NIST Special Publication 800-33

IT セキュリティのための基本テクニカルモデル

米国立標準技術研究所による勧告

Gary Stoneburner

コンピュータセキュリティ

コンピュータセキュリティ部門
情報技術研究所
米国立標準技術研究所
Gaithersburg, MD 20899-8930

2001 年 12 月

米国商務省 長官

Donald L. Evans

技術管理局 技術担当商務次官

Phillip J. Bond

米国立標準技術研究所 所長

Arden L. Bement, Jr.

この文書は下記団体によって翻訳監修されています

独立行政法人 情報処理推進機構
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

NRI SECURE TECHNOLOGIES

本レポートは、原典に沿ってできるだけ忠実に翻訳するよう努めていますが、完全性、正確性を保証するものではありません。翻訳監修主体は本レポートに記載されている情報より生じる損失または損害に対して、いかなる人物あるいは団体にも責任を負うものではありません。

コンピュータシステム技術に関するレポート

米国立標準技術研究所（NIST; National Institute of Standards and Technology）のITL（Information Technology Laboratory）は、国家の評価基準および標準化インフラストラクチャの技術的なリーダーシップを提供し、米国の経済および公共福祉に貢献している。ITLは、テスト、テスト技法、参照データの開発、概念インプリメント、技術的分析の検証を行い、情報技術の開発と生産的な利用の発展に努めている。ITLの責務は、技術的、物理的、および管理上の標準とガイドラインを開発し、連邦政府のコンピュータシステム内の、センシティブな非機密扱い情報のセキュリティとプライバシーをコスト効率の高い方法で確保することである。NIST Special Publication 800シリーズでは、コンピュータセキュリティにおけるITLの調査、ガイダンス、成果を報告し、産業界、政府機関および教育機関との共同活動についても報告する。

このドキュメントでは、実験的な手順および概念を的確に記述するために、特定の商用事業体、機器、または資材に触れることがある。特定された商業事業体、装置および資料名は、米国立標準技術研究所による推奨または支持を意味するものではなく、またその事業体、資料、装置が目的に最適であることを示すものでもない。

NIST Special Publication 800-33
NIST Special Publication 800-33 27 ページ（2001 年 12 月、英文 ）
CODEN: NSPUE2

米国政府印刷局
ワシントン: 2001 年

政府刊行物管理局、米国政府印刷局より販売
インターネット: bookstore.gpo.gov — 電話: (202) 512-1800 — Fax: (202) 512-2250
郵送: Stop SSOP, Washington, DC 20402-0001

目次

図

1.0 はじめに

作成機関

このドキュメントは、米国立標準技術研究所（NIST; National Institute of Standards and Technology）が、1987年のコンピュータセキュリティ法（Computer Security Act）および1996年の情報技術管理改革法（Information Technology Management Reform Act）、合衆国法律集第15編第278条g-3(a)(5)項に基づくその法的責任を推し進めるために作成したものである。

本書は、合衆国法律集第15編第278条g-3(a)(3)項の範囲内でのガイドラインではない。

このドキュメントは、センシティブ情報[1]を扱う連邦政府組織が使用するために推奨されるものであり、OMB Circular A-130、付録IIIの要件に準拠している。

ここでの推奨事項は強制力または拘束力を持つ標準ではない。このドキュメントは、非政府機関が自発的に使用でき、著作権の制約はない。

このドキュメントにおける一切は、商務長官が法的権威に基づき連邦機関に対して義務および拘束力を与えた標準およびガイドラインを否定するものではない。また、これらの推奨は、商務長官、行政管理予算局長、または他のすべての連邦政府当局者の既存の文書を改ざんしたり、これらに取って代わるものと解釈してはならない。

目的

このドキュメントの目的は、安全な情報技術（IT）の基盤となる、「モデル」と呼ばれる技術的な基礎を説明することである。

技術的なセキュリティ機能の設計と開発において考慮する必要のあるモデルを、簡潔に示すことを意図している。これらのモデルには、教訓、グッド・プラクティス、特定の技術的検討事項が含まれている。

対象とする読者

以下のような、政府機関および民間部門の読者を想定している。

- システムセキュリティの理解を高めたいITユーザー
- セキュリティ機能を設計および構築するエンジニア、設計者
- セキュリティ機能のインプリメントに使用する、ガイダンスの開発担当者

[1] コンピュータセキュリティ法では、「センシティブ情報」を次のように定義している。
損失、悪用、不正アクセス、改ざんによって、国益または連邦政府のプログラムの遂行を阻害し、または、合衆国法律集第5編第552a項（プライバシー法）に基づいて確保されるプライバシーが侵害される恐れがあるが、大統領令または連邦議会制定法によって制定される規準下では、国家防衛または外交政策のためには非公開にすることが特定的には認められていない、いかなる情報。

2.0 セキュリティの最終目標と達成目標

セキュリティの最終目標

情報技術におけるセキュリティの最終目標は、以下のとおりである。

> 組織、パートナー、顧客に対する IT 関連リスクの懸念を十分に考慮したシステムをインプリメントすることで、組織がそのミッション/ビジネス上の目標をすべて達成できるようにする。

セキュリティの達成目標

セキュリティの最終目標は、以下のセキュリティの達成目標を実現することで達成できる。

1. Availability：可用性（システムとデータを目的とする用途でのみ使用する場合）

> 可用性とは、システムが適切に稼働し、許可されたユーザーに対してサービスが拒否されないことを保証するための必須条件である。この目標によって、以下の状況から保護される。
>
> ・ 下記のような、意図的または偶発的な現象
> - データの不正な削除、または
> - サービスまたはデータの利用拒絶
>
> ・ 許可されていない目的で、システムまたはデータが使用されること
>
> 可用性は、組織におけるセキュリティ上の最重要目標とされることが多い。

2. Integrity：完全性（システムおよびデータ）

> 完全性には、2 つの側面がある。
>
> ・ データ完全性
> データ保管中、処理中、または転送中に、データが不正な手段で改ざんされていないというプロパティ
>
> ・ システム完全性
> 意図した機能を、不正操作がない状態のもと、損害を与えない方法で実行した場合にシステムが保つ品質
>
> 完全性は一般に、可用性の次に組織にとって最も重要なセキュリティの達成目標である。

3. Confidentiality：機密性（データおよびシステム情報）

> 機密性は、承認されていない個人に個人情報または機密情報が開示されないことを要求する。機密性保護は、ストレージ内、または処理中、転送中のデータに適用される。
>
> 多くの組織では、機密性は可用性および完全性よりも重要度が低いとされることがある。しかし、特定のシステム、またはほとんどのシステム内にある特定のデータタイプ（認証子など）について、機密性は極めて重要である。

4. Accountability：アカウンタビリティ（個人レベルまで特定）

アカウンタビリティは、あるエンティティのアクションが、そのエンティティまで追跡できることを要求する。

アカウンタビリティは、ほとんど例外なく組織のポリシーとして必須であり、否認防止、抑止、欠陥特定、侵入検知と防御、事後の回復と法的措置を直接サポートする。

5. Assurance：保証（他の 4 つの目標が十分に達成されること）

保証は、技術的および運用上の両方のセキュリティ対策が、意図したとおりに機能してシステムおよびその処理情報が確実に保護されるための基礎である。その他の 4 つの目標（完全性、可用性、機密性、アカウンタビリティ）は、以下の事項が実現される場合に、適切に満たされていることになる。

・ 要求される機能が存在し、正しくインプリメントされている。
・ 予期しないエラー（ユーザーまたはソフトウェアによる）に対する十分な保護機能がある。
・ 意図的な侵入またはバイパスに対する十分な対策を施している。

保証は不可欠であり、これを抜きにしては他の目標を達成できない。しかし、段階的措置が取られるべきものであり、必要な保証のレベルはシステムによって異なる。

セキュリティ目標の相互依存性

5つのセキュリティ目標は、互いに依存関係にある。その他の目標を考慮せずに、1つの目標のみ達成することはほぼ不可能である。図 2-1 は依存性を示すもので、以下で詳説する。

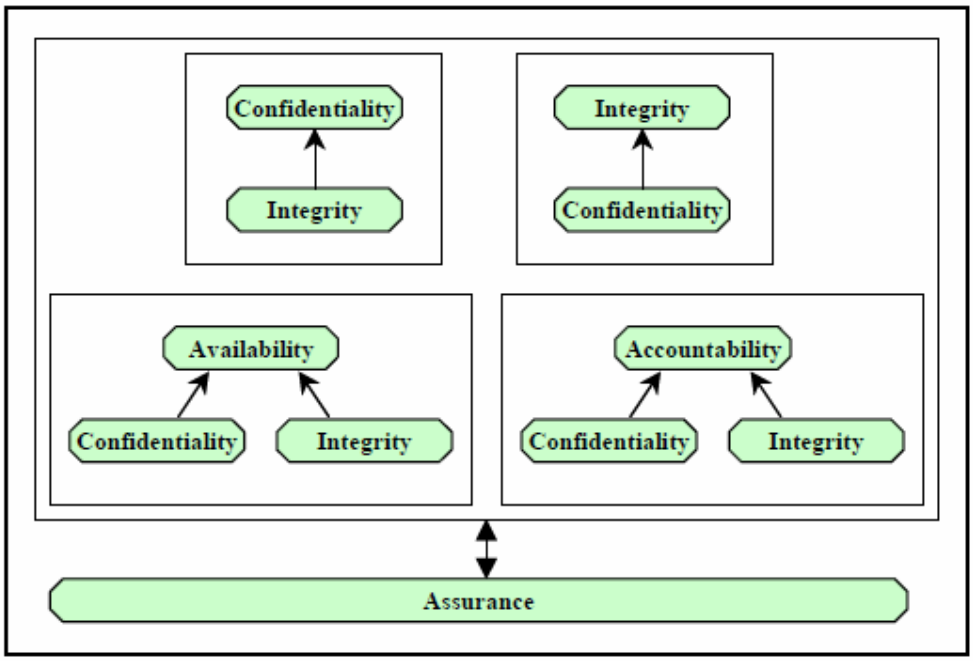

図 2-1 セキュリティ目標の依存関係

図 2-1 は、以下の依存関係を示している。

機密性は完全性に依存し、システムの完全性が失われると、機密性メカニズムがその後も有効であるという合理的な推測が成り立たなくなる。

完全性は機密性に依存し、ある情報の機密性（スーパーユーザーのパスワードなど）が失われると、完全性メカニズムがバイパスされることがある。

可用性とアカウンタビリティは、以下の点で、機密性と完全性に依存する。

- ある情報の機密性（スーパーユーザーのパスワードなど）が失われると、これらの目標を実現するメカニズムのバイパスが容易になる。
- システムの完全性が失われると、これらの目標を実現するメカニズムの有効性に対する確信も失われる。

これらの目標すべては、保証と相互に依存する。システム設計時に、設計者またはエンジニアは、保証レベルをターゲットとして設定する。このターゲットは、その他の 4 つの目標それぞれに必要な機能を定義し且つ満たすことによって達成されるものである。また、それによってふさわしい「品質」がもたらされる。保証は、システムが安全であるためには意図された機能を提供するだけでなく、望ましくないアクションが発生していないことを確保する点にも焦点を当てる。

3.0 セキュリティサービスモデル

基盤となる技術的なセキュリティサービスのモデルを、図 3-1 に示す。この図では、情報技術のセキュリティ機能のインプリメントに使用される主要なサービスおよびサポート要素と、それらの主要な関係を示している。本モデルでは、主要目的別にサービスを次のように分類している。

- サポート（Support）
  このサービスは一般的で、大部分の情報技術セキュリティ機能の基礎となる。
- 防止（Prevent）
  このサービスは、セキュリティ侵害の発生防止を重視する。
- 回復（Recover）
  このカテゴリに該当するサービスは、セキュリティ侵害の検出と回復を重視する。

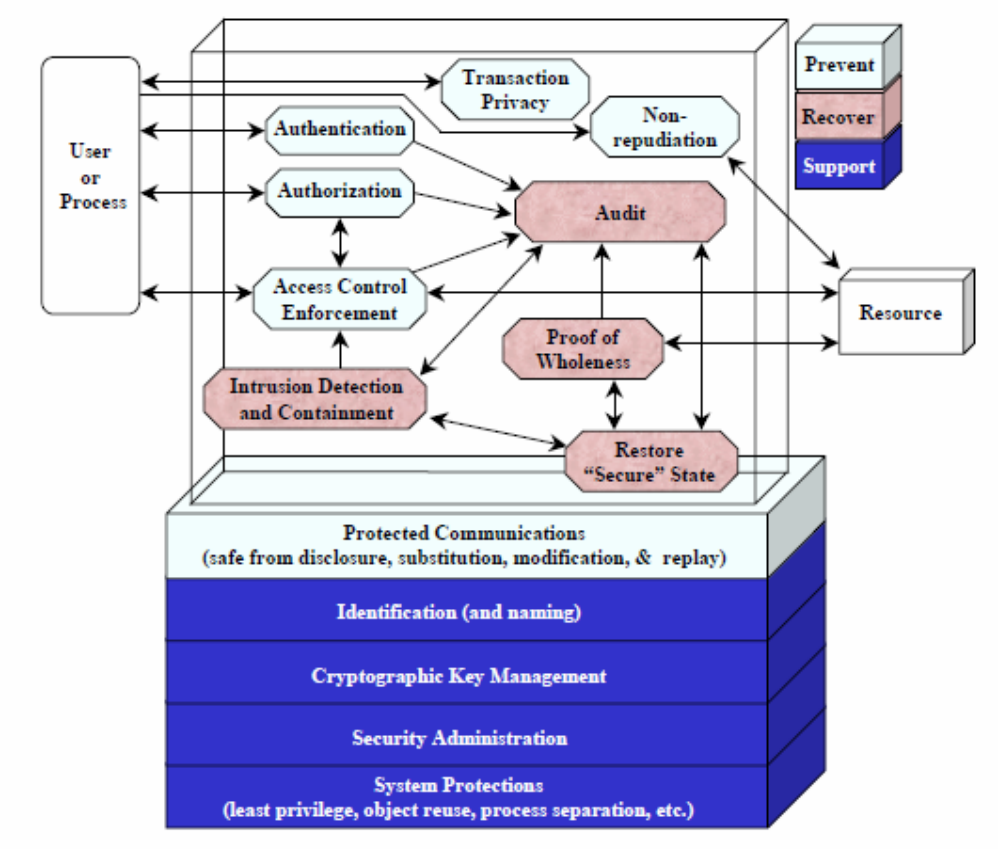

図 3-1 セキュリティサービスモデル

本項のロードマップ ： この項では、以下について説明する。

- 本モデル内の各サービスの定義
- 本モデルを 5 つのセキュリティ目標に分解した上での、各目標を実現するための主要なサービス

3.1 サービスの定義

サポート:

サポートサービスは、本質的に、普遍的で他の多くのサービスと相互関係がある。サポートサービスには、次のものがある。

- 識別（および名前付け）
  他の多くのサービスをインプリメントするためには、サブジェクトとオブジェクトの両方が識別可能であることが重要である。このサービスは、ユーザー、プロセス、情報リソースを特定する機能を提供する。
- 暗号鍵管理
  暗号化機能が様々なサービスでインプリメントされている場合、暗号鍵は安全に管理される必要がある。
- セキュリティアドミニストレーション
  特定のインストールニーズを満たし、運用環境での変更に対応するためには、システムのセキュリティ機能を管理する必要がある。
- システム保護
  様々なセキュリティ機能を有効にするには、確実な技術のインプリメントが前提となる。これは、使用された設計プロセスとインプリメント手法の両面から見た、インプリメントの品質を表している。システム保護の例として、残余情報の保護（オブジェクト再利用ともいう）、最小特権、プロセス分離、モジュール化、階層化、信頼を得るために必要とされるものの最小化が挙げられる。

防止:

以下のサービスは、セキュリティ侵害の発生を防止する。

- 保護された通信
  分散システムでは、セキュリティ目標を達成する能力が、信頼できる通信に大きく依存する。保護された通信サービスでは、転送中の情報に対する完全性、可用性、機密性が確保される。多くの状況では、3 つの要素すべてが必須の要件で、機密性は少なくとも認証情報にとって必要である。
- 認証
  申請されたアイデンティティの正当性を保証することは、非常に重要である。認証サービスは、サブジェクトのアイデンティティを検証する手段を提供する。
- 承認
  承認サービスによって、所定のシステムに対して許可されたアクションの指定と、その管理が可能になる。
- アクセスコントロール･エンフォースメント
  アクセスを要求するサブジェクトが特定のプロセスへのアクセスを正当と認めた場合にも、定義されたセキュリティポリシーをエンフォースすることが必要である。アクセスコントロール･エンフォースメントサービスによって、このエンフォースメントが提供され、しばしばこのエンフォースメント･メカニズムはシステム全体に適用される。アクセスコントロールの精度のほか、アクセスコントロール･エンフォースメントの強度によっても、得られるセキュリティのレベルは異なる。アイデンティティと要求されたアクセスを、アクセスコントロールリストに照合させることが、アクセスコントロール･エンフォースメントメカニズムの基本である。ファイル暗号化は、アクセスコントロール･エンフォースメントメカニズムのもう 1 つの例である。
- 否認防止
  システムアカウンタビリティは、送信者が情報の送信を拒否できないようにする、または受信者が情報の受信を拒否できないようにする機能に依存する。否認防止は、防止と検知に関わる

サービスである。インプリメントされるメカニズムはアクションの否認を防止するものであるため、このサービスは防止カテゴリに分類されてきた。結果として、このサービスは通常、送信または受信の時点で実行される。

・ トランザクションプライバシー
政府機関と民間の両方のシステムにおいて、システムを使用する個人のプライバシーを保護する必要性が高まってきている。トランザクションプライバシーサービスは、個人が実行したトランザクションについてプライバシーが侵害されないように保護する。

検知と回復:

完璧な防止対策は存在しないため、セキュリティ侵害を検知して、その影響を抑制するための措置をとる必要がある。

・ 監査
セキュリティ関連イベントの監査は、セキュリティ侵害の事後検知およびセキュリティ侵害からの回復において主要な要素である。

・ 侵入検知および封じ込め
安全ではない状況を検知することは、タイムリーに対応するために不可欠である。また、セキュリティ侵害の検知は、効果的な対応措置がインプリメントされなければ役に立たない。侵入検知と封じ込めサービスは、この 2 つの機能を提供する。

・ 網羅性の検証
完全性が侵されていないことを判定するには、情報またはシステムの状態に欠陥がある可能性があることを検知できる機能が必要である。網羅性の検証サービスでは、この機能が得られる。

・ 「安全」な状態の復元
セキュリティ侵害が発生した場合、システムは安全な状態に戻ることができなければならない。これが、このサービスの目的である。

3.2 セキュリティ目標の達成

下に挙げる図では、次のセキュリティ目標を達成するために重要なサービスを示す。

図 3.2-1 – 可用性

図 3.2-2 – 完全性

図 3.2-3 – 機密性

図 3.2-4 – アカウンタビリティ

図 3.2-5 – 保証

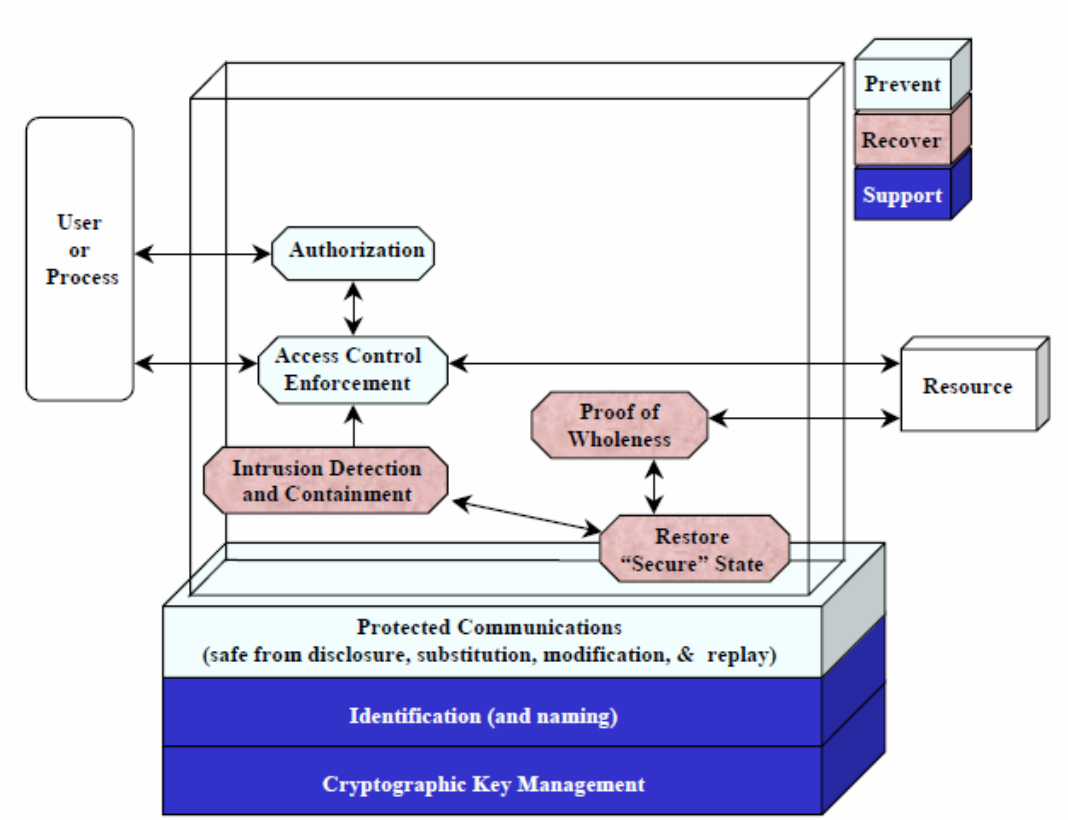

図 3.2-1 主要な可用性サービス

主要な可用性サービスは、オペレーション面の有効性を維持するシステム機能に直接影響を与えるものである。有効性を維持する 1 つの局面として、承認されたアクセスを定義し、この定義をエンフォースすることによって、不正な変更または削除から保護することが挙げられる。ミッションの有効性もまた、侵入を検知し、網羅性の欠如を検知し、安全な状態へ戻る手段を提供することによって維持される。

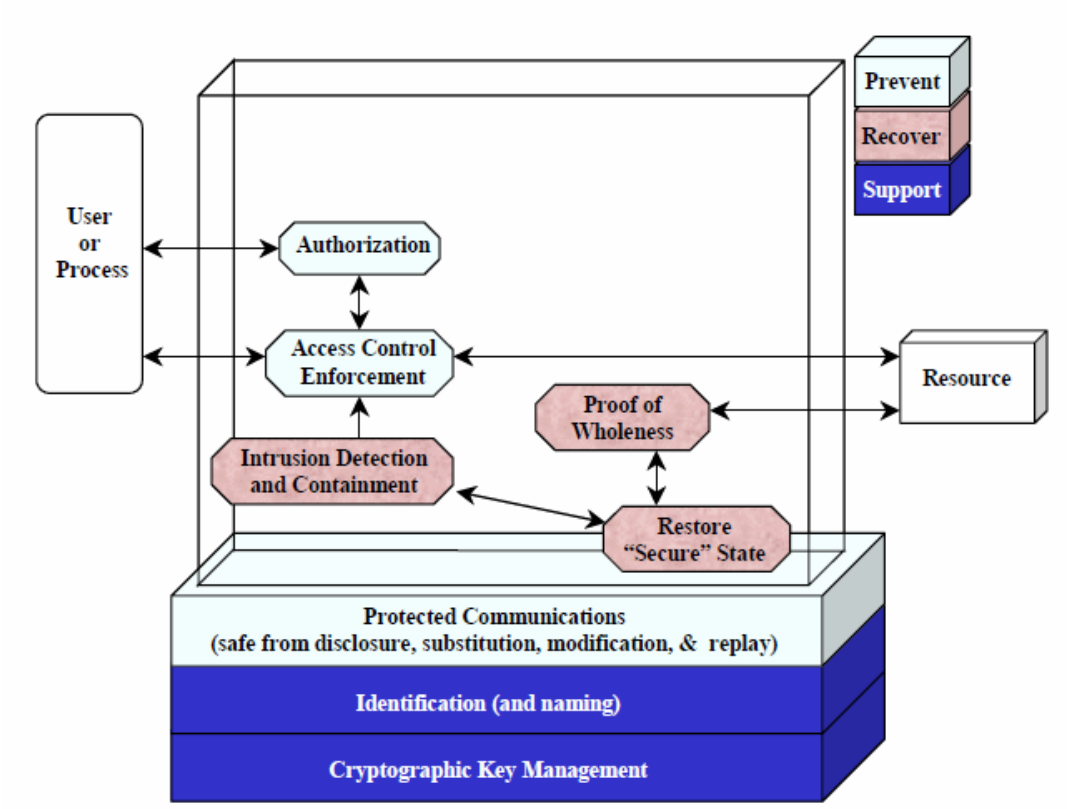

図 3.2-2 主要な完全性サービス

可用性を提供するサービスは、完全性も提供する。その理由は、完全性の維持または復元が、可用性の維持には必須だからである。可用性は、ミッションに影響する変更（または削除）に関連するが、実際には、承認されないアクセスがあったり、網羅性が欠如しているからといって、適用されるセキュリティメカニズムが異なることはない。

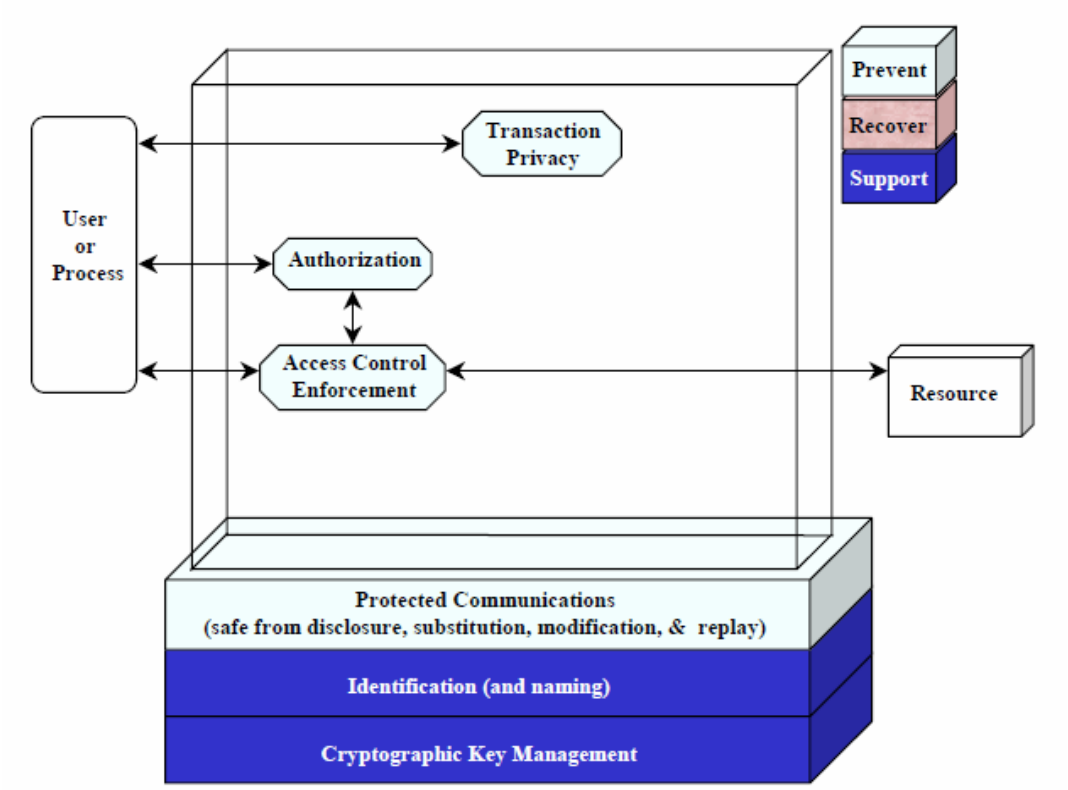

図 3.2-3 主要な機密性サービス

機密性は、一度失われると回復することはできない。そのため、可用性および完全性を維持する上で重要な役割を果たす検知および回復サービスは、機密性には適用されない。通信の開示防止、承認された読み取りアクセスの適用、プライバシー保護機能によって、機密性が保たれる。

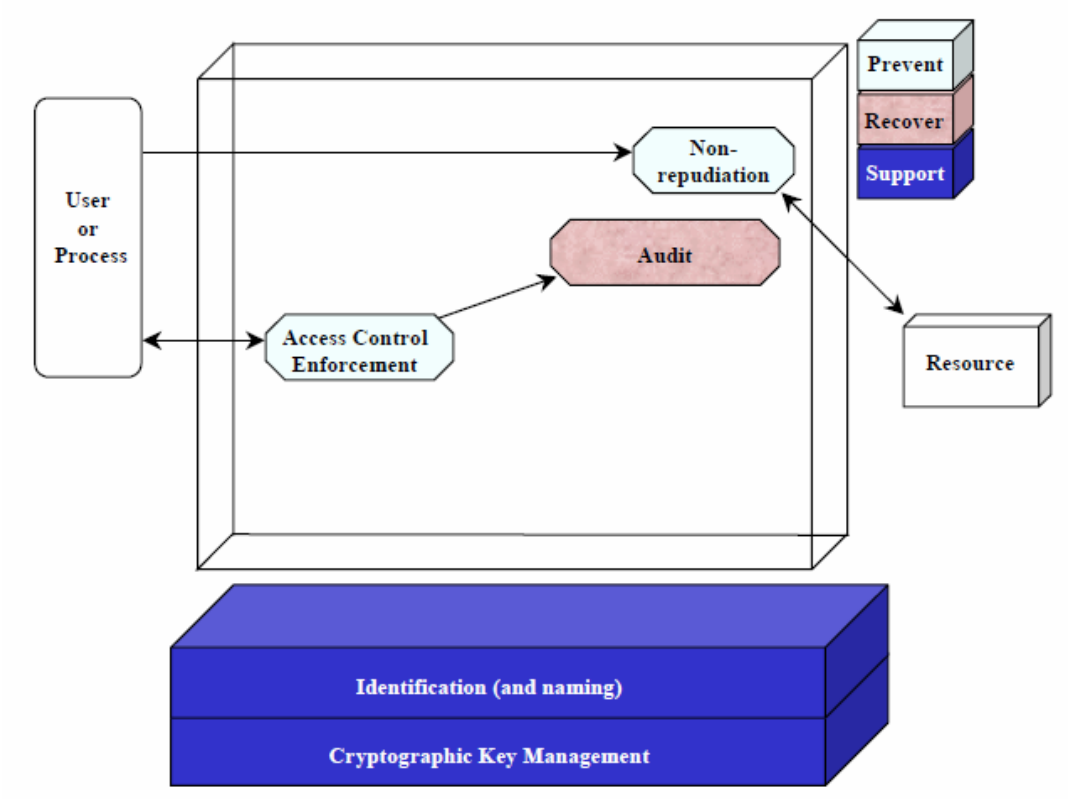

図 3.2-4 主要なアカウンタビリティサービス

ユーザーアクションに対するアカウンタビリティの維持は、主に監査と否認防止サービスによって実行される。アクセスコントロール・エンフォースメントも、ユーザーアクションの記録生成元として含まれる。

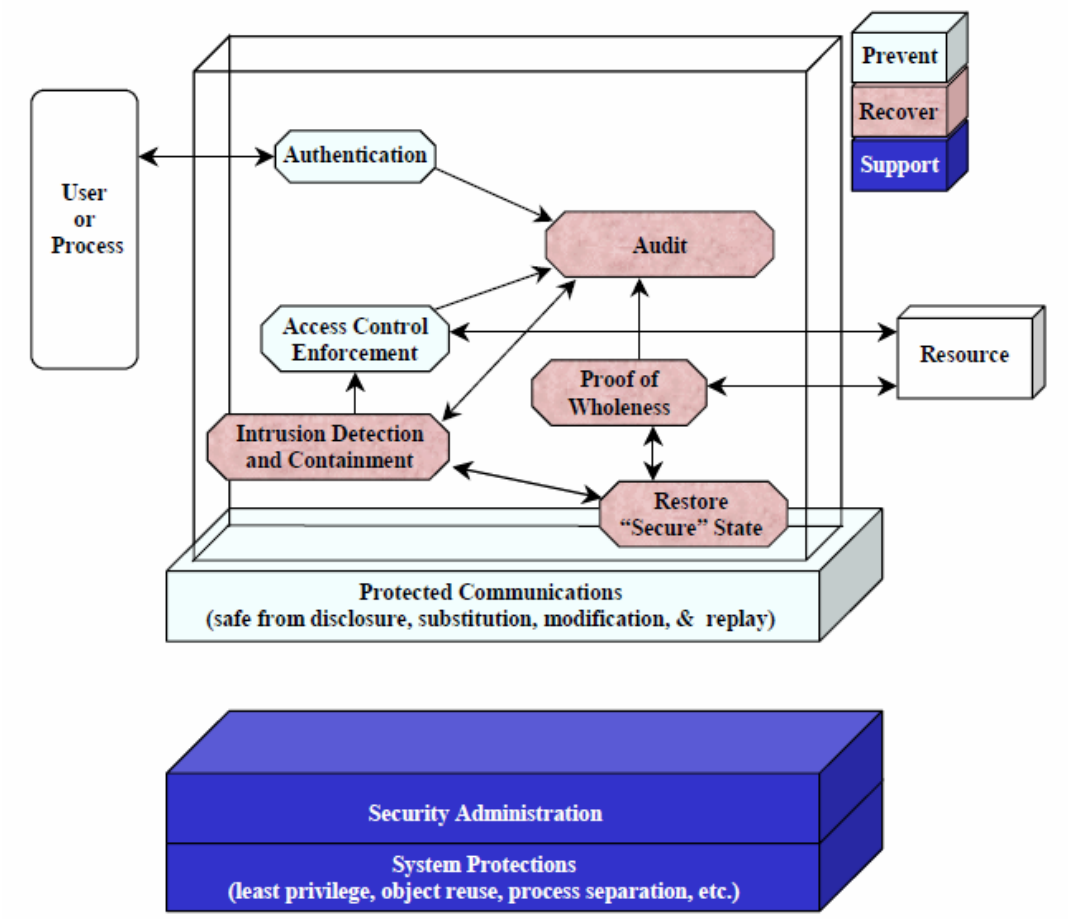

図 3.2-5 主要な保証サービス

保証は、第 2.0 項で述べたように、セキュリティ目標が達成されていることを確保するものであり、正確で且つ十分なセキュリティ機能を包括するものである。これには、「何」が「どのように」提供されるのか（アーキテクチャ、設計、インプリメント）を考慮することが要求される。また、第 4.1 項で後述するように、保証は論理的および物理的にシステム全体に影響する。明らかに、保証は普遍的で、複数の観点から検討され得るものである。特定のセキュリティサービスの観点からは、保証は、正確で継続的なシステムのセキュリティ機能に直接影響を与えるサービスによって、大きく異なる。このことから、実行される認証の性質とアクセスコントロール・エンフォースメント機能の強化が極めて重要となる。さらに、効果的な回復機能が存在することによって、信頼性が確保される。監査サービスは、その弱点を認識した上で効果的に使用すれば、保証の達成において非常に有益である。最後に、システムのセキュリティ機能を確保するための客観的な基礎を構築する上で、適切なセキュリティアドミニストレーションとシステム保護が必須である。

4.0 セキュリティ目標のインプリメント – 分散システム

この項では、分散システムに関する以下の側面について述べる。

・ 物理的および論理的に分散したセキュリティサービス
・ セキュリティドメイン
・ ネットワークビュー

4.1 分散セキュリティサービス

図4-1は、分散セキュリティサービスと、ネットワーク全体の物理的、論理的分散によるサービス間の依存関係を示す。さらに、同図は、すべてのサービスは最終的にはオペレーティングシステムメカニズムに依存し、システム保証が機能全体を取り囲む重要な要素であること、さらに、システム管理もまた効果的なセキュリティ機能の重要な側面であることを示す。

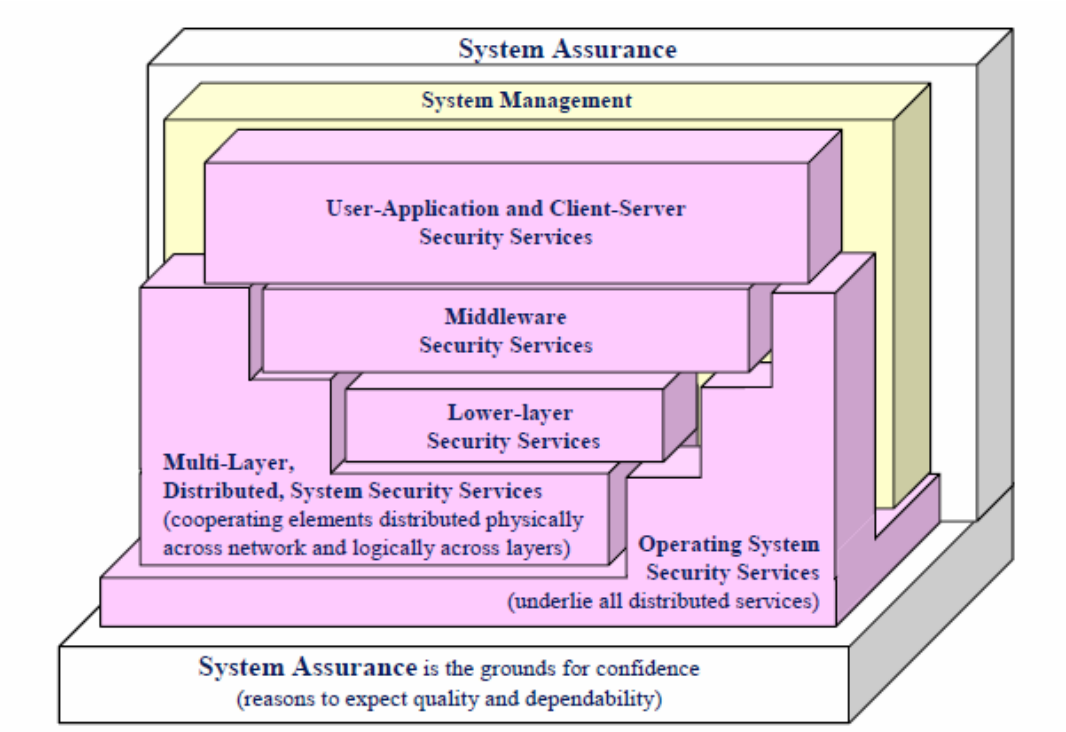

図 4.1-1 分散セキュリティサービス

分散セキュリティサービスは、システム保証とオペレーティングシステムセキュリティサービスを基礎とする。

a. システム保証

保証とは、エンティティがセキュリティ目標を満たしているという信頼性の根拠となるものである。[1] 保証はまた、システムが意図された目標を満たしているという信頼性につながるシステム特性とも言える。安全なシステムのインプリメントには、セキュリティメカニズムの正確なオペレーションや、故意または偶発的なシステムへの侵入を許さないようにするレベルの品質が要求される。情報システムの保証を提供し且つ測定する技術が開発されている。システム保証は、以下のような手段で強化することができる。

- 技術的に複雑ではないソリューションを適用する
- より信頼性の高いコンポーネントを利用する
- 脆弱性範囲の制限および検知/回復機能のインプリメントにより、侵入被害を抑制するアーキテクチャを採用する
- オペレーション環境の点から技術を統合する
- 非技術的な対応策を利用する

図 4.1-1 に示すように、システム保証はアーキテクチャをサポートするとともに、アーキテクチャ全体に影響する。

b. オペレーティングシステムセキュリティサービス

このようなサービスにおけるシステムセキュリティは、最終的にはオペレーティングシステムサービスと s そのメカニズムに依存する。こうした基盤のサポートが弱ければ、セキュリティがバイパスされたり破壊されたりする。システムセキュリティが、基盤のオペレーティングシステムより強力になることはない。図では、この重要な概念を明確にするために OS の個々のセキュリティ階層を示している。

一部のサービスはシステム階層の特定の論理レベルに存在するが、サービスの多くは、物理的にも論理的にシステムにもまたがるメカニズムによってインプリメントされている。これは、図 4.1-1 のアプリケーション/クライアントサーバー、ミドルウェア、下位層に示される。各層は、下位層の機能に依存し、図示されているようにオペレーティングシステムメカニズムに直接的に依存する。

さらに、分散サービスのなかには、1 つのレベルではなく、複数のレベルにまたがるメカニズムによってインプリメントされるものもあることが示されている。分散サービスの一般的な例として、識別および認証（I&A）がある。通常アプリケーションレベルのソフトウェアの一部であるユーザーインターフェース（Telnet クライアントなど）は、ユーザーとやりとりして必要な情報を得る必要がある。この情報はデータが正しいかどうか判定されるプロセスに渡される必要がある。このプロセスは、通常はオペレーティングシステムレベルで実行される。または、国際標準化機構（ISO）の OSI モデル[3,4]のプレゼンテーション、セッション、ネットワークレベルで実行されることもある。あるマシンで収集された情報が、ネットワークを介して他のマシン（ネットワーク認証サーバーなど）に転送されることは珍しいことではない。このネットワーク認証サーバーを使用した I&A の例では、セキュリティサービスは物理的に最低 2 台のマシンに分散し、OSI の 7 つの階層すべてのメカニズムが連携して機能することが要求される。

4.2 セキュリティドメイン

IT セキュリティの基礎は、セキュリティドメインと、このドメイン間あるいはドメイン内でのデータおよびプロセスフローの制限のエンフォースメントに関わる概念である。

ドメインは、アクティブなエンティティ（人、プロセス、デバイス）、そのデータオブジェクト、共通のセキュリティポリシーの集合である。

ドメインは論理的にも物理的にも捉えることができる。組織のコンピューティング環境をドメインに分割する作業は、フェンス（各種のセキュリティバリア）を建て、フェンスの内側に門を設置（ファイアウォール、ゲートウェイ、内部プロセス分離）し、門の通行に警備員を配置（技術的または手続き的なセキュリティサービス）するのに似ている。

ドメインは、以下の要因のいくつかを組み合わせて定義される。

- 物理的（建物、キャンパス、地域など）
- ビジネスプロセス（人事、財務など）
- セキュリティメカニズム（Microsoft NT ドメイン、Sun Network Information System (NIS)など）

ドメインを定義する上で取り上げる必要のある主な要素として、柔軟性、カスタマイズされた保護、ドメイン相互関係、情報技術セキュリティにおいて何が重要かを決定するための複数の観点の使用が挙げられる。

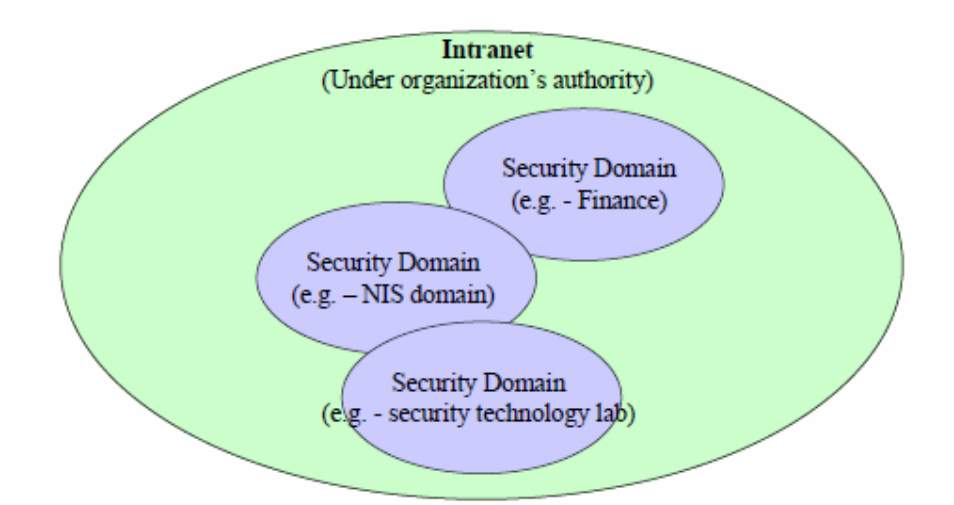

図 4.2-1 セキュリティドメインのオーバーラップ

4.3 ネットワークビュー

分散イントラネット

組織のイントラネットは通常、物理的に分散され、相互接続されているが、その接続が組織によって管理されていないことがある。図 4.3-1 にその状況を示す。

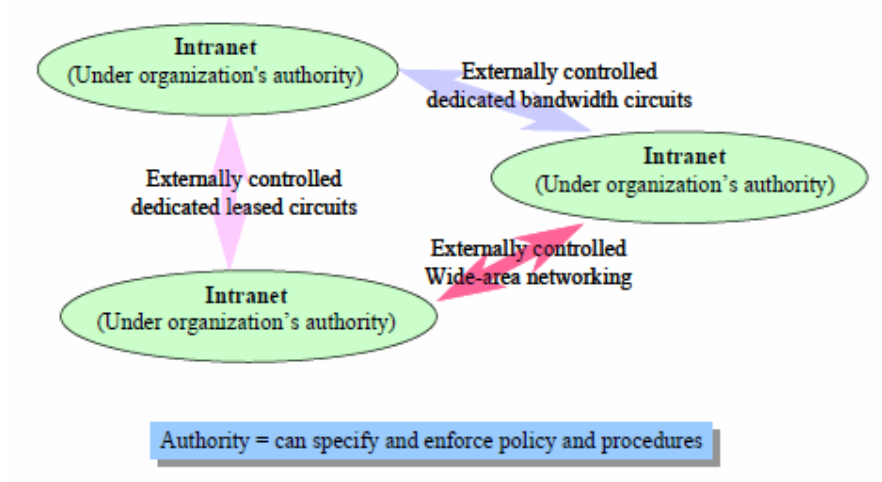

図 4.3-1 分散イントラネット

イントラネットのコンパートメント化

組織内には、船内に防水ドアを設置するように、組織はイントラネットのコンパートメント化を考慮する必要がある。これによって、組織のポリシーを徹底させ、セキュリティ侵害が発生しても損害を限定的にすることができる。図 4.3-2 にこの概念を示す。

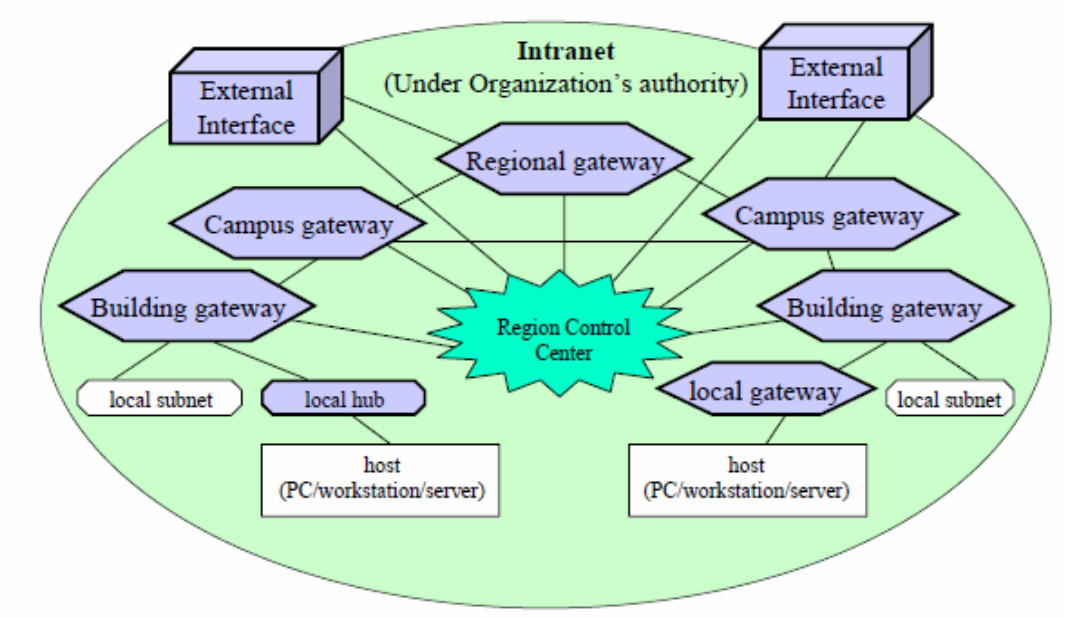

図 4.3-2 コンパートメント化されたイントラネット

「内部」対「外部」

「外部」を断定することは、容易ではない。実際の「外部」からのトランザクションと内部のトランザクションとを区別することは可能である。図 4.3-3 に示すように、エンドツーエンドの暗号化パスを使用すると、こうしたソリューションが可能になる。

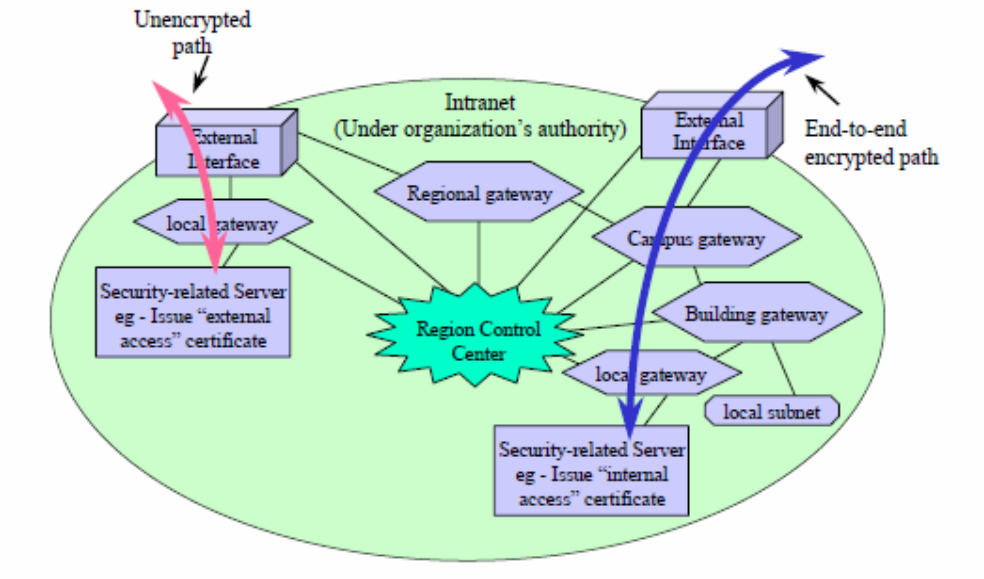

図 4.3-3 「外部」トランザクション

検知と抑制

セキュリティ侵害を検知してそれに対処する機能は、効果的な情報技術セキュリティ機能にとって不可欠である。図 4.3-4 に示すように、検知、分析、応答コンポーネントを組織のイントラネットに統合することで達成できる。

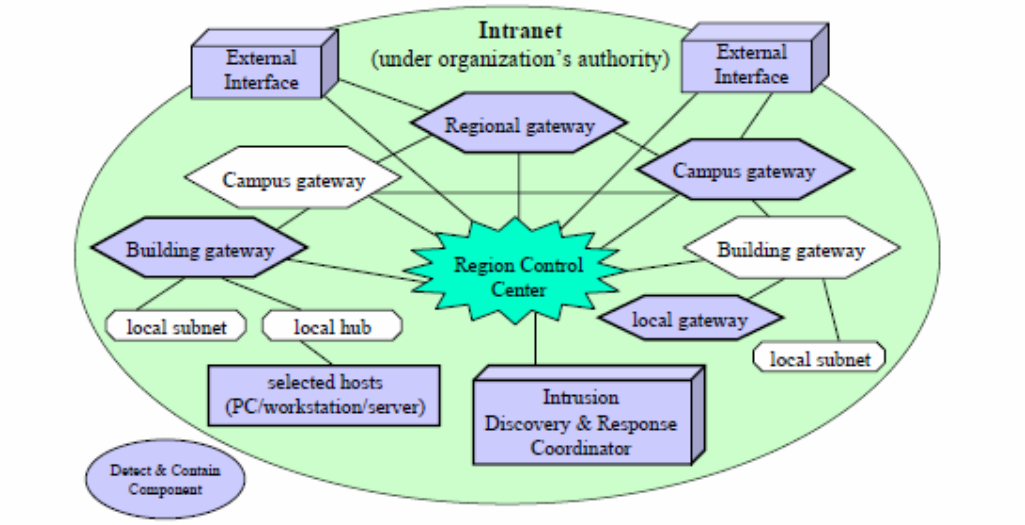

図 4.3-4 検知と抑制

5.0 リスクマネジメント

この項では、リスクを低減するためにどこで技術を適用するかを明らかにする目的で、リスクマネジメントの概要を説明する。用語集に挙げるように、以下の定義を使用する。

脆弱性	偶発的に発生または意図的に悪用される可能性があり、システムのセキュリティポリシー違反につながる可能性のある、システムセキュリティ手順、設計、インプリメント、内部統制などにおける弱点。
脅威のソース	(1) 脆弱性の意図的な利用を目的とする意図または手法、または (2) 偶発的に脆弱性を引き起こす恐れのある状況および手法。
脅威	特定の脆弱性を悪用したり (意図的)、引き起こしたり (偶発的) する「脅威のソース」の潜在的存在。
リスク	特定の脅威のソースが特定の情報技術の脆弱性を悪用または引き起こすことによる、ネットミッション/ビジネスへの影響 (影響と結びついて発生する可能性)。IT関連のリスクは、以下を起因とする、法的責任またはミッション/ビジネス上の損失から発生する。 ・ 情報の承認されていない (悪意のある、悪意のない、偶発的な) 開示、修正、破壊 ・ 悪意のないエラーと欠陥 ・ 自然災害および人災によるITの破壊 ・ ITインプリメントと運用における不注意と怠慢

図5-1は、意図的な「攻撃」に直面した際のリスク低減の達成方法を示す。「攻撃」と強調するのは、意図的であって、悪意がないことを示すためである。セキュリティに関しては、「ただ仕事をするだけ」というように、悪意のない目的で意図的に「攻撃」することが、比較的一般的である。

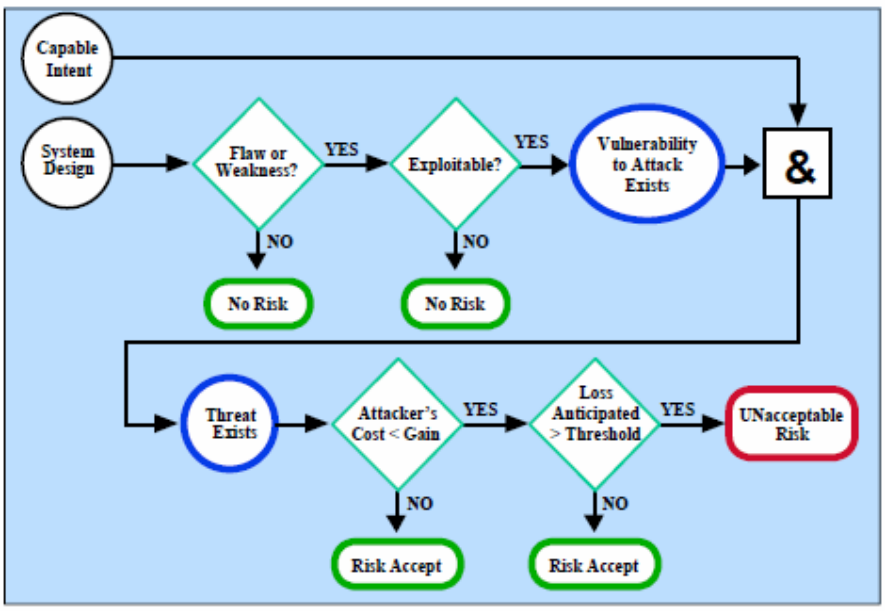

図 5-1 リスク低減の基礎 - 「攻撃」

技術的手段による攻撃からのリスク低減は、以下の点で達成できる。

- 欠陥がある。
  対処法: 保証テクニックをインプリメントして、欠陥を低減させる。
- 欠陥が悪用される可能性がある。
  対処法: 多層保護とアーキテクチャ設計を適用し、悪用できないようにする。
- 攻撃者のコストが利益より小さい。
  対処法: 保護を適用して、攻撃者のコストを増大させる（処理対象を制限するなどの非技術的な方法で、攻撃者の利益を大幅に削減できる）。
- 損失が大きすぎる。
  対処法: 設計原則、アーキテクチャ設計、技術的な保護を適用して、攻撃の範囲を限定することで損失を縮小する。（ここでも、プロセス対象を制限するなどの非技術的な方法がリスク低減に効果的である。）

図 5-2 は、システムエラーまたはセキュリティポリシー違反を意図しないユーザーアクションを起因としたリスクを低減する方法を示す。以下の状況では、リスク低減の方法は非常に類似している。

- 欠陥がある。
  対処法: 保証テクニックをインプリメントして、欠陥を低減させる。
- 欠陥が搾取される可能性がある。
  対処法: 多層保護とアーキテクチャ設計を適用し、悪用できないようにする。
- セキュリティ違反が明示的な決定によるものではないので、攻撃者のコストは考慮しない。
- 損失が大きすぎる。
  対処法: 設計原則、アーキテクチャ設計、技術的な保護を適用して、セキュリティ違反の範囲を限定することで損失を縮小する。

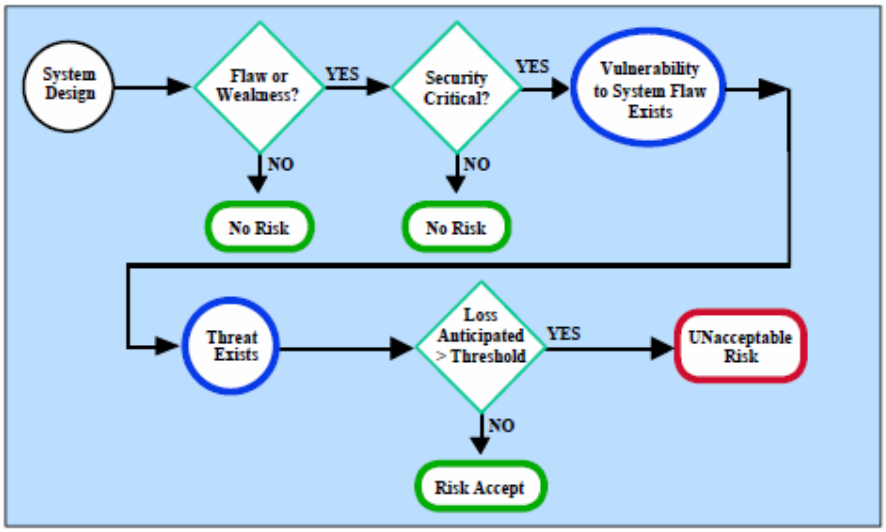

図 5-2 リスク低減の基礎 – エラー/ミス

6.0 定義

用語	定義
アクセスコントロール	リソースの承認された利用を可能にし、承認されていない使用、または承認されていない手段での使用を防止する。
アカウンタビリティ	あるエンティティのアクションが、そのエンティティにまで追跡できることを要求するセキュリティ目標。これによって、否認防止、抑止、欠陥特定、侵入検知および防御、事後回復および法的措置がサポートされる。
保証	その他の 4 つの目標（完全性、可用性、機密性、アカウンタビリティ）が特定のインプリメントによって適切に満たされていることを確保するための基盤。「満たされる」とは、（1）正確に実行する機能、（2）予期しないエラー（ユーザーまたはソフトウェアによる）に対する十分な保護、（3）意図的な侵入またはバイパスに対する十分な対策、を含む。
認証	システムのリソースへのアクセスを許可する前提条件として、ユーザー、プロセス、デバイスのアイデンティティの有効性を証明する。
承認	ユーザー、プログラム、プロセスへのアクセス権の認可または拒否
可用性	（1）データの不正な削除、または（2）サービスまたはデータの利用拒否、意図的または偶発的な試みから保護することを要求する、セキュリティ目標。
機密性	許可されていないデータ読み取りの実行に関わる、意図的または偶発的な試みから保護を要求する、セキュリティ目標。機密性保護は、ストレージ内、またはプロセス中、転送中のデータに適用される。
コンピューティングセキュリティ手法	コンピューティングセキュリティ手法は、ネットワーキング、ハードウェア、ソフトウェア、ファームウェアを使用する IT 内にインプリメントされたセキュリティ保護措置。これには、（1）セキュリティ機能をインプリメントするハードウェア、ファームウェア、ソフトウェア、（2）システム保証要件を満たすために使用される設計、インプリメント、検証テクニック、が含まれる。
データの完全性	データが承認されていない方法で改ざんされていないことを証明すること。データ完全性は、ストレージ内、または処理中、転送中のデータに適用される。
データ作成元認証	受信したデータのソースの有効性を証明すること。

サービス拒否	リソースへの承認されたアクセスの阻止、またはタイム・クリティカルなオペレーションの遅延。
ドメイン	「セキュリティドメイン」を参照。
エンティティ	サブジェクト（情報またはシステム状態のオペレーションに関わるアクティブな要素）またはオブジェクト（情報を保持または受信する、受身の要素）。
完全性	データ完全性（データが承認されていない方法は改ざんされていないことを証明すること）またはシステム完全性（システムが、不正を伴わずに、正しい方式で意図された機能を実行するときに有する品質）を侵害するような、意図的または偶発的な試みから保護することを要求する、セキュリティ目標。
アイデンティティ	セキュリティドメイン内の固有の情報であり、そのドメイン内で特定のエンティティを示すものとして認識される情報。
アイデンティティベースのセキュリティポリシー	アイデンティティ、および/または、アクセスされるオブジェクト（システムリソース）とアクセスを要求するサブジェクト（ユーザー、ユーザーグループ、プロセス、デバイス）の属性に基づくセキュリティポリシー。
IT 関連のリスク	特定の脅威のソースが特定の情報技術の脆弱性を悪用または引き起こすことによる、ネットミッション/ビジネスへの影響（影響と結びついて発生する可能性）。IT関連のリスクは、以下を起因とする、法的責任またはミッション/ビジネス上の損失から発生する。 1. 情報の承認されていない（悪意のある、悪意のない、偶発的な）開示、修正、破壊 2. 悪意のないエラーと欠陥 3. 自然災害および人災によるITの破壊 4. ITインプリメントと運用における不注意と怠慢
IT セキュリティアーキテクチャ	セキュリティ原則の記述および、システム設計を推進する原則に準拠する全体のアプローチ。たとえば、様々な分散コンピューティング環境における特定のセキュリティサービスの配置とインプリメントに関するガイドラインなど。
IT セキュリティ目標	「セキュリティ目標」を参照。

非コンピューティングセキュリティ手法	非コンピューティング手法は、IT のハードウェア、ソフトウェア、ファームウェアを使用しないセキュリティ保護対策である。非コンピューティング手法には、物理的セキュリティ（コンピューティングリソースへの物理的アクセスの制御）、人的セキュリティ、手続きによるセキュリティがある。
オブジェクト	情報を保持または受信する、受身のエンティティ。オブジェクトへのアクセスは、それが含む情報へのアクセスを意味することがある。
参照モニタ	セキュリティエンジニアリングの IT 機能用語で、(1) すべてのアクセスを制御し、(2) バイパスが不可能で、(3) 改ざんしにくく、(4) これらの 3 つの項目が確実にインプリメントされるようにする。
残余リスク	すべての IT セキュリティ対策が採用された後に残る、潜在的なリスク。各脅威に関連する残余リスクがある。
リスク	このドキュメントでは、「IT 関連のリスク」と同義。
リスク分析	システムセキュリティに対するリスクを特定し、発生の可能性、それによる影響、影響を低減するさらなる防護策を判断するプロセス。リスクマネジメントの一部で、リスク評価と同義。
リスクアセスメント	「リスク分析」を参照。
リスクマネジメント	情報技術関連のリスクの特定、コントロール、低減の総合プロセス。リスク分析、費用便益分析のほか、防護策の選定、インプリメント、テスト、セキュリティ評価も対象となる。この総合的なシステムセキュリティ評価によって、効果･効率性、ミッション/ビジネスに対する影響、ポリシー、規制、法による制約が検討される。
ルールベースのセキュリティポリシー	すべてのサブジェクトに適用される、グローバル･ルールに基づくセキュリティポリシー。これらのルールは通常、アクセスされるオブジェクトの機密性と、アクセスを要求するサブジェクトが持つ属性とを比較する。
セキュリティ	セキュリティは、システムのプロパティである。セキュリティは、機能とメカニズムの集合に限らない。情報技術セキュリティは、システム特性があり、物理的および論理的にシステムにまたがるメカニズムの集合である。
セキュリティドメイン	サブジェクト、その情報オブジェクト、共通のセキュリティポリシーの集合。
セキュリティ目標	IT セキュリティの目標は、「組織、パートナー、顧客に対する IT 関連リスクの懸念を十分に考慮したシステムをインプリメントすることで、組織がそのミッション/ビジネス上の目標をすべて達成できるようにす

	る」ことである。
セキュリティポリシー	情報オブジェクト保護に要求されるステートメント。
セキュリティ目標	5 つのセキュリティ目標は、完全性、可用性、機密性、アカウンタビリティ、保証である。
サブジェクト	オブジェクト間の情報の移動やシステム状態の変化につながる、通常は人、プロセス、あるいはデバイスの形を取る、アクティブなエンティティ。
システム完全性	システムが、不正を伴わずに、正しい方法で意図された機能を実行するときに有する品質。
脅威	ある脆弱性を悪用したり（意図的）、引き起こしたり（偶発的）する「脅威のソース」（下記で定義）の可能性。
脅威のソース	(1) 脆弱性の意図的な悪用を目的とする手法、または (2) 偶発的に脆弱性を引き起こす恐れのある状況および手法。
脅威分析	特定のオペレーション環境における特定のシステムに対する脅威を決定するために、システム脆弱性に対する脅威のソースを調査すること。
トラフィック分析	トラフィックフロー（プレゼンス、アブセンス、量、方向、頻度）の監視による、情報推移の推論。
トラフィックフロー機密性	トラフィック分析に対して保護する機密性サービス
脆弱性	偶発的に起動または意図的に悪用される可能性があり、また、システムのセキュリティポリシー違反につながる可能性がある、システムセキュリティ手続き、設計、インプリメント、内部統制などにおける弱点。

付録 A: 参照

1. __*Common Criteria fore Information Technology Security Evaluation(CC),* Version 2.1, August 1999.

2. Stoneburner, Gary; *Developing a Commercial Security Architecture*, tutorial presented at the 11th Computer Security Applications Conference, New Orleans, LA, December 1995.

3. __*Open Systems Interconnect Reference Model*, ISO 7498, Organization for International Standardization(ISO).

4. Shipman, Stephen; *Mr.Shinpman's Network Primer*; Chapter 1 "The OSI Model", http://personal.hartfordschools.org/~stephen/library/network_primer/ch01.html