63—R 008

2010年の情報化社会とセキュリティ

「ライフスプリング計画II」：生活の情報化とセキュリティシステム

平成元年3月

財団法人　日本情報処理開発協会

この報告書は，日本自転車振興会から競輪収益の一部である機械工業振興資金の補助を受けて，昭和63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

わが国の各種情報システムは，ハードウェア，ソフトウェアの進展と社会的ニーズの拡大に伴い，急激な発展をし，より高度な情報化社会を築きつつある。

この情報化社会における各種情報システムが大規模・複雑化するに従って，そのシステムの機能停止等が社会に与える影響は，飛躍的に拡大する。このため，各種情報システムの安全性を確保するためのセキュリティ対策は，ますます重要性が増している。

本調査研究は昭和61年度から実施してきたが，本年度は，

第１に，急速に発展する情報化社会の現状をふまえつつ，国際化そして高齢化が進展する社会，グローバル化・ハイテク化する企業，多様な価値観とより快適性を追求する個人生活などの視点から，約20年後，すなわち2010年における高度情報化社会の状況を描写し，それを社会生活の安全性の確保と，より豊かな情報化社会のセキュリティ対策のあり方についての検討の前提とした。

第２に，昭和61年度の整理したセキュリティ産業の分類の中から，コンピュータ犯罪防止等のためのアクセスコントロール，インフラストラクチャとしての通信など主要な分野を抽出し，現状のセキュリティ対策と2010年代への課題について考察した。

第３に，昭和62年度に取り組んだ「ライフスプリング計画」（"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検討した。）を一歩前進させた。これは，基本的な考え方，仕組みなどについては前年度計画を踏襲するとともに，さらに2010年の情報化環境を想定して，人間の快適性と安全性を追求した生活のセキュリティという視点から「ライフスプリング計画Ⅱ」として展開を図ったものである。

本調査研究が，今後急激に発展するであろう情報化社会におけるセキュリティ産業の発展，およびより快適で健全な生活環境を維持するためのセキュリティ対策，セキュリティサービスのあり方などを考えるうえでの一助となれば幸である。

最後に，本調査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。

平成元年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㈱　代表取締役社長
委　員	植木　規男	シーアールシーテクニカル㈱　機器開発部長
	北村　亘	ビック情報機器㈱　代表取締役社長
	高坂　毅	㈶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㈱　産業技術渉外部長
	坂本　憲治	㈱熊平製作所　取締役企画部長
	柴田　正和	日本電気フィールドサービス㈱　施設部技術課長
	高尾　典生	㈱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㈱　大阪営業所長
	田中　正憲	富士通㈱　情報システム事業本部企画部標準推進部 部長付
	服部　直	清水建設㈱　情報システム部　副部長
	深井　寧	㈱電通　第９営業局営業部参事
	古川　弘	新日鉄情報通信システム㈱　関東支社 技術部　技術室長
	真島　凱氾	松下電工㈱　東京特機営業所長
	山本　英己	㈳情報サービス産業協会　調査企画部
	小林　登	㈶日本情報処理開発協会　常務理事

目　　次

第1章　総　　論

1. 研究の視点

セキュリティ産業の研究に最初に取り組んだのは昭和61年度であり，今年で3年目である。セキュリティ産業を研究テーマに選んだ理由は，昭和58年12月，産業構造審議会情報産業部会が提出した中間答申の中で，今後政府が講ずべき措置の1つとして，次のとおり「セキュリティ産業の振興」を提言しているためである。

「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う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・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。」

この提言を生かすためには，まず，セキュリティ産業の研究を進め，産業基盤を明確にして，社会的に認知される産業として確立をはかる必要がある。次に，セキュリティ産業の育成・振興をはかることにより，セキュリティ対策のための各種機器・装置・サービス等の創出を促進させることができる。その結果，社会各層におけるセキュリティ対策の選択の巾が広がり，最適化したより精度の高い対策が可能になる。

以上のような観点に立ち，セキュリティ産業の研究を進めており，これにより，終局的には，高度情報化社会の健全化に貢献することを目的としている。

2. セキュリティ産業の概念確立

昭和61年度は，初年度であることから，セキュリティ産業の概念を確立させることに目標を置いた。そして，1年間に及ぶ検討の結果，表1のとおり，セキュリティ産業の範囲を14分類に整理した。これで付言しておかなければならないことは次の2点である。第1は，この分類は情報システム関連に限定して，その中でできる限り範囲を広げたということ。したがって，防衛，原子力その他のセキュリティは含まれていない。第2は，現時点での分類としては妥当なものと評価できるが，将来に向けて，さらに，より良い分類へと展開できる機会があれば幸いと考えていることである。

また，61年度は，上記分類に従って，既存の各業種が，どのような分野に進出しているか，その進出形態（製造，販売，設計・施行，保守，サービス提供）はどのようになっているかをアンケート方式で調査した。この調査では，"今後5年間の成長が著しいと思われる分野"についての意識も調査しているが，その結果は次のとおりである。

- 1位　　通信回線分野
- 2位　　アクセスコントロール分野
- 3位　　監視分野
- 4位　　セキュリティソフトウェア分野
- 5位　　コンサルティング分野
- 6位　　防災・防犯分野
- 7位　　バックアップサービス分野

表1. セキュリティ産業の分類

	分　類	機器・装置・機能　（例示）
	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，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（　〃　）

機器・装置（含ソフトウェア）		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

3. セキュリティ産業の実態

昭和62年度は，前年度のセキュリティ産業の分類について，個別分野がそれぞれ独立して把握できるかどうか検証することを目標として研究を進めた。その結果，一部の分野で，セキュリティ用のみを切り離して把握することに困難が伴う部分があるが，おおむね把握可能であることがわかった。

62年度のもう１つの目標は，生活の情報化分野の急速な進展に伴うセキュリティ対策のあり方，および豊かな生活を営むための新しいセキュリティサービスのあり方などを，生活の情報化が本格化する前に検討し，情報化を進める上で発生する可能性のある弊害を未然に除去するための研究を進めた。このため，ライフスプリング計画を立案し，具体的な構想づくりに取り組んだ。

4. セキュリティ重視時代の到来

これまで述べてきた過去２年間の研究成果をふまえ，本年度はさらに一歩前進させるため，セキュリティが充実した社会を想定（約20年後の2010年を想定）し，そこにおけるセキュリティ意識の高まりとセキュリティ産業の意義・役割を検討することとした。また，ライフスプリング計画も，第２段階として，2010年のセキュリティが充実した社会におけるプランを模索してみた。将来を予測するにあたっては，現状を振り返り，基本に立ち戻ることも重視した。

4.1 情報の価値と位置づけ

われわれは，前提条件として，ここでもう一度初心に立ち帰り，情報について考え直してみる必要がある。

情報化の進展に伴って，セキュリティ対策の強化は，社会の基盤的条件となっている。もし，セキュリティ対策を否定したり，軽視する者がいるとすれば，彼らは情報化の担い手にはなりえない。

情報が，人・物・金に次ぐ，あるいはそれ以上の経営資源，生活資源となっている今日，情報に関連するセキュリティ対策が重視されることは，情報の重要性から考えて当然のことである。しかし，情報の大切さについては，情報化の進展でより重要に

なってきていることは間違いないが，その昔においても，情報が決定的要素をはたした出来事が多数あることをわれわれは歴史に学ぶべきである。

例えば，孫子の用間篇では，「間者によい地位や報酬を与えることを惜しんで，敵の情報を知ろうとしない者は，不仁の至である。指導者としてふさわしくない。」といっている。その理由は，間者たちが国王や将軍たちにとって大切な情報をもってくるからである。孫子は，一国の命運を賭ける情報にそれだけの価値を認めていたのである。

この場合の情報は，今日的な言葉でいえば，ナショナルセキュリティ（国防）に関する情報ということになるが，遠い昔において，情報を制する者が国を制したことを物語っている。ひるがえって，今日のわが国の情報化社会を考えてみると，情報を制す者がビジネスを制すという状況を呈しているのである。したがって，情報を保護するため，また情報を断絶させないために，セキュリティ対策がきわめて重要になっていることは当然の帰結である。

4.2　情報の保護

わが国で過去数年間に発生した情報の漏洩・破壊，情報伝達手段の破壊・盗用の実例から代表的なものを揚げると次のとおりである。

- 1984年，私立大阪工業大学中央研究所の磁気ディスクの中にあったプログラム数千件が消去されていた。
- 同年，電電公社世田谷電話局管内でケーブル火災が発生した。全面復旧まで約8日間を要し，大手銀行をはじめとして各個人にいたるまで，はかり知れないほどの被害を与えた。
- 翌1985年，筑波研究学園都市にある文部省の高エネルギー物理学研究所のコンピュータシステムに西独のハッカーが侵入した。
- 同年末から1986年初頭にかけてＫＤＤのビーナスＰ回線が何者かによって盗用されていた。

以上のうち，世田谷ケーブル火災事件を除き，事故の発見がいずれも事件発生後かなりの日数を経た後のことであったことにも注目しなければならない。

これらの漏洩や破壊から情報を護り，社会活動，経済活動に大きなダメージを与えないようにする手段が，セキュリティ対策である。従来の「護る」という語感からい

えば，鍵を掛けて大切にしまっておけばよさそうなものであるが，情報というものは本質的に無体物であるので，そこが物と異なり，管理上の問題が出てくる点である。

わが国では，昔から「符丁」という方法が考えられてきた。商品の仕入値という情報は，顧客に知られてはまずい。場合によっては，同業者にも知られたくない。そこで，数字を他の文字に置き換える。第三者が聞いても読んでも理解できない。置き換えの方法はもちろん秘密である。一子相伝の商家が今でもある。符丁も一種の暗号である。このように，わが国でもビジネス上の情報保護の歴史は，非常に古いのである。

会話からはじまり，狼煙，文字，手旗，電信，電話，ラジオ，テレビなど，通信の手段は長足の進歩を遂げた。また，情報処理の方法も同様に，ソロバンから始まってコンピュータに至るまで急速な進歩を遂げた。科学技術の進歩で，通信と情報処理手段とが結び付き，巨大な情報ネットワークを形成するに至った。

このようにして，セキュリティの概念は，単に符丁とか2点間情報伝達の暗号化などという範囲を超え，近代社会のインフラストラクチャであるコンピュータを含む巨大な情報ネットワークを，天災・人災から防御する手段となった。その技術は複雑かつ多岐化し，その守備範囲はますます広くなっている。

4.3 ネットワークのセキュリティ機能

大切なものを守るために金庫があるように，ネットワークを流れる情報にも安全性確保の仕組みが必要である。すなわち，伝送する情報に対して，保全性(Integrity)，機密性(Confidentiality)，可用性(Availavility)の3つを確保することが重要である。

保全性とは，情報に対し，その内容に変更がないことを保証する仕組みのことである。例えば，銀行の窓口にある現金自動支払機は，客へ現金を支払うが，それに相当する情報センターへ送り，センターの元帳が更新される。このようにネットワーク上を流れる情報は現金に相当し，ホームバンキングやファームバンキングなどにより，著しく増加すると予想される。このような情報は，途中で紛失することも，また，人為的な改ざんを受けることも絶対に許されない。逆に，そのようなことのないような仕掛けがその普及の鍵を握っている。デジタル署名，メッセージ認証等は，保全性確保等のための技術である。

最近話題になっているコンピュータウィルスは，プログラムに対する保全性の弱い

パソコンなどで発生し始めている現象でもある。2010年から，現在を振り返ると，コンピュータウィルスはネットワークも含めた情報システムの安全性の重要性を再認識させた出来事であったと，セキュリティの歴史では言われることになるであろう。

機密性とは，権限のない者に情報が漏れても，内容を解読不可能にする仕掛けのことである。さまざまな情報が電子化されてくると，単に第三者に漏れても判らなくするだけでなく，解読できる人をきめ細かく指定できる機能が要求されてくる。いわゆる情報に対するアクセス制御である。このような機密性確保の仕組みは，情報センター内でのデータやプログラムに要求されるのは当然として，ネットワークでも必要となる。伝送情報の暗号化はその代表例であり，それ以外でも，通信事業者が課金のために収集する情報などは，利用者のプライバシー保護という意味でアクセス制御が要請される。

可用性とは，自然災害，機器の故障，破壊行為等，ネットワークの稼動を妨げる要因に対し，稼動率の向上を目指すものである。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等，独立した事業者の提供するサービスの他，通信サービス提供者によるネットワークのメッシュ化（迂回ルートの確保），ユーザによる回線の二重化や通信衛星の利用等，さまざまな対策が取られなければならない。

4.4　高度化・専門化の必要性

日本人は，安全と水はタダと思い込んでいるとよくいわれる。しかし，実際には，安全にはコストがかかるのである。

情報の重要性とその処理技術の進歩とは，相互に刺激する要因となった。その結果は，前述の巨大な情報ネットワークの出現である。これを構築する要素は，単にハードウェアだけではなく，ソフトウェアも重要な部分となり，運営主体でもあり受益者でもある人間をも包含してしまう。まことに複雑多岐である。

したがって，その安全対策も，設備，セキュアＯＳ，運用管理手順，人事管理，教育訓練，システム監査等の広範囲にわたる考慮が必要となってきた。そして，それぞれがさらに細分化され高度化されつつある。

ここに，新しいセキュリティ機器・装置・サービス等が求められる要素があり，より専門的な知識・技術が必要とされる時代になってきていることがわかる。そして，まさに安全にもコストがかかるという意識が出てきた。

このような状況の中で，早急にセキュリティ産業を確立させ，各分野，各層において十分なセキュリティ対策が実施できるようサポートしなくては，これからの高度情報化社会はその存立基盤が危うくなるであろう。

第２章　2010年の情報化社会

1.　21世紀への流れ

現在，技術革新は日進月歩，いや，時進日歩の早さで進んでいる。社会の変革のスピードは現在より速くなることはあっても遅くなることはないであろう。このような時に20年先の情報化社会を想定することは簡単ではないが，大胆に想定してみよう。

現在から21世紀を展望した時に，いろいろな未来予測が行われているがここではキーワードとして，野村総研の村瀬光正氏の説*を参考とした。

1.1　ボーダレス化

(1)　経済活動のボーダレス化

現在，世界的な注目のもとに急激な円高が進んできており，輸出比率の高い大企業においては，製造工場はもちろん，本社機能についても，一部を海外に移転しつつある。これら大企業の動向のもと中小企業についても生産拠点を海外に移転しようとしている。このような海外進出企業は，現地の人を採用し，数少ない日本人をもって運営している。21世紀においては，現地人の管理者による経営がなされているであろう。

一方，貿易摩擦の緩和を図るため，輸入制限の縮小や外国企業の日本進出に対する制限の縮小等が行われ，モノの市場開放とともにサービス貿易の自由化も進展し，情報の国際流通と共に，外国企業が日本に進出しつつある。今後，食管制度の改革，流通機構の改革等により，ますます外国企業の日本進出や外資との合弁企業の設立が激しくなるであろう。

このように日本企業と外国企業の相互進出・提携などに伴い，経済のボーダレス（ボーダレスエコノミー），すなわち，人，物，カネ，情報に国境という意識がなくなってくるであろう。

(2)　業界垣根の消滅

各企業においては，効率的経営のためのニュービジネスの模索や組織の見直しが盛んに実施され，子会社を設立して本来業種以外の業界に進出する等，多角的経営

戦略を展開している。また，社会の進展に伴い，今までの業界以外の産業（すきま産業）が新たに出現しつつある。

今後，ますますこのような状況が進展し，各業界の領域がなくなるものと考えられる。

(3) 24時間化

すでに為替・証券においては，ロンドンーニューヨークー東京の三極を中核とした24時間化が世界的に進んでいるが，物流等その他の分野においても，ますます24時間化が進展するものと考える。生活においても，夜間勤務の増加等により，コンビニエンスストアはじめ，夜間営業店が増加するなど，その兆しは十分見えており，今後24時間化は一層進むものと考えられる。

1.2 ゼロベース化

(1) 在庫レス化

現在のコンビニエンスストアの販売管理システムや，ＰＯＳシステムにみられるように，死に筋商品の排除とジャストインタイム化による在庫圧縮化が各種産業においても進展しつつある。納期管理はこの数年きわめてシビアになってきており，徹底的なコスト削減を目的として大企業は，資材調達を製造ラインと結びつけてトータルな生産管理システムを構築している。この典型的な一例がトヨタ自動車のカンバン方式である。このように，在庫を減少させてコストダウンをはかるばかりでなく，従来倉庫であった場所を活用するなど，在庫レス施策がさらに新しい戦略へと進展しつつある。

(2) 無　人　化

すでに，企業の工場においてはＦＡの導入により，自動生産管理のシステムが進み，また，事務部門においてもＯＡ化が図られるなど，人員を削減し，効率的経営が図られつつある。今や世界最高水準になった日本の賃金レベルを考えた時，今後，ＡＩの発展，リストラクチャリングによる業務・事務の見直しなどで，できるだけ人間のゼロベース化を図り，人件費を抑え，効率的経営を図るであろうと思われる。

(3) リスクゼロ化

現在，金融機関において最も必要性が叫ばれているが，経営上のリスク回避が将来展望の困難な時代において重要である。また，企業経営において，情報システム

への依存度はますます高くなる。一部企業においては，このような情報システムの停止に伴うリスクを未然に防止したり，リスクの減少を図るため，システム監査を導入しているところもあるが，わが国においては，歴史的風土ともいうべきか，災害に対する姿勢は淡白であり，現在の利便追求を重視し，リスクの未然防止・分散等の考え方は消極的である。何か事故があって初めて，その影響の大きさを知り，あわてて対処するのが現状である。しかしながら，今後，情報システムが発展し，より大規模となるに伴い，情報システムの停止等における社会的影響，損失の増大が認識され，企業としても，社会としてもリスクの未然防止，事故があった場合のリスク分散・緩和を図るなど，リスクゼロ化の研究が進むことになるだろう。

今後，情報システムが大規模となるに従い，1回の事故が致命傷となり，企業が倒産するケースもあり得るであろう。

1.3 ネットワーク化

(1) 情報ネットワークの複雑・高度化

コンピュータシステムは，事業部門別の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，使い込まれていきながら，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た。現在においては，さらに進んで企業間・異業種間の水平型の共同利用システムがネットワークにより形成されつつある。このようなネットワークは，金融，保険，流通，物流など多くの分野で発生し，また巨大化している。

今後，ネットワークは，各業界内にとどまらず，業界をまたがってますます巨大化・高度化するであろう。また，日本国内のみでなく，世界的な巨大なネットワークが形成されるものと思われる。

(2) 組織構造の変化

企業における組織構造は，今までピラミッド型が主体であったが，今後は，必要な情報の多様化，迅速な意思決定，多角的経営，効率的な組織運用等の観点から，フラットでダイナミックな組織構造とする必要性がでてきた。すでに一部企業においては，事業部制を実施し，各事業部の責任・権限を強化し，企業内における事業部の独立採算性を実施するところも多い。

これからの企業組織を展望すると，構造の変化はネットワーク型になると思われる。

2. 2010年の情報化社会の状況

2010年の情報化社会について，全般的に網羅はできないが，独断的，偏見的にいくつかの角度から考察してみたいと思う。

社会の状況は，企業の内外相互進出・連携に伴い国際化が進み，都市化現象もさらに拡大するが，高齢化，情報化，ソフト化，24時間化，労働時間の短縮，女性の社会進出など生活環境を大きく変更させる要因も並行して急速に拡大する。このような状況から，社会生活としては個々の価値観によるライフスタイルが主張されて快適性を追求するとともに，安全指向・健康指向の人達が多数を占めるであろう。

また，現在の日本の社会でインフラストラクチャといえば，水道，電気，ガス，交通，電話等をいうが，2010年においては，これらについても，より付加価値の高いものや，情報化の進展に伴う新たな設備・サービス（例：ISDN，衛星通信）がインフラストラクチャとして定着するであろう。

企業においては，制度その他の環境から本社機能を海外移転させる等による無国籍企業(?)の出現も考えられ，情報機能はますます重要性を増してこよう。また高齢化の進展に伴って高度な自動化が図られ，人間の行う事は，経営戦略，企画，サービス等，真に人間でなければならないことが主体となろう。大企業はもちろん，中小企業においても，企業生き残りのため戦略的経営をするために，条件分析やシミュレーションをコンピュータシステムより実行し，経営判断を行わざるを得ない状況となっているであろう。

また，例えば知識・経験豊富な高齢者や，有能な女性は特種能力の保持者として企業に求められ，自由契約またはパート的な活用による，より効率的な経営施策が当たり前になっているであろう。

個人においては，急激な国際化とソフト化に伴い，勤労者は非定型勤務・海外勤務・転職が日常茶飯事となり，ストレス発散の場や趣味の多様化によるレジャー指向が強くなるとともに，安全，健康，快適，利便，自由な生活を目指すであろう。また，各地域に情報を中心としたコミュニティ活動がより活発化すると思われる。

ところで，人間が生きていく時に，「他の人と同じでありたい」と思う願望がある。過去の例をみても，テレビ・電子レンジ・自家用車・ファミコン等の急激な普及にあるとおり，家計の許すかぎり（多少無理をしてでも），新しいシーズが進むかぎり，個人

はどんどん取り入れるであろう。反面，「人とは違った人間でありたい」，すなわち，人よりも一歩抜きんでた知識・能力・趣味・物品等を保有したいという願望がある。例えば他人の自動車とは一味違う自動車の保有願望等である。今後，この「同じでありたい」と「一味違う」矛盾した欲求は，情報化面においては特に顕著に現れると考えられる。2010年においては，保有するメディア（機器），情報，アクセス特権（利用権）などにこのような傾向がますます強くなるであろう。言い換えると，地域を越えて趣味や関心を共有する結合が情報・通信を経済に活用して多く誕生していると思われる。

以下に社会環境の変化として現在すでにその兆しもあり，すでに足を踏み入れていると思われるものを挙げ，２～３将来のあるべき視点や情報化の方向を考えてみたい。

2.1 高 齢 化

老人夫婦世帯，老人単身世帯の増加により，高齢者のみの旅行やサークル活動の活発化，健康意識の高まりがある。また，寝たきり老人の増加等があり，情報システムとしては，老人向けのセキュリティシステム，災害に対する緊急避難システム，健康チェック・健康管理システム等が普及しつつある。

しかし，今後の高齢者福祉の方向は豊富な知識・経験を活用し，社会に役立っているという意識（老人の存在感）をより強く持たせ，老若男女の融和（断絶のない世代）を図ることが重要である。

2.2 国 際 化

知識人や労働力の雇用で外国人の国内滞在人口が増大し，企業の中においても日本人，外国人の区別がなくなる。また，海外生活の一般化，海外旅行の日常化など行動の様式の国際化が進み，犯罪の国際化も顕著となる。

このような状況の中で，金融・流通等をはじめとする多くの情報システムは24時間利用が定着しているであろう。また，大企業のグローバルな情報・通信ネットワークがハイパフォーマンス型に構築されており，通信ノードにはコンピュータ翻訳機能等が導入され，かなり自由に異言語通信に利用できるであろう。日本人が他に誇れる文化・風土を残し，高めつつ国際社会に融和・貢献していく形で情報化を高めていくことが必要であろう。

2.3 ハイテク化

現在芽が出始めた，通信分野におけるISDN，およびコンピュータ分野におけるAI，ファジー・ニューロコンピュータ，これらは2010年には，十分実用化されているであろう。

また，バイオ・素材の技術進歩によって，社会の様相は非常に変革されているであろう。超電導については，装置の中，企業構内，家庭内等の狭い地域に活用されているだろう。しかしながら，離れた地点間で電気エネルギーを通す電力線は2010年では一部分しか活用されていないものと考える。

宇宙においては，新素材の研究開発・製造（特種材料の無重力製造工場）が実施されているものと思うが，一般人の宇宙観光旅行についてはまだ時期尚早かと思われる。

衛星通信の利用は量，質ともに現在に比べると飛躍的に発展しているであろう。衛生通信利用上の制約は現在では静止衛星の赤道上の個数にあるが，2010年にはダイナミックな追跡制御システム技術により移動衛星利用が可能となっているとみたい。

2.4. 価値観の多様化

社会が，高齢化，国際化，ハイテク化するに従い，技術者はますます専門・分業化されることなどをはじめ，政治家，実業家，技術者，学者，芸術家，スポーツマン，老若男女など，それぞれの立場において現在以上に個人能力が尊重される一方，趣味，感性，信条など個人の好みや主張はますます強まり，価値観が多様化するものと考える。

今後，次の事項については，激変要素となろう。

(1) レジャー化

休暇の長期化，バカンス時期における休暇の一斉化，週休2日制または3日制の定着，労働時間の短縮等による自由時間等の増大などにより，別荘，リゾート需要の増大と共に，ストレスの解消のためのレジャーが多様化しているであろう。これは，旅行，スポーツ等のように外に出るものだけでなく，今後は居ながらの知的レジャーのウエイトも高くなるものと考える。たとえば，通信系を取り込んだ在宅囲碁，在宅競技等である。

このようなことから，在宅レジャー支援システム（情報の提供，参加権の取得・決済，ゲームの提供）等，新たなニーズに基づくシステムが数多く出現しているも

のと考える。

(2) 女性の社会進出

思考力のある有能な女性の就業意欲および女性の感性を引き出す目的での企業側の要請から，多くの女性が社会に進出しているであろう。その結果，シングルライフの増加，昼間留守宅の増加，託児施設の増加，鍵っ子の増加，女性の深夜活動の増加，主婦による在宅知的作業の増加，このため女性の地位が向上するとともに収入も増大しているであろう。

このような状況から，無店舗販売・決済システム，キャッシュレスシステム，時間指定宅配システム等が定着しているものと思われる。

(3) ライフスタイルの変化

「生きるために働く」から「楽しむために働く」人の比率が増大し，土地価格の高騰，週休二日／三日制の発達，非拘束勤務者の増加などと相まって，住居のあり方も都会では固定型から移動・転居自在型に変化すると思われる。また，セカンドハウスが都会（オフィスの近く）にあり，本居を自然に近いところに構える企業家・勤労者も相当増えると考えられる。

また，大学等の地方分散化も進んで若者の街は都心から郊外へと場所を変えるであろう。そして若者のライフスタイルや興味の焦点も変わっているであろう。

これら，高齢化，国際化，ハイテク化，価値観の多様化が相互に関連しながら進化し，高度情報社会が築かれていくものと思われる。

3. 豊かな情報化のために

前述のように，ハイテク化が進む中で，それぞれの製品・サービス等が，空気・水のようになっていく時，その製品・サービス等が故障・中断した場合，対象物はブラックボックスであり，その対処（生活を含む）をいかにすればよいかわからなくなるであろう。

ハイテクにうずもれたような生活では，常に，それが使用できなくなった場合を考えておくことが肝要であり，また，そのような事態が起こらないように，事前のアセスメントやセキュリティ対策が重要であることが認識できるであろう。

一例をあげるならば，昔は電気が切れた場合，照明の代替として，臘燭やランプがあ

ればよかったが，現在においては，電気の停止により，照明はおろか，風呂や調理・暖房器具も使用できない状態であり，多くの器具，システム等が電気に依存する環境となり，生活に多大な支障をきたすであろう。このような事態の未然防止対策は，十分意識されておらず，部分的にしか実施されていない状態である。トータル的な未然防止対策は，今後積極的に研究を要する分野であり，その研究成果を実現するとともに，成果の累積により早急に欠陥を是正する必要がある。

3.1 情報断絶の回避

「世田谷通信ケーブル火災事故」の例を見ても，トータルなセキュリティ対策の必要性については，十分理解できるであろう。事前にセキュリティ対策がたてられていたならば，あのような大きな混乱とはならなかったであろう。確かに対策に要するコストは大であり，事故は起こるか起こらないか分からない以上，誰がそのコストを負担するかなどは大変難しい課題ではあるが，事故があった場合の社会的影響，経済的損失等を考えると安いものであろう。

金融の分野では，銀行間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あり，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，物流などあらゆる分野において存在する。

このような時，例えば，地震，火災，犯罪，事故などの要因で，システムが停止すると，日本の経済秩序に大きなダメージを与え，パニックに発展する可能性さえある。情報システムの規模が大きくなるに従い，社会に与える影響が大となる。

オルタナティブを用意したセキュリティ対策は，コストがかかるが，個人・企業・社会が支払う必要がある「費用」であることを認識しなければならない。

3.2 コンピュータ犯罪の防止

近年，情報システムの発展に伴い，コンピュータ（データ）の不正操作，コンピュータ情報の不正入手・漏示，コンピュータ破壊（妨害），コンピュータの無権限使用などのコンピュータ犯罪が多発しつつある。情報システムが巨大なネットワークになるにつれて，そのコンピュータ犯罪の形態は多様化しつつある。

このようなコンピュータ犯罪の社会に与える影響や，損害金額は，今後飛躍的に増

大していく可能性がある。そこで，そのようなコンピュータ犯罪の未然防止，損害を最小限にするためのセキュリティ対策が重要となってきた。具体的には，アクセス権，ファシリティマネジメント，通信回線等の対策であろう。このような対策は，知恵較べ的な要素はあるがシステム監査の導入等により，不備事項を是正し，改善をはかり続けることにより安心して利用できる情報システムとする必要がある。

3.3　人間性疎外の克服

現在，コンピュータ化の恩恵は，その迅速性，合理性によって経済・社会活動のすべてに及んでいるが，人間が人間として人間らしく生きるとの観点からは好ましくない弊害が出ているものも多々ある。その一例に，受験のための偏差値問題がある。これは人間の生き方を小さくしているものの１つであろう。コンピュータの計算した点数に左右され，一握りの優秀者を除き親も子も，自分の進む道をあきらめの中に見出すしかない状態に陥っている。真の勉強とは，より高い望みをもって人格を高めるためにトライすることと考えるが，今の若者はその意欲をもつことを阻害されている，といっても過言ではない。これはまさにコンピュータの進歩が生んだ社会現象であり，今後，国民的コンセンサスを得て，システム化しないとか，出力等を公表しない等のアセスメントがあってもよいと考える。

現代の豊かさは，刹那主義的（外見上，表面上の豊かさ）である。真の豊かさは，健全な社会であり，そこには夢があり，心なごむ，安心した生活があるべきである。

個人，企業からみて決して破滅に至らない安心できる社会が期待される。

3.4　トータルセキュリティ対策

今後，情報化が高度化するに従い社会に与える影響はますます大きなものとなる。そのために，常にどのようなリスクがあり，その対策をいかにするかという研究をしておかなければならない。

人間が安心した生活を営むためには，部分的なセキュリティ対策はもちろんであるが，トータル的なセキュリティ対策を確立する必要がある。セキュリティ対策には相当大きな経費がかかることから，また，犯罪の予防措置として，法律的手当，金銭的手当等の施策が国に期待される。

このような対策は，高度情報化社会において，避けて通れない人間の責務であろう。

わが国は，他国と比べて狭い土地，多い人口，少ない産出資源等の特性を持っており，より付加価値の高い情報化社会を築き，経済大国として国際的にも誇れる社会を造成し，世界に範たる国となるように，国・企業・個人がそれぞれの立場において，成すべき責務を果たすべき時代であろう。

そして，輝かしい豊かな情報化社会が出現する。

参 考 文 献

*『週間東洋経済』昭和63年12月24日号，東洋経済新報社

4. 2010年の情報化社会のイメージ調査

この表は，2010年の情報化社会を描写する仮定で各委員に対して，2010年の社会・企業・個人の切り口で社会の状況・情報システムがどのようになっているかにつきイメージを調査し，その結果をとりまとめたものである。

付表1. 社 会

項 目	社 会 の 状 況	情 報 シ ス テ ム
高 齢 化	1.会員制老人クラブの増加 2.高齢者の旅行・サークル活動の活発化 3.医療および医療相談の多発 4.疾病者の看護 5.ケア付老人ホームの増加	1.医療相談システム 2.疾病者監視(看護)システム *3. 統合監視通報システム(防犯・防災) *4. 広域セキュリティシステム *5. ヒューマンスクランブルシステム
国 際 化	1.衛星放送・通信システムの拡充 2.在日外国人の増加 3.1ドル＝100円時代の到来 4.犯罪の国際化	1.金融グローバルネットワークシステム 2.コンピュータ翻訳システム
レジャー化	1.3V時代の到来 海外旅行（VISA） 別荘生活（VILLA） 交際訪問（VISIT） 2.趣味の多様化による新しいレジャーの出現 3.完全週休2日制(3日制？)の定着	1.趣味の分野別データベースシステム 2.旅行情報案内システム 3.レジャー情報案内システム *4. グリーンアメニティシステム 5.レジャー施設総合管理システム

項　目	社　会　の　状　況	情　報　シ　ス　テ　ム
女　性　の 社会進出	1. 独身者の増加 2. 育児・教育サービスの普及 （家事代行サービス） 3. 情報通信ビジネスへの主導権は女性へ	1. 無店舗販売・決済システム 2. 時間指定宅配システム *3. 統合監視通報システム（防犯・防災）
キャッシュレス化	1. プリペイドカードの範囲増大 電話，鉄道，飲料，ハイウェイ，タクシー，タバコ，ビル・商店街，チェーンストア，レジャー施設 2. 信用取引の拡大 3. カード社会（プラスチックマネー）	1. 24時間キャッシュレスシステム 2. 個人支払状況チェックシステム 3. 個人識別システム 4. 信用供与管理保険システム *5. コンフェレンスシステム
コミュニティ化	1. 地域情報システムの個人への拡がり 2. 知的スポーツとしてのネットワーク利用 3. 情報交換，提供の拡大 4. CATVの普及 5. カルチャーセンター増加	1. コミュニティ情報案内システム 2. 生涯教育，グローバル教育システム 3. コミュニティセキュリティシステム
その他 合目的化 適正化 多様化	1. 政治 (1) 在宅選挙 (2) 聴聞会，アンケートの通信，コンピュータ利用 (3) 一部土地の公有化 2. 学校 (1) 週5日制 (2) 平日学校と土・日のみ学校の出現（専修学校） (3) 自宅学習の導入 3. インフラストラクチャ (1) 首都圏100㎞はリニアモーターカー (2) コミューター（ヘリコプタを含む）の発達 4. 病気・健康・悩み等 (1) 遠隔診断の体系化 (2) 医・薬の分離 (3) リッチ ― プア 格差拡大	1. 在宅選挙システム 2. 在宅学習システム 3. 交通情報案内システム 4. 新交通管理システム 5. オンライン診断システム *6. カウンセリングサービスシステム *7. 生活環境セキュリティシステム

付表 2. 企　業

項　目	社　会　の　状　況	情　報　シ　ス　テ　ム
高　齢　化	1. 従業員の高齢化 (1) 健康弱者への施設的配慮 (2) 健康状態の監視 (3) 労働時間の短縮 (4) フレックスタイム化 (5) 在宅勤務化 (6) 選択定年制 2. 高齢者の雇用は，嘱託，アルバイト 3. 資本集約・知識集約業務の拡大 4. 家庭から職場までの一貫したトラッキングシステムなども可能となる 5. 簡易に使用できるＯＡ機器の普及 6. シルバー産業の増加	1. 在宅勤務サテライトオフィスシステム 2. 社員管理システム 3. 社内情報伝達・蓄積システム 4. 高度オフィス環境維持システム
国　際　化	1. 国際競争力の変化に対応して企業の海外進出が活発となる 2. 外国人雇用の増大（知識人・労働力） 3. 海外勤務者率大幅増 4. 海外事業所との遠隔会議 5. 国際分業化進展，物流，情報の拡大 6. 通信システム，コンピュータシステム，オフィスの24時間利用 7. 他国語間，非同期および24時間コミュニケーションが重要となる 8. 世界的に貿易摩擦が激化 9. 従業員の多国籍化と複数言語の日常的使用	1. 国際ＶＡＮシステム 2. グローバルネットワークによる経営管理システム 3. 自動翻訳システム 4. 遠隔会議システム 5. 高速コミュニケーションシステム（大量のデータ伝送を可能にする） 6. 24H対応ビル入退管理システム
レジャー化	1. 自由時間の増大 (1) 長期休暇制度の普及 (2) 週休２日制・３日制の普及 (3) フレックスタイム化 (4) サテライトオフィス，リゾートオフィス，在宅勤務の普及 (5) 労働時間の短縮	1. ＯＡ・ＦＡ高能率化システム 2. 社内エキスパート情報伝達・蓄積システム 3. リゾートセキュリティシステム

項　目	社　会　の　状　況	情　報　シ　ス　テ　ム
	2. 情報の共有化，蓄積情報活用の重視 3. 非同期および同報コミュニケーションの確保が従業員のモラール高揚上必須となる	
女　性　の 社会進出	1. 女性の進出により，時間的・場所的自由度の一層の拡大が求められ 例 1. フレックスタイム化，パート化 例 2. 直行直帰，サテライトオフィス 例 3. 在宅勤務 等が普及浸透する 2. 女性の職種は，営業・企画・研究開発分野と単純事務分野のように 2 極分化が起こる 3. 女性経営者，管理者の増加 4. 人材流動化の促進 (1) 中途採用，短期労働者の増加 (2) フレックスタイム化，在宅勤務化 (3) 長期産休，託児所付オフィス (4) フリーの雇用契約増加	1. ＯＡ・ＦＡ高能率化システム 2. 社内エキスパート情報伝達・蓄積システム
キャッシュ レス化	1. 関連法制度の緩和等と現金出納のシステム化，決済のシステム化に伴い，企業内外さらに社会一般で 例 1. キャッシュレス化 例 2. ペーパーレス化 が進む 2. 国民総背番号制の採用，プライバシーに関する情報の機密保護など安全性確保が重要課題となる 3. 企業間ネットワークの成熟 4. コンピュータ犯罪の増加 5. ＩＤカード等，個人認識技術の発達 6. 総ての取引が電子化	1. 無店舗販売・決済システム 2. 企業間ネットワークシステム 3. 名寄せシステム 4. リザベーションシステム
コミュニティ化	1. マルチメディアコミュニケーションの整備 (1) インテリジェントシティの登場 (2) セキュリティセンターによる24Ｈ×365日サービス (3) セキュリティセンターと広域セキュリティシステムとの連携 2. 自治体主導型地域リゾート産業の増加	1. インテリジェントＶＡＮシステム 2. 企業間ネットワークシステム

項　目	社　会　の　状　況	情　報　シ　ス　テ　ム
	3. 地域ＤＢ事業の発展 4. 企業間ネットワークの成熟 5. 企業間での情報，施設の共有化，相互利用 6. 情報プロテクト規準の明確化 7. 地方分散化の進展	
その他	1. 組織構造の変化 (1) 企業活動に関する情報の一元管理が進むことにより，意思決定・情報伝達の構造がピラミッド型からフラット型(文鎮型)に移行する (2) フラット型(文鎮型)の意思決定構造になると企業トップ個人のキャラクターが出やすくなる 2. ミニ家族化 (1) 高齢化，レジャー化，女性の社会進出などを背景として，フレックスタイム，直行直帰，在宅勤務が導入されることに伴い，家庭内にテレコミュニケーション機能を備えたインテリジェントルームが必要となる。 (2) このインテリジェント・ルームが社会への絆として，ミニ家族化に伴う脆弱性を補完することになろう 3. 学校 (1) 人材育成上，学校－企業の提携増加 (2) 社内ＣＡＩ普及 4. ベンチャービジネスのリスクが大きく変化している 5. 知的所有権にしばられる	1. 企業内情報伝達ネットワークシステム 2. 全社ＤＢシステム 3. 在宅勤務システム 4. サテライトオフィスシステム 5. リゾートオフィスサポートシステム 6. 在宅学習システム

付表 3. 個　人

項　目	社　会　の　状　況	情　報　シ　ス　テ　ム
高　齢　化	1. 単身または老夫婦世帯にＴＶ電話 2. 防犯・防災遠隔監視 3. 年金族の増加 4. 四世代同居 5. 家族・世代間のコミュニケーション円滑化 6. 健康指向による高齢者スポーツの増加 7. ボケ防止にワープロ・パソコン利用	1. ＴＶ電話 *2. 健康チェック(ホームドクター)システム *3. 運動能力向上システム *4. ヘルシーシステム （老化防止，健康増進，ストレス解消） *5. 生きがい追求システム *6. ヒューマンスクランブルシステム （屋外緊急システム） *7. ホームキーピングシステム
国　際　化	1. 海外旅行の増加と円滑化 2. 海外生活の増加 3. 転職があたりまえとなる 4. 深夜・早朝活動の活発化 （24時間化）	1. 海外情報案内システム 2. 自動翻訳システム 3. 交通情報案内システム *4. 統合監視通報システム （家庭セキュリティシステム）
レジャー化	1. 会員制リゾート(会員権市場成立)の増加 2. 買物の３パターン化 （レジャー型，生活型，通販型） 3. 日本型のホームパーティ （会社を離れた趣味の同好者，コミュニティメンバー，友人） 4. バカンスの増加	1. レジャー観光案内予約システム *2. コンフェレンスシステム （リゾート案内等） *3. 統合監視通報システム （外出中の家庭セキュリティ等） 4. 各種ゲーム提供システム *5. ホームコンピュータシステム
女　性　の　社　会　進　出	1. ワンストップショッピング等家事の簡略化 2. 主婦の在宅知的作業の増加と収入増加 3. 無店舗販売・宅配ニーズの拡大 4. 独身者(男女とも)の増加 5. 昼間留守宅の増加	1. 無店舗販売・決済システム 2. 時間指定宅配システム *3. コンフェレンスシステム （商品案内等） *4. 統合監視通報システム （外出中の家庭セキュリティ等） *5. ヒューマンスクランブルシステム *6. ホームオートメーションシステム

項　目	社　会　の　状　況	情　報　シ　ス　テ　ム
キャッシュレス化	1. カード利用の拡大 2. 背番号制の確立	1. カードチェックシステム 2. 医療支払システム 3. 背番号支払システム（背番号クレジット） *4. 情報サービスセキュリティシステム
その他 合目的化 多様化	1. 文化や自然に親しむ形の任意参加型の集まりが増える 2. コミュニティ内の情報化 3. 休日子供と遊べる親，遊べない親の2種化 4. サラリーマン(首都圏)は家が持てない	*1. 快適環境システム *2. オープンスペースサプライ 3. コミュニティセキュリティシステム *4. 衛生管理システム

＊：ライフスプリング計画で採用しているシステム

第3章　主要セキュリティ産業の発展形態と問題点

1.　アクセスコントロール

アクセスコントロールという言葉は，専門家を除いて一般には，まだ耳慣れない言葉であるが，それがセキュリティシステムの関連の用語として使われ始めたのは，ここ十数年来のことであろうと思われる。

このアクセスコントロールという言葉の概念は，昭和62年度報告書「セキュリティ産業の実態と新しい課題」によれば，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制御することから始まって，現在では，これらのエリア入退出管理だけでなく，情報システム，通信回線等への不正な（許可されていない）接近の制御，許可された情報レベルに限定するといった制御，さらに，その状況を監視し，記録をとり，警報の送出等を行うところまで包含するにいたっているという概念設定がなされている。

本項では同報告書と同じ観点にたって，アクセスコントロールについて，先ず基本的な概念，構成などの現状について述べ，さらに特定者の識別（アクセスすることを認められ，その権限が与えられている者の識別，保証），動作（出入口の開閉），システムへのデータ入力，記録，監視に分け，さらにそれぞれが2010年頃どう展開しているかなどについて考察をすすめたい。

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の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が，別項目で記述することとし，本項では省略する。

(1) 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1に示す通り，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。

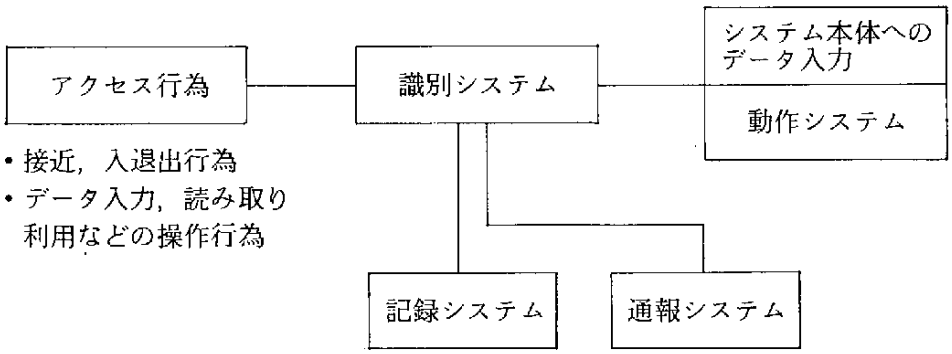


図1. アクセスコントロールシステム

□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出を行う。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。

基本的には，2010年頃のアクセスコントロールのシステム構成も上記に近いものであろうが，それぞれのシステムが格段に高性能化され，よりコンパクトに変化していると思われる。

(2) 識別システム

アクセス者を識別する方法は，鍵やカードを用いる方法，ＩＤ番号やパスワードで識別する方法，指紋や音声，掌形，サイン，印鑑などを用いる方法などいろいろあるが，前述のように，「人の携帯物による識別」と「身体上の特徴による識別」「記憶による識別」に大別される。いずれも識別のために照合するデータなどが予め登録されている必要がある。

① 人の携帯物による識別

現在，最も一般的なものは身分証明書や鍵，磁気カードなどのカード式であるが，これらは紛失したり，他人に貸与したりして，悪用されるケースも考えられるので，カード式と暗証番号とを組み合わせて使うなど，２種類以上の方法を併用してより安全性を高める方法が増えつつある。

また，アクセスコントロールという範疇からは少しはずれるが，識別して，正当性を認証する方法として，見逃せないものとして署名と実印の問題がある。そのことについても少し触れておきたい。

現在のビジネス取引で使用されている契約書などは，その正当性を証明するために，自筆の署名や実印の捺印，印鑑証明などが使われている。つまり署名の筆跡や実印の印影をもって，契約書が正当な人物の発行によることを他のものと識別し証明している。

日本では，署名より実印のほうが多く使われていて，これまではあまりトラブルも発生しなかったのであろうが，実際には実印の偽造はそれほど難しいものではない。今後，国際化がますます進んでくると海外諸国との取引も増え，契約書なども印鑑より，英語のサインが使われるものが圧倒的に増えてくる。またカード社会になれば，取引き本人の正当性の識別のためのサインの必要性もますます増えてくるものと思われる。

しかしながら，サインの筆跡や実印の印影は，コンピュータシステムやデータ通信システムにはそのまま使うことはできない。

例えば，ＦＡＸで転送されたものやコピーされた印影や筆跡は容易に偽造できるので，法的には正式な文書とは認められていない。

それでは，これらのものは2010年頃にはどのように進展しているのであろうか。

結論的にいえば，人の携帯物（ここでは署名を含めて）による識別は，一方では非常に素朴な鍵と，また他方では非常に高度な情報化社会に適合できるカード（多くのデータを記憶させ多目的に使える）や暗号，パスワード，さらにディジタル署名のような携帯物とはいい難いようなものに分化しながら，次第に淘汰され，やがて多機能，ハイブリット化したものに集約される道を辿るものと思われる。現在の携帯物による識別方法を表２に示す。

表 2.　携帯物による識別

種　類	方　式	説　　明
鍵	符　号　錠	ダイヤルの回転方向と暗証番号記憶の有無による識別（解錠）
	キーロック	一般的な鍵の所有による識別（解錠）
押ボタン	暗証番号	任意の数字などの押ボタンにより暗証番号やパスワードなどを入力し識別
カード	接　触　式	カードに記録された情報をカードリーダーに挿入し読み取らせて識別 ・磁気方式―磁気ストライプによる情報磁性の針金による情報 ・ホログラム方式―レーザー光によるホログラム情報 ・ＩＣカード方式―ＩＣメモリに記録された情報
	非接触式	カードまたはリードステーションから電磁波などを発し，その情報により識別 ・電磁波方式―電磁波情報を識別 ＊カードの方から電磁波を発するものと ＊発せられた電磁波をカードが受けるものとに区別

② 身体上の特徴による識別

身体上の特徴による識別は，顔，声，掌形，指紋，網膜などによる識別方法があるが，古くは，痣，ほくろ，特殊な傷なども識別の手段として使われていた。

これらの方法による識別は，まず正当なアクセス者として認証するための基本データを蓄えておいて，アクセス時に比較判断し，識別する必要がある。

そのデータ蓄積の方法として，端末のＩＣメモリーに記憶させる方法とコンピュータの磁気媒体に記憶させ，ファイルする方法がある。スタンドアロンで使用する場合は前者，オンラインの場合は後者を使うのが一般的である。現在の身体上の特徴による識別方法を表３に示す。

表 3. 身体上の特徴による識別

種類	方式	説明
指紋	指紋特徴点指摘方式	指紋の特徴点（マニューシャ）を選び出して予め登録してあるデータと比較し識別
網膜	毛細血管特徴点方式	眼底の毛細血管の特徴点を選び，予め登録してあるデータと比較し識別
掌形	掌の形状比較 各指の長さ測定	掌全体の形状により識別 各指の長さを測定比較して識別
音声	話者認識	音声スペクトルの時間的な変化を図形化した声紋を予め登録してあるデータと比較し識別
	音声認識	音声波から音韻データを抽出して言葉（暗号文など）を判定して識別

これらのものは前述の携帯物による方法と比べて，紛失や忘れたりして他人に容易に悪用される心配がないという利点がある。

しかしながら，指紋や掌形は手首と指を切断されて，悪用される危険性が皆無とはいえない。また話者認識による識別は音声を登録した時の体調や時期のずれにより声紋が変化することがあるので，いかにして変化しない特徴をみつけだすかが，

今後の重要な課題となる。

③ 記憶，その他による識別

記憶による識別は暗証番号，暗号文，サインなどである。サインをここに分類するのは必ずしも適当でなく，身体上の特徴として分類する向きもあるが，本項では一応，サインの癖，筆勢などを記憶の範疇として区別した。

その他については，未知の分野で必ずしも，実用性があるかどうか分からないが，将来発達の可能性もあるかも知れないので，挙げておく。

顔や頭蓋骨，コンピュータへのキータッチの癖，体臭などによる識別である。それぞれの簡単な説明を表4に示す。

表4. 記憶、その他による識別

種　類	方　式	説　明
記　憶	暗証番号，暗号文	記憶した暗証番号や暗号文と照合し識別（データの暗号化については省略）
	サ　イ　ン	サインの形状，筆勢，筆圧などを登録データと照合して識別
その他	顔	写真やビデオなどの画像と比較して識別
	頭　蓋　骨	頭蓋骨の形や寸法を測定して，法医学的に識別
	コンピュータへのキータッチ	コンピュータへキー入力する時の癖を予めコンピュータに学習させておき，キー入力されたデータと比較し識別
	体　　臭	警察犬が犯人を追跡するように，臭いのデータを数値化したものを記憶しておき識別

以上，識別の方法について，現在のものを中心に説明した。

それでは，これらの識別方法は2010年頃には，どのように変化しているのであろうか，推測してみよう。

当然，2010年頃の社会は，高度に発達したＯＡ機器と情報通信ネットワークが広範囲に組み合わされたシステムがほとんどの分野に普及している社会で，まさに高度情報化社会の名に相応しい社会に発展しているであろう。

ビルのインテリジェント化はオフィスだけでなく，ホテルも，病院も，学校も，さらに一般住宅へも普及し，特に都市を中心にインテリジェントシティが出来上がっているかも知れない。

そうした社会では，セキュリティシステムも広範なネットワークが構築されているはずであるから，そのサブシステムとしてのアクセスコントロールシステムのための本人識別データなども，セキュリティセンターのホストコンピュータにファイルされていて，アクセス者のセキュリティエリアへの入退出の識別や制御はもとより，コンピュータにファイルされているデータへのアクセスの識別・制御なども瞬時に行われ，セキュリティセンターに適切に通報され，記録が取られるようになっている。

そこではもはや，現在のような識別の方式は一部の分野を除いては，淘汰され，より高度なものに変化しているであろう。

つまり，現在，指紋や声紋，網膜，あるいは各種カード類が使われていて，これらの技術は，多分，将来は誤認率とか，手間の掛かる点などは，当然解決されるであろうが，それでも，人が目と頭脳で識別する方法と比較すれば，便利さにおいても，技術的にも相当の差があるといわざるをえない。

2010年頃は，そうした問題をクリアして，人や物体の存在を，ただ存在の認識だけでなく，誰か，あるいはどんな物体かを非接触の状態で正確に識別する方法が開発されるものと期待される。

(3) 動作システム機器

動作システムは前述の通り，識別システムからの情報を受けて，電気錠や自動ドア，自動シャッターなどを作動させ，出入口の開閉を管理するシステムであり，単なる錠前や自動ドアそのものなどの単体とは区別しておきたい。つまり識別システムからの情報（電気的な信号も含めて）によって適切に作動するようにシステム構成されていなければならない。

それでは，これらの動作システム機器は，2010年頃にはどのように進歩しているのであろうか。識別システムの進歩と並行して，大手企業，金融機関，官公庁，大学，

研究所，病院，原子力施設，さらに高級住宅などの出入口はほとんど全て，アクセスコントロールシステムの一環として，電気的に解施錠される自動ドアや自動シャッターになっているだろう。しかもドアやシャッターの材質などは硬質の強化ガラスかプラスチックのような軽くて強く低コストな防御素材が開発されていて，実用化されているものと思われる。

ただし，一部の企業や一般家庭には，まだ現在と同じようなものが残されていることも考えられる。

1.2 監　視

監視は「みはる…気をつけて見守る」ことであるが，ここではアクセスコントロールの中の監視に範囲を絞って述べる。

アクセスコントロールでいう監視には，

① セキュリティエリアへの不審人物の不法侵入の監視

② コンピュータシステムをサポートしている設備機器の運転制御，稼動状況あるいは設備環境の監視

③ 老人や患者，乳児などセキュリティを必要としている人々の監視

④ ある区域や機器類，現金や宝石，美術品などの貴重物件の監視

⑤ オフィスビルや家庭の環境（温度，湿度など）セキュリティの状況などの監視

⑥ コンピュータのデータやデータ通信ネットワークへのアクセス監視（識別・認証）

以上のものがあり，異常時には警報を発するとともに，アクセスコントロールシステム機器へ必要な情報（電気的な信号も含む）をインプットする。

(1) 監視の方法

① 機械的装置による監視

錠前，鍵，電気錠などについては，現在ではすでに鍵の集中管理をして鍵の在否で人の在否を監視するとか，電気錠からの情報（信号）によって，人の侵入を監視するとか，部屋の電源の点滅を制御するシステムが数多く採用されている。

さらに2010年頃は，高級住宅ばかりでなく，一般住宅にもホームオートメーショ

ンが普及し，その一環として，電気錠はもとより，システマティックに制御される錠前やセンサー類が数多く採り入れられて，人の侵入の監視・防御や照明・空調などの電源のＯＮ・ＯＦＦを，必要に応じて，遠隔操作で制御するシステムも広く普及し，これまでの単純な鍵は，次第に減少していくものと思われる。

② 映像による監視

a. ＴＶカメラ

ＴＶカメラでセキュリティエリアを撮影し，監視室のモニターテレビで監視し，異常が発生するとＶＴＲ装置で記録をとり，必要に応じて警察や中央管制塔に通報という監視システムから，現在では，ＣＣＤビデオカメラのような小型で高性能なカメラの進歩とともに，電子カメラや電子フィルム(Electronic Image Memory Device) あるいは画像電送技術の発達で静止画像の電送，さらにマルチ画像電送による遠隔監視も可能となっている。

2010年頃には，これらの装置や機器類はさらに高性能化，小型化し，種々のセンサーと結びついて，静止画像から動画像による遠隔出入口監視，行動監視，状況監視など高度な総合監視システムがトータルセキュリティシステムのなかに組み込まれているものと思われる。

b. 防犯用カメラ

セキュリティエリアに向けて，長尺の写真フィルムを装填した防犯用カメラを設置して，状況に応じて撮影し，記録写真（犯罪の証拠写真）を残すものであるが，2010年頃には，高性能ビデオカメラや電子カメラ，電子フィルムの普及で，解像度のよい証拠写真も出力されるようになると思われる。もし，現在のものがこのまま進歩しなければ，電子化の流れの中でだんだんと淘汰されてしまう。

③ センサーによる監視

センサーは，監視システムのアンテナとして，インテリジェントビルのビルオートメーションシステム，セキュリティシステムはもとより，一般企業，工場の設備機器類，一般住宅の設備にいたるまで，非常に広範に実用化されている。

ここではスペースの関係もあって，それらを網羅して記載することは省略するが，アクセスコントロールの面から，2010年頃には，センサーによる監視の中心的存在になると思われるものに，「ビデオセンサー」があげられる。

現在でも「ビデオセンサー」と呼ばれているものは，相当数あるが，高価なため

と技術的にも未解決の部分が残されているためか，広く普及するまでにいたっていない。

ビデオセンサーは，簡単にいえば，ビデオカメラに頭脳がついたようなもので，ビデオカメラで撮影されたものが何であるかを，その頭脳（コントロール装置）が判断する。

技術的には画像処理，画像認識，パターン認識の分野であり，また，写ったものが何かを判断するＡＩ（人工知能）技術の分野も関連してくる。

2010年までには，ビデオカメラ技術もＡＩ技術も長足の進歩を遂げ，高性能で小型のビデオセンサーが開発され，監視システムを始め多くの分野に普及しているであろう。

そうして全てのアクセス者や物の動作や動きは逐一，ビデオセンサーがとらえ，適切な情報（識別データも含めて）をセントラルおよびローカル双方のセキュリティセンターの管制塔に報告し，管制塔からの制御指令情報で必要な制御が，瞬時に行われるようになるであろう。

④　ソフトウェアによる監視

セキュリティシステムのためのソフトウェアは，現在，主として後述のものがあるが，ここでいうソフトウェアによる監視は，コンピュータシステムへのアクセスをパソコンや端末機によって，データ通信回線などを使って行おうとする場合の正当な方法を，ハードでなく，ソフトウェア的に指定することによって，アクセス有資格者（データの読取りと書込みを区別）を認証するというのが一般的であり，したがって監視と限定するよりも，識別・認証の表現の方が適切であろう。

なお，現在，ソフトウェアによる監視・識別・認証には，主として次のものがある。

a.　識別・認証ソフトウェア

アクセス者のインプットした情報と予め記憶（登録）しておいた情報とを照合し正当なアクセス者を識別する。また，同時に記録（時刻，場所，アクセス者氏名など）し，アクセス有資格者にはアクセスを認証し，必要なアクセス方法・領域等を指定し，その情報を発する。

また，無資格者が誤った操作や誤ったアクセスデータをインプットしても，アクセスできないことはもちろん，他の防犯システムなどからの異常警報や情報により，

システム運転の一時停止，緊急停止，あるいは必要なデータを切り離して保護するなどの処置をソフトウェア的にとる。

また，コンピュータ端末以外のものへのアクセスであれば，例えば，電気錠の解錠，ドアの開閉などの動作指示情報を発する。

b. 監視ソフトウェア

防犯システムからの異常警報を受けて，異常の確認，場所の特定，セキュリティセンターへの通報，記録および対処の指示情報（避難，消火など）を発する。

情報システム用の設備機器の運転制御，運転環境のチェックなどを行い，関係部署やセキュリティセンターなどへ必要な情報の受発信を行う。

これらのソフトウェアは，今後，さらに一段とその重要性が高まり，何かのシステム設計がなされる場合は，必ずこうした監視・識別・認証のプログラムが，あらかじめ組み込まれるようになる筈である。また，こうしたソフトウェアに対する価値も認められ，対価も支払われるようになるであろう。

3.1 アクセスコントロールシステムの将来展望

(1) 2010年のアクセスコントロールシステム

現在，コンピュータシステムを中心として企業の情報システム化がすすみ，それが社会のインフラストラクチャとしての通信ネットワークと結びついて，いわゆる「情報化社会」が形成されつつあるが，21世紀に向けて，情報処理技術や通信技術，マイクロエレクトロニクス技術などが，さらに高度に発達して，企業だけでなく，家庭の情報化，地域社会の情報化，国全体の情報化，国際間の情報化へとその範囲を拡大し，より広大で複雑な「情報化社会」が構築されつつある。

2010年頃の高度情報化社会における情報通信システムのセキュリティは，現在では想像がつかないくらいに，その重要度を増していると思われる。

当然，情報通信システムの複雑化や広がりに対応して，セキュリティシステムも，より高度で複雑なトータルシステムとして広域ネットワーク化が促進されているに違いない。

そうした状況にあって，高度情報通信システムへのアクセスコントロールは，トータルセキュリティシステムのサブシステムとして位置づけられ，他のシステムともネットワークを構築して，正当なアクセス者の識別・認証や有資格者への適切なアクセ

ス方法とアクセスできる情報およびネットワークの領域の範囲を指定するという機能を果たすことになろう。

また，そのためのソフトウェアも優れたものが数多く開発されているに違いない。

さらに，平素の監視システムネットワークも張りめぐらされて，エリア内に何か異常が発生すれば，監視システムから瞬時に警報が発せられるとともに，必要な対応策が講じられるようになっているであろう。

2010年のアクセスコントロールの技術的進歩も，この素晴らしい科学技術の進歩の産物に他ならない。それらは，これまでに推測してきたものの延長線上にあると思われるが，その代表格は，やはり人間の目と耳によって脳が知覚することにより近い形の「音声認識と人・物体認識」に集約されるであろう。そのためのソフトウェアも優れたものが開発され，しかもそれらが単体でなく他の監視システムや防犯システムとも効果的に結びついてトータルセキュリティシステムを形成していると思われる。

実際に，アクセスコントロール分野がどれほどの産業規模に成長しているか，正確に推測することは難しいが，21世紀の高度に進歩した情報化社会にとってセキュリティシステムの一翼を担うアクセスコントロールは，一方で世界的な広がりを持つと同時に，われわれの身近で，地域社会にがっちり根を下ろした産業として繁栄していることは間違いないであろう。

2010年のわが国におけるアクセスコントロール分野の市場規模を予測することは難しいが，現在の4倍から5倍位への成長が期待されるところである。

2. 通　　信

2.1　信頼性・安全性対策

(1)　通信システムの動向

1982年に中小企業ＶＡＮが認められ，3年後の1985年には電気通信事業法が施行となり，通信サービス事業への新規参入者数は着実に増加しつつある。

1988年の情報化白書によると5年後における通信回線の利用予想は，専用線，高速デジタル回線，ＤＤＸパケット交換等の通信サービスが増加し，帯域，符号，高速デジタル回線の利用が，現状の3倍に伸びる見通しであり，通信システムをとりまく状況は急激に変化している。また，近年衛星通信も本格的な実用段階に入りつ

つある。

やがて，近い将来には，音声，画像などの異なった情報を単一の網により提供可能なＩＳＤＮ（総合デジタル通信網）が従来の電話網にとって替わるものと思われる。

一方，通信システムを利用する企業のオンライン状況は，通産省の62年度情報処理実態調査（5,520社）によると，オンライン化率78.8％（前年度調査76.0％），1企業あたりのオンライン端末数176.9台（前年度調査129.3台），通信回線の使用数178,444回線（前年度調査161,344回線），1企業あたりの通信回線の使用数32.3回線（前年度調査28.5回線）となっており，コンピュータを利用する企業の情報通信システムは拡張しつつある。

このような情報化の進展に伴い，社会や企業の活動における情報通信システムへの依存度は今後ますます高まることであろう。その情報通信システムに万一の事態が生じた場合に被る被害は，非常に大きなものとなるであろう。

すでに情報化社会の想定で述べた各種情報通信システムは，通信回線が安全に確保されて初めてその機能が発揮されるものである。すなわち，高度情報化社会は，通信システムの機能喪失事態を想定すると，潜在的にきわめて脆弱な特質を持つことになるといえる。高度情報化が進む今日，通信の途絶による連鎖的な影響はさまざまなものがあるが，金融・物流など特に社会経済活動の中枢的機能の混乱は重大である。

(2) 通信網の信頼性・安全性対策

故障発生率を小さくするためには，装置自体の信頼性を向上させる方法があり，高信頼度部品の使用や電子回路の高集積化による部品個数の削減等が行われている。また，通信システム全体の信頼性を確保するためには，種々の回線構成法がある。

① 網手法による対策

a. 多ルート化

面的な広がりをもつ通信システムにおいて，より一層の信頼性を得るため，その特徴を生かし，網的な規模で機能の代替や危険分散を行うのが網的手法による信頼性対策であり，その伝送路網における対策には，伝送路の2ルート化，多ルート化，伝送関門局分散があり，1つのルートの切断または回線品質の低下に対し，他のルートを使用して信頼性・安全性を確保しようとするものである。その具体例には次のようなものがある。

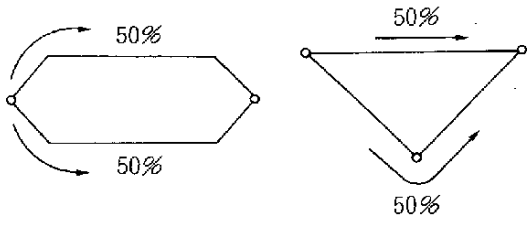


図 2. 伝送路の 2 ルート化

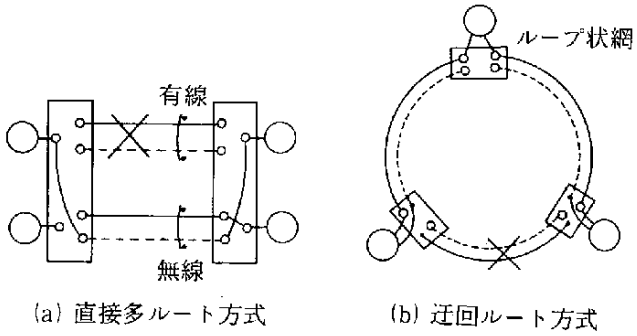


図 3. 伝送路の多ルート化

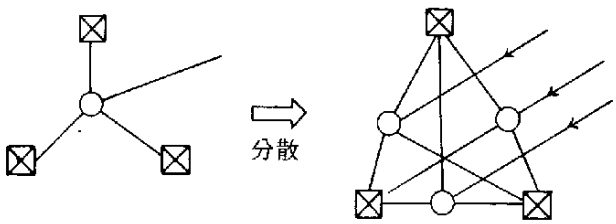


図 4. 伝送関門局の分散

b. 機能の分散・移転

交換網における対策には，ユニット分散，交換局分散，斜め回線の設定などがある。

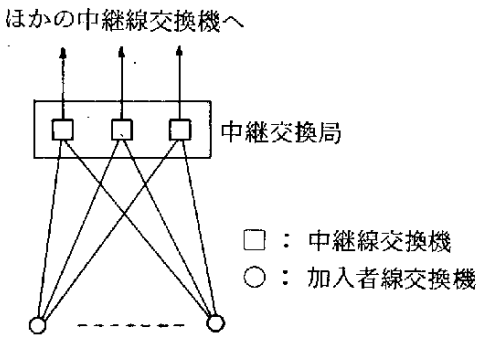


図 5. 中継線交換機の交換ユニット分散

通信網は一元化・集中化されるほど災害に対して脆弱である。一方多層的，多元的通信網（複数の通信網，ルート，メディア）である場合，設備の冗長性

が生じる可能性はあるが，リスクが分散されるという利点がある。

② 緊急時対策

災害・大規模事故等の不意急襲的な発生に対しては，迅速に対処しうる移動無線車（衛星通信用，マイクロ回線用等）を適切な地域に配置し，不意の災害・事故等による社会的な混乱を最小限にするなどの対策が構じられている。

③ トラフィックの輻輳対策

トラフィックの輻輳に対しては，その規模，範囲，継続時間などによって異なるが，つとめて通話の疎通を確保し，その拡大を防止し，重要通話の疎通を優先して確保することを基本とし，次のような対策がとられている。

a. 空き回線，予備設備などを使用して，臨時回線，臨時電話の設備

b. 代替回線など他のルートによる迂回ルートの使用

c. 市内交換機における発信規制

d. 着信側の交換機や中継交換機における接続規制制御（トラフィック制御）

④ 犯罪等の対策

a. 物理的破壊・故障の対策

通信設備（交換局・中継所・伝送路等）の物理的破壊にたいしては，通信回線の統制局等における常時モニター監視と定期・臨時の巡回点検が実施されている。

b. 電波障害等への対策

無線系における妨害電波（気象条件等の変化による電波障害等も同じ）に対しては，予備の周波数を保有し，ただちに予備周波数への切り替えや，有線系メディアへの切り替えなどの対策が考えられている。

c. データ保護対策

通信網を盗聴などの悪意から守るためには，設備的な対策が種々考えられている。また，送受するデータの完全性チェック，交換網における閉鎖接続等が実施されている。

⑤ そ の 他

現在，基幹通信網を構成する伝送路は，有線系で同軸ケーブル，光ファイバー，無線系では地上マイクロ回線が主体であるが，衛星通信も将来の主要な伝送メディアと考えられている。ここでは伝送系の特性について考えてみたい。

a. 有線系の特性は，長所として安定した回線と大容量の回線を確保できることである。昭和63年の電気通信審議会の発表によると，現在の光ファイバーの伝送容量は，ファイバー芯を1システムとして，1システムあたり約23,000 chであり，今後の技術進歩により，近い将来現在より1桁上の大容量になるものと考えられている。

反面短所として，災害・事故等によるハード的な通信の切断・通信品質低下の可能性が大である。また長距離回線の設置は多くの経費と長期間を要し，軽易な経路変更等の融通性に欠ける。とくに，最近の都市化集中傾向や，地下の有効活用等により，市街化地域においてはますますその設置等が困難となりつつある。

b. 地上無線回線は，小容量から大容量までの広い領域での経済的利用が可能である。昭和63年の電気通信審議会の発表によると，マイクロ回線の場合，現在1システムあたり5,760 chであるが，技術進歩にともない，将来は現在の数倍程度の大容量化が見込まれている。

衛星通信は全国エリアをカバーでき，任意の地点に地上局を設置すれば，全国的な情報通信システムに即応でき，災害時対策を含む回線需要の変動に対する柔軟な回線設定が可能となり，放送などの広域通信への利用も有効と考えられている。

しかし，無線系は周波数の制限を受けるとともに傍受（盗聴），妨害および気象条件の変化による電波障害の影響を受ける。したがって，データ保護や電波妨害・障害に対する処置が必要となる。

2.2 信頼性・安全性の低下事例等

通信システムの伝送メディアは，地震，火災，水害，事故，犯罪等によりつねに通信の切断・回線品質の低下，通信内容の漏洩等の脅威にさらされている。

(1) 地　震

現在，関東大震災クラスの地震が起きれば，通信網にも相当の被害が考えられ，都市機能を麻痺させることも想定されよう。

現在のように東京への都市集中化傾向が将来にわたって進むならば，インフラストラクチャとしての通信システムの破壊は，東京の都市機能の麻痺にとどまらず，

日本全体への影響ははかり知れないものがある。

昭和43年５月16日の十勝沖地震においては，地下ケーブル切断，無線中継所の被害により，本州－北海道間の通信が約２時間にわたり途絶し，社会の反響は大きなものであった。また，58年５月の日本海中部地震は，地盤の液状化などにより，電柱，管路，マンホールが傾斜，浮上，沈下するなどの現象があり，また，トラフィックの異常輻輳が起きた。後者は比較的都市機能が集中していない地域であったため，小規模な被害にとどまったと思われる。

しかし，都市機能が集中している地域で，かつ，対策が不十分であるならば，その被害は大規模となり，社会に与える影響は非常に大きなものとなるだろう。とくに地震は，地盤のずれ，浮上，沈下，ゆれ等により通信ケーブルの切断等，通信設備に対する影響が大である。

(2) 火　　災

洞道内のケーブル焼損が引金となって広範な災害連鎖を引き起こした59年11月の東京世田谷電話局ケーブル火災は，社会的インフラストラクチャとしての情報系の重要性を皮肉な形で世に知らしめることとなった。また，合成樹脂による被覆ケーブルの火気に対するもろさが改めて明らかにされ，これを教訓に洞道内のケーブルについては難燃処理および被害の極小化対策が施されることになった。

(3) 水　　害

58年７月の島根豪雨においては，道路決壊，橋梁流出，土砂崩れなどによる電柱倒壊，通信ケーブルの損傷や交換局の水没などがあり，その結果通信が途絶している。

過去の台風などの被害状況をみると，このような通信ケーブルの切断，通信設備の水没などによる機能停止がみられる。

通信ケーブルは，水圧などによる物理的損壊を受けやすく，また，電源設備などは比較的低いところに設置される場合が多いため，浸水の可能性が大である。このように通信システムはそれなりの対策は施されているものの，水に対して脆弱な面を有している。

(4) 事 故 等

① 設備の故障

通信設備の故障には，交換設備・伝送設備等の本体の故障ばかりでなく，電源

設備の故障も見逃せない。最近では，ハードウェアばかりでなく，ソフトウェアのバグ，オペレーションミスによる機器の故障なども情報通信システムの脅威となる重要な要素である。

② 停電による影響

通信システムは，停電もまた大きな脅威の１つである。その例が，62年７月に起きた首都圏の大停電である。

クーラーの一斉使用などで，短時間に急激に電力使用量が上昇し，３ケ所の超高圧変電所において供給量が需要量を超え，次々に送電不能となってしまった。

また，都内にある信号機のうち，1,296基が停止し大きな交通渋滞となった。

一方，銀行でもオンラインシステムが一時的なストップに見舞われた。このように停電も社会に与える影響は大きなものがある。

③ トラフィックの輻輳による影響

トラフィックの輻輳には災害型輻輳，企画型輻輳などがある。

災害型輻輳は，災害発生時や大事故時に起こる突発的な輻輳であり，特定の利用者や地域への通信（通話）要求が殺到するなど，通信設備の使用飽和によって起こる障害である。

また，企画型輻輳は，電話予約等の特定日・特定時刻に集中する呼，人気テレビ番組へのリクエストなど，特定の加入者への通話要求が一時的に増大し，異常トラフィックの結果起きる通信障害である。

⑸ 犯　　罪

各種情報通信システムが発展するにともない，犯罪の脅威も増大する。すなわち，破壊活動や通信回線からのデータ盗聴，不正データの入力等をはじめ，各種情報通信システムへの不法接近による信頼性・安全性の低下が重視されている。これらについては，通信の秘密・データ保護・プライバシーの保護等の観点からも今後さらに重要な分野となるであろう。

2.3　2010年における情報通信システムの課題

2010年における情報通信システムの信頼性・安全性の確保は，脅威（地震・火災・水害・事故・犯罪等）の対象と各設備の特性を考慮して推進されるべきであり，具体的には，経済性，信頼性，耐災害性，柔軟性（代替の難易性）等を勘案した総合的判

断により最適な方法を創造し，長期的計画のもとに実行しなければならない。今後豊かな情報化社会を構築するためには，国，企業，個人等それぞれの立場において責任ある対策を構じるべきものと考えられる。

(1) 新しい通信方式の確立

例えば，通信回線は，光ファイバーの登場によって飛躍的に通信容量が大きくなっている。すでは昭和62年に，基幹ルートでは，1芯で電話23,000回線分の伝送が実用化されている。今後の技術革新により，2010年頃においては，現状よりはるかに拡大しているものと思われる。

このように，伝送路の大容量化が進展すればするほど，故障発生時の影響度も大きくなる。したがって，大容量化しても，それに比例して事故の影響が広がらないようにする対策が不可欠である。このためには，現在の技術原理や構造にとらわれない新しい発想や方式の出現が期待される。

(2) 被害の極小化

今日，情報通信システムは相互に接続されるなど，拡大の一途を辿っている。このような状況下で，仮に1つのネットワークの故障が他のネットワークに波及して影響範囲が拡大していくようでは情報化社会の安定はない。とくに，これからの国際化を考慮した場合には，故障の波及がより一層問題を大きくするものと思われる。

そこで，ネットワークの故障が発生した場合に，その影響を狭める方向での対策が必要になる。そのためには，たとえばニューロコンピュータやファジー理論の応用などで，故障範囲を極小化するなどの技術開発が待たれるところである。そして，そのような技術を採用したインテリジェントネットワークを実現する必要がある。

(3) 間接被害の拡大への対応

通信サービスの提供者は，たとえ，部分的な故障で直接的な被害者が限定されたとしても，当該被害者の情報通信システムを利用している顧客全てに被害が及ぶということを考えなければならない。例えば，昭和59年11月の世田谷ケーブル火災において，同地区にコンピュータセンターを設置している三菱銀行では，コンピュータシステムに異常はなかったが，通信回線が切断されたことにより，全国の顧客が影響を受けた。また，この事故で個々の電話加入者が通話不能となっただけでなく，通信しようとする相手が全て影響を被ったことに注目する必要がある。

すなわち，通信回線の事故では，その回線を利用している企業や個人が直接的に

受ける被害もさることながら，その企業のサービスを利用している顧客が被害者になることや，通信相手が間接的な被害者となっていることを理解しておかなければならない。情報通信システムおよびネットワークの大規模化に伴い，この間接被害がますます広がっていくことになる。

そこで，今後の通信システムの信頼性・安全性対策においては，いかにして間接被害を最小限に食い止めるかという観点も，より前面に押し出される必要性がある。

(4) ソフトウェアによるセキュリティサービスの向上

現在情報通信システムの拡大に伴い種々の問題が発生している。その1つに異機種間の相互接続が容易でない事実がある。その解決策としてコンピュータ相互接続の手続き・プロトコルの標準化があるが，国際標準化団体において検討中であり，データの送受信に関する標準仕様はほぼ完成し，それを実装した製品も世に出る段階にある。したがって，2010年にはコンピュータ間の接続問題はほとんど自由に行われている時代になっていると考えられるが，送受信データのセキュリティに関し，種々の機能が開発され，例えば，次のようなサービスが普及しているものと思われる。

① 通信相手の正当性を保証するサービス（Authentication Service）

② 情報通信システムへの不当アクセスを防止するサービス（Access Control）

③ 送受信データを秘匿するサービス（Date Confidentiality）

④ データの改ざんを検出するサービス（Date Integrity）

⑤ 送受信事実を記録するサービス（Non-repudiation）

今後の情報通信システムの拡大を考えると，このようなセキュリティソフトウェアは，その利用を通して効果を確認し，研究開発とその成果の累積という繰り返しによって，逐次信頼性・安全性の向上を図るという手順が必要である。

(5) 利用者ルールの確立

各種情報通信システムが進展するに伴い，紙幣や硬貨などの現金による直接決済は，電子決済などによりその比重が下がり，現金に相当する情報が通信回線上を多く流れることとなろう。また現在でも個人・家庭においてホームバンキングが普及しつつあり，このような現金同様の情報量は将来著しく増加するものと思われる。この情報の紛失・改ざん・盗聴・漏洩などは社会的問題に発展する可能性があり，絶対に許されない。このような事故・犯罪の未然防止対策として，伝送情報の暗号

化・完全性チェックやアクセスコントロールなどによる身元確認が広く実施されていると考えられる。

また，不特定多数の加入者が利用するパソコン通信の掲示板は，すでにマスメディアの性格を帯びつつあり，ISDNの普及とともにパソコン通信はもとより，より便利で高度な通信がさらに発展している。個人においても，文字，図形，映像，音声等の情報提供が可能なパーソナルメディアとマスメディアの仕組みが相補いながら発達し利用されているものと想定される。

このように便利な各種情報通信システムを利用するにあたっては，最低限の利用者ルールが必要であり，全利用者がそのルールを守ることにより，初めて情報通信システムを安全に，かつ，有効に活用できるものである。ルールの遵守は利用者の果たすべき責務であろう。この利用者ルールは現在確立しているとは思えない。したがって，2010年では情報通信システムの利用者ルールの確立と普及はますます重要となろう。

(6) コンピュータ犯罪の防止

最近話題になっているコンピュータウィルスや種々のハッカーによる不法侵入は，通信システムを介したコンピュータ犯罪として，情報通信システムの脆弱性を社会的に再認識させた。今後通信サービスの多様化とその普及が予想されることから，コンピュータ犯罪も増加することが考えられる。このような状況からコンピュータ犯罪に対しては，法制度やシステム機能の面などから各分野において対策が研究されているが，さらに利用者側の利用ルールに基づいたモラルの向上が重要となるであろう。

このため，2010年代に情報通信システムの提供・利用双方において，トップあるいは中堅となるべき現在就学中の世代に対し，情報通信システムの役割および重要性を十分に認識させ，不当な行為を行わないようモラル教育を徹底させることが急務である。

3. コンピュータシステムのバックアップ

コンピュータシステムは，2010年には無人化，リモートコントロール化が進み，コンピュータセンターは高度にセキュリティ対策の整備された無人化センターとなるであろう。

したがって，生活，生産活動が地方へ移動することになり，都市の一極集中から地方分散へと進むことになろう。これは，情報基地(コンピュータセンター)の地方分散であり，そのことが"地方の情報都市化"をもたらすことになると思われる。

3.1 コンピュータシステム障害の影響

政治，経済，社会活動の全てにわたり，基盤となるコンピュータシステムに障害が発生し，機能しなくなった場合はどうなるであろうか。その与える影響は極めて大きく，大きな混乱を生じる。経済活動は停止し，企業にとっては生存を，医療サービスの停止は人命救急を脅かす。

したがって，システムの障害防止，機能復旧に対する備えは便利で，豊かさを守るために必須の備えを言わねばならない。これは，企業，行政当局の大きな社会的責任である。

3.2 バックアップシステムの方法

コンピュータシステムのバックアップには，莫大な投資を余儀なくされる。データ，ハードウェア，通信の3つについての安全対策，リスクの分散，復旧対策が必要である。

一企業，一地方自治体では，そのコストを負担できないところも多くなろう。また，対策の範囲をどうするかも問題である。したがって，社会・経済活動のある程度の混乱は容認し，克服しつつ，障害に対応することも必要であろう。

(1) バックアップの現状

① データのバックアップ

データの保管事業については，近年，トランクルームサービス業（磁気テープ，書類のほか家財，美術骨董品，毛皮等の保管を含む）の発展が著しい。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とされている。

データの安全保管のためには，災害から同時被災を避ける地理的条件，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ている。

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を，現時点で本格的に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。

しかし，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。

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。コンピュータユーザでは，平常時利用と併せて災害対策として通信回線の二重化をはかったり，衛星通信の利用を検討したりしているが，問題はコスト的に大きな負担となる点である。

(2) バックアップの方法

コンピュータシステムのバックアップは，将来的にはデータ，ハードウェア，通信を含めた総合的な機能を有するセンターとなる必要があろう。しかし，これにはコストの問題もあるので，現実的な解決策として各種バックアップを考えてみると，次のような方法がある。

① システムが復旧，再構築されるまでの応急処置対策

- 手作業による業務体制の整備，マニュアル化。
- コンピュータメーカ，情報処理業者との特約。

② 安全な立地へのセンターの移転

- センターの郊外移転（ヘッドオフィスとバックアップオフィスの分散化）。

③ 重要なシステムの自社による分散二重化

- 同時被災を避け得る立地におけるシステムの完全二重化（あるいは，一部重要システムの二重化）。

④ システムの分割・分散化

・コンピュータの一部重要システムを分割し，安全な立地に移し，通常運用をリモートコントロールとする。

⑤ 提携による相互バックアップ

・同業者等で，有事において必要最小限の情報処理を行って相互にバックアップする提携を結ぶ。

⑥ 共同バックアップセンター（ホットサイト，コールドサイト）の利用

・民間独自の共同バックアップセンターの建設促進。

・官民による第３セクター方式の共同バックアップセンターの建設。

・同業者による共同バックアップセンターの建設。

とくに，人命救急という観点からの医療サービスや，バンキングシステム等の共同バックアップセンターは重要であると思われる。また，共同バックアップセンター相互のネットワークを作り，相互に補完する体制も作る必要があろう。

4. ファシリティマネジメントサービス

4.1 ファシリティマネジメント（ＦＭ）サービスの状況

(1) 高度情報化社会になると，コンピュータハードウェア（ホストコンピュータ）の運用状態は大幅に変わるだろう。つまり，地方公共団体，企業等のオフィスでは，ワークステーション等の端末装置を利用した情報処理の受益者のみとなり，ホストコンピュータは，この情報化社会のインフラストラクチャとして，地方の情報基地等に展開されていく。さらにこれを支える通信ネットワークも，大容量高速化と高信頼度が実現し，この傾向に一層拍車をかけるであろう。

また，個人の各種情報処理サービスは，地方公共団体を中心とした，個人情報処理サービス業者が情報処理サービスを提供し，地域に根ざしたきめ細かいサービスを展開するであろう。

そして，センターの運用は，コンピュータシステムの自動・無人運転が，信頼性高く利用できるようになったこと，センターの地方分散化の影響でほぼファシリティマネジメント（ＦＭ）業者に委ねられることになるだろう。

センターの運用をＦＭ業者に委ねた結果，センターの運用に自社社員が当たる必

要性が少なくなり，センターで総括的な業務を行う程度となる。とくに，システムの監視を本社等管理センターで集中的に行うため，このセンターでの管理要員は専門職である必要はなく，Uターン希望者等を配置することも可能になるだろう。

さらに，大都市近郊では，その個人向け情報処理需要の多さからＦＭ業者が独立し，情報処理サービス業とタイアップし，個人向け情報処理サービスを展開するケースも見られるであろう。

このような背景下でＦＭサービスは，従来のコンピュータシステム総合運営管理サービスに，コンピュータ用設備の設計，施工，運用といったサービス，さらにコンピュータセンター全体の運用管理までサービスするようになる。とくに安全管理サービスとして，自社でデータ保管倉庫，バックアップセンターを設け，総合的な安全管理サービスを行う業者も出現してくるだろう。つまり，情報処理システムは，ほぼＦＭ業者により運用されているといっても過言でない状況になってくる。センター，コンピュータシステムの資産的な管理主体は，地方公共団体，企業等であるが，運用上は，ＦＭ業者が管理主体になる。ただし，プログラム，データ等のソフトウェア資産，セキュリティの観点から，運用上も管理上も地方公共団体，企業等が直接的にコントロールすることになる。

また，この頃になると，システム設計サービスを行う能力を有し，システム導入に当たって，業務分析，諸企画，計画，システム決定，導入といったサービスを業務に加えるべく試行する業者も現れ始めることになるだろう。

① ＦＭサービスの内容は次の通りである。

- 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

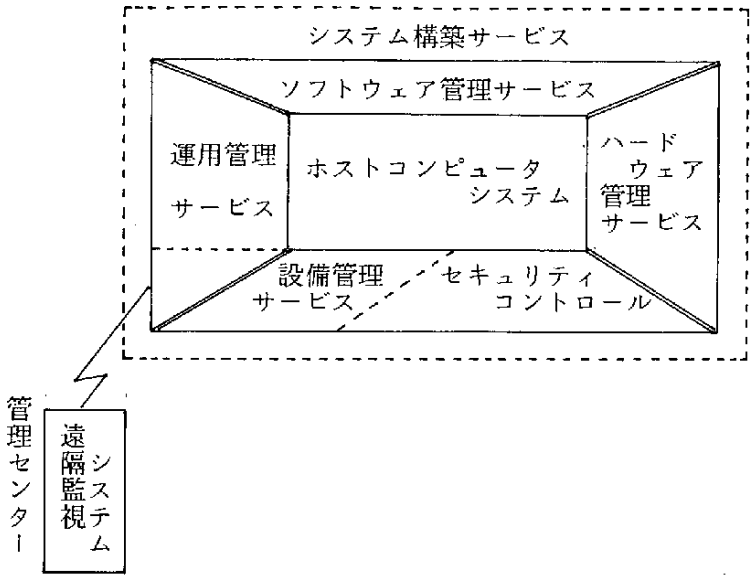


図 5.　FMサービスの概要

② FMサービスの対象は次の通りである。

① VANセンター ……┬ホストセンター ┐
　　　　　　　　　　└サブセンター　┘…FMサービス
　　　　　　　　　　└アクセスポイント …FM巡回サービス

② 一般ホストセンター … FMサービス

③ 個別コンピュータシステム … 補助的なFMサービス
（機密性の高いシステム）

(2) ホストコンピュータ総合運営管理サービス

システム運用については，管理センターの遠隔監視システムからの指示（例えばジョブスケジュール投入等）に基づき，自動起動，無人運転されているため，コンピュータセンターでは，基本的には次の事項を行う。

○運転／実行状況の監視／管理

○遠隔監視システムからの指示に基づく緊急対応

○遠隔監視システムからの指示に基づくCMT等の回収／着装等の操作

しかし，客先の規模によっては，管理センターの運営管理サービスも行い，システム運転管理（ジョブスケジュールの投入，自動起動指示等）のように，本来シス

テム利用者側で行う業務まで代行することもある。

(3) ソフトウェア保守管理

ソフトウェアの保守は，本来利用者側が管理センターの許可のもとに実行するが，これも利用者側からの依頼に基づき，ユーザソフトウェアばかりではなくＯＳレベルまでの保守管理を行う。このサービスは，単なるソフトウェアの保守といった作業ばかりでなく，システム設計書作成からプログラム変更まで，各種のレベルをサービスする業者も出現しているであろう。

(4) ハードウェア保守管理

ハードウェアの保守は，メーカ保守会社，第三者保守会社等が行うが，範囲はコンピュータばかりでなく通信回線をも含むハードウェア全般の保守管理を行う。基本的には次の通りである。

○定期保守管理

○管理センターからの指示に基づく障害保守管理

○保守作業管理

○日常点検，清掃

さらにサービス内容に，一次保守およびメーカ保守会社とのタイアップにより，自らサードパーティとなり保守サービスまで行う業者も出現するであろう。

(5) 設備運用管理・安全管理

設備運用管理・安全管理とは，ホストコンピュータの稼動にかかる諸設備（電源・空調等）の運転と，センター運用にかかわる一般の諸設備の運転と，それらの管理およびセンター全般の安全管理を行うものである。

① コンピュータ用設備運転管理

これらの設備は，ホストコンピュータに連動し自動運転されているが，これは単に起動，停止程度であり，運転状況等が遠隔監視システムに通報されているものの，運用自体が本サービスに委ねられており，運転にかかわる諸操作等は，センター側で行われる。基本的には，次のことを行うものである。

○運転状況の管理

○緊急時の対応

○定期保守管理，保守作業管理

○諸操作，日常点検，清掃等

さらに，次の事項を行うこともある。

○一次または二次保守

○設備の増設，更新等の設計，施工等

② センター運用設備運転，管理

ホストコンピュータに直接関係ないセンター全体の，一般的な設備の運用管理についてもサービス内容として含む。基本的には次の通りである。

○設備の運転

○運転状況の管理

○緊急時の各種操作等の対応

○保守，保守管理

○設備の増設，更新等の設計，施工等

○日常点検，清掃等

③ 安全管理

センター運用に関し，次のことを行う。

○入退場管理

○館内外の安全パトロール，侵入防止等の防犯

○火災，水害等の防災の監視

○緊急時の対応

○防犯，防災設備機器の保守管理，修理，増設，移設の設計，施工等

これ以外にもデータ保管倉庫やバックアップセンター等を設け，委託されたセンター運用に関し，さらに高レベルの安全度を提供するサービス業者も出現してくる。

(6) システム構築サービス

主に，システム運転状況のデータを蓄積し，定期的に報告を行うだけでなく，システムキャパシティの分析，グレードアップ等に対するユーザアドバイスを行うサービスを開始する業者も出現する。

また，この頃より徐々にこのサービスが延長され，システム設計，導入といったシステム構築サービスまで業務範囲が広がることが予想される。

4.2 ＦＭ業界の課題

(1) 将来像として，コンピュータシステムの構築から運用にいたるまでのハードウェアに関する全てをカバーすると考えられ，情報化社会のインフラストラクチャとしてその資質が重要となる。したがって，安全対策に関しより厳格に自らを律し，さらに守秘義務等運用について，より高いレベルの安全に関する動機づけが望まれるだろう。

(2) センター運用の中心ともなるものであり，その人的資質の高さが要求される。

したがって，これらの人の育成に関し，専門的な教育と共に，高いモラル教育が望まれる。

(3) 個人向け情報処理サービスは，対象が個人であり，そのサービスの継続性（連続性）は重要な要因である。したがって，これに要する設備，保守機材等に関し，その充実が急務となろう。

5. 防犯・防災

5.1 防　　犯

(1) 社会環境に変化を与える要素

2010年の防犯に関し，被害および対策の両面で直接・間接に影響を与えると思われる要素をあげてみると次のようなことがある。

① 人口構成の高齢化

1980年の総人口に占める65才以上の老年人口割合は10.3％であったが，今後，増加基調で推移し，2010年には20％前後になるといわれている。これに伴い，生産年齢（15才～64才）は，現在の老人１人当り 6.6 人から，2010年には３人前後に減少するものと予測されている。このような傾向は，世帯構成の変化をもたらすことになる。

② 単身世帯の増加・世帯人数の減少

晩婚化・未婚率の増加・離婚率の増加・高齢単身世帯の増加により，都市部を中心に単身世帯の増加が考えられる。また，出生率の低下，子育てが終った老人夫婦のみ世帯の増加も予想される。すなわち，今後とも世帯人数の減少傾向が続くことになる。

③　余暇時間の増大

就労時間の短縮，価値観の変化により，余暇時間が増大し，趣味，学習，教育，文化，レジャー，コミュニティ活動等多種多様な活動，行為が生活の中に組み込まれてくる。これらは，住環境の個性化およびリゾート指向へと結びついていく。

④　女性の社会進出

女性就業率は年々増加しており，女性の社会進出も増大していくものと考えられる。したがって，共働きがますます増加し，そのような家庭における子供の生活のあり方がクローズアップされてくる。

⑤　国際化

国際化による国際交流の増加，慢性的肉体労働者の不足による開発途上国からの労働者の流入等，在日外国人が年々増加しており，今後も加速度的に増大していくものと考えられる。これらの受入体制について，制度面および異文化交流面から，国としての対応が求められるようになる。

⑥　エレクトロニクスの高度化

マイクロエレクトロニクス，マイクロコンピュータの高度化が進み，ますます小型化，高性能化するものと考えられる。したがって，その応用範囲は各分野へ広がっていき，社会あるいは労働者へ与えるインパクトが問題視されてくる。

⑦　情報化の進展

コンピュータ，通信機器の発達は情報化の進展を促進し，かつ1985年の通信自由化により急速に加速されており，インテリジェントビル・インテリジェントシティ・インテリジェントハウスといったことが騒がれてきている。このようなインテリジェント化が社会の各分野で進んでいくと考えられる。

(2)　2010年における環境条件

以上述べてきたように，2010年の社会環境は，今日とはかなり変化していることが予測される。このような中におけるセキュリティ機能の高度化・システム化が求められるようになると思われる。

①　防犯監視の必要性

老人世帯の増加は社会的弱者の増加であり，犯罪対象になり易い。また，単身滞在の増加は結果的に不在住宅の増加とも結びつき，かつ，隣組意識の欠如によ

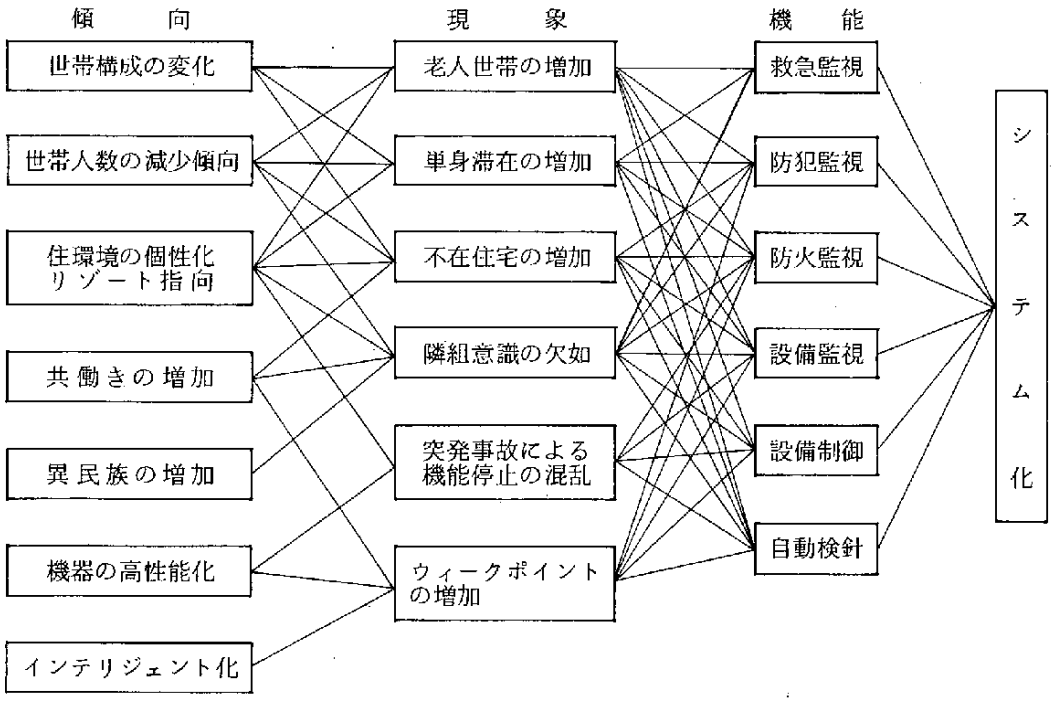


図6.　2010年の社会とセキュリティ機能

る無関心化から，侵入犯の増加を招く恐れがある。全体的には，個人所得の伸びにより裕福な生活者の増加となろうが，一方では貧困者の存在はなくならず，犯罪の増加に結びつくことになると思われる。また機器の高機能化，インテリジェント化等は，それらを悪用するコンピュータ犯罪，その他の知能犯を増加させる可能性がある。このことは個人生活だけでなく，社会全体の問題である。

② システムの必需性

防犯監視の必要性は上記の通りであるが，老人世帯の増加，単身滞在の増加は緊急監視の必要性を産み，快適生活環境条件が求められることから，設備監視，設備制御も必要となる。機器の高機能化はこれらの監視，制御のみならず，自動検針をも可能としているが，予防的なセキュリティと発生した事象に対応する体制，突発事故等に対するバックアップできる体制等が必要であり，トータル化されたシステム化が必要となってくるであろう。

5.2 防　災

(1) 社会環境の変化に対応する防災

現在の日本の防災は，消防法に基づいて自動火災報知設備や自動消火設備が設置されている。その対象物件はテナントビル，劇場，ホテル，旅館，工場等のように，一般住宅でない比較的規模の大きい建物を対象として設備されている。これらの防火対策はあくまでも個々の建物ごとの防災であり，町全体，都市全体のシステム化された防災対策ではない。

高度情報化社会における災害は，万一，現在の東京に関東大震災と同等の地震が起きた場合，大きな損害となるだろうと予想される。また，その及ぼす影響は株式の売買停止，為替の停止等から日本経済全体に及び，果ては世界経済にまで及ぶ事になろう。

2010年を想定した時，防災対策の重要性は今や経済大国日本として必須の条件であり，高度情報化の推進とともに万全の対策が実行されなければならない。

(2) 防災体制

防災には，地震，火災，水害，人災等種々の災害が含まれるが，大きく分けて日常生活における災害と，天変地異による大災害とに分けられる。

① 日常の防災

(イ) 火災報知設備

現在センサーの誤報が大きな問題となっているが，火災の条件がセンサーがマイコンで判断する高度なセンサーが開発されるだろう。この開発が完成すれば，消火装置と連動して初期消火が可能になる。もちろん大きな建物だけでなく，一般家庭向けの商品も開発される。

(ロ) 消火装置

火報と連動することで，更に需要は増大する。その種類も，水，強化液，ハロンガス，粉末を火災の種類によって使い分けられる設備となろう。

また，スプリンクラーのような配管方式は，水害の方が大きくなるケースもあるし，工事費が高くなるので，ロボット方式の配管なしの消火システムに変っていくだろう。

(ハ) 通報システム

一般家庭のホームオートメーションの中で初期消火は行われるものとしても，

消火できない場合があるので，消防機関への通報として，民間警備会社への即時通報システムが普及する。

またビルの大半は，夜間無人となるため，火災時の自動通報システムは義務付けられることになる。

(ニ) 救急システム

医療機関と官民一体のシステムが構築され，応急処置 ― 患者の輸送 ― 本格的な医療がシステマティックに行われるようになる。

② 天変地異に対する防災

(イ) 東京をいくつかのゾーンに分割し，各々に地下コントロールセンターを設置し，災害時には各ゾーンごとにヘリにより，災害状況を無線でセンターに送信し，センターからは災害用無線でゾーン内の都民に避難指示，その他の情報を流す。

ゾーン内には数ケ所の地下避難カプセルを設置し，その中に避難する食糧，水，生活に最小限必要な物資は備えておく。

(ロ) 各ゾーンごとを結んだ中央センターを公的機関の地下に設け，国としての情報，救援活動の指示等を流すとともに，災害後の復旧活動のセンター機関とする。

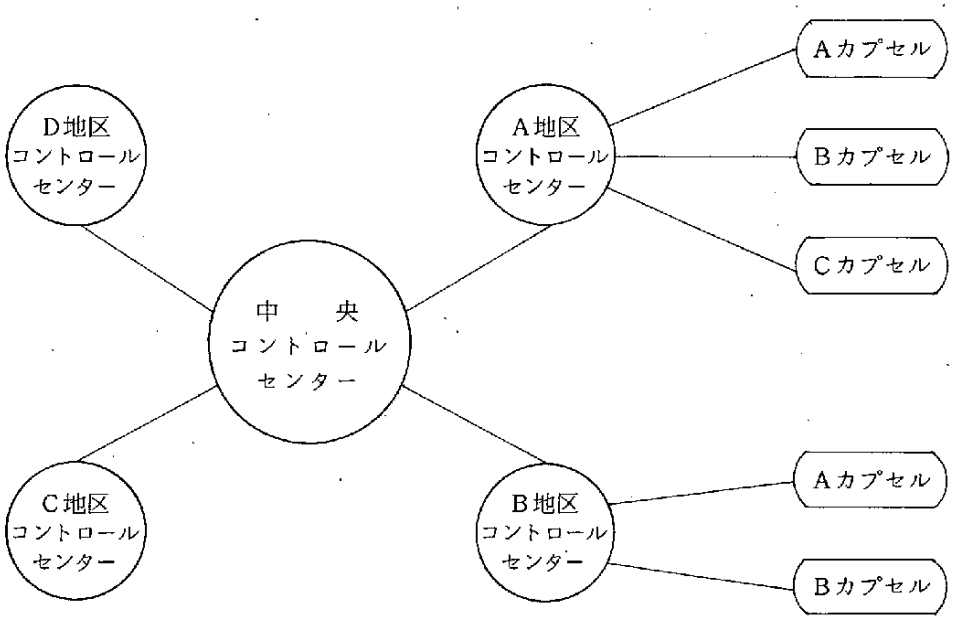


図 7.　センター構成図

「ライフスプリング計画II」

：生活の情報化とセキュリティシステム

はじめに

今日、我が国は戦後のめざましい経済発展により、社会状況は大きく変貌している。ことに高度情報化の進展にともない文化・科学・政治・経済・社会・生活など、さまざまな分野の情報が、さらに複雑化・多様化するものと思われる。このような情報を効率良く処理するためにＩＳＤＮをはじめ、高度情報ネットワークがインフラストラクチャ(社会基盤)として計画・実施推進されている。2010年においては、システムの知能化・高速化が進み、より生活に密着した快適で利便性の高い情報ネットワークが要請される。

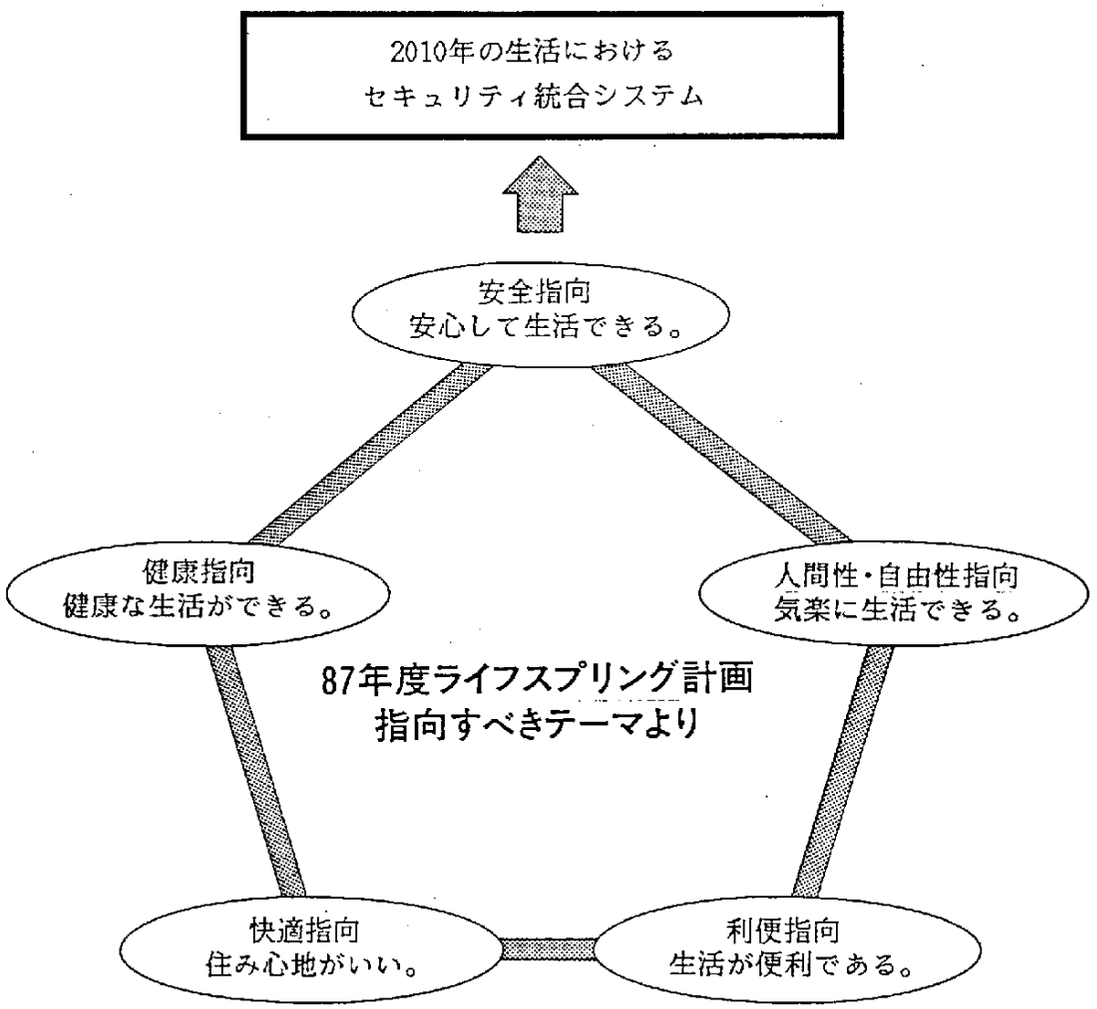
一方、現状における個々の生活環境は、かなり立ち遅れた状況と言わざるを得ない。2010年の生活環境を想定した場合、高齢化や女性の社会進出、ビジネス形態の変容など、社会的な諸事トレンドとともに、<住まい><住まい方>が大きく変化しているであろう。また情報ネットワークにおいても、個々の家庭からネットワークへの情報アクセスが頻繁に行われていると思われる。

2010年の生活環境は、各居住者のライフスタイルに合わせ、より快適で健全な生活環境の維持のための『セキュリティシステム』が重要視されるに違いない。

今回の提言では、'87年度の“ライフスプリング計画”の基本的な考え方、仕組みなどを踏襲し、2010年の生活を想定することにより“ライフスプリング計画II”として展開をはかる。

これにより、将来迎えるであろうセキュリティの時代に対し、より効率良く生活に密着した『セキュリティ統合システム』を掘り下げることができると考える。

'88年度ライフスプリング計画II



■基本的考え方

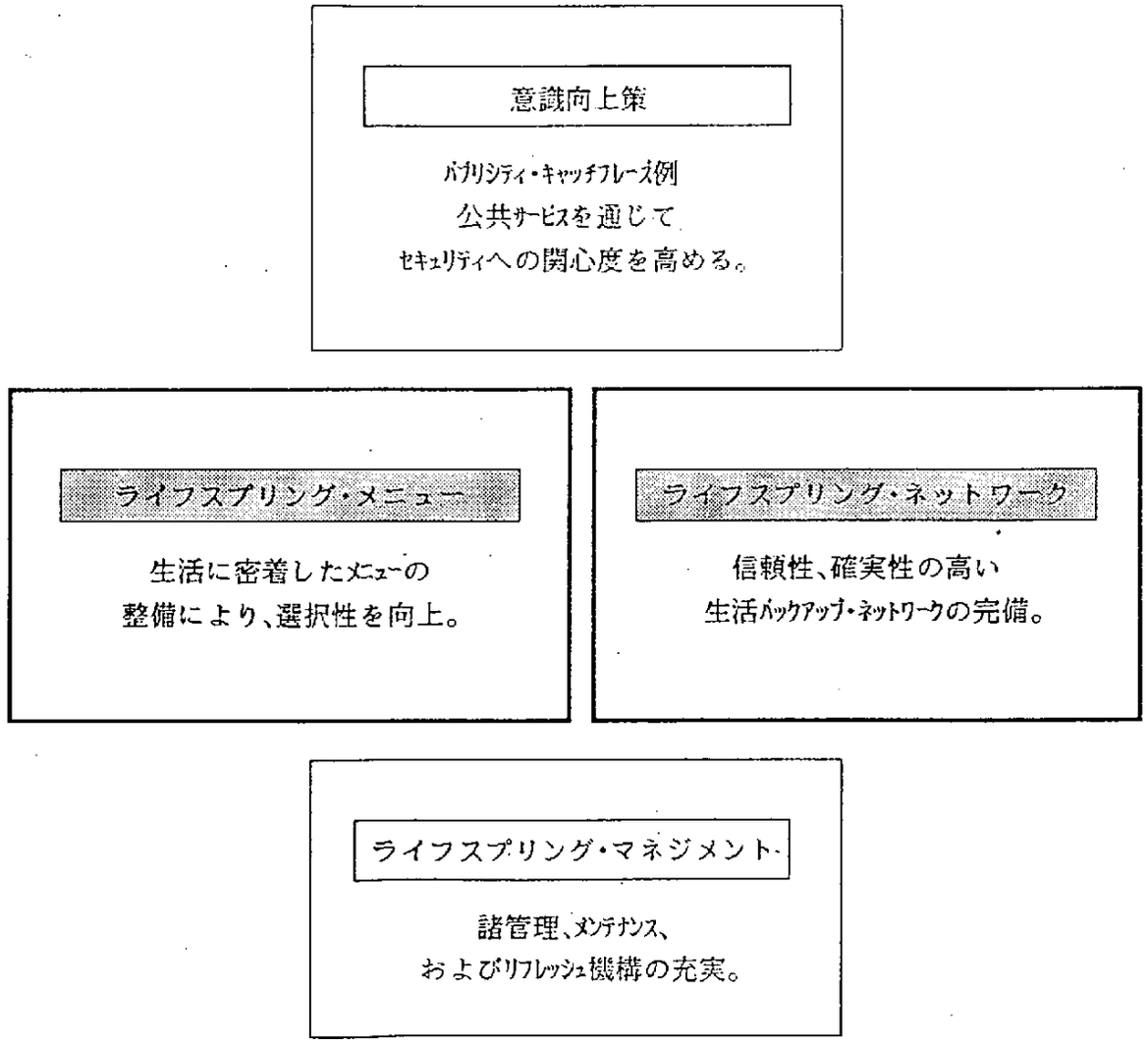
1.生活の情報化を高める。
2.生活のためのセキュリティシステムを構築する。
3.生活関連システムのセキュリティ対策を構築する。
4.現役引退後の生活を豊かにする。
5.情報化の弊害は情報化で克服する。

2010年のセキュリティ意識とテーマ

2010年のライフスタイルを推測すると、家族中心のライフスタイルから、各個人レベルの生活志向を持つパーソナルなライフスタイルへの比重が高まっているであろう。また、国際化がさらに進展してグローバルな意識が高まり、生活環境はより拡大したものとなるであろう。こうした生活環境の変化は、『セキュリティ』への意識が、現在のやや「受動的な意識」から、生活者個人が自分の生活を保護し、積極的に快適性を求める「能動的な意識」への移行を物語るものだといえる。

“ライフスプリング計画II”は、そのような変化に鋭敏に対応するためハードウェア、ソフトウェアの両面から、その在り方の展開をはかる。
また、計画の普及のためには、右図のような居住者のセキュリティ意識の向上、アフターサービス・メンテナンスの在り方および経済性など多くの問題を含んでいる。
ここでは、‘88年度のテーマである『2010年セキュリティ社会』のライフスプリング・メニューとライフスプリング・ネットワークを核にイメージ・コンセプト構築のための基盤を固めていく。

ライフスプリング計画IIのテーマ



2010年の生活環境とセキュリティの方向

2010年の居住スタイルは、現在とは変貌し、今日のような家族との集合的な住み方、これによる一戸建庭付きの大きな家への憧れ、また世襲制の習慣が残った長期居住型の住まいなどに対する指向が薄れていき、<住まい><住まい方>が大きく変革しているものと思われる。

- 自己表現・自己実現への志向
- 快適性への志向
- 健康志向

など、個々の生活への質的なニーズが高まっていると予想できる。

また、社会的傾向として、都市化現象がさらに拡大する。家事の外部化、情報化、ソフト化、24時間化、国際化、高齢化、労働時間の短縮化など、生活環境を大きく変更させる要因が増加する。

右図では、2010年の<住まい><住まい方>を想定したものである。

2010年のセキュリティシステムは、こうしたライフスタイル傾向を前提とし個人生活・家庭生活・社会生活を含んだ各生活環境に対して、

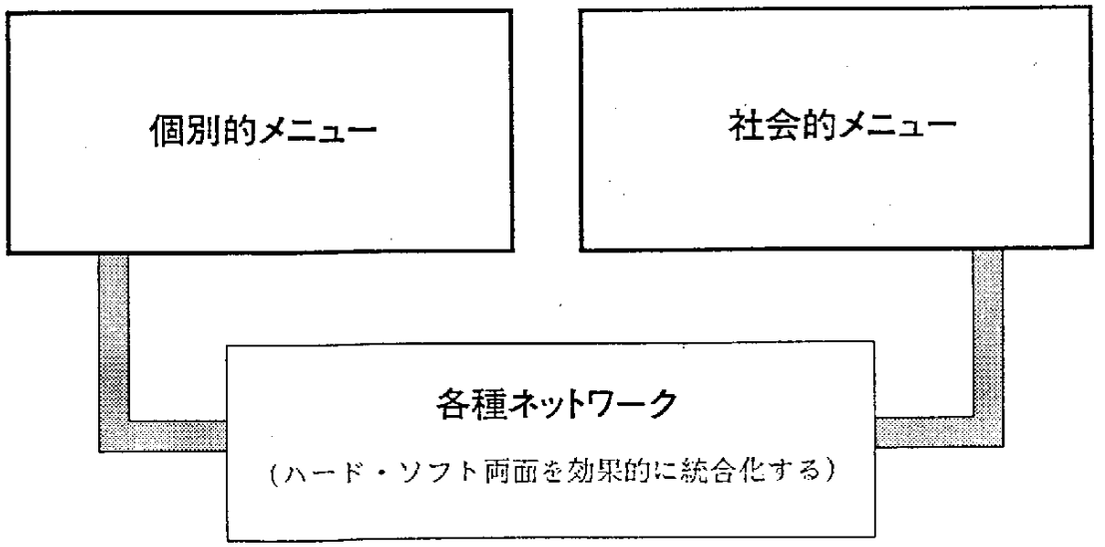
- 個別的な生活に直接影響を与える『セキュリティシステム』
- 社会生活とのインターフェースを持つ『セキュリティシステム』

の両面を掘り下げることにより、よりよい生活のステージを構成、演出するものでなければならない。

2010年の生活環境予測

- 生活の変化(日常的、および居住者の状況別)に対応することのできる住まい
- 複数の家を所有し、労働・生活・余暇の使い分けの実現
- 国際化の推進による24時間リアルタイムで情報交換のできる住まい方
- さらに密着した、医療およびセキュリティのシステム
- 充実した周辺施設の高度利用によるシンプルな住まい
- 個性を重視した、ハイクオリティな住まい

多様化、高品質化する生活ニーズに対応して、
よりよい生活環境の創出をバックアップする『セキュリティシステム』とする。

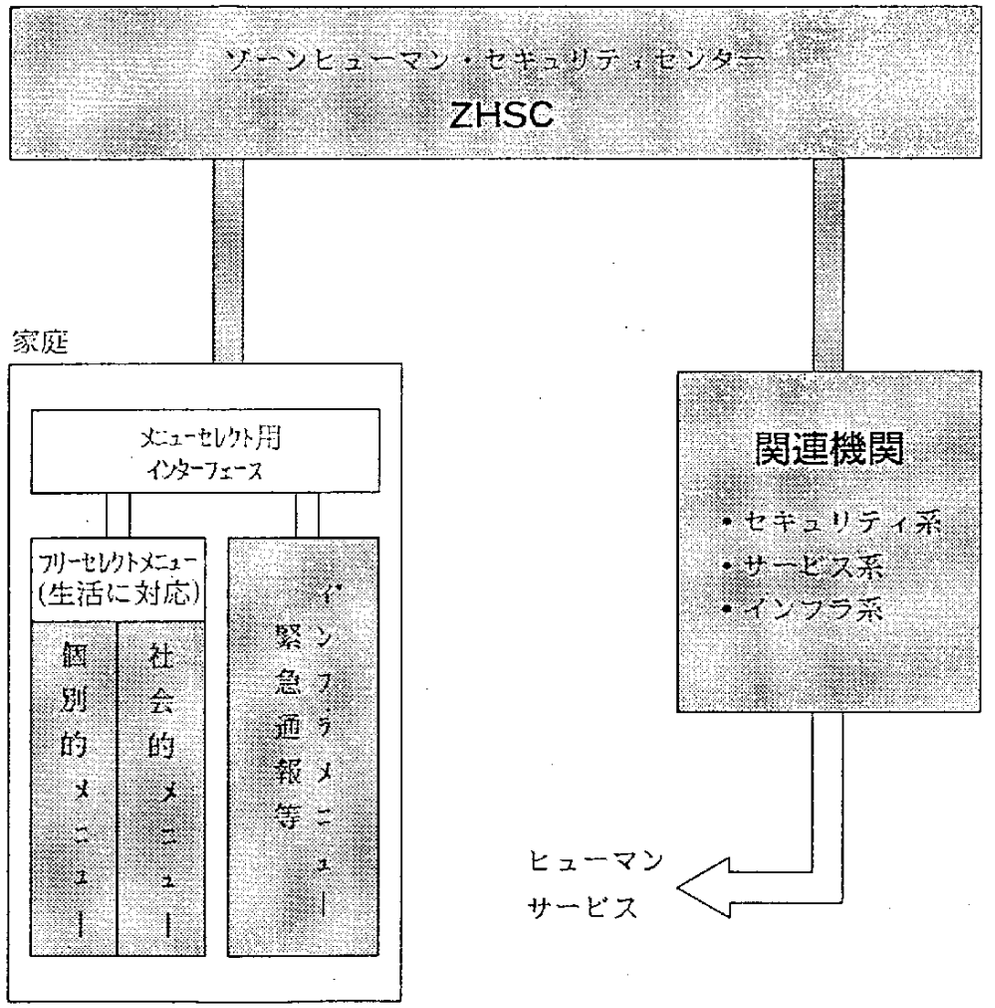


ライフスプリング ネットワーク概念

ライフスプリング・ネットワークは、生活環境の変化に対し、柔軟で発展的に対応できる拡張性と互換性のあるものとする。
また、各生活者にとって最適のシステムが自由に選択できるメニューセレクト方式を確立していなければならない。
トータルなシステムとしては、'87年に提言したゾーンヒューマン・セキュリティセンター(ZHSC)のように、居住区単位に分割したネットワークの整備が必要となる。

右図は、その一単位を表現したものである。個々のセキュリティシステムの充実だけではなく、居住区の活性化と高度情報化および各種ネットワークによる知的生産価値の創造を、バックアップするシステムが完備されていなければならない。

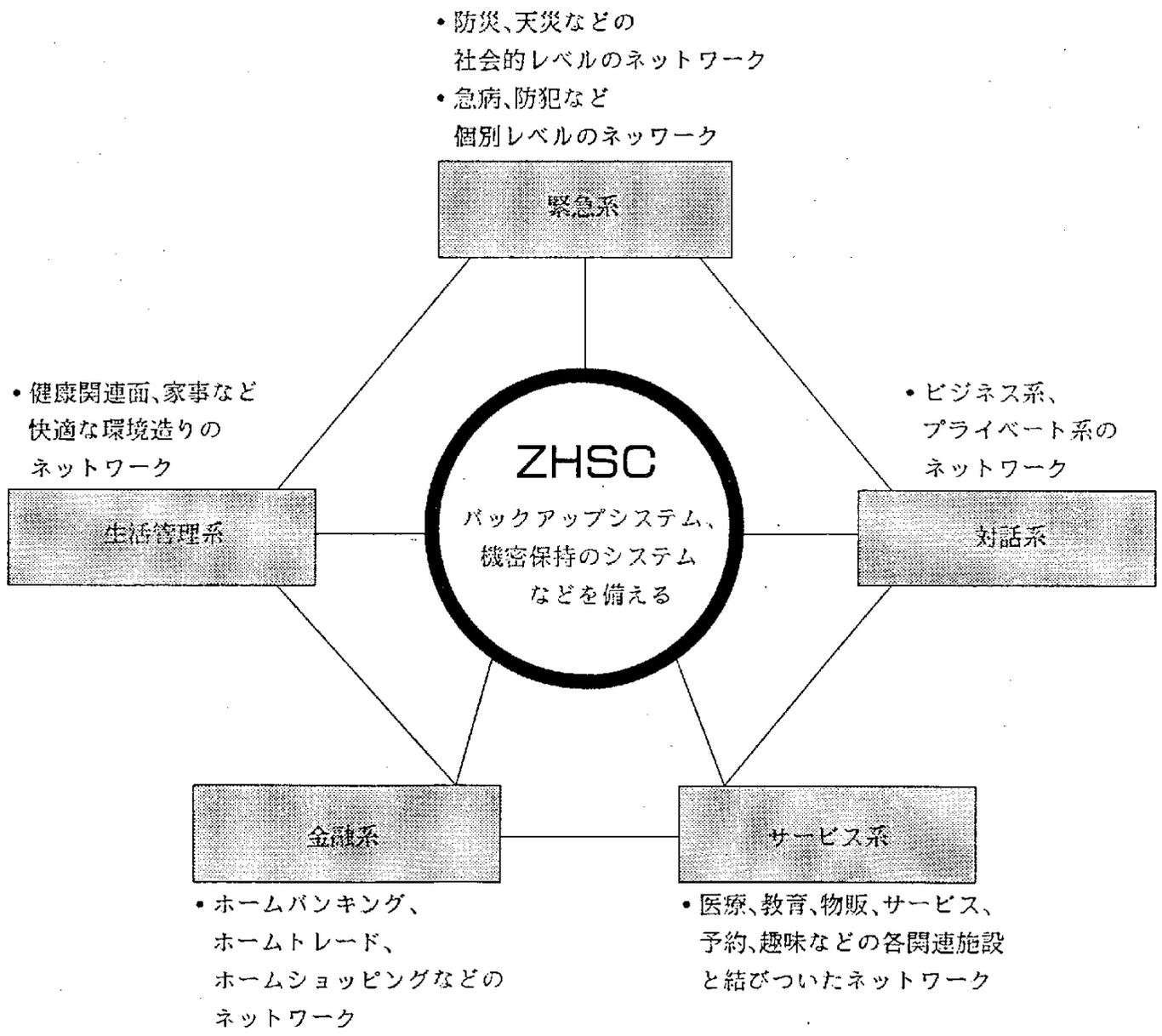
ライフスプリング・ネットワーク



・インフラメニューは、居住ゾーンの機能により異なるが常設型メニューである。

ライフスプリング ネットワーク機能

2010年には、快適で健全な生活環境の維持のために『セキュリティシステムのネットワーク』が、あたかも人間の静動脈のごとく居住区に張り巡らされていよう。従って、そうしたネットワークでは、より緻密で統合性の高いものが要求されることとなろう。
ここでは、設定したメニューを5ネットワークに分類し、評価を試みた。ハッカーなどからの防御、プライバシーの保護といった分野と情報提供の分野など各種情報の区分を明確にしたシステムが、要求されてくるだろう。また、『セキュリティシステム』が生活に密着すればするほど、システムの維持をするためのバックアップの在り方が、必須なものとなろう。
『ライフスプリング・ネットワーク』では、インフラストラクチャーとしての情報路においては、より信頼性・統合性の高いネットワークを構築するため、右図のように、系統別なポジショニングを行い、ＺＨＳＣに統合的・中心的な機能を持たせることとした。



ライフスプリング メニュー

ここでは、5つのコンセプトメニューに従ったメニュー例を掲げる。さまざまなネットワーク化が進展した2010年には、セキュリティの内容も拡大しているであろう。
セキュリティの本来的な意味での財産や人命の保護といった機能に加え、人間にとり健康・快適性のバックアップのシステムを考え、柔軟な対応をはからねばならない。

機能内容	メニュー例(内容)	緊急系	生活管理系	対話系	金融系	サービス系
■安全指向メニュー 日常生活を安心して送ることができるよう、個人レベルからさまざまな集団・組織に至るまで、システムごとの連係を考慮した上でバックアップする。	• 統合監視通報システム……防犯・防災・天災など、緊急・有事の際の通報から対処、避難指示・誘導。	○				
	• 広域セキュリティ・システム……センター(町・市)ごとのセキュリティ防災情報サービスの提供、管理(病院・気象・災害等)。	○				
	• ヒューマンスクランブル・システム……外出時の急病・誘拐・迷子の発生の際、居場所のモニターおよび適切な対応。	○				
	• プライバシー保護システム……家庭・個人情報に関するプライバシーの保護。	○	○	○	○	○
■健康指向メニュー 人間生活の根底にあり、すべての活動を底辺から支えるのが、身体である。その人それぞれの個性を捉えたうえでの健康管理が必要である。最適なアドバイスと管理を行う。	• 健康チェック(ホームドクター)システム・各個人の健康度をチェック、カルテ管理および通告。		○			
	• ヘルシー・システム……老化防止、健康増進、高度情報化社会におけるテクノストレス解消などの諸システム。		○			○
	• 運動能力向上システム……オフィス機能の向上に起因する運動能力の低下防止および向上。		○			○
	• 衛生管理システム……ダニ・ユキノなど健康を害する病原菌からの保護。		○			○
■快適指向メニュー 一日のルーティーン・ワークを効率化することで、その一日の気分までが向上する。無駄を省き、快適な日常を獲得するための、パーソナルそしてパブリックなシステムといえる。	• 生活環境セキュリティ・システム…水・空気・光・電波など家庭生活に必要不可欠な要因の管理、保護。		○			○
	• ホームキーピング・システム……家庭内の電気設備・機器のセルフクリニックによる故障・誤動作に関する警報セフティ。	○	○			○
	• 快適環境システム……温湿度・気圧・空気など、エアーコントロールによる快適性の向上。		○			○
	• 24Hオンライン・システム……エレクトロニクスへの依存度の高い家庭センター間の回線の監視と停止時のバックアップ。	○				○
	• グリーンアメニティ・システム……地域環境に応じた自然保護運動の実現。		○			
■利便指向メニュー 金融機関との折衝、パソコン通信による情報交換など。決していいかげんには処理できない業務を効率化することにより、自己の知的生産性の向上を支援する。	• 情報サービスセキュリティ・システム…ホームバンキング、ホームマネージメントなど、各種システムのバックアップ。				○	
	• ホームコンピュータ・システム……センター、ホーム間での情報交流(教養・一般情報)による知的生産性の向上。			○		○
	• コンフェレンス・システム……公共および民間の案内サービス(税金・財テク情報等)。			○		○
	• リテイベーション・システム……商品のオーダーからメンテナンス、アフターサービスに至る総合サービス。					○
■人間性・自由性指向メニュー 時代とともにアメニティの形態も変貌する。公共および民間設備の効果的な活用により、個性を豊かにするシステムが整備される。	• オープンスペースサプライ・システム……公共スペース、イベントスペースの情報提供とセレモニー、イベントのサポート。			○		
	• カウンセリングサービス・システム……人間関係の希薄化の防止(フェイス・トゥ・フェイスで実施される各種相談サービス)。					○
	• 生きがい追求システム……高齢者を対象とした社会参加の場の情報提供および支援。			○		

ライフスプリング計画 II

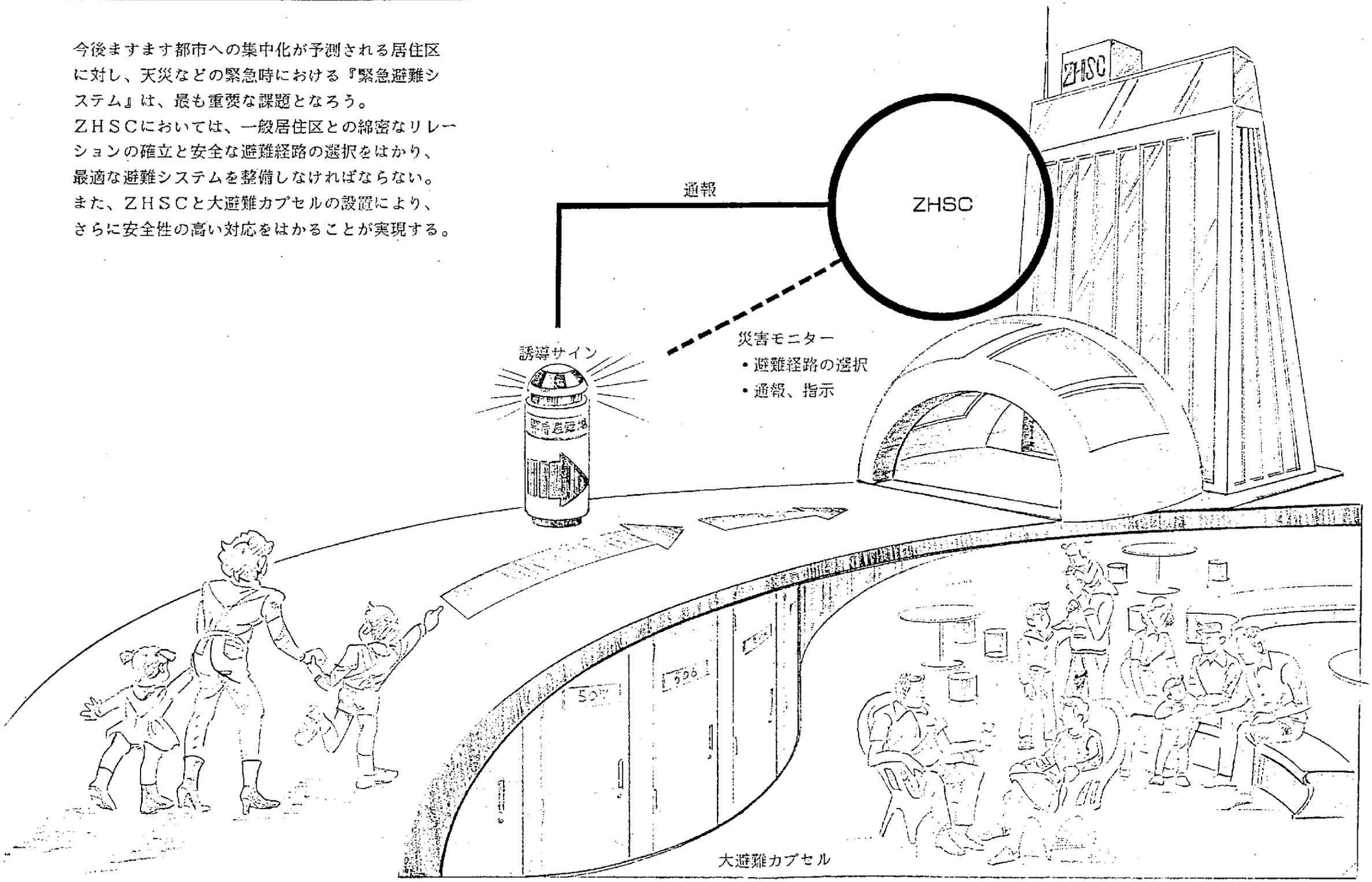
2010年 ライフステージ例

これまで、“ライフスプリング計画II”のシステム構築として、ネットワークおよびメニューの展開をはかってきたが、計画を実施に移す段階において、それらの整合性・妥当性を評価、確認する必要があろう。
ここでは、2010年の生活ステージを想定することにより機能性を評価する。
事例としては、2010年において予想されるライフスタイルと、そのワンシーンを表記してみる。
さらに評価の精度を高めるためには、時間軸、場面軸など、全方位的な指向からの検討が必要であろう。

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→ ツーインカム居住者の生活例

ゾーンステージ→緊急避難システム

今後ますます都市への集中化が予測される居住区に対し、天災などの緊急時における『緊急避難システム』は、最も重要な課題となろう。
ＺＨＳＣにおいては、一般居住区との綿密なリレーションの確立と安全な避難経路の選択をはかり、最適な避難システムを整備しなければならない。
また、ＺＨＳＣと大避難カプセルの設置により、さらに安全性の高い対応をはかることが実現する。



使い分けライフ→夫婦の生活例

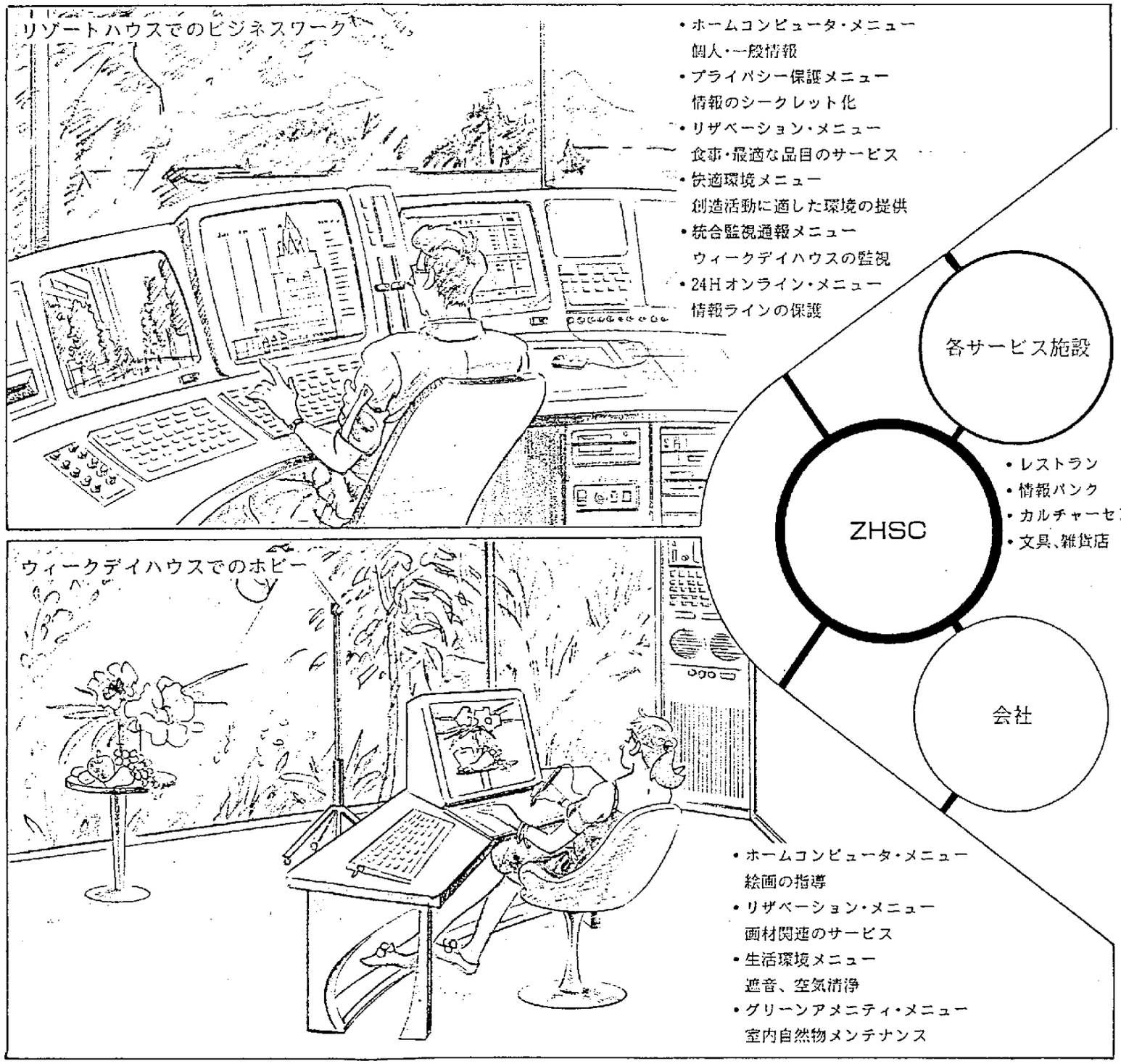
ビジネスステージの都市型ライフとライフステージの郊外型ライフ、創造ワークとハンドワークやホビーワーク、リゾートライフとビジネスライフなど、複数のライフステージを持つ人々が、ライフステージの使い分けにより知的生産性を向上させることができる。
自己に適したライフステージの選択と組み合わせが、多様化した時代の人々の指向を捉える。
今後、このような生活パターンを持つ人々が急速に増えていくであろう。

生活シチュエーション例

夫婦の生活例

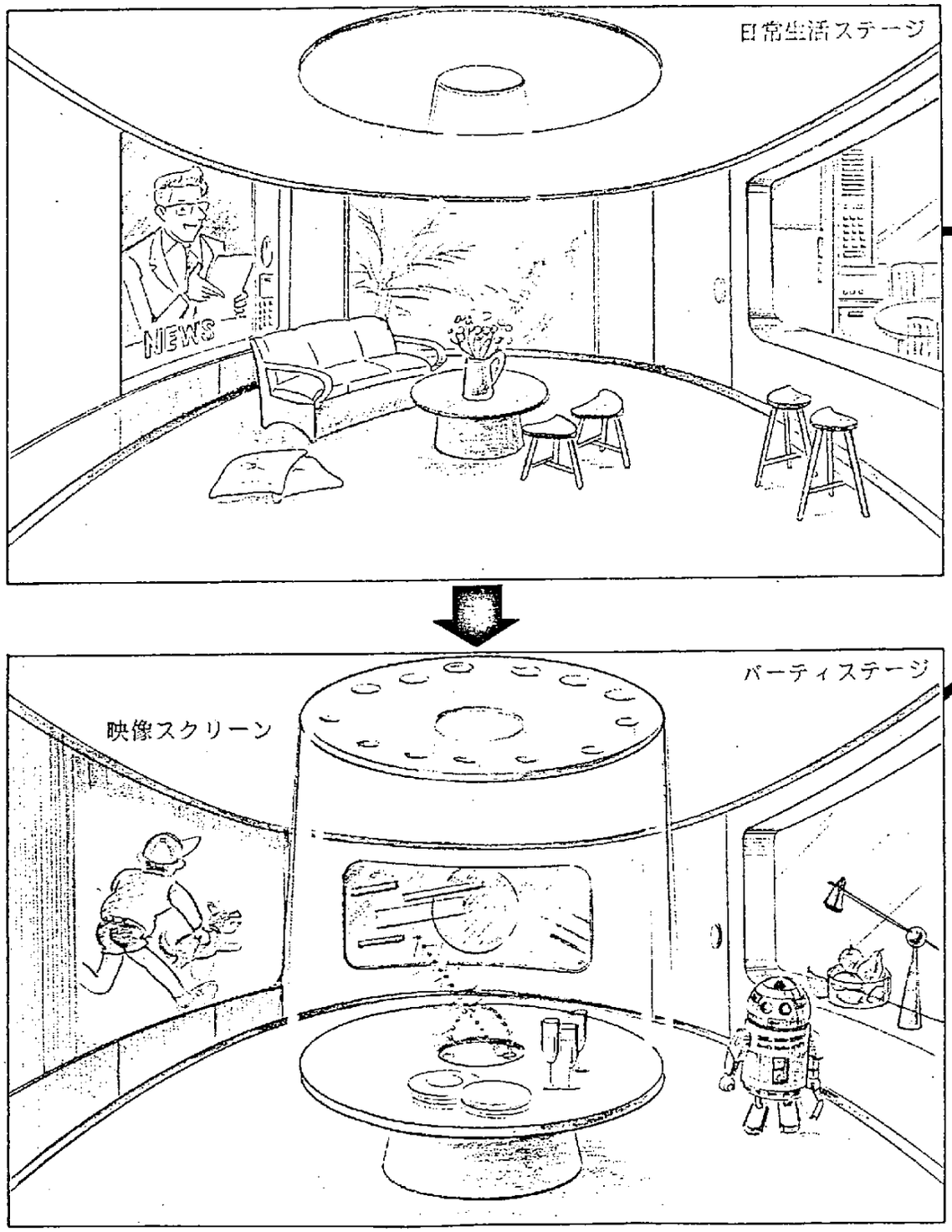
ここでは、それぞれにビジネス、趣味をもつ夫婦のワンシーンを考える。
妻は、趣味である絵画をウィークデイハウスでドローイングコンピュータにより制作中。
夫は、独創的な企画の立案のため、静かな自然に囲まれたリゾートハウスで仕事に取り組んでいる。
お互いの安全とコミュニケーションはＺＨＳＣを通じて管理される。

●セキュリティ指向
ホームコンピュータ化が普及するなか、ネットワーク上での機密保持システムの充実がはかられる。一方、それぞれの活動に最適で快適な環境システムも、セキュリティの一環として発展しているであろう。



フレキシブルライフ→子供ひとりの夫婦の生活例

欧米の習慣が、日本にさまざまな形で浸透している。ディナーやティーパーティなど、友人を自宅に招いて交歓の場を持つ習慣は、現在の我が国においても重要視されている。
そうした接客の際、パーティスペースや寝室など、接客状況の変化に応じてフレキシブルに対応する空間が必要となる。
また、長期間にわたる視野からライフステージを考えた場合、
• 子供の成長に合わせて……
• 自分自身が若いとき、そして老いたとき……
など、生活者の変化に応じて柔軟なステージづくりが行える空間活用が実現する。



ZHSC

各サービス
各関連機関

• パーティショップ
• イベントホール

• 快適環境メニュー
空調、香り、湿度
演出のための諸コントロール
• リザベーション・メニュー
パーティ用準備
• プライバシー保護メニュー
来客者からのシークレット保持
• オープンスペースサプライ・メニュー
大画面モニターによるバック効果
• 総合監視通報メニュー
来客者宅のモニター

生活シチュエーション例

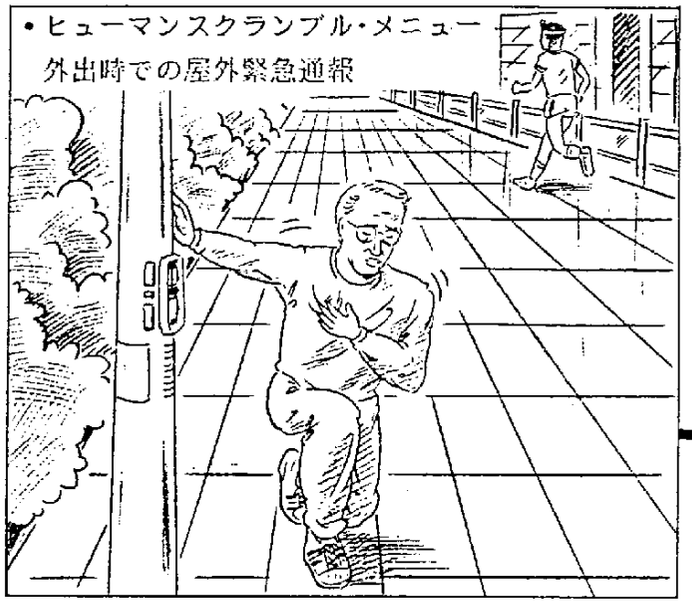
子供ひとりの夫婦の生活例

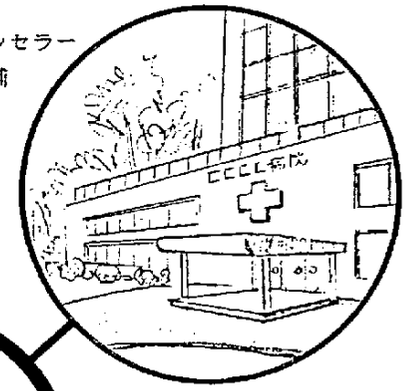
この家族の子供は、ワンパク盛りであり小学4年生(男子)である。
子供を中心とした隣人との付き合いは活発で、ホームパーティはしばしば開催される。
そうしたパーティの際、日常の生活空間からパーティスペースへの転換と演出は、床・壁・天井への家具の収納および配置をはじめとした簡単な操作で行われる。

●セキュリティ指向
電装化が進展する生活においては、電源へのバックアップ・装置の安全なシステムが完備する。またレジャー化、女性の社会進出により、いろいろな場所への移動が増し、移動先から自宅の安全確認、制御、モニタ、通知が自在となる。

セーフティライフ→高齢者の生活例

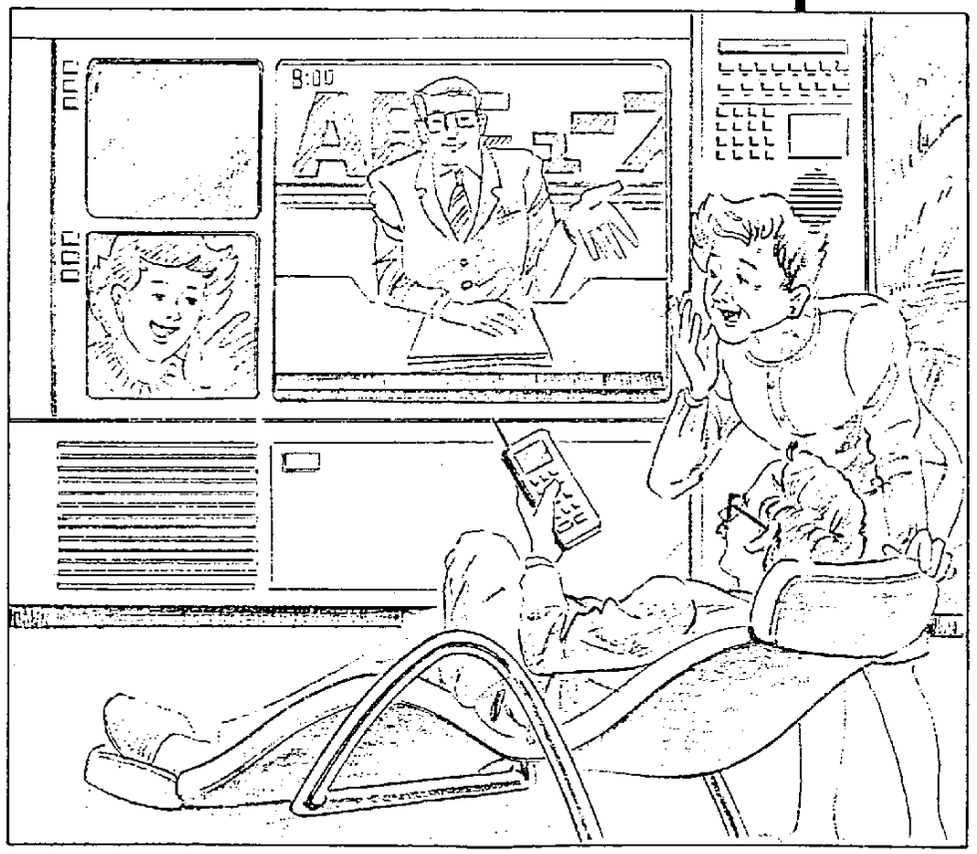
2010年には、日本の総人口は1億3582万人となりピークを迎える。2020年に高齢者は実数で3188万人、つまり4人に1人（23.6%）が65歳以上の高齢社会になると予想される。
このような高齢者、そして女性の社会参加がさらに活発化する。また、シングル生活者が増加する。彼ら(彼女たち)が、社会構造のなかで多くのウェイトを占めることになる。
そうした人々の、より安全な生活環境の保護が重大な社会問題として浮上する。
セキュリティの面からバックアップする必要が生じるのは言うまでもないことである。

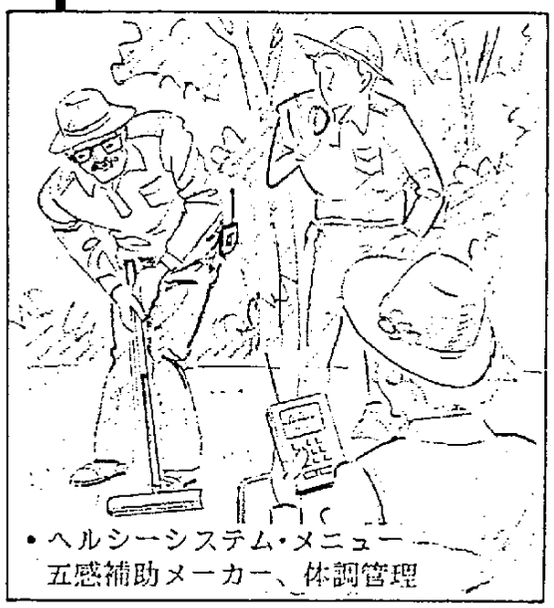




ZHSC

- 健康チェック・メニュー
  カルテ管理
- ヘルシーシステム・メニュー
  花など趣味のフォローと健康管理
- 生活環境セキュリティ・メニュー
  衰えた肉体機能のバックアップ
- リザベーション・メニュー
  生活必需品、食事のサービス
- カウンセリング・サービス
  話し相手の確保
- 生きがい追求メニュー
  社会参加の情報提供





生活シチュエーション例

高齢者の生活例

高齢のため現役を退き、夫婦ふたりの生活を満喫している老夫婦を例にとる。
地域社会で催されるイベントへの参加意欲も高く、自宅ではパソコンによる財テクを行っている。収入は比較的安定している。
また、健康管理へは細心の注意を払っている。
彼らの楽しみは、すこし離れたところに住む娘とのコミュニケーションである。

●セキュリティ指向
高齢による心身の衰え、弱者救済を“セキュリティ”としていかにバックアップできるか、また身体的なトラブルなどの緊急時のシステムを、いかに緻密で周到なものにするかが重視される。

パーソナルライフ→シングル女性の生活例

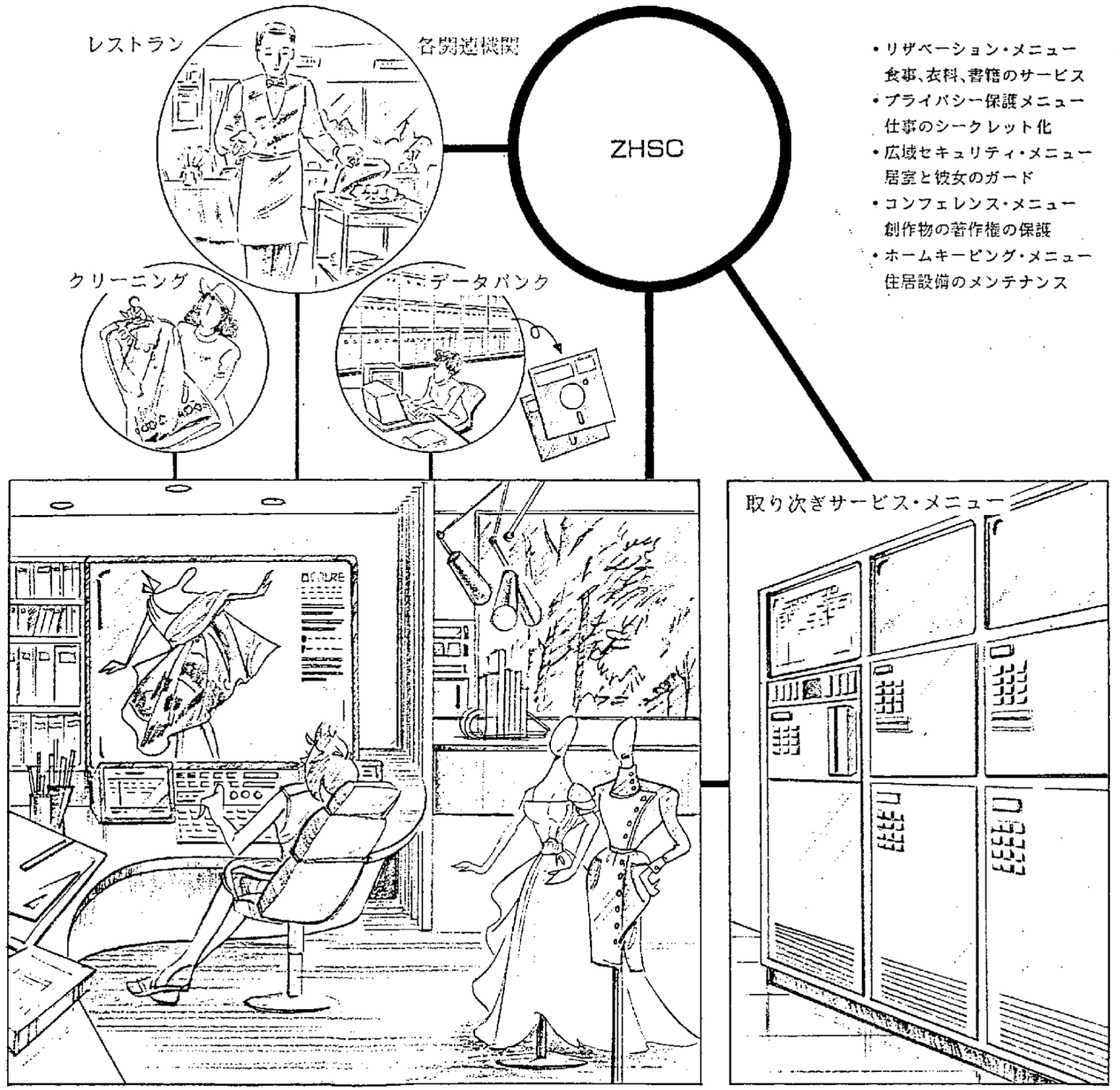
個人の生活を重視する傾向が、2010年にはさらに高まることが予想される。
各生活者に固有の自己実現の夢あるいは要求が育まれ、人々を啓発・教育する機関が整備される。
防犯・防災を始めとしたセキュリティシステムの整備が、個性的に自己を形成したいと願う彼らのシングルライフを支援する。

生活シチュエーション例

シングル女性の生活例

ファッションデザイナーである彼女の勤務形態は、在宅・出勤が半々の状態である。
優雅な暮らしではあるが、食事・クリーニング・郵便物の取り次ぎなど、留守時の防犯には気を配らざるを得ない。
ここでは、週末に提出しなければならない作品の創作活動に、自宅で邁進している場面を考える。

●セキュリティ指向
ビジネス、一般生活上のプライバシーの保護。シングルライフへの支援(防犯、緊急避難、取り次ぎ)など、健全で利便性の高い環境の維持が、セキュリティとして重視される。



- リザベーション・メニュー
  食事、衣料、書籍のサービス
- プライバシー保護メニュー
  仕事のシークレット化
- 広域セキュリティ・メニュー
  居室と彼女のガード
- コンフェレンス・メニュー
  創作物の著作権の保護
- ホームキーピング・メニュー
  住居設備のメンテナンス

コンポーネントライフ→シングル男性の生活例

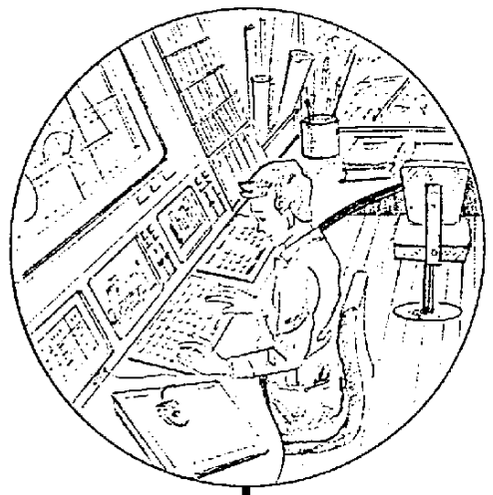
人口の都市への集中は、公共・民間を問わず都市における設備環境の充実を促した。また、地価の高騰そして自己所有することのできるスペースの極小化といった問題を生んだ。
2010年においては、自身の所有するスペースの有効活用の見地から、また購入せずに利用できる設備の向上面から、生活に必要となる住居設備を最小限度にとどめ、業務レベルまたは趣味の範囲で備品の必要性が生じた場合には、その都度そうした設備を活用することで対応する人々が増加するであろう。

生活シチュエーション例

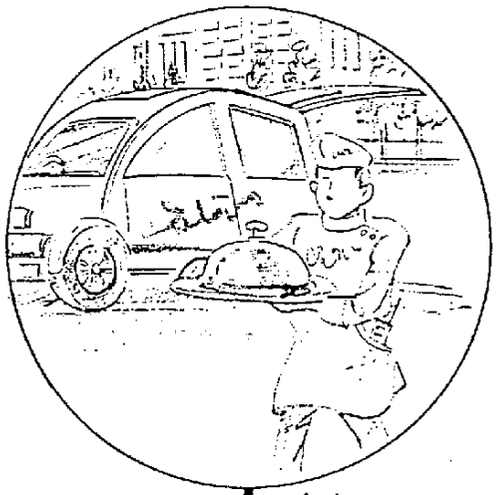
シングル男性の生活例

都心に住みたいと願う彼は、ベッドルームといえる省スペース型のワンルームマンションに居住する。
都心区域においては、さまざまなサービス機関が利用でき、彼は極めて充実した暮らしぶりである。
彼は自分の健康状態に注意を払うため、フィットネスクラブやヨガ教室に定期的に通っている。

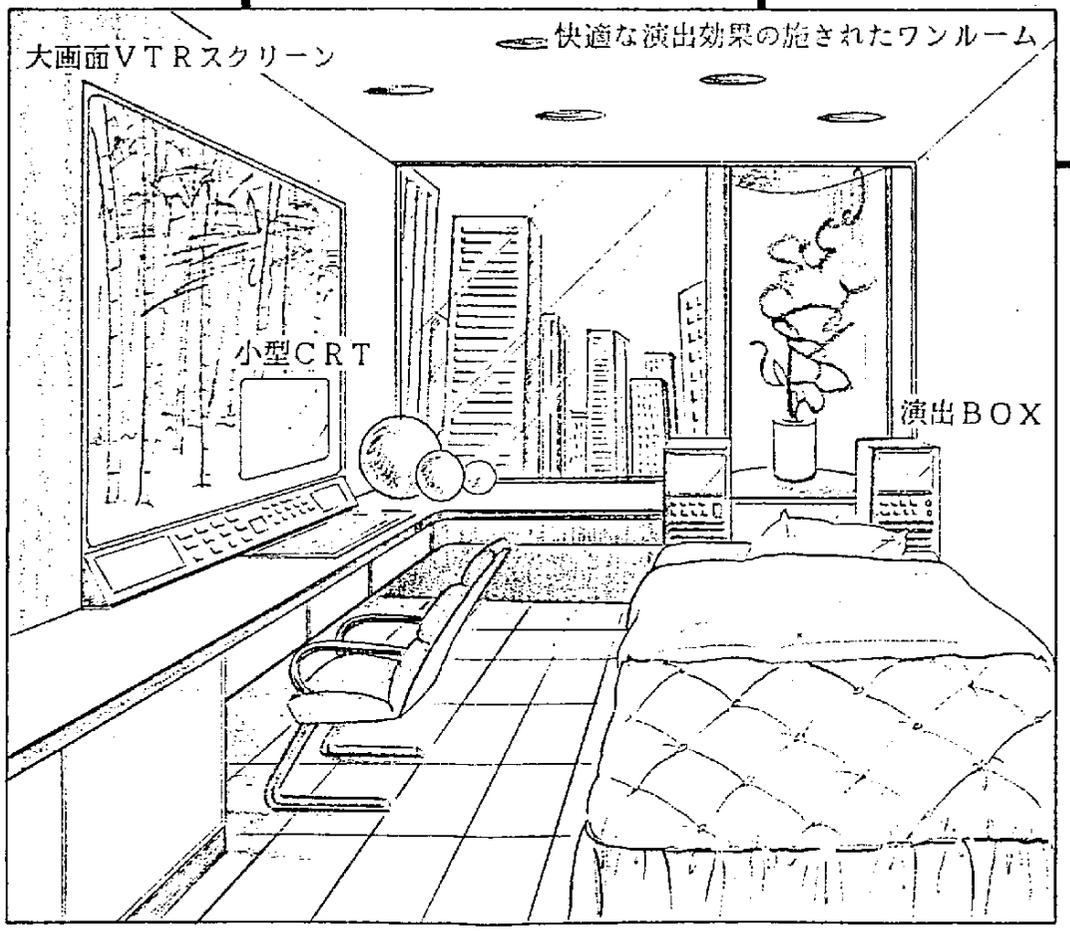
●セキュリティ指向
高度で多様な情報システムを保有する関連施設が居住区に増え、そのバックアップシステムが重視される。また、高密度化した住居においては、安全な避難を含めたセキュリティシステム・健康で快適な室内環境の維持もセキュリティ機能として重視される。


レンタル・オフィス


メンタルケア・クラブ


食事のサービス

ZHSC



- リザベーション・メニュー
  日常生活に関する最寄品のルームサービスなど
- 快適環境メニュー
  空調、香り、映像による環境演出
- 衛生管理メニュー
  ダニ、ゴキブリ等の病原菌からの保護
- 健康チェック・メニュー
  簡易な体調チェックとカルテ管理

グローバルライフ→ツーインカム居住者の生活例

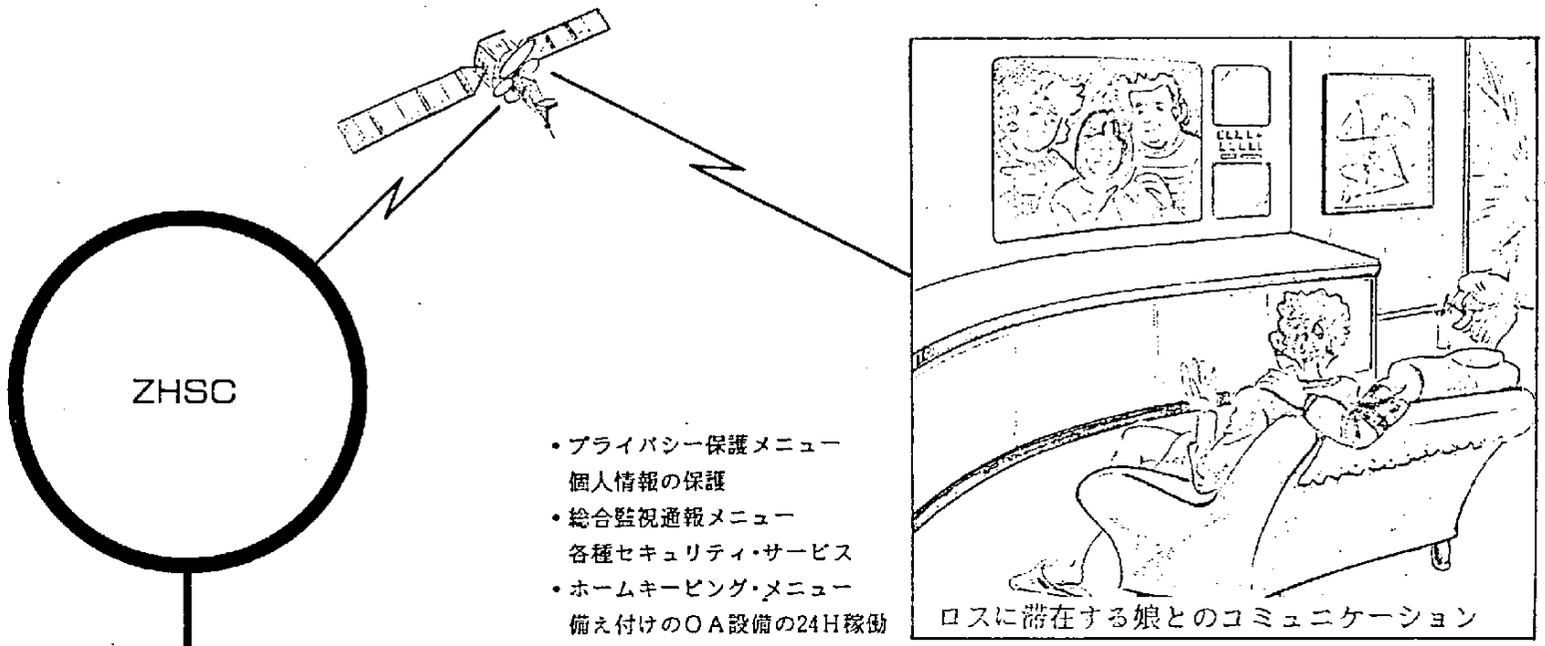
2010年では、個人レベルにおいても、インターナショナルそしてグローバルなコミュニケーションが実現され、さまざまな情報が行き交う生活環境となっていよう。
そこでは、24時間稼働する施設が整備し、情報の送受信がリアルタイムで行える。また、ビジネスのみならず、財テクや趣味にもパソコン通信などが活発化し、その精度が問われるであろう。
従って、リアルタイムでの情報交換が大きな価値を生むことになり、その維持がセキュリティとして重要な課題となろう。

生活シチュエーション例

ツーインカム居住者の生活例

娘は、ヨットで知り合ったロスの友人宅にホームステイ中。娘とのコミュニケーションは、ＤＢＳを利用した映像TELにて定期的に行う。
彼は、会社でのビジネスの他に趣味を活かしたマリン・コンサルタント業務を行っている。
婦人は、ファッション・コラムニストで、パリ、ニューヨークなどの情報を直接受信している。
従って、諸設備がリアルタイムで利用できるためのセキュリティシステム、留守時での防犯体制への意識は極めて高い家庭である。

●セキュリティ指向
・24時間リアルタイムの情報活動におけるバックアップシステムが必要とされる。
情報・ノウハウが集積された、自宅に対するセキュリティは、全方位(停止、誤動作、防犯面)なものが望まれる。



あとがき

『2010年の生活』として、多方面からさまざまな展開を試みることができるが、今回はその一部を提出する。
高度情報化の波は、2010年を迎える頃にはさらに大きくなるとともに細分化し、技術・装置・設備は、ますます巨大化、高密度化していく。
現在、安全性を念頭に置いていたにも拘らず、チェルノブイリ原発事故、ジャンボ機の航空事故といった大規模なヒューマンエラーが発生している。情報サービスの多様化、統合化が進展するなかで、何を重んじることが本当にヒューマンであるのかが考えさせられる。セキュリティの在り方として、人間性を重視した環境づくりが、あらためて問われてくる。
“ライフスプリング計画”は、人間を優しく包みこむ『セキュリティ』という視点から、人間の快適性と安全性を追求していくプロジェクトである。そして、セキュリティ本来の意味を問い続けるとともに、発展させていく人間的で機能的なシステムである。

平成元年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 03（432）9387

印刷所　株式会社 東京矢野企画
東京都港区芝大門2丁目1番18号
GSハイム 209
TEL（459）0831（代表）