最も高度な保証作業は、愚かなロボットによって制御される運動装置と地獄の機械の領域で行われました。  
– EARL BOEBERT  
政府の電話のパスワードは常に下がっているようで、私はそれを理解することができませんでした。米国の外交官で元CIAの担当者であるKURT VOLKERが、自分の個人用電話からテキストメッセージを送った理由を説明しました。あなたが漏れます。彼/彼女は分類された情報を漏らすことによって犯罪を犯します。  
  
9.1はじめに  
セキュリティポリシーは、私たちが達成しようとしていることを簡潔に説明したものです。これは、回避したい悪い結果を理解し、エンジニアリングを推進することによって推進されます。  
 機密情報、機密情報、極秘情報など、さまざまな分類レベルで情報を保持する多くの軍事システムや諜報システムで使用されるポリシーモデル  
このようなポリシーは、情報フロー制御（IFC）としても知られるようになりました。  
政府の請負業者のために働くつもりがない場合でも、これらはいくつかの理由で重要です：1。  
したがって、モデルは非常に詳細に検討され、熱意をもって単一の政策目標を追求することの二次的な影響を理解することができました。 2。  
 第6章で説明したように、マルウェアの改ざんからコアコンポーネントを保護するために、Android、iOS、Windowsなどのすべての主要なオペレーティングシステムに実装されていました。 3。  
たとえば、安全性が重要なシステムは、多くの安全度整合性レベルを使用します1。  
セキュリティエンジニアリングは通常フォックスの領域にありますが、マルチレベルセキュリティはハリネズミアプローチの例です。  
9.2セキュリティポリシーモデルとは  
このプロセスの重要で、しばしば無視されている部分は、セキュリティポリシーです。  
これは、脅威に対する私たちの理解によって推進され、次にシステム設計を推進します。  
これは、システムの保護要件を指定し、それらが満たされているかどうかを評価するのと同じ役割を果たし、システム仕様は機能性について、安全性については安全ケースで行います。  
多くの組織では、図9.1のように、「セキュリティポリシー」という表現を使用して、空虚なステートメントの集まりを意味しています。1この用語は、安全工学の分野によって異なることに注意してください。  
このポリシーは経営陣によって承認されています。  
すべてのスタッフは、このセキュリティポリシーに従うものとします。  
データは、「知る必要がある」者のみが利用できるものとします。  
このポリシーの違反はすべて、一度にセキュリティに報告されるものとします。  
それは中心的な問題、つまり「誰が「知る必要があるか」をどのように決定するかを回避します。  
。  
 従順はシステムによって強制される必要がありますか、それともユーザーは「名誉」に基づいていますか？  
 考えてみると、これは政治的な言葉です。  
「セキュリティポリシー」という用語は、政治にセキュリティを使用することを意味するように乱用されることが多いため、セキュリティエンジニアはより正確な用語を使用するようになりました。  
その重要なポイントは通常、1ページ以下で書き留めることができます。  
それはまた、正式な数学的分析の基礎になるかもしれません。  
。  
保護プロファイルはセキュリティターゲットのようなものですが、製品に依存しない方法で表現され、製品やバージョン間で比較可能な評価を可能にします。  
保護プロファイルは、コモンクライテリア[1396]に基づいて評価される製品の要件です。  
 それほど正確である必要がない場合は、「セキュリティポリシー」という語句を使用して、セキュリティポリシーモデルまたはセキュリティターゲットを指す場合があります。  
2大きなプロジェクトは、仕様が政治的になると企業で失敗することが多く、政府が運営する場合はさらに失敗します。問題についてはパート3で詳しく説明します。  
より一般的には、モデルがすでに存在しています。適切なものを選択し、それをセキュリティターゲットに開発する必要があります。  
本のこのセクションでは、いくつかのセキュリティポリシーモデルを提供し、実際のシステムのコンテキストでそれらを説明し、エンジニアリングメカニズム（および関連する制約）を調べます  
  
1940年3月22日、ルーズベルト大統領は大統領令8381に署名し、特定の種類の情報を制限付き、機密、または秘密に分類できるようにしました[978]。  
これは、文書の機密性のための一般的な保護マーキングスキームに発展し、冷戦時代にもNATO政府によって採用されました。。  
政府の従業員と請負業者は、彼らが吟味されたケアに応じて許可を得ています。たとえば、米国では、「秘密」のクリアランスにはFBI指紋ファイルのチェックが含まれますが、「トップシークレット」には、以前の5〜15年の雇用に加えて面接と、多くの場合、ポリグラフテスト[548]のバックグラウンドチェックも含まれます。  
アクセス制御ポリシーはシンプルでした。クリアランスがドキュメントの分類と少なくとも同じ高さの場合にのみ、ドキュメントを読むことができます。  
そのため、情報は機密情報から機密情報、さらには極秘情報へと上向きにしか流れませんが、許可された人が意図的に情報を分類解除しない限り、下向きになることはありません。  
文書を分類するための損傷基準は、軍事的影響の可能性から3に拡大されました。2015年6月に、中国の諜報機関によって人事管理局から約2000万人のアメリカ人の通関審査データが盗まれました。  
振り返ってみると、敏感な仕事ですべての市民のすべての汚れを集めることは素晴らしいアイデアではなかったかもしれません。  
分類も公開もされていない情報は、「管理された未分類情報」（CUI）と呼ばれます  
特にSecret以上の情報をさらに制限できるコードワードのシステムもあります。  
一部のコードワードは、特定の軍事作戦または情報源に関連しており、指名されたユーザーのグループのみが使用できます。  
分類ラベルと一連のコードワードは、セキュリティカテゴリを構成します（または、少なくとも1つのコードワードがある場合）。  
コンパートメントは通常、任意のアクセス制御メカニズムを使用して今日実装されています。これについては次の章で説明します。  
記述子は「管理」、「予算」、「予定」などの単語です。これらは特別な処理要件を呼び出さないため、「機密-管理」とマークされたファイルを単に「機密」とマークされているかのように扱うことができます。  
NATO5などの国際防衛機関のマーキングもあります。  
より詳細な説明は[1562]にあります。  
9.3.1アンダーソンレポート  
USAFで働いていたPaul Kargerは、機密システムからログオフし、庭を横切って別の小屋に行き、武装した警備員にパスを見せてから、シークレットシステムにログインしてログオンする必要があると説明しました。 1日に数十回。  
 オペレーティングシステムのバグが1つ修正されるとすぐに、他の脆弱性が発見されます。  
未熟なユーザーでもCUIシステムを採用する前に4が常に心配されていたため、米国には、管理対象であるが分類されていないデータについて、公式使用のみ（FOUO）を含む50を超える異なるマーキングがありました  
、独自仕様（PROPIN）  
、機密ですが未分類（SBU）  
一部の機関は、調整なしで独自のラベルを作成しました。  
このマーキングの管理から単一の中央管理された政府全体のシステムへの移行には10年以上かかり、現在も継続中です。  
5不思議なことに、英国では「NATOシークレット」は「シークレット」よりも秘密度が低いため、コンテンツを格子ではなく上に移動させる一種のアンチコードワードです。  
（ウイルスは1980年代まで発明されませんでした。70年代の懸念はトロイの木馬でした。）  
 トロイの木馬攻撃に対して脆弱でした。これは、使用を「トップシークレット」のクリアランスを持つ人々に制限する効果があり、不便でした。  
参照モニターの概念を導入しました。これは、アクセス制御の決定を仲介し、分析とテストの対象となるのに十分なほど小さいオペレーティングシステムのコンポーネントであり、その完全性が保証されます。  
。  
 その正しい機能は、セキュリティポリシーが適用されることを保証するのに十分であり、またはより明確に、その失敗はセキュリティポリシーの違反を引き起こす可能性があります。  
  
広く受け入れられたマルチレベルのセキュリティポリシーモデルは、1973年にDave BellとLen LaPadulaによって提案されました[210]。  
より正式には、Bell-LaPadula（BLP）  
これは、読み取りなし（NRU）とも呼ばれます  
これは、ノーライトダウン（NWD）とも呼ばれます。  
\*プロパティはBellとLaPadulaの重要なイノベーションでした。  
クリアされていないユーザーがトロイの木馬を作成し、システム管理者が「シークレット」にクリアすることを許可する場所にトロイの木馬を放置する可能性があります。次に、システムの「秘密の」部分に自分自身をコピーし、そこでデータを読み取り、何らかの方法で信号を送ろうとします。次に、作成者がそれらを読み取ることができる場所までそれらを書き留めることができれば、セキュリティポリシーに違反したことになります。  
悪意のあるコードやバグのあるコードなどの脆弱性が想定されています。  
したがって、既存の文化では、セキュリティポリシーはユーザーの操作とは無関係に実施されると想定されていました。 Bell-LaPadulaは、ユーザーの直接的なアクションだけでなく、間接的なアクション（ユーザーが実行するプログラムによって実行されるアクションなど）からも独立してそれを強制することを目指しています。  
したがって、「秘密」で実行されているプログラムが「未分類」のファイルに書き込むことを防ぐ必要があります。  
ユーザーのアクションとは無関係にセキュリティポリシーを適用するシステムは、ユーザーがファイルに関する独自のアクセス決定を行うことができるUnixなどのシステムの任意アクセス制御とは対照的に、必須のアクセス制御を持つと説明されています。  
両方の単純なセキュリティプロパティを指定（読み取りなし）  
、さまざまな結果を証明できます。特に、開始状態が安全であれば、システムは安全です。  
  
BLPの導入は多くの興奮を引き起こしました。ここでは、防衛組織が望んでいたことを実行したセキュリティポリシーがあり、直感的に明確でありながら、人々が定理を証明できるようにしました。  
最初の大きな論争は、ジョンマクリーンのシステムZに関するものでした。これは、ユーザーがシステム管理者にファイルを一時的に高から低に分類解除するように要求できる追加機能を備えたBLPシステムとして定義されました。  
Dave Bellは、System Zがモデルで許可されていない操作を実行することで不正行為を行っていると反論しました（ラベルの変更は、この状態では有効な操作ではありません）。  
この問題は、静けさの特性を導入することによって処理されます。  
なぜ静寂が弱いのですか？  
その後、機密のメールにアクセスすると、セッションは自動的に「機密」にアップグレードされます。一般に、プロセスはより高いレベルでデータにアクセスするたびにアップグレードされます（最高水準点の原則）  
サブジェクトは通常、プロセスではなくメモリ管理サブシステムとファイルハンドルを抽象化したものであるため、これは、データが実際に移動するときではなく、アクセス権が変化したときに状態が変化することを意味します。  
したがって、「Secret」と「Crypto」でファイルを読み取ったプロセスは、その後「Secret Crypto」とマークされたファイルを作成します。  
その後、「Secret Nuclear」でファイルを読み取ると、それ以降に作成されるすべてのファイルに「Secret Crypto Nuclear」というラベルが付けられ、「Secret Crypto」で一時ファイルに書き込むことができなくなります。  
 MLSプラットフォームで実行します。  
また、失効の問題は、現在のオペレーティングシステムでは、少なくとも完全な形では一般に解決できないため、アプリケーションは何らかの方法で対処する必要があります。  
これを防ぐために、ラベルは一般にMLS機構の外に持ち出され、任意アクセス制御メカニズムを使用して処理されます（これについては次の章で説明します）。  
BLPのもう1つの問題、そしてすべての必須のアクセス制御システムには、ユーザーとプロセスの分離が簡単な部分があります。難しいのは、制御された相互作用が必要な場合です。  
BLPは、システムがこのようなアプリケーションを保護する方法については何も述べていません。  
最後に、ハイウォータマークの精緻化を行っても、BLPはサブジェクトまたはオブジェクトの作成または破棄をまだ処理しないことに注意してください（これは、実際のMLSシステムを構築する際の難しい問題の1つです）。  
  
マルチレベルのセキュリティポリシーは、実用世界と研究世界の両方で並行して進化しています。  
これは、レベル、コンパートメント、およびグループの3つを使用し、グループはファイル、ユーザー、端末、およびジョブです。  
 対象であったため、トロイの木馬の攻撃に対して脆弱でした。  
次の大きなステップはMulticsでした。  
ポールカーガーとロジャーシェルによって行われた評価は非常に影響力があり、マルウェアがコンパイラに隠されている可能性があるという考えが最初に現れ[1019]、ケントンプソンの有名な論文「Retrustions on Trusting Trust」につながりました。 10年後[1883]。  
1980年代からマルチレベルのセキュリティに注がれた研究資金の急流は、いくつかの代替的な定式化につながりました。  
このプロパティを持つシステムでは、HighのアクションはLowが見ることができるものに影響を与えません。99％の確実性でHighの入力についてのLowの推論を止めることができないため、非推定性は弱すぎることがわかりました。  
 ポリシーは、最高水準点ポリシー[2040、807]のように、フローティングラベルを使用して情報の分類をモデル化しようとしました。  
 Earl BoebertとDick Kain [271]によるモデルで、後にLee Badgerと他の人々によってドメインおよびタイプ施行（DTE）に拡張  
これにより、サブジェクトがドメインに、オブジェクトがタイプに割り当てられます。マトリックスは、許可されたドメイン-ドメインおよびドメイン-タイプの相互作用を定義します。  
実際には、これは2番目のアクセス制御マトリックスです。ユーザーIDとグループIDに加えて、各プロセスにはセキュリティID（SID）があります。  
Linux Security Modulesフレームワークは、SIDを操作するルールを設定できるプラグイン可能なセキュリティを提供します。  
、およびパス名に基づいたファイルの暗黙の型指定。そのため、特定のサブディレクトリ内のすべてのオブジェクトは、特定のドメインにあると宣言できます。  
初期の用途の1つは、信頼できるパイプラインを適用することでした。アイデアは、パイプライン内の一連のプロセスを制限して、それぞれが前のステージと次のステージとしか通信できないようにすることです。  
型強制メカニズムはコードとデータを認識でき、特権をコードにバインドできます。その結果、静けさの問題は、データが読み取られるときではなく、実行時に処理できます。  
たとえば、Sidewinderファイアウォールで使用されます。  
他のメカニズムを使用してポリシーの複雑さを管理できます。たとえば、プロトタイプをしばらく実行して、通常の動作と見なされるものを観察します。次に、DTEをオンにして、これまでに見られなかったすべての情報フローをブロックできます。  
また、兵士が電話をかけるための設備など、高ネットワークでの低トラフィックについて考える必要があるかもしれません。  
1992年、役割ベースのアクセス制御（RBAC）  
これは、個々のユーザーやマシンではなく、主にロールに適用されるルールを正式化します[678、679]。  
。  
たとえば、「Ross as Professor」、「Ross as the members of Admissions Committee」、「Ross reading private email」など、さまざまなアクセス権を付与することで、きめ細かな制御が可能になります。  
、コンテキストを追加して、「研究室の彼のワークステーションにあるロス」と「地球上のどこかにある彼の電話のロス」を区別できるようにします。  
SELinuxはTEの上にそれを構築するため、ユーザーはログイン時にロールにマップされ、ロールはドメインに対して許可され、ドメインにはタイプへのアクセス許可が与えられます。  
したがって、たとえば、ネットからダウンロードされた信頼できないソフトウェアを呼び出すプロセスは、機密性の高いシステムファイルへの書き込みに必要なロールメンバーシップを失う可能性があります。  
  
マルチレベルの整合性モデルをWindows 7に組み込んだことで、1975年にケンビバ[237]が考案したセキュリティモデルへの関心がよみがえりました。これは整合性のみを扱い、機密性を無視します。  
したがって、BLPを上下逆にすることで整合性ポリシーにリサイクルできます。  
校正データは破損から保護する必要があるため、通常のユーザーはデータを読み取ることはできますが、書き込むことはできません。通常のユーザーがデバイスをリセットすると、現在のユーザー状態（つまり、メモリ内の患者データ）が失われます  
許可された技術者のみがキャリブレーションをやり直すことができます。  
 より低いレベルに書き込む（つまり、キャリブレーションプロセスはユーザープロセスのバッファーに書き込むことができます）  
信頼できない可能性がある–データ。  
これは整合性の最初の正式なモデルでした。  
たとえば、鉄道の乗客情報システムは信号システムから情報を取得できますが、それに影響を与えることはできません。また、電力会社の配電システムは、安全システムの状態を確認できますが、それらに干渉することはありません。  
Windows、バージョン6以降（Vista）  
重要なファイルはシステムにあり、他のオブジェクトはデフォルトで中程度にあります–低にあるブラウザを除いて。  
目標は、マルウェアによる被害を制限することです。  
多数の例外がなければ、実際の運用にうまく対応できません。  
たとえば、車のエアバッグはエンジンよりも重要度の低いバス上にありますが、それが展開するときは、燃料が燃えるリスクがあり、エンジンをオフにすることを想定しています。  
Windowsの場合、MicrosoftはNoReadDown制限を廃止し、その整合性モデルを使用してユーザーから基本システムを保護することはしませんでした。これは、より頻繁なユーザー確認が必要になるためです。WindowsにTEが組み込まれていないのは残念です。  
9.4 MLSシステムの歴史的な例  
  
重要な製品はセキュア通信プロセッサ（SCOMP）でした  
これは、米国国防総省が複数のレベルの分類でメッセージングを処理するために必要であると信じていたものの費用節約のない実装でした。  
そのオペレーティングシステムであるSTOPは、Multicsのリングシステムを使用して、最大32の個別のコンパートメントを維持し、コンパートメント間で適切な一方向の情報フローを可能にしました。  
これらは、メールが低から高に通過することを許可するが、その逆は許可しないファイアウォールです[538]。  
 SCOMPの後継であるXTS-300は、C2G、コマンドおよびコントロールガードをサポートしていました。  
 その機能は、米軍の移動と関連するロジスティックスを計画することでした。  
これは、1985年に導入され、最終的に2000年12月に廃止された、安全なコンピュータシステムに関する最初の体系的な標準セットでした。  
Orange Bookを使用すると、システムをさまざまなレベルで評価することができ、A1が最高で、B3、B2、B1、C2からC1に下がっていきます。  
また、公開された文献にも広く記載されていました。  
AT＆TのSystem V / MLS [47]など、MLSバージョンのUnixは1980年代後半に登場し始めました。  
この本の第2版（2007年）  
コンパートメントモードワークステーション（CMW）  
エンジニアリングについては、[635、636]を参照してください。  
9.4.2データダイオード  
第1世代のMLSメカニズムは、リアルタイムサービスには非効率的でした。  
 したがって、ポンプを開発しました–一方向のデータ転送デバイス（データダイオード）  
主な問題は、データをLowからHighに送信するのは簡単ですが、伝送の信頼性を保証する必要があるということは、確認メッセージをHighからLowに送り返す必要があるということです。  
このアプローチの魅力は、データダイオードを使用して異なるセキュリティレベルで個別のシステムを接続することにより、MLSシステムを構築できることです。  
 コンポーネント。  
ハードウェアのコストが下がったため、これが推奨されるオプションになり、世界の軍事基地にはKVMスイッチがいっぱいになりました（キーボード、ビデオディスプレイ、マウスをローシステムとハイシステムの間で切り替えることができます）。  
。  
初期のアプリケーションはロジスティクスでした。  
これらすべてを管理するために必要なシステムは、構築するのが難しい場合があります。米国と英国の両方でのMLSロジスティクスプロジェクトは、高額な災害に終わりました。  
 10年（1989–99）  
ジェット燃料とブーツポリッシュには「制限」、核爆弾などの特別な店には「シークレット」の2つのレベルで動作するように設計されています。  
プロジェクトは、要件の忍び寄る変化によって引き起こされるコストの増大の古典的な物語になりました。  
その結果、「秘密」の情報のほとんどすべてが静的であることがわかりました（たとえば、空中核爆弾の操作マニュアルは現在、基地ではなく戦略的備蓄に保管されています）  
お金を節約するために、「秘密」の情報はCDに保存され、金庫に保管されます。  
調査の対象者は盗聴されていることを知らないはずなので、第三者は沈黙している必要があります。電話会社が盗聴を無言の電話会議として実装し始めたとき、電話会議の料金は盗聴者ではなく、盗聴者に支払わなければなりませんでした。目標。  
隠れチャネルを排除することは、見た目よりも困難です。 2000年代半ばの調査については、[1707]を参照してください。容疑者は盗聴装置をハッキ​​ングしたり混乱させたりする可能性があるため、純粋なMLSセキュリティポリシーでは不十分であり、したがってオンラインでの改ざんに抵抗する必要があります。  
電話会社は7,600万ユーロ（ほぼ1億ドル）を支払いました  
最近のVoIPシステムで盗聴を管理するためのクリーンな方法は、すべてをディスクに書き込み、後で必要なものを抽出することです。  
MAC：MLSからIFCと整合性へ軍用組み込みシステムも数多くあります。  
船が港にいるときに機器が最高機密にならないようにする必要があるため、エンジニアリングがより複雑になり、メンテナンスが複雑になります。  
レーダーの速度が意味をなさないめちゃくちゃ速いUFOを見ているF-16パイロットの話を読むとき、2つと2つを組み合わせることができます。  
  
この本の初版では、改ざんを防止し、リアルタイムのパフォーマンス保証を提供するために必須のアクセス制御を使用する傾向に言及し[1313、1018]、「多分システムの実際の未来はおそらく機密性に欠けている、しかし誠実さ。」政府機関は、MACがマルウェアを阻止するために必要なものであることを知っていました。Windowsでは、すべてのプロセスが実行され、すべてのセキュリティ保護可能なオブジェクト（ディレクトリ、ファイル、レジストリキーを含む）  
ファイルオブジェクトはデフォルトで「中」と表示されますが、Internet Explorer（およびそれを使用してダウンロードされたすべてのもの）  
したがって、既存のファイルを変更する前に、ダウンロードしたコンテンツをアップグレードするためのユーザーアクションが必要です。  
これらはデフォルトではインストールされません。マイクロソフトは、マルウェアがシステムにインストールされてから隠れることを懸念していました。  
 システムの残りの部分を検査すると、隠蔽が難しくなります。  
これはすべて[1634]のJoanna Rutkowskaによって議論されています。また、仮想化に基づく興味深い潜在的な攻撃についても説明します。  
9.5.2 SELinux  
SELinux [1187]は、ポリシーを施行メカニズムから分離するFlaskセキュリティアーキテクチャ[1811]に基づいてNSAによって実装されました。セキュリティコンテキストには、Flaskのサブジェクトまたはオブジェクトに関連付けられているすべてのセキュリティ属性が含まれています。これらの属性の1つには、タイプ強制タイプ属性が含まれています。  
これは、ポリシー決定が行われる場所であり、パフォーマンスのためにカーネルに常駐します[819]。  
サーバーは、残りのカーネルにセキュリティAPIを提供し、その背後にセキュリティモデルが隠されています。  
2000年代半ば以降の一般的なLinuxディストリビューションでは、さまざまなサービスを分離するために使用されていたため、Webサーバーを乗っ取った攻撃者がDNSサーバーを取得することもありませんでした。  
  
Bibaモデルのバリアントを実装するフィールドシステムは数多くあります。  
たとえば、電力会社では、通常、最高の安全度レベルで完全に独立して動作する安全システムの階層があります。これらは、電力供給などの運用システムからは見えますが、影響を受けることはありません。小売レベルのメータリングシステムは、課金システムによって監視できますが、影響を受けません。  
ラジオでは、悪意のあるアプリがブレーキを操作できるようにしたくないので、自動車では、ほとんどのメーカーがパワートレインとキャビンに別々のCANバスを持っています（2010年に、セキュリティ研究者は、分離が完全に不十分であることがわかりました） [1085]）  
単純な整合性制御は、マルウェアがマシンを乗っ取ることを停止するだけであることにも留意する必要があります。低コンパートメントへの感染を阻止し、それを他の場所に拡散したり、他のマシンに指示を出すための踏み台として使用することはありません。  
ですから、これから説明するいくつかの障害モードを実行します。  
9.6間違ったこと  
高レベルの保証を備えた単純なポリシーに従うためにシステムを構築するために費やされた数十億ドルは、情報フロー制御の多くの2次および3次の結果を明らかにしました。  
  
2つの「High」入力H1とH2を受け入れる単純なデバイスを考えます。それらを多重化します。ワンタイムパッド（ランダムジェネレーター）でXORすることで暗号化します  
、図9.4のように。  
ただし、フィードバックが許可されている場合は、H3からの出力をH2にフィードバックできます。その結果、高入力H1が低出力Lに現れます。  
。  
（単純な情報フローは構成されません。干渉も推定も不可能です。）  
ただし、現実にはフィードバックが行き渡り、セキュリティのプロパティの構成は、インターフェイスの問題や機能の相互作用などによってさらに難しくなる可能性があります。  
また、安全なコンポーネントの構成は、上位レベルの非互換性に不満を感じることがよくあります。  
  
合成問題の例は、カスケード問題によって示されます（図9.5）  
オレンジの本が一連の評価レベルを導入した後、これはシステムが動作できるレベルの数に関するスパン制限ルールにつながりました[548]。  
トップシークレットシークレットシークレット未分類図9.5：–カスケード問題図が示すように、このポリシーが破られるような方法で2つのB3システムを接続することは簡単です。  
これにより、スパン制限が無効になります。  
9.6.3隠れチャネル  
1973年にランプソンによって最初に指摘された[1125]秘密チャネルは、通信用には設計されていませんが、悪用されて情報が高から低に伝達されるメカニズムです。最新のマルチコアCPUでは、時刻tiで使用しているCPUコアのクロック周波数を上げて、トップシークレットファイルのi番目のビットが1であることを通知し、そのビットが0。  
2018年以降、CPU設計者は、CPUマイクロアーキテクチャを利用する一連のカバーチャネルに苦労しています。 Meltdown、Spectre、Foreshadowなどの名前で、HighがLowに信号を送るだけでなく、Lowがアクセス制御を回避してHighでメモリを読み取る方法を提供しています。  
開発者が通常のオペレーティングシステムで機密保護を一貫して行うことができた最善の方法は、1秒あたり1ビット程度に制限することです。  
 衛星写真などの大きなTS / SCIファイルがTS / SCIユーザーから「シークレット」ユーザーに漏れるのを防ぎたい環境では、1秒あたり1ビットは許容できるかもしれません。  
これは、特別な目的のハードウェアで暗号化を行うという軍および銀行の法理の理由の1つです。  
この場合、秘密チャネルの帯域幅は毎秒数メガビットであるため、レーダーコードは信頼されている必要があります。  
9.6.4マルウェアからの脅威  
彼の最初の実験では、書き込みに8時間しかかからなかったファイルウイルスが、以前はマルチレベルで安全であると考えられていたシステムに侵入することができました[450]。  
悪意のあるコードを使用してアクセス制御を破る方法はたくさんあります。  
 マルウェアは破損する可能性があり、マルウェアは、たとえば不正なクリアランスを発行することにより、システム全体を攻撃者に配信できます。  
ただし、TCBがそのまま残っていても、マルウェアはそれ自体を低から高にコピーする可能性があります（これはBLPでは防止されません）。  
  
研究コミュニティを動かしたもう1つの問題は、多インスタンス化です。  
MLSオペレーティングシステムが彼を禁止している場合、情報が漏洩します。つまり、エージェントがHighにあるというファイルがあります。  
多くの場合、低ユーザーと高ユーザーに異なるディレクトリを割り当てるなど、命名規則によって問題を解決できます。  
Highユーザーが船に分類された貨物を割り当てるとします。  
ここでは、米国と英国の慣行が分かれています。  
したがって、基礎となるデータは図9.6のようになります。  
利用可能な2つのビューは、図9.7のようになります。  
また、カバーストーリーで発生する可能性があるミスや隠れたチャネルも防止します（たとえば、低ユーザーがキプロスの弾薬のコンテナを追加しようとします）。  
欠点は、誰もが自分の仕事を成し遂げるために利用可能な最高のクリアランスを必要とする傾向があることです。  
   
マルチレベルの安全なシステムは驚くほど高価であり、構築と展開が困難です。  
1。  
2。  
訓練を受けたUnix管理者は、有意義な訓練をせずにMLSのインストールを行うことはできません。多くのMLSシステムは、機能を使用せずにインストールされます。  
MLSオペレーティングシステムで実行するには、多くのアプリケーションを書き直すか、少なくとも大幅に変更する必要があります[1629]。  
新しいラベルが表示されると、プロセスは自動的にアップグレードされるため、プロセスが使用するファイルもそうでなければなりません。  
これらすべての結果、物事が過剰に分類される慢性的な傾向があります。  
したがって、信頼できるコンピューティングベースに配置され、オペレーティングシステムのかなり不快な部分（ユーティリティ、ウィンドウシステムソフトウェア、データベースソフトウェアなどのミドルウェア）が含まれます。  
この「TCB膨張」は、評価のコストを常に押し上げ、保証を減らします。  
データの分類は複雑になる可能性があります。•衝突の前段階で、食品などの「無害な」店舗の場所が戦術的な意図を明らかにする可能性があるため、突然アップグレードされる可能性があります。 •分類は常に単調であるとは限りません。  
インテリジェンスアナリストは、TS / SCIで分類された衛星写真を撮り、それを「秘密」のフィールド司令官の評価に貼り付ける必要がある場合があります。  
1つのオプションは、ドキュメントをビットマップに変換し、追跡可能にするためにログに記録する「印刷とFAX」メカニズムです。  
たとえば、衛星写真を1つでも機密解除してもかまいませんが、コレクション全体を機密解除すると、監視機能と機密情報の優先順位の履歴が明らかになります。  
 •同様に、分類されていないデータに作用する分類されていないプログラムの出力は分類されます。たとえば、オンラインフォーラムに適用される標準のデータマイニング技術がテロの疑いのリストを表示する場合などです。MLSシステムは望ましくないもの（情報漏えいなど）を防ぐことができますが  
。  
9月11日以降、多くのルールが緩和され、情報の共有を可能にするために、トップシークレットを超えるアクセス制御は通常任意です。  
7。  
故上院議員ダニエル・モイニハンは、その実際の目的と、米国の外交および軍事問題における莫大な費用について批判的な研究を書いた[1346]。  
彼が述べたように：「部門と機関は情報を蓄え、政府は一種の市場になります。  
、そしてコロナウイルス危機の間のイギリス政府のキャビネット会議のための悪名高い安全性のないズームビデオ会議システムの使用（政府の暗号化されたビデオ会議端末は分類されているので、大臣は家に持ち帰ることができません）  
これは、怒り狂った英国の将軍の短所を思い起こさせます。「ジュラシックパークと国防省の違いは何ですか？  
MitreのJASONプログラムによる米国の分類システムに関する2004年のレポートは、それが目的に適合していないと結論付けました[978]。  
攻撃が比較的容易なため、政府のシステムは保守的でリスクを回避しすぎています。  
代わりにマイターは、特に戦術的な区画に傷みやすい情報を取得する場合、特定の目的のために柔軟なコンパートメントを設定することを提案しました。権利の管理や仮想化などのテクノロジーをインテリジェントに利用できること。そして、クリアされた個人に対する生涯の信頼は、取引リスクに焦点を当てたシステムに置き換えられます。  
現在、ほとんどの政府システムはシステムを高いレベルで運用しています。つまり、完全に公式、またはシークレット、またはトップシークレットです。  
したがって、展開されたMLSシステムは、異なるレベル間のファイアウォールまたはメールガードになる傾向があり、多くの場合、新しい頭字語MILS（複数の独立したレベルのセキュリティ）によって参照されます。  
実際の分離は、未分類のネットワーク、Secret Internet Protocol Router Network（SIPRNet）の間のネットワークレベルにあります。  
 トップシークレットの資料を処理し、そのシステムがセキュアコンパートメント化情報施設（SCIF）に保管されている  
HighのユーザーがLowのWebサイトを表示できる「ブラウジング」システムなど、恐ろしい回避策が時々あります。ボタンやリンクをクリックしてナビゲートでき、テキストを入力することはできません。  
  
必須のアクセス制御は当初、軍事用に開発されましたが、特殊なファイアウォール（ガードおよびデータダイオード）でも使用されています。  
ただし、最近のMACメカニズムの主な用途は、Android、iOS、Windowsなどのプラットフォームであり、オペレーティングシステム自体をマルウェアから保護しています。  
プラクティショナーが長所と短所の両方を理解することが重要です。それにより、適切な場合に研究資料を利用し、適切でない場合に過剰設計に引き込まれないようにすることができます。  
すべてのセキュリティ問題をヘッジホッグ問題としてキャストしようとすることにより、MLSはしばしば不適切なセキュリティ目標、ポリシー、およびメカニズムにつながります。  
。  
モノのインターネットで広く使用されていると思いますか？  
 NSAは、これまでよりも低いレベルではありますが、現在IFCの名称でMLSの研究に資金を提供しています。  
現代のオペレーティングシステムの本質的な複雑さに加えて、携帯電話には大量のサイドチャネルがあり、そのアプリは多くの場合、実際の大きな作業を行わなければならないクラウドサービスとの通信にのみ役立ちます。  
別の一連の研究課題が実際の軍事作戦を取り巻いており、現実は政策にはるかに及ばない。  
英国海軍は2009年に電話を禁止しようとしましたが、あまりにも多くの船員が去りました。  
規律は、船員が地雷の処分を急いで見られるときなど、緊急の運用上の脅威に焦点を合わせる傾向があります。問題は、地雷の近くで無線機を使用するリスクです。さまざまな海軍がさまざまなことを試みてきました。ノルウェー人は船員のための独自の特別なネットワークを持っており、米国はMLS機能を備えた電話を試みています。  
そしてイスラエル人でさえ、兵士たちがヨルダン川西岸とゴラン高原で携帯電話を使うことに問題を抱えています。  
 2018年11月に政府セキュリティのWebページ[802]でリリースされました。そして、公共部門での廃棄物、詐欺、管理ミスを隠すための分類プロセスの乱用に関する古典は、チャップマンによるものです[407]。  
NSAサプライヤーコミュニティの未分類のbashは、コンピューターセキュリティアプリケーション会議（ACSAC）です。  
 IEEEが発行。  
この分野の古典的な初期の論文の多くは、NISTアーカイブ[1395]にあります。 NISTは、1999年までマルチレベルセキュリティに関する会議シリーズを開催しました。