

金融機関のコンピュータ・ネットワーク
システムにおける安全対策

黒川恒雄

日本銀行電算情報局

最近の海外およびわが国におけるコンピュータ・ネットワークの安全対策研究のなかから、①国際決済銀行（BIS、スイス、バーゼル在）が資金決済システムの安全対策問題についてその研究成果をとりまとめた冊子「電子決済システムの安全対策と信頼性確保」、通称“BISのYellow Book”と②わが国の（財）金融情報システムセンターがとりまとめた「金融機関等コンピュータシステムの安全対策基準」、および③国際情報処理連合（IFIP）の第11技術委員会（安全対策）における最近の研究活動についてそれぞれの概要を紹介する。

Security of Computer and Communications

Systems in Financial Institutions

Tsuneo KUROKAWA

Computer and Data Processing Dept. The Bank of Japan (〒103)

This paper introduces "the Security and Reliability in Electronic Systems for Payments" published by the Bank for International Settlements (Switzerland), "Standards on Security of Computer Systems of Financial Institutions" prepared by the Financial Information Center (Japan) and the studying activities on security in the technical committee of International Federation for Information Processing, with the latest information for making recommendations, rules and laws concerning the security and reliability of computer & communications systems by related parties such as the government and banks both foreign and domestic.

1. コンピュータ・セキュリティ を巡る米国および国際金融機関 (B I S)の研究

(1) 米国

コンピュータ犯罪の増加に対して米国では、これを防止するため特別法を立法化する方向にある。連邦議会で連邦法が検討されている一方(例えば1977年のリビコフ法案の提案)、州議会では州法(例えば1978年アリゾナ、フロリダ両州)が次々と成立している。

また、関係官庁等では連邦標準局(NBS)がセキュリティ・ガイドラインを公表、国防省(DOD)がCSC(Computer Security Center)を設置したり、司法省(DOJ)が「コンピュータ・セキュリティ・テクニツク」や「EFTシステムと犯罪」などの出版物を刊行している。

金融機関関係では1968年に制定された銀行保護法に基づき、連邦通貨監督官、連邦準備制度理事会、預金保険公社等の金融監督機関がそれぞれ「安全基準」を作成。ここでは、管理者の責任、コンピュータ関連施設等の設計方法、運営方法、安全教育につき詳細にガイドラインを規定している。

連邦準備制度(FED)はFEDWIREと呼ばれる広域通信網を形成し、各種データ通信を行つているが、通信ネットワークシステムのセキュリティに関して米国国防省も利用しているセキュリティ関係コンサルタント、MITRE社に検討を依頼、「セキュリティ・アーキテクチャ」の検討を進めている。これはセキュリティ対策を講すべき金融業務の処理、機能に対し、リスクあるいは脅威事項を対応づけ、各リスクに対するシステムの脆弱性を考慮して各処理、機能ごとの安全対策を確立しようとするものである。

* B I S : Bank for International Settlements

また、連邦預金保険公社(FDIC)でもEFT関連の種々な出版物を刊行し加入金融機関のセキュリティ対策を勧奨している。このうち、1977年に発行した「EDPおよびEFTのセキュリティ・ガイド」においては、20の職務別に事故・犯罪防止のための管理項目等についてガイドラインを提示している。

なお、米国で注目すべきことは、民間金融機関が専門的なセキュリティ対応プロジェクトの開発に取り組んでいることで、なかでもシティバンク、チエースマンハッタン、セキュリティ・パシフィック・ナショナル等の銀行が積極的である。

(2) 国際決済銀行(BIS、スイス、バーゼル在)

先進中央銀行の意見交換の場でもある国際決済銀行では、かねてよりコンピュータ・ネットワークを利用した資金決済システムの安全対策問題に多大の关心を示し、加盟主要国の実情、問題点などについて具に調査、検討を重ねてきた。

その研究結果は「電子決済システムの安全対策と信頼性確保」(原題: Security and Reliability in Electronic Systems for Payments)、通称 "Yellow Book"と題して1975年に公表され、その後逐次増補、改訂されてきた。

"Yellow Book"は安全対策の詳細なチェック・リスト(リスク対策)357項目を単に掲載するにとどまらず、そのチェック・リストの総合評価手法である「安全対策のプロファイルによる評価」や「リスク分析のためのマトリックス手法の採用」などの工夫をこらして他の安全対策基準関係の類書にはない特色を持つている。

① 安全対策と信頼性確保に関する

チェック・リスト

高度に安全で信頼性のあるコンピュータ・ネットワークを利用する資金決済システムの構築には、自然災害、機器の障害、不正行為などによるシステム障害の発生を未然に防止すると共に発生時の影響を最小化し、早期回復に心要とされる安全対策基準項目を整備しておく必要がある。

"Yellow Book" では、①設備などに対する物理的安全対策、②システム構成装置のハードウエア、ソフトウエア面での技術対策、③システムの開発、運用管理体制面での対策に分けて 357 項目にのぼるチェック・リストを掲載している。

① 設備などに対する物理的安全対策

……主として同書第 2 章「物理的安全対策」に掲載の 107 項目……

物理的安全対策は対策実施対象を、立地環境、建物、部屋、設備ごとに取りまとめたものである。

コンピュータ・センタの建物、関連設備（電源、空調、回線、データ保管など）について、洪水、悪天候、電磁界の有無などの各種自然災害や侵入、破壊などの不法行為、機器故障などから守るために予防、応急対策を具体的に示している。また、C D、A T M などが設置された自動機器室を運営する上で室や設備に要求される必要な対策も列挙されている。

② システム構成装置のハードウエア、ソフトウエア面での技術対策

……主として同書第 3 章「安全対策と信頼性確保のための設計上の要件」に掲載の 121 項目……

技術対策にはシステムの信頼性向上対策と安全性侵害対策がある。

システムの信頼性向上対策は、コン

ピュータ・ネットワーク・システムの障害発生を極力減少させ、万一障害が発生してもその影響を最小限に食い止め、速やかに回復させるものであり、ハードウエア、ソフトウエアおよび運用時の信頼性向上対策がある。

ハードウエアの信頼性向上対策とは予防保守〔例えば、機器の各部品の MTBF(平均故障間隔)およびMTTR(平均修復時間)の把握〕やハードウエアの予備〔デュプレックス・システムやマルチプロセッサ・システムおよびロードシェア・システム〕などである。

また、ソフトウエアの信頼性向上対策とは、開発時の品質確保〔例えば、信頼度の高い設計に配慮したエラー局所化ルーチン、標準化設計技法の採用〕やメンテナンス時の正確性確保などである。

運用時の信頼性向上対策には、オペレーションの自動化・簡略化・チェック機能〔例えば、テープハンドリングの極少化、データ入力作業の自動化、入力のチェック、および各種合計の突合機能〕、負荷状態監視制御機能などがある。

障害の早期発見・早期回復対策には、障害の検出・切り分け機能〔運転状況（稼動・停止・エラー）の監視機能やエラー発生時の状態に関する詳細情報のロギング機能、切り分けるための折り返しテスト機能〕や局所化、リカバリー機能〔縮小・再構成機能や取引制限機能、各種リカバリー用ジャーナル機能〕などである。

安全性侵害対策には、データの保護対策および不正使用防止対策がある。

データ保護対策とは漏洩防止〔暗証番号やパスワードなどの非表示、非印字、重ね打ちなどの対策〕や破壊・改ざん防止〔ファイルに対する排他制御、アクセス制御機能や不良データ検出機能〕や検知策〔故意または過失によるファイル間の不整合を早期に発見する

ためのファイル統合機能]などである。

また、不正使用防止対策は、本人確認機能〔カード、役席キー、PIN(個人暗証番号)、パスワードなどの使用〕や端末確認機能〔業務内容の必要性に応じ、端末ID、電話番号、コールバックによる確認〕またはその組合せにより、アクセス権限の確認をすること。

アクセス権限確認が十分でない場合または不正アクセスの危険性が高いと認められる場合には、利用範囲を制限する対策〔端末権限規制、取引規制、取引禁止などの機能〕を講ずるとともに、検知策として不正アクセスや異例取引の監視機能〔暗証番号の入力エラー監視、何回かのアクセスの失敗に対し強制終了、取引禁止等を行う機能〕を設けること、などである。

⑩ システムの開発、運用管理体制面での対策……主として同書第4章「事務準則」、第5章「管理上の配慮事項」に掲載の129項目……

ここではコンピュータ・ネットワークを使用した資金決済システムに係わる組織、責任体制、承認手順等を中心に取りまとめている。

すなわち、コンピュータ・センターの業務組織の整備、規程の整備、入退管理、システムの関連機器などの運用管理やシステム開発・変更に係わる承認・確認手順また各種設備管理、運用全体に係わる教育・訓練、要員管理、さらにシステム監査、検査体制についても言及している。

管理体制は、運用管理に係わる基本であり、管理には①入退館(室)管理〔資格付与、鍵、磁気カード、識別コードなどの管理〕、②コンピュータ・システム関連機器、設備などの運用管理と監視〔通常時および障害時マニュアルの整備、アクセス権限の管理、オペレーション管理、データ・ファイル管

理、プログラム管理、ドキュメント管理、帳票管理など〕のほか、前述の「設備などに対する物理的安全対策」や「システム構成装置のハードウエア、ソフトウェア面での技術対策」を踏まえて、安全体策に係わる運用を的確に行うため、③教育・訓練〔オペレーション習熟のための訓練、障害時・災害時に備えた運用訓練や防災・防犯訓練〕および要員管理〔人事および健康管理〕が必要である。

また、いかように事故防止装置が完備され、しかも事故発生時の処理方法が詳細に規定していても、これらが作動しなければ無意味である。安全対策の実施状況を客観的に評価分析し、実効性を上げるために、十分作動するよう定期的に検査、監査制度によつてチェックすることが必要である。

さらに新しいシステム構築に際しては、その計画段階から安全性や管理办法に十分注意する必要があり、したがつて検査、監査制度が計画の初期段階から関与する方がよいと提言している。

また、経営陣はコンピュータ・ネットワーク・システムを使用する資金決済システムに関しリスクの本質を熟知すると同時に、安全対策が一旦破壊された時の影響は一国の銀行制度の信用喪失にいたるほど重大なことからリスク対策についても十分理解していなければならないと勧告している。

② 安全対策のオーバビューやプロファイルによる評価

オーバービュー(Overview)やプロファイル(Profile)とは管理者が前述357項目にのぼるチェック・リストに対する解答を何らかの形で集計し、安全対策の望ましい水準に到達していない分野を見分け、かつシステムを総合的に評価するための手段として考案されたものである。

コンピュータ・ネットワークを使用する資金決済システムから得られる便益は、そのシステムで利用（あるいは所有、リース、契約）される諸々の資源を、安全対策の三つのキー・ワードすなわち、

① アクセス (Access)

② 信頼性の確保と緊急時対策
(Reliability & Contingency Plan)

③ 管理責任の分担 (Accountability)
で評価して判断される。

これを具体的に言えば、①資源が許可されてないアクセスから守られているか、②望ましいレベルの信頼性が保証されているか、そして緊急時においてもこの資源が正常な状態と同じ機能を発揮できるか、③資源に対する管理責任は明定され、しかるべき割当てられているか、という三つのキー・ワードによる評価は「致命的欠陥あり」(Critical Deficient)、問題あり (Questionable)、許容できる (Acceptable)、良好 (Good) および大変堅固 (Very Strong) の五つに区分される。

ここでいう資源とは、施設、ユーティリティおよび公共サービス、ソフトウェア、計画と手順、データ、人員、契約、協約等である。

経営者がシステムの安全対策と信頼性確保に関するオーバービューを理解する一助として典型的な電子決済システムの資源のうち特に重要なものは次のとおりである。

①施設（中央、バックアップ、再配置の場所）……不動産および建物、コンピュータ、ターミナル、通信ネットワーク、ビルディング設備（暖房、通風装置と空調、電気、機械、水道工事、警報器、防護装置、消火器）オフィス

と他の設備（オフィス、家具、エレベーター、階段と廊下、その他の設備休憩場所等）と金庫室。

②ユーティリティとその他の公共サービス……電気、電話、燃料、水、オフィスの提供するもの、その他外部からのサービス（警察、消防、医者）等。

③ソフトウェア……オペレーティング・システム（アプリケーション、機能管理、送信サブシステム）、ソフトウェアの開発とメンテナンス、ドキュメンテーション等。

④計画と手順……オペレーションの手順と安全対策および制御手順。緊急時対策、再スタートないしフォールバックの手順、用地計画。

⑤データ……メッセージ／伝送（付替）と要求／応答。レコード、ファイル、ディスク、テープ、ドキュメント。

⑥人員……スタッフ（オペレーター、サポート、管理者）、メーカーとその他の訪問者。

⑦契約・協約等……顧客、銀行と他の金融機関、他の決済システムメーカーと提供者、ユーティリティ、コンサルタント、保険会社との間の契約等システムの安全性および信頼性を確保するうえでシステムの所有者なり管理者が危険の度合いをどのように判断するかが1つのポイントである。他の事情が等しければ、危険の度合は投下する資本と支払う費用に逆比例する。

経営者は危険の確率を評価し、その他の要因も考慮して危険とコストのバランスをどのようにとるかを決定する。

安全対策と信頼性の確保が必要とされる度合いはシステムにより異なるがシステムとその利用者の長期的な利益を守るには実施可能な最も高いレベルの安全対策と信頼性を確保することが必要となる。

いま、同じようにコンピュータ・ネットワークを利用する二つのシステム

すなわちメッセージ交換システムと資金決済システムを例にとると、資金決済システムは単なるメッセージ交換に止まらず、支払という行為とそれに関連するサービス（価値の移転、清算）を行い、勘定と責任関係が含まれ、その性質上、全関係者の利益を保護するため単純な指示メッセージ交換システムより一層レベルの高い安全対策と信頼性の確保が必要とされる。

資源グループごとに集計された評価（プロファイル）は次表に例示された望ましい水準に達しなければならないし、また達成のため改善を必要とする分野を認識し、適切な改善処置をとることとなる。

(表) メッセージ交換および資金決済システムにおける資源別必要安全対策と信頼性確保のレベルのオーバビュー

安全対策と三つのキーワード ① Access, ② Reliability & Contingency Plan, ③ Accountability

3つのキーワードによる 資源評価		欠陥あり	問題あり	許容出来ぬ	良好	大変堅固
設 備				↓		
ユーティリティ等				↓		
ソフ トウエア				↓		
計 画 と 手 順				↓		
デ ー タ				↓		
職 員				↓		
契 約 ・ 協 約 な ど				↓		

↑
(メッセージ交換)
(資金決済)

③ リスク分析のためのマトリックス手法

マトリックス手法はコンピュータ・ネットワーク・システムに固有なリスクの水準をかなり正確に評価する手段として " Yeowl Book " (C 1985 年 1 月追録された。

アメリカの中央銀行である連邦準備制度は FEDWIRE と呼ばれる広域のコンピュータ・ネットワーク決済システム

を運用しているが、そのセキュリティ対策としてこのマトリックス手法を「セキュリティ・アーキテクチャ」と名付け、コンピュータ・ネットワーク・システムのリスク（脆弱性）を綿密に調査し、これをリストアップして、それについて対策を立てるのに使用している。

「セキュリティ・アーキテクチャ」（マトリックス手法）の構築方法は概略次の通りである。

① システムの主要処理・通信機能の確定

先ず、セキュリティ対策を講ずべきシステムの主要な機能（ Functions ）を確定する。例えば、資金付替および決済業務（ Automated Clearing House ）、金融統計報告、経理や内部管理情報交換などの機能である。

② 機能とリスクのマトリックス

各機能に対するリスク（ Threats ）をマトリックス形式で表わす。リスクには、内部あるいは外部の者が許可を得ないで情報を見ること、データの修正を行うこと、不注意によるデータ変更、メッセージあるいは取引が伝送されないこと、短・長期にわたる業務拒否などが挙げられ、各機能はリスクごとに、高度（ High Concern ）、中度（ Medium Concern ）、低度（ Low Concern ）のランクが付けられる。

③ リスクに対するシステムの脆弱性のマトリックス

各リスクに対応するシステムの脆弱性（ Vulnerabilities ）をマトリックスに表わす。システムの脆弱性は、通信面（ 盗聴によるメッセージの挿入、改ざんなど）、ソフトウェア面（ 設計・開発・更新時点における不正、メーカー提供管理システムの不良など）、要員/手続き面（ データの不正入力、不正

オペレーションなど)、機器(ハードウェアの障害、設備不良など)ごとにリストアップし、各リスクに対応する評点を計算する。

⑩ システムの脆弱性に対する安全対策のマトリックス

安全対策は個々のリスクに対応する防御手段である。安全対策は極めて数多く、技術的安全対策、物理的安全対策、手続き、経営方針など色々と異なるカテゴリに分類される。

上記3つの基本的なマトリックス、すなわち(1)機能とリスク、(2)リスクとシステム脆弱性、(3)システムの脆弱性と安全対策マトリックスから始まり、これらのマトリックスを掛け合わせることにより、その論理積(帰結)として最も重要な(4)機能と安全対策のマトリックスが導き出される。

マトリックス手法を有効に利用するためには次の2点に配慮すべきであるといわれている。

第一はマトリックスのセル(cell)の評価を決定する際に、注意深く判断しなければならないということである。

評価とは(1)“機能とリスク”および、(4)“機能と安全対策のマトリックス”では高、中、低の程度であり、(2)リスクと脆弱性、および(3)脆弱性と安全対策のマトリックスでは、その関係の有無である。これは構成要素の数が増えるために一段と難解となり、その間の齊合性も問題になるためである。

第二は上記の理由およびマトリックス個有の複雑さのため、パソコンなどを使用し、手法を自動化する必要がある。

アメリカ連銀でのパソコン利用の経験では、マトリックスが複雑であるため、マトリックスのセルに関連して取らねばならぬ判断は通常数千個に達するようである。

この手法のもう一つの特徴は、個々のマトリックスが、それぞれ個別の評価を行うため極めて重要であることがある。一つは技術者にとつて重要な“システムの脆弱性—安全対策マトリックス”、もう一つは経営者、利用者にとつて重要な“機能—安全対策マトリックス”である。

このようにマトリックス手法は、システムを評価する上で疑う余地もない有効な手段で、とりわけマイクロコンピュータによる自動処理の柔軟性を考慮して、構築されたものである。

さらに、調査対象のシステムの安全性水準を評価するため、技術者と経営者が別個に調査結果を提出できるユニークなシステムであることを強調しておきたい。

2 我国関係官庁のセキュリティ対策と金融機関の安全対策基準

(1) 関係諸官庁

米国にはまだ遠く及ばないものの、日本でも通産省、郵政省、警察庁などがコンピュータ・ネットワークの安全対策に積極的に取り組む姿勢をみせている。

通産省は情報処理開発協会(略称、JIPDEC)などの報告書や情報化月間の行事を通じてこれまで継続的に安全対策の必要性を強調してきた。1984年7月、コンピュータ・システムの安全性を確保するため「電子計算機システムの安全対策基準」の改訂版を公表した。

新基準は1977年4月に策定したものをコンピュータ・システムの大規模化やネットワーク化に伴つて全面的に改訂したものである。旧基準ではコンピュータ室の物理的な安全対策や運用面の配慮が中心であつたが新基準ではコンピュータをシステムとしてとらえ

ハードウエア障害やソフトウエア・エラーに対して保護すべき対策も追加された。また、コンピュータ犯罪に対処するためにコンピュータ・システムへのアクセス・コントロール基準も盛り込まれている。

郵政省はデータ通信ネットワークの安全性や信頼性対策の指針となる「電気通信システムの安全・信頼性対策の在り方」についての中間報告を85年12月に発表した。この中間報告は郵政大臣の諮問機関である電気通信技術審議会が作成したもので、安全・信頼性対策のガイドライン(案)である。特徴としては「伝送路の複数ルート化対策」、「データの保護対策」、「ネットワークの稼動状況の監視のあり方」「衛星回線の利用など」最新技術を利用したデータ通信ネットワーク環境についての安全対策項目が含まれていることである。

郵政省はこの中間報告を土台にして、通信システムの種別ごとに安全・信頼性対策のあり方を分類・検討し、マニュアルとして利用出来るものを取りまとめたり、また、82年10月に策定した「データ通信ネットワーク安全・信頼性基準」を昭和61年度中に改訂し発表したい考えである。

警察庁は85年初めにコンピュータ犯罪や事故を未然に防止するために「コンピュータシステム安全対策基準」(案)の骨子をとりまとめた。この基準(案)は同庁が将来、「電算システム防護法」(仮称)を制定するためたたき台としてまとめたものである。同庁は「コンピュータ・システム安全対策研究会」にこの基準案を提示して検討してもらい、87年を目標に基準づくりのための最終報告を出す考え方であるが、そのための中間報告を86年1月に「コンピュータ・セキュリティ確保のために」と題して発表した。

この中間報告の特徴は、コンピュータと通信を一体的にとらえ、過去のコンピュータ犯罪や事故事例と安全・防護対策とを対応づけてまとめているため理解しやすい点にある。

(2) (財)金融情報システムセンター

大蔵省の金融機械化懇談会が84年3月報告した「金融機械化システムの安全対策」の提言骨子は、①金融システムの安全対策関連データの収集および管理、②金融システムの安全基準の策定である。

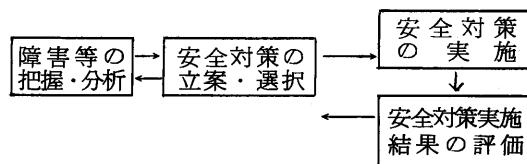
この提言に盛り込まれた安全対策関連データを収集、管理するための機関として84年12月、金融情報システムセンターが設立され、同センターは85年12月に「金融機関等コンピュータシステムの安全対策基準」をとりまとめた。

(安全対策の基本的考え方)

この安全対策基準は次のような考え方で策定されている。

①まず、各種障害等の原因、影響を正しく把握、分析し、②具体的な安全対策の立案・選択を行うには、障害の発生段階に応じて(予防策)、(検知策)、(予備策)、(復旧策)、(監査)の観点からの検討が必要であり、③実施された安全対策内容については、実施結果や技術進展等に応じ、常に見直し、より良い安全対策していくことが必要であり、次図のように、把握・分析、立案・選択、実施、評価の循環の中で改善すべきだとしている。

安全対策の循環図



(基準の内容と構成)

本基準は、自然災害、機器の障害、不正行為等から生ずる金融機関等のコンピュータシステムの障害等の発生を未然に防止すると共に、発生時の影響を最小化し、早期の回復を図るために必要とされる安全対策を金融機関等の業務の実態に合わせて、コンピュータセンターおよび営業店のそれについて226項目にのぼる対策を記述したものである。

本基準は「設備基準」、「技術基準」「運用基準」から構成されている。

①設備基準はコンピュータセンターおよび営業店の建物、設備を自然災害、不正行為等から守るための設備面の対策で、113の小項目から構成されている。

②技術基準はコンピュータシステムにおける信頼性および安全性向上に関するハードウェア、ソフトウェア等技術面の対策で、33の小項目から構成されている。

③運用基準はコンピュータセンターおよび営業店のシステム開発、運用管理体制等について、システムの信頼性および安全性向上を図るために運用面の対策で、80の小項目から構成されている。

設備、技術、運用の各基準は、大項目、中項目、小項目によつて構成されており、大項目または中項目については当該項目の目的、効果等の概要について説明が付されている。

また、小項目で記述された安全対策を適用するに当つての具体的な内容、方法、対象範囲等の考え方を「適用に当たつての考え方」で示し、金融機関等が基本的に取り入れる必要のある基準項目については、「……すること」とし、金融機関等の経営判断により、取り入れることが望ましい基準項目については、「……することが望ましい」と2通りの表現で区分けしている。

また、同センターではこの基準をもとに図解やイラスト入りのマニュアル「金融機関等コンピュータシステムの安全対策基準解説書」を今春作成、セミナーなどのかたちで、金融機関等への周知をはかつている。

3. 国際情報処理連合(IFIP)TC-11 のセキュリティ研究活動

1981年ダブリンで開催されたIFIP総会でセキュリティを研究するTask

Forceが発足した。Task Forceは1983年5月にIFIP、SEC'83をストックホルムで開催、この際に技術委員会(TC-11)および2つの作業部会(後出)の創設を提案した。

1983年9月パリで開催されたIFIP総会でTC-11の創設が認められ、議長にはスエーデンのK. Beckmanを選出した。第1回TC meetingは1984年9月トロントでSEC'84の際に行われた。

1984年9月、Beckman議長の死去によりP. Hoving(スエーデン)が臨時議長に選出された。第2回TC meetingは1985年8月ダブリンでSEC'85の際に行われた。

TC-11の活動目標は次のとおり、①安全対策基準の制定。②セキュリティ関連の実務経験に関する意見交換。③最新のセキュリティ技術情報の普及と評価。④情報処理システムに不可欠なセキュリティ対策の推進。

また、TC-11のもとに現在次の5つの作業部会(WG)が設立されることになつた。

WG1. 安全対策の管理('84設置)

WG2. OAの安全対策('84設置)

WG3. データベースの安全対策

WG4. 暗号の管理

WG5. ADPと監査

なお、IFIPのSEC'83(ストックホルム)およびSEC'84(トロント)で開催された会議に提出、討議された論文をその論題別にグループ分けすれば次のような分野となる。

①セキュリティ管理、

②EDPセキュリティ、

③アクセス制御、

④OAのセキュリティ、

⑤センターの安全対策、⑥リスク分析、

⑦セキュリティ対策の教育、

⑧情報処理システム監査、

⑨暗号、⑩緊急時対策、

⑪コンピュータ犯罪と法律、

⑫OS、⑬データベース、

⑭通信・ネットワーク、

⑮マイクロ・パーソナルコンピュータ、等安全対策

①～⑪はSEC'83分、SEC'84には⑫～⑯の新しい論題が加わつている。

以上