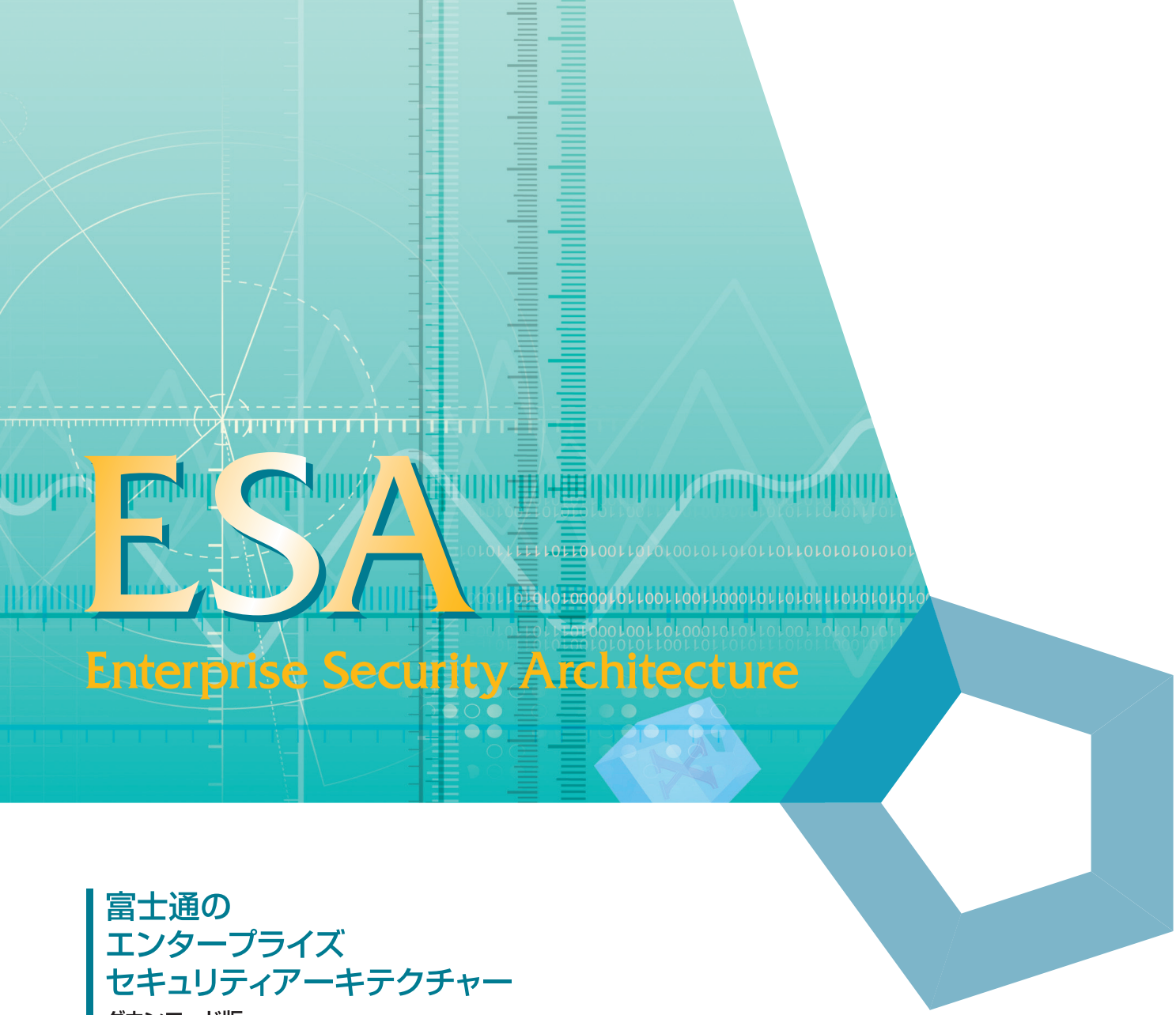


富士通の
エンタープライズ
セキュリティアーキテクチャー

ダウンロード版

富士通株式会社
情報セキュリティセンター

ごあいさつ

近年、情報セキュリティに対する関心は、ウィルスや不正アクセスなどの外部からの脅威に対する対策から、個人情報の漏洩事件に代表される内部からの脅威対策に広がってきました。

経済産業省の「企業における情報セキュリティガバナンスのあり方に関する研究会」ではその報告書で、セキュリティ対策の視点の変化として以下の項目を挙げています。

- 「技術」中心　→　「マネジメント」重視
- 「予防偏重社会」　→　「事故前提社会」として考える
- 「情報システムの問題」　→　「経営者の問題」
- 「システムを止めない」　→　「ビジネスを止めない」
- 「収益を生まない分野」　→　「信頼性を確保するための分野」

さらに、個人情報保護法や内部統制報告制度（金融商品取引法）などのコンプライアンスや、グローバルなオープンフレームワーク（ISO）への対応、事業継続の観点からのセキュリティへと広がってきています。今後は、企業戦略と一致したセキュリティ戦略を有し、具体的なセキュリティ活動目標とそのモニタリングの仕組みを備え、さらにセキュリティ投資の評価まで実装された『情報セキュリティガバナンス』の確立が重要になってきます。

当社では情報セキュリティガバナンスを確立するためには、「情報セキュリティアーキテクチャー」と「マネジメントフレームワーク」の確立が重要であると考えています。

アーキテクチャーとは、建物の建築様式が建物全体で統一されているように、システムの仕様に秩序（統一性）を与えるものと定義することが出来ます。企業にはさまざまな業務システムが存在しますが、求められるセキュリティの機能要素を整理し、システム形態や業務システムに統一した秩序を与えておくことにより、C（機密性）、I（完全性）、A（可用性）だけでなく、対策の有効性や効率性を図ることができます。さらに、セキュリティ投資の観点からみると、セキュリティ活動の達成目標や評価指標（メトリクス)の正しい考察とその可視化の仕組みが重要です。

本改版では、全体的な構成の見直しに加え、ESA に基づいたシステムのあり方の詳細説明と可視化のためのセキュリティダッシュボードのあり方を追記いたしました。

本書で記載されている内容は、当社のセキュリティソリューションを構成する製品・サービスの基本的要求事項ですが、一般の業務システムにおいてもその概念は共通と我々は考えています。

本書が、皆様の情報セキュリティ戦略の立案と実装のお役に立てれば幸いです。

富士通株式会社 セキュリティソリューション本部

情報セキュリティセンター

センター長 塩崎哲夫

執筆者紹介

氏名	経歴	執筆担当
塩崎　哲夫	セキュリティソリューション本部 情報セキュリティセンター長 ・IPA 脆弱性情報取り扱い委員 ・CISSP CBK Forum メンバー ・日本情報セキュリティ監査協会　認定委員 CISSP、CISA、CISM、公認情報セキュリティ主任監査人。	はじめに 1 章
奥原　雅之	セキュリティソリューション本部 情報セキュリティセンター ソリューション企画部長 ・ISO/IEC JTC1 SC27 WG4 メンバー ・公認システム監査人、CISSP、CIW SecurityAnalyst	2 章、3 章、 4 章、7 章 14 章～18 章
下江　達二	ソフトウェア事業本部 システムマネジメント・ミドルウェア事業部 第三開発部 プロジェクト部長 ・CISSP	4 章、5 章
畠山　卓久	ソフトウェア事業本部 事業計画統括部 プロジェクト課長	6 章
相澤　泰介	ソフトウェア事業本部 システムマネジメント・ミドルウェア事業部 第三開発部 プロジェクト部長	7 章
鈴木　俊之	ソフトウェア事業本部 システムマネジメント・ミドルウェア事業部 第五開発部 プロジェクト部長	8 章
小暮　淳	富士通研究所 セキュアコンピューティング研究部 主任研究員	9 章
鳥居　直哉	富士通研究所 セキュアコンピューティング研究部 部長 ・NICT/IPA CRYPTREC 暗号モジュール委員会メンバー ・INSTAC 耐タンパー性標準化委員会 委員	10 章
堀口　敦	セキュリティソリューション本部 セキュアファシリティ部 プロジェクト課長	11 章
吉川　信雄	セキュリティソリューション本部 情報セキュリティセンター ソリューション企画部 ・CISSP ・Master CIW Administrator, CIW SecurityAnalyst	12 章
鈴木　拓也	セキュリティソリューション本部 情報セキュリティセンター ソリューション企画部 ・ISMS 審査員補、情報セキュリティアドミニストレーター ・テクニカルエンジニア（ネットワーク）	13 章

目次

用語

以下に、本書で使用している主な用語の定義を示します。なお、定義の出典があるものは文末[　]内に示しています。

I		
IT ガバナンス	IT governance	組織戦略と組織目標の維持・拡大に企業の IT が寄与することを保証するための、リーダーシップと組織の構造・プロセス。
IT システム	IT system	業務処理を遂行するためのデータ、プログラム、ハードウェアリソースで構成される IT インフラの総称。（第 12 章）
あ		
アイエスオー／アイイーシー15408	ISO/IEC 15408	IT 関連製品およびシステムが適切に設計され、その設計が正しく実装されていることを評価するための国際標準規格。
アイデンティティ	Identity	サブジェクトに関する情報をパッケージ化した概念。
アクセスコントロール	Access control	IT システムに対するアクセスを防御または制御すること。データへのアクセスの防御または制御、プログラムへのアクセスの防御または制御を指す。
え		
エンタープライズセキュリティアーキテクチャー	Enterprise Security Architecture	企業が持つ業務システムにおける、セキュリティのあり方を体系化した情報。
か		
可用性	Availability	情報または資源への不正な妨害を防止すること[ITSEC]。認可されたエンティティが要求したときに、アクセスおよび使用が可能である特性。 [JIS Q 13335-1:2006]
監査証跡	Audit trail	監査の目的で必要となる情報の総称。
監査ログ	Audit log	監査証跡のうち、IT システムで自動的に生成される定型書式の情報。
完全性	Integrity	情報の不正な変更を防止すること[ITSEC]。資産の正確さおよび完全さを保護する特性。[JIS Q 13335-1:2006]

き		
機密性	Confidentiality	情報の不正な暴露を防止すること[ITSEC]。認可されていない個人・エンティティまたはプロセスに対して、情報を使用不可または非公開にする特性。[JIS Q 13335-1:2006]
強制アクセス制御	Mandatory Access Control	Object（データ）の中に含まれているセキュリティ要求（ラベル）と対応する Subject（利用者・プログラム）のセキュリティの許可の度合いによって変わるデータアクセス制限手法。
こ		
コーポレートガバナンス	Corporate Governance	経営者が株主のために企業経営を行っているかどうかを企業外部から監視する仕組み。
コンプライアンス	Compliance	企業が経営や活動を行う上で、法令や各種規則などのルール、社会的規範などを守ること。
さ		
最小特権	Least privilege	システムのユーザとプロセスの両方において、割り当てられた機能の実行に必要なリソースだけアクセスするよう制限するポリシー。
サブジェクト	Subject	アクセス制御においてアクセスするもの（人、プログラムなど）の総称。
し		
識別	Identification	サブジェクトを確実に区別し、見分けること。
資産	Asset	組織にとって価値を持つもの [JIS Q 13335-1:2006]。
情報セキュリティ	Information security	情報の機密性、完全性および可用性を維持すること。さらに、真正性、責任追跡性、否認防止および信頼性のような特性を維持することを含めてもよい。[JIS Q 13335- 1:2006]
情報セキュリティガバナンス	Information security governance	情報セキュリティ投資の有効性と効率性を、ステークホルダーに説明可能なように戦略性を持って投資を進める考え方。
情報セキュリティコントロール	Information Security Control	情報セキュリティの目標を達成するために実施しなければならないことの集合。セキュリティコントロール、セキュリティ管理策とも呼ばれる。

情報セキュリティ評価基準	ITSEC	1990 年に欧州4カ国（イギリス、ドイツ、フランス、オランダ）の共同作業として策定されたセキュリティ評価基準。
情報セキュリティポリシー	Information security policy	組織全体に対するセキュリティ方針と命令[GMITS]。
情報セキュリティマネジメント	Information security management	情報セキュリティコントロールの実施を確実にするための組織活動。
情報セキュリティマネジメントシステム	ISMS	マネジメントシステム全体の中で、事業リスクに対する取り組み方に基づいて、情報セキュリティの確立、導入、運用、監視、レビュー、維持および改善を担う部分。[JIS Q 27001]
職務と職責の分離	Separation of duties	統制活動に対する要求事項の一つ。職務が従業員や業務プロセスにおいて論理的に分離されていること。
せ		
セキュリティ機能	Security function	セキュリティを確保するために実装する機能。本書では、「認証」、「アイデンティティマネジメント」、「アクセスコントロール」、「証跡管理」、「集中管理」、「暗号」などを指す。
セキュリティ機能項目	Security functional requirement	セキュリティ機能を実現するための実装項目。
そ		
ソーシャルエンジニアリング	Social engineering	人に対する、人間系の不正アクセス。
た		
多層防御	Defense in depth	セキュリティ対策を多重に適用し安全性を向上させ、また防御突破までの時間を稼ぐ考え方。
と		
トラステッドコンピュータセキュリティ評価基準	TCSEC	1985 年に米国国防総省コンピュータセキュリティセンターによって制定されたセキュリティ評価基準（DoD 5200.28 － STD）。「オレンジブック」の名で知られている。

に		
任意アクセス制御	Discretionary access control	Subject（利用者・プログラム）が属するグループの確認情報を基に Object へのアクセス可否を決定するアクセス制御。
認可	Authorization	データに対するアクセス可否を決定するための判断と判断後の処理。
認証	Authentication	システムへのアクセス可否を決定するための判断と判断後の処理。
ふ		
プロテクションプロファイル	Protection Profile	ISO/ISE 15408/JIS X 5070 で規定された用語、基本的なセキュリティ要件をまとめた文書。
り		
リソース	Resource	ハードウェアリソース上に、プログラム、またはプログラムとデータを格納した資源の単位。例）Web サーバ、DB サーバ等。（第 12 章）

第一部 エンタープライズセキュリティアーキテクチャーとは

1. 企業の IT セキュリティと情報セキュリティガバナンス

今日の企業においては、IT システムは業務に不可欠なインフラになっています。そして、この IT システムをリスクから守るためにはセキュリティ対策を欠かすことができません。一般的にセキュリティ対策に掛ける投資金額は、IT 全体に対する投資の 3～5%程度であると言われてきました。わが国においては、セキュリティ投資比率はそれ以上に増加しており、平均すると 5%を超えるという結果も報告されています。[*1]

しかしその一方で、企業からの個人情報漏洩や社会システムのダウンなど、重大なセキュリティ事故は後を絶ちません。このことは、今なお多くの企業において、セキュリティ対策がいわば「場当たり」的な発想で行われており、投資に対するセキュリティ対策効果が思うように表れていないという現実を示しています。

そこで、従来、後ろ向きの投資と考えられてきた情報セキュリティ対策を、企業価値向上に向けた前向きの投資として企業全体で取り組むという考え方が提唱されるようになりました。これが「情報セキュリティガバナンス」です。

情報セキュリティガバナンスの目標の一つは、導入している情報セキュリティ対策の効果を客観的に第三者に説明できるようにすることです。すなわち、情報セキュリティ対策の有効性（対策として役に立っているか）と効率性（効果に対して投資が過剰になっていないか）を、株主をはじめとするステークホルダーに説明できることが必要です。2005 年 3 月に経済産業省商務情報政策局情報セキュリティ政策室が公表した「企業における情報セキュリティガバナンスのあり方に関する研究会　報告書」では、このような情報セキュリティガバナンスの推進を支援する、次の 3 種類のツールを提供しています。

- 情報セキュリティ対策ベンチマーク
- 情報セキュリティ報告書モデル
- 事業継続計画策定ガイドライン

これらのツールを活用することで、企業は自身の情報セキュリティ対策の有効性と効率性を分かりやすく伝えることができます。また、企業内部における情報セキュリティ対策の必要性と正当性を説明できるようになり、より組織的な情報セキュリティ対策の実施が容易になります。

*1　日本ネットワークセキュリティ協会「IT セキュリティ対策施策の導入・実施状況とその満足度調査」、2004 年

2. エンタープライズセキュリティアーキテクチャー(ESA)

2.1 企業における ESA の必要性

大型計算機が誕生したころは、情報セキュリティは「他人のデータには触れることができない」程度の概念でした。1980 年代中ごろ、米国国防総省がコンピュータのセキュリティ調達基準である「トラステッドコンピュータセキュリティ評価基準」(通称:オレンジブック)を策定したことにより、認証やログの記録など、情報セキュリティの各種の機能が広く技術者に意識されるようになりました。そして 1990 年代、いわゆる「オープンの時代」を迎え、情報セキュリティ対策の世界は大きな転機を迎えます。

大型計算機の時代は、メーカーが独自に情報セキュリティのコンセプトを策定し、設計し、実装し、出荷していました。しかしオープンな規格の普及によって、システムは複数のメーカーやベンダーが提供する機器によって構成されることが当然となり、これに伴い、情報セキュリティ機能も多くの機能部品に細分化されるようになりました。このことはコスト削減や選択の自由度拡大など、多くのメリットを利用者にもたらしました。しかしその一方で、利用者は自らの責任で各構成機器を選択しなければならなくなりました。機器同士の相互接続性、データフォーマットの一致、管理方法の整合性など、統一したシステムとして運用するための配慮は、すべて利用者の責任となったのです。特に情報セキュリティの分野では、機器やソフトウェアの組み合わせにより安全性が変化する可能性があるため、利用者は細心の注意を求められます。結果的に、不適切な組み合わせによる事故や問題が多数発生することになり、「情報セキュリティは難しい」「情報セキュリティはコストがかかりすぎる」という観念が定着してしまいました。

これを解決するのが、「エンタープライズセキュリティアーキテクチャー(ESA)」です。エンタープライズセキュリティアーキテクチャーは、企業内における情報セキュリティ対策の技術的な基本方針を明確にするセキュリティのあるべき姿を体系化する文書です。企業は情報セキュリティ対策のシステムを構築する場合あるいは機器を調達する場合、常に自社のエンタープライズセキュリティアーキテクチャーへの適合性をチェックします。その結果、エンタープライズセキュリティアーキテクチャーに適合しないと認められたシステムや機器は、企業内で採用することは認められません。こうすることで、企業内の情報セキュリティは統一的で整合がとれたものになり、セキュリティ投資の有効性と効率性が保証されます。

2.2 ESA とセキュリティマネジメントフレームワーク（SMF）

ISMS をはじめ一般的な情報セキュリティマネジメントシステムでは、さまざまなセキュリティ対策（管理策）に対して、その有効性を管理するためのマネジメントプロセスを整備することを求めています。マネジメントプロセスはいわゆる PDCA（Plan-Do-Check-Act）プロセスを構成し、継続的な改善・是正活動を通じてセキュリティマネジメントレベルを維持・向上させます。組織のリスクに応じて管理策を選定し、その効果を測定することもマネジメントプロセスの役割です。このマネジメントプロセスを確立し、効率的に運営するための手法やノウハウを体系的に整理したものがセキュリティマネジメントフレームワーク（SMF）です。

一方 ESA は、このようにして選択された管理策に、統一された技術的な指針を与え、セキュリティ投資としての効率性と、対策としての有効性を担保するための文書です。従って、SMF と ESA はマネジメント（管理）とテクノロジー（技術）の両面から情報セキュリティマネジメントシステムを支援する知識体系と位置付けることができます。

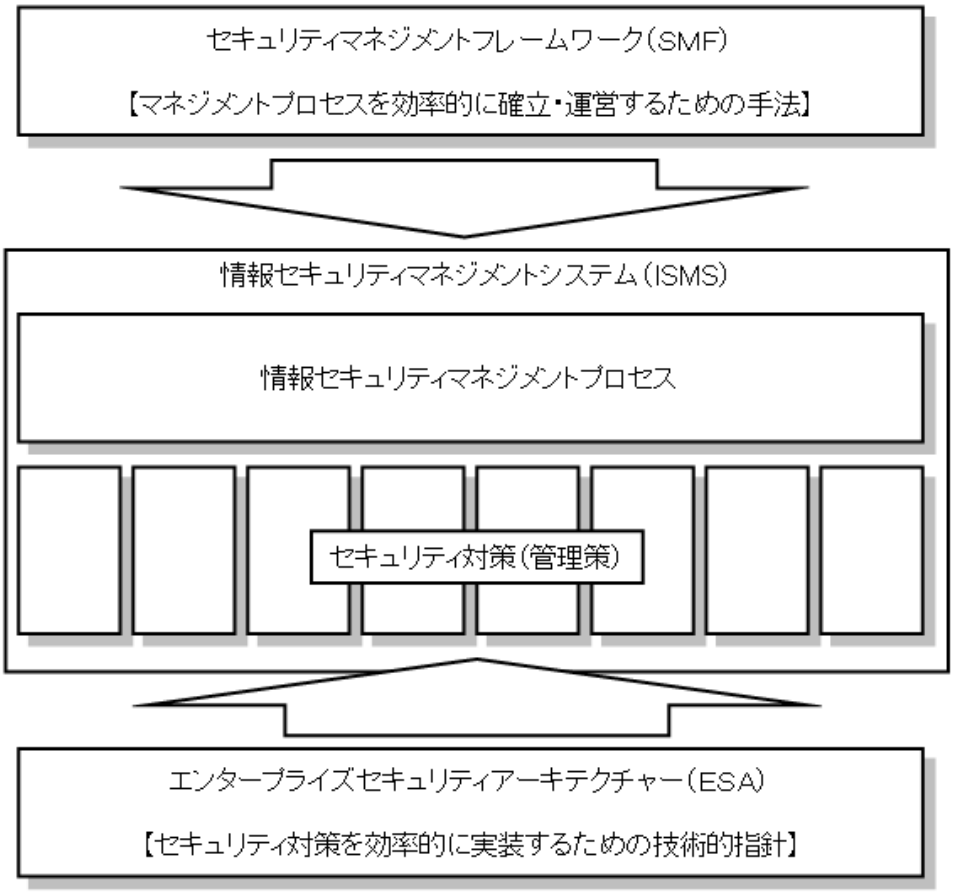


図 2.2-1 ESA と SMF の関係

2.3 ESA の確立

組織内のセキュリティアーキテクチャーを確立するためのプロセスは、一般的には以下のようになります。

1) 一般的なセキュリティ要求事項の調査

国際標準や各種のガイドラインを中心に、一般的に求められているセキュリティ要求事項を調査します。

2) 自組織内のセキュリティ要求事項の分析

一般的な要求事項とは別に、自組織の中で求められるセキュリティ要求事項を分析、整理します。例えば、すでに存在する情報システムのセキュリティ機能から来る制約や、自組織のセキュリティポリシーから来る要求事項を調査します。

3) セキュリティ機能実装モデルの作成

システム全体で、セキュリティ機能をどのように実装するかを検討するための、実装モデルを定義します。本書の第二部には、このようなモデルの例が提示されています。

4) アーキテクチャーの明文化

実装モデルに基づき、その組織にふさわしいセキュリティアーキテクチャーを決定し、明文化します。場合によって異なりますが、明文化されたセキュリティアーキテクチャーは以下のような文書に反映されます。

- 組織内のセキュリティスタンダード文書
- 情報システムの調達要件書
- プロテクションプロファイル（PP）

5) システムへの実装

定められたセキュリティアーキテクチャーに従ってシステムを実装します。どの程度、システム要件をアーキテクチャーで制約するべきかは、場合によって異なります。一般に、強いアーキテクチャー制約を与えればそれだけアーキテクチャー統一の効果は上がりますが、その分、システム設計の自由度が奪われます。

確立されたセキュリティアーキテクチャーは、セキュリティ技術の進歩などにより時代遅れとなることもあります。この場合は、セキュリティアーキテクチャーを見直すことも必要です。しかしながら、必要以上に頻

繁にアーキテクチャーを変更することは望ましいことではありません。アーキテクチャーの変更は、システム機能の統一というアーキテクチャーの本来の目的に反するものであることに常に留意するべきです。

2.4 企業の ESA と本書（富士通の ESA）の関係

エンタープライズセキュリティアーキテクチャーは、その企業の情報投資戦略から導き出されるものであり、企業ごとに異なる固有のアーキテクチャーが定められます。しかしながら今日、調達可能なセキュリティ技術は多岐にわたるため、これら技術の整合性をとりながらアーキテクチャーとして選択していくことは容易ではなく、時間とコストのかかる作業になります。

そこで当社では、一般的な企業に必要となるセキュリティ要件の共通要素を分析し、広く適用できるように考慮した標準的なエンタープライズセキュリティアーキテクチャーを作成しました。これが「富士通エンタープライズセキュリティアーキテクチャー」（本書）です。

本書では、アーキテクチャーの検討を進める上で必要になる情報セキュリティ知識の共通基盤、企業内のあるべき情報セキュリティ運用の仕組み、それを実現するのに必要となる情報システムのセキュリティ機能要件などを網羅して記述しています。

2.5 本書の構成

本書は全体で第一部～第三部および付録によって構成されています。

「第一部」では、エンタープライズセキュリティアーキテクチャーの背景、位置付けなどを説明しています。

「第二部」では、エンタープライズセキュリティアーキテクチャーを確立するために必要となる基本概念についてまとめています。例えば、「認証」「アイデンティティマネジメント」「アクセスコントロール」などの代表的なセキュリティ機能について、基本的な概念や用語の説明、現在主流になっている考え方、代表的なセキュリティ技術、構築の代表的なモデルなどを解説しており、本書の中心をなす部分です。

「第三部」では、第二部で提示したアーキテクチャーの考え方に基づいて実際にシステムを構築する場合、およびシステムを運用する場合の基本的考え方と代表的なモデルについて説明しています。

「付録」では、本来エンタープライズセキュリティアーキテクチャーの範囲外ではありますが、同時に整備が必要なマネジメントフレームワークの整備例として、リスク分析解説資料、セキュリティポリシーのサン

プルなどを掲載しています。また、その他エンタープライズセキュリティアーキテクチャーを確立する上で有用な資料も収載しています。

各章の記載内容と、組織を運営するための各種の情報セキュリティガバナンス活動との関係を示すと、以下の図のようになります。組織戦略から、情報セキュリティマネジメントシステムおよびその出力としてのセキュリティ管理策／セキュリティポリシーが策定されます。これをどのようにシステム化するか、あるいはどのように運用するかがエンタープライズセキュリティアーキテクチャーの取り扱い領域になります。また、情報システムをサービスとしてとらえた場合のサービスレベルアグリーメント(SLA)がセキュリティ運用のもう一つのインプットとなります。

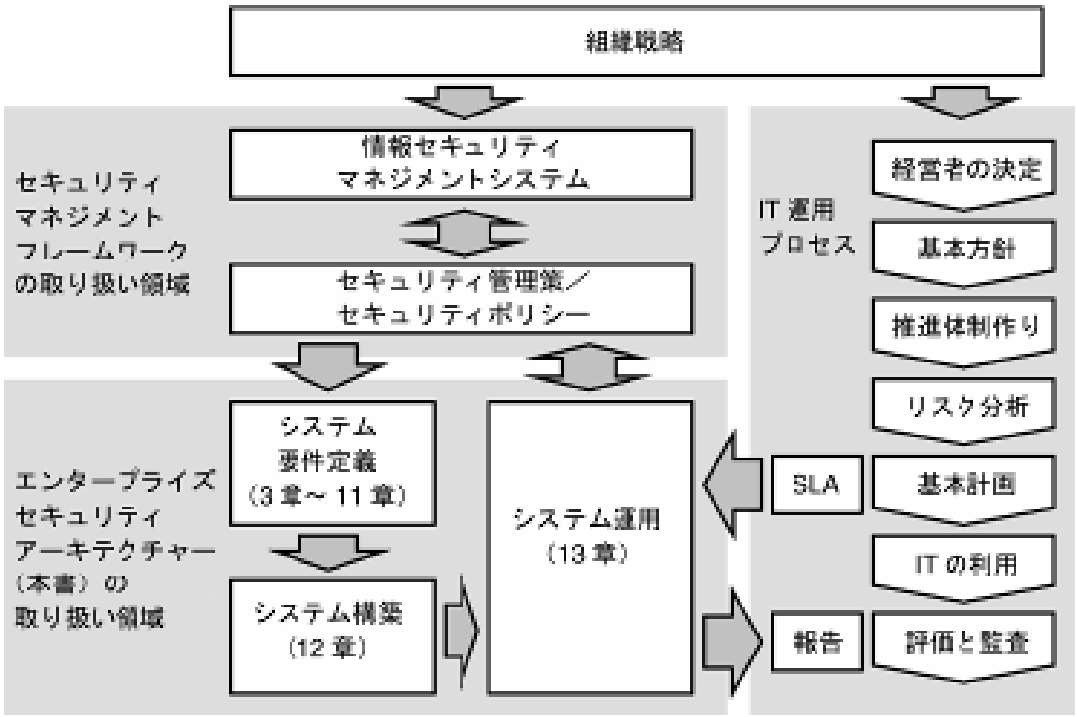


図 2.5-1 本書の取り扱い領域と周辺領域の関係

第二部 エンタープライズセキュリティアーキテクチャーの基本概念

3. 基本的なモデル

3.1 エンタープライズセキュリティアーキテクチャーの体系

今日の情報システムに求められるセキュリティ要件は、非常に多岐にわたっています。効率的なアーキテクチャーを定義するためには、まずセキュリティ要件を能率的に分類し、体系化することから始めなければなりません。

セキュリティ要件を体系化する試みは、これまでにもさまざまな場面で行われてきました。例えば、ISO/IEC15408[*2]は情報システムに要求される機能要件と保証要件を幅広く網羅した完成度の高い体系を提供しています。しかしながら、この標準を理解するにはかなりの専門知識のバックグラウンドを必要とします。また、組織内システムというかなり抽象度の高いレベルで議論するには、この標準の細かさ(粒度)では詳細過ぎて全体が見えなくなってしまう傾向があります。

このため、本書ではあえて別の観点でセキュリティ要件を整理しています。組織内のセキュリティ統制を検討する上で骨格となるべき「認証・アイデンティティマネジメント」「アクセスコントロール」「証跡管理」「集中管理」を主軸に据え、その周辺にある技術を含めて体系化することを試みています。

本書の第二部では、下の表の分類に沿って、セキュリティ要件の説明を行っていきます。

表 3.1-1 本書の分類体系

大分類	機能分類	第二部での記述章
認証・アイデンティティマネジメント	認証	6 章
	アイデンティティマネジメント	7 章
アクセスコントロール	アクセスコントロール	8 章
証跡管理	証跡管理	9 章
集中管理	集中管理	10 章
個別技術	暗号	11 章
	鍵管理	12 章
	フィジカルセキュリティ	13 章

*2 ISO/IEC 15408-1:2005 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model 他

3.2 アクセスコントロールの基本モデル

情報セキュリティに最初に求められた要件は、「ある情報を特定の人だけに知らせ、それ以外の人には知られないようにすること」でした。例えば暗号はまさにこの目的を達成するための技術です。このような要件を情報セキュリティの世界では一般に「機密性(Confidentiality)の確保」と呼びます。しかし、情報システムの取り扱う領域が拡大し、扱う量もまた増大するに従って、機密性を確保すること以外にもセキュリティとして取り扱うべき要件があることが分かってきました。一つは情報の信頼性を守るために「不正に情報を書き換えられないようにすること」で、「完全性(Integrity)の確保」と呼ばれます。また、故意にデータを破壊したりシステムをダウンさせたりする脅威に対抗するため、「情報あるいはそれを取り扱う情報システムが必要なときに使える状態にあること」という要件も追加されました。これは「可用性(Availability)の確保」と呼ばれます。これらの要件の対象となっている「機密性」「完全性」「可用性」の三つを総称して一般に「情報セキュリティの 3 要素」と呼びます。この情報セキュリティの 3 要素の概念は、1980 年代後半から 1990 年代初頭にかけて成立しました。例えば 1991 年に制定された欧州の情報セキュリティ評価基準(ITSEC)[*3] では、この情報セキュリティの 3 要素がセキュリティの定義として明示されています。

これらの要件を実現するための仕組みを考えるためには、一般的なモデルがあると便利です。いちばん簡単な機密性の例で考えます。まず、守るべき「情報」があります。また、情報を知ろうとする「人」がいます。さらに、人が情報を知るという「行為」があります。機密性の確保とは、知るという「行為」が許可される「人」と「情報」の組み合わせと、同じ「行為」が禁止される「人」と「情報」の組み合わせを明確に区別し、それを強制的に実現することだと言い換えることができます。

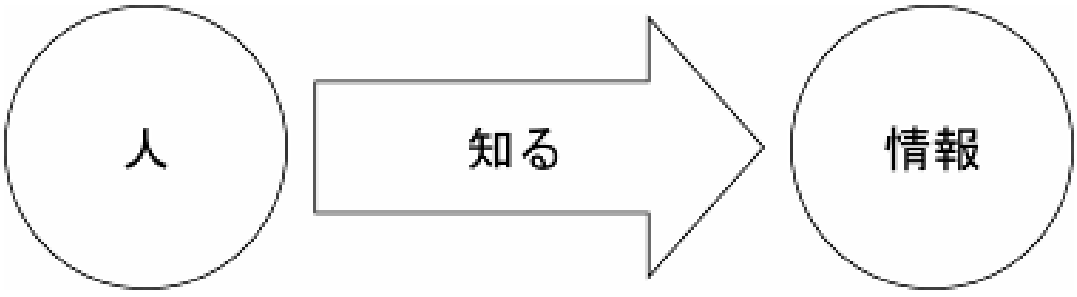


図 3.2-1 機密性のモデル

ここで「行為」を「知る」から「変更する」に変えると、完全性の確保も全く同じ形で書くことができます。そ

*3 IT Information Technology Security Evaluation Criteria, 1990

こで「行為」の内容を「操作する」という一般的な用語で書くことにします。機密性の場合は「読むという操作をする」、完全性の場合には「書き込むという操作をする」と表現します。これにより、情報セキュリティの一般的な要件を実現するためには、「人」による「情報」への「操作」を適切に許可または禁止すればよいという言い方ができるようになります。

操作の種類は、対象が情報である限りは、基本的に「読む」と「書き込む」の 2 種で十分です。しかし、UNIX などの当時の OS がプログラムをデータファイルと同様に扱うことでアクセスコントロールを統一的に扱うというアプローチを取ったために、この概念に拡張が必要になりました。まず、「情報」に加えて「プログラム」が操作の対象になりました。これに伴い、操作の種類として「実行」が追加されました。こうすることで、セキュリティを実現するさまざまなアクセスコントロールが同じ形式で記述できるという利点が生まれました。

このため、その後もアクセスコントロールの対象は増えていきました。情報とプログラムに加え、ディレクトリ、IO ポートなどさまざまな物が対象となっていきました。そこで、これらを総称する概念が必要になりました。この操作の対象となる物を総称してオブジェクト（対象、Object）[*4]、資源（Resource）などと呼びます。本書ではオブジェクトと呼ぶことにします。

さらに、操作する側も「人」以外の物が想定されるようになりました。例えば人によって起動されたプログラムであったり、プロセスであったり、リモートにあるホストであったりということが考えられるようになりました。そこで、これら操作する側のものを総称してサブジェクト（主体、Subject）[*5]、プリンシパル（Principal）などと呼びます。本書ではサブジェクトと呼びます。

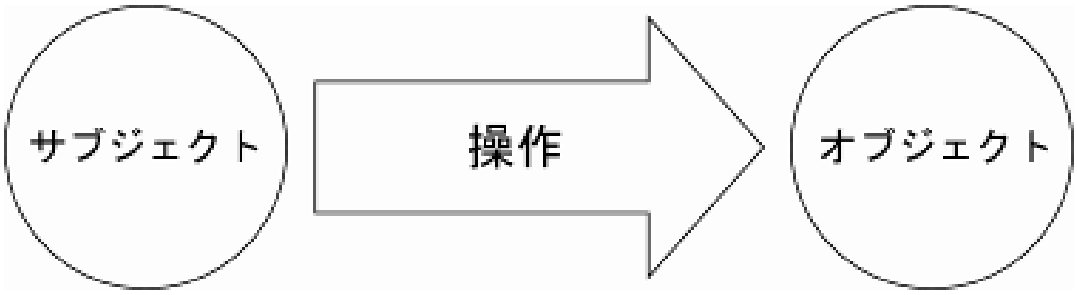


図 3.2-2 一般的なアクセスモデル

*4,5 例えば ISO/IEC 15408

これらの概念を使えば、情報セキュリティに必要なアクセスコントロールは、サブジェクトとオブジェクトと操作の組み合わせに対して、許可される操作と禁止される操作を明確に区別し、それを強制する仕組みを作ることという一般的な表現で表すことができます。次節では、より一般的なモデルについて説明します。

3.3 一般的アクセスコントロールモデル

情報システムに必要なアクセスコントロールの機能モデルは、操作される「オブジェクト」、操作する「サブジェクト」、サブジェクトによるオブジェクトの操作を許可するかどうかを決定する「認可」、および認可処理の判断に用いる「権利」から構成されます。また権利は、サブジェクトとオブジェクトの組み合わせに対して記述する「認可規則」、サブジェクトやオブジェクト以外の環境に対して記述する「利用条件」、操作時または操作後にサブジェクトに発生する「義務」から構成されます。

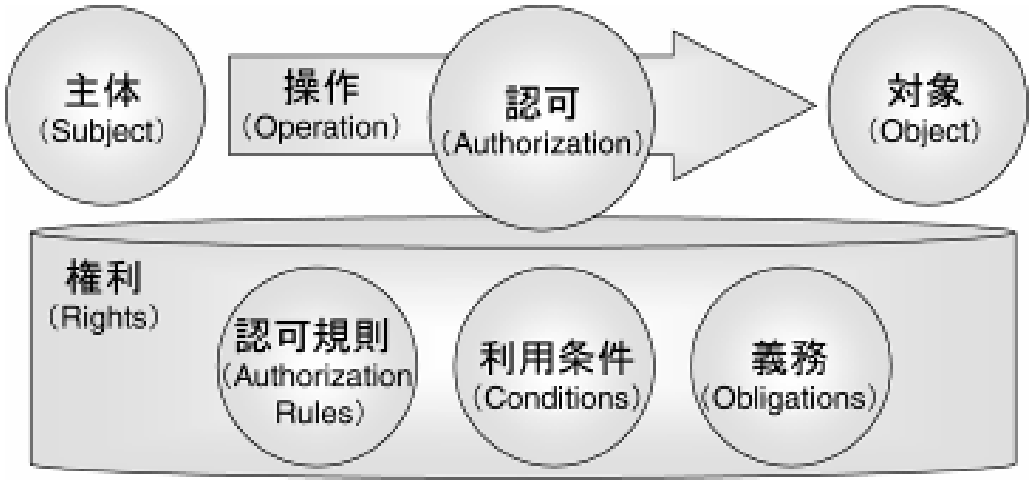


図 3.3-1 アクセスコントロールの機能モデル

各構成要素の例は、次のとおりです。

- サブジェクト(主体):利用者や利用者のエージェント(代理)としてのプロセス
- オブジェクト(対象):データ、プロセス、I/O、ネットワーク等の計算機リソース
- 操作:RWX(読み出し、書き込み、実行)、権利操作、コピー、印刷、編集等
- 認可規則:ラベルセキュリティ、RBAC、アクセスコントロールリスト
- 利用条件:時間帯、端末(ハードディスク ID や TCG チップ)等の環境条件
- 義務:アクセスログ、重畳印刷(可視/不可視すかし)等

4. 認証

4.1 識別

情報システムにおいては、サブジェクトが本当にそのサブジェクトかどうかを確認することがすべてのセキュリティの基礎となります。このために、情報システムにおいては「識別」および「認証」の機能が必要になります。

識別（Identification）とは、サブジェクトを確実に区別し、見分けることです。情報システム上でサブジェクトを識別するためには、確実に同じものがない名前を付ける必要があります。この目的のためにサブジェクトに付けられた名前を識別子（Identifier, ID）と呼びます。

全く同じものがないことを保証されていることを「一意（Unique）である」といいますので、情報システム上の識別は「一意の識別子」によって行われるということができます。人は、一般には氏名によって識別されています。しかし、氏名には同姓同名があるため、厳密には一意にはならないので、確実に識別が必要な場合は、住所その他の付加情報を加えて一意になるように運用されています。

情報システムにおいては、識別子は通常、数字列や文字列で表されます。識別子は多くの場面で利用されるため、処理するときに性能面で有利な固定長の識別子が多いのですが、近年の情報システムの処理性能向上により、可変長の識別子を採用するシステムも次第に増えてきました。

識別子の設計で考慮すべきことは、識別子を付与するときにどのようにして一意性を確保するかです。例えば、次のような方法が考えられます。

- システム上で一意になるように採番する。例えば、識別子を連番とし、最後に付与した識別子の次の番号を次の識別子に使う。
- すでに一意になっている情報を利用する。例えば、従業員番号やメールアドレスを識別子として使う。
- 識別子を自由に選択し、その都度それまでに付与した識別子と重複しないかを確認する。

また、識別子を利用者が記憶しなければならないシステムの場合は、覚えやすい識別子を付与することも考慮に入れなければなりません。

4.2 認証と認証要素

認証（Authentication）とは、情報システムにおいて、サブジェクトが情報サービス提供者等の他の当事者にとって想定したものであることを確認する機能あるいは行為のことを指します。一般には、サービスを提供するシステム側が、サブジェクトに対して正しいサブジェクトだけが提示できる何らかの情報を要求し、それを提示させることで認証を行います。最も分かりやすい例がパスワードです。パスワードは、それを提示した利用者しか知らない情報であるという前提があるため、認証の手段として利用することができます。この例におけるパスワードのように、サブジェクトを認証するための根拠となる情報を認証情報、クレデンシャル（Credential）[*6]、秘密（Secret）[*7]などと呼びます。

認証情報が何らかのものに格納されている場合は、そのものをトークン（Token）と呼ぶことがあります。例えば、認証情報が USB メモリに格納されている場合には、その USB メモリをトークンと呼ぶことがあります。

認証情報やトークンなど、認証に用いられるものを総称して認証要素と呼びます。認証要素には、さまざまな種類があります。これらの要素は、それぞれ達成できるセキュリティレベルが異なり、コストや利便性などにも違いがあります。そのため、セキュリティレベルが高いものを利用することが必ずしも最適な解とは限らないことに留意が必要です。セキュリティの世界には、「安価、手軽、安全。選べるのは二つ」（Cheap, Fast or Secure? Pick Two.）という言葉があります。すべての点で満点を取る方法がないということは、例えば次の図のような三角形上にすべての認証要素を配置できることを意味しています。代表的な認証要素の例をあわせて図中に示します。例えば、IC カードと PIN 認証の組み合わせは比較的高い安全性と安価なコストを実現しますが、利便性が単体の IC カード認証よりも低くなっていることを示しています。

*6 例えば「本人認証技術の現状に関する調査報告書」情報処理開発協会、2003 年
*7 例えば ISO/IEC 15408-1

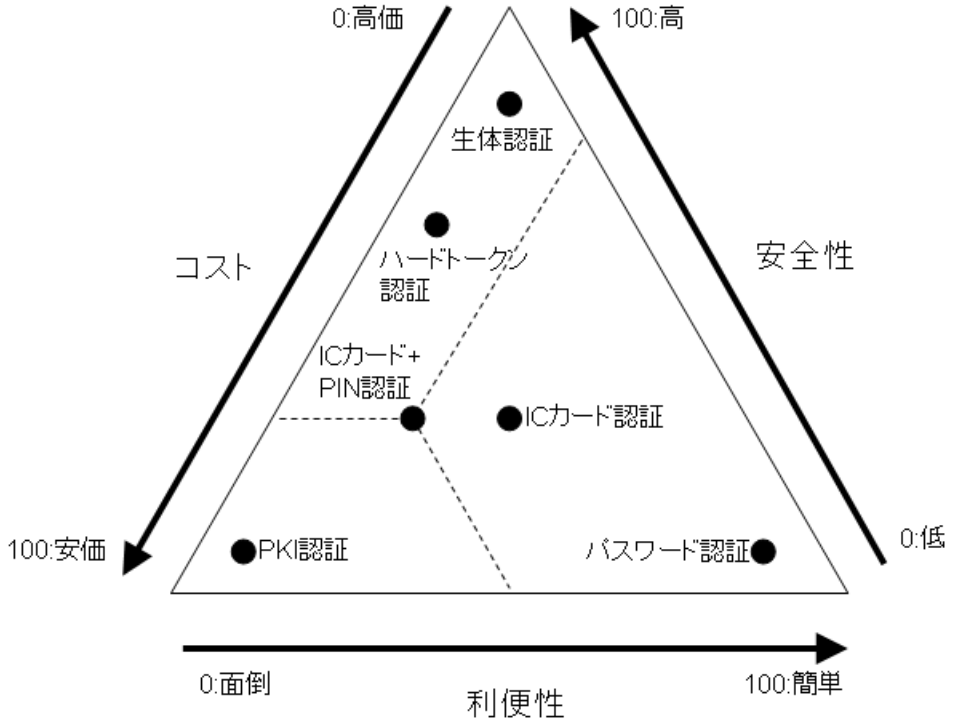


図 4.2-1 認証要素の位置付け

利用者を認証する場合の認証要素は、以下の 3 種類に分類することができます。

■ 知識情報を用いた認証（Something you know）

利用者の記憶している情報に基づいて認証する方法です。当該情報は利用者のみが知り、第三者が知り得ない秘密情報であるという前提を基に、それを知っていることが証明になり、それによって認証を行います。パスワード、パスフレーズまたは PIN（Personal Identification Number）などがこの方式に該当します。パスワードによる認証は端末に特別な仕組みを入れる必要がなく、一般的に広く使用されている手段です。しかし、セキュリティ強度の観点から言えば、この方式は利用者の記憶と運用に頼る部分が大きいため、高いセキュリティ強度を期待することはできません。高いセキュリティ強度が要求される場合には、後に述べる所有物や生体認証を用いた二要素認証での確実な認証が必要とされます。

■ 所有物を用いた認証（Something you have）

所有物を用いた認証の例として、スマートカード等の持ち運び可能な可搬デバイスを使った認証があります。デバイスの中に認証に利用する情報（パスワード、秘密鍵／証明書等）を格納し、これを認証の際に使用します。

所有物の場合は紛失による第三者の利用というリスクがあるため、これを使う際には別途 PIN の入力により、所有者を特定する方法が用いられます。この方法によれば、知識情報による認証と比べて、所有物が必須である分だけセキュリティレベルを高めることができます。また複数の情報を所有物に格納することで、端末やサービスごとに異なる知識情報を「覚える」という負担から利用者を解放し、運用の問題から来るセキュリティレベル低下を防ぐことができます。

■ 生体情報を用いた認証（Something you are）

生体情報を用いた認証方式の例としては、指紋認証や手のひら静脈認証等があります。これらの生体情報は一人一人異なり、かつ時間の経過により変化しにくいという特長があり、この特長を利用して利用者を認証します。生体情報は「覚える」ことや「持ち運ぶ」必要がないため、利用者負担が少ないのが特長です。

4.3 二要素認証

認証方式には、それぞれ利点や欠点が存在しますが、それぞれの認証方式での欠点を補完するよう複数の方式を組み合わせて認証することで、認証強度を高めることができます。このように 2 種類の認証要素を組み合わせて認証を行う方法を二要素認証といいます。

例えば、パスワードだけでは類推されたり盗み見られたりすることでなりすましがされる可能性がありますが、PKI（Public key Infrastrucure、公開鍵暗号基盤）の鍵と証明書を格納したスマートカードを所持し、その鍵を有効とするためにはパスワード（PIN）の入力が必要とするよう組み合わせておくことで、スマートカードが盗難に遭ってもパスワードが分からなければ利用できないし、パスワードを盗み見られてもスマートカードがなければ認証されないようにすることができます。

4.4 認証デバイス

認証デバイスは、パスワードや PKI 私有鍵などの秘密情報をセキュアに格納する媒体です。認証デバイスの代表格はスマートカードですが、他の認証デバイスもいろいろなものが出現しています。スマートカードにおいても、これまで、接触型スマートカードが認証デバイスとして多く使用されてきましたが、非接触型スマートカードの認証デバイスも使われ始めています。

これらの認証デバイスは、デバイスの種別ごとに別々の物理的なインターフェースを持っています。そのため認証デバイスを使える環境は、認証デバイスの種類ごとに異なります。非接触型スマートカードでは、幾つかの互換性のない標準も存在します。

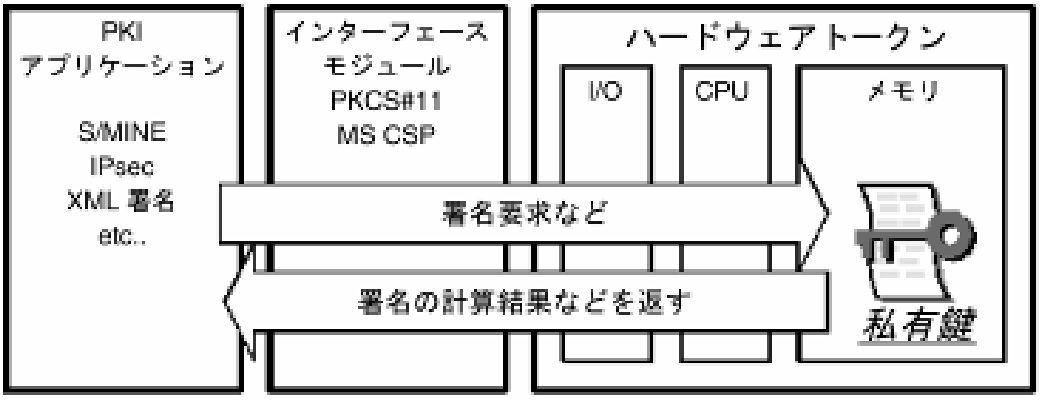


図 4.4-1 認証デバイス

表 4.4-1 認証デバイスの種類と特徴

種類	特徴
接触型スマートカード	古くから使用されているため電子政府などでも標準的な認証デバイスとしてみられている。スマートカードの形状なども標準化されており、表面に写真などを印刷して ID カードなどの用途にも使用しやすい。その一方、歴史がある分、多くの派生した仕様が存在し、相互運用性の確保に問題がある。PC などで使用する場合、カードリーダなどが必要になる。
非接触型スマートカード	公的個人認証基盤の証明書が格納可能であるとされている住民基本台帳カードでは、非接触型スマートカードが使用されている。
USB トークン	形状はスマートカードと異なるが、仕組みは接触型スマートカードと類似している。物理的 I/F は USB であり、USB の I/F が搭載されているパソコンの場合、カードリーダが不要という利点がある。
セキュリティチップ（TCG/TPM）	セキュリティチップは、PC などに取り付けて、暗号化・復号化、署名の検証などを行うICである。正式には、TPM（Trusted Platform Module）と呼ばれており、TCG[*8] が仕様を策定している。パソコンなどのマザーボード上に実装されるため、厳密には認証デバイスではないが、PP[*9] が整備され、EAL[*10] 3+認定製品も出ており、秘密情報の格納媒体としてのセキュリティ要件を備えた製品が出ている。
指紋 match on Card	スマートカード上に指紋照合装置が実装されたスマートカードのこと。

4.5 認証モデル

認証モデルを考える場合、まず、認証の範囲を整理することが必要です。一般に、認証が有効な範囲は、次の三つに分けて考えることができます。

■ ローカル環境の認証

クライアント機器などローカル環境の PC へログオンする際の認証は、その機器内でのみ有効です。この場合、管理者は OS の利用者管理機能を使用して ID を管理します。ローカル環境に保護を必要とする

*8 Trusted Computing Group： TCG は、さまざまな部品やプラットフォーム内にある重要なデータを横断的に保護するため、それらの製造に携わる企業を支援するオープンな業界標準化団体。非営利団体として設立され、マルチプラットフォームや周辺機器、デバイスに至るまで、高セキュリティ、高信頼性を備えたハードウェアやソフトウェアの標準化仕様を開発、策定、促進している。

*9 プロテクションプロファイル（Protection Profile）：ISO/ISE 15408/JIS X 5070 で規定された用語、基本的なセキュリティ要件をまとめた文書。

*10 Evaluation Assurance Level： ISO/ISE 15408/JIS X 5070 の共通基準（Common Criteria）で定める機能要件をどこまで保証しているかを表す尺度。セキュリティの強度を示す尺度として利用されている。7 段階で表記され、数字が大きいほど安全性が高い。

資産がある場合（例えばワープロ文書など、クライアント上で作成され管理される資料がある場合など）は、ローカル認証が唯一の認証による防御ポイントになります。また、ネットワークの MAC アドレスなど、機器に固有の情報をセキュリティ対策に利用している場合も、ローカル認証の強度がセキュリティの信頼の起点となります。このような、より強いセキュリティレベルが要求される場合は、二要素認証を採用します。場合によっては、二要素認証のうちの一要素に生体情報を使った認証を加えることで、さらにセキュリティレベルの強化を行います。

■ ネットワーク環境の認証

企業内システム（inB）の場合は、企業内ネットワークへの接続時の認証で主体（利用者または利用者の機器）が認証された場合に、その企業内ネットワークへ入ることができるようになります。また、企業対顧客のシステム（B2C）の場合は、サービス提供者により主体の認証が行われ、主体が認証されることで、接続が可能となります。

■ 業務やサービスの環境の認証

企業内の業務システムやお客様向けサービスへの認証は、上記のローカル環境およびネットワーク環境の認証行為で認証された主体が、企業内の業務システムまたはお客様向けサービスを利用するために受ける認証です。また、大型汎用機システムで提供する認証システムなど、専用端末から直接認証行為を行う場合も含みます。

4.6 認証に関するその他のセキュリティ要件

重要な業務システムを利用する際は、すでに認証を実施している場合でも、再度認証を行うことを考慮します。これは、すでに実施されている認証の強度が十分でない場合や、時間が経過しているため、認証時の操作者と現在の操作者が同一であることが十分に信頼できない場合に必要になります。例えば、パスワードの変更などセキュリティに直結する操作を行うときは、すでに認証済みであっても再度その操作の直前に認証を求めることが有効です。

認証にパスワードを使用する場合は、そのパスワードの強度（パスワードの品質ともいいます）をシステムが強制的にコントロールできることが求められます。例えば「1111」や「ABC」といった単純なパスワードは、他人に容易に推測されてしまうため、パスワードとしての機能を十分に果たすことができません。このようなパスワードを「強度が弱い」、あるいは「品質が低い」と表現します。強度が弱いパスワードのうち、かなりの部分はプログラムで機械的に判断することができますので、パスワード変更時に利用者が選択した

パスワードが十分な強度を持たない場合に、そのパスワードの選択をシステムが拒否することが可能です。強度が弱いパスワードを判断する条件例として、以下のものがあります。

- パスワード長が短い
- パスワードに使われている文字種（英字、数字、記号）が偏っている
- ID と同一である
- 利用者から簡単に推測できる情報を使用している（生年月日、電話番号など）
- 同じ文字の連続（1111、AAA など）
- 単純な文字の順列（1234、ABC など）
- パスワードとしてよく使われる用語リスト（パスワード辞書）に載っている単語を使っている

また、パスワードは利用者の運用によっても強度が低下します。以下の条件でパスワード強度の低下をシステムで判断できます。

- 同一のパスワードが長期間使用されている
- 同一のパスワードの使用期間が制限されている場合、いったん別のパスワードに変更し、直ちに元のパスワードに再変更している
- 2 種から 3 種程度の少ないパスワードを交互に利用している

これらのパスワード強度の低下をシステムが検知し、そのようなパスワードの使用を利用者に許可しないような機能がシステムに装備されていることが望まれます。ただし、具体的にどのレベルの強度が必要か（例えば、パスワードは何文字以上とするか）は、その組織およびシステムのポリシーに依存しますので、実装の際はポリシーに応じて可変に設定できることが望ましいでしょう。パスワードのポリシーについては、本書の運用編で詳しく述べます。

5. アイデンティティマネジメント

5.1 ID 管理の必要性

企業内に導入されているオープン系の大規模な分散コンピューティング環境では、プラットフォームだけを見ても UNIX 系 OS（Solaris, HP/UX, AIX 等）や Windows 系 OS（Windows2003）、Linux（RedHat）等の複数のプラットフォームが共存する環境があります。また、複数のミドルウェア、パッケージソフトウェア、業務アプリケーションが、独自の実装での認証・認可の機構を持つ場合もある等、さまざまなミドルウェア、アプリケーションも共存しています。

すべての OS、ミドルウェア、アプリケーションで認証・認可の環境が統合されており、シングルサインオンのサービスが提供されていることが理想ですが、既存環境に業務システムを追加していく場合には、基盤をすべて再構築することは困難です。そのため、利用者管理やアクセスコントロール情報の管理といったID管理は、異なった方式のまま拡張せざるを得ず、大規模環境のほとんどの場合では、ID管理は統合されていない環境になりがちです。特に、オープン系の大規模分散環境では、その傾向が顕著でした。こうした環境が、不適切な認証の ID 管理や ID に対応するアクセス権限管理の不備を生み出す温床となり、ひいてはセキュリティ上の脆弱性につながります。事実、過去に ID 管理の不備に起因する情報漏洩事件も発生しています。

5.2 ID 管理への要求事項

2006 年 6 月に成立した金融商品取引法により、2008 年 4 月 1 日以後開始する事業年度から、上場企業を対象にした内部統制報告制度が導入されます。これに伴うIT内部統制の一環として、以下のようなセキュリティ面の管理の強化が求められています。

- プラットフォームの特権資格、管理者資格等の特権を統制して管理すること
- IDやアクセス権の権限付与を行う際に申請者と承認者が完全に分離されていること
- 退職者のIDが残ることがないように運用されていること
- 最小限のアクセス権限付与（Least Privilege）が管理されている統制環境になっていること

今後、企業の IT 環境では、このようなセキュリティのコントロール（統制）が重視されるようになっていくと予測されます。ID 管理は、このコントロールを強化するための技術手段として欠かせない技術として注目されています。

利用者が持つ権限を変更する場合は、申請者と承認者、運用管理者を分離するセキュリティの原則（職務と職責の分離、Separation of duties）を厳格に適用して運用することが非常に重要です。また、データやサービスにアクセスする人は必要最小限にとどめる原則（最小特権、Least Privilege）を厳守しなければなりません。アクセス権を付与していた利用者が長期間そのサービスを利用しなかった場合には、その利用者の ID の存在が脆弱性につながらないように権限を取り消すなどの、ID 利用状況を監視する仕組みの実装も必要です。さらに、単に ID 情報の同期を図るだけではなく、ID 情報の作成、アクセス権限等の属性情報の変更、ID 削除といったライフサイクルを統制する環境を確立することが重要です。

5.3 LDAP ディレクトリ

ID 管理の技術として普及している技術の一つが LDAP ディレクトリです。LDAP ディレクトリは、利用者に関する情報のリポジトリ（格納庫）の役割を担います。認証に用いる利用者の基礎情報を LDAP ディレクトリで一元管理を行うことで、管理情報の一元化・統合化を図る際によく利用されます。LDAP ディレクトリの主な用途を次にまとめます

表 5.3-1 LDAP ディレクトリの用途

件名	用途	検索対象
電子電話帳	検索アプリケーションと連動し、個人情報を検索する。	姓名、所属情報、役職、Email、TEL、FAX、など
統合アドレス帳	メールクライアントやグループウェアのメール機能と連動し、あて先のメールアドレスを検索して利用する。	姓名、Email アドレス
利用者認証	Web サーバや認証システムと連動し、利用者情報を利用して認証・認可を行い、アクセスコントロールを行う。	利用者 ID、パスワード

LDAP ディレクトリは LDAP（Lightweight Directory Access Protocol）[*11] と呼ばれるプロトコルで要求を受け付けます。システムの構築においては、各種サービスを LDAP に対応させることがポイントになります。

LDAP ディレクトリを利用することにより、複数のコンピュータやシステム間で利用者の情報を共有することができるようになりました。しかし、どの利用者がどの情報にアクセスしてよいかなどのアクセスコントロールに関する情報まで共有することは、LDAP では困難です。これを実現するためには、その利用者の役職や役割、情報アクセスが許可されるルールなど、LDAP ディレクトリでは扱うことが難しい情報を共通で管理する仕組みが必要です。

一つのアプローチが、LDAP ディレクトリ全体を管理する別のディレクトリを追加する方法です。この方式をメタディレクトリと呼びます。メタディレクトリは LDAP ディレクトリ間の項目の違いを吸収したり、複数の LDAP ディレクトリの同期を取ることができます。そして、利用者の詳細な属性を統合的に管理するために作られたもう一つの考え方が、アイデンティティマネジメントです。

5.4 アイデンティティマネジメント

アイデンティティ（Identity、識別情報とも呼ばれる）は、サブジェクトに関する情報をパッケージ化した概念です。サブジェクトに割り当てられた識別子、サブジェクトのクレデンシャル、サブジェクトに関するいろいろな属性情報（Attribute）などが、アイデンティティを構成する要素になります。

属性情報には、更新頻度が比較的多い静的な属性情報（Static Attribute）と、比較的少ない動的な属性情報（Dynamic Attribute）の 2 種類があります。静的な属性情報の例として、氏名、住所、所属、役職などがあります。また動的な属性情報の例として、利用者の現在位置などがあります。属性情報全体をプロファイル情報と呼ぶこともあります。

このアイデンティティを統合的に管理する技術が、アイデンティティマネジメントです。その一つとして、SOA アーキテクチャー上でアイデンティティマネジメントを実装するモデルが OASIS[*12] から提唱されています。この方式では、SAML[*13]、XACML[*14] などの XML ベースのプロトコルでアイデンティティ情報を共有する仕組みになっています。

*11 RFC2251-Lightweight Directory Access Protocol（v3）
*12 Organization for the Advancement of Structured Information Standards
*13 Security Assertion Markup Language, OASIS
*14 eXtensible Access Control Markup Language, OASIS

■ SAML

SAML（Security Assertion Markup Language）は、OASIS の Security Services Technical Committee で策定されている標準仕様です。2002 年 11 月に V1.0、2003 年 9 月に V1.1 が OASIS 標準となり、2005 年に V2.0 の策定が行われました。すでに SAML2.0 を実装したソフトウェアパッケージ製品が複数のベンダから出荷されています。今後、2.0 準拠の製品が、今後市場の主流になると予測されます。

SAML は、セキュリティ情報を交換するための XML ベースのフレームワークを提供します。このセキュリティ情報はサブジェクトに関するアサーション（assertions; 表明）という形式で表現されます。

SOAP/XML 技術を利用したアサーションは、サブジェクトにより遂行された認証行為に関する情報、サブジェクトの属性に関する情報、ある資源へのアクセスをサブジェクトが許可されているかどうかの認可決定に関する情報を運ぶことができます。一つのアサーションの中に、認証、認可、属性に関する異なるステートメントを含むこともできます。

■ XACML

XACML は、SAML 同様に OASIS で標準化されたアクセスコントロールポリシー交換のための標準仕様です。XACML では、アクセスコントロールのための認可条件などのポリシーを XML で表現します。また、条件確認のための要求および応答のプロトコルも規定しています。

- アイデンティティマネジメントのモデル

  マスターとなる ID 管理のリポジトリと管理対象の ID 管理簿の同期を ID プロビジョニングと呼びます。ID プロビジョニングでは、管理者やエンドユーザの ID 情報や属性情報（アクセス権限、管理者権限など）を統合的に管理し、新規追加、変更、削除などの処理を一元的に処理します。ID プロビジョニングを実現するためには、統合アイデンティティマネジメントの機構を導入する必要があります。統合アイデンティティマネジメントは、ID 情報の管理機構を持つ物理セキュリティシステム、ネットワーク、サーバ OS、ミドルウェア、アプリケーション、レガシーシステムなど、幅広いシステムを管理対象とします。

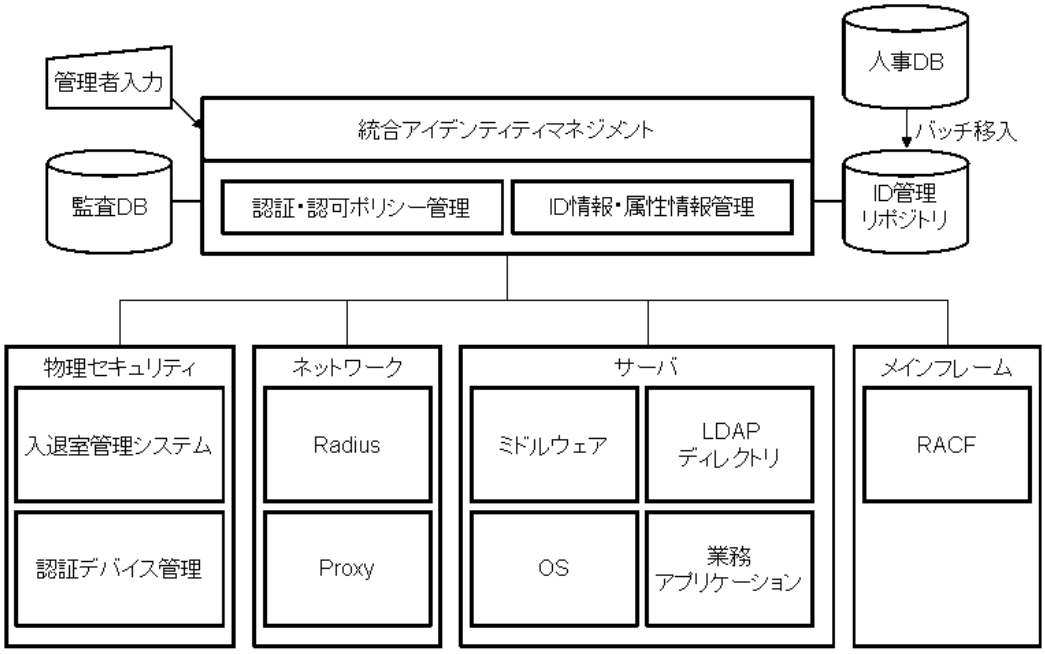


図 5.4-1 統合アイデンティティマネジメントのモデル

■ アイデンティティマネジメントのアーキテクチャー

アイデンティティマネジメントは、以下のコンポーネントから構成されています。

- ID プロビジョニングサーバ（同期機能）
- ID 管理機能
- 同期アダプタ
- ローカルエージェント
- リモートエージェント
- リポジトリ
- ワークフロー
- 監査証跡・監査機能

ID 管理のアダプタと管理対象サーバ側（OS、ミドルウェア、アプリケーション）間の連携方法には、幾つかの方法があります。製品固有の独自方式では、telnet や Open SSH が利用されたり、リモート側に対して標準プロトコルの LDAP で同期を図る方式もあります。個々の ID 管理ミドルウェアが、売れ筋の ISV ミドルウェアに対しては、標準アダプタを提供しているケースが多いのですが、業務アプリケーションの場合、個別開発が必要となります。

6. アクセスコントロール

6.1 アクセスコントロールの方式

「基本的なモデル」の章では、アクセスコントロールを「サブジェクトとオブジェクトと操作の組み合わせに対して、許可される操作と禁止される操作を明確に区別し、それを強制する仕組みを作ること」と表現しました。この章では、この目的を達成するために必要なアクセスコントロールの仕組みの実装技術について説明します。

計算機システムのアクセスコントロールの方法として歴史が古く、今日でも多くのシステムで採用されているのが、オブジェクト（ファイルなど）の所有者が誰にアクセスを許可するかを指定するという方法です。例えば、Unix 系の OS であれば、ファイルの作成者は「自分自身」「自分と同じグループの利用者」「それ以外」の三つのカテゴリの利用者に対して、それぞれ独立に「読み出し」「書き込み」「実行」を許可するかどうかを指定することができます。このような方式を「任意アクセス制御」（Discretionary Access Control; DAC）[*15] と呼びます。

任意アクセス制御を実現するためには、あるオブジェクトに対して、誰がどのようなアクセス権限を持つかという情報をシステムが維持する必要があります。これを表の形で表現したものがアクセスコントロールリスト（Access Control List; ACL）です。ACL はアクセスコントロールの基盤ですから、不正なアクセスから守られるように厳重に管理されなければなりません。

任意アクセス制御方式においては、アクセス権限の設定は全面的にオブジェクトの所有者に一任されています。従って、この方式がアクセスコントロールとして有効に機能するためには、オブジェクトの所有者が常に正しくアクセス権限を設定するという前提が必要です。オブジェクトの所有者が不適切なアクセス権限を設定してしまえば、任意アクセス制御方式のシステムはそのオブジェクトを保護することは不可能になってしまいます。

この「オブジェクト所有者は常に適切な設定をする」という前提は、組織が大きくなればなるほど、その維持が困難になります。例えば、ファイル作成者の不注意で不適切な読み出し権限をファイルに与えてしまったり、また作成者自身の悪意により、本来は権限のない利用者にファイルへのアクセスを許すことなどの問題が発生する可能性があります。さらに、利用者の権限が委譲されたプログラムを不正に乗っ取り、

*15 例えば米国防総省 Trusted Computer System Evaluation Criteria, DoD 5800-28 STD を参照

利用者が意図しないアクセス権限をプログラムに勝手に設定させるような攻撃手法(トロイの木馬)も出てきました。これらの問題を根本的に解決するためには、オブジェクトの所有者が自由にそのオブジェクトのアクセス権限を指定できるという、任意アクセス制御モデルの前提を変えなければなりません。

この問題を解決する方法として考えられたのが、アクセス権限の付与をルール化して、すべての利用者がそのルールに従うようにする方式です。この方式では、オブジェクトの所有者であっても、アクセス権限を自由に設定することはできません。そのオブジェクトの性質によって、誰がそのオブジェクトにアクセスしてよいかは、システムによって強制的に決められてしまいます。このようなアクセスコントロールの方式を「強制アクセス制御」(Mandatory Access Control; MAC)[*16]と呼びます。

強制アクセス制御では、常にオブジェクトの性質やサブジェクトの状態(どの権限を持つ利用者として現在アクセスしているか)を意識して処理しなければならないため、アクセス制御の実装は任意アクセス制御に比べてはるかに複雑なものになります。一般に、オブジェクトの性質を正確に表現するために、すべてのオブジェクトにその性質の情報を付与し、その一貫性がシステム上で常に維持できることをシステムが保証することが必要になります。このような目的でオブジェクトに付与される情報を「ラベル」(Label)と呼び、このラベルを一貫して取り扱う機能を持っていることを「ラベルセキュリティ」と呼びます。ラベルは ACL と同様にシステムによって厳密に管理され、利用者がこれを削除したり改変したりすることは一切できません。

強制アクセス制御やラベルセキュリティは、一般に「トラステッド OS」と呼ばれる高セキュリティ機能 OS などに実装されています。強制アクセス制御を運用するためには、取り扱うすべてのオブジェクトに対して、どのようなアクセス権限が許されるかというルールを事前に決めておく必要があります。このため、取り扱う情報が多岐にわたる OA 系システムなどで強制アクセス制御を採用するためには、非常に大きな運用コストが必要となります。強制アクセス制御は強力なアクセス保護機能ではありますが、この運用コストの点にも留意し、適用範囲を検討することが必要です。一般に、IT 化されていない一般的な文書の取り扱いルールが厳密に定められていない組織の環境では、強制アクセス制御の導入は効率的ではありません。

次節以降で、アクセスコントロールに利用される技術と要件の詳細を説明します。

*16 例えば米国防総省 Trusted Computer System Evaluation Criteria, DoD 5800-28 STD を参照

6.2 アクセスコントロール技術

■ ロールベースアクセスコントロール（RBAC）と最小特権

一般的なシステムに用意されている万能の管理者アカウントであるスーパーユーザ（例えば UNIX 系 OS における root）を認めず、システムの管理作業に必要な権限だけを持つ複数の役割（ロール）を定義し、各役割に対応するアクセスコントロール機能を提供します。各ロールには、権限に応じた最小限の役割しか与えません。このポリシーを「最小特権」（Least Privilege）と呼びます。最小特権機能はスーパーユーザの最高権限を複数ロール（運用と監査等）に分散します。このモデルは複数の管理者が運用業務に当たる中大規模システムで必要になり、このモデルの採用により「利用者や管理者の内部犯行」／「外部からの侵入」による被害を局所化します。

■ ラベルセキュリティ

前に述べたように、強制アクセス制御を実装するモデルです。すべてのサブジェクトとオブジェクトに対し、それぞれが属する区画（ドメイン／カテゴリ／階層）をラベル付けし、区画間の認可規則に従い認可処理を行います。区画間の認可規則はアクセスコントロールポリシーとしてシステム設計時に決定され、運用時は管理者も変更できません。認可規則は次の 2 種類に分けられます。

- 包含関係ポリシー：指定サブジェクトのみ指定区画内アクセスを許可する。
- 階層ポリシー：上位から下位へ情報を流さない。

なお、異なるカテゴリ間のアクセスは、任意アクセス制御と同様に禁止されます。

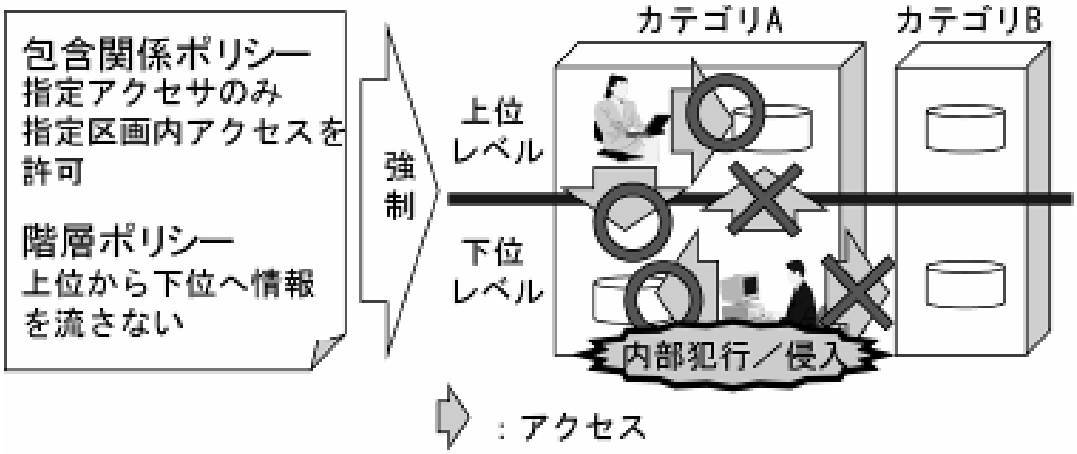


図 6.2-1 ラベルセキュリティ

■ VM による区画化

脆弱性のない仮想隔壁を持つ VM（仮想マシン）による情報システム全体の保護は、包含関係がなく、区画と階層ポリシーが一つのラベルセキュリティによる保護に相当します。これにより、万が一被害が生じた場合の被害の範囲を一つの VM 内にとどめることができます。

■ 利用制御（UCON：Usage Control）

認可規則のみでなく、利用条件と義務も権利の要素として定義・強制することが可能な方式のモデルです。このモデルはオブジェクトへのアクセスのみでなく、アクセス後の利用についても（「実行」のみでなく）細かく制限可能なため、「利用制御」（Usage Control; UCON）と呼ばれ、今後の主流となるモデルであると考えられています。

UCON モデルの認可規則は上記三つのアクセスコントロールモデルの任意の組み合わせとして実装します。UCON モデルは、さらに利用条件や義務もアクセス権として管理する著作権保護（Digital Rights Management; DRM）、プライバシー保護等の方式を含みます。

6.3 アクセスコントロールの実現および有効な運用のための前提

アクセスコントロールがその役割を有効に果たすためには、次の機構との連携が前提です。

- 脆弱性管理：アクセスコントロール機構を構成するすべてのモジュールとモジュール構成の脆弱性検査と修正。
- 識別と認証：アクセスコントロール機構と連携する利用者識別・認証機構が正しく利用者のログオン状態を判定していること。

また、アクセスコントロール機構は、計算機の資源アクセス時に必ず通過しなければならない処理機構として、アクセス可否判定結果を資源アクセスログとして生成する役割をも果たします。資源アクセスログは、監査証跡として最も重用される監査証拠情報です。

6.4 アクセスコントロールの実装と導入

脆弱性のないアクセスコントロール機構の実装には考慮するべき項目も多く、十分な知識・経験と細心の注意およびテストを必要とします。OS やミドルウェアなどの既存の安全なアクセスコントロールフレームワークが利用できるのであれば、できるだけそれを利用するべきです。アプリケーション開発時に独自のアクセスコントロール機構を安易に実装することは逆に脆弱性を拡大することになり、推奨できません。ま

た、脆弱性のないアクセスコントロール機構を独自に実装することは、高度なセキュリティ技術者による高コストでの設計・開発を必要とし、一般には得策ではありません。

また、ラベルセキュリティはシステムのセキュリティ強化に有効ですが、その採用を検討する場合は、導入・運用にかかる負荷とコストを過少評価しないように留意する必要があります。ラベルセキュリティを導入して、正常運用するには、OS やミドルウェアを含むソフトウェアモジュールの関係と情報セキュリティに関する高度な知識・経験および技術が必要です。

6.5 アクセスコントロールポリシーの一貫性と集中管理

アクセスコントロールは VM、OS、ミドルウェア、アプリケーションの各レイヤーで設定され、実施されるため、システム全体のアクセスコントロールポリシーを一貫して運用しなければ、同じリソースへのアクセスコントロール設定なのにレイヤーによって異なる設定になる可能性があり、注意が必要です。こうした一貫性のない設定がシステムの脆弱性を生み出す原因になるため、アクセスコントロールポリシーの一貫性を維持し、ポリシー運用管理の TCO を削減するために、アクセスコントロールポリシーの集中管理が必要になってきています。アクセスコントロールポリシーに必要な利用者属性情報を集中管理するための仕組みであるアイデンティティマネジメントの詳細については、「5.アイデンティティマネジメント」の章を参照してください。

6.6 アクセスコントロール機構の分類

アクセスコントロール機構には、次のようなものがあります。

- 物理的機構（入退室管理、耐タンパモジュール、電磁波遮断ガラス等）
- 論理的ハードウェア機構（電子回路等による制御）
- 論理的ソフトウェア機構（条件文を用いたプログラム）
- 暗号化

アクセスコントロールを用いて守る範囲［物理空間、内部ネットワーク、計算機システム、計算機リソース、それらの集合］により、利用できるアクセスコントロール機構が異なります。守る範囲と適用できる制御機構を整理すると、以下のようになります。

表 6.6-1 アクセスコントロール機構の分類

アクセスコントロール機構	説明
ネットワークアクセスコントロール	ネットワーク機能の一部として実装。ファイアウォールなど。
リモートアクセスコントロール	各サーバ／クライアントシステム内で、外部からのネットワークアクセスを制限。Webアクセスコントロール、NFSのアクセスコントロールなど。
ローカルアクセスコントロール	外部および内部からのリソースアクセスを制限。OS や DB のアクセスコントロール。
利用制御 （Usage Control; UCON）	リモートかローカルかを問わず、サブジェクトとオブジェクトと操作の観点のみで操作制限を実現。

6.7 多層防御モデルによる被害局所化

アクセス制御などによる情報セキュリティ上の被害の防止には限界があり、万が一被害が生じた場合の被害の局所化を何重にも考慮しておくことは、より安全で安心できるシステムを目標とする場合に重要になります。この考え方を、「多層防御」（Defence in depth）と呼びます。最も信頼できるはずの管理者までも含め、正規利用者もミスのみならず、故意に被害をもたらした場合を想定し、アクセスコントロールの一環として被害の範囲を局所化する対策を各レイヤーで取ることが重要です。

表 6.7-1 各アクセスコントロール方式による被害局所化範囲

被害局所化の範囲（単位）	アクセスコントロール方式
内部ネットワーク	フィルタリング（Firewall）と検疫
計算機システム	ログオン制御（識別と認証）
仮想マシン（VM）	VM による区画化
管理者が操作を許諾された範囲	最小特権指定可能 RBAC
リソースの集合（タイプ／カテゴリ）	ラベルセキュリティ
リソース（情報，プロセス等）	ACL（アクセスコントロールリスト）

7. 証跡管理

7.1 証跡の分類

今日の企業活動においては、多くの場面で証跡が必要とされます。それぞれの証跡は、その目的によって性格が大きく異なります。ある証跡は大量に保存する必要がある一方で、別の証跡は量は少ない代わりに直ちに管理者の元へ届くことが求められたりします。このような証跡の性格を整理することが、証跡を効率的に管理するための前提条件になります。

本書では、証跡を以下の 4 分類に分けて検討します。

表 7.1-1 証跡の分類

分類記号	証跡分類名	定義
M 型	マネジメント状況把握型	情報セキュリティマネジメントシステムやマネジメントプロセスが正しく機能していることを確認するための証跡。
C 型	コントロール状況把握型	個々の情報セキュリティ対策が正しく機能していることを確認するための証跡。
D 型	セキュリティ不正検知型	不正な行為によって個々の情報セキュリティ対策が脅威に面していることを知らせるための証跡。
T 型	セキュリティ追跡性確保型	不正な行為があったときに、その行為の内容や影響範囲を事後的に確認するための証跡。

■ マネジメント状況把握型（M 型）

情報セキュリティマネジメントシステムやマネジメントプロセスが正しく機能していることを確認するための証跡です。文書や報告書など自由形式で記録されることが多いため、システムで自動的に処理するのには向きません。版管理や承認履歴など文書としての正当性に対する要件が多いので、文書管理システムなどで取り扱うことが有効です。証跡としてのデータ量は決して多くはありません。また、集中管理する必要性もそれほど高くありません。

■ コントロール状況把握型（C 型）

個々の情報セキュリティ対策が正しく機能していることを確認するための証跡です。パッチ適用状況、セキュリティソフトの導入状況、ファイアウォールの稼働状況などがこれに相当します。一般的に、日常的なセキュリティチェックリストに記載される項目がほぼこれに当たります。セキュリティ対策が機能しなくなっ

た場合には速やかにその事実を検知する必要がありますから、この証跡には適度なリアルタイム性が求められます。証跡としてのデータ量は多くありません。状況を的確に把握するために、集中管理を行うインフラが求められることがあります。

■ セキュリティ不正検知型（D 型）

不正な行為によって個々の情報セキュリティ対策が脅威に面していることを知らせるための証跡です。セキュリティの異常ログやファイアウォールの遮断ログなどがこれに当たります。かなり緊急性が高い性質のものを含みますので、証跡の収集には一般に高いリアルタイム性が求められます。証跡としてのデータ量は比較的少量です。その特性上、このカテゴリの証跡はよくセキュリティ監視の対象となります。

■ セキュリティ追跡性確保型（T 型）

不正な行為があったときに、その行為の内容や影響範囲を事後的に確認するための証跡です。実際にどの情報にアクセスしたか、どのような操作をしたかなど事後に検証できるようにするために、正常な業務の結果を記録する必要があります。このため、データ量が大量になる傾向があります。収集のリアルタイム性は高くはありませんが、目的によっては例えば「72 時間以内に事実を確認できること」といった時間制約が付くこともあります。集中管理できることが望ましいのですが、データ量が多いため、データ集約のコストが高くなりがちです。管理方法は、大容量データの保管に最も適した方法の選択が最優先される傾向があります。事件の証拠として証跡を用いる場合（いわゆるフォレンジックの用途）は、上書きできない記憶媒体を利用するなどのデータの正当性の保証対策が求められますが、厳密にこの保証を担保しようとするとデータ量の多さから莫大な投資を必要とする場合もあり、費用対効果の考量が必要です。なお、証跡をフォレンジック用途に利用する場合は、証跡が通過するすべてのプロセスにおいて情報の信頼性を保証する chain of custody の概念など、フォレンジックに特有の概念を理解しておく必要があります。

7.2 証跡の収集と記録の方針

前項では証跡を 4 種の類型に分けましたが、現実にはこれらの証跡は複雑に絡み合っています。例えば、同じ機器で発生するログでも、失敗ログは D 型（セキュリティ不正検知型）、成功ログは T 型（セキュリティ追跡性確保型）になるのが一般的です。どちらか一方だけを記録するのであればさほど問題はありませんが、両方を記録するならば、それぞれの証跡類型に求められる要件の双方を満たさなければなりません。

D型とT型の証跡は、論理的にはITシステム上の資産を利用する場面で常に取得することが可能です。この資産利用時のD型・T型の証跡を、本書では監査ログと呼びます。7.3節以降では、監査ログに一般的に求められる要件を整理していきます。

また、C型（コントロール状況把握型）とD型は、一般にモニタリングの対象となります。セキュリティ管理はPDCAが継続的に行われ改善されていくことが重要です。そのためには、システムの運用が監視（モニタリング）され、対処・見直しが必要な問題を早期・確実に発見できることが必要となります。セキュリティ管理上、モニタリングに求められるものは、以下のとおりです。

- セキュリティに関する機能（製品の設定等）が計画どおりに実施されている／されていないことが確認できること。また、実施されていない場合、管理者に通知されること。
- 対処・見直しが必要となる事象発生が通知・記録されること。

一方で、セキュリティ問題の影響把握、業務継続性の観点から、システム全体の運用が正常に行われていることをモニタリングできている必要があります。つまり、システムの監視、運用管理とセキュリティ管理のモニタリングは切り離せない関係であるといえます。このことから、セキュリティ管理とシステム運用を統合管理でき、役割（セキュリティ管理者、運用管理者、業務担当者等）に合わせて管理できることが求められます。モニタリングの対象となるのは、以下のような事象です。

- システム異常（ハード、ソフト）
- 性能情報（CPU、メモリ、ディスクI/O、ネットワーク・トラフィック）
- セキュリティ管理製品のアラート
- ログの異常

性能情報のモニタリングは、システムのキャパシティ・プランニング以外にもDoS攻撃によるネットワーク・トラフィックの増加等を検出できる可能性があり、セキュリティ上も有効な監視項目です。ログの異常とは、ログ（例えば、IDSのログなど）に直接的に異常を示す情報が出力されることや、特定パターンのログが出力された場合に警告をあげられるようなログのコリレーション監視のことを指します。モニタリングがログのコリレーション（Correlation; 相関分析）機能を持つことは、ノウハウの蓄積により異常検出パターンを追加でき、監視精度を上げるのに非常に有効です。

7.3 監査ログの技術要件

■ 記録するべき項目

監査ログに記録すべき事象には、以下のものがあります。

- 保護対象資源の生成・変更・削除
- 保護対象資源に対するアクセス権の設定・変更
- 保護対象資源に対するアクセス
- システムの構成・設定変更
- ログオン、特権を必要とする操作(権限取得)

これらの事象に対して 4W1H(When:いつ／Who:誰が／Where:どこから／What:何を／How:どうしたか)の情報を記録することが必要とされ、以下のものを基本として機能に応じた情報を補足します。

- 事象発生日時
- 利用者識別子(利用者 ID 等)
- 利用場所(要求元 IP アドレス等)
- 事象の種別
- 対象資源
- 事象(要求)の成否

ただし、機密・保護対象そのものである情報(例えば、パスワードなどの認証情報)は、たとえ暗号化していようともログ出力してはいけません。監査情報としての必要性がない上に、セキュリティリスクの拡大になるためです。

```
2006/06/30 01:30:10,user01,clientA,"Security:  情報: 0001:セキュリティポリシー
が適用されました。(name:xxxx/value:yyyy)"
2006/06/30 01:40:25,user21,clientB,"Security:  警告: 0002:セキュリティポリシー
が変更されました。(name:xxxx/value:zzzz)"
```

図 7.3-1 ログの出力例

複数のログを用いて監査や、分析、事象の原因追跡を行う場合、それらのログは一つのルールで正規化されていることが理想です。例えば、共通の意味を持つ発生日時、利用者情報、IP アドレスなど、ログごとに固有な拡張情報が一つのフォーマットで共通スキーマ(構造)に格納できれば、ログの活用用途は大

きく広がり、情報としての価値が向上します。この正規化は、XML などの情報に意味付けをできるインターフェースを持つ、ログ出力の共通基盤や変換アダプタという形で実現されます。

■ 監査ログ出力基盤

監査用のログは、その出力時点から改ざん・破壊が行われないよう、その完全性を保証する必要があります。現在はログを出力する各アプリケーションで、ログを守る仕組みを実装しているものがあります。しかし、システムレベルでログを保証するためには、共通のログ出力機能・改ざん防止機能を備えた監査ログ出力基盤が求められます。監査ログ出力基盤には、以下の機能が求められます。

- ログの完全性保証:ログ出力の内容が変更されていないことを保証
- ログ内容の正規化:出力された情報の意味、書式、単位、文字コードを同一基準に変換して保存

ログを正規化して出力するためには、そのフォーマット、スキーマを定義する必要があります。

■ 時刻同期

複数のコンピュータでシステムを構成する場合、各コンピュータの時刻が正確に同期されていないと、コンピュータを跨いだ処理のログ間で関連付けを行うことが困難になります。これを防止するためには、運用において時刻同期を確実に行うことが必要です。時刻同期においては「いつ、どれだけ補正されたか」をログに記録できることも重要です。

■ 監査ログの収集

悪意のある不正アクセス者は、その形跡を消すために監査ログの改ざん・破壊を試みます。このようなリスクに対して、監査ログは安全に保管されている必要があります。多くのログはテキストファイルに追記型で記録されており、改ざん・破壊に対する防御が行われているものは多くありません。そういったログを安全に保管する仕組みが必要となります。

- 問題が発生したシステム上のログはそれ自体の信憑性に問題が出るため、ログは別のシステム上に記録されること
- システムを構成する複数の機能のログが一元管理されていること

収集すべきログは例えば、以下のようなものになります。

- OS のログ UNIX:syslog、 lastlog、 sulog、 pacct 等 Windows:イベント・ログ
- Web サーバ、アプリケーション・サーバのログ
- ネットワーク機器、セキュリティ対策製品のログ(IDS、 Firewall 等)
- クライアントの操作ログ

- データベースの監査ログ
- システムの運用管理ログ

ログの収集には、収集対象サーバに収集エージェントを導入する方法と、エージェント・レスで OS のファイル転送機能（ftp など）や syslog プロトコルでのログ転送を利用する方法があります。一般的に、エージェントを利用する方法では、収集設定の自由度が高く、安全・確実な転送機能を利用できるメリットがあります。

■ 監査ログ管理基盤

各サーバ上に散在するログをサーバごと、アプリケーションごとに収集・管理するのはとてもコストが掛かります。また、監査用情報としての安全・確実な管理にも問題があります。ログは監査ログ管理用のサーバ上に収集し、一元的に管理するべきです。そのためには、あらゆるログ形式に対応し、ログの追加・変更に柔軟に対応できる監査ログ管理基盤を利用することが有効です。

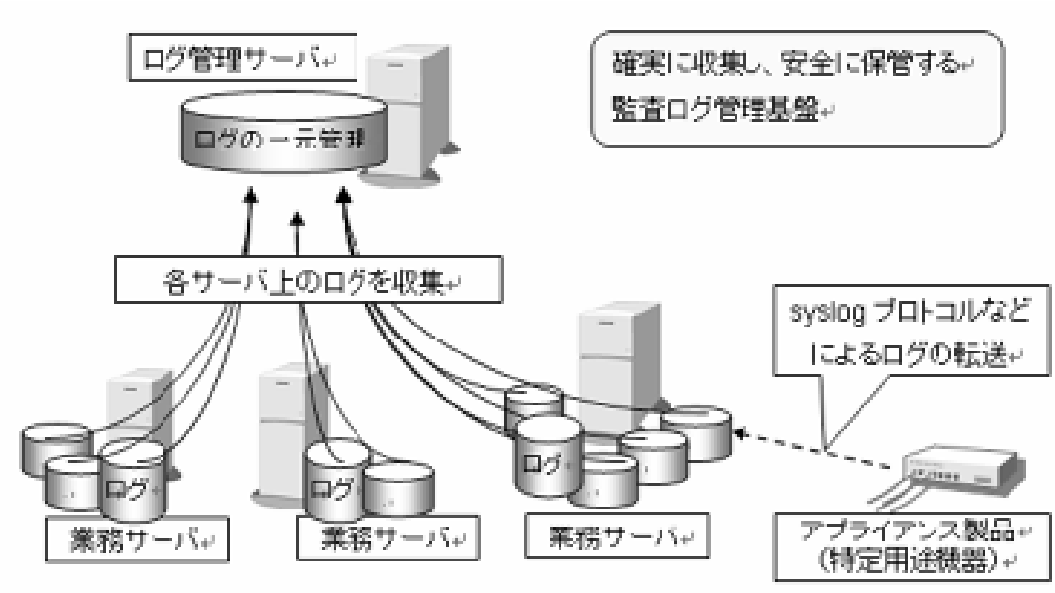


図 7.3-2 ログの管理基盤

■ 監査ログの保管

セキュリティ問題はその発生後すぐに検出されるとは限らず、発生からかなりの時間が経過した後で監査ログの調査が必要になることがあります。そのようなことも考慮して、監査ログを安全に長期間保存する方法を決めておくことも必要です。

ログの保管期間は、最低でも 1 年程度、通常 3～7 年となります。実際には、システム、取り扱う情報、セキュリティポリシー等を考慮して決定し、決められた期間のログを確実に管理・保管する必要があります。

大量・長期間の保管となるため、ログ量を見積もりに応じた余裕のある記憶装置はもちろん、あふれ対策として、外部記憶媒体への退避なども考慮します。

さらに、ログの完全性を確保するためには、書き換え不可能な追記型装置の使用も有効です。また、保管されたログの真正性を保証するためには、ログのハッシュ値をログとは別に保管しておくことが有効です。

■ ログの監査・分析

ログの分析は、セキュリティインシデントや障害が発生したときだけでなく、日常的に行っておくことも重要です。日ごと、曜日ごと、時間帯ごとの処理内容を集計し、傾向を把握しておくことで、普段とは違う事象、すなわち異常の兆候を検出することもできます。こうした分析を定期的に行うことで、システムの状態を監査できます。

ログの監査・分析では、以下のような点も考慮し、セキュリティ管理の PDCA サイクルを回すようにします。

- ログは、セキュリティポリシーに従って定期的に監査し、検出される異常についてアラートを通知すること
- アラート発生時は、関連する複数のログを横通しで分析して事象を追跡でき、インシデント管理システムに登録できること
- ログ分析の結果から監査ルールを更新し、次回の監査時に過去の課題が解決されていること。また、その改善を確認できること

一連の処理を記録した複数のログを関連付けて分析する場合、利用者識別子や要求元IPアドレスがそのキーとなります。そのため、異なる利用者管理システム間の関係情報や、クライアント（操作端末）情報の管理も合わせて行う必要があります。この問題は、ログ分析と統合アイデンティティ管理やクライアント管理との連携で解決します。下図は3階層 Web システムの場合の監査ログの収集・横通し分析のモデルです。

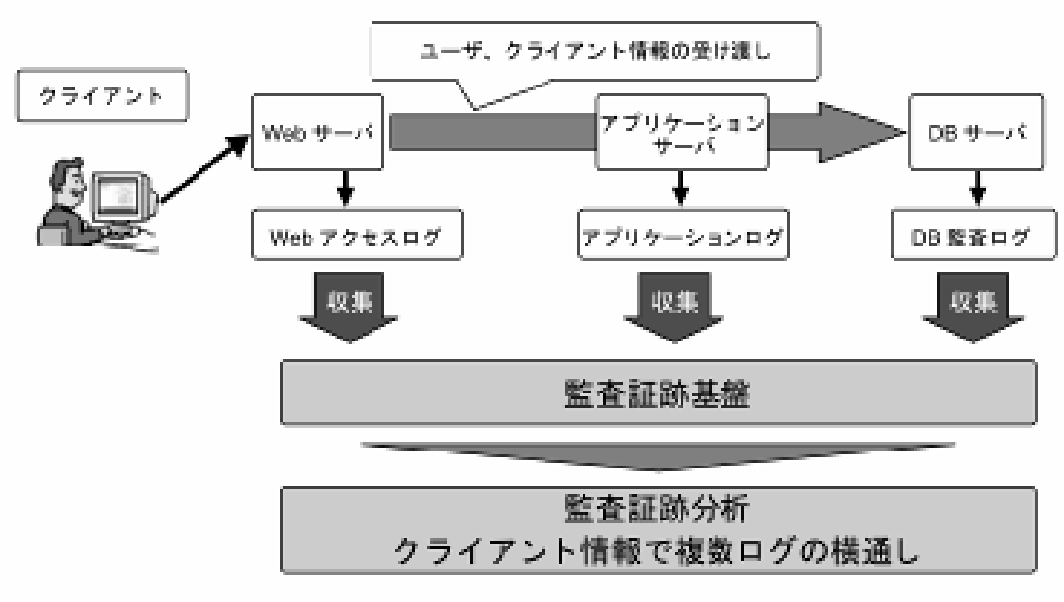


図 7.3-3 監査証跡分析のモデル

その他、ログを分析するために必要な機能として、以下のようなものが挙げられます。

- 特定の条件にマッチするログだけを選択するフィルタリング機能
- 任意の項目を指定して順序を並べ替えるソート機能
- 任意の項目から特定のデータを発見する検索機能（正規表現マッチングなどを含む）
- 特定の条件にマッチするログを除外するクリッピング機能
- 平均値、データ件数などを表示する集計機能
- 複数のログの間の関連を調べる相関分析機能
- 回帰分析、傾向分析などの高度な統計機能

7.4 証跡管理のモデル

本章で説明した証跡管理を構成する機能をまとめたコンポーネント・モデルを、以下に図示します。

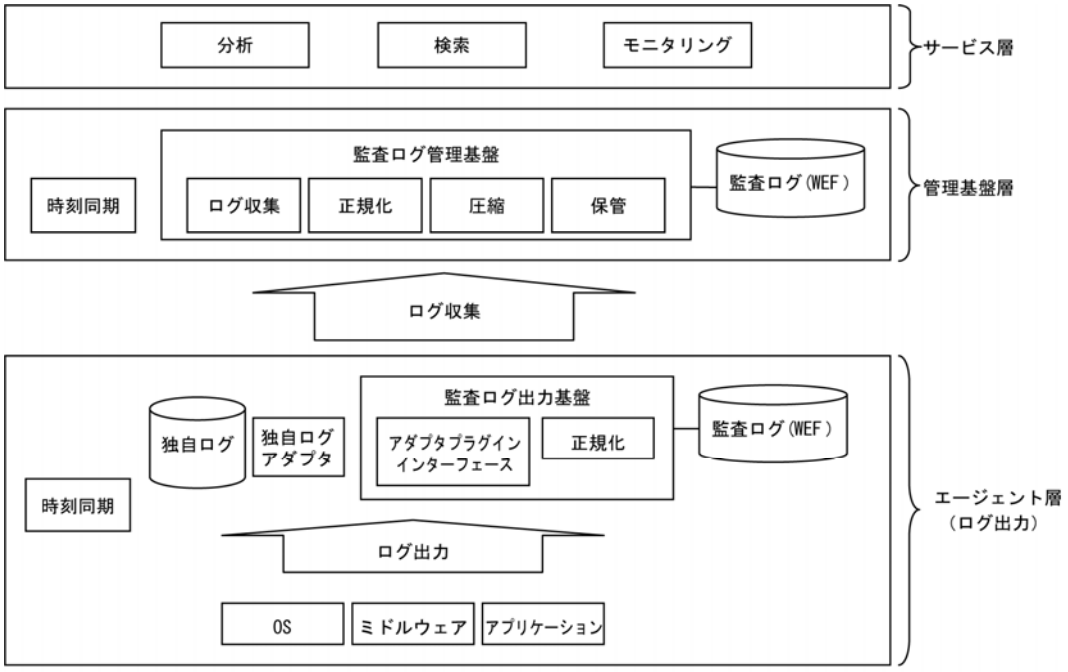


図 7.4-1 証跡管理のモデル

8. 集中管理

8.1 ITIL と集中管理の基礎知識

情報システムの運用管理では、従来、管理対象であるシステム側の視点で管理作業を行っていました。つまり、サーバでならサーバ管理者、ネットワークであればネットワーク管理者、ストレージならストレージ管理者が、それらのライフサイクル（設計、構築、設定、運用、廃棄）を管理していました。また、これらの管理者を支援するためにベンダが提供する運用管理製品も管理対象ごとに存在していました。

しかし、情報システムは、これらの構成要素が相互に関係し合うため、管理対象ごとに独立した管理では、情報システム全体の安定運用が難しく、運用コストも増大してしまうという問題がありました。また、内部統制、IT ガバナンスの実現という要件から、さらに、情報システムごとの最適化ではなく、企業内の情報システム全体の最適化を求める要件が高まっています。こういった背景から、情報システムの運用管理には、企業内で一貫したポリシーに基づいて、運用プロセスを共通化・標準化することが不可欠なのです。この一貫したポリシーに基づいて運用プロセスを共通化・標準化するためのフレームワークとして代表的なものが ITIL（IT Infrastructure Library）[*17] です。ITIL では、インシデント管理、問題管理、変更管理、リリース管理など標準的なプロセスを策定して、情報システム全体で共通の運用管理を行います。これにより、運用コストを最適化し、情報システムの安定稼働・運用品質の向上を実現します。また、運用プロセスの共通化・標準化には、これらのプロセスの中で扱う情報の一元化が必要になります。この情報の一元管理を構成管理、情報を管理するデータベースが、CMDB（Configuration Management DataBase）になります。

また、情報セキュリティや日本版 SOX 法への対応を視野に入れて、企業活動の透明性の確保、業務の効率性、投資効果の評価が必要になります。そのためには、情報システムに対して、いつ、誰が、どんな操作を行ったか、それにより、システムはどう変化したか、などの履歴（情報システムの操作ログ、データへのアクセスログ、システム、アプリの状態遷移、更新のログ等々）を管理すること、業務システムのサービスレベルが確保されていることの管理も必要になります。ITIL では、情報システムの稼働管理、サービスレベル管理、IT サービス管理を規定していますが、さらに、監査証跡管理も必要になります。これらを集中的に管理することがポイントになります。

*17 IL についての詳細は itSMF のサイト http://www.itsmf-japan.org/itil/index.htm を参照

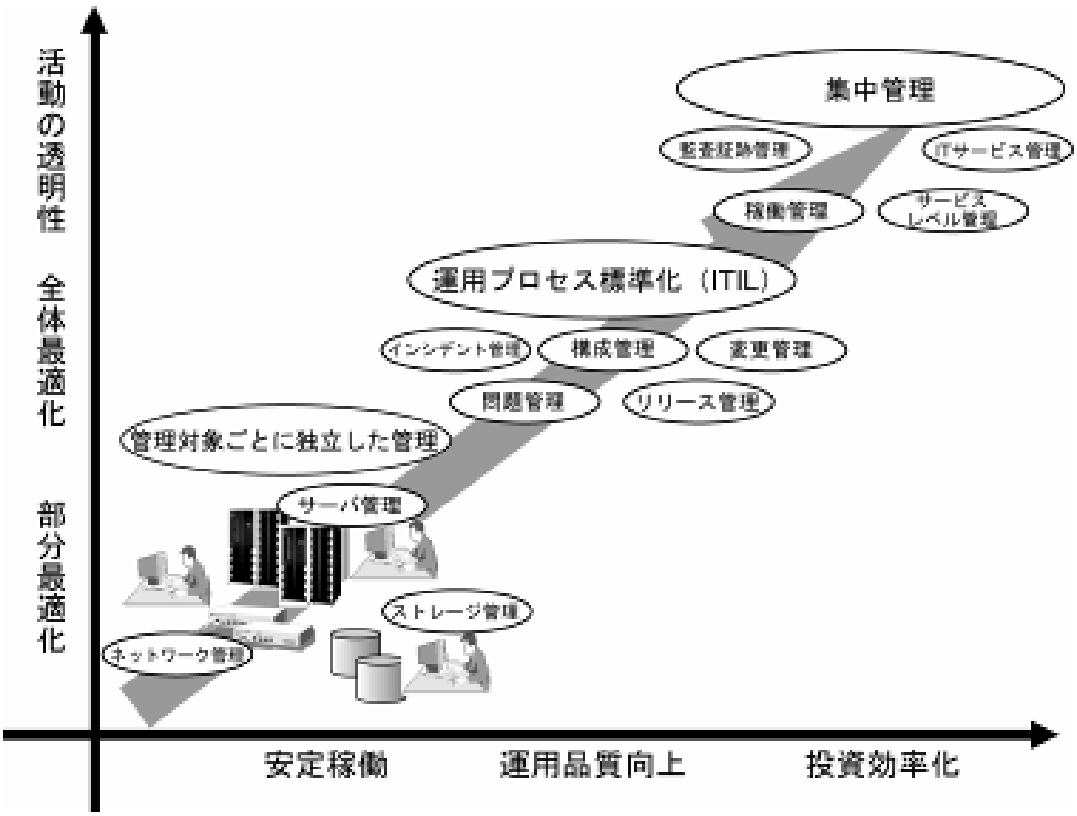


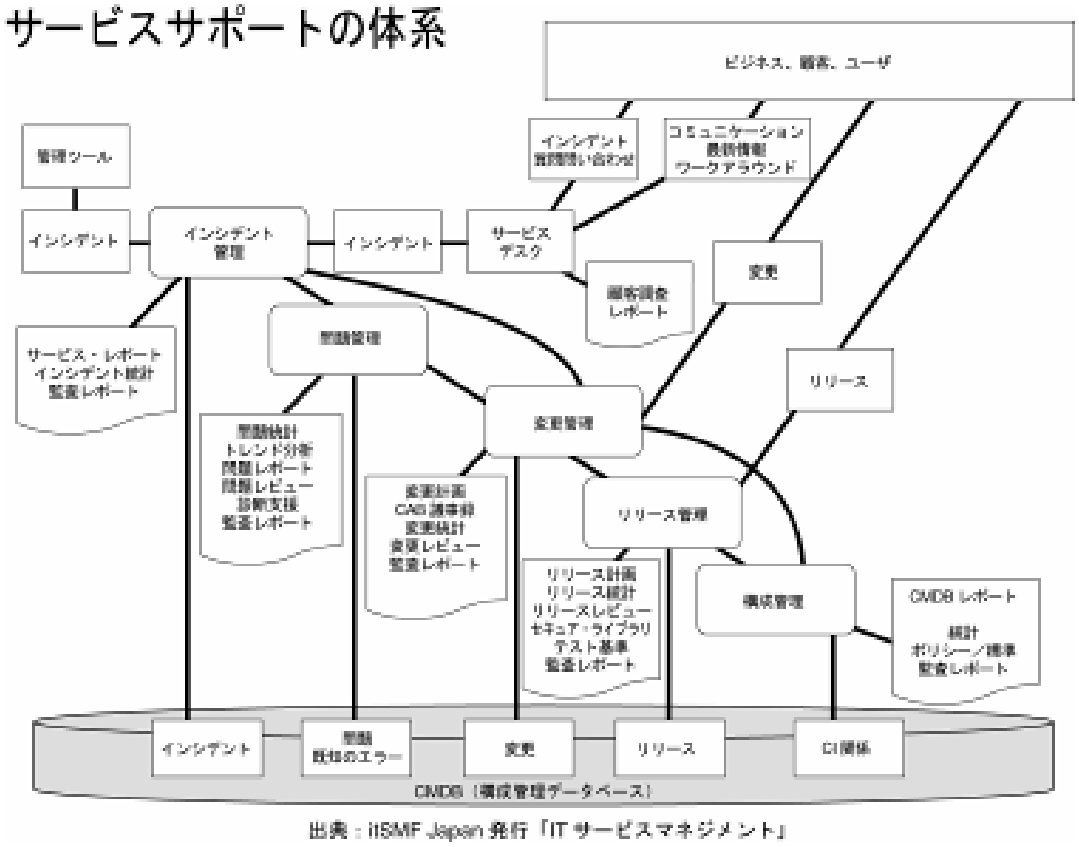
図 8.1-1 集中管理の位置付け

8.2 集中化の概念

情報システムを構成する構成要素であるネットワーク、サーバ、クライアント、ストレージ、アプリケーションなど、それぞれの構成情報・稼働情報・性能情報を管理することは必要不可欠です。ネットワーク管理、システム管理、ストレージ管理、クライアント管理など、管理対象に特化した管理機能が集中管理の中に位置付けられます。次に、これらの構成要素は独立しているのではなく、相互に関連し合ってシステムを構成していますので、管理機能間の相互の関係を管理することが必要になります。集中管理では、これらの管理機能をシームレスに統合するだけでなく、相互の関係の管理と整合性・一貫性を持たせること（管理情報の連携）を行います。情報システムを運用する視点で、情報システムの運用に対する役割・プロセスを共通化・標準化します。共通化・標準化した運用プロセスの計画、実行、評価を管理するフレームワークが、ワークフローの機能を持つ運用プロセス管理です。運用プロセスの中で利用する情報は、プロセス間での整合性・一貫性が必要であり、運用プロセス管理からは、一元的に管理された情報に、必要なときにアクセスすることができます。また、運用プロセスの中で、実際の情報システムへの操作（システムの構成変更や業務アプリケーションの状態切り替えなど）が必要になります。一貫したポリシーで統制された運

用プロセスから一元的に管理されている構成情報を利用して情報システムの制御を行うことで、システム全体の最適な運用を実現できます。

ITIL の言葉で言い換えれば、サービスサポートのカテゴリであるインシデント管理、問題管理、変更管理、リリース管理は、運用プロセスに視点を置いて、登場する人物の役割や作業プロセスを標準化しています。そして、これらのプロセスは、相互に関連しています。これらのプロセス間で利用する情報を一元的に管理するのが、構成管理データベース(CMDB)です。



出典：itSMF Japan 発行「IT サービスマネジメント」

図 8.2-1 サービスサポートの体系

各構成要素に対する管理が、情報システム全体へ及ぼす影響(インパクト)・投資効果を考慮しつつ、情報システムの安定稼働・運用品質の向上を実現してゆくフレームワークになります。

また、サービスデリバリのカテゴリでは、業務の効率性、投資の有効性を把握・分析し、改善・再投資へつなげるプロセスを規定しています。ここでは、情報システム全体のビジネス、投資効果に視点を置いて、業務システムを構成する各要素が有効かつ効果的に稼働して、サービスレベルを維持していることを管理します。

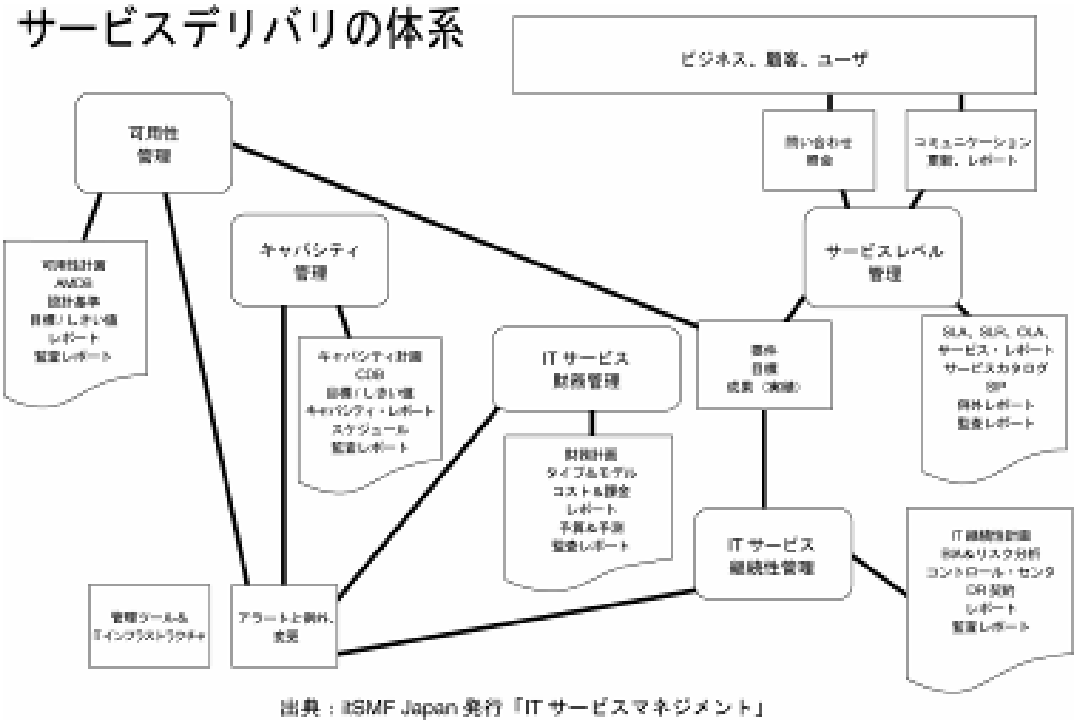


図 8.2-2 サービスデリバリの体系

情報セキュリティガバナンスの実現に当たっては、規定した役割・プロセスが確実に実施されていることや、想定したサービスレベルを満たしていることを証明できる情報をレポートします。そのためには、製品やツールの整備だけでなく、プロセス、情報、インターフェースを体系化したスキーマが必要です。

従来のネットワーク管理、システム管理、ストレージ管理、クライアント管理の機能は、運用プロセスから利用できるようにその管理機能を SOA 化して、構成管理（CMDB）で管理する個々の構成要素が持つ機能として利用できるように連携します。

8.3 インシデント管理、問題管理

インシデント管理は、情報システムの安定稼働、トラブル発生時の早期復旧を目的として、情報システムに対する問題（インシデント）への対処を行うプロセスです。インシデント管理においては、インシデントの受付、復旧、調査、改善など役割・作業プロセスを明確にして、対処状況のみえる化や対処結果のノウハウの一元管理が求められます。以下に、典型的なインシデント管理の流れを示します。

表 8.3-1 典型的なインシデント管理の流れ

（1）	**インシデントの受付** **（インシデント発行）インシデントには、情報システムの利用者からの指摘、情報システムの運用管理ツールからの通知などによる要求がありますが、窓口は一本化して、一元的に管理します。**
（2）	**分類・切り分け** **発生している事象からインシデントの原因・復旧方法を切り分けます。**
（3）	**解決と復旧** **過去の事象や現象を分析して、問題の解決、情報システムの復旧を行います。**
（4）	**インシデントの記録** **対処方法、復旧確認などを記録してインシデントをクローズします。**
（5）	**インシデントの分析** **定期的に発生したインシデントの分析を行い、情報システムの評価、問題点の改善を行います。**

ITIL では、インシデント分析などから来る問題点の改善を問題管理として、長期的に改善するプロセスとして区別していますが、これらは一連の作業プロセスになります。

インシデントの分類には、情報システムの不具合や操作ミスなどさまざまですが、情報セキュリティガバナンスの視点では、企業で設定したセキュリティポリシー（例えば、ウィルス対策、ファイアウォールの侵入検知など）の違反に対するインシデントを確実に監視して、対処することが求められます。これらを検知するために、複数のベンダからさまざまな製品やサービスが提供されており、これらを組み合わせて運用しているのが現状です。しかし、このような状況では、一貫したセキュリティ対策が難しくなります。さまざまなセキュリティ事象を統合的に管理するツールの導入が効果的です。セキュリティ事象には、不正アクセス検知、ウィルスの発見、機密情報の漏洩が挙げられます。統合管理ツールとインシデント管理を連動させることで、一貫性があり効率的なセキュリティインシデントの検出が可能になります。以下に、インシデント管理を支援する運用管理の位置付けを示します。

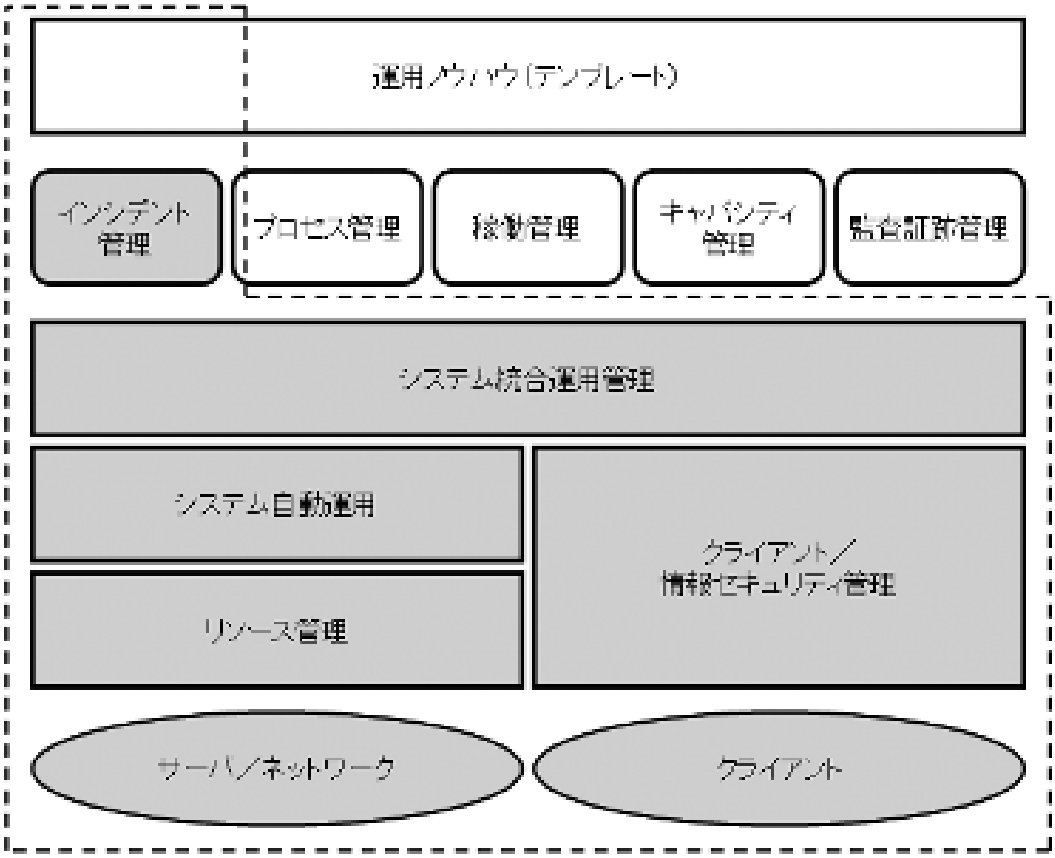


図 8.3-1 インシデント管理の位置付け

情報システムを構成するサーバ、ネットワーク、クライアントなどの異常(メッセージ)、稼働状態、性能をそれぞれの監視機能で監視し、情報システム全体として、統合運用管理が集約します。

統合運用管理では、あらかじめ設定したルールに従って、インシデント管理ツールへ通知します。

インシデント管理は、通知されたインシデントに対して、復旧・調査・対処などのプロセスを支援しますが、必要に応じて、統合運用管理と連携して構成情報や性能情報などの参照を行うことで、迅速な対処が可能になります。また、インシデント管理の作業で行った操作や履歴は、ノウハウとして蓄積できますので、分析や改善に活用する事ができます。

8.4 変更管理、リリース管理

変更管理とは、情報システムに対する各種の変更作業の予定および実績を管理することです。例えば、アプリケーションの変更は、それに伴うサーバ、ストレージの変更、変更における運用への影響などを考慮して進める必要があります。従って、変更を行うに当たっては、変更要求の申請書(Request For Change; RFC)を作成して、変更のインパクト・効果を分析してから実施します。以下に、典型的な変更管理の流れを示します。

表 8.4-1 典型的な変更管理の流れ

(1)	変更申請書(RFC)の作成 変更理由、内容などを管理票に記入します。
(2)	影響調査(インパクト分析) 変更計画の妥当性／投資効果などを分析します。
(3)	変更計画書の作成 影響調査結果、変更のスケジュール・手順を作成します。
(4)	変更計画の承認 関係する部門も含めて変更計画を検討し、実施の可否を判断します。
(5)	変更計画の事前検証 計画書に沿ったリハーサルを実施します。
(6)	変更計画の実施 計画書に沿って変更作業を実施します
(7)	実施結果の確認 計画どおりの変更が実施されたことを、計画と結果を比較して監査します。

ITIL では、(5)以降は、リリース管理という呼び方で変更管理とは区別していますが、これらは一連の作業プロセスになります。

情報セキュリティガバナンスの実現においては、このプロセスの中で、変更作業により、セキュリティレベルに悪影響を及ぼさないように、(3)のプロセスは、セキュリティレベルへの影響調査、(4)では、調査結果による判断、そして、(7)では、実施結果の監査を行うことが必要になります。また、内部統制の実現においては、これらの変更作業が確実に実施されたことを作業ログとして収集して監査できることが求められます。以下に、変更管理を支援する運用管理の位置付けを示します。

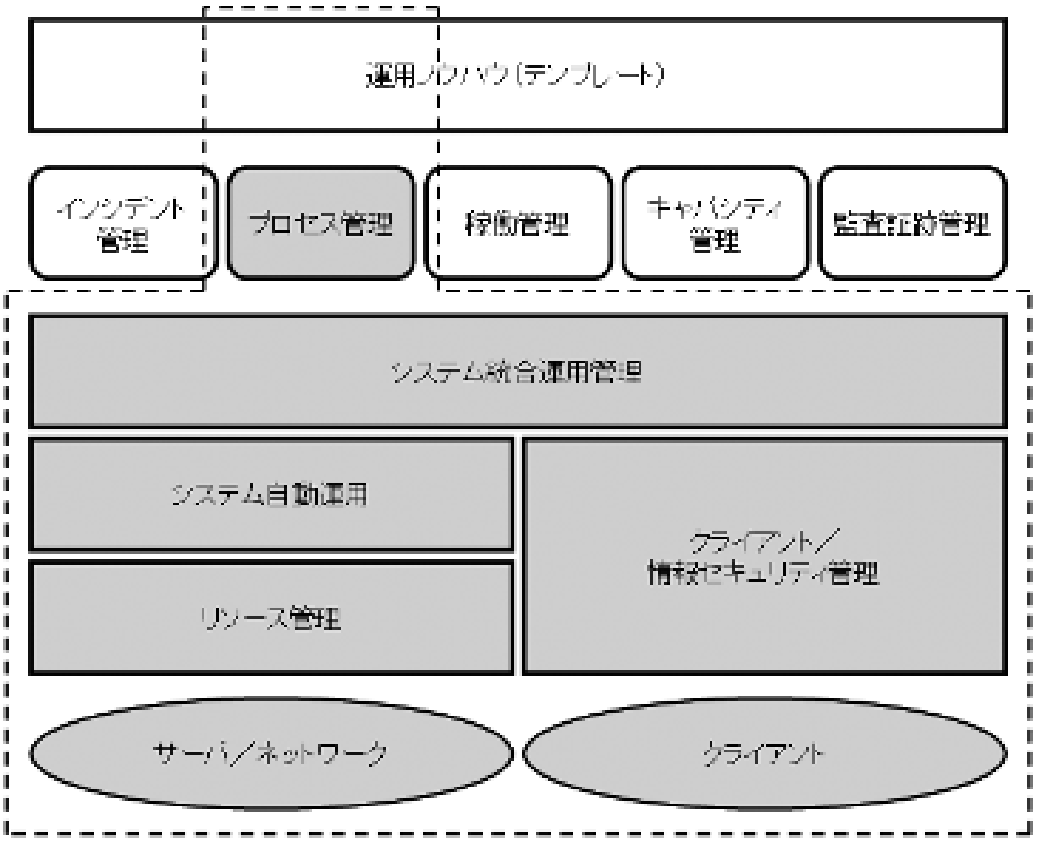


図 8.4-1 変更管理の位置付け

運用プロセス管理では、計画した変更プロセスに従って一連の作業を管理し、計画どおりの実行、作業の記録を行います。変更プロセスの中の、システムへの操作、システムの変更は統合運用管理やシステム自動運転と連動して行います。これにより、作業漏れ、確認漏れ、操作ミスを防止できます。また、プロセスの進行状況や実施結果の履歴を管理する機能を提供します。

8.5 集中管理のアーキテクチャー

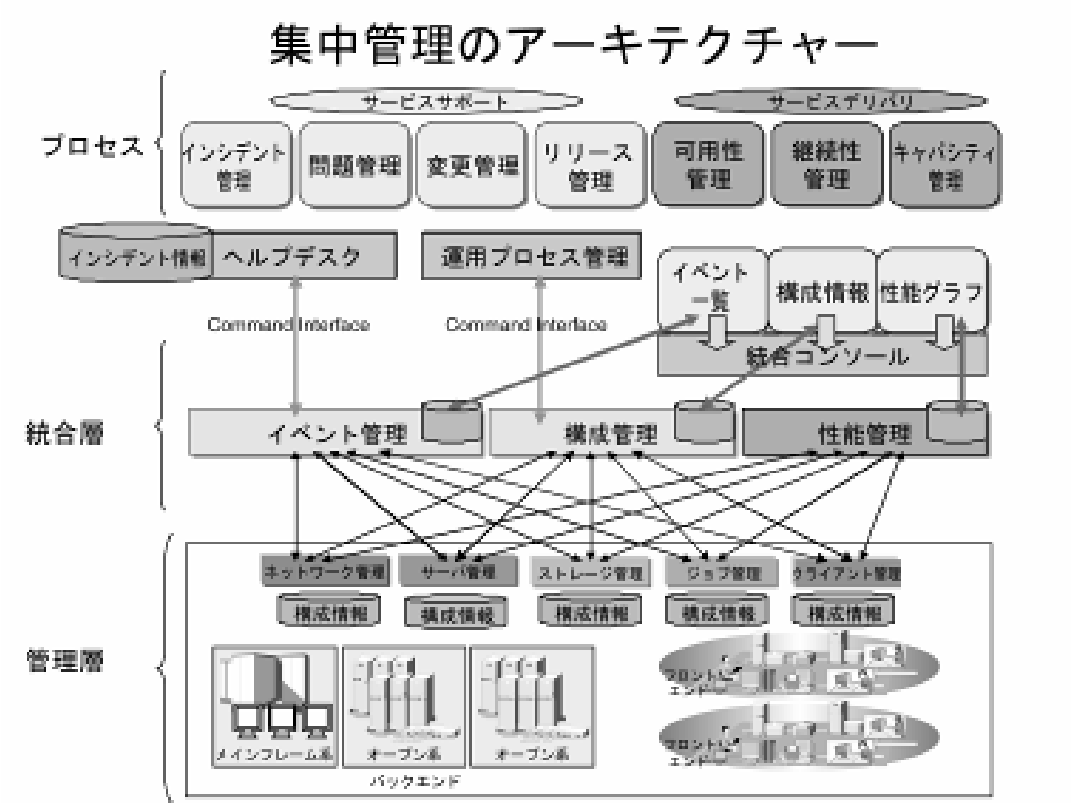


図 8.5-1 集中管理のアーキテクチャー

管理層は、情報システムを構成する個々の資源を管理する機能群です。情報システムのバックエンドには、ネットワーク、サーバ、ストレージなどがあり、それぞれの資源に対して、これらを管理する管理機能が必要です。ネットワーク管理、サーバ管理、ストレージ管理などがそれに当たります。これらは、管理対象の特性に合った管理機能を提供します。フロントエンドには、クライアント PC やエンドユーザが利用する情報があります。そして、それらのライフサイクルを管理するクライアント管理の機能が必要です。

統合層は、情報システム全体のライフサイクル管理では、複雑化する管理機能を統合して管理します。「イベント管理」では、それぞれの資源およびそれらを管理する機能が出力したイベントを統合して、一括して把握できるようにします。また、発生した事象をインシデント管理ツールへ自動的に通知することができます。

「構成管理」では、情報システムを構成するさまざまな資源の情報を統合して、情報システム全体が俯瞰できる構成を表示します。すべての構成資源の詳細な情報まで表示することは不可能であり、詳細な情報は、必要時に、それぞれの管理機能の詳細なビューをドリルダウンして表示します。変更管理のプロセ

スの中では、変更前後に実システムから収集した構成情報と変更計画(RFC)の情報をチェックすることで、その品質を評価します。

「性能管理」では、個々の資源の性能情報と情報システム全体で見た性能情報を評価することで、システム全体のサービスレベルの評価、ボトルネックの検出に利用します。

8.6 次世代の集中管理アーキテクチャー

次世代の集中管理について紹介します。以下に、次世代集中管理の全体像を示します。

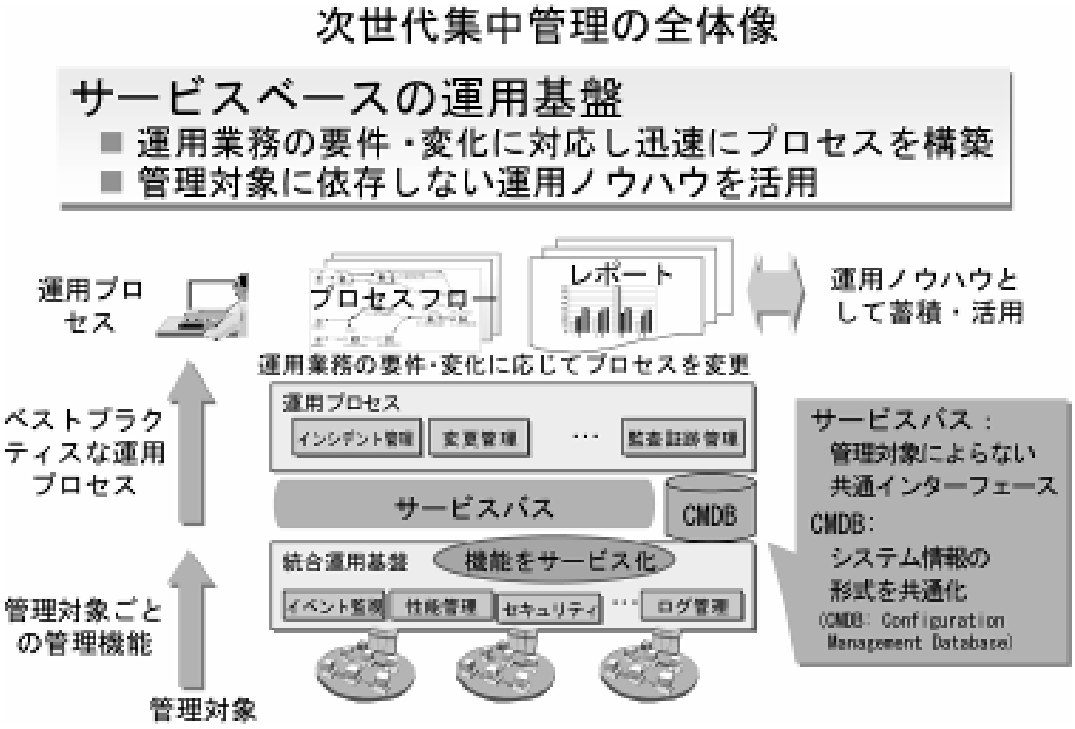


図 8.6-1 次世代集中管理の全体像

上位の運用プロセスおよび情報連携を効率的かつリアルタイムに実現するために、管理対象ごとの機能をサービス化します。これにより、必要なときに、適切な機能・情報へアクセスできるようになります。これらのサービスをサービスバスで連携し、情報は共通の形式(CMDB)として管理します。これにより、上位の運用プロセスにおいては、必要な機能や情報が適切な形で利用できることになり、運用プロセスの連携がスムーズになります。

次に、次世代集中管理のアーキテクチャーを示します。ITIL のプロセスを実現するためのアーキテクチャーを、三つのレイア(層)に分けます。

表 8.6-1 次世代集中管理のアーキテクチャー

(1)	管理層(Element Manager) 管理対象ごとの機能を提供するネットワーク管理、サーバ管理、ストレージ管理、ジョブ管理、クライアント管理などです。単独で存在するのではなく、共通の CMDB に管理される構成情報に対して、Web Services のインターフェースで機能を提供します。
(2)	統合層(Manager of Managers) 管理層の機能と情報を統合して、共通のスキーマを使って関係を管理します。構成管理(Federated CMDB)もこの層に入ります。管理層および ITIL 層の機能間を Web Services のインターフェース(Enterprise Service Bus)でつなげるために、管理層および ITIL 層が管理する情報および提供する機能とそのエンドポイントを管理します。全体で整合性の取れた共通のスキーマで関係を管理するので、一元的に管理することができ、必要な情報や機能にアクセスすることができます。共通のスキーマを利用することで、他ベンダの管理ツールやお客様が独自に作成した管理ツールも統合可能になります。また、スキーマを拡張することで、業務の管理やビジネス管理の情報も統合できます。
(3)	ITIL 層(Service Management Toolset) 運用プロセスを管理するためのツール群です。インシデント管理のためのヘルプデスク機能、運用プロセスを管理するワークフロー機能(運用プロセス管理)、情報システムの状態や各種情報を表示するビュー、分析機能(ダッシュ・ボード)が位置付けられます。

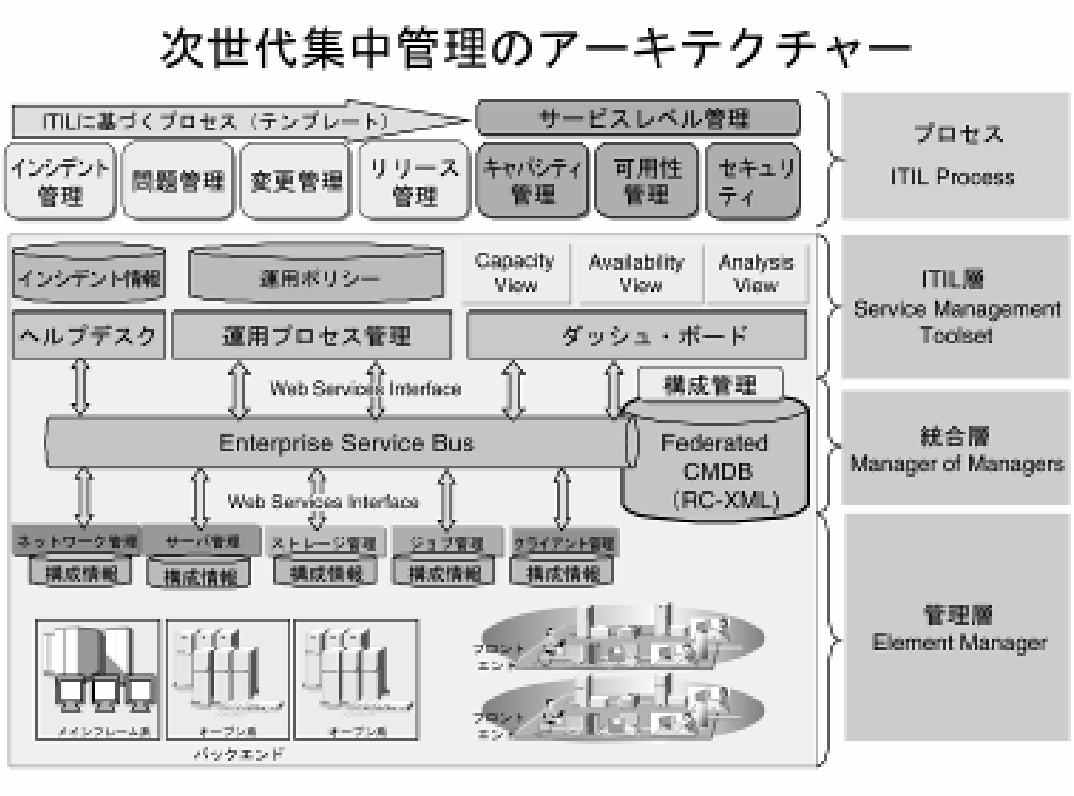


図 8.6-2 次世代集中管理のアーキテクチャー

8.7 資産管理

資産管理とは、企業が IT 資産として保有するクライアント PC、サーバ、ネットワーク機器、ストレージ機器などのハードウェアおよびこれらの上で動作するソフトウェアの資産について購入計画から稼働状況、廃棄までのライフサイクルを一元的に管理することで、ライセンスの稼働率や IT 投資効果を評価するプロセスです。以下に、典型的な資産管理のプロセスを示します。

表 8.7-1 典型的な資産管理の流れ

(1)	資産購入計画を立てる 目的に合わせて資産の購入計画を立てます。
(2)	購入計画を承認する 目的・投資効果などから購入計画を検討、承認します。
(3)	導入・構築する 購入した資産の導入・構築を行います。
(4)	利用状況を収集する 資産の利用状況の監視、情報収集を行い、購入した資産の活用を評価します。
(5)	資産を廃棄する 減価償却した資産を確実に廃棄します。

資産管理の情報は、システム管理者だけでなく、経理担当者、部門の情報担当者など、多方面の関係者がそれぞれの役割・視点で活用できることが求められており、一元的に管理することが求められます。

情報セキュリティガバナンスの視点では、違法コピー対策、ウィルス対策、セキュリティ対策といった目的で利用できることが必要です。ライセンス管理では、違法コピー対策として、購入したライセンス数と稼働しているライセンスの数が同じであることが証明できます。また、資産の償却という観点で、購入したライセンスが計画どおりに償却・廃棄されるまでの管理も行います。さらに、PC を廃棄するときには、ハードディスク内のデータを完全消去すること、消去したことを記録することも重要です。

特に、ソフトウェア資産では、運用中に、ウィルス、セキュリティ対策が必要になりますが、利用者(エンドユーザ)任せでは、確実に実施できず、問題が後を絶たないのが現状です。ウィルスパターンやセキュリティパッチの適用は、集中的に管理して、確実に適用できる仕組み、および結果を証明できる仕組みが必要になります。

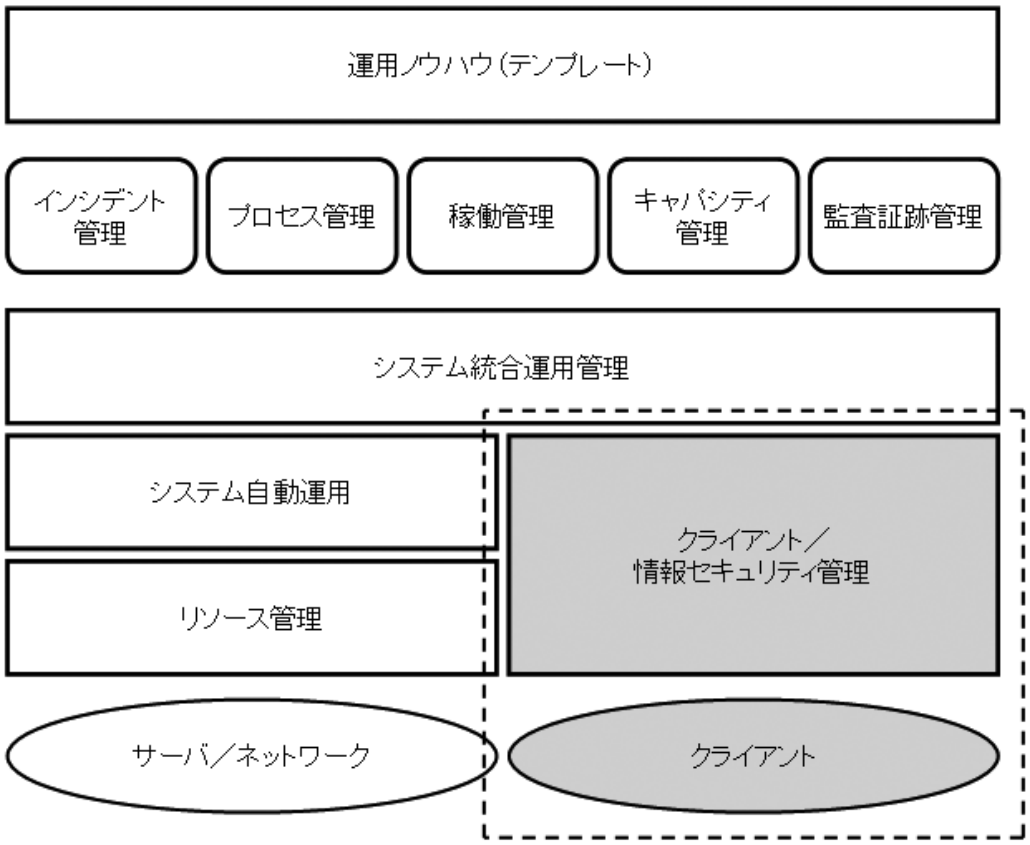


図 8.7-1 資産管理の位置付け

クライアント管理では、PC クライアントに対して、計画から破棄までのライフサイクル、クライアント PC 上のソフトウェア資産を管理する機能を提供します。また、これら PC クライアント情報資産に対する情報セキュリティを管理する機能を提供しています。

8.8 統合セキュリティ管理（運用管理システムとの連携）

システムの運用管理とセキュリティ管理は密接に関係しており、両者のモニタリングを統合して管理するべきです。運用管理とセキュリティ管理の統合効果として考えられる例を、以下に挙げます。

- セキュリティ管理製品で検出したアラートを運用管理のコンソールへ通知し、システム全体のモニタリング事象を一元的に管理する。

  通知手段としては、以下の方法が考えられます。

  - 運用管理システムが持つイベント通知コマンド／API による通知
  - SNMP トラップによる通知
  - イベントログ／Syslog に出力するメッセージの監視
  - ログファイルに出力するメッセージの監視
- 運用管理コンソールへ通知されたセキュリティ管理製品のアラートに対して、リモートコマンドの発行、自動アクションの設定。
- 運用管理コンソールで表示されているイベントやシステム構成部品から、関連するセキュリティ管理製品のコンソールを起動する。

この統合セキュリティ管理のコンポーネントモデルを、下の図に示します。

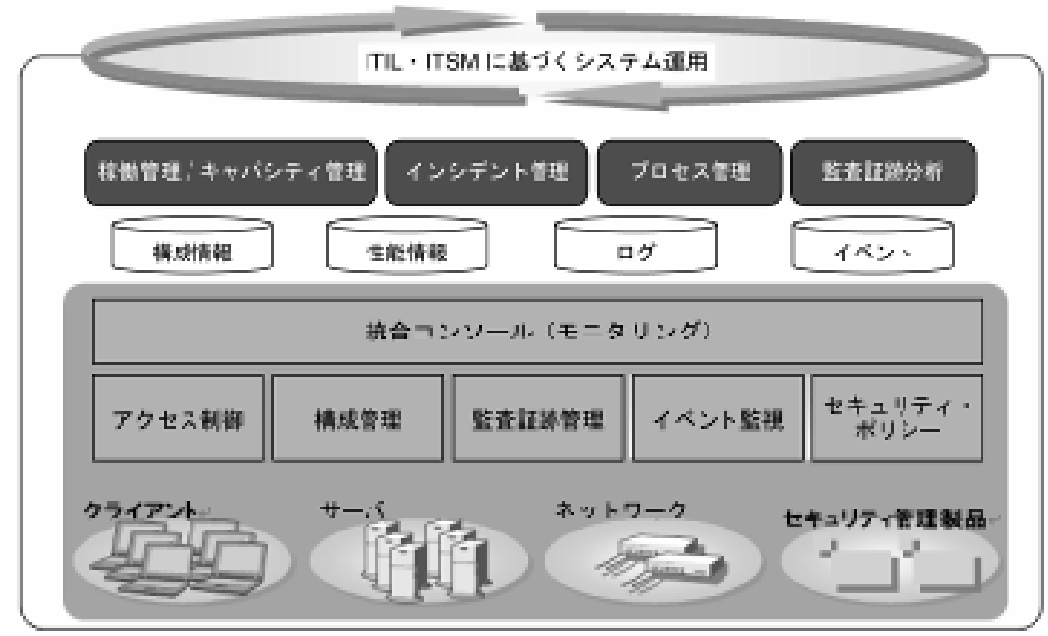


図 8.8-1 統合セキュリティ管理のコンポーネントモデル

9. 暗号

9.1 暗号技術

暗号技術の目的は、情報の秘匿(暗号化)と認証に大別されます。秘匿のための暗号化には、暗号化と復号の鍵が同じ鍵である共通鍵暗号と、暗号化と復号の鍵が異なる公開鍵暗号とがあります。前者は大容量データの暗号化など高速な処理に適していますが鍵の共有が難しく、後者は処理速度が低速ですが、一方の鍵を公開できるため鍵共有の必要がないという利点があります。実用に際しては2者を組み合わせたハイブリッド暗号を用いることが一般的です。認証については、共通鍵系の MAC(Message Authentication Code)や公開鍵系の電子署名を用いる方式があります。

以下に、それぞれの概念図を示します。

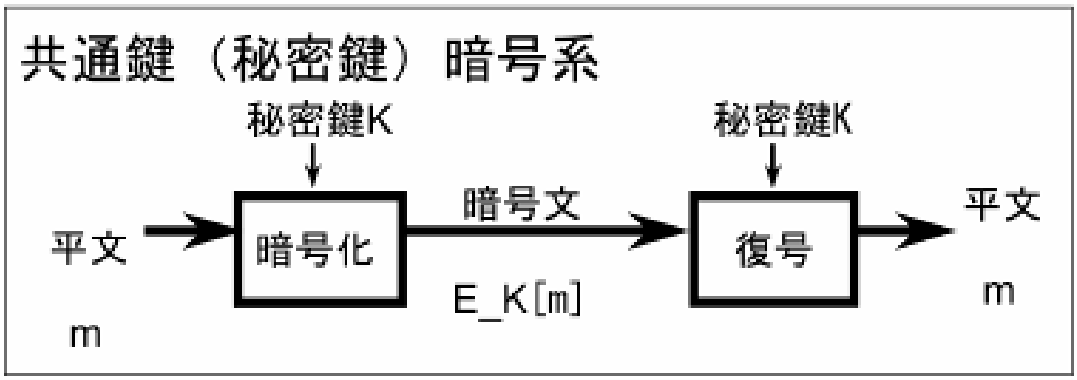


図 9.1-1 共通鍵暗号系

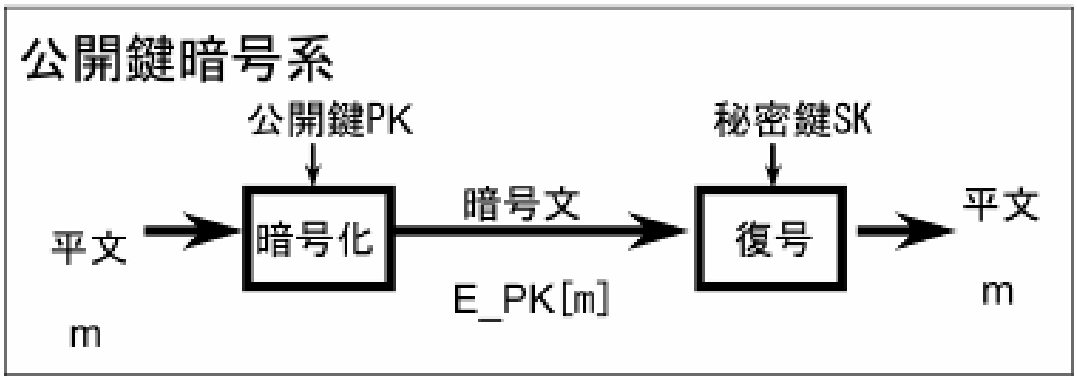


図 9.1-2 公開鍵暗号系

暗号アルゴリズムの強度は、暗号鍵の長さが長いほど強くなります。しかしながら、鍵が長くなればそれだけ処理速度が低下します。従って、アプリケーションにより、必要な暗号強度と処理速度とのバランスを取る必要がありますが、あらゆる局面において最低限必要な暗号強度の目安が必要であると考えます。アルゴリズムの種類により、同じ鍵長が必ずしも同じ強度とはならないため、統一的な基準として「セキュリティのビット長」により、暗号強度を表します。今後十分な安全性を確保するためには、「セキュリティのビット長」が 80 ビット以上である必要があります。

9.2 標準化

日本国内では、2000 年度～2002 年度に総務省および経済産業省の主導により、電子政府推奨暗号アルゴリズムが制定されました。このプロジェクトでは、公開鍵（秘匿・署名・鍵共有・認証）・共通鍵・ハッシュ関数・擬似乱数の各用途向けアルゴリズムを公募し、国内外一線級の暗号学者により評価を行いました。この報告は CRYPTREC のサイト[*18]で公開されています。

米国では、長らく標準であった DES（Data Encryption Standard）の後継を決めるコンテストを NIST が主催して行い、2000 年に共通鍵ブロック暗号の AES（Advanced Encryption Standard）が制定されました。欧州では産学による評価プロジェクト NESSIE が行われ、各種用途の暗号アルゴリズムが 2002 年に選出されました。

国際標準の世界では、ISO/IEC18033[*19]において、ストリーム暗号、ブロック暗号、公開鍵暗号、ハッシュ関数が国際標準化されています。

9.3 共通鍵暗号

共通鍵暗号は、暗号化と復号の鍵が同じ鍵の暗号アルゴリズムであり、一般にデータの暗号化など高速な処理に適しています。現在、最もよく使用される暗号は、米国の暗号標準である AES、および TDES（Triple DES）です。

AES は、128 ビット入力に対し、128 ビットの暗号文を出力する暗号関数です。鍵は、128（AES-128）、192（AES-192）、および 256 ビット（AES-256）のいずれかを選択できます。TDES は、64 ビット入力に対し、64 ビットの暗号文を出力する暗号関数です。鍵長は、112 ビット 2TDES（2-key TDES）および 168 ビット

*18 http://www.cryptrec.org/
*19 ISO/IEC 18033-1:2005 Information technology -- Security techniques -- Encryption algorithms -- Part 1: General など

3TDES（3-key TDES）のいずれかを選択できます。AES は、安全性が評価されており、全数探索（総当たり攻撃）以上に有効な攻撃法は発見されていない（「セキュリティのビット長」＝「鍵のビット長」）ため、特に問題のない場合は、AES の使用を推奨します。TDES は、一世代前の暗号アルゴリズムですが、相互接続性を重視すると現在でも実用的です。ただし、2TDES は、全数探索（総当たり攻撃）以上に有効な攻撃法が見つかっており、その安全性は、「セキュリティのビット長」が 57 ビット相当に落ちる場合があるため、相互接続性が必要などの理由により AES が使用できない場合を除いては、使用すべきではありません。3TDES も、「セキュリティのビット長」が 112 ビット相当に落ちる場合があるため、同様です。

その他、さまざまな暗号アルゴリズムが提案され、製品化されていますが、第三者の評価のない暗号アルゴリズムやアルゴリズムが未公開の暗号の使用は、一般的には推奨できません。また、公開アルゴリズムに対し高速化や小型化のために一部改変を行うことは暗号の安全性の想像以上の低下をもたらす可能性があるため、やるべきではありません。改変する場合は、暗号の専門家に相談が必要です。

安全性評価を行った結果、発表されているものとしては、国内では、CRYPTREC で選択された電子政府推奨暗号があります。欧州でも NESSIE Project に選抜されたリストが公表されています。さらに、2006 年に ISO/IEC 18033 で暗号アルゴリズム国際規格が制定されています。これらに記載されているアルゴリズムは、現在のところ安全性の問題は発見されていないと考えられます。暗号アルゴリズムの利用に当たっては、これらの中から選択すべきです。AES は、いずれのリストにも掲載されています。

なお、AES 暗号、および TDES については、ライセンスフリーとなっています。公表されている安全なアルゴリズムの中には、ライセンスが必要なものがあるので、使用に当たっては確認が必要です。

9.4 公開鍵暗号

公開鍵暗号は、暗号化と復号の鍵が異なる暗号アルゴリズムであり、一般に暗号鍵の暗号化やデジタル署名などに用いられます。公開鍵暗号は、大きく分けて 3 種類あります。RSA（Rivest-Shamir-Adleman）暗号などの素因数分解の困難さを安全性の根拠としている方式（Integer Factorization Cryptography; IFC）、DSA（Digital Signature Algorithm）や DH（Diffie-Hellman）など有限体上の離散対数問題の困難さを安全性の根拠にしている方式（Finite Field Cryptography; FFC）、および ECDSA（Elliptic Curve Digital Signature Algorithm）など楕円曲線上の離散対数問題の困難さを安全性の根拠としている方式（Elliptic Curve Cryptography; ECC）です。

公開鍵暗号の安全性は、一般に鍵が長くなればなるほど安全となりますが、反面、長い鍵を使用すると処理速度が落ちます。FFC と IFC は、同じ鍵長ならほぼ同じ安全性ですが、ECC は、より短い鍵で同じ安全性を実現できます。NIST Special Publication 800-57（次頁表参照）によると、1024 ビット鍵の FFC の安全性は、160-223 ビット鍵の ECC の安全性と同程度であると考えられています。

RSA 暗号解読の世界記録は、現在 663 ビットであり、768 ビットも射程圏内に入ってきたと考えられます。近年、RSA 暗号解読専用ハードウェアの脅威が懸念されていましたが、実装実験に基づいた安全性評価では、理論で言われているほどの脅威になる可能性は低いという結果が出ています。今後 RSA 暗号で十分な安全性を確保する場合には、1024 ビット以上の鍵を使用する必要があります。DSA、DH に関しても同様です。ECC 解読の世界記録は、現在 109 ビットであり、今後 ECC で十分な安全性を確保する場合には、160 ビット（「セキュリティのビット長」は 80 ビット）以上の鍵を使用する必要があります。安全な鍵長についての詳細は、「9.6 暗号鍵長の考え方」を参考にしてください。

一般的には、RSA の使用を推奨します。暗号化、署名ともに使用できますし、ソフト／ハードのライブラリも選択枝が多いためです。なお、RSA 暗号については、基本特許は、すでに期限が切れており、DSA については、米国が特許を保有しておりライセンスフリーです。楕円曲線暗号については、権利を主張している企業があるため、利用に当たってはライセンスの要不要について確認をする必要があります。

9.5 輸出規制

暗号を含んだ製品は、日本の輸出規制の対象となります（署名は、対象でないことに注意）。輸出相手国、適用製品、鍵長などにより、必要な手続きが異なります。暗号を含んだ製品を輸出する場合は、関係機関、部署に確認が必要です。

9.6 暗号鍵長の考え方

強度(「セキュリティのビット長」)を同程度とした場合の暗号の鍵長の比較表を下記に示します。(NIST Special Publication 800-57 の 63 ページ Table2)。ただし、これらは、計算機の発達や暗号理論の進捗により変化します。現在の技術での比較表です。

表 9.6-1 強度比較

セキュリティのビット長	共通鍵暗号	FFC (DSA,DH 等)	IFC (RSA 等)	ECC (ECDSA 等)
80	2TDES	L=1024 N=160	k=1024	f=160-223
112	3TDES	L=2048 N=224	k=2048	f=224-255
128	AES-128	L=3072 N=256	k=3072	f=256-383
192	AES-192	L=7680 N=384	k=7680	f=384-511
256	AES-256	L=15360 N=512	k=15360	f=512+

L:FFC の公開鍵長、N:FFC の秘密鍵長、k:IFC の鍵長、f:ECC の鍵長

一般的には、共通鍵暗号の鍵を公開鍵暗号で暗号化して配送する場合、共通鍵暗号より強い公開鍵暗号で暗号化する必要があるといわれています。この原則によると、AES-128 の鍵は、FFC3072 ビット以上の鍵で暗号化する必要があることになります。公開鍵暗号は、鍵が長くなると鍵生成のための時間や処理時間が長くなるので、現在は、この表のとおりには実装されていません。

実際の適用に当たっては、米国政府向けの推奨アルゴリズムと最小鍵長の関係を示した下表「表 9.6-2 推奨アルゴリズムと最小鍵長」[*20] が参考となります。この表は、例えば 2005 年にデータを暗号化する場合に、そのデータを 2015 年まで暗号化するなら TDES は推奨しないという意味です。この場合は、公開鍵暗号も 1024 ビット RSA 暗号ではなく 2048 ビット RSA 暗号が推奨されます。

*20 出典: NIST Special Publication 800-57 66p. Table4

表 9.6-2 推奨アルゴリズムと最小鍵長

アルゴリズムセキュリティのライフタイム	共通鍵暗号（暗号と MAC）	FFC（DSA,DH 等）	IFC（RSA 等）	ECC（ECDSA 等）
2010 年まで （80 ビット以上の強度）	2TDES 3TDES AES-128 AES-192 AES-256	L=1024 N=160 以上	k=1024 以上	f=160 以上
2030 年まで （112 ビット以上の強度）	3TDES AES-128 AES-192 AES-256	L=2048 N=224 以上	k=2048 以上	f=224 以上
2030 年以降 （128 ビット以上の強度）	AES-128 AES-192 AES-256	L=3072 以上	k=3072 以上	f=256 以上

L：FFC の公開鍵長、N：FFC の秘密鍵長、k：IFC の鍵長、f：ECC の鍵長

9.7 ハッシュ関数

ハッシュ関数は、任意長の長さを固定長に圧縮する関数です。圧縮された値をハッシュ値といいます。セキュリティで用いられるハッシュ関数は、現在、米国標準（FIPS180-2）で 4 種のハッシュ長が決められています。SHA-1、SHA256、SHA-384、および SHA-512 で、ハッシュ値は、それぞれ 160 ビット、256 ビット、384 ビット、および 512 ビットとなります。現在は、SHA-1 が多く用いられています。そのほか、欧州で開発された RIPEMD- 160 や Whirpool などがあります。

ハッシュ関数に関しては、2004 年 8 月以降、新しい研究成果が発表されるなど安全性に関する研究が急速に進んでいます。現在、SHA-1 の衝突耐性に関する安全性は「セキュリティのビット長」が 61～62 ビット相当程度に落ちている（当初は 80 ビット相当）と考えられており、今後十分な安全性を確保する場合には、ハッシュ値が 224 ビット（「セキュリティのビット長」は 112 ビット）以上のものを使用する必要があります。

9.8 暗号アルゴリズムの危殆化への対応

暗号アルゴリズムが研究されることにより、設計時に想定したものよりも簡単な方法で暗号を解読できるようになることがあります。このような状況を危殆化と呼びます。危殆化した暗号アルゴリズムは設計上の強度が保証されないので、速やかに別のアルゴリズムに切り替える必要があります。何らかの理由で暗号アルゴリズムやハッシュ関数が危殆化したり、ある鍵長以下での安全性が低下し、延長しなければならない場合に、暗号アルゴリズムや鍵長を変更することができるスキームをあらかじめ決定しておかなければなりません。

9.9 暗号スキーム

現代の暗号技術は、最も強力と考えられる「適応的選択暗号文攻撃」（Adaptive Chosen Ciphertext Attack）に対しても、いかなる部分情報も漏らさない（Semantic Security）ことが要求されます。最も原始的な暗号アルゴリズム（プリミティブ）だけではこの要求を満たせないため、これを補う技術として考案されたものが暗号プリミティブのスキーム化です。暗号スキームは暗号プリミティブをベースにして、ある仮定のもとでの安全性を保証します。すなわち、暗号の安全性を困難と考えられている問題（例えば、素因数分解問題）の困難性に帰着します。暗号を解くことができれば、困難と考えられている問題が解けることを示すことにより、暗号の安全性を主張する方式であり、証明可能安全性（provable security）と呼ばれています。

10. 鍵管理

10.1 基礎知識

暗号鍵は、暗号やデジタル署名を行うために最も安全に管理を行わなければならない対象です。鍵管理の目的は、必要な暗号処理を行う場合にそれらに必要な鍵の使用をコントロールすることです。また、鍵の生成から破壊までのライフサイクルにわたって、その安全性が確保されていることが確認できることです。より正確な定義の例として、例えば、FIPS140-2 には「セキュリティポリシーに従った、鍵要素の生成、登録、証明、登録抹消、配送、インストール、保存、保管、廃止、 導出および破壊の管理および使用」と定義されています。

金融機関向けやスマートカード向けには鍵管理の国際標準や、暗号鍵を守りつつ必要な暗号処理を行う暗号モジュールについてのセキュリティ要件などの基準が存在しますが、一般には、ある鍵管理が妥当かどうかは、必ずしも基準があるわけではなく、セキュリティポリシーや適用するシステムにより異なってきます。

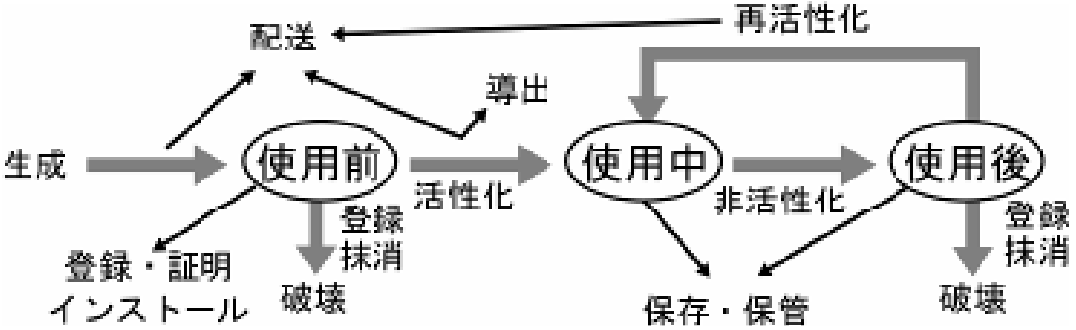


図 10.1-1 鍵のライフサイクル

具体的な鍵管理の原則の参考として、小売店でのバンキングシステムに対する規格[*21]を示します。

1) 平文の秘密／プライベート鍵に対して一人でアクセスや確認ができてはならない

2) システムは、データを現在保護していたり、将来保護する可能性のある秘密／プライベート鍵の漏洩を防がなくてはならない

3) 秘密／プライベート鍵を生成する場合に、その値を予想できてはならない

*21 ISO 11568-1:2005 Banking -- Key management (retail) -- Part 1: Principles 他

4) システムは、秘密／プライベート鍵の危殆化や意図した目的以外の使用への試みを検出しなければならない

5) システムは、その目的以外の秘密／プライベート鍵やその一部の使用、および偶然や許可されない鍵の変更、使用、置き換え、削除、挿入を防ぎ、検出しなければならない

6) 鍵は、利用期限までに、次に使用する新しい鍵に変更しなくてはならない

7) 鍵は、古い鍵で暗号化されたデータの辞書攻撃が成功すると推測される時間以前に新しい鍵に変更しなくてはならない

8) 鍵が危殆化した場合、あるいはそれが疑われる場合には、利用をやめなければならない

9) あるグループで共有している鍵が危殆化した場合でも、それによって他のグループの鍵が危殆化してはならない

10) 危殆化した鍵は、その鍵の替わりに利用する鍵について、いかなる情報も与えてはならない

11) 鍵は、それを格納するデバイスが、適度に安全であり認証されない改ざんや置き換えができないと確認できた場合にのみ格納されるべきである

10.2 鍵のタイプと関連情報

暗号システムで用いられる鍵は、暗号用や署名用など使用目的(タイプ)が決められます。また、暗号アルゴリズムや鍵に関するドメインパラメータや初期ベクトルなどの関連情報があります。具体的な鍵のタイプや鍵関連情報をまとめたものとして SP800-57 や ISO/IEC11770 があります。例えば、データの暗号化に用いる鍵であるデータ鍵や、データ鍵を暗号化する鍵暗号化鍵などが鍵のタイプとなります。

一般的には、一つの鍵は、決められたタイプ、すなわち一つの目的のために使用すべきであり、複数の用途に適用すべきではありません。一つの鍵を複数用途で使用するとセキュリティが低下します。例えば、データを暗号化するときは、鍵暗号化鍵(データ鍵を暗号化するための鍵)を使用すべきではありません。平文が知られているデータに対して鍵暗号化鍵で暗号化してはいけません。

10.3 鍵の生成

鍵の生成は、安全な乱数生成関数を用いて作成しなければなりません。乱数は、第三者が予想できないこと、および、ある関数出力からその前後の値が予想できないことが要件となります。

乱数の生成方式として、擬似乱数と呼ばれる乱数の種データから乱数系列を出力する関数を用いる方法と、熱雑音などの物理的性質を用いる物理乱数と呼ばれるものがあります。いずれの場合も、必要な乱数の検定を通ることが基本となります。擬似乱数を用いる場合は、種データが第三者から予想できないようにしなければなりません。また、乱数生成を利用する場合は、運用時にも乱数生成関数が正常に動作しているかどうかの検定を行うなど、ヘルスチェックの仕組みを考慮しておかなければなりません。

暗号に用いる乱数生成関数とその検定については、ISO/IEC18031 や ANSI X9.82 で標準化されているので、それらを参照すべきです。擬似乱数生成の関数には、ハッシュ関数や公開鍵暗号で用いるアルゴリズムを用います。共通鍵暗号を用いて擬似乱数生成関数を構成する方法もあります。ANSI X9.17 Annex C に記述されている方法で、乱数を種と時刻情報であるタイムスタンプを更新しながら乱数を生成します。X9.17 は、3DES ベースで記述されていますが、AES や他のブロック暗号でも使用することができます。これらの乱数生成は、共通鍵暗号、公開鍵暗号ともに鍵生成に利用することができます。簡易な乱数生成法として知られている合同乱数法や線形フィードバックレジスタを用いた M 系列などは、安全でないため、暗号／署名で用いる鍵の生成に使用してはなりません。

■ 共通鍵暗号の秘密鍵生成

共通鍵暗号の鍵は、上記乱数生成関数を用いて生成すべきです。

■ 公開鍵暗号の鍵生成

公開鍵暗号の場合は、まず乱数生成を行い、必要な条件を満たすパラメータかどうかの検定を行います。公開鍵暗号の鍵生成は、IEEE P1363 の Annex A や FIPS186-3 の Appendix 3 に掲載されている方法を参考にすべきです。

RSA 暗号の鍵生成で必要な素数の生成については、Miller-Rabin テスト（IEEE P1363A.15、ANSI X9.80 参照）を用い、DSA や ECDSA を用いる場合は、FIPS186 の方法を採用すべきです。また、RSA 暗号の鍵生成については、強い乱数という言い方で特殊な形をした素数を避けるように生成を要求される場合があります。この場合は、ポックリントン法などが適しています（ANSI X9.80 5.2.4.1.2 参照）。

楕円曲線暗号で用いられる楕円曲線パラメータは、FIPS186-3 や ANSI X9.31 などの標準に記載されているものを使用すれば安全性に問題はありませんが、独自で生成する場合は、CM 法よりスクーフ法を用いるのが安全性の観点から望ましいといわれています。

なお、鍵の生成は、第三者による改ざんや置き換え、または盗難が起きないような安全な領域で行わなければなりません。具体的には、暗号モジュールといわれる耐タンパーモジュールであるハードウェア内部で行うことが望ましいとされています。ソフトウェアで生成する場合は、少なくともアプリケーションから鍵は利用できても、生成した鍵が直接参照できないように実装する必要があります。

10.4 鍵配送

暗号鍵の安全なシステム間の移動については、鍵ローディングデバイスを用いて手動で行う場合と、自動で電子的に配送プロトコルを用いて行う方法があります。基本は、自動鍵配送とすべきです。

SSL/TLS や IPsec でも鍵配送のための自動の鍵配送プロトコルが標準化されています。IPsec の場合は、手動の鍵設定ではなく、自動で鍵配送を行う ISAKMP/Oakley の使用を基本とすべきです。これらは、公開鍵暗号と第三者からの証明書を用いて信頼できる鍵配送を行う手法です。

共通鍵暗号における信頼できる第三者機関を用いて行う方法もあります。これは、Kerberos がよく知られています。

新規に独自で自動の鍵配送プロトコルの設計を行うことは、避けるべきです。それぞれのプロトコルについて、なりすましや再送攻撃への耐性、あるいは、鍵失効時の対応等検討すべき多くのことがあるからです。どうしても必要な場合は、ISO/IEC11770 シリーズなどに記載されている従来ある鍵配送の方式をベースに検討すべきです。また、セキュリティ専門家に相談すべきです。

10.5 安全な鍵の保管

安全な鍵の保管の要件として、正当な利用者しか該当する鍵の入力、操作、置き換え、および削除ができないことが挙げられます。また、保管場所や保管方法を最小限にとどめることも必要です。

一般的に、安全な鍵の保管のためには、ハードウェアが用いられる場合が理想的ですが、ソフトウェアで行う場合には、アプリケーションからは鍵は見えず、該当する鍵の操作だけが見える API を準備して処理を行います。このような API として PKCS#11 が知られています。

ハードウェアについては、論理的に鍵を守る方法と同時に、物理的な攻撃への耐性が必要になってきます。一般的な暗号モジュールについての要件としては、FIPS140-2 やこれをベースとした ISO/IEC 19790 が知られています。認証局のルート鍵を守るためには、FIPS140-2 のレベル 3 相当以上のセキュリティレベルが要求されます。

これらの機能要件のほかに、実装における脆弱性がある場合、安全に保管しているつもりでも、鍵が取り出せる場合もあります。WEB アプリケーションの脆弱性を突いた攻撃や、IC カードの場合でも電磁波攻撃やフォールト攻撃、およびそれらが複合した攻撃手法が開発されており、採用に当たっては、これらの耐性も含めて安全性の評価を行う必要があります。

10.6 鍵のバックアップ

バックアップや鍵の移動のために鍵を保管する暗号モジュールにアクセスする場合は、Split Knowledge と Dual control の原則を適用すべきです。すなわち、一人だけの権限ではなく複数人の認証がないと処理が行えないようにします。また、安全な領域でない鍵の取り出しは、一人がすべての（暗号化した）鍵の情報を持つのではなく、分散して管理する必要があります。このためには、秘密分散法が用いられます。例えば、5 つのピースに秘密鍵を分散し、そのうち任意の 3 ピースが集まれば元の鍵が復元できる方法です。

10.7 鍵の更新と破棄

鍵の更新とは、暗号強度や漏洩の危険性から、ある鍵の使用を中止し、別の鍵を使い始めることを言います。暗号の鍵については、公開鍵暗号、および共通鍵暗号ともに、データ鍵なのか、鍵暗号化鍵なのかなど鍵のタイプにより、鍵を利用する期間を決めることができます。

一般的に、ある鍵で暗号化したデータが第三者に入手される量が多ければ多いほど、解読される可能性は、高くなると考えられます。よって、その鍵の利用頻度や暗号化／復号、および署名したデータの量やそのデータの性質により、鍵の更新期間が決まってきます。一般的な、鍵のタイプと利用期間の考え方については、SP800-57 の 5.3.6 節を参照ください。

近年の e 文書法に対応するための電子化された文書の安全な保管のためには、長期にわたるデータの署名鍵やタイムスタンプの鍵の更新も含めて、鍵の更新についてあらかじめそのスキームを決定してお

かなければなりません。また、暗号アルゴリズムと同様に、何らかの理由で鍵、あるいはその一部が漏洩した場合に、安全に鍵を置き換えるためのスキームをあらかじめ決定しておかなければなりません。

鍵を破壊するときは、完全に消去しなければなりません。具体的には、例えば複数人によって、鍵の格納された暗号モジュール内の暗号鍵を完全に初期化、あるいは物理的に破壊します。同時に、バックアップしている鍵に関しても同様の手続きによって破棄します。なお、鍵を消去した場合は、それまで暗号化したデータが復号できなくなるため、それらの対処の方法についても決めておく必要があります。

10.8 鍵管理のアーキテクチャー

現在、アプリケーションごとに個別に行われている鍵管理を、システム全体で整合性のとれたものとするためのアーキテクチャーが今後必要となってきます。それには、利用されるシステム形態、扱う情報の重要性、さらに、鍵のライフサイクルの観点から検討しなければなりません。

鍵の安全性を高めるための基本的な考え方は、鍵を管理・運用するために高い耐タンパー性を持った暗号モジュールと呼ばれる専用ハードウェアを安全性の起点として、そこに格納されているマスター鍵を基本に鍵管理システムを構成することです。これらを実現するためには、幾つかの観点からの検討が必要です。

■ 複数の暗号モジュールを 1 ヵ所に集める暗号鍵の集中管理

現在、安全性を求められるアプリケーションにおける鍵管理では、サーバ単位で暗号モジュールに鍵を格納し、それを信頼点としてシステム全体で使用する鍵を体系化し、集中管理することによりシステム全体の鍵管理を行っています。しかし、この方式だと鍵管理の手間が大きいため、今後は、個々のサーバでの鍵管理を統合し、鍵管理を集中的に行うアーキテクチャーが必要になると考えられます。個々のアプリごとの鍵管理を統合することにより、扱う情報の重要性に応じた鍵の適切な統合管理の実現が可能となります。

■ 一つのサーバ内上の複数の VM を一つの暗号モジュールで管理

今後、VM によるサーバ統合が行われる場合に、安全な鍵管理のために一つのサーバ上に複数の VM での鍵管理を一つの暗号モジュールで統合管理するアーキテクチャーが必要となると考えられます。

■ クライアント PC 上の個別のアプリケーションの鍵管理を統合

クライアント PC の個別アプリケーションで使用する鍵をオンラインで接続した鍵管理センターで集中管理することにより、企業における不用意な鍵の漏洩を防ぐシステムが構築されます。現在、認証のために PKI やケルベロスのようなインフラが提供されていますが、今後はさらに、クライアント PC におけるファイル暗号や SSL、IPsec などで使用されるマスター鍵を適切に集中管理することにより、企業システムの安全性を高めるアプローチがとられると考えられます。

■ 各組み込み端末などすべてのユーザ機器に安全な鍵管理のための仕組み

ユーザが使用する携帯電話や組み込み機器などに暗号モジュールが搭載され、すべての処理、通信が安全に実行されます。これらの機器は、顧客の個人情報や機密情報が格納される可能性も高く、また、企業内の業務システムとの連携が行われると考えられます。一方で紛失や故障させてしまう可能性も高いため、必要な情報をより厳格に運用管理していく必要があります。これら端末における秘匿・認証のための鍵管理のためのアーキテクチャー（例えば Trusted Platform Module;TPM など）が必要となると予想されます。

11. フィジカルセキュリティ

11.1 フィジカルセキュリティとは

フィジカルセキュリティには、基準・規約等による明確な定義はありません。さまざまな基準の中では、情報資産を保護する観点から記載されています。広義の意味では、情報資産が設置されている建築設備、電気設備、空調設備、防災設備までを含んでいます。

それに対し、情報セキュリティでは、「職務の分離」を実施し、それぞれの職務に対するセキュリティ対策を実現しています。フィジカルセキュリティは、鍵、カード、生体認証、映像等を利用してファシリティインフラの侵入防御手段として構築されています。本書では、フィジカルセキュリティは、人や情報資産を守るセキュリティ対策として、情報セキュリティと融合し、多層防御の思想に基づき企業資産全体のセキュリティ対策を実現するものと定義します。

また、日々進歩する技術に対し、構築したセキュリティが危殆化し、当初のセキュリティレベルの維持管理が困難になる可能性があります。フィジカルセキュリティにおいても認証、アクセスコントロール、証跡管理、集中管理による PDCA サイクルを構築し、日々改善しながら発展していく必要があります。

11.2 フィジカルセキュリティに求められる要件

フィジカルセキュリティにおいても、その要件は、大きくエンタープライズセキュリティアーキテクチャーの体系に分類して定義することができます。

以下、それぞれの機能分類について示します。

■ 認証・アイデンティティマネジメント

フィジカルセキュリティにおける識別は、四つの要素があります。

- 「人」が知っている知識である ID、パスワード情報
- 「人」が持っている ID 情報（IC カード等）
- 「人」に属する情報（生体認証等）
- 機器に属する情報（セキュリティチップ）

フィジカルセキュリティは、これら要素を利用形態に応じて組み合わせることで、より確実なセキュリティを実現します。情報セキュリティと同様に認証は、ID、パスワードによって行います。ID を使ってアクセス

できるゾーンの設定を行い、「人」や「モノ」の管理を行うために、それらを識別する必要があります。生体認証データは、ID データやパスワードデータとして位置付けられ、IC カードや生体認証を組み合わせて本人確認を行う必要があります。

フィジカルセキュリティにおいて認証を行うためには、利便性やコストを考慮した設計・運用などが重要となります。特に利便性では、入退室管理システムと業務アプリケーションの連携やアイデンティティマネジメント(ID 統合管理)の導入などが考えられます。

フィジカルセキュリティでの認証の基本は、ID とパスワードの組み合わせですが、より高いセキュリティレベルを目指す場合には、唯一性の高い生体情報を使用した、生体認証装置と組み合わせるなど、複数要素による認証を導入します。生体認証方法には、幾つか方法がありますが、最近は、識別精度が高いことから、静脈認証の採用が増加しています。

11.3 アクセスコントロール

フィジカルセキュリティにおけるアクセスコントロールとは、人がどのエリアに入ってよいのかのゾーニング設計を基に、人のアクセスを識別し、コントロールすることです。また、アンチパスバック機能に代表される入室した「人」しか退室できない認証を行い、共連れを防止することなどもアクセスコントロールの機能であり、特にお客様の情報を扱っている部門などにおいては、高いアクセスコントロールが必要となります。

図 11.3-1 アクセスコントロールの設定例

11.4 証跡管理

内部統制の実施とその検証のためには、監査のためのログが正しく記録されていることが重要です。フィジカルセキュリティでは、識別・認証の記録として「人」や「モノ」の入退場の履歴を管理します。それらのログを収集し、保管し、分析する仕組みが必要となります。なりすましや、しかるべき手順を通って入場してこない者のログを映像などで一元管理します。また、情報セキュリティのアクセスログと合わせて管理することで、「人」の出入の履歴とネットワークへのアクセスログを含めた「人」の動作の証跡を追跡できることが必要です。

11.5 集中管理

フィジカルセキュリティにおける集中管理は、対象項目が多岐にわたります。セキュリティ統制の実現には、代表的な管理項目例として、以下を考えます。

部屋の増設やレイアウト変更、またセキュリティレベル変更に伴う設定変更などによる構成変更に対応し、最新の構成情報を管理する「構成管理」。

フィジカルセキュリティの事件・事故に備え対応計画を準備するとともに、発生した場合には迅速に対処を行う「問題管理」、「インシデント管理」。

また、従来、認証状況やアクセス状況、映像情報を個別に管理しているケースが大半でしたが、今後は、監査証跡のデータ量が膨大かつ複雑になることから、トータルに管理できる機能が、運用を効率良くかつ確実に行うために必要となります。

その他として、映像による不審物の監視、機器の監視などや、重要施設においては、危機管理システム（コンティンジェンシプラン）との連携も考えておくことを推奨します。

11.6 考慮すべき要求セキュリティ仕様

フィジカルセキュリティの構築には、IT ネットワーク上の見えない「人」ではなく、脅威にさらされている施設、情報資産の前にいる「人」の視点から要件を整理する必要があります。以下に、フィジカルセキュリティを実現するために考慮すべき事項について紹介します。

■ フィジカルセキュリティレベルの設定

事業を行う施設の中で、どのような「人」が活動し、どのように動くかを考慮しながら、企業におけるセキュリティポリシーを勘案し、各ゾーンにセキュリティレベルを設定します。執務する従業員の業務内容および設置されている資産の重要性を含めて、レベルごとにセキュリティ対策（Layerd Security）を設定します。

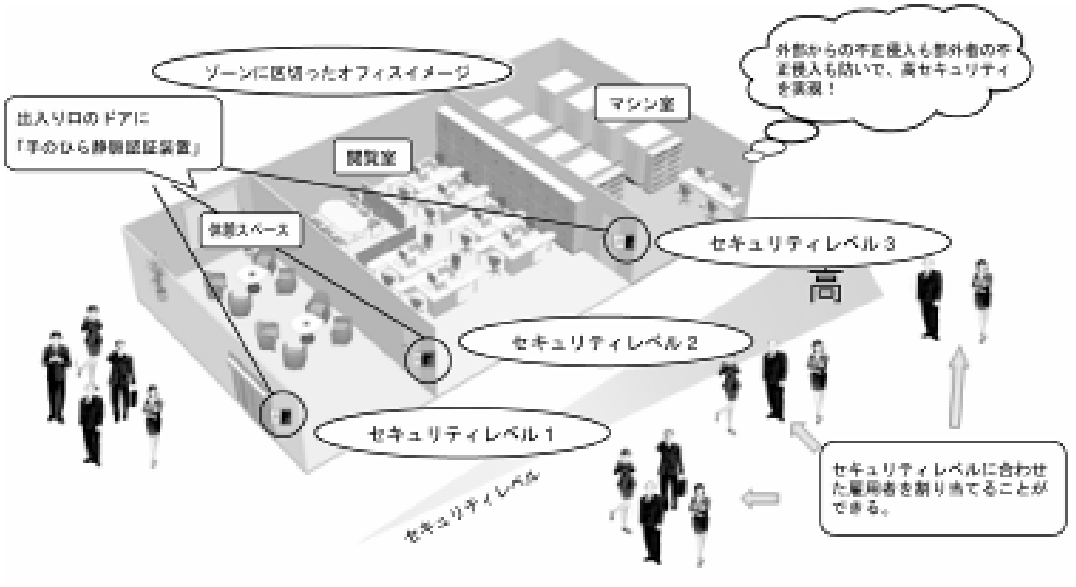


図 11.6-1 セキュリティレベルの設定例

セキュリティレベルは、レベルが高くなればなるほど機密性が高いエリアとなります。しかし、施設内では、自然災害や事故等による火災等が発生した場合、避難路を確保するためにセキュリティレベルを開放しなければなりません。その際は、ネットワークアクセスの遮断を全館で実施する等の IT へのセキュリティを維持しながら、各ゾーンセキュリティが開放されることを考慮しておく必要があります。

■ 動線計画とゾーニング計画

動線計画は、証跡管理の基本となる計画です。想定されるすべての人員に対し、人の動きを設定する必要があります。また、「人」の識別・認証の結果ログによる動作履歴を管理することで、不審動作を把握する必要があります。

さらに、動線計画を実行できるよう、ゾーンごとにセキュリティレベルを設定し、段階的にゾーンを移動することができるようにします。隣接するゾーンは、一段階異なるゾーンとなるよう設定します。

■ 情報システムとの連携

フィジカルセキュリティシステムと情報システムが連携することで、強固なセキュリティを確保することができます。ただし、組み合わせるためには、データの管理方法、同期方式に注意しなければなりません。

フィジカルセキュリティにおける識別、認証、許可、ID 管理は、統合アイデンティティマネジメントシステムを構築することで情報システムと連携することができます。このイメージを、次の図に示します。

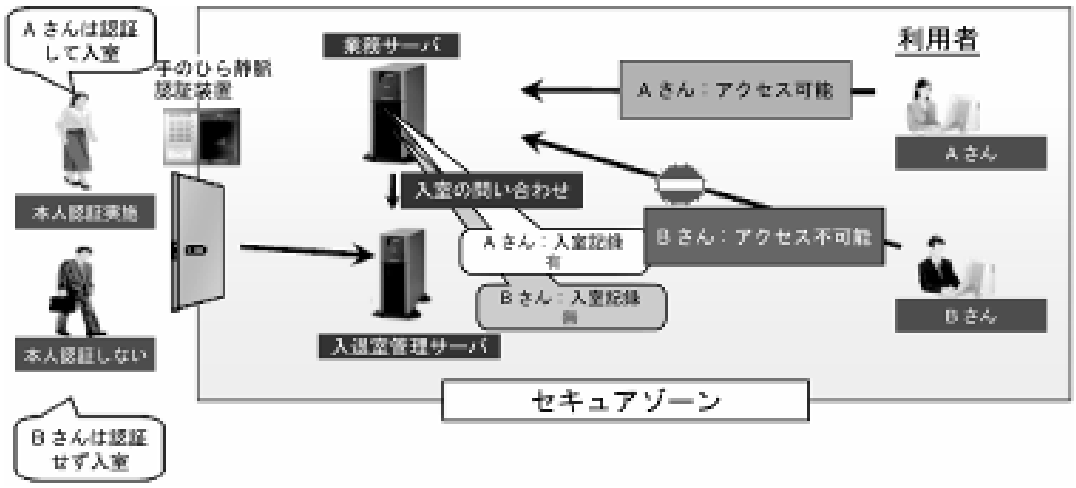


図 11.6-2 アイデンティティマネジメント導入の効果

情報システムの場合と同様に、フィジカルセキュリティの場合も証跡の取得と管理は重要なセキュリティ要素です。フィジカルセキュリティで収集すべきログには、以下のようなものがあります。

- ゾーンの入出時間
- ゾーンに入った ID
- 映像情報

また、ログの分析に際しても、情報システムとは異なる以下の視点が必要です。

- ゾーンへのアクセス権限の有無
- ゾーンへのアクセス回数
- ゾーンの入出数と映像による出入状態確認

さらに、ログ情報と映像保存情報をデータベースでリンクすることで、「ゾーンの入出」「入出時のログと人員の数の照合」「ログ検出時の挙動を映像で監視」をログ管理しておくことが必要です。

映像については、セキュリティレベルまたは監査証跡の観点から、監視方法、録画方法を考慮する必要があります。セキュリティレベルの高い環境における映像監視においては、動き検知機能の実装や録画映像の画質レベル、改ざん防止機能、録画期間などをあらかじめ詳細に決めておく必要があります。

11.7 フィジカルセキュリティによる利便性の追求

フィジカルセキュリティによる入退室管理を徹底させると非常に窮屈になり、効率的な業務活動に支障を来す場合があります。そのため、ゾーンのレベルによって素材の選定を図りながらセキュリティの高度化と利便性を両立させる方法を考えます。例えば、生体認証、映像、RFID(※)を使用することより、強固なセキュリティを保ちながら、オフィスにおいても、端末のアクセス権を得ることができ、離席時は、セキュリティモードに自動的に変更するなどの運用も可能となります。

また、情報資産の出力管理として、生体認証とプリンタを組み合わせたドキュメントセキュリティや書庫管理などを実施し、通常業務の利便性を追求しながらセキュリティを高めるシステム構築と運用手順の確立が望まれます。

※タグを使った動線管理、重要施設へのアクセス確認や映像とのひも付けにより、強固な監査証跡にもなり得ます。

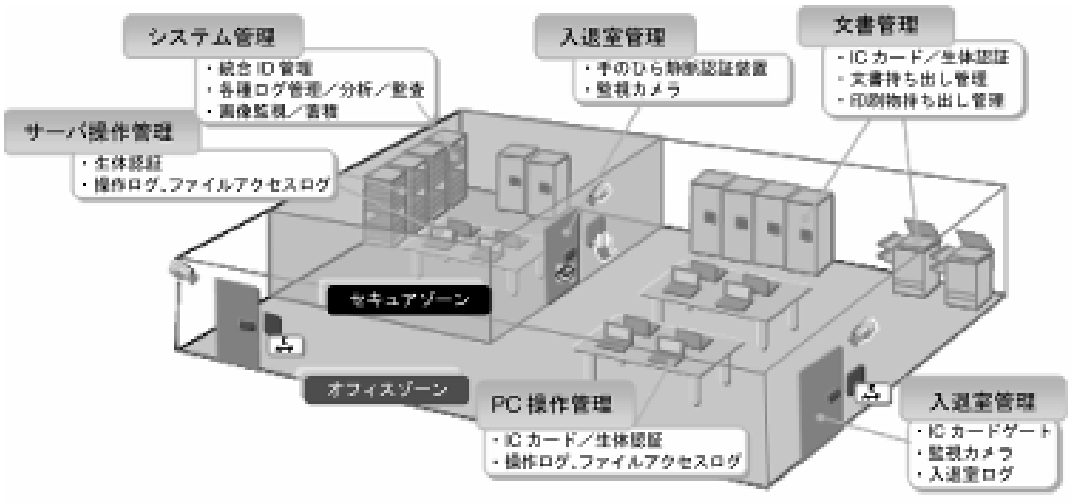


図 11.7-1 フィジカルセキュリティの利便性の追求

11.8 生体認証装置のポイント

生体認証装置は、その情報が唯一であることから、入退室管理に使用することで高いセキュリティレベルを実現できます。しかし、設置検討においては、操作において1:1の確認が必要であり、動線計画上、人だまりが起こらない場所で構築する必要があります。また、生体認証は、利用できない人がいることを考慮しておく必要があります。身体部位を限定した生体認証が利用できない人のための代替案を考慮しておかなければなりません。

11.9 映像の利用

映像をただ撮るだけでは、セキュリティ対策になりません。いかにその映像素材をセキュリティ対策に転換できるかを考えることが重要です。例として、次の二つの要素が入ることでセキュリティ対策として実現できます。

- 警告情報や認証情報と映像を照合することによる識別・認証精度の向上
- 映像化された動態のデータ変異による識別と認証、警告情報の通知

■ 入退室管理

ID カードなどを使った入退室システムに連携し、補助的に映像を記録します。入退室の行為を検出し、前後数秒の映像を記録します。入退室の検証に有効です。

入場者の制限をしないセキュリティレベルのエリアでも、入退室者を記録することも考慮します。ゲートとなる場所にカメラを設置し、画像処理により人物を特定または分類し、認識結果とキャプチャ画像を保存します。エリアの利用についての統計的管理や、セキュリティ上の記録として利用できます。

ただし、映像情報はデータ量が膨大であるため、長期保管をはじめとした運用管理に注意が必要です。

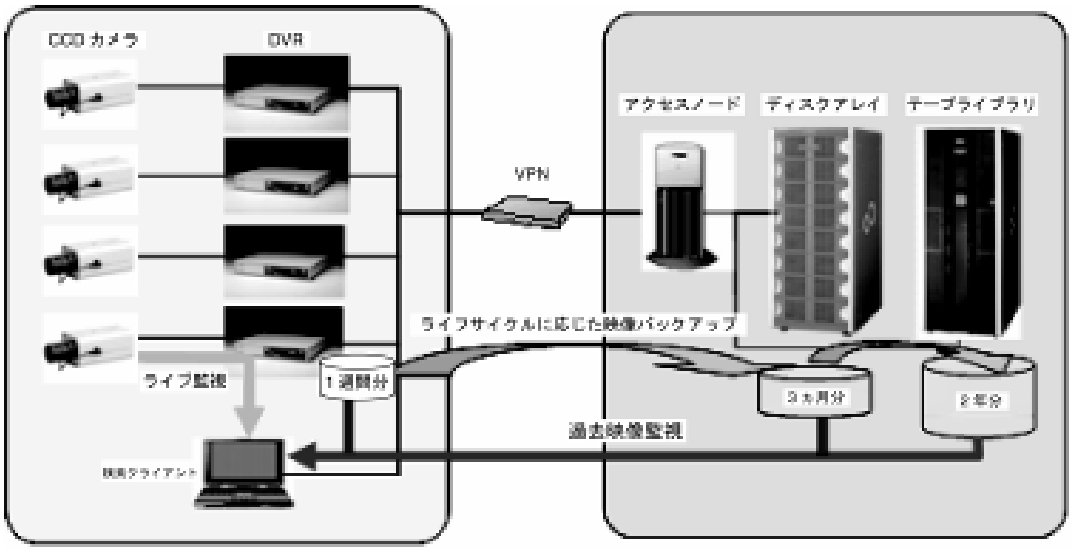


図 11.9-1 映像長期保存の構築例

■ 機器の管理

施錠や入退室管理システムでのエリア管理以外に、機器の管理という側面で映像の利用が考えられます。カメラで被監視対象の機器を映し、画像処理により、機器の移動を検出します。あるいは、作業エリアに不審物が持ち込まれないか、カメラにより監視し、持ち込まれた物体が放置されていないか、画像処理により検出します。24 時間 365 日動作するシステムではネットワーク監視のほか、目視による機器の見回り監視をシステム化した、映像によるリモート監視の導入も選択肢の一つとなります。

以上のシステムで記録した映像は、他の管理情報と同様に適切に管理されている必要があります。また、リモート環境から映像を閲覧する場合、ネットワーク上でのデータ漏洩がないように、暗号化などの施策を実施する必要があります。

■ RFID タグによるセキュリティ

RFID には、パッシブタイプとアクティブタイプの 2 種類があります。パッシブタイプは、情報セキュリティの ID 管理や PKI で広く実施されています。アクティブタイプは、現在まだ用途が限られていますが、位置検知の観点で今後の発展性に注目されています。アクティブタイプの利点である、同時検知や数十mスパンでの検知可能な機能がセキュリティ対策として利用できます。

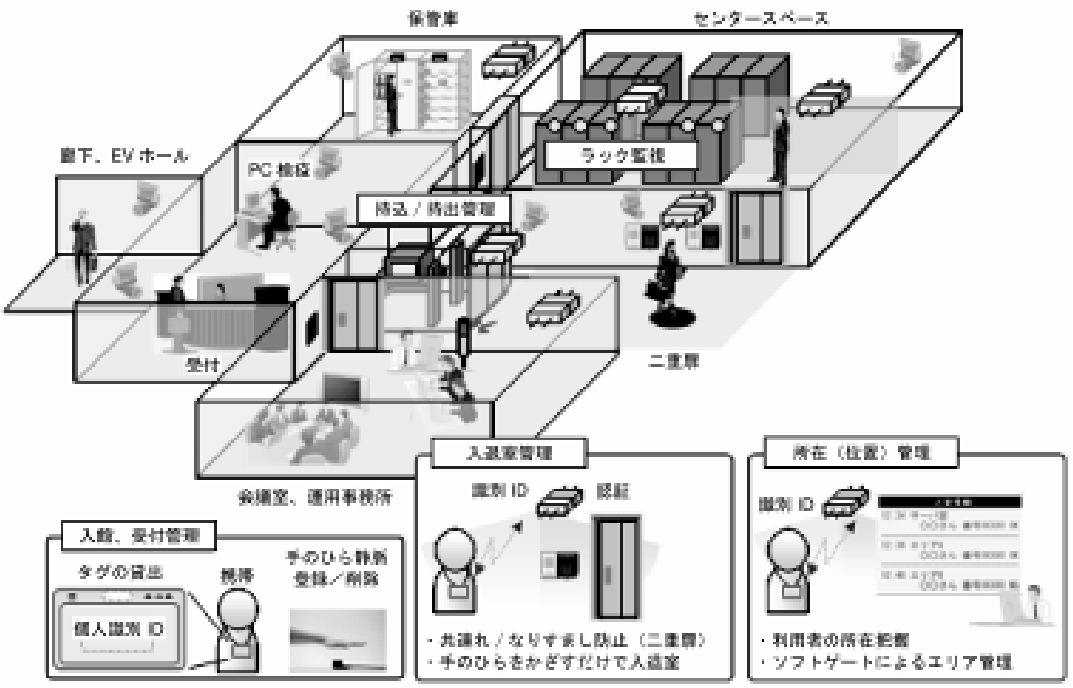


図 11.9-2 RFID によるオフィスでの実施例

第三部 ESA に基づいたシステムのあり方

12. システム構築

IT システムへのセキュリティの実装を考える上で最も重要なことは、資産（データ、プログラム、ハードウェアリソース）がさまざまな攻撃から守られるようなアクセスコントロールを実現することです。外部からの多様な攻撃を防御し、内部からのアクセスを正しく制御することで、資産を保護することができます。

また、侵入者、内部犯罪者がアクセスコントロールを侵害していないかどうかを検証するために、これらに対する検証の手段を実装することも必要です。

第二部では、エンタープライズセキュリティアーキテクチャーを確立するために必要となる基本概念についてまとめました。本章では、第二部で提示したアーキテクチャーの考え方に基づいて、システムを構築する場合の基本的な考え方と代表的なモデルについて説明します。

本章では、IT システムへのセキュリティ機能の実装に着目するため、IT システムは物理的に守られていることを前提にします。物理的なセキュリティの考え方と対策についての詳細は第二部 11 章「フィジカルセキュリティ」をご覧ください。

12.1 セキュリティ機能実装のためのモデル

IT システムは、データ、プログラムをいずれかのハードウェアに格納した「リソース」を、何らかの通信方法でつなぎ合わせた、「リソースと通信部分の集合体」と言うことができます。このため、リソース単体に対するアクセス行為へのコントロール対策と、リソースとリソースを結ぶ通信部分に対するアクセス行為へのアクセスコントロールを行うことで、IT システムに対するアクセス行為をコントロールすることができると言えます。

ここでは、理解を深めるために具体的なシステムの構成の説明に入る前に、モデルを使って考え方を説明します。

まず使用する言葉について確認します。

- 情報フロー部：データ通信が行われる部分
- 情報処理部：データを受け取り、処理し、渡す部分。主にアプリケーションサーバ
- 情報保存部：データ保存する部分。主にデータベースサーバ
- データ：ITシステムで取り扱う電子データ全般
- プログラム：主に情報処理部で動作する業務プログラム

- ハードウェアリソース:情報フロー部、情報処理部、情報保存部で使用するハードウェア

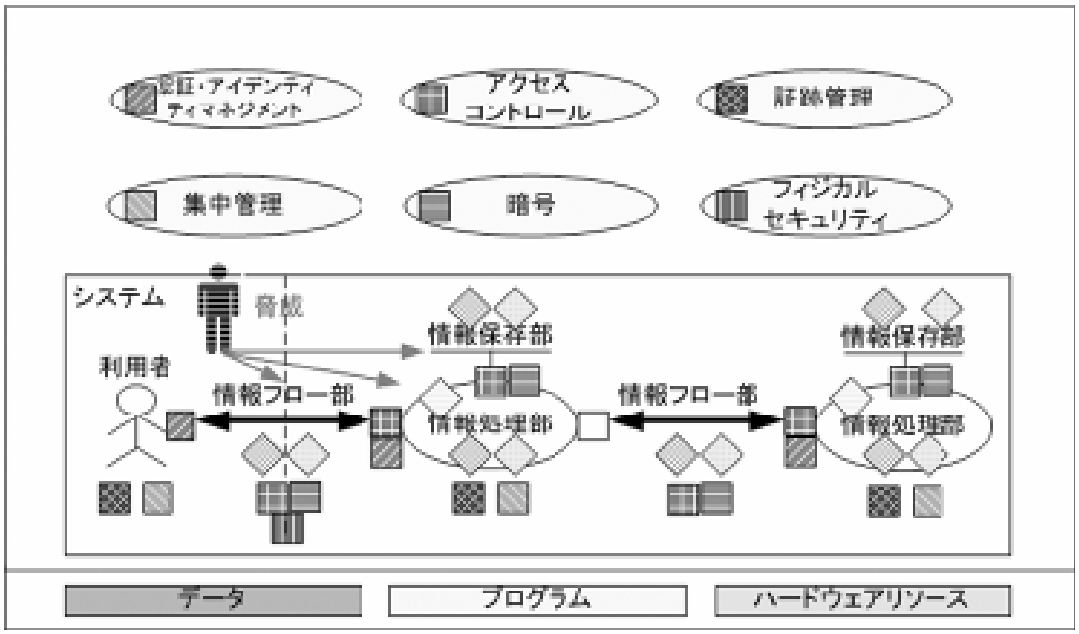


図 12.1-1 リソースとセキュリティ機能

「図 12.1-1 リソースとセキュリティ機能」は、一般的なシステムにおけるリソースとセキュリティ機能の関係をモデルとして示したものです。図中の7種の正方形は、セキュリティ機能としてそれぞれ、 : 認証・アイデンティティティマネジメント、 : アクセスコントロール、 : 証跡管理、 : 集中管理、 : 暗号、 : フィジカルセキュリティ、および : 情報処理部間の通信元プログラムを表しています。また、3種の菱形はそれぞれ : データ、 : プログラム、 : ハードウェアリソースを表しています。

この図は、IT システムの概観をモデル化したものであり、IT システムは、処理、およびデータの受け渡しを行う「情報処理部」、データ通信路である「情報フロー部」、およびデータを保存する「情報保存部」によって構成されているということができます。この図から、IT システムにおけるセキュリティ対策は、情報処理部のデータの出入り口、情報保存部のデータの出入り口、およびデータ投入を行う利用者について、必ず認証・アイデンティティティマネジメント、およびアクセスコントロールの機能を配置し、情報処理部では必ず証跡管理機能を配置する必要があることが分かります。

このモデルに従えば、身元の保証された利用者は、クライアント PC を介して、情報処理部であるアプリケーションサーバーに情報フロー部であるネットワークを通じてアクセスし、業務処理を行い、情報保存部であるデータベースへ情報を格納するまでのあいだに、少なくとも6つ以上のセキュリティ機能を通過します。企業が、例えば上記のような6つのセキュリティ機能を配置することをルールとし、それぞれのセキュリティ機能の配置・方法等を定めれば、そのルールを変更しないかぎり6つのセキュリティ機能で実現できる

12. システム構築

セキュリティレベルは企業内の他のシステムにも引き継がれます。これが、システム構築におけるエンタープライズセキュリティアーキテクチャーです。

セキュリティ機能の実装は、以下の手順で進めます。リスクや脅威の分析については、第四部の参考資料も参考にしてください。

1) 資産の明確化

保護すべき資産を抽出し、明確化します。資産の明確化はセキュリティ対策の出発点です。

2) 処理フローの明確化

資産が、IT システム上のどこに存在し、どのように処理され、どこに格納されるかといった資産の処理フローを明確にします。これにより、それぞれの処理フロー上で実装すべきセキュリティ機能が明確になります。

3) 脅威の抽出

資産と資産の場所が明確になった後、その資産に対する脅威を抽出します。脅威が抽出されることで、対策を決めることができます。

4) セキュリティ機能のサーバ、ネットワークへの配置

抽出した脅威に対抗するためのセキュリティ対策を決めます。まず、Web サーバや DB サーバといったサーバごとに実装するセキュリティ機能を決めます。次に、サーバ間受け渡し等、ネットワークへの対策を決めます。資産がファイアウォールをまたがって渡される場合、渡し元のサーバのセキュリティ機能で確保されたセキュリティ強度が、渡された先へ引き継がれなくてはなりません。これにより、最初のセキュリティ強度を最後まで維持することができます。

5) セキュリティ機能の集約

IT システムは、通常複数の機器によって構成されています。そして、それぞれの機器ごとにセキュリティ機能は存在します。例えば、複数系統ある業務システムを構成する機器のほとんどに、ID 管理機能があり、ほとんどに認証機能があります。二重化されているデータベースサーバには、それぞれに ID 管理機能やアクセスコントロール機能があるでしょう。

しかし、これらのセキュリティ機能は、必ずすべてその場所に必要でしょうか。ユーザ ID をそれぞれのサーバーで別々に管理することは、一般的に運用管理費用の増加を招きます。また、複雑すぎるアクセスコントロールは、性能の劣化を招くこともあります。

ESA では、有効性・効率性を考え、安全性を低下させることなく、安全性が確保されることを前提に、複数存在するセキュリティ機能を「集約」していくことを推奨しています。集約とは、ファイアウォールなど、アクセスをフィルタリングする装置などによって、安全性が確保されることを前提に、冗長に存在し費用の増大を招いているセキュリティ機能をまとめていくという考え方です。集約の対象とすべきセキュリティ機能は、「認証機能」、「アクセスコントロール機能」といった比較的大きな機能から、「利用者登録」、「利用者削除」といった詳細な機能までさまざまです。

ここからは、集約の概念と、集約を考える際に外してはならないことについて説明していきます。

12.2 集約の概念

業務システムを構成する機器上に、複数のセキュリティ機能が分散配置されていることについて述べました。ここでは理解を早めるために、とてもシンプルな3層 Web システムをモデルとして集約の概念を説明します。

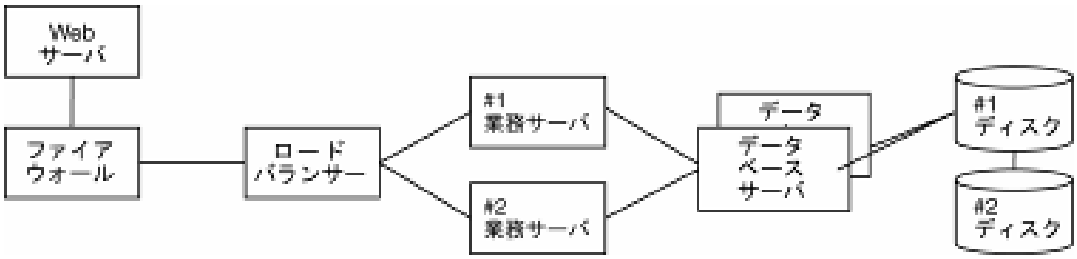


図 12.2-1 二重化に着目した機器構成

ここで認証・アイデンティティマネジメントを例にとって考えます。一般的なシステムで考えた場合、この機器構成のどこに認証機能と ID 管理機能が配備されるでしょうか。管理機能を含めれば、すべての機器にその機能が配備されます。

この構成の場合、ファイアウォールより後ろは、外部から直接アクセスされることはありません。言い換えると、ファイアウォールによって得られる安全性は、ロードバランサー、業務サーバ、データベースサーバ、ディスクに継承されています。

このような場合、二つの業務サーバが別々に認証機能や ID 管理機能を持つことはあまり意味がありません。逆に、別管理することにより運用ミスを起こして業務に影響を与えたり、運用コストの増加を招いたりすることがあります。

そこで、機能の集約を考えます。二つの業務サーバから、認証機能や ID 管理機能を除き、その機能を専用サーバに任せる認証サーバや、シングルサインオンシステムなどがよい例です。運用ミスや運用コストの削減だけでなく、業務サーバで実施していた認証や ID 管理といった作業がなくなり、性能向上にもつながります。

また、Web サーバ、業務サーバ、データベースサーバなど別々の業務処理を行う機器間でも集約が可能な場合があります。例えば、Web サーバ、業務サーバで動作するアプリケーションプログラムなどがその例です。業務処理を行う利用者は、Web サーバのみにログインするだけで、アプリケーションプログラムが動作し、必要なデータベースレコードにデータが書き込まれます。この場合、実際には業務サーバやデータベースサーバには、利用者の ID や認証情報が管理されているわけではなく、アプリケーションユーザーや、データベースユーザーなどのシステムユーザーが Web サーバで行われた、認証や ID 管理を継承しており、言い換えると、Web サーバに認証機能や ID 管理機能を集約したと言えます。この集約により、業務システム上には、「知る必要性」に応じたユーザーの管理が実現されます。

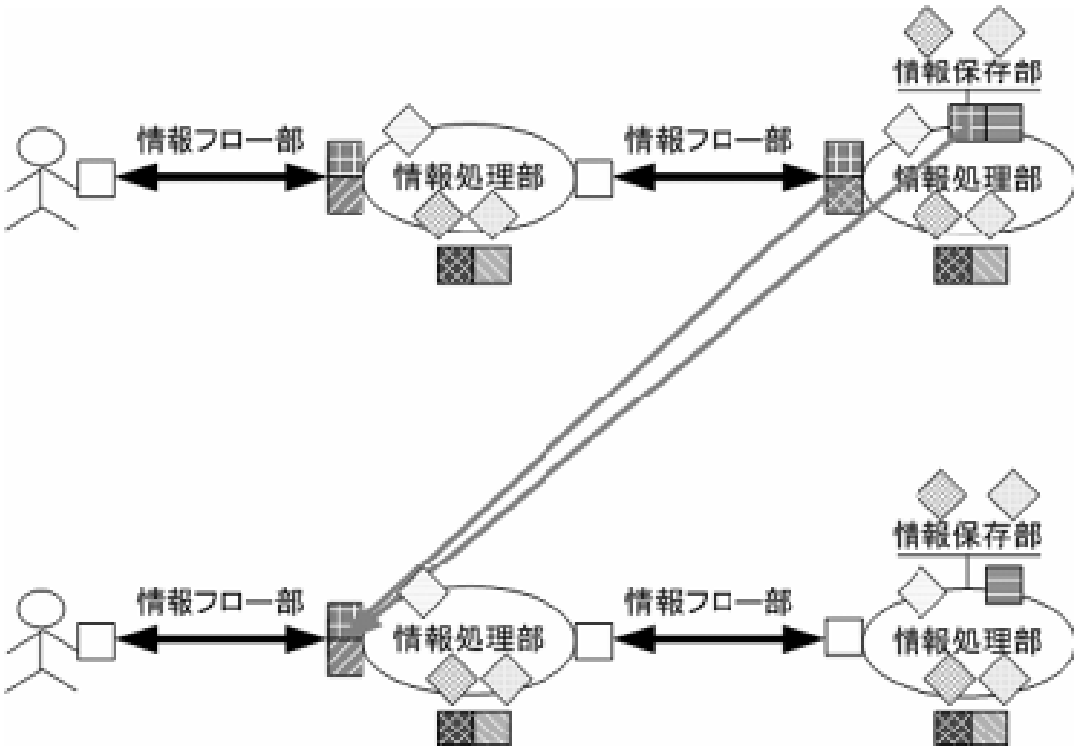


図 12.2-2 集約配備

ESA では、このように、同じ業務処理を性能や信頼性向上のために並列に並べた業務サーバなどのセキュリティ機能を集約していくことを、横並びを集約するという見かけから、「横集約」と呼び、Web サーバと業務サーバ、業務サーバとデータベースサーバなど、利用者からデータベースまで横集約と直行した縦並びの機器のセキュリティ機能を集約していくことを、「縦集約」と呼ぶことにします。

これからのシステム開発やシステム改修は、「システムを止めない」への意識から、「業務を止めない」へと意識変革しなければなりません。「横集約」、「縦集約」を十分に意識して、無駄のない、安全なセキュリティ対策を実現していく必要があります。

12.3 集約の進め方

集約を考える場合には、構築するまたは改修するシステム全体をよく見て、「資産」がどこに保存され、どこを「通り」、どのように「アクセス制御」され、最終の目的地に到達するかという処理フローを明確にします。IT システムには、データ（命令なども含む）が停止しているか移動しているかのどちらかしかないため、その両方を確実に把握することが集約の第一歩となります。

処理フローを明確にした後に、セキュリティ機能として何を考え実装すべきか、またそれをどこに配置すべきかを明確にしていくことが次の一歩となります。さまざまな要件で開発されるITシステムの実現方法は多様です。ここでは、すべての IT システムで最低限実装すべき内容について説明します。

ここまでで、集約の準備が整いました。最後の一歩として、具体的な集約を考えます。本項では、集約の方針を説明していきます。

12.4 集約の方法

集約を行うためには、前章で説明した三つのステップ「1. 資産の処理フローを明確にする」、「2. 実装すべき内容と配置を考える」、「3. 集約の方法を考える」で進めていきます。

ここでは、セキュリティを考える上で重要な4項目について、「実装すべき内容と配置について」、および「集約の方針」について説明します。システム開発者、改修者は、この二つの項目を基に、三つのステップで集約の方法を決めていくことが重要です。

＜セキュリティを考える上で重要な4項目＞

- 認証・アイデンティティマネジメント
- アクセスコントロール
- 証跡管理
- 集中管理

セキュリティ全体を考える場合には、IT、非 IT を考慮し、フィジカルセキュリティについての考慮も必要ですが、ここでは集約を考える上で IT システムで実装するべきセキュリティを示すことを目的としているた

め対象外としています。ただし、入退室の管理システムとITを連動するなどのシステムを考える場合は、必要に応じて集約を検討していくことが必要です。

本章では、四つのセキュリティ機能の中でも、最もITシステムの安全性・信頼性に影響のある「認証アイデンティティマネジメント」を例に、集約までの作業内容と集約方針を説明します。

12.5 認証・アイデンティティマネジメントでの集約例

認証とアイデンティティマネジメントは、それぞれ違う機能ですが、業務システムに対するアクセスを考えると、本人であることとその本人がシステムを利用する(プログラムのセッション管理も含む)ための認証行為は一般的に同時に行われます。例えば、Aさんからのアクセスを業務システムが実行する場合、業務システムは、Aさんの識別情報と、識別情報と対で管理される認証情報を確認し、違いがなければ実行するといった具合です。認証・アイデンティティマネジメントの詳細については、第4章「認証」、第5章「アイデンティティマネジメント」を参照してください。

ここでは、業務システムへのアクセス行為を正しく管理・制御することがシステム構築時に考慮すべきセキュリティの大原則ととらえて、認証とアイデンティティマネジメントを一緒に考えていきます。

■ 基本的な考え方

認証・アイデンティティマネジメント機能と、先に述べた4つの重要な項目と、利用者認証の関係は、次の図のようになります。

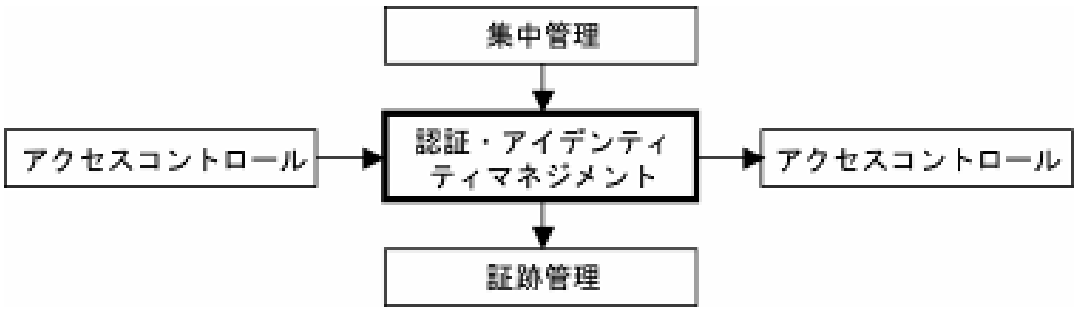


図 12.5-1 セキュリティ機能関係図

上図は、ITシステムのすべてのデータがアクセスコントロールされ、アクセスコントロールとアクセスコントロールの間には、必ず認証・アイデンティティマネジメントが行われ、すべて集中管理され、すべて証跡管理されるということを表しています。

■ 認証・アイデンティティマネジメント機能を実現するための基本的なケースとプロセス

認証・アイデンティティマネジメント機能を実現するために考慮すべき基本的なケースと、そのケースを具体化する基本的なプロセスを説明します。ここでは、「プロセス」をコンピューター処理でのプロセスではなく、処理の進行、過程といった意味で使用しています。

認証・アイデンティティマネジメント機能には、利用者認証機能、および認証情報管理機能の2つの機能があります。

認証・アイデンティティマネジメント機能を実現するには、少なくとも、表に示す基本的なケースに示す5つのケースと、それに対応する詳細なプロセス(図中では、「詳細プロセス」)を実装する必要があります。

表 12.5-1 セキュリティ機能と基本的なケースの関連

セキュリティ機能	基本的なケース	対応する詳細プロセス図
利用者認証機能	① 利用者初回認証	ー 図 12.5-2 利用者初回認証ケースのプロセス
	② 利用者定期認証	ー 図 12.5-3 利用者定期認証ケースのプロセス
認証情報管理機能	③ 利用者登録	ー 図 12.5-4 利用者登録ケースのプロセス
	④ 利用者削除	ー 図 12.5-5 利用者削除ケースのプロセス
	⑤ 利用者停止・復旧	ー 図 12.5-6 利用者停止・復旧ケースのプロセス

①利用者初回認証

利用者がIDやパスワードなどを含む識別認証情報を入手している状態で、最初にアクセスしようとした際に行うクライアント、およびサーバのプロセスについて示します。図中の「C」、「S」は、それぞれ、Cはクライアント側動作を、Sはサーバ側動作を表しています

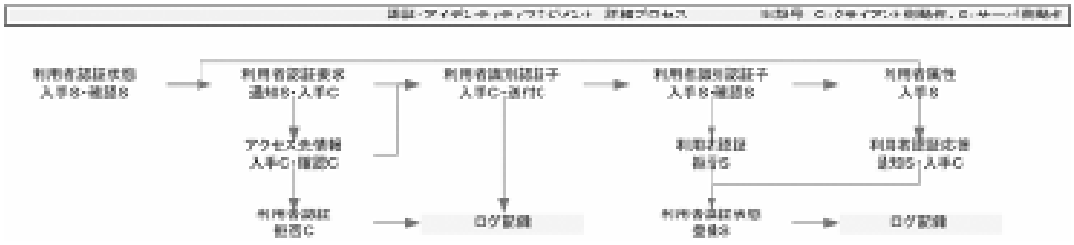


図 12.5-2 利用者初回認証ケースのプロセス

図は、利用者認証状態から始まっています。利用者初回認証は、最初の状態によって状態が変わります。すでに認証を受けている場合はその利用者属性入手から処理を開始します。まったく認証を受けていないシステムへの利用者初回認証の場合は、利用者認証要求通知S・入手Cから開始します。開始要求には、利用者によるログインまたはプログラムなどによる要求などがあります。「利用者認証機能」は要求を受け取った後、アクセス先認証が既に行われているか判断し、行われ

ていなければ確認し、問題があれば認証を拒否し、記録に残します。問題がなければ利用者識別情報と、認証情報をアクセス要求先へ送付します。アクセス要求先は、要求を受け取った後、問題があれば認証を拒否し、状態を記録します。問題がなければ、利用者識別情報の属性情報を入手した後、要求元へ認証通過の通知を行い、状態を記録します。具体的な実装には、利用者認証機能、認証情報管理機能についてプロセスを詳細機能化し機能設計します。

② 利用者定期認証

初回認証が行われた状態に対して、自動で定期的に再認証を行う場合のプロセスについて説明します。

図 12.5-3 利用者定期認証ケースのプロセス

利用者が IT システムにアクセスする環境は、時々刻々と変化しています。セキュリティ対策を考える上では、そのような状況にも考慮する必要があります。

このため、IT システムでは、定期的な再認証の仕組みを考慮します。

利用者定期認証ケースのプロセスは、時刻情報入手Sを起点に、開始します。IT システムは時間監視を行い定期的に再認証要求を行います。利用者認証機能は、設定した時刻を検知すると、再認証ルールにのっとり再認証のプロセスを開始します。認証行為は、初回認証と同じ仕組みで実施します。利用者認証機能は、再認証を完了したのち、状態を記録します。

③ 利用者登録

利用者認証には、利用者認証機能のほかに、認証情報を管理する「認証情報管理機能」が必要です。利用者登録は、利用者認証を行うために利用者の情報を IT システムに登録するための管理機能です。以下に、利用者登録を行うためのプロセスについて説明します。

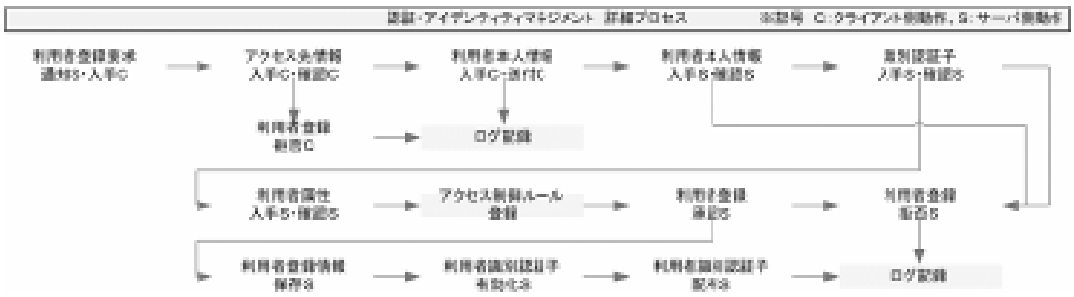


図 12.5-4 利用者登録ケースのプロセス

利用者自身が行う利用者登録処理を受けた、利用者登録要求通知S・入手Cが起点となり処理を開始します。運用管理者が、登録行為を行う場合も要求の起点は利用者登録要求です。利用者登録を行うクライアントは、登録先のシステムを確認し、問題があれば、状況を記録し、終了します。問題がなければ、利用者情報を登録先へ送信します。登録要求を受け取った登録先は、登録者の本人情報の確認を行い問題があれば利用者登録を中止し、状態を記録します。問題がなければ、利用者属性を入手し、アクセスコントロール機能の基本的なケースである、「アクセス制御ルール登録」にアクセスコントロールのルール登録を要求します。アクセス制御ルール登録から復帰した後、利用者登録承認プロセスは問題があれば利用者登録を中止し、状態を記録します。問題がなければ、利用者情報を登録し、利用者識別子を有効化し、状態を記録します。

④ 利用者削除

利用者削除は、何らかの理由で利用者情報をITシステムから削除するための基本的なケースです。以下に、利用者削除を行うためのプロセスについて説明します。

図 12.5-5 利用者削除ケースのプロセス

利用者の削除は、誤処理が業務に与える影響がとても大きいため、削除要求を受けた後、利用者初回認証と同じプロセスで要求元の認証を行います。利用者初回認証から復帰し、要求元に問題がある場合、利用者情報削除プロセスは削除処理を中止し、状態を記録します。問題がない場合は、利用者識別情報の無効化を行った後、アクセスコントロール機能の基本ケースである「アクセ

ス制御ルール削除」にアクセスコントロールのルール削除を要求します。その後、利用者識別情報を削除し、利用者の認証状態を初期化し、状態を記録します。

⑤ 利用者停止・復旧

利用者情報の停止・復旧要求があった場合の、プロセスについて説明します。

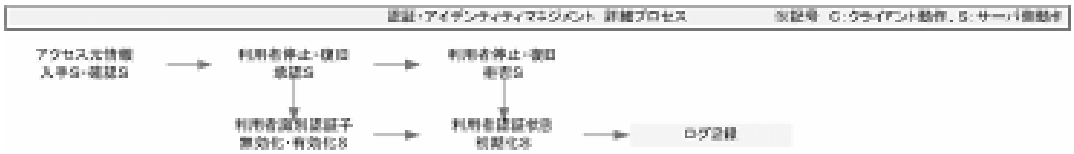


図 12.5-6 利用者停止・復旧ケースのプロセス

利用者停止・復旧要求を受け取った、利用者停止・復旧承認プロセスは、アクセス元情報に問題があれば利用者停止・復旧を中止し、利用者認証状態を初期化し、状態を記録します。問題がなければ、利用者識別情報の無効化または有効化を行った後、利用者認証状態を初期化し、状態を記録します。

■ 利用者認証における集約の方針と方法

ここまで、利用者認証で必要な二つのセキュリティ機能（5つの基本的なケース）について、その処理プロセスに注目して説明してきました。ここからは、これらのセキュリティ機能やプロセスが複数、分散して冗長に存在した場合に行う、集約について説明します。

すでに、集約には、「縦集約」と「横集約」があり、それぞれを組み合わせ、無駄のない、安全なセキュリティ対策を行うことが重要であることは述べましたが、ここでは利用者認証における縦集約と横集約を考えていきます。

● 集約の方針

集約は、ESAの目的である「有効性」、「効率性」を向上させるために実施します。ここでは、利用者認証における集約の方針について整理しています。

先に、認証・アイデンティティマネジメントのセキュリティで行われる行為を総称して利用者認証と呼ぶと定義しました。言い換えると、ここで説明する方針は、「認証・アイデンティティマネジメントの集約方針」と言うことができます。

＜有効性向上のための集約方針＞

① 実現手段

－ 保護資産の存在場所ごとに、利用者が識別・認証情報を入力します。

- 識別情報と属性情報（例：利用者権限など）を管理します。

② ポイント

- IT システム上の利用者認証機能、および認証情報管理機能を集約配備します。
- 利用者が IT システムを利用する場合の入力場所を集約配備します。
- 管理者の設定場所を集約配備します。

③ 条件

- 集約が、IT システムのボトルネックにならないこと。

＜効率性向上のための集約方針＞

効率性向上については、いきなり効率性の高いシステムを要求すると、導入費用が増大する可能性などの問題が発生することが考えられるため、三つの段階に分けて順次、機能拡張、範囲拡大を考えます。

- **第一段階**

① 実現手段

- 保護資産を利用者の属性ごとに分離したシステム構成にします。
- 利用者ごとの識別認証情報を共有化し集中管理します。

② ポイント

- IT システムへのアクセス部のみに利用者認証機能を集約配備します。
- IT システムへのアクセス部のみで利用者が入力します。
- 管理機能のリソースを集約配備します。

③ 集約の実装例

- OS 認証、ネットワーク認証、Web 認証システム
- LDAP サーバなど

- **第二段階**

① 実現手段

- IT システムへのアクセス部のみで利用者が識別認証情報を入力して認証します。
- 保護資産の存在場所すべてで利用者に関連付けられたサブジェクトで自動認証します。
- 利用者ごとの識別認証情報と属性情報を共有化し、集中管理します。

② ポイント

- IT システムへのアクセス部のみで利用者が入力するようにします。
- 管理機能のリソースを集約配備します。

③ 実装例

- シングルサインオン認証（業務処理の認証、データベース認証連携など）システム
- 認証サーバなど

● **最終段階**

① 実現手段

- IT システムへのアクセス部のみで利用者が識別認証情報を入力して認証します。
- システムごとの識別認証情報と属性情報を集中管理します。

② ポイント

- 最初のシステムへのアクセス部のみで利用者が入力します。
- 管理機能のリソースを集約配備します。

③ 実装例

- シングルサインオン認証システム
- ID プロビジョニングサーバ

● **利用者認証における集約の方法**

集約の方針を受けて、利用者認証における集約について、縦集約と横集約に分けて方法について説明します。

＜縦集約＞

縦集約は、主に処理目的の異なる機器で集約可能な機能を持っている場合に使用する方法です。

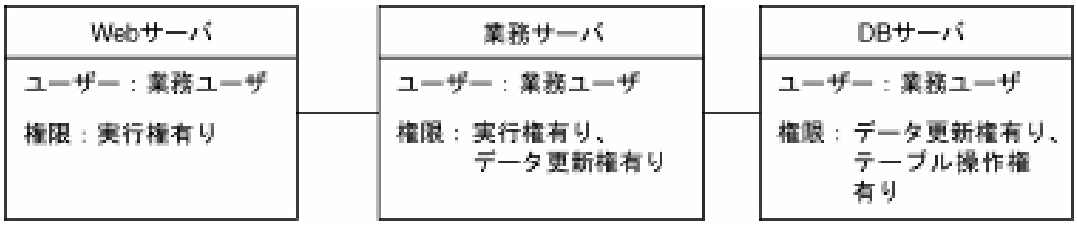


図 12.5-7 一般的なユーザー登録の状態

上図は、Web3階層システムを構成する一般的なユーザ登録の状態を簡単に表したものです。Web サーバ、業務サーバ、DB サーバそれぞれに業務ユーザーが登録され、それぞれのサーバ上でアプリケーションの実行権限や、データの更新権限、データ更新権限をもつユーザ設定です。

また、今まで述べてきた認証・アイデンティティマネジメントの5つの基本的なケースを考えた場合、それぞれのサーバに重複したユーザーが登録されてしまうことも考えられます。

しかし、これでは、セキュリティの大原則である、知る必要性に応じた設定、かつ最小権限の設定という考え方に反します。そこで、利用者の集約を今までに述べてきた方法で、実現する必要があります。以下の図は、Web サーバの利用者認証に利用者を集約し、業務サーバ、DBサーバには実行可能ユーザー、操作可能ユーザーを残しません。下図は、集約後のユーザーと、権限の登録状態です。

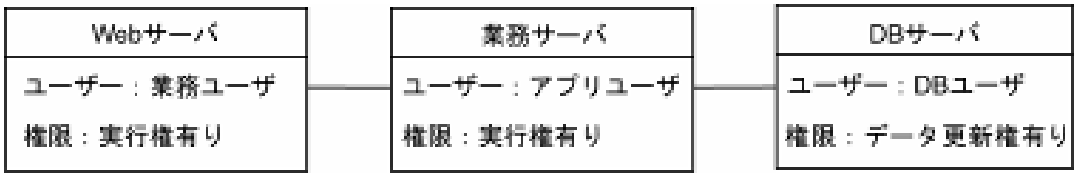


図 12.5-8 集約後のユーザー登録の状態

これにより、業務サーバではアプリケーションユーザを、データベースサーバでは DB ユーザという共通ユーザのみ準備すればよいことになり、セキュリティの大原則にも沿った対策となります。

＜横集約＞

横集約とは、同じ業務処理を並列に並べた業務サーバなどのセキュリティ機能を集約する方法です。

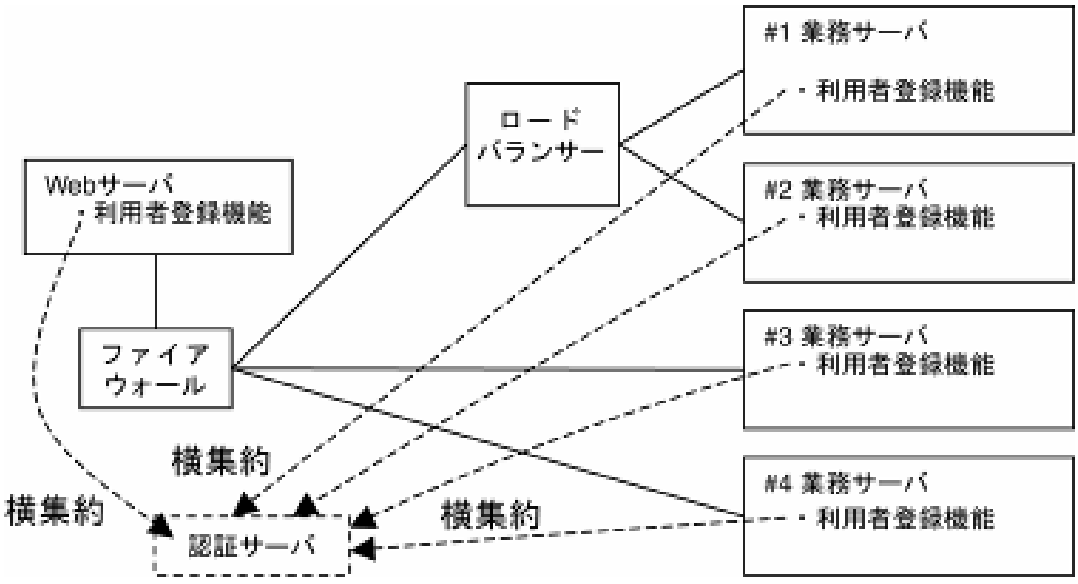


図 12.5-9 横集約の例

上図のように、IT システムを構成している複数のサーバ上に、同じ機能が分散している場合、最大でサーバ台数分の5カ所に利用者登録機能が分散しています。

このような場合、利用者登録機能を別サーバに抽出し、1 カ所に集約します。

ただし、集約を進めることは、同時に単一障害点を増やすことになりますので、集約したポイントが障害を起こした場合への十分な考慮が必要です。

12.6 ESA に基づく 3 階層 Web システムモデル実装例（利用者への対策）

ここまで、ESA の考え方、認証・アイデンティティマネジメントを例にした集約の方法など、セキュリティ機能の実装の考え方の基本を説明してきました。

次は、3 階層 Web システムモデルを通して具体的に、「リソースごと」、「リソース間」の観点でどのようなセキュリティ機能を実装するかを見ていきます。

ここからは、認証・アイデンティティマネジメントのほか、アクセスコントロール、証跡管理、集中管理についての集約も行い、システム全体の実装例と方法について説明しています。

3 階層 Web システムは、現代のコンピュータ社会の中心的なシステム構成であり、最もセキュリティ上の考慮要請事項が多いシステム構成と言えます。このため、ESA の考え方に基づいた最初のモデルは、3 階層 Web システムを選定しました。3 階層 Web システムモデルの利用者側からのセキュリティ対策について、詳細に見ていきます。

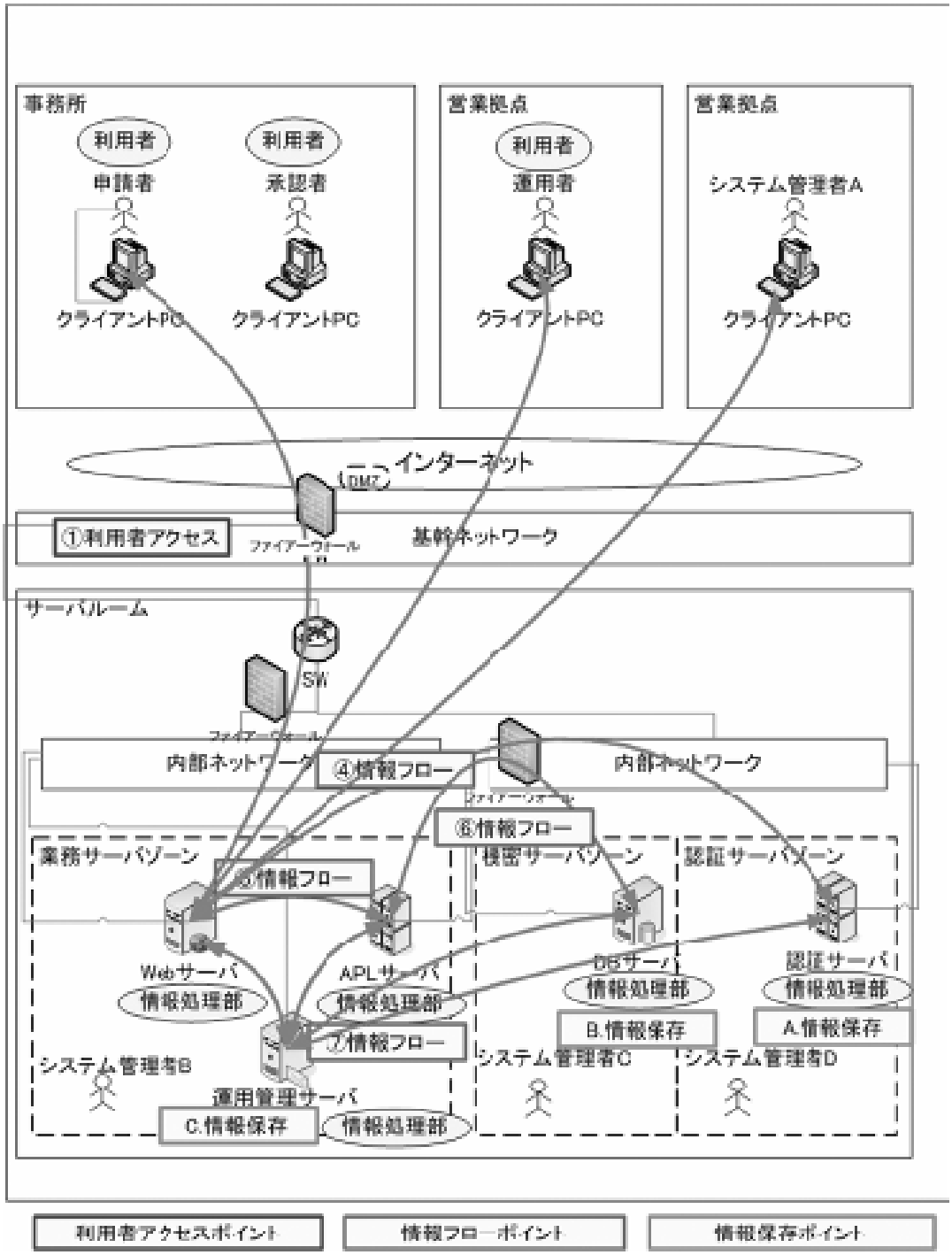


図 12.6-1 3 階層 Web システムモデル(システム構成・アクセス関係図)

個々のリソース、リソース間のセキュリティ機能を見る前に、まず、システム全体でリソース同士のアクセスの関係がどのようになっているのかを確認します。このシステムモデルでは、事務所や営業拠点といった利用者端末から、インターネットを経て社内のファイアーウォールを通り、社内の Web サーバ、認証サーバ、AP サーバ、DB サーバの順にデータが流れます。矢印曲線は、データの流れを示しています。また、このモデルでは業務サーバゾーン、機密サーバゾーン、認証サーバゾーンの三つのゾーンを構成

し、ゾーンを超えてリソースにアクセスするためには、ファイアーウォールを通じてアクセスする、多重防御の構成にしています。

次の図は、3 階層 Web システムモデルにおいて実装すべきセキュリティ機能項目の全体俯瞰図です。それぞれのリソースごと、リソース間の詳細について見ていきます。

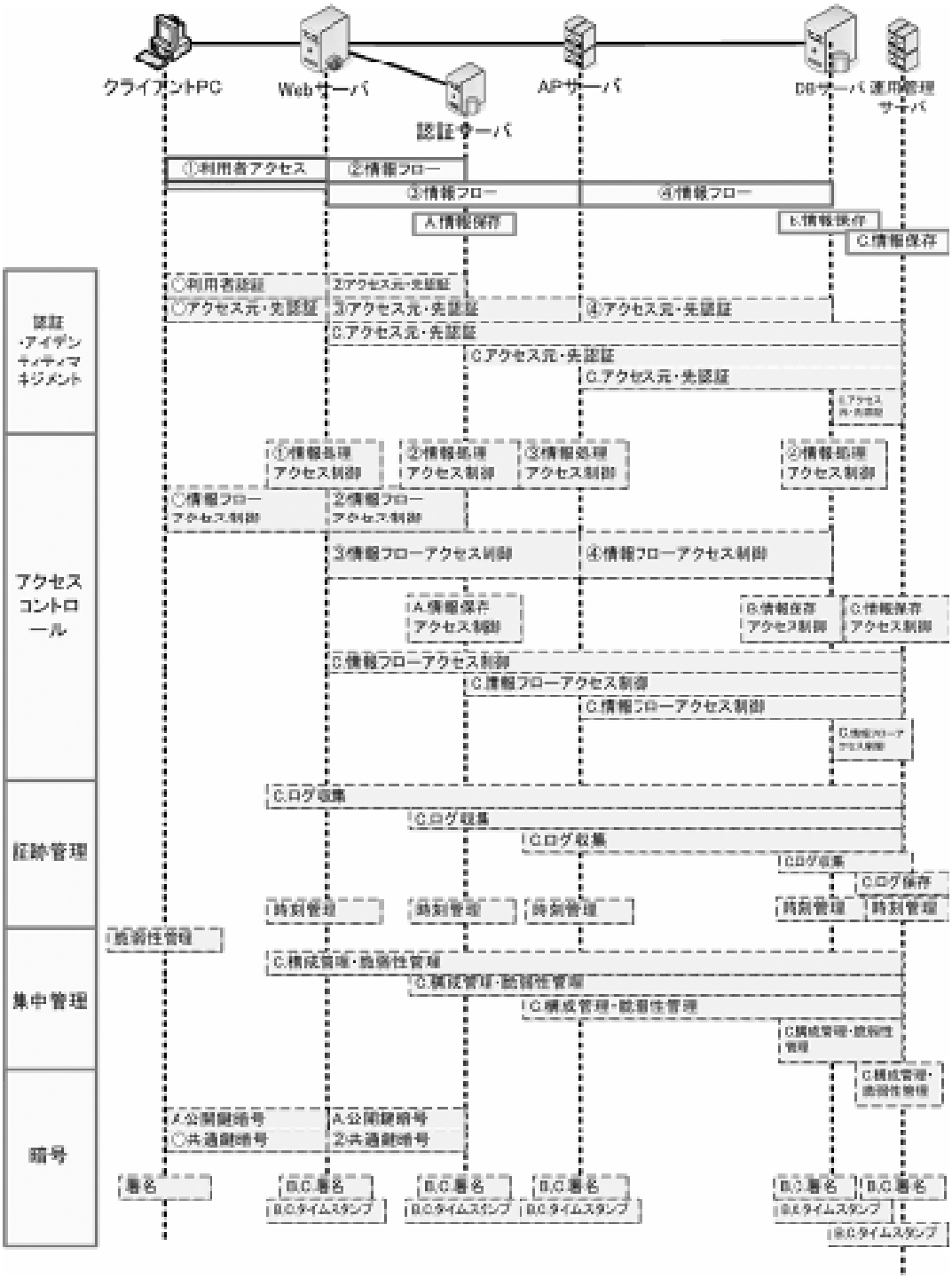


図 12.6-2 3 階層 Web システムモデル（実装すべき機能の全体俯瞰図）

■ 3 階層 Web システムモデルにおけるセキュリティ機能実装の考慮点

このモデルにおけるセキュリティ機能を集約した上で必要になる考慮点をまとめると、以下のようになります。

- 認証・アイデンティティマネジメント
  - リソース間で安全性を引き継ぐため、リソース同士の認証機能を考慮する。
  - IT システムの不正利用を防止するため、利用者に与える権限は必要最小限とする。
  - 利用者の職務と職責は必ず分離し、不正行為を行うことができないようにする。
  - 運用性向上とセキュリティ事故防止を考慮し、利用者のユーザアカウントは統合管理する。
- アクセスコントロール
  - 保存するデータに関するアクセスコントロールを考慮する。
  - 利用者によるデータ操作(直接操作、アプリケーション経由の操作等)を考慮する。
  - プログラムに対するアクセスコントロールを考慮する。
  - データの流れに対するアクセスコントロールを考慮する。
  - 安全性が確保されたゾーン内では集約を考慮する。
- 証跡管理
  - 証跡の正確性を確保するため、時刻合わせについて考慮する。
  - 証跡の法的有効性を確保するため、署名とタイムスタンプの付与について考慮する。
  - 運用性を考慮し、証跡は統合管理する。
- 集中管理
  - 脆弱性に関する修正は、常に最新状態を保つことを考慮する。
  - IT システムに加えられる変更処理は、すべて構成管理対象とする。
- 暗号
  - クライアント PC 単体の暗号化は行わない。
  - クライアント PC から業務処理を行う場合に送付する利用者情報は、暗号化する。
  - Web サーバから認証サーバへ送付する利用者情報は、暗号化する。
  - ファイアーウォールの内側の安全性が確保されたゾーンに存在するサーバ間の通信は、暗号化しない。

■ 認証・アイデンティティマネジメント機能の実装

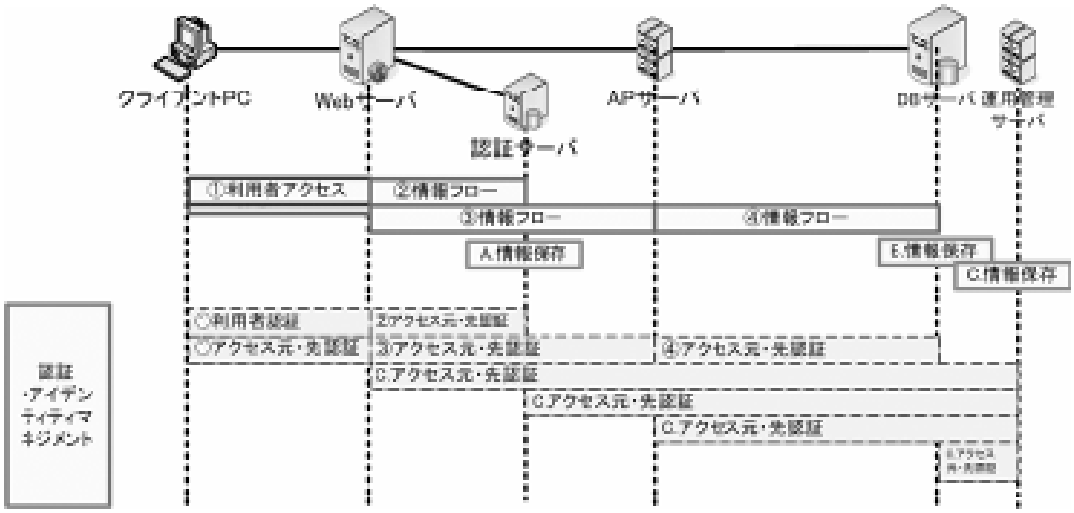


図 12.6-3 認証・アイデンティティマネジメントにおける機能実装

- クライアント PC

  本モデルでは、すべての業務資産を DB サーバに保管します。クライアント PC には情報を保存しません。このため、クライアント PC には強固な認証・アイデンティティマネジメントの仕組みは必要ありません。ただし、想定外利用者による利用を避けるため、利用者を限定した ID 管理機能は必要です。

- クライアント PC、Web サーバ間

  クライアントPCからのなりすましを防止するためにアクセス元とアクセス先の機器間の認証を行います。このため、通信にはSSLクライアント認証方式を使用します。SSLクライアント認証方式を使用することで、通信路の安全性、およびなりすましの防止を行うことができます。また、SSL 通信は暗号化にも利用でき、費用も比較的安価です。

- Web サーバ

  Web サーバ単体で保持するユーザアカウントは、管理者アカウントのみとします。業務で利用するユーザアカウントはすべて認証サーバで一括管理し、Web サーバはクライアント PC から認証依頼を受け付け、認証サーバへ認証の依頼を行います。

- Web サーバ、認証サーバ間

  クライアント PC から受け取ったユーザアカウントと認証情報を基に、LDAP などの認証サーバへ認証依頼を行い、認証サーバから得る認証成功、不成功の情報を基に、処理を続行します。

- 認証サーバ

  ユーザアカウントの管理が分散していると、サーバごとに管理者が必要となったり、メンテナンスにサーバ台数分の時間がかかったりします。また、認証情報の管理が複数となり、セキュリティ事故を招く恐れもあります。このため IT システム利用者のユーザアカウントは、認証サーバで一括管理します。職務と職責の分離の原則はセキュリティの基本であるため、確実に実施します。また、集約配備を考慮し、すべての認証は Web サーバから受け付け、認証の結果を Web サーバに返却します。認証が成功した場合は、当該ユーザアカウントが持つ権限情報とともに Web サーバに返却します。ただし、各サーバの管理者アカウントは各サーバで管理します。

- Web サーバ、AP サーバ間

  Web サーバ、AP サーバ間で相互認証を行います。

  相互認証は、Web サーバ、AP サーバが業務サーバゾーンに存在すること、認証サーバで正しく認証されたユーザアカウントが AP サーバ上のプログラムを起動することを前提に、サーバ間の IP アドレス認証とします。集約配備を考慮するためには、何らかの方法でサーバ間の相互認証の実装が必要です。

- AP サーバ

  AP サーバ単体で保持するユーザアカウントは、アプリケーション実行用のユーザ、管理者アカウントのみとします。業務で利用するユーザアカウントは、すべて認証サーバで一括管理します。

- AP サーバ、DB サーバ間

  AP サーバ、DB サーバ間で相互認証を行います。

  相互認証は、AP サーバ、DB サーバがそれぞれファイアーウォールの内側の信頼性が確保された場所に存在すること、認証サーバで正しく認証されたユーザアカウントが AP サーバ上のプログラムを起動することを前提に、サーバ間の IP アドレス認証とします。

- DB サーバ

  DB サーバ単体で保持するユーザアカウントは、AP サーバ上のプログラムが接続しデータ操作をするための DB ユーザアカウント、管理者アカウントのみとします。データの修正は、AP サーバから実施します。DB サーバ上からは、データの操作ができないようにします。

- 運用管理サーバ

  運用管理サーバ単体で保持するユーザアカウントは、管理者アカウントのみとします。運用業務で利用するユーザアカウントは、すべて認証サーバで一括管理します。

- 各サーバ、運用管理サーバ間

  各サーバ、運用管理サーバがそれぞれファイアーウォールの内側の信頼性が確保された場所に存在すること、認証サーバで正しく認証された運用管理ユーザアカウントが証跡を送信するということを前提に、各サーバと運用管理サーバ間は IP アドレス認証を行います。

■ アクセスコントロール機能の実装

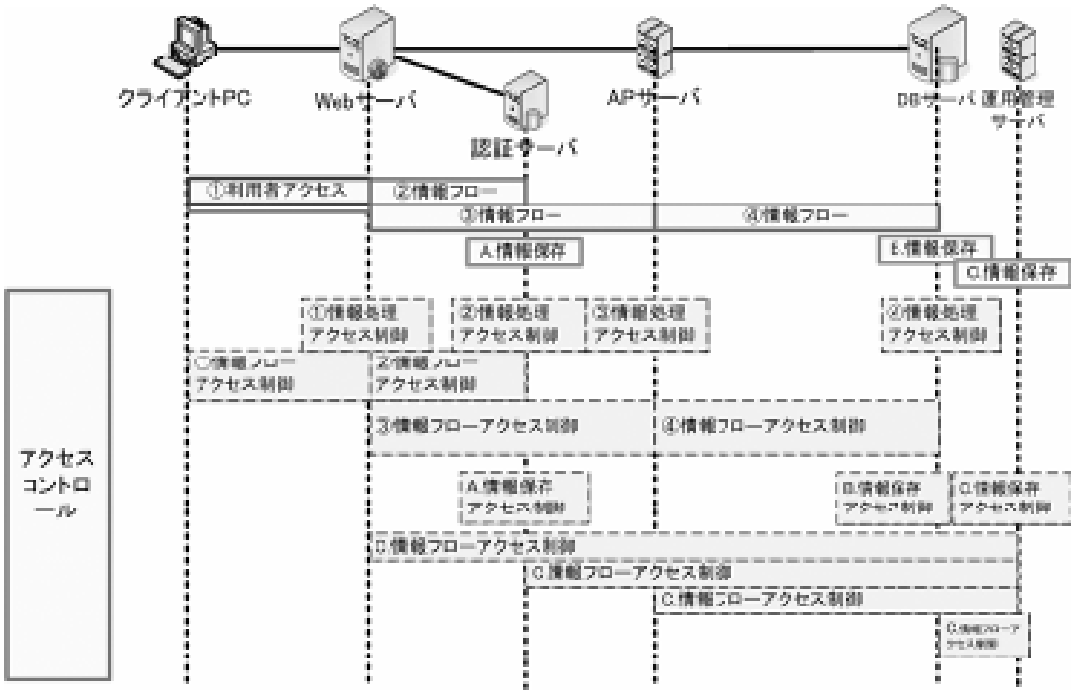


図 12.6-4 アクセスコントロールにおける機能実装

- クライアント PC

  情報をローカルに保存しないため、ファイルシステムへの書き込みは強固にコントロールしません。

- クライアント PC、Web サーバ間

  クライアント PC からのログイン要求、業務処理結果のクライアント PC への送付など、クライアント PC との通信時の安全性を確保するためには、意図した利用者のみとの通信を確立することが重要です。このため、SSL クライアント認証を使用し、意図しない者からのアクセスをコントロールします。

- Web サーバ

  Web サーバの OS レベルのアクセスコントロールは、運用性を考慮し、任意アクセスコントロールとします。

  Web サーバ上のアクセス管理対象は、プログラム、処理中の業務データ、ログ、管理者アカウント情報とします。

  サーバの管理者による特権を使用しての業務処理や不正な操作をできなくするため、管理者のアカウントからは、業務データの更新、業務アプリケーションの処理操作、およびログ更新の権限を外します。

- Web サーバ、認証サーバ間

  通信路のアクセスコントロールは、認証・アイデンティティマネジメントの機能で意図したアクセスをコントロールするため、実装項目はありません。

- 認証サーバ

  認証サーバの OS レベルのアクセスコントロールは、運用性を考慮し、任意アクセスコントロールとします。

  認証サーバ上のアクセス管理対象は、プログラム、ユーザアカウント情報、管理者アカウント情報とします。

  サーバの管理者による特権を使用しての業務処理や不正な操作をできなくするため、サーバ管理者のアカウントからは、ユーザアカウント情報の操作権限、ログの更新権限を外します。

- Web サーバ、AP サーバ間

  Web サーバ、AP サーバが、業務サーバゾーンに存在するため、サーバ間の相互認証を前提に、Web サーバを経由し認証サーバで行われる認証行為の結果で得られる権限を引き継ぎます。

- AP サーバ

  AP サーバの OS レベルのアクセスコントロールは、運用性を考慮し、任意アクセスコントロールとします。

  AP サーバ上のアクセス管理対象（オブジェクト）は、プログラム、処理中の業務データ、ログ、管理者アカウント情報とします。

サーバの管理者による特権を使用しての業務処理や不正な操作をできなくするため、サーバ管理者のアカウントからは、業務データの更新、業務アプリケーションの処理操作、およびログ更新の権限を外します。

- AP サーバ、DB サーバ間

  業務サーバゾーンと、機密サーバゾーンは、それぞれファイアーウォールの内側の安全性が確保された中に存在するため、サーバ間の相互認証を前提に、Web サーバを経由し認証サーバで行われる認証行為の結果で得られる権限を引き継ぎます。

- DB サーバ

  DB サーバの OS レベルのアクセスコントロールは、運用性を考慮し、任意アクセスコントロールとします。

  DB サーバ上のアクセス管理対象は、業務取引データ、業務マスターデータ、ログ、ユーザアカウント情報、管理者アカウント情報とします。

  サーバの管理者による特権を使用しての業務処理や不正な操作をできなくするため、管理者のアカウントからは、業務データの更新、およびログ更新の権限を外します。

- 運用管理サーバ

  収集した証跡は、改ざんを防止するため、管理者を含めて更新・削除ができないようにします。

- 各サーバ、運用管理サーバ間

  すべてのサーバは、ファイアーウォールの内側の安全性が確保されたゾーンに存在するため、サーバ間の相互認証を前提に、Web サーバを経由し認証サーバで行われる認証行為の結果で得られる権限の設定を引き継ぎます。

■ 証跡管理機能の実装

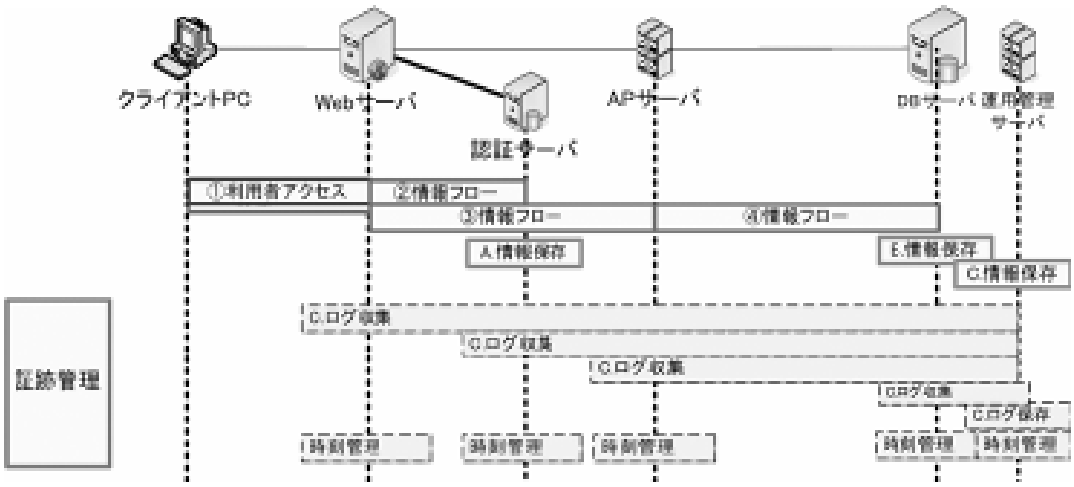


図 12.6-5 証跡管理における機能実装

- クライアント PC

  起動ログ、ログイン認証ログ、セキュリティ監査ログを取得します。

  また、業務処理に関する証跡は、運用管理サーバで一括管理します。クライアント PC では業務処理を実施しないため、特にログを取得する必要はありません。

- クライアント PC、Web サーバ間

  通信部分のログは、通信路両端のリソース上で取得するため、実装項目はありません。

- Web サーバ

  Web サーバは企業内の NTP サーバ、または日本標準時サーバの時刻と自動同期します。同期の間隔は、システム稼働までの間に平均誤差を集計し、間隔を決定します。

  証跡は、コントロール状況把握型（C 型）、セキュリティ不正検知型（D 型）、セキュリティ追跡性確保型（T 型）に属する Web サーバ上で発生するすべてのイベント事象を収集します。具体的な取得対象ログは、第 7 章「証跡管理」を参照ください。

  収集したログは、サーバ証明書に対応する秘密鍵を使用してデジタル署名、タイムスタンプを付与し、ログ管理機能を経由して運用管理サーバへ送信します。

- Web サーバ、認証サーバ間

  通信部分のログは、通信路両端のリソース上で取得するため、実装項目はありません。

- 認証サーバ

  認証サーバは企業内の NTP サーバ、または日本標準時サーバの時刻と自動同期します。同期の間隔は、システム稼働までの間に平均誤差を集計し、間隔を決定します。

  証跡は、コントロール状況把握型（C 型）、セキュリティ不正検知型（D 型）、セキュリティ追跡性確保型（T 型）に属する AP サーバ上で発生するすべてのイベント事象を収集します。具体的な取得対象ログは、第 7 章「証跡管理」を参照ください。

  収集したログは、サーバ証明書に対応する秘密鍵を使用してデジタル署名、タイムスタンプを付与し、ログ管理機能を経由して運用管理サーバへ送信します。

- Web サーバ、AP サーバ間

  通信部分のログは、通信路両端のリソース上で取得するため、実装項目はありません。

- AP サーバ

  AP サーバは企業内の NTP サーバ、または日本標準時サーバの時刻と自動同期します。同期の間隔は、システム稼働までの間に平均誤差を集計し、間隔を決定します。

  証跡は、コントロール状況把握型（C 型）、セキュリティ不正検知型（D 型）、セキュリティ追跡性確保型（T 型）に属する AP サーバ上で発生するすべてのイベント事象を収集します。具体的な取得対象ログは、第 7 章「証跡管理」を参照ください。

  収集したログは、サーバ証明書に対応する秘密鍵を使用してデジタル署名、タイムスタンプを付与し、ログ管理機能を経由して運用管理サーバへ送信します。

- AP サーバ、DB サーバ間

  通信部分のログは、通信路両端のリソース上で取得するため、実装項目はありません。

- DB サーバ

  DB サーバは企業内の NTP サーバ、または日本標準時サーバの時刻と自動同期します。同期の間隔は、システム稼働までの間に平均誤差を集計し、間隔を決定します。

  証跡は、コントロール状況把握型（C 型）、セキュリティ不正検知型（D 型）、セキュリティ追跡性確保型（T 型）に属する AP サーバ上で発生するすべてのイベント事象を収集します。具体的な取得対象ログは、第 7 章「証跡管理」を参照ください。

  収集したログは、サーバ証明書に対応する秘密鍵を使用してデジタル署名、タイムスタンプを付与し、ログ管理機能を経由して運用管理サーバへ送信します。

- 運用管理サーバ

  IT システム内で発生したすべての証跡は運用管理サーバに収集し、一括管理します。

- 各サーバ、運用管理サーバ間

  通信部分のログは、通信路両端のリソース上で取得するため、実装項目はありません。

■ 集中管理機能の実装

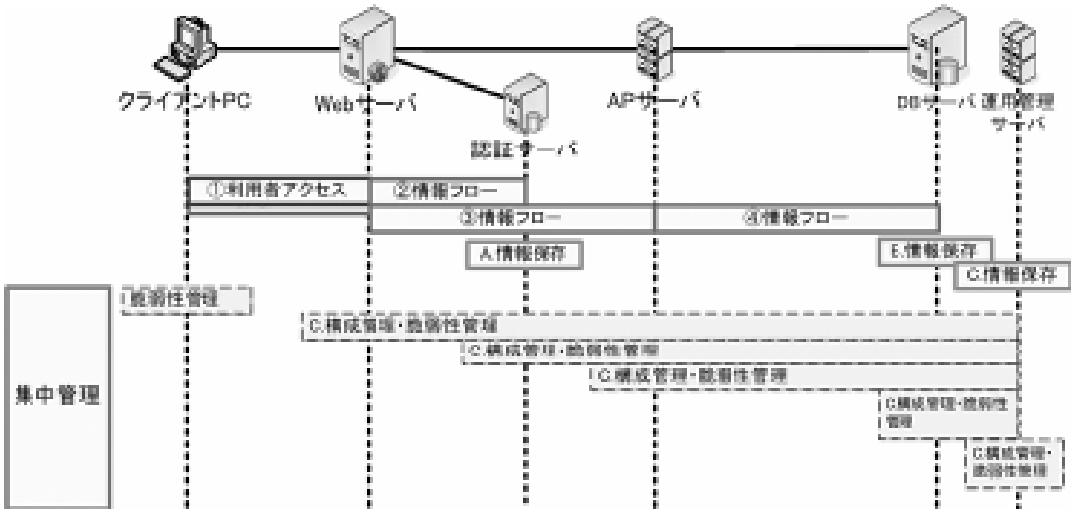


図 12.6-6 集中管理における機能実装

- クライアント PC

  クライアント PC の構成管理は実施しません。ただし、脆弱性管理の中のセキュリティパッチについては、常に最新状態を保つように管理します。

- クライアント PC、Web サーバ間

  クライアント PC と Web サーバの通信部分に関する集中管理への実装項目はありません。

- Web サーバ

  脆弱性管理を実施します。セキュリティパッチは、常に最新状態を保つように管理します。

  セキュリティパッチの適用状況は、構成管理機能を経由して運用管理サーバへ送信します。

- Web サーバ、認証サーバ間

  Web サーバと認証サーバの通信部分に関する集中管理への実装項目はありません。

- 認証サーバ

  脆弱性管理を実施します。セキュリティパッチは、常に最新状態を保つように管理します。

  セキュリティパッチの適用状況は、構成管理機能を経由して運用管理サーバへ送信します。

- Web サーバ、AP サーバ間

  Web サーバと AP サーバの通信部分に関する集中管理への実装項目はありません。

- AP サーバ

  脆弱性管理を実施します。セキュリティパッチは、常に最新状態を保つように管理します。

  セキュリティパッチの適用状況は、構成管理機能を経由して運用管理サーバへ送信します。

- AP サーバ、DB サーバ間

  AP サーバと DB サーバの通信部分に関する集中管理への実装項目はありません。

- DB サーバ

  脆弱性管理を実施します。セキュリティパッチは、常に最新状態を保つように管理します。

  セキュリティパッチの適用状況は、構成管理機能を経由して運用管理サーバへ送信します。

- 運用管理サーバ

  脆弱性管理を実施します。セキュリティパッチは、常に最新状態を保つように管理します。

  セキュリティパッチの適用状況は、構成管理機能で管理します。

- 各サーバ、運用管理サーバ間

  各サーバと運用管理サーバの通信部分に関する集中管理への実装項目はありません。

■ 暗号機能の実装

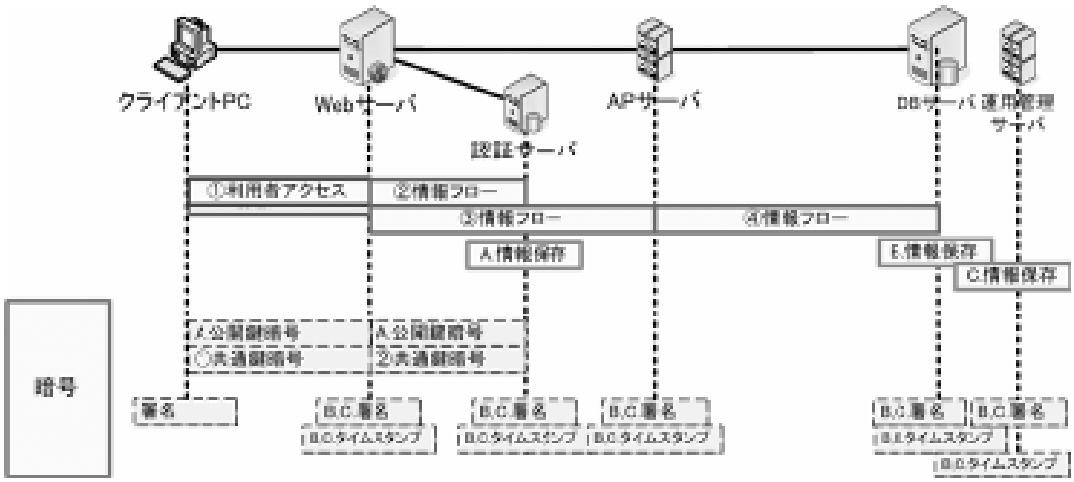


図 12.6-7 暗号における機能実装

- クライアント PC

  クライアント PC には業務データを格納しないため、クライアント PC 単体の暗号化は実施しません。ハードディスク暗号化も必要ありません。ただし、SSL クライアント認証を行うための署名は実施します。

- クライアント PC、Web サーバ間

  画面上で入力した項目を送信する際の機密性、および Web システムから得る情報の機密性を確保するため SSL クライアント認証を利用した暗号通信を行います。企業内部アクセスを考慮する場合には、SSL-VPN により通信経路を暗号化します。

- Web サーバ

  運用管理サーバへ送信する証跡には、法的有効性にかんがみ、署名とタイムスタンプを付与します。

- Web サーバ、認証サーバ間

  クライアント PC からの認証要求で得た認証情報を認証サーバへ送信します。送受信時には、LDAPS 通信を利用して暗号通信を行います。

- 認証サーバ

  ユーザアカウントの情報は、すべて暗号化します。

  また、運用管理サーバへ送信する証跡には、法的有効性にかんがみ、署名とタイムスタンプを付与します。

- Web サーバ、AP サーバ間

  Web サーバ、AP サーバは、業務サーバゾーンに存在するため、盗聴などによる情報漏洩はないものとし、暗号化は行いません。

- AP サーバ

  運用管理サーバへ送信する証跡には、法的有効性にかんがみ、署名とタイムスタンプを付与します。

- AP サーバ、DB サーバ間

  AP サーバ、DB サーバがそれぞれファイアーウォールの内側の信頼性が確保された場所に存在し、また DB サーバへの処理依頼は、AP サーバのアプリケーションユーザのみであることから、通信路は暗号化しません。

- DB サーバ

  DB サーバ（ディスクを含む）は、機密ゾーンに存在するためデータの暗号化は実施しません。ただし、運用管理サーバへ送信する証跡には、法的有効性にかんがみ、署名とタイムスタンプを付与します。

- 運用管理サーバ

  運用管理サーバへ送信する証跡には、法的有効性にかんがみ、署名とタイムスタンプを付与します。

- 各サーバ、運用管理サーバ間

  運用管理サーバは、業務サーバゾーンに存在しますので、通信路は特に暗号化しません。

以上、3 層 Web システムモデルにおける ESA の考え方に基づいたセキュリティ機能の実装を見てきました。

今まで、セキュリティ機能の実装は何を実装してよいか分かりにくいと考えられてきました。これに対し、本章では「集約配備」の考え方、およびその実装例として 3 層 Web システムモデルを使用して実際に着目すべき点を説明してきました。本システムモデルに合致するシステムでは、このまま利用することができますが、ほとんどのシステムには何らかのカスタマイズや機能拡張が必要であったり、全く違うシステム形態であったりすると思います。しかし、どのようなシステム形態にせよ、本モデルで考えた、セキュリティポリシーを損なうことなく集約配備するという考え方が基本です。

12.7 ESA に基づく 3 階層 Web システムモデル実装例（管理者への対策）

一般的に、システム管理者権限はすべての操作を行うことができます。しかし、これは管理者機能が乗っ取られた場合、悪意のある操作を自由に行えるということでもあります。

システム管理者権限を考える場合は、知る必要性に応じた最小特権の付与と合わせて、認証機能をはじめとした強固なセキュリティ機能を考える必要があります。

以下に、管理者機能の視点からのセキュリティ対策についてシステム構成、アクセス関連図、およびセキュリティ対策の全体俯瞰図を示します。

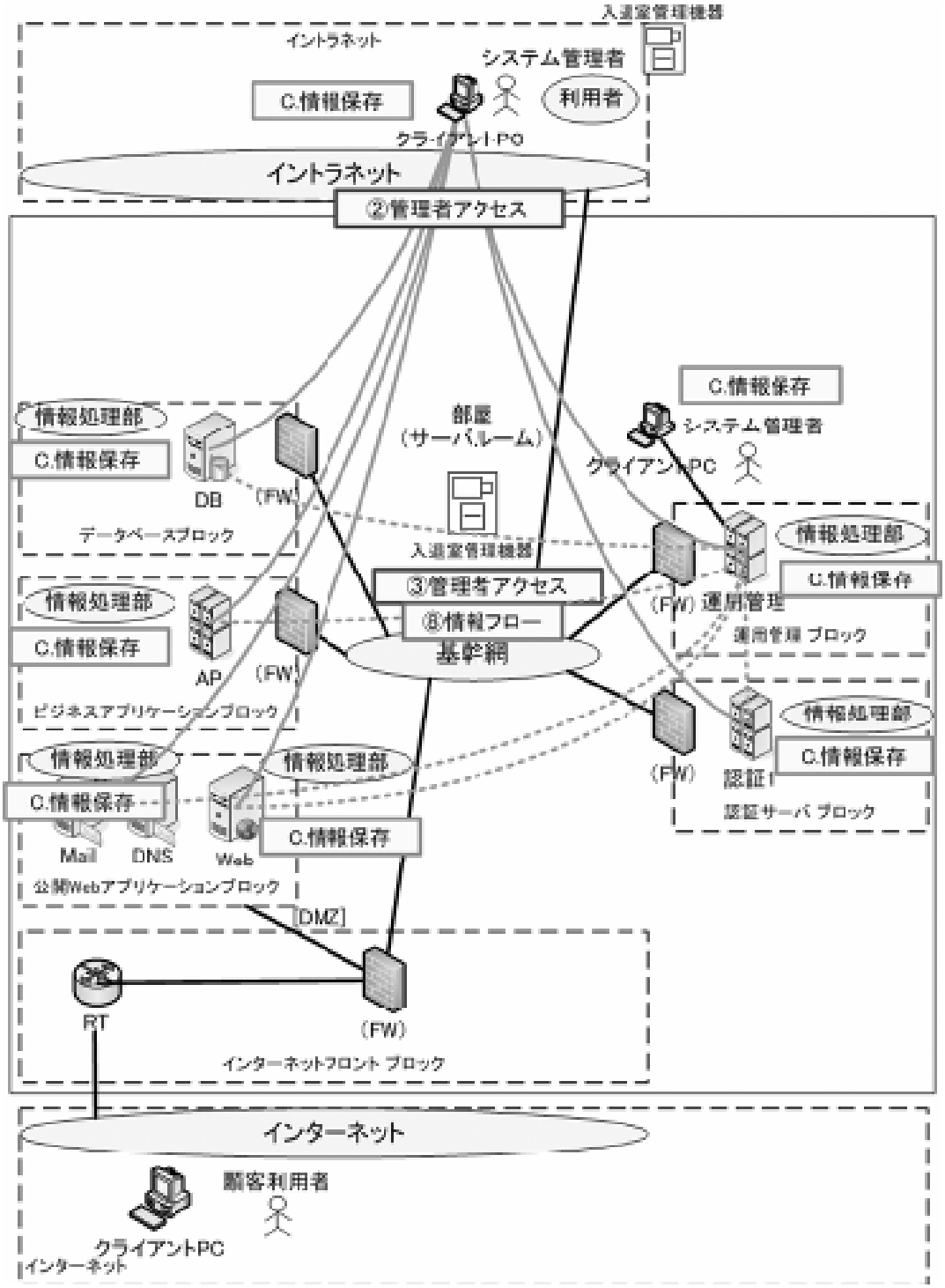


図 12.7-1 3 階層 Web システムモデル（管理者機能：システム構成・アクセス関連図）

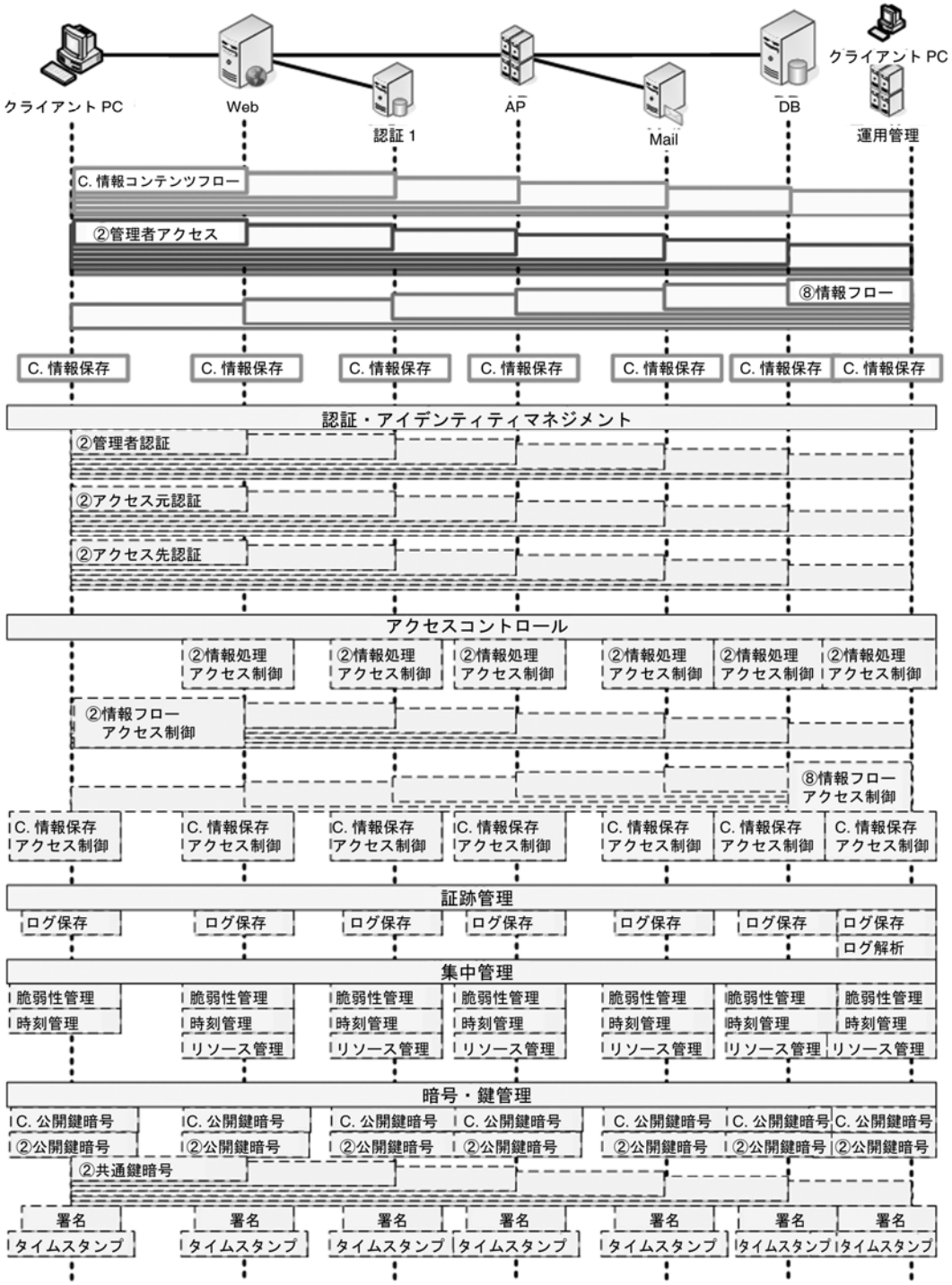


図 12.7-2 3 階層 Web システムモデル（管理者機能：全体俯瞰図）

12.8 ESA に基づくリモートアクセスへの実装例

本節では、企業内システムへのリモートアクセスにおけるセキュリティ対策の実装例について示します。

12.3 節、12.4 節で述べてきた 3 階層 Web システムの情報保存部に格納される機密情報のほか、企業の基幹システムには重要な機密情報が多く保存されています。3 階層 Web システムへセキュリティ対策を実施するのと同様に、企業内システムへのセキュリティ対策はとても重要です。

以下に、リモートアクセスにおけるセキュリティ対策についてシステム構成、アクセス関連図、およびセキュリティ対策の全体俯瞰図を示します。

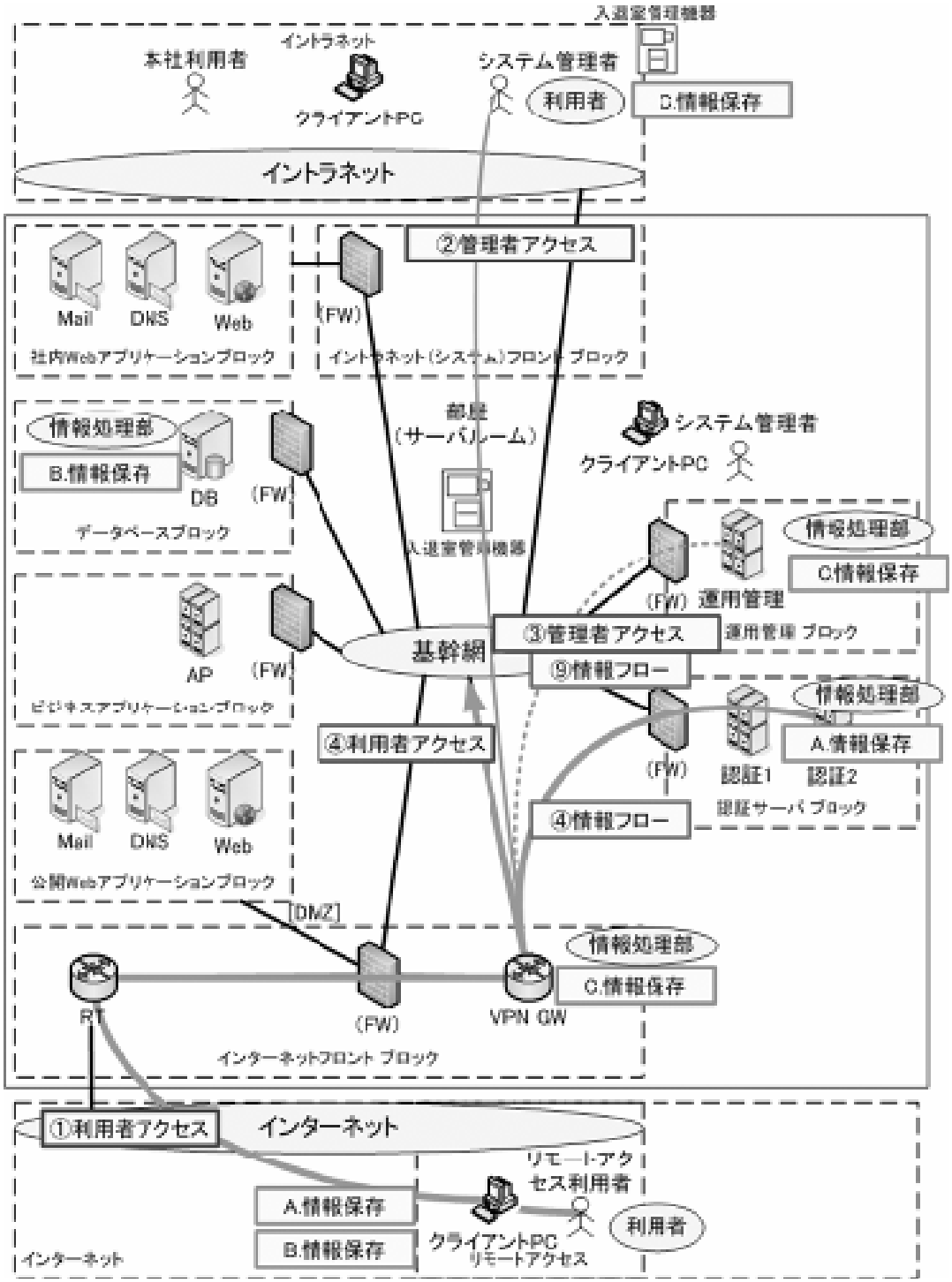


図 12.8-1 企業内システムへのリモートアクセス（システム構成・アクセス関連図）

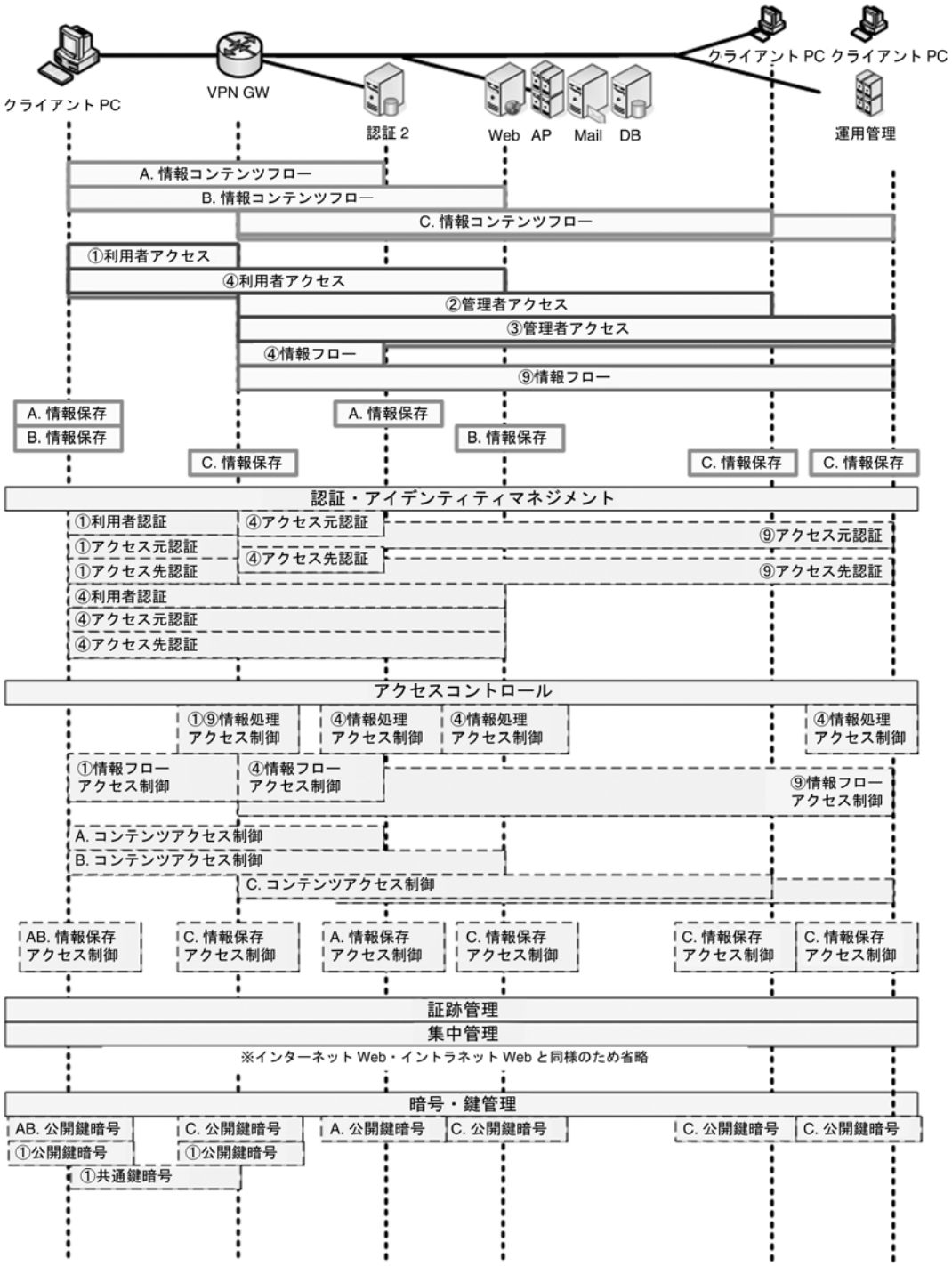


図 12.8-2 企業内システムへのリモートアクセス（全体俯瞰図）

13. システム運用

13.1 システム運用の概要

組織における情報セキュリティ対策を考えるに当たっては、前章までに示した技術的な視点とあわせて、マネジメントの視点を考慮することが重要です。情報セキュリティマネジメントは、セキュリティ機能を持つ IT システムを効果的に活用し、維持していくために、それを取り巻く人や組織がどのように行動しなければならないかを示し、実行する必要があります。

現在、情報セキュリティマネジメントを構築するに当たり、参考となる代表的なフレームワークには、以下のようなものがあります。各フレームワークの詳細は、第四部 14 章の「代表的なフレームワーク」を参照ください。

- 品質保証に関する要求事項として規格化したもの
  - ISO 9000 シリーズ[*22]
- 情報セキュリティマネジメントの基準、および具体的な管理策や実践規範を記述したもの
  - ISO/IEC 27001[*23]
  - ISO/IEC 17799[*24], ISO/IEC 27002[*25]
  - JIS Q 27001[*26], JIS Q 27002[*27]
  - 情報セキュリティ管理基準[*28]など
- 個人情報保護に関する要求事項として規格化したもの
  - JIS Q 15001[*29]
- IT 全般統制（IT ガバナンス）のための実践規範を記述したもの
  - COBIT（Control Objectives for Information and related Technology）[*30]
  - システム管理基準および追補版[*31]など

*22 IISO 9001:2000 Quality management systems -- Requirements 他
*23 ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems – Requirements
*24 ISO/IEC 17799:2005 Information technology -- Security techniques -- Code of practice for information security management
*25 ISO/IEC 17799:2005 を基に、ISO/IEC 27002 として ISO/IEC27000 シリーズに統合予定
*26 JIS Q27001 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項
*27 JIS Q27002 情報技術—セキュリティ技術—情報セキュリティマネジメントの実践のための規範
*28 経済産業省 情報セキュリティ管理基準 http://www.meti.go.jp/policy/netsecurity/law_guidelines.htm
*29 JIS Q15001 個人情報保護マネジメントシステム－要求事項
*30 ISACA 情報システムコントロール協会 東京支部のサイトを参照 http://www.isaca.gr.jp/homepage_j.htm
*31 経済産業省「システム監査基準」、および「システム管理基準 追補版（財務報告に係る IT 統制ガイダンス）（案）」

これらのフレームワークでは、それぞれの管理目的や管理策について述べられています。しかし、管理策を実際の IT システムにどのように実装して管理目的を実現すればよいか、そして、実装した管理策をどのように運用して、IT システムにおける情報セキュリティマネジメントの向上へと結び付けていくかといった部分について具体的に触れられていません。本章では、前章までのシステム構築において管理策を実装した IT システムの運用を記載します。

13.2 本章の目的

■ システム運用における課題

情報セキュリティのマネジメントを行う上で、組織が直面する問題として、システム運用における推進体制や仕組みといったマネジメントの枠組みが存在しない、構築したシステムに必要な運用の内容が分からないといったことが考えられます。こうした問題を解決するために、本章では IT サービスの視点から、システム運用のフレームワークと手引き、およびプロセスの視点から必要な作業への落とし込みの手順を提示します。

■ 本章に期待される効果

本章では、IT システムを効果的に活用し維持していくために必要な「ビジネス」と「IT サービス」という二つの観点から要件を整理します。これにより IT システムのセキュリティ機能やシステムの運用に必要な項目を網羅することが可能となります。また、情報セキュリティのプロセスを整理し、IT システムへの要件対応を可能とします。

13.3 システム運用プロセスの全体像

■ ビジネスの観点から見た情報セキュリティ

IT システムに実装した管理策をどのように運用していくかを考えるためには、ビジネスの観点から見た IT システムにおける情報セキュリティの対策と、それに合った運用の観点が必要です。また、情報セキュリティがどのようにビジネスに寄与したかの評価も重要なポイントです。

組織にはそれぞれ目的があり、ビジネスのプロセスは、こうした目的を達成するためのものです。最近では、ビジネスのニーズを満たすため、IT システムへの依存度はますます増大しています。こうした中で、IT システムに対する情報セキュリティへの要求も、より高度になってきています。

重要なのは、情報セキュリティ対策は、それ自体が目的ではなく、組織の目的を達成するための手段の一つだということです。そのため、情報セキュリティは、組織とそのビジネスの利益を阻害するものであってはなりません。一般に、すべての情報や IT システムの価値が、組織にとって同等というわけではありません。従って、一律に、厳しければよいというものではありません。情報セキュリティのレベルや緊急度は、情報や IT システムの価値に見合うものでなくてはなりません。情報セキュリティ対策とそれに要するコストのバランスを取ること、そして、情報の価値とそれが扱われる環境におけるリスクのバランスを取ることによって、初めてその組織に見合った情報セキュリティ対策とそのマネジメントが実現できます。

IT システムにより情報セキュリティ対策を実現することは、企業にとって IT システムに重要な付加価値を与えることになります。IT システムが適切な情報セキュリティ対策と品質・効率性を備えたワークフローに組み込まれることで、多くの業務が適切で信頼性のある手続きで処理されることになります。これは、企業にとって非常に価値のあることです。情報セキュリティ対策により実現した価値が、ビジネスにどう寄与したかという評価も重要なポイントの一つです。

■ システム運用の位置付け

ビジネスの観点から見た情報セキュリティの視点に基づき、実際のシステムを運用することになります。本章では、組織における ESA に基づいたシステム運用のフレームワーク確立を支援するために、以下の整理を行います。

- ESA における、「コントロール（Control）」、「計画（Plan）」、「導入およびサービスの提供（Implement）」、「監視・測定およびレビュー（Evaluate）」、「継続的改善（Maintenance）」、「報告（Report）」の各プロセスで、必要となる作業を抽出します。
- 各作業における必須要件とセキュリティの機能要素を関連付けます。

本書における本章の位置付けは、図 13.3-1 のとおりとなります。

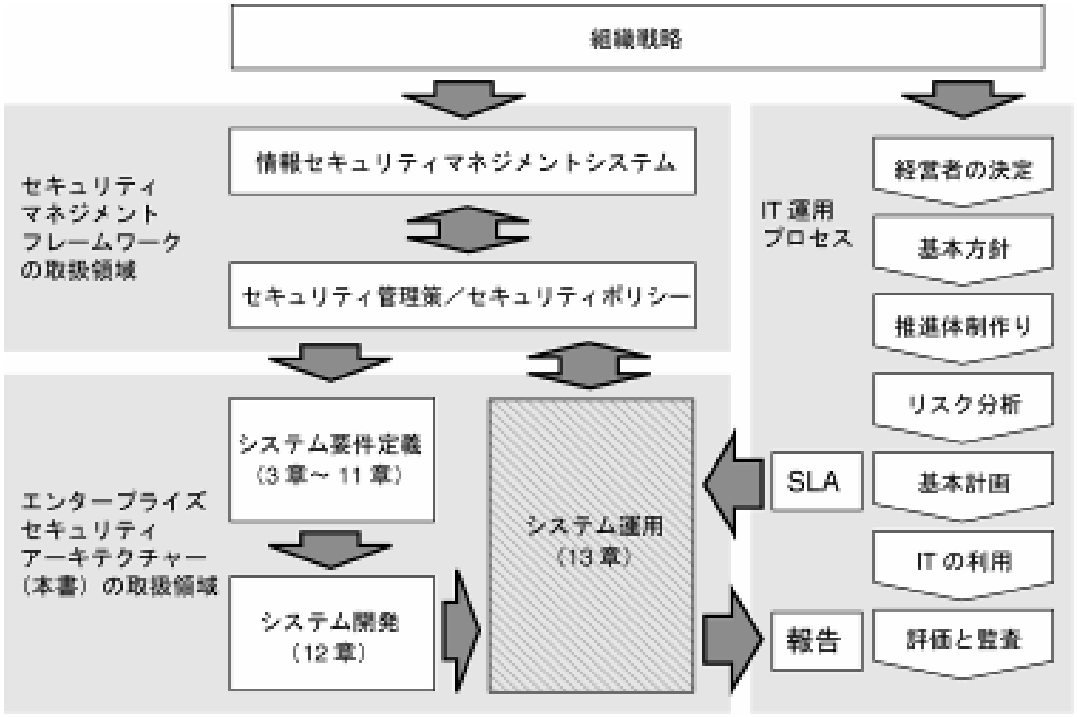


図 13.3-1 本章の位置付け

■ システム運用のフレームワーク

本章では、IT システムとその運用により提供される情報セキュリティのプロセスを、ビジネスのプロセスを支援するための一連のコンポーネントの一部としてとらえます。

例えば、IT システムの運用・管理業務に関する体系的なガイドラインとして知られている ITIL[*32] では、この一連のコンポーネントを「IT サービス」ととらえ、ビジネス戦略と結び付けるため、プロセスアプローチによるベストプラクティスを提供しています。

本章は、この ITIL の「セキュリティ管理」ライブラリに書かれているプロセスを参考に、IT サービスの観点から ESA に求められるシステム運用のフレームワーク[*33] を説明します。

セキュリティへの機能要件は、組織の規模、業種、風土やマネジメントシステムの導入状況などにより異なります。こうしたさまざまな要件に基づいて構築した IT システムや機器において、本章を有効に活用するためには、以降に示すシステム運用のフレームワークを基に自らの組織や運用形態に合わせて、フレームワークの「最適化」を行うことが重要です。

*32 IT Infrastructure Library 詳細は、itSMF Japan のサイト http://www.itsmf-japan.org/itil/index.htm を参照。*7 例えば ISO/IEC 15408-1

*33 フレームワーク（枠組み） 本章では、システムを運用する際に汎用的に適用できるプロセス構造やプロセス間の関係を指します。

13.4 IT サービスにおける情報セキュリティマネジメント

情報セキュリティの対策面から見た情報セキュリティマネジメントの全体プロセスは、図 13.4-1 のようになります。

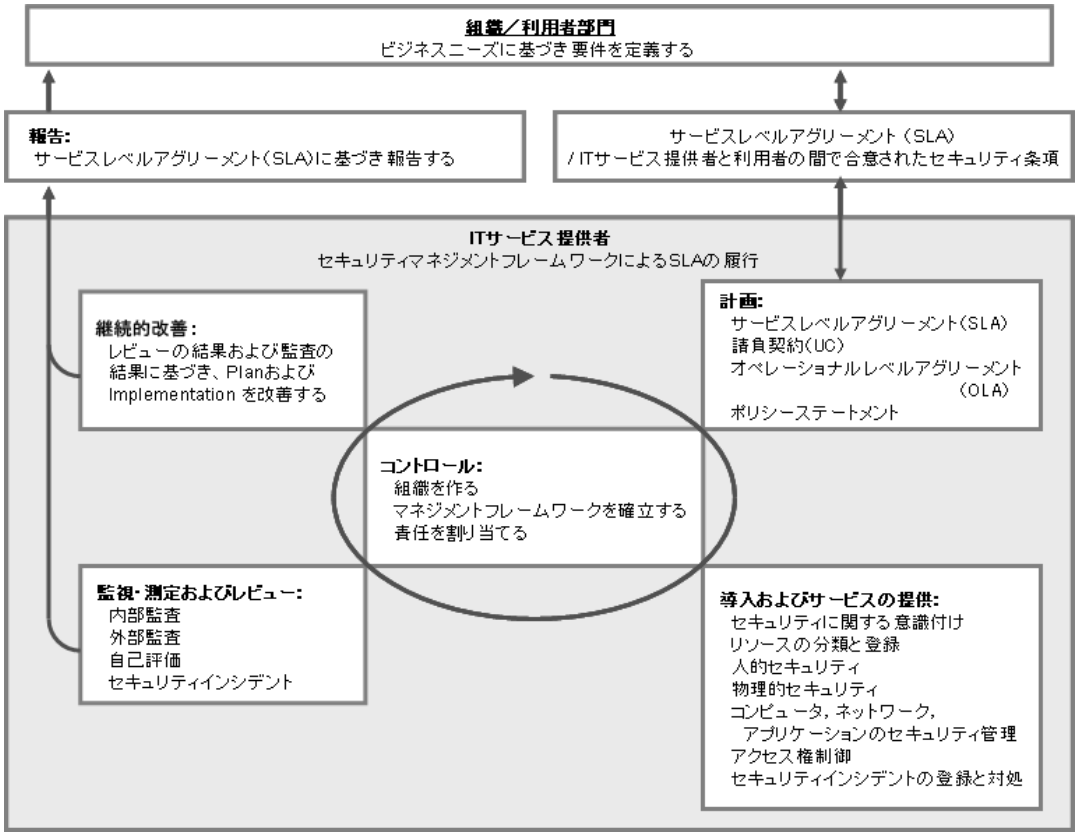


図 13.4-1 セキュリティマネジメントプロセスの全体図[*34]

初めに、IT サービス提供者とサービスの利用者との関係を定義します。このとき、IT サービス提供者とは、組織内の IT サービス部門である場合とアウトソーシングされた IT サービスプロバイダーである場合が考えられます。しかし、どちらの場合にも大きな差異はありません。組織内の IT サービス部門と利用者部門の間で、サービスレベルを合意し、サービスレベルアグリーメント（SLA）[*35]を取り交わすことは、責任を明確にする上で有効です。IT サービス提供者にとって、ビジネスの観点から見た情報セキュリティの基本方針およびリスク分析は、利用者部門の責任となります。利用者部門の情報セキュリティの基本方針とリスク分析の結果から導かれるセキュリティの要件に基づき IT サービス提供者は、「計画」プロセスを実施する

*34 出典：ITIL Security Management
*35 利用者部門に提供するサービスを定量的に定義した正式な協定文書。定量的な定義により、容認可能なサービスのしきい値、サービス提供者が目指すべき目標値、あるいはそれを上回るように努める期待値などの測定基準（メトリックス）を制定しなければならない。

ことになります。

IT 環境における情報セキュリティ管理においても、組織全体および利用者部門におけるプロセスが重要となります。初めに、組織全体および利用者部門が関係するプロセスについて触れます。次に、情報セキュリティ管理において IT サービス提供者が関係するプロセスの概要を示します。

■ 組織全体および利用者部門が関係するプロセス

次の図は、組織全体および利用者部門が関係するプロセスのモデルを示したものです。

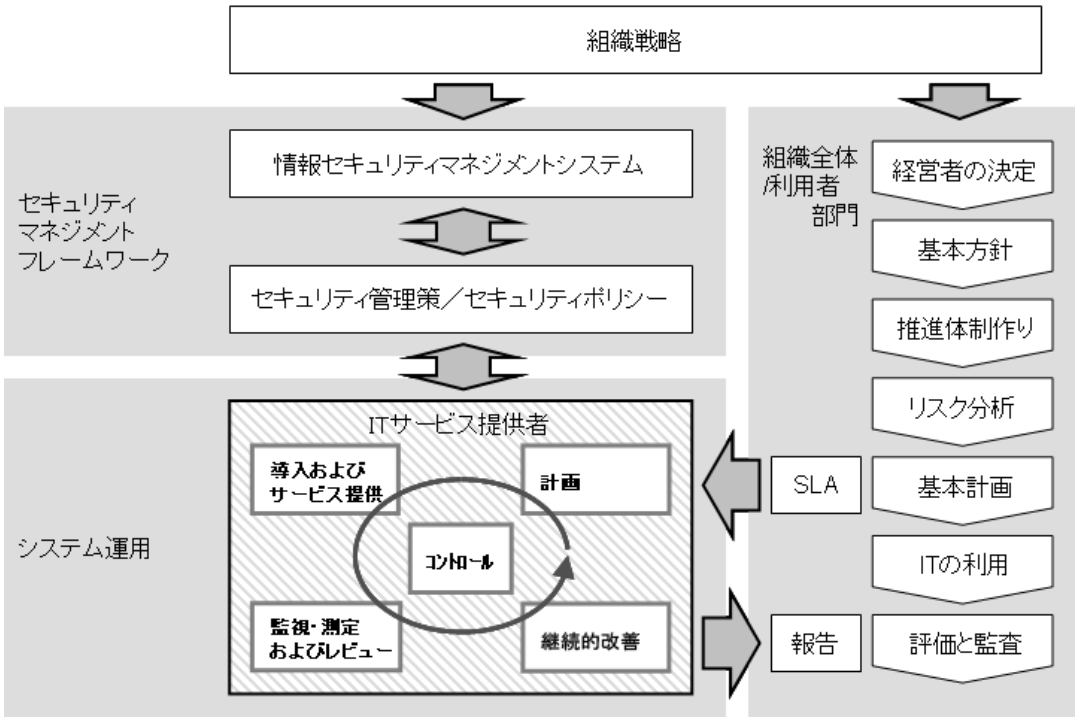


図 13.4-2 ビジネスの観点から見た情報セキュリティマネジメントモデル

組織および利用者部門における主なプロセスは、「経営者の決定」「組織の基本方針」「推進体制作り」「リスク分析」「情報セキュリティ基本計画」「IT の利用」「評価と監査」になります。

情報セキュリティにおいては、経営者の関与が必須です。情報セキュリティに取り組むためには、組織とインフラそれぞれへの投資が伴うため、経営者が情報セキュリティに取り組むことを決定し、強い意志を示すことが実質的な情報セキュリティマネジメント構築の出発点となります。この「経営者の決定」に基づき、推進体制、責任、適用範囲などを記した情報セキュリティの基本方針を定めます。この情報セキュリティの基本方針で、責任と義務と権限を明確にします。この情報セキュリティの基本方針に基づき、「推進体制作り」を行います。

情報セキュリティの基本方針では、大きく「何を」「どのように」「どの程度」守るのかを表明します。具体的に書くべき内容には、以下のようなものがあります。

- 情報セキュリティに関する包括的指針（全般的認識）
- 目標および活動の状況や効果を評価するための指標設定の枠組み
- 情報セキュリティに関する行動の原則
- 組織が守るべき法令、規制、契約などのうち、代表的なもの
- 情報セキュリティマネジメントを構築し、維持するための組織体制
- リスク分析の指針（どのような資産、要件を重視するのか）

情報セキュリティに影響を与える環境の変化として、内部的な要因と外部的な要因があります。内部的な要因は、組織の判断によるものです。外部的な要因は、ビジネスのプロセスが置かれた環境によるものです。これらが、情報セキュリティマネジメントの課題となります。

プロセスの適応が必要となる環境の変化には、以下のようなものが考えられます。

- 業務自体の変更または業務の重要度の変更
- 物理的な変化（例えば、移転など）
- 環境の変化
- IT の利用に関するアセスメントの変更
- ビジネスドメインの変更
- 法的ドメインの変更
- ハードウェアやソフトウェアの変更
- 法的要求事項の変更
- 脅威の変化
- 新しい技術の導入

「リスク分析」では、上記のようなビジネスの置かれた環境の変化にも着目し、情報セキュリティに対するリスクを特定します。この分析により、現在の情報セキュリティに関するステータスと情報セキュリティの品質を明確にすると同時に、実施すべき情報セキュリティ対策を明確にします。これが、現在の状況とあるべき姿になります。なお、リスク分析には、一般的な手法が幾つかあります。その一例を、第四部 15 章「リスク分析の手法（例）」に記載します。

リスク分析の結果を基に、現在の状況からあるべき姿へ移行するための情報セキュリティに関する「基本計画」を作成します。これに基づいて、IT サービス部門とのサービスレベルアグリーメント（SLA）を作成します。

「評価と監査」では、組織および利用者部門は、採用した情報セキュリティ対策が有効かつ効率的に機能しているかをレビューします。このレビューを基に、「計画」と「導入およびサービスの提供」プロセスを見直します。また、このレビューの結果は、組織および利用者部門が実施する「監査」の結果とあわせて、定期的なセキュリティ改善計画の作成やサービスレベルアグリーメント(SLA)の見直しに利用します。

特に、実施している情報セキュリティ対策の有効性および効率性を評価することは、組織および利用者部門の重要な責任となります。これを評価するために測定基準(メトリックス)を定めることが有効です。これに関しては、COBIT 等を参考とすることが有効です。

■ IT サービスの観点から見た情報セキュリティ

IT サービス提供者が関係する主なプロセスは、「コントロール」「計画」「導入およびサービスの提供」「監視・測定およびレビュー」「継続的改善」「報告」の6つのプロセスです。この各プロセスをブレークダウンしたものを、本章ではサブプロセスと呼びます。このサブプロセスごとに運用の具体的な作業に落とし込むことで、必要な項目を網羅できます。

ITIL では、「コントロール」プロセスで、主に組織および利用者部門の情報セキュリティ基本方針、情報セキュリティ基本計画などに基づき、IT サービス提供者における推進体制、各プロセスの責任者などを決定します。

表 13.4-1 「コントロール」プロセスの概要

項	サブプロセス	サブプロセスの内容
(1)	情報セキュリティのための組織体制	□情報セキュリティ推進のための枠組み整備 □責任の割り当て □ITシステムに関する認可プロセス □専門家の支援体制 □独立したチェック □外部の利用者によるアクセスへの対応 □外部委託サービスの契約

ITIL では、「計画」プロセスで、IT サービス提供者のポリシーステートメント、情報セキュリティ実施計画、サービスレベルアグリーメント(SLA)[*36] に対するオペレーショナルレベルアグリーメント(OLA)[*37] や請負契約書(UC)を決定します。

*36 Operational Level Agreement(OLA) IT サービス提供者が所有する内部文書。組織内の各職域間の関係を定義する。(itSMF IT サービスマネジメント用語集より)
*37 Underpinning Contract(UC) IT サービスを利用者部門に提供する場合に役立つ製品やサービスを提供する外部サプライヤとの契約。(itSMF IT サービスマネジメント用語集より)

表 13.4-2 「計画」プロセスの概要

項	サブプロセス	サブプロセスの内容
(1)	ポリシーステートメント	□IT サービス部門のポリシーステートメント作成
(2)	OLA	□OLA(オペレーショナルレベルアグリーメント)の定義と合意
(3)	UC	□UC(請負契約)の定義と合意
(4)	セキュリティ実施計画	□プロファイルの定義 □セキュリティ実施計画の策定

同様に、「導入およびサービスの提供」プロセスで、情報セキュリティ実施計画書に基づき、以下の作業を実施します。

- 情報の分類と割り当て
- IT システムへのセキュリティ機能の実装
- IT システムの運用管理
- 教育
- セキュリティインシデントへの対応
- 定常的なモニタリング

表 13.4-3 「導入およびサービスの提供」プロセスの概要

項	サブプロセス	サブプロセスの内容
(1)	資産分類とコントロール	□資産の管理責任 □資産の分類 □分類の指針
(2)	人的資源のセキュリティ	□職務記述書(JD)[*38] □選考 □機密保持契約 □すべての構成員に対する教育および訓練 □セキュリティインシデントへの対応 □情報セキュリティに関する予兆事象および脆弱性の報告 □懲戒手続き □情報セキュリティの意識向上
(3)	通信および運用管理	□運用の手順と管理責任 □運用手順の文書化 □セキュリティインシデントの管理手順 □職務および職権の分離 □開発環境と運用環境の分離 □外部委託サービスの管理 □情報の取り扱いと受け渡し □ネットワークの管理 □ネットワークに対する要件
(4)	アクセスコントロール	□アクセスコントロールの維持と管理 □利用者部門の責任 □ネットワークのアクセスコントロール □コンピュータのアクセスコントロール □業務アプリケーションのアクセスコントロール □アンチウィルスについてのコントロール方針 □IT システムのアクセスと利用に関するモニタリングと監査

「監視・測定およびレビュー」プロセスで、内部監査および外部監査や自己評価などを実施し、評価レポートを作成します。

*38 Job Description(JD) ある職務に関し、合意された内容を記述した文書。(itSMF IT サービスマネジメント用語集より)

表 13.4-4 「監視・測定およびレビュー」プロセスの概要

項	サブプロセス	サブプロセスの内容
(1)	評価の実施	□IT システムの正しい活用 □セキュリティポリシーとスタンダードの遵守状況の確認 □法的要求事項の遵守状況の確認 □技術的要件との適合性確認 □IT システムの監査 □監査ツールの保護

「継続的改善」プロセスで、「監視・測定およびレビュー」プロセスの結果である評価レポートを分析し、セキュリティ改善計画の作成や改善活動の実施、サービスレベルアグリーメント(SLA)の見直しに反映します。

表 13.4-5 「継続的改善」プロセスの概要

項	サブプロセス	サブプロセスの内容
(1)	評価分析、計画と改善活動, SLA 見直しへのインプット	□評価レポートの分析 □セキュリティ改善計画の作成と改善活動の実施 □SLA 見直しへの反映

「報告」プロセスで、組織全体および利用者部門への報告になります。実施計画、対策の実装状況に関する定期報告、モニタリングに関する報告、特別に報告が必要なイベントなどが含まれます。

表 13.4-6 「報告」プロセスの概要

項	サブプロセス	サブプロセスの内容
(1)	報告の実施	□「計画」の活動におけるレポート □「実装」の活動における定期的なレポート □「評価」の活動における、および活動以外でのレポート □特別に報告が必要なイベント

13.5 サブプロセスの具体例

ここでは、サブプロセスから運用の具体的な作業への落とし込みについて、具体的な内容を例示します。運用を設計する場合には、前述の各サブプロセスに沿って、以下のようにブレークダウンをするとよいでしょう。

例えば、ISO/IEC27002 や ITIL などのベストプラクティスを基準に、基準と対比しながら具体的な作業へ落とし込む手法があります。このような手法をベースラインアプローチと言います。本書の別冊「富士通規準セキュリティポリシー 2007」を、基準として使用することもできます。

ここでは、ITIL のベストプラクティスを基に、「コンピュータのアクセスコントロール」について例示します。

■ コンピュータのアクセスコントロール

- 目標
  - 情報の機密性を保護するために、情報と IT システムへの許可されていないアクセスを防止します。
  - 情報または IT システムを未許可で変更することを防止します。
  - 許可されていないアクセスによる、情報または IT システムの損害および破壊から守ります。
  - 通常の運用環境における混乱を防止します。
- 具体的な作業
  - すべてのワークステーションとターミナルを識別して、認証してください。
  - 最小限の情報が提供される標準的なログオン手続きを強制的に使用するようにしてください（例えば、システムの種類や組織名の詳細を提供しないなど）。
  - 常に、利用者を識別して、認証してください。監査のためには、IT システムにおける処理が、実際の人と結び付いている必要があります。例えば、パスワード、スマートカードまたは認証デバイス（ハードトークン）などを基に識別が可能です。
  - 強制アラーム：重要な IT 資産の場合には、強制アラームの実装を考慮してください。これを実装することで、認可された利用者が、やむを得ず操作を行っているかどうかが明確になります。
  - 自動タイムアウト：一定時間以上操作が行われなかった場合に、自動タイムアウト機能により、ワークステーションまたは利用者を自動的にログオフするか、接続中のセッションを切断してください。
  - 利用時間の制限：IT システムの利用を、通常の利用時間（例えば 8:00 時から 19:00 時まで）に制限してください。
  - あらかじめ定めた回数以上、アクセスを失敗した場合には、アクセスをロックアウトしてください。

- 外部から接続する利用者については、認証デバイス（ハードトークン）やスマートカード、チャレンジ・レスポンス方式などにより、厳しいログインチェックを行ってください。
- なりすましの脅威を排除し、確実な本人認証を行わなければならない場合には、二要素認証を採用してください。
- 認証デバイス（ハードトークン）を本人に渡す場合には、必ず適切な本人確認を行った上で付与しなければなりません。この運用に問題があると重大な脆弱性となるため、特に注意が必要です。
- 認証方式は、保護しなければならないデータ、扱う業務の機密性の程度によって、適切な認証方式を選択してください。
- 特に大規模組織の場合、退職などにより、データ・業務の利用資格を失った場合には、自動的に ID を削除する運用を確立しなければなりません。
- 長期間、ログインした履歴のない ID は、ログイン資格を一時凍結したり削除したりする運用を行う必要があります。
- ログインした日時とログアウトした日時は、監査証跡として認証システム（または、SSO システム）が必ず採取しなければなりません。
- ベーシック認証による認証方式を採用する場合には、以下のパスワードポリシーを利用者に強制してください。このためには、パスワードポリシーを管理する機能の利用が有効です。
- 8 文字以上のパスワード
- 英数字のみのパスワードや同じ文字、単純な順列の文字列によるパスワードの禁止（特殊文字を必ず1文字以上入れること）
- ID と同一のパスワードや利用者から推測可能なパスワードの禁止
- 定期的にパスワードの変更を強制すること。その際、世代を連続しての同一パスワード設定を認めないポリシー強制を自動化ですること。

また、このサブプロセスに関連する IT 資産およびセキュリティ機能と要件を、以下のような表に整理しておくことで、それぞれの作業においてどんな点を考慮する必要があるかを明確にすることができます。

- 関連する IT 資源

例えば、コンピュータへのアクセスコントロールに関連するIT資源として、人、アプリケーション、テクノロジが挙げられます。

IT 資源	
✓	人
✓	アプリケーション
✓	テクノロジ
	設備
	データ

✓ 該当

- 関連する機能

同様に、関連するセキュリティ機能として重要なものは、「認証とIDM」および「アクセスコントロール」が挙げられます。また、「証跡管理」および「集中管理」によりアクセスコンロトールに対する機能を補完します。

セキュリティ機能	
P	認証と IDM
P	アクセスコントロール
S	証跡管理
S	集中管理
	暗号
	物理セキュリティ

(P)主, (S)従

- 関連する要件

コンピュータへのアクセスコントロールに対応する要件は、主に機密性と完全性となります。これを考慮した運用を実施する必要があります。

セキュリティ要件	
P	機密性
P	完全性
	可用性

(P)主, (S)従

13.6 IT サービスにおける他のプロセスとの関係

12.3.2 項にて説明した各プロセスは、IT サービスを提供するために必要な他のプロセスとの関係が重要です。これは、IT サービスを提供する上でのあらゆるプロセスは、セキュリティを考慮する必要があることを指しています。本項では、ITIL で提示されているプロセスを例に、それら考慮すべき点について説明します。こうした点への考慮は、8 章で述べた「集中管理」の機能を利用することで効果的な運用が可能です。

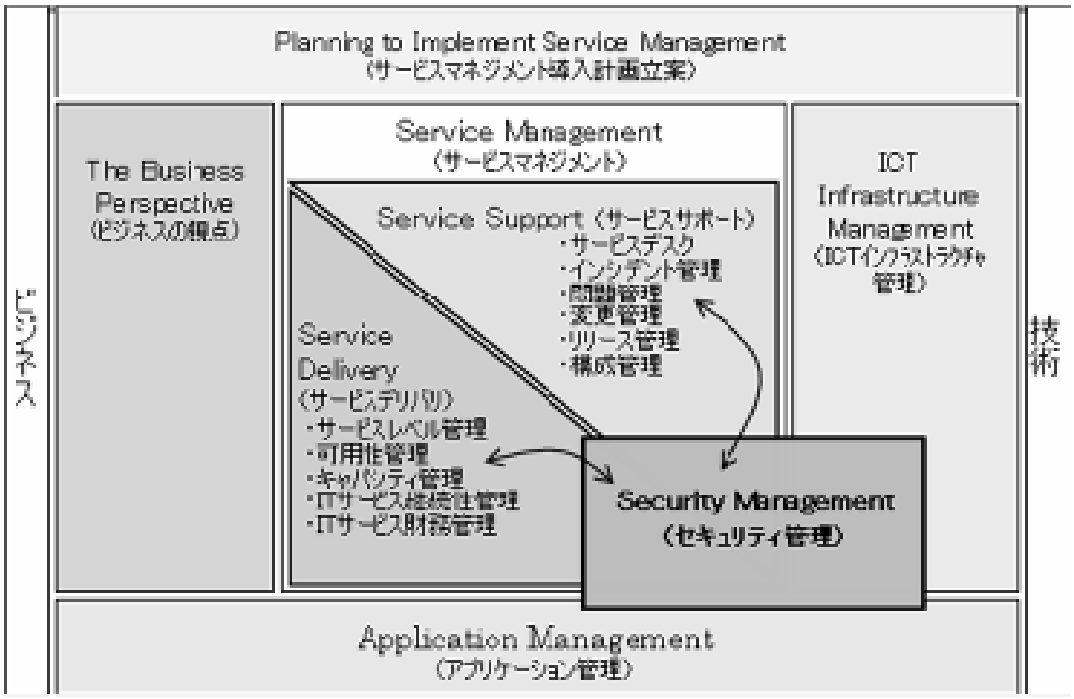


図 13.6-1 ITIL のライブラリ体系図(セキュリティ管理の位置付け)*39

図 13.6-1 は、ITIL のライブラリ体系におけるセキュリティマネジメントの位置付けを示したものです。セキュリティマネジメントが最も密接に関係しているのは、サービスサポート、サービスデリバリにおける次のプロセスです。

*39 出典 itSMF Japan 発行「IT サービスマネジメント」

サービスサポート	インシデント管理 問題管理 変更管理 リリース管理 構成管理
サービスデリバリ	サービスレベル管理 可用性管理 キャパシティ管理 IT サービス継続性管理

これらのプロセスが、セキュリティマネジメントとどのように関係しているかを、各プロセス自身の説明を含め、説明します。

■ インシデント管理

セキュリティインシデントは、通常のインシデントとは異なった対応手順を適用する場合が多いため、両者を識別／分類できることが必要不可欠です。SLA で定めるセキュリティ要件の達成を妨げるかもしれないインシデントはすべてセキュリティインシデントと分類されますので、あらかじめ、セキュリティインシデントと見なされるインシデントの定義を SLA に明記しておくことをお勧めします。

また、セキュリティインシデントは、緊急性やインパクトの程度が高いことが多く、インシデント自体の機密性も考慮する必要があることから、その連絡手順（組織の階層的エスカレーション方法など）やインシデントへの記載内容をあらかじめ決定し、組織内に周知・徹底しておくことが重要です。セキュリティインシデントへの記載事項には、例えば以下のようなものがあります。

- インシデント番号、インシデント発行日時
- インシデント発生日時
- 報告者に関する詳細情報（例外として匿名での報告を認めるか否かも記載しておく）
- インシデント件名
- インシデントの詳細内容
- インパクト（損害額の見積もりなど）
- 緊急度
- インシデントの発生部門、または発見部門
- 影響範囲（システム、機器, 設備など）

- 報告元の連絡先
- エスカレーション状況
- 解決策

セキュリティインシデントを考慮する際に重要となるのが、7 章の「証跡管理」で述べた「セキュリティ不正検知型（D 型）」の証跡です。この証跡をどう扱うかが、情報セキュリティに関するインシデント管理の要点となります。

■ 問題管理

問題管理の主な目的は、問題における根本原因を究明することです。セキュリティインシデントが問題として認識された場合、問題解決に向けた活動を開始させることが必要です。注意しなければならないのは、セキュリティの問題発生そのものが組織に大きな打撃を与える可能性があるため、関係者を絞り込む必要があります。

また、問題や既知のエラーに対する解決策やワークアラウンド[*40]は、新たなセキュリティの問題を起こさないように常にチェックすることが重要です。情報セキュリティに関する問題を考慮する際に重要となるのが、9 章の「証跡管理」で述べた「コントロール状況把握型（C 型）」の証跡です。また、「セキュリティ追跡性確保型（T 型）」の証跡の検証が必要となる場合があります。これらの証跡の扱いが、情報セキュリティに関する問題管理の要点となります。

■ 変更管理

変更管理では、日常的な運用においてセキュリティを考慮すべきです。これは、通常の変更処理が行われる場合には、常にセキュリティに関係した問題が発生する可能性があるからです。このため、変更諮問委員会（CAB）[*41]には、セキュリティ管理者および利用者部門のセキュリティ責任者を含める必要があります。

また、セキュリティ対策を含んだ変更が行われる場合、通常の機能テストとは異なった観点でのテストが必要です。通常の機能テストでは、定められた機能が使えるかを確認しますが、セキュリティ対策を含んだテストでは、セキュリティ機能の可用性だけでなく、セキュリティを低下させる望ましくない機能がないことも確かめます。

*40 顧客が障害の原因とされる構成アイテム（CI）に左右されない暫定的な処置、または手法を実行する、インシデントや問題の回避：Work-around （itSMF IT サービスマネジメント用語集より）
*41 インパクトの大きい変更要求（RFC）すべてに関して、事業および技術的観点から評価を行う権限のある代表者のグループ RFC の優先順位に関する変更管理（CM）への助言、変更の実装に必要なリソースの割り当てに関する提案などを行う。 Change Advisory Board （itSMF IT サービスマネジメント用語集より）

■ リリース管理

リリース管理は、新しいバージョンのソフトウェア、ハードウェア、データ通信機器などの投入をコントロールします。このプロセスでは、以下のことを保証します。

- 正しいハードウェアやソフトウェアが使われている。
- ハードウェアやソフトウェアは使う前にテストを受けている。
- 導入は変更によって正しく許可されている。
- ソフトウェアは合法的なものである。
- ソフトウェアはウィルスに感染しておらず、配布時にウィルスが紛れ込むことはない。
- バージョン番号が分かっており、構成管理により構成管理データベース(CMDB)[*42]に記録されている。
- 投入は効果的に管理されている。

テストや受け入れ時には、SLA で定義されているセキュリティ要件や対策に基づいたセキュリティ面を考慮することが重要です。

■ 構成管理

構成管理は、構成アイテム(CI)[*43]の分類を行うことができるため、構成管理は情報セキュリティにとって最も関係のあるプロセスです。CI の分類は、必要な機密性、完全性、可用性を示すものとなります。この分類は SLA のセキュリティ要件に基づいており、利用者部門が分類を決定します。また、各分類レベルに応じたセキュリティ対策を SLA で定義することができます。

分頼の仕組みは常に利用者部門の体制に合わせて作られているべきです。しかし、管理を簡単にするため、IT システムを利用する複数の利用者部門がある場合でも、分類の仕組みを統一することが勧められます。

■ サービスレベル管理

サービスレベル管理の主な目的は、提供するサービスのレベルを SLA に合わせ最適化することです。サービスレベル管理には、数多くのセキュリティ関連の活動があり、この中でセキュリティ管理は重要な役割を果たします。主な活動は、以下の 6 点です。

*42 各構成アイテム(CI)の属性および履歴についての詳細、および CI 間の重要な関係の詳細を格納するデータベース。Configuration Management Database (itSMF IT サービスマネジメント用語集より)
*43 IT インフラストラクチャーのコンポーネントを指す。SLA や変更要求などの文書も含む。 Configuration Item (itSMF IT サービスマネジメント用語集より)

1） 利用者部門のセキュリティに関するニーズを識別する。セキュリティのニーズはビジネス上の利益に基づくため、そのニーズを判断するのは利用者部門の責任である。

2） 利用者部門のセキュリティ要件の実現可能性を確認する。

3） SLA における IT サービスのセキュリティレベルについて提案、協議、定義を行う。

4） IT サービスの OLA に記載した内部セキュリティ要件の識別、検討、定義を行う。

5） OLA に記述したセキュリティ評価指標の監視を行う。

6） 提供した IT サービスに関する報告を行う。

上記の活動 1～3 について、セキュリティマネジメントのプロセスが、サービスレベル管理の基となります。同時に、サービスレベル管理のプロセスをサポートします。活動 4 と 5 は、セキュリティマネジメントのプロセスで実施します。セキュリティマネジメントならびに他のプロセスが、活動 6 の基となります。サービスレベル管理者とセキュリティ管理者は協議の上、誰が実際に活動を行うかを決定します。

SLA を定義するに当たり、通常は一般的な基本レベル[*44]のセキュリティ対策を想定しますが、もし利用者部門からの追加的なセキュリティ要件がある場合は SLA に明確に追加定義する必要があります。

■ 可用性管理

可用性管理では、IT システムを構成する要素の技術的な可用性を取り上げます。可用性の品質は、障害への弾力性を含む信頼性、保守性およびサービス性によって保証されます。可用性管理は最も直接的にセキュリティマネジメントと関係するプロセスです。セキュリティ対策の多くは、セキュリティ面の機密性、完全性、そして可用性のどれにも利益をもたらすため、この可用性管理と後に述べる IT サービス継続性管理は、セキュリティマネジメントとお互いに協調が必要です。

■ キャパシティ管理

キャパシティ管理の主な目的は、SLA で利用者部門と合意したとおりに IT システムのリソースを最大限に利用することです。IT システムのパフォーマンス要件は SLA で定義される定量的および定性的な評価基準に基づきます。キャパシティ管理のほとんどすべての活動は可用性に影響を与え、さらにはセキュリティ管理にも影響を与えることになります。

*44 一般的に、これをベースラインと呼ぶ

■ IT サービス継続性管理

IT サービス継続性管理の主な目的は、緊急事態のインパクトを利用者部門と合意したレベルまで抑えることです。緊急事態が、必ずしも災害になるとは限りません。IT サービス継続性管理の主な活動は、緊急事態計画を策定し、実行し、予防処置を取ることです。セキュリティの面から、IT サービス継続性管理はセキュリティマネジメントと結び付いています。

13.7 まとめ

本章で述べたとおり、セキュリティ機能を持つITシステムを効果的に活用し維持していくためには、ビジネスの観点から見た「IT 運用プロセス」とITサービスの観点から見た「システム運用」のそれぞれを考慮する必要があります。

IT 運用プロセスには、経営者を含む組織および利用者部門がビジネスの観点から実施すべきプロセスがあります。一方、IT サービスの観点から見たシステム運用は、ITIL のような「IT サービス」のプロセスを基に、具体的なセキュリティ機能と必要な運用の内容を結び付けることで、例えば、ISO27001 に述べられているような管理策のうち、IT システムのセキュリティ機能やシステムの運用に必要な項目を網羅することができます。また、情報セキュリティのプロセスと他のITサービスのプロセスとの関係を整理することで、内部統制、IT ガバナンスの実現や企業内の情報システム全体の最適化を求める要件への対応が可能となります。

- 参考文献

ITIL® Security Management

「IT サービスマネジメントーITIL 入門」 itSMF

「IT サービスマネジメント用語集」 itSMF

第四部 参考資料

14. 代表的なフレームワーク

表 14-1 代表的なフレームワーク

名称	策定者など	適用範囲
ISO/IEC 27001	ISO/IEC	情報セキュリティマネジメントのための要求事項
JIS Q 27001	JISC	
情報セキュリティ管理基準	経済産業省	
ISO/IEC 17799:2005	ISO/IEC	情報セキュリティマネジメントのための具体的な管理策や実践規範
JIS Q 27002	JISC	
JIS Q 15001	JISC	個人情報保護に関する要求事項
ISO/IEC 20000:2005	ISO/IEC	IT サービスマネジメントのための要求事項
ITIL（IT Infrastructure Library）	英国商務局	IT サービスマネジメントのための具体的な実践規範
COBIT（第 4 版）	IT ガバナンス協会	IT 全般統制(IT ガバナンス)のための実践規範
システム管理基準，および追補版	経済産業省	

14.1 ISO/IEC 27001，JIS Q 27001

ISO/IEC27001 は、英国規格 BS7799-2 をベースに作成された情報セキュリティマネジメントシステムの国際規格です。情報セキュリティのための要求事項を網羅しており、リスク分析に基づいたマネジメントプランの立案、必要な資源配分および運用を監視し客観的に見直すというマネジメントサイクルにより、情報セキュリティを維持・改善することを目指しています。日本では JIS Q27001 として規格化されています。

14.2 ISO/IEC 17799（JIS Q 27002）

ISO/IEC 17799（JIS Q 27002）は、上記 ISO/IEC 27001（JIS Q 27001）から参照され、情報セキュリティマネジメントのための具体的な管理策や実践規範が記述されています。

14.3 情報セキュリティ管理基準

ISO/IEC17799:2000（現在の ISO/IEC 17799:2005）を基に、情報資産を保護するための最適な実践慣行を帰納要約し、情報セキュリティに関するマネジメントおよびコントロールの項目を規定したものです。

14.4 JIS Q 15001

個人情報保護を実践するためのマネジメントシステム規格です。2006 年 5 月に JIS Q 15001:2006「個人情報保護マネジメントシステム」として個人情報保護法とさらに深い関係を持つ規格に改版されました。入手手段にかかわらず、また顧客情報だけでなく、従業員情報などすべての個人情報について適用される規格です。PDCA をベースとした規格で、プライバシーマーク制度はこの規格を基にできています。

14.5 ITIL (IT Infrastructure Library)

IT サービスマネジメントに関するベストプラクティスを集めたフレームワークです。IT 運用における実際の知識・ノウハウが集約されており、欧米では業界のデファクト・スタンダードと認知されています。

ITIL は、以下の 7 つの書籍から構成されています。

- Service Delivery：サービスデリバリ
- Service Support：サービスサポート
- Security Management：セキュリティ管理
- The Business Perspective：ビジネスの観点
- ICT Infrastructure Management：ICT インフラストラクチャー管理
- Applications Management：アプリケーション管理
- Planning to Implement Service Management：サービスマネジメント導入計画立案

ITIL のコアとなる IT サービスマネジメントのフレームワークは、上記のサービスデリバリとサービスサポートにて構成され、サービスデリバリでは IT サービス提供にかかわる中長期的な計画と改善に関する 5 つのプロセス「サービスレベル管理」、「可用性管理」、「キャパシティ管理」、「IT サービス継続性管理」、「IT サービス財務管理」が、サービスサポートでは日々の IT サービスの運用とサポートにフォーカスした 5 つのプロセス「インシデント管理」、「問題管理」、「変更管理」、「リリース管理」、「構成管理」と一つの機能「サービスデスク」が、それぞれまとめられています。

14.6 ISO/IEC20000:2005

上記の ITIL を基に規格化された英国規格 BS15000 をベースとして作成された国際規格です。組織が効果的かつ効率的に管理された IT サービスを実施するためのフレームワークと評価仕様を示しています。この規格に基づくマネジメントシステムは、IT 部門が組織内部に導入することも、IT サービスを提供する企業が外部から実施することもできます。

14.7 COBIT (Control Objectives for Information and related Technology)

組織における IT ガバナンスの指針として、米国の情報システムコントロール協会（ISACA）などが提唱する IT ガバナンスの実践規範です。IT 戦略を立案し、システムを開発し、運用・保守を行うまでの業務プロセスを、「計画と組織（PO）：10 プロセス」、「調達と導入（AI）：7 プロセス」、「サービス提供とサポート（DS）：13 プロセス」、「モニタリングと評価（ME）：4 プロセス」の 4 ドメイン：34 プロセスに分割し、プロセスごとに詳細な IT 統制目標を定義しています。

14.8 システム管理基準，および追補版

上記 COBIT 同様、IT ガバナンスの実践規範として経済産業省が策定した基準です。「情報戦略：47 項目」、「企画業務：23 項目」、「開発業務：49 項目」、「運用業務：73 項目」、「共通業務：76 項目」の 5 カテゴリ：287 項目の基準から構成されています。また、追補版では、財務報告に係る内部統制を念頭に、主要なケースを想定しつつ IT 統制に関する概念、経営者評価、導入ガイダンスなどが示されています。

15. リスク分析の手法（例）

15.1 リスクコントロール

情報セキュリティを管理する上で、リスク管理は重要な概念です。いかなるビジネス（活動）においても、その情報セキュリティリスクを定義・管理しなければなりません。ISACA によると、リスク管理の定義は、以下のように表されています。

『ビジネス目的を達成するために、情報セキュリティリスクを定義および管理（識別、分析、評価、対応、監視）すること』

15.2 リスク管理の概要

リスク管理は、企業がビジネス活動を行う上で、利用する情報資産について、「脆弱性」、「脅威」を明確にし、情報資源の資産価値に基づいて、リスクを受容できるレベルまで軽減するために対策を実施するプロセスのことを言います。その概念は、以下の等式で表されます。

『リスクの総和＝脅威×脆弱性×資産価値』

リスクに対処する対策については、以下の選択肢があります。

- リスクを伴うビジネス活動を停止する（Terminate the activity）。
- リスクを他の団体に移転（Transfer）する（保険加入、アウトソーシングなど）。
- リスクを軽減（Reduce）する（セキュリティコントロール・対策を導入）。
- リスクを受容（Accept）する。

一般的に、対策費用は、そのビジネス活動から得られる期待利益を上回ることはありません。リスク管理の体系について、世界的には以下が有名です。

- Australian/New Zealand Standard on Risk Management（AS/NZS 4360）[*45][*46]
- 米国 NIST's Risk Management Guide for Information Technology System、Special Publication 800-30（SP800-30）[*47][*48]

*45 http://www.webstore.jsa.or.jp/webstore/Top/index.jsp?lang=jp
*46 http://www.riskmanagement.com.au/
*47 http://csrc.nist.gov/publications/nistpubs/index.html
*48 http://www.ipa.go.jp/security/publications/nist/

15. リスク分析の手法（例）

リスクマネジメントの重要な要素は、リスクの軽減、または対応のプロセスです。

リスク対応のプロセスは、以下の図で説明されます。

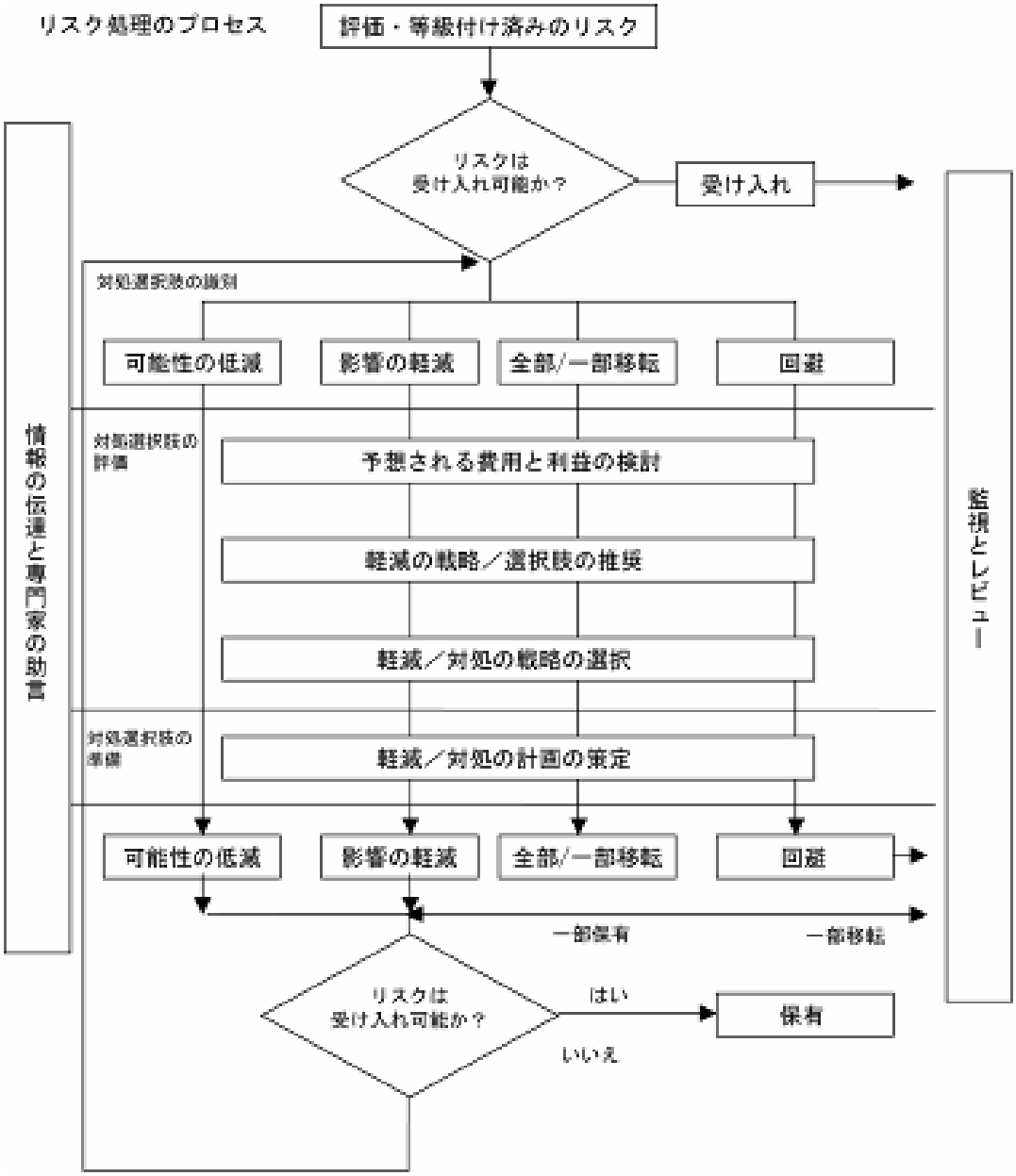


図 15.2-1 リスク処理のプロセス（出典：AS/NZS:4360:1999）

16. リスクマネジメントのプロセス

16.1 計画策定

リスクマネジメントを行うには、計画の策定とその責任者を割り当てる必要があります。その場合、重要な業務部門の代表者の参加は必須であり、その策定は、技術主導でなく業務主導で進めなければなりません。計画書には、以下の項目を定義します。

- リスクアセスメントの目的、適用範囲
- リスクコントロールの目標水準
- リスクコントロールの組織体制
- リスク評価方法
- リスク処理選定基準

16.2 資産の査定

情報資産を分類する目的は、資産価値とリスクに応じた適切な保護策を決定するための判断基準を明確にすることです。情報資産の分類(Information classification)は、その情報資産の持つ機密性と重要性に基づいて行います。またそれぞれの分類カテゴリごとに、その情報資産へのアクセス権、アクセス権の決定権、承認権を明確にする必要があります。情報資産の分類の一般的な考慮点を、以下に示します。

- 分類の深さ(階層)
- 情報資産の場所
- 分類の決定権は誰が持つか
- いかに扱うか
- いかに印を付けるか(識別するか)
- 誰がオーナーか
- 誰がアクセス可能か
- アクセス決定権は誰が有するか
- いかに移送するか

16.3 リスクアセスメント

リスクアセスメントでは、脅威評価と脆弱性評価を行い、これらの評価結果からリスク評価を行います。

16.4 脅威評価

脅威とは、システムの脆弱性を突くことにより、潜在的に情報資産に危害を及ぼす事象を指します。

例）エラー、悪意のある攻撃、自然災害、システム停止、詐欺などの人的行為。

脅威分析は、基本的アプローチとベースラインアプローチの二つの方法に分類することができます。

16.5 脆弱評価

脅威は、脆弱性によって引き起こされます。脆弱性の主なものには、以下があります。

例）不具合のあるソフトウェア、不適切な設定、ユーザのセキュリティ意識の欠如、脆弱なパスワード、冗長性の欠如、保守・運用の不備。

16.6 リスク評価

定量的評価と定性的評価があります。定量評価では、

リスク評価額＝予想損失額×事故発生確率

定性評価では、リスクの事象ごとに、脅威の度合い、脆弱性の度合い、リスク発生確率などから事故発生時の管理対象に対する影響度合いを、3 段階あるいは 5 段階で評価し、リスク事象の相対的な大きさを査定します。

- コントロール評価

  リスク管理の重要なプロセスは、リスク軽減または対処のプロセスです。リスク対処のプロセスは、以下の図で示されます。

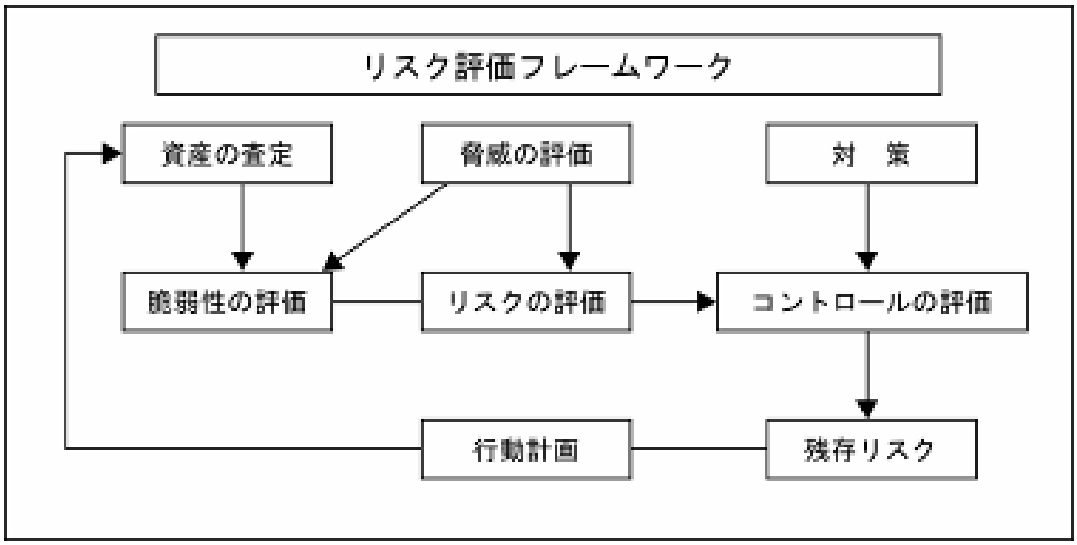


図 16.6-1 リスク評価フレームワーク

16.7 残存リスク

リスクの軽減およびその優先付けを行い、リスクの許容レベルを決定します。受容リスクは経営者によって承認されます。受容リスクを決定する上で、以下の点(リスクを低減する観点)を考慮する必要があります。

- 情報セキュリティガバナンス方針(セキュリティポリシー)と一致しているかどうか。
- 過度なレベルの、対策／コントロールが導入されていないかどうか。
- リスクアセスメント方法の不確実性部分がないかどうか。
- 導入コストが有効であるかどうか。

16.8 行動計画

残存リスクを含めたリスクの監視とそのエスカレーションルールの確立などの行動計画を策定します。リスク管理は、変化する脅威や脆弱性に適時に対応できるように、継続的かつダイナミックなプロセスでなければなりません。そのためには、以下の活動が必要です。

- 監視とレビュー
- 報告(重大なセキュリティ違反や事象の上級管理者への報告)
- ライフサイクルプロセス(変更管理など)への統合

16.9 リスクの軽減の方法

リスクを軽減するには、包括的な検討を行う必要があります。技術的、組織的能力および費用対効果を考慮して多層的なコントロールを検討する必要があります。

- 抑止（Deterrent）コントロール
- 予防（Preventive）コントロール
- 発見（Detective）コントロール
- 訂正（Corrective）コントロール

16.10 情報資産の RTO(Recovery time objectives)

「情報セキュリティに完全はなく事故は起こり得るものである」という概念が定着してきました。この概念に対応するにはリスク評価の一環として、情報資産の事故に対する復旧時間（RTOs）を決めておく必要があります。各重要な情報ごとに RTOs を決めておかなければなりません。RTOs は、ビジネス継続計画の作成と連携した、BIA（ビジネスインパクト分析）において実施されます。

17. 定量リスク分析の基礎

17.1 期待値

確率の世界には「期待値」という考え方があります。この「期待値」は、定量リスク分析の基本となる重要な考え方です。まず、この期待値から見ていきましょう。

ある賭けを例に考えます。6 面のサイコロを 1 回振ります。1 が出れば「当たり」で 600 円もらえます。それ以外はハズレで、1 円ももらえません。この賭けの期待値はいくらでしょうか。

期待値を計算するには、期待される利益とその確率を掛け合わせます。今回の例では、6 回に 1 回の確率で利益 600 円を得ることができます。6 回に 1 回の確率は、1/6 ですから、

期待値 ＝ 確率 × 利益 ＝ (1/6) × 600 ＝ 600/6 ＝ 100

となります。つまり、この例での期待値は 100 円です。

期待値という数字は、どういう意味を持つのでしょうか。期待値は、1 回当たりの平均の利益を示します。今回の賭けでは、長い間繰り返していると、大体 1 回当たり 100 円利益が得られるということです。例えば、この賭けを 1000 回実施したとすると、よほどの幸運や不運がない限り、利益の合計は 100 円×1000 回＝10 万円ぐらいの金額になっているはずです。これは、賭けを実施するかどうかを考えるときの目安になります。この賭けに参加するために 1 回 200 円の参加料を払うことになっているならば、長い間には必ず平均して 1 回当たり 200 円（参加料）－100 円（期待値）＝100 円の損をすることになるはずです。

期待値は、損失に対しても使うことができます。同じ賭けで、支払う側の立場に立ってみれば、6 回に 1 回の確率で 600 円損をするのですから、同様にして損失の期待値を 100 円と計算することができます。損失の場合は、

損失の期待値 ＝ 確率 × 損失

と書き換えると分かりやすいでしょう。これが、リスクを定量化上での基本となります。

17.2 リスクの定量化

リスクの定量化にはいろいろな方法がありますが、最も一般的で直感的にも分かりやすいのが、リスクによる損失の期待値を使う方法です。例えば、ある建物の火災の発生確率が 100 年に 1 回、その平均損害額が 1000 万円だとするならば、その火災のリスクの大きさは

リスク ＝ 損失の期待値 ＝ 確率 × 損失 ＝ 1/100 × 10000000 ＝ 100000（円／年）

となり、1 年当たり 10 万円と計算できます。このケースでは、損害が全額補償されるのであれば、年間 10 万円以下の保険料の火災保険に入るメリットがあります。この方法で求めた 1 年当たりの損失の期待値を一般に年間予想損失額（Annual loss expectancy; ALE）と呼びます。

実際にこの方法でリスクを定量化しようとすると、各リスクの発生確率と平均の損失金額を知る必要があります。地震や火災のような災害や、犯罪などは一般的な統計が参考になる場合もありますが、多くのリスクについてはそのような基礎情報がないため、正確なリスクの値を計算することは困難です。厳密なリスク分析を行おうとすると、たいていここで壁に当たってしまいます。

そこで、厳密なリスクの値を求めるのではなく、複数のリスクの比較ができる程度のリスクの概算値を求めることを考えます。リスクというのは、実はとても大きな数値の幅（ダイナミックレンジ）を持っています。金額でも 10 円、100 円といった日常生活レベルから、国家予算規模のリスクまでありますし、発生頻度も毎日起こるようなことから、数百年に 1 回というめったに起こらないことまであります。例えば、平均的日本人が一年に交通事故に遭ってけがをする確率は 0.0001 程度なのに対し、隕石に当たってけがをする確率は 0.0000000001 程度でしょう。その違いは約 100 万倍です。ここで、隕石のほうの確率が 0.00000000011 か、あるいは 0.00000000010 かを議論することはあまり意味がありません。いずれにしても交通事故のほうがはるかに大きいリスクであるという事実に変わりはないからです。1 に対して 10 倍、100 倍という差があるものを比較する場合、0.1 や 0.2 の違いは問題にならなくなってしまいます。

このことを背景に、リスクを「桁でとらえる」ことを考えます。1 年当たりのリスク期待値として、「10 円程度」「100 円程度」「1000 円程度」「1 万円程度」「10 万円程度」と考えると、一般的な個人に関するリスクはこの 5 分類のどれかに入ると思います。火災や事故などの大きなリスクは最後の「10 万円程度」近辺に来るのが普通ですから、保険によってリスクを移転することが一般に行われています。このように、リスクを「桁でとらえる」ことは、正確な値を必要とせずにリスクの比較を可能にします。これが、正確な統計値がない場合にでも定量リスク分析を可能にするコツなのです。

17.3 リスクの指標化

前節の「桁でとらえる」ことを数式で表してみましょう。

一般に、リスクの平均被害金額 V は

V ＝ a × 10^x （10^x は 10 の x 乗を表す）

と書けます。この x の部分が「桁でとらえる」と述べていた部分です。x が 1 ならば 10^1は 10 なので V は「10 円程度」となりますし、x が 3 ならば 10^3 は 1000 なので V は「1000 円程度」となります。a は 1 から 10 の範囲を取る数で、a=3, x=3 ならば V は 3×10^3＝3000 で 3000 円になります。

同様に、リスクの発生確率 P は

P ＝ b × 10^y

と書けます。確率は 1 より小さくなければならないので、y はマイナスの数字になります。b は a と同様に 1 から 10 の範囲を取る数です。b=6, y=(-3) ならば P は 6×10^(-3)=0.006 で 1000 分の 6 になります。

このとき、リスクの期待値 E は

E ＝ V × P

＝(a × 10^x)×(b × 10^y)

＝ a × b × 10^x × 10^y

＝ ab × 10^(x + y)

となります。「ab」の項は、1 から 100 の間を取り、平均は 10 程度になる数です。そしてリスクの期待値の桁を主に決めるのは「10^(x + y)」の項で、(x + y)の値が期待値の桁をほぼ支配していることが分かります。従って、桁数だけを知りたいのであれば、発生確率の桁数を示す指数の y と被害金額の桁数を示す指数の x を単純に足せばよいということが分かります。

具体例で見てみましょう。まず、被害金額の指数を下記の表で定義します。

指数 x	被害金額の目安
4	10^4 = 10000 円
3	10^3 = 1000 円
2	10^2 = 100 円
1	10^1 = 10 円

同様に、被害発生確率も定義します。

指数 y	発生確率の目安
-1	10^(-1) = 0.1 回/年
-2	10^(-2) = 0.01 回/年
-3	10^(-3) = 0.001 回/年
-4	10^(-4) = 0.0001 回/年

被害金額と発生確率を表にすると、以下の表になります。被害金額と発生確率を掛け合わせた数字が、リスクの値になっています。

リスク（実数表記）		被害金額			
		10000	1000	100	10
発生確率	0.1	1000	100	10	1
	0.01	100	10	1	0.1
	0.001	10	1	0.1	0.01
	0.0001	1	0.1	0.01	0.001

この表を、指数を使って書き直してみます。

リスク（指数表記）		被害金額			
		10^4	10^3	10^2	10^1
発生確率	10^(-1)	10^3	10^2	10^1	10^0
	10^(-2)	10^2	10^1	10^0	10^(-1)
	10^(-3)	10^1	10^0	10^(-1)	10^(-2)
	10^(-4)	10^0	10^(-1)	10^(-2)	10^(-3)

上の表の指数部だけを記述する（例えば「10^4」を「4」と書く）と、この表になります。

リスク（指数部のみ）		被害金額			
		4	3	2	1
発生確率	-1	3	2	1	0
	-2	2	1	0	-1
	-3	1	0	-1	-2
	-4	0	-1	-2	-3

この表では、被害金額と発生確率の指数部の足し算でリスク値の答えが出ることが見て分かると思います。例えば被害金額が「4」、発生確率が「-1」の部分のリスクが「3」になっていますが、これは 4＋(-1)＝3 の答えと一致しています。つまり、式で書くと下記のようになります。

リスク指標 ＝ 被害金額指標 ＋ 発生確率指標

表の中にマイナスがあるのが分かりにくいという方のために、発生確率に一律5を加えると、次の表になります。相対的に比較するだけならば、一律に値を足しても本質的に問題はありません。これは、理論的には「1年当たりの発生頻度」を「10万年当たりの発生頻度」に修正したことと同じです。この形ならば、多くのリスク分析の文献で目にすることが多いと思います。

リスク(指数部)		被害金額			
		4	3	2	1
発生確率	4	8	7	6	5
	3	7	6	5	4
	2	6	5	4	3
	1	5	4	3	2

17.4 コートニーの方法

定量リスク分析の手法の一つである、コートニーの方法は、これと同じ考え方を使っています。コートニーの式は、以下で定義されます。

E = 10^(P+V-3)/3

V:当該脅威発生時の予想損失額(金額を指数化したもの)

P:当該脅威の発生頻度(3000年当たりの発生回数を指数化したもの)

E:リスク額(年間)

この式ではPの発生頻度が「3000年当たり」で記述されているため、年間のリスク金額に直すには、計算結果を3000で割る必要があります。コートニーの式の中の「/3」は「3で割る」、指数の「-3」は「10^3=1000で割る」ことを意味しますので、これらの項により、この式ではリスクの値を「3000」で割っていることになります。

E =(10^(P + V))/3000

=(10^(P + V))/(3 × 10^3)

=(10^(P + V)) × 10^(-3)/3

=(10^(P + V - 3))/3

Eの値を決める上で中核になっているのは「P+V」の部分であり、これは前節までに述べてきたように、指数の積が和で表せることを利用しているのです。

17.5 脆弱性および対策の考え方

脆弱性と対策は表裏の関係にあります。つまり、対策が十分にされていない状態が脆弱性です。これらによって、リスクの値が変化すると考えれば、定量分析に組み込むことができます。下の表は、その一例です。

脆弱性指標	対策指標	リスクへの影響	指標への修正
-3	3	1/1000 にする	-3
-2	2	1/100 にする	-2
-1	1	1/10 にする	-1
0	0	無影響	0

例えば、脆弱性指標を使用する場合、損失金額と確率から計算したリスク指標に「脆弱性指標」を加えれば、リスクへの影響を加味することができます。この場合、リスク指標の求め方は

リスク指標 ＝ 被害金額指標 ＋ 発生確率指標 ＋ 脆弱性指標

となります。同様に、対策指標を使用する場合は、リスク指標に「－対策指標」を加えます。この結果、リスク指標は

リスク指標 ＝ 被害金額指標 ＋ 発生確率指標 － 対策指標

となります。このように、指標上ではリスクを増やす要素は「＋」で、減らす要素は「－」で現れてきます。

17.6 いろいろな応用

■ 基本的なパターン（コートニーの方法）

変数	代表値	指標
被害金額Ｖ	10 万円以下	1
	100 万円	2
	1000 万円	3
	1 億円以上	4
発生確率Ｐ	300 年に 1 回	1
	30 年に 1 回	2
	3 年に 1 回	3
	3 ヵ月（≒0.3 年）に 1 回	4

この場合は E=V+P の値によって、以下のリスク値になります。

変数	指標	リスク値（年間）
リスク指標Ｅ	2	約 300 円
	3	約 3000 円
	4	約 3 万円
	5	約 30 万円
	6	約 300 万円
	7	約 3000 万円
	8	約 3 億円

■ 脆弱性の大きさを入れたパターン

リスク値は E=V+P+H-1 で、前の表で求めます。

変数	代表値	指標
被害金額Ｖ	10 万円以下	1
	100 万円	2
	1000 万円	3
	1 億円以上	4
発生確率Ｐ	300 年に 1 回	1
	30 年に 1 回	2
	3 年に 1 回	3
	3ヵ月(≒0.3 年)に 1 回	4
脆弱性Ｈ	軽微	0
	重大	1

■ 被害金額を細分化したパターン(その1)

変数	代表値	指標
被害金額Ｖ	10 万円以下	1
	30 万円	1.5
	100 万円	2
	300 万円	2.5
	1000 万円	3
	3000 万円	3.5
	1 億円以上	4
発生確率Ｐ	300 年に 1 回	1
	30 年に 1 回	2
	3 年に 1 回	3
	3ヵ月(≒0.3 年)に 1 回	4

10^0.5=約 3.1 なので、指標を 0.5 上げるには代表値を約 3.1 倍すればよいことになります。

変数	指標	リスク値（年間）
リスク指標 E	2	約 300 円
	2.5	約 1000 円
	3	約 3000 円
	3.5	約 1 万円
	4	約 3 万円
	4.5	約 10 万円
	5	約 30 万円
	5.5	約 100 万円
	6	約 300 万円
	6.5	約 1000 万円
	7	約 3000 万円
	7.5	約 1 億円
	8	約 3 億円

■ 被害金額を細分化したパターン（その2）

変数	代表値	指標
被害金額 V	10 万円以下	2
	30 万円	3
	100 万円	4
	300 万円	5
	1000 万円	6
	3000 万円	7
	1 億円以上	8
発生確率 P	300 年に 1 回	2
	30 年に 1 回	4
	3 年に 1 回	6
	3 ヵ月（≒0.3 年）に 1 回	8

前の例の指標を全体で 2 倍したもの。指数の底を 10 ではなく 10^0.5 にしたことに相当します。リスク値表は前の例と同様なので、省略します。

17.7 誤りの例

定量リスク分析の文献の中には、被害金額や発生頻度などの値が明らかに指標値（1段階で 10 倍に増えるようなスケールの指標）を取っているにもかかわらず、リスク値を出すために各指標の積を取っている例があります。これまでと同様に式で表現すれば

リスク指標 ＝ 被害金額指標 × 発生確率指標 × 脆弱性指標

というようなケースです。期待値を議論の出発点にしている限り、これは誤りであり、指標で期待値を求めるためには掛け算ではなく足し算で計算しなければなりません。これと、正しい形である

リスク指標 ＝ 被害金額指標 ＋ 発生確率指標 ＋ 脆弱性指標

で計算結果がどれくらい違うか見てみましょう。

まず、絶対的な値の違いです。試みに、被害金額指標、発生確率指標、脆弱性指標がいずれも 3 だったと仮定します。正しく計算すれば

リスク指標 ＝3＋3＋3＝9

すなわち、リスクは 10 の 9 乗＝約 10 億円／年です。しかし、積を取ってしまうと

リスク指標 ＝3 × 3 × 3＝27

すなわち、10 の 27 乗という答えが出てきます。これは正しい答えの 10 億倍の、さらに 10 億倍に相当します。

また、複数のリスクを比較するという目的でも間違った答えを導きます。例えば、以下のような二つのケースでリスク値を比較します。

ケース	A	B
被害金額指標	2	4
発生確率指標	2	1
脆弱性指標	2	1

この二つのケースはいずれも指標の合計は 6 なので、リスク値はどちらも同じ 10^6＝100 万円/年です。しかし、積演算だと異なる値になります。

ケース A:2×2×2＝8

ケース B:4×1×1＝4

その差は指標値で 4、すなわち 10^4 = 10000 倍のリスク値の違いとして現れます。このように積演算では、各項目が平均して高いリスクが、どれか一つが突出して高いリスクよりも激しく大きくなる傾向がありま

す。この特性は、リスクを評価する上で合理的なものではありません。例えば、一般に被害金額が大きいリスクは、発生頻度が低くても、人は心理的にリスクとして大きく評価する傾向があることが知られています（プロスペクト理論）。こういった心理的要素を反映するための補正ならばまだ合理性はあるのですが、この積演算は実際には逆方向へ評価値をずらす性質のものであり、合理的説明ができないものになっています。

17.8 期待値による定量リスク分析の限界

これまで期待値による定量リスク分析について述べてきましたが、この分析方法によるリスク評価の結果が、一般的な管理者の直感と異なるケースがあります。一つは、前節で述べたプロスペクト理論です。一般に、期待値が同じ場合に、発生確率が低くても被害の絶対額が大きいリスクを、人はより大きく評価する傾向があります。もう一つは、リスクの変動そのものがリスクという考え方（ボラティリティリスク）です。すなわち、小さい被害で確定できてしまうリスクであれば、期待値がやや高めでも受容してしまうという考え方です。これらの考え方は単純な期待値同士の比較では反映できませんので、期待値を絶対の指標と考えるのではなく、あくまでリスク評価の指標の一つととらえることが望ましいといえるでしょう。

18. セキュリティ評価指標とセキュリティダッシュボード

セキュリティダッシュボードは、ある組織内の情報セキュリティに関する情報を集約して表示するアプリケーションです。この章では、セキュリティダッシュボードを実現するための考慮事項を説明します。

18.1 セキュリティダッシュボードの利用者

初めに、セキュリティダッシュボードの利用者像を確定します。ある組織において、情報セキュリティに関係する人物は多数存在します。これらを代表する役割として、例えば、以下のような人物像を想定することができます。これらの利用者は、それぞれ異なる立場、異なる職責を持ちますので、同じ情報セキュリティの可視化というテーマでも、それぞれ興味の対象領域や、必要になるリアルタイム性は異なってきます。

■ システム管理者

情報システムを管理するシステム管理者は、自身の担当している情報システムにおけるセキュリティの現状を知る必要があります。特に、システムにおけるセキュリティ事故の発生や、セキュリティインシデントの発生、不正な攻撃の予兆などの情報を、的確かつ、できるだけ早く知ることが求められます。

■ 組織のセキュリティ管理者

組織のセキュリティ管理者やセキュリティ管理に責任を負う部門長は、自組織におけるセキュリティマネジメントの定着状況や、各種のセキュリティ管理策（セキュリティ対策）の実施状況について、正確に把握する必要があります。

■ CIO または CISO

CIO（Chief Information Officer）や、CISO（Chief Information Security Officer）は、組織全体のセキュリティ状況を常に知るべき立場にあります。また、自組織に導入した各種のセキュリティ対策投資がその効果を発揮しているか、もし有効に稼働していないならその原因は何かなどを把握し、セキュリティ投資計画に反映する責を負っています。

18.2 ダッシュボードへの入力情報

情報セキュリティで可視化の対象領域となり得る情報は非常に多岐にわたります。例えば、ISO/IEC 27001 に基づく情報セキュリティマネジメントシステムにおいても、マネジメントシステム自身の有効性と、導入したセキュリティ管理策の有効性を把握することを求めています。これに関連して、セキュリティ測定の実施方法を記述するISO/IEC 27000ファミリ標準(ISO/IEC 27004の番号が仮に振られています)の検討が ISO/IEC JTC1 で行われています。

セキュリティに関するログが 4 種類あることは第 7 章ですでに述べました。これを手掛かりにして、セキュリティダッシュボードへの入力情報も4種類に分類すると見通しが良くなります。

■ セキュリティマネジメントの可視化

情報セキュリティマネジメントシステム(ISMS)の状況を把握し、維持・改善するために取得するべき情報です。主に、情報セキュリティマネジメントシステムで言うPDCAループのC(チェック)フェーズに相当し、ISO/IEC 27001(JIS Q 27001)では 4.2.3 項「ISMS の監視およびレビュー」の要求事項にほぼ相当します(ただし、このうち 4.2.3C に定義されている管理策の有効性測定は後述の「セキュリティコントロールの可視化」に相当します)。米国国立標準技術研究所(NIST)が発行している SP800 シリーズでは、SP800-55 などにマネジメントとして収集すべき指標の一部が記載されています。可視化対象の例としては、以下のようなものが挙げられます。

- セキュリティマネジメントの確立状況を示す指標(セキュリティ関連文書の整備率、年間セキュリティ計画の策定率など)
- セキュリティマネジメントの定着状況を示す指標(教育実施回数、教育の出席率、セキュリティ委員会の参加率など)
- 内部監査の結果と是正・予防状況
- 認証に必要なエビデンス(証跡)の整備状況

■ セキュリティコントロールの可視化

具体的なセキュリティ対策であるセキュリティコントロール(管理策)の状況を把握し、対策の実効性低下がないかどうかを確認するための情報です。ISO/IEC 27001(JIS Q 27001)では、4.2.3 項「ISMS の監視およびレビュー」の要求事項 C にほぼ相当します。米国国立標準技術研究所(NIST)が発行している SP800 シリーズでは、主に SP800-55 に指標測定方法が記載されています。

この領域では、導入されたセキュリティ対策が「設計時に期待された効果を発揮しているか」という観点で測定情報を選択します。この可視化対象の例としては、以下のようなものが挙げられます。

- セキュリティ対策の稼動状況を示す指標（ファイアーウォールや侵入検知システムの稼動状況）
- システム利用者のパスワード変更状況
- システムのセキュリティ設定の現状
- システムまたは PC へのセキュリティパッチ適用状況
- ウィルス対策ソフトの検出パターンアップデート状況
- PC の外部持ち出し状況

■ セキュリティリスクの可視化

情報セキュリティリスクの発生状況を把握するための情報です。ISO/IEC 27001（JIS Q 27001）では 4.2.1 項「ISMS の確立」において、組織に存在するリスクを特定・分析することを求めています。しかしながら、組織の内外に存在するリスクを網羅的かつリアルタイムに把握することは難しく、現在では確立した一般的な手法がない領域でもあります。「セキュリティマネジメントの可視化」「セキュリティコントロールの可視化」のうち、指標の低下がセキュリティリスクに直結するものは、この指標にも重複して該当することがあります。この可視化対象の例としては、以下のようなものが挙げられます。

- 組織内の分析済みリスクの一覧
- リスク対応の状況一覧
- 脅威の発生状況（侵入検知システムで検出された攻撃状況、組織外でのウィルス発生状況など）
- インシデントの発生状況（侵入検知システムで検出された侵入成功の事実、組織内でのウィルス発生、システム利用者から報告されたセキュリティ事故報告など）
- セキュリティ規定の順守状況の低下によるリスク発生状況（セキュリティマネジメントの可視化と重複）

■ セキュリティトレーサビリティの可視化

情報セキュリティに関する統制状況を客観的に記録し、第三者にその事実を証明することを目的とする情報です。事実の証明が必要になる場面は、法制度の要請（個人情報保護法など）、認証制度の要請（プライバシーマーク認証など）、会計制度の要請（日本版 SOX 法など）、業界ガイドライン、訴訟対応など多岐にわたります。後日の開示に備えて記録する（消極的利用）と、定期的に記録を調査して事件の兆候などの検出を試みる（積極的利用）の 2 種類の利用方法があります。この可視化対象の例としては、以下のようなものが挙げられます。

- 利用者によるシステムへのログイン、操作のログ
- 特権利用のログ
- 利用者への権限付与履歴
- 承認権限者による承認履歴
- 電子メール発信記録

18.3 セキュリティ評価指標の決定

情報セキュリティの可視化対象の中には、指標化できるものがあります。特に、情報システムから得られる情報の一部は、そのまま数値として利用できるものがあります。しかし一般には、このような「生の」情報をそのまま利用するのではなく、利用者にとって理解しやすいように何らかの形に加工することが必要です。このような加工の例として、以下のようなものがあります。

- 情報を集計する（合計を出す、平均値を取るなど）
- 目的値（理想値）と現状値の差（乖離）を表示する
- 母数に対する比率（達成率など）を表示する
- 複数の指標の相関を表示する（相関係数を計算する、散布図を描くなど）
- 過去の履歴の最大値や最小値を表示する
- 過去からの累積値を表示する
- 過去の平均値や標準値からの乖離を表示する（前年同日比や前週同日比など）
- 単調増加や単調減少などの傾向を分析する
- 閾値を超えているかどうかのみを表示する（警報型の指標）
- 多数の1ビット指標がある場合に、その AND または OR を取る
- 問題を発見するために、より高度な統計手法を用いる（多変量解析など）

特に、ある標準値（目標値、理想値など）に対して現状の値がどうなっているかということが比較できる指標は、多くの場合に有効な指標となります。この場合、目標となる標準値をどのように決めるかが重要です。マネジメントに関する指標の一部については、ISMS などのマネジメントシステムがその材料を提供しますが、多くの指標は組織の方針や考え方に基づいて独自に定義する必要が出てきます。

18.4 セキュリティダッシュボードの設計

セキュリティダッシュボードを実現するために、それぞれの利用者にどのような形で可視化された情報を提供するかを整理します。ここで考慮するべき事項として、以下のようなものがあります。

■ リアルタイム性の検討

可視化対象の情報がリアルタイムに表示されることは、ダッシュボードの目的の一つです。しかし一方で、情報をリアルタイムに取得し、表示することはシステム的に非常にコストが高い処理です。可視化対象情報ごとに必要なリアルタイム性への要求を整理し、必要なだけのリアルタイム性を厳選して実現するように配慮する必要があります。また、警報のような特に緊急性の高い情報については、メールの自動送信など、能動的に情報を通知する仕組みを持つことを併せて検討します。

■ 表示方法の選択

どのような形で情報を表示するかは、ダッシュボードを検討する上で最も重要な要素の一つです。定量的な情報は、グラフ化することで直感的にその意味をとらえやすくなります。このとき、指標の評価目的に応じて最適なグラフを選択しなければなりません。複数のデータの絶対値を比較するときは棒グラフ、時間変化を読み取るときは折れ線グラフ、データの比率を見るときは帯グラフかパイグラフ（円形グラフ）が基本です。2 種のデータの相関を見るときは散布図が適切です。さらにn、品質管理で使われる各種の管理図や、進捗を管理するガント図など、特定の目的のために使われるグラフも多数あります。

管理状況などを包括的に見る場合は、警報ランプや信号機のような、状況を集約して結果だけを明確に示すことが有効な場合もあります。この場合は、どのような集約方法で多数の情報を一つの結果にするかについて、利用者と合意することが必要です。

定量化できない情報は、元データをそのまま表示することが主流になります。この場合は、対象となるデータの検索方法や、画面での表示方法が主な検討対象になります。

■ 画面レイアウトの検討

表示方法とともに、画面のレイアウトも検討が必要です。最大の達成目標は、利用者にとって理解しやすい形で、必要な情報をできるだけコンパクトに配置することです。

画面上の配置が利用者にとって意味があるものになっていれば、利用者は情報の把握をより的確に行うことができます。この、利用者にとっての意味は、ダッシュボードの性格や利用者の視点によって変化します。例えば、画面上に表示する、利用者が管理するべき組織の組織図イメージをそのままダッシュボー

ド画面上に表示し、画面レイアウトの基本設計にすることなども考えられます。画面レイアウト設計時は、利用者と意見交換を密に行い、利用者の視点を明確にダッシュボードに反映しなければなりません。

18.5 セキュリティダッシュボードの実装

セキュリティダッシュボードを実現するためには、以下の機能をソフトウェアで実現する必要があります。

- 可視化対象情報を持つ IT 機器から表示対象となるデータを抽出し、セキュリティダッシュボードシステムにデータを転送する機能（データコレクタ）
- IT 化されていない情報を可視化するためのデータ入力システム
- 転送されたデータを集約し、統一された形式でデータベースに格納する機能
- 集約されたデータを加工し、ダッシュボードに表示する情報に変換する機能（可視化エンジン）
- 利用者がアクセスするダッシュボード画面を生成する機能（ダッシュボードサーバ）

これらの機能の一部は、一般に市販されているミドルウェアを利用することもできます。例えばデータコレクタの部分は、システム集中管理のパッケージでかなりの部分をカバーすることができます。しかし、ダッシュボードシステム全体の構築は、個別のシステムインテグレーションとなることが一般的です。

18.6 セキュリティダッシュボードの将来像

現在の IT 技術に基づく限り、セキュリティダッシュボードの構築は個別開発の要素が強く、そのためにはかなりのコストがかかるのが現状です。将来的には、ダッシュボードの各機能要素や可視化のための画面部品の共通化が進み、実在の機械でメーターを組み合わせるように、短期間かつ低価格でダッシュボードの構築ができる環境が整うことが期待されます。Web を使った Saas などの技術は、これらのダッシュボード構築の強力な支援技術になる可能性があります。

富士通のエンタープライズセキュリティアーキテクチャー

2006 年　11 月	初版第二刷発行
2007 年　 5 月	二版発行
2007 年　10 月	三版発行
2008 年　 5 月	四版発行

著者	富士通株式会社 情報セキュリティセンター ESA プロジェクト
編集・発行	富士通株式会社 情報セキュリティセンター
	東京都大田区新蒲田 1-17-25 富士通ソリューションスクエア