

01 — R 005

# 21世紀へ飛躍するセキュリティ産業

## 2010年におけるセキュリティ産業市場

平成 2 年 3 月

**JIPOEC**

財団法人 日本情報処理開発協会



この報告書は、日本自転車振興会から競輪収益の一部である機械工業振興資金の補助を受けて、平成元年度に実施した「セキュリティに関する調査研究」の一環としてとりまとめられたものです。





## 序

当協会では、高度情報化社会に向けて、情報システムの脆弱性を克服するために、セキュリティの重要性を早くから指摘すると共に、その対策の研究に取り組んできた。一方、産業構造審議会（通商産業大臣の諮問機関）の情報産業部会が、昭和58年12月に提出した中間答申においては、今後政府が構すべき措置の1つとして「セキュリティ産業の振興」が提言されている。このような背景のもとに、当協会では、昭和61年度より、セキュリティ産業研究委員会を設置して調査研究を進めてきた。本プロジェクトでいうセキュリティ産業とは、セキュリティ対策のために利用される製品・装置あるいはサービス等を供給する事業の総称とした。しかし、その範囲があまりにも広く、全ての分野を取り上げることが難しいため、ここでは情報システムとそれに関連する分野に限定した。

本報告書は、4年間にわたって実施してきたセキュリティ産業に関する研究の成果をとりまとめたものである。とくに本年度は、2010年におけるセキュリティ産業の市場規模を予測してみた。かなり困難を伴う予測ではあったが、一応、セキュリティ産業の将来像を描いてみる事ができたと考えている。本報告書が、セキュリティ産業を健全に拡大し、豊かな情報化社会の構築に貢献し、かつ、セキュリティ対策やセキュリティサービスのあり方などを考えていく上で、役立つことを願ってやまない。

最後に、本研究を推進するにあたって、ご協力を賜った委員をはじめ関係各位に対して、心から感謝する次第である。

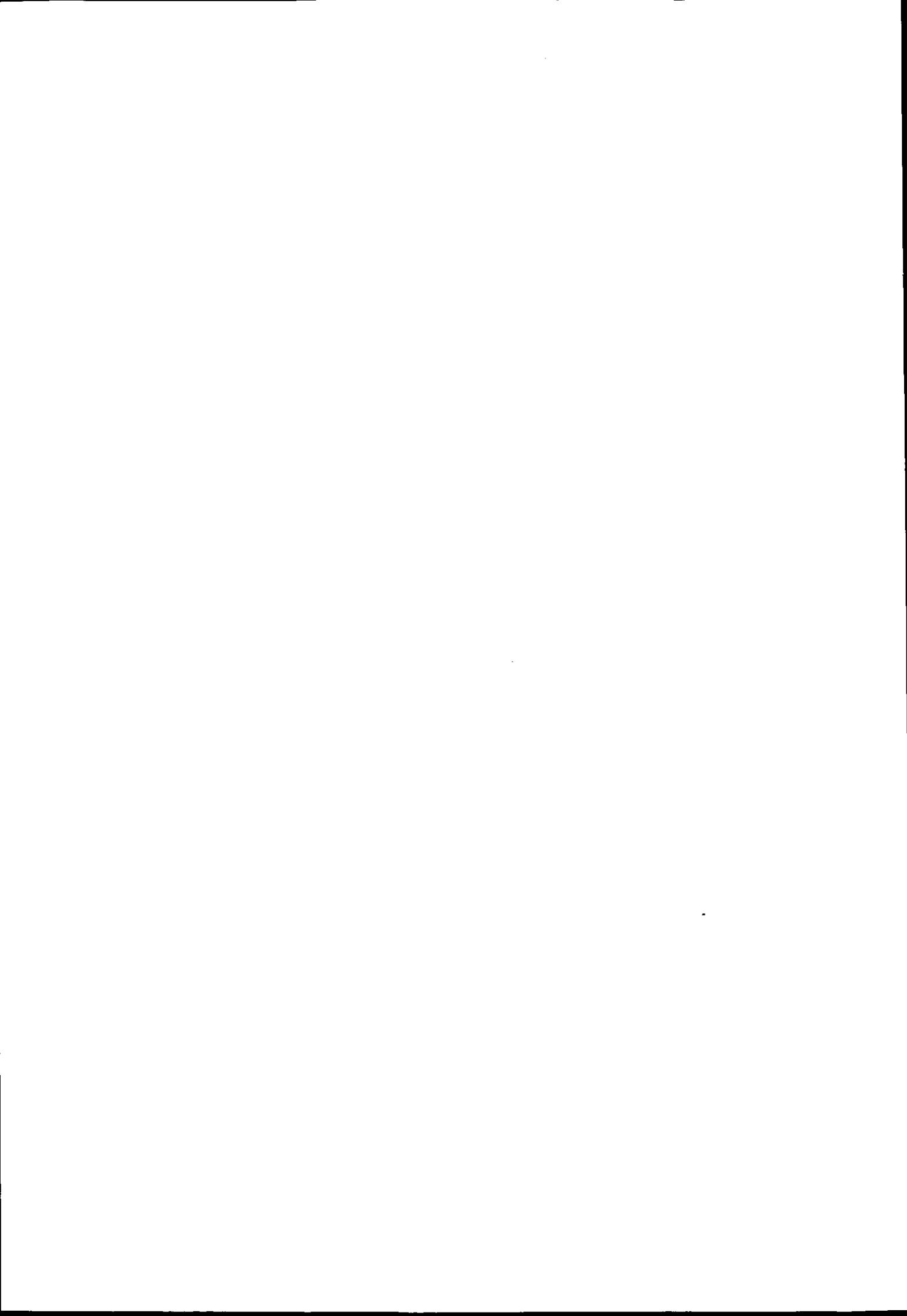
平成2年3月

財団法人 日本情報処理開発協会



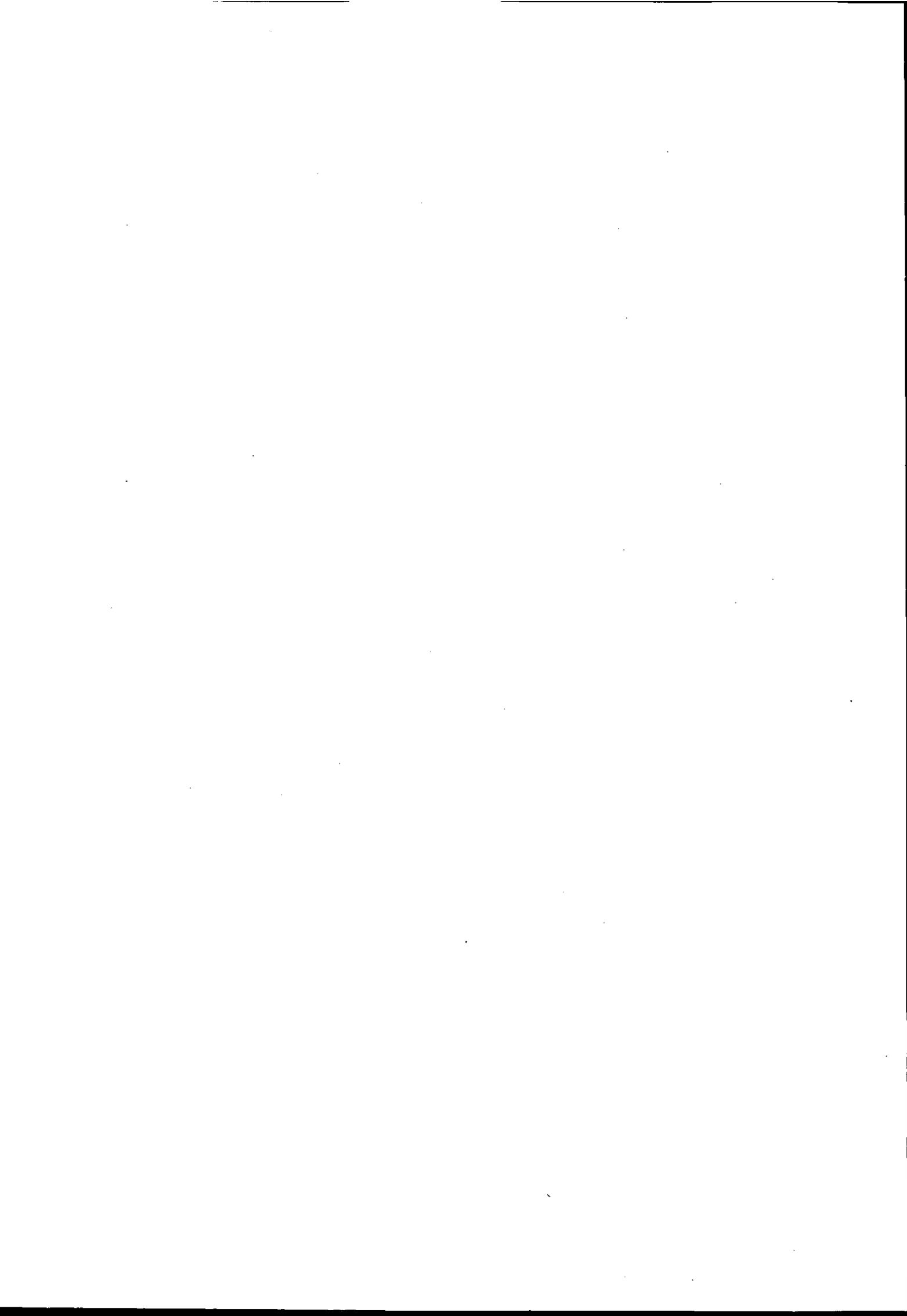
## セキュリティ産業研究委員会 委員名簿

委員長	安 保 二見男	日本コンピュータセキュリティ(株) 代表取締役社長
委員	北 村 巨	ビック情報機器(株) 代表取締役社長
	高 坂 毅	(財)機械電子検査検定協会 南関東事業所 コンピュータ・セキュリティ担当部長
	今 野 衛 司	日本アイ・ビー・エム(株) 産業技術渉外部長
	柴 田 正 和	日本電気フィールドサービス(株) 施設本部技術部長
	高 尾 典 生	(株)ワンビシアーカイブズ 取締役営業部長
	田 口 孝 弘	国際ファジィ工学研究所 常務理事
	田 中 正 憲	富士通(株) 情報システム事業本部企画部標準推進部 部長付
	研 井 堅	(株)熊平製作所 取締役技師長
	服 部 直	清水建設(株) 情報システム部 副部長
	深 井 寧	(株)電通 第9営業局 参事
	古 川 弘	新日鉄情報通信システム(株) 関東支社 技術部技術室長
	真 島 凱 汎	松下電工(株) 東京特機営業所長
	小 林 登	(財)日本情報処理開発協会 常務理事
専門委員	小河原 俊 二	セコム(株) 商品企画室長
	安 野 実	松下電工(株) 環境開発エンジニアリングセンター 課長



## 目 次

第1章 セキュリティ産業研究の経緯 .....	1
1. 研究活動のスタート .....	1
2. これまでの研究成果 .....	1
第2章 セキュリティの観点からみた2010年情報化社会の基本理念 .....	8
1. 2010年の情報化社会に対する視点 .....	8
2. セキュリティ産業の展望と課題 .....	9
第3章 2010年のセキュリティ産業市場の予測 .....	13
1. アクセスコントロール .....	16
2. 防災・防犯 .....	19
3. 非常用電源設備 .....	22
4. 監視 .....	28
5. 保管設備 .....	29
6. 暗号 .....	32
7. セキュリティ用ソフトウェア .....	38
8. バックアップサービス .....	40
9. ファシリティマネジメントサービス .....	44
10. 教育 .....	51
11. コンサルティング .....	53
12. 警備 .....	55
13. 保険 .....	58
14. コンピュータ専用ビル .....	61
15. 工事施行およびメンテナンス .....	63
第4章 生活の情報化とセキュリティ .....	69



## 第1章 セキュリティ産業研究の経緯

### 1. 1 研究活動のスタート

高度情報化社会を迎えて、社会の各分野において情報システムへの依存度がますます大きくなり、それにつれて、エラー、事故、犯罪等の発生による影響範囲も飛躍的に大きくなってきている。このような状況のなかで、セキュリティ対策の重要性が叫ばれているが、現実には、各企業においてセキュリティ対策の方針が確立できていない状態にある。当協会では、その理由の1つにセキュリティ産業の未成熟もあると判断している。すなわち、セキュリティ産業が確立していないために、どこに、どのようなセキュリティ製品が存在するのかすらわからない状態であるとすれば、ユーザのセキュリティ対策の選択の幅も小さくなり、ひいては情報化社会の脆弱性を抑制することがうまくいかないとの危惧もあった。

わが国において、セキュリティ産業が公式の場にて議論されたのは、昭和58年の産業構造審議会情報産業部会での審議においてが初めてである。同部会は、同年12月に中間答申を提出しているが、そのなかで、今後政府が構すべき措置の1つとして、「セキュリティ産業の振興」を提言している。その提言の内容はつぎのとおりである。

「コンピュータシステムの広範な普及とその社会・経済活動における重要性の高まりを背景に、コンピュータセキュリティに関連する種々の機器、サービスを提供するセキュリティ産業ともいえるべき産業が形成されつつある。このようなセキュリティ産業は、コンピュータールームに設置される消火設備、防犯設備等の開発、供給、重要データ等の保管サービス、さらにはバックアップセンターによる非常時のバックアップ機能の提供等を通じて、コンピュータシステム全般のセキュリティの向上に貢献している。

このため、政府としても、各コンピュータシステムにおけるセキュリティ対策が一層円滑に実施されるようセキュリティ産業を情報処理産業の一環として位置づけ、その育成・振興を図っていく必要がある。」

本研究プロジェクトは、この答申の趣旨に沿って、わが国におけるセキュリティ産業の概念、範囲を明確にし、高度情報化社会における当該産業の位置づけと社会的役割を明確にすることをその出発点とした。そして、このために、当協会内に関連各界を代表する専門家で構成する「セキュリティ産業研究委員会」を設置し、調査・研究をすすめてきたものである。

### 1. 2 これまでの研究成果

#### (1) 昭和61年度

昭和61年度は、セキュリティ産業のフレームワークづくりを行い、表1のとおり分類した。また、その分類に基づき情報システムを中心としたセキュリティ対策用の製品あるいはサービスにはどのようなものがあるかについてアンケート調査を実施した。その結果、従来の業種がセキュリティ産業のどのような分野へ進出しているのかが分かるなどの成果をあげることができた。

表1. セキュリティ産業の分類

	分 類	機 器 ・ 装 置 ・ 機 能 ( 例 示 )
機 器 ・ 装 置  (含 ソ フ ト ウ ェ ア)	1. アクセス・ コントロール (接近および 操作の制御)	識別(カード、カードリーダー、判別機器<本人確認用機器>等)
		開閉(ロック、シャッター)
		監視(在室検知等)
	2. 防災・防犯	火災(センサー、受信、報知)
		地震( " )
		漏水( " )
		侵入( " )
		消火
		避難器具
		非常照明
	3. 非常用電源設備	発電機
		バッテリー
		C V C F (Constant Voltage Constant Frequency)
		A V R (Auto Voltage Regulator)
	4. 監 視	サーベランスカメラ(防犯用写真カメラ)
		ビデオ(防犯用TVカメラ、ビデオ)
		遠隔監視制御装置(建物外での制御)
		ローカル監視制御装置(同一建物内での制御)
	5. 保管設備 (データ保管用)	保管庫
		金庫
6. 暗 号	暗号装置	
	暗号ソフトウェア	
7. セキュリティ用ソフトウェア	セキュリティソフト	
8. 通信回線	回線不正接続防止装置	
	回線アナライザー	
	ネットワーク管理装置	
	非常用移動通信装置(衛星通信地上局 等)	
9. バックアップ サービス	センタバックアップ	
	情報保管	
10. 教 育	教育・訓練	
11. コンサルティング	セキュリティ	
	システム監査	
12. 警 備	機械警備	
	常駐警備	
	輸送警備	
13. 保 険	損害保険	
	賠償責任保険	
14. 防災・防犯工事 施工および メンテナンス	防災・防犯工事施工およびメンテナンス	

## ①建設

建設業は、ビル管理の自動化、あるいはインテリジェントビルへの進出など、本来業務のエレクトロニクス化の進展がめざましいこと、ビルを建設するので当然セキュリティが重視されることなどを背景として、建物に関連すると思われる分野へはすべて進出している。この建設業のセキュリティ分野への進出における特徴は、当然のことながら「設計・施工」を中心としていることである。

## ②印刷

印刷業は、アクセスコントロール分野の、とくに識別分野、すなわちカード分野への進出、および一部は情報保管業務へ進出している企業もある。

## ③化学

化学工業は、範囲が非常に広いので一概に言えないが、セキュリティ産業への進出分野はアクセスコントロールの識別分野、防災・防犯の火災、地震、漏水、侵入、消火分野などである。

## ④非鉄金属・金属製品

この業界は、自社業務の延長線上で、それぞれ広汎な関連分野へ進出している。具体的にはつぎのとおりである。

- ・アクセスコントロール；開閉分野
- ・防災・防犯；火災、漏水、侵入、消火、避難器具、非常照明分野
- ・非常用電源設備；バッテリー、C V C F、A V R分野
- ・監視；サーベランスカメラ、ビデオ、遠隔監視制御装置、ローカル監視制御装置分野
- ・セキュリティ用ソフト；セキュリティソフトウェア分野
- ・通信回線；ネットワーク管理装置分野
- ・コンサルティング；セキュリティ分野
- ・警備；機械警備分野
- ・防災・防犯工事施工およびメンテナンス；この分野への進出の特徴は、製造 — 販売 — 設計・施工 — 保守までを扱うか、またはサービスまでも含めて扱うケースが多い。

## ⑤機械

機械工業は、アクセスコントロールの識別分野、警備の機械警備分野に進出している。

## ⑥電気機器

この業種もいろいろな企業が広範囲に進出しているが、1社ごとの進出分野は限られている。監視のサーベランスカメラ分野、バックアップサービスのセンタバックアップ分野、警備の輸送警備分野、保険分野などに進出している。

## ⑦精密機器

精密機器は、アクセスコントロールの識別分野、監視のサーベランスカメラおよびビデオ分野に進出しているが、これらは本来業務の範囲内であり、新規の進出ではない。

## ⑧商社

商社の中には、総合商社もあれば専門商社もある。現段階では、ごく限られた分野の製品を取り扱っているに過ぎない。

### ⑨損害保険

損害保険は、保険分野を扱っているだけで、他のセキュリティ産業分野へ新規に進出する傾向は見あたらない。

### ⑩不動産

不動産業は、非常用電源設備を中心とした保守に進出している。

### ⑪電力・ガス

電力は非常用電源設備のCVC分野、ガスは防災・防犯のうちの火災分野に進出している。また、ガスの場合は、ガス洩れ警報機の販売を行うなどの傾向もみられる。

### ⑫情報サービス

情報サービス業は、警備および保険を除く全ての分野に進出している。進出形態としては、サービス提供が非常に多く、次いで販売-設計・施工となっている。

### ⑬倉庫

倉庫業のセキュリティ産業への進出は限定されており、バックアップサービスとセキュリティコンサルティング分野である。これらは、従来の倉庫業から派生してきた新規分野と見ることができよう。

### ⑭金庫・保管庫

この業種は、関連分野への積極的な進出が目だっている。具体的には、つぎのような分野に進出している。

- ・アクセスコントロール；識別、開閉、監視分野
- ・防災・防犯；火災、地震、漏水、侵入、消火分野
- ・監視；サーベランスカメラ、ビデオ、遠隔監視制御装置、ローカル監視制御装置分野
- ・保管設備；保管庫、金庫分野
- ・防災・防犯工事施工およびメンテナンス分野

### ⑮警備

警備業そのものがセキュリティ産業の一角を形成するものであるが、大手企業は各分野へ広く進出している。

- ・アクセスコントロール；識別、開閉、監視分野
- ・防災・防犯；火災、漏水、侵入、消火分野
- ・非常用電源設備；バッテリー分野
- ・監視；サーベランスカメラ、ビデオ、遠隔監視制御装置、ローカル監視制御装置分野
- ・保管設備；金庫分野
- ・セキュリティ用ソフトウェア分野
- ・教育分野
- ・コンサルティング；セキュリティ、システム監査分野
- ・警備；機械警備、常駐警備、輸送警備分野
- ・保険；賠償責任保険分野
- ・防災・防犯工事施工およびメンテナンス分野

### ⑯会計事務所

大手の会計事務所では、システム監査部を設けているところが多く、システム監査コンサルティングおよびそれに関連する教育分野に進出している。

## (2) 昭和62年度

昭和62年度は、前年に引き続き、各セキュリティ産業分野ごとに実態把握のための追跡調査を行った。さらに、現状のままで家庭生活分野における情報化が進展した場合、将来においてセキュリティ上の問題点はないのかという面について検討を加えた。その結果、今のままでの状態では、いずれ大きな問題を引き起こす可能性があるとの結論を得た。すなわち、自動化による事故の恐れがあり生命・財産に影響を与えかねないこと、外部との接続が多くなった場合の事故の影響やプライバシー保護のあり方、新しいサービスについてのアセスメント等、基本的にセキュリティ対策のあり方について研究を行う必要性が強いことがわかった。この結果、これらを解決するための方法を研究し、望ましい「セキュリティプラン」を立案するために、新たに「ライフスプリング計画」(Lifespring: 家庭は生命の泉)を発足させた。

このライフスプリング計画の基本方針としては、つぎの5つの事項を重視して具体化を図ることとした。

- ・生活の情報化を高める
- ・生活のためのセキュリティシステムを構築する
- ・生活関連システムのセキュリティ対策を構築する
- ・現役引退後の生活を豊かにする
- ・情報化の弊害は情報化で克服する

そして、このような基本方針の実現のために、新たに次のような5大テーマを設定した。

- ①安全性指向; 安心して生活ができる
- ②健全性指向; 健康な生活ができる
- ③快適性指向; 住心地がいい
- ④利便性指向; 生活に便利である
- ⑤自由指向; 気楽に生活できる

以上のように、基本方針と5大テーマを設定したのち、ライフスプリング計画のコンセプトづくりに取り組んだ。(図1参照)

## (3) 昭和63年度

昭和63年度は、2010年における高度情報化社会を描写し、そこにおける主要セキュリティ産業の発展形態と問題点をとりまとめた。さらに、ライフスプリング計画についても、生活の情報化とセキュリティシステムという観点から内容を一步前進させた。

2010年の高度情報化社会については、現在すでに兆候の出ている変化もあるが、一般的には予測不可能な部分の方が多いものと思われる。そのような中で、社会環境の変化を想定するわけであるから困難も伴う。ここでは、とくにつぎの点は共通の認識として配慮するよう考慮した。

- ①全般的傾向
  - ・高齢化
  - ・国際化
  - ・ハイテク化
  - ・価値観の多様化

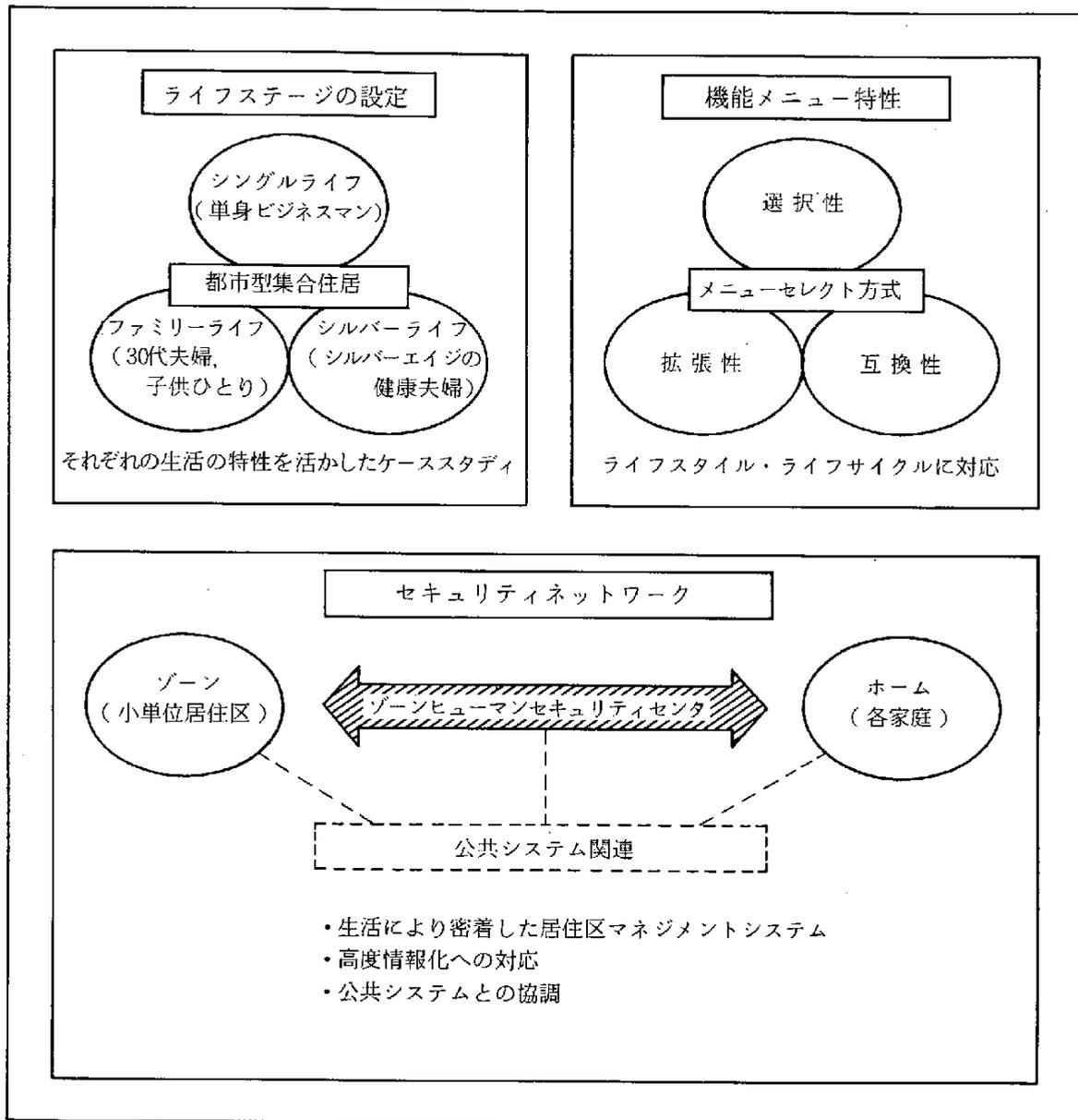


図1. ライフスプリング計画のコンセプト

## ②情報化の観点

- ・情報断絶の回避
- ・コンピュータ犯罪の防止
- ・人間性疎外の克服
- ・トータルセキュリティ対策

### (4) 平成元年度

平成元年度は、初年度にまとめたセキュリティ産業の分類に若干の検討を加えた。すなわち、通信回線分野は大変重要な分野ではあるが、実際にセキュリティ対策用として利用されている部分がどの程度であるかの推定なども非常に困難であることから、今回の分類からは外すこととした。しかし、バックアップ用の通信回線がセキュリティ対策用であることは間違いなく、今後も伸びていくであろうことも間違いのないであろう。すなわち、通信回線は、情報化社会のインフラストラクチャとして考え、個別のセキュリティ産業分野からはずしたものであり、軽視したということではない。

逆に、ここでは、新たに2つの分野を追加した。それは、ファシリティマネジメントとコンピュータ専用ビルである。これらは、独立した分野として把握可能であるし、将来的に伸びる分野と考えられるからである。

以上のようなことから、平成元年度は、従来セキュリティ産業分類を修正してつぎのような個別15分野とした。そして、これらの個別分野について、将来の市場規模を予測することとした。

- ・アクセスコントロール
- ・防災・防犯
- ・非常用電源設備
- ・監視
- ・保管設備
- ・暗号
- ・セキュリティ用ソフト
- ・バックアップサービス
- ・ファシリティマネジメントサービス
- ・教育
- ・コンサルティング
- ・警備
- ・保険
- ・コンピュータ専用ビル
- ・工事施工およびメンテナンス

## 第2章 セキュリティの観点からみた2010年情報化社会の基本理念

### 2. 1 2010年の情報化社会に対する視点

2010年のわが国経済社会を予測することは非常に難しいことである。しかしながら、情報化という観点からは、社会一企業一個人生活のあらゆる分野が情報化され、社会全体が情報システムにより運営されるように構造的な変化を来すという点では一致している。その結果、新しくセキュリティを売り物とするサービスが出現すると共に、各種のコントロールも情報システム自体により行われるようになる。したがって、エラー、事故、犯罪等が発生すると、これらの情報化構造に歪が出ることになる。しかも、ネットワークの拡大にともなって、エラー、事故、犯罪等の影響を及ぼす範囲はますます大きくなってきている。

このようなことから、2010年の情報化社会については、情報の保護、セキュリティ対策、あるいは最低限守らなければならない処理ルールなど、基本理念を明確にしておくことが求められる。そして、その主なものをあげるとつぎのようになる。

#### (1) セキュリティの基本理念の確立

国および企業における社会との融合を重視した情報化の基本理念が明確に把握できる状態になっていると思われるので、情報システムの目的、情報の性格、規模、ユーザ数等を勘案した上で、セキュリティ対策にも万全を期す必要がある。すなわち、情報化の基本理念に基づいたセキュリティの基本理念を明確にして、セキュリティ対策の全体的な枠組みをつくり、それに基づいて、具体的なセキュリティ構造を構築していかなければならない。その場合、社会全体の枠組みで考え、社会との融合を重視しなければならない。

#### (2) 情報化行動規範の確立

これからの情報化社会は、その構造あるいは体系自体が今日とは一変してしまうため、企業の行動規範あるいはコンピュータ要員等の行動規範を早急に確立する必要がある。このことにより、企業による情報公害の発生とその影響を未然に防止することが可能になる。また、コンピュータ要員について言えば、行動規範の存在により、やってよいこと、やってはならないこと、やらねばならないこと等の基準が明確になり、コンピュータ犯罪等の抑制にも役立つものと思われる。

#### (3) セキュリティ関連教育の振興

情報システムを開発し、運用するのが人間である以上、情報化に関する教育が重視されるのは当然のことである。とくに、現在欠落しているセキュリティ教育やシステム監査教育について早急に検討する必要がある。たとえば、今日のコンピュータ教育が、利用の側面のみを片寄りがちである点を、コンピュータ教育の開始とともにセキュリティ教育も実施するように改める必要がある。また、システム監査教育については、その裾野を広げる意味からも、大学教育過程に組み込んだ教育が必要である。そして、これらの地道な活動が、コンピュータ要員のレベルの向上に役立ち、ひいては事故や犯罪を抑制する早道にもなる。

#### (4) 情報管理・機密保護の徹底

情報の氾濫は、善意であるか故意であるかに係わらず、一步間違えば誤情報を与えてしまう危険性を持っている。それが、個人情報である場合には、プライバシーの侵害と言うことになる。情報化社会においては、情報が人を傷つけるという考え方をもち、十分に対策を施す必要がある。

#### (5) セキュリティ対策責任者の設置

情報システムは、それぞれの目的に応じたセキュリティ対策が準備されねばならないが、そのシステムに異常が発生したような場合に、どのような対処が可能であり、影響範囲をどこで喰い止めうるか等を十分研究しなければならない。システム設置者は、人手による対応策を含むトータルなセキュリティ対策を確立しておく必要がある。

#### (6) コーディネータ職の設置

情報システム部門においては、従来になく業務が複雑になってきている。したがってSEやプログラマなどの従来の職種に加え、ゼネラリストとしてのコーディネータを養成して、常に大所高所から情報システムを監視させると共に、システム上、あるいは社会的側面との調整などの問題を多面的に解決していく担当者を置く必要がある。

#### (7) システム監査の実施

情報システムの脆弱性を発見し、取り除くためには、システム監査の実施が不可欠である。システム監査は、2010年においては情報化社会の基盤的条件として、すべてのユーザで実施されることが望まれる。もし、企業内にシステム監査人が得られない場合には、外部のシステム監査コンサルタントを利用して実施すべきである。

#### (8) 多国間による調整

今日、すでに情報流通において国境はない。したがって、エラー、事故、犯罪、プライバシー侵害等の対策については、一国のみの対策では限界があり、関係各国がそれぞれ同じレベルの対策を施す必要がある。セキュリティでは、どこかレベルの低いところがあると、そこで問題が発生し全体に影響を及ぼすので全体のレベルを向上させなければならない。すべての国がネットワークで結合されている状況においては、これはもはや避けて通れない問題である。具体的には、セキュリティに関する各種基準、ガイドライン、法律などで、多国間調整の必要性が出てきている。

### 2. 2 セキュリティ産業の展望と課題

セキュリティは、2010年における情報化社会の基盤的要件の1つである点については誰も異論がないであろう。この2010年におけるセキュリティに関する重要性の差が、今日と20年後の最も大きな相違点であるとも言える。そこで、このような時代においては、セキュリティ産業が発展しなければ、ユーザのセキュリティ対策も選択の幅がせまくなり、情報システムにうまく合致した対策を構築することが困難になる。そうなれば、情報化社会の健全化が阻害されることにもなる。そこで、将来の情報化社会の健全化・安定化のためにますます重要になることが明白なセキュリティ産業について、今からその育成・振興を計画的に進めていく必要があり、必要性が認め

られる場合は、積極的に財政投融资や優遇税制などの助成策を講じるべきである。そして、21世紀には、セキュリティ産業が確固たる地位を築いている必要がある。その際、ユーザにおいては、セキュリティ方針を確立しておくことが求められる。そのもとで、具体的なセキュリティ構造を構築していかなければならない。その場合の基本は、たとえどのような形態の組織体であっても社会との融合を考慮しなければならないことであろう。

#### (1) アクセスコントロール

アクセスコントロールは、今後、身体的な特徴を利用した生物学的な方式が増加するものと思われる。技術的には、現在わが国では実用化されていない音声式や署名式も一般化しているものと思われる。この分野の市場規模は、米国の10分の1ないしは20分の1程度と推定され、現状はあまりにも小さい。積極的な技術開発の支援と、導入促進の支援とが求められる。

#### (2) 防災・防犯

コンピュータセンタにおいては、消火剤としてハロン1301が多く使用されている。地球環境汚染の観点からは、ハロンもフロンと同様にオゾン層を破壊する作用を持つことから、一刻も早く代替物質を開発しなければならない。これが、この分野において解決しなければならない大きな問題である。

#### (3) 非常用電源設備

バックアップ用の電源として利用できる燃料電池の実用化が望まれる。技術開発を支援するための具体的なプロジェクトの発足が待たれる。

#### (4) 監視

監視・確認用の機器あるいは装置としては、CCTV、防犯カメラ、画像付ドアホンなどがある。これらの監視装置は、特定分野ではかなり普及しているものの、全般的にはまだまだといった感がある。これらの装置については、今後、質的な向上を図ると共に、積極的に普及をはかることが望ましい。

#### (5) 保管設備

情報の保管については、検索の即時性が求められている。したがって、将来的には、大容量高速通信によるオンライン情報保管が主流になる可能性がある。また、可視情報の不可視化による保管は、スペースの有効利用上のみならず、セキュリティ上もきわめて効果的な方法であるため、法定保存期限をもつ情報についても、磁気記録等による保管を認めるようにすべきである。

#### (6) 暗号

すでに、暗号やメッセージ認証などの基礎技術は確立されつつあるが、実用的な観点からの応用研究が立ち後れている。産・官・学による応用研究を行うとともに、実用的、かつ安価な本人確認技術の開発が求められている。

(7) セキュリティ用ソフトウェア

情報システムを直接的に保護するための方法として、セキュリティソフトウェアの採用がある。とくに、コンピュータ犯罪の防止に有効であることから、中規模以上の情報システムでは採用することが望ましい。あるいは、将来的にはシステムの基本的な機能として、セキュリティ対策の義務づけ等も検討しなければならない可能性が強い。

(8) バックアップサービス

将来は、オンラインによるバックアップサービスが主流になる可能性があるが、ビジネスとしては、1システムで複数のシステムをバックアップしなければコスト的に高くなりすぎる面がある。また、複数システムをバックアップするためには、互換性という問題も出てくるであろう。これについては、OSIをはじめとする標準化の進展に期待したい。わが国のバックアップサービス企業は、現在一社のみであるが、日本進出を決めている米国企業もすでにあり、今後の展開が注目される状況になってきている。

(9) ファシリティマネジメント (FM) サービス

FMサービスは、オペレーション中心の運用管理サービスから、システムインテグレーション (SI) の方向へ動くという見方が出てきている。すなわち、FMサービスが総合化・多様化する可能性を持っているということになる。しかも、情報関連産業の各分野から企業が進出してきている可能性がある。それらの中で、システム等管理運営サービスは、直接セキュリティと関連してくる。このFMサービスは、2010年頃には情報システム運営に係るセキュリティサービスそのものへと変身している可能性がある。

(10) 教育

これからの情報化社会においては、セキュリティやシステム監査が一般ビジネスマンの基礎教育に加えらる必要がある。それが、セキュリティの観点からの情報化社会の土台づくりという意味を持つことになる。したがって、学校・企業等において、情報セキュリティ、システム監査などの教育を普及させる必要性が高まってきている。

(11) コンサルティング

セキュリティコンサルティングおよびシステム監査コンサルティングは、21世紀には情報システムを外部からささえる専門家集団としての地位を固めるであろうと思われる。

また、わが国では、現在、コンサルティングに依拠していても、それが無償サービスとして受け止められるケースが多いがいずれ対価を支払う慣習が根づいていくものと思われる。

(12) 警備

警備にはいろいろな形態があるが、その中でセキュリティ産業という視点から重視しているのは、情報システムとネットワークを駆使した機械警備といわれる分野である。この分野では、これらの装置を活用した新しいセキュリティサービスの出現も期待される場所である。すなわち、すでにネットワークで企業や家庭と接続されている有利さを利用して、その延長線上で顧客と密着した各種サービスが幅を広げていくものと思われる。

### (13) 保 険

情報システムが重要になればなるほど、万一、システムに不具合が生じた場合の対策が重要になる。それでも、なお危険性をゼロにすることはできない。そこで、そのような事態に備えて、一時的に多額のコスト負担を強いられることを緩和するため、保険の役割が重要になる。

現在、情報分野を専門とした保険には、情報化保険がある。情報化の進展が早く、情報化環境の変化が激しいことから、この保険の改訂、あるいは新保険の開発等、新しい動きも出てきている。

### (14) コンピュータ専用ビル

コンピュータ専用ビルは、構造、設備等において高信頼性・高安全性を実現した賃貸ビルである。情報システムが業務処理の中核をなすようになるにつれて、スペース確保およびセキュリティの観点からコンピュータセンタを別に建設する傾向が強いが、それがコスト的に不可能な企業も多い。そのような企業には、コンピュータ専用ビルへの入居という代替手段が可能になっているので、今後の需要の伸びは相当に大きいとみることができよう。したがって、コンピュータ専用ビルに対する基準の設定が必要であり、さらに事故処理のルール確立、補償問題などを解決しておかなければならない。

### (15) 工事施工およびメンテナンス

情報システムの高信頼性・高安全性を保証するための、施設に装備されるセキュリティシステムをめぐる設計・施工およびメンテナンスの金額も巨額になってきている。一方では、技術者の質的レベルを確保するためのスキルアップおよび維持の解決策を検討しなければならない。

### 第3章 2010年のセキュリティ産業市場の予測

これまでの実績を踏まえて、セキュリティ産業の各分野における現状の市場規模を把握し、それを基に、2010年の市場規模を予測した。しかしながら、各分野は、それぞれ異なる歴史を持ち、異なる発展形態を示してきているため、同一の予測方法を当てはめることが不可能である。

2010年におけるセキュリティ産業の市場規模を予測するに当たって、ここで共通認識として定めたことは、コンピュータの稼働金額の伸び率を年率10%としたことのみである。ただし、この数字は、予測のために各分野で必ず使用したというものではなく、使用する場合は10%とするという意味であるが、成長率の予測に影響を与えていないとは言えない。

この前提条件については、人により、立場により、異なる意見があろうことは十分考えられる。そのような向きは、現在の市場規模に自らの予測値を作成して計算してみるのも1つの方法であろう。

これ以外の要因については、市場の成熟度や成長率などが各分野によってまちまちなことを配慮して、予測もその分野特有の各種制約条件を個々に検討する方法をとった。また、分野によっては、現在まだ市場が明確に確立していないものがあるし、現時点における単独商品の中には、将来は他の商品に組み込まれてしまうと思われるものがあることも事実である。予測のために使用する各種数値、推定方法などについても、分野ともかなりの困難をとめない、完璧な予測ができたものとは考えていない。現段階で出きる限りの努力をしたということである。

以上のようなことから予測した結果は、以降に述べるとおりであるが、セキュリティ産業の成長率や、2010年の市場規模の予測等を要約すると、表2、3のとおりである。この表の中で、「現在」とあるのは、厳密に1990年をさすものではなく、現時点で把握できる数字を基礎としている。

また、各分野は、それぞれ独自に予測したものであるため、他の関連分野と重複する部分があることも考えられる。しかし、ここでは、重複部分を削除することはしていない。

表2. 2010年までの産業別市場規模伸び率予測

セキュリティ産業分類	市場推定 (成長率等)
1. アクセスコントロール	年率15%
2. 防災・防犯	今後10年間年率15% その後年率10%
3. 非常用電源設備	今後5年間年率20% その後年率10%
4. 監視	年率15%
5. 保管設備	今後10年間年率20% その後年率10%
6. 暗号	センタ型は2010年の暗号実装率 100% 端末型は5年後から複合端末で暗号実装率50%
7. セキュリティ用ソフトウェア	年率14%
8. バックアップサービス	今後10年間は大中型コンピュータの設置台数の80% その後年率10%
9. ファシリティマネジメントサービス	今後10年間年率13% その後システム等管理運営サービスについては年率10%
10. 教育	今後10年間年率15% その後年率30%
11. コンサルティング	今後10年間年率10% その後年率30%
12. 警備	年率10%
13. 保険	今後10年間年率13% その後年率10%
14. コンピュータ専用ビル	賃貸面積の予測から算出
15. 工事施工およびメンテナンス	工事費から予測

表3. 2010年のセキュリティ産業予測

セキュリティ産業分類	現 在	2010年	倍 率	対 象 ・ 範 囲 等
1. アクセスコントロール	(億円) 150	(億円) 2,450	16.5	識別方式
2. 防災・防犯	1,790	21,000	12	自動火災報知設備、ハロン消火設備、 および同保守 防犯機器
3. 非常用電源設備	700	8,700	12.5	発電機、バッテリー、CVCF、AVR
4. 監 視	1,000	16,400	16.5	CCTV、防災カメラ
5. 保 管 設 備	65	1,000	15.5	情報の保管
6. 暗 号	5 (市場未確立)	4,500	900	暗号装置 メッセージ認証装置
7. セキュリティ用ソフトウェア	700	14,100	20	リソースアクセスコントロール用ソフト
8. バックアップサービス	10	2,400	240	大型・中型ユーザ
9. ファンリティマネジメント サ ー ビ ス	3,447	19,000	5.5	システム運用委託、設備管理等運用 保守サービス
10. 教 育	5	300	60	セキュリティ教育 システム監査教育
11. コンサルティング	30	1,000	36.5	セキュリティコンサルティング システム監査コンサルティング
12. 警 備	2,184	17,800	8	機械警備
13. 保 険	567	3,800	6.5	コンピュータ関連の火災保険、 動産総合保険、情報化保険
14. コンピュータ専用ビル	130	2,200	17	賃貸料
15. 工事施工および メンテナンス	8,100	75,500	9	各種施設の建設工事における専用セキ ュリティ対策工事費
合 計	18,883	190,150	10	

## 1. アクセスコントロール

### 1. 1 アクセスコントロールの基本的な考え方

アクセスコントロールには、次の3つの側面がある。

第1は、セキュリティエリアなどの保護対象区域への出入りの資格を認められた人物を識別し、記録し、出入口の開閉を行い、資格のある人は入退室をさせ、資格のない人は入室を禁止するという人の動作やドア開閉を伴う物理的な入退出管理面。

第2は、端末機を通じてのホストコンピュータへのアクセス者を識別し、その資格のない者には、システム本体に蓄えられたデータを読んだり、利用したりすることができないように制御する入力・操作管理面。

そして第3は、ネットワークシステムへのアクセス者を識別して、不正な侵入からシステム本体を防御しようとするものである。

### 1. 2 アクセスコントロールの基本構成

アクセスコントロールシステムは、図2に示すとおり、基本的に識別システム、入出力システム、動作システムから構成される。

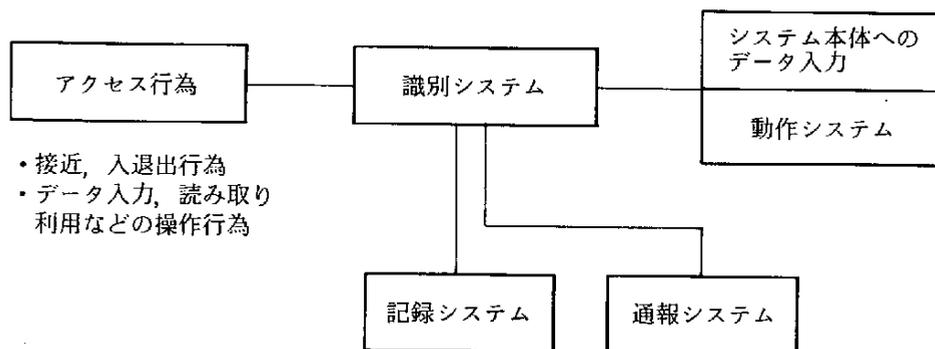


図2. アクセスコントロールシステム

- 識別システムは、アクセスコントロールシステムの頭脳部で、アクセス行為の識別とそのデータの送受を行う。そのシステムは日進月歩で、種々製品化されている。それらは大別すれば、人の携帯物によって識別するシステムと人の身体上の特徴によって識別するシステムとがある。
- 記録システムは、識別システムからのデータを受け、アクセス者、場所、年月日時刻などを記録し、出力する。
- 通報システムは、識別システムからのデータを受けて、必要な所に通報する。
- システム本体へのデータ入力（接続）は、識別システムからのデータをシステム本体にパスワードなどと併用して入力（接続）する。
- 動作システムは、識別システムからのデータを受けて、主として電気錠、自動ドア、自動シ

ャッターを動作させ、出入口の開閉を管理する。

### 1. 3 アクセスコントロールの範囲

以上のように、アクセスコントロールといっても多岐にわたる。しかし、ここで対象とするアクセスコントロールは、金額による把握が可能な識別分野とし、識別方法もカードなどの携帯物による方式と生物学的な方式になるものに限定する。

携帯物による方式としては、次のようなものがある。

- ① 磁気ストライプカード：キャッシュカードなどに使われている方式
- ② 磁気スポットカード：磁気をスポットで配列しておき、その配列のパターンを登録しておく方式
- ③ パッシブ（電波）カード：受信機能を持ったカードで、特定の電磁波にのみ反応する。
- ④ アクティブ（電波）カード：発信機能を持ったカードで、特定の電磁波を発信する方式
- ⑤ ウィガンドカード：カード内にスチールのワイヤを平行に複数本埋め込み、その長さの配列の仕方を登録しておく方式

また、生物学的（Biometric）による方式としては、身体的な特徴を利用するもので、掌形式、指紋式、網膜式、音声式、および署名式などがある。しかし、音声式と署名式は、わが国ではまだ一般的に利用されていない。

### 1. 4 米国の市場規模

わが国の市場規模を予測するうえでは、米国を参考にするのがよい。米国の状況は、一般論としては日本の市場規模の10～20倍であろうという見方がある。米国における各識別方式のシェアは、次のようになっている。

磁気ストライプカード式	40%
ウィガンドカード式	30%
電波カード式	12%（アクティブとパッシブの両方を含む）
その他の携帯物によるもの	10%
掌形・指紋・網膜等	8%（生物学的な方式によるものは米国でもまだ少ない）

つぎに、米国におけるアクセスコントロールの市場規模の見通しは、93年まで次のように試算されている。

89年	10億ドル	(1,500億円)
90年	15億ドル	(2,250億円)
91年	20億ドル	(3,000億円)
92年	27億ドル	(4,050億円)
93年	35億ドル	(5,250億円)

### 1. 5 わが国の市場規模

まず、米国はわが国よりもセキュリティに対する意識が高く、これが主たる理由で市場が拡大していると思われる。わが国の場合でも、アクセスコントロール分野が伸びるであろうが、米国のような高成長率ではないであろう。わが国では、平均して年率15%程度の成長率と見てよいのではないかとと思われる。

つぎに、わが国のアクセスコントロール市場を、米国の15分の1と仮定してみたい。そして、米国の90年の試算である15億ドルをもとに、2010年のわが国の市場規模を予測してみると次のようになる。

$$2,250\text{億円} \times \frac{1}{15} \times (1.15)^{20} = 2,455\text{億円}$$

参考文献 Frost & Sullivan ; SECURITY GAZETT, Oct. 1989, P17.

## 2. 防災・防犯

### 2. 1 防災市場の現状

防災市場の動向は、未曾有の建築ラッシュを反映して自動火災報知設備の機器の検定数量からも平成元年4月から9月までで14.5%の伸び率となっている。建築業界の見込みも当初は前年比6%と推定していたが、すでに13%の伸び率を示し、とくに建物の大型化が目立ち、そのうち首都圏に80%集中している。したがって、防災業界も各社共10%~15%伸びることは間違いないが、今後も当分の間上昇傾向で推移すると見ている。防災市場はゼネコンの受注より1年~2年のずれで受注になることから上記の見通しはほぼ間違いない傾向といえる。

#### (1) 現状の動向

従来防災設備は、建物の規模や用途により消防法、消防法施行規則等により義務づけられている。したがって、この業界の市場は、義務設置物件の建物が年間に建築される数によって決まってしまうため、自己のコストダウンや開発による市場の拡大はあまり望めなかった。逆に法による保護のもとで、一定の市場は間違いなく確保できる安定市場でもあった。

また、機器については、消防法に基づいて検定制度があり、検定合格品以外は使用できないことから、外部からの参入もほとんど無いと同時にメーカーの特殊性も出せない状況であった。

しかしながら、昨今の建築物の形態は高層化し巨大化し大きく変貌してきたことにより、自動火災報知設備のあり方も必然的に見直す必要が出てきた。消防庁の指導もここ数年前から建物の用途、構造により対応できるよう、日本消防設備安全センターの性能評定制度を設け、新しい建物に適用した防災システムが認められるようになった。とくにインテリジェントビルの出現によって、情報化時代に適合したシステムの新規開発も必要となり、この業界も新しい市場に向けて動き出した。

一方、従来義務設置対象の建物だけであったものが、老人弱者の防災対策を行政側が強く打ち出してきたため、義務設置対象以外の市場のニーズが出てきた。

#### (2) 今後の問題点

##### (a) ハロン消火設備

防災設備の中で今、オゾン層の破壊問題として、世界各国が論議しているフロンガスの問題がある。現在消火剤としてコンピュータールームやクリーンルームに広く使用されているハロン1301もフロン系ガスとして対象になっており、1990年6月に予定されているISOの国際会議において、ほぼ確定的な方針が打ち出される見込みである。

ハロンガスは、消火剤として使われているので、その量は全体のフロンガスの使用量から見れば数パーセントに過ぎないし、大気中に拡散される危険性もほとんど無いといってよいが、世界の趨勢としては今後減産、そして中止となると思われる。代替品がハロンガスについては、いまだできていないので、中止の時期は現在いまだ明確ではないが、方向としては暫時使用できなくなる。

今後の情報化社会の中で、コンピュータ等の電子機器に2次災害が無いハロン消火装置は、これからの防災設備として極めて重要な役割となる時期だけに、今後の代替対策が大きな課題となる。

## (b) スプリンクラ消火設備

先に述べたとおり建築物の高層化にともない、スプリンクラの需要は急激に増加してきたが、工事人の不足が今や極めて深刻な状況となっている。スプリンクラヘッドの取り付け工事は熟練した職人が必要で、パイプに高い水圧がかかっているため、馴れない職人が施工すると後で水漏れが起きることがあり、この職人の確保が極めて難しい現状となっている。今後工事方法の改善、あるいは新しいタイプのスプリンクラの開発が必要となってきた。

## 2. 2 防災の2010年の推定市場

今後の防災市場は種々の問題点はあるが、現在の建築ブームは向こう5年間程度は10%程度の伸び率で推移すると思われる。防災市場としては、それに加えて義務設置対象物件以外の一般任意設置市場も出るとして、今後10年間程度は年間15%の伸び率はあると推定した。その後の伸び率については、大型プロジェクトが一段落したとしてもレジャー関連事業や一般住宅を対象とした需要も高まると思われるので、ここでは年率10%の伸び率として2010年における推定市場を出した。

今から20年後の技術革新が防災分野でどのようなようになってくるか。とくに伸び率の早い情報関連の防災がどのような伸び率を示すかについては、現時点での予測は非常に難しいが、一応前述した現状からの推定によると表4のとおりとなった。

表4. 2010年の防災市場

(単位：億円)

項 目	年	機 器	工 事	合 計
自動火災報知設備	1989	546	364	910
	2010	6,575	4,384	10,959
ハロン消火設備 (2010年は代替消火設備となる)	1989	222	148	370
	2010	2,674	1,782	4,456
同 上 保 守	1989	400	—	400
	2010	4,817	—	4,817
合 計	1989	1,168	512	1,680
	2010	14,066	6,166	20,232

## 2. 3 防犯機器の市場

防犯機器の市場は、警備会社が運用の中で使用しているものが大半で、それ以外の市場は日本においては限られた商品となっている。

警備会社が使用している主な商品は、

- ・ドア、窓のマグネットセンサ
- ・赤外線センサ
- ・アットセンサ
- ・超音波センサ
- ・ガラスの振動センサ

等でそれぞれの目的に応じて、使い分けている。

また、電話機に接続して 110 番にオートダイヤルで通報し、情報をテープで知らせる機器等もあるが、現状の市場としては未だ年間 100 億円程度と推定される。しかし情報化が進むにつれて、警備市場も多角化し、またネットがらみのセキュリティ市場も拡大すると、必然的に防犯機器も新しい分野の商品に拡大されていくと思われる。

2010 年にはネットワークを通した一般住宅関係の防犯機器が主力となってくると思われるが、具体的な商品化については現状では確定することは難しいが、一応 2010 年の市場推定として表 5 のように予測してみた。

表 5. 2010 年の防犯機器市場  
(単位：億円)

年	防 犯 機 器
1 9 8 9	1 1 0
2 0 1 0	8 2 2

### 3. 非常用電源設備

情報システムの広範な普及と社会、経済活動における重要性の高まりとハイテク化により、入力電源の品質と、電力の継続的な供給が大きな問題となってきた。電源の停止は、情報システムの停止につながり、社会、経済活動に多大な支障をきたすことは、近年よく報告されていることである。

このような事態の未然防止策として、非常用電源設備が用いられていることは、よく知られている。この非常用電源設備としては、セキュリティ産業の分類に基づけば、

- ・発電機
- ・バッテリー
- ・CVCF
- ・AVR

が、対象機器として例示されている。

この分野の産業規模を考えるに当たり、情報システム用としては、CVCF+バッテリーの組合せが一般的であり、これを中心に検討した。

#### 3. 1 非常用電源設備について

##### (1) 非常用電源設備の現状

非常用電源設備として、

- (i) CVCF+バッテリー
- (ii) CVCF+バッテリーおよび発電機

の組合せで使われる。このCVCFは、現在では静止型が使われているが、以前はさかんに回転型（いわゆるMG）が使われていた。

非常用電源設備としては、(i)の場合5分～15分程度の、また(ii)の場合4時間程度から10時間程度の停電をカバーするのが一般的である（12時間以上のものは常用発電機と同じになる。）

この非常用電源設備を使用した電源システムのブロックダイヤグラムを図3に示す。

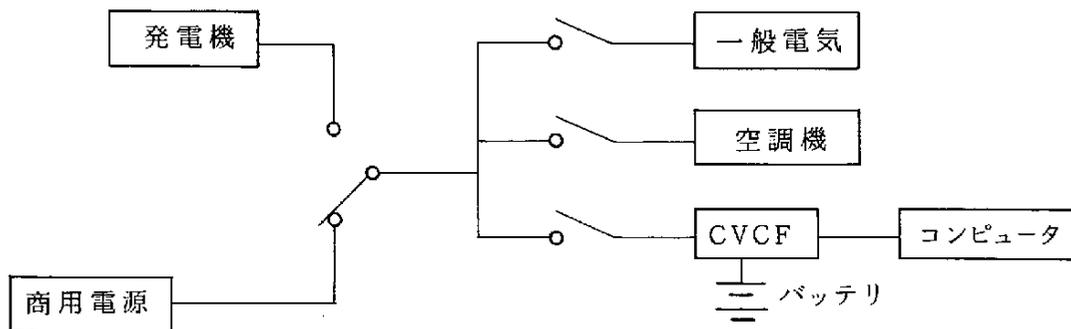


図3. 電源系統図（非常用電源設備系）



みて、次の新しいシステムまたは装置が実用化されるためには現在なんらかの技術的な検討が開始されていなければならないと考える。開発から実用化を経て世代交代に20年程かかると思われている。

技術革新と言う観点からみると、初期のサイリスタ I の第一世代から現在の第四世代へと変化しており、これによる CVCF の大きさは、約  $1/3$  になっている。このような技術革新は今後も続くであろう。

(b) バッテリー

ここ20年間、若干の技術的変化は見られたものの、基本的には、ほとんど変わっていない。しかし研究段階にあるものでは、次のようなものがある。

①太陽電池

太陽電池については、かなり研究されているが、その効率、夜間等の充電の問題等から考えて、ここ20年で実用化され、現在のバッテリーに代わることはないだろう。

②燃料電池

一般用としての実用化段階の一步前だろう。発電効率等からみて新たなエネルギー源とみられている。

ただし使用方法は、現在の鉛バッテリー、アルカリバッテリーと直接置き換わるものではなく、次に述べる新世代の安定化非常用電源設備に用いられるものとみている。

(c) 発電機

太陽電池、燃料電池は、バッテリーであると同時に、発電機でもある。したがってこれが発電機に置き換わると考えられるが、これ以外には若干の技術革新を除き、目新しいものはないだろう。

(d) 非常用電源設備の利用動向

1975年頃は、商用電源を直接使用することが主流で、CVCF+バッテリーの利用はあまりなかった。これが1985年頃まで続いた。その後情報システムが、社会生活のインフラストラクチャとなり、その稼働の停止は、大きな社会問題となり始めた。このため CVCF の導入が促進された。現在はこの導入促進の時代で、1995年頃まで続くだろう。その後は、高い導入の時代が続くだろう(図5)。

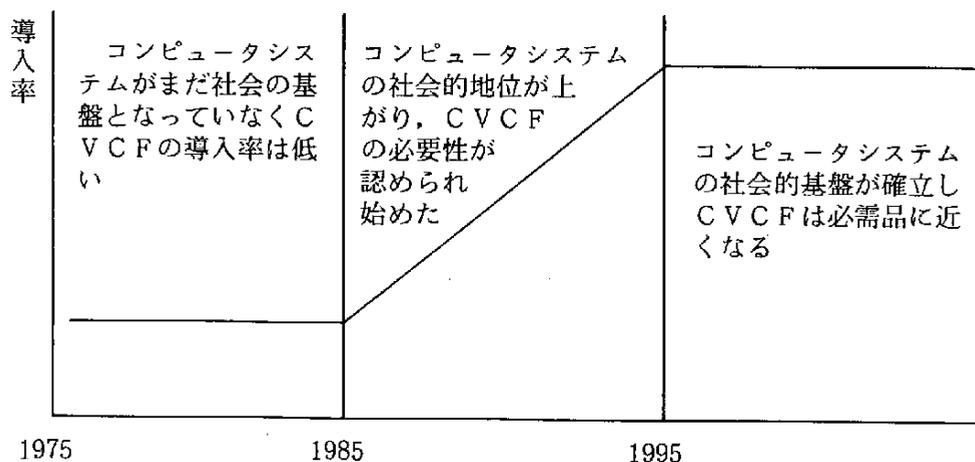
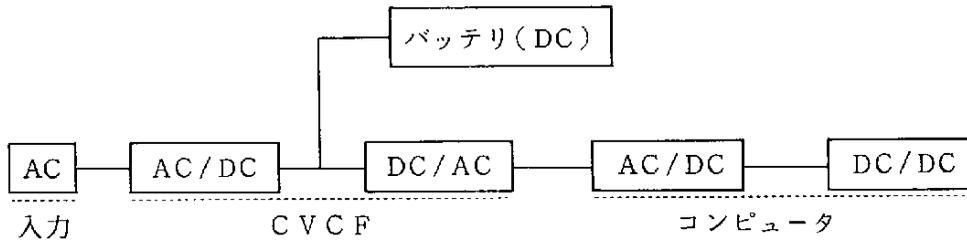


図5. CVCF導入率の推移

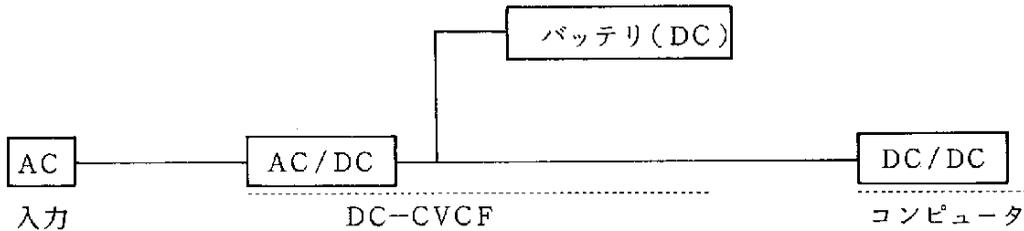
(3) 新非常用電源設備

現在の非常用電源設備は、図3に示す方式で使用されているが、電気エネルギー的には次のような変換が行われている。



つまり3回のAC-DC（またはその逆）の変換を行っている。このためのエネルギーロス、回路素子の増加による信頼性への影響等は一考を要するものがある。

この解決策として、コンピュータのDC受電と、DC-CVCFが考えられる。つまり先の変換を次のようにする。



1回のAC-DC変換ですむ。

(a) DC非常用電源設備

AC-DC変換が1回ですみ、かつ発電機/バッテリーとして燃料電池を用いることにより、効率の良い非常用電源設備が提供されるだろう。さらに空調機がDC化されれば、図3の電源系統はコンピュータ系に対し図6のごとくなる。またこの燃料電池は、発電コストが商用電源とほぼ同等にまで下がるとも言われ、燃料供給方法さえ解決できれば、商用電源の有力な代替可能な電力源となり、安定化非常用電源設備として用いることも可能だろう。

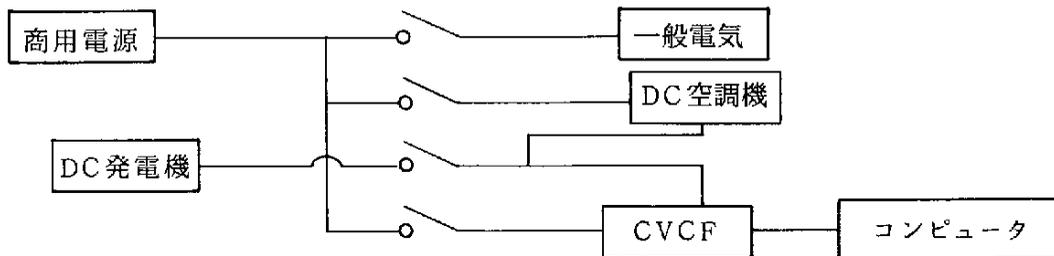


図6. DC発電機系統

(b) DC非常用電源設備の問題点

これを実用化するためには、DC-CVCFの小型化とコンピュータ室への設置が必要条件となる。また燃料電池も同時に小型化され、コンピュータ室のごく近くに設置することが

可能でなければならない。もしこれが遠く離れるようであれば、DC送電と同じ問題を引き起こすだろう。

### 3. 2 非常用電源設備の市場規模の推定

#### (1) 現 状

1989年のCVCF+バッテリーの市場規模の推定は、矢野経済研究所の報告書に推定値として述べられている。

#### (2) 市場規模推移予測の根拠

##### (a) 過去の推移（1985～1989）

図7に1985年から1989年のCVCF+バッテリーのデータを示す（容量ベース）。これによるとこの5年間で平均22.8%の伸びを示している。

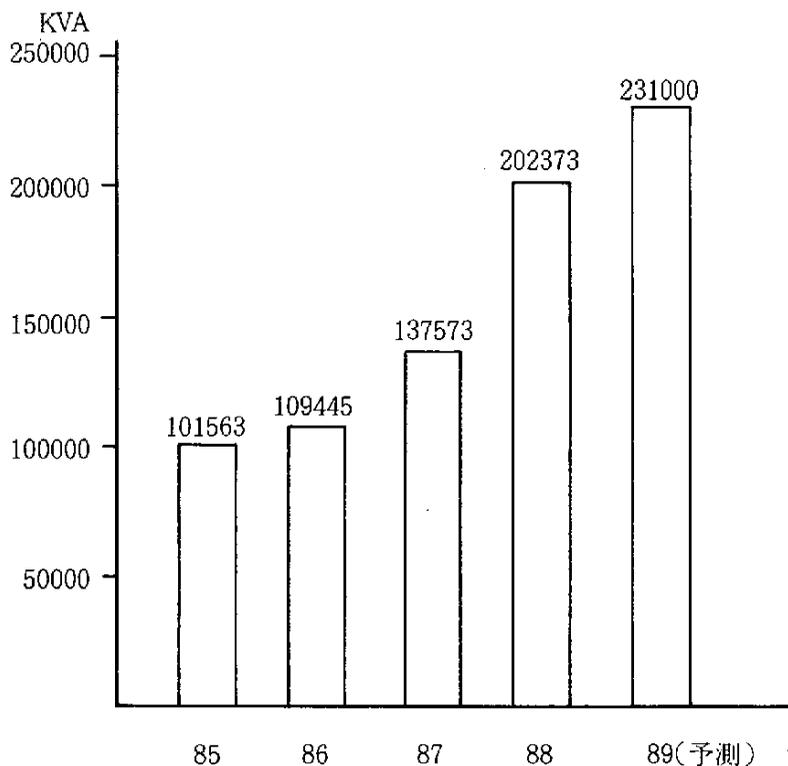


図7. CVCFの出荷推移

##### (b) 今後の予測 I（1990～1995）

この5年間は、前の5年間の伸びを持続するだろう。このCVCFの伸びは、コンピュータシステムの伸びを超えている。これは従来バンキング等に主に用いられていたものが、情報システムの社会的な重要度（システムが社会活動に占める地位）が増すにつれ高くなっていくと考えられるからである（図5）。

したがってこの5年間は20～25%の高いほうの伸びを示すものとする。

ただしこれも容量ベースの伸びで、価格ベースでは、技術革新等による価格低下を加味し、これほど高い伸びはないと予測した。ここでは、一応20%とした。

(c) 今後の予測Ⅱ（1996～2010）

この間の伸びは、コンピュータシステムの伸びとほぼ同じ傾向になるだろう。一応この期間は、容量ベースで10～13%程度、価格ベースで10%程度とした。

(3) 市場規模の推定

(a) 現状（1989年）

約 70,000百万円

(b) 2010年

約873,100百万円

3.3 課 題

2010年の情報化社会を支える安定化非常用電源設備として、CVCF+バッテリーの重要性は非常に高いものと言える。このためには、数々の課題をクリアしなければならない。

(a) アクティブフィルタ

CVCFの小型化効率化のために、主回路のキャリア周波数の高周波化が必須である。これがEMI、受電設備の大容量化、他の電気回路への障害等種々の問題をおこす。この障害防止として、アクティブフィルタの取り付けがある。高効率アクティブフィルタの開発研究が急がれる。

(b) DC電力化

- ① コンピュータシステムのDC受電のための考え方の統一
- ② DC空調機の開発
- ③ DC-CVCFの開発

(c) 燃料電池

- ① 大電力高効率および小型燃料電池の開発
- ② 燃料電池のための燃料供給ネットワークの充実
- ③ 高効率燃料貯蓄

(d) 高効率鉛バッテリー

- ① 高効率小型シールバッテリーの開発

## 4. 監視

### 4. 1 監視の範囲

ここで監視（装置）とは、監視・確認用のCCTV（Closed Circuit Television）、防犯カメラおよび民生も含む通路用映像確認タイプのドアホンをいうこととする。製造を主体とし、据付とメンテナンス費用、および放送用テレビジョン装置等は含まない。

一般によく知られているように、防犯・防災分野で最大の市場を得ているものは、CCTV使用のセキュリティシステムである。

### 4. 2 CCTV市場

監視確認用のCCTVカメラについては、ビデオカメラの固体化とカラー化が進行中であるといえる。それは、「保守不要」と「監視効果の向上」が大きな要因である。設置先別にみれば、流通店舗（コンビニエンスストア等）、金融関係、電力・ガス・工場等、遊戯場、交通関係などである。

特に、コンビニエンスストアは、年間3,000店以上増加するといわれているが、CCTVの普及率は高い。金融関係のCDやATMコーナーにもセキュリティ用のカメラが設置されている。将来一般家庭にも普及するものと思われる。

米国では、CCTVは監視装置のなかで、93年には13%のシェアを占めるようになろうとしているといわれている。

### 4. 3 2010年の市場規模

監視・確認を主としたわが国のCCTV市場は、約1,000億円とみられ、成長率は年平均15%程度とみるのが妥当であろうと思われる。したがって、2010年の市場規模は、次のようになる。

$$1,000\text{億円} \times (1.15)^{20} = 16,366\text{億円}$$

参考文献 Frost & Sullivan ; SECURITY GAZETTE, OCT.1989, P17.

## 5. 保管設備

### 5. 1 市場の背景

#### (1) 情報量の増大

経済の発展、コンピュータリゼーションの進展、あるいは国際化と共に、情報量は膨大なものとなっている。あらゆる情報処理がコンピュータ処理に依存するようになり、データベース化され、磁気テープに蓄積保管される。一方、紙記録においては、一般文書、伝票、契約書の類はもちろんであるが、コンピュータ処理にともなう膨大な各種出力帳票の保存が問題となりつつある。日常業務において、OA機器に依存することが多くなり、これがペーパーレス化の狙いを生かせずに、オフィス内において“紙の洪水”化している傾向も見受けられる。

#### (2) スペースコスト対策

各企業とも、オフィスが狭く、地価高騰もあってスペースの確保が極めて困難な状況にあり、その対策に頭を傷めている。したがって、情報の保管に対するスペースコスト対策、オフィススペースの確保、オフィス機能および環境の改善等を図るうえからも外部保管のニーズが高まってきている。また、情報の管理と最も密接な関係にある事務センタにおいては、膨大な情報処理および保管のために、スペースと人の確保が問題となっている。

#### (3) 情報の安全管理

人、物、金とともに、第4の資源といわれる情報の価値は金銭で買えないものであり、安全管理体制が重要である。すなわち、セキュリティを基本にした事業であるため、安全対策には万全を期す必要があり、単に保管施設を設ければ良いというものではない。

#### (4) 効率的な運用管理

オフィスの文書記録を分析すれば、オフィス内で保管活用されるべきものが30%、廃棄されるべきものが40%、コストの安い場所へ置き換えすべきものが30%といわれる。すなわち、管理不十分のため、単にストックされているケースが多い。ユーザは、外部保管に対して、保管だけではなく、事業者による集配送も含めた一貫体制を望んでいる。集配送については、方法によっては機密性の保持から問題が出てくる。また、FAXサービス等の即時閲覧サービスへのニーズも増えている。すなわち、ユーザの情報を総合的に管理するサービスが必要である。

#### (5) 機密保持

情報は、ほとんどが内部から漏洩、流出している。これは管理がズサンであったり、重要な情報にいつでも、内部の人間は誰でも、自由に接する機会が多いことによる。厳重な保管設備、監視体制、受渡し方法が確立していれば、むしろ、外部保管の方が機密漏洩防止に効果的であるといえる。

#### (6) OA機器の活用と媒体変換

膨大な情報は、単にストックされるだけで、活用しなければ全く意味がない。そのために、ペーパーレス化に取り組み、情報の蓄積・検索のためのOA機器導入・活用の見直しや電子媒

体への変換が進んでいる。磁気媒体も小型・高密度型へ急テンポで進んでいこう。紙記録の情報を電子的情報に置き換える問題については、保管義務に関わる法律の問題もある。

## 5. 2 情報の保管市場

### (1) 現在の保管市場

#### (a) 保管設備

情報を保管する事業者は、商品等を主として取り扱う一般倉庫と区別し、非商品を扱う事業者として、運輸省は「トランクルーム事業」と規定している（昭和61年度トランクルーム約款制定）。わが国ではこれを専業する事業者は1社のみで、他は物流事業との兼業が多い。したがって、設備は従来の物流の中心となる港湾・河川部、街道筋の倉庫で事業をしているケースが多い。当該企業はセキュリティを基本とした設備でなければならない、大多数の既存設備は多くの問題を抱えている。

#### (b) 現在の利用状況と市場規模

セキュリティ事業としてとらえた場合いろいろな問題を含んではいるが、一般倉庫、トランクルームを含めて、潜在的にはかなり外部倉庫が利用されている。これには2通りがあり、1つはトランクルーム業者に寄託し、管理を委ねているケース、2つは、企業が外部倉庫を賃借して保管し、自社管理あるいは子会社に管理させているケースである。

トランクルーム業者への寄託については、昭和61年度よりトランクルーム約款が制定され、従来の一般倉庫と区分しトランクルームの統計数字が発表されるようになったが、1988年度のトランクルーム売上額は140～150億とされている。これは家財道具、美術品、衣類等（運輸省による呼称「フレイトビラ」）と情報記録物（同じく「ドキュメントビラ」）に分類しなければならないが、そのうち、情報記録物の割合は約45%を占めているとみられ、約65億円が現在の保管業者の売上額と推定される。

### (2) 2010年の市場

#### (a) 保管設備

情報量はさらに膨大なものとなり、その活用と安全な蓄積保管が要求されることになろう。情報が、企業戦略上ますます重要となり、ユーザの外部保管のニーズはセキュリティと情報の活用・管理システムを具備した事業者を求めることになろう。

運輸省は、昨今の都心の地価高騰に鑑み、オフィススペースの有効利用をテーマにトランクルーム促進の一環として、「ドキュメントビラ」（書類の別荘）の推進普及を図っており、当然のことながら、そのようなユーザニーズに沿ったセキュリティ倉庫事業者へ転化していくものと思われる。

#### (b) 利用状況と市場規模

現在のトランクルームの事業規模の拡大と同時に、潜在している自営の設備による事業化も顕在化するものと思われる。一方、前述したように、OA機器の活用によるペーパーレス化、メディアの小型・高密度化、電子情報化等によるスペース対策の促進、また、情報の有効活用と検索の迅速化、あるいは法改正による媒体変換の促進等、技術の進捗にともなって大きな変化も予測され、これらは市場規模にも影響を与えるものと思われる。

大量の情報を取り扱う事務センタがその情報の処理、保管とそれに従事する人（社員、パ

ート)のためのスペースの確保に頭を痛めており、情報の保管業者がその業務をセットにした事業も出現しよう。

いずれにしても、市場は拡大進展していくが、前半10年の伸びが大きく、年率約20%、後半10年はかなり市場も熟成するため伸び率は鈍化し、年率約10%位ではないかと思われる。したがって、2010年の市場規模は約1,000億円と予測される。

## 6. 暗 号

### 6. 1 暗号装置の現状

情報が第三者に漏れたとしても、その内容を理解できなくする暗号装置は、古くから、一部の領域では利用されてきている。たとえば、外交関係の文書の送受信、防衛関係の各種の指令情報などにおいてである。一方、民間の情報システムにおいても、システムの安全確保の重要性に対する認識が高まるとともに、徐々にではあるが、導入ユーザが増えてきているのが現状である。ここでは、特定のユーザ向けの特殊な暗号装置を除き、情報処理機器の1つとして一般に販売されている機器の市場規模を推定することにする。

現在、わが国においては、計算機メーカーや商社を始め、10社位が、84年前後から暗号装置を販売している。価格は、数10万円から100万円を越えるものまでさまざまである。販売台数は累計で1,000台程度と推定される。したがって、現在の市場は普及という点では黎明期といえ、規模は、50万円×1,000台=約5億円程度と考えられる。

### 6. 2 今後の動向

暗号装置の今後を予想する上で重要な事柄は、ユーザニーズとの関係である。現在のセキュリティの中には、従来のように、重要な情報に対し暗号化を施し、情報のコンフィデンシャルリティを高めたいというものがある。このニーズは、さらに暗号化すべきデータの場所により、2つに分かれる。1つは回線上を流れるデータの暗号化であり、もう1つは、磁気ディスクや磁気テープのように、取り外し可能な磁気媒体に格納されるデータの暗号化である。

もう1つのセキュリティニーズは、データが正しく送受信されたかを保証する仕掛けである。これは情報のインテグリティ確保のニーズである。また、この仕掛けは、メッセージ認証やデジタル署名などの呼び方がされている。いずれにしろ、そのような装置の基盤には、暗号装置の技術が用いられる。その意味で、将来市場の推定に含めることとした。

#### (1) コンフィデンシャルリティの市場予測

日本情報処理開発協会のアンケート結果によると、暗号の使用率は、現在が16.6%であり、5年後の採用希望ユーザは20.7%である。この4.1%の伸びが継続的に続くとすれば、2010年の使用率は33%に達する。これだけの高い使用率が予想され、かつ、情報システムの安全性確保に必須の機能は、従来のように、単独の暗号装置として存在するのではなく、通信処理装置、デバイスコントローラ、計算機本体等、高価な装置には標準装備され、パソコンやワープロのような低価格な装置にはオプションとして装備されると思われる。

##### (a) 回線上のデータ暗号

回線上のデータ暗号装置であるが、これには2種類のタイプが考えられる。これをここでは仮にセンタ型と端末型と呼ぶ。センタ型とは、複数の相手と同時に暗号通信が可能な装置であり、データベースの置かれる大型の計算機等に装備されると考えられる。端末型は逆にそれらのデータベース計算機に接続されるアクセス用の端末などに装備されるもので、センタ型に比べて、比較的簡易な作りとなっている。

生産動態統計(表6)によると、過去5年の汎用機の生産台数は、12,000台前後で一定に

なっている。この状態が今後続くと仮定し、センタ型には標準装備されるとすれば、市場は次のようになる。

$$12,000\text{台} \times 50\text{万円/台} = 60\text{億円}$$

一方、端末型は、パソコン、端末装置、ファクシミリ、日本語ワープロ等に採用されると考えられる。これらの装置は今後もそれぞれの分野で著しい伸びが予想される。ここでは、台数は、過去5年の伸び率で今後5年推移し、その後、機能的に融合した複合端末のリプレース時代になると仮定する。また、このときのオプション採用率を50%とすると、市場は次のようになる。

$$\text{ファクシミリ} : 430\text{万台} \times (1.71)^5 \times 0.5\text{万円/ボード} \times 50\% = 1,572\text{億円}$$

$$\text{パソコン} : 240\text{万台} \times (1.11)^5 \times 0.5\text{万円/ボード} \times 50\% = 101\text{億円}$$

$$\text{端末装置} : 110\text{万台} \times (1.12)^5 \times 0.5\text{万円/ボード} \times 50\% = 48\text{億円}$$

$$\text{ワープロ} : 260\text{万台} \times (1.85)^5 \times 0.5\text{万円/ボード} \times 50\% = 1,409\text{億円}$$

#### (b) 磁気媒体上のデータ暗号化

外部記憶装置の伸びは、生産動態統計によると44%の伸びを示しているが、これは、パソコン等に接続されるフロッピィやディスクの寄与が大きいと思われる。暗号の必要とされるデータは、むしろ、データベース計算機に格納される企業機密に属するデータなどである。したがって、ここでは、データベース計算機に接続される磁気ディスクのコントローラレベルで暗号機能が実装され、システム当たり平均10台の暗号機能付きコントローラが装備されるとして、その市場は次のようになる。

$$12,000\text{台} \times 10\text{コントローラ} \times 20\text{万円/コントローラ} = 240\text{億円}$$

#### (2) インテグリティの市場予測

現在、データが送受信された事実を保証する仕掛けは、ごく一部で、実用化されているにすぎない。たとえば、国際的な資金移動電文の送受信サービスを行っているSWIFT (the Society for Worldwide Interbank Financial Telecommunication)である。このようなサービスが広くEDI (Electric Data Interchange) に適用されるためには、利用者層のコンセンサスが得られ、それに応じた制度面の見直し等、多くの課題が残っている。

ここでは、2000年には銀行と企業間における資金移動、役所と企業間における各種許認可などが、ネットワークを経由してやりとりする環境が整い、その後、徐々に市場を形成していき、2010年には実社会に定着していると仮定する。

##### (a) 金融機関

現在、ファームバンキングにより即時資金移動サービスは、表7のアンケート結果によると、すでに延べ7万弱の企業を対象に始まっている。端末は、 пейバイフォン、パソコン、キャプテン端末、FB専用端末とさまざまであるが、2010年には標準化も進み、また、そこに実装されるセキュリティ機能も充実し、送受信事実をより厳密に特定できる機能が備わっていると思われる。

表8に金融機関の店舗数を示す。2010年には、粗く約7万店舗に資金移動用の設備が、平均して5台位設置されると仮定して、その市場規模は次のようになる。

$$7\text{万店舗} \times 5\text{台} \times 50\text{万円/台} \times 5 = 350\text{億円}$$

(b) 一般企業

表9に、法人企業数の伸びを示す。2010年の企業数を過去10年で36%の伸びから推定し、さらに、インテグリティ機能の導入率を、

- ・資本金500万円未満の企業の10%が1台
- ・資本金500万円以上1億円未満の企業の50%が2台
- ・資本金1億円以上の企業の100%が10台

導入すると仮定する。この仮定から市場を推定すると次のようになる。

$$(105万企業 \times 10\% + 72万企業 \times 30\% \times 2 + 2.2万企業 \times 10) \times (1.36)^2 \\ \times 20万円/台 \times 1/5 = 560億円$$

(c) 公共団体

地方公共団体の現状は、都道府県47、市町村3,322であり、表11より、ほとんど電算機を導入済である。また、そこでの電算機業務数は、実施率にバラツキはあるものの、それぞれ約70である。2010年には、団体数はほぼ現状と同じで、業務の暗号装置共同利用率を50%と見なし、市場を予想すると次のようになる。

$$3,369団体 \times 70業務 \times 50\% \times 50万円/台 \times 1/5 = 118億円$$

(3) 2010年の市場規模予測

以上のことから、2010年の市場規模は次のようになる。

コンフィデンシャリティ関連：3,430億円

インテグリティ関連：1,028億円

ただし、この推定において不確実要因も多い。以下それを列記しておきたい。

- ・暗号装置は市場が形成されるにつれ、低価格化が進むと同時に機能の充実が図られる。ここでは、単純にセンタ型は現在価格に、また、端末型は現在価格が10分の1程度下がるとして将来価格とした。
- ・将来の端末機の普及は、いずれ飽和に達すると思われるが、その時期や台数の正確な推定は難しい。ここでは、粗く5年と推定した。

表6. 情報処理機器、通信機器等の伸び

品目(数量)	84年	85年	86年	87年	88年
通信機器及び無線応用装置	23,471,659	23,687,757	26,050,794	—	—
ファクシミリ		865,575	1,235,001	2,411,221	4,333,834
電子計算機及び関連装置	12,370,325	18,803,606	28,832,232	36,308,335	42,955,702
計算機本体	1,578,315	2,026,493	2,120,167	2,111,327	2,605,585
汎用コンピュータ	12,762	14,138	9,445	11,095	13,150
パーソナルコンピュータ	1,500,810	1,923,757	2,004,157	1,973,880	2,388,383
周辺装置	9,898,387	15,866,782	25,332,351	33,138,160	39,109,894
外部記憶装置	5,530,051	8,386,518	15,181,839	21,126,420	23,792,659
端末装置	657,894	690,902	875,804	1,039,584	1,085,452
日本語ワープロ	210,620	1,122,753	2,043,581	2,188,064	2,564,446

表7. 主要金融機関店舗数の推移（本店、支店、出張所など）

	85.3	86.3	87.3	88.3	89.3
都市銀行	3,169	3,228	3,392	3,438	3,533
地方銀行	6,746	6,926	7,042	7,171	7,313
信託銀行	391	389	394	401	407
長期信用	79	80	82	83	88
第二地銀	4,213	4,333	4,319	4,416	4,510
信用金庫	6,859	7,124	7,385	7,551	7,754
信用組合	2,797	2,839	2,871	2,897	2,924
農業協同	16,437	16,465	16,536	16,357	16,314
漁業協同	2,151	2,148	2,141	2,130	2,138
労働金庫	579	602	621	635	642
郵便局	23,561	23,671	23,745	23,830	23,914
合計	66,982	67,805	68,528	68,909	69,557

出所：金融情報システム白書

表8. ファームバンキング（即時資金移動）アンケート結果

アンケート先	対象	回答	サービス先企業数			
			①	②	③	④
都市銀行	13	13	38,338	6,537	731	8,513
長期信用銀行	3	3	275	29	0	5
商中・農中	2	2				
信託銀行	7	7	68	41	9	0
地方銀行	64	64	9,787	1,480	105	1,300
相互銀行	68	68	903	52	0	54
信用金庫	455	385	1,503	1	0	0
信用組合	121	85	データ無し			
合計	738	627	50,874	8,140	845	9,872

端末種別：① ペイバイフォン

② パソコン

③ キャプテン

④ FB専用端末

出所：(財)金融情報システムセンター

(88年末の調査)

表9. 法人数の累年変化

資本金 年代	500万以上		1000万以上	1億以上	10億以上	指数
	500万未満	1000万未満	1億未満	10億未満		
1977年	918,318	189,561	189,464	12,837	2,044	100
1978年	925,869	202,161	206,190	12,973	2,142	103
1979年	944,550	220,308	221,512	13,477	2,213	107
1980年	961,580	237,674	233,947	14,066	2,282	110
1981年	978,836	251,525	251,457	14,713	2,357	114
1982年	986,078	267,174	270,316	15,276	2,455	117
1983年	999,540	279,407	281,012	15,923	2,570	120
1984年	1,017,005	292,936	295,302	16,292	2,726	124
1985年	1,019,712	311,392	308,949	17,087	2,870	127
1986年	1,031,621	321,698	327,539	17,740	3,044	130
1987年	1,049,935	358,655	352,527	19,097	3,220	136

出所：国税庁

表10. 1987年分の業種別、資本金階級別法人数

区 分	500万以上		1000万以上	1億以上	10億以上	合 計
	500万未満	1000万未満	1億未満	10億未満		
農 林 水 産 業	8,587	3,431	3,274	118	10	15,420
鉱 業	1,950	1,193	1,769	109	113	5,134
建 設 業	150,577	57,023	57,550	1,082	158	266,390
織 維 工 業	13,474	4,545	5,606	267	53	23,945
化 学 工 業	18,857	7,723	11,249	1,283	448	39,560
鉄鋼金属工業	36,194	11,437	11,655	754	178	60,218
機 械 工 業	43,484	15,554	16,425	1,607	488	77,558
食料品製造業	23,609	8,004	9,213	554	113	41,493
出版印刷業	26,016	6,396	5,711	237	21	38,381
その他の製造	57,692	20,241	18,516	765	134	97,348
卸 売 業	132,240	60,915	71,378	3,745	293	268,571
小 売 業	190,011	50,214	29,208	976	137	270,546
料理飲食旅館業	60,450	18,258	13,819	831	86	93,444
金融保険業	14,315	3,672	4,908	921	315	24,131
不 動 産 業	94,336	30,035	33,770	2,115	186	160,442
運輸通信公益事業	24,799	15,452	19,951	1,445	302	61,949
サ ー ビ ス 業	150,220	43,551	36,298	2,081	182	232,332
その他の法人	3,124	1,011	2,227	207	3	6,572
合 計	1,049,935	358,655	352,527	19,097	3,220	1,783,434

出所：国税庁

表11. 地方公共団体の電子計算機利用状況（利用団体）

		77 年	82 年	86 年	87 年
都道府県	単独 導入	46	47	47	47
	委託	1	0	0	0
市町村	単独 導入	361	587	1,064	1,247
	委託	1,832	2,022	1,787	1,646
	小 計	2,193	2,609	2,851	2,893
	共同 導入	265	288	253	235
	委託	120	153	108	90
	小 計	383	441	361	325
	合 計	2,578	3,050	3,212	3,218
参考) 地方公共団体数		3,326	3,325	3,323	3,322

出所：自治省

## 7. セキュリティ用ソフトウェア

高度情報化社会と呼ばれるこれからの社会では、諸々の社会活動の情報への依存度がますます高まっていくことについては議論の余地がない。したがって、将来に向かって情報の収集・蓄積・加工・整理・検索・配布等をあずかるコンピュータシステムのセキュリティがますます重要になってくる。

### 7. 1 セキュリティソフトウェアの現状

しかしながら、一方、肝心のユーザ側においては、コンピュータセキュリティの重要性についてある程度の理解は示しながらも、セキュリティ対策が直接的に生産性の向上をもたらす類のものではないこともあり、なかなか実施に取り組み難いという事情がある。このように、セキュリティ対策の実施は必ずしもはかばかしくないというのが実情である。

ここでは、セキュリティ用ソフトウェアについて考える。セキュリティ用ソフトウェアとしては、たとえば最近話題になってきているコンピュータウイルスを防御するための検査プログラムやワクチンプログラムから、情報が盗まれても解読を不能ならしめるための暗号プログラム等までいろいろある。ここでは最も基本的なものとして、無用の端末ユーザの不法侵入からシステムを守るための、いわばシステムに鍵をかけるアクセスコントロールプログラムをとりあげることとする。この種のプログラムは、システムのセキュリティ対策の第一歩として実施さるべきものといってもよい。その意味では、原則的には全システムが対象であり、システムのすべてが対象市場であるということができる。

しかし、現実には、前述のようにセキュリティ対策は直接生産性向上をもたらすものではなく、むしろ程度の差こそあれ、生産効率の制約条件となる面がある。したがって、すべてのシステムがアクセスコントロールプログラムを導入してセキュリティ対策を実行に移すというわけではない。幸いにして、わが国ではこれまでのところコンピュータ犯罪が少ないからであろう。その結果、理屈の上では全システムが対象になり得る性質のものであるにも拘らず、実際にはアクセスコントロールプログラムを導入して不法侵入を防御しているシステムは全体の20%に満たないのが現状である。

ここでは、潜在需要は一時おいて、顕在需要をもとに市場規模を推定してみたい。具体的には、ある代表的なアクセスコントロールプログラムをとりあげ、そのユーザ数に当該プログラムの価格を乗じ、当該プログラムのメーカーの市場占有率を加味すれば全市場における顕在市場規模相当のものを推定できる。このようにして得られた現在の市場規模は、700億円となった。

### 7. 2 2010年の市場規模

2010年に向けてセキュリティ用ソフトウェア市場がどのようなようになるかを考えてみたい。まず、今後の環境の変化を簡単に整理すると次のようにいえる。

- ①情報システムと社会活動との連携は今以上に深まり広がっていく。
- ②パソコン等の普及、オンラインシステムの増加・拡張により、エンドユーザの数は増加するし、技術レベルも上がる。
- ③コンピュータ犯罪の危険度（頻度、犯罪のもたらす被害の深刻さ等）は増加する。
- ④危険度の増加の認識の深まりと、実際に発生する犯罪実例に促されて、セキュリティ対策の実施に踏みきるユーザが増加する。

一方、製品の側においても、セキュリティソフトウェア、とくにアクセスコントロールプログラムのような基本的なものは、現在のように独立したソフトウェア製品として別途販売されるのではなく、ハードウェアの機能の一部として組み込まれるか、少なくともオペレーティングシステムに組み込まれることになると思われる。つまり、別途購入しなくても、基本機能として付加されてくるようになるであろう。

以上のような状況に鑑み、現在対策を実施していない80%のユーザの約半数は実施するようになると考えてもよいであろう。すなわち、実施ユーザの比率は現在の20%から60%位まで高まると考えられる。したがって、2010年の市場規模はつぎの要領で予測することとする。

- 1) コンピュータシステムの伸びは、10%とみる。
- 2) アクセスコントロールの普及割合は現在の3倍とみる。

以上により計算すると、2010年の市場規模は1兆 4,100億円程度になると推定される。これは、かなり魅力のある市場規模といえるであろう。

## 8. バックアップサービス

### 8. 1 現 状

#### (1) ユーザニーズの状況

##### (a) バックアップ対策ニーズについて

ここでバックアップサービスとは、コンピュータユーザがバックアップ対策ニーズ実現を自社内で完結する手段を取らず、一部または全部を外部の業者のサービスを利用することと考える。

バックアップ対策ニーズについては、昭和63年6月発表された「コンピュータ・バックアップセンタの機能と役割に関する調査研究（財団法人 産業研究所、財団法人 日本情報処理開発協会）」によると（以下、同書のデータおよびアンケート調査結果を使用する）、一般的には次のようなことが言える。

システムダウン等による損害を回避する手段としてのバックアップ対策は、システム内容のバラツキにもかかわらず、80%以上の企業が何らかの対策が必要であるとしている。しかしながら、中期的に考えて今後5年以内にバックアップセンタの構築や、利用の計画がある事業体は12%に過ぎないという結果が出ている。潜在ニーズがあると解釈できる反面、「日本は空気と水と安全はタダ」という意識から抜け切れず、総論賛成、各論反対、必要性の認識のレベルの低さ、バックアップシステム保有のための各種障害（とくにコストがかかる、手間がかかる）の多さを如実にあらわしている。

コンピュータシステムの企業活動に占める重要性は、各事業体において相当の開きがある。たとえば、金銭の受払い・残高を管理する金融システムや、商品の受発注・出荷・在庫管理を一括した物流システム等、社内的、社会的に重要度の高いものから単なる計算業務や累積データの検索業務等、他手段で容易に代替できるものや、必然性の低いものまであらゆる目的に利用されている。

ただし、コンピュータシステムの高度化、世田谷のケーブル火災、サンフランシスコ地震による被害等で徐々にバックアップ対策に関する認識は高まりつつあることは事実である。

とくに、公共性の高い金融機関においては、すでに実施済みのところも一部出ており、未実施のところは現在真剣に検討中である。また、一般企業でもコンピュータシステムを高度に組み入れた物流システムを稼働させている企業や、日本で活躍している外資系企業は、本国のシステム監査の指摘を受け、すでに実施しているところや、真剣に検討中のところが多い。

すなわち、現在のバックアップ対策ニーズの状況は、金融機関、高度物流システム保有企業、外資系企業の一部から定着しつつある状況で、今後、時間をかけて徐々に裾野を広げていくと考えられる。

##### (b) バックアップサービスのニーズ

現在、大手金融機関の一部では、自社独自で東西2センタ方式でバックアップ体制を整えつつある。しかし、バックアップ機能を充分保有するには、莫大なコストがかかり、よほど余裕のある企業でないと実施できない状況にある。

自社内完結バックアップ対策では、コスト的に厳しい。共同化、集中化のメリットで安価にし、その他専門サービス、多様サービスを提供するバックアップサービスのニーズには必

然性がある。

今のところ、バックアップ対策ニーズが低いことから、バックアップサービスニーズも低い。今後、経済性、便利性を考えれば圧倒的多数がこのサービスを利用する方向を選択すると考えられる。

## (2) バックアップサービスの提供状況

国内におけるバックアップサービスは、1社が60年12月に開始し、

- ・共同ホットサイトサービス
- ・コールドサイトサービス
- ・専用ホットサイトサービス
- ・バックアップシステム保有コンサルティングサービス

を提供しているが、いまだ萌芽期にある状況で、今後、機種を揃えること、専用ホットサイトサービスのためのビル建設、回線利用によるバックアップデータ保管サービス等を企画、徐々に拡大を狙っているところである。

その他、バックアップサービスを広範囲にとらえるなら、データ類、用紙類、回線、コンピュータ設置ビルスペース、コンピュータ機器、ソフトウェア開発等で、バックアップ対策用のものを提供するものは全て関係してくるが、ここでは、これらを含めずバックアップシステムの提供、または、サポートを目的として、事業を行うもののみでとらえることとする。

## (3) 市場規模推定

バックアップサービスの市場規模は、前項の範囲として考えた場合、現在サービス提供しているのは、今のところ1社である。したがって、潜在市場は大きい。顕在化している市場規模は10億円程度と考えられる。

# 8. 2 2010年までの経過予想と市場規模

## (1) ユーザニーズの状況

### (a) バックアップ対策ニーズについて

今後、情報化社会はますます進展し、コンピュータは、企業活動の範囲から個人生活に密着したものまで、広く深く浸透すると考えられる。したがって、万一のシステムダウンが一企業の影響に止まらず、経済社会全般に大きく影響を及ぼすので、バックアップ対策ニーズは確実に拡大し、2000年にはコンピュータのバックアップシステム保有は普遍化・常識化し、バックアップシステムを保有しないコンピュータシステムなど考えられない状況になると考えられる。

もちろん、技術革新その他が進み、コンピュータシステムがイメージ処理型、非ノイマン型、ニューロコンピュータ等に変化し、バックアップシステム保有に予想できない技術的困難が生じたり、また、回線事情の好転、OSIの普及、コンピュータOSの統一化等、従来よりも保有を容易にする要因も発生すると考えられる。

いずれにしても、バックアップ対策実施の困難性、容易性にかかわらず、バックアップ対策ニーズは必ず向上していくと考えられる。ただし、その向上速度は事故・災害の発生や景気の変動、その他に影響され非常に予測困難である。

あえて、バックアップ対策ニーズの拡大状況を時系列で予測してみると次のように考えられる。

1990年代前半：浸透期・啓蒙期；先進コンピュータユーザが対策を実施し、徐々に浸透して行く。

1990年代後半：発展期；一般コンピュータユーザも対策を実施し、常識化する。

2000年～

2010年：定着期；すでにほとんどのコンピュータユーザが対策を実施している状況で手段の改良、高度化が進むのみとなる。

#### (b) バックアップサービスニーズの状況

バックアップ対策ニーズが、今後、大きく顕在化して行く時、経済性、効率性、便利性からそのほとんどは、外部専門業者のバックアップサービスを要望することは明らかである。そして、最初は初歩的で超低コストのバックアップサービス、すなわち、保有のためのコンサルティングや簡単なシステムのバックアップのニーズであり、発展期、定着期には、有効性を十分考慮したユーザニーズ多様化に対応できるサービスが要望されると考えられる。

#### (2) バックアップサービス提供の状況

バックアップサービスを事業としているのは現在1社であるが、今後ニーズの増加により、専門業者として新しくスタートするもの、また、従来より広義のバックアップサービスを一部事業として行っていたものがその比重を増し、当事業をメインとして参入する等、バックアップサービス業者がかなり増加すると予想される。

たとえば、従来コンピュータセキュリティコンサルティングの一部にバックアップシステム保有のコンサルティングを行っていたものが、1分野独立して、これのみを行うこともバックアップサービス提供であるし、また、ユーザサービスでバックアップサービスを行っていたコンピュータメーカーが事業として行うようなこと、あるいは、コンピュータビル賃貸業者がバックアップマシン専用ビルとし、付加機能をつけて専用バックアップファシリティを提供する等のことも考えられる。いずれにしても2000年代には、各種サービスについて各々独自性、優位性を発揮して競われる状況になるであろう。

現在のところバックアップサービスとして目立ったものになるであろうと予測されるものとして次のものが考えられる。

- ・バックアップシステム保有コンサルティング
- ・バックアップデータの伝送受信サービス
- ・専用バックアップシステムの運営受託サービス
- ・衛星通信、高速デジタル回線を使ったリモートバックアップサービス

#### (3) 2010年の市場規模の推定

市場の拡大状況は、前述どおりの動向が予測されるので、2000年までは現在のコンピュータのニーズ顕在化を中心に検討し、2000年から2010年は、一定伸び率で算出してみる。

##### (a) 2000年での市場規模推定

昭和61年国内の型別コンピュータ保有事業所数は、

大型 4,130社

中型 15,730社

である。

毎年、増加しているが簡単にするため、伸び率を無視して2000年も同数として計算する。

バックアップサービス利用希望事業所数は、アンケート調査では、

大型 71.6%

中型 63.4%

であった。

2000年には、バックアップ対策は普遍化し、常識化するとはいうものの、利用率はこれの80%と考えるのが妥当と考える。

したがって、バックアップサービス利用事業社数は、

大型  $4,130(\text{社}) \times 0.716 \times 0.8 = 2,365$ 社

中型  $15,730(\text{社}) \times 0.634 \times 0.8 = 7,978$ 社

大型のバックアップサービス利用金額を年間1,500万円、中型のバックアップサービス利用金額を800万円とすると推定市場金額は、

$2,365(\text{社}) \times 1,500\text{万円} + 7,978(\text{社}) \times 800\text{万円} = 9,929,900\text{万円}$

したがって、2000年での市場規模は1,000億円と推定される。

(b) 2000年から2010年までの市場規模の推定

2000年から2010年までは、バックアップシステムの改良、高度化のニーズに対するサービス提供であり、伸び率は毎年10%程度と推定し計算をすると2010年には、2,357億円となる。

したがって、2010年には、大略2,400億円の市場となっていると推定される。

## 9. ファシリティマネジメントサービス

現在、情報システムの運用管理は、一部システムのオペレーションを中心に外部に運用管理サービスを委託しなければならない状況にある。

また、システムの高度化、複雑化が進み、情報システムの運用ばかりでなく電源、空調設備の運用もシステムの信頼性に影響を与えつつある。つまりこの情報システムの運用をサポートしている安定化電源設備（非常用電源設備）、空調設備また通信ネットワーク等の安定稼動がシステムの安定稼動のための1つの要因となってきた。

さらに、セキュリティ管理面でも、システム運用管理、ファイル管理等、ますます高度化・複雑化していく中で、いかに安全を確保するか、緊急に解決しなければならない現状である。

このため、自社でこれからの運用に関して専門家の雇用と育成を行い、実行するには種々の問題があるだろう。次第に専門企業に業務委託をすると考えられる。

ファシリティマネジメントサービスは、これに対応するため現在の個別サービスから、総合化され、総合運用管理サービスとなり、システム構築までそのサービス範囲に含むようになるだろう。いわゆるS Iの方向へ向かうものとする。すなわち、次のような項目がある。

- ① ホストコンピュータシステムの総合運営管理サービス
- ② ソフトウェアの保守管理サービス
- ③ ハードウェアの保守管理サービス
- ④ 設備運用管理サービス
- ⑤ 安全管理サービス
- ⑥ システム構築サービス

### 9. 1 ファシリティマネジメントサービスについて

#### (1) サービスの現状

##### (a) アメリカにおける考え方（情報サービス産業白書1989より）

アメリカにおける情報サービス産業の分類の1つにプロフェッショナルサービスがあり、

- ・ファシリティマネジメント
- ・受託ソフトウェア開発
- ・コンサルテーション
- ・教育・訓練

をこの分野のサービスとしている。

このサービスは、他の分野……情報処理サービス、ソフトウェアプロダクト、Value Added Resale……に比べ極めて専門色が強く、利益を生み出す資源としての特長を持っているとされている。本サービスを提供する企業は、トータルな問題解決を提供する企業としての地位が確立されている。そして、従来の単純なプログラム処理等による量的拡大戦略から、質的向上戦略へと戦略転換が図れ、企業のレベルアップにつながる。さらに、

- ・高レベルのシステムエンジニアの育成が図れる
- ・高付加価値の業務への移行による収益性、生産性の向上が可能になる
- ・エンジニアの階層構造化が実現し、技術企業としてのキャリアパスが確立する

といった利点が、呼び起こされるとしている。

(b) わが国の現状

わが国では、アメリカにおけるサービスの実態（本報告で定義するサービス）にはいまだ到達していないのが現状であろう。しかし、個別に見たとき、システム等管理運営委託、労働者派遣、ビル管理サービス、警備サービス等、すでに情報システム運営に深く携わっており、これを総合化専門化することにより、高いスキルレベルに到達するものと期待できる。

(c) セキュリティとの係わり

システム等管理運営サービスは、セキュリティとは直接認識されないで、1つの産業分野を形成している。しかし、労働者派遣等も含めシステム運用に深く携わっており、のサービスは、セキュリティに対し何ら関係がないとするのは非常に危険である。これらの分野は、存在そのものがセキュリティをベースにしたものであると認識する必要がある。つまりこのファシリティマネジメントサービスは、情報システム運営に掛かるセキュリティサービスそのものであり、かつ高レベルの専門家集団であることができる。

このような認識に立ったとき、現状ははなはだ問題が多いと言えよう。諸安全対策基準は、これらのサービスを受けるとき、外部委託として、委託契約時に委託先にも発注者と同じレベルのセキュリティ水準を求めているものも、この認識によるものであろう。

(2) 今後の動向

情報システムは、社会活動のインフラストラクチャになるに従い、その運営に対する考え方は厳しくなり、セキュリティへの期待は増大するであろう。これに対応して、情報システムの運営方法も大きく変わってくるであろう。

(a) 都市機能の変化

東京等の大都市は、情報の集中化等でその機能を高度化し、本社機能等企业活動の中核となり、高度な判断・決定のために必要な人・設備等が集中するであろう。この結果、情報システムを設置するための、フロアスペース、コストはそれを許さなくなってくると思われる。

一方、地方都市においては、地域産業の活性化のため、企業誘致、情報団地の造成等の施策を実行し、情報システム運営本体の地方進出が容易になる下地ができはじめるだろう。

(b) 生活環境の変化

日常生活においては、アメニティ指向がますます強くなる。このため、豊かな生活空間を求めて地方都市へ移住、また、サテライトオフィス、リゾートオフィス、在宅勤務は、大都市圏への極度の人口集中を避ける傾向に拍車をかけることになる。

この結果、大都市において情報システムを維持管理する要員を確保することが困難になってくるであろう。

(c) 技術の進捗

① 通信ネットワーク

通信ネットワークは、高速大容量化が実現し、高信頼度、高密度化し、さらに通信コストの低下もみて、ネットワークの利用において、情報システムの処理速度からみて何ら支障のないレベルに達するであろう。

② 情報システムの運転管理

情報システム本体の運転管理は、ほぼ自動化が完了し、バックアップテープ等分散管理用の媒体のハンドリング、センタジャーナルデータの取り出し等一部の作業を除き、シス

テムの管理に直接人手がかかることはなくなった。このためシステムを利用部門の近くに設置する必要はなくなってきた。

(d) 社会的必然性（リスク分散）

わが国においては、地震を始めとする自然災害に対し十分な対策が必要とされ、リスク分散が真剣に検討されはじめた。現在はいまだ企業内でのリスク分散であるが、これが社会的必然性として要請されるようになってくる。

(e) 企業ニーズ

アメリカにおけるプロフェッショナルサービスでみたように、情報サービス産業は、高付加価値による収益性、生産性改善の方向として、本サービスを指向してくるだろう。企業として単純な量的拡大による企業戦略から、質的拡大による企業戦略に変化するのとは必然的なことであろう。

(3) 利用形態

社会情勢（ニーズ）の変化は、企業自身が情報システムを設置運用することから、セキュリティスキルの高い、技術スキルのある専門企業に業務委託する方向へと変わって行くであろう。この利用形態は、企業の規模により変わると思われる。

(a) 利用形態 I

大企業等においては、複数の地方に情報システムを自ら設置し、本サービスを受けるだろう。システムは大都市にある管理中枢から直接指示されるだろう（図8）。

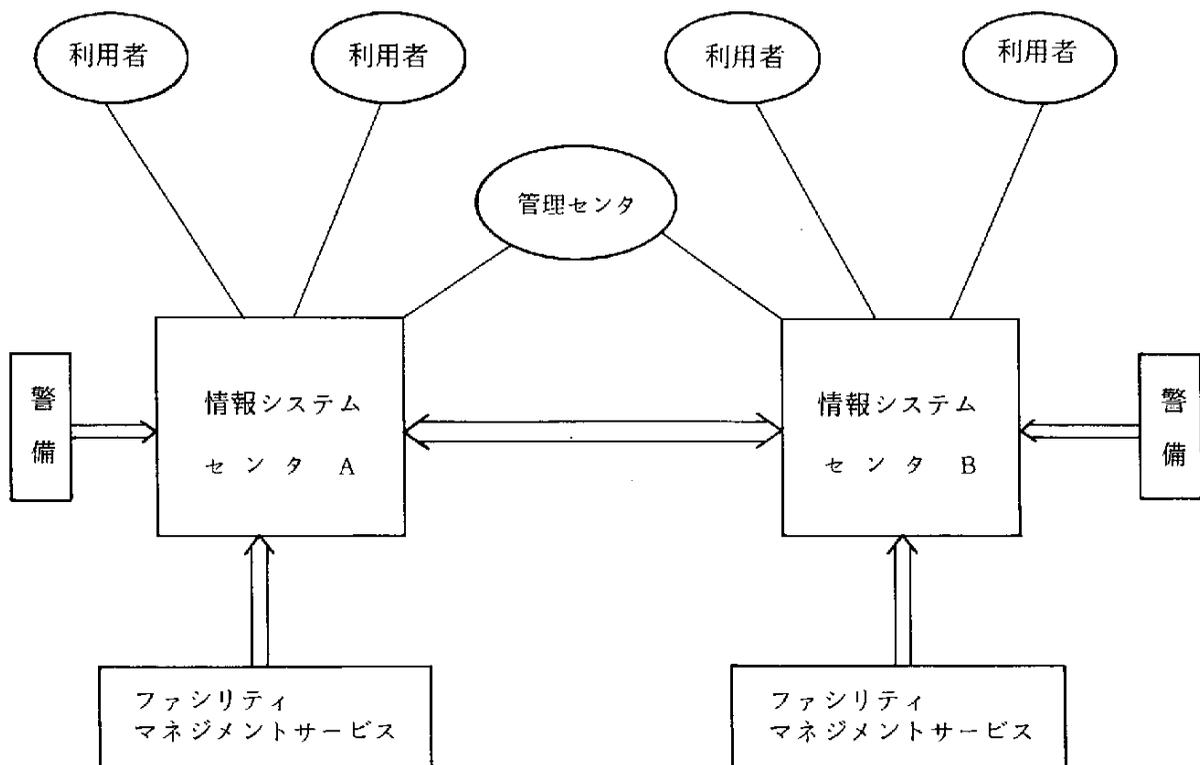


図8. 利用形態 I

(b) 利用形態Ⅱ

中小企業等においては、自社で情報システムを設置することもあるだろうが、建物、リスク分散のための情報システムの設置は、このようなサービスを受けるであろう（図9）。

(c) 利用形態Ⅲ

ファシリティマネジメントサービス企業が情報システムを設置し、全てのサービスを提供し、利用者はこれを使用することが便利なこともある。

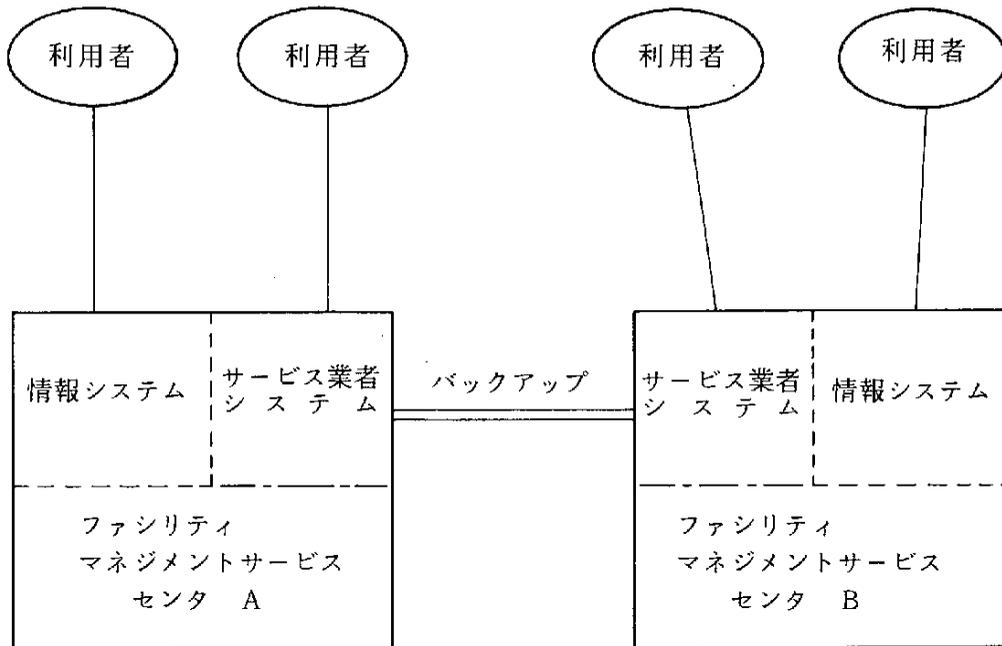


図9. 利用形態Ⅱ・Ⅲ

9. 2 ファシリティマネジメントサービスの市場規模の推定

(1) 現 状

ここで定義した総合的なサービスはほとんど存在しないが、個別には、先に述べたようにそれぞれ存在している。オペレータ等労働者派遣を含めると大きな市場といえる。これをセキュリティ産業と分離できないので、これを現状の市場とした。

1987年度のデータが情報サービス産業白書1989に報告されている。1989年度については、次に述べる過去の推移のデータから推定した。

これ以外に警備、設備等運営管理サービス等があるが、現状は、サービス実態はあるもののいまだ本研究で検討している業態になっていないとして、割愛した。

(2) 市場規模の推定予測根拠

(a) 過去の推移

情報システムのシステム等管理運営委託の1975年から1987年の売上高を図10に示す（情報サービス産業白書1989）。

ここで1985年の低下は、有力な調査対象企業の補足もれ、1987年は労働者派遣による売上高の別途計上によるものと解説されている。

単純にこの機関の数値だけで伸び率を計算すると、年平均29.5%に達する。1983年からの伸びはあまり高くないが、一応計算すると3.1%である。

1989年の売上は、一応この2つの数値の単純平均とした。

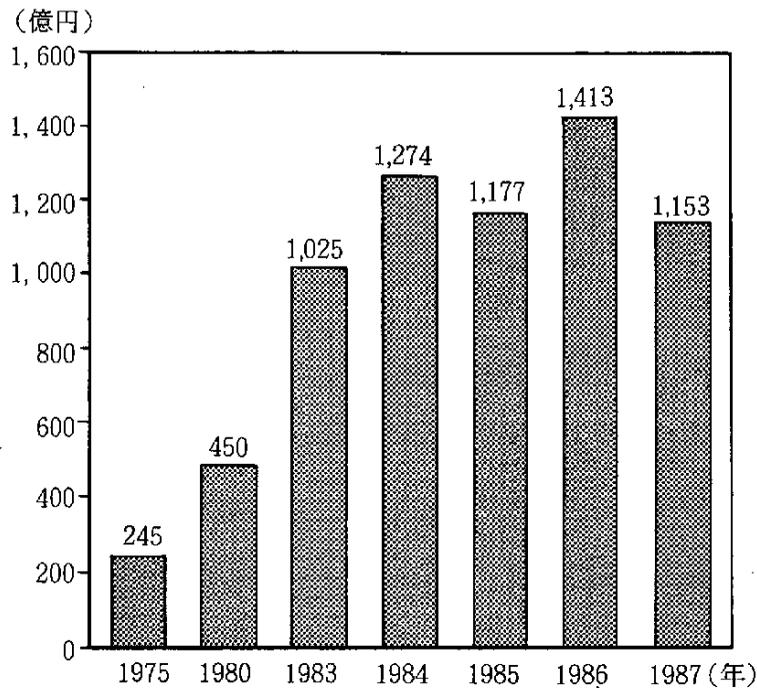


図10. 過去の推移

(b) 今後の推移 (1990~2000)

この10年間で、徐々にここで述べるサービスが提供されはじめるであろう。

しかし、いまだ事業として形成されたとはいいい難く、ここでは情報サービス産業分野に限定した(1989年の推定と同じ)。

この期間の伸びも情報サービス産業白書1989によった。伸び率は13%と報告されている(図11)。

(c) 今後の推移 (2001~2010)

この10年でほぼサービスの実態が整うと考えられる。しかし、企業としては、参入間もない未成熟企業が雨後の竹の子のように乱立ぎみで、成熟した産業として整理統合されなければならないと思われる。

市場規模としては、前述したシステム等管理運営サービス、労働者派遣に加え、警備サービス、設備等管理保守サービス、ビル賃貸サービス等が加算されるだろう。

① システム等管理運営サービス

2010年までの伸びは、情報産業全体の伸びと比例するが、これまでの伸びに比べれば鈍化する。一方、成長期の分野にみられる激しい価格競争がここでもみられ、売上高的には、さほどでなく、一応10%程度と予測する。

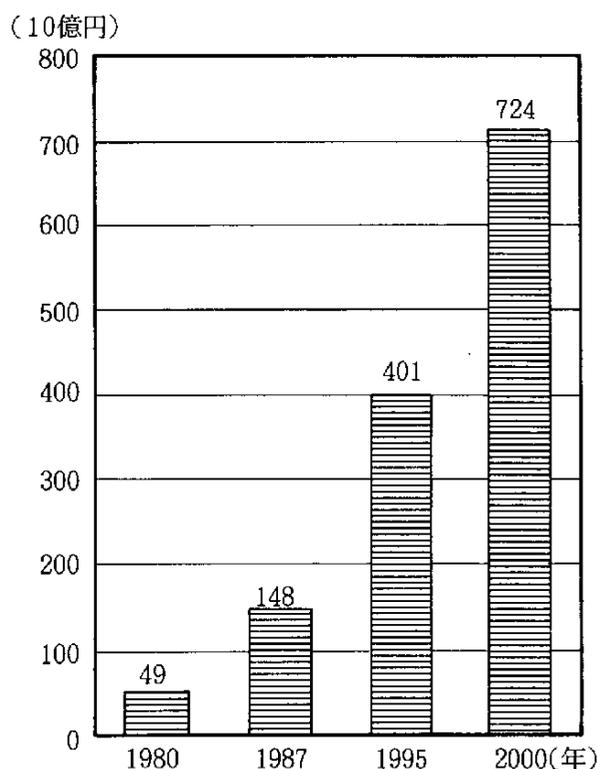


図11. 2000年までの伸び予測

② 労働者派遣

現在と同じような単純な労働者派遣は、内容的には存在するも、実態的にシステム等管理運営サービスに吸収されるであろう。つまり派遣される労働者も、セキュリティスキルの高い技術者とされ、高い付加価値が求められているからである。

③ 警備サービス

情報システムに対する警備サービスは、別項で報告される。

内数でみたとき次のように計算されるだろう。大型システムは、利用形態Iで述べたように、独自の契約となるだろう。その他の部分がこのサービスを受ける。金額としては、中型システムが情報システム全体の約20%、このうち50%が本サービスを受けるとする。

④ 設備等運営管理保守サービス

設備等運営管理保守サービスは、現在ほぼハードコストの0.2~0.04%程度である。今後この傾向は変わらないとし、さらに本サービスを受けるシステムはこのうち50%とした。

⑤ ビル賃貸サービス

ファシリティマネジメントサービス企業が自らビルを持ち、フロア貸与もサービスする。ここではいまだ計算するほどないので割愛した。

(3) 市場規模の推定

(a) 現状 (1989年)

システム等管理運営委託	156,600百万円
労働者派遣	188,100百万円
計	344,700百万円

(b) 2010年

システム等管理運営委託	1,877,900百万円
警備サービス	( 142,000百万円)
設備等管理運営保守サービス	25,600百万円
計	<hr/> 1,903,500百万円

(注) カッコ内は加算していない。

## 10. 教 育

セキュリティ産業の範疇としてとらえる教育は、一般的に、セキュリティ教育とセキュリティ対策を補完するという視点からのシステム監査教育をあげることができる。

### 10. 1 ビジネスとしての基盤

セキュリティ教育およびシステム監査教育は、共に、情報化社会の安定化のための基礎固めに重要であり、そのために認識が高まっているものである。したがって、これらの教育により、収益が向上するとか、新しいビジネスチャンスが生まれる等に直結するとは考えにくい。この点が、セキュリティ教育やシステム監査教育がビジネスとして成立しにくい一面である。

しかし、21世紀の情報化社会を想定した場合には、セキュリティ対策の重視されかたは今日の比ではなく、情報システムの前提条件としてセキュリティ対策が問われるようになるものと思われる。そのような時代になれば、基本的に教育問題がクローズアップされてくる。

まず、セキュリティ教育については、時々短期の講習会が行われている程度である。いずれも単発的に実施されており、定期的な開催はあまり見あたらないし、長期のコースは皆無である。現時点においてビジネスとして行われているセキュリティ教育を金額で把握したとしても、微々たるものと推定される。

つぎに、システム監査教育については、短期および長期（ただし毎日ではない）の講習会が定着しはじめているように見受けられる。一方では、通信教育もさかんに行われていて、この分野を取り扱っている大手の通信教育を営む企業が5社ほどあるが、受講者は年間約3～4,000人程度と思われる。

以上のような状況から、セキュリティ教育およびシステム監査教育の現在の総売上高は、わずかに5億円程度と推定される。

### 10. 2 これからの方向

上記のように、セキュリティ教育やシステム監査教育を独立した形で、しかもビジネスとして行うケースはまだ少ない。しかしながら、最近のコンピュータ教育あるいは情報処理教育とよばれるものとは、セキュリティやシステム監査が1コマ組み込まれるケースが非常に増えてきている。この傾向は、今後とも強くなるものと思われる。その過程では、当然、内容の充実も求められるようになるであろうから、セキュリティ教育やシステム監査教育が独立したコースとして成長していくものと期待される。

今日、情報化の進展はめざましく、情報化環境は常に変化している。このような社会情勢下において、セキュリティ対策およびシステム監査が、社会的な基盤整備として求められるようになっていくことも事実である。いずれにしても、長期的にはビジネスとしての展望も明るいといえる。

### 10. 3 大学教育の動向

セキュリティ教育にしろ、システム監査教育にしろ、その意識を高め、質的な向上をはかり、裾野を広げるという意味からは、大学教育に取り入れるのが効果的であろうと思われる。しかし、これらの講座を開設している大学はまれである。

わが国には、国公立と私立を合わせて 490の大学があり、このほか、短期大学が 571校ある（昭和64年版全国大学職員録、廣潤社）。この職員録で、各教官の「担当学科目」を調べてみた結果、情報セキュリティ論（名称は問わない）という講座は皆無で、システム監査論という講座が次の私立大学2校で開設されているのみである。

- ・横浜商科大学 商学部 経営情報学科
- ・南山大学 経営学部 情報管理学科

このように、大学における情報セキュリティやシステム監査の教育は、これから具体化しなければならないという、いわばスタートラインにいたばかりである。計画的な展開に期待される場所である。いずれにしても、今日、またこれからの情報化社会を考えた場合、これらの教育が大学で導入される必要性は高く、将来的には普及するものと思われる。

#### 10. 4 2010年の展望

以上のことから、セキュリティ産業の範疇におけるセキュリティ教育とシステム監査教育の、2010年の規模を予測すると、前半の10年は15パーセント程度の伸び率で、後半の10年が30パーセント位の伸び率と思われる。すなわち、前半の成長率はあまり高くなく、新規に参入してくる企業も少ないと思われる。しかし、後半になると、市場も大きくなり参入企業も増え、ビジネスとして成立するものと思われる。これらのことから、2010年のこの教育市場は、約 280億円位になるものと思われる。

## 11. コンサルティング

セキュリティ産業分野におけるコンサルティングとして、ここでは、セキュリティコンサルティングとシステム監査コンサルティングをとりあげることとした。その理由は、最近、情報産業分野に限らず、多くの業種において、情報システムによるコントロールが増え始め、それらの分野におけるセキュリティ関連のコンサルティング業務が出てきていることと、それと裏腹の関係にあるとも言えるセキュリティの状態の監査についてのニーズも出てきているからである。

ただし、わが国には、モノに対しては対価を支払うが、目に見えない頭脳労働に対してはなかなか対価を支払わないという慣習が長い間根づいてきているため、コンサルティングもビジネスになりにくいといわれている。この慣習も打破しなければならない重要な要素である。

### 11. 1 セキュリティコンサルティング

セキュリティコンサルティングについての最も明確な分野としては、通産省の安全対策実施事業所認定制度や、郵政省のネットワーク登録制度に基づく事業として、認定や登録をサポートするコンサルティングが成立している。しかし、この分野は、金額的にはさほど大きくない。

また、最近とくに変化し始めていることは、大規模システム開発に関して、セキュリティ面のコンサルティングを重視する傾向が見え始めたことである。しかし、まだ明確にシステムコンサルティングやシステム診断などといわれている分野から切り離されて、独立した分野に成長したとは言い切れない部分もある。だが、近い将来、この分野も必ず成立するものと思われる。

情報産業以外の分野においても、たとえば、インテリジェントビルやその他の工事施工についても、セキュリティ関連の工事が増加し、そのような場合の設計・施工についてもセキュリティコンサルティングが発生している。しかも、この分野は、金額的に非常に大きくなるのが特徴である。ただし、この分野は、社会的に明確に認知されないと、他の名目で計上されるため、金額的に把握できたとしても、他の分野と重複して計上する可能性がある。

### 11. 2 システム監査コンサルティング

わが国のシステム監査コンサルティングは、現在のところ、大手の監査法人がシステム監査部を設置して、ニュービジネスとして積極的に取り組んでいこうとする姿勢を見せて進出しているのが中心的な存在である。他には、情報サービス業において、社内のシステム監査を実施すると共に、システム監査コンサルティングビジネスにも進出するケースが現れている。なかには、システム開発過程において、システム監査人を配置して開発に当たるなど、サービスの差別化にシステム監査を取り入れている企業も出てきている。

システム監査コンサルティングとしては、現時点ですでにビジネスとして成立している部分と、独立したビジネスとまでは至っていないが、いずれ1つのビジネスとして成立するであろうと見込まれる部分とが混在している。いずれにしても、将来的には明るい分野であるといえる。

### 11. 3 2010年のコンサルティングビジネスの市場規模

セキュリティコンサルティングの市場は、前述の認定制度や登録制度に関連したコンサルティング分野が約5億円、システム開発に関連するセキュリティについてのコンサルティング分野が約20億円程度である。システム監査コンサルティングの市場は、大手の監査法人を中心に約5億

円程度である。

以上、現在の市場は、約30億円である。今後の伸び率は、個々の分野ごとに異なると思われる。元が小さいせいもあるが、今後10年間位は、全体として平均年率10%程度、その後の10年間は、平均年30%程度の成長が見込めるとと思われる。したがって、2010年のセキュリティ産業におけるコンサルティング分野の市場規模は、約 1,100億円になるものと推定される。

## 12. 警 備

### 12.1 警備市場の現状

#### (1) 警備業の概要

昭和61年12月現在の業者数は、4,282業者で警備員数が188,554名であったが、昭和63年12月現在では、業者数4,896業者、警備員数は218,880名に増加している。

また、警備業全体の昭和61年の売上高は、7,300億円であったが、昭和63年は、9,006億円と上昇している。

とくに、近年金融機関を始め各企業が週休2日制の導入を行い、休日夜間等における無人建物の増加、さらに独居老人、老人家庭、母子家庭の増加にともなう社会的弱者に対する福祉等のための需要が拡大された。

#### (2) 警備業の種別

警備業の種別は1号より4号までの4種類に分けられ、1号は、施設警備すなわち常駐警備と機械警備で警備業者は合わせて3,751社を占め、全警備員数も121,950人となっており、警備業の主力となっている。

2号は交通警備、3号は現金輸送警備、核燃料物資の警備、その他で、4号が身辺警備となっている。これに従事する警備業者数および警備者員数を表12に示す。

表12. 警備業の種別業者・警備員数

	種 類	適 用	業者数	警備員数[名]
1号	施 設 警 備	常駐警備	3,751	121,950
		機械警備	679	25,511
2号	交 通 警 備	交通警備・工事現物等	2,084	71,309
3号	現金輸送警備	現金及び貴重品の輸送	142	8,702
	核燃料物資等	核燃料・原子力施設等	8	507
	そ の 他		19	140
4号	身 辺 警 備	要人の警備	14	186

#### (3) 機械警備業の現状

全体警備業の中で、とくに情報化に関するのは機械警備業であることから、機械警備業の現状をみると、昭和63年12月現在で前年比41業者増(6.4%)の679業者になっており、全警備業者の13.9%を占めている。また対象施設(基地局、待機所)では前年比42,451施設(11.4%)の増となり、昭和63年12月現在416,295施設となっており、ますます増加の傾向を示している。

機械警備業者の規模別の状況を見ると、対象施設が200未満の警備業者が541業者で機械警備業者全体の79.7%を占めており、対象施設が2,000以上の業者は僅か23業者で全体の3.4%にすぎず、大半の業者はその地域に集中した業務を行っている。したがって、全国的なネットワークを利用した機械警備システムを実施している業者は極めて少数の企業といえる。

(以上、SECURITY TIME 1989. 7月号, 警察庁保安部防犯企画課 黒木一郎氏の“警備業の現

状と問題点等について”より)

## 1.2.2 2010年の警備市場の推定

現在の警備業界は、防犯防災を中心とした常駐警備から始まって現在に至っており、前段で述べたとおりいまだ全体の警備業の中で占める常駐警備の分野は65%を占めている。

本研究は、情報化社会に関連するセキュリティ産業として2010年を推定するので、ここでは機械警備を取りあげて、2010年の市場を推定することとする。

### (1) 警備内容の変革

#### (a) 高齢化

2010年における65歳以上の老人は、人口の20%を越えると推定される。この場合、在宅独り暮らし老人、寝たきり老人等に対する緊急セキュリティシステムが実施され、医療、救急を含めた社会的なシステムとして運用されることになるであろう。

また、健康な老人に対しても、健康管理システム、健康チェック等が日常できるようシステムが構築され、警備業者のあり方もシステムとヒューマンサービスの両面から多面化してくると思われる。

#### (b) ライフスタイルの変化

日本人の生活環境が、「より楽しく生活する」ために働くスタイルが変わってくると、休日の増加にともないレジャー産業がますます発展し、セカンドハウスも多くの人々が持つようになる。このようなライフスタイルの変化により、交通網の整備、移動時間の短縮化、それにとまなう情報が各個人単位で取られるようになる。ホームセキュリティの分野が大きく変化し、これらに対するセキュリティシステムと運用が必要になってくるであろう。

#### (c) インテリジェント化

事務所・マンション、倉庫等の建築物がインテリジェント化し、コンピュータも点から線に、線から面に、そして面から多角化に変貌していく。このようなハイテク化の中でのセキュリティは、事故が起きる前の予防的な運用がより行われなければならない。

#### (d) コンピュータ犯罪の増加

現在でも、すでに国際的なネットワークを使用したコンピュータウイルスの犯罪が発生し始めている。2010年の世界のネットワークは、さらに複雑化し多様化したものとなっているので、犯罪も場所と時間を越えて行われるようになる。この場合、日本だけの犯罪対策では防げなくなるので、国も民間も国際的な情報を基に防犯対策を行うとともに、民間の警備もハイグレードのセキュリティを持ち運用する必要がでてくるであろう。

#### (e) トータルセキュリティの確立

2010年の警備業は、機械システムと人間による対応、それにサービスを加えたトータルのセキュリティビジネスとして、情報化社会の変改にとまなうセキュリティニーズに応じて、それに対応して行く業界として確立されるであろう。

### (2) 機械警備市場の推定

昭和63年の全警備業売上高は、警察庁防犯企画課発表によれば、9,006億円、昭和61年7,300億円、昭和62年8,300億円となっている。

そのうち機械警備の物件数は、9%の伸び率である。

昭和62年末 373,844件

昭和63年末 416,295件

機械警備の63年の市場を予測するためには下記の方式を当てた。

警備料金は、レンタル契約であるため、上記件数より昭和63年6月(中旬)の数を推定し、これを395,070件とした。平均契約料を月額45,000円として12ヵ月を掛ける。

$395,070 \text{件} \times 45,000 \text{円} \times 12 \text{ヵ月} = 2,133 \text{億円}$

これに付帯する工事費は1件平均120,000円として、下記となる。

$(416,295 \text{件} - 373,844 \text{件}) \times 120,000 \text{円} = 51 \text{億円}$

2010年までの推定年間伸び率は10%とすると、2010年の推定市場は表13のとおりとなる。

表13. 2010年の機械警備業の予測

(単位：億円)

年	機械警備全体	内 訳	
		警 備 料	工 事
1988	2,184	2,133	51
2010	17,778	17,363	415

## 13. 保 険

### 13.1 情報システムに利用されている保険

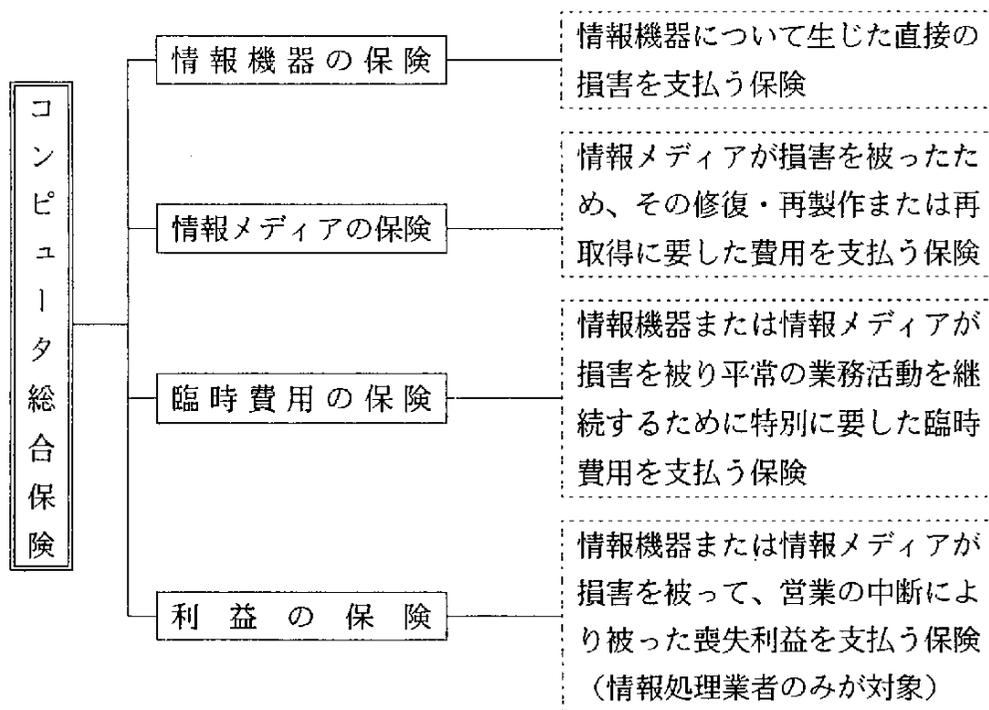
昭和50年9月に情報化保険が発表された。情報システムに付保されている保険は、企業が自ら所有する情報システムについては、動産総合保険、または火災保険が多く利用され、リース物件についてはリース会社が動産総合保険を付保しているケースが圧倒的に多い。これは賠償責任保険を別として、コンピュータ総合保険が従来の動産総合保険をベースに考えられている事などにより、両者の差異が大きくなることに起因していると思われる。両者の保険料率は次のとおりである。

① 動産総合保険／火災保険

保険料は、保険金1,000円について、1.8円～2.4円程度

② コンピュータ総合保険

保険料は、保険金1,000円について、2.4円～3.6円（情報機器）、臨時費用（4円～10円）、メディア（2円～3円）、平均3.3円程度である（条件により料率が変わる）。

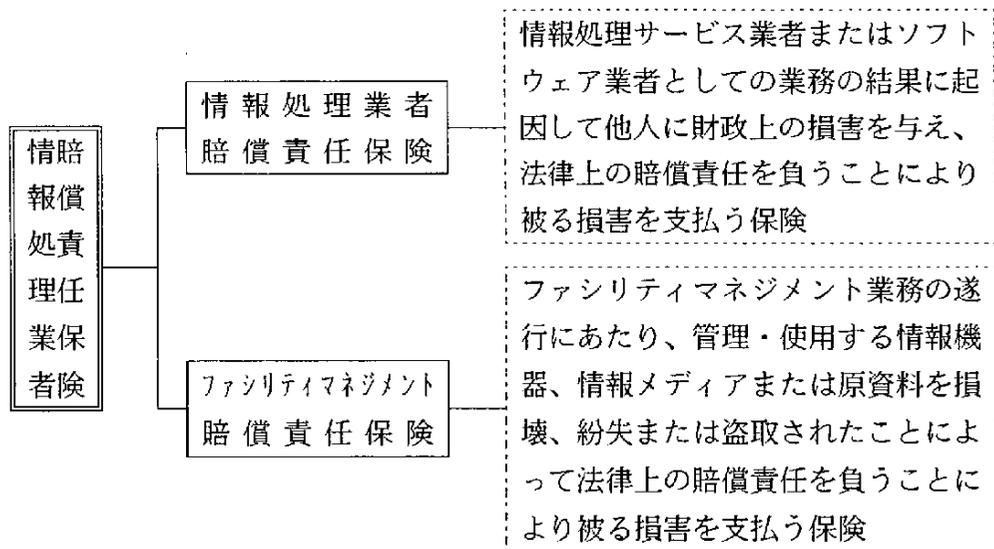


(注) 契約者は上記4つの担保条項のうち、希望する保険を選択して、付保することができる（ただし、臨時費用、利益の保険については、実務上は情報機器または情報メディアの保険に付帯して引き受けることが原則となっている）。

図12. コンピュータ総合保険の構成

③ 情報処理業者賠償責任保険

保険料は、売上高、てん補限度額、免責額により変わるが、てん補額1,000円に対し2.7～10円程度である。



### 13.2 付保の現状

昭和62年度、わが国のコンピュータ総合保険の売上は約20億円、賠償責任保険は4,000万円程度である。また、ユーザの選択した付保対象は、昭和61年5月、JECC（日本電子計算機㈱）ユーザの調査結果は表14のとおりである。

表14. 保険対策

システム合計（付保ユーザ件数 1,037件）

	建 物		電子計算機		機 械 室 専用設備		ドキュメント		情報メディア		臨時費用		喪失利益		損害賠償		合 計	
	件数	%	件数	%	件数	%	件数	%	件数	%	件数	%	件数	%	件数	%	件数	%
火災保険	951	100.0	151	61.1	188	77.7	18	51.4	23	34.8	0	—	8	47.1	0	—	1,339	83.9
動産総合保険	0	—	72	29.1	42	17.4	4	11.4	12	18.2	0	—	0	—	0	—	130	8.2
情報化保険	0	—	15	6.1	10	4.1	13	37.1	29	43.9	24	96.0	7	41.2	8	66.7	105	6.6
その他保険	0	—	9	3.6	2	0.8	0	—	2	3.0	1	4.0	2	11.8	4	33.3	20	1.3
合 計	951	100.0	247	100.0	242	100.0	35	100.0	66	100.0	25	100.0	17	100.0	12	100.0	1,595	100.0

(1986. 5 JECC調査)

件数で情報化保険が6.6%であるので、これを金額に置き換えて、ユーザの所有する情報システム全体の保険料に予測すると次のようになる。

$$20億4,000万円 \times \frac{100}{6.6} = 309億円$$

この額に、リース会社資産への付保分が加わる。すなわち、リース会社資産を全ハードウェアの70%として、同様に件数から金額に置き換えて計算すると次のようになる。

$$309億円 \times \frac{247件}{1,595件} \times \frac{70}{30} = 117億円（ハードのみ）$$

以上、309億円と117億円を加えて、合計426億円（ハードウェア165億円、その他261億円）が、

わが国における情報システム全体に掛けられた年間保険料と推定される。

### 1.3.3 保険市場の将来

#### (1) 情報化の成熟に伴う市場へのインパクト

保険商品を構成する基本的要件は、次の3点であるといえる。

- ① 事故が客観的に確認でき損害額も定量的に把握できること。
- ② 各種の危険や損害について偶発的なものを対象とすること。
- ③ モラルリスク（保険金搾取）の排除が可能であること。

これらの要件が満たされないため、従来不可能であった分野に、技術の進展と社会的なコンセンサスから適用できるようになる新保険が誕生する可能性が高い（動産総合保険からの離陸）。

#### (2) 賠償責任保険等プロフェッショナル向保険のニーズ

現時点におけるこの分野での実績は極めて低い状態（前述426億円うち4,000万円程度）である。しかし、情報サービス業の発展とともに増大する面と、企業自身の活動の中で必要が高まってくる面の双方からの需要が、この4～5年の間に急速に高まるであろうと思われる。すなわち、付保対象が物（コンピュータ設備）からサービス（ソフト）へ転換されていく面がでてくるであろう。

#### (3) リスクマネジメントとしての需要の増加

賠償責任保険へのこの面からのニーズは、情報システムの利用面での多様化や多接点化にともない、適用業務によっては、現在でも重要な問題である。少なくとも臨時費用保険と合わせて、近い将来セキュリティに投入する付加コストに占める保険料の割合は大幅に上昇するであろう。

#### (4) 2010年の情報システムの保険市場

1987年（62年）について、前述のように426億円を推定したが、2010年（23年後）については次のように予測した。

$$426\text{億円} \times (1 + 0.10)^{13} = 1,470\text{億円 (2000年)}$$

$$1,470\text{億円} \times (1 + 0.10)^{10} = 3,812\text{億円 (2010年)}$$

汎用ハードウェアの実働額の増加傾向は、55年から62年の7年間、平均伸び率は13.5%である。一方、情報処理産業の成長は、汎用ハードウェアの伸び率を上回り、この10年間20%台に達している。

このように、汎用ハードウェアの実働金額や情報処理産業の著しい成長を背景とする面と、(4)で上げた保険に対するニーズの変革による面の2面から、2010年における情報システムに係る保険市場は約3,800億円と予想される。

## 14. コンピュータ専用ビル

### 14.1 現状認識

情報通信システムの規模の拡大にともなって、金融機関を中心にコンピュータセンタ（専用ビル）が建設されてきた。近年は都心地区の地価の高騰やオフィスの賃貸料の上昇のため、コンピュータ部門あるいはコンピュータシステムを郊外、周辺地区へ移転させる企業が増加してきており、建設はますます盛んになりつつある。いわば、コンピュータ機器をコストの高いオフィスに設置する必要はないという考え方が、経営者の共通認識になってきたからであろう。もちろん、その分、通信コストが低下してきたという裏付けがでてきたからである。その上、専用ビル化することによって、設備機器や管理システム等をより合目的的に装備することが可能となり、高機能・高性能で、かつ、より安全な空間を確保できるからである。

一方、都心地区であっても立地条件の悪い土地は、たとえオフィスビルを建設したくても入居企業が集まらないため、周辺より安い賃貸料を設定するか、あるいは他の施設を建設することが一般的であった。そこで生まれてきたアイデアがコンピュータ専用の賃貸ビルである。1社で単独にコンピュータセンタを建設するほどの規模のシステムを保有していない企業や、コンピュータシステムの拡大のスピードが速すぎるためその設置スペースに不足をきたした企業等を顧客とするものである。ビルのオーナーにしてみれば、このような付加価値を付けることによって周辺と同程度の賃貸料を確保することができることとなる。

このような賃貸ビルは、前述のように合目的設計・建設されていることから、最大の特長の1つがセキュリティであるといつてよい。一般の事務所ビルでは享受できないような多面的に検討されたセキュリティ対策が装備されているからである。この意味でコンピュータ専用ビルの賃貸は、ある種のセキュリティビジネスであるといえよう。

なお、現在、コンピュータ専用の賃貸ビルは、首都圏に10数棟、京阪神に4棟、名古屋に1棟建設されている程度であり、確立した市場とは必ずしもいえない状況にある。

### 14.2 現状の市場規模

- ① 現在計画中の賃貸用コンピュータ専用ビルは、4件であり、延べ床面積は合計で約45,000㎡（約13,600坪）である。
- ② したがって、これらの現在の建設市場であると仮定するならば、その規模は次のようになる。  
 $13,600\text{坪} \times 150\text{万円} \times 1.3 = \text{約}300\text{億円}$ 
  - ・一般の事務所ビルの建設工事単価：150万円/坪
  - ・コンピュータ専用ビルの場合：一般のオフィスの30%高
- ③ 現在賃貸中の専用ビルは全国で約20棟である。これらの総床面積は、1棟当たりの床面積を約10,000㎡（約3,500坪）と仮定するならば、賃貸料の相場が坪当たり13,000～15,000円/月であることから、次のようになる。

$$3,500\text{坪} \times 20 \times 15,000 \times 12\text{ヵ月} = \text{約}130\text{億円}$$

#### 14.3 2010年における市場規模

- ① 「工事施工およびメンテナンス」で述べるように、事務所ビルはコンピュータ機器が主体のコンピュータ専用ビルと人間主体のオフィスビルとに分化していくものと想定される。

コンピュータセンタ（専用ビル）は、現在はほとんどが自社ビルであるが、今後は次の理由により、賃貸用の専用ビルが増加するものと考ええる。

- ・設備投資が巨額になるため、規模の効果が出てくる
- ・バックアップセンタの設置の増加
- ・情報システム部門の独立、小規模企業の大型コンピュータ保有の増加

など比較的小規模なスペース需要の増加が予想される。

したがって、2010年においてはコンピュータ専用ビルの30%が賃貸用となるものと仮定する。

- ② 2010年におけるコンピュータ専用ビル建設工事費の想定は、4,000億円である（工事施工およびメンテナンスを参照）。したがって、賃貸用コンピュータ専用ビルは、次のようになる。

$$4,000\text{億円} \times 0.3 = 1,200\text{億円}$$

- ③ 現在から2010年までの約20年間、賃貸用ビルの建設工事量の伸びが一定であると仮定すれば、2010年までの賃貸用コンピュータ専用ビルの総量は、次のようになる。

$$(300 + 1,200) \times 20 \div 2 = 1\text{兆}5,000\text{億円}$$

- ④ 現在賃貸中の専用ビル20棟の建設工事費は、オフィスビルの坪当たり単価の平均を100万円とすれば、次のようになる。

$$3,500\text{坪} \times 20\text{棟} \times 100\text{万円} \times 1.3 = 900\text{億円}$$

このような建設工事費のビルからの賃貸料収入が、年間130億円であるというわけであるから、賃貸料収入の価格構造が現在と変わらないものと想定すれば、次のようになる。

$$130\text{億円} \times (1\text{兆}5,000\text{億円} \div 900\text{億円}) = 2,200\text{億円}$$

## 15. 工事施工およびメンテナンス

### 15. 1 現状認識

近年、企業の経営環境はますます複雑化し、絶えず変化している状況にある。このような経営環境の変化をいかに早く把握し、的確に対応するかが企業経営上の最大の問題であり、場合によっては企業の存続をも危うくしかねない。このようなところから、企業における情報処理の迅速化、意思決定者に対する情報提供の質的向上の必要性が非常に高まってきているのは当然のことといえよう。一方近年、エレクトロニクス技術の発達には目覚ましいものがあり、情報通信機器の利用が急速に普及し、日常生活の隅々までコンピュータシステムが入り込んできた。いわゆる高度情報化社会の到来である。

このように、情報通信機器は企業活動にとって必要不可欠のものとなり、かつ大きなウエイトを占めつつあることから、オフィス内にはOA機器が氾濫し、巨大なコンピュータシステムが装備され、24時間稼動するような状況が生まれてきている。反面いろいろな問題も発生してきた。いわゆるオフィス環境の悪化であり、防災・防犯対策など諸設備の必要性の増大である。一方、オイルショック時に大きな問題となった建物の省エネルギー化要求は、建物オーナーの運営コスト低減要求と相俟って、ビル設備監視システムの普及をもたらした。

この結果、情報通信機器が重装備されることをあらかじめ想定し、その更新へのフレキシビリティを有すると共に、オフィス環境の高度化を計り、オフィス業務の生産性向上に寄与するような情報通信サービスを組み込んだインテリジェントビルが生まれ、一般化してきた。このようなインテリジェントビル自体コンピュータで制御され、管理されるようになるのは当然である。

このように、ビル内に装備されるさまざまな情報通信システムに対して、建設工事として組み込まれるセキュリティ対策は、基本的には通産省の電子計算機システム安全対策基準を始めとする諸基準に沿ったものとなるが、概ね次のような項目があげられよう。

#### (1) 災害対策

- |         |  |
|---------|--|
| ① 従業員確保 | ・ 飲料水、非常食の保持方法等  |
| ② 停電対策  | ・ 発電機、燃料の確保等<br>・ 冷却水の確保   |
| ③ 出水対策  | ・ 防潮設備、地階への浸水防止<br>・ 内部漏水対策（床防水、漏水検知機の設置）<br>・ 排水設備の設置   |
| ④ 火災対策  | ・ 内部不燃化<br>・ 延焼防止対策（防火区画）<br>・ 近火対策（外壁）<br>・ 消火方法<br>・ 耐火・防水保管庫  |
| ⑤ 地震対策  | ・ 建物自体および設備機器の耐震設計<br>・ フリーアクセスフロア対策（免震、脱落防止）<br>・ コンピュータ機器および家具什器類の転倒防止<br>・ 各種設備機器、天井材等の取付方法（配管類も含む） |

- ⑥ 落雷対策                   ・避雷設備
- ⑦ 大気汚染                   ・外気清浄化装置

(2) 防犯対策

- ① 人間の出入               ・ I Cカード他による入退出管理システム（門、玄関、執務室、コンピュータ室、エレベータ、階段等）
- ・ 外注要員・物品搬出入業者の区別（アクセスルート執務スペース）
- ② 車の出入                 ・ I Cカード他による入退出管理システム
- ③ 不審者の監視           ・ I T V遠隔監視、赤外線センサ等による検知
- ・ 在館人員管理システム、時間外勤務管理
- ・ 駐車場監視システム（不審車の発見）
- ④ 外部開口部の補強       ・ 外壁、重量スチールドアシャッター、窓
- ⑤ 機密管理                 ・ 保管庫、鍵管理システム
- ・ 建物の電磁波シールド、磁気シールド

(3) その他諸設備の故障対策

- ① コンピュータ電源       ・ C V C Fおよびその予備機の設置、並列運転
- ・ C V C F用バッテリー装置の設置
- ・ 幹線配線の二重化、階別系統分け
- ・ ノイズカット対策
- ② 通信回線                 ・ 局線二重化にともなう引込み口の二重化
- ③ 受電・変電設備         ・ 二系統引込み、ループ受電
- ・ 変・配電機器の予備機の設置
- ④ 熱源                     ・ 冷凍機の予備機の設置
- ・ 冷水・温水蓄熱槽の設置
- ・ 冷温水配管の多重化
- ⑤ 空調機                  ・ 予備機の設置

(4) 管理システム

- ① 中央監視システム       ・ 設備稼動監視、防災集中監視、集中警備
- ② コミュニケーション    ・ 構内各スペースとビル管理センタとの連絡、構内ページングシステム

なお、これらのセキュリティ対策は、その建物に装備される情報通信システムの規模をどの程度に想定するかにより、当然そのグレードは異なってくる。

## 15. 2 建設工事におけるセキュリティ対策工事

建設工事におけるセキュリティ産業の市場規模については、建設市場そのものについての統計データも必ずしも十分でないこと、セキュリティ対策工事自体が最近まで特に意識されていたわけではなく、独立した一工事項目として必ずしも分類されていないこと等から、一般的に通用する基礎データはまったく存在しない状況にあるといっても過言ではない。したがって、市場の推定は、かなり大胆な仮説を設定したうえで類推を重ねたものとならざるを得ないのが実態である。以下に推定の方法について説明する。

なお、ここで推定できるセキュリティ工事量は、電気設備工事あるいは最近独立した工事項目となることもある情報通信設備工事の一部としてとらえられるものに限られる。すなわち、耐震工事のように元来建築工事であるもの、受電・変電工事のように電気設備工事として行われているもの等は対象外となる。ただし、コンピュータ専用ビルのようにその内容がとくにセキュリティ対策を意識した大規模なものであれば、算定の対象となってくる。

さらに、セキュリティ工事は、建設工事業者が担当している部分と、コンピュータメーカーが担当している部分とがあり、その分担が必ずしもはっきりしているわけではない。たとえば、工事発注者の自社使用ビルの場合、情報通信システム工事の大きな部分をコンピュータメーカーが施工していることが多い。このため、ここでもある種の想定をせざるを得ない。

### (1) 現状の市場規模予測のための前提条件

- ① 情報通信システムは、全ての用途の施設に組み込まれつつあり、当然そのセキュリティ対策工事も全ての施設に対して行われていると言えるが、用途によりかなりレベルが異なる。すなわち、工場や医療施設は本体設備と一体化してかなり重装備となっているが、反面住宅や教育施設はほとんど情報装備されていない状況にある。

したがって、ここでは事務所ビルを中間的装備の施設と想定し、事務所ビル工事におけるセキュリティ対策工事の比率が全施設における平均的比率を示しているものと仮定する。まず事務所ビルにおけるセキュリティ工事市場を算定し、その結果を他の用途の施設にも適用する方法で全セキュリティ工事市場規模を推定する。ただし、施設としては、工場、医療施設を対象として含め、住宅、店舗、学校等は含めないものとする。

- ② 事務所ビルにおける情報通信システムの装備もまた、施設の規模によりレベルが異なるものと想定する。すなわち、コンピュータ装備をほとんど意識していないビルには小規模なものが多くと考えられるし、逆に重装備を設計条件としているビルは、ほとんどが大規模ビルであるといえるからである。

したがって、ここでは事務所ビルをその規模により3つに大別する。

- ・小規模ビル：情報通信システムの装備を全く想定していないビル……2,000㎡未満。
- ・大規模ビル：大型コンピュータを保有し、大規模なシステムを装備するビル……10,000㎡以上。
- ・中規模ビル：中規模以下のコンピュータあるいは端末・OA機器群の装備想定しているビル……2,000～10,000㎡。

- ③ 大規模な情報通信システムの装備を想定しているビルにおける電気設備工事費は、建設工事費全体の20～40%を占めるものとする。

また、一般オフィス環境で設置されるような中小型コンピュータやOA機器が相当な台数装備されることを想定しているビル（複数テナントが入居する一般的な賃貸用インテリジェ

ントビルが代表的なもの)における電気設備工事費は、建設工事費全体の20%を占めるものとする。

- ④ 大規模ビルにおけるセキュリティ対策工事費は、電気設備工事費の30~40%を占めるものとする。また、中規模ビルの場合は、20%とする。
- ⑤ 事務所ビルの建設工事費単価は、建設延床面積により、次のとおりとする。
  - ・中規模ビル：1,500千円/坪
  - ・大規模ビル：1,800千円/坪
- ⑥ コンピュータメーカーが施工しているセキュリティ工事量は、建設工事業者の50%と想定する。

## (2) 現状の市場規模

- ① 1988年度事務所ビル建築着工床面積（建築着工統計より）
  - ・小規模ビル：2,820千坪
  - ・中規模ビル：1,715千坪
  - ・大規模ビル：1,040千坪
- ② 1988年度建築工事量（建築着工統計より）
  - ・全工事量：36兆2,500億円
  - ・事務所：3兆7,100億円
  - ・工場・医療施設：2兆9,800億円
- ③ 電気設備工事費
  - ・中規模ビル：1,500千円×1,715千坪×20%=5,200億円
  - ・大規模ビル：1,800千円×1,040千坪×(20~40%)=5,600億円
- ④ 事務所ビルにおける建設工事業者によるセキュリティ工事市場
  - ・中規模ビル：5,200億円×20%=1,000億円
  - ・大規模ビル：5,600億円×(30~40%)=2,000億円
  - 合計：1,000+2,000=3,000億円
- ⑤ 事務所ビルにおけるセキュリティ工事市場  
3,000×1.5=4,500億円
- ⑥ 全セキュリティ工事市場  
4,500×(3.71+2.98)÷3.71=8,100億円

## 15.3 2010年の市場規模予測

### (1) 市場規模予測のための前提条件

- ① 特殊な設備工事が必要となるような現在の大型コンピュータを中心とする大規模な情報通信システムは、コンピュータ専用ビルに装備されるようになる。一般のオフィスビルは人間にとっての居住環境を最優先に設計したものとなり、いわゆる執務スペースに設置されるような超小型の情報通信機器がふんだんに使用されているにすぎない状況となる。

すなわち、コンピュータ機器が主体のコンピュータ専用ビルと人間主体のオフィスビルとに分化していくものと想定する。

コンピュータ専用ビルにおいては、装備される情報通信システムが現在よりはるかに高度

化、複雑化していることは明らかであることから、電気設備工事費が大きく増加するものと予想される。したがって、建設工事費全体に占める比率は現在より増大し、40～60%に達するものと想定する。

一方、一般オフィスビルにおける建設工事費全体に占める電気設備工事費の比率は、現在と変わらないものと想定する。

- ② 情報の集積度が飛躍的に高まり、個人の生活から企業活動、政治経済の動き等全てに、しかも24時間常に情報通信システムが関わる状況となっている。当然、個々の情報通信機器・システムの信頼性も格段に向上しているが、施設に組み込まれるセキュリティシステムも一層高度化しているものと考えられる。とくに機密保護対策は、人間の意図的な行動に対応するものであり、本質的に「いたちごっこ」的にならざるを得ず、機密が損なわれた場合の損害の増大、情報へのアクセスの容易化とのトレードオフ的に増大する損失機会への対応等からいくらかでも高機能化、高性能化することは明らかである。

ex. 建物電磁シールド

顔、声による個人識別を利用したアクセス制御

機密情報媒体の廃棄システム（自動搬送・焼却システム）

したがって、セキュリティ対策工事費は当然増大するものと考えなければならないが、反面、個々の情報通信機器のセキュリティ対策が向上する分、工事費の負担が軽くなるとも考えられる。そこで、電気設備工事費に占めるセキュリティ対策工事費のウエイトは双方で相殺され、現在と変わらないものと想定するが、建築工事部分で増大する分があることを考慮して、建設工事費全体に占めるセキュリティ対策工事費の比率を若干増加させるものとする。

- ③ コンピュータ専用ビルに装備されるような大規模情報通信システムは、大型コンピュータが中核となっていると言えることから、大型コンピュータは全てコンピュータ専用ビルに設置されるものとする。

エレクトロニクス技術等の発達によりコンピュータの規模は、機能・性能に対するその物理的大きさは相対的に縮小しつつあるが、一方でシステム規模自体が拡大していることから、いわゆる「大型コンピュータシステム」の必要床面積はむしろ増大しているのが現状である。

そこで、ここでは、双方が同程度のスピードで進展するものと考え、2010年における「大型コンピュータシステム」の必要床面積は、現在と変わらないものとする。

- ④ 事務所ビル建設工事費におけるセキュリティ工事費の比率が、全施設の平均レベルであるという想定は変わらないものとする。したがって、事務所ビルにおける工事費推定結果を工場、医療施設に加えて、店舗、倉庫、学校他建築工事全体に当てはめることとする。ただし、建築工事全体に占める事務所ビルのウエイトは現在と変わらないものとする。

また、コンピュータメーカーが行うセキュリティ工事費は、建設工事業者の50%であるという想定は変わらないものとする。

## (2) 2010年の市場規模

- ① 2010年における建築工事費（財団法人国民経済研究協会長期経済予測）

・2000年における工事量：64兆7,000億円

・2010年における工事量：93兆9,500億円（2000年以降年3.8%伸び率想定）

- ② 2010年に事務所ビルの建設工事量

・全建築工事量に対する事務所ビルの比率：9.93%

(建築着工統計 1985～1988年度4年間の平均)

- ・したがって、事務所ビルの工事量は、次のようになる。

$$93兆9,500億円 \times 9.93\% = 9兆3,300億円$$

③ 2010年におけるコンピュータ専用ビル建設工事量

- ・現在の大型コンピュータ新規設置金額：9,500億円

コンピュータ総需要 1兆3,600億円の70% (電子産業ビジョン)

- ・情報通信システムの設置に必要な床面積は、システム金額1.5億円に対し約100㎡ (実例ベース) とすれば、必要床面積の総量は、次のとおりとなる。

$$9,500億円 \div 1.5億円 \times 100㎡ = 約200千坪$$

- ・コンピュータ専用ビルの建設工事費は、通常のオフィスビルの30%割増し。したがって、2010年におけるコンピュータ専用ビル建設工事費は、現在の価格で、次のとおりである。

$$200千坪 \times 150万円 \times 1.3 = 約4,000億円$$

④ 電気設備工事費

- ・コンピュータ専用ビル：4,000億円  $\times$  (40～60%) = 2,000億円

- ・一般オフィスビル：(9兆3,300億円 - 4,000億円)  $\times$  20% = 1兆7,900億円

⑤ 事務所ビルにおける建設工事業者によるセキュリティ工事市場

- ・コンピュータ専用ビル：2,000億円  $\times$  (30～40%) +  $\alpha$  = 1,000億円

- ・一般オフィスビル：1兆7,900億円  $\times$  20% +  $\alpha$  = 4,000億円

合計：1,000億円 + 4,000億円 = 5,000億円

⑥ 事務所ビルにおけるセキュリティ工事市場

$$5,000億円 \times 1.5 = 7,500億円$$

⑦ 全セキュリティ工事市場

$$7,500億円 \div 0.0993 = 7兆5,529億円$$

## 第4章 生活の情報化とセキュリティ

前章までに述べてきたことは、いわば企業を対象としたセキュリティニーズに基づく分野である。しかし、情報化という観点からは、生活（あるいは家庭）の情報化についてもセキュリティ対策が求められる時代となっている。すなわち、ホームオートメーションとかホームセキュリティと呼ばれる分野についても、セキュリティ対策の基本を確立する必要がある。この生活の情報化分野は、対象が全国の約4,000万世帯ということもあって、市場としては非常に大きく、魅力のあるものとなっている。

そこで、本プロジェクトでは、昭和62年度に「ライフスプリング計画」を立案した。すなわち、生活の情報化が進展し、情報化の弊害が家庭においても現れる可能性があるとするれば、それを事前に把握・分析し、情報化によって防止することを考えなければならない。生活の情報化は、これから本格化すると思われるので、この時点において生活の情報化におけるポリシーを明確にし、セキュリティプランを確立すに必要があるとの認識に立ってライフスプリング計画を検討したものである。

### 4.1 ライフスプリング計画の概念

生活の情報化は、個人生活の場における情報化であるから、個々人の豊さに対する欲求との関連が強い。しかし、一方では、その求める豊さが多様化し、一律ではなくなっていることも事実である。

人間の欲求については、心理学者マズロー（A.H. マズロー）が、自著「モチベーションとパーソナリティ」で、新しいモチベーション理論として、欲求段階理論を展開している。これは、心理学分野よりも経営学分野での方が知られている。マクレガー（D. McGregor）は、マズローのいう欲求をつぎの5段階に整理している。

- ①生理的欲求
- ②安全の欲求
- ③社会的欲求
- ④自我の欲求
- ⑤自己実現の欲求

安全の欲求とは、危険や脅威等からの防衛をさしている。そして、この基本的な欲求は、情報化社会においても同じである。しかし、情報化社会の場合は、生活の情報化自体が豊さを志向したものである点が異なり、豊さの中での安全の欲求であり、危険や脅威等からの防衛といっても自ずとそのレベルがちがうといえよう。

このようなことから、このライフスプリング計画は、生活の情報化でセキュリティ上の問題が発生すれば、被害を受けるのは個人であり、生命の危険にも及ぶことになる。すなわち、事前の手当が何よりも重要であることから、ライフスプリング計画を通じてこれらの諸問題の解決にあたりたいと考えたのが、研究の出発点である。

## 4. 2 ライフスプリング計画の展開

### (1) 基本理念

ライフスプリング計画を推進するにあたっては、具体化を図るための前提条件がある。それはつぎのとおりである。

#### (a) 基本的考え方

- ・生活の情報化を高める
- ・生活のためのセキュリティシステムを構築する
- ・生活関連システムのセキュリティ対策を構築する
- ・現役引退後の生活を豊かにする
- ・情報化の弊害は情報化で克服する

#### (b) ライフススプリング計画の5大テーマ

- ・安全性指向：安心して生活できる
- ・健全性指向：健康な生活ができる
- ・快適性指向：住みごこちがよい
- ・利便性指向：生活が便利である
- ・自由指向：気楽に生活できる

### (2) ラーフスプリング計画の骨格

この計画は、一定の地区を対象とすることを想定している。そして、居住区を小単位のゾーンに区分けし、その中心にZHSC（ゾーンヒューマンセキュリティセンタ）を設置して管理するシステムとする。

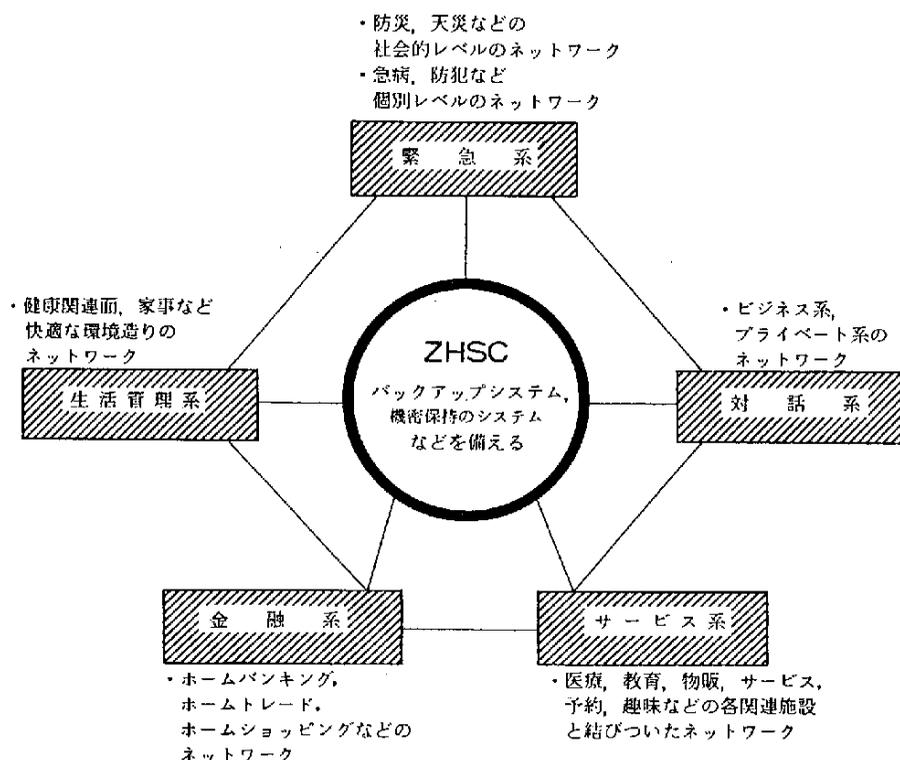


図13. ラーフスプリング計画の骨格

### (3) ZHSC

ZHSCは、ライフスリング計画を実現させるための中枢となるセンタであり、全てのサービスはZHSCを介して提供される。また、ZHSCは各居住区単位に構築されるコントロールタワーであり、快適な生活を維持するための各種システムとのインターフェイス（アクセスポイント）でもある。したがって、センタのハード・ソフトすべてに関して、万全のセキュリティ対策を実施する必要がある。

### (4) ライフステージの設定

2010年を代表するであろうライフスタイルのシーンを設定して、機能および住みごごち等を評価する必要がある。このため、次の7つのライフステージを描いた。

- ①ゾーンステージ：緊急避難システム
- ②使い分けライフ：夫婦の生活例
- ③フレキシブルライフ：子供ひとりの夫婦の生活例
- ④セーフティライフ：高齢者の生活例
- ⑤パーソナルライフ：シングル女性の生活例
- ⑥コンポーネントライフ：シングル男性の生活例
- ⑦グローバルライフ：ダブルインカム居住者の生活例

### (5) 個別メニュー例

#### (a) 統合監視通報システム

地震や水害などの天災、犯罪や火災などの人災など、有事における通報や避難・誘導が迅速かつ確実に伝達されることによって、被害や混乱が最小限に食い止められることは明らかである。

地震、水害などの天災の観測体制が確立され、予知の正確性も恒常するであろうから、通報体制もそれに並行して確立され、個人、家庭、社会全体に迅速・確実に避難の指示・誘導が伝達されることが肝要である。

ほとんどの監視、通報が自動化されているわけであるが、絶対にあってはならないのは、誤報と監視・通報システムジャックである。一度の誤報によって生じる社会全体の混乱は計り知れないものがある。誤報防止のため二重三重のチェック体制、システム停止や不良作動防止のための監視体制とバックアップ体制の確立には万全を期して対処すべきであろう。

また、これと同じく最優先で考えるべきものとしてシステムジャックや破壊活動に対するセキュリティの確立がある。システムジャックによるデータの破壊や、施設の破壊、不正情報の伝達などによる社会の混乱防止の確保が必要である。

総合監視システムのセキュリティ確保を支える安全な建築物の建設、コンピュータシステムの構築、これらの運転を支える電源設備や空気調和設備の安全性の確保はみな同一レベルで考えられるべきであって、どれかひとつでも低レベルであってはならない。

建築物の免震化や制震化による耐震性の確保、火災の超早期発見システムとQガス超高速消火システムによる火災予防により、総合監視システム、コンピュータシステム、電源設備、空気調和設備の安全性が確保できる。また諸設備、システムの連続運転のための電源設備の二重化や、長時間運転を確保した自家発電設備の整備と、空気調和設備の二重化により、セキュリ

ティの確保がより確実なものとなる。また防犯対策としてI T Vや各種センサ警報装置を組み込んだ監視設備の整備により、不審者の早期発見を行い、不正行為防止を図ることが重要である。

(b) 広域セキュリティシステム

ネットワーク化されたセキュリティシステムにより、国全体のセキュリティ情報、地域ごとのきめ細かいセキュリティ情報・医療情報などが、地域住民の日常生活における安全性確保のため、的確に地域住民に伝達されるように、情報システムの構築にあたっては、障害防止と障害排除対策に十分配慮することが必要である。そのためにはシステムの二重化やセンタの分散化、不正アクセスの排除とモニター等は最低限行わなくてはならない。

(c) 生活環境セキュリティシステム

水、空気、光、電波などの家庭生活に必要な要因の管理・保護を行うため、監視・モニター・分析・コントロール体制を整備し、環境状況を地域情報として常時提供する。

(d) ホームキーピングシステム

家庭内の諸設備の作動状況を監視し、故障箇所の早期発見・誤動作防止のために、警報機能の充実、自動回復機能の組み込みによるメンテナンスフリーシステムを確立する。

#### 4. 2 ライフスプリング計画の実現化

(1) 実現化へのステップ

ライフスプリング計画を実現させるためには、パイロットスタディを実施し、十分な評価を加える必要がある。その手順を図に示すと図14のようになる。

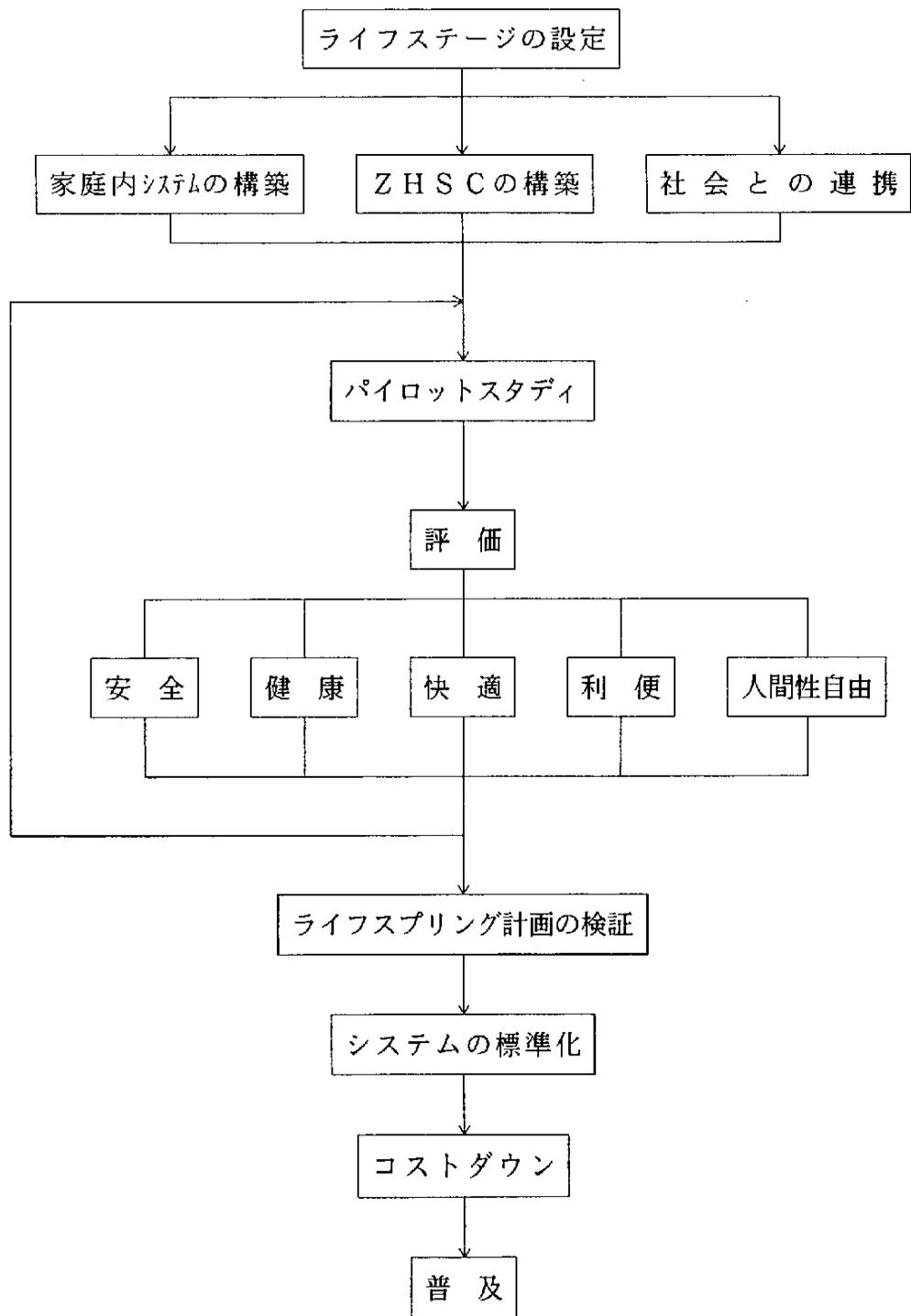


図14. 計画実現へのステップ

(2) 解決すべき課題

パイロットスタディをスタートさせるにしても、実際のハード・ソフトの開発やネットワークを構築する必要がある。また、開発を推進させ、情報システムや運用組織を構築したとしても、パイロットスタディとしての実運用を検討する場合は、解決すべきさまざまな課題が残されている。

(a) 規格統一・標準化

住まい手が求める居住空間の質的な向上と快適指向の居住環境を実現させるためには、家庭内システムをいかにシンプルかつ自由に組み立てられるかが1つのポイントとなる。

そのために、関連業界が技術開発・規格統一に積極的に取り組んでいる。こうした活動の成果に期待するとともに、これを活用するというコンセンサス作りが必要となるであろう。

(b) 法規制

情報のリアルタイム化やサービス・取引の電子化はさまざまな矛盾と既製概念の否定を生じさせる。現在の法規制そのものが、ライフスプリング計画を実現させる上での阻害要因となるとすれば、これを排除しなければならない。

そのためには、行政の理解とバックアップが必要であり、官民一体となった普及・促進のための体制作りが必要となる。

(c) 安全性・信頼性の確保

生活の情報化・ホームオートメーション化は、快適な生活を実現させるための手段であり道具であるといえる。したがって、道具であるシステム、あるいはその道具を備えた居住空間・環境そのものが、安全であると同時に信頼性があるものでなければならない。

これらを確保するためには、今までにない安全基準や信頼性の基準を設け、全ての面でセキュリティ対策を完備しなくてはならない。

(d) 基盤整備

社会との連携なくしてライフスプリング計画は実現しない。したがって、社会との連携をとるために必要なネットワークや運用組織を基盤として整備する必要がある。

〈参 考〉

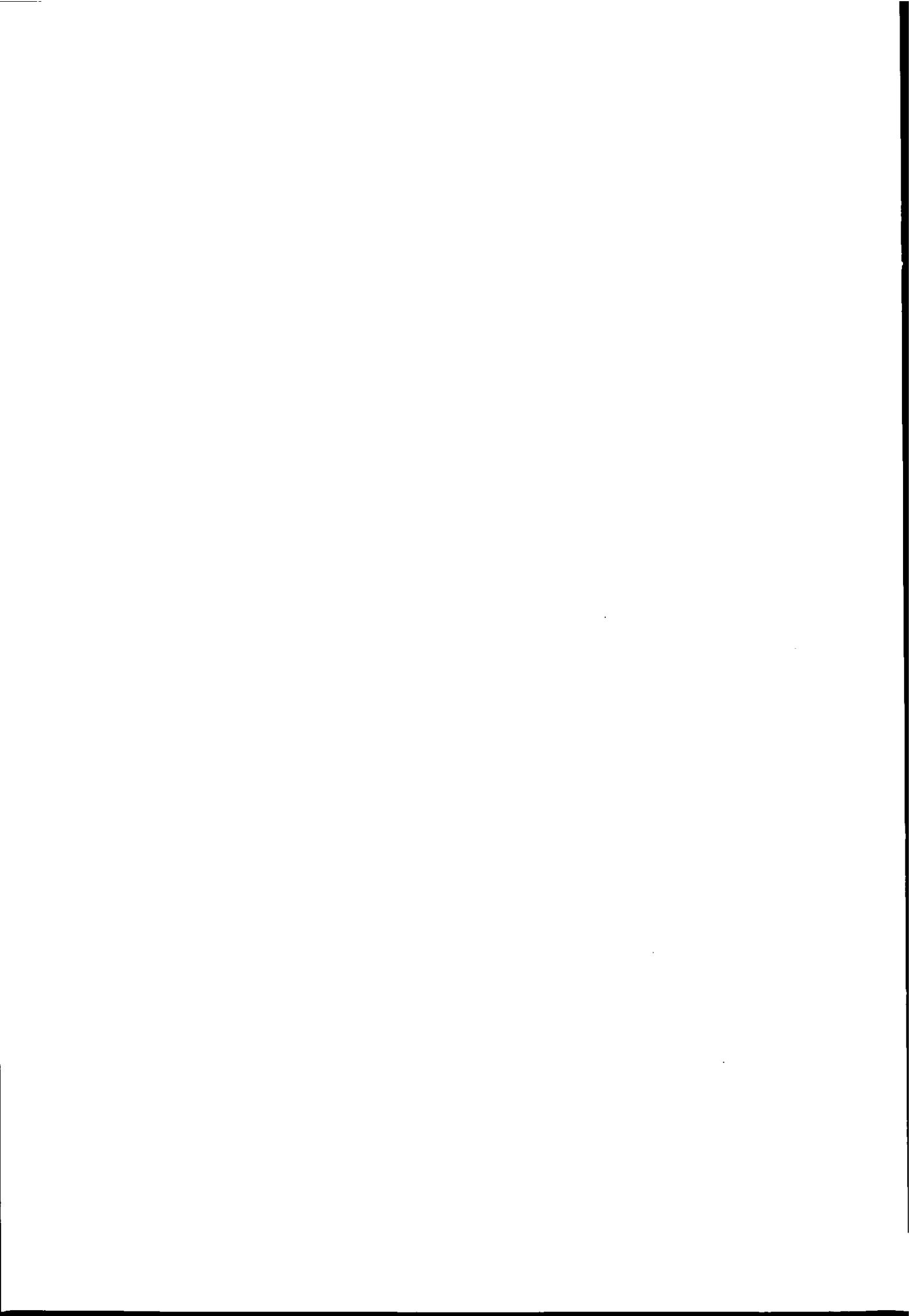
本調査研究でとりまとめた報告書は次のとおりである。

「セキュリティ産業の成立と今後の展望」, 昭和62年3月

「セキュリティ産業の実態と新しい課題」, 昭和63年3月

「2010年の情報化社会とセキュリティ」, 平成元年3月

「21世紀へ飛躍するセキュリティ産業」, 平成2年3月



—— 禁 無 断 転 載 ——

平成 2 年 3 月 発行

発行所 財団法人 日本情報処理開発協会  
東京都港区芝公園3丁目5番8号  
機 機 振 興 会 館 内  
TEL (432) 9384

印刷所 株式会社 正文社  
東京都文京区本郷3丁目12番2号  
TEL (815) 7271

