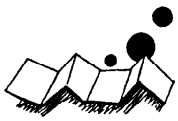
解　説



情報セキュリティ技術の現状と課題†

土　居　範　久††

1. はじめに

コンピュータ・セキュリティ，データ・セキュリティあるいは情報セキュリティといった用語の定義は必ずしも明確でなく，ほぼ同義に用いられているようである．

情報セキュリティとは，地震・火災・水害といった**自然災害**，運用上のミス・エラー，設備・機器の故障・障害，ソフトウェアの故障・障害等の**障害・ミス・エラー**，および破壊活動，犯罪，不正行為等の**意図的行為**といった**脅威**(threat)から，計算機システムを中心とした情報処理活動に係わる資産を守ろうとすることであるということができるだろう[1),2)]．そして，セキュリティ対策は，計算機システムの外側の問題すなわち設備・運用・制度に係わる問題を扱う**外部セキュリティ制御** (external security control) と計算機システムの内部での問題を扱う**内部セキュリティ制御** (internal security control) に分けることができる[3)]．

本稿では，まず，**2.** で外部セキュリティ制御の日本の現状について述べ，**3.** で内部セキュリティ制御のうちのアクセス制御とフロー制御とを上手く扱おうとするセキュリティ核の概念について述べる．

2. 外部セキュリティ制御

外部セキュリティ制御のための主な手段として，物理的対策，管理運用上の対策，リスク管理，システム管理がある．

2.1 物理的対策と管理運用上の対策

物理的対策とは，計算機システムおよび関連設備等の被害を防ぐことを目的とするものであり，管理運用上の対策とは，システムの運用に係わる人および部外者の行動を規制する手続き的な対策である[4)]．これらの対策の基準としては，我が国においては，1977年4月に制定された「電子計算機システム安全対策基準」があり，米国においては，米国商務省標準局が1974年6月に制定した「自動データ処理の物理的セキュリティおよびリスク管理のためのガイドライン」がある[5),6)]．

「電子計算機システム安全対策基準」の概要は**図-1**の通りである．この安全対策基準は，守るべきものをすべて網羅したものであり，

（1） 計算機システムを停止させないための対策
（2） データ等を保護するための対策
（3） (1)と(2)を共に含んでいる対策

に大別することができる[5)]．したがって，基準にもられている対策を一律に適用する必要はなく，システムの性格に応じて対策を立てることになる．基準は A, B, C の三段階に区分されている．Aが最も厳しく，Cが最も緩い．対策ごとに，この段階の区分が指定されているが，どの段階を適用すべきかは，財産・生命・機密，その他の社会・経済活動に与える影響の重要度に応じて，対策内容ごとに判断することになる[5)]．

物理的対策の基本的事項は次の通りである．

（1） 耐　水
（2） 耐　震
（3） 耐火および消火器の設置
（4） 計算機室内の静電気防止
（5） 監 視 対 策

また，計算機システムおよび関連設備の所在を明示しないようにすること，計算機室やデータ保管室は外部の者が容易に接近できない位置に設けたり，不特定多数の人が出入りする場所から隔離したり，1階以下に設置する場合には無窓にしたりすることといった，意図的行為からの安全対策内容がもられている．

管理運用上の対策の基本的事項は次の通りである．

（1） 運用管理者の設置および作業分担の明確化
（2） 入退室管理
（3） 機密データの廃棄手続き
（4） 外部委託に対する規則

† On the State of the Art of the Information Security by Norihisa DOI (Institute of Information Science, Keio University).

†† 慶応義塾大学情報科学研究所

1. 安全をおびやかす要素
2. 基準前提
   2.1 安全対策基準の適用方法及び実施にあたっての留意点
   2.2 安全対策基準に係る法規等
   2.3 用語の定義
3. 設備基準
   3.1 共通事項
      1. 立地及び環境
      2. 設備一般
   3.2 建築物
      1. 建物の位置，周囲，利用形態
      2. 開口部
      3. 屋根及び外壁
      4. 主要構造部
      5. 防火及び防煙区画
      6. 建築設備との隔離
      7. 内装等
      8. 防犯設備
      9. 避雷設備
      10. 火災報知設備
      11. 消火設備
      12. その他の消防設備
      13. 排煙設備
      14. 避難設備
      15. 建築物の排水設備
   3.3 電子計算機室
      1. 位置及び配置
      2. 開口部
      3. 構造
      4. 内装等
      5. 設備
   3.4 電子計算機システム
   3.5 データ等保管室
      1. 位置及び配置
      2. 開口部
      3. 構造
      4. 内装等
      5. 設備
   3.6 電源室，空気調和室等
      1. 位置及び配置
      2. 開口部
      3. 構造
      4. 設備
   3.7 電気設備
      1. 電源設備
      2. 接地
      3. 配線
      4. 防災・防犯用予備電源
      5. その他
   3.8 空気調和設備
      1. 空気調和設備
      2. 空気調和用ダクト
      3. 空気調和用配管
      4. 空気調和設備制御装置
   3.9 監視制御
4. 運用基準
   4.1 組織体制
      1. 防火・防犯管理体制
      2. 運用管理体制
      3. 教育・訓練体制
   4.2 建築物
      1. 入退館管理体制
      2. 社員の入退館管理方法
      3. 他社勤務者の入退館管理方法
      4. 訪問者の入退館管理方法
      5. 巡回管理
   4.3 電子計算機室，電子計算機システム及び同関連設備
      1. 運用管理
      2. 電子計算機室の入退管理
      3. 電子計算機室の巡回警備
      4. 電子計算機室の緊急時の防護体制
      5. 電子計算機室への物品持込み，持出しの管理
      6. 電子計算機室の整理・整頓
      7. 電子計算機及び端末機器の不正使用防止
      8. 電子計算機システム関連設備室の入室管理
      9. 電子計算機システム関連設備の作動管理，巡回管理
      10. 要員管理
      11. 保守管理
      12. バックアップシステムの整備
   4.4 記録媒体及びドキュメント
      1. データ保護管理
      2. プログラムライブラリ管理
      3. 記録媒体及びドキュメント管理
      4. 災害時の緊急対策
      5. 磁気テープの品質管理
   4.5 外部委託
      1. 作業報告及び監査
      2. 外部への作業委託

図-1 「電子計算機システム安全対策基準」の概要

さらに，通産省は，情報処理サービス業における計算機システムに関する安全対策の実施の促進を図り，情報化の健全な発展に資することを目的として，1981年7月に「電子計算機システム安全対策実施事業所認定制度」を発足させている[7),8)]．認定の基準は，計算機システムおよび関連設備に関する事項と事業所の管理および運用に関する事項からなっている．これらの事項はおおよそのところ電子計算機システム安全対策基準の段階Bに相当する．1983年9月現在の認定事業所数は31であるが，本年中には60事業所ぐらいにな

	団体数	計算機を利用している団体数 (A)	データ保護規定制定団体数					委託処理契約書（含覚書）にデータ保護条項を規定している団体数
			条例	規則	訓令その他	計 (B)	B/A (%)	
都道府県	47	47	—	—	42	42	89.4	47
市区町村	3,278	3,050	123	143	359	625	20.5	2,523

図-2　地方公共団体におけるデータ保護対策の状況（1982年4月1日現在）

ることが予想されている．ただし，現在，情報処理サービス業者は約1,300社あるが，そのうちの約70%は入退管理しか行っていないのが現状のようである．そこで，認定基準に合格するためには，多額の資金を必要とするようである．中規模センタで，設備については最低3,500万円，運用に関しては月額400万円かかるという試算がでている[9]．

国の各機関での計算機処理に係わるデータで，特に漏洩・滅失・毀損等を防止する必要があるものについては，その管理を的確にするために，1976年1月29日の事務次官等会議申合せ「電子計算機処理に係るデータの保護について」があり，各地方公共団体には同日付で自治大臣官房長通知が出されている．これは，各機関において管理規定を整備することを求めたものであり，最低限の「電子計算機処理データ保護管理準則」を示したものである．対象となるデータは，個人・法人等に関するデータのうち外部に知られることが適当でないもの，または事故等が発生した場合に復元することが著しく困難である恐れのあるデータである．準則では，管理組織，データの管理，ドキュメントの管理，オペレーションの管理，計算機室および磁気ファイル等の保管施設の管理および保安，委託およびデータの提供についての管理運用等の対策を規定している．目についた準則としては，データ管理体制の第4項に「取扱責任者は，電子計算機処理に係る入力帳票の設計およびデータせん孔の委託に際しては，必要に応じ，その内容のコード化等により，第三者が記載内容を認識することができないように配意するものとする」という項目がある．

また，地方公共団体では何らかのデータ保護対策をとっているところが次第に増えつつあるが，その状況は図-2の通りである[9]．データ保護条例の主な特徴をあげると，およそ次のようになる．

（1）　個人的秘密を守ることを目的とする．

（2）　個人情報は，範囲が規定された事務で，法令に定めのあるものか本人の申告，届出または申請がなされたものより収集する．

（3）　思想，信条，宗教，人種，社会的身分等に関する事項は記録してはならない．

（4）　国や他の地方公共団体等と通信回線を介して計算機システム同士を結合してはならない．

（5）　自己の個人情報については開示・訂正請求ができる．

なお，東京都豊島区のように，特別な事由により区長がやむを得ないと認めた場合を除き，個人情報の計算機による処理は委託してはならないと定めているところもある．

2.2　リスク管理

リスク管理とは，情報処理に係る施設およびその利用者が被る可能性のある損失を見積り，最少の総コストで年間の損失推定額を最少にする一連の救済対策を選定することによって，効果的にセキュリティ対策を行おうとする活動である[6),11),12)]．

分析の対象としては次のものがある[6)]．

（1）　物的資産の破損または盗難

（2）　データおよびプログラム・ファイルの紛失または破損

（3）　情報の盗難

（4）　間接資産の盗難

（5）　計算機処理の遅滞または妨害

また，救済対策としては次のものがある[6)]．

（1）　脅威にさらさないようにするための環境の改善

（2）　脅威の影響を軽減するための対策

（3）　統制手続きの改善

（4）　非常対策

コンピュータを収容する建物		火災保険
コンピュータ・情報機器・周辺設備	リースまたはレンタル	動産総合保険
	買取り	火災保険，コンピュータ総合保険
情報メディア		火災保険，コンピュータ総合保険
情報処理業者		情報処理業者賠償責任保険

図-3　付保の方法

コンピュータ総合保険

a．情報機器条項	情報機器に生じた偶然の事故による直接の損害を補償.
b．情報メディア条項	情報メディアに偶然の事故により直接損害が生じた場合，その再製作費用を補償.
c．臨時費用条項	情報機器または情報メディアに損害が生じた場合，平常通りの業務を続けるために要した臨時費用を補償.
d．利益条項	情報機器または情報メディアに損害が生じ，営業活動が休止または阻害された場合に，休業損を補償.

情報処理業者賠償責任保険

a-1 情報処理業者賠償責任保険	情報処理サービス業者またはソフトウェア業者としての業務に起因して，他人に損害を与えた場合の賠償責任を負うことにより被る損害賠償金，争訟費用を補償.
a-2 システム設計，プログラム作成特約条項	システム設計またはプログラム作成上の過失により，第三者に経済損害を与えた場合の賠償責任を負うことにより被る費用を補償.
b-1 施設賠償責任保険	所有または管理する施設の欠陥または管理上の手落ちとか従業員が業務中に他人の身体や財物に損害を与えた場合の賠償責任を負うことにより被る費用を補償.
b-2 ファシリティ・マネジメント特約条項	ファシリティ・マネジメント業務にともない管理する情報機器・情報メディア・原資料の損壊・紛失・盗取による賠償責任を負うことにより被る費用を補償.

情報処理業者だけを対象

図-4 情報処理に係る保険の概要

定量的に扱う方法の基本は，可能性のある脅威が生じる確率と被る損失との積和を求めて年間の損失推定額を計算することである[1),6),10),11)]．そこで，問題は客観的に見積る方法がないことである．

リスク管理を行う際に考慮すべきものとして各種損害保険がある．情報処理に係る設備・機器，業務に起因する損害等に対する付保方法は**図-3** のようになる[9)]．コンピュータ総合保険および情報処理業者賠償責任保険は，1975年9月に発売されたもので，その概要は**図-4** の通りである[12)]．コンピュータ総合保険については，施されている安全対策に応じて，保険料は割引かれたり割増されたりして調整される．これらの保険で特筆すべき事項を列記すると以下の通りである．

（1） コンピュータ総合保険 b. 情報メディア条項

損害額は，損傷したものと同様・同等のものを再製作するために実際に要した費用であり，再製作されない場合には，白紙のメディア自体の購入価格である．不法侵入者以外による情報のみの損害は免責．

（2） 情報処理業者賠償責任保険

販売分析・販売予測・財務分析のミスによる責任およびシステム設計・プログラム作成上のミスによる責任は免責（ただし，後者は次に示す特約を付けることによって担保できる）．

（3） システム設計・プログラム作成特約条項

システム設計またはプログラムの仕事を完了し顧客に引渡し後6カ月以内に，損害賠償請求があったとき，またはその恐れのある事態が発生したことを知ったときは免責．

2.3 システム監査

セキュリティ制御を評価し，セキュリティ計画を改良・更新するための手段として，システム監査あるいは EDP 監査 (Electronic Data Processing Audit) がある．我が国では“システム監査”という用語が一般に普及しているが，これは日本情報処理開発協会が1974年頃から用いだしたもので，「システム監査とは，監査対象から独立した客観的な立場で，コンピュータを中心とする情報処理システムを総合的に点検評価

監査区分	監査主体	監査内容			法規定
		会計監査	業務監査	経営監査	
外部監査	公認会計士	○	△		証取法193条の2 監査特例法2条
内部監査	監査役	○	○	○	商法274条，275条 281条，282条
	内部監査人	○	○	△	な し

図-5　監査の種類（文献13）による）

し，関係者に助言・勧告することをいい，その有効利用の促進と弊害の除去とを同時に追求し，システムの健全化をはかるものである」と定義し，内部監査として位置づけ，1980年には，システム監査の一般基準と実施基準である「システム監査基準(試案)」を公表している（**図-5** 参照）[13),14)]．米国内部監査人協会（The Institute of Internal Auditors, Inc.）が SRI に依頼して行った Systems Auditability and Control の研究報告書では，EDP 監査は内部監査として位置づけている[16)]．ところで，日本公認会計士協会では，「企業およびその他の組織体において，データ処理の一部または全部が EDP システムによっている場合，これを対象として監査することを EDP 監査という．監査目的を達成するために，コンピュータを利用することもあれば，利用しないこともある」と定義し，外部監査としての立場を示している[13),15),17)]．

システム監査は，システムの信頼性監査と有効性・採算性・効率性監査に大別でき，公認会計士監査はあくまでも財務諸表監査であるので前者に属するが，内部監査では両者を対象とすることになる[13),14)]．セキュリティ監査は，もちろん，前者に含まれる．

システムの信頼性監査の手法としては，静的な手法と動的な手法がある．静的な手法の代表は内部統制質問書を用いるものであり，日本公認会計士協会の「EDP システムの内部統制質問書」がある．動的な手法としては，プログラムを監査するための手法，監査データを収集するための手法，各種データ・ファイルを直接アクセスし信頼性をチェックするための汎用監査ソフトウェアを用いる方法などがある．

通産省は，今秋までに「システム監査基準」を作成すること，および1985年度から情報処理技術者試験に“システム監査士”の試験を追加することを決めたようであるが，システムの開発から参加できるだけの知識を有するシステム監査人を早急に育てる必要があることは確かである．

3. 内部セキュリティ制御

内部セキュリティ制御としては次の四つがある[3),20)]．

（1） アクセス制御 (access control)

システム内の対象への直接のアクセスは，すべて正当と認められたもの，すなわち権限が付与されたものであることを保証する．

（2） フロー制御 (flow control)

正当なアクセス権をもつ主体によって，権限をもたない主体にデータが漏洩することを防ぐ．

（3） 推論制御 (inference control)

公開されている各種統計データを互いに関連させることによって，特定の個人に関する秘密データを推論することを防ぐ．

（4） 暗号化制御 (cryptographic control)

データを暗号化することによって，データが不当に露見したり修正されたりすることを防ぐ．

また，計算機システムに含まれるデータが，その**セキュリティ方策** (security policy) で正当と認められている方法でしか操作することができないとき，その計算機システムは**安全** (secure) であるという．この場合，セキュリティ方策としては，ふつう，アクセス方策 (access policy) とフロー方策 (flow policy) を対象とする．

上記のセキュリティ制御の各論は，本特集号の他の解説で行われるので，本稿では，これ以上ふれず，以下では“安全な”計算機システムを構築する際の基本的なアプローチの一つである**セキュリティ核** (security kernel) について述べる．

3.1 セキュリティ核

セキュリティ核は，アクセス制御およびフロー制御を行うための機構を組み込んだ**参照モニタ** (reference monitor) を実現する小さなシステム核である．参照モニタは，アクセス制御のための抽象モデルである**アクセス行列** (access matrix) の**対象モニタ** (object monitor) のアクセス検査機能を抽象化したもので，**主体** (subject) による**対象** (object) への“いちいちの”アクセス（参照）を検査し，そのアクセスがシステムのセキュリティ方策のもとで正当かどうか決定するものである[19),20),28)]．セキュリティ核は，この参照モニタを実現するハードウェアとソフトウェアの結合体であり，セキュリティ方策を実施する“核”と一群の**信用プロセス** (trusted process) とからなる[19)]．信

用プロセスは，セキュリティを犯さないことが“信用”できるプロセスで，個々のシステムに特有の，基本となるセキュリティ規則に縛られることのないセキュリティ方策を実現するためのものである．

セキュリティ核を実現する際の基本原則は次の通りである[18]．

（1） 完全性 (completeness) 対象へのアクセスはすべて核が仲介しなければならない．

（2） 隔離 (isolation) 核は干渉されることがないよう保護されていなければならない．

（3） 検証可能性 (verifiability) セキュリティ方策と実現との間で一致していることを示さなければならない．

3.2 セキュリティ・モデル

どの実現でも実施されなければならないセキュリティ規則を定義したものを**セキュリティ・モデル** (security model) といい，システム設計のためにも使用者がシステム操作を理解するためにも基本となるものである[18]．形式的に記述したものは，仕様の検証に用いることができる．Mitre Security Kernel[22]，MULTICS[23]，Scomp[24] をはじめとするほとんどのセキュリティ核は，Bell-LaPadula モデルにもとづいている[19]．UCLA の DSU (Data Secure Unix)[29]は資格 (capability) による制御を行い，核の外の方策管理プロセス (Policy manager) に Bell-LaPadula 規則が実現されている．

セキュリティ核で用いないものも含め，形式的なセキュリティ・モデルについては文献 27) に詳しく解説されている．

3.3 Bell-LaPadula モデル

米国国防省で極秘の情報を処理するシステムを認定するために用いる 4 種の処理様式の一つである**多重レベル・セキュリティ** (multilevel security) 方策を支援するためのモデルである[19),27]．このモデルは**セキュリティ・クラス** (security class. **アクセス・クラス** (access class) とか**使用許可** (clearance) ともいう) と呼ぶセキュリティ識別子 (security identifier) を参照モニタの各対象（主体を含む）与えることにより，アクセス制御機構を拡張することでフロー制御を行う．そして，このセキュリティ・クラスを数学的な構造である**束** (lattice) にし，束でフロー制御方策を定義する (D. E. Denning の**束モデル** (lattice model)[20),25] は Bell-LaPadula モデルを拡張したものである)．

Bell-LaPadula モデルでは，対象のセキュリティ・クラスは不変であると仮定し，これは公理によって形式化されている．多重レベル・セキュリティは，次の二つの公理で与えられる[18),27]．

（1） 単純セキュリティ条件 (simple security condition) 主体には，セキュリティ・クラスがそれ以下の対象にしか“読取りアクセス (read access)”権がない．

（2） ＊（スター）-性質 (＊-property) 主体には，セキュリティ・クラスがそれ以上の対象にしか“書込みアクセス (write access)”権がない．

＊-性質は，“トロイの木馬”問題を解決するためのものである[1),18]．また，＊-性質に縛られない信用プロセスを許している．

3.4 システムの検証

セキュリティ核は高水準言語で実現することを前提としているが，セキュリティ方策モデルから実現に至る間には，モデルと形式的な高水準のインタフェース仕様との間，インタフェース仕様と中間段階の仕様との間，詳細な仕様と実現との間の検証を行う必要がある[18]．これらの検証を行うために，これまでのセキュリティ核の開発では，SRI の SPECIAL を用いた HDM (Hierarchical Design Methodology)，Southern California 大学の Information Science Institute の AFFIRM，Texas 大学の Gypsy，SDC の FDM (Formal Development Methodology) 等が用いられているが，これらおよびこれらを用いた検証に関しては文献 26) に詳しく解説されている．D. E. Denning 等は，コンパイル時にフローを検査するための手続きを与えている[3),20]．また，G. R. Andrews 等は，束モデルおよび C. A. R. Hoare 流の公理的方法に基づいて，並行プログラムまで含んだ情報フローの検証方法を与えている[21]．

3.5 問 題 点

セキュリティ核アプローチを採用したシステムは，既にいくつか開発されており，さらに数多くの開発計画が進められている[19]．しかし，既存のオペレーティングシステムを利用しようとする汎用のシステムでは，そのオペレーティングシステムをエミレートするように作られているので，システムの性能は，セキュリティ核を組み込まない場合の 10～25% 程度でしかない．これは，対象に対するいちいちのアクセスに核が介入する必要があるにもかかわらず，それを支援するアーキテクチャをもたないふつうの計算機を用いていることに起因する．性能を上げるためには，相異る

計算を隔離し，隔離した状況間での情報の流れを単純でしかも効率よく制御し，各種の対象を一様に取り扱い，すべてのデータへのアクセスを効率よく仲介できるような機構をもつハードウェアを用いる必要があるが，これらは現在までに開発された機構で実現可能であり，特別，このための新規のアーキテクチャは必要としないで済ませることができるものと思われる[18),19),24)].

次の問題は検証である．Bell-LaPadula モデルでは，最高水準の仕様とモデルとの間の整合性の検証方法は一応確立されたようである．しかし，信用プロセスがセキュリティ方策を満たしているかどうかの検証には，依然として問題がある．Bell-LaPadula 以外のモデルに対しては，信用プロセスまで含めて，Gypsy 等の自動化された検証道具が用いられ成功しているようであるが，検証技術およびそのための道具が完全に確立されていない現状では，むずかしい問題が多い．

4. おわりに

情報セキュリティ技術を外部セキュリティ制御と内部セキュリティ制御に分け，前者については日本の現状について，後者については“安全な”計算機システムを作るためのアプローチとして注目されているセキュリティ核について述べた．

ハードウェアにおける目覚しい技術革新と急激な応用分野の拡大に起因して，ますます複雑なシステムが要求されるようになってきているが，高信頼化対策が追い付かず，計算機システムの様々な脆弱性が指摘されている．健全な情報化社会を築くためには，解決しなければならない問題も多く，それらに対する対策の研究を着実に進めていく必要がある．

参考文献

1) Parker, D. B.: Computer Security Management, Prentice-Hall (1981) [邦訳．日本情報処理開発協会監訳：コンピュータ・セキュリティ，企画センター (1982)].
2) 日本情報処理開発協会：データ通信におけるセキュリティに関する調査報告書 (1983).
3) Denning, D. E. and Denning, P. J.: Data Security, Computing Surveys, Vol. 11, No. 3, pp. 227-249 (1979).
4) 田口孝弘：セキュリティ概論，日本情報処理開発協会情報処理研修センター (1983).
5) 通商産業省：電子計算機システム安全対策基準 (1977).
6) National Bureau of Standards: Guideline for Automatic Data Processing Physical Security and Risk Management, FIPS PUB 31 (1974).
7) 通商産業省：情報サービス業電子計算機システム安全対策実施事業所認定規定 (1981).
8) 日本情報センター協会：情報サービス業電子計算機システム安全対策実施事業所認定制度解説書 (1981).
9) データ通信におけるセキュリティに関する調査委員会資料，日本情報処理開発協会 (1983).
10) Courtney, R.: Security Risk Assessment in Electronic Data Processing System, Proc. of NCC, Vol. 46, pp. 97-104 (1977).
11) 上園忠弘：コンピュータ・セキュリティ，近代科学社 (1981).
12) 岡本行二，田口孝弘：コンピュータ安全管理マニュアル，オーム社 (1980).
13) 宇佐美博：システム監査概要，日本情報処理開発協会情報処理研修センター (1983).
14) 日本情報処理開発協会：システム監査実施への道標 (1980).
15) 松尾 明：公認会計士による EDP 監査とその手法，日本情報処理開発協会情報処理研修センター (1983).
16) The Institute of Internal Auditor, Inc.: System Auditability & Control Executive Report (1977).
17) 日本公認会計士協会電子計算機会計委員会：EDP システム監査基準および監査手続試案 (1976).
18) Ames, S. R., Gasser, M. and Schell, R. R.: Security Kernel Design and Implementation: An Introduction, Computer, Vol. 16, No. 7, pp. 14-22 (1983).
19) Landwehr, C. E.: The Best Available Technologies for Computer Security, Computer, Vol. 16, No. 7, pp. 86-100 (1983).
20) Denning, D. E.: Cryptography and Data Security, Addison Wesley (1982).
21) Andrews, G. R. and Reitman, R. P.: An Axiomatic Approach to Information Flow in Programs, ACM Trans. on Programming Languages and Systems, Vol. 2, No. 1, pp. 56-76 (1980).
22) Millen, J. K.: Security Kernel Validation in Practice, CACM, Vol. 19, No. 5, pp. 243-250 (1976).
23) Schroeder, M. D., Clark, D. D. and Saltzer, J. H.: The MULTICS Kernel Design Project, Proc. 6th SOSP, ACM Operating Systems Review, Vol. 11, No. 5, pp. 43-56 (1977).
24) Fraim, L. J.: Scomp: A Solution to the Multilevel Security Problem, Computer, Vol. 16, No. 7, pp. 26-34 (1983).
25) Denning, D. E.: A Lattice Model for Secure Information Flow, CACM, Vol. 19, No. 5, pp. 236-243 (1976).

26) Cheheyl, M. H., Gasser, H., Huff, G. A. and Millen, J. K. : Verifying Security, Computing Surveys, Vol. 13, No. 3, pp. 279-339 (1981).
27) Landwehr, C. E. : Formal Models for Computer Security, Computing Surveys, Vol. 13, No. 3, pp. 247-278 (1981).
28) Graham, G. S. and Denning, P. J. : Protection-Principles and Practice, Proc. of AFIPS SJCC, Vol. 40, pp. 417-429 (1972).
29) Walker, B. J., Kemmerer, R. A. and Popek, G. J. : Specification and Verification of UCLA Unix Security Kernel, CACM, Vol. 23, No. 2, pp. 118-131 (1980).

(昭和59年3月14日受付)