COTIS資料

米国におけるコンピュータ・セキュリティのガイドライン

（米国　商務省　標準局 刊
FIPS文書31号, 41号より）

昭 和 52 年 2 月

JIPDEC

財団法人　日本情報処理開発協会

この資料は，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調査研究」の一環としてとりまとめたものであります。

目　　次

第　1　部

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

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。

1. ＡＤＰセキュリティ分析

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。

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。

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，妨壁，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

近接ーを充分想定し，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。

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。

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。

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

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		S 9,700	S 6,850	S 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。

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。

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，

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仕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。

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。

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。

2. 自然災害の予測

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。

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。

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

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。

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。

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充填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。

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。

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，泥物，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。ここでは鉄鉋水が発生しやすい。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遭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。

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

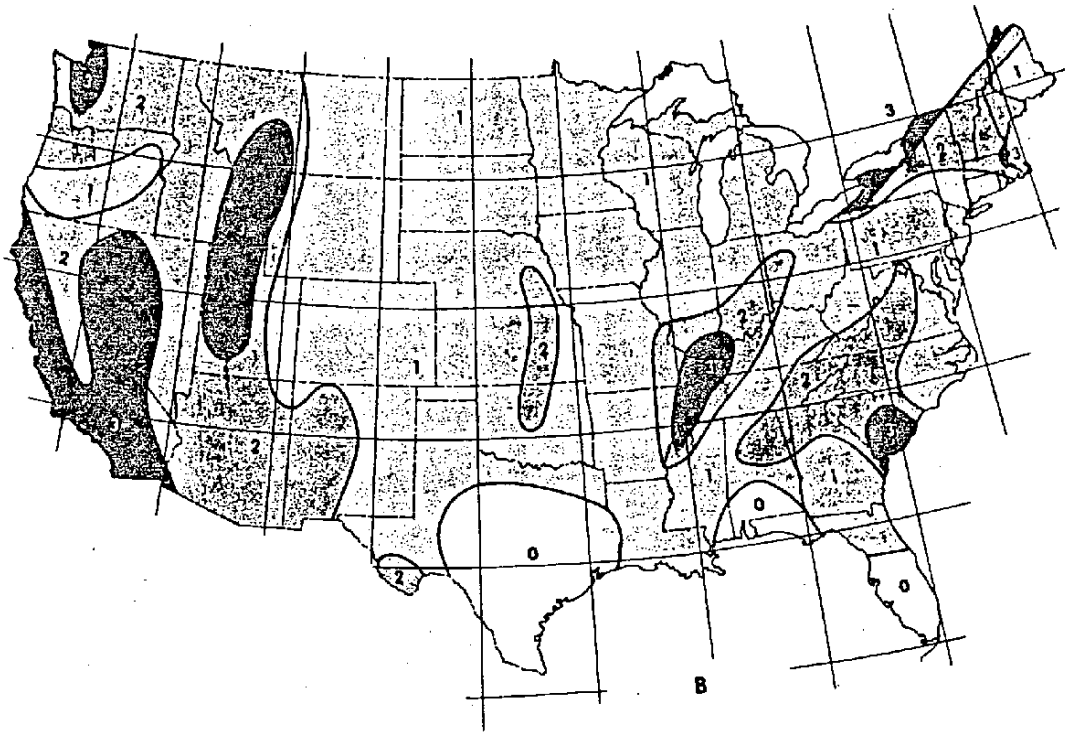


図２－２　米国の地震危険分布図

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。

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。

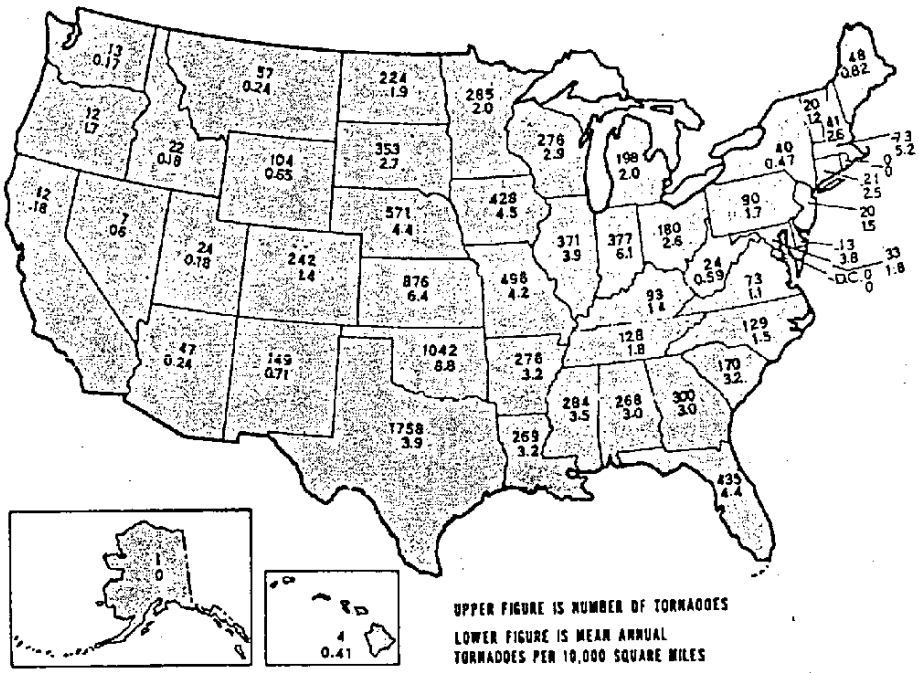


図２－３　州別の大型竜巻発生件数（１９５３～１９６９年）

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。

3. 補助設備

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。

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。

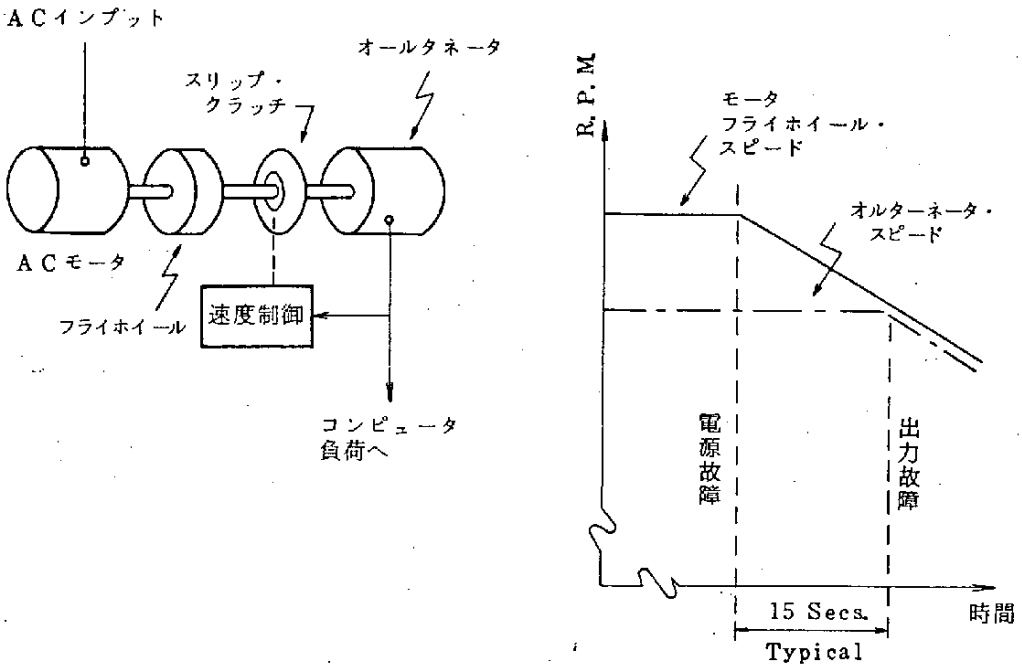


図３－１フライホイール・エネルギー貯蔵装置付
代表的モータ・オールターネータ

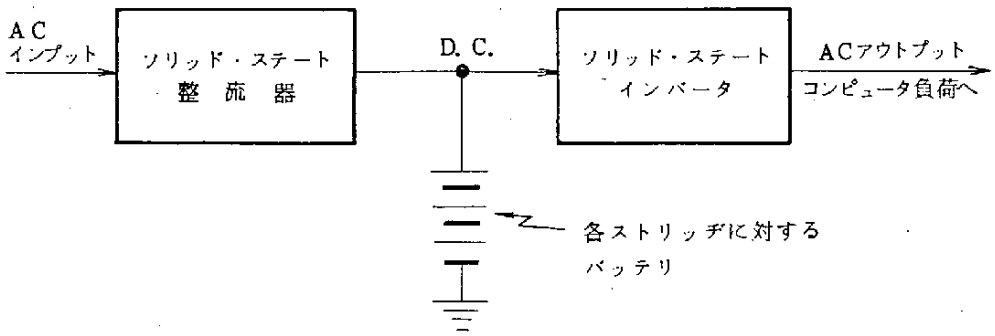


図３－２不断電源の単純化ブロック・ダイヤグラム

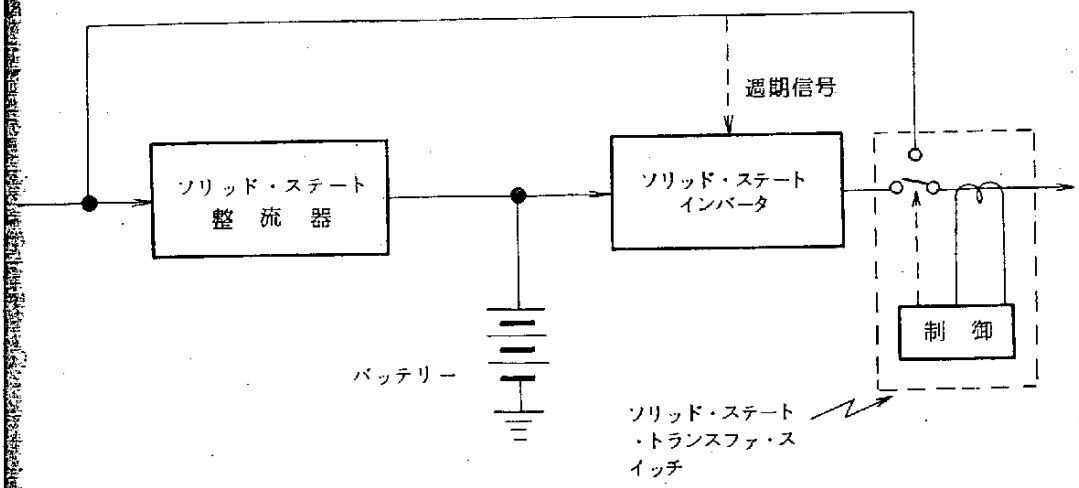


図３－３トランスファ・スイッチ付ＵＰＳ

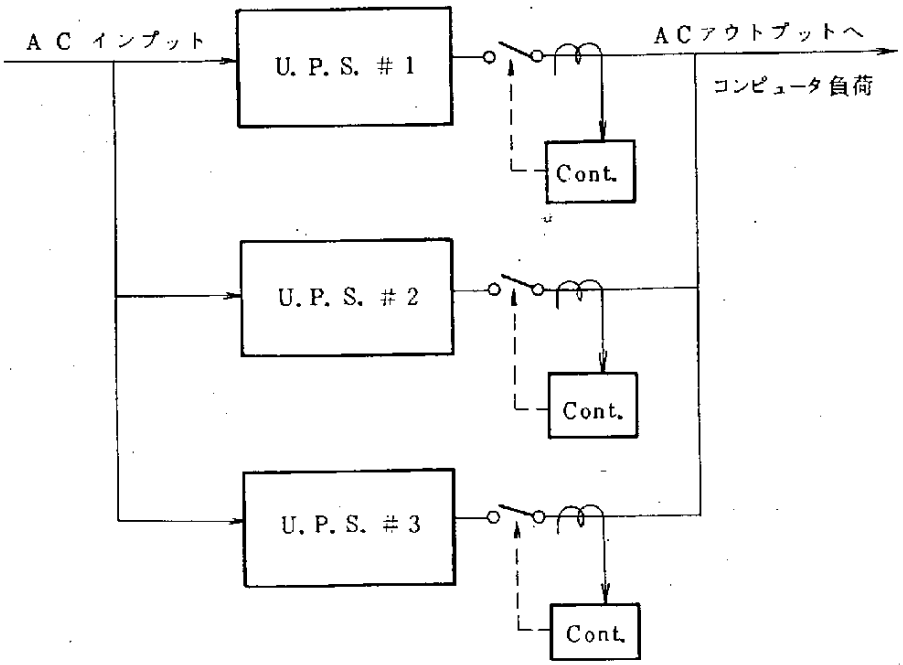


図３－４複合独立ＵＰＳ装置

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。

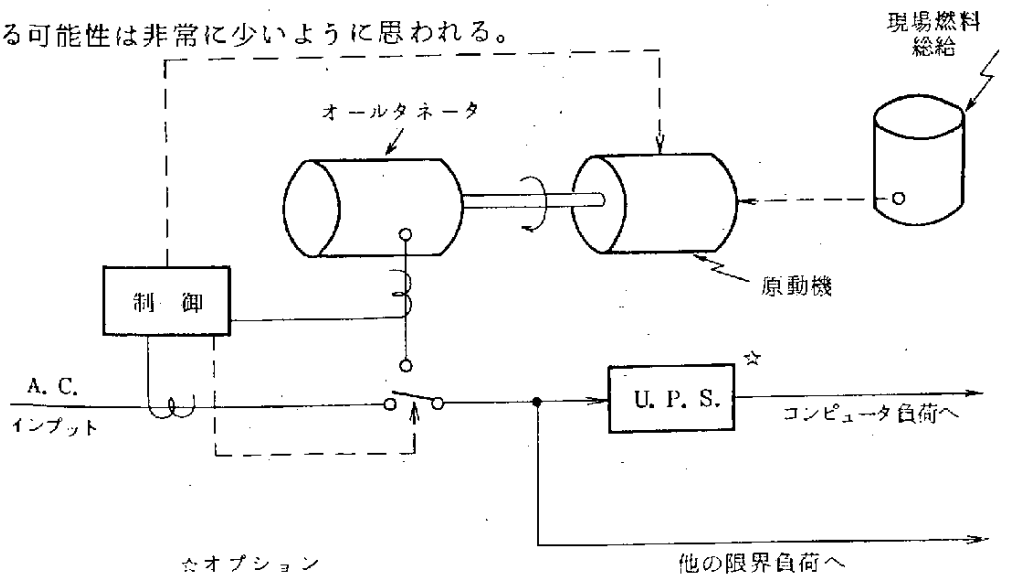


図３－５オンサイト・ジェネレーション付ＵＰＳ

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，通降変圧器，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。

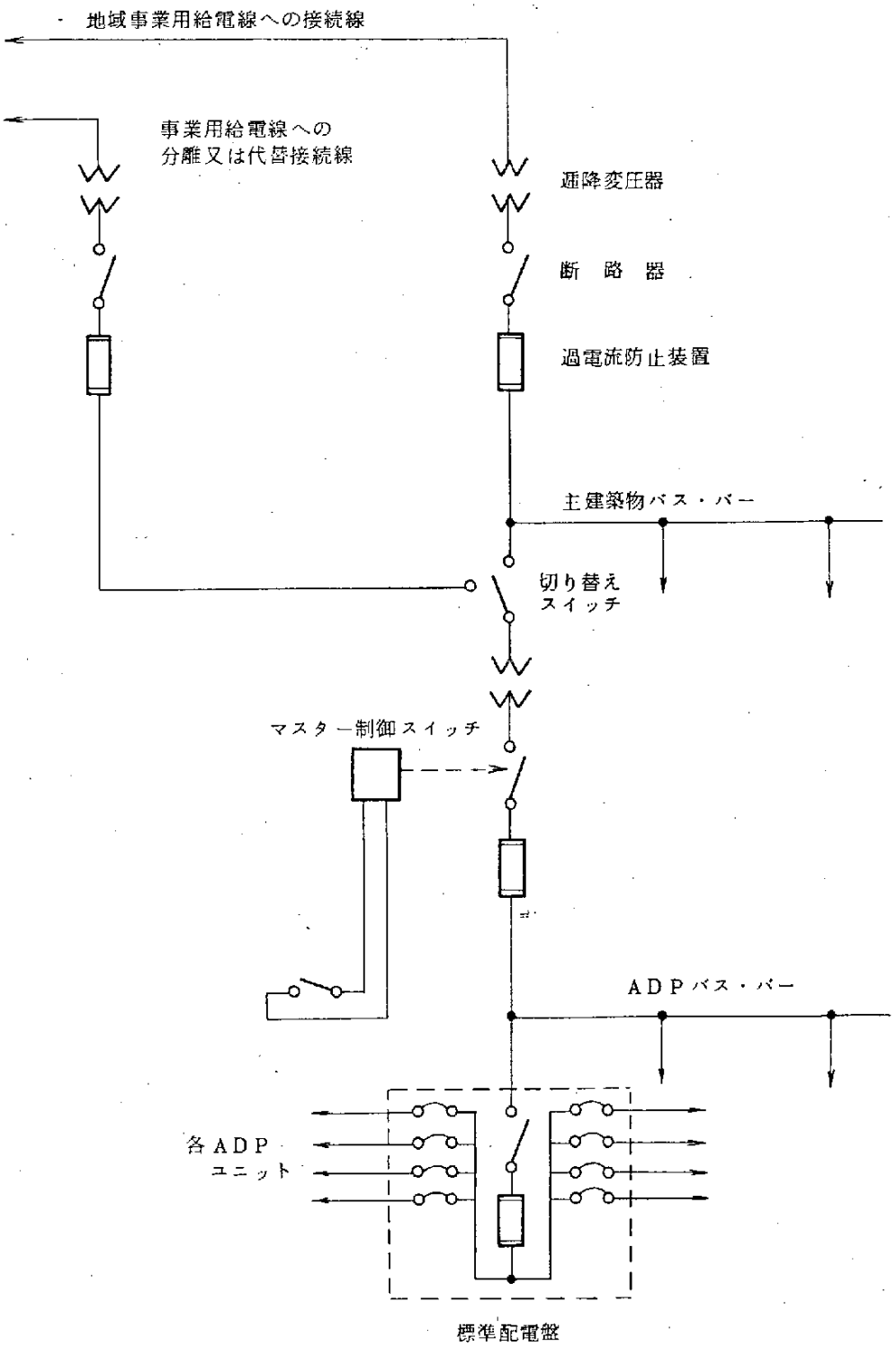


図３－６配電の概略ワン・ライン図表

(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。

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。

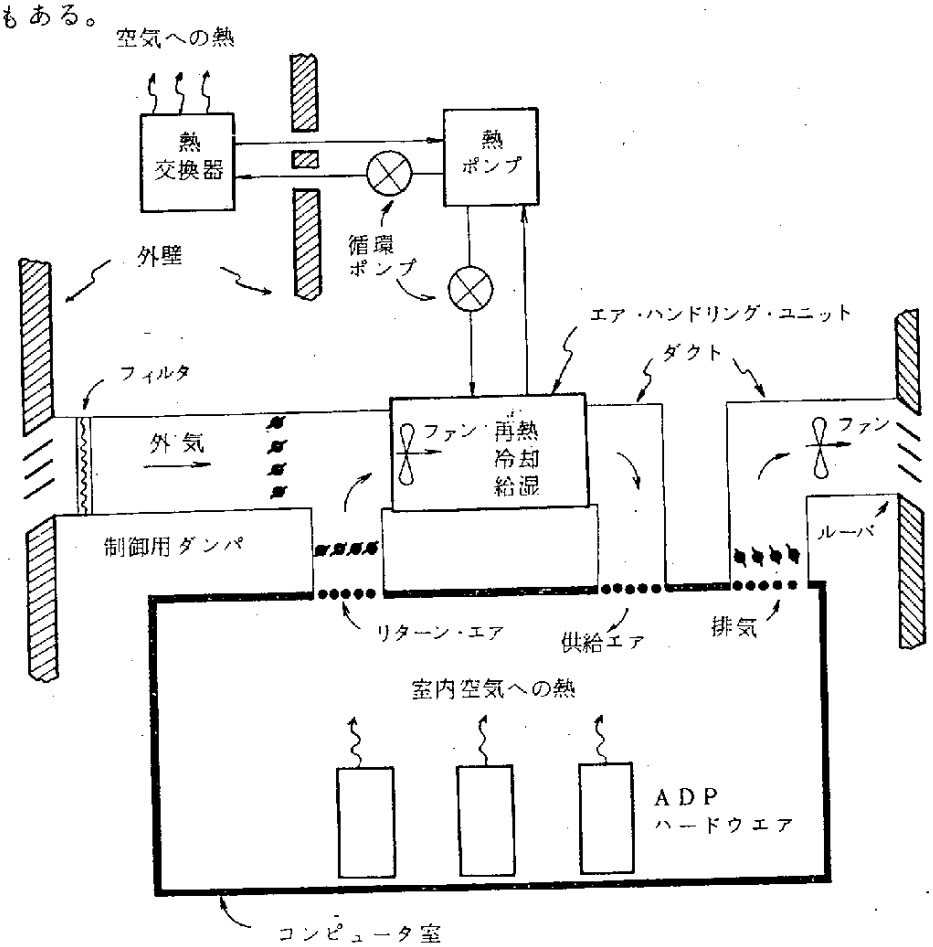


図３－７ 標準空調システムの概略横断面図

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	
AHU1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

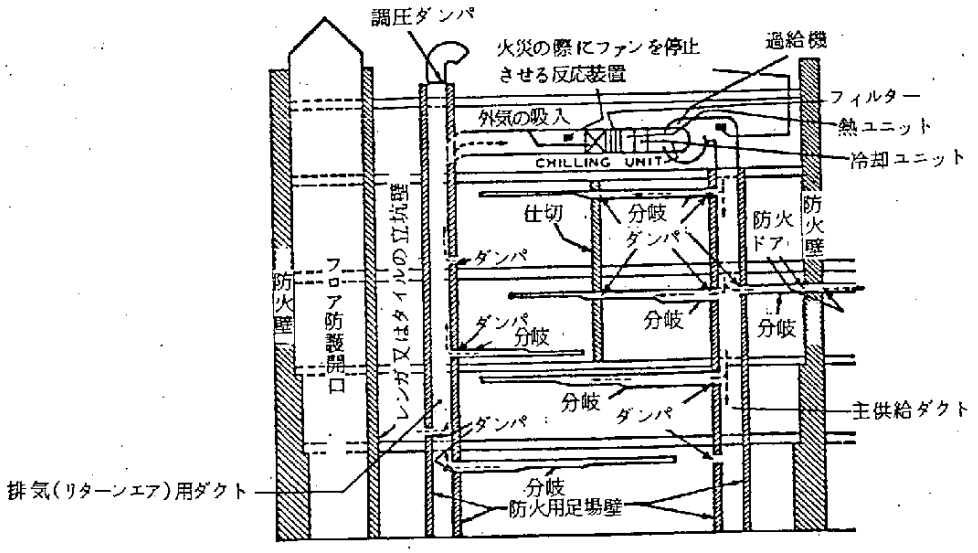


図３－８防火ビルの標準空調システム

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°C），50％ＲＨ，露点52～55°F（11～13°C）に維持され，冷却に使用される冷却水が，水温42°F（6°C）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。

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。

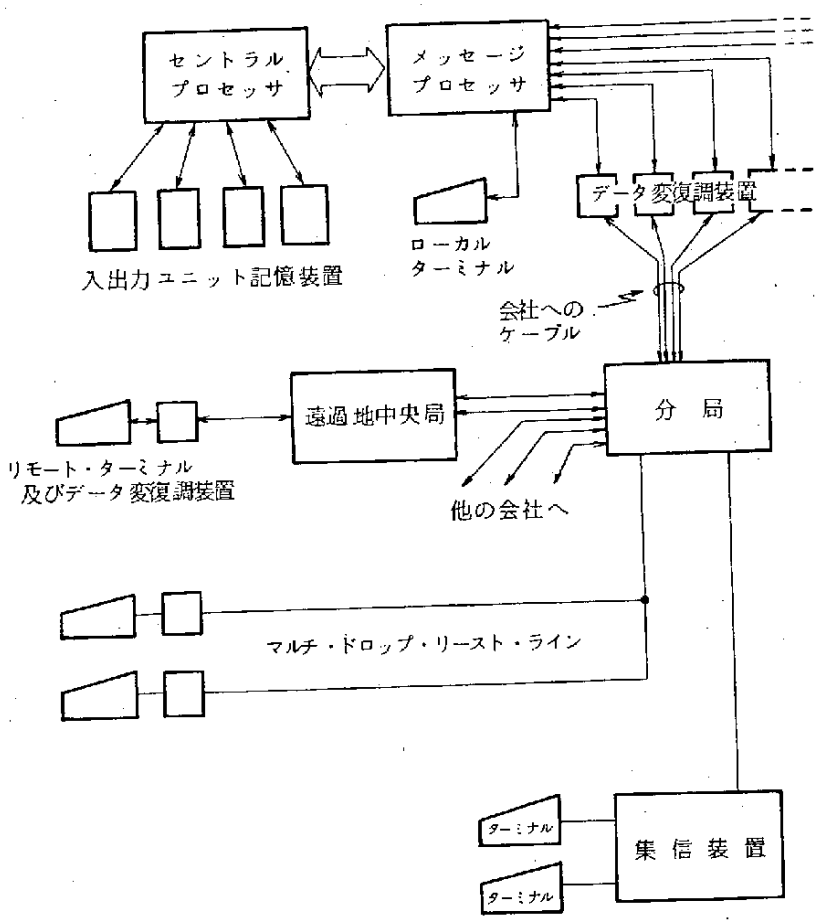


図 3-9　標準のテレプロセシング設備の配置

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，建設工事の堀削，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。

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. コンピュータ・システムの信頼性

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。

4.1 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。

4.2 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。

4.3　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。

5. ＡＤＰファシリティの物理的保護

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。

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。

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。

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。

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。

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。

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。

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㎝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。

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。

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。

6. 内部管理

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。

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。

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。

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。

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。

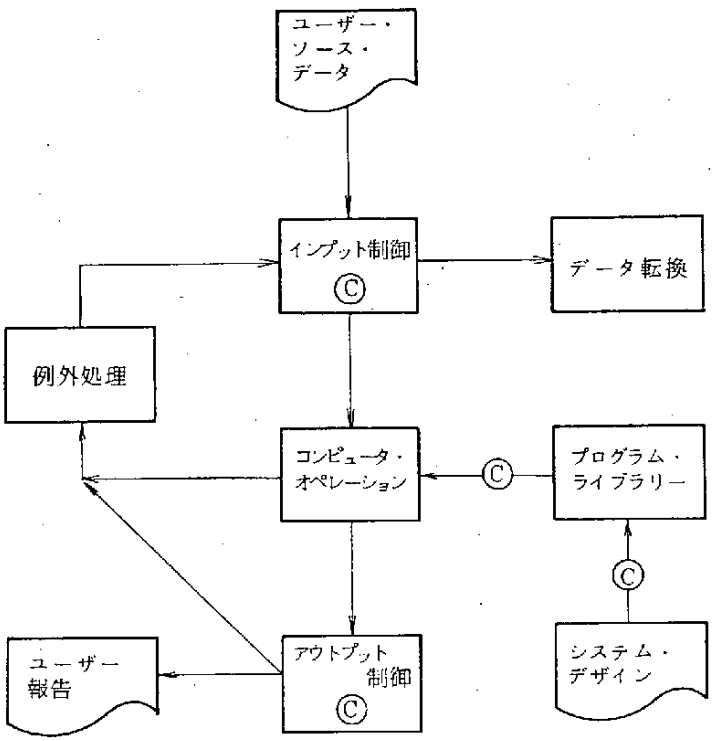
最後に，よき担当責任者はスタッフの各メンバーが割り当てられた任務を履行できるかどうか注意して見定めることである。無能力はいかなる作業状況でも許されるものではないが，ＡＤＰ関係においては結果がことさら判断を誤らせることがある。プログラムは間違った指示をいつまでも忠実に繰返すであろう。一瞬の不注意なオペレーションによってハードウェアが稼動すれば，ファイルを破壊することもある。また，間違ったテープを使う事は仕事を遅らせることがある。エラーや失敗は決して完全には除去できないので，担当責任者は個人を仕事に上手く調和させ，彼に必要な援助とトレーニングを与えるために最善の努力を払うよう自覚すべきであろう。

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**。

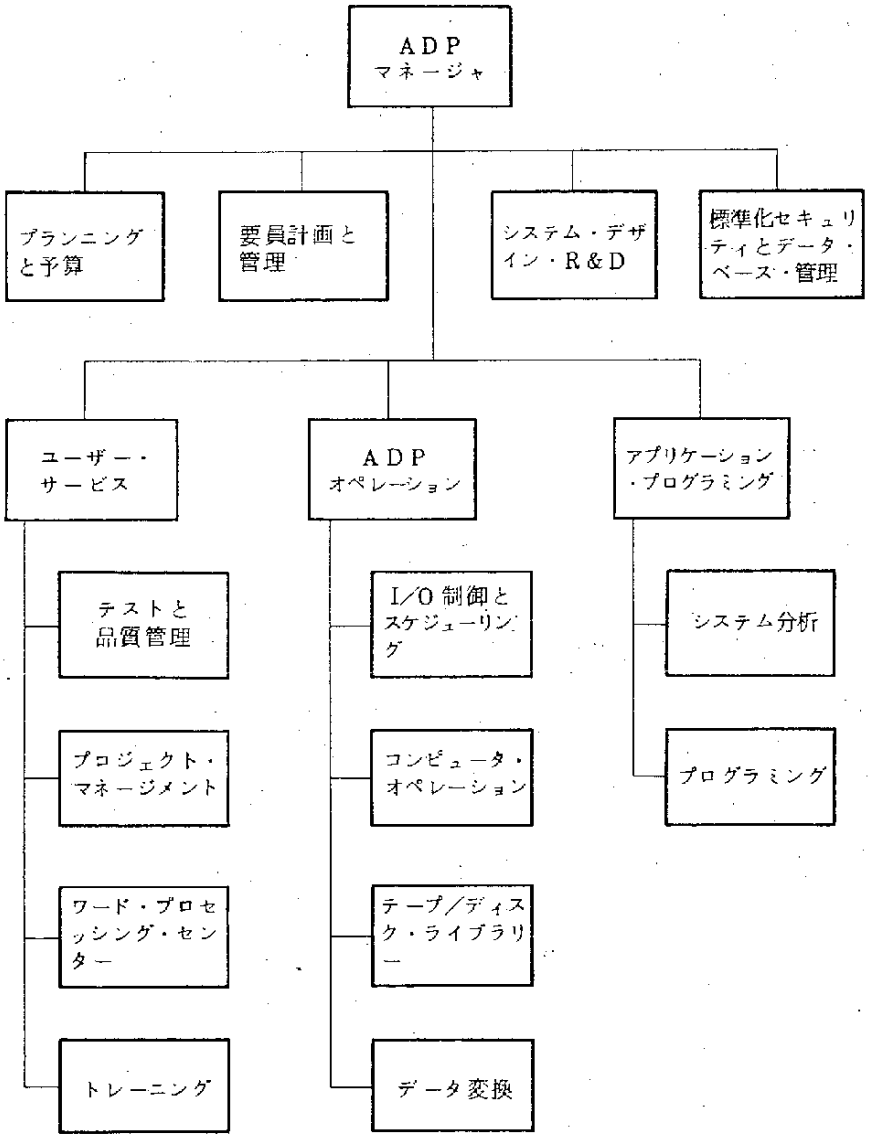


図 6－2　プロトタイプの組織図

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。

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。

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。

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。

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。

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。

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

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。

7. オフサイトＡＤＰ施設のセキュリティ

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。

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。

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。

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。

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。

8. 偶発事故対策計画

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。

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。

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

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。

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

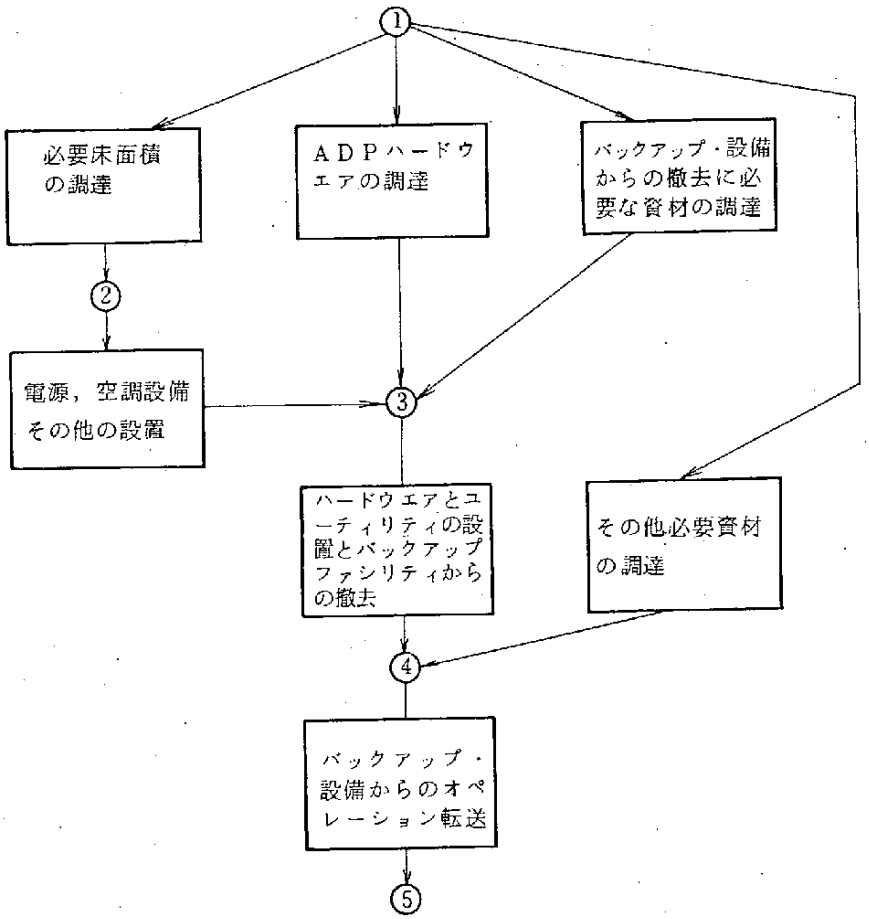


図８－３　ＡＤＰ設備復旧のPERTダイアグラム

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。

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。

9. セキュリティ意識とコミュニケーション

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。

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。

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。

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。

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。

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。

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。

10. 物理的安全性の内部監査

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。

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。

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　線塵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

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，卒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。

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

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, 32p.

[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.

第　2　部

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

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，オペレーションに出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。

1. まえがき

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。

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。

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。

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

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。

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

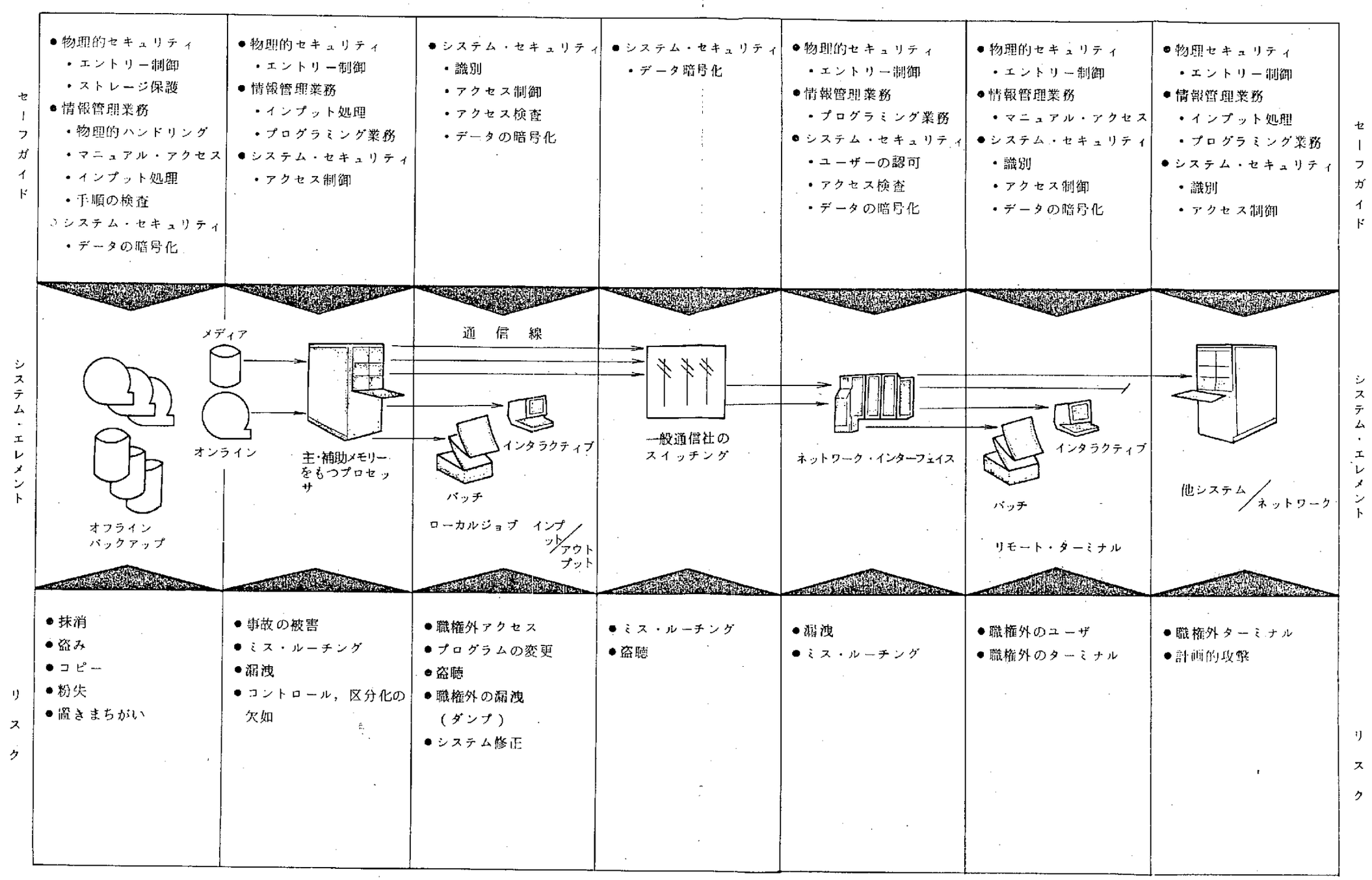


図 2－1　技術上のセーフガードと情報セキュリティ・リスク

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

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。

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。

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。

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。

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

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。

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。

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。

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。

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。

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。

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。

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。

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，当該ファイルが盗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。

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。

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。

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. 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。

5.1 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り，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。改善の方法は，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。

5.2 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。

5.3 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。

5.4 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 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。

5.5.1 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。

5.5.2　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。