本書の日本語訳は、原文の内容を保証するものではありません。正確な規定や推奨については原文をお読みください。

トラステッド・システムにおける監査を理解するためのガイド

(**原訳：日本ユニシス株式会社 五十嵐 智研究員** 2005/07/06，**改訂** 2005/11/11
追訳：日本セキュリティ・マネジメント学会セキュア OS **研究会は、五十嵐 智氏の好意により原訳に修正を加えました。 最終改訂** 2006/09/19)

NCSC-TG-001
Library No. S-228,470

本書「トラステッド･システムにおける監査を理解するためのガイド」は、米国国防総省(DoD)の指示書 5215.1 **に従いその権威の下で国家コンピュータ･セキュリティ･センター(NCSC)が発行した。本書に記述されたガイドラインは、機密及びその他の取扱注意情報を処理する自動データ処理システムにおける、監査の好ましい実践方法を集めたものである。このガイドライン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通して国家コンピュータ･セキュリティ･センターが半年毎にレビューを行う予定である。適切なチャネルを通しての改訂のためのすべての提案は、以下に送付のこと。**

National Computer Security Center
9800 Savage Road
Fort George G. Meade, MD 20755-6000
Attention: Chief, Computer Security Technical Guidelines
Patrick R. Gallagher, Jr. 28 July 19971987
Director
National Computer Security Center

謝辞

本書の準備と作成を行ったプロジェクトマネージャーである NCSC **の** James N. Menendez **氏に特に謝意を表する。**

本書を作成するために技術的な支援をいただいた NCSC **プロダクト評価チームと、レビューに積極的に参加して時間と専門技術を提供していただいたコンピュータセキュリティ･コミュニティのメンバーに同じく謝意を表する。**

(**訳者謝辞：翻訳に当たって、ベースとなる “** the Department of Defense Trusted Computer System Evaluation Criteria **”の日本語訳「国防総省 トラステッド･コンピュータ･システム評価基準」を参考にし、引用させていただいた。翻訳を行った日本セキュリティ･マネジメント学会セキュア** OS **研究会のメンバーに感謝の意を表する。原文で参考文献**[1] **を引用している部分の訳は、すべて同日本語訳から引用させていただいた。**)

目　次

序文

このガイドラインを通して、トラステッド･コンピュータ･システム評価基準（以下、評価基準）には記述されていない勧告を行う。評価基準に記述されていない推奨事項は「望ましい」（"should"）と記述し、要求事項は「しなければならない」（"shall"）と記述する。これにより混乱が避けられれば幸いである。

1. 序説

1.1 国家コンピュータ･セキュリティ･センターの歴史

DoD セキュリティ・イニシアチブによって開始された作業を拡張するため、DoD コンピュータ･セキュリティ･センター(DoDCSC)が 1981 年1月に設立された。国家コンピュータ･セキュリティ･センターの長官は、コンピュータセキュリティのすべての分野に関する、標準とガイドラインを作成し発行する責任を負っている。連邦政府におけるコンピュータセキュリティに対するそれらの責任を反映させるため、DoDCSC は 1985 年に国家コンピュータ･セキュリティ･センター(National Computer Security Center)に改称された。

1.2 国家コンピュータ･セキュリティ･センターの目標

国家コンピュータ･セキュリティ･センターの主な目標は、トラステッド・コンピュータシステムの有効性を広く推進することにある。その目標へ近づくために、コンピュータシステムのセキュリティに関する評価を行う指標として “the Department of Defense Trusted Computer System Evaluation Criteria (the Criteria)”(「国防総省 トラステッド･コンピュータ･システム評価基準(以下、評価基準と表現する)」)が作成された。その評価基準は、CSC-STD-001-83 として 1983 年 8 月 15 日に初めて発行された。DoD は多少の変更を加えて、国防総省標準 DoD 5200.28-STD としてそれを 1985 年 12 月に採用した。中でも、国防総省命令 5200.28 “Security Requirements for Automatic Data Processing (ADP) Systems”(「自動データ処理(ADP)システムにおけるセキュリティ要件」) は、国防総省が使用する場合に、国防総省トラステッド･コンピュータ･システム評価基準を要件とすることを記述したものである。この評価基準は、ADP システムに実装されたセキュリティ制御の効果を評価するために使用する標準である。評価基準は、4 つに区分されている。D、C、B、および A がある。階層化された順序で示され、最高区分の(A)は、保証の可能な限り最高のレベルを与えるシステムのために予約されている。区分 C と B においては、クラスと呼ばれるいくつかの小区分がある。これらのクラスも階層化された順序でセキュリティの異なるレベルを表している。

2. 目的

クラス C2 から A1 まで、評価基準は、ユーザの行動が監査による精査に対してオープンでなければならないことを要求している。安全なシステムの監査プロセスというのは、セキュリティに関連したシステム上における任意あるいはすべての行動を記録し、調査し、レビューするプロセスである。このガイドラインは、監査の仕組みの実装と評価に影響する重要な点を議論するつもりである。本書の目的は二つある。システムにおける効果的な監査の仕組みをどのようにして設計し具体化するかを製造者への手引きとして提供し、信頼できるシステムによって提供される監査能力の効果的な使用方法を実装者への手引きとして提供する。本書は、監査証跡としてどのような情報を記録するのが

望ましいのか、監査はどのようにして実施するのが望ましいのか、そして監査リソースに適合してどのような保護手段が採られるのが望ましいのか、という提案を含んでいる。

本書におけるいかなる例も評価基準の要求を満たす唯一の実装であると解釈してはならない。例示は適切な実装のための単なる提案にすぎない。本書の中の勧告についても、評価基準の補足的な要求と捉えてはならない。評価基準は、評価されるべきシステムに対する唯一の基準である。

このガイドラインは、評価基準の課題と、評価基準で記述された特徴に対して有用な指針を示す、継続的なプログラムの一部である。

3. 範囲

クラス C2 から A1 までの区分の重要なセキュリティの特徴は、任意のあるいはすべてのシステム上の動きを監査できる ADP システムの能力にある。このガイドラインは、評価基準の要求を満たす目的で作られるコンピュータシステムとその製品に適用する監査および監査ファシリティの特徴について記述している。

4. コントロール目標

トラステッド･コンピュータシステム評価基準は、次のような「アカウンタビリティのコントロール目標」を与える：

「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証しなければならない。さらに、アカウンタビリティを保証するためには、認可され権限のある正当な者が、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。」[1]

「アカウンタビリティのコントロール目標」は、監査に関連するときには、次のような監査のためのコントロール目標を導く：

「トラステッド・コンピュータシステムでは、権限のある者に、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し、あるいは生成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される。しかしながら、監査イベントから、その行為を誰が（あるいはどのプロセスが）行ったのかを、あるいは誰の利益のために行われたのかを、具体的な個々ユーザの行動を追跡し特定することができるために、監査データには十分な粒度がなければならない。」[1]

5. 監査原則の概要

監査証跡はコンピュータシステムへの侵入を検知および防止し、不正使用を見極める方法を明らかにするために使用される。監査人の自由裁量で、証跡を特定のイベントに制限したり、システム上のすべての行動を含むようにしたりしてもよい。TCSEC では要求されていないが、これは監査の仕組みの対象として、主体(Subject)と客体(Object)のいずれに対しても可能にするのが望ましい。すなわち、原子炉ファイルがアクセスされるあらゆる瞬間と同様に、John がシステムにアクセスするすべての瞬間を、監査の仕組みがモニターできることが望ましい。John が原子炉ファイルにアクセスする瞬間も同様である。

5.1 監査の仕組みの目的

コンピュータシステムの監査の仕組みには、5 つの重要なセキュリティ目標がある。第１に、監査の仕組みは、「個々の客体(Object)へのアクセスのパターン及び特定のプロセスや個人のアクセス履歴がレビュー可能で、システムが提供する様々な保護機構の使用と効果をレビューできるように」[2]しなければならない。第２に、監査の仕組みはユーザと部外者が繰り返して保護機構を回避しようとする試みを検知できなければならない。第３に、監査の仕組みは、プログラマから管理者へ移行するような、自分自身より高い権限の機能を備えていると考えてユーザが利用する、特権の使用を発見できなければならない。セキュリティ制御を回避しなくても侵入される可能性があるためである。第４に、監査の仕組みは、加害者が習慣的にシステム保護機構を回避しようとすることに対して抑止力として働かなければならない。しかしながら、抑止力として働くためには、加害者がシステム保護機構の回避の試みを検知する監査の仕組みの存在とそれが動作していることに気づかなければならない。第５に、監査の仕組みの目標は、「保護機構を回避する試みは記録され発見されるというユーザ保証についての追加の定まった手続き」[2]を提供しなければならない。保護機構回避の試みが成功した場合でも、侵害によって受けた被害を見定めることを手助けすることによって、監査証跡は相変わらず保証を提供することになる。

5.2 監査の仕組みの使用者

「監査の仕組みの使用者は２つのグループに分けられる。最初のグループは、監査人である。監査人は、管理義務を負う者であり、システムの監査すべきイベントを選択し、それらのイベントの記録を行う監査フラグを設定し、監査イベントの証跡を解析する。」[2] いくつかのシステムにおいて、監査人の任務はシステムセキュリティ管理者の任務を兼ねても良い。また、下位のクラスでは、システム管理者が監査人の役割を執行しても良い。この監査のガイドラインは ADP システムにおけるシステム管理者かつ／またはシステムセキュリティ管理者かつ／または独立した監査人にも適用できると考えられるが、本書では、監査に責任を負う者をシステムセキュリティ管理者と呼ぶ。

「第２の監査の仕組みの使用者グループは、システムのユーザ自身である。このグループは、管理者、オペレータ、システムプログラマ、および他のすべてのユーザを含む。彼らは、監査の仕組みの使用者とみなされる。彼らと彼らのプログラムが監査イベントを発生させるだけでなく」[2]、彼らは監査の仕組みが存在し、その機構上でいかなる影響があるかを理解していなければならない。さもなければ、監査の仕組みのユーザ抑止力とユーザ保証の目標は達成できない。

5.3 効果的監査の側面

5.3.1 識別と認証

システムへのログインでは、一般にユーザが特定の識別子(例えば、ログイン ID、磁気ストライプ)およびパスワード(あるいは他の機構)の特定形式を入力することを要求する。この情報が有効か否かにかかわらず、ログイン手続きの実行は監査イベントであり、入力された識別子が監査可能な情報であることが重要である。パスワードのような入力された認証情報は監査証跡として残さないことが望ましい。入力された識別子が有効でないと認識されたイベントでは、システムはこの情報を監査証跡から省くべきである。その理由はシステムがログイン ID を要求しているときに、ユーザがパスワードを入力したかもしれないからである。この情報が監査証跡に書かれると、ユーザのパスワードとセキュリティの信頼性が低下する。

しかし、無効な識別子情報を記録することによって影響を受けたリスクが減少するような場合がある。形の決まった端末をもつシステムでは、識別子の欄にパスワードを入力する可能性は明らかに

減少する。このため、識別子情報の記録は、大きな脅威にはならないかもしれない。識別子情報を記録することの利点は、侵入の試みをより簡単に検知し、犯人を見つける手助けにもなるかもしれないことである。ここで収集された情報は、セキュリティ侵害を追及する法的な告発に必要とされるかもしれない。

5.3.2 管理面

クラス C2 とそれ以上のクラスに適合するすべてのシステムは、監査能力をもたなければならず、監査手続きに対する責任者として指名された者がいなければならない。C2 と B1 のクラスについては、システムオペレータの職務は監査人の職務を含むすべての役割を包含してもよい。B2 クラスからは、オペレータと管理者の役割の分離を支援するための TCB に対する要件がある。さらに、B3 クラスとその上位クラスでは、システムセキュリティ管理者の役割を識別することが要求されている。システム上のシステムセキュリティ管理者の役割を引き受ける場合、たとえばログイン手続きなど、後に明確に監査可能な行動をとらなければならない。役割を与えられた特権をもつ者がシステム上にある場合、その役割の行動もまた監査可能なイベントにしなければならない。

5.3.3 システム設計

システム設計にはシステムセキュリティ管理者の要求によって監査機能を有効にする機構を含んでいるのが望ましい。また、イベントが監査証跡の対象に含めるように選択されているかどうかを調べる機構が含まれているのが望ましい。イベントの事前選択が実装されていない場合、監査可能なすべてのイベントを監査証跡に残すのが望ましい。ユーザ識別および／または客体の機密種別を基本とするイベントを選択できる管理者のための評価基準の要件は、依然として満たさなければならない。この要求は、問い合わせを使用してイベントの事後選択を可能にして満たすことができる。監査証跡を解析するために使用する整理ツールがいかなるものであれ、それはベンダーによって提供されなければならない。

5.4 監査のセキュリティ

監査証跡そのものと同様に、監査証跡ソフトウェアもトラステッド･コンピューティング･ベース(TCB)によって守られていることが望ましい。また、厳密なアクセス制御に従うことが望ましい。監査の仕組みのセキュリティ要件は次のとおりである：

(1) イベントの記録機構は TCB の一部でなければならない。そして、許可されていない変更や回避から保護されていなければならない。

(2) 監査証跡自身が許可されていないアクセスから TCB によって保護されていなければならない(即ち、監査人のみが監査証跡にアクセス可能とするなど)。また、監査証跡は許可されていない変更から守られていなければならない。

(3) 監査イベントの有効／無効を選択する機構は、TCB の一部でなければならない。そして、許可されていないユーザがアクセスできないよう継続しなければならない。[2]

少なくとも、監査証跡上のデータは取扱注意情報であると考えることが望ましく、そして監査証跡自身はシステム内にある最も厳重な取扱注意情報と同程度に機密であると考えなければならない。

監査証跡を含む媒体が物理的に ADP システムから取り外される場合、その媒体はシステム内にある最高位の機密レベルのデータに要求されるものと同程度に、物理的に保護されることが望ましい。

6. 評価基準の要求との調和

本ガイドラインのこのセクションは評価基準の中の監査に関する要求を記述し、いくつかの追加の推奨事項を提示する。監査要求には 4 つのレベルがある。最初のレベルは C2 評価クラスであり、B3 評価クラスまで要求は連続して発展する。これらのそれぞれのレベルにおいて、本ガイドラインは監査可能であることが望ましい幾つかのイベントと、監査証跡上に残すことが望ましい情報、および監査のためにどのような基準で選択されるイベントを選ぶかを列挙する。すべての要求事項は、「しなければならない」(“shall”)と記述し、追加の推奨事項は「望ましい」(“should”)と記述する。

6.1 C2 監査の要求

6.1.1 監査可能とするイベント

次のイベントは C2 クラスにおいて監査対象でなければならない：

- 識別と認証の機構の使用
- ユーザアドレス空間への客体(Object)の作成
- ユーザアドレス空間から客体(Object)の削除
- コンピュータオペレータとシステム管理者、かつ／またはシステムセキュリティ管理者がとる行動
- すべてのセキュリティ関連イベント(本ガイドラインのセクション 5 で定義されている)
- プリントアウトの作成

6.1.2 監査可能な情報

次の情報は、C2 クラスにおける監査証跡上に記録しなければならない：

- イベントの日付と時刻
- イベントを起こした主体(Subject)を操作した者の固有の識別子
- イベントのタイプ
- イベントの成否
- 識別と認証のイベントに関する要求元(例えば、端末 ID)
- ユーザアドレス空間に対する、作成、アクセス、削除された客体(Object)の名前
- ユーザとシステムのセキュリティデータベースがシステム管理者によって変更された内容

6.1.3 監査の基本項目

C2 レベルでは、ADP システム管理者は個人の識別を基本とする監査を行うことが可能でなければならない。

また、ADP システム管理者は客体(Object)を基本とする監査ができることが望ましい。

6.2 B1 監査の要求事項

6.2.1 監査可能なイベント

評価基準では、B1 クラスで監査可能としなければならないイベントリストに、次の項目を具体的に追加している：

・ハードコピーにおいて人間が判読可能な印の修正(機密レベル印の更新とラベル付けの機能の停止を含む)

・通信チャネルあるいは入出力デバイスの指定(シングルレベルからマルチレベルへ、あるいはマルチレベルからシングルレベルへ)の変更

・シングルレベル通信チャネルまたは入出力デバイスに対応する機密レベルの変更

・マルチレベル通信チャネルまたは入出力デバイスに対する範囲の変更

6.2.2 監査可能な情報

評価基準では、B1 クラスで監査証跡に記録しなければならないリストに次の項目を具体的に追加している：

・客体(Object)のセキュリティレベル

次の情報は、B1 クラスの監査証跡に記録することが望ましい：

・主体(Subject)の機密保持レベル

6.2.3 監査の基本項目

前述の選択基準に加えて、B1 レベルでの評価基準は、ADP システム管理者が個人の識別と客体(Object)のセキュリティレベルを基本とする監査を可能としなければならないことを具体的に要求している。

6.3 B2 監査の要求事項

6.3.1 監査可能なイベント

評価基準では、B2 クラスで監査可能としなければならないイベントリストに次の項目を具体的に追加している：

・隠れストレージチャネルが使用される可能性があるイベント

6.3.2 監査可能な情報

B2 クラスで新しく追加される要求項目はない。

6.3.3 監査の基盤

前述の選択基準に加えて、B2 レベルでの評価基準は、「TCB は隠れストレージ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。」ことを

具体的に要求している。トラステッド・コンピュータ・ベースは毎秒 10 ビットを超える隠れストレージチャネルを監査しなければならない。[1]

また、トラステッド･コンピュータ･ベースは、10 秒に 1 ビットの割合を越えるバンド幅の隠れストレージ機構の使用を監査する能力を提供することが望ましい。

6.4 B3 監査の要求事項

6.4.1 監査可能なイベント

評価基準では、B3 クラスで監査可能としなければならないイベントリストに次の項目を具体的に追加している：

・システムのセキュリティポリシーの切迫した侵害(例えば、隠れタイミングチャネルの利用)を示すようなイベント

6.4.2 監査可能な情報

B3 クラスで新しく追加される要求項目はない。

6.4.3 監査の基盤

前述の選択基準に加えて、B3 レベルの評価基準では、特に以下を要求している。「TCB は、セキュリティポリシーへの切迫した侵害を示す可能性のある、セキュリティ監査すべきイベント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。閾値を超過した場合、このメカニズムはシステム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い。これらが継続して累積された際には、システムは最も破壊性が低いようにイベントを終了するための処置を講ずるものでなければならない。」[1]

切迫したセキュリティ侵害を示すイベントは、隠れタイミングチャネルを利用するイベントと繰り返して失敗するログインの試行を含む場合がある。隠れタイミングチャネルは毎秒 10 ビットの割合を超える可能性がある。

通常はイベントが起こった後のシステムセキュリティ管理者による監査証跡のレビューが要求されているのみだが、閾値を超えた場合にシステムセキュリティ管理者に即座に通知することが可能であるためには、メカニズムはセキュリティポリシーの侵害について、評価基準の低いレベルで要求される早さよりも早く識別し、報告し、応答しなければならない。侵害の通知は「オペレータへの他の TCB メッセージと同じ優先度で行われる のが望ましい。」[5]

「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、最も破壊が低いようにイベントを終了するための処置を講ずるものでなければならない。」[1] この処置はイベントを起こしているユーザの端末をロックしたり、疑わしいプロセスを終了させたりすることを含む。一般には、最も破壊性の低い処置はアプリケーションに依存し、その処置がすべての可能な処置のうちで最も破壊性の少ないことを説明することは要求されない。イベントを終了させるどのような処置も受け入れられるが、システムを停止することは最後の手段であることが望ましい。

6.5 A1 監査の要求事項

6.5.1 監査可能なイベント

A1 クラスで新しく追加される要求項目はない。

6.5.2 監査可能とする情報

A1 クラスで新しく追加される要求項目はない。

6.5.3 監査の基盤

A1 クラスで新しく追加される要求項目はない。

7. 可能な実装方法

監査の要求事項を実装する技法は、それぞれシステムによって異なり、ソフトウェア、ファームウェア、ハードウェアの特徴や追加可能とする機能に依存する。技術の進歩によって可能となった技法は、費用対効果とパフォーマンスの場合と同様に、必須のセキュリティを提供するシステム設計に最良の利点として用いることが望ましい。

7.1 監査イベントの事前／事後選択

クラス C2 とそれ以上のクラスでは、すべてのセキュリティ関連イベントは監査可能である、ということが要求される。しかし、これらのイベントは、監査証跡として常に記録されているかもしれないし、常には記録されていないかもしれない。どのイベントが監査対象として望ましいのかを選択することが可能になるオプションには、事前選択と事後選択の機能が含まれている。システムは、両方のオプションを実装するか、事前選択オプションあるいは事後選択オプションの一方のみを実装することを選んでもよい。

システム開発者が一般の事前／事後選択オプションを実装しないことを選んだ場合であっても、評価基準のすべてのクラスで管理者が特定のユーザの行動を選択的に監査することを可能とする要求に変わりはない。B1 クラスからは、管理者は客体(Object)のセキュリティレベルを基本として監査をすることが可能であるべきである。

オプションは、ユーザを個人かグループのいずれかにより選択することを許すのが望ましい。例えば、管理者は特定の個人に関連するイベントを選択するかもしれないし、特定のグループに含まれる個人に関連するイベントを選択するかもしれない。また、管理者は選択された監査ファイルに関連するイベントを指定してもよいし、クラス B1 とそれ以上のクラスでは最高機密などの選択された機密レベルの客体 (Object)へのアクセスを指定してもよい。

7.1.1 事前選択

それぞれの監査可能なイベントに対して、TCB はイベントが監査証跡に記録されるべきであるか否かを表示する機構を含むことが望ましい。記録されるべきイベントを選択できることを承認されるのはシステムセキュリティ管理者あるいは指名された者のみでなければならない。事前選択はユーザ認証で行ってもよいし、B1 クラスとそれ以上のクラスでは、事前選択は客体(Object)のセキュリティレベルによって可能としてもよい。システムセキュリティ管理者は記録されるべきイベントを選択

することを承認されなければならないが、システムセキュリティ管理者は監査されることから彼自身を免れることができないことが望ましい。

推奨はしないが、システムセキュリティア管理者は、評価基準の要求にかかわらず、いずれのイベントも選択しないことができてもよい。ここで述べる意図は、柔軟性を与えるためである。システムに監査機能を設計する目的は、それを必要としないユーザに評価基準を押し付けることではなく、単に要求を実装するための能力を提供することにある。

事前選択の欠点は、将来の時点でのセキュリティに関連する関心事となるかもしれないイベントを予測することが非常に難しいことである。事前選択されていないイベントがある日にセキュリティ関連イベントになる可能性が常にあり、これらのイベントを監査しないことで起こる潜在的な損失は、調査を不可能にするかもしれない。

事前選択の利点は、システム上のすべてのイベントを監査しないので、おそらくパフォーマンスが向上することである。

7.1.2 事後選択

存在する監査証跡から特定のイベントのみを選択する事後選択を実装した場合、ここでも、権限を付与された個人のみがこの選択をできるようにしなければならない。このオプションを含める場合、システムは、問い合わせ要求と回復要求を受け付け、圧縮されたデータを解凍し、要求されたデータを出力する、信頼できる設備(セクション 9.1 で記述されている)を持つのが望ましい。

事後選択の主な利点は、監査の試行時に将来も利用されることが保証される情報がすでに監査証跡上に記録されていることであり、いつでも問い合わせられることである。

事後選択に関する欠点は、非常に大きな監査証跡になると思われる書き込みと蓄積のために、おそらくパフォーマンスが落ちることである。

7.2 データ圧縮

監査情報を記録する場合に、「監査すべきすべてのイベントを選択するシステムは非常に大きなデータを作り出すため、容量を消費しないようにデータをエンコード（コード化）し、必要とするプロセッサの時間を最少にすることが必要になる」[3]。監査証跡をエンコードするのであれば、必要とするときにデータをデコード（可視化する）する補足的な機構を含まなければならない。監査証跡のデコード（可視化）は、データベースによって監査レコードがアクセスされる前に事前処理として、あるいは関連する情報が見つかった後に事後処理として行われてもよい。このようなデコード（可視化）は、管理者の端末とバッチレポートの両方で理解可能な形でデータを表示する必要がある。監査証跡の圧縮コストは圧縮処理と解凍処理のために時間が必要となる。データを圧縮する利点は、監査証跡として記録を書き込むためのストレージと時間の節約である。

7.3 複数の監査証跡

監査証跡に含まれるすべてのイベントは同一の監査証跡の一部として書き込まれてもよいが、あるシステムでは、いくつかの別個の監査証跡を持つことを望むかもしれない。例えば、「ユーザ」のイベント、「オペレータ」のイベント、「システムセキュリティ管理者」のイベントなどである。これはその後の解析に対して、より小さい証跡を提供する。しかし、あるケースでは、不審なイベントが起こったときに、それが起きた時のイベント順の合成を得るために、証跡から情報を結合する必要

があるかもしれない。複数の証跡がある場合には、複数のログにわたって正確な、少なくとも同期したタイムスタンプが要求される。

いくつかの個別の監査証跡に分ける方法を紹介したが、TCB がすべての監査データを一つの包括的な監査証跡として提出することが可能であることが、しばしばより便利であることに注意することは重要である。

7.4 物理的なストレージ

監査証跡のために使用する媒体の選択を考えるためのひとつの要素は、システムの利用予測である。少ないユーザが少ないアプリケーションを実行しているシステムのための入出力量は、多数のユーザが様々なアプリケーションを実行する大規模システムのものとはまったく異なる。しかし、どのような場合でも、監査証跡の媒体が格納能力の限界に近づいた時には、システムはシステムオペレータかシステム管理者に通知するのが望ましい。人間の介在が必要とされる場合には、オペレータへの適切な事前の通知が特に必要である。

監査証跡のストレージ媒体が交換される前にあふれた場合、オペレーティングシステムは、これを検知しなければならず、次のような適切な行動をとらなければならない：

1．媒体が「満杯」であり、アクションが必要であることをオペレータに通知する。その後、システムは停止し、再起動を要求することが望ましい。有効なオプションであるが、このアクションはサービス妨害(DoS)攻撃という極めて大きい脅威を作り出す。

2．通常の操作可能な媒体へ後に移行することを目的として、現在の監査レコードを一時的な媒体に保存する。このようにして、監査を継続することを可能とする。この一時的なストレージ媒体は、改ざんする試みを防ぐために、通常の監査ストレージと同様の保護を与えることが望ましい。

3．監査の仕組みを使用することが要求されるアクションを制限するために、新たな行動の入力を遅らせ、現在の操作をスローダウンさせる。

4．管理者が監査記録を書き込む容量を確保するまで、停止する。

5．システムセキュリティ管理者の判断の結果として、監査機能全体を停止する。ストレージのオーバーフローに対応するためにとるいかなるアクションも監査されなければならない。しかしながら、記載する価値のある監査ではないようなアクションが存在する。システム管理者の判断をシステムロジックの中に埋め込むことは可能である。システムロジックに埋め込まれたそのような事前にプログラムされた選択は、自動的に起動され、このアクションは監査されなくてもよい。

また、媒体の動作スピードもさらに考慮すべき事柄である。大勢のユーザがシステム上にいて、すべての監査イベントが記録されるべきであるような「最悪ケース」の条件に適応できるようにすることが望ましい。この最悪ケースの程度はシステム設計の段階で評価されるのが望ましく、そしてこの目的のために適切なハードウェアを(可能なときに)選択することが望ましい。

システムが監査証跡のオーバーフローをどのように扱うかにかかわらず、監査データをすべて保管する方法がなければならない。

7.5 ライトワンス・デバイス

下位のクラス(例えば、C2、B1)のために、監査証跡はセキュリティ侵害を検知するのに役立つメジャーツールかもしれない。

このことが暗黙に意味することは監査リソースが可能な最大の保護を与えるのが望ましいということである。監査証跡を保護するために用いられる一つの手法は、監査証跡をライトオンリー･デバイスとして設計された機構に記録することである。他の選択は、読み込み機構を使用不可にしたライトワンスモードに設計されたデバイスを設置することである。この方法は、攻撃者が変更しようとする監査証跡のデータをさかのぼって読んだり見つけたりすることができないため、すでに書き込まれたデータを攻撃者が削除したり変更することを防止できる。

媒体にデータを書くことのみしか許されていないハードウェアデバイスが使用できれば、書き込み済みのデータの変更は、非常に難しい。疑わしいメッセージは記録されるが、すでに記録されたメッセージの位置を見つけ変更することは困難である。ライトワンス･デバイスを使用しても、現在の監査証跡については、バッファなどのメモリ上にある監査リソースの変更を侵入者から防ぐことはできない。

監査証跡の記録にライトワンス･デバイスが使われた場合、システム侵入の試みを検知しなければならないので、承認された個人が証跡の情報を解析することを可能とするために、媒体は互換性のある読み込みデバイスへ後に変更されるはずである。侵入者が証跡に記録されるのを妨害するために監査ソフトウェアを変更した場合、長期にわたるデータの不在がセキュリティ侵害の可能性を示唆するであろう。ライトワンス･デバイスを使用する欠点は、管理者によって監査証跡の解析が行われるまで、遅延が余儀なくされることである。この欠点は、システムセキュリティ管理者がすべての監査レコードのコピーを入手してこのような方法でデバイスに書き込むことによって、リアルタイムで監査証跡をレビューすることを可能にすることにより、相殺できるかもしれない。

7.6 監査データの転送

ファシリティが許すならば、監査証跡を保護するもう一つの方法は、専用のプロセッサに転送することである。監査証跡はシステムセキュリティ管理者による解析にとって、より簡単に利用できるようにすることが望ましい。

8. その他の事項

8.1 監査データの削減

システムの稼動量と使用した監査の選択プロセスによって、監査証跡の大きさは様々である。しかし安全のため、監査証跡が監査データを削減する何らかの方法を必要とする大きさに膨らむことを、仮定しておく。最も有望なデータ削減ツールはシステムセキュリティ管理者へのインターフェースとなるバッチプログラムであろう。このバッチの実行は、データベースの問い合わせ言語と標準化された監査ファイルを入力としたレポート生成の組み合わせで実現できる。

これは TCB の一部である必要はないが、監査データ削減ツールはシステムの他の部分と同様に、同じ構成管理システムの下で保守されることが望ましい。

8.2 監査データの可用性

標準的なデータ処理では、監査情報はそれ自身が発生したときに記録される。情報の大部分は、リアルタイム解析のため即座に利用されることを必要としないが、システムセキュリティ管理者は、それが記録された直後に監査情報を引き出す能力を利用できることが望ましい。監査情報の記録とそれを利用可能にする間の遅延は、数分の範囲で最小限にすることが望ましい。

即座に注意を促すことを要するイベントについて、B3 クラスとそれ以上のクラスにおいては、システムセキュリティ管理者へ警報が送られなければならない。監査証跡をバッファに溜め込むシステムでは、システムセキュリティ管理者は、バッファの内容を書き出す能力を利用できることが望ましい。リアルタイムの警報に関しては、送信される場所はシステムに依存する。

8.3 監査データの保存

監査証跡の保存が求められる正確な期間はサイトに依存するが、サイトの操作手続きマニュアルには、この保存期間が記述されていることが望ましい。監査証跡の保存に最適な期間を決めるためには、ストレージ媒体の時間的な制限を考慮することが望ましい。使用されたストレージ媒体は、サイトが要求するすべての期間に亘って、監査データを信頼性を持って保存できなければならない。

監査証跡は少なくとも週に一度はレビューされることが望ましい。週に一度では監査証跡をレビューするのを待つ期間としては長すぎる可能性が多いにある。システムが予測する監査データの総量に依存するが、この頻度は適宜調整されることが望ましい。監査証跡のレビューとレビューの間の推奨期間は、高信頼ファシリティマニュアルに文書化されることが望ましい。

8.4 テスト

TCB で保護されている他の全のリソースに加えて、監査リソースは評価クラスが高くなるにつれて保証の要求が高くなる。下位のクラスでは、監査証跡が侵入の試みを検知する主な要素である。残念ながらこれらの下位クラスにおける監査リソースは侵入および破壊の被害をより受けやすい。「TCB は、管理者が使おうとしたときにデータが依然としてそこにあるという何らかの保証を提供しなければならない。」[3] テストの要求事項は、監査証跡の脆弱性を認識するもので、C2 クラスからは、監査証跡を改ざんあるいは破壊する明らかな欠陥の探索を含まなければならない。監査証跡が改ざんあるいは破壊された場合、そのような欠陥の存在はシステムが侵入可能であることを示している。また、テストは監査の仕組みを回避するどのような方法も明らかにするように実施されることが望ましい。「テストで見つかった欠陥は、数ある方法のうちのいくつかを用いて無効化してもよい。システム設計者が利用できる方法のひとつは、欠陥が見つかった機構のすべてのユーザを監査し、そのようなイベントをログすることである。」[3] 欠陥の排除は試されるべきである。

クラス B2 とそれ以上のクラスでは、検知したすべての欠陥は修正されなければならない。さもなければ、下位の評価が与えられる。テストによって監査証跡が有効であることが判明したならば、監査証跡に含まれるのが望ましいイベントが正確に反映されているか否かをデータの解析によって確認できる。システムの保証水準は上位のクラスで高くなるとしても、監査証跡は、実際のセキュリティ侵害やその可能性の検知に利用可能であるのと同様に、テストフェーズでも依然として有効なツールである。

8.5 文書化

C2 クラスからの文書化では、監査の要求事項に関する内容が高信頼ファシリティマニュアルに含まれなければならない。高信頼ファシリティマニュアルでは、監査ファイルの記録、調査、および保守の手順を説明しなければならない。監査イベントそれぞれのタイプの監査レコード構造を詳細に記述しなければならず、それぞれのフィールドが何であり、フィールドの大きさがいくつであるかを含むことが望ましい。

また、高信頼ファシリティマニュアルは、監査の仕組みのインターフェース、望ましい使用方法、デフォルトの設定、様々な設定や能力を使う場合のトレードオフに関する注意事項、および監査データが適切に保護されるシステムの設定と実行方法について、完全な記述を含んでいなければならない。

監査イベントが事前選択あるいは事後選択される場合、マニュアルはツールとその仕組みが利用可能であることと、それらをどのように使うかについても記述するのが望ましい。

8.6 回避できないセキュリティのリスク

単にイベントの発生を防ぐ方法がないという理由で、監査プロセスにはある種のリスクが含まれている。監査の実施では明確には予測できない要因(例えば、人間、自然など)があるため、監査の仕組みは決して 100%信頼できるわけではない。そのような要因の可能性を最小にするために、監査の仕組みにより提供されるセキュリティに逆に影響するような予防策が取られるかもしれないが、いかなる監査の仕組みもリスクから逃れることはできない。

8.6.1 管理者と内部の者の脅威に対する監査

セキュリティ侵害を検知し阻止する適切な監査機構を用いていても、システムセキュリティ管理者やシステムセキュリティの設計を行った誰かが加害者となる脅威は常に存在する。セキュアなシステムのシステムセキュリティ管理者が、個人的な利益のためにシステムに入りファイルを改ざんする間、その活動の監査を停止することが可能なのである。識別と認証の情報にもアクセスできるこれらの承認された個人は、にせの識別子(ID)で犯罪を行うために、他のユーザになりすましてシステムに侵入することも選択できる。

経営者はこのリスクに気づき、そしてシステムセキュリティ管理者の選定は慎重に行うことを確認しておくことが望ましい。システムセキュリティ管理者のように信用が要求される地位に選ばれるべき人は、ある日雇い主に対して使用されるかもしれない特権を与えられる前に、素性調査を受けることが望ましい。

また、システムセキュリティ管理者は、通常の任務で説明できない逸脱行為が無いことを明らかにするために監視出来るべきである。作業の規範からの逸脱は、セキュリティ侵害が起こったことあるいは起こりつつあることを示している可能性がある。

こういった内部からの脅威をコントロールするその他のセキュリティの手法は、システム管理者と監査の責任者を、確実に異なる二人の人物にすることである。「監査人の機能、データベースおよびアクセス権限をシステム管理者から分離することは、権限の分離と最少特権原則の重要な応用である。万一こういった分離が行われなかったり、管理者が監査人の機能を引き受けるべきかあるいはその逆を行ったりしたら、すべてのセキュリティ機能は一人の説明責任が不明確な個人の責任に帰すことになるだろう。」[2]

もう一つの代案は、監査人雇用に当り役割を分離することである。このような場合は、一人に監査機構を停止する権限を与える一方、もう一人に開始する権限を与える。この場合、誰も監査機構を止めてシステムを侵害し、しかる後に監査機構を動かすという一連の動作を行うことは出来ない。

8.6.2 データ損失

監査のソフトウェアとハードウェアは信頼できるセキュリティ機構であるが、絶対に確実なものではない。システムの他の部分のように、それらは電源のコンスタントな供給に依存し、機械的なあるいは電源の故障によって簡単に中断させられる。これらの故障は、貴重な監査データの損失や破壊

を引き起こす。システムセキュリティ管理者はこのリスクを知っておくこと、そして監査証跡がいずれかに保存されていることを確実にする何らかの手順を確立することが望ましい。システムセキュリティ管理者は、システム故障の発生によるデータ損失を最少にするために、ある時点でリムーバルメディア上の監査証跡の複製を作成することが望ましい。高信頼設備マニュアルには、データ損失の可能性と、発生するデータ損失の性質がいかなるものか、および、災害が起こったときに、どのようにしてデータを復元するかを含めていることが望ましい。

機械的なあるいは電源の故障が起こった場合も、システムセキュリティ管理者はシステム復旧の後にも、監査機構が正しく動いていることを確認することが望ましい。例えば、システム異常の前に事前選択オプションを使用した監査機構はシステム復旧後もそれが作動していなければならない。

9. 監査のまとめ

C2 とそれ以上のクラスでは、TCB は「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、そして、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」[1] ことが要求されている。監査証跡は、システム障害の場合に、損害評価を行う鍵となる役割を果たす。

監査証跡は、識別と認証の機構の使用、ユーザアドレス空間への客体(Object)の導入、システムからの客体(Object)の削除、システム管理者の行動、およびシステムのセキュリティポリシー侵害の試みなどのような、すべてのセキュリティ関連イベントの足跡を記録しなければならない。すべての動作を監査するか、システムセキュリティ管理者が監査すべきイベントを選択できるか、いずれかのオプションがあることが望ましい。すべての動作を監査するのが望ましいと判断した場合、考慮すべきオーバーヘッドの要因が存在する。監査証跡のために必要なストレージ容量は、データの損失を防ぎ十分な保護を提供するために、オペレータの保守を一般にはより多く必要とする。承認された個人が監査証跡に記録されたすべてのイベントを読めるようにしなければならないという要求がある。総合的な監査証跡の解析は、管理者にとって難しく、手間のかかる仕事であるかもしれない。したがって、事前選択か事後選択かいずれかを選択するオプションが必要である。

監査証跡の情報は、セキュリティ関連イベントおよびシステムにおけるプロセスの完全な順序を再構築するのに十分であることが望ましい。そのためには、監査証跡は次の情報を含まなければならない。即ち、イベントの日付と時間、ユーザ、イベントのタイプ、イベントの成否、要求元、ユーザアドレス空間に作成された客体 (Object) 、同アクセス、ストレージシステムからの削除、および B1 とそれ以上のクラスでは客体(Object) の 機密レベル、である。

監査証跡はトラステッド・コンピューティング・ベースに含まれていなければならず、TCB と保護が同一でなければならないことを覚えておくことが望ましい。監査証跡は、厳格なアクセス制御に従わなければならない。

効果的な監査証跡は、システムへの好ましくない攻撃を検知し評価するために必要である。

用語集

管理者(Administrator)－ADP システムのすべてあるいは一部を監督するために割り当てられた人々のグループの任意の一人。

アーカイブ(Archive)－オフラインで記録をファイルするかまたは保存すること。

監査(Audit)－システムの記録および行動を独立的にレビューし検査すること。

監査人(Auditor)－管理義務を負った承認された個人。システムの監査されるべきイベントの選択、それらのイベントの記録を可能にする監査フラグを設定、監査イベントの証跡の解析がその任務に含まれる。[2]

監査機構(Audit Mechanism)－システムの行動を収集し、レビューし、調査するために使用されるデバイス。

監査証跡(Audit Trail)－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順方向へ、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。[1]

監査可能なイベント(Auditable Event)－監査証跡に含めるために選択することができるイベント。これらのイベントには、セキュリティ関連イベントに加えて、障害の後のシステムを復旧するために行ったイベント、及び後にセキュリティに関連したことを証明できるイベントを含めるべきである。

承認されたユーザ(Authenticated User)－有効な識別子と認証の組み合わせによって ADP システムへアクセス可能なユーザ。

自動データ処理(ADP) **システム**(Automatic Data Processing(ADP) System)－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。[1]

カテゴリー(Category)－取扱注意として分類されたあるいは分類されない、正式に承認されるか他の適切な承認がある場合にのみ個々人がアクセスを許可されることを示す、追加の制限レベルが適用された情報(例えば占有の区分された情報)をグループにしたもの。[4]

隠れチャネル(Covert Channel)－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。[1]

隠れストレージチャネル(Covert Storage Channel) －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。[1]

隠れタイミングチャネル(Covert Timing Channel)－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。[1]

欠陥(Flaw) －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。[1]

客体(Object) －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、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。[1]

(訳注：日本セキュリティ・マネジメント学会による[1] の翻訳では、「オブジェクト」となっているが、本書では 「客体(Object) 」と記載した。)

事後選択(Post-Selection)－承認された者によって、監査証跡に記録された特定のイベントを選択すること。

事前選択(Pre-Selection)－承認された者によって、監査証跡に記録されるべき特定のイベントを選択すること。

セキュリティレベル(Security Level)－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。 [1]

セキュリティポリシー(Security Policy)－一連の法律、規則および習慣であって、機密度の高い情報を如何に管理し、保護し、分配するかを規制するもの [1]

セキュリティ関連イベント(Security-Relevant Event)－システムのセキュリティ状態の変更を試みる全ての出来事（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全ての出来事。（例：極めて多数のログイン試行、装置の強制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） [1]

取扱注意情報(Sensitive Information)－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目に見える損害を生じさせるので、権限ある当局によって決定せられた保護されなければならない情報。 [1]

（訳注：日本セキュリティ・マネジメント学会による [1] の翻訳の例にならい、“ Sensitive Information ”は「取扱注意情報」と翻訳した。）

主体(Subject)－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。 [1]

（訳注：日本セキュリティ・マネジメント学会による [1] の翻訳では、「サブジェクト」となっているが、本書では「主体（Subject）」と記載した。）

主体取扱注意レベル(Subject-Sensitivity Level)－主体が読み書きの両方のアクセスを行う客体の取扱注意レベル。主体の取扱注意レベルは、常に主体が関連付けられたユーザの許可レベルと同等かそれより低くなければならない [4]

システムセキュリティ管理者(System Security Administrator)－ 自動情報システムのセキュリティ責任を持ち、児童情報システムへアクセスする全ての他の者にセキュリティの防衛手段を強制する権限を持つ者。 [4]

トラステッド・コンピューティング・ベース(TCB)（Trusted Computing Base）－ 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のメカニズム全体。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一つ以上のコンポーネントによって構成される。正しくは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。[1]

ユーザ(User)－直接コンピュータシステムとやり取りする人 [1]

引用文献

[1] National Computer Security Center, DoD Trusted Computer System Evaluation Criteria, DoD, DoD 5200.28-STD, 1985.

[2] Gligor, Virgil D., "Guidelines for Trusted Facility Management and Audit," University of Maryland, 1985.

[3] Brown, Leonard R., "Guidelines for Audit Log Mechanisms in Secure Computer Systems," Technical Report TR-0086A(2770-29)-1, The Aerospace Corporation, 1986.

[4] Subcommittee on Automated Information System Security, Working Group #3, "Dictionary of Computer Security Terminology," 23 November 1986.

[5] National Computer Security Center, Criterion Interpretation, Report No. C1- C1-02-87, 1987.