51—R 005

総合貿易情報システム調査報告書(Ⅴ)

昭和52年3月

JIPDEC

財団法人　日本情報処理開発協会

この報告書は，日本自転車振興会から競輪収益の一部である機械工業振興資金の補助を受けて昭和51年度に実施した「総合貿易情報システムに関する調査研究」の成果を，とりまとめたものであります。

序

貿易業務の簡易化と貿易情報の総合的な活用を目的に，コンピュータを中心とした情報システム形成上の問題について，昭和４７年度より当財団に「総合貿易情報システム調査委員会」（ＣＯＴＩＳ）を設け，国連ヨーロッパ経済委員会（ＥＣＥ）を初め海外における貿易関係諸機関との情報交換を行いながら，調査研究を進めて参りましたが，今年度をもって５年目をむかえました。

本報告書は昭和５１年度に実施した第２貿易情報システムの形成，港湾情報システムの設計，セキュリティ問題等の調査研究の成果をとりまとめたものであります。ここに本報告書のとりまとめにご尽力頂いた委員各位に心より感謝の意を表しますとともに，本報告書が広く各方面に利用され，わが国の情報処理の発展に資することを念願する次第であります。

もとより，本報告書に盛り込まれた内容は調査研究の一部であり，調査研究の過程で収集されたセキュリティ関係の資料等については，紙数の関係から十分に掲載することが出来ず，本報告書を掘下げてご利用されるむきは，併せてこれらの資料もご利用頂ければ幸甚に存じます。

昭和５２年３月

財団法人　日本情報処理開発協会
会長　植　村　甲午郎

総合貿易情報システム調査委員会構成

（敬称略）

	氏　名	所　属
委員長	林　周二	東京大学教養学部教授
委員	伊藤栄一	情報処理振興事業協会理事
	伊藤皇	大蔵省関税局関税参事官
	今坂芳正	新日本製鉄㈱情報システム部長
	梅本章夫	㈱東京銀行事務管理部次長
	菊池右享	三菱商事㈱調査部長
	功力喜久男	日本貿易会企画部長
	小林永門	松下電器産業㈱東京支社次長
	斉藤成雄	通商産業省貿易局輸入課長
	正岡芳郎	㈱三菱銀行外国業務部考査役
	芝辻正一	三井物産㈱システム管理部部長代理
	鈴木秀郎	日本郵船㈱情報システム室次長
	高見玄一郎	港湾経済研究所所長
	田中勇一	東京海上火災保険㈱貨物業務次長
	田村倉由	日本船主協会常務理事業務部長
	長谷川寿彦	日本電信電話公社データ通信本部総括部調査役
	名取慶二	通商産業省貿易局輸出課長
	藤原正明	国際電信電話㈱総合開発センター データ通信開発担当部長
	松田季彦	富士通㈱システム部長
	宮本治男	日本貿易振興会企画部長
	油井兄朝	㈱日立製作所システム技術本部副技師長
	水野幸男	日本電気㈱情報処理営業計画本部長
	山口孝明	日本航空㈱貨物郵便運送部調査役
	関収	通商産業省機械情報産業局情報処理振興課長
	横田正雄	日本国際航空貨物輸送業者協会事務局長
	岡本行二	東京芝浦電気㈱第一電子計算機第二システム技術部長
	吉田剛	㈶日本情報処理開発協会専務理事
事務局	㈶日本情報処理開発協会　技術調査部調査課	

総合貿易情報システム調査専門委員会構成

（敬称略）

	氏　名	所　属
委員長	水野幸男	日本電気㈱情報処理営業計画本部長
委員	秋草直之	富士通㈱第5システム部部長代理
	伊藤昭	日本郵船㈱情報システム室第1チームリーダー
	奥村久一	三菱商事㈱EDPシステム部部長代行
	上条史彦	情報処理振興事業協会開発振興部長
	亀井慶紀	三井情報開発㈱社会システム事業本部 応用システム部部長代理
	北野睦郎	山下新日本汽船㈱情報システム部部長
	小暮健	大蔵省関税局伊藤参事官室課長補佐
	伊藤和男	東京芝浦電気㈱第一電算機システム支援部 第三システム支援課長
	鈴木浩	東京海上火災保険㈱貨物業務部統計課
	高見玄一郎	港湾経済研究所所長
	清木栄二	㈱東京銀行事務管理部開発第4課部長代理
	猫本春雄	㈱三菱銀行外国為替事務合理化グループ調査役
	林裕	日本電気㈱電々システム事業部 第2システム部システム課長
	櫛笥隆恭	日本航空㈱情報システム部 情報システム訓練課課長補佐
	町村信孝	通商産業省機械情報産業局 情報処理振興課課長補佐
	儘田清	通商産業省貿易局輸出課課長補佐
	宮崎敦夫	㈱日立製作所ソフトウェア工場 第1オンラインプログラム部
	村上雅之	日本電信電話公社データ通信本部 総括部企画調査担当調査役
	関戸秀明	通商産業省貿易局輸入課課長補佐
	市川隆	㈶日本情報処理開発協会技術調査部調査課長

COTIS システム小委員会構成

（敬称略）

	氏　名	所　属
主　査	伊　藤　昭	日本郵船㈱情報システム室第1チームリーダー
	五十嵐　誠	日新運輸倉庫㈱社長室主査
	奥　村　久　一	三菱商事㈱EDPシステム部部長代行
	西　川　浩　一	㈱上組東京支店プラント1課課長代理
	福　田　敏　雄	三井物産㈱運輸総括部部長代理
	水　野　幸　男	日本電気㈱情報処理営業計画本部長
	市　川　　隆	㈱日本情報処理開発協会技術調査部調査課長

COTIS セキュリティ小委員会構成

（敬称略）

	氏　名	所　属
主　査	水　野　幸　男	日本電気㈱情報処理営業計画本部長
	内　田　幸　久	日本電気㈱基本ソフトウェア開発本部 第一開発部技術主任
	猫　本　春　雄	㈱三菱銀行外国為替事務合理化グループ調査役
	村　上　雅　之	日本電信電話公社データ通信本部 総括部企画調査担当調査役
	吉　村　鉄太郎	㈱管理工学研究所取締役
	市　川　　隆	㈱日本情報処理開発協会技術調査課長

目　　次

第 1 部

総　　論

第１章　総合貿易情報システムに関する調査

1.1　は　じ　め　に

総合貿易情報システム調査委員会（以下COTIS と略）は，昭和４７年度に，貿易情報の円滑な流通と効率的な活用を目的としてコンピュータを中心とした情報処理技術を利用する総合システムの構想を提案，そして総合システムを第１から第４までの４つのサブシステム（図２－１参照）に分け，貿易取引完了後から船積までの第２貿易情報システムを中心に，その後は構想の具体化についての調査研究を重ねてきた。

この結果，昭和５１年度の調査研究において一応実用化可能なシステム概念をまとめるに至った。

現在研究している課題は３つに分かれ，(1)第２貿易情報システムの中心である商社 － 海貨業者 － 船社を流れる貿易情報と書類作成システムの研究，(2)港湾における上屋搬入から船積までの共同利用システム，(3)データ共用システムにおけるセキュリティ問題である。

COTIS が研究対象とした総合システムは，貿易データの共用システムであって，一連の貿易手続の流れに沿い異業種間を流通する貿易データを１度の入力でもって，必要の都度必要な書類を関係先に出力することにより，入力作業，多くの書類作成作業，手続作業を省力化するとともに貿易手続の簡素化をねらいとしたものである。

(1)　第２貿易情報システム（商社，海貨業者，船社書類作成システム）

今回まとめたシステム概念は，実用可能性を重視して，現実の商慣習，制度に制約される部分もあったが，基本的には上記の考え方を導入または効果を産むことが可能なシステムとして設計されている。今後は，プロトタイプのシステムを作成し，実用性の実験と経済性な効果分析を行い本COTIS 研究の成果として完成させる予定である。

(2) 港湾における共同利用システム

総合貿易情報システム形成における問題のうち，わが国特有の複雑な港湾地域に新規システムを導入する事の実現性について，幸いにも現在新設中の横浜大黒埠頭に進出が予定されている港湾運送業者のご協力を得て，共同利用のモデルシステムの研究を進めることができた。共同利用システムは，上屋への貨物搬入以後の海貨業者における貨物の在庫管理システムおよび書類作成システムを中心として取り上げた。ここでは，過去に提案した貨物動静情報を的確に把えるシエッドマスターを導入したシステムを具体化した。

(3) データ共用システムとセキュリティ問題

総合システムは，機能的には貿易データの共用システムであるが，異業種異企業における貿易データの共用のニーズがあり，効果が高くても競争原理にある企業例から見て，貿易データのセキュリティ問題が，どれだけ高い確度で保証されるかが明らかでなければ共用システムに参画するのが困難となる。

セキュリティ問題には，データの正確性を保持すること（integrity）とデータの機密を保持する（security）と２つの側面があり，予め予想される事故に対し，如何なる対策を講じるかが研究課題である。コンピュータ技術的には，一応の対策が可能であるが，貿易業務手続，従事者等に対する対策が問題として残されている。

1.2 総合貿易情報システム形成の必要性

総合貿易情報システム形成について調査研究を行うに至った背景は，第１に貿易手続関係の遅れによる経済的損失をいくらかでも軽減する必要があること，すなわち，需要面における問題，次に企業における情報処理システム化の効果をより一層高める問題，第３に海外ネットワークとしての対応等である。

(1) 需要サイドからのニーズ

国際貿易において，貨物の輸送設備手段が急速に合理化し，流通速度が高

まっているのに比べ，法律・制度および商慣習に拘束される貿易手続関係については必ずしも物流速度に対応して合理化されてはおらず，手続にもとづく書類の遅れによる貨物の滞留による倉庫料，滞留貨物の金利負担ほか倉庫建設費，土地代等経済的な損失が非常に大きい。また，1件の貿易手続のために注文書から船積書類まで多種の書類を作成する事務費の支出も増大している。このため貿易関係企業においては，既に物流速度に合わせた書類作成手続の迅速化などに個別的に努力を行っているが，それにも限界があり，手続の遅れを生じないように更に人手や機械化に再投資を行うというような結果になっている。

このような問題は，1企業や1業界の努力のみでは解決が困難であり，官民が一体となって貿易手続全体の流れを合理化するという観点に立って対処する必要がある。特にわが国のように，貿易によって成り立つ国では，日本の事情だけで対策を講じては問題を残すので，国際的な観点からの対応が要請されよう。

貿易手続の合理化については，昭和49年末以来JASTPROが国際的な動向を勘案しつつ，手続，書類，コード等の簡素化，標準化に努力されているが，いずれの問題をとってみても難問で，各界の意見の集約を得るまでに時間を要し，実行までとなると更に時日が費される。欧米先進国では，相当早くからこの問題に関心をもって検討を始めており，改善方策の見方も不必要な書類を排除する方向で検討が行われている。貿易立国として，この問題に対するニーズが高いながらも後発国の日本としては，時間的に見て何等かの抜本的な対策を必要とする。

(2) 情報処理システム化からのニーズ

企業では，貿易関係書類作成のために，事務処理の機械化やワンランメソッド等何等かの合理化を行なっているが，単純な事務機械では機械化できる範囲も限られていて，人手による作業との整合性がとれないなどから事務作業の混乱を生じる要因ともなり，貿易業界全般では，人海戦術によ

る方法が大半を占めている。

コンピュータを導入している企業では，このため，書類作成をプログラム化し，この複雑な業務処理を合理化している。また，オフィスコンピュータやマイクロコンピュータの進展により，コンピュータメーカーは，容易に書類作成可能なプログラムを提供する方向にあり，中小企業でもコンピュータ化が行われるようになろう。

しかし，コンピュータの導入は，現状の問題を解決する手段として考えられているに過ぎなく，本質的には貿易手続の簡素化による合理化にまつことはことさら述べるまでもないことである。

貿易企業における情報処理システム化，オンラインシステムの導入，国際的なネットワーク形成などは，わが国のコンピュータ利用の高度化に先導的な役割を果している。このように個別システムの情報化のレベルは高くなっていることは，情報化投資が多額となり，評価指標である費用対効果にも，自から限界があることは容易に想像されるところである。そこで，効果をより一層高める方向として，異業種異企業間とのシステム化がある。最近のデータ入力機器の発達によって，入力作業が軽減されたとはいえ，多量な貿易データの入力に要する費用は相当な額に達している。貿易書類作成には共通性のあるデータが多く，また貿易業務の流れに従い許認可情報や交渉結果のデータが付加される性質がある。このため異業種異企業間とのシステムを形成し，データ入力作業の分担および個別システムを接続し，貨物輸送や取引に関するメッセージの交換を行おうとするものである。

ところで，民間企業の場合，このような企業間システム形成は，取引関連が密接にあり，効果の高いところに限定されるし，個々の企業の事情によって都合のよい方法によりシステムが構築される。

総合的なシステムにおいて，個別システムがどのように形成されようと介入する立場にないが，総合システムの有効性や効率を問題にするときに，ネットワークに接続される個別システムからのデータ入力や，どんな情報

出力を行うか等によって具体的な機能や仕様が決定されるし，また個別システム側から見て，総合システムや，他の個別システムがどのような構成や仕様により構築されるかが，システムのインターフェース上重要な問題となる。換言すると，総合システムの形成により個別システム拡張の際のベクトル方向を示すものとなろう。

個別システム拡張の将来像として，ドキュメントレスの方向が検討されている。この兆候は，現在既に行われているテレックスによる貿易メッセージの交換において現われており，実際の貿易業務は，テレックスメッセージより遂行され，後刻届けられる書類はテレックスメッセージの確認行為のみの役割を果している場合も多い。異企業間システムや，総合システムが形成されると，現在貿易書類のためのデータ入力，帳票の出力といったことは重要な対象でなく，貿易メッセージの伝達，関係部署への分配，それにより判断情報の提供，記録等本来の情報処理機能が果すことになる。問題は，現在の書類が持つ信用保証を代替する方法が残されるが，解決が困難というほどの問題ではない。

(3) 国際ネットワークからのニーズ

貿易情報のネットワーク化については，各国とも関心が高く，既に米国がCARDIS（Cargo Data Interchange System）を昭和53年の稼動を目途に開発中であり，カナダでは，COSTPROが昭和55年までに全国的なネットワークを完成する計画で，とくに米国との接続も配慮されている等である。

日本が国内独自のニーズにもとづく貿易情報のネットワークが，海外諸国におけるネットワークとどのように関連をもたせるかという問題は非常に重要である。

日本が先進的にネットワークを形成し，海外のネットワークに対し，メッセージ形式，データ形式等のインターフェースを考慮するよう働きかけるようにするか，海外諸国からの要請によりネットワークのインタフェー

スをとるようにするかであるが，現在のところ諸国におけるシステム化の進展から見て後者の立場をとらざるを得ない状勢にある。

インタフェース問題は，国際的には，国連欧州経済委員会貿易手続簡易化部会で検討中であるが，これがまとまる以前に，前述のように各国で貿易ネットワークが形成されるとすれば，日本としては各国別のインタフェースを用意しなければ，貿易手続が円滑に進みにくいといった障害が生じる可能性がある。貿易業者が，インタフェースを用意するためには，相互の政府間で合意した標準的なインタフェースにもとづき，システム化を計るということになれば能率的である。

その時に，わが国の貿易情報ネットワークが形成されていると，標準としての役割を果すことになるが，形成されていない場合には新たに設定しなければならない。いずれにしても，海外ネットワークとのインタフェース問題は要検討事項である。

1.3 総合システムをサポートする情報処理技術

総合システム構想を可能とする背景に情報処理技術の発展があげられる。COTIS 研究の間にも種々の技術が完成，新製品が発表されたが，そのうち，コンピュータ・ネットワーク技術およびマイクロプロセッサ技術は，総合システム化にとって重要なものである。

(1) コンピュータ・ネットワーク技術

リソースシェアリング・コンピュータ・ネットワークと呼ばれる本技術は，独立して動作する個別システムが持つ，ハードウェア，ソフトウェアおよび各種データ等のリソースを相互に共同利用することを目的に複数のコンピュータを通信回線で接続するものである。

コンピュータ・ネットワークは，ネットワークに接続されるコンピュータ（ホストコンピュータと呼ぶ）群とホストコンピュータ同士を結合するための高速通信回線からなるデータ交換網から構成される。接続されるホ

ストコンピュータは，全てが同機種（オペレーティングシステムを含む）で構成される場合と異機種のものが接続される場合とがある。

総合貿易情報システムは，前述のとおり，機能的にはデータ共用システムであるが，システム構造的には，特定地域に置かれる地域共同利用センター（地域センターと呼ぶ）とこれに通信回線で接続される個別システムおよび端末機で構成される地域ネットワークと，いくつかの地域ネットワークを接続した全国ネットワークとの階層構造を持つことになる。そして，コンピュータ・ネットワークを形成することとなる。

このように構成されたネットワークは，貿易情報のニーズによって，その利用形態は様々であるが，地域ネットワークにおいては，地域内における関連企業間のデータ交換，書類作成，貿易データに対する照会，統計分析等が行われるのに対し，全国ネットワークにおいては，各地域センター相互間のメッセージ伝送や全国規模の貿易企業間におけるデータ処理・交換が行われよう。

最近，このコンピュータ・ネットワーク技術を利用した分散システム化が話題となっているが，これは，予じめ各ホストコンピュータが持っているリソースを利用するというよりは，ネットワークを構築する時に，ホストコンピュータの機能を予じめ設定して，ネットワーク全体を1つのシステムとして設計するものである。

貿易情報の総合システム化においては，扱うデータが大量であり，一連の手続による書類完成までのトランザクッションデータで，寿命が最長6カ月程度ということで，データファイルを物理的に分散して保有する方が利点が多い，あるいは，処理の分散でも，タリフ計算，揚地の港湾事情，船舶動静，統計処理等関連システムを各々のホストコンピュータを設定してニーズに応じる等が考えられる。

このように，コンピュー・ネットワークは，総合システムにおける主要な技術であるが，われわれ貿易情報側から特に関心を寄せなければならな

い問題にプロトコルがある。

プロトコル（protocol）は，コンピュータ・ネットワークにおける各機器間のメッセージ・データの受渡の手順，そのフォーマットおよび内容等に関する規約であり，図1に示すように様々なレベルがある。このうち，高位プロトコルは利用者が直接かかわり合いを持つレベルで，現在，端末機からネットワークにアクセスする場合のプロトコルについて，基本的なキャラクタ・レベルにおいては，国際英文字№5を使うことで標準化されようとしている。したがって，ファイルテキストを転送する場合には，余り問題がない。しかし，文字ストリングに依存する多くの端末機よりアクセスする場合の国際的標準化は，相当困難と見られ，このまま放置するならば利用者はメーカー標準によらざるを得ないのではないかといわれる。

このため，貿易書類作成といったように端末機の使用目的が決っている貿易業界として，何等から標準を設定することにより，メーカ側においても共通仕様の機器を提供できるといったメリットが考えられるのである。

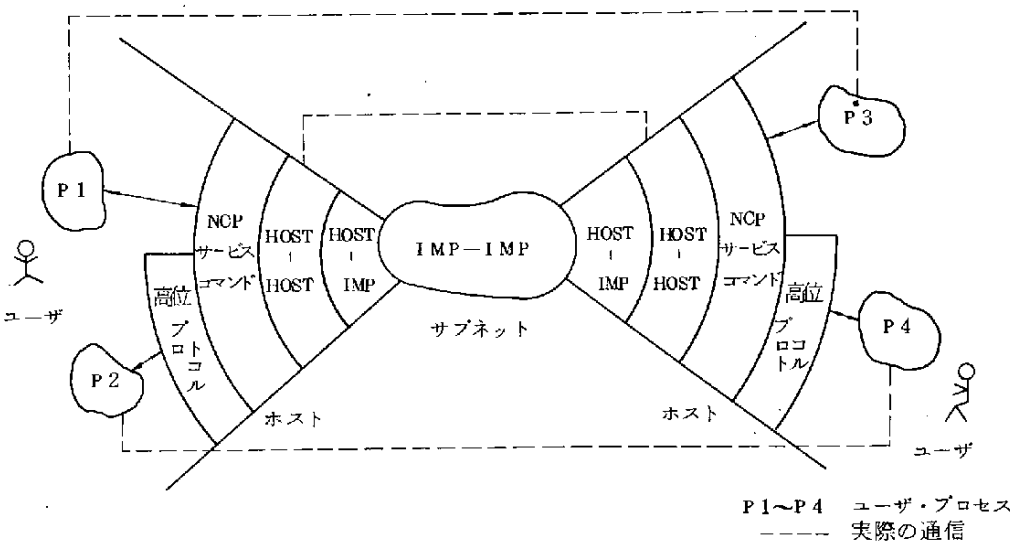


図1　プロトコルの階層

① コミュニケーション・サブネットの効果的な運転を実現するための IMP－IMP プロトコル。

② ホストＩＭＰのつなぎとして主としてデータの送受方式を規定する HOST－IMP プロトコル。

③ ホスト同士が交信する方式を規定するHOST－HOST プロトコル。

④ HOSTがユーザ・プロセスに対してサービスするコマンドを規定したプロトコル。

⑤ ユーザに対して機能レベル（ユーティリティ）のサービスをおこなう高位のプロトコル。

このうちユーザ・プロセスが直接かかわりあうのは，④と⑤であり，①，②，③はシステムレベルのプロトコルである。

ＩＭＰ：Interface Massage Processer

ＮＣＰ：Netwark Control Program

(2) マイクロ・プロセッサ

マイクロ・プロセッサは，コンピュータの回路素子である集積回路を1個または数個組合せて，演算制御装置を作り，簡易な入出力機を接続して，コンピュータシステムの機能を果すものである。利点は，超小型で低廉であることから，コンピュータシステムというより，各種の制御機構に組み込まれ使用されてきている。そして，今後とも，大規模集積回路（ＬＳＩ）や超ＬＳＩの開発によって，ますますその応用域を拡大することが予想され，各層の情報化の中枢をなすものといわれている。

貿易情報化にとっても，利用が進展するものと考えられる。このマイクロ・コンピュータは，機能的には限定されているが，安価にコンピュータが使用できるということから，小規模貿易業者や事務所に導入が考えられる。そして貿易情報ネットワークを容易に利用することによって，中小規企業が合理化されることが大いに期待されるのである。

1.4 問　題　点

総合システム形成における問題点として次の諸点が挙げられる。

(1) 貿易関係手続簡易化事業の促進

COTIS における総合システム化の研究において当に問題になるのは，法律・制度にもとづく手続改善に関する事項である。その具体的問題点は，第2部をご参照頂きたい。

この問題は，システム的に見て，不合理なことがあっても容易に改善できない事項が多く，システム検討する場合，システム化における制約事項として問題提起を行うか，あるいは，制約事項として認め，これをシステムの中で如何に処理するか，というように，その立場によって観点が異なる。当初COTIS では総合システム化における問題点発見という観点からアプローチしたが，システムの実現性が乏しくなるということから，現在は数年先でも実現可能なシステムということで，後者の立場にある。

いずれにしても，貿易手続簡易化事業は，時日を要する問題が多いが，コンピュータを利用するという立場からの問題解決を促進することが要請される。

(2) ドキュメント・レスに対する検討

現在，わが国のシステム化問題は，現行書類をどう処理するかについて重点がおかれているが，貿易情報ネットワークを前提として，貿易関係書類のうち，廃止すべきものと残すべきものとをよく吟味し，全体的にドキュメント・レス方式のあり方，そのアプローチ方法等について討議を重ね，各界のコンセンサスを得ておく必要があろう。

(3) セキュリティ問題

総合貿易情報システムはデータ共用が中心機能であるが，企業がこのシステムに参加するか否かは，データセキュリティがどれだけ保証されるかにかかってくる。

一般的に，わが国の場合，セキュリティ問題に対して非常に厳しい側面

とルーズな面とがあり，また，セキュリティに対する認識があいまいな点があるように思われる。

貿易情報のネットワーク化の方向は，その形態は別としても，今後の問題であり，必然的な方向と考えられるが，セキュリティ問題に対し，機械的な対策，人為的な問題に対する対策について検討が必要とされる。

第２章　昭和５１年度調査研究の概要

2.1　今年度調査研究の位置付け

当事業は総合貿易情報システムに関する調査研究として，昭和４６年以来５年にわたり，「総合貿易情報システム調査委員会」（ＣＯＴＩＳ）のもとに調査研究を実施してきた。初年度における総合貿易情報システムのコンセプト作りに始まり，これまでの４年間に国内の貿易関係業界における情報フロー分析を行うとともに，海外における動向を把握しつつ，業界各分野におけるサブシステムとしてのあり方について研究を行ってきた。

今年度は，これまでの調査研究において，システム化のメリットが高く，総合商社という日本独特の業界を含む第２貿易情報システムの範囲について，より詳細な分析を行った。第２貿易情報システムとは，貿易取引契約の締結後における船積までの情報処理システムと規定し，船腹スペースの予約，通関書類の取揃え，船荷証券の作成などを含む。

第２貿易情報システムにおいては，シッパー（商社），海貨通関業者，エゼント業者，検定・検数業，船会社等が密接な関係をもって業務を行っており，情報の伝達，フィードバックが緊密に行われているため，この部分における情報の伝達，処理，やデータの共同利用のコンピュータ化による効果は非常に大きなものといえる。

これに含まれない他の情報システムはサブシステムに分離することが容易なものが多く，官庁，業界間の関係の位置付けを明確にすることが可能であるのに対し，第２貿易情報システムにおいては，Ｂ／Ｌ発行により銀行買取書類が揃うまでに，業界間においての情報の流れは一方通行ではなく，多くのフィードバック情報のもとに業務が進められており，また，情報の修正，不確定情報が何段階かのステップを経て，確定するといった過程を経ており，非常に複雑かつ密接な情報フローの関係となっている。

こういった意味からこの分野における情報の一元的，総合的管理及び共同利

用の効果は測り知れない。従って本年度は，小委員会構成のもとに，第２貿易情報システムにおけるデータ・アイテムの整理とシステム化の可能性について研究を行い，その詳細を第２部に掲げた。

貿易情報システムによるデータの共用にあっては，多くの業界の関係者がデータにアクセスするとともに，これらの人々は必ずしもコンピュータ・システム操作の専門家でないため，エラーの発生する可能性も大きい。このような状態において，故意または過失によって競争会社に企業機密が洩れたり，データが破壊されたりしないためには，データのセキュリティが大きな問題となってくる。

貿易情報システムにおいては，企業内システムと異なり，データの入力や出力が非常にオープンであって，利害の対立する関係者が同じコンピュータ・リソースを共同利用するとともに，第３者がコンピュータ・システムやデータにアクセスする可能性も大きい。

セキュリティ対策は，このような故意の侵入者に対するとともに，人間のエラー，機械のミス・オペレーション，通信回線による伝送エラーといったものから守られなければならない。

また，文書による情報の伝達にあっては，印鑑，サインといった方法によって証明されてきた情報の確認を，コンピュータによるデータ伝送によって行うためには，データの一部に当事者のみが判別できる暗号を組み込むなど情報のオーセンティケーションを考慮する必要がある。

このような観点から，ＣＯＴＩＳではセキュリティ小委員会を設け，調査研究を行うとともに，国連欧州経済委員会（ＥＣＥ）へもセキュリティ問題の重要性への認識を喚起した。

貿易情報システムにおいて，各業界の関係者がデータを共同利用するとともに，海外とメッセージ交換を行う場合には，ＡＤＰ施設の物理的保護，データの盗難や破壊，人間によるエラー，通信回線上でのデータの変質といった全ての被害の可能性があり，情報処理分野全般におけるセキュリティ問題の研究が

必要であるとともに，メッセージ発信者の確認，許認可情報の伝達，金額支払いの伝送による処理といった貿易分野で特に重要な問題も存在する。

これらの問題は，コンピュータ・メーカー，大学や研究所，各コンピュータ・ユーザーといった多くの方面においても，調査や研究が行われており，COTISで行っているものと重複するおそれがある。このため，主に文献を中心に他機関等で行われている研究動向を十分把握するとともに，あまり詳細な部分へは立ち到らず，貿易情報システムにおいて，問題なる部分を浮き彫りにすべく，セキュリティ問題の全体把握と貿易特有の問題の抽出に重点をおくこととした。

貿易情報システムの実用化には，セキュリティ問題のみならず多くの障害や解決すべき問題がある。第2貿易情報システムのうちでも，特に港湾においては，海運貨物取扱業，ランディング・エゼント，はしけ回漕業，ステベドア等細分化された職種が，業務の分担区分，因習の法的正当化等によって複雑にからみ合っており，これにシッパーが加わって，過度な臨機応変を行う場合もあり，システム化を推進するに当っては多くの問題点が含まれていることが予想される。

こうした中にあって，これらの業界の中では，コンピュータを導入し，社内業務の処理を行うとともに，貿易業務のシステム化を図っている企業も多い。このような実態動向を踏まえて，総合的な貿易情報システム化の観点より，各業界の情報フローをシステム化し，情報の共同処理，情報伝達のオンライン化等を推進するとともに，自からコンピュータを持たない企業も共同利用センターの形でシステムへの参加を求めることは大いに意義あることといえる。

このような目的から，現状の問題点は直視しつつも，システム化の可能性を探索し，将来のシステム化の在り方を見極めるため，港湾における情報システム化について具体的な地域をモデルにしてフィージビリティ・スタディを行い，その詳細を第3部にとりまとめた。

2.2 第2貿易情報システムの研究

貿易取引にかかわる諸業務のうち，商社－海貨業者－船会社にまたがる情報フローを第2貿易情報システムとして把え，ここにおける輸出業務についてシステム化の研究を行った。

第2貿易情報システムにおいては，各業界間の情報フローが多種に及び，またフィード・バック情報が重要となる。この間の複雑な情報伝達，処理，フィードバックをコンピュータへ一度入力することにより共用データとして，情報の有効利用が可能となる。

しかし，現在の文書による情報の伝達・処理をコンピュータを用いた情報システムへと変換するためには，法的，商習慣上等多くの問題がある。情報システム化においては，文書情報との併存等，過度的な手段もとられるであろうが，ここではシステム化への多元的展開を考慮に入れて，共通エレメントの抽出と大枠のシステム構想を打ち立てることに留めた。

貿易業務は，取扱商品の種類によって相当異なる場合があるため，プラント，化学品等の輸出者にヒアリングを実施し，その特殊性を探るとともに，問題点の摘出を行った。そこには，情報フローのシステム化以前の多くの障害もあり，今後の改善が望まれるが，これらの問題点及び官庁，他業界への要望事項は，システム化における問題とも深く関わるので整理して掲載した。

また，システム化に当っての各種帳票の標準化，手続の簡易化は(財)日本貿易関係手続簡易化協会（ＪＡＳＴＰＲＯ）の活動と関係が深く，今後の進展を踏まえてシステム化を推進する必要がある。

データ・エレメントについては，多種類の帳票のうちから，主要帳票１２の現行帳票による２２０データ・エレメントをもとに各帳票への出現頻度，各データ・エレメントの重要性を勘案し，５５のデータ・エレメントに集約した。

これらのデータ・エレメントはデータの共用とともに，各業界間の情報交換を行うための一つの目やすになるとともに，これ以外のデータ・エレメント及び他業界よりのフィード・バック・データを入手することにより，殆どの帳票

は作成可能になるとともに，これらのデータ・エレメントを基に，処理可能な情報処理システムの概要を覗い知ることができる。

また，これらのデータは，必ずしもデータ通信によるオンライン伝達に限らず，磁性媒体の持ち運び等によっても伝達可能であり，媒体の複製も容易かつ迅速であり，オフラインでの磁気テープの読み取りも可能である。

これらのデータ・エレメントは個別企業間の交換に初まり，やがてはメッセージ・スイッチ的な交換，セキュリティ問題の解決と，官庁業界の同意に基づく，データバンク的データの共用へとシステムが発展してゆくことが考えられる。

2.3 海貨取引情報システムの研究

貿易に関わる諸手続きのうちでも，港湾における部分においては，多くの企業が関係し，情報の伝達も複雑である。港湾というある限られた地域内で，多くの企業が情報の伝達，フィードバックを行っており，ここにおける情報フローのシステム化とデータの共同利用は，他の貿易情報システムと同様大きなメリットを生む。しかし，現状の業態において，情報のシステム化を行う為には多くの問題点がある。

このため，新たに外貿埠頭公団によって建設されている横浜港大黒埠頭を対象に，具体的情報システムの設計を行い，その可能性を探ることとした。

当システムの主たる目的としては，ドキュメンテーションと貨物管理のシステムであって，S／O，B／L等の船積書類を作成するとともに，シェッド・マスターと名付ける帳票を新たに設けて，貨物の受領から船積までの貨物管理を行う。

システム化にあたっては，コンピュータの共同利用センターを設けて，オンラインによるデータベースの利用という形態で実現する。そして，各業務ごとにジョブ処理をシステム化し，これを全体構想とつなげている。

ファイルとしては，シェッドマスター・ファイル，ブッキング・ファイル，

ドキュメント・ファイル，ローディング・ファイルの4ファイルを持ち，これらは，ドキュメンテーションと貨物管理システムとの共用ファイルとなっている。

今回設計した輸出入情報システムについて，5段階点数制により，省力化，迅速化，管理水準の向上等の面から評価を行った。

また，これら各評価面の海貨，エゼント，検数，検量等の各業界別のメリット分析を行った。

これらメリットとともに，システム開発・運営の費用と省力化，迅速化に基づく節約の効果を金額的に分析した。費用には，研究開発費，設備投資費，運営費等が含まれ，効果には，省力化，日数短約に基づく金利軽減等が含まれる。

2.4 ＥＣＥ貿易手続簡易化部会の活動状況

国連欧州経済委員会（ＥＣＥ）貿易拡大委員会貿易手続簡易化部会では，ＡＤＰとコーディング専門家会議（ＧＥ１），記載データとドキュメンテーション専門家会議（ＧＥ２）を設け，貿易手続の簡略化と標準化の作業を着実に推進している。特に，帳票，コード等の標準化と手続きのＡＤＰ化は大きな課題となっている。

数種の帳票の項目の位置を揃えて，1回のタイプでこれらの帳票を作成するワンラン・メリッドを目指したＥＣＥレイアウト・キーの制定に引き続き，国名アルファベット・コードの国際標準化とともに，通貨コード，ポート・コード，船名コード等の標準化についても鋭意検討が進められている。

国際間における貿易メッセージ交換についても，英国ＳＩＴＰＲＯ(Simplifi－cation of International Trade PRO cedure)の提案に基づいて，研究が行われ，メッセージ交換におけるシンタックスへの展開と研究が進んでいる。

１９７５年にはタスク・チーム（T.T）が設置され，データ・エレメントとコード，トレード・データ・インタチェンジ，統一書類とＡＤＰ等のテーマのもとに，小人数のグループのもとに，緊密な研究が行われている。

日本からも１９７５年来，国内における貿易手続き簡略化，システム化の研究動向や成果が発表された。

ＣＯＴＩＳよりは，今年度，昨年度からのセキュリティ問題の一環として，データベース内の機密保持の具体的方法，セキュリティ問題の作業範囲等について，研究成果の報告を行い，同作業部会出席のメンバーに対し，セキュリティ問題の重要性の認識を得るとともに，今後の具体的作業方法について提案を行った。

国際貿易に大きな位置を占める日本としても，こうした国際会議の動向を十分に把握するとともに，日本側の意見もこれら会議の動きに組み入れて行く必要がある。そのためには，日本としてもこれら会議の進行に貢献し，メンバーとしての位置を確実にしてゆく必要があろう。

ＥＣＥ会議へ報告したレポートの詳細については，第４部において詳述することとする。

第　2　部

第2貿易情報システムの調査研究

第1章　はじめに

昭和５１年度第１回総合貿易情報システム調査専門委員会会議において，51年度の作業計画の一つとして，過去４年間にわたって調査研究を重ねて来た総合貿易情報システムの内，昭和４７年度の作業報告の中から，第２貿易情報システム（図２－１参照）の実用化について，更に具体的に研究を進めることが決定された。

この決定に基づき，昭和５１年５月２０日，第２貿易情報システムの実用化における問題点の調査研究及び，貿易に関するデータの共用についての調査を主題とした，システム小委員会（旧ワーキング・グループ）を発足させ，調査研究を行って来たが，ここに漸く，第２貿易情報システムの実用化の可能性について結論を得た。

尚，調査及び検討作業の詳細については第４章にまとめてあるので参照されたい。

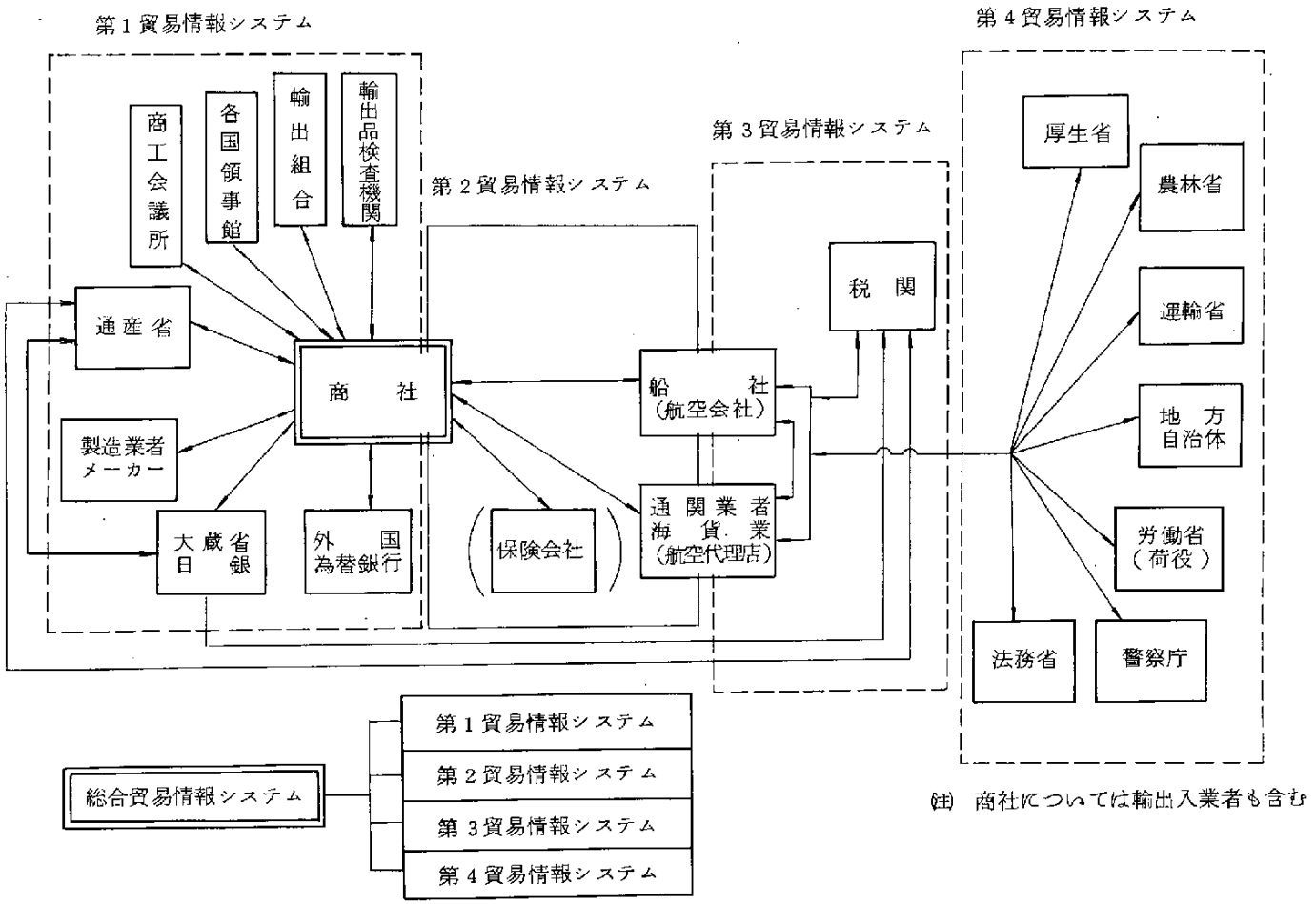


図 2 － 1　総合貿易情報システム構成図

第2章　想定される第2貿易情報システム

2.1　システムの概要

小委員会において，本システムの実現性について鋭意検討を重ねたが，システムの範囲として，

(1)　輸出業者（Shipper）

(2)　海貨通関業者

(3)　船　　会　　社

を主体とし，輸出業務に限定し，かつ輸出業者の取引きにおいて，契約が成立した以降，船積み Bill of Lading （B／L）発行までの，ドキュメンテーション処理を中心としたシステムとして策定したものである。また更に，本システムの実用化という点から考えて，輸出業者の，関係官庁への許認可諸手続き及び保険，銀行決済等の問題に関するものも除いてあり，これらの問題は，別途，他のサブ・システムとして，或は本システムを効率よく運用させるためのサポート・システムとして，改めて検討，策定し，将来的には本システムと接続するものであるとの判断からこのシステムには含めていない。従って，今回検討されたもの，第2貿易情報システムといっても，極めて範囲の狭いものである。

2.2　システムの目的

本第2貿易情報システムは，コンピュータ・システムを前提とし，貿易関係書類作成業務の合理化と，共通情報の業界相互間での有効利用を目的とするものである。即ち情報源における一回の入力により，これを各企業内及び各業界内にて繰返し利用すると共に，自己の業務に必要な情報を順次追加し，他の業界に提供し，更にはそれら情報を相互にフィード・バックして，それぞれの業務の合理化と，メリットを互に享受することを目的とするシステムである。

2.3 システム構想図

このシステム構想図（図２－２）は，それぞれの企業又は各業界の業務を中心にして画いたものである。

従って業界相互間で受渡しするデータの伝達方法については

① 相互に手交する方法。

媒体としては一応磁気テープを想定したものであるが，これはペーパー・テープ又はディスケット等でもよい。

② オン・ラインまたは，オフ・ラインによるデータ伝達による交換。

のいずれでもよいことを示している。またこのシステム構想は，概要の項でも述べた様に，範囲も限定された狭いものである。

このシステムが適用される一つの方法としては

① １輸出業，１海貨通関業者及び１船会社といった企業単位の縦の関係のシステム化

② 企業グループ単位で多少横の関係をも含めたシステム化

を前提としたシステム化構想である。

このシステム構想は情報の有効利用をねらったものである。

図 2 － 2　システム構想図

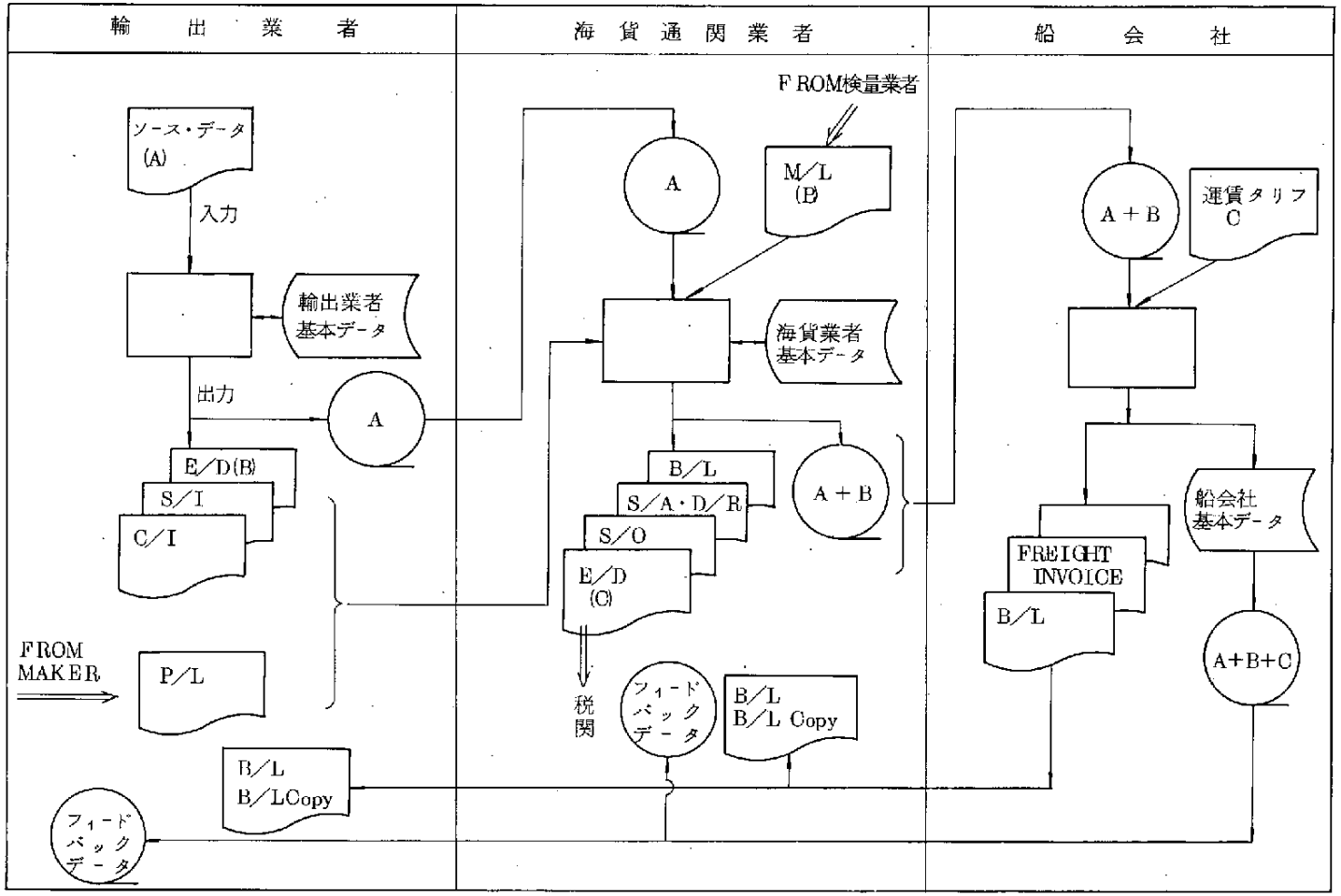
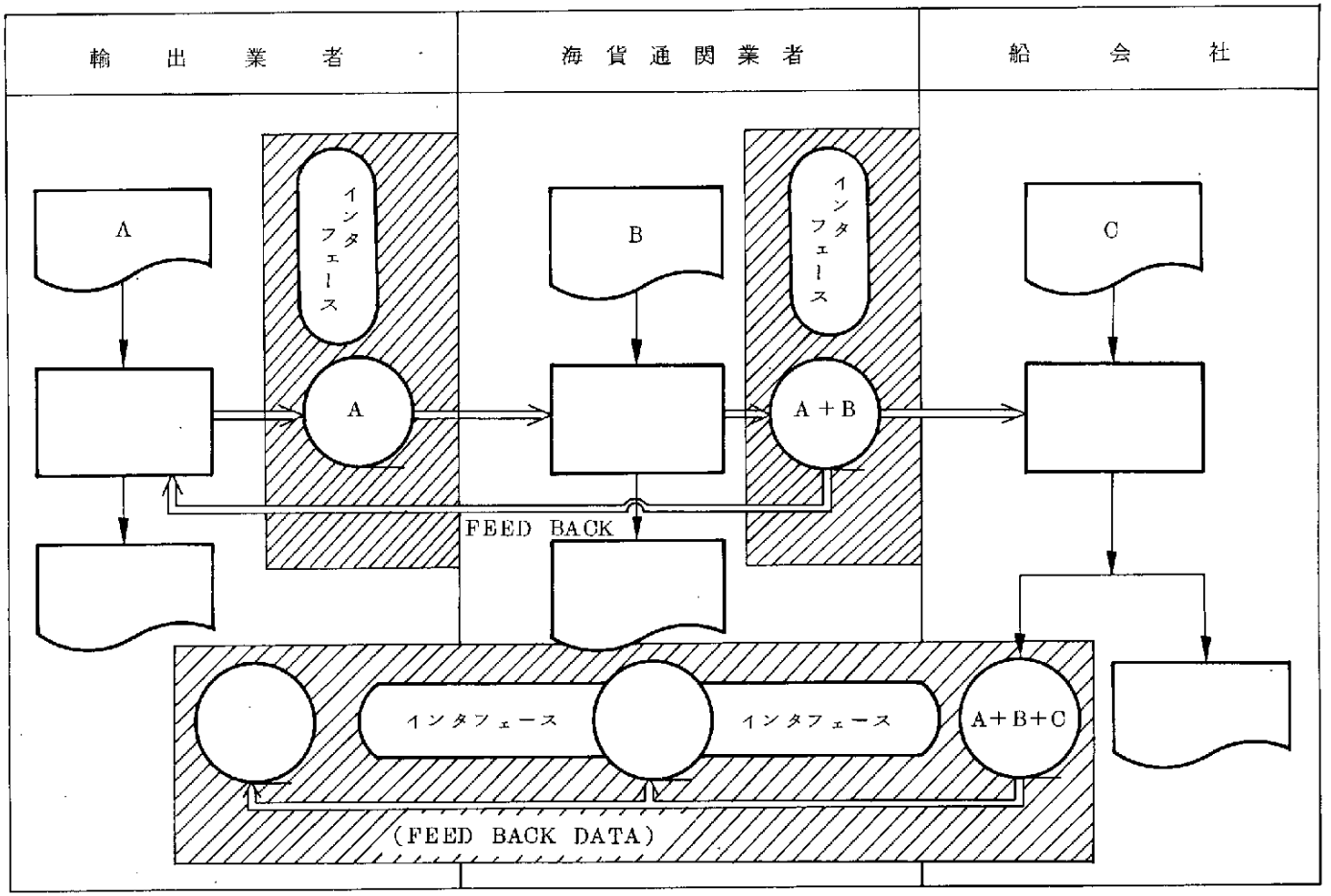

輸出業者
海貨通関業者
船会社
FROM検量業者
ソース・データ
(A)
入力
輸出業者
基本データ
出力
A
E/D(B)
S/I
C/I
FROM
MAKER
P/L
B/L
B/LCopy
フィードバックデータ
A
M/L
(B)
海貨業者
基本データ
B/L
S/A・D/R
S/O
E/D
(C)
税関
フィードバックデータ
B/L
B/L Copy
A＋B
A＋B
運賃タリフ
C
船会社
基本データ
FREIGHT
INVOICE
B/L
A+B+C

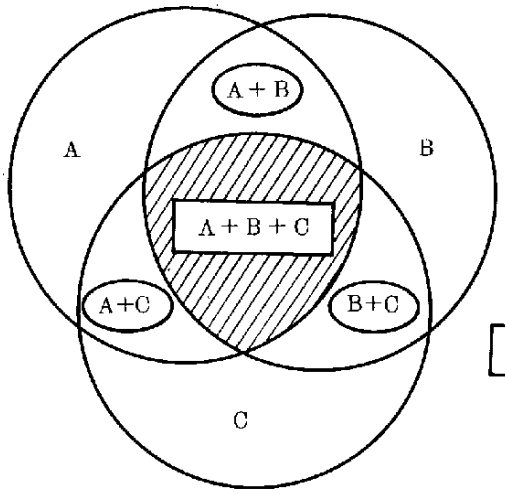
図 2 － 3


輸　出　業　者
海 貨 通 関 業 者
船　会　社
A
インタフェース
A
B
インタフェース
A＋B
C
FEED BACK
インタフェース
インタフェース
A+B+C
(FEED BACK DATA)

2.4 共通情報の抽出

各業界で必要とするもしくは，入力する情報（データ）の内，二業界または三業界で共通に必要な情報を抽出する必要がある。

図２－４



A：輸出業者が必要とするデータ
B：海貨通関業者が必要とするデータ
C：船会社が必要とするデータ
A+B ＝2業界で共通に必要なデータ
A+B+C ＝3業界で共通に必要なデータ

ただし，この想定システムが有効に運用されるためには

(1) 各業界での入力のタイミング

(2) 各業界におけるデータのコレクション（訂正）処理

(3) 情報源（輸出業者）及び仲介業者（海貨通関業者）へのデータのフィード・バックとそのフィード・バックのタイミング

等が適切に行われなければならないという条件があり，また

○ 各業界で必要な書類の抽出選定すべきものとして次のようなものがある。

(1) 自からのデータで作成するもの

(2) フィード・バック・データ又は伝達されたデータを利用して作成するもの

○ 各書類毎に必要なデータ・エレメント

○　各業界毎にフィード・バックが必要なデータ・エレメント

2.5　関連必要ドキュメント

本システムにおいて，各業界毎に必要とする自から作成する書類及び，フィード・バック・データ，または他業界から伝達されるデータによって作成する書類を挙げれば次の通りである。

(1)　輸出業者が自から作成する書類

①　コマーシャル・インボイス（C／I）

②　シッピング・インストラクション（S／I）

③　インシュアランス・アプリケーション　（I／A）

④　銀行認証用E／D

※⑤　パッキング・リスト（P／L）…MAKER　として

尚次に挙げる各書類については本システムの対象から除いてある。

○　輸出取引承認申請書

○　輸出承認申請書

○　輸　出　承　認　書

○　輸出検査証明書

○　デザイン・商標判定書

(2)　海貨通関業者が作成する書類

①　輸出申告書（通関用E／D）

②　シッピング・オーダ（S／O）

③　シッピング・アプリケーション　（S／A）

④　メイツ・レシート（M／R）

⑤　ドック・レシート（D／R）

⑥　船荷証券（B／L）

⑦　メジャー・リスト（M／L）…検量業者より入手

(3)　船会社として必要な書類

① コマーシャル・インボイス（C／I）

② パッキング・リスト（P／L）

③ シッピング・オーダ（S／O）

④ シッピング・アプリケーション （S／A）

⑤ メイツ・レシート（M／R）

⑥ ドック・レシート（D／R）

⑦ コンテナ・ロード・プラン（CLP）

⑧ 輸出申告許可書（通関E／D）…コンテナ船

2.6 関連共通データ

本システムの目的において述べた通り，このシステムは，共通情報の業務相互間での有効利用を前提としているため，各業界で作成または，必要とする書類に記載されているデータ・エレメントを調査したが，これによると

○ 初期調査の段階では

C／I等13種類の書類で220データ・エレメント

○ 次の段階では11種類の書類にしぼったところ，122データ・エレメントとなった。

これらデータ・エレメントを更に共通に3回以上繰返し使用されている項目を抽出したもの及び特に必要と認められるものが表2－1に示されている如く，55のデータ・エレメントである。

2.7 各業界での期待されるメリット

本システムは，社会情報システムの一つのパイロット・システムとして官庁主導型のものと，業界主導型としたものとの二つのアプローチが考えられる。本システムでは，後者の業界主導型のシステムとして考えた。従って新しく構築されるシステムに参加する企業，業界にとって何らかのメリット，利益が期待できなければ何の意味もなく，結局は『絵に画いたモチ』となってしまうで

あろう。

本システムは，後述するが現在各業界がかかえている輸出諸手続きおよび業務における問題点を洗い出し，これらのうちのいくらかでも改善，合理化が期待でき，またその実現性も十分にあるとの判断により，システムの策定を行った。

(1) 輸出業者が第2貿易情報システム機能に期待する事項

① 貿易業務全般のファンクションを区分すると，

(A) 引　　合

(B) 成　　約

(C) 受 渡 し

(D) 代 金 決 済

の四つに大別されるが，これらのファンクションのうち，本システムとの関連づけを整理すると(C)の受渡しファンクションがその対象の大部分を占めることになる。

② 次に(C)の受渡しファンクションで必要とする情報は，

(A) 船舶動静，船舶要目，運賃情報

(B) 港湾荷役情報（積，揚地の両方）

(C) 船積貨物の各種ステータス情報

(D) その他関連情報

a．貿易取引に関連する改善，諸制度の行政情報

b．官庁の許認可手続き作業の進行情報

c．船積みのため積地倉庫の搬入から本船船積みまでの諸手続き進行情報

以上の点を全て，今回策定のシステムの中に組み込むことは作業量ならびに時間的な制約もあり，不可能であったが，これらのうち，輸出業者が必要とする書類の作成に共通データの繰返し利用による業務の軽減と，海貨通関業者および船会社からのフィード・バックされるデータ（情報）の有効利用により，

輸出業者自身の事務合理化もある程度期待できる。また将来はこのシステムとリンクするであろう他のサブシステム（例えば船舶動静，港湾情報システム等）が構築されれば，その効果は非常に大きなものになると思われる。

(2) 海貨通関業者が第２貿易情報システムに期待する事項

海貨通関業者は，輸出業者の受渡しファンクションに関連した業務および海貨通関業としての本来の業務のうち，本システムの有効活用により，通関および船積関係書類作成業務の合理化が相当期待できる。

このうち，特に船会社からのフィード・バック・データ（運賃関係データ）の早期入手が可能となればその効果は大きいものと思われる。

(3) 船会社が第２貿易情報システムに期待する事項

船会社は，本システムのなかでは，貿易関係データ（情報）処理における時系列的な面から見れば最後に位置し，貨物の船積情報の入手が，より早く，正確に，かつその入手媒体が直接コンピュータ・システムに入力できるものであれば，これによる揚地用（揚地通関用および，受荷主用）各種書類作成業務（ドキュメンティション処理）および企業内諸業務の合理化，省力化が期待できる。その一つの例としてＢ／Ｌの早期発行，および運賃関係情報の輸出業者への早期フィード・バックが考えられる。

表２－１　輸出ドキュメントと主要データ・エレメンツ

No.	Data Element	Remarks	Document										
				B/C (B)	C/I	S/I	P/L	M/I	B/C (G)	S/O	M/R	S/A	D/R	B/L
1	輸出者名	Shipper（荷送人）		○	○	○	○	○	○	○	○	○	○	○
2	Invoice No.				○	○	○							
3	Invoice 作成地				○	○	○							
4	Invoice 作成日				○	○	○							
5	Consigned to Messer	買主		○	○	○								
6	Consignee on B/L	荷受人		○	○	○				○	○	○	○	○
7	Notify Party	連絡先				○				○	○	○	○	○
8	輸出者コード	Shipper's Code							○	○	○	○	○	
9	海貨業者名	海貨業者				○				○	○	○	○	○
10	海貨業者コード									○	○	○	○	
11	S/O No.									○	○	○		○
12	B/L No.									○	○	○	○	○
13	Local Vessel	第１船　（在来船）				○				○	○	○		○
14	From	1st Loading Port（在来船）								○	○	○		○
15	Precarrier	Loading Port 迄の Carrier（コンテナ船）											○	○
16	Place of Receipt	荷受地（含む 1st Loading Port）											○	○
17	Port of Loading	積地			○	○	○	○	○	○	○	○	○	○
18	Port of Discharge	揚地			○	○	○	○	○	○	○	○	○	○
19	Transhipment at	接続地			○	○	○			○	○	○		○
20	Place of Delivery	荷渡地　（コンテナ船）				○							○	○
21	Final Destination	最終仕向地			○	○				○	○	○	○	○
22	Ocean Vessel	本船名			○	○	○	○	○	○	○	○	○	○
23	Voy No.	本船航海次号								○	○	○	○	○
24	Sailing Date	出帆年月日			○	○	○	○	○					
25	Marks and Nos	Cargo Mark and No.			○	○	○	○	○	○	○	○	○	○
26	Container No./Seal No.	（コンテナ船）											○	○
27	Commodity	B/L 面上の代表品目名		○	○	○	○	○	○	○	○	○	○	○
28	Description of Goods	取引上の品目名（含む，規格）		○	○		○		○					
29	統計品目コード	H T N		○					○	○	○	○	○	
30	Nos of Package	個数		○	○	○	○	○	○	○	○	○	○	○
31	Kind of Package	荷姿（梱包形態）		○	○	○	○	○	○	○	○	○	○	○
32	Quantity	取引上の数量		○	○		○		○					
33	Cargo Weight(Gross)	貨物の重量（含む，単位）					○		○	○	○	○	○	○
34	Cargo Measurement	貨物の容積（　〃　）					○			○	○	○	○	○
35	Total Nos of Package	貨物の総個数			○	○	○	○	○	○	○	○	○	○
36	Total Weight	（含む，単位）					○	○		○	○	○	○	○
37	Total Measurement	（　〃　）					○	○		○	○	○	○	○

No.	Data Elemnt	Remarks	Document											
				W/D (B)	C/I	S/I	P/L	M/L	E/D (C)	S/O	M/R	S/A	D/R	B/L
38	L/C No.			○	○	○								
39	Amount FOB Value	（含む，通貨）		○	○				○					
40	Freight and Charges											○	○	○
41	Revenue Ton											○	○	○
42	Tariff Rate	同盟タリフ				○						○	○	○
43	Per	Revenue Ton算出基準										○	○	○
44	Freight and Charges 支払条件	Prepaid/Collect				○						○	○	○
45	Prepaid Amount	（含む，Currency）										○	○	○
46	Collect Amount	（　〃　）										○	○	○
47	Exchange Rate	円貨換算用（ＴＴＳ）										○	○	○
48	Prepaid at	前払精算地				○						○	○	○
49	Payable at	後払精算地				○						○	○	○
50	Total Prepaid in Yen	前払の円貨総額										○	○	○
51	Place of B/L Issue	Ｂ／Ｌ発行地				○						○	○	○
52	B/L Issue Date	Ｂ／Ｌ発行年月日				○						○	○	○
53	Nos of Original B/L	Ｂ／Ｌ発行枚数				○						○	○	○
54	船会社名	本船の船会社				○				○	○	○	○	○
55	岸壁／荷扱識別符号									○	○	○		

E/D(B)；Expert Declaration (B)（銀行用輸出申告書）
C/I　；Commercial Invoice　（商業送状）
S/I　；Shipping Instruction　（船積依頼書）
P/L　；Packing list　（包装明細書）
M/L　；Weight/Measurement List
E/D(C)；Expert Declaration (C)　（通関用輸出申告書）
S/O　；Shipping Order　（船積指示書）
M/R　；Mate's Receipt　（本船受取書）
S/A　；Shipping Application　（船積申込書）
D/R　；Dock Receipt
B/L　；Bill of Lading　（船荷証券）

（注）　このデータ・エレメント分析表には，Insurance Application（保険申込書）のデータ・エレメントは含まれていない。

第３章　本システム策定の背景

才１章でも述べてある通り，本システムの策定は総合貿易情報システムの実現の可能性の追究と，実現するために必要な諸条件の設定等について，一つの具体的目標を決めて作業をする必要があった。また一つには，昭和４７年以来研究して来た総合貿易情報システム構想についても５年目を迎えるに当って，一応の締括りの意味も含めてシステム化策定を行うことになった。

この作業を実際に行うワーキング・グループとして昭和５１年５月２０，システム小委員会を発足させ，昭和５２年１月までに１７回の研究会を持って検討を行い，ここに一つの結果を取り纒めることが出来た。

3.1　システム小委員会の活動状況

システム小委員会の活動状況は次の通りである。

才１回　昭和５１年５月２０日
　　昭和５１年小委員会（旧ワーキング・グループ）運営方針の検討

才２回　―　〃　―６月４日
　　「共用貿易データ・エレメントおよび処理システム構想について」ヒヤリング及びフリー・ディスカッション

才３回　―〃―　６月１７日
　　才２貿易情報システムにおける各業界（商社，海貨通関業者，船会社）の問題点についての検討

才４回　―〃―　６月３０日
　　直貿メーカ（電気・通信）において輸出手続上抱えている問題点等のヒヤリング及び検討

才５回　―〃―　７月１６日
　　直貿メーカ（プラント，化学品）において輸出手続上抱えている問題点等のヒヤリング及び検討

第６回　―〃―　７月３０日

「第２貿易情報システムを中心に各業界から提示された問題点」の検討

第７回　―〃―　８月２０日

第２貿易情報システムにおける具体的な，輸出貨物と手続書類の流れについての検討

第８回　―〃―　９月１０日

第２貿易情報システムにおける輸出手続書類の分析

第９回　―〃―　９月２８日

同　上

第１０回　―〃―　１０月５日

第２貿易情報システムのサブシステムに関する調査研究

第１１回　―〃―　１０月２２日

各業界毎に必要とする書類及びその項目の抽出検討

第１２回　―〃―　１１月８日

各業界毎に必要とする書類及びその項目の分析

第１３回　―〃―　１１月２４日

第２貿易情報システムにおいて必要とする書類および項目の分析(1)

第１４回　―〃―　１２月１０日

同　上　(2)

第１５回　―〃―　１２月２２日

同　上　(3)

第１６回　昭和５２年１月１２日

同　上　(4)

第１７回　―〃―　１月２１日

同上(5)及び本小委員会作業に関する報告案について検討

3.2　システム小委員会において検討した内容

本章では，本システム小委員会が行った調査研究及び検討した具体的な問題についてその概要を述べる。

3.2.1　システム小委員会の作業に当つての基本方針

COTIS における総合貿易情報システムに関する調査・研究は昭和47年度より開始され，貿易業界全体を商取引関連のシステム（オ1貿易情報システム），輸出業者と船会社のシステム（オ2貿易情報システム），通関システム（オ3貿易情報システム），官庁の統計システム（オ4貿易情報システム）と四つのサブシステムに分け，一種の社会情報システムとして把らえて来た。具体的には貿易データ・バンクの構築を目指し，大きく分けて次の4点について調査研究を実施して来た。即ち

A　共用データ項目

B　国内外の貿易情報システムの動向調査

C　セキュリティー問題

D　情報処理技術

である。

しかるに昭和51年度の調査・研究方針としては事務局から提示された"昭和51年度 COTIS ワーキング・グループ（51年8月にシステム小委員会と改称）調査・研究項目（案）"に基づいて，前年迄の調査・研究を参考にして，オ2貿易情報システムを中心に，具体的なテーマを選択して調査・研究を進めていくこととした。

この調査・研究に関連して，国内の制度・法制，商習慣的な問題は，具体的なシステム設計・構想の組立ての際に必ず出て来る問題である。これについては，JASTPROの調査専門委員会で検討しているテーマとも共通点が多いと思われるので適宜連繋をとると共に，現状をベースとしたシステム設計，策定を前提とする。また，これと関連して，各業界，企業間の利害関

係等の問題も検討するものとする。

本システム小委員会の運営については，ＪＡＳＴＰＲＯのＡＤＰ専門委員会が，コードの標準化等に主眼を置いているのに対し当小委員会はＡＤＰ技術を用いた貿易情報処理システムの具体化に主眼を置く。また，社会情報システム指向という点で，行政官庁の問題が出て来るが，本システム小委員会がパイロット・システムを構想する場合，行政官庁主体のものと，業界主体としたものと，二つのアプローチが考えられるが，基本的には業界主体型として論議を進めて行き，対行政官庁の問題が発生した時点で改めて討議し，官庁より委員が参加しているＣＯＴＩＳ調査専門委員会へ提案して行くこととする。

以上の基本方針に基づいて作業を行った。

3. 2. 2　現状における各業界の問題点の把握

システム化構想またはシステム設計に際して，現状把握及び問題点の洗出しを行わずして実現性のあるシステム構想の組立て及び設計は出来ない。本システム小委員会も，この点に重点を置いて各業界，即ち

A　輸出業者（商社，メーカ）

B　海貨通関業者

C　船　会　社

のかかえている輸出における貿易手続き及びその処理業務上の問題を洗出し分析する作業を行った。問題点洗出し調査を行った対象会社数は

A　輸　出　業　者 …… 5社

1. 総　合　商　社 …… 2社

2. メ　ー　カ …… 3社（含むプラント）

B　海　貨　通　関　業 …… 2社

C　船　会　社 …… 2社

である。

これら各業界の問題点及び要望事項は表２－２に示す通りであるが，要約すると，それぞれ関連業界と官庁に対するものとに分けることが出来る。即ち

輸出業者については

対　船　会　社

対　官　庁

海貨通関業者においては主として

対輸出業者

対　船　会　社

船会社においては

対輸出業者

への問題点及び要望事項をかかえている。

これらの問題点及び要望事項の内，対官庁に対するものについては，基本方針に基づき別途検討又は，他のサブシステムとして改めて策定するか，あるいは制度・法制上の問題についてはＪＡＳＴＰＲＯと連携して対処することとし，その他それぞれ業界に対する問題点及び，要望事項については，想定されるシステム構築の段階で，解決出来るものは極力吸収する方向で分析を行った。

また，現状における輸出手続の径路についても調査し，これを"輸出手続経路図"として図２－５にまとめた。

３．２．３　想定されるシステムの目的の設定

オ２貿易情報システム化構想を検討する場合，帳票の統一，法的問題といったコンピュータ以前の問題点の簡易化，標準化という事もあるが，これらの事項は，ＪＡＳＴＰＲＯ等他の関係機関の検討にまつとして，本システム小委員会の検討すべき課題，目的はコンピュータ・システムを前提とする。これを利用してオ２貿易情報に係わる各業界が共通する情報を有効に利用して貿易手続の合理化のためのシステム開発の可能性を探ることである。情報

表２－２　「才２貿易情報システム」関係業界における問題点と要望事項（輸出業務）

	業界		対官庁	
	問題点	要望事項	問題点	要望事項
プラントメーカー	○Ｅ／Ｌ取得上，プラントの詳細が未決定のまま，大まかな金額で契約を行っている。	○諸手続きの進行，Ｅ／Ｌの取得状況の把握（対商社）	○プラントの仕様変更があった場合，延払い調書の再提出を求められる。	○延払い調書について，再提出ということではなく，アメンドという形式がとれないか。
	○プラント輸出では，無替為輸出が伴なうことが多い。	○最近の船舶，船腹動静の情報提供（対船社） ○レシーブドＢ／Ｌの発行（対船社）	○プラント用輸出統計品目コードが設けられてない為，通関手続きが繁雑となる。 ○プラントに対する考え方，統計品目区分の認識において通産省，大蔵省で相違があるのではないか。	○プラント統計品目コードの設置
	○単体でも1,600ｔを超える重量物があり，船型，仕向地の港湾施設状況の問題			
	○設計過程における仕様の変更，製作の遅延による船積み作業は繁雑なものとなる。		○各関係機関への無替為輸出申請において，内容に重複が多い。	○無替為輸出手続きの簡略化（船積の際，Ｅ／Ｄ，Ｂ／Ｌのヘッドに記入することによって，即時輸出可能とならないか，日銀への申請は省略できないか。）
	○エンジニアリング会社が直接，機器製作を行ってない為，船積み直前まで内容が		○工材等が分割輸出で，輸出完了途中で仕様変更があった場合，工材単価が変って	

	分らないことがある。		しまう為，通関時において説明に困る。 ○ＣＯＣＯＭ規制品目に対するＥ／Ｌのアメンド申請は船積み２０日以前，他品目は１５日前でないと間に合わないのが現状 ○プラントにおける官庁の許認可の問題として (1)役務輸出の許可 (2)ドロー・バックカーゴの許可 (3)外貨送金の許可（外国ライセンス利用，仲介貿易の場合）	○ＣＯＣＯＭ規制品目の輸出手続きの簡略化，規制緩和 ○各種の品目コードの国際的統一
化学品メーカー	○海外の市場調査は商社に頼っているのが現状 ○納期の問題もからみ，定常的取引のある客ではＬ／Ｃ到着以前に製造手配を行っている。		○円クレジット取引において相手国の通貨等で差が生じた場合，その変更手続きが複雑で手間がかかる。 ○ケニア，キューバ等特定な国では領事査証へのサインは第三者機関登録のものを要求される。	○円クレジットの変更手続きの簡略化

	業界		対官庁	
	問題点	要望事項	問題点	要望事項
	○東南アジアのバイヤー等で，フレート変更に関して差額負担の交渉がスムーズにいかない。 ○仕向地によって梱包形態，船選定の問題があり，商社海貨通関業者との緊密な連絡が必要。	○運賃のゼネラル・インクリース情報の早期アナウンス（対船社） ○連絡上のミスの解消	○通関の際，製品の成分表の提出を求められるが，アンダ・パテントの製品の場合は困る。 ○ライセンス製品に関して，通産省の輸出認可といった問題 ○化学品メーカーの場合，月に1度通産省へ指定統計の提出，総括的報告がある。	
商社	○成約，受渡時の各種書類のフォーマットの標準化を今後とも強力に推進する必要が痛感される。	○船舶，船腹の動静の提供（対船社）	○通産省，大蔵省（税関），各種民間団体（日本貿易会等）より統計資料を求められる。	○COCOM諸国に対する輸出可能範囲の最新情報の提供
その他・シッパー	○揚地の情報が明確でない場合，ブッキングが出来ない事がある。 ○各種同盟タリフの問題で貿易取引の採算計算が難しい。 ○荷主より輸出品の正確な情	○タリフの明解化（対船社） ○貨物の通関状況，ステータ	○輸出申請およびその許認可に時間がかかる。	

	報が取りにくい。	ス情報を把握し，提供願いたい。（対海貨）		
海貨通関業者	○他業界（商社，メーカー等のShipper）からの貿易情報及び貨物情報が業務の出発点であるため，それらの情報の正確性，内容の充実性及び入手時期が以降の業務処理に大きく影響する。 ○また現在事務処理上もS/I C/I，P/L 等の提出書式が多様であることが，機械化等による生産性の向上に障害となっている。	○貨物の搬入に際しては事前連絡を徹底させて欲しい。（特に大量貨物，重量物貨物）〔対荷主〕 ○通関書類は船社締切りの3日前までに現場店に受領したい。書類が遅れて緊急扱いとなるものが多い。（約30％）〔対荷主〕 ○危険品，有害品については規定の書類「危険品，有害物事前連絡表」を添付するようメーカーに指導願いたい。〔対荷主〕 ○搬入貨物のマーク・荷姿と書類面のマーク・荷姿が異なる場合が多い。〔対荷主〕 ○搬入貨物にGross W/T が表示されない貨物がときたまあるが，これは労働安全		○Plant貨物の場合，通産省と税関との統一見解 ○通関手続の簡素化

	業界		対官庁	
	問題点	要望事項	問題点	要望事項
		法に違反するので，メーカー経由梱包業者に指導願いたい。〔対荷主〕 ○欧州・中南米同盟に対する加入番号の連絡が不徹底である。〔対荷主〕 ○ＣＩＦ，Ｃ＆Ｆ契約の場合インボイスにＦＯＢ価格を表示願いたい。〔対荷主〕 ○現地サイトまでの一貫輸送契約の場合，現地での事故発生時の事後処理が問題化することが多いので商習慣となっている。貨物保険と共に現地輸送業務の求償権放棄特約の付保を徹底願いたい。〔対荷主〕 ○Ｂ／Ｌフォームのサイズ・書式の統一。 フォームが多種多様であるため機械化による事務合理化も困難である。		

		〔対船社〕 ○フレート計算に要する手数（船社との連絡事務を含めて）が多い。 料金体系の簡素化，税関品目コードとの連結フレート計算の機械化等の方法がないか。〔対船社〕 ○Bookingに関するトラブルが多い。 1.営業窓口と船積部門との連絡ミス 2.営業窓口と船積部門との間での締切日時に対する認識が異なり，船積時点でトラブルが発生することが多い。 〔対船社〕		
船　　社	○各同盟が多種多様のタリフを有しており，運賃計算が複雑。 ○タリフに当てはめ難い「商品名」がB／L上に記載さ	○B／L記載の「商品名」はタリフに当てはめ易いもの		

	業界		対官庁	
	問題点	要望事項	問題点	要望事項
	れることがあり運賃計算に困る。 ○揚地オプションの貨物がある場合，積載順等の問題があり，処理に困る。	の使用を願いたい。 〔対荷主・シッパー〕		
	○運賃が揚地清算の場合「DESTINATION」とだけの表示が多く，処理が複雑となるばかりでなく，収納に時間と手間がかかる。	○揚地清算の場合，清算地を明記して欲しい。 〔対荷主・シッパー〕		
	○荷が着いても，書類が届いていなかったり，品名，個数がブランクであったりする。→B／L作成が遅れる。	○ブッキングの精度があがらないか。 〔対荷主・シッパー〕		

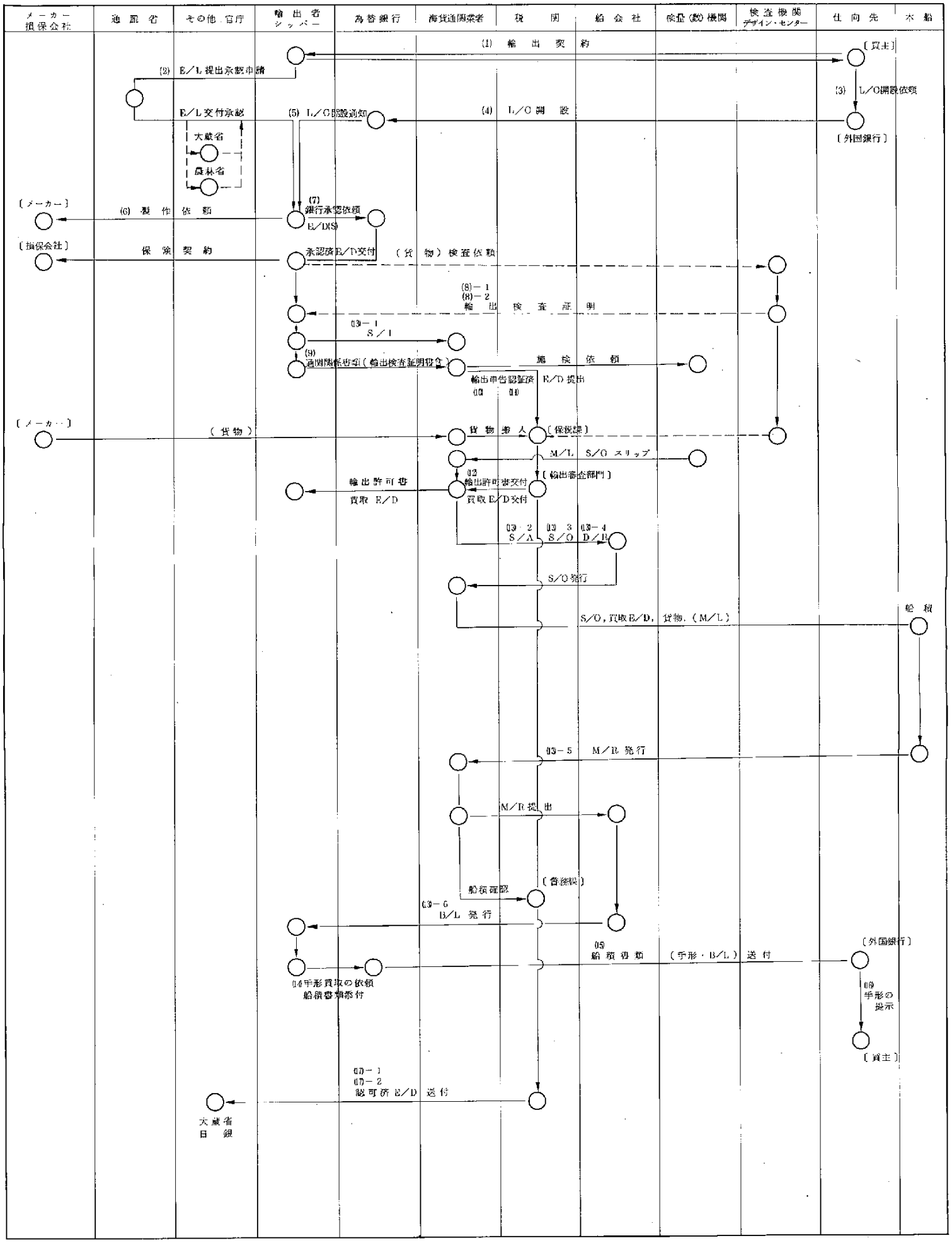

メーカー
損保会社
通産省
その他官庁
輸出者
シッパー
為替銀行
海貨通関業者
税関
船会社
検量(数)機関
検査機関
デザイン・センター
仕向先
本船
(1) 輸出契約
〔買主〕
(2) E/L提出承認申請
(3) L/C開設依頼
E/L交付承認
(5) L/C開設通知
(4) L/C開設
大蔵省
農林省
〔外国銀行〕
〔メーカー〕
(6) 製作依頼
(7)
銀行承認依頼
E/D(S)
〔損保会社〕
保険契約
承認済E/D交付
(貨物)検査依頼
(8)－1
(8)－2
輸出検査証明
(10)－1
S/I
(9)
通関関係書類(輸出検査証明書含)
検査依頼
輸出申告(証)済 E/D提出
(10) (11)
〔メーカー〕
(貨物)
貨物搬入
〔保税課〕
M/L S/O スリップ
(12)
輸出許可書交付
〔輸出審査部門〕
輸出許可書
買取E/D
買取E/D交付
(13)－2
S/A
(13)－3
S/O
(13)－4
D/R
S/O発行
船積
S/O, 買取E/D, 貨物, (M/L)
(13)－5 M/R発行
M/R提出
〔倉庫課〕
船積確認
(13)－6
B/L発行
(15)
船積書類 (手形・B/L) 送付
〔外国銀行〕
(14)手形買取の依頼
船積書類添付
(19)
手形の提示
〔買主〕
(17)－1
(17)－2
認可済E/D送付
大蔵省
日銀

図２－５　輸出手続経路図

の有効利用については，オ２貿易情報システムにおいて，各帳票の情報源となる輸出業者，仲介業である海貨通関業者，両業界からの集積情報をもとにB／Lを発行する船会社との間における情報の流れ（フィード・バックを含めて）と，これら情報の各業界における入力タイミング，フィード・バック・タイミング及び，データの訂正処理方法も含めて，これをシステム化することにより，企業内での情報の繰返し利用はもとより，業界相互間での授受により，共通データを繰り返し有効に利用することである。

また，業界相互間での情報の有効利用を計るためには，データ（情報）授受のインタフェースの問題もあり，システムはこれを十分にカバー出来るものでなければならない。しかしながら，今回の調査・研究においては残念ながら，この様な細かな点まで検討する時間的余裕がなかったので次の機会にゆずることとなった。

3．2．4　各業界において必要な書類と項目の抽出及び分析

前項において述べた業界相互間で有効利用する共通情報（データ）を抽出するためには，先ず各業界で必要とする書類の洗出しが先決である。この書類の洗出・分析についても前述の"輸出手続経路図"図２－５とも対応させ，それぞれの書類の作成者，提出先，他の利用者，また，その作成のタイミング等についても細目に渡って分析を行った（詳細は表２－３，４参照）。

その結果，輸出業者の取引成約後といっても相当膨大な書類が必要であることが判明した。しかし，これら全ての書類を，想定されるオ２貿易情報システムに組み入れることについては，検討の結果，色々問題があり，非現実的であるとの結論に達した。よってこれら書類の中から，オ２貿易情報システムに適用し得るものを更に選別抽出することとし，次の１２種類の書類を選択した。

A　輸出業者関係

(i)　コマーシャル・インボイス（C／I）

(ii) 銀行認証用輸出申告書（E／D Bank）

(iii) シッピング・インストラクション（S／I）

(iv) パッキング・リスト（P／L）

(v) インシュアランス・アプリケーション （I／A）

B 海貨通関業者及び船会社関係

(i) メジャー・リスト（M／L）

(ii) 通関用輸出申告書（E／D Customs）

(iii) シッピング・オーダー（S／O）

(iv) メイツ・レシート（M／R）

(v) シッピング・アプリケーション （S／A）

(vi) ドック・レシート（D／R）

(vii) 船荷証券（B／L）

尚，輸出業者関係で必要な書類の内でも，

- 輸出取引承認申請書
- 輸出承認申請書
- 輸出承認書
- 輸出検査証明書
- デザイン・商標判定書

等については別途検討することとして，取り敢えず才2貿易情報システムの対象から除いた。これは才2章の2.4項で述べた通りである。但し，これ等の書類は輸出業務及び手続上欠くことの出来ない重要なものであることから，何等かの形（例えば手続関係の他のサブシステム）で取り上げねばならないものである。

次にこれら必要書類に記載されている各項目，即ちデータ（情報）の抽出，分析を行ったが，それぞれの書類に記載されている項目は一見，同じ内容の様に思われても，各々の書類の持つ機能が異なるのと同様，必ずしも同一内容とは限らず，また，項目の見出し（表現）は簡単であっても，その欄に記

載される内容が極めて細かなものまで記述されていたりして，この項目の洗出し・分析，及びその項目のデフィニションの作業には多大の時間（５回に亘って討議した）を要した。

例えば，

- インシュアランス・アプリケーション　（Ｉ／Ａ）
- 銀行認証用輸出申告書（Ｅ／Ｄ　Bank ）
- 通関用輸出申告書（Ｅ／Ｄ　Custom ）

等にあってはそれぞれの項目が特殊で，特にＩ／Ａについては特殊の項目が多く，また同一項目であっても，スティタスによって記載する内容が全く異なってしまうものもあり，残念ながら，必要書類として取り上げたにもかかわらず，共通データの洗出し，及び定義付けの段階で，別途検討という事で除かざるを得なかったものもある。従って最終的には，データ・エレメント（項目）の分析対象として取り上げた書類はＣ／Ｉ以下１１種となった。

才一回目の項目洗出し分析においては，１３種類の書類で２２０項目を抽出したが，これを基に才２回目の検討分析により，デフィニションをも含めて１１種類（Ｉ／Ａを除いた）で約１２０項目にコンデンスされた（表２－５データ・エレメント一覧表参照）。

更にこれら項目を，少なくとも３種類の書類に繰返し記載されている項目を抽出したところ，才２章2.6：関連共通データで述べた如く，５５項目に集約された（表２－１参照）。

尚，当作業において項目の抽出と併せて，各項目の定義付けを行ったが，これは当システム小委員会の限られた委員の間で取り決めた約束にすぎず，それぞれの項目の定義付けについては改めて，関係業界の専門家を交えて行う必要があろう。

表２－３　輸出関係書類手続きの分析

番号	①	②	③	④
関係帳票	契約書	輸出承認申請書	信用状開設依頼書	（開設通知依頼）
目的	契約内容の確定	特定輸出内容の承認申請	信用状（Ｌ／Ｃ）の開設を依頼（信用状への依頼内容を呈示）	Ｌ／Ｃ開設銀行が通知銀行を通じて輸出者へＬ／Ｃ開設を通知
作成者（申請者）	輸出者	輸出者	輸入者	Ｌ／Ｃ開設銀行
作成方法	タイプ（カーボン・コピー）サイン	タイプ（カーボン・コピー）	タイプ	署名鑑交換による電信伝達が多い
使用様式（枚数）	自由 (2)	Ｔ１０１５ (4)	開設銀行様式	
作成時期	契約時	契約前後	契約直後	Ｌ／Ｃ開設直後
作成労力（Man × Hour）				
提出先（窓口）	輸入者（バイヤー）	通産省又は地方通産局の商品輸出担当課	開設銀行	輸出国通知銀行（電信）
戻し先	――――	輸出者	――――	――――
連絡先	――――	――――	――――	開設銀行→通知銀行→輸出者
手続処理に要する日数	――――			
承認／決済主体	輸出者／輸入者	通産大臣又は各税関長及び関係大臣	開設銀行	――――
提出先における処理	ファイル	通産大臣，各税関長の承認，関係大臣の同意後，押印	輸入者の信用状態を審査し，Ｌ／Ｃを開設する。	――――
書類の利用形態	契約内容の確認	輸出申告書に添付して外為銀行へ提出する。その後通関書類に添付	Ｌ／Ｃ開設控え	輸出者は商品製造手配
問題点				
備考		次のようなもの時に必要 ○戦略物資 ○国連決議物資 ○特定仕向地向 ○特定契約 ○特定決済方法 その他		通知銀行が，そのＬ／Ｃの引受け保証を確認する場合がある。（確認銀行）

番　　号	⑤	⑥	⑦	⑧－1
関係帳票	商業信用状	注　文　書	輸出申告書 （銀行認証用）	輸出検査証明書
目　　的	開設銀行が輸入代金の支払いを保証する。	輸出者が商社である場合に製品の発注を行う。	輸出の内容を諸官庁へ届け出るとともに確認を受ける。	粗悪品の輸出チェック
作成者 （申請者）	L／C開設銀行	輸　出　者	輸　出　者	メーカー
作業方法	様式にタイプ，サイン	タ　イ　プ	タイプ（カーボン，コピー）	タイプ，検査機関押印
使用様式（枚数）	１００信用状統一規則	自　　由	(4)	施規様式　1
作成時期	信用状開設依頼の後	L／C入手後	契約後かつ，承認済輸出承認申請書 入手後	梱　包　前
作成労力 （Man×Hour）				
提出先 （窓　口）	輸出者（通知銀行経由エアメイル）	製造メーカー	外国為替公認銀行	政府検査機関及び民間検査協会
戻し先	――――	――――	輸　出　者	輸　出　者
連絡先	――――	――――	――――	
手続処理に要する日数				
承認／決済主体	開　設　銀　行	――――	外為銀行（日銀）	機関，協会等の長
提出先における処理	荷為替手形買取時まで保管	確　　認 フ　ァ　イ　ル 製　造　開　始	輸出者へ２通押印の上返却し，１通自行控え１通を通産省又は地方通産局へ提出する。	書　類　審　査 現　物　審　査
書類の利用形態	荷為替手形買取時に添付	――――	通関書類に添付	通関書類に添付
問　題　点				
備　　考			添付書類 ○支払方法を証明する書類（承認済輸出承認申請書等）	輸出検査品令 （合計３３４品目）

			通関関係書類	
番　　号	⑧－2	⑨	⑨－1	⑨－2
関係書類	デザイン・商標判定書	通関書類	商業送状	梱包明細書
目的	模倣品の輸出のチェック	貨物の輸出通関のため関係書類を一式そろえる。	輸出商品の明細を表示する。	梱包の内容，数通荷印等を示す。
作成者（申請者）	メーカー	輸出者	⟶	⟶
作成方法	タイプ，デザイン・センター等押印		タイプ，サイン	タイプ，サイン（ゴム印）
使用様式（枚数）			自由（最低6枚）	
作成時期	通関申告時までに作成	輸出通関の申告まで	輸出申告Bの作成時	梱包後
作成労力（Man×Hour）				
提出先（窓口）	日本機械デザイン・センター，日本雑貨振興センター，その他	各税関	⟶	⟶
戻し先	メーカー	海貨業経由輸出者	⟶	⟶
連絡先				
手続処理に要する日数				
承認／決済主体	機械・センター等の長	税関長		
提出先における処理	登録台帳へ記載認定証明書の発行機関誌へ公示	海貨業へ返却	審査後ファイル	審査後海貨業へ返却
書類の利用形態				
問題点				
備考				

	通関書類			
番号	⑩	⑪	⑫	⑬－1
関係帳票	輸出申告書（通関用）	為替銀行買取用通関済輸出申告書（銀行認証用）	輸出許可書	船積依頼書（S／I）
目的	通関申告用 統計の為	銀行認証済輸出申告書を税関で審査	通関を行ない輸出を許可する	船荷証券作成の為の船積依頼書
作成者（申請者）	海貨業者			輸出者
作成方法	タイプ（カーボン） 通関士記名押印	⑦を税関で審査の上押印する	⑩に押印	タイプ（カーボン）
使用様式（枚数）	C－5010 (3)	⑦に同じ	⑩に同じ	自由 (3)
作成時期	通関申告時	通関後	輸出審査後	船積書類作成後
作成労力（Man×Hour）				
提出先（窓口）	税関			海貨業者
戻し先	海貨業経由輸出者へ	→	→	
連絡先	―――	―――	―――	
手続処理に要する日数	48時間			
承認／決済主体	税関長	→	→	
提出先における処理	審査押印	銀行認証用E／Dは日銀へ	―――	これを基にS／A，S／O，B／Lを作成船社へ提出
書類の利用形態	通関済EDとして大蔵省関税局へ	手形買取用	無為替ライセンス用口銭取得用	
問題点				
備考				

番号	⑬－2	⑬－3	⑬－4	⑬－5
	船積関係書類			
関係帳票	船積申込書（S／A）	船積指図書（S／O）	貨物受取書（D／R）	本船受取書（M／R） Mate's Receipt
目的	輸出船積申込	輸出船積指図	コンテナー船用 輸出船積受取	本船側の輸出 貨物の受領書
作成者 （申請者）	海貨業者	海貨業者	⟶	海貨業者
作成方法	ワンライテングでタイプ（邦船5社のみ）	ワンライテングでタイプ（邦船5社）	⟶	S／Oと共にタイプ
使用様式（枚数）	邦船5社(1)	2～3枚（含コピー）	7 枚	2枚（含コピー）
作成時期	検量結果判明 運賃計算後	検量結果判明後	検量結果判明 運賃計算後	S／O作成時
作成労力 （Man×Hour）	15分	10分	15分	10分
提出先 （窓口）	船社	船社	CFS，CY経由 船社	一等航海士
戻し先	———	———	———	海貨業→船社
連絡先	———	———	———	———
手続処理に要する日数	2 日	2 日	1 日	2 日
承認／決済主体	船社の担当課で確認	船社の担当課で確認	ターミナル・オペレータ CFSオペレータ （サイナー）	
提出先における処理	船社内処理	船社内処理	⟶	船社内保管
書類の利用形態				
問題点		邦船5社が使用している様にOne Writing方式にして欲しい。さらに又，各社共通の様式が良い。		S／Oに同じ
備考				

番　　号	⑬－6	⑭	⑮	⑯
関係帳票	船荷証券	荷為替手形買取		荷為替手形
目的	輸出商品を担保とする有価証券	荷為替手形の買取りを船積書類一式を添えて外為銀行へ依頼する。	荷為替買取銀行よりL／C開設銀行へ荷為替手形，L／C等輸出書類を送付する。	輸送貨物を担保として振出される手形
作成者（申請者）	⟶	輸出者		輸出者
作成方法	タイプ	タイプ		タイプ，サイン
使用様式（枚数）	20～50枚			手形法による (2)
作成時期	検量結果判明運賃計算後	船積が完了して買取用書類が揃った時点		船荷証券入手後
作成労力（Man×Hour）	15分			
提出先（窓口）	船社	外為銀行	本邦外為銀行 ↓ 外国外為銀行	輸入者
戻し先	海貨業→輸出者			
連絡先				
手続処理に要する日数	1日			
承認／決済主体	外為銀行			———
提出先における処理	荷主に対して発行，コピー保管	承認許可済輸出申告書をチェックの上買取りに応じる。		手形に対し，代金を支払うという約束のもとに船荷証券を輸入者が引受ける。
書類の利用形態				
問題点				
備考				

番　　号	⑰			
関係帳票	輸出申告書 （銀行認証用）			
目　　的	当初の銀行認証と通関後の輸出内容の照合，チェック			
作成者 （申請者）	――――			
作成方法	――――			
使用様式（枚数）	⑧と同じ			
作成時期	⑧と同じ			
作成労力 （Man×Hour）				
提出先 （窓　口）	日　　銀			
戻し先				
連絡先				
手続処理に要する日数				
承認／決済主体	日　　銀			
提出先における処理	承認銀行経由（銀行認証用）と（買取用）の輸出申告書を照合，チェックする。			
書類の利用形態				
問題点				
備　　考				

表２－４　必要書類の一覧表

	帳票名	作成者	利用者又は受領者	第二次情報システムの要否	利用方法の想定
1	契約書	輸出者	契約当事者双方	否	
2－1	輸出承認申請書	同上	輸出者，為替取扱銀行，通産省，大蔵省，海貨業者，税関	要	輸出者の申請手続の簡素化が図れる。各官公署がシステム的に連繋された情報を利用して認許可業務を行い，管理機能も果せる。
2－2	輸出取引承認申請書	同上	輸出者，輸出組合	否	
3	信用状開設依頼書	輸入者	L／C開設銀行	否	
4	L／C開設通知依頼	L／C開設銀行	被通知銀行，輸出者	否	
5	商業信用状（L／C）	同上	通産省，輸出者，為替取扱銀行，大蔵省，海貨業者	要	L／Cそのものの全文が必要なのは輸出者，外為銀行であり，大蔵省，税関は金額決済経路別分類など特定の管理目的に叶える項目だけでよい。
6	注文書	輸出者	製造業者，製品供給者（輸出者の仕入先）	否	
7	輸出申告書（銀行認証用）	同上	輸出者，外為銀行，日銀，通産，大蔵，海貨業者，税関	要	全項目に亘って多角的に活用される。
8－1	輸出検査証明書	製品供給者（メーカー）	海貨業者，税関，メーカー，政府検査機関，民間検査協会，輸出者	要	
8－2	デザイン，商標判定書	同上	輸出者，海貨業者，日本機械デザインセンター，日本雑貨振興センター	要	
9－1	商業送状	輸出者	海貨業者，船社，商工会議所，領事館，輸出者，取引相手先，税関，為替取扱銀行	要	全項目を必要とするのは輸出者，取引相手先，為替取扱銀行，海貨業者，税関であり，有効に活用できるItemではないか。
9－2	梱包明細書	輸出者（梱包業者）	輸出者，梱包業者，メーカー，検量業者，取引相手先，海貨業者，税関，為替取扱銀行，船社	要	商業送り状で大体カバーされるので添付書類としての価値判断による。
10	輸出申告書（通関用）	海貨業者	輸出者，税関，大蔵省関税局，海貨業者	要	17のfeed back dataとして全利用者に有効活用が期待出来る。
11－1 11－2	為替銀行買取用通関済輸出申告書（銀行認証用）	輸出者	(11-1)税関，輸出者，為替銀行，日銀 (11-2)税関，日銀	要	

12	輸出許可書	海貨業者	税関，海貨業者，輸出者，エージェント，船社（ターミナル，オペレータ，CFSオペレータ）	要	
13－1	S／I	輸出者	海貨業者，輸出者	要	輸出者，海貨業者，船社に限定されるのではないか。
13－2	S／A	海貨業者	船会社，海貨業者	要	
13－3	S／O	同上（発行者船社）	船会社，海貨業者，エージェント	要	
13－4	D／R	同上（発行者船社）	船社（ターミナル，CFSオペレータを含む）海貨業者	要	
13－5	M／R（本船受取書）	同上（発行者船社）	S／Oと同じ（船社，海貨業者）	要	
13－6	船荷証券（B／L）	船会社	輸出者，輸入者，為替取扱銀行，船会社，海貨業者	要	利用者が限定される。
16	荷為替手形	輸出者	輸入者，為替取扱銀行	否	
17－2	輸出申告書（銀行認証用）	同上	為替取扱銀行	要	
18	保険申込書	同上	保険会社，為替取扱銀行，税関，通産省	要	

データ・エレメント一覧表

表2－5　(Shipping Documents and Data Elements)

No.	項　　目	REMARKS	C/I	E/D (B)	S/I	P/L	M/L	E/D (O)	S/O	M/R	S/A	D/R	B/L
1	輸出者名	Shipper(荷送人)	○	○	○	○	○	○	○	○	○	○	○
2	輸出者署名		○	○	○	○							
3	Invoice No.		○		○	○							
4	Invoice 作成地		○		○	○							
5	〃　作成日		○		○	○							
6	Contract No.		○										
7	Contract Date		○										
8	Buyer's Order No.		○			○							
9	Consigned to Messer	買　主	○	○	○								
10	Consignee on B/L	荷受人	○	○	○				○	○	○	○	○
11	Notify Party				○				○	○	○	○	○
12	輸出者コード	Shippers Code						○	○	○	○	○	
13	海貨業者名	Forwarder							○	○	○	○	○
14	〃　コード	Forwarder Code							○	○	○	○	
15	S/O No.								○	○	○		○
16	B/L No.								○	○	○	○	○
17	Booking No.											○	
18	Local Vessel	在来船(第一船)							○	○	○		○
19	From	在来船 1st Loading Port							○	○	○		○
20	Pre-carrier	コンテナ船										○	○
21	Place of Receipt	荷受地(含む1st L.Port)										○	○
22	Port of Loading	積　地	○		○	○	○	○	○	○	○	○	○
23	Port of Discharge	揚　地	○		○	○	○	○	○	○	○	○	○
24	Transhipment at	接続地(在来船)	○		○	○			○	○	○		○
25	Place of Delivery	荷受地(コンテナ)										○	○
26	Final Destination	仕向地							○	○	○	○	○

No.	項目	REMARKS	C/I	E/D(B)	S/I	P/L	M/L	E/D(O)	S/O	M/R	S/A	D/R	B/L
27	仕向国			○				○					
28	Ocean Vessel	船名	○		○	○	○	○	○	○	○	○	○
29	Voy No.	航海次号							○	○	○	○	○
30	Sailing Date	出帆年月日	○		○	○	○	○					
31	Marks & Nos		○		○	○	○	○	○	○	○	○	○
32	Container No./Seal No.	コンテナ										○	○
33	Description of Goods	品目名	○	○	○	○	○	○	○	○	○	○	○
34	統計品目コード	(BTN)		○				○	○	○	○	○	
35	Nos of Package	個数	○	○	○	○	○	○	○	○	○	○	○
36	Kind of Package	荷姿	○	○	○	○	○	○	○	○	○	○	○
37	Cargo Weight (Net)	(含む単位)				○			※△	※△	※△	※△	※△
38	Cargo Weight (Gross)	(〃)				○		○	○	○	○	○	○
39	Cargo Measurement	(〃)				○			○	○	○	○	○
40	Cargo Measure	縦, 横, 高の寸法					○						
41	Total No. of Package						○		○	○	○	○	○
42	Total Weight	(含む単位)					○		○	○	○	○	○
43	Total Measurement	(〃)					○		○	○	○	○	○
44	L/C No.		○	○	○								
45	L/C 発行銀行		○	○									
46	Unit Price Per		○										
47	Amount FOB VAL		○	○				○					
48	〃 建値		○	○									
49	Freight of Charges										○	○	○
50	Revenue Ton										○	○	○
51	Tariff Rate				○						○	○	○
52	Per	Revenue Ton 算出基準									○	○	○
53	Freight 支払条件	Prepaid Collect			○						○	○	○
54	Prepaid	(Amount of Currency)									○	○	○
55	Collect	(〃)									○	○	○

※印はパレタイズ・カーゴ

No.	項　　目	REMARKS	C／I	E／D(B)	S／I	P／L	M／L	E／D(C)	S／O	M／R	S／A	D／R	B／L
56	Exchange Rate	（TTS）									○	○	○
57	Prepaid at	前払精算地									○	○	○
58	Payable at	後払精算地									○	○	○
59	Total Prepaid in Yen										○	○	○
60	Place of B/L Issue	B／L 発行地			○						○	○	○
61	B/L Issue Date	B／L 発行年月日			○						○	○	○
62	Number of Original B/L	B／L 発行枚数			○						○	○	○
63	Weight/Measure List 枚数				○								
64	船会社名				○				○	○	○	○	○
65	CY／CFS Service Type	コンテナ			○							○	
66	Type of Goods											○	
67	Inland Carrier at D.Port	コンテナ										○	
68	Reefer Temp				○				○	○	○	○	○
69	Dangerous Cargo Label											○	
70	岸壁／船積識符号								○	○	○		
71	Ware House				○								
72	Cargo Ready				○								
73	Maker 名				○								
74	L／C Latest Date	（船積 Date）			○								
75	L／C Expiry Date				○								
76	Delivery Terms				○								
77	E／Lに関するRemarks				○								
78	M／L 作成年月日						○						
79	M／L No.	（発行番号）					○						
80	検量場所						○						
81	〃　年月日						○						
82	Measurement Per Package						○						
83	Measurement Total	Lot 別Measurement Total					○						
84	Weight Per Package						○						

No.	項目	REMARKS	C/I	E/D(B)	S/I	P/L	M/L	E/D(C)	S/O	M/R	S/A	D/R	B/L
85	Weight Totat	Lot 別 Weight Total					○						
86	税関名							○					
87	E/D 申告年月日							○					
88	通関業者名							○					
89	本船扱/ふ中扱							○					
90	E/D 申告番号							○					
91	積込港符号							○					
92	船(機)籍符号							○					
93	貿易形態別符号							○					
94	仕向国符号							○					
95	E/D 添付書類関係							○					
96	申告書枚数							○					
97	法令関係							○					
98	蔵置場所							○					
99	(L/C)決済条件			○									
100	承認又は許可番号	E/D (Bank)		○				○					
101	銀行認証年月日	—〃—		○									
102	銀行認証番号			○				○					
103	外国為替種類			○									
104	外国為替手形期限			○									
105	信用状内容未使用残高			○									
106	信用状授受年月日			○									
107	信用状有効期限			○									
108	Bank E/D 参考事項			○									
109	認証銀行名			○									
110	—〃— 署名			○									
111	統計用コード ①~⑥	(通産省用)		○									
112	外国為替決済方法 L/C			○									
113	— 〃 — その他			○									

No.	項　　目	REMARKS	C／I	E／D(B)	S／I	P／L	M／L	E／D(C)	S／O	M／R	S／A	D／R	B／L
114	外国為替決済 L／C　買取日			○									
115	〃　その他			○									
116	〃　金　額　L／C			○									
117	〃　その他			○									
118	税関輸出許可年月日			○									
119	税関輸出許可番号			○									
120	決済銀行　記名／署名			○									
121	US$　換　算　額			○									
122	Bank　E／D用 備考			○									

第4章　本システム策定における問題点と今後の課題

第2貿易情報システムの実現性の検討ならびに，本システムの策定に先立って，当システム小委員会としては，先ず現状の貿易実務，貿易に係わる諸手続きの実態とその問題点を把握することが必要であるとのことから，輸出業者，海貨通関業者および船会社について調査研究を行った。

この実態調査の結果，次の問題点があげられた。

(1)　官庁に対する許認可，諸手続きに係わる法制上の問題。

(2)　商習慣上の問題，または関係業界に係わる問題。

(3)　必要とされる関連サブシステムの問題。

(4)　その他書類フォーマット，コード等の標準化の問題。

これらの問題について，本システム策定に際し，法規制度，商習慣に関しては，今後の解決にゆだねることとして，現行のなかで，また，関連サブシステムについては，将来同システムが構築された時点で接続することを前提とした。

なお，本システムの範囲については，輸出業者の成約後から船積・船荷証券（B／L）の発行までとし，その範囲を限定したことにより，システムの機能とその効果も，初期の構想よりは限定された狭いものになった。

しかしながら，本システムを，一つのパイロット・システムとして考えるならば，前述の諸問題が逐次解決されることにより，順次システムの範囲の拡大が図られ，広く業界に利用される可能性を持っていると思われる。

以下に，前記の問題点について述べる。

4.1　許認可諸手続きに係わる法制上の問題とその改善要望事項

輸出業務における許認可手続きに係わる法制上の問題として業界別に要約すると次の通りである。

A．輸出業者（プラント・メーカ）

①　プラントの仕様変更があった場合，延払い調書の再提出を要求され業務

が重複し，煩雑となっている。また，工材等が分割輸出の場合，輸出完了途中で仕様変更があった場合，工材単価が変ってしまうため，通関時に種々と問題が生じている。

② プラント輸出では，無為替輸出がともなうことが多いが，各関係機関への無為替輸出申請において内容の重複が多い。

③ プラントに対する考え方，統計品目区分の認識において，関係官庁間で相違があるように見受けられる。また，プラント用輸出統計品目コードが設けられていない。

④ プラントにおける官庁の許認可の問題として，

a．役務輸出の許可

b．ドロー・バック・カーゴの許可

があり非常に煩雑である。

B．輸出業者（商社およびその他輸出業者）

① COCOM規制品目に対するE／Lのアメンド申請は船積み２０日以前，他品目は１５日前でないと間に合わないことがある。（これはプラント・メーカにおいても同様である）

② 円クレジット取引において相手国の通貨等で差が生じた場合，その変更手続きが複雑で手間がかかる。

③ 通関の際，製品の成分表（例えば化学製品の場合）の提出を要求されるが，アンダ・パテントの製品の場合問題がある。

④ E／Lに該当する製品に関して通産省の輸出認可に時間がかかる。

⑤ その他，全般的に輸出申請およびその許認可に時間がかかりすぎる。

⑥ 関係官庁から種々の統計資料の提出を要求され相当の負担がかかっている。

C．海貨通関業者

一般に通関手続き業務が複雑である。これ等問題点に対する改善要望としては，

a．延払い調書について，再提出ということではなく，訂正（アメンド）という形式がとれないか。

b．無為替輸出手続きの簡略化。（船積の際E／D，B／Lのヘッドに記入することによって，即時輸出可能とならないか，また日銀への申請は省略できないか）

c．COCOM規制品目の輸出手続きの簡略化，規制緩和，また輸出許可範囲の最新情報の早期提供。

d．プラント統計品目コードの設定。

e．円クレジットの変更手続きの簡略化。

f．通関手続きの簡略化。

等があげられる。

4.2 商習慣上の問題，または関連業界に係わる問題とその改善要望事項

商習慣上，または，関連業界に係わる問題を各業界別に要約すると，次の様なものがあげられる。

A．輸出業者（プラント・メーカ）

① 単体でも1,600トンを超える重量物があり，船型，仕向地の港湾施設状況の問題がからんでくる。

② 設計過程における仕様変更，製作の遅延により，船積作業が煩雑なものとなる。

③ 揚地の情報が明確でなかったり，船舶動静の情報が十分でない場合に，ブッキングできないことがある。

④ 各同盟タリフの問題で貿易取引きの採算計算が難かしい。

これらの問題点に対しての要望事項としては，

a．最新の船舶，船腹等の動静情報の提供。……対船会社

b．レシーブド・B／Lの発行。……対船会社

c．同盟運賃タリフの簡略化と，運賃ゼネラル・インクリーズ情報の早期

通知。……対船会社

d．貨物の通関状況，およびステータス情報の把握と提供。……対海貨通関業者

等があげられる。

B．海貨通関業者

① 輸出業者からの正確な貿易情報および貨物情報が遅いため，これら情報の入手以降の業務処理に色々と影響することが多い。

② 各同盟の運賃タリフが複雑，難解で，フレート計算に多大の手間がかかっている。

③ 貨物の搬入に際して事前連絡がないことが多く業務に支障をきたしている。また，搬入貨物にGROSS WEIGHTの表示のないものがあり，非常に困っている。

これらの問題点に対しての要望事項として，

a．貿易情報，貨物情報等，正確かつ，タイミングよく提供してほしい。……対輸出業者。

b．通関関係書類は船会社締切りの3日前までに受領したい（書類が遅れて緊急扱いのものが約30％もある）。……対輸出業者。

c．危険品，有害品については，規定の書類「危険品，有害物事前連絡表」を添付する様，メーカに指導願いたい。……対輸出業者。

d．貨物の搬入に際しては，必ず事前連絡をする（特に大量貨物や重量物貨物）と共に，搬入貨物には必ずGROSS WEIGHTを表示願いたい。……対輸出業者

e．欧州・中南米同盟に対する加入者番号の連絡を徹底してほしい。……対輸出業者。

f．CIF，C&F契約の場合は，インボイス上に必ずFOB VALUEを表示願いたい。……対輸出業者。

g．運賃タリフの簡略化。……対船会社

h．BOOKINGに関し，

㈠　営業窓口と船積部門との連絡

㈡　営業窓口と船積部門との間での締切日時についての連絡を十分にとって，船積時点でのトラブルを無くしてほしい。……対船会社

C．船　会　社

①　しばしばかけ込み貨物があって船積業務に支障を来たすことが多い。

②　揚地オプション貨物については，船積業務に支障をきたしたり，色々と問題がある。

③　運賃の精算地が不明。または揚地精算の場合「DESTI NATION」のものが殆どで，処理が繁雑になったり，収納時間がかかる。

④　貨物が船側やターミナルに着いても書類が届いていなかったり，品名，数量が不明のものがあってB／L発行が遅れることがある。これらの問題に対する要望事項としては，

a．貨物情報，書類は正確にかつ早めに提供願いたい。……対輸出業者／海貨業者

b．B／L記載の商品名はタリフに当てはめやすい様に表示願いたい。……対輸出業者／海貨業者

c．運賃揚地精算の場合，精算地を明記してほしい。……対輸出業者

d．BOOKINGの精度を上げられないか。……対輸出業者（海貨業者）

等があげられる。

4.3　必要とされる関連サブ・システムの問題

第2貿易情報システム策定に際して色々検討を行った中で，現状における問題点の洗い出しと，本項における必要関連サブ・システムの問題が大きなファクターとしてクローズアップされた。

特に第2貿易情報システムを有効に機能させるためには，本第2貿易システム単独では非常に難かしいのではないか。また単独では余り効果は期待出来な

いのではないかという点に論議が集中した。

しかしながら，今直ちに必要関連サブシステムが構築されるわけではなく，今後並行的に，又は，第2貿易情報システム策定後，引続き検討を行うか，いずれにしても，先ず本第2システムの必要性を浮彫りに出来るとの判断で作業を行った。

ここで必要関連サブシステムとして考えられるものは，

① 代金決済に係わるサブシステム

② 船舶動静に係わるサブシステム

③ 港湾荷役に係わるサブシステム

④ 通関に係わるサブシステム

⑤ 官庁許認手続に係わるサブシステム

等である。なお，第1および第3貿易情報システムは当然のことながら必要関連サブシステムとして考えた。

これら各サブシステムが相互にうまく機能して初めて，本第2貿易情報システムの効果が期待されるものである。

4.4 その他，書類フォーマットの標準化の問題

この問題は，コンピュータ・システム以前の問題であるが，本システムを十分に機能させるためには必要な条件である。

書類フォーマットの標準化については，ここ数年来，JASTPRO（旧貿標より継続）にて検討を行っており，近々日本スタンダード・マスターが完成する予定とのことである。今後もJASTPROにおける同作業に期待したい。

第5章　ま と め

第2貿易情報システムの策定を行うため，昭和51年5月以降，52年1月迄に17回のシステム小委員会を開催し，作業を行って来たが，特に調査の段階で，調査すればする程，現状における問題点が余りにも多いことが判明した。しかもこれらの問題点が，殆どのものが，いわゆるコンピュータ・システム以前のもので，しかもどれ一つとして一朝一夕には解決出来る様なものではなかった。

この様な状況のもとで，実現性のある貿易情報システムを策定することは，正直なところ非常に難かしい問題であった。

しかしながら一つのパイロット・システムとして実現性を見い出すことは可能であるとの判断から，また問題点は問題点として別の機会に改めて検討するなり，あるいは官庁，他の関連機関の検討を待つとして，想定される第2貿易情報システムの策定を行った。従ってシステムの機能，範囲も相当に限定された狭いものとなってしまった。しかも，第2貿易情報システムの枠組みの検討にとどまり，具体的なまた，技術的な問題を検討する時間的余裕がなかった。

今後は，本システムの枠組の中で，具体的な問題の検討，技術面の検討を加え，第2貿易情報システムを設計する必要がある。

また，出来ることならば，何らかの形で実験を行い，真のシステムの実現性を確かめることが望ましい。そして，この実験結果をもとに，システムの範囲，機能等枠組も修正し，より現実的なシステムの構築を検討すべきと考える。

以　上

第　3　部

海運貨物取引関係情報システムの調査研究

1. 序論 — 海運貨物取引関係情報システムの概要

1.1. 実験システムのモデル設定

当調査研究においては，過去5年間にわたり，総合貿易情報システムの概念のもとに第2貿易情報システムの輸出入業務の現状分析を行って来た。この結果，海港における貿易業務の実態を明確にし，各種業務のフローと問題点の摘出，データ・エレメンツの時系列的配列相互関係データサイズの検討等については，一応の結論を得ることができた。今回の調査研究は，これらの過去の調査の結論にもとづき，データベースによる実験システムの可能性を検討することである。

調査研究が，この段階に達した場合に必要なことは，新しく検討するシステムが，ある程度の実施可能な条件を持たなければならないこと，すなわち実用可能の条件を与えることであると考えられる。この観点から，報告書の作成とは別に，その背景となる環境条件の検討と確認とが必要となった。これについて，第1の問題は，貿易情報システムと港湾情報システムとの概念の混乱を整理し，両者の関係を明確に区分することである。第2の問題は，わが国の港湾においては，欧米の港湾と異なって，極めて複雑な業態を持っていることの認識である。

以上のような予備的，ないしは基礎的研究を経た後に，今回実施する研究調査のモデルを，どこを対象として考えるかという問題があった。これについては，横浜に建設中の外貿埠頭を対象としてとりあげた。その理由とするところは，次の通りである。

a) 新しく建設中の埠頭であるため新規の構想を設定するのに適している。

b) 外貿埠頭公団バースであるため，業者の専用使用の形をとり，公共埠頭と違って業務が比較的単純であり，且つ純粋に民間の立場で，言葉を変えて言えば，純粋に貿易情報システムの立場から，システムの開発が可能である。

c) 埠頭建設費の高騰のためリース料金が値上げされ，業者として徹底した業務の合理化を必要としている。

このような条件のもとにおいて，何よりも先ずこのシステムの調査研究を進めるために関係者の了解と協力を得ることが必要であったが，この問題に関し，関係当局および各業者間の了解と協力が得られたことは幸いであった。

以上のような努力によって，環境条件がひとまず整備されたことは，前もって整えられねばならない最少限の前提であった。

1.2 本システム開発の基本方針

1.2.1 システム開発の対象と範囲

将来構想をも含めたこのシステムの考え方は，かなり壮大なものである。しかしながら，今回のシステム開発の対象となるものは，その中で最も基本的なものであると考えられるドキュメンテーションと貨物管理のシステムである。但し，これは概念的区分で，実際の処理は両者を統一的に処理しなければならないであろう。

ドキュメンテーションは，本来海貨通関業者の業務であるが，ライナーバースに進出する一種業者（エゼント業者）もまた社内に海貨通関業の免許を持っているので，その基本的部分は共同利用センターにおいて，共同で利用することができる。現在財団法人日本貿易関係手続簡易化協会（JASTPRO）において作成中の標準帖票を使用することを前提として考察する。ドキュメンテーションの領域を更に細分すると次のようになるであろう。

a) 荷主を代行して海貨通関業者が作成する輸出書類。

b) 荷主が作成し，海貨通関業者が受領して処理する輸出書類。

c) 海貨通関業者が作成する輸出申告書，輸入申告書等，通関に必要な書類。

d) 海貨通関業者が作成するS/O，B/L等船積書類。

これらのものは，国際貿易業務の基本帖票であるので，貿易情報システム

の中の重要な部分を占めている。かつそれは国際的な標準化の線に沿うものでなければならないので基本的なカテゴリーとして抽出した。

次に貨物管理の考え方においては，次のような方策を考えた。

a) 貨物送状は，現在英国のShipping Noteの考え方を受け容れて，JASTPROが検討しようとしている標準帳票によることを考えているが，これはまだフォームが決定していないので仮空のものである。これに海貨通関業者（エゼント業者の海貨部門を含む）の受領書，および同一フォームにより，新らしく考案されたシェッド・マスターをワンライティングでセットする。

b) シェッド・マスターとは，海貨通関業者（含エゼント業者海貨部門）が，港湾において貨物を受領するときに，統一的に使用するもので入力のためのデータシートを兼ねるものとする。これによって，港湾全体の受入れ貨物情報が共同利用センターにファイルされて，貨物情報の統一および，そこからそれぞれの業者が社内業務に展開することのできるマスター・ファイルを設定することを目的とした。

c) 港湾において貨物を受入れた段階においては，各種の貨物データは，まだ不完全なものである。これがフローの進行過程において加工され変換されて正確なものとなってゆく。シッパーから正確な完全なデータが入力されることは，先ず不可能である。すなわち

イ) 検才量による貨物の重量と大きさの確定

ロ) シッピング・インストラクションによる船積データの確定

ハ) 通関による内貨から外貨へのステータスの変換

ニ) 運賃料率によるフレートの確定

ホ) S/O，B/L による運送責任単位の確定

が行われ，輸出貨物は，入庫単位，申告単位，B/L単位，本船単位と仕分けされ，組立てられてゆく。

d) 以上のような経過をたどって船積が行われるのであるが，船積計画の

段階において，港全体の船積作業を最適化する目的をもって，ローディング・マスター・ファイルを設定する。これは将来考察されなければならないレーバーシステムに展開することも考慮したものである。

e) シェッド・マスターからローディング・マスターに至る貨物処理をもって，この実験システムにおける貨物管理の範囲とするが，われわれの考え方の基本は，貨物処理を書類事務とを統一的に処理することにある。何故ならば，貨物のステータスをチェックすることなしに書類は作り得ないし，また書類をチェックすること無しに貨物は動かし得ないからである。したがって，ドキュメンテーション・システムと言い，貨物管理システムと称するのは，概念的な区分に外ならないであろう。

1.2.2 データベースによるオンライン・システム

a) 共同利用センター方式

海貨通関業者，エゼント業者，検定，検数業者等が，共同で利用するセンターは，港湾管理者の港湾情報センターおよび将来設置されるであろう税関のシステムとリンクすることを目的とする。

この構想は，外貿埠頭公団のライナーバースを対象として進められているが，埠頭建設の進捗状況や業者の事業計画等との兼ね合いから，海貨通関業者とエゼント業者（埠頭経営者）との間で若干の考え方のちがいが出て来る。

海貨通関業者の場合には，共同利用センターを海貨センターとしてここに全関係業者を収容し，貨物処理をも共同で行うこと，そのような物的施設を設けること，すなわち業務の集中処理をすることを目的とする。これに対してエゼント側は多数のバースおよび上屋に分散する。したがって，その海貨通関部門はシステム的にこのセンターに集中するが，実際の埠頭業務は，それぞれのバースにおいて行われることになる。かつ建設中の埠頭であるため，まだ半数以上のものが，埋立工事中であって，実際にどの

ような貨物を扱い，どのような船をつけるかについての計画もまだ明確でない。したがって供用開始のはじまった数社の例を勘案して，一応仮設的に標準のシステムを考えざるを得ない。これに対して本来の海貨業者は荷主代行業務というたてまえから，過去の実績の延長として，比較的容易にその業務の内容を把握することができる。但し，特定の埠頭の業務だけを対象として電算化することはメリットが無いので，港全体を対象として考えなければならない。そしてこれは，公共埠頭を介して，港湾管理者の情報センターとリンクする。これは管理者のシステムをバックアップするうえから，大きな効果をもたらすであろう。

次に共同利用センターは，海貨通関業者，エゼント業者，検定，検数業者が共同で使用するものであるが，荷主，船社，および各関係業者（銀行，保険等々），さらに港湾管理者および諸官庁と直接リンクし，それぞれの外部のシステムとのインタフェースを持つことが必要である。

b) 共同利用センターとライナーバースの関係

ライナーバースの経営を行うエゼント業者の殆どすべてのものが，既にコンピューターを所有し，既にそれぞれの社内システムを開発している。これら既存のシステムは，センターと接続することを必要とするが，この場合，処理基準，コード，インタフェース，セキュリティ等についての，いくつかの原則は共通のものでなければならないと考えられる。

それぞれの上屋に端末機を置き，センターと接続するが，それぞれのエゼント業者の本社または支店とセンターともまた直接的に接続することを必要とする。さらに共同利用センターが，エゼントおよび海貨通関業者その他多数の業者が利用することになるので，センター内に端末機の共同利用センターを設置することが必要であろう。

また，データベース自体が，内部に持っていなければならぬ，特定のプログラム，たとえばトランザクッションの追跡監査等々，がいくつか考えられなければならない。但しこれらの内容は，今回の報告の中には含まれ

ていない。

c) 共同利用センターにおける電子計算機システムの概要

共同利用センターにおける電算機処理はオンライン・リアルタイム処理を基本として，一部即時処理を要しない業務はオンライン・バッチ処理，統計・管理資料作成（週・月・年報等）はバッチ処理を基本とする。このシステム設計で対象となった業務のほとんどは，オンライン・リアルタイム処理を要するものである。そこで共同利用センターのホストマシンは安全性を十分考慮して中央処理装置を2台とするデュプレックス方式を採用する。ホストマシンの規模は業務量と採算性を検討した結果，中型機クラスの大規模システムを想定した。

補助記憶装置としては，大容量の磁気ディスク装置に各種ファイルを収容する。磁気テープ装置は，入出力，ファイル更新等の全処理をジャーナル・テープとして記録し，オンライン処理の障害発生時のリカバリーにも利用する。また処理記録結果よりセキュリティ対策のデータとしても十分活用できることになる。

このシステムの利用者が使う端末機は，ディスプレイ装置・プリンター付きのインテリジェント・ターミナルとする。各利用者が端末機側でインプット・データのチェックや簡単な出力帳票の作表ができるようにする。原則としては各利用者の本社・事務所に設置するが，業務量の少ない自社端末機を導入できない利用者を考慮して，共同利用センターにも共同利用端末機を設置する。さらに自社システムを持っている利用者がデータの交換を必要とする場合はデータ伝送によりデータの交換を行う。

1.2.3 本システム開発のために設定する前提条件

a) この実験システムの規模は，ライナーバース完成時における貨物量を推計して定められる。但し，建設途上の埠頭であるため，現実の埠頭の営業には，いくつかの段階が考えられる。すなわち

比較的少数の業者が利用する段階　（ 1977～1978 ）

ライナーバース完成の段階　（ 1980 ）

１０年後の段階　（ 1990 ）

更に埠頭の利用方法が，本格的な埠頭経営でなくて，既存の埠頭業務をサポートするための目的に使用される等のことも有り得るので，現在の時点において，ライナーバース全体の経営の実態，あるいは個々のバースの事業計画等を推定することは困難である。

したがって，われわれのアプローチは，論理的に可能な，標準的処理を考察し，実際の業務を離れることなく，またある部分は合理化された形態を考慮しつつ研究を進めた。それ故に，ここに報告するものは，あくまでも，実験的なもの，すなわちパイロット・システムである。

b) 後に述べるメリット計算に明らかなように，関係する業者のメリット，デメリットは決して一様ではない。特に，港湾における作業は，荷主および船社に対して受動的なものであるので，このシステムから得られるメリットの主要な部分が，荷主および船社にもたらされるであろう。したがって，システム設定の前提条件として，メリットの合理的配分を考え，既存の業者が生きてゆける方法を考え，特定の場所にのみメリットが集中することなく，公平なメリットの配分が，センター存立の基礎とならなければならない。その詳細な内容は，センター設立のときの議定書に，明記せられるべきであろう。

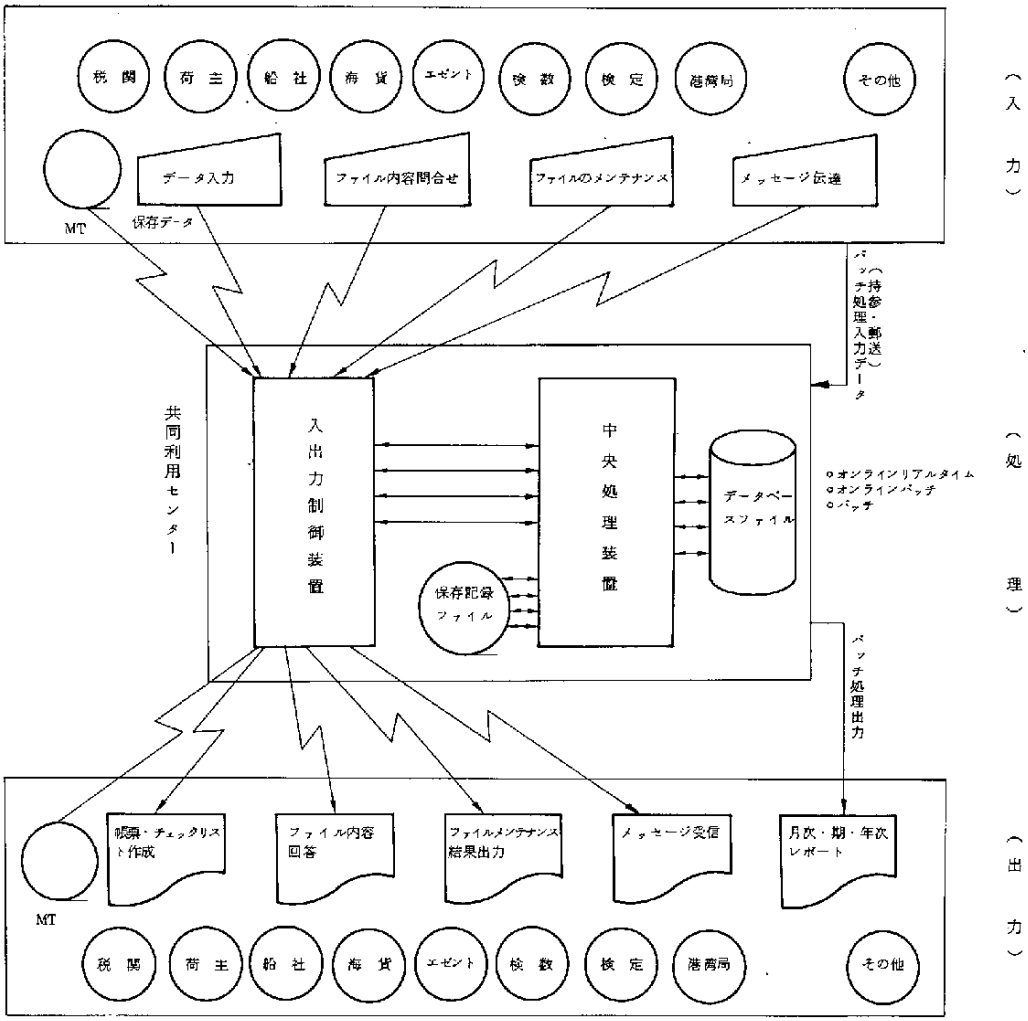


図３－１　共同利用センターにおける情報処理の概要

c) 大黒埠頭に共同利用センターを設置するに当たっての仮定条件

① データ量の基礎としての貨物取扱い量

大黒埠頭の整備計画に基づく全体の計画規模では，コンテナー・バースが2，ライナー・バースが8，年間総取扱い量は1,100万トンと見積られている。この取扱い量は，横浜港の公共埠頭扱い貨物量の約30%に当たり，当面は公共埠頭扱い分が大黒埠頭へ転移してくるのではないかとみられている。（トン数は船内ベース）

ひるがえって，ライナー・バースを借受け，専用埠頭として埠頭を経営しようとする借受者すなわちエゼント業者にとって経営目標となるのは年間50万トン（1バース当たり）とされ，1バースを2社ないし3社で共同借受けする場合は，1社当たり25万トンないし17万トンとみなされる。この数値によれば，共同利用センターで取扱われるべきデータ量の基礎は，

50万トン×8バース＝400万トン以上

としなければならないわけである。

これはバース接岸本船の面からみると，1社で毎月4隻，1バースで毎月8隻着岸し，滞留3日間，年間96隻が1バースごとに出入することになる。したがって，1隻当たり5,200トン，横浜港の現行輸出B/L件数は，40,000件並びに輸入B/L件数はその半分と見積り，大黒扱いはその30%，すなわち，輸出13,500件，輸入6,000件，計19,500件とみなした。なお，コンテナ・バース扱い分は半分とし，ライナー・バース分輸出9,000件，輸入3,000件，計12,000件，1バース当たり月間1,500件，1船200件となる。

② 対象貨物の性格と限定

横浜港で取扱われる輸出入貨物について，特に在来貨物の流れを現状のビジネスの仕組みにおいて量的に示すと，次の通りである。

（輸出の場合）

◇保　　管　　本船着岸同一埠頭内　１８％

　　他　地　域　　８２％

◇搬出方法　　は　し　け　　７６％

　　ト　ラ　ッ　ク　　２４％

（ただしB/L件数では６９％）

この傾向は，神戸港のポートアイランドにおける公団ライナーバースの運営現状にも非常に酷似している状態である。この業務の仕組みは，基本的には，港湾における貨物の集貨機能，港湾運送料金の体系，B/L発行条件，公共上屋の利用条件，海運貨物保管施設の整備状況，通関その他官庁手続きの能率・法的制約などが複雑にからみ，様々の要因が重なり合っているが故に起こっている。

東京港公団ライナー・バースの実情を視察した結果では，最近の貨物の種類は次のようになっている。

同バースは，昭和４８年３月に第１から第４バース，同４９年７月に第５から第９バースの供用を開始し，第２バースは特殊燻蒸上屋として，青果物専門埠頭となっているが，

昭和５０年は，輸出691,450トン，輸入429,420トン，

合計1,120,872トン

入港船，定期船３２隻，不定期船２７９隻

（但し，隻数には重複がある）

で輸出のウェイトが逐年重くなってきている。うち金属機械工業品450千トン（４０.１％），鉱産品１６０千トン（１４.２％），林産品１６０千トン（１４.２％），農水産品１４４千トン（１２.９％），軽工業品８２千トン（７.３％）等の順となり，プラントの輸出基地化してきていることがわかった。わが国の貿易構造と港の立地からみて，横浜港の大黒埠頭の取扱貨物の種類は，東京と近似してくることが予想され，借受

者２１社も大黒埠頭と重複するものが多いところから，貨物上の特性をもって，データネットの限定を行うことは，やはり困難のように思われる。ただし，コンテナ貨物は，ＣＹ貨物，ＣＦＳ貨物とも論理的には対象外とされているので，除外した。（実際上区分はしがたい）

したがって，共同利用センターで取扱うべきデータ源となる貨物は，

① 輸入については，大黒埠頭着岸本船積載陸揚げ貨物

② 他所揚げ本埠頭上屋等搬入未通関貨物

③ 輸出については，大黒埠頭上屋等搬入未通関・既通関貨物

④ 大黒埠頭着岸本船船積み貨物としてブッキングされ，他地域で保管または通関された貨物

貨物保管場所が「上屋等」となっているのは，公団ライナーバースの上屋，野積み場のほか，大黒埠頭内に設置されるであろう公共施設，公共野積み場，想定される海貨センター（共同の上屋・野積み場），私設の上屋，倉庫，野積み場を含むものとするからである。

d) 今回の報告は，ここに考察されているシステムの概要設計へのアプローチを示している。すなわち，その初期評価の部分および，概要設計の基本的な部分である。われわれはこのアプローチにおいて，米国のCARDISが実施したシステム設計の方法論を利用することができる。次に示すものは，CARDISの報告書に示されているものであるが，これを，わが国で利用できるように若干の修正および追加を行っている。特に下部のラインの機能をJASTPRO と COTISに分割し，且つセキュリティ問題の重要性にかんがみて，これを追加した。初期評価に関するものは，図３－２左上にワクをもって囲んである。

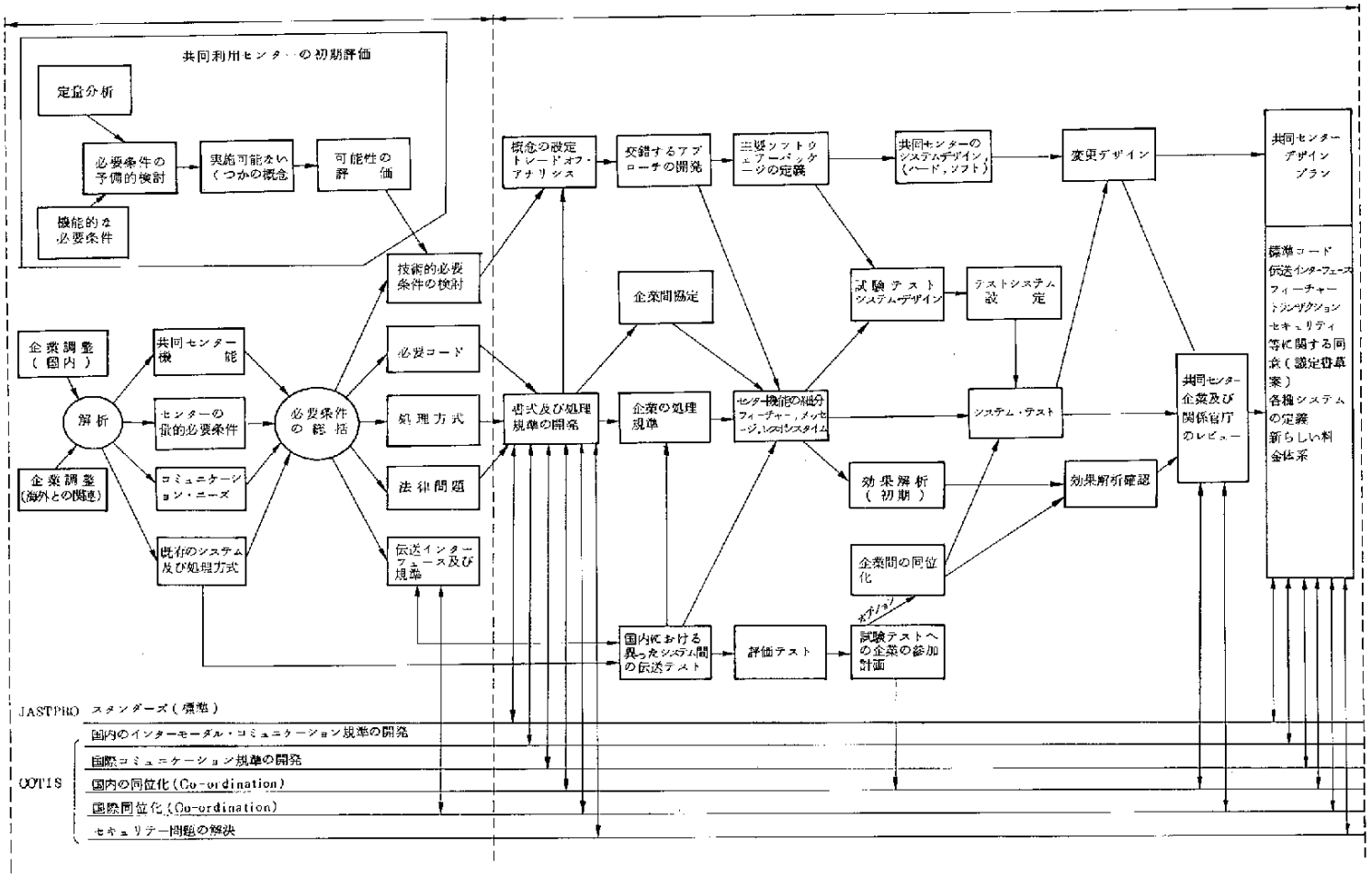


図３－２　海貨情報センター開発スケジュール草案

1.3　システム設計へのアプローチ

1.3.1　共同利用センターのシステム構想図試案

別掲図表（図3－3）に示すような，共同利用センターのシステム構想を設定した。図は，輸出および輸入のフローを処理するそれぞれのサブシステムおよび，業界および官公署への関連を示したものである。この図表においては，ドキュメンテーション・ラインと，貨物管理ラインとが概念的に区別して記されている。

ドキュメンテーション・ラインとは，COTISの第2貿易情報システムの範囲に属するCommercial Invoice，Packing List，Shipping Instruction，保険関係書類，買取用E/D，等々，輸出者（荷主）が作成するシッピング・ドキュメンツ，輸出申告書（税関用E/D）等の通関書類，およびS/O，B/L等の船積書類，それに船社の手仕舞業務に属するところのFreight ListおよびCargo Manifestもこれに含めるべきであろう。これらのものは，国際的商取引に必要な書類，国際的な海上運送に必要な書類，通産省および大蔵省が外国貿易に関して要求する書類（輸出申告書）であって，これらのものの作成処理を通常ドキュメンテーションの範囲に含めるので，今回もこの考え方に従うことにした。この外に，貨物処理のために多数の帖票が作成されているが，これらのものはドキュメンテーションの範囲から外した。また輸入の場合には，ドキュメンツは一括して外国から来る。それで輸出の場合のような体系的な書類作成事務は存在しない。ただ輸入申告書および通関用のマニフェスト作成事務等が，このカテゴリーに含まれるだけである。

貨物管理ラインは，工場において貨物を港湾へ向けて発送することからはじまる。但しこの場合，工場が輸出者である場合と，商社が輸出者であって工場は商社からの注文を受けた単なる生産者の場合と2種類に分れる。後者の場合には，港湾に対する貨物の発送は，しばしば輸出者に対する納品の形式をとっている。またトラック業者の運賃請求書，包装業者の納品書，倉庫

業者や工場の出庫指図書等々が，しばしば，便宜的に港湾に対する輸出貨物の送状として使用されているのが現状である。これを受理して，海貨通関業者が，輸出貨物としてのステータスを作りあげてゆくわけであるので，非常な手間と労力を必要とする。この輸出貨物の発送に関する合理化，制度化のため，標準的な貨物送り状が必要である。英国のSITPRO Boardがこれをとりあげて Shipping Noteという形で標準フォームを制定し，わが国のJASTPROもまた同様にこれを標準化しようとしている。

したがって，われわれの実験システムにおいては，ドキュメンテーション・フェーズにおいて，JASTPROの標準帖票によるたてまえをとっているので，この場合もJASTPROの帖票にしたがう考え方をとった。但しこの帖票は，まだフォームが定まっていないので，こゝでは，かりに「貨物送り状」とし，後に示すように，これに「貨物受領書」および「シエッド・マスター」を3点セットとし，シエッド・マスターは，貨物情報のマスター・ファイルに入力するデータ・シートの機能を持たせるのが合理的であると考えた。

次に通関をすませて，船積計画の段階で，最終的に仕上げられた確実な船積貨物情報をファイルするローディング・マスターを設定する。このファイルは，貨物の在庫管理，出庫業務，船積業務の作業面の情報のマスター・ファイルであって，将来開発されるであろうと考えられるレーバー・システムとリンクすることを考慮する。シエッドマスター・ファイルおよびローディングマスター・ファイルの体系は，埠頭（港湾）全体の貨物の流れを合理化し，スピードアップすることを基本的目的としたものである。

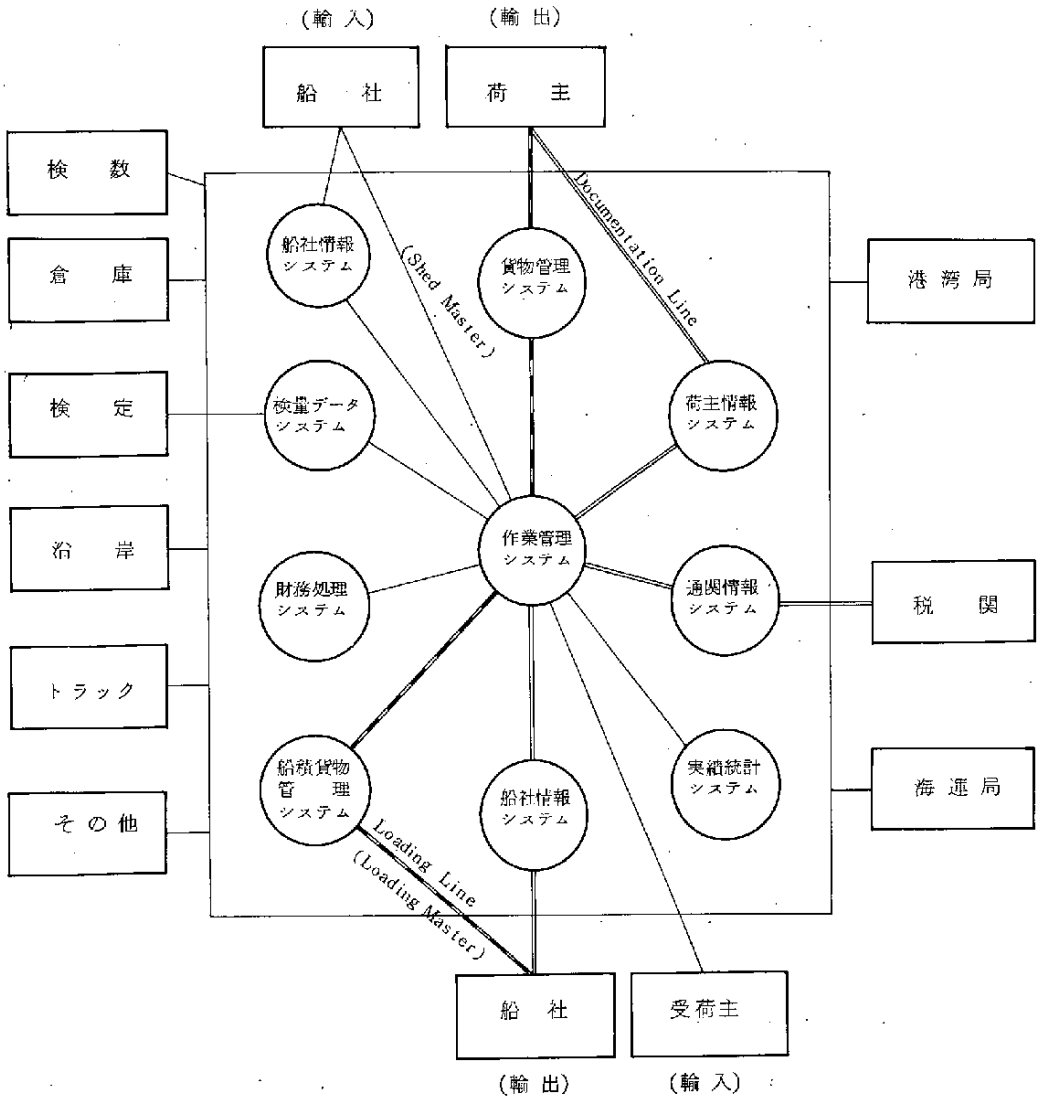


図３－３　共同利用センターシステム構想図試案

1.3.2 それぞれの業界の標準的フローとインタフェース

共同利用センターのシステム概念を設定した後で，われわれの作業は，それぞれの業界の標準的フローを作成し，これを輸出業務，輸入業務の流れをふまえて，それぞれの処理ノード（節）にまとめることであった。次に示すフローチャートがそれである。

a) 海貨センター業務フローの概念図

海貨通関業者は，一つの処理センターに集結するというのが，この実験システムの前提となっている。これをかりに「海貨センター」と呼ぶことにする。ところで，このセンターにはエゼント業者（ライナーバース埠頭経営者）の海貨部門も参加するので，実質的な共同利用センターとなるものである。こゝにおいて，それぞれの処理フェーズを次のようにまとめた。

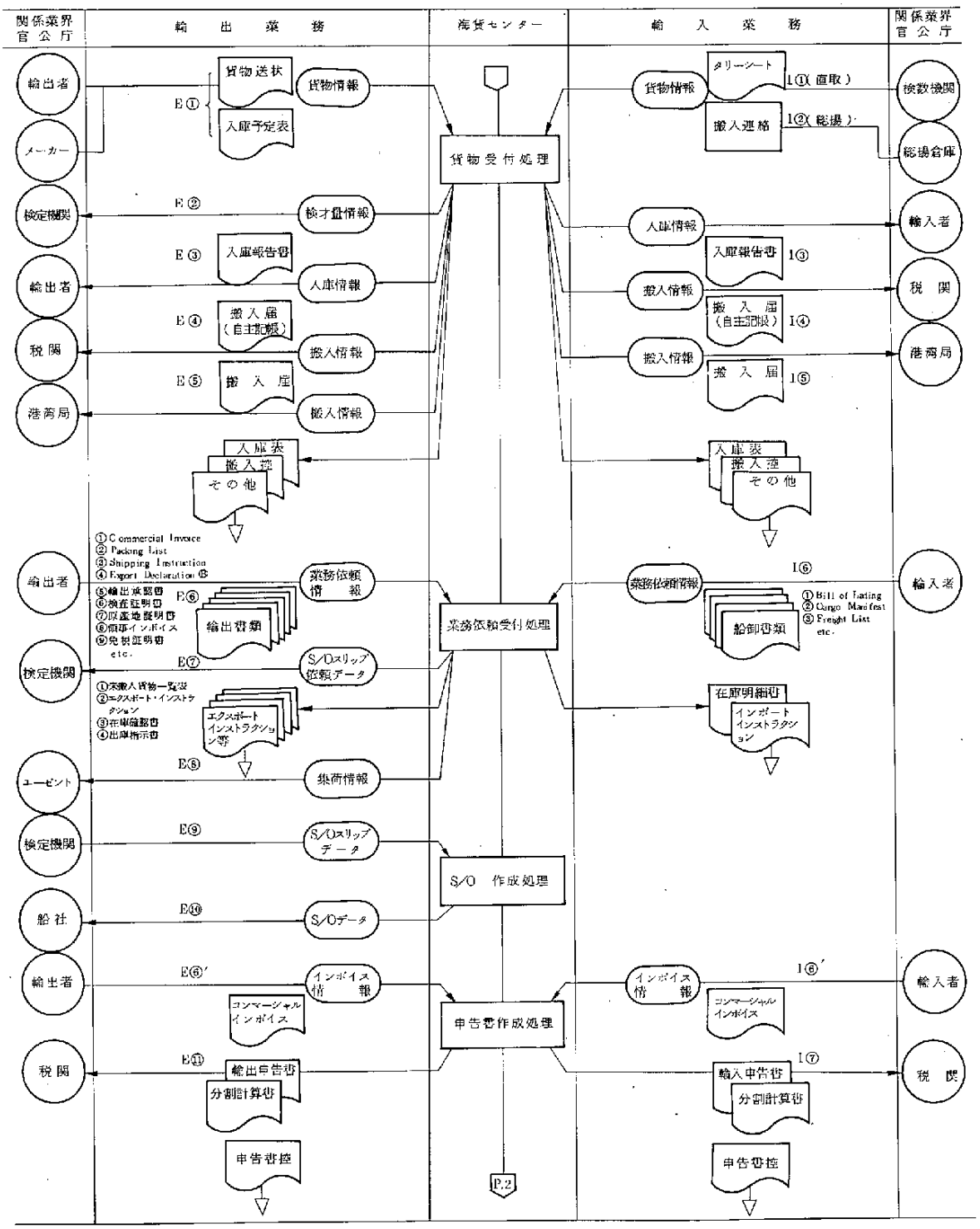
(1) 貨物受付処理
(2) 業務依頼受付処理
(3) S／O 作成処理
(4) 申告書作成処理
(5) B／L 作成処理
(6) 作業管理処理
(7) 出庫管理処理
(8) 在庫処理
(9) 財務処理
(10) 実績統計処理

これらの処理フェーズは，それぞれ輸出および輸入の業務を処理できるように考案されている。そのフローを図３－４に示す。

他業種および官庁等とのインタフェースを持つ帖票に，輸出の場合には，Ｅ１，Ｅ２，Ｅ３……の記号，輸入の場合には，Ｉ１，Ｉ２，Ｉ３……の記号を付し，さらに，輸出入とも共通に処理できるものについては，ＩＥ１，ＩＥ２，ＩＥ３……の記号が付してある。これらの帖票のデータエレメンツ

の概要およびその相互の関連は，前年度報告書に示されている。

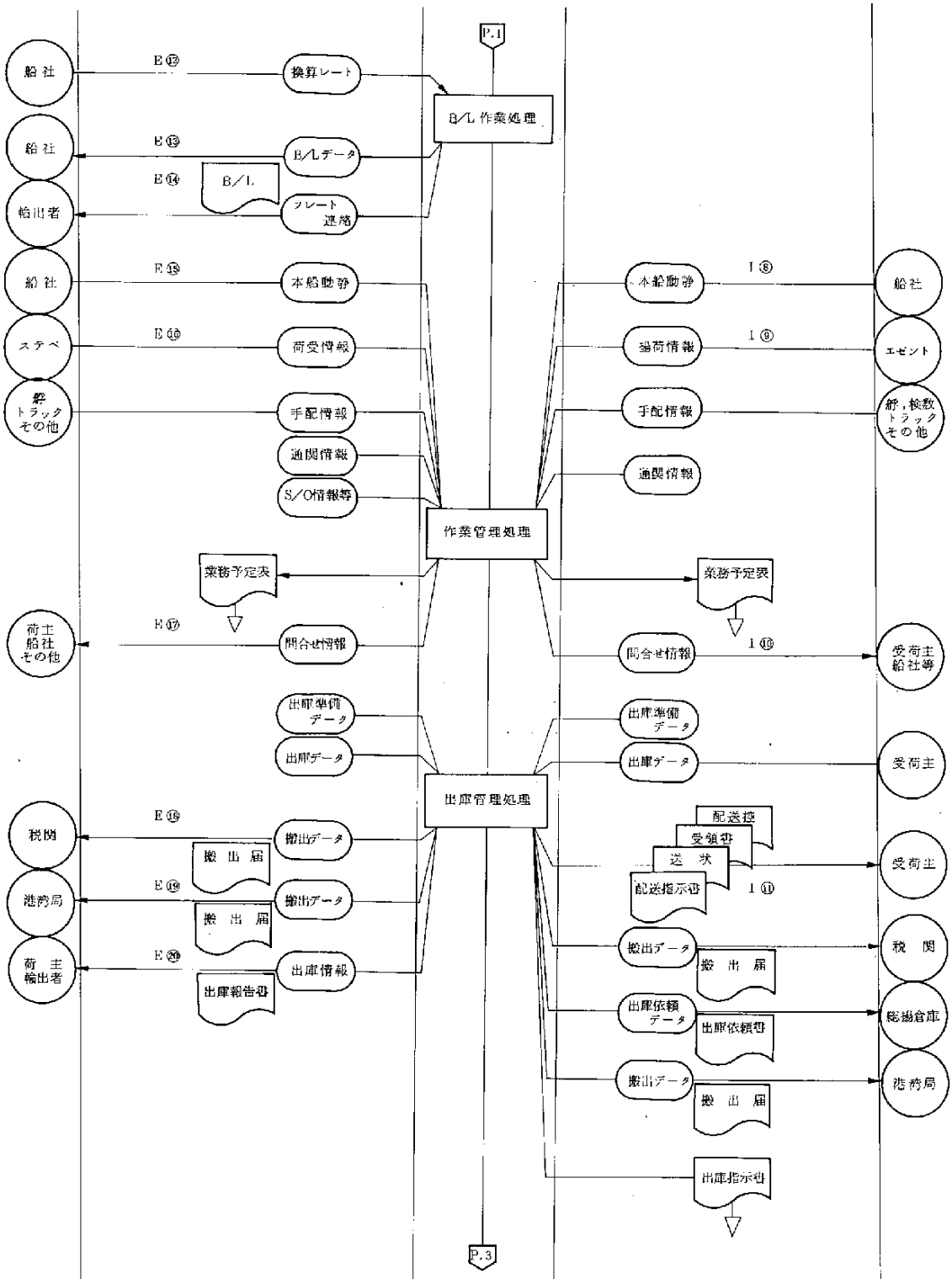
さらに，図３－５に示したような，輸出入業務の情報処理に必要なファイル構成を考えてみた。こゝでB/L作成に必要な「運賃率マスター」，あるいは通関に必要な「税関統計品目ファイル」その他が追加されている。



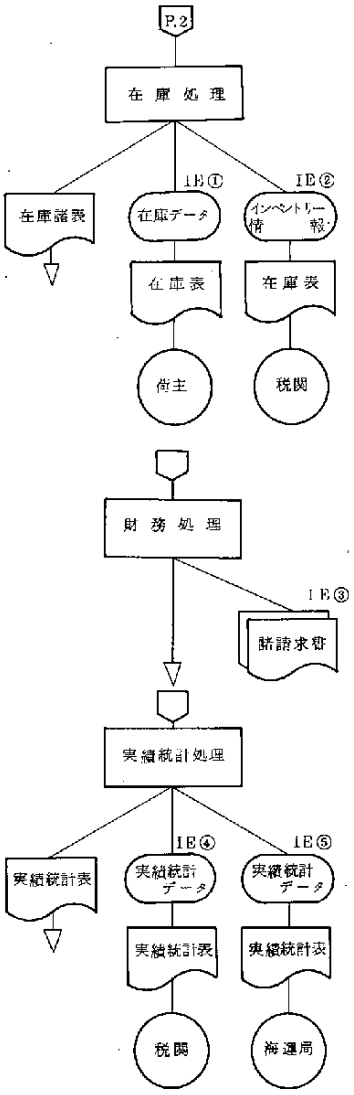
註 E①, E②, E③…… はそれぞれの帳票（情報）に対して Export 1, 2, 3, ……の記号を与えたもの。
I①, I②, I③…… はそれぞれの帳票（情報）に対して Import 1, 2, 3, ……の記号を与えたもの。
これらの記号を附したものが，他業種間の Interface 部分である。

図３－４　海貨センター業務フローの概念図

前頁続き


P.1
船社
E⑫
換算レート
B/L 作業処理
船社
E⑬
B/Lデータ
E⑭
B/L
輸出者
フレート連絡
船社
E⑮
本船動静
ステベ
E⑯
荷受情報
検数トラックその他
手配情報
通関情報
S/O情報等
作業管理処理
業務予定表
荷主船社その他
E⑰
問合せ情報
出庫準備データ
出庫データ
出庫管理処理
税関
E⑱
搬出データ
搬出届
港務局
E⑲
搬出データ
搬出届
荷主輸出者
E⑳
出庫情報
出庫報告書
本船動静
I⑧
船社
積荷情報
I⑨
エゼント
手配情報
艀,検数トラックその他
通関情報
業務予定表
問合せ情報
I⑩
受荷主船社等
出庫準備データ
出庫データ
受荷主
配送控
受領書
送状
配送指示書
I⑪
受荷主
搬出データ
搬出届
税関
出庫依頼データ
出庫依頼書
蔵場倉庫
搬出データ
搬出届
港務局
出庫指示書
P.3

前頁続き



(注) IEは Import and Exportの略で輸出入業務の双方に共通に使用されるデータを意味する。

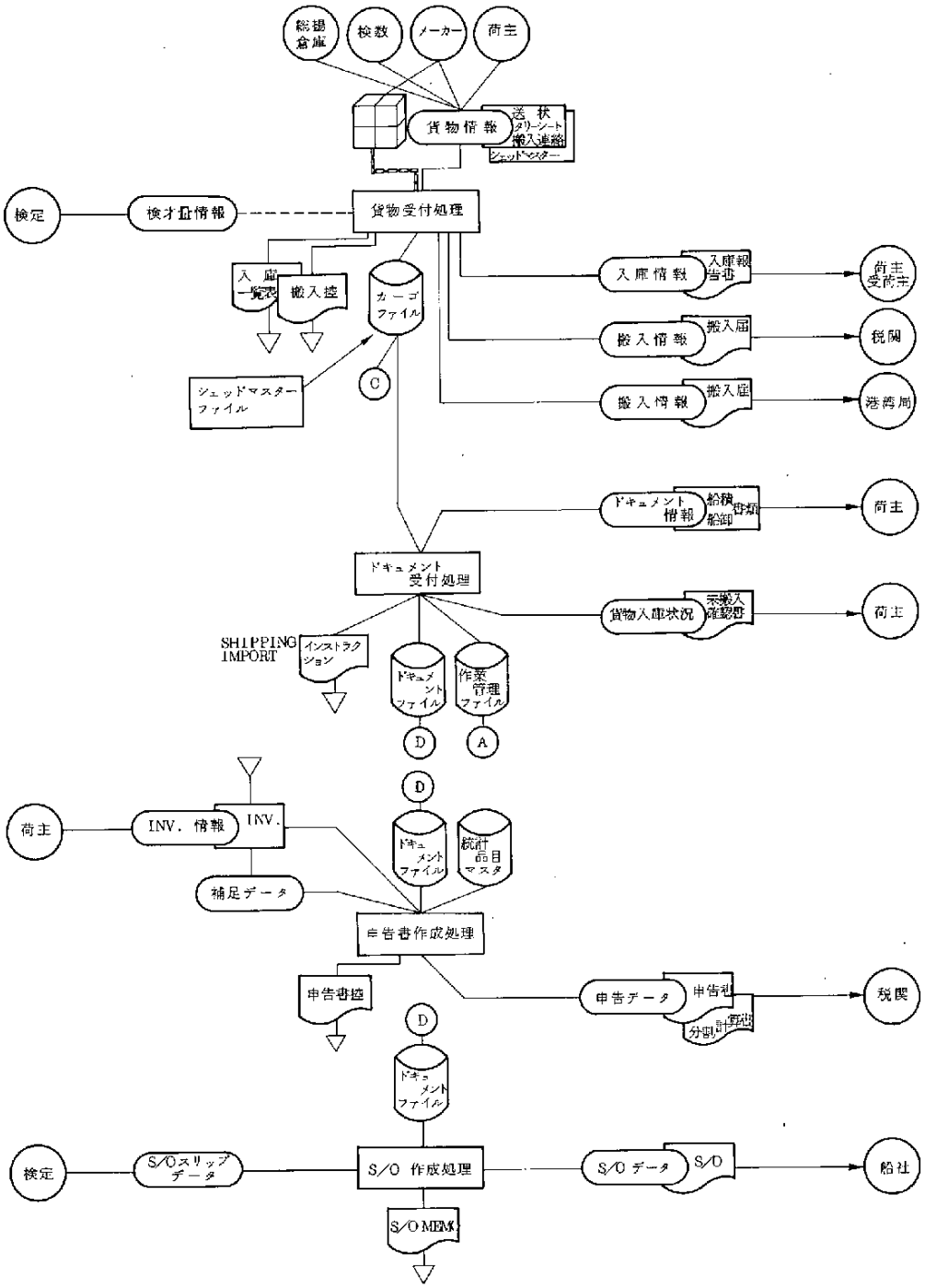
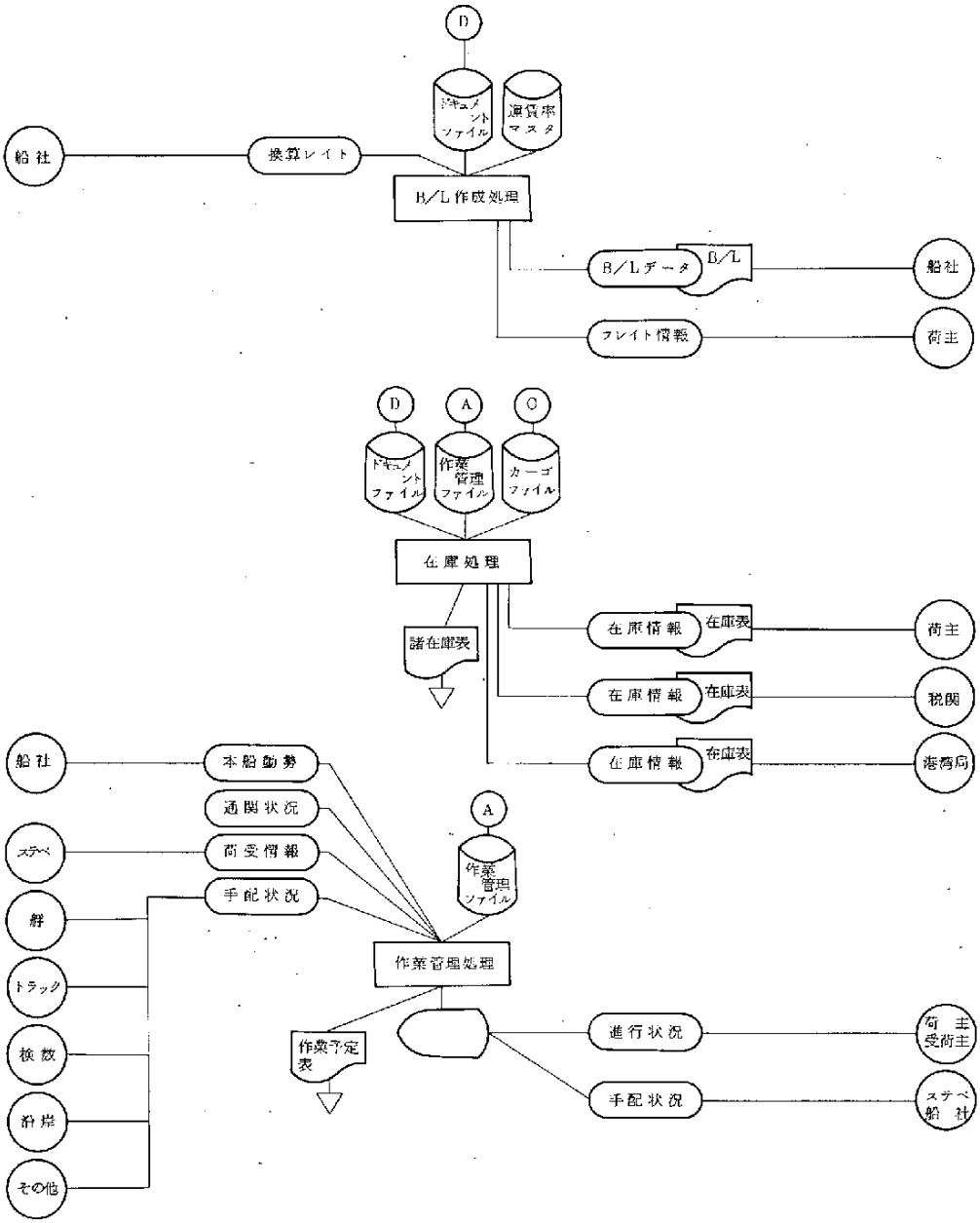
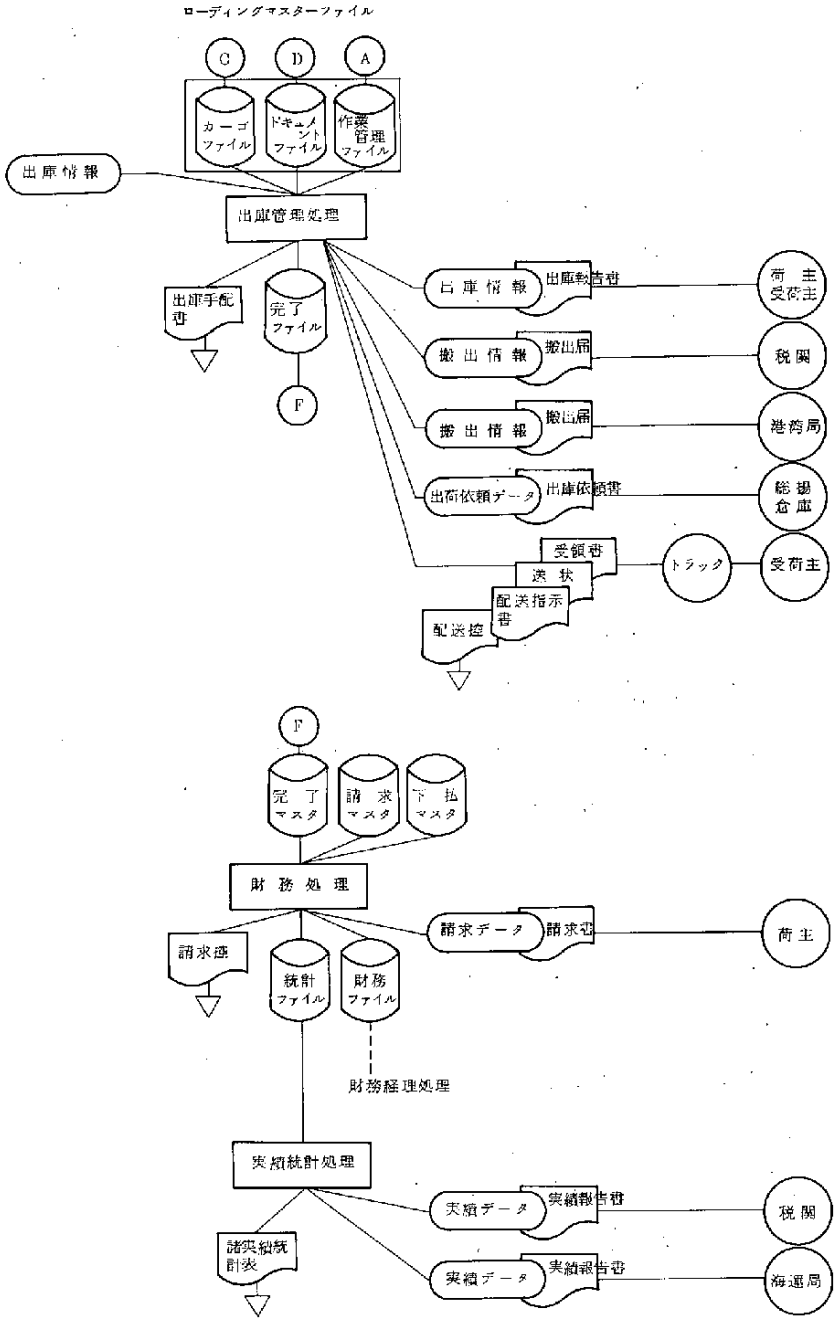


図３－５　輸出入業務の情報処理におけるファイル構成

前頁続き


D
ドキュメントファイル
運賃率マスタ
船社
換算レイト
B/L作成処理
B/Lデータ
B/L
船社
フレイト情報
荷主
D
A
C
ドキュメントファイル
作業管理ファイル
カーゴファイル
在庫処理
諸在庫表
在庫情報
在庫表
荷主
在庫情報
在庫表
税関
在庫情報
在庫表
港湾局
船社
本船動勢
通関状況
ステベ
荷受情報
艀
手配状況
トラック
検数
沿岸
その他
A
作業管理ファイル
作業管理処理
作業予定表
進行状況
荷主
受荷主
手配状況
ステベ
船社

前頁続き


ローディングマスターファイル
C
D
A
カーゴファイル
ドキュメントファイル
作業管理ファイル
出庫情報
出庫管理処理
出庫手配書
完了ファイル
F
出庫情報
出庫報告書
荷主受荷主
搬出情報
搬出届
税関
搬出情報
搬出届
港務局
出荷依頼データ
出庫依頼書
総揚倉庫
受領書
送状
配送指示書
配送控
トラック
受荷主
F
完了マスタ
請求マスタ
下払マスタ
財務処理
請求控
統計ファイル
財務ファイル
請求データ
請求書
荷主
財務経理処理
実績統計処理
諸実績統計表
実績データ
実績報告書
税関
実績データ
実績報告書
海運局

b) エゼント業，検定等，検数業の標準フロー

共同利用センターを利用するところの他の業種，すなわちエゼント業，検定業，検数業について，同様の方式で標準的フローを作成した。

〔エゼント業〕

エゼントとは船積，船降し作業についての船社の代理業務である。図3－7に標準的フローを作成し，インターフェースを持つ帖票について輸出はＡＥ1，ＡＥ2，ＡＥ3……輸入はＡＩ1，ＡＩ2，ＡＩ3……の記号を附し，処理フェーズを次のようにした。

(1) 業務依頼受付処理

(2) 貨物搬入処理

(3) 出庫処理

(4) 本船作業管理

(5) 料金計算処理（財務処理）

(6) 実績統計処理

この処理業務は，ライナーバースにおける業務を対象としているものである。エゼント業務の営業の主体は，輸入貨物の処理にあるので，特に輸入貨物の在庫管理について図3－4を加えた。エゼント業務自体の中には，さきに規定したドキュメンテーションは存在しない。またこの業務処理のあるものは，検数業者に委託しているものがある。

〔検定業〕

図3－9に示したものが検定業者の業務処理で，この部分は日本海事検定協会および検定新日本社において，ほぼ同様な方式でシステム化されている。このチャートは，両者合意の上確認された標準的なものである。帳票のインタフェース記号には，ＳＥ，ＳＩのそれぞれ1，2，3の記号が付されている。処理フェーズは，

(1) 輸出入貨物情報処理

(2) コンテナ貨物情報処理

の二つである。検定業務は，一つの証明行為であって，全体の輸出入業務のフローの1部に介入するだけで比較的単純であり，すでにコンピュータ処理を行っているので「それぞれの業者のシステムを生かす」という前提から，共同利用センターとは，システムのリンクが存在するだけである。但し共同利用センターのコンピュータを使用するという考え方も成り立つ。これは業者の意志決定に待つ外ない。検定業者が，センターとどのような関係に立つかということは，これから先の業界の話合いによらなければならないが，一つの考え方として，検数業者と共に，センターのオペレータとなるということも成り立つのであるが，ここでは現状のままを基準とした。

また検定業務の作業形態は，原則として入庫検定を採用した。これは，貨物の到着と同時に検才量を行う方式で，最も合理的な方法である。すなわち在来の方式にくらべると，上屋の中で貨物のリハンドリングの手間と経費を無くし，かつ早い時点で正確な貨物データが得られるというメリットがあり，現在すでにかなりの程度に実施されている。この実験システムの対象となる公団ライナーバースにおいては，それぞれのエゼント上屋において確実に実施し得るし，かつ海貨センターにおいては，すべての海貨通関業者の輸出貨物の検才量を一括して行うという極めて合理的な方法が可能となるからである。

更に検定部門にのみ，コンテナ貨物情報処理があるが，これはライナーバースにおけるバンニング，デバンニングを対象としているもので，フル・コンテナ船に対するコンテナ貨物情報処理は，今回の研究対象から外してある。

〔検　数　業〕

検数業務も検定業と同様に証明機関であって，本来の貨物処理ないしは，ドキュメンテーションに対する責任はないが，検定業と同様に多くの作業部門において，海貨通関業者，エゼント業者，船社等の業務を代行してい

る。

業の性質上，海貨通関業者，エゼント業者と同様な作業のフェーズをつくることが困難であるので，フローチャートは輸出，輸入にわけ，それぞれ次のようなフェーズに分けた。

輸　出

(1)　船積情報処理

(2)　荷役計画情報処理

(3)　積荷情報処理

(4)　検数情報処理

(5)　本船作業情報処理

(6)　社　内　処　理

輸　入

(1)　スタンバイ処理

(2)　検数情報処理

(3)　本船作業情報処理

(4)　沿岸検数情報処理

(5)　社　内　処　理

インタフェースを持つ帖票については，それぞれＴＥ（輸出），ＴＩ（輸入）の記号のもとに１，２，３……の番号を付した。

このフローは日本貨物検数協会，および全日本検数協会が，同一システムを使用するという合意のもとにつくられたものである。センターに対する関係は検定業と同じであるが，検定業の説明の折にのべた諸関係を図示すると，次のようになる。

Shipment (1)	Shipment (2)	Shipment (3)	……	Shipment (n)
S1	S2	S3	……	Sn
I/C1	I/C2	I/C3	……	I/Cn
F1	F2	F3	……	Fn
M1	M1	M1	……	M1
W1	W2	W3	……	Wn
B/C1	B/C2	B/C3	……	B/Cn
T1	T1	T1	……	T1
N1	N2	N3	……	Nn

（注）
S ：Shipper シッパー
I/C：Inland Carrier トラック
F ：Forwarder フォーワーダー
M ：Measurer 検定
W ：Warehouse 倉庫
B/C：Barge Carrier はしけ
T ：Tallyman 検数
N ：Navigation Company 船社

図３－６　シップメント別関係者関連表

図３－６に見るように，それぞれのシップメントに対して，関係ある業者は異なって来るが，検定および検数は何れの場合にもほぼ１である。実際にはそれぞれ２団体であるが，同一システムを使用するという前提でこれを１とすることができる。かつＭもＴも，港湾の作業現場に数千名の職員を配し，彼等が証明した最新の正確なデータを一つの中心，すなわちセンターに集中する機能を持っている。これは外国には見られない，わが国独得の制度であって，貿易情報システムから注目すべきものである。この関係から，共同処理センターとＭおよびＴとの特殊な関係ないしは，シス

テムのオペレーション上の特別の役割を持つという考え方が出て来るであろう。

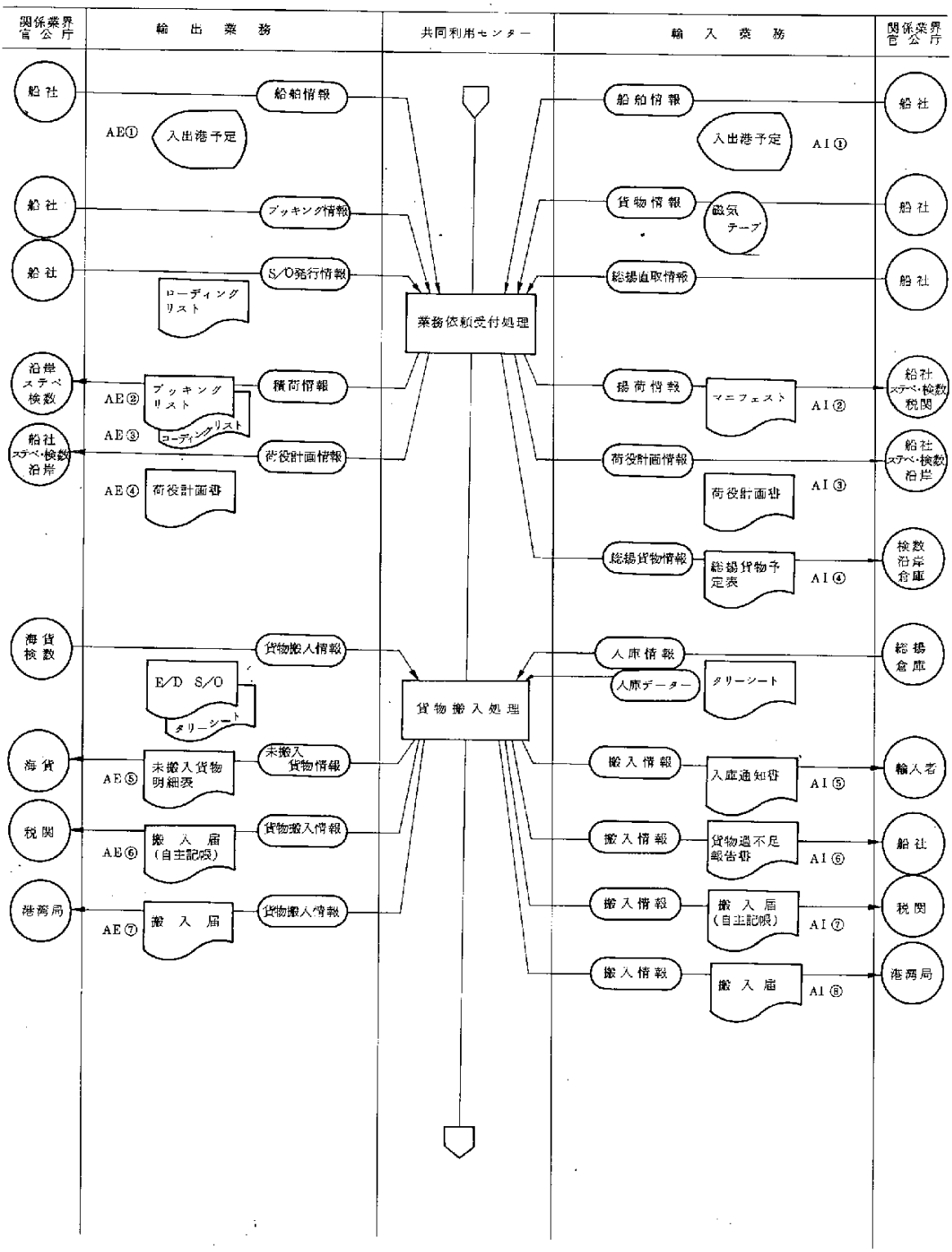
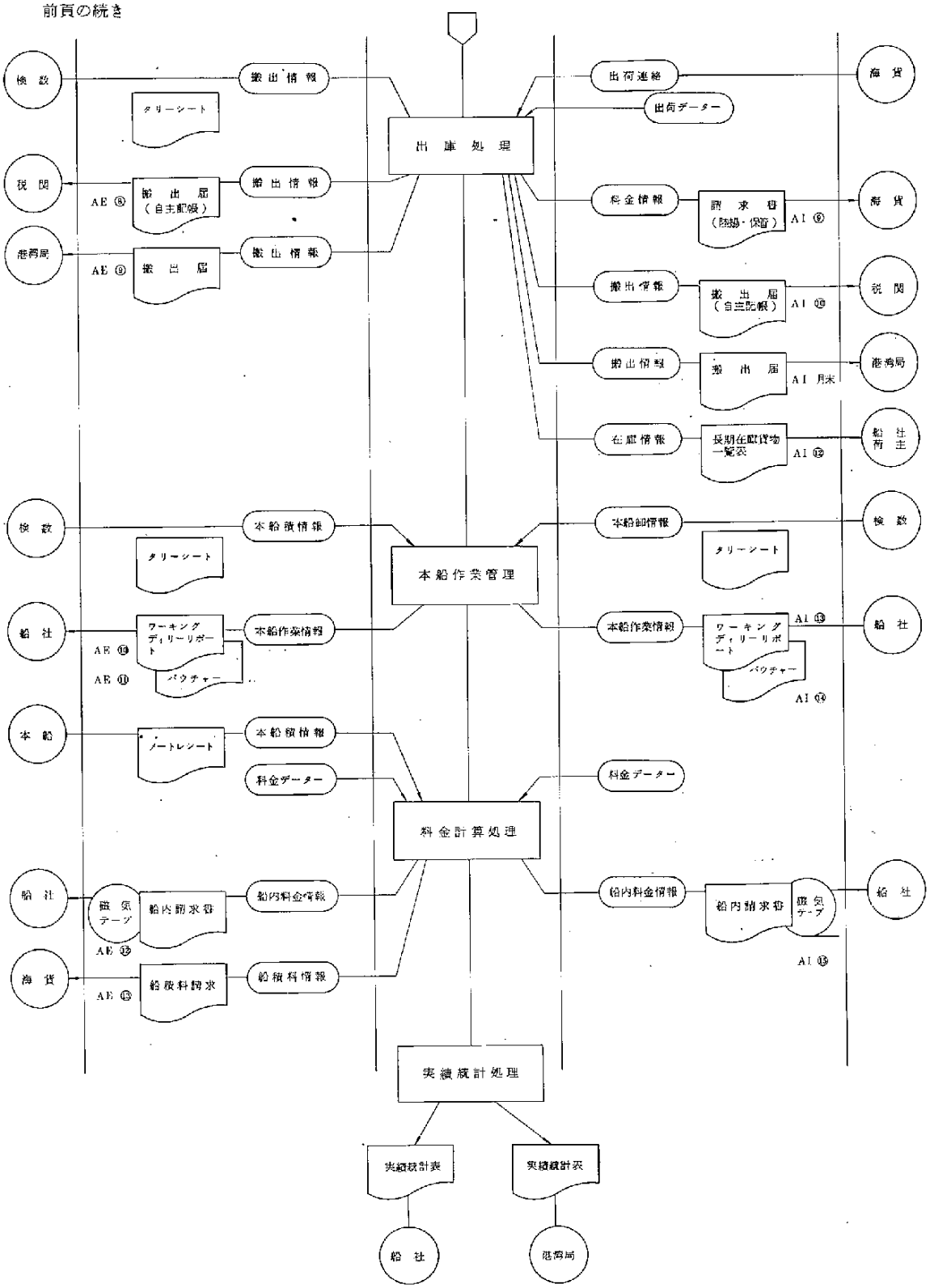


図3－7　ライナーバース・エゼント業者のシステム構想

前頁の続き


検数
税関
港湾局
荷主
船社
本船
搬出情報
タリーシート
搬出届（自主配帳）
搬出届
出荷連絡
出荷データー
料金情報
請求書（陸揚・保管）
搬出情報
搬出届（自主配帳）
搬出情報
搬出届
在庫情報
長期在庫貨物一覧表
出庫処理
本船積情報
タリーシート
ワーキングディリーリポート
バウチャー
本船積情報
料金データー
磁気テープ
船内請求書
船内料金情報
船積料請求
船積料情報
本船作業管理
料金計算処理
本船卸情報
本船作業情報
ワーキングディリーリポート
バウチャー
料金データー
船内料金情報
船内請求書
磁気テープ
実績統計処理
実績統計表
実績統計表
AE ⑧
AE ⑨
AE ⑩
AE ⑪
AE ⑫
AE ⑬
AI ⑥
AI ⑩
AI 月末
AI ⑬
AI ⑭
AI ⑮

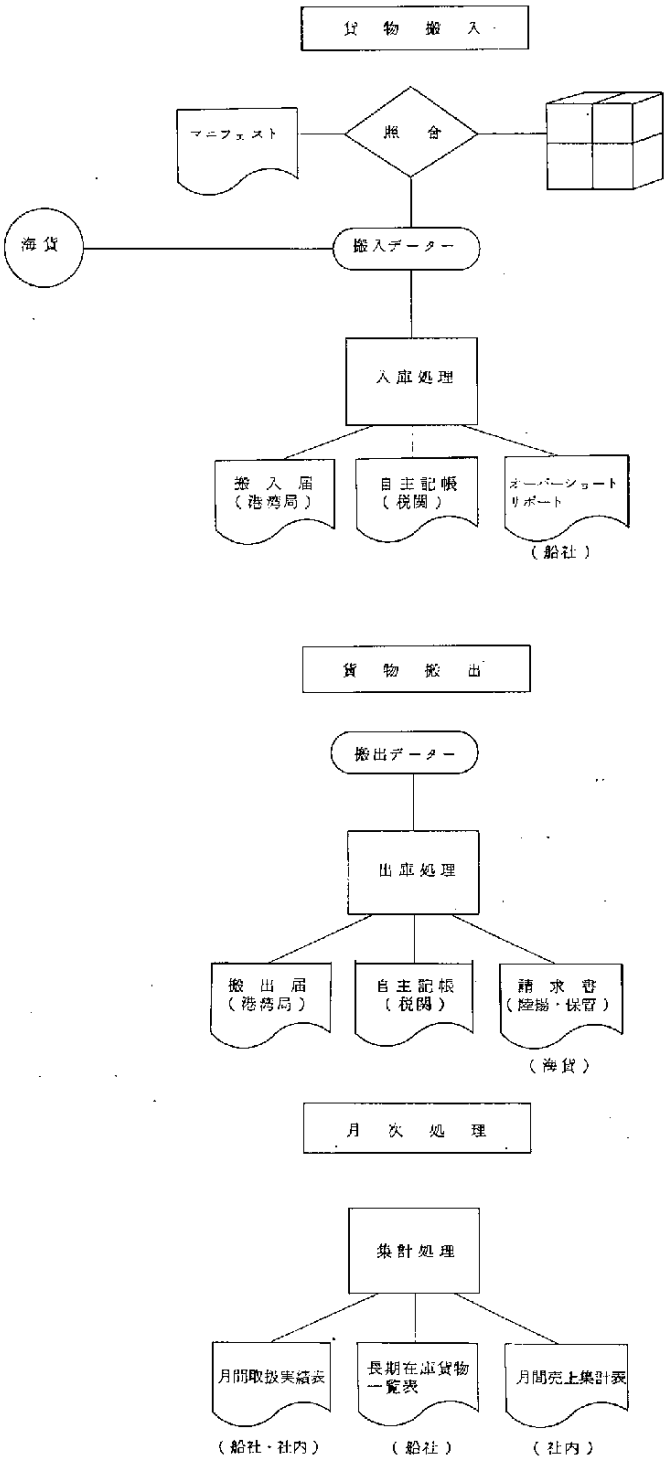


図３－８　エゼント業の輸入在庫管理

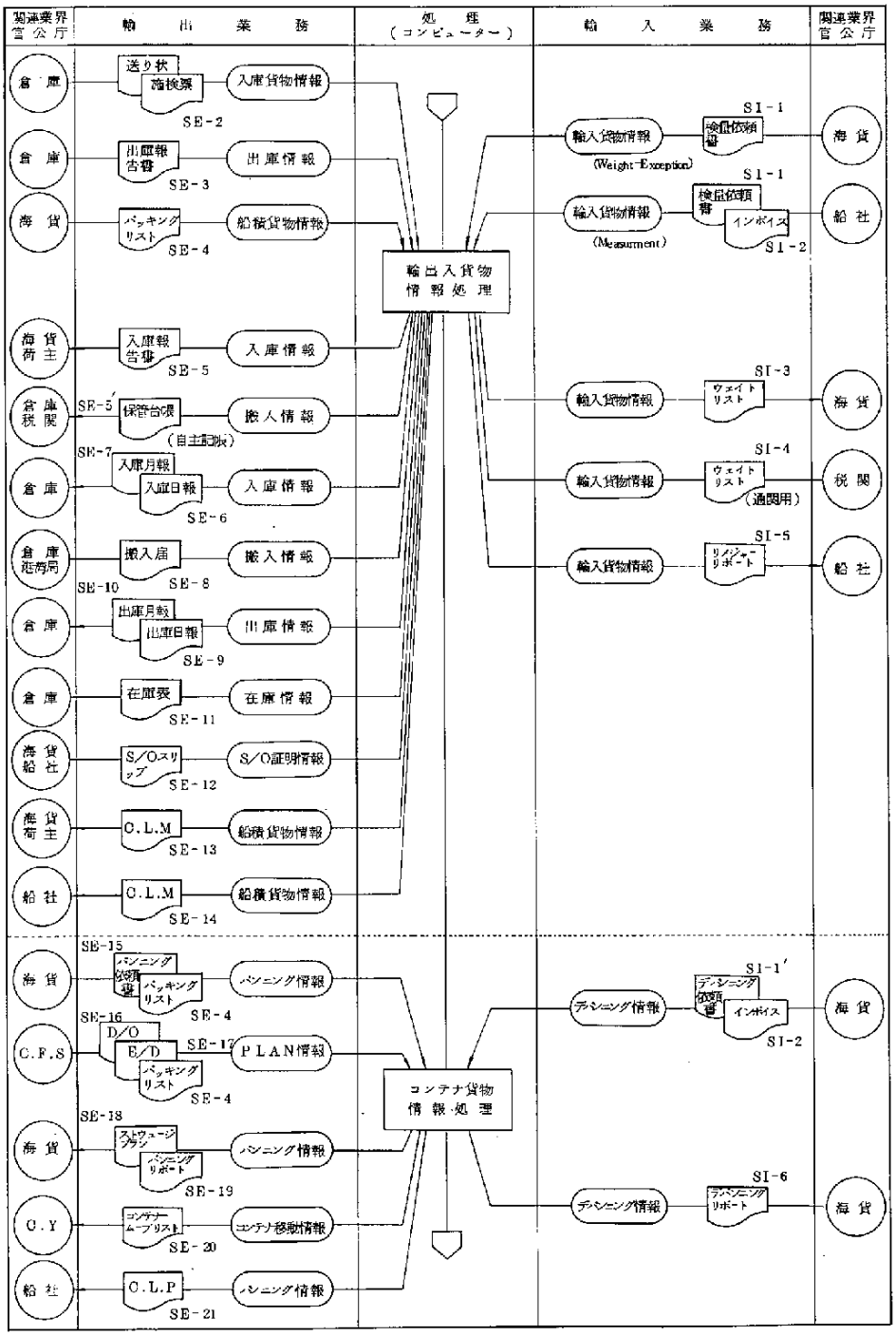


図３－９　検定業者のシステム構想

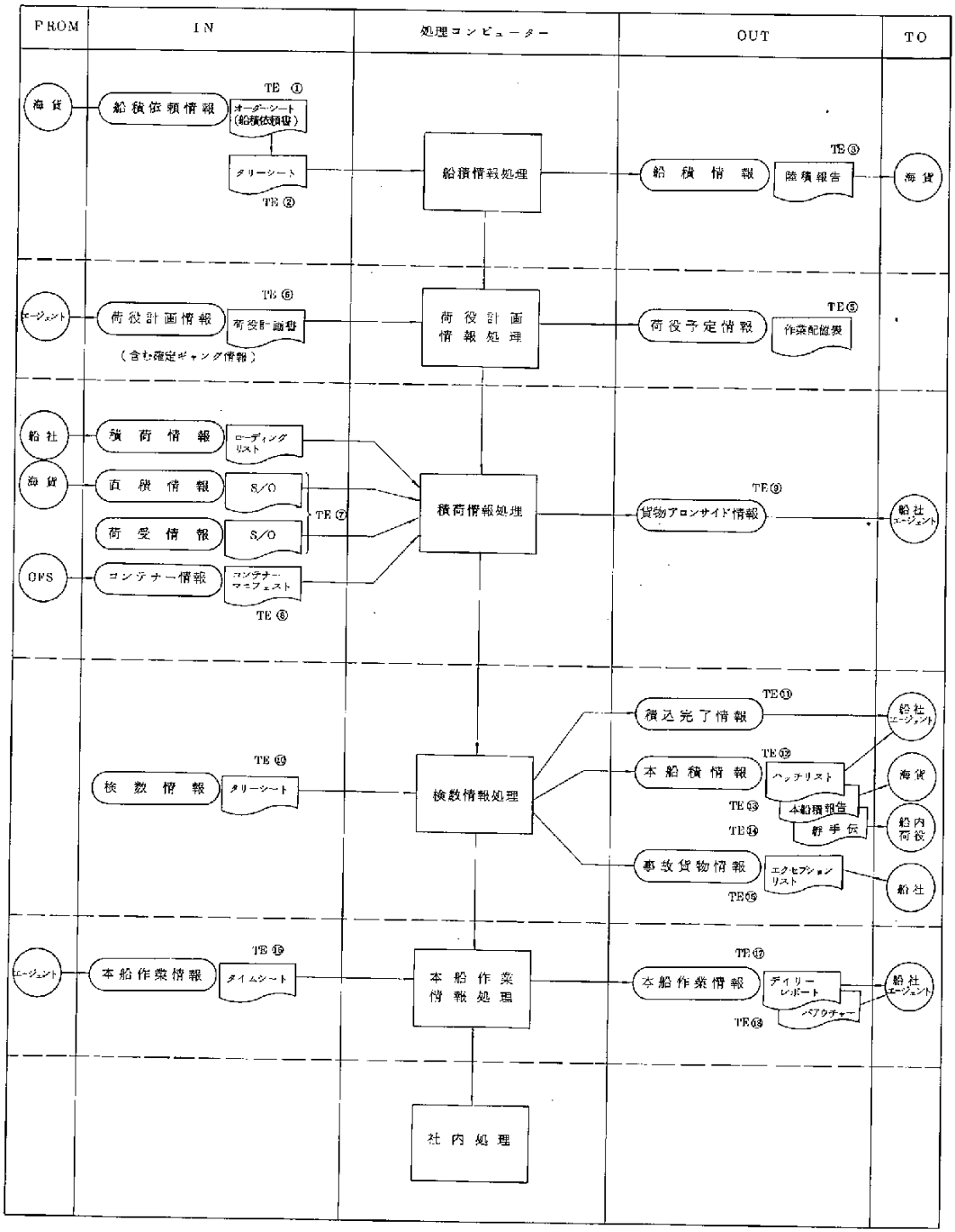


図３－１０　輸出検数業務のシステム構想

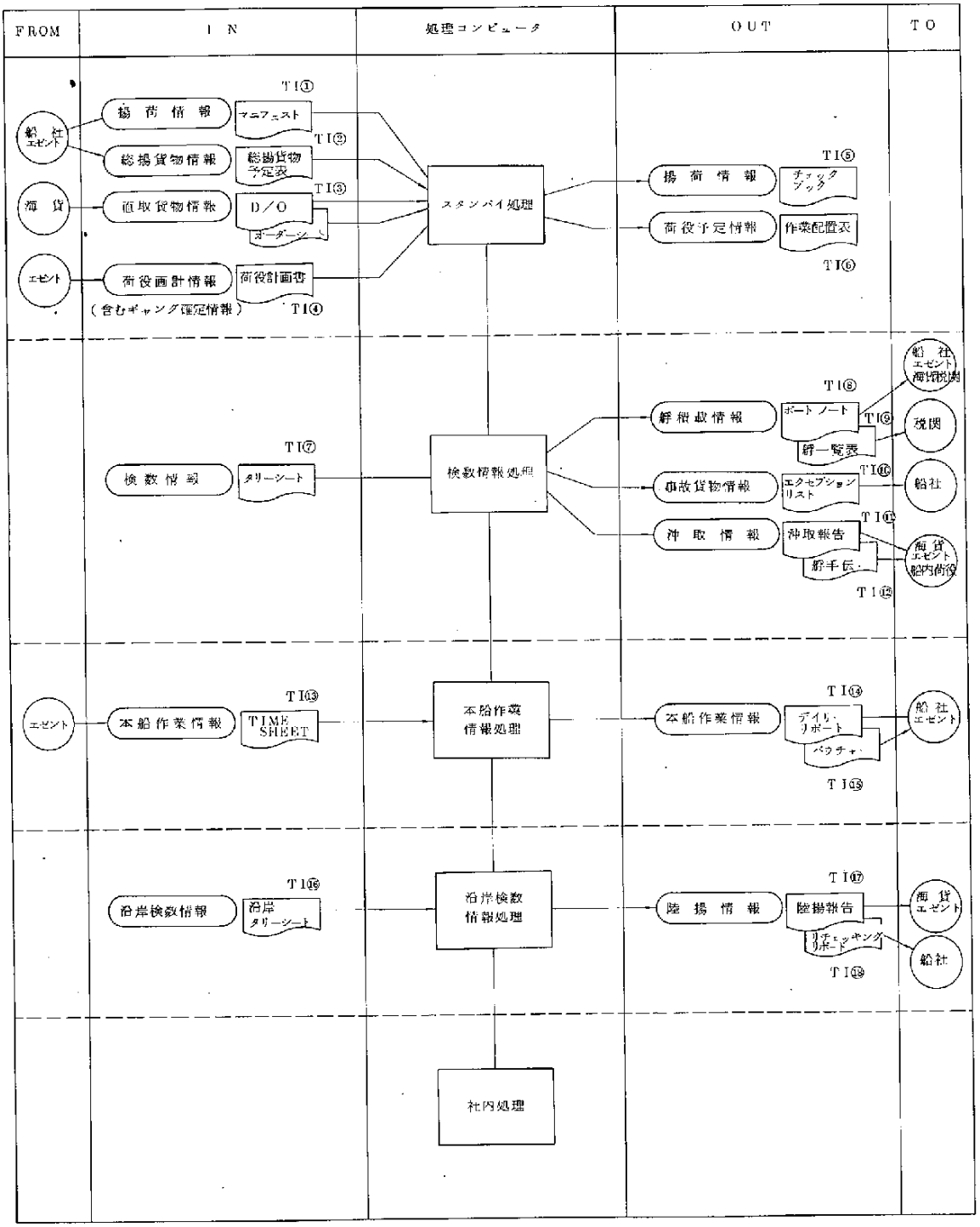


図３－１１　輸入検数業務のシステム構想

1.3.3　データエレメントの現状分析

海貨業者を中心として，現在使用されている帳票の項目がどのように発生，追加，更新されているかの現状分析を行った。そこでわれわれは，現行帳票をドキュメンテーションと貨物管理の二つに分けて，輸出および輸入業務について分析を行った。

縦軸に各帳票で使用する項目をデータ名として整理し，横軸に輸出入業務に使用する帳票名を記した。そして各データ項目がどの帳票によって新しく発生し，どう転記され，更新されるかを見るため7種類の記号を設定して，データ動静が一覧できるようにした。

記号の区分

① ◎印　固定データ

② ○印　受取データ

③ ⊕印　発生データ

④ ⊖印　転記データ

⑤ △印　受取不確定データ

⑥ ⧋印　不確定発生データ

⑦ ⧊印　不確定転記データ

表３－１　輸出入ドキュメントデータ動勢表

◎ 固定データ　⊕ 発生優先データ　△ 受取不確定データ　⚠ 不確定データ発生　○ 受取データ　⊖ 転記データ　→ 不確定データ転記

輸出														データ名	輸入										
依頼書	INV.	P/L	Ⓑ E/D	S/I	Ⓒ E/D	S/O	B/L								依頼書	B/L	INV.	P/L	IMPORT INST.	D/O	Ⓒ I/D				
⊖	⊖	⊖	⊖	⊕	⊖									INSTRUCTION NO.					⊕		⊖				
○				◎		◎	◎							海貨通関業者名	○	△			◎						
				◎		◎	◎							〃 コード		△									
				⊕										受註年月日（受付）					⊕						
○				⊕										諸掛負担先	○				⊕						
△				⚠										CONTAINER SERVICE											
				⊕										通関地	△										
○				⊕	出港予定年月日 ⊕									ETA/ETD 入出港予定日	△		△		⊕						
○				⊖										M/W LIST枚数											
○				⊖										B/L COPY枚数	△										
				←	⊕									許可年月日					⊖						
				⊕										入庫 〃					←						
				⊖	⊖									搬入場所	△				⊕		⊖				
				⚠										船側搬入年月日											
				⊕										船積完了年月日											
				⚠										搬出年月日	△				⊕						
														倉入又は移入先					⚠		→				
				⊕										エゼント名	△				⊕	○					
				⚠										艀名					⚠						
				⚠										検数業者名					⚠						
				⚠										トラック業者名					⊕						
				⚠										トラック種類					⚠						
△				⚠										リマーク					⚠	△					
△				→										BOOKING NO.		△									
				⊕	⊖	⊖								SHIPPERS コード		△									
○				⊖			◎							船社	△	○			⊖						
														D/O 発行年月日						○					

輸出														
依頼書	INV	P/L	Ⓑ E/D	S/I	Ⓒ E/D	S/O	B/L							
△	△	△		→										
△	△	△		→										
△	△	△		→										
△	△	△		→										
△	△	∧	○	→										
△	△	△		→										
△				→										
△				→										
△	△	△	○	→										
△	△	△	○	→	→									
○	△	△	○	→										
△	○	○		⊖										
△	△	∧		→										
△	○	○		⊖		⊖	⊖							
△	○	○	○	⊖		⊖	⊖							
○	○	○		⊕	⊖	⊖	⊖							
○	○	○		⊕	⊖	⊖	⊖							
○	○	○		⊕	⊖	⊖	⊖							
△	△	△		⊕		→	→							
○	○	○		⊕	⊖	⊖	⊖							
○	○	○		⊕		⊖	⊖							
○	△	△	○	⊖		⊖	⊖							
	○	○		→	⊖	→								
△	△	△	△	→	⊕	→	→							
	○													
	△													
	△		△											
	○		○	⊖										
△	○		○	⊖										
		○												
		○			⊕									
		○			⊖									

輸入														
データ名	依頼書	B/L	INV.	P/L	IMPORT INST.	D/O	Ⓒ I/D							
SALES NOTE №.	△													
〃 DATE	△													
CONTRACT №.	△													
〃 DATE	△													
L/C №.	△		△											
〃 DATE	△		△											
LATEST SHIPPING DATE														
EXPIRY DATE														
ISSUING BANK														
BANK CERTIFICATE №.														
決済条件														
INVOICE №.	△		○	○										
〃 PLACE & DATE			○	○										
CONSIGNEE		○				○								
NOTIFY PARTY		○												
船名	○	○	○	○	○	○								
積込港		○	○	○		○								
仕向地		○	○	○		○								
FINAL DESTINATION		△												
MARKS & NUMBERS	△	○	○	○	⊖	○								
NUMBER OF P'KGE	△	○	○	○	⊕	○								
L/C品名		○			⊖	○								
INV品名	○	△	○	○	→	△								
品名(オプション)		△			→	△								
UNIT PRICE			○											
小計金額														
ADDITIONAL CHARGE														
決済建価	○		○											
決済金額	○		○											
P/L量目 @			∧	○										
〃 計(小計含)			△	○										
〃 単位			△	○										

輸出															データ名	輸入													
依頼書	INV	P/L	Ⓑ E/D	S/I	Ⓒ E/D	S/O	B/L									依頼書	B/L	INV.	P/L	IMPORT INST.	D/O	Ⓒ I/D							
			○		⊕										統計品目番号					○										
			○		⊕										US $ 換算額															
			○		⊖										仕向国			○												
			○												外為種類															
			○												〃 手形期限															
			○												信用状未使用残高															
			○												〃 接授年月日															
			○												〃 有効期限															
			○												銀行認承年月日															
					㊀										申告税関名							⊕							
				←	⊕										申告年月日					⊖		㊀							
					◎										代理人住所氏名印							◎							
					⊕										本船・ふ中扱区分															
					⊕										保税運送区分															
					⊕										〃 期間															
				←	⊕										申告書枚数・欄数					⊖		⊕							
					⊕										船(機)籍符号							⊕							
					⊕										積込港符号															
					⊕										仕向国符号															
					⊕										貿易形態別符号							⊕							
				←	⊕										申告番号					⊖		⊕							
					⊕										取扱区分（他法令）															
					⊕										単 位							⊕							
					㊀										申告価格（F.OB）															
					⊕										通関士記名押印							⊕							
○	○	○	○		→	→	→								輸出者住所氏名		○					⊖							
○	○	○	○												〃（入）印															
				○		→	→								WEIGHT & MEASUREMNT		○		△		○									
															回															
															HATCH NO															
															RECEIVED IN ALL															
															〃 DATED															

輸出														データ名	輸入													
依頼書	INV	P/L	Ⓑ E/D	S/I	Ⓒ E/D	S/O	B/L								依頼書	B/L	INV.	P/L	IMPORT INST.	D/O	Ⓞ I/D							
														CHECKER サイン														
														MANAGER サイン														
				←		⊕								S/O NO.														
				←			⊕							B/L NO.	○	○			○	○	⊖							
														上屋・艀区分														
														品目コード														
							⊕							FREIGHT & CHARGES	△	○												
				⊕			⊕							REVENUE TONS		○												
				⊕			⊕							FREIGHT RATE	△	○												
							⊕							PER		○												
							⊕							PREPAID OR COLLECT計		○												
				⊕			⊖							EX. RATE														
○				⊖			⊖							FREIGHT 支払地 (PREPAID AT PAYABLE)		○												
							⊕							FREIGHT 円価	△													
○				⊖			⊖							B/L ORIGINAL枚数	△	○												
							⚓							COMBINE B/L作成地														
							⚓							〃 海貨業者名														
							⚓							〃 品目														
○				⊖			⊕							B/L 発行地														
							○							B/L サイン		○												
				←			○							B/L DATE		○												
△				→		→	→							VOY NO.	△	△			△	○								
														D/O NO.						○								
							→							D/O サイン						○								
△				→		→	→							TRANSHIP TO		△												

輸出															輸入													
依頼書	INV.	P/L	Ⓑ E/D	S/I	Ⓒ E/D	S/O	B/L							データ名	依頼書	B/L	INV.	P/L	IMPORT INST.	D/O	Ⓒ I/D							
														引取形態区分 (CY・CFS 直取総揚)					⊕									
														入港年月日					⊕	○	⊖							
														搬入予定年月日					⊕									
														〃 年月日					⊕									
														仮搬入年月日					⊖									
														I/L期限					⨹									
														〃 枚数	△				⨹									
														出荷先名	△				○									
														〃 住所	△				○									
														運送保険金額(国内)					△									
														運賃支払区分(元着)	△				○									
														評価申告番号	△				○									
														船(取)卸港符号							⊕							
														原産国(地)符号							⊕							
														輸入者符号							⊕							
														船(取)卸港							⊕							
														原産地(都市)(国)							⊕							
														積出地(都市)(国)							⊖							
														税 番	△				○		⊕							
														申告価格(CIF)					○		⊕							
														税 率	△				○		⊕							
														関税額					○		⊕							
														減免税条項適用区分							⊕							
														評価申告欄							⊕							
														税額合計					○		⊕							
					⊕									他法令添付チェック					⨹		⨹							

表３－２　貨物管理上のデータ動勢表

記号説明

◎ 固定データ　△ 受取不確定データ　⊖ 転記データ　⏃ 発生データ　○ 受取データ　⊕ 発生・優先データ　→ 不確定転記データ

輸出														輸入														
入庫予告	送状	自主記帳台帳又は◎搬入届	貨物受領書	施検票	港湾局搬入届	入庫才検量報告書	入庫報告書	船積作業指示書	自主記帳台帳又は◎搬出届	港湾局搬出届	船積報告書			データ名	搬入連絡	タリーシート	自主記帳台帳又は搬入届	港湾局搬入届	入庫報告書	業務予定表	配送指示書	配送控	自主記帳台帳又は搬出届	港湾局搬出届	出庫依頼書	送状	貨物受領書	配送案内
△														発送予定年月日						⊕								
△	△		→				⊕	⊕			⏃			諸掛請求先					⊕	⊖		⊖						⊖
△	△	⊕	⊖	⊖	⊖	→	⊕	⊕	⊖	⊖	⊖			荷主名	○	○	⊕	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖
△	○		⊖											出荷主名							⏃	→			→	→	→	→
△	○		⊖											輸送業者名						⊕	⊖	⊖			⊖	⊖	⊖	⊖
△	○	⊖	⊖	⊖	⊖	⊖	⊖	⊕	⊖	⊖	⊖			品名	○	○	→	⊖		⊕	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖
△	○	⊖	⊖	⊖	⊖	⊖	⊖	⊕	⊖	⊖	⊖			個数（ロット数）	○	○	→	⊖	⊖	⊕	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖
	○		⊖											発送年月日							⊕	⊖			⊖	⊖	⊖	⊖
△	○	◎	⊖	◎	◎	⊖	◎	◎	◎	◎	◎			海貨通関業者名	○	○	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎
	△	→	→	→	→	→	→	⊕	⊖	⊖	⊖			船名	○	○	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖
		→	→											積出地	△	△	△	△	△									
	△	→	→	→	→	→	→	⊕	⊖	⊖	⊖			仕向地														
	△	→	→	→	→	→	→	⊕	⊖	⊖	⊖			シッピングマーク	○	○	⊖	⊖	⊖		⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖
	△	→	→	→	→	→	→	⊕	⊖	⊖	⊖			ケース№	△	△	→	→	→		→	→	→	→	→	→	→	→
	⊕	⊕	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖				搬入場所名	○	○	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖
	⏃		→				⊖	⏃			⏃			リマーク欄	△	△	→	→	→									
	⊕		⊕											荷受者印又はサイン														
	⊕		⊖	⊖	⊖	⊖	⊖			⊖	⊖			入庫（受取）年月日	○	○			⊖									
	⊕	⊕	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖			入庫番号			⊕	⊖	⊖		⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖
		⊕			⊕				⊕	⊕				届出年月日			⊕	⊕					⊕	⊕				
		⊕			⊕									搬出予定年月日						⊕								
		⏃							⏃					搬入出に関する許可又は承諾の種類・番号・年月日			⏃						⏃					
		⊕							⊕					容積	○		⊖		⊖	⊖			⊖					
		⊕							⊕					重量	○		⊖		⊖	⊖			⊕					
		⊕							⊖					搬入年月日			⊕	⊖					⊖	⊖				
				⊕		⊖	→							ディメンション														
				⊕		⊖	→							@WEIGHT 又は TOTAL WEIGHT														
				⊕										検量担当サイン又は印														
						⊕	→	⊖			⊖			MEASUREMENT & WEIGHT														
					⊕					⊕				入港年月日			⊕	⊖	⊖	⊖	⊖							
					⊕					⊖				蔵置場所の種類				⊕						⊖				
					⊕					⊕				重量トン				⊕						⊕				

輸出												
入庫予告	送状	自主記帳台帳又は◎搬入届	貨物受領書	施検票	港湾局搬入届	入庫才検量報告書	入庫報告書	船積作業指示書	自主記帳台帳又は◎搬出届	港湾局搬出届	船積報告書	
								⊕	⊕		⚓	
								⊕			⊕	
								⊕			⚓	
								⊕				
								⚓				
								⊕			⊖	
								⊕				
								⚓				
								⊕				
									⊕	⊕		
	△	→					→	→	→		→	
△	△	→		→		→	→	→	→		→	
											⊕	
		\⊕			⊖				⊖	⊖		
	△							⊕			⊖	

輸入																				
データ名	搬入連絡	タリーシート	自主記帳台帳又は搬入届	港湾局搬入届	入庫報告書	業務予定表	配送指示書	配送控	自主記帳台帳又は搬出届	港湾局搬出届	出庫依頼書	送状	貨物受領書	配送通関
CE/D(I/D) No.						⊕	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖
船積形式	○	○			⊖									
バース	△	△												
ステベ	△	△												
船名	△	△												
S/I No.														
S/O No.														
検数業者名	△	○												
出庫予定日時														
搬出年月日							⊕	⊖	⊖	⊖	⊖	⊖	⊖	⊖
ドキュメントKEY No.						⊕	→	→	→	→	→	→	→	→
貨物KEY No.	△	△					→	→	→	→	→	→	→	→
船積卸完了日														
運送方法						⊕								
積出港														
揚地	○	○												
D/O No.						⚓								
B/L No.						⚓								

1.3.4　共同利用センターにおける総括的システム・フロー

前項の業種別業務標準フローを，共同利用センターにおける総括的システム・フローに整理して得たものが，図３－１２に示すフローチャートである。先ず輸出と輸入とに分け，それぞれの処理手順にしたがって，輸出の場合には，それぞれの処理ノードにＥ０１，Ｅ０２，Ｅ０３……の記号を附した。この中にＰ－Ｘという記号があるが，これは，港湾管理者のポート・システムのＸであるという意味である。輸入については，それぞれＩ０１，Ｉ０２，Ｉ０３……の記号を附した。これらの記号は，次に出て来るジョブ処理概要に記入されている「ジョブ名」のそれぞれの番号に一致する。

コンピュータ処理をどこから始めるかという点について，海貨通関業者が貨物を受取った時点で，データをインプットすることにした。これは現在の業務の関連から最も現実的な方法である。但し，将来構想としては，さきに述べたように貨物送り状，受領書，シエッドマスターの三点セットの標準帳票をつくり，これを海貨通関業者が受領しインプットする。（将来構想①）。更に次の段階においては，輸出者自身が入力する（将来構想②）。この関係は図７－２に示されている。

この処理フローで明らかなように，ドキュメンテーションと貨物管理とは実際の処理においては，分割し得ないものである。この報告書で，ドキュメンテーションと貨物管理とをとり出して，別々に後に記述するが，この区分はあくまでも概念的なものである。特にドキュメンテーションは国際的標準化と関連を持つので，標準化の観点から現在ＪASTPROが作成している標準帳票をベースにするたてまえから，このような区分をしたものである。また，輸入においては，体系的なドキュメンテーション，すなわち書類作成事務は，I／D 等，１，２のものしか存在しないので，これを省略した。

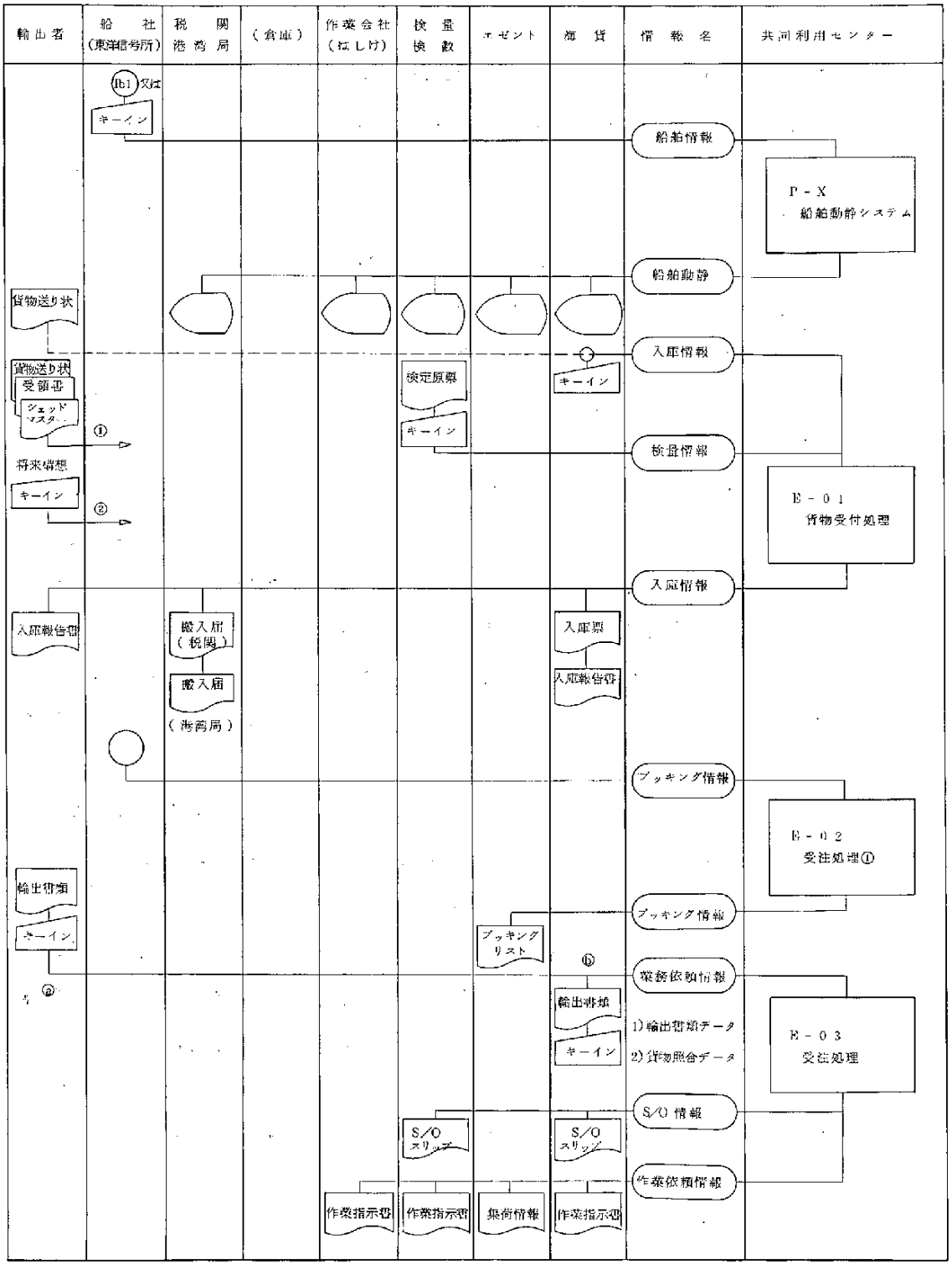
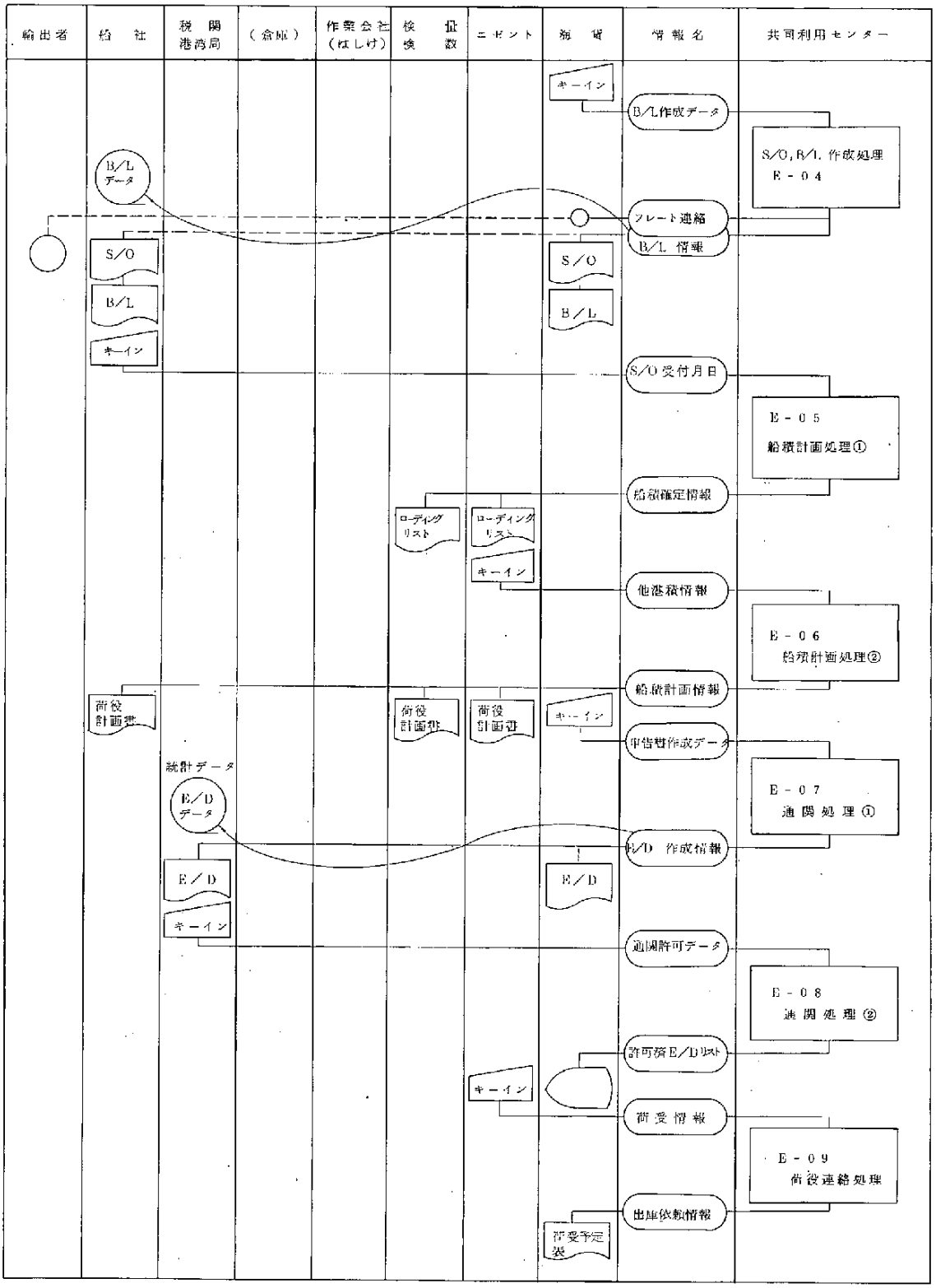


図３－１２　共同利用センターにおける輸出業務処理フロー(1)

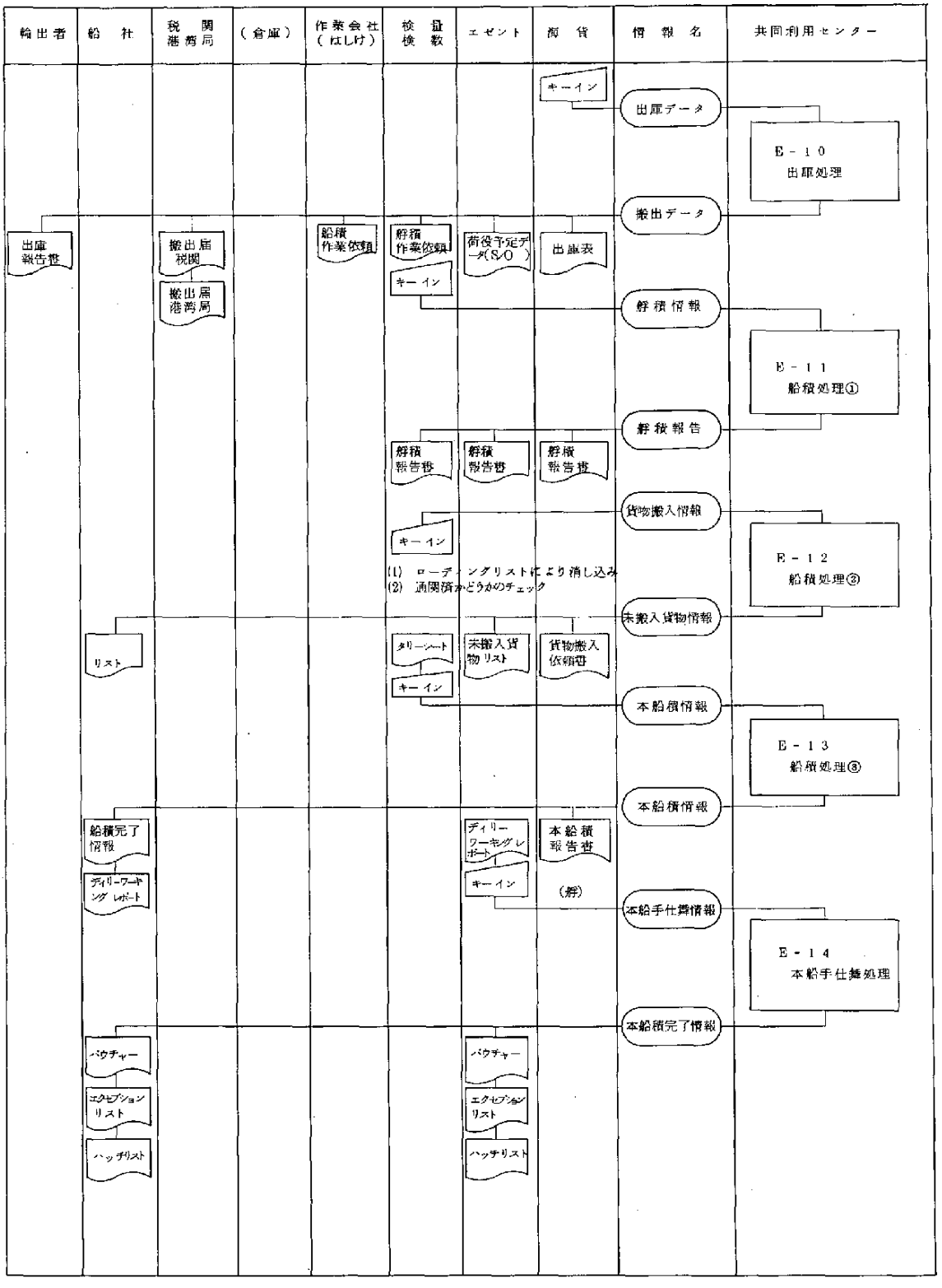
前頁の続き

輸出業務処理フロー(2)



前頁の続き

輸出業務処理フロー(3)



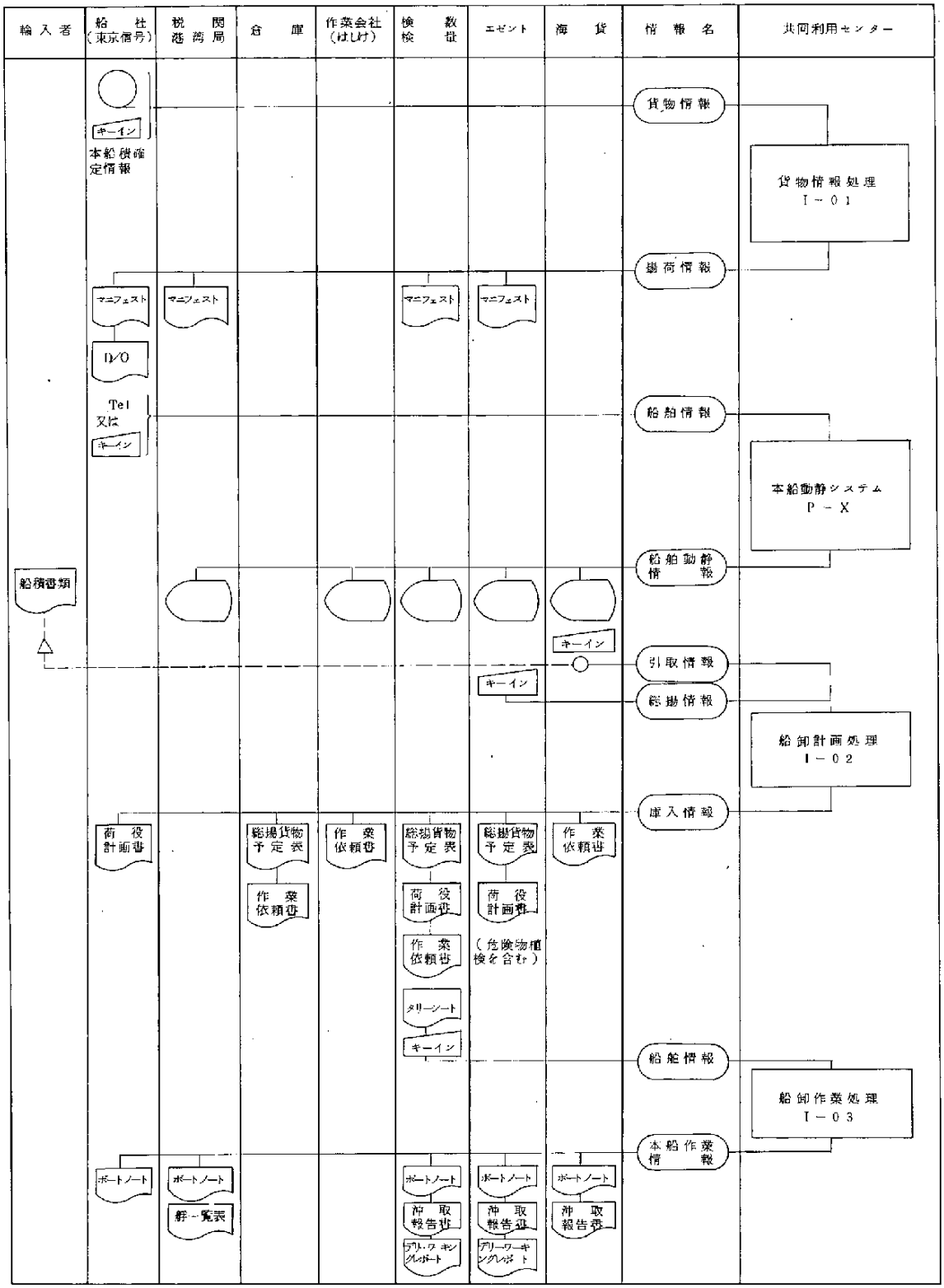
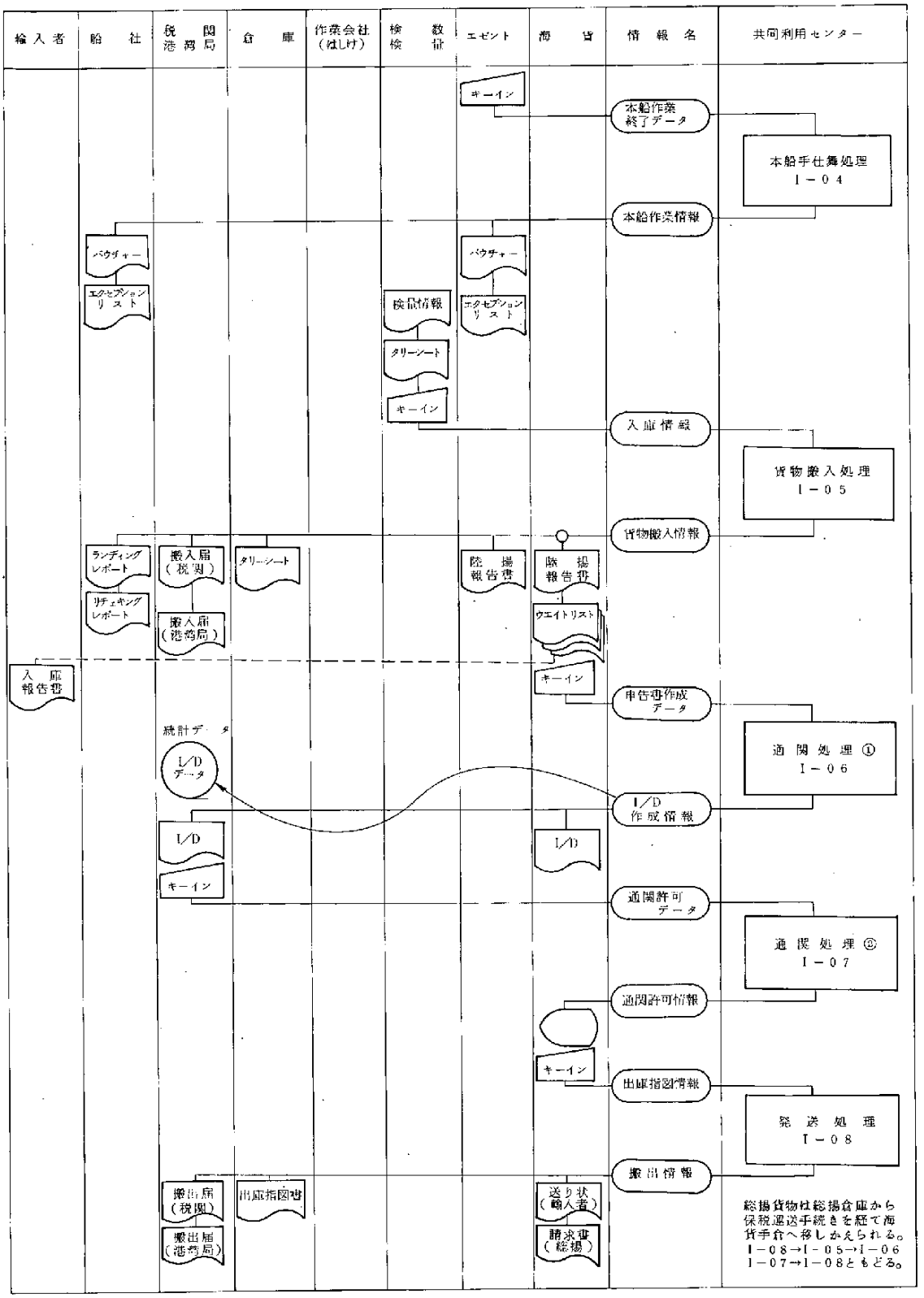


図３－１３　共同利用センターにおける輸入貨物処理フロー（1）

前頁の続き

輸入業務処理フロー（2）



1.3.5 共同利用センターにおけるセキュリティ対策

－ 主としてデータの機密保護の面から －

共同利用センターによると，データの機密性を保持するのは非常に難しいと一般的に受け取られている。機密の漏洩は，情報の集積が大きくなると危険性が増し，また共同処理という業務体制によって他社の情報にアクセスしやすくなる。

特にコンピュータによるデータの集積と共同利用においては，オンラインにより遠隔地からでも顔を見られずに，データにアクセスすることが可能である。持ち運び可能な一巻の磁気テープには数千万字が収容されていて，1本でも盗まれると大変なことになる。また，コンピュータに記憶されているデータの探索は非常に容易になっており，必要なデータを僅かの時間で取り出すことが可能である。

このためコンピュータ室への入室管理，データベースへのアクセス・コントロール，オンライン端末のユーザーの確認等，多くの対策を立てることが必要となる。

1シップメントごとのセキュリティを確立するために，

① 当該シップメントに携わる関係者を登録する。これ以外からの問い合わせには応じない。

② 端末機とオペレーターのパスワードを設ける。他の方法，他の者にはタッチさせない。

③ 共同利用目的に沿う事項に限り，集積，処理する。機密事項に関わる事項は除外する。（例，コマシャール・インボイスの価格等）

④ 請求業務は，エゼント業務の一部を除くほか，原則的には社内業務処理に委ねられている。（共同集金のできるものは，実施可能である。）

データはエレメントについてではなく，データの1シップメントごと，1隻ごと，1パースごとが機密保持の対象となりうるので，個々のデータエレメントにマスクをかけることは意味がない。検索項目の限定により行う。

2. ジョブ処理の概要

2.1 ジョブの配列

さきに総論において述べたように，ドキュメンテーションと貨物管理とは，このオンライン・データベースの考え方においては，分割し得ないものであるが，記述の便宜上，ないしは個々の企業のシステム開発の手順の上から，両者を別々に開発することが有り得る。このような観点から，本報告書においては，次章に示すように，ドキュメンテーションと貨物管理との二つのカテゴリーに分けて記述する。その方が概念的に理解しやすいし，かつ一般的だからである。

但しここにジョブ処理の概要を説明するに当っては，ゼネラルフローとの対比上，輸出と輸入に分けて作業の時系列にしたがって配列する。

a) 輸　出

E－01　貨物受付処理
E－02　受注処理①
E－03　受注処理②
E－04　S/O，B/L 作成処理
E－05　船積計画処理①
E－06　船積計画処理②
E－07　通関処理①
E－08　通関処理②
E－09　荷受連絡処理
E－10　出庫処理
E－11　船積処理①
E－12　船積処理②
E－13　船積処理③
E－14　本船手仕舞処理

b) 輸　　入

Ｉ－０１	貨物情報処理
Ｉ－０２	船卸計画処理
Ｉ－０３	船卸作業処理
Ｉ－０４	本船手仕舞処理
Ｉ－０５	貨物搬入処理
Ｉ－０６	通　関　処　理　①
Ｉ－０７	通　関　処　理　②
Ｉ－０８	発　送　処　理

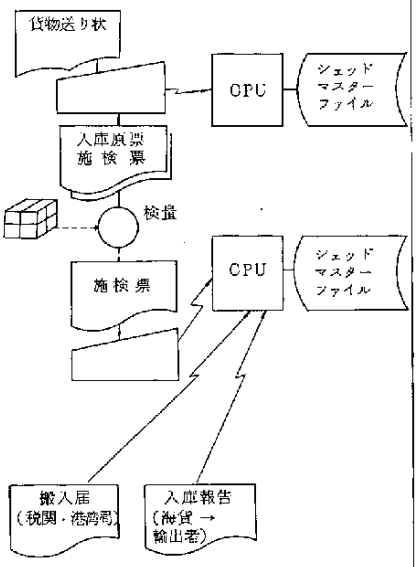
2.2　ジョブ処理の内容

以上の配列にしたがって，先ずジョブ毎の処理チャートを示し，作業の流れと入出力関係，ファイルとの関係を示し，処理の前提条件，処理概要の説明を行い，処理形態（オンライン・リアル，リモート・バッチ，バッチ），キー・アイテムの選定を行った。次に入出力，ファイル名を列記し，それぞれＩ（インプット），Ｏ（アウトプット），Ｆ（ファイル）の別を記入した。次にそれぞれのアイテムに対する入出力先，および媒体を明記し，それぞれについて必要ある場合には備考欄に説明を加えている。

ジョブ処理概要（1）

ジョブ名	業務名		処理形態			キー・アイテム
E－01 貨物受付処理	輸出		①オンラインリアル 2 リモートバッチ 3 バッチ			入庫 No

（ジョブチャート）



処理概要

処理の前提条件

① 搬入先（上屋名，スペースの有無）が決まっている。

② 貨物を搬入現場で受付る際のシステム

処理の概要

① 貨物送り状によって，入庫原票（ジェッドマスター及び施検原票）を端末機によって出力する。

② 施検票によって，入庫検量を行い，検量データを入力する（キーは入庫ナンバー）

③ 入庫報告書，搬入届の出力

④ 税関，港湾局へ搬入届の出力

入出力・ファイル名	I・O・F 区分	桁数	入出力先	媒体	備考
貨物送り状	I	743	海貨	キーイン	キーアイテムは入庫ナンバー
施検結果	I	554	検量	キーイン	施検票と共通
入庫原票	O	554	海貨	リスト	
入庫報告書	O	644	海貨→輸出者	リスト	
搬入届	O	566	税関	リスト	
搬入届	O	566	港湾局	リスト	
ジェットマスタ ファイル	F	1,185		ディスク	貨物送り状及びディメンションのアイテムに有効情報が盛られている。

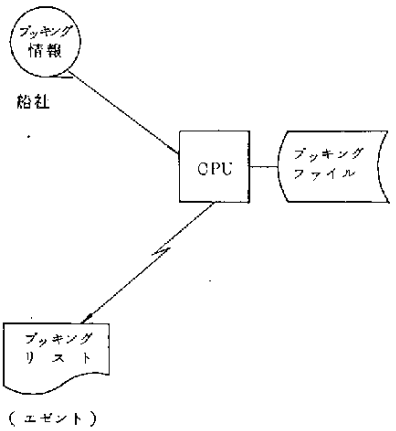
備考

図3－14

ジョブ処理概要（２）

ジョブ名	業務名		処理形態			キー・アイテム
E－０２ 受注処理①	輸出		①オンラインリアル ２リモートバッチ ３バッチ			ブッキング No.

（ジョブチャート）



処理概要

前提条件

① ブッキング締切と同時に船社よりブッキング情報をバッチでもらう。

② 貨物の予約情報とみなす。

処理概要

① 船社により，ブッキング情報をＭＴで入力する。

② ブッキングリストをエゼントに出力する。

③ Ｓ／Ｏナンバー確定段階（Ｅ－０５処理後）で消込みする。

入出力・ファイル名	I･O･F区分	桁数	入出力先	媒体	備考
ブッキング・テープ	I	２４０	船社	ＭＴ	
ブッキング・リスト	O	２４０	エゼント	リスト	
ブッキング・ファイル	F	３８２		ディスク	

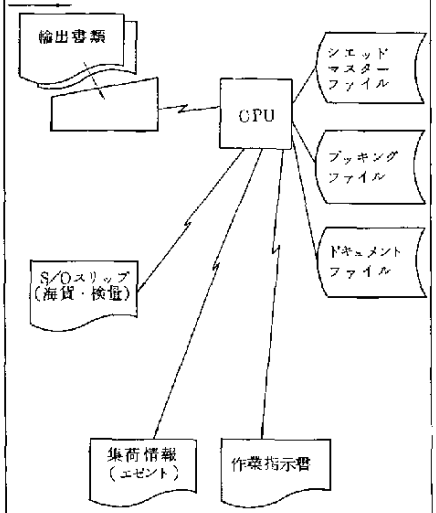
備考　ブッキング締切は船腹いかんにより，出港直前までに至ることがある。

図３－１５

ジョブ処理概要（３）

ジョブ名	業務名		処理形態			キー・アイテム
E－０３ 受注処理②	輸出		①オンラインリアル ２リモートバッチ ３バッチ			入庫No ブッキングNo INVOICE No

（ジョブチャート）



処理概要

前提条件

① 海貨は輸出書類一式を受け取る（輸出者より）

② 貨物が入庫済又は未入庫の状況がある。

③ ブッキング済であること（ブックしていない場合はＥ－０２受注処理に遡及してブックする）

概要

① ブッキングNoによって確認，本船データを入力

② PACKING LIST によって入庫Noを参照　入庫データを索引

③ 未入庫については入庫No（入庫データ待ち）は無し

④ S/INSTRUC によってドキュメント情報の入力（ドキュメントファイル）を作成　キーアイテムはインボイスNo

⑤ 入庫データは輸出書類単位でまとめられて（Ｓ／Ｏ単位）Ｓ／Ｏスリップ作成

⑥ 作業指示情報の出力

⑦ ブッキングデータの検索によってエゼントは集荷情報が入手可能

入出力・ファイル名	I・O・F区分	桁数	入出力先	媒体	備考
輸出書類　（S／I）	I	1,010	輸出者→海貨	キーイン	
〃　（P／L）	I	955	〃　〃	〃	
S／O スリップ	O	982	検量・海貨	リスト	
作業指示書	O	784	作業会社	〃	
			検数	〃	
			海貨	〃	
集荷情報	O	240	エゼント	リスト	ブッキングファイルと共通
シェッドマスター・ファイル	F	1,185		ディスク	
ブッキング・ファイル	F	382		〃	
ドキュメント・ファイル	F	1,963		〃	

備考

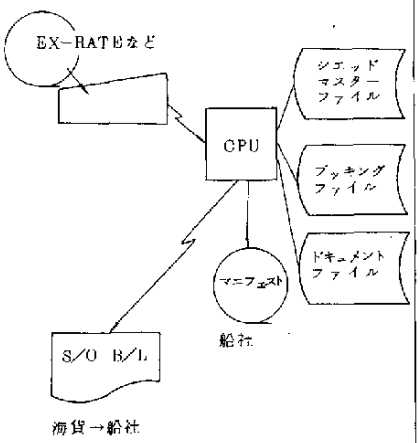
1. 現状では，海貨が社内処理上Ｓ／Ｉ Noを基準としている。
2. ドキュメント・ファイルの入力は，輸出者(a)，海貨(b)の２通りあげてあるが，海貨が荷主に代行して作成することがある場合を示している。

図３－１６

ジョブ処理概要（４）

ジョブ名	業務名		処理形態			キー・アイテム
E－０４ S/O,B/L 作成処理	輸出		①オンラインリアル ２リモートバッチ ３バッチ			ブッキングNo インボイスNo

（ジョブチャート）



処理概要

前提条件

① 貨物入庫済（E-01 貨物受付処理）輸出書類入手済（E-03 受注処理②），ブッキング済（E-02 受注処理②）が完了している。

② 本船出航予定日（その前日の為替レートEX-RATE）が決まる。

概要

① 同盟タリフによって，フレートの算出

② フレート情報を海貨→輸出者に提供

③ S/O，B/L の出力

④ 出力されたS/O,B/Lのオリジナルを海貨は船社に持って行ってサインを受ける。

⑤ 船社はS/O,B/Lの受付（サイン）によって，次のE-05 船積計画処理の入力データとなる。

⑥ 一定時点（バッチ処理）に船社に対しデータ（マニュフェスト）をM/Tで提供する。

入出力・ファイル名	I・O・F区分	桁・数	入出力先	媒体	備考
B/L 作成データ	I	185	船社→海貨 （船社入力か？）	キーイン	EX-RATE，本船出港予定日など
S/O，B/L セット	O	1,189	海貨→船社	リスト	
マニュフェストテープ	O	610	センター→船社	M/T	輸入マニフェストの共通
シエッドマスターファイル	F	1,185		ディスク	
ブッキング・ファイル	F	382		〃	
ドキュメント・ファイル	F	1,963		〃	

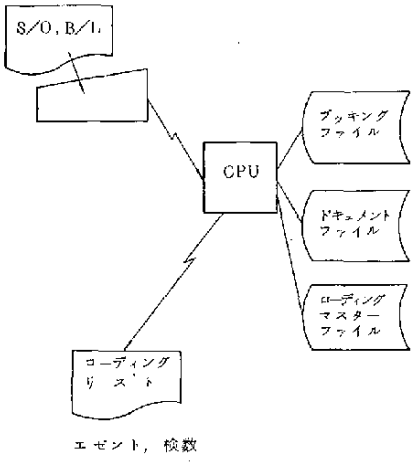
備考

図３－１７

ジョブ処理概要（５）

ジョブ名	業務名		処理形態			キー・アイテム
E－０５ 船積計画処理①	輸出		①オンラインリアル ２リモートバッチ ３バッチ			ブッキング No. インボイス No. B/L No. 船舶コード Voy No.

（ジョブチャート）



処理概要

前提条件

① 貨物受付→S/O,B/L作成（E-01,02,03,04）が完了している。

② アレートの支払い条件が決まっている。

③ 同盟タリフ社ファイル化していること。

概要

① 船社に荷貨が持参したS/O,B/Lを受け付けたことによって，B/L番号などを入力

② ブッキング ファイルに船積許可（船社が）の情報を付加することによって消し込む。

③ 船積確定情報としてローディング リストを出力する。

④ ローディング・マスター・ファイルをつくる。

入出力・ファイル名	I・O・F区分	桁数	入出力先	媒体	備考
S/O 受付データ	I	28	船社	キーイン	SO No. 10　受付年月 8　B／L No. 10
ローディング・リスト	O	462	エゼント	リスト	
			検数	〃	
ブッキング・ファイル	F	382		ディスク	ブッキング・ファイルは，S／O受付けによって消し込みを行い，ローディングマスターファイルを作る。
ドキュメント・ファイル	F	1,963		〃	
ローディング・マスタ・ファイル	F	644		〃	

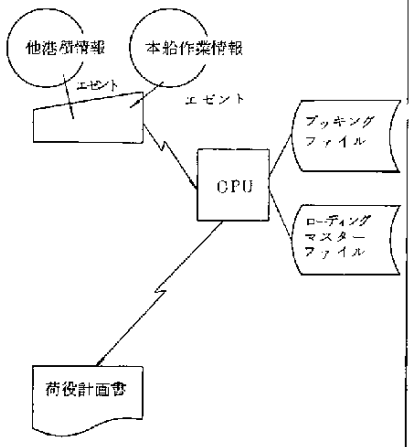
備考

図３－１８

ジョブ処理概要（6）

ジョブ名	業務名		処理形態			キー・アイテム
E－06 船積計画処理 ②	輸出		①オンラインリアル 2 リモートバッチ 3 バッチ			ブッキング No. インボイス No. B/L No. 船舶コード Voy No.

（ジョブチャート）



（船社・エゼント・検数）

処理概要

前提条件

① ブッキング締切日までE－02受注処理完了

② S/O受付（E－05船積計画処理）まで完了しているものはその付加されたデータを使い，無い場合はブッキング情報を使う。

③ エゼントに本船の他港積情報を電話などで収集可能とする。

概要

① 他港積情報として本船既積は情報を入力することによって，本船スペース（これから積み込める）を勘案して，ブック情報を充填する。

② 荷役計画書を出力する。ストウエージ・プランの資料とする。

③ ローディングマスターを展開することによって，レーバーシステムにつなげる。

入出力・ファイル名	I・O・F 区分	桁数	入出力先	媒体	備考
他港積情報	I	610	エゼント	キーイン	マニフェストと共通
本船作業情報	I	542	エゼント	キーイン	
荷役計画書	O	255	エゼント 船社検数	リスト	輸出入共通
ブッキングファイル	F	382		ディスク	
ローディング・マスター・ファイル	F	1,185		ディスク	

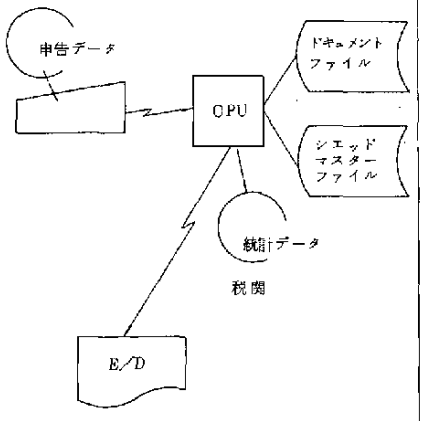
備考

図3－19

ジョブ処理概要（７）

ジョブ名	業務名		処理形態			キー・アイテム
E－０７ 通関処理①	輸出		①オンラインリアル １リモートバッチ ２バッチ			インボイスNo. 入庫No.

（ジョブチャート）



処理概要
前提条件

① 貨物受付処理（E－０１）が完了していること。

② 輸出申告の入力（E－０３）が完了していること。

③ 統計品目番号等コード等はファイル化していること。

概要

① 申告データ（申告税関名，換算レート，統計品目番号，輸出形態データなど）を入力する。

② 輸出申告書を出力する。

③ 統計テープの出力

入出力・ファイル名	I・O・F区分	桁数	入出力先	媒体	備考
申告データ	I	221	海貨	キーイン	
E／D	O	790	海貨	リスト	
統計データ	O	790	税関	M／T	E／Dと同じ
ドキュメント ファイル	F	1,963	センター→税関	ディスク	
シェッドマスター ファイル	F	1,185		〃	

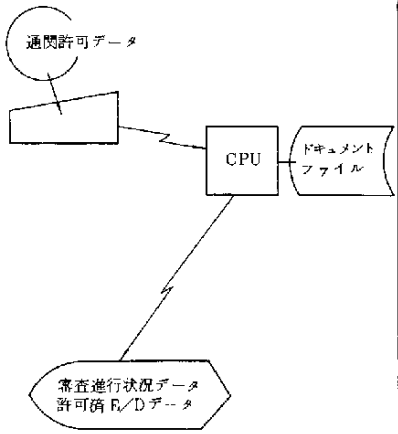
備考

図３－２０

ジョブ処理概要（８）

ジョブ名	業務名		処理形態			キー・アイテム
E－０８ 通関処理②	輸出		①オンラインリアル ２リモートバッチ ３バッチ			E／D No.

（ジョブチャート）



処理概要
前提条件

① E－０７ 通関処理が完了している。

② 許可書は海貨が税関から承認印を押したものを受けとる。

概要

① 許可番号，年月日，審査進行状況などを入力し，ドキュメント・ファイルに記録する。

② 海貨業者は随時通関許可の可否をディスプレイで確認する。

入出力・ファイル名	I-O-F区分	桁数	入出力先	媒体	備考
通関許可データ	I	１５	税関	キーイン	
許可済E／Dデータ	O	７９０	海貨	ディスプレイ	
ドキュメント・ファイル	F	1,963		ディスク	

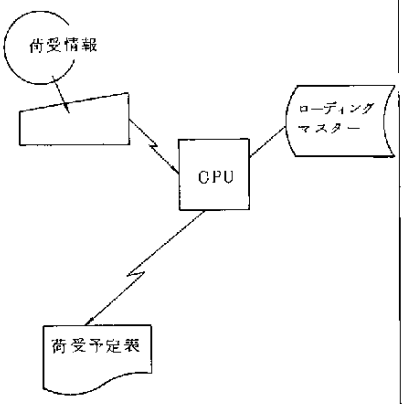
備考

図３－２１

ジョブ処理概要（９）

ジョブ名	業務名		処理形態			キー・アイテム
E－０９ 荷受連絡処理	輸　出		①オンラインリアル ２リモートバッチ ３バッチ			船舶コード Voy・No. インボイスNo.

（ジョブチャート）



処理情報
前提条件

①　E－０５．E－０６の船積計画処理が完了している。

②　本船入港日時，バースなどが確定している。

概要

①　荷受情報を入力する。

②　荷受予定表を出庫依頼情報として海貨に出力。

入出力・ファイル名	I・O・F区分	桁数	入出力先	媒体	備考
荷受情報	I	２３	エゼント	キーイン	SO／VO，荷受年月日と時間，バッチNo.
荷受予定表	O	４５８	海　貨	リスト	ローリングリストより２項目１６桁消除して２項目１　桁追加
ローディング・マスター・ファイル	F	６４４		ディスク	

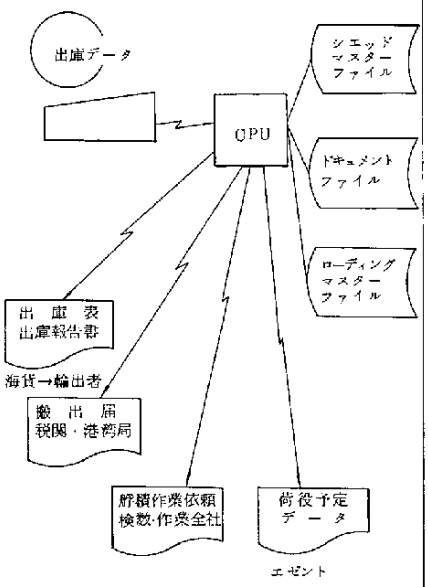
備考

図３－２２

ジョブ処理概要（10）

ジョブ名	業務名		処理形態			キー・アイテム
E－10 出庫処理	輸出		①オンラインリアル 2 リモートバッチ 3 バッチ			・インボイスNo ・入部No ・B/L No (S/O No)

（ジョブチャート）



処理概要
前提条件

① E－04 S/O，B/L作成処理とE－08通関処理②が完了している。

概要

① 出庫データ（インボイスNo，運送方法，船名，など）を入力

② 出庫表，搬出届，解積作業依頼，荷役予定などの出力

入出力・ファイル名	I・O・F区分	桁数	入出力先	媒体	備考
出庫データ	I	49	海貨	キーイン	
出庫表・出庫報告書	O	566	海貨→輸出者	リスト	搬出届と同じ
搬出届	O	599	税関・港湾局	〃	
解積作業依頼書	O	542	検数・作業会社	〃	
荷役予定データ	O	458	エゼント	〃	荷受予定表
シェッド・マスター・ファイル	F	1,185		ディスク	
ドキュメント・ファイル	F	1,963		〃	
ローディング・マスター・ファイル	F	644		〃	

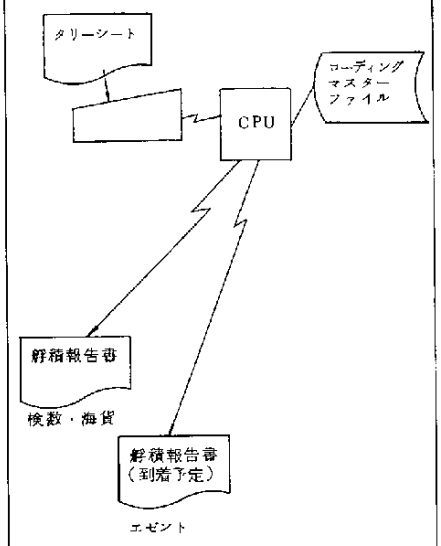
備考

図3－23

ジョブ処理概要（11）

ジョブ名	業務名		処理形態			キー・アイテム
E－11 船積処理①	輸出		①オンライン リアル 2 リモートバッチ 3 バッチ			B／L No 船舶コード Voy No.

（ジョブチャート）



処理概要
前提条件

① 船積作業が完了している（B／L 単位で，但し，ロット物の場合は船単位の情報を入力）

② 海貨上屋端末より（検数が）入力可能とする。

概要

① 船積タリーシートより入力する。

② 船積報告書の出力

③ エゼントに対しては貨物到着予告となる。

入出力・ファイル名	I・O・F 区分	桁数	入出力先	媒体	備考
タリーシート	I	689	検数	キーイン	
船積報告書	O	768	検数・海貨	リスト	
〃 （到着予告）	O	768	エゼント	リスト	
ローディング・マスターファイル	F	644		ディスク	

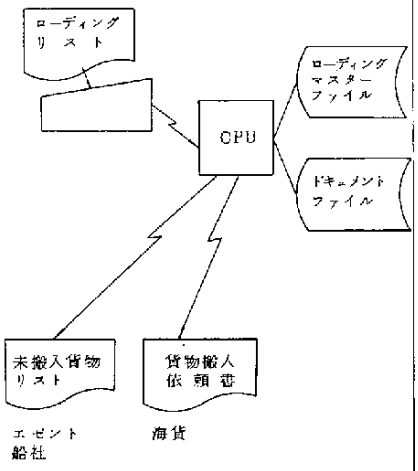
備考

図3－24

ジョブ処理概要（12）

ジョブ名	業務名		処理形態			キー・アイテム
E－12 船積処理②	輸出		①オンラインリアル 1 リモートバッチ 2 バッチ			B/L No. 船舶コード Voy No.

（ジョブチャート）



処理概要
前提条件

① GO-DOWN 貨物についてはS/O，E/Dが貨物と同時に到着していること。

② 直積貨物はS/O貨物が同時に到着している。

概要

① ローディング・リストより到着貨物の消し込み（B/L No個数など）によって入力し，ローディング・マスターファイルに登録する。

② ドキュメント・ファイルを参照して通関済か否かの確認

③ 未到着貨物について，未搬入貨物リストを出力し（船社，エゼントに対し），貨物搬入の催促を海貨に対し行う。

入出力・ファイル名	I-O-F区分	桁数	入出力先	媒体	備考
貨物搬入情報 （ローディング・リスト）	I	462	検数	キーイン	
未搬入貨物リスト	O		エゼント・船社	リスト	
貨物搬入依頼	O		海貨	リスト	
ローディング・マスターファイル	F	644		ディスク	
ドキュメント・ファイル	F	1,963		ディスク	

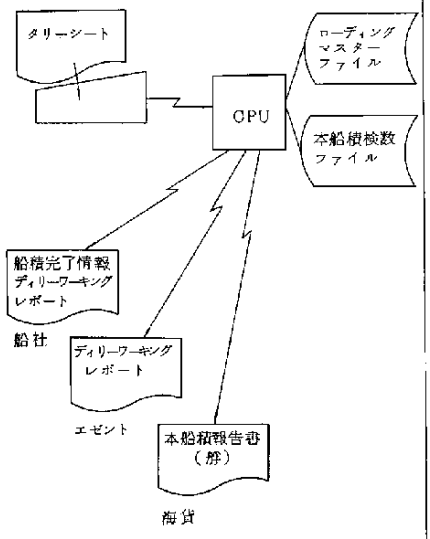
備考

図3－25

ジョブ処理概要（13）

ジョブ名	業務名		処理形態			キー・アイテム
E－13 船積処理③	輸出		1 オンラインリアル ②リモートバッチ 3 バッチ			B/L No. 船舶コード Voy No.

（ジョブチャート）



処理概要

前提条件

① バースごとに端末機を設置する

概要

① 本船積タリーシートによって入力する（タイムシートデータを含む）

② ローディングマスターファイルを消し込み，本船積検数ファイルを作成する。

③ 船積完了情報（確認），ディリーワーキング・レポート，本船積報告書（解）の出力。

入出力・ファイル名	I・O・F区分	桁数	入出力先	媒体	備考
タリーシート	I	689	検数	キーイン	
船積完了情報	O	240	船社	リスト	
ディリーワーキングレポート	O	240	船社・エゼント	リスト	
本船積報告書	O	240	荷貨	リスト	
ローディング・マスターファイル	F	644		ディスク	
本船積検数ファイル	F	1,238		ディスク	本船積貨物の確定情報

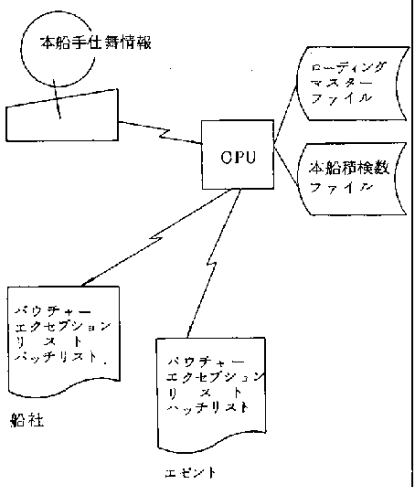
備考

図3－26

ジョブ処理概要（14）

ジョブ名	業務名		処理形態			キー・アイテム
E－14 本船手仕舞処理	輸出		1 オンラインリアル ②リモートバッチ 3 バッチ			B／L No. 船舶コード Voy No.

（ジョブチャート）



処理概要

前提条件

① 船積が完了（E－13船積処理③）している。

② ローディング・マスターの消し込み残（不積分）の処置が船社の承認の許に決定していること。

概要

① 船積終了情報の入力

② 本船積検数ファイルからバウチャー・エクセプションリスト
バッチリストを出力する。

③ エクセプションリストの中のキャンセル分をローディング
マスターファイルによって参照する。

入出力・ファイル名	I·O·F 区分	桁数	入出力先	媒体	備考
本船手仕舞情報	I		エゼント	キーイン	
バウチャー	O	509	船社・エゼント	リスト	
エクセプションリスト	O	505	〃 〃	〃	
バッチリスト	O		〃 〃	〃	
ローディング・マスターファイル	F	644		ディスク	
本船積検数ファイル	F	1,238		〃	

備考

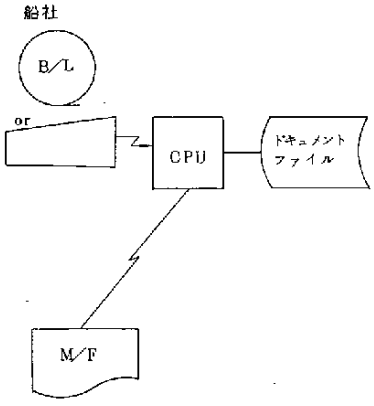
エクセプションリストにはキャンセルNoが入る。

図3－27

ジョブ処理概要（15）

ジョブ名	業務名		処理形態			キー・アイテム
I－01 貨物情報処理	輸入		1 オンラインリアル ②リモートバッチ 3 バッチ			B／L No. 船舶コード Voy No.

（ジョブチャート）



処理概要
前提条件

① 本船入港前に船社より貨物情報をもらう。

処理概要

① 船社よりM／Tまたはキーインで B／L データを入力する。

② ドキュメントファイルを作成する（キーは，船舶コード Voy No. と B/L No. とする）

③ マニフェストを出力する船社には，この他に D／O，A／N の出力ができる。

入出力・ファイル名	I・O・F 区分	桁数	入出力先	媒体	備考
B／L	I	1189		M／T	
ドキュメントファイル	F	775		キーイン ディスク	
M／F	O	610	エーゼント・検数 税関・船社	リスト	

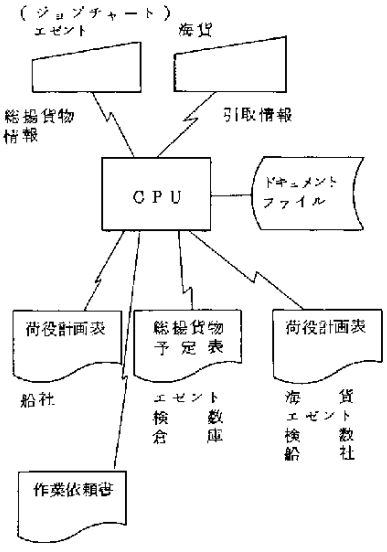
備考

図3－28

ジョブ処理概要（16）

ジョブ名	業務名		処理形態			キー・アイテム
I－02 船荷計画処理	輸入		1.オンラインリアル ②リモートバッチ 3.バッチ			B／L No. 船舶コード Voy No.

（ジョブチャート）



註　作業会社はエゼント又は海貨よりもらう。

処理概要
前提条件

① 海貨よりの引取情報が必要である（倉庫　）

② エゼントによる総揚貨物情報（危険品・唯検・倉庫名等）が必要である。（①を第1前提）

処理概要

① 海貨が輸入者より船積書類を受けて，引取情報（総揚げ直取りの別，倉庫名等）を入力する。

② エゼントは総揚貨物情報，品名コードを入力する。

③ ドキュメントファイルの不足データがカバーされる。

④ 底入情報として，海貨には作業依頼書（　），エゼントには総揚貨物予定表，荷役計画表，検数には総揚貨物予定表，荷役計画表，作業依頼書，倉庫には総揚げ貨物予定表，作業依頼書，作業会社（はしけ）には作業依頼書，船社には荷役計画表を出力する。

入出力・ファイル名	I·O·F区分	桁数	入出力先	媒体	備・考
総揚貨物データ	I	115	エーゼント	キーイン	
引取データ	I	775	海貨	キーイン	
ドキュメントファイル	F			ディスク	
D／O	O	475	船社	リスト	
総揚貨物予定表	O	653	海貨・検数・倉庫	リスト	
荷役計画表	O	255	海貨・エーゼント 検数・船社	リスト	
作業依頼書	O.	542	海貨・エーゼント 検数・倉庫	リスト	作業会社は海貨又はエーゼントよりリストをもらう。

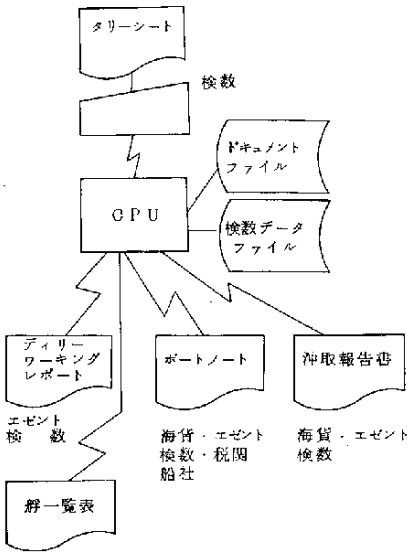
備考

図3－29

ジョブ処理概要（17）

ジョブ名	業務名		処理形態			キー・アイテム
I－03 船卸作業処理	輸入		①オンラインリアル 2 リモートバッチ 3 バッチ			船舶コード Voy No. B/L No. はしけ No.

（ジョブチャート）



処理概要

前提条件

① バースごと（あるいは本船ごと）に端末機を設置する。

処理概要

① 検数によりタリーシートのデータを本船近隣端末機より入力する。（タイムシートデータを含む）

② ドキュメントファイルの消込み照会を行い，リマークデータを追加し，検数データファイルをつくる。

③ 本船作業情報として，海貨にはB／N，沖取報告書，エゼントにはB／N，沖取報告書，DWR，検数にはB／N，沖取報告書，DNR，税引にはB／N，舲一覧表，船　　B／Nを出力する。

入出力・ファイル名	I-O-F区分	桁数	入出力先	媒体	備考
船卸しデータ	I		検数	キーイン	タリーシートをもとに入力する。
ドキュメント・ファイル	F	775		ディスク	
検数データ ファイル	F	1,238		ディスク	この処理で新しく作る。
デイリーワーキングレポート	O	240	エーゼント・検数	リスト	
ポート ノート	O	504	海貨・エーゼント 検数・税関 船社	リスト	
沖取報告書	O	782	海貨・エーゼント 検数	リスト	
舲一覧表	O	172	税関	リスト	

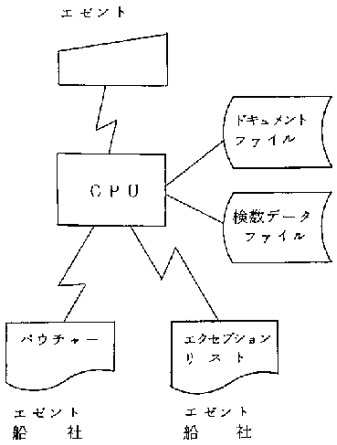
備考

図3－30

ジョブ処理概要（18）

ジョブ名	業務名		処理形態			キー・アイテム
I－04 本船手仕舞処理	輸　入		①オンラインリアル 2 リモートバッチ 3 バッヂ			船舶コード Voy No.

（ジョブチャート）



処理概要
前提条件

① 本船荷役終了日に行われる。

② 請求（対船社）データをもれなく入力する。

処理概要

① エゼントより本船作業終了データを入力する。

② 検数データ・ファイルよりエゼント・船社にはバウチャーを出力する。

③ ドキュメントファイルよりエゼント・船社にエクセプションリストを出力する。

入出力・ファイル名	I·O·F 区分	桁数	入出力先	媒体	備考
本船作業終了データ	I		エーゼント	キーイン	
ドキュメントファイル	F	775		ディスク	
検数データファイル	F	1,238		ディスク	
バウチャー	O	509	エ…ゼント・船社	リスト	
エクセプションリスト	O	505	エ…ゼント・船社	リスト	

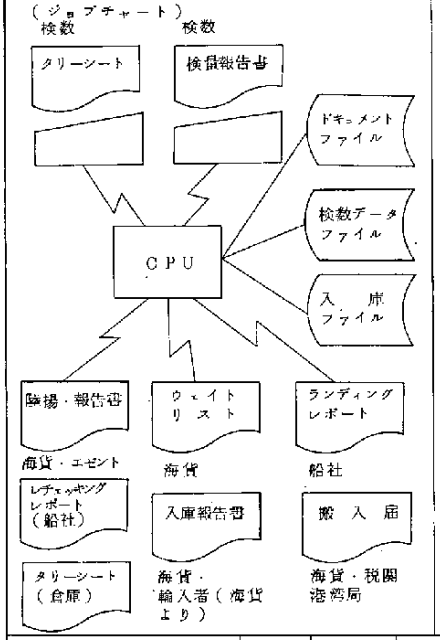
備考

図3－31

ジョブ処理概要（19）

ジョブ名	業務名		処理形態			キー・アイテム
I－05 貨物搬入処理	輸入		①オンラインリアル 2 リモートバッチ 3 バッチ			保管場所コード B/L No. 船舶コード Voy No. 搭 No.

（ジョブチャート）



処理概要

前提条件

① 貨物が倉庫・上屋等に搬入された時

② 解中扱いについては，通関処理①，②の処理後

③ 自主部帳による。

処理概要

① 検数より沿岸作業タリーシートデータを搬入場所近接の端末機より入力する。

② 検量より検量証明書データを搬入場所近接の端末機より入力する。

③ 貨物搬入情報を海貨には，陸揚報告書，ウェイトリスト，エゼントには陸揚報告書，倉庫には沿岸作業　シート，税関・港湾局には自主記　の型で，搬入届，船社にはランディングレポート，リチェックキング　ポート，　には海貨を通じ入庫報告書を出力する。

④ 入庫ファイルを新しく作成する。

入出力・ファイル名	I·O·F区分	桁数	入出力先	媒体	備考
揚荷データ	I		検数	キーイン	
検量データ	I		検量	キーイン	
ドキュメント・ファイル	F	775		ディスク	
検数データファイル	F	1.238		ディスク	
入庫ファイル	F	778		ディスク	
陸揚報告書	O	794	海貨・エゼント	リスト	
ウェイトリスト	O		海貨	リスト	
ランディングレポート	O		船社	リスト	
レチェッキングレポート	O	709	船社	リスト	
入庫報告書	O	476	海貨（輸入者）	リスト	
搬入届	O	545	海貨・税関・港湾局	リスト	
タリーシート	O	689	倉庫	リスト	

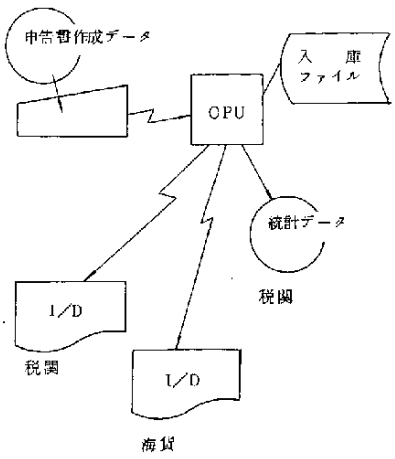
備考

図3－32

ジョブ処理概要（20）

ジョブ名	業務名		処理形態			キー・アイテム
I－06 通関処理①	輸入		①オンラインリアル 2 リモートバッチ 3 バッチ			B/L No 船舶コード Voy No インボイスNo 入庫No

（ジョブチャート）



処理概要

前提条件

① 貨物搬入処理（I－05）が完了していること。

② 船卸計重処理（I－02）が完了していること。

③ 評価申告等の諸手続きは完了しているものとする。

概要

① 申告データ（申告税関名，統計品目番号等）の入力

② 輸入申告書を出力する。

③ 統計テープの出力

④ 入庫ファイルを参照して数量などの申告データを追加登録する。

入出力・ファイル名	I・O・F区分	桁数	入出力先	媒体	備考
申告書作成データ	I		海貨	キーイン	
輸入申告書（I／D）	O		税関・海貨	リスト.	
統計テープ	O		センター→税関	M／T	
入庫ファイル	F	778		ディスク	

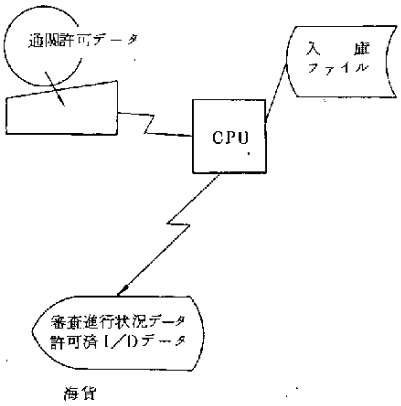
備考

図3－33

ジョブ処理概要（21）

ジョブ名	業務名		処理形態			キー・アイテム
I－07 通関処理②	輸入		①オンラインリアル 2 リモートバッチ 3 バッチ			I／D No

（ジョブチャート）



処理概要

前提条件

① 通関申告（I－06）が完了していること。

② 許可書に海貨が税関から承認印を押したものを受け取る。

概要

① 許可番号，年月日，審査進行状況などを入力し入庫ファイルに記録する。

② 海貨業者は随時，通関許可の可否をディスプレイで確認する。

入出力・ファイル名	I-O-F区分	桁数	入出力先	媒体	備考
通関許可データ	I		税関	キーイン	
許可済I Dデータ	O		海貨	ディスプレイ	
入庫ファイル	F	778		ディスク	

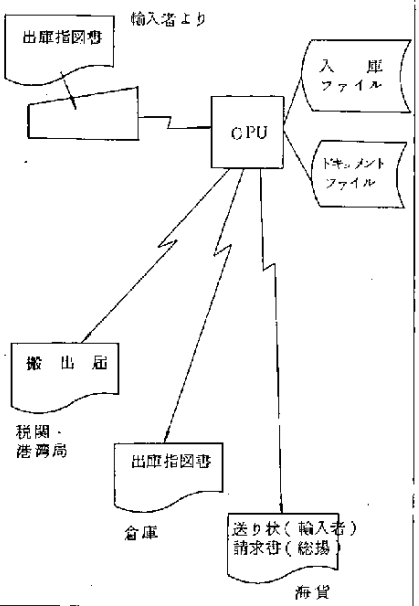
備考

図3－34

ジョブ処理概要（22）

ジョブ名	業務名		処理形態			キー・アイテム
I－08 発送処理	輸入		①オンラインリアル 2 リモートバッチ 3 バッチ			入庫No

（ジョブチャート）



処理概要

前提条件

① 通関許可（I－07）が完了していること。

② 保税運送の場合は貨物搬入処理 I－05 が完了していること。

概要

① 出庫指図書によって、入庫Noを参照、入庫データを索引する。

② 搬出届、出庫指図書（海貨から倉庫に対して）送り状（総揚の際の輸入諸掛の請求書など）を出力する。

入出力・ファイル名	I・O・F区分	桁数	入出力先	媒体	備考
出庫指図書	I		輸入者→海貨	キーイン	
搬出届	O	473	税関・港湾局	リスト	
出庫指図書	O	447	倉庫	リスト	
送り状・請求書	O	447	海貨	リスト	
入庫ファイル	F	778		ディスク	
ドキュメント・ファイル	F	775		ディスク	

備考

図3－35

3. 共同利用センターにおける輸出入情報システムのメリット

3.1 本システムのメリット評価の方法

3.1.1 メリットの評価項目

本輸出入情報処理システムの評価をするにあたり，次の方法によってメリットの評価を行った。

1) 評価項目

評価の角度として，このシステムの関係者が具体的なメリットがあると思われる四つの項目についてまとめてみた。

① 省力化

各種ドキュメント類作成作業，チェック作業，提出作業，連絡情報提供作業（電話・打合せ），自社システム情報入力作業等の省力化のメリットなどを含む。

② 迅速化

帳票・管理資料作成の迅速化，情報検索・伝達の迅速化のメリットがある。

③ 正確化

入出力情報の正確化の向上〔データの正確化（各種チェックシステムによる），転記ミスの減少〕によるメリットがある。

④ 簡素化

各業者間の電話問合せ，打合会合などの減少，帳票類の整理統合による簡素化などのメリットを含む。

⑤ 管理水準の向上

管理資料作成，管理項目の細分化，管理サイクルにマッチした管理資料の提供，リアルタイムでできる情報検索などにより管理水準の向上にメリットがあるものを含む。

3.1.2　4項目の評価の方法　　5段階点数制の採用

現状の作業水準をベースにして，このシステムが完成し，十分に期待通りに運営された場合を設定し5段階点数制で評価を行った。

㋑	非常にメリットのあるもの	＋2点
㋺	メリットのあるもの	＋1点
㋩	現状と変わらないもの	0点
㋥	デメリットが出るもの	－1点
㋭	非常にデメリットが出るもの	－2点

3.1.3　評価を行った者

本システム設計作業を行ったワーキング・グループメンバーである各業者（海貨・エゼント・検数・検量業者）の委員が，自己の業界を担当し，原案を出し，委員全員で検討を行った。

ただし，税関および港湾局のメリット評価は，ワーキンググループ全員で討議を重ねて推定した。（表3－3～表3－5の共同利用センターによる処理評価表）

3.1.4　対象業務

共同利用センターで行う業務を輸出業務は15処理，輸入業務は9処理計24処理について評価を行った。各業務処理を行うことによって受ける各利用者のメリット，デメリットをそれぞれ評価した。

（表3－6～表3－22の共同利用センターによる処理評価表）

3.2　輸出入情報システムのメリット評価

3.2.1　全体の評価

輸出入情報システム全体として265点のメリットがあると評価した。（表3－3）これを評価項目別にみると（図3－36参照），正確化のメリ

ットが第1位（６９点，全体の２６％）を占め，迅速化（６１点，２３％），簡素化（５９点，２２％），管理水準向上（５２点，２０％）がほぼ同水準で続いている。これに反して省力化のメリットは２４点，９％と小さく評価されている。

本システム開発のねらいが業務処理の正確化・迅速化・簡素化に大きなウェイトを占めていることが明らかになっている。

観点を変えて利用者別に共同利用センターのメリットを見ると，（図３－３７）エゼント業者が（６７点，２５％）と一番メリットを受けている。次に海貨業（５５点，２１％），検数業者（５５点，２１％）がこれに続き，この3業者で全体の６６％を占めていることがわかる。この3業者が共同利用センター利用の中核的存在になるであろう。

業者別に見てメリットの大きな項目は，海貨業者では業務処理の簡素化が３１％でトップを占め，迅速化，正確化がこれに続いている。海貨業者では省力化効果が７％と少いのが特徴である。これはインプットデータ作成作業が多いためである。

エゼント業者では迅速化が全体の３１％で最大のメリットを生じ，省力化のメリットがこれに続いており，海貨業者と好対照である。検数業者は正確化（３６％），管理水準向上（３３％）とこの二つで６９％と過半数を占め，逆に省力化効果は入力作業の増大により現行よりデメリットがあると評価している。しかしそのデメリットは少なく，全体の５％でその他のメリットで十分カバーしている。

その他の利用者は前述3業者に比較してメリットは少ないが，検量業者では省力化のメリット，倉庫業者では省力化と簡素化のメリット，税関では正確化のメリット，港湾局では迅速化と正確化のメリット，船社では簡素化のメリットがそれぞれ一番大きくなっている。

輸出業務と輸入業務とのメリットの比較検討すると次の事が明らかになる。（図３－３８参照）輸入業務のメリット合計は１３０点，輸入業務は135点

とほぼ同じ量のメリットが出ると評価した。メリット項目別に見ると輸出業務は管理水準向上メリットが多く，逆に省力化のメリットは一番少ない。迅速化，正確化，簡素化のメリットは輸出業務，輸入業務ともほぼ同じ水準にある。輸入業務は省力化のメリットが輸出に比較して大きい事が特色といえる。

荷主と船社への波及効果

このメリット評価において荷主は，共同利用センターを直接利用しないため評価対象から除外した。しかし共同利用センターでドキュメンテーション処理が迅速に行われ，B／Lが1日早く荷主に渡れば，月間にして数億円の金利負担が軽減されると考えられる。

船社は共同利用センターとインタフェースを持ち，その直接的メリットは評価の対象とした。さらに船社にとっては，輸出入業務処理の迅速化が促進されると，本船（1万トンクラス）の出港が1日早まれば約100万円の経費節減が見込まれる。

以上のごとく共同利用センターを利用する港湾業者のメリットより，荷主および船社が受ける波及効果は非常に大きなものである。

3.2.2 輸出業務処理のメリット

① 評価項目から見ると

輸出業務処理のメリットを5評価項目から見ると，正確化，迅速化，管理水準向上，簡素化のメリットがほぼ同水準（21～27％の巾にある）にあり，省力化のメリットが極めて少ない（9点，7％）のが特色である。

これはデータ入力作業が多く，あまり省力化が期待できないためである。（表3－7，図3－8参照）

② 利用者別メリット評価

輸出業務処理を共同利用センターで行い最も大きなメリットを受ける業者は海貨業者である（33点，25％）。海貨業者のメリットで一番大き

いのは簡素化のメリット（１１点，３４％）で，管理水準向上，正確化，迅速化のメリットがこれに続き，省力化のメリットは（３点，９％）と小さい。つぎにエゼント業者（３１点，２４％），検数業者（25点，19％）であり，この3業者で全体のメリットの６８％を占め，3業者へのメリットのウェイトが強いことが明らかになった。

港湾局，船社，税関にとっては正確化，迅速化メリットが多く出ている。（図３－８，図３－９参照）

③ 対象業務

輸出業務処理として１５業務について検討をしてみると，本船手仕舞処理が全体のメリットの１６％を占め，電算化効果が一番出る業務である。つぎにドキュメンテーション・システムの中心をなすS／O，B／L 作成処理の１３％と続き，B／L作成の電算化が重要なキーになっていることがわかる。この2業務に船舶動静システムを加えると全体の４１％のメリットを占めている。さらに貨物受付処理・荷受連絡処理・出庫処理の3業務を加えると全体のメリットの約７０％に達し，上記6業務が輸入業務処理のメインをなすことが明らかになった。

逆にメリットの少ない業務は通関処理①，受注処理①，船積処理，船積計画処理㋐などがあるが，これらの業務は，現行処理とほとんど変更がないもの，単独業務としてはメリットは少ないが関連業務を含めるとメリットが出てくるものなどのためである。そのためメリットが少ないため業務処理をやめるわけにはいかないものである。（図３－５）

3.2.3 輸入業務処理のメリット

① 評価項目から見ると

輸入業務処理のメリットは正確さ，迅速化，簡素化がそれぞれ全体の２６％，２３％，２３％と計７２％を占め，この三つにメリットが集中している。輸出業務処理と異なり，エゼント業者を中心に省力化のメリット

が出ているのが特徴である。（表３－５，図３－４３）

② 利用者別メリット評価

輸入業務処理ではエゼント業者のメリットが一番大きい(36点, 27％)。次に検数業者（３０点，２３％）でこの両者で全体の５０％のメリットを受けている。これに海貨業者を入れると全体の６６％となり，輸出入業務ともこれら3業者のメリットが他業者に比較して大きいことがわかる。

エゼント業者は管理水準向上メリットはあまりなく他の４項目はほぼ同じ割合である。検数業者は，正確化，簡素化，管理水準向上のメリットが大半で，省力化，迅速化のメリットはほとんどない。業者間の業務の特性がはっきり表われている。

③ 対象業務

九つの輸入業務処理のうち，船卸計画処理，貨物搬入処理，発送処理，本船動静システムの４業務で全体のメリットの７７％とほぼ大勢を占めている。このうち船卸計画処理は２３％を占めて，輸入業務処理ので最もメリットの出るもので，業者の受ける効果は非常に大きくなる。

表３－３　共同利用センターにおける輸出入業務処理のメリット評価表

評価項目＼業者名		海貨		エゼント		検数		検量		倉庫		税関		港湾局		船社		計	
①省力化	点数	4		15		-3		2		3		1		4		-2		24	
	%	17	7	62	22	-13	-5	8	40	13	28	4	5	17	13	-8	-10	100	9
②迅速化	点数	12		20		6		1		2		7		8		5		61	
	%	20	22	33	31	10	11	2	20	3	18	11	32	13	26	8	25	100	23
③正確化	点数	12		14		20		0		1		9		8		5		69	
	%	17	22	20	21	30	36			1	9	13	40	12	27	7	25	100	26
④簡素化	点数	17		9		14		1		3		2		5		8		59	
	%	30	31	15	13	24	25	1	20	5	27	3	9	8	17	14	40	100	22
⑤管理水準向上	点数	10		9		18		1		2		3		5		4		52	
	%	19	18	17	13	34	33	2	20	4	18	6	14	10	17	8	20	100	20
計	点数	55		67		55		5		11		22		30		20		265	
	%	21	100	25	100	21	100	2	100	4	100	8	100	11	100	8	100	100	

図３－３６　共同利用センターにおける輸出入業務処理のメリット（メリット別）

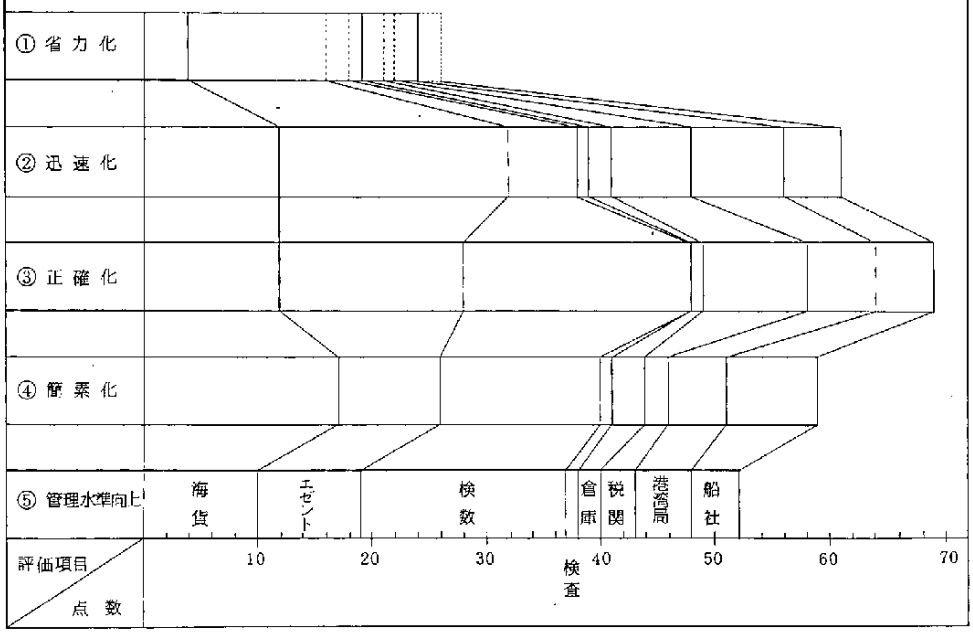


図３－３７　共同利用センターにおける輸出入業務処理のメリット（利用者別）

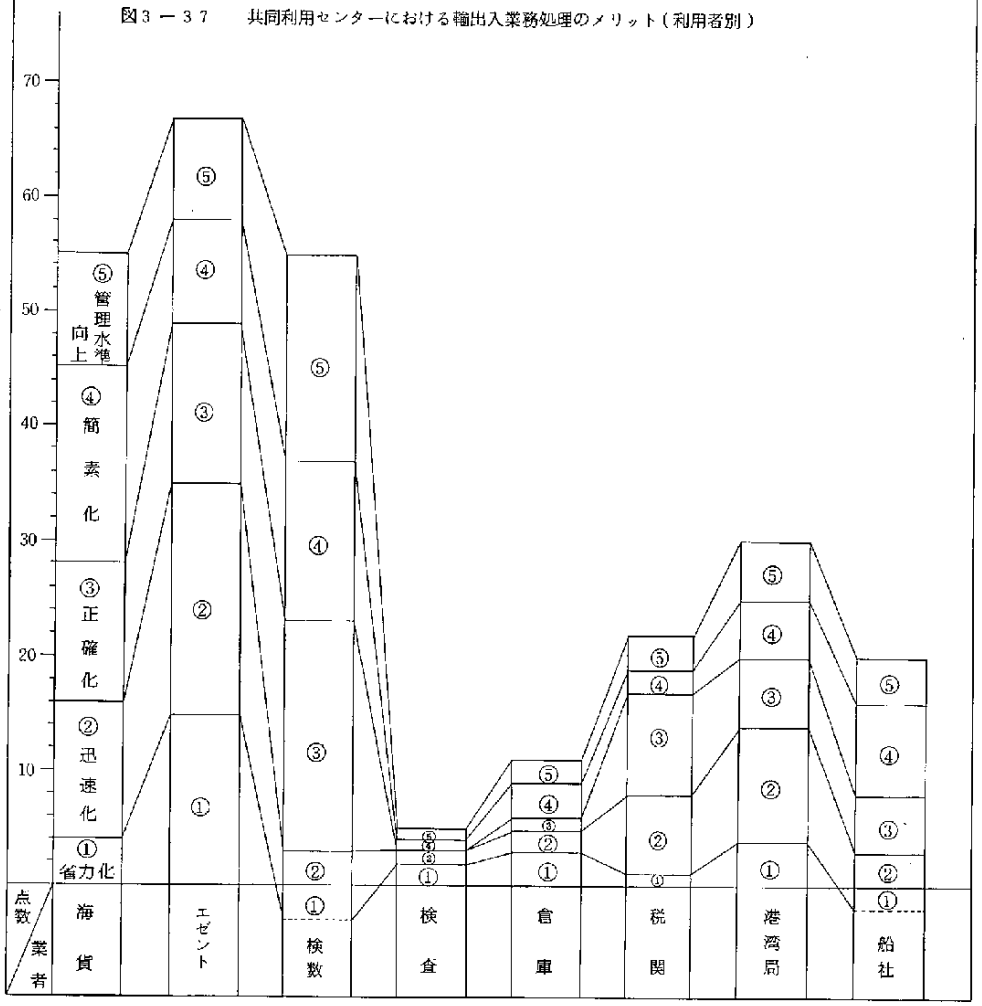
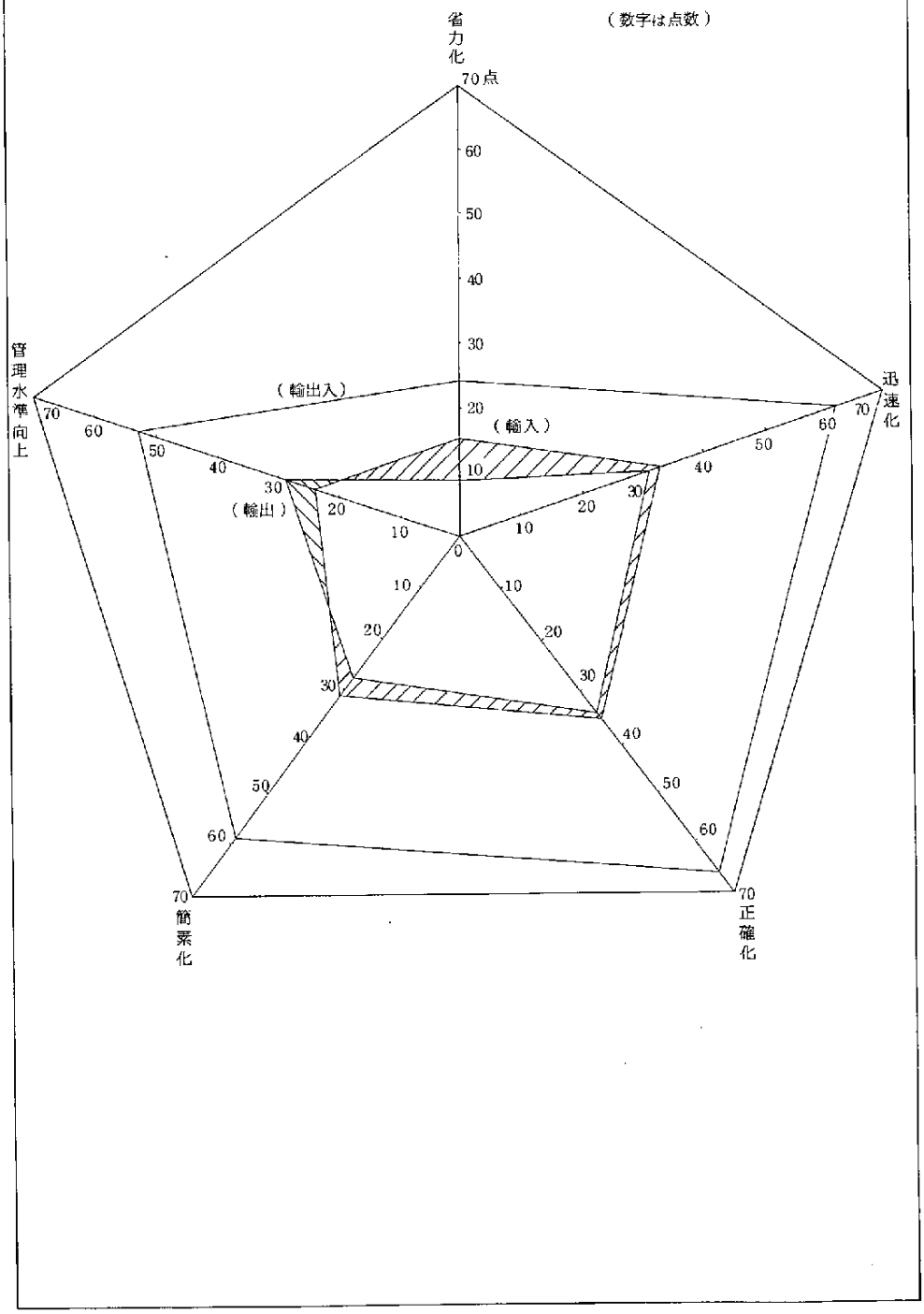


図３－３８　共同利用センターにおける輸出入業務処理のメリット



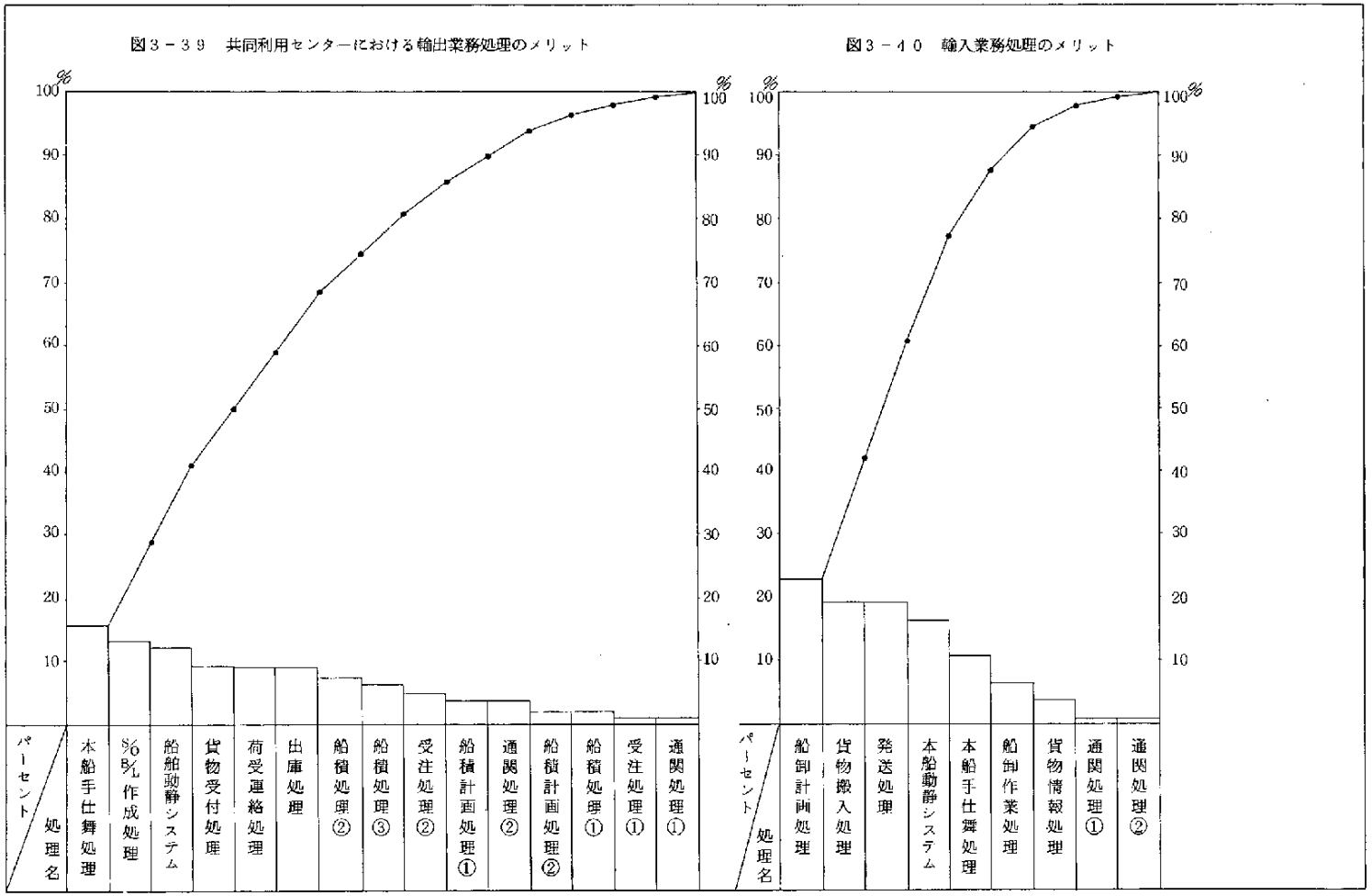


図３－３９　共同利用センターにおける輸出業務処理のメリット
%
100
90
80
70
60
50
40
30
20
10
パーセント
処理名
本船手仕舞処理
S/R作成処理
船舶動静システム
貨物受付処理
荷受連絡処理
出庫処理
船積処理②
船積処理③
受注処理②
船積計画処理①
通関処理②
船積計画処理②
船積処理①
受注処理①
通関処理①
図３－４０　輸入業務処理のメリット
%
100
90
80
70
60
50
40
30
20
10
パーセント
処理名
船卸計画処理
貨物搬入処理
発送処理
本船動静システム
本船手仕舞処理
船卸作業処理
貨物情報処理
通関処理①
通関処理②

表３－４　共同利用センターにおける輸出業務処理のメリット評価表

評価項目＼業者名		海貨	エゼント	検数	検量	倉庫	税関	港湾局	船社	計
①省力化	点数	3	7	−3	1	0	0	2	−1	9
	%	9 33	23 78	−12 −33	50 11	0 0	0 0	13 22	−7 −11	100 7
②迅速化	点数	5	11	4	0	0	3	4	3	30
	%	15 17	36 37	16 13	0 0	0 0	30 10	27 13	21 10	100 23
③正確化	点数	6	5	10	0	0	5	4	4	34
	%	18 17	16 15	40 29	0 0	0 0	50 15	29 12	29 12	100 27
④簡素化	点数	11	2	5	1	0	1	3	5	28
	%	34 38	6 7	20 18	50 4	0 0	10 4	20 11	36 18	100 21
⑤管理水準の向上	点数	8	6	9	0	0	1	2	3	29
	%	24 27	19 21	36 32	0 0	0 0	10 3	13 7	21 10	100 22
計	点数	33	31	25	2	0	10	15	14	130
	%	100 25	100 24	100 19	100 2	0 0	100 7	100 12	100 11	100

図３－４１　共同利用センターにおける輸出業務処理のメリット（メリット別）

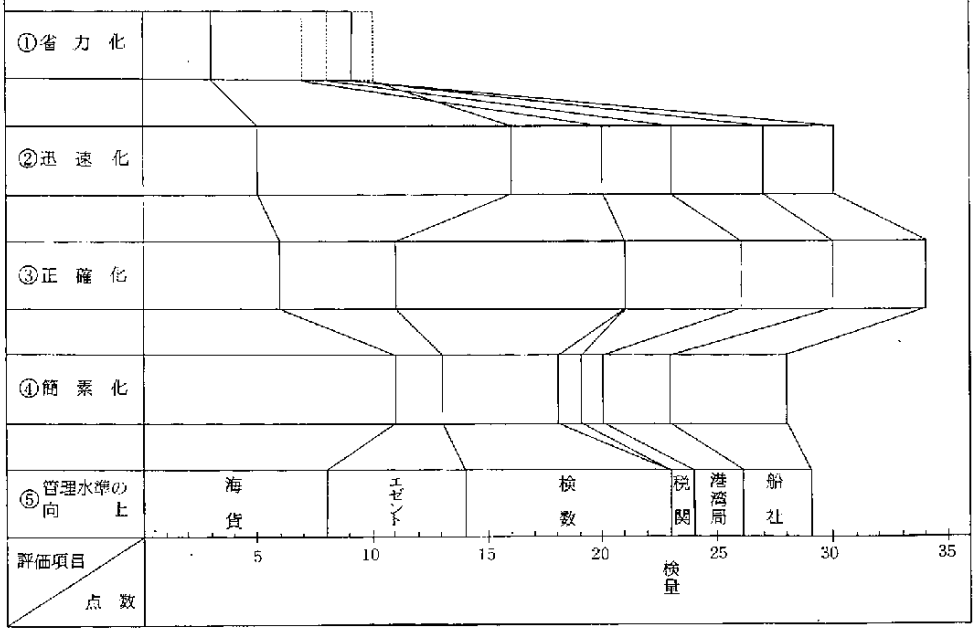


図３－４２　共同利用センターにおける輸出業務処理のメリット（業者別）

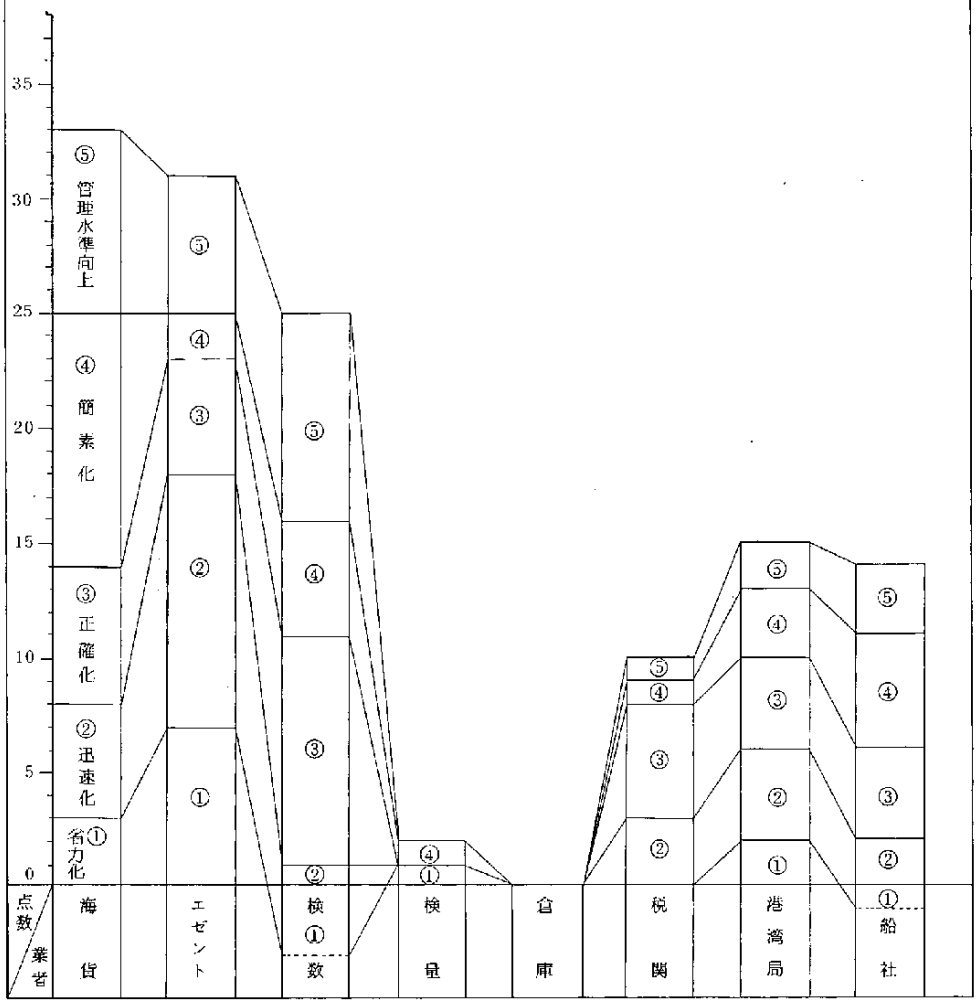
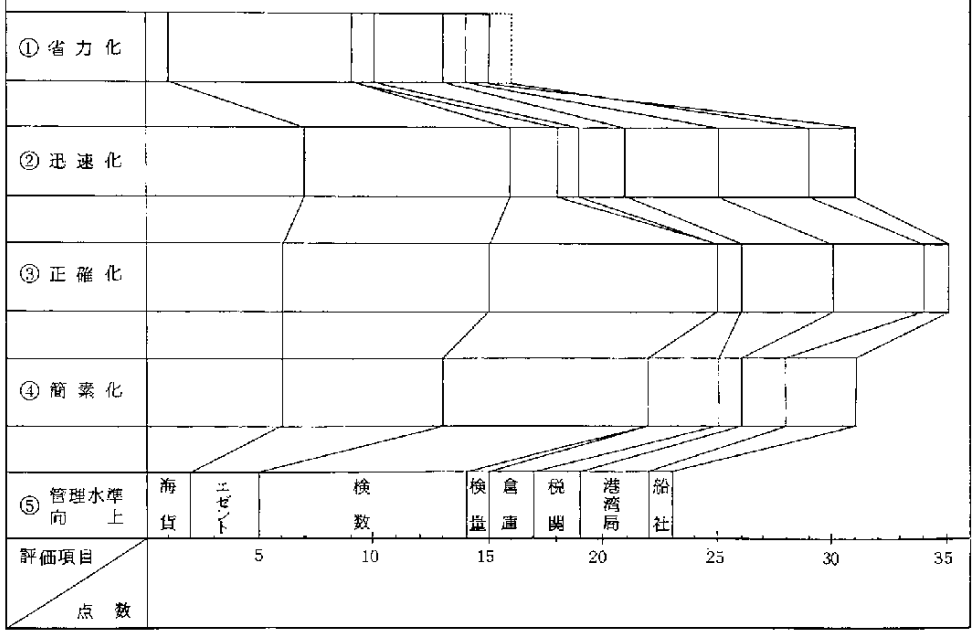


表３－５　共同利用センターにおける輸入業務処理のメリット評価表

評価項目＼業者名		海貨		エゼント		検数		検量		倉庫		税関		港湾局		船社		計	
①省力化	点数	1		8		0		1		3		1		2		−1		15	
	%	7	5	53	22	0	0	7	33	20	27.5	7	8	13	13	−7	17	100	11
②迅速化	点数	7		9		2		1		2		4		4		2		31	
	%	23	32	30	35	6	7	3	33	6	18	13	34	13	27	6	33	100	23
③正確化	点数	6		9		10		0		1		4		4		1		35	
	%	17	27	26	25	29	33	0		3	9	11	34	11	27	3	17	100	26
④簡素化	点数	6		7		9		0		3		1		2		3		31	
	%	19	27	23	20	29	33	0		10	27.5	3	8	6	13	10	50	100	23
⑤管理水準の向上	点数	2		3		9		1		2		2		3		1		23	
	%	9	9	13	8	39	30	4	34	9	18	9	16	13	20	4	17	100	17
計	点数	22		36		30		3		11		12		15		6		135	
	%	100	16	100	27	100	23	100	2	100	8	100	9	100	11	100	4	100%	

図３－４３　共同利用センターにおける輸入業務処理のメリット（メリット別）



3-86

図３－４４　共同利用センターにおける輸入業務処理のメリット（業者別）

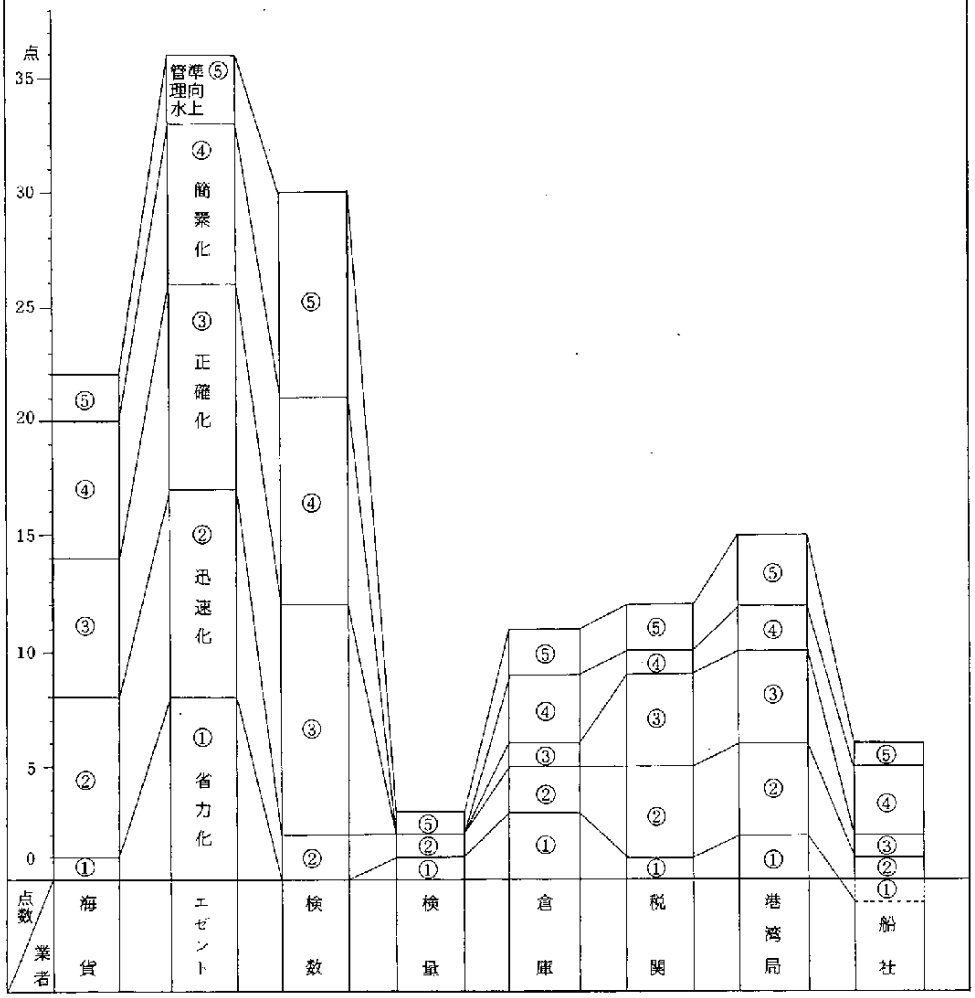


表３－６　総括表　共同利用センターによる処理評価表（輸出Ⅰ）

処理名	評価基準	海貨業	エセント	検数業	検量業	倉庫業	税関	港湾局	船社		合計	条件・備考
船舶動静システム	省力化	1	1					2	−2		2	
	迅速化	1						2			3	
	正確化		−1					2			1	
	簡素化	1		1				2	2		6	
	管理水準向上			1				2			3	
	小計	3	0	2				10	0		15	
貨物受付処理	省力化				1						1	
	迅速化	1					1	1			3	
	正確化	1					1	1			3	
	簡素化	1			1		1	1			4	
	管理水準向上	1									1	
	小計	4			2		3	3			12	
受注処理①	省力化		1						−1		0	
	迅速化		1								1	
	正確化										0	
	簡素化								1		1	
	管理水準向上										0	
	小計		2						0		2	
受注処理②	省力化	−1									−1	
	迅速化		1								1	
	正確化	1									1	
	簡素化	2									2	
	管理水準向上	1	2								3	
	小計	3	3								6	
処理作成処理	省力化	2							2		4	
	迅速化	1							2		3	
	正確化	1							2		3	
	簡素化	2							2		4	
	管理水準向上	1							2		3	
	小計	7							10		17	
船積計画処理①	省力化		2								2	
	迅速化		2								2	
	正確化		1								1	
	簡素化										0	
	管理水準向上										0	
	小計		5								5	
船積計画処理②	省力化		−1	1							0	
	迅速化			2							2	
	正確化			2							2	
	簡素化		−1								−1	
	管理水準向上										0	
	小計	0	−2	5							3	
通関処理①	省力化										0	
	迅速化										0	
	正確化	1									1	
	簡素化										0	
	管理水準向上										0	
	小計	1									1	
通関処理②	省力化										0	
	迅速化	−1	1				1				1	
	正確化		1				1				2	
	簡素化										0	
	管理水準向上		1				1				2	
	小計	−1	3				3				5	

表３－７　総括表　共同利用センターによる処理評価表（輸出Ⅱ）

処理名	評価基準	海貨業	エヂント	検数業	検量業	倉庫業	税関	港湾局	船社		合計	条件・備考
荷受連絡処理	省力化	1	2								3	
	迅速化	1	1								2	
	正確化	1									1	
	簡素化	1	2								3	
	管理水準向上	1	2								3	
	小計	5	7								12	
出庫処理	省力化	−1									−1	
	迅速化		1	2			1	1			5	
	正確化			2			1	1			4	
	簡素化	1									1	
	管理水準向上	1		2							3	
	小計	1	1	6			2	2			12	
船積処理①	省力化			−2							−2	
	迅速化	1	1	−2							0	
	正確化	1		2							3	
	簡素化	1		−2							−1	
	管理水準向上	1		2							3	
	小計	4	1	−2							3	
船積処理②	省力化	1	−1	−2							−2	
	迅速化			2			1		1		4	
	正確化		1				1		1		3	
	簡素化	1	−2	2							1	
	管理水準向上	1	1								2	
	小計	3	0	2			2		2		9	
船積処理③	省力化		1	−2							−1	
	迅速化	1	1	−2							0	
	正確化		1	2							3	
	簡素化	1		2							3	
	管理水準向上	1	3	2							3	
	小計	3		2							8	
本船手仕舞処理	省力化		2	2							4	
	迅速化		2	2							4	
	正確化		2	2			1		1		6	
	簡素化		2	2							4	
	管理水準向上			2					1		3	
	小計	6	8	10			1		2		21	
	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
合計	省力化	3	7	−3	1			2	−1		9	
	迅速化	5	11	4			3	4	3		30	
	正確化	6	5	10			5	4	4		34	
	簡素化	11	2	5	1		1	3	5		28	
	管理水準向上	8	6	9			1	2	3		29	
	小計	33	31	25	2		10	15	14		130	
	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											

表３－８　総括表　共同利用センターによる処理評価表（輸入Ｉ）

処理名	評価基準	海貨業	ニセント	検数業	検量業	倉庫業	税関	港湾局	船社		合計	条件・備考
貨物情報処理	省力化											
	迅速化			2							2	
	正確化			2							2	
	簡素化											
	管理水準向上			2							2	
	小計			6							6	
本船動静システム	省力化	1	1				1	2	2		3	
	迅速化	1					1	2			4	
	正確化	1	−1				1	2			3	
	簡素化	1		1			1	2	2		7	
	管理水準向上			1			1	2			4	
	小計	4	0	2		5	10	0			21	
船卸計画処理	省力化	−1	1	2		1			1		5	
	迅速化	1	2	2		1			1		7	
	正確化	1	2	2		1			1		7	
	簡素化	1	2	2		1			1		7	
	管理水準向上	1	1	2		1			1		6	
	小計	3	8	10		5			5		31	
船卸作業処理	省力化			−2							−2	
	迅速化	1	1	−2							0	
	正確化	1	2	2							5	
	簡素化	1		2							3	
	管理水準向上			2							2	
	小計	3	3	2							8	
本船手仕舞処理	省力化		2	2							4	
	迅速化		2	2							4	
	正確化		2	2							4	
	簡素化		1	2							3	
	管理水準向上											
	小計		7	8							15	
貨物搬入処理	省力化	1	2	−2	1	1					3	
	迅速化	2	2	−2	1		1	1	1		6	
	正確化	1	2	2			1	1			7	
	簡素化	1	2	2		1					6	
	管理水準向上	1		2	1						4	
	小計	6	8	2	3	2	2	2	1		26	
通関処理①	省力化	−1									−1	
	迅速化	1									1	
	正確化	1									1	
	簡素化	1									1	
	管理水準向上										0	
	小計	2									2	
通関処理②	省力化										0	
	迅速化	1									1	
	正確化										0	
	簡素化										0	
	管理水準向上										0	
	小計	1									1	
発送処理	省力化	1	2			1					4	
	迅速化		2			1	2	1			6	
	正確化	1	2				2	1			6	
	簡素化	1	2			1					4	
	管理水準向上		2			1	1	1			5	
	小計	3	10			4	5	3			25	

表３－９　総括表　共同利用センターによる処理評価表（輸入Ⅱ）

処理名	評価基準	海貨業	エゼント	検数業	検量業	倉庫業	税関	港湾局	船社		合計	条件・備考
計	省力化	1	8		1	3	1	2	−1		15	
	迅速化	7	9	2	1	2	4	4	2		31	
	正確化	6	9	10		1	4	4	1		35	
	簡素化	6	7	9		3	1	2	3		31	
	管理水準向上	2	3	9	1	2	2	3	1		23	
	小計	22	36	30	3	11	12	15	6		135	
	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											

表3　10　海貨の共同利用センターによる処理評価表（輸出Ⅰ）

処理名	評価基準	海貨業	エゼント	検数業	検量業	倉庫業	税関	港湾局	船社		合計	条件・備考
船舶動静システム	省力化	1										○即時処理が可能であること。
	迅速化	1										○受入側の社内システムの対応の工夫次第で，プラス面が期待できる。
	正確化	0										
	簡素化	1										
	管理水準向上	0										
	小計	3									3	
貨物受付処理	省力化	−1										○キーインのシステムにネックがある。（入庫時の入力対策による）
	迅速化	0										○迅速化の判断は即時処理可能であれば＋1。
	正確化	0										○正確性は入力データのチェック機構の良し悪しで＋1が期待できるかどうか。
	簡素化	1										○オペレーションを伴う以上に省力化の意味に於てはマイナス要素がある。
	管理水準向上	1										
	小計	1									1	
受注処理①	省力化	0										
	迅速化	0										
	正確化	0										
	簡素化	0										
	管理水準向上	0										
	小計	0									0	
受注処理②	省力化	−2										○キーインに多大の労力を必要とする。（入力内容の範囲による）
	迅速化	−1										○入力用端末が海貨の受付窓口のタイプライタの数量＋αが必要。（従来，荷主がS／Iを作成しているものをも吸収する意味に於て）
	正確化	0										○端末コストの大きくなる　　キーイン手段の改善，OCR等でどうか，ERR対処が難しいか
	簡素化	2										○出力サイドには効果あり。
	管理水準向上	1										
	小計	0									0	
S/R作成処理	省力化	2										○キーインの程度が問題。簡潔なら省力化に於てプラス。
	迅速化	−1										○迅速性については出力帳票の収集方法によって，マイナス面が考えられる。
	正確化	0										○社内システムの簡素化にはプラスとなる。（完全にのればよい）
	簡素化	1										○但し，処理可能な船社の範囲次第で総点マイナスとなる可能性もある。
	管理水準向上	0										
	小計	2									2	
船積計画処理①	省力化	0										
	迅速化	0										
	正確化	0										
	簡素化	0										
	管理水準向上	0									0	
	小計	0										
船積計画処理②	省力化	0										
	迅速化	0										
	正確化	0										
	簡素化	0										
	管理水準向上	0										
	小計	0									0	
通関処理①	省力化	0										○キーインのあり方がネック。
	迅速化	0										○マスター化部分が設定可となる点で多少の正確性にプラスか。
	正確化	1										○迅速性，簡素化等については，機械化効果のある件数が占める割合による。（100%やりうるか，どうか疑問　E／D作成前の分割が問題）
	簡素化	0										
	管理水準向上	0										
	小計	1									1	
通関処理②	省力化	0										○データ集収に限り，迅速性はプラスとならぬでもない。
	迅速化	1										○実務上はオリジナルの受渡しがベースであるので，大きな効果は期待薄。
	正確化	0										○システム上，オリジナル処理が簡素にできれば効果は期待可。
	簡素化	0										
	管理水準向上	0										
	小計	1									1	

表３－１１　海貨の共同利用センターによる処理評価表（輸出Ⅱ）

処理名	評価基準	海貨業	エゼント	検数業	検量業	倉庫業	税関	港湾局	船社		合計	条件・備考
荷受連絡処理	省力化	0										○全てタイミングの良し悪しと，出力内容の正確性による。（この出力によって，前日スタンバイが可能であること）
	迅速化	1										
	正確化	0										
	簡素化	1										
	管理水準向上	1										
	小計	3									3	
出庫処理	省力化	-1										○キーインが簡単であることと。（データ再入力は意味なし） ○オペレーションの面で省力化にはマイナスとなるか（通常S／Iオリジナルをまわしている） ○社内処理に簡素化期待可。
	迅速化	0										
	正確化	0										
	簡素化	1										
	管理水準向上	0										
	小計	0									0	
船積処理①	省力化	0										○従来方式より処理が早くなることと。
	迅速化	1										
	正確化	0										
	簡素化	1										
	管理水準向上	1										
	小計	3									3	
船積処理②	省力化	1										○データサイクルが実務上役立つ範囲であることと。 ○問合せ等，業務の繁雑性が改良。
	迅速化	0										
	正確化	0										
	簡素化	1										
	管理水準向上	1										
	小計	3									3	
船積処理③	省力化	0										
	迅速化	1										
	正確化	0										
	簡素化	1										
	管理水準向上	1										
	小計	3									3	
本船手仕舞処理	省力化	0										
	迅速化	0										
	正確化	0										
	簡素化	0										
	管理水準向上	0										
	小計	0									0	
	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											

表３－１２　エゼント共同利用センターによる処理評価表（輸出Ｉ）

処理名	評価基準	海貨業	エゼント	検数業	検量業	倉庫業	税関	港湾局	船社		合計	条件・備考
船舶動静システム	省力化		+1									○輸入と同じ
	迅速化		0									
	正確化		−1									
	簡素化		0									
	管理水準向上		0									
	小計		0									
貨物受付処理	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
受注処理①	省力化		+1									○Booking データを船社から受けるため
	迅速化		+1									
	正確化		0									
	簡素化		0									
	管理水準向上		0									
	小計		+2									
受注処理②	省力化		0									○Bookingされた貨物の所在，取扱海貨，貨物の情況等の把握が可能となる。
	迅速化		+1									
	正確化		0									
	簡素化		0									
	管理水準向上		+2									
	小計		+3									
S/S作成処理	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
船積計画処理①	省力化		+2									○Looding List を現在エゼントが作成している場合にのみ省力効果が出る。
	迅速化		+2									
	正確化		+1									
	簡素化		0									
	管理水準向上		0									
	小計		−5									
船積計画処理②	省力化		−1									○他港積み情報を入れても，ハッチプランに結びつくかどうかわからない。
	迅速化		0									
	正確化		0									
	簡素化		−1									
	管理水準向上		0									
	小計		-2									
通関処理①	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
通関処理②	省力化		0									○船積予定貨物の通関情況が把握可能となり，作業計画上便利である。
	迅速化		+1									
	正確化		+1									
	簡素化		0									
	管理水準向上		+1									
	小計		+3									

表３－１３　エゼント共同利用センターによる処理評価表（輸出Ⅱ）

処理名	評価基準	海貨業	エゼント	検数業	検量業	倉庫業	税関	港湾局	船社		合計	条件・備考
荷受連絡処理	省力化		+2									○Booking情報を基礎として，僅かの入力で海貨への連絡が速やかに行うことができる。（船の動静変化に対処できるが前日情報でよいか，ただし一斉連絡が可能となるのでよい）
	迅速化		+1									
	正確化		0									
	簡素化		+2									
	管理水準向上		+2									
	小計		+7									
出庫処理	省力化		0									荷受の参考となる。（情報が陳情化する場合も起こる）
	迅速化		+1									
	正確化		0									
	簡素化		0									
	管理水準向上		0									
	小計		+1									
船積処理①	省力化		0									
	迅速化		+1									
	正確化		0									
	簡素化		0									
	管理水準向上		0									
	小計		+1									
船積処理②	省力化		−1									○理論的には有効であるが，実作業とのタイミングが問題である。（予定と実績の比較ができればよいが，追いかけ仕事となる見込みなのでマイナスになりかねない。）
	迅速化		0									
	正確化		+1									
	簡素化		−1									
	管理水準向上		+1									
	小計		0									
船積処理③	省力化		+1									○枚数への委託業務が減少する。（本船上の情報のInputとサインの問題がある）
	迅速化		+1									
	正確化		+1									
	簡素化		0									
	管理水準向上		0									
	小計		+3									
本船手仕舞処理	省力化		+2									○枚数への委託業務が減少する。 Manifest の作成はフォーマットの統一が前提となる。
	迅速化		+2									
	正確化		+2									
	簡素化		+2									
	管理水準向上		0									
	小計		+8									
	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											

表３－１４　検数　共同利用センターによる処理評価表（輸出Ｉ）

処理名	評価基準	海貨業	エゼント	検数業	検量業	倉庫業	税関	港湾局	船社		合計	条件・備考
船舶動静システム	省力化			0								
	迅速化			0								
	正確化			0								
	簡素化			1								
	管理水準向上			1								
	小計			2								
貨物受付処理	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
受注処理①	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
受注処理②	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
SO処作成処理	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
船積計画処理①	省力化			0								○船社，エゼントよりLooding List をもらっているので変化はない。
	迅速化			0								
	正確化			0								
	簡素化			0								
	管理水準向上			0								
	小計			0								
船積計画処理②	省力化			1								○Display装置でも常時検索できるようなシステム事前に荷役計画が把握できる点有効。
	迅速化			2								
	正確化			2								
	簡素化			0								
	管理水準向上			0								
	小計			5								
通関処理①	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
通関処理②	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											

表３－１５　検数　共同利用センターによる処理評価表（輸出Ⅱ）

処理名	評価基準	海貨業	エゼント	検数業	検量業	倉庫業	税関	港湾局	船社		合計	条件・備考
荷受連絡処理	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
出庫処理	省力化			0								省力化は現在と変わらない。船積作業依頼書を直接受けられれば迅速化．正確化に役立つ）
	迅速化			2								
	正確化			2								
	簡素化			0								
	管理水準向上			2								
	小計			6								
船積処理①	省力化			−2								新たに入力作業が生じる 輸入船卸作業処理と同じ条件
	迅速化			−2								
	正確化			2								
	簡素化			−2								
	管理水準向上			2								
	小計			−2								
船積処理②	省力化			−2								新たに入力作業が生じる 輸入船卸作業処理と同じ条件
	迅速化			2								
	正確化			0								
	簡素化			2								
	管理水準向上			0								
	小計			2								
船積処理③	省力化			−2								新たに入力作業が生じる。 本船単位で本船の直近でデータを入力できるシステムであること。
	迅速化			−2								
	正確化			2								
	簡素化			2								
	管理水準向上			2								
	小計			2								
本船手仕舞処理	省力化			2								
	迅速化			2								
	正確化			2								
	簡素化			2								
	管理水準向上			2								
	小計			10								
	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											

表３－１６　税関　共同利用センターによる処理評価表（輸出Ｉ）

処理名	評価基準	海貨業	エゼント	検数業	検量業	倉庫業	税関	港湾局	船社		合計	条件・備考
船舶動静システム	省力化	0					0					とん税を納付しなければ出港不能なので税関としては変化はない。
	迅速化	0					0					
	正確化	0					0					船舶日報（東洋信号所発行）により把握しているので機械に問合せていない。
	簡素化	0					0					
	管理水準向上	0					0					
	小計											
貨物受付処理	省力化	1					0					搬入届を税関でチェックするならプラス１
	迅速化	1					1					
	正確化	1					1					
	簡素化	1					1					
	管理水準向上	1					0					
	小計											
受注処理①	省力化	0										ブッキングはシッパーが行うが海貨の場合もあり得る。
	迅速化	0										
	正確化	0										
	簡素化	0										
	管理水準向上	0										
	小計											
受注処理②	省力化	1										シッパーから海貨の必要とする情報がすべて入力されることは先ず考えられないのでプラス１。
	迅速化	1										
	正確化	1										税関はノータッチ
	簡素化	1										
	管理水準向上	1										
	小計											
／／作成処理	省力化	2										税関には関係なし。
	迅速化	2										
	正確化	2										入力が正確であればプラス2，ただし他港積と一括（コンバイン）してＢ／Ｌが作られる場合に問題が残る。
	簡素化	2										
	管理水準向上	2										
	小計											
船積計画処理①	省力化											海貨には関係ない。直積はＳ／Ｏ発行の折船社でつかめる。
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
船積計画処理②	省力化											税関とは無関係。
	迅速化											
	正確化											海貨とは係わりない。
	簡素化											
	管理水準向上											
	小計											
通関処理①	省力化	1										輸出申告提出前の段階で税関はタッチしない。ただし大蔵省の意向を打診することは不可欠である。
	迅速化	1										
	正確化	1										入力が正確ならプラス２であるが，完全な入力は期待できないのでプラス１とした。（品目分類が手がかかる）
	簡素化	1										
	管理水準向上	1										
	小計											
通関処理②	省力化	0					0					
	迅速化	0					1					
	正確化	0					1					
	簡素化	0					0					
	管理水準向上	0					1					
	小計											

表３－１７　税関　共同利用センターによる処理評価表（輸出Ⅱ）

処理名	評価基準	海貨業	エセント	検数業	検量業	倉庫業	税関	港湾局	船社		合計	条件・備考
荷受連絡処理	省力化	1										税関行政に関連しない。
	迅速化	1										海貨として荷受日時がポイントになる（解運航にも関係する）
	正確化	1										
	簡素化	1										
	管理水準向上	1										
	小計											
出庫処理	省力化	0					0					保税運送は，自主記帳に任されているが，搬出のチェックを行うとしたら，プラス１。
	迅速化	1					1					
	正確化	1					1					
	簡素化	0					0					
	管理水準向上	1					0					
	小計											
船積処理①	省力化	0					0					輸出許可後船積までの貨物につき税関は追及していない。（輸出許可後船積みの確認日の記入がなされない） 本船直積は荷受日時の正確さが肝要，これにより艀の稼動が向上する。（時間が問題となる艀の有効利用に役立つ）
	迅速化	1					0					
	正確化	1					0					
	簡素化	0					0					
	管理水準向上	1					0					
	小計											
船積処理②	省力化						0					輸出許可後船積まで税関はチェックしていない，船積に間に合わず他港まで追いかける場合は別に手続を要するこの場合不積をチェックするならプラス１。（税関がチェック）
	迅速化						1					
	正確化						1					
	簡素化						0					
	管理水準向上						0					
	小計											
船積処理③	省力化	0					0					この段階では税関は関係なし。
	迅速化	1					0					
	正確化	1					0					ゴーダウンも又荷受時間がポイント　プラス１ （トラックの有効利用に役立つ）
	簡素化	0					0					
	管理水準向上	0					0					
	小計											
本船手仕舞処理	省力化						0					税関ではローディングリストの提出を求めていないが将来の取扱法を考えるとその必要が生じるかも知れないのでプラス１
	迅速化						0					
	正確化						1					
	簡素化						0					
	管理水準向上						0					海貨は無関係。
	小計											
その他	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											

表３－１８　海貨　共同利用センターによる処理評価表（輸入）

処理名	評価基準	海貨業	エセント	検数業	検量業	倉庫業	税関	港湾局	船社		合計	条件・備考
受注処理	省力化	−1										○在庫情報の確認も同時に可能であること。 ○業務依頼情報の入力が簡潔であること。 ○入力～出力までの処理に対応性があること。（マル特処理可能，ないし他の方法で処理可能であること。）
	迅速化	1										
	正確化	0										
	簡素化	1										
	管理水準向上	1										
	小計	+2									2	
本船動静システム	省力化	1										○即時処理（必要な時に，随時情報を得られる。）が可能であること。 ○受入れる社内システムの考慮が必要
	迅速化	1										
	正確化	0										
	簡素化	1										
	管理水準向上	0										
	小計	+3									3	
船卸計画処理	省力化	0										
	迅速化	0										
	正確化	0										
	簡素化	0										
	管理水準向上	0										
	小計	0									0	
船卸作業処理	省力化	0										○リマーク等の確認，対応が可能であること。
	迅速化	1										
	正確化	0										
	簡素化	1										
	管理水準向上	0										
	小計	2									2	
本船手仕舞処理	省力化	0										
	迅速化	0										
	正確化	0										
	簡素化	0										
	管理水準向上	0										
	小計	0									0	
貨物搬入処理	省力化	0										○リマーク等の確認・対応が可能であること。
	迅速化	1										
	正確化	0										
	簡素化	1										
	管理水準向上	0										
	小計	2									2	
通関処理①	省力化	−1										○簡素化は具体化されるとき当然行なわれるであろうという事で＋１。 ○ＥＤＩＮ　直接Ｉ／Ｄ作成の関係の上で，効果が出るか省力化の点では疑問。
	迅速化	0										
	正確化	0										
	簡素化	0										
	管理水準向上	0										
	小計	0									0	
通関処理②	省力化	0										○情報とオリジナル帳票との性格の不一致の解消は困難。 ○許可データの集収についてのみ効果を期待することができるか？
	迅速化	1										
	正確化	0										
	簡素化	0										
	管理水準向上	0										
	小計	1									1	
発行処理	省力化	1										○入力が簡潔であること。
	迅速化	0										
	正確化	1										
	簡素化	1										
	管理水準向上	0										
	小計	3									3	

表3 －19　エゼント　共同利用センターによる処理評価表（輸入）

処理名	評価基準	海貨業	エゼント	検数業	検量業	倉庫業	税関	港湾局	船社		合計	条件・備考
受注処理	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
本船動静システム	省力化		+1									情報の源は船社であるため，船社に直接問合わせる方が情報の質，量共制限がなく優れている。ただし，海貨からの電話問合せに対する応答が軽減され，その点でのメリットは考えられるが，エゼントとして積極的なニーズはない。
	迅速化		0									
	正確化		-1									
	簡素化		0									
	管理水準向上		0									
	小計		0									
船卸計画処理	省力化		+2									
	迅速化		+2									
	正確化		+2									
	簡素化		+2									
	管理水準向上		+1									
	小計		+9									
船卸作業処理	省力化		0									船内荷役に関する書類は，本船，エテベ，検数等関係者のサインを要するため，本船の指定バース接岸が条件となる。又帳票の統一も必要である。
	迅速化		+1									
	正確化		+2									
	簡素化		0									
	管理水準向上		0									
	小計		+3									
本船手仕舞処理	省力化		-2									当処理は検数が代行しているが，機械化により，検数への委託が不要となり，料金面でのメリットが出る。
	迅速化		+2									
	正確化		+2									
	簡素化		+1									
	管理水準向上		0									
	小計		-7									
貨物搬入処理	省力化		+2									
	迅速化		-2									
	正確化		+2									
	簡素化		+2									
	管理水準向上		0									
	小計		+8									
通関処理①	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
通関処理②	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
発送処理	省力化											発送時点でのメリットだけでなく，以后の社内会計処理，月末在庫処理等へデータ処理の展開が可能である。
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											

表３－２０　検数　共同利用センターによる処理評価表（輸入）

処理名	評価基準	海貨業	エセント	検数業	検量業	倉庫業	税関	港湾局	船社		合計	条件・備考
受注処理	省力化			0								
	迅速化			2								
	正確化			2								
	簡素化			0								
	管理水準向上			2								
	小計			6								
本船動静システム	省力化			0								ディスプレイ装置だけでなく，ハードコピーでも情報がとれるシステムとする。
	迅速化			0								
	正確化			0								
	簡素化			1								
	管理水準向上			1								
	小計			2								
船卸計画処理	省力化			2								
	迅速化			2								
	正確化			2								
	簡素化			2								
	管理水準向上			2								
	小計			10								
船倒作業処理	省力化			-2								省力化・迅速化につながらないのはTALLY SHEETの入力作業が新たに発生するため。従って入力作業の簡素化を図れば効果は大きい。
	迅速化			-2								
	正確化			2								
	簡素化			2								
	管理水準向上			2								
	小計			2								
本船手仕舞処理	省力化			2								本船単位で本船の直近でデータを入力できるシステムであること。
	迅速化			2								
	正確化			2								
	簡素化			2								
	管理水準向上			0								
	小計			8								
貨物搬入処理	省力化			-2								省力化・迅速化につながらないのはTALLY SHEETの入力作業が新たに発生するため。従って入力作業の簡素化を図れば効果は大きい。
	迅速化			-2								
	正確化			2								
	簡素化			2								
	管理水準向上			2								
	小計			2								
通関処理①	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
通関処理②	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
発送処理	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											

表3－21　検定　共同利用センターによる処理評価表（輸入）

処理名	評価基準	海貨業	エセント	検数業	検量業	倉庫業	税関	港湾局	船社		合計	条件・備考
受注処理	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
本船動静システム	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
船卸計画処理	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
船卸作業処理	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
本船手仕舞処理	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
貨物搬入処理	省力化				1							輸出入を問わず検定システム社データの提供者にあることから検定内部のメリット・デメリットは重視する必要なしと思考する。
	迅速化				1							
	正確化				0							
	簡素化				0							
	管理水準向上				1							
	小計				3							
通関処理①	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
通関処理②	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											
発送処理	省力化											
	迅速化											
	正確化											
	簡素化											
	管理水準向上											
	小計											

表３－２２　税関　共同利用センターによる処理評価表（輸入）

処理名	評価基準	海貸業	ユセント	検数業	検量業	倉庫業	税関	港務局	船社		合計	条件・備考
受注処理	省力化	0										海貸はドキュメントを受けてから活動開始となる。海貸が求めている完全な情報はのぞむべくもないがその概要をつかんだ点でもプラス１。ただし省力化にはつながらない。
	迅速化	1										
	正確化	1										
	簡素化	0										
	管理水準向上	0										
	小計	2										
本船動静システム	省力化	1					1					
	迅速化	1					1					
	正確化	1					1					
	簡素化	1					1					
	管理水準向上	0					1					
	小計	4					4					
船卸計画処理	省力化						0					海貸には関係ない。
	迅速化						0					
	正確化						0					
	簡素化						0					
	管理水準向上						0					
	小計											
船卸作業処理	省力化	0										乗船職員は廃止されたので税関は無関係である。 海貸としては直取の状況を把握できるのでプラス１。
	迅速化	1										
	正確化	1										
	簡素化	0										
	管理水準向上	0										
	小計	2										
本船手仕舞処理	省力化						0					海貸のタッチすることではない。
	迅速化						0					
	正確化						0					
	簡素化						0					
	管理水準向上						0					
	小計						2					
貨物搬入処理	省力化	1					0					税関で搬入をチェックするとしたらプラス１。
	迅速化	2					1					
	正確化	2					1					
	簡素化	1					0					
	管理水準向上	1					0					
	小計	7					2					
通関処理①	省力化	0										航空貨物ならであるが海の貨物については受注処理のデータによるがプラス１程度
	迅速化	1										
	正確化	1										
	簡素化	0										
	管理水準向上	0										
	小計	2										
通関処理②	省力化	0					0					
	迅速化	0					0					
	正確化	0					0					
	簡素化	0					0					
	管理水準向上	0					0					
	小計	0										
発送処理	省力化						0					
	迅速化						2					
	正確化						2					
	簡素化						0					
	管理水準向上						1					
	小計						5					

4. ドキュメンテーション・システムの概要

4.1 ドキュメンテーション・システムの業務処理概要

ドキュメンテーションと貨物管理は，実務上相互依存関係にあり，分割できにくいものである。そこでここでは，ドキュメンテーションは国際的標準化と関連を持つので，概念的に区分して次の７業務を対象とした。

1) ドキュメンテーションの中心的業務　　３業務

① E－０３　受注処理②

② E－０４　S／O－B／L作成処理

③ E－０７　通関処理①

2) ドキュメンテーションに関連する業務　　４業務

①	E－０１	貨物受付処理	E－０３受注処理②にファイルを提供する。
②	E－０２	受注処理②	
③	E－０５	船積計画処理①	S／O受付データをドキュメントファイルに入力
④	E－０８	通関処理②	通関許可データをドキュメントファイルに入力する。

業務処理の内容と入出力については，前述のジョブ処理概要に記載した。そこでここではドキュメンテーション・システムのジョブ処理の流れをファイル中心に展開することにした。図３－４５ドキュメンテーションの処理フローチャートにおいて，中心的業務である「E－０３　受注処理②」，「E－０４S／O B／L作成処理」，「E－０７通関処理」の３業務の処理フローは枠でかこみ入出力を記入した。その他の関連業務は処理名とファイルのみを記した。ドキュメンテーションの関連業務は本来は貨物管理システムの範囲に含まれるが，ドキュメンテーションシステムに必要な情報の追加，更新および後処理を各ジョブ処理で行うものである。

E－０１　貨物受付処理

この処理ではシェッド・マスター・ファイルがつくられる。

E－０２　受注処理①

船積み予約システムで，ブッキング－ファイルがつくられる。

E－０３　受注処理②

この処理は，ドキュメントファイルの入力部であり，輸出ドキュメントデータが入力される。シェッドマスターファイルとブッキング・ファイルとつきあわされ，ドキュメントファイルとなり，その後の処理に展開される。シップメント単位の発行者ごとの出力が容易となる。

E－０４　S／O－B／L作成処理

S／Oスリップが E－０３で出力されたのを基に，S／O－B／L を作成する処理である。このシステムでは，フレート計算がポイントとなる。センターでは円貨換算レート，同盟フレート・レートのマスターとしてのメンテナンスもできる。船社は磁気テープでB／Lデータを受領でき，その後の社内処理に展開できる。

E－０５　船積計画処理①

E－０４の受入行為（船積確定）に基づく，船社からのS／O受付データをドキュメント・ファイルに入力し，あわせてブッキング・ファイルから船積確定分ごとにローディング，マスターファイルを作成するシステムである。ローディング・マスター・ファイルもブッキング・ファイル，B/Lデータと同様に船舶コード航海No.ごとであることは，いうまでもない。

E－０７　通関処理①

ドキュメンテーション・システムの２番目の柱のシステムである。既存のドキュメント・ファイルに申告データを海貨がインボイスNo.をキーに入力し，輸出申告書を出力する。税関はM／Tで統計データを受領できる。

E－０８　通関処理②

E－０７を完了させる処理であり，税関の通関進行状況，許可の状況を

海貨側が確認でき，許可データはドキュメント・ファイルに入力される。

4.2 ドキュメンテーション・システムの仕様

4.2.1 入力概要

ドキュメンテーション・システムの７業務処理のうち，５業務処理より入力データとして６種類がある。Ｅ－０１貨物受付処理とＥ－０５船積計画処理の入力データは貨物管理システムの範囲を含めた。

入力データ一覧表（表3－２３）で帳票名，処理サイクル，項目数，桁数，入手源の各項目をまとめて記した。各入力データの項目名，桁数は輸出ドキュメンテーション・データ動静表（表３－２５）にまとめてある。なおブッキング・データは輸出貨物管理データ動静表（表３－２９）のブッキング・ファイルの項目と共通とした。

入力データのインプット方法は，基本的には各業者に設置する端末機よりキーインすることとする。ただしブッキング・データは，船社より磁気テープ電送で入力することとした。

輸出ドキュメンテーション・データ動静表（データエレメントのファイル関連表を含む表３－２５）は縦にデータ名，横に帳票名とファイル名をとり各データがどの帳票から入力され，転記，更新されていくかを明らかにするために作成した。表中に記した記号は欄外に説明をつけたので参照のこと。このデータ動静表より各データをコンピュータ・システムのファイル項目として，データ・エレメントのファイル項目として採用し，データ・エレメントのファイル関連表に○印をつけ関連ずけた。

入力先を利用者別にみると，６件のうち４件は海貨業者が行い，船社と税関が各１件となり，海貨業者が入力作業の大半を占めている。

4.2.2 出力概要

ドキュメンテーション・システムの出力として，９種類の帳票が７利用者

に提出される。出力基本帳票一覧表（表３－２４）にその概要をまとめた。なお各利用者が任意に問合せる検索結果は，ここでは出力として取扱っていない。出力の形態としては，帳票類の出力を基本とするが，独自のコンピュータシステムを有する利用者にはオンラインでデータを提供する。船社にはマニフェスト・データを，税関には通関統計データを磁気テープで出力することとした。通関処理②における許可済Ｅ／Ｄデータはディスプレイ表示で処理することにし，ハードコピー出力は不要と判断した。

4.2.3 ファイル概要

ドキュメンテーション・システムで用いるファイルは次の４種類である。

ファイル名	項目数	桁　数
① シェッド・マスター・ファイル	44(22)	1,185 (744)
② ブッキング・ファイル	12(12)	382 (382)
③ ドキュメント・ファイル	77(68)	1,963 (1,674)
④ ローディング・ファイル	31(24)	644 (568)

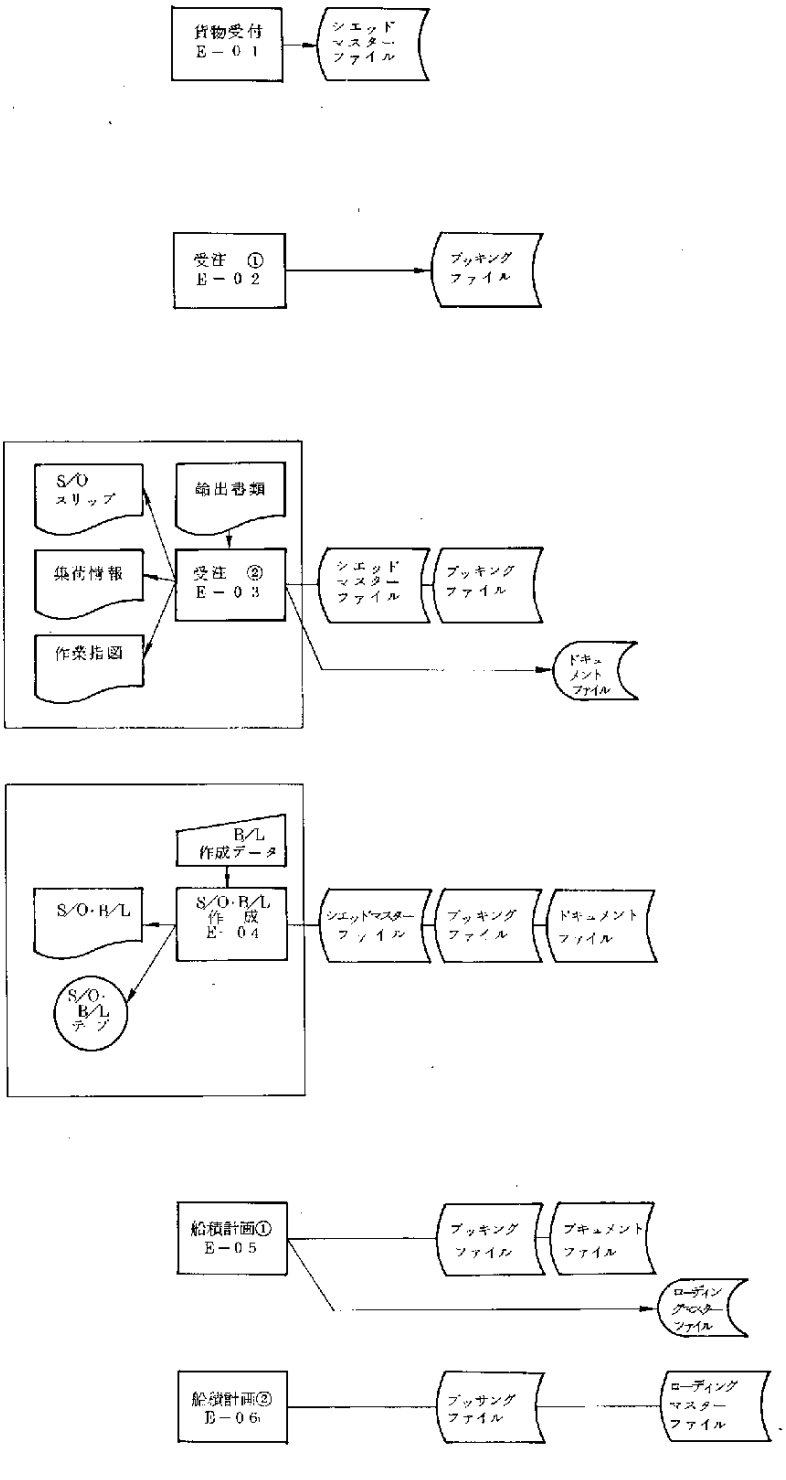
上記のカッコ内の数字は，ドキュメンテーション・システムで用いる個有の項目数と桁数である。

なお，この４ファイルは輸出貨物管理システムと共通のファイルとして使用するもので，ドキュメンテーション個有のファイルではない。ドキュメンテーション・システムで利用する各ファイルの項目名，桁数は，データ・エレメントのファイル関連表に○印を記し，下段に項目数と総桁数を集計した。

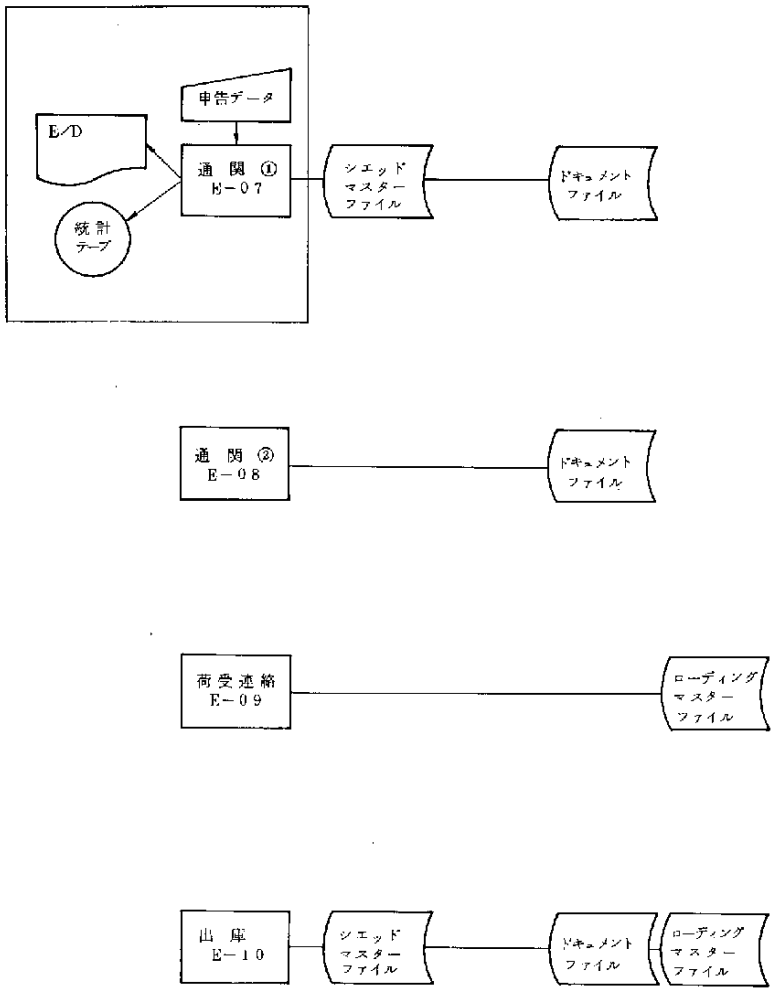
① シェッド・マスター・ファイル

シェッドマスターファイルは，貨物送り状を原始データとする貨物管理システムの基本ファイルである。ドキュメンテーション・システムにおいては，ドキュメント・ファイルの内容に貨物の動静情報を追加することに

図３－４５　ドキュメンテーション・システムのゼネラルフロー



前頁の続き


申告データ
E/D
通 関 ①
E－07
統計
テープ
シエッド
マスター
ファイル
ドキュメント
ファイル
通 関 ②
E－08
ドキュメント
ファイル
荷受連絡
E－09
ローディング
マスター
ファイル
出 庫
E－10
シエッド
マスター
ファイル
ドキュメント
ファイル
ローディング
マスター
ファイル

よりドキュメンテーションの出力をサポートする。

② ブッキング・ファイル

貨物の船積予約を行うために必要なデータを集めたファイルである。ドキュメンテーション作成（B／L中心）の準備作業に必要な情報を提供することを主目的とする。

エゼントに対してはブッキング・リスト，集荷情報の提供を行ったり，ドキュメント・ファイルとローディング・マスター・ファイルとの照合，データの消し込みを行う。

③ ドキュメント・ファイル

ドキュメンテーション・システムのマスター・ファイルである。輸出者の輸出書類（S／I・P／L）を基本入力データとして，E－03受注処理②でこのファイルを作成する。この際輸出書類（S／I・P／L）とシェッドマスター・ファイルおよびブッキング・ファイルと照合を行い，インボイスNo.をキーとするドキュメント・ファイルを作成する。

このファイルをマスターとして，海貨業者はEX-RATE，本船出港予定日等のB／L作成データをキーインし，S／O，B／Lの作成を行う。さらに海貨・税関に対して輸出申告書（E／D）を作成する。

④ ローディング・マスター・ファイル

貨物が書類通りに船積みされているかをチェックすることを主目的とする。

4.3.4 キーコード一覧表

ドキュメンテーション・システムのファイル，入力，検索，出力の際のキーとなるコードをまとめたものである。基本となるキーコードは，ブッキングNo.，入庫No.，インボイスNo.，E／DNo.，の4種類である。この4種類のキーコードを組合せて，各業務処理を行う。その使用目的はキーコード一覧表（表3－26）を参照のこと。

表３－２３　入力データ一覧表　　輸出ドキュメンテーションシステム

帳票名	入／出	処理サイクル	項目数	桁数	入手源										使用目的・備考
					荷主	船社	海貨	エゼント	検数	検定	税関	港湾局	倉庫		
1 （磁気テープ）ブッキングデータ	入力	デイリーバッチ	5	240		○									E-02 受注処理①
2 輸出書類（S/I）	〃	オンラインリアルタイム	49	1010			○								E-03 受注処理②
3 輸出書類（P/L）	〃	〃	18	955			○								E-03 〃
4 B/L 作成データ	〃	〃	9	185			○								E-04 S/O，B/L 作成処理
5 申告データ	〃	〃	20	221			○								E-07 通関処理①
6 通関許可データ	〃	〃	2	15							○				E-08 通関処理②
計						1	4				1				6件3利用者

表３－２４　出力基本帳票一覧表　　輸出ドキュメンテーションシステム

帳票名	入/出	処理サイクル	項目数	桁数	提出先										使用目的・備考
					荷主	船社	海貨	エゼント	検数	検定	税関	港湾局	倉庫	作業会社	
1 ブッキング リスト	出力	デイリーバッチ	5	240				○							E-02 受注処理①
2 S/O スリップ	〃	オンラインリアルタイム	23	982			○			○					E-03 受注処理②
3 作業指示書	〃	〃	23	784			○		○					○	E-03 〃
4 集荷情報	〃	〃	5	240				○							E-03 〃
5 S/O,B/L セット	〃	〃	23 32	982 1189		○←	○								E-04 S/O,B/L 作成処理
6 (磁気テープ)マニュフェストデータ	〃	デイリーバッチ	17	610		○									E-04 〃
7 E/D	〃	オンラインリアルタイム	32	790			○				○				E-07 通関処理①
8 (磁気テープ)通関統計データ	〃	デイリーバッチ	32	790							○				E-07 〃
9 (ディスプレイ)許可済E/Dデータ	〃	オンラインリアルタイム	32	790			○								E-08 通関処理②
計						2	5	2	1	1	2			1	9件14利用者

表3－25　輸出ドキュメンテーションデータ動静表

データ名	依頼書	INV	P/L	⑧ E/D	S/I	© E/D	S/O	B/L	データエレメントのファイル関連表 シェッドマスターファイル	パッキングファイル	ドキュメントファイル	ローディングマスターファイル	コード化可能	桁数
INSTRUCTION No.	⊖	⊖	⊖	⊖	⊕	⊖					○			30～10
海貨通関業者名	○				◎		◎	◎	○	○	○	○		30～10
〃　コード					◎		◎	◎	○	○	○	○		5
諸掛負担先	○				⊕									30
CONTAINER SERVICE	△				▲					○	○		○	7
ETA／ETD 入出港予定日	○				⊕	出港予定年月日 ⊕			○		○			16
許可年月日					▲	⊕			○		○			8
入庫 No					⊕				○		○			12
搬入場所					⊖	⊖			○		○	○	○	30
船積完了年月日					▲						○	○		8
搬出年月日					▲				○			○		8
エゼント名					⊕					○	○	○	○	30～10
船名					▲							○	○	25～30
検数業者名					▲						○	○	○	30～10
トラック業者名					▲				○			○	○	30～10
リマーク	△				▲				○		○	○		50
BOOKING No.	△				▲									10
SHIPPERS コード					⊕	⊖	⊖		○	○	○	○		5
船社	○				⊖			◎		○	○	○	○	30～10
CONTRACT No.	△	△	△		▲						○			10
L／C No.	△	△	△	○	▲						○			15～10
LATEST SHIPPING DATE	△				▲						○			8
EXPIRY DATE	△				▲									8
INVOICE No.	△	○	○		⊖						○			10
CONSIGNEE	△	○	○		⊖		⊖	⊖			○			120
NOTIFY PARTY	△	○	○	○	⊖		⊖	⊖			○			120
船名	○	○	○		⊕	⊖	⊖	⊕	○	○	○	○	○	25～30
積込港	○	○	○		⊕	⊖	⊖	⊖	○	○	○	○	○	30
仕向地	○	○	○		⊕	⊖	⊖	⊖	○	○	○	○	○	30
FINAL DESTINATION	△	△	△		▲		▲	▲			○			30
MARKS& NUMBERS	○	○	○		⊕	⊖	⊖	⊖	○		○			210
NUMBER OF PKGE	○	○	○		⊕		○	⊖	○	○	○	○		5
L／C 品名	○	△	△	○	⊖		⊖	⊖			○			30～60
INV 品名		○	○		▲	⊖	▲				○			30～60
品名（オプション）	△	△	△	△	▲	▲	▲	▲	○	○	○			60
P／L 重目　計（小計含）			○			⊕								10
〃　単位			○			⊖								10
統計品目番号				○		⊕					○			7
仕向国				○		⊖					○		○	15
申告税関名						⊕					○		○	15

前頁の続き

データ名	領収書	INV	P/L	⑧ E/D	S/I	ⓒ E/D	S/O	B/L	データエレメントのファイル関連状 シニッド マスター ファイル	ブッキング ファイル	ドキュメント ファイル	ローディング マスター ファイル	コード 化可能	桁数
申告年月日					△	⊕			○		○			8
本船・ふ中扱区分						⊕			○		○		○	1
保税運送区分						⊕					○		○	1
〃 期間						⊕					○			17
申告書枚数・欄数					▲	⊕					○			2
船(機)籍符号						⊕					○			3
積込港符号						⊕					○			3
仕向国符号						⊕					○			3
貿易形態別符号						⊕					○			3
申告番号					△	⊕					○			12
取扱区分(他法令)						⊕					○			13
単位						⊕					○			4
申告価格(F.O.B)						⊕					○			10
通関士記名押印						⊕					○			20～30
輸出者住所氏名	○	○	○	○		⊖	⊖	⊖	○	○	○	○		120
WEIGHT & MEASUREMNT					○		⊖	⊖	○		○	○		36
HATCH No							✓					○		1
RECEIVED IN ALL							✓					○		1
〃 DATED							✓					○		8
S/O No					△		○		○		○	○		10
B/L No					▲			○	○		○	○		10
上屋・蔵区分							✓				○	○		1
品目コード							✓				○			7
FREIGHT & CHARGES								⊕			○			10
REVENUE TONS					⊕			ⓘ			○			7
FREIGHT RATE					⊕			⊕			○			5
PSR								⊕			○			5～10
PREPAID OR COLLECT 計								⊖			○			10
EX-RATE					⊕			⊖			○			5
FREIGHT支払地 (PREPAIDAT (PAYABLE)	○				⊖			⊖			○			30
FREIGHT 円価								⊖			○			10
B/L ORIGINAL枚数	○				⊖			⊖			○			1
COMBINE B/L作成地								▲			○			30
〃 海貨業者名								▲			○			30
〃 品目								▲			○			40
B/L 発行地	○				⊖			⊕			○			30
B/L DATE					▲			○			○			8
VOY No	△				▲		▲	▲			○			10
他法令添付チェック						⊕					○			3
計 79項目	28	16	18	8	49	32	23	32	22	12	68	24		
桁数計	1135	935	955	422	1010	790	982	1189	744	382	1674	568		

◎固定データ　⊕発生優先データ　△受取不確定データ　▲不確定優先データ　○受取データ　⊖転記データ　▲△不確定転記データ
✓検数・ニセント・船社記入データ

表３－２６　キーコード一覧表　輸出ドキュメンテーションシステム

コード名	桁数		使　用　目　的	備　　考
1. ブッキングNo.	10		船社よりブッキングテープを入力し，ブッキングNo.をキーにブッキングファイルを作成する。ブッキングリストの出力	E－０２　受注処理①
入庫No. 2. ブッキングNo. インボイスNo.	12 10 10		海貨は（S/I）（P/L）輸出書類よりインボイスNo.をキーとしてドキュメントファイルを作成する。	E－０３　受注処理②
3. ブッキングNo. インボイスNo.	10 10		船社（海貨）はB/L 作成データ（EX-RATE，本船出港予定など）を入力し，ドキュメントファイルの更新を行い，S/O B／L（セット）を出力，マニフェストテープを船社に出力する。	E－０４ S/O，B/L 作成処理
4. インボイスNo. 入庫No.	10 12		海貨はインボイスNo.，入庫No.をキーとして申告データを入力し，ドキュメントファイル，貨物ファイルを更新しE／Dを出力する。税関に統計テープを出力する。	E－０７　通税処理①
5. E／D No.	12		税関はE／D No.をキーに通関許可データを入力しドキュメントファイルを更新する。	E－０８　通税処理②

5. 輸出入貨物管理システムの概要

5.1 輸出貨物管理システムの業務処理概要

輸出貨物管理システムは，次の10業務処理から構成されている。さらに分類すると，中心的業務処理として5業務処理，関連業務処理として5業務処理から成っている。輸出貨物管理システムの範囲は，輸出者から海貨業者が受けとる貨物送り状の受付処理をスタートとして，貨物の船積のために行う出庫処理をもって終了するものとする。これ以降は，本船荷役作業のための船積処理から本船手仕舞処理となり輸出業務の全処理は終了する。われわれは，輸出貨物システムの範囲として，本船荷役作業情報としてのローディング・マスター・ファイルの提供をもって一応の区切りとしが，実務上の処理を円滑に行うために本船手仕舞処理までを共同利用センターの業務処理に含めた。

1) 輸出貨物処理の中心的業務　5業務

① E-01　貨物受付処理

② E-03　受注処理②

③ E-07　通関処理①

④ E-09　荷受連絡処理

⑤ E-10　出庫処理

2) 輸出貨物処理に関連する業務　5業務

① E-02　受注処理①

② E-04　S/O，B/L 作成処理

③ E-05　船積計画処理①

④ E-06　船積計画処理②

⑤ E-08　通関処理②

E-01　貨物受付処理

港頭地区に送られてくる貨物に添付されている「貨物送り状」の現状が，非常に多様な名称と様式，データ内容である。貿易情報システムの設計に当

たっては，このフォーム，データ内容統一と輸出者側での早期の採用を再びここにおいて強調しておく次第である。

現在，入庫検定制度下におかれている輸出貨物は，全施検貨物の約６０％位とみられている。しかし源となる施検貨物量は，輸出貨物の約４５％ほどと見積られ特定品目例えば自動車，鉄鋼などは施検率が極端に低く，また航路によっても施検率の低い，例えば中国航路のようなところがある。しかし，入庫検定は，貨物受付以降の貨物管理に不可欠であるので，大黒埠頭を通過する輸出貨物は，保管場所が大黒埠頭内であると否とにかかわらず，所定のデータ内容を具備していなければならない。他所に保管される貨物は，大黒埠頭着岸本船名が決定次第，本船名・航海Noをキーとして取扱われる。他税関において通関済みとなった場合も，全く同じである。

この貨物受付処理の段階では，入庫Noがキーである。現在，海事検定機関で使用されている入庫番号の構造は，入庫検定の契約主体の違いにより相違がある。一般的には，

① 貨物到着順位（１年，月の各期ごとに分かれることもある）

② 扱い者（協同組合上　で使用）

③ 蔵置場所（庫名－納入されたセクション）

横浜港としては，もちろん未だ統一されたものが，保管場所コードとしても設定されていないので，入庫番号の統一はこれからである。海貨業者によっては，別に整理番号として，荷主別に付けるところもあるが，現行の最大桁数は12桁である。

大黒埠頭で使用する場合，上記要素は必要条件となる。

この処理は，入力するデータ・ネットからいえば，横浜港（公共）輸出貨物の３０％はカバーしなければならなくなるので，横浜港の輸出貨物の施検対象となるもののほとんどをカバーしうるようになるであろう。そのことに

って，輸出されるべき貨物の動静がまず現在どれ位の在庫状況にあるかを知ることができて，船社としては，横浜港積みの把握が容易となってくる。一方，輸出者においては，輸出されるべき貨物の港頭地区到着の状況，荷揃いの状況が常握しやすくなる。

ファイルはシェッド・マスター・ファイルと称しているが，正しく横浜港に保管された貨物の実態を反映するため，港湾局，税関は，搬入届については，このファイルに依存することで，上屋利用の統計，保管料等の請求，通関されるべき貨物の所定保管場所における存否などを算出，確認することができる。また搬入届では，不確実な容積重量も確定データとして収録できる。

E－０２　受注処理①

この処理は，輸出者が船社に対し，船腹スペースを確保するために行う船積みの予約行為であるので，センターは船社から常にブロキング情報を受けとる処理となり，データの更新が常に行われる。また後のE－０４，E－０５処理と連結してくる。ただし，これは輸出貨物管理システムには属せしめない。

E－０３　受注処理②

輸出書類は海貨が受領し，これを入力する。海貨は荷主別のS／INo.を設定し，社内帖票へ展開している。インボイスNo.及びUCRN（Unique Consignment Reference Number）の国際的統一が行われれば，S／INo.，及び入庫No.に代えることができる。基本となる取引関係フォーマットはJASTPROが手がけているので除外される。

入庫No.を付された貨物とインボイス，パッキング・リストの記載内容の統一の段階であるので，入庫No.の異なる貨物同士の組合せ，入庫No.の同一の貨物群の分割が行われる。この組合せ・分割は，現在はP／Lデータをキーに保管台帖をめくり，入庫No.と貨物品名，数量，マークを点検し，海貨より検定機関へ入庫No.を明示してP／Lをハードコピーで渡している。この作業は，

貨物の実態と取引データとの照合である。

ドキュメントの範囲については，JASTPRO の同一フォーマットで展開されるもののほか，輸出申告書Ⓑ及びⒸなどがある。

シェッド・マスター・ファイルに入力される入庫データのうち，現在のビジネス・システムでは検定機関の検量証明行為が必要なので，海貨がS／O及びB／Lで使用されるウェイト・メジャーについては，一旦S／Oスリップのリストの形で出力してもらわなければならない。作業指示書の内容は，予定であって確定情報とはいえない。

E－04　S／O，B／L作成処理

ドキュメンテーションシステムの一つめ柱であって，貨物管理システムとの関連では，シェッド・マスター・ファイル上に船舶コード，航海No.が確定データとして入力される段階である。

E－05　船積計画処理①

ドキュメンテーション・システムに属すがここでは船社からのS／O受付データが確定データとなる。この結果，新たにローディング・マスター・ファイルが作成され，同時にリストとして一定のバッチ処理において出力される。現在，S／O受付，ローディング・リストの授受は，ハードコピーによる手渡しである。

E－06　船積計画処理②

貨物管理システムそのものではないが，貨物の船倉内積付けのための情報として予測－計画システムに当たる。現在手順は他港積み情報を電話で船社から収集したエゼントが，ブッキング情報と組合せ，プレストウェージ・プランを作成し，船社と打ち合わせている。計画システムであるため，他港の船積み結果を迅速に受理し，入力する必要がある。

E－０７　通関処理①，E－０８　通関処理②

ドキュメンテーション・システムを通して，輸出申告書を作成し，通関状況の照会を可能にすることと税関への統計データの提供（許可前データであるので，税関でデータの選択ができる）及びE／DNo.をキーとして，正規の保管施設に保管されている貨物であるかどうかのチェック（申告前では海貨が，申告後は税関）を行い，税関が検査を必要と認めれば，検査場搬入命令を出せる。ドキュメント・ファイルに結果は入力される。

E－０９　荷受連絡処理

エゼントがローディング・リストに基づき，当該貨物の本船積み作業予定の情報をE－０６の処理の延長として計画・予測し，海貨に伝達するシステムである。

作業能率の向上に極めて大きい効果がある。システムの性格上，データの更新が頻繁であることと，貨物の移動（横持ち）が遠隔地であればあるほど，その効果は交通条件（時間的制約）に左右されやすい。

E－１０　出庫処理

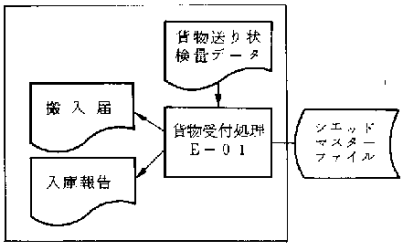
現在，この処理はほとんどがハードコピーの手渡しで伝達している。貨物が移動を開始する段階のため，貨物の実態の掌握が必要である。保管中，貨物の梱包・包装表示（特にマーク）の変更が行われている場合には，シェッド・マスター・ファイル上もデータの更新が行われていなければならない。貨物の実態掌握のため船，トラックなどによる運送のため，検数，運送業者へ作業依頼書がリストで出力される。

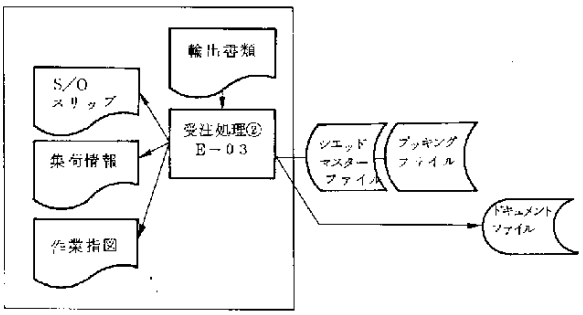
E－０３の段階とは異なり，確定データである。エゼントには，貨物そのものに添付されるS／Oと同内容のデータが出力され荷受予定の作業に役立てられる。現場ではS／O及びE／Dが貨物に添付される。税関－港湾局への搬出届は，貨物搬出指示書と同時に出力可能である。

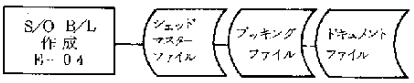
この段階でシェッド・マスター・ファイルの機能はローディング・マスター・ファイルに転換され，ローディング・マスター・ファイルのみにより，以後の貨物管理は行われる。

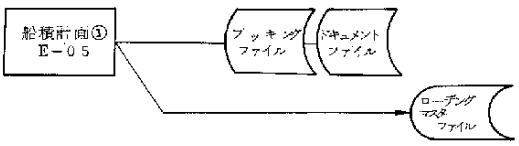
これ以降は，貨物の流れは，船による海上経由か，トラックによる岸壁経由かに分かれ，本船荷役作業へと続く。フェイズは海貨業務よりエゼント業務が中心となる。

図３－４６　輸出貨物管理システム

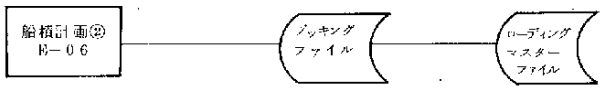


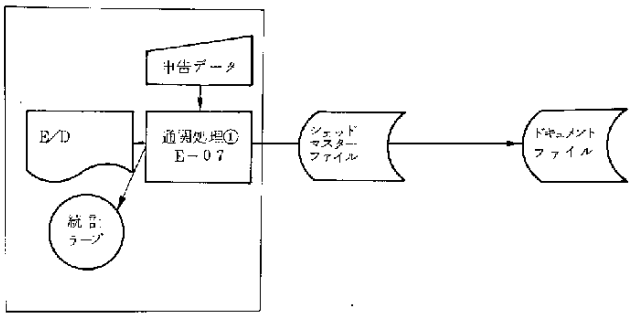




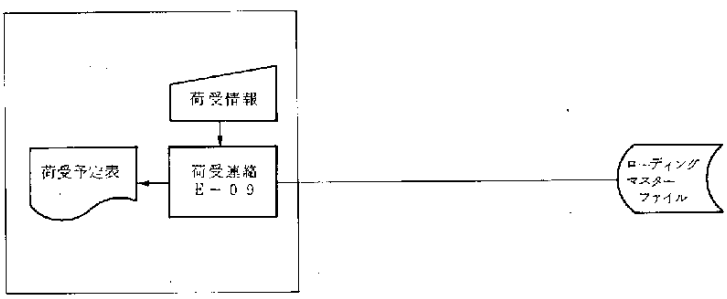


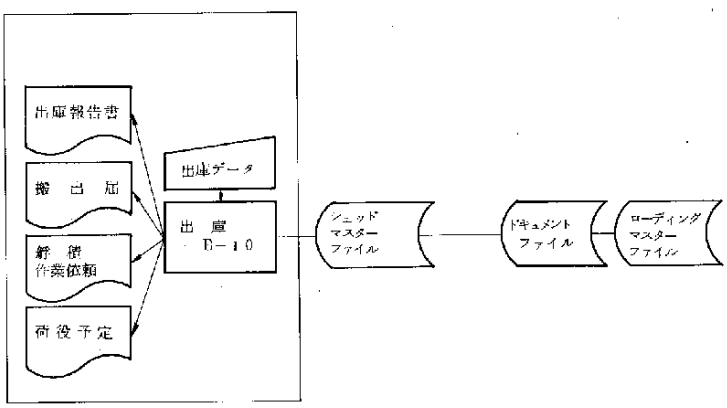
前頁の続き


船積計画㉒
E－06
ブッキング
ファイル
ローディング
マスター
ファイル


申告データ
E/D
通関処理①
E－07
統合
ラーゾ
シェッド
マスター
ファイル
ドキュメント
ファイル


通関処理②
E－08
ドキュメント
ファイル


荷受情報
荷受予定表
荷受連絡
E－09
ローディング
マスター
ファイル


出庫報告書
搬　出　届
解　錠
作業依頼
荷役予定
出庫データ
出　庫
E－10
シェッド
マスター
ファイル
ドキュメント
ファイル
ローディング
マスター
ファイル

5.2　輸出貨物管理システムの仕様

5.2.1　入力概要

輸出貨物管理システムの入力情報は10件，７業務処理で行われている。〔入力データー覧表（表３－２７）参照のこと〕

入力源の利用者をみると，海貨業者５件，エゼント業者３件，検定業者１件，船社１件から成っており，ドキュメンテーション・システムの入力源と同様海貨業者が一番多い。

入力データは各業者が設置する端末機からキーインにより入力される。各入力情報のデータ項目名と桁数は輸出貨物管理データ動静表（表３－２９）に記載されている。このデータ動静表のデータ記号（◎・△・⊖etc）の動きを見ることにより，各帳票ごとにデータがどう転記，更新されていくかの変化が追跡できる。すなわち電算処理システムでは各ファイルのデータの追加，更新の状態がこの表から明らかになる。

5.2.2　出力概要

７業務処理より１４種類の出力が１０利用者の端末機に出力される。出力はすべてオンラインリアルタイム処理で行なわれ，帳票として出力される。なお各利用者はこれらの情報をディスプレイによって検索することもできる。また独自のコンピュータシステムを有する利用者には，これら出力情報をオンラインで伝送されることが可能であり，自己システムとのインタフェースをとることができる。出力基本帳票一覧表（表３－２８），輸出貨物管理データ動静表（表３－２９）を参照のこと。

5.2.3　ファイル概要

ドキュメンテーション・システムと共通の下記４種類のファイルを用いる。

輸出貨物管理システムで利用する各ファイルの項目名と桁数は表３－２９の中にあるデータエレメント・ファイル関連表に○印で記してある。

① シェッド・マスター・ファイル

このファイルは貨物管理システムの基本となるものであり，貨物送状を原始データとして作成される。このファイルを中心として，港湾全体の貨物情報が集約され，船積計画処理のマスター・ファイルであるローディング・マスター・ファイルに貨物情報は引きつがれる。

② ブッキング・ファイル

貨物の船積予約を行うために必要なデータからなるファイルであり，ドキュメンテーション・システムに情報を提供する役割が大きい。貨物管理システムの範囲としては，エゼント業者に集荷情報の提供を行い，ローディング・マスター・ファイルとのデータの照合，消し込みを行う。

③ ドキュメント・ファイル

貨物管理システムにおけるドキュメント・ファイルは，貨物の動静状況情報をシェッド・マスター・ファイルおよびローディング・マスター・ファイルから受け，ドキュメンテーションを作成する。また逆に通関処理におけるごとく，ドキュメント・ファイルのデータ項目の確定情報（通関許可データなど）を貨物管理システムに提供して貨物の移動開始のチェック・ポイントとなる。

④ ローディング・マスター・ファイル

貨物の船積確定情報のマスター・ファイルとして，E－０５船積計画処理にて，ブッキング・ファイル，ドキュメント・ファイルから作成される。貨物の船積処理に関する情報は，ローディング・マスター・ファイルに集約され，船積計画処理が行われ，通関許可がされると船積準備の管理がこのファイルを中心に行われる。次のステップにて，船積作業管理情報とし

ての本船積検数ファイルをローディング・マスター・ファイルから作成する。

5.2.4 キーコード一覧表

輸出貨物管理システムにおけるキーとなるコードは次の6項目であり，各処理においてはこの6項目の組合せをキーコードとして用いている。

1) 入庫No. 10桁

2) ブッキングNo. 12桁

3) インボイスNo. 10桁

4) B／L No. 10桁

5) 船舶コード・Voy No. 10桁

各キーコードの使用目的，組合せ，各処理名はキーコード一覧表（表3-30）に記載した。

表３－２７　入力データ一覧表　輸出貨物管理システム

帳票名	入/出	処理サイクル	項目数	桁数	入手源										使用目的・備更
					荷主	船社	海貨	エゼント	検数	検定	税関	港湾局	倉庫		
1 貨物送り状	入力	オンライン リアルタイム	18	743			○								E-01 貨物受付処理
2 施検票（デメンション）	〃	〃	13	554						○					E-01 〃
3 輸出書類（S/I）	〃	〃	49	1010			○								E-03 受注処理②
4 輸出書類（P/L）	〃	〃	18	955			○								E-03 〃
5 S/O受付データ	〃	〃	3	28		○									E-05 船積計画処理①
6 他港積情報データ	〃	〃	17	610				○							E-06 船積計画処理②
7 本船作業情報データ	〃	〃	14	542				○							E-06 〃
8 申告書データ	〃	〃	20	221			○								E-07 通関処理①
9 荷受情報データ	〃	〃	4	23				○							E-09 荷受連絡処理
10 出庫データ	〃	〃	4	49			○								E-10 出庫処理
計						1	5	3		1					10件　4利用者

表３－２８　出力基本帳票一覧表　　輸出貨物管理システム

帳票名	入/出	処理サイクル	項目数	桁数	提出先										使用目的・備考
					荷主	船社	海貨	エゼント	検数	検定	税関	港湾局	倉庫	作業会社	
1 入庫原票	出力	オンライン リアルタイム	13	554			○								E-01 貨物受付処理
2 入庫報告書	〃	〃	16	644	○		○								E-01 〃
3 搬入届	〃	〃	17	566							○	○			E-01 〃
4 S/O スリップ	〃	〃	23	982			○			○					E-03 受注処理②
5 作業指示書	〃	〃	23	784			○		○					○	E-03 〃
6 集荷情報	〃	〃	5	240				○							E-03 〃
7 ローディングリスト	〃	〃	19	462				○	○						E-05 船積計画処理①
8 荷役計画書	〃	〃	8	255		○		○	○						E-06 船積計画処理②
9 E/D	〃	〃	32	790							○				E-07 通関処理①
10 荷受予定表	〃	〃	19	458			○								E-09 荷受連絡処理
11 出庫表・出庫報告書	〃	〃	17	566	○		○								E-10 出庫処理
12 搬出届	〃	〃	17	566							○	○			E-10 〃
13 解積作業依頼書	〃	〃	14	542					○					○	E-10 〃
14 荷役予定データ	〃	〃	19	458				○							E-10 〃
計					2	1	6	4	4	1	3	2		2	24件 10利用者

表３－２９　輸出貨物管理データ動静表

データ名	入庫予告	送状	自主記帳台帳又は◎搬入者	貨物受領書	施検票	港務局搬入届	入庫検才量報告書	入庫報告書	船積作業指示書	自主記帳台帳又は◎搬出者	港務局搬出者	船積報告書	データエレメントのファイル関連表 シェードマスターファイル	ブッキングファイル	ドキュメントファイル	ローディングマスターファイル	コード化可能	桁数
発送予定年月日	△												○					8
諸掛請求先	△	△		⚠				⊕	⊕			⚠	○		○			30
荷主名	△	△	⊕	⊖	⊖	⊖	⚠	⊕	⊕	⊖	⊖	⊖	◎	◎	◎	◎	○	120
出荷主名	△	○		⊖									○				○	30
輸送業者名	△	○		⊖									◎				○	30
品名	△	○	⊖	⊖	⊖	⊖	⊖	⊖	⊕	⊖	⊖	⊖	◎		◎			30～60
個数（ロット数）	△	○	⊖	⊖	⊖	⊖	⊖	⊖	⊕	⊖	⊖	⊖	○					5
発送年月日		○		⊖									○					8
海貨通関業者名	△	○	◎	⊖	◎	◎	⊖	◎	◎	◎	◎	◎	○	◎	◎	◎	○	30～10
船名		△	⚠	⚠	⚠	⚠	⚠	⚠	⊕	⊖	⊖	⊖	○	◎	◎	◎	○	25～30
積出地（港）		△	⚠	⚠					⊕			⊖		◎	◎	◎		30
仕向地		△	⚠	⚠	⚠	⚠	⚠	⚠	⊕	⊖	⊖	⊖	○	◎	◎	◎		30
シッピング　マーク		△	⚠	⚠	⚠	⚠	⚠	⚠	⊕	⊖	⊖	⊖	○		○			200
ケース　No.		△	⚠	⚠	⚠	⚠	⚠	⚠	⊕	⊖	⊖	⊖	○		○			10
搬入場所名		⊕	⊕	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖		◎		◎	◎	○	30
リマーク欄		⚠		⚠				⚠	⚠			⚠	◎		◎	◎		50
荷受者印又はサイン		⊕		⊕									○					30
入庫（受取）年月日		⊕		⊖	⊖	⊖	⊖	⊖			⊖	⊖	○					8
入庫番号		⊕	⊕	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	◎		◎			12
届出年月日			⊕			⊕				⊕	⊕		○					8
搬出予定年月日			⊕			⊕							○					8
搬入出に関する許可又は承認の種類・番号・年月日			⚠							⚠			○					20
容積			⊕							⊕			○					8
重量			⊕							⊕			○					
搬入年月日			⊕							⊖			○					
ディメンション					⊕		⊖	⚠					○		○	○		
@WEIGHT 又は TOTAL WEIGHT					⊕		⊖	⚠					○		○	○		
MEASUREMENT & WEIGHT							⊕	⚠	⊖			⊖	◎		◎	◎		
入港年月日						⊕					⊕		○					
蔵置場所の種類						⊕					⊖		○					
重量屯						⊕					⊕		○					
©E/D(I/D) No.									⊕	⊕		⚠			○	○		
船積形式									⊕			⊕			○	○		
バース									⊕			⚠				○		
ステベ									⊕							○	○	
艀名									⚠								○	
S/I No.									⊕			⊖	○		○			
S/O No.									⊕				◎		◎	◎		
検数業者名									⚠						◎	◎	○	
出庫予定日時									⊕				○			○		
搬出年月日										⊕	⊕		◎			◎		
船積卸完了日												⊕				◎		
運送方法			⊕			⊖				⊖	⊖				○			
計　43項目	8	18	18	18	13	17	14	16	23	18	17	19	34	5	21	19		
桁数計	313	743	617	743	554	566	564	644	784	599	566	630	861	240	575	462		

記号説明：　◎固定データ　△受取不確定データ　⊖転記データ　⚠発生データ　○受取データ　⊕発生・優先データ　⚠ 不確定転記データ

（注）データエレメントのファイル関連表の◎印はドキュメンテーションデータと共通項目

表３－３０　キーコード一覧表　輸出貨物管理システム

コード名	桁数		使　用　目　的	備　　考
1.入庫No.	12		入庫No.をキーにして検量業者は施検票によって入庫検量を行い，検量データを入力する。	E-01 貨物受付処理
2.入庫No.	12		海貨業者はパッキングリストによって，入庫No.をキーとして入庫データ索引	E-03 受注処理②
3.ブッキング No.	10		海貨業者はブッキングNo.をキーとして本船データを入力	E-03　〃
4.インボイス No.	10		海貨業者はインボイスNo.をキーとしてS／Iよりドキュメントファイル作成	E-03　〃
5. ブッキング No. インボイス No. B/L 船舶コード・Voy No.	10 10 10 10		①船社はS／O，B／L受付けB／L No.を入力する この５つのキーによりローディングマスターファイルを作り，ローディングリストを出力する ②エゼントは他港積情報，本船作業情報をこの５つのキーにより入力し，ブッキングファイルとローディングマスターファイルの更新を行い，荷役計画を作成する。	E-05 船積計画処理① E-06 船積計画処理②
6. インボイスNo. 入庫No.	22		海貨はインボイスNo.，入庫No.をキーとして申告データを入力，ドキュメントファイル，貨物ファイルの更新を行いE／Dを出力	E-07 通関処理①
7. 船舶コード・Voy No. インボイスNo.	20		エゼントは船舶コード，Voy No.，インボイスNo.をキーとして荷受データをローディングマスターに入力し，荷受予定表を出力	E-09 荷受連絡処理
8. インボイス No. 入庫 No.	32		海貨はインボイスNo.，入庫No.，B／L No.をキーとして出庫データを入力し，貨物ファイル，ドキュメントファイル，ローディングマスタファイルを更新し，出庫表，搬出届，船積作業依頼書，荷役予定データを出力する。	E-10 出庫処理

5.3　輸入貨物管理システムの業務処理概要

輸入貨物管理システムは，四つの中心的業務処理と三つの関連業務処理をその範囲として，輸出の場合と同じように，本船動静システムと本船手仕舞処理は除外した。しかし共同利用センターの処理として行うこととしている。すなわち本船荷役作業にかかわる処理をわれわれは対象外としたが，その結果の情報を輸入貨物管理システムに提供する必要があるためである。

1）輸入貨物管理の中心的業務処理

①　I－02　船卸計画処理

②　I－03　船卸作業処理

③　I－05　貨物搬入処理

④　I－08　発送処理

2）輸入貨物管理に関連する業務処理

①　I－01　貨物情報処理

②　I－07　通関処理①

③　I－08　通関処理②

5.3.1　輸入貨物管理システム

I－01　貨物情報処理

貨物情報としては，積み港のマニフェストないしB／L情報である。現在，船社よりハードコピーで入手しているものを磁気テープで入力することにより，荷役手配，搬入先確認などに広く活用できる。

I－02　船卸計画処理

この処理では，直取りデータ及び総揚げデータを入力し，本船荷役作業以降の作業管理情報が速やかに伝達される。ドキュメント・ファイルに追加入力される。

I－03　船卸作業処理

貨物の船卸し情報を記録する処理である。タリーシート・データを入力することにより，検数データ・ファイルを作成する。これは輸入貨物管理シス

テムの一つの柱である。

Ｉ－０５　貨物搬入処理

貨物が保管場所に搬入される際の貨物の実態を確認し，記録する処理である。データは艀より貨物が陸揚げされた時点と，陸揚げ後，入庫した時点の２段階で発生する。ただし，確認行為は主に検数の業務とされているので，貨物が陸揚げ後，直接搬入される場合は，同一データを使用できる。出力帳票名が異なっているものでも，データとしては，同一内容のものが多いので，かなり帳票整理はできる。

税関，港湾局への搬入届についても同様である。この処理で重要なのは，沿岸タリーシートまたは検量リポートのデータ入力により，入庫ファイルが新たに作成されることであり，貨物管理システムの二つ目の柱となる。

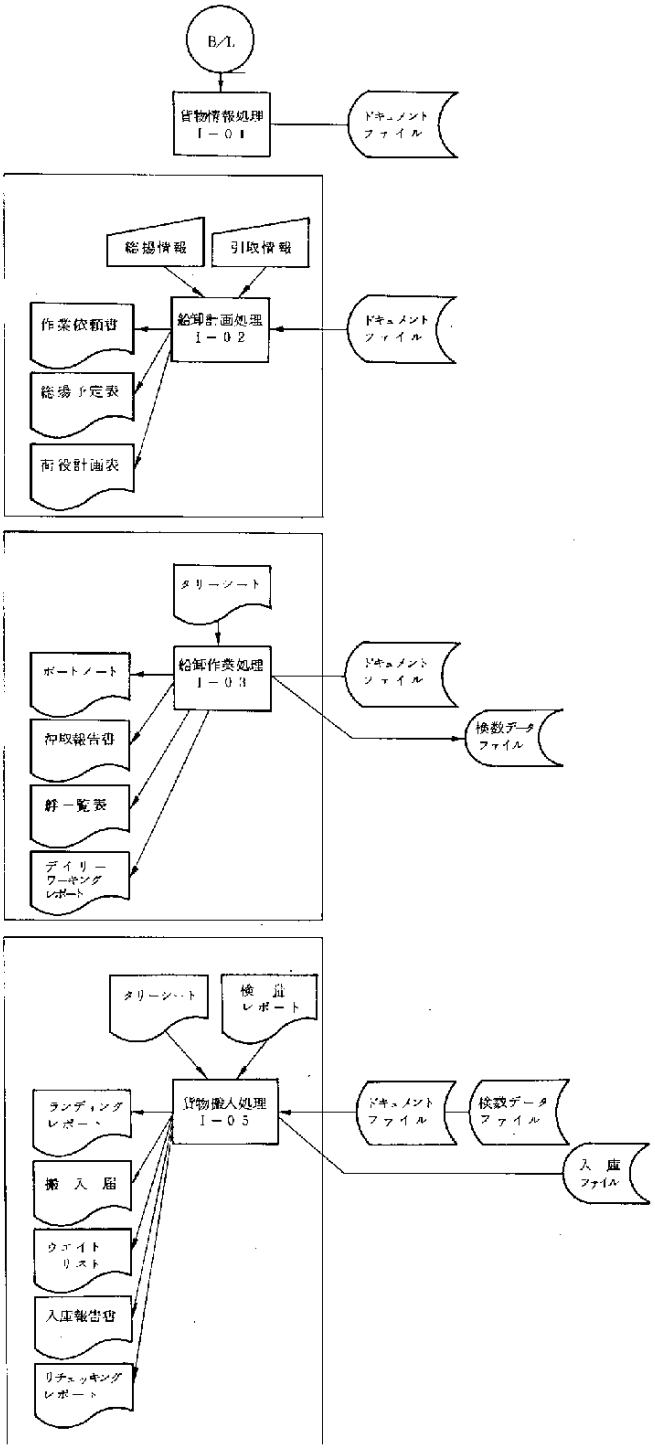
Ｉ－０６　通関処理①　　Ｉ－０７　通関処理②

申告データを入力し，輸入申告書を出力する。税関は磁気テープで統計データを受領できる。税関の通関進行状況，許可状況を照会でき，通関貨物の保管場所の確認もできる。許可データは入庫ファイルに入力される。

Ｉ－０８　発送処理

貨物の流れによっては，Ｉ－０５処理の後，Ｉ－０８処理を経て，再びＩ－０５の処理にのせられるものがある。入庫ファイルが二つできるようではあるが，保管場所ごとの記録であるので貨物データの側からみると，入庫Noが変わり，その他のデータは移し変えられたものにすぎない。総揚げ倉庫の入庫ファイルと海貨手倉庫の入庫ファイルとでは，海貨のファイルの方がデータ内容は豊かである。総揚げ倉庫が参照するドキュメント・ファイルは，Ｉ－０１で固定したデータであるが，海貨が参照するドキュメントは，取引データとか国内へ向けての輸送データなどが加わるためである。輸入貨物管理は，船卸し貨物が分割，通関，発送されることが多いため，輸出のようなマスター・ファイルは，入庫ファイルである。

図３・４７　輸入貨物管理システム（通関を含む）



前頁の続き

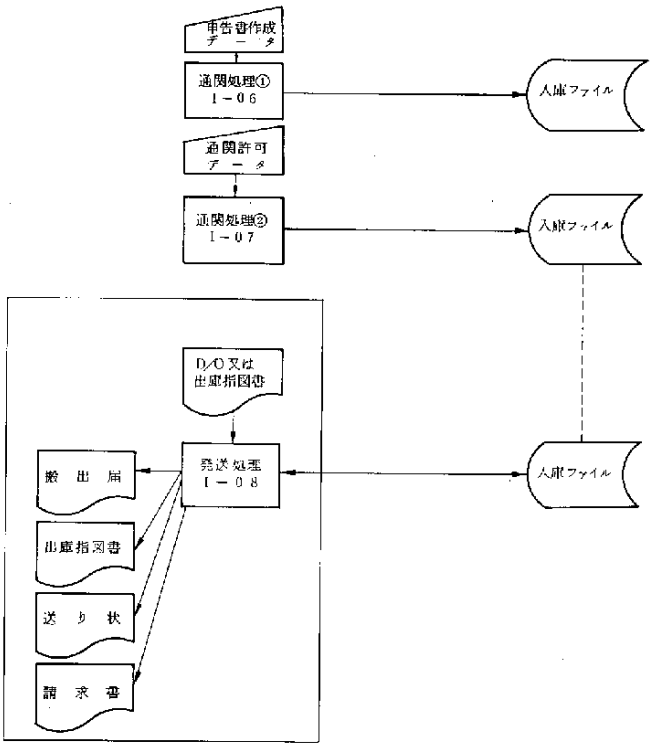

申告書作成
データ
通関処理①
I－06
入庫ファイル
通関許可
データ
通関処理②
I－07
入庫ファイル
D/O又は
出庫指図書
発送処理
I－08
入庫ファイル
搬出届
出庫指図書
送り状
請求書

表３－３１　入力データ一覧表　　輸入貨物管理システム

帳票名	入/出	処理サイクル	項目数	桁数	入手源										使用目的・備考
					荷主	船社	海貨	エゼント	検数	検定	税関	港湾局	倉庫		
1　B/L		デイリーバッチ	32	1189		○									I－01　貨物情報処理 キーイン又は磁気テープ
2　総揚貨物データ	〃	リアルタイム	8	115				○							I－02　船卸計画処理
3　直取データ	〃	〃					○								I－02　船卸計画処理
4　船卸データ(ターリーシート)	〃	〃							○						I－03　船卸作業処理
5　本船作業終了データ	〃	〃						○							I－04　本船手仕舞処理
6　揚荷データ	〃	〃							○						I－05　貨物搬入処理
7　検量データ	〃	〃								○					I－05　〃
8　申告書作成データ	〃	〃					○								I－06　通関処理
9　通関許可データ	〃	〃									○				I－07　〃
10　出庫指図書	〃	〃					○								I－08　発送処理
計						1	3	2	2	1	1				12件 6利用者

表３－３２　出力基本帳票一覧表　　輸入貨物管理システム

帳票名	入/出	処理サイクル	項目数	桁数	提出先										使用目的・備考
					荷主	船社	海貨	エゼント	検数	検定	税関	港湾局	倉庫		
1 M/F	O	デイリーバッチ	17	610		○		○	○		○				I-01 貨物情報処理
2 D/O	〃	リアルタイム	9	475		○									I-02 船卸計画処理
3 総揚貨物予定表	〃	〃	8	115			○		○				○		〃 〃
4 荷役計画表	〃	〃	8	255		○	○	○	○						〃 〃
5 作業依頼書	〃	〃	14	542			○	○	○				○		〃 〃
6 デイリーワーキングレポート	〃	〃	14	240				○	○						I-03 船卸作業処理
7 ボート ノート	〃	〃	15	504			○	○	○		○				〃 〃
8 沖取報告書	〃	〃	17	782			○	○	○						〃 〃
9 艀一覧表	〃	〃	8	172							○				〃 〃
10 バウチャー	〃	〃	9	509		○		○							I-04 本船手仕舞処理
11 エクセプション リスト	〃	〃	17	505		○		○							〃 〃
12 陸揚報告書	〃	〃	15	768				○							I-05 貨物搬入処理
13 ウエイト リスト	〃	〃													〃 〃
14 ランディング レポート	〃	〃	15	768		○	○								〃 〃
15 チェンキング レポート	〃	〃	18	709		○	○								〃 〃

帳票名	入/出	処理サイクル	項目数	桁数	提出先										使用目的・備考
					荷主	船社	海貨	エゼント	検数	検定	税関	港湾局	倉庫		
16. 入庫報告書	O	〃	11	476			○								I-05 貨物搬入処理
17. 搬入届	〃	〃	13	545			○				○	○			〃 〃
18. タリーシート	〃	〃	16	689									○		〃 〃
19. 輸入申告書(I/O)	〃	〃					○				○				I-06 通関処理①
20. (磁気テープ)統計テープ	〃	月1回									○				〃 〃
21. (ディスプレイ)許可済IDデータ	〃	リアルタイム					○								I-07 通関処理
22. 搬出届	〃	〃	12	473							○	○			I-08 発送処理
23. 出庫指図書	〃	〃	8	447									○		〃 〃
24. 送り状 請求書	〃	〃	8	447			○								〃 〃
計						7	12	9	7		7	2	4		48件 7利用者

5.4　輸入貨物管理システムの仕様

5.4.1　入力概要

入力データ一覧表（表３－３１）の通り，１０種類の入力情報が各利用者の端末機よりキーインで入力される。各入力データの項目名と桁数は輸入貨物管理データ動静及びファイル関連表に記載されている。（表３－３４）この表の⊕記号が発生データすなわち入力データである。データの入力源は海貨業者が３件と一番多く，エゼント，検数業者が各２件，検定業者，船社，税関がそれぞれ各１件となっている。輸出入業務とも海貨業者が入力情報を一番多く提供している。

5.4.2　出力概要

２４種類の出力が７利用者の端末機に出される。海貨業者に１２種類と全体の半数の出力が提供され，続いてエゼント業者に９種類，船社，税関，検数業者に各７種類，倉庫業者に４種類，港湾局に２種類が出力される。出力基本帳票一覧表（表３－３２）を参照のこと。なお各出力の項目名と桁数は輸入貨物管理データ動静表（表３－３４）にまとめてあり，各項目のデータの動静は６種類の記号（○，◎，△など）で明らかにされている。

5.4.3　ファイル概要

輸入貨物管理システムに用いるファイルは，次の３種類である。

①	ドキュメントファイル	２６項目	７７５桁
②	検数データファイル	４７項目	1,２３８桁
③	入庫ファイル	３３項目	７７８桁

各ファイルの項目名と桁数は輸入貨物管理データ動静及びファイル関連表（表３－３４）に○印で表示してある。

① ドキュメントファイル

Ｉ－０１貨物情報処理にて，船社からのＢ／Ｌ情報をソースとして船舶コード・Voy No.，B/L No. をキーコードして，ドキュメント・ファイルが作

成される。以後ドキュメント・ファイルは五つの業務処理に利用され，輸入貨物管理システムのメイン・ファイルであり，タリーシート情報とドキュメント・ファイルとの消込み，チェックを行い，リマーク・データを追加して，検数データ・ファイルが作られる。この二つのファイルと検数，検量データが加わり入庫ファイルが作られる。このようにドキュメント・ファイルは輸入貨物情報をベースに船卸計画・船卸作業および通関処理に必要なデータを提供する基本的なマスター・ファイルである。

② 検数データ・ファイル

検数データ・ファイルは，Ｉ－０３船卸作業処理にてタリーシートとドキュメント・ファイルとを照合し，リマーク・データを追加して作成される。検数データ・ファイルは，本船作業終了データを追加して，貨物の搬入作業のための必要情報を中心に構成され，このファイルとドキュメント・ファイルを照合して，各業者に貨物搬入作業情報を提供する。

③ 入庫ファイル

ドキュメント・ファイルと検数データ・ファイルを照合して，入庫ファイルが作成され，通関処理の基本ファイルとなる。入庫ファイルをベースにして，輸入申告書が作成され，通関状況の検索のファイルとして使われる。さらに通関データを提供して輸入貨物発送処理が行われる。

5.4.4 キーコード一覧表

輸入貨物管理システムにおいては，７種類のキーコードが８業務処理にて使用されている。これらのコードは，B/L No. と船舶コード Voy No. など組合せて使われることが多い。

使用目的と組合せはキーコード一覧表（表３－３５）を参照頂きたい。

表３－３４　輸入貨物管理データ動静及びファイル関連表

記号説明　◎固定データ　△受取不確定データ　㊀転記データ
○受取データ　㊉発生・優先データ　㊀△不確定転記データ

項目名＼帳票名	MANIFEST	DELIVERY ORDER	搬入連絡	総揚情報	作業依頼書	TALLY SHEET	TIME SHEET	CARGO BOAT NOTE	沖取報告書	DAILY WORKING REPORT	艀一覧表	VOUCHER(A)	VOUCHER(B)	EXCEPTION LIST(A)	EXCEPTION LIST(B)	沿岸タリーシート	陸揚報告書	RECHECKING REPORT
荷主名	◎	○	○		◎				㊉㊀							○	㊉㊀	
本船名	◎	○	○		◎	㊀		㊉㊀	㊉㊀	㊉㊀	㊉㊀	㊉㊀	㊉㊀	㊉㊀	㊉㊀	○		㊉㊀
入港月日					◎		○	㊉㊀	㊉㊀	㊉㊀	㊉㊀	㊉㊀		㊉㊀	㊉㊀	△		
バース			△		△	㊉	○	㊉㊀	㊉㊀	㊉㊀	㊉㊀			㊉㊀	㊉㊀	△		
船内	㊉		△		△				㊉㊀		㊉㊀					△		
揚場所			○	㊉	◎			㊉㊀	㊉㊀							○	㊉㊀	㊉㊀
ポートノート仕向先					◎													
B／L番号	◎	○		○	◎	㊉㊀		㊉㊀						㊉㊀	㊉㊀			㊉㊀
荷印	◎	○	○		◎	㊉㊀		㊉㊀	㊉㊀					㊉㊀	㊉㊀	○	㊉㊀	㊉㊀
品名	◎	○	○		◎	㊉㊀		㊉㊀	㊉㊀	㊉		㊉		㊉㊀	㊉㊀	○	㊉㊀	㊉㊀
個数（ロット数）	◎	○	○		◎	㊉㊀		㊉㊀	㊉㊀					㊉㊀		○	㊉㊀	㊉㊀
屯数	◎	○			△	㊉㊀			㊉㊀								㊉㊀	
艀名			△		△	㊉㊀		㊉㊀	㊉㊀		㊉㊀					△	㊉㊀	㊉㊀
海貨名			○		◎	㊉㊀		㊉㊀	㊉㊀		㊉㊀			㊉		○	㊉㊀	
コンテナ　種類	◎																	
〃　番号	◎																	
〃　内蔵個数	◎																	
仕出地	◎	○	△											㊉	㊉	△		
仕向地（引渡し地）	◎																	
荷姿	◎							㊉						㊉㊀	㊉㊀			㊉
PORT（揚港）						㊉㊀							㊉㊀	㊉㊀	㊉㊀			
作業日						㊉㊀	○		㊉㊀			㊉						
HATCH No.						㊉㊀		㊉	㊉㊀					㊉	㊉			
作業時間						㊉㊀			㊉㊀								㊉㊀	㊉
天候			○			㊉			㊉	㊉㊀							㊉	
次号	△	○	△	○				㊉㊀		㊉㊀				㊉㊀	㊉㊀			㊉㊀
レマーク						◎		㊉㊀								△		㊉㊀
時間外屯数						㊉			㊉									
出港日										㊉		㊉		㊉	㊉			
船積形式			○													○		
ケースNo.	㊉		△													△		

項目名＼帳票名	MANIFEST	DELIVERY ORDER	搬入連絡	総揚情報	作業依頼書	TALLY SHEET	TIME SHEET	CARGO BOAT NOTE	沖取報告書	DAILY WORKING REPORT	解一覧表	VOUCHER(A)	VOUCHER(B)	EXCEPTION LIST(A)	EXCEPTION LIST(B)	沿岸タリーシート	陸揚報告書	RECHECKING REPORT
シフト別屯数（昼　間）												㊀						
（前半夜）												㊀						
（後半夜）												㊀						
OVER																	㊀	㊀
SHORT																	㊀	㊀
BOAT NOTE No.								㊉			㊀							
検数会社名											㊉					○		
本日揚高（個数）			△	◎												㊉	㊀	
（屯数）																㊉	㊀	
船会社名	◎			㊉														㊀
現　出																		
不現出																		㊉
GANG数（昼間）																		㊉
〃　（夜間）							○			㊀			㊀					
HATCH別個　数							○			㊀			㊀					
〃　重量屯										㊀								
〃　容積屯										㊉								
〃　作業時間							○			㊉								
〃　作業内容							○			㊀			㊀					
蔵置場所の種類										㊀			㊀					
搬入場所名			○	○												○		
入庫年月日（受取）			○	㊉														
入庫No.				㊉												○		
届出年月日			△															
搬入出に関する許可又は承認の種類・番号・年月日																		
搬出年月日																		
桁数計	610	475	653	115	542	689	98	504	782	240	172	509	171	505	467	794	768	709
計　57項目	17	9	18	8	14	16	8	15	17	14	8	9	17	17	14	19	15	18

項目名＼帳票名	自主記帳台帳搬入届	港湾局搬入届	入庫報告書	荷役計画表	配送指示書	配送控	自主記帳台帳搬出届	港湾局搬出届	送状	貨物受領書	配送指図	ドキュメント・ファイル	検数データ・ファイル	入庫ファイル	コード化可能	桁数
荷主名	⊕	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	○	○	○		120
本船名	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	○	○	○	○	20~30
入港月日	⊕	⊖					⊖	⊖				○	○	○		8
バース												○	○		○	4
船内												○	○		○	30~10
揚場所												○	○	○		5
ボートノート仕向先												○	○			30
B／L番号				⊕								○	○	○		10
荷印	⊖	⊖	⊖		⊖	⊖	⊖	⊖	⊖	⊖	⊖	○	○	○		200
品名	⊖	⊖		⊕	⊖	⊖	⊖	⊖	⊖	⊖	⊖	○	○	○		30~60
個数	⊖	⊖	⊖	⊕	⊖	⊖	⊖	⊖	⊖	⊖	⊖	○	○	○		5
屯数												○	○	○		7~10
艀名													○	○	○	25~30
海貨名												○	○	○	○	30~10
コンテナ 種類												○	○	○		2
番号												○	○	○		14
内蔵個数												○				4
仕出地	△	△	△									○	○	○		30
仕向地（引渡し地）												○	○	○		30
荷姿												○	○	○		15
PORT（揚港）													○		○	30
作業口													○			8
HATCH No.													○			7
作業時間													○			210
天候													○			1
次号（Voy No.）												○	○	○		10
レマーク	△	△	△									○	○	○		50
時間外屯数													○			24
出港日													○			8
船積形式			⊖											○	○	1
ケースNo.	△	△	△		△	△	△	△	△	△	△	○	○	○		10

項目名 ＼ 帳票名	自主記帳台帳搬入届	港湾局搬入届	入庫報告書	荷役計画表	配送指示書	配送控	自主記帳台帳搬出届	港湾局搬出届	送状	貨物受領書	配送指図	ドキュメント・ファイル	検数データ・ファイル	入庫ファイル	コード化可能	桁数
シフト別屯数（昼間）													○			4
〃（前半夜）													○			4
〃（後半夜）													○			4
OVER													○			4
SHORT													○			4
BOAT NOTE No.													○			10
検数会社名												○	○	○	○	30~10
本日場高（個数）														○		4
〃（屯数）														○		7
船会社名												○	○	○	○	30~10
現出												○	○	○		4
不現出												○	○	○		4
GANG数（昼間）													○			7
〃（夜間）													○			7
HATCH別個数													○			5
〃 重量屯													○			4
〃 容積屯													○			7
〃 作業時間													○			28
〃 作業内容													○			61
蔵置場所の種類		⊕						⊕						○	○	2
搬入場所名	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖		○	○	○	10
入庫年月日（受取）			⊖	⊖										○		8
入庫No.	⊕	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖			○		12
届出年月日	⊕	⊕					⊕	⊕						○		8
搬入出に関する許可又は承認の種類・番号・年月日	△						△							○		2
搬出年月日							⊕	⊕						○		8
計 項目	12	13	11	8	8	8	12	12	8	8	8	26	47	33		
桁数計	545	545	476	255	447	447	473	471	447	447	447	775	1238	778		

表３－３５　キーコード一覧表　（輸入貨物管理システム）

コード名	桁数		使用目的	備考
1. B/L No.	10		ドキュメントファイル作成する	I-01 貨物情報処理
2.船舶コード Voy No.	14		〃	〃
3. B/L No.	10		ドキュメントファイルの不足データ追加	I-02 船卸計画処理
4.船舶コード Voy No.	14		〃	〃
5.船舶コード Voy No.	14		ドキュメントファイルの消込み，照合，リマーク・データを追加し検数データファイルを作る。	I-03 船卸作業処理
6. B/L No.	10		〃	〃
7.はしけ No.	16		〃	〃
8.船舶コード Voy No.	14		バーチャー，エクセプションリストの出力	I-04 本船手仕舞処理
9. 保管場所コード	6		出力リスト作成	I-05 貨物搬入処理
10. B/L No.	10		〃	〃
11.船舶コード Voy No.	14		〃	〃
12. 艀No.	16		〃	〃
13. B/L No.	10		輸入報告書の出力　入庫ファイルの更新追加 統計テープの作成	I-06 通関処理①
14.船舶コード Voy No.	14		〃	〃
15. インボイス No.	10		〃	〃
16. 入庫No.	12		〃	〃
17. I/D No.	12		入力ファイルの更新	I-07 通関処理②
18. 入庫No.	12		搬入届，出庫指図書，送り状作成	I-08 発送処理

(注)　本コードは仮定的ではあるが，それぞれの根拠となるのは，

①　船舶コードVoy No.は，国際電気通信条約付属無線通信規則による船舶局の呼び出し符号４桁，航海番号１０桁

②　艀コードは地方海運局登録港運船番号を港名称表示部分を４桁，港運船種別１桁，社名部分を６桁，通し番号部分２桁，　　数（馬力）３桁とした。

③　保管場所コードは本報告書(II)に所収

6. 共同利用センターの
コンピュータ・システムの規模と費用

6.1 対象とする業務量の推定

大黒埠頭の計画バース数は８バースである。この各バースあたり取扱いできる船数は，平均で８船／１バース，月と推定できる。大黒埠頭の帳票（B／L）の，月間当りの件数は，188件／船位と推定した。以上の仮設をもとに大黒埠頭の全体B／L件数を設定する。

- １バース当りのB／L件数

  188件／船×８船／バース，月＝1,500件／バース，月

- 大黒埠頭全体のB／L取扱い件数

  1,500件／バース，月×８バース＝12,000件／月

この月間当り全体のB／L取扱い件数は，「総合貿易情報システム調査報告書（IV）」（財日本情報処理開発協会発行）中の横浜港における月間平均値のB／L件数37,000件／月平均の３２％に相当する量である。

大黒埠頭全体の帳票処理件数を横浜港のと比較して記述する。

（単位　件／月）

	（昭．５０年推計） 横　浜　港	（埠頭完成時の推計） 大 黒 埠 頭
EXPORT DECLARTION	50,000	16,200
BILL OF LADING	37,000	12,000
SHIPPING ORDER	37,000	12,000
COMMERCIAL INVOICE	50,000	16,200
合　　計	174,000	56,400

（注）１船当りのB／L件数は，貨物の性格によって著るしく変化して来る。こゝに示した数値はあくまで仮設にもとづくものであって，雑貨を主体として考える。１隻当りのB／L件数を１８８件としているが，これは可な

り少なめの推定である。

① 共同利用センターへのアクセス頻度

データ・ベースを設定し，主要業者が，各々データ・ベースへアクセスする割合（トランザクション頻度）を考えてみる。主要業者としては海貨通関係者である。

この業者のセンターへのアクセスを推定するあたり，主要業務を分類すると，貨物管理，E／D作成業務，B／L作成業務の三つに大別できる。貨物管理の件数は，日によって異なり1社で1日1～2件のこともあれば，300件にも達することもある。センターへのアクセスは，その3倍と見ておく必要がある。E／D，B／Lは大体同じ数と見られるが，これも日によって異なる。埠頭全体の量を考察すれば，E／D1件に対して，それぞれS／I，B／Lも1件づつと仮定する。この仮定は若干の誤差を含むが，業界の経験からすると，その誤差の割合は5％以内にとどまる。又，月間労働日数20日，1日の労働時間数を7時間，大黒埠頭利用海貨通関業者60社の仮定を基礎して算出する。

- 日単位のE／D件数　16,200件／月÷20日／月＝810件／日
- 1海貨通関業者単位のE／D件数

  810件／日÷60社＝13.5件／日，社
- 時間単位のE／D件数　810件／日÷7時間／日≒116件／時間
- 1海貨通関業者単位のE／D件数

  116件／時間÷60社≒2件／時間

1時間あたりの海貨通関業者のセンターへのトランザクション・アクセス頻度は，

(1) 貨物管理　116件×3アクセス＝　348
(2) S／I　116件×2アクセス＝　232
(3) E／D　116件×2アクセス＝　232
(4) B／L　116件×1アクセス＝　116

(5) その他　　１１６件×２アクセス＝　２３２

合　計　　1,１７０回／H

となる。大黒埠頭利用業界・団体のうち海貨通関業者数は６０社で全体の６６.７％をしめ，残り３３.３％をしめる約３０社が他関連会社及び団体が利用すると考えられる。これら他関連会社及び団体等がセンターを利用すると仮定するなら，トランザクション・アクセス頻度は５０％アップの約2,０２０回／時間と推定できる。

6.2　共同利用センターのホスト・コンピュータの構成

共同利用センターのホスト・コンピュータの規模と機器構成は，図３－４８のごとく設定した。中央処理装置は，オンライン・リアルタイム処理の故障による処理不能をさけるために，デュプレックス方式を採用し，予備として１台追加設置した。端末機との接続は１２５台であるが将来の拡張も考慮に入れて，最大２００回線まで使用可能とした。

データベースに用いる各ファイルの大きさは，業務量の推定を基準として計算し，これを基礎に磁気ディスク装置の容量の台数の見積りに用いた。

磁気テープ装置は６台設置し，入出力，問合せのジャーナル記録と取引完了ファイルの記録として利用する。また本体故障による処理の中断時の再現のためにも利用できる。さらにデータ・セキュリティ対策の記録保存の機能も有している。

以下ラインプリンター２台，カード読取装置，カードせん孔装置は，バッチ処理用および受託処理用にも活用する。

その他，業務処理の数等を検討した結果，共同利用センターのホストマシンとして，中型機クラスの大規模構成のシステムを採用することとした。

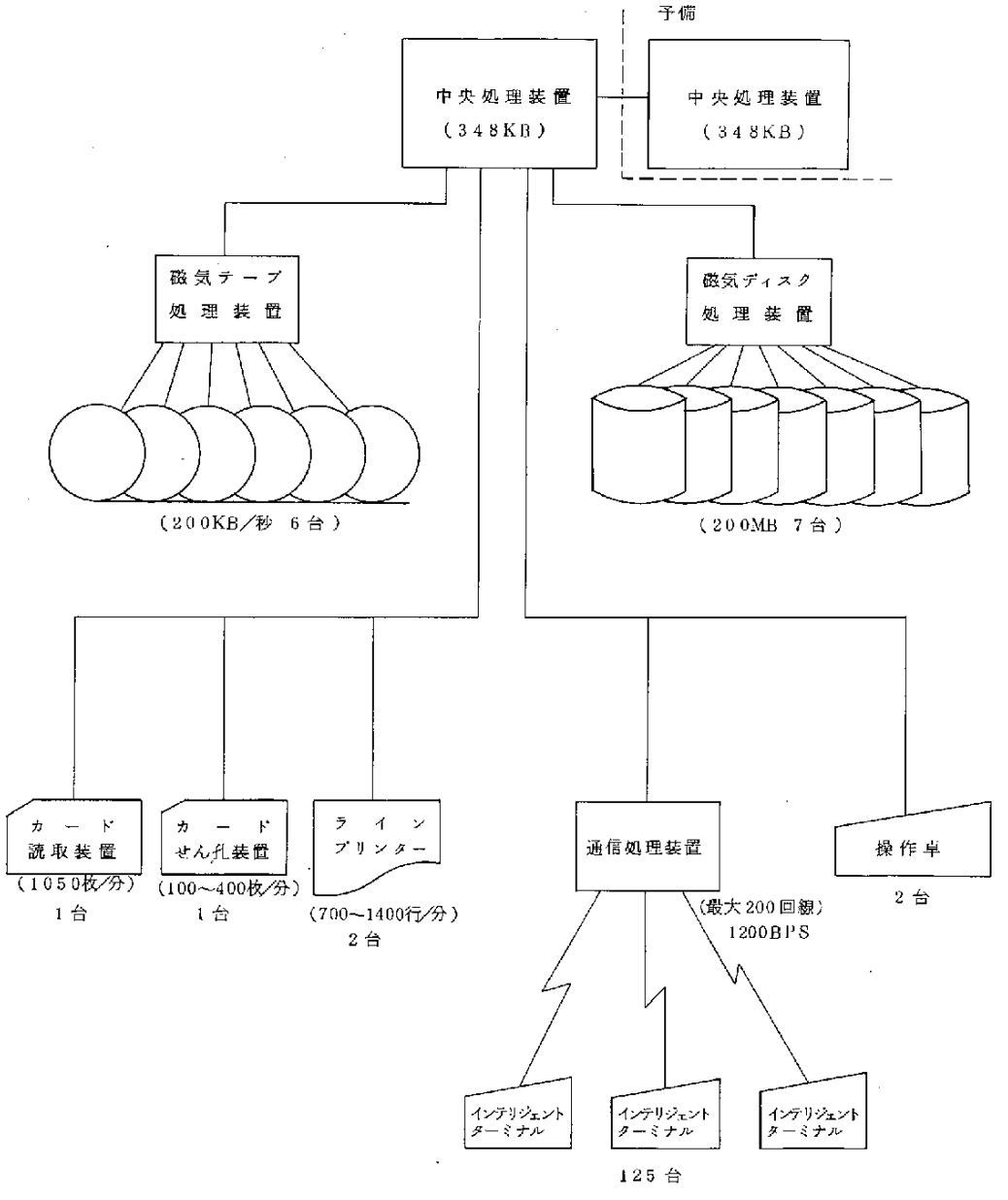


図3－48　共同利用センターのコンピュータシステムの機器構成

6.3　利用者側に設置する端末機（インテリジェント・ターミナル）

6.3.1　端末機の設置台数

センターのコンピュータを利用する形態としては三つの方法がある。

(1)　センター内の端末を共同利用

(2)　自社に端末を導入してセンターの電算処理を行なう。

(3)　センター内に自社費用で端末を導入利用

利用業者・団体名		端末数（台）	備考
海貨通関業者	規模小	30社　10台	共同利用できるようにする 利用海貨業社30社とする
	中	(a)　20社×1台＝　20	台数内訳 大黒埠頭1台
	大	(b)　10社×3台＝　30	台数内訳 大黒埠頭2台，本社1台
エゼント業者		16社×3台＝　48	設置台数内訳 大黒埠頭2台，本社1台
検数業者		2社×2台＝　4	設置台数内訳 大黒埠頭1台，本社1台
検定業者		2社×2台＝　4	〃
税関		1　×1台＝　1	
船会社		6社×1台＝　6	
港湾局		1　×1台＝　1	
東洋信号所		1　×1台＝　1	
合計		89団体　125台	

本システムにおいては上記のごとく，89団体125台を設定した。共同利用センターの中枢的利用者である海貨業者とエゼント業者（大規模業者は海貨業兼務がある）に，全体の86%を占める108台を設置した。海貨業者は，それらの企業規模によって，業務量が大きく異なるため，大・中・小の3分類に分けた。大規模業者は10社とし，端末機は大黒埠頭2台，本社1台計3台，中規模業者20社は，大黒埠頭に各1台設置するものとする。

小規模業者３０社は採算性，業務量からみて独自に端末機を設置するのは困難と判断し，共同利用センターに端末機を１０台置いて共同利用することとした。

エゼント業者は１６社が共同利用センターを利用するものとし，各々大黒埠頭に２台，本社に１台端末機を設置した。検数・検定業者については，検数・検量結果を端末機より直接入力し，関連業者にその結果を出力するとともに，センターより作業予定情報を出力する。そのために検数２社４台，検定２社４台をそれぞれ設置する。

その他，税関に１台，船会社に各１台，港湾局に１台，本船情報を得るため東洋信号所に１台設置する。

6.3.2 端末機（インテリジェット・ターミナル）の仕様

利用者側に設置する端末機の主な仕様は次の通りとする。

① インテリジェント・ターミナルの採用

ⓐ センターのホストマシンの処理効率を上げる。

ⓑ 利用者側のニーズにあった出力形式が得られる。

ⓒ 社内システムへのデータの授受が可能となる。（入出力装置付加により）

② ディスプレイ装置をつけ，情報検索を簡単にする。

③ 補助記憶装置（プロッピィーデイスク・磁気カセットなど）をつける。

ⓐ 入力データのチェックが端末機サイドである程度出来るようになる。

ⓑ 帖票出力でプリント時間のかかるものは，データを一担補助記憶装置に入れて，端末機側で編集出力する。

(イ) センターとの接続時間が短くなり，センターのホストマシンの処理効率が上る。

(ロ) 利用者にマッチした出力形式が可能となる。

④ プリンターのプリント速度は４０字／秒程度のものとする。

⑤ インテリジェット・ターミナルの価格

買取価格１台３５０万円とした。

月額リース料９８千円（リース料率５年間2.3％，保守料率0.5％）

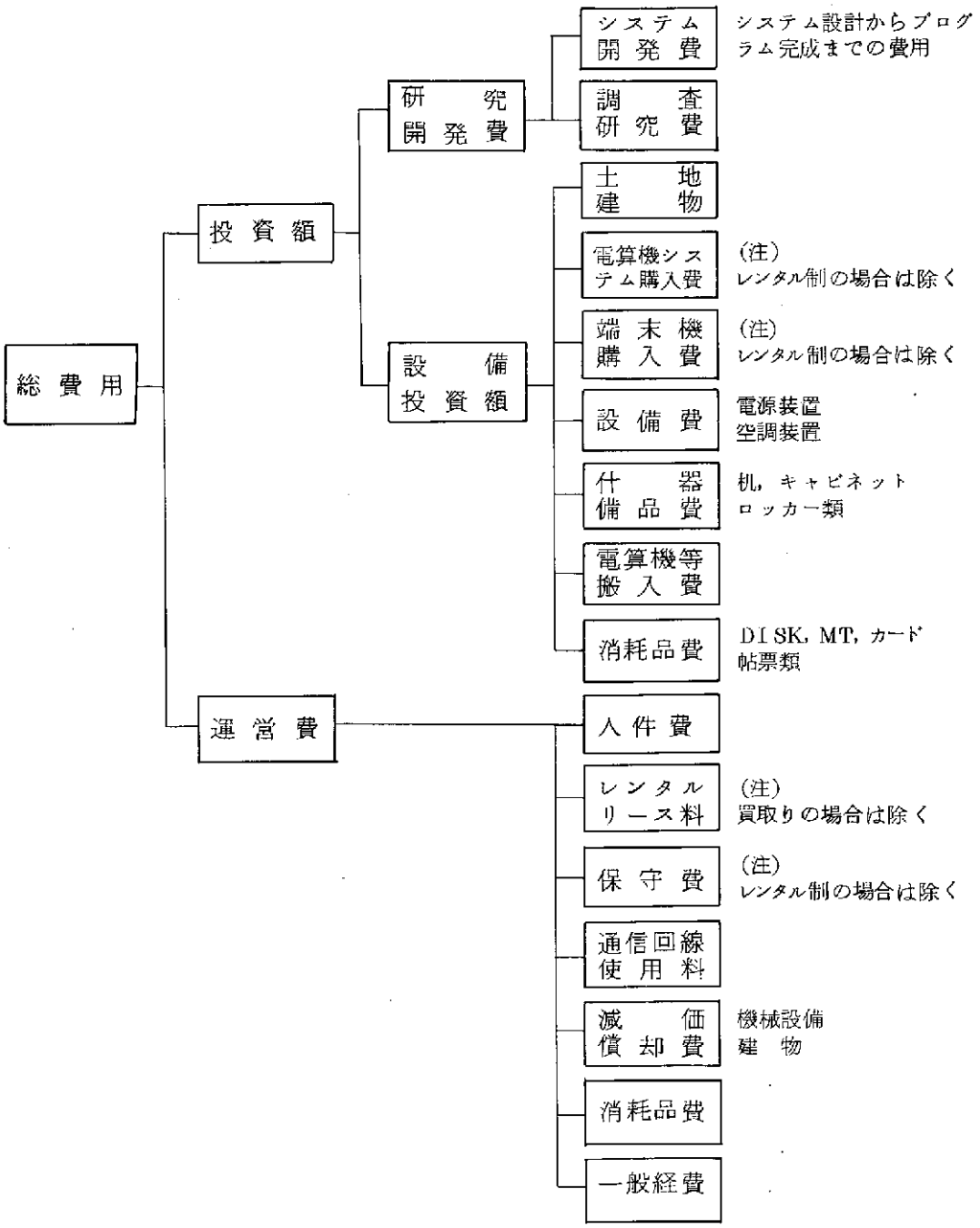


図３－４９　共同利用センターに要する費用の体系図

表3－35　コンピュータ・システムの機器構成と費用見積り

前提：1.　機種，中型機大規模構成システムとする。

2.　データ量の推定は月間全データ件数約21万件／月とする。

3.　オンライン端末機は125台とする。

機器名称	台数	賃貸料（千円／月）	
1. 中央処理装置（384K MAX）	2	6,840	(a)32Kにつき増設費用 145千円 (b)付加　160千円含む
2. システム制御装置	1	110	
3. 操作卓	2	260	
4. 通信処理装置	1	920	200回線使用可能
5. 磁気ディスク装置	7	2,820	1台，200MB容量
6. 磁気テープ装置	6	1,380	
7. ラインプリンター	2	680	
8. カード読取装置	1	150	
9. カードせん孔装置	1	200	
合計		13,360	買取　6億120万円

		千円／月	
オンライン端末機（インテリジェント・ターミナル）	125台	12,250	買取価格350万円 （リース料2.3%，保守料0.5%） 98千円／月　リース料

（端末機買取価格計4億3,750万円）

6.4　共同利用センター費用概算

共用利用センターの費用見積りをするにあたり，共同利用センターに要する費用の体系を図3－49のごとく把握することにした。ただし今回は概要設計の段階であるため，ハードウェアの費用見積りを中心として行い，システム開発費・設備費・運営費等の費用はごく大ざっぱに見積ることとした。なお，コンピュータはレンタル制をとることとし，端末機は5年リースのリース料金を算出した。それ故，投資額すなわち研究開発費と設備投資額もすべて総発生費をレンタル料にならって3年償却（３６ヶ月）し，月額で把握することとした。

① 研究開発費　　2億7,５００万円（７６３８千円／月）

開発要員　１０名，　開発期間　3年，　人件費　１人５００万円／年

人件費＝１０名×３年×５００万円＝１億5,０００万円

コンピュータ使用料　　１億2,０００万円

（レンタル月額1,０００万円，使用期間１年）

その他諸経費　　５００万円

② 設備投資額（電源装置，空調装置，什器備品費，電算機搬入費等を含み，土地建物は除く）

概算で約0.2億円程度とする。（５５６千円／月）

③ 運　営　費　　２５,０００千円／月

センター運営費　　１３,０００千円／月

端末機運営費（１２５台分）　１２,０００千円／月

運営費は一般的にレンタル料とほぼ同程度と言われているので，ここではレンタル料にほぼ見合った費用を概算計上した。

④ ハードウェア費用　　２５,６１０千円／月

コンピュータ本体　　１３,３６０千円／月（レンタル料）

端末機（１２５台）　　１２,２５０千円／月（リース料）

共同利用センターの費用概算（月額）

①	研究開発費	7,638千円／月
②	設備投資費	556千円／月
③	運営費	25,000千円／月
④	ハードウェア費	25,610千円／月
	計	58,808千円／月　年間約70,560万円

6.5　共同利用センターの費用の評価尺度

共同利用センターの費用は約5,880万円／月が見込まれるが，この費用を次の5項目と対比させて，コンピュータ費用の評価尺度としてみる。

① 貨物取扱量1トン当り　176円　（5,880万円÷33.3万トン／月）

② 1本船当り　92万円　（5,880万円÷64船／月）

③ 1バース当り　734万円／月（5,880万円÷8バース）

④ B／L1件当り　4,892円　（5,880万円÷12,000件／月）

⑤ 1端末機当り　47万円／月（5,880万円÷125台）

6.6　1シップメント当たりの費用負担区分と効果

輸出，輸入の各業務処理を1シップメントの流れとして捉え，これを現行の費用と比較したものが，次の表である。

共同化費用の算出に当たっては，次の手順を経ている。

① 全処理費用について，輸出，輸入のウェイト比率を算定し，B／L件数，業務処理数から輸出，輸入それぞれの費用を算出した。

輸出　78%　4,229万円

輸入　32%　1,221万円

② 業務処理のグレードをインプットの難易，使用エリアの大きさ，処理の煩簡を念頭において，輸出，輸入各業務処理に付した。

③ 輸出，輸入の1シップメント当たりの費用は，

輸　出　　4,８００円

輸　入　　4,１００円

④　業務処理ごとの費用をウェイトに従い配分した。

⑤　現行費用は，所要時間で見積り，予想される付帯費用は除外し，労働コストにのみ，置きかえた。労働コストは，年間３６０万円，月間３０万円，１分当たり３０円と見積られている。

以上の作業結果から，次の点が明らかとなった。

a　時間（スピード）では，輸出１６８分，輸入１３９分かかっている現行処理が３０%短縮され，

輸　出　　５４分の時間節減

輸　入　　４２分の時間節減（総揚げ貨物については４４.７分）

b　費用面では，

輸出は現費用より　６００円減

輸入は現費用より　　７０円減（総揚げ貨物では１３０円減）

c　費用負担区分は，

表３－３６　費用負担区分とメリット帰属

△は節減

	輸出			メリット		
	共同化後	現行	現行時間	費用	時間	備考
海貨	円 2,840	円 2,900	分 130	円 △1,060	分 △39	
エゼント	円 1,960	円 1,500	分 50	円 460	分 △15	
計	円 4,800	円 5,400	分 180	円 △ 600	分 △54	
	輸入			メリット		
	共同化後	現行	現行時間	費用	時間	備考
エゼント	円 2,190	円 1,650 (1,950)	分 55 (65)	円 460 (400)	分 △16.5 (△19.5)	( )内は総揚げの場合
海貨	円 1,910	円 2,520	分 84	円 △530	分 △25.2	
計	円 4,100	円 4,170 (4,470)	分 139 (149)	円 △70 (△130)	分 △41.7 (△44.7)	

表3－37　業務処理費用比較　（輸出1）

○は新規可能処理

処理名	Grade	百分率構成(%)	B/L当たりの配分値	アウトプット帳票・データ名	負担先又は出力量	1出力単位当たりコスト	現行作成コスト	算定理由	比較増△減
貨物受付 E－01	10	5.0	240円	施検票 入庫報告書	海貨 海貨	60円 60円	3分　90円 5分150円		△30円 △90円
				搬入届（税関） 搬入届（港湾局）	海貨 海貨	60円 60円	現行ワンライティング 5分150円		△30円
受注① E－02	5	2.5	120円	○ブッキングリスト	エゼント	120円	受領はテレックス打かえ 2分　60円		60円
受注② E－03	30	15.0	720円	S/O スリップ 作業指示書	海貨（出力先2） 海貨（出力先4）	300円 300円	5分150円 ワンライティング 7分210円		150円 90円
				○集荷情報		120円	電話問い合わせ（複数回） 5分150円		△30円
S/O・B/L E－04	35	17.5	840円	S/O・B/L セット ○マニフェスト・テープ	海貨 船社	540円 300円	30分900円 手作業　10分 300円		△360円 0円
船積計画① E－05	5	2.5	120円	○ローテイングリスト	エゼント（出力先2）	120円	リスト受取り 2分　60円		60円

業務処理費用比較　（輸出２）

処理名	Grade	百分率構成(%)	B/L当たりの配分値	アウトプット帳票・データ名	負担先又は出力量	1出力単位当たりコスト	現行作成コスト	算定理由	比較増△減
船積計画② E－06	１５	7.5	３６０円	○荷役計画書	エゼント (出力先３)	３６０円	５分１５０円		２１０円
通関① E－07	２０	10.0	４８０円	E／D ○統計データ	海貨 (出力先２) 税関	４８０円 無料	２０分６００円 なし		△１２０円
通関② E－08	5	2.5	１２０円	○許可済E／D チェック	海貨	１２０円	税関連絡立ち合い １５分４５０円		△３３０円
荷受連絡 E－09	5	2.5	１２０円	荷役予定表	海貨 エゼント	６０円 ６０円	５分１５０円 ５分１５０円		△９０円 △９０円
出庫 E－10	２０	10.0	４８０円	出庫表 出庫報告書	海貨 海貨	８０円 ８０円	ワンライティング ３分　９０円 ３分　９０円		△１０円 △１０円
				搬出届（税関） 搬出届 （港湾局）	海貨 海貨	８０円 ８０円	搬入届とワンライティング探す作業打ち込み ５分１５０円		１０円
				船積作業依頼書 ○荷役予定データ	海貨 (出力先２) 海貨	８０円 ８０円	電話 ６分１８０円 ３分　９０円		△１００円 △１０円

業務処理費用比較　（輸出３）

処理名	Grade	百分率構成(%)	B/L当たりの配分値	アウトプット帖票・データ名	負担先又は出力量	１出力単位当たりコスト	現行作成コスト	算定理由	比較増△減
船積① E－１１	１０	5.0	２４０円	船積報告書	海貨 (出力先３)	２４０円	ワンライテイング １０分３００円		△６０円
船積② E－１２	１０	5.0	２４０円	○未搬入貨物リスト ○貨物搬入依頼データ	エゼント(出力先２) エゼント	１２０円 １２０円	３分　９０円 電話連絡 ３分　９０円		３０円 ３０円
船積③ E－１３	２０	10.0	２４０円	○船積完了情報 ディリーワーキングリポート	エゼント エゼント (出力先２)	６０円 ３４０円	３分　９０円 ２分　６０円		△３０円 ２８０円
				本船積報告書	海貨	８０円	５分１５０円	B/L件数はゴーダウン貨物の方が多い作成頻度は３５％程度	△７０円
本船手仕舞 E－１４	１０	5.0	２４０円	バウチャー(A.B.C.D) エクセプションリスト(A.B)	エゼント エゼント	８０円 ８０円	４分１２０円 ４分１２０円		△４０円 △４０円
				ハッチリスト	エゼント	８０円	２分　６０円		２０円
計	２００	100.0	4,800円				１８０分 5,４００円		△５４分 △６００円
					海貨 エゼント	2,８４０円 1,９６０円	130分 3,900円 50分 1,500円		△1,０６０円 ４６０円

表3－38　業務処理費用比較　（輸入１）

処理名	Grade	百分率構成(%)	B/L当たりの配分値	アウトプット帖票・データ名	負担先又は出力量	１出力単位当たりコスト	現行作成コスト	算定理由	比較増△減
貨物情報	１５	8.8	360円	○マニフェスト	エゼント	３６０円	機械化していて		２１０円
					(出力先4)	マニフェストより社内で展開	１分ただしデータは手渡し手作業５分１５０円		
I－０１				（D／O	船社）				
船卸計画	２５	14.7	600円	デリバリーオーダー	エゼント	２００円	手作業		５０円
					エゼント		５分１５０円		
I－０２				総揚貨物予定表	(出力先3)	１００円	３分　９０円	総揚貨物の一部	１０円
				荷役計画表	エゼント (出力先3)	１００円	２分　６０円		４０円
					エゼント	１００円	５分１５０円		△５０円
				作業依頼書	(出力先2) エゼント				
					(出力先2)	１００円	５分１５０円		△５０円
船卸作業	３０	17.7	730円	デリーワーキンググリボート	エゼント (出力先2)	３４０円	２分　６０円		２８０円
					海貨				
I－０３				ボートノート	(出力先5)	１６０円	５分１５０円		１０円
				沖取報告書	海貨	１８０円	３分　９０円		９０円
					(出力先4)				
				解一覧表	エゼント	５０円	２分　６０円		△１０円
本船手仕舞	１０	5.9	230円	バウチャー（A.B.C.D）	エゼント (出力先2)	１１５円	４分１２０円		△５円
				エクセプションリスト（A.B）	エゼント				
I－０４					(出力先2)	１１５円	４分１２０円		△５円

業務処理費用比較　（輸入２）

処理名	Grade	百分率構成(%)	B/L当たりの配分値	アウトプット帖票・データ名	負担先又は出力量	1出力単位当たりコスト	現行作成コスト	算定理由	比較増△減
貨物搬入	30	17.7	730円	陸揚報告書	海貨	180円	3分　90円		90円
I－05				ウェイトリスト	海貨	15円	常時とるものではない		－
				ランデイングリポート	エゼント	180円	5分150円		30円
				リチェッキングリポート	エゼント	15円	常持とるものではない		－
				入庫報告書	海貨	110円	5分150円		△40円
				搬入届（税関）	海貨	60円			
					（エゼント）	（60円）	5分150円		△30円
				搬入届（港湾局）	海貨	60円	（150円）		
					（エゼント）	（60円）			（△30円）
				タリーシート	エゼント	110円	3分　90円	庫入れ機数	20円
通関①	25	4.7	600円	輸入申告書（I／D）	海貨	600円	30分900円		△300円
I－06				○統計テープ	税関	無料			
通関②	5	2.9	120円	○許可済I／Dデータ	海貨	120円	15分450円		△330円
I－07									

業務処理費用比較　（輸入３）

処理名	Grade	百分率構成(%)	B/L当たりの配分値	アウトプット帖票・データ名	負担先又は出力量	1出力単位当たりコスト	現行作成コスト	算定理由	比較増△減
発送 I－０８	３０	17.7	７３０円	搬出届（税関） 搬出届 （港湾局）	海貨（エゼント） 海貨（エゼント）	６０円（６０円） ６０円（６０円）	５分１５０円 （５分　１５０円）		△３０円 （△３０円）
				出庫指図書	海貨	１１０円	５分１５０円		△４０円
				送り状	海貨	１００円	３分　９０円		△１０円
				請求書	エゼント	４００円	１５分（事前連絡を含む） ４５０円		△５０円
計	１７５	100.0	4,100円		（）内は総揚貨物の場合		１３９分 （１４９分） 4,170円 （4,470円）		△41.7分 （44.7分） △７０円 （△１３０円）
					海貨 エゼント	1,910円 2,190円	８４分 2,520円 ５５分 （６５分） 1,650円 （1,950円）		△16.5分 （△19.5分） ４６０円 （４００円） △25.2分 △５３０円

（註）　グレードの点数は，単純転記を５とし，これを基準値とした。

〔i〕 荷主に与えるメリット

想定される大黒埠頭のライナーバースの年間輸出入取扱件数は，

輸　出　　108,000件

輸　入　　36,000件

である。これを昭和51年の横浜港通関実績を基礎にして1件当たりの取引金額を求めると（雑貨に限定し，保税運送分は含んでいる）

輸出1シップメント取引額　　855万円

輸入1シップメント取引額　　513万円

となる。時間短縮により，荷主側に発生するメリットは，

貿易金融　年利8.5％　日割0.0002328（0.02328％）を基準として

輸　出　54分減

輸　入　41.7分減

がもたらす影響について，主に輸出面から検討してみた。

① 輸出の場合のB／L発行日の迅速化による金利負担の軽減

本システムでは，B／Lあげ日（本船積み確認と発行者サイン日）が早くなり，日割での金利軽減が図られる。現行では入港日1週間前より荷受けは行なわれるが，エゼント搬入は荷役日に殺到する。このため，本船に貨物が積付け完了したという情報は，出港後でなければ確認しがたい（大量貨物に限り，荷主の便宜を図るという場合もある）。在来船は，3日とみられるので，入港日に受けた貨物は，4日目ないし5日目にB／Lの発行となる。また船積み後24時間以内に税関の船積確認の手続きをとらなければならない（検数が代わって手続きをしている.）。こうして発行条件は延びがちである。この条件が検数情報を本船々上ないし船側バースで入力すれば，船積確認は最も遅い船積みの場合でも，完了後24時間以内に確認できることになる。したがって平均2日分の金利を生み出すことができる。すなわち，

855万円×9,000件×0.0002328×2＝35,827,920円／月

年間に直せば，実に４２９,９３５,０４０円つまり４億３千万円／年の金利負担を免がれることができる。１シップメントでは３,９８０円８８銭である。

② 荷役時間に与える影響からターミナル費用のうち，荷主側軽減となるのは，次の算定式によって求めると，

在来船の荷受方式においては，本船々側までは，すべて荷主側のアカウントとなっている。したがってターミナル費用を分解すると，

輸出の場合（機械類（１個５トン未満）の１トン当たり輸出船積み料金及び付帯料金）

船積形態	港運料金適用記号	港運料金	船積事務作業費(内数)	受け渡し方式
上屋入れより艀取り本船積み	A 表 はしけ荷捌料金(卸積み)	円 4,3 5 5.2 0 1 7 2.0 0 計4,5 2 7.2 0	円 1,2 3 0.0 0	はしけ積み方式
直背後上屋入れより接岸本船積	B 表	3,3 9 6.2 0 計3,3 9 6.2 0	1,1 7 7.0 0	戸前受け制度（TRS方式）
上屋入れより接岸本船エプロン上へ横持ちし船積み	C 表 横持料金 トラック積卸手数料金	4,3 4 2.6 0 ※4,0 0 0.0 0 6 6 0.0 0 計9,0 0 2.6 0	1,2 2 1.0 0	Godowo方式
私設倉庫会社の上屋倉庫前河岸はしけ受けより本船積み	D 表 はしけ内荷捌料金 倉出荷役料金	2,7 8 0.9 0 1 7 2.0 0 8 9 1.0 0 計3,8 4 3.9 0	1,1 6 4.0 0	かんづめ等特定貨物

※ 本料金は変数で，一応の目途を示している。

これは貨物の流れにかかる費用であるが，本船の入港予定が各バースごとに明らかとなるので，「直背後上屋入れより接岸本船積み」への傾斜が強くなってくる。現行は貨物の「荷揃い」，「手入れ」，「通関手続き」，「ストック・ポイント機能」等の理由から，直背後上屋へ搬入する割合は１０％台にも満たない状況であるが（上屋入れより艀取り本船積みの場合が７０％台を占めるのは横持ち費用が小さいこと，上屋戸前出し本船積み料金いわゆるゴーダウン料金を海貨がエゼントないし沿岸業者に，下払いしなければならないことなどによる），「着岸バース不明」原因で貨物を横持ちする費用を最小にするのは，本システムが直接役立つものではないが，入港予定日時の伝達機能，Ｂ／Ｌあげの迅速化は，本埠頭へ貨物を吸引する役割を果たし，貨物の流れも，直背後上屋入れか，これにほぼ近い背後地のいわゆる海貨センター（共同上屋）入れとなる。料金も直背後上屋入れ3,396円20銭と上屋入れエプロン出し9,002円60銭の中間上屋艀取り4,527円20銭を下まわる大黒埠頭の輸出船積みに係わる特殊料金が設定されるようになろう。１トン当り１００円減となる。

③ これに関連して，現行の輸出貨物の上屋保管料は，機械類（プラントを除く）の場合，１５日以内の保管期間ではトン当たり６１円７０銭である。保管料の面からの削減としては，荷主が港頭の保税上屋を内陸の倉庫機能の延長として期待して，本船名未定のまま送貨してくる場合には，削減効果を問題にすることは意味がないが，通関待ちのため滞留する場合を想定した場合，１日の短縮は６１円７０銭（トン当たり）を生じるから，上屋滞留日数の最多部分は，

貨物受領から通関済みまで	３日以内	44.9％	
	４～７日以内	39.3％	平均1.9日 すなわち２日
通関済みから船側まで	通関済み当日	46.1％	
	２～３日	41.5％	平均0.5日 すなわち１日

の現状から，貨物受領から上屋出しまでに平均３日滞留する。通関済情報の迅速化，荷受連絡の迅速化により全輸出貨物に１日ずつの滞留日短縮（貨物の港頭着の調節も逆に可能）するとすれば，

9,000×61.70＝555,300円　月　55万5,300円の保管料節減

年間　6,663,600円の節減

１シップメントにすると493円60銭減となる。

以上，荷主の輸出にかかわるコスト節減を要約すると，

１シップメント当たり

B／Lあげ迅速化金利軽減		3,980円	
貨物荷役費	〃	100円	トン当たり
保管料	〃	61円70銭	トン当たり
計		4,141円70銭	

荷主の輸入面のメリットの検討は省略する。金融，市場要因が大きいためである。

〔ii〕 船社に与えるメリット

船社が本システムに係わる場合，入力負担は輸出にあっては，ブッキング情報，ローディングリスト情報，輸入にあってはマニフェスト情報であり，従来からエゼントとの間では交信されている内容であって，負担となるものはない。逆に出力あるいは受領できるものとして，

輸出では，①新たにB／LデータがM／Tで受領，以後の社内業務に展開できる。

この費用は，社内担当者の１名分は減員できる作業量（１船200件とすると３日程度の作業量，１社で大黒埠頭に寄港する船が月間64隻中，７隻ならば完全に減員。）に当たっている。１船単位で，43,200円相当の節減

② 船積完了情報の早期入手が可能，荷主サービスはもちろん，B／L発行手数等の節減，フレートの問い合わせサービス不要

③　集荷状況の掌握，荷役計画の掌握，荷役進行状況の掌握

輸入においては，荷役進行状況の掌握，未引渡し貨物の掌握が容易となる。船社のターミナル費用は，船内荷役料金を中心としており，本システムの効果は，在来型荷役の作業能力を直接左右するものではないが，ギャング手配の上から，ロスタイムの節減に役立つとともに，本船入出港の計画化，運航計画の維持に寄与することができる。以上②，③からターミナル費用トン当たり５０円節減と評価する。

〔iii〕港湾内部に与えるメリット

A　エゼント（ライナーバース・オペレータ）

エゼントが本システムにより蒙る費用は，現行より負担増のようにみえている。

システム費用を敢えて負担して償うとすれば，なにが他に利益の源泉となるかといえば，後方要員の大巾減員と１船当たりの船積み卸し貨物量の増加である。

人間が行っている作業を本システムは３０％減少する。エゼント業務に係わる指標は1,000件の輸出入貨物の後方業務処理（現場への書類持ち歩き連絡，帖票作成等）に５名を要している。１船輸出２００件，輸入７０件平均とすると，５名ないし６名が係わることになる。この人員は２名減員できるから，月間１バース当たり２７０件×８隻＝2,160件ほぼ１１名の要員が必要であったのが，３名減員でき，１バース当たり９０万円節約できる。

１シップメントに直せば，４１７円節約できる。

次に貨物の吸引に本システムが役立つことは，荷主の項で触れたが，これは１バースごとの貨物取扱い量に反映して，埠頭経営面からの収入増を促がすことになる。

B　海　　貨

海貨にもたらされる本システムのメリットは，費用面に直接反映され

ている。また時間面での業務処理速度においても短縮される。省力化とコスト節減が同時に可能となる。

海貨は事務処理能力の飛躍的向上が図られる。

① 現行の事務処理能力を3割は引上げられる。（輸出入とも時間は現行の30%減）

② 直接事務処理費を25%引下げられる。（輸出入とも）

③ データ確認が単純化し，データのやりとりは正確化し，通信時間，通信費用が減る。

④ 現場派遣人数の減員が期待できる。

通関（E／D，I／D作成），S／O－B／L作成に要したタイプ要員，データ収集要員は月間1人200件の能力であったが，30%の処理能力増とみれば12,000件／月で60名を要したのが18名減員できる。月間540万円の節約である。1シップメントでは450円の船積（船卸）事務作業費の節減ができる。

沿岸荷役等下払いが直営費用に対し，下まわるような制度と料金体系が制定されれば，現業人員の節減は進むが，本システムはソフト面以外にビジネスの仕組みにも手をつけていかなければ効果は少ない。また申告税関別の派遣要員も同一の通関システムにのせれば，減員させられる。

C 検　数

本船派遣の現業員は1ハッチに件数が多い場合は2～3名ついている。平均で1.5名が実績であり，ドキメンテーションの軽減が本システムで図られるので，1.2名に減員でき，1船1名は減員できる。1船30万円の節減，月間30万円×64隻＝1920万円の節約，このほか，チェック・ブック（ソート・ブック）作成要員2名減，月間60万円節減。

D 検　定

月間の採算基準は1人600件＝3,000トンとなっており，入庫検量

方式は電算化とともに普及しているが，大黒埠頭の場合，チェック・ポイントをいくつにするかにより，検量人の減員は制約される。１人当たりの能率はあると予想され，チェック・ポイントの通過貨物量が多くなれば，検量技術の機械化が進めうる。データの入力担当者は大黒埠頭だけとすれば６名必要であり，入庫検量データは大黒埠頭に限ることは難しいので，現行要員の減員はできない。海貨側の検量人派遣費用は，減少させることはできるであろう。

E　作　業　会　社

沿岸は貨物の取扱量が高くなれば，作業能率は高くなり，駐在作業員当たりの生産性が高まる。船内は一定作業量が確保できれば，料金完全収受ができる。

はしけ運送は，船側の滞船が少なくなり，安全の確保と運航能率が図られる作業情報は艀の共同配船を可能にする。経営の安定に寄与する。

6.7　結　　論

6.6で検討した結論をつぎに港湾，荷主，船社がいかに本システムのメリットを享受し，費用を負担しありかをまとめて述べておくことにしたい。

まず，港湾内部での収支をとりあげる。

(1)　エゼント

輸出関連で本システムで負担する費用　　４１４万円

１シップメント当たり４６０円増×月9,０００件＝４１４万円

輸入関連で本システムで負担する費用　　１３８万円

１シップメント当たり４６０円増×月3,０００件＝１３８万円

本システム費用計　　４１４万円＋１３８万円＝５５２万円

これに対し，１バース当たり減員３名×３０万円×８バース＝７２０万円節減

差額　　７２０万円(△)－５５２万円＝１６８万円(△)

トン当たり　１６８万円÷３３.３万トン／月間扱い量＝５円５銭減

(2) 海　　貨

輸出関連システムで節減できる額　　９５４万円／月

１シップメント1,０６０円（△）×9,０００件＝９５４万円

輸入関連で本システム節減できる額　　１５９万円／月

１シップメント５３０円×3,０００件＝１５９万円

節減総額　　９５４万円＋１５９万円＝1,１１３万円／月

１トン当たり　　1,１１３万円÷３３.3万トン＝３３円４２銭減

(3) 検　　数

１船当たり１名節減（３０万円）×８隻×８バース＝1,９２０万円／月

トン当たり　1,９２０万円÷３３.３万トン＝５７円６６銭減

(4) 検　　量

予想輸出検量対象量　　３３万3,０００トン×６０％＝１９９,８００トン

現行予想検量人数　１９９,８００トン÷3,０００トン＝６７名
9,０００件÷６００件＝15名　いずれか大なる方67名

本システム適用　　６７名×３０％減員＝２０名

２０名×３０万円＝６００万円／月

トン当たり　　６００万円÷１９９,８００トン＝３０円3銭減

港湾内部　計　　１２６円８８銭 節減

エゼント　　５円　５銭

海　　貨　　３３円４２銭

検　　数　　５７円６６銭

検　　量　　３０円　３銭

荷　主

① 輸出平均トン数　　１９９,８００トン÷9,０００件＝２２.2トン

１シップメント当たりＢ／Ｌあげ金利負担減　　3,９８０円

１トン当たり　　3,９８０円÷２２.2トン＝１７９円３２銭 減

② 特殊料金設定による港運料金減額　１トン当たり　１００円 減

③　保管期間短縮による保管料節減

1トン当たり　６１円７０銭減

荷主節減額　トン当たり　３４１円２銭

船　社

①　１船当たり手仕舞要員費用節減　　４万3,２００円

４３,２００円×６４隻＝2,７６４,８００円／月

１トン当り　2,764,800円÷１９９,８００トン＝１３８円３８銭減

②　ターミナル費用節減　トン当たり　５０円減

船社節減額　トン当たり　１８８円３８銭減

総　　計　　トン当たり　　６５６円２８銭減

港　湾　　１２６円８８銭　　１９.３３％

荷　主　　３４１円　２銭　　５１.９６％

船　社　　１８８円３８銭　　２８.７０％

トン当り収支表

現行費用節減額			
港　湾	１２６円８８銭	システム費用	１６６円
エゼント	５円　５銭		
海　貨	３３円４２銭		
検　数	５７円６６銭		
検　量	３０円　３銭		
荷　主	３４１円　２銭		
船　社	１８８円３８銭	差引利益	４９０円２８銭
	６５６円２８銭		６５６円２８銭

（註）　エゼントが本システムでは，事務処理費用の現行額との比較で，節減されずに，反って費用負担増の現象を呈するのは，

① ターミナル・オペレーションの実情は作業管理と現場連絡業務に重点がおかれ，自らドキュメンテーションを行う業務処理が海貨に比べ少ない。

② エゼントのドキュメンテーションは，検数によって補われている。

エゼントと検数の業務内容が重層している（委託されている）ことによる。

③ 検数の高能率は，エゼントの業務処理に直接能率向上となって反映する。

以上の実態があり，エゼントは運送責任を担保することによって，ターミナル経営の基礎が与えられている。こうして，システム面では，メリットは直接あらわな形では出てこないで，作業収入等の面で能率の良否に比例してメリットがあがってくる。

本システムが生み出すメリットは金額に換算して，新たに

月　　４９０円２８銭×３３３０００トン＝１６,３２６,３２４円

年　　１６３２.６万円×１２ヵ月＝１億９,５９１.０２万円

を　出するものと予想される。

第 4 部

国連欧州経済委員会(ECE)の活動

第1章　ECEとCOTISの交流の経過

昭和47年10月に開催された国連欧州経済委員会（ECE）貿易手続簡易化部会第3回ADP とコーデング専門家会議へCOTISより水野専門委員長他11名を派遣して以来，毎年ECE会議へ出席し，交流を図ってきた。

この間ECE会議においては，商品，国名，通貨，船名等多くのコードについて検討が行われるとともに，ワンラン・メソッドの研究，メッセージ交換におけるINTERFACE 問題等，多くの調査研究を行ってきており，1974年にはECEにおける検討をもとに，アルファベット2桁国名コードがISOより発表された。

COTIS は，ECEにおいて採り上げられている貿易メッセージの構成様式であるINTERFACEについて研究を進め，ここにおいて，貿易メッセージ伝達エラー問題をとりあげた。

ここでの研究の成果を"Problems of Errors in Data Transmission"（ECE/TRADE/WP. 4/GE.1/R.56）としてとりまとめ，昭和50年6月度の会議へ発表した。

第2章　セキュリティ問題への展開

COTIS ではその後も続行してエラー問題を採り上げ，研究を行ってきたが，貿易情報システムの実現のためには，コンピュータを中心としたネットワークにおけるセキュリティの問題が重要であるとして，コンピュータの物理的保護，アクセス・コントロール，要員の問題等セキュリティにおける重要な問題を指摘するとともに，国際的な場において論ずべきテーマに言及した。そして，データ・ファイルへ権利のないものがアクセスするのをコントロールするアクセス・コントロールとデータの有効利用と迅速な処理を可能にするデータベース・ストラクチュアの問題とを国際的に提案すべきであると提案した。

1976年6月においては，米国CODASYL 標準を中心にアクセス・コン

トロールの方法について解説したレポートを提出した。このレポートは，データベース内におけるデータをいかに保護するかについて，具体的に例をもって説明している。

それまでのレポートにおいては，コンピュータを利用した国際的ネットワークによる貿易データ交換の実現は，現在の各の貿易情報システム化の状況に照して，かなり迫ってきていること，そこにおける貿易データのセキュリティ対策が非常に重要であることについて，ＥＣＥのＡＤＰとコーディング専門家会議のメンバーに訴え，認識を深めることに主眼があった。

１９７６年１１月の会合においては，日本より"Scope of Work for Security Problem"として，セキュリティ問題の今後の取組方法として，具体的にＡＤＰシステムの問題，通信の問題，人の問題等を設定して，調査研究の方法を提示した。（第５部資料編1. Scope of Work for Security Problems ）

その後もＣＯＴＩＳではセキュリティ問題の検討を進め，ＣＯＴＩＳ委員会でのセキュリティ問題に関する認識を深めること，及び一般の理解を深めるため，貿易情報システムにおけるセキュリティ用語解説を作成した。（資料2.コンピュータ・セキュリティに関する用語）

また，この問題に関する海外文献を調査して，セキュリティ文献リストを作成するとともに，文献を収集した。（資料3.情報処理セキュリティ関係文献リスト）

米国においては情報処理に関するセキュリティ対策の研究が進んでおり，米国商務省の標準局が作成したコンピュータ・セキュリティのガイドライン（ＦＩＰＳ 文書 ４１号）等を翻訳して，参考のため掲載した。（資料編4.自動データ処理における物理的セキュリティ及び危険管理のためのガイドライン，5. プライバシー法（１９７４年）の施行に係るコンピュータ・セキュリティ・ガイドライン）

第 5 部

資　料　編

1. Sope of Work for Security Problems

I. Introduction

While much of the international exchange of messages related to trade today is being carried out by teleprinter, it is anticipated that with increased use of automatic data processing and data transmission systems in the future, large volumes of information will come to be transmitted with greater speed in the form of accumulated data. Improved transmission efficiency will be bring about rapid progress in the exchange of international trade information.

While Automatic Data Processing (ADP) systems which include international data communications facilities will provide us with many amenities, if the use of ADP systems should spread haphazard and unsystematically, it could result in occurrences of intentional or accidental breakdowns and, consequently, a state of confusion. For the sake of the maintenance of security, therefore, it is imperative that a special study be conducted regarding this matter.

II. Importance of Security Problems

In order to illustrate the importance of security problems, we can describe them in terms of an analogy.

Today, the automobile is an essential means of transportation in our daily life. In order that we can all drive on public roads in safety, we have instituted various regulations.

By issuing driver's licenses, we permit only those who have certain qualifications to drive. With regard to the manufacture and maintenance of automobiles, we have stipulated safety standards to prevent people from driving vehicles in

dangerous condition. We have adopted traffic laws which require drivers to observe the various traffic signals and signs. Those who violate these rules are subject to police action.

If the number of cars was very low or if driving were to take place solely on private property, it would not be necessary to institute regulations or prosecute offenders.

When computers are being used similarly within a given business enterprise or within a given business group, security-related problems should probably be resolved internally by the individual organization.

But when we consider the case of trade data exchange via telecommunication circuits by ADP systems used by shippers, forwarding agents, carriers of many countries for sending international messages, security measures become a major task for the purpose of safeguarding the security of individuals and businesses.

Much of information transmitted across national boundaries must be kept confidential and is of such nature that transmission errors would have grave consequences. In order to make ADP systems for this type of information feasible, therefore, it is necessary to give adequate consideration to measures for guaranteeing the integrity and the confidentiality of the information.

In this connection, one may cite the example, the system of Society for Worldwide Interbank Financial Telecommunications (SWIFT), a data exchange system, designed with ample consideration devoted to security measures, which is to go into actual operation shortly. This system has many features of interest to us.

In the world of trade, it is expected that progress in

the use of ADP systems will be accompanied by an essential need for the establishment of a multi-faceted international trade information system covering such areas as commercial transaction information and information regarding transportation of goods. The need to devise adequate measures in the area of security problems is thus likely to become even greater.

III. Background of Work for Security Problems

Having had security problems on the agenda since June of last year, we have discussed the following items. As far as security measures are concerned, however, we have not yet begun discussing in concrete terms such security-related matters as concepts, regulations and modes. In view of the fact that the use of ADP systems in the area of trade information is spreading faster than we had expected, we should set out the work to undertake concrete projects for the purpose of, among other things, providing a guideline for those installing such systems.

June, 1975: Regarding transmission errors in message exchange through INTERFACE, we divided the problem into the two areas of commercial practices and system procedures and made a proposal regarding method of investigation on the latter.
Reference: TRADE/WP.4/GE.1/R 56 Problems of Errors in Data Transmission

September, 1975: On security problems in transmission and data processing of international trade messages using communications facilities and computers, we made a proposal and gave a description regarding the importance of the matter and the scope within which a study should be conducted.

Reference: TRADE/WP.4/GE.1/R 66 Security Problems

June, 1976: In connection with access control of data base as proposed in TRADE/WP.4/GE.1/R 66 (Security Problems), we described an example based on CODASYL standards.

Reference: TRADE/WP.4/GE.1/R 74 Security Problems

IV. Aspects to be Considered in Study of Security Problems

A study conducted under international collaboration on security problems in the use of ADP systems in international trade should be advanced by taking the following aspects into consideration.

(1) International trade is conducted with the participation of countries all over the world, and the number of businesses and individuals involved in trading operations is vast. Some ADP systems in the international trade are already in use and are expected to continue to expand in the future.
In view of this situation, it is necessary to undertake a study aimed at standards and unified concepts which will integrate on a long term basis the points of view of different countries regarding security problems in the use of international data transmission and ADP systems.

(2) Depending on the subject of study, it will be necessary to implement research projects in collaboration with the task teams, i.e. TT 1.1 (Data Element and Codes), TT 1.2 (Interface), TT 2.2 (Legal Problems), etc.. Also, it would be desirable to conduct

exchange of information with such international agencies as International Organization for Standardization (ISO), International Chamber of Commerce (ICC) and International Telecommunication Union (ITU).

(3) Since security problems cover a wide area, it is necessary to define the scope of study, determine the subjects to be studied and establish their priority in the order of their importance so that the study can be conducted efficiently.

(4) Since security problems relating to trade information span international boundaries and involve a large number of people, it would seem that such items as problems during data transmission, problems associated with ADP systems, problems of the personnel concerned, the authentication of messages and the security level of the data element are particularly important.

V. Scope of Work for Security Problems

1. With regard to security problems in the processing of trade information by ADP systems including international data communications, a specific study should be conducted from such aspects as commercial practice, technology and personnel in order to establish an approach aimed at the formulation of unified interpretations and countermeasures by the different nations involved.

2. Security problems shall be considered in terms of the problems of telecommunications (e.g. encipher, error check), ADP systems (e.g. database access control, systems auditing), personnel requirements (e.g. qualification of operators,

registration of accessors) authentication of transmitted messages and security level of data element (e.g. security level among special parties, security level of common data elements) in order to define subjects of the study and to clarify the nature of the study; at the same time, the findings from research implemented by other organizations should be clarified and background materials relevant to the trade information processing inventried and studied.

3. Medium- or long-term schedules shall be formulated for such specific subjects of research. The followings may be incorporated in the work programs which should be implemented as the first step.

(1) Survey of security measures being impremented by SWIFT as a concrete example.

(2) Survey of the attitude and measures toward security problems being taken by such international agencies as ICC, ITU and ISO.

(3) Establishment of terminology relating to security consideration.

Appendix: Security in Automatic Data Processing System

1. Motives of infiltration into systems

(1) Access to file and data base for the purpose of reading, modifying or erasing the information

(2) Unlawful use primarily to get financial gains, such as free use of hardware and software leased on fee basis

(3) Sabotage against systems for social and political reasons

(4) Other motives such as detection of system know-how and amusement

2. Forms of infiltration into information systems

(1) Infiltration due to accidental mishap: Hardware breakdowns, faulty maintenance of software

(2) Intentional infiltration: Infiltration into systems through normal procedures (pretending as a regular user or abusing one's authority), infiltration into system through means other than normal procedures (taking advantage of hardware or software defects, unlawful attachment of special equipment to circuits), abuse by system operator, etc. Aquisition of printer output, ribbons, etc., capturing of magnetic flux from communication circuit.

3. Vulnerability of systems

The reason for the occurrence of the types of infiltration listed in Section 1 lies in the existence of weaknesses within the particular systems. These weaknesses may be classified into the following three

categories:

(1) Infiltration into hardware
Terminals, circuits, communications control devices, CPU, channels, storages, other peripheral devices

(2) Unlawful use of software
Operating System (O/S), command systems, library programs, maintenance programs

(3) Infiltration by personnel
Operators, maintenance engineers, system programmers, management personnel

4. Security and security measures

4-1. Condiseration to security and security measures

(1) Method for protection of information from being read by those who have no right to know

(2) Method for preventing information and systems from destraction

(3) Method for protecting information/system from accidental mishaps and human error

(4) Method for recovering information/systems

(5) Maintenance security measures for computer system environment from physical and mechanical aspects as well as management aspect

(6) Legal protection of personal information

4-2. Various countermeasures against infiltration

(1) Control and identification of users and terminals

* User number and password, magnetic card, key, physical description (e.g. fingerprint)

* Changeability of password
* Identification of computer from terminals, identification of terminals (automatic response)

(2) Information access control
* Control of access mode (read, write, update, execute, etc.)
* Management of access control information (capability list, access control list)

(3) Audit trail
Monitoring and recording of such items as rejected calls, use of password, calls to special files, long-time access, command assignment patterns, etc.

(4) Encipher of information
Safeguarding of information on circuit and in data base (especially removable media) by means of enciphering

(5) Improvement of safeguarding capability for software
Improvement of safeguarding capability with respect to system programs, command programs, program language level, etc.

(6) Protection of information from statistical deciphering and other methods

5. Problems concerning security measures

5-1. Problems with usual password control modes
* Simple dependence on reliability of access control built in the O/S
* Over concentration of information on passwords system into the hands of small number of personnels
* Potential danger of lakage of password list

5-2. Problems with O/S in use

* Defects in program design
* Function for identifying program callers and called program
* Lack of guarantee with respect to correctness/ completeness

5-3. Problems with enciphering

Consideration is necessary to adopt a enciphering system which corresponds with the data structure in the file. Enciphering of messages on telecommunication circuits is different in nature from enciphering of information within the ADP system (e.g. data base), so it is necessary to adopt a coding mode which can be adapted to both coding schemes taking these inherent difference into consideration.

Scope of Work for Security Problems邦文

I　はじめに

現在，国際貿易において，国際間のメッセージ交換の多くは teleprinter exchange により行なわれているが，今後 autmatic data processing system の利用が進み多量な情報がより高速に，また伝送効率を高めるために集積して伝送されるようになり，貿易情報の交換が急速に進展するものと予想される。

国際データ通信を含んだＡＤＰ system は，国際貿易の分野において多くのメリットをわれわれに与えてくれるが，個別に無秩序にＡＤＰシステムが利用されるようになると，貿易メッセージやデータに対し故意または偶発的な事故が起り，混乱を招く恐れがあり，security保護の面から特別に考慮を行なう必要がある。

Ⅱ　security問題の重要性

我々はsecurity　問題の重要性を理解するためにaralagicalな例により解説を試みる。

現在，自動車はわれわれの生活に必要不可欠のものとなっており，公道をお互いに自動車を安全に運転するためにわれわれはいくつかのルールを定めている。

運転免許証を発行して一定の資格を有している人にのみに運転することを認めている。自動車の製造・整備に対して安全規準を設け危険な車では運転しないようにしている。道路交通法により各種の信号機や標識を遵守するようにしている等々である。そして，これらのルールを違反する者を警察官が取締っている。

貿易分野においても貿易情報の交換，ＡＤＰシステムのオペレーション等自動車の安全対策と同じように，セキュリティ対策について何らかの処置が

必要となる。

コンピュータを個々の企業とか特定の企業グループ内でのみ利用しているときにはセキュリティ問題は，個々の問題として解決を計るべきであろう。

しかし，コンピュータを通信回線を介して多数で共同利用するとき，特に国際貿易の分野において，各国のmaker shipper, forwarder, carrier, 銀行等が国際的に相互にメッセージ伝送，データ処理を行なうＡＤＰシステムを考えてみると，自動車の安全対策に対応するものとして，セキュリティ対策が個人や企業の安全を守るための重要な課題となる。

国際的に伝送される情報の多くは，機密性を要するもの，内容が誤って伝えられたときの影響が非常に大きいものであり，この種のＡＤＰシステムを実用化するためには情報のインテグリティおよび機密保持の対策を十分検討しなければならない。

例えば国際的なデータ交換システムとして，Society for Worldwide Interbank Financial Telecommunications（SWIFT）system が計画されセキュリティ対策が十分に配慮されており，近々実稼動に入るが，我々の研究に参考になる点が多い。

貿易業界におけるＡＤＰシステム利用の進展にともない貿易取引情報や貿易物資輸送情報に関する多面的な国際貿易情報システムの形成が必須のものと予想されるが，より一層security問題について十分な対策を講じなければならないであろう。

Ⅲ　経緯およびタスクチーム作業

我々は，昨年６月よりsecurity問題を議題に採り上げ下記に掲げるテーマについて討議してきた。しかし，security対策について具体的にsecurity 問題の考え方，ルール，方式等の検討を未だ着手していない。貿易情報分野へのＡＤＰシステムの利用は，我々が考えるよりも早く進んでいるので，systemの設置者に対してsecurity対策の方向付を示すことからも具

体的な作業に着手することを提案する。

１９７５年６月：INTERFACE によるメッセージ交換におけるエラーメッセージの問題についてCommercial Practice とSystem Procedure に分け後者について調査方法を提案した。

資料　TRADE／WP．４／GE．１／R56 problems of errors in data transmission

１９７５年９月：通信設備とコンピュータを利用した国際貿易メッセージの伝送及びデータ処理におけるセキュリティ問題についてその重要性と検討すべき範囲について提案解説した。

資料　TRADE／WP４／GE．１／R66 Security problems

１９７６年６月：TRADE／WP．４／GE．１／R．６６ で提案したaccess control におけるprivacy locksについてCODASYL の標準にもとづいた事例を解説した。

資料　TRADE／WP４／GE．１／R．７４ Supplementary masterial for TRADE／WP４／GE．１／R．６６

Ⅳ　セキュリティ問題研究にあたっての視点

国際貿易におけるＡＤＰシステムの利用におけるsecurity問題について国際的な協力のもとに行なう研究は，次の視点に立って進める必要がある。

(1)　国際貿易には世界の国々が関与し，また貿易業務に携わる企業や人々が多数である。また国際貿易分野へのＡＤＰシステムの利用が既に進んでおり今後とも増加していくものと予想される。

このためＡＤＰシステム利用におけるセキュリティ問題について，長期的見通しに立って各国の意見を総合した統一的な考え方，標準化　早急に

研究する必要がある。

(2) 研究すべきテーマによっては，既存のタスクチーム，TT 1.1 data element and Codes, TT 1.2 interface, TT2.2 legal problems 等と協力して研究作業を行なう必要がある。また，ＩＳＯ，ＩＣＣ，ＩＴＵ等の国際機関とも情報交換を行うこととしたい。

(3) セキュリティ問題は広範囲にわたるので，研究範囲を見究めるとともに検討すべきテーマを明確にし，その採り上げる順序の優先度を定めて効率的な研究を行う必要がある。

(4) 貿易情報におけるセキュリティ問題は国際的にまたがること，関係者が多数であることなどから，通信途上の問題，ＡＤＰシステムにおける問題，関係する人の問題，メッセージのオーセンティケーション，データエレメントのセキュリティ・レベル等が重要と思われる。

V Scope of Works for Security Problems

1. 国際的データ通信を含むＡＤＰシステムによる貿易情報の処理におけるセキュリティ問題について，Commercial Practice，技術，人などの局面から専門的に研究を行い，この問題に関して国際間で統一的な見解及び対応策を作成する。

2. セキュリティ問題を通信ＡＤＰシステム，要員，伝達されたメッセージのオーセンティケーション，データエレメント等の問題としてとらえ，さらに具体的な研究テーマ，研究内容等を明確にするとともに，他の機関で実施された研究成果を調査し，貿易分野からの観点から整理研究する。

3. 具体化された研究テーマに基づき，中期的あるいは長期的スケジュールを作成する。

直ちに着手すべき作業プログラムとしては，次のようなものが挙げられる。

(1) security の task team における研究内容を明確にするため，SWIFT システムで行なわれているセキュリティ問題について事例研究を行なう。

(2) ＩＣＣ，ＩＴＵ，ＩＳＯ等他の国際機関でとりあげられているセキュリティ問題の取組み状況について調査する。

(3) Security問題に使われている用語の整理と定義付を行なう。

Appendix　　ADPにおけるセキュリティ

1　システムに対する侵入の動機

(1)　情報の読出し，改変，消去を目的としたファイル及びデータ・ベースへの接近

(2)　ハードウェア，有償ソフトウェアの無料使用といった金銭的利益を主目的とした不正使用

(3)　社会的，政治的な動機によるシステムのサボタージュ

(4)　その他，システムのノウハウ探知，遊戯的な動機によるもの

2　情報システムに対する侵入の形態

(1)　偶然の事故による侵入，ハードウェア上の故障・ソフトウェア上の不備による偶発的侵入

(2)　故意の侵入；正規の手続きによるシステムへの侵入（正規ユーザーとしての擬装，職権の乱用），正規の手続きによらないシステムへの侵入（ハード又はソフト・ウェア上の欠陥の利用，回線への特殊機器の不正接続），システム・オペレータによる不正使用等

　プリンタ出力，リボン等の取得，回線上における漏洩電磁エネルギーの捕促等

3　システムの弱点

第1節にかかげた侵入を許す原因はそのシステム内に弱点が存在するからで，それはハード・ウェア，ソフト・ウェアおよび人的問題の3領域に分けて考えることができる。

(1)　ハードウェアの侵入

　端末，回線，通信制御装置，ＣＰＵ，チャネル，記憶装置，周辺装置

(2)　ソフトウェアの不正使用

O／S，コマンドシステム，ユティリティ群，保守プログラム

(3) 要員による侵入

オペレータ，保守技術者，システムプログラム，管理者

4 Securityとその対策

4－1 対策の考え方

(1) 知る権利のない者に情報を知られないための方法

(2) 権利のない者に情報／システムを破壊されないための方法

(3) 偶然の事故，人間のミスから情報／システムの破壊を守る方法

(4) 破壊された情報／システムを回復する方法

(5) コンピュータ・システム環境の物理的／機械的並びに管理面からの安全維持対策

(6) 法による個人的情報の法護

4－2 システム侵入に対する諸対策

(1) 利用者及び端末の監理と識別

- 利用者番号とパスワード，磁気カード又は鍵，身体的特徴の抽出
- パスワードの管理，更新（磁気カード，reader/writer. etc ）
- 端末より計算機に対する識別，端末自体の識別（ automatic response ）

(2) 情報の呼出し管理（ access control ）

- 呼出しモード（ read, write, update, execute, etc ）の制御
- 呼出し制御情報（ capability list, access control list ）の管理

(3) 呼出しの記録（ audit trail ）

呼出拒否の記録，パスワードの使用，特定ファイルの呼出し，長時間アクセス，コマンド指定パターン等の監視と記録

(4) 情報の暗号化

回線上，およびデータ・ベース内（特にremovable mediaの情報暗号化による保護

(5) ソフト・ウェアにおける保護能力の強化

システム・プログラム，コマンドプログラム，プログラム言語レベル等に対する保護能力の強化

(6) 統計的処理等による情報解読からの秘匿

5 セキュリティ対策における諸問題

5－1 通常パスワード管理方式のもつ問題点

- O／Sが持つ呼出し管理方式の信頼性に直接依存
- システム管理者に全てのパスワードに関する知識が集中
- パスワード表の部外漏洩による被害の大きさ。

5－2 現用O／Sにおける諸問題（Security対策面）

- プログラム設計の不備
- program caller とcaller program subjectを明確（Identify）にする機能
- correctness／completenessの保証の欠如

5－3 暗号化に関する諸問題

ファイル上のデータ構造との対応を考慮した暗号化方式の採用が必要である。

通信回線上のメッセージにおける暗号化とADPシステム内部（i.e. database）における暗号化はその性質が異っており，この性質の相異を考慮しつつ，両局面に融和する暗号方式の採用が必要である。

2. コンピュータ・セキュリティに関する用語

（１） Access：ADPシステムのリソースに対する接近，データの記憶または検索，対話あるいは使用に必要とされる能力および手段。

（２） Access category: ＡＤＰシステムのリソースまたはリソースの集合に対する利用の権限が与えられている各ユーザー，プログラムまたはプロセスに対して割り当てられる分類。

（３） Access control：ADPシステムのリソースに対するアクセスを，正当と認められたユーザー，プログラム，処理およびコンピュータ・ネットワーク内における他のＡＤＰシステムなどにのみ制限する手続き（Controlled accessも同じ）。

（４） Accountability（責任体制）：ＡＤＰシステムの機密を侵害したり，故意に侵害しようとする原因となった者を追跡調査することができるような特性あるいは状態。

（５） Administrative security（管理的機密保護）：影響の大きいデータに対して，許容できるレベルでの保護を行うために設定された管理上の強制，運用手続き，責任規定および追加的な管理。

（６） ADP system security(ADPシステム機密保護）：組織の資産および個人のプライバシーの保護を確実にするために，ハードウェア，ソフトウェア，データに対して設定され適用される技術的保護対策および管理手続きのすべて。

（７） Audit(監査）：システムの管理が適切に行われているかを調べ設定された方針や操作手順が守られているか，また，管理，方針ならびに手順を変更する勧告を行うために，システムの記録および活動状況をそれぞれにレビューし，かつ検査すること。

（８） Audit trail：トランザクションの開始時点から最終結果の出力まで

の過程における各事象をとりまく，あるいは導いたりする周囲の状況や活動の系列に再現し，評価し，検証することができるようにシステムの活動を時系列的に記録したもの。

(9) Authentication（確認）：

① 特定の範疇に属する情報にアクセスしようとしている発信ステーション，発信者あるいは個人が，適切な資格を持っているかどうかを識別あるいは検査する行為。

② 伝送，メッセージ，発信者などに関する合法性の尺度を設定することによって，不正な伝送を防ぐように設計された手段。

(10) Authenticator：

① 情報の特別な範疇に対しアクセスする部局，開始者又は個人の適格性を確認または立証するための手段。

② メッセージや伝送のオーセンティケーションのために，決まった方法で通常は決まった位置に入れられる一つの記号あるいは一連の記号やビット。

(11) Authorization（許可）：ユーザー，プログラム，処理などに対してアクセスの権利を与えること。

(12) Certification：特定のコンピュータ・システムのネットワーク設計およびその施行があらかじめ設定（予定）された一連の機密保護要件を満す範囲を確立するための認定手続きの一部または支援としてなされる技術的評価。

(13) Cipher system（暗号システム）：固定長の平文エレメントに暗号術が適用されている暗号術的システム。

(14) Cyphertext（暗号文）：暗号方式（Cypher system）を使用して生成された解読できない本文（Text）または信号。

(15) Code system：

① コミュニケーション・システムにおいて，可変長の平文のテキストを一群のシンボルで表わすようにしたシステム。

② 最も広い意味では，情報の伝達あるいは暗号化（例えばコード化された話法，モールス符号，テレタイプ・コード）に適した形に変換する手段。

③ 語，句，文章などの集合からなるテキストを，文字，数字，あるいはその両方からなる無意味な組合せに置換するための暗号化対応〔通常コード・グループと呼ばれる〕をもつ暗号化システム。

(16) Communications security：通信の取得からもたらされる情報の価値を権限のない人から守るための防御手段を適用し，真実性を保証する保護。

(17) Compromise（譲歩，妥協）：Sensitive informationの不当な暴露又は漏洩。

(18) Confidentiality：機密扱いのデータに適用され，かつ法人のみならず個人のデータについて適用しなければならない保護の状態と程度を述べるための概念。

(19) Cost-risk analysis：ＡＤＰシステムのデータ盗難や滅失の潜在的危険に対し，データ保護を行った場合と，そうでない場合とのコストのアセスメント。

(20) Cryptography（暗号法）：平文を解読できないように表現したり，暗号化されたメッセージを理解できるような形式に変換するための取扱い原則，手段方法の技法又は科学。

(21) Data base：情報処理システムのためのデータの集合であって，データの種類，量，構造およびその検索方法が多くの目的に適合するよう統一的に設計されたデータ・ファイル群のこと。

(22) Data contamination（データ汚染）：オリジナル・データの保全性に変化をきたすような故意または過失による処理あるいは行為。

(23) Data integrit（データ保全性）：コンピュータで処理されたデータが，原始書類と同じであること，およびそれが偶然または悪意の変更あるいは破壊にさらされていない状態。

(24) Data security（データ保護）：データの故意または事故による変更，破壊あるいは暴露を防ぐこと。

(25) Decipher（暗号解読）：適切なキーを用いて暗号化〔Encrypted, Encoded, Enciphered〕されたテキストを等価の平文テキストに変換すること。

(26) Decode：コード化の逆方向の操作，コード解読。

(27) Decrypt ：＝Decipher

(28) Emanation security（放射保護）：電磁放射の傍受と分析によって引き出される情報の価値を不当な人に与えないように設計された全ての手段による保護。

(29) Encipher：暗号化

(30) Encode：平文をコード・システムに従う形式に変換すること。

(31) Encrypt ：平文を暗号（encrypt ）システムを用いて解読できない形式に変換すること。

(32) Error check：ＡＤＰシステムによって処理，伝送されるデータの誤りを検査し発見すること。

(33) External security audlt（外部保護監査）監査される側とは独立の組織によって行われる保護監査。

(34) File protection：ファイルの不当なアクセス，汚染又は消去を禁ずるためにＡＤＰシステムに設計され，組み込まれた全ての処理及び手続きの総体。

(35) Identification（識別）：通常，コンピュータで読み出せる個有の名前を利用してユーザーあるいはリソースがあらかじめＡＤＰシステムに登録されたものと同一であることを認識できるプロセス。

(36) Integrity（保全性）：データの真正である状態を保つこと。

(37) Internal security audit（内部保護監査）：監査すべき組織を管理する責任を有する人物による保護監査。

(38) Key：暗号術において，暗号化と暗号解読の実行を行うための一連の記号。

(39) Lock-and-key protection system：各アクセス要求に対してキーやパスワードをつき合せる保護システム。

(40) Logical security：コンピュータおよび関連機器へのアクセスを制御するためにソフトウェア技術を利用すること。

(41) Operating system：入出力装置，中央演算装置，主記憶装置などを効率的にコントロールするとともに，言語処理プログラム，各種サービス・プログラムなどを機能的に採用して，コンピュータのパフォーマンスを全体的に管理する基本的システム。

(42) Password（パスワード）：保護された語または文字の列で，ユーザー，特定のリソース，アクセスのタイプなどを識別〔Identify〕あるいは確認〔Authenticate〕するためのもの。

(43) Penetration（侵害）：ＡＤＰシステムに対して，無許可のアクセスに成功すること。

(44) Personnel security（従事者保護）：何らかの影響の大きい情報に対してアクセスするすべての人が，適切な認可を得ていることを保証するために設定された手続き。

(45) Physical security（物理的保護）：

① コンピュータおよび関連機器へのアクセスを制御するため

の，鍵，見張り，バッジおよびそれに類似した管理的手段の使用。

② コンピュータ，その関連機器，およびそれらの内容などが収納された構造物を，偶然による破損，火災，環境上の危険から守るために必要とされる手段。

(46) Privacy(プライバシー)：

① 個人に関する情報をどれだけ他に与えるかについて，本人が自分自身で決定できるような個人の権利。そのような情報は，他の個人あるいは組織の間に無許可で流布されると，名誉の毀損を生じることがありうる。

② 個人および組織〔いずれも複数形〕がもつ情報あるいは個人および組織に関する情報の収集，貯蔵，配布を制御する権利。

(47) Privacy protection(プライバシー保護)：データ保護およびデータの機密性を確実にするため，また，保護および機密性を，予期しうる脅威あるいは危険〔情報を保持する個人に対して，事実上，損害，困惑，不便，不公正を与える結果になるおそれがあるもの〕から守るため，適切な管理的，技術的，物理的安全対策を確立すること。

(48) Procedural security (手続的保護)：administrative security(管理的保護)と同義語。

(49) Procedures：手続き

(50) Protection：保護

(51) Resource：ＡＤＰシステムにおいて，ユーザーやプログラムに割当てられる機能，機器又はデータの集合。

(52) Risk analysis(リスク分析)：システムの実体とその脆弱性についてある事象がある確率で発生し，推定される損失を明らかに

するために分析すること。

(53) Security（機密保護）

(54) Security audit（保護監査）：データ保護の手順および手段が，設定された方針のもとで妥当であるか，また，柔軟性があるかを評価するために行う監査。

(55) Sensitive Information：ある程度の保護が必要であり，一般使用にはすべきでない情報。

(56) System integrity（システム保全性）：ＡＤＰシステムが，すべての条件下で，オペレーティング・システムの論理的正確性と信頼性，およびデータの保全性に立脚していることを完全に保証する状態が存在すること。

(57) Terminal identification：ＡＤＰシステムにより，端末機の一意的認定を確証するための手段。

(58) Test key：ユーザー，メッセージ，プログラム等が正当なものであるかをアイデンティファイまたはテストするために組み込まれた暗号。

(59) Validation：セキュリティの仕様及び必要条件との合致を決するテスト及び評価における成績。

(60) Verification ：ＡＤＰシステムにおけるユーザー，プログラム，処理などが正当なものであることの証明。

(61) Wiretapping（盗聴）：ニセのメッセージまたは制御信号を発生したり，正規のユーザーの通信を変更したりして，データにアクセスするために無許可の機器例えば端末装置を通信回線に接続すること。

3. 情報処理セキュリティ関係文献リスト

- A Framework for Computer Security (Revised Edition). System Development Corp, Jun 75, 158p
- A Study of Computer Based Data Security Techniques. Naval Postgraduate School, Jul. 73, 77p
- Access control models. G. J. Popek, Center for Resarch in computing Technology. Harvard University, Feb. '73
- AFIPS System Review Manual on Security, AFIPS 1974
- Analysis of Some Abstract Measures of Protection in Colorado Univ., May 74, 46p
- Computer and security; A comprehensive annotated bibliography, MIT, Jan. '74
- Computer Data Security. Naval Postgraduate School, Jun. 74, 39p
- Computer Security Technology Planning Study. Anderson (James PO) and Co., Oct. 72, 43p
- Computer Security Technology Reference Manual. TRW System Group, Nov. 75, 343p
- Concept of Operation for Handling I/O in a Secure Computer at the Air Force Data Services Center. Mitre Corp., Apr. 74, 40p
- Data Security and Data Processing; Volume 1, Introduction and Overview. IBM
- Data Security and Data Processing; Volume 2, Study Summary. IBM
- Data Security and Data Processing; Volume 3, Part 1, State of Illinois: Executive Overview. IBM
- Data Security and Data Processing; Volume 3, Part 2, Study Results: State of Illinois. IBM

- Data Security and Data Processing; Volume 4, Study Results: Massachusetts Institute of Technology. IBM

- Data Security and Data Processing; Volume 5 Study Results: TRW Systems, Inc. IBM

- Data Security and Data Processing; Volume 6, Evaluations and Installation Experiences: Resource Security System. IBM

- Data Management System Test Methods for Security and Restart/Recovery. System Development Corp, Mar. 74, 121p

- Design of a Secure Communications Processor; Central Processor. Mitre Corp., Jun 74, 98p

- Design of a security; kerner for the POP-11/45, Mitre Corp, Dec. '73

- Downgrading in a Secure Multilevel Computer System; The Formulary Concept. Mitre Corp, May 75, 63p

- Information theory and privacy in data banks, I.S. Reed, RAND Corp, Jan. '73

- Initial Structured Specifications for an Uncompromisable Computer Security System.
  Case Western Researve Univ., Jul. 75, 195p

- Languages for Specifying Protection Requirements in Data Base Systems, ... A Semantic Model.
  Ohio State Univ., Aug. 75, 248p

- Making Computers Keep Secrets.
  MIT, Feb. 74, 395p

- On Computational Security.
  Illinois Univ., Jan. 74, 102p

- On the evaluation of reliability and security measures in a computer network. Bennet P. Lientz, California University, Dec. '74

- Privacy Transformation for Data Bank Systems.
  Rand Corp., May 73, 51p

- Protection in Programmed Systems.
  Carnegie-Mellon Univ., Jun 73, 145p

- Removing the Dynamic Linker From the Security Kernel of a Computing Utility.
  MIT, Jun 74, 130p

- Research in micro-terminal development and network end-to-end error recovery, R.F. Bryan, California University, Feb. '75

- Secure Computer Systems; Mathematical Foundations.
  Mitre Corp., Nov. 73, 41p

- Secure Computer System; Unified Exposition and Multics Interpretation.
  Mitre Corp., Mar. 76, 131p

- Secure Computer System; Unified Exposition and Multics Interpretation.
  Mitre Corp., Jan. 76, 130p

- Secure Data Management System.
  System Development Corp., Nov. 75, 197p

- Secure On-Line Processing Technology.
  Mitre Corp., Aug. 74, 118p

- Security and Programming Languages, Research Inst., of National Defence, Apr. 74, 21p

- Security Analysis and Enhancements of Computer Operating Systems.
  California Univ., Apr. 76, 70p

- Security for Computer Systems. NCC PUBLICATIONS
  M.A.L. Farr BSC, Consultant
  B. Chadwick GRAD, Consultant
  K.K.Wong BSC, PhD, AFIMA, Senior Consultant

- The Architectural Design of a Secure Data Base Management System.
  Ohio State Univ., Nov. 75, 295p

° Guidelines for Automatic Data Processing Physical Security and Risk Management	Federal Information Processing Standards Publication (31)
° Glossary for Computer Systems Security	Federal Information Processing Standards Publication (39)
° Computer Security Guidelines for Implementing the Privacy Act of 1974	Federal Information Processing Standards Publication (41)
° Data Security and Data Processing Volume 1 Introduction and Overview	IBM
° Data Security and Data Processing Volume 2 Study Summary	IBM
° Data Security and Data Processing Volume 3 Part 1 State of Illinois: Executive Overview	IBM
° Data Security and Data Processing Volume 3 Part 2 Study Results: State of Illinois	IBM
° Data Security and Data Processing Volume 4 Study Results: Massachusetts Institute of Technology	IBM
° Data Security and Data Processing Volume 5 Study Results: TRW Systems, Inc.	IBM
° Data Security and Data Processing Volume 6 Evaluations and Installation Experiences: Resource Security System	IBM
° AFIPS Systemreview Manual on Security	AFIPS 1974

情報処理セキュリティ関係文献リスト（邦文）

- コンピュータのための機密保護と安全管理

  岡本行二著　オーム社　１９７４

- コンピュータ安全管理マニュアル

  W. F. ブラウン著　海外技術資料研究所　１９７２

- システム安全性工学入門

  W. P. ロジャーズ著　鹿島研究所出版会　１９７４

- コンピュータ犯罪

  堀内恭一著　日本工業新聞社　１９７４

- 計算機セキュリティ研究開発の動向

  日本電子工業振興協会セキュリティ専門委員会編　１９７６

- 機密管理マニュアル

  W. ウェイド著　商事法務研究会　１９６８

- 情報防衛マニュアル

  安川秋一郎著　文化社　１９６９

- セキュリティ

  米国情報処理学会システム改善委員会編　秀潤社　１９７７

4. 自動データ処理における物理的セキュリティおよび危険管理のためのガイドライン

目　　次

序　　言

米国商務省標準局（ＮＢＳ）の刊行する連邦政府情報処理の標準化に関する文書（ＦＩＰＳ：Federal Information Processing Standards）シリーズは，米国公法89-306号（ブルックス法）及び連邦法令コード第15主題第6部の規定に従い公布され，かつ実際に採用されている諸標準を対象とした公式文書である。これらの法制的・行政的規定は商務長官に，連邦政府機関におけるコンピュータの利用管理やＡＤＰ（Antomatic Data Processing）システムの導入を促進する重要な責任を付与している。この商務長官の責務を遂行するため，ＮＢＳは，その翼下にあるコンピュータ科学技術研究所を通じて，当該分野のガイドライン及び標準の開発に向けて関係省庁の作業を調整し，技術的指導を行なうとともに全体の主導権を握っている。

個人のプライバシー・データの機密保持並にコンピュータ・セキュリティのテーマは，関係分野の中でもとりわけ国家の安全と国民の利益に密接に結びついており，商務長官は，これらのテーマが含む技術的問題の解決に必要な努力を，商務省全体の活動とは区別して直轄事項であると決定した。

データの機密やコンピュータ・セキュリティの成否は，バランスのとれた管理・技術両面のセーフガードを採用することいかんにかかっている。セキュリティ保全の全体計画を考慮すると，ＮＢＳとしては，各連邦政府機関がこのＡＤＰ物理的セキュリティ及び危険管理のガイドラインを実施運用することを切に望むものである。

コンピュータ科学技術研究所所長

ルース・Ｍ・デービス

解　　説

ＦＩＰＳ文書31号－自動データ処理における物理的セキュリティ及び危険管理のためのガイドラインは，公法89－306号（79 Stat. 1127）として修正された大統領命令11717号（38FR. 12315，1973年5月11日）により施行された1949年の連邦財産管理法と，連邦法令コード（ＣＦＲ：Code of Federal Regulations.）第15主題第6部の規定に従い，標準局（ＮＢＳ）の手により発行されたものである。

標準名称　自動データ処理における物理的セキュリティ及び危険管理のためのガイドライン。

標準カテゴリー　ＡＤＰオペレーション，コンピュータ・セキュリティ。

解説　このガイドラインは，ＡＤＰ装置設備の物理的セキュリティと危険対策の諸計画を体系化しようとする政府機関の手引書として刊行されたものでその主要な取扱事項としては，**セキュリティ分析，自然災害，サポート施設，システムの信頼性，手続上の措置とその管理，オフ・サイト設備，偶発事故対策，安全意識，セキュリティ監査**等が挙げられる。またコンピュータ・データや装置類の物理的セキュリティにまつわる様々な統計結果や情報を併記し，更に専門的な特定主題に関連した刊行物一覧も掲載している。

はじめに

ＮＢＳコンピュータ科学技術研究所は，本文書の監修者として努力して戴いたSENTOR Security Group社のRobert V. Jacobson副社長及び，その執筆協力者のWilliam F. Brown博士（Ball State大学）とPeter S. Browne氏（General Electric社Information Systems部）に深く感謝の意を表したい。こうした執筆活動は同研究所のシステムズ＆ソフトウェア部門との契約のもとに実施された。

コンピュータ科学技術研究所はまた，ＮＢＳの安全性・火災防止部門とＮＢＳ火災防護局，並びに総合調達庁連邦資産保護管理局と連邦火災対策協議会の協力に対しても深く感謝するものである。これらの諸機関は，関連条項の吟味や修正の面で多大の尽力をしていただいた。

またＩＢＭ社の後援を受けて運営されているリサーチ・グループのAlfred M. Pfaff氏の協力も看過することは出来ない。同氏には図表を中心として草稿全体に目を通していただき，文章上の修正を含む様々な勧告を提示された。刊行に至る原稿の編集にはSusan K. Reed女史（システムズ・ソフトウェア部）の努力に負うところが大きい。

提　　言

本文書が提起している勧告の基本的なものは，この部分に要約されており，ガイドラインの対象分野を明示するとともに，ＡＤＰ施設における物理的なセキュリティ対策計画の策定・運用・維持に関わる活動項目の輪郭を総覧している。

Ⅰ　ＡＤＰ施設における物理的セキュリティ対策プランの組織化

ＡＤＰの物理的セキュリティに対する責任を明確化し，ＡＤＰセキュリティ計画立案を担当する作業チーム（タスク・フォース）を組織する。

リスクの事前評価を実施し，主要な問題領域の確定，暫定的な保安手段の選択を行なって当該領域の問題解決に供する。

Ⅱ　リスク分析の実行

ＡＤＰ施設及びＡＤＰユーザーが被る可能性のある被害の概要を推定する。その分析対象項目としては，

(1)　物的資産の物理的破壊及び盗難

(2)　データ及びプログラム・ファイルの逸損或は破壊

(3)　情報の盗難

(4)　間接資産の盗難

(5)　コンピュータ処理オペレーションの遅滞或は妨害

等が挙げられる。

五つの被害分野に分けたＡＤＰ施設に対する脅威及び影響の発生率を推定する。年間の被害推定額を算出するためには，被害領域と脅威の発生頻度の双方を合一して推定する。

年間被害推定額の総額を最少化するため，復旧手段の組合せを調整選択する。復旧手段には，

(1) 危険にさらす度合を低減するために環境を変化させる

(2) 脅威の影響を柔げるための手段をとる

(3) 管理手順を改善する

(4) 早期発見体制の完備

(5) 偶発事故対策

等が含まれる。

Ⅲ 局地的な自然災害の発生予測

ＡＤＰ施設の火災に対する安全性（敷地の位置，建物構造，収容能力，管理）を事前評価し，火災の発生検知と消火活動に備え，更に出来得るならば，よく訓練された消防組織を確立する。

内外からの水の侵入にさらされる危険性を評価し，建屋の出水保護対策を用意する。必要ならＡＤＰハードウェアの配置替え，配管ルートの再検討，出水防護設備（ポンプ，防水布等）の準備を行なう。またハリケーン，竜巻やその他の暴風害にさらされた場合を想定し風と水に対する建屋の抵抗力を評価する。

Ⅳ セキュリティ・プログラムの立案

復旧手段を選択的に導入するためのプラン及びスケジュールを策定する。指針と計画を盛り込んだ手引書を作成し常時維持する。その内容に含まれる事項としては，

(1) ＡＤＰにおける物理的セキュリティの対処指針

(2) セキュリティ対策上の指示手順

(3) システム設計，プログラミング，検査及び保守に関するセキュリティ・ガイドライン

(4) 偶発事故対策計画

(5) 安全意識教育の素材

(6) セキュリティ監査プログラム

等が挙げられる。

V　サポート施設の保護

過渡電流，低電圧状態，給電の中断等の数値及び継続時間を評価し，年間損耗額を推算する。電圧調節用変圧器，複式給電器，非中断型電源，自家発電装置並びにＡＤＰ用分離回路等の防護装置を採用する。所定の作業計画と局地的な年間温湿度推移を考慮して空調の失敗を予測し，空調故障の頻度と継続時間との推算を合一して，年間推定損耗値を推定評価する。必要な個所に対しては，装置を重複させて機能の信頼性を高め，外気の緊急使用の用意をし，平均修復時間を低減するためメインテナンス能力を増強する。

テレプロセシング回路故障から生じる年間平均損耗額を推算する。コスト的に無理がないなら，通信回線を重複させて信頼性を高め，中断時間を減少させるための復旧設備の増強をはかる。ソフトウェアは，通信の途絶から生じるエラーの影響を最小化するよう設計されねばならない。

ＡＤＰオペレーションが，水，天然ガス，電流，エレベーター或は郵便物コンベア等のサポート設備の故障で中断され得るか否かを裁定し，必要ならば，信頼性を向上させ平均修復所要時間を低減させる策を講じるべきである。

Ⅵ　コンピュータの信頼性の最適化

重大なハードウェア故障の発生頻度及び継続時間，並びにそのＡＤＰオペレーションに対する影響等を推定評価するため，故障分析を実施する。コスト枠が許すならば，周辺機器を増結したり，機器構成（コンフィギュレーション）を多重化したりしてシステムの信頼性を向上させる。またメインテナンス設備も再検討すべきだ。故障傾向を早急に割り出し予防保守手段を最適化するため，全てのハードウェアの故障を記録・分析する。

Ⅶ　物理的保護手段の提供

様々なＡＤＰ区画，つまりコンピュータ・ルーム，データ管理，変換区画，データ・ファイル蓄積区画，プログラマーの担当区画，書式蓄積区画，保守部門及び機械装置室等の位置・重要性を確定し，それに充分な物理的保護とアクセス・コントロールを施す。

また盗難，サボタージュ，スパイ行為，市民的抵抗及びその他の不自然な侵入等に対処するため，侵入攻撃探知システムの増強，扉や窓及びその他の開閉口に於ける物理的障壁の設置等で警戒措置を強化する。

機械的又は電子方式の施錠，人員物資の動向に対する保安要員や受付係による監視，管理手順の整備（出入記録，ＩＤカード又はバッジ，物品の通過・受領に関する書式），その他の管理規定等の手段により，重要区画やＡＤＰ施設へのアクセスをコントロールする。

Ⅷ　内部手続上のセキュリティ増強

ＡＤＰ作業のワーク・フロー及び性格を分析することによって，リソースに対する不正行為，盗難，誤用等が発生する可能性を推定する。損害を受ける危険性を最小化する手順を組み込む。このような手順には，

(1)　重要作業に携わる要員相互の協力を強め

(2)　点検・限界比較の回数を増やし

(3)　リスクの高いオペレーションに対する基準を定式化し

(4)　品質管理工程を分離する

等の方策が含まれる。

ＡＤＰマネジメント，システム・プログラミング，プログラム・ライブラリー管理，入出力コントロール，例外処理，アプリケーションズ・プログラミング，データ・ベース管理，品質管理，内部監査，ハードウェア保守等における重要なポジションを指定し，雇用前に適切な選択作業を実施する。

全てのＡＤＰ要員が内部管理に対する理解を高め，その要求に応じ得るよう訓練し監督する。

不正なプロセシングを排除するため，ジョブの開始，スケジューリング，出力の配分等の管理手順及び記録保管手順を定着させる。

データの保全を維持し，ストーレッジ媒体を保護し，データ・ファイルの保管状況を追跡し，更に不正使用を排絶するため，物理的データ・ファイルへのアクセスを制御する。手動並びに自動追跡監査手続が導入されるべきであろう。

データ・ファイルやプログラムの保管方式や手順を整備し，次のような要件を満足させねばならない。

(1) バックアップ・オペレーション

(2) 関係法令や規則との調和

(3) オペレーションの監査及びマネジメント

(4) オペレーションの統計分析

(5) データ保全問題の解決

等がそれに当る。

(1) 監査能力

(2) 自動合否判定テスト

(3) コントロール・プログラムの保守

(4) 入力データの品質管理

(5) システム及びプログラム

に関して個々人の知識に重きを置かないやり方等の要件を満たすプログラミング，テスティング，ドキュメンテーションの標準を運用すべきである。

Ⅸ 偶発事故対策計画

バックアップを必要とする非常事態の範囲を想定し，それらに適応する一連の支援計画を策定する。この様な偶発事故対策の目的は，ＡＤＰ施設ユーザーを受け入れ難い損害から守ることである。各々の緊急対策を対象とした性能仕

様，作業指示及び技術要件（システム・ハードウェア，ソフトウェア，プログラムとデータのファイルおよびプリプリンテッド・フォーム等）を文書化しておく。

ＡＤＰ関係外の緊急支援対策を立て，定期的に点検する。またセキュリティ計画の立案に参画する。

オフ・サイト施設の使用中や輸送中のソース・ドキュメント，入出力データ及びプログラムに対する防護策を講じる。

(1) バックアップ資材の予備を確実なオフ・サイト地点で保持し

(2) 適切なオフ・サイトＡＤＰ施設からも充分に利用出来る時間を確保し

(3) バックアップ要員を必要に応じ稼動させるため

これらの関連手順を確立する。

破壊後ＡＤＰ施設を再建するには，次の様な仕様を考慮して計画が立てられねばならない。

(1) フロアー・スペース（使用機能別の床面積，積載荷重率，位置）

(2) 隔壁，電源，空調，通信，セキュリティ，防火

(3) ＡＤＰハードウェア，事務機器，用品

生命の安全を保証し，損害を抑制し，ＡＤＰオペレーションの混乱を極小化し，更に復旧作業をはかどらせるため，火災や洪水及び市民の騒擾に対するＡＤＰ非常事態計画と「施設の自己保全プラン」の両者を有機的に総合する。

X 安全対策意識の向上発展

ＡＤＰスタッフ，上級管理者及び建築要員を対象とした安全訓練要綱を策定する。

適切な保安意識対策を選択・採用する。その中には，

(1) トレーニング講座やセミナー

(2) ポスター

(3) オリエンテーション案内書

(4) 被雇用者のセキュリティに対する責任感を高めるため職務分析記録を手直しする

(5) 局部的なセキュリティ上の出来事に対する広報活動

(6) セキュリティを損なう異常を未然に防止した従業員の表彰

などの手段がある。

懲罰規定の制定と広報も考慮に入れるべきであろう。

XI 物理的セキュリティの監査

当該機関の監査，建物警備，ＡＤＰ要員の代表とユーザー組織の代表を含め，内部的な監査チームを構成する。

全ての重要な保全手段及び非常措置を体系的に機能させる監査プランとスケジュールを立案する。

監査報告書で，如何なる措置の改良と差し替えが必要か明記すべきだ。各々の不備が早急に整備されるには，チェック・シート（問題分析記録，行動責任，フォローアップ）をまず用いること。

4.1 ＡＤＰセキュリティ分析

4.1.0 まえがき

自動データ処理（ＡＤＰ）を想定して**セキュリティ**という用語が使われる場合，この言葉はしばしば，悪意に満ちた暴露に対する防護，或はＡＤＰ施設に対する積極的な攻撃を防ぐ保護といった意味に理解される。だが，Webster辞典では，「secure」は，「故障したりあばかれる恐れのない；確実な；堅固な；安定している……」と定義されている。このような定義内容は，確かにＡＤＰ施設にとって望ましい特徴であり，本ハンドブックで取り上げているセキュリティを広義に解釈すれば，これらを含んでいると言えよう。またＡＤＰマネージャーや関係機関が，ＡＤＰセキュリティの物理的側面の要素を定義し，徹底した物理的セキュリティ計画を立案運用し，更にこうした計画の監査方式を確立する諸過程も考慮に入れられるべきであり，このガイドラインの設定趣旨にはこうした作業に助力を与えることも含まれている。ＡＤＰ施設のユーザーは，このハンドブックを利用して，当該設備全体のセキュリティ評価，セキュリティ・プランニングの能率的遂行，及び行き届いたバックアップ計画の立案等を行ない得る。また連邦政府機関のＡＤＰ施設は，その上部機関や外部のユーザーの使命を達成させるためにあり，従って，物理的セキュリティ・プログラムの目標は，こうした作業使命がおかされる状況を未然に防ぎ，ＡＤＰ施設を円滑に運用させるため，あらゆる適切な手段をとらせることに置かれている。

4.1.1 対象領域

ここで取扱う領域については，第１，２節で詳述するが，概括するとＡＤＰ施設に影響を与える物理現象や状況を扱っていると言える。アクセシビリティ（Accessibility）を制御する手段はこのハンドブックから除外されている。「制御されるアクセシビリティの項目一覧」〔46〕の中で，この手段は，データに対す

る不正なアクセスを防止するためとられるハードウェア及びソフトウェアの技術的利用手段として定義されている。またプライバシー及び機密は，データの性格やアクセスする有資格者に関する概念として規定されている。だがＡＤＰセキュリティの諸側面にキチッとした境界を設けることの困難さは，一様に理解されるべきであろう。一つの防護手段が所期の目標以上の成果をあげることもあろうし，特定の要件を効果的に処理するために複数の原則や機能が要求されることもあろう。だから，調査・プランニング段階では，テーマの全貌を常に視野に置くことが重要になる。

ＡＤＰセキュリティ・プランナーという用語の表現は，ここでは"ＡＤＰセキュリティ・プランニングに責任を負う人"という意味に使用され，非常に便宜的な用いられ方をしているが，ある一人にあらゆる分野の能力を期待して使用される訳ではない。つまり，各ポイントごとに，必要な専門知識の素が要求されることになる。ＡＤＰ施設の管理運営者は，セキュリティを現在進行中のオペレーショナルな機能として把握し，この機能をサポートするために十分な要員と予算を手当てするならば，本書から大概の必要事項を修得することが出来るだろう。

物理的セキュリティ計画の研究開発や運用に関して本書で示唆されている様々な手順を要約すると次のようになる。

- セキュリティ政策を展開させるため，その基礎作業としてリスクを分析する。
- 障害にさらされる危険度を低減するため適切なセキュリティ保護手段を選択運用する。
- バックアップ・オペレーション，災害復旧，緊急事態等を考慮した偶発事故対策を立案する。
- 作業要員に対し教育訓練を施す。
- 継続的なテスト及び監査を立案実施し，必要に応じてセキュリティ防護手段及び偶発事故対策を調整する。

4.1.2 ＡＤＰオペレーションに対する様々な脅威

このハンドブックは，ＡＤＰ資産や資本設備に対する諸脅威，通常の継続的オペレーションに対する物理的災害等を対象にしており，以下はその概要である。

まず，特定な場所や設備など内部の管理物に対する盗難，放火，破壊，干渉，妨害といった行為，あるいは，情報に対して誤った処理を行なわせるために人為的になされる，許可されない，いわゆる"**不正なアクセス**"（unauthorized access が挙げられる。この種のアクセスの管理を行なうためには，防壁，隔壁，施錠ドア等の物理的障壁，コントロール・ポイントにおけるガードマンや受付係，専用テレビや侵入検知器などの電子機器，地域規制や識別バッヂ等の管理手段が考えられる。

ＡＤＰハードウェアの障害を原因とするデータ処理オペレーションの中断を最少限に抑制する手段として，ハードウェア構成の重要部分にリダンダンシーを導入すること，予防的なメインテナンス，精密なモニタリング，ハードウェア故障の原因分析等が含まれる。

電源，空調設備，通信回線，エレベーター，郵便物コンベア等**サポート施設の障害**の防護的措置としては，重要エレメントへのリダンダンシーの導入，精密なモニタリング，外部からの干渉や自然災害に対する物理的保護，応急措置の用意等が含まれる。

洪水，暴風雨，火災，地震等の**自然災害**

ＡＤＰ収容建物の注意深い場所の選択，建築設計や構造の詳細な立案，緊急事態の発生に対処する手段の事前準備等に留意すべきである。

人為的なエラーの対策としては，要員訓練，監督，管理等の運用を効率化し人間のエラーを極小化する手段が講じられねばならない。

重要要員の配置に柔軟性を持たせる。すなわち，重要な位置を占めるキー要員には，クロストレーニングを施こし，緊急的の処理に幅を持たせる。

周辺の危険要素－化学処理設備や爆発物作業現場，空港，犯罪多発地域等への

近接一を充分想定し，サイトの選定，建物設計仕様の立案，ＡＤＰ施設からのこうした危険要因の除外，緊急対策等を考慮し保護手段を講じなければならない。

不正目的によるインプット，プログラムおよび**データ・ファイルへの干渉**は物理的なアクセス・コントロールに加えて，この種の行為を検出し防止する内部管理やその手順が用意されねばならない。

音響的または電磁的なＡＤＰハードウェアに対する**妨害行為**によるデータの不正処理への対抗手段には，妨害装置が設置される可能性のある場所からＡＤＰハードウェアを隔絶すること，ＡＤＰハードウェアやコンピュータ・ルームの遮蔽，電源線の被覆等が考えられる。（盗聴やその他のデータ通信回線への不正接続による妨害行為は，本書では取り扱わない。）

勿論すべてのＡＤＰ施設がこうした脅威にさらされているわけではない。個々の脅威のインパクトは，ＡＤＰ施設の地理的位置によることもあるし（地震），局地的環境（洪水），窃盗犯から見た資産やデータの潜在的価値（金額未記入署名入り小切手あるいは商品投機家に対する情報価値），活動家やデモ参加者或は破壊分子に対する当該機関の重要性によることもあるだろう。

4.1.3 リスク分析

過去の経験によると，リスクの量的分析が次のような効果をもたらすことを示している。

- セキュリティ計画の目標は，当該機関の使命と直結している。
- セキュリティ防護手段の選択の任にある人々は，各手段に充当されるべき適切な経費額をはじき出せる。
- 長期計画の担当者（プランナー）は，場所の選定，建築設計，ハードウェア構成，ハードウェアの調達，ソフトウェア・システム，内部管理等の作業項目にセキュリティ面の配慮を加味することが出来る。
- 偶発事故に対するバックアップ・オペレーション計画の立案と評価，自然災害や緊急事態に対処する復旧手段等の基準を設定することが可能となる。

・保護されるべきものは何か，セキュリティ計画の実施，検討，報告等には誰があたるのが適当か等を明示した確固たるセキュリティ政策が策定出来る。

こうした全ての理由から，ＡＤＰ施設のマネジメントはまずセキュリティ計画の展開でリスク分析から始めるべきだと言えよう。その手続や手順については以下の節で概要を述べてみたい。

4.1.3.1 損失の潜在評価

リスク分析の第一段階は，ＡＤＰ施設が被る可能性のある潜在的損失の推定評価である。この潜在的損失の評価が目的とするところは，ＡＤＰ施設のオペレーションの重要局面を確認し，推定損失額を算定することにある。損失が発生する状況は，非常に多くの場合が考えられる。

有形資産の物理的破壊または盗難－この場合の潜在的損失は，逸失資産を補充するコストや処理遅延によるユーザーへの被害となって現象する。

データまたはプログラム・ファイルの損失－これが逸失すると，バックアップ・コピーやソース・ドキュメントからファイルを再構成しなければならないし，ユーザーに処理遅延による被害が生じることは勿論である。

情報の窃盗－この潜在的損失を量化することは難しい。例えば収集され，編集され，更に公的に流布されている情報で市場活動に影響を与えているものについて考えてみれば良い。流布される以前ならば，この種の情報に関する知識は特定の商人に利益をもたらし，それを知らない他の商人達は，当の商人の利益に相当する損失を受けることになる。だが取扱機関はそれ自身直接の損害を被らないとしても，その事業上の使命で失敗したことになるのは明らかだ。場合によっては，情報自体が，専用権付きソフトウェア・パッケージや転売可能な名簿リストのように市場価値を持つことも考えられる。

資産の間接的窃盗－もしＡＤＰシステムが，現金，在庫品目，あるいはサービス行為の認定書のような他の資産をコントロールするため使用されているならば，このシステムはこれら資産の窃盗にも転用出来るはずで，この場合の潜在的損失

は窃盗された資産の額に相当し，損害額の上限は探知を確実とする額まで許容されることになる。

処理業務の遅延－恐らくどのようなアプリケーションであっても何らかの時間的制約を持っているだろうし，それ故時間通りに業務を遂行させるため生じる無理から，ある程度のロスをもたらすものと思われる。また潜在的な損失が比較的容易に算出される場合もあろう。例えば，支払小切手の即時処理の失策は，支払償還の実施に支障をきたし調達契約の円滑な履行を妨げるであろう。同様に，在庫管理システムの遅延は，倉庫要員の勤務時間を無駄にし，更に建築現場の労働者のような倉庫に貯蔵されている資材の受け取り手にも遊休時間帯を作り出すことになる。ところが，給料支払小切手の発行のように，その業務の遅延が直接的なロスとなって現れないような場合もある。業務の遅延が多少なりとも運用機関のオペレーションを中断される場合は，その機関の日常運用経費を，遅滞した処理業務コストの推定額として代用すれば良いだろう。

損失は一般に遅延時間の増加に比例して増大する。従って"損失を生じない"最大遅延時間と，全部が破壊されたＡＤＰ施設の再建に必要な時間の中間値を推定することが重要になってくる。損害が著しい場合の遅延損失の評価は，この2つの域内にある遅延時間ごとに推定されねばならない。損失の傾向を識別するには，一般的には３～４の代表的な時間帯を設定すれば充分である。

物理的な破壊損失の潜在評価は極めて簡単である。ＡＤＰセキュリティ・プランナーは，建築物の管理者や調達部門の助けを得て，ＡＤＰ施設の物的資産の補充コストの一覧表を作成することが出来る。この表には次のような項目が含まれる。

- 建築物の本体
- 空調設備，電源，給電設備，持ち上げ式の床などＡＤＰ施設をサポートとする特別な装置設備
- デコレーター（ decollator ），マイクロフィルム・プロセッサー，キーパンチ等のＡＤＰハードウェアやその他の特殊装置

・磁気テープ，ディスク・パック，諸書式，リボン等の消耗品

・机，椅子，ファイル・キャビネット，棚，タイプライター等の事務用品

こうした特定分野別に作成された表は，特に留意されるべき領域の識別にも貢献する。事務用品分野に含まれるもののコストは，1平方フィート当り5～10ドルだが，コンピュータ・ルームの内容物は1フィート当り500～2,000ドルに相当しよう。この試算額は，**第8.4節**で述べる災害の復旧計画で役立つはずである。

上述した潜在的損失の対象物の残る4つの部分は，ＡＤＰ施設が行なうデータ処理作業の性格に規定されるところ大である。ＡＤＰセキュリティ・プランナーは，各タスクごとに，それがどのような損失を蒙る可能性があるか，あるいは如何なる要因が損失の大きさに影響をもたらすか検討する必要がある。プランナーは，全ての損失ファクターを考慮することなど出来ないはずだから，これらの評価を実施する上でユーザーを訪問し協議することになろう。

時間を最も有効に使用するため，ＡＤＰセキュリティ・プランナーは，著しい潜在損失を内蔵しているタスクを識別すべくある種の事前選択作業を行なうことも出来る。例えば次に示すような予備調査表を構成することも可能である。

表１－１　潜在損失発見のための予備調査表

タスク名	ランタイム	ファイル再構成	重要データ	専用データ	管理資産データ	損失を生じぬ遅延時間
P	1.5時間／日	容易	無	有	現金	1日
Q	オンライン	非常に困難	無	無	無	2時間
R	2.5時間／日	困難	有	無	現金	8時間
S	2.0時間／週	Ｐファイル使用	無	無	無	1週間
T	0.5時間／日	非常に容易	有	無	在庫	4日

この例では，タスクＰは1日1時間半稼動し，再構成しやすいファイルを持っている。更に取扱いに注意を要するデータはないが専用データは保持しており，現金を管理している。また1日間の遅延ならば目立った損失コストが生じないの

が一目瞭然である。だが実地の場合ＡＤＰセキュリティ・プランナーは，もっと詳しい項目内容に配慮しなければならない。つまり，どのファイルが利用されているか，何故そのファイルの再構成が容易なのか或は困難なのか，どのデータが専用なのか，どの程度の現金が処理対象となっているのか……などである。

このような分析を経て後，はじめてプランナーは最初の結論を下すことが出来る。

表１－２　損失の発生

タスク	データの損失	情報の盗難	資産の盗難	処理の遅延度
Q	有	無	無	顕　著
R	有	有	有	並
P	無	有	有	並
T	無	有	有	軽　微
S	無	無	無	非常に軽微

このプランナーが表１－２でタスクの重要度をベースに配列替えしている点に注意されたい。タスクＱとＲは，強い関心と詳細に亘る評価を受けたはずだ。またタスクＳは潜在的損失が軽く，予備鑑定の確認を殆ど必要としないことになる。

重要なタスクを識別するための予備調査（スクリーニング）を終えた後，ＡＤＰセキュリティ・プランナーは，次に微妙なタスクやそれらが他の活動に与えるインパクトに精通しているユーザーの助けを借り，各々の潜在的損失程度をより正確に量化すべきだろう。彼はまた，万一の場合を想定して何如に支障が起こるか，どの程度の損失が生じるかについても考慮しなければならない。ある特定のタスクが不正の為使用されないことがあっても，その事実は将来の過失の皆無を保障するものではないからだ。リスク分析のこの段階では，プランナーは最悪の事態を常に想定すべきだ。その発生可能度の推定評価は後の段階ですることになっているので，この段階ではセキュリティ計画に組み込めるよう著しい損失をも

たらすもの全てを識別しておく必要がある。

4.1.3.2 ＡＤＰ施設に対する諸脅威の分析

リスク分析の第２段階は，ＡＤＰ施設に対する脅威の評価である。比較的重要な影響を持つ脅威やファクターについては既に第1.2節で述べた。これらの脅威の詳細については以下の章節で述べられており，その発生頻度に関する一般的情報も出来る限り収録した。ＡＤＰセキュリティ・プランナーは，各脅威の発生頻度を評価するに当って，こうしたデータと常識を大いに活用すべきだ。

全般的なリスク分析は勿論プランナーの手によらねばならないが，脅威の分析にはそれ以外の人々の貢献度も無視出来ない。そうした人々の助力も積極的に求められるべきだろう。次に列挙しているのは，諸脅威のリストとそれの各々の分析に当って助言を得られる機関である。

表１－３　脅威リスト

脅威名	情報源	参照項目
火災	建築火災消防主任及び各地域の消防署	2.1
洪水	陸軍工兵隊	2.2
地震	全国地震情報センター	2.3
暴風雨	海洋気象局及び各地の測候所	2.4
給電故障	建築技師及び地方の公共事業体	3.1
空調設備故障	建築技師及び空調設備機器メーカー	3.2
通信不良	Federal Telecommunications System（ＦＴＳ）及び建築会社，電話会社	3.3
ＡＤＰハードウェア故障	ハードウェア・メーカー及び連邦政府調達局	4.0
侵入，破壊，その他	建築物管理者，保安監督者及びＧＳＡ（総合調達本部）の保護サービス管理局	5.0

漏洩	ハードウェア・メーカー及びＧＳＡの保護サービス管理局	5.2
内部的な窃盗・誤用	システム設計，内部監査及び人事の各部門	6.0

4.1.3.3 年間損失推定

リスク分析の第３段階は，潜在的損失額の推定と損失発生の可能度を結合して，年間損失の程度を推定することである。その目的はセキュリティ手段の選択基準に必要で重大な脅威を抽出し，各脅威に支出されるべき経費を決定する尺度を策定することにある。換言すれば，ある特定のセキュリティ手段のコストを，保護が与えられる対象である損失と関連づけることと言えよう。

年間損失推定額を算出するためには，脅威と潜在的損失のマトリクスを構成すべきである。その各交差で，所定の脅威が一定の損害を生じるかどうか確かめる。例えば，火災，洪水及びサボタージュは，情報盗難による被害を引き起こさないが，程度の差こそあれ，この３要因は，物理的破壊損失や処理遅延による損害をもたらすというような決定を下すことが出来る。同様に，内部の干渉も間接的な資産盗難を引き起こす。著しい損害が生じる場合は，潜在的損失額にその脅威の発生予測度を掛けて年間損失推定額を算出する。

損害予測の一例として次に示すのは，処理業務の完了時に遅延に帰因するロスが生じた３種のＡＤＰタスクを採り上げたもので，判り易いよう状況を簡素化している。

表１－４　遅延継続時間とその損失額の予測例

タスク	１時間	４時間	８時間	１　日
A	—	—	10,000ドル	45,000ドル
B	—	5,000ドル	12,000 〃	55,000 〃
C	3,000ドル	16,000 〃	45,000 〃	160,000 〃
総　計	3,000 〃	21,000 〃	67,000 〃	260,000 〃

更に，給電故障に帰因する各遅延継続時間の年間発生頻度を，各々 0.75，0.31，0.01および0.09と推算した場合を想定してみよう。停電による年間損失推定額は次の計算から，3万8,860ドル／年となる。

0.75×3,000ドル＋0.31×21,000ドル＋
0.10×67,000ドル＋0.09×260,000ドル＝
38,860ドル／年

停電の損害コスト計算は，発生率やオペレーションに対する影響がかなり正確に量化出来るので，比較的推定しやすい。空調設備や通信回線の故障の場合もこのクラスに入るだろう。だが火災の損害を量化するのはまた別の問題となる。表1－5に示すように，被害程度の等級や様々な損害タイプを考慮して処理しなければならないからである。発生頻度は，第2.1節で示す固有の火災に対する安全性から割り出されるものであるし，損害額は，第1.3.1項で示した潜在的損失の評価にまたねばならない。このような手続手法は，地震，洪水，暴風雨，その他の自然災害にも採用することが出来る。

表1－5　火災による損害額の推定の例

		火災種別		
		ADP区域の小火災	建物の大火災	全焼
発生頻度		0.10	0.05	.0005
潜在的損失のタイプ	建物被害	$10,000	$100,000	$3,700,000
	ADPハードウェア	50,000	10,000	2,100,000
	一般装置	5,000	—	285,000
	備品その他	10,000	—	130,000
	タスクDの遅延	—	—	35,000
	タスクEの遅延	5,000	7,000	100,000
	タスクFの遅延	12,000	20,000	250,000
	ファイル再構成	5,000	—	85,000
潜在的損失総額		97,000	137,000	6,685,000
年間損失額		$ 9,700	$ 6,850	$ 3,342

人間の行為を推定するのは一層難しい。というのは，発生頻度を予測する簡単な方法が全くないからである。しかしながら，許容し得る確度でその潜在的損失を予測し，重大な脅威を抽出評価することは出来よう。例えばプログラムの改ざんによる詐欺行為を考えてみよう。資金の支払いを扱うタスクを検討して次のような事柄が判ったとする。

タスク	1周期当りの金額	予想されるプログラム変更（次の12ケ月）
J	20,000,000ドル	5
K	200,000ドル	25
L	5,000,000ドル	10

もし1％の窃盗が明らかに検知出来，横領犯人が10回の変更中1度以上の悪質なプログラム変更を行なっていないと仮定すると，次のような結論が導き出されるだろう。

タスク	窃盗可能額	不正頻度	損失推定額
J	200,000ドル	0.5	100,000ドル
K	2,000 〃	2.5	5,000 〃
L	50,000 〃	1.0	50,000 〃
			155,000ドル

このような結論は一見ありそうにもないように思える。恐らく前提条件が妥当なものでないからであろう。判断要因はこうした結論に到達するまでに重要な役割をはたす。この種の試みを繰り返すうちに，判断の方法が純化されてくるだろう。分析作業を反復すれば，タスクJの年間損害額は10,000ドルかあるいはKの場合の2倍近くになるだろう。また，タスクLの場合，Kのそれと等しい額で大体5,000ドル程となろう。そしてこれら3タスクの年間損害推定額は，合せて僅か20,000ドル位までに修正されるに至るだろう。

この作業のキーポイントは，推定評価を試みる中で重大な外部への流出が一層鮮明になり，かつ合理的な基準が浮かび上って来ることだろう。最後の段階では，タスクKがタスクJと同等に重要であることが判明している。というのは，例え

周期ごとの取扱額の100分の1を支払うものであったとしても，プログラムは依然として流動的な状態にあり，犯行を受けやすいことには変りないからである。計量化作業が続けられた後では，各々の脅威の発生率やＡＤＰ施設へのその影響はより実際的に検討出来る。

こうした手法が科学的と呼べないことは明白だ。損失推定額が一応信頼出来る結果を示すまでには，最初に最も重大であると認識された分野に集中して，脅威や損失の再評価を繰り返す必要があろう。ある場合には，概算推定値以上のものを入手することは難しいかも知れないが，こうしたリスクに対する原則的な処理思考は，物事を量的に判断しようとする努力に多大の恩恵を与えることだろう。

4.1.3.4 救済手段の選択

年間損失額の推定作業が終了すると，ＡＤＰ管理者は，影響力の大きい脅威とＡＤＰ面の重要なタスクについてその概要を知ることが出来よう。この種の脅威に対する反応として次のようなパターンが現れてこよう。

まず，発生頻度を低減させるための**環境の変更**が考えられ，極端な場合，脅威を受けにくい他の地域への移転という形を取ることもある。ＡＤＰ施設内部或はそれに隣接した障害発生要因を，どこか他所へ移すことも考慮されるだろう。

次に脅威から**防護する障壁の設置**も検討され，これらは，自然災害，サボタージュ，破壊行為から建物を守り強化する改良作業という形をとるだろう。電源の信頼性を高めるため特殊な装置が導入されることもあろう。また重要地域へのアクセスをコントロールするため，特殊なドアー・ロック，ガードマン，侵入探知装置等の方策も講じられよう。

さらに管理上のギャップを埋め合せる**手順の改善**を画り，オペレーション面の管理強化，雇用前のスクリーニングの徹底，プログラミング及びソフトウェア・テストの標準策定などの方策が考えられる。

早期検知も重要な問題で危機的状況を早期に発見すれば当然損害を最小限に抑えられる。火災報知機や侵入探知器の設置を万全にする必要がある。

そして，**偶発事故に対する計画を**策定しておけば，被害があった後の当該機関の業務が円滑に進められる。プランに含まれるものとしては，人的，物的資産を保護し損害を抑制するための非常事態への即時的対応措置，外部のバックアップ・オペレーションに必要な計画や資材の準備，ＡＤＰ施設の損害や破壊に対処出来る復旧計画の立案等があげられる。

特定の救済措置を選択するにはその基準として，救済措置の年間コストが予想される年間損害額の低減幅より少ないものであること，それらの諸措置の組み合せが最低のトータル・コストとなることが考慮されねばならない。

この最初の基準は，セキュリティ計画の適正コストを念頭に置いたもので，当該救済手段が必要とする年間経費は，ＡＤＰ施設に期待出来る年間削減利得より少ないものでなければならない。このような視点は自明のことのように見えるが，ＡＤＰマネージャーの中には，リスク分析することなしにセキュリティ手段を要求する者が多い。経験に基づく判断が彼に，ある特定の行為だけが望ましいと言わせるわけだが，こうした直感が大手を振って歩けばリスク分析など必要でなくなる。真に重要なのは，重大なしかし計量化されていない潜在的損失がどの程度のものであるか認識することである。ＡＤＰマネージャーは彼の判断を仔細に分解検討してリスクの量的分析に資することが望ましいだろう。

また第２の基準は，ある特定の救済措置が複数の脅威対象に対して有効である場合がある事実を反映している。その相関を図示すると次のようになるだろう。

表１－６　脅威に対する救済措置の関連

救済手段	脅威種別				
	火災	内部盗難	外部盗難	ハリケーン	サボタージュ
火災検知システム	X				X
損害制御チーム	X			X	X
移動警備パトロール	X	X	X		X
侵入探知器		X	X		X
要員スクリーニング		X			
自家発電設備				X	X
バックアップ計画	X			X	X

ある特定の救済措置が1種類以上の脅威に有効な場合があるので，諸措置のどのようなコスト組み合せが最低となるか即断出来ない。最近コスト・ミックスを選別する可能な方法としては，まず年間損失推定額が最大の脅威から検討し始めてもよいだろう。その状況に適当と思われる救済手段を想定し，次にそれらの年間コストが，期待し得る年間損害額の削減幅より少ないものをリストアップする。（この時点では必ずしも正確なコスト及び損害削減の推定評価を必要としない。）もし2種類以上の措置が同一分野で損害の低減をもたらすなら，それらを全部リストアップするがリダンダンシーには特に注意すべきである。この過程を次いで重大な脅威グループにも適用し，ある脅威を対象とする措置でコスト的に不適当なものが出て来るまで続ける。ある救済手段のコストが増加した時，もしこれが他の脅威をカバーするために拡大されたものであるなら，そのコスト増は特に留意されねばならない。この時点で，個々の脅威と救済措置のマトリクスを作成し，損害削減額とコストを推定し更に純節減額の推定を行なう。表にして示すと次のようになる。

表1－7　損害のコスト分析

救済措置	脅威											
	A			B			C			D		
J	20*	9	11	10	0	10	4	1	3	2	5	−3
K	20*	15	5	12	0	12	6	0	6	4	2	2

＊同一効果

この表では，各脅威ごとに，損害削減推定額，救済手段コスト，純損害減少額がこの順序で示されている。脅威Aに対し9,000ドルをかけて救済措置Jを適用することにより，2万ドルの損害削減が期待出来るわけだ（純節減額は1万1,000ドル）。更に救済措置Jは，脅威Bの損害を追加投資なしで1万ドル削減し，脅威Cに対しては僅か1,000ドルの追加投資で4,000ドルの損害額減少を期待出来る。だが最後の脅威Dに対して救済措置Jを適用すれば，節減額より経費の方が

上回るので，JはDに対して不適当と言わざるを得ない。Jの措置から得られる純損害減少額は次の式で表わすことが出来る。

$$J(A, B\&C) = 11 + 10 + 3$$
$$= 24,000ドル$$

この表からすると，JとKは脅威Aに対して同じ削減効果を持っていることになる。Kのコストは J より多い故，却下されるだろう。しかしながら，

$$K(A, B, C\&D) = 5 + 12 + 6 + 2$$
$$= 25,000ドル$$

更に，
$$J(A, B\&C) + K(A, B, C\&D)$$
$$= -4 + 22 + 9 + 2$$
$$= 29,000ドル$$

となる。

従って，JとKが脅威Aに対して同様な効果をもたらす一方，Kの方がJより他の脅威については有効に見えるが，より詳細にチェックするとこの両者の併用が最大の純損害減少額を生み出すことが判る。

上述したプロセスを辿りコストと損害削減額を予備的に推定評価することによって，ADPセキュリティ・プランナーは，様々な救済手段の組み合せをテスト出来る。こうした作業を経て，最も効果的と考えられる救済措置のサブセットを把握出来る。ADPプランナーはこの時点で，候補となるサブセットの評価結果を再検討し，仮選択の信頼度を確定するため必要に応じてそれらを手直しすべきである。限界状況においては，最適サブセットにも変更が余儀なくされることもあるはずで，この過程を何度か繰返せば，ADPセキュリティ・プランナーは，信頼度の高い救済措置の組み合せを勧告し得る地点に到達出来るだろう。また，コスト的に正当化し得ない救済手段を自信を持って却下する能力も重要な意味を持っている。

これまで述べた全ての手順が完了すれば，以下の事項が確定され文書化されているはずである。

・重大な脅威とその発生する可能性
・各脅威を対象とした重要な作業とその年間ベースの損害推定額
・最大の純損害削減額を生み出す救済手段とそれらの年間コストのリスト

このような情報を手にしてこそＡＤＰ管理者は，容易に物理的セキュリティ計画の推進に踏み出すことが出来るのだ。救済手段の分析で最大のインパクトを持つ手段が確認されれば，採用を想定した相対的なプライオリティを決定することも出来る。

4.1.4 セキュリティ計画の採用

前節 1.3 ではリスク分析の応用についてＡＤＰセキュリティ計画の立案という観点から述べた。セキュリティ計画の採用は，地域的な条件や時間，予算両面の実際的な制約に左右されるだろうが，必ずしもどこから着手すべきかという面での順序はない。一般的に応用される手順を概説すれば次の様になる。

・**予備的なプランニング**。ＡＤＰセキュリティ研究チームを結成し，予算，スケジュール，責任分担の指定の３つの面に関する作業要綱を中心としたセキュリティ計画草案を作成する。
・**主要な問題分野を判定する**ため予備的なリスク分析を実施する。
・緊急に必要なセキュリティ措置を**状況に応じて**選択実施する。
・**詳細なリスク分析**を行ない，再検討および関係者からの承認に供するためその結果を文書化する。
・承認されたリスク分析の結果を基にしてコストの適正配分と**活動計画の文書化**を行なう。この計画には，セキュリティ手段の予算とスケジュール，偶発事故対策，要員訓練計画，テスト・監査プラン等が包摂される。
・承認を受けた**活動計画の実行**。
・テスト結果，監査，環境の変化等を考慮しつつ，少くとも年１回の定期的なサイクルで**詳細なリスク分析とその予後の措置を繰り返す**。

この活動計画には，充分なドキュメンテーションが必要であり，その内容とし

ては次の文書が含まれねばならない。

- 一般的なガイダンスを与え責任の所在を明文化したセキュリティ施策説明書
- セキュリティ計画とその手順，ＡＤＰ要員，ユーザー及びサポート要員の各々の責務について述べたセキュリティ・ハンドブック
- セキュリティの目標を投影したシステム設計，プログラミング，テスティング及び保守のための技術標準
- バックアップ・オペレーション，災害復旧，応急措置等を対象とする偶発事故対策
- セキュリティ計画の一環としてのＡＤＰスタッフ教育手引書

これらの文書は，関係ＡＤＰ施設の通常業務の性格によって，全く別扱いにされることもあろうし，他の文書の一部として含まれることもあろう。一例を示すと，ＡＤＰ施設向けの非常事態対策プランは，当該機関の施設自衛計画に含まれるだろうし，同じく技術的なセキュリティ標準は，現行ドキュメントに追加することも出来る。

最後に付け加えなければならないのは，セキュリティ計画の継続的監査と再点検の重要性である。当初のリスク分析に充分な注意が払われねばならないことは勿論であるが，それが完了してからは，定期点検と更新が素速く処理される必要がある。機関の役割，地域的環境，ハードウェア構成，処理業務等に変化があればそれを評価した上で，ＡＤＰセキュリティ・プランナーは，セキュリティ計画を円滑裡に推進し続けるため如何なる変更を加えるべきか決定することになるだろう。

4.1.5 サポート書類

ＡＤＰセキュリティに関連した連邦政府文書の中には，セキュリティ・プランナーに役立つものが沢山ある。これらは，他の有益な参考文献とともに本書末尾に添付された付録の書誌目録にリストアップしてある。この関係文書が内蔵する広範な知識のたくわえを利用するためには，プランナーは各々の作業領分において早期に本リストを参考にすべきである。

4.2 自然災害の予測

4.2.0 まえがき

本章に取り上げられているのは，火災，洪水，暴風雨，地震である。これらの事象はすべてＡＤＰオペレーションに対し同様な影響をもたらす傾向にある。つまり施設やその内容物の物理的破壊，通常オペレーションの中断といった形で発生する。更にこれらの災害は，ＡＤＰ要員の生命にも当然脅威を及ぼす。以下の章節では，自衛手段と災害にさらされる状態に対する評価要因について述べる。非常事態への対応計画は第８章で偶発事故対策計画として触れることにする。

4.2.1 火災に対する安全性

過去20年間の経験は，ＡＤＰ施設が火災による打撃にもろく，オペレーションに混乱が生じやすいことを教えている。例えば，100万ドルのコンピュータ・システムを収容している部品倉庫が火災で完全に崩壊してしまった事例がある。この建物は敷地面積0.8平方マイル（２ヘクタール）の大きさで，不燃構造を持っていたが，スプリンクラー，防火隔壁，仕切り等の設備は全くなかった。更に，課税率が低いという理由からだろうが，この建物位置は市の防火対策地域の外になっていたのだ。火事は，床の密閉剤を除去するために使われていた可燃溶剤に電気のスパークが引火して起った。構造物，内容物並びにコンピュータ・システム等は完全に破壊されたけれども，この会社の緊急対策の一環として磁気テープの保管を地下室と定めていたので，テープ類は殆ど被害を受けなかった。ハードウェア・メーカー側の努力で，新しいコンピュータ・システムが火災後４日目にして代替地で稼動し始めたが，このエピソードは，火災に対する安全性と偶発事故対策の双方が重要なことを明示している。こうした重大な被害を受けた事例の中には，不燃建築も多く含まれている。重要なテープが防護されておりコンピュータ・ハードウェアも比較的簡単なものの場合，その復旧も早く日単位で元に戻

ることもある。だが，大規模な構成のシステムが破壊されたり，バックアップ・レコードが不充分な場合，何週間或は何ケ月にも亘る修復期間が必要となろう。

火災対策はＡＤＰ施設の物理的セキュリティ計画の中心的課題とすべきものであり，考慮すべき要素には次のものが含まれる。

- 火災被害にあう可能性を最小限に抑えるためＡＤＰ施設の位置，設計，構造，メインテナンスに留意する。
- 火災の早期発見及び発生後の応急対策を確実にする手段を用意する。
- 十分な消火手段と素速い要員配置を図る
- 被害をおさえ復旧を早めるための手段と人員の準備を行なう

これらの各ポイントについては以下の節で述べることにする。防火対策を包括的にとりあつかったものに「防火ハンドブック」〔24〕がある。この書自身から引用すると，「内容は火災及びその管理に関する権威ある百科辞典であり，防火科学を習得する人々にとっての教科書とそれ自体独自の参考資料という二面的性格を兼ね備えている」このハンドブックは，建築設計や構造に関する防火対策，数百の資材を対象とした火災危険要素の一覧表を所載しており，また水力エンジニアリングの手引書ともなっている。

4.2.1.1 ＡＤＰ施設の火事被災

ＡＤＰ施設の火災に対する安全性を評価する際第一に考慮すべき要因は，ＡＤＰ施設と近接建築物の性格からどのような火災形態が生起するかである。一般的には，一定区画の危険度は，可燃性材料の量，引火しやすい程度，発火点となり得る可能性等にかかっている。また次の様な要件が特に危険を内包しているものと考えられる。工事中の建築物，布や繊維類の加工物，化学薬品やプラスチック及び塗料，石油等の加工処理，電気装置アセンブリー，鋳物類，紙製品，保管・倉庫業務等である。これらの要素に内在する危険度は，内容物の燃焼熱量（燃料負荷）の関数で火災の激しさとして測定することが出来る。この関係を表示すると次の表２－１のようになる。

表２－１　燃焼物の潜在熱量及び火災時の燃焼程度の対比

燃焼物荷重（１平方フィート当りの材木使用量（ポンド）に換算）	潜在熱量（１平方センチメートル当りのキロカロリー）	火災の激しさ（継続時間）
5	11	0.5
10	22	1
20	43	2
30	65	3
50	110	6
70	152	9

金属製家具と保管キャビネットを備えているオフィスを例にとると，その燃焼物荷重は，5～15ポンド／平方フィート（11～33キロカロリー／㎠）程度であろう。用紙類やパンチカードの保管室や磁気テープ・ライブラリーでは，この燃焼物荷重が50～80ポンド／平方フィート（110～175キロカロリー／㎠）となる。一方，火災の激しさや構造物内容物に支えるその影響度は，温度上昇率と被災時間による。その燃焼物荷重が発火や引火を妨げる構造になっていれば（金属ファイル・キャビネット内の紙テープやパンチカードのように），温度は比較的ゆっくり上昇するはずである。またもし磁気テープがオープン・ラックに貯蔵されているような燃焼物の荷重形態であれば，燃焼温度は急激に上昇するものと考えられるが，燃焼時間の方は案外短かいはずである。

火災に対する安全性の第２番目のファクターは，建築物の設計及び構造である構造の基本タイプは次の５種類に要約出来る。

- **耐火構造**－骨材，床，壁，屋根等の建築構造物が，不燃材料で構成されており火災による強度の減失を防ぐよう配置されている。
- **重量用材**－外壁が２時間は不燃性を保ち，柱，梁，床，屋根が太い木材を用いている。この種の重量用材は燃焼が遅いという特徴を持っているので，不燃材料よりよい実績を示すだろう。

・**不燃構造**－構造同体は不燃性であっても，構造材に加わる燃焼効果に対する防護に弱い面がある。つまり，不燃建築の火災は構造物自体からは燃料要素を供給されないが，火災による熱は構造物を崩壊させてしまう可能性がある。こうした不燃ビル火災の典型的な例にはミシガン州の送電施設火災があげられる。構造材自身は火災の直接的な燃焼材料を提供しなかったが，屋根上のアスファルトが燃え，建築物の全焼につながった。

・**通常の建築構造**－これは構造用材の寸法が重量用材よりずっと小さいという点を除けば，重い構造材を使った建築物と何ら変りはない。

・**木造建築**－これは，厚さ2インチ（5センチ）のフレームと1インチ（2.5センチ）の板を使った典型的な住居構造である。

上記した5タイプを要約し，耐火性を増す設計仕様をこの際無視すれば，以下の表のようにまとめられる。

表2－2　建築構造と火災の関係

建築構造タイプ	火災分類
耐火構造	2～3時間
重量用材	1時間余
不燃構造	1時間
通常建築	1時間以内
木造建築	分単位

建築物の実際的な強度は，その建築構造のタイプだけでなく，次の様な設計仕様にも左右される。

・建築物を火災に応じて分割してしまう**防火壁**

・建築物内部の延焼を防ぐ防火隔壁

・建築物内部の火と煙の蔓延を防ぐ目的で設置された**吹抜き，ダクトの調節弁やシャッター**，床と壁の接触部に設けられた防火材

・火災の延焼を止める**低燃焼材**を床や壁や天井へ用いること

火災に対する安全性を構成する4つの基本要因とその影響は，次表のように要約出来る。

表2－3　火災要員とその影響

要　　因	影　　響
位置状況	火災発生の可能性
燃焼物荷重	火災の激しさと時間
建築構造	構造物の損壊に対する抵抗力
構造の設計詳細	火災の延焼防止

ここまでの議論は，多分に簡略化されたものである。だが，ＡＤＰ施設のセキュリティに責を負うプランナーがこれらの要因を考慮するなら，防火対策に彼が払うべき関心の程度が判ろうというものである。プランナーはＡＤＰ施設の火災に対する安全性を評価しその危険度を判定する際には，有能な防火エンジニアの助力を必要とするはずだ。こうした点については，「建築火災安全基準」〔13〕の中で詳しく論じられよう。

ミズーリ州オーバーランドで1973年7月に起った米陸軍人事記録センターの火災については，他のリスクには必要以上の防護措置が検討されたのに対し，火災の安全性に対する充分テストを経た設計基準が無視されたために生起した不幸な実例である。スプリンクラーの不足，火災現場への進入経路が確保出来なかったこと，設計仕様の様々な欠陥等がからみ合って，消火活動は著しく阻害され，人事記録はスプリンクラーの散水による損害にとどまらず，甚大なダメジを受ける結果となった。

火災に対する安全性を考慮する上で第3のファクターとなるのは，建物の運用形態である。ある建物の安全性は，不注意な運営によって著しくその効果を減ずることを銘記すべきである。これに含まれる事例としては，支柱等で開け放しにされた防火扉，ごみやくずの著しい累積，可燃溶液や溶接機材，切断火口等の不用意な扱い，標準を無視した電気配線，オーブンやボイラーの不充分な安全管，

可燃材料の過度の集積があげられる。ＡＤＰ施設を考えると，カードや紙の取り扱いから糸くずや紙ぼこりが生じその累積から甚大な被害が生じることもある。ＡＤＰ物理的セキュリティ計画の策定に当っては，建物保守要員と協力して，この種の危険性を認識し除去することが考慮されねばならない。更にセキュリティ管理の責任分担にも常に意を配るべきだ。セキュリティ監査計画では，あらかじめ定められた基準に合致しているか否かのチェック作業も当然含まれる。

ＡＤＰ施設建設の特殊なガイダンスについては，「基本電気設備の防火」〔9〕第２章で述べられている。この文書（以下ＲＰ－１と略す）は，ＧＳＡオーダーＰＢＳ 5920.4Ｂの規定により若干の修正が加えられて全てのＧＳＡ施設に適用されている。

4.2.1.2 火災探知

ＡＤＰ施設の位置，設計，構造，運用等に深い注意を払ってもなお火災発生の可能性は存在する。過去の経験は，早期発見が被害を少なくする重要な要因となることを教えている。大体火災の進行は３段階にわけられる。絶縁不良を原因として引火が生じるとする。電気的な火災はしばしば長時間くすぶる。炎が発生すると，比較的ゆっくり炎は燃え移り周囲の温度を引き上げる。この段階の継続時間は，発火点近くにある可燃材料に左右される。そして遂に温度は，隣接した可燃物が燃えやすいガスを発散させる臨界点に達する。この段階になると火は急速に拡がり，直接的に燃え移るだけでなく，熱の放射で発火が起る。第３段階では高温と充満した煙・有毒ガスを特色とし，消火活動は極めて困難になる。

第３段階に至る前に火災を発見するには，気温上昇の探知だけに頼っていたのではどうしても限界がある。この理由からＲＰ－１は電気設備区画に煙探知器を備えるよう要求している。この種の探知装置は，燃焼に付随して空気中に放出される異常成分の存在を検知するため電気回路を使用している。

早期発見を効果的に行なうためには，火災探知システムの設計面で次のような点が考慮されねばならない。

・**探知器の位置と分散配置**は，空気の流れの方向と速度，澱んだ空気の位置，装置の設置場所と火災発生潜在地点の関係等を考慮すべきである。探知器は，天井だけでなく底上げした床下，吊り天井の上，空調ダクトの中等にも必要な場合がある。また電話装置や通信ケーブルの導管の内部にも設置した方が良いだろう。

・**探知制御卓の設計**は，警報を発している検知器の所在を容易に識別出来るものでなければならない。このことは，明確な地域にある（例えばテープ保管室，コンピュータ・ルームの両端など）探知器が制御卓の上に一群としてディスプレイされることを意味している。換言すれば，警報発生時にコントロール・パネルを見ればどの地域でアラームが発生したか一目瞭然の状態になければならないということだ。通常，各探知器は警戒状態にある時点灯するパイロット・ライトを備えている。コントロール・パネル上に各探知器ごとに独立した表示ランプが必要な場合もある。また警報システム自体の信頼性も重要な問題だ。電源故障やシステムの一部不良が発生すればトラブル発生警報が出るよう設計すべきである。またシステムが徐々に，或は突然活動を停止することがないような構造も考慮されるべきだろう。最近起ったテープ・ライブラリーの放火の例では，煙探知システムのスイッチが切れていた。

・もし探知警報システムにそれなりの価値を持たせようとするなら，それは，**人が適切な反応をこのシステムに示す**ことが不可欠となる。つまり火災探知システムは，誰かが常に火災警戒態勢にあるよう構成される必要がある。例えばコンピュータ・ルームの場合，そのスタッフがＡＤＰ施設警報システムからのアラームに即応出来る態勢である。また現場だけでなく建物内の離れた別地点にも警報装置が置かれるべきであり，警備室，セキュリティ・センター建築技師室がそれらの対象となろう。このような配備になっていれば，支援活動もし易く，コンピュータ設置部分に人がいなくてもその対応策をとりやすい。もし何らかの理由で遠隔警報地点での常時監視が出来ないならば，消防署の近くとか自衛消防隊の詰所等に第３の警報ポイントを設けるべきであろう。

・**適切なメインテナンス**は，火災探知システムには不可欠な要素である。煙探知

器の性格から，空気中のほこりや他の要因で誤った警報が出る場合もある。また間違った警報を防ごうとするとどうしても機器の鋭敏さをそこなうことが多く，その結果実際の火災発生時に探知が遅れることもある。従って正常な運用を保証するため，有資格者（提供メーカーの要員や建築技師）がシステムの導入時と以後の年１回の点検に従事することが肝要だ。勿論故障はすぐ修理されねばならない。だが残念なことにこうした点検作業時には，火災探知システムのスイッチを切るか，警報ベルを一時中断させねばならないことだ。もしこの作業時に火災が起これば何の対応策もとれないのが現状であり，何らかの改善が必要であろう。

探知装置は，火災の発生を通報するだけでなく，空調システムの制御にも使用出来る。探知と同時に空調装置の機能を自動的に中断させ，炎や煙が蔓延するのを防ぐ形態をとるわけだが，難点もある。というのは誤った警報でこうした一連のプロセスが進行することもあるからだ。より効果的な方法は，煙の再循環をストップさせ排出してから，室内の空気を100％外気と入れ替えてしまうことだ。空調装置の調節弁制御機能に若干の手直しを加え，火災探知システムと同調させれば，この仕組みは完成する。この項のより詳しい説明は第3.2節に譲る。

4.2.1.3 消　　火

消火は４つの方法で達成出来る。

- **携帯消火器**。これは火が手元で制御出来る間に鎮火させてしまう用具だ。
- 専門の消防士により使用される水で消火するための**ホース**。
- 気温が135～280°F（57～138°C）の想定温度に達した時作動する**自動散水システム（スプリンクラー）**。
- HALON−1301を用いて，燃焼プロセスを妨害するガスを室内に充満させ消火する**充填消火システム**。

連邦消防会議（Federal Fire Council）は，電子装置を含む様々な火事の歴史とその消火機器の有効性について再検討し，ＲＰ－１の第３章で示されているような数多くの要件をまとめあげた。

その第１は，各装置の50フィート（15メートル）以内に，容量15ポンド（6.8kg）の二酸化炭素消火器１台以上と2.5ガロン（9.5リットル）入り水消火器１台を備えるべきであるとしている。これらの消火器は，ＡＤＰ施設の要員が応急消火活動に使用するものだ。火災の早期発見とよく訓練された要員の適切な処置およびコンピュータ区画の危険要素が除去されていること等の条件が整っていれば，こうした携帯消火器の使用で大低の火災は未然に防ぐことが出来る。

携帯用消火器の効用を確かなものにするには次の様な考慮がなされねばならない。まず消火器の位置だが，これは角や装置の背後ではなく，すぐに手にする場所でなければならない。また直ちにその設置位置が確認出来るよう適切な表示が必要だ。各消火器位置の壁面や柱に大きな赤丸や赤いテープをつけるべきだ。全ての消火器を定期点検することも重要だ。（「携帯消火器」〔44〕参照）各消火器に荷札をつけ，点検日時とその担当者をその都度記すようにする。上述した消火器の他に，５ポンド（2.3kg）容量の二酸化炭素消火器も備えておく方が良い。重い物を持ち運べる職員がいないような地区には便利だ。

ＲＰ－１が示す第２の要件は，コンピュータ区画は，自動スプリンクラーを備えるべきであるとされている。建物が耐火又は不燃構造でないなら，この装置は建物全体に備えるべきだ。スプリンクラーがなかったり，外部からのホースの引き入れが困難な建物部分には，貯水塔や内部のホース装置が有効だ。自動スプリンクラー装置は，色々な点で推薦出来るものだ。だがＡＤＰ施設の管理者は，スプリンクラーの作動でＡＤＰ施設が水の被害を受ける点を考慮に入れねばならない。ＡＤＰ施設に起り得る最悪の事態が，コンピュータ・ハードウェアの冠水ならスプリンクラーの使用を除外してもよかろうが，何と言っても最悪の事態は建物全体が焼失してしまうことだ。副次的被害をなくして有効な消火活動を行なおうとすれば，HALON--1301充塡システムがどうしてもクローズアップされるだろう。二酸化炭素利用の消火システムは，生命に危害を加えることも多く余り薦められない。自動スプリンクラーとHALON--1301の特徴を比較対照してみたのが次の表２－４である。

表２－４　消火設備の比較

	自動スプリンクラー	HALON－1301
消火機構	火災現場での散水と冷却	燃焼プロセスの化学的阻害
信頼度	非常に高い。水の供給の信頼性により左右される。	非常に高い。探知システムの信頼性により左右される。
効　率	非常に高い	現場で有効濃度が確保出来れば非常に高い。
生命の危険	無	濃度が１０％を越せばやや危険
副次作用	散水により空気の冷却・清浄化が促進されるが，内容物への被害をともなう（冠水）。	通常の場合は無。異常の場合，腐食性の有害複混合物を生じる。
導入コスト	新規の場合，１ドル／平方フィート。既設ビルへの追加の場合，３ドル以上／平方フィート。	保護容積を基準とし0.５ドル／立方フィート。
放出制御復元時間とそのコスト	気温（又は自動再循環）分単位，５～20ドル	探知システム又は手動。時間単位，設置コストの40％

コストの低廉，証明済みの有効性，装置自体の安全性等の理由から，自動スプリンクラーが大抵の場合最も有用な消火システムである。HALON－1301は，テープやディスクの保管場所，ハードウェアの設置区画等の重要地域や，底上げした床やケーブル導管のようなスプリンクラー・システムでは効果的に処理出来ない部分に対する初期消火に有効である。

自動スプリンクラー・システムは，防火体系に組み込むべき機能も有している。つまり，フロー・センサーと呼ばれる装置も利用出来，これはスプリンクラー・パイプに挿入すれば水流を探知することが可能となる。この水流アラームは，取

水源や配管の主要な分岐点に設置したり，火災警報パネルに接続したりする。火災が発生しスプリンクラーのヘッドが開いて散水し始めると，警報が非常要員に知らされる仕組みをとる。この機能は，作業現場の無人時間帯には特に有効で，スプリンクラーの作動がセキュリティ要員にすぐ通報され，しかも鎮火直後に水流を止めることも可能となる。この仕組みを最大限活用するには，スプリンクラー・システムの配管時にパイプが単一地点からコンピュータ区画に通じるようにし，閉鎖バルブを操作の容易な部位に装着することである。また全てのスプリンクラー・システムの閉鎖バルブは，マスタースイッチに接続され，バルブの閉鎖を警報パネルに通報するようにすべきであろう。これは重要なことだ。というのは，スプリンクラーの制御バルブが不注意によって締められたままで，火が完全に鎮火していない場合が往々にしてあるからだ。バルブがわざと閉じられる場合も想定される。

ガス消火システムもまた，消火活動をより効率的にする特徴を備えている。この装置は，ガスの著しいロスを検知し警報を発することが出来る。システムは通常，最初の警報からガスの放出までに1分以内のずれを持つよう設置されている。二酸化炭素システムにあっては，この時間的ずれの間に，要員が現場からの退去を完了するよう想定されている。というのもガスの放出が人体に著しい害をもたらすからである。一方HALONシステムの場合，このかなり高価な消火剤の実質的な放出を手操作で停止させるため，この時間的ずれが設けられている。火災が発生していなかったり他の携帯消火器でも容易に処理し得る場合があるからだ。

もし消火装置を常に作動可能な状態に置きたいならば，有資格要員が定期的に保守作業を行なう必要がある。「消火機器」〔11〕は，消火器の点検とメインテナンスにとって恰好の手引書である。またＡＤＰセキュリティ・プランナーは，建物管理者と消防署長と緊密な連係を保ち，効果的なメインテナンス計画を実施すべきだ。文末の参考文献リストには，全米防火協会の発行になる全国火災コード（National Fire Code）〔22－43〕から採られた基準，ガイドライン，勧告が数多く所収してある。

4.2.1.4 消火活動

この項では，素速いかつ効果的な消火活動の意義について述べよう。実際の消火任務を負う人についてはまずＡＤＰ施設管理者が挙げられるが，彼は個々の問題に最もマッチしたアプローチを決定する為，地域的な条件に注意を注ぐべきだろう。ＡＤＰ施設には大規模な工業地帯に置かれているものも多く，防火専門要員を雇っていたり，高度の訓練を積んだ自前の消防隊を擁している場合がかなり見られる。自治体の消防署に近接したものもある。これとは反対に，距離的に消防隊やよく訓練された防火要員の消火活動を期待出来ない遠隔地に置かれているＡＤＰ施設もある。言うまでもなく，まさかの場合に専任の防火隊員が即応出来る態勢が最善である。だがそれが実現不可能な場合，全く別の対応策が案出されねばならない。特に，ＡＤＰ施設内部に通常設置される高価な装置のことを考えれば尚更である。

きっと見識のあるＡＤＰ施設管理者なら，消防士や熟練防火要員が火災発生を通報してから消火作業に移るまでの被災に対し，まず第一の防衛線を敷こうとするだろう。その規模に拘らず，工場施設は火災に対する安全性に精通し訓練も経た要員を必要としている。またどのような防火組織も，実際的かつ効果的であるためには，火災発生地点で即応態勢をとれるような仕組みを持っていなければならない。その為には，どの組織単位や区域にも，教育訓練を完了し火災発生の初期に素速い消火活動をとれる中核要員を配置することが必要だ。こうした人員配置をとれば，彼等は特定の防火作業や関係施設に適用し得るシステム等について精通することも可能となる。つまり，警報の出し方，どのような火災形態に対し如何なるタイプの消火器を使うべきかの区別，またこれら機器の使用法等が体得されるという訳だ。更にこうした配置要員は，常駐監視員としての役割も果たし，火災発生を潜在化している状況の探知，通報，矯正等に当れるはずだ。消火装置の適正位置の確認と保守，消火活動を妨げるような貯蔵品の過度の集積のチェック等にも彼等は取り組み，火災のリスクを極小化するため一般的な建物管理にも

気を配ることになろう。

ＡＤＰ施設防火組織を設立する決定が下されたなら，必ずＮＦＰＡの「産業消防隊トレーニング・マニュアル」を参考にすべきだ。この小冊子は消防隊の形成と訓練のための手引きとも言うべき性格を持っている。ＡＤＰ消火隊の構成は，隊長，副隊長，そして各勤務シフト毎の数人の防火要員という規模になろう。大規模なＡＤＰ施設では当然増員が考えられる。火災発生時には，防火要員以外の施設職員は構内から退去すべきである。

選任された防火要員は，コンピュータ区画用の消火器を使って毎年実際的な消火作業を行ない，訓練を積むべきである。更に，彼等は，火災探知器，警報器，スプリンクラー等を含むあらゆる防火機器の運用を修得理解すべきである。また係員の適性を維持するため，消防組織は定期的に，少くとも２～３ケ月毎に簡単な訓練セミナーを開催した方が良い。一方消防隊長は，新しい装置や手順が採用されればその都度点検する必要がある。彼はまた仮説としての火災発生状況の処置についても討議を組織し，どのような装置のスイッチを切るべきか，最も近接している消火器はどこか，それ以外の消火器で近いものはどこか，火災現場に近づく上で何らかの困難があるか，誰にまたどのように通報すべきか……。隊長はまた，新しく登場した防火上の問題についても討論を組織すべきだ。建物防火主任や地域の消防署もこうした訓練計画にその素材や設備，助言等の点で寄与出来るだろう。

ＡＤＰハードウェアの特殊な性質及びそのオペレーションの中断を極力避けねばならない立場からして，消火手段や損害抑止手段は注意深く構成される必要がある。ＡＤＰ管理者とシステム・オペレーションの監督者は，建物防火主任や消防隊長とともに，ハードウェアのパワーダウン，空調設備の停止，関連手段の行使等の決定の基礎となるガイドラインを，協力して策定すべきである。全ての火災制御手段は防火部門の活動と調整され，ＡＤＰ装置設備の保全に資するものでなければならない。また防火部門の存在を周知徹底させるため現場の訪問も行なわれねばならない。通常及び非常用の出入口，電源スイッチ，消火ホース及び消

火器，スプリンクラー制御バルブ，装置用シートのありか，換気扇及び排出口のスイッチ，可燃性貯蔵品，建築構造とその特徴，その他関連項目等の知識は特に重要だ。ディスクやドラムの表面汚染（帯磁など）の如き特殊なＡＤＰ被害や，床下にあるプラグ差込口の存在等については，必ず指摘される必要がある。

非常事態の対応計画については第８章で詳しく触れる。

4.2.2 洪　　水

前節で取り上げた自動スプリンクラーの項で，その作動による水の被害はＡＤＰ施設に対する著しい脅威とは考えなくてもよいという印象が残っているかもしれない。確かに，１～２のスプリンクラー・ヘッドの作動による被害は少なく，火災による煙害や熱害とは比べものにならないが，洪水はまた別問題である。洪水の水質が，沖物，石油，化学物質で汚染されているかも知れないし，建築物は単なる損害にとどまらず，全壊の危険すら持っているのだ。

熱帯性の嵐Agnesは1972年6月ペンシルバニア州を席捲し，大洪水を引き起こした。各新聞の集計によると，数百のコンピュータ・システムが泥や水につかってしまったと言われる。これらのシステムの損害は主に地理的位置に起因するものと思われるが，復旧所要時間は，２日間のものもあれば２ケ月に及ぶものもあった。ペンシルバニア情報システム管理局（Pennsylvania Burean of Management Information Systems）の報告によると，同所の大型コンピュータは６フィートもの深さの水につかってしまったようだ。週間4,500万枚も使用されていたある書式の予備品は，別のコンピュータ施設の被害で失なわれてしまい，残ったのは僅か１週間分だったという。また多くのコンピュータ・センターは，バックアップの無いデーター・カードのファイルを失ってしまった。

この経験から２つの問題が指摘出来る。その第一は，もしＡＤＰ施設が低い地盤のしかも地下室に置かれていたなら，洪水の被害は殆ど不可避であること，また第二は，バックアップ・オペレーション体制に充分な配慮があれば，非常事態が起っても通常のオペレーションの回復に必要な時間が大幅に削減出来ることだ。

1966年8月に出された行政命令11296号は，連邦関係施設の洪水被害に関する関心の急激な高まりに応えるためだけでなく，氾濫区域の安全で効果的な利用について連邦政府機関によって保証がなされたものであった。要約するとこの行政命令は，行政機関が新規施設を設立したり，各施設へ援助資金を支出したり，処分を予定している連邦関係施設の将来の利用価値を評価したり，あるいは"氾濫区域の不経済な危険要素の強いそして不必要な利用を避けるため"土地利用計画を調整したりする際，洪水の危険性を厳密に評価することを要請したものである。経済的に実現可能ならば，既存の構造物に対しても，洪水対策がとられるべきことを規定している。

洪水に関する危険情報は，陸軍工兵隊，テネシー河流域開発機構（ＴＶＡ），農務，内務，商務，住宅都市開発の各省および非常事態計画局から得られる。州及び地方自治体の機関で，過去の洪水情報を提供しているところも多い。洪水対策の基本的なガイドラインは，「連邦政府機関用洪水危険評価ガイドライン」〔54〕に示されている。このガイドラインでは，洪水が起こる危険性のある地域を３つに分類している。まず第一は，大量の降雨や雪解け水，あるいは流域中の溢路等が原因となって洪水がおこる河岸の氾濫区域である。また第二は，海岸線の氾濫区域で一体の澱みと境を接している場所で，こうした地点では高潮，風波，津波（海底地震に起因する高波）等で洪水が発生する。最後の危険地帯は，山から流れ出た水により山麓に堆積した岩屑丘である。ここでは鉄砲水が発生しやすい。ＡＤＰ施設がこうした地域に設置されているなら洪水対策は欠かせないものとなろう。

自然の洪水にさらされる危険性を判定する際，ＡＤＰセキュリティ・プランナーはまず，行政命令11296号に従って所属機関が出した規則や準則を検討すべきである。次に彼は，彼が担当する建築物や隣接する他の連邦施設等に適用し得る洪水被害評価結果を見直す必要がある。こうした作業は，さらされる危険を直視しなければならない必要性を強く認識させることになろう。入手した情報でＡＤＰセキュリティ・プランナーは，洪水に被災する可能性を数段階に分けて推定出

来ることもあろう。更に，建築物の立地条件の再検討で彼は，内容物の損壊，停電，通信途絶，建物への接近困難等の要因が与える影響についても予測出来るだろう。これらの影響予測をリスク分析と相関させれば，予想される洪水損害額を割り出せるし，洪水対策措置の予算要求の基礎も算出出来る。

洪水の全体的な影響に加えて，あらゆる原因から生じる洪水被害も検討調査すべきである。その第一段階は，建物内部のＡＤＰ施設の位置の評価である。地下室は本来最も避けねばならない場所だ。というのも，大雨でかさを増した水流や消火水が地下室に流れ込む可能性が強いからである。たまり水には排水口を，逆流の防止には調節弁を用意することが出来る。また電動の排水ポンプを備えて，水はけを改善する方法も有効だろう。だが，非常事態にあってはこうした手段は間に合わない。階上の火災発生中は，消火ホースから１分間に1,000ガロン以上の水が吐き出されるのでポンプや排水溝では対処出来なくなってしまう。更に火災現場で生じる種々の破片が排水溝やポンプをふさいでしまうこともあろう。火災やハリケーンで停電が起こり排水ポンプのモーターが最も肝心な時に作動しなくなってしまうこともあるはずだ。ＡＤＰセキュリティ・プランナーはまた洪水を対象とするとき，施設が地下室に置かれているために生じる物理的な防備力を差し引いて考え，純粋に洪水にさらされる危険性を判断しなければならない。もしＡＤＰ施設が地下室に置かれていてしかも洪水に遇う可能性が顕著な場合は，その対抗手段として次のようなものが適切だと思われる。

- ガソリン駆動モーターの**非常用排水ポンプ**（１台以上）
- 逆止め弁を持った**排水溝**
- 地上の洪水の流れが著しく脅威となる場合に備えて土手を早急に構築するための**砂袋**を手近かに準備しておく。低い位置にある外扉を密閉するための高性能粘着テープも役立つ。
- 洪水流の方向を転換させるため，ＡＤＰ区画の周囲に縁石をめぐらせる。この措置は規模の小さな洪水にのみ有効だが，努力してみる価値は充分にある。

以上述べた手段は，洪水被害が比較的軽微か，原因が内部にある場合に有効と

なろう。外部の洪水の流れにさらされる危険性が大きな既存施設のためには，全面的な洪水対策が必要である。「洪水対策規定」〔51〕はこうした事例に大いに役立つと思われる。この文書は，建築のモデル規準の形態をとっていて，建物自体の洪水被害を極力抑え，構造物を損害から保護するための手引書となっている。

出水は配管の水漏れから起こることもある。脅威評価の一部として，ＡＤＰ施設の天井に置かれた配管やその為の穴も考慮に入れるべきだ。理想的には，ＡＤＰ区画の上に何のパイプも通さない方が良い。だが設計上どうしても配管を避けられないならば，閉鎖バルブを手近かなところに配すべきだ。同じ様に，ＡＤＰ区域内の空調設備をサポートしている冷却パイプや圧縮水管も，水漏れを分離するため閉鎖バルブを備える必要がある。主要な配水管は，急激な圧力低下 — 破局の前兆である — を検知し，ビルの管理者に通報し，出水量をおさえるため自動的にポンプを閉じる仕組みを備えていることが肝要だ。ＡＤＰ施設の床板にある穴はすべてセメントがそれに類似した材料で埋められねばならない。多くの建物には所謂濡れ柱（ wet column ）が備わっており，これは通常立上り管（riser）と呼ばれる垂直配管を附随した構造材である。普通これを埋め込んである壁は，パイプを収容するスペースをとるため通常の柱より厚くなっているので識別しやすい。この柱は水漏れや出水にさらされる危険度も高いゆえ，ＡＤＰ区域からはずすことが望ましい。事情でそうもゆかないなら，各柱は，どのような漏出も床下に排出出来るようチェックされていなければならない。

コンピュータ・ルームは大抵底上げ床を採用し，キャビネット間の接続線や電力線を収める保護空間を備えている。また空調システムの完全換気に利用されている場合も多い。もし出水がこの底上げした床の下に集まるならば，これらの電線に影響が出る危険性が生じる。端末にコネクターを持ったキャビネット接続線は耐水性が強いが，床のコンセントにプラグで差し込まれている電力線は，ショートや腐食の可能性がある。出来るなら，コンセント・ボックスは，床から少くとも８～10センチ上に配置し，配線は頑丈なコンジット（線渠）に納めてしまう方がよい。また床には，６メートル間隔で排水溝を備える措置も有効であろう。

このことは特に，底上げした床を周囲の部屋の床と同じ高さにするため，二重床の下部が押し下げられている新工法では重要である。この建築方式では当該区画の水平差に配慮する必要性がないが，押し下げられた下部の床面にたまる水の排出を積極的に行なわなければ，多量の水が底上げ床の下に集中するのは自明のことである。こうした事態を放置すれば，ケーブルが水につかるだけでなく，1インチ水かさが増えるだけで約5ポンド／平方フィートの活荷重が生じる。これは構造物に損害を与えるだけでなく，極端な場合その崩壊をもたらすことになる。

最近のＡＤＰ施設には非常時のＡＤＰハードウェア防護に備え，プラスチックのシートを用意するところが多い。配管故障や階上の消火作業による出水をこうしたシートで防ぎハードウェアの保全をはかった例も数件報告されている。水に対する対抗手段としては，コスト，効果の両面で有効と思われるので，積極的にとり入れられるべきだろう。

4.2.3 地　　震

地震は2つの理由からＡＤＰオペレーションに脅威を与える。その第一は，直接的な影響で，地震の発生によりＡＤＰ施設を収容している建築物の構造上の損壊，電気回路や通信回線の中断，停電や断水等の公共サービスの途絶が引き起こされる。また第二は，より広汎な周囲への影響である。輸送のストップとそれによる食糧や生活必需品の欠乏等が生じれば，ＡＤＰスタッフは作業報告を送ることも出来なければ，サポート・サービスも受けられなくなる。

米国で地震が記録されるようになってからまだ日が浅いので，地震の発生予測は容易なことではない。図２－１は有感地震の数と激しさを示したものだ。また図２－２は，これらのデータに基づいた地震危険分布地図である。注意しなければならないのは，この地図が予測し得る激しさを示したものであって，決して発生の可能性を表わしているものでない点だ。現在連邦政府がバックアップして実施されている研究調査が成果をあげるようになれば，長期の発生予測だけでなく，目前の発生も予報出来るようになるだろう。しかしこうした技術開発が成功する

まで，第３ゾーンにあるＡＤＰ施設は，少くとも１週間の機能停止を伴なう地震が50～100年の間に起こるものとして防護されるべきだろう。更に主要断層から5～10マイル以内に位置するＡＤＰ施設は，同様な発生予測期間にたってその施設の完全な崩壊を考慮に入れておかねばならない。

図２－１　1966年までに米国内で発生した大規模な地震（省略）

作成：米国地震情報センター（ＮＥＩＣ）

環境科学サービス局沿岸測量部

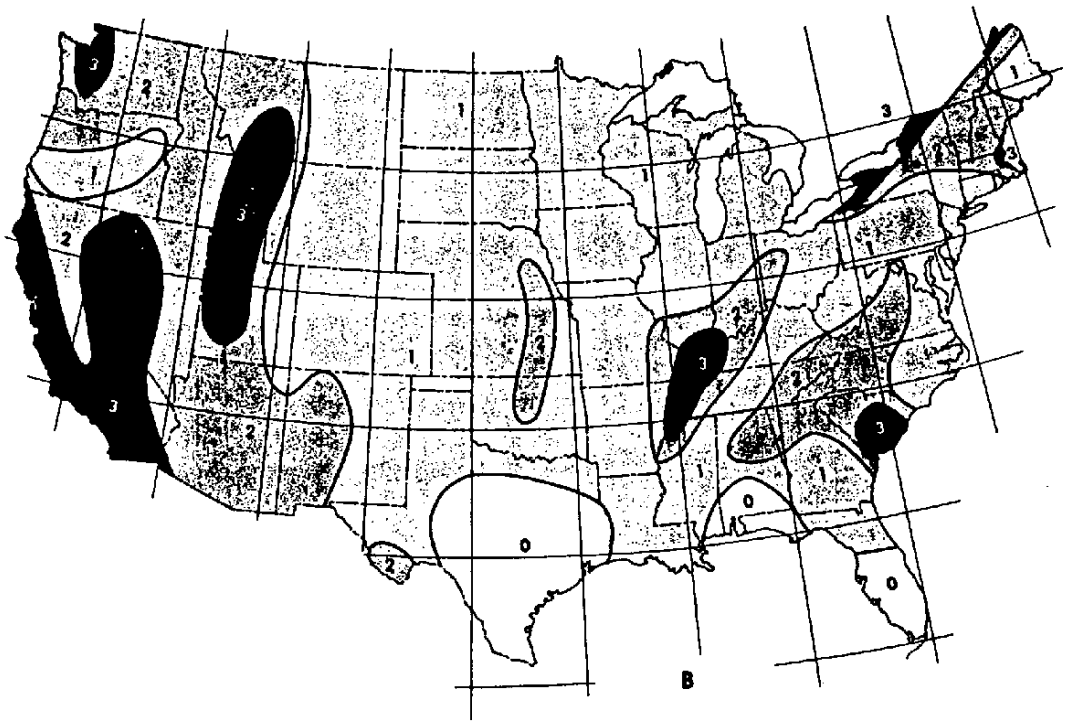


図２－２　米国の地震危険分布図

第０ゾーン ― 被害無し

第１ゾーン ― 被害軽微。遠方の地震は１秒以上の周期で構造物に被害を与える可能性もある。改正メリカル震度階※5と６に相当。

第２ゾーン ― 中程度の被害。改正メリカル震度階７に相当する。

第３ゾーン ― 強度の被害を受ける。改正メリカル震度階８以上に相当。

この分布地図は，過去の損害が大きかった地震の分散状況とこれらの地震が示した改正メリカル震度階を基礎に作成されたものである。引っぱり強力によって起きた変化，主な地質構造，地震活動の影響を受けた領域等も同時に考慮された。各ゾーンの破壊的地震の発生頻度は，この多様なゾーンの等級分類作業では特に考慮されなかった。

※1931年制定の改正メリカル震度階

地震危険分布地図。米国での地震記録の歴史は比較的浅いので，この分布地図は長期的な危険要素を大雑把に予測しただけのものである。地図は，実際に発生した地震，主要な地質構造，特徴的な地質地域を基礎にしているが，局地的な物理条件は組み込んでいない。また共通の時間的尺度は特に想定されていない。実際問題として，大型地震による被害が西海岸の第3ゾーンより東海岸の第3ゾーンの方が頻繁に起り得るとは考えにくい。図2－1の地図は1948年～1952年に編纂されたもので数々の建築規準や建築法規を盛り込んだものだ。点は，被害甚大であったこれまでの地震を示していて，次の様に定義されている。最小の点はきちんとした設計のビルには無視出来る程度の損害しか生じなかったことを示し，次の小さな点は，同上のビルに軽い被害があったことを表わしている。その一段階上の点はかなりの程度の被害，最大の点は，被害甚大で地面には亀裂が生じ，眼に見えるほどの垂直水平両方向の地動があったことを示す。図2－2の地図は1969年に作成されたもので，その後の地質調査の成果を追加してまとめられた。（ＥＳＳＡ／ＵＳＣ&ＧＳ）

可能性のある対抗措置には2種のタイプがある。まず第一は，高度な耐震性を持ち隣接ビルの損壊から影響を受けないような配置の建築物を選ぶことである。避けられるべき場所としては，山や丘の中腹，盛り土地域，水際，燃料貯蔵区域，高層建造物（ＡＤＰ施設上に倒壊する恐れのある高層ビルディング，電波塔，送電線），あるいは地下燃料輸送管の埋設地帯等があげられる。またサンフランシスコ大地震の被害は，消火用水の欠乏が原因となって猛威をふるった大火災によるものが殆どであった事実を忘れてはならない。従って，スプリンクラー・システムに耐震性を持たせ火災現場での消火を確実にするため，振動支柱や自在ジョイントの使用に関心を払うべきだろう。

これらの予防手段に加えて，ＡＤＰセキュリティ・プランナーは，ＡＤＰ施設偶発事故対策計画にオフサイト・オペレーションを追加することによって所属組織の使命達成を保全しようとするだろう。このような場合，同じ地震で被害を受けない程度の地理的距離は保たれねばならない。更にバックアップ・ファイル，

ドキュメンテーション等が損害を受けずにしかも地震発生後すぐに確保出来るよう。その保管施設の位置と建築にも充分な注意が必要だ。リスク分析と復旧手段のガイダンスとしては「被害軽減の為の建築計画」〔59〕を参照されたい。

4.2.4 暴風雨

暴風雨，ハリケーン，竜巻等はすべてＡＤＰ施設に対する脅威を潜在化している。ハリケーンは，強風と豪雨を伴ない構造物の破壊，氾濫，停電をもたらす。1954年から1966年にかけて起った主要な米国内の送電途絶148件のうち，17件はハリケーンが原因となったものであり，年間平均1.3件であることを示している。1970年のハリケーンCeliaは，Corpus Christi地区の50ケ所に及ぶデータ処理施設に被害を与え，破局的な損害を与えた例も示している。この時の停電は36時間も続いた。「米国の大西洋沿岸部におけるハリケーン発生頻度」〔48〕は，1886年から1970年までのハリケーンを対象にした報告書であるが，ADPセキュリティ・プランナーにとっては，相当施設がさらされる危険性を推測するには恰好の素材だと言えよう。発生頻度が高い地域はこの調査結果では次の様にまとめられている。

年間発生率（%）	地　　域
16	Fort Landerdale（フロリダ州）
15	Palm Beach（　〃　）
14	Brazoria County（テキサス州）
13	Lafourche Parish（ルイジアナ州）
13	Mobile, Alabama－Pensacola（フロリダ州）
13	Key West（　〃　）
12	Chambers County（テキサス州）
11	Carteret County（ノースカロライナ州）
9	Matagorda County（テキサス州）
9	Franklin Parish（ルイジアナ州）
9	St. Bernard Parish（　〃　）

メキシコ湾岸及びフロリダ半島沿岸には，この発生率が４～８％のところが多い。上述した地域に含まれていない大西洋岸はこの数字が０～７％である。そのＡＤＰ施設が頻度係数の高い地点またはその近くにあるなら，ＡＤＰセキュリティ・プランナーはハリケーンの脅威に十二分の配慮を払うべきであろう。

このガイドラインの到る所で出水と電気系統の故障に対する防御手段に触れているが，これとは別に風による損害，特に風が吹き上げる破片で窓に加わる被害や倒木，電柱の倒壊等に対するＡＤＰ施設建築の抵抗力にも関心を寄せるべきだ。トラブルの起る可能性のある個所を巡視すればかなりの程度は未然に防げるはずだ。通常警報は十分組織化されているので，初期の段階では扉や窓にベニヤ板で防護措置を施すことなども考慮されて良いだろう。

図２－３は，1953年から1969年にかけて発生した大型竜巻の州別の統計である。年間平均で642件の竜巻が起ったことになる。

ごく限られた地域であるが，竜巻が再発する傾向の強いところも報告されている。従って，発生する可能性を予測する場合，上述した数値だけには頼れない面もある。ＡＤＰ施設がロッキー山脈の東側に置かれているならば，ＡＤＰセキュリティ・プランナーは，ＡＤＰ施設の立地条件の評価に当って，気象庁の最寄りの測候所に過去のデータを問い合せるべきであろう。

最近ジョージア州で起った竜巻では，あるデータ処理施設のコンピュータ・ルーム上を走っている配水本管が破裂し，その為に起った出水で建物全体がひどい損害を受けた。復旧作業はかなり迅速に行われたが，これは，隣接企業ビルのコンピュータ・ルームの修復が早かったのと，ＡＤＰスタッフ及びメーカー側のエンジニアが昼夜を分かたず努力したからである。業務の一部はオフサイト施設で代行され，１週間後には仮設施設で通常サイクルのオペレーションが開始された。

例え建物自体に損害が生じなくても，ＡＤＰ施設は側を通過した竜巻で停電の被害を受けているかも知れない。1954年から1967年にかけて起った竜巻による主な停電件数は，10件と報告されている。一方強風によるものは７件であった。

要約すれば，歴史的データは，ハリケーン，大型の竜巻及び暴風の潜在的発生

予測に貴重な素材を提供していると言えよう。少くとも何らかの脅威が発生する可能性があるなら，ＡＤＰセキュリティ・プランナーは，建物被害，出水，電気系統の故障についてその防護手段を講ずべきであり，偶発事故対策プランには，こうした事態を十分想定した対抗手段が盛り込まれねばならない。

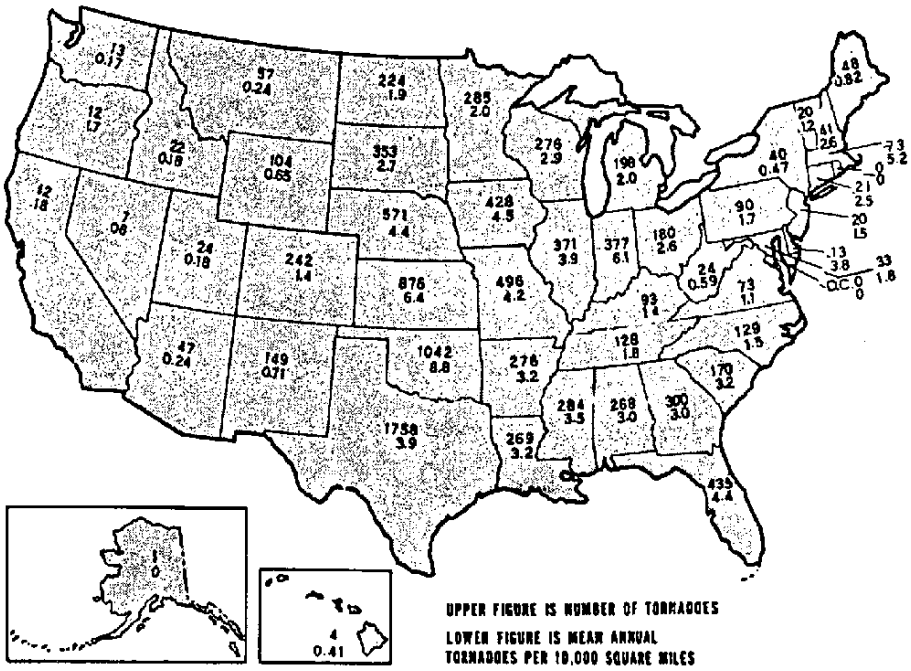


図２－３　州別の大型竜巻発生件数（１９５３～１９６９年）

図２－３　州別の大型竜巻発生件数（1953～1963年）

上段数字は竜巻の総発生件数。

下段数字は１万平方マイル当りの年平均発生件数。

4.3 補　助　設　備

4.3.0 まえがき

すべてのＡＤＰ設備は電源，空調設備，およびシステム操作上使用するコミュニケーション設備，水道，エレベータ等の補助設備に依存している。ＡＤＰの安全計画立案者は故障，サボタージュ，破壊行為，火災，洪水等の上記補助設備に対する事故の発生の可能性および影響を考慮に入れておく必要がある。この場合，計画立案者はその影響を危険分析によって得られたＡＤＰ設備の必要性に関連させて説明することができる。本章では上述のような事故およびそれに対する対策について論ずることにする。

4.3.1 電　　源

電源は，ＡＤＰ操作に影響を与えるものであるが二つの重要な特徴を有している。即ち，特性及び信頼性である。特性とは，ここでは非常に小さくて各電力会社では記録することはできないが，ＡＤＰハードウェアに依存して，ＡＤＰハードウェアの操作に対しては影響を与えるほど大きい，正常波形の変形が存在することを指している。ＡＤＰハードウェアは交流電気を整流し，その結果生ずる直流をフィルターにかけ，電圧調整を行ない，これをＡＤＰ回路に送る。フィルターおよび調整によっても一定範囲以上の電圧変化を除去することは期待できない。仮に，線電圧が，４ミリ秒以上の間，定格の90％以下，もしくは16ミリ秒以上の間，定格の120秒以上である場合，ハードウェア回路に対する直流電圧の過剰な変動が予測される。この回路に対する影響は変動の量及び継続時間及びハードウェアの状態に依って変るため，予測することは困難である。また，ロジック・エラー，データ移送上のエラー，さらに極端な場合にはハードウェアに対する故障も予想される。通常このような事態は，他の影響がかなり後まで発見されないのに比して，事後に察知される。

このような電源ライン変動は通常トランジアントと呼ばれているが，雷の衝撃によって生ずる。その発生の可能性は雷雨の発生回数，変電所間，地下配線（空中に対して）の使用状況，配線によって決る。

電力会社がトランジアントを予測するのはさらに困難であるが，電力の需要が高まり，力率補正装置がオフラインにスイッチされる朝の7時半頃にトランジアントが発見されることがある。通常このようなトランジアントはＡＤＰの操作には影響を与えないが毎朝大きな影響が生じたという例も報告されている。

内部的に発生したトランジアントは建物内部の配電状態と個々のスウィッチングによって起る負荷の最大の値のトータルによって表わされる総負荷のパーセンテージに依って決る。内部トランジアントの影響は他の建物の負荷からＡＤＰを遮断することにより最小限におさえることができる。理想的なのは，コンピュータ範囲の配電盤は第一次給電線に直接接続されており，他の負荷，特に高馬力モータと逓降変圧器を共有しないようにすることが必要である。図に代表的な配電システム例が示されている。

ここでは電源ラインのトランジアントの原因および影響を説明したが，抽象的に検討しただけでは発生頻度を正しく推定することは困難である。幸いなことに，トランジアントが実際に発生するのを測定する装置がある。代表的なものとして，短くて小さいトランジアントも永続的に記録するストリップ・チャート・レコーダ及び電子回路を有する装置がある。トランジアントが生ずる時間と異常操作のコンソール・ログ・レコードを比較することにより，通常所定の期間における破壊性トランジアントの数を測定することができ，さらにトランジアントの原因を調べることができる場合が多い。このような測定は少くとも1カ月間行なわれるべきであり，ＡＤＰの設備によっては継続的に行なう必要がある。しかしながら，ここに二つの落し穴がある。その第一は，検流計記録計は短いトランジアントに対しては反応しないため線電圧の傾向のみを示すということである。このため，この種の記録計はトランジアントを扱う上では役に立たない。第二に，資格を有する電気技術者が測定を綿密に監視しているか否かに注意することが重要である。

仮に測定が有効でなければならない場合，これを正しく行い，正確に解釈し，他のインプットと関連させていかなければならない。また，地方の電力関係の代表者と話し合うこともトランジアントの原因を理解する上で役に立つであろう。

第二の電力の基本的特性である信頼性は，線電圧が一定のレベルから，おちこんでトランジアントと見なすことができないほど長く続いた場合における回数および継続時間と関係を有する。これには，継続的な電圧不足（ブラウンアウト）もしくは停電（ブラックアウト）が考えられる。ブラウンアウトは起電容量に近いか等しい負荷の結果に依るものである。極端な場合において，需要に見合った起電容量を拡げるために最大値８％だけ線電圧を減ずる電力会社もある。最後の手段として，"ロード・シェディング"と呼ばれる措置のように負荷の一部を切り離してしまうようなことがあるが，この対象になった電力使用者はブラックアウトの状態となる。更に，ブラックアウトは暴風，洪水および同様の原因（第２章で述べた），電気設備の故障，稀には人間の間違いによって起るものである。

1965年の有名なノースイーストのブラックアウトは，装置および電力プール管理上の欠陥を浮きぼりにしたものであった。

幸いにも，その時に取られた国内の電力システムの信頼性強化の措置によりこのような事故の再発はあり得えない。然しながら未だ問題は残っている。例えば発電装置固有の信頼性，特に大型の装置についての問題がある。さらには新たな問題としては環境保護の方策という問題があり，新たな建設に関して，数々の要請に見合った面倒な手続きが必要となってくる。ブラックアウトの発生の可能性は，大体において定率の不定期な故障および余備発電容量の大きさに依って決る。各々のファクターは個別に評価されなければならない。

1967年前半中，米国における，52件の顕著な不定期の電源故障例が連邦電力委員会（ＦＰＣ）〔10〕によって報告されている。これは代表例であり，同様の故障が将来においても同率で生ずると見るのが適当であると思われる。ただし，トランス故障，地域的電線切断，その他の事故のような，全体的でないそれほど重要でないものについてはあまり報告されていない。これらの不定期もしくはそ

れに近い事故の頻度を予測することは不可能である。

同じＦＰＣの報告によると不定期に生じたブラックアウトの継続時間を以下の表に提示している。

表３－１　ブラックアウト継続時間の分布

継　続　時　間	全体のパーセンテージ	累　積　総　計
9 ～ 15 分	6 %	6 %
15～30 分	36 %	42 %
30～60 分	18 %	60 %
1～2 時間	14 %	74 %
2～4 時間	10 %	84 %
4～8 時間	8 %	92 %
8～16 時間	6 %	98 %
16 以上	2 %	100 %

ブラックアウトもしくはロードシェッディン（地方の電力会社による）に帰因する故障発生の可能性はその発電容量，その予備量，さらには電流の信頼性および保守の状態に精通することによってある程度まで予想することができる。

予備容量がピーク・ロードの20％である場合，負荷に関連したブラックアウトの可能性は非常に小さい。予備容量が最大の単一発電装置容量に近づくにつれ，ブラックアウトの可能性が急速に上昇し，予備容量が小さい場合でも不安定な状況を示す。このことおよびこれに関連した分野における最新情報はＦＰＣ報告書および国内電気信頼性に関する会議（ＮＥＲＣ）〔22〕に採録されている。

これらのすべてのファクターを考慮することにより，電力トランジアントおよび故障の影響をある程度の信頼性をもって推定することができる。危険分析に戻ると，ＡＤＰ設備に対するこれらのトランジアントおよびブラックアウトのコストを推定することができる。このコストの推定は保護対策をコスト面での妥当性をみる上で利用される。もちろん，将来的なロスの可能性を予測する上で，リア

ルタイムもしくはテレプロセシングのような特に高度な利用方法が進んでくることを考慮に入れることに留意する必要がある。

潜在的なロスを適用に見積ることにより，ＡＤＰの安全性立案者は，コスト及び性能をベースとした候補対策を評価することができる。一定のコスト範囲において，１ないしはそれ以上の特性問題に対する可能と思われる対策が多数存在する。引き続いての検討において，一般価格範囲が含まれており，負荷のキロボルトアンペア（ＫＶＡ）に依って述べられている。これらの価格は予備的分析に役立つものであるが，慎重に利用しなければならないし，最終決定は正確な推定に基づいて行なわなければならない。

保護措置の分析の一部分として，ＡＤＰセキュリティ・プランナーは負荷のこれらのタイプを正確に作表する必要がある。データ伝送装置を含むＡＤＰハードウェア，データ変換装置，空調装置，通常および最小照明，その他ボイラー，自動ドア等に緊急操作に必要な装置を含むＡＤＰハードウェア。また，彼は各ブレーカ・パネルのレベルまで，建物，特に上記の負荷に対し，"one－line" 図表を作成する必要がある。

これらのデータは，記述すべき修理対策を評価する上で必要なものである。

仮に，大きなロスが内部に発生したトランジアントより生じた場合，電力配分の再配置により，この問題を効果的に解決することができる。これは特殊な状況の詳細によって決定されるため有効なコストの指針を出すことができない。

場合によっては，トランスファー・スイッチを通じて１本以上の給電線に建物の配線を接続することが可能である。このように，１本の給電線が故障しても，建物の負荷（もしくはメインの電線を臨界負荷のみに分割して起きる負荷）は交換給電線に移送することができる。この技術は，この二つの給電線が異る変電所に接続している場合，更に重要である。二重の給電線は局所的なブラックアウトに対してのみ保護されているため，その価値は限定的なものであるが，場合によってはコストが適当である場合がある。

電圧調整変圧器（ＶＲＴ）は，小規模な長期間トランジアント（千ミリ秒もし

くはそれ以上）およびＫＶＡ当りの負荷につき100ドルから200ドルのコストがかかる電圧不足に対して，非常に顕著な保護作用を示す。しかし，ＶＲＴは短く，高強度のトランジアントもしくは実際の電源故障に対しては保護されていない。

ＫＶＡ当り200ドルから300ドルのコストが要る負荷に対する保護対策としては図３－１に示されるようなエネルギー貯蔵フライ・ホイールをもつモータ・オールタネータ（モータ・ジェネレータ）を設置することができる。このような配置は約15秒間までのトランジアントおよび電源故障に対して非常に有効に保護するものである。信頼性が非常に高い場合，定期保守を割引いて考慮してもよい。騒音レベルが非常に高く，床負荷が定常以上であるため装置に対する特別のスペースをとっておく必要がある。

不切断電源（ＵＰＳ－uninterruptable power supplies）と呼ばれるものが多数市販されている。代表的なＵＰＳは，バッテリーを充電状態に維持し，ソリッドステート・インバータを駆動させるソリッドステート整流器よりなる。インバーターはコンピュータに対して交流を合成する。単純化したブロックダイヤグラムは図３－２に示されている。

実際に，ＵＰＳは広大フライホイールとして作動するバッテリーをセットされたモータ・フライホイール・ゼネレータ装置をシミュレートする。バッテリーのアンペア時容量に依り，ＵＰＳは入力電気なしで45分間その負荷をサポートすることができる。同時に，それは，トランジアントをフィルターにかけ，ブラウンアウトを補正する。ＵＰＳに対するコストは，ＫＶＡ当り700ドルから900ドル，これに設置および設置場所改装費（空調設備の追加及び床の補強）をプラスした程度である。

充分な容量を与え，負荷の故障を除去し，ＵＰＳの故障に対し保護するため，図3-3のようにＵＰＳとコンピュータ負荷との間に静止トランスファー・スイッチを挿入することができる。静止スイッチに対する制御回路は過電流状態を感知し，大きなトランジアントを起すことなく第一次電源に負荷をスイッチすることができる。

全負荷が100ＫＶＡ程度を越えた場合，図3-4に示すように複合，独立のUPS装置を経済的に使用することができる。各装置が独立にスイッチを持っているため，何らかの理由で故障するような場合，オフラインに切り換わるようになっている。

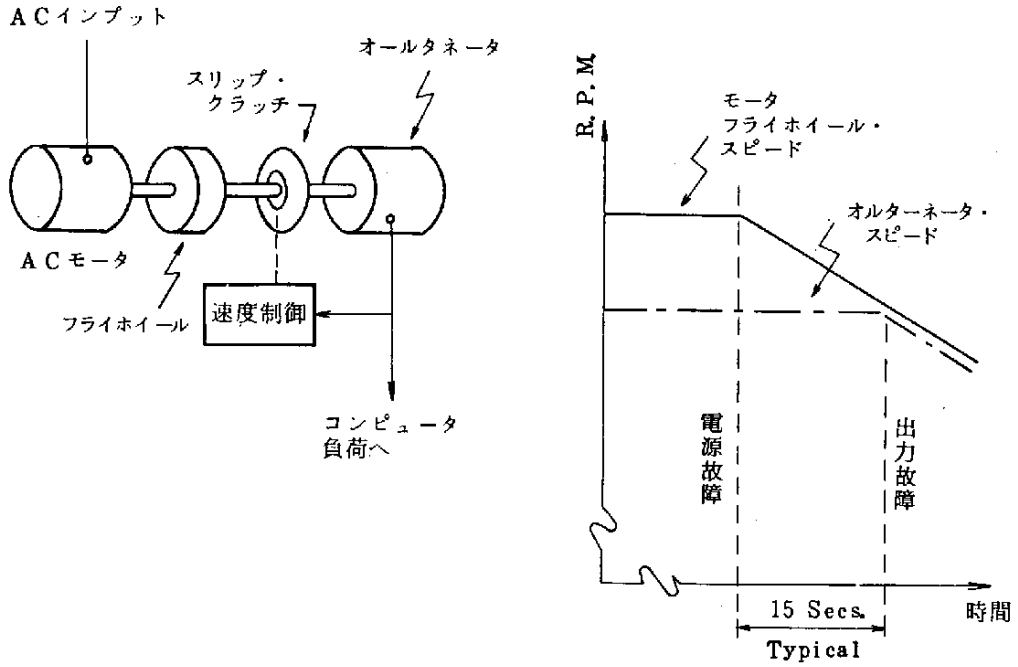


図３－１フライホイール・エネルギー貯蔵装置付
代表的モータ・オールターネータ

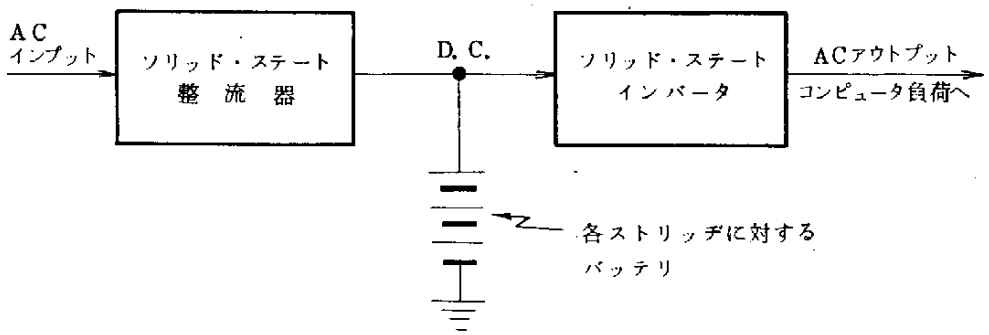


図３－２不断電源の単純化ブロック・ダイヤグラム

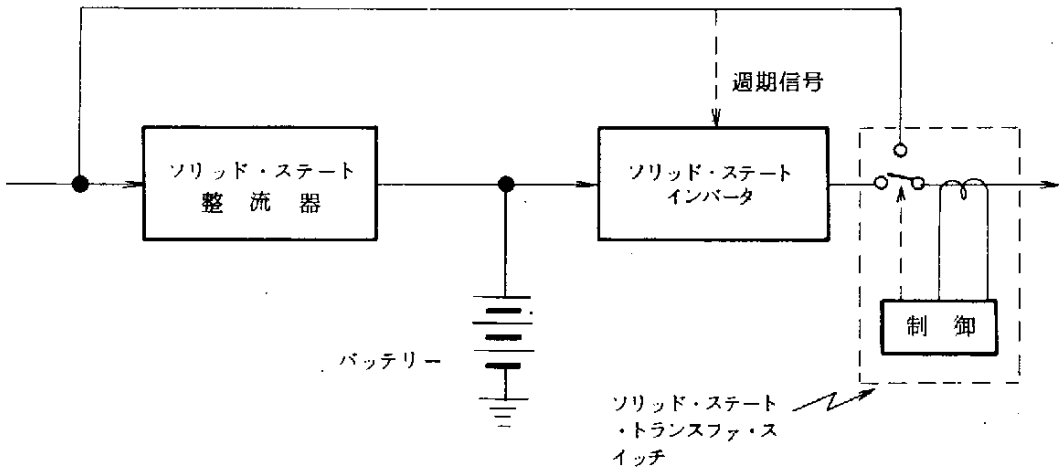


図３－３トランスファ・スイッチ付ＵＰＳ

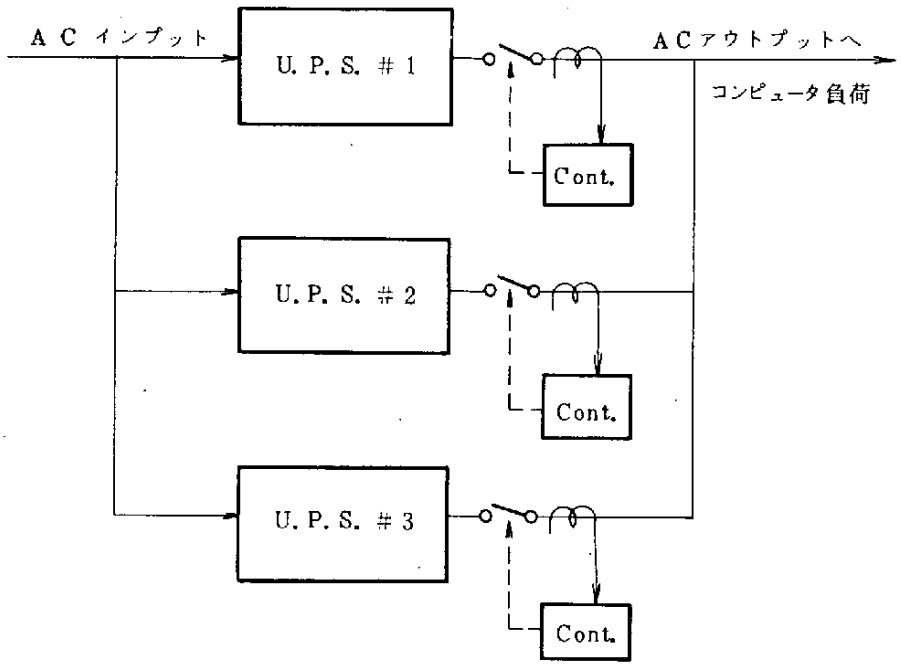


図３－４複合独立ＵＰＳ装置

最後に，30～45分を越える停電による大きな損失を示した場合，ＫＶＡ当り約100ドル，プラス架設および用地準備費で図3-5に示すような，オンサイト・ジェネレーションを取り付けることができる。原動機はディーゼル・モーターもしくはタービンでも良い。外部電力が故障した場合，制御装置が自動的に原動機を始動させ，原動機が発動機を動かす。この点において，ＵＰＳは発動機側に切り換わる，ハードウェアの故障を防止して，システムは原動機に燃料油がある限り，接続負荷を支持する。発動機は空調，最小照明等の主要負荷およびＵＰＳ負荷をサポートするのに十分大きくなければならないことに留意する。

以下に示すように，配置の仕方は多様である。これらの測定の1またはそれ以上がコスト的に妥当とみられる場合，特定の配置を決定する前に，最良の性能仕様および建物の電力分布への統合の問題に対する最良の解決策を決定する上で専門家の援助を求めるべきである。更に，上述の大まかなコストの指針に加えて，特別な設置コスト，装置が必要とするフロアの費用，装置保守費用，付随電源の費用（装置が消費する）を考慮しておかなければならない。これらのコスト・ファクタが複雑であるため，その分析には面倒な手順が必要となる。ここでの議論はＡＤＰセキュリティ・プランナーが詳細な分析が保障されているか否かを決める上で十分な情報を提供するものであることが望ましい。以上のことは「不切断電力供給（ＵＰＳ）システムに関するコンサルタント・ガイド」〔57〕に収録されている。

火事，洪水もしくは他の緊急事態が発生した場合，迅速に容易に，かつ選択的に電源を遮断できるということが非常に重要なことである。第一に，各装置の上にある電源切断スイッチを使用するという方法がある。ただし，この場合，内蔵の電源切断スイッチを含む（ここまでの）電力ケーブルおよび回路がまだオンされたままであることに留意しなければならない。これらは，配電盤にあるブランチ・サーキット・ブレーカを手動でトリッピングすれば解除される。次にこの操作を容易に，かつ効果的に行なうために，いくつかの条件を整えておくべきで，配電盤はコンピュータ室に設置し，配電盤に対するアクセスは障害のない状態でな

ければならない。また，配電盤が他の装置の陰にかくれたり，近づきにくい例は稀れである。各サーキット・ブレーカはどのサーキット・ブレーカが各々のハードウェアと接続しているが正確に，かつ迅速に分るようにはっきりと印を付けておく必要がある。最後に，部屋の照明を除くコンピュータ室の負荷の電源すべてを切断することができるようにする。この操作は所要の切断スイッチを付けることによって行なうことができるが，設置場所がコンピュータ室からある程度離れていることが考えられる。この問題を解決するために，ＲＰ－１（〔９〕2.1.1に前出）では，マスター・コントロール・スイッチ（これを押すとすべての電子機器に対する電源が切れる）がコンソールの近く，コンピュータ室への各主要入口の内側に設置することを要求している。NFPA基準№73〔34〕では排気装置に対する電源も切断されていなければならないとし，しかし，これは初めに第3.2節に述べたファクターを考慮すべきであると指摘している。このマスター・コントロール・スイッチは重要な緊急動作を行なうものであるが，その不注意な操作は装置を破壊する可能性が強い。このため，このスイッチが操作別に明瞭なマークが付いているか，その操作に関し慎重さを要求するようにデザインされているか否かをチェックすることが重要である。したがって，マスター・コントロール・スイッチは床面上約６フィート（約2.0メートル）位置するプラスチックス製の箱に入れて置くのが望ましく，これにより，偶然の操作，もしくは不注意の操作が起る可能性は非常に少いように思われる。

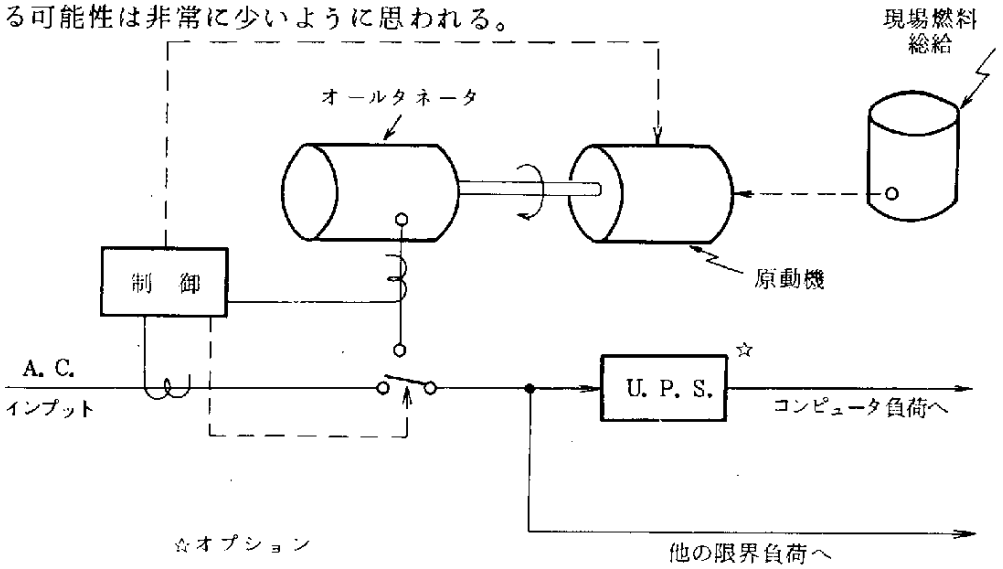


図３－５オンサイト・ジェネレーション付ＵＰＳ

先に述べた論議を明瞭にするために，図３－６に，標準的な建築物配電システムのワン・ライン図表を示してある。上部を起点として，逓降変圧器，切断器及び過電流防止装置（フューズ）を通じて電流が流れ，各配電盤に到る様子が分かる。各配電盤は，遮断器で保護され，各ハードウェア・ユニットに接続する分岐回路を備えている。この基本的な配置については，品質又は信頼性を高めるために数多くのバァリエーションが可能である。第一のバァリエーションとして，高馬力モーター等のトランジャントを生じさせる装置から，ＡＤＰ回路を分離する場合がある。他の条件が全て同じ場合，ＡＤＰ装置と変電所との間の距離に比例して，給電線の破損の可能性が増加する。給電線の破損が有意な脅威をもたらす可能性がある場合には，通常，第二の給電線（異なる変電所からの給電線である事が理想）をＡＤＰ装置に引く事ができる。破損が生じた場合に，一次給電線から予備給電線に切り換えるための切り換えスイッチ（手動又は自動）を使用する。これに替えて，ＡＤＰバス・バー，ＡＤＰ空気調整，非常照明，安全用ハードウェア等の限界負荷を分離し，全く別の配電システムを通じて，これらに給電することもできる。この場合には，限界負荷の部分のみを，予備給電線に切り換えるものとする。この処置によって分離が保証され，全建築負荷を負う必要がないため，予備給電線のコストが軽減される。この処置が，コスト上昇に対して，主要な抑止力となると考えられる。

ＡＤＰセキュリティ・プランナーは，建築監督又は土木工事スタッフの支援を得て，配電システムについて，以下の点を点検せねばならない。

(a) 電線が全国電力法（National Electric Code）〔55〕，NFPA 75号〔34〕及びＲＰ－１〔９〕に合致しているか否か

(b) 電力保守作業と，コンピュータ室，空気調整又は通信施設用電力の不注意による遮断を避けるためのＡＤＰ操作との調整を可能にする手順が，建築監督との同意に基づき，設けられているか否か。手動切断器に，コンピュータ室の「up stream」のラベルを貼る事が望ましいが，妨害者に合図を送るような結果になる方法はよくない。

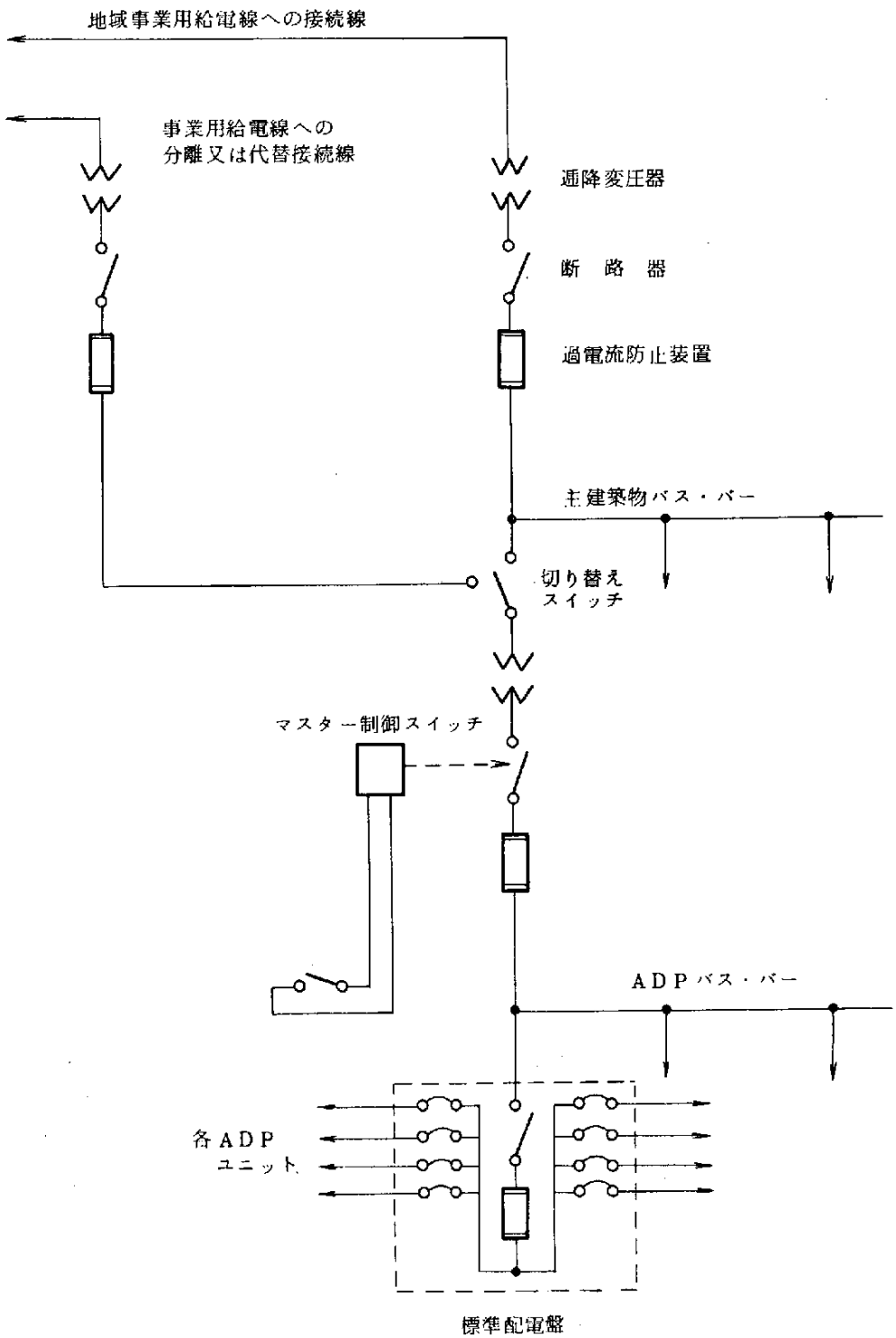


図３－６配電の概略ワン・ライン図表

(c) 全ての配電設備が，不時の破損又は妨害行為を物理的に，適切に防止しうるか否か。防止措置には，電気設備室及び納戸への通路の点検，電話線用電柱及び外部変圧器用パットを車両による破損から保護するための防壁，火災の延焼の回避等が含まれる。

要するに，電力の特性及び信頼性がＡＤＰ設備の要請に見合う事を保証する適切な措置をとる事が必要である。これらの措置には，危険性の分析及びコスト要因に基づく，配電システムの配置，２重給電線，トランジアント　過装置，非遮断式給電方式，ブラウンアウト用補償装置，現場発電機の変更，及びいたずら，妨害行為又は事故の物理的防止が含まれる。更に，配線は，適用しうる法規に従い，防火計画により適宜に統合されねばならない。

4.3.2 空気調整

コンピュータ室の空気の適切な調整は，３つの理由から重要である。第１に，電子回路の構成部分は，不規則な操作を最小限に抑えるために，極めて厳密な温度限界を必要とする。温度が高い場合（30℃以上）には，ＡＤＰハードウェアに恒久的な損害が生ずる場合がある。第２に，製表カード装置及びテープ装置の正しい操作を保証するために，湿度調整が必要とされる。湿度が高すぎる場合には，カードが吸水膨脹し，不規則な給電が起る場合がある。湿度が極めて低い場合には，テープ・ハンドラー，ライン・プリンタ，時には，ＡＤＰハードウェア自体に影響を与えうる静電気の蓄積を引起しやすい。最後に，ディスク装置のヘッド破損を生じさせるような腐食，伝導性又は広範な汚濁に，室内の空気が汚染されていない事が重要である(*)。温度，湿度又は汚濁の調整が行なわれない程度に応じて，ＡＤＰ操作は妨害され，ハードウェアは損害を受ける。極端な場合には，

（＊） ある種の給湿気は，水を霧状にさせて，それを空気中に噴射させる。この種の給湿気は，水分中の鉱物がＡＤＰハードウェアに堆積するため，硬水地域では，使用すべきでない。

状態が矯正されるまで，操作を中断せねばならない場合も出てくる。更に，コンピュータ室が建築物全体を占める空気調整システムの一部である場合には，建築物の他の場所における火災による煙がコンピュータ室に流入する場合がある。

これらの潜在的な危険の可能性を正しく評価するために，ＡＤＰセキュリティ・プランナーは，建築監督と共に，ＡＤＰ設備用空気調整システムを綿密に点検せねばならない。図3-7には，概略的に，標準的な空気調整システムを記してある。このシステムの心臓部は，エア・ハンドリング・ユニット（ＡＨＵ）で，これを通じて，コンピュータ室の空気がファンにより循環する。ＡＨＵの機能は，温度及び湿度の調整，空気の濾過である。室内の空気を清浄化するためには，外壁のルーバを通じて外気を引入れ，内気と混合する。この他，排気用ファンを取り付ける場合もある。

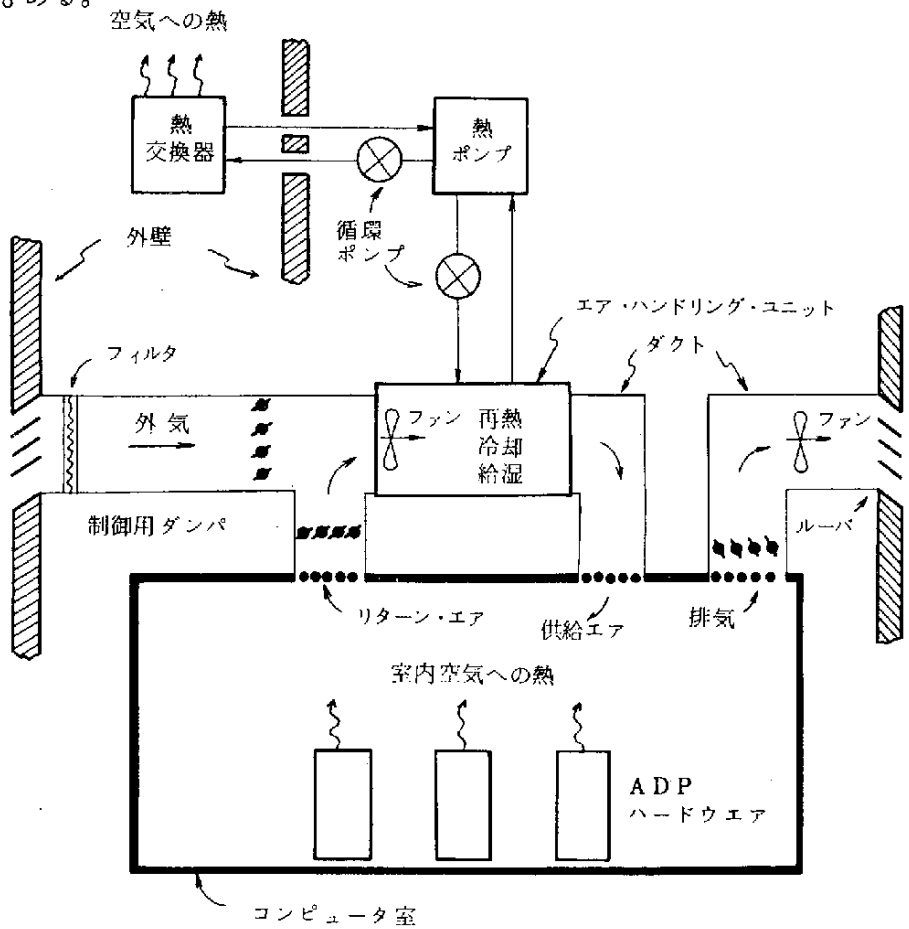


図３－７標準空調システムの概略横断面図

空気は，通常薄板金で作られたダクトを通じて流れ，空気の配分は，モーター付ダンパで調整される。ＡＨＵは，自らの機能を遂行するために，低湿期間中は，給湿のために，水又は蒸気を供給し，室内の空気から除去された熱を排出する手段を採用せねばならない。後者については，冷凍剤（例：冷水）を循環させる一種の熱ポンプ（冷却機，直接膨脹ユニット等）をＡＨＵに連結する方法をとる。同様の趣旨から，熱ポンプには，熱を発散させる冷却塔又はコンデンサ等の装置を取り付けねばならない。

システムの各エレメントの実際の配置は，システムの規模と地域の条件による。例えば，標準的な住宅用ウインド型空気調整器には給湿以外の全ての機能を，単一のユニットにまとめたものを使用する。コンピュータ室には，吸・排気及び熱交換を除く全ての機能を果す，いわゆるパッケージ式空気調整ユニットを使用する場合が多い。大きな建築物においては，コンピュータ室用ＡＨＵと同様の快適な空気を供給するための１機又は数機の熱ポンプを使用するのが極めて普通になっている。これまでの論議から，ＡＤＰ操作に対して様々な結果をもたらす故障が多くの様々な装置に発生することが考えられる。主な破損の形態，その影響及び考えられうる対策を，一般的な言葉で，表３－２にまとめてある。

表３－２

破　損	故　障　の　状　態	対　　策
外気用ダンパ，ファン	外気が無となるか通常は臨界値以下	外気の出所を複数とする
ＡＨＵファン	空気循環がとまる温度の上昇	ＡＨＵファンを複式とする
ＡＨＵ湿度調整装置	湿度調整の不機能，外気湿度が極めて低いか高い場合には臨界となる	ＡＨＵ湿度調整装置を複式とする
ＡＨＵ温度調整装置	温度の上昇	ＡＨＵ温度調整装置を複式とする
循環ポンプ熱ポンプ又は熱交換器	温度の上昇	影響を受けたユニットを回路からはずせるよう複式ユニットとする。暫定的に外気及びフロア用ファンを使用する

破損の影響を最小限に抑えるためには，影響を受けたユニットを回路からはずしたり，緊急の場合に外気を使用したりできるように複式ユニットを使用することができる。例えば，コンピュータ室に50トンの冷気を要し，建築物の平衡が快適な空気調整に100トンの冷気を要し，水冷システムを使用する場合を想定してみよう。2つの異なるシステム配置を以下にまとめてある：

単　　式		複　　式	
150トン用冷却機	1機	50トン用冷却機	3機
冷水循環用ポンプ	1機	冷水循環用ポンプ	3機
50トン用コンピュータ		20トン用コンピュータ	
AHU 1機	1機	AHU	3機

単式システムが要件を満すとなれば，設備の部分のいずれが破損しても，ADP操作は数分から30分停止を余儀なくさせられると思われる。複式システムは幾分コスト高となるが，特定のユニットの破損も緩和することができる。1機又は2機の冷却機又は循環ポンプが故障した場合でも，建物内のバランスを保つよう空気調整の程度を落す事で，コンピュータ室の空調を行なうことができる。コンピュータ室のAHUが故障した場合には，熱負荷を落す事で操作を継続することができる。熱負荷の軽減は，照明を減らし，重要性の低いADPハードウェアを遮断する事で実現できる。

緊急措置，通常のエネルギー保護の双方の手段として，温度，湿度が十分に低い場合に，外気を冷却用に使用することができる。外気の温度と冷却効果との関係は，最大許容室周囲温度又は装置吸気温度（双方又はいずれかを規定することができる），エア・ハンドラー及びダクト内に生ずる熱量，使用される外気（再循環の暖気と反対向き）の量，の3点に負うところが大きい。現在の空調装置は，外気のみの吸入を可能にするダクトと通気の改良を行なう事ができ，効果を高める事のできるものもあるが，大半は，外気のみの吸入は不可能となっている。

外気の吸入と室内空気の排気を100％保証した場合には，AHUへの吸気温度

とコンピュータ室内のもっとも暖かい地点の温度との差が15°F(8°C)まで許す事が可能である。したがって，コンピュータ室内の最大許容温度を90°F(32°C)とした場合，使用される外気の最高温度は75°F(24°C)付近となる。しかしながら，これについては，機器の仕様及び空調設備の配置に基づき，各装置ごとに決める必要がある。

極めて緊急の場合，コンピュータ室内の空気を建築物の他の部分に排出するためのフロア・ファンを使用することもできる。

現在取り付けられているシステムの信頼性を査定する場合には，これまでに述べた要素，過去の破損及び修理に要すると予想される時間を考慮する必要がある。修理時間については，予備部品及び有資格修理要員の利用しうる程度にかかっている。建築土木工事スタッフは，信頼性の査定及びより信頼性の高い別の装置の採用に関して，アドバイスを与えることができる。パフォーマンスを監視するための温度・湿度計を1機又は複数取り付けることも望ましい。正常な操作を保証するために週毎に，記録を点検し，誤まった又は不適当なパフォーマンスを発見し，原因を究明し，矯正作業を行なう事が必要である。これらの計器の内，1機は，週毎の比較が可能なように，中央位置に固定して維持するものとする。コンピュータ室では，1,000平方フィート(100㎡)を上回る表面積を，付属固定ユニットが占める事が望ましい。均等な温度配分について，問題が生じた場合，抜き取り検査用の付属レコーダを取り付ける事が有用となる。

コンピュータのハードウェアは汚れやさびに比較的弱いため，外気の取り入れ口や濾過装置が重要となる。吸気用ルーバが地表面に置かれている場合には，過度のほこりや危険な煙が吸込まれる危険性がある。吸気用ルーバ近くにいたスカンクが草を刈っていた維持作業員を悩ませた例もあった。このにおいで，3階建てのビル全体の排気を行なわねばならない羽目となったのである。更に重要な事は，フィルタが適切であるか否か，定期的に点検され，必要に応じて清掃，交換されているか否かを確認する事である。

空調システムは，建築物内の空気を移動させるために使用されるため，火災を

予報でき，火災中でも操作をコントロールできる事が重要である。図3-7 を参照すると，リターン・エア用ダンパを閉じ，吸排気用ダンパを全開する事で，空調設備を，コンピュータ室から煙を排気する目的に使用できることがわかる。迅速な煙の排除が損害を抑え，消火活動を可能にするため，空気調整の完全な停止よりも，この処置が好ましい。ただし，煙が建物の他の部分に入り込んだり，ダクトが高温になったりした場合には，運転停止が必要で，これは，第 3.1 節に記した主制御スイッチの機能の一部に含まれる。

図3-8 には，標準的なビル用空調システムが記してある。リターン・エアとフレッシュ・エアがビルの最上階で混合され，ＡＨＵを通り，主供給ダクトを通じてビルの各階に配分される。このシステムでは，防火用ダンパが取り付けられていない場合には，１階での火災の煙がたちまちビル中に広がってしまう事が図からわかる。更に，ダクトの管路が，火災の延焼の通り道となる場合も考えられる。最近のＡＤＰ設備の火災の際には，空調用ダクトが地下の天井に沿って火の通り道となり，フロアのスラブの穴を通じて１階のコンピュータ室に延焼した。地下に保存されている包装材料から出火した時には，これらのダクトがすぐに壊れ，熱と炎がコンピュータ室に及び，ハードウェアと備品に極度の損害が生じた。このような理由から，空調システムは，ＲＰ－１〔９〕に規定されている通り，ＮＦＰＡ基準９０Ａ号〔28〕に合致せねばならない。図3-8 には，多くの要件が記されてあるが，それを要約すると以下のようになる。

- ダクトが防火壁を通る箇所では，防火壁に，自動式防火ドアを取り付ける。
- 延焼を抑止するための防火用定格壁，垂直立坑の開口及び他の同様の箇所には防火用ダンパを取り付けねばならない。
- システムを煙や高温空気から保護するために，ダクトの適当な位置には煙・熱探知機を取り付け，非常停止用調整装置を備える事が必要である。

ＮＦＰＡ基準90Ａ号〔28〕も，ダクト，フィルタ及び他の部分が不燃性でなければならない事，電線及び電気設備が全国電気法〔55〕に合致せねばならない事，一般的に言って，空調システムが火災延焼防止を目的とした建築物の特徴を損な

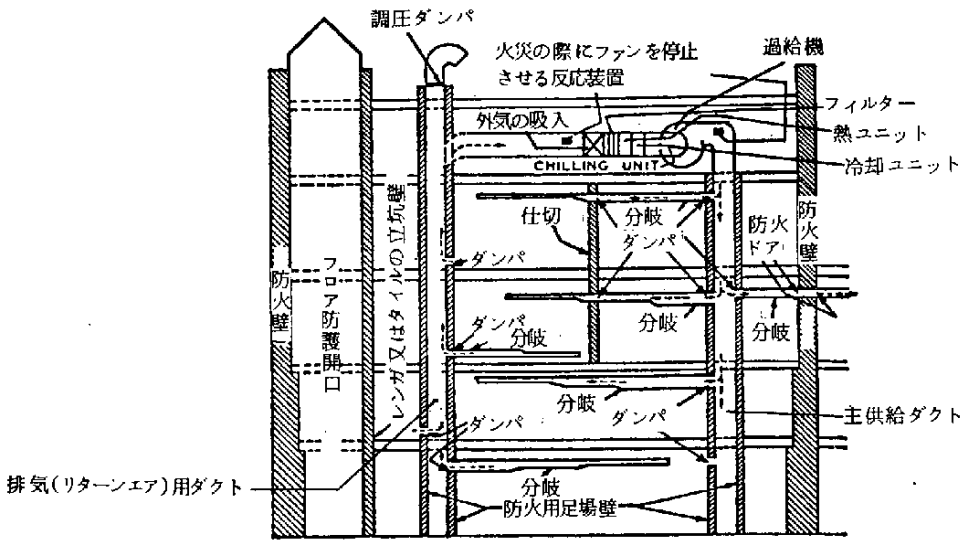


図３－８ 防火ビルの標準空調システム

ってはならない事を規定している。同基準には，先に述べたコンピュータ室の煙排除システムが安全に使用しうるか否かの決定基準も含まれている。キーとなる要素は，高温ガスを処理するシステムの能力及び人命救助目的に関する効果である。要するに，ＡＤＰセキュリティ・プランナーが，防災効果を果すビルの空気調整の操作を理解し，ＡＤＰ設備の保護に要する矯正活動を見きわめる事が，最低限の照明，空調に要する電気量の他，ＡＤＰ装置用の電気量も維持するべき旨が記されている。したがって，空調システムの効率は，システム自体の運転コストのみならず，非常用発電機の大きさとコストにも影響を与える事になる。ＡＤＰ空調システムの運転に要する電力はかなりの量に上り，ＡＤＰ設備，照明及び他の負荷が要する電力の 40％～75％である。この事は非常の際に除去される負荷１キロワットあたり，入電力量が約 1.5 キロワット軽減される事を意味している。

重要な設計上の条件として，エネルギーのコスト及び無効率，非常用発電機の基準を考慮して設計されているＡＤＰ空調システムは少ない。これが，コンピュ

ータ室内が実際に，72～75°F（22～24℃），50％ＲＨ，露点52～55°F（11～13℃）に維持され，冷却に使用される冷却水が，水温42°F（6℃）で供給されるという実態の1つの理由となっている。したがって，冷却用ユニットは，常に，空気から水分を抽出する結果となっている。この点が冷却効率を落し，相当量の余分のエネルギーを要する原因となっているばかりでなく，通常，蒸気噴射（これがまた冷却を妨げる）で行なわれる給湿（相対湿度50%の状態に戻す）に更に別のエネルギーが必要となるのである。現在の空調システムでは，相対湿度を下げる，コンピュータ室温を下げる（特に，再循環される空気が冷却されている場合），冷却水の温度を上げる（この場合，冷凍／圧縮コストが軽減できる）という3つの処理の内のいずれかを行なって，エネルギーの軽減をはかっている。新しい設備では，非常用発電機の必要性と石油コストの上昇が，最良の解決をはかるにあたって，新たなファクターとして付け加わっている。

以上の提言を実現するにあたっては，ＧＳＡを通じた暖房・空調専門家又は企業の設備担当の建築技師による徹底的な点検を受けねばならない。静電気による障害が生ずる可能性があるため，相対湿度が35％RH以下になってしまうような特意な湿度低下が起きないかどうか，設備製造業者に確認せねばならない。

4.3.3 通信回線

ＡＤＰシステムが，迅速なデータの入出力のために通信回線を使用する傾向がますます強くなってきている。通信回線の信頼性及び完全性がＡＤＰ設備の規準に合致する事を確認する事が重要である。図3-9には，標準的なテレプロセシング設備の配置が記してある。固有のテレプロセシング設備で，図3-9に記してあるエレメントの内の1つ又は複数を使用することができる。原則として，コンピュータと，各ターミナルを結ぶ回線との間のインタフェイスとして働く特定のハードウェア・ユニット（ここでは，メッセージ・プロセッサを言う）が存在する。回線は，硬質ワイヤ製ＤＣ回線でもよく，図に記されている変復調装置を使用し

てもよい。ターミナルは，リースト・ライン，アクセス用ダイヤル・アップ・ネットワークのいずれかを用いて，**「スタンド・アローン」**の状態でもよい。ターミナルは，**マルチ・ドロップ・リースト・ライン**を共有する数個のターミナル（通常は数地点）の内の１つ，又は**コンセントレータ**を通じて高速リースト・ラインを共有する数個の低速ターミナル（通常は同一の地点）の内の１つであってもよい。標準的には，ダイヤル・アップ・コールの毎分ごとの料金，ＷＡＴＳ（広域電話サービス）のリースト・ラインの月間料金，ターミナル，変復調装置等のリース経費又は資本費用を計算し，総直接費用を最少限にできる配置が選択されている。しかしながら，通信の不通から生ずる遅延経費が有意なものとなり，信頼性を高めるための措置の直接費用を引出す口実を与える場合がある。危険性の分析によって，プロセシングの遅延で有意な損失が生ずる可能性が指摘された場合には，ＡＤＰセキュリティ・プランナーは，不通の程度及び期間の見積り，コストとして引き合う修復措置の検討にとりかからねばならない。以下が，起りうる不通の形態である。

メッセージ・プロセッサの１チャンネル、ローカル変復調装置，分局と接続する１電話回線のいずれかが破損した場合。破損エレメントが修復されるまでは，１チャンネルが使用不能となる。破損時にそのチャンネルが動作中である場合には，不完全なメッセージの伝送が行なわれる。ダイヤル・アップ・ネットワークを通じてアクセスが行なわれている場合には，リモート・ターミルで，ＡＤＰシステムのアクセスを行なうことができる。ただし，回線が詰っている時間には，待ち時間が長くなることもある。リースト・ラインを通じてアクセスが行なわれている場合には，不通となった回線に接続したリモート・ターミナル(*)のみが影響を受ける。メッセージ・プロセッサ回線の不通は，ユニットが修復されるまでは直らない。ただし，不通回線にすみやかに取って代わりうるスペース回線があ

(*) マルチ・ドロップ回線又はコンセントレータ回線の不通が複数のターミナルに影響を与える場合もある事に注意。

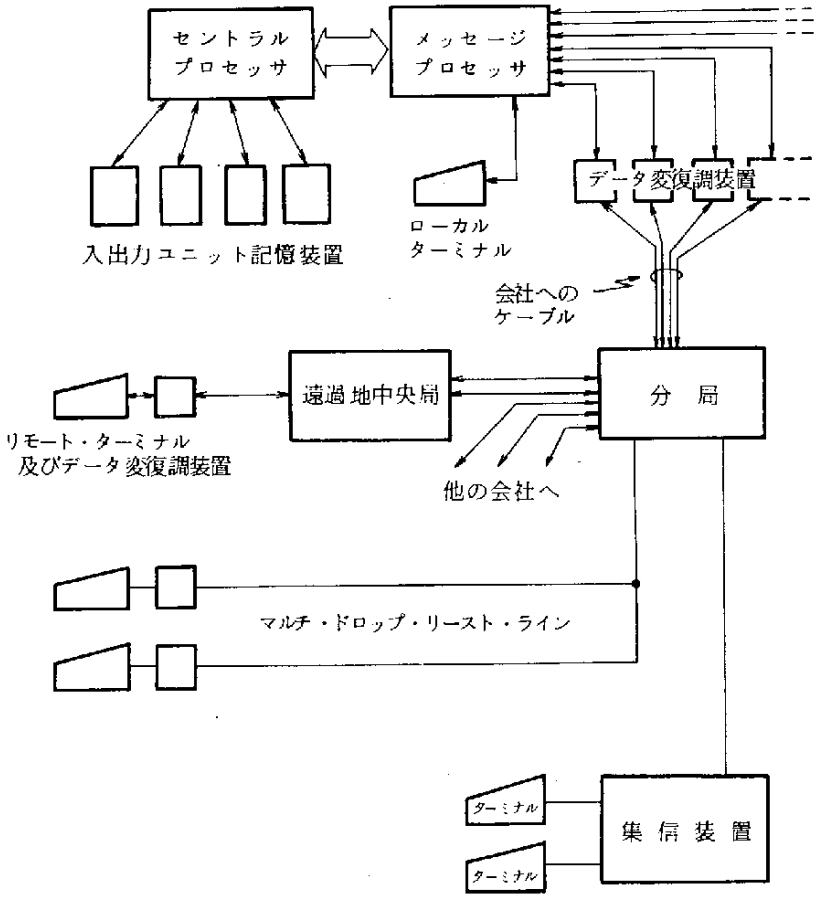


図 3-9　標準のテレプロセシング設備の配置

る場合にはこの限りではない。

破損した変復調装置を代替ユニットに替える事は，概して，比較的容易でなければならない。分局に接続する回線の修復は，大半の場合，数時間以内に終わるが，危険性の分析で，1回線又は複数のスペース回線を必要とする場合もある。

メッセージ・プロセッサ全体，分局に接続する全回線，中央局自身のいずれかが破損した場合。全リモート・ターミナル，メッセージの伝送が不能となる。メッセージ・プロセッサの破損が3つの内もっとも起りやすく，修復時間も極めて長くかかる。ＡＤＰ安全設計者は，ユニットの以前の状態について，販売業者に質問し，これを検討した後に，破損率及び平均修復時間の見積りを行なわねばな

らない。危険性の分析に基づき，コストが引き合い，技術的に可能であれば，単式ユニットの破損が大損害をもたらさないように，共通の伝送量負荷を共有する複式ユニットを取り付ける事を選択することもできる。ＡＤＰセキュリティ・プランナーは，地方電話会社又は連邦電信電話システム（ＦＴＳ）の代表と協議の上，別の中央局に分離回線網を敷設する事が実用性をもつか否かを裁断することができる。中央局に接続する全回線の不通の可能性が極めて低い場合でも，決してゼロとはならない。1973年6月には，泥棒が盗難防止用自動警報機中央ステーションに接続する電話ケーブルを切断した事件が報告されている。泥棒は，中に押し入り，ケーブルが修復される前に，敷地内の備品を盗んでいった。この事件は，妨害行為や破壊行為の可能性が存在する事を示唆している。ケーブルは，この他，建設工事の掘削，着水を起す暴風雨，電話線用電柱の倒壊，マンホール爆発，洪水，建物内の火災，地震等の危害にさらされている。

分局からリモート・ターミナルに到る回線の不通，ターミナル又はその変復調装置の破損の場合。1つのターミナルのみに影響を与え，ＡＤＰ操作には関係しないため，不通の可能性はもっとも低い。ターミナル又は変復調装置の修復時間は，販売業者のサービスをどの程度利用しうるかにかかっている。ターミナル及び変復調装置の予想破損率，その平均修復時間を見積った上で，ＡＤＰセキュリティ・プランナー及びターミナルの利用者は，あらゆる損害の可能性を予想し，代替設備がコスト的に引き合うか否かを裁断することができる。遠隔地に多くのターミナルが存在せず，業務がさほど緊急を要しない場合には，代替設備の設置の必要性は薄いと言える。

不通の形態をこのように概略的に分析してゆくと，ＡＤＰセキュリティ・プランナーが配慮すべきいくつかの点が明らかになる。

ダイヤル・アップラインとリースト・ライン。伝送量が多く，ダイヤル・アップ料金よりリースト・ラインが安くつく場合又はデータの伝送率条件を満す回線が必要である場合には，一般に，リースト・ラインが選択される。リースト・ラインには，ダイヤル・アンプ・ネットワーク固有の信頼性と柔軟性に欠けている。

利用者がアプリケーションに緊急性を要求する場合には，追加リースト・ライン又は予備ダイヤル・ラインを敷設することもできる。ただし，予備ラインを完全に利用するためには，ハードウェア（回線交換），ソフトウェア，および操作手順を整える事が必要である。最後に一言付け加えれば，ダイヤル・アップは，外国のターミナルにシステムをさらすことになる。

ＡＤＰセキュリティ・プランナーは，通信回線の信頼性及びその平均修復時間を調査すると同時に，災害時に，替わりの場所で，**通信を再開する**措置を検討せねばならない。ＡＤＰ安全設計者は，更に，他のリモート・ターミナル又は現場入出力装置等の利用者の入出力を処理する代替措置を考慮せねばならない。この情報は，第８章に記す予備計画の発展に鋭い刺激となるであろう。

ＡＤＰセキュリティ・プランナーは，**テレプロセシング・ソフトウェア・ハンドル**が故障する形態を調査せねばならない。キイ・ポイントは以下の通りである。

- コンソールの故障および有用な診断メッセージの生成の確認
- 割り行みメッセージの正しい取り扱い。とりわけ，ファイル最新情報に影響を与える可能性がある場合。
- 故障チャネルを調整しうるソフトウェアの柔軟性及びチャネル又はターミナルの交換に関する利用者の再委託。
- 予備入出力手段を調整するための代替ソフトウェア。

最後に，通信回線の安全性か検査されねばならない。ターミナル・ボードや他の装置は出入りを制限できる錠付きの室に収納するものとする。ケーブルについては，出来れば，堅牢な導管に収納し，物理的損害を防がねばならない。電話システムの変更及び修理を調達するための手続きを確立せねばならない。地下ケーブルの位置をＡＤＰ設備現場図面に記す場合には細心の注意を払い，後の堀削の際には，正しい計画をたて，ミスによりケーブルを切断しないよう厳しい監督を行なうものとする。

通信回線は巧妙ないたずらの対象ともなる。１９７１年の新聞記事(*)はストライ

(*)　「電話妨害行為」Computerworld　１９７１年１２月１５日　Ｐ１

キ参加者がシステムの妨害行為をなしたと記している。報告に依れば，コンピュータのポーリング・コマンドはテープに記録され，次に，ダイアル・アップを経て，離れた端子に送られた。その結果は，コンピュータによる端子の付随的なポーリングを防止することであった。25の端子がほぼ1ケ月間影響を受けた。この例は，"ソフトウェア・サボタージュ"と呼ぶべきものの可能性を示している。ＡＤＰセキュリティ・プランナーはコミュニケーション・ソフトウェアおよび手順を再検討すべきであり，仮に，タンパーリングに顕著な露出がある場合，その露出を軽減する修正を確認し，迅速な修復を保障し，考えられる損失を最小限に抑えなければならない。

ワイヤ・タッピング；メッセージ・インターセプト，変更，回送などダイアル・アップネットワークを通じての未公認ユーザによるアクセスおよび他の制御アクセシビリティについては，本書では省略する。

4.3.4 その他のサポート装置

電力，空気調和とコミュニケーションは，明らかにＡＤＰ操作に重要であるが，その他の装置もまた通常の操作に必要とされうる。

以下は検査をうけるべき可能性のある諸事例である。

給水　なぜなら水は空気調和システムや暖房装置に必要とされる公算が大きく，水圧の減損は操業の停止をもたらしうるからである。飲料水や消火用水の一時的な減損は，即座に操業の妨げとなる可能性はないであろう。水は，マイクロフィルムやその他の写真メディアの製版にもまた必要とされうる。

エレベーター，とくに高層ビル内においては，人間やデータや供給品の移動にとって重要である。電力事故の場合を除いては，全てのエレベーターが同時に故障することはありえない。しかしながら，もし1台のエレベーターの操作を保持することが必須とされるならば，オンサイト発電機を準備しなければならない。それは，当然のことながら，ＡＤＰハードウェアにも必要とされうる。

いくつかの大施設では，内部での**メイルコンベイヤー**や気圧式伝送機が，ソースドキュメントやアウトプットを配送するために使用されうる。また，必要な場合には手による配送に代替することも考えられるが，ＡＤＰセキュリティ・プランナーは，このことを確認し，事故が発生した場合，輸送中の緊急を要する資料が装置内にトラップされうるかを検討しなければならない。

場合に依っては，**建物の暖房および空調**は建物外部で発生する蒸気によって行なうことができる。この場合，ＡＤＰセキュリティ・プランナーは，代替ソースもしくは突発的事故に対する計画における特別な準備の必要性を検討するためソースの信頼性及び故障の影響を調査しなければならない。建物の暖房および空調は公益企業による天然ガスに依存している場合がある。この際配慮すべきことは外部蒸気源の場合とほぼ同様である。仮に，不切断の電力供給が必要であると判断された場合，危険分析を行なうことにより，現場補給電源のコスト面での妥当性が明らかとなるであろう。

上記のこと及び関連事項の分析を行ない，コストおよび対策の可能性を検討するために，ＡＤＰセキュリティ・プランナーは資格を有する専門家（ビルの管理者から技術専門家の中でプランナーにとって可能な者）の援助を求めることが必要である。

暖房，空調，電力との相互関係のため，最近のビルの多くはいわゆる全面エネルギー・システム（ＴＥＳ）を利用している。簡単に言って，ＴＥＳはこれらのエレメントを単一システムに集約し，上述の三機能すべてを付与したものである。代表的な例を挙げるならば，電力は現場で作られ，排出熱は建物の暖房に利用されている。報告例によると，全コストはシステムが個別になっている場合よりも低く，エネルギー源に対するコントロール上の利点があるということである。このことは，信頼性および特性がユーザーの特殊な要求に合せることができるということを意味している。このため，新たに設備を考慮する場合，ＴＥＳを検討してみる価値があるといえる。しかしながら，ＡＤＰセキュリティ・プランナーは，それ以前のシステムに適用したのと同様の特性および信頼性に対する基準を適用し，ＡＤＰ装置の必要条件が実際に満されていることを確認しなければならない。

4.4 コンピュータ・システムの信頼性

4.4.0 まえがき

コンピュータ・システムの信頼性は，間違いなく，ＡＤＰ操作にかかっている。しかしながら，その信頼性を何に帰すべきかがしばしばはっきりしないために，コンピュータの信頼性は適切な処置を必ずしも受けていない。この章では，３つの基本的な領域 — 現存するコンピュータの信頼性，保守マネージメント，新しいシステムの導入，についての紹介と方向について述べている。

4.4.1 コンピュータ・システムの信頼性

典型的なコンピュータは，割り当てられたデータ処理業務を達成するために必要な機能を果たす多くの相互に連結された装置からできている。最も簡単な場合には，コンピュータは，単一の業務を達成して，その業務に必要な最小限のハードウェア・エレメントを使用するように配列される。だから，エレメントのいづれかでも故障した場合には，操作は停止する。もっと典型的な，多様業務については，すべての業務でコンピュータの装置全部を使うとは限らない，そこで，ひとつふたつの故障は，必ずしも全業務の達成をさまたげるものではない。大部分のコンピュータは，ジョブの流れをコントロールし，メモリーと，周辺装置を個々のジョブに割り当てるためにオペレーティング・システムを用いる。各々の特徴に従ってオペレーティング・システムは，ハードウェア，警報装置の指示を受けて故障を探知し，その故障の箇所を確めたり，制限するように試みる，そしてコンソール・オペレーターに連絡し，ジョブの流れの調節を，操作持続が可能な業務量が最大値になるように合わせる。

もちろん，セントラル・プロセッサのコントロール・ロジックに欠陥が生じた場合は，ふつう，操作は停止する。（しかし，欠陥が探知されないままであれば，アクセスを調節するハードウェアを損傷する恐れがあるということに注意。）同様に，周辺装置の一部分の故障もそれらを使うすべての業務を妨げる。このように，故障が生じると，すべての業務が低効率で処理されたり，一定の業務の達成を妨げたり，あるいは，操作を完全停止するという事態を招くかもしれない。

ＡＤＰオペレーションの信頼性に対するハードウェアの故障の影響を理解するために，ＡＤＰセキュリティ・プランナーは，特徴的なハードウェア故障の影響を検査することによって，システム故障のモード研究を指導するべきである。彼は，危険分析によって，検査時期が来ている，と確認された各用途に必要なコンピュータ・システム機器に注目することによってこれを行なうことができる。もし，システムが複雑化した場合には，彼は，ハードウェアとオペレーティング・システムについて責任のある職員や，システム販売者側の技術指導者に相談することが望ましい。

典型的なＡＤＰ業務の実行は，システム導入の要求に応えるデモンストレーションの実施の規準を設けることが必要である。導入テストの書類を再検討することはＡＤＰセキュリティ・プランナーが，装置の信頼性を推定したり，最も故障を生じやすい装置を確認したりする上で，しばしば役に立つ。

その目的は，ＡＤＰ装置がハードウェアの故障によって生じると予想されるロスを考慮するために，故障のモード分析や，緊急業務のロス電位，故障率や修理時間の推定に利用することにある。その考案によって，ＡＤＰセキュリティ・プランナーは，操作に対して，故障が最も限界となるハードウェア装置を，補修のコスト算出のもとになるものとして，突発的な事故に備える計画を推進させるためのガイド，あるいは，将来の使用決定の助けとなるものとして確認することができる。

もし，それらの分析によって，ハードウェア故障から重大なロスの可能性が示されたら，ＡＤＰセキュリティ・プランナーは次のような事項について考慮する

ことができる。

- 分析によって，限界にきているとわかった場合，予定されている業務を達成するのに最小の稼動状態をカバーできるようにして，装置が故障している状態でも操作持続が可能であるようにひとつか，またはそれ以上の**補助装置**を構成する。
- あるいは，**故障の恐れのある周辺装置をはずして**，技術的処理で代用する。すなわち，故障により生じたロスに会うと，特殊なインプット装置の使用によって，操作コストの節約度がより大きくなることが可能である。
- 第4.2節で述べているが，**故障数を減らす**，そして補修時間をスピードアップするための処置を講ずる。
- 普通の業務量を処理できる**2台かそれ以上のコンピュータを設置する。**もし1台で，コンピュータに故障を生じたら，たとえ，最小の危険性の業務でも達成できない。
- どちらのシステムも割り合てられた全業務を遂行できるように，**同じ様に構成された2台の（あるいは実際には数台の）コンピュータ**を設置する。この方法（デュアルコンピュータ，あるいは，マルティプル・コンピュータ）は，多くの場合，コストがかかりすぎるが，非常に重大な，あるいは故障に対して非常に過敏な業務に対する，唯一の適切な解決策である。

4.4.2 ハードウェア・メンテナンス・マネージメント

確立した信頼性の目標を獲得することによって，システム配列を最大限に活用することは別に，ハードウェアのメンテナンスマネージメントについて適切な策と処置を確立することは重要である。効果的な保守マネージメントとは，次のようなことである。

- 最適な**予防的メンテナンスのスケジュールと範囲**を決定し，できるならば，故障が，許容できるレベルにまで減るように進行中の管理を調整する。規則

については，予防的保守の規定は，適用される連邦機関への調度規定に従うが，売り手側と政府間の相互の合意にもとづいて修正することができる。

重大な故障の傾向を探り，適時に補修手段をこうじるために**ハードウェア故障について、統計的分析**を行ない，報告する。したがって，ＡＤＰオペレーション部門は，技術スタッフが，故障の原因を決定できるように，充分詳細に全部のシステム故障を報告せねばならない。システムが明白な原因に気づかないでダウンした場合はいつでもシステム事故レポート（ＳＩＲ）がオペレーションによって用意される。ＳＩＲの様式は，日付時間，システムステイタス，そのシステムにおける業務やジョブ，診断に役立つメッセージ，コアダンプ等々の有効性についての十分な情報を要求する。また，それは，ＳＩＲの作成目的や，事故の最終的処置に関する情報を記入する欄も設けている。同時に，ＡＤＰ技術サービス部門（ＴＳＢ）によって，事故は，未解決事故の欄に加えられる。事故がハードウェアによってひき起こされたと思われる場合には，販売者側に速やかに知らせる。原因がソフトウェアであるかあるいはわからない場合は，ＳＩＲは，処置をカレントシステム部門に移行する。事故の原因が発見されたら，所定の機関が，必要な補正措置を講じる。ＳＩＲが完成し，十分に機能を果たすために補助書類が配布されたのちに欄の記入は終了する。以上のような，あるいはこれと同様な処置によって問題は発見され，効果的に処理されて，システム操作に必要な情報の維持が保証される。

システムの信頼性に対して責任を割り当てられたＡＤＰのスタッフメンバーは，不調の傾向を確認するためにこれらのレポートを分析せねばならない。意味のある，詳細なレポートをもとにして，注意深くメンテナンスを行なうことはたいへん重要である。そうしなければ，ハードウェアの不調の傾向は，不必要なまでに長期間に渡って見落され，その情報が実際には得られているにもかかわらず，原因の確認は，はるかに遅れてしまう。オペレーティング・システムに適用しやすいエラーレポーティングの特長を十分に利用すべきで

ある。

- **修理保守**には継続的な注意が必要である。ハードウェア故障に伴う損失の可能性を分析すると，修理のための時間を減少させる努力は，特にコスト面から見て有効である。修理保守の規定は，適用される連邦機関への調度規定に記載されているが，分析によって必要性が維持され得る所では，ＡＤＰ装置は，現場の保守要員を配置し，故障しやすいと思われる予備部品を準備することにしている。

4.4.3 新システムのための信頼性の考察

新システム計画にあたって，従来のシステムの信頼性については，詳細な考察がほとんど加えられないということは，めづらしいことではない。連邦財産保守規則〔15〕の101－32 402-7項は，次のようにデータシステムの明細を規定している。「データ・アウトプットとその計画的利用，データ・インプット，データファイル，記録内容，データ量，処理頻度，タイミング，そしてシステムを十分に記述するために必要なその他の事項」を含むものである。……ここで言われている「その他の事実」には，当然，信頼性の考察を含んでいる。

典型的な連邦機関への調度規定（ＦＳＳ）は，90%のシステム効率（ＳＥＲ：稼働時間を稼働時間と損失時間で余したもの）。システム設計者はこの数値を，推定仕事量と，稼働時間が同等に正確であると認識した上での推定効率の数値であると受けとっているようだ。経験によると90%のシステム効率は，典型的なバッチモード操作なら受け入れられるが，オン・ライン操作には95％のシステム効率が要求される。もしＡＤＰシステムが，何らかの生命保持に関係する場合には，ずっと高い数値が要求されるだろう。ＡＤＰのセキュリティ・プランナーは，システムの信頼性の仮定がかなり正確であることをテストするために計画され，推定される仕事量についての内容を充分に研究しなくてはならない。ＳＥＲ（システム効率）は，平均故障間隔（ＭＴＢＦ）を，故障時間と修理時間（ＭＴＴＲ）

を足したもので余した値とだいたい等しいことに注目されたい。つまり，一週間（８時間制で20交替）に対して 160 時間が見込まれている場合，ダウン・タイムを１８時間とし，さらには 90%の効率を達成することができる。仮に，予定した仕事量の内容により，このダウン・タイムが回復できないものとなった場合，信頼性について別の検討が準備されている。既存のシステム（デュアル・システム，システム内部の冗長，迅速補修）に関して既述の措置は新システムにも適用されるが設置後よりもシステムの設計中に最初の２方法による検討を利用した方がより簡単であろう。

ＡＤＰハードウェアが他により重要な用途を持っている場合，売り手側からＭＦＴＢおよびＭＴＴＲに関するより現実的な数値を得ることが可能であると思われる。このような場合，信頼性分析は，契約の必要条件として信頼性に関する数値を包含することが適当でない場合でも利用できる。これは，システムの信頼性が９０％のＳＥＲに基づいて限界であるとみられる場合，特に当てはまるものであるが，補正努力がコスト面で容易に妥当性をみつけることができない。信頼すべき，売り手側の見積りが，より高い比率の達成が可能であることを現実的に示している場合，システムの信頼性は受容できるものと結論することができるであろう。

最後に，ＳＥＲはハードウェアの故障の中断期間を示すことができないことを指摘しなければならない，上述の例を続けて，１週間につき１８時間の中断１回，３時間の中断３回もしくは作業要員の反応時間に依ってのみ限定されるその他のコンビネーションが生ずるとすれば，このため，ＡＤＰのセキュリティ・プランナーは中断期間の予想配分を求め，緊急作業の実施についての意味を検討することが必要である。これは６回の３時間中断は何ら大きな損失を与えるものではないが，単一の１８時間の中断は極めて重大となる可能性を有するからである。

4.5 ＡＤＰファシリティの物理的保護

4.5.0 まえがき

この章では，ＡＤＰ装置のある場所に出入する資格のある者が実際にファシリティにアクセスする過程において物理的保護上考慮されるべき諸要件について述べる。ここでは，問題を便宜的に次の３つの問題に区切って考える。

(1) **ＡＤＰ関係者の役割**　つまりコンピュータ室のオペレータ，ＡＤＰプログラマ，売り手側の保護上の役割に関する問題。

(2) **各設備空間の重要性**　つまり敷地，建物内の共用の場所，機械装置室，テープ・ライブラリなどの保護上の重要性に関する問題。

(3) **業務時間**　つまり平常の業務時間，コンピュータ室のシフト時間，ＡＤＰ装置休止時間における保護上の問題。

物理的保護プランの目的は，上記の３項の問題の全ての組み合せに対して適，不適の規準を確立することであり，ひいてはそれらの規準を適用する具体的な方法を決めることである。これらの適，不適の規準を決定するためにＡＤＰセキュリティ・プランナーは，ＡＤＰ装置が直面する脅威やＡＤＰ装置を備える建物の物理的特徴，ＡＤＰ装置の構成と機能を組織的かつ包括的に分析しなければならない。しかしＡＤＰ関係者による物理的保護やオーバーアクセスのコントロールは，実現させるにも運用するにも，また，ＡＤＰの作業の流れを多少なりとも妨害してしまうことが予想されるという意味からしても，不経済であろうが，ＡＤＰ装置の安全性が不充分であってはならないし，かといって不必要に高価でも煩瑣でもいけない，……要は安全性と費用の両面で妥当な水準の保護体制を実現することなのである。しかも，すべての予想されるリスクに対応できる保護体制でなければならない。ある大銀行の役員は，最近，ＡＤＰ装置の安全処置の偏りを評し

て「紙の壁に鉄の扉を付ける傾向がある」(*)と言ったがこれは的確な指摘と言わねばなるまい。従って，現状をわきまえたうえで必要な保安処置を決定する努力こそ現在求められているものなのである。

4.5.1 保護要件の限定

この定義の第1段階は，ＡＤＰ装置に対して部外者によってひきおこされる可能性のある脅威を検討することである。これは人間的な動機が関係してくる事柄だけに，それを質的に限定することは容易ではない。とは言え，この種の脅威を以下のように分類して，その特質をＡＤＰ作業との関係において明確に限定しておくことは必要であろう。特に，ＡＤＰ装置および同一建物内のテナントとが妨害者の眼にどう映るかについて考えなければならない。なぜなら妨害者は，その成功の見込みを推測しながらそれに要する労力を計算するものだが，保護体制しだいでは，やすやすと成功に向けて全力を尽す気をおこさせてしまうからである。

一般犯罪の場合には，政府財産の窃盗に関係してくる。ＡＤＰ装置を備えている建物を見て盗みに入ろうとするような，いわゆる泥棒がいるだろうか？いるとすれば，事務用機器，拳銃，薬品，現金，個人的な持ち物などの簡単に故買にさばける品物か別の犯行に利用できそうな品物を狙ってのことだろう。

政治的活動家については盛んに議論されているが，この分野で活動中の，もしくは活動していると考えられる政府機関があるだろうか？ＡＤＰ装置を備えた建物は，直接的なデモの効果のある，格好の象徴的攻撃目標と考えられている。中西部のある研究所のＡＤＰ装置に一団の活動家グループが押し入り，かねてからこのグループが反対していた研究プロジェクト用の磁気テープデータファイルを破壊しようとしたことがあった。事件当時，研究所員は誰もおらず，活動家たちも

(*) 出典：1973年6月13日号「コンピュータワールド」1ページ「ＩＢＭ，ソフトウェアの強度に関する安全性テスト」

ハードウェアには手を出さなかった。しかし多くのテープが消去され，パンチカード類が床にバラまかれた。このグループは侵入中には発見されず，数日後，記者会見を行なって犯行を宣言した。被害に遭った研究所では，以後パトロールを強化し，また侵入探知器の導入も検討しているという。この時の被害は10万ドル以下だったが，しかしこの事件は侵入に対するＡＤＰ装置の保安設備を充実させることの重要性を示したものといえる。

スパイ行為による影響を考えてみると，経済活動や連邦政府発行の国債の将来の配当金などのように公衆に先んじて知ることが部外者にとって利益となる種類の情報とか詳しい個人情報などのデータを，ＡＤＰ装置が保有したり処理したりしているだろうか？否である。

破壊者，ＡＤＰ装置は，破壊主義が荒れ狂っているような地域に設置されるだろうか？否である。

次に，この分析の第２段階は，施設内部を目的別に区別けして，表に示すことである。この表には各エリアの場所，機能，アクセスの要件（「誰」が「いつ」ということ）のほか，各区域の重要性（犯罪者の狙いとなりそうな内容や活動）についての説明を加える。もちろん，細部は建物によってまちまちであろうが，以下は考慮すべきエリアの模範例である。

部外者用の入口とロビー
物資の積み下し場所
他テナントの占有スペース
ＡＤＰ施設への受付窓口
ＡＤＰインプット／アウトプット用のカウンタ
ＡＤＰデータ変換用作業場所
テープライブラリ
システム分析およびプログラム作成場所
コンピュータ室
通信装置室（Communication equipment rooms）

空調設備その他電気・機械装置スペース

以上の点に関してＡＤＰ装置とその周辺を対象に，無警戒の部分やすでに適所に設定されている区域についての安全処置の確認，未設定の場所の実地検査による常用位置の決定などのために完全な調査を行なうことが保護上有益であろう。連邦調達庁（ＧＳＡ）はある任意の施設（ただし建物内部のＡＤＰ装置部分は除く）の物理的安全性調査に関して次のような指示を与えている。

4.5.1.1 施設の物理的安全性調査のための指示（ＧＳＡ）

Ａ． 施設内部の全てのアクセス・ポイントを含めた全エリアとそれに付属するあらゆる隣接部分（駐車場や倉庫など）を表わした現状の平面図を作成すること。

Ｂ． 施設周辺での調査を開始して以下の諸点をチェックすること。

(1) 敷地の境界線の特徴と形式。もしあれば塀，　などの障壁についても記す。また，その状態，ゲートなど開口部の数と型と用途，および警備方法，境界線の警備員詰め所の有無。

(2) 屋外の駐車設備。その囲いの有無と管理状態。さらに有人管理，無人機械管理の別。

(3) 施設周辺。全運搬装置と歩行者用入口のチェック。また，それらの管理が行なわれている場合の管理手段のチェック。全てのドア（数，警備方法，警報装置やキーカード装置などの管理機器を含めて）のチェック。全ての地下室と地下室の明り窓のチェック（警備方法，網張りなどの別とそれぞれの弱点）。その他の入口のチェック，（すなわち通風孔やマンホールなど，その警備の有無，警備方法。）非常口のチェック。（数，位置）非常口も含めて窓，ドア，屋根などから施設内部への接近の難易度のチェック。これらの接近路の警備方法もチェックすること。

(4) 内部の安全性。最上階か地下室からチェックを開始する。火災報知システムおよび機器の型，位置，数を含めてチェック。報知先の確認。電話および電気用配線室の施錠チェック。電気・機械室の施錠と警備方法のチェック。

現在ある全警報器の型と数の調査。各警報器の報知先のチェック。警備員詰め所の数と位置，警備時間と交替時間の決定。

(5) モニター機器。位置，モニター係員，応答係員，型，モニターの対象となっている警報器の数をチェック。

C．以下の質問事項が，物理的安全性調査に含まれる。

(1) 装置／建物は警報システムで守られているか？

(2) 保護対象の建物内部には，保護すべき領域が幾つあるか？

(3) 警報システムは充分か？またそれは要求される保護水準に達しているか？

(4) 保護体制の弱いエリア，周辺部，警報システムでカバーされていない開口部はないか？

(5) 音量，機能その他で平常業務を妨害する率の高い警報はないか？

(6) 警報システムは，必要なとき動作するように適宜検査およびテストされているか？

(7) 警報システムは，どの段階でどの警報が鳴るかを熟知している正式に訓練された保安係員によってバックアップされているか？

(8) 警報システムの物理的機械的経年変化に備えて，定期的検査が実施されているか？

(9) 警報システムは，その性能保証のための改造防止スイッチを備えているか？

(10) 警報システムは，周囲もしくは保護用の外被またはカバーを備えているか？

(11) 停電の場合の警報システム動作用分割電源または非常用交替電源があるか？

(12) 報知ユニットはどこに配置されているか？（警報の報知先が１箇所に集中されているのか分散されているのかの別）

(13) 警報装置のメンテナンスは誰が，いかに行なうか？（外部機関との契約，リース装置，ＡＤＰ装置内部のメンテナンス専従要員の別）

(14) 現状警報装置は旧式ではないか？

(15) 時間，日付，位置，作動，作動理由を含めて全ての受信した警報シグナルの記録は保管してあるか？

(16) 警報は，警報システムの感応点と不感応点を調整するために適宜試験されているか？

物理的安全性の調査が終了したら，現在使用中の警報システム本体とその位置，警備員詰め所の数と位置および詰め所の警備員数と時間割を明記した表（写真なども利用）を作成して施設内に配布すべきである。

以上の諸事項の調査結果を総合すれば，ＡＤＰセキュリティ・プランナーは現在のアクセス・コントロールと保安方法を評価し，手直しや特別な方法が必要とされるエリアの識別を行なうことができる。以下の諸項目に述べるのは有効な管理や方法のいろいろであるが，もちろんそれは一般的なガイダンスにとどまる。実際には，建物の管理者やＧＳＡの連邦保安サービス（the Federal Protective Service <FPS> of the General Services Administration）に援助を要請すべきである。事情の許すかぎりＦＰＳは要請に応じて建物の安全性調査を行ない，専門家によるアドバイスや安全のためのハードウェアについてのガイダンス，また連邦保安係官（Federal Protective Officers）ないし民間のガードマンによるサービスを提供してくれる。

また，現在使用中の保安力を増強するためにいろいろな型の装置を利用することも検討すべきである。そのような装置を利用することによって，物資搬入用および歩行者用出入り口のいくつかの常設警備員詰め所を廃して，そこの人員を別の区域や施設にふりむけることができる。

4.5.2 境界線の保護

ＡＤＰ施設に対する脅威を分析すると，建物の敷地境界線での保護対策が必要であることが分かる。ここでの保護対策は，フェンスその他の物理的障壁，外部照明，周辺侵入者探知器などの設置あるいはパトロールを利用することになるだろう。これらの保護対策をいくつか組み合わせるのも効果的である。障壁の高さは，だいたい次のように決められる。衝動的な侵入者を思い止まらせるには，３～４

フィート，簡単には登れない高さは 6 ～ 7 フィート，計画的な侵入者を妨害するためには，3 本撚りの有刺鉄線で高さ 8 フィートの障壁を作る。境界線全体を障壁で囲う必要のない場合もありうる。重要な区域，たとえば，トラック寄せ場（truck dock ）とか駐車場（特に夜間用の駐車場），または建物の監視困難な箇所等だけに限ってもよい。

障壁の替わりに，泥棒の気持を挫く広範囲にわたる照明を利用することも考えられる。この方法は，脅威の低い場所あるいはコスト面と外観の問題から障壁が適当でない場合の効果的な解決策である。重要な区域，たとえば，出入口，駐車場，あるいは現状の外灯ではカバーできない場所には特別注意を払うべきである。出入口が建物内部の警備員によって守られているか日没後だけ警備員が配備される場合には，外部照明を広範囲にゆきとどかせることは大変有効である。また，そのような場所には青味がかったガラスは使わない方がよい。なぜなら日没後は外部が見えにくくなるか，ひどい場合には全然見えなくなってしまうからである。

周辺保護のための 3 番目のテクニックは，侵入者によって赤外線もしくは超音波が遮られると作動する探知装置を利用することである。このような装置は直線 1 メートル当たり 1 ドルから 7 ドルの範囲の費用で設置でき，物理的障壁とちがって美的景観をそこねることもない。しかし，このような装置を使った場合には，衝動的な侵入を思い止まらせる効果や群衆をコントロールする機能は期待できないし，熟練した侵入者に対しては余り役に立たない。さらに，侵入探知装置を利用したとしても，実際に警報が鳴ったとき，迅速かつ効果的に侵入者に対応できる警備員を配置しておかなくてはならない。また使用する装置の特徴と位置によっては誤った警報が出ることも覚悟しておかなければならない。このような理由から，侵入探知装置の用途は限定される。高度の保護体制を要求される場所に障壁のバックアップとして利用するとか，あるいは障壁を使えない場所に利用すれば効果的であろう。

フェンスをよじ登ったりかいくぐったりして侵入してくる者に対しては，振動感知器（vibration sensors）をフェンスに装備するとよい。このシステムは，

各ゲートおよびフェンスの支柱２～３本ごとに取り付けられる小型感知器を利用したものである。各感知器は，コントロールパネルにワイヤーで接続され，フェンスをよじ登る力に見合ったフェンス面の動きを感知すると警報が鳴る仕組みである。費用は，フェンス１メートル（直線として計算）当たり１ドルから３ドルの範囲内である。

ＡＤＰ施設のある建物が政府関係の建築群の一部をなしており，外部から侵入される危険が強く，しかも障壁がないような場合には，屋外のパトロール部隊が最も有効な保安手段である。パトロール部隊の構成，装備（乗物，無線機，番犬など），巡回の規則は保安の必要度と最低限の費用とを見合わせて入念に決定すべきである。これらの問題は，ＦＰＳの手によって規則としてまとめられることになっている。ＡＤＰセキュリティ・プランナーは，この規則に従って提供される保安水準を把握し，ＡＤＰファシリティの必要に見合うよう，必要なら適当に調整してこれを利用することが望まれる。

ある場所，たとえば，犯罪発生率の高い従業員用駐車場などには，夜間監視用に低明度でも機能する構内テレビ（CCTV; closed circuit television)システムが有効である。このシステムは，必要なエリアをカバーするように１台もしくは数台のCCTVカメラを設置して，これを中央保安室（central security location)のモニターテレビに接続したものである。普通，各カメラは監視員がリモート・コントロールできる映写角可変台（pan-tilt mount）に取り付けられ，同じく監視員が操作できるズームレンズを備えている。この２つの装備によって，監視員は平常時には広範囲を監視でき，必要に応じて特定の場所をクローズアップできる。ただし装置の種類と設置場所の条件によっては，カメラとモニターのテレビの１組で4,000ドルから10,000ドル以上の費用がかかる。機械部分は，正式な資格をもつ訓練された係員によって適合するように調整される。しかし，実際問題として監視員が長時間モニターテレビを監視しつづけるということは期待できない。従って定時的に画面を見つめるか，警報で異常事態を監視員に報知できるよう侵入者探知装置を併せて装備すべきである。だが，合理的に設計

されたＣＣＴＶシステムを適切に利用すれば，監視員１人で広範囲を監視できるので巡回式のパトロールよりも費用が安くつく場合もしばしばである。

屋外の監視にＣＣＴＶシステムを利用すれば，デモやその他の大衆行動の目標となった施設が侵入しようとする大衆をコントロールする場合，非常に有効である。なぜなら，モニターテレビによって一目で全状況を確認できるので，保安の責任者は保安力をいつでも適切に配置できる上に，状況の変化に応じて迅速にその配置の度合を変えることができるからである。このテクニックは，ある主要な政府研究機関で大成功をおさめた実績がある。

ここでＧＳＡが管理する建物用にＣＣＴＶ装置が調達されるのに先立って，いくつかの指摘が連邦保安サービス管理事務局システム部門（ the Office of Federal Protective Service Management, Systems Branch ）に対してなされたことに注目する必要がある。

その指摘をまとめると次のとおりである。

- **フェンスその他の障壁**は，群衆をコントロールし，衝動的な侵入者の気持を挫き，出入口への接近をコントロールするのに有効であるが，費用がかかる上に，計画的侵入者を食い止めることはできないし，美観をそこねる。
- **侵入探知装置**は，侵入を迅速に探知でき，フェンスを設置できない箇所に適しているが，誤った警報を出しがちであり，かつ熟練した侵入者には効果もなく，また警報に対する警備員の対応が不可欠となる。
- **パトロール部隊**は，柔軟な対応が可能である。（特に緊急事態の場合）また，効果的な侵入予防力を備え，特に建物群の保安には有効だが，何といっても費用がかさむ。
- **ＣＣＴＶシステム**は，１人の人員で広範囲を監視でき，発生事態を正確に報知できるが，その機能を充分に発揮させるためには侵入探知装置や定時的な監視などが必要であり，警備員がいつでも対応できるように準備されていなければならない。

4.5.2.1 放射波（emanations）

ＡＤＰ施設周辺の保護対策の必要性を考える上で，ＡＤＰセキュリティ・プランナーはＡＤＰハードウェアから放射される電磁波あるいは音波が傍受される危険性についても考慮しておく必要がある。このような放射波からの傍受や解読が可能なことは，技術的な専門家による，一般的に使用されているＡＤＰハードウェアを使った実験から明らかになった。経験的にいって放射電磁波の傍受は，半径300ｍ以上の範囲では困難である。しかし，ＡＤＰセキュリティ・プランナーが傍受については潜在的な危険性があると判断した場合には，正式の売り手側からの技術ガイダンスを要求すべきである。傍受の危険性のある地点から無線装置を物理的に隔離するかあるいは遮蔽壁を用いるかの選択は，相対コストの分析に基づいて行なうべきである。政府関係以外のテナントが入っている民間の建物にあるリモート・ターミナルの場合には，傍受に対して特に注意が必要である。

4.5.3 出入口ドアのコントロール

ＡＤＰ装置周辺の保護の目的は，衝動的な侵入の防止と同時に従業員，視察員，一般顧客をそれぞれ決まった出入口へ通すことである。出入口ドアのコントロールとは，適当な場所で入室者の検査を行ない，入室を禁じたり，建物へ出入する品物の流れを管理したりすることである。

入室者の検査（スクリーニング）には２つの方法が用いられている。警備員による入室者の個人的な確認もしくは利用許可証＊を受け取る方法と，入室者がドアを解錠するのに必要な器具を所有しているか否かによって識別する方法の２つである。

(＊) 入室者のスクリーニングに当たる警備員に提示する証明書には，スクリーニングの明確な責任者を記入しておくべきである。その責任者は，制服を着た警備員の替わりに受付員でもトラック用駐車場監視員でもコンピュータ要員でもかまわない。

警備員によるスクリーニングは，入念に行なわれた場合には他のどの方法よりも確実である。しかし，状況によって出入口1箇所につき1時間当たり2ドルから10ドルの費用がかかる。これに対して入室者の所持品のスクリーニングには，電子的または機械的な装置が必要である。つまり，入室資格のある者は，鍵（電子式もしくは従来型）を持っていなければならないとか，押しボタン式錠前の組み合せ番号を記憶しておくとか，あるいは入室資格のある者についてあらかじめ記憶された情報と入室者の特色（手形，指紋，声紋）とを比較照合する装置などを備えなければならないのである。警備員の替わりにこれらの鍵やスクリーニング装置などに頼るアクセスコントロールには，いくつかの欠点がある。鍵や組み合せ番号は，部外者の手に渡ることもありうるし，入室資格のある者の背後に隠れてすばやく行動すれば鍵その他を持たなくとも侵入できてしまう。（これはしばしば「テール・デーティング」と呼ばれる。）また，熟練した侵入者なら錠を破ってしまうだろう。これらの欠点は，鍵の取り扱いを注意し，保安意識を高め，防犯ドア（正規の鍵以上のもので錠をいじると警報を鳴らすドア）を採用することなどで補えないこともないが，ＡＤＰセキュリティ・プランナーは常にこれらの欠点に気を配り，「このドアはいつでも鍵がかかってますよ」とか「この鍵は複製できません」とかいう漠然とした言葉や宣伝文句の罠にひっかからないように用心しなければならない。なお各種のドアコントロール装置の特徴は，以下に要約したとおりである。

従来型の鍵および錠前セット

費用は最小ですむ。鍵1つ当たり1ドル以下，シリンダ錠1つ当たり約5ドルである。ほとんど全てのタイプのドアに取り付けられる。しかし，鍵は簡単に複製できるし，錠も容易に破れる。鍵さえ持っていれば，いつでも入室できてしまうので，品物の出入りに対して何らチェックできない。

防犯型錠前セット

従来型に比べると，2倍から3倍の費用がかかり，鍵も比較的複製しにくく錠も破りにくい。それ以外は従来型と同じ性能である。

電子キーシステム

これは，電子ドアの柱側の受け穴に作用するよう特別にコード化されたカードを用いる戸締り方法である。従来の錠では，鍵が錠のボールト（鍵の回転によって錠から出入りする金属棒のこと）を柱側の受け穴から錠本体へ引っ込ませてドアが開くような仕組みだったが，電子キーシステムでは，ボールトは錠本体へ引っ込むようにはできておらず張出したままで，電子ソレノイド（solenoid）が柱側の受け穴を引っ込ませてドアが開くように工夫されている。システムの特徴と装置によるが，費用はドア1枚当たり約400ドルから数千ドルまでさまざまである。またコード化されたカードは，1枚当たり数ドルである。この種のものでも，単純なシステムは，防犯型錠前セットと同様の性能である。高価格のシステムは，指定されたカード（たとえば紛失届のあったカードなど）では作動しないようにしたり，指定された時間のアクセスを制限したり，あらゆる出入りを記録したり，ある何枚かのドアに対するアクセスを各カードでできるようにそれらのドアをコントロールしたりする機能を備えている。

電子式組み合せ錠

この種の錠は，電子式押しボタンを備えているタイプが普通で，この押しボタンに電子式の柱側の受け穴に作用する組み合せキーが組み込まれているのである。入室するのにコード化されたカードが必要ないことを除いて，その他の性能および費用はだいたい電子キーシステムと同様である。また，この種の錠のうちには，たとえば侵入者に強迫されてドアを開かねばならないような場合にそなえて，特別のコードを使えばドアは開くが，それと同時に別室（警備室やモニター室）の警報も鳴らす機能を持ったものがある。この種の錠は，ドア1枚当たり約500ドルである。

機械式押しボタン組み合せ錠

正しい組み合せを押すと，ボールトが引っ込みドアが開く仕組みになっている。電子錠のような性能は持っていないが，費用はずっと安く，ドア1枚当たりで普通40ドルから80ドルである。

入室者の肉体的特徴を識別する錠

費用は，ドア１枚当たり数千ドルかかり，入場者は電子式キーカードを所持しなくてはならない。このシステムが，人間によるスクリーニングに最も近い。すなわち，手形や指紋など，入室者の肉体的特徴の一部を検証する機能を持っているのである。しかし，入室の可否を決定するのはアナログ・インプットに基づくので，誤動作，すなわち入室の資格のある人に対して入室を拒否したりその逆に作動したりすることも起りうる。さらに，このような装置は比較的新しいので，どの程度まで信頼できるのか，またどの程度この装置をごまかせるのか，といった点については明らかになっていない。

警備員によるスクリーニングが必要で，監視すべきドア数が多く，しかも通行量が比較的少ない場合，ＣＣＴＶシステムを利用すれば警備員は１人で充分であるからコスト的に大変有利になる。各ドアにＴＶカメラ，信号装置，インタホーン，電子式のドアストライク（柱側の受け穴）を取り付けておく。出入の両方をさばくために，それぞれ専用のリモートコントロール式のドアが１枚ずつ必要になる。ただしこの仕組みは施設に対して慎重に計画するよう要求されている非常出口の問題と矛盾する。またある商業ベースのシステムにはモニター・カメラの他に入室者の証明書写真カードのクローズアップを行なう特別ＴＶカメラを１台備えているものもある。ＣＣＴＶモニターに映る入室者の映像と，インタホーンを通しての会話によって，警備員は実際に対面しているのとほとんど同じに入室者を検査できるのである。また，入室者ばかりでなく品物の移動を監視できることも忘れてはならない。このシステムのハードウェアの費用は，出入口１箇所当たり3,000ドルから6,000ドルであるが，これはＣＣＴＶの導入で節約できる人件費ですぐに埋め合せがついてしまうはずである。ただしスクリーニングをすると１分間当たり４～５人程度しか入室できないのであるから，通行パターンを特にシフト交替時について注意深く分析して，くれぐれもスクリーニングの影響で必要な人員移動に極端な遅れが出ないように配慮すべきである。人員移動の遅れは，支払い給料総額を実働時間で割ってみた場合，かなり大きな損失の要素とな

るだろうから，ＣＣＴＶを含めてすべての無用なスクリーニングについて考慮しておくべきである。人員や物資のスクリーニングの効果を上げてゆくに従って，スクリーニングに充当する費用の方もせりあがってゆくわけであるから，全努力を傾けて無駄な出費を避けるために各出入り口に要求される機能を詳細にまとめ，できれば不必要な出入り口は撤廃するように心掛けるべきである。

以上のほかに各出入り口ドアには，力づくでの侵入や秘かな潜入を防ぐだけの強度が要求される。これがドア自体とその設置についての考察の最後の要件である。しかるべき場所には，頑丈な錠や補強ストライクプレート（柱側の錠受け穴を囲む金属板で，受け穴に対する侵入者の細工を防ぐ）および補強ドアフレーム，防犯式蝶番，防弾ガラス嵌殺しの覗き窓などを用いるとよかろう。これについてＡＤＰセキュリティ・プランナー防犯分野の専門家とよく相談して決めるべきである。

ドアの補強に加えて，特に重要なドアにはドアが開いている時に警備員に信号を送るような警報システムを接続しておくとよい。電子式ドアストライクが取り付けられたドアなら，通常の出入りの場合には警報は鳴らず，無理に侵入しようとしたときだけ警報が鳴るようにも工夫できる。

4.5.4 建物周辺からの侵入者に対する保護

出入り口以外の警戒を要する部分，たとえば窓，変圧室，空調用ルーバー，天窓などの建物周辺もチェックすべきである。侵入ルートとなる危険性のある各場所には，適宜，物理的な保護手段や警報システムを取り付けておく。たとえば，柵や鎧戸の備えのない窓には防弾ガラスか防弾プラスチックを嵌めるとか，ルーバーは重い規格のスクリーンで防護する，などである。計画的に侵入者が，余り人目につかず，しかも盗み出すつもりの品物に充分な価値があると判断したならば，壁や屋根を破っても押し入ろうと図るだろう。そのような侵入に対する物理的な保護対策も適切な監視体制も用意されていない所（たとえば，政府で管理してい

るのではない建物など）では，窓，物資の積み下し場，建物の全周などに特別な感知器を必要に応じて設置するとよい。

電気メカニズム型の侵入探知システムが，今日では広く利用されている。このシステムは連続した電気回路で構成され，平常時には電気的平衡が保たれているが，回路内に変化や破壊が起るとその平衡が崩れて警報がどっと鳴り出す仕組みになっている。このような電気回路は，たとえば次のようなもので構成される。窓には窓を破ると同時に破れるような金属の箔片，ドアには磁気スイッチとか接触スイッチ，その他の開口部には角度を変えられる水銀スイッチ，壁には振動探知器，こじあけられるおそれのある合せ釘部分や壁，天井，床などには細い導線を一面に埋め込むなどして回路をつくるのである。こうしてできあがったシステムの電気回路および機械部分に対してどんな細工をしても，警備本部の警報が鳴り出すのである。これらの装置は比較的単純なので，よく建物周辺の保安用に利用されている。また，このシステムは，他の探知装置の作動を妨害しないので，どんなタイプの保安システムとでも（建物を部分的にカバーするものとでも全体をカバーするものとでも）併用できる。以下にこのシステムを構成する装置の種類を記す。

窓用金属箔　窓ガラスやガラスドアに貼りつける金属製のテープである。ガラスが割られると箔も破れて電気回路が開き（電気回路の平衡が崩れ），警報が鳴る。箔に毛髪状の切り傷やひっかき傷がついただけでも警報が鳴るようにできている。

導線の編み合せ　細い導線をスクリーン状に編み合せたもので，ドアパネル，床，壁，天井に埋め込んでおく。侵入によって編み合せの一部でも破れると，警報が鳴る。

トートワイヤ（taut wire）　特に重要な保護区域への侵入を探知するための装置である。エアダクトやダストシュート用のトンネルなどの開口部内側に強く張られた細い撚り線（導線）で，張り具合のどのような変化にも敏感に反応して警報を鳴らす。

防犯スイッチ　磁気式あるいは機械式の防犯スイッチがドア，窓，天窓などの侵入可能な開口部の保安用によく利用されている。これらのスイッチは，表面に張り出すか逆に埋め込むように取り付けられる。

- **磁気式防犯スイッチ**　このスイッチは，磁石部とスイッチ部の２つの部分からできている。磁石がスイッチ部に規定どおりに向き合うか，あるいはスイッチ部に密着している状態では，スイッチは電気回路の平衡を保つように作動しているが，磁石が少しでも動くとスイッチの作動が止まり（電気回路の平衡が崩れて）警報が鳴る。普通，磁石部の方がドアや窓あるいは保護対象物の可動部分に取り付けられる。
- **機械式防犯スイッチ**　このスイッチも，ドア，窓，天窓などが開くと警報を鳴らすように働く。プランジャー型はそれらの箇所に埋め込むタイプであるが，その手間の分だけ費用が高くなる。レバー型はプランジャー型に比べて安く取り付けられるが，侵入者の眼に付きやすい。また，機械式スイッチはいずれにしても気候の影響を受けやすく，気温による機械部分の膨張や錆などで円滑に動作しなくなったり凍結したりすることがある。

以上，さまざまな装置について述べてきたが，最も効果的な侵入防止策は，要約すると侵入者が狙いをつけそうな場所を監視するか，あるいはそこを完全にアクセス・コントロールすることであり，同時にその他の建物周辺部については，やはり監視するか警報システムを設置しておくことであると言えよう。ところでほとんどの建築構造が計画的な侵入者に対しては無力であるということを，最近発表された「Ｊ－ＳＩＩＤＳ障壁突破テスト」〔21〕という報告書が明らかにしている。これは，人間１人が侵入するための必要最少限の大きさと考えられる８インチ×１２インチの穴を実際に各種の壁にあけてみるテストで，その結果は表５－１のとおりである。

表５－１　壁面突破テスト

壁　の　構　造	使用した道具	突破所要時間
間柱（studs）；2″×4″（インチ） 角に両面付板（siding）；1″厚	○手回しブレース ○電動サーベル型鋸切り	１分５５秒
炭殻ブロック；8″厚	○大ハンマ	１分５２秒＊
炭殻ブロック；8″厚に片面ブリックベニヤ（brickveneer）	○大ハンマ	２分１２秒＊
強化コンクリート；$5\frac{1}{2}$″厚	○ロートハンマドリル ○大ハンマ	５分４４秒＊
強化コンクリート；8″厚	○ロートハンマドリル ○大ハンマ	約10分00秒＊

ただし，＊については，補強ロッド（鉄筋）を除くのに要する時間としてそれぞれ１分を加える。

4.5.5　重要な区域のコントロール

たとえ建物内部の全ての人間が建物周辺部でチェックされているとしても，ＡＤＰファシリティ内部では，全てのエリアに対して均等なアクセスが行なわれるわけではない。以下にあげる区域は，ＡＤＰファシリティの運用時間および休止時間の両方におけるアクセス許可を決定する上で分析する必要のある最少限の区分である。

コンピュータ室

データ記憶ライブラリ

インプット／アウトプット区域

データ変換区域

プログラマ区域／ファイル

ドキュメント・ライブラリ

コミュニケーション装置区域

コンピュータ・メンテナンス室

機械装置室

電　話　室

補給倉庫

データファイルの機密性と完全性の保護という立場のほかに，大切な資材を守り，盗難や破壊やサボタージュを防ぎ，部外者による侵害に対して一瞬たりとも侵入するスキを与えないようにするといった立場からも区域を設定する重要性を考察する必要がある。

この分析の目的は，まず全ての重要な区域を識別し，作業の流れとジョブの割り当ての検討によってどの人員がいつアクセスを許可されるべきかを決定することにある。そしてその次に，人員に対するコントロールの体系立った方法を選定すべきである。その際の基本的なテクニックは，第5.3節で外部ドアについて述べたこととほとんど変わらないが，2点だけ重要な違いがある。

第1点はここで言うような区域は，使用されていないで施錠されているか，あるいは出入資格のある者によって使われているかの2つの状態しかありえないことである。従ってもし第9章で述べるような明確な規則が作成され，それが遵守されれば，出入資格のない者が使用中のエリアに入ろうとしたらチェックできるわけである。

第2点はここで扱うようなエリアでは，作業の流れを不必要に妨げないようにすることが特に重視されるということである。このことは，さして重要でない区域への通路に当たる場所に重要な区域を設定するというような明白な誤りを避けるために，ＡＤＰセキュリティ・プランナーがＡＤＰファシリティ内部の物理的レイアウトと作業の流れや人員との関係あるいは情報や物資との関係を綿密に検証しなければならないということを意味している。さらに，重要な区域への指定

順路が遠回りで，近道しようと思うと非常口などの誰が通っても構わない通路ではなく，重要な区域を通り抜けするようになってしまうといった設定も避けるべきである。遠回りになるような場合，人情として近道を使いたくなるものだからである。しかし，指定順路が適切に設定されている場合でも，非常口が濫用されていることが多い。そんな場合には，非常口に警報器を取り付けるのが普通である。集中警報システムを備えたファシリティならば，非常口が開いているときはいつでも信号が集中警報システムの管理室へ流れるようにセットしておくとよい。だが最も効果的なのは，通路に警報ベルが聞えるようにすることである。そのためには，非常口に取り付けられる自動警告器が利用できる。これは約 10×20×7 cmくらいの大きさのものが普通で，不要時には警告ベルを鳴らさないようにできる「準備／解除」スイッチが付属している。ドアが開かれると，内蔵したバッテリーの力でけたたましい警告ベルが鳴り出し，準備／解除スイッチで「解除」に切り換えるまで鳴りつづける仕組みである。費用は，1台およそ60ドル程度である。

ＡＤＰセキュリティ・プランナーは，アクセスコントロールの努力が人命に対する安全保護対策と対立してはならないことを考慮すべきである。NFPAの「生命の安全保護に関する規定」〔30〕によって，建物の使用時間および建築構造に応じた非常口の数，大きさ，位置が決められている。このような規準や建物に適用される政令規則を遵守することが大切である。

休止時間中の重要区域へのアクセスないし休止時間中の警備に関する技術的な方法がいくつかある。そのうちの2つはすでに検討したものである。つまり，出入り口を明るく照明する方法とＣＣＴＶシステムである。しかし，ＣＣＴＶシステムは他の警備システムから警報が出た後の区域の状態を確認する場合にだけ最大の能力を発揮するということに注意すべきである。ＣＣＴＶシステムよりも積極的なものは，侵入探知器である。侵入者を探知するには，少くとも4つの独特な技術がある。

① **光度測定システム**　これは消極的な探知システムで，照明装置の点灯や継

続的に点灯している照明光の反射もしくは吸収によって区域の光度に変化が起きると，それを探知する仕組みである。このシステムは周囲の光度にきわめて敏感に反応するので，窓のない区域やカーテンなどの備えのある所でしか利用できない。

② **動作探知システム**　このシステムの原理は，ドップラー効果である。音源や電磁波信号源，もしくはそれらの信号を反射するものが受信器に近づいたり遠ざかったりすると，信号の音程や周波数がそれぞれ高くなったり低くなったりする。この原理によって音波や電磁波のエネルギー源と受信器を備えた部屋の中で体を動かせば，その動作が受信波形の周波数変化として探知されるのである。受信器は，周波数変化の強弱にかかわらず変化を探知することができる。

- **音波**　音波探知システムは，1,500～2,000ヘルツあるいはそれ以上の可聴周波数帯域内の音波を利用する。ただし，この持続音は，可聴帯域にありかつ高い音圧レベル（デシベル：ＤＢ）で聞えるので非常に耳ざわりである。音波で区域内の全領域をカバーするために，このシステムではそれぞれ複数の発信器と受信器を使用する。これらの発信および受信用のトランスデューサは永久磁石式スピーカ（ＰＭスピーカ）で，同じ部屋の対向壁面に取り付けるのが普通である。受信器は発信音と反射信号音を比べ，保護区域内部に異物が侵入すれば必ず起こる音パターンの変化を探知して警報を鳴らすのである。
- **超音波**　超音波探知システムは，19,000～20,000ヘルツの高周波音を利用する以外は，可聴音探知システムと同様である。可聴周波数帯域内の上限周波数を使用しているので，少数の人（主に子供）には信号音が聞えてしまうことがある。
- **超短波**　超短波システムは，上記２システムと同様の構造で作動する。違いは，超短波が高周波電波だという点である。この種の電波は，400～10,000メガヘルツの周波数で発信される。超短波信号は使用アンテナのタ

イプを変えることにより，保護区域の広さに応じてコントロールできるし，1つの保護区域に複数のアンテナを使うこともできる。またアンテナ1本のシングル・ユニットでも数本使ったマルチ・ユニットでも，可聴音もしくは超音波ユニットとの併用が可能である。

③ **音波振動システム**　（オーディオ）このシステムは，マイクロフォン型の装置を使って保護区域内に侵入した異常ノイズを探知するものである。ただしこのシステムは，たとえば飛行機や工場などの人工的な騒音が侵入してくる場所には，誤動作を起してしまうので当然利用できない。また，中には雨音や雷鳴に反応してしまうものさえある。このシステムの種類としてはノイズの発振源とマイクロフォン型の装置との媒体として，空気を利用する（つまり可聴音に反応する）タイプと壁面などの建築構造体を伝わる機械的振動だけに反応して可聴音には反応しないタイプの2つがある。

- **音波をとらえるタイプ**　（オーディオ）。可聴音探知システムは，保護区域内に設置されたマイクロフォンを使って侵入者を探知する仕組みで，ノイズを探知すると警報が鳴る。このタイプのシステムには，飛行機や雷などによる誤動作を避けるためノイズの原因を電子的に判別する機能を持った取り消しおよび識別ユニットを一緒に取り付けると便利である。
- **機械的振動をとらえるタイプ**　（振動）　このタイプのシステムの作動原理は，上記の音をとらえるタイプと同様である。ただし極端に敏感なマイクロフォンをファイルキャビネット，金庫，窓，壁，天井などに直接セットする点が異る。これらの物体の機械的振動を探知すると警報が鳴りだす。このシステムの場合にも，取り消しおよび識別ユニットが誤動作防止のために必要である。

④ **接近探知システム**このシステムにはたくさんの種類があるが，いずれも異物や人間の接近あるいは出現を探知する仕組みになっている。原理的にいうと，接近探知システムは電界を利用しており，何か物体が侵入してこの電界が　乱されると警報が鳴るようにできている。この電界は，キャビネットの

周囲を導線で取り巻くだけでできあがる。電界は電磁界でも静電界でもよく，いずれにせよ平衡，不平衡の原理が適用できる。電界を設定する方法は，数種類ある。各システムのメーカーによって方法に多少の違いがみられる。また，このシステムは磁気フェンスとして知られているやりかたで設置すれば，キャビネットなど単体の品物だけでなく，ある区域全体の保護用としても利用できる。磁気フェンスは，接近探知システムの総合的な使用例の一つである。その他の利用法としては，ドアや窓の監視用に使われている例がある。

ところで接近探知システムはあくまでも他のシステムの補助として設計されたもので，主警備システムとして使用するには適さない。なぜならば，このシステムは電源電圧の変動とかシステム近くのモップやバケツによっても反応してしまうなど敏感すぎるからである。余り敏感すぎると動物や鳥にまで反応してしまう。従ってやはりこのシステムは，他のシステムのバックアップとして利用すべきものである。

表５－２は，最も一般的な６種の屋内監視システムの比較を示している。

表５－２　屋内監視システムの比較

感知器のタイプ	費用の概算	使用上の注意	突破工作に対する抵抗力
光　度　測　定	＄５００	・エリア外部からの光の遮蔽 ・使用は屋内に限定	高　い
動　作　探　知（超音波）	＄２５０	・風などの空気の動きにより誤動作のおそれあり	中くらい
動　作　探　知（超短波）	＄５００	・超短波エネルギーは壁などを貫通するので誤動作のおそれあり	高　い
音波振動探知（可聴音）	＄２５０	・外部からのノイズによって誤動作のおそれあり	高　い
音波振動探知（機械的振動）	＄１００	・誤動作の原因の発見がむずかしい	高　い
接　近　探　知（区域全体）	＄３５０	・敏感すぎて誤動作のおそれあり ・他システムのバックアップに適する	高　い

重要な区域に対する保安計画を立てる場合，以上に述べた各種の侵入探知器の利用を考慮するほかにも警備員や特に指名されたＡＤＰファシリティ関係者，あるいは施設内部の間仕切りを利用した物理的障壁などによるコントロールを心掛けるべきだろう。間仕切りを設ける場合には，ＡＤＰセキュリティ・プランナーは建築工事の詳細を入念にチェックしなければならない。現代のオフィス建築に多用されている天井構造の制約から，屋内の間仕切りは天井裏までは仕切れない。このことは，侵入者が天井パネルる押し開けば間仕切り壁を超えてどの部屋へも入りこめるということを意味している。侵入の痕跡も残さず，道具も使わずに静かに素早く侵入できるわけだから，これは特に厄介な問題なのである。きらに，間仕切り用のドアフレームはたいていが軽量構造だから簡単に押し入られてしまう。従って屋内の間仕切りを過信しないことが大切なのである。

4.5.6 警備隊の運用

物理的な保安手段，物理的障壁，侵入探知器なども，結局は人間の手が介入しなければ充分に機能しないのである。全時間帯にわたる警備が必要な場所は，ＧＳＡの政府保安サービス（ＦＰＳ－Federal Protective Service）から配属される連邦保安係官が契約を交わした民間の警備保障会社の警備員が監視するとよい。任務の割り当てはＡＤＰセキュリティ・計画に従うが，その際それぞれの職務内容について再確認しておくことが望ましい。

まず，常駐の警備が必要な場所の警備員を指定する。つまりロビー，出入り口ドア，トラック寄せ場，正門，保安本部の常駐員である。これらの場所に配属された警備員の受け持つ仕事は，以下のとおりである。

- 入室許可証のチェックおよび入室者リストの作成
- 外来者に対する識別用のバッジの配布ならびに回収
- 侵入警報システムならびに火災報知システムのモニターと，各警報に対する警備員の迅速な派遣

- 建物に出入りする物資の流れの管理と通行規則の正確な実施
- 建物に対する規則および規準の正確な実施
- 書留郵便の受領

警備員を最も効率的に活用するためには，各警備員の担当任務が必要にして充分なものであることと，各警備員が正規の訓練を受けていることが重要である。たとえば，テープ，ディスクその他のＡＤＰメディアの動きを管理する警備員は，まずそれらの品物を見わけられなければならないしさらに品物の動きについての知識が要求される。また，ある警備員が外来者の受け付けや外来者識別用バッジの準備，案内電話などに忙殺されてしまうなら，とてもＡＤＰ施設要員の身分証明書検査にまで手が回らないだろう。従ってＡＤＰセキュリティ計画に従って警備員の割り振りを行なおうとするＡＤＰセキュリティ・プランナーは，各警備員の担当任務と作業負担を建物の保安責任者（ building security director)ともう一度よく検討して，予定の割り振りが適当かどうかを確認する必要がある。

次に，見回り順路ないしは一般区域の徒歩または乗物による巡回パトロールを行なう警備員を指定する。巡回パトロール員の担当任務は，次のとおりである。

- ドア，窓，その他の開口部が休止時間中，規則どおりに施錠されているか否かの確認。
- 引火物，放置された機器類，通路等の障害物，開放されたままの非常口などの検査，修正，報告。
- 消火器，消火ホース，自動式スプリンクラー・システムの確認。
- ファイル，金庫，機密区域が規定どおり保守されているか否かのチェック。
- 不審人物，不審な動き，異常な匂い，漏電，その他の異常に対する警戒。

巡回パトロールを有効に行なうためには，パトロール員を何らかの形で管理する必要がある。そのためにはパトロール本部に直接戻るか電話による定時報告を実施するか，あるいは携帯２ウェイ無線機を支給するなどの措置が要求される。特に無線機を支給しておけば，緊急事態が発生したときでも直ちに応援にかけつけられるし，応援を呼ぶこともできる。常駐警備員の場合と同様に，ＡＤＰセキ

ュリティ・プランナーはパトロール員の担当任務に無駄や無理がないか，パトロール員はＡＤＰファシリティ保護のための正規の訓練を受けているか否かをチェックしておく必要がある。たとえば，思いもよらないコンピュータ室からきな臭い匂いがしてきたら，パトロール員は警報を鳴らす他に何をすべきだろうか？接触不良のスイッチが原因だったとして，その部屋の電源スイッチを切り，不良のスイッチの位置を探知することができるだろうか？ＡＤＰセキュリティ・プランナーは空調設備，ガス管もしくは水道管の漏れその他，思いがけない時間に発生するＡＤＰ関係の緊急事態についても同様に問題を設定し，これを入念に分析して適切な措置を体系化する一方，各事態に対応して適切な措置をとれるように訓練された警備員を選別しておかなければならない。

第９章で述べる安全教育プログラムを作成する場合に考慮すべき最後の問題は，このプログラム作成に当たる専門要員たちに連邦保安係官や警備契約を結んでいる民間警備保障会社派遣のガードマンを教育の対象として軽視したり無視したりする傾向が認められることである。そうした傾向が専門警備員（連邦保安係官や民間のガードマン等）の感情に及ぼす悪影響はもちろんのこと，この態度はＡＤＰの保安対策を完成させるうえで重要な役割りを演ずる専門警備員に，実際の職務を遂行するに当たって誠意を失わせることにもなりかねない。そのようなことにならないよう，ＡＤＰ管理者や幹部は諸規則を進んで遵守するとともに平常の態度をとおして専門警備員が職務を遂行していたら，懇いの言葉をかけるなどして警備任務に対する理解を示しておくとよいだろう。

4.5.7 物理的保安対策の総合的運用

この章の以上の諸項では，物理的保安に関するさまざまな技術問題について論じてきた。しかし，ＡＤＰ施設においてはそれぞれの項目について新たな安全問題や緊急事態への対応の問題が生ずることも珍らしくない。（各項で明示してきた出来事の結果としてそのような必要が生ずることさえしばしばなのである。）

従って今度はその新たな問題を処理する対抗策が必要になるのだが，そのために物理的保安計画全体がバラバラに展開して統一がとれず，保安システムは費用がかさみ，かつ煩瑣になってしまいがちである。しかし一方では，新たな安全問題や緊急事態の問題，人員や手順に関する問題を全体的に検討することにより，最少の費用で最大の効果をあげるためにはどうすれば良いかを探りあてることもできるはずであろう。

たとえば，以下に挙げるシステムなどはそのような検討を経て実用化されたのである。

ＡＤＰ区域煙探知システム

スプリンクラー・システム作動警報器

建物内全域火災報知器プルボックス

建物周辺侵入探知器

ドア状態探知器

重要区域侵入探知器

区域監視用ＣＣＴＶ

出入口コントロール用ＣＣＴＶ

電子式ドア用錠前

以上は特殊な状況で必要となるシステムであるから，物理的保安計画にはこの中からいくつかを選んで使用するとよい。必要なシステムを一つずつ指定して調達することもできるけれども，必要な全システムをまとめて調達するようにプランニングすると２つの利点がある。１つは，それぞれの警報発令時における人員の反応の点で有利になることである。なぜなら，各警報のコントロールパネルやＣＣＴＶモニターを設置する場所を最少限にまとめられるので，システムをコントロールする人員も最少限ですみ，従ってどの警報が鳴っても適切な処置の指示が迅速に行なえ，しかも実際に処置にまわる人数も余裕をもって確保できるからである。もう１つは，まとめて調達するようにプランニングしたほうが，システムの無駄を省けるという利点がある。すなわち多くの警報器を１箇所のコントロ

ール・パネルに接続するに当たって単一の電気回路で間に合わせられるのであるから，第一に配線工事費が倹約できるし，さらにメンテナンスについても1システムずつ調達した場合に比べてずっとやりやすくなるのである。こうした利点が最も顕著にあらわれるのは，警報器の取り付けが必要な場所のそれぞれについて，数種の感知器が併用できるという点である。また，高級なシステムでは電子ドアのコントロールや各感知器および建物の機械装置の監視などを1台のプロセスコントロール用ミニコンピュータで行なうようになっているので，必要なシステムをまとめて調達した場合の利点はさらに明白となるだろう。

このようなハードウェアの総合的な調達に加えて，ＡＤＰセキュリティ・プランナーは建物の管理者および保安責任者と共同して作業を進めながら，物理的保安計画を支える人的資源についても充分に配慮をめぐらすべきである。全時間帯をカバーする外部の専門警備員のほかに，平常の職務を害さない限りで以下のような人員にも警備を分担させることが望ましい。

受付および案内所の要員

建物の技術要員

建物および敷地のメンテナンス要員

物資の配送係

メッセンジャー

区域監督者

郵便室の要員

以上のような人員の配備場所と物理的保安計画の必要とをにらみあわせて合理的に警備任務を分担すれば，警報発令時にも最少限の専門警備員で必要な処置がとれるようになる。ただし，こうした非専門警備員の活用まで考慮に入れるようになると，もう一度保安システム，特に各種の探知器の設置場所について見直す必要があるだろう。

この章では保安用機器や警報システムについての詳細には，２つの理由からわざと触れなかった。つまり，この分野のテクノロジーは急速に進歩しており，新

製品がほとんど毎日といってもよいくらい市場に出回っているからである。さらに，ＧＳＡの連邦保安サービス（ＦＰＳ）が，各施設の保安要件に対していちいち詳しいアドバイスと専門的なガイダンスを与えてくれるからである。

物理的保安計画が完成したら，ＡＤＰセキュリティ・プランナーは２項目の最終チェックを行なう必要がある。第１項目は，ＡＤＰ施設に対する保安計画や保安規定，保安用機器，警報器，施錠システム，その他の保安関係の事項などが関係者以外，外部に漏洩していないことの確認である。第２項目は，緊急事態の起っている間，緊急事態に対する対応計画と物理的保安方法とが全体的安全性の維持を保証するように入念にまとめられていることの確認である。つまり，たとえば火災警報の悪用に対する警戒が必要であって，ある区域から警報が発令された場合，その区域へ警備員が集中してしまう結果，他の重要なエリアの警備に破綻を生じてしまうというようなことは絶対に避けなければならないのである。

4.6 内 部 管 理

4.6.0 まえがき

前の4つの章では，ＡＤＰセキュリティの目標をささえる物理的方法を示した。本章では，要員，組織構造，データ・ベースおよびプログラミングの4つの分野における物理的保護を強化するために，内部管理の効用について検討する。一般的に言えば，予想される損失の減少の面に限って，内部管理のコストを判断する必要はないであろう。なぜなら，ふつうは管理はおよそ他の目標，たとえばコスト計算，エラーの検出と訂正，マネージメント報告などを行なうのに有効な手段であると思われるからである。ＡＤＰセキュリティ・プランナーは，必要な管理がすでに存在し，どのような修正と拡大が必要であるのかを決定すればよいか，というような事態に出会うかもしれない。基礎的なリスク分析は重要な分野と適用範囲を認識しているであろう。また，物理的セキュリティ対策は人間の介入，支援およびオペレーションを要求するであろう。内部管理がセキュリティ目標を反映する構造になっているのを確かめるべきセクションについて検査する時に，ＡＤＰセキュリティ・プランナーはこれらの要因を心にとどめておくべきである。

4.6.1 要 員 管 理

疑うまでもなく，人間の問題はＡＤＰ施設の最も重要な部分であり，その組織の活動を十分に果すように訓練されたスタッフがいなければ，いかなるＡＤＰ装置も機能することはできない。要員管理は，重要なポジションに対して経験を積んだ信頼できる人々を注意深く選択する必要性，ＡＤＰの任務を十分にはたすために適切なトレーニングを行なうことの重要性，さらに高水準のモチベーションを

達成する際のすぐれた監督の価値を十分に活かすべきである。

4.6.1.1 要員の選択

要員の選択には，トレーニング，才能および経験により，候補者が割り当てられる任務を履行できるかどうかの決定を下す能力が一般に要求される。仕事の熟練度についてのこの決定に加えて，重要なＡＤＰポジションに対する選択プロセスは適切な雇用前のスクリーニングによって重要なポジションに対する候補者の信頼性も確めるべきである。いくつかの水準のスクリーニングが利用できるが，当然ながら，調査が詳細になるにつれて有効性もコストも増加する。従って，利用するスクリーニングの水準は各ポジションの相対的な重要度を反映すべきである。それぞれのＡＤＰ機能に対して，特に重要なポジションをあらかじめはっきり確認しておくべきであり，一般的には，それらは主なアプリケーションとシステムのコンピュータ・オペレーション，データ・コントロール，マネージメント，オーディティングおよび使用テストと保守まで含めたプログラミングを指しているフロードに対するリスク分析によってリスクが発生するぎりぎりの接点を確かめられる。その問題がただ一人の個人にかかわっているような場合には，そのＡＤＰ分野はかなりその一人によって影響を受けやすい状態になっている。このことは，チェックとバランスが欠けていて，隠れたインターフェース，たとえばただ一人のプログラマーがクリティカル・プログラムのクリエーティング，テスティング，デバッキングおよびインストーリング等の業務の相互間の調整に責任を負っている場合に特に当てはまる。最も影響を受けやすい立場にいる者にしばしばシステム・プログラマーであることが多い。オペレーティング・システムの保守を行なう優秀な実行者はデータ・プロセッシングに携わる他のほとんどの人よりも多くの損害を与えることがあり，しかも見つかることが少ないのである。

各々の連邦政府の中央機関または独立機関はある水準あるいはそれ以上の水準の分野の影響度ならびに各影響度の水準に適用されるスクリーニングを指定する際の規定および手順を定めている。ＡＤＰセキュリティ・プランナーはそれぞれ

のＡＤＰ業務の分野に適用する適切な水準を定めるべきである。要員配置の手順は，「アメリカ国家公務員任用委員会フォーム２のPart Ⅰの職種の影響度，Item E — 要員の行動に対する要請」に決定されているように影響度の水準を正しく反映するように定めるべきである。

4.6.1.2 トレーニング

オペレーションの問題とセキュリティの違反の驚くべき数は，個人をその能力以上の立場につけることから生じている。このような人々は非力を認めるというよりも，欠点を隠そうとしてソース・ドキュメントを破壊したり報告を偽造することが知られている。

ＡＤＰ施設を利用してこうしたセキュリティとインテグリティの問題を最小にするためにその要員訓練計画を建てることができる。それぞれの特定の仕事に対するトレーニングは完全で，効果的で，十分であるべきである。しかし，強力な動機を与えることは技術的能力とまったく同じに本質的なものである。各従業員には，その属する機関と役割，ＡＤＰ施設および彼自身の経験の積み重ねの機会についての適切なオリエンテーションを与えるべきである。個人に即したセキュリティ・トレーニングが不可欠といえよう，それはセキュリティ・プログラムの目標とそのオペレーションだけではなく，各スタッフ・メンバーの任務と義務も含むべきである。詳細については，第９章で述べる。

4.6.1.3 監　督

各ＡＤＰ担当責任者はいくつかの方法でセキュリティ・プログラムに大きく貢献することができる。まず第一に，彼は自分を含めたスタッフ一同がセキュリティ規定およびコントロール手順の記述ならびにその意味するところに従っているのを確かめることができる。また，セキュリティを改善するための有効な方法を積極的に求めることもできる。

次に，よき担当責任者は彼のスタッフと緊密かつ効果的な連絡を保つことに努

力する。かなり強い不満が見受けられる時には，しっかりとした処置がとれるように，彼は鋭い感覚と態度を養うべきである。矛盾が解決されないままだとフラストレーションや衝動的な行動に至ることがあるので，状況を無視するよりもその解決を求める方がはるかによいといえる。

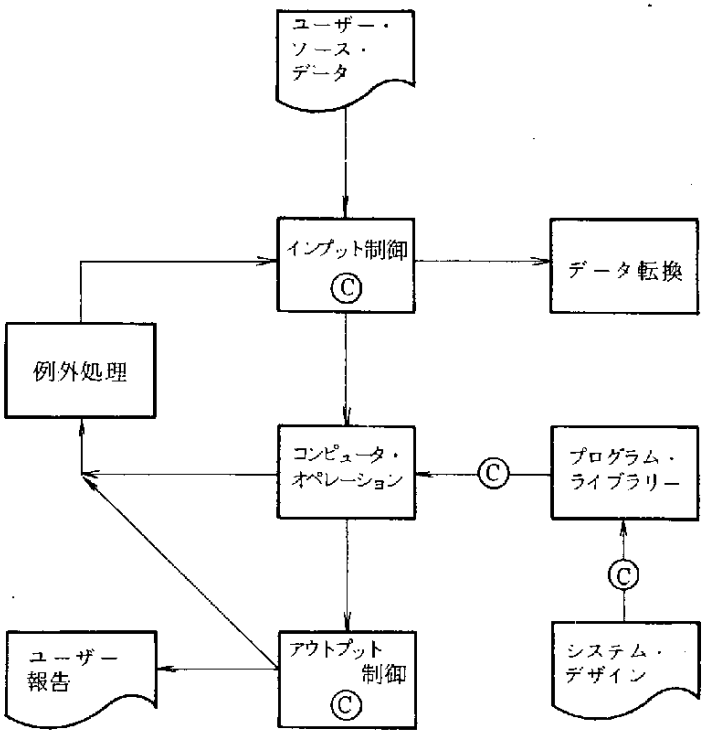
最後に，よき担当責任者はスタッフの各メンバーが割り当てられた任務を履行できるかどうか注意して見定めることである。無能力はいかなる作業状況でも許されるものではないが，ＡＤＰ関係においては結果がことさら判断を誤らせることがある。プログラムは間違った指示をいつまでも忠実に繰返すであろう。一瞬の不注意なオペレーションによってハードウェアが稼動すれば，ファイルを破壊することもある。また，間違ったテープを使う事は仕事を遅らせることがある。エラーや失敗は決して完全には除去できないので，担当責任者は個人を仕事に上手く調和させ，彼に必要な援助とトレーニングを与えるために最善の努力を払うよう自覚すべきであろう。

4.6.2 内部管理のための組織化

任務の分担としてしばしば引用されるテクニックであるが，内部管理の基本原則の一つは，重要な機能の遂行を二人以上の人間に分割することである。理論的には，いく人かの人間が同じ処置を検査する場合にはエラーが見すごされることが少くなり，もし故意に共謀してやろうとしても不正は妨止される。一人の個人は与えられる活動に対して決して全責任を負うべきではなく，特に重要なアプリケーションの処理や開発に関係している場合にはそのようにいえる。行動を起す際に二人の個人が別々ではあっても協力して動くというこの原則は，データ処理の実行にも適用することができる。任務の分担を行なうべき正確なポイントを決定するのに最もよい方法は，ＡＤＰ分野に対する基礎的リスク分析を参考にして弱点の部分を見きわめ，次に侵入者が利用するかもしれないこれらの部分への段階を認識することである。最終的には，その段階ごとの要点をも発見することがで

き，そうなれば任務の分担は望ましい水準の保護を提供することになろう。一般に，任務を分担することによって重要なアプリケーションを管理し，アクセス・コントロールを行なう場合の妥協を防ぎ，拒否するか，受けいれるかの判断における弊害を避けられるであろう。

図６－１は典型的なＡＤＰオペレーションの一般図式であり，有効な管理のポイントが示してある。エラーや失敗を防ぐ対策を計る場合に管理が効果的になるポイントを決定し，またセキュリティの必要性に沿って既存の管理をどのように拡大すべきかを決定するために，ＡＤＰセキュリティ・プランナーはそれぞれの重要なＡＤＰ作業を見通すべきである。例として，給与計算処理（ペイロール・プロセッシング）を考えてみよう。管理は，インプットが正確で有効でありながら，アウトプット，ペイチェック，給与の個人のレコードなどが間違えて他人の手に入らないようにすべきである。ペイロールが大きければ，エクセプション・プロ



Ⓒ：潜在的管理ポイント

図６－１　ワーク・フローと管理ポイント

セッシングは恐らく大事なものとなる。それ故，インプットを準備する事務員はチェック・サインとディストリビーションあるいはペイロール・ファイルへの訂正を管理すべきではない。同様に，ペイロール・プログラムを維持するプログラマーもそのテストを管理すべきではない。これらの係はもちろんもっと単純化される。これらの問題は実際には，直接的に検討してもなかなか明確にならない。大事なことはそれぞれの隠された部分を検討し，任務の分担が損失を食い止めるのに役立ちうるようなワーク・フローにおいてポイントを見きわめることである。

多くのアプリケーションは無効なインプットのリジェクションとその訂正および再入力方法に当てられる。これは貴重な品質管理技術であるが，リジェクトのマニュアル・プロセッシングの導入はフロートならびにエラーに対する意味のある機会を提供する。リジェクトの処理に対する有効な管理は，すべての不完全なトランザクションの様子を見るためにシステム・ジェネレイテッド・ログまたはブックキーピング・ジャーナル・レコードを利用することである。これらのレコードは管理目的に対して独立した監視機能を与えるであろう。任務の分担はログのクリアリングに適用すべきである。また，間違ったインプットの訂正を行なう人物以外の誰かがログ・エントリーのクリアリングの処置を開始すべきである。

計画と手順の変更についての管理はＡＤＰセキュリティ・プランナーから特別の注意を受けるべきである。プログラムをテストから本稼動に移行させる時に，システムを勝手に変更して，そのまま見すごしたり，あまりに移行を急ぎすぎて，不適切なテストによるデータ・インテグリティの損失をまねくことがよくある。営業が出来るプログラムを変更する場合に理想的な方法をとるには，いくつかの異なる組織機能がかかわってくるようなよく整ったシステムが必要である。ユーザー，プログラマー，オーディターおよびオペレーション要員はすべて承認プロセスにかかわるべきである。プログラミングの品質管理は製造における品質管理と同じように重要な概念である。組織的に分離したチェックとフォローアップ機能はプログラムの品質基準を維持する際に価値を発揮することができるのである。

それに，比較的大型のＡＤＰ装置を持つところは最終開発段階に達したすべてのプログラムに対して分離した試験機能を確立することを考慮すべきである。

管理は人間によって行なわれるので，基本的な組織構造は希望する内部管理に答えるものでなければならない。図６－２はプロトタイプの組織図である。キーとなる管理機能，すなわちテストと品質管理，プロジェクト・マネージメント，インプット／アウトプット制御，テープ／ディスク・ライブラリーおよび基準，セキュリティとデータ・ベースの管理が生産機能から分離されていることに注意されたい。これはチェックと管理が効果的に機能するかどうか確かめるのを容易にしている。もちろん，特定のＡＤＰ施設に対する詳細なチェックと管理はそのサイズと内容に依存するであろう。大型のＡＤＰ施設の主な問題がしばしばリソースの効果的な管理であるのに対して，小型のＡＤＰ施設それは任務の分担に際して要求される十分なだけの任務別の人員を確保するという。おそらくは実際的な問題になるだろう。このような場合であって，しかも一人以上の人員が非常に広範囲な管理を受け持つ必要があるとすれば，オーディテイングに頼る必要があるかもしれない。この場合には，よいオーデイト・トレイルが実施されねばならない。

以上を要約すれば，次のようになる。

- 重要なＡＤＰ分野に対して**要員を選択する際には**十分注意する。それぞれの人間が十分なトレーニングと厳重で効果的な監督を受けるようにする。これらの措置は強力なＡＤＰスタッフへの基礎を与えるであろう。
- 損害を与えるエラーやフロードについての要因とメカニズムを見きわめるために，ＡＤＰ施設によって行なわれる**タスク**ならびに管理される資産を**分析する**。
- エラーを最小にしフロードを防止するために，ＡＤＰスタッフの規模の面から許される限度まで，キーとなる管理ポイントで**任務の分担化を図る**。
- セキュリティ目標を満すのに適切なものとして，**内部管理を伴う**任務の分担を**拡大する**。

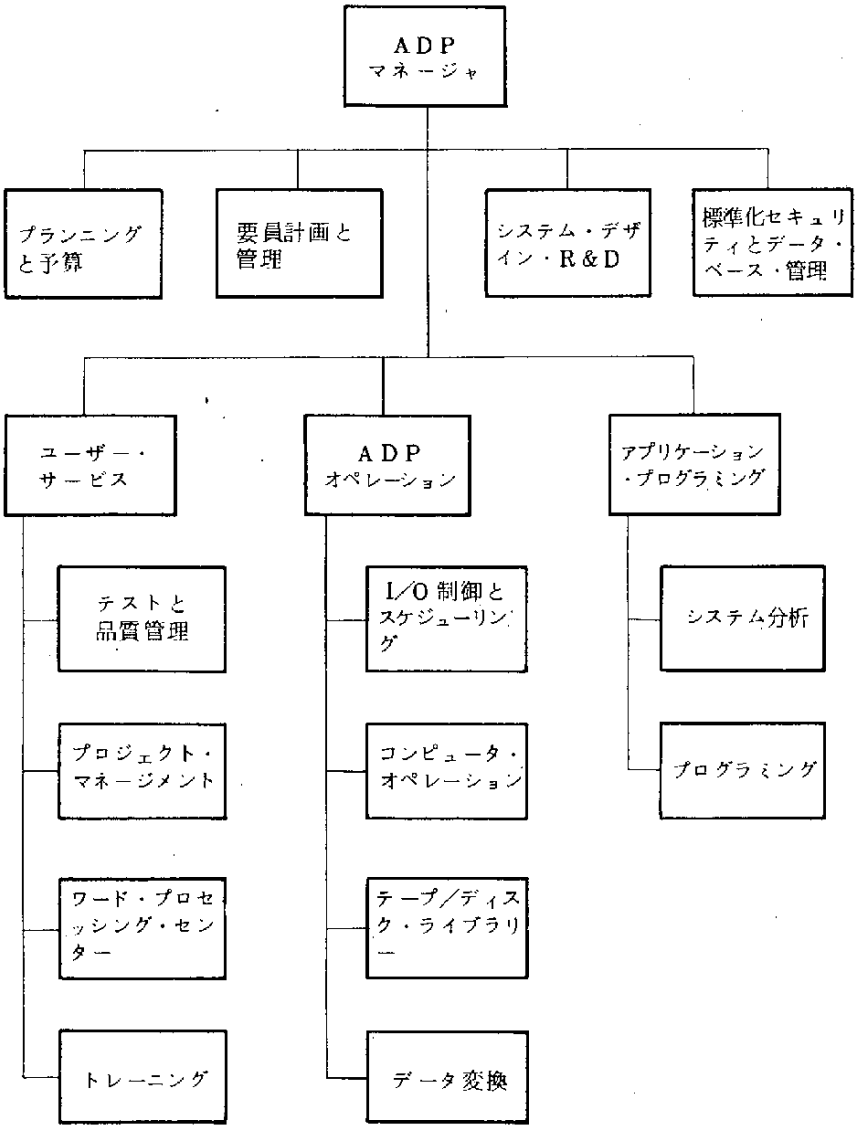


図 6 － 2　プロトタイプの組織図

4.6.3　データ管理

一般的な内部管理は別にして，ＡＤＰセキュリティ・プランナーはデータ・ファイルの管理と保護を特に確めるべきである。連邦政府の規定によって重要であ

ると指定された情報がＡＤＰデータ・ファイルに入れる時に正しく保護されているように注意しなければならない。これは特別の取り扱いや区別あるいは国家安全保障情報に利用されるものと似た他の技術を要求するかもしれない。

ＡＤＰセキュリティ・プランナーはすべてのポイントにおけるデータ・ファイルの物理的取り扱いについても検討すべきである。また，取り扱い中ならびにカストディアル・ストレージ中に，考えられる損失や破壊から保護するのに管理が必要となるインプット／アウトプット・インターフェースのポイントを見きわめるために，ＡＤＰ装置の中のデータの流れを調査すべきである（損失が検出されるかどうか確かめるのにも重要となる）。データが行方不明になった場合には，ＡＤＰ装置は決められた手順に従って運営されなければならない。手による管理技術はテープ／ディスク・ムーブメントの管理形式，インベントリー・ログ，利用についての許可およびクリティカル・アイテムに対する特殊な取り扱いを含むかもしれない。

データ・ファイルの管理にコンピュータ・システムを利用することは，ファイルの数が多ければ特別の考慮に値する。多くの売り手から提供されたテープまたはディスクのライブラリー・マネージメント・システムは巻数，通し番号および名前によってテープのロッキングと管理を与え，データ・ファイルの未許可の消去を防ぎ，自動バックアップ設備を提供する。このようなシステムはオンラインとオフ・ラインの両方のファイルを取り扱う。

似たようなシステムはプログラム・ライブラリーを管理する際にも利用することができる。典型的なシステムは前のすべてのバージョンを保持しながら開発されつつあるプログラムの頻繁な修正を許容する。それは未許可の修正に対する保護を与え，プログラム修正のマネージメントを手助けする。このようなパッケージは，購入されようと自社開発されようと，データとプログラム・ファイルの運用および管理に非常に役立ちうるものである。

コンピュータ以前の時代には，重要な情報，会計元帳，非常に重要な記録などは必要がなければ机の引出し，ファイルまたは金庫にしまっておくのが常識であ

った。コンピュータを使った貴重なデータにも同じ原則を適用すべきである。用事のない人物や許可を受けていない人物を排除するような場合には，テープ・ライブラリーは閉鎖しておくべきである。データの金庫と保管室およびデータ管理室はしまっておく物資（データ）の重要性と価値に従って保護されるべきである。磁場への露出は現実に即して検討し〔12〕，妥当な措置を取るべきである。コンピュータからプリントアウトされたものは暴露を防ぐために正しい手順に従って廃棄すべきである。コンピュータやプログラミングの区域からのデータの盗み出しに対して大規模なセキュリティ管理を施し，しかも同じ情報が紙くず箱，物置ごみの山などから得られるというのでは何の役にも立たない。ＡＤＰセキュリティ・プランナーは第５章に述べた物理的保護プログラムの中にデータの管理の要領が正しく反映されるようにすべきである。

4.6.4 データ保管とバックアップ

前のセクションでは，一般的なデータ・ファイルの保護について検討した。次にすることは通常の保管目標をささえるために非常に重要な記録のマネージメント・プログラムをデータ・ベース・マネージメント・プログラムと統合することである。一般的に言えば，短期と長期の両方のバックアップが要求される。

4.6.4.1 短期バックアップ

短期バックアップは中断やエラーによる仕事の取り消しのような局部的または一時的なロスに対して保護を与える。中断は１ミリセカンド程度しか続かないかもしれず，プログラム（特に，短いものであれば）は容易に再開されるかもしれない。しかしながら，仕事が14時間のプロセッシングにおいて13時間目に中断するならば，仕事を再び始めなければならないのは不経済であろう。従って，すべての長時間にわたる仕事については，中間点でのチェックポイント，リスターティング，リカバーリングおよびバックアップを考慮する必要がある。これはＡＤＰ

設備を運転する誰にとっても耳新しいことではない。それにもかかわらず，一貫したバックアップ・プログラムはまれにしか見られない。

短期バックアップの要領を決定する際には，コスト面への配慮が大きな役割を演じる。たとえば，Xドルのコストでいつでもチェックポイントを出せると仮定しよう。全体の仕事を行なうのにXドルかかるとすれば，どのようなチェックポイントを利用してもコストの上では効果的ではないであろう。また，仕事を行なうのに200Xかかるとすれば，中間点でデータをバックアップするのが恐らく賢明であろう。第4章に述べたシステムの信頼性を再検討することが最善の決定を下すのにおそらく役立つであろう。

4.6.4.2 長期バックアップ

過去のエンバイロンメントを保持したいと望む理由は6つある。

① 過去においてデータ・インテグリティの問題を生み出したエラーの発見。たとえば，6ケ月前に溯るが，昨日まで発見されなかった一連の誤りをたどること。

② 災害の復旧を支援するバックアップ。これらの状況は第8章に詳しく述べてある。

③ マネージメント・パフォーマンスの検査またはプランニング。過去の活動についての情報が保持できるならば，ＡＤＰ設備の将来の目的と活動はもっと容易に予測することができる。また，経験的なデータがインプットとして利用されるならば，シミュレーション・モデルまたは他のプランニング・ツールの利用も高められる。

④ 統計報告上の要件。過去のデータは傾向の分析と外挿法に必要となるかもしれない。

⑤ オーディット要件（内部的および外部的）。過去のエンバイロンメントを分析する能力はオーディターの基本的要件である。特殊な要件については，第10章で検討する。

⑥ 法律上の要件。他の政府機関がデータを必要とするかもしれないし，それらを保持する法令上の要件があるかもしれない。

これらの理由のいずれもが，一定の時点で利用されたプログラム・ソース・コード，ドキュメンテーションおよびデータ・ファイルを少なくとも保存すべきことを示すであろう。ＡＤＰセキュリティ・プランナーは何を保持するかについて考えるべきである。それは全体的なオペレーティング・システムの構成，すべてのドキュメンテーション，コンパイラー，エギュゼキューション・ジョブの言語プログラム，そしてデータ・ファイルであろうか。それとも，プロセッシングのチェインジング・エレメントだけであろうか。何を保持するかをいったん決定したならば，彼はいかにしてそれを保持するかについても決定しなければならない。高度な技術のよきアウトラインは「リアルタイム・システムの信頼性」〔60－65〕の中で得ることができる。

4.6.5 プログラミング管理

技術的に正しいプログラムを作るというはっきりした目標に従って，ＡＤＰセキュリティ・プランナーはプログラム設計，導入テストおよび標準化の問題についてもその管理を行なうべく次のような検討を加えなければならないだろう。

4.6.5.1 プログラム設計

デザインがセキュリティに貢献できる主なプログラムの対象部分は５つある。第一はプログラミングの過程でつねにオーディット・トレイルを考慮することである。基本目標はいかなる時点でもある与えられたデータの状態を把握できるようにすることである。ほとんどの場合，システム分析者とシステム・デザイナーは設計段階に監査者を投入したいと望むであろう。なぜなら，彼はオーディット・トレイルと管理の最適の配置を想定できると思われるからである。

第二は，事後の対策を考えるのでなく，プログラム設計作業の一部として，考

えられるインプットのすべてのエレメントやそれぞれの新しいプログラムのインターフェイスと実際の運営を考慮するようなテスト・プランの開発である。現実に近いインプットの範囲に対してプログラムを試験するだけでは十分ではない。ありそうもない，不法で不可能なインプットに対しても試験すべきである。さらに，単体のテストは一定のプログラムやモジュールの妥当性を確立するのには十分でないのが普通である。すべてのプログラムが同じテスト基準を満す必要はないが，テストの厳格さは重要性，複雑性および影響度に従って決められるべきである。ＡＤＰ設備の必要性に合わせた試験手引書の作成がすぐれた管理を達成するための重要なステップとなる。

第三の管理部分はプログラムの変更についてである。プログラムは将来の変更に対し，やりやすいように設計されるべきである。どんな変更でも，一つのステートメントしか含まないものであっても，許可を求め，承認を受け，すべて例外なく，文書にしたためるべきである。さもなければ，管理が無意味なものになり，プログラム設計の過程をコントロールすることができなくなる。前にも述べたように，プログラム・ライブラリーのメンテナンス・パッケージはプログラムの変更についての管理と保守を助けることができる。変更の詳細を記録することはプログラムの変更についての管理の基本的なものである。今日の傾向はすべてのＡＤＰアプリケーションに対して総合したデータの定義に向っているので，あらゆるエレメントが一意的に決められている。

データ・レコードの精度についての管理が第四の目標である。フィールド，セルフ・チェッキングおよびコントロール・フィールドについての既定の法的価値に対して，キーパンチ・ベリフィケーション，コンピュータ・マッチングを含む広範囲なチェックが考えられる。標準的なデザイン基準はどのような新しいアプリケーション，あるいは旧来の改訂されたものにも施されるべき質的管理を当然含まれよう。

最後に，量的管理は，実行可能であれば，設計過程の段階にも行なわれた方がよい。これらはコントロール時間の合計，ラン・ツー・ラン累計（ハッシュ・トー

タル），トレイラー・レコード，ドル・コントロール，自動チェック・ポイント／インターラプション・ルーチン，インプットとアウトプットのレコード・カウントの検査等その他の類似のものがあげられる。質的管理と量的管理での違反はエラーの未処理状態のまま維持されるエラー通告を出来るようにしておくことが大事である。

量的管理と質的管理の必要性はリスク分析によって決定されるべきである。アプリケーションが非常に重要であるかきわめて危険をおかしやすいものか，あるいは大量のＡＤＰリソースを使用するような場合には，これらはさほど重要でなく，危険度が低いアプリケーションよりさらに注意が払われなければならない。

4.6.5.2 プログラム導入

プログラミング段階における最も敏感なポイントの一つは，アプリケーションの生産体制への導入とライブ・データ・ベースに対するそのオペレーションである。新しいプログラムの導入は，プログラムとシステムの徹底的なテストが実施され承認された後にのみ行なうべきである。この承認を受けたプログラムがより構造的に優れていれば，それだけ管理もしやすくなる。プログラマー，テストまたは品質の管理を行なう部門，オペレーション部門およびユーザーは，プログラムを設計から最終導入テストに持っていき，さらに現在稼動中のシステムに入れる際にすべての者が参加する方がよい。しかしながら，承認が単なる儀式にならないように注意を要する。それぞれのプログラムは詳細で独立した検査を受けるべきである。大型のＡＤＰ装置を持つところではプログラムテストと管理のグループを分けて検査を行なうようにするとよいだろう。小規模のＡＤＰ装置ならば，プログラムを導入する過程に必要な特別な手順を決定するだけで十分であろう。その過程は既存のグループによって実行されることになっており，そのためには，可能な限り業務を再調査し，分離する必要がある。繰りかえしていえば，独立した主体により再調査され，承認された十分で完全な書類がないかぎり，どんなプログラムも受け入れることはできない。災害や中心的なプログラムが役に立たな

いといった場合に，その文書が不十分なものであれば，ＡＤＰ装置は損失にたいし極めて弱点をもっていることが明らかになるだろう。図６－３には，技術情報と同様，管理を必要とする文書を，一組にして示してある。

略　号

Ｉ：ドキュメントを作成する

Ａ：ドキュメントを承認する

Ｕ：ドキュメントを使用する

		ユーザ	システム設計	プログラミング	ジョブ・コントロール	オペレーション	ＡＤＰ管理
実行研究	研究要請	I	U				A
	システム要求	I	U				
	コストとスケジュール	A	I				A
システム設計	システムのフローチャートと説明	A	I	U	U		A
	ソースドキュメントとインプット	A	I	U	U		
	レコードとファイルの組織		I	U	U		
	アウトプットとレポートのフォーマット・インストラクション	A	I	U	U	U	
	ユーザ，キーパンチ，コントロールのインストラクション	A	I	U	U	U	
プログラミング	プログラム説明とフローチャート			I			A
	コーディング			I			
	プログラム・テストの要求とスケジュール			I	U		A
システムテスト	テスト要求とスケジュール	A	I	U	U	A	A
	テストレポート	A	A	A	I	A	A
インプリメンテーション	インプリメンテーション・スケジュール	A			I	U	A
	データ変換プラン	A			I	U	A
	ユーザの受入	A			I		A
オペレーション	プログラム保守		I	U	U		A
	プログラム修正	I	U	U	U		A

図６－３

4 6.5.3 ドキュメント管理

上述のデータやオペレーション，システム設計，プログラミング，導入テストについては，それらが十分に効果的なものとなるためには，ドキュメント化される必要がある。そのために用意すべき書類は，手順マニュアル，オペレーションおよびユーザーのハンドブックなどといった名前で呼ばれる。そうした書類を作成する責任を負うのは，規模の大きいＡＤＰ装置の手順について扱うグループである。規模の小さいＡＤＰ装置では，その特殊な分野を文書化することを個人に要求することになろう。いずれの場合にも，ＡＤＰセキュリティ・プランナーが参加することになる。プランナーは上述のＡＤＰ装置のセキュリティ対象を分析したうえで，セキュリティ目的を達成するための実行あるいは標準の役割を決定すべきである。ＡＤＰの管理目標と同様，それらのセキュリティ対象にもとずき，そのＡＤＰ装置に見合った手順の計画を形成すべきである。プログラミングの手順マニュアルに必要な例としては付録に掲載した。

4.7 オフサイトＡＤＰ施設のセキュリティ

4.7.0 まえがき

オフサイト（遠隔地）のＡＤＰ施設を利用するのは，以下の４つの基本的な理由のためである。

① 一つの機関のＡＤＰニーズは，イン・ハウスＡＤＰ施設を認めるには小さすぎる。日常のデータ処理がサービスビューローで最も経済的に行なわれる業務は，その一例である。

② オンサイト（センター）のＡＤＰ施設の効率化と経済化が，オフサイト施設を業務のピーク時の処理に利用することにより図れる。

③ オンサイト施設からは経済的に提供されない特殊サービスが，オフサイトＡＤＰ施設から入手できる。特殊なジョブのために相互タイムシェア・コンピュータを使用できることが，オフサイト施設を利用するうえでの特徴である。

④ オンサイトＡＤＰ施設にたいして壊滅的事故や重大な被害のあった場合，重要なＡＤＰ作業は，オペレーションを支援するため事前に選定されたオフサイト施設に移すことが出来る。

①～③は現在日常，行なわれている利用の理由を表わしており，それは連続して前年を上回る傾向にある。④はインハウスＡＤＰ施設のための当面の計画作業，あるいはオフサイトＡＤＰ施設のバックアップの結果として，使用されるものである。ここで推奨されていることは，オンサイトＡＤＰ施設を目的とした以上のガイドラインのなかに表現されている，基本的セキュリティについての考え方がオフサイトＡＤＰにも同様に適応できるということである。

本章では，オフサイトＡＤＰのセキュリティを評価するにあたり，ＡＤＰセキュリティプランナーが当面しなければならない問題について触れてみよう。基本

的には，オフサイトＡＤＰのユーザーの位置は，銀行における預金者の位置と非常に似ている。すなわち，ある１人の資産の保護が，別の組織に引きわたされる。不幸なことに，オフサイトＡＤＰのユーザーは銀行の預金者に与えられているような保護 — 法律，独立した監査，FDICなどを受けていない。実際，個人ユーザーのセキュリティ要求と関係のないユーザーにたいしては，ＡＤＰサービス・ビューローはせいぜい一定水準のセキュリティ（それも，時として不明確な）を提供しているだけである。一般に，典型的なＡＤＰサービス・ビューローはユーザーにたいする特殊なレベルでのセキュリティ保護は保障しないし，データの盗難により，ユーザーが処理の遅延やそれ以外の被害によって損失を受けることがあっても，その責任を負わない。

以上の理由から，オフサイトＡＤＰ施設で処理されている仕事が十分なセキュリティ手段によって保護されていると仮定しても，それはユーザーにとっての安全を意味しない。結論すれば次のようになる。ある機関がそのデータの一部あるいは全部の処理をオフサイトＡＤＰ施設（そのオペレーションを機関としては制御できない）で行なうことは，そのデータの紛失や誤った使用について機関の責任を軽くすることにはならず，機関の業務を行なう上で障害になる処理の遅れを回避することにならないということである。事実，利用機関がセキュリティを直接にコントロールできないという事実は，セキュリティの分析をより重要なものとしている。従って，オフサイトＡＤＰ施設を使用している機関は，本章で述べたようなＡＤＰのセキュリティ・プログラムを支持するように推奨することができる。

オンサイトおよびオフサイトによるＡＤＰが組合わされて使用される場合，オンサイトＡＤＰのセキュリティ計画に責任をもっている人間は，たぶんオフサイトＡＤＰ計画についても同様に責任をもつべきである。またオンサイトＡＤＰ施設が無い場合には，ＡＤＰのセキュリティ・プランナーは，機関のなかで重要なレコード管理の責任をもっているか，あるいはＡＤＰの主要ユーザーのなかから，最善を尽して選択されるべきである。指名を受けたＡＤＰのセキュリティ・プラ

ンナーは，機関内の全ＡＤＰユーザーから支持と協力を取りつけるべきであり，また第 1. 3. 2 項で触れた専門家の忠告を受けたり相談をしたりすべきである。

4. 7. 1 セキュリティ要求の分析

第 1. 3 節で述べたリスク分析にたいして，基本的な技術が適用する間は，オフサイトＡＤＰ施設が使用される時，以下のアプローチは役に立つであろう。

- 第 1. 3 節で述べたように，使用機関に対して，**ロスの潜在的見積り**をする。
- 第 1. 3. 2 項で述べたように，**脅威の分析を行なう**。ただし，1 種類の環境にたいして（オンサイトＡＤＰ施設については第 1. 3. 2 項の討論に暗示してある），一般には，以下の 4 種類の異なったセキュリティ状況と環境があることを考慮すべきである。

  ① 利用している代理機関に管理されている間の，ソース書類，データファイル，ＡＤＰドキュメントのデータ・エントリーとアウトプット・ハードウェアおよび関連事項の保護。

  ② 利用している代理機関とオフサイトＡＤＰ施設の間を伝送中のデータの保護。データは電気的あるいは物理的にも転送可能である（ソース書類，機械読取りメディアあるいはアウトプット・レポートとして）ことに注意する。

  ③ オフサイトＡＤＰ施設でＡＤＰオペレーション利用をしている代理機関のセキュリティ。その機関は，オフサイトＡＤＰ施設によって管理されている既存のセキュリティ計画に参加するか，あるいは，機関自体のオフサイトＡＤＰオペレーションを保護するために，独自の暫定プランを作り，それを推持する方を選ぶかもしれない。

  ④ 利用している代理機関のオペレーション計画を支持するために，オフサイト位置に貯蔵されているデータやプレプリント・フォーム，それ以外の資材の保護。

• 第1.3.3項に述べたように，**年間の予定されるロスを見積る。**見積りの基礎は，多方面にわたって一つのサイトだけの場合と当然違ってくるはずである。利用している代理機関は，オフサイトＡＤＰ施設での有形の資産の破壊（自機関のテープやディスクパックなど以外）により，損失を受けることはない。同様に，バックアップする場所でのデータファイルやそれ以外の資材が破壊されても，それを取り替えるための費用がかかるにすぎない。それらの条件については，第1.3.1項にあげた潜在的な損失の５類型について，以下の表７－１に集計してある。Yesの項は，損失の潜在性が完全なオンサイトＡＤＰ施設と同様であることを示し，Noの項は，損失のメカニズムが存在しないことを意味し，Minorは，データやドキュメンテーション，関連項目の取替えに要する費用が比較的小さいものに損失が限定されていることを示している。

ＡＤＰ施設のプランナーは，自分の行なった損失の見積りが全ての重要なファクターを含んでいることを確認するために，自分の特殊な立場に合わせて，表７－１に示された仮説の妥当性を試してみるべきである。

表７－１

潜在的な損失の類型	損失の場所			
	オンサイト	伝送中	オフサイト	バックアップサイト[e]
物理的損失	Yes[a]	Minor	Minor	Minor
データの紛失	Yes	Yes	Yes	No
データの盗難	Yes	Yes	Yes	Yes
間接的盗難	Yes	No[b]	Yes	No[c]
処理の遅延	Yes	Yes	Yes	No[d]

（注）

a　ハードウェアがリモートターミナルに限定されているため，完全なオンサイトＡＤＰ施設の場合に比べ，可能性はずっと低くなるであろう。

b　転送中のデータに干渉しても発見されないことが確認されている。

c　バックアップ・ファイルの利用に圧力をかけるために，横領犯人が保護の不十分なファイルに干渉し，オンサイト・ファイルを破壊する可能性は考えられる。しかしながらこれは相当に不自然なコジツケに近いシナリオである。

d　オペレーションの場所と同じように大事件により，バックアップ用の資材が破壊されれば，同時に，処理の遅れが始まる。仮に，オペレーションおよびバックアップの場所が同一の地震断層線上にあったとしても，バックアップの場所は，関連被害の可能性を最少にするように選定されている。

e　利用している代理機関がオフサイトＡＤＰ施設でのオペレーションをバックアップするために，資材を貯蔵するところとして自社の設備を使用する可能性があることに注意を要する。

4.7.2 オンサイト・セキュリティ

ＡＤＰ操作のオンサイト部分についてのセキュリティ分析は，本書のこれまでの各章で述べた方針によって行なわれる。明らかなことは，処理がオフサイトで行なわれるとしたら，ＡＤＰセキュリティ・プランナーは，広い幅をもった複雑なＡＤＰ施設の保護について自分では直接手を下す必要がなくなるが，以下の諸点について，考えてみてもよいだろう。

- 物理的保護，アクセス制御，**ソースデータに対するデータ制御**が集中しているところで，そこは犯罪人が狙う場所に十分なりうるか，あるいは，データの完全性に対する責任がユーザーからＡＤＰのオペレーションに移るところでもある。
- 誤用やサボタージュ（物理的アクセス制御にする妨害）などの脅威，火災や水害による被害，ターミナルにたいする物理的被害，あるいは電力，通信回路にたいする妨害によって引きおこされる処理の遅延などから，**リモートターミナルを保護する。**
- **オンサイトに保存されている**データファイル，ドキュメンテーション，それ以外のバックアップ資材の物理的保護。

4.7.3 輸送中のセキュリティ

セキュリティ分析をするにあたり，データやドキュメントが輸送されている間の漏洩について考える必要がある。本書の取扱い範囲から除外されている電子データ転送の妨害は別として，以下の諸点を考慮にいれる必要がある。

- **インプットの物理的損失**　再構成に要する費用や処理の遅れによる損失が大きい場合には，輸送中に破壊あるいは紛失されたインプットを早急に取替える処置を施すべきである。磁気メディアの事故による消去は事情が異なり，磁気的にシールドされた船舶用の容器を用いることにより，簡単に保護することができる。熱，X線，レーダーなどは，いずれも過大評価された脅威であり，ミネソタ鉱業製作所から出されたテクニカルレポート〔19〕およびNBSレポート〔12〕にもとづき，常識的な予防策で防ぐことができる。しかしながら，幾分かはこれらの危険にたえずさらされており，また積み荷の宛名が間違っていたり落とされたりする可能性もある。
- **アウトプットの物理的損失**　印刷物やマイクロフィルムの形をとっているアウトプットは，一般郵便物と同様の危険にさらされている。しかしこの場合，配達が確認されるまで，オフサイトＡＤＰ装置のアウトプットされたデータファイルを保管するという簡単な方法で保護できることは明らかである。結局，配達されていないという連絡があれば，すぐに替りの手段を講じることができる。換言すれば，未配達（可能性の少ないことだが）が一定の時間内に報告されなければ，オフサイトＡＤＰ施設側では配達されたものと仮定し，それ以上，アウトプットファイルを保存する必要がなくなる（この場合各々の配達があったという報告よりも，例外的な報告によるリスクがはるかに大きい）。
- **漏洩にたいする保護**　紛失の可能性の分析により，インプットであれ，アウトプットであれ，それらは傷つきやすいものであり，悪意による暴露から保護する必要があると結論されるかも知れない。恐らく，必要とされる保護の

程度は，潜在的な加害者にとって暴露する価値と保護する側にとってそれらの利用価値の水準との関係で決まるだろう。輸送中の重要度によってクラス分けされた資材にたいして，適用される保護技術は，分けされていないが影響を受けやすい情報にたいし，保護技術を開発するうえでのガイドラインとして使われる。

- **干渉からの保護**　紛失の可能性の分析により，インプットであれアウトプットであれ，それらが不正な目的による干渉の対象となることがある。インプットの保護は，一般に同種類のコントロールに役立てることができる。たとえば，インハウス処理に応用できる。しかしながら，その手段がインプットデータだけでなく，コントロール情報も同様に保護するかを調べるために考慮する必要がある。その理由は，誰かがデータをコントロールするために，インプットデータを隠し，別の物を補って干渉する可能性があるからである。

理想的には，情報のコントロールはオンサイトで行なうべきであり，アウトプットはオンサイトのコントロールデータにたいして照合されるまで，手離されるべきではない。しかしながら，時間的な拘束からオフサイトＡＤＰ施設において照合する必要がある場合には，コントロール情報は輸送の間，保護されなければならない。最終的に防止する価値に重きを置くとすれば，たとえ遅れたとしても，後になってのオンサイトの確認過程で干渉は発見される。

ＡＤＰセキュリティ・プランナーが記憶にとどめなければならないことは，多くの例の詐欺行為が，形を変えたアウトプットの偽物によって隠蔽されてきたことである。たとえば，最近の報告によれば，銀行の休止中の口座から基金を横流ししたことは，その口座の持主に形を変えた声明を送ることによって隠蔽されていたという。この詐欺は，処理が遅れた結果，横領犯人が代替物を作ることを妨害して発見された。*このエピソードは，この種の詐欺は詳細なアウトプットレポートさえあれば発見されること，また，そうしたアウトプットレポートに干渉することにより（少なくとも一時は）隠蔽される

＊　「128,000 $の銀行の紛失におけるＤＰ図」Computerworld，1973年2月3日号，Ｐ1。

ことを指摘している。船便によって，ある場所から遠く離れた別の場所へ送られるアウトプットが，代替物を考えた干渉の対象として一番狙われるようである。

4.7.4 オフサイト・セキュリティ

インハウスＡＤＰ施設のところで述べた技術が，同様に，オフサイトＡＤＰ施設のセキュリティ分析に用いられるが，ロスの可能性の違いの結果として，強調する点が異なっている。たとえば，バックアップ側で全体の時間の0.5％オペレートすると見積るならば，遅延による処理のロスは，正常に用いられているＡＤＰ施設において等価物の0.5％に似かよったものとなるだろう。換言すれば，バックアップ側で我々が少しだけオペレートするつもりであれば，我々にとっての信頼性もそれだけ重要なものでなくなるということである。従って，有用性や処理の完全性，技術的両立性，便宜性などを評価する場合，我々はそれらのファクターを更に強調することができる。

日常的に用いられているオフサイトＡＤＰ施設を強調することは，オンサイト設備を強調することと同じである。ただし，その人の関心が自分の資産にだけ限定されていることが明らかな場合は例外である。ＡＤＰセキュリティ・プランナーは，オフサイトＡＤＰ施設のセキュリティ分析を開始するにあたり，オフサイトＡＤＰ施設から入手できる以下のドキュメントの見直しから着手することができる。

- 最新の**リスク分析**のコピー
- **当面の計画**のコピー ― 今日まで残っている場合は，テストされたなかで一番新しいもの。
- 最新の**セキュリティ検査**のコピー。日付と担当者。
- **セキュリティ政策**と手段のコピー。
- それ以外のＡＤＰの**物理的セキュリティ**について，全てのコピー。

入手できる書類を基礎に，オフサイトＡＤＰ施設の観察と調査，機関のもつロスの可能性についての見積りなどに関し，ＡＤＰセキュリティ・プランナーはオフサイト施設について次の結論のなかから１つを引き出すことができる。

① オフサイトＡＤＰ設備におけるセキュリティ・プログラムは受けいれることができるが，分離したバックアップの用意をする必要はない。恐らく，使用機関はオフサイトＡＤＰ施設におけるセキュリティ計画に参加し，協力するであろう。

② 使用機関のデータやそれ以外の資材についての保護は十分であるが，信頼性と暫定計画は不十分である。すなわち，処理の遅れにたいする危険性は，受け入れがたいものと考えられている。使用機関がそれ自体のバックアップ計画を開発し，維持することが可能であることを発見したと仮定すれば，そのセキュリティ・プログラムが不完全なものであるにもかかわらず，オフサイト施設の使用は正当化されることになる。しかしながら，その独立したバックアップ計画のコストは，オフサイトＡＤＰ施設の価格／業績評価のファクターとなるであろう。

③ オフサイトＡＤＰ施設におけるセキュリティは，不十分であると判断されている。この場合，オフサイトＡＤＰ施設の管理を調整することは可能である。その目的は，セキュリティの全般的な質の向上か，あるいは必要とあらば，利用している代理機関のデータの特別な操作など，利用している代理機関が特殊な方法を講ずるかの，いずれかである。しかしながら，管理上，セキュリティの質の向上が思わしくないか，あるいは不可能な時は，その機関は別のところでＡＤＰサービスを探す必要がある。

リスク分析が完了し，オフサイトＡＤＰ施設が選択されたら，その利用している代理機関は，本書の別の部分で述べられているＡＤＰセキュリティ計画を支持しなければならない。特に，以下のことは忘れてはならない。

① セキュリティ政策と手順は文書化しておくべきである。

② ＡＤＰのセキュリティの責任を負っている機関の要員に，適切な教育，訓

練，管理を受けさせておく必要がある。

③　ＡＤＰセキュリティの検査プログラムを確立しておくべきである。利用している代理機関は，オフサイトＡＤＰ施設によって実行された検査が，たとえ全体にわたらなく，検査を必要とする部分にたいしてであっても，それを信用することができることにとに気付くであろう。

4.8 偶発事故対策計画

4.8.0 まえがき

各連邦政府機関にはそれぞれに分担された任務があり，この任務を遂行し完成するための計画が立てられている。このような計画設定の際，ノーマルな労働条件，機関のリソースおよび人材，組織全体の落着いた環境等が備わっていることが前提とされる。しかし，ＡＤＰセキュリティ・プランナーは，保安対策をいかに慎重に実行したとしても，正常なオペレーションを妨げ，その機関の任務の遂行を妨害するような突発事故が起り得るという点を考慮に入れなければならない。このような理由から，偶発事故の対策がＡＤＰセキュリティ計画に含まれなければならない。

ＡＤＰ施設のための偶発事故対策計画として次の３種類の対策が考えられる。

緊急対策：火災，水害，市民の妨害，天災，爆撃の脅威などの非常事態が発生した場合，生命を守り，資産へのダメージをできるだけ制限し，ＡＤＰオペレーションに対するインパクトを最少限にとどめるための対策

バックアップ・オペレーション：ＡＤＰが破損されても本質的なタスク（リスクの分析によって識別されたような）をそのファシリティが十分に復旧するまで続行して完成するためにバックアップ・オペレーション計画が準備される。

復旧：復旧計画は，ＡＤＰ施設の物理的な破損や大きなダメージをスムーズにかつ迅速に修復するための対策である。

4.8.1 偶発事故対策計画の準備

偶発事故対策の上手なプランニングは安定したＡＤＰオペレーションを保証し，

それによって実質的な効果が得られる。一方，公式的には任務の分担は，第1.4節で説明されたセキュリティ・プログラムの一環である適切な目標設定，予算，スケジュールによって決定されると言うことができる。さらに，他の分野からの適切な要員の参加も必要となるだろう。図8－1は任務がどのようにセットアップされ，割当てられるかを示したものである。言うまでもなく，各ＡＤＰ施設が，それぞれ独自のやり方を採用し，そのリソースを十分に利用しようとするのは当然である。

役割	任務の担当要員									
	ユーティリティ・プランナーADP管理者及びセキ	ユーザーの代表	建物の管理	建物の保安	法律コンサルタント機関	調達部門	公共建築サービス(GSA)	機関の監査役	機関のマネジメント	参照すべき章、節
1. 任務分担の設定	*								*	8.1
2. 復旧のための所要時間の予測	*		*			*	*			8.1
3. 故障モードの分析										8.1
ＡＤＰハードウェア	*									4.0
ユーティリティの故障	*		*							3.0
火災，水害など	*		*	*						2.0
4. 潜在的損失	*	*			*			*	*	1.3
5. 緊急対策計画	*		*	*	*				*	8.2
6. バックアップ・モードの選択	*	*		*	*			*	*	8.3
7. 復旧計画	*	*	*			*	*		*	8.4

図８－１　偶発事故対策計画のための組織と役割

バックアップ・モードの選択(6)は，部分的には２つの基本的な要素に依存している。復旧に要する時間(2)は，バックアップ・オペレーション時間の許容最大限

度を決定する。個々のＡＤＰ任務に関連のある潜在的損失(4)によって，大きな損失をひき起さない程度のプロセシングの中断時間の最大許容限度が決まる。故障がこの限度を超えて続くような場合には，バックアップ・オペレーションが始動する。

故障モードの分析(3)によって，ＡＤＰセキュリティ・プランナーはバックアップ・オペレーションを促進させなければならないような事態をひき起こす事故を識別することができる。基本的には，そのアプローチはリスクの分析によって主に３種類の等級に分られる破損の程度によって決まる。その程度は，機能の局部的損失，オペレーションの中断，大規模なダメージ又は破壊の３種である。これを表にすると次のようになる。

表８－２　ＡＤＰ施設の被害とその原因

破損の程度	主　な　原　因
ＡＤＰ機能の局部的損失	1. 主要周辺装置の故障 2. 空調装置などの局部的損失 3. 通信回線の故障 4. キー・プログラム，ファイル，プリプリント・フォームの損失 5. 要員のミス
装置にダメージをほとんど，もしくは全く受けないでＡＤＰオペレーションが中断した場合	1. 労働争議，デモンストレーション，市民の妨害 2. 電源，空調装置の故障 3. 爆撃の脅威，ガス漏れによる退去 4. 主要なＡＤＰハードウェア・ユニットの故障 5. コンピュータ室の火災，ＡＤＰハードウェアのサボタージュ，局地的水害 6. 煙，ほこり，ちりの侵入
ＡＤＰファシリティや内部の装置の大きなダメージや破壊	1. 大規模な火災 2. 地震，洪水，あらし 3. 爆撃，爆破，飛行機の墜落

図8-2で示された3種類の破損にはそれぞれ次のような特徴がある。

機能の部分的損失　これによって影響を受けるのは，わずかなタスクに限られる。どのようなバックアップが必要かを決めるために，セキュリティ・プランナーはそれぞれの原因を影響を受けたＡＤＰ任務に関連させて調べなければならない。このような役割は修復の時間的余裕や潜在的損失という点でそれぞれ異なる。例えば，ソース・ドキュメントからのデータをエントリするのにＯＣＲ装置を利用している場合を考えてみよう。修復時間がＯＣＲを利用したタスクのサイクル・タイムより短かい場合，恐らくバックアップすることはできないだろう。一方，ＯＣＲが1日3シフト，フルに稼動している場合，交互にデータ・エントリを行なう方法が必要となるのは明白である。

もう一つの例は部分的な空調装置の故障である。コンピュータ室に3つの異なる空調装置があると仮定して，修復時間が8時間かかり，３０分のうちに室の温度が許容限度を超えるとしよう。ＡＤＰハードウェアを止めて，室の照明を消すことによって，室温を許容レベルに保つことができる。ＡＤＰセキュリティ・プランナーは，これらの業務を果せる，熱をあまり出さないノーマルなコンピュータのサブセットがあるかどうかを調べるために，8時間の遅れによって損害をこうむるような業務のリストをチェックする。それができない場合は，空調装置の故障をバックアップする操作が必要となってこよう。

オペレーションの中断　ダメージをわずかに受けたか又は全く受けないでオペレーションが中断した時は，ＡＤＰ業務全体が影響を受けるが，中断の原因が除去されると，装置の正常なオペレーションが再び始められる。典型的な原因の例を調べてみると，中断時間はコンピュータ室の火災の後の復旧の所要時間であるとか，市民による妨害や電源の故障などのようなＡＤＰ設備の管轄外の要素に依存していることがわかる。

大きなダメージや破壊　ＡＤＰ施設の所在地一帯に及ぼすほどの大規模なダメージに耐えることは不可能であり，バックアップ・オペレーションが必要とされる。もとの正常な状態に戻すにはＡＤＰ施設全体の修理と再構成が必要である。

ＡＤＰセキュリティ・プランナーは，バックアップ復旧対策計画がこの非常事態に十分に対処するものであるかどうかを検討しなければならない。

大きなダメージを受けた場合，バックアップ・オペレーションに切換えなければならないことは明白である。局部的なダメージや中断の場合，どうすべきかということはそれほど明確ではない。適確な決定を下すために，ＡＤＰ責任者はどの業務が被害を受けたか，復旧に何時間かかるか，修理をして，もとの状態に戻すために必要な情報と援助を得るには誰に頼めばよいかということを考えるだろう。このような事故を分析していくうちに，ＡＤＰセキュリティ・プランナーは多くの必要な情報を集めることができるはずである。この情報にほんの少し手を加えるだけで，ＡＤＰ責任者は判断を下すための有効な資料を得ることができるだろう。この資料となるドキュメンテーションは，それぞれの事故に関する次のような要素を含んでいなければならない。

- 正常なオペレーションが再開されるまでの中断時間を予測するためにあらかじめ準備できる事項。
- 事故がどれくらいの時間続くかを推測するのに必要な情報を提供できる個人又は機関
- 正常な状態に戻す作業を依頼できる個人又は機関

収集されるべき情報の例を下に示めしてみよう。

空調システムの故障

(1) 修理時間

サーキュレーティング・ポンプ — ｘ時間

チラ — ｙ時間

(2) 修理時間の予測

建築技術 — Mr. S. Smith

内線　３４５

(3) 修理協力者

建築技術 — Mr. J. Jones，　内線　５６７

電源の故障

(1) 修理の所要時間

その建物だけの停電 — x時間

局地的な停電 — y時間

広汎な地域全体の停電 — z時間

(2) 復旧時間の予測

建築技術 — Mr. S. Smith　内線　345

電力会社の急報 —（電）　321－7654

(3) 復旧サービス

ビルの電気技師 — Mr. J. Jones,　内線　789

電力会社の地域修理事務所 —（電）　567－6543

ＡＤＰハードウェアの故障

(1) 修理時間

ＣＰＵ — x時間

マルチプレクサ・チャネル — y時間

ディスク・ストレイジ・コントロール — z時間

(2) 修理時間の予測

売り手側Ａ代表者 — 内線　543

売り手側Ｂ代表者 — 内線　789

(3) 修理協力者

ＡＤＰオペレーション・マネジャ — Mr. W. Brown,　内線 555

以上は，規準をどのように設定したらよいかを示す一例にすぎない。これには，修理時間とか，夜間，週末，交代時間などサービス要員が手薄なため，サービスが不十分であることなどに影響を受ける要素についての簡単な注釈もつけ加えておくとよい。決定的な遅れを起しそうもないような事故に関する情報まで集める必要はないだろう。

4.8.2 緊急対策計画

ここで言う緊急対策計画とは，非常事態が生じた直後，生命や財産を守り，非常事態のインパクトを最少限にとどめるためにとられる対策を指している。「ファシリティの自衛計画モデル」〔14〕は典型的な政府関係の建物に共通な条件を考慮して作成されている。ＡＤＰセキュリティ・プランナーは，市民の妨害から装置を守ったり，火災や洪水などの後に起るコントロールの破綻など，ＡＤＰオペレーションを左右するような非常事態に伴なう様々な現象を確認するためにリスクの分析を再検討しなければならない。プランナー自身がそのような事態を体験すれば，ＡＤＰ施設の特別なニーズを満すために，ファシリティの自衛計画を改正せざるを得なくなるだろう。また，プランナーは役に立つ管理手順について述べた，「火災時のマネジメント・コントロール」〔31〕や市民自衛救命訓練計画の復活と救命用具のリストを含む「非常救命訓練」〔8〕についても意見をきくことになるだろう。

コントロールの破綻は特にＡＤＰ施設にとって深刻である。最近起った多くの火災や洪水によって，ダメージを制限するための準備がいかに大切な要素であるかということは十分，証明済みである。各部門の責任者がオペレーションおよび主要な装置や記録物の蔵置場所を再検討することによって，ＡＤＰセキュリティ・プランナーは次のような方法を推進することができる。

(1) オンライン・ユーザーにサービスの中断を知らせる。

(2) 進行中のジョブを中止する。

(3) 磁気テープを巻きとり，取りはずす。ディスク・パックを動かし，カードリーダをクリアする。

(4) ＡＤＰハードウェアの出力を下げ，プラスチックのシートか又は防止カバーをかける。

(5) テープ，ディスク，カード・デック，ラン・ブック（運転指示書），ソース・ドキュメントなどを安全な場所へ移す。

(6) 空調装置の出力を下げる。

作業場からの退去が命じられたら，全要員は次の指示に従わなければならない。

(1) 作業書類などは机やファイル・キャビネットの中にしまう。

(2) 装置の稼動を止めて，照明をつけたまま室を出る。

(3) エリアから退去する時にドアを閉める。

コントロールに破綻をきたした場合の対策としては，手順をしっかりと決めてその責任を割当て，手近な場所で必要な資材や用具を供給することを忘れてはならない。全対策を行なえるだけの十分な時間的余裕がある場合もあるが，きわめて危険な状況にあっては生命の安全を守るためすみやかな退去が命じられる。従って，この場合の対策計画では緊急事態発生時に生命を危険にさらすことなく装置や記録を守るためにはどうすべきかを判断し，それに応じてＡＤＰ要員に指示を与える責任者を各ＡＤＰ部門から一人又はそれ以上選任しなければならない。

第２章では火災，洪水，嵐，その他の天災から建物を守るための方法について検討した。ＡＤＰセキュリティ・プランナーはＡＤＰ施設の特別な必要条件が満たされているかどうかを確認するためビルの管理者と共に保安対策計画を再検討する必要がある。その際にプランナーはビルの管理者にＡＤＰプランについて説明し，助言を求め，協力を得るよう努める。ＡＤＰのコントロールの破綻を補なうためビルの管理要員の助けを借りることもできよう。

緊急対策計画が完成し，認可されたら，次に示す火災の場合の例のように実行のためのわかりやすい説明を文書で通知する。

火災の場合の緊急対策

1. 火事の発生を知らせる（電話番号リスト）
2. 人命の危険があるかどうかみきわめる
3. 必要ならば施設から退去する
4. コントロールを失った場合の処理を開始する

4.8.3 バックアップ・オペレーション計画

ＡＤＰユーザーである機関の業務を無駄に遅らせないためにバックアップ・オペレーションがどうしても必要となるような状況がどのようなものかについては，リスクの分析を通して識別することができたはずである。次の段階は，経済的，技術的に安全で運用上も安全なバックアップ・オペレーション計画を研究することである。計画の細部は各ＡＤＰ施設の事情によって異なるだろうが，バックアップ・オペレーションが必要な項目の選択をするうえで一般的なガイダンスがあるにこしたことはないだろう。

施設の機能に部分的な損害がある場合にはバックアップ・オペレーションはその施設のオン・サイト施設で行なえるが，全面的なダメージや破壊があった場合にはオフ・サイトの１箇所あるいはそれ以上の場所でのバックアップが必要となる。従ってバックアップの手順は，それぞれの場合に応じて平常のオペレーションをそのままなぞるように反復するか，あるいは全く違ったものになる。バックアップについて検討しているＡＤＰ管理関係者は，オンサイトのＡＤＰシステムの完全な複製はバックアップとして役に立たないことや，１日当たりのバックアップ可能な時間が全ての指定された業務を実施させるためには少なすぎることなどに気付いて，早急にバックアップは不可能であると結論してしまうことがよくあるけれども，実は逆にバックアップに利用できる多くの事柄があるのである。以下にその例を挙げる。

緊急を要さない業務の延期　ＡＤＰセキュリティ・プランナーは，リスクの分析に基づいてＡＤＰの各業務を緊急を要する順に表を作り，その表を見ればＡＤＰ管理関係者は，災害が起ってから平常状態に復帰できるまでの時間を算定して，どの業務を後まわしできるかを迅速に判断することができるわけである。ここで後まわしにされる業務としては，プログラム開発，周期の長い処理（月単位，四半期単位，年単位），広範囲にわたるプランニングなどが考えられる。平常状態が回復したあとで適切な挽回時間を得られるように心掛けさえすれば，かなりの

数の業務を延期しても支障はないはずである。

代替手段の採用　コストの割り高なことと，サービスが質的に若干低下することに少々目をつぶれば他の方法を利用することも可能である。たとえば，被害をうけたＯＣＲユニットのかわりにパンチカード・インプットを利用することもできるだろう。また，プリンタの機能が止っている場合には，オフライン印刷用のバックアップ設備にプリント・テープを持ってゆけばよい。さらにオンライン処理のかわりにバッチ処理で間に合わせることもできよう。置き換えのきくようなハードウェアが利用できない場合には，通常使用しているパッケージと機能的に同一で技術的にはバックアップ用の外部のＡＤＰハードウェアでも処理できるような予備のソフトウェア・パッケージを利用すればよいのである。

業務の簡略化によるランタイムの節約　バックアップ・リソースの利用時間をできるだけ有効にひきのばすためには，複雑な処理を必要としない情報だけのレポートとか緊急を要さないファイルの更新など，業務の一部を省略したり後回しにしたりすればよい。また，場合によっては，ある１つの業務のサイクルタイムを２倍にすることも役に立つことがある。つまり毎日の業務を１日おきに実行するのである。

各業務について以上に述べたような可能性を検討することによって，ＡＤＰセキュリティ・プランナーはバックアップに必要な最少限の要件（ＡＤＰハードウェア，リソース，１日当たりのバックアップ可能時間などの規模）を決定することができるのである。その規格は，バックアップとして利用できそうなオフ・サイトの候補施設を決めるのに役立つだろう。バックアップ・オペレーションが可能な場所は以下のとおりである。自機関内部の別のＡＤＰ施設，他の政府機関のＡＤＰ施設，民間企業のサービス・ビュロー。ところで，政府機関どうしがこの問題で接触する場合には，ＡＤＰセキュリティ・プランナーは最寄りのＡＤＰシェアリング・エクスチェンジに対してバックアップに利用できる外部のファシリティの選定について諮問しなければならない。政府全体のＡＤＰシェアリング計画は，ＧＳＡの自動管理規格部（The Office of Automated Management

Regulations of GSA)〔15〕によって管理運営されている。

バックアップ・モードおよびバックアップ用の外部ファシリティを決めるために，ＡＤＰセキュリティ・プランナーは以下に示すようなコスト要因について検討する必要がある。

- ＡＤＰハードウェアの使用料金
- 要員，必要物資などの移動ならびに運搬
- 外部のファシリティ要員の人件費
- ユーザー（政府機関）と外部のＡＤＰ施設との間のインプットおよびアウトプットの運搬
- ＡＤＰ要員に対する残業手当ならびに臨時要員（おそらく，必要になると思われる）に対する手当

また，ＡＤＰセキュリティ・プランナーは通常のＡＤＰコストのうちにはバックアップ・オペレーション期間にかぎって節減できるものがあることについても留意しなければならない。すなわち，電力料金，電話料金，ハードウェアのレンタル料などである。

以上の要因についての検討，つまり重要な業務，特定のバックアップ・モード，利用できる外部のＡＤＰ施設などの識別に関して一応のメドがつけば，最適なバックアップ計画の概要が浮かび上ってくるはずである。一般的には，以下のような数種類のバックアップ計画を作成することが望まれる。①遅滞を引き起した要因がさらに大きく広がらないうちに，異常時には強制的にそれに切り換わるようなバックアップ・オペレーションの計画。すなわち，最優先のＡＤＰ業務だけを対象にした時間的に最少限のバックアップ・オペレーションの計画である。つまり軽微な損害に対するバックアップを中心にした計画。②ＡＤＰ施設が全面的に破壊された場合の復旧までの間のバックアップ・オペレーション計画，もしくは比較的損害が大きい場合を対象とした計画。③最も損害が小さい場合と最悪の場合との中間程度のバックアップ・オペレーション期間を対象とした計画。④ファシリティの主要部が機能低下をきたした場合の計画。

以上のように個々の計画はそれぞれ違った目標を持つが，作成する時には共通の基準から出発すればよい。全面的な破壊が最も重大な状況であるから，まずこれについての詳細は計画を作成することがたいていは一番効果的である。そしてこの計画を基準として状況や要素をスケールダウンしてゆけば，損害の程度に応じた計画がスムーズに作成できる。

各バックアップ計画は，次に挙げる5つの基本エリアをカバーしていなければならない。

(1) 作業規格

これは，バックアップ・オペレーション時における各業務の作業を平常のそれらから区別するための特定の方法について明記したものである。つまり，延期される業務，サイクルタイムやスケジュールの変更などについて記す。

(2) ユーザ・インストラクション

バックアップ・オペレーション時には，ユーザも平常とは違った形のインプットや別の場所へのインプットもしくは変更された手順を余儀なくされる。従って，混乱や無駄な動きを避けるためにユーザ・インストラクションが不可欠になってくる。

(3) 各ＡＤＰ業務に対する技術的注意事項

ＡＤＰ業務のバックアップ・オペレーションには，バックアップを供給する外部のＡＤＰ施設が所有している次のようなソフトウェアを利用しなければならない。つまり，現用のプログラムやデータファイル，インプット・データ，データ・コントロール，オペレーション・インストラクション（これはバックアップを行なう外部のＡＤＰ施設の通常のインストラクションとも違うはずである），その他プリプリント・フォーム，紙送り制御用テープなどである。これらについての注意事項は，各業務について明記されなければならない。またバックアップ・オペレーションに必要な資材はバックアップしてくれるファシリティの現用ベースでまかなわなければならないが，それを

確保するための手順も確立しておく必要がある。

(4) コンピュータ・システムの明細

1つないしはそれ以上の外部のコンピュータ・システムが，バックアップ・オペレーションに利用される。従って次のような情報が，各システムについて記録されていなければならない。すなわち，バックアップに使われる期間およびコストに関する管理情報，システムの位置，構成およびソフトウェアオペレーティングシステム，バックアップ・オペレーションの利用スケジュール，そのシステムで実行されるＡＤＰ業務の暫定的スケジュールなどである。

(5) 管理情報

バックアップ・オペレーション時には，特別の要員の確保と特別の処理手順，一時雇用もしくは要員の再配置，特別なメッセンジャの使用，平常時とは異なる部局の使用などを余儀なくされる。こうした変更などについての詳細は，当事者の了解を取り付けた上でガイダンスに従ってまとめておく必要がある。

またバックアップの必要から保持されるように決められたレコードは，重要レコード管理プログラムで保持されるように決められたものと同一である。従って，二重手間にならないように2つのプログラムを調整しておく必要がある。

さて，それぞれのバックアップ計画を完成する場合には，計画は全ドキュメンテーションを対象として含んでいなければならないが，その一つの目的は管理部門の賛同を得ることにある。そうした場合，それぞれの計画の間に二重手間，三重手間を生むことになるかもしれないが，各計画が何の見落としもないことを保証するためにそのような作業が要求されるのである。以上のような検討を経てできるバックアップ計画のフォーマットの一例を次に示す。

(I)　緊急事態の評定規準

ここでは第8.1節で述べたように，バックアップ・オペレーションが必要か否かをＡＤＰ管理部門が決定するうえで役立つ情報を含めて緊急事態の評定規準を明示する。

(II)　バックアップ・プランＡ ― 2日間のオペレーション

A　告示

これにはバックアップを行なうファンクション名，場所，電話番号，輸送機関案内を明示する。

1.　ＡＤＰ施設要員

2.　バックアップ用オフサイト設備の場所

3.　バックアップ設備の所属する政府機関名．交通機関，臨時バックアップ要員の在住地，連絡方法など

4.　バックアップ機関のユーザー代表者名

B　テクニカル・プラン

1.　実行すべき業務．外部の設備，オペレーティング・スケジュール，実行する必要のない業務などの概略説明

2.　業務Ａ

a　オペレーションに関する説明，特に平常時との相違について

b　ＡＤＰハードウェアの構成と1日の必要なラン・タイム

c　プログラム，データ・ファイル，プリプリント・フォームその他必要な特別の資材 ― ランブックなど，バックアップコピーの保管場所

d　バックアップ・オペレーション時のＡＤＰ要員の指名と必要な臨時要員

e　ユーザのための特別インストラクション

f　平常のオペレーションに復帰するための手順

3.　業務Ｂ

……

……

一般的にはルーズリーフ式のフォーマットを利用するのがよいだろう。あらゆる要員がすべての資料を必要とするわけではないのだから，１ページには１項目と限定して使うことが望ましい。また，ページ付けは付加資料が必要になったときに簡単に挟み込めるよう，単純な方法を採る方がよい。

4.8.4 復旧計画

バックアップ施設の使用は，極端に費用がかさむとともにサービス・パフォーマンスの低下を招くのが普通である。従って復旧に要する時間を最少限にとどめるようなサポーティング・ドキュメントの開発と保有ならびに復旧作業自体について検討してみることが必要なのである。さらに，ＡＤＰ要員は，バックアップオペレーションによって負担が増しているので，ＡＤＰ要員以外の人員の手で復旧を行なえれば，非常事態中のＡＤＰ要員の作業負担は軽減され，プロセスも効果的に行なえるようになることは間違いない。ところで全面的な破壊からの復旧には，以下に記すような作業を完全に終らせなければならない。

- ＡＤＰハードウェアとユーザおよびＡＤＰ要員のための空間として必要で，かつ稼動能力を備えたＡＤＰ施設を設置するのに必要な広さの床面積を確保すること。
- 稼動に必要な部分，すなわち上げ床，配電設備，空調設備，連絡設備，保安設備，防火設備その他設備の改修作業。
- ＡＤＰハードウェアの調達と設置
- 必要資材，事務用機器，事務机などの備品，テープ保管用ラック，デコレータなどの調達。
- 全ての必要なハードウェア，機械装置，資材が調達され，稼動の準備が整っていることの検査。検査の結果，不足がなければバックアップ設備から復旧されたＡＤＰファシリティへのオペレーションの転送。

必要な文書があらかじめＡＤＰ要員の手で準備されていれば，上記の最後の作

業を除いた全ての作業はＡＤＰ要員のほんの僅かな援助を受けるだけで政府機関の調達部門が遂行することができるはずである。必要なドキュメンテーションのプランニングと開発および迅速な復旧能力を保有するための技術についての考えを以下に提案してみよう。

第１段階は，復旧用地の選択規準の研究であるが，これには大きな労力は不要である。次に示すような現在使用中のＡＤＰ施設の特徴に従って，表を作ってみるとよい。

- 作業区分別の項目に従ってリストにまとめる。すなわち，コンピュータ室，テープ・ライブラリ，インプット／アウトプット・コントロールなどについて，最少限の面積と望ましい面積，必要な有効負荷，他の区域との望ましい近接の程度，該当区分に必要な人員数，必要な中心的ハードウェアおよび特殊電源，空調設備を明示する。
- 必要な一般用地の選定を行なう。すなわち，ＡＤＰ要員の住宅と適当な近さにユーザの用地を選定する。この場合の望ましい近接の程度（つまり必要な公共交通機関，連絡用交換局，その他の特別な要所など）および望ましい分離の程度（つまり火災あるいは洪水の危険を避ける上での緩衝地帯の規模）などを本書等に基づいて表にまとめる。
- 予想される調達物のリストを作成する。（つまりその費用，リース料金などについてである。）

用地の選定規準をもう一度確認して，問題がないようならそこを復旧するＡＤＰ施設用地に充当することの認可をうける。このとき，２，３の候補用地のリストおよび調達文書が，該当する政府機関の調達部またはその他の責任官庁で利用されるのである。こうしておけば災害に襲われてもすぐ次の段階で必要な用地を獲得でき，ＡＤＰ施設を受け入れられるように用地の整地にとりかかれるのである。図８－３は，このような復旧のための努力の簡単なPERTダイアグラムである。

第２段階は，ＡＤＰハードウェアの調達書類の草案を準備することである。こ

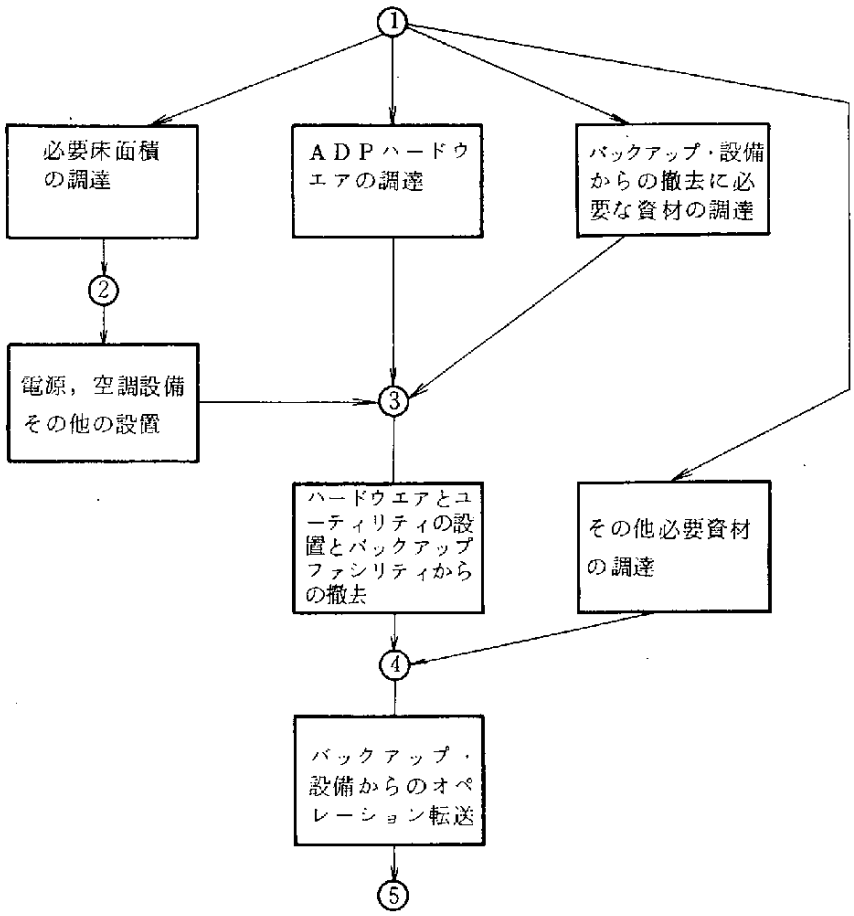


図８－３　ＡＤＰ設備復旧のPERTダイアグラム

ういう場合の傾向として，今まで使ってきた構成を単純にそのままなぞるように復元しようとするものだが，次のような２つの場合は例外である。最初の例外は，ハードウェアの搬入に手間取る場合である。ところで，ＡＤＰセキュリティ・プランナーは，調達部門，売り手側の代表，公共企業体などに諮問して図８－３に示した各措置を完了するまでに要する時間を算定できる。この算定の結果，ＡＤＰハードウェアの調達がネックになっているようなら，ＡＤＰシステム・プランナーは．（ハードウェアの調達に要すると予想される時間がきわめて長い場合には特に）替わりのシステム構成を検討することが望ましい。システム構成を新しくすればソフトウェアの手直しも避けられないことは目に見えているが，実際問

題としてはそのほうが望ましいのである。もう一つの例外は，システム構成の変化（グレードアップによるとか，新システムを導入するとかによって）がすでに予期される場合である。新しい構成の調達に要する時間が従来の構成の調達時間とほとんど変わらないならば，すぐに新しい構成に切り換えなければならなくなる従来の構成は捨てて最初から新しい構成を調達することの利点を採るべきであろう。

第3段階は，必要な資材や機材を調達するための文書の草案を作成することである。これには，以下の事柄が含まれる。

- **オフィス用の備品**　机，椅子，テーブル，ファイル・キャビネットなど。
- **事務用機械**　タイプライタ，筆記用具，加算器，卓上計算器，時計，複写器など。
- **特別なＡＤＰ資材**　磁気テープ，ディスクパック，フォームならびにパンチカードの予備，テープおよびディスクパック保管用ラック，カードデック保管用キャビネット，テープ運搬用台車，デコレータおよびバースト機器など。

なお新たに補給がつくまで重要な業務を継続するうえで必要なプリプリント・フォームは，ＡＤＰ施設内の災害によっても被害を受けそうもない場所に保管されなければならない。上に記したような資材の調達に時間を取って復旧がおくれるなどということはありえないが，もし不安ならＡＤＰセキュリティ・プランナーは予定の調達先をチェックしておけばよい。

最後の段階は，ＡＤＰ施設が復旧作業を遂行するうえで従わなければならない特別規則その他の必要な諸規則について，調達部その他の関係各官庁と協議することである。それらの規則と調達許可を得るために踏まねばならない事務手続きを表にまとめれば，最も手間取る手続きがどれかを識別できるだろうし，手続きに要する時間を短縮することもできよう。また同時に，復旧のための各タスクに対する関係各官庁の責任を，暫定的にではあるが明確にすることができる。

(1)　復旧作業のネックを識別し，もしそれが解決困難ならば善後策を検討する。

(2) 遂行しなければならない業務とそれに対して責任のある政府機関を識別する。

(3) 非常事態の間，ＡＤＰ要員は，各政府機関にその機関の責任である業務の進捗状況を通知する。ただしＡＤＰ要員は，この作業に余り労力を費すべきではなく，最少限の労力でこれを行なうようにする。

4.8.5 テスト用の偶発事故対策計画

非常事態というものはそうは起こらないものであるから，定期的な訓練とテストなしに要員や対策計画の熟練と妥当性を保証することは困難である。従って，定期訓練と定期テストの計画を立て，そのための予算を計上する必要がある。テストは，ハードウェアを除いて全ての配置をバックアップ設備と同じに設定して１つの特定の業務の反復を試す形で行なう。それによって必要なバックアップ・ファイルの有効性がテストできるわけである。経験が，バックアップの準備を確認するためのこのようなテストの有効性を証明している。細心の注意を注いでつくられた計画にもかかわらず，大きな落とし穴がひそんでいたということはよくあることなのである。また，１つもしくはそれ以上の実際の業務を実行することによって，指定されている外部の設備がバックアップ能力を維持していることを定期的に確認しておくべきである。多くのＡＤＰ施設が，全経費の一部をこうしたテストに振り当てている。

消火，ロス・コントロール，避難，爆撃その他の脅威に対する対応の手順についても同様のテストが行なわれ，各対策計画が充分に役立つことを保証すると同時にＡＤＰ要員に訓練の機会を提供している。それぞれのテストははっきりした目標を設定している必要がある。そのためにはテストをコントロールし，観察し，結果を評価するためにテスト用のシナリオを準備するチームを組んでおくとよい。このチームによる評価は，非常事態対策計画および非常訓練を改良するためのガイダンスとして役立つはずである。重要なことは，非常事態対策計画が実用的で

あり，ＡＤＰ施設の安全に実際に寄与するものであることを保証することなのである。

4.9 セキュリティ意識とコミュニケーション

4.9.0 まえがき

このハンドブックには，多くの安全規準について述べてあるが，この規準を有効なものにするＡＤＰ要員やユーザーの協力がなければ，安全性（セキュリティ）計画の効果は大幅に減少し，中には全く効を奏さない規準も出てくるにちがいない。**なぜセキュリティのための計画が必要なのか、その問題点は何か、そして特に要員やユーザーの役割は何か**について理解されれば，ＡＤＰ関係者のＡＤＰセキュリティ計画に対する関心はますます深まり，その貢献の度合も増すことになる。

ＡＤＰセキュリティ計画の重要性をできるだけ早く喚起するために，プランナーたちのアポイントメントを公表し，同時にプランナーたちに全要員のＡＤＰセキュリティに関する意見を知らせるよう訴えかけることによってセキュリティ計画に関する情報の交換を開始しなければならない。

物理的な安全性の規準としてのＡＤＰ施設内の一般的な環境は変化する。例えば，コンピュータ室へのアクセスは短縮されるだろうし，現在大部分の人々はエスコートなしにコンピュータ室に入ることは許されていない。この新しい安全性のための環境は要員にとってネガティブな心理的圧迫ともなりうるのである。つまり，要員は自分たちの誠実さが疑われていると感じ，自己規制をすることにもなるのである。ＡＤＰセキュリティ計画を発展させるためにはＡＤＰファシリティ以外の多くの組織の人々のサポートと協力が必要とされる。特に防火，監視，保険，要員対策，建築工学，設備の調達等の分野からの直接的な協力が必要とされる。情報の漏洩（間接的には金銭的な被害）に通ずる潜在的な要因ともなり，またそれがユーザーのファイルに関係のある場合は処理の遅れを招く要因ともなる欠陥を浮き彫りにするためにユーザーの代表はＡＤＰセキュリティ・プランナ

ーに必要な情報を提供するよう要求される。

セキュリティ計画の目標は，ＡＤＰ要員はもちろん，すべてのユーザーに知らされなければならない。特に，事実を歪曲したり回避することによって，中傷されたり，専門家としての名声を傷つけられ，挙句は仕事を失なったりすることのないように十分注意しなければならない。

4.9.1 シニア・マネジメント

シニア・マネジメント（特にＡＤＰ施設における指令系統については）と安全性の問題にとって必要なことは，効果的かつ能率的なセキュリティ計画を促進することである。シニア・マネジメントのこの問題に対する積極的な関わりありをぬきにしては，セキュリティ計画の充実は疑わしい。両者のかかわり合いは次の点に関して行なわれることが望ましい。

- ＡＤＰセキュリティ計画を設定する。
- すべてのＡＤＰセキュリティ政策のステートメントを再検討し確認する。
- リスクの分析と具体的なセキュリティ計画を再検討し認可する。
- 誰かのドキュメンテーションに責任を持つかを決定する。
- ＡＤＰ安全性プログラムにおいて必要とされるサポートを行なう機関（すなわち，機械装置の保全と消防）と協力する。
- データ・セキュリティのニーズを定義するよう各分野のユーザーに働きかける。
- ＡＤＰセキュリティ計画に必要な予算を組む。
- 得られた結果とミドル・マネジメントのパフォーマンスを評価する。
- 安全性のための規則を積極的に守る要員の例を示す。

4.9.2 セキュリティ計画の伝達

セキュリティ計画を伝達することの重要性から，近代的なコミュニケーション手段を利用した特別なＡＤＰセキュリティ・コミュニケーション・プランが促進されるようになってきているが，その際に次の点が考慮されなければならない。

4.9.2.1 ＡＤＰセキュリティ・プランの対象者

ＡＤＰ施設要員全員は定期的にＡＤＰセキュリティ計画を提示されるべきである。ＡＤＰ施設以外の組織に属する全メンバーにも，計画に関する情報が彼らによって反映されるように，その情報を伝えるべきである。

4.9.2.2 伝達の計画の内容

ＡＤＰ施設要員に提供される情報の中で，司法に基いて自分たちの財産を守り，要員自身によって遵守されるべき規則を定めることが何故ＡＤＰ要員の責任であるかという点が指摘されなければならない。ＡＤＰ要員がセキュリティ計画をより良く理解し，さらにできれば現在の安全性の規準の中に含まれる新たな脅威や欠陥を認識するためには，脅威の種類について説明されなければならない。

ＡＤＰ施設のオペレーションをサポートするユーザーや要員は，機関の運営機能を左右してしまうコンピュータの災害というインパクトに注意を払わなければならない。ＡＤＰ施設がダメージを受けるか破壊された場合，ＡＤＰの業務はランされないし，あるいはもっと悪い場合は重要なレコードが失なわれることもありうるということが指摘されるべきである。ＡＤＰセキュリティ・プランナーがリスクの分析を行なうためにユーザーにどのような情報を求めているかということをできるだけ明確にユーザーの代表者たちに理解させるためには，第1.2節で扱われたような出来事のインパクトについて説明されなければならない。

4.9.2.3 コミュニケーションの方法

セキュリティ計画を伝達する方法として，以下のものが考えられる。

ジョブの記述　ＡＤＰジョブの記述にはすべてＡＤＰの安全性に関する責任についての明確な説明が加えられなければならない。

要員のオリエンテーション　新規採用の従業員はすべて，現在の新従業員オリエンテーションとは別に，あるいはその一部として，ＡＤＰセキュリティ・オリエンテーションの講習を受けなければならない。従業員がＡＤＰセキュリティ・オリエンテーションを受けたことを証明し，その機関に対する従業員の責任とＡＤＰセキュリティの重要性を理解させるような方式を採用することも考慮されるべきである。同様に退職する時も，ＡＤＰ施設のセキュリティ・オペレーションに関する情報を外部に漏らさないという誓約書に署名するよう従業員に求めるべきである。

新規採用の従業員を多勢抱えているような，大規模なＡＤＰ施設の場合，一般的な用語で書かれたセキュリティ計画の小冊子を準備する。それには重要区域・アクセス・コントロール，非常手続き，施設内の通路システム，識別カード，ドアの鍵の控えリスト，その他一般的な話題に関する記述が含まれる。すでに従業員教育用の小冊子がある機関の場合は安全性に関する章をそれに追加する。ＡＤＰセキュリティ計画の変更に関する補充報告書を従業員全員か，または少なくとも要職にある役員たちに対して配布する。このような簡単な報告書は，テスト，ドリル，検査等の結果を伝達するのにも利用することができ，それによって欠陥の報告と同様，好ましい結果の報告も重要であるということがわかるのである。

掲示板　安全性に関する特別な掲示板をＡＤＰ施設内部に設置する。これによってＡＤＰ要員のための新しい安全性規定を急告することができる。

ポスター　ポスターは読むというよりむしろ一瞥する場合が多いので情報を詳細に伝える手段としては余り効果的とは言えない。しかしポスターは簡単なメッセージで，迅速かつ広範囲な情報の伝達を可能にする。ＡＤＰセキュリティに関

する多くのポスターは米国政府印刷局（U.S. Government Printing Office）文書管理室（Superintendent of Documents）から発行しているものがよい。

ニュース・メディア　新聞，雑誌関係の従業員の場合，ＡＤＰセキュリティに関する記事を定期的に掲載することができる。技術専門（誌）や一般（誌）に掲載された関係記事はＡＤＰ要員やユーザーに配送される。

実施方法に関する指示　このハンドブックの他の箇所で何度も検討した様に，ＡＤＰセキュリティ・プランを実施するためのインストラクションを推進していかなければならない。安全性を保証する各装置は明解に説明されたインストラクションを備えていなければならない。大抵の場合，このようなインストラクションは，第1.4節で述べたセキュリティ・ドキュメンテーションから引用される。例えば，ＡＤＰ緊急班のメンバーは（第2.1.4項参照），火災を発見した時に，彼らがとるべき行動に関するインストラクションを常に頭に入れておかなければならない。

トレーニング　フィルム，オーディオ・カセット，ディスカッション，レクチャー，インストラクション，セミナーなど様々な手段によって安全性のトレーニングが行なわれる。ＡＤＰの火災に関するフィルムはＧＳＡの国立オーディオビジュアル・センター（National Audiovisual Center）から入手できる。このフィルムは，"Fire Loss Management, Part Ⅱ : Computer Installations" である。このようなトレーニングの手段を利用して，ユーザーグループにＡＤＰセキュリティの重要性，ユーザーがＡＤＰセキュリティに対していかに影響力を持つか，なぜユーザーがＡＤＰセキュリティ・プランナーに自分たちの特別な要求を伝えることが大切なのかということについて啓蒙していかなければならない。レクチャーやディスカッションもきわめて効果的なトレーニングの手段となりうる。

4.9.3 まとめ

ＡＤＰプランナーにとってＡＤＰセキュリティ・コミュニケーション・プランの効率を評価することは容易なことではないが，コストは他のＡＤＰセキュリティ規準に比べてそれほどかからない。コミュニケーション・プランには最低限，新規採用の従業員向けオリエンテーションとＡＤＰ要員とユーザー・グループのためのトレーニング・プログラムは入れるべきである。

ＡＤＰセキュリティ・プログラムを促進していく場合，成功のポイントは，このプログラムに快く応じてくれる忠実な，専門的な従業員にあることを忘れてはならない。このプランナーとＡＤＰ要員，そしてユーザーとの協力事業は，ＡＤＰセキュリティ計画が明確に伝達されてはじめて成功するのである。

4.10 物理的安全性の内部監査

4.10.0 まえがき

これまでの章ではＡＤＰの物理的安全性（セキュリティ）計画を促進するための方法について述べてきた。この計画を完全にするための最後の段階，再検討または監査（audit）のプロセスである。ＮＢＳ／ＡＣＭ Workshop on Controlled Accessibility〔47〕の報告書は**監査**を次のように定義している。

「情報システムとその利用に関する独立した客観的な検査（組み込まれた構成機器も含む）

a　コントロールが適切であるか，リスクの程度，危険度の高い箇所，規準や手順に従っているかどうかを検査する。

b　信頼性，能率性，安全性がしっかり守られているか，という点についてシステムの管理が適切で効果的かどうかを決める。」

「独立」と「客観的」という言葉がこの定義の鍵である。これらの言葉には，監査が普通表面的な運営の監視と，報告システムを補い，しかもその種の管理の一部でもなければそれに属するものでもないことを意味するのである。

この監査による効果は一体どのような点にあるのだろうか？まず第一に，これによってＡＤＰ施設のためのセキュリティ管理を評価することができる。第二にセキュリティ計画を改良し更新するチャンスをつかむことができる。第三に従業員や管理体制を常に緊張させる。最後に，成功すれば，セキュリティ対策が適切でなかった不完全な部分を知ることができる。システムの完成に伴って，リスクも替り，新たな脅威が生れるだろう。

内部監査の頻度を決める場合に考えなければならない重要な要素は，外部監査の回数，ＡＤＰシステム変換の割合，コントロールの量とそれが十分かどうかと

いう点，装置が直面する脅威，前回の監査結果などである。この監査は，ＡＤＰ施設全体の支配権を持つ最も高度な管理活動であると言ってさしつかえないだろう。

4.10.1 監査の準備

監査班を選ぶ時の主な原則の一つは，その班のメンバーはＡＤＰオペレーションに責任のない人間でなければならないという点である。なぜなら，監査はＡＤＰマネージャの管轄外の部門又は機関の指揮のもとに行なわれなければならないからである。メンバーはデータ処理の知識とできれば基本的な監査の規則をある程度知っていた方がよい。プログラミングやＡＤＰオペレーションの経験はあることが望ましいが，なくてもかまわない。ＡＤＰサービスの熟練したユーザーならこれに必要な資格を備えているだろう。監査班の役割は，セキュリティの管理を促進することではなく，現在の管理と手順を評価することにある。管理の方法を実行することに対する責任は監査班にあるのではなく，ＡＤＰの運営にある。

監査班の各メンバーの性格はきわめて重要である。判断力，客観性，知能，証明能力が監査の成功を大きく左右する。この班のリーダーには各メンバーの成果をまとめ，内容のしっかりした報告書を作成し，問題点を指摘できるだけの能力が要求される。リーダーに技術的な専門知識がない場合は，技術的な判断を下すことのできるＡＤＰの専門知識を持った人がリーダーを補助する。

班の規模は設備の大きさと監査の範囲によって決る。大規模な設備の場合，次の分野の専門家を監査班に加えるべきである。

- **内部監査**

  監査を行なうための知識と規則は，内部監査の専門家が示すことができる。好奇心の強さ，証明能力，細部への関心などは専門の監査役の典型的な特質である。たとえ監査の専門家がデータ処理テクノロジーに通じていないのが

普通であっても，ある程度のデータ処理の知識のある監査役をみつけるのはそれほど難しいことではない。

○ **安全性**

監査班は，安全性の専門知識をある程度持っていなければならない。セキュリティの責任者は監査班の追加メンバーとして最適である。その役割については，すでに第5.1節で十分に検討した。

○ **データ処理**

データ処理分野の技術的専門知識も必要である。プログラミングの知識もオペレーションの経験も役立つ。恐らくデータ処理内部のセキュリティの責任者はこのような知識と経験をもっているはずである。もしそうなら，監査班のメンバーとしてかけがえのない候補者ということができる。評価されるべきＡＤＰ施設からその関係者を選んで監査の補助を頼んでも必ずしも監査の過程における客観性を著しく左右することにはならない。

○ **ユーザー**

効果的な監査から最も大きな利益を得るのは，ＡＤＰ施設への依存度から言ってもユーザーであるはずなのに，ユーザーのＡＤＰ管理やセキュリティ規準に対する関心はあまりにも稀薄である。ＡＤＰセキュリティ・プログラムに参加して情報を提供したユーザーにとって，その情報が調整され，そのまま発表され，あるいは抹消されたりしたことが，監査班への参加を促す要因となりうるのである。

○ **建物管理と建築工学**

監査されるべき物理的セキュリティの管理の大部分（火災予防，火災報知，空調設備，電力アクセス・コントロール，災害防止）は，建築管理と建築工学に関係がある。

○ **外部の専門家**

外部のコンサルタントによって提供される独自の経験に裏づけられた観点は非常に役立つものがある。

監査班の構成は柔軟性に富んだものになる。大切な条件の一つは，この班は客観的な人々によって構成されなければならないということである。監査されるＡＤＰ施設が一つだけである場合，班のメンバーは一時的にその監査班に加わり監査が終ると平常の仕事に戻る。ある機関の管轄下に多くのＡＤＰ施設がある場合，全装置をくり返し再検討するために恒久的な監査班を常設することが望ましい。いづれにしても，常に新鮮な観点と新しく多様な監査技術を採り入れるために定期的に班の構成を換えるべきである。

4.10.2　監査計画

安全性の内部監査を適切に行なうためには総合的な監査計画を促進しなければならない。それは実際の作業を中心としており，行なわれるべき作業がリストアップされているものがよい。それは特殊な装置に対して設計されていなければならない。このことは，この計画促進においてはごく少量の仕事しか要求されないことを示している。

第一段階は，ＡＤＰ施設のためのセキュリティ対策を検討することである。この対策は機関，部門の全体または一単位のＡＤＰ施設に対して適用される。どの場合でも，それは再検討され，その後の調査のために役立つような適切なセキュリティを目的としたものでなければならない。次の段階は，特殊な装置に顕著な弱点を識別するリスクの分析計画を再検討することである。第三は，特別な安全性のオペレーティング手順が何であるかを決めるためにＡＤＰ施設のセキュリティ・マニュアル，オペレーション・マニュアル，などこの種の文書を再検討することである。最後に，特別なセキュリティや内部管理に対して責任を持つポジションを確認するためにＡＤＰ施設の組織図とジョブの記述を検討する。これらのものは，監査計画を推進するための基礎となるだろう。監査計画を作成する際に考慮されねばならない一般的な問題は次のように沢山ある。

○　セキュリティに関する重要なポイントは何か。ＡＤＰ施設は分類されたデ

ータ若くはその他の詳細なデータを処理するか。その処理はその他のデータ・センターの処理と重複し，それによって一種のバックアップをしているかあるいは不慮の故障の場合の替りを務めるのだろうか。あるいはそれは独自の業務のための単独の処理なのか。重要な業務は何か？監査に重点を置いてみた場合の重要な業務とは何か？

○　平常のオペレーションで一番テストされていないセキュリティ対策はどれか？例えば，コンピュータが電力切り換えのために毎日4時15分にフェイルするとしたら，即時のバックアップや復旧のための必要条件は明確に系統立てられ，そのための安全対策は十分にテストされているだろう。しかし，災害の場合の復旧計画は，それを実行するための特別な対策が講じられない限りテストされないだろう。この点が肝心である。この種のセキュリティ対策は不十分なまま実行されることが多い。

○　どのような監査が，最少限の努力で最大限の効果を上げることができるか。緊急事態の火災探知器のテストは警報器の反応だけでなく，消防隊の反応や撤去計画の効果についても行なわれる。同様に，コンピュータ・センターの侵入者を捕える措置の場合も，アクセス・コントロールだけでなく，従業員への警報や特別エリアの安全性についてもテストされうる。要員に対するインタビューの際の質問は総合的な答えを引き出すように考えられていなくてはならない。例えば，「認定されていないジョブが入ってきた場合，どうしますか？」という質問は，「ジョブの認定管理は効果的に行なわれていますか？」という質問よりも多くの情報を引き出すことができる。後の質問に対する答として最も考えられるのは「はい」という単純そのものの答えである。

○　どのようなセキュリティが優先的に採られるべきか。検査の要求や損失事件，中断や妨害などは特殊な方法が必要なので，特別なセキュリティ対策のテストの方が重要ではあるがその他の非今日的な同程度の問題よりも重点が置かれる。しかし，計画の中のある一面だけを強調することは避けねばならない。最近のセキュリティの不備がもたらした厳重すぎる警備は，コンピ

ュータのセキュリティについての全局面を調査するための合理的なアプローチによって調整されるべきである。

監査計画を推進する過程のもう一つの段階は前回までの監査報告書を再検討することである。これによって，修正された欠陥や注意すべき箇所を知ることができるので，これからの監査で特に注意すべき事柄を確認することができるのである。

特に初めての監査の場合は，入手可能ならば他の機関において開発されたプログラムを参考にしたり，またはSAFE（Security Audit and Field Evaluation〔18〕やAMRのコンピュータおよびソフトウェア・セキュリティへのガイド〔3〕のような問題を扱ったコンサルト出版物を見るのもよいだろう。後者のAMRのガイドから抜すいした監査計画の見本の一部を下に示すことにする。

物　理　的　施　設

A　火　災

① コンピュータを耐火性のある，もしくは不燃性の建物に設置する。

② コンピュータ室は不燃性の仕切り，壁床，ドアによって隣りのエリアから区切り，危険物を近づけない。

③ 床や吊り天井，サーポート・ハードウェアは不燃性であること。

④ 床の被い，備品，窓の被いは不燃性であること。

⑤ 紙やその他の供給物はコンピュータ・エリアの外に備えること。

⑥ 発火を促すようなあるいはその他危険を伴なう行動は，コンピュータ室やその隣接エリアでは避けるよう注意する。

⑦ コンピュータ・エリア（インプット／アウトプット室，コンピュータ室，テープ・ライブラリ）での喫煙を禁止する。

⑧ 火災の生じた場合の消火訓練と個人の責任の分担を再検討する。

⑨ 自動消火システムが適切かどうかを調べ，それを準備する。

⑩ 携帯用消火器を，火災の発生場所を明確に示す装置のあるエリアの周辺に設置する。

⑪ 緊急時の電力切断コントロールは簡単にアクセスできるように出口の所に設置すること。

⑫ 緊急時の電力切断の効果を調べる。

⑬ 切断のチェック・リストを利用するかどうかを決める。

⑭ 煙探知器の設置場所を決める。

⑮ 煙探知器を活用する場合の効果を調べる。この探知器を一定の規準でテストする。

⑯ 火災訓練スケジュールとその手順を再検討する。

⑰ 消火用水を十分に給水することができるようにする。

⑱ 火災警報システムを再検討する。どこで警報器が鳴っているかを確認できるようにする。

⑲ どのように火災警報を稼動させるかを決める。

⑳ 米国保険協会（American Insurance Association）の標準消防隊評価スケジュール（Standard Fire Defense Rating Schedule）によって，地方の消防隊に対する評価を定め，火災防止施策に関するその評価の効果を調べる。

㉑ コンピュータのメンテナンスに使われる発火しやすい物質の補充を点検する。それは規定の容器内にごく少量入っている可能性がある。

㉒ 非常の場合の救助員が直ちに装置にアクセスするための手順を再検討する。

㉓ 床パネルのリフターが役に立つかどうかを調べる。

B 水 害

① コンピュータの位置を調べる。コンピュータが低い場所にあるのかどうか。

② 頭上のスチームや水道管を点検する。これらはスプリンクラ・システム専用のものにするべきである。

③ コンピュータ・エリアとその隣接エリアや床上に十分な排水システムがあ

るかどうかを調べる。

④ 天井に水が漏れる穴が傷がないかどうか調べる。

⑤ 高くなった床の下にある電源の接続箱を点検する。これには水害を防ぐため板をかぶせる。

⑥ 外側の窓とドアが防水になっているかどうか調べる。

⑦ たまった雨水や屋上のクーリング・タワーのしづくを防ぐにはどのような方法が役に立つかを調べる。

C 空 調

① コンピュータ・エリア用の空調システムをテストする。

② 線渠やフィルタが不燃性であるかどうか調べる。仕切り壁で火のいきおいを弱める装置が備え付けられているかを確かめる。

③ コンプレッサの場所を確認する。これはコンピュータ室から離れた所に置く。

④ クーリング・タワーのための保全が適切であるかどうか調べる。

⑤ 空調装置をバックアップする方法について討論する。

⑥ 空気の取り入れ口を確かめる。取り入れ口はおおいをかけ，排気ガスやゴミなどが入らないよう道路の高さより上にとりつける。

⑦ 煙を排出する方法をテストする。

D 電 気

① 回線の電圧モニターを調べる。ボルト・メーターの記録を利用しているかどうか調べる。

② 中断することのない非常用電源の検査が行なわれているかどうか確かめる。

③ 非常時の照明システムと電源を点検し，その取扱い方を確かめる。

④ 電気装置のメンテナンスが十分に行なわれているかどうか再検討する。

E 天 災

① 天災に対する防衛手段が適切であるかどうか再検討する。

② 建物や装置が雷に対して十分にアースされているかどうかを確かめる。

F アクセス・コントロール

① 破壊への危険が計算されているかどうか確かめる。

② これまでに起った装置の破壊について再検討する。

③ 建物の入口にどのようなアクセス・コントロールを取り付けるかを決める。（平日用と週末用）

④ コンピュータ・エリアのための２４時間制の警備員について検討する。

⑤ 従業員を識別するための写真バッジ・システムについて検討する。

⑥ データ・センターの中心エリアへの出入りを誰に許可するかを決める。

⑦ コンピュータ・エリアでバッジ着用の必要性を検討し，テストする。

⑧ キー，暗号錠，バッジ・リーダー，その他アクセス・コントロールのための安全装置の利用を再検討する。

⑨ 外来者の識別の誤りを確認するための措置をテストする。

⑩ 外来者を管理する方法やコンピュータ・エリアの巡回コースを再検討する。その方法をテストする。

⑪ セキュリティ・ガードや従業員のいないオフ・シフト時間中に誰かがアクセスするのを防ぐための方法を決める。そのシステムをテストする。

⑫ コンピュータ室の位置の表示に関する機関の方針について検討する。

⑬ アクセス・コントロールが電気によって行なわれるシステムの場合，それをいつでも使えるように充電したバッテリーによってオペレートできるのかあるいは手に入れやすいキーによって稼動を止めることができるのかどうかを確かめる。

G 施設内の衛生管理

① コンピュータ・エリアでゴミがたまるのを防ぐ方法を考える。

② 掃除機をかける時と場所のスケジュールを再検討する。

③ 床をふく責任者を決める。そのスケジュールを再検討する。

④ 高くなっている床の下を掃除する手順を再検討する。その部分を検査する。

⑤ ゴミ入れをどこに置くかを決める。 ゴミやほこりによる損傷を少なくするため，この作業はコンピュータ・エリアの外で行なわれなければならない。

⑥ 敷物や床のワックスを調べる。これらは静電気を起さないものでなければならない。

⑦ コンピュータ室での飲食に関する方針を討議する。

⑧ 熱に弱い容器を使用するかどうか決める。正しく使われているかどうかを監視する。

⑨ コンピュータ室での喫煙について討議する。

⑩ メンテナンス・エリアが清潔に整頓されているかどうかを監視する。

H その他のファシリティに関する注意事項

① 保安要員やオペレータに市民の妨害に対してどう対処すればよいかについて知らせる。

② 電話による爆破の脅しにどう対処すべきかを要員に知らせる。

③ 州法の執行機関に関連したプログラムを再検討し評価する。

組 織 と 要 員

A 組 織

① 組織図と職制を調べる。

② 重要な機能は区別する。

③ 各部門によって管理されるコンピュータの安全性（セキュリティ）について討議する。

④ コンピュータの安全性を保証する活動の管理責任者を決める。

⑤ コンピュータの安全性のための対策を再検討する。

⑥ 次の各分野におけるコンピュータ・センターとインハウス・サービス部門，地方機関，外部コンサルタントとの関係を調べる。

a．プラント・エンジニアリングとその設備，電気調節装置と用地の確保

b．工場又は建物の保全（火災予防，警備員，緊急のサービス，政府が決めた条件）

c．重要記録の管理

d．法律担当のスタッフ

e．要員

f．監査役（システム設計，対策と手順）

B　要　員

① 新規採用の従業員をチェックするための対策を講ずる。

② 従業員を定期的に再チェックする対策を講ずる。

③ 従業員の交換トレーニングを再検討する。すべてのジョブが適切にバックアップされているかどうかを調べる。

④ 従業員の不満の原因となる問題について話し合う。どのようにやり方が指示され，どのような手順に従うべきかを決定する。

⑤ 装置に対して何らかの脅威を加えた従業員の免責や解雇に関する方針を再検討し，評価する。

⑥ 各部門は，コンピュータの安全性についての要員の教育プログラムを継続的に行なうようにする。

バックアップと復旧

A　データとプログラムのバックアップ

① 重要な複写ファイルをどこにストアするか決める。

② 重要ファイルを識別する方法とそれの保存期間を再検討する。

③ 重要ファイルの最近の目録を調べる。

④ プログラムを熱に強い容器にストアする。

⑤ 模擬実験を行なうことによって，ファイル・バックアップ・システムの安定性と的確度を試めす。各部門は周期的に模擬実験を行なうべきかどうかを決める。

⑥ ファイルのバックアップをどのように行なうかを決める。

⑦　バックアップおよび復旧方法の報告書を再検討する。

B　バックアップ設備

①　バックアップ・コンピュータのプランを調べる。装置の位置，契約上の協定，定期的なテスト，機能的な関係などを決める。

②　バックアップ装置の稼働計画を評価する。この計画は再検討され，定期的にテストされなければならない。

③　スペア部分は地方でも入手できるようにする。

④　バックアップ設備にストアされているデータ・ファイルやその他の物質の物理的安全性を評価する。

⑤　バックアップ設備で非常時のオペレーションが行なわれている間の保全設備を評価する。

C　不慮の事故対策

①　主な事柄をすべて規定した対策計画を作成，評価する。

②　この対策計画に書かれた各機能部門の責任者を決める。

③　この計画の実施のための詳細な通知方法を再検討し，評価する。

④　故障の程度を決める規準を再検討する。

⑤　各アプリケーションのソース・ドキュメントやデータ・ファイルを保有することの責任を決める。

⑥　ＥＤＰ要員のための不慮の事故のトレーニング・プログラムを再検討する。

磁気テープと磁気ディスク

A　責　任

①　利用回数や利用規定に応じたテープやディスクに対する責任の程度を決める。

②　貯蔵室やコンピュータ・センターからテープやディスクを移す際の規定手続きを決める。

③　個人のテープやディスクの場所をどのように説明するかを決める。

B　衛生管理と保管

①　磁気テープやディスクのファイリング・システムを再検討し，評価する。

②　テープやディスクのクリーニングのスケジュールを再検討する。

③　テープが利用される時以外は容器に保管されることを注意する。

④　テープの容器をどれくらいの割合で清掃したらよいかを決める。

⑤　テープヘッドをどれくらいの割合で清掃すべきか決める。

⑥　ドロップアウトのためのテープの定期的な模擬テストの方法を再検討する。

⑦　古くなったリーダ（先導テープ）は定期的にとり除かれ，廃棄処分にする。

⑧　保管場所はテープやディスク・パックを十分に保全できるように設計する。

⑨　マグネット・ディテクタを利用すべきかどうか決める。

⑩　輸送中のテープやディスクのために適切な安全対策を講じるかどうかを決める。

⑪　テープやディスクのリハビリテーションやバックアップ・メディアを含むプログラムの再利用について検討する。

監査計画には，記録の検査や非常時の反応テストと同様，視察も含まれることになるだろう。初めての監査の場合は関係者とのインタビューも行なわれる。安全性関係の組織図は，インタビューの対象としてふさわしい人物を選び出すのに役立つ。図 10－1 は 2 つの安全性の分野を簡単に説明したものである。このようなインタビューをする前に大ざっぱな監査計画を立てておくべきである。このインタビューは最終的なプランニングに大いに役立つであろう。

	要求	促進	再調整	認可	履行	メンテナンス
○物理的アクセス・コントロール						
ＡＤＰセキュリティ・プランナー	x	x				
ＡＤＰサービスのユーザー			x			
ＡＤＰマネジメント			x	x		
オペレーション		x	x		x	
アプリケーション・プログラミング			x			
建　築　管　理		x	x	x	x	x
○バックアップと復旧						
ＡＤＰセキュリティ・プランナー	x	x				
ユ　ー　ザ　ー	x		x		x	x
ＡＤＰマネジメント			x	x		
オペレーション			x		x	x
アプリケーション・プログラミング					x	x

図 10－1　安全性の責任

4.10.3　監査のやり方

前もって計画された監査も不意に行なわれる監査も両方とも効果がある。前もって予定された監査は特別な装置の条件に合った方針のもとに，毎年行なわれる。外部の機関によって行なわれる大部分の監査や内部監査（ガイドラインに従って）あるいは前回の監査報告の中にある注意すべき特別な事項を再検討するために行なわれる部分的な監査などがそれにあたる。この種の監査の特徴は，データセンターにその準備のために大騒ぎをさせるような，前もって知らされている監査で

あるという点にある。前もって知らされることによって，監査にそなえて今までルーズにされていた部分が整えられるという長所もあるが，反面本来監査によって得られるはずの効果を限定することにもなるのである。一方，不意打ちの監査は平常通りの安全性と管理の要素をテストするように考えられている。これは同一機関又は外部の監査班によって行なわれ，火災の場合の反応，アクセス・コントロール，要員のゆだんなど不意を突くことによって最も効果的にテストすることができるような要素がその対象となる。

監査の実施の第一歩として，不意の試験が必要な時は別として，ＡＤＰ要員へのインタビューが行なわれるのが普通である。最初は大低，データ処理マネジャーや，関係要員とのインタビューである。質問は指導するためにするのではなく調査のために行なわれることを念頭におく。回答者に対する最も効果的なアプローチの仕方は，できるだけ自由に話をすることである。回答者を自分の答えを証明するような立場にたたせるような質問をするとよい。例えば，「アクセス・コントロールの最大の問題は何だと思いますか？」と聞くべきであって，「あなたのところではバッジを着けますか？」と尋ねるべきではない。どのようにしたら不法侵入やサボタージュができると思うかという質問もするべきである。同じ質問をくり返しすることをちゅう躇してはならない。いかに多種多様な答えがかえってくるかをみるのも興味のあることである。インタビュアーの態度は重要であって，回答者との関係をオープンにするよう心がけ，プライベートな情報をほのめかすことは避けて，第三者や他の事柄への関係をふせたりあるいはほかの方法でそのことを煙にまいてしまうよう工夫しなければならない。言うまでもなく人間関係のテクニックを上手に利用してこそインタビューを成功させることができるのである。相手に敵対するような挑戦的なインタビュからは何も得られない。インタビュアーの態度はてきぱきとして好奇心を強く持ち，しかも落着きと誠実さ，率直さを持ちあわせていなければならない。漠然とした用心深い返答は詳しく追求していくべきである。

メモをとるかどうかは好きずきである。返答を聞きながら適切にメモをとる人

もいれば，返答を聞きとることに全神経を傾けなければならない人もいる。メモをとることが問題である場合は２人で組んでインタビューをすることもできる。あるいは，前もって相手の承諾を得て，ポータブル・テープ・レコーダを使ってもよい。いずれも不可能な場合は，インタビュアーは相手の言うことに全神経を集中させて聞きとり，インタビューのメモを直後とり，印象を書きそえておく。

評価テストは前もって知らされている場合もあれば，不意に行なわれることもある。ほとんどのセキュリティの監査には，火災，撤去，災害の復旧作業などの非常時のテストが含まれている。アクセス・コントロールも抜きうち検査をするべきである。このテストは周到に準備するか，あるいは，監査員たちに対する心の準備ができてしまってからよりは，監査の初期の段階で行なわれた方がよいだろう。プログラム・コントロールやデータ承認が適切であるかを，このようなコントロールを回避するために企てられたジョブを行なうことによってテストすることもできる。その時に生のデータをこわさないよう気をつけなければならない。しかし，ＡＤＰ管理者が誤り検出とコレクション・コントロールが実際によく稼働していると確信しているなら，これらのコントロールをテストするために故意にエラーを入れることに反対しないはずである。

監査班は，一日の活動の終りにその日の行動を反省し，ノートを比べるために全員集合する。欠陥のあるエリアに焦点があてられ，さらに関係のある特殊なエリアを調査するための追加テストやインタビューの予定が組まれる。監査書類のコピーは，わかりやすいように，再調査しやすいように，比較しやすいように分類され，番号付けされ，日時が書込まれて整理される。

監査が終ると，印象がまだ鮮明なうちに報告書の作成を始める。原則として監査報告書には次の項目が含まれていなくてはならない。①まとめ，②監査に関する記述 ― 日時，場所，範囲，対象など，③観察されたことに関する詳細な報告，④観察によって得られた結論，⑤修正された作業に対する勧告。得られた協力についても書き添えられ，好ましい結果についても，欠陥についての記述と同じ位重点をおいて報告されなければならない。図表や結果のマトリックス，総計的なテ

ストとその結果なども大いに役立つ。プランニングの段階では，最後の報告書がＡＤＰ施設や機関の運営にいかに貢献したかということに関する一致した意見について触れるべきである。

4.10.4　フォロー・アップ

監査は，その結果が今後の改良と修正，マネジメントの基礎となるのでなければ，何の意味もない。これらの作業を行なう責任は，ＡＤＰ設備責任者にあるのが普通である。修正のための作業の責任は順番に割当てられることになっている。最良のアプローチは，要求，問題の定義，責任，行なわれるべきあるいは要求される作業，そして，それに続く今後の作業の概要を書いたコントロール・シートの主な欠陥をまとめることである。さらに，その作業を終了すべき日時とそれを続行すべきかどうかの指示を行なう。修正作業の中には，追加資金を必要とするものもでてくるだろうが，それを書きとめておく。

修正作業，続行，欠陥の処置などの作業は機関のマネジメントの報告書作成のサイクルに合せて行なわれる。季刊の報告書は，管理項目がまだ決っていない監査に対して推せんできる資料である。

最後の段階は，ＡＤＰ設備責任者と監査班による監査そのものに対する率直な評価である。将来の監査方法とそのプロセスをより良くするためにグループ・ディスカッションを開催する。監査プランは必要ならば修正され，また班の構成も必要に応じて変えられる。監査は，ＡＤＰファシリティの安全性とその管理の改良を促進する一手段として効果を常に発揮していることを忘れてはならない。

付　録

プログラミング・プロセデュア・マニアル（プログラム手引書）の目次例

406. 責任のインターフェイス：アナリスト

406－1　連絡と照会

406－2　ジョブの依頼

407. 責任のインターフェイス：内部サービス

407－1　キーパンチ

408. トレーニングの責任

500　ドキュメンテーション・プロセデュア

501. プログラム配給コントロール（PIC Program Issuance Control）機能

502. 問題の報告

502－1　プログラムの問題

502－2　システムの問題

503. プロセデュア／システム・マニュアル・フォームの完成

503－0　ジョブ・ストリーム・フロー

503－1　ジョブ・ストリーム・ドキュメンテーション

503－2　ジョブ・ドキュメンテーション

503－3　メッセージとコード

503－4　パンチ・アウトプット・カード

503－5　テープ又はディスク・データ・セット

503－6　フォーム／リポート

503－7　キャリッジ・テープ（紙送りテープ）

503－8　レコード・フォーマット

504. モジュール

504－1　モジュール・ネーミング規定

504－2　モジュール・フォルダ

505. プログラム

505－1　プログラム・ネーミング規定

505−2　プログラム・フォルダ

506. 見本のフォーム

600　ジョブ・コントロール・ランゲージ（ＪＣＬ）プロセデュア

601. 序

602. ＪＣＬコーディング・レスポンシビリティ

603. ジョブ・カード

604. 実行カード

605. データ分類カード

606. ジョブ区切り文字カード

606−1　カラー・コード

606−2　デックの識別

606−3　カラム１，２の識別

607　ＪＣＬ規定

608. オペレーティング・システム

609. 主要サブシステム

610. システム・インプットの考察

611. システム・アウトプットの考察

612. ジョブ・アカウンティング

612−1　ジョブ・カード・アカウンティング・パラメータ

612−2　アカウント・ナンバの利用

612−3　ユーザ・ビリングの実際

613. デフォルト・オプション

700. ソフトウェア・プロセデュア

701. プログラミング言語の標準

701−1　システム・ジェネレーションの選択

701−2　プログラミングの制約

702. アセンブラ言語の標準

702−1　システム・ジェネレーションの選択の制約

702−2　プログラミングの制約

703.　標準的なユーティリティ

800.　オペレーション・プロセデュア

801.　受入れ手順

802.　非常時の作業（火災，電力の誤りなど）

803.　リモート・ジョブ・プロセシング

804　テレプロセシング・プロセデュア

805.　オペレーションの制約

806.　スケジューリング

806−1　優先順位

806−2　ジョブ・クラス

900.　データ・マネジメント・プロセデュア

901.　データ・セット識別

902.　データ・セットの保持

903.　インデックス構成

904.　ボリュームのレベリング

904−1　直接アクセス

904−2　テープ

905.　パーティション・データ・セット

906.　マルチ・ボリューム・データ・セットの利用

907.　ライブラリのメンテナンス

907−1　新ファイル・プロセシング

907−2　ユニバーサル・データ・セット・コピープロセデュア

907−3　機密データの取扱い

907−4　非常時のプロセデュア

907−5　重要記録の保安

907-6　テープ・アクセス・プロセデュア

1000　コントロール・プロセデュア

1001. データ・コントロール

1001-1　データ・エレメント・マトリックス

1001-2　ファイル／プログラム・マトリックス

1001-3　モジュール／プログラム・マトリックス

1002. 品質管理

1002-1　ドキュメンテーションの再検討

1003. 安全性管理

1003-1　装置の保全

1003-2　データの保全

1003-3　コンピュータ室へのアクセス

1004. テスト

1004-1　テストの段階についての記述

1004-2　デュアル・ラン・スタンダード

1160. コードおよびシリアル・ナンバー

9800. クロス・レファレンスの発表

9900. 用　語　集

付　録

文　献　索　引

[1] Baker, H. R., P. B. Leech, and C. R. Singleterry, Surface Chemical Methods of Displacing Water and/or Oils and Salvaging Flood Equipment, U.S. Naval Research Laboratory, Washington, D.C., NRL Report 5680, September 1961, 14p.

[2] Barker, B. C., Jr., Joint-Service Interior Intrusion Detection System, in Proceedings of the 1973 Carnahan Conference on Electronic Crime Countermeasures, University of Kentucky, Lexington, College of Engineering, April 1973, p. 20-27, 2 refs.

[3] Brown, W. F., M. B. Greenlee, and R. V. Jacobson, AMR's Guide to Computer and Software Security (AMR International, Inc., New York, 1971), 208p.

[4] Brown, William F. and David H. Hawkins, Remote access computing: the executive's responsibility, Journal of Systems Management, Volume 23 (May 1972), p. 12-16.

[5] Brown, William F. and David H. Hawkins, Remote access computing: the executive's responsibility, Journal of Systems Management, Volume 23 (June 1972), p. 32-35.

[6] The Canadian Institute of Chartered Accountants, Computer Control Guidelines, Toronto, Canada, 1970, 135p.

[7] Computer Fraud and Embezzlement, EDP Analyzer, 11:9 (September 1973), p. 1-14.

[8] Emergency Rescue Training, U.S. Government Printing Office, Washington, D.C., Office of Civil Defense Student Manual SM 14-1, January 1968.

[9] Federal Fire Council, Fire Protection for Essential Electronic Equipment, Recommended Practices No. 1 (Revised), Washington, D.C., July 1969.

[10] Federal Power Commission, Power Disturbance Report, Washington, D.C. (issued quarterly; special issues on power interruptions as appropriate).

[12] Geller, S. B., The Effects of Magnetic Storage Media Used in Computers, Nat. Bur. Stand. (U.S.), Tech. Note 735, 30 pages (July 1972).

[13] General Services Administration, Building Firesafety Criteria, Washington, D.C., GSA Handbook, July 1965.

[14] General Services Administration, Model Facility Self-Protection Plan, Washington, D.C., Region 3, Federal Protective Service Division, April 1973, 37p.

[15] General Services Administration, Procurement and Contracting, Government-Wide Automated Data Management Services, in Federal Property Management Regulations, Subpart 101-32.4.

[16] Helmick, C. G., Consultant's Guide to Uninterruptible Power Supply Systems (Westinghouse Electric Corporation, Buffalo, New York, May 1972), 82p.

[17] Jacobson, D. W., Automatic Sprinkler Protection for Essential Electrical and Electronic Equipment, Fire Journal 61:1 (January 1967), p. 48-53.

[18] Krauss, L. I., Security Audit and Field Evaluation (SAFE), (Firebrand Krauss and Company, Inc., East Brunswick, New Jersey, 1972), 284p.

[19] Minnesota Mining and Manufacturing Company, Magnetic Tape Erasure—How Serious is the Threat, St. Paul, Minnesota, Magnetic Products Division, January 1972.

[20] Moore, R. T. Penetration Resistance Tests of Reinforced Concrete Barriers, U.S. Department of Commerce, National Bureau of Standards, Washington, D.C., National Bureau of Standards Interim Report 73-101, December 1972, 81p.

[21] Moore, R. T., Penetration Tests on J-SIIDS Barriers, U.S. Department of Commerce, National Bureau of Standards, Washington, D.C., National Bureau of Standards Interim Report 72-223, June 1973, 84p.

[22] National Electric Reliability Council, Review of Overall Adequacy and Reliability of the North American Bulk Power Systems, Princeton, New Jersey, September 1971.

[23] National Fire Protection Association, Care and Maintenance of Sprinkler Systems 1971, Boston, Massachusetts, NFPA Standard No. 13A, 1971, 27p.

[24] National Fire Protection Association, Fire Protection Handbook, 13th Edition, Boston, Massachusetts, 1969.

[25] National Fire Protection Association, Guard Service in Fire Loss Prevention, Boston, Massachusetts, NFPA No. 601, 1968, 15p.

[26] National Fire Protection Association, Halogenated Extinguishing Agent Systems—Halon 1301, Boston, Massachusetts, NFPA Standard No. 12A, 1971, 73p.

[27] National Fire Protection Association, Industrial Fire Brigades Training Manual, Fourth Edition, Boston, Massachusetts, 1968, 148p.

[28] National Fire Protection Association, Installation of Air Conditioning and Ventilating Systems, Boston, Massachusetts, NFPA Standard No. 90A, 1973, 82p.

[29] National Fire Protection Association, Installation of Sprinkler Systems, Boston, Massachusetts, NFPA Standard No. 13, 1973, 168p.

[30] National Fire Protection Association, Life Safety Code, Boston, Massachusetts, NFPA Standard No. 101, 1973, 241p.

[31] National Fire Protection Association, Management Control of Fire Emergencies, Boston, Massachusetts, NFPA Standard No. 7, 1967, 24p.

[32] National Fire Protection Association, Private Fire Brigades, Boston, Massachusetts, NFPA No. 27, 1967, 11p.

[33] National Fire Protection Association, Protection from Exposure Fires, Boston, Massachusetts, NFPA Standard No. 80A, 1970, 20p.

[34] National Fire Protection Association, Protection of Electronic Computer—Data Processing Equipment, Boston, Massachusetts, NFPA Standard No. 75, 1972, 33p.

[35] National Fire Protection Association, Protection of Records, Boston, Massachusetts, NFPA Standard No. 232, 1970, 93p.

[36] National Fire Protection Association, Recommended Good Practice for the Maintenance and Use of Portable Fire Extinguishers, Boston, Massachusetts, NFPA No. 10A, 1973, 35p.

[37] National Fire Protection Association, Standard for the Installation of Portable Fire Extinguishers, Boston, Massachusetts, NFPA No. 10, 1973, 40p.

[38] National Fire Protection Association, Standard for the Installation of Standpipe and Hose Systems, Boston, Massachusetts, NFPA No. 14, 1973, 26p.

[39] National Fire Protection Association, Standard for the Installation, Maintenance and Use of Auxiliary Protective Signaling Systems for Fire Alarm Service, Boston, Massachusetts, NFPA Standard No. 72B, 32p.

[40] National Fire Protection Association, Standard for the Installation, Maintenance and Use of Central Station Protective Signaling Systems for Guard, Fire Alarm and Supervisory Service, NFPA No. 71, 1972, 48p.

[41] National Fire Protection Association, Standard for the Installation, Maintenance and Use of Local Projective Signaling Systems for Watchman, Fire Alarm and Supervisory Service, Boston, Massachusetts, NFPA Standard No. 72A, 1972, 38p.

[42] National Fire Protection Association, Standard for the Installation, Maintenance and Use of Proprietary Protective Signaling Systems for Watchman, Fire Alarm and Supervisory Service, Boston, Massachusetts, NFPA Standard No. 72D, 1973, 51p.

[43] National Fire Protection Association, Standard for the Installation, Maintenance and Use of Remote Station Protective Signaling Systems, Boston, Massachusetts, NFPA Standard No. 72C, 1972, 33p.

[44] Occupational Safety and Health Administration, Portable Fire Extinguishers, Washington, D.C., OSHA Regulation 29CFR—1910. 157, 1973.
[45] Post, R. S. and A. A. Kingsbury, Security Administration—An Introduction, Thomas Books, Springfield, Illinois, 1973, 351p.
[46] Reed, Susan K. and Martha M. Gray, Controlled Accessibility Bibliography, Nat. Bur. Stand. (U.S.), Tech Note 780, 11 pages (June 1973).
[47] Reed, Susan K. and Dennis K. Branstad, Editors, Controlled Accessibility Workshop Report, Nat. Bur. Stand. (U.S.), Tech. Note 827, 86 pages (May 1974).
[48] Simpson, R. H. and M. B. Lawrence, Atlantic Hurricane Frequencies Along the U.S. Coastline, U.S. Department of Commerce, National Oceanic and Atmospheric Administration, Fort Worth, Texas, Southern Region Headquarters, National Oceanic and Atmospheric Administration Technical Memorandum NWS-SR-58, June 1971.
[49] U.S. Atomic Energy Commission, Security of Automatic Data Processing Systems, Washington, D.C., U.S. Atomic Energy Commission Manual Appendix 2703, June 1973, 37. (Unclassified)
[50] U.S. Atomic Energy Commission, Standard for Fire Protection of AEC Electronic Computer/Data Processing Systems," Washington, D.C., Division of Operational Safety, WASH 1245-1, July 1973, 38p.
[51] U.S. Department of the Army, Flood-Proofing Regulations, Washington, D.C., Office of the Chief of Engineers, June 1972, 79p.
[52] U.S. Department of Defense, Security Requirements for Automatic Data Processing (ADP) Systems, Washington, D.C., Department of Defense Directive 5200.28, December 18, 1972, 17p.
[53] U.S. Department of Defense, Industrial Security Manual for Safeguarding Classified Information—DoD 5220.22M, Washington, D.C. (available through U.S. Government Printing Office, Washington, D.C.), March 1971.
[54] U.S. Water Resources Council, Flood Hazard Evaluation Guidelines for Federal Executive Agencies, Washington, D.C., May 1972.
[55] Watt, J. H. (Ed.), NFPA Handbook of the National Electric Code, McGraw-Hill Book Company, New York, 1972, 748p.
[56] Webb, B. L., R. C. Addicks, Jr. and Claude C. Lilly (compiled by), Risk Manager's Guide, The National Underwriter Company, Cincinnati, Ohio, 1973, 590p.
[57] Westinghouse Electric Corporation, Consultants Guide to Uninterruptable Power Supply Systems, Buffalo, New York, May 1972.
[58] What to Do After the Flood, McGraw-Hill, Inc., New York, January 1965, 30p.
[59] Wright, R., S. Kramer and C. Culver, Building Practices for Disaster Mitigation, Nat. Bur. Stand. (U.S.), Bldg. Sci. Ser. 46, 474 pages (February 1973).
[60] Yourdon, Edward, Reliability of Real-Time Systems. Part 1. Different Concepts of Reliability, Modern Data, 5:1 (January 1972), p. 36-40, 42.
[61] Yourdon, Edward, Reliability of Real-Time Systems, Part 2. The Causes of System Failures, Modern Data, 5:2 (February 1972), p. 50-54, 56.
[62] Yourdon, Edward, Reliability of Real-Time Systems, Part 3. The Causes of System Failures (continued), Modern Data, 5:3 (March 1972), p. 36-41.
[63] Yourdon, Edward, Reliability of Real-Time Systems. Part 4. Examples of Real-Time System Failures, Modern Data, 5:4 (April 1972), p. 52-57.
[64] Yourdon, Edward Reliability of Real-Time Systems. Part 5. Approaches to Error Recovery, Modern Data, 5:5 (May 1972), p. 38-40, 43, 46, 48-49, 52.
[65] Yourdon, Edward, Reliability of Real-Time Systems. Part 6. Approaches to Error Recovery (continued), Modern Data 5:6 (June 1972), p. 38-39, 41-46.

5. プライバシー法(1974年)の施行に係るコンピュータ・セキュリティ・ガイドライン

目　　次

序　言

技術上および手続き上のセーフガードを選択し，適用することは，プライバシー法（1974年）によって要求されている諸個人の秘密を守るうえで，連邦政府にとっての重要な作業の一部となっている。当刊行物によって明らかにされているガイドラインは，現行の自動化システムに保有されている個人のデータが権限を越えて暴露された場合の危険を見積り，その危険を最小限にくいとめるために，一連のセーフガードを開発するものである。そのセーフガードはＯＭＢ（予算管理局）のプライバシー法を施行するプログラムの全体のコンテクストの範囲内で，連邦機関に利用される。

コンピュータ科学技術研究所長

ルース・Ｍ・デービス

公　告

ＦＩＰＳ文書はＮＢＳから刊行されたものである。その準じているところは，ＦＰＡＳ法（連邦財産・行政サービス法，1949，修正），パブリック法89－306条（７９項1127），大統領命令11717（38項12315，1973年5月11日付）による施行，およびＣＦＲ第15条第６項などである。

ガイドラインの名称：

プライバシー法（1974年）の施行に係るコンピュータ・セキュリティ・ガイドライン

ガイドラインのカテゴリー：

コンピュータ・セキュリティのＡＤＰオペレーション

説　明：

プライバシー法（1974年）により，諸個人に関するデータのミスユーズあるいは危険にさらされることを防止するために，連邦政府各機関には無数の要求が出されている。個人データを処理している連邦政府ＡＤＰ組織は，たとえ意識的に行なわれたものであれ，事故あるいは不注意の結果であれ個人データが権限を越えて暴露されたり，破壊あるいは修正されることを，適度に防止する必要がある。

それらのガイドラインにより連邦組織にはハンドブックが与えられることになり，その結果，同法を施行するためにはいかなるコンピュータ・セキュリティ・セーフガードの施行に際しても，同ガイドラインが採用されることになる。そこに述べられていることは，リスクとその見積り，物理的セキュリティの方法，特殊情報管理の実際，コンピュータ・システム― ネットワーク・セキュリティ制御などである。

適　用：

当ガイドラインは，予算管理局の特別な要請により作成されたものであり，その目的は，プライバシー法（1974年）により義務づけられたコンピュータ・セキュリティを施行することである。ガイドラインは実際に役立つセーフガードの主旨を設定するのに，全般的なコンピュータ・セキュリティ問題を扱っているので，同時にそれは，個人のプライバシーとは無関係なコンピュータ・セキュリティ問題にも広く適用されることになる。

施　行：

個々の連邦政府ＡＤＰ組織は，プライバシー法（1974年）に起因する，コンピュータ・セキュリティに対する特殊な要求をもっている。特殊なニーズを決定するのは，その組織が保有している個人データの処理任務であり，その処理環境である。これらのガイドラインに含まれた広い範囲にわたるセーフガードについての

記述を活用するためには，組織は自身の特殊なニーズを満たすことのできる，バランスのとれた組み合せを選択することになるだろう。

資　格：

本資料は１セットのガイドラインを提供しており，連邦政府組織はその中から，技術上およびそれに関連した手続き上のセーフガードを選択して，自動情報システムに保有されている個人データを保護することができる。そこには，権限をもった機構の作業に供される，個人データやその関連物を保守するうえで必要とされる決定などのような話題は含まれていない。また，管理上の従業員規則，そのスクリーニングやトレーニングなどといった問題も，本資料の範囲外である。

各組織には，その環境や機能，オペレーションに由来する特殊な要求や，考慮すべきリスクがあるので，全般的に必要なセーフガードのリストを作成することは不可能である。各組織がそれ自体の必要性を分析する必要がある。コンピュータ・セキュリティはプライバシー法（1974年）を施行するための１つの小さな局面にすぎない。従って本資料は，予算管理局（ＯＭＢ）や連邦調達庁（ＧＳＡ），米国人事院（ＣＳＣ）などの他の出版物との関係で考えるべきである。

行政上の概況

プライバシー法（１９７４，５U.S.C. 552ａ）により，連邦政府各機関に対して無数の要望が出され，個人に関する情報のミス・ユーズを防止し，その完全と安全がはかられることになった。これらの要求を満たすためには，選択された管理上，行政上，技術上の手順を応用しなければならず，それらを組み合わせて始めて同法の諸目的を遂げることができる。

本資料により，自動情報システムが保有している個人データの安全をはかるうえでの技術手順を運用するための１セットのガイドラインが提供される。管理上および行政上の手順 — たとえば，個人データを保護するための必要なことに関

連した基本的決定について，それと権限をもった機能の作業との関係，管理上の従業員規則，従業員のスクリーニングとトレーニングなど — は本資料の範囲外である。これらのガイドラインは，1975年3月12日付の予算管理局（ＯＭＢ）メモ「1974年プライバシー法の施行」に応じて作成されたものであり，同法の規準を満たすため，全ての連邦政府機関に提供され，利用されるものである。しかしながら，同法を施行するためにＯＭＢに与えられた，政府レベルの全体計画から見ればこのガイドラインは１つの断片にすぎない。従って，この問題に関する他の全てのガイダンスとの関係で考える必要がある。

技術上のセーフガードには３種類のカテゴリーがあり，それによって，個人情報の完全性を守り，権限外の利用を防止することになっている。３種類のカテゴリーとは，

物理的セキュリティ手順

情報管理の実施

コンピュータ・システム — ネットワーク・セキュリティ制御

である。ガイドラインは３つのカテゴリーの全てをカバーしており，どのカテゴリーの一つだけを取りあげてみても，それ自体ではプライバシーを侵害する全ての危険を防止することはできない。しかしながら，この３種類のカテゴリーのなかから適当な要素を注意深く選択し，個々の必要に応じて，それらをバランスのとれたセーフガードに組み合わせれば，防御の程度は妥当なコストで効果は非常に高いものとすることができる。

それらの技術上の手順の関連性と便益については，プライバシー法（1974年）のコンテクストで見るならば，一目瞭然である。本書第200頁の図1−1は，セーフガードの適応を内包している同法の原理的規定を明らかにしており，また３種類のカテゴリーのそれぞれが，それらの規定を施行するうえでいかに貢献するかを示している。図１－１のユトリックスからも明らかなように，その手順は同法の多彩な規定を管理することと関連して用いられるだけでなく，セーフガードのいくつかは同時に１つ以上の規定を満足するうえで貢献することができる。また，自動情

報システムにおいてデータの完全と保護を保障することは，物理的セキュリティと情報管理の実施によって，かなり達成することが可能であり，複雑なコンピュータ・システム— ネットワーク制御に必ずしも頼る必要のないことが明らかにされている。この意義はきわめて大きい。

プライバシー法のなかで，コンピュータ・システム—ネットワーク制御の使用を最も直接的に意味している主要な規定としては次のようなものがある。権限をもった人間および機関にたいし個人的な情報を漏らすことを制限している5U.S.C.節552a，小節（ｂ）；正確で，関連性があり，タイムリーで，完全なレコードの保守を要求している小節（ｅ）(5)；レコードの保護と完全を保障するためにセーフガードの使用を要求している小節（ｅ）(10)などがそれである。同法は権限をもたない公開にたいし立法上の禁止を用意しているものの，システム— ネットワークのコントロールについても，個人データにたいするアクセスを適度にコントロールして，故意あるいは事故によって保護や完全性が侵害されることのないようにすることを確認しなければならない。

それらのコントロールに含まれる技術としては次のようなものがある。そのシステムおよび遠隔ターミナルの権利をもったユーザの確実な識別をする技術，他のユーザーとともに共有している1つのシステムにおいて，識別したユーザーが特殊なデータにアクセスする権利を確証する技術；そのユーザーが権利をもっていないデータかつ，またプログラムへはアクセスをさせない技術；最後に，システムに内部検査機能を与え，規定されたセキュリティ条件にモニターを通じて守らせる技術などがそれである。個人データをターミナルとコンピュータ・システムの間，あるいはシステムとシステムの間で自動的に転送することを含む場合には，データの暗号化技術を是認するために，保護要求はしばしば十分に強いものであると判断されがちである。

これまでに述べたように，プライバシー法の規定の方面から，技術上のセーフガードを考えるだけでなく，セキュリティ・リスクが起こり，適当なセーフガードが適用できる。コンピュータ・システム— ネットワークの範囲内でのコント

ロール・ポイントとして，同じことを考えることも有効である。この見通しについては第203頁の図2－1に示されている。同図には，機械で読み取り可能なメディア（たとえば，テープやディスク）におけるデータのオフライン・ストレージに始まり，地方や遠隔地に位置しているコンピュータ・ターミナルの相互利用や，通信網を経由しての地方システムのリンクを含む，数多くの可能な処理モードを通じて行なわれる処理など，コンピュータ・システム― ネットワークの諸エレメントが示されている。それによって前段で述べたタイプのコンピュータ・システム― ネットワークのセキュリティ制御にとって，物理的セキュリティおよび情報管理業務の価値をあげるのに主要なたすけとなっていることを再度強調している。

保護手段を適用するうえでの確実性と有効性とを提供するために，ＮＢＳでは以下に述べるような代表的な部分についての，技術上の標準およびガイドラインに関する要求を明示した。

- 物理的セキュリティ
  - リスク管理
  - 火災およびその他の災害
  - 物理的保護
  - 不慮の事故への備え
- 情報管理
  - データの入力，記憶，ハンドリング
  - レコード定義
  - メディア・コントロール
  - セキュリティのためのプログラミング技術
  - ソフトウェア文書類
  - データ・エレメント
- コンピュータ・システム― ネットワークのセキュリティ制御
  - ユーザーの識別

ターミナルの識別

データ・アクセス制御

データの暗号化

セキュリティ検査

これらの代表分野のなかでも，ＮＢＳは次のガイドラインについては既に提供しており，付録にも明らかのように，それらを利用することが可能である。

・コンピュータ・セキュリティの実用的ガイド

・ＡＤＰの物理的セキュリティと危険管理のためのガイドライン

ここで意図されていることは，既に述べた規準とガイドラインが，日常のあるいは緊急の手順を利用するなかで検証され，開発され次第有効であると認められることである。なぜならば，そうした手順は，プライバシー法を施行した経験から得られた必要性や問題を満たし解決することと両立するからである。当面，本資料に記載されているガイドラインは，技術上の手段についての声明と考えられる。この技術上の手段は管理者が自己の特殊な操作上の必要性や環境に適合させるべく，バランスのとれた１セットのセーフガードを決定するにあたって，管理上および行政上の手順とともに考慮に入れなければならない。

5.1 まえがき

5.1.1 1974年プライバシー法

プライバシー法（1974年）により，個人に関するデータのミスユーズを防止し，その秘密を尊重し，その完全性を保障するために，連邦諸機関には数えることのできない程の要求が出されている。各連邦政府機関では，同法の目的を達成するうえでの管理上，行政上，技術上の諸手順を選択し，組み合わせることによって，上記の要求を満たすことが可能となる。

プライバシー法のなかで，コンピュータ・セキュリティについて最も直接的に表現している規定は，5.U.S.C. 552, a.にある以下の部分である。

- 小節(b)，個人的情報を公認された個人および機関に漏らすことを制限している。
- 小節(e)(5)，正確で，関連性のある，タイムリーな，完全なレコードを要求している。
- 小節(e)(10)，セーフガードを用いて，レコードの信頼性と安全性とを保障することを要求している。

同法は，悪用にたいしては立法上の禁止措置を設けてはいるものの，その措置に従うことが，無理なく出来る信頼を築きあげるためには，技術上および関連した手順が必要となる。たとえ故意に行なわれたものであれ，また事故あるいは不注意の結果であれ，個人のデータが不法に暴露されることにたいしては，適度の保護をほどこす必要がある。

5.1.2 ガイドラインの範囲

本書はＯＭＢの要請により作成されたものである。このなかには，自動情報システムに保有されている個人データを保護するうえでの，技術上およびそれに関連した手続き上の方法を詳細に述べた，１セットのガイドラインがあり，プライバシー法の施行をめぐるＯＭＢの一連の資料とつきあわせて利用した方がよい。管理上，行政上の手順，たとえば，個人データを保守するうえでの必要事項，自動化機能の実行の妥当性，管理上の従業員規則，従業員のスクリーニングとトレーニングなどについての基本的決定に関する手順は，本資料の範囲外にある。本資料の諸ガイドラインは，連邦政府の範囲で考えた施行上の１つの局面にすぎない。

同様に，ＮＢＳ，ＧＳＡ，ＣＳＣでも，ＯＭＢの指示を受けて，特殊項目についてのガイドラインを出している。

5.1.3 定　　義

以下の用語は本資料を通じて用いられており，データの取り扱いについて述べたものである。

- 秘密性（コンフィデンシァリティ）

  データに適用される概念。不法の公開から保護する必要のあるデータに準じた状態のことである。

- 情報の集中性（データ・インテグリティ）

  データが引き出されソースデータと一致しており，しかも，事故あるいは悪意から変更，漏洩，破壊されていない時の，データの状態。

- 情報のセキュリティ

  事故あるいは故意の，不法な修正，破壊，漏洩から，データを保護すること。

データを保護するセーフガードは３種類のカテゴリーに分けられる。すなわち，

- 物理的セキュリティの方法
- 情報管理の実施
- コンピュータ・システム — ネットワークのセキュリティ制御

である。それを明確にすれば次のようである。

- 物理的セキュリティの方法

  システムの物理的資産および関連設備を，環境上の危険あるいは計画的な行為から防衛するための方法

- 情報管理の実施

  データを収集し，認識し，処理し，制御し，分布する手順。

- コンピュータ・システム — ネットワークのセキュリティ制御

  コンピュータ・システムあるいはネットワークのハードウェアおよびソフトウェアに用いられる技術で，データの処理やアクセス，それ以外の資産をコントロールする。

5.1.4 セーフガード

これらの技術的なセーフガードの関連性と有益性については，プライバシー法(1974年)のコンテクストで見るならば，容易に理解することができる。図1－1には，セーフガードの適用を伴うプライバシー法の基本的な規定が識別されており，また3種類のカテゴリーのいずれもが，それらの規定を施行するうえでいかに貢献するかが示されている。図1－1のマトリックスはまた，特殊なセーフガードを採用することにより，同法の1つ以上の要求を満たす助けとなることを，明瞭に図示している。同時にそれは，自動情報システムにおいて，データの保護をすることは，必ずしも複雑なコンピュータ・システム — ネットワークのテクノロジーに頼る必要はなく，物理的セキュリティの方法と情報管理の実施を慎重に進めることにより，かなりの程度まで達成されることが示されている。その意義は大きい。

ここで論じているセーフガードは，コンピュータ・システムの個人データにたいし，権限外のアクセスを防止するという特殊の目的をもったものである。しかしセーフガードの多く，特に物理的セキュリティと情報管理の分野のセーフガードは，自動システム同様，手動のシステムにも適応できる。それらのほとんどは，個人的データだけでなく，それ以外の種類のデータの保護をすることもできる。しかしながら，現在の力点は個人データに置かれているため，本資料ではこれ以後，「データ」といえば「個人データ」と同義語である。

図１－１には，プライバシー法の具体的な規定にたいする技術上のセーフガードが述べてある。そのセーフガードはセキュリティがおびやかされ，そして，そのために適当なセーフガードが施こされるコンピュータ・システム― ネットワークの範囲内の，コントロールする必要のあるポイントとの関係で，それらを検討する必要がある。この見通しについては，203頁の図２－１において述べられている。また図１－２には，機械による読取りメディア（すなわち，テープやディスク）におけるデータのオフライン記憶に始まり，種々の処理モードを経由して処理される。コンピュータ・ネットワークの諸エレメントが述べられている。そのなかには，地方や遠隔地におけるコンピュータ・ターミナルの相互利用，通信網を経由しての地方システムとの連結なども含まれている。そこで再度強調されることは，コンピュータ・システム― ネットワーク制御との関係における，物理的セキュリティの方法と情報管理業務の価値である。

これらのガイドラインは，すでに第1.2節で明らかにしたように，3種のカテゴリーのセーフガードを包括している。ある1つのカテゴリーが他の1つのカテゴリーを含むという考え方をすると，プライバシーを侵害する全リスクにたいし，個人データを防衛することができなくなる。しかしながら，注意深くセーフガードを選択しバランスよく組み合わせれば，妥当なコストで，保護レベルを大きく向上させることが可能である。

セーフガードの種類	ガイドラインのセクション	5V・S・C552aの項目 要求	(b) 漏洩の制御	(c)(1) 漏洩の計算	(d) レコードへのアクセス	(d)(4) 疑いのある情報	(c)(1) 職権目的にのみ関係データを使用	(c)(5)、(6) 正確で完全なレコードの保守	(c)(10) 信頼性の保障 レコードの完全性、安全性、	(1)(1) レコードの保有、獲得ストレージ
物理的セキュリティ	3.0									
エントリー制御	3.1		X						X	
ストレージ保護	3.2		X					X	X	X
情報管理業務	4.0									
データのハンドリング	4.1		X		X				X	X
レコードの保守	4.2		X	X					X	
データ処理業務	4.3		X	X		X	X	X	X	
プログラミング業務	4.4		X	X		X	X	X	X	
任務の割当て	4.5		X						X	X
手順の検査	4.6		X	X		X		X	X	X
システム・セキュリティ	5.0									
識　別	5.1		X		X		X		X	
アクセス制御	5.2		X		X		X	X	X	
アクセス検査	5.3		X	X	X		X		X	X
データの暗号化	5.5.2		X				X	X	X	X

図１－１　プライバシー法（１９７４年）の要求に適合する技術的セーフガード

5.2 セキュリティ・リスクの見積りとセーフガードの選択

連邦政府機関にとって，最も重要な管理上の行為として第1に挙げなければならないことは，その機関自体で保有しているレコードのなかから，合法的な機関としての機能を果たすうえで，必要かつ適切なレコードを選ぶことである。また第2に個人データにアクセスするための認可を制限し，最小にすることである。プライバシー法の基礎となっている根本原理は，個人に関する情報は誤って利用されて当人に損害を与えてはならないということである。このように非本質的な情報を除外することは，危険な行動の可能性を減少されるだけでなく，レコードをする業務を最小にすることにより，本質的なデータのセーフガードを容易にする。

個人データに関する信頼性，完全性，安全性を保障することについての，プライバシー法の技術上の条件は，それ以外の要求に比較すれば，それほど細分化，特殊化されていない。プライバシーを支えるために必要なセキュリティの水準を決定するものは，レコードから加工して利用されるもの，それらが不注意あるいは故意に暴露された場合，それを第三者によって利用されること，当人に結果的に与える危険などである。それ以上に，セキュリティの必要性は，そのシステムのレコードが操作される環境によって左右される。ある与えられたシステムを保護するために，どのようなセキュリティ・セーフガードが必要であるかを決定する人間の条件は，保有されている情報に精通しており，同時に，システムが作動する環境について，行政的，技術的，物理的に知り尽していることである。

5.2.1 セキュリティ・リスクの見積り

システムのセキュリティを向上させるための第1ステップは，そのセキュリティ・リスクを決定することである。

セキュリティ・リスクの見積りをしておけば，機関にとっては次の3点について恩恵があることになる。

(1) セキュリティ・セーフガードの追加をする場合，判断の基準となる。

(2) 追加されるセキュリティ・セーフガードによって，重大なセキュリティ・リスクを克服する手助けとなる。

(3) 全体のリスクや漏洩に対し，あまり効果があがらないと見られるセーフガードに係る経費を節約する。

リスクを見積る目標は，個人データの完全性と信頼性をおびやかすような事柄の内容を確認し，その重要度の順序を決定することである。リスクの重大性を左右するものは，その事例のもつ潜在的インパクトであり，それによって引きおこされる可能性のあるインパクトの大きさである。

第2.2節においては，ある一般的なリスクを明らかにし，その一般的な優先順位につい論じることになろう。リスクを見積っておくことは，たとえそれが，最大のリスクについて明らかにし，そのレベルで規制措置を考慮しなくても，ある程度は成功するといえる。しかしながら，そのリスクの程度は，可能ならば，定量的に見積っておく方がよい。そうしておけばどのようなセーフガードが必要であり，妥当であるかを決定する時の，よりよい判断材料となる。時として，数値的なリスクの見積りで多少正確性には欠けるが適当なセーフガードを選択する目的は十分はたすことがある。

事故リスクの予想頻度を見積るには，その機関のこれまでの経験や，同一のレコード・システムを有する他の機関の経験をもとに生かすことができる。計画的な行動から発生するリスクについては，その脅威を実行するためのコストを見積

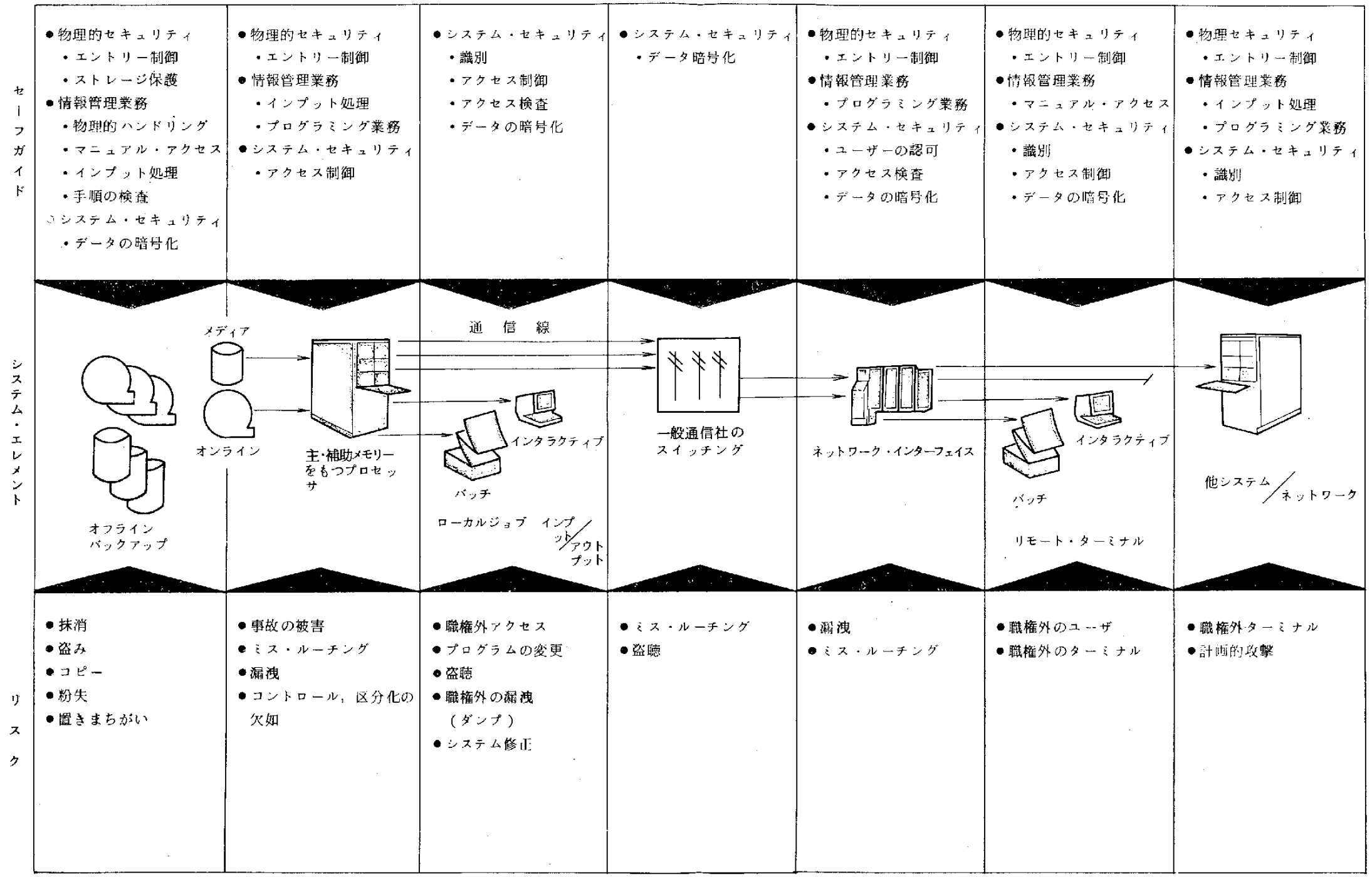


図２－１　技術上のセーフガードと情報セキュリティ・リスク

ればよい。計画的な侵入によるリスクについては，その行動により誰かが実質的な利益を受ける場合，そして，その行動には何らの努力なり知識なりを必要としない場合には，ためらわずにそのコストを見積るべきである。機関のＡＤＰセンターに自由にアクセスできるオペレータならば実質的には自分の金を払わずに，重要なファイルからあるデータを抜き出すことができる。それにたいし，個人でコンピュータ伝送を途中でカットして傍受することは，相当な資本とオペレーション投資が必要となる。

一般にリスクを見積るには，あらゆるリスクを考慮しなければならない。これらのガイドラインは個人データのセキュリティを強調している一方で，最良の道は，ワンセットになった統合されたセーフガードを開発し，そのシステムの有効性を示す資料データを強調することである。

リスクの見積りを行なうチームは，その情報の日常的なハンドリグや処理のなかで発生する問題について，精通していなければならない。リスクを見積るチームの関係者には以下の事項について経験をもった指導者を加えるべきである。

(1) 検討されるデータについて，権限をもっているか，あるいはサポートしているオペレーティング・グループ

(2) 検討されるオペレーションあるいはファンクションをサポートする責任のあるプログラマ

(3) ＡＤＰオペレーションの管理に責任をもつグループ

(4) 機関から独立した機能として，システム・プログラマが居る場合には，そのシステム・プログラマ

(5) システム・セキュリティを監督し，検査する責任をもった人間

(6) 物理的セキュリティの責任を負う人たち

5.2.2 セキュリティ・リスクのカテゴリー

本節では，セキュリティ・リスクの一般的等級を，リスク見積りの冒頭のイラストとして，また関連セキュリティの範囲を理解していくためのステップとして，カテゴリー別に明らかにしてある。リスクはそのシステムに保有されている個人データのあらゆるファイルに関して見積られなければならない。各機関はそのリスクを識別し，情報ファイルの方面からリスクのインパクトを評価しなければならないことになるだろう。

以下の項に挙げたリスクは，不注意によってシステムに侵入した行動結果として出され，それには高度の技術的ソフィスティケーションが要求される。リスクは一般にそれが起こりそうな順序でリストされる。しかしながら，各機関が気付くべきことは，環境が特殊な場合は，リスクは違った優先順位になるということである。新たなＡＤＰシステム ― 特に大規模，リモート・システム ― を設計中の諸機関にあっては，そのシステム構成を決定するにあたり，故意によるシステム侵入のリスクを考慮に入れるべきである。

5.2.2.1 事故、エラー、脱落

最も一般的に遭遇するセキュリティ・リスクが，事故，エラー，脱落であることは経験的に証明されている。これらの事故によってもたらされる被害は，それ以外の原因によるセキュリティ・リスクの総計をはるかに上回っている。情報管理業務を完全に行なうためには，事故，エラー，脱落によってもたらされる被害を少なくする必要がある。

この種のリスクには次のようなものがある。

- インプット・エラー

  データがシステムにインプットされる時に，その一貫性や妥当性についてのチェックを受けなかった，もしくは，インプット処理の過程で，データが漏洩，修正，紛失あるいは誤認された。

・　プログラム・エラー

プログラムの作成にあたって業務能力が貧弱であったり，広範囲にわたるテストを受けなかった場合には，プログラムのなかに，数多くの好ましからざるエラーが含まれることになる。プログラム・エラーは，好ましからざる修正，重要な情報の暴露あるいは破壊の結果である。

・　データの誤った処理

不適当なデータをアップデートして処理する時，たとえば，テープが不適当な日付などを修正する場合など。

・　データの紛失

紙や磁気テープ，それ以外の動かすことのできる記憶メディアにプリントされたデータは，紛失，誤った場所に置かれる，破壊されるなどの可能性がある。

・　不適当なデータの記録の取り扱い

記録されたデータが，ルートやラベルを間違えた可能性がある。それには期待とは異った個人情報が含まれることになる。

・　不注意による処分

個人データが，捨てられた紙くずや磁気テープ，不用になったファイルから修複されることがある。

5.2.2.2 コントロールされていないシステムのアクセスによるリスク

連邦政府機関が不必要なリスクにさらされるのは，ＡＤＰシステムで処理されている個人データのアクセスを担当している人員についての，コントロールが確立されていない場合である。なぜなら，部外者が個人データに自由にアクセスするはずがないからである。機関の従業員で個人データのアクセスを担当する要員数は，その機関の使命を妨げない限りにおいて，最小限にすべきである。

システムのアクセスを制御するうえで，物理的セキュリティの方法はたえず必要とされる。ＡＤＰシステムを利用する人間の全てが処理されている個人データ

にアクセスする権限をもっていると仮定すれば，物理的セキュリティの方法によって，システムのアクセスを十分にコントロールすることは可能である。また，そのシステムが，個人データの全タイプにアクセスする権限はもっていない人間によっても制御するためには，情報の操作及び取扱いの業務とシステム・アクセスを制御する必要がでてくる。

可能性のあるリスクには次のようなものがある。

- オープンシステム・アクセス

  ＡＤＰシステムを利用できると同時にコンピュータルームにも入れる人間のコントロールがなされていない可能性がある。

- データの盗難

  個人データがコンピュータルームあるいはそれ以外の保存場所から盗まれる可能性がある。

- 保護されていないファイル

  データ・ファイルが，ＡＤＰシステムの他のユーザーによって権限を越えてアクセスすることから守られていない可能性がある。そのことは，オンライン・ファイルおよび磁気テープなどのオフライン・ファイルにもあてはまる。後者の場合は，それが掲載されることを要求することにより，容易にアクセスすることができる。

- ダイアル・イン・アクセス

  リモート・ダイアル・イン・アクセスが認められている場合，職権外の人間がそのシステムをアクセスするという重大な危険性がある。

- 異常時のオープン・アクセス

  正常にオペレートしている時は十分に保護されているデータも，異常な環境になると十分には保護されなくなる可能性がある。異常環境としては，電力低下，爆弾の脅威のほか，火災や水害などの自然災害も考えられる。

5.2.2.3 個人データを利用する公的ユーザーにおけるリスク

計画的な行動による重大なリスクのほとんどが，データを扱っている従業員のしわざであることは，コンピュータ関係の犯罪の経験からも証明されている。情報関係の労働者はセキュリティ・セーフガードが実際にどのようなものであるかを正確に知っており，それにたいしどのように対応するかということについても，同様に知っている可能性がある。こうした公認されたアクセスの悪用から，個人データを保護することは，大切なセキュリティ業務の１つである。

そうしたリスクの一団となるにも次のようなものがある。

- 公認されたアクセスにたいして，基準の定義が不明確である。

  職員か，他の職員かデータ条項にアクセスする権限をもっているか否かについて，知らされていない。

- 従業員の不誠実にたいする手ぬるい態度

  従業員の不誠実については，相当に一般的であり，管理上，寛容であることが多い。個人データにアクセスすることのできる機関従業員にたいし，管理規則を作る必要がある。

- 個人データへの検査を受けないアクセス

  個人データにアクセスすることのできるある人間が，自分のアクセスを記録する検査上の手がかりが無いことを知ったと仮定すれば，自分のその行為にたいしては責任を問われる可能性のないことを直感するであろう。

5.2.2.4 物理的環境および悪意の破壊行為によるリスク

ＡＤＰシステムの物理的破壊あるいは無力化が，プライバシーにとって，常に主要なリスクというわけではない。環境の危機や悪意の行為により，プライバシー法の必要としているレコードが破壊されたり，それらのレコードの精度，時宜性，完全性が損われる可能性がある。しかしながら，そのリスクが重大であるのは，破壊されたかも知れないソース・データそのものの価値の損失の故であり，

また，機関の使命はＡＤＰシステムに保有されているレコードに左右されるが故である。ファイルのバックアップや偶発事故対策計画を含めたセキュリティ・セーフガードが，以上に述べたような他の理由からも必要であり，そうすることにより，各種のリスクからプライバシーを防衛するうえでより十分なものとすることができるだろう。

そのようなリスクとして，以下のことが考えられる。

- 火事，熱や水による被害，水害
- 電力の低下
- 従業員あるいは部外者による悪意の破壊行為

5.2.2.5 計画的な侵入によるリスク

現在のコンピュータ・システムは計画的な侵入にたいしては弱点をもっているが，それは日常的なセキュリティ・コントロールによって回避することができる。こうした種類の侵入をふせぐのに必要な条件は，特殊な技術知識をもった人間の協力である。現在までのところ，そのような計画的侵入によって引きおこされた，実質的な被害の例はあまりない。今のところ現れているリスクの実態は，これまでに述べてきたリスクの規模が大きいのに較べれば，はるかに小さいものである。専門知識をもった侵入者は理性的に行動するのが常であり，目標になった個人データが，その侵入者にとって魅力的な価値をもっていることは間違いない。しかしながら，機関が知っておくべきことは，その侵入者が，個人データが安全ではないことを宣伝することにより，機関を苦境に陥れようと試みる可能性のあることである。

将来，計画的な侵入によるリスクは一段と顕著なものになるであろう。その潜在的リスクは，コンピュータ・ネットワークが大規模になるにつれて，著しく増大するであろう。将来にむけて規模の大きいネットワークの設計を進めている機関は，計画の初期段階において，これまでに述べてきたリスクを考慮すべきである。

計画的な侵入によるリスクには次のようなことが考えられる。

- 誤認によるアクセス

コンピュータあるいはデータへのアクセスを制御するために，パスワードが使用されることが多い。しかし，それが注意深くコントロールされて使用されない場合，非常に容易に入手することができる。さらに言えば，公認されたユーザーが使いっぱなしにして動かせる状態のままにして放っておいたターミナルを，ある人間が使用する可能性はあり，あるいはその人間は，公認されたユーザがそれから離れようとした時に，コミュケーション・ポートを入手する可能性がある。

- オペレーティング・システムの欠陥

オペレーティング・システムにおいて，設計および実行のエラーがあれば，ユーザーはそのシステムをコントロールすることができる。ひとたびユーザーがコントロールを開始すれば，彼はそのシステムについて，検査コントロールを無力化し，検査トライアルを抹消し，どんな情報をもアクセスすることが可能となる。

- プログラムの破壊

プログラムにサブ・プログラムが含まれていて，それがセキュリティ保護を無力化する場合には，それ以外のプログラムは，秘密裡に個人ファイルをコピーしたり，保護がゆるやかになる時にファイルを誤認するようになる。

- ペテンにかける

システムの要員やシステムのソフトウェアをミスリードするための行動がなされることがある。その結果，一見すると正常であるが，実際は承認された以外のアクセスまで行なわれることになる。

- 盗　聴

通信線が許可された以外の不法なターミナルによって「モニター」されることがある。その目的は情報の取得あるいは修正，もしくはＡＤＰシステムへ許可範囲外のアクセスをすることにある。

5.2.3 セーフガード選択におけるコストの考慮

各政府機関はセーフガードをめぐる複数のオプションのなかから選択するにあたり，各々のコストを当然考慮しなければならない。各機関がコストを見積るにあたり，その独自の環境を考慮しなければならない以上，コスト係数を推定する一般的なガイドラインは，プロセスの優先順位を明らかにするための手助けとなるだろう。

コストは二つの主要な分野に分けられる。すなわち，原価と運営費である。原価に含まれるものとしては，新しいシステム・エレメントの取得，そのエレメントを受入れるための既存システムの修正，新エレメントを支えるための一時的な管理上の方法，新しいシステムの初期テストなどに要する費用がある。運営費として考えられるものは，その強化されたシステムを運営するために増大した日常的な経費があり，そのなかには人件費，コンピュータの処理や記憶，システムのモニタリングなどのコスト要素が含まれることになる。

プライバシーにとってセキュリティは必要条件であるが，それ以外にもセキュリティを必要とする数多くの理由がある。金融の記録や給料支払簿など，貴重なデータを保護するに足る基本的なセキュリティ・セーフガードは，プライバシーを保護するうえでも十分なものである。コンピュータ・セキュリティに要する経費全体のなかのほんのわずかな部分が，プライバシーのために大いに役立っているわけである。各政府機関は可能な限り，プライバシーを確保するための経費とは異なる，それ以外の理由のために設置されたセキュリティの方法に要する経費を確保すべきである。

リスクの見積りをすることにより，コントロールの必要があるリスクが明らかにされるであろう。第3，4，5項では，よく使われるいろいろなセキュリティ・コントロールについて述べた。それらの保護メカニズムが選択された結果，補助手段としてのシステムが形成されることになり，必要な場所を保護することになる。各々の保護手段は，追加経費によって行なわれた強化された保護の方面から

評価されるべきである。保護のための少額の支出が，許容範囲を超えて，計画的な被害を与えるために要するコストが増大するかも知れない。テープ・キャビネットに施錠をすることが，一定のファイルに必要な保護の全てを意味することがある。というのは，その結果，「錠をこわす」という不法な行為がなされたことが直ちに判明するからである。しかし一方では，野蛮で非理性的な行為にたいしては，施錠は何の役にもたたない。

物理的セキュリティについては最初に検査し，必要があればいつでも向上させるべきである。ほとんどの機関では，物理的セキュリティの方法を応用することにより，そのデータにたいする故意あるいは公然たる外部からの行為にたいして，有効な保護を行なう。しかしながら，ファイルにたいする事故や不慮の被害，もしくは公然とした内部の行為にたいして，それは無防備である。適切な**情報管理業務**が行なわれていれば，物理的セキュリティによってカバーすることのできない数多くのリスクにたいしても，かなりの程度で保護を行なうことはできる。データの感度が物理的セキュリティや情報管理業務による保護以上のものを必要とする機関にあっては，**システム・セキュリティ・セーフガード**を考慮すべきである。

5.3 物理的セキュリティ

物理的セキュリティがデータの保護に関している限り，それはデータ以外のリソースの保護に用いられる物理的プロテクションと異なるところはない。つまり，施錠，ガード，管理上の制御手順を用いることによって実行されるものである。それらはコンピュータや関連設備を設置している構造物を保護するうえで必要とされる方法と同様なものであって，その内容物を保障するために，事故や火災の被害，環境上の危険に備えているのである。物理的セキュリティのリスクを見積るうえでの多方面にわたるガイドラインおよび適切な方法の採用については，第1部の

「ADP処理の物理的セキュリティおよび危険管理のためのガイドライン」

に述べられている。ここでは，物理的セキュリティの方法について，その必要性の決定および採用に関する考え方にスポットをあててみよう。

コンピュータセンターの入口でのセキュリティについては，固く決意した侵入者以外は，入室をはばむことができる。権限をもたないで施設に侵入することを防止する目的は，防衛力をつけるだけでなく，外部からのアクセス可能な手法を全部コントロールすることにより，その目的を達することができる。そのなかには，排気孔などの関係のなさそうな部分も含まれている。またその手段としては，署名の手順，許可された要員のつけるバッジ，特殊錠，外部の照明，テレビカメラ，フェンス，侵入防止装置などの使用が考えられる。

ファシリティの環境を完全に調査すれば，ある分野における特殊な危険性を明らかにすることができる。すなわち，化学的あるいは爆薬物をめぐる動き，洪水の動向，可燃物の異常な貯蔵，来訪者の不十分な管理，データが破壊されたり，暴露されて，広く知れわたったり，偶然に移動される結果になるかも知れない情況が予想される，明らかな被害などについてである。実際，コンピュータ施設の

位置を選定するに先だち，時として不可避的なものもあるが，上述の危険を考慮に入れなければならない。

火災や爆破，自然災害からの防御は，いかなるコンピュータ設置にも利用できると仮定することはもっともであることだが，管理上の方法によっても，レコードの信頼性と安全性を保障できることを忘れてはならない。災害的な情況によって引きおこされるデータのリスクは，現実のカタストロフのなかから発生する破壊にたいしてもっている。データの記憶メディアの脆弱性に原因しているだけでなく，結果的には，破壊された設備に保有されていたメディアやレポート・ソース材料を外部に明らかにすることになる。災害や事故であろうがなかろうが，保有されているデータにたいするリスクには，気象や消防活動，救急活動，野蛮な行為，脅威などの結果として考えられる被害が考えられる。

ある状況を対象とした物理的な防護手段の必要性やその程度を決定する際，特別な規定といったものは存在しないが，考慮すべき数多の可能性は確かにある。例え如何に特殊な施設や設備であっても，不正な破壊活動や個人データの暴露及び修正に対するセーフガードを確立する為には，以下に示すような一連の手段が選択対象とならざるを得ない。

5.3.1 エントリー・コントロール

- コンピュータ施設への出入りを最少限に抑制する。（この手段は特に防火責任者や建物管理者との協調が必要である。）また扉は強引な侵入を防ぐに足る充分な強度を保持しなければならない。
- あらゆる入口に監視設備（screening device）を設置する。ガードマン，バッジ・リーダー，電子ロック，他所でリモート・コントロールされるＴＶカメラ，物理的なロック等がこれに相当する。可能ならば，全ての出入りを日誌に記録する方法も良い。当該施設に出入りする全ての物品をモニターし，配送予定表に記載されていたか否かをチェックするのも必要だ。

- 保護を必要とする領域が広汎なものであるなら，外灯，ＴＶカメラ，巡視パトロール，侵入探知器等の使用を考慮すべきである。だがこのような防護措置は普通ＡＤＰ管理者の責任外である。
- 侵入者が入り込んだり物品の授受を行ない得る全ての開口部の安全を期す。
- 入場許可を示すバッジの使用。このバッジは警備係がバッジ所有者をチェック出来ない程多量に発行すべきものではない。職員が勤務を離れる際は，その理由の如何を問わず交付を受けたバッジや鍵が回収されねばならない。外部の訪問者にも職員との相違が一見して判別出来る臨時バッジを発行する。
- 停電，爆弾破裂，失火警報等の注意をそらせる異常な変化があった場合，施設の点検を徹底的に実施し，混乱に乗じて起こるかも知れない破壊活動や損傷を摘発，防止しなければならない。入退場記録簿や他の記録を再検討する必要がある。こうした措置が取られれば異常事態を引き起した加害者を確認することが出来よう。
- コンピュータ施設内に置かれていないリモート・ターミナル，テープ・ライブラリー，廃棄物処理設備等の保護にも留意すべきだ。

5.3.2 ストレージ保護

- データ記憶媒体の防火対策を策定する。この際消火活動が蓄積データに与えるリスクも考慮すべきだ。テープやディスクのライブラリー保管室は，熱や火炎だけでなく水からもその中味を保護出来るような特別な保護評価を与えられねばならない。この評価の作業は，ストレージ設備の選択時から行なわれる必要がある。
- 災害対策計画には当然防護手段を含むべきである。また災害復旧の手順は定期的に検査し試用されねばならない。記憶媒体，コンピュータ・プリントアウト，公表記録，原資料等の保管場所を移動する際には，勿論こうした手直しを行なう。もし略奪や窃取の危険性があるなら，警備員を配置すること

も考えられる。またデータが水の被害に弱いなら，プラスチック・カバーで保護することも出来よう。

・ データの保護を十分に実施するためには，不定期のセキュリティ点検を行なう。ロックされていない扉，開け放されたままの扉，掛け金をおろしていない錠，敏感すぎてスイッチを切られたままになっている火災報知器や侵入探知装置等のチェックが対象となろう。

物理的なセキュリティ手段は，人的行為の不可測性や環境の不確定要素から生じるリスクを防御する最初のディフェンス・ラインである。非常に簡単なセーフガードの形態をとるものも多く，その導入所要時間も短かいのが普通である。当然のことながら，あらゆるサイトに全ての物理的セキュリティ手段を採用する必要はない。むしろ支出を抑制する方向で総合的に考慮し，妥当に選択されることが必要である。

5.4 情報管理業務の実施

この情報管理業務とは，当該機関の目標を達成するために情報に加えられる数々のオペレーションを対象にしており，そのオペレーションの制御に使用される技法や手順を意味している。機関の使命や性格に関連した情報の必要性や利用を決定する基本的な管理業務にまで及ぶものではないことに留意されたい。この文脈から，情報管理には，データ収集，チェックや変成，情報処理，記録保管，情報の制御やディスプレイ等の表示，情報管理業務の標準化が含まれることになる。

こうしたプロセスを効果的に実行すれば，プライバシー法案の目的である正確かつ完全なデータの維持に大いに寄与することになろう。従って現行業務の再検討は，修正や強化が必要か否かを決定するためには，まず第一に実施されねばならない。また現行業務の変更は，追加支出や総経費に様々な程度の差をもたらす。つまりケース・バイ・ケースという訳だが，これは従来の管理業務がどのようにうまく遂行されているかによるだろう。

以下に示す情報管理ガイドラインは，各々の説明を容易にするため主要分野別に分類されている。だが，記載されている業務のすべてが，あらゆるデータ処理施設に要求されるのではない。採用業務の選択は当然，各機関の置かれている状況を反映したものになるはずだ。例えば，人事データだけを取り扱っている施設は，個人データを含む蓄積媒体の分類だけでは円滑な業務を遂行出来ない。

5.4.1 個人データの取り扱い

- 全ての個人データを物理的に処理する時間中の予防手段及びコンピュータ要員の責務を記載した手順のハンドブックを用意する。これには，プライバシー法案に規定された政府の契約当事官庁が参照利用出来るような手順のレ

ファレンスが含まれるべきだ。

- 個人データを含む全ての記録媒体を分類する。この分類作業は，個人データの不時の誤用を少なくし，不注意による誤用や故意の悪用が発生した時点での責任の所在を明らかにするものだ。
- 個人データをユーザーが利用する場合，その機密保持を条件づける形で蓄積することが必要だ。一例を挙げると非使用時には必ずロックしておく旨の規定がこれに相当する。
- もしプログラムが個人データを含んだレポートを作成するなら，こうしたデータの存在を指示する何らかのプリントが記されねばならない。
- 法的に要請された特別な保護を付与するため，個人データを内包する全てのコンピュータ入出力カード整理箱，ディスクパック・カバー，テープ・リールにはカラー・コードをつける。
- コンピュータが作成したレポートに含まれるあらゆる分野の個人データの記録を保管し，当該機関によるこの種のデータ・ファイルの確認やその他の日常利用を容易にする。
- 個人データの不法な暴露を防ぐため，中間処理段階の生成物，つまりディスクパックやスクラッチ・テープの管理を徹底する。
- 個人データへのアクセスを許されている人々（システム・ユーザーのみならずコンピュータ要員も含む）の最新ハードコピー認可リストを常に保管し，アクセス制御や認可チェックの態勢を確保する。オペレーション要員やシステム・スタッフは彼等が取り扱うデータに関与している点を忘れられてはならない。というのも，異常事態が発生する前提として彼等が持っているデータ内容の知識が介在することもあり得るからだ。
- 責任とリスクの関係を明確にするため，コンピュータ施設内部の個人データ・ファイルの在庫をリストアップし，それを常に最初にハードコピー・データ目録としてまとめておくべきである。

5.4.2 個人データの利用経過記録のメンテナンス

- コンピュータ施設に持ち込まれた全ての新しい個人データに対して常に正確な報告を保証する手順を確立すべきだ。
- 個人データを含む記憶媒体のコンピュータ施設への出入りを記録する移動簿を用意する。
- システム・ユーザーによる個人データへのターミナル・アクセスをその都度記す記録簿を保管する必要がある。

5.4.3 データ処理業務

- 個人データの受領時や入力，蓄積，処理が行なわれている間の数量を確認出来るよう制御ナンバーを用いる。
- 個人データの収集・入力方式の厳密さを常にチェックする。
- 全ての個人データの正確な計算を保証するためテープ，ディスク等の記憶媒体の在庫管理を定期，不定期に行なう。
- 個人データのバックアップ手順の確立。法的に要請されているなら，データ・コピーの第二の保管場所を用意すべきだ。
- 全ての個人データをカバーする記録保有時間表を作成し，少くともデータ・タイプ，保有期間，保有に責任を負う機関名称などは記載されねばならない。
- コンピュータに何らかの故障が起った時，個人データに間違いが生じなかったかどうかを確認するため，故障時に処理されていた全個人データをチェックする。
- もしデータ量が経済的に処理し得るものならば，取り扱いに注意を要するアプリケーションには専用処理時間を設けてもよい。
- 個人データを含んでいることがはっきりしているファイルは，データ内容をみだりに更新されないよう常に監視されねばならない。この種のファイル

がどのような場合に引き渡せるかについて，正式な決定・認可プロセスが確立される必要がある。

- データを収集する際，当該ファイルが醸む魅力をもつだけの価値があるかどうかに常に留意する。
- 個人データの収集とその結合を行なう際，いかなる個人情報の追跡も不可能にしておく。個人データを取り戻すための推測や入手方法が解らないようにすることも大事である。

5.4.4 プログラミング業務

- 全てのプログラム開発・修正作業は，監督者の指示に基づいてその業務に直接関らないプログラマーの独自のチェックを受けなければならない。
- 個人データの処理またはアクセスが想定される既存プログラムの在庫目録を作成し，正式利用の経過をチェックする。
- コンピュータ・プログラムに何らかの個人データを用いているプログラミング作業は公明正大に実施されかつ確認されねばならない。
- ソフトウェア・セキュリティを内包するあらゆるオペレーティング・システムの変更に対しては，書面による手続きを経て厳格に管理する。

5.4.5 責任の所在

- 特定の個人を選んで人事データの蓄積，利用，処理等の業務の責任者とし，併せて物理的なセキュリティ手段の使用，情報管理業務及びコンピュータ・システムへのアクセス制御をも管轄させる。この責任者は，データの内部使用だけでなく認可を受けたデータの外部への移動にも配慮し，リスクに関連した情報を運営機関に報告する。
- 各処理時間（シフト）の責任者を置き，要員配置に意を配らせるとともに

個人データ保護政策が円滑に履行されているかどうか確かめさせる。

- 個人データの処理に携わる全職員に行動綱領を順守させる。

5.4.6 手続きの監査

適当な機会を選んで既存の手続きや手順の再検討を行なう。監査の対象には，特定の情報フローだけでなく，一般的な業務も含まれる。監査の実施に当って考慮すべきポイントは次の如くである。

- 監査グループは組織内にも設置出来るが，対象業務に直接責任を負う職員から独立したものでなければならない。
- 不定期的に外部の独立監査機関に業務を委託することも可能だ。
- 監査報告書は，以後の通常点検のために保管し，機密の漏洩を調査する際の参考データとする。

5.5 システム・セキュリティ

物理的なセキュリティ手段と情報管理業務が軌道に乗ると，大規模な情報システムの管理者の中には，システム自体をベースにしたデータ保護手法を採用しようとする者も出てくるだろう。これらの方法の中には，ユーザー確認手続き，システム活動を追跡調査するアクセス監査，データ・アクセスを制御するシステム構成等が含まれるが，今日のシステムでは全て内部に組み込めるものばかりだ。こうした方法と適用し得る状況について以下少し詳しく触れてみよう。

5.5.1 個人の確認

システムを利用することを許された各個人を識別確認することは，当該システムに内蔵されたデータを防護する最初のステップである。大抵の場合ユーザーの確認は，2段階のプロセスつまり識別と立証で構成されていて，システムを利用しようとするユーザーはまず彼が誰であるかを述べ，これに応じてシステムは彼が本当に本人であるかどうかをチェックする。確認の決定は，バッチ・ジョブを希望するユーザーをシステム要員が識別する人為的なものから，リモート・ターミナルからの要請を全自動式にシステムのログ・オンの手順で行なうものまで実に幅広いパターンが存在する。誤認する危険性は，ジョブがリモート・サイトからＡＤＰ施設に直接要請される時最も大きく，更にＡＤＰ施設へのアクセスが通常の通信回線を使って行なわれる時この危険性は増大する傾向を持つ。

情報システムへのアクセスを許可する際，特定個人の確認に用いられる方法には3つのカテゴリーがある。これらの方法は，個別的にも，また組み合わせても利用することが出来る。

① 当該本人の知っていること

② 当該本人の持っているもの

③ 当該本人を証明するもの

第一のカテゴリーに含まれるものには，パスワード，鍵の組み合わせ，特定個人の経歴に含まれる事実がある。また第二のカテゴリーは，バッジ，機械の読み取りが可能なカード，鍵等が該当し，第三のカテゴリーは，特定個人の容貌，指紋，掌紋，声，署名等の特徴的なもので構成される。また最後のカテゴリーには，警備員による判別も含まれ，不正なアクセスに対してこの方法が最も有効に働くことも多い。

バッジ，機械読取情報を持ったカードまたは鍵は，遠隔ターミナル・ユーザーの確認に有効だが，それ以外の立証手順にも関心を払う必要がある。バッジや鍵の物理的なセキュリティ管理については第3.1節で触れているが，確認プロセスで果す役割は大きい。

パスワードは，システム・アクセスへの許可付与のために今日最も普及している確認手段である。これらのパスワードは，システム・ユーザーと，アクセス権が認められている特定のシステム・リソースとを関係づけるために用いられていて，しばしば特別なアプリケーションや情報ファイルに付随した形をとっている。利用度が高いので，パスワード使用にまつわる経験の蓄積もかなりのものがある考慮すべき点をまとめてみると，

- パスワードは，個人の責任を明確にし，パスワードの不法な第三者へ貸与することを防止するため，必ず個々人に帰属させねばならない。またパスワードは，ユーザーの確認だけでなく，ユーザーの使用が許されているデータやシステム・リソースの管理にも用いられる。
- パスワードは覚え易い方が良いが，名前のイニシャルや生年月日に基づくものであってはならない。最善の方法は，システムの運営管理者がユーザーのために任意のパスワードを付与することだ。
- パスワードは一定期間毎に変更されるべきであり，不正使用が発見されたり予想され得る場合は，勿論言うまでもない。

5.5.2 システム・アクセスの制御

ユーザーの確認はシステムの不正利用に大いに効果があるが，データの利用にも一定の制約を加えるべきであろう。アクセス・コントロールはこの目的のために用意するものだ。ひとたび当該システムにアクセスしたユーザーが，思い通りにデータを変更したり破壊したりするのを防ぐ役割を持っている。ある活動の実行または特定データへのアクセスを許可されたユーザーのリストを作成し，正式なデータ活動だけが行なわれるのを保証するためにこれらをコンピュータに蓄積すればよい。

この方法を実施するにあたっては次のことを考慮したい。

- 商用化されたシステムの中には，データ・アクセス・コントロールを内蔵しているものもある。だが大抵の場合，現行のアプリケーションを再プログラム化する努力が必要とされるので，この方法が採用されないことの方が多い。しかしながらアクセス・コントロールを用いることでデータ保護が著しく向上することも確かである。
- アプリケーション・プログラムは，もし，オペレーティング・システムがアクセス・コントロール機能を持っていなければ，同機能を果す内部メカニズムを備えることが可能である。

5.5.3 アクセス監査

誰がどのデータにアクセスしたかを記録する機能は，アクセス・コントロール機能を問題にする時，重要な意味を持つ。コントロール・メカニズムはデータ利用報告書の基礎となるものであり，これらの報告書は，全てのシステム活動，全てのデータ・アクセス及び変則的な活動等をリストアップ出来るような構成を持つべきであろう。またデータの不正暴露の点検にも大きな役割を果たすことが出来る。

上述した報告書を作成する監査能力は，現在料金計算で実用化されているシステム利用自動記録の増強にも利用出来る。こうした利用法から得られる利益の一部として，アクセス・コントロール機能の導入コストが部分的に相殺されることがあげられる。セキュリティ記録や監査結果はコストがある程度回収出来るということになるだろう。というのは，システム利用に対するより正確な料金計算，システム故障原因の一層早い確定，事故発生後のデータベース復元の容易さ等が期待出来るからだ。

5.5.4 ネットワーク・システム

コンピュータ・データが受けるリスクは，あるネットワーク内のコンピュータ間で転送されたり，あるデータ・バンクとリモート・ターミナル間でやり取りされる時にも大きくなる。ネットワーク内でアクセス出来るデータの量が増え，特定データを利用するユーザー数が増加し，更にネットワークの地域的な分散化が進行するにつれて，故意の悪用がふえている。特に，データの伝送中にこうした事件が多く発生している。またメッセージが修正されたり，他の内容に置き換えられる事例もみられる。ネットワーク・ユーザーやターミナル側の不正な作為により，エントリーの確認があやまらせられることもある。最後になったがアドレスの突然なあるいは故意の変更でデータ・トラフィックが全く違った目的地に通じることもある。

暗号化の連邦標準草案が現在作成されつつあるが，個人データの転送を保護する実際的な暗号化方式の事例はまだない。未来のシステムの設計に携わる人々の便宜を考え，暗号化については第 5.5.2 項で特に触れている。だがネットワーク上のデータ保護手段は，他にも可能性を秘めたものがかなりある。考慮すべき論点をひろい出せば，

- 他のシステムの場合と同じように，ネットワークにおいても，ユーザーの確認，アクセス・コントロール，アクセス監査等の要件を確定するべきだ。

- ネットワーク・アクセスの管理を厳密にする。有効な手順の一つとして，全てのコンポーネント（コンピュータ，端末機器，通信制御装置）の位置を指定したコンピュータ・ネットワーク・アーキテクチャーの構成図を作成することがある。各コンポーネントは独特な識別によって分類され，ネットワーク利用を許可された人はターミナルのリストも用意される必要がある。このリストには，アイデンティファイアー，利用許可を受けたターミナル，データ・アクセス権，アクセス制限等が各々の場合に応じて記載される必要がある。また当然のことだが，このリストの訂正，アクセスする個人や権利の追加削除に関する規定も立案されるべきだろう。
- データの公開件数を算定するため，個人データの移動をセキュリティ監査簿に記録としてとどめる。
- 例え最初のシステム・アクセスがその要求者に許可されていても，微妙なデータを含んでいる特別なリクエストにはコンピュータ・オペレーティング・システムへの問い合わせが必要だ。
- ネットワーク・セキュリティ責任者を任命する。

5.5.5 将来のＡＤＰシステムのためのプランニング

将来システムの開発計画に参画している人々にとってコンピュータ・セキュリティ分野のテクノロジーの発展を正確に予測することは，とりわけ重要である。システム設計に最初から新しいテクノロジーを組み込めれば，これにまさることは無いからだ。以後の議論は，この点に絞って進めよう。

5.5.5.1 内部コントロール

現在のコンピュータ・テクノロジーでは，ある種の内部システム・セキュリティの問題を解決出来ないのが現状である。こうしたセキュリティ上の問題は，どのような特別なセキュリティ・コントロールを用いても間接的で精巧な侵害を回

避することが不可能である事実に帰因している。確かにこの種のセキュリティ問題はあるが，発生する可能性を過大評価しないこともまた重要だ。この種の攻撃は，ある有能な個人がＡＤＰシステムへの意図的な侵入計画に膨大かつ献身的な努力を払わなければ起り得るものでないからだ。歴史的にみてもその動機は大半が金銭である。これまで述べて来た様々なシステム防護措置は，間接的な攻撃の企画や実行を増々困難にしつつある。セキュリティ監視記録は，攻撃の探知と犯人の逮捕の可能性を高めているので，この種の攻撃には現在のところ最も有効であると言えよう。また，オペレーティング・システムへの干渉のような複雑な間接的攻撃に対抗し得るセーフガードを用意するのは可能だが，コストとの兼ね合いで非現実的なものと認めざるを得ない。

テクノロジーの進歩は，内部のシステム・アクセスの制御を回避する試みに対抗し，しかも対費用効果面でも釣り合う方式を編み出すだろう。1970年代後半あるいは80年代初頭以降にコンピュータ・システムを導入しようと考えているユーザーは，こうしたテクノロジー進歩の成果を利用出来るかも知れない。

さて次に示すガイダンスは，現行のコンピュータ・テクノロジーを基礎にしたデータ処理設備向けに作成したものだ。

- 微妙な情報は，一時にしかもひとところに置かれないようデータ処理活動を分断することも必要だ。
- コンピュータ・セキュリティの脅威にさらされるかも知れない個人データは，厳重な物理的コントロール下に置かれて処理されねばならない。例えば，データは専用モードで取り扱うことも可能だし，システムへのリモート・プログラミング・アクセスは，当該情報の処理中は停止するといった方法もある。

5.5.5.2 データの暗号化

データ処理ネットワークのプランニングと設計は，微妙な情報がネットワーク内で転送されている時，それを通信設備を使って横取り出来ないような防御手段

を講ずべきである。高度のリスクが存在するような条件下では，コンピュータ・ネットワーク内の個人データ保護のためにデータの暗号化が必要とされるだろう。次に示す素材は，将来のネットワーク計画の設計者が考慮に入れてほしい基礎的な情報である。

暗号化は，極秘のプロセスかあるいは秘密のパラメーターに依処した通常のプロセスで達成される。代表的なネットワーク構成で暗号化プロセスの互換性を保証するためには，むしろ後者の方が適しているだろう。暗号化プロセスは，あるアルゴリズムで規定されるのが普通であり，このアルゴリズムに提供される秘密のパラメーターは，キーと呼ばれる。

標準局（ＮＢＳ）は，1975年3月17日付けのFederal Register にある暗号化アルゴリズムの事例を公表したが，これは一応，データ暗号化標準として満足すべきレベルのものである。この標準は連邦情報処理標準（FIPS）の一つとして正式に公布される予定である。またこのアルゴリズムは，現在の技術水準で採用可能なものであると考えられている。

暗号化装置向けにデータを書式化し，暗号データを送受信するために，その制御装置の開発が必要だ。これはコンピュータ・コンポーネントとこれに接続される通信ネットワークを主軸にすることだろう。

複雑な暗号化装置がネットワーク・データ用に調達される前に，まずコンピュータ・システム内部のユーザー確認，アクセス・コントロール，アクセス監査が保証されねばならない。だが，暗号化，暗号化装置の可用性，ネットワーク制御装置等を考慮する際，次の注意が払われるべきであろう。

- 第5.4節で述べたネットワーク・ダイアグラムと認可リストを用いるに当って，このダイアグラムは暗号化装置の配備によって強化されねばならない。これは，データがネットワーク・セキュリティの脅威に弱い場所で特に個人データを保護する必要があるからである。
- データ暗号化のキーは，権威あるネットワーク要員の手で作成配布される必要がある。このキーは，常時保護され，そしてしばしば変更されねばなら

ない。定期的な変更は勿論のこと，侵入事件が起こるかまたはその可能性があったと判定し得る時は直ちに手直しされねばならない。

昭和52年3月発行

発行所　財団法人　日本情報処理開発協会
東京都港区芝公園3－5－8
機械振興会館内
TEL(434)8211(代表)

印刷所　株式会社　正文社
東京都文京区本郷3丁目38番14号
TEL(815)7271(代表)

51−R005