62－R009

セキュリティ産業の実態と新しい課題

「ライフスプリング計画」：生活の情報化にもセキュリティ対策を

昭和63年 3 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６２年度に実施した「情報処理に関する普及促進」の一環としてとりまとめたものであります。

序

わが国でもセキュリティ産業がテイクオフし、21世紀に向けて急速に成長するものと推測されている。この揺籃期にあるセキュリティ産業をいかにして健全に育成するかが、これからの高度情報化社会の安全性を左右するといっても過言ではない。産構審情報産業部会の答申「2000年の情報産業ビジョン」（昭和62年6月19日）においても、ニーズの変化に適切に対応するセキュリティ対策の確保が重要であると提言されているところでもある。

本研究プロジェクトは、昭和61年度にスタートし、アンケート調査を実施して、わが国セキュリティ産業の概略を把握するとともに，セキュリティ産業の概念確立のために，その分類・整理を行った。

昭和62年度は，前年度に確立したセキュリティ産業の個々の分野について，具体的に実態を把握すべく調査を行った。精粗の差はあるが，これにより，産業としての実態をある程度把握することができた。

本年度のもう一つのポイントは，セキュリティ・システムが産業および企業から，生活分野へと進出してきている事実をとらえ，その総合的な対策を検討して，「ライフスプリング計画」を立案したことである。すなわち，生活の情報化に対するセキュリティ対策のあり方，および生活の向上のために望まれるセキュリティ・サービスのあり方を，地域単位において解決してみようとの試みで計画したものである。今後，各方面の意見を聴取し，さらに具体的かつ詳細な計画立案へと進めてまいりたい。

最後に，本調査研究を推進するにあたって，ご強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。

昭和63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	中　山　隆　夫	(財)日本情報処理開発協会　常務理事
委　員	安　保　二三男	セコム(株)　常務取締役
	植　木　規　男	シーアールシーテクニカル(株)　機器開発部長
	北　村　　亘	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
	小　西　二　郎	松下電工(株)　東京特機営業所長
	今　野　衛　司	日本アイー・ビー・エム(株)　技術渉外　部長
	柴　田　正　和	日本電気フィールド・サービス(株) 施設部　技術課長
	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	日本電子計算機(株)　大阪営業所長
	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
	古　川　　弘	新日本製鐵(株)　ｴﾚｸﾄﾛﾆｸｽ・情報通信事業本部 情報通信ｼｽﾃﾑ部　技術室　部長代理
	森　山　積　善	(株)熊平製作所　取締役東京研究所長
	吉　原　紀　生	(株)野村総合研究所　運用技術部　次長

目　　次

第１章　　総　　論

1. 概要

コンピュータ・システムの普及，発展とその社会・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，システム，サービスを提供する「セキュリティ産業」というべき新しい産業分野が形成されてきた。このようなセキュリティ産業を分類すると，機器・装置（含ソフトウエア）の分野では，①アクセス・コントロール（接近及び操作の制御），②防災・防犯，③非常用電源設備，④監視，⑤保管設備，⑥暗号，⑦セキュリティ用ソフトウェア，⑧通信回線の8種があり，サービスの分野では，⑨バックアップ・サービス，⑩教育，⑪コンサルティング，⑫警備，⑬保険，⑭防災・防犯工事施工及びメンテナンスの6種があり，表1のとおり合計14分野38分類となっている。そして，このセキュリティ産業は，現在のところ年率20％以上で急速に成長しつつあり，1990年には，巨大産業に成長するものと思われる。

2. システムのオンライン化とセキュリティ

セキュリティ産業の14分野について，今後5年間の成長が著しいと思われる分野を調査（61年度，セキュリティ産業に関するアンケート調査）すると，次のような順位となっている。

（回答数／63社）

第1位	通信回線分野	52.4％
第2位	アクセス・コントロール分野	28.6％
第3位	監視分野	27.0％
第4位	セキュリティ用ソフトウェア分野	25.4％
第5位	コンサルティング分野	19.0％
第6位	防災・防犯分野	14.3％
第7位	バックアップ・サービス分野	11.1％

このように，通信回線の分野が最も関心を集めているのは，セキュリティ産業が，単体のセキュリティ関連商品を提供する業務（例えば，鍵，金庫，消火器等）から，総合化され，システム化され，ネットワーク化されたサービスへ進化しつつあることを示している。

1986年９月末現在での，日本の汎用コンピュータの設置台数は27万台を超え，パソコンは 500万台，ワープロも 500万台を超えたと推計されている。したがって，全産業分野にコンピュータは普及し，高度に利用される状況となり，コンピュータ・セキュリティの問題も程度の差はあれ，全産業共通の問題となりつつある。

表1.　セキュリティ産業の分類

	分　類（大分類）	機器・装置・機能（小分類）
機器・装置（含ソフトウェア）	1.　アクセス・コントロール（接近及び操作の制御）	識別（カード，カードリーダ，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　犯・防　災	火災（センサー・受信・報知）
		地震（センサー・受信・報知）
		漏水（センサー・受信・報知）
		侵入（センサー・受信・報知）
		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
		ＣＶＣＦ（Constant Voltage Constant Frequency）
		ＡＶＲ（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）
サービス	9. バックアップサービス	センターバックアップ
		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・防犯工事施工及びメンテナンス	防災・防犯工事施工及びメンテナンス

コンピュータ・システムは，企業に導入された当初は，スタンドアロンのバッチ・システムとして企業の各部門に導入された。バッチ処理のコンピュータであっても，企業にとって重要な情報である財務・会計，人事，マーケティング情報が収録されており，企業機密として護るべき技術情報やノウハウも蓄積されている。したがって，建物やコンピュータ室へのアクセス・コントロールや防犯・防災，監視，データ保管用の設備，警備などが必要となるが，そこで要求されるセキュリティは，あくまで企業の事業部門別のセキュリティであり，セキュリティ対策も個別の対策で，システム化され総合化されたものではない。コンピュータの登場以前から存在した現金・有価証券・原簿・帳簿などのセキュリティ対策と基本的には似ている。

現在，バッチ・システムは，個別企業のオンライン・システムへと逐次移行しつつあり，東証１部・２部上場企業では，すでに80％がオンライン化を終えている。バッチ・システムは，科学技術計算や各種の事務計算のように，計算の目的だけで使用されている場合はバッチ・システムのまま残るが，多くのシステムは，使い込まれていく中に，通信回線と接続して，個別企業のオンライン・システムへと移行していく。コンピュータ・システムがなぜオンライン化するのか，その理由は，バッチ・システムでは，投入される伝票や文書が郵送か使送されるため，常に時間的に集計が遅れるからである。とくに，全国的なシステムになると時間的に遅れるだけでなく，伝票が途中で紛失したり，入力に誤りを生じたりしやすくなる。これに対して，システムがオンライン化すると，伝票や文書は顧客と面接しながら，情報が発生したその場で入力されるため，誤りが少くなるとともに，情報は迅速に伝達，処理され，常に現状に維持されることになる。したがって，バンキング・システム，座席予約システム，受発注システム，集配送システムなどの分野で，バッチ・システムとオンライン・システムが競合すると，オンライン・システムが必ず勝つことになる。このように，競争市場では，システムはオンライン化の方向に進むことになるが，一方では，オンライン化によってリスクが増大し，システムの脆弱性が増し，

セキュリティの問題がクローズアップされてくる。

第1に，オンライン化によって，ネットワークの範囲が拡大し，バッチ・システムが点のセキュリティであるのに対し，オンライン・システムは面のセキュリティとなる。オンライン・システムの場合は，端末機，建物内配線，市内および市外伝送路，交換局，処理センターと諸設備が全国的に展開し，どこからも侵入可能であり，またどの部分を破壊しても，システムは故障することになる。

第2に，システムはオンライン化によってファイルが集中し大容量化するため，これが壊れると全情報が失われるので，アクセス・コントロールや防犯・防災対策は極めて重要となる。

第3に，システムはオンライン化により，即時処理（リアルタイム処理）となるため，業務の処理は効率化し，情報は常に現時点で把握することが可能となるが，万一故障が発生すると，業務は全社的，全国的なスケールで停止する。したがって，セキュリティ用ソフトウェア，非常用電源設備，バックアップ・サービス，監視などのセキュリティ・サービスが重要視されてくる。即時処理によって，業務処理は便利になり，迅速化する反面，停止すればシステムが停止するだけでなく，日常の生産活動，業務活動が止まるため，システムの脆弱性は高まり，セキュリティ対策は全社的な経営上の問題として重視されてくる。したがって，フォールトレラント・システム（対故障性システム）やホットスタンバイ機能（二重化）が，新しく要求されるようになってくる。

第4に，オンライン化によって，システムのプログラムは高度化して複雑化し，一ヵ所でもバグがあると，システムは停止するため，セキュリティ用のソフトウェアは極めて重要となる。また，オンライン化によってネットワークが全国的規模で拡大し，処理する業務トラフィックの変動や集中といった新しい社会的な要因がシステムに加わるため，ソフトウェアの設計は難しくなる。

3. ネットワーク化の進展とセキュリティ

コンピュータ・システムは，バッチ・システムから個別企業のオンライン・システムへと発展し，使い込まれていく中に，自企業だけでなく取引先や下請企業，顧客まで包含した垂直型の共同利用システムへと発展していく。図1にみられるとおり，大手企業による垂直型の系列化を強化するシステムが業界内に展開すると，その動きに対抗して，中小企業を主体とした水平型の共同利用システムが発達してくる。例えば，金融の分野では，都市銀行，地方銀行の個別または系列別の垂直型のシステムに対抗して，相互銀行，信用金庫，労働金庫，信用組合，農業協同組合などの業界内で，水平に団結した共同利用システムが発展している。さらに，これらを相互に接続する大きなネットワークである全国銀行為替交換システムや現金自動支払システムが生まれ，個別のシステムも共同利用のシステムも全部包含し，巨大なネットワークを形成する。このような動きは，証券，保険，流通，物流など多くの分野で多く発生している。

このように，複数の企業がネットワークで相互に接続されると，そのセキュリティも，企業グループ全体のセキュリティ，業界全体のセキュリティへと重要性が増していく。例えば，全国銀行為替交換システムが，地震，災害，犯罪，事故などの要因で止まると，全国的な規模で送金が止まるため，日本の金融秩序に大きなダメージを与える。宅配のシステムが止まれば，物流が全国的な規模で止まるし，航空路レーダ情報システムが止まれば，各航空会社の空の便は全国的に停止する。航空貨物通関システムが止まると，輸出入の貨物の通関が止まるため，滞貨の山となり，日本全体の流通に故障をきたす。

したがって，共同利用型システムのセキュリティは，その産業全体のセキュリティへ，さらに経済活動全体のセキュリティへと発展していく。また，共同利用型のシステムを構築するためには，業界内，企業グループ内で協調して，伝文フォーマット，企業コード，商品コード，プロトコルなど，いわゆるビジネス・プロトコルの標準化，統一化を図り，インターオペラビリティ（相互運用性）を確保しないと，相互接続は不可能となる。しかし，インターオペラビ

リティが確保されるということは，異企業間，異システム間で相互に乗り入れが可能になるところから，参加企業のセキュリティ対策が不十分であったり，接続する他のシステムのセキュリティ機能が弱いと，ネットワーク・システム全体のセキュリティが低下することになる。一企業のシステムのセキュリティだけでなく，システム全体のセキュリティを向上させる必要があり，異なるシステムのどの端末からも侵入が可能になるため，アクセス・コントロールの分野でも，カード，ＩＤコード，パスワードなどによる識別機能の充実が大切となる。また，異企業間が通信回線で相互に接続されるため，暗号装置や暗号ソフトウェアが重要な役割を果す。参加企業の職員に，万一不心得な者がいると内部犯罪的な事故を防止することは難しくなるので，人間関係管理も重要となる。したがって，教育とかコンサルティングの分野がセキュリティ対策としてもクローズアップされてくる。このようにして，セキュリティ対策は，一企業の問題から分離して総合的な対策として，専門化し，新しい産業として独立する様相を呈している。

大型のネットワーク・システムにおいては，参加企業に事故があった場合，例えば，倒産したり，決済不能に陥ったり，誤りを生じた場合にどうなるかという新しい電子取引や電子決済ルールの問題がある。そして，即日決済にするか後日決済とするか，与信限度をどう設定するか，法的証拠の確保，事故があった場合の訴訟手続，賠償責任の決め方，保険制度など，新しいルールと商慣習を作ろうという動きがでてくる。

したがって，セキュリティ対策は技術的な対策，設備的な対策，ソフトウェア的な対策だけでは対応しきれなくなり，人間関係管理から，システム監査制度対策，法制的対策へと発展し，総合的に学問的に体系づけられたコンサルティング業務を必要としてきている。

4. 国民生活のセキュリティ

各産業の分野で発展しつつあるコンピュータ・システムは，最終的には公衆

ネットワークである電話網，ＤＤＸ（公衆データ網），テレビ網，ファクシミリ網，パソコン・ネットワーク，画像通信網と接続し，各家庭や中小企業のデスクにまで入り込むようになる。現在，世界的に進行しているＩＳＤＮ（総合ディジタル通信網）が，各家庭や中小企業のデスクにまで普及するのは，10数年先(2,000年頃）と想定されており，光ケーブルと電子交換局を通じて，各種のコンピュータ・システム，ＶＡＮ，ＬＡＮ，画像情報，ファクシミリ情報，音声通信などがすべてディジタル化され，総合化されて相互に接続されることになる。また，家庭のテレビは，ハイビジョン（高品位テレビ）として，光ケーブルと接続して，多チャンネル化し，画像情報は，従来のテレビ放送の受信だけでなく，映画，スポーツ，演劇，学習，教育，医療，美術，レジャーなど多くの分野で多彩なサービスを提供すると考えられる。

現在，各産業分野で発展している受発注システムは，各家庭のデータテレフォン，パソコン，ワープロ，ファクシミリの端末と接続し，ホームショッピングやダイレクトショッピング（無店舗販売）として普及すると想定される。

すでに，書籍，酒類，地方の名産品，各種のブランド商品の分野では，ホームショッピングは実施されているが，さらに多彩化する方向に進みつつある。また，新幹線，航空機，ホテルなどのホームリザベーション・システムは，すでにキャプテン・システム，データテレフォン，音声応答システム，ファクシミリ情報システムで実施されているが，今後は，チケットの出力と支払決済機能を装備して，各家庭やオフィスに普及すると考えられる。

現在，防犯・防災のシステムは，すでにオンライン化し，ネットワーク化して，金融機関，工場，倉庫，病院，家庭へと浸透しつつあり，警備システムや監視システムと連動して，新しいセキュリティ産業の分野を拡大しつつある。最近登場したインテリジェントビルでは，アクセス・コントロール，防犯・防災，監視，警備と，従来ばらばらに使われていたシステムが，オンライン化され総合化されて発展しつつある。

医療システムは，各病院の管理システム，会計システム，医療データベース，

各種の診断システムとして，個別に発展してきている。救急医療情報システムの場合は，各家庭の端末機から，救急車の手配，病院の選択，血液，血清，医師の確保などが可能となり，すでに三分の一の地方公共団体で導入されており，将来は全国に普及すると考えられる。とくに，高齢化社会が近づくにつれ，医療システムや救急医療情報システムは，各家庭のセキュリティとしては，不可欠の存在となり，将来は，全世帯が必要とする。

教育や学習の分野では，ファクシミリを使用した学習塾のシステムやパソコンを端末機としたコンピュータ教育システムが家庭に入り始めており，家庭のパソコンからデータベースへの接続も可能になりつつある。

将来，ハイビジョンの普及とあいまって，語学，コンピュータ言語，医学，歴史，地理，美術など，画像・映像と結びつけて教育・学習した方が効果的な分野では，大きく発展すると思われる。

このように，システムは規模の大きなネットワークやディジタル化，総合化したネットワークと結びつくことにより，各家庭や中小企業のデスクに至るまで広く普及し，後述するように，家庭の情報化に関連したセキュリティ・システムとして，社会全体，国民生活全体のセキュリティを分担することとなる。そして，ネットワーク・システムによって，家庭生活が便利になればなるほど，事故によるシステムの停止は，市民生活のセキュリティを脅かすことになる。

また，コンピュータ・システムが，各家庭や中小企業のデスクまで広く普及していくためには，(1)一層の技術革新を進め，各種機器の価格の低廉化と性能の向上を図ること，(2)インターオペラビリティを確保し，各家庭に標準端末機があれば，ショッピング・システム，予約システム，バンキング・システム，各種のデータベースに接続しうるようにしなければならない。このために，各業界，各システムごとに，ビジネスプロトコルの標準化を進める必要がある。(3)家庭の主婦，老人，子供までが端末機を操作しうるよう，操作手順を簡素化，統一化し，ユーザ・フレンドリィなシステムを作る必要がある。

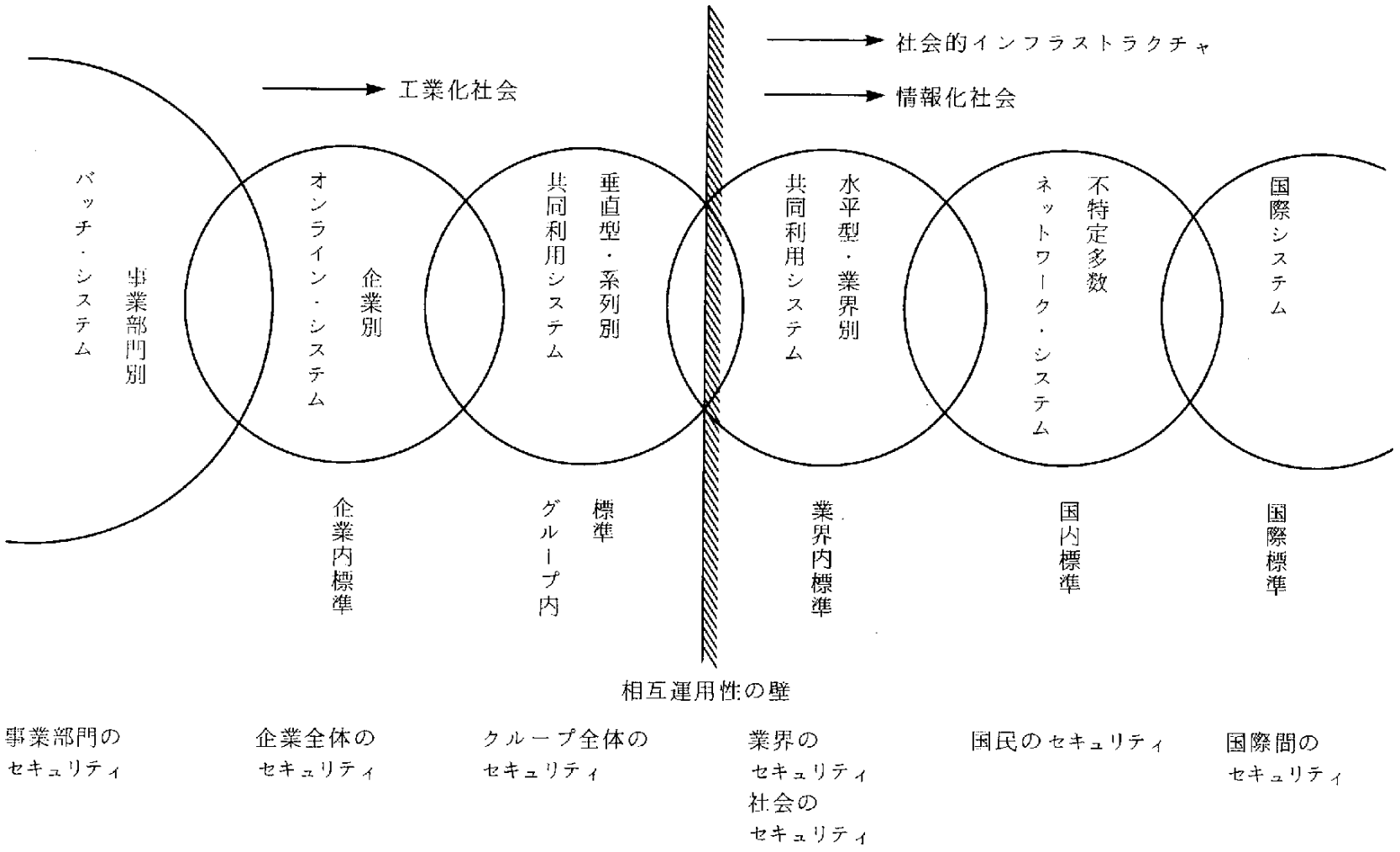


図１　コンピュータ・システムの発展形態（システムの進化）

5. 社会的インフラストラクチャとしてのセキュリティ産業

コンピュータ・システムが全産業に浸透した結果，セキュリティの確保は，産業の安全対策の問題となり，政府，地方自治体へのコンピュータ・システムの普及は，国・自治体・公共機関の安全対策と市民生活の安全の問題となった。さらに，システムが公衆ネットワークと接続して，各家庭にまで普及すると，社会全体と国民生活全体のセキュリティ問題となる。

今後，各企業が競争で育成していくべき産業のセキュリティ分野と，国や自治体が責任を持つべき公共のセキュリティ分野と，中立的な第3セクタが責任を持つべきセキュリティの分野に分れて発展し，最終的には社会的インフラストラクチャとして，相互に融合し，セキュリティ産業を形成していくと考えられる。

各種のセキュリティ・システムが家庭や中小企業にまで普及していくと，その対象は，世帯数約 3,800万，事業所数約 620万，合計約 4,400万という膨大な需要を形成するので，ホームショッピング，ホームセキュリティ，ホームバンキング，在宅学習など，どれをとっても「X万円× 4,400万」という兆円単位の内需の拡大を生ずることになる。

現在，データベースや処理センターの90％は，東京，大阪，名古屋の大都市圏に集中しており，地震，災害などの発生により，産業活動，社会活動，国民生活全般に機能の麻痺が起こる危険性がある。

停止する代表的なシステムとしては，銀行の送金業務，資金決済，ＣＤによる預金引出し，新幹線の運転，航空機の運行，座席予約，交通管制，受発注などの流通システム，集配送などの物流システム，電話，ファクシミリ，データ通信などの通信システム，ガス・水道・電気などの供給管理システムなどがあげられる。

セキュリティ対策上，データベースや処理センターの地方分散を図るとともに，社会的インフラストラクチャを形成しつつあるシステムの共同バックアッ

プ・センターを地方都市に構築する必要がある。

家庭のセキュリティ・システムは，兆円単位の内需の拡大を生むため，これを構築するセンター，ソフトウェア産業，セキュリティ産業がすべて大都市圏に集中することは，地域経済の振興対策上好ましいことではなく，計画的に分散を図る施策が期待されるところである。

6. 内需の拡大と産業構造の転換を促進するセキュリティ産業

安全の問題がセキュリティ産業として形成されてくる背景には，システム開発やコンピュータ・システムの普及発展に図2のような流れがあるからである。

(1) 現在，汎用コンピュータは約27万台が稼働しているが，その40％は物の生産管理システム，エネルギーの供給管理システムであり，国全体の生産活動を支えてきた。また，この分野のシステムが日本経済の豊かさを支えてきた。

(2) 生産活動を効率的に維持し発展させていくためには，交通，流通，物流，金融等のシステムを普及，発展させる必要があり，便利性，効率性を支援するシステムが現在，発展している。

(3) これらのシステムが普及した結果，豊かで便利で効率的な社会が実現しているが，システムは国民生活，社会生活に不可欠の存在となっており，システムの故障，地震，災害，犯罪等によってその機能が停止すると，直ちに不便で能率の悪い社会へ逆もどりする。

したがって，豊かで，便利な社会になったがために，システムのセキュリティ対策は重要な課題として浮上してきた。

(4) ネットワーク化したシステムのセキュリティ対策は，いまや，技術だけの問題でなく，総合的な科学となり，学術的，業際的，国際的に協力しないとその実現は不可能となってきている。

したがって，ＣＡＩ，ＡＩ，ＤＢといった学習的，文化的システムの支援と新たな開発が必要となってくる。

セキュリティ確保のため，ハードウェア，ソフトウェア等の技術的対策は重要であるが，技術面だけでセキュリティを確保することは難しくなってきているので，

① 保険制度，損害賠償制度，システム監査制度

② プライバシー保護制度，消費者保護制度

③ 刑法，訴訟法，各事業法の罰則

④ 法的仲裁機関のような組織

を整備していく必要がある。

(5) 図2「システム開発の流れとセキュリティ」に示されるとおりに，システム化が進展していくと，経済が物の生産と供給を重視した産業構造から，サービス化しソフト化した産業構造へと転換していくことを示している。また，家庭のセキュリティ・システム分野にまで進むと，内需の拡大効果は極めて大きいので，産業構造のウェイトは明らかに変わっていく。

(6) 従来の物やエネルギーを効率的に安く・早く・大量に生産し，競争に勝って豊かになることを重視する価値観から，便利な社会と安全な社会の実現をも重視する価値観へ，さらに創造性を重視する価値観への転換をも意味している。

7. セキュリティ産業の育成と今後の課題

セキュリティ産業の育成については，今後民間企業がそれぞれの産業分野で責任を負わなければならない分野と，国または自治体が責任を負う分野と，社会的インフラストラクチャとして第3セクタ方式で開発を進めなければならない分野に分かれる。

セキュリティ・システムは，今後，ヒューマンサービス・メニュー，インフォメーション・メニュー，防犯防災メニュー，ヘルシー・メニュー，アメニティ・メニュー，シルバー・メニューなどを包含した生活の情報化を前提としたセキュリティ・システムとして，各家庭へ普及していくことになる。

これを促進していくためには，セキュリティ産業は情報産業と一体となって，今後，多様化，複雑化するニーズに応えていくことが求められる。具体的には，

(1) コンピュータ技術，ネットワーク技術，センサー技術の開発促進，ソフトウェアの供給力の向上，各種データベース・サービスの充実などを図り，セキュリティ関連コストを低廉化させる。

(2) セキュリティ・システムの端末機を各家庭，中小企業のオフィスなどに多数設置することはできないので，インターオペラビリティ（相互運用性）を確立するために，端末機の操作方法，接続手順，ネットワークのインターフェイスなどを標準化し，社会的インフラストラクチャとして育成する。

(3) 各家庭やオフィスに設置されるシステムは，相互接続の不可能な縦型の閉鎖網であってはならない。広く 110番， 119番，病院，交通機関，福祉施設，地方公共団体の諸設備と接続し，相互にサポートしあえるインターオペラビリティのとれたネットワークでなければならない。

(4) これらの機関はいずれも国，自治体，民間企業の異なる組織に帰属するため，セキュリティ・システムとしてまとめるには，横に調整を図り，オルガナイズする必要があり，システム・インテグレーション・サービスなど，新規の産業分野が形成されなければならない。

(5) 大都市圏だけでなく，地方でもセキュリティが確保され，地域経済・社会の活性化のために，セキュリティ産業が発展するよう的確な対応策が必要である。

なお，通商産業省・産業構造審議会・情報産業部会・基本政策小委員会・長期展望分科会より，昭和62年６月19日に答申が出された「2000年の情報産業ビジョン」の中でも，情報産業の発展の方向として，ニーズの変化に対する適切な対応を図るセキュリティの確保が必要である旨，つぎのように指摘されている。

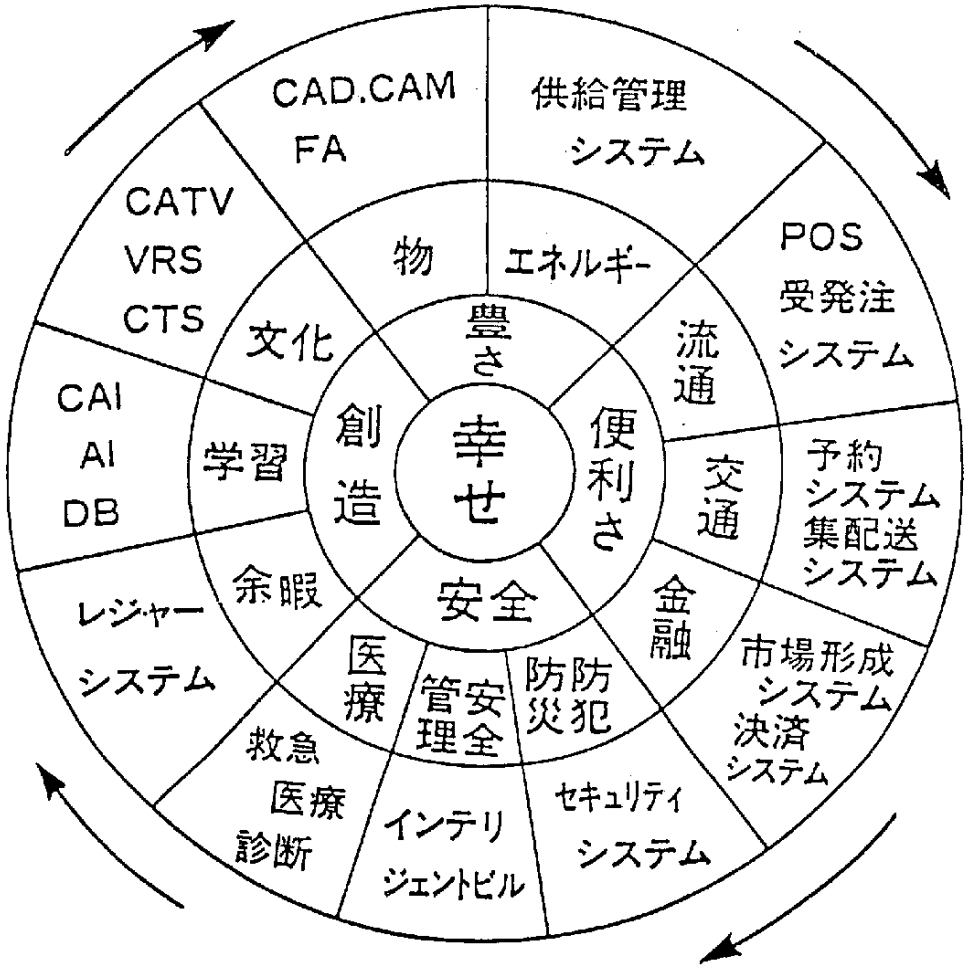


図２　システム開発の流れとセキュリティ

- ニーズの変化に対する適切な対応

  我が国の情報化をめぐるニーズは，近年大きな変革の途上にある。情報化を担う情報産業は，今後多様化，複雑化するニーズに適切に応えていくことが求められる。具体的には，①一層の技術開発の推進，ソフトウェア供給力の向上，データベースサービスの充実など，情報産業の各部門の高度化の推進，②インターオペラビリティの確保やユーザフレンドリーなシステムの開発などユーザへの負担の軽減，③システム・インテグレーション・サービスなどの新規分野の形成，④セキュリティの確保や地域経済社会の活性化など社会的要請などについて的確な対応を図っていくことが必要である。

本報告書では，産業分野におけるセキュリティ対策の実態を調査するとともに，情報関連内需の発展のために，第3章で提唱する「ライフスプリング計画」を，生活の情報化とセキュリティ・システムの観点から，ニーズの変化に対応するセキュリティ産業の新しい課題としてとりあげた。

第２章　セキュリティ産業の実態

I. 通 信 回 線

通信回線分野は，大きく通信機器を製造する分野とそれらの装置を用いて通信サービスを提供する分野（コモンキャリア）に分けることができる（図. 3）。

これらの分野が提供する通信機器や通信サービスは，ユーザの業務に使われるだけでなく，通信装置の二重化，バックアップ回線など，システムのアベイラビリティ向上策としても用いられる。その意味で，セキュリティ産業における通信回線分野は，セキュリティ専業というより，ユーザ側のセキュリティ用途を対象としている。

通信回線分野の提供する機器やサービスは，近年の著しい技術進歩や法制度の改正などにより，多様化の方向にあり，それを利用して構築されるセキュリティ対策も多種・多様化の方向にある。

そこで，多様化する通信サービスの現状全般とセキュリティの関係を概観し，つぎにコモンキャリア，ユーザ，メーカの安全性，信頼性向上対策をながめ，さらに通信機器の市場動向と普及推進上の課題について考察してみたい。

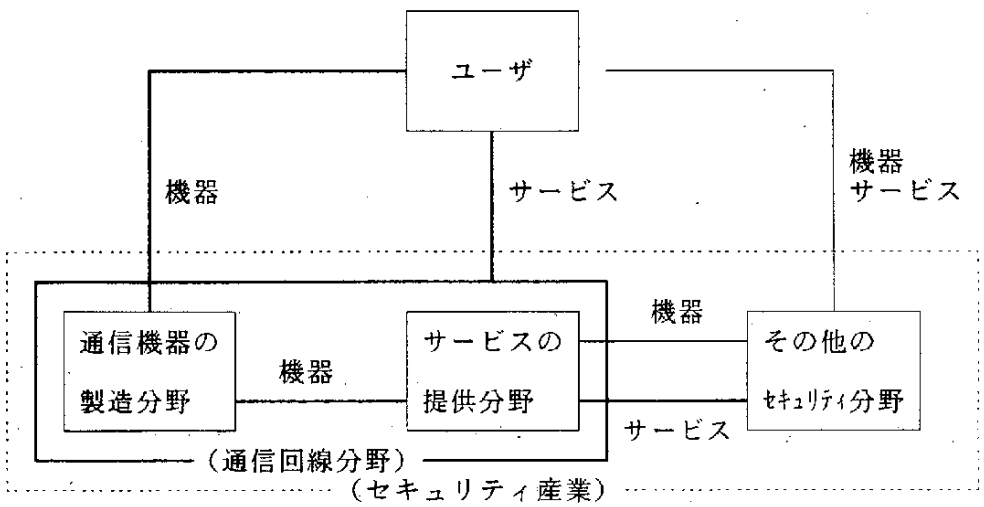


図. 3　通信回線分野の位置づけ

1. 現状把握

近年の通信回線分野は，ニューメディアという言葉に代表されるように，さまざまな通信機器やサービスが出現し，今，フィーバーぶりは納まってきたとはいうものの，それぞれのメディア（サービス）に合った用途には至っていないように思われる。したがって，ここでは過渡期的状況にある通信系メディア全体を概観することとしたい。

1.1 多様化する通信メディアとセキュリティ

(1) 多様化する通信メディア

従来の大規模な通信系メディアは，アナログ伝送をベースとした有線系の電話網と無線系の放送網（テレビ，ラジオ）が主流であった。しかし，近年の著しい技術進歩により，有線系では，ディジタル伝送をベースとしたサービスが可能になり，ＤＤＸ網，ＦＡＸ網，ビデオテックス網などが普及し始め，さらに，ＩＳＤＮ網も実用化されようとしている。一方，無線系においても，衛星通信，衛星放送による文字多重放送などが実用化され，また，難視聴地域への放送網としてスタートしたＣＡＴＶも，都市ＣＡＴＶとして新たな方向を模索しつつある。さらに，これらの通信系メディアに付加価値をつけたＶＡＮサービスも着実に地位を固めつつある。

また，企業の構内通信でも，従来の電話網に加えて，データ伝送を主体とするＬＡＮが普及し始めている。

このような多様化する通信メディアは，セキュリティ範囲の拡大，内容の充実にも多大な貢献をしている。即ち，一般企業には，地震，火災などの自然災害に対するバックアップ回線の選択範囲を拡大させ，監視産業には，エレベータ，ＡＴＭなどのリモート監視業務の拡大，効率化に役立ち，また，公的機関には，異常事態の速報手段を提供し，さらに，一般家庭には，出先

から家庭のガス，電気などのリモート制御も可能としてきた。

(2) 情報形態の統合化

従来は，音声，コードデータ，イメージなど情報の形態に応じて，使用するネットワークを使い分け，場合によっては，ディジタル／アナログ変換を必要としたが，大容量，高速伝送が可能な光ファイバなどの技術進歩により，ディジタルをベースとした混在伝送を可能となり，また，マルチメディア多重化装置のように，各情報形態を時分割多重し，伝送を行う装置も出現し，簡易映像の伝送もできるようになった。

これらにより，セキュリティのための情報形態も，制御情報のみから，図形や音声など色々な形態の同時伝送が可能になり，地図付きの医療案内システムなど，より分かりやすいセキュリティ・システムの構築が可能となってきた。

(3) 機器の多様化，サービスの充実

ネットワーク技術の進歩と同時に，コンピュータ技術の進歩も著しく，システム形態もバッチからオンラインへと，それに伴い，オフィスには，オフコン，パソコン，ワープロ，テレビ会議装置，ディジタルＰＢＸに接続された電話，ファクシミリなどが，営業店舗には，ＰＯＳ，ＣＤ／ＡＴＭなどの端末が普及，また，家庭にも，テレビ，電話に加えて，パソコン，各種のアダプタが普及し始めている。また，これらの各種機器の相互接続を目指して，プロトコルの標準化（ＯＳＩ等）や製品への適用も進んでいる。

通信機能を備えた情報処理機器の多様化，多機能化の傾向は今後も続くと思われ，また，その用途の一つであるセキュリティ分野でも，特殊なセンサーの付いた専用装置，汎用製品へのセキュリティ・アダプタ，汎用製品でのセキュリティ・サービスなど，多様化が続くと思われる。

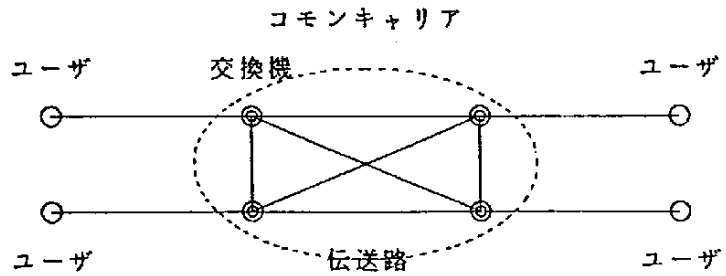
1.2　ネットワークの安全性，信頼性対策

ネットワーク自身の安全性，信頼性対策を，通信サービスを提供する立場（コモンキャリア）とそれを利用するユーザの立場からながめてみると次の通りである。

(1)　コモンキャリア側での対策

高度情報化社会のインフラストラクチャとしての通信路の安全性，信頼性確保は，社会的要請である。そのために，地理的に網目状に伝送路を張り迂回ルートを確保し，交換機を二重構成にしアベイラビリティの向上を図り，また，部分的に集中するトラフィックの制御や異常箇所の切り離しなどの管理機能も必要となる。さらに，それらの効率的運用のため，集中管理も必要とされる。また，これらの伝送路，機器に対し，防災，防水，停電などの自然災害対策も要請される。

また一方では，ユーザ側のセキュリティ対策が容易なように，限定されたユーザ間でのみ通信を可能とする閉域サービス，発信者の識別子を通知するサービスなど，サービス内容の充実も必要となる。



図．4　コモンキャリアでの対策

(2)　ユーザ側での対策

ユーザ側での必要なセキュリティ対策のレベルは，業種により異なるが，

金融機関のシステムなど，システム停止が社会的混乱を招く恐れがある場合，より厳密な対策が必要とされる。通信回線に対しては，通常業務用の他に，交換回線や通信衛星などをバックアップ回線として用意し，また，処理センターや通信装置の二重化も必要となり，場合によっては，バックアップ処理センターを地理的に離れた所に設置するなど危険分散の対応も必要である。さらにネットワークの効率的運用のため集中管理も必要である。

同一企業から，同一業種，さらに，異企業へとネットワークが拡大するにつれ，伝送情報に対する犯罪への備えも要請されてくる。例えば，企業機密に属する情報の盗聴防止のために暗号化を施したり，決済に関する情報に，改ざん検出のためのメッセージ認証子を付加するなどの対応である。

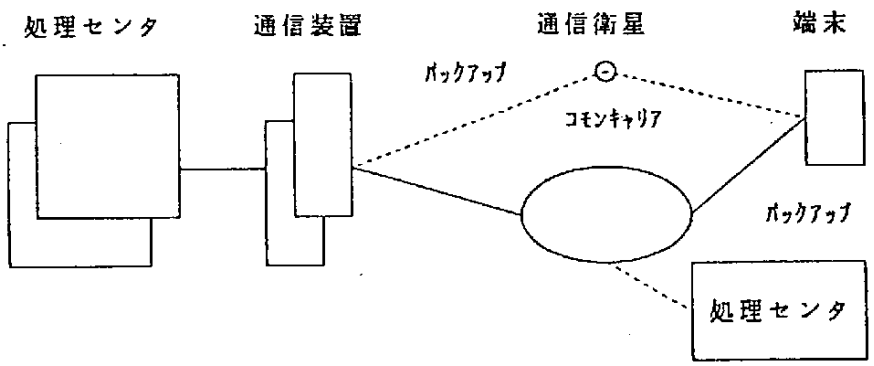


図. 5　ユーザでの対策

(3)　メーカ側での対策

従来は，通信装置で使用する部品の高信頼化やそれらを使用する際のパスワード機能などの対策がとられていたが，最近では，ネットワークの構成要素の異常を検出し，故障箇所を切り離して運転する，いわゆる，縮退構成機能を持つ制御装置へと拡大し，システム全体の稼働率向上に寄与している。

また，ハードウェアでの対応に加えて，ソフトウェアの比重も高まりつつある。その代表的なものが，ＯＳＩ（Open Systems Interconnection）におけるセキュリティ機能で，現在以下のサービスが検討されている。

- エンティティ認証：通信相手（プログラム）の正当性を認証するサービス
- アクセス制御：ＯＳＩのシステム資源への不正なアクセスを防止するサービス
- データ秘匿：伝送データが盗まれても，データの意味を判らなくするサービス
- データ完全性：伝送データの改ざんを検出するサービス
- 否認不可：データ送信事実の否認や受信データの改ざんを防止するサービス

2. 市場規模

通信回線分野の市場は，通信機器とサービスから成り立つが，ここでは前者について見てみる。通産省の「生産動態統計」によると通信機器の総生産は，昭和61年度で１兆 7,970億円，過去３年の平均伸び率は10.3％になっている。平均伸び率を見ると，搬送装置の22.8％の伸びが顕著であり，これは，ネットワークのディジタル化投資の結果と見ることができる。と同時に，その影響が，コモンキャリアに加えて，企業内ISDN構築に向けてのディジタルＰＢＸ需要の形で，交換機の伸びにも大きく寄与していると思われる。また，電信・画像装置は 3,271億円と，全体の18％を占める。これは急速な普及を続けるファクシミリの影響であり，また，61年度の伸び率の低下は機器の低価格化の影響である。

また，電話機が59年度から60年度にかけて大きく伸びているのは，60年４月の通信事業法の改正結果である。

表2.　通信機器の生産動向

（単位：億円）

年度	58	59	60	61	58～61平均伸び
通信機器	13,405	16,151	17,471	17,970	10.3%
有線通信機器	10,479	12,617	13,943	14,270	10.8%
電話機	603	769	1,061	1,017	19.1%
電話応用装置	2,629	2,966	2,633	2,356	-3.6%
電信・画像装置	2,119	2,783	3,241	3,271	15.5%
交換機	2,576	2,830	3,035	3,515	10.8%
搬送装置	1,942	2,636	3,457	3,596	22.8%
有線部品	609	633	517	515	-5.4%
無線通信装置	2,926	3,534	3,528	3,700	8.0%
固定局	1,631	1,797	2,030	2,118	9.1%
移動局	1,296	1,738	1,498	1,582	6.9%

出所：通産省「生産動態統計」

3.　ユーザの現状

ユーザのコンピュータ・セキュリティに対する認識度，ならびに対策の実施度をながめてみると次の通りである。

- 当協会が昭和61年3月に発表した「コンピュータ・セキュリティ実態調査報告書」によれば，通産省が策定・公表した「電子計算機システム安全対策基準」について，その存在を名称のみ知っているのが43.5%，11.9%は知らないと回答している。
- 警察庁の昭和62年12月に発表した「情報システムの安全対策に関する調査」によれば，現状のセキュリティ対策について，37.3%はきわめて不十分，17.8%は未だ対策が必要と回答している。

最近は，コンピュータ・セキュリティが取り沙汰される場面も増え，啓蒙活動もいろいろ行われ，社会的関心も高まってきているかに見えるが，肝心のユーザの問題認識は前述の調査結果に見るように未だしというのが現状である。

つぎに，通信システムということを意識しつつ対策の実施状況をながめてみよう。通信システムのセキュリティ対策として，すでに実施されているもの，これから実施されようとしているもの，さらにはこれから実施技術あるいはツールの開発を待たなければならないもの等いろいろあろうが，現段階で実施し得ると考えられる種々の対策について，実際にユーザでどの程度実施されているのかをみてみたい。

通信システムのセキュリティを論じる際に，まず通信システムというものをどの範囲でとらえるかを決めなければならないが，モデムから先の回線のみとするのでは問題が多いので，回線に接続された情報処理機器を含めた統合的なシステムを考えることとする。

実施しうる対策として，第一に考えられるのは，機器が破壊されることを防御するためのいわゆる「物理的セキュリティ」 — 機械室への立入り制限，耐震・防火・防水設備，緊急給配電設備等 — であるが，これらはあまりに普遍的であり，通信システム以前の問題であるのでここでは省略する。

第二に考えるべきことは，システムに蓄積されている種々の情報を破壊・改ざん・剽窃から防御することである。システムが通信システムで，不特定多数の人がアクセスしうる環境下においては，この問題はますます危険性を増しており，対策の必要性が高まってきている。この問題に対して採られる対策は，特定の認可された人以外にはシステムへのアクセスを許さないという仕組みを取り入れることである。アクセスの認可のやり方も，ユーザの環境に応じて，プログラム単位，ファイル単位等アクセスされる側の区分けに依って決めるやり方，あるいはユーザ別，回線別等，アクセスする側の区分ごとに決めるやり方等いろいろある。このようにして区分したグループごとにアクセスの認可・不認可を決め，認可する場合のみアクセスするための鍵（認証）を渡すわけで

ある。現在使用可能な認証の種類としては，パスワード，磁気カード，ＩＣカード，指・声紋，印鑑，サイン等がある。

第三に考えなければならないのは，伝送途中での情報の剽窃，改ざんの防止である。このための対策の一つとして一般的なのは情報の暗号化である。暗号化の方式は古来種々研究されてきたが，ユーザではメーカー提供の方法を採用しているところ，独自の方法を使っているところ等さまざまである。

さて，これらの種々の対策は，仕組みとしてシステムに組み入れるだけでなく，実際に機能するように管理することが不可欠である。

そのため，不法なアクセスの試みがあったかどうかを常時モニターし，もしあった場合には，それがどういうことで発生したのかを追跡調査して，同じことが再び起らないように対策を講じて行くことをやらないと，防止システムを一応組み入れても形骸化し機能しなくなることにもなる。

上述のような対策・方式について，実際にユーザではどの程度実施されているのかを表３に示す。

セキュリティ対策として，上述のような種々の方策が指摘・議論され，そのための実施手段やツールが提供されたのは新しいことではないといえるが，実施しているユーザは大雑把にいって半分以下というのが現状であり，満足すべき状況にあるとはいい難い。

4. 将来展望

企業を中心としたディジタル化の波は今後も続くと予想され，仮に，年平均10％の伸びが続くと仮定すれば，昭和70年度には，通信機器の市場規模は４兆２千億円にもなると予想される。さらに，ディジタル化の波が家庭をも巻き込む時には，市場の飛躍的な拡大が予想され，また，その間には，ファクシミリのような利便性の高い機器の出現やニューメディアの市場定着も予想され，市場拡大に相乗効果を及ぼすであろう。

表3　セキュリティ対策・方式

セキュリティ対策・方式			467企業中実施済の%
アクセス制御	アクセス制御ソフトウェア	プログラム単位	41.1%
		ファイル単位	36.2
		レコード単位	7.3
		項目別	8.4
		ユーザ別	49.5
		回線別	8.8
		ユーザ毎コマンド制限	45.4
		端末毎コマンド制限	33.6
		デジタル署名	0.2
		ＲＡＣＦ等の利用	18.4
	認証	パスワード	85.4%
		磁気カード	17.1
		ＩＣカード	1.1
		指・声紋	0.2
		印鑑・サイン	4.3
暗号		独自の暗号を使用	10.7%
		ＤＥＳの利用	2.1
		公開鍵	1.1
		重要情報蓄積時の暗号化	3.4
		重要情報伝送時の暗号化	2.8
		Ｓ／Ｗで暗号化	10.7
		Ｈ／Ｗで暗号化	1.9
モニタリング		使用ユーザ	56.7%
		使用端末	62.3
		使用回線	38.8

出所：「コンピュータ・ネットワークのセキュリティに関する調査開発報告書」より，情報処理振興事業協会，昭和62年３月

このような市場規模の中で，セキュリティ関連の比率がどの程度になるかは明確ではないが，今後新製品開発等も含め，セキュリティ対策の充実をはかることが当面の課題である。

急速に拡大を続けるネットワークの健全な発展のためには，通信回線による通信機器やサービスの開発努力とユーザによる安全性確保とのバランスが重要である。世田谷のケーブル火災，筑波の文部省高エネルギー物理学研究所のハッカー事件などにより，セキュリティの重要性が認識されつつあるが，未だ具

体的には至っていないのが現状である。

ネットワークのセキュリティ向上のためにはいろいろな問題点がある。それらを要約すると次のようになろう。

(1) 設備投資への支援

セキュリティ対策の普及における一番の課題は，その必要性は認識しているものの投資効果がすぐ得られないという点にある。設備の二重化，バックアップ回線の確保などのセキュリティ対策には多大の投資を必要とする。しかし，構築されるネットワークは貴重な社会の財産であるという立場からすれば，それを守るため，積極的な安全対策を国としても推進する必要がある。推進策の一例として，設備投資に対する財政的支援や税務上の配慮が考えられる。但し，通信回線分野は一用途としてセキュリティがあるので，その辺の配慮が必要であろう。また，投資に対するインセンティブを与えても，未だ投資に踏み切れない企業も多いと考えられ，そのような企業に対しても，共同利用型のバックアップセンター／回線が提供できる仕組みの導入が必要であろう。

(2) 業種の育成

通産省を始めとして，各官庁による安全対策のガイドラインが作られている。しかし，このガイドラインに沿って対策を取るためには，高度な技術力と経験を必要とし，個々の企業がこのような人材を育成するには多大の時間と経費が必要となる。米国にはセキュリティ専門のコンサルタント会社が多くあり，わが国においても，このような業種を育成するなど，個々の企業の負担を軽減する対策が必要と考える。

(3) 世界への貢献

企業を中心にネットワークのディジタル化が進展しているが，いずれは，家庭にも延びるであろう。とくに，電話回線の数千倍の伝送容量が可能な光ファイバであれば，映像情報の伝送が容易であり，また，双方向通信も可能となり，その用途はセキュリティも含めたさまざまな形態が考えられる。こ

のような家庭生活をより豊かにする光ファイバの家庭への普及を世界に先駆けて推進し，そこで得られたノウハウを他国へ技術供与するなど，世界規模での安全性確保に貢献すべきである。

Ⅱ．アクセス・コントロール及び監視

昭和61年度の報告書「セキュリティ産業の成立と今後の展望」の中で，今後5年間の成長が著しいと思われている分野の2位がアクセスコントロール，3位が監視である。

この両分野は，機能的には相互に密接に関連しており，

① 警　戒
② 監　視
③ 感　知
④ 防御／制御
⑤ 通　報

の要素から成り，相互に関連して総合的なシステムを構成している。

これの大規模なものは，コンピュータ・システムを駆使して地域的レベルで行うものから，小は家庭のドアの錠前まで千差万別といえる。

ここでは，これらを「アクセス・コントロール」，「監視」，「ソフトウェア」に分けて考察したい。

まず「アクセス・コントロール」であるが，この概念は初期の頃には，ある建築物またはセキュリティエリアに人が入ることを規制することから始まって，現在では，これらのエリアだけでなく，情報システム，データ通信等への不法な（許可されていない）接近を規制し，または許可された情報レベルに限定するといった制御，さらに記録をとり，警報の送出等を行うといったことまで包含するにいたっている。

「監視」については，セキュリティエリア等への不法侵入を「みはる」ことから始まって，コンピュータ・システムの運用をサポートしている設備（電源装置，空調設備等）の運転制御，稼働状況，コンピュータ・システムの設備環境条件の監視を行う。そしてセキュリティを必要とする人（シルバーエイジ，

患者等），区域，機器，物件（データファイル，現金，宝石等），環境（温度，ホームセキュリティ等々）を監視し，異常時（不法侵入，設備異常，環境変化等）には警報を出し，必要に応じシステム自身がハードウェア／ソフトウェア的手段で防御する，または防御の指示を出すことも行う。

「ソフトウェア」は，これら「アクセス・コントロール」，「監視」用のソフトウェアに限定して考察した。今後システムが大規模化，総合化するに従い，需要も増大するし，また情報システムとのインターフェイス，情報システム内部での対応等，その使われ方も規模も増大すると考えられる。特にホームセキュリティ／シルバーセキュリティの分野では，対象の変化に柔軟に対応する必要性から，この需要が増大するものと考えられる。

1. アクセス・コントロール

アクセス・コントロールとは，保護対象への接近，または操作に際し，その接近または操作が正規であるか否かを判断し，制御することである。またこの状況を監視することも含まれる。

具体的には，正規の出入口にて，入室（館）者，退室（館）者を識別し，記録し，出入口の開閉を行い，同時にしかるべき部署へ報告する。これにより，出入口よりの不法な入退室（館）を防止する。

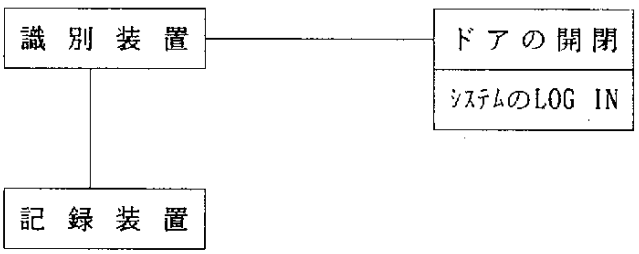
また，端末機，システム本体へのアクセスに際し，ハードウェア的な手段としてアクセス者を識別し，これと合わせて用いられるパスワード等のソフトウェア的手段とで，正規のアクセス者であるか否か，またはデータ，プログラム等へのアクセス権限の判別，制御を決定する。これにより不正なアクセス，権限外のデータ等へのアクセスを防止する。この分野では，不法侵入等のコントロールは含まれない。

この分野は，昨年度の報告書「セキュリティ産業の成立と今後の展望」によれば，今後成長が著しいとみられ，人為的なアクセス・コントロールから，機械的なコントロールへ，個別的・網羅的なコントロールへと変化すると考えら

れる。

1.1　基本的な構成

アクセス者が正規（許可された）な者か否かを識別し，信号を送出する識別装置と，これを受け必要なアクション（ドアの開閉，システムへのＬＯＧＩＮ等）を行い，必要があればこれを記録する記録装置から構成される。



① 識別装置　：アクセス・コントロールを行う心臓部分で，アクセス者の識別，信号の送出を行う。その方式は種々製品化されている。

② 記録装置　：識別装置からの信号を受け，コード表示等を印字するものである。

③ ドアの開閉　：主に電気錠が用いられるが，これを自動開閉装置と組合わせても用いられる。

④ システムLOG IN：主として識別装置からのコードと，パスワード等の組合せで用いられ，ソフトウェア的にシステム等への接続を行う。

1.2　識別装置の分類

(1) 直接識別

個人を特定する特徴を検出し，識別する方法である。この場合，他人に利用される（悪用）ことはなく，確実に本人であることが識別される。しかし検出・識別精度とコストの問題がある。さらに未だ開発途上といってもよく，

今後，カードレス化の方向と共に成長が期待される方式と考えられる。

- 指紋照合 …… 指紋による識別
- 網膜照合 …… 目の網膜の文様により識別
- 掌形照合 …… 手の大きさ，手指の長さ等により識別
- そ の 他 …… 声紋，掌紋等による識別方法等が発表されている。

(2) 間接識別

個人に貸与されたカード等，いわゆる鍵に相当する物により，その所有者を識別する方法である。この場合，他人に貸与したり，紛失したりした場合に，悪用されることも考えられる。

また，磁気カード等再書込みが可能なものについては，他人のコードを盗用することも可能になる。

従って，カード方式と押ボタン方式を併用する等，2種以上の方式の併用により，悪用の可能性を極力少なくする方法が用いられたりする。

- カード
  - 接触式 —— カードリーダーに挿入したカード上に記録されたコードにより識別
    - 磁気方式 ：磁気ｽﾄﾗｲﾌﾟによるコードを表現
    - ﾎﾛｸﾞﾗﾑ 方式：ﾎﾛｸﾞﾗﾑによりコード表現
    - ICｶｰﾄﾞ 方式：ICﾒﾓﾘに記録した信号により表現
    - ﾊﾟﾝﾁｶｰﾄﾞ方式：ﾊﾟﾝﾁ穴によりコードを表現
  - 非接触式 —— リードステーションまたはカードから電波等を放射し，このデータにより識別
    - 電波方式 ：電波の周波数等によりコードを表現
    - 磁気方式 ：磁気の有無等によりコードを表現
- 押ボタン —— 任意の数字等の押ボタンにより暗証番号を入力し識別
- 鍵
  - 符号錠 —— ダイヤルの回転と暗証番号による解錠
  - キーロック —— 一般的な鍵による解錠

1.3　応用例

(1)　入室管理

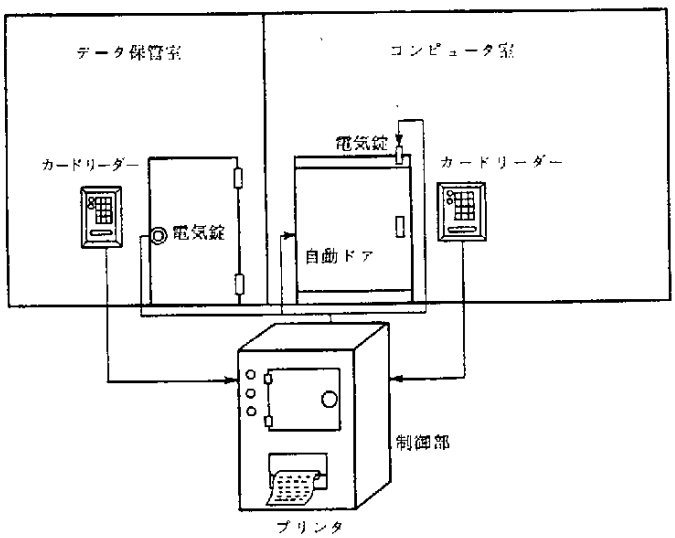
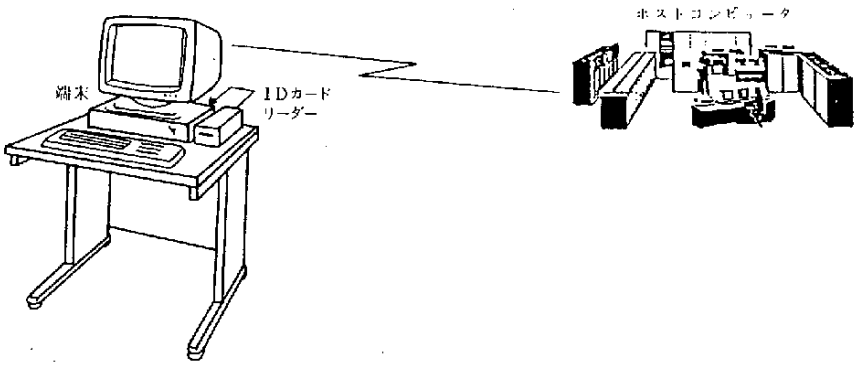


図6　入室管理

コンピュータ室，データ保管室等の入口にカードリーダーを設置し，カードのコードとテンキーからの暗号を制御部にて照合し，正規のカードであれば電気錠を解錠し，自動ドアの場合，自動ドアを作動させる。

(2) 端末管理



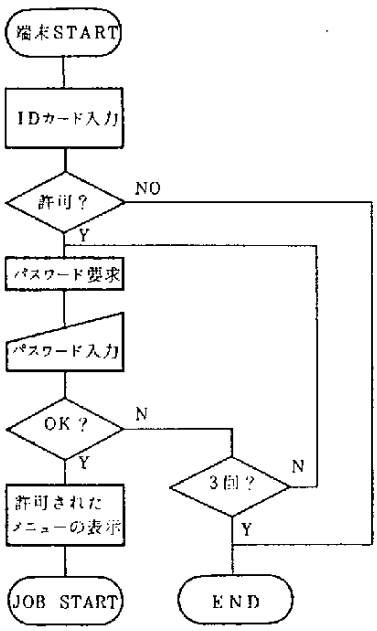


図7　端末管理

端末キーボードより，ＬＯＧ　ＩＮ要求を出し，ＩＤカードをＩＤカードリーダーに入れホストコンピュータでチェック後，パスワードをキーボードより入力する。

これにより個人を特定し，ホストコンピュータは，端末機の接続の可否，データ等へのアクセス範囲を設定する。

2. 監　　視

昭和61年度報告書「セキュリティ産業の成立と今後の展望」には，セキュリティ産業の監視分野を次のように分類している。

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）

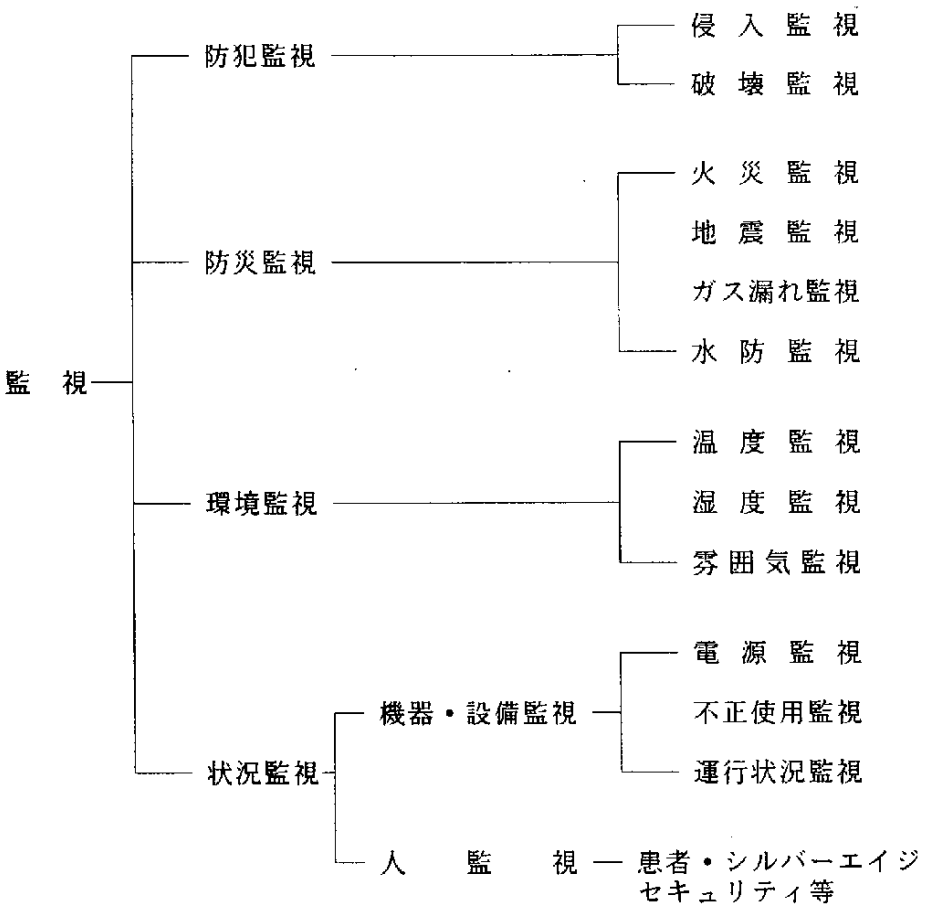
（同報告書３ページ）

また，「アクセス・コントロール」の監視として在室検知等もここに分類している。当初，監視分野は，セキュリティエリアの不法侵入を「みはる」目的から出発した分野であるが，監視機器や通信技術・システム技術の発達とセキュリティ監視を必要とする分野の拡大と相まって，今やインテリジェントビルの総合的なセキュリティ・システムに例を見るように，その裾野を広げている。

ここでは，そのような拠点からセキュリティ産業の「監視」分野をながめてみたい。

2.1　分　　類

監視を機能の面から分類すると，次のようになる。



これらの機能を果たすために，簡単なものは，センサーと警報装置が直結するものから，人間の五感に相当する各種のセンターや計測装置を駆使して，コンピュータ・監視盤と連結して，監視対象を管理制御する大掛かりなシステムまで実用化されている。

2.2　監視方法

監視方法には次のものがある。

①　機械的装置による監視

錠前と鍵等

②　映像による監視

a．フィルムカメラによる監視

b．テレビカメラによる監視

③　各種センサーによる監視

④　ソフトウェアによる監視

(1)　機械的装置による監視

錠前と鍵を使用して内からの施錠か，外からの施錠かを判別する電気錠がある。これを利用して人の出入り，潜在などを判別し，照明点滅などを管理するシステムが構築できる。またインテリジェントビルには，部屋鍵の集中管理を行い，鍵の在否によって，人の潜在・照明・空調の点滅を制御するシステムが採られているものがある。

(2)　映像による監視

(a)　フィルムカメラによる監視（サーベランスカメラ・システム）

犯罪の舞台になりそうな場所に向けて，長尺フィルムを装填した防犯用写真カメラ（サーベランスカメラ）を設置し，状況に応じて撮影するもので，

①　防罪の抑止力

②　証拠写真の撮影

を主目的とする。

主として，金融機関のロビー，カウンター，キャッシュサービス・コーナーに設置され，監視・ＩＤのためにはインターバル撮影・１コマ撮影，事件発生時には連続撮影が行われる。

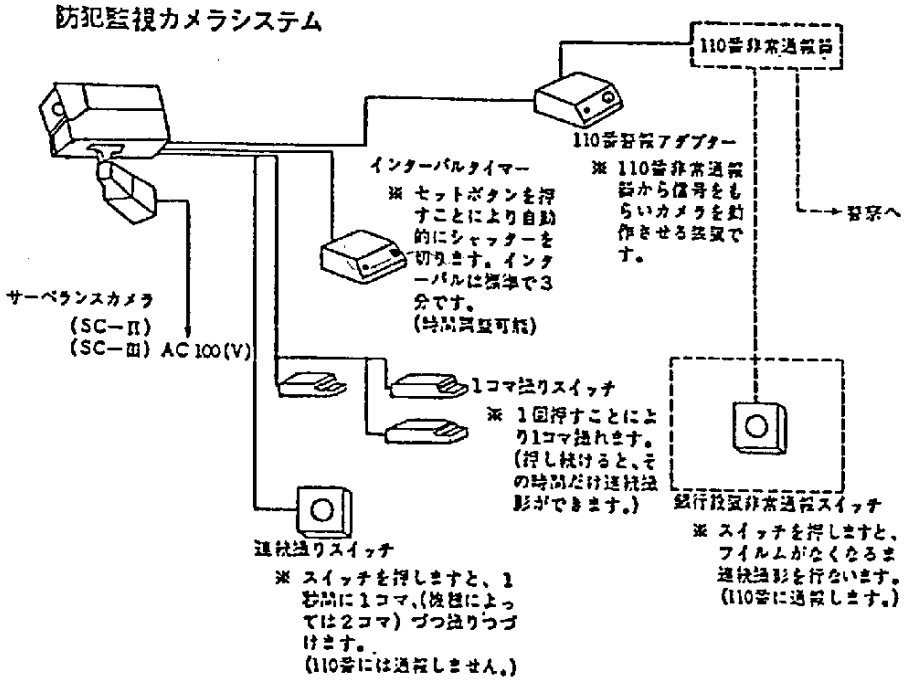


図8　サーベランスカメラ・システム

(b)　テレビカメラによる監視（防犯用ＴＶカメラ・ビデオシステム）

ＴＶカメラでセキュリティエリアを撮影し，オペレータはモニターテレビを通じて監視し，異常が発生するとＶＴＲ装置で記録したり，警察に通報したり，適切な処置をとるのが初期の監視システムであった。

カメラ技術の進歩は，撮像管からＣＣＤカメラへと進み解像力の向上，カメラの小型化が計られ，一方，画像伝送技術の発達で静止画像伝送，マルチ画像伝送などを利用した遠隔監視も可能となり，単に出入口監視システムだけでなく行動監視・状況監視・設備機器の状態監視など総合的な監視システムに組み込まれている。

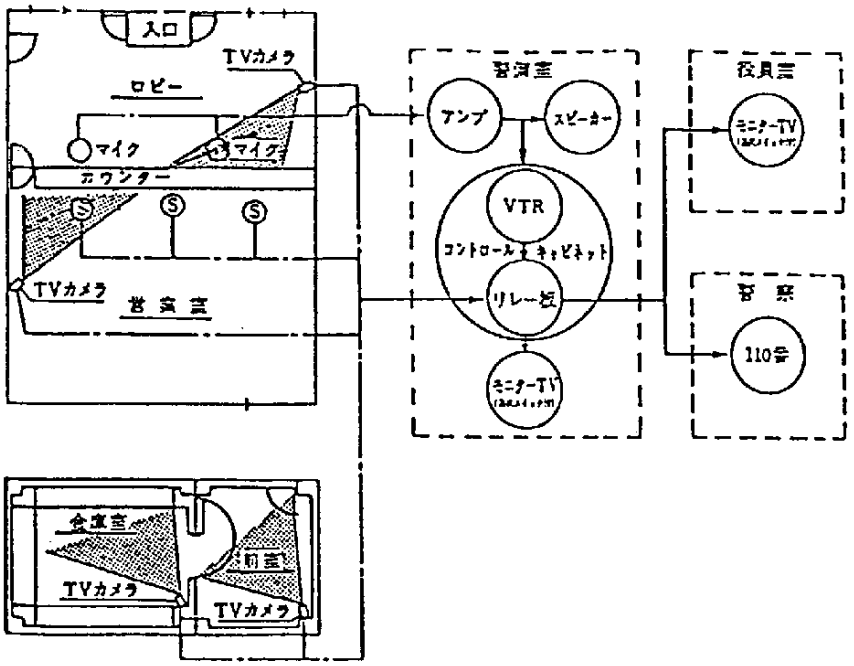


図9　防犯用カメラ・ビデオシステム

(3)　各種センサーによる監視

侵入監視・火災監視からインテリジェントビルにおけるビルセキュリティのシステム，ビルオートメーション・システムとして，機器の運行状況監視分野まで極めて広範囲に実用化されている。各種センサー，計測機器の開発・改良や通信技術の発達，コンピュータとの組み合せにより警報発報から機器・環境の制御まで広い利用が可能であり，監視システムの主流であろう。

表4　セキュリティ・システムとセンサー

分類	機能	センサー	監視・制御システム
防犯監視	侵入監視	錠前と鍵	防犯監視システム
		マグネットスイッチ	・外周警戒システム
		ガラスセンサー	・面積警戒システム
		金属箔センサー	・点警戒システム
		マット差動圧センサー	サーベランスカメラ・システム
		振動感知センサー	テレビカメラ・ビデオシステム
		光電ビームセンサー	ホームセキュリティ・システム
		超音波システム	原子力施設ＰＰ（Physical Protection）システム
		マイクロウェーブシステム	
		赤外線センサー	
		熱線感知センサー	
		テレビカメラ	
		フィルムカメラ	
	破壊監視	振動感知センサー	
		音響感知センサー	
		静電界容量センサー	
		熱センサー	
		テレビカメラ	
		フィルムカメラ	
	火災監視	温度センサー	防災監視システム
		煙センサー	・火災検知・報知システム
		漏電センサー	・自動消火システム
		漏水センサー	排煙制御システム

分類	機能		センサー	監視・制御システム
防災監視	地震監視		地震感知器 地震計	エレベータ 火災・地震管制運転システム 自家発電源管制システム
	ガス漏れ監視		ガスセンサー	ホームセキュリティ・システム
	水防監視		マグネットスイッチ 防水ケーブル 漏水センサー（線状） 圧力センサー	
環境監視	温度監視		温度計 温度センサー	データ保管設備 空調制御システム
	湿度監視		湿度計	
	雰囲気監視		ガスセンサー	
状態監視	機器設備	電源監視	漏電検出機 電圧・電流計 絶縁抵抗測定器	受変電設備監視システム 自家発電設備監視システム 漏電監視システム
		不正使用監視	鍵・カード 識別装置	アクセス・コントロール・システム
		運行状況監視	電圧・電流計 熱センサー 回転計 絶縁抵抗測定器 テレビカメラ	設備機器最適制御システム CD・ATM遠隔制御システム エレベータ運行管理システム
	人		テレビカメラ 押しボタンスイッチ マイクロウェーブ・システム	シルバーエイジ・セキュリティ・システム 患者監視システム

・遠隔監視とローカル監視

これらのセンサーを活用するシステムには，遠隔監視方式とローカル監視方式がある。遠隔監視方式はセントラル・ステーション方式ともいわれ，多数の保護対象と警備保障会社とが警戒監視の契約を結び，地区ごとにまとめて警報を受け付ける監視制御装置（ステーション）を設備する方式である。

ローカル監視方式は，建築物内部の監視室に監視制御装置（ステーション）を置く方式がある。

最近の大型ビルやインテリジェントビルでは，防犯・防災システムだけでなく，ビル内のあらゆる設備機器を総合的に監視・コントロールするビル管理システム（中央管制ステーション）が採られ，そのうちから防犯・防災システム，エレベータ管理システムなど，個別の監視システムがさらに遠隔監視方式で外部のセントラル・ステーションに接続されるものがある。

(4) ソフトウェアによる監視

通信ネットワークにおける回線上の割り込み対策のため，ネットワーク監視など，今後ソフトウェアによる監視も重要なセキュリティ対策となるであろう。

3. アクセス・コントロール及び監視ソフトウェア

高度情報化社会を迎え，情報システムのセキュリティ対策は必須事項となってきている。これと共に個別に対応していたアクセス・コントロール，監視についても，総合的なシステムに組込まれる必要性が高まり，また情報システムもこれらのシステムからの情報を基にデータの退避等自らを護る処理が必要になる。

また，ますます発達するシステムのネットワーク化に対応し，セキュリティシステムもネットワーク化が促進されると考えられる。

このため，監視についても，局部（ビル単位等）の監視，地域ごとの監視またその上部の監視等の階層化された監視が行われ，これらの相互間の通信，情

報システムとの間の通信等，ソフトウェアの重要性が増大する。

また，監視システムの階層化と情報システムの階層化（ネットワーク化）が一致しないことも考えられ，ソフトウェアのパッケージ化，標準化も重要になる。

個別にみると，識別装置の内，個人の特徴を検出する直接識別のシステムでは，個人の情報のデータベース及び照合ソフトウェアは識別精度の問題と共に今後重要になる。

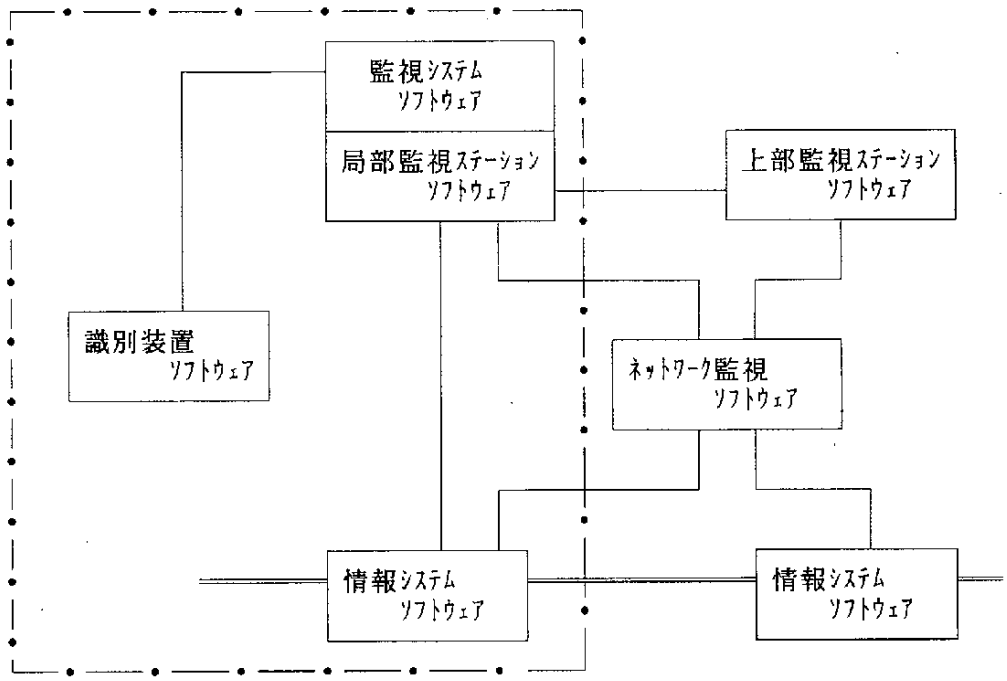


図10　情報システム・ネットワークの基本的構成

3.1　ソフトウェアの種類

(1)　識別装置ソフトウェア

(a)　照合ソフトウェア

照合ソフトウェアは，磁気カード等からの入力カードと記録しているデータを突合し，正規／不正規を判定する。また同時にこれを時刻データ等と共に記録し，開錠等の動作指示を行う。

端末管理の場合は，基本的にはコード読取りのみで，情報システム側にこの照合ソフトウェアが組み込まれる。

なお，識別装置の内，個人の特徴を識別する直接識別方式の場合，照合ソフトウェアは，精度にもよるが，大規模なものになると考えられる。

同時に，個人情報に関するデータベースも大容量になると考えられ，初期入力の工数が大きくなる。

(b) 監視ソフトウェアとのインターフェイス

基本的には，不正アクセスの場合の通報と装置異常程度で，大規模なソフトウェアにはならないと考えられる。

(2) 監視システムソフトウェア

(a) 監視ソフトウェア

防犯システムからの異常警報を受け，異常の確認，場所等の特定を行い，関係部門への通報（警報），記録，必要に応じ対処の指示（避難，消火等）を行う。また定期的にセンターの異常のチェックも行う。

(b) 整備運転ソフトウェア

情報システム用の設備（電源・空調等）の運転制御を行う。省エネルギー運転も行う。これらの制御は，情報システムとの間でＯＮ／ＯＦＦの指示ばかりでなく，情報システムの運転環境のチェックと可否についての情報の送受を行う。

(c) 局部監視ソフトウェア

監視ソフトウェア，設備運転ソフトウェアからの信号を基に，状態の表示，警報の鳴動，上部監視ステーション，情報システム，ネットワーク監視システム等との情報の送受を行う。

(3) 情報システム／ネットワーク監視システム・ソフトウェア

監視システム・ソフトウェアからの情報に基づき，システム運転の一時停止，システムの縮退運転，システムの退避，緊急停止等を行う。また，ネットワーク・システムでは，対象となる情報システムの切離し，迂回指示等も

行う。

3.2 応用例

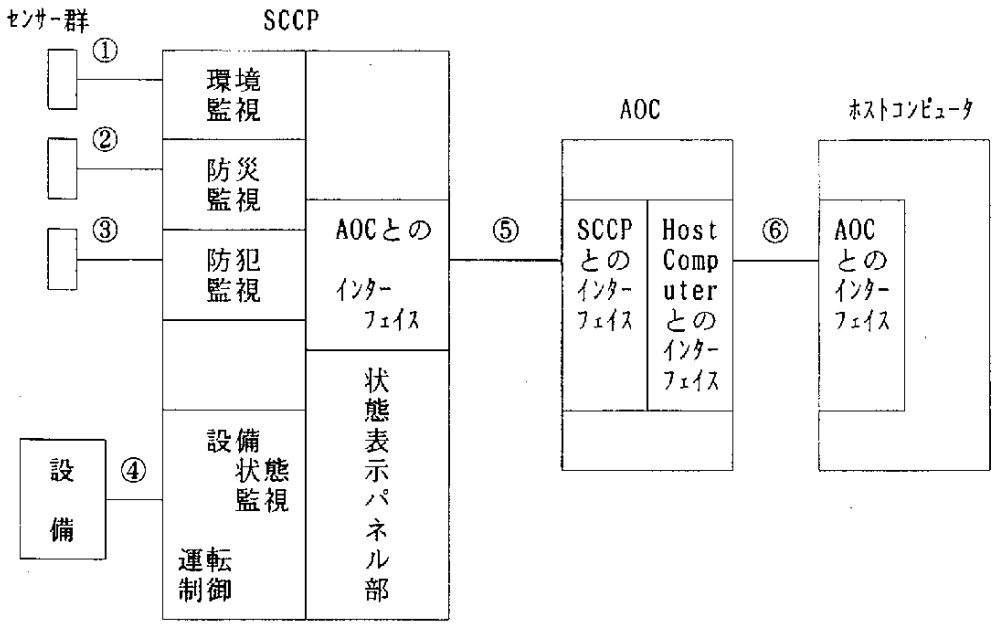


図11 監視システムソフト

① 環境センサーからの信号の受信と異常のレベル判定
（温度，湿度等）

② 防災センサーからの信号の受信と異常のレベル判定
（火災，漏水等）

③ 防犯センサーからの信号の受信と異常時の処理
（侵入等）

④ 設備のＯＮ／ＯＦＦの信号の送受と順次運転制御
設備の運転状況の確認と異常時の処理

⑤ ＳＣＣＰの集めた情報を一括しＡＯＣに送信
ＡＯＣからの設備指示等を受信

⑥ ホストコンピュータの運転状況のチェック
ホストコンピュータの停止に関する情報の送受

4. 将来展望及び市場規模

4.1 アクセス・コントロール

(1) アクセス・コントロール分野への進出

昭和61年度の報告書「セキュリティ産業の成立と今後の展望」では，識別装置について81社の回答中29社が進出しており，その内訳は次の通りである。また，製造，販売，設計・施工で25社が進出している。

製　造	１０社
販　売	２１社
設計施工	１８社
保　守	１５社
サービス提供	１６社

(2) 将来の展望

昭和62年度の警察庁の調査結果「情報処理システムの安全対策に関する調査概要」によれば，アクセス・コントロール関連の実施状況と将来の実施計画は次の通りである。

	実施状況	将来の実施計画
コンピュータ室等の出入口及び開口部への侵入検知センサーの設置	21.5%	14.9%
コンピュータ室等出入口，窓等の閉鎖，施錠	74.5%	21.2%
端末起動のための鍵の利用等の端末操作管理	23.6%	16.5%

コンピュータ室の施設については，かなり高い実施率になっているが，端末機利用については，まだ低い実施率のままである。

(3) 市場規模

(a) 錠前市場

開閉装置として使用される金庫用符号錠・錠前の市場は，現在次のように推定される。

符号錠（鉄扉，金庫用）	3社	約4億円
錠　前（金庫・保管庫用）	5社	約20億円
建築用錠前（電気錠を含む）	主要3社他	約110億円

アクセス・コントロール，監視分野に使用されるのは，主として電気錠であるが，錠前市場における電気錠の割合は不明である。いずれにしても，金庫用・保管用の符号錠・錠前の需要は，将来とも現状規模で推移するものと推定されるが，この分野も各種個人識別装置と組み合わせた電子化が増えていくものと思われる。

建築用錠前については，かなりの成長性が期待され，中でもシステム錠と呼ばれる各種電気錠の成長性が高い。

(b) 識別装置

識別装置（主に入室管理）の市場は，現在約40億円と推定されている。この伸びは，61年度は 150%，62年度は 130%と推定され，少なく見積っても今後 120%の成長が見込まれる。

(4) コード体系統一の課題

個人の特徴を検出する方法は，指紋のように，生涯不変かつ排他性を持つものについては特に問題ないが，カード等コードを利用するものについては，何らかのコード体系の整理統一が必要となろう。

同時に電波等を利用するものについては，その技術基準が必要となる。

4.2 監　　視

(1) 監視分野の動向

昭和61年度報告書「セキュリティ産業の成立と今後の展望」によれば，“成長が著しいセキュリティ分野”の2位にアクセス・コントロール分野，3位に監視分野が挙げられている。また同報告書は，既存業種からセキュリティ産業への進出状況について触れているが，アクセス・コントロール分野および監視分野について見ると，別業種からの新分野への参入というよりも既存技術の延長・応用の傾向が強い。これは，それだけセキュリティ産業の需要範囲が拡大しつつあることを意味するのではないかと思われる。

前述したように，監視分野は監視－感知－警報で完結する単独システムよりも，各種制御システムと一体になったビル管理・オフィス管理などの総合的なシステムの方が成長性は高いと思われる。

(2) 市場規模

(a) フィルムカメラ（サーベランスカメラ）市場

サーベランスカメラの国内市場規模は，長尺フィルムの供給も含めて約40億円と推定される。サーベランスカメラは，その写真の証拠能力が高いことから，主として金融機関の監視用として使用されているが，最近はテレビカメラの性能向上などにより，徐々に防犯用ＴＶカメラにとって替わられつつある。

(b) テレビカメラ（防犯用ＴＶカメラ・ビデオ）市場

ＣＣＴＶによる監視システムの市場規模は，現在約 600億円と推定される。（ただし，ビデオカメラ，レンズ，ハウジング，伝送装置，モニター，ビデオ，コンソールなどを含むが，ビデオ産業向けは含まない。）

先に述べたように，各種センサーを組み合わせる監視システムにより，この分野はかなりの成長性が期待されるのではないかと思われる。

(c) センサーによる監視市場

各種センサー・計測器・監視盤及び監視用ソフトは極めて多岐にわたっ

ているため，市場規模を把握することは難しい。その上セキュリティ分野に限定すると，ほとんど推定が不可能である。しかし，この分野の成長性が極めて高いことは容易に推定されるところである。

関連する分野の市場規模を次に示す。

防犯機器	……	センサー類	約１００億円
		監視盤と送信機	約３００億円
防災機器	……	火災報知設備	約６００億円
		ガス漏れ警報機など	約３００億円

4.3　アクセス・コントロール及び監視ソフトウェア

識別ソフトウェア，監視ソフトウェアとも，現状はハードウェアの一部としてみられている程度で，市場を形成するに至っていないと考えられる。しかしながら大規模化，ネットワーク化，一般社会への普及と共に，ハードウェアから分離し，一定の市場を形成するものと考えられる。

現状では，ハードウェアに付属するものとして扱われ，ほとんどソフトウェアでの市場を形成するに至っていないと考えられる。今後，これが一定の市場を形成するように，指導，啓蒙する必要がある。

Ⅲ．セキュリティ・ソフトウェア

1. セキュリティソフトの重要性

近年，コンピュータの発達，ネットワークの広がり，異機種間接続，パソコンの氾濫等，情報化の進展に伴い，セキュリティ上の問題が発生してきた。

第1は，自分がセンターに入れたデータやプログラムが無事であるか，他人に使われてはしないか。

第2は，顧客からのデータやプログラムがセンター内で無事に保管されているか。

第3は，コンピュータ・リソースが無断で利用されていないか。

第4は，コンピュータ・システムの内部に「トロイの木馬」が侵入していないか。

これらは，セキュリティ面からはコンピュータ・システム（ネットワーク，パソコンを含めた）のアクセス・コントロールだけを頼りに構築されてきている。このアクセス・コントロールのみで，今日の複雑なコンピュータ・システムが安全に，かつ，安定的に稼働できるのかが問題となる。

2. コンピュータ・リソースに対するセキュリティ

(1) アクセス・コントロール

一般的なアクセス・コントロールは，ＩＤ番号，パスワード等が一致すればコンピュータ・システムを自由に使える。これからは，単にパスワードの一致にとどまらず，通信回線自体のセキュリティとしての暗号化装置は勿論の事，通信回線上のデータそのものをソフトウェアにより暗号化する方向にある。

パスワード：第二次的セキュリティでソフトウェア対応で可能であり，特別なハードウェアを必要としない。

暗号化　：①暗号化ハードウェアをコンピュータ間に設置し，ネットワーク上からのセキュリティを確保。コンピュータのネットワーク回線の数だけハードウェアが必要となる。

②コンピュータ自体で転送データの暗号化を行い，コンピュータには特別なハードウェアは必要としない。ただし，暗号化のソフトウェアをコンピュータに処理させるために効率の問題が発生する。

パスワード等による接続許可は基本的には当然必要であり，今後も重要と考えられる。そして，一次的には，接続許可を含めたデータそのものに対するセキュリティを，現状では暗号化手法を用いる事が現実的といえる。

さらにコンピュータメーカが供給している標準ＯＳの中のセキュリティ・ソフトウェアを利用しているのが現状だと思われるが，このメーカ標準のセキュリティソフトで充分であるのかが問題である。ユーザ各社は，独自のセキュリティソフトを標準ＯＳに付加してセキュリティの確保に努めているのが実情であろう。

(2)　保存データに対するセキュリティ

ユーザは普通，処理終了後のデータやプログラムについて，外部記録媒体に保存する。現状，多用されている媒体としては，オープンリール磁気テープ，カートリッジ磁気テープ，フロッピーディスク等である。

しかし，通常，これらの媒体は，内外メーカを問わずにどのコンピュータでも読み取り可能である。つまり，アクセス・コントロールに強力なセキュリティを付加しても，磁気テープを持ち出せば全てのデータやプログラムは自由になるといえる。

この状態を解決するには，磁気テープへの出力時に暗号化を行い，読み取る時に復元させる方法がある。暗号化の方策として，画像処理等で多く使われている。データ圧縮化の手法を用いれば，セキュリティは保持され，データ容量が増加する。

ただし，これにも問題がある。つまり，自社コンピュータ内では，互換性はとれるが，第三者のコンピュータに対しては互換性がとれなくなることである。もちろん，暗号化の処理技法を利用者間で共同利用すれば良いが，これらの管理をどうするのかが大きな問題である。

一つの提案であるが，特定グループで委員会を作り，その委員会で手法や運営，運用について検討し，会員組織で暗号化技術を共同利用する方法が考えられる。いずれにしろ，保存データのセキュリティについて真面目に取り組む必要がある。

(3) ソフトウェア・プロダクトに対するセキュリティ

特にパソコン用ソフトウェア（数千円～数百万円）については，大量に販売する事を目的として価格も安く設定されている。

ソフトウェア供給側にとっては，その資産を守るためにコピープロテクトが重要なポイントであった。しかし，ユーザ側からは，購入ソフトがバックアップ・コピーも不可能なために，常にリード不能の危機におびえながらの利用となっている。

今日では，コピーフリーのソフトが多くなりつつある。これは，供給側と利用者側の両方にとってメリットが大きい。セキュリティはどうするのかというと，一種の暗号化装置をソフトウェアに付属させて，ソフトウェアの使用に際してはその暗号化装置をパソコンに取り付けて使用する方法が注目されている。

また，大型コンピュータ用ソフトウェアについては，供給側と利用者側の契約等により規制されていたり，ソフトウェア自体で使用回数や使用時間がシステムに自動的にファイルされるような構造であったりするので，不正使用はより困難であるといえる。

(4) ビルオートメーション．ソフトウェア

コンピュータ・センターのセキュリティになると，コンピュータへの論理的アクセス（通信回線経由等）と物理的アクセスとに分かれている。ここで

は，物理的なコンピュータ・セキュリティについてのソフトウェアについて考えてみたい。

まず第一に，入退室（館）管理については，現状のコンピュータ設置場所には何らかのガードシステムが設置されていると思われる。しかし，一部大手センターを除いて，大部分は単に暗証番号のみとか，カード保持者はフリーとか，簡易システムでの運用がほとんどと思われる。そこで，入退室（館）管理はどうあるべきか，どのようなソフトウェアで制御されるべきかが問題となる。

物理的ガードシステムの第一ステップである入退室（館）システムは，

①個人識別ができること

②２重以上のチェックを行うこと（カード＋暗証番号等）

③正常，不正を問わず記録が完全に残ること

④不正解錠，不正解扉が検知できること

⑤個人に対して各種のレベル設定が可能なこと

⑥パスバック制御可能なこと

⑦個人の登録，抹消を随時行えること

⑧他のビル管理機器との連動がとれること

次に，ビルオートメーションについての，現状のビル管理システムは，監視が主目的であって，積極的に制御を行っていない。しかし，インテリジェントビルの出現により，ビル管理はビルオートメーションへと発展し，監視から制御に移る必要性が生じてきている。

これまでの監視に加えて，空調，電気，エネルギー等のリアルタイム制御（停電時のバックアップ，石油ガス等のエネルギーコスト）が必要となる。これからは，スケジュール運用＋リアルタイム制御＋コジェネレーション制御のビルオートメーション・システムが注目されると思われる。

Ⅳ. コンサルティング

1. 分類と概念

セキュリティに関連するコンサルティングとしては，いくつかの分野にわけることができるであろうが，ここでは次の3つをとりあげ，その内容を概観することとしたい。

そのひとつは，コンピュータ・システムそのものに対するものであり，いまひとつは，コンピュータ・セキュリティにしぼったものである。そして，これらの他に，システム監査に関するコンサルティングが誕生している。

1.1 コンピュータ・システムに対するコンサルティング

企業が保有するコンピュータ・システムは，それぞれ多種多様の悩みをかかえているといっても過言ではない。コンピュータ・システムが単純な事務合理化のツールであった時代には，種々の計算を機械化する道具として，コンピュータはそれなりの成果をあげてきた。ところが，昨今のようにコンピュータ・システムそのものが経営戦略に直接影響を与える時代となり，システムの内容も高度化，複雑化してくると，そのシステムの良し悪しが企業そのものの存続にかかわるといえる。

このような時代になると，「良いシステムづくり」に企業は必死になって取り組まなくてはならないが，世の中の動きが速くシステム化のノウハウが社内には十分に蓄積されていないなどの理由により，新しいシステムづくりの方向性に悩んでいる企業が多い。

具体的にコンピュータ・システムに対する問題意識をピックアップしてみると，次のようなことがいえる。

- システム化計画が十分に検討されていない。
- システム導入の結果に満足していない。

・コンピュータメーカの指示にたよりすぎている。
・同業他社のシステムの動きをしっかり把握できていない。
・ユーザサービスにシステムを十分活用できていない。
・コンピュータ要員教育が期待どおりの成果をあげていない。
・コンピュータ情報は十分に入手し理解されていない。
・将来の環境変化に対応できるだけの準備がなれていない。
・安全性が十分考慮されていない。

このように，コンピュータ・システムに対して多くの問題意識を持つ企業は，ますます増加するものと考えられ，さらには，それらの問題を解決してゆくために幅広いノウハウが必要になるので，それぞれ自社内では解決が困難になってくる。

したがって，必然的に「コンピュータ・システムに対する総合的専門知識」を持った外部機関にコンサルティングを依頼したいというニーズが強くなっているのが現状である。なお，この分野では，システム・クリニックという表現も使われている。

1.2　コンピュータ・セキュリティのコンサルティング

コンピュータ・システムが単純な事務合理化のツールであった時代は終わり，企業経営にとっても，また，巨大システムであれば社会にとっても，大切なインフラストラクチャアである。従って，コンピュータ・システムが安全に運用されるということは，ひとつの社会的要請である。

ところが，コンピュータ・システムは，特別な注意を払って運用しなければ，社会的要請に耐え得ない本質的な脆弱性を秘めている。この社会的要請と脆弱性との間のギャップを埋めて行く手段をコンピュータ・セキュリティとして考えてみたい。

この手段を次の３つのカテゴリーにわけてみる。

・ハードウェアの問題

・ソフトウェアの問題

・人間の問題

最初のハードウェアの問題は，コンピュータのハードウェアおよび設置などに，2番目のソフトウェアの問題は，コンピュータ・ソフトウェア（セキュアOSやアプリケーション・ソフトウェアに関するプログラム・テクニック上の対策）および手続規程類などに，3番目の人間の問題は，資質，配員・教育訓練などにわけて考えることができる。

各カテゴリーに属する諸問題が満足できる状態にあれば，一応はよいであろうが，さらに，これらのカテゴリー別の手段が満足すべき状態にあるか否か，ないならばそれに対してはいかなる措置をとるべきかを「視る」必要がある。これを監査と位置づけることができよう。

上述の手続規程類および教育訓練のうち，設置は「電子計算機システム安全対策実施事業所認定規程」にもとづく設備基準に，他は運用基準に記載されている項目である。コンピュータ・セキュリティのコンサルティングは，これらの各項目に関してクライアントの相談に応ずるものである。

主な項目は次の通りである。

・安全対策ということの考え方に関する事項

・認定基準に関する項目（設備，運用とも）

・規程類の整備に関する事項

・教育訓練に関する事項

・内部監査に関する事項

・認定申請に関する事項

これらに付随する事項もあり，相談などの範囲はかなり広く，安全対策にからむ組織論から始まり，キー・エントリー・オペレータの頚肩腕症候群にまで及ぶ。

1.3　システム監査のコンサルティング

大手の監査法人では，システム監査部を設置してコンサルティング事業に乗り出すケースが増えている。これらは，従来，財務諸表監査の一環として行われていたが，今日では財務諸表監査の流れの中で行うものとは別に，別途独立したシステム監査コンサルティング事業が出現している。

監査法人以外でも，ソフトウェア・メーカーをはじめ，システム監査コンサルティング分野に進出しようとする企業が増加してきている。いずれにせよ，収益があがるという段階よりも，ニュービジネスとして注目されている段階といえよう。

2.　コンピュータ・システム・コンサルティングの例

A社では，第三者的・中立的な立場でのコンピュータ・システムに対するコンサルティングをビジネス化した。その分野は，コンピュータ・システムに対する問題意識全般にわたっており，各企業がかかえている悩みに幅広くカウンセリングしていこうというものである。対象分野を具体的にあげると次の通りである。

(1)　計画・管理に関するもの

- 短，中，長期計画立案
- プロジェクト・マネジメント
- 標準化
- システム移行
- 機種選定
- 要員教育
- 安全対策，災害対策
- その他

(2)　設計・開発に関するもの

- ネットワーク設計

・データベース・システム設計

・オンライン監査ユーティリティ

・コンピュータ・周辺機器の性能評価

・ソフト開発ツール

・対外接続

・ソフトウェア・ハウスの活用方法

・その他

(3) 運用・管理に関するもの

・マネジメント，スケジューリング

・オペレータ部門管理

・ネットワーク管理

・端末側指導

・設備管理（コンピュータ，電源，空調）

・安全基準認定

・トラブル対策（オンライン，バッチ）

・その他

(4) アプリケーションに関するもの

・流通情報処理

・資金決済処理

・ストア・オートメーション

・物流コントロール

・クレジット・オーソリゼーション

・財務会計，管理会計

・営業情報システム

・その他

(5) 機器導入に関するもの

・コンピュータ及び周辺機器

・オンライン端末，ＰＯＳ端末

・その他

(6) 保守，移行に関するもの

・テスト検証ツール

・異機種間移行

・システム監査

・コンピュータ・センター移行

・その他

(7) 最新技術

・複合ネットワーク・システム

・海外複合ネットワーク・システム

・ＶＡＮ

・ＬＡＮ

・異機種間接税

・ＡＮＳＥＲ，ＦＡＸ変換

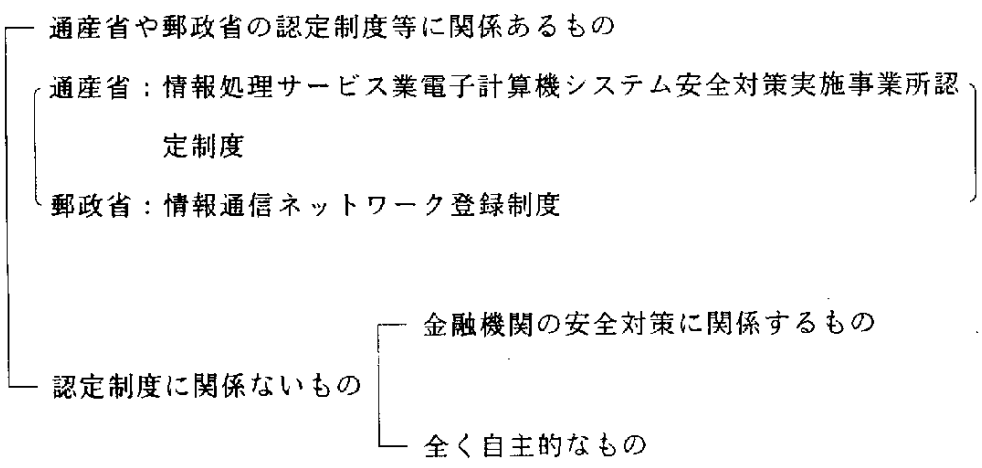
・複合インテリジェント・ターミナル

・その他

以上，多岐に亘っており，幅広いユーザニーズに応えようとするものである。現実にこの企業は，前述した種々のジャンルで多くの企業に対するコンサルティングを実施中であり，コンサルティング・ニーズはますます増加するものと考えられ，潜在ニーズは計り知れない。

3. コンピュータ・セキュリティ・コンサルティングの例

B社は，コンピュータ・セキュリティ・コンサルティングに早くから着手している。その内容を分類してみると，次のとおりになる。



コンサルティングの事例として圧倒的に多いのは，通産省の認定を得るためのものである。主として次の項目にかかわる。ただ，広狭深浅は，全くクライアントの要望によりかわってくる。

- 安全対策の考え方について
- 認定を得られるようにするための設備について

  （最初の段階からはじまったり，すでに設計が決まってしまってから相談を受けたり，種々のケースがある）
- 社内規程類の整備について
- 認定申請書の整備について
- その他

つぎに，金融機関の安全対策に関するものがある。これは，通産省や郵政省の認定制度等と関連あるものがかなり多く含まれている。したがって，相談項目は，上述の通産省の認定制度に関するものと大同小異といってもよい。認定制度と無関係のときは，上述項目から認定申請書の整備に係るものが除外されることになる。

少数例ではあるが，全く自主的に安全対策の現状を設備・運用両面にわたってチェックし，その不備な点を指摘し改善策をもとめたり，または規程類の整備（作成）をもとめたりする例がある。

4. システム監査コンサルティングの例

C社は，システム監査部を設置して，システム監査のコンサルティング事業を展開している。対象分野を具体的にあげると次の通りである。

(1) 監査（信頼性中心）

- アプリケーション・コントロール
- 情報システム部門のコントロール
- 実行（ＣＡＴＴＳ）

(2) 評価

- 情報戦略
- システム開発監査
- セキュリティ監査
- パッケージ評価

(3) 教育

- 社内
- 社外（顧客，一般）

5. 将来展望と課題

(1) コンピュータ・システムは，今後ますます複雑化，多様化の一途をたどりその信頼性，安全性をおびやかす要素もホスト・コンピュータからネットワーク，端末まで範囲が広がる。各企業が，企業生命をかけて行っているシステムに対するセキュリティ対策は，より重要度を増すことになる。

これからは，コンピュータ・システムに対するセキュリティ対策，システム監査は，より高度に要求されてくると考えられ，各企業ともそれに対する高度なノウハウを必要とするため，専門機関に対するコンサルティング・ニーズも大きくなろう。

(2) 情報やノウハウに対価を払うというセンスは，実際にビジネスをとおして少しづつ変化を感じとることができる。

また，単に「マンパワーを節約するためにコンサルタントのところにくる」という考え方から，「コンサルティングからノウハウを買う」というような考え方にかわりつつあるように見受けられる。クライアントの態度に微妙な変化を感じることができる。この傾向はつづくであろうし，またそうあってほしい。

(3) 海外，特に米国における安全対策の「認識面」として次のような指摘があげられる。まず，「安全対策は経営の資産である。」という認識が浸透しているという。すなわち，安全対策ということは資産の保護（貸出資産と同等であり，安全対策の怠慢は資産の償却）であるということである。つまり，保険料とか必要悪的経費とかいう考え方とは全く対照的な認識をもっているということである。水と安全はタダと思い込んでいる我々に対してはよい警告となろう。

V. 防犯・防災センター

1. 防　犯

1.1　情報化社会と防犯

これからの高度情報化社会における犯罪は，従来のような単純な犯罪と異なり，極めて知能的でかつ多様化してくるものと考えられる。例えば，銀行強盗のような犯罪よりも，コンピュータを駆使した巧妙な新しい手口の犯罪が増加することになると思われる。

現在でも金融機関などでは，すでに外部からのコンピュータ犯罪に対しては相当の防護策が施されているといえるが，今後各家庭が情報ネットワークに入ってきた場合を想定すると，ホームセキュリティは究めて重要な位置づけになる。

内容も，単なる防犯（すなわち犯罪を防ぐ）のみでなく，医療，衛生管理，老人対策，地域がらみのセキュリティ等，日常の安全を基本として，これらを保護することが必要になってきている。

さらに，企業間においても，ビルはインテリジェント化され，各種の企業がネットワークによって結ばれ，国際的に情報が流通している時代に入っている現在，セキュリティは不可欠の要素となっている。そして，このような社会の変革にともなって，警備業の実態も大きく変わりつつある。

1.2　警備業の現況

(1)　概況

警備業は，原子力発電所，インテリジェントビル等から一般家庭に至るまでの各種の施設，建物の規模，目的によって，人による常駐警備から建物全体のセキュリティ等まで，その需要がますます増大している。

警備業者数も年々増加傾向を示し，昭和61年12月現在では，4,282業者，警備員の数は約18万 8,554名となっており，警備業法施行時（昭和47年11月1日現在の警備業者 775業社，警備員4万 1,146名）に比較すると警備業者数は 5.5倍，警備員数は約 4.6倍に達している。

特に近年は，夜間，休日の無人化が，金融機関の土曜休日化にともなうCD，ATMの自動化等によて促進され，機械警備分野の需要が急速に増大している。したがって，機械警備業者は，認定業者全体の14.2%を占める 608業者，機械警備業務対象施設は33万 5,645か所に及んでおり，機械警備は警備業の主流になりつつある。さらに，警備内容も従来の防犯，防災に設備関連（満減水，エレベータ等）の監視等のニーズもでてきたため，この分野の役割も警備業者が担っていくことになると思われる。

(2) 警備業者の規模別状況

資本金別にながめると，1,000万円未満の企業が59.8%と過半数を占め，それに個人経営を含めると66.0%に達する。1億円以上の企業は，2.5%にすぎない。

警備員数では，50人未満の企業が81.8%と圧倒的に多く，500人以上の企業はわずか 0.7%にすぎない。

表5　資本金別業者数

資本金規程	業者数	%
個人企業	267	6.2
50～1000万円未満	2,562	59.8
1000～5000万円未満	1,214	28.4
5000～1億円未満	134	3.1
1億円以上	105	2.5
合計	4,282	100.0

表6　警備員数業者数

警備員数	業者数	%
50人未満	3,505	81.8
50人～99人	458	10.7
100人～499人	290	6.8
500人以上	29	0.7
合計	4,282	100.0

1.3. 今後の方向

現在の警備業の市場は，年間 2,600億円程度といわれているが，実態は極めて不明確である。警備内容については，防犯，防災が主力であるが，今後は防犯，防災に加えて設備関連を中心とした情報化に伴う分野に拡大していくであろう。これらは，あくまでも機械警備の発展を意味するものであるが，人による警備も単なる常駐警備に止まらず，数々な分野でのヒューマンサービスに転換していくものと思われる。

機械警備は，通常，マン・マシン・システムと呼ばれる通り，機械と人とのリレーションによって運用されているが，メーカーと異なり，人によるサービス体制がこの業種の特徴であり，今後ともシステムが発達してもそれなりにヒューマンサービスの必要性は増大するものと思われる。

また，防犯関連のメーカーは，現在防犯センサーを中心として製造し，警備会社に対して販売しているが，警備内容が多角化することで使用するセンサー類およびセンサーマシンも変わってくることが予想されるので，参画するメーカーも増えるし，現在の防犯機器メーカーも新しい機器の開発を迫られることなろう。

2. 防災

2.1 情報システムと防災

情報システムに関連して，防災がクローズアップされるのは，通常，実際に災害が発生してからのことである。わが国でも，防災を認識させるうえで転機となった出来事はいろいろある。

例えば，昭和53年６月に発生した宮城県沖地震では，大は建物の崩壊から，小はＣＰＵの横すべりまで，同地域の数多くの情報システムが影響を被った。その結果，情報システムへの地震対策が大きな問題となり，対策が進展するきっかけともなった。

また，昭和59年11月に発生した電電公社世田谷電話局管内におけるケーブル火災では，情報化社会において情報サービスが切断されることがいかに重大な問題であるかを国民全般に認識させ，火災対策やバックアップ対策が大きくクローズアップされた。

これらの他にも，いろいろな事故や事件が発生し，その都度コンピュータ・セキュリティが問題視されてきた。そして，防災面からも，コンピュータへの影響を最小限にとどめるための方策などもとられてきている。例えば，コンピュータ室の消火設備としては，ハロンガスが着実に伸びていることなどはその例である。

2.2 防災関係業界の現況

(1) 火災報知機

火災報知機は，消防法に基づいて設置が義務づけられている関係上，メーカーではビルなどの義務設置対象物件の新設に対応して製造販売（工事を含む）を行っている。

自動火災報知設備の市場は，年間約 1,200億円～ 1,300億円と推定されているが，値引競争が激しく実質需要は 700億円～ 800億円程度となっている。

この業界の特徴は，消防法によって，義務づけられているため，年間のビ

ル新築件数により確実に一定量の需要が確保されている。その反面，新しい市場に対する進出は究めて消極的であるとともに，値引き競争により新規開発が思うようにできないのが現状である。

近年，インテリジェントビルが建て始めたことで，火災報知システムも大型物件については大きく変わりつつある。また消防側でも検定規格外の機器を承認する制度が設けられるなど，新しいシステム分野では門戸が開放されたので，今後技術面でも変わっていくものと思われる。

(2) 消火設備

自動消火設備には，次のような種類がある。

（イ）スプリンクラー，消火栓，ドレンチヤー・・・一般ビル，神社，仏閣，他

（ロ）泡消火設備・・・ガレージ，石油コンビナート

（ハ）粉末消火設備，消火液，・・・厨房等

（ニ）ハロンガス消火設備・・・・・コンピュータ室，機械室等

消火設備も，消防法に定められた基準で義務づけられているので，火災報知機と同様に一定量は確実に需要がある。消火装置は年間実質ベースで以下の通りである。

• スプリンクラー	420億円
• 泡消火設備	70億円
• ガス消火設備	210億円
• プラント	100億円
• 道路防災	40億円
計	840億円

消火設備の主流は，スプリンクラーであるが，現在水関係の下請業者が年々減少傾向にあって，工事を取っても下請業者がいないという現象すらみられる。ガス（ハロン1301）については，コンピュータ室，機械室，動力室等は二次災害のないハロンを使用している。これは，炭酸ガス消火設備と

較べて，消火原理が窒息消火ではなく化学反応による消火反応による消火方式なので，人畜無害の点で最近は年々増加している。特に情報化時代となった今日，電算室にはほとんど設置されている。

消火設備は，配管工事が主体で，機器の占める比率は，10％程度で，昨今のエレクトロニクス技術に負う部分が極めて少なく，従って技術面での改新が非常に難しい状況である。近代化するビルの消火剤として水を使用することは，二次災害の点からも種々問題をかかえているが，未だに水にかわる消防設備は確立されていない。しかし，火災報知機を含めて，将来のホームセキュリティの中での防災を考えると，そのニーズは高く，業界としてはこれからの研究開発を推進する必要に迫られている。

(3) 消火器

消火器の主力商品は粉末消火器（95％）で，昭和58年は年間 400万本，59～62年までは平均 300万本～ 330万本，63年は64年２月の型式失効期限があるため，約 370万本が見込まれている。年間の需要は卸売価格で 200億程度の市場である。消火器は火災報知機，消火装置と同様，消防法による義務設置のため一定の需要はあるが，消耗品ではないのでその伸びは小さい。しかし，59年～62年までの市場のうち，40％は法適用外に販売されているので，少しづつ一般需要者への市場に進出し始めてきたといえよう。

欧米を中心とした海外市場は，ハロンガス系の消火器が急速に増加している。欧米では，ガスボンベの規格が日本と較べて厳しくなく，プラスチック製ボンベでも強度があれば認められているため，取扱い上便利なハロンガスを使用した消火器が普及している。日本の場合，ボンベの規格が現在でも高圧ガス基準によって鉄製品のものしか認められないので，ガス系の消火器が普及していない。

今後は，海外から，これらの低価格の消火器が大量に日本に上陸してくる可能性が大きく，その場合，国内の現メーカーの対応が大きな脅威にさらされることになろう。ただし，昨今，米国でフロンガスの大気汚染の問題が取

上げられ，ハロンガスもフロン系ガスとして今後規制の対象となってくる可能性もある。日本としては，今後いずれにせよ海外商品と競合できる商品を開発する必要がある。消火器も，義務設置外の一般需要は未だ伸びる余地があるので，低価格化，メンテナンスフリーの商品が開発されれば，需要は大きく拡大されると思われる。

(4) 今後の方向

現在の防災業界は，総括して消防法に基づいて過去伸びてきた業界で，その点非常に手堅い需要に支えられている反面，新しい市場開拓が難しい。需要者側のニーズが「消防に規制されるから設置する。」という考え方が現在でも強いことと，メーカー側の新規市場（義務設置外）を開拓する積極性も余りない。

一方，従来は消防法に基づく検定規格がきびしく，防災機器はすべてこの規格の適合しなくては売れないことになっていた。このために，新しいエレクトロニクスを使用した商品化が遅れたこともあって，最近は自治省消防庁が，検定規格外の新しいシステムでも，日本消防安全センターの主宰する委員会で認められれば設置できるようにした。今後の情報化社会については，セキュリティの中で防災の占める分野がさらに大きくなるのは明らかであり，新しいニーズも多面化してこよう。業界がこれらのニーズにどう対応するかが，これからの問題である。市場はますます拡大するが，業界自体が従来の体質から早く脱皮して，急速に変化する今後のニーズに対応していくことが必要である。

Ⅵ. システム・バックアップ

コンピュータ・システムは，データ，ハードウェア，通信が結合したものである。システムが社会経済活動の中枢的役割を果たしており，全産業的に浸透し，セキュリティの確保は産業の保護の問題となり，ネットワーク化の進展に伴って社会的インフラストラクチャを形成しており，企業の社会的責任の問題でもある。

従って，企業は自らのシステムに対する災害予防対策の確保は当然であるが，さらに被災時復旧対策を構築しておく必要がある。

1. システム・バックアップの現状

1.1 データのバックアップ

データの保管事業について，運輸省が行なったトランクルーム・サービス業者（磁気テープ，書類のほか家財，美術骨董品，毛皮の保管を含む）の実態調査結果（61年運輸白書）によると表7の通りである。

しかし，これはただ単に非商品保管倉庫事業（いわゆるトランクルーム）としての状況であって，システムの重要データをバックアップする設備としては保管形態に問題がある。

データの安全保管のためには，災害から同時被災を避けて50㎞以上離れたロケーション，強固な地盤，安全な環境，データの搬送から保管までの一貫性が必要条件とされるが，事業者のうち以上の条件を全て備えているところは極めて僅かである。

表7　トランクルーム・サービス　取扱い品目別事業者数

（昭和62年7月調査）

取扱品目	取扱事業者	備考
書類	44社　72営業所	うち書類のみ14社15営業所
家財（ピアノを除く）	42　81	うち家財のみ11社18営業所
衣類（毛皮を除く）	19　24	
美術骨董品	16　23	
毛皮	15　19	
ピアノ	21　31	
磁気テープ マイクロフィルム	18　27	うち磁気テープのみ1社 マイクロフィルム1営業所
貴金属・装身具	2　4	
その他	17　19	精密機械，レコード， 祭礼用品等

1.2　ハードウェアのバックアップ

ハードウェアのバックアップセンター事業者として，現時点で本格的にバックアップセンターを運営している事業者は1社である。他には計算センター等でコンピュータの余力をバックアップ用に提供するとしているところがある。

現在，大手金融機関等が，自前で本格的なバックアップを構築中であり，ほかに一部大手企業ではシステムの一部を自社内バックアップすることを検討している。

この事業には莫大な投資が必要とされる。また，とりわけ地震等の広域災害時のバックアップ対策には限界があり，ユーザのニーズに対応できないことが問題点である。

1.3　通信のバックアップ

通信のバックアップ事業者となり得るのは，ＮＴＴ，第２電々グループ，衛星通信業者グループである。企業自身が，平常時利用と併せて災害対策として地上回線の二重化をし，衛星通信の利用を検討しているもので，企業にとっては大きな負担となっている。

2.　米国におけるコンピュータ・システムのバックアップの現状

米国においては，“情報は資産”との認識と同時に“情報の安全保管・運用は社会的義務”（特に対株主，投資家，官公庁）との認識が，日本以上に企業のマネジメント・クラスに強いと言える。この理由としては，次のようなことがあげられる。

(1)　1977年のＦＣＰＡ（海外不正取引防止法）等に見られるように連邦法上から，マネジメントの企業データ保護が義務づけられている。

(2)　企業会計のＧＡＡＰ（一般会計原則）として，企業資産であるデータ保護のために必要なコントロールを講じる事が一般常識化している。

(3)　ＦＦＩＥＣ（連邦金融機関検査協議会）やＡＢＡ（米国銀行協会）等の各種機関・団体等が積極的にセキュリティ・ガイドラインとかバックアップ・マニュアルを作成・公表しプライベート・セクターの啓蒙運動を積極的に行っている。

(4)　連邦政府のセキュリティ対策促進機関が大きくいって商務省標準局（ＮＢＳ）と一つの窓口となっており，各種の情報提供やアドバイスを効果的に一本のパイプで提供している。

(5)　企業における情報システムの内部監査体制の一環として，システム監査制度がかなり浸透している。

以上のようなシステム・セキュリティに対する関心の強さ・積極性の反映として，ハード，ソフト（データ）に対するバックアップの現状も以下のように

わが国と異なった面を呈している。

まず，データのバックアップに関しては，正確な統計はないが国内のデータ保管企業数は約 200社位あるといわれている。保管内容は，例えば病院のメディカルレコード（カルテ，レントゲンフィルム）等のように毎日多量に発生する書類及びコンピュータ・メディア，マイクロフィルム等があり，それらに対する外部分散保管の需要が増大している。保管形態としては安全保管のための物理的条件（空調，電源，消火設備，監視設備等）を備えた地上建物の他に，鉱山跡や洞窟や地下道（鉄道からの払い下げ）を利用したものもある。

また，ハードのバックアップに関しては，自社によるバックアップ・システムの構築，他社システムとの相互バックアップ・センターの利用，第３者提供のバックアップ・サービスの利用等が積極的に実施されている。特に第３者提供のバックアップに関しては，わが国のホットサイト（代替コンピュータ設置済）サービス企業が１社であるのに対して，米国には30社近くあり，またコールドサイト（コンピュータ無しで設置スペースを提供）サービス企業も15社近くある。勿論，全国に拠点を持つ企業では，各センター間でのバックアップ等もかなり行われている。また，米国では特定機種（ＩＢＭ）ユーザのシェアが大きいこと，国土の時差が大きいこともバックアップ体制をとりやすい環境にある。

そして，代替システム用通信回線は，従来の電話回線利用から高速デジタル回線利用が進んでいる。

3. システム・バックアップの将来

コンピュータ・システム時代のインフラストラクチャ整備として，そのバクアップの必要性はますます高まり，その投資規模は大きな産業振興となろう。

3.1　設備について

結論的にいえば，データ，ハード，通信の3つを総合的にバックアップする機能をもったセンターが必要となろう。

(1)　データのバックアップ

データの保管形態については地震災害（広域災害）に対応できるセンター，即ち，同時被災が避けるロケーション，強固な地震，安全な環境，データの搬送から保管までの一貫性が必要条件とされるべきである。また，通信によるデータ・バックアップの即時性も要求される。

(2)　ハードのバックアップ

○　バックアップの形態

会員制による共同バックアップ・センター（ホットサイト・タイプ）と災害時にユーザがコンピュータを持込設置するために建物・施設を提供するセンター（コールドサイトタイプ）があるが，ホットサイトの場合単独災害についてはかなりの企業を対象にサービスを提供できるが，地震等の広域災害については災害ユーザへのサービス提供に限界があり，マシンの時間貸的なものが考えられる。

○　機種の互換性

同一機種のバックアップ・サービスは，各機種の設置で莫大な投資となる。従って，ハード，ソフトの互換性の解決が課題である。

○　企業内バックアップの促進

○　企業間提携によるバックアップの促進

○　要員及び良好な生活環境の確保

(3)　通信のバックアップ

バックアップとして回線の二重化はますます増加すると思われる。そのためには回線の低コスト化が課題である。とりわけ，衛星通信への期待は大きくなる。これはセンターの，郊外の安全な環境立地を可能にすると同時に，全国的なシステムのバックアップを可能にする。

また，データバックアップのオンライン化によりファイル保全と処理代行の二つのサービスを可能にする。

3.2　政策的助成について

企業の安全対策に対する投資が少ない。保険で見ると日本は個人の立場では保険天国であるが，企業の社会的責任から見た場合の保険投資（即ち，安全対策投資）は少ない。従って法制化，行政指導によってバックアップ体制を促進させることが肝要である。また，バックアップ事業の投資額は大きく，採算的にも長期的考えに立つ必要があり，この事業に対する税制上の配慮と低利融資等の政策的助成が必要である。

Ⅶ．ファシリティマネジメント・サービス

ファシリティマネジメントは，設置・調整が終了し，運用に入ったシステムの日常の運転，システムの増設等，ソフトウェア（ＯＳを含む）の保守，ハードウェアの保守等の総合設備管理を意味する。

セキュリティ・システムについても，日常の運用・監視・システム（センサー系を含む）の増・移設，ソフト保守，ハード保守等が発生する。特にセキュリティ・システムの場合，受益者にとって，直接運用等にかかわることが少なく，あたかも空気や水のごとく，直接的にシステムを認識することはほとんどないといえる。

従って，このファシリティマネジメント・サービスは，非常に重要な意味がある。特に緊急時の，また故障（障害）発生時の対応時間が重要になる。

1. 目　　的

これは，セキュリティ・システムの運用開始後のシステムの運用，ソフトの保守・ハードの保守の全般にわたる業務である。

システムの運転は，監視または機械警備の担当者を兼ねることになるが，基本的には技術者が行うものと定義する。そしてシステムの稼働，記録等を行い，必要があれば一次保守を行う。

また，システム（センサー系を含む）の増移設の工事の管理を行い，システムの保守（ハード）についても，定期的および障害時に行う。

さらに，システムのソフトウェア（ＯＳ，アプリケーションいずれも）のバージョンアップ，増設等に基づくシステム・ジェネレーション等の保守を行う。

2. 分　類

2.1　システム運転・監視

セキュリティ・システム各種設備の運転・監視を行う。同時に緊急時の一次対応，関係部門への通報等，システムをカバーして人為的に行う。

同時にシステムの増移設に際しては，設計のチェック，工事方法のチェック，進行管理，システムとの連携（システムの一時停止等），完成チェック等を行う。

特に全システム（セキュリティ・システムばかりでなく情報システム／ネットワークまで）の把握と，担当システムの位置づけ等，総合システム技術が要求されるようになる。

2.2　ハードウェア保守

各装置にシステム等のレベルでハードウェア上の障害の摘出と修理を行う。また，定期的に予防保守も行う。

2.3　ソフトウェア保守

各装置，システムの基本ソフトウェア，システムごとの応用ソフトウェアまた情報システムのソフトウェア等の変更・更新，増設によるソフトウェアの変更等の保守を行う。

3. 市場規模

3.1　ハードウェア保守現状

日経コンピュータ誌（1986年7月7日号）によれば，次のようになっている。

(1)　保守拠点

コンピュータメーカは，保守対応期間1～2時間を目途に拠点を設けており，300拠点程度（国産メーカ）を設けている。

(2) 保守要員

コンピュータメーカ8社で約19,000人程度の保守要員をかかえている。

(3) 売上げ

コンピュータメーカ8社で次のようになっている。

1983年	2,783億円
1985年	3,458億円
年平均	11%の伸び

3.2 将来の展望

ハードウェアの保守ばかりでなく，ソフトウェアの保守，設備の保守等，今後システム化されるに従い大きな成長が見込まれる。

4. 問題点と対策

4.1 問題点

(1) 保守対応時間

情報システムが社会に密接にかかわり合うに従い，情報システム，セキュリティ・システムの障害が重大な問題を引き起すことになる。従って障害発生時の対応，修理の迅速化が問題になる。

(2) 保守要員の問題

急速な情報化社会への発展に伴う保守要員，特に総合システムを管理するスキルを持つ保守要員の育成が求められる。

4.2 対策

(1) 保守拠点の整備

現在コンピュータメーカは，国産3社はそれぞれ約 300拠点程度を整備し，保守対応1～2時間を確保しているが，これと同等またはそれ以上の拠点の整備が求められ，この整備のためのコストに対応する措置が求められる。

(2) 保守部品の整備

保守拠点の整備と同時に，保守部品の整備が必要となり，この保守部品の投資コストに対する補助，及び資産としての税制上の措置が求められる。

(3) 技術者の育成

保守体制の急速な立上りを求めるための技術者の育成が求められ，当面，育成にかかるコストへの補助が求められる。

第３章　ライフスプリング計画

「ライフスプリング」計画

1. 基本的視点

セキュリティ産業において産出される製品やサービスは，今後，急速に家庭へも浸透していく可能性を見せている。その1つが，ホーム・オートメーションの進展である。ホーム・オートメーションに対するセキュリティ対策が重要なことは当然であるが，他方，人間として豊かな生活を営むためのセキュリティ・サービスにも着目しなければならない。

家庭の情報化が進展し，情報化の弊害が現れる可能性があるとすれば，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ねばならない。家庭の情報化は，これから本格化すると思われるので，それに対するポリシーを明確にしておく必要がある。なぜなら，家庭の情報化で問題が発生すれば，それは年齢に関係なく即一般国民に被害が及ぶことになり，事前の手当がより重要だからである。このような観点から，この「ライフスプリング」計画は，大都市における人間性回復を基本とし，安心して生活できるライフステージを提案するものである。本年度は，その初年度としての概要計画であるが，次年度以降，さらに具体的な詳細計画の立案へと進める予定である。

2. 現状認識

今日，大都市におけるサラリーマン生活は，あらゆる意味で限界に達している。物価は高く，土地の高騰は住民を周辺に追い出し，通勤に往復4時間が常識化しつつある。マイホームを取得すれば，遠く，小さく，ウサギ小屋からマッチ箱へ，そしてローンだけが肩に重くのしかかるといった具合になりかねない。

この結果，サラリーマンは，仕事でのストレスに加えて，超過密の通勤地獄によるストレスが重なり，放置すれば，ただ単に生きているだけの人生になり

かねない危機的状態にある。これが豊かな国といわれる日本の大都市（とくに首都圏）周辺サラリーマンの実態である。サラリーマンは諦め，都市が嘆いている。これらについて，回復の手立てはないのだろうかという発想が，この計画の立案にとりかかった動機である。

資源が乏しく，創意工夫で成長してきたわが国経済にとって，サラリーマンが疲弊し，活力を失ってしまっては未来は絶望的になる。このままで，都市と生活との融和が完全に壊れてしまう。この時点において，21世紀に向けての大都市におけるサラリーマン生活の再構築を，都市との融和の中で検討してみる必要がある。

しかしながら，基本的な問題として，土地問題が横たわっている。この土地問題は，土地政策の問題であり，われわれに解決できるものではない。したがって，ここでは，住機能，住環境，住空間等の問題に焦点をしぼり，情報化にて解決することを基本とした。

3. ライフスプリング計画

上記のような問題意識から，本委員会では，“21世紀における大都市のサラリーマン生活のあるべき姿”を，生活の情報化とセキュリティ・システムの観点から，1年間にわたり検討してきた。ここでは，“人間性の尊重”という原点にもどり，Home is Lifespring（家庭は生命の源泉）を計画の基本的思想としてセキュア・ホームシステムをデザインした。

(1) 計画の基本

本計画を推進するにあたっては，次の事項を重視して具体化をはかることとした。

① 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

② 5大テーマ

・安全性指向：安心して生活できる

・健全性指向：健康な生活できる

・快適性指向：住みごごちがいい

・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) ライフステージの設定

本計画では，3つのライフステージを設定し，それぞれ前述の基本的考え方を踏襲するとともに，個々のライフステージの特色を次のように定めた。

① シングルライフ

機能性，オフィス性を協調し，家庭に情報センター機能を持ち込む。

② ファミリーライフ

コミュニケーション，くつろぎを協調し，家庭に大自然を呼び込む。

③ シルバーライフ

温り，生きがいを強調し，日本的な隣組みの良い点を情報化で復活させる。

4. 実現のために基本的条件

本計画の実現をはかるための条件は，詳細計画にまで堀り下げた時点で基本的に出てくる。

現段階においては，基本的な事項として次のような条件をあげることができる。

(1) パイロット・スタディの必要性

家庭の情報化が，何の制約もないままこれ以上進展する前に，特定地区にて国民的視野からモデル・システムを試験的に実施にうつし，安全性の面か

ら問題点がないことを確認する必要がある。そして，パイロット・スタディの成功により，システムの標準化とコスト・ダウンがはかれる。

(2) 資金面における援助

本計画を実施にうつす場合，多額の資金が必要になる。この点に関しては，商業ベースで実施できるようになるまでの間，補助金による援助が求められる。

(3) 諸制度の見直し

本計画を詳細に堀り下げていく場合，現行の諸制度による制約が出てくるものと思われる。これに対しては，官民一体となって，大所高所より調整をはかる必要がある。

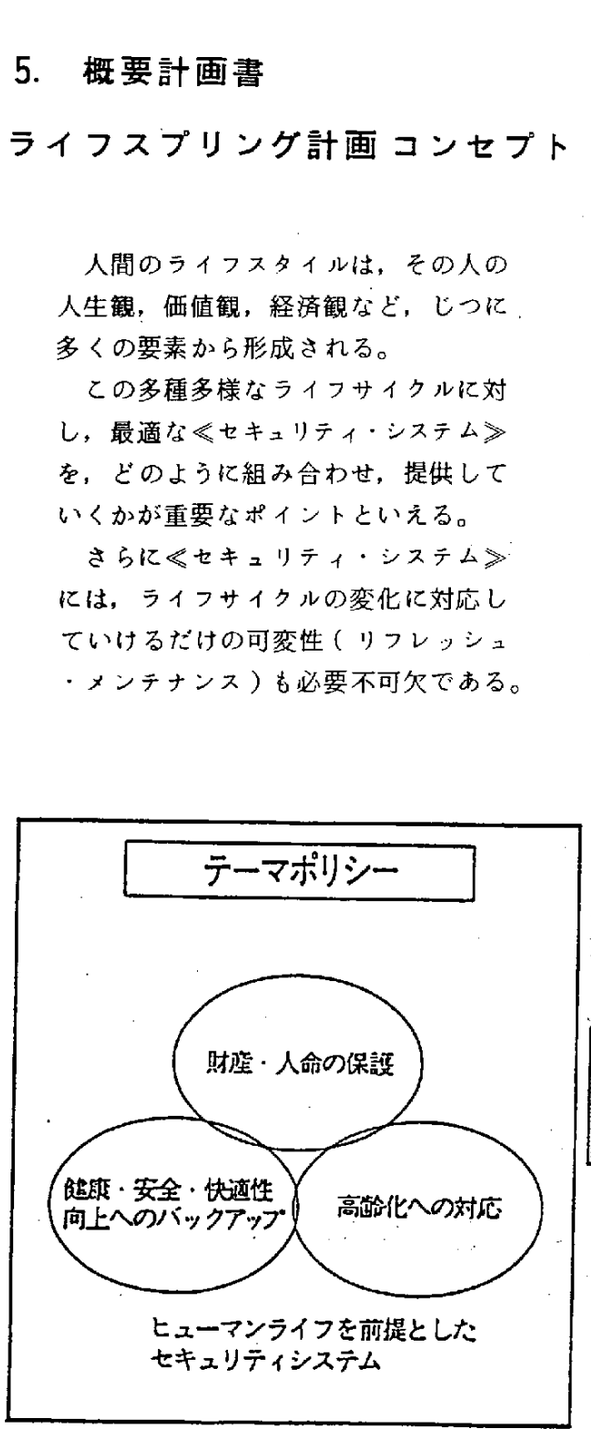
5. 概要計画書

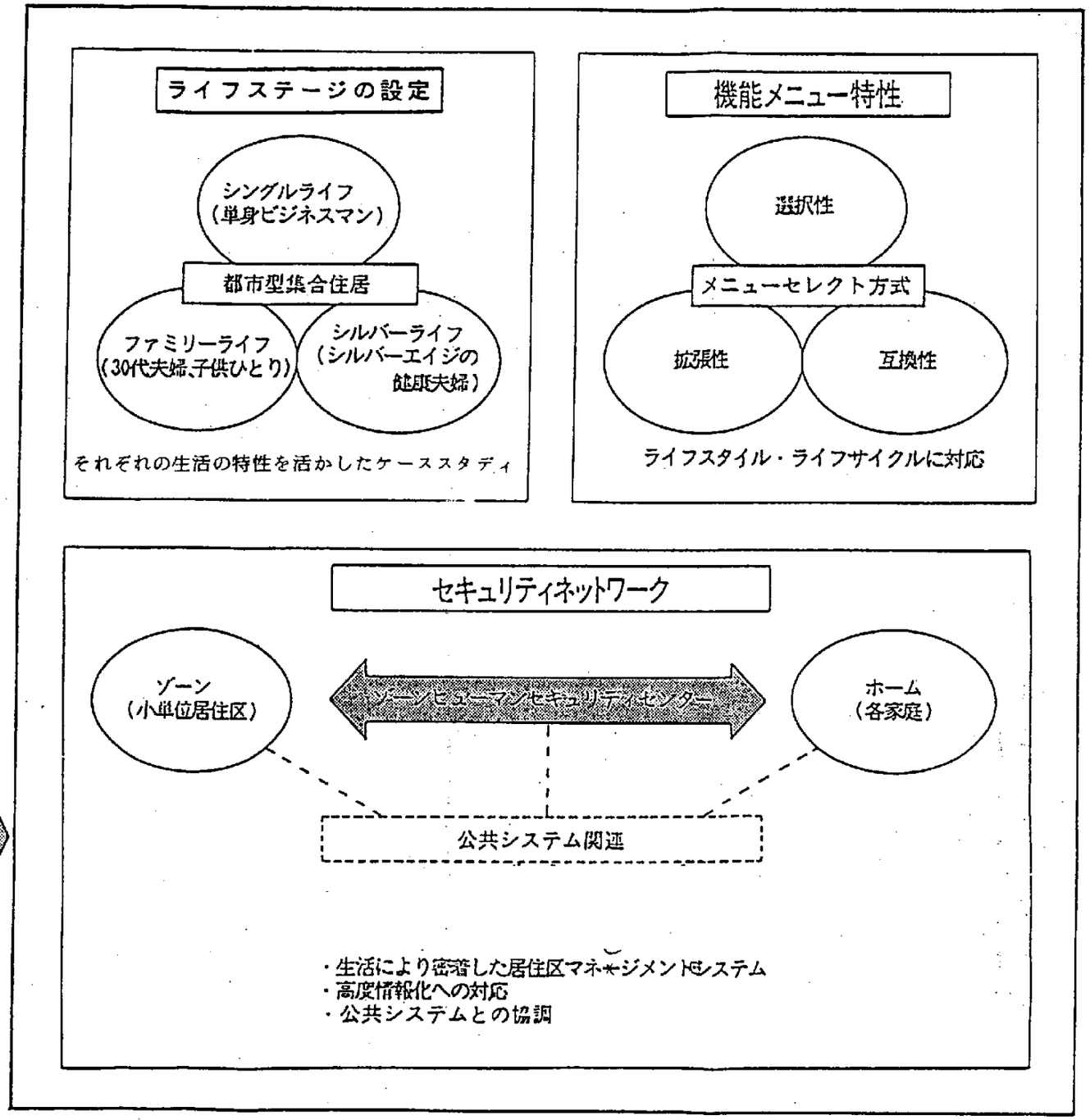
ライフスプリング計画 コンセプト

人間のライフスタイルは，その人の人生観，価値観，経済観など，じつに多くの要素から形成される。

この多種多様なライフサイクルに対し，最適な≪セキュリティ・システム≫を，どのように組み合わせ，提供していくかが重要なポイントといえる。

さらに≪セキュリティ・システム≫には，ライフサイクルの変化に対応していけるだけの可変性（リフレッシュ・メンテナンス）も必要不可欠である。





ライフスプリング計画システム概念図

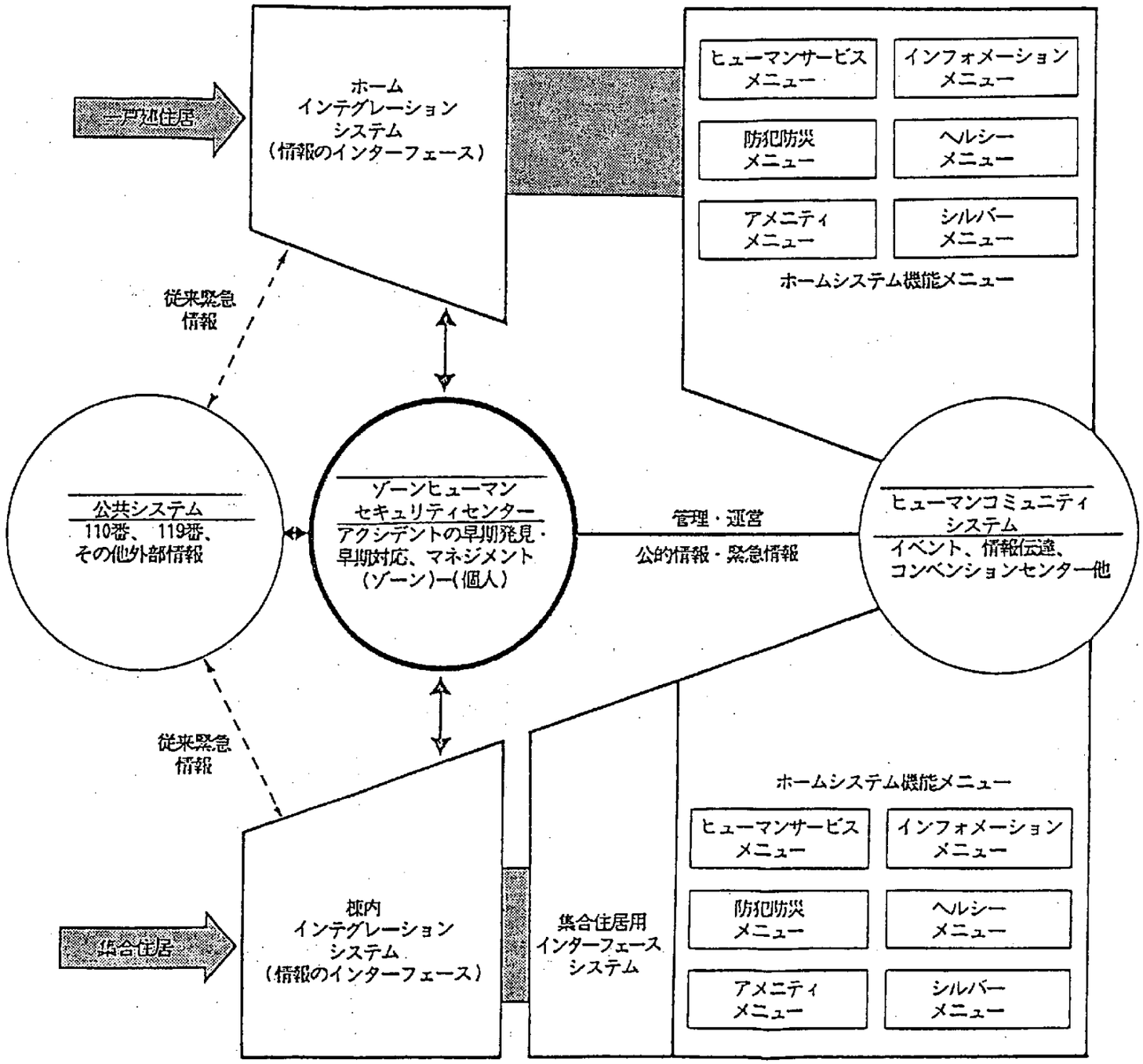
さまざまなニーズに対応できる，きめ細やかな≪セキュリティ・システム≫を提供するためには，居住区を小単位のゾーンに区分した管理システムが必要となる（ゾーン・ヒューマン・セキュリティ・センターの設置）。

そして，住民相互の関心が稀薄な時代にあって，ゾーン住民間のコミュニケーションを促進することが，地域生活の充実ばかりでなく，地域セキュリティの意識向上につながっていく（ヒューマン・コミュニティ・システムの設定）。

各家庭に対しては，後述の≪メニューセレクト方式≫による各種セキュリティ関連機能の選択採用により，最適な≪セキュリティ・システム≫を提供する。

また，110番（警察庁），119番（消防庁）など，公共システムとの情報協調を十分に図り，より安全性の高い，豊かなシステムを創造する。

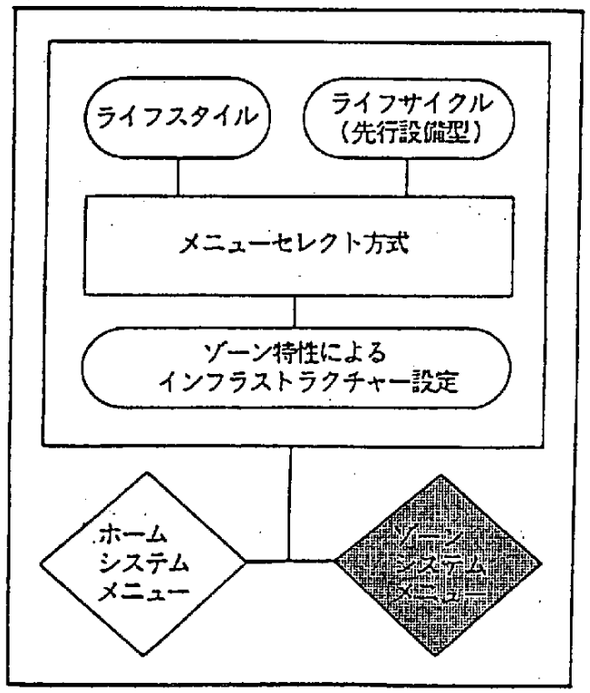
なお，ゾーン・ヒューマン・セキュリティ・センターを中心としたセキュリティ・ネットワークは，セキュリティ分野のクローズド・システムではなく，高度情報化の各種ネットワークにも対応可能なオープン・システムを採用する。



ライフスプリング計画機能メニュー

将来の変化に対して発展的に対応できる拡張性と，各企業間や対公共システムとの互換性にも優れた機能メニューを用意している。

ラインアップした各種機能アイテムは，居住者の自由な意志と，居住ゾーンの特性という２つの側面から選択可能である。これにより，最適な≪セキュリティ・システム≫が実現される。



ヒューマンサービス・メニュー

◇理容・美容巡回サービス・システム —— 定期的巡回による家庭での理容・美容サービス
◇インテリアサービス・システム —— 毎月違った絵画や植木等が楽しめるインテリアコーディネート・サービス
◇集中監視システム —— 緊急時にバックアップ体制が発揮されるセキュリティ・システム
◆オープンスペースサプライ・システム —— ゆとりの持てるスペースを設け、情報提供やイベントをサポート
◆カウンセリングサービス・システム —— フェイス・ツー・フェイスの各種相談サービス

インフォメーション・メニュー

◆地域セキュリティ情報サービス・システム —— 病院の案内や予約、気象・交通情報等、各種情報の提供
◆プライバシー保護システム —— 家庭・個人のプライバシーを保護

防犯防災メニュー

◇集中監視システム —— 緊急時にバックアップ体制が発揮されるセキュリティ・システム
◇鍵なしドア管理システム —— 音声認識、指紋、カード等をＩＤとした鍵不要のドア管理
◇自然環境セキュリティ・システム —— 地震、風雨等の天災から家屋全体を保護
◆避難誘導システム —— 有事に避難地まで住民を無線によって誘導
◆スクランブル・システム —— 急病、誘拐、迷子等の発生において、発信者本人の居場所を認識
◆地域型防災システム —— 近隣火災等の情報サービスを付加した、市および町単位の防災管理
◆緊急警戒放送システム —— 地震、火災等の災害を、テレビ・ラジオ等に割り込ませ、警戒内容を放送
◆映像による監視システム —— ２４時間オンラインによる回線監視とともに、停電時には電源を供給

ヘルシー・メニュー

◇健康チェック・システム —— ライフセンサーにより、つねに各人の健康をチェック
◇衛生管理システム —— 健康を害するカビ、ダニ、ゴキブリ等に対する衛生保護

アメニティ・メニュー

◇◆生活環境セキュリティ・システム —— 放射能、電波等が生活に悪影響を及ぼさないための環境保護
◇ホーム機器キーピング・システム —— 家庭内の機器が自己判断により危険状態を検知し、警告
◆地域セキュリティ情報サービス・システム —— 病院の案内や予約、気象・交通情報等、各種情報の提供

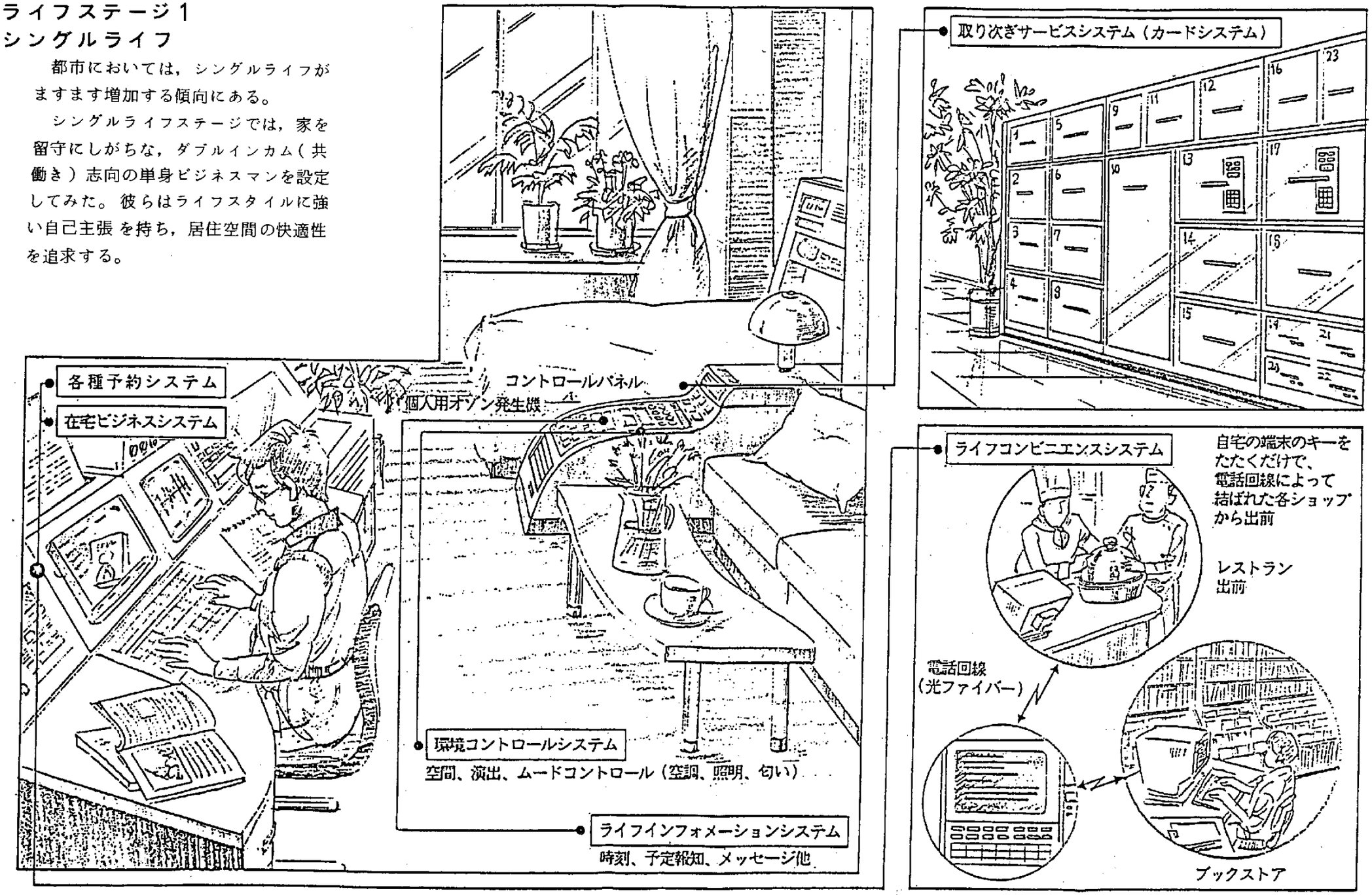
シルバー・メニュー

◇（老人）健康チェック・システム —— ライフセンサーにより、つねに老人の健康をチェック
◆スクランブル・システム —— 老人、急病等の発生において、発信者本人の居場所を認識

ライフスプリング計画
ライフステージ1
シングルライフ

都市においては，シングルライフがますます増加する傾向にある。

シングルライフステージでは，家を留守にしがちな，ダブルインカム（共働き）志向の単身ビジネスマンを設定してみた。彼らはライフスタイルに強い自己主張を持ち，居住空間の快適性を追求する。

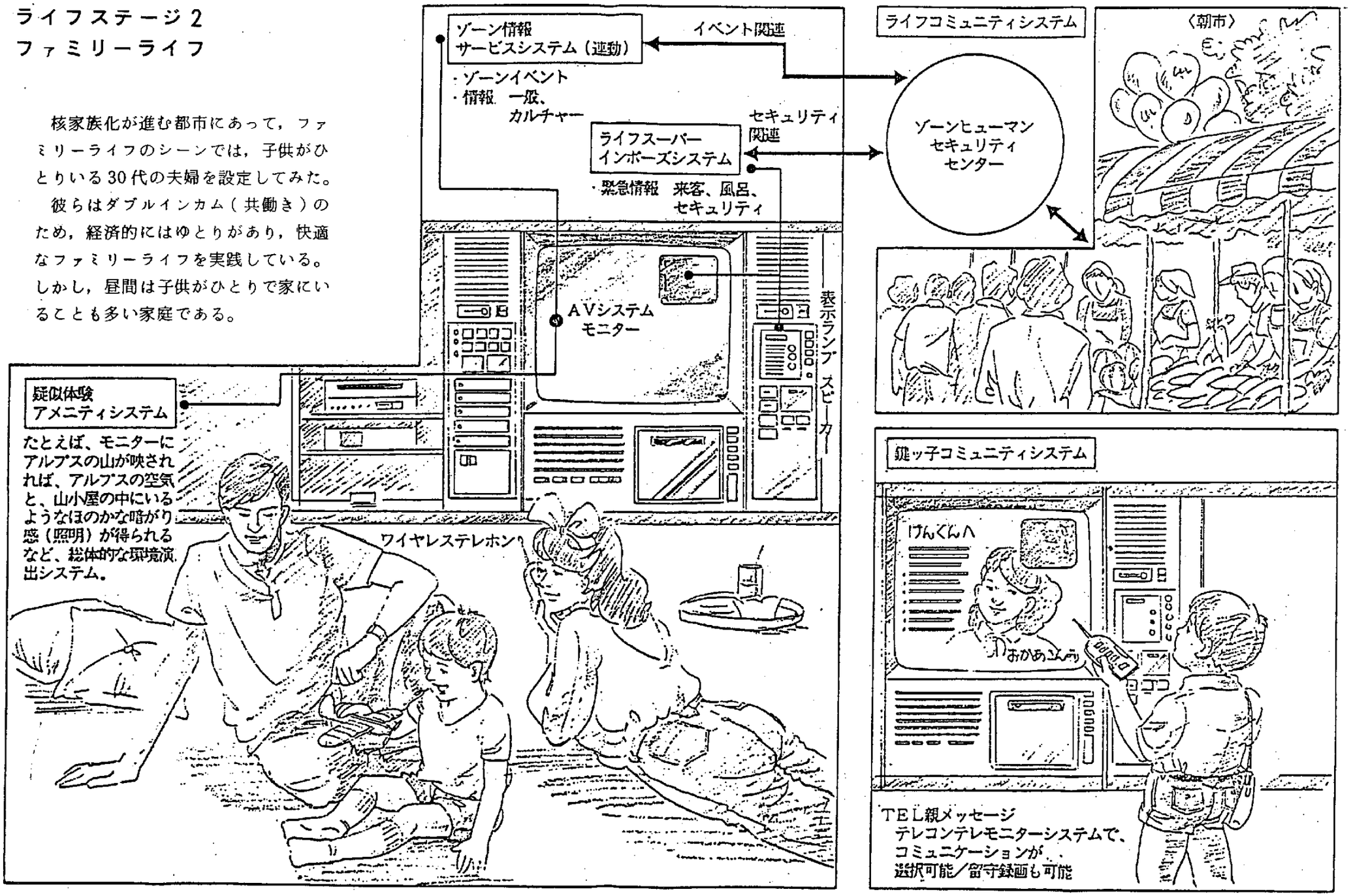


ライフスプリング計画

ライフステージ2
ファミリーライフ

核家族化が進む都市にあって，ファミリーライフのシーンでは，子供がひとりいる30代の夫婦を設定してみた。

彼らはダブルインカム（共働き）のため，経済的にはゆとりがあり，快適なファミリーライフを実践している。しかし，昼間は子供がひとりで家にいることも多い家庭である。



ライフスプリング計画

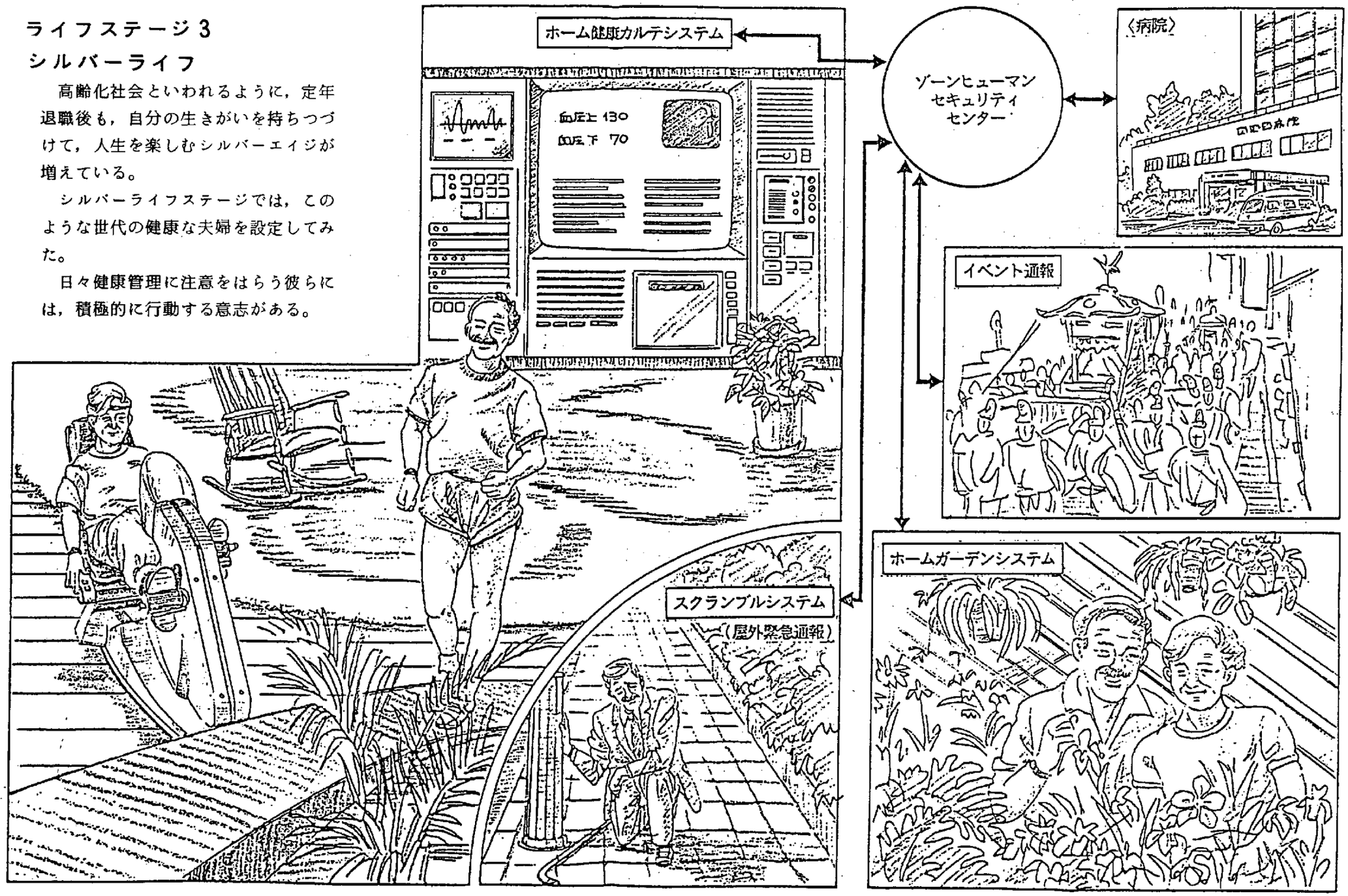
ライフステージ3

シルバーライフ

高齢化社会といわれるように，定年退職後も，自分の生きがいを持ちつづけて，人生を楽しむシルバーエイジが増えている。

シルバーライフステージでは，このような世代の健康な夫婦を設定してみた。

日々健康管理に注意をはらう彼らには，積極的に行動する意志がある。



付属資料

セキュリティ関連機器と基準等

機器類			基準等
防犯関連	出入管理装置（電子式，機械式等のキーシステム）	電磁波カード	
		磁気カード	
		ホログラムカード	
		テンキー	
		指　紋	
		掌　紋	
		アイマーク	
		インターフォン	
		モニターカメラ・テレビ	
	警報装置（接近，開閉，侵入破壊）	赤外線センサー	
		マグネットセンサー	
		振動センサー	
		超音波センサー	
		電磁波センサー	
防災関連	煙感知器		消防法施行令第21条 同施行規則第23条，第24条
	熱感知器		
	ハロゲン化物消火設備		消防法施行令第17条 同施行規則第20条
	炭酸ガス消火設備		消防法施行令第16条 同施行規則第19条
	温湿度検知器		
	温湿度記録計		JIS7305，JIS7306
	地震感知器		

機器類			基準等
防災関連	漏水検知器：	電極式	
		コード式	
	携帯電灯		JIS C8104
その他機器	鋼製事務用ロッカー		JIS S1035
	耐火庫		JIS S1037
	鋼製書架		JIS S1039
	鋼製物品たな		JIS S1040
	移動式鋼製たな ：	手動式	
		電動式	
	カセットテープ収納たな		
	安全帽		JIS T8131
	静電気帯電防止用安全・作業靴		JIS T8103
	フリーアクセス床 ：	耐震構造	
		免震構造	
	フリーアクセス床：パネル	ｱﾙﾐﾀﾞｲｷｬｽﾄ 系	
		木質系	
		セメント系	
		プラスチック系	
	無停電電源装置 ：	ＣＶＣＦ	電気用品取締法
		バッテリー	

昭和63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
機械振興会館内
TEL（432）9382（代表）

印刷所　三協印刷株式会社
東京都渋谷区渋谷3丁目11番11号
TEL（407）7316

62－R009