物流情報システム納入ガイドライン

2011年4月

一般社団法人
日本物流システム機器協会
The Japan Institute of Material Handling

機種別部会
情報系委員会

分科会の構成と開催経緯

●分科会の構成(50 音順・敬称略)

委員長	：浅井　覚	三機工業㈱
副委員長	：吉田　勝	㈱ダイフク
ｺｰﾃﾞｨﾈｰﾀｰ	：伊達　浩章	三機工業㈱
副ｺｰﾃﾞｨﾈｰﾀｰ	：山下　佳一	㈱岡村製作所
メンバ	：西田　光男	㈱アイオイ・システム
〃	：大西　孝司	オークラ輸送機㈱
〃	：井上　幸範	㈱岡村製作所
〃	：関　　隆志	㈱コンテック
〃	：秋川　健次郎	㈱サトー
〃	：谷川　裕俊	新光電子㈱
〃	：稲野　俊治	㈱寺岡精工
〃	：岩瀬　緑朗	トーヨーカネツソリューションズ㈱
〃	：十河　信宏	トーヨーカネツソリューションズ㈱
〃	：鳥海　和敏	トーヨーカネツソリューションズ㈱
〃	：松原　弘一	㈱日立プラントテクノロジー
〃	：宮田　和久	㈱PFU
〃	：大津　真人	㈱PFU
〃	：井上　忍	ムラタシステム㈱
〃	：森川　秀二	リンテック㈱
〃	：斉藤　浩樹	リンテック㈱

●開催経緯

日程	テーマ
第 1 回 2009 年　4 月 26 日(月)	分科会のテーマ検討
第 2 回 2009 年　7 月　2 日(木)	分科会のテーマ検討、委員長、副委員長決定
第 3 回 2009 年　9 月　9 日(水)	物流システムガイドライン見直しにテーマ決定 現状の問題点及び展開方針、スケジュール決定
第 4 回 2009 年 11 月 18 日(水)	分担決定
第 5 回 2010 年　2 月 10 日(水)	2009 年度活動結果報告、2010 年度活動方針報告
第 6 回 2010 年　4 月 26 日(月)	ガイドライン検討
第 7 回 2010 年　6 月 29 日(火)	ガイドライン検討
第 8 回 2010 年　8 月 26 日(木)	ガイドライン検討
第 9 回 2010 年 12 月 16 日(木)	ガイドライン検討
第 10 回 2011 年　2 月　9 日(水)	ガイドライン読み合わせ
第 11 回 2011 年　3 月　8 日(火)	ガイドライン読み合わせ

目　次

はじめに

本ガイドラインの原本は、前社団法人　日本ロジスティクスシステム協会　物流システム機器推進部会　ＩＴ分科会にてまとめた 2003 年 4 月のガイドライン本編その後 2006 年 3 月のコンピュータウイルス対策編、2008 年 3 月のセキュリティ編である。
今回、一般社団法人　日本物流システム機器協会（以下ＪＩMH）機種別委員会　情報系委員会にて再度見直し再編集して 1 冊にまとめることとなった。

本ガイドラインの目的は、近年MH（マテリアルハンドリング）とＩＴ（情報技術）を活用していかにシステム的に工場や物流センターを運営していくかが企業経営の課題となっている。こうした背景のもと、ＪＩMHにて物流システム機器における情報システムを現視点から再度見直し、現在の環境・技術を鑑みながら再編集した。

本書は、物流システム機器における情報システムを納入する際の契約～品質保証～教育～保守に至るまでをベンダ視点で配慮すべき事項と、セキュリティ対策として、不正アクセスによる情報漏洩やデータ破壊などのリスクに対して、我々ベンダが取るべき対応・対策をまとめている。合わせてコンピュータウイルス対策として、ネットワーク社会を前提とした現在では、常にウイルス感染への対応が求められている。これを前提に、ベンダ・ユーザ共に配慮しなければならない具体的事項を取りまとめている。
システムを納入する際のガイドラインとして有効に活用、利用されることをお願いする次第である。
そしてこの資料を通して我々ベンダもユーザもお互いに健全なる企業活動を行うことが出来れば幸いである。

今回のガイドライン見直しに一年半を要しましたが、会員企業の皆様ご協力有難う御座いました。

2011 年 3 月

一般社団法人　日本物流システム機器協会
機種別委員会　情報系委員会
委員長　浅井　覚
副委員長　吉田　勝

１．契約

契約とはベンダがユーザに対し必ず伝え承認を得ておくべき事項である。
ベンダは契約の締結をもってハードウェア・ソフトウェア・エンジニアリング、その他の役務の手配及び設計を開始することができる。

1.1 前文

1)タイトル

契約内容が一目でわかるようにする。
記載例
「ソフトウェア開発委託基本契約書」

2)当事者の表示

契約書には契約の当事者を表示する。
法人の場合、本社の所在地住所と法人名で記入する。
前文のところで「以下〇〇株式会社を甲、□□株式会社を乙という」と断ったうえで、それ以降の契約条項中では「甲」「乙」と略記する。

3)目的条項

第一条として契約の趣旨、目的や目的物の内容を具体的に記載する。
記載例
「甲は、本契約に定める条件で、対象ソフトウェアの開発に係る業務を乙に委託し、乙はこれを受託するものとします。」

4)個別契約

対象となるソフトウェアの開発にあたり、サービス内容を個別に分け個々に契約を結ぶ。
個別契約に於ける取引条件を定める。
取引条件は、
・各サービスの前提となる資料の特定
・各サービスにおける作業範囲の明細
・双方の役割分担
・作業スケジュール
・納入物品の明細、納入期日、納入場所
・検収方法
・対価の支払い条件
などがある。
個別契約には本契約の各条項が共通に適用されるが、個別契約と本契約が異なった場合は、個別契約が優先される。

1.2 推進体制の強化

1)窓口の一元化

当事者はシステム構築履行のための連絡、確認を行う主任担当者をベンダ、ユーザそれぞれ一名ずつあらかじめ定め、書面をもって相手方に通知すること。また主任担当者の変更があった場合には、直ちに相手方に対して、書面をもって通知する。

2)定期協議会の開催

当事者はソフトウェアの開発が完了するまでの間、その進捗状況の報告、問題点の協議・解決、その他ソフトウェア開発の推進のために必要な事項を協議するため、定期的に協議会を行うものとする。協議会の開催頻度は両当事者が協議のうえ定めるものとする。また、ベンダは必要に応じて本ソフトウェアの直接利用者等、必要なユーザの従業員を会議に出席させるようユーザに対し要請ができるものとし、ユーザはそれに応ずるものとする。

3)役割分担

ユーザおよびベンダ双方の役割分担を定め円滑な遂行が行えるようにする。

1.3 仕様の確定

1)仕様の作成主体

ソフトウェアを構築するための仕様書を作成する作業の形態を取決めておく。一般的には、ベンダが仕様の作成を請負、これを完成させるものとし、またユーザはベンダに対し必要な情報を提供する。

2)仕様の検収

ベンダは仕様が完成したとき、これをユーザに引渡すものとし、ユーザは遅滞なくこれを検査し、その結果をベンダに報告する。

3)仕様の確定手続

双方の責任者が仕様書に署名捺印を行うことをもって、仕様が確定されたものとする。

1.4 仕様の変更

解約も含め、仕様変更が発生した場合の手続きを取決めておく。

1)変更の申し入れ及び受入れ方法

ユーザ、ベンダ双方からの仕様変更の申し入れ及び受入れ方法を定める。

双方の協議によって定められた書面により変更の内容、理由等を明示してソフトウェア開発責任者の署名捺印を行ったうえでこれを相手方に通知する。

相手方から仕様変更の申し入れがあった場合、双方にて変更の内容及びその可否について協議を行うものとする。

協議の結果、変更の内容が契約に定める金額、納期その他の契約条件に影響を及ぼすものであると両当事者が判断した場合には変更契約を締結して契約内容を変更することの

みによって、仕様の変更を行うことができる。
協議期間を定めそれまでに締結できない場合は変更前の内容で業務を進めることができる。

2)変更仕様書の作成
仕様の変更が行われた場合、ベンダは変更仕様書の作成を行う。
双方、協議の結果、変更内容が軽微なものと判断された場合には、変更の内容、理由等を明示した書面をもって変更仕様書に替えることができる。

3)変更された仕様書の確定手順
双方の責任者が変更仕様書、またはそれに変わる書面に署名捺印することにより仕様の変更が確定されたものとする。

1.5 検収
1)検収の基準
ユーザ及びベンダは協議のうえ、検収の基準となる仕様書、テスト項目、テストデータ及びテスト方法等を定めた「検査仕様書」を作成する。

2)検収の期間
検査仕様書には検査の長期化を防ぐため期間を定める。ユーザ側の検査の結果、成果物が検査基準に合致することを確認した場合は、両者協議のうえ定める検査合格書にユーザ側ソフトウェア責任者が署名捺印を行ったうえでこれをベンダに交付する。
検査合格書が交付されない場合であっても、検査期間内にユーザから書面による異議の申し出がない場合は、当該期間を持って、検査は合格したものとする。
なお、検査合格をもって、ユーザの検収は完了したものとする

3)検収の方法
検収方法については、検査仕様書を作成し、事前にユーザ側と内容のすり合わせを実施した後、これを基に検収検査をユーザ立会の下実施する。

1.6 瑕疵担保責任
1)瑕疵とは
瑕疵というのは“欠陥”である。すなわち、契約内容と照らしてみて性能などの点で不完全な部分があり、ユーザが期待していた性能、ソフトウェア会社が保証していた性能などが備わっていないことをいう。
また、提供したものが著作権などの第三者の権利を侵害していた場合も瑕疵である。
しかし、瑕疵担保責任で問題となる瑕疵とは「隠れたる瑕疵」である。これは表面に現れていない部分や引渡しを受けた際に通常の購入者がある程度注意をしても分からない瑕疵のことである。

2)瑕疵担保責任と無過失責任

取引の目的物に瑕疵があった場合は、その目的物の提供者は無過失責任を負う。すなわち、過失の有無にかかわらず瑕疵が存在したということだけで責任を負わなければならない。

ただ、瑕疵のあるものを引渡した場合、そのものが不完全であることから債務不履行の一類型である不完全履行を構成するか（未だ引渡しが完全に行われていないとするか)、それとも一応引渡し義務を履行したということを前提とする瑕疵担保責任とするかが問題となる。

3)損害賠償の範囲

ソフトウェアにおける欠陥や仕様との不一致が発見された場合、ベンダの責任に於けるユーザの損害についての賠償は、免責されるものとする。

4)瑕疵担保責任期間

ベンダが無償で修正する期間、及び瑕疵責任を負う期間は、引渡しから１年間とする。

1.7 知的財産権

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。

【所有権に帰属するもの】（請負契約によって作成されたソフトウェア）

・プログラムを自己のために利用すること
・他の人に利用させて収益を上げること
・第三者に売買などにより処分すること

【著作権に帰属するもの】

・複製、翻訳等をすること

（注記）著作権法：著作者の創作行為を保護する目的であるため、「全ての権利は発注者に帰属する」となっていても現実に著作物を創作した者が、原始的に取得する。

1)プログラムの権利の帰属

プログラム全体に関する権利については、ベンダに帰属するものとし、使用権をユーザに与えるものとする。この内容を契約書に盛り込む。

「プログラムの著作権については、ベンダに帰属するものとし、使用権をユーザに与えるものとする。」

2)ドキュメントの権利の帰属

ドキュメントに関する権利については、ベンダに帰属するものとし、この内容を契約書に盛り込む。

「ドキュメントの著作権については、ベンダに帰属するものとする。」

3)ルーチン、モジュール等の権利の帰属

プログラム中に使用されている既存、新規に開発されたルーチン、モジュール等の権利は、ベンダに帰属するものとし、この内容を契約書に盛り込む。

「プログラム中に使用されている既存、新規ルーチン、モジュール等の権利は、ベンダに帰属するものとする。」

4)無形情報の取扱い

本契約に基づき開発されたアイディア等については、両当事者が適当と判断する方法によりこれを使用できるものとする。

1.8 機密保持義務

契約期間中及び契約終了後の機密保持に関して取決めておく。

ベンダ及びユーザ双方の機密保持について相互に契約内容を盛り込む。

「ベンダ及びユーザはお互い知り得た情報を第三者に漏らしてはならない」ことを前提に下記に、ポイント、目的、他を述べる。

1)機密保持契約のポイント

機密保持には２つの側面がある。１つは委託者であるユーザの機密保持であり、もう１つは外注先に対して自社・ユーザの機密をいかにして保持するかである。

ユーザの機密保持には、以下の点を十分に検討する

・機密保持の目的
・機密の範囲
・機密保持の内容（開示できる人の範囲、下請けの問題、管理方法、無断の複製・廃棄禁止・返却義務、従業員との契約）
・適用除外事項
・機密保持の期間
・ペナルティ
・協議事項

2)機密保持の目的

ユーザの機密資料を一方的に預かる場合と共同開発のようなケースでは機密保持契約内容も自ずと異なってくる。従って、機密保持の目的を明確にする必要がある。

3)機密保持の内容

(1)開示できる人の範囲

単に「第三者に機密を開示してはならない」といった程度に留めるか、「指定した担当者以外その機密資料を取扱いしてはならない」といった厳しい取決めをするのか検討する。

(2)下請けの問題

特定の業務について一切下請けを禁止するのか、下請けに対し必要な機密保持の措置

をとらせるのか検討する。

(3)管理方法

具体的な管理方法を検討する。(鍵のかかる場所に保管する。担当者以外立入ることのできない収納場所に保管する等)

(4)無断複製・廃棄禁止・返却義務

無断複製・廃棄・目的外利用禁止は当然であるが、それを担保するための立入り検査条項を入れるといった検討をする。

(5)従業員との契約

従業員との間で特別に機密保持契約を締結するかどうか検討する。

(6)適用除外事項

既に入手している情報、公開している情報、周知の情報など機密保持の適用除外の項目について、具体的に明らかにしておく必要がある。

(7)機密保持の期間

いつまで機密保持義務を負うのか、２年、５年といった合理的な期間を定めておく。

(8)ペナルティ

従業員の故意・過失によって機密が漏洩したような場合の責任を制限しておく必要がある。

(9)協議事項

どうしてもあいまいな項目も残るので、協議事項を入れておくのが望ましい。

1.9 その他

1)支払遅延

本契約または個別契約により生じる債務の弁済を怠ったときは、支払期日の翌日から完済の日まで年利〇%の割合による遅延損害金を支払うといった取決めを行う。

2)契約の解除

ユーザ又はベンダが下記のいずれかに該当したときは、相手方はなんらの通知、催告を要せずただちに本契約および未だ履行の完了していない個別契約の全部または一部を解除できるものとする。

(1)手形または小切手が不渡りとなったとき

(2)差押え、仮差押え、競売の申立があったとき、もしくは租税滞納処分を受けたとき

(3)破産、会社整理開始、会社更正手続き開始または和議の申立があったとき、もしくは清算に入ったとき

(4)解散もしくは営業の全部または重要な一部を第三者に譲渡しようとしたとき

(5)契約の基づく債務を履行せず、相手方からの相当の期間を定めて催告を受けたにもかかわらず、その期間内に履行しないとき

(注記) 損害賠償について

上記のいずれかに該当したことにより相手方に損害を与えた場合、両者にて損害額等を協議のうえ、本契約又は個別契約に定める作業に対する代金相当額を限度として賠償責任を負わなければならない。

(注記) 損害賠償の範囲について

当事者の責に帰すことのできない事由から生じた損害、予見の有無を問わず特別の事情から生じた損害、逸失利益については、賠償責任を負わないものとする。責任を負う期間を、検収完了日より〇ヶ月といったように定めるものとする。

3)輸出管理

本契約または個別契約により納入された成果物（納入物品）を輸出する場合は、外国為替、外国貿易管理法等、技術輸出に関する関連法規を遵守するものとする。

4)裁判管轄

一般的には被告の所在地を管轄する裁判所となっているが、金銭的な面については義務履行地となっている。よって、契約書では自社の所在地を管轄する裁判所とすることを取決めておく。

5)誠実協議

本契約に定めがない事項について双方が円満に解決することの旨を記載する。

6)作成年月日

契約の成立の日を証明する記載として、大変重要。日付は、契約の有効期間を確定し、正当な期限のもとに作成されているかを判定する基準となる。実際に契約書を作成した日を記載する。

7)契約当事者の署名押印（記名捺印）

本店住所・法人名を記載し、代表者（株式会社であれば代表取締役、公益法人などでは理事・代表理事など）が、署名・押印する。

印鑑は、通常、登録してある印鑑（実印）を押印するのが望ましい。

8)目録（物件目録・見積書 etc）

契約の対象物を記載する。この表示は、契約条項中に記載してもかまわない。但し、物件の数が多いときには、別紙として物件目録に物件や商品名を表記し、契約条項本文では、それを引用する方法がとられる。

9)収入印紙の貼付

印紙税法の定めにより、請負契約書等には、収入印紙を貼付する必要がある契約書を複数作成する場合は、それぞれに印紙の貼付が必要となる。ただ、印紙の貼付の有無と契約の効力とは直接の関係はない。印紙がなくとも契約は有効である。貼付した印紙には、契約書に使用した印鑑で消印をする必要がある。

10)作成通数の記載

当事者間で合意が成立した旨、契約書の体裁を整える文章を置き何通作成したかを記載する。

＜補足＞

物流情報システム開発の契約類型について

物流情報システム開発の受託に当たっては、プロジェクト活動における成果物・役割分担について、ユーザ・ベンダ間に共通の理解が得られない事に起因するトラブルが多々ある。具体的には、仕様齟齬・仕様ミス・業務範囲の食違い等である。これらトラブルが発生した場合、プロジェクト進捗に悪影響を与えると共に、最終的な対処（仕様変更・仕様追加等）の費用負担をユーザ側に請求できない（泣き寝入り）ケースも散見される。
上記の様な問題を未然に防ぐためにも、開発フェーズの各段階において契約類型（請負型か準委任型）を分ける、多段階契約（方式）の採用が望ましい。

請負契約と準委任契約について

請負契約は「仕事や物（プログラムなど）の完成」を約束することが契約の目的であり、準委任は「プログラムを開発するために知識や労力といったサービスの提供」をすること自体が契約目的となっている。故に、請負契約においてその活動の対価を得るには、プログラムを完成させなければならない。
準委任において対価を得るためにはプログラムを開発するために知識や労力などのサービスを提供する必要はあるが、プログラムの完成ということは約束されていない。すなわち、プログラムが完成しなくても、それまでに提供したサービスの割合に応じて対価を得られる。
また、請負では費用が当初の計画より増加しても契約金額を変更することは、原則的に出来ない。一方、委任の場合は、サービスの提供（プログラム開発）のために必要な費用は請求ができる。
従って、新規の取組で難易度が高く、開発コストの見積もりが困難な場合にはシステム開発契約は準委任型をとるべきである。

＜システム開発業務と推奨契約類型＞

フェーズ	対象業務	推奨契約類型	
		準委任	請負
企画	システム化計画	○	
	要件定義	○	
開発	システム設計（外部設計）	○	△
	システム設計（内部設計）		○
	プログラム設計		○
	プログラム製作		○
	単体・結合テスト		○
	総合テスト	○	△
	導入支援	○	
運用	運用支援	○	
保守	保守	○	○

凡例　○：推奨　△：案件の事情により適用

２．品質保証体系

2.1 契約仕様書・製作仕様書の位置付けの明確化

システムの開発において、そのシステムの品質特性を明らかにする。そのためにユーザとの契約において契約仕様書・製作仕様書を作成し、ユーザからの要求事項を明確にする。

さらに、

・ユーザとベンダの役割分担

・完了時期

を明確化する。

システム検収時に、性能テストによりユーザとベンダ双方で品質を確認し、それぞれの責任範囲を明確にする。

これにより、ユーザの品質要求事項のギャップをなくし、曖昧さにより発生する「瑕疵担保責任」等による手直しを未然に防止する。

1)契約仕様書・製作仕様書に記載するべきこと

(1)システム化の目的と方針

(2)狙いとする効果

(3)マスタ工程

開発計画をマスタ工程にしたがって工程管理するため、ユーザ・ベンダとも工程を厳守する規定も契約仕様書にて明確に規定しておく。

(4)開発プロセス開始の条件

製作仕様書の承認をもってスタートとする。

(5)システム開発の条件

システム化の範囲と既存システムとの関連及び検収時の留意点を述べておく。

(6)開発プロセス作業中の体制や環境条件

ユーザとベンダの役割分担と完了時期を明示する。

(7)貸与物件・資料

開発作業に必要な資料・伝票・書類・機器類等の貸与条件や機密保持条件及び返却の必要性明記する。

(8)開発機器・使用材料の負担

開発に必要な資材や機器の費用負担・端末や周辺機器の導入時期や費用などの条件を明示する。

(9)仕様変更への対応手順と管理方法

打合せ議事録などの位置付けも契約仕様書などに明確化しておく。

(10)検査成績書など提出書類

2)製作確認事項

(1)システム化の概要

新規製作か既存システムの改造などを明確化させる。

(2)システム化の内容

上記システム化の概要の詳細

(3)ハードウェア・ソフトウェア・ネットワークの構成
現行のシステム構成を継承するか新しいハードウェア・ソフトウェア・ネットワークの構成とするかを明示する。
(4)システムの運用計画
システムの稼働時間や稼働環境に関する運用計画を明示する。
(5)成果物・納品物
製作納品する成果物・納品物を明示する。
(6)パッケージソフトウェアの使用
システム構成に使用するパッケージソフトウェアを明示する。
(7)工程計画
受注からシステム開発作業での企画プロセス・開発プロセス・運用プロセスの各工程計画を明示する。
(8)性能と品質の内容の確定
品質で重要なことはユーザが要求した機能､性能が十分満足されているか否かである。そのためその性能、機能を具体的に明示し確定させる。なお性能、機能を品質的に具体的に示した品質仕様書を明確にしておく。
(9)性能と品質の確認手段
開発システムの品質・性能に関して相互に確認するための保証手段たとえばテスト方法・テストツールの種類など品質と性能の確認手段を明示する。
(10)納期と稼働までのスケジュール
ハードウェア・ソフトウェア・ネットワークの導入時期、開発システムの納期、そして稼働までの運用テスト・教育・訓練期間を明示する。

2.2 ユーザ検収の規定と検査結果に基づく責任範囲の明確化
ユーザからベンダへの引渡しのため作業確認として検収がある。
検査基準や終了手続きが不明確であるとトラブルが発生し、無償保証の延長という状況がおこりうる。
検収実施の詳細に関しては検査仕様書を作成し、ユーザ側と内容のすり合わせを行い承認してもらうこと。
また、ユーザの検収時にすべての項目を検査することは難しいため、内容に応じてはベンダにて事前に検査を実施し検査成績書を作成し、それをユーザに提出し確認して頂く方式を事前にユーザとコンセンサスをとっておくこと。　スムーズに引渡すために検収条項を契約書に明示しておく。

1)検査仕様書作成時の記載内容と確認事項
(1)検収日時と場所の確認
(2)検収時に納入する物件の確認（事前にドキュメントやプログラム等の一覧について確認する。）
(3)立会い者の確認
(4)その場で確認できる内容と後日でなければ結果が確認できないこと内容の明確化（後日確認する項目に関してはその確認方法の手順の確定）

(5)妥当性確認のスケジュールの確定
(6)検収方法（検査基準・検査期間）
(7)検収終了手続き
以上により検収条件が明確化される。

2)考慮すべき事項
(1)ハードウェア・ソフトウェアとも実際の稼働環境においてテストし、その機能・性能を確認すること。
(2)システム内容によりヒートランテストを自主的に実施すること。

3)ドキュメントの検収
(1)システム仕様書にレビューの承認があるか確認する。
(2)システム仕様書に仕様変更や追加事項などの記載漏れがないか確認する。
(3)納入するドキュメントのうち、操作マニュアルと保守マニュアルの内容については記載項目に誤りがないかを確認する。

4)検収・引渡し手順と責任範囲の明確化
(1)機能確認
1つ1つの機能が要求仕様書通りに作動するかシステムを確認する。
(2)上位システムとの整合性の確認
上位システムとの間にデータの相違がないか、データの受渡しの方法、時間の整合性がとれているか確認する。
(3)性能確認
要求性能に対して、要求通りの動作を行い要求時間内に処理が完了しているか確認する。
(4)障害回復処理の確認
障害を発生させて、回復処理が正しく行われるかを確認する。
(5)操作の確認
キーボードが操作しやすいか、画面が見やすいか等の操作性の確認をする。
(6)検収終了後のオペレーション教育実施・完成図書及び鍵の引渡し等の終了。
(7)工事完成後、ユーザが実施する試運転の結果、設計・製作・施工上の不備・欠陥がないと判断した場合、ベンダよりユーザに書面にて完成確認書を提出する
これにより工事が終了し完成・引渡しとなる。
(8)ユーザは、完成確認書を受領後に速やかに工事完了証明書をベンダに発行する。この工事完了証明書の発行をもって検収日とする。
但し、完成図書の提出が検収日以降になる場合は提出日についてユーザとコンセンサスをとること。
以上の手順にて所有権及び危険負担はユーザに移転したことになる。

2.3 ベンダ責任の基準と保証範囲

検収後に納入されたシステムや機器に対しては、一定期間ベンダ保証が実施される。
検収後にシステム仕様書との不一致や不良が発見され、その原因がベンダの責任と判断された場合には瑕疵担保条件に従い対応する。
また検収後に出された機能追加や改善の要求は仕様変更とし、追加工事として処理する。
保証範囲は受注契約したシステム及び機器である。その保証内容などは、契約時に契約書でユーザと取決めた保証条項によって決定される。
保証条項で明確にしておくのは下記の事項である。

1)保証範囲の内容と基準

(1)ハードウェア・ソフトウェア・ネットワーク

ハードウェア・ソフトウェア・ネットワークに関する保証期間、およびハードウェアの機能・性能に関する保証要件や限界性能、ソフトウェアのバグ及びネットワークの機能や接続台数に関する保証要件を明示する。

(2)システムの品質保証要件

納入するシステムの品質保証要件を明示する。
なお、稼働後に不良が多発する場合を想定し品質向上作業を実施するかの基準なども定めておく。

(3)性能保証要件

システムとしての性能、たとえば応答性などの保証範囲を明示する。

(4)セキュリティ

システムの利用に際しての機密保護や安全性に対する保証範囲を明示する。

３．検収

設計製作後、工場出荷時立会検査・現地据付・調整・運転試験（受入検査）などの工程を経てユーザにシステムが引渡される。ユーザは契約時または契約後の打合せにて確定させた検査条件に従い受入検査を実施し、受入検査合格をもって検収となる。検収をもって、納入物品の所有権および危険負担はユーザに移転する。

このように検収は、顧客へのシステム納入における重要な条件であり、以下にその要点を示す。

3.1 契約書に記載すべき完成引渡し条件（検収条件）

契約書に以下の内容を明記する。

1)検収の基準

ユーザおよびベンダは、別途協議のうえ、契約仕様書または契約後ベンダより提出される製作仕様書に基づき、ユーザの受入検査の基準となる仕様、テスト項目、テストデータ、テスト方法および合格基準値を定めた検査仕様書を作成するものとする。

2)検収の期間と条件

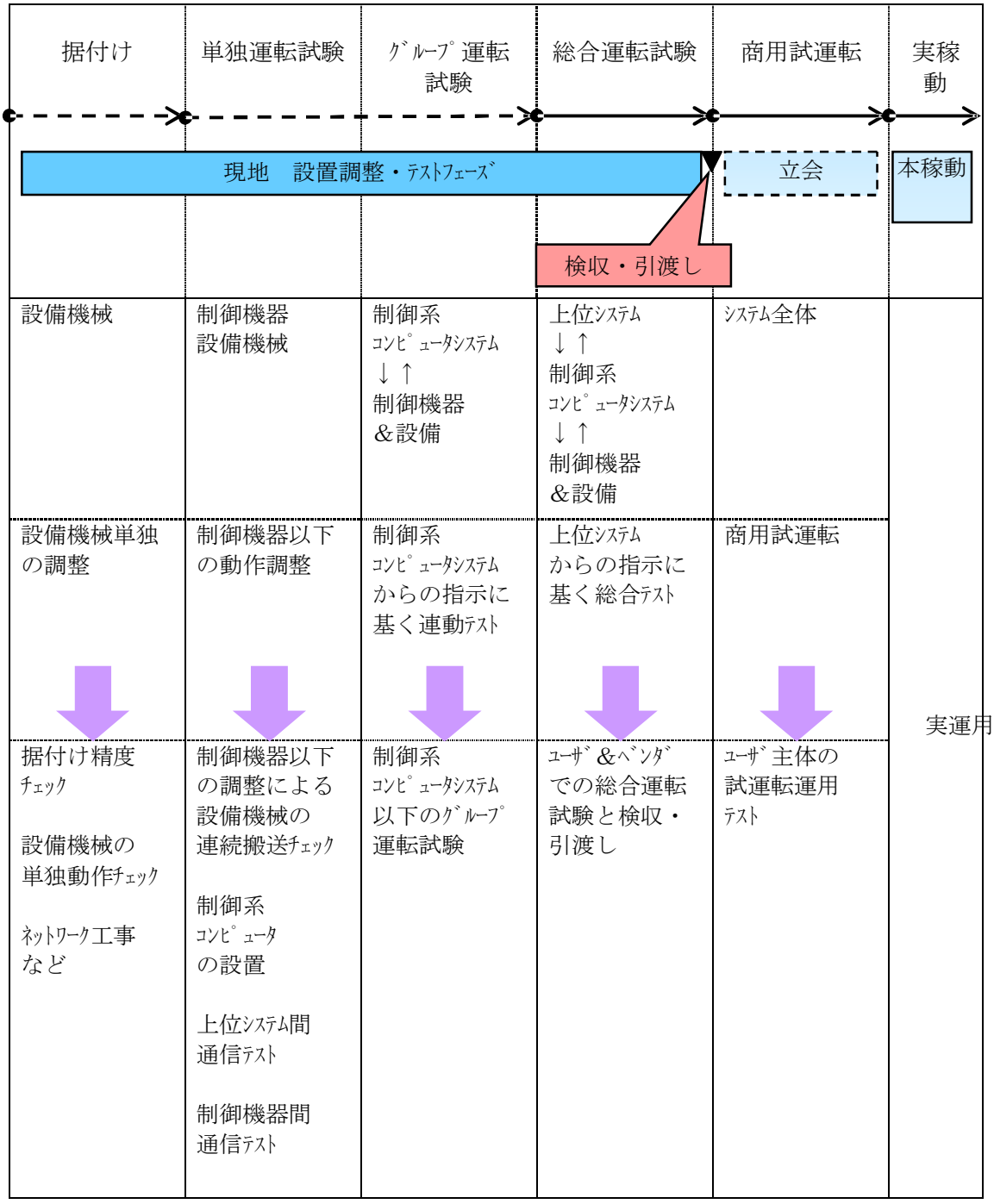
ユーザは、納入後〇〇日以内に検査仕様書に基づき受入検査を行い、検査基準に合致することを確認した場合は、両者で協議のうえ定める検査成績書にユーザにおける責任者が署名捺印を行い、これをベンダに交付し、検収完了とする。

3.2 検査仕様書

総合運転試験はベンダとユーザが共同して実施する業務である。必要な人員、日程、内容等、ユーザ要求を確認して検査仕様書を作成し、双方で内容を合意する。仕様書には、現地据付からの調整・総合運転試験（受入検査）・引渡しまでの手順、テスト項目・テストデータ・テスト方法・合格基準値およびユーザとベンダの役割分担を記載する。

1)引渡しまでの手順

次の図は現地据付後の調整から総合運転試験（受入検査）を終えてシステムを引渡し、実稼動に入るまでの手順と主たる作業の概要を示す。


据付け
単独運転試験
ｸﾞﾙｰﾌﾟ運転試験
総合運転試験
商用試運転
実稼動
現地　設置調整・ﾃｽﾄﾌｪｰｽﾞ
立会
本稼動
検収・引渡し
設備機械
制御機器
設備機械
制御系
ｺﾝﾋﾟｭｰﾀｼｽﾃﾑ
↓ ↑
制御機器
＆設備
上位ｼｽﾃﾑ
↓ ↑
制御系
ｺﾝﾋﾟｭｰﾀｼｽﾃﾑ
↓ ↑
制御機器
＆設備
ｼｽﾃﾑ全体
設備機械単独の調整
制御機器以下の動作調整
制御系
ｺﾝﾋﾟｭｰﾀｼｽﾃﾑ
からの指示に基く連動ﾃｽﾄ
上位ｼｽﾃﾑからの指示に基く総合ﾃｽﾄ
商用試運転
据付け精度ﾁｪｯｸ
設備機械の単独動作ﾁｪｯｸ
ﾈｯﾄﾜｰｸ工事など
制御機器以下の調整による設備機械の連続搬送ﾁｪｯｸ
制御系ｺﾝﾋﾟｭｰﾀの設置
上位ｼｽﾃﾑ間通信ﾃｽﾄ
制御機器間通信ﾃｽﾄ
制御系
ｺﾝﾋﾟｭｰﾀｼｽﾃﾑ
以下のｸﾞﾙｰﾌﾟ運転試験
ﾕｰｻﾞ＆ﾍﾞﾝﾀﾞでの総合運転試験と検収・引渡し
ﾕｰｻﾞ主体の試運転運用ﾃｽﾄ
実運用

2)テスト内容

契約仕様書または製作仕様書に記載された機能の確認を行う。テスト項目・テストデータ・テスト方法・合格基準値を明記する。

例として、以下のテスト項目に対し、各テストデータの確認を行う。

テスト項目	説明
単独運転試験	
起動時間	システムの起動時間に制約がある場合、起動時間を計測する。
システム切替時間	クラスタ構成等でシステムの切替りに制約がある場合､システム切替り時間を計測する。
停電時処理	停電時の UPS と連動した自動シャットダウンを確認する。
外部通信テスト	
送受信データ	送信データと受信データとが一致していることを確認する。
グループ運転試験（連動テスト）	
受信タイミング	制御装置からの受信タイミングが正しいことを確認する。
制御装置への指示	制御装置への指示のタイミングとデータが正しいことを確認する。
画面表示内容	各画面表示内容を確認する。実状態は現場から作業員が報告する。
帳票印字内容	各帳票印字の内容が正しいことを確認する。
総合運転試験	
受信タイミング	上位システムからの指示の受信タイミングが正しいことを確認する。
上位システムへの送信	上位システムへの実績データ送信のタイミングとデータが正しいことを確認する。
画面表示内容	連動テストで未確認の画面表示内容の確認と画面データの更新時間、画面の切替に制約がある場合はそれぞれの時間を計測する。
帳票印字内容	連動テストで未確認の帳票の印字内容が正しいことを確認する｡搬送対象物の個数等は作業員が計数する。
メモリ余裕	メモリの使用率に規定がある場合は、メモリ使用状況を確認する。
ディスク余裕	ディスクの占有率に規定がある場合は､ディスク空き容量を確認する。
CPU 稼働率	CPU の稼働率に規定がある場合は、CPU 負荷率を確認する。
LAN トラフィック余裕	LAN でのトラフィックに規定がある場合の確認はもちろんであるが、規定がなくてもデータとして計測しておくことを推奨する。
システム異常	納入システムで発生することが予測される異常に対する対応を確認する。

3)標準的なテストチェック項目（サンプル）

標準的なテストチェック項目

契約社名　　：
最終需要社名　：
工事名称　　：

ページ　：　／

チェックリスト記入者　：
記入日　：　　－　　－

チェック項目	記載例/（項目説明）	確認	備考
1製作仕様書 の仕様確認			
システム構成図	システム構成の装置&機器が合致しているか		
ハードウェア仕様			
機器リスト	画面サイズを含む機器仕様とその台数		
ユーティリティ	電源、接地、無停電電源装置の有無		
備品リスト	予備品、消耗品、工具の種類と員数		
2システム稼働条件	24時間運転、自動立上げ/立下げは機能するか		
3通信機能確認			
上位システム との送受信	上位システムとのデータ交換、テキスト内容		
下位制御装置 との連携	システムとの制御データ交換、テキスト内容		
ﾈｯﾄﾜｰｸ施工	ﾈｯﾄﾜｰｸ構築とセグメント化（ｽｲｯﾁ、ﾘﾋﾟｰﾀ）		
4ソフトウェア 機能確認			
入庫機能	入荷、入庫、入庫経路，棚引当条件など		
補充機能	補充タイミング		
出庫機能	出庫、出荷、引当条件など		
ピッキング機能	ピッキング経路、操作性		
積み合わせ機能	ユニット、バラ混載、梱包明細		
検品機能	検品機能&操作		
梱包&仕分け機能	方面別、商品別		
出荷機能	送り状、出荷明細		
棚卸機能	棚卸機能、操作性		

記入部分：太枠部

確認記号　○：合格　△：不明確（要明確化）　×：不合格　－：記述不要

標準的なテストチェック項目

契約社名　　：
最終需要社名　：
工事名称　　：

ページ　：　／

チェックリスト記入者　：
記入日　：　－　－

チェック項目	記載例/（項目説明）	確認	備考
５ソフトウェア 仕様条件			
データ処理	演算処理、収集タイミング、トランザクション処理		
データ管理	データ件数、データ保存、保存期間		
在庫管理	棚管理、総在庫数管理、更新タイミング		
画面表示	画面レイアウト、動作&操作性		
帳票印字	印刷帳票機能・数・レイアウト		
システム管理	システム運転開始から終了までの操作機能		
監視・記録機能	監視・記録機能は実現するか		
６システム異常対策			
システム インタロック	棚満了、搬送物とデータ不整合の対策と復元		
設備機器故障対策	機器故障とダウン対策		
瞬停対策	UPS、CVCF などの停電対策と復電		
コンピュータ 機器故障	機器故障とダウン対策		
データ復旧	ロールバック処理		
ファイル復旧	外部媒体復元とリカバリ処理		
７可用性向上と 冗長性	信頼性要件の為の DISKRAID 機能、CPU 二重化、CPU クラスタリング機能の実現		
８その他	拡張性、移植性		

記入部分：太枠部

確認記号　○：合格　△：不明確（要明確化）　×：不合格　－：記述不要

3.3 検査における役割分担

受入検査は承認した検査仕様書に基いて調整を完了したシステムの機能・動作が正常に製作されているかテストを通して確認する作業である。このテストはユーザとベンダ双方の共同作業で実施する。特にこの受入検査は荷役作業を伴うテストとなることが多く、その作業工数により多額の費用を要するケースも考えられる。従って作業工数が計画を大幅に超える事態を防ぐには

・テストデータの作成
・テスト用搬送ワーク準備
・作業人員の確保

などについて事前にユーザと共に入念なテスト計画を立案すると同時に、ユーザとの間での役割分担を明確に決めておく必要がある。この役割分担は契約条件でもあるので、契約時にはユーザとベンダとの分担が曖昧にならないように確定しておく。

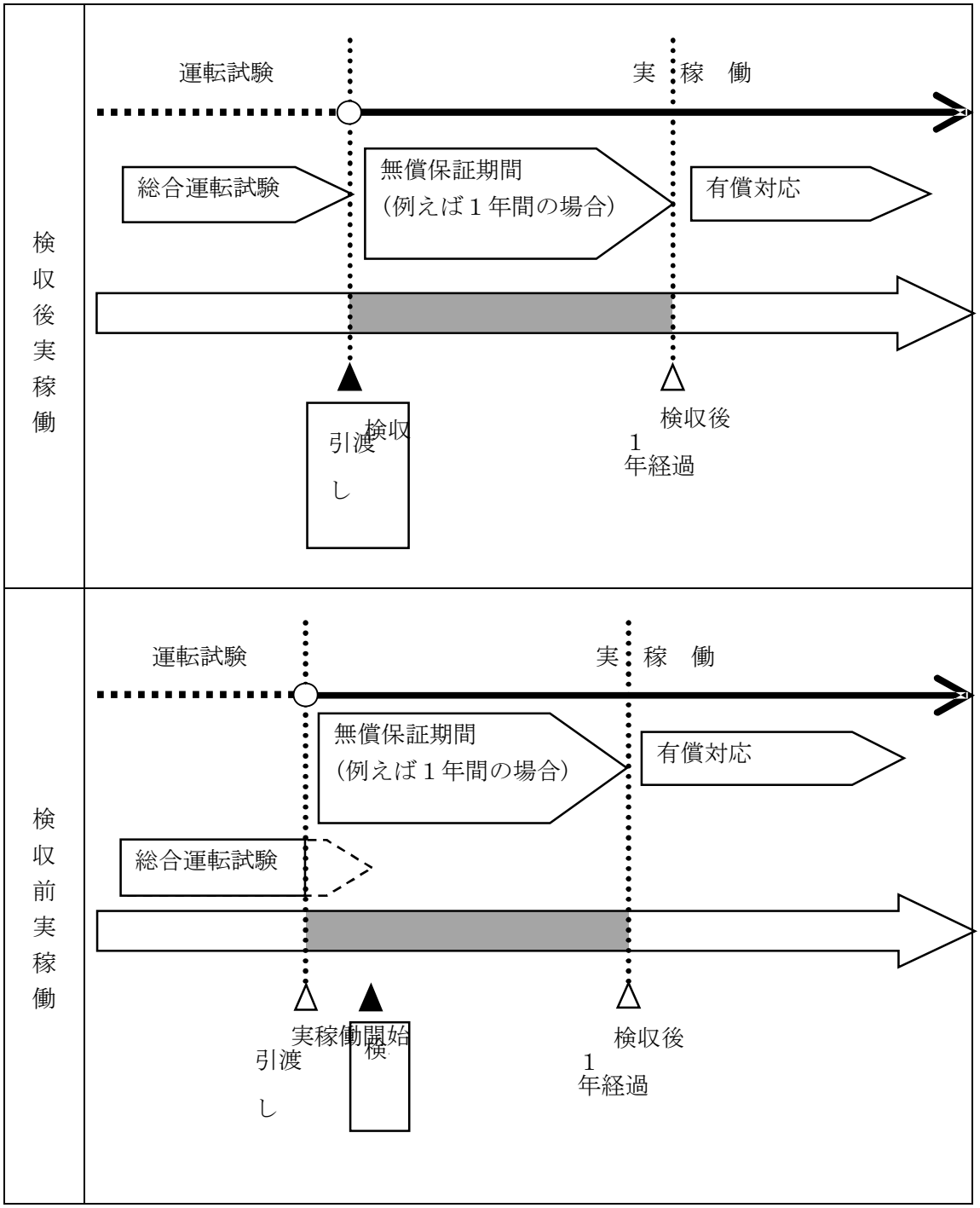
役割分担例を以下に示す。

作業	ユーザ	ベンダ	備考
役割分担表			
検査要求の作成	○		
検査項目の作成		○	ユーザが承認したシステムの仕様書を使用
検査仕様書の作成		○	
検査仕様書の承認	○		提出後２週間
検査日程の調整	○		日程、人数
検査要員配置計画	○		
検査用データの準備			
マスタデータ	○		
入荷／出荷計画データ等	○		
検査の実施			
物流機器の運転	○		現地運転員の配置も含む
搬送対象物の手配	○		搬送対象物の移動も含む
検査の進行指示		○	
検査結果の確認	○	○	
検査成績書の作成	△	○	検査仕様書への検査結果記入にて対応
検査成績書への合格署名捺印	○		

記号　○：主担当　△：場合により部分を担当

3.4 検収と保証期間

保証期間は検収によりシステムをユーザに引き渡すと同時に開始する。ただ検収前に実稼働に入る場合は、納入物品の所有権および危険負担もユーザに移転するとともに保証期間も開始となる。この保証とは保証期間内にユーザよりベンダの瑕疵による不適合が報告された場合、ベンダはその不適合対応を無償で行うことを言うが、この検収と保証期間の関係を次に図示する。



【参考】

参考１．検収・引渡しにおける問題点

1)工場出荷時の検査・現地での運転試験などの契約条件に従って遂行しているが、ユーザから見れば本運転経過後のシステム安定まで面倒を見て欲しい気持ちがあり、システムの完成の承認がなかなか得られない。検収の完了が明確な形で確認できないと、検査の長期化につながる。

2)検査の対象となる仕様が明確に確定されていたとしても、その仕様に合致していることをすべてについて検査することは現実的でない。広範囲に検査をすればするほど検査期間の長期化を招き、いつまでも検収されないという不都合を招く。

3)受入検査時に実用機能との違いが発生し、機能追加・変更要求が出され、検査不合格となることがある。特に、受入検査に引続き商用試運転が実施される場合、受入検査と商用試運転との境界が曖昧になる。その結果、商用試運転で問題とされるべき改善要求や追加要求がなされることがある。

参考２．検収・引渡しにおける問題への対策

上記問題における対策を以下に示す。

1)完成引渡し条件（検収条件）を契約書に明記する。

2)検査期間を具体的な日数で規定し、その期間内に検査を終了させること、またその期間内に意義がなければ検査合格とみなすこと、合格については書面で確認することなどを検査の基準とともに契約書で明示する。

3)改善要求や機能追加要求は受入検査と分離して考える。限られた期間における受入検査には限界があり、検査後に瑕疵が発見されることもあるが、これらは瑕疵担保条件に従い対応がなされる。また検査後に出される改善要求や機能追加要求は、仕様変更として対応する。

４．教育

4.1 教育の目的と位置付け

1)設備の操作運転方法を説明し理解させることを目的とする教育

(ユーザがベンダの補助がなくても望ましい操作(作業)ができることを目標とするもの)

・設備引渡しの条件として位置付けられる教育

・通常、契約範囲に含まれる。

・教育の範囲、日数あるいは回数は、契約時に取決めて置くことが望ましい。

・単品の装置などでは、取扱説明書として製品に添付し提供されることもある。

2)設備運営の効率向上を目的とする教育

(作業者を対象として、稼働中に常に適切な判断を行える能力を養成するもの:ユーザが独自に行う教育、ベンダがユーザから委託され有償で行う特定の教育)

・設備運営の観点から作業効率向上を目指す手段として位置付けられる教育

・明確な規定が無い場合は、契約に含まれない。

・教育の範囲と内容は様々であり、案件ごとでの対応となる。

4.2 教育の仕様

1)教育の範囲と内容

教育はユーザとベンダの相互協力によって効果するものであり、教育の目的に従ってその範囲と内容を明確にする過程でそれぞれの役割を確認する。

ただし、納入設備の構造、機能、操作（運転方法、想定される障害発生時の復旧方法を含む）についてはベンダの責任で教育を行う。

教育がその目的を達成できるように契約の範囲内であるか否かを含め位置付けを明確にし、ユーザとベンダ各々の責任において何を準備するかを事前に確認する。

・教育の目的（習得すべき事項）と実施方法

・他の工程との摺り合わせ

・教育に使用する（テスト）搬送物等の手配及び取扱と管理責任者の明確化

＜引渡し時の教育仕様例＞

教育の実施時期
トレーニング（シミュレーションテスト,運用テスト,仮稼働等）開始前に行う
総合試運転時に教育計画を組込む

	教育の実施方法
事前説明	操作マニュアル等による机上での説明
実施説明	総合試運転時に OJT による実地訓練を行う
反省会	質疑応答による補足と、感想文等による理解度の記録を残す

＜引渡し後の教育例＞

教育の効果を高めるために実施するもの。

但し、これらの教育の扱いは契約時点で明確にしておくことが望ましい。

(1)本稼働後一定期間（約１～３ヶ月）経過後の教育

(2)保証期間切れ（検収後１年経過）時の教育

(3)現場担当者の大幅異動時の教育

2)教育項目と対象者

教育の目的および項目と、その対象者を選定し、教育が効果的なものと成るようにする。

対象者選定の際には、短期間に最大の効果を得るためにキーマンへの教育を優先する。

＜教育対象者の例＞

教育対象者	職務概要
システム管理者	システムの内容及びコンピュータ運用知識を有する専任者
現場責任者	現場運用の責任者あるいは、現場運用チームごとのリーダ

（注記）個々の作業者に関する教育は、現場責任者・現場リーダが行うものとし、ベンダは、立会い期間内での支援とする。

教育項目　*1)	対象者	
	システム管理者	現場責任者
システムの立上げ	○	○
始業前点検　*2)	○	○
システムの立下げ	○	○
通常運用+例外処理	○	○
異常処理	○	△
消耗品交換　*3)	○	○

*1) 各教育項目の受講者に対し、その力量（資格、教育受講実績、実務経験等）が受講条件として要求される場合は、それを明確にする。

*2) 電源やハードディスクの LED 確認、異音異臭の有無など業務開始前の実施が望まれる事柄。

*3) プリンタヘッド、用紙の交換や消耗品の摩滅等による故障時の一般的対応方法。

3)教育の計画

教育の実施計画を策定する際には、教育対象者のスケジュールを調整・確保し、無理のない日程を定め、関係者への意識付けを図る。

4)教育の教材と役割分担

教育を効果的に行うために適切な教材を選定し、その準備に当たり役割分担を明確にする。

机上での説明から、実際の設備を使った OJT まで、教育の目的に応じて最適な方法で実施する。

それらの教育を実施するに当たり何を教材とするかを明確にし、さらに、その準備について分担を明確にする。

＜教育における役割分担例＞

	ユーザ	ベンダ	備考
標準マニュアルの準備		○	標準の操作マニュアル、取扱説明書など
標準教育の実施		○	標準コースより選択
システム仕様書の準備	○		ユーザが承認したシステムの仕様書を使用
運用・運転マニュアルの作成	○		現地運転要員用の社内マニュアルの作成
運用・運転マニュアルの説明	○		現地運転要員の教育

５．完成図書

5.1 提出図書

提出物は、以下のものとする。

No.	名称	概要	部数	提出時期
1	システム仕様書	・システムの基本仕様 ・画面仕様 ・帳票仕様 ・ホストコンピュータとの通信手順 ・他社設備との通信手順等を記述したもの	３	検収時
2	操作マニュアル	・基本的な操作方法 ・トラブルシューティング等を記述したもの	３	検収時

下記の図書類は原則として提出図書には含まない。

No.	名称	概要
1	テーブル・ファイル仕様書	DB や内部使用のファイルレイアウト等
2	プログラム仕様書	個別プログラムの詳細設計書
3	自社設備とのインタフェイス仕様書	自社搬送設備との通信仕様書
4	ソースプログラム	
5	その他内部文書	

（注記）特にソースプログラムは、非公開を原則とする。

5.2 電子データ

完成図書に関しての電子データは、変更・追加ができない仕様にて提出する。

今後、資源節約の観点からも積極的に推奨し、完成図書の部数を減らすよう努力する。

（例）

ファイルフォーマット	PDF
提出時媒体	CD-R　/　DVD-R
閲覧ソフト	Acrobat リーダ Vxx 以上　　＊4）
閲覧機器	Acrobat リーダ Vxx 以上が動作するパソコン

６．保証

納品した物流情報システムが、「システム仕様書」で規定された仕様・品質に適合することを約束することであり、保証期間内にユーザより不適合が報告された場合はその不適合対応を無償で行うことを意味する。

通常、物流情報システムは、その構成要素としての市販製品（ハードウェアやソフトウェア）と、これらを利用・適用する形のカスタムソフトウェアにより構成される。保証としてはカスタムソフトウェアを主としたシステム保証と、その構成要素である各市販製品に対する製品保証とを分けて定義しておく。

6.1 システム保証の内容

1)保証対象

ベンダが何を保証するのか、その対象範囲・内容を具体的に定義する。

例えば「システム仕様書との合致を保証する」などである。特にベンダが“物流情報システム”という呼称で指す範囲に関して具体的に定義し、保証の対象を明確にしておく。また既存システムに対する増設、改造、リニューアルなどの場合についても、保証対象・範囲の明確化、ユーザからの支給品の取扱いなどに関しても明確にしておく。

2)保証方法

保証すべき事項が発生した際における対応方法を決めておく。

例えば「障害原因の切分けを行い、障害原因となった対象部位の保証内容に従い対策を行う」「障害原因の切分けを行い、運用における回避策の提示を行う」など。

3)保証条件

保証を受けるための条件を定義しておく。

例えば「ユーザがベンダの承諾を得ずに独自にシステムの改変を行った場合は保証範囲外とする」など。ベンダの責によらない例としては「ユーザによるソフトウェアのバージョンアップや追加・削除、改変」「ユーザによるシステム構成の変更」などがある。

4)保証期間

保証を受けることができる期間や開始日を定義しておく。

例えば「納入後 12 ヶ月とする」「リニューアル時の保障期間は新規部分のみ 12 ヶ月とする」「支給品については対象外とする」などである。

なお保証開始日は検収引渡し日とするが、稼働がこれに先立つ場合は稼働日を持って保証開始日とする場合もある。

5)窓口・時間帯

受付窓口、受付時間帯、作業時間帯などを定義する。時間帯としては、平日の 9：00～17：00 が一般的である。

また 24 時間対応などの保証を実施する場合、24 時間対応がコールを受付ける体制を指すのか、具体的な保証行為を実施するまでを範囲とするのかを明確にしておく必要がある。

6)保証期間終了後の対応

保証期間を過ぎてから発生した問題、発見された不具合について無償・有償の区分を明確にしておく。原則として保証期間を過ぎたものはすべて有償対応とする。

7)補償について

補償問題を回避するための内容を明確にしておく。

例えば「瑕疵担保責任、債務不履行責任、不法行為責任などの理由を問わず損害賠償その他の責任を問わないものとする」「納期遅れに対する責任は負わないものとする」「操業補償、生産補償に類する責は負わないものとする」など。

6.2 製品保証の内容

製品保証は各製品メーカの保証内容（使用許諾書の範囲による）によって保証するものであり、以下の項目により定義される。これらは製品ごとに異なる為、一覧表などで提出するのがよい。

1)保証対象

以下のような内容を記載しておく。

・分　類 ： 一般名称（プリンタ、PC、データベース、等）
・品　名 ： メーカ品名
・メーカ ： メーカ名
・型　式 ： 型式番号、バージョン
・S/N　 ： メーカのシリアルナンバ

2)保証方法

保証を受けるべき事態が発生した場合、どのように保証を行うかを記載しておく。

・「ソフトウェア不適合を修正したメディアを無償提供する」
・「オンサイト修理またはセンドバック修理」など。

3)保証条件

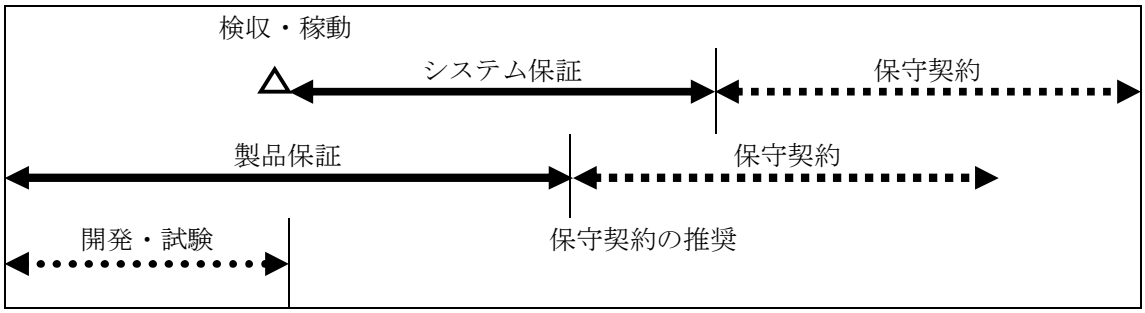
保証を受けるための条件を記述する。

たとえば「ソフトウェア不適合あるいはハードウェア瑕疵が製品メーカの責によらない場合は無償保証を適用しない」など。製品メーカの責によらない原因の例示としては、「ユーザによるソフトウェアの改変・追加が原因」「ユーザによるハードウェアの修理・改変が原因」「設置環境面が原因」「地震、火災、落雷などの不可抗力が原因」などがある。

4)保証期間

保証を受けることができる期日を定義する。

開発などのため機材を事前に購入することがあるが、保証開始日は製品メーカからベンダへ納品された時点となることを明記しておく。（検収や稼働日ではない）



製品の機能として累積稼動時間・累積稼動回数を保持できるものについては、その内容を保証期間とすることも可能である。またはその双方の何れか短いほうをその期間とする場合もある。なお、累積稼働時間・累積稼動回数をその期間とする場合はその測定方法を明確にしておく。

・保証開始日：製品の無償保証開始日
・保 証 期 間：期間または累積稼働時間・累積稼動回数
・保証終了日：製品の無償保証終了日

また、既存システムに対する移設、オーバーホールなどの場合も保証期間を明確化しておく必要がある。例えば「移設した製品についての保証は行わない」などである。またユーザからの支給品については保証の対象から外すようにする。

5)窓口・時間帯

連絡先窓口がベンダであるのか製品メーカであるのか､また時間帯などを明記しておく。

・対応曜日・時間帯
・連絡方法
・連絡先

6)保証期間終了後の対応

保証期間を過ぎた製品の問題について無償・有償の区分を明記しておく。
たとえば「無償・有償の区分は各製品の保証内容による」など。

7)補償について

補償問題を回避するための内容を明確にしておく。
例えば「瑕疵担保責任、債務不履行責任、不法行為責任などの理由を問わず損害賠償その他の責任を問わないものとする」「納期遅れに対する責任は負わないものとする」「操業補償、生産補償に類する責は負わないものとする」などとする。

7．保守

7.1 保守

本書で述べる保守とは、物流情報システムを安定的な稼働状態に保つこと、またはその状態に修復する業務である。保守は日々の運用の中でユーザが行うものであるが、ユーザ独自で保守を行えない場合、ベンダ、２次ベンダまたは第三者と保守契約を締結し保守業務の一部もしくは全てを委託することになる。保守業務を受託するものはユーザの抱える問題に対し、より満足のゆく保守サービスを提案して行く必要がある。従って、委託範囲とサービス内容については、システム納入前に打合せを行っておくことが望ましい。

1)保守の形態

(1)物流情報システムの保守

①定義

・システムの保守とは、製品間にまたがる問題を取り扱う保守である。

②ユーザと保守受託者の相互の責務

・システム上の障害原因の切り分け、組合せに関わる問題の解決など。

・保守受託者は技術継承と技術者の確保。

・必要な保守部品の維持や交換、場合によってはユーザに対してソフトウェアのバージョンアップ、部分更新、一括更新などの提案を行う。

③委託形態

・ユーザ自身で保守

・物流情報システムベンダへ委託

・２次ベンダ，第三者へ一括または部分委託

(2)製品の保守（コンポーネントの保守）

①定義

製品の保守（コンポーネントの保守）とは、システムを構成している個々のハードウェアおよびソフトウェア製品（コンポーネント）に対する保守である。

②製品（コンポーネント）の保守条件の整理

種々のハードウェア､ソフトウェアは製品ベンダが異なっており､製品ベンダごと、製品ごとに保守、保証内容、そしてその対応を受ける条件を導入前に検討・整理しておく必要がある。

・保守条件：製品の保守を受けるための条件有無の確認。

・動作環境：ハードウェアにおいては環境条件(温度、湿度、塵埃、腐食性ガス等)が多い。ただし、オフィスユースでは、明確な数値が出ていないことも多い。

ソフトウェアにおいては、ハードウェアが正常に動作している、およびハードウェアの動作環境を満たしている。当該ソフトウェアが動作できるソフトウェア環境（OS など）が満たされている等がある。

・責任範囲：各製品（コンポーネント）の保守責任の範囲を把握する。例えば、ソフトウェアにおいては、バグの修正をする・しない、保守の問い合わ

せに応じる・応じない、等がある。

・現地引取：保守を受けるために、現地へのサービス技術者の派遣をしてもらえるのか、製品を製品ベンダへ送り返して修理をうけるのか、送り返し時に代替えが用意されているか等がある。

③委託形態

・ユーザ自身で保守（修理は製品ベンダへ依頼）

・個々の製品の保守をそれぞれの製品ベンダへ委託

・個々の製品の保守を第三者へ一括または部分委託

以上のように、オープンな製品は、保守条件を考慮しつつ、どのように安定して使うのかが求められる。

2)保守契約の締結

保守を円滑に行うためには普段からの協力関係、事前の準備を計っておく必要がある。このことを保守契約として取決め、各関係者の役割を明確にし、不都合の事前防止を図る必要がある。また、保守契約を行う場合と、行わない場合のリスク想定も重要である。

①保守契約（役割の明確化）の効果

・有償であること

・費用対効果により選択された保守業務

保守契約を行っているユーザでは、あらかじめ不具合情報は通知され対策を講じることができる。対策には、コンピュータ製品そのもののバージョンアップによる方法の他、運用で回避するために使用方法を制限する方法なども含まれ、保守契約を行うことによって、これらの選択枝を検討しておくことが可能となる。

②保守契約を行わない場合のリスク

・突然のコールにおいては、復旧の長期化ばかりでなく、対応できない、事態の悪化を招く。

・市販ソフトウェアにおいては、年間保守契約を結んでいない場合バージョンアップの権利がない、問い合わせに対応してもらえない事がある。

・原則として不具合情報は通知されないため、事前に対策も講じることができないまま不具合に直面する場合がある。

・物流システムベンダは納入システムのコンピュータ製品の技術継承やバグ情報・互換性などを常に管理していない。従って、ユーザから問合せを受けても、必ずしも的確な回答が出来ない。

3)保守の期間

製品ベンダによる保守が可能な期間を保守期間といい、保守期間が終了する期日を保守期限または保守限界と言う。保守期限後は製品ベンダによる保守支援、定期点検、障害対応、品質予防対策などが停止される。システムを構成する製品の保守期限を超えてシステムの保守を行う場合、その製品に対する特別な対応が必要となる。

①システムの保守期間

システム保守期間とは、従来は物流設備の保守期間と同じと考えられてきたが、ハードウェア、ソフトウェアが短命であり個々の製品により異なることから、一律の期間

を定めることは困難になっている。保守契約によって継続的に保守をすることにより、個々のハードウェアの交換、ソフトウェアのバージョンアップを続けることでシステムの保守が可能となり、この部分的な対応が可能な期間をシステムの保守期間とする。

②ハードウェア製品の保守期間

故障修理、オーバーホールなどに対応できる期間が保守期間である。

・標準製品に対しては製品毎に期間が定められる。

・カスタム製品はユーザ個別に製作された製品であるので、保証期間後の保守については個別にその期間および必要な措置を確認する必要がある。

保守期限は、部品枯渇、製造設備維持費用、製造設備保守停止対応費用、需要低下、技術者確保難、技術者確保費用などの状況により決定される。

③ソフトウェア製品の保守期間

障害要因調査、不適合修復などに対応出来る期間が保守期間である。

・は製品毎に期間が定められる。バージョンアップが行われた場合、旧バージョンの保守が停止となり、新バージョンで保守対応となることがある。

・カスタム製品はユーザ個別に製作された製品であるので、保証期間後の保守については個別にその期間および必要な措置を確認する必要がある。ソフトウェアは劣化しないので保守期限後も使用継続できるが、障害対応で支障をきたすことがあるので注意が必要である。

保守期限は、技術者確保難、技術者確保費用、開発設備維持費用、開発設備保守停止、開発設備保守停止対応費用、需要低下などの状況により決定される。保守期間を延長するには増加する費用が加算されることになる。

7.2 保守業務

保守業務は、次のような項目に分類され、その内容を表 7-1 に示す。

表7-1　物流情報システムの保守業務の内容

保守業務
1)技術支援
ハードウェア保守支援
ソフトウェア保守支援
2)定期点検
システム定期点検
ハードウェア定期点検
ソフトウェア定期点検
3)障害対応
窓口対応
現地対応
ハードウェアの修復作業
ソフトウェアの修復作業
第三者製ソフトウェアの修復作業
障害対応報告
4)品質予防対策
定期交換部品の推奨
既納品対策
5)特別対応
故障解析と報告
待機
コンサルテーション・教育

1)技術支援

保守支援を委託された者が行う保守支援業務とは、ユーザが行う保守業務を円滑に遂行する為に必要な支援体制を整備し維持することである。

(1)ハードウェア保守支援業務

障害対応待機	待機体制・インフラ
保守部品の維持管理	保守部品の供給確保と健全性の維持、保守部品の代替品や後継品の開発
予防保全活動	納入システムの履歴管理。既納入品対策（他ユーザ発生不良対策の反映）の納品管理
保守技術維持管理	保守技術員の維持、定期保守、障害対応時の後方支援体制

(2)ソフトウェア保守支援業務

障害対応待機	連絡網などの体制
プログラムコードの維持管理	プログラムコードの媒体供給あるいは保管。ハードウェア及びプラットフォームの仕様変更に伴う変更や改良開発。なお、データの維持保管は原則としてユーザが行う。
予防保全活動	納入システムのソフトウェアバージョン履歴管理。既納入品対策（他ユーザ発生不良対策の反映）のための管理
保守技術維持管理	ハードウェア障害、ソフトウェア障害対策の後方支援体制

2)定期点検

定期点検とは、システムの健全性を維持し、障害の要因や徴候を事前に把握・除去し、障害の発生を未然に防止することを目的としている。

(1)システム定期点検

①エラーログ、パフォーマンスパラメータ等を採取することによりシステム異常、ハードウェア劣化、ノイズ増加などの兆候を把握出来、事前の対応が可能となる。

②定期点検の対象、方法

・メモリリークなどに起因するシステム停止
・ソフトウェア実行環境変化によるシステム異常
・通信負荷増大によるシステム異常

(2)ハードウェア定期点検

①ハードウェア健全性の点検、清掃、調整が行われ、必要に応じてオーバーホール・部品交換・環境対策などを行う。

②定期点検の対象、方法

・設置環境（温湿度、塵埃、腐食性ガス、振動など）の影響
・有寿命部品（モニタ、HDD、ファン、ヒューズ、バッテリなど）の劣化
・精度確認と調整
・バックアップ機能の動作確認

③ベンダは製品ごとに定期点検の項目・周期などの推奨基準を提示する。ユーザはシステムの重要度・使用状況・設置環境を考慮して、定期点検の内容を決定する。

④ユーザ独自で実施できない項目について、製品ベンダあるいは第三者へ点検業務を委託する。

⑤点検業務を受託した者は、点検終了時に、調整・修理・交換などの作業内容の報告とともに点検所見をユーザに報告する。

(3)ソフトウェア定期点検

長期間の運転によるデータファイルの肥大化、ハードウェアリソース不足等の原因でソフトウェアの動作スピードが遅くなったりするため、動作環境の最適化を図る意味で、ソフトウェア定期点検は有効である。

①定期点検の項目

・デフラグ（ディスクの最適化）
・不要ファイルの整理

・バージョン管理
・ログファイルの解析

②リモートメンテナンス機能を備えた製品においては、遠隔地にいるソフトウェア製品やカスタムソフトウェアベンダによるソフトウェア定期点検が可能であり活用するとよい。

3)障害対応

(1)保守サービスの体制や費用負担

障害対応とは、障害のすみやかな復旧と再発の防止を行うことであり、そのためには保守サービスの体制や費用負担などをユーザ･保守受託者間であらかじめ決めておく必要がある。

物流情報システムは複数社の製品で構成されていることが多い。

システム障害が発生したとき障害対応保守を請け負った会社はその障害原因の切り分けと修復を行うが、障害の原因が他社製品にあった場合、ハードウェアの故障修理・ソフトウェアの不適合修復など障害原因の除去はその製品ベンダが行うことになる。

(2)障害対応手順

①障害対応は、次の手順で行われる。

・ユーザから所定窓口へ障害連絡
・電話による障害対応
・現地への人員派遣による障害対応（電話対応で解決できない場合）

②障害対応は、窓口対応と現地対応に分けられ、受付窓口、窓口受付時間帯、障害対応時間帯、現地対応までの時間、障害対応に必要な修正費用などは保守契約内容に従うことになる。

(3)窓口対応（オンコール）

窓口対応は、ユーザからの問合せに対して電話、ファックス、電子メールなどで回答する行為であり、障害内容の切分けや対応処置の一次対応を行う。

①質問事項対応

システムの取扱いや操作方法についてのユーザからの問合せに対応する。

②障害の一次切り分け

システムに何らかの障害が生じた場合に電話などで装置ごとに大まかな原因の切り分け、影響範囲の限定化、ユーザミスの有無判定などを行う。

③誤操作対応

操作ミスによる障害について、機器操作の説明、回復処置方法の伝達などの復旧支援及び運用支援を行う。

④ユーザ要望事項対応

システムの使用方法、若しくは運用方法の相談を受けて、現状システム構成内でのユーザ要望の実現支援を行う。

また、リモートメンテナンス機能を備えた製品においては、事前に障害情報を収集し障害原因をより正確に推定することができるため、より早い対応が可能となるので活用するとよい。

(4)現地対応

窓口対応で障害対処出来なかった場合、現地へ要員を派遣し契約内容に従い障害の切り分け作業、修復作業を行う。

①障害の切り分け作業

障害事象の把握を行い、速やかにその要因を究明し、障害発生部位を明らかにし処置方法を決定する。

②修復作業

障害原因の除去・修復や運用方法変更による障害回避を行う。

(5)ハードウェアの修復作業

ハードウェアの修復作業には保守部品が必要になり、その入手時間により修復時間が決まる。保守部品の入手方法は次のとおりであり、障害発生部位の緊急度に合わせて選択する。

①故障した部品が修理されるまで待つ。保守部品を購入し納入されるまで待つ（緊急度小）

②製品メーカと保守部品契約を結んでおき、製品メーカから保守部品を供給（緊急度中）

③ユーザ保有の保守部品を使う（緊急度大）

(6)ソフトウェアの修復作業

①システムの保守を行う者は、システム障害発生時、障害の原因を切り分けその対応を行う。

②保守契約が締結されていない場合、システム構成確認、バージョン確認、プログラムコードの入手、技術者の確保に時間を要し、障害復旧までに時間を要する場合がある。

(7)障害対応報告

①障害対応を行った者は障害事象とその対処内容の報告を行う。

②但し、故障原因の解析などの調査と報告については、基本的に障害対応業務の範囲外である。(注記：7-2 5)「保守業務　特別対応」参照)

(8)障害対応における留意点

①障害原因の直接除去

システムを構成している個々の製品の不適合修正はそれら供給者が行うものである。しかし、個々の不適合はその都度には修正されず、次回の機能拡張バージョンアップにて対応となることがある。また、運用上の回避策が障害対応策として提示されることもある。このように、不適合がその都度修正されず障害原因の直接除去が速やかに行えない場合、次のような処置で障害対応を行う。

・障害原因はそのままとし、運用面で障害を回避

・障害原因はそのままとし、他のソフトウェアの変更などシステムの変更により障害対策を行う。

・次回の機能拡張バージョンアップ版で障害原因を取除く

②ソフトウェア保守契約

製品供給者標準ソフトウェアであっても、ソフトウェア保守契約を継続していないと保守対応を受けられない製品がある。そのような場合、ユーザはその製品供給者

と別途ソフトウェア保守契約を継続しておく必要が生じる。また、ユーザ個別に製作されたカスタムソフトウェアの保証期間後の保守に対しても、別途保守契約を締結し技術者・開発設備・プログラム・各種仕様書などを確保しておくことが、迅速な障害切分けと修復に重要となる。

③カスタムハードウェアの保守部品

カスタムハードウェアはユーザ個別に製作されたものであるため、製品供給者には在庫はなく、また製作には時間を要する。したがって、カスタムハードウェアが故障した場合、その修理を待つかあるいはユーザ保有の保守部品を使用することになる。重要なシステムにおいては、ユーザが前もってカスタムハードウェアの保守部品を購入しておくことが推奨される。

④契約の内容

システムの障害対応保守を契約する場合、下記点を明確にしておく。

＜契約対象＞

・システム範囲、製品範囲

＜契約範囲＞

・ハードウェア故障修理

・ソフトウェア不適合修復に要する個々の費用。

・システムの変更により障害対応を行う場合、その費用。

・障害切分けに他社製品の調査費用が発生する場合、その費用。

⑤費用負担

障害切分け作業、障害修復作業、保守部品取得に対し費用が発生する。これらを都度の費用負担とするか、保守契約でまかなうかの選択がある。また、保守契約有無によりサービスレベルに差がでることがあるので確認が必要である。

4)品質予防対策

品質予防対策とは障害の発生を未然に防止するための情報をユーザに伝える業務である。予防保全に係わる連絡は、保守契約によって登録されたユーザに情報を公開し、ユーザが実施を希望する場合に予防対策を有償で実施することを原則とする。

(1)定期交換品の推奨

有寿命機器・部品について、定期的な交換・オーバーホールをユーザに推奨する。

(2)既納入品対策

通知すべき障害が認知された場合は、ユーザに対してその回避策を推奨する。ユーザはその費用対効果を算出し対策実施要否を判断する。

5)特別対応

保守業務に加え、ユーザより次の様な要請が出た場合の内容・範囲・期間・費用において、ユーザ・保守受託者間で調整を行った上で別途契約し対応する。

(1)故障解析と報告

障害対応を行った者は、保守業務の一環として障害事象とその対処内容とをまとめ障害対応報告を行う。障害対応報告以外にユーザが故障原因の解析・究明を必要とする場合、下記の事項を認識したうえで、その内容・範囲・期間・費用を保守受託者と製

品供給者間で協議し別途の業務として契約する。

①故障部品の特定化コスト

故障ユニットを特定化し交換した後、故障ユニットは修理されることなく破棄される。よって故障部品の特定化には別途技術者を確保するコストが発生する。また、非定常業務のため必要工数の見積りが難しい場合、出来高払いとするのが双方にとって安全である。

②部品の故障解析

故障部品の故障原因解析は部品供給者に依頼することになる。部品供給者は故障原因解析の可能性・費用・期間を見積ることができないので故障部品が特定化できた段階で、その後の費用・期間を見積り、後工程の契約を行うのがよい。

③故障解析の効果

部品の故障解析から得られるものがユーザの期待を満たせない場合がある。例えば、故障原因が偶発故障（初期故障期間を過ぎ摩耗故障期間に至る以前の時期に偶発的に起こる故障）であった場合、とるべき対策はあまりなく、ユーザは費やした費用に見合った成果を得ることができない。従って、ユーザは費用対効果を十分検討したうえで、製品供給者に故障解析業務を委託する必要がある。

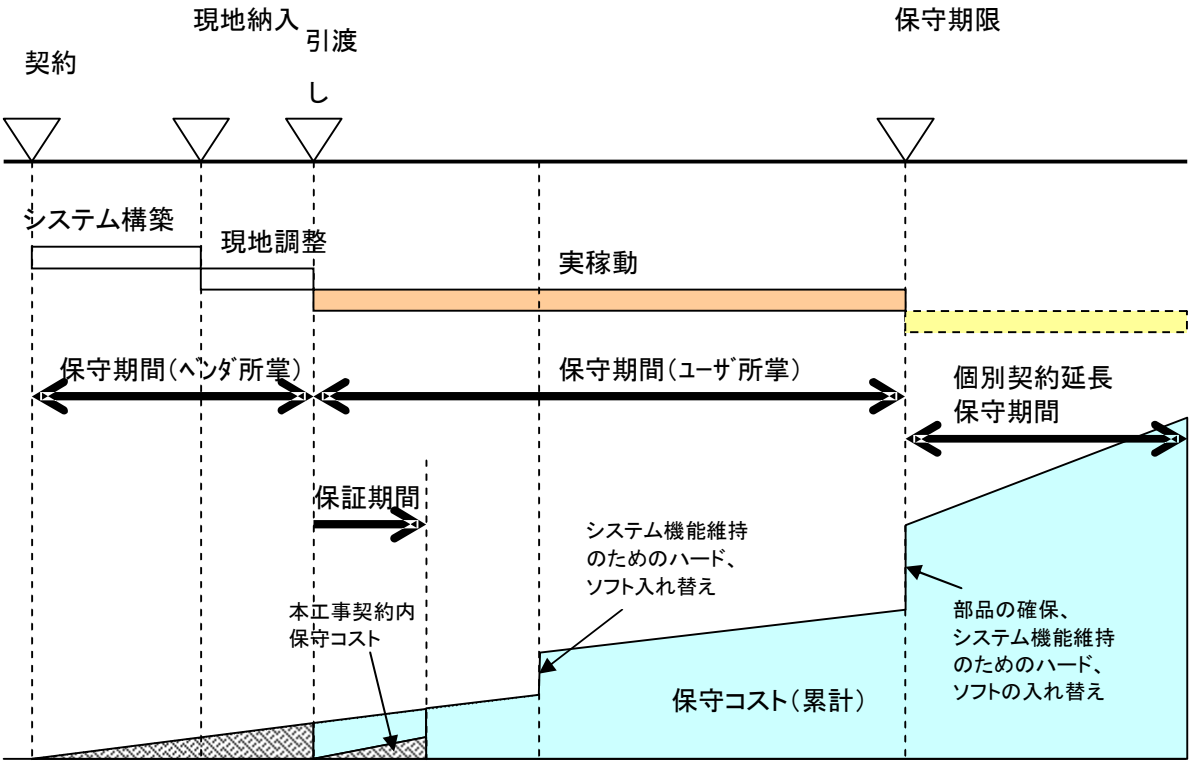
7.3 ライフサイクル管理

物流情報システムを構成する各製品の改廃サイクルと、ユーザが期待するシステム運用期間とが相容れない場合、このライフサイクル管理に必要な事項の説明を行うが、これらのライフサイクル管理には技術力と労力が必要となる。ユーザがライフサイクル管理を行えない場合、ライフサイクル管理のコンサルティング、支援あるいは管理そのものをシステム供給者または第三者へ委託するとよい。

1)システムのライフサイクル

物流情報システムのライフサイクルの例を図 7-1 に示す。

図7-1 物流情報システムの保守期限の例



2)ハードウェア保守部品

物流情報システムは、システムベンダを含む複数社のハードウェア製品で構成されていることが多く、またコンピュータハードウェアの製品寿命は短い。したがってユーザは、誰が、どの保守部品を、どの位の期間、どのような意図で用意しているか把握したうえで保守計画を行う必要がある。

(1)保守部品の確保

①有寿命品

通常使用期間中に劣化故障期間（故障率が急激に増大する期間）に到達するもの。たとえば、ヒューズ、二次電池、電解コンデンサ、モニタなど、機器構品およびこれらより構成されるユニットである。ユニットの例としてはモニタ、ファン、HDD、

電源などがある。重要度の高いシステムにおいては、定期交換あるいはオーバーホールなどの予防保全が必要になる。

②長寿命品

偶発故障期間（故障率がほぼ一定と見なせる期間）が長く、通常使用期間中には劣化故障期間には到達しないもの。たとえば、有寿命部品をもたないプリント基板などであり、偶発故障に対し事後保全で対応するのが一般的である。

③消耗品

システムの運用により消費されるプリンタ用紙、記録紙、トナー、インク、一次電池などである。製品ベンダは、製品ごとに定める保守対応期間に必要とされる保守部品を必要数量保有し、その製品の保守（故障修理）に対応している。一方、ユーザ個別に作成されたカスタム製品の保守部品確保については、ユーザは保守受託者と個別に協議する必要がある。

(2)保守対応期間の把握

ユーザはシステムを構成している製品ごとの販売停止時期および保守対応期間を把握する必要があり、保守受託者はそれらの情報をユーザに提供する必要がある。しかしユーザがこれらの情報を的確に把握するためには、下記のような問題に対処しておく必要がある。

①製品ベンダの通知

製品ベンダからの販売停止情報、保守対応期間情報は正確さを期すため、型式による通知となる。ユーザは当該型式の製品がシステムで使用されているか確認する必要がある。また、ユーザは、これら情報の深刻度を検討し、保守停止にそなえた保守部品事前購入の必要性を決定する必要がある。

②エンドユーザとしての製品ベンダ情報の入手方法

コンピュータなど汎用製品においては、製品ベンダはエンドユーザの全て把握することはできない。また、産業用機器であっても、多様な販売ルートにより広く販売されている場合も同様である。

従って、製品ベンダから各ユーザへ情報を個別に通知しようとしても、それらが全てのエンドユーザへ届くとは限らない。また、コンピュータなどの汎用製品においては、ユーザへの個別通知はなく「完売をもって販売停止」「販売停止後保守○年」などを原則とし、製品ごとの情報を提供していない場合が多い。ユーザが製品ベンダ情報を的確に入手するには以下の様な方法がある。

・ユーザが製品ベンダに適宜問合せを行う
・製品ベンダ情報が的確に入手できるように製品ベンダと契約を締結する
・ユーザが第三者と保守契約を締結し、製品ベンダ情報入手業務を委託

③情報の忘却や散逸可能性への対応

産業用機器においては、製品ベンダは十分な猶予期間をもって保守対応終了情報をユーザに通知することが多い。しかし、通知した情報が下記理由によりユーザ側で散逸・忘却されてしまうことがある。

・通知した情報がユーザ側の適切な部署へ伝わらない
・猶予期間が長いため、その間に情報が忘却されてしまう
・猶予期間が長いため、その間のユーザ側人事異動などにより情報が散逸する

ユーザがこれらの問題に対応できない場合、製品ベンダあるいは第三者と契約を締結しこれらの問題対処を委託するとよい。また製品ベンダは、販売停止予定・状況、保守停止予定・状況などの情報をWEB 公開、定期通知することなどにより、ユーザにもれなく情報が伝わるよう努力をする必要がある。

(3)ユニット交換における保守部品の仕様

①代替品、後継品を適用する際にはインタフェイスの互換性をソフトウェアで対応する場合が多く、ソフトウェアのバージョンアップなどを伴うこともある。また、あるソフトウェアをバージョンアップするためには、他のソフトウェアのバージョンアップも必要になることがある。

②生産中止に対するユーザ・保守受託者間の情報交換（生産中止連絡・需要調査など）を密にして同一品確保か代替品・後継品の採用かの判定を行う。

ユニット交換で保守を行う保守部品は仕様上次のように分類される。

・同一品･･･納入品と全く同一仕様・同一型式

・代替品･･･仕様はほぼ同一であるが型式名が異なる

・後継品･･･機能的に同一仕様とみなされるが形状や性能・容量・インタフェイスの同等性保証がない

製品ベンダは部品供給の停止に備えて、同一品の確保や代替品、後継品の開発・維持に努める必要がある。代替品、後継品を適用する際にはインタフェイスの互換性をソフトウェアで対応する場合が多く、ソフトウェアのバージョンアップなどを伴うこともある。また、あるソフトウェアをバージョンアップするためには、他のソフトウェアのバージョンアップも必要になることがある。

保守費用の適正化をユーザ独自で行えない場合、第三者と保守契約を締結し、その業務の一部あるいは全てを委託するとよい。

3) ソフトウェアバージョンアップの対応

物流情報システムは、複数のソフトウェア製品で構成されている。ソフトウェア製品は各々にバージョンアップ版がリリースされ、旧バージョンのソフトウェアは販売中止、保守が停止となるが、継続使用は可能である。旧バージョンソフトウェアを継続使用するかバージョンアップを適宜行って行くかの判断、および第三者に保守を委託する場合などの費用対効果を検討する必要がある。

(1) ソフトウェア品質予防対策情報

①システムの保守には各社ソフトウェア製品の品質予防対策情報を入手する。

②各ベンダからその情報を入手し、システムへの影響度を検討したうえでバージョンアップを行うか否かの判断を行う。

③保守停止となった旧バージョンのソフトウェアに対する品質予防対策情報は入手困難となる。

(2) ソフトウェアのバージョンアップ

①システム中のあるソフトウェアをバージョンアップする場合、他のソフトウェアのバージョンアップやハードウェアの変更が必要になることがある。

②必要なバージョンアップ範囲の検討およびその検証・実施には時間と費用がかかることがある。

(3) 旧バージョンソフトウェアの継続使用

①新バージョンのソフトウェアがリリースされると、旧バージョンの技術支援や不適合修正などの保守は停止され、関係した障害の原因究明や対策が困難になる。

②ハードウェア保守部品として、旧バージョンソフトウェアに適合した「同一品」を確保しておく必要がある。ハードウェアが故障し「代替品」「後継品」を使用することになると、ソフトウェアもバージョンアップを余儀なくされることがある。

4) ハードウェア製造中止時の対応

ハードウェア製造中止の対応には大きく分けて３つの方法があり、その選択はユーザ判断となる。

(1) システム凍結形

システム構成およびバージョンを凍結し、予め確保した「同一品」で保守を行う方法

①システムの運用期間が短い場合、増改造をしない場合などに有効である。

②但し、ソフトウェアバージョンアップに伴いハードウェアのバージョンアップが余儀なくされ、事前購入した「同一品」が無駄になることがある。

③また、保守停止となったハードウェア・ソフトウェアを使用し続けることになり、障害発生時に製品供給者から技術支援を受けられない可能性がある。

(2) 発展追従型

システムのバージョンアップを継続し、最新のハードウェア、ソフトウェアで保守を行う方法

①システムの運用期間が長い場合に有効である。

②ハードウェア、ソフトウェアのバージョンアップ費用を保守費用として継続確保する必要がある。

(3) 一括更新

システムの構成およびバージョンを凍結し、保守に耐えきれなくなった時点でハードウェアおよびソフトウェアを一括更新する方法

①ハードウェア､ソフトウェアともに最新バージョンまでの乖離が生ずることがあり、ソフトウェア資産継承の検討と検証が必要となる場合がある。
例えば、データ変換はバージョンごとに順次段階をふんで実施する等である。

②したがって、一括更新には費用と時間が多く必要となり得るので、その時期設定および予算取得を計画的に行う必要がある。

5) 増設・改造対応

年数を経たシステムの増設・改造を行う場合、部品調達で支障をきたすことがある。また、システム構築時の技術情報を収集しきれないこともある。

(1) ハードウェア

製品ベンダに、同一品、代替品、後継品に関する販売期間終了後の対応方針などを確認し、システム構成を評価するとよい。

(2) ソフトウェア

①増設を行う場合、既設と同一バージョンのソフトウェアが必要となる場合がある。

②新バージョン発売にともない旧バージョンのソフトウェアは販売停止となっている

ことがある。

③ユーザはソフトウェアの改廃情報を的確に入手し、適切な時期に事前の策を講じておくことが望ましい。ユーザでの対応が難しい場合、これらを保守業務として外部委託するとよい。

(3)履歴管理

①増設・改造を行った場合、その結果を図面・仕様書・完成図書などに反映し、最新の形態を各種仕様書に残し管理しておく必要がある。

②これらはユーザ所掌であるが、ユーザにその余力が無い場合、これらを保守業務として外部委託するとよい。

(4)技術情報

システムの増設・改造には、既設部分の技術内容に熟知した技術者が必要になるが、世代交代・人事異動などにより、システム構築を行った技術者を増設・改造時に確保できる保証はない。

ユーザの対応策として以下の様なものがある。

①保守業務を外部委託し、そのなかで技術者を育成する。(人による技術の伝承)

②システム構築における技術情報の資料化をシステムベンダに発注する。(資料による技術の伝承)

(5)増設・改造の影響

ある部分の変更がネットワーク上の別システムに問題を発生させることがある。

①増設・改造に際し、問題発生の範囲・深刻度を広い範囲で事前評価し、必要な体制構築などの策を講じておく。

②事前評価の対象範囲はシステムベンダの範囲を超えて行う必要がある。

③事前評価の取りまとめはユーザ所掌となる。

6)保守期間満了後の保守

保守期間満了後もシステムを継続使用する場合、ユーザによる保守部品の確保、保守技術の確保などが必須となる。ユーザーは、システムベンダあるいは製品ベンダとできるだけ早い段階から協議を行い、以下のような方法で保守部品確保を行う。

①ユーザの保有する相当品を保守部品とする。

②更新または撤去した自社システムから保守部品取りを行う。

③他ユーザが更新または撤去・遊休化したシステムから保守部品取りを行う。

④同一品を製作する。

枯渇した部品を入手可能な部品で置き換えるべく設計変更を製品ベンダに依頼する。ただし、再設計品の価格がユーザの期待に合わない、また技術的に不可能な場合も多い。

⑤ユーザが上記のような保守部品確保を独力で行えない場合、その業務の一部または全てを第三者に委託する。

８．セキュリティ対策

8.1 セキュリティの定義とガイドラインの目的

1)セキュリティの定義

本ガイドラインのセキュリティとは、物流情報システム内のデータおよびプログラムリソースを適切に管理し、機密を守る為の考え方、対策案のことである。これらをフェーズごとの物流情報システムに関する「セキュリティの対象」と「リスク」として詳細を示す。

2)セキュリティガイドラインの目的

物流機器ベンダが共通にセキュリティ上のリスクを認識し、ユーザと協力して適切なセキュリティ対策を講じることができることである。

3)その他特記事項

ユーザからの具体的な情報セキュリティポリシーによる追加要請があればベンダはそれに従う。ただし、この要請を実現するために物流情報システムに新たな費用が発生する場合は、応分の有償対応とする。

ユーザとベンダとの間で秘密保持契約を締結し、事前にベンダの対応するべき事項と責任範囲を明確にすることを推奨する。

また、納入する物流情報システムにどの程度のリスクを想定し対策を講じるかを、ユーザ・ベンダ互いにその考え方を明示し合意することが望まれる。

重要なことは、各業務フェーズにおけるリスクを認識し、物流機器ベンダとして適正な対策を講じることである。但し、個々のシステムや環境の特性、価格ユーザのセキュリティポリシー、など条件は様々であり、それぞれで対策方法が異なる。リスクのレベルによって、ユーザとの間で、事前に制約条件、責任範囲を明確にすることが大切といえる。

8.2 セキュリティの対象

セキュリティの対象については、下記の 2 点に大別される。

1)物流情報システムが扱うデータ

電子ファイル、印刷物など、ベンダがユーザ側から提供される情報（商品、売上、受発注データ、搬送実績、社員マスタなど従業員の個人情報に関するデータなど）

2)情報システム資源

物流情報システムのアプリケーションソフト、データベース定義やシステムパラメータなどベンダがユーザの要求を満たすために設計、構築したもの

8.3 各業務フェーズと考え方

業務フェーズは、提案から廃棄まで下記の 1)～5)までに分かれる。

1)提案フェーズ

ユーザより要件を確認しベンダがシステム提案を行う

2)開発フェーズ

ユーザとの契約時点からベンダがシステム要件をまとめ、システムを開発する

3)納入フェーズ

開発したシステムをユーザに持ち込みテストを行い引き渡す

4)運用フェーズ

ユーザへの納入後に、システムの運用・保守を行う

5)廃棄フェーズ

システムの稼働終息や更新によってシステムの廃棄を行う

8.4 各業務フェーズで発生するリスクについての考え方

1)提案フェーズで発生するリスクについての考え方

ユーザより検証のために預かったデータを意図しない目的に使用され、そのことによるプライバシーの侵害など、ユーザへの損害を防がなければならない。

また、ベンダとしても、社会的信頼の損失や金銭的な損失になる恐れがあるため、組織的な取り組みとして、その流出をくい止めなければならない。

提案フェーズではユーザの計画、要求仕様、分析用データを元に、ベンダから提案仕様や分析したデータが発生する。これらのドキュメントやデータを漏洩させないようにするためには組織的に基本的な考え方（情報セキュリティポリシー）を定め周知、遂行させる必要がある。

リスクの内容としては、下記の項目が考えられる。

(1)データ受け渡し時の漏洩、紛失

①Ｅ－ｍａｉｌによる情報漏洩

②媒体送付による紛失／情報漏洩

(2)ベンダ内で検証時の漏洩、紛失

①外部からの不正アクセス

②内部の不正アクセス

③外部から感染したウイルスなどによる漏洩

④預かった媒体の盗難

⑤預かった媒体のコピーの盗難

⑥媒体内データを印刷した紙の流出

(3)検証が終了した媒体からの流出

①不要となった媒体からの情報流出

ベンダで作成した提案書には、ユーザの営業上の重要事項が含まれている。

また、ベンダの著作権保護やコンプライアンスの観点から、双方での流出・流用の防止に努めるものとする。

2)開発フェーズで発生するリスクについての考え方

システム開発においては、多くの異なる組織の要員が関わり、情報の連携が必要となるため、それに伴うリスクが発生する。

開発フェーズでは、「仕様の確定」「ソフトウェア開発」「テスト」等の成果物やユーザから提供されたデータ等がセキュリティの対象となる。

これらのドキュメントやデータを漏洩させないためには、予め当該業務のセキュリティ

ポリシーを、この業務に携わる全ての要員に対し、適切な手段で周知させる。
リスクの内容としては、下記の項目が考えられる。
(1)仕様の確定段階での仕様ドキュメントの授受における漏洩、紛失
①Ｅ－ｍａｉｌによる情報漏洩
②媒体送付による紛失／情報漏洩
(2)ソフトウェア開発段階で開発作業域内での情報漏洩
①取り外し可能な電子媒体からの漏洩
②ネットワークを経由した不正アクセスによる情報漏洩
③開発作業域への不正侵入による盗難
(3)テスト段階での情報漏洩
①ソフトウェア開発段階と同様
ベンダはユーザからの要求があれば、上記対応策の実施項目について説明する。

3)納入フェーズで発生するリスクについての考え方
ベンダの開発場所を出て、セキュリティ対策のとり難い状態が予想される工事中の現地に、設置・運転される。
納入フェーズでは、納入する機器、システム、ドキュメント、テスト等のアウトプットがセキュリティの対象となる。
これらを漏洩・紛失させないために、ユーザの管理下で運用が開始されるまでの間、ベンダは安全・防犯などに特別な配慮が必要である。
リスクの内容としては下記の通りである
(1)開発場所から納入場所への輸送・設置で一時管理下を離れる
①運搬途中での紛失、盗難
②納入場所での受け入れ時の紛失、盗難
(2)納入時点でユーザ、ベンダ以外の不特定多数の関係者が入場する場合
①夜間、休日などユーザ、ベンダ不在時、環境への不正立ち入りによる盗難
②ネットワークへの不正アクセス
ユーザの指示がある場合は、その指示に従う。

4)運用フェーズで発生するリスクについての考え方
運用フェーズとはユーザへの納入が終わり、システムの運用を行い、廃棄されるまでの期間を指す。システムが稼働しているのでその稼働しているシステムからデータ流出、バックアップからの流出、ドキュメントの流出、保守関連の流出が考えられる。
特にシステムが稼働状況にあり、外部との接続されている可能性が高いため、情報の流出の可能性が高くなる。運用はユーザの管理下で行われるため、ユーザサイドでシステムと繋がる他のシステムやシステムを操作する人など多くの流出の可能性がある。
その為、ユーザ側にて情報が流出しないような運用手順を明確にしておく必要がある。システムを操作する人間を制限することやデータを安易に触らないようにするなどが必要である。ユーザが悪意をもってシステムに障害を与えないことを前提とするが、ユーザサイドでも検討が必要である。それらは、原則としてユーザの善管注意義務の範疇とし教育などで対応をして頂く。

5)廃棄フェーズで発生するリスクについての考え方

廃棄フェーズでは以下の廃棄・返却などを想定して対応をとるものとする。

(1)システムが稼働停止して、関連機器を廃棄･返却する

(2)部分的にシステムを更新し廃棄する

(3)故障した機器を廃棄・返却する。

電子情報の廃棄に関しては特にユーザが管理していただく事項となるが廃棄に伴う危険としては、廃棄・返却時に稼働していたシステムから電子データの流出、ドキュメントの流出が考えられる。

8.5 ウイルス対策の考え方

物流設備に付帯する情報システムは、それを構成する機器の大半がオープン系に属するためコンピュータウイルス（以下、ウイルスとする）に侵される可能性があり、ベンダ各社も供給者として「コンピュータウイルス対策基準」平成 12 年 12 月 28 日（通商産業省告示　第 952 号）（以下、『対策基準』とする)に準じた対策を講じる必要性がある。しかしながら、ウイルス対策をより確かなものにするには間断の無い対応が必要不可欠であり、そのためには、ユーザの理解と協力を得ることが重要である。

1)対策規準

(1)ベンダは、ウイルスに感染していないシステムを納入するために『対策基準』に準じた供給者としての活動を実践する。

(2)納入後のシステムは、ユーザの責任でウイルスに感染しないように、『対策基準』の該当事項に準じた対応を実施する。

2)ウイルス対策ソフトの扱いにいて

ウイルス対策ソフトは、次のような理由からシステム納入時には、原則として組み込まないものとする。

・納入アプリケーションのレスポンスに影響する場合がある。

・定期的に定義の更新が必要となり、その際外部システムとの接触による感染が考えられる。

・ウイルス対策ソフト自体のバグによりシステムに重大な影響を与える可能性がある。

3)有償対応

ユーザから「ウイルス対策ソフトを組み込んで納入してほしい」との要望がある場合は、個別に検討を加え、前述のリスクについてユーザに理解してもらったうえで対応の可否を決定する。ただし、ウイルス対策ソフトを組み込んで納入するための、動作確認を含む作業等については、有償とする。

なお、稼働後、納入システムに対するウイルス対策作業が必要となりユーザから対応の要請があった場合は、保守契約締結の有無にかかわらず、有償での対応とする。

8.6 ウイルス対策の実施

1)納入前

(1)ウイルスチェックの実施について

ベンダは、ユーザへ納入する際にウイルスを持ち込むことを防止する目的で、自社の開発場所の出荷時にウイルスチェックを実施し、その時点で入手可能な最新情報により納入システムがウイルスに感染していないことを確認する。また、現地調整中に外部で開発されたソフトの持ち込み等、様々なケースにより再度ウイルス感染が無いことを確認するために現地調整完了時の確認を推奨するものである。

(2)システム開発中のベンダの注意事項

ベンダは、『対策基準』の 6 項（ソフトウェア供給者基準）に準じる環境を整備することに最大限の注意をする。特に開発中システムとインターネット等の外部ネットワークとの接続を排除、また、電子メールの送受信システムと切り離す等、ウイルス感染の可能性を最小限にした環境での開発を実施する。

(3)現地調整中のベンダの注意事項

ベンダは、現地調整中のウイルス感染の可能性排除に対して注意をする。ウイルスチェック確認対象となっている納入用コンピュータハード以外に、調整時に持ち込むパソコン、媒体（FD、CD、USB メモリー等）も全てウイルスチェックの対象とし、感染が無いことをベンダの管理者が確認し使用すること。可能な限り、確認書で持ち込み分も管理することが望ましい。また、連動するユーザシステムについても確認の協力を依頼すること。

2)納入後（稼働後）

納入後のウイルス対策は総合的に各ユーザにて実施されるべきものと認識する。ここでいうウイルス対策とはウイルス対策ソフトの導入やバージョンの更新のみを指すのではなく、システムの運用管理から使用者の教育等様々なものを指す。詳細は、『対策基準』の 4 項（システムユーザ基準)、5 項（システム管理者基準）を参照のこと。

(1)既納ソフトウェア改造及びハードウェアの増設

開発環境、持ち込む媒体・パソコン、増設するハードウェアについては、8-6 1)の納入前の注意事項と同様とする。

(2)リモートモニタリング・メンテナンス時

ベンダの事務所より、ユーザへの納入システムに公衆回線等を利用し、リモートモニタリング･メンテナンスを行う場合には､開発中と同等のウイルス対策を行っているパソコンより行う。

8.7 ウイルス対策ソフトのインストール条件

基本的に納入システムにはウイルス対策ソフトをインストールしないこととするが、ユーザからの要望があり、かつユーザとベンダとの間で以下の項目に関して協議・合意を得て、ウイルス対策ソフトのインストールを行うこととする。

1)ベンダの責任

ウイルス対策ソフトをインストールしても、ウイルスに感染しないことを保証するもの

ではない。また、ウイルス対策ソフト及びその更新が原因で納入システムに何らかの障害が発生してもベンダの責任範囲外とする。

2)ウイルス対策ソフトの選定
ベンダ推奨のウイルス対策ソフトが望ましい。

3)ウイルス対策ソフトの購入
ライセンスの更新やサポートを考えた場合、ユーザが購入することが望ましい。

4)インストール作業
ウイルス対策ソフトをインストールしても問題がないか確認する必要があるの で､ベンダが作業することが望ましい。作業範囲は下記とする。
(1)システムの事前バックアップ
(2)ウイルス対策ソフトのインストール
場合によってはOSのサービスパックのバージョンアップを含む
(3)ウイルス対策ソフトの動作設定
(4)システムの動作確認
なお、動作確認で問題が発生すれば、システムを元に戻す。
また、ユーザがウイルス対策ソフトのインストールを行う（行った）場合、
ベンダとしてシステムの保証はできない。

5)ウイルス対策ソフトの更新
検索エンジンとパターンファイルの更新は、ユーザの保守・点検の一環と位置づけ、それらに関するルールを決定する。どのような更新方法(自動更新/手動更新)でどこが(ベンダ/ユーザ）行うかを決める。

8.8 ユーザの環境・運用に関する要望および感染時の対応
1)使用環境に対する要望
ネットワークの構築にあたり、納入システムのネットワークは独立したものとする。
※外部環境と直接接続されない環境での稼働（物理的切断や、ファイアーウォールの導入など）を推奨

2)運用に対する要望
(1)納入後のシステムは、ユーザにてシステム管理者を立て管理する。
(2)原則として、納入ソフト以外のソフトはインストールしない。
(3)納入システムに、メールソフトをインストールしメールをしない。
(4)納入システムにて、インターネットブラウザを起動させ、インターネット
を閲覧しない。
(5)納入システムとベンダ納入外のシステムとの間に、お互いの取り決めなく
共有フォルダを設定しない。
(6)ベンダ納入外の機器を、納入システムのLANに接続しない。

(7)データ交換時に使用する媒体（CD、USB メモリ等）は、
ウイルスチェックされたものを使用すること。

3)感染時の対応
ユーザから、対応要請（原因調査・ウイルス駆除・システム復旧等）があった場合は、速やかに対応する。

8.9 ウィルス対策のまとめ
ウイルス感染に対する保証は、ベンダが開発納入するアプリケーションソフト、OS、購入パッケージにおける瑕疵担保責任とは違った扱いとなる。ベンダはウイルス感染の有無に関して完全な確証が取れないこと、また、将来においてウイルス感染の回避を保証できないからである。また、システム引渡後はウイルス感染のリスク回避責任主体は、ユーザ（システム使用者）になりベンダの責任範囲とはならないからである。
よってウイルス対応に関しては、「8.6.ウイルス対策の実施」に則った作業手順で納入することを責務とするが、その結果については保証、責任を負うものではない。そのためには、その旨ユーザに説明し、基本契約書や覚書等でこれらを記述することが望ましい。
当然ではあるが納入後のウイルス感染による損害賠償は免責される。

リンク

ウイルス対策に関連する最新情報、用語、法律、ガイドラインについては、以下の URL から参照のこと。

独立行政法人　情報処理推進機構：コンピュータウイルス用語集
http://www.ipa.go.jp/security/virus/beginner/dic/dic_top.html

日本マイクロソフト株式会社：セキュリティ用語集
http://www.microsoft.com/japan/security/glossary.mspx

株式会社シマンテック：用語解説
http://www.symantec.com/region/jp/avcenter/refa.html

トレンドマイクロ株式会社：用語集
http://jp.trendmicro.com/jp/threat/glossary/index.html

マカフィー株式会社：ウイルス用語集
http://www.mcafee.com/japan/security/glossary.asp

経済産業省：コンピュータウイルス対策基準
http://www.meti.go.jp/policy/netsecurity/CvirusCMG.htm

経済産業省：情報セキュリティに関する法律、ガイドライン等
http://www.meti.go.jp/policy/netsecurity/law_guidelines.htm

付録　1

《　セキュリティにおけるリスクと主な対策事例　》

No	リスク	運用面の対策事例	技術的な対策事例
1)基本的事項			
a. モラル			
	リスクの存在に対する認識		
1	認識不足によるリスクの増加	情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰに沿った教育	
2	管理命令系統の異なる複数の組織	社内規定等による統制の確保	
		基本契約による協力会社との連携	
b. 脆弱性			
1	脆弱性についての対応遅れ	脆弱性情報の共有化による迅速で効果的な対応	
2	不適切なセキュリティ設計	ｾｷｭﾘﾃｨ設計の有効性の検討	
3	形骸化した脆弱性対策の実装	実装の最適化による調和の確保	
2)提案から運用にいたるリスクと対応例			
a. 漏洩			
1	E−Mailによる情報漏洩	アドレス間違い防止	パスワードによる保護、暗号化
		添付するファイルのウィルスチェックの実施	ウィルス対策ソフト
		重要情報の書き換え／削除	
2	媒体送付による紛失／情報漏洩	追跡調査可能な配達方法を選択	パスワードによる保護、暗号化
		媒体のウィルスチェックの実施	ウィルス対策ソフト
		重要情報の書き換え／削除	
	不正利用による情報の漏洩		
3	外部からの不正アクセス	モニタリングによる監視	認証技術
		営業機密として十分な管理	アクセスコントロール
		パスワードの漏洩対策	ファイアウォール
		ネットワークの外部との遮断	
4	内部の不正アクセスによる情報漏えい	アクセスログによる牽制	パスワードによる保護、暗号化
		教育	アクセスコントロール
		営業機密として十分な管理	
		教育による防止	
		パスワードの漏洩対策	
		システムモニタリング、	
		オペレーションログ分析	
5	サーバからシステム、データ、運用データが外部メディア（コンピュータ含む）に不正コピー	外部メディアの使用禁止	ログイン制限
		教育による防止	
6	ベンダのバックアップメディア、ユーザーのバックアップメディアから不正コピー	外部メディアの使用禁止	
		バックアップメディアの保管強化	
7	なりすましによる漏洩	監視カメラによる監視、ログ	認証技術
8	盗聴による漏洩	ネットワークの外部との遮断	ネットワークの閉域化
			専用回線、VPN
			データの暗号化
	不正ソフトによる情報の漏洩		
9	外部から感染したウイルスによる漏洩	早期復旧対策	ウィルス対策ソフト
		ネットワークの外部との遮断	情報の暗号化
10	ベンダ、ユーザ、他ウイルスに感染した二次感染等による漏洩	電子媒体によるアクセルを禁止する。	ウィルス対策ソフト
		物理的に外部との接触を絶つ。	情報の暗号化
11	共有ソフト（Winny）等によりデータが流出	システム納入品以外のソフトインストール禁止	監視ソフトの導入
		ネットワークの外部との遮断	
	媒体の物理的流出		
12	媒体の盗難	バックアップメディアの金庫保管	
		教育による徹底	
13	媒体のコピーの盗難	コピーの配布先を明確にしておく	
		コピー媒体の金庫保管	
		教育による徹底	
14	媒体内データを印刷した紙の情報の流出	印刷済書類の処分教育	
15	システム定義書の紙の情報の流出	教育のよる徹底	書類保管管理強化
16	不要となった媒体からの情報流出	直ちにユーザに返却する	
		媒体の物理的破壊	
		分析・検証PC内のHDよりデータ消去	

	不正使用による情報の改ざん		
1	ベンダー、ユーザーが過って修正する場合	運用手順の教育	バックアップシステムの構築
		照合のシステム化	
		アクセスログ	
2	外部からの不正アクセス(情報の改ざん)	モニタリングによる監視	認証技術
		営業機密として十分な管理	アクセスコントロール
		パスワードの漏洩対策	ファイアウォール
		ネットワークの外部との遮断	
3	内部の不正アクセス(情報の改ざん)	モニタリングに監視	パスワードによる保護、暗号化
		アクセスログによる牽制	アクセスコントロール
		教育	システムのバックアップ
		営業機密として十分な管理(訴訟)	デジタル署名
		教育による防止	
		パスワードの漏洩対策	
		システムモニタリング、	
		オペレーションログ分析	
	不正ソフトによる情報の改ざん		
4	外部から感染したウイルスによる情報の改ざん	早期復旧対策	ウィルス対策ソフト
		ネットワークの外部との遮断	システムのバックアップ
			データ監視ソフト
5	ベンダ、ユーザ、他ウイルスに感染した 二次感染等による改ざん	電子媒体によるアクセルを禁止する。	ウィルス対策ソフト
		物理的に外部との接触を絶つ。	情報の暗号化
c. **破壊**			
	不正使用による情報の破壊		
1	ユーザーが不用意に破壊する場合	運用手順の教育	バックアップシステムの構築
2	外部からの不正アクセスによる情報の破壊	モニタリングによる監視	認証技術
		営業機密として十分な管理	アクセスコントロール
		パスワードの漏洩対策	ファイアウォール
		ネットワークの外部との遮断	
3	内部の不正アクセスによる情報の破壊	アクセスログによる牽制	パスワードによる保護、暗号化
		教育	アクセスコントロール
		営業機密として十分な管理(訴訟)	システムのバックアップ
		教育による防止	
		パスワードの漏洩対策	
		システムモニタリング、	
		オペレーションログ分析	
	不正ソフトによる情報の破壊		
4	外部から感染したウイルスによる情報の破壊	早期復旧対策	ウィルス対策ソフト
		ネットワークの外部との遮断	システムのバックアップ
			データ監視ソフト
5	ベンダー、ユーザー、他ウイルスに感染した 二次感染による破壊	早期復旧対策	ウィルス対策ソフト
		ネットワークの外部との遮断	システムのバックアップ
			データ監視ソフト
	媒体の物理的破壊		
6	バックアップメディアの破壊	バックアップメディアの金庫保管	
		教育のよる徹底	
7	システム定義書の紙の情報の破壊	コピーによる運用(原本金庫保管) 書類保管管理強化 教育による徹底	
	事故・災害による物理的破壊		
8	停電などによる障害		非常時電源を確保する。
			データバックアップ
9	水害によるもの	予測できる場合は事前にデータなどのバックアップを取る。	データバックアップ
		設置計画時に水害対策を採る(高所設置など)	
10	地震による障害	災害時の非難策、復元手順の策定と訓練	データバックアップ
		予備部品の確保	保守契約による速やかな回復
			転倒防止対策
11	輸送の破損・・設置時の破損	バックアップの単独保持	
d. その他			

d. その他			
1	工事中サイトなど不特定多数の関係者による 不正アクセス、媒体の盗難などのリスク	保管場所、立ち入り制限などの管理徹底	ログイン制限、パスワード保護
		教育による防止	
2	踏み台に利用される	ネットワークを外部と遮断する	ネットワーク監視
			ファイアウォールの構築
3	DOS攻撃を受けネットワーク上外となる	ネットワークを外部と遮断する	ファイアウォールの構築
		Webサーバなどを設置しない。	
3)通常状態で無い場合の使用			
a.保守メンテ			
1	リモートネットワークで外部よりアクセスを受ける。	・アクセスルールの確立	コールバック
		本人確認(パスワード、コールバック)、アクセス範囲	事前バックアップ
		作業手順(バックアップの有無)	ネットワークの閉域化
		・リモートは通常時はoffの状態にしておく。	専用回線、VPN
2	保守メンテ時の障害	作業手順の確立(事前バックアップ、稼動の影響対策)	予備部品の確保
3	システム保守のためのシステムバックアップからの流出		パスワードによる保護、暗号化
4	システム保守のために実機から抜いた 運用データのメーカからの流出		パスワードによる保護、暗号化
5	システム保守のために持っている書類のメーカからの流出	契約によるシバリ	
b.その他			
6	システム監査などによる想定外の使用	作業手順の確立(事前バックアップ、稼動の影響対策)	常時暗号化した状態で利用する
4)廃棄			
1	廃棄時の情報の漏洩	媒体処分に関する廃棄ルールを作成し実施する。 (初期化して廃棄　又は物理的な破壊処理等)	常時暗号化した状態で利用する
		処分記録の作成と保管	盗難、紛失等を想定した適切な対策 (保管場所の施錠設備、 入退出記録装置等の設置による入退出管理)
		管理対象の漏れの無い洗い出し	
		外部委託の場合廃棄処理の適切な業者の選定と 監督・指導の実施	
2	リース返却時の情報の漏洩及び他のシステムの 運用上の支障	廃棄時のリスク対策に準じる	
	故障部品の廃棄処理		
3	システム保守のために実機から抜いたデータの流出	媒体処分に関する廃棄ルールを作成し実施する。 (初期化して廃棄　又は物理的な破壊処理等)	常時暗号化した状態で利用する
		処分記録の作成と保管	盗難、紛失等を想定した適切な対策 (保管場所の施錠設備、 入退出記録装置等の設置による入退出管理)
		管理対象の漏れの無い洗い出し	
		外部委託の場合廃棄処理の適切　な業者の選定と 監督・指導の実施	
	その他の媒体の廃棄		
4	CD, FDなどの記憶媒体からの情報の流出	媒体処分に関する廃棄ルールを作成し実施する。 (初期化して廃棄又は物理的な破壊処置等　)	常時暗号化した状態で利用する
		処分記録の作成と保管	盗難、紛失等を想定した適切な対策 (保管場所の施錠設備、 入退出記録装置等の設置による入退出管理)
		管理対象の漏れの無い洗い出し	
		外部委託の場合廃棄処理の適切な業者の選定と 監督・指導の実施	
5	印刷した情報の流出	シュレッダーで処分する	
		外部委託の場合廃棄処理の適切　な業者の選定と 監督・指導の実施	

付録　2

《　共通技術、共通事項などの説明　》

セキュリティ対策に関連する共通技術、共通事項について下記に説明を記述する。

1)バックアップ対策

RAID 技術などによってディスクシステムの耐障害性は向上しているが、それだけでは万全とはいない。例えば、ユーザが誤ってデータを消してしまった場合やコンピュータウイルスに感染してしまった場合、 地震などの災害が起こった場合は RAID では対応できない。

よって速やかに普及できるようバックアップを取得するとともに、復旧処理を確立する。

(1)対象データ

・システムのバックアップ
・アプリケーションプログラムのバックアップ
・マスタデータのバックアップ

(2)タイミング

・アプリケーションプログラムの更新時

(3)メディアの保管

・保管場所（複数場所保管や金庫保管など）
・保管メディア
・管理方法（バージョン管理、管理者）
・その他
復旧を早めるためには日々の運用データのバックアップも重要になり、定期的の運用データをバックアップも必要。(システム内他の媒体にバックアップなど)

(4)バックアップデータを保存するデバイス／メディア

・ハードディスク
ハードディスクのバックアップのために、大容量のハードディスクを利用することもある。
・光メディア
DVD、CD-R などがバックアップ用に使われている。
・テープデバイス
バックアップ用途に最も利用されてきたメディア。
DAT などがバックアップ用に使われている。

2)バックアップ方法

(1)リアルタイムバックアップ

バックアップ装置と常に同期をとりながらバックアップする。
よってバックアップ装置は常に最新の状態になっている。
バックアップ装置は併設する場合と遠隔にある場合がある。

(2)フルバックアップ

定期的にバックアップを行うもので全データを一括してバックアップするものである。
全データを対象とするため時間がかかるが、最も確実な方法である。

(3)差分バックアップ

更新されたもののみを定期的にバックアップするものである。対象データが絞られるため作業時間は比較的短い。復元する場合にはバックアップの順番を考慮する。

(4)遠隔バックアップ

災害対策などを考慮して遠隔地にバックアップするものである。ネットワークを介して行う場合と、バックアップ媒体を送る場合がある。

3)漏洩に関する法的対応と注意事項

企業の営業機密の保護については、営業機密が機密として十分管理されていることが前提。管理されていない場合は不可罰となる。

不正アクセスが照会のみで、変更や削除を行なわず、誰にも損害を与えなかった場合も不可罰となる。

(1)機密情報

著作権法、不正アクセス禁止法、個人情報保護法等の法令で保護されている情報。漏洩することにより、企業の信用に大きな影響を及ぼす情報。

(2)営業機密

不正競争防止法により企業の「営業機密」は保護され、営業機密が侵害された場合に企業が責任をおえるようになっている。

「営業機密」である為には以下のことが必要。

①秘密に管理されていること

②有用であること

③非公知であること

そのため、企業は、機密として保護したい情報を、この３つの要件を満たすよう管理することが必要。

たとえば、社内文書やパソコンのデータ、データを保存した媒体に「秘」と明記すること、当該機密情報へのアクセス権者を限定すること、当該機密情報を保管する場所を設置すること、機密情報の中でも保護に値する情報と保護に値しない情報をある程度ランク分けして、保護に値する情報のみに限定して管理すること、および過去に刊行物や論文などで発表されていないもののみを管理すること。

4)専用線、専用回線

電気通信事業者が提供する特定顧客専用の有線・無線通信回線である。二地点間のものだけではなく、星型・分岐型の構成も可能である。専用の通信線路や電波周波数帯域を用いるとは限らず、他の回線と多重化されているものの方が多い。

利用者自身で設置するものを私設線、加入者間で相手先を任意に変更できるものを公衆網と呼ぶ。

特徴として次のような点がある。

・公衆網の輻輳に影響されない。

・公衆網と比較して、情報漏洩・盗聴・改竄の可能性が低い。

・定額料金であるので、通信頻度が多く・占有時間が長い場合、公衆網より安価である。

・二地点間を直接結ぶものの場合、接続動作が不要である。

・回線設備の敷設・保守を電気通信事業者が行うので、顧客の技術的負担が私設線より小さい。

5)VPN (Virtual Private Network)

外出先などからインターネットを使って安全に社内へアクセスしたり、特定のビジネスパートナーに対して安全に情報提供したりする場合に利用する仮想的な専用線。専用線や、Web ベースでの暗号化接続を提供する SSL やメールの暗号化という方法を用いたくてもネットワークの保護ができる。

6)ウイルス対策について

ウイルス対策には以下の項目の検討が必要である。

・ウイルス対策ソフトの選定
・パターンファイル、検索エンジンなどの更新
・ウイルス対策ソフトの影響調査
・ウイルス感染時の責任
・ウイルス感染時の対処方法

(1)ワクチンソフト

コンピュータウイルスを除去するソフトウェア。ウイルスに感染したファイルを修復し、コンピュータを感染前の状態に回復するアプリケーションソフトのこと。「ワクチンソフト」「アンチウイルスソフト」などとも呼ばれる。他のコンピュータとの通信状況を監視し、ウイルスの侵入を予防する機能を備えるものもある。

ワクチンソフトは予め用意されたウイルス検知パターンとファイルを比較してウイルスを検出するため、検知パターンが登録されていない新種のウイルスを検出することはできない。

検知パターンはワクチンソフトメーカによって定期的に更新され、最新のパターンはインターネットなどを経由して取得できるようになっている。感染力の強い新種ウイルスが発見されると、大規模な感染を防ぐため、そのウイルスを除去するためだけの機能限定のワクチンが無償で配布されることもある。運用面では常に最新のソフトとウイルス検地パターンに更新できる環境を提供する必要がある。しかしこれらも万全ではないので、感染源を絶つのが好ましい。

7)書類保管・廃棄基準

書類管理は以下の内容を検討する必要がある。

(1)書類保管

・保管場所の閉塞化
・持ち出し基準の策定

(2)書類廃棄

・書類の期限管理
・管理責任者の明確化

8)アクセスコントロール

アクセスしてきた人を認証によって特定し、情報のサービスの使用を適切な資格を持つ人に制限するための方策のことをいう。

認証の方法はいろいろあるが最も一般的で､安価なのは ID とパスワードを入力する方法

である。しかしそれらはシステムごとに割り当てられることが多いので、ユーザも数が多くなると管理不能になり、漏洩にもつながりかねない。そこでシングルサインオンなどの工夫が必要である。

そのほかの認証としては USB などの認証用の機器を用いる方法もある。これは使い勝手はよいが、その機器の管理に注意する必要がある。

生体認証は指紋や静脈、網膜、人相といった各個人固有の身体的特徴をもとに本人認証を行なう技術で、「バイオメトリクス」と言われる。パスワードや鍵といったものが無いため、盗聴やなりすましが事実上不可能なため、現時点で最も確実な認証方式である。

(1)シングルサインオン

1 回の ID／パスワード入力で、認証が必要な複数のアプリケーションを利用可能とするもの。しかし全てに利用できるとは限らない。

(2)暗号化（encryption）

情報の表現を組み替えて第三者が利用できないようにすること。ネットワーク上でのセキュリティ保護などで重要な役割をもつ。暗号化された文を暗号文（cryptograph）という。よく使われている暗号方式に公開鍵方式や秘密鍵方式があり、アルゴリズムとしては RSA 方式が知られている。インターネットでは Versign 社の SSL（Secure Sockets Layer）があり、Internet Explorer や Firefox , Google Chrome、等ほとんどの PC ブラウザが対応している。

暗号化用のソフトウェアはフリーソフトでもあり利用も容易になっている。

以下のような場合は暗号化を図るとよい。

・サーバ上のデータ（漏洩対策）
・メールでの添付ファイル（盗聴、漏洩対策）
・外部媒体での持ち出しデータ（盗難、漏洩対策）

9)監視ソフト

監視ソフトとはネットワークのトラフィックを監視するものから、直接クライアントのデスクトップを覗けるものまである。ほとんどのものはバックグラウンド（ユーザ側から操作できない状態）で動くため、ユーザは気付かないことが多い。

(1)ネットワーク監視ソフト

ＰＣにプログラムを悪用して対象のコンピュータを使用不能にする攻撃などが行われている。そのような攻撃からＰＣを防御してくれる。

サーバの監視や、ルータ等のトラフィック監視、ネットワークへの不正なＰＣの接続検知・通信遮断などを行なう。

(2)サーバ監視ソフト

LAN/WAN に接続されているサーバー・ワークステーション・ルーター等のハードウェアと、データベース・バッチジョブ等のソフトウェアに発生する障害を一括して監視・通知・復旧するもの。障害をすばやく検知し管理者に通知、そして復旧処理を自動実行も可能。

10)デジタル署名

デジタル文書の正当性を保証するために付けられる、暗号化された署名情報。公開鍵暗

号を応用したもので、文書の送信者を証明し、かつその文書が改竄されていないことを保証する。

11)コールバック
回線交換電気通信において、呼び出し側から着信側に電話番号などを通知した後、一旦通信回線を開放し、着信側から発信側を呼び出して通話を継続する通話法である。

12)ファイアーウォール
組織内のコンピュータネットワークへ外部から侵入されるのを防ぐシステム。また、そのようなシステムが組みこまれたコンピュータ。企業などのネットワークでは、インターネットなどの外部ネットワークを通じて第三者が侵入し、データやプログラムの盗み見・改ざん・破壊などが行なわれることのないように、外部との境界を流れるデータを監視し、不正なアクセスを検出・遮断する必要がある。このような機能を実現するシステムがファイアーウォールである。多くの場合はソフトウェアの形で提供され、コンピュータに組みこんで使用するが、高い性能が要求されるため、専用のハードウェアが用いられる場合もある。

13)セキュリティ教育
セキュリティ教育を行うに当たりカリキュラムが好ましい。
(1)専任者への教育
・情報セキュリティ概論
情報セキュリティの基本的な概念についての学習
・セキュリティへの脅威
どのような種類があるのか、またどのような経路や手段などが用いられるのかを理解。
・ネットワークセキュリティ
ネットワークを構築・運用する際に利用可能なセキュリティ技術。
・OS セキュリティ
個々のコンピュータ、特にＯＳに関連して、コンピュータを守るために利用可能なセキュリティ技術を習得。
・アプリケーションセキュリティ
Web ブラウザ、電子メールソフト等を中心とするアプリケーションに関して、利用可能なセキュリティ技術を習得。
・認証・アクセス制御
要素技術を習得。
・ネットワーク技術
基礎的な知識を習得。
・暗号技術
共通鍵暗号、公開鍵暗号、ハッシュ関数、デジタル署名、鍵管理といった暗号技術利用方法について習得。
・PKI

デジタル証明書の役割、認証局の役割や仕組み、電子公証や時刻認証などを習得。

・情報セキュリティマネジメント
基礎的なサイクル、及び物理的、人的セキュリティの側面を習得

・情報セキュリティポリシ
必要性を認識、構成の理解、方針や規程類の策定方法を習得

・リスクアセスメント
組織が保有する情報資産を適切に評価し、それら資産を取り巻く脅威、脆弱性に基づいてリスクを分析、評価を習得。

・クライシスマネジメント（危機管理）と事前準備
万が一クライシスが発生した際の基本的な対応方策を習得。

・法令と標準化
情報セキュリティを維持する上で有益な各種の規格・基準・指針・ガイドラインについて概観を習得。遵守が必須となる法令について習得。

・個人情報保護
プライバシーポリシの策定やJISコンプライアンスプログラム等を習得。

・システム開発管理
自組織において情報システムを開発し、それを安全に運営するため必要となる、ライフサイクルに沿ったセキュリティの考え方を習得。

・情報管理
資産のインベントリ管理、著作物の知的財産権の管理、企業の営業機密等の管理について習得。

・教育・訓練
管理する立場の者として必要な、利用者の啓発や教育訓練、また技術者の育成等に関する教育の方法・効果測定法などを習得。

・監査
管理する立場の者として必要な、情報セキュリティ監査、システム監査に関する基礎的な知識や手法を習得。

(2)利用者への教育

・啓発教育

・基本教育

14)セキュリティへの脅威

セキュリティへの脅威として、以下のようなものが考えられる。

(1)ネットワークからの脅威

・サービス妨害攻撃

・盗聴、改ざん、情報漏洩

・不正侵入

・踏み台

・メール爆弾

(2)組織内環境での脅威

・媒体盗難、紛失

・論理爆弾
・メールの転送
・バックドア
・誤操作による情報漏えい
・ソーシャルエンジニアリング

(3)物理的脅威
・災害
・破壊、妨害行為

(4)コンピュータウイルス、ワーム、マルウェアによる脅威
・感染先による分類
・隠蔽手法による分類
・ウイルスが利用する技術による分類
・ウイルスの活動による分類
・デマウイルス

(5)電子商取引とコミュニケーション上での脅威
・二重発注
・ユーザなりすまし
・否認
・名誉毀損
・サイバースクワッティング
・spam

(6)モバイル環境における脅威

15)ネットワークセキュリティ

セキュリティ上の検討事項としては、以下のものが考えられる。

(1)ネットワーク構成

(2)境界防御
・ネットワーク境界の考え方
・DMZ (DeMilitarized Zone)
・ネットワークアクセスコントロール
・ファイアーウォール

(3)ネットワークの管理
・SNMP (Simple Network Management Protocol)
・VLAN (Virtual LAN)

(4)NAT・NAPT

(5)ファイアーウォール
・アクセス制御
・パケットフィルタリング
・アプリケーションゲートウェイ(Proxy)
・ファイアーウォールの運用管理

(6)IDS (不正侵入検知システム)

(7)無線 LAN のセキュリティ

16)情報システムの情報セキュリティ規定の作成

情報システムの情報セキュリティ規定の作成項目として、以下が考えられる。

・インターネット・イントラネット利用規定
・インターネット向け公開サーバの設置および管理規定
・社内サーバ・FW/IDS およびクライアントの設置および管理規定
・リモートアクセス規定
・アプリケーションインストール規定
・情報管理の規定
・コンピュータウイルス対策運用規定
・クライシスマネジメント（危機管理）の規定
・情報セキュリティ監査・システム監査の規定
・情報システム管理者の規定
・ネットワーク管理者の規定
・システム開発の規定
・規定の承認・変手続き

17)クライシスマネジメント（危機管理）と事前準備

クライシスマネジメント（危機管理）と事前準備として、以下の項目が考えられる。

(1)情報収集
・CERT/CC, JPCERT/CC, IPA セキュリティセンター
・関係組織・マスメディア・通信事業者とのコミュニケーション

(2)エスカレーションポリシ
・予防策
・検知と初期対応
・被害の局所化（拡大防止）
・被害の撲滅
・復旧
・事後分析

(3)事故（インシデント）対応マニュアル
・インシデント予防策
・インシデントの分析（ハードウェアとソフトウェア）
・インシデント分析のリソースリスト
・インシデント対応ツール（セキュリティパッチ、OS のバックアップ等）

(4)証拠収集と証拠保全

(5)組織内のインシデントレスポンスチーム

(6)災害時復旧計画、事業継続計画

(7)事後報告
・CERT/CC, JPCERT/CC, IPA セキュリティセンターへの連絡と報告
・関係組織・マスメディア・通信事業者への連絡と報告

９．参考資料

9.1 ドキュメント名称と内容

ドキュメント名称	ドキュメント内容
契約仕様書	契約する時にユーザに提出する仕様書
契約書	契約条件が記載されている
工程を厳守する規定	契約時にユーザと取り交わす厳守お互いに遵守すべき工程の規定
要求仕様書	ユーザがベンダに対し要求する仕様書＝ＲＦＰをさす
品質仕様書	ユーザが要求した性能、機能を具体的に品質的に明示した仕様書
システム仕様書	ユーザに対し、システム製作の内容の承認（確認）を取り交わす機能仕様書(概要仕様書とも称する)
製作仕様書	システム仕様書に基づいてシステムを製作するための詳細条件を記載した仕様書（原則ベンダには提出しない）
検査仕様書	ベンダがユーザに対し検査を実施する内容を記載した仕様書
検査成績書	ベンタが検査仕様書に基づき検査を実施した検査結果を記載した書類
操作マニュアル	ベンダがユーザに対しシステムを操作するために必要な事項を記載した操作手引書（取り扱い説明内容含む）
保守マニュアル	ベンダか実施する保守点検の条件と点検内容を記載したマニュアル
完成図書	システム工事完成時に提出する図書を指す（システム仕様書の納入版）
完成確認書	ベンダからユーザにシステム工事完了の旨を書面にて提出する書類
工事完了証明書	完成確認書に対しユーザが発行する工事完了を証する書類

物流情報システム納入ガイドライン

2011 年 4 月　発行

一般社団法人 日本物流システム機器協会

〒104-0032　東京都中央区八丁堀 3-3-1
TEL　03-6222-2001
FAX　03-6222-2005
