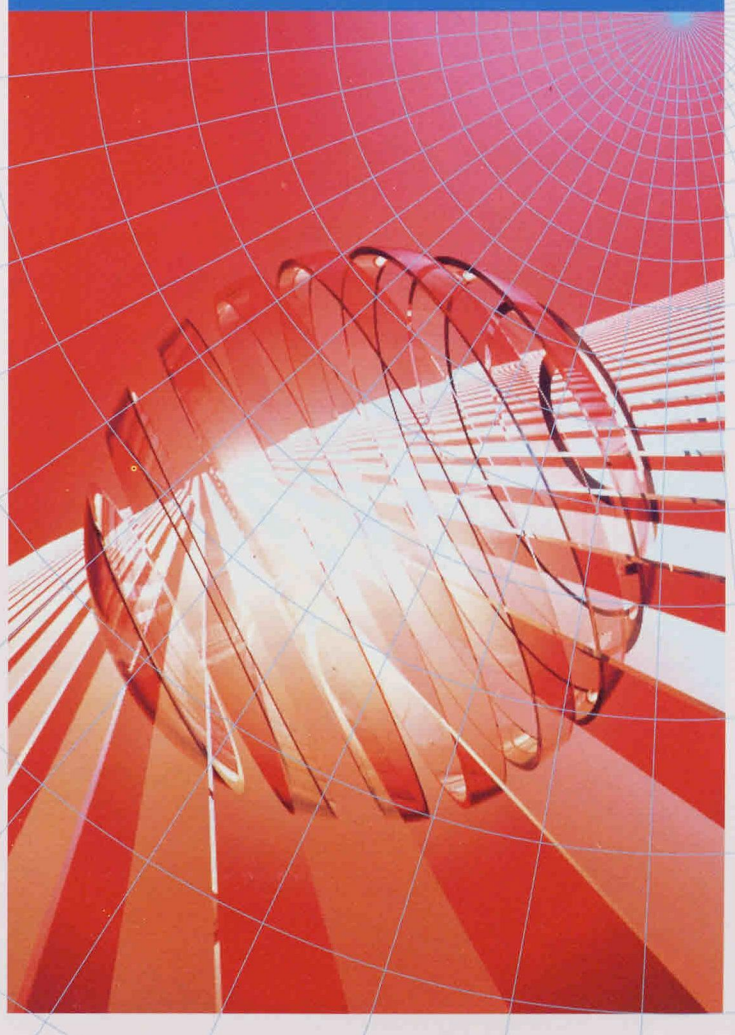
JIPDEC ジャーナル



●JIPDEC REPORT

平成9年度情報化月間

ネットワーク社会の進展とセキュリティ

高度情報化人材育成標準カリキュラムの改訂について

システム監査白書1997-98年版の概要

ネットワークおよびAI関連の情報技術の研究開発動向

No.95
1997

JIPDEC ジャーナル

No.95 目　次

JIPDEC REPORT

平成9年度情報化月間 …… 1

ネットワーク社会の進展とセキュリティ …… 14

高度情報化人材育成標準カリキュラムの改訂について …… 45
中央情報教育研究所

システム監査白書1997-98年版の概要 …… 48
情報セキュリティ対策室

ネットワークおよびAI関連の情報技術の研究開発動向 …… 56
先端情報技術研究所

JIPDECだより

情報セキュリティ対策室 …… 62

調査部 …… 63

技術企画部 …… 65

中央情報教育研究所 …… 66

情報処理技術者試験センター …… 68

産業情報化推進センター …… 72

STEP推進センター …… 83

先端情報技術研究所 …… 86

お知らせ …… 90

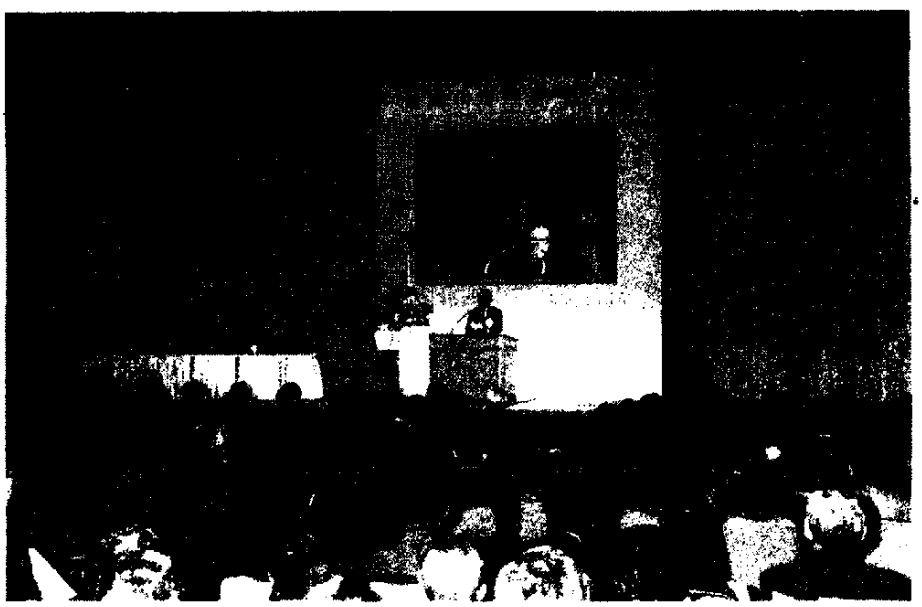
平成9年度情報化月間

情報化月間は，情報化社会の健全な発展を進めていくために，広く国民各層に情報化に対する正しい認識と理解を深めることを目的に関係9省庁（総務庁，経済企画庁，科学技術庁，大蔵省，文部省，通商産業省，運輸省，郵政省および平成6年度から自治省が参加）による政府行事として，毎年10月に行われています。本年度で通算26回目を迎えました。

情報化月間は，昭和47年に10月第1週を「情報化週間」と定め発足しましたが，昭和57年からは，情報化が産業分野から社会・生活分野へ，大都市から地方都市へと面的拡がりを見せ始めたのに伴い，10月を「情報化月間」と改め，各行事の量的増大，質的向上と動員数の増加を図っています。

今年も10月を中心に全国各地で，関係省庁，地方自治体，諸団体等により様々な行事が開催されました。その冒頭を飾る行事として，10月1日（水）に「情報化月間記念式典」が情報化月間推進会議（議長：井川 博・(財)日本情報処理開発協会会長）の主催により，東京全日空ホテルにおいて挙行されました。

記念式典は，井川 博 議長の式辞に始まり，来賓として堀内 光雄 通商産業大臣をはじめ，総務事務次官，運輸，郵政の各政務次官が大臣の代理として列席され，ご挨拶がありまし



式典の模様

た。引き続き情報化の促進に多大の貢献があった個人，企業等の皆さんへの各大臣表彰と優秀情報処理システムへの情報化月間推進会議議長表彰がそれぞれ行われました。

また，「全国高校生・専門学校生プログラミングコンテスト」の入選者に対しても堀内通商産業大臣から表彰が行われ，表彰状と副賞が授与されました。

当日は，同じく東京全日空ホテルにおいて情報化月間を記念し，記念式典特別行事として

①当協会と情報処理振興事業協会の主催により
情報化月間記念国際シンポジウム「ネットワークの進展とセキュリティーネットワーク犯罪とその対応ー」

②情報処理振興事業協会と電子商取引実証推進協議会の主催により
情報化月間記念ECシンポジウム「インターネットが開くEC時代」

③(財)コンピュータ教育開発センターの主催により
「新100校プロジェクトー関東地区活用研究会ー」

④(財)ソフトウェア情報センター主催により
「SOFTICセミナー　データベースサービスと契約上の問題　WIPO商標・ドメインネーム会議報告」

の各シンポジウム・セミナーが，また，記念式典併設行事として「全国高校生・専門学校生プログラミング・コンテスト入選作品展示・デモンストレーション」がそれぞれ開催され，各会場とも満員の来場者を集め，熱心に聴講される受講者やデモンストレーションを見学する人々で盛況な催し物となりました。

なお，記念式典後情報化月間の開始を祝し，情報化関係団体の主催による記念パーティが催され，主催者を代表して井川 博 情報化月間推進会議議長のご挨拶および来賓として小渕 恵三 外務大臣・自由民主党情報産業振興議員連盟会長の丁重なるご挨拶，そして堀内 光雄 通商産業大臣による乾杯の音頭により記念のパーティが開会されました。

関係各方面から多数の参加者をはじめ，記念式典において表彰を受けられた方々も加わり，なごやかな懇親の場となりました。

平成九年度情報化月間記念式典次第

一、開　会
一、挨　拶
一、表　彰
① 情報化促進貢献個人の表彰
② 情報化促進貢献企業等の表彰
③ 優秀情報処理システムの表彰
④ 全国高校生・専門学校生プログラミング・コンテスト入選作品の表彰
一、受賞者代表挨拶
一、閉　会

以上

井川 博 情報化月間推進会議議長の挨拶

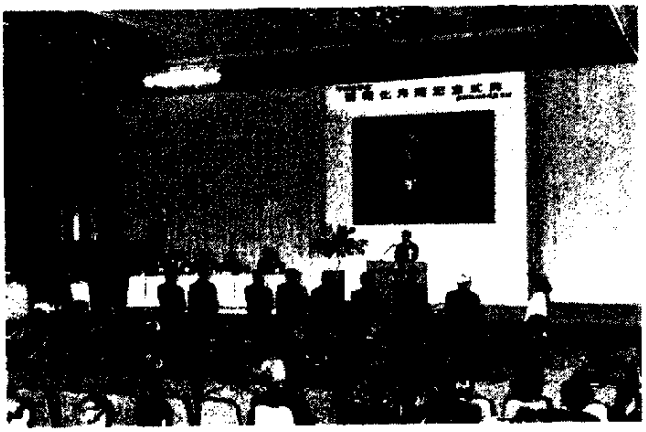
堀内 光雄 通商産業大臣の挨拶

陶山 晧 総務事務次官の挨拶

中谷 元 郵政政務次官の挨拶

江口 一雄 運輸政務次官の挨拶

1. 平成９年度情報化促進貢献個人受賞者一覧



通商産業大臣表彰

氏　名	所　　属	業　　績
板井　裕	沖縄県ソフトウェア産業振興協会会長 (64)	情報処理技術の研究開発，普及啓発等を進める団体を設立し県下の情報サービス産業の発展のための基盤づくりに尽力するとともに，沖縄県高度情報化推進懇話会委員等数々の要職を務め，地域の情報化の促進に貢献をした。
佐野　博持	㈱ユニオン・エンジニアリング 代表取締役社長(69)	(社)日本システムハウス協会の設立に尽力しその後，役員を長年歴任し，システムハウス業の経営基盤の強化に努めるとともに，マイクロコンピュータ応用システムの普及促進，地域の情報化等に貢献した。
高橋　啓介	㈱インターコム 代表取締役社長 (50)	(社)日本パーソナルコンピュータソフトウェア協会の役員活動に精励するとともに，先駆的なパソコン通信ソフトウェアの開発・普及等によりネットワーク関連のソフトウェア開発の促進に貢献した。
高原　友生	㈱CRC総合研究所 相談役 (72)	(社)情報サービス産業協会の会長として卓抜した指導力を発揮し協会の基盤づくり，世界情報処理産業会議の主宰等国際化の促進に尽力するとともに，産業構造審議会等の委員を歴任し情報サービス産業の発展に貢献した。
中村　雅哉	㈱ナムコ 代表取締役会長，兼社長 (72)	(財)マルチメディアコンテンツ振興協会等の役員を長年歴任し，コンピュータグラフィックとアミューズメントの技術交流・融合の促進及び家庭分野への普及等によりマルチメディア関連産業の発展に貢献した。
鳴戸　道郎	富士通㈱ 専務取締役 (62)	WIPO（世界知的所有権機関）におけるベルヌ条約採択，国内知的財産権関係法の改正等に関し産業界のとりまとめに尽力し知的財産権の基盤整備・国際協調を促進することにより情報サービス産業の国際化等に貢献した。
根橋　正人	(財)ニューメディア開発協会顧問 (73)	(財)ニューメディア開発協会の役員を長年歴任し，ニューメディア・コミュニティ構想等に基づき，地域ニーズに即応する情報システムの構築・調査研究等を指導的立場で推進し，地域情報化の促進に貢献した。
宮原　秀夫	大阪大学大学院 基礎工学研究科教授 (54)	情報通信分野における「システムのモデル化と性能評価」の研究を進めネットワーク構築の高度化に貢献するとともに，地域の先進的アプリケーション基盤施設の整備及び高度技術者の育成等地域情報化の促進に貢献した。

総務庁長官表彰

氏　名	所　　属	業　　績
堀川　榮一	(財)保安電子通信技術協会 技術参与　(64)	警察庁における情報化に当初から携わり，警察行政の情報システム化に貢献するとともに，行政機関相互間の情報通信ネットワーク構築のための委員会等委員として，政府全体の行政情報通信ネットワークシステムの基盤整備に貢献した。

運輸大臣表彰

氏　名	所　　属	業　　績
野末　尚次	(財)鉄道総合技術研究所　技術開発事業本部技師長　(54)	コンピュータ情報処理技術をいち早く利用し，交通計画関連業務における各種の意思決定支援システムの開発に努め，情報化の促進に多大の貢献をした。

郵政大臣表彰

氏　名	所　　属	業　　績
加納　貞彦	日本電信電話㈱ 常務理事　研究開発本部副本部長　(56)	国際電気通信連合電気通信標準化部門(ITU-T)第11研究委員会(SG11)の議長職を務めるなど，ITUの活動を通じてB-ISDN等に関する標準化の作成及び普及に寄与し，日本の国際的な標準化活動に大きく貢献した。
敦井代五郎	北陸瓦斯㈱ 代表取締役会長　(79)	(財)信越移動無線センターの設立に尽力するとともに，長年にわたり同財団の理事長を務め，各種災害への救援・復旧支援活動に業務用無線(MCA)を活用するなど，MCA無線の普及促進に多大な貢献をした。
山口　正之	愛知電子㈱ 代表取締役会長　(73)	(社)日本CATV技術協会の活動を通じCATV技術者の育成等に尽力するとともに，多年にわたりケーブルテレビ関連技術の開発に努めるなど，ケーブルテレビの普及発展に大きく貢献した。

2. 平成９年度情報化促進貢献企業等受賞者一覧

通商産業大臣表彰

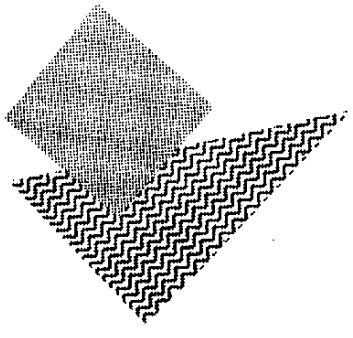
企業等の名称	代表者	業　　績
IS&C委員会	代表者 松井　美楯	X線写真等に代わる電子媒体を用いた医用画像の電子保存について産学共同研究を推進し，データの互換性やセキュリティの確保に必要なデータフォーマット等の規格・仕様書を作成し，医療分野の先駆的な標準化に貢献した。
関西電力㈱	代表取締役社長 秋山　喜久	高度情報技術を活用した経営革新に取り組み，対顧客業務や，流通・発電等の基幹業務などに関し大規模な情報ネットワークを構築し各種サービスの向上，業務処理の効率化等を進め，高度情報化による業界の発展に貢献した。
㈱西武百貨店	代表取締役社長 米谷　浩	顧客情報と商品情報を統合した先進的な顧客管理システムや取引者間で共有できる商品管理システムを構築し，また全社的情報ネットワークを推進するなど大規模な情報システム化を図り流通業界の発展及び情報化に貢献した。
日本ナレッジインダストリ㈱	代表取締役社長 春日　正好	(社)情報サービス産業協会の普及啓発活動に積極的に参画し情報サービス産業界の地位向上に尽力するとともに，コンサルテーション，調査研究等を含む高付加価値のある情報サービス業に取り組み情報化の促進に貢献した。
日立電子サービス㈱ 社会保険庁保守グループ	グループ代表 畠山　雅夫	社会保険庁社会保険業務センターにおける公的保険のデータベース，支払システム等の保守・管理の着実な履行により，社会保険業務システムの長期にわたる円滑な運用に寄与し，社会保険制度の情報化の推進に貢献した。
㈱富士銀行	頭取 山本　恵朗	電子商取引における電子決済システムの先駆的な取組，インターネット技術を活用した双方向通信によるバンキングサービスの提供など先進的技術の開発・導入により，金融業界の高度情報化に先導的な貢献をした。
㈱メルコ	代表取締役社長 牧　　誠	多種のマルチメディア関連機器の開発や，パーソナルユーザーの多様なニーズに的確に応えられるコンポーネント組立によるパソコンの開発・普及活動を進め，情報処理技術の高度化及びパソコンの普及促進に貢献した。

運輸大臣表彰

企業等の名称	代表者	業　　績
岡田運輸㈱	代表取締役社長 岡田　勇	中小のトラック運送事業者として，業界初の衛星通信による情報ネットワークを構築し，情報化への対応の先駆的役割を果たすとともに，利用者利便の向上及び事業の効率化など企業の情報化の促進に貢献した。

郵政大臣表彰

企業等の名称	代表者	業　　績
ISDN国際共同研究会	事務局長 松本　允介	昭和63年の設立以来，「ISDN分野」におけるアジア諸国との共同研究を実施し，参加各国の技術者の育成に寄与するとともに，平成９年度までに全参加８か国でのISDN商用サービスを開始することを実現させるなど情報通信を通じた国際協力に大きく貢献した。
小田急電鉄㈱	代表取締役社長 北中　誠	昭和62年より他社に先駆けて，列車内におけるラジオ放送の再送信設備の導入に取り組み，ラジオ放送の聴取困難なエリア解消を通じて乗客の利便向上に努めるとともに，その導入に当たり，標準的な列車内再送信技術を開発するなど，技術面においても列車内再送信の普及に大きく貢献した。
(社)テレコムサービス協会マルチメディア実験協議会	会長 一力　健	口座振替とファクタリング(代金収納代行)を利用した電子決済システムの開発，デジタルコンテンツのオンライン販売への取組等を通じ，マルチメディアサービスの実用性を検証し，情報通信を活用したサイバービジネスの実現に大きく貢献した。



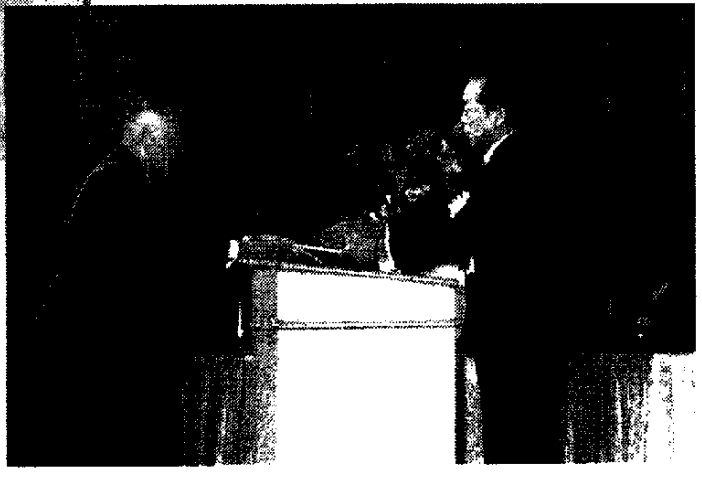
3. 平成９年度優秀情報処理システム受賞者一覧

情報化月間推進会議議長表彰

システムの名称	表彰理由
[部品化手法によるアプリケーション開発ツール「SSS」] ウッドランド(株)	中堅中小企業向けの販売管理システムを業態ごとのモデルシステムを雛形とすることで，システム開発における高生産性や高品質を確保し，ユーザーニーズに応じたカスタマイズの両立を実現し，高い評価を得た。
[テレホンバンキング「センギン・ダイレクトホン」] ㈱泉州銀行	テレホンバンキングシステムの構築において，暗証番号に加え，声紋照合による本人確認や，音声伝票や音声申込書を用いた取引承認，取引内容の記録によりセキュリティを確保するなど先駆的技術を導入し，高い評価を得た。
[テトラリエンジニアリングインフォメーションシステム(TETRIS)] (株)テトラ	土木建築業界において工事管理業務に関する全国規模のワークフローシステムを先駆的に導入するとともに，リモートクライアント操作も可能なヘルプデスクの設置等，システム利用が社員全員に定着するための工夫を行い，中堅企業におけるリエンジニアリングのためのシステム導入の優れた先行事例となった。
[NICE80] ナカシマプロペラ(株)	電子掲示板や個人スケジュール管理のみならずCAD図面等の設計情報の流通といったEDIの基盤となる機能を持つとともに，操作性がよく拡張の自由度の高い社内情報共有システムを構築し，高い評価を得た。
[JALインターネット国内線チケットレス予約システム] 日本航空(株)	インターネットを利用し，セキュリティが確保され，24時間利用できる利便性の高い航空機チケットの予約及びチケットレス予約(決済)システムを構築し，電子商取引の進展，普及に貢献した。
[ナースネット] 日本電子計算(株)	携帯医療端末を利用したベッドサイドでの看護情報記録等の看護業務を支援するシステムを，ユーザーである看護婦にとって優しい操作性を持つよう考慮して構築し，現場レベルでの医療の情報化に貢献した。
[「チケットぴあ」ニューチケッティングシステム] ぴあ(株)	会社としての基幹業務であるだけでなく，社会性・公共性が高く，かつ高速トランザクション処理が必要となるチケット予約・販売業務の処理をクライアント／サーバシステムにより実現し，高い評価を得た。
[ILIS／X-10] (株)富士通東北システムエンジニアリング	優れたデータベース処理が行えるとともに，図書検索が容易にできる音声合成・タッチパネル対応の利用者開放端末等豊富な機能を持つ図書館システムをパソコンベースで構築し，市町村レベルの図書館の情報化に貢献した。
[兵庫県災害対応総合情報ネットワークシステム] 兵庫県	兵庫県下全域の防災計画・被害予測等の危機管理を行い，また災害発生時において，災害情報の集約，県の意思決定・初動体制確保の支援及び県民や関係機関に関連情報を提供する防災情報システムを構築し，県防災行政の基盤整備を行うとともに，他府県のモデルとなった。
[ニュー新幹線システム(COSMOS)] 東日本旅客鉄道(株)	新幹線輸送にかかわる計画業務・指令業務の大半を占める定型作業の情報システム化を図ることにより，単純繰り返し労働の整理・分離・自動化が可能となり，鉄道業務の効率化に貢献した。
[気象情報提供システム] 大阪湾海上交通センター	船舶運航者，漁業関係者及び海洋レジャー関係者に，大型船舶等の航路入航予定情報，気象情報及び操業漁船情報等を自動収集・編集し，ファックスサービスすることにより，情報提供の迅速化が図られ，船舶の航行安全に貢献した。
[沿岸気象海象情報配信システム(COMEINS)] (財)沿岸開発技術研究センター	波浪実況情報と高精度な波浪予測情報及び関係気象情報をユーザーに24時間オンラインでリアルタイムに提供することにより，港湾工事，船舶の運航を安全かつ効率的に管理することを可能とし，沿岸防災に貢献した。
[オホーツク・インターネット] オホーツク委員会	小規模自治体が連携してインターネットを活用したネットワークを構築し，地域情報化への取組に活用するなど，情報通信ネットワークの新しい運営形態の先駆的事例として地域生活基盤の整備及び情報化の促進に大きく貢献した。
[公共料金等の事前一括請求・一括支払サービス] 清水建設㈱	企業・金融機関・公共サービス機関等をネットワーク化した公共料金等の一括請求・一括支払のシステムを開発し，公共料金の請求・支払手続きの情報化・ネットワーク化による事務の効率化の促進に貢献した。
[Hospi-net(ホスピネット)] セコム㈱	医療機関の撮影したMR／CT画像をデジタル回線(ISDN)を介し，専門の読影医師が画像読影を行う遠隔診断支援システムとして，医療サービスの効率化，地域格差の是正に大きく貢献した。

優秀情報処理システム表彰風景

受賞者代表挨拶（高原友生氏）



4．平成９年度全国高校生・専門学校生プログラミング・コンテスト入選作品

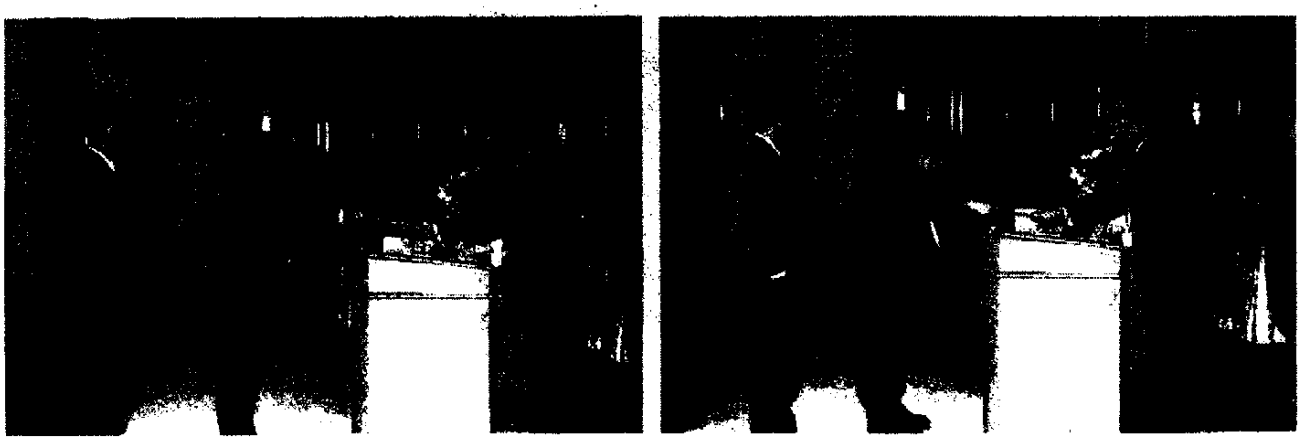
全国高校生・専門学校生プログラミングコンテストは，通商産業省が次代を担う青少年の情報教育の重要性に着目し，昭和55年から情報化月間の主要行事として「全国高校生プログラミングコンテスト」を実施しております。平成７年度からは，将来各種の高度情報処理技術者となるための基礎的な知識・技術を備えた人材として期待される専門学校生もコンテストの対象に加え，専門学校生の部を設けました。

今年度は，８月15日（金）に応募を締め切り，総数で123点（高校生部門77点，専門学校生部門46点）の力作が寄せられました。応募作品は「全国高校生・専門学校生プログラミングコンテスト審査委員会」での厳正公正な審査により，以下の８作品（高校生部門５点，専門学校生部門３点）が入選されました。

入選された方々には，10月１日（水）の「情報化月間記念式典」におきまして，堀内通商産業大臣から賞状，記念の楯と副賞のパーソナルコンピュータ（(社)日本電子工業振興協会の協力）が贈られました。

また，入選作品は，記念式典の併設行事として，展示・デモンストレーションを行い，多数の来場者に紹介されました。

高校生部門表彰風景



専門学校生部門表彰風景

(高校生の部)

	作品名	作成者		作品の概要
		学校・学科・学年	氏名	
最優秀賞	Window Master	駒場東邦高等学校 普通科 2年	栗原 賢一	Finderでは，ファイルの管理を行えるが整理しすぎるとフォルダの数が増えてかえって能率が下がる。ルーチンワーク等で同じフォルダを開く場合，自動で開くようにした。また，使いづらいFinderの機能を使いやすいようにプログラムを作った。 複数のウィンドウの位置・大きさを記録し，任意に呼び出す，開かれているウィンドウをスタック状に並べる，ウィンドウの表示法の設定，全てのウィンドウを閉じる等の機能がある。
優秀賞	手話っち点字君97	埼玉県立新座総合技術高等学校 情報技術科 3年 〃 3年 〃 3年 〃 3年	坂口 功 遠藤 剛 小沼 元輝 前田 浩隆	身障者用の言語である手話は単語と接続詞を持った1つの文としてやりとりされることが多い。そのような通常使用されている形の手話ができないかと思いこのプログラムを作成した。さらに点字にも目を向け，点字文書へ変換する機能を追加した。 入力された任意の文章を手話により表示するため，文章を単語や文節などから文を解析し，手話を組み立てるシステムを独自に作り上げ，動きを示すポリゴンシステムにより手話アニメーションを実現した。 点字入力のための画面に表示されるソフトキーボードを開発し，マウス操作だけで文字入力を可能にした。
	バーチャル交通安全教室	私立大牟田高等学校 電気科 3年 普通科 3年 工業Ⅱ類 1年 〃 1年	坂本 智輝 西本 葉月 藤澤 武士 吉田 聡	交通事故に遭って初めて事故の恐ろしさや責任・規則を自覚するものだと思われるが，そうなってからは手後れになる。そうなる前にコンピュータで作り出す仮想現実空間で交通事故の疑似体験をし，交通安全意識を高め，悲惨な交通事故を少しでも減らすことに役立てることを目的に作成した。 交通安全指導の手引き（歩行者，自転車，二輪車，車，事故等），交通事故データベースを利用した交通事故報告書作成，交通標識の学習，映像で学習する交通安全教室（交差点の危険性，二段階右折等），高齢者事故防止のために地図上の走行軌跡・写真データ・音声データで危険箇所を指摘して道案内する等の機能がある。
努力賞	3DIM for Windows	昭和学院 秀英高等学校 普通科 3年	五十嵐 誠	化学物質等の構造をパソコン上で立体的に見たいと思いプログラムを作成した。 3次元の直交座標を入力することにより，その図形を立体的に表示し立体的な図形を好きな方向にマウスで回転させることができ，その図形のステレオ図（2つの図形を重ね合わせて立体感を表現）を出力することができる。
	ホームページ簡単作成ワープロ HOPE	岡山県立 水島工業高等学校 情報技術科 3年 〃 3年 〃 2年	掛谷 満広 西牧 宏晃 横溝 洋市	HOPE（Home Page Editor）は市販の高機能ビルダーの操作が複雑でHTMLの知識のない初心者には使えない，HTMLに変換してくれるワープロもあるが変換に時間がかかる等の不満を解決したホームページビルダー＆ワープロである。文字のサイズ，色などワープロと同じ操作でホームページが作成でき，HOPEで作成した文書を他のワープロソフトでも利用できる。

(専門学校生の部)

	作品名	作成者		作品の概要
		学校・学科・学年	氏名	
優秀賞	シューティングゲーム	岩崎学園情報科学専門学校新横浜校 情報工学科 2年	笹尾健太郎	JAVA言語によるアクションゲームである。JAVA言語とブラウザの特性を理解し，ゲームで要求される動作スピードを保持するためのロジックをプログラムに組み込み，また，ゲームデータベースの作成，メンテナンス等の機能もあり，パラメータにより他のゲームに簡単にカスタマイズできる。
努力賞	DOTTER TOOL	日本コンピュータデザイン専門学校 SEゲームソフト学科2年	細田 丈治	シミュレーションゲーム制作ツール。ゲームの内容は戦争ゲームである。その際に32×32ドットサイズの戦車や戦闘機などの絵を画面上に表示するのと，戦車が爆発するシーンや，キャラクターが歩いたりするシーンもあり，この作品はキャラクターの作成・編集ツールである。
	おざなりメンテ	日本工学院専門学校 情報処理科3年制 3年	中原 周一	MS-DOS環境においては，ファイル操作を行う場合，行いたい操作を実現するためにコマンドを入力しなければならない。その操作を行うためには，MS-DOS環境に関する知識が必要とされた。これらの知識が乏しい利用者等のために，ファイル操作等が簡単に行えるツールである。 ドライブの移動，ファイルの検索，ファイルのコピー，ファイルの移動，ファイルの閲覧，ファイル・ディレクトリの削除，DOSコマンドの実行，プログラムの実行等の機能がある。

展示・デモ風景

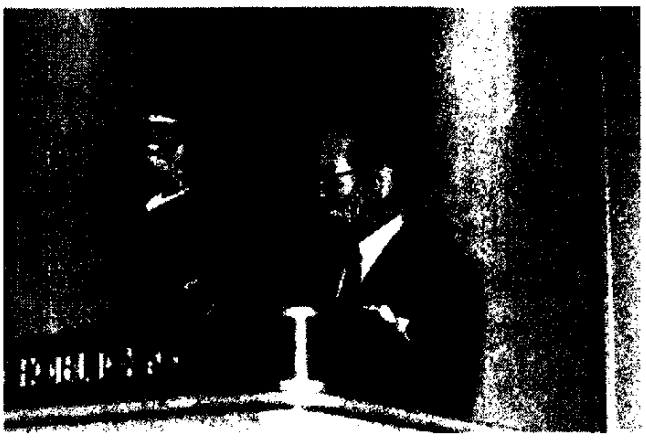
なお，本コンテストは，来年度も今年度と同様の日程で実施される予定になっています。詳しくは，下記までお問合せください。

事務局：〒105 東京都港区芝公園3-5-8
財団法人日本情報処理開発協会
情報化月間担当
Tel：03-3432-9381／Fax：03-3432-9389

5. 記念祝賀会

記念祝賀会　主催者挨拶　井川 博 情報化月間推進会議議長

記念祝賀会　来賓挨拶
小淵 恵三 外務大臣・
自由民主党情報産業振興議員連盟会長



記念祝賀会　乾杯
堀内 光雄 通商産業大臣

ネットワーク社会の進展とセキュリティ

――ネットワーク犯罪とその対応――

「情報化月間記念国際シンポジウム」講演録から

当協会と情報処理振興事業協会では，平成９年度情報化月間の記念行事として，平成９年10月１日（水）に東京全日空ホテルにおいてネットワーク社会の進展とセキュリティを統一テーマとした国際シンポジウムを開催しました。

テーマの背景としては，インターネットの急速な普及に伴う不正アクセスをはじめとするさまざまな障害の急増があります。

近年のインターネットに代表されるネットワーク化は，産業界はもとより，社会，個人・家庭にいたるあらゆる分野に拡がってきております。

電子商取引に見られるようにインターネットの商用利用は，消費者にとっての利便性の向上だけでなく，産業界にも大きなビジネスチャンスをもたらすものとして期待されています。

しかし，ネットーク化はわれわれの社会生活に多大の利便性をもたらす反面，その対応を誤ればはかり知れないマイナスの影響をもたらす危険性をはらんでおり，ネットワークに対する信頼性，安全性の向上が社会的な要請となっています。

そのため，不正アクセス等セキュリティにかかわる問題やネットワーク上を流れる有害情報への対応など，ネッワーク化に伴うさまざまな課題について十分な対応が図られなければなりません。

本シンポジウムでは，ネットワーク化の進展がもたらすさまざまな課題について明らかにし，健全な情報ネットワーク社会の実現を

目指すことを目的として開催しました。

シンポジウムには，760人を超える参加申込みがあり，ネットワーク時代のセキュリティのあり方に対する関心の高さがうかがわれました。

本稿では，シンポジウムからビル・ハンコック氏，リチャード・ペシア氏の講演およびパネルディスカッションの模様を要約してご紹介します。

ビル・ハンコック 氏

Network-1 Software & Technology 社
筆頭副社長兼技術担当最高責任者

ネットワークセキュリティおよびネットワークセキュリティの将来について，どのような技術を使ってネットワークセキュリティを確保しなければならないか，また，どういった概念に基づいてネットワークセキュリティを考えていかなければならないかについて，お話しようと思います。はじめに，セキュリティの技術面をご紹介してから，ネットワークセキュリティ戦略の10のステップをお話したいと思います。

まず，なぜネットワークのセキュリティが確保されていないかということです。この対処としてパスワードの暗号化が考えられます。しかし，パスワードの暗号化ができていても，コンピュータを接続してコンピュータ対コンピュータでOSが違うとパスワードが暗号化されていない場合があります。

次に，人員の問題です。携わる要員のセキュリティに関する経験が乏しいということ，セキュリティの経験が欠けていることです。

３番目に重要な問題として，経営者のバックアップが挙げられます。これには，２つの側面があります。まず権限です。セキュリティの問題を解決するために何が認められているか，ということと責任の問題です。経営者の側では，この問題がうまく取り扱われていません。よく経営者サイドでは，テクニカルチームの方にネットワークセキュリティの責任を課したりするわけです。ところが，反面十分に対策をとるための権限を与えていない場合があります。ネットワークセキュリティの責任を課すわけですが，経営者は警察の関与などを求めるという権限を与えていないし，いろいろな対策をとる権限というものも与えていない場合があります。

Why Networks are Not Secure

- u Lack of password encryption
- u Lack of personnel with experience
- u Lack of management backing
  - u Authority
  - u Responsibility
- u Legal and political issues
- u Lack of recurring effort
- u Budget

お金をかければセキュリティの問題は解決するのだ，もっと別の経営問題を解決すれば良いと考えている経営者がいるわけです。セキュリティをその程度の経営戦略的な視点で考えている経営者が多いわけです。しかし，セキュリティは車の洗車と同じで，１回洗車してもまた汚れてまた洗車しなければなりません。洗車には相当時間をかけなければなりません。ネットワークセキュリティも同じです。繰り返しやらなければならないし，繰り返し運用コストが発生するということです。

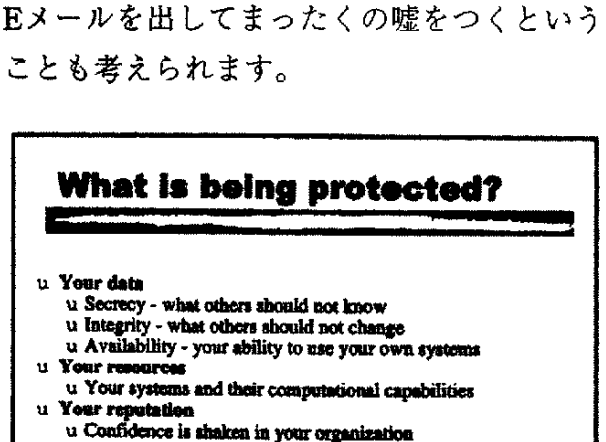
次に予算です。セキュリティの最も大きな問題として，ほとんどの企業においてセキュリティは，オーバーヘッドとしてとらえられています。すなわち資本金，あるいは利益を還元するような資本とは考えられてはいません。そのため多くの経営者にとって，セキュリティにかかる予算というのは，企業の収益に貢献しない予算であると考えています。

そこで多くの経営者はセキュリティというのは，最初に削減の対象として検討しがちです。その次に教育費とかあるいは出張費とかの順番で削減されてしまいます。その結果，深刻なセキュリティの問題を抱えることになるわけです。しかし，それを解決する予算がありません。悪い事態が発生した時に，これは大変だ，どうしようもないと思うわけです。そして過剰反応が見られることになるのです。

つまり，予算の削減がよく起こるのは，セキュリティというものが，利益に対して貢献する要素として容易に測定できないからです。しかし実際には利益に貢献しているのです。セキュリティがなければ会社が破綻してしまう，資産を失ってしまう，多くのお金をかけて回復をはからなければならないからです。

ネットワークセキュリティを考えるに際し，どのようにしてわれわれの資産を守るかということがあります。３つの保護の側面を考えなければなりません。まず，秘密性です。人々が知るべきでない情報です。２番目に整合性です。整合性というのは，項目として変えるべきでないものです。例えば見積書をどこかに出すかもしれませんが，その数字を変えられてしまったら大変なことになってしまうかもしれません。そこでデータの整合性に悪影響を及ぼすことが考えられるわけです。それから，システムを使うことができるか。リソースを活用することができるかということです。

ネットワークセキュリティの大きな問題として５つあります。まず，組織に対する信頼というものが揺らいでしまいます。つまり，人の信頼を失ってしまうということです。２つ目に犯罪の出発点として，サイトを悪用されてしまうという可能性です。３つ目に不要なデータ配信のサイトに利用されてしまうということも考えられます。４番目になりすましということが考えられます。これによって社会的な混乱がありうるわけです。５番目にEメールを出してまったくの嘘をつくということも考えられます。



企業にとって一番の脅威というものは，あらゆる調査から社内の人間であるということがわかります。現在の従業員，あるいは元従業員だったということもあるわけです。会社に対して反感を持っている人達です。外部からのネットワークのハッカーやクラッカーなどは依然としてあります。それから産業スパイが急増しています。産業スパイの例ですが，冷戦の終了とともに，KGBとかドイツのシュタージとか，あるいはブルガリア秘密警察の元技術者という者達がいます。彼らは，非常にいいトレーニングを受けています。そうした人たちは今や，フリーでもってインターネットでいろいろな情報入手のサービスを提供しています。また，トップマネージメントに対する個人攻撃もみられます。これによって，企業の混乱とかトラブルを起こします。

1997年4月時点で，コンピュータの侵入，あるいはネットワークの侵入は，内部の人間によるものが55%，ダイヤルアップのプライベートネットワークによる侵入が15%で，すべての侵入のうち，70%が内部によるものです。しかし実際に社内の数字はもっと高いといわれています。

企業は侵入されたことを隠すために，その実体はつかむことができないといわれています。ますますこうした状況は増えてくると思われます。電子商取引も普及して来ますし，電子マネーも対象となるわけです。それから家庭からコンピュータをビジネスの目的で使うことになるわけですけれども，個人攻撃もコンピュータによって行われるということが考えられます。

多くの企業が犯すネットワークセキュリティの過ちとしては，ベンダーに言われたままにものを買ったりする。しかし，例えば航空会社を例にしますと，一番の脅威というのは予約システムであると考えられがちですが，それはまったくの間違いです。止まってしまう一番の脅威は，データベースの変更です。予約システムを止めたとしても何とか飛行機には乗れます。しかし重量とバランスが間違っていて，そしてバランスも離陸速度も変えられてしまった場合には，飛行機は飛び立つことはできません。これが飛行機にとっての一番の脅威です。そこのセキュリティを第一に確保しなければ，問題の解決にはならないわけです。

まず，何を解決しようとするかを理解しなければ，正しく予算を配分することができません。多くの企業では一番のセキュリティの脅威というものを理解していません。それを理解すれば当然ながら，次に何をしなければならないかがはっきりしてくるわけです。多くの企業はここで過ちを犯してしまいます。

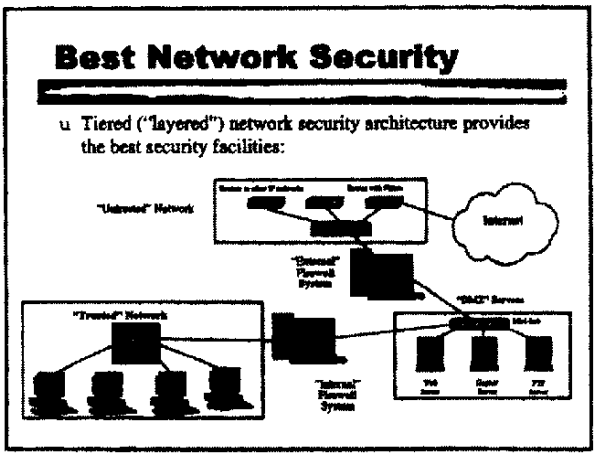
いずれにしても，セキュリティシステムを構築し，世界各地で展開しようとした場合には，本当の意味でのセキュリティというものを考えるならば，言語の問題，それからローカライズの問題も考えなければなりません。

Spoken Language Problems

- In any security system, most consumers do not have enough expertise to properly configure and manage the systems themselves
- If a system is written in English and used in Japan, there will be additional interpretation problems with messages and configuration
- It is critical that security systems be adaptive and localized to the in-country language to simplify security management

いろいろな種類のハッカーの攻撃方法があります。主なものは，嘘をついて侵入する，また憶測によってパスワードを当てるなどです。英語圏においては猥褻な言葉を使うことによって大体30%から40%くらいのパスワードがわかってしまいます。それから技術的なツールがあります。サービス拒否というのも1つの攻撃方法です。ネットワークにおいて大量のデータを出すことによってネットワークの障害を起こすわけです。あるいは人が使えなくしてしまうわけです。メール爆弾という攻撃方法もあります。ホワイトハウスのインターネットのホームページにメール爆弾が送られたのです。大型のEメールのメッセージが5万回も出されました。それから愚かな行動，事故があります。バックアップの必要性というものを，クラッシュの経験から学んだ。そこで毎日45人がCD-ROMをバックアップしたのです。その結果，ネットワークが障害を起こしてしまうというようなことなどです。また，情報の盗難もあります。データを盗んだり，あるいはネットワークに侵入することによって，情報を盗ったりしています。

ネットワークセキュリティというのは，ただ単にファイアウォールを設けるだけではありませんし，また侵入を検出するだけでもありません。またVPN（Virtual Private Networks）だけでもありません。これらはすべて含まれます。そしてより多くの要素も加わってくるわけです。もっとも良いネットワークセキュリティというのは，階層化されたレイヤードアプローチです。階層化することによって，より良いセキュリティ環境を整備し，侵入者をくい止めることができます。そして別個の機能と連携しながらいろいろな脅威に対処するというやり方です。



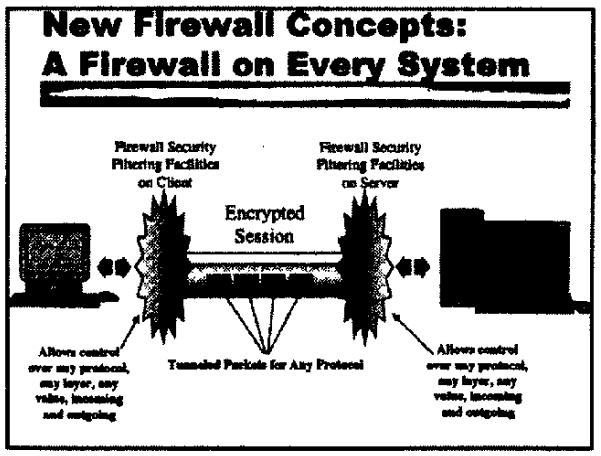
もう1つ，S／WAN（Secure/Wide Area Network）というもの，これはIPsecという名前で呼ばれているものです。それから認証サーバです。傾向としては，ますますユーザ毎の認証が行われます。"token device"を使った認証が行われるようになるだろうということです。

アメリカの3大銀行がスマートカードを統合化しようとしています。クレジットカードの機能と一体化することにより，セキュリティとIDの面を改善しようとしています。スマートチップとメモリがカードそのものの中に内蔵されています。こうしたカードにかかわるプライバシー侵害についての懸念としては，カードの中には大量のストレッチがあって，クレジットの履歴，それから治療歴，更には軍隊に入っていたことがあるかどうか，その他いろいろな情報を1つのカードに入れてしまうということが可能になるのです。ということは，そのカードがもし盗まれてしまえば，沢山の情報が盗られてしまうということになります。もう1つ，カードに関して忘れてはならないのは，共通の利用ということです。共通のフォーマットが使われれば，ますますこれが破られる可能性が高くなるわけ

です。

ファイアウォールの分野においては様々な変化が起こっています。例えば，ウイルスの検出ができるようになっている。あるいは認証の権限，またはストリームワークス，ビデオマスター等々といったアプリケーションプロトコルが出ています。IPsecのインテグレーション，それからNCSAの認証機能も変わってきており，また，OSの機能の１つとしてベンダープロキシの機能があります。

ファイアウォールの新しいコンセプトとしてあらゆるシステムにファイアウォールをという考え方があります。ネットワーク間だけに設けるのではなく，どこにでも設けるというわけです。



アクセスコントロールをネットワークのインタフェースに提供する。それぞれのマシンに提供するということは，何が入ってくるか，また何が出て行くか，つまりマシンの出入りを大変高いレベルで厳しくコントロールできるようになるわけです。今はまだ，これは存在していません。これは，あらゆるマシンに通じるもので，単にPCとかサーバだけの問題ではなく，ファイアウォールの機能すべてに内蔵させることになれば，大変高いレベルのアクセスコントロールを行うことができるのです。マシンとの接続に関し，またOSに対するアタックも防ぐことができます。

新しいファイアウォールのタイプも出ています。OSにおいてもデスクトップ上でセキュリティを実現しようとする試みが見られます。バーチャルリアリティという概念が，ファイアウォール管理の分野でも出て来てテストされています。バーチャルリアリティネットワークマネジメントというコンセプトで，ヘルメットとグローブを使ってネットワークを管理する。ネットワークの中を移動し，ルーターを見ることもできます。このようなアプローチをとることで，視覚的にネットワークがどういう状況にあるかを一目で把握できるわけです。これによって何ページものリストを読むとか，あるいは大量の解析をすることなしに，どういう状況になっているかが仮想空間の中で一目瞭然で分かるようになるわけです。

今後，企業で採用されていくと思われるのが，総合的なセキュリティサービスです。社内で独自のセキュリティスペシャリストを持つことができないということから，その支援を受ける体制を整えていくということです。

人間ということを考えますと，今は認証を受けている特殊な専門家CISSP（Certified Information System Security Professional）という資格が出てきていて，第４年度に入っています。それにより，この認定を受けているネットワークエキスパートが強化されてくる状況が出てきています。この分野において，彼らはセキュリティの専門家として活躍するわけです。そのためのテスト，資格を受けるということは非常に難しく高度であって，い

ろいろな専門，そして資格のチェックが行われるわけです。しかしそれだけの価値はあるということは言えます。いろいろな所でこのような公認の資格を持った認証のセキュリティプロというものの出現が見込まれています。

Security Certification

- u Certified Information System Security Professional (CISSP) now in year four
- u Effort to combine with Certified Computer Professional of ICCP
- u Enhancement to Certified Network Expert testing for security facilities
- u More effort by traditional security organizations to emphasize technical security as well as management issues

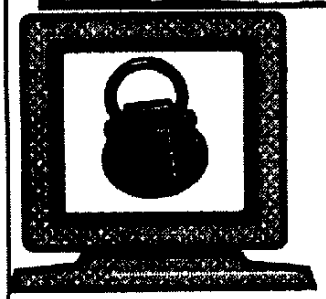
次に，ネットワークのセキュリティという面から企業内でどのような対策をとっていくかということです。企業としては，まずどの程度脅威があるか。どのような人から，何がアタックされるのであろうかということを見極めなければならない。2番目に，その対策のためにどの程度の予算が措置できるかということ。そしてどのような企業内の問題があるかということがはっきりしていなければ，ネットワークセキュリティを確立していくことはできません。

Step 2: Politics and Budget

- u How much does it cost?
- u Who does it make angry?
- u How does lack of action end up affecting politics and budget at the company?
- u How are responsibility and authority dealt with at the company?

セキュリティの問題というのは，対策を単独でそのまま付けたらそれでいいというものではない。必ずその知識を持った人間が管理しなければならない。また，プロダクトのレベルでも暗号，パスワード，ID，キー管理とかいろいろなものがあるわけです。こういうものを使いこなして，脅威というものに対しての対策を図っていくわけです。

Step 6: Security Products



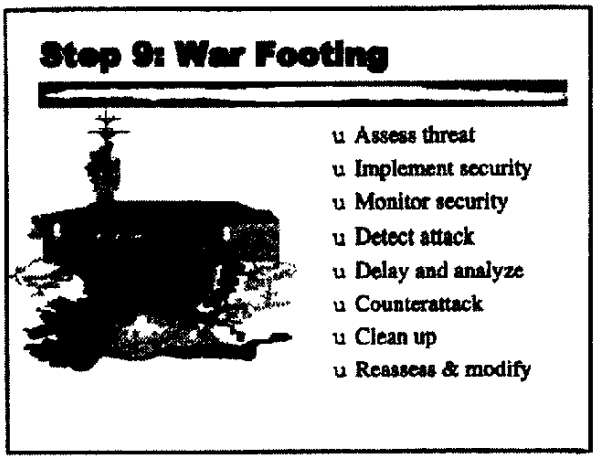
- u Authentication
- u Encryption
- u Passwords
- u Audit and logging
- u Key management
- u Certificate authority
- u Digital signatures
- u TCB and OS tools
- u Firewalls

そしてそこに1つの計画を立て，テストをしてチェックリストを作り，何が，どこがまずかったかということをはっきりさせなければなりません。経営トップもそれを認識し，ネットワークの拡大に伴なって対策も拡大させていかなければなりません。必ず，セキュリティはテストをして，検証していかなければならない。データベースと同じです。間違ったものを作ってしまうとデータベースに対するいろいろな不正アクセスが出て来てしまう。

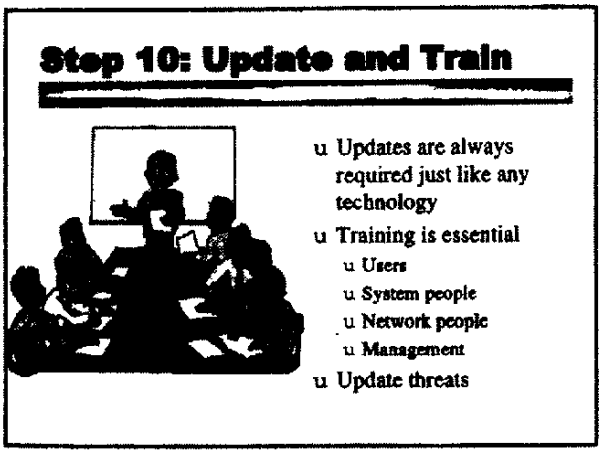
セキュリティも同じで，間違ったセキュリティ対策を立てれば他から侵入されてしまうということです。ですからテストをしてそれを防護して，そしてトラフィック管理を行っていくということが必要なわけです。

セキュリティということを考える時には，まず戦争というメンタリティを考える必要が

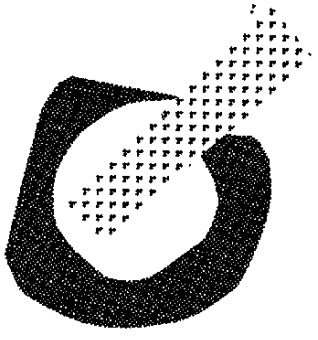
あります。必ず狙っている人間がいるということを想定する必要があるわけです。これは決して悪い態度ではありません。そのテクノロジーセキュリティを実施して，モニターしてアタックがあれば検出して必ず分析して，それに対するカウンタアタックを立て，後始末をし，再評価をし，変更をしてゼロからまたやり直すということです。これが日々のルールであって，それこそがネットワークセキュリティです。



必ずアップデートすること。そして研修をするということです。いろいろな立場の人を教育しなければセキュリティというものが理解されないし，実施されることもない。そして本当にアタックが起きた時に対策を実施することもできなくなるわけです。



インターネットをはじめ，ネットワークではいろいろな問題があります。必ずファイアウォールフィルタを通って来るものがある。そして外部からのハッカーの侵入ということについて言えば，人々は外部から必ずや入って来ようとするということです。しかし，時々そのパートナーだとか，知っている人だとか，顧客がそういった行動に出るということも知っておかなければなりません。インターネットには多くの問題が付随しています。ですから例えば，ウェブサイトにはパーソナル情報，人事情報等を置いてはいけない。人間に関する情報であるから必ずこれはプライバシーの問題がつきまとうということを考えなければなりません。そして法的な問題が起こり得る。非常に悪い訴訟にまで発展することになる。あなたがその対応している相手は誰かを見極め，そして必ず法律的な支援またはアドバイスも受けて行く必要があると思います。われわれはその適切な処置をとってセキュリティを確立していく必要があると思います。



リチャード・D・ペシア 氏

米国CERT
ネットワークシステム安全対策担当責任者

CERTは1988年国防総省から発足したものです。CERTの目的と致しましては，インターネットにおけるコンピュータセキュリティの問題を調査したり，あるいはネットワーク技術における脆弱性というものを研究しています。ハードやソフトの方面においても活躍しています。インターネットの世界において啓蒙活動も進めています。また，どういう課題があるか，どういう対処方法があるかを教育しています。

劇的な変化がネットワークに起きていることを説明しなければなりません。この５年の間の動きですけれども，88年にCERTが発足した時には20万人のインターネットの利用者がありました。ネットワークは大学機関および政府の施設によって利用されており，主に研究目的に利用されていました。ネットワークにおける動きの殆どは，科学技術の推進の活動でした。また，インターネットコミュニティというのは，オープンなものでなければならないという姿勢のもとで非常に信頼があり，小さな町の雰囲気でした。しかし，現在のインターネットというのは劇的に変化しています。インターネット利用者は，何十万人単位ではなく，何千万人単位となっています。そして，研究だけではなく，商用目的のためにも使われています。また製品の供給等における共同活動にも利用されています。本当の意味で国際的なネットワークになっています。

このような状況の中で，テクノロジーのサポートにおいても大きな状況の変化が起きています。より多くの人達がこの技術を利用するようになってきています。しかし，不幸なことに可能性と共にいろいろな問題も発生しています。コンピュータおよびネットワークというのはビジネスのやり方を変えています。革命が起きているわけです。その一方で，脆弱性があり，そして深刻な攻撃を受ける可能性があるのです。

多くの企業にとっては，インターネットというのは非常に重要なものとなってきています。そのためインターネットが使えなくなった場合には大きな問題になり得るわけです。脆弱性だけでは全体像を把握することはできません。実際に脅威があり，それに対処しなければならないことを認識しなければなりません。89年に１年間で140例が報告されました。96年，昨年ですが，12ヶ月で2,600例が報告されました。過去１万１千ものセキュリティ関連の例が報告されており，６万７千ものサイトが影響を受けました。ですからこれはたまにしか起こらないということではなくて，日々起こりうるものなのです。６万７千もの会社，あるいは組織のサイトが影響を受けたのですから，皆さんの中にもまったく自分で知らないのにこういうことが起こってい

るかもしれません。

今日70%の人たちは，我々の方から知らされてはじめて知ったということがわかっています。内部のオペレーションでは問題が検出されず，我々の方にいろいろと異常が報告されていましたので，侵入があった事実が判明しました。侵入者がデータにアクセスしていた後を残していたため，それを追いかけていたら，被害者が特定されたということがあります。

侵入者はどういう人間かということですが，ハッカーに対して皆さんにはイメージがあると思います。10代で，技術的な技能を持ち，社会的に方向性を誤っており，コンピュータのハッキングに興味があるのは，技術的なチャレンジととらえているからだ，というイメージです。確かに，何年かの間，そういうイメージ通りであり，それはそれで今日も有効ですが，しかし，今は，そういった社会的適応ができない人間だけではなく，社会に溶け込んでいる人間もハッカーになっているのです。そういった人たちがネットワークに対していろいろな不正を行っているのです。その例として，ウェブサイトに落書きをしてしまうといったものがあります。アメリカですと，よく壁にスプレーペイントで落書きをしてあるのが見られます。都市のきれいなところが無惨な状況になってしまっているのですが，これが今インターネットでも起こっているのです。好奇心でやっているというものではなく，今はデータ破壊にまで繋がっているわけです。社会的なメッセージを伝えようとすることもあります。インターネットのオペレーションを邪魔することで，何らかのメッセージを伝えようとするものです。

それから普通の，昔からいたような泥棒があります。金目当ての犯行で，価値のあるものを盗んで，それを売ろうとするわけです。皆さんの情報資産，これは無形資産です。我々がますます情報技術に対して依存性を高め，いわゆる知識の時代へと移っている中において，情報の価値が高まっていますから，我々は他の資産を守るのと同様，これらにも目を光らせなければなりません。

我々がこのテジタル技術をもって，効率的なビジネスと思っているのと同じように，組織犯罪者もまたビジネスの効率化をはかる上で，ネットワークの効率を利用しようとしており，積極的に使おうとしているわけです。さらに，それを超えるとテロ組織があります。軍事的な作戦をなんらかの形で展開するというものです。

防御手段が高度化するに従って，攻撃の方も巧妙になってきました。例えば，OSのソースコードやネットワークのソースコードを使って，ネットワークの弱点を学び，あるいは，ネットワークプロトコルの弱点などを知ってしまう。これらは大変に防御の難しいものです。

強力な暗号化技術を使うということによって，データファイルに侵入者の足跡がもう残らなくなってしまっている。こうした侵入者はますます頭が良くなっている，ということを良く理解しなければなりません。どういう形の手口になっているのか，そしてシステムをどうやって利用しているか，ということを理解しなければなりません。我々の持っている弱点を理解するとともに，我々には脅威が迫っているのです。

この10年の間，大きな変化として一極集中

的なメインフレームから分散型のクライアントサーバーへと構成が変わってきました。いろいろな機種が導入され，しかも１機種だけのベンダーが存在するようになりました。ということは10年，15年前にやっていた手段というものが，上手く使えなくなっているのです。かつてシステム管理担当者は，自分の技術がどういうものなのかをよくわかっていたし，その施設についてもきちんと管理し，コントロールしていました。一握りの人たちがこの技術やシステムについて習熟しており，すべてを一手に引き受けていました。セキュリティだけでなく，日々のオペレーションに関しても，どんなアプリケーションのシステムの上で走っているのかも，新しいソフトの獲得に関しても，ソフトをいかに今日のオペレーションに組み込んでいくかもわかっていました。きちんと１人でコントロールしていましたから，多大な影響力を持っていたわけです。そして効果的に様々な問題に対処することができていました。しかし分散型のシステム構築が行われ，管理も分散化しますと，多くの人達が技術を運用管理することになります。しかし，その人たちが必ずしも技術について理解しているわけではない，という状況になってしまいました。技術的にますます解決が難しくなっただけでなく，今や問題に対処する責任が多くの人の手にまたがってしまった。しかもその人たちの技術に対する習熟度が様々であるからなおのこと厄介な問題になってしまったわけです。

全体像が非常に複雑化しております。侵入の検出システムというものが出てきましたが，現状の技術はまだまだそれほど進んでおりません。問題の解決策というのは，皆さんの方が先にしなければいけない，つまりベンダーの方が責任をとっているのではなく，皆さんが責任を持ってセキュリティに取り組まなければいけないのです。ということは，現在の状況というのは，使い勝手の良さということのエンジニアリング，すなわち，そもそもこの技術の普及に一役かってきたエンジニアリングというのが，運用管理とか特にセキュリティの高い運用管理ということについては，まだ生かされていないということです。

普通我々が問い合わせを受ける場合は，システム管理者と話すわけですが，技術的なスキルというのは10年前の平均的なシステム管理者よりも劣っています。また，いろいろな組織にとってもセキュリティというのは，ポリシーと手順の問題だと考えがちです。しかし，技術というものはセキュリティのソリューションにあたって重要な要素です。セキュリティの監査を行うわけですが，我々自身が行ったり，あるいは外部の機関に依頼するものもありますが，ポリシー面はよく見ます。また手順面もよく見ます。しかし，テクノロジーを十分に見ていない場合が多いわけです。

組織においては，セキュリティというのはただ単にコストとしてのみ見られているのです。これは追加の経費と見られがちであって，企業の収益を上げるものではないと考えがちです。実際に脅威があるのであれば，それはどこかと聞かれる。しかし，正確なその問題の規模は把握されていないという問題点があるのです。

まず，セキュリティというものは，１回きりで対策をとるものではありません。常に現状をアセスメントしなければなりませんし，またどういった改善をしなければならないか

を，常に考えていかなければなりません。新しい脅威，新しい技術の台頭と共に運用面でその対策を考えなければなりません。それを繰り返し進めていかなければなりません。すなわち，セキュリティは長期的な投資として考えなければなりません。

それから，ユーザーの確認および認証というものが重要な部分です。もし，インターネットからリモートアクセスを認めている，そして再利用可能なパスワードを使っているのであれば問題は必ず起きてしまいます。

多くの企業におきましては，社内の人は企業内のすべてのものをアクセスすることができる。そして社外の人は一切アクセスが認められていない。オール・オア・ナッシングの解決策が多いわけです。しかし，誰が何をアクセスすることができるかという権限というものを考えなければなりません。社外に対する問題だけではなく，社内の問題に対しても考えなければなりません。

企業は，他の組織と共同作業を進めています。また合弁事業などが行われています。それからお客様のニーズとして特定のデータをアクセスしなければならないということがあります。そのため，多くの企業にとってはアウトサイダーであった人間が，今やインサイダーであるということもあるわけです。

責任所在の問題それから，違反をどう報告するか，組織の中で誰がセキュリティの責任をとっているか，それは意志決定をする人間なのか，ビジネスの人間が運用について意志決定権があるのか，アプリケーションをどのようにユーザーに提供するか，どういうサービスをお客様にネットワークを経由して提供するのかということです。もし責任の所在さえはっきりしていれば，かなりいい状況だと思います。というのは，運用面での意志決定をする人たちが，そういう責任を持っている人たちということになるわけですから。

セキュリティの責任とそれから運用面での責任をマッチしなければなりません。責任の所在というものは，権限を伴なうようにしなければなりません。

もう１つの点として考えなければならないのは，違反の報告です。情報セキュリティの運用にあたって重要な点として，もしポリシーの違反があった場合，意図的，あるいは事故で起きた場合，あるいは知らずに起きた場合を問わず，そういった違反というものは必ず組織の中の誰かに報告しなければなりません。そして対策がとれるようにしなければなりません。慎重にどういう対策をとるかということを考えなければなりません。違反が発生した場合に，もし懲罰を加えるということになれば，おそらく違反の報告を受ける可能性というものは少なくなります。

重大なトレーニングを行ったり，対策をとったり，もっと多くの投資をしなければなりません。ただ単に個人に対して罰を加えるだけでは不十分です。

もう１つ非常に難しい問題としてどうやって物を購入するかということです。

多くのビジネスのオペレーションというのは，市販されているソフトを使っています。お客様として我々の方では直接ベンダーに対して変更を依頼することができない状態になっています。そのために何を買うかということを考える場合に，ソフトを評価し，そしてそれをどう構成するか，どうインストールするかを理解しなければなりません。それはベ

ンダーの問題でなく，お客様の方でやらなければならない。この問題にも注目しなければなりません。

また，重要な問題としてアウトソーシング，外部委託です。外部委託をする場合には情報の運用にあたって，契約上調査する手段を確保しておかなければなりません。セキュリティ面の監査ができるようにしておかなければなりません。内部的に情報システムを分割するかということで，例えどこかが攻撃を受けてもいかにそれを封じ込めるか，あるいはくい止めるかということです。いろいろな組織や会社がこの周辺には大変目を光らせるけれども，内部にはとても統制が緩いという場合，この外の壁が破られてしまえば完全にこの攻撃に対して弱くなってしまうわけです。ですから内部をうまく区分しなければなりません。ユーザーや顧客に使わせるソフトに関しては必要なものは提供するけれども，必要以上のものを提供してはなりません。

システムを導入するにあたって，常に新しいセキュリティシステムに目を向けておくということ，変更があれば，例えば新製品に関して，また新しい脅威に関しても常にそういった情報収集に努めて下さい。そうしないと効果的に問題に対応できません。またよく見落とされがちなものが，大きな企業，組織において十分なトレーニングを行っていないという点があります。単にユーザーに対するトレーニングだけではなく，マネージャーとかシステム管理者に対するトレーニングが不十分です。多くの責任をこのシステム管理者の方に対して与えておきながら一方，その難しい仕事をこなすうえでのサポートが不十分なのです。

セキュリティに対する意識を常に組織全体で高めていくということが必要です。

最後にセキュリティの問題は，仮に起こりうるということではなくて，現実に起こっている問題だということ，しかもその結果代償はとても高くついてしまうのだということです。ですから皆さん是非セキュリティをもっと投資の対象となるものだと考えて下さい。その見返りがある。それからセキュリティというのは，ある１つの状態，つまりあるかないかというものではなくて，常に変化するプロセスであるということです。技術や脅威の変化，内部の業務の変化にも常に目を向けて下さい。またシステムに接続している人たちの関係にも常に変化が起こっているということを理解して下さい。そしてその理念としては，長期的な取り組みが必要だということです。短期的にこの問題に取り組めば，すべて解決できるというものではありません。JPCERTその他，様々な組織で取り組んでいるところとも，常に連絡を取り合って下さい。そしてそれによってより低いコストで利益をあげることができるように努力なさっていただきたいと思います。

パネルディスカッション

コーディネータ	石田 晴久 氏	東京大学名誉教授 JPCERT／CC（コンピュータ緊急対応センター）代表
パネリスト	デレク・K・シンメル 氏	米国CERT／CC 技術担当
	山口　英 氏	奈良先端科学技術大学院大学助教授 JPCERT／CC運営委員会委員長
	牧野 二郎 氏	弁護士 インターネット弁護士協議会代表
	ビル・ハンコック 氏	Network-1 Software & Technology 社 筆頭副社長兼技術担当最高責任者

コーディネータ
石田　氏

最初にアメリカCERTのデレク・シンメルさんに，２番目にJPCERTの運営委員会の委員長をやっておられます奈良先端科学技術大学院大学の山口先生から日本の状況についてお話をお伺いします。つぎに今朝お話がありましたハンコックさんから話し足りなかったことをお話し頂いて，それから牧野先生からやはり言い足りなかったことを追加してお話頂こうと思います。その後に皆様方からいくつか質問をいただいていますので，その質問を中心に議論したいと思います。それでは最初にシンメルさんからお願いします。

パネリスト
シンメル　氏

CERTコーディネーションセンターで何をやっているのかをご紹介致します。また，ネットワークシステムのサバイバビリティプログラムについてもご紹介いたします。

はじめに，CERTコーディネーションセンター（CERT／CC）ですが，1988年に発足しました。有名なインターネットワームという問題がありまして，それに応えるために出来たものです。役割としては，まずインターネットにおけるセキュリティ上の緊急事態に対応すること。セキュリティの報告についての中心点になるということ。世界各地におけるこういった問題に対する対応に関して，あるいは同じような対応チームの活動を助ける上でのモデルになっていく。それからセキュリティの問題についての意識を高めていくというものです。

今では70以上の関連レスポンスチームがあります。アメリカの国防総省の中には５つのチームが存在しています。インターネットの関係者の間での意識を啓もうするというのも重要な任務です。システム関連者，その他多くの人達に対して公の形でインターネットにかかわる管理の問題についてのコースを提供したり，ワークショップを行ったり，あるい

はチュートリアルといったような形での意識の啓もうに努めています。

この１年の間，我々の気付いた事から申し上げますと，残念なことですが，まず第１に被害額というのが増えています。大体インターネットの成長率と同じような伸びで報告されています。また，侵入者の技術レベルが上がっています。侵入者は常にOSについて，あるいはプロトコルの弱点について学んでいます。そして新しい攻撃方法を考えています。ですから，我々の方も常に目を光らせて十分な時間とお金をかけて自らの防護策を講じていかなければなりません。侵入者はまた単にOSについての知識を深めているだけではなく，ネットワークのトポロジーですとか，あるいはその運用についての知識を構築しています。また侵入者は自動化を活用しています。侵入者は素晴らしいツールを持っていて，ただ単に侵入が迅速に起こるというだけではなく，新米の侵入者であってもこうしたツールにアクセスが取れれば，熟練した侵入者と同じように侵入してしまうのです。

侵入者の方はますます自らの行動をうまく包み隠すようになっています。優れたツールキットを持って，我々が防護策を講じれば講じる程，同じような技術を敵も使っているわけです。システム管理者の方がある特定な挙動を明らかにするために使っているものを活用して，侵入後，そのプログラムをすぐに偽物のバージョンで置き換えてしまう。そして自分の行動を隠してしまうわけです。また，自分たちのデータを隠すために暗号化も行っています。

それから，インターネットサービスプロバイダーに対する攻撃，およびネットワークのインフラそのものに対するアタックが増えています。ドメインネームとか，そういったものがどんどん攻撃の対象になっています。その他にも困った点があります。１つはベンダーの側においてセキュリティの改善があまり見られないということです。つまり，新製品が出されても必ず新しい弱点が見つかります。しかも，同時に古い問題も再度顔を現わします。つまり，前のバージョンの改良点が，新しいバージョンには入っていないということがあるのです。また，どうも総合的なセキュリティのソリューションは出てこないように思われます。現在，有用なツールはありますが，しかし問題の一部に対応しているだけなのです。

ベンダーの方は余り高い金をかけて，セキュリティの管理がしやすいものを作ろうとしません。つまりシステム管理者にとって，仕事がしやすくなる使い勝手の良いソフトというのは重視されますけれども，しかしセキュリティの方はまだまだ難しいままです。

次に，情報インフラがますます複雑でダイナミックになっています。つまり複雑な環境の中ではセキュリティを一貫した形で適用するというのが難しくなっています。異機種の環境の中で，様々なネットワークタイプ，様々なOS，そして様々なハードが存在している中において，１つのソリューションあるいは，少数のソリューションを多種多様な環境に適用することはとても難しくなっています。

一方，残念なことに十分熟練したシステム管理者，深い経験を持っている，あるいはセキュリティについてのトレーニングを受けた人の数というのは，なかなか増えておりませ

ん。企業，組織がインターネットに対する接続を深めている中で，人材がそれに追いついていません。セキュリティに関する知識というのはやはり何と言っても現場で習得するものが一番です。にもかかわらず熟練した経験を十分持った管理者がなかなかいないのです。そこで96年にSEIにおきましては，もっとプロアクティブな形で積極的にこのセキュリティの面での努力を行っていくことにいたしました。ネットワークシステムサバイバビリティプログラムという名前で知られています。CERTはこのプログラムの中心になっています。

3段階の戦略がとられました。第1に，我々が持っている最大のノウハウを活かして問題を食い止め，そしてシステムを復旧できるようにしようというものです。これは短期的な対策ですが常に必要です。次の段階としては，最初に自らの防護ができるようにするというものです。そのためには，我々がこういった弱点分析から得られた，あるいは事例に対応した結果得られた知識を使ってセキュリティを改善するための実践やツールを設けていこうというものです。セキュリティを高めることで，でき得る限り速やかに防護を張る。そして被害が起こらないようにする。最終的には研究結果をもとに，生存できるネットワーク技術を作っていこうというものです。セキュリティを最初から頭に入れた形でエンジニアリングを行っていきます。

セキュリティの高いエンジニアリングとソフトウェアのシステム，実践を通して少なくとも前と同じ手には乗らないぞというようなシステムを作っていきたいと考えています。

コーディネータ　石田　氏

どうもありがとうございました。次に日本にもCERTがあります。山口先生，本職は奈良先端科学技術大学院大学の先生ですけれども，JPCERTの活動については中心的な役割を果たされています。日本でどういうコンピュータ犯罪が起きていて，日本のCERTがどういう対応をしているのかということについてお話しをお願いします。

パネリスト
山口　氏

奈良先端科学技術大学院大学の山口です。JPCERTコーディネーションセンターの運営委員会のチェアをやっています。そういう関係からJPCERTの活動内容をご紹介します。どんなことが今，行われているのかというようなことをお話します。全体に多分JPCERTのことを知っている方はまだまだ少ないと思いますので，その歴史的な所からお話したいと思います。

まず，制度上の話ですが，コンピュータの不正アクセスということに，行政は何をやったかということですが，通商産業省が，昨年の8月にコンピュータ不正アクセス対策基準というものを作りました。基準を出すということ自体なかなか大変だったんですけれども，出したらそれで良くなるかというと，良くはなりません。出すだけでは駄目で，それを実施して問題がある所は何か，というのを明らかにしなければなりません。そして，何かトラブルが起きた時にそれに関する情報を正し

く流通させて，それで国内のインターネットに接続されている組織の管理者，あるいはそこに携わるマネージャたちがそれを認識して対策を立てる，という一連の動きがないとなかなかネットワーク環境は良くならないわけです。

もう1つとして，トラブルでは，どういうことが起きていて，そしてそのトラブルに対してどういう対策を立てたらいいのか，どういったことが助けになるのかということを支援する組織を昨年，96年中に設立をしたわけです。これがコンピュータ緊急対応センター（JPCERT／CC）です。通産省が基準を発表するのと同時に組織を設立しまして，10月1日より，すなわち今から1年前に活動を開始しました。

トラブルが発生した時にどうアクションをとればいいのか，場合によってはあるソフトウェアが関連しているとなったら，そのソフトウェアベンダーと話して，その対策を作ってもらう活動が必要なわけです。そういったコーディネーションをやっていく役割として，アドバイザリーグループというのが活動しています。

現在の活動内容は，基本的に不正アクセスの情報を受けつけて，その情報をもとに被害状況を把握し，技術的に見てどういう手口を使ったのか，という侵入手口を解明し，もしもそれに新しい対策が必要ならばそれを作るということをコーディネーションしていく。あるいは，ある特定の手口のものが広くいろいろな所で使われているのであれば，国内のインターネット全体に対して，今こういうことをやる人が沢山いるので気をつけるようにというアラートを出す，というような活動をしています。これがいわゆる不正アクセスに対する対応になります。もう1つは，それだけでは駄目で，セキュリティ技術の啓もう啓発活動が必要でして，これは今のインターネットの中で使われているツールのセキュリティパッチや，あるいはインターネットの運用上で役立つツールなどがいろいろあるわけですけれども，こういったものに関する情報を集めて，正しく管理者あるいはオペレータに対してサーキュレイトしていくということですね。あるいは，CERTアドバイザリーのように我々からも，こうすると対策が立てられますよというような文書を出したり，あるいはいくつかの技術資料を出したり，セミナーを実施するというような活動をしています。

現在，国際的観点から見た関係組織との関係確立というのが必要でして，日本で起きている事は日本でクローズしているわけではないし，米国にいるイントルーダーが日本のシステムに入って来ることがあったり，あるいは逆の場合もあるわけです。どうしても連携プレーというものがどんな場合でも必要になる。どうやって協調して活動して行くのがいいだろうかということを考えています。

JPCERTは，完全にニュートラルな立場を守っています。どういう意味かと言うと，例えば警察とか，司法機関，政府，あるいは企業，ある特定の企業からの影響を受けないで，インターネットにおけるセキュリティの問題を技術的にバイアスがかからない状態で考える組織として動いていくようにしています。もちろん，これは国家機関でもありません。営利を目的としている機関でもありません。それからもう1つ，JPCERTはインターネットの警察だ，みたいなことを書いたメディア

の方々もいたんですけれども，我々は警察機構の下部組織でもありませんので，司法権限は一切持っておりません。我々の立場というのは任意の団体であって，セキュリティのトラブルに関しての情報を収集し，そこで技術的な観点からその解析を行って，必要な人に対して必要な機関に対してその対策の情報を出していく。そういうインフォメーションセンターとしての役割が一番大きなものになっています。不正アクセスを受けて問題を抱えている人と，その問題を解決できる人，それをどう橋渡ししていったらいいのか，センターとしての一番大きな目的はそこにあるわけです。

さて，それで日本国内ではどういう傾向があるかということですが，依然として古典的な電子メールのアタックですね。それからニュースサーバへのアタックとか，パケット盗聴を行うとか，非常に古典的なトラブルが今だに沢山行われています。これらのトラブルというのは，ソフトウェアのバージョンを上げることで結構対策はとれるのです。しかし，企業ではなかなかソフトウェアのバージョンアップができない。古いソフトウェアを使っているシステムが多くて，これを徹底して狙われているというのが今のところ日本の現状です。それから最近問題だなと我々が思っているのが，ダイレクトメール的に膨大な量の電子メールを出すというサービスをやっている人達がいます。が，sendmailがハングったりですね，システムがハングるということがすごく多くて，これに対しても我々は問題だと思っています。

不正アクセスを行われるということは，直接的な被害もあるわけですが，それ以外にも一旦どこかのシステムに入って，そこから他のシステムにアタックをかけるという，踏み台に自分がなってしまって，他の人にも迷惑をかけることもあるわけです。ですから，自分の所は別にセキュリティのことに関して気にしてはいない，壊されるのなら壊されてもいいよ，ということは非常に我がままな意見になるわけです。人に迷惑がかかることがあるわけですから，そういった意味でネットワークに繋がるところである程度きちんとしたセキュリティマネジメントを行って，自分のリソースを守っていく。そして，人にも迷惑をかけないようにするという常識をそろそれ持ってくれたらなと思うわけです。

不正アクセスを受けたサイトとか，何かおかしいぞということがあれば，その連絡先と何が起きたのかということ，それからどういうことをやられたのかということを是非ともJPCERTにご連絡して頂きたいですね。その情報が他のサイトのアタック防止に繋がったり，あるいは皆さんが不正アクセスを受けた時の原因解析の助けにもなるわけです。

我々は，できないことは沢山ありまして，例えば事件の捜査はできませんし，あるいは犯人は誰かと特定することは我々の仕事ではないわけです。これは司法当局がやればいい話であって，我々はできない。あるいは証拠物件を強制的に押収して保全してくれと言われてもやっぱりできない。あくまで我々は情報センターという立場です。それから損害賠償請求したいから法律面で支援してほしいと言われても，我々は法律家の団体ではありませんので，これはプロの弁護士，牧野先生とかがヘルプする人になるわけです。

将来構想ですけれども，今後共国際的な協

力というのは必要でして，例えばAPCERTというアジアパシフィックにおけるCERTの機能を持った組織の設立に我々は協力していく。それ以外にも各国のところと，例えばファーストというようなIRTのフォーラムの場でですね，意見交換をしていくというような活動も積極的にやっていく。もう１つは運営基盤の強化です。我々のサポーティングメンバー，会員を募ってですね，そこからの資金援助も受けながら，ずっとこの組織が日本できちんと活動していけるような体制にして行こうと考えています。会員制度ということをやるにしても，ニュートラルの立場を守っていかないといけない，というところが我々の悩みです。そういう中で今JPCERT／CCの会員制度導入というものを考えています。多分，募集開始をするのはおそらく年末12月くらいにアナウンスをかけて，年度中に第１次会員募集を終えるというように考えているわけです。それに関してはoffice@jpcert.or.jpの方にメールをして頂けると嬉しいです。我々からの情報の発信場所というものがあります。我々もウェブサイトを使っていて，URLに行くとですね，最近の不正アクセスの傾向からそれに対してどういう対策をしていったらいいのかとか，技術的なドキュメントを公開しています。それから，情報提供用のフォームを用意しています。是非このフォームを使って何かあった時には連絡して頂きたい。コンタクトはinfo@jpcert.or.jp（電子メール）です。

何か不正アクセス系の問題があれば是非コンタクトして頂けると幸いです。

コーディネータ　石田　氏

ただいまのJPCERTからのお願いについては，私も関係者の１人ですので，重ねてお願いですけれども，日本では従来，自分の会社のコンピュータ，あるいはネットワークがアタックされたという場合に，関係者の方がひた隠しにするという傾向がどうもあるんですね。やはりやられたということは恥である，というような考えがあって，隠されちゃうんですね。隠されますと対策の立てようがありません。是非隠さないで頂きたい。JPCERTでは，届け出頂いた場合にプライバシーは完全に守るようになっていますので，どこの会社がアタックされたかというような名前は決して言いません。内容だけで，こういうアタックがあったので，こういう対策を立てて下さいというようなことです。プライバシーは絶対に守りますので是非積極的に届けて頂きたいということですね。それから来年の４月からは独立採算でやらなきゃいけない。会員募集ということになるんじゃないかと思います。その時は，積極的に会員になって頂ければ有り難いと思っています。

次は，招待講演をされましたハンコックさんからまた別の観点から，特にネットワーク犯罪の対応という視点から少し付け加えて下さい。

パネリスト　ハンコック　氏

それでは，多少付け加えさせて頂きたいと思います。最初に，世界のトップにネットワークセキュリティに関する研修をしたい。既に4,300以上のネットワーク，そして450万以上のノードを抱えた大規模なネットワークを構築してきましたし，MCI，AT&T，スプリント，ブリティッシュテレコム等の仕事をしてきました。また，コンサルテーションも行っておりまして，これは監査の分野，それからペネトレーションスタディと呼んでいま

す。例えばハッカーが，友軍として入って来るわけですね。そしてどこに欠陥があるかを見極めるということをするわけです。これを商業的なレベルでもしていますし，全世界のいろいろな各省庁等でカスタマーサイドに入って来た場合に，その実態を調べてそれを省庁に報告する。そしてそれを取締り，また警察当局等の犯罪取締りに繋げていくようにしています。

また，フルサービスのセキュリティサービスをどこであれ，必要な所に提供します。1つ我々が心配していますのは，ネットワーク製品やセキュリティ関連の製品において，セキュリティの問題を独自に，自分で認識できるもの，つまり言われなくても分かるものが必要だということです。その結果，AIとかエキスパートシステムを考えました。現在製品について研究開発を行い，少し違ったものを侵入者検出システムにおいて実現しようとしています。AIを使う，これをネットワーク管理とセキュリティの双方に役立てます。というのも両者の間はもう微妙な一線で画されているに過ぎないからです。

コーディネータ　石田　氏

どうもありがとうございました。アメリカの場合にはこういうセキュリティ関係の仕事はもう立派なビジネスになっているんですね。日本の場合には展開するとすれば，日本だけではマーケットが小さすぎるかもしれませんけれども，これから日本でもいろいろな事故が起こるようになると案外ビジネスになるかもしれません。それから先程山口さんがアジアパシフィックとの連携ということを言っておられましたけれども，アジアパシフィックの国々と一緒に仕事をする。あるいはもちろん欧米と一緒にやると日本ベースのセキュリティビジネスも段々成り立つようになるんじゃないかなと思います。

それでは，4番目のスピーカとしまして牧野先生にお願いしたいと思います。牧野先生は先程いろいろな問題をお話しされましたけれども，多分まだお話し足りないことがあるのではないかと思いますので，補足をお願いします。

パネリスト
牧野　氏

郵政省が調べたインターネットプロバイダに対するアンケート調査というのがありまして，そこで非常に惨澹たる状況と言いますかアンケート結果が出ています。まず，専任のセキュリティ管理者はいますか，という質問に対して35.8%がいない。それからセキュリティ対策をしていますか，ということでファイアウォールをちゃんと取っているのは43.5%，半分に至っていません。半分のインターネットプロバイダはファイアウォールすら設置していない。それからソフトウェア面，あるいは運用面でセキュリティ対策を講じてますか，という質問に対して，異常の発生を速やかに検知できる機能を整備していると回答したのが36.7%，データの改ざんまたは盗用を防止する措置を取っているという回答は，26.6%ということです。言ってみればセキュリティのシステムがいくらあってもですね，実際にセキュリティの必要性を全く感じておられない。あるいはそういうシステムを作ろ

うとしていない企業が多すぎるということではないかと思います。

弁護士というのはどちらかと言うと，法制度などは作るなと，法律ほど良くないものはないというのが基本的な発想です。法律というのはどうしても動きが悪いですから，企業がきちっと対応しておればそんな物はいらんのだと思うんです。しかし，こういう事実を目の前に突き付けられると，私たちの個人的な情報ですとか，企業の重要なデータが集まっている部分でセキュリティが守られていないということになれば，法的強制力を導入するしか措置がないんじゃないかと思うんです。その辺もちょっと御意見頂きたいところだなと思います。

被害者の方から，私のパスワードとID番号が盗まれて，毎月の請求代金が30万，40万来る。それが発覚したので大至急何か対応したいのだけれどもどうしたらいいのだろうかと相談がある。この点に関しては，今現実に起きている事実に対してどう対処したらいいか，という点について法的な援助というものは全くないというのが実感ですね。そういう事態が起きた時に，我々はすぐに警察に被害届けを出しに行きなさい，と言うんです。警察が何を言うかというと，あなたの言っている事が嘘じゃないという証拠を持って来いと言うんですね。そんな証拠が出せれば，侵入者にとってはそれこそ自殺行為ですね。すぐに捕まえに行きます。それが出来ないから困っているから助けて下さいと言っているのに，証拠を持って来ないと警察は動きません。

そんな場合に，素人考えですけれども，パスワードを変えないでアクセスさせておけと。アクセスさせておけば何等かの形で，こちらがいい意味でのハッカーをお願いして，逆に追跡するということをやったらどうか。追っかけというか，泳がしと言いますか。

実際には事業者の方には電気通信事業法があって，通信プライバシーということもありますから，そう簡単に口を開かないという部分があります。それは義務ですから仕方がないことなんですが，一定の法的な制度を使うことによって，例えば仮処分とか，あるいは研究の証拠保全措置といったようなものを活用することで，対応すべきなのかなと考えます。

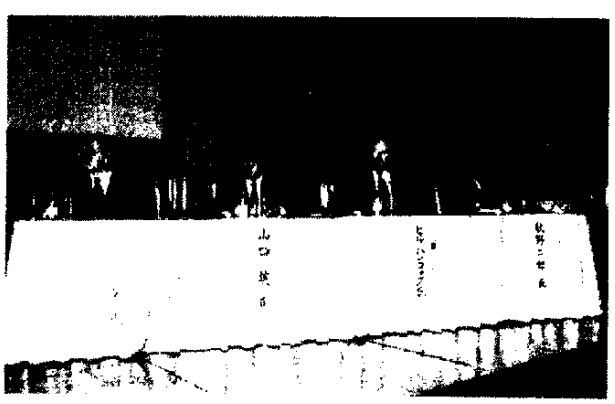
それからそういう被害が出た時に，本当に被害なのかどうかということを確認すべくですね，民間の追跡捜査と言いましょうか，証拠を挙げるとか，あるいはハッカーの集団が被害救済に立ち上がってくれるというようなことがないと，我々弁護士がきちっと法的対処をしましょう，と言ってもなかなか現実にはできません。警察が動くケースというのは，非常にエキセントリックな場合とか，あるいは何て言いますかマスコミ的に非常にヒットするような内容，これについてはすごく乗ってくれるのですね。か弱い女の人がいじめられたとか，ネットストーカーの問題だとか，それからわいせつ事件ですね。こういうものは目の色を変えて追っかけて来る。ところが，今申し上げたような実際の被害なんですけれどもよく見えない，というものについては非常に冷たい対応をする。その辺が課題かなと思っています。

不正アクセスとかセキュリティの問題をどうするかという問題で，日頃から法律相談等を受けている立場から言いますと，問題をこう分けて考えて貰えないかなというのが皆さ

んへのお願いなのです。消費者に対してセキュリティを求めることは極めて難しいだろうと思うんですね。本当にパスワードを変えられるだろうか。正直言って変えづらいですね。いくつもパスワードを持っているわけにいかないですから。そうすると全部のシステムを，パスワードを統一せざるを得ない。手帳に書いておけば手帳を落っことしたらどうするんですか，と言われますよね。手帳にも書けない。じゃ3つも4つもパスワードを覚えられますか。皆さんだって，キャッシュカードの暗証番号は，1つぐらいでしょう。そうなってくるとパスワードとかIDというのはアクセスのための制度であって，セキュリティシステムではない。だとすれば，パスワードとか，IDとかでセキュリティを求めて，それで消費者に責任転嫁するのは止めてほしい。むしろセキュリティ管理はファイアウォールのような形をとってきちっと対応させていく。将来的にはさらに進んだ認証制度というのでしょうか，署名等で個人を識別するというようなものを積極的に採用して頂いて，消費者を守るというようなシステムを作ることが必要ではないか。

それから，本当の素人でも自由に行けて安全であって，自分のパスワードが盗られても安全，というようなシステムを考えてあげる必要があるのではないでしょうか。ネットワークは危険だとか，あるいはインターネットは犯罪人の巣窟だというようなことをマスコミベースでどんどん流していく。それでセキュリティがないということを言っていたのではだめだろう。そうなって来ると事業者の方のよほど強い自覚がないとだめなのではないか。その時に事業者の自覚があって，自主的にきちっとした保護措置をとっておく。で，消費者はそれに安全に乗れるシステムを作る。そういう対応策をとらないと，消費者に対して危険だ，危険だと言ったら消費者は皆逃げてしまうわけです。

最後に，自主規制の問題ですけれども，いろいろガイドラインが出ています。注意しなければいけないのは，ガイドラインというのが日本の企業構造の中でいわゆるギルド的な縄張り，カルテルになってしまう危険が極めて高いということです。自主規制という意味をですね，よくよく検討して頂きたい。自主規制というのは，皆で一緒になって同じ規則を作って守るということではなくて，各企業，各事業体が自分の実力と，その持っているデータの重要性に応じて自主基準を立てて，それを守りきるということです。決して右見て，左見て同じことをやっておけばいいんですよ，というそういう無責任な体制ではないはずです。ちょっと気のついた事，言い忘れた事を申し上げました。



コーディネータ　石田　氏

牧野先生，どうもありがとうございました。今，牧野先生から非常に興味のある問題が提起されました。今まで論じられて来たネットワーク犯罪というと，企業に対してですね。

企業のシステムがアタックされたという想定ですけれども，今の話のようにエンドユーザと言いますか，コンシューマ，あるいは個人がこの犯罪の被害に遭うということが起きていますし，これから増えそうな感じですね。その場合にどうしたらいいか。

まず山口先生，先程牧野先生から問いかけがありましたけれども，さっきの話ですと30万とか40万円とかの請求書を貰っちゃった。誰かの不正行為のために。それをJPCERTに訴えて来た時に，JPCERTとしてはどうするか，あるいはそういう人はどうしたらいいのだろうか，という辺りはどのようにお考えですか。

パネリスト　山口　氏

基本的に企業からあるいは個人から来ても，我々の対応は殆ど変わりないです。技術的にどういう対応をしたらいいか，というコンサルテーションと共にですね，必要な機関は誰であるか。例えば，警察に訴えたいんだったら警察のコンタクトポイントを教える。それから問題解決のサービスを今求めているならば，そこの担当者なりそういったインタフェースを教える，ということまでがJPCERTとして出来るところではないかなと思います。救済というところまでは我々にはできない。個別ケースに深く入って行くこともちろん可能なんですけれども，個々のケースに全て深く入って救済措置までは我々にはできない。本当は助けたいと個人的にも結構思う時あるんですけれども，そこまではできない。限界を感じているのは事実です。先程牧野先生から言われたように，誰が救えるのかと考えると，警察は救えないし，JPCERTも多くの場合救いにくい。多分弁護士さんも救えなくて，結局誰も救えないまま日本は放置されていて，どうしたものかと皆考えあぐねているってところじゃないでしょうか。

コーディネータ　石田　氏

シンメルさんにもお伺いします。アメリカのCERTでも個人に対してどうこうというのはできないと思うんですけれども，アメリカでは，個人が被害に遭うという事件がどの程度起きているのか，それからどこか個人が訴える，あるいはヘルプを求める場所があるのかどうか，という点についてお話下さい。

パネリスト　シンメル　氏

アメリカにも同じ問題があります。一般の人々が簡単に救いを求めることはできません。我々の方からカスタム化されたセキュリティコンサルタントサービスを提供することはできません。しかし，もし誰かが被害に遭った場合，法的措置をとりたい場合，起訴したいということであれば，被害者の要請があれば私どもはできるだけ控え目に取締当局と協力します。私どもは，起訴する立場にはありません。また，個人に対するコンサルタント活動をしている組織でもありません。今現在は極めて難しいプロセスです。

アメリカで何をやっているかと言いますと，いかにして消費者を不正取引から防護することができるかということです。消費者保護というのは確かに大きな問題であります。多くの消費者は技術的に知識を持っていないわけです。そうするとなかなか苦労します。

セキュリティの不正取引ということになれば，ベンダーの耳を傾けさせるというのは個人であった場合には難しいわけです。どうやればいいかということは分かっていても個人

としては大変です。不幸なことに，個人のための組織というものがないわけです。セキュリティの問題に対処するための組織というのがないわけです。

アメリカにおきましては，金融機関の間でウェブをベースとしたクライアントサービスというものを提供しています。これは恐ろしいと私は思っています。さらに申し上げますと，アメリカにおいて税金を納めた場合には，ソーシャルセキュリティタックスというのがあります。これは社会福祉のためです。最近ソーシャルセキュリティの管理によりまして，ウェブサイトで3日間も出たわけですけれども，始めてから30分以内にハッカーが侵入しました。例えば，家を買うためにローンを確保しようとした場合，信用報告の機関というものがサービスを提供しており，正当な目的のためにそういうサービスがインターネットで提供されているのであれば，必ず既得権を持った人たちがそのようなサービスのアタックを仕掛けて来ることは想像できます。

コーディネータ　石田　氏

これは会場からの質問ですけれども，タイガーチームというシステムチェックがあるのですけれども，セキュリティレベルの向上にどう役に立つのか。それから日本の国内でそういうものを作った事例があるのかということです。ハンコックさんに伺いますけれども，タイガーチームというものはどういうものですか。何故そういう名前が付けられたのですか。

パネリスト　ハンコック　氏

タイガーチームというのは1800年代に遡るかと思います。かつて，ビルマへ虎を取りに行ったわけです。虎を捕らえにいく度に誰かが噛まれたり，あるいはけがを負ってしまい，回復しなければならないということで，虎を捕らえに行くチームを結成する場合，常にメンバー構成が違っていたということから，このタイガーチームという名前が付いたわけです。その考え方というのはセキュリティでもテクノロジーとして導入されています。すなわち非常にフォーカスを絞ったグループで，各分野の専門家がセキュリティの問題を分析します。そしてセキュリティの問題を解決します。あるいは既存のある環境のセキュリティ上の問題を監査するわけです。タイガーチームが何故重要かと言いますと，特定の事態あるいはポイント的な問題を直すために有用です。ファイアウォールを新たに入れた場合には，タイガーチームでどういった所に抜け穴があるか，ということをわざわざ指摘してくれるわけです。問題を解決することができます。しかし，タイガーチームは，企業全体のセキュリティを検討する際には余り役に立ちません。タイガーチームというのは全てではなく，ある特定の問題に目を向けるからです。

パネリスト　山口　氏

米軍およびその他の組織ではタイガーチームを使って戦術としてシステムチェックを行っています。ハンコック氏がおっしゃったとおりです。特定の問題を同定することはできます。しかしそれらは短期的なものです。長期的に，継続的にセキュリティの改善を図り，そのプロセスを維持するためには，もっと何が悪いのか知らなければならないし，またそれ以上にどうやってシステムの再設計を行うかということを考えなければなりません。そ

して，いろいろな問題からどう保護するかということを考えなければなりません。CERTのコーディネーションセンターでは，情報セキュリティの評価を行っています。システムをアタックするのではなく，我々の方では面接を行ったりします。組織の各レベルの人間を面接します。そうすることによって組織の方ではセキュリティのコミュニティ上の問題がどういう所にあるかということを理解できます。ユーザがもし怪しい状況を見た場合に誰と話せばいいか。独自に運用ができなくて誰に報告すればいいかということを分からなかった場合には，どんな高度な対策をとったとしても問題は発生するわけです。また情報セキュリティの評価の一環として，ネットワーク環境のキーの部分を見て，そしていくつかのテストを行います。そして特に弱い所を見つけ出そうとします。それを分析して，組織に報告しています。調査結果を提供しているだけではなく，面接から指摘された点も報告していますし，我々の経験をもとにして最も良い対策は何であるかということも提言しています。長期的なセキュリティの改善を図ることができるように手助けしようとしています。それはタイガーチームではできない作業です。

コーディネータ　石田　氏

日本での事例はありますか。

パネリスト　山口　氏

多分誰もやっていない。ただし，例えば新しいプロダクトを作った時に，そのセキュリティ関連のプロダクトだとそれをエバリュエーションするというプロセスの中で全然別のチームを用意して，彼等が徹底してチェックするというようなことをタイガーチーム手法というのであれば，それはもう至る所で行われているような気がします。ハンコックさんが言われたように，非常に限定された期間，限定されたエリア，特に新しいセキュリティプロダクトのエバリュエーションとか，チェックとか，そういった意味では非常に役立つと思います。

コーディネータ　石田　氏

次の質問，最初シンメルさんに答えて頂こうかと思うのですが，犯罪者，犯人が日本に来る，その人がどこか別の国にあるサーバを使って犯罪をした。それによる被害者がまた別の３番目の国に行ったというような時に，どの国が犯人を捕まえることができるのか。国際的に跨がった犯罪ですね。その扱いはどうなるのでしょうか。

パネリスト　シンメル　氏

一般的に申し上げまして，出発点として被害者の所在地です。侵入されたとします。第三国に被害者がいたとします。侵入者がどこにいるかというのが分かった場合に被害者はまず現地の警察当局と協力し，そして海外の警察と協力しなければなりません。この例におきましては，別の国にサーバがあったわけです。即ち，犯罪者はある２番目の国のサーバに侵入して，そのシステムを使って被害者の国のサイトに侵入したわけです。もし，自分がその真ん中にあったサーバのオーナーであった場合には，それは自分の責任になるでしょうが，適切な処置をとらなくて自分のシステムが利用され，他の人のアタックに利用された場合にはどうなるか。即ち，自分自身のデータ，あるいはリソースを保護するため

に，自分のシステムを保護するだけではなく，より大きなコミュニティのメンバーとしてシステムが利用されてしまうことを防止しなければならない。不正利用を防止しなければならないということです。

コンピュータそのもの，OS，あらゆるインターネットと接続されたものは侵入者にとって貴重な資源であり，これらを利用して別のサイトに対するアタックを掛けることができますし，本当に高度な侵入者というのは次々といろんなシステムを跨がって世界各地を回って，そして自分の身元を隠すようにしています。そのため，管轄という問題を考えた場合には，究極的にはその侵入者が誰であるかを判断できるかどうかにかかるわけです。そして被害者は現地の当局と協力して，国際協力をしてアタッカーを捕まえるようにしなければなりません。場合によっては，アタッカーの国においては，アタッカーがやったことは犯罪として見なしていない場合があるわけです。そうすると全く打つ手はないということがあり得ます。

コーディネータ　石田　氏

犯人は日本にいる日本人だとして，しかし日本では誰も被害は受けていないという場合，日本の扱いはどうなるのでしょうか。

パネリスト　牧野　氏

日本の刑法は，基本的には日本国民を守るためのものです。それから日本の国益を守るものとなって，日本人以外の者に対する侵害行為があったとすると，日本の刑法自体は基本的には適用にはならない。ただ，日本人の国外犯というのがありまして，例えば日本の通貨を偽造するとか，あるいは内乱罪というような重罪については，何人が犯しても日本の刑法を適用するというような規定があります。逆に見ますと，他の国の刑法，今おっしゃったとおり，被害者の国の刑法，あるいは刑罰法規でその国の人間でなくても処罰するという規定がある。いわゆる捜査協力，国際的な捜査協力を得て，逮捕するということになるのでしょう。その場合は海外の法律を使うということになるのではないでしょうか。犯罪によっていろいろ形が違うかなと思います。著作権法に違反したような場合は，ベルノ条約とか万国著作権条約で，著作権がどこのものであっても，自国と同様に扱うという規定もありますので，そうすると著作権侵害がどこで行われていても，その国がきちっと対応する。自国民と同様に取り扱うという規定もありますので，そういう類型にあてはまる犯罪であれば，日本の犯罪者を日本の捜査当局が逮捕するということもありうると思いますね。ようするに犯罪によってかなり異なるかなと思っています。

コーディネータ　石田　氏

次の質問は，ハンコックさんにお伺いしますけれども，アメリカの国防総省では，インフォメーション・ウォー・フェア，情報戦争の研究が進められていると聞いている。これが民間会社，証券会社とか銀行とか，あるいは情報インフラ関係の会社での対応はどの程度進んでいますか，またどのような対応が必要ですかというんですけれども，まず，そのインフォメーション・ウォー・フェアって我々あまり聞き慣れない言葉なんですが，これどういったものを指すんですか。

パネリスト　ハンコック　氏

これは国レベルでとらえるのと，企業レベルでとらえるのとは違ってまいります。この国レベルで情報戦争といいますか，これをとらえる時に国が他の国に電子的な戦争能力を持つ国に対して対戦をしかけるということです。例えば91年にイラク戦争がありましたけれども，襲撃が始まった時にレーダーの破壊のために電子的な措置をとって攻撃をしかけたわけです。

国レベルでその情報戦争ということが起こりますと，それは決定的に国の防衛，国防ということに繋がるし，また，技術的な能力があった場合には，攻撃戦争ということにも発展してしまうわけです。そしてその時にコンピュータネットワークが使われるということになります。しかし，企業レベルでのインフォメーション・ウォー・フェアということになりますと，2つのレベルが考えられると思います。どの程度に，どのようにして他社から自分を守っていくか，すなわち自分の機密情報をどのようにプロテクトしていくかということになると思います。もう1つは企業が他の企業を攻撃して，いわゆる産業スパイをして情報を入手しようとするような状況が考えられます。このようなことは実際起こりうるということを企業は認識しておくべきだと思います。それが起こった場合には戦略を持っていなければならないということだと思います。非常に良い本がでています。インフォメーション・ウォー・フェアというウィン・シュワルトさんが書いたものです。

ここで根本的なことは国レベルでのインフォメーション・ウォー・フェアというのは企業レベル，民間レベルのものとは全く違う。企業レベルということになりますと，大きな企業，シティーバンクとかロシアのマフィアに攻撃された銀行もあるわけです。その犯人を確定するまでにも非常に長い時間がかかった。資産の大きな大企業というものは，インフォメーション・ウォー・フェアというものを企業レベルで考えていかなければならない。企業として何ができるか，非常に特殊な分野ですから，一般的なというよりも，特殊な状況としてとらえていく必要があると思います。

コーディネータ　石田　氏

関連した話題としては，アメリカの国防ではマルチ・レベル・セキュリティというシステムが使われているというんですが，これ民間企業の場合に，そういうものが，必要なのかどうか，必要だとすると特にどの業種で必要なのかという質問なんですが。

パネリスト　ハンコック　氏

セキュリティということに関与している方は，セキュリティというものは高ければ高いほどいいと，そしてユーザーの怒りを買えば買うほどいいということ，つまり反発を受ける位のセキュリティは持つべきだということです。私から申し上げれば，企業ごとにセキュリティのレベルは変えていいと思う，リスクが違うのですから。しかし，いつもしなければならないのは，その基本的なリスクというものは確認しておくということです。ですから企業別に違う。

また1つ提案しておきたいことは，一体何を保護しようとしているのか，防御したいのか，第2の点としては脅威が何か，リスクが何かということ。セキュリティというものは本質的にマルチ・レベルであるべきだと思いますし，またその範囲としましては，例えば企業の規模であるとか，内容が何であるかに

よって変わってくると思います。

パネリスト　山口　氏

日本はどうなっているかというと，日本の企業は大企業がたくさんあるおかげで普通，マルチ・レベル・セキュリティを入れていて，それをやっていない企業は非常にダサイ企業で，クールではない企業と我々は認識している。それくらい，通常マルチ・レベルのいろいろな種類のセキュリティ・レベルを設定して，ネットワーク組みをやるのが，もはや日本の大企業の常識になっています。

コーディネータ　石田　氏

次の質問ですけれども，ネットワークの上でのソフトウェアの流通，そしてディストリビューション，これがこれから盛んになるだろう。その場合，心配なのはウィルスが入っていやしないか，あるいはシステム破壊プログラムがその中に入っていたらどうしようということがあるのですが，そういったもののセキュリティ確保についてはどのように対応していくのか，山口先生にお伺いしましょうか。

パネリスト　山口　氏

基本的に言えることは，まずは信用するしかないなってこと。売っているものは信用する。フリーソフトウェアは自分の責任で使うしかない。という原則があって，フリーソフトウェアでソースコードのないものは，手も足もでないんでやはりこわい。でソースコードのあるものは，少なくともチェックはできるから，まだましかな。これくらいです。オンラインの流通になると，例えばPGPのフットプリントをつけてくれたり，MDチェックサムをつけてくれたりするサイトも出てきているわけです。そういった技術がどんどん一般的になって行かないと，逆にオンライン流通はうまく行かないのではないかなという気はしています。

パネリスト　ハンコック　氏

ソフトウェアの流通の問題というのは，ネットワークでの流通ですね。ベンダーとしては，出荷する前にコードを必ずしもチェックするとは限らないということです。コンシューマーの方でベンダーへの圧力をかけることが必要だと思います。会計ソフトであれ，ウィルスワクチンであれ，Eメールであれ，いろいろなものに適用されるわけだと思います。といいますのは，コンシューマーの方からベンダーに対して圧力をかけてソフトウェアテクノロジーを入れるように，そしてソフトウェアと自ら保護するようにさせるべきであります。そうでなければ，ウィルスキラーのようなものをいれてもらわなければ問題は起こるわけです。ここでひとつするべきは，ベンダーに対しての圧力ということが1つ，必ず何かのメカニズムを考えてくれと，いうことです。山口先生がいったように，例えばPGPを使えとか，MD4，MD5のようなシチュエーションを提供してくれと，いうことでそこからスタートしていかなければいけないと思います。

コーディネータ　石田　氏

牧野先生におうかがいします。マイクロソフトのActiveXの製品だとこの製品はどこどこによって内容が保証されていますという，証明書がついてきたりするんですね。でもそれにもかかわらず，ウィルスが入ったような

時に，ウォーニングを出したということは，免責になるんでしょうか。

パネリスト　牧野　氏

今の段階ですと，ソフトに関するPLというんでしょうか，いわゆる製造物責任というものがはっきりしていないんですね。ですから警告を，契約上は警告をしたんだから，ダウンロードした時に契約が成立して，その契約条項を認めてとったんだ。そうなってくると，受け取った側には本当に安全かどうか全くわからない状態でそういう警告だけが流されて，あとはもう完全にリスクは消費者の負担でやるというような仕組みになっている。それについては疑問があるんですけれども，まだ十分法的に検討されていないし，法的責任というところでも，明確にされていないですね。本当にわからない状態で，言ったもの勝ちみたいな世界になっていると思いますね。

コーディネータ　石田　氏

最後に各パネリストからファイナルコメントを簡単にいただきたいと思いますけれども，シンメルさんと山口先生に大学関係ということで，もう１つ質問が出ているのですが。教育の問題ですね。セキュリティ技術者の育成というのはこれからの課題だと思うんですが，その辺どのように考えておられるかということを，ファイナルコメントにお願いできればと思います。まず，シンメルさんから，教育問題について一言お願いします。

パネリスト　シンメル　氏

我々コーディネーションセンターにおきまして，ワークショップなどを開催しています。管理および経営者レベルにおいてのトレーニングを行っています。主にこれらはセキュリティの認識を高めるためのトレーニングです。いくつかの商業活動を行っている企業が，細かいトレーニングを提供しているところもあります。そういった所を検討されたらいかがでしょうか。そしてシステムおよびネットワークの管理におきましても，また経営者に対してもそういったトレーニングを受けさせるというのはどうでしょうか。情報システムの管理をしているあらゆる人間がそういったトレーニングを受けられれば良いと思います。また経験ある人たちと，新米の人たちとの間で教育をするという制度を設けたらどうでしょうか。経験のある人たちが新しい人たちに対して，援助するということであれば，またいろいろなチャンスがあると思います。教育はいろいろな観点から努力をするべきだと思います。

コーディネータ　石田　氏

山口先生，日本ではどうもこの辺のところの教育がどうも手薄な感じがしますが，どうでしょうか。

パネリスト　山口　氏

教育に関しては，多分ユーザーに対するとか，学生とか，社員とかいろいろな立場の人，セキュリティの管理者，それからマネージャー，お金を握っている人たちに対する教育というのは全部必要で，日本の場合この３つとも結構欠けている部分が多くて，どれもやっていく必要があるのかなと思います。

今一番急務なのは，シンメルさんの発表の中にもありましたけれども，とにかく今セキュリティ・エキスパートがあまりにも少ないので，システムをどうセキュアにしていくか

というコンサルテーションすら十分に提供できていない。これは大学の立場で言うと，今の大学の教育，トレーニングのコースの中にはあまりにもできない部分が多い。これに対して民間の人たちはどうしたらいいのか，プライベート・セクターの人たちはどうしたらいいのかということは，結構問題だろうと思います。

我々大学からセキュリティをどうしていったらいいのかというのは，重要なポイントなので，今ほとんどの大学で行われているはずです。コースの中にほとんど組み込まれている。それは例えばネチケットという名前になっているかもしれないし，コンピュータ・リテラシーという名前になっているかもしれませんが，その中で行われている可能性が高い。

それからもう1つマネージメント層，エグゼクティブなマネージャー層をどう教育していくかというのは，日本の場合はほとんど行われていなくて，これは一番大きな問題だろうと思います。ようするにどれだけの投資をして，システムを守って，それによってどういう効果があって，会社として企業としてどういうメリットがあって，長期的に何を考えなくてはいけないかということを，日本の経営者たちはほとんど何も考えていないのではないかと思われる位，今のところ意識が低いと思うわけです。経済界がみんなして意識改革するのかよくわかりませんけれども，財界の人たちですね。これからも継続的に多分解決しなければならない問題がたくさんあるだろうと思っています。

コーディネータ　石田　氏

どうもありがとうございます。あと，ハンコックさんと牧野先生に言い足りなかったこと，ファイナルコメントをお願いします。

パネリスト　牧野　氏

結局，今の山口先生の話もそうだと思うのですが，セキュリティが弱い，セキュリティ対策ができていないでいろいろな問題が出てくると，どうしても最後には法律を作って，規制しましょう，責任を認めましょう，そして処罰しましょうという形にいかざるを得ないですね。私たちが思うのは，この世界というのは，非常に進み方が早いので，へたに法律を作ると経済の勢いを潰してしまう。

ですから情報インフラが成長するのにあわせて，きちっと対応できるようなシステムを考えなければいけないだろう。その時にアメリカ型というのでしょうか，財界がリーダーシップをとって自主規制なり自分たちの必要なソフトをどんどん作ってそれを実装していくというようなシステム，それで法律のガチガチな規制は避けていくという，非常に賢い選択ではないかと思うのです。

同じようなことを，はじめての経験だと思いますけど，日本の財界もやっていただかなければいけないのではないか。自力で自主的な規制，あるいは管理システム，あるいは，山口先生をそこらじゅうに呼んで，来ていただいて，徹底的な管理教育をする。

そういうことをやらないと，ガチガチの法律でみなさんをハッキングにあった場合に刑務所に入っていただくというような，非常にまずい結果になるのではないか。ですから法律を引き出す前に，もっと賢い選択をするべきだと，それが今我々日本人に求められている方向性ではないかなという気がしています。

コーディネータ　石田・氏

ハンコックさん，何か最終的なコメントはありますか？

パネリスト　ハンコック　氏

ほとんどの経営者というのは企業においては，セキュリティの問題がなくなればいいと思っているだけですが，決してなくなりはしません。そして他の技術同様ますます複雑化していきます。そして無視することによって，さらに悪化するだろうと考えられます。

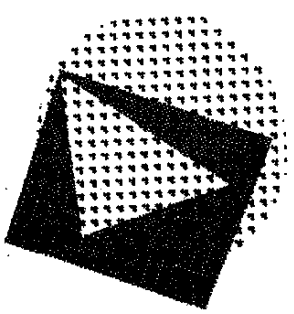
企業としてやらなければならないことは，セキュリティの脅威にさらされているということを認識して対策をとらなければなりません。なくなるだろう，決してうちではおこらないだろうという態度ではダメです。もし，我々がとりあげたような点というものを，検討して採用していった場合，セキュリティにおいて企業として相当進歩が見られるだろうということです。そうすることによって，我々の助けを必要としなくなるということが考えられます。ハッカーのアタックがあっても，防止できると思います。

いずれにしても，責任の所在，そして権限というものは，セキュリティの時代においては，はっきりと確認しなければなりません。企業としてはセキュリティというのはただ単に自動的に発生するのではなく，セキュリティを確保するための努力をしなければなりません。毎日取り上げなければなりませんし，なくなりはしないということです。そして放っておけばより大きな問題に発展していくことです。

コーディネータ　石田　氏

どうもありがとうございました。今まで日本は非常に安全な国ということで，セキュリティに関する関心が一般的に低かったと思うんですけれども，インターネットの場合はこれからユーザーが非常に増えてきて，しかも国際ネットワークになっていて，外国からでも誰でも日本に入ってこられる。あるいは日本のシステムを踏み台にして悪さをするなんてこともありますので，そろそろ我々としても，真剣にこのセキュリティ問題に取り組まなければいけないと思うんですね。したがってこのパネルを機会に皆様方にもっと考えて，関心をもっていただけるとありがたいと思います。

これをもって，本日のパネル討論を終わりにしたいと思います。最後にパネリストの方，および質問をお寄せいただいた方，それから熱心に議論を聞いていただいた皆様方に，全ての方に感謝したいと思います。本日はどうもありがとうございました。



高度情報化人材育成標準カリキュラムの改訂について

中央情報教育研究所

当協会中央情報教育研究所（CAIT）では，平成５年12月に作成した高度情報化人材育成標準カリキュラム（以下「標準カリキュラム」，全17種）を，その後の情報技術等の進展に合わせるべく改訂し，平成９年10月15日に公表しました。

標準カリキュラムは，高度情報化社会において求められる情報処理技術者の類型（平成４年に通商産業大臣の諮問機関である産業構造審議会情報化人材対策小委員会が策定）に従い，各人材を効果的，効率的に育成するために作成したもので，現在，専門学校をはじめ各種研修機関等において，このカリキュラムに準拠した教育が実施され，教育カリキュラムと評価制度の一貫した人材育成システムとして，「情報処理技術者試験」（「情報処理の促進に関する法律」第６条に基づく国家試験）が行われています。

なお，標準カリキュラムの改訂に伴い，情報処理技術者試験（現在13の試験区分で実施）は，平成10年10月（予定）の試験（秋期試験）から改訂された標準カリキュラムに準拠して実施されます。

1. 標準カリキュラムとは

平成４年12月，産業構造審議会情報化人材対策小委員会は，その中間報告において，今後わが国が安定的な経済成長を図り，豊かな国民生活を実現していくためには，新情報革命ともいうべき情報化の飛躍的な推進が不可欠と指摘するとともに，その担い手となるべき「システムアナリスト」等10種の新しい情報化人材像と，それらの人材を効果的に育成するために解決すべき課題と対応の基本的な方向を提言しました。平成５年５月の同委員会における最終報告では，これらの新情報化人材の育成に向けた総合的な支援策，標準カリキュラムの体系，標準カリキュラムと連動した新しい試験制度のあり方，各教育機関の役割と連携のあり方が提言されました。

平成５年12月，CAITでは同提言をうけ，通商産業省の指導の下，「情報化人材育成カリキュラム委員会（委員長：影山 衛司・(財)日本情報処理開発協会会長（当時））」を設置し，提言に沿ったカリキュラムの検討を行い，全17種から成る標準カリキュラムを取りまとめました。

標準カリキュラムは，高度情報化社会において求められる高度情報処理技術者の育成を目的にしたもので，①専門分野に特化した高度なスキルを持った人材を育成するための「高度情報処理技術者育成カリキュラム」13種類，②その前段階である入社後１～５年程度の間に修得すべき基礎的な知識・実務能力の範囲を明らかにした「共通カリキュラム」２種類，③情報システムを利用する側の人材

の育成・指導に当たる「システムアドミニストレータ育成カリキュラム」２種類，の計17種類から構成されています（図１）。各カリキュラムの内容は，基本的に「実務能力をいかに修得させるか，そのために何を，いかに教えたらよいか」にポイントを置いたものとなっています。

平成６年度より，専門学校や情報処理技術者教育機関等において標準カリキュラムに沿った教育が実施されるとともに，平成６年10月より教育と評価の一貫した人材育成策として，情報処理技術者試験（国家試験）の出題範囲がこのカリキュラムに準拠することとなりました。

2. 改訂の経緯

標準カリキュラムの作成当時，５年先程度を見越した人材の育成を目標としていましたが，その後の情報技術の進展速度は予想を上回り，クライアント／サーバーシステムが情報システムの主流になるとともに，マルチメディア化，ユーザーインタフェースおよびインターネット／イントラネットなどのネットワーク環境等が著しく進展し，またこれに伴いパソコンも急速に浸透しました。

このような情報技術の進展との整合性を図る観点から，また，人材育成の評価としての情報処理技術者試験（国家試験）が本カリキュラムに準拠し出題されていることから，５年を待たずして一部を見直すこととし，平成８年12月，CAIT内に「標準カリキュラム調整委員会（委員長：上條 史彦・東海大学教授）」を設置して，情報技術の進展に合わせるべく改訂作業を進めてきました。

今回の改訂は，情報技術の急激な進展に伴い，所要の改訂を行うべく，以下の基本的な考えの下に行いました。

①高度情報化人材類型，標準カリキュラム体系は現状を前提とする。

②標準カリキュラムとして示すべき技術，利用環境を最新の状況に合うように追加・更新する。

③カリキュラムの利用経験を踏まえ，以下のような事項についても改善する。

・教育目標，学習目標
・章，節等の記述の順序
・講義や演習の学習時間
・指導上の留意点
・参考文献　等

なお，教育エンジニア育成カリキュラムなど４種のカリキュラムについては，改訂を行っていません。

3. 改訂の主なポイント

今回の標準カリキュラム改訂の主なポイントは次のとおりです。

①パソコン，インターネット，グループウェア等の普及に伴う関連技術の見直し

②構成や表現の見直し，重複内容の整理，用語の統一，他カリキュラムとの関連の調整，学習目標・学習時間等の見直し

③開発工程，成果物名等の見直し

④システム監査基準等各種基準・規格等の改訂に伴う見直し

4. カリキュラムの頒布等

改訂された標準カリキュラムは次のとおり頒布を行います。

①頒布開始：平成９年11月20日

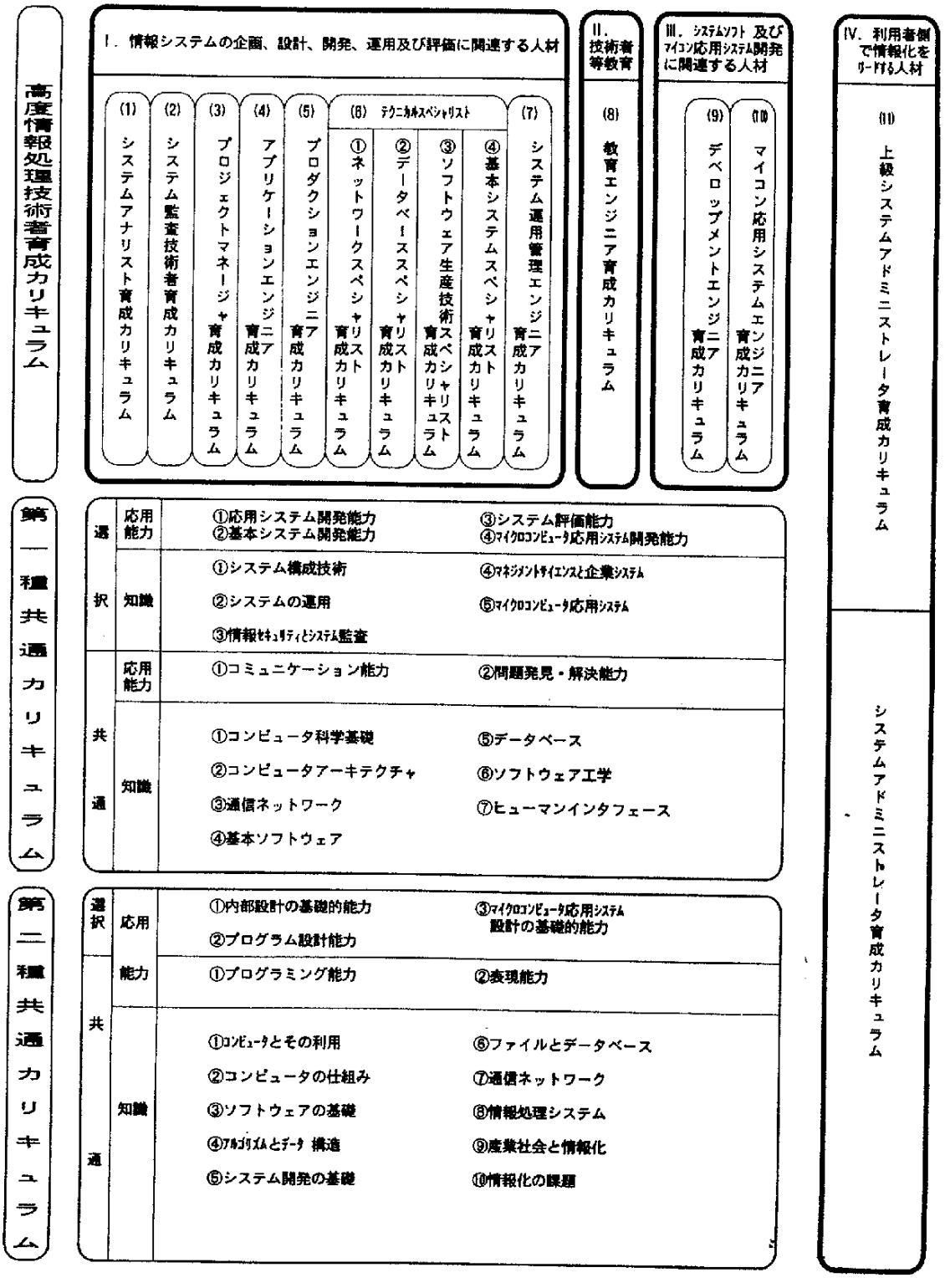
②媒体：CD-ROM for Windows（17種収録／枚）

③価格：12,000円／枚（税別）

また，標準カリキュラム改訂についての説明会を研修（有料），地域交流セミナー（無料）として，通産局所在地を中心に平成９年11月～平成10年２月にかけて行う予定です。

なお，申込み等に関するお問い合わせは，中央情報教育研究所・普及振興課（TEL：03-5531-0177，ホームページURL：http: //www.interport.ne.jp/cait/）までお願いいたします。

▼図１　標準カリキュラム体系図



システム監査白書1997-98年版の概要

情報セキュリティ対策室

このたび「システム監査白書97-98年版」を11月14日に刊行しました。本白書は，システム監査の普及啓蒙の一環として，わが国におけるシステム監査の実態，国のシステム監査関連施策，現在の情報化環境に対するシステム監査の必要性について取り上げています。

本白書の構成は，以下のとおりです。

第１部　システム監査関連施策

情報化の進展により情報システムと社会全般のかかわりが深まるにつれ，当然のことながら情報システムに対するリスクもますます深刻化してきています。このような情報システムのより一層の利用促進を図るため，通商産業省ではこれまで多くのセキュリティ関連基準や制度を制定してきました。本編ではシステム監査基準をはじめ，これまで制定されてきた各基準，制度について概要をとりまとめています。

また，平成８年に改訂されたシステム監査基準の内容，システム監査台帳制度の動向，システム監査技術者試験制度の活用方法について詳しくとりまとめています。

第２部　情報化環境の変化とシステム監査

本編では，2000年問題，情報共有化，電子商取引等，最近の情報化環境とシステム監査のポイントについてとりまとめています。

第３部　システム監査実態調査

本調査は，若干の調査項目を除き，１年おきに実施している継続的な調査です。調査対象を監査部門と被監査部門（情報システム部門）とし，システム監査の実態，情報化一般，2000年問題，コンピュータ不正アクセス対策等について意識調査を行い，分析しています。

資料編

本編では，実態調査の集計結果，現在策定されているシステム監査関連の基準，規則等を網羅しています。

今回は，西暦2000年を２年後に迎え，コンピュータの「2000年問題」の解決が早急に迫られている中，被監査部門（情報システム部門）および監査部門が2000年問題にどう対応しているのか，実態調査の分析結果をご紹介します。

1.　被監査部門の対応

各企業が2000年問題にどう対応しているか，監査部門および被監査部門に対し調査を行った。

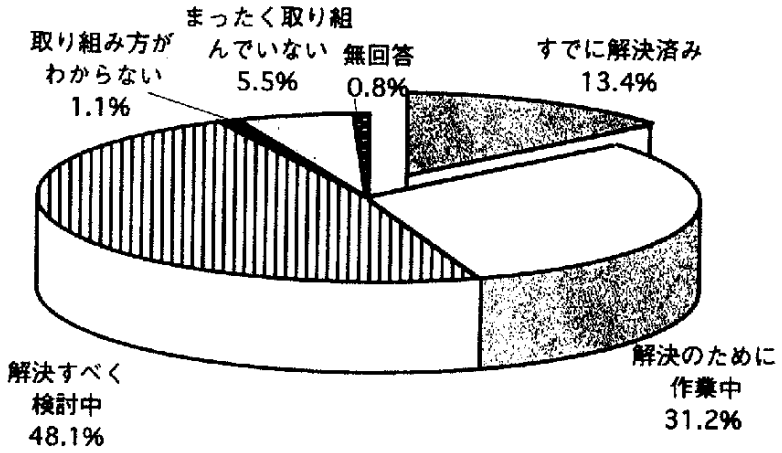
(1) 被監査部門の対応状況

被監査部門では調査時期（96年12月時点）ですでに「問題解決している」企業が13.4%，「現在作業中」31.2%，「検討中」48.1%と，

ほとんどの企業が何らかの解決策を講じており，2000年問題が情報処理部門にとって重要な問題であることがうかがえる。

しかし，解決しなければならないとの意識を持ちながらも，具体的に作業に取り組んでいない企業や全く取り組んでいない企業が約5割を占めており，2000年問題への対応が遅れていることがわかる。

図1. 2000年問題の対応状況（被監査部門）



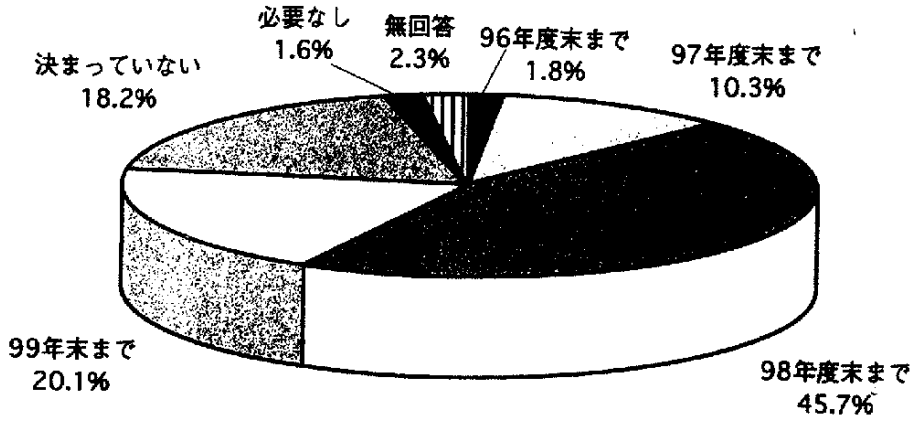
(2) 問題解決の完了時期

2000年問題の解決をいつまでに完了すべきかについては，「96年度末」1.8%，「97年度末」10.3%，「98年度末」45.7%という結果となった。これにすでに作業完了済みまたは必要としない企業1.6%を合わせると，59.4%の企業が98年度末までには作業を完了していることとなる。

しかしこれはあくまでも計画であり，実際にテスト，移行段階において支障がきたすおそれがあることを考慮すると，スケジュールに余裕を持たせておく必要があろう。なお，作業が集中するであろう98年度には，要員確保の困難が予想される。

しかし，「99年度末まで」（20.1%）と期限間際まで作業を予定している企業，具体的に「決まっていない」（18.2%）企業については，期限内にすべての問題を解決できるのか不安が残る。

図2. 2000年問題の解決時期（被監査部門）



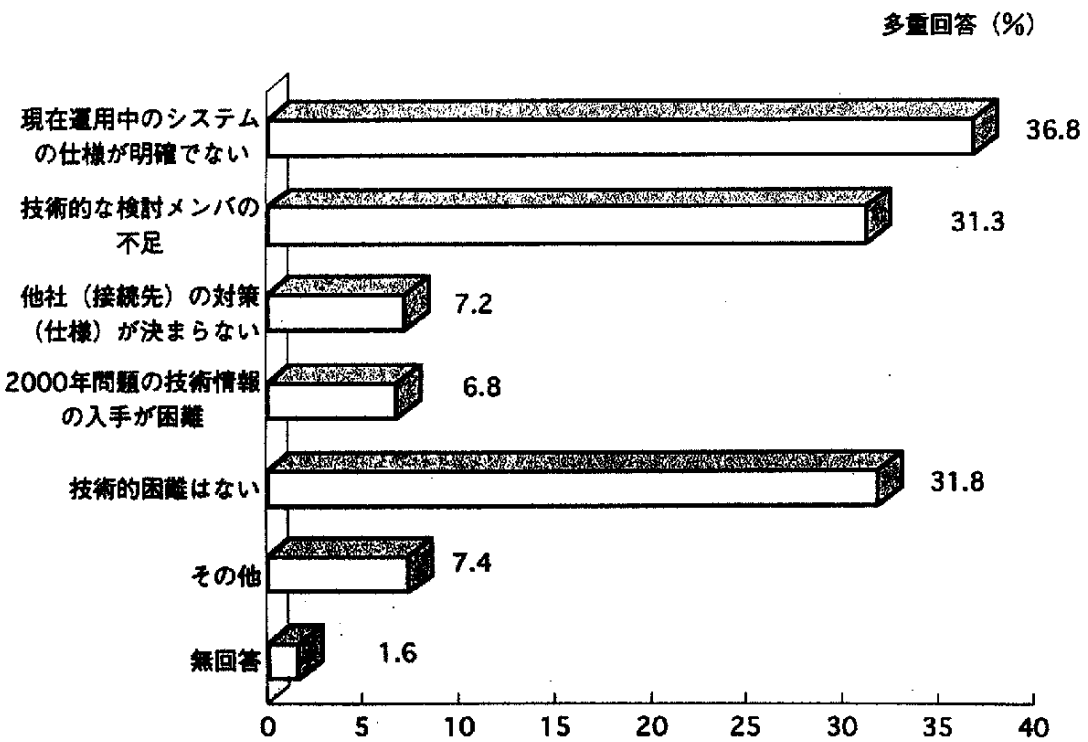
(3) 技術的問題

2000年問題を解決する上での技術的問題について，31.8%の企業が「技術的困難はない」と答えているが，反面，「運用中のシステムの仕様が明確でない」(36.8%)，「技術的な検討メンバの不足」(31.3%)，「他社（接続先）の対策（仕様）が決まらない」(7.2%)，「技術情報の入手困難」(6.8%) と，今後の解決がスムーズにはいかないと考えている企業が多いことがわかる。

特にシステム仕様が不明確ということは，システムの修正作業に要する費用，工数の算定がつかず，今後の作業に影響を及ぼしかねないことであり，早急に解決すべき問題である。

その他の意見としては，「対応工数が定まらない」，「テスト環境」，「各部署で各導入している小規模システムへの対応」等の意見があった。

図3. 2000年問題解決にあたっての技術的困難（被監査部門）



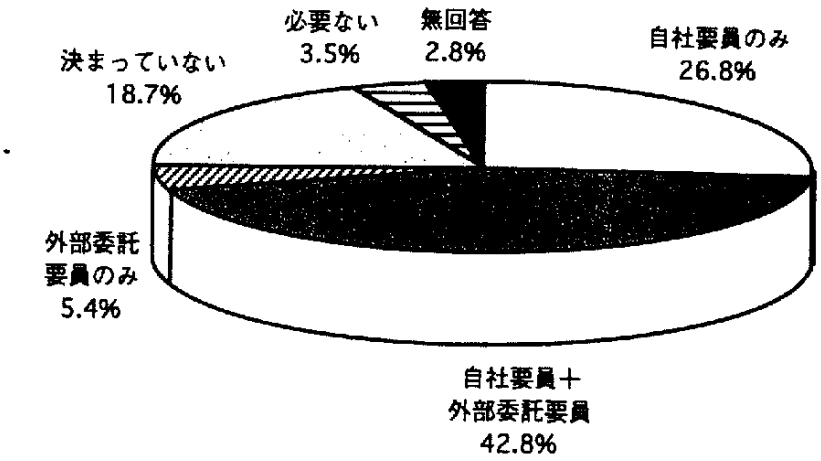
(4) 要員の確保

2000年問題解決にあたり，企業は要員確保についてどのような対応を考えているのか。

作業実施にあたり，「自社要員と外部委託要員」で対応する企業が42.8%と最も多く，次いで「自社要員のみ」(26.8%)，「外部委託要員のみ」(5.4%) となっている。

多くの企業が自社要員でまかなえない分を外部委託要員に依存せざるを得ないと考えており，技術要員の確保はますます困難になることが予想される。

図4. 2000年問題解決のための技術要員（被監査部門）



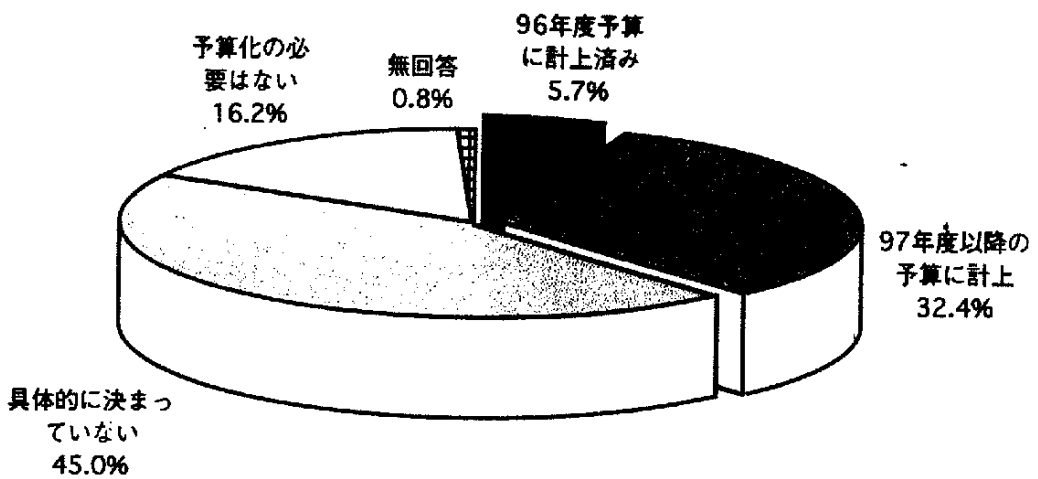
(5) 予算

経費の確保については，すでに「96年度予算に計上済み」5.7%，「97年度以降に計上予定」32.4%，と合わせて38.1%の企業がすでに予算を確保して早期対応を試みていることがわかる。

「具体的に決まっていない」と答えた企業が45.0%あるが，これは今後の対応にどれだけの費用を要するのか，計画段階のため判断できないためなのか。いずれにせよ，早期の予算検討を期待したい。

なお，「予算化の必要はない」と答えた企業は16.2%であった。

図5. 2000年問題解決費用の予算化（被監査部門）



2. 2000年問題とシステム監査

(1) システム監査の実施状況

2000年問題について監査部門では87.3%が認識している。しかし，2000年問題に関する監査の実施状況については調査時点（96年）ではまだ6.5%の企業でしか行われておらず，2000年問題はまだ先の問題，または自社にとってはそれほど重要と感じていない企業が多いのかもしれない。

図6. 2000年問題に対する認識度（監査部門）

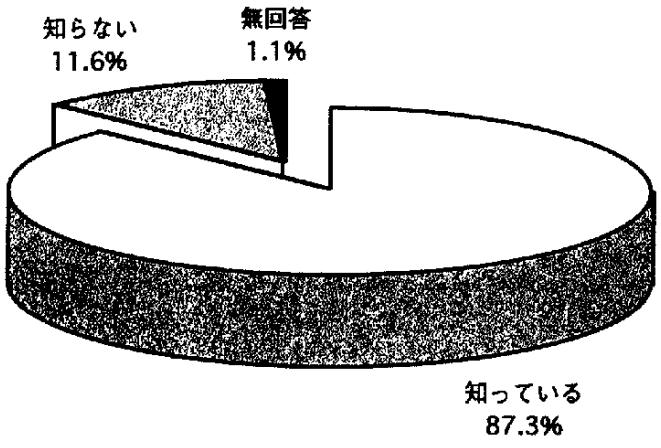
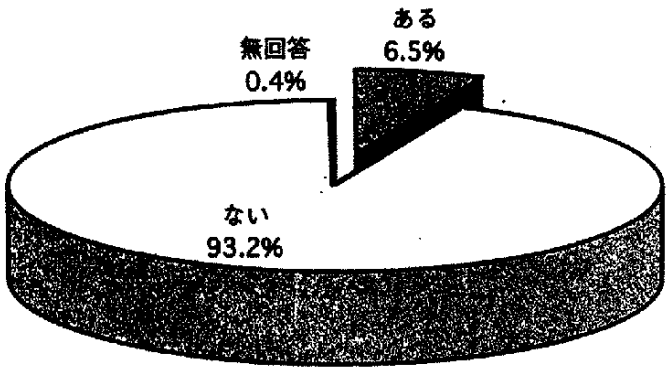


図7. システム監査実施状況（監査部門）



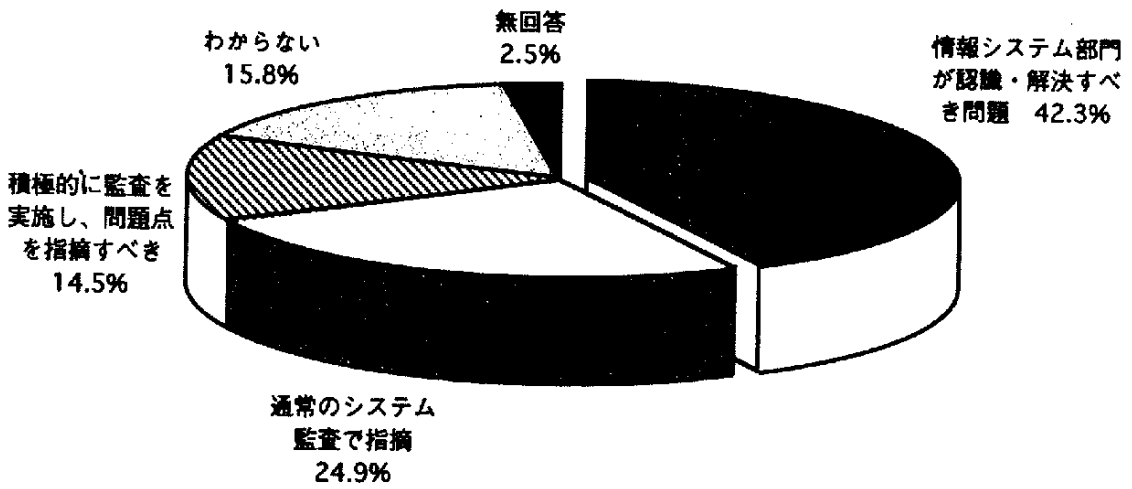
(2) 監査部門の取り組み方

被監査部門では，約9割が解決に向けて作業完了または検討中であるのに対し，監査部門は2000年問題にどう取り組むべきなのか。

監査部門では「情報システム部門が認識，解決すべき問題であり，システム監査で指摘すべきではない」（42.3%）と全社で対応すべき問題ではなく，あくまでも情報システム部門内の問題との意識をもっている企業が多い。

その反面，「積極的にシステム監査を行い，問題点を指摘すべき」14.5%，「通常のシステム監査の中での指摘でよい」24.9%を合わせると，約4割が何らかの形でシステム監査人が2000年問題に取り組まなければならないと認識していることがわかる。

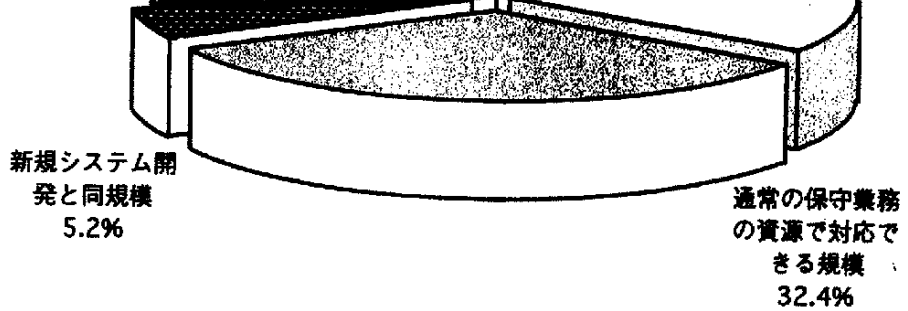
図8. システム監査人が取り組むべき姿（監査部門）



(3) 資源の規模

監査部門では問題解決に要する資源がどれだけ必要だと考えているのか。「システム更改と同規模の資源で大丈夫」が34.4%，「通常の保守業務の資源で対応可能」が32.4%と，通常業務以上の資源は必要ないと思っていることがわかる。逆に新規のシステム開発と同規模が必要と感じているのは5.2%と少ない。

図9. 2000年問題解決にかかる資源規模（監査部門）



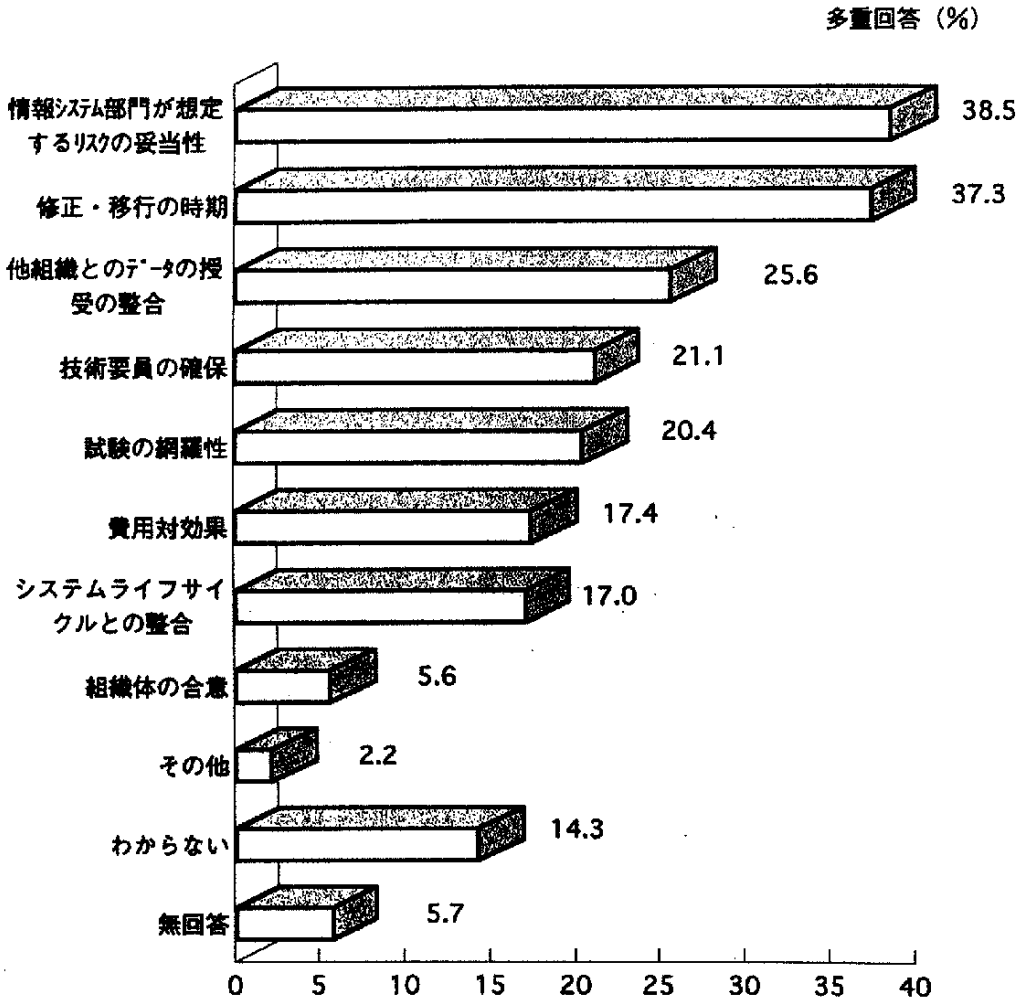
(4) 監査のポイント

監査部門が2000年問題を監査する場合のポイントは，「情報システム部門が想定するリスクの妥当性」38.5%，「修正・移行の時期」37.3%，「他組織とのデータ授受の整合」25.6%，「技術要員の確保」21.1%の順となっている。

その他の意見としては，「外部委託の管理」，「2000年問題と同様な問題発生の防止」，「パソコン等ホストシステム以外の対応計画」等があげられている。

2000年問題についてシステム監査を行う場合には，単にシステムの運用状況のみならず，計画段階から要員問題等，多方面からのチェックが必要となる。

図10. 2000年問題を監査する場合の監査ポイント（監査部門）



＜参考＞

システム監査のチェックリストの例

（情報収集と取り組み）
・経営者やユーザの理解を得た上で全社的な課題として取り組んでいるか
・「2000年問題」対応の基本方針を明確にしているか
・「2000年問題」の対応体制は適切か
・「2000年問題」に対し必要な技術情報を収集しているか
・対応が必要なハードウェア，基本ソフトウェア，ミドルウェア等を把握しているか
・「2000年問題」に対する内外の影響範囲と影響度を適切に把握しているか
（計画）
・「2000年問題」の対応計画を立案しているか
・対応が必要な業務システムとその優先順位を明確にしているか
・「2000年問題」への対応は，解決の期限からみて適切か
・「2000年問題」への要員計画は，技術レベルや要員確保の面からみて適切か
・対応が必要なハードウェア，ソフトウェア，関連機器を資源計画に反映しているか
（具体的な対応）
・対応が必要なプログラムを明確にしているか。また，対応方法は適切か
・内外の関連組織に対して必要な情報を伝えているか
・テスト環境やテスト方法は適切か
・テストケースやテスト期間は適切か
・テストは内外の関連組織を考慮して実施しているか
・テストの検証方法は適切か
（移行）
・移行時期と体制は適切か
・移行後のトラブルに対する体制は適切か

（システム監査白書97-98より）

実態調査概要

1．調査対象：JIPDECが実施している「コンピュータ利用状況調査」の母集団4,812事業体を対象

2．調査時期：1996年11月27日～1997年2月10日

3．回収状況：

発送数	4,812	
監査部門	639	（13.3%）
被監査部門	927	（19.3%）

4．回答事業体の平均従業員数：

監査部門	3,722人
被監査部門	3,203人

5．調査項目

(1) 監査部門

①システム監査一般について
②貴社の監査体制について
③1995年度のシステム監査実施について
④未実施の理由について
⑤実施可能性について
⑥2000年について
⑦コンピュータの不正アクセスについて

(2) 被監査部門

①システム監査一般について
②1995年度のシステム監査実施について
③システム監査のあり方について
④情報化一般について
⑤2000年問題について
⑥ソフトウェアの違法複製について
⑦コンピュータの不正アクセスについて

ネットワークおよびAI関連の情報技術の研究開発動向

先端情報技術研究所

1. 調査の背景

この数年の間にパソコンやインターネットが急速に普及し，情報分野に大きな変革の波が押し寄せて来ています。これに伴い，従来は種々の制約のために実現困難であった電子図書館，電子商取引，遠隔医療診断等の様々な情報サービスが，現実的なものとして取り上げられるようになりました。これらが身近に提供されるようになれば，経済的効果も含め，社会に大きなインパクトを与えると思われます。しかし一方では，専門家でない普通の人々にとっては情報環境が複雑になり過ぎて，その全容を理解することも，望む情報を得るためのコンピュータ操作を習得することも難しくなるという状況が生じています。

この機会を機敏に捉えて，新たなニーズに応えるべく情報処理技術のイノベーションの進展する方向を見定め，それに向かって適切な研究開発投資を行うことが，日本の情報産業にとって非常に重要なことだと考えられます。

先端情報技術研究所では，このような観点から，インターネットに代表されるネットワーク関連の新技術，人間とコンピュータとのインタフェースに関わるAI技術，それらを土台とする応用ソフトウェア技術を主題としたワーキンググループを組織し，将来の情報産業の土台を生み出すと思われる基礎技術分野から，重要と思われる応用分野まで，幅広く検討しています。主査にはNTT基礎研究所の奥乃 博 主幹研究員，メンバーにはこのワーキンググループで取り上げる各技術分野，応用分野の専門家10人に集まっていただき，調査を実施します。

2. 技術調査対象テーマ

インターネット普及のきっかけとなったWWWは，ウェブブラウザを用いて，世界中のコンピュータに蓄積された情報を簡単な操作で閲覧できるようにしました。これはインターネットを単なる通信手段から，誰にでも開放された巨大なデータベースシステムに変容させました。しかし，自発的な分散管理を前提とするインターネットでは，そこに接続されているコンピュータの構成は刻々と変動し，そこで提供される情報も日々更新されるうえ，別々の情報源から得た情報の内容が相反していることもまれではありません。

従来のデータベース管理システムは，静的で，かつ全体構成について既知であることを前提としていました。これに対してインターネットのような開放型システムではその前提が崩れており，このような不完全性に対する新しい理論を確立して，そこから適切に情報を取り出すことが求められています。

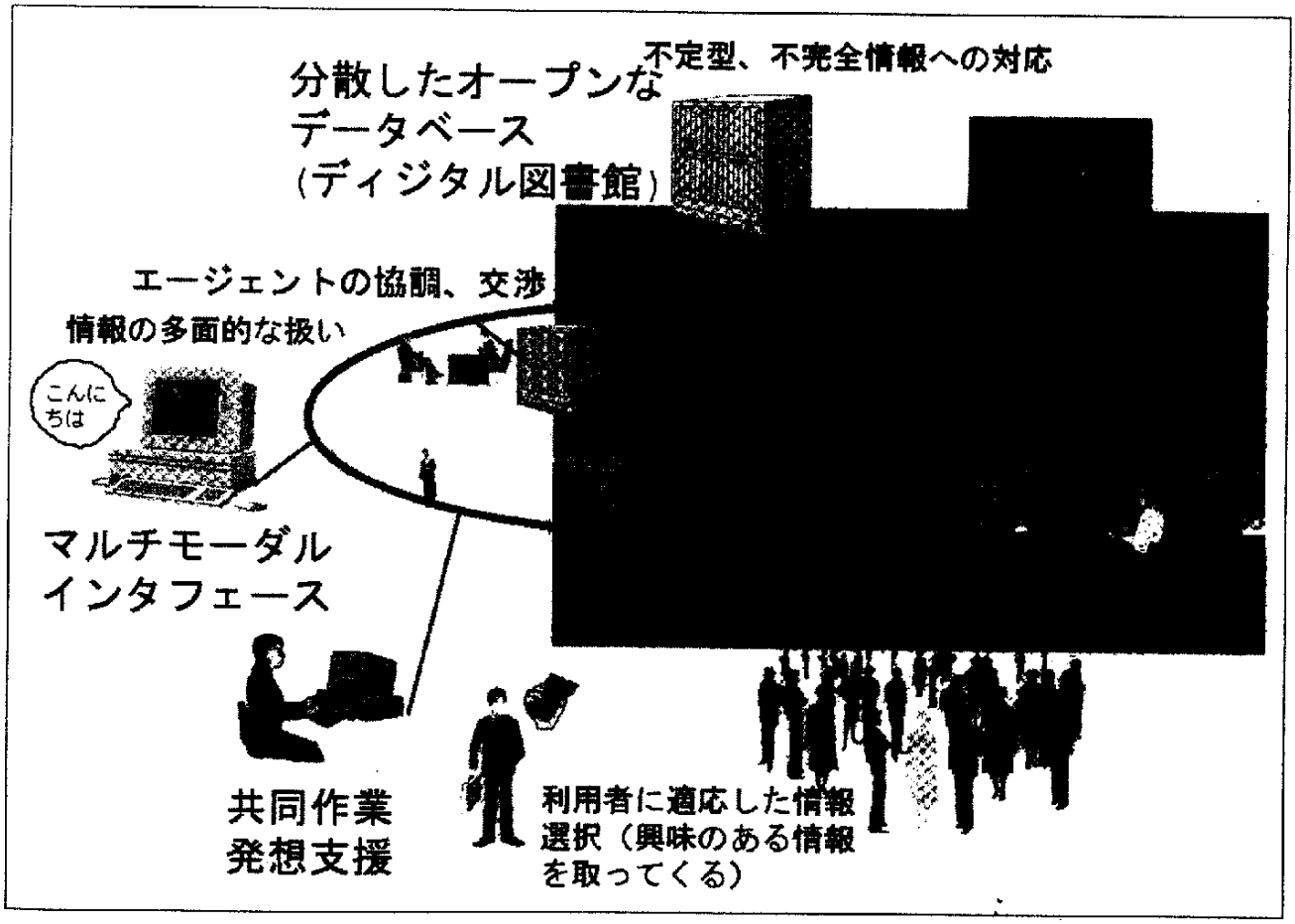
一方，これからは情報インフラを使いこな

せるか否かが，社会生活上の基本能力のひとつになると予想され，人にやさしい（「優しい」と「易しい」という二重の意味で）ヒューマンインタフェースの提供が，今まで以上に重要な課題となってきます。これに応えるために，音声，図形などのパターン認識技術や知識処理技術を利用したユーザー支援の仕組みが必要となっています。

このようにネットワークおよびAIに関連する研究分野は，激しい拡大発展の最中にあり，わが国の研究開発力がすべての分野で卓越することは不可能な状況です。そのため，注力する研究分野を選別し，そこに人材や費用などの資源を集中させることが重要となってきます。本ワーキンググループでは，そのような戦略をたてる際の参考とするため，新しい技術の萌芽となるような研究テーマについて検討し，リストアップしています。また，その研究を効果的に進めるために必要なインフラの整備や，そのような研究開発投資が社会に与える波及効果についても調査しています。

取り上げた研究テーマは，①共同作業支援，発想支援などの新しい利用形態，②ネットワーク上の処理を含むデータベース技術，③エージェント指向コンピューティング，④マルチモーダルインタフェース技術，⑤社会サービスおよびそれを構成するために必要な情報処理技術（電子図書館，ネットワークを利用した知的CAI）ですが，これらのテーマには様々な技術分野が関わっており，種々の社会システムを知的に支援するソフトウェアを構築するための重要な要素技術となります。

▼図　インターネットを取り巻く知的技術



3. 米国の研究開発動向

米国は世界の情報技術をリードしており，インターネット発祥の地でもあることから，そこでの研究開発動向を調査することは，研究開発テーマや研究開発の進め方を考えるうえで重要だと考えられます。以下に，米国政府が支援している情報技術研究開発テーマの中から，今回の調査に関係の深いものについて記します。

(1) HPCC計画からCIC研究開発計画へ

米国では国民的情報基盤の構築を国家戦略と定めて，NII（National Information Infrastructure）構想を打ち出し，それを実現するためにHPCC（High Performance Computing and Communications）計画を進めてきました。これは米国連邦政府が支援する情報技術研究開発の中心的な計画となっており，この中には，本調査で取り上げている研究開発テーマも多く含まれています。

HPCC計画は1991年から5年間の予定で開始され，96年には計画年限を迎えましたが，優れた成果を多くあげたという評価を受け，計画継続の方向が打ち出されました。97年からは計画および運営組織の構成が整理され，新たにCIC（Computing, Information, and Communications）研究開発計画がスタートしました。

(2) CIC研究開発計画

CIC研究開発計画は5つの部分領域から構成されており，これをPCA（Program Component Area）と呼びます。PCAの構成は，HPCCの元の5つの部分領域（HPCS, NREN, ASTA, IITA, BRHR）から発展したものです。PCAは，この研究開発計画に参画している連邦政府機関に対して，優先度の高い投資領域を示しています。以下に，各PCAについて説明します。

①High End Computing and Computation (HECC)

高性能計算分野で，最先端ハードウェアとソフトウェアの革新的研究を支援します。例えば，グランドチャレンジ級のアプリケーションを扱うために必要なモデリング，シミュレーション用のアルゴリズム，ソフトウェアなどが対象です。

②Large Scale Networking（LSN）

高性能ネットワーク構成要素，無線，光，移動体，有線通信の技術，大規模ネットワーク技術，管理，サービス，ネットワーク中心の情報処理向けシステムソフトウェアとプログラム開発環境を対象としています。

③High Confidence System（HCS）

利用者に高水準のセキュリティ，プライバシー保護，データ保護，信頼性を提供する技術を開発します。

④Human Centered System（HuCS）

ネットワーク上の仮想共同研究室，分散したデータ格納庫から知識を提供する技術，マルチモーダル対話システム，仮想現実環境を通して，情報処理および通信をさらに利用しやすくします。

⑤Education, Training, and Human Resources (ETHR)

新しい教育訓練技術の研究を支援します。これには生涯学習，遠隔教育，カリキュラムの開発を支援する技術も含まれます。

これらの中で，本調査で対象とする研究開発テーマは④のHuman Centered Systemに最も多く含まれていますので，これについて次の節で詳述します。

(3) Human Centered System（人間主導型システム）

情報処理システムと通信ネットワークをさらに使いやすくし，幅広い利用者層に提供します。この利用者には，科学者および技術者，教育者および学生，労働者，一般大衆が含まれます。このようなシステムを可能にする主な技術には，以下のものがあります。

①「知識リポジトリ」と「情報エージェント」

多彩なマルチメディアデータ，および複数情報源からの情報を管理，解析，表示する技術です。

②ネットワーク上の仮想共同研究室知識

リポジトリへのアクセスを提供し，知識の共有，共同執筆，遠隔機械の制御を可能にします。

③マルチモーダル・ヒューマン・システム・インタラクション

音声，触覚，ジェスチャーの認識，および合成などのインタラクションを可能にするシステムです。

④仮想現実環境と応用

科学研究，健康管理，製造，訓練などへの応用研究です。

▼表　Human Centered Systemの主な研究テーマ

- 知的システムおよびソフトウェア
- 知識獲得，融合，集合，要約ツール
- 遠隔装置を操作する仮想環境
- マルチモーダルコミュニケーション，音声認識
- ネットワーク上の仮想共同研究室
- グループオーサリングツール
- 医療用グラフィカルユーザーインタフェース
- 電子カルテ
- 診断支援
- 可視化人体データベース
- ディジタルライブラリにおける環境データの可視化
- 自動文書翻訳

(4) 電子図書館プロジェクト

このように米国では，情報技術に対して非常に広範囲に渡って支援をしていますが，ここではさらに，ネットワークの重要な応用である電子図書館に焦点を絞って，その実現に必要とされる各種の技術について，米国での取り組みを述べます。

電子図書館は，コンピュータとネットワークでディジタル化された環境で，様々な情報資源を利用者に提供します。一般の図書館では，資料を収集，組織化して蓄積するとともに，情報アクセスのための情報（2次情報，メタデータ）を作成して検索に利用しますが，これは電子図書館においても同様です。

米国の電子図書館研究開発プロジェクトは，大きく2種類の性格に分けられます。1つは，議会図書館における電子図書館プロジェクト（NDLP）や大学図書館における電子図書館プロジェクトであり，これらは主として，既存の資料の電子化とその提供を目的としています。これらの資料はインターネットでアクセスできるようになっています。

他の1つは，NSF/DARPA/NASAの共同助成による電子図書館プロジェクト（Digital Library Initiative,以下DLI）であり，これは将来の電子図書館に向けた新しい情報技術の研究開発という性格があります。94年から4年間の計画で行われており，情報インフラ上の新しい情報技術と図書館像を作り出すプロジェクトとして非常に注目を集めています。この研究助成プログラムでは，計算機科学や図書館情報学，その他の分野からの研究者が参加することと，大量のデータを持つ機関（出版社，政府機関，図書館）との共同プロジェクトを進めていることが特徴的です。また，これらは将来の大規模なシステムのため

の実験台（テストベッド）構築を目指しています。

電子図書館プロジェクトには，以下のサブプロジェクトがあります。

①カーネギーメロン大学（CMU）：
Informedia Interactive On-line Video Digital Library

画像認識，音声認識，自然言語理解などの技術を総合し，放送局から提供されるビデオ映像を音声などで対話的に検索と視聴ができるシステムを作り上げます。

②ミシガン大学（University of Michigan）：
The University of Michigan Digital Library（UMDL）

宇宙・地球科学分野の多様な資料を利用するマルチメディア環境を構築し，高校生から研究者まで，幅広く多様な利用者に合わせて提供することを目的としています。この研究では，ユーザーインタフェースエージェント，仲介エージェントといったソフトウェアエージェントを利用します。

③イリノイ大学アーバナ・シャンペイン校（UIUC）：Interspace

IEEEやその他の出版社と協力し，大量の科学技術分野の学術文献を非常に多数の利用者に提供します。雑誌論文をSGML（Standard Generalized Markup Language）に基づく全文データベースとして蓄積し，巨大なテキストデータの空間から所望の情報を導きだすシステムの構築を目指しています。

④カリフォルニア大学バークレイ校(UCB)：
Electronic Environmental Library

拡張性のある知的分散型ライブラリのプロトタイプ開発を目指しています。カリフォルニア州が持つ大量の環境情報に関する大規模データベースを構築します。環境関連の条例，報告書だけでなく，航空写真，ビデオ，コンピュータ上の環境モデリング，地図および環境データ等の多様な情報を含んでいます。環境に関する計画，研究を州およびそれ以下の地域レベルで可能にするために，専門家から一般利用者までの多様な利用者に提供する環境を構築します。

⑤スタンフォード大学：Stanford Integrated Digital Library Project

ネットワーク上に提供されるさまざまな情報を，仮想的な１つの図書館として利用できるような統合環境を開発します。

⑥カリフォルニア大学サンタバーバラ校（UCSB）：Alexandria Digital Library

地図や航空写真などの空間情報，地理情報の相互利用性を高め，大規模データベースを構築することを目的とします。

1998年からは，次世代の電子図書館プロジェクトであるDLI2も始められようとしています。DLI2ではさらに新しい領域を開拓し，相互運用性，技術統合を重視すること，Human Centered Systemとしての電子図書館を目指すことが提唱されています。

このように米国では，電子図書館という統合テーマの中で，既存の文書の電子化や図書館の情報化にとどまらず，ネットワーク上に散在する情報を統一的に扱う分散マルチメディアデータベース研究の視点を中核に，人間とのインタフェースを容易にするパターン認識やマルチモーダルインタフェース，図書館司書の果たしている仕事を代行するソフトウェアエージェントなど，多くの研究開発テーマが重層的に取り上げられています。さらに，関連する研究分野として，書誌情報（メタデータ）の標準化，データマイニング，情報源

間の交渉，協調機能など，高度なデータベースの利用のために，知的情報処理を導入するアプローチが試みられています。

4. まとめ

以上のように，米国では，CIC研究開発計画の中で，数々の情報関連研究テーマが大規模に取り上げられ，医療，教育，環境などの様々な社会システムに適用できる効率的で使いやすい情報環境の構築を目標として，基礎研究から開発までを幅広く行なっています。それに対して日本では，方法論指向で小規模の基礎的研究が中心となっているように見えます。アプリケーションの開発も，個別のアプリケーションに特化した形で行なわれることが多く，基礎研究との連携が考慮されず，また，個々の技術が他のアプリケーションに転用できるように考えられていないのが現状です。これは，わが国においては，新技術が，その必要性が認識されるからというよりは，米国の後追いを動機として研究開発される傾向が依然として残っているためと思われます。今後はわが国でも，情報を広く社会システムに利用するという視点に立ち，フロントランナーとして情報技術の最先端を開拓するという意識に基づく研究開発が望まれます。

各部・室・センター活動状況

情報セキュリティ対策室

1. セキュリティ対策に関する調査・研究

情報技術は，急速に進展を遂げています。情報システムに係るセキュリティに関しても，技術の進展によって新たなリスクが発生することとなり，セキュリティ対応策も従来のままでは十分に機能しないことが考えられます。そこで，当室では学識者，有識者から成る「セキュリティ対策検討委員会（委員長：今井秀樹・東京大学教授）」を設置して，セキュリティ技術の現状と今後の進展の方向性を検討し，将来的なセキュリティ対策技術の整理を行うことによって，セキュリティ技術とその産業のあり方を探るための調査研究を進めています。

また，わが国の現状のセキュリティ対策の状況を把握するために，情報システムのユーザー企業等約4,800社に対してアンケート調査を実施しており，今年末には調査結果を取りまとめる予定です。

2. システム監査の普及に関する調査・研究

システム監査は，昭和60年１月に通商産業省が「システム監査基準」を公表したことを受けて，わが国においても本格的にスタートしました。昭和61年には情報処理技術者試験にシステム監査技術者の区分が加わったこともあり，システム監査への関心が盛り上がりました。その後10余年を経過したのですが，当室のアンケート調査によると，システム監査を実施している企業は，回答企業の30%程度に落ち着いたままの状況が続いています。

これは，システム監査技術者試験に合格したシステム監査人の数が約3,600人と少ないこと，システム監査が情報システムを構築し運用するために必須の活動として理解されていないこと等が原因と考えられています。

そこで，情報システムの総合保有コスト（TCO）の低減やセキュリティ対策の向上等の役割を担っているシステム監査が，今後の高度化された情報化社会には不可欠であることから，その普及策について検討しています。

その一環として，システム監査の普及・啓発用の小冊子「システム監査概要」，「システム監査Q&A110」の改訂・発行を行うべく準備を進めています，また，通商産業省の監修を得て，「システム監査白書98-99」をシステム監査学会との協力で作成し発刊しました。

3. プライバシーに関する調査・研究

欧州諸国等を中心とした先進諸国が法律によって民間事業者が収集している個人情報の保護を行っているのに比べ，わが国では，通商産業省等の定めた「ガイドライン」によって自主的な対応を採っています。そのため，自主的な対応策の実効性がEU諸国等から指摘されているところです。

当室では，平成７年（1995年）10月24日にEU委員会が採択した「個人データ処理に係

る個人情報の保護及び当該データの自由な移動に関する欧州会議及び理事会の指令」（EU指令）への対応の具体策の検討を，業界団体からのご協力を得ながら「個人情報保護に係る環境整備検討委員会（委員長：堀部政男・中央大学教授）」において進めています。

4. 暗号・認証に係る調査研究

認証実用化実験協議会（ICAT）との連携によって，公開鍵発行管理機構（CA等），暗号に係わる基礎技術等について調査研究を行っています。

また，ICATの事務局として実験的に17の企業・団体・学術系機関等に証明書発行・管理サービスを行っています。

現在は，公開鍵発行管理機構について，特に広域認証に必要な認証局間の連携機構について調査研究を行っており，その成果を基に今後は実際に連携構築する予定です。

なお，調査研究活動については，ICATホームページ（URL：http://www.icat.or.jp/）で随時報告します。

5. JPCERT/CC（コンピュータ緊急対応センター）の運営

JPCERT/CCが平成８年10月１日から実質的な活動を開始してから１年が経過しました。この間（平成９年10月末まで）に，383件の被害の相談を受けて対応してきました。これらの被害相談から，対応策を検討して“緊急情報”や四半期毎の“報告”としてホームページを通じてアラートを発信しています。

しかしながら，依然として古典的な方法による不正なアタックを受ける等の相談が跡を絶たない状況です。そのため，JPCERT/CCは各種セミナーを開催したり，企業等のセミナーに協力すること等を通じて，ネットワーク管理者等に注意を喚起しています。

JPCERT/CCの活動状況や，不正アクセスに関する最新のセキュリティ技術情報に関しては，今後もホームページ（URL：http://www.jpcert.or.jp/）を活用して発信する予定です。

調査部

1. 情報化白書1998年版の編集

平成10年５月末の発行を目指し，「情報化白書1998年版」の企画・編集作業を進めています。情報化白書編集委員会（委員長：石井威望・慶應義塾大学教授）および編集専門委員会（主査：廣松 毅・東京大学教授）で全体構成を検討・審議し，現在，原稿執筆に取りかかっています。

今回の総論では，情報化の経済・社会への浸透が深まるにつれて，装備を中心としたインフラ整備のみならず枠組みやルールづくりといった環境整備の必要性が高まっている現状を踏まえ，電子利用環境の整備に向けた枠組みづくりをキーコンセプトとして取りまとめていく予定です。また，各論についても著しく進展する各分野の情報化の動向をわかりやすく紹介いたします。

2. 海外における情報化の動向

アメリカにおける情報政策に関する調査として，７月１日に発表された”Framework for Global Electronic Commerce”を中心にとりまとめました。本ペーパーは政府の，EC振興を目的とする「政府による規制を極力規制排除，民間主導」といった基本姿勢を打ち

出したものとして興味深いものです。

ヨーロッパについては，情報政策関連のコミュニケを中心として調査を行い，特に昨年11月に発表された”Europe at the Forefront of the Global Information Society：Rolling Action Plan”の改定版（7月発表）をとりまとめました。前回発表のアクションプランのうち，20項目が採択時期の遅れ等から更新され，「欧州のコンテンツ産業の将来に関するコミュニケ」等26項目が新しい課題として採択されました。このコンテンツ産業に関するコミュニケとは，域内の豊富なコンテンツ資源，文化的豊かさ，言語の多様性を基盤として欧州におけるコンテンツ産業の強化を目的としたものです。

3. 日独情報技術フォーラムの開催

第11回日独情報技術フォーラムが，平成9年11月11～13日に，長野市の信州松代ロイヤルホテルで開催されました。両国の情報技術分野における第一線の研究者が一堂に会し，最新の情報技術研究の成果について情報交流を行いました。今回の第11回における基調講演は「Bioinformatics」について，日本側から東北大学電気通信研究所長・沢田康次教授が，ドイツ側からマックス・プランク研究所・Dr.Peter Fromherzがそれぞれ講演されました。

なお，詳細は，本誌次号(No.96)のJIPDEC REPORTに掲載の予定です。

4. 情報化に関する海外向け広報

今年度第1号であるNo.110では「日本の情報通信産業」をテーマとして取り上げ，統計資料をもとに豊富な図表で日本の現状を紹介しています。情報サービス産業，電子機器製造業，電気通信事業を合計した1996年の日本の情報通信産業の売上は，前年比14％増の36兆6,286億5,300万円に達しています。次号では，社会システムの情報化という観点から，例として医療システムを中心に取り上げる予定です。以下，今後の動向を見ながら，タイムリーな話題を海外に紹介していきます。

5. 情報化月間の開催

平成9年度の情報化月間は，10月1日（水）に東京全日空ホテルで挙行された「情報化月間記念式典」を皮切りに，全国各地でさまざまな行事が開催されました。記念式典では，

①情報化促進貢献個人の表彰
②情報化促進貢献企業等の表彰
③優秀情報処理システムの表彰
④全国高校生・専門学校生プログラミング・コンテスト入選作品の表彰

が，通商産業大臣，総務庁長官，運輸大臣，郵政大臣，情報化月間推進会議議長からそれぞれ当該受賞者に対して行われました。

なお，詳細は，本誌JIPDEC REPORTをご覧下さい。また，当協会のホームページ（URL http://www.jipdec.or.jp/）でもご覧いただけます。

6. 情報化月間記念国際シンポジウムの開催

当協会と情報処理振興事業協会では，10月1日（水）に行われた情報化月間記念式典の併設行事として，国際シンポジウムーネットワーク社会の進展とセキュリティーを東京全日空ホテルで開催しました。

シンポジウムは，750名余の参加申込みがあり，多数の参加者の中，米国Network-1 Software & Technology社筆頭副社長のビ

ル・ハンコック氏の招待講演に始まり，海外から４名，国内から３名の講師による講演やパネルディスカッションが行われ，活発な意見交換がありました。

なお，詳細は，本誌JIPDEC REPORTをご覧下さい。

技術企画部

1. 複雑系に関する調査研究

人工知能（AI）をはじめとする情報技術の高度化は，社会・経済・科学におけるさまざまな問題の解決に大きな成果を上げつつあります。しかし，処理対象をモデル化し，解決法を見い出すこれまでの手法は，持続的に変化し，その変化の予測が難しい現実世界の複雑な諸問題の解決には必ずしも十分とは言えません。

近年，このような現実世界の問題領域について，分析的にモデル化するのではなく，構成（機能）要素を細かく分けても単純にならない「複雑系（Complex System）」と捉え，その様態の解明や諸問題の解決のための基礎理論や要素技術に関する研究が急速に進んでいます。

本調査研究では，人工知能等の知的情報処理の視点から，複雑系にかかわる基礎理論や要素技術等の動向を調査するとともに，関連する理論，諸技術の応用の方法や範囲について調査研究を行い，人工知能等知的情報技術の今後の研究開発のあり方などについて検討を行います。

本調査研究にあたっては，複雑系情報処理調査専門委員会（委員長：中島 秀之・電子技術総合研究所主任研究官）を設置し，期間は本年度より２年間の予定です。

2. 次世代電子図書館システム研究開発事業

分散情報処理技術に関する新技術の開発を目的とした当事業は平成11年度までの事業として昨年度開始された事業です。

今年度事業の内容は，技術開発面では昨年度開発に着手した次世代電子図書館システムのアーキテクチャおよび個別技術を中心として開発を実施し，成果物としての実装規約書を作成するとともに，実証ツールを作成して，個別技術の実証実験も行うこととしています。このためアーキテクチャWG,プロトタイプ検討WGをはじめとして，いくつかのサブWGにおいてシステムとしての整合性を取るための検討を継続に行う一方，ユーザーサイドからは，電子図書館に関与するメンバーで構成されたユーザWGを中心として，ユーザーニーズとしての「電子図書館のあるべき姿」について検討しています。この検討結果は，システム構築において，開発者の参考となることを狙いとした報告書としてとりまとめることとなっています。

3. 産学官研究開発コミュニティに関する構築・運用

本研究開発は，わが国における産学官の研究開発情報の円滑・適切な交流を図り，わが国の技術開発資源のさらなる有効活用を図るため，WWWを介して，研究開発情報を一元的に管理し，国内外に情報提供するシステムを構築するとともに，GIIの１つのプロジェクトであるグローバルインベントリ・プロジェクト（GIP）による国際的な情報交換の促進を目指すものです。この活動を通し，わが

国の技術開発資源のさらなる有効活用と，海外を含めた産学官交流による新規技術の輩出と新規産業の創造に寄与します。

上述の目的を実現するため，電子情報通信分野の研究開発に関する多種多様な情報を収集・管理し，各種のナビゲーション機能（検索機能含む）によりインターネットを介して，適切な最新情報を提供する産学官研究開発コミュニティの構築・運用を行っています。

また，国家プロジェクトの情報提供については，G7のグローバルインベントリ・プロジェクト（GIP）として位置づけ，G7各国と有機的に連係し，同コミュニティの１つのサービス機能として構築・運用しています。

さらに，本年度は，インターネット上で稼働する視覚化ツールキットなどの研究開発を行い，産学官研究開発コミュニティのサービス機能の一部に取り込む予定です。

本事業の関連サイト：

・G7 Global Inventory Project（GIP）
　http://www.gip.int/
・産学官研究開発コミュニティ
　http://www.gip.jipdec.or.jp/
・情報化関連政策ホームページ
　http://www.gip.jipdec.or.jp/policy/

中央情報教育研究所

中央情報教育研究所では，高度情報処理技術者育成等のために，次の研修事業，調査研究事業，および普及啓蒙事業を実施しています。

1. 平成９年度下期研修事業

(1) 情報処理技術インストラクタ研修

情報処理専門学校・高等学校等の教員や企業における情報処理教育担当者等に対する標準カリキュラムに基づいた情報処理教育の指導ポイントに重点を置いたコース，および広い対象の情報処理技術や指導者等に対する最近の技術動向等の研修を実施しています。今後の研修日程や内容の詳細については，教務第一課（TEL：03-5531-0175）までお問い合わせ下さい。

・教育エンジニアコース
・システムアドミニストレータコース
・情報化人材育成・指導コース
　（標準カリキュラム改訂に係わる研修を含む）
・技術動向コース
・システム技術コース

(2) 高度情報化人材の研修

高度情報化人材育成標準カリキュラムに基づいた次の研修を実施しています。今後の研修日程や内容の詳細については，教務第二課（TEL：03-5531-0176）までお問い合わせ下さい。

・プロジェクトマネージャ　２/18～３/13
・プロダクションエンジニア　３/３～３/10
・ネットワークスペシャリスト　１/27～３/13
・データベーススペシャリスト　２/18～３/５
・システム運用管理エンジニア　２/２～３/５

2. 調査研究事業

(1) 情報処理教育実態調査

わが国の情報処理教育に関する最新情報を把握し，施策検討に資することを目的として，平成９年度も継続してアンケート調査（発送数：企業，学校等教育機関あて，合わせて約3,500件）を実施します。

現在，調査項目の検討を行っていますが，

企業および学校における情報処理教育の体制，内容，方法の実態を把握するための従来からの固定的なテーマに加え，情報化環境の変化に対応して，企業が望む情報化人材とはどのようなものかを検証し，情報化にかかわる人材育成という視点からの企業と学校教育との連携についての方策を探るための項目を盛り込む予定です。

また，情報・通信機器の進展に伴い，それらが教育研修にどのように利用されているか，今後の利用効果や可能性とも合わせて，方向を探る項目についても検討しています。

平成９年内に調査票を発送し，年度内に報告書をとりまとめる予定です。

(2) 地域交流セミナー等

産業界のニーズに即した高度情報処理技術者教育の推進と，地域における情報処理技術者の育成を活性化し，地域の情報化の推進に資するため，情報化人材育成学科認定校をはじめとする専門学校の教職員や企業における情報処理教育担当者を対象に，改訂版標準カリキュラムに係る経緯，改訂の概要等を内容とした「地域交流セミナー」を平成10年１月～２月にかけて，全国９ヵ所で開催する予定です。

また，情報化人材育成学科認定校の質的向上を図るため，Ⅰ類校19校の持ち回り見学会を実施する予定です。

(3) 高度情報処理技術者育成指針に関する調査研究

平成５年12月に作成した高度情報化人材育成標準カリキュラム（以下「標準カリキュラム」，全17種）を，その後の情報技術等の進展に合わせて13種改訂し，10月15日に通産省公報等を通じて公表しました（詳細は JIPDEC REPORT を参照)。また，改訂版標準カリキュラムの概要を作成し，前記の「地域交流セミナー」で利用します。

(4) 国際化に対応した情報処理技術者の育成に関する調査研究

わが国においては，アジア諸国との情報サービス産業における国際間分業の推進と発展途上国の情報化の推進の観点から，各国固有の情報処理技術者の育成方法，情報化人材像の区分，評価方法について既に検討が行われている東南アジア地域コンピュータ連合（SEARCC）情報処理技術者専門部会（SRIG-PS）等との有機的な連携を図り，かかる検討活動に積極的に参加・協力していくことが望まれています。

このため，SEARCC等の活動に対する協力の一環として教育カリキュラムや教材の評価（年度後半に予定），作成等に関する支援およびSRIG-PS活動への助言・情報提供（７月および12月に数名をSRIG-PSへ派遣）を行うとともに，このような国際化時代の情報処理技術者の育成方法等について調査研究を実施しています。

(5) 高度情報処理技術者育成のための基盤整備

昨年度に引き続き標準カリキュラム改訂の支援作業を行っています。前述の公表後，改訂カリキュラムを刊行する作業および今後の改訂に備えてデータベース化する作業等を実施しています。

(6) 高度情報処理技術者育成のための応用調査研究

マルチメディア教材整備の一環として，システムアドミニストレータ育成用ホームページ教材（プロトタイプ）の機能強化を図っています。また，第一種共通テキストの学習科目のうちマルチメディア化の効果が期待され

る科目について，同様にプロトタイプを作成しています。

3. 普及啓蒙事業

10月15日の改訂版標準カリキュラムの公表を受けて，標準カリキュラム17種を含むCD-ROMの販売を11月20日に開始しました。詳細は調査企画部普及振興課（TEL：03-5531-0177）までお問い合わせください。

また，現在，第二種共通カリキュラムおよびシステムアドミニストレータ育成カリキュラムに準拠したモデルテキストを作成しており，来年始め頃に刊行する予定です。

情報処理技術者試験センター

情報処理技術者試験センターでは，情報処理技術者試験の確実な実施と情報処理技術者の育成・評価に寄与すべく啓蒙普及活動，調査活動に取り組んでいます。

今回は，４月に行われました平成９年度春期情報処理技術者試験の状況を紹介します。

情報処理技術者試験は，昭和44年の試験制度スタート以来，平成９年度春期試験までの応募者総数は699万人，合格者総数は64万人となっています。平成６年秋期試験からの制度移行後の３年間では，応募者数147万人，合格者数15万人となっています。

平成９年４月に実施された春期の情報処理技術者試験は，応募者数22万766人（前年同期比マイナス2.0％），受験者数13万8,555人（前年同期比マイナス2.0％），受験率62.8％，合格者数１万7,900人，合格率12.9％という結果となりました。

試験区分別の応募者数をみると，増加しているのはプロダクションエンジニア（PE）試験とデータベーススペシャリスト（DB）試験の２区分のみで，他はすべて減少しています。これは，情報システムがオープン化，ネットワーク化，データベース化の傾向にある中で，応募者がテクニカルスペシャリスト系の人材を目指している傾向にあると見受けられます。第一種，第二種試験では，ここ数年応募者数は減少傾向にありますが，減少幅（昨年：第一種マイナス10.2％，第二種マイナス9.1％）はかなり小さくなってきています。これは，情報処理産業の業績の回復や，新規採用者数の回復などが１つの要因と考えられます。昨年から実施されたマイコン応用システムエンジニア試験については，627人（マイナス21.0％）減となりました。（表１）

合格者の発表は，第二種が６月13日，第一種が７月８日，プロジェクトマネージャ，システム運用管理エンジニア，プロダクションエンジニア，データベーススペシャリスト，マイコン応用システムエンジニア試験の各試験は７月25日に行われました。

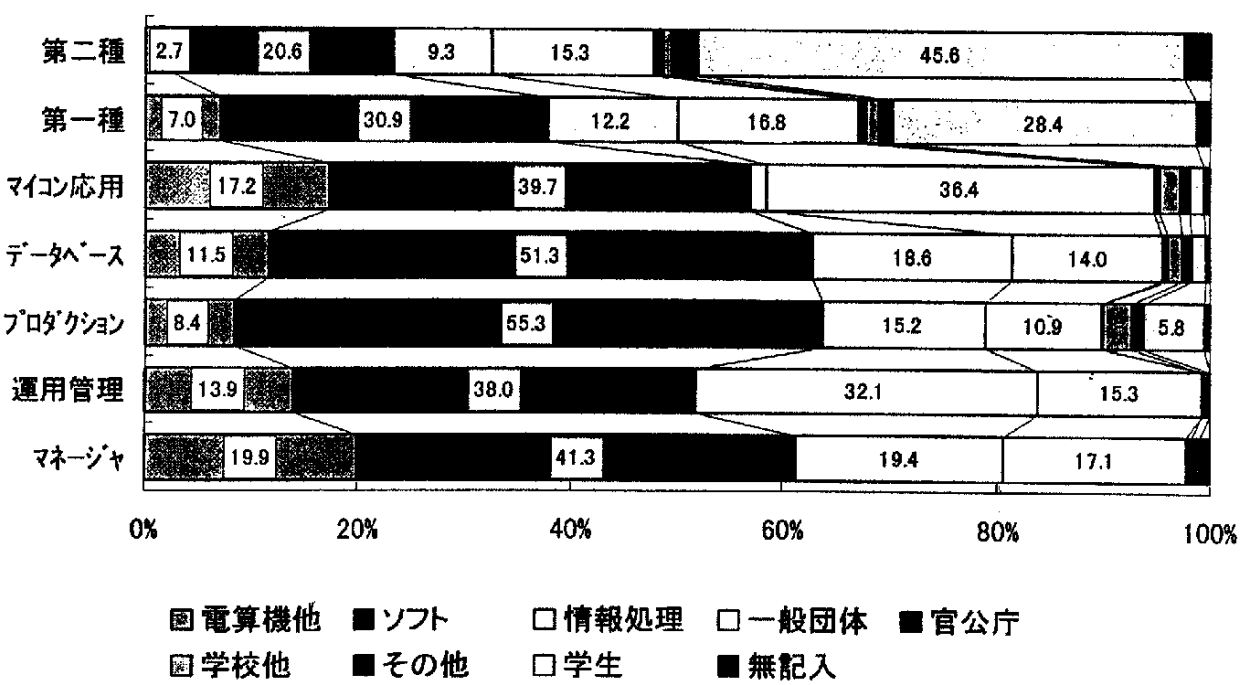
(1) プロジェクトマネージャ（PM）試験

合格者は346人（合格率7.1％）となり，前年より人数で23人，合格率で0.6％増加しました。合格者の勤務先別内訳では，ソフトウェア企業が41.3％を占め，次に電算機製造または販売企業，情報サービス企業等の順となっています。この３種類の勤務先を合計すると，実に合格者の80.6％の人が情報処理関係の勤務者であることが分かります。最終学歴別内訳では大学・旧制高校卒業者が全体の79.2％を占め，続いて大学院卒業生が9.5％を占めています。なお，学生の合格者はいません。経験年数別内訳では，10年以上15年未満の情報処理に関する経験者が44.8％を占め，

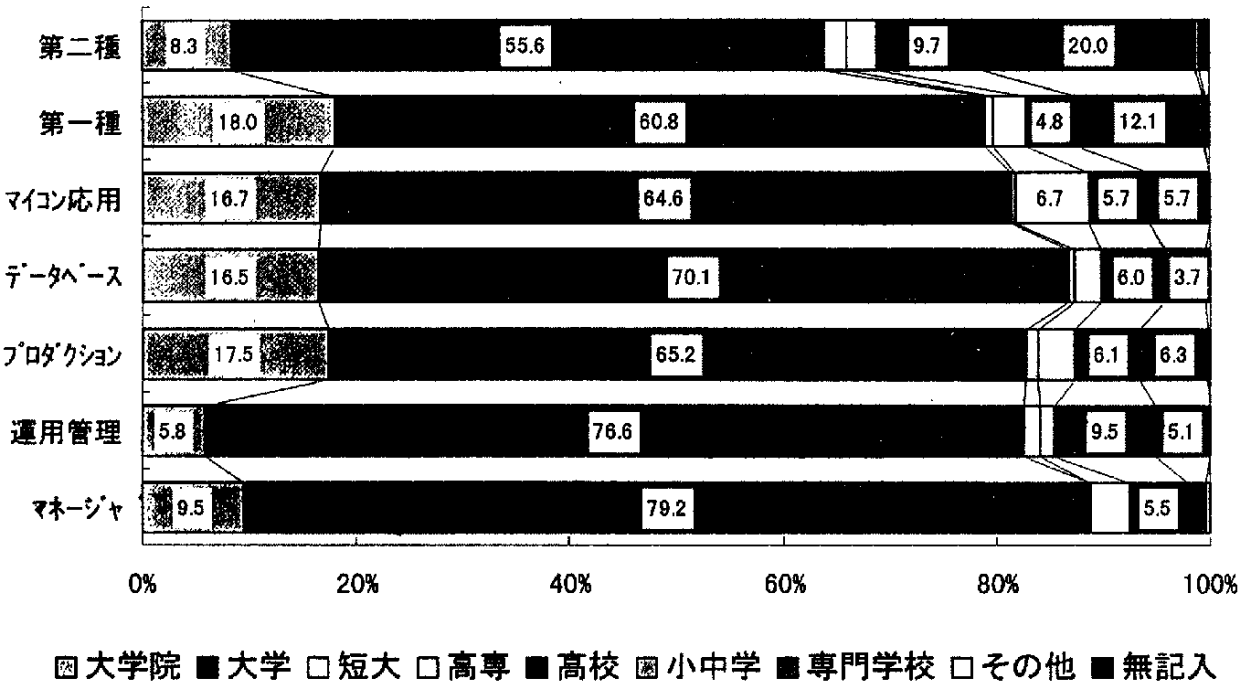
▼表1　平成9年度春期　応募者数一覧

試験区分	応募者数	前年同期比(%)	合格者数	合格率(%)
プロジェクトマネージャ	10,052	−2.2	346	7.1
システム運用管理エンジニア	3,849	−7.5	137	6.9
プロダクションエンジニア	13,328	1.6	788	9.6
データベーススペシャリスト	10,662	17.2	485	8.3
マイコン応用システムエンジニア	2,353	−21.0	209	13.8
第一種情報処理技術者	75,255	−3.8	5,309	11.5
第二種情報処理技術者	105,267	−1.9	10,626	15.2
合　　計	220,766	−2.0	17,900	12.9

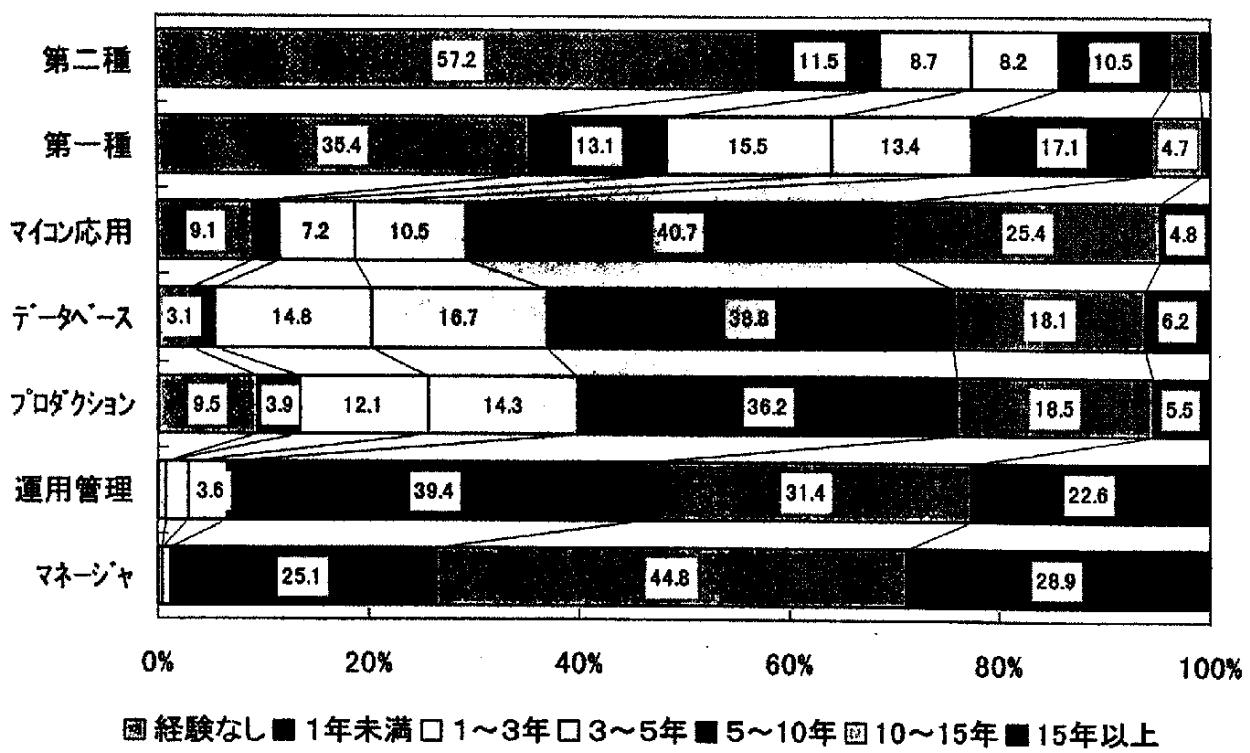
▼図1　勤務先別　合格者　構成比（平成9年度春期）



▼図２　最終学歴別　合格者　構成比（平成9年度春期）



▼図３　情報処理業務の経験年数別　合格者　構成比（平成9年度春期）



15年以上の経験者28.9%，5年以上10年未満の経験者25.1%という順序になっています。

(2) システム運用管理エンジニア(SM)試験

合格者は137人（合格率6.9%）となり，前年より人数で3人，合格率で0.8%減少しました。合格者の勤務先別内訳では，プロジェクトマネージャと同様にソフトウェア企業が40.0%を占め，次に情報サービス企業等，電算機製造または販売企業の順となっています。この3種類の勤務先を合計すると，実に84.0%の人が情報処理関係の勤務者であることが分かります。最終学歴別内訳では大学・旧制高校卒業者が全体の76.6%を占めています。続いて高校・旧制中学の卒業生，大学院卒業生という順になっています。なお，学生の合格者はいません。経験年数別内訳では，5年以上10年未満の情報処理に関する経験者が39.4%，10年以上15年未満の経験者が31.4%という順序になっています。

(3) プロダクションエンジニア(PE)試験

合格者は788人（合格率9.6%）となり，前年より人数で195人，合格率で2.3%増加しました。合格者の勤務先別内訳では，ソフトウェア企業が半数以上の55.3%を占めています。次に情報サービス企業等，一般企業・団体の順となっています。ここで，PM，SM試験と異なる点は一般企業・団体の割合が高くなっている点です。これは，一般企業・団体の情報システム関係者がPE，DBといったテクニカル系の人材を目指している傾向にあるものと見受けられます。最終学歴別内訳では，大学・旧制高校卒業者が全体の62.8%を占め，続いて大学院卒業生，高校・旧制中学の卒業生の順となっています。経験年数は，5年以上10年未満の情報処理に関する経験者が36.2%，10年以上15年未満の経験者が18.5%，3年以上5年未満の経験者が14.3%となっています。

(4) データベーススペシャリスト(DB)試験

合格者は485人（合格率8.3%）となり，前年より人数で144人，合格率で1.6%増加しました。合格者の勤務先別内訳では，ソフトウェア企業が約半数の51.3%を占めています。次に情報サービス企業等，一般企業・団体の順となっています。最終学歴別では，大学・旧制高校卒業者が全体の69.5%を占め，続いて大学院卒業生，高校・旧制中学の卒業生と続いています。経験年数は，5年以上10年未満の情報処理に関する経験者が38.7%を占めています。続いて，10年以上15年未満の経験者18.1%，3年以上5年未満の経験者16.7%という順序になっています。全体としては，PE試験と同様の傾向にあるようです。

(5) マイコン応用システムエンジニア（ME）試験

合格者は209人（合格率13.8%）となり，前年より人数で67人，合格率で0.4%減少しました。合格者の勤務先別内訳では，ソフトウェア企業が39.7%，一般企業・団体36.4%，電算機製造または販売企業17.2%の順となっています。ME試験が他のPM，PE試験などと異なる点は，一般企業・団体の割合が大きいことです。家電製品，自動車，ゲームなどマイコンを応用した製品の多様化により，電機，製造業など幅広い分野にマイコン応用システムエンジニアが求められている結果と見受けられます。最終学歴別内訳では，大学・旧制高校卒業者が全体の64.1%を占め，続いて大学院卒業生，高等専門学校の卒業生の順で続いています。経験年数は，5年以上10年未満の経験者が40.7%を占め，続いて10年以上15年未満の経験者25.4%，3年以上5年未

満の経験者7.2%という順序になっています。

(6) 第一種情報処理技術者試験

合格者は5,309人（合格率11.5%）となり，前年より人数で900人，合格率で1.6%減少となりました。合格者の勤務先別内訳では，ソフトウェア企業が30.9%を占めています。次に学生が28.4%を占め，その後に一般企業・団体，情報サービス企業等と続き，学生の割合が高いことが分かります。また，合格率をみると，社会人9.4%に対し，学生は24.9%と非常に高い値を示しています。最終学歴別内訳では，大学・旧制高校卒業者が47.5%，大学院卒業生13.3%となっています。学生では大学生13.2%，専修学校生8.8%となっています。経験年数別内訳では，5年以上10年未満の情報処理に関する経験者が17.1%を占めています。続いて1年以上3年未満の経験者15.5%の順になっています。

(7) 第二種情報処理技術者試験

合格者は1万626人（合格率15.2%）となり，前年より人数で159人減少し，合格率で0.5%増加となりました。合格者の勤務先別内訳では，学生が45.6%を占めソフトウェア企業20.6%，一般企業・団体15.3%の順で続いています。合格率をみると，社会人17.7%に対し，学生は13.3%と低い値を示しています。最終学歴別内訳では，大学・旧制高校卒業者が33.4%，大学生22.2%，専修学校生15.2%の順となっています。経験年数別内訳では，1年未満が11.5%，5年以上10年未満10.5%，1年以上3年未満8.7%の順になっています。

産業情報化推進センター

1. ビジネスプロトコルに関する検討

当センターでは通商産業省からの委託を受けて，「EDIに関する調査研究」事業を行っています。本年度は，「請求支払EDI」ならびに「EDI海外接続」の2つのテーマについて調査研究およびトライアルを進めています。

また，当センターでは，EDIに積極的な情報処理ベンダー各社の参加を得て，シンタックスルール検討委員会を設置し，CIIシンタックスルールの保守を行っています。この度本委員会では，CIIシンタックスルールの新バージョン3.0の検討を行っています。新バージョンでは，近年特に関心の高いセキュリティ機能の強化，国際対応などが盛り込まれ，平成9年10月までに基本的な検討を完了しました。新バージョンは平成9年度末のリリースを予定しています。

現在，EDIFACTのシンタックスルールの最新バーションであるISO9735バージョン4の規格案についてISOで賛否の投票が実施されました。当センターでは，学識者，業界有識者等から成るISO/TC154国内審議委員会を設置して，この規格案の分析検討を行っています。平成9年4月の投票で日本から提出した提案が盛り込まれ，平成9年末にはバージョン4がISO化される見込みです。

上述のCII，EDIFACTの2つのシンタックスルールについて，新バージョン開発と並行して，当センターでは，電子データ交換標準化調査研究委員会を設置して，平成7年度から3年計画でJIS化の検討も進めており，今年度末にはJIS原案を作成する予定です。

さらに，EDIの普及に資するため，業界横断的に使用可能な標準企業コードの登録管理

を行っています。この登録社数はCII標準に基づくEDIを実施している企業数の目安とすることができますが，平成９年９月には3,400社を超えました。このことから，CII標準の普及が依然堅調に推移していることが伺われます。

2. ユーザーシステムの高度化に関する研究

(1) EDIにおける「情報通信技術」の研究

EDIを実現する情報通信技術としてどのようなものが適するか，ユーザーとともに現状を調査し，メーカーを交えて業界および業際の標準として推奨できる仕様を検討しています。今後はオープンなネットワークについて，EDIでの利用可能性を調査研究していく予定です。

また，「全銀協標準通信プロトコルTCP/IP手順」の製品への実装に伴う仕様の解釈および拡張仕様の統一について検討を行い，開発された製品の接続試験を実施しているところです。

(2) 「二次元コード」の標準化に関する研究

通信ネットワーク上のEDIと並行して，実際に生じる物流を情報と一体化させるための二次元コードの標準化について，ユーザー環境を中心に検討を行っています。今年度は二次元コードを利用するシステムの代表的な業務として「物流」を例に挙げて業務フローを示し，そこで使われるデータ内容について標準的な様式を設定した「ガイドライン」を報告書として作成する予定です。

3. 産業界のシステム化およびそれに係る制度問題の調査研究

産業界における企業間ネットワーク化およびEDIの進展によって，電子取引という新しい取引形態が活発化しており，これに伴い従来の商慣習や法律，規則等では対応できない問題の発生が予測されています。この調査研究では法律の専門家および企業等の実務家による法的問題を調査研究する委員会を設置して，これらの法的諸問題の対処のあり方等について詳細な検討を行っております。昭和63年度から８年間，クローズな企業間取引についての検討を行い，平成７年度は，EDI取引を行う際に考慮すべき法的な事項を踏まえたデータ交換協定書（参考試案）を作成しました。昨年度からは今までのクローズなEDI取引を中心とした検討に加えて，最近注目されております電子商取引やCALSなどのオープンネットワーク環境での電子データ交換についても視野に入れ制度的な問題の検討を行っています。

本年度は，昨年度に引き続き新しい企業間電子取引について検討するとともに，既に作成しました「データ交換協定書（参考試案）」にこの研究成果を反映させ，より適用範囲の広いものにすることとしています。

4. EDIの普及促進

わが国のEDIの普及・啓蒙，業種横断的な共通課題の検討および関係者の情報交換の場として，60（平成９年10月現在）の業界団体および関係４省庁（オブザーバ）で組織する「EDI推進協議会」の事務局として，今年度も各種活動を行っています。まず，平成９年度の普及・啓蒙活動としては，年４回の普及研修会とEDIフォーラムがあります。６月24日に開催した第１回普及研修会「国内外のEDI最新事情」には206名，９月５日の第２回普及研修会「物流EDI現状と課題」には

154名，12月５日の第３回普及研修会「オープンネットワーク環境とEDI」には207名といずれも当初予定の定員を大きく超えるご参加をいただきました。また，７月16日には「企業間高度電子商取引（EC）プロジェクトの現状と今後」と題して「EDIフォーラム1997」を開催し，206名のご参加をいただきました。

また，同日行われました，平成９年度EDI推進協議会総会では，新会長，副会長の選任と平成９年度の事業計画等が承認されました。総会終了後は，電子商取引関連５団体（EDI推進協議会，JIPDEC・STEP推進センター，CALS推進協議会，CALS技術研究組合，電子商取引実証推進協議会）合同の技術交流会が通商産業事務次官の臨席をいただき開催されました。

なお，今後の研修会等のプログラムの詳細はEDI推進協議会のホームページをご覧ください（http://www.ecom.or.jp/jedic/index.htm）。EDI推進協議会の会員の皆様のご協力により平成８年度に実施しました「国内外のEDI実態調査」を，本年度は，年内に実施することを予定しておりますので，ご協力のほどお願い申し上げます。昨年度の調査結果につきましては，「国内外のEDI実態調査報告書」（平成９年６月発行）をご参照ください。

EDIに関する各種の国際活動への対応の検討や情報交換を行っていますが，その一環として，本年度は既に，４月のEDICOM'97（シンガポールで開催）と，９月のAPEC-TEL（アジア太平洋経済協力会議－電気通信ワーキンググループ：ニュージーランドで開催）に参加しました。特に，APEC-TELには，通商産業省とともに参加し，APEC域内での「インターネットEDIパイロットプロジェクト」についての中間報告と情報交換を行い，APEC参加メンバーから高い関心を寄せられました。さらに，米国以外で初めて開催された「CALS Expo International 1997, TOKYO」（11月，東京）において，EDI推進協議会の立場でわが国におけるEC/EDI等についての報告を行いました。

5. 普及・広報

(1) 「産業情報化シンポジウム」の開催

平成９年度の「産業情報化シンポジウム」を，平成９年10月31日（金）に日経ホール（東京都千代田区大手町）で開催致しました。今年度のテーマは「デジタル経済の時代の幕開け」です。なお，シンポジウムの詳細は平成10年２月発行予定の会議録をご覧ください。

(2) 広報誌「産業と情報」の発行

わが国産業界の情報化動向を広く各方面に周知するため，「産業と情報」を発行（年２回：９月，３月）し，会員・関係者へ配付しております。また一般の方々には有料でお分けしております。なお，最新号（９月末発行，35号）は，EDIフォーラム1997特集号です。

＜電子商取引実証推進協議会＞

1. 運営委員会／理事会／総会の開催

平成９年３月に行われた平成８年度第３回運営委員会および平成８年度第２回理事会において平成９年度事業計画案／予算案が審議の上，承認されました。また，平成９年５月に開催された平成９年度第１回運営委員会および６月に開催された平成９年度第１回理事会において，平成８年度事業報告案／決算報告案が，審議の上承認されました。

平成９年６月10日に開催された平成９年度総会では，平成９年７月１日以降の理事・監事が選任されました。これを受けて，平成９年度第２回理事会ではECOM会長および運営委員が選任され，会長には井川 博 氏（(財)日本情報処理開発協会会長）が再選されました。また，平成９年度第２回運営委員会では運営委員長の選任が行われ，中西 英夫 氏（(財)日本情報処理開発協会常務理事）が再選されました。

2. ワーキンググループ（WG）の活動

ECOMのWGでは，平成８年度活動の成果として，ECに関する様々な約款やガイドラインのアルファ版，中間成果を取りまとめました。各WGの中間成果報告書の概要は次のとおりです。

モール構築技術検討WGの「モール構築技術実証評価モデル（表現・表示および操作性)」（アルファ版）は，①「ユーザーインタフェース実現技術」，②「表示技術」，③「表示データの蓄積及び検索技術」，④「システム構築技術」について，モールの表現・表示および操作性に関する事項を重点的に実証評価し，共通プラットフォームおよびモールの構築・運営のガイドラインとなる実証評価モデル（評価項目および評価方法）をまとめたものです。

商品属性技術検討WGの「商品属性情報標準化に関する調査報告書～中間報告書～」は，「商品」それぞれが持つ属性情報の表現をどのように標準化したらよいか，商品属性情報の構造・内容・標準化表現・標準の管理方法等がどうあるべきかを検討することを目的に調査・検討をまとめたものです。

複合コンテンツ対応技術（エージェント機能）検討WGの「複合コンテンツ対応技術（エージェント機能）に関する調査結果」は，コンピュータ（エージェント）が利用者と対話しながらニーズを把握し，利用者の性別，年齢や過去の買い物履歴を考慮した上で，インターネットの世界から該当情報を集め，価格情報も含む確定情報や推薦のための比較情報を提示する複合コンテンツ対応技術（エージェント機能）の現状調査結果です。

コンテンツプロバイダ／モール間ビジネスプロトコル検討WGの「消費者・企業間ECにおけるビジネスプロセス・ビジネスモデル解説書（α版)」は，インターネットに代表されるオープンネットワーク上で，一般の消費者を対象とした商取引の過程を商品毎に分析したビジネスモデルを集大成したものです。また「消費者・企業間ECにおけるEDIの現状調査報告書」は，国内におけるEDIの現状，アメリカにおけるEDIの現状，EDIFACTの現状と課題について調査研究をまとめた報告書です。

共通セキュリティ関連技術検討WGの「共通セキュリティ関連技術検討WG中間報告書」では，ICカード使用の電子マネーシステムにおけるビジネスモデルを設定し，脅威の洗い出しおよび脅威に対するリスク分析や対策，また機能要件等の整理を行い，ICカード型電子マネーシステムセキュリティガイドラインをまとめました。さらにインターネット上のクレジット決済におけるノード蓄積情報やノード間伝送情報を明確にし，脅威の洗い出しおよび脅威に対するセキュリティ機能を整理しました。

本人認証技術検討WGの「本人認証技術検討WG中間報告書」は，①個人の識別を行い，事前に登録されている本人であることを確認

する技術である本人認証技術の概説，②本人認証の基本原理を抽出して抽象モデル化した本人認証参照モデル，③本人認証技術・製品・システムの特性を客観的に把握し，比較を可能にするための共通基盤である本人認証技術の評価基準（バージョン0.5）により構成されています。

ICカードWGがまとめた「ICカードの現状調査報告書」は，ICカードに関する現状の課題，問題点の整理，標準化の状況，制度的課題等，国内外で実証実験が推進されている状況を整理し，各種業界標準仕様をコマンド毎に類似点・相違点を解説したものです。アプリケーション識別子（AID）の国内登録機関の早期設立およびICカード普及における端末仕様等を一元管理する管理事務局の早期設置を提言しています。

認証局検討WGがまとめた「認証局検討報告書」は，①公開鍵基盤を構成する暗号サービス，認証書管理サービス，その他関連するサービス等認証局が提供し得るサービスに基づき，認証局に関する業務要件やマネジメント要件などについて提示している「認証局ガイドライン」と，②公開鍵基盤に基づいた認証局間の相互認証技術について調査検討結果をまとめた「相互認証技術解説および基本仕様案」の２部構成になっています。また「海外認証局活動調査報告」は国際間取引における相互認証のための基盤ルール，仕組の検討を行うための基礎資料的な報告書です。

国際取引WGがまとめた「国際電子商取引の制度的課題」は，消費者が安心して国際取引を行い，かつ事業者の円滑な参入を促進し得る秩序ある国際電子市場の仕組形成と制度的課題の検討をまとめました。また「サイバーモールに関するモデル契約の検討」はモールに関連する契約関係について国内外の事例調査，契約・約款等の分析に基づくビジネスモデルの検討を行い，①消費者―モール運営者／利用規約，②出店者―モール運営者／出店契約，③モール間クロスリンク契約のモデル契約書をまとめたものです。

プライバシー検討WGがまとめた「電子商取引における個人情報の保護に関する中間報告」は，①電子商取引にかかわるモールやショップ等の個人情報を取り扱うものに対するガイドラインとして，民間部門における電子商取引にかかる個人情報保護のガイドライン（α版）と，②欧米諸国の個人情報保護についての取り扱い状況ならびに電子商取引における検討状況について取りまとめた海外調査報告の２部で構成されています。

電子商取引決済関連問題検討WGがまとめた「電子商取引決済関連問題検討WG中間報告書」はオープンネットワーク上で安全かつスピーディなクレジット取引を実現することを目的としており，クレジット会社，クレジット加盟店，消費者間の取引ルールを定める約款の標準モデルとして，EC用加盟店標準約款ならびにEC用会員標準特約で構成されるクレジットタイプ標準約款案他をまとめたものです。また「ECOM CASH約款α版」は充填可能なICカード型電子マネー「ECOM CASH」利用の当事者間ルールについて規定しました。

消費者取引検討WGがまとめた「電子商取引における消費者取引の課題に関する中間報告書」は，電子商取引の健全な発展のための取引ルールについてのガイドラインを策定しました。電子商取引において消費者に商品等を販売する事業者に指針を示すことで，取引の公正および消費者の保護を図り，トラブル

を防止することに主眼を置いています。

電子公証検討WGがまとめた「電子公証検討調査報告書（電子公証システムガイドライン作成に向けて）」は，オープンネットワーク上での商取引における安全性・信頼性確保のためのガイドライン作成に向け，電子公証の必要性と目的，企業間取引の取引形態の特性，企業間取引および企業内業務での実ビジネス上での電子公証に対するニーズ調査や電子公証を実現するのに必要な基本的な機能について検討をまとめたものです。

国際連携WGの「海外のEC関連企業・組織の動向調査」は７ヶ国，39企業・組織の動向をまとめたものです。またコンタクトパーソンやメールアドレス，ホームページのアドレスも記載している事による手引書の役割も果たしています。

これらの中間成果報告書（計17冊）については会員への発送後，WWW等で一般の方々にも公表しています。また，報告書をご入用の方については，実費にて頒布しています。さらに報告書の概要は英訳して英文ホームページでも紹介しており，海外からも高い評価を得ています。詳しくはECOMホームページ（URL：http://www.ecom.or.jp/seika/doclist.htm）をご覧ください。

作成WG	報告書タイトル
WG01	モール構築技術実証評価モデル　ー表現・表示及び操作性ー（アルファ版）
WG02	商品属性情報標準化に関する調査報告書ー中間報告書ー
WG03	複合コンテンツ対応技術（エージェント機能）に関する調査報告書
WG04	企業・消費者間ECにおけるビジネスプロセス・ビジネスモデル解説書（α版）
	企業・消費者間ECにおけるEDIの現状調査報告書
WG05	共通セキュリティ関連技術WG中間報告書
WG06	本人認証技術検討WG中間報告書ー参照モデルと評価基準v0.5-
WG07	ICカードの現状調査報告書
WG08	認証局検討報告書
	海外認証局活動調査報告
WG11	国際電子商取引の制度的課題
	サイバーモールに関するモデル契約の検討
WG12	電子商取引における個人情報の保護に関する中間報告書
WG13	電子商取引決済関連問題検討WG中間報告書
WG14	電子商取引における消費者取引の課題に関する中間報告書
WG15	「電子公証検討調査報告書」ー電子公証システムガイドライン作成に向けてー
WG21	海外のEC関連企業・組織等の動向調査

3. プロジェクト連絡調整委員会の活動

プロジェクト連絡調整委員会では，毎回2～3プロジェクトからの現状報告やECOM WGの活動状況報告を行い，相互の連携，調整，交流を図っています。平成9年2月から9月までの間に，第9回から第14回まで計6回プロジェクト連絡調整委員会を開催しました。

4. 普及広報関連の活動

(1) ECOMかわら版の発行

会員向けニューズレターとして「ECOMかわら版」を4月～9月の間に2回発行し，WGの進捗状況等を会員に報告しました。

(2) ECOMセミナーの開催

4月～9月は以下の日程でECOMセミナーを開催しました。

◆ 第12回ECOMセミナー

日時：平成9年5月22日(火) 14:30～16:45

プログラム：

・「電子商取引と消費者問題について」
　松本 恒雄 氏（一橋大学教授，消費者取引検討WG主査）
・「個人情報保護と電子商取引について」
　堀部 政男 氏（中央大学教授，プライバシー問題検討WG主査）

◆ 第13回ECOMセミナー

日時：平成9年5月30日(火) 14:00～17:15

プログラム：

・「モール構築技術（表現・表示・及び操作性）について」
　東 昌弘 氏（モール構築技術検討WG主査）
・「商品属性情報標準化検討の中間報告」
　田中丸 愼二 氏（商品属性情報標準化検討WG主査）
・「複合コンテンツ対応技術検討の中間報告」
　白井 万佐寿 氏（複合コンテンツ対応技術検討WG主査），松坂 修 氏（同WG副主査）
・「コンテンツプロバイダー／モール間ビジネスプロトコル検討の活動報告」
　大野 仁勝 氏（コンテンツプロバイダー／モール間ビジネスプロトコル検討WG主査）

◆ 第14回ECOMセミナー

日時：平成9年6月10日(火) 13:45～16:00

プログラム：

・「ICカード型電子マネーセキュリティガイドライン」
　五味 俊夫 氏（共通セキュリティ関連技術検討WG主査）
・「本人認証の評価基準v.0.5」
　菅 知之 氏（本人認証技術検討WG主査）
・「国際電子商取引の制度的課題」
・「サイバーモールに関するモデル契約の検討」
　長 博連 氏（国際取引WG主査）

◆ 第15回ECOMセミナー

日時：平成9年7月14日(月) 14:30～16:50

プログラム：

・「特許から見た電子マネー」
　廣岡 浩平 氏（特許庁審査第五部計算機応用上席総括審査官）
・「電子マネーシステムについて（NTT)」
　藤岡 淳 氏（日本電信電話(株)情報通信研究所 分散環境アーキテクチャ研究部主任研究員）

◆ 第16回ECOMセミナー

日時：平成9年9月26日(金) 13:30～17:00

プログラム：

・「米国EC最新事情－前川レポート総集編－」
　前川 徹 氏（情報処理振興事業協会 技術センター所長）
・「メディアポート名古屋」

新保 尚二 氏（(株)名鉄コンピュータサービス マルチメディア事業部副長）

・「カードレス・カードシステム・プラットフォーム開発実験」

濱島 幸生 氏（(株)野村総合研究所 サイバーコマース事業部副主任コンサルタント）

・「SECE」

古田 茂樹 氏（富士通(株)ソフトウェア事業部主席部長）

舘上 章 氏（(株)日立製作所 ビジネスシステム開発センタ エグゼクティブコンサルタント）

竹谷 清康 氏（日本電気（株）EC推進本部企画開発部）

(3) EC関連5団体合同懇親会

平成9年7月16日（水）に東京全日空ホテルにおいて，EDI推進協議会，CALS推進協議会，STEP推進センター，CALS技術研究組合との共催で，電子商取引推進のための技術交流会を開催しました。

席上，企業消費者間EC推進事業の紹介として，「Cybernet Club」（(株)ユーシーカード），「EC実験における複合コンテンツサービス開発・提供プロジェクト」（ぴあ(株)），また企業間ECの事例として「VFMネットパッケージシステム開発・実証実験プロジェクト」（ジェフサセントラル(株)），「自動車産業におけるCALS実用化研究事業」（生産・調達・運用支援統合情報システム技術研究組合）のデモンストレーションが行われ，参加者の強い関心を集めていました。

(4) 展示会への参加

◆ダイレクト・マーケティング・フェア '97－広がる通販ワールド展－への参加

昨年に引き続き，平成9年9月17日（水）～21日（日）に池袋サンシャインシティ文化会館で行われた標記展示会にECOMブースを出展しました。一般来場者が多かったため，まだ電子商取引という言葉に馴染みのない消費者の方々に対してECおよびECOMの活動を広く紹介しました。

同会場において行ったECに関する意識調査の結果は，10月28日（火）にプレス発表を行い，朝日新聞を含む4紙に取り上げられました。また現在，ECOM機関誌，WWW等で公表しています。

◆COM JAPAN 1997への出展

平成9年11月4日(火)～7日(金)に東京ビッグサイトにおいて行われたCOM JAPAN 1997に，実証実験プロジェクトとECOM合同で「コンシュマーECパビリオン」を設け，プロジェクトおよびECOMの活動を広くPRしました。パビリオン来場者数は4日間で5,983名と非常に多くの方が来場され，電子商取引に対して強い関心を持っている事が裏付けられました。この展示会への参加は以下の13プロジェクトとECOM事務局です。

・サイバースペース上でのECを利用した商施設プロデュースの実験
・エレクトロニック・マーケット・プレース
・JapanNet
・Cyber Net Club
・多目的ICカードによる利便性の高いショッピングシステム
・メディアポート名古屋
・Smart Commerce Japan
・仮想展示会を中心としたECの大規模実証実験
・バーチャルシティ構想
・カードレス・カードシステム・プラットフォーム（CCP）開発実験
・EC実験における複合コンテンツサービス

開発・提供プロジェクト

・コマース・ナビゲーション・システム

・セキュアコマースプロトコルを実現する共通プラットフォームの開発（SECE）

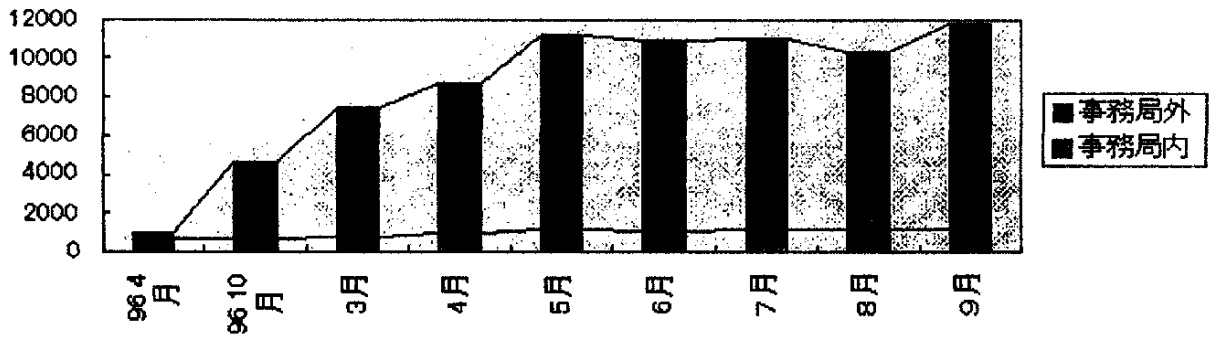
(5) WWWサーバーによる情報提供

What's newの項目を設け，ECOMに関する情報や電子商取引に関する情報を会員および一般の方にいち早く提供するとともに，メーリングリストの活用により，新規情報をホームページ上に発表する毎に電子メールで知らせるサービスを実施しています。なお，WGの中間成果等を順次掲載するなど，ホームページ情報の更新に力を入れた結果，アクセス件数は昨年を上回る結果となっています。

ECOM－WWWアクセス状況

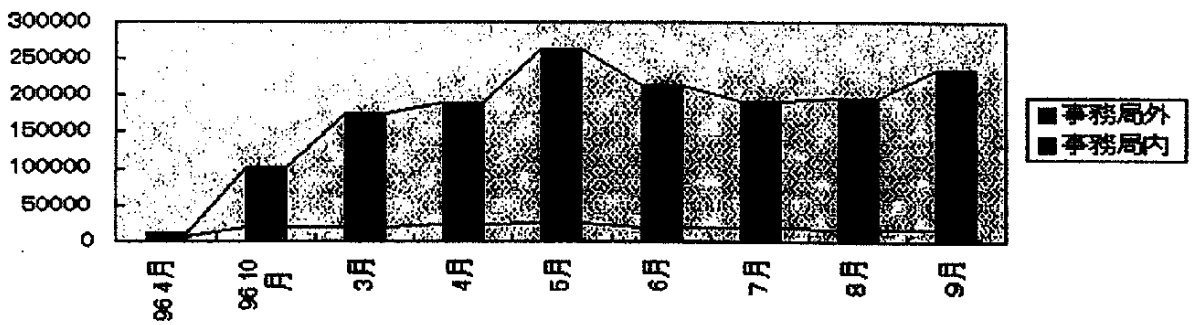
ホームページへの来場件数の推移

	96年4月	96年10月	97年3月	4月	5月	6月	7月	8月	9月
全体	933	4626	7400	8665	11190	10884	11016	10329	11779
事務局内	638	637	799	916	1175	1032	1192	1131	1179
事務局外	295	3989	6601	7749	10015	9852	9824	9198	10600



ホームページへのget数の推移

	96年4月	96年10月	97年3月	4月	5月	6月	7月	8月	9月
全体	10162	102714	174239	189856	262391	211736	190802	195205	233910
事務局内	6574	18697	17647	22558	24434	19030	18117	15735	16281
事務局外	3588	84017	156592	167298	237957	192706	172685	179470	217629



5. プロジェクトの進捗状況

ECOM活動の柱のひとつとして，19の実証実験等の連携・調整があります。これらのプロジェクトは通商産業省および情報処理振興事業協会（IPA）の「エレクトロニック・コマース推進事業」として進められているものです。

(1) サイバースペース上でのECを利用した商施設プロデュースの実験

1997年4月より実験サービスを開始しました。現在出店企業は94社，1,100点を超す商品を揃え，バーゲンやお勧め商品企画などを実施しています。さらに，「まちこ」では3次元の街を歩いている人とチャット（会話）が楽しめるのが特徴です。

(2) エレクトロニック・マーケット・プレイス

1997年4月よりモニター数2,000名にて電子決済実証実験を開始しました。また7月より実商店実証実験を開始しました。現在三鷹を中心として幕張，銀座，自由が丘等で使用する事ができます。特徴として，希望者には三鷹市の市民カードの機能を追加する事ができます。

(3)「上田地域仮想社会におけるケーブルインターネットの構築と実証実験」

1997年10月から実証実験がスタートしました。現在60を超える企業が仮想行列，仮想商店街，仮想百貨店，仮想国内見本市等に参加しています。

(4) JapanNetプロジェクト

1996年11月より実証実験を開始しました。現在相互認証を目的とした最終フェーズに入っています。特徴として独自の認証局を立ち上げ，ECの基盤となる技術開発を行っています。

(5) Smart Collar Club電子商取引実証実験

1997年7月より実証実験を開始しました。現在，電子決済システムの開発に着手しています。特徴としては，電子小切手を用いるスマートチェック方式と，国際標準と目されるSETをベースとするクレジットカード方式の2通りの決済方法を提供しています。

(6) Cyber Net Club

1996年6月に実証実験プロジェクトのトップを切って実証実験が開始されました。実用化を目指したクレジットカード決済スキームの確立を目的として現在，10万人規模の実証実験を目指しています。

(7) 多目的ICカードによる利便性の高いショッピングシステム

電子マネーの技術開発プロジェクトとして現在，開発中です。特徴としてICカードを媒体とした高いセキュリティと利便性を兼ね揃えています。コンソーシアム形成後，実証実験も行う予定です。

(8) CCC（サイバーコマースシティ）

1996年10月に実証実験を開始しました。オール関西プロジェクトとして，特に中小企業や地場産業の活性化に焦点を当てています。現在，クレジットカード決済とともに新しく銀行決済も導入し，より高い利便性を提供しています。

(9) メディアポート名古屋

1997年4月に実証実験を開始し，7月に電子決済も開始しました。現在，120社を超える企業が参加しており，バーチャルモールの存在意義を考え，利用者にとって本当に魅力的な仮想都市を目指しています。

(10) 電子商取引における認証／暗号／決済の方式開発と実用性の実験（Smart Commerce Japan）

1997年10月に実証実験を開始しました。現在，３万人のモニターを対象に，神戸市内でダイエーグループのスーパー，コンビニエンスストア，ホテルなど60店舗に加え，市内の大学，一般店舗などに合計約1,000台の端末を設置しています。

(11) 仮想展示会を中心としたECの大規模実証実験

1997年６月にエンドユーザー向けのサービスを開始しました。現在，登録ユーザー数は１万人を超え，情報ナビゲーション機構に関するアンケート実施しています。

(12) バーチャルシティ構想

1997年５月に実証実験を開始しました。現在，銀行口座決済のサービスを開始しており，またSMMK（スーパーマルチメディアキオスク）を三越本店（６/17），ひらまつ原宿店（７/29），ひらまつ広尾店（７/31）に設置しています。

(13) 電子公共サービス統合システム
～ワンストップ・サービスの実現～

1997年７月に実証実験を開始しました。現在，市役所をはじめとして更埴市各所にパブリック・ターミナル（利用者端末）を設置し，１つの端末で電気，ガス，水道等の手続きを可能にしています。

(14) カードレス・カードシステム・プラットフォーム（CCP）開発実験

1997年11月に実証実験を開始しました。現在，会員数は6,000名を超え，11月にはSET準拠のオンラインクレジット決済システムの導入予定です。

(15) EC実験における複合コンテンツサービスの開発・提供

現在，複合サービスの検索機能，および単体サービスの作成機能の開発を進めています。また間もなく，複合サービスの作成機能の開発に取りかかる予定です。

(16) 会話型マルチメディア情報（MHEG）相互交換実験

マルチメディア国際標準MHEG-5を利用する規定である実装規約と，それに対応したソフトウェアプロダクト MHEGビューア，MHEGオーサリングツールの開発を進めており，現在，多通信用実装規約とソフトウェアプロダクトを公開しました。

(17) コマース・ナビゲーション・システム

現在，プログラミングなどは完成しており，実験という形でオープンにしていく準備をしています。11月には一般に公開できる予定です。

(18) セキュアコマースプロトコルを実現する共通プラットフォーム開発

1997年10月に研究会のまとめとしてクレジットカード支払に関しては，SECE研究会クレジット部会報告書とSECE研究会クレジット部会報告書付録，また銀行取引に関しては，SECE支払決済（銀行取引）概説書を公開しました。

(19) EC用非接触ICカードおよび汎用端末用リーダライターユニットの技術開発

1997年８月にISO/IEC10536に準拠した密着型ICカード，またリーダライターユニットの試作が完了し，各仕様書に基づいて検証評価を行っています。

STEP推進センター

STEP推進センターは日本情報処理開発協会に移管されて以来，平成９年末でほぼ２年半になります。平成８年秋の事務局体制の大幅強化から１年以上が経過，平成９年度は従来からの国際標準化，JIS原案作成，標準化調査プロジェクトなどのほか，CALS技術研究組合などとの連携によるCALS/STEP連絡会およびCALS/SGML連絡会の運営など，前年度からの活動も順調に進んでいます。また，STEP実用化促進のための「HLDAI（High Level Data Access Interface）開発プロジェクト」も最終年度を迎え，今年度中に成果がまとまる予定です。

1. 国際標準化事業

(1) ISO国内対策委員会の開催

製品モデルデータ交換のための国際規格（STEP）の開発に関する審議を行ない，DIS（Draft International Standard）13件，CD（Committee Draft）22件，NWI（New Work Item）７件，その他18件に対して回答および投票を行いました。

(2) ISO国際会議への参加と交流

チェスター（イギリス），サンディエゴ（アメリカ），フローレンス（イタリア）で開催されたISO TC184/SC4/WGsの会議に参加し，STEP規格開発の各WG審議に出席して，日本からの意見提案を行なうとともに，各国STEPセンターとの情報交換を行ないました。

韓国で行われたチュートリアルワークショップに主任研究員を講師として派遣し，日本のSTEP関連活動を報告したほか，台湾，EUからのミッションの訪問を受け，STEPに関連する状況について情報交換を行いました。

(3) 産業別AP開発組織とのリエゾン

業種別CALSプロジェクトでのSTEPへの取り組みに対して，AP規格，開発環境，ツール等につき，セミナー，情報交換，技術支援を実施しています。また，各プロジェクトが効率よく推進できるよう，今後も積極的に取り組みます。STEP規格開発は佳境に入っており，産業界のニーズに答えるため，そしてP-Member国として対応するための組織について検討を進めています。

2. JIS原案作成事業

平成７年にPart1（概要および基本原理）ほか７分冊，平成８年度にPart44（製品構造形態）ほか３分冊についてJIS原案を作成したのに続き，平成９年度はPart105（キネマティクス），Part202（製品モデルとの関連を持つ図面表現）のJIS原案作成作業を進め，今後制定されるSTEP国際規格への対応を検討しました。また，STEPに関する用語集（Version2.0）を作成，冊子にして関係者に配布するとともに，ホームページに掲載し広く発信しました。

3. プロジェクト推進事業

前年度に引き続き，標準化動向を調査し，発電プラントで用いられる製品モデルデータの表現技術，交換技術等に関する調査研究を行うとともに，今後重要となる基礎技術について８つのワーキンググループ（WG）に分かれて活動を展開，その成果を報告書にまとめます。なお，前年度までの「製品管理WG」は活動を終了し，「３次元設計WG」については内容を一部変更して名称を「設計部門におけるSTEP活用技術WG」としました。

各WGと研究テーマ：概要は次の通りです。

①発電プラントWG

発電プラントのライフサイクル全般を支援するプラント・プロダクト・モデルの検討を進めます。本年度は平成８年度に開発したARMの評価のため，机上シミュレーションを実施し，ブラッシュアップを図ります。

②設計でのSTEP活用技術WG

STEPの実用期を迎えようとしている現在，製図・PDM（Product Data Management），TDP（Technical Data Package）などの分野に産業界の強い関心が注がれています。本WGでは，この設計部門での利用技術に関する日本および世界の状況について調査検討を行い，実用化の現状とその利用技術に関する知見を得るものとします。

③生産設計WG

前年度から着手した実証推進プロジェクトの１つ「AP224を中心とした設計から生産準備への情報伝達モデル実験」の開発作業を積極的に支援するとともに，そこで開発されたシステムを利用して，設計・生産のインタフェースに関連するSTEP開発技術の企業での有効性を検討・確認します。

④アセンブリモデルWG

これまでのアセンブリモデルの検討に基づき，本年度はキネマティックスモデルのスキーマ構造に基づいたデータベースの開発およびアセンブリモデルとそのデータベースの開発を行います。

⑤パラメトリックスWG

前年度はパラメトリックモデル化技術等に関して既存CADのベンチマークを含めて調査研究を実施しました。本年度はこの成果を踏まえ，パラメトリックモデルの仕様検討を加速します。また，大型車両・橋梁・ビル・土木などのユーザーニーズを調査するとともに，上記ユーザーに関するベンダー側の開発計画を踏まえてユーザーニーズの方向性との整合を確認します。

⑥プロダクトモデル記述言語WG

前年度に引き続き，プロダクトデータ記述言語に関する技術調査（基礎技術とEXPRESS/SDAI関連技術）を行います。さらに，プロダクトデータ記述言語の要求仕様について素案のとりまとめを行います。

⑦機械部品WG

前年度に引き続き日本版P-LIB（パーツ・ライブラリ，ISO-13584の日本版インプリメント）の技術評価および普及・検討を実施します。さらに，標準部品利用時の設計知識ベース構築法の調査研究を実施します。

⑧実証推進WG

プロジェクト最終年度（平成10年度）に向けて，プロダクトモデルデータ交換実験を行います。その具体的な実施テーマは，「AP202図面データ交換とAP203とのインターオペラビリティ検証」および「AP224を中心とした設計～生産準備への情報伝達モデル実験」です。本年度は，交換実験に向けてその環境設定と一部データ準備を行います。

4. 調査・研究事業

STEP普及促進活動の一環としてセミナーなどを開催しイベントに参加しています。

(1) STEPセミナーの実施

◆「欧州に於けるSTEP実装技術の最新動向」

日時：平成９年６月17日(火) 14:00～17:00

場所：STEP推進センター会議室（タイム24ビル10階）

講師：Peter Smith 氏（ICS社）

参加人数：20名

内容：AP221をベースとするデータウェアハ

ウス実装システムの概要説明と，その対象となったETAPプロジェクトの事例を紹介。

◆「AP203の基礎と概要」

日時：平成９年８月29日(金) 10:30～17:30

場所：青海フロンティアビル２階大会議室

参加者数：102名

内容：

・「AP203/CC1概要と構造の紹介」
滝本 郁也 氏（川崎重工業(株)航空宇宙事業本部情報システム部主幹）

・「AP203/CC6概要と構造の紹介」
宇田川 佳久 氏（CALS技術研究組合（NCALS）実証第4G（三菱電機(株)），工学博士）

・「Part42概要と構造の紹介」
小林 一也 氏（県立富山大学工学部機械システム工学科助教授，工学博士）

◆「CALS/STEPによる製造業のデジタル・プロセス革新」
（「第８回生産技術に関する国際会議」のプログラム）

日時：平成９年８月20日(水) 13:50～15:30

場所：札幌市　北海道大学学術交流会館

主催：精密工学会北海道支部

共催：(財)日本情報処理開発協会STEP推進センター

協賛：北海道通産局，北海道，札幌市

内容：

・「電子商取引による産業経済社会の将来像」
芳川 恒志 氏（通商産業省情報政策企画室長）

・「CALS/STEPによる製造業のデジタル・プロセス実証実験」
杉本 岑生 氏（STEP推進センター技術部長）

・「STEP/AP203による次世代CAD/CAM統合技術」
坂本 千秋 氏（アプライドコマツテクノロジー（株）ディレクター）

参加者数：約100名

(2) 平成８年度成果報告会の実施

◆標準化調査プロジェクト事業

日時：平成９年７月15日(火) 10:00～17:00

場所：有明TFTビル東館９階903号室

内容：平成８年度各WG主査によるプレゼンテーション

出席者：90名

◆調査普及事業

日時：平成９年７月16日(水) 13:00～15:30

場所：有明TFTビル東館９階903号室

内容：

・「情報技術革新とSTEP—ユーザーの期待とベンダーの課題—」
綾 日天彦 氏（調査普及委員長）

・「STEP実用化に向けての調査報告—米国及び日本—」
松崎 幸一 氏（STEP推進センター主任研究員）

出席者：71名

(3) 展示会への出展

◆ICCAS' 97(注) 併設展示会

主催：(社)日本造船学会

期日：平成９年10月14日(火)～16日(木)

場所：パシフィコ横浜　会議センター

JSTEP出展内容：パネル展示，資料配付

・STEPの意義
・JSTEPの活動内容
・HLDAI開発の意義と内容

(注) ICCAS＝International Conference on Computer Applications in Shipbuilding

◆CALS Expo' 97

主催：CALS推進協議会，NCALS，(財)日本情報処理開発協会など

期日：1997年11月４日(火)～７日(金)
場所：東京国際展示場（東京ビッグサイト，有明）東１ホール
JSTEP出展内容：ビデオ，パネル，インターネットによる展示，資料配付
・STEPの意義
・JSTEPの活動内容
・HLDAI開発の意義と内容
・生産設計WGの成果紹介(AP203と224によるCAD/ACAM結合)

5. IPA事業（企業間高度電子商取引推進事業）

(1) HLDAIの開発

HLDAIの開発はSTEPを利用するために必要なシステム構築を出来るだけ容易にする機能を構築する目的で，情報処理振興事業協会（IPA）との契約に基づき平成８年度に着手しました。前年度の基本設計に続いて，平成９年度はプログラムの製作と，HLDAIを実際のSTEPデータ交換処理システム開発に利用する実験を行い，その機能，特性を検証し，HLDAIのSTEP実装ツールとしての実用性を実証します。

6. CALS/STEP，CALS/SGML両連絡会の運営

STEP，SGMLを利用する業種CALSプロジェクト間の進捗状況把握，実装のための技術的課題，共通インフラ部分の知識共有など技術交流を活性化することを目的にしています。両連絡会ともに月１回程度の開催で，並行してメーリングリストを開設し随時，情報や意見の交換を行っています。参加メンバーは通商産業省機械情報産業局関係者，業種CALSプロジェクトの担当者，JSTEP主会員専門技術者，JSTEP技術部・業種支援Ｇなどで構成し，人数はともに50名程度です。

先端情報技術研究所

先端情報技術研究所（AITEC：Research Institute for Advanced Information Technology）では，内外の先端情報技術の研究開発動向調査を通じて，政府支援の研究開発のあり方について検討する調査研究事業（技術調査部）と第五世代コンピュータ技術研究成果の普及促進事業（第五世代普及振興部）の両事業を実施しています。

ここでは，これまでの経緯を含めて，平成９年度事業について紹介します。

1. 技術調査部の活動

(1) 情報技術の政府支援研究開発のあり方に関する調査研究

わが国のソフトウェア産業を中心とする情報産業について，その国際的な競争力をいかにして確保するか，ならびに，その解決策として，国の研究開発のあり方をいかに変革すべきかといった問題に関連する調査活動を行っています。

この調査の実施にあたり，平成８年度は，第１に，従来のわが国情報産業の育成策や国家プロジェクトの枠組み，実施体制について問題点の整理を行い，今後へ向けての改善策を検討し，「資料-1　わが国が行う情報技術研究開発のあり方に関する調査研究」としてとりまとめました。

次に，先端的な情報技術の先進国であり，世界市場の大半を独占している米国において，先端的ソフトウェア技術や情報技術を生み出

している産・学・官の連携のメカニズムや政府支援策について調査を行いました。この調査においては，研究者のアイデアが研究開発へと成長していく上流部分と，研究開発成果を磨きあげ製品化し，さらに市場を創造していく下流部分に分けて，その成功の要因を探り，「調査資料-1　米国における政府系研究予算の戦略的決定・執行体制」，「調査資料-2 米国情報産業における研究成果の製品化・市場創造プロセス」としてとりまとめています。

この結果，米国における成功の要因として，大学と産業界の密な協力体制と，省庁間の公開的かつ競争的（オープン&コンペティティブ）なファンディングによる優れた研究の選択と自然発生的な省庁間連携が重要な役割を演じていることがわかりました。

平成９年度は，平成８年度の調査結果を基に，わが国の政府支援情報産業のあり方について検討を進めています。

(2) 先端情報技術の研究開発動向調査

今後の情報産業を牽引する可能性のある技術に関して，その現状と将来動向を調査しています。

①ペタフロップスマシン技術調査

現在，米国において15年先を目指して行われているペタフロップスマシンの研究開発プロジェクトについて，平成８年度はその研究開発動向を調査し，「資料-2　ペタフロップスマシン技術に関する調査研究」としてとりまとめました。

平成９年度は，ペタフロップスマシンなどの超並列コンピュータの応用からのニーズ，研究実施の動機を分析するとともに，技術開発状況の日米比較，開発潜在能力などの調査を通じて，中期的な研究課題を明らかにし，これらの研究開発における政府支援の関与はどうあるべきかについて検討することとしています。

②ヒューマンセンタードインテリジェントシステム技術調査

情報技術の新たなニーズを満たすべく活発に研究開発が行われているネットワークやAI関連の技術テーマに関しても，最近注目を集めているソフトウェア技術を中心に調査を行っています。平成８年度は，その研究開発動向を調査し，「資料-3　ネットワーク及びAI関連新技術に関する調査研究」としてとりまとめました。

平成９年度は，ネットワークやAI関連の新技術として，エージェント指向ソフトウェア，マルチモーダルインタフェース，仮想現実などの研究を「人間を中心とした利用技術」として体系的に捉えて，研究課題を明らかにしていくこととしています。

インターネットのようなグローバルなネットワークで接続された世界では，それが通信を行なう場としてだけではなく，それらのコンピュータが保持しているデータ群を巨大なデータベースとして捉えることができます。このネットワークから情報をうまく取り出したり，その情報を利用してコミュニケーションを効率化するための新技術の実現手段として，上記新技術の相互関係を検討しています。

2. 第五世代コンピュータ技術開発成果の普及

第五世代コンピュータ技術の成果であるICOTフリーソフトウェア（IFS）の普及を図るため，以下の業務を実施しています。

(1) IFSの維持改良および公開

第五世代普及振興部では，IFSの普及促進策の一環として，平成８年度の委託研究成果

物（27テーマのうち16テーマについては平成７年度からの継続）をWWW上に公開しました。

また，第五世代普及振興部では，平成９年度の委託研究の内容を紹介するため，22テーマについてHTML化を図っています。

(2) IFSをベースとした新しいソフトウェア資源の創造

第五世代普及振興部では，ネットワーク社会を迎え，さらに重要性を増している並列知識情報処理技術の活用促進を目的に，IFSを核とした知的ソフトウェア資源の研究開発を，内外の大学への委託により実施しています。

また，IFSや新たに作成する知的ソフトウェア資源の創造と共有するためのメカニズムに関する調査研究を実施しています。

①知的ソフトウェア資源の実験的研究開発

第五世代普及振興部では，平成７年度より知的ソフトウェア資源の委託による研究開発を継続して実施しています。

平成９年度は，公募の対象を国内の大学に限らず，海外の大学も対象にしたところ，多数の応募がありました。

応募してきた提案書は，例年通り，数十人の査読者による査読と知的ソフトウェア委託研究審査委員会（委員長：淵 一博・慶応義塾大学理工学部管理工学科教授）での評価・審査を行いました。

今年度の審査では，大学や企業の研究者が，次の研究や開発のツールとして役立つものに重点をおいた審査を行い，22件の研究開発委託が決まりました。

今回の公募は，研究開発期限を１年のものと２年のものの２通りで行ったところ，１年のものが24件，２年のものが13件，合計37件の応募がありました。さらにこれを，国内，国外別の応募状況について見ますと，国内は，１年のものが15件，２年のものが７件，海外は，１年のものが９件，２年のものが６件でした。

このうち，国内，国外別の合格状況について見ますと，国内は１年のものが９件，２年のものが４件，合格しました。また，海外は，１年のものが４件，２年のものが２件，合格しました。

なお，研究開発委託の件数は，平成８年度からの継続分の合格が３件あったため，今年度分の合格19件と合わせて22件となりました。

国　別	応募数		合格数	
	１年	２年	１年	２年
国　内	15	7	9	4
昨年度継続	—	—	3	—
国　外	9	6	4	2
アメリカ	5	3	2	0
イギリス	1	1	0	1
オーストラリア	2	0	1	0
フランス	1	0	1	0
ロシア	0	1	0	0
オーストリア	0	1	0	1
合　計	24	13	16	6

②知的ソフトウェア資源の創造と共有メカニズムの調査研究

この事業は，IFSを含む知的ソフトウェア資源の研究開発とそれをフリーソフトウェアにすることによって共有し，次の研究や商品開発のツールとするための仕組みに関する調査研究を行い，情報処理の研究や商品開発に役立てることを目的として実施しています。

今年度も，先進的ソフトウェア普及促進策調査研究委員会（委員長：田中 穂積・東京工業大学大学院情報理工学研究科教授）および作業部会（主査：小林 慎一・（株）三菱総合研究所経営システム研究センター情報技術開発部長）を設置し，調査検討および取りまとめを行っています。

今年度の調査に当たっては，対象を大学に限定し，AITECが実施している委託研究の方式の有効性の検証，平成９年度から実施している海外への委託研究の成果と国内への委託成果の比較等を行い，指針として取りまとめを行います。

(3) IFSの普及広報等

①IFS講習会の実施

平成９年９月30日に，「KLICプログラミング・コンテスト」の一環としてAITECにおいて「KLIC講習会」を開催し，12人の参加がありました。

平成９年10月９日には，神戸大学・滝川記念会館における「INAP'97 PROLOG産業化シンポジューム」において「KLIC：並列論理型言語KL1の汎用機上での処理系」（講師：近山 隆 氏・東京大学教授）についての講演を行い，IFSの普及に努めました。

平成９年10月22・23日の両日には，慶應義塾大学にてKLIC講習会を行いました。

②KLICプログラミング・コンテストの実施

AITECでは，前年度に引き続き「KLICプログラミング・コンテスト実行委員会」（委員長：溝口 文雄 氏・東京理科大学教授）を設けて，KLICを用いたプログラミング・コンテストを実施しています。

今年度の課題は，「逐次環境部門」が「１人ポーカーゲーム」，「並列環境部門」が「LIFEゲーム」に決まりました。昨年と比べて今年の課題は難しいとの事ですが，どのような作品が集まるか事務局としては楽しみです。

なお，多くの皆様に参加して頂くために，KLICプログラミング・コンテストの広報活動として情報処理学会誌，ビット，UNIXマガジン（10月号）に広告を掲載しました。また，同時にNewsgroupへの投稿やWeb上でも参加を呼びかけました。

課題が昨年と比べて難しい，ということで参加登録は48件で昨年と比べて少ないようです。

③IFSのアクセス状況

平成４年８月より公開を行っているIFSは，世界中から数多くのアクセスがあります。平成９年９月末時点では，50ヶ国以上の国々から累計で約３万7,700件のアクセスがありました。

アクセスが多い上位５位までのソフトウェアは，

1) 並列論理型言語KL1の汎用機上の処理系：KLIC
2) 制約論理型言語：cu-Prolog
3) 形態素辞書
4) 囲碁対局システム：逐次版「碁世代」GOG
5) 構文解析処理プログラム

となっています。中でもKLICのアクセス件数の伸びが顕著で２位を大きく離しており，約1,630の方々からFTPされています。

平成９年度下期研修のご案内

(1) 情報処理技術インストラクタ養成等　短期研修

	コース番号	研　　修　　名	開催日・開催地	研修料
情報化人材育成等コース	ISDA1	表現技法	10.3.23～27	75,000
	ISDB1*	改訂：第二種共通カリキュラム共通知識指導ポイント	10.3.23～26	60,000
システムアドミニストレータコース	ISED1	システムアドミニストレータのためのWebマスター入門	10.3.25～27	45,000
教育エンジニア等コース	ISAA2	教育エンジニア～企画型業務	10.2.16～20	75,000
	ISAB2	教育エンジニア～インストラクション業務	10.3. 9～13	75,000
	ISAC2	説得力を高めるマルチメディアプレゼンテーション技法	10.3.18～20	45,000
	ISAD2	教育心理学入門	10.3.25～27	45,000
技術動向コース	ISBA2	PCネットワーク技術動向とインターネット/ホームページ概説	10.3.23～24	30,000
	ISBB2	オープンシステム技術	10.3.20	15,000
	ISBC2	教育・広報に役立つマルチメディア技術の基礎	10.3.20	15,000
システム技術コース	ISCB2	実践的クライアントサーバ環境アプリケーション開発実習	10.3.16～18	45,000
	ISCC2	VisualC++の実践演習（基礎）	10.3.16～17	30,000
	ISCF2	Java活用テクニック（J++環境）	10.3.26～27	30,000
	ISCG2	小規模（部門内）ネットワークの設定と運用基礎	10.3.19～20	30,000
	ISCI3	イントラネットにおけるWebサーバ業務システム構築法	10.2.25～27	45,000

＊・研修は原則10:00～17:00までの６時間です。（一部に時間延長があります。）
・「ISDB1」は改訂カリキュラムに基づいた内容で実施します。
・開催地の明記がない研修は、すべて東京（中央情報教育研究所）です。
・研修料には消費税を含んでいません。別途５％の消費税を申し受けます。

(2) 高度情報化人材の研修

コ　　ー　　ス　　名		日　数	期　　間	研修料
プロジェクトマネージャ	・プロジェクト管理総論	３日間	２月18日～２月20日	72,000
	・プロジェクトの品質管理	２日間	３月 5日～３月 6日	48,000
	・協力会社管理	３日間	２月25日～２月27日	72,000
	・プロジェクトの進捗管理	３日間	３月11日～３月13日	72,000
プロダクションエンジニア	・内　部　設　計	４日間	３月 3日～３月 6日	96,000
	・品　質　管　理	２日間	３月 9日～３月10日	48,000
ネットワークスペシャリスト	・データ伝送技術とアーキテクチャ	３日間	１月27日～１月29日	72,000
	・通信回線と通信機器	３日間	２月 3日～２月 5日	72,000
	・ネットワークソフトウェア	２日間	２月12日～２月13日	48,000
	・ＬＡＮの要求定義・設計・構築・評価	３日間	２月17日～２月19日	72,000
	・ＷＡＬの要求定義・設計・構築・評価	４日間	３月10日～３月13日	96,000
	・ネットワークシステムの運用と保守	３日間	２月24日～２月26日	72,000
データベーススペシャリスト	・データベースの基礎理論	２日間	２月18日～２月19日	48,000
	・データベースシステムの設計と運用	３日間	２月23日～２月25日	72,000
	・データベース技術動向	２日間	３月 4日～３月 5日	48,000
システム運用管理エンジニア	・運　用　管　理	４日間	２月 2日～２月 5日	96,000
	・資　源　管　理	２日間	２月 9日～２月10日	48,000
	・障　害　管　理	２日間	２月12日～２月13日	48,000
	・システム保守とセキュリティ管理	２日間	２月16日～２月17日	48,000
	・性能管理とシステム評価	３日間	２月23日～２月25日	72,000
	・運用システム・標準化・開発環境	２日間	３月 2日～３月 3日	48,000
	・移行・運用テストとシステム移行	1.5日間	３月 4日～３月 5日	36,000

・研修料には消費税を含んでいません。別途５％の消費税を申し受けます。

財団法人　日本情報処理開発協会　中央情報教育研究所　教務部
〒135-73　東京都江東区青海2-45　タイム24ビル　19階
TEL.(1) 教務一課　03-5531-0175　　FAX.03-5531-0170
(2) 教務二課　03-5531-0176　　ホームページURL http://www.interport.ne.jp/cait/

情報処理教育関係者必携の書

―― 高度情報化人材育成標準カリキュラム（改訂版）発刊 ――

中央情報教育研究所は，平成５年度に「通商産業省産業構造審議会情報産業部会情報化人材対策小委員会」の提言を受けて，「高度情報化人材育成標準カリキュラム」（17種）を人材別に刊行いたしました。

以来，約３年を経て情報処理技術の飛躍的進展，環境の変化等により改訂の必要性が議論され，ここに情報処理産業界有識者等のご支援・ご協力を得て13種の改訂を行い，下記のとおり刊行することとなりました。本標準カリキュラムは，**平成10年秋期情報処理技術者試験**から反映されることとなりますので，情報処理技術者育成に携わっておられる皆様におかれましては，教育の指針ともなりますので，必携の書として是非ご購入をご検討下さるようお願い申し上げます。

記

1．発刊時期	平成９年11月20日
2．発刊形態	CD-ROM for Windows（１枚に17種収録されています。） なお，冊子形式をご希望の方は，下記へお問い合わせください。
3．お申し込み方法	当研究所へFAX（FAX：03-5531-0170）により直接お申し込みください。
4．販売価格	12,600円／枚（本体価格12,000円＋消費税） 送料は，１枚－200円，２枚－270円，３～４枚－390円です。 それ以上はお問い合わせください。
5．その他	申込後１週間位でお届け致します。 CD-ROMの開封後の返品は，お受けしかねます。 なお，ご不明な点があれば03-5531-0177（普及振興課）へお問い合わせください。

以　上

CAIT (財)日本情報処理開発協会
中央情報教育研究所
〒135-73 東京都江東区青海2-45 タイム24ビル19階
http://www.interport.ne.jp/cait/

平成10年度 春期 情報処理技術者試験実施のお知らせ

平成10年度春期試験を，次のとおり実施する予定です。
受験を希望される方は，試験案内書・願書を取り寄せて，手続きをしてください。

1. 試験の区分及び受験資格

・プロジェクトマネージャ試験	平成10年４月１日現在　27歳以上
・システム運用管理エンジニア試験	平成10年４月１日現在　25歳以上
・プロダクションエンジニア試験	制限なし
・データベーススペシャリスト試験	制限なし
・マイコン応用システムエンジニア試験	制限なし
・第一種情報処理技術者試験	制限なし
・第二種情報処理技術者試験	制限なし

2. 試験日

平成10年４月19日（日）

3. 案内書・願書の配布及び受付期間

平成10年１月６日（火）～平成10年２月６日（金）

4. 受験料

5,100円

5. 試験地

全国56か所

6. 案内書・願書の配布場所

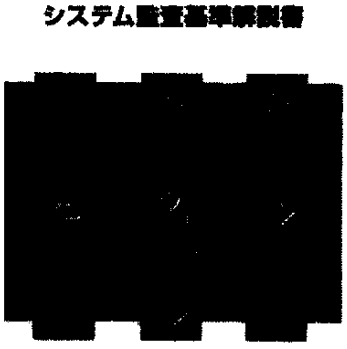
情報処理技術者試験センター各支部（電話番号は次のとおりです）

北海道支部	011-727-8556	東北支部	022-227-0901
関東支部	03-3436-1321	中部支部	052-261-6818
近畿支部	06-946-6301	中国支部	082-221-4505
四国支部	0878-37-2640	九州支部	092-472-4575
沖縄支部	098-862-2137		

■好評基準解説書シリーズ

改訂版システム監査基準解説書

監修 通商産業省　　発行（財）日本情報処理開発協会



情報システムは、従来のメインフレームを中心とする集中処理型のシステムから、クライアントサーバーのような分散処理型のシステムへ変化するとともに、オープンなコンピュータネットワークの世界的な広まりへと進展しています。

このような情報化の環境変化にともない通商産業省では昭和60年1月に策定・公表されたシステム監査基準を平成8年1月30日に全面的に見直しを行い「改訂システム監査基準」を公表いたしました。

改訂の主なポイントは、ダウンサイジング、ネットワーク化等情報化環境の変化への対応、阪神・淡路大震災を踏まえた地震対策の強化、国際化への対応等となっています。

全体構成は、総括的事項を示した「一般基準」、システム監査の具体的内容を示した「実施基準」、監査結果の取りまとめ事項を示した「報告基準」の3基準で旧基準と変りはありませんが、一般基準9項目、実施基準191項目、報告基準8項目の合わせて208項目（旧基準は127項目）と今回の改訂により大幅な増強・増補がなされています。

本書は、「改訂システム監査基準」を詳細に解説したもので、基準の改訂に合わせて全面改訂を行いました。

【目次】

1. システム監査基準
2. システム監査基準の解説
3. 一般基準
4. 実施基準
   ⑴企画業務
   ⑵開発業務
   ⑶運用業務
   ⑷保守業務
   ⑸共通業務
      ①ドキュメント管理
      ②進捗管理
      ③要員管理
      ④外部委託
      ⑤災害対策
5. 報告基準

＜参考＞
- 情報システム安全対策基準
- コンピュータウイルス対策基準
- ソフトウェア管理ガイドライン
- コンピュータ不正アクセス対策基準

【価格】

一般 4,078円／会員 3,262円（税込み・送料別）

B5判、カバー付、496ページ

【申し込み先】 財団法人 日本情報処理開発協会 調査部 普及振興課　FAX：03-3432-9389　E-mail：fukyu@jipdec.or.jp

※会員とは、当協会の賛助会員をいいます。
※全国の政府刊行物サービスセンターおよび政府刊行物サービスステーションでもお求めいただけます。

■好評基準解説書シリーズ

コンピュータ不正アクセス対策基準解説書

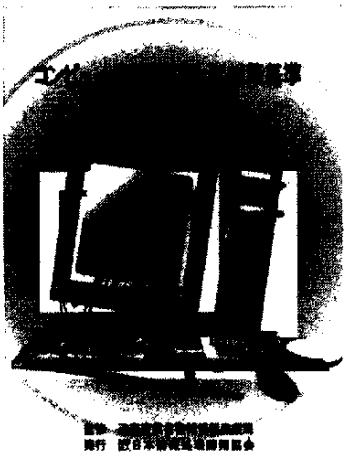
監修　通商産業省　　発行（財）日本情報処理開発協会

近年インターネットの普及と拡大が進むにつれ、セキュリティの重要性が注目されいています。

特に、他人のコンピュータにネットワークを介して侵入し、データの改ざんや破壊、不正な利用等を行う不正アクセスに対する認識が高まっています。米国では、すでに不正アクセスが社会問題化していますが、最近わが国でも不正アクセスの被害が起き始め、その対応への取り組みが始まりつつあります。

こうした状況から通商産業省では、不正アクセスによる被害の予防や発見および復旧ならびに拡大および再発防止について、企業等の組織および個人が実行すべきポイントをガイドラインとして取りまとめ、平成8年8月8日に「コンピュータ不正アクセス対策基準」を策定・公表いたしました。

本書は、基準全体の構成に沿い「システムユーザ基準」、「システム管理者基準」、「ネットワークサービス事業者基準」、「ハードウェア・ソフトウェア供給者基準」の全136項目について詳細に解説したものです。



【目次】

1. コンピュータ不正アクセス対策基準
2. コンピュータ不正アクセス対策基準の解説
3. システムユーザ基準
4. システム管理者基準
5. ネットワークサービス事業者基準
6. ハードウェア・ソフトウェア供給者基準

＜参考＞
- 通商産業大臣が指定した者(届出先)
- 情報システム安全対策基準
- システム監査基準
- コンピュータウイルス対策基準
- ソフトウェア管理ガイドライン

【価格】

一般 3,058円／会員 2,446円 (税込み・送料別)

B5判、カバー付、294ページ

【申し込み先】 財団法人 日本情報処理開発協会 調査部 普及振興課　FAX：03-3432-9389　E-mail：fukyu@jipdec.or.jp

※会員とは、当協会の賛助会員をいいます。
※全国の政府刊行物サービスセンターおよび政府刊行物サービスステーションでもお求めいただけます。

■好評基準解説書シリーズ

改訂版コンピュータウイルス対策基準解説書

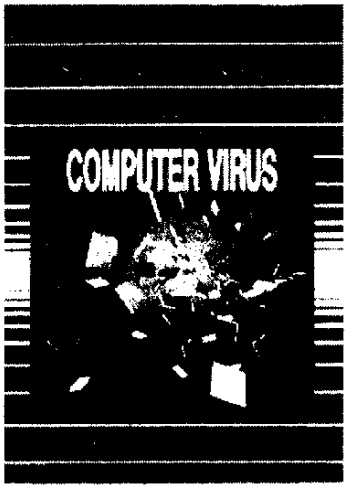
監修　通商産業省　　発行（財）日本情報処理開発協会

情報化社会の進展は、私たちに様々な恩恵をもたらす一方で、コンピュータウイルスという新たな社会問題を生み出しました。

通商産業省では、平成2年4月10日「コンピュータウイルス対策基準」を告示（第139号）してから今日まで、コンピュータウイルス対策の指導に取り組んできました。

この間、情報システムを取り巻く環境はネットワーク化の進展とも相まって著しい変化を遂げています。そのため、通商産業省では同基準を情報システムの現状に即した内容とするため全面的に見直しを行い、平成7年7月に「改訂コンピュータウイルス対策基準」を公表いたしました。

本書は、基準全体の構成に沿い、「システムユーザ基準」、「システム管理者基準」、「ソフトウェア供給者基準」、「ネットワーク事業者基準」、「システムサービス事業者基準」の全104項目について詳細に解説したものです。



【目次】

1. コンピュータウイルス対策基準
2. コンピュータウイルス対策基準の解説
　解説についての留意点
　⑴システムユーザ基準
　⑵システム管理者基準
　⑶ソフトウェア供給者基準
　⑷ネットワーク事業者基準
　⑸システムサービス事業者基準
3. コンピュータウイルスの概要

＜参考＞
・通商産業大臣が指定した者（届出先）

【価格】

一般 2,625円／会員 2,100円（税込み・送料別）

B5判、カバー付、206ページ

【申し込み先】　財団法人 日本情報処理開発協会　調査部 普及振興課　FAX：03-3432-9389　E-mail：fukyu@jipdec.or.jp

※会員とは、当協会の賛助会員をいいます。
※全国の政府刊行物サービスセンターおよび政府刊行物サービスステーションでもお求めいただけます。

当協会への連絡窓口

本　部

東京都港区芝公園3-5-8（〒105）
機械振興会館内

総務部	TEL (03)3432-9371
企画室	TEL (03)3432-9372
情報セキュリティ対策室	TEL (03)3432-9387
調査部	TEL (03)3432-9381
開発部	TEL (03)3432-9391
技術企画部	TEL (03)3432-9390
総務関係	FAX (03)3432-9379
調査関係	FAX (03)3432-9389
開発関係	FAX (03)3431-4324

（コンピュータ緊急対応センター事務局）
TEL (03)5575-7762
FAX (03)5575-7764

付属機関

中央情報教育研究所
東京都江東区青海2-45（〒135-73）
タイム24ビル19階　TEL (03)5531-0171（代表）
FAX (03)5531-0170

情報処理技術者試験センター
東京都港区虎ノ門1-16-4（〒105）
アーバン虎ノ門ビル8階　TEL (03)3591-0421（代表）
FAX (03)3591-0428

産業情報化推進センター
東京都港区芝公園3-5-8（〒105）
機械振興会館内　TEL (03)3432-9386（代表）
FAX (03)3432-9389

（電子商取引実証推進協議会事務局）
東京都江東区青海2-45（〒135-73）
タイム24ビル10階　TEL (03)5531-0061（代表）
FAX (03)5531-0068

STEP推進センター
東京都江東区青海2-45（〒135-73）
タイム24ビル10階　TEL (03)5500-0521（代表）
FAX (03)5500-0520

先端情報技術研究所
東京都港区芝2-3-3（〒105）
芝東京海上ビルディング2階　TEL (03)3456-2511（代表）
FAX (03)3456-3158

平成9年12月　発行

JIPDECジャーナル　No.95

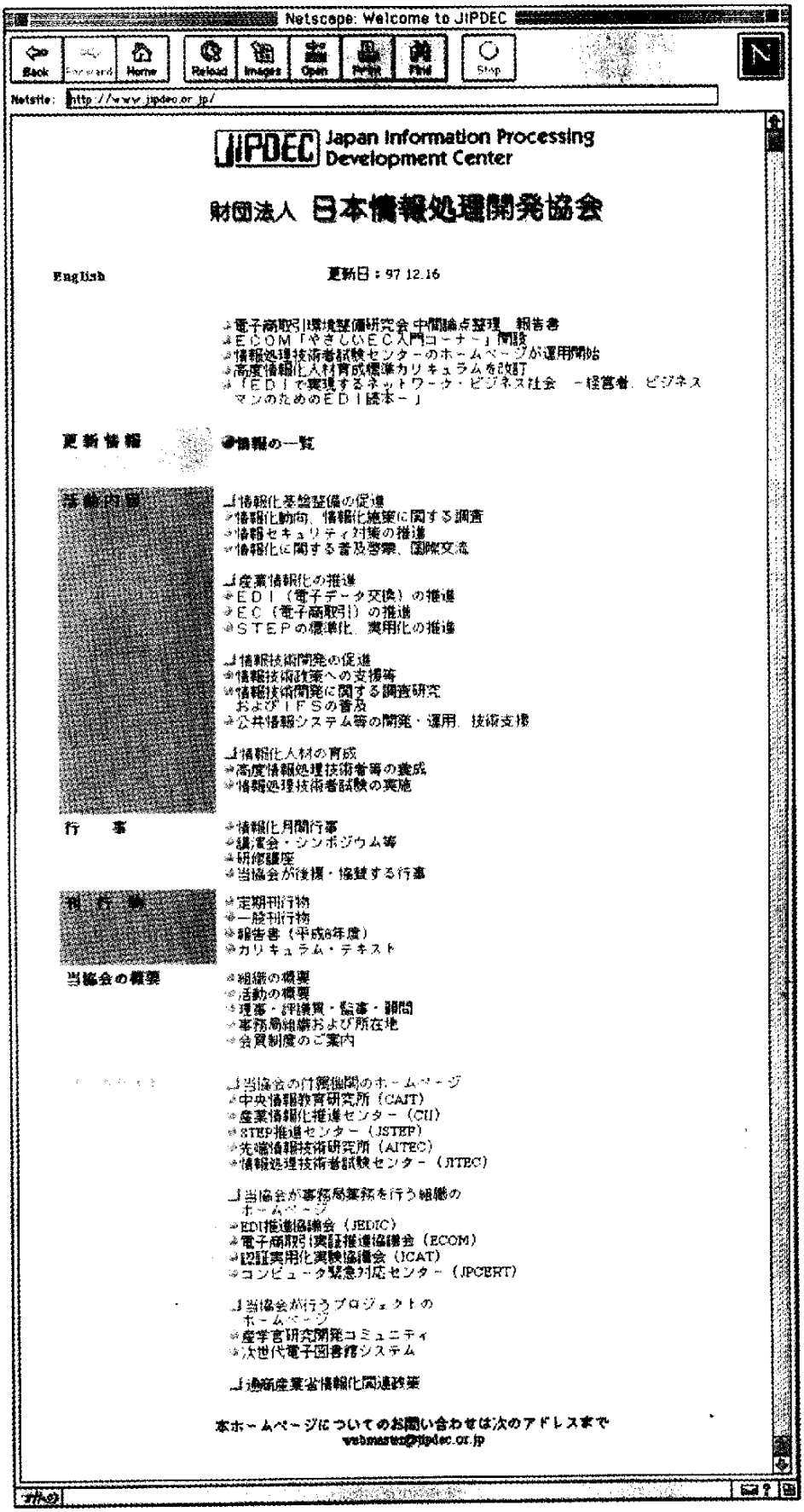
発行人・照山正夫／編集人・日高良治

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
郵便番号105　電話 03（3432）9382
URL：http://www.jipdec.or.jp/

※本誌送付付宛先の変更等については当協会調査部（03-3432-9382）までご連絡ください。

JIPDECホームページ

URL：http://www.jipdec.or.jp/



Netscape: Welcome to JIPDEC

Back Forward Home Reload Images Open Print Find Stop

Netsite: http://www.jipdec.or.jp/

JIPDEC Japan Information Processing Development Center

財団法人 日本情報処理開発協会

English

更新日：97.12.16

- 電子商取引環境整備研究会 中間論点整理　報告書
- ＥＣＯＭ「やさしいＥＣ入門コーナー」開設
- 情報処理技術者試験センターのホームページが運用開始
- 高度情報化人材育成標準カリキュラムを改訂
- 「ＥＤＩで実現するネットワーク・ビジネス社会　－経営者、ビジネスマンのためのＥＤＩ読本－」

更新情報　●情報の一覧

活動内容

- 情報化基盤整備の促進
  - 情報化動向、情報化施策に関する調査
  - 情報セキュリティ対策の推進
  - 情報化に関する普及啓発、国際交流
- 産業情報化の推進
  - ＥＤＩ（電子データ交換）の推進
  - ＥＣ（電子商取引）の推進
  - ＳＴＥＰの標準化、実用化の推進
- 情報技術開発の促進
  - 情報技術政策への支援等
  - 情報技術開発に関する調査研究およびＩＦＳの普及
  - 公共情報システム等の開発・運用、技術支援
- 情報化人材の育成
  - 高度情報処理技術者等の養成
  - 情報処理技術者試験の実施

行　事

- 情報化月間行事
- 講演会・シンポジウム等
- 研修講座
- 当協会が後援・協賛する行事

刊行物

- 定期刊行物
- 一般刊行物
- 報告書（平成8年度）
- カリキュラム・テキスト

当協会の概要

- 組織の概要
- 活動の概要
- 理事・評議員・監事・顧問
- 事務局組織および所在地
- 会員制度のご案内

リンク集

- 当協会の付属機関のホームページ
  - 中央情報教育研究所（CAIT）
  - 産業情報化推進センター（CII）
  - STEP推進センター（JSTEP）
  - 先端情報技術研究所（AITEC）
  - 情報処理技術者試験センター（JITEC）
- 当協会が事務局業務を行う組織のホームページ
  - EDI推進協議会（JEDIC）
  - 電子商取引実証推進協議会（ECOM）
  - 認証実用化実験協議会（JCAT）
  - コンピュータ緊急対応センター（JPCERT）
- 当協会が行うプロジェクトのホームページ
  - 産学官研究開発コミュニティ
  - 次世代電子図書館システム
- 通商産業省情報化関連政策

本ホームページについてのお問い合わせは次のアドレスまで

webmaster@jipdec.or.jp

JIPDEC

財団法人　日本情報処理開発協会
Japan Information Processing Development Center
（本部）東京都港区芝公園3丁目5番8号　機械振興会館内（〒1050011）
電話　03-3432-9381　FAX　03-3432-9389
ホームページ　http://www.jipdec.or.jp/