国防総省標準

国防総省トラステッド・コンピュータ・システム評価基準

＜日本セキュリティ・マネジメント学会　セキュアＯＳ研究会　仮訳＞

はしがき

今回の翻訳作業は、今日のコンピュータセキュリティの礎を築き、ISO/IEC15408 へと発展していった TCSEC（Trusted Computer System Evaluation Criteria）を紐解くことで、我が国のコンピュータセキュリティへの理解を高める一助となることを願い行った。

TCSEC の正式発行は 1985 年になるが、コンピュータセキュリティに関する考え方や、その構造体系には今日でも目を見張るものが存在する。

特に強制アクセス制御や特権制御という制御機能（機構）や、リファレンスモニタコンセプトや隠れチャネル（コバートチャネル）という概念は、今日のコンピュータセキュリティを考えていく上で、極めて重要であると共にややもすれば欠落する箇所ではないかと思われた。

部分的に意訳を行った箇所もあるが、極力原文に忠実に翻訳を行ったつもりである。

平成１７年６月１日
日本セキュリティ・マネジメント学会
セキュア OS 研究会　一同

《フォーマル記述理解のための補足》

DTLS で言う「インフォーマル」は、フォーマル記述のように数学的に定義され決められた形式記述言語を使用しません。TCSEC は、発展して CC となり、その中で formal、semiformal、informal も定義されていますが、一般的傾向として、評価保証レベルが高い領域で、あいまいさを減らし正確さを高めたいときに formal な記述が要求されます。国際相互承認協定(CCRA) の範囲の EAL4 までは、formal 記述が要求されることはありません。

一方、formal 記述だけでは読者が理解できないので、たいていの場合、informal 記述による補足が義務付けられます。特に、仕様の是非を人間が判断するような場合は、informal 記述を用いないと内容を適切に理解できません。CC では、これらを「形式的」、「準形式的」、「非形式的」と訳しています。

≪Sensitive Information の日本語訳≧

用語集の Sensitive Information は、当初「機密情報」と訳しましたが、次のような事例か幾つかあったため「取扱注意情報」に改めました

To provide DoD components with a metric with which to evaluate the degree of trust that can be placed in computer systems for the secure processing of classified and other sensitive information.

本文中の翻訳も「極秘及びその他の機密情報」ではなく「機密及びその他の取扱注意情報」と訳してあります。

原文

DOD 5200.28-STD Supersedes CSC-STD-00l-83, dtd l5 Aug 83 Library No. S225,7ll
DEPARTMENT OF DEFENSE STANDARD
DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA
DECEMBER 1985

ASSISTANT SECURITY OF DEFENSE COMMAND, CONTROL, COMMUNICATIONS AND INTELLIGENCE DoD 5200.28-STD December 26, 1985

監訳＜辻井　重雄＞
翻訳＜日本セキュリティ・マネジメント学会＞

金子 敏信	東京理科大学
富山 茂	元 大阪国際大学
大井 正浩	中央大学研究開発機構
澤田 栄浩	日本高信頼システム
五十嵐　智	日本ユニシス
一瀬 智司	（社）国際都市コミュニケーションセンター
伊藤 昇	電子商取引安全技術研究組合
川口 元	キャノン
済賀　宣昭	東海ソフト
佐藤　祐介	ソニーデジタルネットワークアプリケーションズ
鮫島 吉喜	日立ソフト
鈴木正弘	
高橋 陽一	高橋 IT 研究所
田場 和弘	（社）国際都市コミュニケーションセンター
田吹 隆明	田吹技術士事務所
力 利則	ＮＥＣ
橋本 純生	富士フイルムコンピューターシステム
橋本 真智子	アップルカンパニー
長谷川 誠志	
中根 勝行	那須大学
中本　雅寛	日本ＩＢＭ
松原 克弥	イーゲル
山内 直樹	アイティリサーチ
和田 康	ソルコム
松並　勝	ソニーデジタルネットワークアプリケーションズ

国防総省標準

国防総省トラステッド・コンピュータ・システム評価基準

はしがき

本出版物「米国国防総省指令 5200.28-STD」は，米国国防総省指令 5200.28「自動データ処理（ADP）システムのためのセキュリティ要件」に準拠し，さらには米国国防総省指令 5215.1「コンピュータセキュリティ評価センター」から任命を受けた責務遂行のため発行された。

その目的は，ハードウェア／ファームウェア／ソフトウェアに関する技術的なセキュリティ基準（criteria）および米国国防総省指令 5200.28 によって公表された自動データ処理（ADP）システム全体にわたるセキュリティポリシー，ならびに評価と承認／認可の責務を支援するために関連技術評価手法を提供することにある。

本文書の配備により，国防長官官房（ASD），軍事省（the Military Department），統合参謀本部（the Organization of the Joint Chiefs of Staff），統合特定司令部（Unified and Special Commnads），防衛庁（Defense Agency）および OSD（以後「DoD コンポーネント」と呼ぶ）によって行政上サポートされる諸活動に適用される。

本文書中に示すように，本出版物は，全ての DoD コンポーネントが，DoD の秘密その他取扱注意情報の処理・蓄積およびアプリケーションに適用可能な,自動データ処理（ADP）システムの技術的セキュリティ評価活動の実施にあたり，直接的な効果があると同時に必須のものである。本出版物の改訂勧告は奨励されており，公式のレビュープロセスを経て国立コンピュータセキュリティセンターによって年 2 回レビューが行われる予定である。改訂に関する提案はすべて，適切なチャネルを通じて NCSC（注：コンピュータセキュリティ標準担当チーフ）へ提出すること。

DoD コンポーネントは自身の出版物チャネルを通じて本出版物のコピーを入手可能である。他の連邦政府機関や一般の人々については，NCSC の標準製品局（Office of Standards and Products）Fort Meade，MD 20755-6000（注：コンピュータセキュリティ標準担当チーフ）からコピーの入手が可能である。

謝辞

本文書の中で理論とポリシーおよび実践を統合し，本文書の作成を指揮された NCSC の Sheila l. Brand 氏に特に謝意を表する。

MITRE 社の Grace Hammonds 氏と Peter S. Tasker 氏，NCSC の Daniel J. Edwards 氏，NCSC の前副所長の Roger R. Schell 氏，NCSC の Marvin Schaefer 氏，そして Sperry 社の Theodore M. P. Lee 氏の貢献にも同じく謝意を表する。これらの方々は，オリジナルの設計者として，本文書中に示された技術問題やその解決策についての系統だった明確な説明を行っている。前 CSC の Jeff Markey 氏，NCSC の Warren F. Shadle 氏，そして NCSC の Carole S. Jordan 氏の貢献にも謝意を表する。これらの方々には本文書の準備を手伝って頂いた。James P. Anderson 社の James P. Anderson 氏，Digital Equipment 社の Steven B. Lipner 氏，System Development 社の Clark Weissman 氏，前米国空軍の LTC Lawrence A. Noble 氏，前 DoD の Stephen T. Walker 氏，DoD の Eugene V. Epperly 氏，そして前空軍の James E. Studer 氏に謝意を表する。これら方々は，本文書のレビューと論評に時間と専門知識を惜しみなく提供してくれた。

そして最後に，この取組みを通じて，熱意ある助言と支援を賜ったトラステッド・コンピューティングに関心を持つコンピュータ会社その他の方々に対し，感謝の意を表する。

目　次

序文

本文書に定義された「トラステッド・コンピュータ・システム評価基準」は，システムを拡張セキュリティ保護の一般的な 4 つの階層に区分している。これらの階層は，自動データ処理（ADP）システム製品に組み込まれたセキュリティ制御の有効性評価に使われる基準を提供する。本基準は，以下の 3 つの目標を念頭に開発された。

(a) 極秘文書その他の取扱注意文書をセキュアに処理するために，コンピュータシステムに内蔵可能な信頼度評価尺度をユーザに提供すること。

(b) トラステッド・アプリケーションの信頼要件を満たすために，本基準を広く入手可能とし，信頼性の高い新製品に組み込むことに関して，メーカにガイダンスを提供すること。

(c) 調達仕様におけるセキュリティ要件を満たすための基準を提供すること。

次の 2 つの要件は，セキュア処理のために記述されている。

(a) 特定セキュリティ機能要件

(b) 保証要件

後者のうちのいくつかの要件によって，要求された機能が意図した通り存在し，かつ機能しているかどうか評価者が判断することが可能になる。これらの基準の適用範囲は，トラステッド・システムを構成しているコンポーネントの集まり（セット）に適用されるものであり,必ずしも各システムコンポーネントに個別に適用されるものではない。(従って，いくつかのシステムコンポーネントは，それ以外のコンポーネントがシステム全体としてとらえた高信頼性製品と比較して，低いかあるいはより高い評価クラスに個別に評価されたとしても，完全には高信頼性を確保していない可能性がある)

リファレンスモニターは，ハイエンドクラスの信頼性の高い製品においても，ほとんどのコンポーネントが完全に信頼できないとするほどの強度をもつ。

本基準はアプリケーションに依存しないことを意図しているが，特定セキュリティ機能要件は，独自の機能要件，アプリケーション，または特定の環境（例えば一般の通信プロセッサ，プロセス制御コンピュータ，および組込みシステムなど）をもつ特定のシステムへ本基準を適用するときの要件であると解釈すべきであろう。

基本的な保証要件については，特別な説明なしに自動データ処理（ADP）システムもしくはアプリケーション処理環境の全域にわたって適用可能である。

序説

歴史的観点

1967 年 10 月、Defense Science Board の援助の下で、リモートアクセス、リソースシェアリングコンピュータシステムにおける、極秘情報を保護するコンピュータセキュリティ防衛手段に対応するためのタスクフォースが結成された。そのタスクフォースの報告書「コンピュータシステムのためのセキュリティ管理」が 1970 年 2 月に発行され、リモートアクセスコンピュータシステムで処理される極秘情報を危殆化する脅威を減じるためにとられるべき行動について、多くのポリシー及び技術上の勧告を行った。[34] 国防総省指令 5200.28 及びそれに付属するマニュアル DoD 5200.28-M は、それぞれ 1972 年と 1973 年に発行されたものであるが、DoD コンピュータシステムによって処理される極秘情報を保護するために、均質の DoD ポリシー、セキュリティ要件、管理上の制御、及び技術的手段を確立することによって、これらの勧告の一つに対応した。[8;9] 空軍アドバンストリサーチプロジェクト局及び他の防衛関連機関が 70 年代の初期から中期にかけて担務した研究開発作業は、リソースと情報をシェアするコンピュータシステムにおける情報のフローに関連する技術的問題を解決するアプローチを開発し実証した。[1] コンピュータセキュリティ問題に対応しようとする DoD の狙いにフォーカスするため、防衛研究・工学次官の賛助の下に、1977 年に DoD コンピュータセキュリティイニシアティブが開始された。[33]

コンピュータセキュリティ問題に対応する DoD の狙いと並行して、標準局 (NBS) の指揮の下で、セキュアコンピュータシステムを構築、評価及び監査するための問題と解決法を明らかにするための作業が開始された。[17] この作業の一部として、NBS は、コンピュータセキュリティの監査及び評価を主題とする二つの招待者ワークショップを開催した。[20;28] 最初のものは 1977 年 3 月に、二度目は 1978 年 11 月に行われた。二度目のワークショップの成果の一つは、技術的コンピュータセキュリティの有効性に対する基準の提供に関する問題についての最終ペーパーだった。[20] この報告書による勧告の結果、さらに DoD コンピュータセキュリティイニシアティブの支援によって、MITRE Corporation は、機密データを保護するためにコンピュータシステムにどの程度の信頼を置けるかを評定するのに使用できるコンピュータセキュリティ評価基準についての一連の作業を開始した。[24;25;31] コンピュータセキュリティ評価の暫定的コンセプトが、政府に加えて産業界、学術界から招かれたコンピュータセキュリティの専門技術を代表する参加者による招待者ワークショップ及びシンポジウムにおいて定義され、かつ拡大された。彼らの仕事は、それ以来、仲間うちでの大量のレビューと、DoD、産業界の研究開発組織、大学、及びコンピュータ製造業者からの技術上の建設的な批評を受けてきている。

DoD コンピュータセキュリティイニシアティブによって開始された作業に職員を配置して拡張するため、DoD コンピュータセキュリティセンター (センター) が 1981 年 1 月に

作られた。[15]　センターの主要な目標は、その DoD 憲章によって示されたように、極秘のあるいはそれ以外の機密情報を処理する人々が使用するトラステッド・コンピュータ・システムの、広範囲にわたる可用性の促進である。[10]　本文書において提示される基準は、初期の NBS 及び MITRE の評価関連資料から発展したものである。

範囲

本文書において定義されるトラステッド・コンピュータ・システム評価基準は、主として、商用品として入手できる高信頼の自動データ処理 (ADP) に適用される。これらはまた、以下で強調されるように、既存システムの評価や、自動データ処理（ADP）システム購買のためのセキュリティ要件の仕様に適用できる。ここに含まれているのは、二つの別個の要件のセット： 1) 特定したセキュリティ機能要件; 及び 2) 保証要件である。特定した機能要件とは、その範囲を、汎用 OS (サポートされるアプリケーションプログラムと区別する) を用いる情報処理システムで典型的に見られる特性に限るものとする。しかしながら、特定したセキュリティ機能要件は、そのシステム自身の機能要件、アプリケーション、あるいは特別の環境を持つ特定のシステム (例えば、通信プロセッサ、プロセス制御コンピュータ、及び一般的な組込みシステム) に適用することもできる。一方、保証要件は、専用制御装置からフルレンジのセキュアリソースシェアシステムまで、フルレンジのコンピューティング環境をカバーするシステムに適用される。

目的

序文 (Preface) に概要を記したように、本基準は、多くの意図的な目的を達するために開発された：

* 機密が重要となるアプリケーションに対して、トラステッド要件を満たす (特にデータの暴露を防ぐ点が強調される) 広く利用可能なシステムを提供するために、新規かつ計画中の商用製品にどのようなセキュリティ機能が組み込まれるべきかについての標準を製造業者へ提供すること。
* 機密及びその他の取扱注意情報のセキュアな処理に対してコンピュータシステムに置き得る信頼の度合いを評価する尺度を DoD 当該部門に提供すること。
* 購買仕様におけるセキュリティ要件を仕様化するためのベースを提供すること。

基準の開発に対する二つ目の目的、すなわち DoD 当該部門にセキュリティ評価尺度を提供することに関して、評価は二つのタイプに総括することができる： (a) コンピュータ製品において、アプリケーション環境を除外した観点で評価を実行し得る; あるいは、(b) 特定の環境でのシステムの運用を許すための適切なセキュリティ手段がとられたかどうかを評定するための評価がなされ得る。評価の前者のタイプは、(DoD の) コンピュータセキュリティセンターが「商用製品評価プロセス」を通して行う。そのプロセスは、附録 A に記述される。

評価の後者のタイプ、すなわち、特定の運用業務に関するシステムのセキュリティ属性を評定する目的に対してなされるものは、認証評価と呼ばれる。形式的製品評価は、特定の

アプリケーション環境で使用されるシステムに対する認証あるいは認定に相当するものでないことを理解しなければならない。さらに言えば、その評価報告書は、コンピュータセキュリティの観点から、製品としてのシステムの強さ、弱さを記述した証拠データに基づき、トラステッド・コンピュータ・システムの評価格付けを提供するだけにすぎない。システムのセキュリティ認証及び公式の承認・認定手続きは、それを発行する当局において適用されるポリシーに従ってなされるもので、極秘情報の処理あるいは取り扱いに使用するシステムの使用が承認可能になる前に行われなければならない。[8;9]　各々の指定承認当局 (Designated Approving Authorities (DAAs)) は、自分が認定するシステムのセキュリティの仕様化に対する最終責任を持つ。

トラステッド・コンピュータ・システム評価基準は、認証プロセスにおいて直接的、間接的に使用される。適切なポリシーと一緒に、トータルシステムの評価、新規購買時のシステムセキュリティ及び認証要件仕様化のための技術的ガイダンスとして、直接的に使われる。認証のために評価中のシステムが「商用製品評価」取得済みの製品を用いる場合には、そのプロセスからの報告書が認証評価の入力として用いられる。技術的データは、設計者、評価者、及び指定承認当局が意思決定を行うための必要事項をサポートするために提供される。

基本コンピュータセキュリティ要件

あらゆるコンピュータセキュリティのディスカッションは、必然的に、要件のステートメント、すなわち、コンピュータシステムが「セキュア」と呼ぶものが本当は何を意味しているか、から始まる。一般的に言えば、セキュアなシステムは、特定のセキュリティ機能を使用することで、適切に許可を受けた人間、あるいは彼らを代行して働くプロセスだけが情報を読み出し、書き込み、生成し、削除するためのアクセスを行うように情報へのアクセスを制御する。6 つの基本要件がこの基本的な目的 (objectives) のステートメントから引き出される；情報へのアクセスを制御するためにどのような要求が規定されるべきかの 4 個の施策 (deals) ；これがトラステッド・コンピュータ・システムで達成されることの信用できる保証がどのように得られるかの 2 つの施策である。

ポリシー

要件 1- セキュリティポリシー

システムで実施される明確で適切に定義されたセキュリティポリシーがなければならない。身元が明らかなアクセス主体（subjects ）とアクセス対象（objects）が存在するとき、そのアクセス主体が特定のアクセス対象を呼び出すことを許可できるかどうか判断するためにシステムが使用する一連の規則が必要である。

関係するコンピュータシステムは、取扱注意(例えば機密)情報を取り扱うためのアクセス規則を効果的に実装できる強制セキュリティポリシーを実施しなければならない。

これらの規則は、例えば、適切なセキュリティ証明書を持たない者は、機密情報にアクセスできない、などの要件から構成される。

さらに、選ばれたユーザあるいはグループだけが (例えば、知る必要性に基づき) データにアクセスできることを保証するため、任意（自由裁量)セキュリティ制御も必要である。

要件 2- マーキング

アクセス制御ラベルは、オブジェクトと関連付けられていなければならない。
コンピュータに格納された情報へのアクセスを制御するため、強制セキュリティポリシーの規則に従い次のことができなくてはならない。全てのオブジェクトに、そのオブジェクトの取扱注意レベル(例えば、機密分類) を確実に識別できるラベルを付けるか、さらに／あるいは、本来そのオブジェクトに潜在的にアクセスできる許可されたサブジェクトのアクセスモードを付ける。

説明責任

要件 3- 識別-

個々のサブジェクトは、識別されなければならない。
情報への各アクセスへの取次ぎは、誰がその情報にアクセスしているか、そして取扱が認可されているのは情報のどの部分かという情報に基づかなければならない。
この識別及び許可情報は、コンピュータシステムにより確実・安全に維持されなければならず、システム内でセキュリティに関連する行動を行う全てのアクティブな要素と関連付けられなければならない。

要件 4- 説明責任-

責任のある団体（party）に対するセキュリティに影響を与える行動が追跡（trace）できるよう、監査情報は選択的に保管および保護されていなければならない。
トラステッドシステムでは、監査ログの中に、セキュリティに関わる一連のイベントの生起を記録できなければならない。
記録すべき監査イベントを選ぶ能力は、監査費用を最小にし、効率的な分析を可能とするため必要である。
監査データは、セキュリティ侵害の検出と事後調査を可能にするため、改変及び無許可の廃棄から保護されなければならない。

保証

要件 5- 保証-

コンピュータシステムは、システムが上記の１～４の要件を施行するという充分な保証を提供することを独立的に評価できるハードウェア/ソフトウェアのメカニズムを保有していなければならない。
セキュリティポリシー、マーキング、識別、そして説明責任の４要件をコンピュータシステムによって実施することを保証するために、これらの機能を実行する、いくつかの識別され、統合されたハードウェアとソフトウェアの制御の集合物が必要である。
これらのメカニズムは、一般的にはオペレーティングシステムに埋め込まれ、割り当てら

れた仕事をセキュアな方法で実行するように設計される。
このような運用セツティングにおける、こうしたシステムメカニズムが信頼できるという根拠は、それらの十分性を独立的に審査できるように、明確に文書化されていなければならない。

要件 6- 継続的な保護-
これらの基本的な要件を施行するトラステッドメカニズムは、勝手なおよび／あるいは無許可の変更に対し継続的に保護されなければならない。
セキュリティポリシーを実施する基本のハードウェアとソフトウェアメカニズムが、それ自身無許可の改変や破壊の対象になるとすると、そのようなコンピュータシステムは真に安全だと考えることはできない。
継続的保護の要件は、コンピュータシステムのライフサイクルにわたって直接的な係わりを持っている。

これらの基本的要件は、各評価分野およびクラスに対して適用できる、個々の評価基準の基礎を形成する。
関心のある読者は、汎用の情報処理システムに適用するときは、これら基本的要件のより完全な議論とさらに拡充させたこの文書のセクション 5、「トラステッド・コンピュータ・システムの制御目標」を、またポリシーとこれらの要件間の関係を敷衍するためにセクション 7 を参照のこと。

文書の構成
この文書のこれ以降の部分は、パート 1 と 2、４つの付属書、および用語集に分かれている。
パート 1（セクション 1～4）では、上記の基本的要件に由来するものを、パート 2 に含まれる根拠とポリシーの抜粋に直接関連する基準の詳細を提示している。
パート 1（セクション 5～10）では、基本的な目的、理論的根拠及び基準の背景にある国のポリシーに関する議論、開発者のための指針を提供する。これらは、強制アクセス制御規則の実装、隠れチャネル問題、およびセキュリティテストに関係する。パート 2 は 6 つのセクションに分かれている。
セクション 5 では、一般的なコントロール目的の利用法を議論し、基準に含まれる３つの基本的なコントロール対象を提示する。
セクション 6 では、基準の背景にある理論的な基礎を提示する。
セクション 7 では、コンピュータシステムによる国家レベルの取扱い注意および機密情報の処理に関する多くのトラステッド要件に関する基礎を提供している、関係する規制、指令、OMB(米国行政管理予算局) 通達、大統領行政指令からの抜粋を提示する。
セクション 8 では、隠れチャンネル問題の取扱いにおいて何を期待すべきかについてシステム開発者への指針を提供する。
セクション 9 では、強制セキュリティを扱う指針を提供する。

セクション 10 では、セキュリティテストの指針を提供する。

４つの附録があり、トラステッド・コンピュータシステムの商用製品評価プロセス(附録 A)、評価レベル(附録 B)とクラス(附録 C)の要約、そして最後に、アルファベット順に並べた要件の一覧から構成されている。さらに用語集も追加した。

基準の構成

本基準は D、C、B、および A の４つのレベルに分けられ、最も包括的なセキュリティを提供するシステムのために留保される最高レベル（A)から階層的な方法で順序付けられている。
各レベルは、機密情報の保護に関して、システムに置くことのできる全般的な信頼度が大きく改善されることを示している。
レベル C および B には、クラスとして知られている複数の小区分がある。
クラスもまた、レベル C とレベル B の下位クラスの代表的なシステムにより階層的な方法で順序付けられ、各々に実装されているコンピュータセキュリティ・メカニズムの集合によって特徴づけられている。
システムに対し正確でまた完全に設計され、実装されているという保証は、主として、システムのセキュリティに関連する部分のテストを通じて得られる。
システムのセキュリティ関連部分は、この文書では、トラステッド・コンピューティング・ベース (TCB)という用語で言及している。
レベル B の上位クラスとレベル A の代表的なシステムは、それらのセキュリティ属性の多くはその設計及び実装構造に由来している。
全ての状況下で、必要とされる機能（features）が有効で、正確で、改ざんされないという保証は、設計プロセスにおけるより厳格な分析を増やすほど高められる。

各クラスにおいて、基準の 4 つの大きなセットへの対応がなされる。
最初の３つは、パート 2、セクション 5 で議論されるセキュリティポリシー、説明責任および保証における広範な管理目標を満たすために必要である。
4 つ目のセット、証拠書類では、各クラスで必要とされるユーザガイド、マニュアル、およびテストと設計文書の形式で書かれる証拠書類の種別を述べている。

この文書を初めて使用する読者は、パート 1 から続けて読むのではなく、最初にパート 2 を読むのが有益かもしれない。

パートⅠ：基準

1.0　区分 D：最小保護 ＜Minimal Protection＞

この区分は、クラスが一つだけである。評価はなされたが、上位の評価クラスに対する要件を満たせなかったシステムのために設けられた。

2.0　区分 C：任意（自由裁量的）保護 ＜Discretionary Protection＞

この区分におけるクラスは、任意（自由裁量) ＜知る必要性＞ 保護を規定し、かつ監査機能を含めることによって､サブジェクの責任及び彼らが始動すべきアクションを規定する。

2.1 クラス (C1)：任意（自由裁量的）セキュリティ保護

クラス（Ｃ１）のトラステッド・コンピューティング・ベース（ＴＣＢ）は名目上、ユーザとデータを分離することで任意(自由裁量)のセキュリティ要件を満たしている。それは、個別にアクセス制限を強制することが可能な、信頼できるいくつかの制御形式を組込んでいて、表面上はプロジェクトや個人情報を保護し、かつ、ユーザに対して他のユーザがデータを誤って読出したり、破壊したりすることから守れるようにするのに適している。クラス（Ｃ１）の環境は同一レベルの機密度でデータを処理する共同ユーザの一人となることが期待されている。次の項は､クラス(C1)システムとして評価するための最小基準です。

2.1.1 セキュリティポリシー

2.1.1.1 任意（自由裁量的）アクセス制御

TCB は、自動データ処理（ADP）システムにおける名前付きのユーザと名前付きのオブジェクト(例えば ファイルやプログラム)の間のアクセスを定義し制御しなければならな

い。
強制メカニズム (例えば self/group/public 制御、 アクセス制御リスト) によって、ユーザがオブジェクトの共有を名前付きの個人、または定められたグループ(あるいはその両方)を単位として、指定および制御できなければならない。

2.1.2 責任

2.1.2.1 識別と認証

TCB が調停することになっている動作をユーザが始めるより前に、TCB はユーザがユーザ自身であることを識別するようユーザに要求しなければならない。そのうえ TCB はユーザの真正性を確認するために（パスワード等の）保護機構を使用しなければならない。TCB は正式な許可されていないユーザがアクセスできないように認証データを保護しなければならない。

2.1.3 保証

2.1.3.1 操作上の保証

2.1.3.1.1 システムアーキテクチャ

TCB は、外部からの妨害または改ざん(例えばコードまたはデータ構造の部分修正による)から自らの保護を実行するためにドメインを維持しなければならない。TCB によってコントロールされたリソースは通常、自動データ処理（ADP）システムの中でサブジェクトとオブジェクトで定義されたサブセットとなる。

2.1.3.1.2 システムの完全性

ハードウェアおよび(または)ソフトウェアの機能（features）は、TCB の
実地におけるハードウェアおよびファームウェア要素の正確なオペレーションを定期的に確認するために使用できるように備えられなければならない。

2.1.3.2 ライフサイクル上の保証

2.1.3.2.1 セキュリティ検査

自動データ処理（ADP）システムのセキュリティ機構は、システムドキュメントにより要求されるようにテストされ動作するか調査しなければならない。テストは、未認証のユーザが迂回するか、さもなければ TCB のセキュリティプロテクション機構を破る明らかな方法が全くないことを保証するために行われなければならない。(参照 セキュリティ テスティング ガイドライン)

2.1.4 証拠資料

2.1.4.1 セキュリティに特化したユーザズガイド

ユーザドキュメントの中の単一の要約、章、またはマニュアルは、TCB によって提供されたプロテクション機構、機構利用におけるガイドライン、及び機構がどのように相互に影響するかを記述しなければならない。

2.1.4.2 信頼できる設備マニュアル

自動データ処理（ADP）システム管理者向けのマニュアルは、セキュア設備を使用する時に制御されるべき機能と特権について警告を示さなければならない。

2.1.4.3 検査証拠資料

システム開発者は、テスト計画について記述したドキュメント、セキュリティ・メカニズムがどのようにテストされたかを示すテスト手続き、およびセキュリティ・メカニズムの機能的なテストの結果を、評価者に提供しなければならない。

2.1.4.4 設計文書

メーカの保護体系の記述およびこの体系がどのように TCB に変換されるかが説明された文書が利用可能でなければならない。もし TCB が別個のモジュールから構成されるならば，これらモジュール間のインタフェースも記述されていなければならない。

2.2 クラス（Ｃ２）：制御付きアクセス保護

このクラスに属するシステムは、ログイン手順、セキュリティ関連イベントの監査およびシステム資源の隔離を通して､ユーザにおのおのの行動に対する責任を与えることにより、（Ｃ１）システムよりさらにきめ細かな任意（自由裁量)のアクセス制御を強制する。次の項では、クラス(C1)システムとしての評価の最小基準です。

2.2.1 セキュリティポリシー

2.2.1.1 任意（自由裁量的）アクセス制御

TCB は、自動データ処理（ADP）システムにおける名前付きのユーザと名前付きのオブジェクト(例えば ファイルやプログラム)の間のアクセスを定義し制御しなければならない。強制メカニズム (例えば self/group/public 制御、 アクセス制御リスト) によって、ユーザがオブジェクトの共有を名前付きの個人、または定められたグループ(あるいはその両方)を単位として、指定および制御できなければならない。また、同メカニズムはアクセス権の伝播を制限する制御方法を提供しなければならない。任意（自由裁量)アクセス制御メカニズムは、明示的なユーザの操作によって、あるいはデフォルトで、正式な許可なしのアクセスからオブジェクトを保護しなければならない。こういったアクセス制御は単一ユーザの粒度でアクセスを可能にしたり不可能にしたりする能力を持たなければならない。オブジェクトへのユーザ毎のアクセス許可権限は、まだ付与されていない場合、正式な許可ユーザによってのみ付与されなければならない。

2.2.1.2 オブジェクト再使用

未使用のストレージ・オブジェクトの TCB のプールからサブジェクトへの初期の割り当て、配分、または再配分に先がけて無効にすべきである。システムにリリースバックされているオブジェクトにアクセスできるいかなるサブジェクトも、事前のサブジェクトの動作によって生成される暗号化表現が含まれる情報を利用できてはならない。

2.2.2 責任

2.2.2.1 識別と認証

TCB が調停することになっている動作をユーザが始めるより前に、TCB はユーザがユーザ自身であることを識別するようユーザに要求しなければならない。そのうえ TCB はユーザの真正性を確認するために（パスワード等の）保護機構を使用しなければならない。TCB は正式な許可されていないユーザがアクセスできないように認証データを保護しなければならない。

TCB は自動データ処理（ADP）システムの個別のユーザをユニークに識別する能力を提供することで個人に責任を強制できなければならない。TCB はまたこの個人の識別とその個人がとるすべての監査可能な動作を関連付ける能力を提供しなければならない。

2.2.2.2 監査

TCB は保護対象のオブジェクトへのアクセス監査証跡を生成し、維持し、そして修正あるいは不正アクセスあるいは破壊から保護することができなければならない。監査データは，それへの読取りアクセスが承認された者に限定されるように，TCB によって保護されるべきである。

TCB は次に示すようなタイプの事象を記録できなければならない。:

識別番号の利用と認証メカニズム，ユーザドレス空間へのオブジェクトの導入（例えばファイルオープンやプログラムの開始），オブジェクトの消去，そしてコンピュータオペレータとシステム管理者，システムセキュリティ責任者と他のセキュリティ関連事象のうちの両方か、もしくはそのいずれかによる活動。

それぞれの記録された事象に対して，監査レコードは以下を特定する：事象発生日時，ユーザ，事象タイプ，事象の成功・不成功の区別。

識別／認証の事象に対して，その要求元（例えば端末 ID）は監査レコードに含まれなければならない。オブジェクトをユーザドレス空間へ導入する事象およびオブジェクトを消去する事象に対しては，監査レコードはオブジェクトの名前を含まなければならない。ADP システムの管理者は，個別属性に基づく任意の 1 人かそれ以上のユーザの活動を選択的に監査できなければならない。

2.2.3 保証

2.2.3.1 操作上の保証

2.2.3.1.1 システムアーキテクチャ

TCB は、外部からの妨害または改ざん(例えばコードまたはデータ構造の部分修正による)から自らの保護を実行するためにドメインを維持しなければならない。TCB によってコン

トロールされたリソースは通常、自動データ処理（ADP）システムの中でサブジェクトとオブジェクトで定義されたサブセットとなる。
リソースがアクセス制御と監査要件の対象であることから、TCB は保護のためにリソースを分離しなければならない。

2.2.3.1.2 システムの完全性

ハードウェアおよび(または)ソフトウェアの機能（features）は、TCB の実地におけるハードウェアおよびファームウェア要素の正確なオペレーションを定期的に確認するために使用できるように備えられなければならない。

2.2.3.2 ライフサイクル上の保証

2.2.3.2.1 セキュリティ検査

自動データ処理（ADP）システムのセキュリティ機構は、システムドキュメントにより要求されるようにテストされ動作するか調査しなければならない。テストは、未認証のユーザが迂回するか、さもなければ TCB のセキュリティプロテクション機構を破る明らかな方法が全くないことを保証するために行われなければならない。(参照 セキュリティ テスティング ガイドライン)テストは、また、資源分離の違反を可能にするか、監査または認証データへの不正アクセスを許すかもしれない明らかな弱点に対する調査を含まなければならない。

2.2.4 証拠資料

2.2.4.1 セキュリティに特化したユーザズガイド

ユーザドキュメントの中の単一の要約、章、またはマニュアルは、TCB によって提供されたプロテクション機構、機構利用におけるガイドライン、及び機構がどのように相互に影響するかを記述しなければならない。

2.2.4.2 信頼できる設備マニュアル

自動データ処理（ADP）システム管理者向けのマニュアルは、セキュア設備を使用する時に制御されるべき機能と特権について警告を示さなければならない。
各タイプの監査イベントの詳細な監査記録構造と同じく監査ファイルを検査し、維持するための手続が与えられなければならない。

2.2.4.3 検査証拠資料

システム開発者は、テスト計画について記述したドキュメント、セキュリティ・メカニズムがどのようにテストされたかを示すテスト手続き、およびセキュリティ・メカニズムの機能的なテストの結果を、評価者に提供しなければならない。

2.2.4.4 設計文書

メーカの保護体系の記述およびこの体系がどのように TCB に変換されるかが説明された

文書が利用可能でなければならない。もし TCB が別個のモジュールから構成されるならば，これらモジュール間のインタフェースも記述されていなければならない。

3.0 区分 B：強制(的)保護 ＜Mandatory Protection＞

機密ラベルの完全性を保持し、それを一連の強制アクセス制御規則を実施するために使用する TCB の概念がこの区分における主要要件である。この区分におけるシステムは、システム内で、主要なデータ構造と一緒に機密ラベルを保持しなければならない。システム開発者は、また、TCB が基礎を置くセキュリティポリシー・モデルを提出し、かつ TCB の仕様を提供せねばならない。リファレンスモニター・コンセプトが実装されていることを実証するために証拠を提出しなければならない。

3.1 ラベル付きセキュリティ保護

クラス（Ｂ１）のシステムはクラス（Ｃ２）の特長要件をすべて要求する。それに付加して、セキュリティポリシーモデル、データのラベル付けや名前付きサブジェクトとオブジェクトに関する強制アクセス制御などのインフォーマルな宣言がなければならない。また、正確にラベル付けされたエクスポート情報のための機能が存在しなければならない。さらに、検査によって確認されたいかなる不具合も除去されねばならない。以下は、クラス(B1)とされるシステムの評価するための最小基準です。

- 3.1.1 セキュリティポリシー
  - 3.1.1.1 任意（自由裁量的）アクセス制御
  - 3.1.1.2 オブジェクト再使用
  - 3.1.1.3 ラベル
    - 3.1.1.3.1 ラベルの完全性
    - 3.1.1.3.2 ラベル付けされた情報のエクスポート
      - 3.1.1.3.2.1 マルチレベル装置へのエクスポート
      - 3.1.1.3.2.2. 単一レベル装置へのエクスポート
      - 3.1.1.3.2.3 人間の判読可能な出力のラベル化
  - 3.1.1.4 強制（的）アクセス制御
- 3.1.2 責任
  - 3.1.2.1 識別と認証
  - 3.1.2.2 監査
- 3.1.3 保証
  - 3.1.3.1 操作上の保証
    - 3.1.3.1.1 システムアーキテクチャ
    - 3.1.3.1.2 システムの完全性
  - 3.1.3.2 ライフサイクル上の保証
    - 3.1.3.2.1 セキュリティ検査
    - 3.1.3.2.2 設計仕様と検証

3.1.1 セキュリティポリシー

3.1.1.1 任意（自由裁量的）アクセス制御

TCB は、自動データ処理（ADP）システムにおける名前付きのユーザと名前付きのオブジェクト(例えば ファイルやプログラム)の間のアクセスを定義し制御しなければならない。強制メカニズム (例えば self/group/public 制御、 アクセス制御リスト) によって、ユーザがオブジェクトの共有を名前付きの個人、または定められたグループ(あるいはその両方)を単位として、指定および制御できなければならない。また、同メカニズムはアクセス権の伝播を制限する制御方法を提供しなければならない。
任意（自由裁量)アクセス制御メカニズムは、明示的なユーザの操作によって、あるいはデフォルトで、正式な許可なしのアクセスからオブジェクトを保護しなければならない。こういったアクセス制御は単一ユーザの粒度でアクセスを可能にしたり不可能にしたりする能力を持たなければならない。オブジェクトへのユーザ毎のアクセス許可権限は、まだ付与されていない場合、正式な許可ユーザによってのみ付与されなければならない。

3.1.1.2 オブジェクト再使用

未使用のストレージ・オブジェクトの TCB のプールからサブジェクトへの初期の割り当て、配分、または再配分に先がけて無効にすべきである。システムにリリースバックされているオブジェクトにアクセスできるいかなるサブジェクトも、事前のサブジェクトの動作によって生成される暗号化表現が含まれる情報を利用できてはならない。

3.1.1.3 ラベル

制御下にある各サブジェクトおよび記憶オブジェクト(例えばプロセス、ファイル、セグメント、装置)に関連性のある機密ラベルは、ＴＣＢによって維持されなければならない。これらのラベルは、強制アクセス制御決定の基礎として使用されなければならない。ラベルが付けられていないデータをインポートするために、ＴＣＢは、正式に許可されたユーザにデータのセキュリティ・レベルを要求し、それを受け取らなければならない。また、そのようなアクションはすべてTCBにより監査可能としなければならない。

3.1.1.3.1 ラベルの完全性

機密ラベルは、それらが関連する特定のサブジェクトまたはオブジェクトのセキュリティレベルを正確に表さなければならない。
TCB によってエクスポートされる時に、機密ラベルは内部ラベルを正確にかつ明確に表すこととし、エクスポートされようとしている情報に付随されなければならない。

3.1.1.3.2 ラベル付けされた情報のエクスポート

TCB は、それぞれの通信チャネルおよび I/O 装置を、単一レベル装置またはマルチレベル装置であると指定しなければならない。この指定のいかなる変更も手作業で行われなければならず、また TCB によって監査可能でなければならない。TCB は、通信チャネルや I/O 装置のセキュリティレベルのいかなる変更も保持し、かつ、いかなる変更も監査可能でなければならない。

3.1.1.3.2.1 マルチレベル装置へのエクスポート

TCB がオブジェクトをマルチレベル I/O 装置にエクスポートする際、そのオブジェクトに紐づけられた機密ラベルも一緒にエクスポートされなければならず、エクスポートされた情報と同じ物理媒体に同じ形式（機械データもしくは自然言語等）で記録されなければならない。TCB がオブジェクトをマルチレベル通信チャネルにエクスポート、あるいはインポートする際、そのチャネルで使用されるプロトコルは、送受される情報と、その機密ラベルの組を明確に示さなければならない。

3.1.1.3.2.2. 単一レベル装置へのエクスポート

単一レベル I/O 装置および単一レベル通信チャネルは、処理している情報の機密ラベルを保守する必要がない。しかしながら TCB は、単一レベルの通信チャネルまたは I/O 装置を介してインポートあるいはエクスポートされる情報の単一のセキュリティレベルを確保するために、TCB と許可されたユーザが信頼して通信するメカニズムを含まなければならない。

3.1.1.3.2.3 人間の判読可能な出力のラベル化

ＡＤＰシステム管理者は、エクスポートされる機密ラベルに関連性のある表記可能なラベル名を指定できなければならない。TCBは、人間に可読でページ付けされている全てのハードコピー出力(例えばラインプリンタ出力)の始めと終わりに、その出力の機密度を正確に*表現する人間に可読な機密ラベルをマークしなければならない。

TCB はデフォルトで、人間の判読可能なハードコピー出力(例えばラインプリンタ出力)の各ページの上部と下部に、その出力の全体的な機密度を正確に*表現する、あるいはそのページ上の情報の機密度を正確に*表現する、人間に可読な機密ラベルをマークしなければならない。

TCB はデフォルトで、そして適切な方法により、人間に可読な他の様式の出力（例えば、マップ、グラフィックス）に、その出力の機密度を正確に*表現する、人間に可読な機密ラベルをマークしなければならない。これらのデフォルトのマーキングに対する、いかなる書換えも TCB により監査可能としなければならない。

3.1.1.4 強制(的)アクセス制御

TCB は、自らのコントロールの下にあるあらゆるサブジェクトとストレージ・オブジェク

ト(すなわちプロセス、ファイル、セグメント、デバイス)に対して強制アクセス制御のポリシーを実施しなければならない。これらのサブジェクトとオブジェクトは、階層的な機密度区分レベルと階層的でないカテゴリーとの組み合わせである機密ラベルを割り当てられることとし、そのラベルは強制アクセス制御の決定のための基礎として使われなければならない。TCB は、ふたつ以上のそのようなセキュリティレベルをサポートできることとする。(強制アクセス制御ガイドラインを参照。)以下の要求事項は、TCB によつて制御されるすべてのサブジェクトと、これらのサブジェクトによる直接または間接的にアクセス可能なすべてのオブジェクトとの間のすべてのアクセスにあてはまらなければならない：サブジェクトのセキュリティレベルにおける階層区分が、オブジェクトのセキュリティレベルにおける階層区分より大きいかあるいは等しく、そして、サブジェクトのセキュリティレベルにおける階層的でないカテゴリがオブジェクトのセキュリティレベルの階層的でないカテゴリの全てを含むのであれば､サブジェクトはオブジェクトを読むことができる。サブジェクトのセキュリティレベルにおける階層区分が、オブジェクトのセキュリティレベルにおける階層区分より小さいかあるいは等しく、そして、サブジェクトのセキュリティレベルにおける階層的でないカテゴリの全てがオブジェクトのセキュリティレベルにおける階層的でないカテゴリに含まれるのであれば、サブジェクトはオブジェクトに書くことができる。識別と認証のデータは、ユーザの本人性を認証するために、そしてまた、個々のユーザのために動作するよう作成される TCB 外のサブジェクトのセキュリティレベルと認可がそのユーザのクリアランスと認可によって支配されることを保証するために、TCB により使われなければならない。

3.1.2 責任

3.1.2.1 識別と認証

TCB が調停することになっている動作をユーザが始めるより前に、TCB はユーザがユーザ自身であることを識別するようユーザに要求しなければならない。さらに TCB は個別のユーザの真正性を確認するための情報（パスワードなど）を含む認証データを保持しなければならない。TCB は、個別のユーザのクリアランスと認可を決定するための情報も同様に保持しなければならない。これらのデータはユーザの真正性を認証するために TCB に利用されなければならない。また個別のユーザに代わって動作するために作られる TCB 外にあるサブジェクト（アクセスの主体）のセキュリティレベルと認可がそのユーザのクリアランスと認可によって支配されることを保証するためにも、これらのデータは TCB に利用されなければならない。

――――――――――――――――――――――――――――――

*人間が認識できる機密レベルにある階層クラシフィケイションの要素は､最も高い階層クラシフィケイションの、またはラベルが示す表示の中にある全ての情報と等しくなければなりません。非階層カテゴリの要素はレベルが示す表示の中に非階層カテゴリの全ての情報を含んでいます。

3.1.2.2 監査

TCB は保護対象のオブジェクトへのアクセス監査証跡を生成し、維持し、そして修正あるいは不正アクセスあるいは破壊から保護することができなければならない。監査データは，それへの読取りアクセスが承認された者に限定されるように, TCB によって保護されるべきである。

TCB は次に示すようなタイプの事象を記録できなければならない。:

識別番号の利用と認証メカニズム，ユーザドレス空間へのオブジェクトの導入（例えばファイルオープンやプログラムの開始), オブジェクトの消去, そしてコンピュータオペレータとシステム管理者，システムセキュリティ責任者と他のセキュリティ関連事象のうちの両方か、もしくはそのいずれかによる活動。TCB は人間に可読な出力表示のマーキングのいかなる書換えも監査できなければならない。

それぞれの記録された事象に対して，監査レコードは以下を特定する：事象発生日時，ユーザ，事象タイプ，事象の成功・不成功の区別。

識別／認証の事象に対して，その要求元（例えば端末 ID）は監査レコードに含まれなければならない。オブジェクトをユーザドレス空間へ導入する事象とオブジェクトを消去する事象については，監査レコードはオブジェクト名およびオブジェクトのセキュリティレベルを含まなければならない。ADP システムの管理者は，個別属性に基づく任意の 1 人かそれ以上のユーザの活動と，オブジェクトのセキュリティレベルのうち，両方もしくはいずれか一方を選択的に監査できなければならない。

3.1.3 保証

3.1.3.1 操作上の保証

3.1.3.1.1 システムアーキテクチャ

TCB は、外部からの妨害または改ざん(例えばコードまたはデータ構造の部分修正による)から自らの保護を実行するためにドメインを維持しなければならない。TCB によってコントロールされたリソースは通常、自動データ処理（ADP）システムの中でサブジェクトとオブジェクトで定義されたサブセットとなる。TCB は TCB のコントロール下で別アドレス空間を提供することを通してプロセス分離を維持しなければならない。リソースがアクセス制御と監査要件の対象であることから、TCB は保護のためにリソースを分離しなければならない。

3.1.3.1.2 システムの完全性

ハードウェアおよび(または)ソフトウェアの機能（features）は、TCB の実地におけるハードウェアおよびファームウェア要素の正確なオペレーションを定期的に確認するために使用できるように備えられなければならない。

3.1.3.2 ライフサイクル上の保証

3.1.3.2.1 セキュリティ検査

自動データ処理（ADP）システムのセキュリティ機構は、システムドキュメントにより要

求されるようにテストされ動作するか調査しなければならない。TCB の特徴の実施を完全に理解する個人からなるチームは、そのデザインドキュメント、ソースコード、およびオブジェクトコードの徹底的な分析とテストに従事することになる。
それらのオブジェクトは次のようでなければならない：TCB により求められる強制または任意（自由裁量)のセキュリティポリシーの下で正常に拒否されたデータを読み、変更、削除するために、TCB の外のサブジェクトを許すというすべてのデザインとインプリメンテーションの弱点を摘発すること。；いかなるサブジェクトも、（そのような認可なしで）他のユーザが開始したコミュニケーションに応じられないような状態にして、TCB に入れないようにするのを保証するのと同様である。すべての発見された弱点は削除されるか、無効にされることとし、TCB はそれらが取り除かれていて、新しい弱点が導入されていないことを証明するために、再テストしなければならない。(参照 セキュリティ テスティングガイドライン)

3.1.3.2.2 設計仕様と検証

TCB がサポートするセキュリティポリシーのインフォーマルモデルおよびフォーマルモデルは、自動データ処理（ADP）システムのライフサイクルを通してモデルの公理と一貫性があることを示すように、保守されなければならない。

3.1.4 証拠資料

3.1.4.1 セキュリティに特化したユーザズガイド

ユーザドキュメントの中の単一の要約、章、またはマニュアルは、TCB によって提供されたプロテクション機構、機構利用におけるガイドライン、及び機構がどのように相互に影響するかを記述しなければならない。

3.1.4.2 信頼できる設備マニュアル

自動データ処理（ADP）システム管理者向けのマニュアルは、セキュア設備を使用する時に制御されるべき機能と特権について警告を示さなければならない。
各タイプの監査イベントの詳細な監査記録構造と同じく監査ファイルを検査し、維持するための手続が与えられなければならない。
マニュアルは、利用者のセキュリティ特性を変更することを含めオペレータと管理者のセキュリティ関連機能を説明しなければならない。システムの保護機能の一貫した効率的な利用、その機能がどのように相互に作用するか、安全に新しい TCB をどのように生成するか､そして安全な方法で設備を運営するために制御される必要のある設備の手続や警告、特権に関するガイドラインをマニュアルは提供しなければならない。

3.1.4.3 検査証拠資料

システム開発者は、テスト計画について記述したドキュメント、セキュリティ・メカニズムがどのようにテストされたかを示すテスト手続き、およびセキュリティ・メカニズムの機能的なテストの結果を、評価者に提供しなければならない。

3.1.4.4 設計文書

メーカの保護体系の記述およびこの体系がどのように TCB に変換されるかが説明された文書が利用可能でなければならない。もし TCB が別個のモジュールから構成されるならば，これらモジュール間のインタフェースも記述されていなければならない。
TCB により実行されるセキュリティポリシーモデルに関するインフォーマルあるいはフォーマルな説明が利用可能であって，セキュリティポリシーを実行する上で十分であると言える説明がなされていなければならない。具体的な TCB 保護メカニズムが確認され，それがモデルを満足することを示す説明がなされていなければならない。

3.2 クラス (B2)：構造化保護

クラス（B2)のシステムにおいては、TCB は、明瞭に定義され、文書化されたフォーマル・セキュリティポリシー・モデルに基づき、クラス（B1）のシステムに見られる任意（自由裁量)および強制アクセス制御の強制が自動データ処理（ADP）システム中の全サブジェクトとオブジェクトに拡張されることを要求する。それに加えて、隠れチャネルに言及される。TCB は保護が重要な要素と非保護が重要な要素へと注意深く構造化されなければならない。
この TCB インタフェースは必要十分に定義されていて、TCB の設計と実装が、より完全な検査とレビューを受けることを可能にする。認証メカニズムが強化され、システム管理者やオペレータの機能に対するサポート形式において信頼できる設備管理が提供され、さらに厳重な構成の管理制御が導入される。このシステムは侵入に対して相対的に抵抗力がある。以下は、クラス(B2)システムとして評価するための最小基準です。

- 3.2.1 セキュリティポリシー
  - 3.2.1.1 任意（自由裁量的）アクセス制御
  - 3.2.1.2 オブジェクト再使用
  - 3.2.1.3 ラベル
    - 3.2.1.3.1 ラベルの完全性
    - 3.2.1.3.2 ラベル付けされた情報のエクスポート
      - 3.2.1.3.2.1 マルチレベル装置へのエクスポート
      - 3.2.1.3.2.2. 単一レベル装置へのエクスポート
      - 3.2.1.3.2.3 人間の判読可能な出力のラベル化
    - 3.2.1.3.3 サブジェクト センシィティビティ ラベル
    - 3.2.1.3.4 装置ラベル
  - 3.2.1.4 強制（的）アクセス制御
- 3.2.2 責任
  - 3.2.2.1 識別と認証
    - 3.2.2.1.1 トラステッド・パス
  - 3.2.2.2 監査
- 3.2.3 保証

3.2.1 セキュリティポリシー

3.2.1.1 任意(自由裁量的)アクセス制御

TCB は、自動データ処理（ADP）システムにおける名前付きのユーザと名前付きのオブジェクト(例えば ファイルやプログラム)の間のアクセスを定義し制御しなければならない。強制メカニズム (例えば self/group/public 制御、 アクセス制御リスト) によって、ユーザがオブジェクトの共有を名前付きの個人、または定められたグループ(あるいはその両方)を単位として、指定および制御できなければならない。また、同メカニズムはアクセス権の伝播を制限する制御方法を提供しなければならない。
任意（自由裁量)アクセス制御メカニズムは、明示的なユーザの操作によって、あるいはデフォルトで、正式な許可なしのアクセスからオブジェクトを保護しなければならない。こういったアクセス制御は単一ユーザの粒度でアクセスを可能にしたり不可能にしたりする能力を持たなければならない。オブジェクトへのユーザ毎のアクセス許可権限は、まだ付与されていない場合、正式な許可ユーザによってのみ付与されなければならない。

3.2.1.2 オブジェクト再使用

未使用のストレージ・オブジェクトの TCB のプールからサブジェクトへの初期の割り当て、配分、または再配分に先がけて無効にすべきである。システムにリリースバックされているオブジェクトにアクセスできるいかなるサブジェクトも、事前のサブジェクトの動作によって生成される暗号化表現が含まれる情報を利用できてはならない。

3.2.1.3 ラベル

制御下にある各サブジェクトおよび記憶オブジェクト(例えばプロセス、ファイル、セグメント、装置)に関連性のある機密ラベルは、ＴＣＢによって維持されなければならない。これらのラベルは、強制アクセス制御決定の基礎として使用されなければならない。ラベル

が付けられていないデータをインポートするために、ＴＣＢは、正式に許可されたユーザにデータのセキュリティレベルを要求し、それを受け取らなければならない。また、そのようなアクションはすべてTCBにより監査可能としなければならない。
ＴＣＢ外部のサブジェクトにより直接あるいは間接的にアクセスできる各ＡＤＰシステムリソース(例えばサブジェクト、記憶オブジェクト、ＲＯＭ)に関連性のある機密ラベルは、ＴＣＢによって維持されなければならない。

3.2.1.3.1 ラベルの完全性

機密ラベルは、それらが関連する特定のサブジェクトまたはオブジェクトのセキュリティレベルを正確に表さなければならない。
TCB によってエクスポートされる時に、機密ラベルは内部ラベルを正確にかつ明確に表すこととし、エクスポートされようとしている情報に付随されなければならない。

3.2.1.3.2 ラベル付けされた情報のエクスポート

TCB は、それぞれの通信チャネルおよび I/O 装置を、単一レベル装置またはマルチレベル装置であると指定しなければならない。この指定のいかなる変更も手作業で行われなければならず、また TCB によって監査可能でなければならない。TCB は、通信チャネルや I/O 装置のセキュリティレベルのいかなる変更も保持し、かつ、いかなる変更も監査可能でなければならない。

3.2.1.3.2.1 マルチレベル装置へのエクスポート

TCB がオブジェクトをマルチレベル I/O 装置にエクスポートする際、そのオブジェクトに紐づけられた機密ラベルも一緒にエクスポートされなければならず、エクスポートされた情報と同じ物理媒体に同じ形式（機械データもしくは自然言語等）で記録されなければならない。TCB がオブジェクトをマルチレベル通信チャネルにエクスポート、あるいはインポートする際、そのチャネルで使用されるプロトコルは、送受される情報と、その機密ラベルの組を明確に示さなければならない。

3.2.1.3.2.2. 単一レベル装置へのエクスポート

単一レベル I/O 装置および単一レベル通信チャネルは、処理している情報の機密ラベルを保守する必要がない。しかしながら TCB は、単一レベルの通信チャネルまたは I/O 装置を介してインポートあるいはエクスポートされる情報の単一のセキュリティレベルを確保するために、TCB と許可されたユーザが信頼して通信するメカニズムを含まなければならない。

3.2.1.3.2.3 人間の判読可能な出力のラベル化

ＡＤＰシステム管理者は、エクスポートされる機密ラベルに関連性のある表記可能なラベル名を指定できなければならない。TCBは、人間に可読でページ付けされている全てのハ

ードコピー出力(例えばラインプリンタ出力)の始めと終わりに、その出力の機密度を正確に*表現する人間に可読な機密ラベルをマークしなければならない。
TCB はデフォルトで、人間の判読可能なハードコピー出力(例えばラインプリンタ出力)の各ページの上部と下部に、その出力の全体的な機密度を正確に*表現する、あるいはそのページ上の情報の機密度を正確に*表現する、人間に可読な機密ラベルをマークしなければならない。
TCB はデフォルトで、そして適切な方法により、人間に可読な他の様式の出力（例えば、マップ、グラフィックス）に、その出力の機密度を正確に*表現する、人間に可読な機密ラベルをマークしなければならない。これらのデフォルトのマーキングに対する、いかなる書換えも TCB により監査可能としなければならない。

3.2.1.3.3 サブジェクト センシィティビティ ラベル

TCB は直ちに、対話型セッションの間にそのユーザと関連したセキュリティレベルにおける各変化を、ターミナルユーザに通知しなければならない。ターミナルユーザは、サブジェクトの完全なセンシィティビティラベルを表示するために、必要に応じ TCB に質問できなければならない。

3.2.1.3.4 装置ラベル

TCB は接続された全ての物理的装置に対し、最少および最大のセキュリティレベルを設定可能であり、これらのセキュリティレベルは、装置の置かれた場所の物理的環境によって生じる制約を強制するために TCB によって使われるべきである。

3.2.1.4 強制(的)アクセス制御

ＴＣＢは、ＴＣＢ外部のサブジェクトによって直接あるいは間接的にアクセス可能な、すべての資源(つまりサブジェクト、ストレージオブジェクト、I/0 装置)に対して強制アクセス制御のポリシーを実施しなければならない。これらのサブジェクトとオブジェクトは、階層的な機密度区分レベルと階層的でないカテゴリーとの組み合わせである機密ラベルを割り当てられることとし、そのラベルは強制アクセス制御の決定のための基礎として使われなければならない。TCB は、ふたつ以上のそのようなセキュリティレベルをサポートできることとする。(強制アクセス制御ガイドラインを参照。) 次の要求事項が、ＴＣＢ外のすべてのサブジェクトと、これらのサブジェクトによって直接あるいは間接的にアクセス可能なすべてのオブジェクト間のあらゆるアクセスにあてはまらなければならない：サブジェクトのセキュリティレベルにおける階層区分が、オブジェクトのセキュリティレベルにおける階層区分より大きいかあるいは等しく、そして、サブジェクトのセキュリティレベルにおける階層的でないカテゴリがオブジェクトのセキュリティレベルの階層的でないカテゴリの全てを含むのであれば、サブジェクトはオブジェクトを読むことができる。サブジェクトのセキュリティレベルにおける階層区分が、オブジェクトのセキュリティレベルにおける階層区分より小さいかあるいは等しく、そして、サブジェクトのセキュリティレベルにおける階層的でないカテゴリの全てがオブジェクトのセキュリティレベルにおけ

る階層的でないカテゴリに含まれるのであれば、サブジェクトはオブジェクトに書くことができる。識別と認証のデータは、ユーザの本人性を認証するために、そしてまた、個々のユーザのために動作するよう作成される TCB 外のサブジェクトのセキュリティレベルと認可がそのユーザのクリアランスと認可によって支配されることを保証するために、TCB により使われなければならない。

3.2.2 責任

3.2.2.1 識別と認証

TCB が調停することになっている動作をユーザが始めるより前に、TCB はユーザがユーザ自身であることを識別するようユーザに要求しなければならない。さらに TCB は個別のユーザの真正性を確認するための情報（パスワードなど）を含む認証データを保持しなければならない。TCB は、個別のユーザのクリアランスと認可を決定するための情報も同様に保持しなければならない。これらのデータはユーザの真正性を認証するために TCB に利用されなければならない。また個別のユーザに代わって動作するために作られる TCB 外にあるサブジェクト（アクセスの主体）のセキュリティレベルと認可がそのユーザのクリアランスと認可によって支配されることを保証するためにも、これらのデータは TCB に利用されなければならない。

3.2.2.1.1 トラステッド・パス

TCB は、それ自身とユーザ間の初期のログインと認証のためのトラステッド・
コミュニケーション・パスをサポートするものでなければならない。このパス経由の通信は、もっぱらユーザによって始められなければならない。

3.2.2.2 監査

TCB は保護対象のオブジェクトへのアクセス監査証跡を生成し、維持し、そして修正あるいは不正アクセスあるいは破壊から保護することができなければならない。監査データは，それへの読取りアクセスが承認された者に限定されるように，TCB によって保護されるべきである。
TCB は次に示すようなタイプの事象を記録できなければならない。:
識別番号の利用と認証メカニズム，ユーザドレス空間へのオブジェクトの導入（例えばファイルオープンやプログラムの開始），オブジェクトの消去，そしてコンピュータオペレータとシステム管理者，システムセキュリティ責任者と他のセキュリティ関連事象のうちの両方か、もしくはそのいずれかによる活動。TCB は人間に可読な出力表示のマーキングのいかなる書換えも監査できなければならない。
それぞれの記録された事象に対して，監査レコードは以下を特定する：事象発生日時，ユーザ，事象タイプ，事象の成功・不成功の区別。
識別／認証の事象に対して，その要求元（例えば端末 ID）は監査レコードに含まれなければならない。オブジェクトをユーザドレス空間へ導入する事象とオブジェクトを消去する事象については，監査レコードはオブジェクト名およびオブジェクトのセキュリティレベ

ルを含まなければならない。ADP システムの管理者は，個別属性に基づく任意の 1 人かそれ以上のユーザの活動と，オブジェクトのセキュリティレベルのうち，両方もしくはいずれか一方を選択的に監査できなければならない。
TCB は隠れストレージチャネルの利用において用いられる特定された事象を監査できなければならない。

3.2.3 保証

3.2.3.1 操作上の保証

3.2.3.1.1 システムアーキテクチャ

TCB は、外部の干渉または改変(例えばコードまたはデータ構造の部分修正による)から TCB を保護する TCB 自身の実行のためにドメインを維持しなければならない。
TCB は、TCB のコントロール下で別アドレス空間の提供を通してプロセス分離を維持しなければならない。TCB の大部分は独立モジュールの中で内部的に構造化されなければならない。TCB は、保護の危機にない要素から、危機にある要素を分離するために、入手可能なハードウェアを効果的に利用しなければならない。TCB モジュールは最少特権の原則が強化されるように設計されなければならない。セグメント化などのハードウェア機能は、個々の属性（すなわち：読込可能、書込可能）を備えた論理上別個のストレージ・オブジェクトを支援するのに使われなければならない。TCB へのユーザインタフェースは完全に定義され、TCB の要素はすべて識別されなければならない。

3.2.3.1.2 システムの完全性

ハードウェアおよび(または)ソフトウェアの機能（features）は、TCB の実地におけるハードウェアおよびファームウェア要素の正確なオペレーションを定期的に確認するために使用できるように備えられなければならない。

3.2.3.1.3 隠れチャネル解析

システム開発者は，隠れストレージチャネルの悉皆探索を実行し，確認された各チャネルの最大バンド幅を決定する（実測または工学的評価法のどちらかを用いて）。（隠れチャネルガイドラインセクションを見よ）

3.2.3.1.4 信頼できる設備管理

TCB は、オペレータと管理機能の分離をサポートしなければならない。

3.2.3.2 ライフサイクル上の保証

3.2.3.2.1 セキュリティ検査

自動データ処理（ADP）システムのセキュリティ機構は,、システムドキュメントにより要求されるようにテストされ動作するか調査しなければならない。TCB の特徴の実施を完全に理解する個人からなるチームは、そのデザインドキュメント、ソースコード、およびオブジェクトコードの徹底的な分析とテストに従事することになる。

それらのオブジェクトは次のようでなければならない：TCB により求められる強制または任意（自由裁量)のセキュリティポリシーの下で正常に拒否されたデータを読み、変更、削除するために、TCB の外のサブジェクトを許すというすべてのデザインとインプリメンテーションの弱点を摘発すること。; いかなるサブジェクトも、（そのような認可なしで）他のユーザが開始したコミュニケーションに応じられないような状態にして、TCB に入れないようにするのを保証するのと同様である。TCB は相対的に侵入に抵抗力があるのを発見されなければならない。すべての発見された弱点は訂正されなければならず、かつ、それらが取り除かれて、新しい弱点が導入されていないことを証明するために、TCB は再テストされなければならない。テストは、TCB インプリメンテーションが記述的なトップレベルの仕様と一致していることを証明しなければならない。
(参照 セキュリティ テスティング ガイドライン)

3.2.3.2.2 設計仕様と検証

TCB がサポートするセキュリティポリシーのインフォーマルモデルおよびフォーマルモデルは、自動データ処理（ADP）システムのライフサイクルを通してモデルの公理と一貫性があることを示すように、保守されなければならない。
TCB の最上位仕様(DTLS)は、TCB の例外、 エラーメッセージ、および効果の観点から完全かつ正確に TCB を記述するように保守されなければならない。また、DTLS が TCB のインタフェースの正確な記述となっていることが示されなければならない。

3.2.3.2.3 構成管理

TCB を開発し維持している間は，構成管理システムは，記述された最上位レベル仕様，他の設計データ，実装作業用文書，ソースコード，オブジェクトの現行バージョン，および試験結果とその文書の変更管理を維持するために，しかるべく機能していなければならない。構成管理システムは，全文書と現行バージョンに対応したコードの間の首尾一貫した対応関係を保証しなければならない。ソースコードから TCB の新バージョンを生成するためのツール類を準備する必要がある。また，意図された変更のみが TCB の新バージョンとして実際使われるコードの中に加えられていることを確かめるために新たに生成したバージョンと前の TCB バージョンとを比較する目的にも，ツール類が利用可能になっていなければならない。

3.2.4 証拠資料

3.2.4.1 セキュリティに特化したユーザズガイド

ユーザドキュメントの中の単一の要約、章、またはマニュアルは、TCB によって提供されたプロテクション機構、機構利用におけるガイドライン、及び機構がどのように相互に影響するかを記述しなければならない。

3.2.4.2 信頼できる設備マニュアル

自動データ処理（ADP）システム管理者向けのマニュアルは、セキュア設備を使用する時

に制御されるべき機能と特権について警告を示さなければならない。
各タイプの監査イベントの詳細な監査記録構造と同じく監査ファイルを検査し、維持するための手続が与えられなければならない。
マニュアルは、利用者のセキュリティ特性を変更することを含めオペレータと管理者のセキュリティ関連機能を説明しなければならない。システムの保護機能の一貫した効率的な利用、その機能がどのように相互に作用するか、安全に新しい TCB をどのように生成するか､そして安全な方法で設備を運営するために制御される必要のある設備の手続や警告、特権に関するガイドラインをマニュアルは提供しなければならない。
リファレンス検証機構を含んでいる TCB モジュールが明確にされなければならない｡TCB 内の任意のモジュールの修正後の新しい TCB のソースからの安全な生成の手続きが示されなければならない。

3.2.4.3 検査証拠資料

システム開発者は、テスト計画について記述したドキュメント、セキュリティ・メカニズムがどのようにテストされたかを示すテスト手続き、およびセキュリティ・メカニズムの機能的なテストの結果を、評価者に提供しなければならない。
それは、隠れチャネルのバンド幅を減らすために使われた方法の有効性を検査した結果を含まなければならない。

3.2.4.4 設計文書

メーカの保護体系の記述およびこの体系がどのように TCB に変換されるかが説明された文書が利用可能でなければならない。
TCB モジュール間のインタフェースは記述されている必要がある。TCB によって実行されるセキュリティポリシーモデルのフォーマルな記述は利用可能であって，かつセキュリティポリシーを実行することが十分であることが証明されていなければならない。
具体的な TCB 保護メカニズムが確認され，それがモデルを満足することを示す説明がなされていなければならない。
最上位仕様（DTLS）は，TCB インタフェースの記述が正確であることを示していなければならない｡文書は TCB がどのようにしてリファレンスモニターの概念を実装するのか，またなぜそれが耐タンパであり，パイパス困難であり，そして正しく実装されるのかについて記述していなければならない。文書は，検査を円滑に進め，最少特権を実行するために，TCB がどのように構造化されているのかについて，記述しなければならない。この文書はまた，隠れチャネルの解析結果およびチャネルの制限に関与したトレードオフを提示すべきである。既知の隠れストレージチャネルの利用に用いられる全ての監査可能な事象は識別されなければならない。既知の隠れストレージチャネルのバンド幅は，監査メカニズムではそれが使われていることを検知できないが，示されていなければならない。(隠れチャネルガイドラインセクションを見よ)

3.3 クラス（B3)：セキュリティドメイン

クラス（B3)の TCB はサブジェクトからオブジェクトへの全てのアクセスを仲介すると言うリファレンスモニターの要件を満たし、不正な変更に耐え、解析と検査を行うのに十分小型でなければならない。

最終的には、TCB は複雑性を最少化する方向で、TCB 設計と実装を通じての重要なシステム・エンジニアリング活動によって、セキュリティポリシーを適用するためには必須でないコードを除外するために構造化される。そして、セキュリティ管理者がサポートを受け、監査メカニズムが信号セキュリティがらみのイベントへ拡張され、システムの回復手順が要求される。当システムは侵入に対して強い耐性がある。以下はクラス(B3)システムとして評価するための最小基準です。

- 3.3.1 セキュリティポリシー
  - 3.3.1.1 任意（自由裁量的）アクセス制御
  - 3.3.1.2 オブジェクト再使用
    - 3.3.1.3.1 システムの完全性
    - 3.3.1.3.2 ラベル付けされた情報のエクスポート
      - 3.3.1.3.2.1 マルチレベル装置へのエクスポート
      - 3.3.1.3.2.2. 単一レベル装置へのエクスポート
      - 3.3.1.3.2.3 人間の判読可能な出力のラベル化
    - 3.3.1.3.3 サブジェクト センシィティビティ ラベル
    - 3.3.1.3.4 装置ラベル
  - 3.3.1.4 強制（的）アクセス制御
- 3.3.2 責任
  - 3.3.2.1 識別と認証
    - 3.3.2.1.1 トラステッド・パス
  - 3.3.2.2 監査
- 3.3.3 保証
  - 3.3.3.1 操作上の保証
    - 3.3.3.1.1 システムアーキテクチャ
    - 3.3.3.1.2 システムの完全性
    - 3.3.3.1.3 隠れチャネル解析
    - 3.3.3.1.4 信頼できる設備管理
    - 3.3.3.1.5 信頼できる復旧
  - 3.3.3.2 ライフサイクル上の保証
    - 3.3.3.2.1 セキュリティ検査
    - 3.3.3.2.2 設計仕様と検証
    - 3.3.3.2.3 構成管理
- 3.2.4 証拠資料
  - 3.3.4.1 セキュリティに特化したユーザズガイド

3.3.4.2 信頼できる設備マニュアル
3.3.4.3 検査証拠資料
3.3.4.4 設計文書

3.3.1 セキュリティポリシー

3.3.1.1 任意(自由裁量的)アクセス制御

TCB は、自動データ処理（ADP）システムにおける名前付きのユーザと名前付きのオブジェクト(例えば ファイルやプログラム)の間のアクセスを定義し制御しなければならない。
強制メカニズム (例えば アクセス制御リスト) によって、ユーザがオブジェクトの共有を指定および制御できなければならない。また、同メカニズムはアクセス権の伝播を制限する制御方法を提供しなければならない。こういったアクセス制御は、名前付きのオブジェクトそれぞれについて、名前付きの個人のリストや名前付きの個人からなるグループのリストと、それらのリスト毎のオブジェクトに対するアクセスモードを指定できる能力を持たなければならない。
その上、それぞれの名前付きのオブジェクトについて、強制メカニズムは、オブジェクトへのアクセスが与えられない名前付きの個人のリストおよび名前付きの個人からなるグループのリストを指定することが可能でなければならない。
オブジェクトへのユーザ毎のアクセス許可権限は、まだ付与されていない場合、正式な許可ユーザによってのみ付与されなければならない。

3.3.1.2 オブジェクト再使用

未使用のストレージ・オブジェクトの TCB のプールからサブジェクトへの初期の割り当て、配分、または再配分に先がけて無効にすべきである。システムにリリースバックされているオブジェクトにアクセスできるいかなるサブジェクトも、事前のサブジェクトの動作によって生成される暗号化表現が含まれる情報を利用できてはならない。

3.3.1.3.1 システムの完全性

ハードウェアおよび(または)ソフトウェアの機能（features）は、TCB の実地におけるハードウェアおよびファームウェア要素の正確なオペレーションを定期的に確認するために使用できるように備えられなければならない。

3.3.1.3.2 ラベル付けされた情報のエクスポート

TCB は、それぞれの通信チャネルおよび I/O 装置を、単一レベル装置またはマルチレベル装置であると指定しなければならない。この指定のいかなる変更も手作業で行われなければならず、また TCB によって監査可能でなければならない。TCB は、通信チャネルや I/O 装置のセキュリティレベルのいかなる変更も保持し、かつ、いかなる変更も監査可能でなければならない。

3.3.1.3.2.1 マルチレベル装置へのエクスポート

TCB がオブジェクトをマルチレベル I/O 装置にエクスポートする際、そのオブジェクトに紐づけられた機密ラベルも一緒にエクスポートされなければならず、エクスポートされた情報と同じ物理媒体に同じ形式（機械データもしくは自然言語等）で記録されなければならない。TCB がオブジェクトをマルチレベル通信チャネルにエクスポート、あるいはインポートする際、そのチャネルで使用されるプロトコルは、送受される情報と、その機密ラベルの組を明確に示さなければならない。

3.3.1.3.2.2. 単一レベル装置へのエクスポート

単一レベル I/O 装置および単一レベル通信チャネルは、処理している情報の機密ラベルを保守する必要がない。しかしながら TCB は、単一レベルの通信チャネルまたは I/O 装置を介してインポートあるいはエクスポートされる情報の単一のセキュリティレベルを確保するために、TCB と許可されたユーザが信頼して通信するメカニズムを含まなければならない。

3.3.1.3.2.3 人間の判読可能な出力のラベル化

ＡＤＰシステム管理者は、エクスポートされる機密ラベルに関連性のある表記可能なラベル名を指定できなければならない。TCB は、人間に可読でページ付けされている全てのハードコピー出力(例えばラインプリンタ出力)の始めと終わりに、その出力の機密度を正確に*表現する人間に可読な機密ラベルをマークしなければならない。

TCB はデフォルトで、人間の判読可能なハードコピー出力(例えばラインプリンタ出力)の各ページの上部と下部に、その出力の全体的な機密度を正確に*表現する、あるいはそのページ上の情報の機密度を正確に*表現する、人間に可読な機密ラベルをマークしなければならない。

TCB はデフォルトで、そして適切な方法により、人間に可読な他の様式の出力（例えば、マップ、グラフィックス）に、その出力の機密度を正確に*表現する、人間に可読な機密ラベルをマークしなければならない。これらのデフォルトのマーキングに対する、いかなる書換えも TCB により監査可能としなければならない。

3.3.1.3.3 サブジェクト センシィティビティ ラベル

TCB は直ちに、対話型セッションの間にそのユーザと関連したセキュリティレベルにおける各変化を、ターミナルユーザに通知しなければならない。ターミナルユーザは、サブジェクトの完全なセンシィティビティラベルを表示するために、必要に応じ TCB に質問できなければならない。

3.3.1.3.4 装置ラベル

TCB は接続された全ての物理的装置に対し、最少および最大のセキュリティレベルを設定可能であり、これらのセキュリティレベルは、装置の置かれた場所の物理的環境によって

生じる制約を強制するためにTCBによって使われるべきである。

3.3.1.4 強制(的)アクセス制御

ＴＣＢは、ＴＣＢ外部のサブジェクトによって直接あるいは間接的にアクセス可能な、すべての資源(つまりサブジェクト、ストレージオブジェクト、I/0 装置)に対して強制アクセス制御のポリシーを実施しなければならない。これらのサブジェクトとオブジェクトは、階層的な機密度区分レベルと階層的でないカテゴリーとの組み合わせである機密ラベルを割り当てられることとし、そのラベルは強制アクセス制御の決定のための基礎として使われなければならない。TCBは、ふたつ以上のそのようなセキュリティレベルをサポートできることとする。(強制アクセス制御ガイドラインを参照。) 次の要求事項が、ＴＣＢ外のすべてのサブジェクトと、これらのサブジェクトによって直接あるいは間接的にアクセス可能なすべてのオブジェクト間のあらゆるアクセスにあてはまらなければならない：サブジェクトのセキュリティレベルにおける階層区分が、オブジェクトのセキュリティレベルにおける階層区分より大きいかあるいは等しく、そして、サブジェクトのセキュリティレベルにおける階層的でないカテゴリがオブジェクトのセキュリティレベルの階層的でないカテゴリの全てを含むのであれば、サブジェクトはオブジェクトを読むことができる。サブジェクトのセキュリティレベルにおける階層区分が、オブジェクトのセキュリティレベルにおける階層区分より小さいかあるいは等しく、そして、サブジェクトのセキュリティレベルにおける階層的でないカテゴリの全てがオブジェクトのセキュリティレベルにおける階層的でないカテゴリに含まれるのであれば、サブジェクトはオブジェクトに書くことができる。識別と認証のデータは、ユーザの本人性を認証するために、そしてまた、個々のユーザのために動作するよう作成されるTCB外のサブジェクトのセキュリティレベルと認可がそのユーザのクリアランスと認可によって支配されることを保証するために、TCBにより使われなければならない。

3.3.2 責任

3.3.2.1 識別と認証

TCBが調停することになっている動作をユーザが始めるより前に、TCBはユーザがユーザ自身であることを識別するようユーザに要求しなければならない。さらにTCBは個別のユーザの真正性を確認するための情報（パスワードなど）を含む認証データを保持しなければならない。TCBは、個別のユーザのクリアランスと認可を決定するための情報も同様に保持しなければならない。これらのデータはユーザの真正性を認証するためにTCBに利用されなければならない。また個別のユーザに代わって動作するために作られるTCB外にあるサブジェクト（アクセスの主体）のセキュリティレベルと認可がそのユーザのクリアランスと認可によって支配されることを保証するためにも、これらのデータはTCBに利用されなければならない。

3.3.2.1.1 トラステッド・パス

ユーザへの積極的なTCB接続が要求される場合(例えば、ログインし、オブジェクトのセ

キュリティ・レベルを変更する)、 TCB は、それ自体と利用ユーザ間の信頼されたコミュニケーション・パスをサポートしなければならない。このトラステッド・パスによるコミュニケーションはもっぱらユーザあるいは TCB によって活性化されるものとし、 論理的に分離され、かつ、他の経路から誤りなく区別できなければならない。

3.3.2.2 監査

TCB は保護対象のオブジェクトへのアクセス監査証跡を生成し、維持し、そして修正あるいは不正アクセスあるいは破壊から保護することができなければならない。監査データは, それへの読取りアクセスが承認された者に限定されるように, TCB によって保護されるべきである。

TCB は次に示すようなタイプの事象を記録できなければならない。:

識別番号の利用と認証メカニズム，ユーザドレス空間へのオブジェクトの導入（例えばファイルオープンやプログラムの開始)，オブジェクトの消去，そしてコンピュータオペレータとシステム管理者，システムセキュリティ責任者と他のセキュリティ関連事象のうちの両方か、もしくはそのいずれかによる活動。TCB は人間に可読な出力表示のマーキングのいかなる書換えも監査できなければならない。

それぞれの記録された事象に対して，監査レコードは以下を特定する：事象発生日時，ユーザ，事象タイプ，事象の成功・不成功の区別。

識別／認証の事象に対して，その要求元（例えば端末 ID）は監査レコードに含まれなければならない。オブジェクトをユーザドレス空間へ導入する事象とオブジェクトを消去する事象については，監査レコードはオブジェクト名およびオブジェクトのセキュリティレベルを含まなければならない。ADP システムの管理者は，個別属性に基づく任意の 1 人かそれ以上のユーザの活動と，オブジェクトのセキュリティレベルのうち，両方もしくはいずれか一方を選択的に監査できなければならない。

TCB は隠れストレージチャネルの利用において用いられる特定された事象を監査できなければならない。TCB はセキュリティポリシーの差し迫った侵害を暗示するセキュリティ監査可能事象の発生または蓄積をモニターできるメカニズムを包含しなければならない。このメカニズムは, 閾値を超えた時点でセキュリティ管理者に直ちに通知することができ, もしこれらセキュリティ関連事象の発生もしくは累積が続くようなら，その事象を終結させるため，システムは破壊的行為を止めなければならない。

3.3.3 保証

3.3.3.1 操作上の保証

3.3.3.1.1 システムアーキテクチャ

TCB は、外部の干渉または改変(例えばコードまたはデータ構造の部分修正による)から TCB を保護する TCB 自身の実行のためにドメインを維持しなければならない。

TCB は、TCB のコントロール下で別アドレス空間の提供を通してプロセス分離を維持しなければならない。TCB の大部分は独立モジュールの中で内部的に構造化されなければならない。TCB は、保護の危機にない要素から、危機にある要素を分離するために、入手

可能なハードウェアを効果的に利用しなければならない。TCB モジュールは最少特権の原則が強化されるように設計されなければならない。セグメント化などのハードウェア機能は、個々の属性（すなわち：読込可能、書込可能）を備えた論理上別個のストレージ・オブジェクトを支援するのに使われなければならない。TCB へのユーザインタフェースは完全に定義され、TCB の要素はすべて識別されなければならない。
TCB は、正確に定義された意味論を備えた 完全で、概念的に単純な保護メカニズムを使用するよう設計され構造化されなければならない。このメカニズムは、TCB とそのシステムの内部構造を強化する際に中心的な役割を果たさなければならない。TCB は、レイヤー化、抽象化およびデータ隠蔽という重要な効用を組み込まなければならない。重要なシステム工学は、TCB の複雑さを最小限にし、保護の危機にない TCB モジュールを除くように指向しなければならない。

3.3.3.1.2 システムの完全性
ハードウェアおよび(または)ソフトウェアの機能（features）は、TCB の実地におけるハードウェアおよびファームウェア要素の正確なオペレーションを定期的に確認するために使用できるように備えられなければならない。

3.3.3.1.3 隠れチャネル解析
システム開発者は，隠れチャネルの悉皆探索を実行し，確認された各チャネルの最大バンド幅を決定する（実測または工学的評価法のどちらかを用いて）。

3.3.3.1.4 信頼できる設備管理
TCB は、オペレータと管理機能の分離をサポートしなければならない。
セキュリティ管理者の役割の下で実行される機能は、それ以外の機能と区別されなければならない。ADP システムの管理要員は、対象となる ADP システム上でセキュリティ管理者の役割を確立するための明確な監査可能行動を取った場合にのみ、セキュリティ管理機能を実行できるようにすべきである。セキュリティ管理役割において実施できる非セキュリティ機能は、セキュリティ役割を効果的に実行するのに必須の事項に厳密に制限されなければならない。セキュリティ管理の役割内で実行される非セキュリティ機能は、効率的なセキュリティの役割遂行に必要なもののみに制限されなければならない。

3.3.3.1.5 信頼できる復旧
ADP システムの故障もしくは他の障害に対して、故障前のシステム保護水準を維持した状態で復旧できることを保証する手続きや機構を提供しなければならない。

3.3.3.2 ライフサイクル上の保証
3.3.3.2.1 セキュリティ検査
自動データ処理（ADP）システムのセキュリティ機構は、、システムドキュメントにより要されるようにテストされ動作するか調査しなければならない。TCB の特徴の実施を完全

理解する個人からなるチームは、そのデザインドキュメント、ソースコード、およびオブジェクトコードの徹底的な分析とテストに従事することになる。
それらのオブジェクトは次のようでなければならない：TCB により求められる強制または任意（自由裁量)のセキュリティポリシーの下で正常に拒否されたデータを読み、変更、削除するために、TCB の外のサブジェクトを許すというすべてのデザインとインプリメンテーションの弱点を摘発すること。；いかなるサブジェクトも、（そのような認可なしで）他のユーザが開始したコミュニケーションに応じられないような状態にして、TCB に入れないようにするのを保証するのと同様である。TCB は相対的に侵入に抵抗力があるのを発見されなければならない。すべての発見された弱点は訂正されなければならず、かつ、それらが取り除かれて、新しい弱点が導入されていないことを証明するために、TCB は再テストされなければならない。テストは、TCB インプリメンテーションが記述的なトップレベルの仕様と一致していることを証明しなければならない。
(参照 セキュリティ テスティング ガイドライン)
設計上の欠陥、修正可能な実装上の欠陥のいくつかはテスト中に発見されないかもしれないが、そのような欠陥はほとんど残っていないという妥当な信頼をおくこととする。

3.3.3.2.2 設計仕様と検証

TCB がサポートするセキュリティポリシーのインフォーマルモデルおよびフォーマルモデルは、自動データ処理（ADP）システムのライフサイクルを通してモデルの公理と一貫性があることを示すように、保守されなければならない。
TCB の最上位仕様(DTLS)は、TCB の例外、 エラーメッセージ、および効果の観点から完全かつ正確に TCB を記述するように保守されなければならない。また、DTLS が TCB のインタフェースの正確な記述となっていることが示されなければならない。
DTLS がモデルと一貫性を持っていると納得できるだけの論拠が与えられなければならない。

3.3.3.2.3 構成管理

TCB を開発し維持している間は，構成管理システムは，記述された最上位レベル仕様，他の設計データ，実装作業用文書，ソースコード，オブジェクトの現行バージョン，および試験結果とその文書の変更管理を維持するために，しかるべく機能していなければならない。構成管理システムは，全文書と現行バージョンに対応したコードの間の首尾一貫した対応関係を保証しなければならない。ソースコードから TCB の新バージョンを生成するためのツール類を準備する必要がある。また，意図された変更のみが TCB の新バージョンとして実際使われるコードの中に加えられていることを確かめるために新たに生成したバージョンと前の TCB バージョンとを比較する目的にも，ツール類が利用可能になっていなければならない。

3.2.4 証拠資料

3.3.4.1 セキュリティに特化したユーザズガイド

ユーザドキュメントの中の単一の要約、章、またはマニュアルは、TCB によって提供されたプロテクション機構、機構利用におけるガイドライン、及び機構がどのように相互に影響するかを記述しなければならない。

3.3.4.2 信頼できる設備マニュアル

自動データ処理（ADP）システム管理者向けのマニュアルは、セキュア設備を使用する時に制御されるべき機能と特権について警告を示さなければならない。
各タイプの監査イベントの詳細な監査記録構造と同じく監査ファイルを検査し、維持するための手続が与えられなければならない。
マニュアルは、利用者のセキュリティ特性を変更することを含めオペレータと管理者のセキュリティ関連機能を説明しなければならない。システムの保護機能の一貫した効率的な利用、その機能がどのように相互に作用するか、安全に新しい TCB をどのように生成するか､そして安全な方法で設備を運営するために制御される必要のある設備の手続や警告、特権に関するガイドラインをマニュアルは提供しなければならない。
リファレンス検証機構を含んでいる TCB モジュールが明確にされなければならない｡TCB 内の任意のモジュールの修正後の新しい TCB のソースからの安全な生成の手続きが示されなければならない。
システムが安全な方法で最初から起動されることを保証する手続をマニュアルは含まなければならない。また、システム操作のいかなる経過の後の安全なシステム操作を再開する手続が含まなければならない。

3.3.4.3 検査証拠資料

システム開発者は、テスト計画について記述したドキュメント、セキュリティ・メカニズムがどのようにテストされたかを示すテスト手続き、およびセキュリティ・メカニズムの機能的なテストの結果を、評価者に提供しなければならない。
それは、隠れチャネルのバンド幅を減らすために使われた方法の有効性を検査した結果を含まなければならない。

3.3.4.4 設計文書

メーカの保護体系の記述およびこの体系がどのように TCB に変換されるかが説明された文書が利用可能でなければならない。
TCB モジュール間のインタフェースは記述されている必要がある。TCB によって実行されるセキュリティポリシーモデルのフォーマルな記述は利用可能であって，かつセキュリティポリシーを実行することが十分であることが証明されていなければならない。
具体的な TCB 保護メカニズムが確認され，それがモデルを満足することを示す説明がなされていなければならない。
最上位仕様（DTLS）は，TCB インタフェースの記述が正確であることを示していなければならない｡文書は TCB がどのようにしてリファレンスモニターの概念を実装するのか，またなぜそれが耐タンパであり，パイパス困難であり，そして正しく実装されるのかにつ

いて記述していなければならない。TCB の実装（ハードウェア，ファームウェア及びソフトウェアにおける）は，DTLS と合致していることがインフォーマルに示されるべきである。
DTLS の要素が TCB の要素に対応していることが，インフォーマルな技法を使って示されなければならない。
文書は，検査を円滑に進め，最少特権を実行するために，TCB がどのように構造化されているのかについて，記述しなければならない。この文書はまた，隠れチャネルの解析結果およびチャネルの制限に関与したトレードオフを提示すべきである。既知の隠れストレージチャネルの利用に用いられる全ての監査可能な事象は識別されなければならない。既知の隠れストレージチャネルのバンド幅は，監査メカニズムではそれが使われていることを検知できないが，示されていなければならない。（隠れチャネルガイドラインセクションを見よ）

4.0 区分 A：検証された保護

この区分の特徴はフォーマルなセキュリティの検証方法を使用することにあり、システムの中で使用される強制及び任意（自由裁量)のセキュリティ制御が、システムによって蓄積され、あるいは処理される機密区分の情報あるいは他の取扱注意の情報を効果的に保護できることを保証する。
TCB が設計、開発、およびインプリメンテーションのすべての面でセキュリティ要件を満たしていることを証明するためには、より詳細な文書が必要である。

4.1 クラス(A1)：検証された設計

クラス(A1)中のシステムは、どの追加のアーキテクチャ上の機能またはポリシー要件も追加されないという点において機能的にクラス(B3)中のそれらと等しい。
このクラスの中のシステムの顕著な特徴は、フォーマルな設計仕様と検証技法により導出される解析と、結果として TCB が正しく実装されることの高い保証の程度にある。
この保証は事実上発展的なものであり、セキュリティポリシーのフォーマルなモデルと設計のフォーマルな最高位の仕様(FTLS)で始まっている。
使われた特定の仕様言語または検証システムから独立して、クラス(A1)の設計検証には 5 つの重要な規準がある：

* セキュリティポリシーのフォーマルなモデルは、そのモデルがその公理と一致していて､セキュリティポリシーを支持することについて十分であるという数学的な証明を含めて、明確に識別され、文書化されなければならない。
* FTLS は TCB が実行する機能と、異なる実行ドメインをサポートするハードウェアおよび/またはファームウェアメカニズムの抽象的な定義を含むよう作成されなければならない。
* TCB の FTLS は可能な(検証ツールが存在している場合)フォーマルな技法により､そうでなければインフォーマルなものにより､そのモデルと一致しているということが示されなければならない。
* TCB のインプリメンテーション(すなわちハードウェア、ファームウェア、およびソフトウェアにおける)は、FTLS と一致していることをインフォーマルに示さなければならない。
  FTLS の要素は、TCB の要素と一致することをインフォーマルな技法を用いて示されなければならない。
  FTLS は、セキュリティポリシーを満たすために必要とされている統合された保護メカニズムを表現しなければならず、それは TCB の要素に対応付けられたこの保護メカニズムの要素である。
* フォーマルな分析技法を用いて隠れチャネルを識別し、解析しなければならない。
  インフォーマル技法を用いて、隠れタイミングチャネルを識別してもよい。
  システム中に識別される隠れチャネルの継続的な存続は正当化されなければならない。

クラス(A1)中のシステムに要求される TCB の詳細な設計と開発分析とを合わせて、より厳格な構成管理が必要とされ､安全にシステムを現場に配備するための手続が確立される。
システムセキュリティ管理者を配置する。

以下はクラス(A1)格付けを割り当てられたシステムのための最小の要件である。

4.1.1 セキュリティポリシー

4.1.1.1 任意 (自由裁量的) アクセス制御

4.1.1 セキュリティポリシー

4.1.1.1 任意(自由裁量的)アクセス制御

TCB は自動データ処理（ADP）システムの中で名称を付されているユーザと名称を付されているオブジェクト(例えばファイルとプログラム)の間のアクセスを定義し、制御しなければならない。

強制メカニズム(例えばアクセス制御リスト)は、ユーザがそれらのオブジェクトの共有を指定し制御することを可能にし、そしてアクセス権の伝播を制限するためのコントロール

を提供しなければならない。
任意（自由裁量)アクセス制御の機構は、明示的なユーザの行為によって、又はデフォルトで、オブジェクトを不正アクセスから保護しなければならない。
これらのアクセス制御は、名称を付された各オブジェクトのために、そのオブジェクトへのアクセスのそれぞれのモードにより、名称を付された個人のリストと名称を付された個人のグループのリストを指定することを可能とする。
さらに、そのような名称を付された各オブジェクトのために、オブジェクトへのいかなるアクセスも与えられない名称を付された個人のリストと名称を付された個人のグループのリストを指定することを可能とする。
未だアクセス権限を有していないユーザによるオブジェクトへのアクセス権限は許可されたユーザによってのみ割り当てられなければならない。

4.1.1.2 オブジェクト再使用

ストレージ・オブジェクトの中に含まれている情報へのすべての付与権限は、TCB の未使用のストレージ・オブジェクトのプールからのサブジェクトの初期の割り当て、配分、または再配分に先がけて無効にすべきである。
情報の暗号化された表現も含めて、サブジェクトの事前の動作によって生成されるいかなる情報も、システムに後にリリースされたオブジェクトへのアクセス権を獲得するいかなるサブジェクトに対して、利用可能であってはならない。

4.1.1.3 ラベル

TCB 外のサブジェクトによって、直接または間接的にアクセス可能な各々の自動データ処理（ADP）システムリソース（例えば、サブジェクト、ストレージ・オブジェクト、ROM）に付されている機密ラベルは、TCB により維持されなければならない 。
これらのラベルは強制アクセス制御の決定のための基盤として使われなければならない。
ラベルのないデータをインポートするために、TCB はそのデータのセキュリティレベルを許可されたユーザに要求し、それを受け取る、このようなすべての動作は TCB によって監査可能でなければならない。

4.1.1.3.1 ラベルの完全性

機密ラベルは、それらが関連する特定のサブジェクトまたはオブジェクトのセキュリティレベルを正確に表さなければならない。
TCB によってエクスポートされる時に、機密ラベルは内部ラベルを正確にかつ明確に表すこととし、エクスポートされようとしている情報に付随されなければならない。

4.1.1.3.2 ラベルを有する情報のエクスポート

TCB は、個々の通信チャネルと I/O 装置を単一レベルまたはマルチレベルで指定しなければならない。
この指定におけるどのような変更も手動でされることとし、TCB により監査可能でなけれ

ばならない。
TCB は、通信チャネルまたは I/O 装置に関連するセキュリティレベルまたはレベルにおけるどのような変化も保持し監査が可能でなければならない。

4.1.1.3.2.1 マルチレベル装置へのエクスポート

TCB がオブジェクトをマルチレベルの I/O 装置にエクスポートする場合、そのオブジェクトに付随する機密ラベルもまたエクスポートされなければならず、エクスポートされた情報と同様に物理メディア上に同じ様式で存在しなければならない（すなわち、機械が可読または人間が可読な様式で）。
TCB がマルチレベルの通信チャネルを介してオブジェクトをエクスポートあるいはインポートする時は、そのチャネル上で使われるプロトコルは、機密ラベルと、送信あるいは受信される対象の情報との間が明白な対になるよう規定しなければならない。

4.1.1.3.2.2 単一レベルの装置へのエクスポート

単一レベルの I/O 装置と単一レベルの通信チャネルは、それらが処理する情報の機密ラベルを維持する必要はない。
しかしながら、TCB は、単一レベルの通信チャネルまたは I/O 装置を介してインポートあるいはエクスポートされる情報の単一のセキュリティレベルを確保するために、TCB と許可されたユーザが信頼して通信するメカニズムを含まなければならない。

4.1.1.3.2.3 人間に可読な出力へのラベル

自動データ処理（ADP）システムの管理者は、出力される機密ラベルに対応する印刷可能なラベル名を特定することができること。
TCB は、人間に可読でページ付けされている全てのハードコピー出力(例えばラインプリンタ出力)の始めと終わりに、その出力の機密度を正確に*表現する人間に可読な機密ラベルをマークしなければならない。
TCB はデフォルトで、ハードコピー出力(例えばラインプリンタ出力)の各ページの上部と下部に、その出力の全体的な機密度を正確に*表現する、あるいはそのページ上の情報の機密度を正確に*表現する、人間に可読な機密ラベルをマークしなければならない。
TCB はデフォルトで、そして適切な方法により、人間に可読な他の様式の出力（例えば、マップ、グラフィックス）に、その出力の機密度を正確に*表現する、人間に可読な機密ラベルをマークしなければならない。
これらのデフォルトのマーキングに対する、いかなる書換えは TCB により監査可能としなければならない。

*人間に可読な機密ラベルの階層区分の構成要素は、そのラベルが関係する出力内の、いかなる情報の階層区分において最大に等しいこととする；階層的でないカテゴリの構成要素はそのラベルが関係する出力内の情報の全ての階層的でないカテゴリを含み、他の階層的でないカテゴリを含まないこととする。

4.1.1.3.3 サブジェクトの機密ラベル

TCB は対話型セッション中、端末ユーザに、そのユーザに関連したセキュリティレベルの各変化をただちに通知しなければならない。
端末ユーザは、TCB に対してそのサブジェクトの完全な機密ラベルを必要に応じて表示するよう問い合わせることができなければならない。

4.1.1.3.4 装置ラベル

TCB は、装着している全ての物理的な装置に、最小と最大のセキュリティレベルを割り当てることをサポートしなければならない。
これらのセキュリティレベルは、装置が設置される物理的環境により課せられる制約事項を守るために TCB により使われる。

4.1.1.4 強制(的)アクセス制御

TCB は、TCB の外のサブジェクトによって直接または間接的にアクセス可能なすべてのリソース(すなわちサブジェクト、ストレージ・オブジェクト、および I/O 装置)上で強制アクセス制御のポリシーを実施しなければならない。
これらのサブジェクトとオブジェクトは、階層的な機密度区分レベルと階層的でないカテゴリーとの組み合わせである機密ラベルを割り当てられることとし、そのラベルは強制アクセス制御の決定のための基礎として使われなければならない。
TCB は、ふたつ以上のそのようなセキュリティレベルをサポートすることができることとする。(強制アクセス制御ガイドラインを参照。)
以下の要求事項は、TCB の外のすべてのサブジェクトと、これらのサブジェクトによる直接または間接的にアクセス可能なすべてのオブジェクトとの間のすべてのアクセスにあてはまることとする：サブジェクトのセキュリティレベルにおける階層区分が、オブジェクトのセキュリティレベルにおける階層区分より大きいかあるいは等しく、そして、サブジェクトのセキュリティレベルにおける階層的でないカテゴリがオブジェクトのセキュリティレベルの階層的でないカテゴリの全てを含むならば、サブジェクトはオブジェクトを読むことができる。
サブジェクトのセキュリティレベルにおける階層区分が、オブジェクトのセキュリティレベルにおける階層区分より小さいかあるいは等しく、そして、サブジェクトのセキュリティレベルにおける階層的でないカテゴリの全てがオブジェクトのセキュリティレベルにおける階層的でないカテゴリに含まれるならば、サブジェクトはオブジェクトに書くことができる。
識別と認証のデータは、ユーザの本人性を認証するために、そしてまた、個々のユーザのために動作するよう作成される TCB 外のサブジェクトのセキュリティレベルと認可がそのユーザのクリアランスと認可によって支配されることを保証するために、TCB により使われなければならない。

4.1.2 責任

4.1.2.1 識別と認証

TCB は、自身が仲介を期待されるあらゆる動作について、実行前にユーザが自分自身の身元を明らかにするようユーザに要求しなければならない。
さらに、TCB は個々のユーザのクリアランスと承認を決定するための情報と同様に個々のユーザ(例えば、パスワード)の真正性（identity）を確認するための情報を含む認証データを維持しなければければならない。
このデータは、ユーザの正当性を認証し、そのユーザのクリアランスおよび認証によって、個々のユーザの代りに作用するかもしれない TCB 外のサブジェクトのセキュリティレベルおよび権限付与を保証するために、TCB によって使用されるものでなければならない。
いかなる無許可ユーザも認証データにアクセスできないように、TCB は認証データを保護しなければならない。TCB は、それぞれ個々の自動データ処理（ADP）システムユーザの独自の正当性を識別する能力を提供することによって、個々の責任能力を強化できるものでなければならない。また、TCB はこの正当性をその個人によって講じられたすべての監査可能な行動に関連づける能力を提供するものでなければならない。

4.1.2.1.1 トラステッドパス

TCB とユーザの間において積極的な接続(例：ログイン、サブジェクトのセキュリティレベル変更)が必要である際に、TCB は自らとユーザとの間でトラステッドパスをサポートするものでなければならない。このトラステッドパスは TCB によって活性化するものとし、他の経路から誤りなく区別可能でなければならない。

4.1.2.2 監査

TCB は、それが保護するオブジェクトに対するアクセスの監査証跡を作成し、維持し、変更、権限のないアクセスまたは破壊から保護することができるものでなければならない。
監査データへの読み取りアクセスが認可済みの人々に制限されるよう、監査データは TCB によって保護されなければならない。
TCB は次のタイプのイベントを記録できなければならない。すなわち、識別と認証メカニズムの使用、ユーザのアドレス空間へのオブジェクトの導入（例：ファイルのオープン、プログラムの開始）、オブジェクトの削除、およびコンピュータオペレータならびにシステム管理者(またはシステムセキュリティ管理責任者<オフィサー>)によって講じられた処置、および他のセキュリティ関連イベント。
また、TCB は人間が判読可能な出力の記録に対するあらゆる無効化についても監査できなければならない。それぞれの記録されたイベントに関しては、監査記録は以下を特定するものとする：イベントの発生日時、ユーザ、イベントのタイプおよびイベントの成功もしくは失敗について。識別/認証イベントのために、リクエスト(例えばターミナルの ID)の出所が監査記録に含まれていなければならない。
ユーザのアドレス空間へオブジェクトを導入するイベント、およびオブジェクト削除イベントのために、監査記録はオブジェクト名およびオブジェクトのセキュリティレベルを含んでいなければならない。

自動データ処理（ADP）システム管理者は、個々の身元および正当性そして/またはオブジェクトのセキュリティレベルに基づき、任意の一人または複数ユーザの行動を選択的に監査できなければならない。
TCB は隠れ記憶チャネルの利用時に使用されるかもしれない識別されたイベントを監査することができなければならない。TCB は、セキュリティポリシーへの切迫した妨害を示す可能性のある、セキュリティ監査すべき出来事の発生か累積をモニターできるメカニズムを含むものでなければならない。しきい値を超過した場合、このメカニズムはセキュリティ管理者に直ちに通知することができなければならず、かつ事件の発生もしくは、これらセキュリティ関連イベントが継続して累積された際に、システムはイベントを終了するために最も破壊性の低い処置を講ずるものでなければならない。

4.1.3 保証

4.1.3.1 操作上の保証

4.1.3.1.1 システムアーキテクチャ

TCB は外部からの妨害または改ざん(例：コードもしくはデータ構造の変更などの)から自身の保護を実行するためにドメインを維持するものでなければならない。
TCB は、その制御下において別個のアドレス空間を提供することを通じてプロセスの隔離を維持しなければならない。
TCB は明確に定義された十分独立性のあるモジュールへと向けて、内部的に構造化されなければならない。
TCB は、保護の危機にないエレメントから危機にあるエレメントを分離するために可能なハードウェアの使用を効果的にさせなければならない。
TCB モジュールは、最少特権の原則が強化されるように設計されなければならない。
セグメント化のようなハードウェアの機能（Features）は、個別の属性（すなわち： 読込可能、書き込み可能）を備えた論理上別個のストレージ・オブジェクトを支援するのに使用されなければならない。
TCB へのユーザインタフェースは完全に定義されなければならない。また、TCB の要素はすべて識別されなければならない。
TCB は正確に定義された意味論を備えた完全な、概念的に単純な保護メカニズムを使用するために設計され、組み立てられるものでなければならない。
このメカニズムは、TCB およびシステムの内部構造を強化する際に中心的な役割を果たさなければならない。
TCB は、レイヤ化、抽象化およびデータ隠蔽という重要な効用を組込まなければならない。重要なシステム工学は、TCB の複雑さを最小限にし、保護の危機にない TCB モジュールを除くように指向しなければならない。

4.1.3.1.2 システムの完全性（Integrity）

ハードウェアおよび(または)ソフトウェアの機能（features）は、TCB の実地におけるハ

ードウェアおよびファームウェア要素の正確なオペレーションを定期的に確認するために使用できるように備えられなければならない。

4.1.3.1.3 隠れチャネルの分析

システム開発者は、隠れチャネルを徹底的に調査して、識別された各チャンネルの最大の帯域幅を実測、または工学的判断のいずれかによって決定しなければならない。
（隠れチャネルガイドラインの節を参照。)
分析には、フォーマルメソッドが使用されなければならない。

4.1.3.1.4 信頼できる設備管理

TCB は、オペレータと管理機能の分離をサポートしなければならない。セキュリティ管理者の役割の下で実行される機能は、それ以外の機能と区別されなければならない。ADP システムの管理要員は、対象となる ADP システム上でセキュリティ管理者の役割を確立するための明確な監査可能行動を取った場合にのみ、セキュリティ管理機能を実行できるようにすべきである。セキュリティ管理の役割内で実行される非セキュリティ機能は、効率的なセキュリティの役割遂行に必要なもののみに制限さればければならない。

4.1.3.1.5 信頼できる復旧

ADP システムの故障もしくは他の障害に対して、故障前のシステム保護水準を維持した状態で復旧できることを保証するための手続きや機構が提供されなければならない。

4.1.3.2 ライフサイクル上の保証

4.1.3.2.1 セキュリティ試験

ADP システムのセキュリティ機構は、システムドキュメントにおいて必須機構として機能するように考え、試験されなければならない。設計ドキュメント、ソースコード、および、オブジェクトコードは、TCB の実装を完全に理解する要員から構成されるチームの管理下に置かれなければならない。これは、完全なテストと解析のためである。試験の目的は 2 つある。第 1 に、TCB 外のサブジェクトが、TCB によって強制されるセキュリティポリシーにより、強制的にもしくは任意でアクセス禁止されているデータの閲覧、変更、削除を許すような設計上の欠陥および実装上の結果をすべて発見することである。第 2 に、他のユーザにより確立された通信に対してレスポンスできないような状態に TCB を追い込むことが可能な（未認証）サブジェクトが存在しえないことを保証することである。TCB は、侵入に対する砦として考える。発見された欠陥はすべて修正され、確認のために TCB の再検査が行われなければならない。この再検査の目的は、発見された欠陥が排除され、新たな欠陥を生み出していないことを確認するためである。検査により、TCB の実装が FTLS に対して矛盾がないことを明らかにしなければならない（セキュリティ検査ガイドラインを参照)。設計上の欠陥、修正可能な実装上の欠陥のいくつかはテスト中に発見されないかもしれないが、そのような欠陥はほとんど残っていないという妥当な信頼をおくこととする。マニュアルもしくは FTLS からソースコードへのマッピングを侵入試験の基礎

としてもよい。

4.1.3.2.2 設計仕様と検査

TCB によってサポートされるセキュリティポリシーのフォーマルモデルは、ADP システムのライフサイクル期間中保持され続けなければならない。ADP システムのライフサイクル期間は、その原理に対して矛盾がないことを維持しなければならない。TCB の DTSL は、例外、エラーメッセージ、影響の点に関して TCB を完全に、かつ正確に説明するために保持されなければならない。TCB の FTLS は、例外、エラーメッセージ、影響に関して TCB を完全に説明するために保持されなければならばい。TCB インタフェースにおいて DTLS および FTLS に関するプロパティを確認することができる場合、DTLS と FTLS は、ハードウェアもしくはファームウェアとして実装された TCB コンポーネントを含まなければならない。DTLS がモデルに対して矛盾がないということに対する説得力のある論拠が与えられなければならない。また、FTLS がモデルに対して矛盾がないということを示すためのフォーマルおよびインフォーマル技術の組み合わせに対しても、DTLS が矛盾していないことを示す論拠が与えられなければならない。この検査証書は、特定のコンピュータセキュリティ機関によって承認されたフォーマル仕様と最新技術による検査システム内で提供されるそれと矛盾がないこととする。正確な情報の証拠を提供するために、マニュアルもしくは FTLS の TCB ソースコードへのマッピングが実施されなければらならない。

4.1.3.2.3 設定管理

設計、開発、運用を含む TCB のすべての段階において、あらゆるところに設定管理システムを配置しなければならない。配置対象は、すべてのセキュリティ関連ハードウェア、ファームウェア、フォーマルモデルの変更操作を保持するソフトウェア、記述的 FTLS、その他の設計データ、実装ドキュメント、ソースコード、実行可能オブジェクトコード、テスト関連物とドキュメントに及ぶ。設定管理システムは、TCB 現バージョンに関連するすべてのドキュメントとコードの間の一貫したマッピングを保証しなければならない。加えて、ソースコードからの TCB の新しいバージョンを生成するための専用ツールが提供されなければならない。また、このツールを用いて TCB 前バージョンと新バージョンを比較することで、新バージョンで使われるコード中の新たに変更された部分を特定することができ、厳格な設定操作下に保持されることを可能にしなければならない。マスターコピー、もしくは、TCB の生成に使われたすべてのマテリアルのコピーを未承認の変更や破壊から保護するために技術的、物理的、手続き的な幾重ものセーフガードを設定しなければならない。

4.1.3.2.4 信頼できる配布

信頼できる ADP のシステム制御と設備配布は、TCB の現在の版を示すマスタデータと現在の版のコードのオンサイトマスタコピーの間のマッピングの完全性を維持するために提供されなければならない。

顧客に配布された TCB ソフトウェア、ファームウェア、およびハードウェアの更新が、マスタコピーによって規定された正にそのとおりであることを保証するための手続(例えば現場でのセキュリティ承認検査)が存在しなければならない。

4.1.4 証拠資料

4.1.4.1 セキュリティ機能のユーザガイド

ユーザ向け文書の証拠資料の中に含まれる 1 つの要約、章、またはマニュアルは、TCB が提供する保護機構、それらの使用時のガイドライン、及びそれらが互いにどのように作用するかを説明しなければならない。

4.1.4.2 信頼できる設備マニュアル

自動データ処理（ADP）システム管理者向けのマニュアルは、セキュア設備を使用する時に制御されるべき機能と特権について警告を示さなければならない。
各タイプの監査イベントの詳細な監査記録構造と同じく監査ファイルを検査し、維持するための手続が与えられなければならない。
マニュアルは、利用者のセキュリティ特性を変更することを含めオペレータと管理者のセキュリティ関連機能を説明しなければならない。
システムの保護機能の一貫した効率的な利用、その機能がどのように相互に作用するか、安全に新しい TCB をどのように生成するか、そして安全な方法で設備を運営するために制御される必要のある設備の手続や警告、特権に関するガイドラインをマニュアルは提供しなければならない。
リファレンス検証機構を含んでいる TCB モジュールが明確にされなければならない。
TCB 内の任意のモジュールの修正後の新しい TCB のソースからの安全な生成の手続きが示されなければならない。
システムが安全な方法で起動されると保証する手続をマニュアルは含まなければならない。また、システム操作のいかなる経過の後の安全なシステム操作を再開する手続が含まなければならない。

4.1.4.3 検査証拠資料

検査計画、セキュリティ機構がどのように検査されたかを示す検査手続、及びセキュリティ機構の機能的な検査結果を説明する証拠資料をシステム開発者は評価者に提供しなければならない。
本証拠資料は、隠れチャネルのバンド幅を減らすために使われた方法の有効性を検査した結果を含まなければならない。
フォーマルな最上位仕様と TCB ソースコードの間のマッピングの結果が与えなければならない。

4.1.4.4 設計証拠文書

製造者の保護の哲学の記載とこの哲学が TCB にどう翻訳されたかの説明を与える証拠文

書が入手可能でなければならない。TCB モジュール間のインタフェースが説明されなければならない。
TCB が強制するセキュリティポリシーモデルのフォーマルな記述が入手可能であり、
そのセキュリティポリシーを強制するのに十分であることを証明しなければならない。
具体的な TCB 保護機構が明らかにされ、さらにその機構がモデルを満足することを示す説明が与えられなければならない。
記述的な最高位仕様(DTLS)は、TCB インタフェースの正確な記述であると示されなければならない。
TCB がリファレンスモニタの概念をどのように実装するか記述し、それがなぜ耐タンパであること、バイパスされないこと、そして正しく実装されていることの説明を証拠文書は与えなければならない。
TCB の実装(すなわちハードウェア、ファームウェア、およびソフトウェア)は、フォーマルな最上位仕様(FTLS)と一致しているとインフォーマルに示されなければならない。
FTLS の要素は TCB の要素と対応することをインフォーマルなテクニックを使って示されなければならない。
検査を容易にし、最少権限を強制するために、TCB がどのように構造化されるかを証拠文書は記述しなければならない。
さらに、隠れチャネル分析の結果とチャネルを制限することに関係しているトレードオフを証拠文書は示さなければならない。
知られている隠れストレージチャネルとして悪用されるかもしれない全ての監査できるイベントは明らかにされなければならない。
(隠れチャネルガイドラインセクションを参照)FTLS において扱われないが、厳に TCB 内部のハードウェア、ファームウェア、およびソフトウェアの機構(例えばマッピングレジスター、直接的なメモリーアクセス I/O)は、明確に説明されなければならない。

4.2 クラス(A1)超

クラス(A1)のシステムが既に与える以上の機能や保証を与えるシステムに予想されるセキュリティの拡張の多くは、現在の技術の域を超えている。
以下の議論は将来の作業を誘導することを意図していて、公共と民間部門の両方において既に進んでいる研究開発活動から引き出された。
より多くの、より良い分析技術が開発されるにつれ、これらのシステムのための要件はより明示的になるだろう。
将来、フォーマルな検証の利用はソースレベルに拡がるだろうし、隠れタイミングチャンネルはより完全に扱われるだろう。
このレベルでは、設計環境は重要になり、検査はフォーマル最高位仕様の解析によって支援されるだろう。
TCB 開発に使われるツール(例えば、コンパイラ、アセンブラ、ローダ)の正確性や TCB が動くハードウェア/ファームウェアの正しい動作への考察が進むだろう。
クラス(A1)を越えるシステムによって扱われるエリアは以下を含む：

*** システムアーキテクチャ**
リファレンスモニターの自己防衛と完全性の要件が TCB に実装されていることを論証(フォーマルまたは別手段で)しなければならない。

*** セキュリティ検査**
現在の最新技術を越える、いくつかの検査事例がフォーマル最高位仕様またはフォーマル低位仕様から自動的に生成されることが予想される。

*** フォーマル仕様と検証**
実現可能でフォーマルな検証の方法を使って、TCB はソースコードレベルまで検証されなければならない。オペレーティングシステムのセキュリティに関連する部分のソースコードのフォーマルな検証は、難しい仕事であると判明している。
2 つの重要な考慮点は、意味論が完全にフォーマルに表現できる上位言語の選択、及び抽象的なフォーマルな設計から低位仕様での実装の形式化への連続した段階を通じた慎重なマッピングである。
最低位仕様が実際のコードと密接に対応している場合に、コードの証明が首尾よく達成できると、経験が示している。

*** 信頼できるデザイン環境**
TCB は、信頼できる施設を使い、信頼できる(許可された)人員のみにより設計されなければならない。

パート II：理論的根拠とガイドライン

5.0 トラステッド・コンピュータ・システムの制御目標

トラステッド・コンピュータ・システムのための制御目標基準は、要件毎にグループ化されたクラスで分類されている。
これらのグループ分けは、コンピュータセキュリティのための 3 つの基本的制御目標が満足され、そして見落としがないことを保証するために創り出したものである。

これらの制御目標では次の点について論ずる：
* セキュリティポリシー
*責任遡及性
* 保証
このセクションでは、信頼できるシステムを設計する観点から、一般的な制御目標とそれらの密接な関係について論ずる。

5.1 合意の必要性

DoD コンピュータセキュリティセンターの主な目標は、コンピュータ産業がトラステッド・コンピュータ・システムおよび製品が商業市場において広く利用されるよう、コンピュータ産業に対しそれらの開発を奨励することである。この目標を達成するためには、そのような製品を必要とし、また要求する公共と民間部門の両方から認知され、そして、意見が表明されることが必要である。

この文書の序章で書いたように、国家安全保障局が使用する金融、医療、及び職員の情報など他の機密データと同様、国家の機密情報の取り扱いに関わる問題を定義し解決する方法を開発する取り組みは、何年もの間、続いている。
パート I で書いたように、基準は、これらの取り組みの到達点を表し、そしてトラステッド・コンピュータ・システム構築のための基本要件を記述している。しかしながら、今日まで、これらのシステムは国家安全保障の必要性のみを満たすだけのものであると、多くの人々に考えられてきた。この認識が続くということは信頼のおけるシステムの製造を動機付ける為に必要なコンセンサスが欠けていると言える。

このセクションの目的は、基本的な制御目標を詳細に記述することにある。これらの目標は、基準では要件のアウトラインとしての基礎を示している。目標は国家安全保障局以外のものが、それらの一般性、そしてさらに拡大して、国家安全保障のため、あるいは、民間のためであろうと全ての種類の取り扱いに注意が必要なアプリケーションを処理するための基準となる要件として一般的に適用可能であることが評価可能となるように、その基礎を説明することにある。

5.2 定義と有用性

「制御目標」という用語は、組織の資源、又は、プロセス、あるいは、その両者に関するいくつかの状況を管理するという意図の表明を指す。コンピュータシステム用語での「制御目標」は、与えられたあらゆるシステムへの一連のセキュリティ要件を遂行するための戦略を策定するフレームワークを提供するものである。
機密データの管理や手続が妥協を予防するための必要性や、あるいは不正を発見するための説明責任を提供するための必要性といった一般的な脆弱性に対応するため開発されたが、「制御目標」は、セキュリティ目標を表現するための有効な手段として認識されるようになった。[3]
制御目標の例には、セクション 6 で述べた、リファレンスモニター・コンセプトの実装における 3 つの基本設計要件が含まれる。それらは：

* リファレンス検証メカニズムは、改ざんできない構造(タンパープルーフ)でなければならない。
* リファレンス検証メカニズムは、常に、呼び出されなければならない。
* リファレンス検証メカニズムは、その完全性を保証できるよう、解析やテストの対象として、十分小さくなければならない。[1]

5.3 制御目標基準

基準の 3 つの基本制御目標は、セキュリティポリシー、責任遡及性、そして、保証、に関係する。このセクションの残りでは、これら基本的な要件について述べる。

5.3.1 セキュリティポリシー

最も一般的な意味では、コンピュータセキュリティは、コンピュータがどのように使用されるかを制御することである。すなわち、コンピュータにより処理される情報がいかにアクセスされ扱われるかを制御することである。しかし、さらに緻密に調査すると、コンピュータセキュリティは、FIPS PUB 39、コンピュータシステムセキュリティ用語集などで参照されるが、コンピュータ・セキュリティとして唯一の定義は存在しない。[16]その代わりに､ADP システムのセキュリティ､制御に関するセキュリティ､データセキュリティ、その他からなる、11 個のセキュリティ定義が存在する。これらの定義についての共通の話題は､「保護」という言葉である。さらに、保護要件の宣言は、国防総省指令 5200.28 で見つけることができる。それには､「機密分類されたデータを処理、保存あるいは使用し、機密分類された情報を生成するシステムは、処理、記憶、あるいは、機密データの利用、機密情報を作りだすシステムについて、a.権限の無い人間による機密資料への故意の、または、不注意なアクセスと、b.コンピュータとその周辺機器に対する権限の無い操作の両方を、合理的な信頼性に基づき防止することを保証する」という、機密分類されたデータの保護に関し容認可能なレベルを記述している。[8]
要約すると、保護要件は、認識されている脅威とリスク、そして、組織の目標という点から定義されなければならない。これは、しばしば、セキュリティポリシーという言葉で述べられる。情報へのアクセスで何が許可されるかを決めるのは、コンピュータの利用とは

無関係に、外部の法律、規則/慣例、条例などであると、その他の文献で指摘している。
特に、一定のシステムでは、特定のポリシーを強制することによってのみ、安全であるとされている。[30]このような、セキュリティポリシーに関する制御目標は、以下のとおりである。

セキュリティポリシー・制御目標
セキュリティポリシーとして知られている、アクセスについての制御と、情報の配布に関する意図の声明は、正確に定義され、機密情報を処理するために使われる各システムにおいて実装されなければならない。
セキュリティポリシーは、由来する法律、規則/慣例、一般的な政策を正確に反映していなければならない。

5.3.1.1 強制(的)アクセス制御
機密に分類された、あるいは、特定の目的で指定された機密情報の管理に適用すべく開発されたセキュリティポリシーには、情報のライフサイクルを通して、その情報をいかに取り扱うかについての詳細なルールが含まれていなければならない。
これらのルールは、その情報が想定できる様々な機密指定、及び、そのシステムがサポートする様々なアクセスの形態を示す役割がある。
強制的セキュリティは、個々の機密情報アクセス資格／権限、情報の機密レベル指定、そして調停されるアクセスの形式の比較に基づいて、アクセス主体による情報へのアクセスに制約を加える一連のアクセス制御ルールを実施することを指す。
強制ポリシーは、要求するものであったり、あるいは、部分的に順序指定を強制できるシステムによって満足させられる。すなわち、その指定は、数学的に"束構造"として知られているもので形作る必要がある。

上記で明らかに推測されることは、機密データに関連する指定は任意に変更できないことをシステムが保証しなければならない。ということである。任意に変更してしまうと、機密情報へアクセスするための適切な権限を持たない個人にも許可を与えることになるためである。
さらにデータの機密レベルを下げることが許可されない限り、より低いレベルの機密指定で保存できないよう、システムが情報の流れを制御することも要件として推測される。

強制(的)セキュリティ管理目標
機密分類された、あるいは、特定の目的で指定された機密情報を処理するため利用されるシステムのため定義されたセキュリティポリシーには、強制アクセス制御のルールの実施のための条項が含まれなければならない。
すなわち、セキュリティポリシーには、直接的には、個々の機密情報アクセス権、あるいは、要求されている情報の機密分類あるいは機密レベル指定の比較に基づいて、そして、間接的には、物理的、及び、他の環境コントロール要因を考慮し、アクセスを制御する一

連のルールを含まなければならない。
強制アクセス制御のルールは、由来となっている法律、規則/慣例、一般的な政策を正確に反映していなければならない。

5.3.1.2 任意(自由裁量)によるセキュリティポリシー

任意（自由裁量)によるセキュリティは、今日のコンピュータシステムにおける主要なアクセス制御方式のひとつである。この種のセキュリティの基礎は、個人ユーザまたはユーザプログラムが、制御下にある情報に対するアクセス制御設定を行うことを認めることである。任意（自由裁量)によるセキュリティが強制的セキュリティと異なる点は、アクセス制御ポリシー設定が、個人の知る必要性（Need-to-Know）に基づいていることである。対して、強制アクセス制御におけるアクセス制御ポリシー設定は、情報の機密区分や機密の指定に基づく。
任意（自由裁量)アクセス制御は、強制アクセス制御の代用とはならない。(米国国防総省のように）情報が機密区分されている環境では、任意（自由裁量)によるセキュリティは強制アクセス制御ポリシーによる全体的規制に加えて、更にきめ細かいアクセス制御を提供するために用いられる。機密情報へのアクセスを許すには、その前提条件として、双方のタイプの制御方式を効果的に導入する必要がある。
一般に、以下の(a)および(b)の両方を満たす場合のみ、機密情報にアクセスすることができる。
(a)アクセスを行うユーザが、信頼できると判定されていること。すなわち、要員として機密情報アクセス資格を与えられた人である。これは、MANDATORY（強制）に関連する。
(b)そのアクセスが、業務の遂行に必要である。すなわち、そのアクセスが、知る必要性に基づいていることである。DISCRETIONARY（任意（自由裁量))に関連する。
言い換えると、任意（自由裁量)によるアクセス制御は、現にどのユーザに対して許可しても差し支えないアクセスの決定を個人の任意（自由裁量)とすることで、強制的ポリシーの制約に優先して矛盾なく機能する。

任意（自由裁量)セキュリティ制御目標：

機密情報、または、取扱注意情報を処理するシステムに対して設定されたセキュリティポリシーは､任意(自由裁量)アクセス制御規則の実施条項を含まなければならない｡つまり、セキュリティポリシーは、情報が必要であると判定された人を識別することによりアクセスを制御し制限するための一貫したルール集を含まなければならない。

5.3.1.3 マーキング

強制的セキュリティポリシーの効果をあげる一連のメカニズムの導入には、システムによって適切な機密区分もしくは機密ラベルを情報にマークし、情報がシステム内で移動するにつれてこれらのマーキングを保守する必要がある。情報に一貫性があり、かつ、正しくマークされていれば、強制アクセス制御のルールに基づいくマークの比較は、正確かつ一

貫して行われる。

システムが機密区分や機密ラベルを内部に持つことにより、システムの出力に対して正しいラベル付けを自動的に行うという付加的機能が備わる。システムによってラベルの正確性と完全性が維持される限り、システムからの出力は正しく存続される。

マーキング制御目標：
強制的セキュリティポリシーを実施するように設計されたシステムは、すべての情報のために、機密区分またはその他の機密ラベルの完全性を記憶し維持しなければならない。システムからエクスポートされたラベルは、エクスポートされた対応する内部の機密ラベルを正確に表現するものでなければならない。

5.3.2 説明責任

第 2 の基本的制御対象はセキュリティの基本原理の一つとして説明責任（アカウンタビリティ）、換言すれば個人のアカウンタビリティを扱うことである。個人のアカウンタビリティは、個人やグループのために情報処理を行うシステムを安全に保ち、制御するときの重要要素である。この目的を果たすために、以下の要件が求められる。

第 1 の要件は、各個人ユーザの ID（識別）のためである。第 2 の要件は、上記の ID を認証するための必要性である。ID は認証と機能上独立している。認証がないユーザ ID は、信頼性がない。信頼できる ID なしでは、正しい認証が行われたことを保証できないため、強制もしくは任意（自由裁量)の何れの方式でも、セキュリティポリシーを適正に実施することはできない。

第 3 の要件は、信頼できる監査能力についてである。すなわち、トラステッド・コンピュータ・システムでは、監査できる能力のある正当な要員に、以下の行為を監査する能力を付与していなければならない。その行為とは、潜在的に機密情報あるいは取扱注意情報にアクセスする可能性のある行為、またはその情報を流出させる行為である。監査データは、特定のインストレーションやアプリケーションの監査の必要性に基づいて、得られる監査情報のなかから選択的に作成する。しかしながら、監査イベントからその行為を誰が行ったのか誰の利益のために行われたのか、具体的な個々ユーザの行動を追跡し特定するのをサポートするのに、監査データは十分な粒度を保たなければならない。
機密情報や機密情報の世代保存版やリリース版に対して、潜在的にアクセスの可能性のあるどんな行為も監査できる能力を備えていると認められた人に提供すべきである

説明責任制御の目的：
極秘情報や取扱注意情報の処理や操作を担うシステムでは、強制もしくは任意（自由裁量)によるセキュリティポリシーが行使されるときは、いつでも個人のアカウンタビリティを保障しなければならない。さらに、アカウンタビリティを保障するためには、資格をもっ

た有能な担当者が、妥当な時間内に安全かつ確実な方法でアカウンタビリティ情報にアクセスし、評価する能力がなければならない。

5.3.3 保証

第 3 の基本的制御対象は、セキュリティポリシーが極めて正確に実装され、システムの保護関連要素がポリシーの意図を正確に仲介して実施していることの保証または提供に関係している。したがって、保証は、システム内の信頼される箇所が意図した通り動作することを含まなければならない。これらの目的を達成するために、ライフサイクル上の保証と操作上の保証の 2 種類の保証が必要とされる。

ライフサイクル上の保証は､定式化された厳密な操作と標準仕様に沿ってシステムの設計、開発、保守が行われるように強制するためのステップとして参照される[17]。

機密情報を保管・処理するコンピュータシステムは、その情報を保護するためのソフトウェアやハードウェアに依存する。つまり、それらソフトウェアやハードウェア自身が、保護機構の誤動作やバイパスを作るような未承認変更から保護されなければならないことを意味する。この理由から、トラステッド・コンピュータ・システムは、設計・開発段階で慎重に評価し、テストされなければならない。そして、保護機構に悪影響を及ぼすかもしれないシステム変更を行った時は、再評価しなければならない。

この方法のみが、ハードウェアやソフトウェアによるセキュリティポリシーの解釈実行が正しく行われていることを確証を与える。ライフサイクル上の保証が、システムの設計、開発、保守の管理・保守に関係するのに対し、操作上の保証はセキュリティポリシーの厳格な実施のためのシステム・アーキテクチャやシステム機能に焦点を置いている。すなわち、セキュリティポリシーは、システムのハードウェアとソフトウェアの保護機能に組み込まれなければならない。この種の信頼性を提供するためにとられる手段の例として、以下のものがある：正しい操作を行うためのハードウェアとソフトウェアの検査法、保護に必要な危険コードの分離、個別のドメインを提供するためのハードウェアやソフトウェアの使用。

保証制御の目的：

機密情報や取扱注意情報を処理し、操作するシステムは、セキュリティポリシーの解釈が正確に行われ、そのポリシーの意図が歪められていないことを保証するよう設計されていなければならない。保証はシステムのライフサイクルを通じて記録されているポリシーの正確なインプリメンテーションとオペレーションに与えるべきである。

ライフサイクル上の保証が、システムの設計、開発、保守の管理・保守に関係するのに対して、操作上の保証は、セキュリティポリシーの厳格な実施のためのシステムアーキテクチャやシステム機能に焦点を置いている。すなわち、セキュリティポリシーは、システムのハードウェアとソフトウェアの保護機能に組み込まれなければならないことを意味する。この種の信頼性を提供するためにとられる手段の例として、以下のものが考えられる：正

しい操作を行うためのハードウェアとソフトウェアの検査法、保護に必要な危険コードの分離、明確なドメイン分離を実現するためのハードウェアやソフトウェアの使用。

6.0 評価クラスの理論的根拠

6.1 リファレンスモニター・コンセプト

James P. Anderson & Co. の運営による Computer Security Technology Planning Study は、1972 年 10 月に米国空軍の電子システム部(ESD)のためのレポート(アンダーソンレポート)[1]をまとめた。このレポートの中で「システムのサブジェクトとオブジェクト間の正当なアクセス関係を強制するリファレンスモニター」のコンセプトが導入されている。リファレンスモニター・コンセプトは、マルチレベルのセキュアコンピューティングの機能と制御を提供するすべてのシステムについて、必須の要素であることが示された。

アンダーソンレポートは、リファレンス認証メカニズムの定義を次のように続けている。「リファレンスモニター・コンセプトの実装は、ユーザに対する参照の許可タイプのリストを用いて、すべてのユーザ(プログラム)によるデータまたはプログラムへの参照を認証するものである。」
さらに参照の認証メカニズムを満たすための三つの要件が記述されている：

a. リファレンス認証メカニズムは耐タンパ性を持たなければならない。
b. リファレンス認証メカニズムは常に実行されていなければならない。
c. リファレンス認証メカニズムは分析とテストを行う上で十分に小さくなければならず、完全であることが保証されているべきである。

アンダーソン委員会のコンセプトの有効性は、広範な研究者のレビューと継続的な調査研究活動によって支持された。リファレンス認証メカニズムの初期段階の例はセキュリティカーネルとして知られている。アンダーソンレポートはセキュリティカーネルを「リファレンスモニター・コンセプトを実装するハードウェアとソフトウェアの組み合わせ」と記述している。この文脈の中で、セキュリティカーネルはリファレンスモニターに対する上記の三つの要件を満たさなければならない、としている。

6.2 フォーマル・セキュリティポリシー・モデル

アンダーソンレポートの公表に続いて、セキュリティポリシー要件のフォーマルモデルとセキュリティカーネルとしてポリシーモデルを実装・適用するメカニズムのフォーマルモデルに対して多くの研究が開始された。それらの研究のうち、ESD が後援した Bell と LaPadula のモデル(BLP モデル)の開発、DoD セキュリティポリシーの抽象的形式記述[2]が有名である。数学と集合論を用いて、セキュアな状態の概念、アクセスの基本モデル、そしてサブジェクトがオブジェクトにアクセスする特定モードを許可する規則を、正確に定義している。最終的には、規則がセキュリティ保護の操作であることを証明することで、セキュア状態にあるシステムにおいて、規則によって連続して遷移するアプリケーションが新しい状態へ遷移した結果も、同様にセキュアであることを、この理論が証明した。この理論は、基礎セキュリティ理論として知られている。

サブジェクトはユーザまたは他のサブジェクトの代理として動作する。サブジェクトは、

明確なユーザの代理として生成され、機密の区分に基づいた形式化されたセキュリティレベルを割り当てられる。フォーマル・ポリシーモデルの状態の遷移と不変式は、ユーザのクリアランス、ユーザの代理として行動するいかなるプロセスのフォーマル・セキュリティ・レベル、および任意のプロセスがアクセスに対して特定のモードを獲得することのできるデバイスと他のオブジェクトのフォーマル・セキュリティ・レベルの間で継続する、不変の関係を定義する。
例えば、BLP モデルは、サブジェクトとオブジェクトのフォーマル・セキュリティ・レベル間の関係を定義する。これは現在、"支配関係(dominancerelation)"として知られている。この関係は、読み込みアクセス、読み書きアクセス、書き込みアクセスを含む基本的なアクセスモードのために、サブジェクトとオブジェクトの間で許可されたアクセスを、明示的に定義する。このモデルは、特定のオブジェクトへの読み込みアクセスの許可を制御する単純セキュリティ特性と、特定のオブジェクトへの書き込みアクセスの許可を制御する*-プロパティ(スター・プロパティ)を定義する。
単純セキュリティ特性と*-プロパティは、両方とも、サブジェクトのフォーマル・セキュリティ・レベルとオブジェクトのフォーマル・セキュリティ・レベルの間の支配関係に基づいた強制的なセキュリティを提供する。任意（自由裁量)的なセキュリティプロパティも定義され、それは、特定のサブジェクトが状態遷移に必要なアクセスの特定モードを認証することを必要としている。このモデルは、サブジェクト(ユーザの代理で動作しているプロセス)の扱いにおいて、信頼されたサブジェクト(すなわち、*-プロパティによって、モデルの中で強制されない)と、信頼されないサブジェクト(*-プロパティによって強制される)とを区別している。

BLP モデルは、任意の順序のすべての状態遷移がセキュリティ保護されていることを数学的に立証するための証明方法のモデルを発展させた。*-プロパティが、トロイの木馬攻撃による情報の脆弱性を排除するのに十分であることも示されている。

6.3 トラステッド・コンピューティング・ベース

トラステッド･コンピュータ･システムの広範囲での商用利用の可能性を促進するために、これらの評価基準はセキュリティカーネルが明確に実装されているシステムだけでなく、セキュリティカーネルが実装されていないシステムにも使用できるようにデザインされている。後者の場合は、リファレンス認証メカニズムのサイズや複雑さのため、要件(c)が完全にはサポートされないシステムを含む。これらの評価基準は、セキュリティカーネルやフロントエンドのセキュリティ・フィルター、トラステッド・コンピュータ・システム全体に対して、リファレンスの認証メカニズムを指し示すために、便宜上、トラステッド・コンピューティング・ベースという用語を使用する。

トラステッド・コンピューティング・システムの中心は、トラステッド・コンピューティング・ベース(TCB)であり、セキュリティポリシーと、保護の基本となるオブジェクト(コードとデータ)の分離とを、責任を持ってサポートするシステムのすべての要素を含んでい

る。TCB の範囲は、いくつかのコンピュータセキュリティの文献に見られる「セキュリティの範囲」と同様である。保護を理解し維持していくためには、TCB は、実行すべき機能と密接に結びつき、可能な限り単純であるべきである。要するに、TCB は、保護の決め手となるハードウェア、ファームウェア、およびソフトウェアを含み、保護を維持して信頼性を高める必要の無い要素からは分離されたシステム要素として、設計および実装されていなければならない。それゆえ、TCB のインタフェースと要素を正しい機能と共に識別することが評価の基本となる。

汎用的なシステムのために、TCB は、オペレーティングシステムのキーとなる要素を含むことになる。また、オペレーティングシステム全体を含む可能性もある。組込みシステムにおいては、セキュリティポリシーは、オペレーティングシステムレベルよりも、むしろアプリケーションレベルで意味のある方法で、オブジェクトを扱うかもしれない。このように、保護ポリシーは、基本となるオペレーティングシステムよりも、アプリケーション・ソフトウェアで適用される可能性がある。必然的に、TCB は、オペレーティングシステムとアプリケーション・ソフトウェアの、ポリシーをサポートするのに必須の部分をすべて含むことになる。TCB のコード量が増えた場合、すべての状況下でのリファレンスモニターの要件を TCB が確実に適用することが困難になっていくことに注意しなければならない。

6.4 保証

三番目のリファレンスモニターの要件の目的は、現在、TCB が「十分に単純な構造で、複雑さは分析とテストを受けるのに十分であり、完全性が保証されていなければならない」という言葉で表されている。

アプリケーションや環境によって分かるシステム操作上のリスクの度合いが増加する時(例えば、システムのユーザ数の増加に伴って拡大する許可の範囲と同様な、システムの保護すべきデータの機密の範囲)、システム内の信頼度を立証するためには、明らかに、保証も強化させなければならない。トラステッド・コンピュータ・システムの評価基準(TCSEC)における評価クラスに現れる要件の階層は、これらの保証要件を反映している。

5.3 節で記述したように、それぞれのトラステッド・コンピュータ・システムで適用するセキュリティポリシーの表現を、評価基準は均一にすることが必要である。さらに、TCB がリファレンスモニターの最初の二つの要件を満足する理由を説明する、納得できる根拠が評価基準には要求される。この根拠は完全に形式的である必要はない。保証制御の目的を満たすために、各候補システムにはこの根拠が必要である。

セキュリティ強制メカニズムが初期からデザインされて組み込まれているシステムに比べて、そのメカニズムを追加したシステムでは、セキュリティカーネルに必要不可欠な単純さに欠けるため、広い分析に対して容易には扱えない。これは、システム全体のほとんど

をカバーするように TCB が拡張されるためである。そのため、信頼度はテスト結果によってのみ得られる。コンピュータシステムのように複雑なものに対する真の意味で完全なテスト方法はないため、他の侵入の試みが成功してしまう可能性を常にはらんでいる。そのようなシステムが、低い評価クラスに落ちるのは、この理由によるものである。

一方、当初から TCB の概念をサポートするようにデザインされて組み込まれたシステムでは、構造的なテストと解析が、より容易に可能である。形式的手法は、システムのセキュリティポリシーを適用したリファレンス認証メカニズムの正しさを検証するために用いられる。あまり形式的ではない根拠を含む他の方法は、アクセス調整の完全性と耐タンパ性の度合いに対する主張を説明するために用いられることがある。より高い信頼性は、整然と構造化されてはいないシステムの結果の上に成り立つのではなく、形式的手法の分析の結果と構造化テストの徹底度合いによって成り立つ。この理由によって、リスクがより高い環境では、これらのシステムを使用できると結論付けるのは妥当と思われる。このようなシステムの実装が成功した場合には、より高い評価クラスに位置づけられる。

6.5 クラス

評価クラス全体のうち、ごく一部のみが強く望まれている。
評価基準には主要な区分が三つあり、4 番目の区分は評価を受けたがセキュリティ保護が受け入れられないシステムのために予約されている。それぞれの主要な評価区分には、トラステッドシステムのデザインと開発の「中間的な」クラスが慎重に定義されている。この中間クラスが基準の中に取り入れられたのは、次のようなシステムを識別するためである。

* 当該評価クラスのための基本要求を満たし、重要でより良い保護と保証を提供するように見えるシステム。
* 中間評価クラスにあるシステムが、例えば次に高い評価クラスの要求を満たす可能性があるなどの、いつか発展することが考えられる理由がある場合。

A 区分以外には、上述した二つの特徴を満たす、追加の「中間」評価クラスが使用されることはないと思われる。

システムアーキテクチャに基づいた区分、セキュリティポリシーの適用、および評価クラス間の信頼性の根拠を定義したため、評価クラス間の「ジャンプ」は、実装者側にかなりの労力と投資を要求する。これに対応するために、より高次の評価クラスのシステムがさらされるリスクとの差分として表現することが望まれている。

7.0 ポリシーと規準の関係

セクション 1（規準、Criteria）は基本的なコンピュータセキュリティ要求事項を提示し、セクション 5（理論的根拠とガイドライン）はトラステッド・コンピュータ・システムのための制御コントロール目的を提示している。

それらはあらゆるセキュアシステムの開発のために有用で、必要な一般的要求事項である。ただし、機密区分または取扱注意情報の処理に使用されるシステムを設計する際は、コントロール目的に適合する機能的な要件はより具体的になる。
一般的な連邦の情報、特に機密情報の取扱いと処理のための手続の基礎を形成する規則、指令、大統領行政府命令、およびＯＭＢ通達という形で大量のポリシーが提示されている。このセクションではこれらのポリシーステートメントから適切な引用文を示し、制御コントロール目的とそれらの関係を論じる。
これらの引用文は、ポリシーと基準との関係を説明する例であり、完全でないかもしれない。

7.1 確立された連邦政府ポリシー

かなりの数のコンピュータセキュリティポリシーとその関連する要求事項が連邦政府の各部署から公表されている。関心のある読者は、参考資料[32]を参照されたい。それは、州や地方自治体や民間セクターの中でも同様に、連邦政府の文民エージェンシーの中でのトラステッドシステムの必要性を分析するものである。この参考資料はまた、以下ではさらには扱わない多くの関連する連邦法令、政策および要件を詳説している。

連邦の自動化された情報システムのためのセキュリティガイドは行政管理予算局（ＯＭＢ）によって提供される。二つの特に適用可能な通達が発表されている。ＯＭＢ通達 No.A-71、伝達覚書 No.1、「連邦自動情報システムのセキュリティ」、[26]は各行政府のエージェンシーに、コンピュータセキュリティプログラムを設立し、維持するように指導している。それは各行政府の支部、部門、部局（エージェンシー）の長を、組織内でまたは商業的に処理されるかどうかにかかわらずすべてのエージェンシーデータのセキュリティの適正レベルを保証するために責任を持たせている。これは、国家安全保障データと同じく、国家安全保障規則にも支配されない、個人的、財産的、その他の機密データを保護するために適切に必要とされる物理的、管理的、技術的な予防手段の設立についての責任を含むものである。

政府の計画の中で詐欺、浪費、乱用を取り除くために出されたＯＭＢ通達 No.A-123,「内部統制システム」[27]が必要とするのは、(a)エージェンシーのトップが、内部統制指令を出し、責任を割り当てること、(b)管理者達が脆弱性を探してプログラムをレビューすること、および(c)管理者達がコントロールの力を評価して、制御コントロールを更新するために定期的なレビューを実行することである。ＯＭＢ通達 A-123 が公表されたすぐ後で、セキュアコンピュータシステムの作成に対してその内部統制の要件の関係が認知された。[4] A-123 における内部統制の定義は、コンピュータコントロールが特に明記されていないが、コンピュータシステムが含まれるべきことは明確である。

「内部統制とは、--組織の計画と、その資源を守るために各部門の中に採用されたすべての方法と手段が、その情報の正確性と信頼性を保証し、適用される法律、規則、ポリシー

の遵守を保証し、運用の経済性と効率性を促進するものである。」[27(sec.4.C]
ＡＤＰシステムによって処理される機密区分された国家安全保障情報の問題は、コンピュータセキュリティの中で重要で拡大する関心を与えられた最初の分野の一つである。
結果として公表されたコンピュータセキュリティポリシーの文書は、概してより詳細で構造的な要件を含んでおり、その結果、それ自体がむしろ明確に表現し構造的な情報セキュリティポリシーを提供するという、信頼された基盤へ照準を合わせている。
この基盤である行政府命令 12356「国家セキュリティ情報」は、それ自身で、機密区分とその取消し、および「国家セキュリティ情報」の安全を守るための要件を明らかにしている。

7.2 国防総省ポリシー

国防総省の中で、これらの広い要件は実施され、さらに２種の主要な規則：を通して特定化される：
1) 米国国防総省規則 5200.1-R [7]。これは国防総省のすべての契約者にそれ自体適用される。
2) 米国国防総省 5220.22-M「区分機密情報を守るための産業のセキュリティマニュアル」[11]。これは防衛産業のセキュリティプログラムの中に含まれる契約者に適用する。
留意すべき点は、後者が米国国防総省の範囲を超えることである。すなわち、それは国防総省のコンポーネントの機密情報を処理する契約者に適用するばかりでなく、18 の他の連邦組織の契約者にも適用する。それらに対して国防長官は、産業のセキュリティサービスをするように行動する権限を与えられている。《注》

（注）NASA, 商務省、GSA, State Department, Small Business Administration, 科学基金、財務省、運輸省、内務省、農務省、情報局、労働省、環境情報局、司法省、武器管理・武装解除局、連邦危機管理局、連邦予備兵システム、会計検査院

ＡＤＰ(自動データ処理)システムのために、これらの情報セキュリティ要件はさらに拡大されて指定される：
1) 米国国防総省取引先(コンポーネント)のための米国国防総省指令 5200.28[8]と米国国防総省マニュアル 5200.28-M [9]；
2) 契約者のための米国国防総省 5220.22-M [11]のセクション XIII。

米国国防総省指令 5200.28(「自動データ処理(ADP)システムのためのセキュリティ要件」)は次のように規定している：
「ＡＤＰシステムの中に含まれている機密区分されたマテリアルはシステムのハードウェアとソフトウェアのデザインと構成の中の保護機能の継続的な採用によって守られることとする。」[8.sec.Ⅳ]　さらに必要なことは、機密データを処理し保存し利用し、機密情報を生成するＡＤＰシステムが、妥当な信頼性をもって安全保護をすることである。

a. 未認証者による機密区分されるマテリアルへの故意のまたは不注意なアクセス および
b. コンピュータおよびその関連周辺機器"の未認証の操作[8、sec.B.03]
これらと同義の要件は米国国防総省 5200.28-M [9]中と米国国防総省 5220.22-M [11]中に示されている。

米国国防総省指令 5200.28 はＡＤＰシステムのためのセキュリティ要件を提供している。米国国防総省指令 5200.28 は､機密区分された情報(SCI)に類するいくつかのタイプの情報のために、他の最小のセキュリティ要件が同様にあてはまることを述べている。
これらの最小要件は、米国国防総省と米国国防総省の契約者のＡＤＰシステムのために DIAM50-4(新参照番号 6)において実施される DCID 1/16(新参照番号 5)の中に見られる。

これらの規則、指令と通達によって課された要件から、アカウンタビリティと保証の制御目標と同様に、セキュリティポリシーの制御目標の三つのコンポーネント、すなわち強制(的)と 任意（自由裁量)のセキュリティ、およびマーキングを、米国国防総省アプリケーションのために機能的に定義することができる。次の論議はこれらのコントロール目的のためのポリシーの更なる具体化を提供する。

7.3 セキュリティポリシーのための制御目標基準

7.3.1 マーキング

マーキングのための制御目標は次のとおりである。:
「強制的なセキュリティポリシーを実施するようにデザインされているシステムは、すべての情報に対して機密度区分または他の機密ラベルの完全性を記憶し保存しなければならない。」「システムからエクスポートされるラベルはエクスポートされる内部の機密ラベルに相当する正確な表現でなければならない。」

米国国防総省 5220.22-M(「機密情報を守るための産業のセキュリティマニュアル」)は第 11 節中でマーキング情報の理由を説明している：
a.一般
「物理的なマーキング、表記法、または他の方法による機密度区分の明示は不正な開示アクセスに対してどの程度の防御ががその情報または資材のために必要とされるかを持ち主に警告し通知するのに役立つ。」(14)
マーキング要件は多くのポリシーステートメントにおいて与えられている。
大統領命令 12356(セクション 1.5.a と 1.5.a.1)は、機密度区分のマーキングが「すべての機密区分される文書の面上で示されるか、関係する媒体に適切な方法で他の形式の機密区分情報と明確に関連付けられていなければならない」と要求している。[14]

米国国防総省規則 5200.1-R(セクション 1-500)は次のことを要求している：
国家のセキュリティにおける未認証の開示アクセスに対する保護を必要とする情報または資材は、3 種の指定すなわち'Top Secret','Secret'または'Confidential' のうちの１つ

に分類されるものとする。[7]（拡張すると、コンピュータ処理の利用に対して、非公式な指定である「非機密」とは、機密情報の他の 3 種の指定の何れにも該当しない情報を示すために使われる。）

米国国防総省規則 5200.1-R(セクション 4-304b)は次のことを要求している：
「そのようなメディアを採用しているＡＤＰ（自動データ処理）システムとワードプロセッシングシステムは、その中にあって再生するか、生成される機密分類された情報が適用可能な機密度区分およびそれと関連したマーキングを持つことを確認保証するために内部の機密度区分に対してマーキングを使用することとする。」
（この規則は、一定の既存のシステムの除外を規定する。そのシステムでは 「内部の機密度区分および適用可能な関連したマーキングは、大規模なシステム修正なしでは実装できない。」[7]
しかし、将来の米国国防総省ＡＤＰシステムが機密区分されたおよび他の機密情報のために適用可能な正確なラベルを提供することができることは明確である。）

米国国防総省マニュアル 5200.28-M(セクション IV、4-305d)は以下を要求している：
「セキュリティラベル --ＡＤＰシステムにより、あるいはその中でアクセス可能なすべての機密区分されるマテリアルは、そのセキュリティ機密度区分とアクセスまたは配布制限について識別されることとし、ＡＤＰシステムのすべてのアウトプットは適切にマーキングされるものとする。」[9]

7.3.2 強制セキュリティ

7.3.2 強制セキュリティ

強制セキュリティのための制御目標は：
「機密区分されたまたは、他の特に分類された機密情報を処理するために使用されるシステムのために定義されるセキュリティ・ポリシーは、強制アクセス制御規則を実施するための規定を含まなければならない。
すなわち、それらは、直接的には、情報に対する個人への許可または承認と検索される情報の機密区分または機密度指定との比較において、間接的には、制御における物理的及び他の環境ファクターを考慮して、アクセスを制御するための一連のルールを含まなければならない。
強制的アクセス制御規則は、正確に、関連する法律、規則、および由来する総合ポリシーを反映しなければならない。
強制セキュリティと関連する多くのポリシーステートメントがある。

大統領命令 12356(セクション 4.1.a)は、述べる。
「特定の者の機密情報へのアクセスは、政府機関長または任命された当局者によって信頼性の判定が提供され、そのようなアクセスが合法であり、承認された政府目的の遂行に不可欠であるとされるならば適格となる。」[14]

米国国防総省指令 5200.1-R(第Ⅰ章、セクション 3)は「特別アクセスプログラム」を「機密、秘密、あるいは極秘の情報へのアクセスのために、「‘ 知る必要性 ’ または通常提供されるものを越えたアクセス制御を認めるあらゆるプログラム」と定義している。そのプログラムには、"特別なクリアランス、判決、あるいは調査要求事項、‘ 知る必要性 ’ の判定権限を与えられた当局者の特別指示、または、‘ 知る必要性 ’ を持つと判定された人の特別リストを含むが、必ずしもこの限りではない。"[7, para. 1-328]

この段落は、知る必要性における ‘ 任意（自由裁量)の ’ 判定と、特別なアクセスプログラムを通して実施されるフォーマルな知る必要性とを区別している。
米国国防総省指令 5200.1-R、パラグラフ 7-100 は、信頼性(クリアランス)と知る必要性の為の一般的な要件を記述し、所有、知識、または機密情報の制御権を持つ個人が、アクセスのための条件が満たされているかどうかを決定することについての最終的な責任を持つことを述べる。
この規定はさらに、”誰も、単にランクまたはポジションの効力で機密情報にアクセスできる権利を持たない ” と規定している。[7, para.7-100]）

米国国防総省マニュアル 5220.28-M(セクションⅡ　2-100)では、"機密あるいは機密資料を開発又はアクセスするために使用されるであろうプログラムを開発、テスト(デバッグ)、保守、又は使用する人員は、システム制約の下で彼らがアクセスするであろう機密資料の最も制約の多いカテゴリと最も高い機密事項用として、アクセス認可(知る必要性）と個人セキュリティクリアランスをもつべきである。"と述べる。[9]

米国国防総省マニュアル 5220.22-M(パラグラフ 3.a)はアクセスを、”「能力と機密情報に関する知識を得る機会」と定義する。
もし、セキュリティ対策によって機密情報についての知識を得ることが妨げられないならば、事実上、こうした情報が保持される場所にいる個人は誰でも、機密情報にアクセスするかもしれない。"[11]

上述の大統領命令、マニュアル、指令、および規則は、はっきりと、トラステッドコンピュータシステムが、適切なクリアランスを欠く個人に機密情報へのアクセスを許可できないよう、機密性の高いデータと機密度区分ラベルが恣意的に交換されることがないよう保証しなければならないことを示している。
また、その「格下げ」が公認されない限り、より高い分類からのデータが下の機密度区分のストレージオブジェクトに置かれることができないように、トラステッドコンピュータシステムが情報の流れを制御しなければならないという必要条件が示されている。

7.3.3　任意(自由裁量)セキュリティ

任意(自由裁量)セキュリティの用語は、個人ベースで情報を制御するコンピュータシステムの能力に関連している。

それは、個人が特定の機密情報にアクセスする全てのフォーマルな（クリアランス）許可を持っていても、情報への各個別のアクセスは、証明された必要性に基づかなければならないという事実に由来している。
このため、この必要条件が、「受け取るかやめるか」という意味において任意（自由裁量)でないことは明らかにされなければならない。

機密情報へのアクセスが許諾される前に、知る必要性テストが十分に行われた後スタートすることを指令と規則は明示的に述べている。
任意（自由裁量)セキュリティのための制御目標は：
「セキュリティ・ポリシーは、機密区分されたまたは他の任意（自由裁量)アクセス制御規則を強制するための条件を含まなくてはならない機密情報の処理に使われるシステムのために定義される。
すなわち、それらは、情報を「知る必要がある」と判定された個人の識別に基づいてアクセスを制御し制限するための一貫した一連の規則を含まなければならない。

既に提供の「知る必要性」に関する引用に加えて、本章は「知る必要性」原則を強調して次のように述べる。このセクションは、「アクセスが公務執行に不可欠（であっても」）-------でなければ、機密区分された情報にアクセスできない」として、知る必要性原則を強調している。[7]

また、米国国防総省マニュアル 5220.22-M(セクション III 20.a)では、以下のように述べている。個人が機密区分された情報へのアクセスを許されるのは、ただ----------契約者が、業務執行または契約又はプログラムの遂行に必須の業務またはサービスへのアクセスが必要と判定された時に限る。すなわち個人が知る必要性を持ったときである。"[11]

7.4 説明責任の制御目標基準：
説明責任のための制御目標とは：
「強制であれ任意（自由裁量)であれセキュリティポリシーが実施される時はいつでも、機密または他の取扱注意情報を扱うまたは処理するために使用されるシステムは、個人の責任を常時保障しなければならない。さらに、責任を確実にするために、承認された、正当な権限をもったエージェントが、適度な時間内に、そして過度の困難なしで、安全な方法によって責任情報にアクセスし、評価しなければならない。

この制御目標は：以下の引用によってサポートされる。

米国国防総省指令 5200.28(VI.A.1)は述べる：
「各ユーザのアイデンティティは明確に確立され、ユーザによるシステムへアクセス、シ

ステム内での活動(アクセスされた素材ととられた行動も含む)が制御され、精密な検査のために開示される。」
米国国防総省マニュアル 5200.28-M(セクション V5-100)は述べる：
「監査ログまたはファイル(マニュアル、マシン、または両方の組み合わせ)は、システム活動の規則的なセキュリティレビューを許すために自動データ処理（ADP）システム使用の履歴として維持されるべきである。
(例えばログは、機密ファイルへの夫々のアクセス(例えばログイン、説明責任のある機密出力の生成、および新しい機密ファイルの作成)とアクセスの性質を含めて、セキュリティに関連したトランザクションを記録すべきである。
各人の‘ジョブ’または‘対話型セッション’間に[個々の参照の数を問わず]首尾よくアクセスされた各機密ファイルも監査ログに記録されるべきである。
このログの中の素材の多くは、システムがログに託された情報の維持を保証するために、必要とされている）」[9]

米国国防総省マニュアル 5200.28-M(セクション IV4-305f)は述べる：
「各ユーザまたはユーザの特定グループが、アクセス制御と個別責任の保障を必要とする場所は、適切な管理の自動データ処理（ADP）システムにより又はハードウェア/ソフトウェアの手段によって識別されなければならない。
そのような識別手段は、自動データ処理（ADP）システムが、ユーザに承認された素材だけを提供することを可能にするために十分に詳細でなければならない。」[9]

米国国防総省マニュアル 5200.28-M(セクション I　1-102b)は述べる：

「構成要素の指名承認機関又はその目的の被指名人は----------を保証するであろう：

(4) オペレーティングシステム(O/S)とそれに対するすべての部分修正のドキュメンテーションの保守、問題発生点またはシステムに含まれるセキュリティ関連欠陥のトレースを可能にするための十分な期間の保持。

(6) 機器の故障または人員の行動を通して明らかなった発見、回復、取り扱い、機密資料の廃棄に係わる手順の確立。

(7) 全ての証明された自動データ処理（ADP）システムでセキュリティ上の欠陥の適切な配備と訂正、システム運用又は監査レコード、セキュリティ違反又はセキュリティに関連したシステム誤動作の記録、および自動データ処理（ADP）システムのセキュリティ機能のテスト記録の効果的な使用と配備。"[9]

米国国防総省マニュアル 5220.22-M(セクション XIII 111)は述べる：「監査証跡」

a. いかなる自動データ処理（ADP）システム監査証跡においても、一般的なセキュリティ要件は、システム使用の文書化された履歴を提供することである。
承認された監査証跡を利用すると機密システム活動のレビューができ、もしセキュリティ故障が発生した場合は、調整案の大きさの程度を決定する目的で行うイベントの復元のために詳細な活動レコードを提供することができる。
この基本的な要件を果たすために、監査証跡システム、マニュアル、自動化された又は双方の組み合わせは、以下の領域で起こっている重要なイベントを文書化しなければならない：
i)入力データの準備と出力データの配布(すなわちユーザとシステムサポート要員間の報告可能な相互運用性)、(ii)ADP 環境に含まれる活動(例えばセキュリティと関連した制御のための ADP サポート人員の調整)および(iii)内部のマシン活動

b. 機密情報を処理するために承認された自動データ処理（ADP）システムのための監査証跡は、上の 3 つの領域に基づかなければならず、特定のシステムに一致されらるかもしれない。
機密処理のために承認された全てのシステムは、以下に掲げられた監査証跡レコードの全て、少なくとも大多数を含むべきである。

契約者の SPP ドキュメンテーションは適用可能性を識別し記述しなければならない：

1. 人員アクセス；
2. 中央コンピュータ施設またはリモート端末エリアへの承認されない内密の入場；
3. 関連するシステムセキュリティの開始と終了イベントを示す機密処理の開始/終了時刻(例えばパラグラフ 107 に準じたアップグレード/格下げ行動)；
4. 自動データ処理（ADP）システムコンソールオペレータによって開始されたすべての機能；
5. リモート端末と周辺機器(パラグラフ 107c)の切断；
6. ログオンとログオフのユーザ活動；
7. すべてのオープン、クローズ、ファイル破壊活動と同様に、ファイルにアクセスする未承認の試み又はプログラム。
8. 識別情報(すなわちユーザ/プログラム名、出来事などの時間と位置等)を含んだプログラムアボートと例外；
9. システムハードウェア追加、削除、およびメンテナンス行動；
10. システムソフトウェアのセキュリティ機能に影響している世代と修正。

c. 自動データ処理（ADP）システムのセキュリティスーパーバイザまたはその指名受領者は、全ての関係した活動が適切に記録され、どのような例外でも訂正のための適切な活動がとられていることを保証するために、少なくとも毎週監査証跡ログをレビューしなければならない。

今日使用中の大多数の自動データ処理（ADP）システムは、前記との協定により監査証跡システムを開発できる；しかしながら、武器、通信、通信セキュリティ、および戦術的なデータ交換、表示システムなどの特別なシステムについては、上記のすべての面に応じるわけにゆかないかもしれず、認識しているセキュリティオフィスによる調整された個別の配慮を必要とするかもしれない。

d. 監査証跡レコードは一つの検査サイクルの間は、保持されていなければならない。[11]

7.5 保証の制御目的基準

保証の制御目標は以下の通りである：機密区分されまたは機密性の高い情報を処理ないしは取扱うために使われるシステムは、セキュリティポリシーによる、正確な説明を保証するように設計されなければならず、またそのポリシーの意図をゆがめてはならない。保証はポリシーの正確な導入と運用がシステムのライフサイクルを通して存在することを規定しなければならない。

この目的のための根本原理は米国国防総省指令 5200.28 の以下のセクション中に記載されている：
米国国防総省指令 5200.28(IV.B.1)は規定する：
「一般に、ADP システムのセキュリティは、システムが最初からセキュリティを提供するように設計されるならば、きわめて効果的で経済的である。機密区分されるマテリアルを処理、保存、使用、あるいは作成する ADP システムの設計を引き受ける国防総省の各構成部署は、次のように行わなければならない。:「設計プロセスの当初から、この指令に規定されたセキュリティポリシー、概念、および手段を考慮すべきである」。[8]

米国国防総省指令 5200.28(IV.C.5.a)は述べる：
「規定は、(開発、実装された変更手続を提供し、機密区分される資源への不正アクセスとシステムとそのコンポーネントの無許可操作の両方を防止するであろう）システムによって実際に処理されている機密区分カテゴリやタイプに必要な保護のレベルに ADP システムエリアコントロールの調整を許可するようにつくられることもある。
システムにアクセスできるユーザの個人のセキュリティ・クリアランスレベルが変わる場合、自動化されたシステムセキュリティ対策、技術、および手続の継続的な保護に特別な配慮をするべきである」。[8]

米国国防総省指令 5200.28(VI.A.2)は述べる：
「環境管理。ADP システムは、システムエントリポイントへの不正アクセス、システムの機密情報へのアクセス、またはシステムへの損害の可能性を最小化するために外部から保護されなければならない。
米国国防総省マニュアル 5200.28-M(セクションの I1-102b)は述べる：
「コンポーネントの指定の承認権限者あるいはこの目的のために指定された人・・・

.は確実にするであろう：・・・

(5) システムのセキュリティ機能に影響する是認された ADP システムの変更についての適切な監視、モニタリングおよびテスト、その結果として安全なシステムが維持される。

(7) 是認されたすべての ADP システムにおけるセキュリティ不備に対する適切な処置と訂正、ハウスキーピングまたは監査レコードの効果的な使用と処置、セキュリティ違反またはセキュリティ関連システムの誤動作の記録、および ADP システムのセキュリティ機能のテスト記録。

(8) 有能なシステム ST&E、システム ST&E リポートの適時のレビュー、および欠陥の訂正の指導によって、機密情報の処理のための ADP システムの条件付き、または最終的な承認あるいは不承認をサポートする必要がある。

(9) 公的機関、これは選択された技術、手続、標準、および ADP システムのセキュリティ機能のテストと評価のために利用されるテスト記録の維持のための、中央 ST&E 統合ポイントとして適切である。なお、ADP システムのセキュリティ機能のテストと評価は、他の国防総省コンポーネントによって行われる適切な検証と利用に適合するとされている。[9]

米国国防総省マニュアル 5220.22-M(セクション XIII 103a)は、次を要求する。
「ADP システムのどのような機密情報も、処理前のセキュリティ審理部局の書面による最初の承認。このセクションでは、初期の承認に引き続いての主要なシステム修正のために、認識しているセキュリティ部局による再承認を必要とする。再承認を必要とするのは、(１)個人アクセス必要条件での主要な変更（２）中央のコンピュータ設備の再配置あるいは構成変更（３）メインフレーム、記憶装置あるいは入力/出力装置への追加、削除あるいは変更（４）セキュリティ保護機能に影響するソフトウェアの変更（５）機密情報アクセス資格、情報の機密解除、監査証跡、あるいはハードウェア/ソフトウェアのメンテナンス手順の任意の変更（６）セキュリティ審理部局によって決定される他のシステム変更である。[11]

保証の主なコンポーネント、ライフサイクル保証は、DoD 指令 7920.l に記述されるとともに、オペレーション同様、開発フェーズにおいてもテストする ADP システムと関係している。(17)米国国防総省指令 5215.1(セクション F.2.C.(2))は「これらの基準に対する、選択された産業および政府で開発されたトラステッドコンピュータシステムの評価」を必要とする」。[10]

8.0 隠れチャネルのガイドライン

隠れチャネルは、システムのセキュリティポリシーに反する方法で情報を転送するためにプロセスが利用可能なあらゆる通信経路である。隠れチャネルにはストレージ チャネルとタイミングチャネル、の二つのタイプがある。隠れストレージ・チャネルは、直接あるいは間接的に、あるプロセスによって割り当てられた記憶領域に書き込み、他のプロセスによって読み出すことを可能とする、全ての伝達手段を含む。隠れタイミング・チャネルは、あるプロセスがそれ自身のシステム資源の使用を変調することにより、第二のプロセスが観測できる応答時間の変化として情報を提供する様な方法で、情報の送信を可能にする全ての伝達手段を含む。

セキュリティの観点からは、低いバンド幅の隠れチャネルは高いバンド幅のそれより低い脅威であると言える。しかし、多くのタイプの隠れチャネルのために、一定のレート(特定のチャネルメカニズムとシステム･アーキテクチャに依存する)以下にバンド幅を減らすために使われる技術は、一方で正当なシステムユーザに提供された性能を低下させる影響がある。そのため、システム・パフォーマンスと隠れチャネルのバンド幅の間のトレードオフが必要となる。機密に分類された情報あるいは取扱注意が必要とされた情報を収容する、どのようなマルチレベルのコンピュータシステムにでも、「汚染」の脅威があり、そのようなシステムは高帯域の隠れチャネルを含むべきではない。このガイドラインは、
システム開発者に、「高い」隠れチャネルのバンド幅がまさにどれほど高いかの概念を提供することを意図している。

100 ビット／秒が、多くのコンピュータ端末が動作する概算値であり、100 ビット秒を越える隠れチャネルのバンド幅は「高い」と考えられる。情報が、一般的に使われる機器の通常の出力速度と等しい速度で汚染される可能性があるならば、コンピュータシステムを「安全である」とみなすのに適切であるとは言えない。

どのようなマルチレベルのコンピュータシステムの中にでも、システム・デザインの深部に潜在する多くの比較的低バンド幅の隠れチャネルがある。そのような隠れチャネルのバンド幅を低減する潜在的なコストの大きさを考慮すれば、大半のアプリケーション環境において、バンド幅が 1 ビット／秒未満のものは容認できる。いくつかのシステムでは、1 ビット／秒以上のバンド幅のすべての隠れチャネルを取り除き、容認できる性能を維持することは実際的ではないかもしれないが、システムの性能に悪影響を与えずにそれらの使用を監査することは可能である。この監査機能は、システム管理部門に重大な「汚染」の検出および手続き的訂正の手段を提供する。従って、トラステッド・コンピューティング・ベース（TCB）は、どのような部分においても、隠れチャネル機構の使用を監査する機能として、10 秒間に 1 ビット以下のレートを検知できる帯域幅を提供しなければならない。

隠れチャネル問題は、多くの作者が取り組んでいる。興味がある読者は、参考文献
[5]、[6]、[19]、[21]、[22]、[23]、および[29]を参照されたい。

9.0 強制アクセス制御機能の構成におけるガイドライン

強制アクセス制御要求は不特定数の階層的な機密レベルとそれぞれの階層的なレベルにおける不特定数の非階層的カテゴリを支援する能力を含む。国家安全保障機関のトラステッド・コンピュータ・システムの設計と開発における一貫性と移植性を促進するために、すべてのそのようなシステムにおいて最小限のレベルとカテゴリをサポートできることが望ましい。以下の提言はこの目的のために提供されている。

* 階層的な機密レベルの数は 16 以上であることが望ましい。
* 非階層的なカテゴリの数は 64 以上であることが望ましい。

10.0 セキュリティ検査に関するガイドライン

セキュリティ･テストに関するガイドラインは､フォーマル製品評価プロセスにおいて米国国防総省(DoD)コンピュータセキュリティセンターが実施するテストの範囲と深度を示すために提供される。本セクションで示すガイドラインは、フォーマル製品評価プロセスを通して DoD コンピュータ・セキュリティセンターが保証するテストの範囲と深さを示すために提供される｡自分たちが評価を行う目的で､｢国防総省トラステツド･コンピュータ･システム評価基準」を使用したいと考えている組織は、本セクションは計画立案に役立つであろう。

パート 1 と同様、強調表示は、ガイドラインにおいて次に低いセキュリティレベルと異なるところを示している。

10.1 区分 C における検査

10.1.1 要員

セキュリティ・テストチームは、コンピュータ・サイエンスの学士あるいは同等の資格を持つ要員が、最低でも２人で構成されなければならない。チームメンバーは、システム開発者が準備したテスト計画を実行する能力と追加事項を提案する能力を持つていなければならない｡｢欠陥仮説法」あるいは同等のセキュリティテスト方法論に精通し、アセンブラレベルのプログラミング経験を持っていなければならない。テストの開始前に、チームメンバーは、評価すべきシステムの機能に関する知識があり、システム開発者による内部講習を修了していなければならない。

10.1.2 検査

チームは、システム開発者が使用するテストとは無関係に、積極的にテストを実践しなければならない。-チームは、システムのセキュリティ・メカニズムをくぐり抜けることを試みるシステム特有のテストを独自に少なくとも５つ設計し、実装しなければならない。
テストの実施期間は、最低でも 1 ヶ月は行わなければならないが、3 ヶ月を超える必要はない。システム開発者が定義したテストとテストチームが定義したテストをやり遂げるのに、実作業時間として 20 時間程度は掛けなければならない

10.2 区分 B における検査

10.2.1 要員

セキュリティ・テストチームは、コンピュータ・サイエンスの学士あるいは同等の資格を持つ要員が最低でも２人と、コンピュータ・サイエンスの修士あるいは同等の資格を持つ要員が最低でも１人からなる構成としなければならない。チームメンバーは、システム開発者が準備したテスト計画に従うとともに追加テスト提案することができ、「欠陥仮説法」あるいは同等のセキュリティテスト方法論に精通し、TCB を実装するさ言語に熟達しており、かつアセンブラレベルのプログラミング経験を持っていなければならない。テストの開始前に、チームメンバーは、評価すべきシステムの機能に関する知識があり、システム開発者による内部講習を修了していなければならない。最低でもチームメンバーの 1 人は、他のシステムでセキュリティテストを経験していなければならない。

10.2.2 検査

チームは、セキュリティに直接関連するハードウェアとソフトウェアをテストするためにシステム開発者が使用するテストパッケージとは無関係に、積極的にテストを実践しなければならない。チームは、システムのセキュリティ・メカニズムをくぐり抜けることを試みるシステム特有のテストを少なくとも独自に１５種類設計し、実装すべきである。テストの実施期間は、最低でも２ヶ月は行わなければならないが、4 ヶ月を超える必要はない。システム開発者が定義したテストとテストチームが定義したテストをやり遂げるのに、実作業時間としてチームメンバーあたり 30 時間程度は掛けなければならない

10.3 区分 A における検査

10.3.1 要員

セキュリティ・テストチームは、コンピュータ・サイエンスの学士あるいは同等の資格を持つ要員が最低でも１人と、コンピュータ・サイエンスの修士あるいは同等の資格を持つ要員が最低でも２人からなる構成としなければならない。チームメンバーは、システム開発者が準備したテスト計画に従うとともに追加テスト提案することができ、「欠陥仮説法」あるいは同等のセキュリティテスト方法論に精通し、TCB 実装言語(群)に熟達しており、かつアセンブラレベルのプログラミング経験を持っていなければならない。テストの開始前に、チームメンバーは、評価すべきシステムの機能に関する知識があり、システム開発者による内部講習を修了していなければならない。少なくともチームメンバーの一人は、保守診断プログラムと補助ハードウェア文書を理解するために、システムのハードウェアに精通していなければならない。最低でもチームメンバーの２人は、事前に、他のシステムでセキュリティテストを完了させていなければならない。システムへデバイス･ドライバを追加するのと同程度の複雑なレベルのテストにおいて、最低でもチームメンバーの 1 人は、システムレベルのプログラミング能力を持っていることを証明しなければならない。

10.3.2 検査

チームは、セキュリティに直接関連するハードウェアとソフトウェアをテストするために

システム開発者が使用するテストパッケージとは無関係に、積極的にテストを実践しなければならない。チームは、システムのセキュリティ・メカニズムをくぐり抜けることを試みるシステム特有のテストを独自に少なくとも 25、種類を設計し、実装すべきである。テストの実施期間は、最低でも 3 ヶ月は行わなければならないが、6 ヶ月を超える必要はない。システム開発者が定義したテストとテストチームが定義したテストをやり遂げるのに、実作業時間としてチームメンバーあたり 50 時間は掛けなければならない。

附録 A

商用製品の評価プロセス

「国防総省トラステッド・コンピュータ・システム評価基準」は、コンピュータセキュリティセンターが商用コンピュータのセキュリティ評価プロセスを実施するための基準である。このプロセスは、政府機関の要求を満たす商用の出荷・保守される汎用オペレーティングシステム製品のためのものである。正式な評価は、既製の商用コンピュータを対象としており、システム全体のパフォーマンスや組み込まれるアプリケーション、個々の処理環境は考慮に入れていない。その評価はコンピュータシステムセキュリティの承認・認定の重要な要素となる。しかし、それはコンピュータシステムの完全なセキュリティ評価を構成するものではない。個々のシステムにおいては、システム固有の環境を考慮しなければならない(例：リファレンス[18])。例えば、オペレーション、特定のユーザ、アプリケーション、データ機密度、物理的・人的セキュリティ、管理上・手続上のセキュリティ、ＴＥＭＰＥＳＴ、および通信上のセキュリティにおける各種の要件を考慮しなければならない。

コンピュータセキュリティセンターによって実施される製品評価プロセスには 3 つの要素がある。

* 予備的な製品評価

－ ベンダとセンターとの非公式な意見交換である。ベンダの製品や基準についての共通認識と正式な製品評価で予想される格付けについての共通認識を得るため、技術情報に関する意見交換を行う。

* 正式な製品評価

－ 米国国防総省が利用可能で評価済み製品リストにその製品の評価結果と格付けが記載されているコンピュータセキュリティセンターによる正式な評価。

* 評価済み製品リスト

－正式な製品評価によって格付けられた製品リスト。

＜予備的な製品評価＞

一般的に製品のライフサイクルの後半では、効果的なセキュリティ評価指標を追加することは難しい。従ってコンピュータセキュリティセンターは製品設計の初期段階にシステムベンダと一緒に検討することに高い関心を持っている。予備的な製品評価により、正式公表前の製品において発見したコンピュータセキュリティ上の課題についてコンピュータベンダとセンターとが協議することが可能となる。

予備的な評価は、セキュリティ機能を実装する新製品、あるいは既存製品のアップグレードとして主要なセキュリティ機能を企画しているコンピュータシステムのベンダによって持ち込まれる。ベンダとセンターの初回打合せ後、開示された情報の機密性を維持するために秘密保持契約を締結する。その後、技術的な打合せを実施し、ベンダからは、評価を

希望する製品（特にその内部仕様と目的）についての詳細な情報を提供する。センターからは、基準に対する適合性評価に加え、ベンダの設計上のセキュリティ面における潜在的な強さと弱さについて、ベンダに対して専門的な評価結果を提供する。一般的に予備的な評価は、ベンダによって製品が完成し出荷準備ができた時点で完了する。完了に当たってセンターはベンダとセンター内に配付する要約レポートを作成する。これらのレポートは秘密情報を含んでいるため、公開されない。
予備的な評価を行うことに対して､ベンダは製品を完成･販売するという義務は負わない。同様に、センターは正式な製品評価を実施するかどうかは確約しない。予備的な評価は、センターまたはベンダのどちらかが、評価を続けることがもはや有効でないということを他方に書面で通知することによって完了することもある。

＜フォーマルな製品評価＞
フォーマルな製品評価は、国家安全保障機関（ＮＳＥ）で利用するためのコンピュータシステムの認定に必要なものであり、評価済み製品リストに記載される唯一の条件である。
フォーマルな製品評価は､ベンダがセンターに対して製品評価を依頼することから始まり、製品そのものと条件を満たした添付ドキュメントに基づいて評価する。
秘密保持契約が締結され、フォーマルな製品評価チームがセンター内に編成される。ベンダとの初回打合せでは、フォーマルな評価のためのスケジュールを調整する。
実装された製品に対するテストは、評価プロセスの重要な部分であるため、システムが稼動するバージョンへの評価チームによるアクセスについてベンダと調整する。ベンダから必要とされる追加のサポートは、設計書、ソースコード、および製品に関する詳細な質問に対応できるベンダ担当者への問合せを含む。評価チームは、評価中の製品に関して、基準を当てはめながら、各要件に対して製品をテストする。
評価チームはシステムに対する発見事項について最終報告書に記載する｡最終報告書は(著作権や機密情報を除いて）公に入手可能であり、システムに対する総合的な格付けならびに評価基準との比較に基づく製品についての評価チームによる発見事項の詳細が記載されている。評価チームによって発見された脆弱性に関する詳細な情報は、フォーマルな製品評価が完了する前に、可能な限り多くの問題を取り除けるように、システム開発者と設計者に提示される。脆弱性分析、さらに著作権や機密情報の扱いは、脆弱性報告プログラムを通してセンターの中で管理され、ベンダに提供されるとともに、知る必要性と秘密保持の原則のもとに米国政府内に配付される。

附録 B

各区分の評価基準の要約

トラステッド・コンピュータ・システム評価基準の基で認められたシステムの区分は以下のとおりである。各区分は、極秘及びそれ以外の機密情報を保護するためのシステムにおいて、総体的な信頼度向上のための主要点を表す。

区分 (D)：最小保護＜Minimal Protection＞

この区分は、クラスが一つだけである。評価はなされたが、上位の評価クラスに対する要件を満たせなかったシステムのために設けられた。

区分 (C)：任意（自由裁量的)保護 ＜Discretionary Protection＞

この区分におけるクラスは、任意（自由裁量) ＜知る必要性＞ 保護を規定し、かつ監査機能を含めることによって､サブジェクの責任及び彼らが始動すべきアクションを規定する。

区分 (B)：強制(的)保護＜Mandatory Protection＞

機密ラベルの完全性を保持し、それを一連の強制アクセス制御規則を実施するために使用する TCB の概念がこの区分における主要要件である。この区分におけるシステムは、システム内で、主要なデータ構造と一緒に機密ラベルを保持しなければならない。システム開発者は、また、TCB が基礎を置くセキュリティポリシーモデルを提出し、かつ TCB の仕様を提供せねばならない。リファレンスモニター・コンセプトが実装されていることを実証するために証拠を提出しなければならない。

区分 (A)：検証された保護 ＜Verified Protection＞

この区分は、システムが蓄積あるいは処理する極秘あるいはその他の機密情報を、システムで用いられる強制的及び任意（自由裁量)セキュリティ制御が効果的に保護できることを保証するフォーマルセキュリティ検証法によって特徴づけられる。TCB が設計、開発及び実装におけるすべての面でのセキュリティ要件を満たすことを実証するため、拡張証拠資料が要求される。

附録　C

各クラスの評価基準の要約

トラステッド・コンピュータ・システム評価基準(TCSEC)のシステムのクラスを以下に列挙する。
それらは、コンピュータ・セキュリティの観点から、望ましさが増す順に並べられている。

クラス（D）：最低レベルの保護

このクラスは、より高度な評価クラスに適合する要件を満たさないシステムのために予約されている。

クラス（Ｃ１）：任意（自由裁量的)セキュリティ保護

クラス（Ｃ１）のトラステッド・コンピューティング・ベース（ＴＣＢ）は名目上、ユーザとデータを分離することで任意(自由裁量)のセキュリティ要件を満たしている。それは、個別にアクセス制限を強制することが可能な、信頼できるいくつかの制御形式を組込んでいて、表面上はプロジェクトや個人情報を保護し、かつ、ユーザに対して他のユーザがデータを誤って読出したり、破壊したりすることから守れるようにするのに適している。クラス（Ｃ１）の環境は同一レベルの機密度でデータを処理する共同ユーザの一人となることが期待されている。

クラス（Ｃ２）：制御付きアクセス保護

このクラスに属するシステムは、ログイン手順、セキュリティ関連イベントの監査およびシステム資源の隔離を通して、ユーザにおのおのの行動に対する責任を与えることにより、（Ｃ１）システムよりさらにきめ細かな任意（自由裁量)のアクセス制御を強制する。

クラス（Ｂ１）：ラベル付きのセキュリティ保護

クラス（Ｂ１）のシステムはクラス（Ｃ２）の特長要件をすべて要求する。それに付加して、セキュリティポリシーモデル、データのラベル付けや名前付きサブジェクトとオブジェクトに関する強制アクセス制御などのインフォーマルな宣言がなければならない。また、正確にラベル付けされたエクスポート情報のための機能が存在しなければならない。さらに、検査によって確認されたいかなる不具合も除去されねばならない。

クラス（B2)：構造化された保護

クラス（B2)のシステムにおいては、TCB は、明瞭に定義され、文書化されたフォーマル・セキュリティポリシー・モデルに基づき、クラス（B1）のシステムに見られる任意（自由裁量)および強制アクセス制御の強制が自動データ処理（ADP）システム中の全サブジェクトとオブジェクトに拡張されることを要求する。それに加えて、隠れチャネルに言及される。TCB は保護が重要な要素と非保護が重要な要素へと注意深く構造化されなければならない。

このTCBインタフェースは必要十分に定義されていて、TCBの設計と実装が、より完全な検査とレビューを受けることを可能にする。認証メカニズムが強化され、システム管理者やオペレータの機能に対するサポート形式において信頼できる設備管理が提供され、さらに厳重な構成の管理制御が導入される。このシステムは侵入に対して相対的に抵抗力がある。

クラス（B3)：セキュリティドメイン

クラス（B3)のTCBはサブジェクトからオブジェクトへの全てのアクセスを仲介すると言うリファレンスモニターの要件を満たし、不正な変更に耐え、解析と検査を行うのに十分小型でなければならない。

最終的には、TCBは複雑性を最少化する方向で、TCB設計と実装を通じての重要なシステム・エンジニアリング活動によって、セキュリティポリシーを適用するためには必須でないコードを除外するために構造化される。そして、セキュリティ管理者がサポートを受け、監査メカニズムが信号セキュリティがらみのイベントへ拡張され、システムの回復手順が要求される。当システムは侵入に対して強い耐性がある。

クラス（A1)：検証された設計

クラス（A1)のシステムは機能上はクラス（B3)のシステムと等価で、そこには、いかなる付加的なアーキテクチャ上の特徴もポリシーの要件も追加されない。このクラスのシステムの際立った特徴は、フォーマルな設計仕様と確認技術から導かれた解析と、その結果TCBが正しく実装されていることへの高度な保証である。この保証は、現実には発展的なもので、セキュリティポリシーのフォーマルなモデルと設計に関するフォーマルな最上位仕様（FTLS)によって始められる。

クラス（A1)のシステムに必要なTCBの厖大な設計と発展的な解析を維持することで、一層厳格な構造の管理が要求され、サイトに対して安全にシステムを頒布（distributing)させる手順が確立される。システムセキュリティ管理者がサポートされる。

附録 D

要件一覧

この附録は「トラステッド・コンピュータ・システム評価基準（TCSEC)」に定義された要件をクラス順というよりアルファベット順に一覧にしたものである。この一覧は全クラスを通じたある要件の展開において役立てようとするものである。各要件に対して 3 つの型の基準が示されている。各型は以下のことを示す NEW，CHANGE，または ADD という単語から始まっている。

NEW：下位クラスにある任意の基準は，次に続く基準によって取って代わられる。

CHANGE：次に続く基準は下位のクラスにあっても，当該クラスのために変更される。前に規定された基準への特定の変更を示すのに，強調表示が使われる。

ADD：次に続くどの下位クラスにおいても要求されなかった基準は、当該クラスにおいてこの要件に対して前に規定された基準に付加される。

省略形は以下のように使われる：

NR：（要件なし）この要件はこのクラスには含まれない。

NAR：（追加要件なし）この要件は前のクラスからは変更されない。

読者は要件に対しての新たな基準をそのクラスの完全な前後関係の中で設定する場合には，本文書のパート I を参照されたい。

図 1 は全クラスを通じて要件の展開の概要を図示したものである。

監査

C1： NR.

C2： NEW：TCB は保護対象のオブジェクトへのアクセス監査証跡を生成し、維持し、そして修正あるいは不正アクセスあるいは破壊から保護することができなければならない。監査データは，それへの読取りアクセスが承認された者に限定されるように，TCB によって保護されるべきである。
TCB は次に示すようなタイプの事象を記録できなければならない。:
識別番号の利用と認証メカニズム，ユーザドレス空間へのオブジェクトの導入（例えばファイルオープンやプログラムの開始)，オブジェクトの消去，そしてコンピュータオペレータとシステム管理者，システムセキュリティ責任者と他のセキュリティ関連

事象のうちの両方か、もしくはそのいずれかによる活動。
それぞれの記録された事象に対して,監査レコードは以下を特定する:事象発生日時,ユーザ，事象タイプ，事象の成功・不成功の区別。
識別／認証の事象に対して，その要求元（例えば端末 ID）は監査レコードに含まれなければならない。オブジェクトをユーザドレス空間へ導入する事象およびオブジェクトを消去する事象に対しては，監査レコードはオブジェクトの名前を含まなければならない。ADP システムの管理者は，個別属性に基づく任意の 1 人かそれ以上のユーザの活動を選択的に監査できなければならない。

B1：CHANGE：オブジェクトをユーザドレス空間へ導入する事象とオブジェクトを消去する事象については，監査レコードはオブジェクト名およびオブジェクトのセキュリティレベルを含まなければならない。ADP システムの管理者は，個別属性に基づく任意の 1 人かそれ以上のユーザの活動と，オブジェクトのセキュリティレベルのうち，両方もしくはいずれか一方を選択的に監査できなければならない。
ADD：TCB は人間に可読な出力表示のマーキングのいかなる書換えも監査できなければならない。

B2：ADD：TCB は隠れストレージチャネルの利用において用いられる特定された事象を監査できなければならない。

B3：ADD：TCB はセキュリティポリシーの差し迫った侵害を暗示するセキュリティ監査可能事象の発生または蓄積をモニターできるメカニズムを包含しなければならない。このメカニズムは，閾値を超えた時点でセキュリティ管理者に直ちに通知することができ，もしこれらセキュリティ関連事象の発生もしくは累積が続くようなら，その事象を終結させるため，システムは破壊的行為を止めなければならない。

A1：NAR.

構成管理

C1：NR.
C2：NR.
B1：NR.

B2：NEW：TCB を開発し維持している間は，構成管理システムは，記述された最上位レベル仕様，他の設計データ，実装作業用文書，ソースコード，オブジェクトの現行バージョン，および試験結果とその文書の変更管理を維持するために，しかるべく機能していなければならない。構成管理システムは，全文書と現行バージョンに対応したコードの間の首尾一貫した対応関係を保証しなければならない。ソースコードから

TCB の新バージョンを生成するためのツール類を準備する必要がある。また，意図された変更のみが TCB の新バージョンとして実際使われるコードの中に加えられていることを確かめるために新たに生成したバージョンと前の TCB バージョンとを比較する目的にも，ツール類が利用可能になっていなければならない。

B3：NAR.

A1：CHANGE：全ライフサイクル中，即ち TCB の設計，開発，保守の間，フォーマルモデル，フォーマルにかつ記述された最上位レベル仕様，他の設計データ，実装作業用文書，ソースコード，オブジェクトの現行バージョン，および試験結果とその文書への変更管理を維持する構成管理システムは,全てのセキュリティ関連ハードウェア，ファームウェア，ソフトウェアに対して，しかるべく機能しなければならない。また，意図された変更のみが, TCB の新バージョンとして実際に使われるコードの中に加えられていることを確かめる目的で新たに生成したバージョンと前の TCB バージョンとを比較するためのツール類が厳格な構成管理の下で維持され，利用可能になっていなければならない。
ADD：技術的，物理的，手続き的な保全措置の組合せを用いて，TCB の生成に使われる全素材のマスターコピーまたはコピーを無認可の改変もしくは破壊から保護しなければならない。

隠れチャネル解析

C1：NR.
C2：NR.
B1：NR.

B2：NEW：システム開発者は，隠れストレージチャネルの悉皆探索を実行し，確認された各チャネルの最大バンド幅を決定する（実測または工学的評価法のどちらかを用いて)。(隠れチャネルガイドラインセクションを見よ)

B3：CHANGE：システム開発者は，隠れチャネルの悉皆探索を実行し，確認された各チャネルの最大バンド幅を決定する（実測または工学的評価法のどちらかを用いて)。

A1：ADD：解析にはフォーマルな手法が使われる。

設計文書

C1：NEW：メーカの保護体系の記述およびこの体系がどのように TCB に変換されるかが説明された文書が利用可能でなければならない。もし TCB が別個のモジュールから構成されるならば，これらモジュール間のインタフェースも記述されていなければならない。

C2：NAR.

B1：ADD：TCB により実行されるセキュリティポリシーモデルに関するインフォーマルあるいはフォーマルな説明が利用可能であって，セキュリティポリシーを実行する上で十分であると言える説明がなされていなければならない。具体的な TCB 保護メカニズムが確認され，それがモデルを満足することを示す説明がなされていなければならない。

B2：CHANGE：TCB モジュール間のインタフェースは記述されている必要がある。TCB によって実行されるセキュリティポリシーモデルのフォーマルな記述は利用可能であって，かつセキュリティポリシーを実行することが十分であることが証明されていなければならない。

ADD：最上位仕様（DTLS）は，TCB インタフェースの記述が正確であることを示していなければならない。文書は TCB がどのようにしてリファレンスモニターの概念を実装するのか，またなぜそれが耐タンパであり，パイパス困難であり，そして正しく実装されるのかについて記述していなければならない。文書は，検査を円滑に進め，最少特権を実行するために，TCB がどのように構造化されているのかについて，記述しなければならない。この文書はまた，隠れチャネルの解析結果およびチャネルの制限に関与したトレードオフを提示すべきである。既知の隠れストレージチャネルの利用に用いられる全ての監査可能な事象は識別されなければならない。既知の隠れストレージチャネルのバンド幅は，監査メカニズムではそれが使われていることを検知できないが，示されていなければならない。（隠れチャネルガイドラインセクションを見よ）

B3：ADD：TCB の実装（ハードウェア，ファームウェア及びソフトウェアにおける）は，DTLS と合致していることがインフォーマルに示されるべきである。DTLS の要素が TCB の要素に対応していることが，インフォーマルな技法を使って示されなければならない。

A1：CHANGE：TCB の実装（ハードウェア，ファームウェア及びソフトウェアにおける）は，フォーマル最上位仕様（FTLS）と合致していることを，インフォーマルに示されなければならない。FTLS の要素が TCB の要素と対応していることが，インフォーマルな技法を使って示されるべきである。

ADD：FTLS においては扱われなく,しかしながら厳密には TCB 内部にある(例えば，マッピングレジスタ，直接メモリアクセス入出力）ハードウェア，ファームエア及びソフトウェアのメカニズムは，明確に記述されていなければならない。

設計仕様と検証

C1：NR

C2：NR

B1：NEW： TCB がサポートするセキュリティポリシーのインフォーマルモデルおよびフォーマルモデルは、自動データ処理（ADP）システムのライフサイクルを通してモデルの公理と一貫性があることを示すように、保守されなければならない。

B2：CHANGE：TCB がサポートするセキュリティポリシーのインフォーマルモデルおよびフォーマルモデルは、自動データ処理（ADP）システムのライフサイクルを通してモデルの公理と一貫性があることを示すように、保守されなければならない。

B2：ADD： TCB の最上位仕様(DTLS)は、TCB の例外、 エラーメッセージ、および効果の観点から完全かつ正確に TCB を記述するように保守されなければならない。また、DTLS が TCB のインタフェースの正確な記述となっていることが示されなければならない。

B3：ADD： DTLS がモデルと一貫性を持っていると納得できるだけの論拠が与えられなければならない。

A1：CHANGE： FTLS が TCB のインタフェースの正確な記述であることが示されなければならない。DTLS がモデルと一貫性を持っていると納得できるだけの論拠が与えられなければならず、かつ、FTLS がモデルと一貫性を持っていることを示すためにフォーマル、インフォーマルな手法が組み合わせて用いられなければならない。

A1：ADD： TCB のフォーマル最上位仕様 (FTLS)は、TCB の例外、 エラーメッセージ、および効果にの観点から完全かつ正確に TCB を記述するように保守されなければならない。もしハードウェアまたはファームウェアの特性が TCB のインタフェース上で可視であるなら、DTLS と FTLS は、ハードウェアまたはファームウェア（あるいは両方)として実装された TCB の構成要素についての記述を含まなければならない。上記のことを検証した証明は、コンピュータセキュリティセンターが推奨して提供する最先端のフォーマル仕様とそれに使われる検証の仕組みとも一貫性がなければならない。正しい実装が行われた証拠として、FTLS から TCB のソースコードへの手作業による写像、あるいは他の方法による写像が実施されなければならない。

装置ラベル

C1：NR

C2：NR

B1：NR

B2：NEW： TCB は接続された全ての物理的装置に対し、最少および最大のセキュリティレベルを設定可能であり、これらのセキュリティレベルは、装置の置かれた場所の物理的環境によって生じる制約を強制するために TCB によって使われるべきである。

B3：NAR

A1：NAR

任意（自由裁量的)アクセス制御

C1：NEW： TCB は、自動データ処理（ADP）システムにおける名前付きのユーザと名前付きのオブジェクト(例えば ファイルやプログラム)の間のアクセスを定義し制御しなければならない。強制メカニズム (例えば self/group/public 制御、 アクセス制御リスト) によって、ユーザがオブジェクトの共有を名前付きの個人、または定められたグループ(あるいはその両方)を単位として、指定および制御できなければならない。

C2：CHANGE： 強制メカニズム (例えば self/group/public 制御、 アクセス制御リスト) によって、ユーザがオブジェクトの共有を名前付きの個人、または定められたグループ(あるいはその両方)を単位として、指定および制御できなければならない。また、同メカニズムはアクセス権の伝播を制限する制御方法を提供しなければならない。

C2：ADD： 任意（自由裁量的)アクセス制御メカニズムは、明示的なユーザの操作によって、あるいはデフォルトで、正式な許可なしのアクセスからオブジェクトを保護しなければならない。こういったアクセス制御は単一ユーザの粒度でアクセスを可能にしたり不可能にしたりする能力を持たなければならない。オブジェクトへのユーザ毎のアクセス許可権限は、まだ付与されていない場合、正式な許可ユーザによってのみ付与されなければならない。

B1：NAR

B2：NAR

B3：CHANGE： 強制メカニズム (例えば アクセス制御リスト) によって、ユーザがオブジェクトの共有を指定および制御できなければならない。また、同メカニズムはアク

セス権の伝播を制限する制御方法を提供しなければならない。こういったアクセス制御は、名前付きのオブジェクトそれぞれについて、名前付きの個人のリストや名前付きの個人からなるグループのリストと、それらのリスト毎のオブジェクトに対するアクセスモードを指定できる能力を持たなければならない。

B3：ADD： その上、それぞれの名前付きのオブジェクトについて、強制メカニズムは、オブジェクトへのアクセスが与えられない名前付きの個人のリストおよび名前付きの個人からなるグループのリストを指定することが可能でなければならない。

A1：NAR

ラベル付けされた情報のエクスポート

C1：NR

C2：NR

B1：NEW： TCB は、それぞれの通信チャネルおよび I/O 装置を、単一レベル装置またはマルチレベル装置であると指定しなければならない。この指定のいかなる変更も手作業で行われなければならず、また TCB によって監査可能でなければならない。TCB は、通信チャネルや I/O 装置のセキュリティレベルのいかなる変更も保持し、かつ、いかなる変更も監査可能でなければならない。

B2：NAR

B3：NAR

A1：NAR

マルチレベル装置へのエクスポート

C1：NR

C2：NR

B1：NEW： TCB がオブジェクトをマルチレベル I/O 装置にエクスポートする際、そのオブジェクトに紐づけられた機密ラベルも一緒にエクスポートされなければならず、エクスポートされた情報と同じ物理媒体に同じ形式（機械データもしくは自然言語等）で記録されなければならない。TCB がオブジェクトをマルチレベル通信チャネルにエクスポート、あるいはインポートする際、そのチャネルで使用されるプロトコルは、送受される情報と、その機密ラベルの組を明確に示さなければならない。

B2：NAR

B3：NAR
A1：NAR

単一レベル装置へのエクスポート
C1：NR
C2：NR

B1：NEW： **単一レベル I/O 装置および単一レベル通信チャネルは、処理している情報の機密ラベルを保守する必要がない。しかしながら TCB は、単一レベルの通信チャネルまたは I/O 装置を介してインポートあるいはエクスポートされる情報の単一のセキュリティレベルを確保するために、TCB と許可されたユーザが信頼して通信するメカニズムを含まなければならない。**

B2：NAR
B3：NAR
A1：NAR

識別と認証
C1：NEW： **TCB が調停することになっている動作をユーザが始めるより前に、TCB はユーザがユーザ自身であることを識別するようユーザに要求しなければならない。そのうえ TCB はユーザの真正性を確認するために（パスワード等の）保護機構を使用しなければならない。TCB は正式な許可されていないユーザがアクセスできないように認証データを保護しなければならない。**

C2：ADD： **TCB は自動データ処理（ADP）システムの個別のユーザをユニークに識別する能力を提供することで個人に責任を強制できなければならない。TCB はまたこの個人の識別とその個人がとるすべての監査可能な動作を関連付ける能力を提供しなければならない。**

B1：CHANGE： **さらに TCB は個別のユーザの真正性を確認するための情報（パスワードなど）を含む認証データを保持しなければならない。TCB は、個別のユーザのクリアランスと認可を決定するための情報も同様に保持しなければならない。これらのデータはユーザの真正性を認証するために TCB に利用されなければならない。また個別のユーザに代わって動作するために作られる TCB 外にあるサブジェクト（アクセスの主体）のセキュリティレベルと認可がそのユーザのクリアランスと認可によって支配されることを保証するためにも、これらのデータは TCB に利用されなければならない。**

B2：NAR
B3：NAR
A1：NAR

ラベルの完全性

C1： NR.
C2： NR.

B1： NEW： 機密ラベルは、それらが関連する特定のサブジェクトまたはオブジェクトのセキュリティレベルを正確に表さなければならない。
TCB によってエクスポートされる時に、機密ラベルは内部ラベルを正確にかつ明確に表すこととし、エクスポートされようとしている情報に付随されなければならない。

B2： NAR.
B3： NAR.
A1： NAR.

人間の判読可能な出力のラベル化

C1： NR.
C2： NR.

B1： NEW：ＡＤＰシステム管理者は、エクスポートされる機密ラベルに関連性のある表記可能なラベル名を指定できなければならない。TCBは、人間に可読でページ付けされている全てのハードコピー出力(例えばラインプリンタ出力)の始めと終わりに、その出力の機密度を正確に*表現する人間に可読な機密ラベルをマークしなければならない。
TCB はデフォルトで、人間の判読可能なハードコピー出力(例えばラインプリンタ出力)の各ページの上部と下部に、その出力の全体的な機密度を正確に*表現する、あるいはそのページ上の情報の機密度を正確に*表現する､人間に可読な機密ラベルをマークしなければならない。
TCB はデフォルトで、そして適切な方法により、人間に可読な他の様式の出力（例えば、マップ、グラフィックス）に、その出力の機密度を正確に*表現する、人間に可読な機密ラベルをマークしなければならない。これらのデフォルトのマーキングに対する、いかなる書換えも TCB により監査可能としなければならない。

B2： NAR.
B3： NAR.

A1： NAR.
*

ラベル
C1： NR.
C2： NR.
B1： NEW：制御下にある各サブジェクトおよび記憶オブジェクト(例えばプロセス、ファイル、セグメント、装置)に関連性のある機密ラベルは、ＴＣＢによって維持されなければならない。これらのラベルは、強制アクセス制御決定の基礎として使用されなければならない。ラベルが付けられていないデータをインポートするために、ＴＣＢは、正式に許可されたユーザにデータのセキュリティ・レベルを要求し、それを受け取らなければならない。また、そのようなアクションはすべてTCBにより監査可能としなければならない。
B2： CHANGE：ＴＣＢ外部のサブジェクトにより直接あるいは間接的にアクセスできる各ＡＤＰシステムリソース(例えばサブジェクト、記憶オブジェクト、ＲＯＭ)に関連性のある機密ラベルは、ＴＣＢによって維持されなければならない。

B3： NAR.
A1： NAR.

強制(的)アクセス制御
C1： NR.
C2： NR.
B1： NEW：TCBは、自らのコントロールの下にあるあらゆるサブジェクトとストレージ・オブジェクト(すなわちプロセス、ファイル、セグメント、デバイス)に対して強制アクセス制御のポリシーを実施しなければならない。これらのサブジェクトとオブジェクトは、階層的な機密度区分レベルと階層的でないカテゴリーとの組み合わせである機密ラベルを割り当てられることとし、そのラベルは強制アクセス制御の決定のための基礎として使われなければならない。TCBは、ふたつ以上のそのようなセキュリティレベルをサポートできることとする。(強制アクセス制御ガイドラインを参照。)以下の要求事項は、TCBによつて制御されるすべてのサブジェクトと、これらのサブジェクトによる直接または間接的にアクセス可能なすべてのオブジェクトとの間のすべてのアクセスにあてはまらなければならない：サブジェクトのセキュリティレベルにおける階層区分が、オブジェクトのセキュリティレベルにおける階層区分より大きいかあるいは等しく、そして、サブジェクトのセキュリティレベルにおける階層的でないカテゴリがオブジェクトのセキュリティレベルの階層的でないカテゴリの全てを含むのであれば、サブジェクトはオブジェクトを読むことができる。サブジェクトのセキュリティレベルにおける階層区分が、オブジェクトのセキュリティレベルにおける

階層区分より小さいかあるいは等しく、そして、サブジェクトのセキュリティレベルにおける階層的でないカテゴリの全てがオブジェクトのセキュリティレベルにおける階層的でないカテゴリに含まれるのであれば、サブジェクトはオブジェクトに書くことができる。識別と認証のデータは、ユーザの本人性を認証するために、そしてまた、個々のユーザのために動作するよう作成されるTCB外のサブジェクトのセキュリティレベルと認可がそのユーザのクリアランスと認可によって支配されることを保証するために、TCBにより使われなければならない。

B2： CHANGE：ＴＣＢは、ＴＣＢ外部のサブジェクトによって直接あるいは間接的にアクセス可能な、すべての資源(つまりサブジェクト、ストレージオブジェクト、I/0装置)に対して強制アクセス制御のポリシーを実施しなければならない。次の要求事項が、ＴＣＢ外のすべてのサブジェクトと、これらのサブジェクトによって直接あるいは間接的にアクセス可能なすべてのオブジェクト間のあらゆるアクセスにあてはまらなければならない：

B3： NAR.
A1： NAR.

オブジェクト再使用

C1： NR
C2：NEW：未使用のストレージ・オブジェクトの TCB のプールからサブジェクトへの初期の割り当て、配分、または再配分に先がけて無効にすべきである。システムにリリースバックされているオブジェクトにアクセスできるいかなるサブジェクトも、事前のサブジェクトの動作によって生成される暗号化表現が含まれる情報を利用できてはならない。

B1： NAR
B2： NAR
B3： NAR
A1： NAR

セキュリティに特化したユーザズガイド

C1： NEW： ユーザドキュメントの中の単一の要約、章、またはマニュアルは、TCB によって提供されたプロテクション機構、機構利用におけるガイドライン、及び機構がどのように相互に影響するかを記述しなければならない。

C2： NAR

B1： NAR
B2： NAR
B3： NAR
A1： NAR

セキュリティ検査

C1： NEW： **自動データ処理（ADP）システムのセキュリティ機構は、システムドキュメントにより要求されるようにテストされ動作するか調査しなければならない。テストは、未認証のユーザが迂回するか、さもなければ TCB のセキュリティプロテクション機構を破る明らかな方法が全くないことを保証するために行われなければならない。(参照 セキュリティ テスティング ガイドライン)**

C2： ADD： **テストは、また、資源分離の違反を可能にするか、監査または認証データへの不正アクセスを許すかもしれない明らかな弱点に対する調査を含まなければならない。**

B1： NEW： **自動データ処理（ADP）システムのセキュリティ機構は,、システムドキュメントにより要求されるようにテストされ動作するか調査しなければならない。TCB の特徴の実施を完全に理解する個人からなるチームは、そのデザインドキュメント、ソースコード、およびオブジェクトコードの徹底的な分析とテストに従事することになる。それらのオブジェクトは次のようでなければならない：TCB により求められる強制または任意（自由裁量)のセキュリティポリシーの下で正常に拒否されたデータを読み、変更、削除するために、TCB の外のサブジェクトを許すというすべてのデザインとインプリメンテーションの弱点を摘発すること。; いかなるサブジェクトも、（そのような認可なしで）他のユーザが開始したコミュニケーションに応じられないような状態にして、TCB に入れないようにするのを保証するのと同様である。すべての発見された弱点は削除されるか、無効にされることとし、TCB はそれらが取り除かれていて、新しい弱点が導入されていないことを証明するために、再テストしなければならない。(参照 セキュリティ テスティングガイドライン)**

B2： CHANGE： **すべての発見された弱点は訂正されなければならず、かつ、それらが取り除かれて、新しい弱点が導入されていないことを証明するために、TCB は再テストされなければならない。**

ADD： **TCB は相対的に侵入に抵抗力があるのを発見されなければならない。テストは、TCB インプリメンテーションが記述的なトップレベルの仕様と一致していることを証明しなければならない。**

B3： CHANGE： TCB は相対的に侵入に抵抗力があるのを発見されなければならない。

ADD： 設計上の欠陥、修正可能な実装上の欠陥のいくつかはテスト中に発見されないかもしれないが、そのような欠陥はほとんど残っていないという妥当な信頼をおくこととする。

A1： CHANGE： テストすることは、TCB インプリメンテーションがフォーマルなトップレベルの仕様と一致していることを証明しなければならない。

ADD： マニュアルもしくは FTLS からソースコードへのマッピングを侵入試験の基礎としてもよい。

サブジェクト センシィティビティ ラベル

C1： NR

C2： NR.

B1： NR.

B2： NEW： TCB は直ちに、対話型セッションの間にそのユーザと関連したセキュリティレベルにおける各変化を、ターミナルユーザに通知しなければならない。ターミナルユーザは、サブジェクトの完全なセンシィティビティラベルを表示するために、必要に応じ TCB に質問できなければならない。

B3： NAR

A1： NAR

システムアーキテクチャ

C1： NEW：TCB は、外部からの妨害または改ざん(例えばコードまたはデータ構造の部分修正による)から自らの保護を実行するためにドメインを維持しなければならない。TCB によってコントロールされたリソースは通常、自動データ処理（ADP）システムの中でサブジェクトとオブジェクトで定義されたサブセットとなる。

C2： ADD：リソースがアクセス制御と監査要件の対象であることから、TCB は保護のためにリソースを分離しなければならない。

B1： ADD： TCB は TCB のコントロール下で別アドレス空間を提供することを通してプロセス分離を維持しなければならない。

B2： NEW：TCB は、外部の干渉または改変(例えばコードまたはデータ構造の部分修正による)からTCBを保護するTCB自身の実行のためにドメインを維持しなければならない。TCB は、TCB のコントロール下で別アドレス空間の提供を通してプロセス分離を維持しなければならない。TCB の大部分は独立モジュールの中で内部的に構造化されなければならない。TCB は、保護の危機にない要素から、危機にある要素を分離するために、入手可能なハードウェアを効果的に利用しなければならない。TCB モジュールは最少特権の原則が強化されるように設計されなければならない。セグメント化などのハードウェア機能は、個々の属性（すなわち：読込可能、書込可能）を備えた論理上別個のストレージ・オブジェクトを支援するのに使われなければならない。TCB へのユーザインタフェースは完全に定義され、TCB の要素はすべて識別されなければならない。

B3： ADD： TCB は、正確に定義された意味論を備えた 完全で、概念的に単純な保護メカニズムを使用するよう設計され構造化されなければならない。このメカニズムは、TCB とそのシステムの内部構造を強化する際に中心的な役割を果たさなければならない。TCB は、レイヤー化、抽象化およびデータ隠蔽という重要な効用を組み込まなければならない。重要なシステム工学は、TCB の複雑さを最小限にし、保護の危機にない TCB モジュールを除くように指向しなければならない。

A1： NAR

システムの完全性

C1：ＮＥＷ：ハードウェアおよび(または)ソフトウェアの機能（features）は、TCB の実地におけるハードウェアおよびファームウェア要素の正確なオペレーションを定期的に確認するために使用できるように備えられなければならない。

C2：NAR
B1：NAR
B2：NAR
B3：NAR
A1：NAR

検査証拠資料

C1：システム開発者は、テスト計画について記述したドキュメント、セキュリティ・メカニズムがどのようにテストされたかを示すテスト手続き、およびセキュリティ・メカニズムの機能的なテストの結果を、評価者に提供しなければならない。

C2： NAR.
B1： NAR.

B2： ADD： それは、隠れチャネルのバンド幅を減らすために使われた方法の有効性を検査した結果を含まなければならない。

B3： NAR.

A1： ADD：フォーマルな最上位仕様と TCB ソースコードの間のマッピングの結果が与えなければならない。

信頼できる配布

C1： NR.
C2： NR.
B1： NR.
B2： NR.
B3： NR.

A1： NEW：信頼できる ADP のシステム制御と配布設備が、TCB の現在の版（現バージョン）を示すマスタデータと現行版のコードのオンサイトにおけるマスタコピーの間のマッピングの完全性を維持するために提供されなければならない。顧客に配付された TCB ソフトウェア、ファームウェア、およびハードウェアの更新が、マスタコピーによって規定された正にそのとおりであることを保証するための手続(例えば現場でのセキュリティ承認検査)が存在しなければならない。

信頼できる設備管理

C1： NR.
C2： NR.
B1： NR.

B2： NEW：TCB は、オペレータと管理機能の分離をサポートしなければならない。

B3： ADD：セキュリティ管理者の役割の下で実行される機能は、それ以外の機能と区別されなければならない。ADP システムの管理要員は、対象となる ADP システム上でセキュリティ管理者の役割を確立するための明確な監査可能行動を取った場合にのみ、セキュリティ管理機能を実行できるようにすべきである。セキュリティ管理役割において実施できる非セキュリティ機能は、セキュリティ役割を効果的に実行するのに必

須の事項に厳密に制限されなければならない。セキュリティ管理の役割内で実行される非セキュリティ機能は、効率的なセキュリティの役割遂行に必要なもののみに制限されなければならない。

信頼できる設備マニュアル

C1： NEW：自動データ処理（ADP）システム管理者向けのマニュアルは、セキュア設備を使用する時に制御されるべき機能と特権について警告を示さなければならない。

C2： ADD：各タイプの監査イベントの詳細な監査記録構造と同じく監査ファイルを検査し、維持するための手続が与えられなければならない。

B1： ADD： マニュアルは、利用者のセキュリティ特性を変更することを含めオペレータと管理者のセキュリティ関連機能を説明しなければならない。システムの保護機能の一貫した効率的な利用、その機能がどのように相互に作用するか、安全に新しい TCB をどのように生成するか、そして安全な方法で設備を運営するために制御される必要のある設備の手続や警告、特権に関するガイドラインをマニュアルは提供しなければならない。

B2： ADD： リファレンス検証機構を含んでいる TCB モジュールが明確にされなければならない。TCB 内の任意のモジュールの修正後の新しい TCB のソースからの安全な生成の手続きが示されなければならない。

B3： ADD：システムが安全な方法で最初から起動されることを保証する手続をマニュアルは含まなければならない。また、システム操作のいかなる経過の後の安全なシステム操作を再開する手続が含まなければならない。

A1： NAR.

トラステッド・パス

C1： NR.

C2： NR.

B1： NR.

B2： NEW： TCB は、それ自身とユーザ間の初期のログインと認証のためのトラステッド・コミュニケーション・パスをサポートするものでなければならない。このパス経由の通信は、もっぱらユーザによって始められなければならない。

B3： CHANGE： ユーザへの積極的な TCB 接続が要求される場合(例えば、ログインし、

オブジェクトのセキュリティ・レベルを変更する)、 TCB は、それ自体と利用ユーザ間の信頼されたコミュニケーション・パスをサポートしなければならない。このトラステッド・パスによるコミュニケーションはもっぱらユーザあるいは TCB によって活性化されるものとし、 論理的に分離され、かつ、他の経路から誤りなく区別できなければならない。

信頼できる復旧

C1： NR.

C2： NR.

B1： NR.

B2： NR.

B3： NEW： ADP システムの故障もしくは他の障害に対して、故障前のシステム保護水準維持した状態で復旧できることを保証する手続きや機構を提供しなければならない。

A1： NAR.

用語集

Access＜アクセス＞
サブジェクトとオブジェクト間で片方から他方へ情報の流れが生じることになる特定の相互作用。

Approval/Accreditation＜承認/認定＞
運用環境において機密情報を扱う ADP システムを許可する形式的な認定であって、そのシステムのハードウェア、ファームウェア、ソフトウェアセキュリティ設計、構成、導入、またその他システムの手続、管理、物理的、テンペスト、要員及び通信のセキュリティ制御の組み込みについての包括的なセキュリティ評価に基づき行われる。

Audit Trail＜監査証跡＞
集合的に提供される一連の記録で、オリジナルのデータ処理から関連する記録と報告まで前方向へ、あるいは同様に記録と報告からそれらの構成要素であるソースとなるデータ処理まで逆方向へのトレースを支援するために利用される、処理の事実を記録した証拠をいう。

Authenticate＜認証＞
主張された識別情報の確認の立証。

Automatic Data Processing (ADP)System＜ADP システム＞
人間の介入を最小限にして、データを分類、整列、計算、集計、要約、送受信、保管、検索の目的で構築されたひとまとまりのハードウェア、ファームウェア、ソフトウェア。

Bandwidth＜バンド幅＞
一定時間内に通過させることができる情報量を示す通信チャネルの特性。通常、bit/秒で表される。

Bell-LaPadula Model＜Bell-LaPadula モデル＞
一連のアクセス制御ルールを記述したコンピュータ・セキュリティ・モデルを数学的に定式化した状態遷移モデル。この形式を整えたモデルでは、コンピュータシステムの構成要素は、サブジェクトとオブジェクトという概念的な二つのセットに分類される。
セキュアな状態の概念が定義され、また各々の状態遷移がセキュアな状態からセキュアな状態へ移動することからセキュリティが保たれることが分かる。
このようにして、対象とするシステムがセキュアであることが帰納的に証明される。
もし、サブジェクトからオブジェクトへ許可されるアクセス・モードだけが、特定のセキュリティポリシーに従うようになっているならば、システムの状態は"セキュア"であると定義される。
特定のアクセス・モードが許可されるか否か決めるために、アクセス主体が持つ機密情報

アクセス資格(クリアランス)がアクセス対象の機密種別(クラス)と比較され、そして、アクセス主体に対して特定のアクセス・モードが許可されるか決定される。
機密情報アクセス資格／機密種別のスキームは、束構造という言葉によって表現される。
Lattice, Simple Security Property, *-Property も参照のこと。

Certification(evaluation)＜認証評価＞
システムのセキュリティ機能 (feature) の技術的評価であり、承認・認定プロセスの一部として、かつそのプロセスを支援するためになされ、ある特定のコンピュータシステムの設計及び実装が、指定されたセキュリティ要件のセットにどの程度適合するかの範囲を明確にするもの。

Channel＜チャネル＞
システム内の情報転送パス。
そのパスに影響を及ぼすメカニズムを指すこともある。

Covert Channel＜隠れチャネル＞
あるプロセスが、システムのセキュリティポリシーを侵害するような形で情報を転送することを許してしまう通信チャネル。
「隠れストレージチャネル」、「隠れタイミングチャネル」を見ること。

Covert Storage Channel＜隠れストレージチャネル＞
隠れチャネルの一つで、一つのプロセスがある記憶位置に直接的あるいは間接的に書き込みし、他のプロセスがその記憶位置から直接的あるいは間接的に読み出しする。隠れストレージチャネルでは、典型的な方法として、異なるセキュリティレベルの二つのサブジェクトが共有する有限のリソース (例えば、ディスク上のセクター) が用いられる。

Covert Timing Channel＜隠れタイミングチャネル＞
あるプロセスが他のプロセスに情報を伝達する隠れチャネルの一つで、プロセスがシステムリソース (例えば CPU 時間) の自分の使用状態を変化させ、その操作が第二のプロセスが観測する実レスポンス時間に影響を及ぼすといった方法をとる。

Data＜データ＞
特定の物理的表現を伴う情報。

Data Integrity＜データの完全性＞
自然言語(例えば英語)またはインフォーマル(注 1)なプログラム設計表記、あるいはそれら 2 つの組み合わせで書かれる最上位仕様。

Descriptive Top-Level Specification (DTLS)＜最上位仕様(DTLS)＞
自然言語(例えば英語)またはインフォーマル(注 1)なプログラム設計表記、あるいはそれら 2 つの組み合わせで書かれる最上位仕様。

Discretionary Access Control＜任意（自由裁量的）アクセス制御＞
サブジェクトや所属するグループの独自性にもとづきアクセス制限を行う手段。その制御は、一定のアクセス権を持ったサブジェクトが全てのサブジェクトに、そのアクセス権限を（多くの場合間接的に）（強制アクセス制御に制約されない限り）譲渡することができるという意味で自由裁量である。

Domain＜ドメイン＞
ひとつのサブジェクトがアクセスできるオブジェクトの集合体。

Dominate＜支配＞
セキュリティレベル S1 の階層的分類がセキュリティ S2 のそれと同等かそれ以上で、S1 の非階層的カテゴリーが S2 のカテゴリーのすべてを部分集合として含むのであれば、S1 は S2 を支配していることになる。

Exploitable Channel＜利用可能なチャネル(経路)＞
トラステッド・コンピューティング・ベース（TCB）外部のサブジェクトによって利用可能な、または検知可能なすべてのチャネル（経路）。

Flaw Hypothesis Methodology＜欠陥仮説方法論＞
システムの仕様書とドキュメンテーションを分析した上で、欠陥の仮説を立てるシステム分析と侵入技法をいう。仮説を立てられた欠陥リストは欠陥が実際に存在する可能性に基づき、かつ欠陥が実際に存在するものと想定して、それを悪用することの容易性、適用されるコントロールまたは受容の程度に基づいて優先順位をつける。優先順位がつけられたリストはシステムの実際の検査を行う際の管理に利用される。

Flaw＜欠陥＞
システムにおける保護機能が迂回されてしまう権限委譲、欠落、見落としによるエラー。

Formal Proof＜フォーマル証明＞
各証明の段階で、1 つまたは複数の定理の真実性に対して、完全な論理的正当性を与える完全かつ納得できる数学的説明。フォーマル検証の過程では、フォーマル仕様の或る特質やコンピュータプログラムがそれらの仕様を満足することの真実性を表すのに‘フォーマル証明’を用いる。

Formal Security Policy Model＜フォーマル・セキュリティポリシー・モデル＞
セキュリティポリシーの数学的に厳密な説明。正確を期すために、モデルはシステムの初期状態、或る状態から他の状態への推移の道筋、システムの安全な状態の規定を定義しなければならない。TCB（Trusted Computing Base 参照）の基礎として受入れ可能なためには、そのモデルはシステムの初期状態が‘安全’状態であり、かつモデルが要求する全ての仮定が効力を有し、将来も全システム状態が‘安全’であることが‘フォーマル（数学論的）証明’によって支えられていなければならない。
いくつかのフォーマルモデル化技術には、状態遷移モデル、時相論理モデル、外延的意味モデル、代数的仕様モデルなどが含まれる。その一例として、文献〔２〕に Bell と LaPadula の記述したモデルを示した。
Bell LaPadula Model, Security Policy Model も参照のこと。

Formal Top-Level Specification ＜フォーマル最上位仕様（FTLS）＞
システムの仕様と正式な要件が一致することを示す定理を仮定し、正式に証明する為の正式の数学的言語で書かれた最高仕様。

Formal Verification＜フォーマル検証＞
システムのフォーマルな仕様とセキュリティポリシーモデル間（設計検証）の、あるいはフォーマルな仕様とそのプログラム実装間（実装検証）の一貫性を示すためのフォーマル証明を用いるプロセス。

Front-End Security Filter＜フロントエンド・セキュリティ・フィルタ＞
定められたセキュリティポリシーに従うデータ処理であり、処理環境外へのデータ出力、ないしは、外部のソースからデータ入力に先立ち起動される処理をいう。

Functional Testing＜機能テスト＞
正しい操作に対してシステムの公表された機能をテストするセキュリティテストの一部。

General-Purpose System＜汎用システム＞
広範・多様な問題解決を支援するために設計されたコンピュータシステム。

Granularity＜粒度＞
機構が適応可能な単位の相対的な細かさや荒さ。「一人の利用者の粒度」とは、アクセス制御機構が、任意の一人の利用者を許容ないしは排除する細かさまで適応可能であることを意味する。

Lattice＜束＞
任意の二つの要素に対する最大下界と最小上界を有する半順序集合。

Least Privilege＜最少特権＞
この原理は、サブジェクトに対する特権付与において、各サブジェクトに対して承認されたタスクの遂行に必要な最少限の特権集合（もしくは、最低限のクリアランス(*)）のみが与えられることを求めることである。
この原理が適用されたシステムでは、事故、エラー、未承認利用により発生する損害が制限される。

Mandatory Access Control＜強制（的）アクセス制御＞
ラベルによって表現されるオブジェクトに含まれる情報の機密度、および、機密情報にアクセスするサブジェクトのフォーマルな承認（クリアランス(*)等）を用いたオブジェクトへのアクセス制限方法（制御）を指す。

Multilevel Device＜マルチレベル装置＞
改ざんリスクなしに 2 つ以上の異なるセキュリティ・レベル（機密度）のデータを同時に処理できる装置を指す。
これを達成するため、機密ラベルは、処理対象データと同じ物理メディアに同じ形式（機械読取もしくは人間可読）で保管される。

Multilevel Secure＜マルチレベルセキュア＞
異なる機密度が設定された複数の情報を保有するシステムクラスを指す。
このクラスのシステムは、セキュリティ・クリアランスや「知る必要性(needs-to-know)」が異なるユーザによる同時アクセスを許容しながら、各ユーザが承認されていない情報にアクセスすることを防ぐことができる。

Object＜オブジェクト＞
情報を含んでいるか若しくは受理する受動の実在。
オブジェクトへのアクセスは、それが含んでいる情報への潜在的なアクセスを意味する
オブジェクトの例としては、レコード、ブロック、ページ、セグメント、ファイル、ディレクトリー、ディレクトリーツリー、およびプログラムがあり、同様の例として、ビット、バイト、ワード、フィールド、プロセッサー、ビデオディスプレイ、キーボード、クロック、プリンタ、ネットワーク・ノードなどがある。

Object Reuse＜オブジェクト再利用＞
1 つ以上のオブジェクトを含む媒体(例:ページフレーム、ディスクセクター、MT)をサブジェクトに割り当てること。
安全に割り当てる為には、対象となる媒体に、以前のオブジェクトの残データが含まれてはならない。

Output＜出力＞
トラステッド・コンピューティング・ベース（TCB）によってエクスポートされた情報。

Password＜パスワード＞
識別情報を認証するために使用される秘密の文字列。

Penetration Testing＜侵入検査＞
システムのセキュリティ機能(feature)の回避を侵入者が試みるセキュリティ検査の一部。侵入者はシステムデザインおよびインプリメンテーション・ドキュメンテーション（それはシステムソースコード､マニュアルおよび回路図形のリストを含んでいるかもしれない）をすべて使用すると仮定される。侵入者は一般のユーザに適用される制約を課されない環境で検査を実施する。

Process＜プロセス＞
実行中のプログラム。
それは、単一の現実行ポイント（マシンステートによって表される）およびアドレス空間によって完全に特徴づけられる。

Protection-Critical Portions of the TCB＜保護＞
TCB の重要部分--これらの部分はその正常な機能がサブジェクト－オブジェクト間のアクセス制御を司る TCB の部分。

Protection Philosophy＜保護哲学＞
採用された保護メカニズムの各々を説明するシステムの包括的なデザインのフォーマルでない記述｡このメカニズムがセキュリティポリシーの実施に適していることを示すために、フォーマルとフォーマルでない技術の組み合わせ（評価クラスに応じた）が使われる。

Read＜リード(読み取り)＞
オブジェクトからサブジェクトへの情報の流れだけが生じる基本的操作。

Read Access＜リードアクセス＞
情報を読みとることの許諾。

Read-Only Memory (ROM)＜リードオンリー・メモリ＞
内容の読みとりは可能であるが通常のコンピュータ処理中に変更することができない記憶装置エリア。

Reference Monitor Concept＜リファレンスモニター・コンセプト＞
サブジェクトによるオブジェクトへの全アクセスを仲介する抽象マシンを指すアクセス制御の概念。

Resource＜リソース＞
機能実行中に、使用される又は消費されるあらゆるもの。リソースの種類：時間、情報、オブジェクト（情報コンテナ)、あるいはプロセッサ （情報を使用する能力。

Security Kernel＜セキュリティカーネル＞
リファレンスモニターの概念を実装する、トラステッド・コンピューティングの基礎となるハードウェア、ファームウェアおよびソフトウェアの要素。

Security Level＜セキュリティレベル＞
情報の機密の程度を表す階層的な区分と一連の非階層的なカテゴリーの結合。

Security Policy＜セキュリティポリシー＞
一連の法律、規則および慣習であって、機密度の高い情報を如何に管理し、保護し、配分するかを規制するもの。

Security Policy Model＜セキュリティポリシーモデル＞
フォーマルセキュリティポリシーモデルのフォーマルでない(非数式的)表現 。

Security Relevant Event＜セキュリティ関連イベント＞
システムのセキュリティ状態の変更を試みるすべての出来事（例：自由裁量アクセス制御の変更、サブジェクトのセキュリティレベル変更、ユーザパスワードの変更など）
さらにシステムのセキュリティポリシー侵害を試みるすべての出来事。
（例:極めて多数のログイン試行､装置の強制的アクセス制御による制限を破壊する試み、ファイル権限の降格など）

Security Testing＜セキュリティ検査＞
システムのセキュリティ特性が設計どおりに実装され、また提案されたアプリケーション環境に適応していることを決定するのに使われるプロセス。
このプロセスには実地での機能検査、侵攻検査および立証を含む機能検査、侵入検査、確認も参照のこと。

Sensitive Information＜取扱注意情報＞
適切な権限を付与することにより、許可なく開示・改変・消失・破壊されることが誰かあるいは何かに対して認知し得る損害を生じさせるので、保護が必要となる情報。適格な権限を持つ者によって決められる。

Sensitivity Label＜機密ラベル＞
オブジェクトのセキュリティレベルを示し、オブジェクトのデータ機密度（例えば極秘）を表わす一つの情報。このラベルは強制的アクセス制御の判断基準としてＴＣＢに利用される。

Simple Security Condition＜単純セキュリティ条件＞
サブジェクトのセキュリティレベルがオブジェクトのセキュリティレベルよりも高い場合、サブジェクトに対してオブジェクトの読み取りアクセスを許可するという Bell-LaPadula セキュリティモデル規則。

Single-Level Device＜単一レベル装置＞
ある一時点では単一のセキュリティレベルのデータを処理する装置。この装置は異なるセキュリティレベルのデータを分けておく必要がないため、機密ラベルを処理中のデータと一緒に保持しなくて良い。

* - Property(Star Property)＜*プロパティ（スタープロパティ)＞
サブジェクトのセキュリティレベルがオブジェクトのセキュリティレベルの下位にある場合にのみ、サブジェクトがオブジェクトに書き込みアクセスすることを許可する Bell－LaPadula セキュリティモデルのルール。
閉じ込めプロパティとしても知られている。（このアスタリスクを「スター」と読む）

Storage Object＜ストレージ オブジェクト＞
読み書きの両方のアクセスをサポートするオブジェクト。

Subject＜サブジェクト＞
能動的なエンティティ（主体）であり、一般には人、プロセス、あるいは装置の形をとり、オブジェクト間に情報の流れを起こし、あるいはシステムの状態を変化させる。

Subject Security Level＜サブジェクト・セキュリティ・レベル＞
サブジェクトのセキュリティレベルは読み書きの両方のアクセス権をもつオブジェクトのセキュリティレベルと同じである。サブジェクトのセキュリティレベルは常時そのサブジェクトが関連づけられているユーザの許可権限に支配されなければならない。

TEMPEST＜TEMPEST＞
ADP 装置から放出される不要な電気信号の検査と制御。

Top-Level Specification＜最上位レベル仕様(TLS)＞
最上位の抽象レベルにおける、システム動作に関する非手続き記述。
一般的には、実装の詳細をすべて省いた機能仕様をいう。

Trap Door＜トラップドア＞
システムの防御機構を回避できる秘密のソフトウェアあるいはハードウェア機構。
これは、ある明白でない方法で利用可能となる(例えば、端末に特定のランダムな文字列を入力するなど)

Trojan Horse＜トロイの木馬＞
外見上、あるいは実際に役に立つ機能を持つが、正規の権限を秘密裏に利用して、セキュリティを侵害するプロセスを呼び出す付加(隠された)機能が含まれているコンピュータプログラム。例えば、トロイの木馬の製作者に送る機密ファイルの隠しコピーを作るなど。

Trusted Computer System＜トラステッド・コンピュータ・システム＞
ハードウェアとソフトウェアによる完全性を実現する十分な手段を採用するシステム
それらの手段は機密や極秘に属する情報を同時に扱うために用いられる。

Trusted Computing Base (TCB)＜トラステッド・コンピューティング・ベース＞
セキュリティポリシーを適用するためのハードウェア、ファームウェア、ソフトウェアおよびそれらの組み合わせを含む、コンピュータ・システムの保護メカニズム全体。
TCB は、製品やシステム上の統一的なセキュリティポリシーを適用するための一つ以上のコンポーネントによって構成される。正しくセキュリティポリシーを具現化するための TCB の能力は、ひとえに TCB のメカニズムと、システム管理者によるセキュリティポリシーに基づいたパラメータ(ユーザの許可など)の正しい入力に依存する。

Trusted Path＜トラステッド・パス＞
利用者が端末からトラステッド・コンピューティング・ベース(TCB)へ直接情報を伝達するときに使うメカニズム。
このメカニズムは、利用者とトラステッド・コンピューティング・ベース(TCB)だけが活性化でき、信頼できないソフトウェアによって模倣することはできない。

Trusted Software＜トラステッド・ソフトウェア＞
トラステッド・コンピューティング・ベース(TCB)のソフトウェア部分。

User＜ユーザ＞
直接コンピュータ・システムとやり取りする人。

Verification＜確認＞
2 つのレベルのシステムの仕様が正しく一致することを比較するプロセス(例えば最上位レベル仕様のセキュリティポリシーモデル、ソースコードが付いている TLS、またはオブジェクトコードが付いているソースコードがある。
このプロセスは自動化されている場合もされていない場合もある。

Write＜書き込み＞
サブジェクトからオブジェクトへの情報の流れだけが生じる基本的操作。

Write Access＜書き込みアクセス＞
オブジェクトへの書き込みの許可。

参考文献

1. Anderson, J. P. Computer Security Technology Planning Study, ESD-TR-73-51, vol. I, ESD/AFSC, Hanscom AFB, Bedford, Mass., October 1972 (NTIS AD-758 206).

2. Bell, D. E. and LaPadula, L. J. Secure Computer Systems：Unified Exposition and Multics Interpretation, MTR-2997 Rev. 1, MITRE Corp., Bedford, Mass., March 1976.

3. Brand, S. L. "An Approach to Identification and Audit of Vulnerabilities and Control in Application Systems," in Audit and Evaluation of Computer Security II：System Vulnerabilities and Controls, Z. Ruthberg, ed., NBS Special Publication #500-57, MD78733, April 1980.

4. Brand, S. L. "Data Processing and A-123," in Proceedings of the Computer Performance Evaluation User's Group 18th Meeting, C. B. Wilson, ed., NBS Special Publication #500-95, October 1982.

5. DCID l/l6, Security of Foreign Intelligence in Automated Data Processing Systems and Networks (U), 4 January l983.

6. DIAM 50-4, Security of Compartmented Computer Operations (U), 24 June l980.

7. Denning, D. E. "A Lattice Model of Secure Information Flow," in Communications of the ACM, vol. 19, no. 5 (May 1976), pp. 236-243.

8. Denning, D. E. Secure Information Flow in Computer Systems, Ph.D. dissertation, Purdue Univ., West Lafayette, Ind., May 1975.

9. DoD Directive 5000.29, Management of Computer Resources in Major Defense Systems, 26 April l976.

10. DoD 5200.1-R, Information Security Program Regulation, August 1982.

11. DoD Directive 5200.28, Security Requirements for Automatic Data Processing (ADP) Systems, revised April 1978.

12. DoD 5200.28-M, ADP Security Manual -- Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating Secure Resource-Sharing ADP Systems, revised June 1979.

13. DoD Directive 5215.1, Computer Security Evaluation Center, 25 October 1982.

14. DoD 5220.22-M, Industrial Security Manual for Safeguarding Classified Information, March 1984.

15. DoD 5220.22-R, Industrial Security Regulation, February 1984.

16. DoD Directive 5400.11, Department of Defense Privacy Program, 9 June 1982.

17. DoD Directive 7920.1, Life Cycle Management of Automated Information Systems (AIS), 17 October 1978

18. Executive Order 12356, National Security Information, 6 April 1982.

19. Faurer, L. D. "Keeping the Secrets Secret," in Government Data Systems, November - December 1981, pp. 14-17.

20. Federal Information Processing Standards Publication (FIPS PUB) 39, Glossary for Computer Systems Security, 15 February 1976.

21. Federal Information Processing Standards Publication (FIPS PUB) 73, Guidelines for Security of Computer Applications, 30 June 1980.

22. Federal Information Processing Standards Publication (FIPS PUB) 102, Guideline for Computer Security Certification and Accreditation.

23. Lampson, B. W. "A Note on the Confinement Problem," in Communications of the ACM, vol. 16, no. 10 (October 1973), pp. 613-615.

24. Lee, T. M. P., et al. "Processors, Operating Systems and Nearby Peripherals: A Consensus Report," in Audit and Evaluation of Computer Security II: System Vulnerabilities and Controls, Z. Ruthberg, ed., NBS Special Publication #500-57, MD78733, April 1980.

25. Lipner, S. B. A Comment on the Confinement Problem, MITRE Corp., Bedford, Mass.

26. Millen, J. K. "An Example of a Formal Flow Violation," in Proceedings of the IEEE Computer Society 2nd International Computer Software and Applications Conference, November 1978, pp. 204-208.

27. Millen, J. K. "Security Kernel Validation in Practice," in Communications of the ACM, vol. 19, no. 5 (May 1976), pp. 243-250.

28. Nibaldi, G. H. Proposed Technical Evaluation Criteria for Trusted Computer Systems, MITRE Corp., Bedford, Mass., M79-225, AD-A108-832, 25 October 1979.

29. Nibaldi, G. H. Specification of A Trusted Computing Base, (TCB), MITRE Corp., Bedford, Mass., M79-228, AD-A108-831, 30 November 1979.

30. OMB Circular A-71, Transmittal Memorandum No. 1, Security of Federal Automated Information Systems, 27 July 1978.

31. OMB Circular A-123, Internal Control Systems, 5 November 1981.

32. Ruthberg, Z. and McKenzie, R., eds. Audit and Evaluation of Computer Security, in NBS Special Publication #500-19, October 1977.

33. Schaefer, M., Linde, R. R., et al. "Program Confinement in KVM/370," in Proceedings of the ACM National Conference, October 1977, Seattle.

34. Schell, R. R. "Security Kernels： A Methodical Design of System Security," in Technical Papers, USE Inc. Spring Conference, 5-9 March 1979, pp. 245-250.

35. Trotter, E. T. and Tasker, P. S. Industry Trusted Computer Systems Evaluation Process, MITRE Corp., Bedford, Mass., MTR-3931, 1 May 1980.

36. Turn, R. Trusted Computer Systems： Needs and Incentives for Use in government and Private Sector, (AD # A103399), Rand Corporation (R-28811-DR&E), June 1981.

37. Walker, S. T. "The Advent of Trusted Computer Operating Systems," in National Computer Conference Proceedings, May 1980, pp. 655-665.

38. Ware, W. H., ed., Security Controls for Computer System：Report of Defense Science Board Task Force on Computer Security, AD # A076617/0, Rand Corporation, Santa Monica, Calif., February 1970, reissued October 1979.