、都度変更を記録する。	・年間サポート計画及び予算には，オペレーティングシステムの変更に必要なレビューやシステム試験を含める。 ・セキュリティ更新などによるオペレーティングシステムへの変更が行われることを前提に、システムの完全性を確認、試験する手順を定める。 ・オペレーティングシステムに対する変更を記録する。 ・変更後に、問題が発生した場合に回復させる手順を定める。	・緊急時に、セキュリティ更新プログラムまたはシステムの設定変更を最短で行うための最低限の手順を定める。			A.12.5.2	
33		無線LAN、リモートアクセスのセキュリティ	外部から接続する利用者を認証する	外部利用者を正しく認証できないと、外部からの不正アクセスで、情報漏えいしたり情報システムが停止したりするおそれがある。	・認証しない。	・内部の情報システムにアクセスする前に、ゲートウェイ等で利用者の認証を実施する。 ・外部からのアクセスは、一箇所のみで受け付ける。	・外部からの認証には、ハードウェアキー及びパスワードを利用する。	・外部からの認証には、ハードウェアキー及びワンタイムパスワードを利用する。 ・外部からの認証には、電子証明書を利用する。			A.11.4.2	
34			モバイルコンピュータの利用を管理する	モバイル中の情報機器が盗難される又は紛失してしまうと、情報が漏えいするおそれがある。	・対策しない。	・モバイルコンピュータは、データの暗号化もしくはハードディスクパスワードを利用する。	---> 前レベルと同様	・モバイルコンピュータは、シンクライアントシステムを導入する。			A.11.7.1	

セキュリティ・可用性チェックシート（詳細項目版）

	技術的セキュリティ対策				推奨レベル			本件業務のセキュリティ仕様			
	要素	分類	対策項目	リスクの詳細	レベル1	レベル2	レベル3	レベル4	該当レベル	対策仕様	JISQ項番	参考文献（JIS Q 27002：2006以外）
35			ネットワークサービスのセキュリティを強化する	拠点間ネットワークが盗聴されると、情報が漏えいするおそれがある。	・対策しない。	・拠点間のネットワークは、VPN等の暗号化もしくはアクセス制御が実施されたネットワークサービスを利用する。	・外部へのアクセスに対してのログをモニタリングして、必要時には自動的に警告する。 ・拠点間のネットワークは、VPN等の暗号化もしくはアクセス制御が実施されたネットワークサービスを利用する。	・外部へのアクセスに対してのログをモニタリングして、必要時に自動的に警告する。 ・危険なWebサイトへのアクセスは自動的に遮断する。 ・拠点間のネットワークは、VPN等の暗号化もしくはアクセス制御が実施されたネットワークサービスを利用する。			A.10.6.2	
36		ログの収集や解析	監査ログを取得する	情報システムの監査ログを適切に記録していないと、発生した不正な活動に気づかないおそれがある。	・監査ログを取得しない。	・情報システムのアクセスログを取得する。 ・アクセスログを、定期的に点検する。 ・アカウントによるログオンイベント（ローカル）を記録する（成功）。 ・アカウントへの管理作業を記録する（成功）。 ・アカウントまたはパスワードのポリシー変更を記録する（成功）。 ・システムに影響のあるイベントを記録する（成功）。	・アカウントによるログオンイベント（ネットワーク、ドメイン、ローカル）を記録する（成功）。	・アカウントによるログオンイベント(ネットワーク、ドメイン、ローカル）を記録する（成功/失敗）。 ・アカウントへの変更(管理作業)を記録する（成功/失敗）。 ・アカウントまたはパスワードのポリシー変更を記録する（成功/失敗）。 ・システムに影響のあるイベントを記録する（成功）。 ・オブジェクト(ファイル等)へのアクセスを記録する（失敗）。			A.10.10.1	
37			システムの使用状況を監視する	情報システムの使用状況を監視していないと、問題が発生した際の原因究明が困難になるおそれがある。	・情報システムを監視しない。	・情報システムへの不正なアクセスを定期的に確認する。	・情報システムが不正アクセスされた際に、自動的に検出し、通知するシステムを導入する。	・システムに重大な影響のあるイベントが発生した場合は、システム管理者に通知する。			A.10.10.2	
38			ログ情報を保護する	ログ情報を保護していないと、内容の改ざんや破棄されるおそれがある。	・ログを保護しない。	・情報システムのログを、オフラインで定期的にバックアップする。 ・情報システムのログにアクセス可能なアカウントを制限する。 ・ログの記録漏れ、上書き等が発生しないよう、十分な記憶容量を確保する。 ・ログが削除された事をログに記録する機能を導入する。	・オペレーティングシステムまたはソフトウェアの機能で、適切なログの保護措置が取られている。 ・ディスク等の容量不足などにより、ログが記録できない場合は、システムを停止する。 ・ログのオフラインでのバックアップは、十分な期間に遡って参照可能とする。	・短いサイクルで、別の情報システムにオンラインでログをコピーまたは移動する。			A.10.10.3	
39			実務管理者及び運用担当者の作業を記録する	一般利用者以上の権限を有する利用者の作業を記録していないと、ポリシーに反する作業に気がつかない、犯罪行為を証明する事ができない、などのおそれがある。	・ログを記録しない。	・実務管理者および運用担当者のログを記録する。	---> 前レベルと同様	・実務管理者及び運用担当者の作業が正当であることを確認するために、作業指示書を作成し保管する。			A.10.10.4	
40			障害発生時の状況を記録する	障害発生状況を記録していないと、障害が発生した際の原因究明が困難になるおそれがある。	・障害発生を記録しない。	・情報システムの障害発生を記録する。	・記録された障害毎に、明確な対応策または運用規則を定める。 ・対応策が決められていない場合の運用規則を定め	・情報システムが障害発生した場合は、システム管理者に通知する。			A.10.10.5	
41		ぜい弱性検査	システムのぜい弱性を管理する	情報システムのぜい弱な箇所を攻撃されると、情報が漏えいするおそれがある。	・ぜい弱性を修復しない。	・全てのソフトウェアに対して、セキュリティパッチの有無を、定期的に自己監査で確認する。	・ぜい弱性検査ツールによる検査を、ツール等で定期的に実施する。	・ぜい弱性検査ツールによる検査を、ツール等定期的に実施し、内部監査を実施する。			A.12.6.1	
42		媒体管理	取り外し可能な媒体を管理する	媒体が正しく運用されていないと、情報が漏えいするおそれがある。	・媒体を管理しない。	・媒体一覧を作成する。 ・媒体の利用記録を作成する。	・媒体の利用可能者を、システム的に制限する。	・媒体に保管した情報の、利用可能者をシステム的に制限する。			A.10.7.1	
43			媒体の配送方法を管理する	配送中の媒体が盗難又は紛失すると、情報が漏えいするおそれがある。	・媒体の配送に関するルールを決めない	・配送中は媒体を手元から離さない。 ・媒体の配送に外部業者を利用する場合は、機密保持や紛失時の損害賠償等について契約書に含める。	・媒体を配送する際は、媒体内データの暗号化もしくはアクセス制御機能つき媒体を利用する。	---> 前レベルと同様			A.10.8.3	
44		メール管理	メール送信のルールを決める	送信したメールが盗聴される、もしくは、メール送信先を間違えることにより、情報が漏えいするおそれがある。	・メール送信のルールを決めない。	・メール送信時は、宛先のメールアドレスを十分に確認するように教育する。	・添付ファイルを暗号化する。 ・メールの送信先を、システム的に制限する。	・メール全体を暗号化する。			A.10.8.4	
45			メール受信のルールを決める	不審なメールを受信してしまうと、悪意あるプログラムに感染する、情報が漏えいする、などのおそれがある。	・メール受信のルールを決めない。	・迷惑メール等を開かないように教育・指導する。	・迷惑メール等を、システム的にフィルタリングする。 ・ログ等で監視する。	---> 前レベルと同様			A.10.8.4	
46		廃棄	コンピュータを安全に廃棄、再利用する	廃棄、再利用したコンピュータに過去のデータが残っていると、情報が漏えいするおそれがある。	・データを消去せずにコンピュータを廃棄する。	・コンピュータの記憶領域について、初期化又はヌル値やランダム値の上書き等、残留データを消去する。 ・物理的に破壊する。	・コンピュータの記憶領域について、初期化又はヌル値やランダム値の上書き等、残留データを消去する。 ・廃棄証明書を履歴として保管する。	---> 前レベルと同様			A.9.2.6	
47			媒体を安全に廃棄、再利用する	廃棄、再利用した媒体に過去のデータが残っていると、情報が漏えいするおそれがある。	・データを消去せずに媒体を廃棄する。 ・紙をそのまま廃棄する。	・媒体の記憶領域について、初期化又はヌル値やランダム値の上書き等、残留データを消去する。 ・紙を廃棄する場合は、シュレッダーを利用する等、紙の復元を困難にする。	・媒体の記憶領域について、初期化又はヌル値やランダム値の上書き等、残留データを消去する。 ・廃棄証明書を履歴として保管する。 ・紙を廃棄する場合は、シュレッダーを利用する等、紙の復元を困難にする。	---> 前レベルと同様			A.10.2.7	
48	情報が事実と等しい（完全性保証）	原本性保証	送受信した情報が同一の内容であることを確認する	送受信した業務メッセージなどの情報が同一の内容であることを確認できないと、改ざんされた情報で業務が混乱するおそれがあ	・送信、受信された業務データの整合性を確認しない。	・送信、受信された業務データを人的手段(電話など）で確認する。	---> 前レベルと同様	・送信、受信された業務データに対して、パリティチェックなどでの整合性チェックをシステム的に実行する。			A.12.2.3	
49		監査	情報システムを監査する	情報システムを定期的に監査しないと、不正な活動が検出できなくて、情報を漏えいするおそれがある。	・内部監査をしない。	・個人的に、定期的な監査を実施する。	・定期的な監視と監視実績に基づいた監査を実施する。 ・監査については、定期的に社内組織に委託する。	・監視計画と監視実績に基づいた、監査を実施する。 ・監査については、定期的に第三者組織に委託する。			A.15.3	
50	システムを稼働し続ける（可用性保証）	冗長化	業務サーバ障害時に短時間で復旧させる	業務を行うためのサーバが停止すると、業務が停止して損失が大きくなる。	・サーバが復旧するまで業務を停止する。	・業務サーバのCPUを二重化する。 ・サーバ停止時にも、業務を数十分～数時間の停止で復旧する。	・業務サーバのCPUを二重化する。 ・サーバ停止時にも、業務を数分～数十分の停止で復旧する。	・業務サーバを二重化する。 ・サーバ停止時にも業務を停止させない。				
51		負荷分散装置の設置	高負荷時を考慮してシステムを設計する	システムや装置が処理できる負荷を超えてしまうと、システムの遅延、停止によって、業務が遅延、停止するおそれがある。	・処理能力を考慮しないでシステムを設計する。	・業務に必要なリソース(ネットワーク負荷）の計画と予測をする。 ・システムを、最大使用量で設計する。 ・高負荷時に、業務が遅延することはあるが、停止することはない設計をする。	・業務に必要なリソース(ネットワーク負荷）の計画と予測をする。 ・システムを、最大使用量よりも余裕を持たせて設計する。 ・高負荷時に、業務が遅延することはあるが、停止することはない設計をする。	・業務に必要なリソース(ネットワーク負荷）の計画と予測をする。 ・システムを、最大使用量よりも余裕を持たせて設計する。 ・高負荷時でも、業務が遅延する（レスポンスが低下する）ことのない設計とする。				
52		容量管理・拡張性	情報システムの処理能力を管理する	情報システムの処理能力が不足すると、情報システムが利用できなくなるおそれがある。	・情報システムの処理能力やディスク容量を監視しない。	・処理能力やディスク容量等について、利用者やデータの伸びに対し、一定期間対応可能な情報システムにする。	・拡張する際に、容易に対応可能な情報システムとする。	・情報システムの稼働能力を監視して、計画的に情報システムの容量の増強をことが容易にできるようなシステムとする。			A.10.3.1	
53		トラフィック監視・制御	ネットワークの運用を管理する	ネットワークの管理方針が整備されていないと、外部からの不正アクセスや情報漏えいのおそれがある。	・社外との境界においてネットワーク管理方針を定義しない。 ・インターネットとの接続箇所に、基本的なアクセスフィルタを実施できる装置(ルータ兼用型など)を設置する。	・社外との境界において適切なネットワーク管理方針を定義する。 ・ファイアウォールやUTM機器を設置して、適切なアクセスポリシーを設定する。	・社外との境界において適切なネットワーク管理方針を定義する。 ・ファイアウォールやUTM機器を設置して、適切なアクセスポリシーを設定する。 ・機器の運用状況を適切にモニタリングする。 ・ぜい弱性などに対するパッチ適用の運用体制を決める。	・社外との境界において適切なネットワーク管理方針を定義する。 ・ファイアウォールやUTM機器を設置して、適切なアクセスポリシーを設定する。 ・機器の運用状況を適切にモニタリングする。 ・ぜい弱性などに対するパッチ適用の運用体制を用意する。 ・運用状況を定期的にレポートする。 ・問題発生時の緊急運用体制を定義する。			A.10.6.1	
54			高負荷時を考慮してネットワークを設計する	ネットワーク障害や大量のデータ転送が発生すると、ネットワークが通常通りに利用できなくなるおそれがある。	・負荷を考慮しないでネットワークを設計する。	・通信会社のネットワークサービスを利用する場合は、帯域保証や稼働率に関する内容を、契約書に含める。	・インターネット接続回線や拠点間ネットワークを多重化する。	・インターネット接続回線や拠点間ネットワークについて、複数の通信会社からサービスを受ける。			A.10.6.2	

セキュリティ・可用性チェックシート（詳細項目版）

	技術的セキュリティ対策					推奨レベル			本件業務のセキュリティ仕様			
	要素	分類	対策項目	リスクの詳細	レベル1	レベル2	レベル3	レベル4	該当レベル	対策仕様	JISQ項番	参考文献（JIS Q 27002：2006以外）
55			ネットワークサービスの利用を管理する	ネットワークサービスへのアクセスを適切に制御しないと、社内外からサービスへの不正なアクセスが発生したり、情報が漏えいしたりするおそれがある。	・ネットワークサービス利用に関する方針を策定しない。	・ネットワークサービス利用に関する方針を策定する。	・ネットワークサービス利用に関する方針を策定する。 ・利用者に対して定期的に周知・徹底する。	・ネットワークサービス利用に関する方針を策定する。 ・利用者に対して定期的に周知・徹底する。 ・定期的な内部監査を行い、方針の運用状況を確認する。			A.11.4.1	
56			外部から接続する利用者を認証する	外部利用者を正しく認証できないと、外部からの不正アクセスで、情報漏えいしたり情報システムが停止したりするおそれがある。	・外部からのアクセスに対して利用者認証、監視、制御を実施しない。	・ユーザ名、パスワードでユーザ認証する。	・パスワードの複雑化や定期的な強制変更を実施する。 ・定期的なレポーティングを実施する。	・ワンタイムパスワードや生体認証などの、より高度なユーザ認証を併用する。			A.11.4.2	
57			ネットワーク上の装置を識別する	ネットワークを通過・拒否される装置が適切に識別できないと、不正アクセスなどの発生時に対応が長期化するおそれがある。	・どんな機器でもネットワークに接続できる。	・ネットワークにアクセスする装置種別(機種名、OS種別、バージョンなど)を判定する機器を導入する。 ・許可されない機器の接続を禁止する。	・外部からアクセスされる装置種別(機種名、OSバージョンなど)を判定する機器を導入する。 ・許可された機器のみ接続する。	・外部からアクセスされる装置種別(機種名、OSバージョンなど)を判定する機器を導入する。 ・ポリシー設定で、許可、不許可を自由にコントロールする。			A.11.4.3	
58			遠隔診断用及び環境設定用ポートを保護する	診断・管理用ポートへのアクセスが適切に管理されていないと、設定情報の不正な改ざん、システムの停止、などが発生するおそれがある。	・専用ポートへ誰でもアクセスできる。	・専用ポートに適切なアクセス権を設定する。	・専用ポートに適切なアクセス権を設定する。 ・マシンルームなどの専用ルームへ設置して、物理的に保護する。	・管理用ネットワークは通常のネットワークとは別に用意し、一般利用者からは物理的、論理的にアクセス不可能にする。			A.11.4.4	
59			ネットワーク領域を分割する	ネットワークを適切に分割しないと、不正にアクセスされるおそれがある。	・ネットワークを全く分割しない。	・ルータとスイッチでネットワークを物理的に分割する。	・プロジェクトもしくは組織単位でネットワークを分割する。 ・L3スイッチでネットワークを論理的に分割する。	・プロジェクトもしくは組織単位でネットワークを分割する。 ・VLANでネットワークを論理的に分割する。			A.11.4.5	
60			ネットワーク接続を制御する	ネットワークへの接続制御を実施しないと、不正アクセスや情報漏えいが発生するおそれがあ	・ネットワーク接続を制御しない。	・各ネットワーク境界で適切にアクセス制御する。	・アクセス違反を適切にモニタリングする。 ・異常時は自動的に警告する。	・アクセス違反を適切にモニタリングする。 ・異常時は自動的に警告する。 ・異常時は自動的に遮断する。			A.11.4.6	
61			ネットワークルーティングを制御する	内部・外部からの不正なルーティング情報が流入すると、既存のネットワーク情報が不正に変更されたり、情報システムが利用できなくなったりするおそれがある。	・制御しない。	・NATを使用し、外部に対して内部ネットワークを不可視にする。 ・静的ルーティングなど、固定的にルーティングを制御する。	・NATを使用し、外部に対して内部ネットワークを不可視にする。 ・管理下以外のネットワーク機器からのルーティング情報をフィルタする。	・NATを使用し、外部に対して内部ネットワークを不可視にする。 ・管理下以外のネットワーク機器からのルーティング情報をフィルタする。 ・ルーティング情報更新に認証情報（パスワードなど）を追加する。			A.11.4.7	
62		ソフトウェア監視	オペレーティングシステムを保守する	OSを保守しないと、業務停止、ぜい弱性の発生、情報の漏えい、などのおそれがある。	・OSを保守しない。	・セキュリティ対策などのパッチを本番機に直接適用する。	・本番相当環境で是正保守をテストし、障害がないことを確認し本番機に適用する。	・本番相当環境で是正保守、予防保守をテストし、障害がないことを確認し本番機に適用する。			A10.1.5？	
63			ソフトウェアを保守する	ソフトウェアを保守しないと、業務停止、ぜい弱性の発生、情報の漏えい、などのおそれがある。	・ソフトウェアを保守しない。	・セキュリティ対策などのパッチを本番機に直接適用する。	・本番相当環境で是正保守をテストし、障害がないことを確認し本番機に適用する。	・本番相当環境で是正保守、予防保守をテストし、障害がないことを確認し本番機に適用する。				
64			ソフトウェア修正情報を収集する	ソフトウェア修正のためのパッチ情報が把握されていないと、必要な是正保守が行われているかどうかが検証できず、ぜい弱性等が放置されるおそれがある。	・情報を収集しない。	・不定期に情報収集する。	・是正保守として、パッチ情報（提供元、種別、相互依存性、更新版の有無、仕様への影響等）の更新やベンダからの情報入手のサイクルを、運用ルールとして規定する。	・是正保守および予防保守として、パッチ情報（提供元、種別、相互依存性、更新版の有無、仕様への影響等）の更新やベンダからの情報入手のサイクルを、運用ルールとして規定する。				
65			パッチ適用の間隔を定める	是正保守としてのパッチ適用間隔がルール化されていないと、作業に長時間かかり、システムを長時間停止するおそれがある。	・パッチを適用しない	・パッチ適用に関するルールを設定しない。	・パッチを適用する間隔を是正保守として規定する。	・パッチを適用する間隔を、是正保守または予防保守として規定する。				
66			パッチ適用による障害の、回避策を定める	二次障害（パッチ適用による障害）への対策を規定しておかないと、システムを長時間停止するおそれがある。	・障害発生時に対応を検討する。	---> 前レベルと同様	・二次障害発生時の復旧（ロールバック等）作業をルール化する。	---> 前レベルと同様				
67			パッチ適用の作業時間を定める	パッチ適用の作業時間がルール化されていないと、システムを長時間停止するおそれがある。	・パッチを適用しない。	・パッチ適用に関するルールを設定しない。	・パッチを適用する作業時間を是正保守として規定する。	・パッチを適用する作業時間を、是正保守または予防保守として規定する。				
68			パッチ適用を検証し、管理する	パッチ適用状態を管理しないと、ぜい弱性等の危険が解消されないで残ってしまうおそれがある。	・パッチを適用しない。	・本番機に直接適用する。	・本番相当環境で是正保守をテストし、障害が無いことを確認し本番機に適用する。 ・適用状態を管理、監視する。	・本番相当環境で是正保守、予防保守をテストし、障害が無いことを確認し本番機に適用する。 ・適用状態を管理、監視する。				
69			ソフトウェアの変更を管理する	ソフトウェアのバージョンアップなどによる変更を管理していないと、業務に障害があった場合に原因の切り分けが遅れ、業務を長時間停止するおそれがある。	・ソフトウェアを変更しない。	・常に最新のソフトウェアを使用する。	・ソフトウェアの変更のたびに、影響度を確認し、承認を得て、テスト環境で実施し、ロールバック計画を立てて、本番環境に適用する。	・定期的に、影響度を確認し、承認を得て、テスト環境で実施し、ロールバック計画を立てて、本番環境に適用する。				
70		機器監視	電気設備を監視する	電気設備を監視していないと、停電や電圧異常で、システムやネットワーク機器が不安定になったり停止したりするおそれがある。	・電気設備を監視しない。	・無停電電源装置（UPS）を使用する。	・無停電電源装置（UPS）を使用する。 ・使用するUPSのログ機能などを使用し、システム上、重要なサーバやネットワーク機器の電圧異常を管理する。 ・異常時に管理者に対して通知する。	・無停電電源装置（UPS）を使用する。 ・使用するUPSのログ機能などを使用し、システム上、重要なサーバやネットワーク機器の電圧異常を管理する。 ・異常時に管理者に対して通知する。 ・建物の停電時に、一定時間システムを稼働し続けら			A.9.2.2	
71			空調設備を監視する	空調設備を監視していないと、温度の異常な上昇などで、システムやネットワーク機器が不安定になったり停止したりするおそれ	・空調設備を監視しない。	・システム上、重要なサーバやネットワーク機器を温度管理された部屋に配置する。	・システム上、重要なサーバやネットワーク機器自身の温度を管理する。 ・異常時に管理者に対して通知する。	・システム上、重要なサーバやネットワーク機器自身の温度を管理する。 ・異常時に管理者に対して通知する。 ・異常時に空調を自動的にコントロールする。				
72			通信ケーブルを使用した不正アクセスを防止する	通信ケーブルを使用した不正アクセスがあると、情報が漏えいするおそれがある。	・通信ケーブルを自由に使用できる。	・未使用ポートを使用不可に設定する。	・未使用ポートを使用不可に設定する。 ・ポートのLinkUp/Downを監視する。	・MACアドレス認証や、HUB接続などの複数機器の接続防止策を用意する。 ・ポートセキュリティを実施できる検疫システムを導入			A.9.2.3	
73			通信ケーブルの誤挿入・誤抜去を予防する	通信ケーブルの誤挿入・誤抜去が防げないと、システムが停止する恐れがある。	・通信ケーブルを自由に使用できる。	・ケーブルに適切なラベルを貼り、容易に識別できるようにする。	・ケーブルに適切なラベルを貼り、容易に識別できるようにする。 ・未使用ポートを使用不可に設定する。	・ケーブルに適切なラベルを貼り、容易に識別できるようにする。 ・未使用ポートを使用不可に設定する。 ・ポートのLinkUp/Downを監視する。				
74			監査ログを取得する	ネットワーク、システムからの異常検出ログを見逃すと、不正アクセスの検出が遅れたり、情報が漏えいしたりするおそれがある。	・監査ログを取得しない。	・各システムの監査ログ(アクセスログなど)を集約、確認できるように設定する。	・IDSなどにより、監査ログを解析して警告するシステムを導入する。	・IPSなどにより、監査ログを元に自動的にアクセスを拒否するシステムを導入する。			A.10.10.1	
75			システムの稼働状況を監視する	情報システムの稼働状況を監視していないと、問題が発生した際の原因究明が困難になるおそれがある。	・システムの稼動状況を監視しない。	・情報システムが正確に稼動しているか、手動で確認する。	・情報システムが正確に稼動しているか、自動で監視する。 ・定期的に監視状況をレポートする。	・情報システムが正確に稼動しているか、自動で監視する。 ・情報システムに障害が発生した際、緊急の警告を発する。			A.10.10.2	
76			ログ情報を保護する	ログ情報を保護していないと、ログへの不正アクセスや情報が改ざんされるおそれがある。	・ログ情報に誰でもアクセスできる。	・ログ情報は適切なアカウント、パスワードを持つ利用者のみがアクセスできるように設定する。	・アクセスできる機器を限定する。 ・成りすましなどによるアクセス対策(パスワードの定期的な変更、トークンなどの併用)を実施する。	---> 前レベルと同様			A.10.10.3	

セキュリティ・可用性チェックシート（詳細項目版）

	技術的セキュリティ対策					推奨レベル				本件業務のセキュリティ仕様			
	要素	分類	対策項目	リスクの詳細	レベル1	レベル2	レベル3	レベル4	該当レベル	対策仕様	JISQ項番	参考文献（JIS Q 27002：2006以外）
77			実務管理者及び運用担当者の作業を記録する	作業ログを適切に記録していないと、誤った作業などに対する事後確認を行うことができないおそ	・作業ログを取得しない。	・作業ログを保存する。	・作業ログを保存する。 ・事前に定めた規定に従い、定期的にレビューする。	---> 前レベルと同様			A.10.10.4	
78			障害発生時の状況を記録する	障害発生状況を記録していないと、障害が発生した際の原因究明が困難になるおそれがある。	・障害ログを取得しない。	・障害ログを含む、各種システムログを個別に取得する。	・システム全体の各種システムログを一元管理する。 ・障害発生時に各種警告を自動的に送る。	・システム全体の各種システムログを一元管理する。 ・障害発生時に各種警告を自動的に送る。 ・障害発生時の対応策を用意する。			A.10.10.5	
79			システム時刻を同期する	各システム時刻を同期させていないと、障害や不正アクセスの解析が煩雑になり、異常が発生した際の対応が長期化するおそ	・各システムの時刻を手動で個別に設定する。	・内部・外部NTPサーバを用意し、各システムをNTPに同期させる。	・複数のNTPサーバを用意する。	・GPSなどを利用した専用装置を設置する。			A.10.10.6	

セキュリティ・可用性チェックシート（詳細項目版）

	物理的セキュリティ対策					推奨レベル			本件業務のセキュリティ仕様			
	要素	分類	対策項目	リスクの詳細	レベル1	レベル2	レベル3	レベル4	該当レベル	対策仕様	JISQ項番	参考文献（JIS Q 27002：2006以外）
80	情報を他人から守る（機密性保護）	セキュリティ区画の定義	業務やプロジェクト単位で作業エリアを区分けする	業務部署やプロジェクトの区画を設定していないと、近隣の部署に情報が漏えいするおそれがある。	・作業エリアを決めない。	・仕切りはないが、業務・プロジェクト単位で島（列）を作る。	・業務・プロジェクト単位に、ついたて等で仕切りを作る。	・業務・プロジェクト単位に部屋を分けて作業する。			A.9.1.1	
81		マシンルームの設置	オフィスや部屋への入退出を管理する	入退出を管理していないと、部外者がオフィスや部屋に入れてしまい、情報を盗まれるおそれがある。	・オフィスや部屋等を施錠しない。	・オフィスや部屋の入退出時を、社員証などのIDで管理する。 ・帰宅時には、オフィスや部屋を鍵で施錠する。	・常時、ICカード又は生体認証等により、部屋の入退室を制限する。 ・守衛や防犯カメラを設置する。 ・部屋の入退室を記録する。	・入室ログのない退室は、許可しない。 ・インターロック（二重扉）を実施する。			A.9.1.3	・金融機関等コンピュータシステムの安全対策基準・解説書（第7版）設16, 連13
82			内部犯による情報機器の盗難を予防する	情報機器が内部の利用者に盗難されると、情報が漏えいするおそれがある。	・情報機器が自由に持ち出せる。	・コンピュータをワイヤー等で固定する。 ・サーバは、施錠されたサーバラック内に保管する。	・コンピュータをワイヤー等で固定する。 ・サーバは、施錠されたサーバラック内に保管する。 ・サーバ類の設置場所を、施錠された区域内にする。	・情報機器の設置場所を、アクセス制御された区域内にする。 ・情報機器（サーバ）の設置場所を、施錠された区域内にして、入退出の記録をとる。			A.9.2.1	・政府機関統一基準適用個別マニュアル群 庁舎内におけるPC利用手順 PCの取扱編 5.2 端末の設置 ・金融機関等コンピュータシステムの安全対策基準・解説書（第7版）設23
83		防犯設備の設置	外部犯による情報機器の盗難を予防する	外部からの侵入者に情報機器が盗難されると、情報が漏えいするおそれがある。	・情報機器の設置場所を監視しない。	・情報機器の設置場所を監視する。 ・外部からの不正な侵入に対して警報を鳴らす。	・情報機器の設置場所を監視する。 ・外部からの不正な侵入に対して警報を鳴らす。	・情報機器の設置場所を監視する。 ・外部からの不正な侵入に対して警報を鳴らし、通報する。			A.9.1.4	
84		マシンルームへの電磁波シールドの設置	情報機器を電磁波から保護する	電磁波からの保護ができていないと、情報データが破壊されるおそれがある。	・電磁波に対するシールド対策をしない。	---> 前レベルと同様	・電磁波に対するシールド対策を、コンピュータやネットワーク機器に施す。	・マシンルームに対して電磁波のシールド対策をする。			A.9.1.4	
85	情報が事実と等しい（完全性保証）	定期的なバックアップ取得	業務データのバックアップを安全な場所に保管する	バックアップを安全な場所に保管しないと、不慮の災害発生時などにシステムを業務可能な状態に復旧できなくなるおそれがある。	・業務データをバックアップしない。	・業務に必要なデータを媒体に、定期的(日次、週次)バックアップを行い、安全な場所に輸送して保管する。	・業務に必要なデータを、遠隔地にリモートで、定期的（日次、週次）にバックアップを行う。	・業務に必要なデータを遠隔地にリモートで、リアルタイムにバックアップする。			A.10.5.1	
86			復旧時間を考慮してバックアップ媒体を選択する	復旧に要する時間を考慮してバックアップ媒体を選択しないと、必要な時間内にシステムを復旧できないおそれがある。	・業務データをバックアップしない。	・バックアップデータを、テープや光ディスクのような運搬可能な媒体に保管する。	・バックアップデータを、ハードディスクに保管する。	---> 前レベルと同様				
87	システムを稼働し続ける（可用性保証）	温度・湿度管理	情報機器の設置場所の環境を適切に保つ	温度や湿度を適切に保たないと、情報システムが正常に動作しなくなるおそれがある。	・空調を設置しない。	・空調を設置する。 ・湿度を40～60%に保つ（静電気対策）。	・空調を設置する。 ・湿度を40～60%に保つ（静電気対策）。 ・結露を発生させない。	・空調を、故障に備えて、冗長化する。			A.9.1.4	・金融機関等コンピュータシステムの安全対策基準・解説書（第7版）設33
88		耐震、耐火、耐水対策済み施設の利用	情報機器を災害から守る	地震、火災、洪水等の災害への対策を整えておかないと、情報システムが故障し、業務が長期間停止するおそれがある。	・災害を考慮しない。	＜耐震＞ ・情報機器を、落下防止金具もしくはバンド等で固定する。 ・サーバラックを、パネルアンカー等で固定する。 ＜耐火＞ ・自動火災報知設備を設置する。 ・消火設備（消火器、スプリンクラー）を設置する。 ・情報機器を、火災の危険性のない場所（火使用設備が隣室又は直上下階にない場所等）に設置する。 ・室内の火気使用を制限する。 ＜耐水＞ ・情報機器を、浸水の危険性のない場所（2階以上、水使用設備が隣室又は直上階にない場所等）に設置する。	＜耐震＞ ・情報機器を、落下防止金具もしくはバンド等で固定する。 ・サーバラックを、パネルアンカー等で固定する。 ＜耐火＞ ・自動火災報知設備を設置する。 ・消火設備（消火器、スプリンクラー）を設置する。 ・情報機器を、火災の危険性のない場所（火使用設備が隣室又は直上下階にない場所等）に設置する。 ・室内の火気使用を制限する。 ＜耐水＞ ・情報機器を、浸水の危険性のない場所（2階以上、水使用設備が隣室又は直上階にない場所等）に設置する。	＜耐震＞ ・建物を、免震建築物もしくは制振建築物にする。 ・情報機器を、免震床に設置する。 ＜耐火＞ ・消火設備（全域放出型消火ガス）を設置する。 ＜耐水＞ ・漏水を排出する排水溝等を設置する。			A.9.1.4	・金融機関等コンピュータシステムの安全対策基準・解説書（第7版）設22, 32, 37, 39, 50
89		無停電電源装置、バックアップ電源等の設置	電力を安定供給する	電力を安定供給しないと、停電や電圧異常で、システムやネットワーク機器が不安定になったり停止したりするおそれがある。	・停電対策を実施しない。	・UPSを設置する。 ・建物に、避雷針を設置する。 ・静電気対策として、アースを利用する。	・自家発電装置を設置する。	・電力会社から、電源を複数回線で引き込む。			A.9.2.2	・金融機関等コンピュータシステムの安全対策基準・解説書（第7版）設62, 64, 65, 69
90		ケーブル敷設経路対策の実施	通信、電源ケーブル配線を保護する	通信、電源ケーブルが切断されてしまうと、情報システムが停止する、長期間利用できなくなるおそれがある。	・通信、電源ケーブルをむき出しにする。	・通信、電源ケーブルは、フリーアクセス床の下を通す。 ・通信、電源ケーブルに、カバーをつける。	---> 前レベルと同様	・通信、電源ケーブルは、専用の配線管を通し、人目につかないように設置する。			A.9.2.3	・金融機関等コンピュータシステムの安全対策基準・解説書（第7版）設97
91		在庫管理	情報資産を管理する	情報資産（情報機器・電子媒体・紙）が管理されていないと、紛失・盗難の検出ができないおそれがある。	・情報資産を管理しない。 ・媒体や紙資産の、保管場所や管理番号がない。	・情報資産を部署単位で管理する。 ・媒体や紙資産については、管理番号は付与せずに、カテゴリ別で保管する。	・情報資産の管理にツールを使う。 ・管理番号を付与して管理する。 ・媒体や紙の資産については、管理番号を付与して、管理台帳等で所在を明確にして、鍵をかける。	・情報資産の管理にツールを使う。 ・管理番号を付与して、定期的に内部監査する。 ・媒体や紙の資産については、管理番号を付与して、管理台帳等で所在を明確にして、鍵をかける。 ・鍵は管理者が管理する。			A.7	
92			情報資産の管理責任を明確にする	情報資産の責任者が明確でないと、資産の管理・保存期限、滅却などが計画的におこなわれず、不要になった資産から情報が漏えいするおそれがある。	・利用者の判断で資産を保存・滅却する。	・資産ごとに管理責任者を決め、管理責任者の判断で資産を保存・滅却する。	・資産ごとに管理責任者・保存期間・滅却期日を決め、定期的に資産を見直す。	・資産ごとに管理責任者・保存期間・滅却期日を決め、資産管理を計画的に実施する。			A.7.1	
93		機器設置スペースの拡張性	機器設置スペースに拡張性を持たせる	機器設置場所に拡張性がないと、情報処理機器をセキュリティが低い場所に設置しなくてはならなくなる。	・設置スペースを拡張しない。	・情報処理機器の設置スペースを確保する時に、現在の業務処理データ量を考慮する。	・将来の業務拡張計画などから、情報処理機器の設置スペースを設計する。	---> 前レベルと同様				

セキュリティ・可用性チェックシート（詳細項目版）

	管理的セキュリティ対策				推奨レベル			本件業務のセキュリティ仕様			
	要素	分類	対策項目	リスクの詳細	レベル1	レベル2	レベル3	レベル4	該当レベル	対策仕様	JISQ項番	参考文献（JIS Q 27002：2006以外）
94	情報を他人から守る（機密性保護）	セキュリティポリシー	セキュリティポリシーを策定する	セキュリティ基本方針を定義しておかないと、一貫したセキュリティ対策がとれず、ぜい弱なシステムになってしまうおそれがある。	・セキュリティポリシーを策定しない。	・現状を把握し、リスク分析の結果をもとに、情報セキュリティ基本方針を策定する。	---> 前レベルと同様	---> 前レベルと同様			A.5.1	
95		利用者管理	情報にアクセスするためのガイドラインを策定する	情報アクセスのためのガイドラインを策定しておかないと、情報を制御する対象や範囲が明確にならない。	・アクセス制御方針を策定しない。	・情報へのアクセス制御方針を文書化する。	・情報へのアクセス制御方針を文書化する。 ・定期的にレビューする。	・情報へのアクセス制御方針を文書化する。 ・定期的にレビューする。 ・アクセス方針に従った業務であることを、監査する。			A.11.1.1	
96			システムの利用者を管理する	情報システムの利用者を管理していないと、部外者がシステムを利用できてしまい、情報が漏えいする可能性がある。	・利用者を登録、管理しない。	・一つのアカウントを複数の利用者で使用しない。 ・利用者の増減や移動に伴い、アカウント及びアクセス権を変更する。	・利用者の増減や移動をシステムで管理し、アカウント及びアクセス権を自動的に変更する。	・利用者の増減や移動をシステムで管理し、アカウント及びアクセス権を自動的に変更する。 ・登録情報として、生体認証を導入する。			A.11.2.1	
97			特権を持つ利用者を管理する	特権を持つ利用者の作業を管理しないと、機密情報を不正に操作されて外部に漏えいされるおそれがある。	・特権ユーザの履歴ログを取得しない。	・特権ユーザを絞り込み、特権ユーザの操作ログを取得する。	・特権ユーザを絞り込み、特権ユーザの操作ログを取得して定期的に監査する。	---> 前レベルと同様			A.11.2.2	
98			利用者のパスワードを管理する	利用者のパスワードを定期的に変更するなどの管理をしていないと、パスワードが流出し、システムに不正アクセスされる、情報が盗まれる、などのおそれがある。	・パスワードを変更しない。	・利用者のパスワードが、定期的に変更されていることをチェックする。	---> 前レベルと同様	・利用者のパスワードが定期的に変更されるシステムを導入する。 ・変更依頼のメッセージをシステムから送る。			A.11.2.3	
99			利用者のアクセス権を管理する	利用者のアクセス権を定期的に見直さないと、プロジェクトや組織の変更にともなって、参照できてはいけないものが継続して見えてしまい、情報が漏えいするおそれがある。	・アクセス権を見直さない。	・アカウント及びアクセス権を、定期的に見直す。	---> 前レベルと同様	・組織やプロジェクトが変更になった場合、ユーザ管理システムと連携して、自動的にアクセス権を変更する。 ・変更になったアクセス権を定期的に監査する。			A.11.2.4	
100			情報処理施設の使用を記録する	情報処理施設が不正に使用されると、情報処理機器へアクセスされて、情報が漏えいするおそれがある。	・情報処理施設への入出や使用を記録しない。	・情報処理施設への入出を記録する。	・情報処理施設の入出記録をシステムで取得する。 ・定期的に監査する。	・情報処理施設の入出記録をシステムで取得する。 ・施設への入館時に、許可されている利用者であるかを自動的にチェックする。 ・定期的に監査を行う。			A.15.1.5	
101			情報を暗号化する	情報の暗号化をルールとして企業内で統一しておかないと、利用者毎に暗号化対象が変わってしまい、重要情報が漏えいするおそれがある。	・暗号化しない。	・個人の判断で、ファイルを暗号化する。	・情報(データ）を強制的に暗号化する。	・すべてのファイルを強制的に暗号化する。			A.15.1.6	
102		入退室管理	作業領域を施錠し監視する	オフィス等の作業領域を施錠、監視しておかないと、部外者が不正に侵入し、情報の漏えいや情報機器の盗難等のおそれがある。	・オフィス等を施錠しない。	・帰宅時には、部屋を鍵で施錠する。	・常時、ICカード又は生体認証等で、部屋の入退室を制限する。 ・防犯カメラを設置する。 ・部屋の入退室を記録する。	・入室ログのない退室は、許可しない。 ・インターロック（二重扉）を実施する。			A.9.1.2	・金融機関等コンピュータシステムの安全対策基準・解説書（第7版） 設16, 運13
103		秘密保持契約	第三者との契約内容を定める	第三者との契約内容をあらかじめ決めておかないと、機密保持契約がないために情報漏えい時の責任追及ができないなど、情報が守られなくなるおそれがあ	・契約内容をあらかじめ規定しない。	・第三者との間で、担当者が機密保持契約を交わす。	・第三者との間で、担当部署間が機密保持契約を交わす。 ・機密保持契約には、情報の入手についてセキュリティを守る条項を明記する。	・第三者との間に、双方の法務部門を通して、会社名義で機密保持契約を交わす。 ・機密保持契約には、情報の入手についてセキュリティを守る条項を明記する。			A.6.2.3	
104		ぜい弱性情報収集と修正プログラム適用	ぜい弱性情報を入手して対策する	OSやアプリケーションのぜい弱性の情報が入手できないと、ぜい弱性がそのまま放置されて、情報が漏えいするおそれがある。	・ぜい弱性情報を収集しない。	・OSやアプリケーションのぜい弱性レポートを定期的に入手して、パッチ適用を計画する。	・OSやアプリケーションのぜい弱性レポートを定期的に入手して、パッチ適用を計画する。 ・本番相当環境で是正保守をテストし、障害がないことを確認し本番機に適用する。	・OSやアプリケーションのぜい弱性レポートを随時入手して、パッチ適用を計画する。 ・本番相当環境で是正保守、予防保守をテストし、障害がないことを確認し本番機に適用する。			A.12.6.1	
105		資産管理	情報資産を管理する	情報資産を正確に管理しておかないと、資産を紛失、盗難しても気付かないおそれがある。	・情報機器の一覧を作成しない。	・情報機器の一覧を作成する。 ・情報機器一覧の棚卸を行う。	・情報資産（情報そのもの）の一覧を作成する。	・情報資産の管理にツールを使い、拾い上げ、管理番号が付与されており、定期的に内部監査などを実施する。 ・媒体や紙の資産については、管理番号を付与して、管理台帳等で所在が明確にして、施錠する。			A.7.1.1	
106			情報資産を分類する	情報資産が重要度に応じて正しく分類されていないと、重要な情報が厳重に管理されず、権限のない利用者に情報が漏えいするおそれがある。	・情報資産の分類基準を作成しない。	・情報資産の分類基準（極秘、秘、社外秘等）を作成する。	・情報資産の分類基準（極秘、秘、社外秘等）を作成する。 ・分類ごとに資産番号を付与する。	・情報資産の分類基準（極秘、秘、社外秘等）を作成する。 ・分類ごとに資産番号を付与する。			A.7.2.1	
107			情報資産を分類に応じて取り扱う	情報資産が分類基準に従って取扱わないと、権限のない利用者に情報が漏えいするおそれがある。	・情報資産を分類基準に従って取扱わない。	・資産ごとに管理責任者を決める。 ・管理責任者の判断で資産を保存・滅却する。	・情報資産に、分類基準に従って分類した結果を明記する。 ・情報資産を、分類基準に従って取扱う。 ・資産ごとに管理責任者、保存期間、滅却期日を決める。	・情報資産に、分類基準に従って分類した結果を明記する。 ・情報資産を、分類基準に従って取扱う。 ・資産ごとに管理責任者、保存期間、滅却期日を決める。			A.7.2.2	
108			机上の情報を保護する	情報が机上に放置や表示された状態になっていると、目視で情報が漏えいするおそれがある。	・机上での情報の取り扱いルールがない。	・帰宅時には、書類を机上に放置しない。 ・一定時間（30分）が経過したら、画面を自動的にスクリーンロックする。	・離席時には、書類を机上に放置しない。 ・離席時には、すみやかに、画面を操作不可能な状態（ログオフ、スクリーンロック等）にする。 ・一定時間（10分）が経過したら、画面を自動的にスクリーンロックする。	・ディスプレイに、盗み見防止のフィルタを装備する。 ・ディスプレイに、電磁波対策のフィルタを装備する。		A.11.3.3	・政府機関統一基準適用個別マニュアル群 庁舎内におけるPC利用手順 PCの取扱編 5.1 端末機能にかかわる検討、5.2 端末の設置(10)
109	情報が事実と等しい（完全性保証）	情報のバックアップ	情報をバックアップする	情報を適切にバックアップしていないと、情報の消失、改ざん等が発生した際に、復旧できなくなってしまうおそれがある。	・バックアップを取得しない。	・バックアップのポリシー（世代管理、バックアップ対象、取得サイクル等）を作成する。 ・ポリシーに従い、情報をバックアップする。 ・リストアが、適切な時間内に可能であることを確認する。	・バックアップ媒体を、同一建物内に保管する。 ・バックアップデータを、暗号化する。	・バックアップ媒体を、遠隔地（60km以上）に保管する。			A.10.5.1	・金融機関等コンピュータシステムの安全対策基準・解説書（第7版） 運27
110		情報システムの正確性	システムを受入れる時に検証する	システムを受け入れる際に十分な検証を実施しないと、運用開始後にシステムの不良に気づくことになり、長期間業務が停止してしまうおそれがある。	・システムをテストしない。	・システムを新たに導入もしくは変更する場合は、本番稼動前にテストする。 ・システム開発者がテストした結果を見て検収する。	・システムを新たに導入もしくは変更する場合は、本番稼動前にテストする。 ・受け入れテストを第三者に委託して、客観的にテストする。	・システムを新たに導入もしくは変更する場合は、本番稼動前にテストする。 ・自社内に受け入れ検査の体制と、受け入れ検査用のデータを用意して、擬似本番環境にて適切な期間検収テストを行う。			A.10.3.2	
111		情報の正確性	入力データの正確さを追求する	入力されたデータが正確でないと、誤りが多い情報になってしまい、業務が停止してしまうおそれ	・入力データをチェックしない。	・入力フィールドには、可能な限り、文字種や桁数等の制限をつける。	・データ入力作業を委託する場合、入力誤り率に関するサービスレベルを契約で取り決める。 ・入力データの妥当性をシステムでチェックする。	---> 前レベルと同様			A.12.2.1	
112	システムを稼働し続ける（可用性保証）	教育と訓練	セキュリティ教育を実施する	セキュリティや情報漏えいに対する基本方針などを利用者が正しく理解していないと、安易に情報を取り扱い外部に漏えいしてしまうおそれがある。	・セキュリティ教育をしない。	・部署単位で、セキュリティ教育を定期的に実施する。	・部署単位で、セキュリティ教育を定期的に実施し、教育受講者を管理する。 ・作業外注者に対してセキュリティ教育を実施する。	・組織のトップから、全社員に対してセキュリティメッセージを通達する。 ・部署単位で、セキュリティ教育を定期的に実施し、教育受講者を管理する。 ・作業外注者に対してセキュリティ教育を実施する。 ・会社組織として、セキュリティ教育推進部署を設置する。			A.8.2.2	
113		運用体制	利用者の活動を管理する	企業内の組織で運用する場合、悪意を持った利用者から情報が漏えいするおそれがある。	・利用者の操作ログを取得しない。	・利用者の操作ログを取得して、定期的に監査する。	---> 前レベルと同様	・複数の責任者で相互に監視する。 ・利用者の操作ログを取得して、定期的に監査する。			A.6.1	
114			外部組織を管理する	運用を第三者組織に委託した場合、委託先から情報が漏えいするおそれがある。	・利用者の操作ログを取得しない。	・利用者の操作ログを取得して、定期的に監査する。	---> 前レベルと同様	・利用者の操作ログを取得して、定期的に監査する。 ・コンピュータの操作画面をモニターする。			A.6.2	

セキュリティ・可用性チェックシート（詳細項目版）

	管理的セキュリティ対策					推奨レベル			本件業務のセキュリティ仕様			
	要素	分類	対策項目	リスクの詳細	レベル1	レベル2	レベル3	レベル4	該当レベル	対策仕様	JISQ項番	参考文献（JIS Q 27002：2006以外）
115		監査	情報システムの運用を監査する	情報システムを定期的に監査していないと、不正な活動を検出できなくて、情報が漏えいしてしまうおそれがある。	・情報システムを監査しない。	・定期的に、個人による監査を実施する。	・監視計画と監視実績に基づいた監査を実施する。 ・監査については、定期的に社内組織に委託する。	・監視計画と監視実績に基づいた監査を実施する。 ・監査については、定期的に第三者組織に委託する。			A.15.3	
116		緊急時対応計画	情報漏えい時の対応を管理する	漏えい事故のレベルによって対応を管理していないと、対応が遅れ被害が大きくなるおそれがある。	・漏えい事故を管理しない。	・漏えい事故を管理する。 ・すべての漏えい事故を同様に扱う。	・漏えい事故を管理する。 ・漏えい事故に対する、レベル判断基準を設定する。 ・漏えい事故のレベルに応じた対応を規定しない。	・漏えい事故に対する、レベル判断基準を設定する。 ・レベルに応じた対応を、組織的な手順として確立する。 ・事故対応の情報、活動が、組織のトップまでスムー			A.13	
117			情報セキュリティ事象を報告する	情報セキュリティに何らかの変化があった場合の報告の仕組みが規定されていないと、対応が遅れて被害が拡大するおそれがある。	・情報セキュリティ事象の報告ルートを規定しない。	・情報セキュリティ事象の報告ルートを規定する。	・情報セキュリティ事象の報告ルート、速やかな報告ルールを規定する。	---> 前レベルと同様			A.13.1.1	
118			セキュリティの弱点を報告する	セキュリティの弱点が発見されても報告する仕組みがないと、報告が遅れ、弱点を攻撃されたり、弱点を利用して情報が漏えいしたりする。	・セキュリティの弱点の報告ルートを規定しない。	・セキュリティの弱点の報告ルートを規定する。	・セキュリティの弱点の報告ルート、速やかな報告ルールを規定する。	---> 前レベルと同様			A.13.1.2	
119			情報の取り扱いを記録する	誰がどのように情報を取り扱ったかを記録していないと、情報漏えい発生時に原因の追及が困難になり、再発を防げないおそれがある。	・情報の取り扱いを記録しない	・情報の取り扱い履歴を、ログに記録する。	・情報の取り扱い履歴を、ログに記録する。 ・利用者の情報の取り扱いを、ログに記録する。 ・情報のログと、利用者のログを利用して、情報の流通経路をトレースするシステムを導入する。	---> 前レベルと同様			A.13.2.3	
120		見直し	情報セキュリティ事故を管理して改善する	情報セキュリティ事故の管理を定期的に見直して改善しないと、同じような事象が発生するおそれがある。	・情報セキュリティ事故を管理しない。	・情報セキュリティ事故を管理する。 ・不定期に事故の改善を実施する。	・情報セキュリティ事故を管理する。 ・定期的に事故の改善を実施する。	・情報セキュリティ事故を管理する。 ・事故発生直後に改善を実施する ・定期的に事故改善を見直す。			A.13.2	

Webアプリケーション セキュリティ・可用性チェックシート（詳細項目版）

	要素	分類	対策項目	リスクの詳細	推奨レベル レベル1	レベル2	レベル3	レベル4	本件業務のセキュリティ仕様 該当レベル	対策仕様	JISQ項番	参考文献（JIS Q 27002：2006以外）
1	情報を他人から守る（機密性保護）	ユーザ認証	パスワードを利用する	パスワードが推測可能な容易なものになっていると、第三者がシステムに不正アクセスし、情報を漏えいしてしまうおそれがある。	・パスワードを設定しない。	・初期パスワードをすみやかに変更する。 ・定期的（六ヶ月毎）に、パスワードを変更する。 ・パスワードは、複雑なもの（八桁以上）を設定する。 ・パスワードは、管理者を含め誰にも教えない。 ・パスワードを書き留めたり、コンピュータ上のファイルに保管したり、メールで送信したりしない。やむを得ず紙片等にパスワードを記載する必要がある場合には、そのパスワードが容易に第三者に見られることがないように保管する。 ・自分のパスワードが他人に漏えいした可能性や疑いがある場合は、パスワードを変更する。	・定期的（三ヶ月毎）に、パスワードを変更する。 ・パスワードは、複雑なもの（八桁以上、パスワード世代管理、三種類以上の文字種の使用）を設定する。	・同一利用者が複数のアカウントをもつ場合は、それぞれ異なるパスワードを設定する。 ・一つのパスワードから他方が推測しやすいパスワードを設定しない。 ・生体認証を利用する。			A.11.2.3 A.11.3.1 A.11.5.2 A.11.5.3	・政府機関統一基準適用個別マニュアル群 庁舎内におけるPC利用手順 PCの取扱編 端末利用者パート 2.3 識別コードの日常の取扱い(2), (3)
2			ログインの認証方法をルール化する	認証に関するルールが明確になっていないと、第三者がシステムに不正アクセスし、情報を漏えいしてしまうおそれがある。	・認証に関するルールを定めない。	・認証の再試行可能回数を定める。 ・再試行可能回数を超えて認証が失敗した場合は、二十四時間当該アカウントを停止する。 ・認証情報はセッションまたはCookieに保存する。 ・ログインID/パスワード等の認証情報をCookie上に暗号化せずに保存する。	・認証画面(機能)を使用して、コンピュータとアプリケーションを利用する。 ・一定回数以上ログオンに失敗したアカウントは、ロックアウトさせる。 ・パスワードの定期的な変更を、システム機能により強制させる。 ・パスワードを他人から推測されにくいものにすることを、システム機能により強制させる。 ・パスワードをシステム内に保存する場合は、暗号化する。 ・パスワードをクライアントーサーバ間で通信する場合は、暗号化する。	・認証のログを採取する。 ・ログインID/パスワードはセッション上に保存せず、利用者をシステム側で管理する一意な文字列をセッションに保存する。			A.11.3.2 A.11.4.2 A.11.5.2	Web Application Security Consortium http://www.webappsec.org/
3			ログイン状態の継続をルール化する	ブラウザを閉じた後もアプリケーションに対しての認証状態を継続させる場合、第三者の操作によって情報が漏えいするおそれがある。	・認証状態の継続に関するルールを定めない。	・ブラウザを閉じた後も、期限を定めずシステムに対しての認証状態を継続する。	・ブラウザを閉じた後も、一定期間システムに対しての認証状態を維持する。 ・認証状態の維持は、ユーザの明確な意思によって行われるものとし、その操作方法について明記する。	・個人情報及び、商取引を行うページへのアクセスの際には、たとえ既にログイン状態であったとしても、再度ログインを行うようユーザに要求し、第三者による不正な操作を防止する。			A.11.4.2 A.11.5.5	
4			認証画面を暗号化する	認証画面へアクセスする際に、SSLによる暗号化などを施さないと、通信経路を傍受され、情報漏えいが発生するおそれがある。	・認証画面を暗号化しない。	・認証画面を暗号化する。 ・SSLの鍵の種類については規定を設けない。	・SSLの鍵長は128Bitを使用する。	・SSL証明書は、EV-SSL証明書を使用する。			A.11.5.1	
5		アクセス権限	アクセス権限を策定する	アクセス権限を策定しないと、利用者のアクセス可能範囲が明確とならないため、不正なアクセスを許してしまうおそれがある。	・アクセス権限を定めない。	・利用者と管理者にクライアントを分類する。 ・利用者は、管理者の機能を使用できないものとする。	・管理者の中に権限の階層を設ける。 ・管理者であっても、所定の権限がない場合はアクセスを許可しない。	・各機能へのアクセスログを採取する。			A.11.2.4 A.11.6.1	
6		暗号化	データを暗号化する	データを暗号化しないと、個人を特定できる情報が漏えいした場合、第三者にその情報が知られるおそれがある。	・データを暗号化しない。	・クレジットカード等の情報に限定して暗号化する。 ・暗号化に使用する文字列を暗号化しない。	・個人を特定できる情報を暗号化する。 ・暗号化に使用する文字列を暗号化する。 ・暗号化に使用する文字列は、管理者以外でも容易に知ることができる。	・全てのデータを暗号化する。 ・暗号化に使用する文字列は、管理者以外に知らせない。			A.10.7.3	
7			パスワードを暗号化する	パスワードを暗号化しないと、第三者によってデータの漏えいが起きた場合、パスワードが第三者に知られるおそれがある。	・パスワードを暗号化しない。	・パスワードは、復号可能な方式を使用して暗号化する。	・パスワードは復号できない方式を使用して暗号化し、たとえシステム管理者であってもユーザのパスワードを復号できないようにする。	---> 前レベルと同様			A.10.7.3	
8		セッション・Cookieの運用	セッションを使用したデータ保持の方法を利用する	セッションの運用ルールを定めないと、第三者によってセッション上のデータが漏えいするおそれがある。	・セッションの使用ルールを定めない。	・セッションIDは、開発に使用するアプリケーションが規定するものを使用する。 ・セッションはWebブラウザを閉じるまでの間有効とする。 ・新規にWebブラウザにてアクセスする度にセッションを作成する。 ・セッションIDはURL文字列またはCookieに保存する。	・一定時間以上アクセスがない場合、システム側でセッションを自動的に破棄し、利用者にはセッションが期限切れとなった旨を通知する。 ・認証及び個人情報を操作する処理においては、アクセスのたびにセッションを再作成する。 ・セッションIDはCookieに保存する。	・セッションを使用するすべての処理で、アクセスのたびにセッションを再作成する。 ・セッションIDを格納するCookieは、暗号化通信が行われている環境下でのみ使用する。			A.11.5.5	
9			Cookieを使用したデータ保持の方法を利用する	Cookieの運用ルールを定めないと、第三者による盗聴等の被害を受けるおそれがある。	・Cookieの使用ルールを定めない。	・ログインID/パスワード等の認証情報をCookie上に保存する。 ・Cookieの有効期限は三十日以内とする。 ・Cookieは保有するドメイン全体で使用する。 （例：xxxxx.com）	・システムが認識できる、意味を持たない文字列を認証情報の代替として保存する。 ・認証情報を扱うCookieについては、セッションの有効期限に準じた有効期限を使用する。 ・その他の情報のCookieへの保存は許可しない。 ・Cookieは使用するドメインでのみ使用する。 （例：www.xxxxx.com）	・利用者の嗜好分析・行動解析に使用する、個人を特定することができない情報に限り、Cookie上への保存を許可する。 ・ログイン情報等を取り扱うCookieについては、Cookieを発行したドメインでのみ使用する。			A.11.5.5	
10		アプリケーションの対策	偽Webサイトによるフィッシング詐欺を対策する	Webサイトでむやみにフレームなどを使用すると、コンテンツの詐称によりパスワードの抜き取りやフィッシング詐欺サイトへの誘導の危険性があります。	・Webサイトのデザインについてのルールを定めない。	・フレームを使用しない。 ・IFRAME/レイヤーについては規定しない。	・IFRAME/レイヤーを使用しない。	・管理者機能の、管理者自らの操作によってHTMLを使用したコンテンツを作成する場合に限り、IFRAME/レイヤーの使用を許可する。			A.10.4.1 A.12.2.4	Web Application Security Consortium http://www.webappsec.org/
11			クロス・サイト・トレーシングを対策する	クロス・サイト・トレーシングが使用されると、他のぜい弱性を利用して、第三者が利用者（会員等）や管理者に成りすますおそ	・「TRACE」メソッドを有効にする。	・「TRACE」メソッドを無効にする。	・「TRACE」メソッドを無効にする。 ・攻撃を検出して、ログをとる。	・WAFを導入する。 ・攻撃を検出して、管理者に通知する。			A.10.4.1	Web Application Security Consortium http://www.webappsec.org/
12			クロス・サイト・スクリプティング（XSS）を対策する	クロス・サイト・スクリプティング（XSS）が使用されると、パスワードの抜き取りやフィッシング詐欺サイトへの誘導、情報漏えい等のおそれがある。	・利用者が入力した値をそのまま利用する。	・利用者が入力した値は、例外なく無害化処理を施した上で表示する。	・攻撃を検出して、ログをとる。	・WAFを導入する。 ・攻撃を検出して、管理者に通知する。			A.10.4.1 A.12.2.4	Web Application Security Consortium http://www.webappsec.org/
13			クロス・サイト・リクエスト・フォージェリを対策する	クロス・サイト・リクエスト・フォージェリを使用されると、第三者によるWebサイトの改ざん等のおそれがある。	・ログイン後の画面を、URL直入力でいつでも表示することができる。	・ログイン後の画面は、URL直入力などによる画面表示を禁止し、正規の画面遷移のみ許可する。	・1アクセス毎に有効な、セッションIDとは異なるIDを利用者に付与しシステム側と照合することで、正規の画面遷移以外を排除する。 ・攻撃を検出して、ログをとる。	・WAFを導入する。 ・攻撃を検出して、管理者に通知する。			A.10.4.1 A.12.2.1	Web Application Security Consortium http://www.webappsec.org/
14			パラメータ改ざんを防止する	パラメータ改ざんが発生すると、第三者が利用者（会員等）や管理者に成りすますおそれがある。	・パラメータ改ざんをチェックしない。	・入力フォームの値について改ざんがされていないか、遷移先のページでチェックする。	・外部から入力（入力フォーム、URLパラメータやhidden、Cookie、ヘッダパラメータ等による入力）について改ざんがされていないか、遷移先のページでチェックする。	・WAFを導入する。 ・攻撃を検出して、管理者に通知する。			A.10.4.1 A.12.2.1	Web Application Security Consortium http://www.webappsec.org/
15			ネットワークの過負荷と、サーバへの過大な同時アクセスを対策する	バッファオーバフローを使用されると、Webサーバのサービス停止や、Webサーバを乗っ取られるおそれがある。	・サーバ上で使用するアプリケーションのバージョン管理をしない。	・アプリケーションのバージョンを管理し、バージョンアップ計画を作成して、順次最新の状態になるように運用する。	・重要なぜい弱性が報告された場合は、即時バージョンアップ対応を行う。 ・対策バージョンのリリースまでに時間がかかる場合に、ぜい弱性の報告内容から自社アプリケーションに該当の事象があるかを調査し、可能な範囲での対策を講じる。	・重要なぜい弱性が報告された場合は、即時バージョンアップ対応を行う。 ・即時対応が不可能な場合はサービスを停止する。			A.12.2.2	Web Application Security Consortium http://www.webappsec.org/
16			サーバへの不正な要求によるサーバ攻撃を対策する	書式文字列攻撃されると、Webサーバのサービス停止や、Webサーバを乗っ取られるおそれがある。	・何も対策を施さない。	・printf等の書式文字列関数のパラメータに、外部から入力したデータを使用する際は、書式文字列攻撃の対策を実施する。	・書式文字列関数を使用しない。 ・攻撃を検出して、ログをとる。	・WAFを導入する。 ・攻撃を検出して、管理者に通知する。				Web Application Security Consortium http://www.webappsec.org/
17		他システム・アプリケーションとの連携	外部プログラムの実行によるぜい弱性を対策する	外部プログラムを不正に実行させると、Webサイトからの情報漏えい、改ざん等のおそれがある。	・Webサーバのユーザ権限を使用する。 ・外部から入力されたデータをチェックしない。	・Webサーバの利用者は既定のユーザを使用する。 ・外部から入力されたデータに、外部プログラムが埋め込まれていないかチェックし排除する。	・Webサーバが実行可能なOSコマンドを制限する。 ・外部から入力されたデータに、外部プログラムが埋め込まれていた場合、ログに履歴を残す。	・基本的にWeb上からOSのコマンドは実行しない。どうしても実行しなければならない場合は、外部から入力されたデータに依存しない方法をとる。 ・WAFを導入する。 ・攻撃を検出して、管理者に通知する。			A.12.2.1	Web Application Security Consortium http://www.webappsec.org/

Webアプリケーション セキュリティ・可用性チェックシート（詳細項目版）

	要素	分類	対策項目	リスクの詳細	推奨レベル レベル1	レベル2	レベル3	レベル4	本件業務のセキュリティ仕様 該当レベル	対策仕様	JISQ項番	参考文献（JIS Q 27002：2006以外）
18			SSI インジェクションを対策する	SSI インジェクション(Server-side Include)を使用されると、パスワードの抜き取りやフィッシング詐欺サイトへの誘導のおそれがある。	・外部から入力されたデータをそのまま使用してSSI箇所を処理する。	・外部から入力（入力フォーム、URLパラメータ、Cookie、ヘッダパラメータ等による入力）されたデータを使用してコードを生成する際は、SSI インジェクション対策を実装する。	---> 前レベルと同様	・SSIは使用しない。			A.10.4.1 A.12.2.1	Web Application Security Consortium http://www.webappsec.org/
19			不正スクリプトの実行を防止する	不正なスクリプトが実行されると、Webサイトからの情報漏えい、改ざん等のおそれがある。	・利用者からアップロードされたファイルの内容を検証しない。	・利用者からアップロードされたスクリプトを実行させない。	・アップロード可能な拡張子を制限する。	・アップロードされたファイルをバイナリレベルで評価し、不正なデータを排除する。			A.10.4.1 A.12.2.1	Web Application Security Consortium http://www.webappsec.org/
20		Webサーバの設定	ディレクトリのファイル一覧表示を防止する	ディレクトリのファイル一覧表示がむやみに許可されていると、攻撃者にWebサイト攻撃のための情報を提供することになるおそれがある。また、セキュリティモラルの低いWebサイトとみなされ、攻撃対象にされるおそれがある。（ディレクトリ・リスティングと同じ[*]）	・ディレクトリ内のファイル一覧表示を許可する。	・ディレクトリ内のファイル一覧表示を許可しない。	・プログラムやHTMLファイルを配置しないディレクトリには、index.html等の名称で、空のファイルを配置する。	---> 前レベルと同様			A.10.7.3 A.12.4	Web Application Security Consortium http://www.webappsec.org/
21			パスの乗り換えを防止する	パスの乗り換えを使用されると、第三者への情報漏えいのおそれがある。	・ドキュメントルートの外に存在するファイルを表示する。	・URLに「..」等の不正な文字列を入力しても削除や置換を行い、不正なパスの切り替えを実施させない。	・既定以上のディレクトリ階層のファイルへのアクセスをアプリケーションの設定で禁止する。	---> 前レベルと同様			A.12.4	Web Application Security Consortium http://www.webappsec.org/
22			Webサーバ上のアプリケーションが特定されるのを防止する	Webサーバ上のアプリケーションが特定されると、種類やバージョン情報から有効な攻撃方法が特定されるおそれがある。	・Webサーバの種類、バージョンを公開する。	---> 前レベルと同様	・Webサーバの種類、バージョンを公開しない。	---> 前レベルと同様			A.10.7.3	Web Application Security Consortium http://www.webappsec.org/
23		アプリケーションのディレクトリ構成	リソースの位置を推測不可能にする	リソースが推測可能になっていると、第三者への情報漏えいのおそれがある。	・推測しやすい名称のファイルやフォルダをドキュメントルート直下に配置する。	・ドキュメントルート直下にAdminのような推測しやすい名称で、管理者用ページを含んだフォルダを配置しない。 ・管理者用ページのパスのように、重要なファイルのパスを含んだ robots.txt を置かない。	・ドキュメントルート直下に、推測しやすい名称のファイルやフォルダを配置しない。 ・robots.txt は配置しない。 ・コンテンツのバックアップとして、.bakや.oldの拡張子でファイルを保存しない。	・ハッカーがよく狙う推測可能なリソース（例：robots.txt)を配置し、アクセスログをとる。				Web Application Security Consortium http://www.webappsec.org/
24		バックアップファイルの取扱い	バックアップファイル等、サーバ上のデータの情報漏えいを防止する	サーバ上のデータが情報漏えいすると、そのシステムを悪用する足掛かりを攻撃者に提供するおそれがある。（「強制ブラウジング」を含む）	・サーバ内にファイルを自由に配置する。	・データベースのダンプファイルやコンテンツのバックアップなど、Webサイトの解析を行う足がかりとなる情報や、個人情報などの重要な情報は、ドキュメントルート下に置かない。	・重要か否かに拘らず、コンテンツ表示に使用しないファイルは一切置かない。 ・コンテンツで参照するデータファイルも外部から直接リンクを張る必要が無い場合は、ドキュメントルート以外に置いて外部から参照させない。	・重要な情報は、一度に多数の情報が閲覧できる一覧表示やCSVファイル出力などは行わない。			A.10.7.3	
25		アプリケーションの欠陥	アプリケーション機能の悪用を防止する	アプリケーション機能が悪用されると、第三者への情報漏えい、改ざん、迷惑メールの踏み台等のおそれがある。	・機能を自由に使用できる。	・Webサイト内検索機能を利用しても、公開を意図しないファイルにはアクセスさせない。 ・ファイルをアップロードする機能を利用しても、内部のファイルを置き換えさせない。 ・Webサイト上のメールの入力フォームを利用しても、迷惑メールを送らせない。	---> 前レベルと同様	・アップロードされたファイルはディレクトリ上に保管せず、所定の検証手続きを済ませた上でデータベース上に保管する。			A.12.2.2	Web Application Security Consortium http://www.webappsec.org/
26			瞬間的なアクセス過多などによるサービス提供不能を防止する	サービス拒否(DoS/DDoS)を実行されると、Web サーバが利用者へ提供するサービスを妨害されるおそれがある。	・全てのリクエストを受け付ける。	想定しうる連続したリクエストを受信した場合でも、耐えることができることを確認する。	・DoS対策機能を持ったファイアウォール、ルータ等の導入もしくは、DoS対策専用機器を導入して対策を講じる。 ・アプライアンスの導入が困難な場合は、OSレベルまたはWebサーバの拡張機能を使用して対策を講じる。	・DoS/DDoS攻撃対策を専門業者に委託し導入する。			A.12.2.2	Web Application Security Consortium http://www.webappsec.org/
27			自動反復プログラムによる不正行為を防止する	利用者の作業を自動化するプログラムによる入力を制御する仕組みを用意しないと、不当に大量の会員登録を行われる等のおそれがある。	・登録フォームに必要情報を入力後、確認画面を表示した後に登録を完了させる。	・登録時は、直接登録完了を行わず、登録したメールアドレスに登録完了画面のURLを送信し、登録を完了させる。	---> 前レベルと同様	・入力フォームにはCaptchaを使用する。			A.12.2.2	Web Application Security Consortium http://www.webappsec.org/
28			プロセスを検証する	プロセス検証が不適切だと、第三者が利用者（会員等）に成りすます等のおそれがある。	・プロセスを確認しない。	・複数の画面を、決められた順番に進めていくプロセスにおいて、順番通りのステップを経てプロセスを進めているかを確認する。	---> 前レベルと同様	---> 前レベルと同様			A.12.2.2	Web Application Security Consortium http://www.webappsec.org/
29		ネットワーク構成	データベースサーバへの攻撃を防止する	データベース（DB）サーバが攻撃されると、DBサーバからの情報漏えい、改ざん等のおそれがある。	・WebサーバとDBサーバを同一サーバに置く。 ・Webアプリケーションからの DBサーバへのアクセスを制限しない。	・WebサーバとDBサーバを同一サーバに置く。 ・Webアプリケーションからの DBサーバへのアクセス権は一般ユーザ権限とする。（管理者権限にしない）	・DBサーバとWebサーバを物理的に別々のサーバに配置する。 ・Webアプリケーションからの DBサーバへのアクセス権は一般ユーザ権限とする。（管理者権限にしない） ・DBサーバはWebサーバ以外からのアクセスが不可能な、ローカルエリア上に配置する。	・機密情報は、DBへの登録内容を全て暗号化し、参照する利用者に応じて復号化して提供する。 ・DBに対して送られたSQL文は全てログとして収集し、DBサーバとは別サーバに保存する。			A.11.4.6	
30			Webサーバの配置場所を検討する	Webサーバが攻撃を受けると、Webサーバの改ざん等のおそれがある。	・Webサーバをそのままインターネット上に公開する。	・Webサーバはファイアウォールを経由して公開する。	・Webサーバは、リバースプロキシや不可分散装置等の一次アクセス受付サーバと、アプリケーション実行用サーバに分割する。 ・一次アクセス受付サーバのみ、外部ネットワークからのリクエストを受け付ける。	・WebサーバはWAFを経由して公開する。			A.11.4.6	
31		情報の交換	業務用情報システムへの不正なアクセスを防止する	業務用情報システムへ不正にアクセスされると、情報の改ざんや漏えいなどのおそれがある。	・認証に関するルールを定めない。	・認証の再試行可能回数を定める。 ・再試行可能回数を超えて認証が失敗した場合は、二十四時間当該アカウントを停止する。 ・認証情報はセッションまたはCookieに保存する。 ・ログインID/パスワード等の認証情報をCookie上に暗号化せずに保存する。	・認証画面(機能)を使用して、コンピュータとアプリケーションを利用する。 ・一定回数以上ログオンに失敗したアカウントは、ロックアウトする。 ・パスワードの定期的な変更を、システム機能により強制する。 ・パスワードを他人から推測されにくいものにすることを、システム機能により強制する。 ・パスワードをシステム内に保存する場合は、暗号化する。 ・パスワードをコンピュータ間で通信する場合は、暗号化する。	・認証のログを採取する。 ・ログインID/パスワードはセッション上に保存せず、利用者をシステム側で管理する一意な文字列をセッションに保存する。			A.10.8.5	
32		電子商取引サービス	取引内容を第三者から保護し、当事者間だけの情報とすることを規定する	コンピュータ間でやりとりされる情報を保護しないと、取引の内容が漏えい、改ざんされるおそれがある。	・データを暗号化しない。	・取引情報を入力する画面はSSLによって暗号化し、入力した取引情報もSSLによって暗号化する。 ・SSL認証は、電子証明書を使ったサーバ認証を行い、利用者はID/パスワードを使用して認証する。 ・取引結果についてはメールにて双方に通知する。	・取引情報を入力する画面データはSSLによって暗号化し、入力した取引情報もSSLによって暗号化する。 ・SSL認証は電子証明書を使ったサーバ認証を行い、利用者はID/パスワードを使用して認証する。 ・取引結果についてはメールにて双方に通知のみを行い、閲覧用のURLから取引結果を確認する。	・利用者のSSL認証はID/パスワードだけではなく、電子証明書を使用して個人認証する。 ・高額取引や原本性を重んじる商取引では、電子署名を使用して電子商取引の内容を保証する。			A.10.9.1	
33			オンラインで取引する	コンピュータ間でやりとりされる情報を保護しないと、取引の内容が漏えい、改ざんされるおそれがある。	・データを暗号化しない。	・取引情報を入力する画面はSSLによって暗号化し、入力した取引情報もSSLによって暗号化する。 ・SSL認証は、電子証明書を使ったサーバ認証を行い、利用者はID/パスワードを使用して認証する。 ・取引結果についてはメールにて双方に通知する。	・取引情報を入力する画面データはSSLによって暗号化し、入力した取引情報もSSLによって暗号化する。 ・SSL認証は電子証明書を使ったサーバ認証を行い、利用者はID/パスワードを使用して認証する。 ・取引結果についてはメールにて双方に通知のみを行い、閲覧用のURLから取引結果を確認する。	・利用者のSSL認証はID/パスワードだけではなく、電子証明書を使用して個人認証する。 ・高額取引や原本性を重んじる商取引では、電子署名を使用して電子商取引の内容を保証する。			A.10.9.2	
34			公開されている情報の改ざんを防止する	価格や情報等、Webサイト上に掲載される情報が改ざんされ、不正に利用される可能性がある。	・情報を確認しない。	・公開前の情報について、内容に誤りがないかを目視で確認する。	・公開された情報に誤りがないことを目視で確認する。	・改ざんを検出するシステムを使用し、情報の改ざんを監視する。 ・改ざんを検出した場合は管理者に連絡する。 ・情報の更新ログを取得する。			A.10.9.3	

Webアプリケーション セキュリティ・可用性チェックシート（詳細項目版）

	要素	分類	対策項目	リスクの詳細	推奨レベル レベル1	レベル2	レベル3	レベル4	本件業務のセキュリティ仕様 該当レベル	対策仕様	JISQ項番	参考文献（JIS Q 27002：2006以外）
35		ログの収集と解析	監査ログを取得する	情報システムの適切な監査ログを記録しないと、発生した不正な活動に気づく事ができないおそれがある。	・ログを取得しない。	・情報システムのアクセスログを取得する。 ・アクセスログを、定期的に点検する。 ・アカウントによるログオンイベント（ローカル）を記録する。(成功) ・アカウントへの変更(管理作業)を記録する。(成功) ・アカウントまたはパスワードのポリシー変更を記録する。(成功) ・システムに影響のあるイベントを記録する。(成功)	・アカウントによるログオンイベント（ネットワーク、ドメイン、ローカル）を記録する。(成功)	・アカウントによるログオンイベント（ネットワーク、ドメイン、ローカル）を記録する。(成功/失敗) ・アカウントへの管理作業を記録する。(成功/失敗) ・アカウントまたはパスワードのポリシー変更を記録する。(成功/失敗) ・システムに影響のあるイベントを記録する。(成功) ・オブジェクト(ファイル等)へのアクセスを記録する 。(失敗) ・特権の使用を記録する。(失敗)			A.10.10.1	
36			ログ情報を保護する	取得したログ情報を保護しないと、内容の改ざんやログが破棄されるおそれがある。	・ログを取得しない。	・情報システムのログのバックアップを、 オフラインで定期的に取得する。 ・情報システムのログにアクセス可能なアカウントを制限する。 ・ログの記録漏れ、上書き等が発生しないよう、十分な記憶容量を確保する ・ログの削除が行われた事をログに記録する。	・オペレーティングシステムまたは、アプリケーションの機能により、適切なログの保護措置をとる。 ・ディスク等の容量不足などにより、ログが記録できない場合は、システムを停止する。 ・ログのオフラインでのバックアップは、十分な期間に遡って参照可能にする。	・ログを短いサイクルで、別の情報システムにオンラインでコピーまたは移動する。			A.10.10.3	
37			障害のログを取得する	障害ログを取得しないと、発生した事象に関して原因究明が困難になるおそれがある。	・ログを取得しない。	・情報システムの障害発生を記録する。	・記録された障害毎に、明確な対応策または運用規則を定める。 ・対応策が決められていない場合の、運用規則を定め	・情報システムで障害が発生した場合は、システム管理者に通知する。			A.10.10.5	
38		Webアプリケーション開発	プログラムに関するコーディング規約を定義する	開発者間で共通したプログラミングに関するコーディング規約がないと、品質と保守性に問題があるシステムになるおそれがある。	・コーディング規約を設けない。 ・単独の担当者でシステムを開発する。	・コーディング規約を定めるが文書化しない。	・コーディング規約を正式に規定し、文書化する。 ・コーディング規約を担当者に周知する。	・プログラムがコーディング規約に準拠しているかを専用のツールを使用してチェックする。				
39			プログラムを作るにあたって守らなければならないセキュリティ方針を策定する	セキュリティ指針を策定していないと、属人的なセキュリティ意識に基づいたプログラミングを行うことになるため、品質とセキュリティ性に問題があるシステムになるおそれがある。	・セキュリティ指針を策定しない。	・セキュリティ指針を策定し、教育を実施する。 ・セキュリティ指針を定期的に見直す。	・社外の作業者に対して、社内と同様の教育を実施する。	・セキュリティ教育の浸透状況を監査する。				
40			プログラム作成後、セキュリティの問題点が無いことをチェックする	セキュリティテストを実施していないと、セキュリティ指針が周知徹底されていた場合でもぜい弱性を含んだシステムになるおそれがある。	・セキュリティテストを実施しない。	・開発者本人による属人的なセキュリティテストを実施する。	・セキュリティテストについての明確な枠組みを作り、テストプロセスに組み込む。	・セキュリティテストは、開発者ではなくテスト専門の担当者が実施する。				
41	情報が事実と等しい（完全性保証）	原本性保証	データがネットワーク上で改ざんされていないことを保障する	データが完全性を保証できないと、メッセージなどの情報が改ざんされて業務を混乱させるおそれがある。	・送信、受信されたデータの整合性を確認しない。	・SSL認証を行い、メッセージを暗号化することで、メッセージの完全性を保証する。 ・SSL認証は電子証明書を使ったサーバ認証を実施し、利用者側はID/パスワードを使用した認証を実施する。	・クライアント側のSSL認証は、ID/パスワードだけではなく、電子証明書を使用した個人認証を実施する。	・電子署名を使用して、送受信メッセージの完全性を保証する。 ・金融、証券など、署名の日時に重要性がある場合は、タイムスタンプつきの電子署名を利用する。			A.12.2.3	
42		監査	情報システムを監査する	情報システムを定期的に監査しないと、不正の検出ができなく、情報漏えいを見逃すおそれがある。	・内部監査を実施しない。	・定期的な個人による監査を実施する。	・監視計画と監視実績に基づいた、監査を実施する。 ・監査については、定期的に社内組織に委託する。	・監視計画と監視実績に基づいた、監査を実施する。 ・監査については、定期的に第三者組織に委託する。			A.15.3	
43	システムを稼働し続ける（可用性保証）	冗長化	サーバを冗長化構成にする	サーバが障害などで停止してしまうと、利用者に提供しているサービスが停止してしまうおそれがある。	・サーバの障害時に、サーバが復旧するまでサービスが停止する。	・Webサーバ及びDBサーバを二重化する。 ・サーバの障害時に、サービスが数十分～数時間の停止後、復旧できるようなシステム構造にする。	・Webサーバ及びDBサーバを二重化する。 ・サーバの障害時に、サービスが数分～数十分の停止後、復旧できるようなシステム構造にする。	・Webサーバ及びDBサーバを二重化する。 ・一部のサーバに障害が発生しても、サービスは停止しないシステム構造とする。				
44			ネットワーク経路を冗長化構成にする	サーバまでのネットワーク経路が遮断されると、利用者に提供しているサービスが停止してしまうおそれがある。	・ネットワーク障害時に、ネットワークが復旧するまでサービスが停止する。	・ネットワーク経路を二重化する。 ・ネットワーク障害時に、サービスが数十分～数時間の停止後、復旧できるようなシステム構造とする。	・ネットワーク経路を二重化する。 ・ネットワーク障害時に、サービスが数分～数十分の停止後、復旧できるようなシステム構造とする。	・ネットワーク経路を二重化する。 ・一部のネットワークに障害が発生しても、サービスは停止しないシステム構造とする。			A.10.6	
45			データを冗長化構成にする	サーバのデータが消失すると、利用者に提供しているサービスが停止するおそれがある。	・データクラッシュ時に、データを復旧するまでサービスが停止する。	・データを二重化する。 ・データクラッシュ時に、サービスが数十分～数時間の停止後、復旧できるようなシステム構造とする。	・データを二重化する。 ・データクラッシュ時に、サービスが数分～数十分の停止後、復旧できるようなシステム構造とする。	・データを二重化する。 ・一部のデータがクラッシュしても、サービスは停止しないようなシステム構造となする。				
46		負荷分散装置の設置	サーバ負荷の設計と分散方式を検討する	サーバが過負荷になると、アプリケーションの停止や、ぜい弱性を原因とする情報漏えいのおそれがある。	・負荷を考慮しない。	・データを二重化する。	・サーバや負荷分散装置を二重化し、耐障害性を高める。	・負荷分散対象サーバを仮想化やクラスタ化し、より大規模な負荷を想定した構成とする。				
47		容量管理・拡張性	サーバの容量や能力を管理する	情報システムの能力が不足すると、情報システムが利用できなくなるおそれがある。	・情報システムの容量監視をしない。	・ディスク容量や処理能力等について、利用者やデータの伸びに対し、一定期間対応可能な情報システムにする。	・情報システムの拡張が、容易なシステムにする。	・情報システムの稼働能力を監視する。 ・情報システムの容量の増強を計画的に実施する。 ・情報システムの容量の増強が容易なシステムにする。			A.10.3.1	
48		保守運用	アプリケーションを保守する	アプリケーションの不具合やぜい弱性を放置しておくと、情報漏えいが発生するおそれがある。	・アプリケーションを保守しない。	・アプリケーションに関する保守や監視を、他業務を兼務する従業員が実施する。	・アプリケーションの保守は専任の情報システム担当者が行う。 ・アプリケーションの監視（特に死活監視）を実施する。 ・アプリケーションに関する不具合やぜい弱性の情報を管理し、計画的に対策する。	・保守作業は事前に保守計画を明らかにし、保守計画に沿った作業のみを実施する。 ・事前に申請のない保守作業は一切禁止する。 ・保守作業の内容は履歴に残す。 ・作業内容の履歴は、管理者であっても変更や削除が不可能な方法で保存する。 ・緊急時の対応について事前に手順を明らかにし、操作手順に沿って作業を実施し、作業履歴は漏れなく保存する。				
49			アプリケーションを更新する	アプリケーションの更新を計画的に実施しないと、ぜい弱性が混入するおそれがある。	・アプリケーションの更新は、動作検証しない。	・アプリケーションの更新は、擬似環境上で問題がないことを確認した上で実施する。	・更新箇所の履歴を管理する。 ・更新にはメンテナンス期間を設け、更新による不具合が本番環境で発生しないことを確認する。	・本番環境上で、メンテナンス期間中に退行テストもあわせて実施する。				
50			アプリケーションのバージョンを管理する	アプリケーションに不具合が発覚した際に、問題の無いバージョンに速やかに退行することが出来ないと、改修が完了するまでの間、アプリケーションの停止またはぜい弱性を抱えたままの運用をしなくてはならないおそれがある	・アプリケーションのバージョンを管理しない。	・アプリケーションのバージョン管理は、旧バージョンのバックアップファイルを残すことでバージョン管理とする。	・アプリケーションのバージョン管理は、バージョン管理ソフトウェアもしくは台帳を使用して管理する。	・アプリケーションの更新を行う際は、関連するプログラム一式を書庫ファイルに整理し、不具合発生時には関連するプログラム一式を速やかに退行できるようにする。				

「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」

＜システム取引におけるトラブル事例＞

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）

契約トラブル事例１

1	ユーザの概要	（①業種　②年商　③従業員数　④システム部門・担当者の有無等） ①調査会社､探偵会社 ②190 百万円前後 ③25 名前後 ④本システム導入に伴い「ＰＣ部」設置
2	開発案件の概要	案件名／概要：新基幹システム（顧客情報、調査情報等の管理、検索システム） 契約金額：約 16 百万円 期間：当初予定　H12.2.15～H13.1.末日 ７回の納期延期により最終はH15.1.末日
3	契約における経緯､ユーザの要求度合い、特徴	・旧システムを同ベンダが作成した実績から、新システムを受注。 ・旧システム開発時も著作権の帰属に関しユーザと一紛争あり。 ・経営者はワンマン。
4	開発プロジェクトの概要	開発体制（ユーザ側・ベンダ側のスキル・人数等)、再委託状況、スキル面など ベンダ側：旧システムの開発を担当したＳＥが当初のメインＳＥ。システム確認書検収後、異動によりメインＳＥは交代。トラブル頻発後は開発体制を強化(本社管理、投入人員増化)して対応。 一部再委託を行っているが、当社ＳＥが中心となって開発。 ユーザ側：ＰＣ部社員（3 名～4 名)。
5	トラブルの内容と対処	H13.5.末日に納品を行ったが、バグが多く、かつ、要求機能を実現していないので使用に耐えないとのユーザ指摘で検収に至らず。その後も納期の再設定を繰り返し、開発体制を強化し完成を目指すも、構築フェーズの検収には至らず。 ユーザが同ベンダ宛、契約解除、損害賠償を求めて訴訟提起。 ユーザ側の主張が裁判所により概ね認められた。
6	契約書条文とトラブルとの考察	ユーザは新システム導入による賃借スペース拡大費用、人員の増加費用等拡大損害分を含む賠償（約 28 百万円)を求めたが、裁判所は、契約金額を賠償の上限とする契約条項を斟酌し、契約金額相当額での和解案を提示した。同案にて和解が成立。
7	契約書サンプル	□添付する　　㋡添付なし
8	その他	ベンダ側の裁判時の主張要旨： 要件定義検収後になって、ユーザから要求変更・新規要求が相次いだために、当初納期を何度も延期せざるを得なくなり、かつ、システムの整合性も図りづらくなってシステムの完成度が大幅にダウンした。事態は、ユーザの帰責性によるものである。 ユーザ側の裁判時の主張要旨： ベンダによるユーザ業務内容の理解不足が原因で、何度も納期が延期され、かつ、納品されても不完全なものであったため、検収印を押さなかった。業務内容の理解不足については、ベンダも自認している。従って、納期延期の点もシステムの不完全性の点も、ベンダが責めを負うべきである。

契約トラブル事例２

多段契約ではあるが相対取引ではなく、ユーザ側の契約主体が超上流フェーズ（企画）および上流フェーズ（要件定義）と下流フェーズ（開発・運用）が異なり、各フェーズにおける契約が有効に機能せず、曖昧部分の大半をベンダ（当協会メンバ）が対応することで、収束せざるを得なかったケースをご紹介します。

1	ユーザの概要	大企業グループにおける契約
2	開発案件の概要	Windows Client＆Server　販売会社向けシステム 契約金額：非公開　/　開発・展開期間：２．５年
3	開発プロジェクトの概要	超上流：大企業　情報システム部門　⇒　ベンダ選択 ↕　業務委託契約 上流　：大企業グループＳＩer　⇒　開発・サポート基本契約 ↕　導入支援契約 下流　：大企業グループ販社　⇒　個別契約
4	トラブル発生までの経緯	①　大企業情報システム部門より、ＲＦＩ・ＲＦＰが提示され、複数ベンダのコペにて、ベンダとして選択されるも、大企業とは直接契約はおこなわれず、グループＳＩerにＰＪ統括を委託しており、グループＳＩerとの契約を指示される。 ②　グループＳＩerと開発・サポートに関する基本契約を締結し、開発またはサポートに関する基本スキームは設定されるがＳＩer の役割は導入支援であり、個々のグループ内販売会社とベンダとは個別契約を締結し、ＰＪを推進するスキームである事が明確となる。 ③　展開段階に入ると個別販社より様々な要求が発生するが、個別契約による個別対応を要求され、基本スキームによる厳しい要求品質と個々は中小企業であることから品質に対するコスト理解が得られず、厳しいＰＪとなる。
5	契約書条文とトラブルとの考察	ユーザ企業グループ間における役割は、相互の契約書で明確に定義されており、しかしながら、各企業とベンダとは四社間契約等の締結は実質困難であり、大企業との契約行為は実質商権に関する履行義務契約となっており、商談としての相対契約はあくまで販売会社との個別契約となっている。 ⇒大企業グループにおける関係会社の情報システム構築はこのケースに近い契約形態が取られており、信頼性を向上させるためには、関係する会社間での相応の責任と役割を定める標準契約の必要性を感じる。

契約トラブル事例３

1	ユーザの概要	（業種・年商・従業員数、システム部門・担当者の有無等） 出版関係のシステム子会社 年商　１００億円　従業員　１５０名 システム部門あり、
2	開発案件の概要	案件名（業務）：　販売管理パッケージ再構築 契約金額（概算）：　当初契約　１．５億円 期間：　　当初１１ヶ月 開発内容環境 言語：.NET　OS：Windows2003　開発人月：契約時１４０人月 要件定義後　２６０人月
3	契約における経緯、ユーザの要求度合い、特徴	・業界における不特定多数向けのパッケージ開発である。 ・現行の古いパッケージの機能は基本的に踏襲する。
4	開発プロジェクトの概要	開発体制（ユーザ側・ベンダ側）、再委託状況、スキル面など ベンダー側　：　弊社（ＰＭ，ＳＥ２名）協力会社のＳＥ２名 ユーザー側　：　システム担当部長以下５名
5	トラブルの内容と対処	要件定義により、開発ボリュームが２倍に増加。 見積提案は、要件定義終了後に詳細見積りとなっていたが、追加費用の提示に対して納得されず金額増加とスケジュールの見直しが認められなかった。
		トラブルをどのように収束させたか 見積時との差異と根拠を詳細に洗い出し金額増加の根拠を提示したが、合意にいたらず、外部設計までの開発を行い以降は、受注取り消しということで合意した。要件定義工数が膨らんだ部分は赤字となった。
6	契約書条文とトラブルとの考察	当初の受注は要件定義からｻｰﾋﾞｽｲﾝまでの全工程を受注しており、要件定義のみ受注後し次工程を受注するという分割受注とすべきであった。 但し、全体費用が見えない状況での発注がされたか疑問である。
7	契約書サンプル	□添付する　　■添付なし
8	その他	（特記事項があればご記入下さい） 提示された RFP を元に見積し請負受注をしたが、打合せを行う中で実際の深さがあることが判明し、現行システムを調査させていただいた結果、業界特有の RFP では推し量れない部分が存在しており開発ボリュームを増大させた事が判った。１ヵ月後に気付いた時点では契約もしており手遅れであった。 受注破棄も考えたが、他の取引もあり困難であった。

契約トラブル事例４

1	ユーザの概要	（業種・年商・従業員数、システム部門・担当者の有無等） 文部科学省関連の社団法人　事業費　６００億円 職員　１５０名 システム部門なし
2	開発案件の概要	案件名（業務）：　流通情報システム 現行 UNIX 機のシステムの老朽化と後継機が無い為、ハード、ソフトを全面的に更新する。構築には最新技術を使いたい。 契約金額（概算）：　　３億円 期間：　　３年間 開発言語：VB.NET　OS：Windows2000、AIX（UNIX）
3	契約における経緯、ユーザの要求度合い、特徴	ＲＦＰをもとに見積算出、入札により契約。
4	開発プロジェクトの概要	開発体制（ユーザ側・ベンダ側）、再委託状況、スキル面など ベンダー側　：　ＰＭ以下ＳＥ，ＰＧＭピーク時は４０名 ユーザー側　：　サブシステム担当者１０名
5	トラブルの内容と対処	ＲＦＰには機能の詳細が記述されていなかったため、一般的な開発ボリュームを想定して工数を算出した。要件定義の段階で複雑な画面やロジックであることが判明したが、入札によりプロジェクト全体を契約していたため追加費用が認められなかった。
		トラブルをどのように収束させたかなど 新機能については追加費用が認められたが、当初の部分についてはコストオーバー分（２億円）が赤字となった。
6	契約書条文とトラブルとの考察	契約書に想定ＳＴＥＰ数等を記載してオーバー分に関しては追加費用となることを明記すべきだった。 遅延損害金が契約条項にあった為、機能定義書の中に未決事項があるにもかかわらず外部設計に入り手戻りが発生した。
7	契約書サンプル	□添付する　　■添付なし
8	その他	当時の PM からトラブルの反省点を聴取し要約したものです。 **見積りと入札** （要求仕様書について） 弊社が○○○○プロジェクトのメンバーを決めたのは、2002 年 9 月からであり、その時担当の PM が○○○○プロジェクトの要求仕様書に対して感じたことを記させていただきます。 1 冊の要求仕様（RFP）に対する入札の結果として弊社が SI 開発を 2 億円弱で落札しているが、要求仕様書を見た感想としては、かなりのページ数があり、きれいにまとまっている印象を受けました。しかし、読んでみても内容がよく

		分からない。当然、書き手は業務や現行システムのことをよく知って書いているのだろうが､その前提がなく初めて読む者にとっては理解し難いものがあり、また、都合よくとれるように予防線を張ったような文章が目立ちました。 その要求仕様書の記述から、機能としてカウントできると思われるところを抜き出して当時の弊社のｿﾘｭｰｼｮﾝ提案部門で見積りを行っていますが､その時点では見積りの妥当性をどこまで正しく判断できたのか疑問が残ります。 （見積りについて） 　入札においては、２００２／７月～約１ヵ月の期間で質疑応答を交わし、提案書を作成しました。しかし、振返ってみるとあの要求仕様書のボリューム・記述内容からすると、相当な質問をして理解しないと見積りは出せないと思いました。 ハードソフトの総合提案であり、短期間でシステム開発の最終工程まで見積もるのは難しく、見積もるだけでも２～３ヶ月のプロジェクトで取り組まないと見積りを作れないくらいであったと反省しています。 実際に精度の高い見積もりを出すためには、弊社で自ら要件定義を実施し、要件定義完了後に見積することが必要でしたが、入札とのことで○○○○様からの要求仕様書及びシステム担当の方への質疑応答により見積もりを行なった結果、誤った見積りを出してしまったということになります。 頂いた要求仕様書で正しい見積りを出せるのは、現行システムに携わり、○○○○様の内部事情に精通し、要求仕様書まで作成した開発会社しかいないと思いました。 要求仕様書を作成した開発会社の提案がどのような内容で、どのくらいで見積もったのかは知りませんが、入札のときに一番理解されているこの開発会社の見積金額を基準にし、基準とあまりにもかけ離れている見積りを出してきた企業は、入札した時点で対象外とするべきではないかと思います。結果的○○○○様と弊社で長期に渡り交渉を重ねた膨大な時間は無駄というしかありません。

契約トラブル事例５

１	ユーザの概要	（業種・年商・従業員数、システム部門・担当者の有無等） 旅行関係 年商　３００億円 システム部門あり
２	開発案件の概要	案件名（業務）：　　Ｗｅｂ予約システム 契約金額（概算）：　　２億円 期間：　　１８ヶ月 開発言語：JAVA　OS：LINUX
３	契約における経緯､ユーザの要求度合い、特徴	現状機能をもとに追加機能を加味して見積提出。納期に対して要求が厳しかったため、一部機能を１次開発とし残りを２次開発とすることで合意し契約。
４	開発プロジェクトの概要	開発体制（ユーザ側・ベンダ側)、再委託状況、スキル面など ベンダー側　：　弊社ＰＭ１名。協力会社ＳＥ３名。 ユーザー側　：　プロジェクトメンバー５名
５	トラブルの内容と対処	当初スケジュールの関係から１次開発と２次開発は一部並行して開発を行う予定であったが、２次の要件定義の途中で１次開発に専念するために２次開発を中断した。１次完了後、２次の要件定義を再開する時点で協力会社から費用の追加を求められた。ユーザーと弊社は請負契約であったが、弊社と協力会社間は要件定義の部分は支援契約（口頭では請負と同様に契約した金額で作業を完了させる約束）のため金額の折り合いがつかず、しかも途中までの費用を請求されている。
		トラブルをどのように収束させたかなど 議事録やメモを元に協力会社と交渉中。プロジェクトについては弊社のＳＥで要件定義をやり直したが、スケジュール遅れのためユーザーからもペナルティーを要求されている。
６	契約書条文とトラブルとの考察	協力会社の社内規定により要件定義は請負契約が出来ないことを承知しながら口頭での約束を信じて協力会社に発注したことが主な原因です。
７	契約書サンプル	□添付する　　■添付なし

契約トラブル事例６

1	ユーザの概要	業種：石油類販売業／輸送事業（複数の子会社を有する企業グループ。システム部門はあるが専門家はいない）
2	開発案件の概要	案件名／概要：共通営業系システム（販売管理・仕入管理パッケージソフトウェアをベースにアドオン開発を実施） 契約金額（概算）：6,000 万円（パッケージ＋アドオン開発） 期間：1 年間　　開発言語：VB.NET ※ユーザの主要取引先の情報システム子会社（A 社）からの発注により案件を受託
3	契約における経緯、ユーザの要求度合い、特徴	ユーザと A 社を中心として RFP を作成。奉行シリーズの導入（パッケージ＋アドオン開発）を企業グループ内の他の企業にも実施していたことから弊社に協力要請があり、弊社パッケージにこだわらないことを前提に RFP 作成に参画。 弊社では、今回の案件については対応が難しいと感じており辞退することを A 社に申し出ていたが、A 社の強い要請により弊社から提案書を提出。Q&A を経て、約 1 ヶ月後に弊社の提案が選出されたとの通知あり。
4	開発プロジェクトの概要	ユーザ側　：　現業部門担当者　2 名、システム部門担当者：1 名 A 社　　：　サブシステム開発を担当（5 名） 弊社側　　：　パッケージ＋アドオン開発を担当。 ピーク時は 20 名（ＰＬ、ＳＥ、ＰＧ）
5	トラブルの内容と対処	本プロジェクトスタート時の全体スケジュール計画と比較して、RFP 提示までのスケジュールが半年ほど遅延しており、機能・詳細仕様面の検討事項が残っているにも係らず、大幅なスケジュール短縮を要求された。開発作業に移行する段階で仕様検討が不十分だったものについては、ユーザ側もしくは A 社側の負担で改修することになっていたが、不具合と認定され弊社での対応を要求されるものも多かった。 開発作業時における仕様変更による追加費用については、各フェーズでユーザの承認を得てきていたが、本番稼動前の仕様変更ボリュームが多いことから、スケジュールの遅延と併せて責任を問われ、現在折衝中。
6	契約書条文とトラブルとの考察	弊社は A 社との契約になるが、A 社の強い要求による受託であったために遅延損害金及び中途解約については適応外の見積書を提出し了承を得ていたが、契約書の締結には至らず（短縮された納期に間に合わせるために開発に着手済）。
7	契約書サンプル	□添付する　　■添付なし
8	その他	上流工程の段階から各社の役割を明確にする必要があるが、その取り決めが機能しなかった場合に開発側（ベンダ・請負先）にしわ寄せがこない取り組みが必要。そのためにも、契約書への明記だけではなく、打合せた内容についてはステークホルダー間で情報共有するためにも、確実に議事録その他で記録を保存しておくことが必要。

契約トラブル事例７

契約書に直接関連する案件トラブルというよりも販売店様との間で締結の打診を行っている段階でのトラブルがありますので、そちらを含めて紹介させていただきます。
販売店数や SIer が限られる地域では先方要望を呑まざるを得ない場合もあるのが現状です。

【例１】範囲が曖昧な部分について予想以上に要求される場合
エンドユーザーとのカスタマイズ請負契約
瑕疵担保期間を記載しているが、「瑕疵」の範囲認識に差が発生します。 大きなカスタマイズ案件ですと開発途中段階でプロトタイプを見ていただく事もありますが、小さな機能追加の場合、ラフスケッチでのやり取りのみで確認をして納品になる場合があります。 納品後にエンドユーザー様から「画面が考えていたイメージと異なる」とのクレームをいただき、後の契約書を修正する事例が発生しました。 明確な瑕疵であれば問題無いのですが、そうとも言えない内容もありました。 【現在の対応】 請負契約書に「インターフェースイメージや仕様書に記載されていない操作性については瑕疵担保の対象外」との文言を入れて対応しています。

【例２】危険負担の範囲の交渉が平行線となる場合１
販売店（甲）・ベンダー（乙）間の納品後の危険負担
甲の主張：甲に帰すべき責の無い場合は全て乙 乙の主張：乙に帰すべき責は乙が負担 →力関係にてベンダーが呑む。

【例３】危険負担の範囲の交渉が平行線となる場合２
販売店（甲）・ベンダー（乙）間でのカスタマイズプログラムについての危険負担
甲の主張：納品後のトラブルは全て乙責任で対応 乙の主張：乙に帰すべき責は乙が負担 案件定義もベンダーが行う事が多く、販売店としては「自分は案件紹介するだけ」との認識です。 →交渉の末、「対応はベンダーが行うが、返品時の対応は甲乙協議」

【例４】第三者権利侵害について「保証できない」と言われる場合
SIer と締結する開発委託契約書
SIer の主張：第三者権利不可侵の保証はできない

→権利侵害とならない旨の調査を SIer の義務とし、SIer に帰すべき責のある場合は SIer の責任において対応とする。としました。

【例５】自社製品のみならず、全取扱製品について品質保証を求められる場合

販売店との契約での品質保証

販売店の主張：取扱製品全てについての品質保証
販売店としては、顧客に対し「全製品品質保証」を謳いたいという方針のようでした。

→当該販売店にて扱う製品は自社製品と一部の限定された製品でした。
それらの製品についてはベンダーとの間での販売代理店契約において品質についても言及していたため、「品質保証する」としました。

契約トラブル事例８

以下は、中小企業案件およびパッケージソフトサポートで、お客様とベンダーがトラブルなるケースについてメモです。他にも、トラブルが生じるケースはたくさんあると思いますが、良くある５つのケースをご紹介いたします。

１．契約の範囲と契約金額
開発・サポートの範囲のあいまいな契約になっており、お客様の要望（パッケージソフトの場合はカスタマイズの範囲）がエンドレスになり、契約金額を大幅に上回る内容になる。競合商談の結果、ユーザー主導の内容の甘い契約になっている場合にこのようなケースが生じる。

２．パッケージソフトの不具合
自社もしくは他社開発のパッケージソフトの品質に不具合が生じ、稼動スケジュールが遅れ、ユーザーにも損害が生じる。特に、パッケージの開発元にサポートやカスタマイズも外注しているケースは、第１契約者と外注先との関係にもトラブルが生じる。

３．お客様の役割とベンダーの役割
お客様の役割とベンダーの役割が契約の中で不明確な場合、お互いの常識にズレがあり、トラブルとなる。
例：ユーザーがアウトソーシングから自社導入に切り替えた場合、導入責任者や運用責任者の役割についてユーザー側に自覚がなく、それについてベンダーも商談段階でわかりやすい説明をしていない場合。

４．打ち合わせ内容についてのユーザートップに対する報告が不足するケース
トップが指名された導入担当者とベンダーが打ち合わせを進め、基本設計や詳細設計を終えた時点で、トップに報告すると、「自分の考えを開きがあり、最初からやり直し」というようなコメントが出るケース。

５．ユーザー側に権限を持った導入責任者・運用責任者が不在
トップがベンダーへの依存心が強く、社内に権限を持つ運用責任者を設置せず、担当者レベルだけの任命となり、ベンダーに指導力を依存するケース。
権限を持つ責任者が不在のため、社内への指示系統があいまいになり、作業が進まず、トラブルとなる。

以上

平成 19 年度 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 活動報告書

平成 20 年 3 月 発行

発行　社団法人コンピュータソフトウェア協会（CSAJ）
〒100-0014　東京都千代田区永田町 2-4-2 秀和溜池ビル 4 階
TEL：03-5157-0780　FAX：03-5157-0781
URL：http://www.csaj.jp/