博士論文

「CC-Case：セキュリティ要求分析・保証の統合手法」

Tomoko　KANEKO
金子　朋子

情報セキュリティ大学院大学
情報セキュリティ研究科
情報セキュリティ専攻

2014 年 3 月

まえがき

CC-Case という開発方法論を研究することになった原点とは何であろうと私自身の過去を振り返ると 3 つの背景が頭に浮かんだ．まえがきとしてそれらを紹介させていただきたい．

「電話とコンピュータとどちらがいいですか？」

筆者が，入社前に尋ねられた言葉である．コンピュータの方が未知数だけれどもこれから普及していくのではないかと考え，分離独立予定であった㈱NTT データ通信本部への配属を希望した．筆者が IT の世界に入った昭和の終わり頃，コンピュータは大学や企業の密室にある大きな箱であり，固定電話の方が身近な存在だった．金融系システムのプログラマーから始め，航空機データ通信システム・通信社システム等の設計、運用・保守に携わった．故障対応のため，解読不能な山と積まれたコードリストとの格闘の中で「何をどう対処したらいいのか？どのようなプロセスで進めればいいのか？どのように作ればお客様に納得してもらえるのか？」も，わからずに働き続けた．後にプロセス標準化・ISO 規格・CMMI などの業務を通じて開発方法論に魅かれていった理由がここにある．「要求を正しく実現し，お客様合意の得られる仕組みづくり」をしたい．これが 1 つ目の原点である．

「情報セキュリティという言葉を初めて聞いたのはいつだっただろう」

筆者は入社 7 年目の頃に、当時社会問題化していたアミューズメント系システムの業務についた．アミューズメント系カードからの金銭搾取を目的とした犯罪集団と戦う職場であった。その当時，情報セキュリティの概念はなく，システムは攻撃者の存在を想定していない性善説のシステム設計だった．対策をたててもいたちごっこは続き，「どうすれば、いたちごっこを抜け出せるのか？」はわからずじまいのままだった．この”？”はずっと心にあったから，初めて「情報セキュリティ大学院大学」の看板を見たときに心が動いたのだろう.これが 2 つ目の原点である．

「ワークライフバランス実現のため越えるべき壁は，またしても情報セキュリティ？」

筆者は結婚後，二人の男の子を出産し，4 年半の育児休業を取得した．復職して，育児と仕事の両立を図る日々はまことに多忙だった．そこで子供との時間を少しでも多くとり，充実した生活をするために社内の働く母たちと力を合わせ，テレワーク社内制度化を実現した．当時のテレワーク制度化に際しての最大の壁は実は情報セキュリティだった.テレワークによる情報漏えいを危惧され，制度実現は一時暗礁に乗り上げた．情報セキュリティにおける保証を得られないと物事は進めない時代になったのだと感じた．これが 3 つ目の原点である．

「情報セキュリティとは何で、安全なシステム開発等の実現にはどのような要求があり，どのような保証を必要とするのか？そしてそれをどう実現すればいいのか？」

こんなことをテーマに，大学院博士課程前期及び後期で学び研究をしてきた．四半世紀前に比べると IT 化は確かに革命的であり，IT の多様化・高度化に伴い，IT 製品・システムは生活のあらゆる側面に利用されている．ネットも携帯電話もなかった時代など想像もできない人も多いはずである．反面，サイバーテロ、金銭搾取目的の攻撃など、情報セキュリティにおける攻撃の巧妙化，組織化も進んでいる．これからも変化するであろう IT のリスクに応じて，より安心・安全な IT 製品，システム，ソフトウェアを世の中にお届けするための一助になることを願ってこの論文を上梓する次第である．

2014 年 3 月 16 日

金子　朋子

目次

1 序論 1
1.1 本研究の概要 1
1.2 本研究の特徴 2
1.3 本論文の構成 2
2 研究の背景 4
2.1 システム開発の要求・保証の現状とリスク 4
2.1.1 セキュリティ要求の分析 4
2.1.2 セキュリティ対策と保証 5
2.1.3 システム開発のリスクとアシュアランスケース 6
2.2 先行研究 8
2.2.1 セキュリティ要求分析手法 8
2.2.2 i*-Liu 法 8
2.2.3 アクタ関係表（ARM）による要求分析 9
2.2.4 アシュアランスケース 10
2.2.5 セキュリティケース 11
2.2.6 コモンクライテリア 12
3 CC-Case の全体像 14
3.1 CC-Case の定義・目的 14
3.2 CC-Case の対象範囲・適用対象とアシュアランスケースの役割 16
3.3 CC-Case のライフサイクルプロセス 16
3.3.1 ライフサイクルプロセスの構造 16
3.3.2 CC-Case のライフサイクルプロセスの詳細 18
4 要求段階の CC-Case 20
4.1 要求段階の CC-Case の概要 20
4.1.1 要求段階の CC-Case の全体像 20
4.1.2 ST の構成とセキュリティ要求分析 21
4.1.3 ST の構成と CC-Case 21
4.1.4 検証・妥当性確認のプロセス 22
4.1.5 SARM と CC-Case のプロセス定義の関係 23
4.2 セキュリティ仕様のアシュアランスケース 24
4.2.1 セキュリティコンセプト定義段階 26
4.2.2 セキュリティ対策立案段階 28
4.2.3 セキュリティ要約仕様化段階 34
5 アクタ関係表による脅威分析と CC 対応 38
5.1 SARM のねらい 38
5.2 対象者，メリット 38
5.3 SARM の作成方法 38
5.3.1 AA（Asset×Attack）表 38
5.3.2 SARM 状況表 39
5.4 CC に対応した SARM の事例 41
5.4.1 AA 表による脅威抽出事例 41
5.4.2 SARM 状況表による脅威分析事例 42

5.4.3 SARM による ST 項目の分析と CC 対応の工夫 47
5.5 スパイラルレビュー手法 49
5.6 詳細レビューによる攻撃者による具体的なタスク分析 49
5.7 SARM と i*-Liu 法のゴール等価性 51
5.7.1 ゴール関係 51
5.7.2 ゴール関係に基づく等価性について 53
5.7.3 ゴール関係の例 54
5.8 研究仮説の評価 56
5.8.1 評価方法 56
5.8.2 ワークショップの開催とアンケートの実施 56
5.8.3 アンケートに基づく仮説の検証 58
5.8.4 スパイラルレビューの仮説検証と初期評価 58
5.8.5 詳細レビューの仮説検証 59
5.8.6 SARM における研究の限界 59
5.8.7 SARM の効果 59
6 ケーススタディ 60
6.1 具体モデルでの適用事例 60
6.2 セキュリティコンセプト定義段階のアシュアランスケースの具体モデル 60
6.3 セキュリティ対策立案段階段階のアシュアランスケースの具体モデル 62
6.4 セキュリティ要約仕様化段階のアシュアランスケースの具体モデル 76
7 考察 80
7.1 要求段階の CC-Case の特長 80
7.1.1 要求分析と保証の手法 80
7.1.2 ステークホルダーの観点でみた利点 81
7.2 セキュリティ課題の詳細と対応の方向性 82
7.2.1 要求の観点でのセキュリティ課題の詳細と対応の方向性 82
7.2.2 保証の観点でのセキュリティ課題の詳細と対応の方向性 84
7.3 システム開発のリスクへの対処 85
7.3.1 システムリスクへの対処の強化 85
7.3.2 事業継続リスクへの対応 88
7.3.3 顧客合意リスクへの対処 90
7.4 CC の課題解決 91
7.5 アシュアランスケースの課題解決 93
8 結論 95
8.1 まとめ 95
8.2 今後の課題 96

謝辞
参考文献
付録Ａ
付録Ｂ
付録Ｃ　研究業績一覧

1　序論

1.1　本研究の概要

近年政府機関や企業へのサイバー攻撃や遠隔操作ウイルス事件など様々なセキュリティ事故が頻発し，メディアを騒がせている．また金銭搾取を目的としてフィッシング詐欺，スマートデバイスを狙った犯行の横行など，個人ユーザに対しても各種の脅威が取り巻いている．こうした脅威はシステム，ソフトウェアの脆弱性を突いて攻撃を仕掛けてくる．

より巧妙化する脅威に対して，より安全なシステム・ソフトウェアを開発するにはどうしたらよいだろうか？解決方法として，開発者に対する教育と訓練，経験の伝達，プロジェクト管理の徹底，運用管理の向上，セキュリティ方針の厳密化などとともに，開発方法論からの対応が必要である．システム・ソフトウェアの作りの仕組みの中に脅威への対抗手段を含めることがより根本的な対策になりうるからである．

システム開発の観点からの取り組みには要求，設計，実装，テスト，保守の各段階からの対応があり，全開発工程に対して安全性を考慮した方法論が望まれる．設計段階ではセキュリティプロトコルの検証，実装段階ではセキュリティメカニズム，セキュリティを意識したコーディング規約，テスト段階では侵入テスト，脆弱性テスト，運用段階ではセキュリティアップデートによる取り組みが可能である．しかし要求段階においては「2.2.1 セキュリティ要求分析手法」に後述するように，セキュリティ要求に関して様々な研究がなされているが，セキュリティ要求を抽出・分析・仕様化，妥当性確認，要求管理する全段階をサポートしている要求分析手法もセキュリティ要求分析の標準的な手法もまだできていない．つまり現在のシステム開発方法論は，要求分析，要件定義プロセスにおいてセキュリティの獲得，分析，定義を行っていないなどセキュリティ要求の取り扱いが不十分な状況にある．

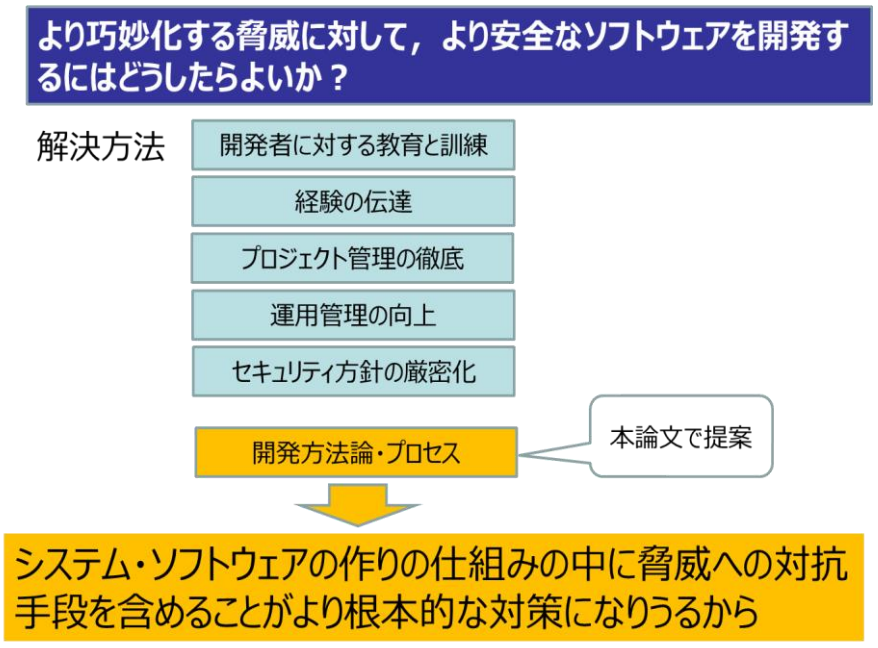


図 1-1　開発方法論・プロセスからの対応

そこで本論文ではシステム開発方法論の現状を踏まえ，より巧妙化する脅威に対して，より安全なシステム・ソフトウェアを開発するために CC-Case と名付けた CC とアシュアランスケースの長所を統合したセキュリティ要求分析手法かつ保証手法を提案する.

1.2 本研究の特徴

CC-Case は以下の特徴をもつ.

本論文で提案する CC-Case は情報セキュリティ評価基準であるコモンクライテリア（CC：Common Criteria. ISO/IEC15408 と同義）[1][2][3]とアシュアランスケース[4]にもとづく体系的な要求分析手順を明確化している.

CC-Case はライフサイクルの全段階に対して安全性を考慮したライフサイクルプロセスをコモンクライテリア(CC)に基づいて定義し，アシュアランスケースで表記している.

ライフサイクルの中でも要求段階における CC-Case はセキュリティ要求を獲得する際の技術的な難しさに対応することと同時に CC 準拠の保証をする. すなわち CC-Case は，CC に則り要求分析の段階で顧客と合意した範囲におけるセキュリティ保証要件を定め，保証をするために必要なセキュリティ機能要件を，CC に準拠して網羅的に抽出・分析・妥当性検証・仕様化・管理を行う要求分析手法である.

更に CC-Case は，脅威に対して保証できる範囲を明確にし，CC に基づくセキュリティ仕様をアシュアランスケースで検証し，顧客と合意の上で決定できる手法である．セキュリティ要求分析の手法は数多いが，CC 準拠と顧客合意，アシュアランスケースで検証による保証を伴う手法は皆無であり，CC-Case の特徴である.

更に本研究では，アクタ関係表によるセキュリティ要求分析手法 SARM を提案している．SARM は一般の機能に対する要求分析に追加してセキュリティ要求分析のできる手法であり，網羅性の高い脅威分析を可能にしている．CC-Case はシステム・ソフトウェアの作りの仕組みの中に脅威への対抗手段として CC に対応した脅威分析を実施する工夫した SARM を含んでいる.

CC-Case は複数の技術要素・手法を組み合わせて，現在の開発におけるセキュリティ上の課題を解決できる仕組みを内在している．そしてその課題解決方法により各種リスクへの対処を行い，CC やアシュアランスケースに内在する課題も解決する.

1.3 本論文の構成

はじめに，本章「序論」で本研究の概要，特徴，構成を示す.

2 章「研究の背景」では 2.1 節にシステム開発の要求・保証の現状とリスクについてセキュリティ要求の分析，セキュリティ対策と保証，システム開発のリスクとアシュアランスケースの観点から論じる．また 2.2 節に先行研究として，セキュリティ要求分析手法，i*-Liu 法，アクタ関係表（ARM）による要求分析，アシュアランスケース，セキュリティケース，コモンクライテリアを説明する.

3 章の「CC-Case の全体像」では，3.1 節には CC-Case の定義・目的，3.2 節には対象範囲・適用対象とアシュアランスケースの役割，3.3 節にはライフサイクルプロセスの構造とその詳細について提示する. CC-Case の目的は開発のセキュリティ上の課題を解決するため，ソフトウェア開発方法論・プロセスからセキュアなシステム開発への対応を実施することである．このセキュリティ上の課題に対して，どのような要素技術で対応するのかを 3~5 章で説明し，6 章ケーススタディではそ

の具体例を示す.

4 章の「要求段階の CC-Case」では 4.1 節でコモンクライテリアにもとづく体系的な要求分析手順や提案手法のセキュリティ保証の詳細に関して，ST の構成とセキュリティ要求分析，検証・妥当性確認のプロセス，SARM と CC-Case のプロセス定義の関係等から説明する．4.2 節ではセキュリティ仕様のアシュアランスケースをセキュリティコンセプト定義段階，セキュリティ対策立案段階，セキュリティ要約仕様化段階ごとに提示する．更に各段階の最下位ゴールの目的，プレーヤー，出力に対する確認方法,プロセス（入力・手続き・出力）を提示する.

5 章の「アクタ関係表による脅威分析と CC 対応」では, 5.1 節 SARM のねらい, 5.2 節対象者, メリット, 5.3 節 SARM の作成方法, 5.5 節スパイラルレビュー手法,

5.6 節 詳細レビューによる攻撃者による具体的なタスク分析，5.7 節 SARM と i*-Liu 法のゴール等価性，5.8 節研究仮説の評価でアクタ関係表によるセキュリティ要求分析手法 SARM を提案している．更に 5.4 節 CC に対応した SARM の事例で SARM の CC 対応について説明する.

6 章の「ケーススタディ」では，セキュリティコンセプト定義段階，セキュリティ対策立案段階，セキュリティ要約仕様化段階の具体モデルの適用例を示す．6 章に提示するアシュアランスケースの証跡の内容は付録 A または付録 B に記載する.

7 章「考察」では CC-Case の利点や開発のセキュリティ上の課題に対してどのように課題解決するのかを考察し, CC-Case の目的はどのように達成できるのかを示す．7.1 節には要求段階の CC-Case の特長を要求分析と保証の手法，およびステークホルダーの観点でみた利点から論ずる．7.2 節には主な課題解決方法について，順次その内容を吟味する．7.3 節には主な課題解決方法の相互関係を示す．また各課題解決方法をもとにシステムリスク，事業継続リスク，顧客合意リスクに対してどのように対処しているかをそれぞれ説明する．更に CC-Case の特長を生かすことにより，7.4 節には CC，7.5 節にはアシュアランスケース自体に内在する問題点を克服できる可能性を議論する.

2　研究の背景

2.1　システム開発の要求・保証の現状とリスク

2.1.1　セキュリティ要求の分析

ソフトウェアのシステム開発において，顧客の要求を適切に把握し，実現させることは非常に大切なことである．ところが，上流工程における要求分析が不十分であるためにシステム開発に重大な影響を及ぼすことは多い．要求分析がうまくいかない理由は，顧客の要望を開発者が仕様化する際にギャップが生じるからである．すなわち，表 2-1-1 に示すように顧客（利用者）の早く，安く，良いものを使いやすくといった要望に対して，開発者は利害関係者の合意を図り，IT 技術・方式を決め，要員のスキルやソフトウェアの再利用方法などを定め，要求仕様を作成しなければならない．この顧客要望の要求仕様への変換時にギャップが生じる．

表 2-1-1 要求分析におけるギャップ

	顧客	VS 問題点	開発者
一般の機能要求	・スピード（早く） ・費用（安く） ・品質（良いものを） ・使いやすく	変換時にギャップ	・仕様の固まり具合 ・利害関係者の合意 ・ＩＴ技術・方式 ・スキル・再利用
セキュリティ要求	・セキュリティは難しいので任せるが費用がかかるのは困る ・特別な要求はないけど、個人情報漏えいは困る ・内部統制も一緒に考えてほしい ・社内の犯行は想定外	更に大きなギャップ	・リスクの洗い出しに漏れはないか不明 ・各工程ごとに何をどこまでやればいいのかわからない ・新たな脅威への対処は現行の設計では無理 ・リスク対策の費用をお客様は負担してくれない

セキュリティ要求分析は，ソフトウェアの一般的機能の要求分析に比べて，顧客と開発者のギャップは更に大きくなる．セキュリティ要求分析は，分析すべき情報が多様であり，お互いが複雑に関連していることやシステムを取り巻く状況の変化が目まぐるしい中で，新たな攻撃に早く対処する必要があること，セキュリティの実現には，利便性などの他の特性と相反する要求が生じ，バランスを取る必要があるなどの難しい課題を抱えていることがその理由として挙げられる．例えば，顧客はセキュリティ機能自体に興味がないことが多く，問題が起きないこと，費用がかからないことを漠然と求める．これに対して，開発者は脅威・リスクの洗い出しに漏れはないかが不明確であり，各工程で何をどこまでやればいいのかも不明確であり，新たな脅威への対処は一般にはわからないので困難であるといった課題を抱えながら，顧客と何らかの合意をとってセキュリティ仕様を定めていかなければならない．

セキュリティ要求は，情報システムに求められる要件のうち一般的機能に関するもの以外の要件を指す非機能要求の 1 つとされる．セキュリティに対して漠然

とした要望はあるものの，セキュリティ自体の知識にとぼしいのでセキュリティ要求は開発者に任せるという顧客が一般的である．また，開発者側でもセキュリティの専門家ではないことが多いので，セキュリティ要求を仕様に入れるのは難しい．こうした問題を抱えているため，セキュリティ要求に関して手順も手法も普遍的に確立されたものはないのが実情である．

セキュリティ要求には，まず脅威の識別，抽出が必要だが，的確に脅威を洗い出すことが必要である．そこで本論文で提案する手法は攻撃シーンと守るべき資源（アセット）との組み合わせを抽出し，同じ表形式を用いて通常機能と攻撃を分析できる網羅性の高い脅威分析を可能としている．更にセキュリティ要求には，多様な IT システム，製品の要求に対して，幅広く対応できることが必要である．

2.1.2 セキュリティ対策と保証

セキュリティ要求には，まず脅威の識別，抽出が必要だが，的確に脅威を洗い出したとしても，それに対する対策が不十分では，顧客が望む品質を確保したとはいえない．システムや製品が望ましい性質をもち，危険な状況に陥らない対策立案と実施及び保証を顧客から望まれているのである．

この現状の課題を解決するために，本論文で提案する手法は CC[1][2][3]とアシュアランスケース[4]を用い，セキュリティ仕様を顧客と合意の上で決定を可能としている．セキュリティ要求分析には様々な手法があるが，セキュリティが必要になる状況の明確化，特定シーンにおける脅威のモデル化やそれに対する対策立案の手法がほとんどである．しかし提案手法はセキュリティ要求分析とともに対策の保証も可能としている．

尚，「本論文での保証とは何なのか」を説明するために，ソフトウェア品質保証とセキュリティ保証の意味について以下に示す．

(1) ソフトウェア品質保証

日本語で保証に該当する英語には，assurance や warranty，guarantee などがある．assurance は「製品が品質基準に合致しているかを，設計・試作・製造・検査の全ての工程で確認する仕組みがあり，それを実行していることを保証する，請合う，自信をもって言うこと」である．これに対して warranty は「出荷後製品が故障したら，無料で修理又は取り替えをする事を利用者に対して保証すること」という意味で使う．一方 guarantee は「もし保証したことが出来なければ，賠償責任が生じるような保証」という意味によく使われる．ソフトウェアの品質保証をする際の保証は assurance の意味であり，保証のためには要求やニーズに適合しているかの確認が必要になる．

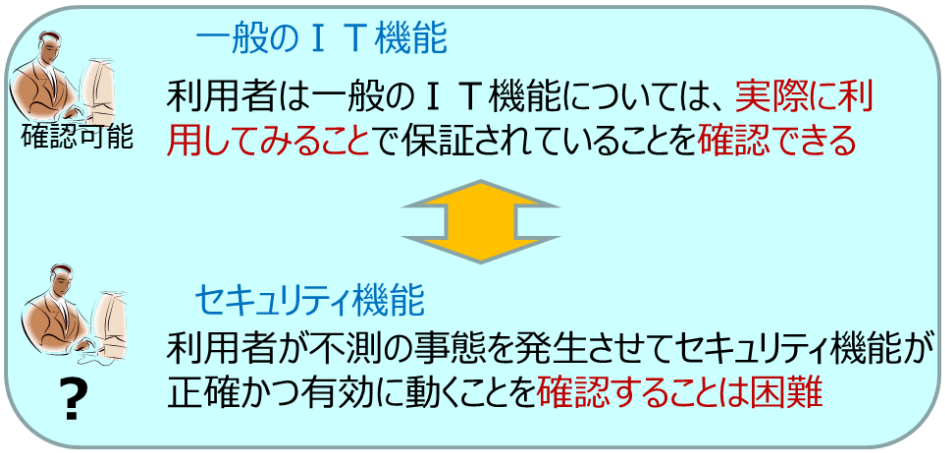
IEEE Std1012-2004[5]によれば，ソフトウェア品質保証のための確認プロセスには開発活動による生産物が開発活動に対する要求に適合していること判定する活動（検証：verification）と，開発されたソフトウェアが意図された利用法とユーザニーズに適合していることを判定する活動（妥当性確認：validation）がある.つまり，ソフトウェアを正しく作っていることを判定するのが検証であり，ソフトウェアが正しいことを判定するのが妥当性確認である[5].

(2)セキュリティ保証

ソフトウェアに対する品質保証は，どのような機能をどのように実現するのかを示す必要があるため困難である． ソフトウェアの品質保証の中でもセキュリティ機能に対する品質保証は，新たな脅威がどのように発生するか予測不可能なため困難さを増す．セキュリティ機能とは個人情報や機密情報を暴露されたり,システムの稼働を妨害されたりすることがないように管理する機能である．セキュリ

ティ機能には①正確に動作する②有効に機能することが要求される[3].一般の IT 機能であれば，利用者はその機能について，実際に利用してみることで保証されていることを確認できる．しかしセキュリティ機能は利用者が不測の事態を発生させてセキュリティ機能が正確かつ有効に動くことを確認することは困難である(図 2-1-2 参照). そこで開発者自身がセキュリティ保証を検証しなければならない.

図 2-1-2　セキュリティ機能の確認



2.1.3 システム開発のリスクとアシュアランスケース

システムの開発において，顧客の要求を適切に把握し実現させることは非常に大切なことである．しかし上流工程における要求分析が不十分であるためにシステム開発に重大な影響を及ぼすことは多い．システムや製品が望ましい性質をもち，危険な状況に陥らないために適切に脅威を分析し，対策をたて顧客の要望を踏まえたうえで対策を実施し，提供するシステムに保証することが顧客から望まれている．システム開発におけるリスクは顧客合意リスク，事業継続リスク，システムリスク[6]の 3 つに分類できる

表 2-1-3　システム開発におけるリスク

分類	従来の開発手法	リスク
顧客合意リスク	対象外	訴訟リスク
ビジネス継続性リスク	対象外	災害・障害等によるビジネスの中断、休止リスク
システムリスク	開発，設計，実装，運用 *第三者による検証はない	開発活動の妥当性を説明することができないリスク

顧客合意リスクは訴訟リスクであり，事業継続リスクは事業継続ができなくなるリスクである．システムリスクは開発活動の妥当性を説明する際のリスクである．しかしながら伝統的な開発において，システムリスクのみが考慮されてきており，他のリスクは考慮されてこなかった．会社のブランド価値は 3 種類のリスクが混在すると大きな経済的なダメージを受けることになる．それゆえ望ましくないリスクに対して回避，低減，移転などの適切な対応をとることが大事になる．リスク管理に対するアシュアランスケースは現代のシステム開発におけるリスクを回避する手法となる．システムがセキュアであることの要求が顧客に対して対象物の証拠によってサポートされることが重要だからである.

セキュリティリスクの対応は大変難しい．何故ならば，セキュリティリスクを適切に扱い，脅威を減らすためには目に見えない攻撃者と戦う必要があるからである．セキュリティリスクも一般的なリスクと同様に顧客合意リスク，事業継続

リスク，システムリスクに分類できる．

セキュリティの顧客合意リスクにはセキュリティ事故が発生した際などの訴訟リスクが考えられる．このリスクに対応するためには契約における顧客合意の正当性を示す証拠が必要になる．

セキュリティの事業継続リスクはセキュリティ上のインシデントによりサービス提供段階における事業継続ができなくなるリスクである．このリスクに対応するためにはリスクモニタリングとコントロールが必要になる．リスクモニタリングの結果はログなどにより，証跡として残しておくことが求められる．

セキュリティのシステムリスクはセキュリティに関わるシステム開発やプロジェクトの進捗，結果，成果物に肯定的または否定的に影響を与える予期できないイベントや活動と定義できる.セキュリティのシステムリスクはセキュリティシステム・製品の要求分析，開発，実装，テストに開発活動を説明するさいのリスクである．このリスクに対応するためにはセキュリティのリスク識別，分析，対応計画の正当性を示す証拠が必要になる．

従来は一般のリスクと同様セキュリティにおいてもシステムリスクのみが検討されてきて，顧客合意リスクや事業継続リスクはセキュリティにおいてもあまり検討されてこなかった．またシステムリスク対応のための実装検証確認は不十分である．「システムがセキュアである」という顧客要求を満たすことを証拠によって示すことが重要である．

2.2 先行研究

2.2.1 セキュリティ要求分析手法

セキュリティ要求分析では，顧客は要求に基づく機能要求の分析に加えて攻撃者の存在を考慮した非機能要求の分析を必要とする．そこでセキュリティ要求はアセットに対する脅威とその対策の記述が必須となる.セキュリティ要求分析のできる手法にミスユースケース[7]，Secure Tropos[8]，i*-Liu 法[9]，KAOS[10]，Abuse Frames[11]などがある．いずれの手法もセキュリティを考慮した脅威分析やそれに対する対策立案・仕様化の手法だが，明示されない非機能要求に関してあらゆる要件をつくすことは難しいのが実情である．セキュリティ要求は非機能要求の一つである．非機能要求について，非機能的要求を明示的に表現し，組織的に取り扱うことが出来る枠組みである NFR フレームワーク[12]が示されている．また発注者と受注者との認識の行き違いや，互いの意図とは異なる理解をしたことに気づかないまま開発が進んでしまうこと状態を防止することを目的としてセキュリティ要求も含めた非機能要求グレード[13]が示されている．これは重要な項目から段階的に詳細化しながら非機能要求の確認を行うツール群である．SQUARE[14][15]はセキュリティのシステム品質を高めるために定められた特定の手法によらないプロセスモデルである. SQUARE は生産物の定義に基づいてリスク分析し，セキュリティ要求を抽出・優先順位付け・レビューする手順である.マイクロソフトのセキュリティ開発ライフサイクル[16] はデータフロー図を詳細化し脅威の観点 STRIDE で脅威分析を実施し，設計による安全性確保を重視し設計段階でセキュリティ要求を抽出している．尚，STRIDE とはマイクロソフトよるアプリケーションに対するセキュリティ上の脅威の分類名の頭文字から 成る語である．Spoofing (なりすまし)，Tampering (改ざん)，Repudiation (否認)，Information Disclosure (情報漏えい)，Denial of Service (サービス拒否)，および Elevation of Privilege (特権の昇格) に分類される．

このようにセキュリティ要求に関して様々な研究がなされている[17]が，セキュリティ要求を抽出・分析・仕様化，妥当性確認，要求管理する全段階をサポートしている要求分析手法もセキュリティ要求分析の標準的な手法もまだできていないのが現状である．

2.2.2 i*-Liu 法

ゴール指向要求分析は，代表的な要求分析法の 1 つであり，個々の要求にはその要求の元となる上位目標があるという前提のもとに，ゴール分解を通して要求の導出を行おうとする手法である．ゴール指向要求分析の特徴は，要求の正当性の確保に重点を置いた分析が行われるところにある．ゴール指向要求分析に着目した要求分析手法の 1 つである i*[18]はステークホルダやシステムをアクタとしてモデル化し，利害関係を，アクタ間の依存関係としてモデル化する有効な手法として期待されている．アクタとは関係者を意味し，モデルを構成する要素の 1 つで、システム（主体）にアクセスする利用者や外部システムが、システム（主体）に対して果たす役割を示したものである．

ゴール指向要求分析のための i*手法をセキュリティ要求分析が実施できるように拡張した手法が i*-Liu 法である．i*の SD(Strategic Dependency)図では，ビジネスを構成するアクタ間の依存関係を現状分析（as-is）する．これに対して i*の SR(Strategic Rational)図は，各アクタ内部で，アクタがソフトゴールを達成するた

めのゴール，タスク（作業），リソース（資源）との階層的な関係を分析できる．尚，ゴールとは開発対象システムが達成すべき目標，ソフトゴールとはシステムに対する非機能要求．定性的であいまいな要求を意味する．

i*-Liu 法では表 2-2-2 に示すように，i*の SD 図と SR 図の分析に加えて攻撃者，悪意，脆弱性，攻撃方法とその対策を分析できる．分析の方法は i*の図式要素に加えて，攻撃者をアクタとして識別する．攻撃者は対応するアクタと同じように，ゴール・ソフトゴール・タスク・リソースを持つ．なお，i*-Liu 法の具体的な記述方法は 5 章で説明する．

表 2-2-2　i*と i*-Liu 法のもつモデルの比較表（○：有，-：無）

モデル	i*	i*-Liu法	
SD	○	○	
SR	○	○	
攻撃者	―	○	攻撃アクタ
悪意	―	○	悪意のソフトゴール
脆弱性	―	○	攻撃対象となるリソース
攻撃方法	―	○	攻撃タスク
対策	―	○	タスク

2.2.3 アクタ関係表（ARM）による要求分析

アクタ関係行列 ARM[19] [20] [21]は，アクタがおかれる問題状況ごとにアクタ間の関係を行列で定義する方法である．アクタの数が多い場合，アクタの関係が複雑で，要求を網羅しているかどうかを i*の図では効率的に確認できない，アクタの置かれたシーンによってアクタが抱える問題や，それに伴うゴール，ソフトゴール，資源が変化する場合，i*では，これらの変化を記述できないという課題がある．これらの欠点を改善し，網羅的に i*の SD 図を作成する方法として，ARM が提唱されている．

ARM はアクタが置かれる問題状況ごとにアクタ間の関係を行列で定義する方法を用いて，網羅的にｉ＊の SD 図を作成する方法である． ARM はゴールと意図としてのソフトゴール，資源，タスクを整理したものである．ARM (Ai,Bj)には受益者 Ai から提供者 Bj への意図 I ij を記入する，また対角要素 ARM (Ai,Aj)にはアクタの内部ゴール Gi を記入する．

ARM には次の３つの有用性がある．

(1)　アクタ間の関係の網羅性を確認できる．

(2)　アクタの関連性の類似性がわかる．

(3)　登場しつつも他のアクタと関連性がないアクタを行列の疎の部分として見極めることができる．

文献[18]において，アクタ関係行列は以下のように定義されている．

【定義】ARM(A１,･･･,Aｎ)

アクタＡ１,・・・，Ａｎに対する ARM(A１,･･･,Aｎ)はｎ行ｎ列の行列である．ここで各行及び各列は，アクタ A１,･･･,Aｎに対応する．第 i 列 j 行は，アクタ Ai が Aj に対して望む意図 Iij である．また，第 i 列 j 行はアクタ Ai が持つ内部ゴール集合 GAi である．

ARMii = ｛Gik｜k=l,･･･li｝

ARMij = ｛Iijk｜k=l,･･･l（i,j）｝

【定義】ARM 要素集合

ARM の要素集合は S(ARM(A１,･･･,Aｎ))で ARM(A１,･･･,Aｎ)の行列要素からなる集合を表す.

＜ARM の作成方法＞

ARM は，ゴールと意図としてのソフトゴール，資源，タスクを整理したものである．ARM(Ai,Bj)には受益者 Ai から提供者 Bj 意図 Iij を記入する．また，対角要素 ARM(Aj,Ai)にはアクタ Ai の内部ゴール Gi を記入する.

表 2-2-3　ARM

	アクタ A	アクタ B	アクタ C
アクタ A	$G_{AB,}$ G_{Ac}	I_{AB}	I_{AC}
アクタ B	I_{BA}	$G_{AB,}$ G_{BC}	I_{BC}
アクタ C	I_{CA}	I_{CB}	$Gc_{A,}$ G_{CB}

G_{ij}：アクタ i の j に対する内部ゴール　I_{ij}：アクタ i の j に対する意図

ここでは 3 次元 ARM を例にとっているが，n 次元に拡大することで，n 個の依存関係を表現することができる.

文献では，シーン別アクタ関係行列を ARM*として別途，定義している．ARM*から i＊フレームワークの SD 図への変換規則は以下の通りであるとしている.

(規則 1)ARM*の ARM*（Ai,Bj）を Ai から Bj へのソフトゴールとする.

(規則 2)ARM*の ARM*（Bj ,Ai）を Bj から Ai へのソフトゴールとする.

(規則 3)それぞれのソフトゴールを，アクタと矢印で結ぶ.

(規則 4)矢印の向きは Ai→Ia→Bj,Bj→Ib→Ai とする.

(規則 5)各ソフトゴールに，アクタが置かれる状況 Sx を記述する.

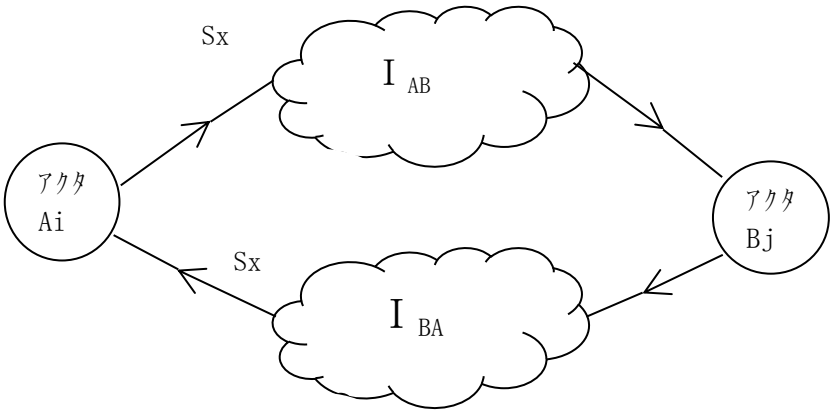


図 2-2-3　SD 図の例

2.2.4 アシュアランスケース

アシュアランスケース（assurance case）とは，テスト結果や検証結果をエビデンスとしてそれらを根拠にシステムの安全性，信頼性を議論し，システム認証者や

利用者などに保証する，あるいは確信させるためのドキュメントである[23]．アシュアランスケースは欧米で普及しているセーフティケース[24]から始まっており，近年，安全性だけでなく，ディペンダビリティやセキュリティにも使われ始めている．その場合，それぞれディペンダビリティケース，セキュリティケースと呼ばれ，アシュアランスケースはこれらを総称した手法である．アシュアランスケースは ISO/IEC15026 や OMG の ARM（Argument Metamodel）[25]と SAEM（Software Assurance Evidence　Metamodel）[26]などで標準化がすすめられている．

ISO/IEC15026 part2 では，対象範囲，適合性，利用法，アシュアランスケースの構造と内容，適用成果物などについて規定している．アシュアランスケースの構造と内容に対する最低限の要求は，システムや製品の性質に対する主張(claim)，主張に対する系統的な議論（argumentation），この議論を裏付ける証跡(evidence)，明示的な前提（explicit assumption）が含まれること，議論の途中で補助的な主張を用いることにより，最上位の主張に対して，証跡や前提を階層的に結び付けることができることである．この定義を満たすものはアシュアランスケースとみなせる．

アシュアランスケースは，解決が必要とされる具体的な表記方法を示すことにより記述が容易になる．代表的な表記方法は，欧州で約 10 年前から使用されている GSN（Goal Structuring Notation）[27]であり，要求を抽出した後の確認に用い，システムの安全性や正当性を確認することができる．他に法律分野でアシュアランスケースの理論的背景となる Toulmin Structures[28]や要求，議論，証跡のみのシンプルなアシュアランスケースである ASCAD[29]もある．日本国内では GSN を拡張した D-CASE [30] [31]が JST CREST DEOS プロジェクトで開発されている．システムのサービス提供段階においてアシュアランスケースを用いた提案[32]もなされている．

2.2.5 セキュリティケース

GSN を提唱した Kelly ら[33]が Security Assurance Cases の作成に関する既存の手法とガイダンス，セーフティケースとセキュリティケースの違いなどを述べているが，具体的に作成したセキュリティケースの事例は示していない．Goodenough [34]らはセキュリティに対するアシュアランスケース（セキュリティケース）作成の意味を説明している．Lipson H[35]らは信頼できるセキュリティケースには保証の証跡こそが重要であると主張している．

Ankrum[36]らは CC，や ISO154971，RTCA/DO-178B という 3 つの製品を保証するための規格を ASCAD でマップ化し，ASCE などのアシュアランスケースツールが有効であり，保証規格を含むアシュアランスケースは似た構造をもつことを検証している．CC に対しては，PART3 セキュリティ保証要件についてのみの検討を行っている．

Bloomfield らはセキュリティに関するアシュアランスケースの検討状況[37] [38] [39]を公開している.CC の役割と保証レベルの関係などを検討しているが，CC の規格全体をアシュアランスケースに利用する方法は検討していない．Vivas [40]らは，システム開発に伴うアシュアランスケースをプラットフォームに統合した保証手法を提唱している. PICOS（コミュニティサービスのプライバシーと識別管理）プラットフォームのもとに開発され，セキュリティのシステム開発のライフサイクルを通じてセキュリティケースを構築，維持するための方法論になっている．但し，この要求段階においては UML と同等の記法を利用している．また，システムセキュリティリスク対策を確認するためにセキュリティ CC 分解の参照モデル [6] [41] [42]が示されているが，CC のプロセスを用いた要求分析手法としてアシュ

アランスケースを用いてはいない．他にセキュリティケースを用いた対策立案方法の提案[43]がなされているが，CC による保証はなされていない．

2.2.6 コモンクライテリア

IT セキュリティ評価の国際標準であるコモンクライテリア（CC :Common Criteria ISO/IEC15408）[1]は,開発者が主張するセキュリティ保証の信頼性に関する評価の枠組みを規定したものである[3]．IT 製品（ソフトウェア，ハードウェア）や情報システムを評価・認証する制度として，日本では「IT セキュリティ評価及び認証制度」が運用されている．また CC 相互承認協定により，自国認証以外の幅広い CC 認証済み製品の国際相互流通を可能としている．

セキュリティ要求のうち，IT を使って実現する部分の信頼性が保証されていることを評価するための国際標準が CC である．CC は，情報技術セキュリティに関連したシステムや製品の開発者だけでなく，製品を導入・利用する消費者，システムや製品の評価者などに，有用な規格である．CC は，評価対象（TOE : Target of Evaluation）と運用環境を正確にモデル化し，資産，脅威および対抗策によるセキュリティの概念と関係に基づいて，セキュリティ機能の評価をする．

CC のパート 1 には評価対象のセキュリティ目標（ST: Security Target）やプロテクションプロファイル (PP：Protection Profile)に記載すべき内容が規定されている(図 2-2-6-1)．ST は評価対象のシステムが装備するセキュリティ機能を適切に定義し，セキュリティ保証の目標を規定した文書である．ST は，情報セキュリティ評価を行う際には必須となる文書である．また，PP は TOE の個々の種別に対するセキュリティ要求仕様のセットである．

CC のパート 2 に TOE のセキュリティ機能要件（SFR：Security Functional Requirement）が規定されている．セキュリティ機能とは，セキュリティ対策方針つまり，識別された脅威に対抗することを実現するために必要な評価対象のすべてのハードウェア，ソフトウェア，ファームウェア機能の集合である．セキュリティ機能要件はセキュリティ機能の確からしさを検証するために準形式的な言語で記載する．準形式化するために，CC パート 2 には機能要件がカタログ的に列挙されており，選択等の操作にパラメータやリストを特定することにより，準形式的に具体的なセキュリティ機能要件の記載ができる．図 2-2-6-2 は CC パート 2 の規定[1]の一部抜粋であり，図 2-2-6-3 が規定を適用した事例である．具体的な適用の一例を説明すると，図 2-2-6-2 において機能要件の FIA_AFL1.1 が規定されており，「TSF は，[割付：認証事象のリスト] 」となっている．そこで図 2-2-6-3 のように「最後に成功した認証以降の各クライアント操作員の認証」，「最後に成功した認証以降の各サーバ管理者の認証」の割付の特定ができる．

CC のパート 3 にはセキュリティ保証要件（SAR：Security Assurance Requirement）が規定されている．EAL（Evaluation Assurance Level）と呼ばれる評価保証レベルを定義し，EAL とそのレベルに合わせた実装方法への要求が規定されている．

図 2-2-6-1　CC 構成と ST の記載内容

CCパート2の規定（一部抜粋）

FIA_AFL.1.1

TSFは、[割付：認証事象のリスト]に関して、[選択：[割付：正の整数値]，「[割付：許容可能な値の範囲]内における管理者設定可能な正の整数値」]回の不成功認証試行が生じたときを検出しなければならない。

図 2-2-6-2　CC パート 2 の規定

準形式的な記載事例

[割付：認証事象のリスト]：

・最後に成功した認証以降の各クライアント操作員の認証

・最後に成功した認証以降の各サーバ管理者の認証

[選択：[割付：正の整数値]，「[割付：許容可能な値の範囲]内における管理者設定可能な正の整数値」]：「1～5回内における管理者設定可能な正の整数値」

図 2-2-6-3　準形式的な記載事例

3 CC-Case の全体像

3.1 CC-Case の定義・目的

CC-Case を「セキュリティ要求分析と保証の開発方法論」と定義する. ここで「セキュリティ要求分析」には脅威への対抗手段を含め，統合開発方法論の「統合」はセキュリティ要求分析を実施するとともに CC 準拠の保証を実施することを意味している．一般にシステム開発手法とはシステムの作り方を指す，広義であいまいな概念であるに対し，システム開発方法論とは体系化されたシステムの作り方のことであり，何らかの原理・意図・観点に基づいて，各種の方法・手順・手段を統合した知的体系として定義される．本論文のタイトルにおいて CC-Case はセキュリティ要求分析と保証の統合手法としているが、1.2 節等に示した CC-Case の特長を鑑みると，手法というより各種技術要素・手法を組み合わせたフレームワークを提示した開発方法論という方がより適切であるため，定義としては開発方法論を用いる.

CC-Case の目的は，より巧妙化する脅威に対して，より安全なシステム・ソフトウェアを開発するために，現在の開発におけるセキュリティ上の課題を解決できるセキュアなシステム開発への対応を実施することである.

では CC-Case の目的に掲げた「開発のセキュリティ上の課題とは何で，その解決方法とは何か？」について概説する．具体的な開発におけるセキュリティ上の課題（図 3-1 の a~h）は，セキュリティ要求獲得（a~c），セキュリティ要求分析・実装・管理©，システム・製品に対するセキュリティ保証の課題（e~h）に分類できる．これらの課題それぞれに対して CC-Case は各要素技術を用いて対処している．要素技術は CC，アシュアランスケース,SARM に集約され，これらの長所を統合した課題対応方法により, CC-Case はセキュリティ要求分析を実施するとともに CC 準拠の保証を実施する.

セキュリティ要求を獲得する際の技術的な難しさには①扱う情報に対する複雑性，②状況の変化，③トレードオフの 3 つの観点があると言われている[44].

要求における課題（a~c）はこの 3 つに(①~③)に対応する．現状のセキュリティ要求分析手法は，特定のシーンにおいての脅威分析やそれに対する対策立案の手法がほとんどであり，上記 3 つの観点に網羅的に適切な対応が可能なセキュリティ要求分析手法はまだ確立されていない.

そこで CC-Case では「a.情報に対する複雑性があるため，セキュリティ要求の獲得が難しい」ことに関して，CC（パート 1）を用いた「①セキュリティ仕様検討のプロセス明示化」で対応する（7.3.1 項参照）.

「b.脅威等の状況変化がはげしくセキュリティ要求の獲得と対策が難しい」課題のセキュリティ要求の獲得に関して，「②一般の要求分析に組み込んだ脅威分析」SARM で対応する（5 章参照）．対策に関しては CC を用いた「④要求，設計，実装，テスト，保守のライフサイクルプロセス対応」で対応する（7.3.2 項参照）.

「c.他の要件とのトレードオフを考慮しなければならないためセキュリティ要求の獲得が難しい」ことに関しては主に「②一般の要求分析に組み込んだ脅威分析」SARM で対応する（7.3.1 項参照）.

「d.システム・製品の仕様要求，セキュリティ要求間の対応関係や論理構造を分析・管理・共有する手段が確立されていない」ことに関しては CC（パート 1）を用いた「①セキュリティ仕様検討のプロセス明示化」と CC（パート 2）を用いた「④セキュリティ機能要件の利用」（7.3.1 項参照），アシュアランスケースを用

いた「⑥論理的証拠の提示」（7.3.1 項参照）で対応する．

要求と保証の双方に関わる課題として「e.仕様が固まった後にセキュリティ要求が作成され，保証要件は不明確である」がある．一般に要求分析において，保証要件までの検討は行わず，保証要件は不明確になりがちである．しかし CC-Case ではこのタイミングのずれを回避し「⑤要求分析と同時に保証要件を決定」（7.3.1 項参照）している．

「f.設計・開発の確実な実施への品質説明力が必要である」は 1.3 節の表 1-3　システムリスクに相当し，アシュアランスケースを用いた「⑥論理的証拠の提示」と「⑦セキュリティゴールに対する検証」（7.3.1 項参照）で対応する．

「g.システム・製品に対して顧客から訴訟を受ける可能性がある」は 2.1.3 節の表 2-1-3　顧客合意リスクに相当し，アシュアランスケースを用いた「⑧顧客との合意プロセスの明示」（7.3.3 項参照）で対応する．

「h.システム・製品によって求めるセキュリティ保証の度合いは異なる」は「⑨CC 基準での評価」（7.3.3 項参照）や CC（パート 3）を用いた「⑩セキュリティ保証要件による保証」（7.3.3 項参照）で対応する．

上記の CC，アシュアランスケース，SARM の要素技術についての詳細は 3~5 章で説明する．課題解決方法の考察は 7 章に述べる．

尚，CC-Case はライフサイクルの全段階に対して安全性を考慮しているが，3.1.1 項に示したようにのシステム開発方法論は，セキュリティ要求の取り扱いが不十分であるため，本論文では特に要求段階のプロセスに重点を当てており，3 章ではライフサイクルプロセスの概要を示し，4 章以降は要求段階を通じて詳述する．

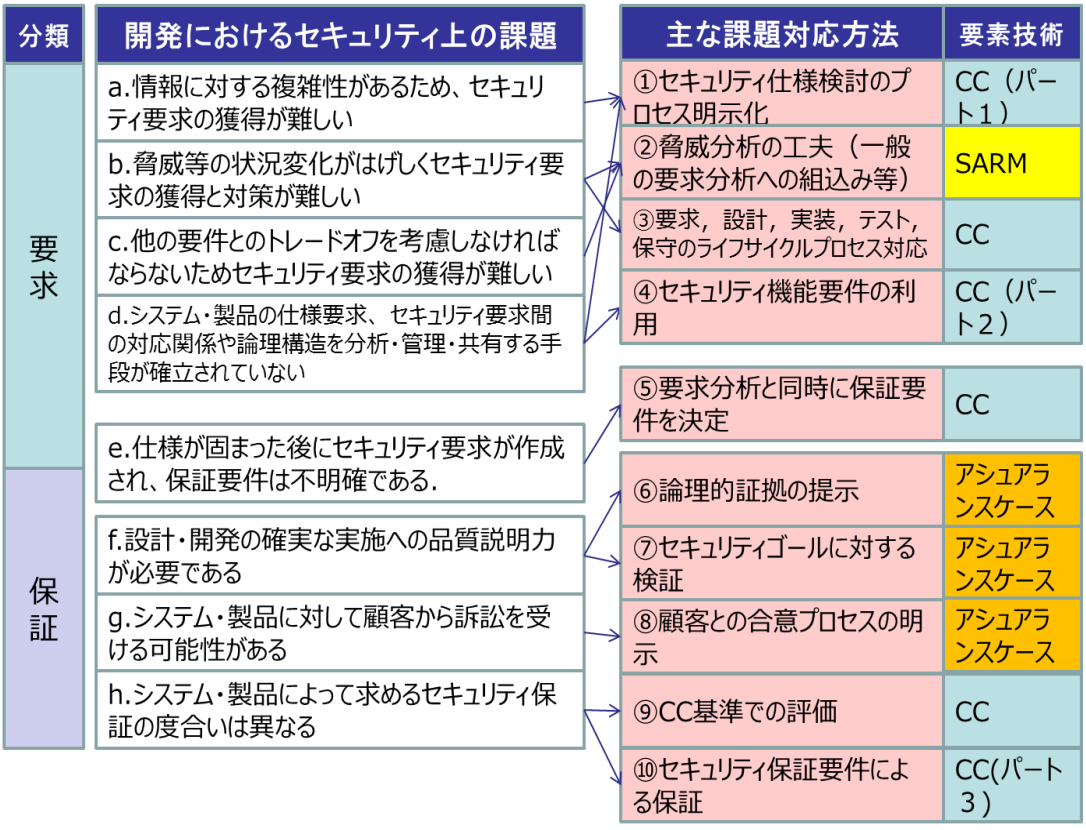


図 3-1 開発のセキュリティ課題に対する CC-Case の解決方法と要素技術

3.2 CC-Case の対象範囲・適用対象とアシュアランスケースの役割

CC-Case の対象範囲は要求，設計，実装，テスト，保守段階までのライフサイクルの全段階を含む．このライフサイクルの全段階のプロセス定義をライフサイクルプロセスとする．

また CC-Case の適用対象はシステムまたは製品である．CC-Case は顧客と開発者との合意を形成する手法であるが，製品開発など，仕様を決める際に承認を取る特定の顧客がいない場合は，要件を決めるうえでの関係者と読み替える．

CC-Case はアシュアランスケースの代表的な記法である GSN[27]を使用する．GSN の構成要素を表 3-2 に示す．GSN の構成要素がアシュアランスケースの中でどのように用いられているかを図 3-3-2 に具体的に説明する．

表 3-2 GSN の構成要素

名称	図式要素	説明
ゴール（主張）		システムが達成すべき性質を示す。下位の主張や説明に分かれる
戦略（説明）		主張の達成を導くために必要となる説明を示す。下位の主張や説明に分解される
コンテキスト（前提）		主張や説明が必要となる理由としての外部情報を示す
未定義要素		まだ具体化できていない主張や説明であることを示す
証跡		主張や説明が達成できることを示す証拠

3.3 CC-Case のライフサイクルプロセス

2.1.3 節に示した 3 種類のセキュリティリスクにはシステムリスクや事業継続リスクが含まれている．システムリスクに対応するためには要求を正しくシステム・製品に実装することが必要である．事業継続リスクに対応するためにはシステム・製品のライフサイクルサポートが求められる．これらのより適切なリスク対応のためにはライフサイクルプロセスを規定した手法が望まれるため，CC-Case はライフサイクルプロセスを具備している．

3.3.1 ライフサイクルプロセスの構造

CC-Case は論理モデルと具体モデルの 2 層構造をもつ．図 3-3-1 に論理モデルと具体モデルの関係を示す．具体的な分け方として，論理モデルは図の上位層にあるライフサイクルプロセスと中位層にある各段階のプロセスをもつ．論理モデルはライフサイクルプロセスの最下位のゴールをトップゴールとして各段階のプロセスを提示する．また下位層は具体モデルである．具体モデルは各段階のプロセスの最下位のゴールをトップゴールとして実際の事例を記述する．

論理モデルは手順を定めたプロセスのアシュアランスケースである．具体モデルは論理モデルの最下層ゴールの下に作成される実際のケースに応じた成果物のアシュアランスケースである．論理モデルは検証の対象を具体モデルに明記できるレベルまで手順を定めている．論理モデルがそれ以上展開できない理由は，要求段階における ST の各項目のレベルにそろえた定義をしており，CC に則ったシステム・製品の対応ができるようにそろえているからである．

要求段階の場合，論理モデルはセキュリティ仕様検討のプロセス（ST に含むべき項目）の明示と顧客合意リスクに対処するための妥当性確認項目の明示とする．また具体モデルは対象となるシステム・製品の ST を満たすセキュリティ要求仕様と顧客との合意結果である．

具体モデルは証跡を最下層に提示するまで適宜論理分解されて記述される．具体モデルは実際のケースにおける証跡と合意による顧客の承認結果を証跡として残す．各種証跡は次々と貯まりその結果，論証に使えるものになる．要望は確定的ではなく，変化することがありうるが，変化に応じた証跡を残すことが必要である．そのため CC-Case では，全ての証跡を DB に格納し，変更要求に随時応じられるようにする．

論理モデルと具体モデルに分ける理由は，論理モデルは下位に続く具体モデルの検証を行う役割があることや以下のメリットを生むことである．

論理モデルでプロセスが規定され，具体モデルのみを更新すれば良いため，修正箇所の特定が早く，変更要求に伴う対応漏れを低減させることが期待できる．

CC-Case は要求管理 DB に CC 認証製品のアーキテクチャを具体モデルとしてモジュール化して管理することにより，部分再利用時のアーキテクチャ上の整合確保がしやすくなり， 再利用を容易化でき，分析漏れによる脅威や脆弱性の低減が期待できる．

CC に基づいた手順は論理モデルとして共通化しており作成不要である．また収集すべき証跡も規定されているため，これらの規定のないアシュアランスケース構築に比べて，生産性向上が期待される．

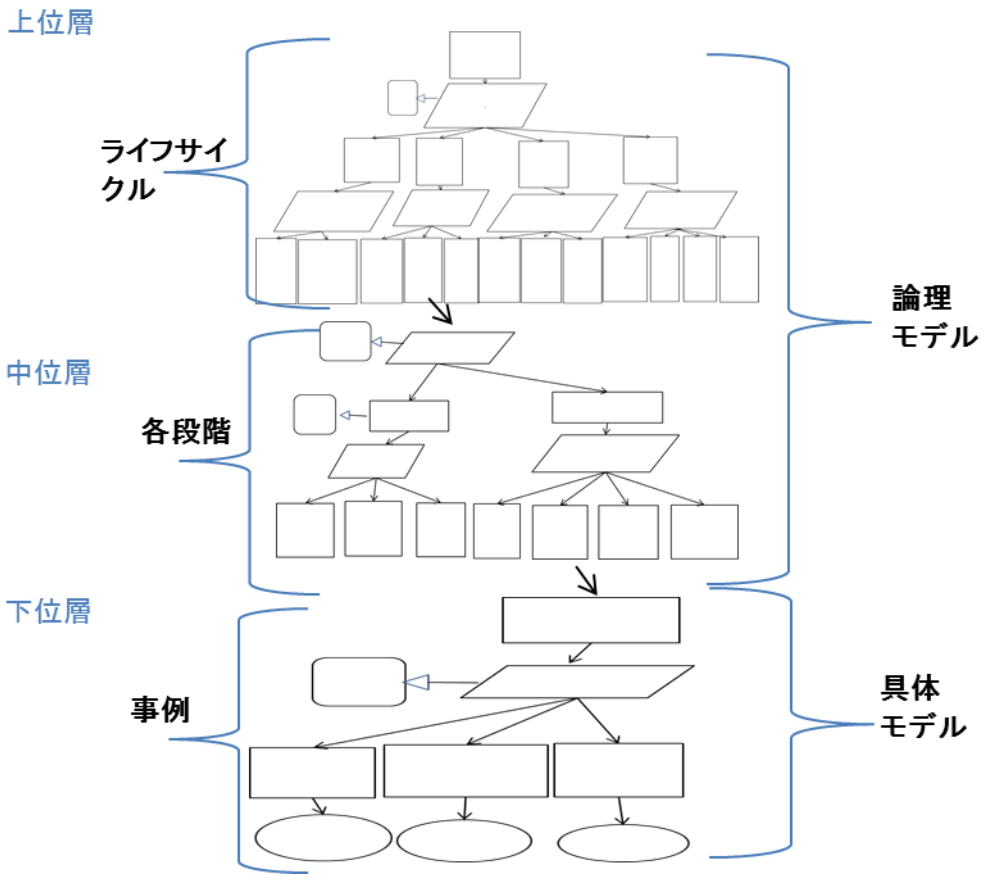


図 3-3-1　論理モデルと具体モデルの関係

3.3.2 CC-Case のライフサイクルプロセスの詳細

CC-Case の要求，設計，実装，テスト，保守段階までのライフサイクルの全段階を含んだライフサイクルプロセスを図 3-3-2 に示す.

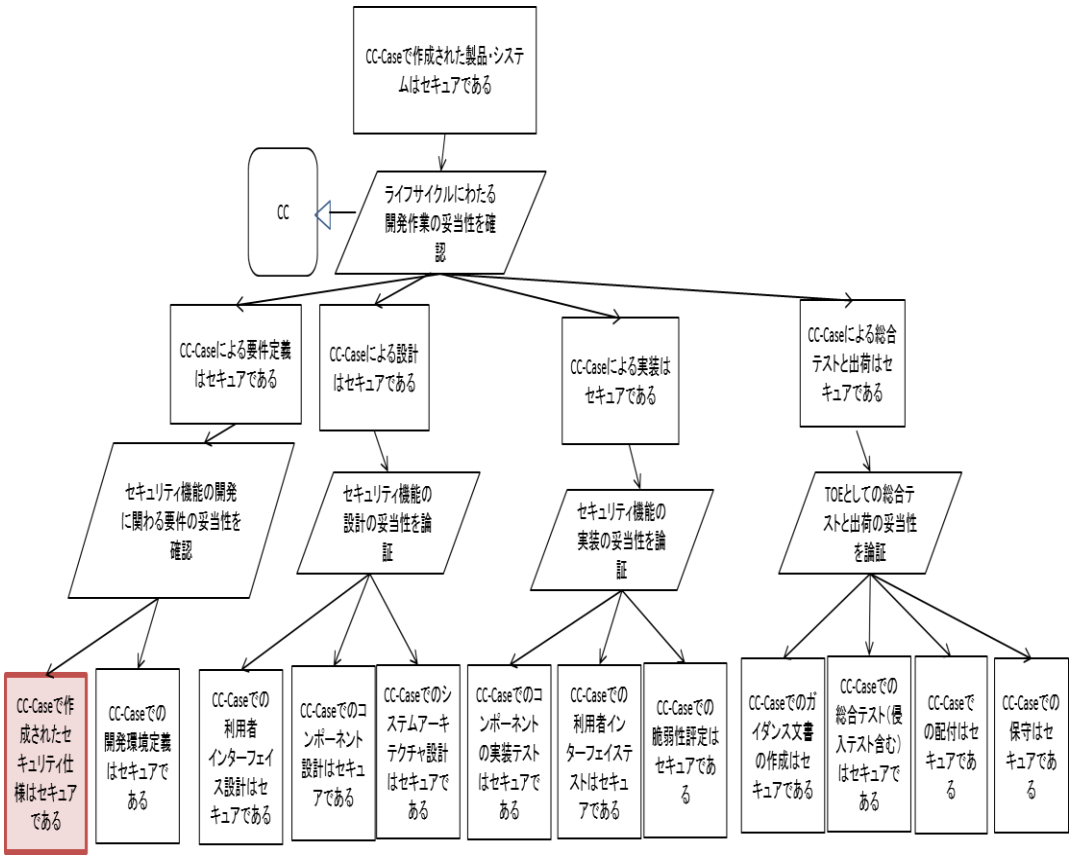


図 3-3-2　CC-Case のライフサイクルプロセス

CC-Case の最上位のゴールは「CC-Case で作成されたシステム・製品はセキュアである」である．これを最上位のゴールとするアシュアランスケースは「CC」をコンテキスト（前提）とし，「ライフサイクルにわたる開発作業の妥当性を確認」する戦略（説明）によって「CC-Case による要件定義はセキュアである」と「CC-Case による設計はセキュアである」と「CC-Case による実装はセキュアである」と「CC-Case による総合テストと出荷はセキュアである」の 4 段階のサブゴールに分かれる．

前提とサブゴールに分かれる戦略の明示により論理関係を明確にしたうえで，各サブゴールが成り立つことで，最上位のゴールが成り立つことが保証される．

「CC-Case による要件定義はセキュアである」のという第 2 階層のゴールは「セキュリティ機能の開発に関わる要件の妥当性を確認」する戦略（説明）を介して「CC-Case で作成されたセキュリティ仕様はセキュアである」と「CC-Case での開発環境定義はセキュアである」の 2 つの第 3 階層のゴールに分かれる．このうち「CC-Case で作成されたセキュリティ仕様はセキュアである」が要求段階の CC-Case で示すセキュリティ仕様のアシュアランスケースのトップゴールに相当する．つまりこのセキュリティ仕様のアシュアランスケースのトップゴールのもとに論理モデルと具体モデルのアシュアランスケースが展開されるのである．セ

キュリティ仕様のアシュアランスケースについては 4.3 節に詳細を後述する.

4　要求段階の CC-Case

4.1　要求段階の CC-Case の概要

4.1.1 要求段階の CC-Case の全体像

要求段階ではセキュアな仕様を作成するために，セキュリティコンセプト定義，対策立案，要約仕様の手順を定め ST に必要な成果物を作成する．この手順をアシュアランスケースとして定義し，証跡を残す．こうして作成したセキュリティ仕様アシュアランスケースは，CC 準拠と顧客と合意による保証の根拠となる．この一連の作業を行う手法が CC-Case である．

図 4-1-1 に CC-Case のセキュリティ仕様作成の手順と用いる入力並びに生成される証跡の関係を示す．セキュリティ仕様のアシュアランスケースは，システム構築時の入力（前提），手順，証跡を含んだ手法である．すなわち，作業は図の前提条件を入力とし，手順に従って進められるが，それとともに生成される証跡によってアシュアランスケースが必要とする情報が出来上がっていく．CC 準拠の保証とは，ST を作成するためのもととなる内容をアシュアランスケースの根拠として残すことである．

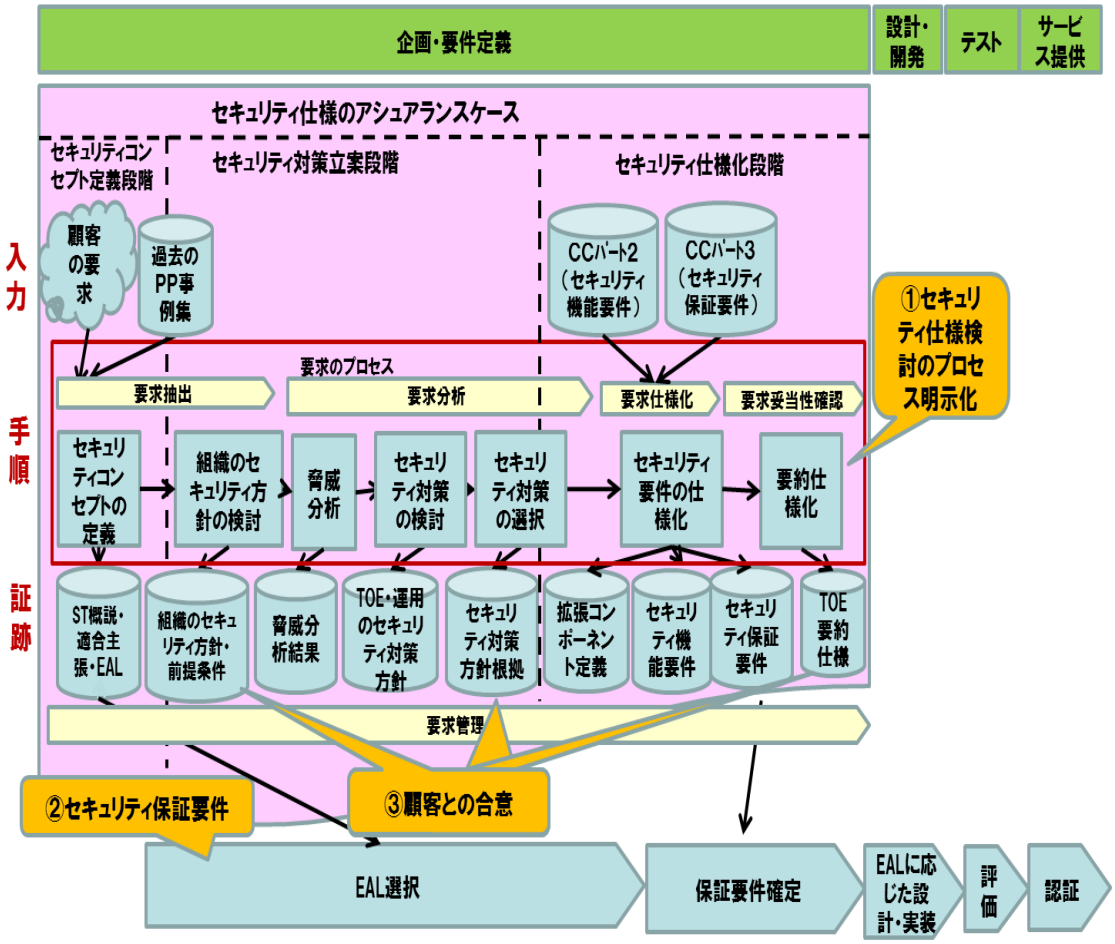


図 4-1-1　要求段階の CC-Case の全体像

図 4-1-1 は CC-Case 要求分析の手順やライフサイクルでの位置づけ，保証の意義を示した全体像である．

4.1.2 ST の構成とセキュリティ要求分析

セキュリティ要求分析として ST に必要な成果物を作成する理由は ST における作業プロセスとセキュリティ要件の解析方法は非常に類似しているからである．ST における作業プロセスは概ね以下の手順で実施される．資産ベースのセキュリティ要件の分析獲得の実施，攻撃者がいかに資産に対して脅威を与えるかについて脅威分析の実施，如何に資産を防御するかについてセキュリティ方針を規定，セキュリティ要件の獲得・分析し，セキュリティ機能として整理する．図 4-1-2 に示すように，セキュリティ要求分析として 2.適合性主張と 6.2 セキュリティ保証要件以外は ST で作成可能である．従来の手法においても，攻撃タスクはミスユースケースに，システムのセキュリティゴールはセキュリティユースケースに，セキュリティ課題定義との関係とセキュリティ対策方針との関係はゴールモデルに対応している．ただし ST 全体をに整合性を保ち，網羅的に分析する手法はない．

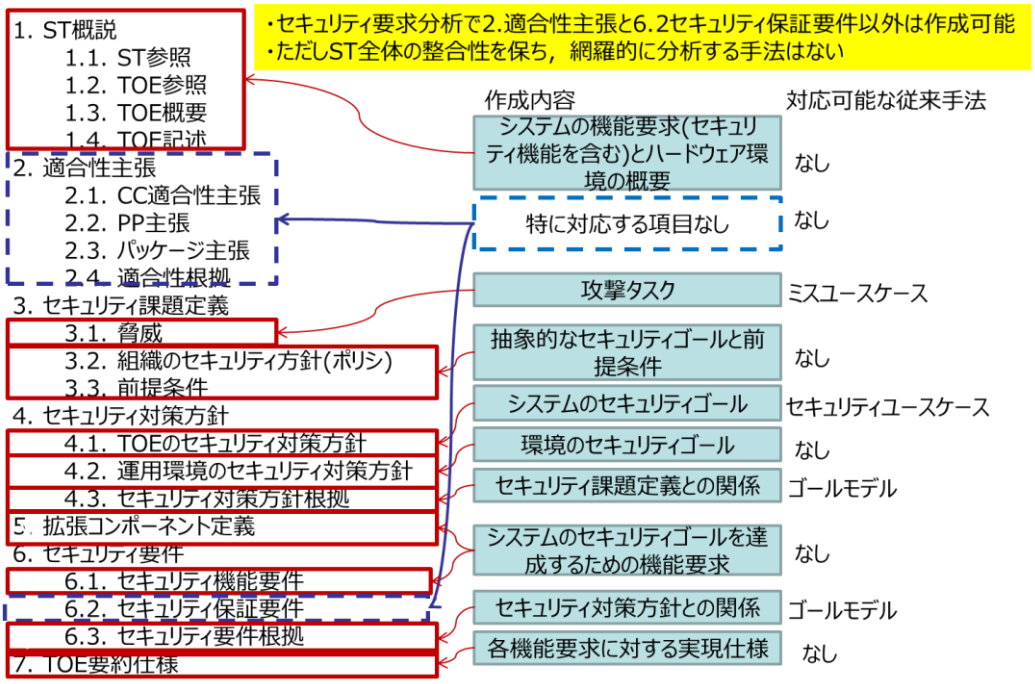


図 4-1-2　ST の構成と対応可能な従来手法

尚，ST における作業プロセスは，現状では開発後に ST は作成されており，開発スタッフと ST 作成のスタッフは別であることが多い．要求分析・獲得フェーズにおいて ST の作成を可能にすることが望まれる．

4.1.3 ST の構成と CC-Case

図 4-1-3 に示すように要求段階の CC-Case であるセキュリティ仕様のアシュアランスケースは，ST 全体に整合性を保ち網羅的に作成することを意図している．

セキュリティ対策立案段階は，システムの機能要求(セキュリティ機能を含む)とハードウェア環境の概要をする「1. ST 概説」と CC バージョン,拡張コンポーネント,PP,パッケージの適合性を主張する「2. 適合性主張」のプロセスを含んでいる．セキュリティ課題定義として，攻撃タスクと抽象的なセキュリティゴールと前提条件を洗い出す「3. セキュリティ課題定義」とこれをもとにシステムのセキュリ

ティゴール，環境のセキュリティゴール，セキュリティ課題定義との関係を示す「4. セキュリティ対策方針」のプロセスを含んでいる．SARM とはアクタ関係表に基づくセキュリティ要求分析手法であり，攻撃タスクを抽出し，「3.1. 脅威」に相当し，セキュリティ対策立案段階のプロセスの 1 つである．尚，SARM の詳細は 5 章，CC-Case と SARM の関係については 4.2.1 項を参照してほしい．

セキュリティ要約仕様化段階は，システムのセキュリティゴールを達成するための機能要求と TOE が ST を満たしているかどうかの評価方法とセキュリティ対策方針との関係を示す「5.拡張コンポーネント定義」と「6. セキュリティ要件」と,各機能要求に対する実現仕様である「7. TOE 要約仕様」のプロセスを含んでいる．

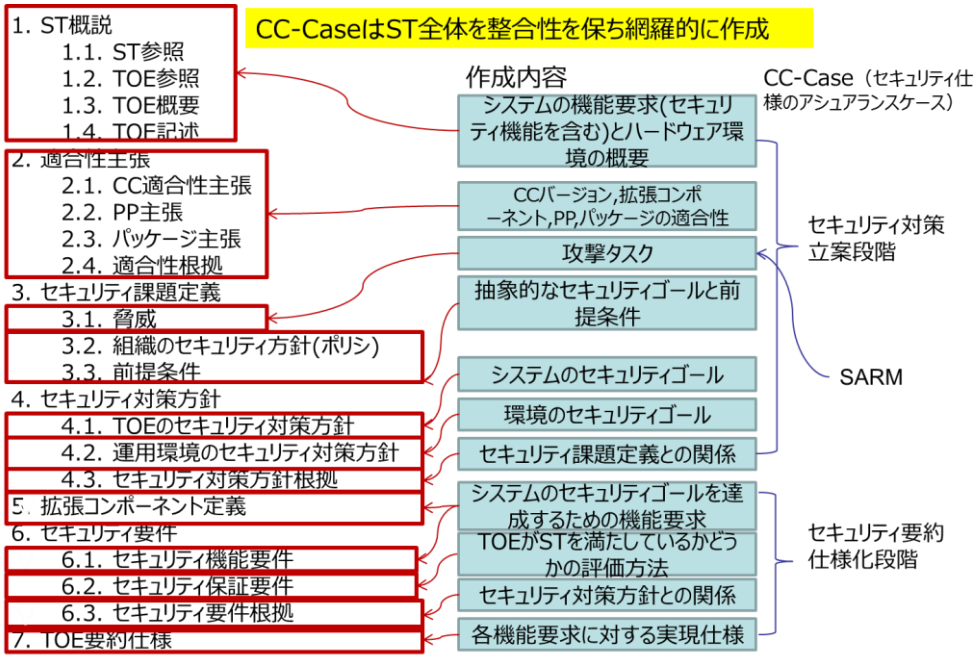


図 4-1-3　ST の構成と CC-Case（セキュリティ仕様のアシュアランスケース）

4.1.4 検証・妥当性確認のプロセス

表 4-1-4 に「セキュリティ仕様のアシュアランスケース」として作成された論理モデルの規模を示す． 3 段階の工程に対して，分類は 4，保証条件数は 23 である．どの段階のゴールも検証と妥当性確認を実施している．尚，具体モデルは実際のケースに応じて記述要素数が違うため，この表には記載していない．このように CC 準拠のセキュリティ要求分析とアシュアランスケースによる検証・妥当性確認のプロセスの双方を実施することにより，CC-Case はセキュリティ要求分析手法かつ保証手法といえる．また CC-Case は PP やセキュリティ機能要件のカタログを利用でき，初めから全てを検討するよりも効率的である．CC-Case が従来の CC の手順と比べて増えているのは顧客の承認による妥当性確認である．表 4-1-4 の対応するプロセスで妥当性確認は合計 5 つであるが，これはコミュニケーションギャップによる手戻りを起こさないために必要なプロセスである．

表 4-1-4　論理モデルの規模

工程	分類（最下層戦略数）	対応するプロセス	保証条件数（最下層ゴール数）
セキュリティコンセプト定義段階	1	要求抽出と検証 妥当性確認	3 1
セキュリティ対策立案段階	3	要求分析と検証 妥当性確認	12 3
セキュリティ要約仕様化段階	1	要求仕様化と検証 妥当性確認	3 1
合計	4		23

4.1.5 SARM と CC-Case のプロセス定義の関係

CC はセキュリティ目標（ST）を作成するための元となる要求分析や脅威分析の手法を定めていない．そこで SARM の利用の仕方を工夫し，CC に対応した脅威分析手法としての CC-Case への適切な対応を図る．

SARM と CC-Case のプロセス定義の特徴を考察してみる．表 4-1-5 に示すように SARM はセキュリティ要求獲得のためのゴール指向要求分析手法であり，セキュリティ要求分析の要となる脅威分析を実施する．CC-Case のプロセス定義は CC に基づくセキュリティ要求分析プロセスを明示したシステム要求を保証するためのアシュアランスケースを要素技術として用いており，要求抽出，要求分析，要求仕様化，要求妥当性確認，要求管理からなる要求のプロセスの全段階を手順化している．しかしながら特定の脅威分析手法はもたない.そこで SARM を CC-Case の脅威分析手法とすることで両者は補完関係をもつといえる．

CC-Case の対策立案段階のアシュアランスケース（詳細は後述）で SARM の適用範囲を考えてみたのが図 4-1-5 である．SARM は図 4-1-5 の最下位ゴールにある「脅威分析はセキュアである」を強化する分析手法に相当する．

表 4-1-5　SARM と CC-Case のプロセス定義

項目	SARM	CC-Caseのプロセス定義
手法	ゴール指向要求分析	アシュアランスケース
用途	システム要求の獲得	システム要求の保証
適用事項	①保護資産と脅威の獲得 ②攻撃者のアクタ別の意図に基づく脅威の洗い出し	①セキュリティコンセプトの検討 ②セキュリティ機能要件の獲得 ③セキュリティ保証要件の獲得 ④STの妥当性確認
特長	・一般の機能分析に付加してセキュリティ脅威分析ができる ・図形式と表形式のスパイラルレビューにより，網羅性を向上	・論理的証拠の提示 ・セキュリティゴールに対する検証 ・顧客との合意プロセスの明示
補完効果	CC-Caseに最適な脅威分析ができる	SARMの脅威分析結果をもとにセキュリティ仕様を作成できる

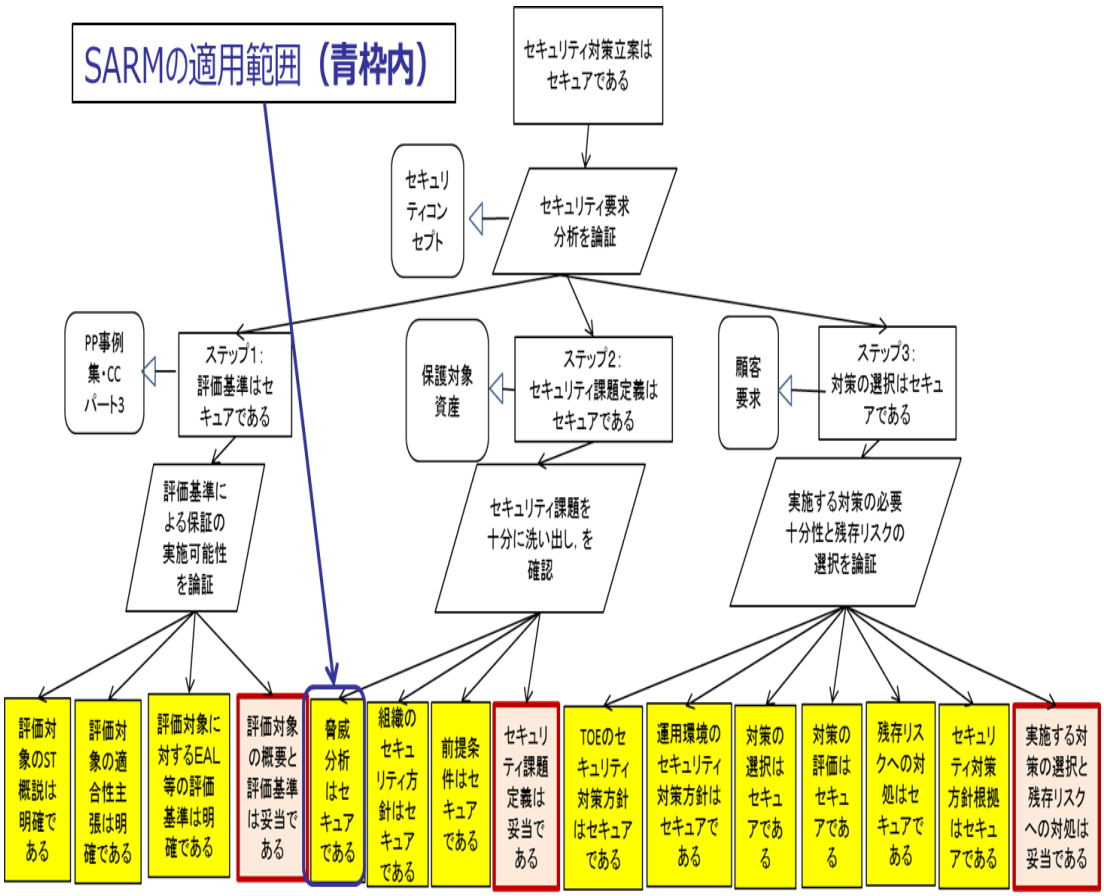


図 4-1-5　SARM の適用範囲

アクタ関係表に基づくセキュリティ要求分析手法（SARM）は本来攻撃と通常のシステム機能との間のセキュリティ上の関係を分析するための要求分析手法である．しかし SARM は利用法の工夫により CC に対応した脅威分析が可能である．脅威分析はセキュリティ要求分析の 1 つのプロセスだが，最重要となる分析である．SARM は利便性の高い表形式で，攻撃シーンごとに攻撃者を含むアクタ間の依存関係を網羅性高く分析できるメリットをもつ（詳細は 5.2 節参照）．そこで CC-Case は脅威分析に SARM を利用することによって網羅的により効果的に脅威分析ができる手法となる．

CC-Case は CC に対応したアクタ関係表に基づく脅威分析（SARM）を含んだセキュリティ要求分析を実施するとともに CC 準拠の保証もできる．つまり網羅的に脅威を分析し，脅威に対して保証できる範囲を明確にし，CC に基づくセキュリティ仕様を顧客と合意の上で決定できる手法となる．CC に対応した脅威分析手法としての SARM は CC-Case の構成要素の一つである．SARM の CC 対応の詳細は 5 章に論述する．

4.2　セキュリティ仕様のアシュアランスケース

図 4-2-1 に示すように要求段階の CC-Case の最上位のゴールは「CC-Case で作成されたセキュリティ仕様はセキュアである」である．これを最上位のゴールとするアシュアランスケースは「CC」をコンテキスト（前提）とし，「ST の元となるセキュリティ仕様の妥当性を論証」する戦略（説明）によって，「セキュリティ

コンセプト定義はセキュアである」と「セキュリティ対策立案はセキュアである」と「セキュリティ要約仕様はセキュアである」の 3 段階のサブゴールに分かれる．前提とサブゴールに分かれる戦略の明示により論理関係を明確にしたうえで，各サブゴールが成り立つことで，最上位のゴールが成り立つことが保証される．

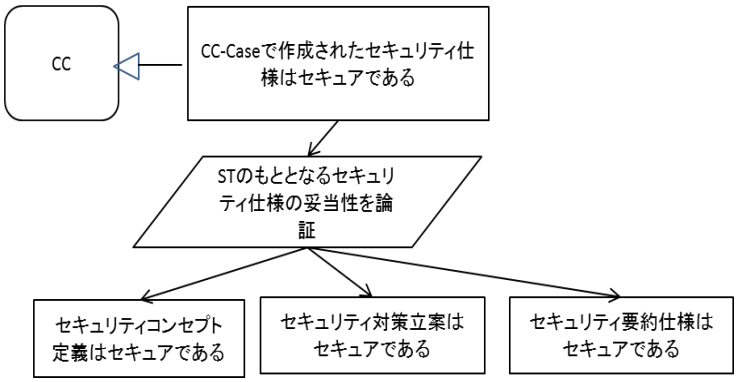


図 4-2-1　セキュリティ仕様のアシュアランスケース

図 4-2-1 はトップのアシュアランスケースであり，そのサブゴールを更に展開していくことにより具体的な作業が決まっていく．すなわち図 4-2-1 の一番左のサブゴールを展開したのが図 4-2-1-1，2 番目のサブゴールを展開したのが図 4-2-2，3 番目のサブゴールを展開したのが図 4-2-3 である．これらの定まった作業の手順が論理モデルであり，図 4-1-1 の手順を詳細化している．論理モデルの各最下位ゴールの下に実際ケースにおいて，ST の内容の証跡とそれに至るまでの論理関係を示すのが具体モデルである．図 4-1 の証跡は具体モデルの ST の内容の証跡に相当する．具体モデルの適用事例は 6 章のケーススタディに詳述する．これらの手順の生成はアシュアランスケースの考え方で展開されている，従ってそれを守ることによりセキュアな仕様が出来上がることを主張することができる．論理モデルを展開した上位ゴールは下位階層にあるものすべてが満たされることが必要であると同時にそれだけで十分であるという展開になっている．これが従来手法の単なるプロセスの流れ図への展開と異なるユニークなポイントであり，手法の完全性を示す．

図 4-2-2 は一般のシステム開発プロセス・セキュリティ対応プロセス（上部）と CC-Case の要求段階のセキュリティ仕様のアシュアランスケースとの関係（下部）を示している．一般の開発プロセスの商品・サービス企画とともにセキュリティプロセスとして実施するのがセキュリティコンセプト検討である．このセキュリティコンセプト検討を実施するのが図 4-2-1 のサブゴールである「セキュリティコンセプト定義はセキュアである」をトップゴールとするセキュリティコンセプト段階である．

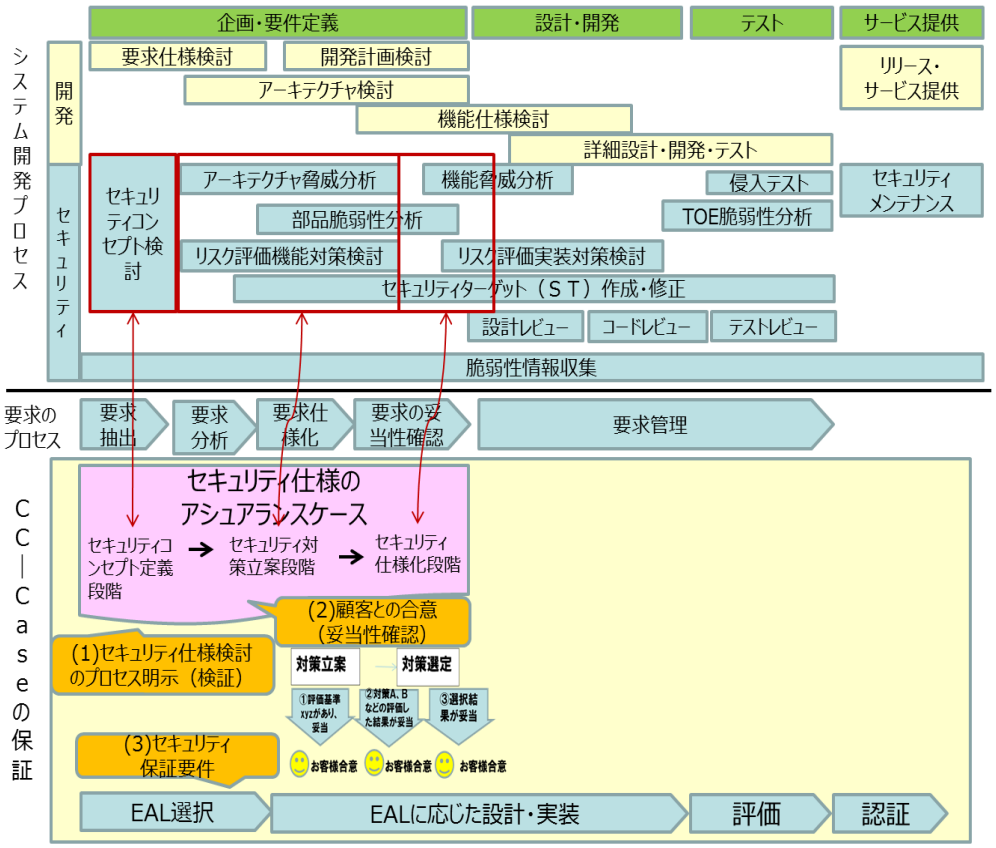


図 4-2-2 システム開発プロセス・セキュリティプロセスと CC-Case（要求段階）の対応

図 4-2-1 のサブゴールである「セキュリティ対策立案はセキュアである」をトップゴールとするセキュリティ対策立案段階は開発プロセスのアーキテクチャ検討とともにセキュリティプロセスとしてアーキテクチャ脅威分析やリスク評価機能対策検討の上のセキュリティターゲット作成に相当する．

図 4-2-1 のサブゴールである「セキュリティ要約仕様はセキュアである」をトップゴールとするセキュリティ要約仕様化段階は一般の開発プロセスの機能仕様検討とともに機能脅威分析を実施し，セキュリティ要件を仕様化するプロセスに相当する．以下，図 4-2-1 の 3 つのサブゴールを更に詳しく展開する．

4.2.1 セキュリティコンセプト定義段階

この段階のアシュアランスケースを図 4-2-1-1 に示す．セキュリティコンセプトは顧客と開発者で何度も繰り返し検討して決めていくものである．本段階ではシステム・製品に求められるセキュリティに関する要求を整理，分析の対象とする範囲と境界を設定，主たる保護資産，想定脅威，対策案，想定アーキテクチャなどを整理する．ST 作成はしない．図 4-2-1-1 の黄色のサブゴールでセキュリティ要求抽出の十分性，検討項目の明確化をする．その上で肌色（太い枠線）のサブゴールで顧客とセキュリティコンセプト定義に対する合意をとることによる妥当性確認をする．このように CC-Case では合意による保証を妥当性確認としている．

表 4-2-1 にセキュリティコンセプト定義段階の最下位ゴールのプロセス定義を示す．最下位ゴールは具体的モデルを記述する際のトップゴールとなるため，具体モデルを記述しやすいように各ゴールの目的，プレーヤー，出力に対する確認方

法を示している．入力・手続き・出力として最下位ゴールの各プロセスを規定する．尚，各手続きには ST における定義をもとにした内容を記載していることが多い．実施すべき手続きがより理解しやすいように将来的な改善が必要である．

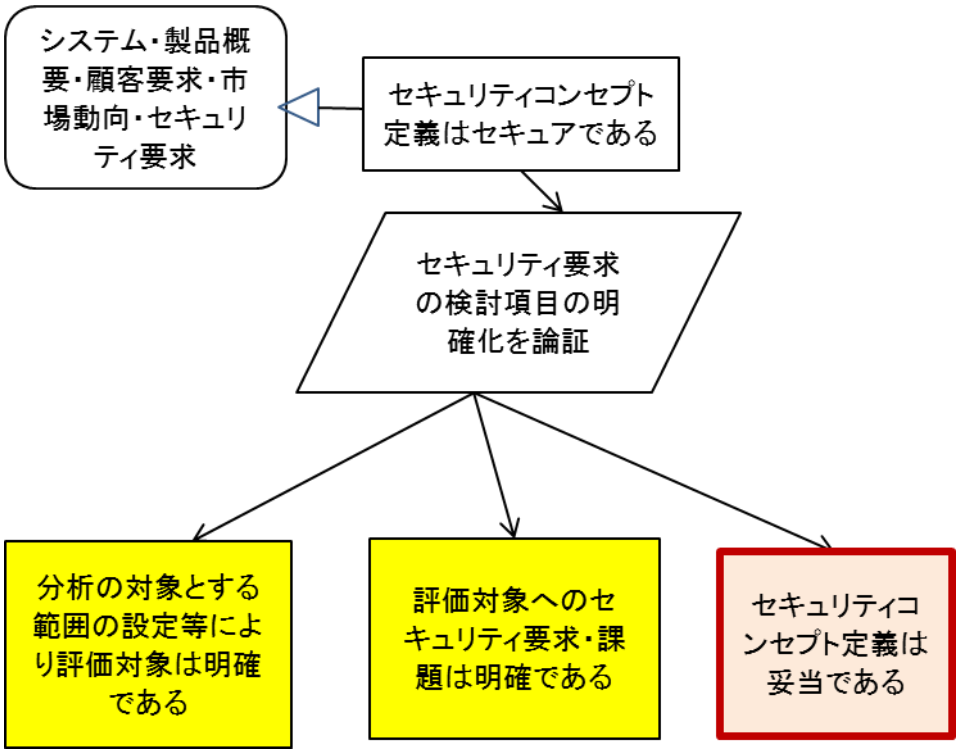


図 4-2-1-1 セキュリティコンセプトの定義段階

表 4-2-1　セキュリティコンセプト定義段階のプロセス定義

段階	No.	ゴール	目的	プレーヤー	出力に対する確認方法
セキュリティコンセプト定義段階	1	分析の対象とする範囲の設定等により評価対象は明確である	評価対象が何かを明確化する	開発者	検証
	2	評価対象へのセキュリティ要求・課題は明確である	評価対象に対してどのような要求・課題があるのかを明確化する	開発者	検証
	3	セキュリティコンセプト定義は妥当である	セキュリティコンセプト定義に対する顧客の承認を得る	顧客	妥当性確認

1)　分析の対象とする範囲の設定等により評価対象は明確である
入力：システム・製品概要

手続き：開発者は分析の対象とする評価対象の利用イメージ・論理的範囲（基本機能・セキュリティ機能）や物理的範囲（構成ツール・アプリケーションソフトウェア）を設定する．評価対象の境界の設定をする．
＊境界の設定に関しては，各種ハードウェアとソフトウェアの一部分や組合せなど一般に理解されているような IT 製品の境界に関連付かない場合もあるので注意が必要である．

出力：評価対象（TOE）・TOE の範囲・セキュリティ機能・構成ツール・アプリケーションソフトウェア等を含むセキュリティコンセプト

2)　評価対象へのセキュリティ要求・課題は明確である
入力：市場動向・セキュリティ要求等

手続き：開発者は市場動向・セキュリティ要求や脅威エージェントから護るべき資産（主に情報資産）等の整理をする．
＊脅威エージェントの例には，ハッカー，悪意のある利用者，(誤りを犯すことがある)悪意のない利用者，コンピュータ処理，及び事故などがある．

出力：保護資産の洗い出し結果・市場動向・セキュリティ要求等を含むセキュリティコンセプト

3)　セキュリティコンセプト定義は妥当である
入力：ユーザニーズ・セキュリティコンセプト

手続き：顧客はコスト等のユーザニーズを踏まえてセキュリティコンセプト定義を決定する．

出力：セキュリティコンセプトに対する顧客の承認結果

4.2.2 セキュリティ対策立案段階

この段階(図 4-2-2)は，セキュリティコンセプトをもとに評価基準を定め，脅威分析を行い，対策の立案と評価，対策の選択をする．そしてそれぞれがセキュアであることを検証する．以上のようにセキュリティ要求間の対応関係や論理関係の分析と根拠を顧客に提示し合意を得て決定していく．これを整理して，以下の 3 ステップとした．

ステップ 1 : セキュリティコンセプトをもとに評価対象の概説や適合性主張を定め，次にどこまでのレベルで保証するのかを EAL として定め，評価基準が妥当であるかを確認し，顧客の承認を得る．適合性主張の対象である PP は公開されており，評価対象の種別に対して適用すべきセキュリティ仕様として適切な PP があれば，それを利用することができる．

ステップ 2 : 保護対象とする資産に関する脅威モデルを定義し，それに基づいて脅威を分析する．更に組織のセキュリティ方針や前提条件を明確化して，セキュリティ課題定義を明確化する．

ステップ 3 : ステップ 2 で抽出したセキュリティ課題定義に対して対策立案をする．技術的な TOE のセキュリティ対策方針と運用環境における対策方針を抽出する．脅威と対策の関係の評価が妥当であることを論証する．セキュリティ対策方針根拠に対する顧客の承認を得る.実施する対策を選択し，対策を実施しないリスクは残存リスクとして管理していく．次にこれらの選択が妥当であることを論証し，セキュリティ対策の選択結果に対する顧客の承認を得る．

この対策立案の 3 ステップは「①評価基準が妥当である，②課題定義が妥当である．③対策の立案・選択が妥当である．」のシステマテックな手順をきちんと

踏んでセキュリティ対策を顧客と合意し，証跡を残すことを規定していることになる．尚，アシュアランスケースを作成する上での議論分解パターンとしてはBloomfield が示した 7 つの分解パターン[6]とその応用パターン[31]があるが，上記セキュリティ対策立案段階には，応用パターンの 1 つである代替案比較パターンを参考モデルにした．

この段階では単に ST 項目の作成プロセスを並べるのではなく，オリジナルプロセスにしている．オリジナルな点は①対策への評価の妥当性確保のためのアシュアランスケースの類型パターンの応用，②顧客合意リスクへの対応など，妥当性確認プロセスを 3 ステップ共に設定，③CC 準拠の保証の確保のための ST の必要項目の列挙，④実施対策の選択プロセスの設定，⑤残存リスクへの対応プロセスの設定の 5 つである．このオリジナルプロセスを設定した理由は脅威分析結果をもとに適切な対策立案を実施するため，ST としての結果に表現される前の現実的な検討必要事項を含めたプロセスにするためである．

表 4-2-2 にセキュリティ対策立案段階の最下位ゴールのプロセス定義を示す．

最下位ゴールは具体的モデルを記述する際のトップゴールとなるため，具体モデルを記述しやすいように各ゴールの目的，プレーヤー，出力に対する確認方法を示している．入力・手続き・出力として最下位ゴールの各プロセスを規定する．

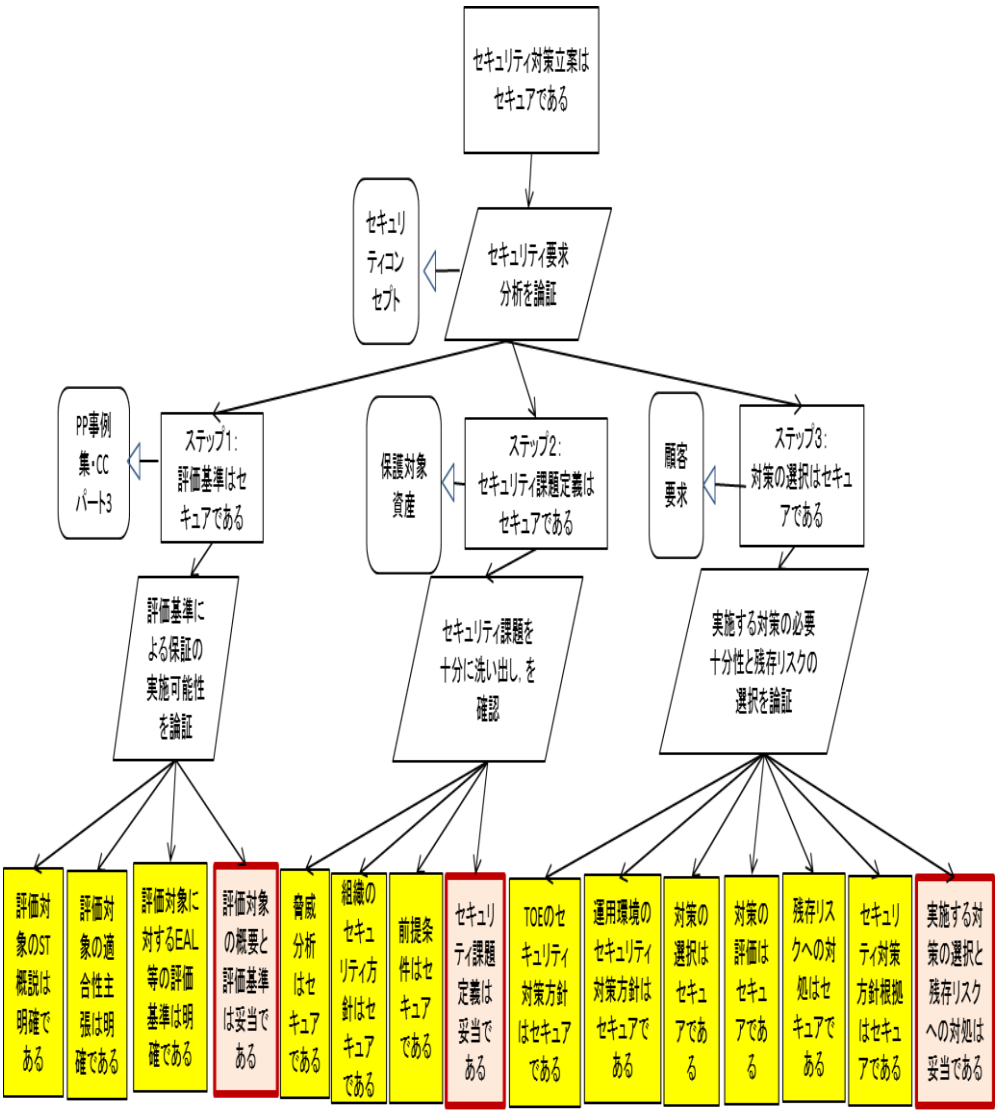


図 4-2-2　セキュリティ対策立案段階

表 4-2-2　セキュリティ対策立案段階の最下位ゴール・プロセス定義

段階		ゴール	目的	プレーヤー	出力に対する確認方法
セキュリティ対策立案段階	1	評価対象のST概説は明確である	評価対象の正確なセキュリティ特性をST概説として規定する.	開発者	検証
	2	評価対象の適合性主張は明確である	評価対象の適合性主張を規定する	開発者	検証
	3	評価対象に対するEAL等の評価基準は明確である	評価基準を明確化する	開発者	検証
	4	評価対象の概要と評価基準は妥当である	評価対象の概要と評価基準への妥当性に対する顧客の承認を得る	顧客	妥当性確認
	5	脅威分析はセキュアである	TOE が対処しようとする特性やセキュリティの範囲を、形式的な作法で定義する(セキュリティ課題定義)ため、評価対象において想定される十分な脅威を引き出し、分析する.	開発者	検証
	6	組織のセキュリティ方針(OSP)はセキュアである	TOE が対処しようとする特性やセキュリティの範囲を、形式的な作法で定義(セキュリティ課題定義)するため、組織のセキュリティ方針(OSP:組織に対するセキュリティ規則、手続き、またはガイドラインのセット)を規定する	開発者	検証
	7	前提条件はセキュアである	TOE が対処しようとする特性やセキュリティの範囲を、形式的な作法で定義(セキュリティ課題定義)するため、前提条件を明確化する	開発者	検証
	8	セキュリティ課題定義(脅威・組織のセキュリティ方針・前提条件)は妥当である	実施するセキュリティ対策をユーザニーズを踏まえて決定する	顧客	妥当性確認
	9	TOEのセキュリティ対策方針はセキュアである	セキュリティ課題定義を技術的に解決するセキュリティ機能性を提供するためにTOEのセキュリティ対策方針を規定する	開発者	検証
	10	運用環境のセキュリティ対策方針はセキュアである	TOEのセキュリティ対策方針によって定義されるセキュリティ機能性を正しく提供するために運用環境のセキュリティ対策方針を規定する.	開発者	検証
	11	対策の評価はセキュアである	セキュリティ対策を評価し、実施する対策を選択する根拠とする	開発者	検証
	12	実施する対策の選択はセキュアである	想定する対策一覧の中から実施する対策または対策の組合せを選択する	開発者	検証
	13	残存リスクへの対処はセキュアである	対処しないことになった対策から生じる残存リスクを認識して、リスク顕在化に備える	開発者	検証
	14	セキュリティ対策方針根拠はセキュアである	セキュリティ対策選択結果に対して、どのセキュリティ対策方針が、どの脅威、組織のセキュリティ方針、及び前提条件に対処するかを示す追跡と効果的に対処されることを示す	開発者	検証
	15	セキュリティ対策方針根拠と残存リスクへの対処は妥当である	実施するセキュリティ対策に対する顧客の承認を得る	顧客	妥当性確認

1)　評価対象の ST 概説は明確である
入力：セキュリティコンセプト

手続き：開発者は評価対象の概要（ST 概説）を規定する.
以下の 3 つの異なる記述レベルで記載する.
・ST 及び ST が参照する TOE の識別資料を提供（ST 参照及び TOE 参照）
・TOE について簡潔に記述（TOE 概要）

・TOE についてより詳細に記述（TOE 記述）

出力：評価対象の概要
・ST の識別情報
・TOE の識別情報
・TOE 種別及び主要セキュリティ機能
・運用環境
・ハードウェア構成
・ソフトウェア構成
・TOE 利用者役割
・TOE 論理的範囲
・TOE 物理的範囲

2) 評価対象の適合性主張は明確である
入力：CC-PART1・PP 事例集

手続き：開発者は ST が コモンクライテリア自体やプロテクションプロファイル(存在する場合)とどのように適合するかを記述する.

出力：CC 適合主張・PP 主張・パッケージ主張

3) 評価対象に対する EAL 等の評価基準は明確である
入力：CC-PART3

手続き:開発者は評価対象に対する EAL(評価保証レベル)等の評価基準を規定する.
＊保証パッケージ(存在する場合)を用いる場合はそのレベルの指定をする.

出力：EAL 等の評価基準

4) 評価対象の概要と評価基準は妥当である
入力：ユーザニーズ・評価対象の概要・評価基準

手続き：顧客はユーザニーズを踏まえて評価対象の概要と評価基準を決定する.

出力：評価対象の概要と評価基準の確認結果

5) 脅威分析はセキュアである
入力：保護資産・セキュリティ機能

手続き：脅威は資産に対する脅威エージェントの有害なアクションから構成されるため，開発者は保護資産・セキュリティ機能を元に SARM の AA 表・SARM 状況表で脅威分析を実施する．想定される脅威を洗い出す.

出力：AA 表・SARM 状況表による脅威分析結果

6) 組織のセキュリティ方針（OSP）はセキュアである
入力：ユーザニーズ・セキュリティの規則・手続き・ガイドライン

手続き：開発者は運用環境のセキュリティの規則，手続き，またはガイドラインを明確化する．
＊OSP は TOE の運用環境を管理する組織によって規定される場合もあれば，立法機関もしくは規制機関によって規定される場合もある．

出力：組織のセキュリティ方針（OSP）

7) 前提条件はセキュアである
入力：TOE 運用環境・ハードウェア構成・ソフトウェア構成

手続き：開発者はセキュリティ機能性を提供できるようにするためにその運用環境に対して設定する前提条件を規定する．
＊前提条件には運用環境の物理的条件，人的条件及び接続に関する条件などがある．
＊TOE がこれらの前提条件を満たさない運用環境に配置される場合，その TOE はそのセキュリティ機能性のすべては提供することができなくなる可能性がある．

出力：前提条件

8) セキュリティ課題定義は妥当である
入力：セキュリティ課題定義

手続き：顧客はユーザニーズを踏まえてセキュリティ課題定義（脅威分析結果，組織のセキュリティ方針，前提条件）が妥当であるかを確認する．

出力：セキュリティ課題定義への承認結果

9) TOE のセキュリティ対策方針はセキュアである
入力：セキュリティ課題定義

手続き：開発者は想定される対策を洗い出し，TOE の技術的なセキュリティ対策方針を自然言語で規定する．
＊TOE のセキュリティ対策方針は作成する．課題の特定の部分
を解決するために TOE 自体が達成すべき目標で構成される．

出力：TOE のセキュリティ対策方針

10) 運用環境のセキュリティ対策方針はセキュアである
入力：セキュリティ課題定義

手続き：開発者は想定される対策を洗い出し，TOE を支援する技術及び手続きに関する手段を自然言語で規定し，実装する．
＊運用環境のセキュリティ対策方針は部分的解決策であり，運用環境で達

成すべき目標で構成される.

出力：運用環境のセキュリティ対策方針

11) 対策の評価はセキュアである
入力：TOE のセキュリティ対策方針・運用環境のセキュリティ対策方針

手続き：開発者は想定されるセキュリティ対策（TOE のセキュリティ対策方針と運用環境のセキュリティ対策方針）を全て洗い出し，対策または対策の組合せについて，実現性，コスト，難易度，緊急度などの観点で評価し，セキュリティ対策を評価し，実施する対策を選択する根拠とする.

出力：想定されるセキュリティ対策一覧と評価結果

12) 実施する対策の選択はセキュアである
入力：想定されるセキュリティ対策一覧と評価結果

手続き：開発者は想定する対策一覧の中から実施する対策または対策の組合せを選択する.

出力：実施するセキュリティ対策

13) 残存リスクへの対処はセキュアである
入力：セキュリティ課題定義・想定されるセキュリティ対策一覧・
セキュリティ対策選択案

手続き：開発者は想定されるセキュリティ対策一覧とセキュリティ対策選択案より実施しない対策と残存リスクを明確し，残存リスクへの対処方針を定める.

出力：残存リスクへの対処方針

14) セキュリティ対策方針根拠はセキュアである
入力：実施するセキュリティ対策・セキュリティ課題定義

手続き：開発者は TOE と運用環境のセキュリティ対策方針でセキュリティ課題定義にどのように対処するかを示すセキュリティ対策方針根拠を規定する.
セキュリティ対策方針根拠の要件を以下に示す.
・各セキュリティ対策方針は少なくとも 1 つの脅威，OSP，前提条件までたどれる.
・前提条件は常に運用環境に対して設定されるため，TOE のセキュリティ対策方針は前提条件までさかのぼらない.
・複数のセキュリティ対策方針が同一のセキュリティ課題定義への対策となりうる.
・セキュリティ対策方針及びセキュリティ対策方針根拠に基づいて，すべてのセキュリティ対策方針が達成された場合すべての脅威，OSP 及び前提

条件は対処される．

出力：セキュリティ対策方針根拠

15) セキュリティ対策方針根拠と残存リスクへの対処は妥当である
入力：ユーザニーズ・セキュリティ対策方針根拠・残存リスクへの対処方針

手続き：顧客はユーザニーズを踏まえてセキュリティ対策・残存リスクへの対処の妥当性確認をする．

出力：セキュリティ対策残存リスクへの対処方針への承認結果

4.2.3 セキュリティ要約仕様化段階

この段階（図 4-2-3）では，拡張コンポーネント定義，セキュリティ機能要件，セキュリティ保証要件，要約仕様がセキュアであることを検証し，顧客との合意を取る．セキュリティ機能要件はセキュリティ対策立案段階で選択した TOE のセキュリティ対策方針を，技術的な対策として実現するために，CC パート 2 からの機能要件の選択により作成する．セキュリティ保証要件は，CC パート 3 からの保証要件の参照等により作成する．CC パート 2・3 だけでは機能要件や保証要件を明確にできない場合に，拡張コンポーネント定義し，拡張した機能要件や保証要件として利用する．要約仕様はセキュリティ機能要件を実システム上で実装する方法を示す．このセキュリティ要約仕様に対して顧客の承認を得て妥当性確認をする．

表 4-2③にセキュリティ要約仕様化段階の最下位ゴールのプロセス定義を示す．最下位ゴールは具体的モデルを記述する際のトップゴールとなるため，具体モデルを記述しやすいように各ゴールの目的，プレーヤー，出力に対する確認方法を示している．入力・手続き・出力として最下位ゴールの各プロセスを規定する．

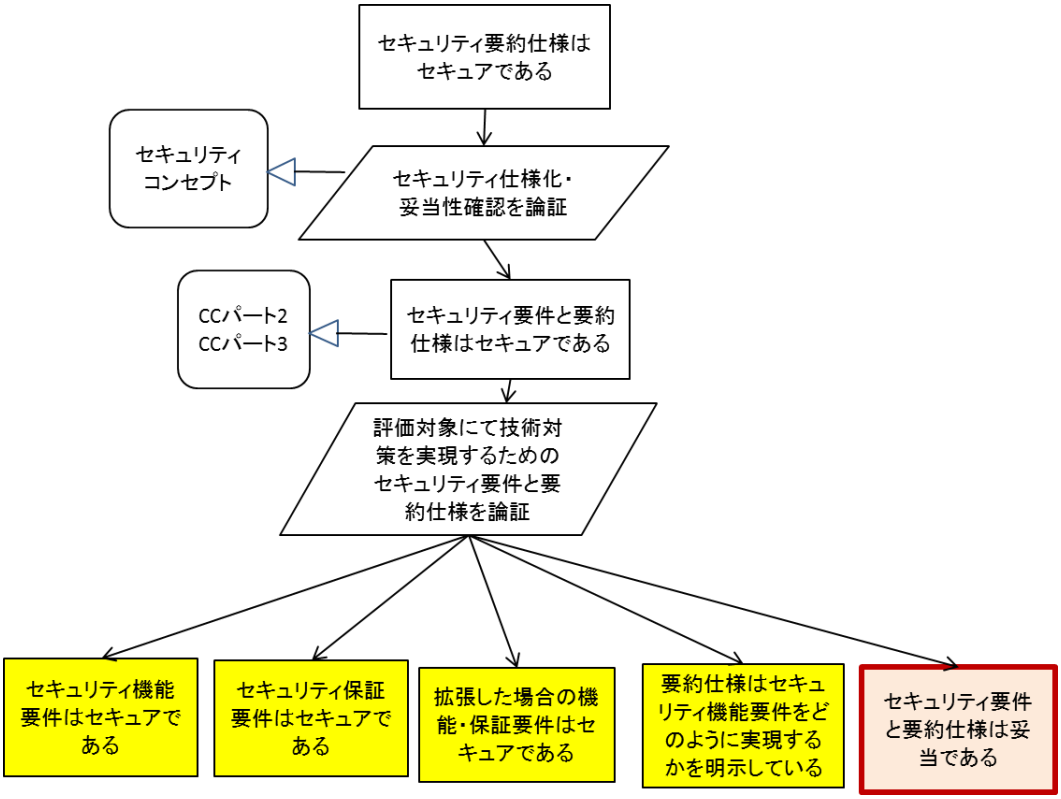


図 4-2-3　セキュリティ要約仕様化段階

表 4-2-3　セキュリティ要約仕様化段階の最下位ゴール・プロセス定義

段階		ゴール	目的	プレーヤー	出力に対する確認方法
セキュリティ要約仕様化段階	1	セキュリティ機能要件はセキュアである	TOEのセキュリティ対策方針をCC-PART2に規定されたセキュリティ機能要件(SFR)で書き換える	開発者	検証
	2	セキュリティ保証要件はセキュアである	TOEを評価する方法をCC-PART3のセキュリティ保証要件で記述する	開発者	検証
	3	拡張した場合の機能・保証要件はセキュアである	CCパート2またはCCパート3のコンポーネントに基づかないSTの要件が存在する場合は、CC のパート 2 に含まれていない機能要件、及び/または CC のパート 3 に含まれていない保証要件を、ST または PP に追加する.	開発者	検証
	4	要約仕様はセキュリティ機能要件をどのように実現するかを明示している	TOEがどのようにすべてのセキュリティ機能要件を満たすかについての記述を、TOEの潜在的な消費者に提供する	開発者	検証
	5	セキュリティ要件と要約仕様は妥当である	セキュリティ要件と要約仕様に対する顧客の承認を得る	顧客	妥当性確認

1)　セキュリティ機能要件はセキュアである
入力：セキュリティ対策選択結果・CC-PART2

手続き：開発者は CC は，次の 3 つの方法でセキュリティ機能要件の規定（書き換え）をサポートすることを検証する.

a) 評価する対象を正確に記述することを目的とし，事前に定義された正確な「言語」を提供する．この言語は，CC パート 2 で定義されるコンポーネントのセットとして定義する．TOE のセキュリティ対策方針から SFR への明

確に定義された書き換えとしてこの言語を使用することは必須であるが一部の例外が存在する.

b) TOE のセキュリティ対策方針をより正確な書き換えるために ST 作成者が SFR を改変することを許可するメカニズムとして操作を提供する.
＊割付，選択，繰返し，及び詳細化の 4 つの許可された操作がある.

c)SFR へのより完全な書き換えをサポートするメカニズムを提供する.
CC パート 2 の言語では，SFR は他の SFR に依存することがある.
これは，ST がその SFR を使用する場合，一般に他の SFR も使用する必要があることを意味する. これによって, ST の作成者が加える必要がある SFR を見過ごす可能性がはるかに少なくなるため，ST の完全性が向上する.

出力：セキュリティ機能要件

2)　セキュリティ保証要件はセキュアである
入力：CC-PART３

手続き：開発者は C パート 3 で定義されるコンポーネントのセットを用いたセキュリティ保証要件を規定を検証する.
標準言語は, いくつかの例外は存在するが, この言語の使用は必須である. CC は, 次の 2 つの方法でこの言語を拡張する:
a) 操作を提供する．ST 作成者が SAR を改変することを許可するメカニズムを提供する．CC には，割付，選択，繰返し，及び詳細化の 4 つの操作がある.
b)SAR へのより完全な書き換えをサポートするメカニズムを提供する.
CC パート 3 の言語では，SAR は他の SAR に依存することがある.
これは，ST がその SAR を使用する場合，一般に他の SAR も使用する必要があることを意味する. これによって, ST の作成者が加える必要がある SAR を見過ごす可能性がはるかに少なくなるため，ST の完全性が向上する.

出力：セキュリティ保証要件

3)　拡張した場合の機能・保証要件はセキュアである

入力：セキュリティ対策選択結果

手続き：開発者が拡張コンポーネントを定義する場合は常に，既存の CC コンポーネントと同様の方法，つまり明確で，曖昧さがなく，評価可能な方法で行わなければならない．評価可能とはそのコンポーネントに基づく要件が TOE に対応するかどうかを系統的に実証することができることである.
拡張コンポーネントは，既存の CC コンポーネントと同様のラベル付け，表現方法，及び詳細レベルを使用しなければならない．また，拡張コンポーネントの定義に拡張コンポーネントのすべての適用可能な依存性が含まれることも確認しなければならない.

出力：拡張機能・保証コンポーネント定義

4) 要約仕様はセキュリティ機能要件をどのように実現するかを明示している

入力：セキュリティ機能要件

手続き：開発者は要約仕様を一般的な技術的メカニズムとして示す．記述の詳細レベルは潜在的な消費者が TOE の一般的な形態及び実装を理解できる程度にする．

出力：要約仕様

5) セキュリティ要件と要約仕様は妥当である
入力：ユーザニーズ・セキュリティ機能要件・要約仕様

手続き：顧客はユーザニーズを踏まえて TOE セキュリティ機能とセキュリティ機能要件の対応関係・セキュリティ要件と要約仕様の妥当性確認をする．

出力：TOE セキュリティ機能とセキュリティ機能要件の対応関係の検証結果と要約仕様に対する顧客の承認結果

5　アクタ関係表による脅威分析と CC 対応

5.1　SARM のねらい

代表的なゴール指向要求工学手法である i*の SD 図に変換可能で，i*の表記の複雑さを解消した表記方法として，2.3 項に示したアクタ関係行列 ARM が提案されている．ARM は i*の課題を克服する手法であるが，セキュリティ対応にはなっていない. そこで ARM をセキュリティ要求分析に適用したアクタ関係表に基づくセキュリティ要求分析手法（SARM）を提案する[46]. SARM のねらいを以下に示す.

(1) ARM の網羅性の高いアクタ分析に，攻撃者の存在を追加して検討することにより，網羅性の高いセキュリティ要求分析を実施する.

(2)　攻撃シーンと守るべき資源（アセット）との組み合わせを検討することにより，セキュアなシステムを実現する．攻撃にはある程度既知のパターンがあるので STRIDE[47]等の分類を適用してある程度定形的な分析が可能になる.

(3)　セキュリティに関しての専門知識が必要とされるため，一般の要求分析工程，設計工程は一般のシステム開発者が担当し，脅威分析とセキュリティ機能分析はセキュリティ担当者が別途実施する方式が現実的である[48]．そこで，同じ表現形式を用いて通常機能と攻撃を分析できる手順とする.

5.2　対象者，メリット

SARM はシステム開発の上流工程において設計者が作成し，ユーザとの要求仕様の洗い出しに使用することを想定している.

SARM のメリットは，利便性の高い表形式で，攻撃シーンごとに攻撃者を含むアクタ間の依存関係を網羅性高く分析できることである．網羅性とはあらゆる脅威を考えることだが，SARM においては，表 5-3-1 に示す①AA 表によって抽出された攻撃パターン単位で攻撃者を加える場合の網羅性と，②攻撃者を加えた後，他のアクタとの関係で場合を尽くす網羅性の 2 段階に分けて，網羅性を向上させている．また，セキュリティと機能要件の両方の分析を 1 つの様式で行えるメリットも併せ持っている.

また ARM は i*の SD 図とは変換可能であるが，SR 図との対応は考慮していない．これに対して SARM はタスク分解，手段目的分解を表現可能であり，SD 図の範囲を超えて SR 図への対応ができる.

5.3　SARM の作成方法

SARM では，まず(1)資源に対して想定される攻撃方法を AA（Asset×Attack）表を用いて記述し，次いで(2) AA 表で特定した各攻撃方法に基づくアクタへの攻撃状況をアクタ間の関係として SARM 状況表で記述する.

5.3.1 AA（Asset×Attack）表

AA 表では攻撃シーンごとに守るべきアセットを特定することを目的として，守るべきアセットと攻撃の組み合わせを整理する．要求定義工程で利用するレベルに絞り込むため，AA 表を用いて STRIDE[16]単位で攻撃と守るべきアセットを特定できるようにする必要がある．STRIDE モデルは Spoofing（なりすまし），Tampering（改ざん），Repudiation（否認），Information disclosure（情報の漏えい），Denial of service（サービス拒否），Elevation of privilege（特権の昇格）の 6 種にマ

イクロソフトが脅威を分類したものである．

一般にセキュリティ要件を検討するときにはどのような攻撃がありうるか不明なところからスタートする．網羅性の向上は要件定義者の知見によることが多いが，セキュリティ知見は専門家に限られる場合も多い．そこでセキュリティ上の網羅性を向上させることを目的として，AA 表では STRIDE モデルを用いて攻撃者による攻撃方法を列挙することとした．STRIDE 単位で SARM 状況表を作成することにより，網羅性が高くかつ細かすぎないセキュリティ要求分析ができる．さらに脅威の詳細化が必要になる場合には, IPA の脅威データベースなども参考にすることができる[49].

以下では，まず AA 表を定義し，次いで具体例を示す.

[定義]AA 表

AA 表の各要素を次式で定義する.

AA[attack, asset] = もし attack が asset を攻撃するなら，○.

そうでないとき，―

AA[attack,種別] = 脅威種別を表す S, T, R, I, D, E などの記号

AA[attack, 攻撃内容]= 脅威に対応する具体的な攻撃内容

AA[attack, 状況表]= 対応する SARM 状況表を識別するための ID

[具体例]攻撃方法の集合 Attack={なりすましによる不正注文,注文情報の改竄,商品注文への否認,情報の漏えい,システムへの DOS 攻撃等,管理人への権限昇格}

資源の集合 Asset ={COOKIE 情報,セッション ID,パスワード,個人情報 }とすると，表 5-3①のような AA 表を作成できる．たとえば,

AA[なりすましによる不正注文, COOKIE 情報] = ○

AA[注文情報の改竄, COOKIE 情報] = ―

となる．なりすましによる不正注文の場合は，各攻撃ごとの脅威種別は S，対応する SARM 状況表を識別するための ID は，A_S を記入する.

表 5-3-1 AA（Asset×Attack）表の具体例

攻撃方法			攻撃対象資源			
種別	攻撃内容	状況表	COOKIE情報	セッションID	パスワード	個人情報
S	なりすましによる不正注文	A_S	○	○	○	○
T	注文情報の改竄	A_T	―	○	○	○
R	商品注文への否認	A_R	―	―	―	○
I	情報の漏えい	A_I	○	○	○	○
D	システムへのDos攻撃等	A_D	○	○	―	―
E	管理人への権限昇格	A_E	○	―	―	―

5.3.2 SARM 状況表

SARM 状況表は攻撃者，悪意，攻撃方法，脆弱性の特定を行うことを目的として，AA 表で抽出した攻撃状況単位で作成する．SARM 状況表では一般アクタだけでなく，攻撃アクタを追加してアクタ関係行列を作成する．ARM は i*の SD 図を表構造を用いて記述する表記方法である．しかし ARM では，AND/OR 等に基づくゴール分解構造を記述することはできなかった．このため，SARM では以下の定義で述べる階層ゴール式を導入することにより，SR 図の内容を表現できるように ARM を拡張した.

[定義]SARM 状況表

SARM[X,Y] = { e:階層ゴール式 }

アクタ X がアクタ Y に対して要求する，ゴール G，ソフトゴール S，タスク T，資源 R としての階層ゴール式の集合を SARM[X,Y] で表す．ゴール G，ソフトゴール S，タスク T，資源 R の各要素に識別番号（ID）を付与して，一意に ID を管理する欄を設定する．また依存先を(to 要素 ID)という形式で示す．ここで，X および Y は，一般アクタか攻撃アクタである． とくに，SARM[X,X] は，アクタ X 自身の目標としてのゴール，ソフトゴール，タスク，資源としての階層ゴール式の集合を表す． なお, +は項目の選択を示し，“S”とは文字 S をそのまま記述することを示している．

[定義]階層ゴール式

<階層ゴール式>::=<階層ゴール基本式><改行><字下げ><階層ゴール式> +
　<階層ゴール基本式><改行><字下げ><積階層ゴール式並び> +
　<階層ゴール基本式><改行><字下げ><和階層ゴール式並び> +
　<階層ゴール基本式>
<積階層ゴール式並び>::=“&” <階層ゴール式> +
　“&” <階層ゴール式><改行><積階層ゴール式並び>
<和階層ゴール式並び>::=“｜” <階層ゴール式> +
　“｜” <階層ゴール式><改行><和階層ゴール式並び>
<階層ゴール基本式>::=
<ゴール> + <ソフトゴール> + <タスク> + <資源> + <攻撃ゴール> +
<攻撃ソフトゴール> + <攻撃タスク> + <攻撃資源>
<ゴール>::=“○”<ゴール名>
<ソフトゴール>::=“☆” <ソフトゴール名>
<タスク>::=“◇” <タスク名>
<資源>::=“□” <資源名>
<攻撃ゴール>::=“●”<脆弱性><攻撃ゴール名>
<攻撃ソフトゴール>::=“★” <脆弱性><攻撃ソフトゴール名>
<攻撃タスク>::=“◆” <脆弱性><攻撃タスク名>
<攻撃資源>::=“■” <脆弱性><攻撃資源名>
<脆弱性>::= “- -” + “-” + “ ”

この表記を用いて作成したなりすまし（A_S）に対する状況表を表 3 に示す．例えば，攻撃者 EVE のゴールが対角行列で表現されている．★ALICE になりすまし，商品を手に入れたいという S8 に依存する意図のもとに, &◆利用者 ALICE に EVE のサイトをクリックさせるという S1 に依存するタスクと&◆COOKIE 情報内のセッション ID を利用するという 2 つのタスクを実施するので，&が前置される．COOKIE 情報という資源が攻撃者のゴール, ソフトゴールに対してどの程度の脆弱性を持つかを i*-Liu 法に準じてーー，ー，未記入からなる 3 段階の接頭辞によって明記する．

また,SARM 状況表は第 1 種 SARM 状況表と第 2 種 SARM 状況表に分類することができる．この 2 種の定義を以下に示す．

[定義]第 1 種 SARM 状況表

SARM[X,Y]要素が(X≠Y)のとき，<階層ゴール基本式＞のみであるとき第 1 種 SARM 状況表という．

[定義]第 2 種 SARM 状況表

SARM 状況表が第 1 種でないとき，第 2 種 SARM 状況表であるという．

このように，SARM 状況表を第 1 種と第 2 種に分けることによるメリットは，①SARM の作成方法を明確にする，②SARM と i*-Liu 法の等価性の証明の根拠を

明確にする，③変換ツールを作成する時の基準を示すことである.

第 1 種 SARM 状況表の対角要素と非対角要素が SR 図の情報に対応する．第 2 種 SARM 状況表の対角要素は SR 図と同じ情報を持つ. 第 2 種 SARM 状況表では，非対角要素として，階層ゴール基本式以外に，階層ゴール式も記述できることから，ゴール分解関係も記述できるという特徴がある．一方，SR 図ではアクタ関係に対してゴール分解することはできない．この点で第 2 種 SARM 状況表は SR 図よりも詳細なアクタ関係を記述できる.

またアクタ関係行列という表形式の手法を使用することにより，表の全ての欄を埋めるように検討を行うことができる点で SARM 状況表では網羅性を向上できる．定義から分かるように，SARM 状況表では，一般アクタと攻撃アクタのゴールとソフトゴール，タスク，資源に対する表現を階層的に記述できる.

このように階層ゴール式による攻撃表現の構造化では，①マークを○ゴール，☆ソフトゴール，◇タスク，□資源のように前置すること，②一般者は白抜きのマーク, 攻撃者は黒塗りのマークを使用すること, ③タスク間の関係は&:論理積（AND）か｜：論理和(OR)を前置し，構造化することにより分かりやすく表現できるようにした．また，攻撃者の目標・意図・タスクを明確にするため，攻撃者欄を灰色に塗りつぶすこともできる．表 5-3-2 に示したのは SARM 対応表の例である.

表 5-3-2　AA 表のなりすまし（A_S）を作成単位とした SARM 状況表の具体例

	利用者ALICE A1		脆弱性のあるシステムBOB A2		攻撃者EVE A3	
利用者ALICE A1	S4	☆色々なサイトを閲覧したい(to S3),(to S5)	S5	☆BOBのサイトを閲覧したい(to A2)	S3	☆EVEのサイトを閲覧したい(to S2)
	G6	&○必要な情報を入力する				
	T3	&◇ログインをする				
脆弱性のあるシステムBOB A2	S6	☆正当な利用者にアクセスさせる(to G8)	G1	○webページを生成する	S7	☆正当ではない利用者にはアクセスさせない(to S2)
			G2	○利用者情報に従って情報を提供する		
			G3	○利用者情報を保護する		
			R2	□利用者情報		
			G4	○利用者ごとの管理をする		
			T4	&◇許可された利用者に情報へのアクセスを許可する(to S6)(to S7)		
			R3	□認証データ		
			T5	&◇COOKIE情報を管理する		
			G5	○商品の販売をする		
			T6	◆ALICEになりすまして、商品の注文をする		
攻撃者EVE A3	S1	★ALICEにEVEのサイトをクリックさせたい(to A1)	S8	★BOBのシステムで商品を注文し、商品を手に入れたい(to T6)	S2	★ALICEになりすまし商品を手に入れたい(to S8)
					T1	&◆利用者ALICEにEVEのサイトをクリックさせる(to S1)
					T2	&◆COOKIE情報内のｾｯｼｮﾝIDを利用する
					R1	■COOKIE情報

5.4　CC に対応した SARM の事例

5.4.1 AA 表による脅威抽出事例

CC に対応した SARM の AA 表を表 5-4-1 に示す. 具体的な例示に関しては, IPA

の ST 事例[45]をもとに記述した. この事例の TOE は「A 社個人情報処理システム」を構成するアプリケーションソフトウェアであり，基本機能及び個人データの漏えいを防止，改ざんを検出するためのセキュリティ機能を提供している．セキュリティ機能には監査機能，操作員管理・アクセス制御機能，識別認証機能，暗号機能，バックアップ・リカバリ機能がある．この事例ではより CC と対応した脅威抽出を行うために STRIDE ではなく TOE のセキュリティ機能を種別としてセキュリティ機能ごとに想定される脅威と保護すべき資産を抽出している．

表 5-4-1　CC に対応した AA 表の事例

種別	脅威	資産		
		個人データ	TSF データ	バックアップデータ
識別認証機能	T.ILLEGAL_LOGON（不正なログオン）	○		
操作員管理・アクセス制御機能	T.UNAUTHORIZED_ACCESS（不正なアクセス）	○		
操作員管理・アクセス制御機能	T.MISUSE（誤操作）	○		
操作員管理・アクセス制御機能	T.INJUSTICE（不正行為）	○		
識別認証機能	T.SPOOFING（なりすまし）	○	○	
暗号機能	T.DISCLOSE_NW_DATA（ネットワークデータ暴露）	○	○	
暗号機能	T.REMOVABLE_MEDIA（リムーバブル媒体）			○
バックアップ／リカバリ機能	T.UNEXPECTED_ACCIDENT（不測の事態）			○

5.4.2 SARM 状況表による脅威分析事例

CC と対応した SARM 状況表として TOE 利用者をアクタに適用した事例を表 5-4-2 に示す．AA 表と同様，IPA の ST 事例[45]をもとに記述した．ST の「TOE 記述」に示される TOE 利用者が一般のアクタに相当する．尚，本事例ではサーバ管理者，監査者，個人情報管理者は不正を犯すことがないことを前提条件にしているため，一つにまとめて記述している．オペレータや個人情報利用者は不正を犯す可能性があることが前提条件になっているため，分けて記述している．従来は攻撃者を追加していたが，攻撃者以外の各アクタ自身の脅威も示すため，攻撃・誤操作として追加する．攻撃者の意図は一番下の灰色の行，各アクタの意図に応じて起こりうる脅威は一番右の灰色の列に示される．尚，本事例はセキュリティ機能に範囲を限定して脅威分析をするため，一般アクタどうしの意図はあまり分析していないが，セキュリティ機能とともに一般的機能も分析する場合はこの欄もより有効に使われるだろう．

また CC と対応した SARM 状況表としてセキュリティ機能をアクタに適用した事例を表 5-4-3 に示す．SARM のアクタは人を設定するだけでなく，システムや機能も設定可能である．TOE 種別をもとにした攻撃種別一覧を表 5-4-4 に示す．機能クラスをもとにした対策一覧を表 5-4-5 に示す．セキュリティ機能をアクタに適用した場合，表 5-4-3 のように TOE 種別をもとに攻撃種別としてカテゴリ化しやすいので，DB 化を図り，SARM で脅威を選択するときに利用することが可能であろう．また SARM で選択された脅威を対策化するときには表 5-4-5 のように機能クラスをもとにした対策のカテゴリ化が可能である．攻撃種別と対策の一覧を知識

資産化して作成し，蓄積されたデータのカテゴリを利用して適切な脅威や対策を選択することにより，より迅速に漏れのない脅威と対策の選択が可能になることが期待できる．

表 5-4-2　TOE 利用者をアクタに適用した SARM 状況表の事例

	サーバ管理者・監査者・ 個人情報管理者	オペレータ	個人情報利用者	攻撃・誤操作
サーバ管理者・監査者・個人情報管理者	☆サーバ管理者自身は、個人データの登録、更新、削除、閲覧・検索、提供、預託、及び加工を行わず、次の業務を行う。 〇基本機能の起動／停止 |〇鍵管理（サーバ共通鍵・処理連携サーバ共通鍵・サーバ公開鍵・サーバ秘密鍵の生成・更新・削除、提供・預託先公開鍵のインポート・削除） □TSFデータ |〇システム環境設定（パスワード試行回数管理、バナー表示メッセージ管理、操作員種別毎のセション確立許可時間帯管理） |〇バックアップ／リカバリ □バックアップデータ |〇個人データの提供・預託データの外部出力 □個人データ |〇監査証跡参照 □TSFデータ ☆監査者には、以下の権限のみが付与され、監査者自身は、個人データの登録、閲覧・検索、提供、預託、加工、更新、及び削除を行わず、次の業務を行う。 〇監査証跡参照 〇監査証跡管理 〇監査証跡退避 □TSFデータ ☆個人情報管理者端末より、個人情報の管理を行う権限を与えられた操作者である。個人情報を管理するため、以下の3つの操作を行う。 〇個人データの閲覧・検索 □個人データ 〇オペレータ・個人情報利用者の操作の承認	〇操作員種別ごとのセション確立許可時間帯の管理）		★個人データ・バックアップデータを喪失 ●T.UNEXPECTED_ACCIDENT（不測の事態） ★誤ってデータを破壊・改ざん・防露 ●T.MISUSE（誤操作）
オペレータ		☆個人データの登録、更新、及び削除にあたっては、オペレータは、個人情報管理者の承認を得るためのデータ（個人情報に関する承認依頼データ（登録用）（更新用）（削除用））を作成する。オペレータが作成したデータは、個人情報管理者が承認することにより反映される。 また、顧客端末からの個人情報登録・更新・削除依頼に対し、処理連携サーバ端末が依頼を受領した旨のメールをオペレータへ送信後、オペレータはサーバ端末を経由して、処理連携サーバ端末DB上の未登録個人データを、サーバ端末DBに格納する。 □個人データ		★個人データ・バックアップデータを喪失 ●T.UNEXPECTED_ACCIDENT（不測の事態） ★誤ってデータを破壊・改ざん・防露 ●T.MISUSE（誤操作） ★個人データを破壊・改ざん・暴露 ●T.ILLEGAL_LOGON（不正なログオン） |●T.UNAUTHORIZED_ACCESS（不正なアクセス） |●T.SPOOFING（なりすまし） ★個人データを暴露 ●T.INJUSTICE（不正行為）
個人情報利用者			☆個人データの提供、及び預託 〇個人情報管理者の承認を得るためのデータ作成 □個人データに関する承認依頼データ（提供用）（預託用） 〇個人情報利用者が作成したデータを個人情報管理者が承認することにより、当該データは暗号化され、サーバ端末DB上に個人データを提供・預託するためのデータとして生成される □個人データの提供データ、預託データ	★個人データを破壊・改ざん・暴露 ●T.ILLEGAL_LOGON（不正なログオン） |●T.UNAUTHORIZED_ACCESS（不正なアクセス） |●T.SPOOFING（なりすまし） ★個人データを暴露 ●T.INJUSTICE（不正行為）
攻撃・誤操作	★個人データを破壊・改ざん・暴露 ●T.UNAUTHORIZED_ACCESS（不正なアクセス） |●T.SPOOFING（なりすまし）	★個人データを破壊・改ざん・暴露 ● T.UNAUTHORIZED_ACCESS（不正なアクセス） |●T.SPOOFING（なりすまし）	★個人データを破壊・改ざん・暴露 ●T.UNAUTHORIZED_ACCESS（不正なアクセス） |●T.SPOOFING（なりすまし）	★個人情報を入手することによって利益を得ることや、A社の業務妨害を目的として個人データを改ざん・暴露・破壊する ●T.UNAUTHORIZED_ACCESS（不正なアクセス） |●T.SPOOFING（なりすまし） ★TSFデータを改ざん ●T.DISCLOSE_NW_DATA（ネットワークデータ暴露） ★バックアップデータを改ざん・暴露 ●T.REMOVABLE_MEDIA（リムーバブル媒体）

表 5-4-3　セキュリティ機能をアクタに適用した SARM 状況表の事例

	基本機能	監査機能	操作員管理・アクセス制御機能	識別認証機能	暗号機能	バックアップ・リカバリ機能	攻撃・誤操作
基本機能	☆個人データの登録、更新、閲覧・検索、提供、預託、加工、削除の機能、未登録個人データの外部入力機能、提供・預託データの外部出力機能、及び監査証跡の退避機能をもつ						
監査機能		☆TOEの監査証跡を採取し、参照・管理を可能にする					
操作員管理・アクセス制御機能			☆TOEにアクセスする利用者の管理、および各利用者に付与された権限に基づきTOEへのアクセス制御する				
識別認証機能				☆TOEへアクセスする利用者の識別認証、端末の検証、パスワードの品質検証、及びアカウントロックを行う			
暗号機能					☆サーバ・クライアント間通信の暗号化、バックアップデータの暗号化・復号、及び個人データの提供データ・預託データの暗号化を行う		
バックアップ・リカバリ機能						☆TOEの復旧に必要なデータのバックアップ／リカバリを行う	
攻撃・誤操作	★TOE(クライアント端末)の正当な基本機能利用者のうち、個人情報利用者、及びオペレータが、故意に許可されていない操作(生成、参照、更新、削除、印刷、及び保存)を行うことにより、利用者データを破壊・改ざん・暴露するかもしれない。 ●.UNAUTHORIZED_ACCESS(不正なアクセス)	★許可された利用者である監査者及びサーバ管理者以外のものが監査証跡の改ざんするかもしれない. ●T.INJUSTICE(不正行為)	★TOE(クライアント端末)の正当な基本機能利用者のうち、個人情報利用者、及びオペレータが、故意に許可されていない操作(生成、参照、更新、削除、印刷、及び保存)を行うことにより、利用者データを破壊・改ざん・暴露するかもしれない。 ●.UNAUTHORIZED_ACCESS(不正なアクセス) ★TOEで利用される各端末の正当な操作員が、誤操作により利用者データを破壊・改ざん・暴露するかもしれない。 ●T.MISUSE(誤操作) ★TOE(クライアント端末)の正当な基本機能利用者のうち、個人情報利用者、及びオペレータが、業務時間外など明らかに管理状態にない場合、TOEを利用し利用者データを暴露するかもしれない。 ●T.INJUSTICE(不正行為)	★攻撃者が、TOEの正当な利用者になりすましてTOEを利用することにより、利用者データを破壊・改ざん・暴露するかもしれない。 ●T.ILLEGAL_LOGON(不正なログオン ★個人情報利用者、オペレータ、及び攻撃者が、TOE(クライアント端末)の正当な基本機能利用者の離席時にクライアント端末を利用して、利用者データを破壊・改ざん・暴露するかもしれない。 ●T.SPOOFING(なりすまし)	★個人情報利用者、オペレータ、及び攻撃者が、サーバ端末とクライアント端末間のネットワーク上でやりとりされる通信データを、不正に入手することで利用者データを改ざん・暴露するかもしれない。 ●T.DISCLOSE_NW_DATA(ネットワークデータ暴露) ★個人情報利用者、オペレータ、及び攻撃者が、バックアップデータ、及び提供・預託データが保存されたリムーバブル媒体を不正に入手することで利用者データを改ざん・暴露するかもしれない ●T.REMOVABLE_MEDIA(リムーバブル媒体)	★火災、天災、ディスク障害、その他の不測の事態により、TOEの動作のために必要なデータが失われるかもしれない。 ●.UNEXPECTED_ACCIDENT(不測の事態)	★個人情報を入手することによって利益を得ることや、A社の業務妨害を目的として個人データを改ざん・暴露・破壊する ●T.UNAUTHORIZED_ACCESS(不正なアクセス) ●T.SPOOFING(なりすまし)

表 5-4-4　攻撃種別一覧

セキュリティ機能	TOE種別	攻撃種別
操作員管理・アクセス制御機能	アクセス制御	T.UNAUTHORIZED_ACCESS（不正なアクセス）
操作員管理・アクセス制御機能	その他	T.MISUSE（誤操作）
監査機能	検知	T.INJUSTICE（不正行為）
識別認証機能	ネットワーク管理	T.ILLEGAL_LOGON（不正なログオン）
識別認証機能	ネットワーク管理	T.SPOOFING（なりすまし）
暗号機能	データ保護	T.DISCLOSE_NW_DATA（ネットワークデータ暴露）
暗号機能	データ保護	T.REMOVABLE_MEDIA（リムーバブル媒体）
バックアップ／リカバリ機能	その他	T.UNEXPECTED_ACCIDENT（不測の事態）

表 5-4-5　対策一覧

攻撃種別	機能クラス	対策名	対策内容
T.UNAUTHORIZED_ACCESS（不正なアクセス）	FDP（利用者データ保護）	O.ACCESS_CONTROL（アクセスコントロール）	TOEは、操作員または操作員を代行するプロセスに対して、各操作員の種別とその操作対象に応じて設定・付与された権限に従った、保護資産へのアクセスを保証しなければならない。
T.UNAUTHORIZED_ACCESS（不正なアクセス）	FDP（利用者データ保護）	O.TAKE_OUT（クライアント端末を経由したTOE外への利用者データの持ち出し禁止）	TOEは、クライアント端末を経由した利用者データのTOE外への持ち出し（保存、印刷）を禁止しなければならない。
T.UNAUTHORIZED_ACCESS（不正なアクセス）	FAU（セキュリティ監査）	O.AUDIT（監査）	TOEは、特定の事象が発生した場合これを監査証跡として保管しなければならない。監査証跡は、TOEのセキュリティ侵害の事後調査における記録として利用されるため、以下を満たすことが必要となる。 ・監査証跡には、事象の日付・時刻、事象個所、及び事象に責任を持つ主体を含め生成されること。 ・対象となるすべての監査事象を監査証跡として取得すること。 ・監査証跡の改ざんを防御し、これを検出できること。 ・監査証跡は許可された利用者である監査者及びサーバ管理者のみが許可された範囲の利用ができること。
T.UNAUTHORIZED_ACCESS（不正なアクセス）	FAU（セキュリティ監査）	O.ALERT（アラート）	TOEは、TOEに対するセキュリティ侵害の可能性を検知しなければならない。またセキュリティ侵害の可能性を検知した場合、サーバ管理者及び監査者に対してその可能性について通知しなければならない。
T.UNAUTHORIZED_ACCESS（不正なアクセス）	その他	OE.AUTHORIZATION_SETTING（権限の設定）	組織の責任者は、TOEに関連する権限・役割をもつ操作員として個人情報管理者、サーバ管理者、及び監査者を任命し、それぞれの権限付与の規定が載っている規則を参照して、それに基づいて権限を付与することにより、TOEに対し行える操作を割り当てなければならない。 個人情報管理者は、オペレータ、及び個人情報利用者の任命・管理を組織の責任者から委任され、TOEに関連する権限・役割をもつ操作員としてオペレータ、及び個人情報利用者を任命し、それぞれの権限付与の規定が載っている規則を参照して、それに基づいて権限を付与することにより、TOEに対し行える操作を割り当てなければならない。
T.UNAUTHORIZED_ACCESS（不正なアクセス）	その他	OE.TRUSTED_ROLE（信頼される役割）	組織の責任者は、サーバ管理者、監査者、及び個人情報管理者の役割に適した者を人選し、その上で、それぞれの役割を理解させる。
T.UNAUTHORIZED_ACCESS（不正なアクセス）	その他	OE.TIME_STAMP（高信頼タイムスタンプ）	TOEでは、監査証跡を生成する際、及び利用時間制限を行う際に、高信頼タイムスタンプが利用できなければならない。

攻撃種別	機能クラス	対策名	対策内容
T.MISUSE（誤操作）	FMT（セキュリティ管理）	O.ACCESS_CONTROL（アクセスコントロール）	TOEは、操作員または操作員を代行するプロセスに対して、各操作員の種別とその操作対象に応じて設定・付与された権限に従った、保護資産へのアクセスを保証しなければならない。
T.MISUSE（誤操作）	FDP（利用者データ保護）	O.TAKE_OUT	TOEは、クライアント端末を経由した利用者データのTOE外への持ち出し（保存、印刷）を禁止しなければならない。
T.MISUSE（誤操作）	その他	OE.TRAINING（教育・訓練）	すべての操作員は、個人データ及びTOEの安全管理に関する操作員の役割及び責任についての教育・訓練を受けなければならない。
T.INJUSTICE（不正行為）	FAU（セキュリティ監査）	O.AUDIT（監査）	TOEは、特定の事象が発生した場合これを監査証跡として保管しなければならない。監査証跡は、TOEのセキュリティ侵害の事後調査における記録として利用されるため、以下を満たすことが必要となる。 ・監査証跡には、事象の日付・時刻、事象個所、及び事象に責任を持つ主体を含め生成されること。 ・対象となるすべての監査事象を監査証跡として取得すること。
T.INJUSTICE（不正行為）	FAU（セキュリティ監査）	O.ALERT（アラート）	TOEは、TOEに対するセキュリティ侵害の可能性を検知しなければならない。またセキュリティ侵害の可能性を検知した場合、サーバ管理者及び監査者に対してその可能性について通知し
T.INJUSTICE（不正行為）	FTA（TOEアクセス）	O.AVAILABLE_TIME_RESTRICTION	TOEは、管理されたセション確立可能な時間に基づき、セションの確立を制限しなければならない。
T.INJUSTICE（不正行為）	その他	OE.TRUSTED_ROLE（信頼される役割）	組織の責任者は、サーバ管理者、監査者、及び個人情報管理者の役割に適した者を人選し、その上で、それぞれの役割を理解させる。
T.INJUSTICE（不正行為）	その他	OE.TRAINING（教育・訓練）	すべての操作員は、個人データ及びTOEの安全管理に関する操作員の役割及び責任についての教育・訓練を受けなければならない。
T.INJUSTICE（不正行為）	その他	OE.TIME_STAMP（高信頼タイムスタンプ）	TOEでは、監査証跡を生成する際、及び利用時間制限を行う際に、高信頼タイムスタンプが利用できなければならない。
T.ILLEGAL_LOGON（不正なログオン）	FIA（識別と認証）	O.I&A（操作員の識別認証）	TOEは、操作員がTOEを利用する時は必ず識別認証されることを保証し、指定された回数以内に識別認証に成功した操作員のみTOEの利用を許可しなければならない。
T.ILLEGAL_LOGON（不正なログオン）	FIA（識別と認証）	OE.PASSWORD_MANAGEMENT（操作員によるパスワードの管理）	すべての操作員は、TOEサービスを提供するシステムにアクセスするための認証情報（パスワード）を記憶し、他人に漏らしてはならない。また推測・解析されやすい認証情報（パスワード）を設定してはならず、適正な間隔で変更しなければならない。
T.SPOOFING（なりすまし）	FTA（TOEアクセス）	O.AUTO_LOGOUT（自動ログアウト）	TOEは、TOEにログオンした操作員から、一定時間TOEへのアクセスがないとき、自動的にログアウトを行わなければならない。
T.DISCLOSE_NW_DATA（ネットワークデータ暴露）	FCS（暗号サポート）	O.USERDATA_PROTECTION（利用者データの保護）	TOEは、以下のデータを秘匿し、改ざんを検出できなければならず、それぞれに対し許可された操作員や端末のみがデータを利用することができなければならない。 ・サーバ管理者が、バックアップデータを利用することができる。 ・個人情報管理者、及び個人情報利用者が、個人データの提供・預託データを利用することができる。 ・サーバ端末－クライアント端末間で通信される利用者データは、当該端末が利用することができる。
T.REMOVABLE_MEDIA（リムーバブル媒体）	FCS（暗号サポート）	O.USERDATA_PROTECTION（利用者データの保護）	TOEは、以下のデータを秘匿し、改ざんを検出できなければならず、それぞれに対し許可された操作員や端末のみがデータを利用することができなければならない。 ・サーバ管理者が、バックアップデータを利用することができる。 ・個人情報管理者、及び個人情報利用者が、個人データの提供・預託データを利用することができる。 ・サーバ端末－クライアント端末間で通信される利用者データは、当該端末が利用することができる。
T.UNEXPECTED_ACCIDENT（不測の事態）	FDP（利用者データ保護）	O.BACKUP_RECOVERY（バックアップ／リカバリ）	TOEは、TOEが正常に動作するために必要な利用者データ及びTSFデータをバックアップする手段を提供しなければならない。また、バックアップした利用者データ及びTSFデータを、TOEの動作を復旧させるためにTOEへリカバリする手段を提供しなければならない。

5.4.3 SARM による ST 項目の分析と CC 対応の工夫

SARM を CC に対応させた事例作成により判明した SARM で表 5-4-6 に示す ST 項目の一部を分析することができることと CC に対応させるため, SARM に記述の工夫ができることを以下に示す(図 5-4).「ST 概説」の「TOE 概要」に記載する「TOE 種別」は，表 5-4-7 に示す分類が CC-portal[1]で提供されている．この分類を利用して，SARM の AA 表で脅威を抽出すると，セキュリティ機能にあわせたシーンで資産と脅威を洗い出すことができる．更に TOE の分類を利用してセキュリティ機能別の脅威をパターン化し利用することも考えられる．従来の SARM は TOE 既知のパターンとして STRIDE[47]等の分類を適用してある程度定形的な分析を可能としていた．しかし CC 対応のためには対象のシステムや生産物に合わせた分類にして状況分析を実施することが大事であるため，TOE 種別の分類の上でセキュリティ機能別の脅威をパターンする方が適している．STRIDE では脅威の対象外だったミスなどの環境・運用的な分類も CC では必要であり，パターンに追加することも可能である．

「ST 概説」の「TOE 記述」に記載する TOE の利用者は SARM の一般アクタとして記述可能である．SARM により，攻撃者による脅威の他に TOE 利用者がどのような攻撃や誤操作を起こしうるかを分析できる．

「TOE セキュリティ課題定義」に記載する「脅威」は SARM による脅威分析の結果を利用できる．

「TOE セキュリティ課題定義」に記載する「TOE 資産」は SARM による資産抽出の結果を利用できる．

尚，CC に対応した SARM 作成を工夫するために SARM の資産，アクタに設定できる資産と処理を分類して，表 5-4-8 に示す．データなど表の資産の欄に○印があるものは資産として抽出可能である．監査・監視，利用主体．情報処理システム，情報機器，セキュリティ機能は SARM のアクタとして分析対象になりうる．

表 5-4-6　SARM に関連する ST 項目

SARMに関連するSTの記述項目			SARMでの対応
ST概説	TOE概要	TOE種別および主要セキュリティ機能	TOEの分類を利用してセキュリティ機能別証跡をDB化
	TOE記述	TOEの利用者の役割	アクタに相当
TOEセキュリティ課題定義	TOE資産		資産に相当
	脅威		脅威の洗い出し ＊人為的ミスなども対象に入れて洗い出す

表 5-4-7　TOE 種別

TOE種別	内容
アクセス制御	アクセス制御機能
パウンダリー保護	ファイヤーウオールやルータなど
データベース	データベース管理機能
データ保護	データのイレーズ機能、暗号チップ等
検知	侵入検知システム（ＩＤＳ）など
ICカード	ICカード関連のチップやソフトウェア
鍵管理	暗号鍵管理
ネットワーク管理	ネットワーク関連の管理機能
オペレーティングシステム	オペレーティングシステム
電子署名	ＰＫＩ関連機能
その他	－

表 5-4-8　SARM に利用できる資産とアクタの分類

		資産	アクタ
データ	可搬媒体	○	
	記憶媒体	○	
	紙媒体	○	
	メモリ	○	
	削除・廃棄	○	
	ネットワーク	○	
	暗号化	○	
	表示	○	
	入力	○	
	印刷	○	
プログラムコード		○	
プログラム実行（サービス）		○	
監査・監視			○
利用主体			○
情報処理システム（利用と運用）			○
情報機器			○
セキュリティ機能			○

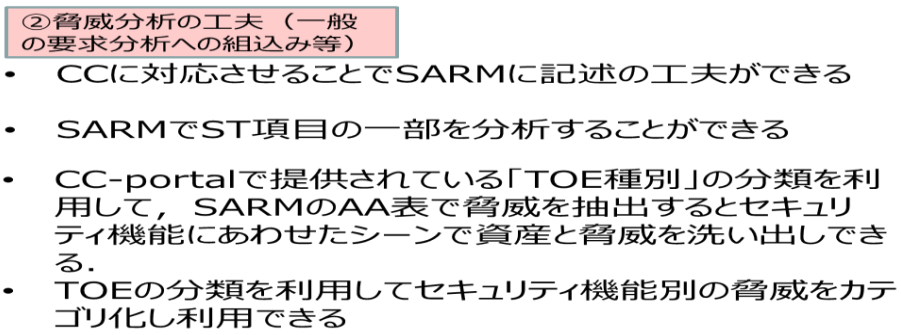


図 5-4　CC に適したデータ利用

5.5　スパイラルレビュー手法

(1) 目的

SARM は網羅性が高いという利点があるので，一人でも網羅性をもって分析することに向いており，i*-Liu 法は一覧性が高く，作成結果を理解しやすいという利点があるので，複数人での分析に向いていると考えられる．そこで，両手法の利点を活用し，より効果的な要求分析を実施するため，SARM と i*-Liu 法の双方を用いたスパイラルレビューを提案する．

スパイラルレビューの手順と事例

SARM と i*-Liu 法の双方を用いたスパイラルレビューの手順を以下に示す．

[手順 1]システム開発者が一般の各アクタ間の要求分析を i*で実施する．

[手順 2]セキュリティ担当者が AA（Asset×Attack）表で守るべき資源と攻撃パターンを洗い出す．

[手順 3]AA 表で洗い出した作成単位で,通常のシステム開発者とセキュリティ担当者がディスカッションツールとして，i*-Liu 法を使用し，結果を作図する．

[手順 4]セキュリティ担当者が，i*-Liu 法を SARM に変換した上で，攻撃者を加えたセキュリティの要求分析を第 1 種 SARM 状況表で実施する．

5.6　詳細レビューによる攻撃者による具体的なタスク分析

(1) 目的

攻撃者による具体的なタスク分析として，第 2 種 SARM 状況表を用いたアクタ間の詳細レビューが実施可能である．第 2 種 SARM 状況表による詳細レビュー実施の目的は現状の i*-Liu 法では詳細に記述できないアクタ関係を SARM でレビューできるようにすることである．現状の i*-Liu 法の記述法や i*-Liu 法と等価性をもつ第 1 種 SARM 状況表では,アクタ間の関係を記述はできるが，この関係を論理的に分解して記述することができない．これに対して第 2 種 SARM 状況表は非対角欄にも対角欄と同様に論理式を記述できるので，アクタ間の関係をより詳細に分析できる．スパイラルレビューに加えて第 2 種 SARM 状況表による詳細レビューを実施する理由は，攻撃者の他のアクタに対する具体的な攻撃は非対角欄に記述することによって，その攻撃タスクが何であるかをより具体的にタスクレベルで抽出する必要があるからである．非対角欄こそが，攻撃者の他のアクタに対する具体的な意図が示される場所であり，詳細レビューの実施に際し，攻撃の具体的なタスクをあげて分析を実施すべき場所となる．

(2) 詳細レビューの手順と事例

第 2 種 SARM 状況表の記述能力の高さを生かすために，図 5-6 のようにして i*-Liu 法と SARM のアクタ間のスパイラルレビュー後に第 2 種 SARM 状況表を用

いて，アクタ間の詳細レビューを実施する．

第 2 種 SARM 状況表による詳細レビュー結果を表 5-6 に示す．表 5-6 では，攻撃者 EVE の脆弱性のあるシステム BOB に対する具体的な攻撃内容が非対角要素に記載されている．たとえば，攻撃者 EVE の脆弱性のあるシステム BOB への意図を★BOB のシステムで商品を注文し,商品を手に入れたい(to T6)というソフトゴールの元に◆ALICE のセッション ID を盗むというタスクがあり,そのタスクを実行するには｜◆Script Insertion か｜◆HTTP レスポンス攻撃か｜◆XSS という具体的な攻撃タスクをあげるといった詳細な記述ができることが分かる．

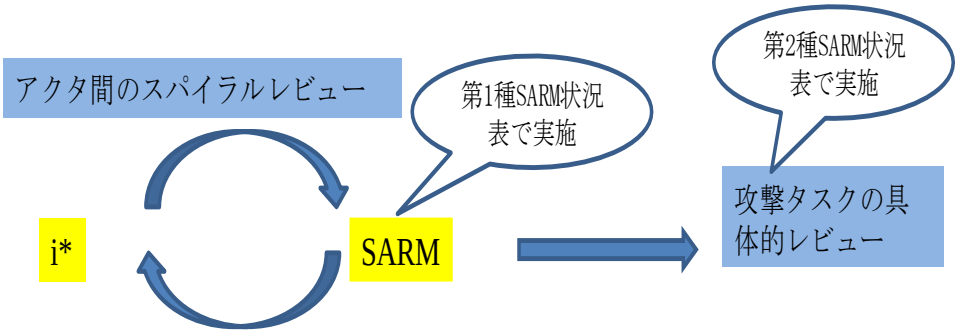


図 5-6　スパイラルレビューと詳細レビューの関係

表 5-6　第 2 種 SARM 状況表の詳細レビュー後の事例

	利用者ALICE A1		脆弱性のあるシステムBOB A2		攻撃者EVE A3	
利用者 ALICE A1	S4	☆色々なサイトを閲覧したい(to S3)	S5	☆BOBのサイトを閲覧したい	S3	☆EVEのサイトを閲覧したい(to T2)
	G6	&○必要な情報を入力する		○webページをリクエストする		◇BOBのサイトにログインしたままEVEのサイトをクリックする
	T3	&◇ログインをする	T7	&◇BOBのサイトのトップページにアクセスする		
脆弱性のあるシステムBOB A2	S6	☆正当な利用者にアクセスさせる(to G2)	G1	○webページを生成する	S7	☆正当ではない利用者にはアクセスさせない(to S2)
	T8	◇ALICEにセッションIDを割り当てCOOKIE情報を通知する	G2	○利用者情報に従って情報を提供する		
			G3	○利用者情報を保護する		
			R2	□利用者情報	T10	◇偽造された認証データの使用を検知または拒否する
			G4	○利用者ごとの管理をする		
			T4	&◇許可された利用者に情報へのアクセスを許可する(to S6)(to S7)		
			R3	□認証データ		
			T5	&◇COOKIE情報を管理する		
			G5	○商品の販売をする		
			T6	◆ALICEになりすまして，商品の注文をする		
			T9	◆XSSの脆弱性によりALICEのCOOKIEをそのままEVEに送信(to T7)		
攻撃者 EVE A3	S1	★ALICEにEVEのサイトをクリックさせたい(to A1)	S8	★BOBのシステムで商品を注文し，商品を手に入れたい(to T6)	S2	★ALICEになりすまし商品を手に入れたい
			T11	◆ALICEのｾｯｼｮﾝIDを盗む	T1	&◆利用者ALICEにEVEのサイトをクリックさせる(to S1)
			T12	｜◆Script Insertion	T15	&◆COOKIE情報窃盗スクリプトを起動(to T5)
			T13	｜◆HTTPレスポンス攻撃	T2	&◆COOKIE情報内のｾｯｼｮﾝIDを利用する
			T14	｜◆XSS	R1	■COOKIE情報

（表注）▭は攻撃タスクの具体的レビュー範囲を表す

5.7　SARM と i*-Liu 法のゴール等価性

5.7.1　ゴール関係

ゴール関係 GR を次のようにして定義する．

[定義]ゴール関係

ゴール関係 GR= <G, S, T, R, A, B, D, L> は，ゴール集合 G，ソフトゴール集合 S, タスク集合 T, リソース集合 R, アクタ集合 A, アクタ所属関係 B⊂(GUSU TUR)×A, 依存関係 D⊂A×(GUSUTUR)×A，ゴール分解関係 L⊂C×(GUSUTUR)×(GUSUTUR) からなる 8 項組である．

ここで，集合 G, S, T, R ならびに A は互いに素である．アクタ所属関係 B は，G, S, T, R の各要素がどのアクタに対応するかを示す G, S, T, R からアクタ集合 A への関係である．依存関係 D は，アクタ間に依存関係としてどのようなソフトゴール，ゴール，タスク，リソースがあるかを表しており，依存元，依存対象，依存先からなる 3 項関係である. したがって依存対象は集合 G, S, T, R の要素である．依存元と依存先は，アクタ集合 A の要素である．ゴール分解関係 L は，分解種別 C={AND,OR}，親ゴール，子ゴールからなる 3 項関係である．ここで親ゴールならびに子ゴールは G, S, T, R の要素である．

[定義] SR 図

SR 図 P には，アクタ集合 Ap，各アクタ a∈Ap についてのゴールのアクタ所属関係 B_{Ap}= {(g, a) |ゴール g∈GUSUTUR がアクタ a∈Ap に含まれる}，各アクタ a のゴール分解 La= {(c,Gparent,Gchild) |c∈C, Gparent∈GUSUTUR), Gchild∈GUSUTUR,ここで Gparent と Gchild はアクタ a∈Ap に含まれる}の集合，ゴール，ソフトゴール，タスク，リソースを依存対象とするアクタ a∈Ap と他のアクタ b∈Ap との依存関係 DAp= {(a,d,b) |a∈Ap, b∈Ap, d∈GpUSpUTpURp，ここで Gp⊂G, Sp⊂S, Tp⊂T, Rp⊂R は，それぞれ P に含まれるゴール，ソフトゴール，タスク，リソースの集合}の集合がある．

このとき，<Ap, Ua∈Ap Ga, Ua∈Ap Sa, Ua∈Ap Ta, Ua∈Ap Ra, BAp, DAp, Ua∈Ap La >を SR 図 P の表現といい，φ(P)で表す.

[命題] SR 図 P の表現 φ(P)はゴール関係である．

[証明] ゴール関係の定義から，SR 図 P の表現 φ(P) =<Ap, Ua∈Ap Ga, Ua∈Ap Sa, Ua∈Ap Ta, Ua∈Ap Ra, BAp, DAp, Ua∈Ap La >の各項がゴール関係の 8 項に対応することは明らかである．（証明終わり）

SARM 状況表 Z は{ e:階層ゴール式| e ∈SARM[X,Y], X∈A,Y∈A}で与えられる．したがってアクタ集合 A と，A の要素としてのアクタ間の階層ゴール式の集合 SARM[X,Y]が SARM 状況表 Z に含まれている．ここで，Z が含むアクタの集合 A はゴール関係の要素である．また非対角要素 SARM[X,Y](X≠Y)はアクタ間の関係 D_A={(X,d,Y) |X∈A, Y∈A, d∈GUSUTUR}を示している. 第 1 種 SARM 状況表の場合，非対角要素は階層ゴール基本式から生成される構造に限定される．つまりゴール，ソフトゴール，タスク，資源もしくは攻撃ゴール，攻撃ソフトゴール，攻撃タスク，攻撃資源だけになり深さが 2 以上の階層構造を持つことはない．一方，対角要素 SARM[X,X]で与えられる階層ゴール式はアクタ X 内部のゴールの階層構造に対応しているので深さが 2 以上の階層構造を持つことがある．

もし Z が含む階層ゴール式の集合がゴール関係を構成することが示されれば，SARM 状況表からゴール関係を導くことができる．階層ゴール式は，複数の階層ゴール式が適用されることで階層構造を生成している．そこで，階層ゴール式の

階層の深さについての帰納法を用いることにより，階層ゴール式からゴール関係を構成できることを示す．なお，以下の議論では，簡単のため攻撃ゴールなどの先頭に接頭辞として付与される脆弱性段階の扱いについては省略した．

[命題] 第 1 種 SARM 状況表からゴール関係を構成できる

[証明]

（段階 1）階層の深さが 1 のとき階層ゴール式は，前述したように，ゴール，ソフトゴール，タスク，資源もしくは攻撃ゴール，攻撃ソフトゴール，攻撃タスク，攻撃資源によって表現される．したがって，深さ 1 の階層ゴール式から$\{G_X| X \in A\}$, $\{S_X| X \in A\}$, $\{T_X| X \in A\}$, $\{R_X| X \in A\}$を構成できる．ここで，攻撃ゴール，攻撃ソフトゴール，攻撃タスク，攻撃資源をそれぞれ，ゴール，ソフトゴール，タスク，資源に含めて考えるものとする．

SARM 状況表の対角要素 SARM[X,X], X∈A についても，階層の深さが 1 であるから，ゴール，ソフトゴール，タスク，資源もしくは攻撃ゴール，攻撃ソフトゴール，攻撃タスク，攻撃資源によって表現される．このとき，各アクタ X∈A とこれらのゴール，ソフトゴール，タスク，資源のアクタ所属関係 B_A= {(g, X) |g∈G_XUS_X UT_X UR_X がアクタ X ∈A に含まれる} を構成できる．

対角要素に含まれるゴールには階層の深さが 1 であることから，親子関係を持つゴールはない．このため，SARM[X,X]の要素に対してゴール分解 L_X= {(ε, ε, G) | G∈GUSUTUR), G は SARM[X,X]に含まれる}を構成する．なお，ε 記号は，対応する AND 記号，OR 記号，親ゴールが存在しないことを表す．

また SARM 状況表の非対角要素 SARM[X,Y], X∈A, Y∈A, X≠Y)についても，階層の深さが 1 であるから，ゴール，ソフトゴール，タスク，資源によって表現される．このとき，各アクタ X, Y∈A とこれらのゴール，ソフトゴール，タスク，資源の関係から，依存関係 D_A= {(X,d,Y) |X∈A, Y∈A, d∈G_ZUS_ZUT_ZUR_Z, ここで G_Z, S_Z, T_Z, R_Z は，それぞれ Z に含まれるゴール，ソフトゴール，タスク，リソースの集合} を構成できる．

以上の議論から階層の深さが 1 のときに第 1 種 SARM 状況表{ e:階層ゴール式| e ∈SARM[X,Y], X∈A,Y∈A}からゴール関係<A, G_Z, S_Z, T_Z , R_Z, B_A, D_A , L_X>を構成できる．

（段階 2）深さ N の階層ゴール式からゴール関係<A, G_Z(N), S_Z(N), T_Z(N) , R_Z(N), B_A(N), D_A(N) , L_X(N)>を構成できるとき，深さ N+1 の階層ゴール式からゴール関係<A, G_Z(N+1), S_Z(N+1), T_Z(N+1) , R_Z(N+1), B_A(N+1), D_A(N+1) , L_X(N+1)>を構成できることを示す．ここで，第 1 種 SARM 状況表のアクタ集合 A はゴール階層と独立なので変化しない．

第 1 種 SARM 状況表では非対角要素には階層性がないので，段階 1 と同じである．したがって D_A(N+1)= D_A(N)である．

対角要素 SARM[X,X]の深さ N+1 の階層ゴール式 e は，階層ゴール式の構文規則から，①深さ N の階層ゴール式，②深さ N の積階層ゴール式並び，③深さ N の和階層ゴール式並び のいずれかに対して親ゴール t が追加される構造になっているはずである．そうでなければ深さが N+1 であることに矛盾する．

場合①については，親子関係(ε, t, g) が追加される．ここで t, g ∈GUSUTUR は SARM[X,X]に含まれる．また t は構文規則<階層ゴール基本式><改行><字下げ><階層ゴール式並び>によって追加される第 N+1 階層の親ゴールである．g は，この同じ構文規則によって親が追加される子ゴールである．このとき，深さ N の階層ゴール式に対するゴール分解 L_X(N)では親ゴールだった g に対するゴール分解(ε, ε,

g)が深さ N+1 のゴール関係のゴール分解 $L_X(N+1)$では削除され，新しい親ゴール t と g のゴール分解(ε, t, g)が追加される．この関係以外は $L_X(N)$と $L_X(N+1)$は変化しない．すなわち，t を階層分解する g に対して $L_X(N)$から(ε, ε, g)を削除し(ε, t, g)を追加することによって $L_X(N+1)$を構成できる．

場合②については，親子関係(AND, t, g) が追加される．ここで t, g ∈GUSUTUR は SARM[X,X]に含まれる．また t は構文規則<階層ゴール基本式><改行><字下げ><積階層ゴール式並び>によって追加される第 N+1 階層の親ゴールである．g は，この同じ構文規則によって親が追加される子ゴールである．このとき，深さ N の階層ゴール式に対するゴール分解 $L_X(N)$では親ゴールだった g に対するゴール分解(ε, ε, g)が深さ N+1 のゴール関係のゴール分解 $L_X(N+1)$では削除され，新しい親ゴール t と g のゴール分解(AND, t, g)が追加される．この関係以外は $L_X(N)$と $L_X(N+1)$は変化しない．すなわち，t を AND 分解する g に対して $L_X(N)$から(ε, ε, g)を削除し(OR, t, g)を追加することによって $L_X(N+1)$を構成できる．

場合③については，親子関係(OR, G_{N+1}, G_N) が追加される．ここで t, g ∈GUSUTUR は SARM[X,X]に含まれる．また t は構文規則<階層ゴール基本式><改行><字下げ><和階層ゴール式並び>によって追加される第 N+1 階層の親ゴールである. g は, この同じ構文規則によって親が追加される子ゴールである. このとき, 深さ N の階層ゴール式に対するゴール分解 $L_X(N)$では親ゴールだった g に対するゴール分解(ε, ε, g)が深さ N+1 のゴール関係のゴール分解 $L_X(N+1)$では削除され, 新しい親ゴール t と g のゴール分解(OR, t, g)が追加される．この関係以外は $L_X(N)$と $L_X(N+1)$は変化しない. すなわち, t を OR 分解する g に対して $L_X(N)$から(ε, ε, g)を削除し(OR, t, g)を追加することによって $L_X(N+1)$を構成できる．

以上の場合①②③について, N+1 階層で追加される t はゴール階層の頂点となるゴールであるから G_Zか S_Zの要素である. t が G_Zの要素であるとき, $G_Z(N+1)= G_Z(N) \cup \{t\}$, $S_Z(N+1) = S_Z(N)$, $T_Z(N+1) = T_Z(N)$, $R_Z(N+1) = R_Z(N)$. t が S_Z の要素であるとき, $G_Z(N+1)= G_Z(N)$, $S_Z(N+1) = S_Z(N) \cup \{t\}$, $T_Z(N+1) = T_Z(N)$, $R_Z(N+1) = R_Z(N)$.
また以上の場合①②③について, 第 N+1 階層の親ゴール t に対して $B_A(N)$に(t, X)を追加することで $B_A(N+1)$を構成できる．

以上から，深さ N の階層ゴール式からゴール関係<A, $G_Z(N)$, $S_Z(N)$, $T_Z(N)$, $R_Z(N)$, $B_A(N)$, $D_A(N)$, $L_X(N)$>を構成できるとき，深さ N+1 の階層ゴール式からゴール関係<A, $G_Z(N+1)$, $S_Z(N+1)$, $T_Z(N+1)$, $R_Z(N+1)$, $B_A(N+1)$, $D_A(N+1)$, $L_X(N+1)$>を構成できることが明らかになった．
したがって任意の階層の階層ゴール式で記述された第 1 種 SARM 状況表からゴール関係を構成できることが証明された．（証明終わり）

[定義]SARM 状況表のゴール表現
SARM 状況表 Z= { e:階層ゴール式| e ∈SARM[X,Y], X∈A,Y∈A}に対して構成されるゴール関係<A, $G_Z(N)$, $S_Z(N)$, $T_Z(N)$, $R_Z(N)$, $B_A(N)$, $D_A(N)$, $L_X(N)$>を Z のゴール表現 π(Z)という．

5.7.2 ゴール関係に基づく等価性について

[定義]ゴール等価

2 つのゴール関係 GR と GR’に対して，GR=GR’となるとき，すなわち，それぞれの 8 項組の各集合が一致するとき, GR と GR’はゴール等価であるという. ここで, アクタ所属関係，依存関係，ゴール分解関係は複数の集合からなる直積集合であり，やはり集合であることに注意する.

[命題]

i*-Liu 法で記述された SR 図を P，第 1 種 SARM 状況表を Z= { e:階層ゴール式| e ∈SARM[X,Y], X∈A,Y∈A}とするとき，φ(P)と π(Z)のゴール等価性を判定できる．ここで，φ(P) =<Ap, ∪a∈Ap Ga, ∪a∈Ap Sa, ∪a∈Ap Ta, ∪a∈Ap Ra, BAp, DAp, ∪a∈Ap La >

$\pi(Z) = <A, G_Z(N), S_Z(N), T_Z(N), R_Z(N), B_A(N), D_A(N), L_X(N)>$

[証明]

φ(P)と π(Z) はゴール関係であること，ならびに，ゴール関係の 8 項組が有限集合から構成されることから，ゴール等価性を判定できる．（証明終わり）

一般には，同じセキュリティ要求に対して記述された P と Z からそれぞれ作成された Q と W が必ずしも一致するとは限らない．もし同じセキュリティ要求に対して記述された P と Z から作成された Q と W がゴール等価でなければ, P と Z のいずれかに抜けや誤りがあるか，ともに抜けや誤りがあることになる．したがって Q と W が一致するように P と Z を見直すことでセキュリティ要求分析の正確性を向上できることになる．この点が，i*-Liu 法と SARM を組み合わせたスパイラルレビューの有効性の根拠である.

5.7.3 ゴール関係の例

依存関係 D は依存元，依存対象，依存先を i*-Liu 法では線で結んでいる．これは SARM では依存先を(to 要素の ID)の形式で示すことで表現可能である.

アクタ所属関係 B は各 A すなわち各アクタがその円の中にある要素を所属させている．これを SARM 状況表では各アクタに所属する i*-Liu 法の要素を各アクタの対角欄に記載することで表現できる.

ゴール分解関係 L は i*-Liu 法ではゴール，ソフトゴール，タスクの各要素とその論理関係を分解種別，親ゴール，子ゴールとして図示する．一方 SARM 状況表では&と|の分解種別を各要素に前置して論理関係を示し, 親ゴールから字下げをして子ゴールを記載することで表現可能である. 図 5-7 の i*-Liu 法に対するゴール関係＜G, S, T, R, A, D, B, L >を作成すると以下のようになる．なお互いに素である集合 G, S, T, R, A には通番を振り, 表 3 に示した第 1 種 SARM 状況表に対する i*-Liu 法の表記例を図 2 に示した. 表 3 では, 第 1 種 SARM 状況表の項目ごとに G,S,T,R,A に対応する項番をふっている．この項目は図 2 の i*-Liu 法の項目に全て一致させて記入することができる．また，i*-Liu 法からも第 1 種 SARM 状況表の項目に全て一致させて記入することができる.

G={G1:Web ページを生成する，G2:利用者情報に従って情報を提供する，G3:利用者情報を保護する，G4:利用者ごとの管理をする，G5:商品の販売をする，G6:必要な情報を入力：する}

S={ S1:ALICE に EVE のサイトをクリックさせたい，S2:ALICE になりすまして商品を手に入れたい，S3:EVE のサイトを閲覧したい，S4:色々なサイトを閲覧したい，S5:BOB のサイトを閲覧したい，S6:正当な利用者にアクセスさせる, S7:正当ではない利用者にアクセスさせない,S8:BOB のシステムで商品を注文し商品を手に入れたい}

T={T1:利用者 ALICE に EVE のサイトをクリックさせる，T2:COOKIE 情報内のセッション ID を利用する，T3:ログインをする，T4:許可された利用者に情報へのアクセスを許可する，T5:COOKIE 情報を管理する T6:ALICE になりすまして商品の注文をする}

R={R1:COOKIE 情報，R2:利用者情報，R3:認証データ}

A={A1:利用者 ALICE,A2:脆弱性のあるシステム BOB,A3:攻撃者 EVE}

アクタ間の関係を示す B,D,L の 3 種類については，紙面の都合上，B,L は EVE に関してのみ D は EVE と ALICE の関係のみを記述する．

B={(ALICE になりすまし商品を手に入れたい，攻撃者 EVE),(利用者 ALICE に EVE のサイトをクリックさせる，攻撃者 EVE),（COOKIE 情報内のセッション ID を利用する，攻撃者 EVE)，（COOKIE 情報，攻撃者 EVE）}

D={(利用者 ALICE に EVE のサイトをクリックさせる, ALICE に EVE のサイトをクリックさせたい,利用者 ALICE), (色々なサイトを閲覧したい, EVE のサイトを閲覧したい, ALICE になりすまして商品を手に入れたい),

L={(ε, ε, ALICE になりすまして商品を手に入れたい),(AND, ALICE になりすまして商品を手に入れたい,利用者 ALICE に EVE のサイトをクリックさせる),(AND,ALICE になりすまして商品を手に入れたい,COOKIE 情報内のセッション ID を利用する)， (ε,COOKIE 情報内のセッション ID を利用する, COOKIE 情報)}

ただし，ε 記号は，対応する AND 記号，OR 記号，親ゴールが存在しないことを表す．i*-Liu 法と同様に SARM 状況表からゴール関係を導出できるが紙面の都合で省略する．

この結果から，第 1 種 SARM 状況表と i*-Liu 法と互いに相互変換できることから，等価性を持つことが示された．ここでは，具体例に対して i*と第 1 種 SARM 状況表が相互に変換できることを確認しただけだが，変換ツールを作成することにより，一方の表現を他方の表現に変換することが期待できる．

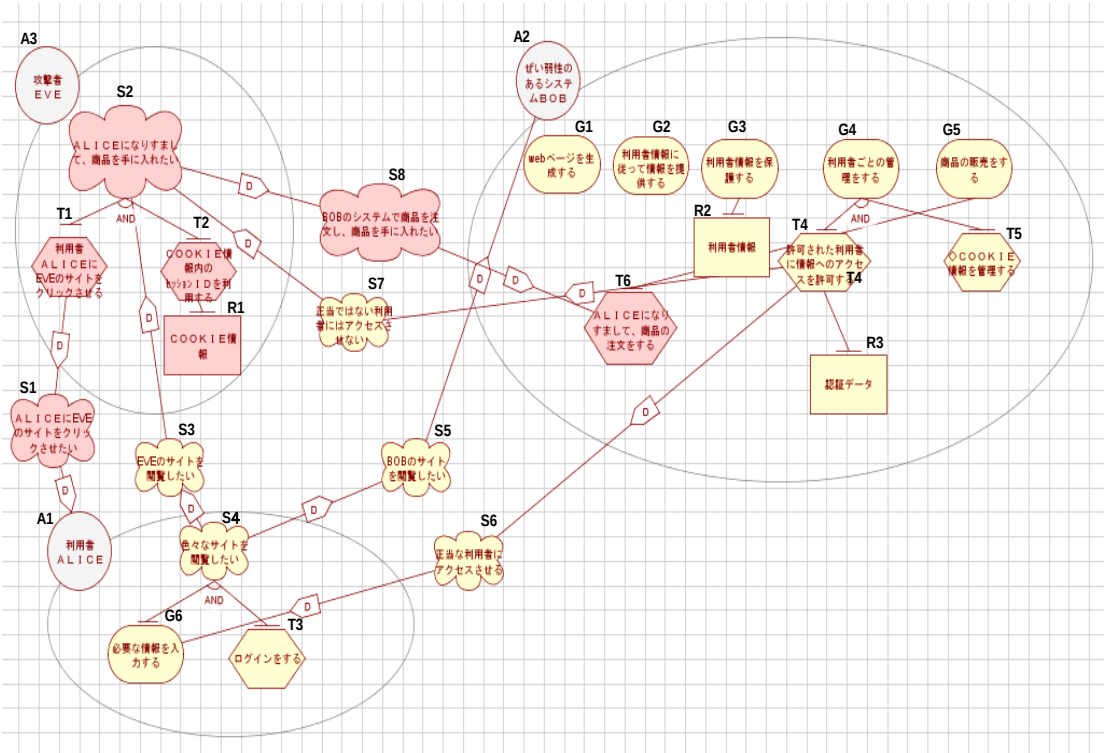


図 5-7　第 1 種 SARM 状況表の G,S,T,R,A に対応する i*-Liu 法の事例

5.8 研究仮説の評価

本研究では，SARM と i*-Liu 法に関する以下の研究仮説を評価する．

A1.SARM のほうが i*-Liu 法よりも覚えやすい．
A2.SARM のほうが i*-Liu 法よりも書きやすい．
A3.SARM のほうが i*-Liu 法よりもセキュリティ要求の網羅性が高い．
A4.SARM のほうが i*-Liu 法よりも分析しやすい．
A5.SARM のほうが i*-Liu 法よりも理解しやすい．
A6.SARM と i*-Liu 法の表現能力は等価である．
A7.SARM と i*-Liu 法を相互変換することでセキュリティ要求をスパイラルにレビューできる．
A8.SARM で詳細レビューを実施することにより，攻撃の具体的なタスク分析が可能になる．

5.8.1 評価方法

仮説 A1，A2，A3，A4，A5 については，アンケート結果に基づいて，5.8.2 ならびに 5.8.3 で評価する．すなわち，仮説 A1 から A5 については，セキュリティ専門家に対するワークショップに基づくアンケートによって評価する．仮説 A6 については，すでに 5.7.1 と 5.7.2 の議論から演繹的に得られる帰結ならびに，5.7.2 で示したように表現能力の等価性を確認するための記述実験に基づいて確認した．仮説 A7 については, 仮説 A1 から A6 までの評価結果に基づいて 5.8.4 で議論する．仮説 A8 については，5.8.5 でレビュー可能性を議論する．

5.8.2 ワークショップの開催とアンケートの実施

ワークショップを開催し，両手法の説明を行った後で，両手法を実際に作成してもらい，アンケートに回答する実験を実施した．

(1)実験の目的

SARM を i*-Liu 法と比較することにより仮説 A1 から A5 を評価する

(2)実験対象としてのセキュリティ要求

i*-Liu 法の論文に記載されている医療現場におけるセキュリティ要求を題材とする．

(3) 実験の参加者

参加者は全員で 11 人であった．このうちセキュリティ専門家が 1 名で，他は情報セキュリティ専攻大学院生が 10 名であった．またセキュリティ設計の経験者はセキュリティ専門家に加えて 2 名の大学院生がいた．

(4) 実験仮説と検証手段

前述の A1，A2，A3，A4，A5 を二項検定で検証し, A3 のセキュリティ要求の網羅性は更に抽出要素数の比較による t 検定を実施し，セキュリティ要求の内容の正しさを検証する．

(5) 実施内容

最初に i*-Liu 法と SARM の手法と作成方法の概要を説明し，i*-Liu 法作成後 SARM を作成するグループと SARM 記入後 i*-Liu 法を記入するグループに分け，実際に作図してもらった．作図するのは，医者，医療システム，患者，攻撃者をアクタとする i*-Liu 法と SARM である．記入するのは攻撃者にかかわる部分のみで他の部分はすでに記入ずみの様式を両手法とも提供し，未記入部分を埋

めてもらった．作成条件を同じにするため，手書きで記入することとした．また，後に作成した図で気づいた点があっても前の図に反映しないこととした．

(6)　計測時間

両手法併せて 20 分程度を作成時間とし，それぞれの図の作成にかかった時間を計測した．尚，最初の手法ばかりに時間がかかってしまわないように，実施すること自体の理解などの時間は計測時間にいれていない．ただし，各手法を個別に理解するのにかかった時間は各手法の所要時間にいれている．分析は 20 分程度で記入できる簡単な分析とした．

(7)　アンケート内容

アンケートでは i*-Liu 法作成にかかった時間と SARM 作成にかかった時間，両手法を比較し，覚えやすさ，書きやすさ，セキュリティ要求の網羅性，分析しやすさ，作成結果の理解しやすさの優れている方を挙げてもらった．この 5 つの評価項目は，ミスユースケースによるセキュリティ要求分析の論文[50]での手法の評価の観点を参考に設定している．

(8)　実験設計上の考慮点

実施時間は両手法とも 20 分としていたが，i*-Liu と SARM のどちらを先に実施したかにより，最初の手法で抽出した内容を 2 回目の手法のほうでもまた記載すればいいという条件の差（慣れによるバイアス）などが生じる．そこで，i*-Liu を適用してから SARM を適用する第一グループと，SARM を適用してから i*-Liu を適用する第二グループにまず大学院生 4 名ずつを割り当てた．つぎに，セキュリティ設計経験のある 2 名の大学院生を第一グループに，そしてセキュリティ専門家を第二グループに割り当てることにした．このようにして 2 つのグループを構成することにより，できるだけ手法の適用順序の差が実験結果に影響しないように配慮した．

(9)　アンケートの実施結果

ワークショップで実施したアンケートの結果を表 5-8 にまとめる．表 5-8 の二項検定の数字欄の値は優れていると回答した回答者数とそのパーセントである．

表 5-8　アンケート結果

		i*-Liu 法	SARM	不明	検定値	
二項検定	A1.覚えやすい方はどちらか？	1(9%)	9(82%)	1(9%)	0.0107	5%　有意
	A2.書きやすい方はどちらか？	3(27%)	7(64%)	1(9%)	0.1719	結論を保留
	A3.セキュリティ要求の網羅性が高い方はどちらか？	1(9%)	6(55%)	4(36%)	0.0625	結論を保留
	A4.分析しやすい方はどちらか？	1(9%)	9(82%)	1(9%)	0.0107	5%有意
	A5.作成結果をみて，理解しやすい方はどちらか？	2(18%)	8(73%)	1(9%)	0.0547	結論を保留
t 検定	A3.セキュリティ要求の網羅性が高い方はどちらか？	要素数 43	要素数 87	-	0.0315	5%有意

5.8.3 アンケートに基づく仮説の検証

アンケートで質問した結果をみると, A1.覚えやすさ A2.書きやすさ A3.セキュリティ要求網羅性の高さ A4.分析しやすさ A5.作成結果をみて理解のしやすさの 5 つの観点から i*-Liu 法より SARM の評価の方が全項目で高い.

表 5 で示したように SARM と i*-Liu 法のどちらが支持されたかを二項分布で検定したところ，有意水準 0.05 で，両者に差がないという帰無仮説は，A1 と A4 については共に 0.0107 で棄却される．よって A1 と A4 では SARM は i*-Liu 法より支持されたといえる．しかし A2，A3，A5 では，有意水準 0.05 では両者に差がないという帰無仮説は棄却される結果となったため，結論を保留する必要がある.

二項検定で結論を保留した評価項目のうち，③セキュリティ要求の網羅性は SARM の特徴であるので，参加者に記述してもらった要素数で，網羅性を更に評価する．正しく抽出されたセキュリティ要求の要素数を比較すると SARM の要素数合計は 87，i*-Liu 法の要素数合計は 43 である．t 検定（等分散を仮定した 2 標本による検定）で有意差があるかを検定すると，SARM と i*-Liu 法の抽出要素数に差がないという仮定は 0.0315 で棄却される. よって SARM の抽出要素数は i*-Liu 法よりも多く，セキュリティ要求の網羅性が高いは SARM であるといえる.

なお，A3 の回答で不明が多い理由は，両手法の図作成時間が合わせて 20 分と短く，網羅性の検証まではできていなかったと被験者が感じているためと考えられる．SARM には①攻撃パターン単位で攻撃者を加えるという攻撃パターン網羅性と，②他のアクタとの関係で場合を尽くす関係網羅性がある．現在の実験では，その一部しか評価の対象にしておらず，また，抽出した要素の内容妥当性をきちんと議論できる程正確なものでもない．したがって，網羅性については今後，それら 2 種の網羅性それぞれについて，要素条件の抽出数，抽出要素種別，抽出した要素内容の妥当性などをきちんと定義した上で再評価する必要がある.

5.8.4 スパイラルレビューの仮説検証と初期評価

仮説 A7 については，仮説 A1 から A6 までの評価結果と 5.7.2 ゴール関係に基づく等価性の証明で Q と W が一致するように P と Z を見直すことでセキュリティ要求分析の正確性を向上できることから，i*-Liu 法と第 1 種 SARM 状況表を組み合わせたスパイラルレビューの有効性を確認した.

さらに提案したスパイラルレビューの初期評価として各手順を以下で吟味する.

①一般の各アクタ間の要求分析を一般のシステム開発者が担当し，脅威分析とセキュリティ機能分析は専門家が別途実施する方式に分けることにより，一定の様式上で通常機能と攻撃を分析できる現実的な手順としている.

②AA 表を作成することによって，STRIDE 単位で各種攻撃のパターンと守るべき資源（アセット）との組み合わせを網羅することができる．これにより，よりセキュアなシステムを実現する.

③i*-Liu 法は多人数でディスカッションしながら，要求分析をするときにわかりやすく，使いやすい．そこで，要求分析の初期段階で通常のシステム開発者とセキュリティ専門家同士が相互理解を図り，ディスカッションツールとして，使用することで特長を生かせると考える.

④i*-Liu 法の図を第 1 種 SARM 状況表に変換し，レビューすることにより，セキュリティ要求分析の網羅性を向上させる. SARM 状況表は個人での要求分析や 1 つのノードの内部構造を詳細化する要求分析のときには，欄ごとに内容を詰める

ことが容易である．i*のように各種の図の中にテキストを記入し，関連性を線で結ぶのではなく，SARM 状況表はテキストにマークを前置するだけで内容を示すので，要素に分解したときの結果を簡潔に作成できる．また，表形式は設計に落としやすいので，議論して作った i*-Liu 法の SR 図を更に細かく分析していくことに適している．i*-Liu 法の図を第 1 種 SARM 状況表に変換するのは，二度手間にはなるが，表 5-8 のアンケート結果では，82%の人が SARM の方が覚えやすいとしており，i*を習得している人ならば，SARM を理解するのは簡単な作業であると考えられる．更に 64%の人が SARM の方が書きやすいとしているので，SARM を書くこと自体は簡単にできる．また，ツールを用いた変換を支援することも考えられる．

5.8.5 詳細レビューの仮説検証

仮説 A8 については，5.6 節で示した第 2 種 SARM 状況表による詳細レビューの実施により，具体的なタスク分析ができることを確認した．アクタ間のセキュリティ要求分析において，攻撃者の具体的なタスクを分析することは，対策立案につながる作業であるため，重要である．

5.8.6 SARM における研究の限界

本論文で小規模なアンケートに基づいて評価しているが，限定されたアンケート評価では仮説検証の一般性に限界がある．また，分析といっても一人による単独分析と複数人による共同分析では，分析のしやすさに差がある． i*-Liu 法では明示的に図で対象が表示されるので，複数人が図を見て議論を進めながら分析するのに適していると考えられる. 一方 SARM は①AA 表を作成することによって，STRIDE 単位で各種攻撃のパターンを網羅している②表として欄を埋めていくので，アクタ間の完全性が向上するという点で網羅性に優れている．アクタ数が多いときや一人で深く分析するときは，欄ごとにつめていけるので SARM には分析しやすいという特長もある．双方の長所をいかすためにスパイラルレビューを提案した．ただし，SARM は位置情報で関係性を示すために，間接攻撃など 2 者間の関係を，要素 ID を付ける形式で表現しているが，視覚的なわかりやすさに欠けるという問題点もあり，今後の改善への課題を残している．

5.8.7 SARM の効果

SARM の効果には，スパイラルレビューを可能にした点と，アクタ関係に対する詳細レビューを実施できる点の 2 つがある．スパイラルレビューが適切な理由は i*-Liu 法と SARM で共通する要素について，視点を変えて確認できることである．次に SARM による詳細レビューが効果的な理由は現状の i*-Liu 法では詳細に記述できないアクタ関係を第 2 種 SARM 状況表でレビューできることである．詳細レビューにより，具体的な攻撃タスクの抽出が可能となり，攻撃に対する対策の立案という次の段階にすすむことができる．

6　ケーススタディ

6.1　具体モデルでの適用事例

CC-Case は具体モデルで実際のケースを記述する. 具体的な例示に関しては, IPA (独立行政法人　情報処理推進機構)の ST 事例[45]に対し, CC-Case をもとに記述した．本章ではセキュリティ仕様のアシュアランスケースの具体モデルを全て記載し，事例全体をアシュアランスケースで書くことが出来ることを示す.

図 6-2-1 から図 6-4-5 は全て論理モデルの最下位ゴールをトップゴールとして作成した具体的な事例である．証跡は ST として作成が必要な具体的な根拠やその前段階として必要な事項である.

以下の CC-Case の具体例の中には赤文字や緑文字で記述された証跡や前提条件がある．この赤文字や緑文字は具体的な内容を巻末の付録 A か B に示している.

付録 A において緑文字はそれに続く黒文字までが緑文字の内容を示し，次に出現する緑文字は別な事項である．緑文字は ST として記載が不要な事項であり，付録 A に具体例を示している.

付録 B において赤文字はそれに続く青文字までが赤文字の内容を示し，次に出現する赤文字は別な事項である．赤文字は ST として記述方法に一定の基準がある事項であり，付録 B に具体例を示している.

6.2　セキュリティコンセプト定義段階のアシュアランスケースの具体モデル

セキュリティコンセプト定義段階のアシュアランスケースの具体モデルを図 6-2 ①から③に挙げている．セキュリティコンセプト定義段階は ST を作成する前段階としてセキュリティコンセプトを決定している段階である．そこで ST に求められるような必要な要素を網羅するための書き方の基準を本段階の証跡には特に求めない.

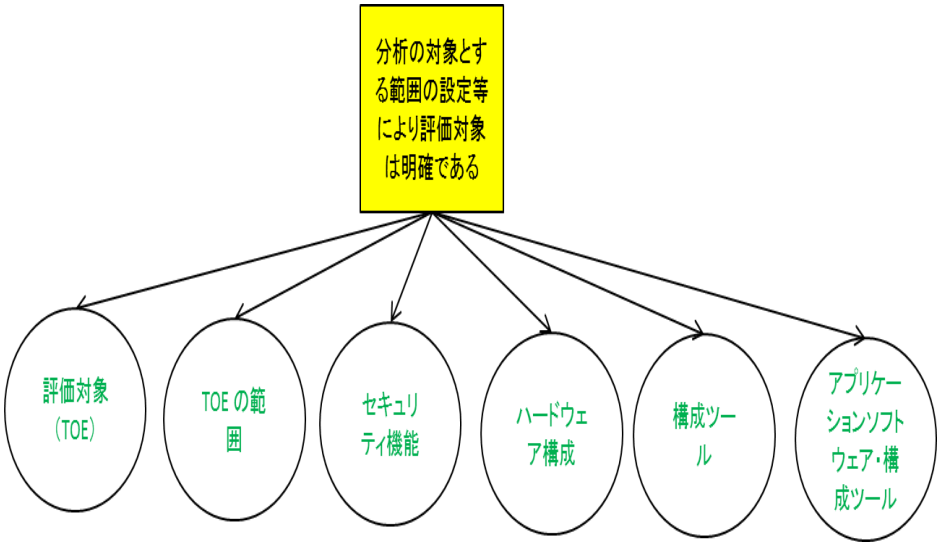


図 6-2-1　評価対象（TOE）

図 6-2-1 は図 4-2-1-1 セキュリティコンセプト定義段階における「分析の対象とする範囲の設定等により評価対象は明確である」を事例化した具体モデルである. セキュリティコンセプトを示す上で必要な証跡とその論理関係が示されている.

このゴールの証跡を付録 A の具体例に示している. 事例としては評価対象(TOE), TOE の範囲，セキュリティ機能，ハードウェア構成，構成ツール，アプリケーションソフトウェア・構成ツールを挙げている．しかしこのゴールとして必要なことはセキュリティコンセプトとして評価対象を何であるのかを明確化することであり，証跡の構成は前述の要素に固定されるものではない.

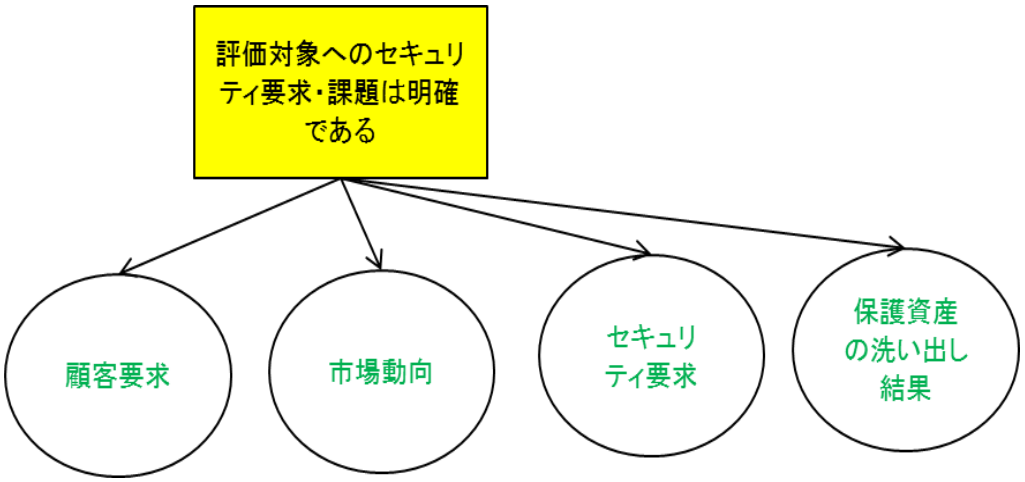


図 6-2-2　セキュリティ要求・課題

図 6-2-2 は図 4-2-1-1 セキュリティコンセプト定義段階における「評価対象へのセキュリティ要求・課題は明確である」を事例化した具体モデルである．セキュリティコンセプトを示す上で必要な証跡とその論理関係が示されている．このゴールの証跡を付録 A の具体例に示している．事例としては顧客要求・市場動向. セキュリティ要求，保護資産の洗い出し結果を挙げている．しかしこのゴールとして必要なことはセキュリティコンセプトとして評価対象に対してどのような要求・課題があるのかを明確化するを特定することであり，証跡の構成は前述の要素に固定されるものではない.

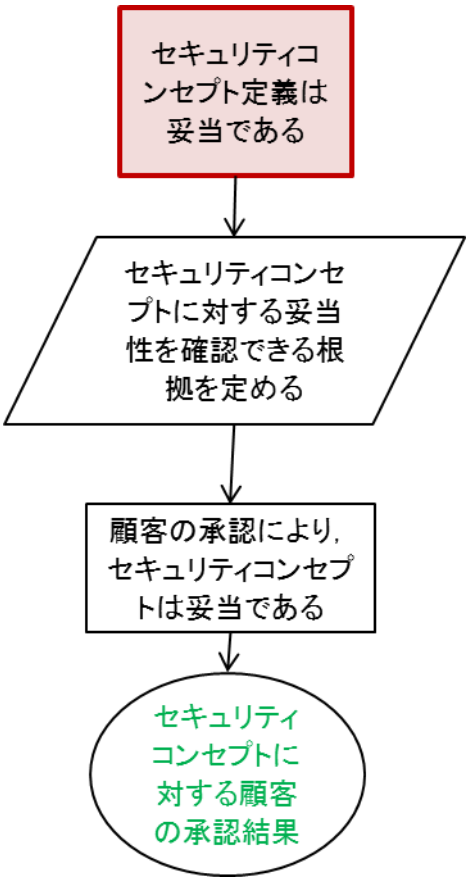


図 6-2-3　セキュリティコンセプト定義

図 6-2-3 は図 4-2-1-1 セキュリティコンセプト定義段階における「セキュリティコンセプト定義は妥当である」を事例化した具体モデルである．セキュリティコンセプトを示す上で必要な証跡とその論理関係が示されている．開発者からみて特定顧客のいる事例であるため，「顧客の承認により，セキュリティコンセプトは妥当である」をサブゴールにしているが，製品など特定の顧客がいない場合は，要件を決めるうえでの関係者の承認になるであろう．このゴールの証跡を付録 A の具体例に示している．事例としてはセキュリティコンセプトに対する顧客の承認結果として，議事録と顧客承認印を挙げている．しかしこのゴールとして必要なことはセキュリティコンセプト定義に対する顧客の承認を得ることであり，証跡の構成は前述の要素に固定されるものではない．

6.3　セキュリティ対策立案段階段階のアシュアランスケースの具体モデル

セキュリティ対策立案段階段階のアシュアランスケースの具体モデルを図 6-3-1 から 15 に挙げている．セキュリティ対策立案段階段階 ST の 1.ST 概説，2.適合主張,3.セキュリティ課題定義, 4.セキュリティ対策方針までを作成する段階である．ST として必要な要素を網羅するために証跡に持つべき基準は事例ごとに示す．

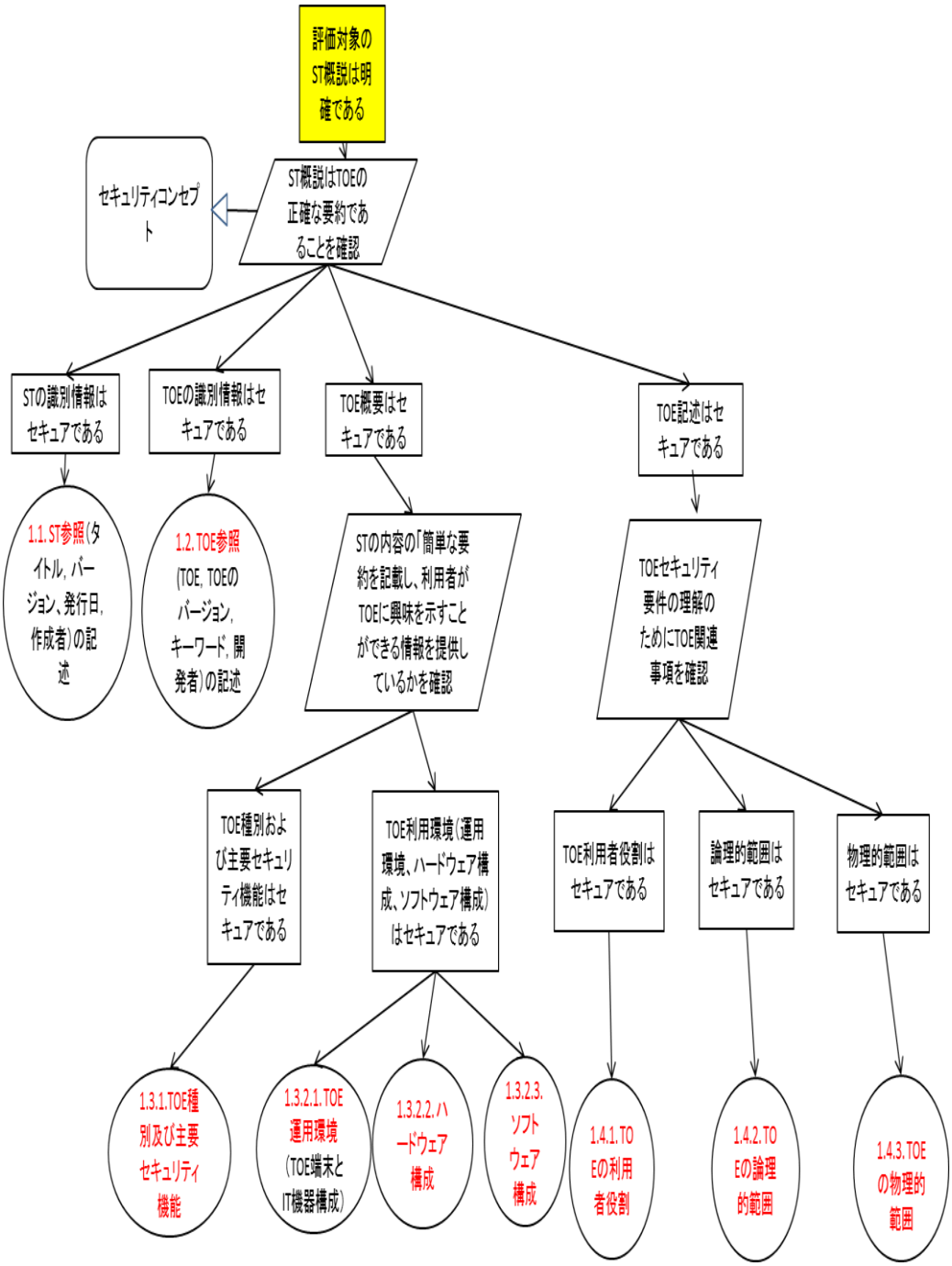


図 6-3-1　ST 概説

図 6-3-1 は図 4-2-2 セキュリティ対策立案段階における「評価対象の ST 概説は明確である」を事例化した具体モデルである．このゴールの証跡を付録 B の具体例に示している．

図 6-3-1 の証跡となる ST 項目の概要を以下に説明する．

1.1. ST 参照：ST の識別情報
例：タイトル，バージョン，作成者，発行日

1.2. TOE 参照：TOE の識別情報
例：開発者名，TOE 名称，TOE バージョン番号

1.3. TOE 概要
利用者に TOE が興味あるものであるか否かの判断(セキュリティに対する要求，サポートされるハードウェア/ソフトウェア/ファームウェアなど)に必要な情報を与える． TOE の利用(usage)と主なセキュリティ機能(major security features)，TOE 種別(type)，TOE が必要とする主な非 TOE のハードウェア/ソフトウェア/ファームウェアを数段落程度で記述する．
事例では 1.3.1.TOE 種別及び主要セキュリティ機能，1.3.2.1. TOE 運用環境，1.3.2.2. ハードウェア構成，1.3.2.3. ソフトウェア構成を含んでいる．

1.4. TOE 記述
TOE の機能とセキュリティ機能の詳細を数ページで記述する
TOE の物理的，論理的な範囲を明確に記述する．
事例では 1.4.1. TOE の利用者役割，1.4.2. TOE の論理的範囲，1.4.3. TOE の物理的範囲を含んでいる．
このゴールとして必要なことは評価対象の正確なセキュリティ特性を ST 概説として規定することであり，証跡の構成は前述の要素に固定されるものではない．

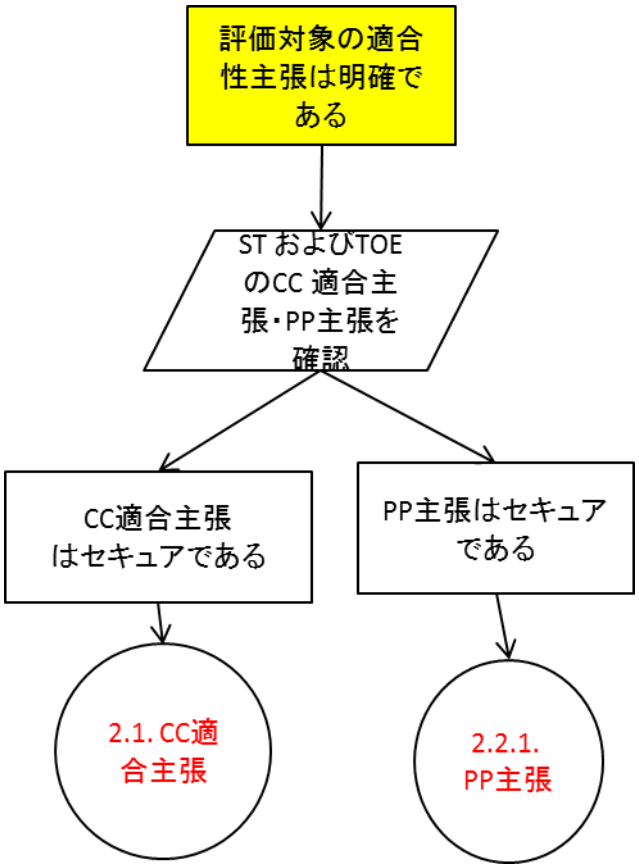


図 6-3-2　適合主張

図 6-3-2 は図 4-2-2 セキュリティ対策立案段階における「評価対象の適合性主張は明確である」を事例化した具体モデルである．このゴールの証跡を付録 B の具体例に示している．

図 6-3-2 の証跡となる ST 項目の概要を以下に説明する.

2. 適合性主張(Conformance claims)

2.1. CC 適合性主張：CC バージョン，拡張コンポーネント使用の有無

2.2.1 PP 主張：適合を主張する PP の一覧

このゴールとして必要なことは評価対象の適合性主張を規定することであり，証跡の構成は前述の要素に固定されるものではない.

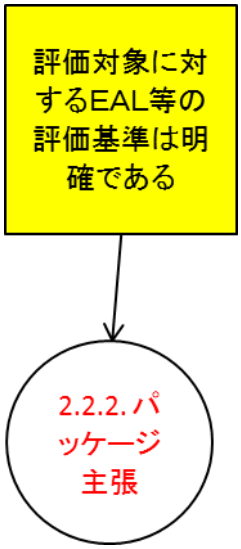


図 6-3-3 評価基準明確化

図 6-3-3 は図 4-2-2 セキュリティ対策立案段階における「評価対象に対する EAL 等の評価基準は明確である」を事例化した具体モデルである．このゴールの証跡を付録 B の具体例に示している.

図 6-3-3 の証跡となる ST 項目の概要を以下に説明する.

2.2.2 パッケージ主張：適合を主張する，EAL などで既定義のパッケージの一覧

このゴールとして必要なことは評価対象の評価基準を明確化することであり，証跡の構成は前述の要素に固定されるものではない.

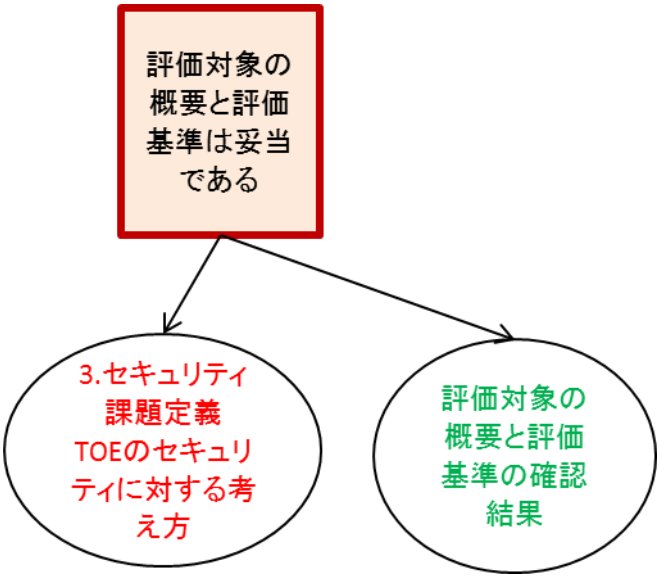


図 6-3-4 評価対象の概要と評価基準の妥当性確認

図 6-3-4 は，図 4-2-2 セキュリティ対策立案段階における「評価対象の概要と評価基準は妥当である」を事例化した具体モデルである．このゴールの証跡を付録 B と付録 B の具体例に示している．

図 6-3-4 の証跡となる ST 項目の概要を以下に説明する．評価対象の概要と評価基準として，3.セキュリティ課題定義の TOE のセキュリティに対する考え方と，この評価対象の概要と評価基準に対しての確認結果を証跡としている．

このゴールとして必要なことは評価対象の概要と評価基準への妥当性に対する顧客の承認を得ることであり，証跡の構成は前述の要素に固定されるものではない．

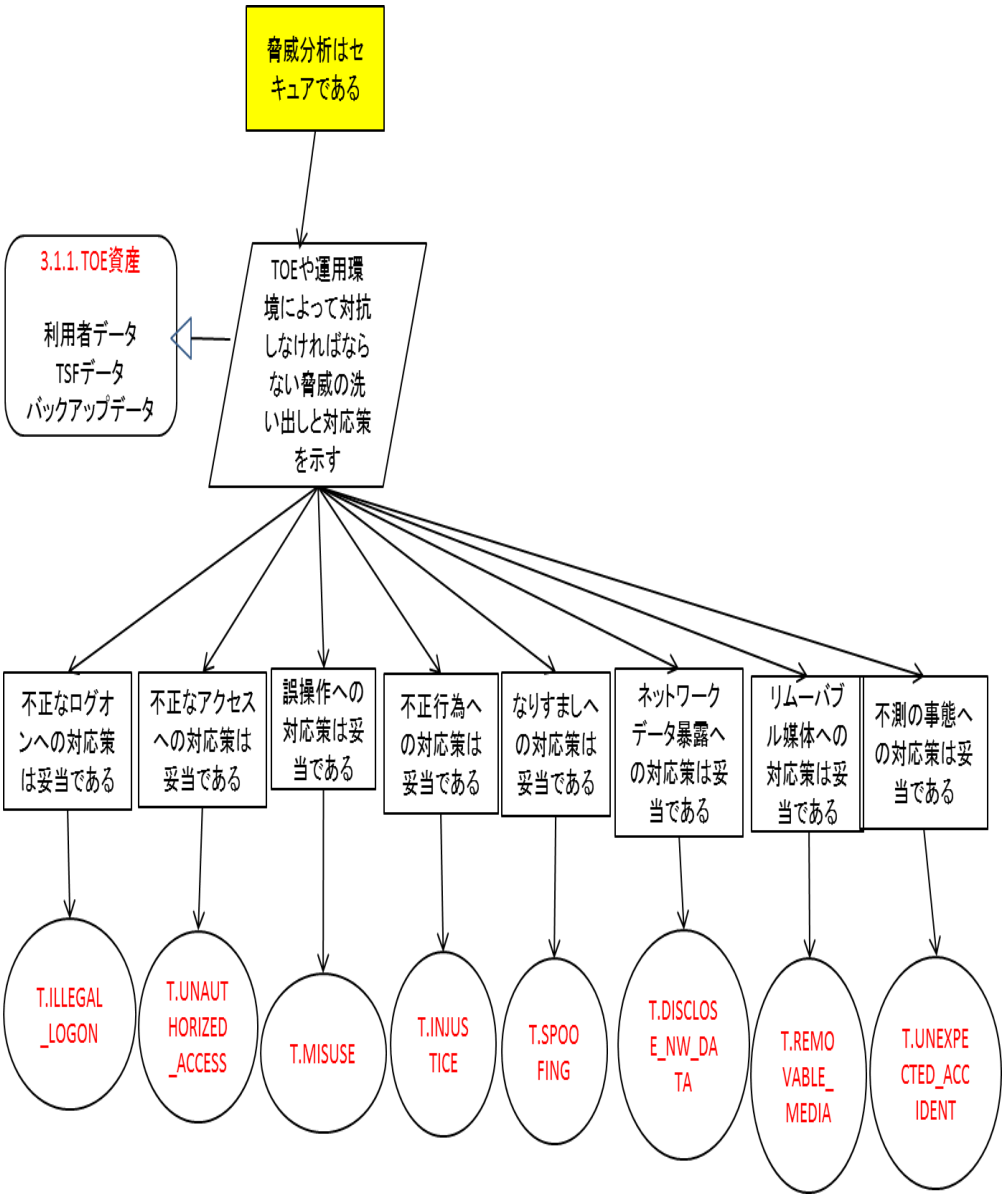


図 6-3-5　脅威分析

図 6-3-5 脅威分析は，図 4-2-2 セキュリティ対策立案段階における「脅威分析はセキュアである」を事例化した具体モデルである．このゴールの証跡を付録 B の具体例に示している．

保護対象資産は利用者データ, TSF データ, バックアップデータが相当し,「TOE や運用環境によって対抗しなければならない脅威の洗い出しと対応策を示す」と不正なログオン，不正なアクセス，誤操作，不正行為，なりすまし，ネットワークデータ暴露，リムーバブル媒体，不測の事態への各対応策が妥当であることを検証し，記述ができることを示される．保護資産とセキュリティ機能をもとに AA 表，および SARM 状況表で各脅威の抽出が可能である．各々の検証結果は T.ILLEGAL_LOGON，T.UNAUTHORIZED_ACCESS 等の脅威分析の証跡として示される．図 6-3-5 は CC パート 1 の附属書 A.6.2 脅威の記載事例に相当し，ST の仕様に則った証跡の検証手段を含んでいる．

図 6-3-5 の証跡となる ST 項目の概要を以下に説明する．

3.1. 脅威：脅威エージェント，資産，および有害なアクション．各項目を接頭辞“T.”の付いた名前で表す．

例：T.ACCESS (アクセス権のない利用者が資源へのアクセスや操作を実行)

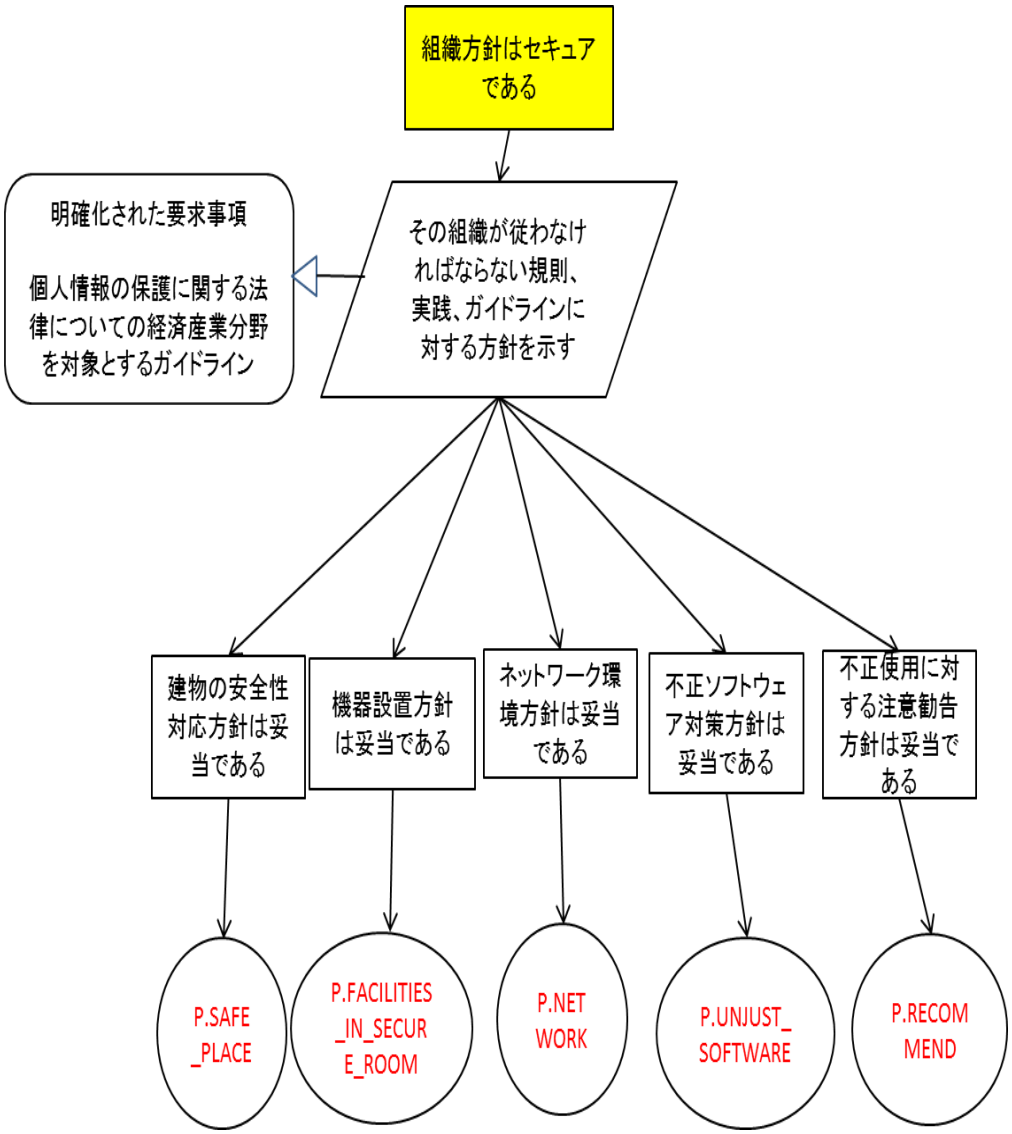


図 6-3-6　組織方針

図 6-3-6 組織方針は，図 4-2-2 セキュリティ対策立案段階における「組織方針はセキュアである」を事例化した具体モデルである．このゴールの証跡を付録 B の具体例に示している．

図 6-3-6 の証跡となる ST 項目の概要を以下に説明する．

3.2. 組織のセキュリティ方針(Organisational security policies，OSPs)

TOE，その運用環境，またはその組合せによって実施する必要がある規則，慣行，またはガイドライン．各項目を接頭辞“P.”の付いた名前で表す．

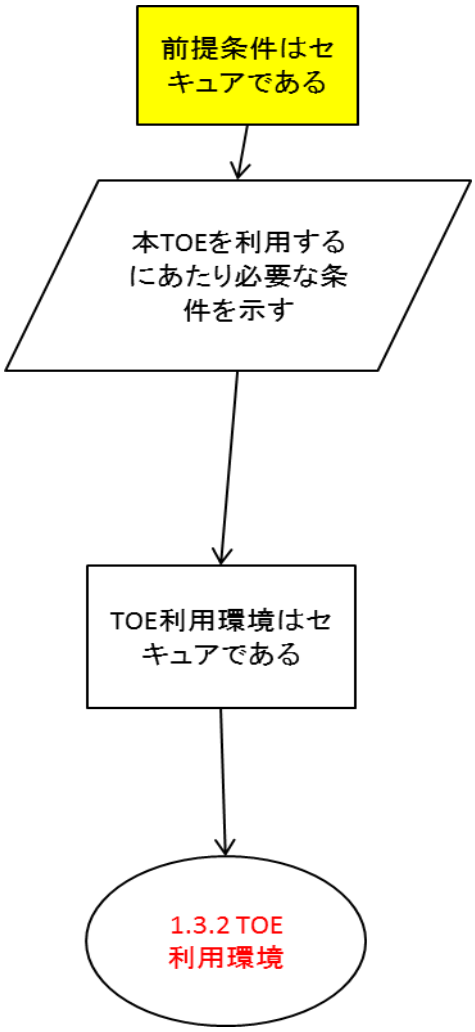


図 6-3-7　前提方針

図 6-3-7 前提方針は，図 4-2-2 セキュリティ対策立案段階における「前提方針はセキュアである」を事例化した具体モデルである．このゴールの証跡を付録 B の具体例に示している．

図 6-3-7 の証跡となる ST 項目の概要を以下に説明する．

3.3. 前提条件

セキュリティ機能の提供のために運用環境に設定される条件

各項目を接頭辞“A.”の付いた名前で表す.

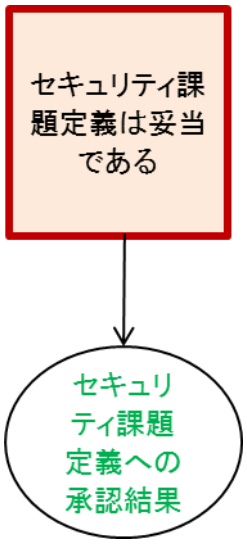


図 6-3-8　セキュリティ課題定義

図 6-3-8 は図 4-2-2 セキュリティ対策立案段階における「セキュリティ課題定義は妥当である」を事例化した具体モデルである．このゴールの証跡を付録 A の具体例に示している．

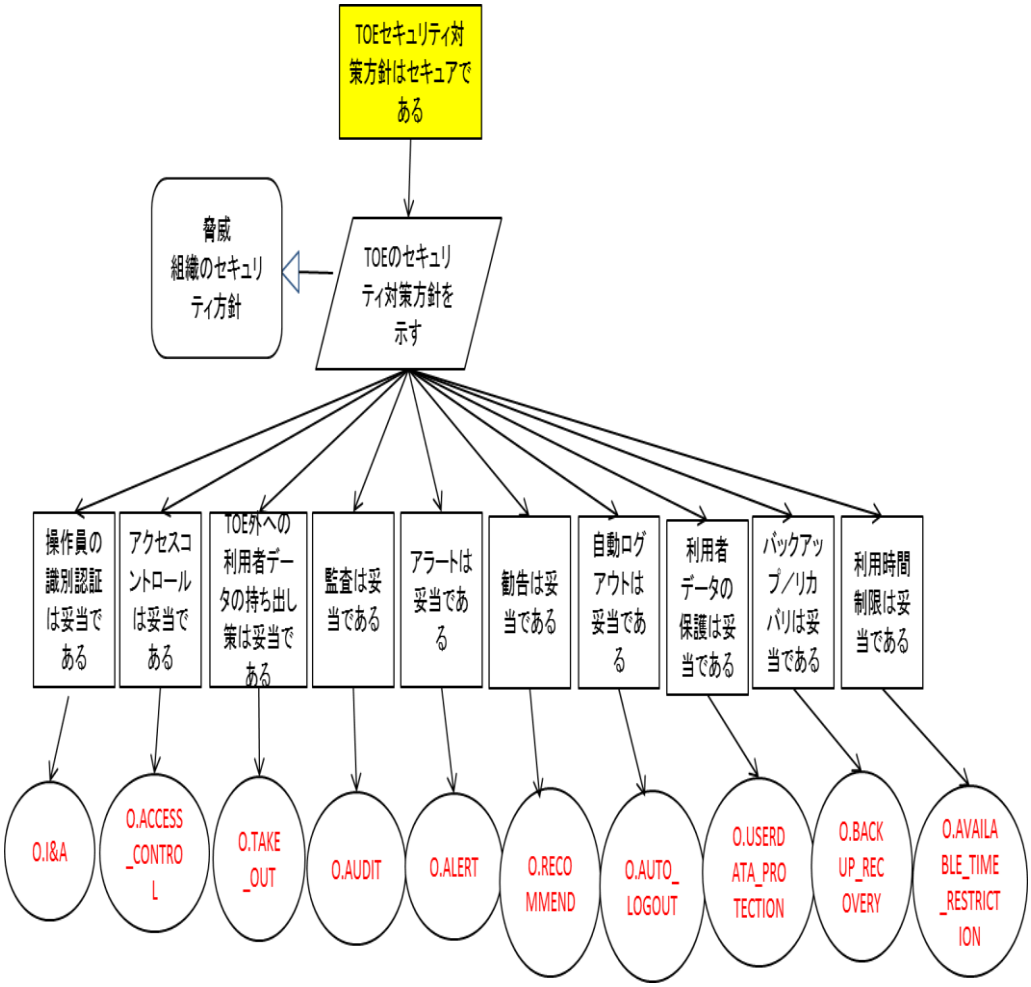


図 6-3-9 TOE セキュリティ対策方針

図 6-3-9 は図 4-2-2 セキュリティ対策立案段階における「TOE セキュリティ対策方針はセキュアである」を事例化した具体モデルである．このゴールの証跡を付録 B の具体例に示している．

脅威の対応策や組織方針に対して TOE が実現すべき対策を示している．図 6-3⑨は CC パート 1 の附属書 A.7.2.1TOE のセキュリティ対策方針の記載事例に相当し，ST の仕様に則った証跡の検証手段を含んでいる．図 6-3⑨は TOE が技術的に対応すべき対策である．

2.2.5 節の文献[6] [41] [42]で示したようにセキュリティケースには共通性があるにも関わらず，プロセスが明確になっていない．このため個別に作成されたセキュリティケースでは品質のバラツキや作成効率が低いという実用性の問題がある．それに対して CC-Case は論理モデルとして共通性を明確化するとともに，具体モデルを追加することで自然にセキュリティケースを作成できる実用性があり，その結果を証跡として残せる長所ももつ．

図 6-3-9 の証跡となる ST 項目の概要を以下に説明する．

4. セキュリティ対策方針(Security objectives)

セキュリティ課題に対する，抽象度の高い解決策を，過度の詳細を省いた，簡明かつ明確な文章で記述．各項目を接頭辞“O.”の付いた名前で表す

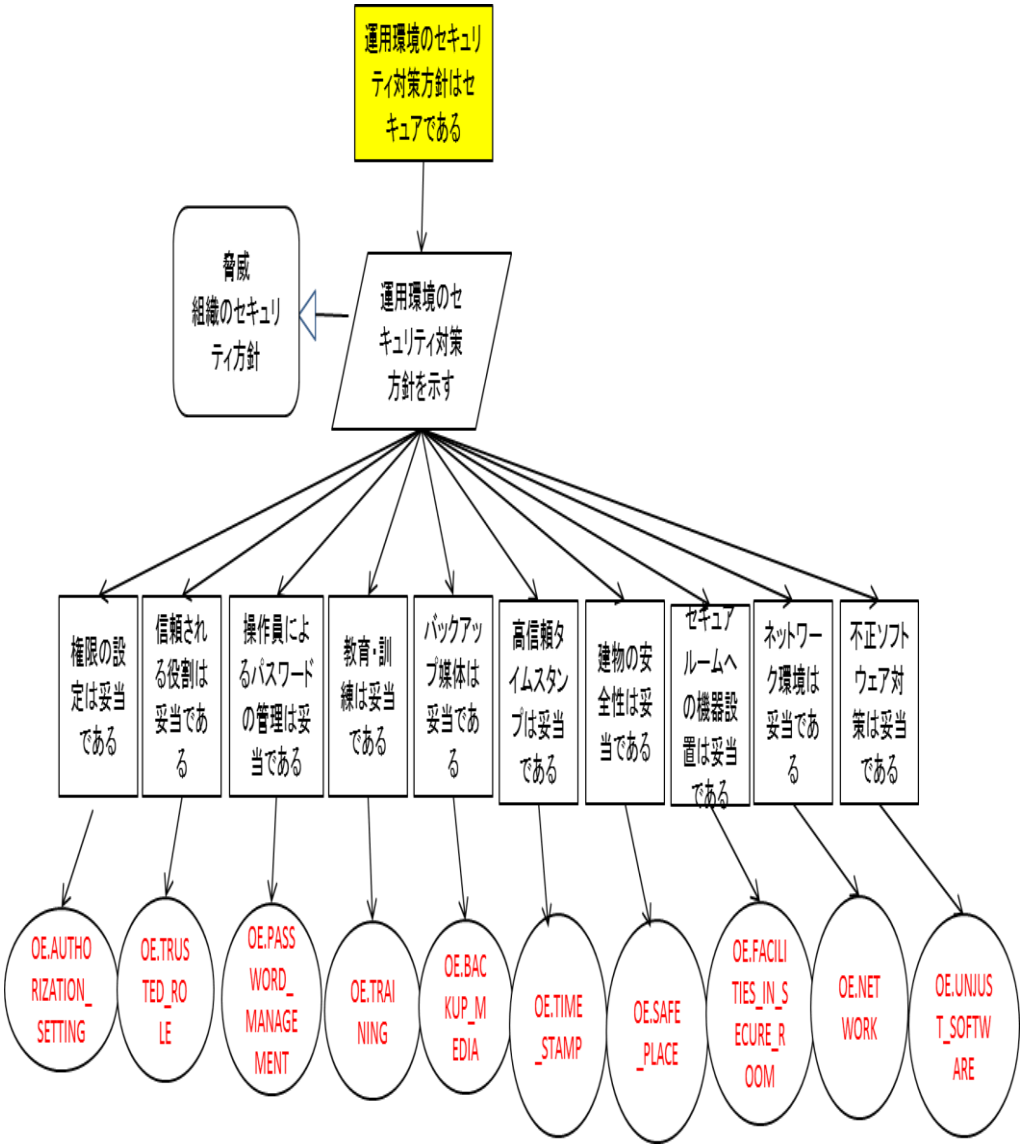


図 6-3-10　運用環境のセキュリティ対策方針

図 6-3-10 は図 4-2-2 セキュリティ対策立案段階における「運用環境のセキュリティ対策方針はセキュアである」を事例化した具体モデルである．このゴールの証跡を付録 B の具体例に示している．

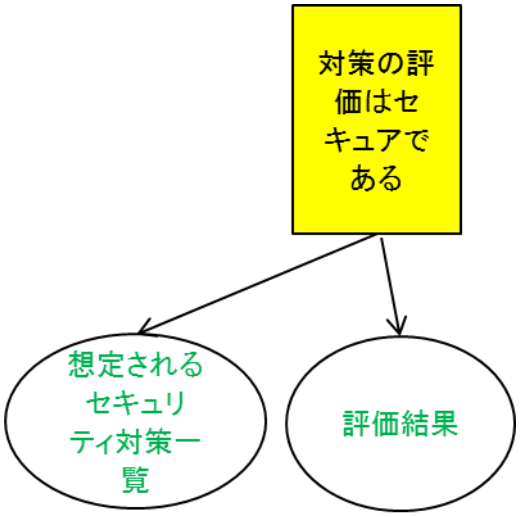


図 6-3-11　対策の評価

図 6-3-11 は図 4-2-2 セキュリティ対策立案段階における「対策の評価はセキュアである」を事例化した具体モデルである．このゴールの証跡を付録 A の具体例に示している．

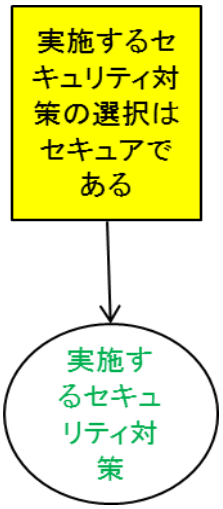


図 6-3⑫　対策の選択

図 6-3-12 は図 4-2-2 セキュリティ対策立案段階における「実施する対策の選択はセキュアである」を事例化した具体モデルである．このゴールの証跡を付録 A の具体例に示している．

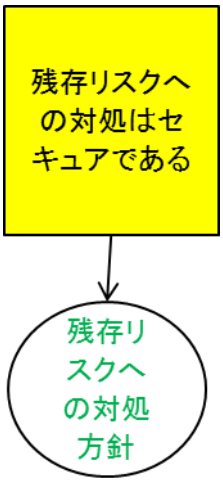


図 6-3-13　残存リスクへの対処

図 6-3-13 は図 4-2-2 セキュリティ対策立案段階における「残存リスクへの対処はセキュアである」を事例化した具体モデルである．このゴールの証跡を付録 A の具体例に示している．

図 6-3-14　セキュリティ対策方針根拠

図 6-3-14 は図 4-2-2 セキュリティ対策立案段階における「セキュリティ対策方針根拠はセキュアである」を事例化した具体モデルである．このゴールの証跡を付録 B の具体例に示している．

図 6-3-14 の証跡となる ST 項目の概要を以下に説明する．

4.3. セキュリティ対策方針根拠：セキュリティ課題との対応.

(tracing)とその根拠．対応は通常表で記述.

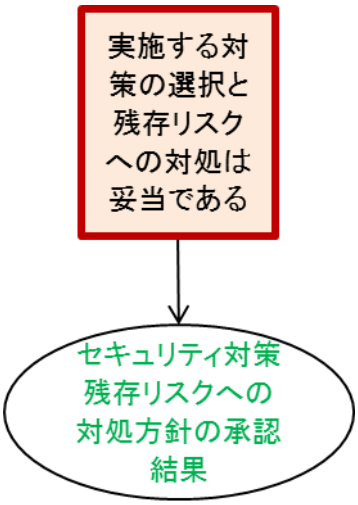


図 6-3-15　セキュリティ対策方針根拠

図 6-3-15 は図 4-2-2 セキュリティ対策立案段階における「実施する対策の選択と残存リスクへの対処は妥当である」を事例化した具体モデルである．このゴールの証跡を付録 A の具体例に示している．

6.4　セキュリティ要約仕様化段階のアシュアランスケースの具体モデル

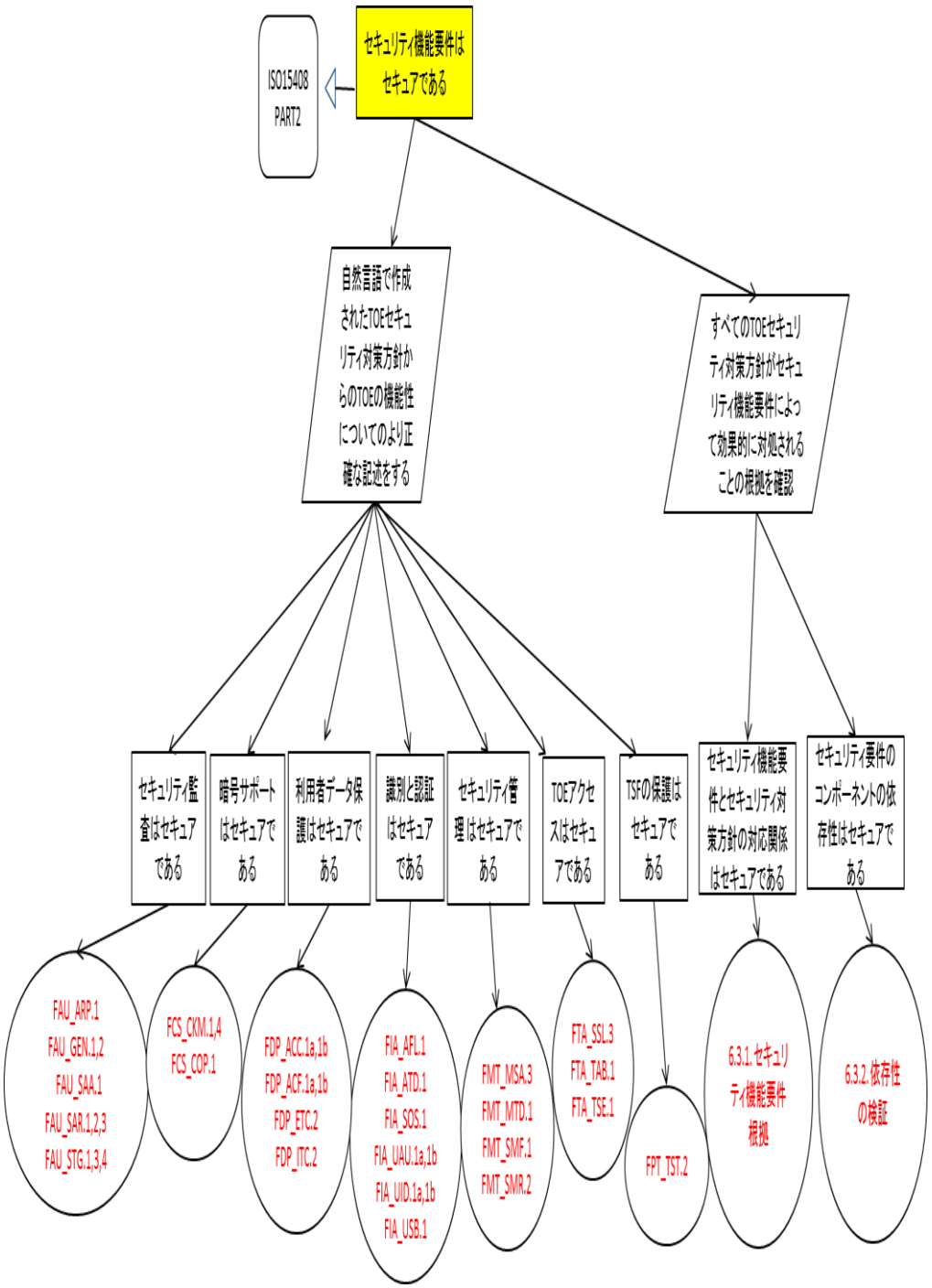


図 6-4-1　セキュリティ機能要件

図 6-4-1 は図 4-2-3 セキュリティ要約仕様化段階における「セキュリティ機能要件はセキュアである」を事例化した具体モデルである．このゴールの証跡を付録 B の具体例に示している．

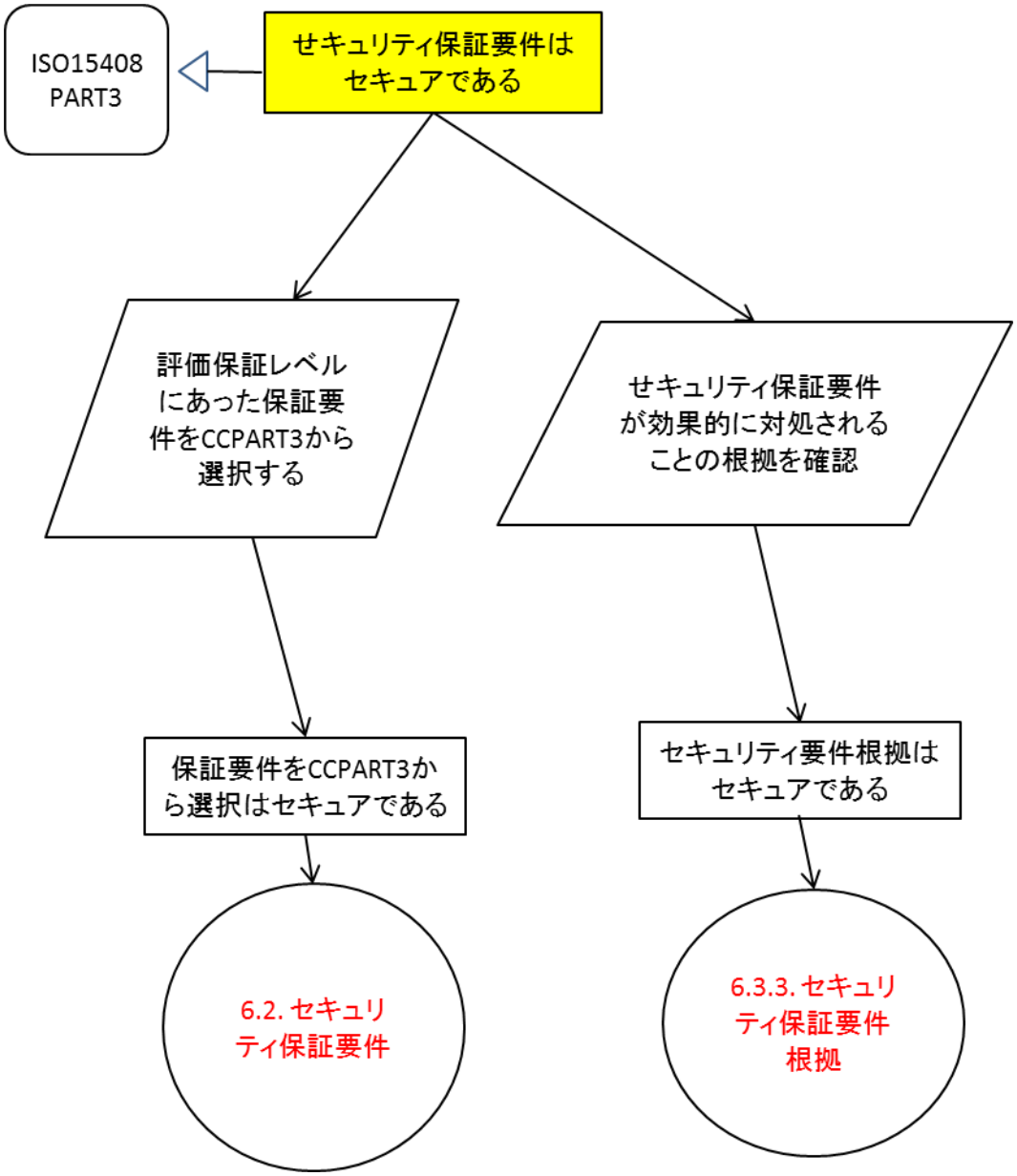


図 6-4-2　セキュリティ保証要件

図 6-4-2 は図 4-2-3 セキュリティ要約仕様化段階における「セキュリティ保証要件はセキュアである」を事例化した具体モデルである．このゴールの証跡を付録 B の具体例に示している．

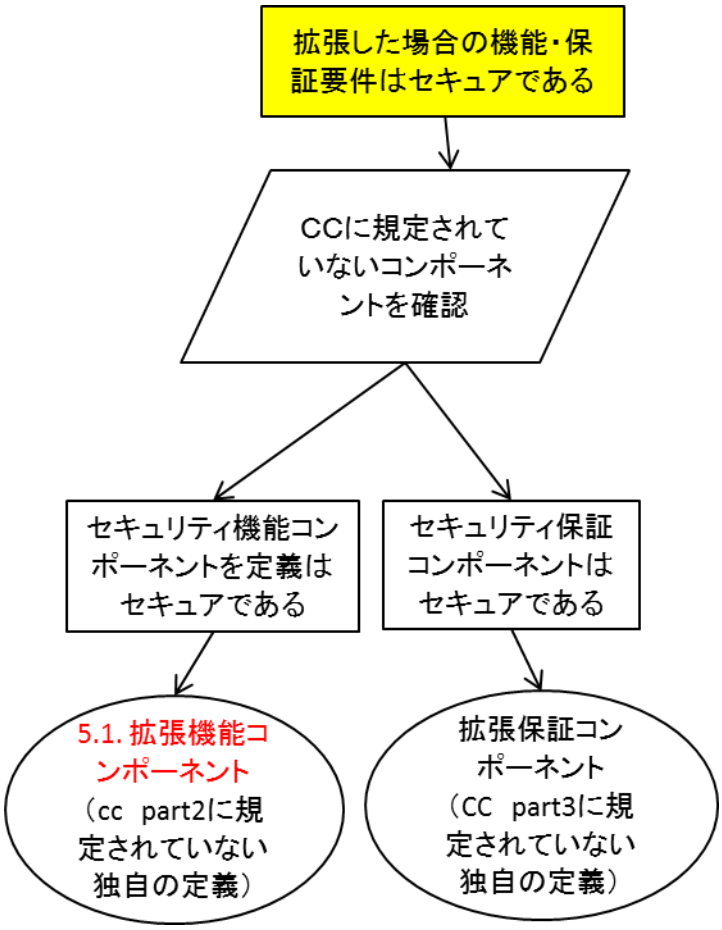


図 6-4-3　拡張コンポーネント定義

図 6-4-3 は図 4-2-3 セキュリティ要約仕様化段階における「拡張した場合の機能・保証要件はセキュアである」を事例化した具体モデルである．このゴールの証跡を付録 B の具体例に示している．

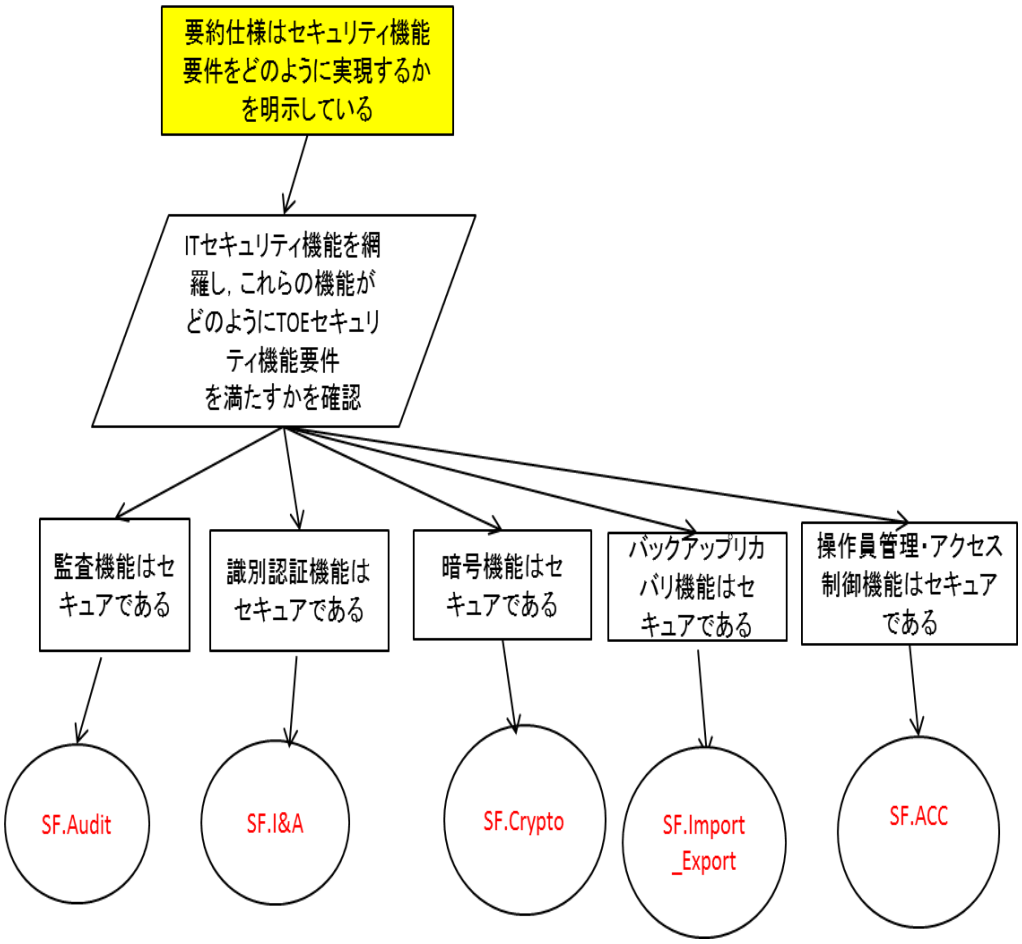


図 6-4-4　TOE 要約仕様

図 6-4-4 は図 4-2-3 セキュリティ要約仕様化段階における「要約仕様はセキュリティ機能要件をどのように実現するかを明示している」を事例化した具体モデルである．このゴールの証跡を付録 B の具体例に示している．

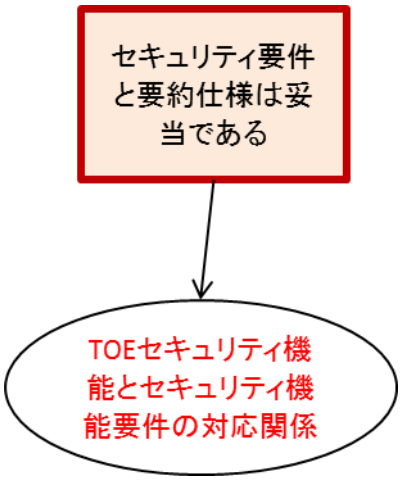


図 6-4-5　要約仕様妥当性

図 6-4-5 は図 4-2-3 セキュリティ要約仕様化段階における「セキュリティ要件と要約仕様は妥当である」を事例化している．

7　考察

3.1 節で示したように CC-Case の目的は開発のセキュリティ上の課題を解決するため，ソフトウェア開発方法論・プロセスからセキュアなシステム開発への対応を実施することである．このセキュリティ上の課題に対して，どのような要素技術で対応するのかを 3~5 章で説明し，6 章ではその具体例を示した．

本章では CC-Case の利点と 3-3 節で述べた開発のセキュリティ上の課題に対してどのように課題解決するのかを考察し，CC-Case の目的はどのように達成できるのかを示す．

7.1 節には要求段階の CC-Case の特長を要求分析と保証の手法，およびステークホルダーの観点でみた利点から論ずる．7.2 節には主な課題解決方法について，順次その内容を吟味する．7.3 節には主な課題解決方法の相互関係を示す．また各課題解決方法をもとにシステムリスク，事業継続リスク，顧客合意リスクに対してどのように対処しているかをそれぞれ説明する．更に CC-Case の特長を生かすことにより，7.4 節には CC，7.5 節にはアシュアランスケース自体に内在する問題点を克服できる可能性を議論する．

7.1　要求段階の CC-Case の特長

7.1.1 要求分析と保証の手法

要求段階における CC-Case はセキュリティ要求を獲得する際の技術的な難しさに対応することと同時に CC 準拠の保証をする．すなわち CC-Case は，CC に則り要求分析の段階で顧客と合意した範囲におけるセキュリティ保証要件を定め，保証をするために必要なセキュリティ機能要件を，CC に準拠して網羅的に抽出・分析・妥当性検証・仕様化・管理を行う要求分析手法である．　更に CC-Case は，①セキュリティ仕様検討プロセスの明示化，②セキュリティ保証要件，③顧客との合意のプロセスの明示化による保証手法である．①と②は CC 準拠による保証である．セキュリティ要求分析の手法は数多いが，CC 準拠と顧客合意の保証を伴う手法は皆無であり，CC-Case の特長である．

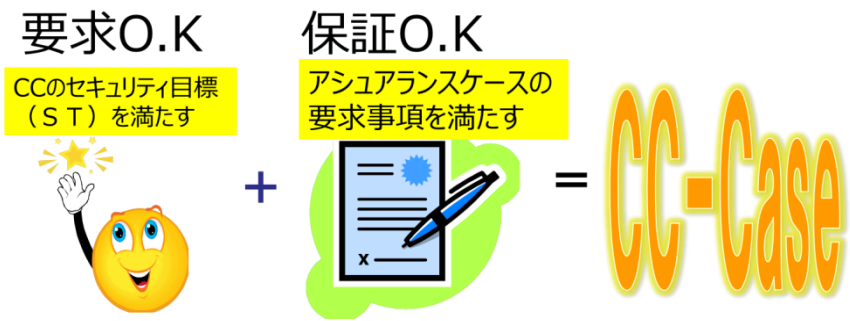


図 7-1-1 CC-Case：要求と保証の手法

以下にプロセスと成果物の観点から，CC-Case はセキュリティ要求分析手法かつ保証手法であることを論述する．

CC-Case のセキュリティ要求分析実施プロセスは「セキュリティ仕様のアシュアランスケース」として ST を作成する際に必要なプロセスが明示化されている．従って CC-Case を利用しない場合より，CC に準拠したシステム・製品の仕様要求，

セキュリティ要求の対応関係や論理構造を網羅的に分析しやすい． IEEE Std1012-2004[5]によれば，検証（verification）とは，ソフトウェア品質保証のための確認プロセスには開発活動による生産物が開発活動に対する要求に適合していることを判定する活動であり，妥当性確認（Validation）とは，開発されたソフトウェアが意図された利用法とユーザニーズに適合していることを判定する活動である．

CC-Case のセキュリティ要求分析実施プロセスでは ST を作成する際の要求に適合していることを検証する．検証の実施個所は図 4-2-1,図 4-2-1-1,図 4-2-2,図 4-2-3 の黄色（細い枠線）のゴールである．セキュリティ保証の観点から検証は正確性，完全性，有効性が検証される．正確性とは内容に誤りがないこと，あいまいさがなく明確であることである． CC-Case のゴールは CC 準拠であること，すなわち各証跡が ST として誤りがないことを検証している．また完全性とは漏れがないこと，余分なことがないことである．CC-Case はセキュリティ対策方針根拠，セキュリティ機能要件根拠やセキュリティ機能要件とセキュリティ機能要約仕様の対応関係において要件の必要十分性の検証を実施する．また，有効性とはセキュリティ機能が目的通りに動作することである．各ゴールに示された「セキュアである」つまり安全であることが保証されることである．

また, CC-Case では各段階で示された証跡がユーザニーズに適合していることを顧客と合意することにより，妥当性確認を行う．尚，証跡は具体モデルの最下位で実際の事例に基づいた根拠を示している．顧客との合意プロセスは図 4-2-1,図 4-2-1-1,図 4-2-2,図 4-2-3 の肌色（太い枠線）のゴールである．

7.1.2 ステークホルダーの観点でみた利点

図 7-1-2 に示すように開発者・保守運用者にとっては，①ST を作成する際に必要なプロセスが明示化され, システムや製品の ST が妥当であることを検証できる．②準形式的なセキュリティ機能要件を利用できるので齟齬が生じず，設計しやすさが期待できる．③証跡を要求管理 DB で管理するので，新たな脅威の発生などに伴う仕様変更の対応が実施しやすさが期待できる．④CC パート 2 に規定されたセキュリティ機能要件は形式化・カタログ化されているので要件を再利用しやすさが期待できる．

顧客（要件決定の関係者）にとっては①妥当性確認のタイミング（肌色・太い枠線の個所）が定められており，段階に応じて，要件が顧客ニーズからみて妥当であるかの判断の根拠が与えられる．②コスト・難易度などセキュリティ以外の他のニーズでもどこまでの保証レベルとするかの主張ができる．③EAL を用いることで，評価保証レベルが明確にし，開発や構成，管理などに関わる個々の保証要件を規定するのではなく，目標とする評価保証レベルだけを指定することができる．必要な保証レベルに応じてシステムや製品を，適正なコストで保証することができる．

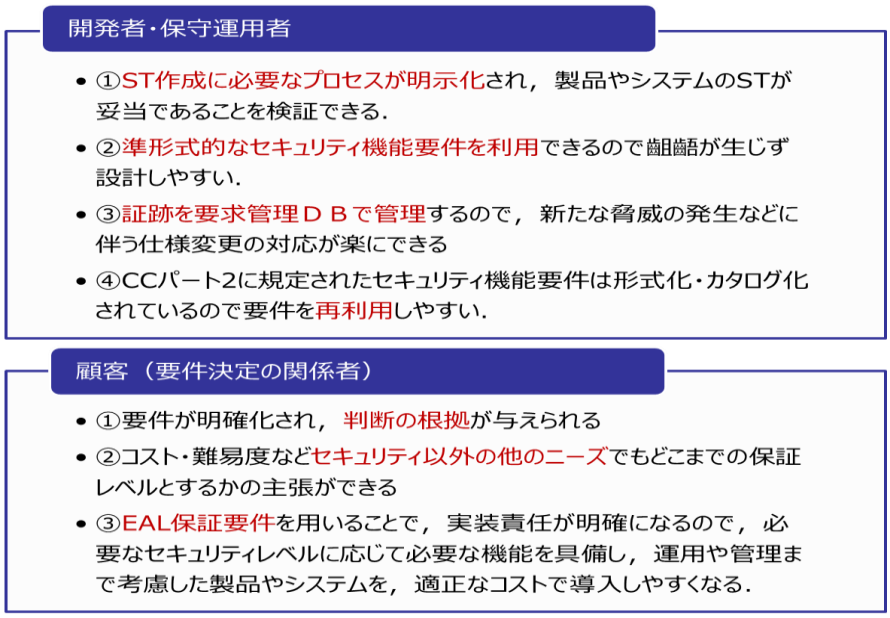


図 7-1-2　ステークホルダーの観点でみた利点

7.2　セキュリティ課題の詳細と対応の方向性

7.2.1 要求の観点でのセキュリティ課題の詳細と対応の方向性

図 7-2-1 は要求の観点から見たセキュリティ課題の詳細と対応の方向性を示している．図 3-1 の開発におけるセキュリティ上の課題の a.b.c は「セキュリティ要求を獲得する際の技術的な難しさ」である①情報に対する複雑性②状況の変化，③トレードオフ[44]に相当している．

本節では要求の課題の詳細として a,b,c,d を説明．対応の方向性から課題対応方法と根拠について説明する．

「a.情報に対する複雑性があるため、セキュリティ要求の獲得が難しい」とは，セキュリティに関する関心事は多く，互いに複雑に関連していることを指す．CC-Case では「a.情報に対する複雑性があるため，セキュリティ要求の獲得が難しい」ことに関しては，CC（パート 1）を用いた「①セキュリティ仕様検討のプロセス明示化」で対応している．「扱う情報に対する複雑性」とは，セキュリティに関する関心事は多く，互いに複雑に関連していることを指す．具体的には分析すべき情報、資産、脅威、機能要件、根拠などセキュリティに関する関心ごとが多いこと，対抗策の妥当性、正当性、機能要件の完全性などの関心ごとが互いに複雑に関連していること，脅威の範囲、前提条件などの開発範囲が不明確であることを指す．2.1 節に挙げたミスユースケース[8]や Abuse Frames[11]などのユースケースのセキュリティ拡張手法や Secure Tropos[7]，i*-Liu 法[9]，NFR フレームワーク[13]などのゴール指向要求分析方法論は，この複雑な関心事を分析する手順があいまいで特定のシーンにおける部分的な分析をする傾向がある．また手順があいまいなため，検討漏れが生じやすい．これに対して CC-Case はセキュリティ要求分析で扱う脅威，リスク，対策，資産等の複雑な情報を CC に則り，より明確に具体的に要求分析手順化する「①セキュリティ仕様検討のプロセス明示化」を実施している．そのため保証に基づいた系統的な分析ができ，検討漏れが発生しづらい．また要求分析をしながら証跡を残していくため論理の完全性を確保できる長所をもつ．

「b.脅威等の状況変化がはげしくセキュリティ要求の獲得と対策が難しい」とは，見えない敵が存在し想定外の新たな脅威が発生することにより，セキュリティ要求の獲得要件が変化し，更なる対策を繰り返す必要が生じる難しさである．CC-Case は，セキュリティ要求の獲得に関しては「②脅威分析の工夫（一般の要求分析への組込み等）」をした SARM で対応する．新たな脅威が増えた場合，SARM 状況表を再利用し，新たな攻撃を追加して分析をする．また CC-Case は要求管理 DB を設定しており，全ての証跡と論理的根拠を残している．これにより当初の想定とは全く違う要求が生じたとき，どの機能にどのような影響があるのか，どのように変更すべきかの判断がしやすく，繰り返される変更に対処しやすい．更に「③要求，設計，実装，テスト，保守のライフサイクルプロセス対応」により，要求以降の段階についても対策が必要な箇所を特定しやすく，繰り返される変更に対処しやすい．

「c.他の要件とのトレードオフを考慮しなければならないためセキュリティ要求の獲得が難しい」とは，セキュリティ要求を考えるときに，競合する要求との間にコストや機能の使いやすさ等，相反する関係が生じることを指す．これに対して主に CC-Case はこれが「②脅威分析の工夫（一般の要求分析への組込み等）」をした SARM で対応している．SARM はセキュリティ機能，攻撃者のゴール，資産の相反する関係を分析する手法だからである．

更に CC-Case はセキュリティ対策の競合する要件を考慮し，顧客と合意の上でどこまでの対策を実施するのかを選択するプロセスを明示して顧客が選択可能にしている．これが「⑧顧客との合意プロセスの明示」である．妥当性確認は顧客との合意という根拠をもってトレードオフに対処する．これは 4.2 節に前述したように，図 4-2-1,図 4-2-1-1,図 4-2-2,図 4-2-3 の肌色（太い枠線）のゴールでの妥当性確認が相当する．

セキュリティ上の課題の d はセキュリティ要求を獲得した後の要求分析・管理・共有する段階での課題である．これは 7.4 節で後述する CC 自体の導入段階の課題である．

「d.システム・製品の仕様要求，セキュリティ要求間の対応関係や論理構造を分析・管理・共有する手段が確立されていない」とは，現在のセキュリティ要求分析手法は限定的なシーンにおいての脅威分析やそれに対する対策立案の手法がほとんどであり，網羅的に抽出・分析・妥当性検証・仕様化・管理を行う手段が確立されていないことである．つまりセキュリティ要求を実装につなぎやすい手法がないことを指している．これに対して CC-Case は①セキュリティ仕様検討のプロセス明示化，④セキュリティ機能要件の利用，⑥論理的証拠の提示で対応している．

分類	開発における セキュリティ上の課題	各課題の詳細		対応の方向性
要求	a.情報に対する複雑性があるため、セキュリティ要求の獲得が難しい	セキュリティ要求を獲得する際の技術的な難しさに網羅的に適切な対応が可能なセキュリティ要求分析手法はまだ確立されていない	①扱う情報に対する複雑性 ・セキュリティに関する関心ごとが多い（分析すべき情報、資産、脅威、機能要件、根拠） ・関心ごとが互いに複雑に関連（対抗策の妥当性、正当性、機能要件の完全性） ・開発範囲が不明確(脅威の範囲、前提条件)	①セキュリティ仕様検討のプロセス明示化
	b.脅威等の状況変化がはげしくセキュリティ要求の獲得と対策が難しい（事業継続リスク）		②状況の変化 見えない敵が存在し想定外の新たな脅威が発生それに対して更なる対策を繰り返す必要が生じる.	②脅威分析の工夫（一般の要求分析への組込み等） ③要求，設計，実装，テスト，保守のライフサイクルプロセス対応
	c.他の要件とのトレードオフを考慮しなければならないためセキュリティ要求の獲得が難しい		③トレードオフ セキュリティ要求と競合する他の要求との間にコストや機能の使いやすさ等，相反する関係が生じる	②脅威分析の工夫（一般の要求分析への組込み等）
	d.システム・製品の仕様要求、セキュリティ要求間の対応関係や論理構造を分析・管理・共有する手段が確立されていない	セキュリティ要求を実装につなぎやすい手法がない	・現在のセキュリティ要求分析手法は限定的なシーンにおいての脅威分析やそれに対する対策立案の手法がほとんどである ・網羅的に抽出・分析・妥当性検証・仕様化・管理を行う手段が確立されていない	①セキュリティ仕様検討のプロセス明示化 ④セキュリティ機能要件の利用

図 7-2-1　要求の観点でのセキュリティ課題の詳細と対応の方向性

7.2.2 保証の観点でのセキュリティ課題の詳細と対応の方向性

要求と保証の双方に関わる課題として「e.仕様が固まった後にセキュリティ要求が作成され，保証要件は不明確である」がある．一般に要求分析において，保証要件までの検討は行わず，保証要件は不明確になりがちである．CC による認証評価を行う際にはセキュリティ目標（ST）を定める必要があり，保証要件は明確になる．しかしこの ST の作成も仕様が固まった後に要求分析とは別に実施されることが多い．要求に保証のタイミングのずれによる実装内容の手戻りを防ぐためにはシステム・製品をできあがったタイミングで評価するのではなく，要求分析・獲得を実施する中で確実に検証・妥当性確認ができることが望ましい．そこで CC-Case では要求分析を実施した後に保証事項を決定するのではなく、要求分析を実施しながら保証を一緒に実施していく「⑤要求分析と同時に保証要件を決定」で対処している．

「f.設計・開発の確実な実施への品質説明力が必要である」とは利用者が不測の事態を発生させてセキュリティ機能が正確かつ有効に動くことを確認することは困難であり，開発者側で品質の説明をする必要があることを指す.この課題に対応するため理論的な論理関係で保証目標に対する妥当性を示し、根拠を示すことによる保証をする．具体的にはアシュアランスケースを用いることで「⑥論理的証拠の提示」と「⑦セキュリティゴールに対する検証」が可能となる．

「g.システム・製品に対して顧客から訴訟を受ける可能性がある」とは一般の機能以上にセキュリティ機能をお客様に納得していただき、双方のギャップを埋めることは難しく、問題を引き起こすもとになることを指す．この課題に対応するため保証する範囲を顧客（関係者）と合意した範囲における保証（妥当性確認）である「⑧顧客との合意プロセスの明示」で対応する．

「h.システム・製品によって求めるセキュリティ保証の度合いは異なる」とはセ

キュリティ保証を体系的に実施し，求める度合いは異なるセキュリティの評価ができる枠組みが不可欠であることを指す．この課題に対して，「⑨CC 基準での評価」や CC（パート 3）を用いた「⑩セキュリティ保証要件による保証」で対応する．

分類	開発におけるセキュリティ上の課題	各課題の詳細	対応の方向性
要求	e.仕様が固まった後にセキュリティ要求が作成され、保証要件は不明確である.	システム・製品ができあがったタイミングで評価するのではなく，要求分析・獲得を実施する中で確実に検証・妥当性確認ができることが望ましい	⑤要求分析と同時に保証要件を決定
保証	f.設計・開発の確実な実施への品質説明力が必要である（システムリスク）	利用者が不測の事態を発生させてセキュリティ機能が正確かつ有効に動くことを確認することは困難	⑥論理的証拠の提示 ⑦セキュリティゴールに対する検証
	g.システム・製品に対して顧客から訴訟を受ける可能性がある（顧客合意リスク）	一般の機能以上にセキュリティ機能をお客様に納得していただき、双方のギャップを埋めることは難しく、問題を引き起こすもとになる	⑧顧客との合意プロセスの明示
	h.システム・製品によって求めるセキュリティ保証の度合いは異なる	セキュリティ保証を体系的に実施し，求める度合いは異なるセキュリティの評価ができる枠組みが不可欠	⑨CC基準での評価 ⑩セキュリティ保証要件による保証

図 7-2-2　保証の観点でのセキュリティ課題の詳細と対応の方向性

7.3　システム開発のリスクへの対処

7.3.1 システムリスクへの対処の強化

図 7-3-1-1 に示すように「①セキュリティ仕様検討のプロセス明示化」は要求のプロセス定義，「⑤要求分析と同時に保証要件を決定」，「⑥論理的証拠の提示」は保証のプロセス定義を実施している． CC-Case では「①セキュリティ仕様検討のプロセス明示化」し，CC に準拠したシステム・製品の仕様要求，セキュリティ要求の対応関係や論理構造を漏れなく分析可能とし ST の要求項目を証跡として全て含んでいることにより要求の十分性確保をしている.「⑤要求分析と同時に保証要件を決定」により，要求分析段階で顧客合意のうえでセキュリティ保証要件を定める．「⑥論理的証拠の提示」により，作業は手順に従って進められるが，それとともに証跡が生成される ST を作成するためのもととなる内容を証跡として残す．これらの対処により，システムリスクへの対処の強化が可能である．

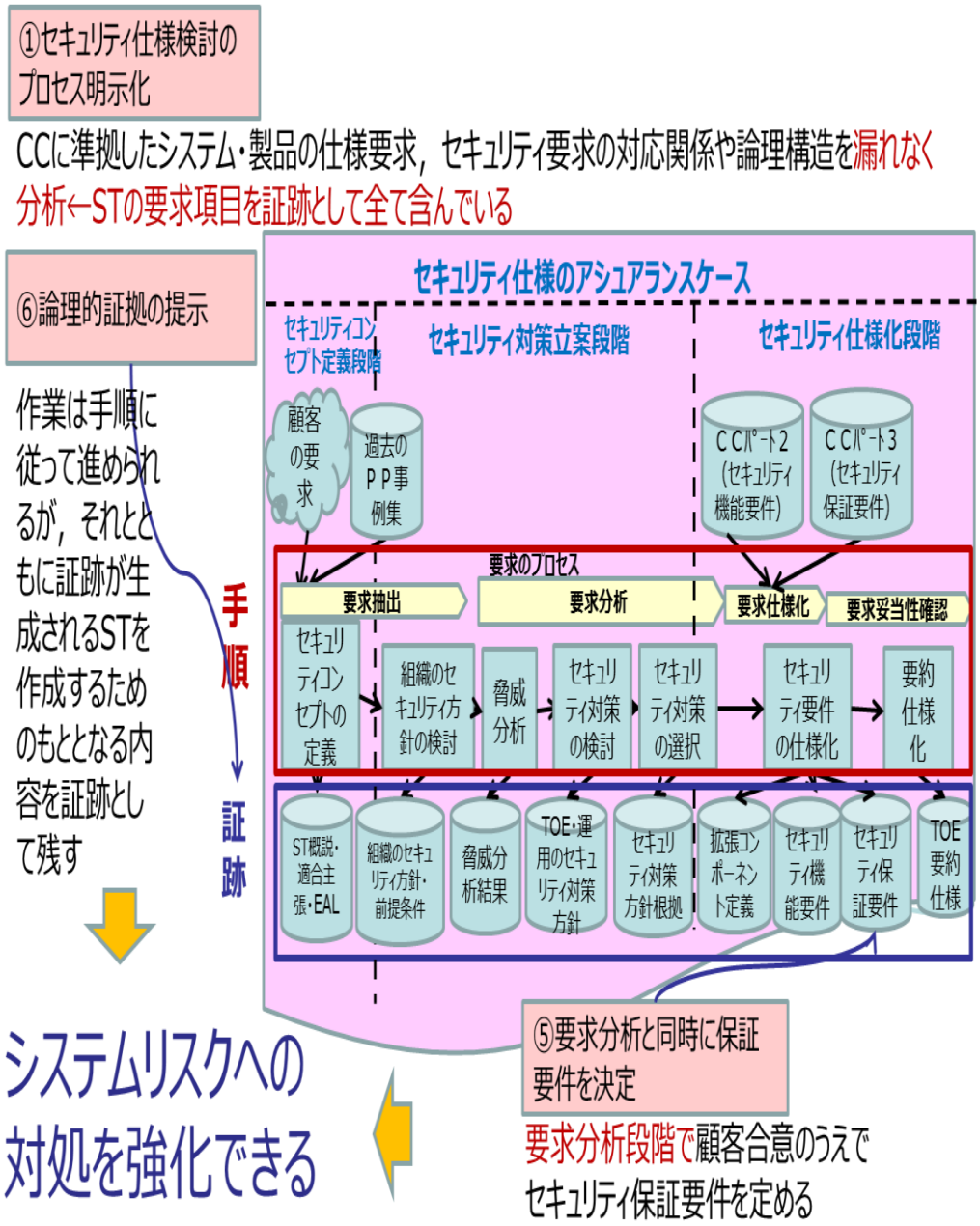


図 7-3-1-1　要求の明確化と保証のプロセス定義によるシステムリスクへの対処

図 7-3-1-2 に示すように脅威分析手法 SARM を用いた「③脅威分析の工夫（一般の要求分析への組込み等）」，「④セキュリティ機能要件の利用」，「⑦セキュリティゴールに対する検証」による実装手法を用いることで CC-Case によるシステムリスクへの対処の強化が実施可能である．

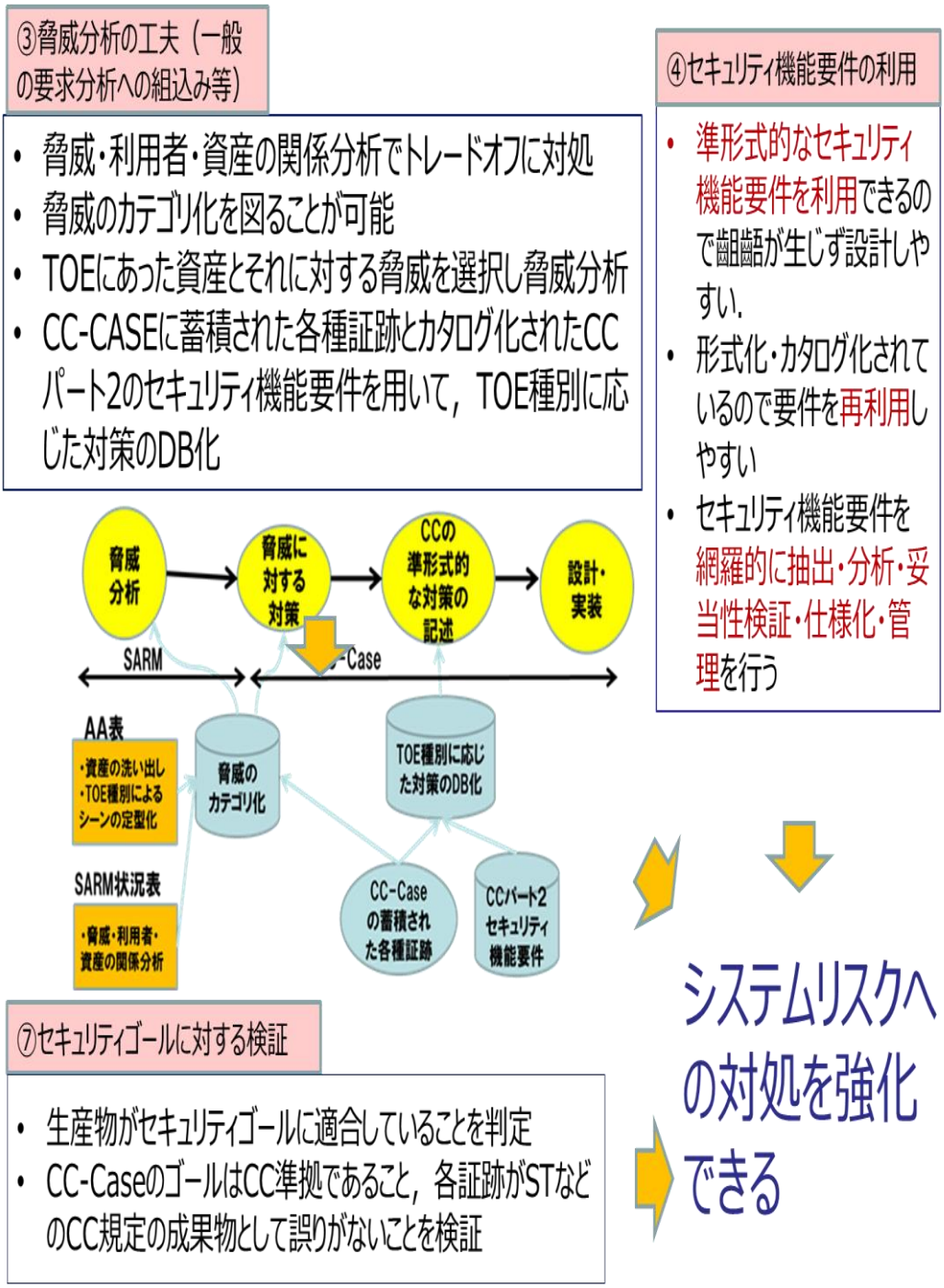


図 7-3-1-2　要求分析と実装の手法によるシステムリスクへの対処

5 章で説明したように脅威分析手法 SARM は一般機能への要求とともにセキュリティ要求を分析可能である．更に SARM の脅威分析を CC に適したものにするための工夫について，その脅威分析の結果を入力：としてどのような処理を実施すれば，CC に適した要求分析ができるのかを考察したい．SARM は AA 表で資産の洗い出しと TOE 種別によるシーンの定型化，SARM 状況表で資産，利用者，資産の関係分析を行い，脅威のカテゴリ化を図ることが可能であろう．更に「セキュリティ脅威とセキュリティ対策方針事例」[3]などを参考に資産と処理ごとの脅威をカタログ的に利用して，TOE にあった資産とそれに対する脅威を選択し，脅

威分析の抽出を CC の脅威情報に統一して実施する．CC-Case の証跡として脅威情報を DB 化することにより効率的な処理が可能となるだろう．この脅威に関して対策もカテゴリ化できる．CC-Case では CC-CASE に蓄積された各種証跡とカタログ化された CC パート 2 のセキュリティ機能要件を用いて，TOE 種別に応じた対策の DB 化を行う．これらの工夫により，CC-Case 自体もより効率的に作成可能となることが期待できる．このような CC に適した SARM の利用の工夫により，システムリスクへの対処の強化が可能なるであろう．

7.3.2 事業継続リスクへの対応

ライフサイクルプロセスの CC-Case はモニタリングとコントロールによる事業継続リスクに対応可能であり，変化するリスクへの対応も強化できる．CC-Case を用いたライフサイクルサポートは要求を正しくシステム・製品に実装することでシステムリスクに対応し，対象システム・製品の開発と保証において規律とコントロールを確立する．つまり CC-Case を要求段階だけでなく ライフサイクルに拡げるメリットは CC-Case の課題を強化出来るのである．

「②要求，設計，実装，テスト，保守のライフサイクルプロセス対応」は見えない敵が存在し想定外の新たな脅威が発生する状況の変化への更なる対策をしやすくする（図 7-3-2 参照）．アシュアランスケースの課題である開発方式、再利用、生産性の向上を期待できる．この詳細は 7.5 節に示すこととする．また CC に基づく保証をライフサイクル（システム・製品の要件定義・設計・実装・テスト・保守）にわたってサポートできる．要求段階における期待としての保証ではなく，実際の生産物を伴う保証が可能である．また，セキュリティ事故・トラブルを起こす本質的な原因を明らかにする「レビューの強化」ができる．このような特長をもって「②要求，設計，実装，テスト，保守のライフサイクルプロセス対応」は事業継続リスクへの対応を可能とする．

ここで，セキュリティ事故・トラブルを起こす本質的な原因を明らかにする「レビューの強化」が可能であることを説明するためにシステム運用情報セキュリティのトラブルと CC-Case の準拠する基準である CC の関係について，その目的と評価の本質を考察してみたい．

システム運用時には「アプリケーションバグや設計ミスでセキュリティ機能が動作しない．処理能力を超えた極限稼動でセキュリティ機能の動作不備が露呈する．本来見えないはずのデータにアクセス可能な方法が存在していた．明らかな使用ルール違反（内部犯罪など）だが痕跡の残らないシステム利用が行われた．」などのセキュリティ関連トラブルが日常的に発生する．

このようなセキュリティ事故・トラブルを起こす本質的な原因とは，脅威分析・システムリスク評価が不十分，各フェーズ間のセキュリティに関する分析の一貫性欠如，セキュリティ対策の検証方法のあいまいさ，設計・実装時のレビューが不十分でシステムバグ（IT または運用環境）を見つけ切れていないとことが考えられる．

CC の目的は情報技術に関連した製品のセキュリティの度合いを系統的に評価できることである．ユーザは必要なセキュリティレベルに応じた適正なコストで，安全なシステムや製品を導入可能であり，開発者にとっては安全なシステムや製品を開発するための指標を提示する．CC はセキュリティ評価の要件，評価対象(TOE)を含む，システム・製品の設計仕様，実際のシステム・製品，(部分的な)セキュリティ要求仕様に相当する TOE が満たすべきセキュリティ目標(ST) を規定している．

更に CC のセキュリティ評価は「ST は必要かつ十分か? 」という ST の妥当性検証，設計仕様のレビュー，システム・製品のテスト結果など「②要求，設計，実装，テスト，保守のライフサイクルプロセス対応」により実施される TOE が ST を達成しているかどうかの検証を実施するものである．

CC を導入し「評価」を受けることの本質はこうしたセキュリティ事故・トラブルを起こす本質的な原因を明らかにする「レビューの強化」である．CC は評価上のポイントを標準化したものであるので，セキュリティ問題に対する確固たるレビュー体制が整備されていれば，セキュリティ評価・認証制度や外部監査等を活用する必要はないかもしれない．もちろんセキュリティの問題は，日々変化する脅威や技術を常に追いかける必要があるため，セキュリティ専門家の知見，ノウハウ，能力にもとづく評価・監査サービスを活用することが有効である．しかし，本質的にはセキュリティ評価・認証制度・外部監査等の活用に関わらず，CC 基準で評価ができる内容でレビューができることが必要なのである．

②要求，設計，実装，テスト，
保守のライフサイクルプロセス対応

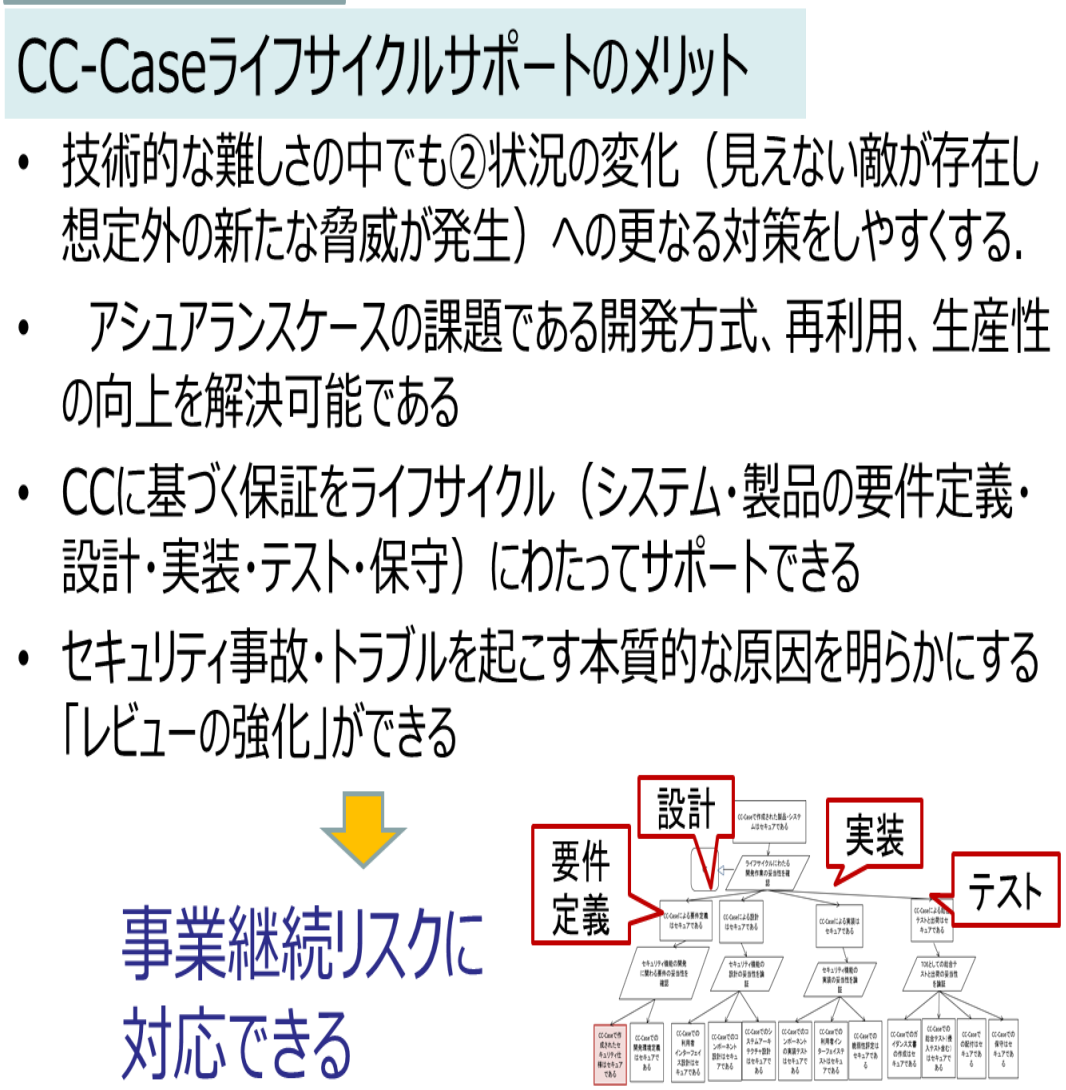


図 7-3-2　CC-Case のライフサイクルプロセスのメリット

7.3.3 顧客合意リスクへの対処

「⑧顧客との合意プロセスの明示」，「⑨CC 基準での評価」，「⑩セキュリティ保証要件による保証」の 3 つの課題解決方法では CC を用いることや妥当性確認のプロセス定義をアシュアランスケースで実施することでユーザニーズに基づく妥当性確認ができること，CC の保証要件で保証内容を明確化でき，顧客合意リスクの低減につながることが想定される(図 7-3-3).

「⑧顧客との合意プロセスの明示」と「⑩セキュリティ保証要件による保証」は CC 準拠の体系的評価とその評価に基づく保証である．CC-Case は CC 基準の評価，評価に適した要求分析手法の明確化，その要求プロセスの中に合意プロセスの定義、保証要件の確定を含んでいる。そしてこれらのプロセス定義化で顧客合意リスクを低減する．

ここで CC 準拠の評価と保証の意義について考察したい. セキュリティ保証を体系的に実施するためには，評価の枠組みが必要である．これを規定している IT セキュリティ評価の代表的な国際標準は CC である．しかし CC は ST を作成するための元となる要求分析や脅威分析の手法を定めていない[51]．この具体的な手順を与えることにより CC-Case は ST を作成するための元となる要求分析や脅威分析を実施し，CC に基づく保証を可能とする．評価対象 TOE の中で合理性に矛盾がなければセキュアでなくても CC に準拠できると考える方がいるかもしれない. しかし最上位のゴールは「CC-Case で作成されたセキュリティ仕様はセキュアである」を満たすためには，下位の全てのゴールの達成が必要である．下位ゴールでは，TOE と運用環境を正確にモデル化し，資産，脅威および対抗策によるセキュリティの概念と関係に基づいて，セキュリティ機能が規定され，セキュアであることを検証される．具体的には想定される脅威に対抗するために適切なセキュリティ対策が策定されていること，セキュリティ対策の実現のために適切なセキュリティ機能要件が選択されていること，選択されたセキュリティ機能要件に対して適切なパラメータの割付などが指定されていること，想定される脅威や期待される確からしさに対応した保証要件が選択されていることなどの条件を検証する．これらの条件を満たせばそのため「CC に準拠すること」のゴールは「セキュアであること」を満たすことになる．

尚，代表的な分析手法である SQUARE[14] [15]，セキュリティ開発ライフサイクル[16]も含め，2.1 節で挙げた従来のセキュリティ要求分析手法には要求分析をしながら，CC のセキュリティ基準に則った保証を可能とする手法はなく，この点で CC-Case にはオリジナリティ及び手法の特長がある．

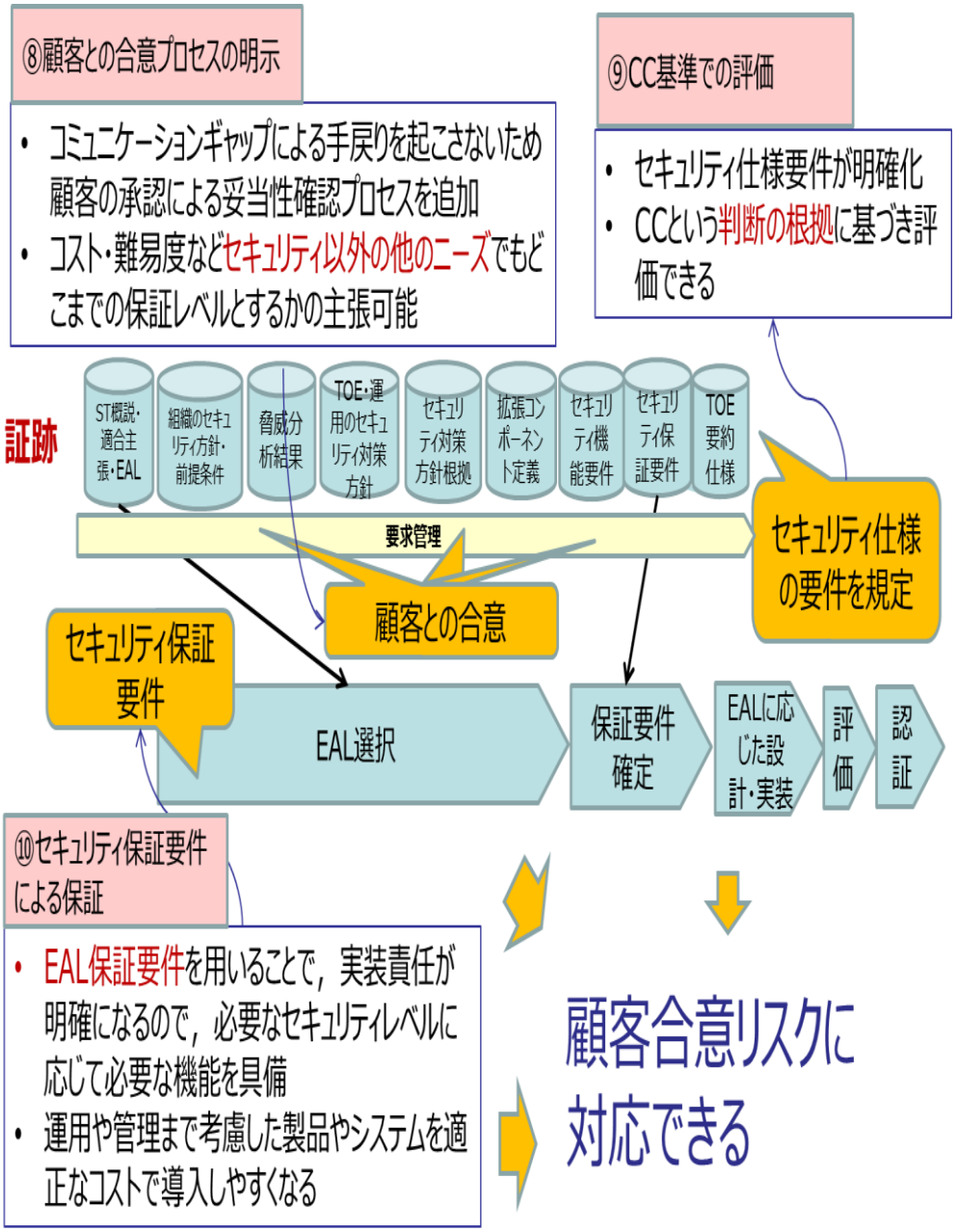


図 7-3-3　CC-Case の保証と顧客合意リスクへの対応

7.4　CC の課題解決

「コモンクライテリアにおけるセキュリティ要求の規定」[51]には，後述の①から⑤の課題が示されている．それに対して CC-Case がどのような課題解決の手段をもつかを示す．尚，CC 認証製品の維持・機能拡張段階，モデル展開段階は本論文の対象段階ではないが，ライフサイクルサポートを今後の検討課題にしており，当該段階での課題解決手段についても検討する．

①CC 導入段階において，CC は ST を作成するための元となる要求分析や脅威分析の手法を定めていない．通常，セキュリティ要件について，市場要求を踏まえ，セキュリティ要件の取捨選択等の現実的な調整が必要である．しかし， 実際には開発者はシステム・製品の仕様要求，セキュリティ要求，および CC で評価するセ

キュリティ要求間の対応関係や論理構造を分析・管理・共有する実用的な手段が存在せず，これが ST 内部の不整合，ST と開発エビデンスとの不整合の原因となる[51]．この課題に対して，CC-Case はシステム・製品の仕様要求，セキュリティ要求の対応関係や論理構造を分析する手段を提供し，見える化を実現している．また市場要求を踏まえ，セキュリティ要件の取捨選択等の現実的な調整を顧客との合意の上で実施することができる. さらに要求管理 DB を導入することは開発の管理・証跡の共有の実用的な手段となる．

②CC 認証製品の維持・機能拡張段階において，変更要求に伴う対応に漏れがないことが必要だが，自然言語で書かれた ST 更新ワークのみでは，分析ツールとしての能力が低く，不完全な修正になる可能性が高い．また，ライフサイクルで一貫した要求管理が不十分であり，脅威事象や個別要求の変化への対応が不完全になり易い[51]．この課題に対して，CC-Case は自然言語で書かれた ST 更新ワークよりも，アシュアランスケースの記法で全体が構造化されて一覧に図示されていることや論理モデルでプロセスが規定され，具体モデルのみを更新すれば良いため，修正箇所の特定が早く，変更要求に伴う対応漏れを低減させることが期待できる．更にまた，証跡は準形式的な CC の記法で表記されているので，パターン化して修正箇所の特定をすることもできる．さらに CC-Case の要求管理 DB を作成することにより，ライフサイクルで一貫した要求管理が期待できる．

③CC 認証製品のモデル展開段階においては，部分再利用時のアーキテクチャ上の整合確保が不十分であり，分析漏れによる脅威や脆弱性が残存する可能性がある[51]．この課題に対して，CC-Case は要求管理 DB に CC 認証製品のアーキテクチャを具体モデルとしてモジュール化して管理することにより，部分再利用時のアーキテクチャ上の整合確保がしやすくなり， 再利用を容易化でき，分析漏れによる脅威や脆弱性を低減可能であろう．

④要求工学的なアプローチを実務で生かすためには CC に最適化した要求記述・分析の方法論やサポートツールが未整備である[51]．この課題に対して，CC-Case はアシュアランスケースとゴール指向要求工学の統合アプローチを補完的に組み合わせており,CC に最適化した要求記述･分析の方法論を目指している．

⑤昨今の製品開発は高度に専門分化され，要求獲得・記述が開発者視点で行われる傾向があり，利用者受け入れ可能な要求獲得が不十分なケースが存在する[51]. この課題に対して，CC-Case は顧客（利用者）と検討・合意するプロセスを規定しており，受け入れ可能な要求獲得が明示的に実施され,それが不十分なケースを低減できよう．

表 7-4　CC の課題解決

	CCの課題	CC-Caseの解決方法
1)CC導入段階	・要求分析や脅威分析の手法を定めていない. ・製品の仕様要求，セキュリティ要求，およびCCで評価するセキュリティ要求間の対応関係や論理構造を分析・管理・共有する手段を持たないケースが多い.	CC-Caseは製品の仕様要求，セキュリティ要求，およびCCで評価するセキュリティ要求間の対応関係や論理構造を分析・管理・共有する手段そのものCC-Caseはセキュリティコンセプト作成のアシュアランスケースやSTのアシュアランスケースにより，STを作成するための元となる要求分析を論理構造の明示化により実施できる. CC-Caseはセキュリティ要件の取捨選択等の現実的な調整ができる→ＳＴ内部の不整合，ＳＴと開発エビデンスとの不整合の原因を防ぐことができる.
2)CC認証製品の維持・機能拡張段階	分析ツールとしての能力が低く，不完全な修正になる. ライフサイクルで一貫した要求管理が不十分であり，脅威事象や個別要求の変化への対応が不完全.	自然言語で書かれたＳＴ更新ワークよりも，CC-Caseのアシュアランスケースを分析ツールとして用いる方が，修正箇所の特定も早い．CC-Caseの要求管理ＤＢを作成することにより，ライフサイクルで一貫した要求管理が可能になる.
3)CC認証製品のモデル展開段階	部分再利用時のアーキテクチャ上の整合確保が不十分であり，分析漏れによる脅威や脆弱性が残存する可能性がある.	部分再利用時のアーキテクチャ上の整合確保がしやすくなり，分析漏れによる脅威や脆弱性を低減可能である.
4)要求工学的なアプローチを実務で生かす	ＣＣに最適化した要求記述・分析の方法論やサポートツールが未整備である.	CC-CaseはＣＣに最適化した要求記述・分析の方法論である.
5)要求獲得・記述が開発者視点で行われる傾向	利用者受け入れ可能な要求獲得が不十分なケースが存在する.	CC-Caseはセキュリティ仕様作成のアシュアランスケースで検討・合意するプロセスを規定しているため，利用者受け入れ可能な要求獲得が明示的に実施され,それが不十分なケースを低減できる.
利用実態	CCはその複雑さからデジタル複合機などの特定のセキュリティ機能をハードウェア製品や政府調達対象案件には利用されているものの一般的な要求分析にはあまり利用されていない	CC-Caseは認証を取るための利用目的だけでなく，一般的なセキュリティ要求分析に利用できることを意図している．CC-CaseはCCのもつ確立されたセキュリティ要求分析手順を広く一般に利用できる手法である.

7.5　アシュアランスケースの課題解決

「主張と証拠」[6]によるとアシュアランスケースには次のように①から④の課題があるが，作成基準のないアシュアランスケースに比べ，CC-Case ではどのように課題解決できるかを以下に考察する．

①開発方式に関して，アシュアランスケースは一般に，作成プロセスを開発することにより管理を容易化する必要がある[6]．これに対して，CC-Case は論理モデルとしてセキュリティ仕様検討のプロセスを明示化しており，個別の管理が必要なのは具体モデルのみである．更に具体モデルの要件は上位の論理モデルによって限定される．従って管理の容易化や品質向上につながることが期待される．

②再利用に関して，アシュアランスケースはパターン化による再利用の容易化を課題としている[6]．Ankrum[36]もアシュアランスケースはプロジェクト固有な部分をもち，再利用可能箇所を区別するのは難しいという課題を挙げている．これに対して，CC-Case は論理モデルとして共通性を明確化しているため，論理モデル部分は再利用が可能である．更に CC-Case はセキュリティ要件を準形式的言語化するので証跡の内容も再利用の容易化が期待できる．

③生産性に関して，アシュアランスケースをモジュール化することで作成を効率化する必要があり[6]，Ankrum もアシュアランスケース構築に時間とコストがかかるとしている[36]．これに対して CC-Case は CC に基づいた手順は論理モデルとして共通化しており作成不要である．また収集すべき証跡も規定されているため，これらの規定のないアシュアランスケース構築に比べて，生産性向上が期待される．

④確信性に関して，アシュアランスケースを構成する下位のサブゴールや戦略ならびに証拠の成立確率に基づいて，アシュアランスケースの充足性を推論する方法を確立する必要があるといわれている[6]．これに対して CC-Case は CC 基準をベースにして，サブゴールや戦略ならびに証拠を作成しているが，その成功確率に関する検討はまだ行っていない．確信性に関しては今後の検討事項である．

表 7-5　アシュアランスケースの課題解決

	アシュアランスケースの課題	CC-Caseの解決方法
①開発方式	作成プロセスを開発することにより管理を容易化する必要がある	セキュリティ仕様検討のプロセスを明示化により管理を容易化
②再利用	パターン化による再利用の容易化が課題	構築のもととなるパターンを規定 →部分再利用時のアーキテクチャ上の整合確保がしやすい アシュアランスケース自体の再利用容易化 セキュリティ要件を準形式的言語化 →証跡の内容も再利用しやすい.
③生産性	モジュール化することで作成を効率化する必要あり	収集すべき証跡も規定 証跡は検証されてSTとして作成 →必要以上の時間・コストはかからない.
④確信性	下位のサブゴールや戦略ならびに証拠の確立に基づいて，アシュアランスケースの充足性を推論する方法を確立する必要がある	今後の課題

8　結論

8.1　まとめ

本論文では，CC とアシュアランスケースの長所を統合したセキュリティ要求分析手法かつ保証手法として CC-Case を提案した．CC-Case の目的，定義，CC-Case におけるアシュアランスケースの役割，特長を示した．更にケーススタディ により手法の妥当性，実用性の事例を示した．

アクタ関係行列（ARM）を拡張したアクタ関係表に基づくセキュリティ要求分析手法（SARM）を提案した．SARM は i*に対してセキュリティ対応をした i*-Liu 法で作成するモデルと等価性をもって表現可能である．SARM と i*-Liu 法を比較・評価した結果，SARM の網羅性の高さと i*-Liu 法の一覧性の良さを確認した．さらに，両手法の特性を生かした効果的な使用方法として，SARM と i*-Liu 法の組み合わせレビュー手法を提案した．また, SARM と i*-Liu 法については定式化し，一般的に相互変換できることを論理的に証明し両手法の等価性を明らかにした．また具体例による確認も実施した．アクタ間の詳細レビューを実施可能なことも SARM の効果である．

CC-Case と SARM の比較により，両者が補完関係にあること，SARM の AA 表による資産と脅威の抽出や SARM 状況表による脅威分析を CC に対応した方法が可能であること，SARM と CC-Case による CC に適したデータ利用の工夫が可能であることを示した．

図 8-1 に示すようにセキュリティ要求を獲得する際の技術的な難しさなどの開発におけるセキュリティ上の課題に対して，主な課題対応方法により，システクリスク，事業継続リスクや顧客合意リスクに対処できることを考察した．更に CC やアシュアランスケース自体に内在する問題点を克服できる可能性について考察した．

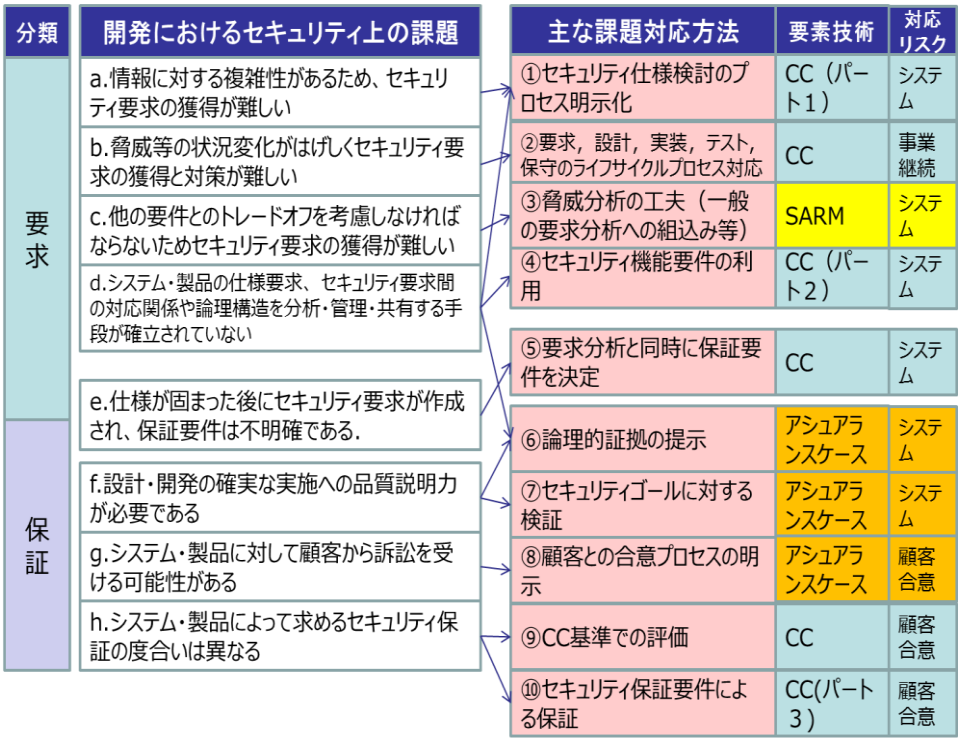


図 8-1　主な課題対応方法と対応リスク

本論文の提案はより巧妙化する脅威に対して，より安全なシステム・ソフトウェアを開発するための新たなフレームワークを確立しようとするものであり，将来のIT業界及びIT製品を利用する多くの人々のために重要な研究となることを目指している．また，本研究はセキュリティ規格に適合したCCに基づくセキュリティ機能要件を利用して対象とするシステムのセキュリティ保証を確保するものであり，CCに基づいたセキュリティ機能要件を利用している．

8.2 今後の課題

6章の考察はいずれも定性的な評価であり，以下の点を今後の課題とする．

(1)CC-Case 適用の効果はシステム開発からサービス提供のライフサイクルにわたって利用することで効果を発揮するものであり，ライフサイクルにわたるアシュアランスケースの作成手順と実例を適用した定量的な効果測定が必要である．

(2)CC はその複雑さからデジタル複合機などの特定のセキュリティ機能のハードウェア製品や政府調達対象案件には利用されているものの，それ以外のセキュリティ要求分析にはあまり利用されていないという課題も抱えている．この課題解決のため，CC-Caseは認証を取るための利用目的以外においても，一般のセキュリティ要求分析に利用できることを示すことをCC-Caseの最終目標と考えている．

(3) 脅威分析結果を対策化する段階の CC-Case の具体モデルとデータ利用の工夫を更に事例化すること，対策の立案の手法やTOE分類の特長ごとの類型化を具体的にすすめること及び本格的な評価並びに変換ツールの開発は今後の課題である．

(4)PPごとにより詳細なセキュリティ機能と保証を規定し利用を推進しようとする最近のCCの動向を踏まえ，このPPの類型化への対処を検討する必要がある．また新しいシステムなどでは適切なPPを特定することが難しい場合やPPが存在しない場合の対処も今後の検討事項である．

(5) GSNと同じ構成要素を備え，同等の表現ができるように意図して表形式のアシュアランスケースを検討している[44]．実際のサービス開発作業では，図形式のアシュアランスケースよりも Excel など表形式で階層を表すことができる方が導入が容易であると判断している. 更にGSN 構文を学習する必要がないことやGSNエディタがまだ普及していない現状では表形式のほうがより作成しやすいという点でもメリットがある． 特にCCの実装段階における詳細な仕様をアシュアランスケース化する上で定義化と利用法の確立を図りたい．

(6)対策立案・選択の枠組みを提示するのがこの論文の主旨であり，選択に必要な条件を提示しどのように選択を行うかについての具体的な手法は今後の研究課題である．

上記のような今後の課題を乗り越え，本研究が現在の開発のセキュリティ上の課題解決に役立つよう，世の中で広く利用されていくことを念願するものである．

謝辞

情報セキュリティ大学院大学に在籍させていただき，本論文をまとめるにあたって，大変多くの方にお世話になりました。ご査読いただき、かつご助言を賜りました情報セキュリティ大学院大学　学長 田中英彦教授，後藤厚宏教授，佐藤直教授，土井洋教授，橋本正樹助教に感謝いたします。

特に主査である田中英彦教授には、本研究及び関連研究を進めるにあたり，お忙しい中毎週のように時間を割いていただき，多くの議論を交わし，多くの示唆をいただきました．大学院入学時には研究など全く念頭になかった私に，相手に効果を納得してもらえるまで客観的な論理・事実を積み重ねる地道な活動としての研究の意義を一から十まで教えてくださいました．几帳面な文字で数十回にわたり添削してくださった先生の論文の赤入れは私の大事な宝物です．

また，田中研究室，後藤研究室及び大久保研究室の皆様には研究室のゼミにおいて，活発なご議論をいただき，数多くのご意見をいただきました．特に大久保隆夫准教授や橋本正樹助教には研究の進め方について的確なアドバイスをいただきました．ここに感謝の意をあらわします．

名古屋大学　山本修一郎教授には私の全ての論文に共著者として優れたアドバイスをいただきました．株式会社 NTT データ　システム科学研究所所長をされていた頃より今日にいたるまで直接の組織的なつながりのない私にありがたくも論文指導をしていただき，アクタ関係表やアシュアランスケースという私の研究の基礎となる要素技術を教え，大変に示唆に富んだご助言を頂きました．深く心より感謝いたします．

故・板倉征男教授には大学院前期博士課程入学の折，勤務しながら学業が遂行できるように格別のお計らいをいただきました．亡くなられた先生の分までこれからも研究を続け，社会に還元していきたいと存じます．

本論文は株式会社 NTT データに勤務しながら，情報セキュリティ大学院大学に在籍し研究を行った成果をまとめたものです．本研究の機会を与えてくださった同社　栗島聡代表取締役常務執行役員，宮崎茂樹 BU 長（現在ＮＴＴデータＳＭＳ事業本部長）にお礼申し上げます．業務上の多大なるサポートをいただきました同社品質保証部　端山毅品質保証部長，藤江宏部長，近藤麻美子部長，矢部智課長，宮本久仁男博士，品質マネジメント担当の皆様に感謝いたします．特に矢部智課長には，研究を継続可能とするよう様々なご配慮と共に国際会議論文への的確なコメント等もいただきました．田中研究室の先輩の宮本久仁男博士には大学院入学より，今日に至るまで，会社員兼研究者としての心がけも含め，様々なアドバイスをいただきました．

国立情報学研究所の吉岡信和准教授，みずほ情報総研株式会社 情報セキュリティ評価室 金子浩之氏に感謝いたします．お二人の情報セキュリティや CC に対する深い見識に触れて本研究の主張を強固に裏付けることができました．

学生の頃より今日に至るまで，私の挑戦の人生を決定づける幾度ものご指導と激励をいただいてきた池田大作 SGI 会長に最大限の感謝の意を捧げます．

仕事・育児を抱えながらの私の研究を心配しつつ，応援してくれた多くの友人・知人の皆様のおかげであきらめずに続けられました．感謝の想いで一杯です．

最後に時機をとらえての学問への挑戦を促してくれた父（中山晟㈱日本システムサービス代表取締役社長）と時に家事を代行して支えてくれた母　典子，いつも広い心で護ってくれた夫　浩と愛する長男　隆と次男　浩明に心から感謝します．本研究を含めた私の成果の全ては家族の支えによるものです．

参考文献

1 Common Criteria for Information Technology Security Evaluation, http://www.commoncriteriaportal.org/cc/
2 セキュリティ評価基準（CC/CEM） http://www.ipa.go.jp/security/jisec/cc/index.html
3 田淵治樹：国際規格による情報セキュリティの保証手法,日科技連，2007 年 7 月
4 ISO/IEC15026-2-2011,Systems and Software engineering-Part2:Assurance case
5 IEEE Std1012-2004 Software Verification and Validation, https://standards.ieee.org/findstds/standard/1012-2004.html
6 山本修一郎：主張と証拠,株式会社アセットマネジメント，2014 年 3 月
7 Mouratidis, H. : Secure Tropos homepage, http://www.securetropos.org/
8 Sindre, G. and Opdahl. L. A. : Eliciting security requirements with misuse cases, Requirements Engineering, Vol.10, No.1, pp. 34-44 (2005).
9 Liu, L., Yu, E. and Mylopolos, J. : Security and Privacy Requirements Analysis within a Social Setting, Proc. IEEE International Conference on Requirements Engineering RE 2003, pp.151-161(2003).
10 Letier, E. : Reasoning about Agents in Goal-Oriented Requirements Engineering, Université Catholique de Louvain(2001).
11 Lin, L. Nuseibeh, B. Ince, D. et al. : Introducing Abuse Frames for Analysing Security Requirements, Proc. IEEE International Conference on Requirements Engineering RE 2003, pp.371-372 (2003).
12 Chung, L. Nixon, B. Yu, E et al. : Non-Functional Requirements In Software Engineering, Academic Publishers(1999).
13 非機能要求グレード,http://www.ipa.go.jp/sec/softwareengineering/reports/20100416.html
14 Mead, N. R., Hough, E. and Stehney, T. :Sequrity Qualty Reqirements Engineering(SQUARE)Methodology(CMU/SEI-2005-TR-009),www.sei.cmu.edu/publications/documents/05.reports/05tr009.html
15 Mead, N. R, 吉岡信和: SQUARE ではじめるセキュリティ要求工学,「情報処理」Vol.50 No.3（2009）
16 Steve, L. Michael, H.:信頼できるコンピューティングのセキュリティ開発ライフサイクル, http://msdn.microsoft.com/ja-jp/library/ms995349.aspx,2005
17 Dubois, E. and Mouratidis, H : security requirements engineering: past, present and future, Requirements Engineering, Vol.15, No.1, pp.1-5 (online), DOI: 010.01007/s00766-009-0094-8(2009).
18 Yu, E. : i*homepage, i* , http://www.cs.toronto.edu/km/istar/
19 井部己文,山本修一郎,佐藤友合子：アクタ関係行列を用いた i スターフレームワーク作成方法の提案，情報処理学会研究報告．ソフトウェア工学研究会報告, Vol.2007, No.0107, pp.1-6(2007).
20 山本修一郎，連載第 39 回アクタ関係分析，ビジネスコミュニケーション,http://www.bcm.co.jp/site/youkyu/youkyu39.html>.
21 Yamamoto, S., Ibe, K. Verner, J. et al. : Actor Relationship Analysis for the i* Framework, Proc. International Conference on Enterprise Information Systems (ICEIS 2009) , pp.491-500(2009).
22 Sindre, G. and Opdahl. L. A. : Eliciting security requirements with misuse cases, Requirements Engineering, Vol.10, No.1, pp. 34-44 (2005).
23 松野裕，高井利憲，山本修一郎，D-Case 入門，～ディペンダビリティ・ケースを書

いてみよう！～, ダイテックホールディング, 2012 ， ISBN　978-4-86293-079-8
24 Tim, K. McDermid, J. A., :Safety Case Construction and Reuse using Patterns", in Proceedings of 16thInternational Conference on Computer Safety, Reliability and Security (SAFECOMP'97), Springer-Verlag (1997).
25 OMG, ARM, http://www.omg.org/spec/ARM/1.0/Beta1/
26 J.R.Inge.The safty case,its development and use un the United Kingfom.In Proc.ISSC25,2007.OMG, SAEM, http://www.omg.org/spec/ SAEM/1.0/Beta1/
27 Tim, K. Rob, W.: The Goal Structuring Notation – A Safety Argument Notation, Proceedings of the Dependable Systems and Networks 2004 Workshop on Assurance Cases (2004)
28 Stephen, E. T.,: The Uses of Argument, Cambridge University Press(1958)
29 The Adelard Safety Case Development (ASCAD), Safety Case Structuring: Claims, Arguments and Evdence,http://www.adelard.com/services/SafetyCaseStructuring/index.html
30 DEOS プロジェクト, http://www.crest-os.jst.go.jp
31 松野　裕　山本修一郎: 実践　D-Case～ディペンダビリティケースを活用しよう！～,株式会社アセットマネジメント，2014 年 3 月
32 小林茂憲，山本修一郎：アシュアランスケースを用いたサービス提供判断方法の提案，電子情報通信学会，信学技報, vol. 111, no. 489, KBSE2011-70, pp. 7-12, 2012 年 3 月
33 Rob, A. et al.:Security Assurance Cases: Motivation and the State of the Art， High Integrity Systems Engineering Department of Computer Science University of York Deramore Lane York YO10 5GH(2011).
34 Goodenough, J. et al.:Arguing Security - Creating Security Assurance Cases(2007). https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/assurance/643-BSI.html
35 Lipson H, Weinstock C.:Evidence of Assurance: Laying the Foundation for a Credible Security Case(2008). https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/assurance/973-BSI.html
36 Ankrum, T.S. Kromholz, A.H. :Structured Assurance Cases: Three Common Standards, Proceedings of the Ninth IEEE International Symposium on High-Assurance Systems Engineering HASE'05, (2005)
37 Robin, B. et al.: Assurance　case　workshop (2005).
38 Robin, B. et al.: International Working Group on Assurance Cases (for Security),IEEE SECURITY & PRIVACY(2006)
39 Robin, B. et al.: Assurance Cases for Security: The Metrics Challenge, 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks DSN'07(2007)
40 Jose, L. et al.: A Methodology for Security Assurance Driven Development," Requirements Engineering Volume 16, Issue 1 , pp 55-73(2011)
41 Yamamoto, S. Kaneko,T. and Tanaka, H.:A Proposal on Security Case based on Common Criteria, Asia ARES2013
42 Kaneko,T.,Yamamoto, S. and Tanaka, H.: Proposal on Countermeasure Decision Method Using Assurance Case And Common Criteria,Promac2012
43 金子朋子，山本修一郎，田中英彦：セキュリティ保証ケースを用いた対策立案方法の提案,2013 年 1 月，SCIS2013
44 吉岡信和, Bashar Nuseibeh，セキュリティ要求工学の概要と展望　情報処理 Vol.50 No.3 Mar.2009
45 A 社個人情報処理システムアプリケーションセキュリティターゲット，www.ipa.go.jp/security/jisec/seminar/documents/st_v3_3_20120702.pdf

46 金子朋子，山本修一郎，田中英彦：アクタ関係表に基づくセキュリティ要求分析手法（SARM）を用いたスパイラルレビューの提案,情報処理学会論文誌 52 巻 9 号
47 Web アプリケーション　セキュリティ強化：脅威とその対策,
http://msdn.microsoft.com/ja-jp/library/ff648641.aspx
48 大久保隆夫，田中 英彦:セキュリティアスペクトの設計手法, 電子情報通信学会, 2008 年 暗号と情報セキュリティシンポジウム,SCIS2008.
49 IPA:脆弱性対策情報データベース,http://jvndb.jvn.jp/
50 Guttorm, S.Andreas,L.O.: Eliciting security requirements with misuse cases. *Requir. Eng.*Vol.10, pp.34-44 (2005).
51 金子浩之，コモンクライテリアにおけるセキュリティ要求の規定の現状と課題，「情報処理」Vol.50 No.3（社団法人情報処理学会）

付録A

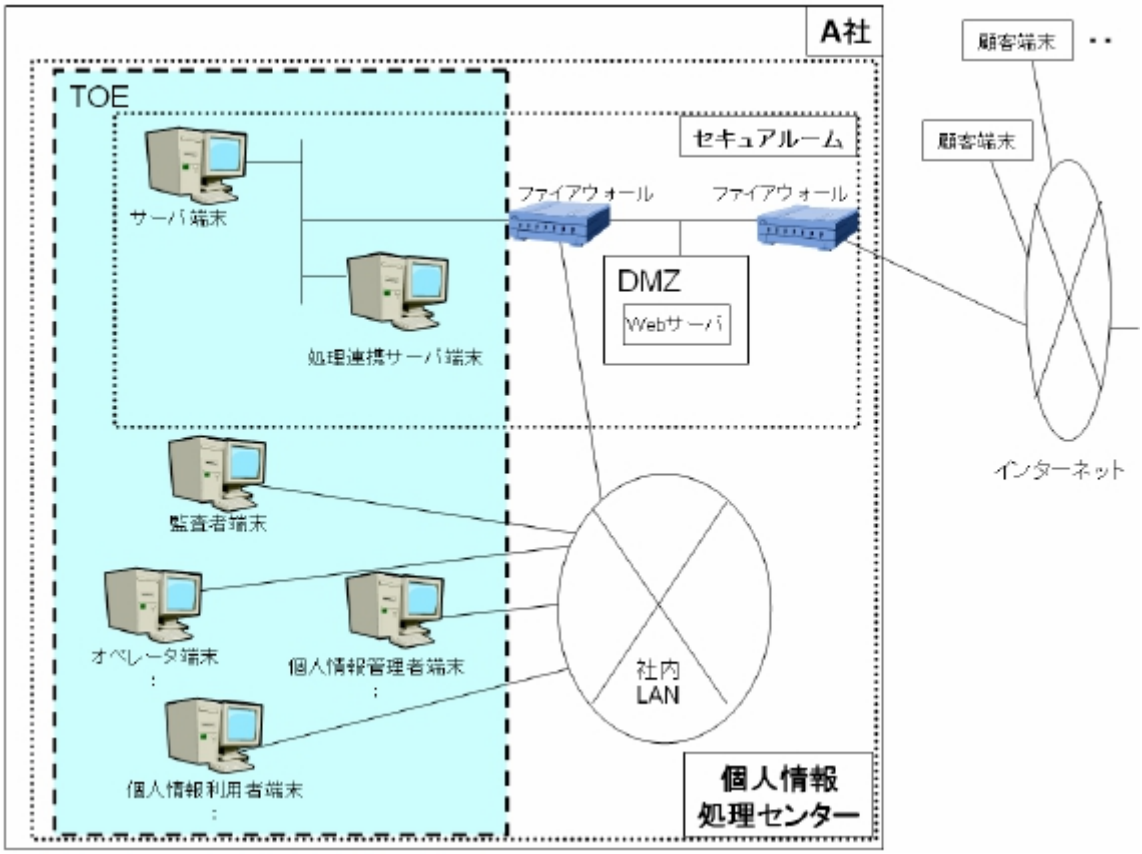
セキュリティコンセプト

評価対象（TOE）

TOE は、個人情報取扱事業者である A 社事業の一つである通信教育事業　において、顧客の個人情報を管理するためのシステム「A 社個人情報処理システム」を構成する.

TOE の範囲

対象範囲は破線で示す境界内にある端末は、オペレータ端末、個人情報利用者端末、個人情報管理者端末、サーバ端末、監査者端末、及び処理連携サーバ端末である.



セキュリティ機能

監査機能・操作員管理・アクセス制御機能・
識別認証機能・暗号機能・バックアップ・リカバリ機能

ハードウェア構成

- 本体　ベンダ名：X 社、製品名：　ExpreZZ 5800/120Lh、型名：　P8100-1132P、DAT 装置　ベンダ名：X 社、製品名：内蔵 DAT（DDS3/4/DAT72）（36GB）、型名：N8151-51A
- 監査者端末、オペレータ端末、個人情報利用者端末、個人情報管理者端末　本体　ベ

ンダ名：X 社、製品名：MaYte MY28V/H-H(XPro)コンパクトタワー型、型名：PC-28VHBE2U8H

- 処理連携サーバ端末　ベンダ名：X 社、製品名：ExpreZZ5800/120Lh、型名：P8100-1132P
- ファイアウォール（ハードウェア）本体　ベンダ名：X 社、製品名：ExpreZZ5800/FW500d、型名：8100-1097、ネットワーク：1000BASE-T（100BASE-TX/10BASE-T 対応）x3 ポート

アプリケーションソフトウェア・構成ツール

- 個人情報処理システムサーバ用アプリケーションソフトウェア：サーバコンソール、サーバセットアップツール、データベースセットアップツール、サーバサブシステム
- 個人情報処理システム連携アプリケーションソフトウェア：中継ツール、メール通知ツール、バックアップ・リカバリツール
- 個人情報処理システムクライアント用アプリケーションソフトウェア：持ち出し制御ツール、暗号ツール

顧客要求

開発コストに関しては，基本機能に対して５千万円、セキュリティ機能に関しては１千万円までとする．　100 万／月の維持コストを前提とした設計とする．

市場動向

「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン（平成 19 年 3 月）　2.法令解釈指針・事例　2-2.個人情報取扱い事業者の義務等　2-2-3.個人データの管理（法第１９条～２２条関連）　2-2-3-2.安全管理措置（法第２０条関連）」に規定される、「講じなければならない事項」を考慮する．

セキュリティ要求

通信教育事業　において、顧客の個人情報の漏えい等、A社が認証取得しているプライバシーマークの要求事項を満たせるように開発する

保護資産の洗い出し結果

TOE の資産は、個人データから成る以下の利用者データである．

- 未登録個人データ（顧客が入力した DB 未登録データ）
- 個人データ（保有個人データ）
- 個人データの提供データ
- 個人データの預託データ
- 個人データの加工データ

・個人データに関する承認依頼データ（登録用）
・個人データに関する承認依頼データ（更新用）
・個人データに関する承認依頼データ（削除用）
・個人データに関する承認依頼データ（提供用）
・個人データに関する承認依頼データ（預託用）

セキュリティコンセプトに対する顧客の承認結果

セキュリティコンセプト検討会　議事録 「A 社個人情報処理システム」におけるセキュリティ機能のセキュリティコンセプトに関して検討を実施。現在のセキュリティコンセプトをもとにシステム要件定義を進めていくことで合意。・・・・・・   A 社システム部長　承認印

評価対象の概要と評価基準の確認結果

評価対象の概要を付録 B の ST 概要に定める
・ST の識別情報
・TOE の識別情報
・TOE 種別及び主要セキュリティ機能
・運用環境
・ハードウェア構成
・ソフトウェア構成
・TOE 利用者役割
・TOE 論理的範囲
・TOE 物理的範囲

評価基準を評価保証レベル 3(EAL レベル 3)とする.

目的：EAL3 は、良心的な開発者が、既存の適切な開発方法を大幅に変更することなく、設計段階で有効なセキュリティエンジニアリングから最大の保証を得られるようにする。EAL3 は、開発者または利用者が、中レベルで独立して保証されたセキュリティを必要とし、大幅なリエンジニアリングを行わずに TOE とその開発の完全な調査を必要とする状況で適用される。

保証コンポーネント

EAL3 は、完全なセキュリティターゲット及びその ST 内の SFR の分析により保証を提供する。この分析は、セキュリティのふるまいを理解するために、機能とインタフェースの仕様、ガイダンス証拠資料、及び TOE の設計のアーキテクチャ記述を使用して行われる。

分析は、TSF の独立テスト、機能仕様及び TOE 設計に基づく開発者テストの証拠、開発者テスト結果の選択的で独立した確認、及び基本的な攻撃能力を持つ侵入攻撃者に対する抵抗力を実証する(提供された機能仕様、TOE 設計、セキュリティアーキテクチャ記述、及びガイダンス証拠に基づく)脆弱性分析によってサポートされる。

また、EAL3 は、開発環境管理の使用、TOE 構成管理の使用、及びセキュアな配付手続きの証拠を通して保証を提供する。この EAL は、セキュリティ機能性のさらに完全なテストカバレージ、及び TOE が開発中に改ざんされないというある程度の信頼を提供するメカニズム及び/または手続きを要求することにより、EAL2 からの有意義な保証の増加を表す。

保証クラス	保証コンポーネント
ADV: 開発	ADV_ARC.1 セキュリティアーキテクチャ記述
	ADV_FSP.3 完全な要約を伴う機能仕様
	ADV_TDS.2 アーキテクチャ設計
AGD: ガイダンス文書	AGD_OPE.1 利用者操作ガイダンス
	AGD_PRE.1 準備手続き
ALC: ライフサイクル サポート	ALC_CMC.3 許可の管理
	ALC_CMS.3 実装表現の CM 範囲
	ALC_DEL.1 配付手続き
	ALC_DVS.1 セキュリティ手段の識別
	ALC_LCD.1 開発者によるライフサイクルモデルの定義
ASE: セキュリティ ターゲット評価	ASE_CCL.1 適合主張
	ASE_ECD.1 拡張コンポーネント定義
	ASE_INT.1 ST 概説
	ASE_OBJ.2 セキュリティ対策方針
	ASE_REQ.2 派生したセキュリティ要件
	ASE_SPD.1 セキュリティ課題定義
	ASE_TSS.1 TOE 要約仕様
ATE: テスト	ATE_COV.2 カバレージの分析
	ATE_DPT.1 テスト: 基本設計
	ATE_FUN.1 機能テスト
	ATE_IND.2 独立テスト - サンプル
AVA: 脆弱性評定	AVA_VAN.2 脆弱性分析

セキュリティ課題定義への承認結果

セキュリティ課題定義報告会　議事録

セキュリティ課題定義に規定された想定脅威分析結果、組織のセキュリティ方針、前提条件をもとに対策を検討していくことで合意。・・・・・・

A 社システム部長　承認印

想定されるセキュリティ対策一覧と評価結果

ID	攻撃種別	損害程度 大/中/小	発生確率 高/中/低	対策名	対策内容	効果 大/中/小	コスト 高/中/低	実施可否 ○/×
1	T.ILLEGAL_LOGON（不正なログオン）	大	中	O.I&A（操作員の識別認証）	TOEは、操作員がTOEを利用する時は必ず識別認証されることを保証し、指定された回数以内に識別認証に成功した操作員のみTOEの利用を許可しなければならない。	大	中	○
2	T.ILLEGAL_LOGON（不正なログオン）	大	中	OE.PASSWORD_MANAGEMENT（操作員によるパスワードの管理）	すべての操作員は、TOEサービスを提供するシステムにアクセスするための認証情報（パスワード）を記憶し、他人に漏らしてはならない。また推測・解析されやすい認証情報（パスワード）を設定してはならず、適正な間隔で変更しなければならない。	大	中	○
3	T.UNAUTHORIZED_ACCESS（不正なアクセス）	大	中	O.ACCESS_CONTROL（アクセスコントロール）	TOEは、操作員または操作員を代行するプロセスに対して、各操作員の種別とその操作対象に応じて設定・付与された権限に従った、保護資産へのアクセスを保証しなければならない。	大	中	○
4	T.UNAUTHORIZED_ACCESS（不正なアクセス）	大	中	O.TAKE_OUT（クライアント端末を経由したTOE外への利用者データの持ち出し禁止）	TOEは、クライアント端末を経由した利用者データのTOE外への持ち出し（保存、印刷）を禁止しなければならない。	大	中	○
5	T.UNAUTHORIZED_ACCESS（不正なアクセス）	大	中	O.AUDIT（監査）	TOEは、特定の事象が発生した場合これを監査証跡として保管しなければならない。監査証跡は、TOEのセキュリティ侵害の事後調査における記録として利用されるため、以下を満たすことが必要となる。 ・監査証跡には、事象の日付・時刻、事象個所、及び事象に責任を持つ主体を含め生成されること。 ・対象となるすべての監査事象を監査証跡として取得すること。 ・監査証跡の改ざんを防御し、これを検出できること。 ・監査証跡は許可された利用者である監査者及びサーバ管理者のみが許可された範囲の利用ができること。	大	中	○
6	T.UNAUTHORIZED_ACCESS（不正なアクセス）	大	中	O.ALERT（アラート）	TOEは、TOEに対するセキュリティ侵害の可能性を検知しなければならない。またセキュリティ侵害の可能性を検知した場合、サーバ管理者及び監査者に対してその可能性について通知しなければならない。	大	中	○
7	T.UNAUTHORIZED_ACCESS（不正なアクセス）	大	中	OE.AUTHORIZATION_SETTING（権限の設定）	組織の責任者は、TOEに関連する権限・役割をもつ操作員として個人情報管理者、サーバ管理者、及び監査者を任命し、それぞれの権限付与の規定が載っている規則を参照して、それに基づいて権限を付与することにより、TOEに対し行える操作を割り当てなければならない。個人情報管理者は、オペレータ、及び個人情報利用者の任命・管理を組織の責任者から委任され、TOEに関連する権限・役割をもつ操作員としてオペレータ、及び個人情報利用者を任命し、それぞれの権限付与の規定が載っている規則を参照して、それに基づいて権限を付与することにより、TOEに対し行える操作を割り当て	大	低	○
8	T.UNAUTHORIZED_ACCESS（不正なアクセス）	大	中	OE.TRUSTED_ROLE（信頼される役割）	組織の責任者は、サーバ管理者、監査者、及び個人情報管理者の役割に適した者を人選し、その上で、それぞれの役割を理解させる。	大	低	○
9	T.UNAUTHORIZED_ACCESS（不正なアクセス）	大	中	OE.TIME_STAMP（高信頼タイムスタンプ）	TOEでは、監査証跡を生成する際、及び利用時間制限を行う際に、高信頼タイムスタンプが利用できなければならない。	大	低	○
10	T.MISUSE（誤操作）	大	中	O.ACCESS_CONTROL（アクセスコントロール）	TOEは、操作員または操作員を代行するプロセスに対して、各操作員の種別とその操作対象に応じて設定・付与された権限に従った、保護資産へのアクセスを保証しなければならない。	大	中	○
11	T.MISUSE（誤操作）	大	中	O.TAKE_OUT（クライアント端末を経由したTOE外への利用者データの持ち出し禁止）	TOEは、クライアント端末を経由した利用者データのTOE外への持ち出し（保存、印刷）を禁止しなければならない。	大	中	○
12	T.MISUSE（誤操作）	大	中	OE.TRAINING（教育・訓練）	すべての操作員は、個人データ及びTOEの安全管理に関する操作員の役割及び責任についての教育・訓練を受けなければならない。	大	低	○
13	T.INJUSTICE（不正行為）	大	中	O.AUDIT（監査）	TOEは、特定の事象が発生した場合これを監査証跡として保管しなければならない。監査証跡は、TOEのセキュリティ侵害の事後調査における記録として利用されるため、以下を満たすことが必要となる。 ・監査証跡には、事象の日付・時刻、事象個所、及び事象に責任を持つ主体を含め生成されること。 ・対象となるすべての監査事象を監査証跡として取得すること。 ・監査証跡の改ざんを防御し、これを検出できること。 ・監査証跡は許可された利用者である監査者及びサーバ管理者のみが許可された範囲の利用ができること。	大	低	○
14	T.INJUSTICE（不正行為）	大	中	O.ALERT（アラート）	TOEは、TOEに対するセキュリティ侵害の可能性を検知しなければならない。またセキュリティ侵害の可能性を検知した場合、サーバ管理者及び監査者に対してその可能性について通知しなければならない。	大	低	○
15	T.INJUSTICE（不正行為）	大	中	O.AVAILABLE_TIME_RESTRICTION	TOEは、管理されたセション確立可能な時間に基づき、セションの確立を制限しなければならない。	大	低	○
16	T.INJUSTICE（不正行為）	大	中	OE.TRUSTED_ROLE（信頼される役割）	組織の責任者は、サーバ管理者、監査者、及び個人情報管理者の役割に適した者を人選し、その上で、それぞれの役割を理解させる。	大	低	○
17	T.INJUSTICE（不正行為）	大	中	OE.TRAINING（教育・訓練）	すべての操作員は、個人データ及びTOEの安全管理に関する操作員の役割及び責任についての教育・訓練を受けなければならない。	大	低	○
18	T.INJUSTICE（不正行為）	大	中	OE.TIME_STAMP（高信頼タイムスタンプ）	TOEでは、監査証跡を生成する際、及び利用時間制限を行う際に、高信頼タイムスタンプが利用できなければならない。	大	中	○
19	T.SPOOFING（なりすまし）	大	中	O.AUTO_LOGOUT（自動ログアウト）	TOEは、TOEにログオンした操作員から、一定時間TOEへのアクセスがないとき、自動的にログアウトを行わなければならない。	大	低	○
20	T.REPUDIATION（事実否認）	小	小	O.NON_REPUDIATION（否認防止）	TOEは、法的に有効なデータを一般利用者との間で送受信する場合は、そのデータの送受信の事実否認を防ぐための手段を提供しなければならない。	中	中	×
21	T.DOS（サービス拒否状態）	中	小	O.DOS（サービス拒否の防止）	TOEのサービスが高頻度で利用された際、TOEは、TOEが誤動作することを防がなければならない。同時接続数の制限、通信量の制限等による対策を想定する。	中	高	×
22	T.DISCLOSE_NW_DATA（ネットワークデータ暴露）	大	中	O.USERDATA_PROTECTION（利用者データの保護）	TOEは、以下のデータを秘匿し、改ざんを検出できなければならず、それぞれに対し許可された操作員や端末のみがデータを利用することができなければならない。 ・サーバ管理者が、バックアップデータを利用することができる。 ・個人情報管理者、及び個人情報利用者が、個人データの提供・預託データを利用することができる。 ・サーバ端末－クライアント端末間で通信される利用者データは、当該端末が利用することができる。	大	中	○
23	T.REMOVABLE_MEDIA（リムーバブル媒体）	中	中	O.USERDATA_PROTECTION（利用者データの保護）	TOEは、以下のデータを秘匿し、改ざんを検出できなければならず、それぞれに対し許可された操作員や端末のみがデータを利用することができなければならない。 ・サーバ管理者が、バックアップデータを利用することができる。 ・個人情報管理者、及び個人情報利用者が、個人データの提供・預託データを利用することができる。 ・サーバ端末－クライアント端末間で通信される利用者データは、当該端末が利用することができる。	大	中	○
24	T.UNEXPECTED_ACCIDENT（不測の事態）	大	中	O.BACKUP_RECOVERY（バックアップ／リカバリ）	TOEは、TOEが正常に動作するために必要な利用者データ及びTSFデータをバックアップする手段を提供しなければならない。また、バックアップした利用者データ及びTSFデータを、TOEの動作を復旧させるためにTOEへリカバリする手段を提供しなければならない。	大	中	○

実施するセキュリティ対策

想定されるセキュリティ対策一覧と評価結果の実施可否欄で○印の対策を実施する.

セキュリティ対策残存リスクへの対処方針

想定されるセキュリティ対策一覧と評価結果の実施可否欄で×印としている O.NON_REPUDIATION（否認防止）と O.DOS（サービス拒否の防止）を実施しないことによる残存リスクに対しては影響度が小さいこととコストが高いため、リスク保有の対処方針とする.

セキュリティ対策残存リスクへの対処方針の承認結果

セキュリティ対策残存リスク検討会　議事録 セキュリティ対策残存リスクへの対処方針について合意。・・・・・・ A 社システム部長　承認印

TOE セキュリティ機能とセキュリティ機能要件の対応関係の検証結果と要約仕様に対する顧客の承認結果

セキュリティ要約仕様等報告会　議事録 セキュリティ要約仕様を元に開発を実施していくことで合意。・・・・・・ A 社システム部長　承認印

付録Ｂ

CC V3.1 対応版

A 社個人情報処理システムアプリケーション
セキュリティターゲット

バージョン：1.0
発行日：　2007 年 8 月 8 日
作成者：X 社

注意事項：
・付録Ｂは、個人情報処理システムアプリケーションの ST 作成時に、参考資料として利用を目的に独立行政法人情報処理推進機構セキュリティセンター情報セキュリティ認証室公開されたセキュリティターゲットである.

・付録Aにおける赤字は 4 章のケーススタディで CC-Case の具体モデル事例の証跡等示される赤字の同じ言葉と対応している．また付録Aの赤字の示す範囲は，赤字以降に後続する青字の範囲とする．前後の文が青字になっている場合、その図・表も直前の赤字の範囲に含まれる.

更新履歴

バージョン	変更概要	変更箇所		変更日	変更者
		章・節・項	内容		
0.7	新規作成	全体	－	2007/4/23	X 社
1.0	レビューに伴う修正・追加	全体	－	2007/8/8	X 社

目次

1. ST 概説 3
1.1. ST 参照 3
1.2. TOE 参照 3
1.3. TOE 概要 3
1.3.1. TOE 種別および主要セキュリティ機能 3
1.3.2. TOE 利用環境 4
1.4. TOE 記述 8
1.4.1. TOE の利用者役割 8
1.4.2. TOE の論理的範囲 10
1.4.3. TOE の物理的範囲 14
2. 適合主張 16
2.1. CC 適合主張 16
2.2. PP 主張、パッケージ主張 16
2.2.1. PP 主張 16
2.2.2. パッケージ主張 16
3. セキュリティ課題定義 17
3.1. 脅威 18
3.1.1. TOE 資産 18
3.1.2. 脅威 19
3.2. 組織のセキュリティ方針 20
3.3. 前提条件 21
4. セキュリティ対策方針 22
4.1. TOE のセキュリティ対策方針 22
4.2. 運用環境のセキュリティ対策方針 24
4.3. セキュリティ対策方針根拠 26
5. 拡張コンポーネント定義 33
5.1. 拡張機能コンポーネント 33
6. セキュリティ要件 35
6.1. セキュリティ機能要件 35
6.2. セキュリティ保証要件 61
6.3. セキュリティ要件根拠 62
6.3.1. セキュリティ機能要件根拠 62
6.3.2. 依存性の検証 69
6.3.3. セキュリティ保証要件根拠 70
7. TOE 要約仕様 71
7.1. TOE セキュリティ機能 71
7.1.1. 監査機能（SF.Audit） 72
7.1.2. 識別認証機能（SF.I&A） 75
7.1.3. 暗号機能（SF.Crypto） 78
7.1.4. バックアップ／リカバリ機能（SF.Import_Export） 80
7.1.5. 操作員管理・アクセス制御機能（SF.ACC） 81
8. 用語・参考資料 87
8.1. 個人情報保護法における用語とその定義内容 87
8.2. 本 ST における用語 88
8.3. 略語・用語 89
8.4. 参考資料 90

1. ST 概説

本章では, ST 参照, TOE 参照, TOE 概要, および TOE 記述について記述する。

1.1. ST 参照

本節では ST の識別情報を記述する。

タイトル : A 社個人情報処理システムアプリケーション セキュリティターゲット
バージョン : 1.0
発行日 : 2007 年 8 月 8 日
作成者 : X 社

1.2. TOE 参照

本節では TOE の識別情報を記述する。

TOE : A 社個人情報処理システムアプリケーション
TOE のバージョン : 1.0
キーワード : 個人情報、個人データ、保有個人データ、システム
開発者 : X 社

1.3. TOE 概要

1.3.1. TOE 種別および主要セキュリティ機能

TOE は、個人情報取扱事業者である A 社事業の一つである通信教育事業において、顧客の個人情報を管理するためのシステム「A 社個人情報処理システム」を構成するアプリケーションソフトウェアであり、基本機能（個人データの登録、更新、閲覧・検索、提供、預託、加工、削除の機能、未登録個人データの外部入力機能、提供・預託データの外部出力機能、及び監査証跡の退避機能）、及び個人データの漏えいを防止、改ざんを検出するためのセキュリティ機能を提供する。

TOE が提供するセキュリティ機能の概要を以下に示す。

［TOE が提供するセキュリティ機能］

監査機能：

TOE の監査証跡を採取し、参照・管理を可能にする

操作員管理・アクセス制御機能：

TOE にアクセスする利用者の管理、および各利用者に付与された権限に基づき TOE へのアクセスを制御する

識別認証機能：

TOE へアクセスする利用者の識別認証、端末の検証、パスワードの品質検証、及びアカウントロックを行う

暗号機能：

サーバ・クライアント間通信の暗号化、バックアップデータの暗号化・復号、及び個人データの提供データ・預託データの暗号化を行う

バックアップ・リカバリ機能：

TOE の復旧に必要なデータのバックアップ／リカバリを行う

1.3.2. TOE 利用環境

1.3.2.1. TOE 運用環境

TOE が稼動する端末と、関連する IT 機器構成を図 1-1 に示す。

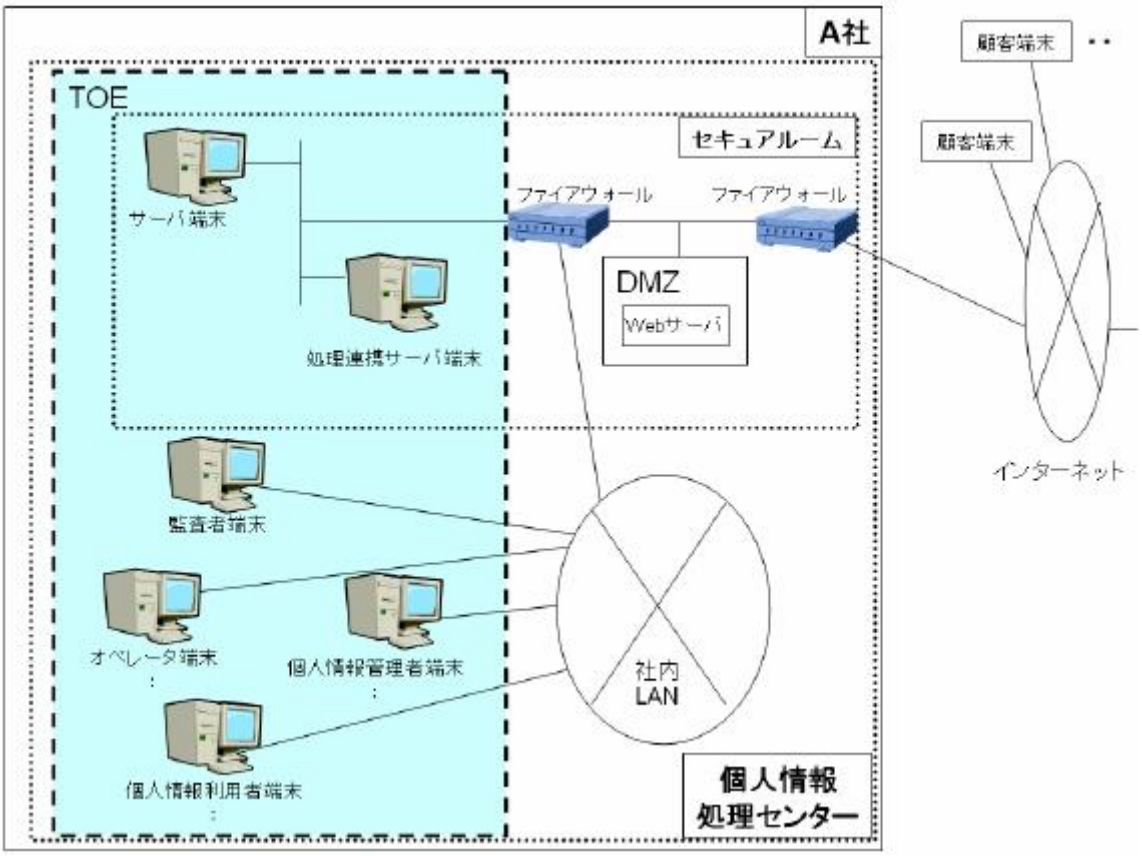


図 1-1 個人情報処理システム運用環境

(1) 物理配置及びネットワーク

A 社の通信教育事業の個人情報処理センターには、複数台のオペレータ端末、複数台の個人情報利用者端末、複数台の個人情報管理者端末、複数台の監査者端末と施錠可能なラック内に収納されているファイアウォール、Web サーバ、サーバ端末、及び処理連携サーバ端末が設置される。TOE の物理的範囲内にある端末は、オペレータ端末、個人情報利用者端末、個人情報管理者端末、サーバ端末、監査者端末、及び処理連携サーバ端末（図 1-1 の破線内）である。

個人情報処理センターは、A 社社員のみが入館できるよう入退館管理された建物に設置されており、個人データを保管するサーバ端末・処理連携サーバ端末は、個人情報処理センターの中で更に物理的に隔てられ別途入退室管理されたセキュアルームで管理される。セキュアルームへは、保管された端末を操作するサーバ管理者、サーバ管理者に許可された者、及び個人情報処理システム以外の機器における管理者等が入室を許可される。サーバ管理者やその他の機器の管理者は、それ以外の者の入室を許可した場合、その者に同行し行動を監視する。

顧客端末から送信されるデータは、インターネット、ファイアウォール、及び Web サーバを経由して処理連携サーバ端末へ格納される。通信内容や Web サーバへの各種攻撃については、ファイアウォールや Web サーバの管理者による各種セキュリティ対策が既に講じられており、安全に通信が行える状態を確保している。また、クライアント端末には個人データを保管しない。

(2) セキュアルームネットワーク

セキュアルーム内のサーバ端末、処理連携サーバ端末のみが接続するネットワークをセキュアルームネットワークと呼ぶ。

(2-1) サーバ端末

サーバ端末は、セキュアルームネットワークに接続される。サーバ管理者が、基本機能の起動／停止、鍵管理、システム環境設定、バックアップ／リカバリ、個人データの提供・預託データの外部出力、監査証跡参照、及び操作員管理を行うために用いる。
基本機能利用者に対しては、役割毎に異なる基本機能を提供し、監査者に対しては、監査証跡参照・監査証跡管理・監査証跡退避機能を提供する。監査証跡を格納するための領域に枯渇の恐れがある時、及び監査対象事象に関して監査者の定めた重要度以上の重要度を含む監査証跡が生成された時には、サーバコンソールにその旨が通知される。また、処理連携サーバ端末のメールサーバを利用して、監査者にその旨を通知する。

(2-2) 処理連携サーバ端末

処理連携サーバ端末は、セキュアルームネットワークに接続される。DMZ 上の Web サーバを経由した顧客端末からの登録・更新・削除依頼を受付、処理連携サーバ端末内の DB に格納する。依頼を受け付けた際にはオペレータにメールで通知する。顧客からの登録・更新・削除依頼に基づくオペレータによる操作により、サーバ端末内の DB を更新する。その際は、オペレータ端末から、サーバ端末経由で処理連携サーバ端末にアクセスする。

(3) 社内 LAN

A 社のネットワークであり、ファイアウォールを介してインターネットと接続されている。セキュアルームネットワークを含み、オペレータ端末、個人情報利用者端末、個人情報管理者端末、及び監査者端末が接続するネットワークである。

(3-1) オペレータ端末

オペレータ端末は、社内 LAN に接続される。オペレータが、個人データを登録、更新、及び削除する際に、オペレータ端末から社内 LAN を介してサーバ端末にアクセスする。

(3-2) 個人情報利用者端末

個人情報利用者端末は、社内 LAN に接続される。個人情報利用者が、個人データを閲覧・検索、A 提供、預託、及び加工する際に、個人情報利用者端末から社内 LAN を介してサーバ端末にアクセスする。

(3-3) 個人情報管理者端末

個人情報管理者端末は、社内 LAN に接続される。個人情報管理者が、個人データを閲覧・検索する際、オペレータ・個人情報利用者の操作を承認する際、操作員管理を行う際に、個人情報管理者端末から社内 LAN を介してサーバ端末にアクセスする。

(3-4) 監査者端末

監査者端末は、社内 LAN に接続される。監査者が監査証跡参照、監査証跡管理、及び監査証跡退避を行う際に、監査者端末から社内 LAN を介してサーバ端末にアクセスする。監査証跡を格納するための領域に枯渇の恐れがある時、及び監査対象事象に関して監査者の定めた重要度以上の重要度を含む監査証跡が生成された時には、その

旨を警告するメールをサーバ端末から受信する。

1.3.2.2. ハードウェア構成

表 1-1 に、TOE の動作環境としてのハードウェア構成を示す。TOE は、表 1-1 を満たす動作環境で、正しく確実に動作する。尚、表 1-1 中の端末名に関しては、図 1-1 を参照されたい。

表1-1 ハードウェア構成

端末・装置名	種別	説明
サーバ端末		
本体	ベンダ名	X 社
	製品名	ExpreZZ 5800/120Lh
	型名	P8100-1132P
	CPU	64 ビット インテリ eXeon プロセッサ（3.20 GHz）
	メモリ	1GB
	HDD	73.2GB × 3
DAT 装置	ベンダ名	X 社
	製品名	内蔵 DAT（DDS3/4/DAT72）（36GB）
	型名	N8151-51A
監査者端末、オペレータ端末、個人情報利用者端末、個人情報管理者端末		
本体	ベンダ名	X 社
	製品名	MaYte MY28V/H-H(XPro)コンパクトタワー型
	型名	PC-28VHBE2U8H
	CPU	インテリ ePentiumⅣプロセッサ（2.80 GHz）
	メモリ	512MB
	HDD	80GB
処理連携サーバ端末		
本体	ベンダ名	X 社
	製品名	ExpreZZ5800/120Lh
	型名	P8100-1132P
	CPU	64 ビット インテリ eXeon プロセッサ（3.20 GHz）
	メモリ	1GB
	HDD	73.2GB × 3
ファイアウォール（ハードウェア）		
本体	ベンダ名	X 社
	製品名	ExpreZZ5800/FW500d
	型名	8100-1097
	ネットワーク	1000BASE-T（100BASE-TX/10BASE-T 対応）x3 ポート

1.3.2.3. ソフトウェア構成

表 1-2 に、TOE のソフトウェア構成を示す。TOE は表 1-2 に識別されたソフトウェア構成によって、正しく確実に動作する。尚、表 1-2 中の端末名に関しては、図 1-1 を参照されたい。

表 1-2 ソフトウェア構成

端末名		
ベンダ名	製品名	備考
サーバ端末		
JISEC 社	JISEC Server 2006, Enterprise Edition; SP1	オペレーティングシステム
JISEC 社	Mailer Express 6.0	メールクライアント
JISEC 社	JISEC Database 10g Release 1(10.1.0)	DBMS
C 社	アンチウイルスソフト	ウイルス対策ソフト
X 社	個人情報処理システムサーバ用アプリケーションパッケージ V1.0	TOE の運用管理に必要となる、サーバ端末用アプリケーションパッケージ
監査者端末、オペレータ端末		
JISEC 社	JISEC XP, Pro; SP2	オペレーティングシステム
JISEC 社	Mailer Express 6.0	メールクライアント
C 社	アンチウイルスソフト	ウイルス対策ソフト
X 社	個人情報処理システムクライアント用アプリケーションパッケージ V1.0	基本機能を利用するための、個人情報処理システムクライアント（オペレータ、個人情報利用者、個人情報管理者、監査
個人情報利用者端末、個人情報管理者端末		
JISEC 社	JISEC XP, Pro; SP2	オペレーティングシステム
C 社	アンチウイルスソフト	ウイルス対策ソフト
X 社	個人情報処理システムクライアント用アプリケーションパッケージ V1.0	基本機能を利用するための、個人情報処理システムクライアント（オペレータ、個人情報利用者、個人情報管理者、監査者）用アプリケーションパッケージ
処理連携サーバ端末		
JISEC 社	JISEC Server 2006, Enterprise Edition; SP1	オペレーティングシステム
JISEC 社	JISEC Database 10g Release 1(10.1.0)	DBMS
JISEC 社	Mailer Express 6.0	メールクライアント
C 社	アンチウイルスソフト	ウイルス対策ソフト
X 社	個人情報処理システム連携アプリケーションパッケージ V1.0	DMZ 上の Web サーバから受信する顧客端末からのデータを、サーバ端末へ中継するための、処理連携サーバ端末用アプリケーションパッケージ

1.4. TOE 記述

本章では TOE の利用者役割、TOE の論理的範囲、および TOE の物理的範囲について記述する。

1.4.1. TOE の利用者役割

TOE で使用される各端末における利用者（以降、操作員と呼ぶ）の役割は以下のとおりである。操作員は、サーバ管理者、監査者、個人情報管理者、オペレータ、及び個人情報利用者のいずれかの操作員種別に分類され、操作員種別毎に付与された権限の範囲の業務を行うことができる。

（1）サーバ管理者

サーバ端末・処理連携サーバ端末の管理者となる。サーバ端末・処理連携サーバ端末に直接ログインできる権限を有する操作者である。サーバ管理者自身は、個人データの登録、更新、削除、閲覧・検索、提供、預託、及び加工を行わず、次の業務を行う。

- 基本機能の起動／停止
- 鍵管理（サーバ共通鍵・処理連携サーバ共通鍵・サーバ公開鍵・サーバ秘密鍵の生成・更新・削除、提供・預託先公開鍵のインポート・削除）
- システム環境設定（パスワード試行回数の管理、バナー表示メッセージの管理、操作員種別ごとのセション確立許可時間帯の管理）
- バックアップ／リカバリ
- 個人データの提供・預託データの外部出力
- 監査証跡参照
- 操作員管理（サーバ管理者、監査者、個人情報管理者の管理）

組織の責任者が、A 社通信教育事業部門員の中から適任者を厳重に人選し、サーバ管理者として任命する。

なおサーバ管理者は、自身の役割をサーバ端末、及び処理連携サーバ端末においてのみ実施することができる。

（2）監査者

監査者端末より、サーバサブシステム（詳細は、「1.3.2.3 ソフトウェア構成」で述べる。）が生成する監査証跡を検査する操作者である。監査者には、以下の権限のみが付与され、監査者自身は、個人データの登録、閲覧・検索、提供、預託、加工、更新、及び削除を行わず、次の業務を行う。

- 監査証跡参照
- 監査証跡管理
- 監査証跡退避

組織の責任者が、A 社通信教育事業部門員の中から適任者を厳重に人選し、監査者として任命する。

なお監査者は、自身の役割をクライアント端末においてのみ実施することができる。

（3）個人情報管理者

個人情報管理者端末より、個人情報の管理を行う権限を与えられた操作者である。個人情報を管理するため、以下の 3 つの操作を行う。

- 個人データの閲覧・検索
- オペレータ・個人情報利用者の操作の承認

・操作員管理（オペレータ、個人情報利用者の管理）

組織の責任者が、A 社通信教育事業部門員（管理職）の中から適任者を選出し、個人情報管理者として任命する。オペレータ・個人情報利用者の選出を委任される。

なお個人情報管理者は、自身の役割をクライアント端末においてのみ実施することができる。

（4）オペレータ

オペレータ端末より、個人データの登録、更新、及び削除を行う権限を与えられた操作者である。

個人データの登録、更新、及び削除にあたっては、オペレータは、個人情報管理者の承認を得るためのデータ（個人情報に関する承認依頼データ（登録用）（更新用）（削除用））を作成する。オペレータが作成したデータは、個人情報管理者が承認することにより反映される。

また、顧客端末からの個人情報登録・更新・削除依頼に対し、処理連携サーバ端末が依頼を受領した旨のメールをオペレータへ送信後、オペレータはサーバ端末を経由して、処理連携サーバ端末 DB 上の未登録個人データを、サーバ端末 DB に格納する。

個人情報管理者が、A 社通信教育事業部門員の中から適任者をオペレータとして選出する。

なおオペレータは、自身の役割をクライアント端末においてのみ実施することができる。

（5）個人情報利用者

個人情報利用者端末より、個人データの閲覧・検索、提供、預託、及び加工を行う権限を与えられた操作者である。

個人データの提供、及び預託にあたっては、個人情報利用者は、個人情報管理者の承認を得るためのデータ（個人データに関する承認依頼データ（提供用）（預託用））を作成する。個人情報利用者が作成したデータを個人情報管理者が承認することにより、当該データは暗号化され、サーバ端末 DB 上に個人データを提供・預託するためのデータ（個人データの提供データ、個人データの預託データ）として生成される。

個人情報管理者が、A 社通信教育事業部門員の中から適任者を個人情報利用者として選出する。

なお個人情報利用者は、自身の役割をクライアント端末においてのみ実施することができる。

また、TOE を直接操作することはないが、関連する者を挙げる。

（6）組織の責任者

A 社通信教育事業部において、サーバ管理者、監査者、及び個人情報管理者を厳重に人選し、それぞれの役割を理解させた上で任命する者。個人情報管理者には、オペレータ、及び個人情報利用者の人選、管理を委任する。組織の責任者は、TOE にはアクセスしない。

A 社通信教育事業部長が担当する。

1.4.2. TOE の論理的範囲

本 TOE は、顧客の個人情報の登録、更新、閲覧・検索、提供、預託、加工、及び削除を行うためのシステムである。A 社個人情報処理システムの利用イメージを図 1-2 に示す。

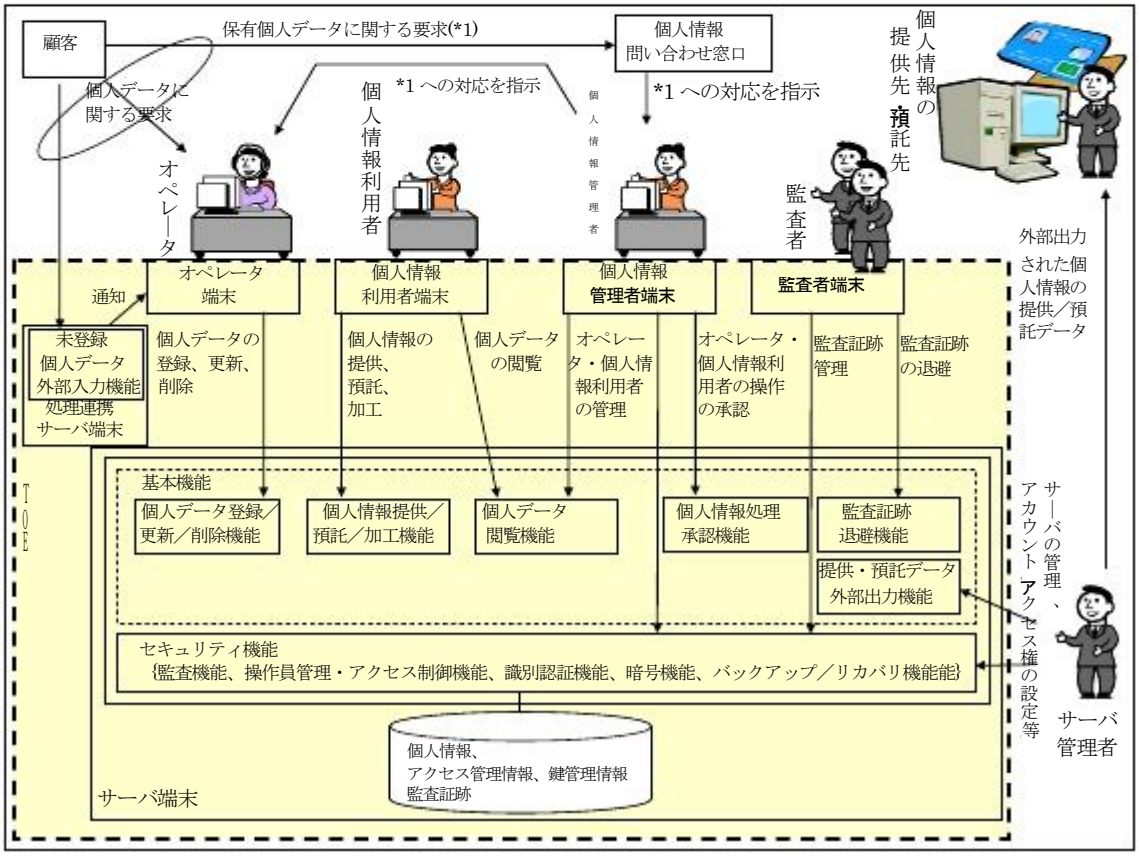


図 1-2　A 社個人情報処理システムの利用イメージ

A 社個人情報処理システムで提供される機能は大別すると以下のように分類される。

(1) 基本機能

1. 個人情報処理メイン機能
   個人データ登録、更新、及び削除に関する機能、
   個人データ閲覧・検索に関する機能、
   個人データ提供、預託、及び加工に関する機能、
   個人情報処理承認に関する機能
2. 未登録個人データ外部入力機能
3. 提供・預託データ外部出力機能
4. 監査証跡退避機能

(2) セキュリティ機能

監査機能、操作員管理・アクセス制御機能、識別認証機能、暗号機能、及びバックアップ／リカバリ機能

1.4.2.1 節、1.4.2.2 節に述べる機能はすべて、TOE の範囲内である。

1.4.2.1. TOE によって提供される基本機能

表 1-3 は、TOE が提供する基本機能である、個人情報処理メイン機能、未登録個人デ

ータ外部入力機能、提供・預託データ外部出力機能、及び監査証跡退避機能についてその概要を記す。

表 1-3　TOE によって提供される基本機能

機能	概要
個人データ登録に関する機能	オペレータが、個人情報登録用のデータを生成し、個人情報管理者に承認を依頼する。個人情報管理者に承認されると、データが DB に登録される。
個人データ更新に関する機能	オペレータが、個人情報更新用のデータを生成し、個人情報管理者に承認を依頼する。個人情報管理者に承認されると、DB 上のデータが更新される。
個人データ削除に関する機能	オペレータが、個人情報削除用のデータを生成し、個人情報管理者に承認を依頼する。個人情報管理者に承認されると、DB 上のデータが削除される。
個人データ閲覧・検索に関する機能	個人情報利用者、個人情報管理者が、個人データ、及び個人データの加工データを閲覧・検索する。
個人データ提供に関する機能	個人情報利用者が、個人データ提供用のデータを生成し、個人情報管理者に承認を依頼する。個人情報管理者に承認されると、データは暗号化され、サーバ管理者に外部出力が依頼される。
個人データ預託に関する機能	個人情報利用者が、個人データ預託用のデータを生成し、個人情報管理者に承認を依頼する。個人情報管理者に承認されると、データは暗号化され、サーバ管理者に外部出力が依頼される。
個人データ加工に関する機能	個人情報利用者が、個人データを複写・加工する。
個人情報処理承認に関する機能	個人情報管理者が、オペレータ・個人情報利用者の操作を承認する。
未登録個人データ外部入力機能	顧客から送信されたデータを DMZ 上の Web サーバで未登録個人データとして生成し、これを処理連携サーバ端末へインポートする。
提供・預託データ外部出力機能	サーバ管理者が、暗号化された提供・預託データを TOE 外へエクスポートする。
監査証跡退避機能	監査者が、監査証跡を TOE 外へエクスポート、TOE 内へインポートする。

1.4.2.2. TOE によって提供されるセキュリティ機能

(1) 監査機能

TOE は、安定的な稼動維持、セキュリティ侵害の検知のために、自身の監査証跡を生成する。ただし、監査証跡に含まれるタイムスタンプは、TOE 範囲外である OS により提供される。

＜アプリケーションの監査証跡＞

サーバ管理者、及び監査者は、監査証跡参照機能、及び監査証跡管理機能を使用して、アプリケーションの監査機能により採取・管理される監査証跡を使用する。

・監査証跡参照機能：

監査証跡の参照及び検索を行うための機能。サーバ管理者、及び監査者が利用可能。

・監査証跡管理機能：

DB 上の監査証跡の削除を手動で行うための機能。監査証跡格納領域の枯渇の恐れがある場合に警告を発信する機能。セキュリティ侵害の可能性を検知するための機能。

- DB 上の監査証跡の削除は、監査者のみが利用可能。
- 監査証跡を格納するための領域に枯渇の恐れがある時、及び監査対象事象に関して監査者の定めた重要度以上の重要度を含む監査証跡が生成された時には、その旨をサーバコンソールに通知するとともに、監査者へメールにより通知する。
- 監査証跡を格納するための領域が枯渇した場合は、領域の枯渇、及び作成日時が古い監査証跡から順番に削除する旨をサーバコンソールに通知するとともに、監査者へメールにより通知する。その上で、監査証跡の作成日時が古いものから順番に削除し、最新の監査証跡を生成する。
- セキュリティ侵害の可能性を検知するため、すべての監査対象事象に対して重要度を設定する。設定された重要度以上の監査証跡が生成された場合、サーバ管理者と監査者に通知する。

(2) 操作員管理・アクセス制御機能

TOE にアクセスする操作員の登録・削除・情報管理を行う。操作員管理を行うことができるのは、サーバ管理者及び個人情報管理者のみである。管理対象とできる操作員は、以下のとおりである。

・サーバ管理者が管理する操作者：サーバ管理者、監査者、及び個人情報管理者
・個人情報管理者が管理する操作者：オペレータ、及び個人情報利用者

管理できる情報は、識別認証機能によって利用される操作員 ID 及びパスワードである。操作員 ID は、アクセス制御機能にも利用される。

サーバ管理者の ID・パスワードの登録は、個人情報処理システムサーバ用アプリケーションパッケージのセットアップ時にサーバ管理者自身が行う。サーバ管理者は、サーバ管理者の ID・パスワードの作成や、ID の削除は可能だが、TOE には必ず 1 名以上のサーバ管理者が存在する必要がある。

TOE の利用者役割に付与された権限に基づき、TOE へのアクセスを制御する。TOE に対してある一定の時間何の操作もしなかった場合には、対話セションを終了する。また、業務時間外に個人データを操作するのを防ぐため、利用時間帯を制限することができる。利用時間帯は、サーバ管理者のみが設定できる。クライアント操作員による個人データの持ち出し（サーバ端末以外への保存、画面コピー、印刷）を禁止する。

(3) 識別認証機能

TOE へアクセスする操作員の識別認証、端末の検証、パスワードの品質の検証、及びアカウントロックを行う。

クライアント操作員の識別認証では、以下のすべてが成功しなければならない。

1. 勧告的警告メッセージの表示
2. セション鍵の生成
3. クライアント端末用パッケージの正当性検証
4. クライアント操作員の ID・パスワード認証

「クライアント端末用パッケージの正当性検証」では、クライアント端末がサーバ端末に対し、自身にインストールされる個人情報処理システムクライアント用アプリケーションパッケージが正当なものであることを証明する。

サーバ管理者の識別認証では、以下のすべてが成功しなければならない。

1. 勧告的警告メッセージの表示
2. サーバ管理者の ID・パスワード認証

操作員のパスワードの品質は、低レベルの攻撃エージェントを想定した機能強度を持

つことが検証される。
サーバ管理者が設定するパスワード試行回数以上、連続してパスワードを誤入力すると当該アカウントはロックされる。

(4) 暗号機能

サーバ端末と、クライアント端末間通信の暗号化、バックアップデータの暗号化・復号、及び個人データの提供データ・預託データの暗号化を行う。また暗号鍵の生成・インポート・破棄を行う。

＜暗号鍵の種別＞

・サーバ共通鍵：サーバ端末のバックアップデータの暗号操作に利用する。
・処理連携サーバ共通鍵：処理連携サーバ端末のバックアップデータの暗号操作に利用する。
・サーバ秘密鍵／公開鍵：サーバ端末ークライアント端末間の通信データの暗号操作に利用する。また、個人情報処理システムクライアント用アプリケーションパッケージ実行コードのハッシュ値に対する暗号操作に利用する。
・提供・預託先共通鍵：提供・預託データの暗号操作に利用する。

＜暗号化の対象となるデータ＞

・バックアップデータ
・通信データ（利用者データ）
・個人データの提供・預託データ

(5) バックアップ／リカバリ機能

TOE の障害に備えて、システムの復旧に必要なデータのバックアップを手動で行う。障害が発生した場合には、バックアップデータをリカバリすることにより TOE を復旧する。バックアップにおいては、DB のイメージコピーが作成される。

本機能は、不測の事態に運用を続けるためのデータのバックアップを目的とする。セキュリティ事故発生時の解析を行うことを目的とした監査証跡のバックアップには、基本機能における監査証跡退避機能が適している。

1.4.3. TOE の物理的範囲

図 1-3 の破線内に示されるコンポーネントが TOE の物理的範囲内である。

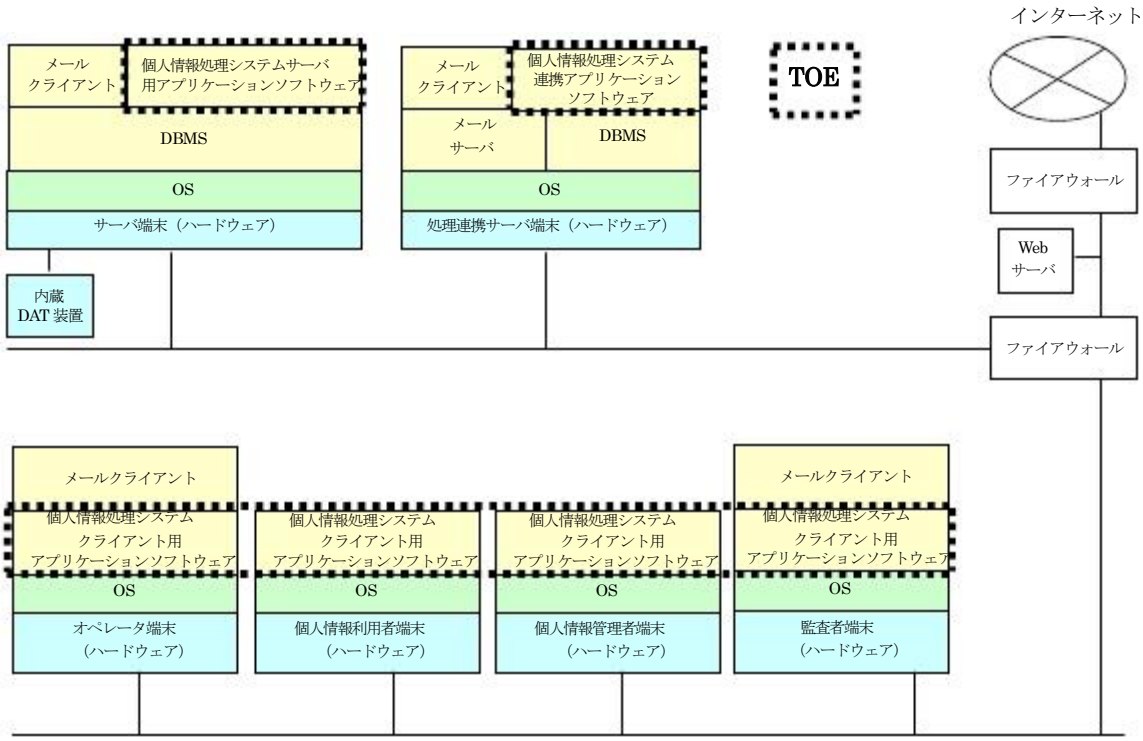


図 1-3　TOE 物理的範囲

図 1-3 に示した TOE を構成する各ツール、およびプログラムを以下に示す。

個人情報処理システムサーバ用アプリケーションソフトウェア：

サーバコンソール：

個人情報処理システムにおけるサーバを管理するために使われる GUI（グラフィカルユーザインタフェース）から構成される。システム管理 GUI、サーバセットアップツール、及びデータベースセットアップツールがある。

システム管理 GUI：基本機能、操作員管理機能、監査証跡参照機能、及びバックアップ／リカバリ機能についての GUI を提供する。

サーバセットアップツール：

新規の個人情報処理システムのサーバをセットアップする。サーバのセットアップでは、監査証跡の最大容量の設定、個人情報処理システムサーバ用アプリケーションパッケージの管理者（サーバ管理者）の登録、及びサーバ公開鍵・秘密鍵の生成が行われる。

データベースセットアップツール：

サーバサブシステムからアクセスする各種データベースを作成する。このツールは、サーバセットアップに先立って実行される。

サーバサブシステム：

以下の機能を提供する。

基本機能、監査機能、操作員管理・アクセス制御機能、識別認証機能、暗号機能、及びバックアップ／リカバリ機能（1.4.2.2 節参照）。

個人情報処理システム連携アプリケーションソフトウェア：

中継ツール：

顧客が行うインターネットを経由した個人情報の登録・更新・削除要求に対して、DMZ 上の Web サーバから送信されてくるデータを受信し、処理連携サーバ端末の DB に格納する。さらに、オペレータの操作によってサーバ端末の DB に反映させる。

メール通知ツール：

DMZ 上の Web サーバから受信したデータが、処理連携サーバ端末の DB に格納される都度、その旨をオペレータにメールで通知する。通知メールには、個人情報は含まれない。

バックアップ・リカバリツール：

処理連携サーバ端末上の DB をバックアップする。また、バックアップしたデータをリカバリする。

個人情報処理システムクライアント用アプリケーションソフトウェア：

持ち出し制御ツール：

個人データの持ち出しを制御する（個人データのクライアント端末・ネットワークドライブへの保存、画面コピーの禁止、印刷の禁止）。

暗号ツール：

サーバ端末との通信時に、通信データの暗号化/復号を行う。

※パッケージには、サーバ端末のセットアップ時に作成されたサーバ公開鍵が含まれる。サーバ公開鍵は、持ち出し制御ツールと同時にクライアント端末にインストールされる。

また、本 TOE を構成するガイダンス文書は以下の通りである。

- 個人情報処理システム インストールガイダンス [IGD0001 20070601]
- 個人情報処理システム 管理者ガイダンス [ADM0001 20070601]
- 個人情報処理システム 利用者ガイダンス [USR0001 20070601]

2. 適合主張

2.1. CC 適合主張

本 ST および TOE の CC 適合主張は，以下のとおりである.
ST と TOE が適合を主張する CC のバージョン：

パート 1:概説と一般モデル 2006 年 9 月 バージョン 3.1 翻訳第 1.2 版
パート 2:セキュリティ機能コンポーネント 2006 年 9 月 バージョン 3.1 翻訳第 1.2 版
パート 3:セキュリティ保証コンポーネント 2006 年 9 月 バージョン 3.1 翻訳第 1.2 版

CC パート 2 に対する ST の適合 ：CC パート 2 拡張
CC パート 3 に対する ST の適合 ：CC パート 3 適合

2.2. PP 主張、パッケージ主張

2.2.1. PP 主張

本 ST が適合している PP はない。

2.2.2. パッケージ主張

EAL3 適合

3. セキュリティ課題定義

本章では、脅威、組織のセキュリティ方針、前提条件について記述する。
まず始めに、TOE のセキュリティに対する考え方について示す。
TOE に対する攻撃を行う者について、以下のとおり想定する。
1.4.1 節で識別された人物のうち、TOE を管理する立場にあるサーバ管理者、監査者、及び個人情報管理者においては、信頼できる人物であり攻撃することは想定されない。ただし、意図せず TOE に対する攻撃となり得る操作を行うことは考えられる。一方、基本機能利用者のうち、個人情報利用者、及びオペレータにおいては、管理状態にない場合、不正な行為を行うことが想定される。また、サーバ管理者によりセキュアルームに入室が許可された者は、サーバ管理者にその行動が監視されるため、物理的な手法による攻撃は想定されない。
その他、攻撃が想定される者（以下、攻撃者と示す。）は、高度な専門知識を持たない、1.4.1 節で識別された人物以外の者である。
これらの攻撃を行う者の主な動機としては、個人情報を入手することによって利益を得ることや、A 社の業務妨害を目的として個人データを改ざん・破壊することが考えられる。

- 機密性：保護資産である個人データは、顧客情報であり、故意・過失によらず暴露された時の影響は多大なものとなり、顧客からの信頼を損なう恐れがある。攻撃者は、社内 LAN 経由、または操作員の不在時に直接 TOE を利用することが考えられる。一方、リムーバブル媒体によって TOE より持ち出されたデータの盗難や紛失、ネットワークにおける伝送中データの取得による暴露が考えられる。よって、これらの TOE へのアクセスに関する機密性について考慮した。
- 完全性：保護資産である個人データは、顧客情報でありサービス提供のために重要となる。顧客情報の改ざんやデータの紛失によって、顧客からの信頼を損なう恐れがある。攻撃者は、社内 LAN 経由による利用や、正当な操作員の不在時に直接 TOE を利用することが考えられる。また、顧客情報が保存されたリムーバブル媒体の紛失や、不正に改ざんされることが考えられる。一方、操作員の誤操作による顧客情報の改ざん、紛失が考えられる。よって、これらの改ざん、紛失に関する完全性について考慮した。
- 可用性：TOE はミッションクリティカルなシステムではないので、システムの二重化は考慮しない。また、システム構成上、DoS 攻撃については考慮不要である。一方、天災等によるデータ紛失によって、顧客情報が失われることは、以後のサービス提供に重大な影響を及ぼすため、データ紛失時にも確実に復旧できる必要がある。よって、不測の事態からの復旧が不可能とならないよう可用性について考慮した。
- 責任追跡性：事件・事故時の原因究明や証拠保存のため、個人データの処理は誰が行ったのか、その処理の主体にたどるための記録の採取が必要となる。よって、TOE への操作に対する責任追跡性について考慮した。
- 真正性：保護資産である個人データの受渡しが発生するのは、顧客から個人情報の提供を受ける際と、第三者に個人データを提供・預託する業務となる。顧客から個人情報の提供を受ける際、本人確認に関しては TOE の管理外であり、真正性については考慮不要である。提供・預託業務については、業務として真正性を要求する必要はないため、真正性については考慮不要である。
- 信頼性：TOE の意図した動作と結果に整合性を持たせるため、外部からの不正なプログラムや、ソフトウェアの既知の脆弱性による意図しない結果が生じないよう、システムの信頼性について考慮した。

3.1. 脅威

3.1.1. TOE 資産

本 TOE の資産は、個人データから成る以下の利用者データである。

- 未登録個人データ（顧客が入力した DB 未登録データ）
- 個人データ（保有個人データ）
- 個人データの提供データ
- 個人データの預託データ
- 個人データの加工データ
- 個人データに関する承認依頼データ（登録用）
- 個人データに関する承認依頼データ（更新用）
- 個人データに関する承認依頼データ（削除用）
- 個人データに関する承認依頼データ（提供用）
- 個人データに関する承認依頼データ（預託用）

TSF データには、以下のようなデータがある。

- 識別・認証情報
- バナー表示メッセージ
- アクセスコントロール情報
- 監査証跡
- セキュリティ侵害の可能性を判断するために用いる監査証跡の重要度
- 操作員の最後に成功した認証以降の不成功認証試行回数
- 操作員種別毎のセション確立許可時間帯
- 暗号鍵

顧客が送信した未登録個人データは処理連携サーバ端末の DB に、これ以外の資産はすべてサーバ端末の DB に保存され、TOE による保護対象となる。

上記の他、バックアップデータ（上記利用者データ、TSF データ）が TOE による保護対象資産である。バックアップデータ、及び提供・預託データが保存されたリムーバブル媒体は、不正に持ち出されないよう保管されるので、バックアップ媒体中のデータの完全性・機密性はセキュアルームに設置されるサーバ端末の DB 内のデータと同等で十分である。

以降、特に断りのない限り、利用者データ、TSF データ、及びバックアップデータは上記で記述した内容を指すものとする。

また、TOE が保護する個人データは、TOE の範囲内で管理された電子データに限り、TOE に登録される前などの紙媒体による個人データに関しては保護の対象とならない。考えられる脅威についても同様である。

3.1.2. 脅威

T.ILLEGAL_LOGON（不正なログオン）
攻撃者が、TOE の正当な利用者になりすまして TOE を利用することにより、利用者データを破壊・改ざん・暴露するかもしれない。

T.UNAUTHORIZED_ACCESS（不正なアクセス）
TOE（クライアント端末）の正当な基本機能利用者のうち、個人情報利用者、及びオペレータが、故意に許可されていない操作（生成、参照、更新、削除、印刷、及び保存）を行うことにより、利用者データを破壊・改ざん・暴露するかもしれない。

T.MISUSE（誤操作）
TOE で利用される各端末の正当な操作員が、誤操作により利用者データを破壊・改ざん・暴露するかもしれない。

T.INJUSTICE（不正行為）
TOE（クライアント端末）の正当な基本機能利用者のうち、個人情報利用者、及びオペレータが、業務時間外など明らかに管理状態にない場合、TOE を利用し利用者データを暴露するかもしれない。

T.SPOOFING（なりすまし）
個人情報利用者、オペレータ、及び攻撃者が、TOE（クライアント端末）の正当な基本機能利用者の離席時にクライアント端末を利用して、利用者データを破壊・改ざん・暴露するかもしれない。

T.DISCLOSE_NW_DATA（ネットワークデータ暴露）
個人情報利用者、オペレータ、及び攻撃者が、サーバ端末とクライアント端末間のネットワーク上でやりとりされる通信データを、不正に入手することで利用者データを改ざん・暴露するかもしれない。

T.REMOVABLE_MEDIA（リムーバブル媒体）
個人情報利用者、オペレータ、及び攻撃者が、バックアップデータ、及び提供･預託データが保存されたリムーバブル媒体を不正に入手することで利用者データを改ざん・暴露するかもしれない。

T.UNEXPECTED_ACCIDENT（不測の事態）
火災、天災、ディスク障害、その他の不測の事態により、TOE の動作のために必要なデータが失われるかもしれない。

3.2. 組織のセキュリティ方針

TOE が従うべき事項として、「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン（平成 19 年 3 月） 2.法令解釈指針・事例 2-2.個人情報取扱い事業者の義務等 2-2-3.個人データの管理（法第１９条～２２条関連） 2-2-3-2.安全管理措置（法第２０条関連）」に規定される、「講じなければならない事項」を考慮する。

P.SAFE_PLACE（安全な建物）
TOE に関連するハードウェア（オペレータ端末、個人情報利用者端末、個人情報管理者端末、サーバ端末、監査者端末、処理連携サーバ端末）は、A 社社員のみが入館できる建物内に設置され、個人データを取り扱う業務は、同所にて実施する。
[ガイドライン]の規程（物理的安全管理措置【各項目について講じることが望まれる事項】①入退館（室）管理を実施する上で望まれる事項：個人データを取り扱う業務上の、入退館（室）管理を実施している物理的に保護された室内での実施）を参考とする。

P.FACILITIES_IN_SECURE_ROOM（セキュアルームへの機器設置）
個人データが格納されている HDD は簡単に取り外されないように保護し、バックアップデータや外部出力された提供・預託データは権限のない者に持ち去られることがないように保護するため、個人データが保存される機器は許可された信頼できる者、または許可された者に認められその行動が監視される者のみが入室できる物理的に隔てられた場所に設置する。
[ガイドライン]の規程（物理的安全管理措置【各項目について講じることが望まれる事項】①入退館（室）管理を実施する上で望まれる事項：個人データを取り扱う情報システム等の、入退館（室）管理を実施している物理的に保護された室内等への設置）を参考とする。

P.NETWORK（ネットワーク環境）
社内 LAN とインターネットとは、外部からの不正な侵入を防ぐ装置なしでの接続は許可しない。また、セキュアルームネットワークは、アプリケーションの機能に必要な通信以外の通過を禁止された特定箇所で社内 LAN に接続する。
[ガイドライン]の規程（技術的安全管理措置【各項目について講じることが望まれる事項】②個人データへのアクセス制御を行う上で望まれる事項：個人データを格納した情報システムへの無権限アクセスからの保護）を参考とする。

P.UNJUST_SOFTWARE（不正ソフトウェア対策）
TOE に関連するハードウェア（オペレータ端末、個人情報利用者端末、個人情報管理者端末、サーバ端末、監査者端末、処理連携サーバ端末）は、ウイルス対策ソフトウェアを導入されるとともに、ウイルス対策ソフトウェアのパターンファイルやセキュリティ対策用修正ソフトウェアが適切に適用される。
[ガイドライン]の規程（技術的安全管理措置【各項目について講じることが望まれる事項】⑤個人データを取り扱う情報システムについて不正ソフトウェア対策を実施する上で望まれる事項：ウイルス対策ソフトウェアの導入。オペレーティングシステム（ＯＳ）、アプリケーション等に対するセキュリティ対策用修正ソフトウェア（いわゆる、セキュリティパッチ）の適用。不正ソフトウェア対策の有効性・安定性の確認（例えば、パターンファイルや修正ソフトウェアの更新の確認））を参考とする。

P.RECOMMEND（勧告）
TOE を使用するにあたって、あらかじめ不正な使用に関する勧告的警告メッセージを表示し、すべての利用者に対し不正な使用に関して注意喚起する必要がある。

3.3. 前提条件

本 TOE は、特定される環境において特定の業務を行うためのものである。
本 TOE を利用するにあたり必要な条件は、「1.3.2　TOE 利用環境」に示されており、それ以外の条件、及び利用にあたり想定される条件(未確定事項)はない。

4. セキュリティ対策方針

本章では TOE のセキュリティ対策方針、運用環境のセキュリティ対策方針、およびセキュリティ対策方針根拠について記述する。

4.1. TOE のセキュリティ対策方針

O.I&A（操作員の識別認証）
TOE は、操作員が TOE を利用する時は必ず識別認証されることを保証し、指定された回数以内に識別認証に成功した操作員のみ TOE の利用を許可しなければならない。

O.ACCESS_CONTROL（アクセスコントロール）
TOE は、操作員または操作員を代行するプロセスに対して、各操作員の種別とその操作対象に応じて設定･付与された権限に従った、保護資産へのアクセスを保証しなければならない。

O.TAKE_OUT（クライアント端末を経由した TOE 外への利用者データの持ち出し）
TOE は、クライアント端末を経由した利用者データの TOE 外への持ち出し（保存、印刷）を禁止しなければならない。

O.AUDIT（監査）
TOE は、特定の事象が発生した場合これを監査証跡として保管しなければならない。監査証跡は、TOE のセキュリティ侵害の事後調査における記録として利用されるため、以下を満たすことが必要となる。
・監査証跡には、事象の日付・時刻、事象個所、及び事象に責任を持つ主体を含め生成されること。
・対象となるすべての監査事象を監査証跡として取得すること。
・監査証跡の改ざんを防御し、これを検出できること。
・監査証跡は許可された利用者である監査者及びサーバ管理者のみが許可された範囲の利用ができること。

O.ALERT（アラート）
TOE は、TOE に対するセキュリティ侵害の可能性を検知しなければならない。またセキュリティ侵害の可能性を検知した場合、サーバ管理者及び監査者に対してその可能性について通知しなければならない。

O.RECOMMEND（勧告）
TOE は、利用者セション確立前に、TOE の不正な使用に関する勧告的警告メッセージを表示しなければならない。

O.AUTO_LOGOUT（自動ログアウト）
TOE は、TOE にログオンした操作員から、一定時間 TOE へのアクセスがないとき、自動的にログアウトを行わなければならない。

O.USERDATA_PROTECTION（利用者データの保護）
TOE は、以下のデータを秘匿し、改ざんを検出できなければならず、それぞれに対し許可された操作員や端末のみがデータを利用することができなければならない。
・サーバ管理者が、バックアップデータを利用することができる。
・個人情報管理者、及び個人情報利用者が、個人データの提供・預託データを利用することができる。
・サーバ端末ークライアント端末間で通信される利用者データは、当該端末が利用することができる。

O.BACKUP_RECOVERY（バックアップ／リカバリ）
TOE は、TOE が正常に動作するために必要な利用者データ及び TSF データをバックアップする手段を提供しなければならない。また、バックアップした利用者データ及び TSF データを、TOE の動作を復旧させるために TOE へリカバリする手段を提供しなければならない。

O.AVAILABLE_TIME_RESTRICTION（利用時間制限）
TOE は、管理されたセション確立可能な時間に基づき、セションの確立を制限しなければならない。

4.2. 運用環境のセキュリティ対策方針

OE.AUTHORIZATION_SETTING（権限の設定）
組織の責任者は、TOE に関連する権限・役割をもつ操作員として個人情報管理者、サーバ管理者、及び監査者を任命し、それぞれの権限付与の規定が載っている規則を参照して、それに基づいて権限を付与することにより、TOE に対し行える操作を割り当てなければならない。個人情報管理者は、オペレータ、及び個人情報利用者の任命・管理を組織の責任者から委任され、TOE に関連する権限・役割をもつ操作員としてオペレータ、及び個人情報利用者を任命し、それぞれの権限付与の規定が載っている規則を参照して、それに基づいて権限を付与することにより、TOE に対し行える操作を割り当てなければならない。

OE.TRUSTED_ROLE（信頼される役割）
組織の責任者は、サーバ管理者、監査者、及び個人情報管理者の役割に適した者を人選し、その上で、それぞれの役割を理解させる。

OE.PASSWORD_MANAGEMENT（操作員によるパスワードの管理）
すべての操作員は、TOE サービスを提供するシステムにアクセスするための認証情報（パスワード）を記憶し、他人に漏らしてはならない。 また推測・解析されやすい認証情報（パスワード）を設定してはならず、適正な間隔で変更しなければならない。

OE.TRAINING（教育・訓練）
すべての操作員は、個人データ及び TOE の安全管理に関する操作員の役割及び責任についての教育・訓練を受けなければならない。

OE.BACKUP_MEDIA（バックアップ媒体）
TOE のバックアップデータ、及び提供・預託データが保存されたリムーバブル媒体は、入退室管理を実施している物理的に保護された室内、及び TOE の遠隔地に所在し入退室管理を実施している物理的に保護された室内において施錠保管され、耐用年数を考慮した運用がなされなければならない。

OE.TIME_STAMP（高信頼タイムスタンプ）
TOE では、監査証跡を生成する際、及び利用時間制限を行う際に、高信頼タイムスタンプが利用できなければならない。

OE.SAFE_PLACE（安全な建物）
オペレータ端末、個人情報利用者端末、個人情報管理者端末、サーバ端末、監査者端末、及び処理連携サーバ端末は、A 社社員のみが入館できるよう入退館管理される建物内に設置され、個人データを取り扱う業務は同所にて実施されなければならない。

OE.FACILITIES_IN_SECURE_ROOM（セキュアルームへの機器設置）
サーバ端末、処理連携サーバ端末、及び個人データが格納されたリムーバブル媒体は、入退室管理（サーバ管理者として許可されている者、及びサーバ管理者に許可された者に制限）されている室内に設置されなければならない。なおサーバ管理者は、自身が許可した者を入室させた場合、その者の行動を監視する必要がある。

OE.NETWORK（ネットワーク環境）
社内 LAN と外部ネットワークとの間には、必要な通信のみに制限する設定がなされたファイアウォールを設置し、不要なパケットの流入を防ぐ。またセキュアルームネットワークは、TOE の機能に必要な通信のみに制限する設定がなされたファイアウォールを介して社内 LAN と接続する。

OE.UNJUST_SOFTWARE（不正ソフトウェア対策）
操作員はサーバ端末、処理連携サーバ端末、及びクライアント端末に、ウイルス対策ソフトウェアをインストールし、サーバ管理者の指定する修正プログラムの適用、ウイルス対策ソフトウェアのパターンファイルのアップデートを行わなければならない。サーバ管理者は、TOE に関するソフトウェアの修正ソフトウェアやウイルス対策ソフトウェアのパターンファイルの有効性・安定性を確認し、クライアント操作員に通知しなければならない。

4.3. セキュリティ対策方針根拠

セキュリティ対策は、セキュリティ課題定義で規定した脅威に対抗するためのもの、あるいは組織のセキュリティ方針を実現するためのものである。 セキュリティ対策方針と対抗する脅威、組織のセキュリティ方針の対応関係を表 4-1 に示す。

表 4-1 セキュリティ対策方針と対抗する脅威、組織セキュリティ方針及び前提条件

	T.ILLEGAL_LOGIN	T.UNAUTHORIZED_ACCESS	T.MISUSE	T.INJUSTICE	T.SPOOFING	T.DISCLOSE_NW_DATA	T.REMOVABLE_MEDIA	T.UNEXPECTED_ACCIDENT	P.SAFE_PLACE	P.FACILITIES_IN_SECURE_ROOM	P.NETWORK	P.UNJUST_SOFTWARE	P.RECOMMEND
O.I&A	×												
O.ACCESS_CONTROL		×	×										
O.TAKE_OUT		×	×										
O.AUDIT		×		×									
O.ALERT		×		×									
O.RECOMMEND													×
O.AUTO_LOGOUT					×								
O.USERDATA_PROTECTION						×	×						
O.BACKUP_RECOVERY								×					
O.AVAILABLE_TIME_RESTRICTION				×									
OE.AUTHORIZATION_SETTING		×											
OE.TRUSTED_ROLE		×		×									
OE.PASSWORD_MANAGEMENT	×												
OE.TRAINING			×	×									
OE.BACKUP_MEDIA								×					
OE.TIME_STAMP		×		×									
OE.SAFE_PLACE									×				
OE.FACILITIES_IN_SECURE_ROOM										×			
OE.NETWORK											×		
OE.UNJUST_SOFTWARE												×	

表 4-1 により、各セキュリティ対策方針は一つ以上の脅威、及び組織のセキュリティ方針に対応している。

次に、各脅威がセキュリティ対策方針で対抗できること、各組織のセキュリティ方針がセキュリティ対策方針により実現できることを説明する。

各脅威に対し、攻撃者を明示し、攻撃者が行う想定される攻撃方法を分析する。次に、攻撃方法に対抗するための有効な対策内容を示し、それがすべて満たされることで脅威に対抗できる十分な対策であることを示す。なお、対策内容は、一つ以上のセキュリティ対策方針がそれを満たし、脅威に対するセキュリティ対策方針として必要であることを示す。

○脅威

T.ILLEGAL_LOGON（不正なログオン）

この脅威は、1.4.1 節で識別された者以外の高度な専門知識を持たない攻撃者によって実行される。このような攻撃者がとり得る具体的な不正にログオンするための方法を示すとともに、それぞれに有効な対抗策について以下に述べる。

a. 利用を許可されていない者が、利用を許可されている者になりすます。

この攻撃に対しては、TOE の利用において識別・認証を行い、TOE の利用を正当な者のみに制限することにより対抗できる。この対抗策に該当するセキュリティ対策方針は、O.I&A である。

b. 正当な識別・認証情報を不正に取得する。

a の対抗策が有効に働くためには、識別･認証に用いられる情報を管理し、不正利用による利用許可者へのなりすましを防止する必要がある。識別・認証情報の不正取得の方法は、正当な操作員からの取得、攻撃者による類推の 2 種類がある。

正当な操作員からの識別・認証情報の取得、及び類推による識別認証情報の取得については、正当な操作員に対して認証情報の決定方法（認証情報を他人に教えない。認証情報は推測・類推されにくいものにする。認証情報は適切な間隔で変更する。）を教育することで対抗できる。また、類推により識別・認証情報を不正に取得されないように、誤った識別認証の連続試行を制限する。この対抗策に該当するセキュリティ対策方針は、O.I&A、及び OE.PASSWORD_MANAGEMENT である。

以上、a、b すべての攻撃方法に対抗することは、T.ILLEGAL_LOGIN に対抗することである。したがって、それぞれの攻撃方法に対する対抗策として該当する、O.I&A、及び OE.PASSWORD_MANAGEMENT によって、T.ILLEGAL_LOGIN に対抗できる。

T.UNAUTHORIZED_ACCESS（不正なアクセス）

この脅威は、基本機能利用者（個人情報利用者、及びオペレータ）によって実行される。個人情報利用者、及びオペレータがとり得る具体的な不正アクセスの方法を示すとともに、それぞれに有効な対抗策について以下に述べる。

a. 許可されていない操作を行う。

この攻撃に対しては、TOE の各操作に対して権限を設定し、操作員毎に許可／禁止される操作を明確にすることで対抗できる。この対抗策に該当するセキュリティ対策方針は、O.ACCESS_CONTROL である。

b. クライアント端末を用いて TOE 外へ利用者データを持ち出す。

この攻撃は、上記 a により参照可能な権限が付与された利用者に対し、参照した利用者データを TOE 外へ持ち出すことであり、この攻撃に対しては、クライアント操作員が用いるクライアント端末を経由したサーバ端末外部への保存と印刷を禁止することで対抗できる。この対抗策に該当するセキュリティ対策方針は、O.TAKE_OUT である。

c. 許可されていない操作について、許可するように権限を改ざんする。

この攻撃に対しては、TOE の各操作に対する権限設定を行える者を制限することによって対抗できる。この対抗策に該当するセキュリティ対策方針は、OE.AUTHORIZATION_SETTING である。

d. 許可されている操作を総当りで探索する。

この攻撃に対しては、許可されている操作を探索している操作を検出することが有効である。TOE で発生した事象についての正確な時刻に裏づけされた記録を採取し、その記録の中から攻撃の可能性を検知した時、その結果を TOE の保護に責務がある者に通知することにより、TOE の保護のための適切な事前処置を促す。この対抗策に該当するセキュリティ対策方針は、記録の採取については O.AUDIT、及び

OE.TIME_STAMP、通知については O.ALERT、TOE 保護の責務に関しては OE.TRUSTED_ROLE である。

以上、a、b、c、d すべての攻撃方法に対抗することは、T.UNAUTHORIZED_ACCESS に対抗することである。したがって、それぞれの攻撃方法に対する対抗策として該当する、O.ACCESS_CONTROL、O.TAKE_OUT、O.AUDIT、O.ALERT、OE.TRUSTED_ROLE、及び OE.AUTHORIZATION_SETTING によって、T.UNAUTHORIZED_ACCESS に対抗できる。

T.MISUSE（誤操作）

この脅威は、操作員によって実行される。操作員がとり得る具体的な誤操作に伴う攻撃ついて示すとともに、それぞれに有効な対抗策について以下に述べる。

a. 許可されていない操作を行う。

この攻撃に対しては、TOE の各操作に対して権限を設定し、操作員毎に許可／禁止される操作を明確にすることで対抗できる。この対抗策に該当するセキュリティ対策方針は、O.ACCESS_CONTROL である。

b. クライアント端末を用いて TOE 外へ利用者データを持ち出す。

この攻撃は、上記 a で許可されている参照権限を越えて、参照した利用者データを TOE 外へ持ち出すことであり、この攻撃に対しては、クライアント操作員が用いるクライアント端末を経由したサーバ端末外部への保存と印刷を禁止することで対抗できる。この対抗策に該当するセキュリティ対策方針は、O.TAKE_OUT である。

c. 意図しない操作を行う。

この攻撃に対しては、操作員の知識・スキル不足によるものであるため、教育を実施することが有効である。この対抗策に該当するセキュリティ対策方針は、OE.TRAINING である。

以上、a、b、c すべての攻撃方法に対抗することは、T.MISUSE に対抗することである。したがって、それぞれの攻撃方法に対する対抗策として該当する、O.ACCESS_CONTROL、O.TAKE_OUT、及び OE.TRAINING によって、T.MISUSE に対抗できる。

T. INJUSTICE（不正行為）

この脅威は、基本機能利用者のうち、個人情報利用者、及びオペレータによって実行される。このような攻撃者がとり得る具体的な不正行為の方法を示すとともに、それぞれに有効な対抗策について以下に述べる。

a. 許可されている操作を利用して不正な行為を行う。

この攻撃に対しては、業務時間外など管理者不在時に個人情報利用者、及びオペレータが管理されていない状況において不正行為が行われる。よって、管理状態にない時には TOE の利用を認めないことにより対抗できる。管理状態にない業務時間外の TOE の利用を、正確なタイムスタンプを用いて厳格に制限する。この対抗策に該当するセキュリティ対策方針は、O.AVAILABLE_TIME_RESTRICTION、及び OE.TIME_STAMP である。

また、管理者不在時であっても、TOE の操作記録が取得され管理者により確認されることで、不正な行為を行う動機を抑止することができる。TOE で発生した事象についての正確な時刻に裏づけされた記録を採取し、その記録の中から攻撃の可能性を検知した時、その結果を TOE の保護に責務がある者に通知することにより、TOE の保護のための適切な事前処置を促す。また、これらの監査行為について、教育プログラムを通じて公表することで、動機の抑制を図る。これらの対抗策に該当するセキュリティ対策方針は、記録の採取については O.AUDIT、及び OE.TIME_STAMP、通知については O.ALERT、TOE 保護の責務については OE.TRUSTED_ROLE、教育については、OE.TRAINING である。

以上の攻撃方法に対抗することは、T.INJUSTICE に対抗することである。

したがって、この攻撃方法に対する対抗策として該当する、
O.AVAILABLE_TIME_RESTRICTION、O.AUDIT、O.ALERT、
OE.TRUSTED_ROLE、及び OE.TRAINING によって、T.INJUSTICE に対抗できる。

T.SPOOFING（なりすまし）

この脅威は、1.4.1 節で識別されたもの以外の高度な専門知識を持たない攻撃者によって実行される。このような攻撃者がとり得る具体的ななりすましを行うための方法を示すとともに、それぞれに有効な対抗策について以下に述べる。

a. 正当な基本機能利用者がログオンした端末を用いる。

この攻撃は、正当な基本機能利用者が、TOE にログオンしたまま離席し、クライアント端末を長時間放置した際に、攻撃者が正当な操作員の権限を用いて TOE を利用することが考えられる。よって、ログオンしたまま長時間放置されたクライアント端末においては、自動的にログアウトすることで対抗できる。この対抗策に該当するセキュリティ対策方針は、O.AUTO_LOGOUT である。

以上の攻撃方法に対抗することは、T.SPOOFING に対抗することである。したがって、この攻撃方法に対する対抗策として該当する、O.AUTO_LOGOUT によって、T.SPOOFING に対抗できる。

T.DISCLOSE_NW_DATA（ネットワークデータ暴露）

この脅威は、1.4.1 節で識別されたもの以外の高度な専門知識を持たない攻撃者によって実行される。このような攻撃者がとり得る具体的なネットワークデータの不正利用の方法を示すとともに、それぞれに有効な対抗策について以下に述べる。

a. サーバ端末とクライアント端末間の通信データを傍受する。

この攻撃は、サーバ端末とクライアント端末間の通信データに対して、通信中のデータを不正に取得することが考えられる。よって、通信中のデータを秘匿し、適切な送受信端末のみが通信データを利用できるようにすることで対抗できる。この対抗策に該当するセキュリティ対策方針は、O.USERDATA_PROTECTION である。

b. 通信データを改ざんする。

この攻撃は、サーバ端末とクライアント端末間の通信中に、データを横取りされ、改ざんされることが考えられる。よって、通信中のデータに対し、改ざんの有無を検知することで対抗できる。この対抗策に該当するセキュリティ対策方針は、O.USERDATA_PROTECTION である。

以上の攻撃方法に対抗することは、T.DISCLOSE_NW_DATA に対抗することである。したがって、この攻撃方法に対する対抗策として該当する、O.USERDATA_PROTECTION によって、T.DISCLOSE_NW_DATA に対抗できる。

T.REMOVABLE_MEDIA（リムーバブル媒体）

この脅威は、1.4.1 節で識別されたもの以外の高度な専門知識を持たない攻撃者によって実行される。このような攻撃者がとり得る具体的なリムーバブル媒体からデータを暴露･改ざんするための方法を示すとともに、それぞれに有効な対抗策について以下に述べる。

a. リムーバブル媒体を入手し、利用者データを不正に取得する。

この攻撃は、バックアップデータ、または提供･預託データを保存したリムーバブル媒体が、攻撃者に不正に入手され、データが不正に利用されることが考えられる。よって、リムーバブル媒体に保存するデータを秘匿し、データの利用が許可された端末のみがバックアップデータ、または提供・預託データを利用できるようにすることで対抗できる。この対抗策に該当するセキュリティ対策方針は、

O.USERDATA_PROTECTION である。

b. リムーバブル媒体を入手し、利用者データを改ざんする。

この攻撃は、TOE からエクスポートされたバックアップデータ、または提供・預託データが、TOE 以外の手段を用いて攻撃者によりリムーバブル媒体に保存された利用者データが改ざんされることが考えられる。よって、リムーバブル媒体に保存されるデータに対し、改ざんの有無を検知することで対抗できる。この対抗策に該当するセキュリティ対策方針は、O.USERDATA_PROTECTION である。

以上、a、b すべての攻撃方法に対抗することは、T.REMOVABLE_MEDIA に対抗することである。したがって、その攻撃方法に対する対抗策として該当する、O.USERDATA_PROTECTION によって、T.REMOVABLE_MEDIA に対抗できる。

T.UNEXPECTED_ACCIDENT（不測の事態）

この脅威は、火災、天災、ディスク障害、その他の不測の事態によって発生する。これらの事象として考え得る不測の事態を示すとともに、それぞれに有効な対抗策について以下に述べる。

a. TOE の設置場所で、火災が発生する。

この攻撃は、個人情報処理センターにて火災が発生し、TOE が延焼することで保護資産が失われることが考えられる。よって、個人情報処理センター外に保護資産を退避させておくことで対抗できる。退避させた保護資産は、必要に応じて TOE で利用できる必要がある。この対抗策に該当するセキュリティ対策方針は、O.BACKUP_RECOVERY である。

b. TOE の設置場所で、広域災害が発生する。

この攻撃は、個人情報処理センターが所在する地で広域災害が発生し、TOE が延焼または破壊されることで保護資産が失われることが考えられる。よって、個人情報処理センター外に保護資産を退避させ、かつ遠隔地に保管することで対抗できる。退避させた保護資産は、必要に応じて TOE で利用できる必要がある。この対抗策に該当するセキュリティ対策方針は、保護資産の退避については O.BACKUP_RECOVERY、遠隔地への保管については OE.BACKUP_MEDIA である。

c. 保護資産を記録するディスクに、障害が発生する。

この攻撃は、TOE のディスク障害が発生するなどし、アクセスできないことにより保護資産が失われることが考えられる。よって、TOE 外に保護資産を退避させておくことで対抗できる。退避させた保護資産は、必要に応じて TOE で利用できる必要がある。この対抗策に該当するセキュリティ対策方針は、O.BACKUP_RECOVERY である。

d. 保管されている退避データが、利用できなくなる。

この攻撃は、リムーバブル媒体等に退避した保護資産が、耐用年数を経過することでアクセスできなくなることが考えられる。また、リムーバブル媒体自体が、不正に持ち出されるなど、紛失することが考えられる。よって、退避した保護資産が、物理的に保護された室内において、耐用年数を考慮した保管が行われることで対抗できる。この対抗策に該当する対策方針は、OE.BACKUP_MEDIA である。

以上、a、b、c、d すべての攻撃方法に対抗することは、T.UNEXPECTED_ACCIDENT に対抗することである。したがって、それぞれの攻撃方法に対する対抗策として該当する、O.BACKUP_RECOVERY、及び OE.BACKUP_MEDIA によって、T.UNEXPECTED_ACCIDENT に対抗できる。

○組織のセキュリティ方針

P.SAFE_PLACE（安全な建物）

この組織のセキュリティ方針は、TOE に関連するハードウェアが設置される場所、及び個人データを取り扱う業務が実施される場所に関するものである。それぞれに有効な対策方針について以下に述べる。

a. TOE を設置する建物を制限する。

TOE（オペレータ端末、個人情報利用者端末、個人情報管理者端末、サーバ端末、監査者端末、及び処理連携サーバ端末）は、入退館管理される建物内に設置し、A 社社員のみが入館できるように管理される。この方針に応じるための環境セキュリティ対策方針は、OE.SAFE_PLACE である。

b. 個人データを取り扱う業務は、同所にて実施する。

TOE を設置した建物内においてのみ、個人データを取り扱うことを許可する。この方針に応じるための環境セキュリティ対策方針は、OE.SAFE_PLACE である。

以上、a、b すべてに応じることは、P.SAFE_PLACE に応じることである。したがって、それぞれの要求に応じる対抗策として該当する、OE.SAFE_PLACE の達成によって P.SAFE_PLACE が実装される。

P.FACILITIES_IN_SECURE_ROOM（セキュアルームへの機器設置）

この組織のセキュリティ方針は、個人データが格納された HDD またはリムーバブル媒体の、持ち出し保護に関するものである。有効な対策方針について以下に述べる。

a. 個人データが格納される機器を設置する、及びリムーバブル媒体を保管する部屋を制限する。

個人データが格納されるサーバ端末、処理連携サーバ端末、及びリムーバブル媒体は、許可された者のみ入室が可能な室内に設置・保管する。この方針に応じるための環境セキュリティ対策方針は、OE.FACILITIES_IN_SECURE_ROOM である。

b. 入室を許可するものを制限する。

入室が許可されるものは、サーバ管理者として許可されている者、及びサーバ管理者に許可された者のみとする。この方針に応じるための環境セキュリティ対策方針は、OE.FACILITIES_IN_SECURE_ROOM である。

以上、a、b すべてに応じることは、P.FACILITIES_IN_SECURE_ROOM に応じることである。したがって、それぞれの要求に応じる対抗策として該当する、OE.FACILITIES_IN_SECURE_ROOM の達成によって P.FACILITIES_IN_SECURE_ROOM が実装される。

P.NETWORK（ネットワーク環境）

この組織のセキュリティ方針は、ネットワーク環境の構築に関するものである。有効な対策方針について以下に述べる。

a. 社内 LAN とインターネットとの接続を制限する。

社内 LAN と外部ネットワークとの接続は、ファイアウォールを用いて必要な通信のみに制限する。この方針に応じるための環境セキュリティ対策方針は、OE.NETWORK である。

b. セキュアルームネットワークへの接続を制限する。

TOE（サーバ端末、処理連携サーバ端末）が接続されるセキュアルームネットワークへは、TOE の機能に必要な通信のみ接続を許可する。この方針に応じるための環境セキュリティ対策方針は、OE.NETWORK である。

したがって、それぞれの要求に応じる対抗策として該当する、OE.NETWORK の達

成によって P.NETWORK が実装される。

P.UNJUST_SOFTWARE（不正ソフトウェア対策）

この組織のセキュリティ方針は、不正なソフトウェアに対する対策に関するものである。有効な対策方針について以下に述べる。

a. TOE 関連ハードウェアにウイルス対策ソフトウェアを導入する。

TOE 関連ハードウェア（オペレータ端末、個人情報利用者端末、個人情報管理者端末、サーバ端末、監査者端末、及び処理連携サーバ端末）に、ウイルス対策ソフトウェアを導入する。この方針に応じるための環境セキュリティ対策方針は、OE.UNJUST_SOFTWARE である。

b. パターンファイル、及びセキュリティ対策用修正ソフトウェアを適切に適用する。

ウイルス対策ソフトウェアのパターンファイル、及びセキュリティ対策用修正ソフトウェアの適用について、サーバ管理者が有効性・安全性を確認し、それらを適用するよう操作員に通知する。この方針に応じるための環境セキュリティ対策方針は、OE.UNJUST_SOFTWARE である。

したがって、それぞれの要求に応じる対抗策として該当する、OE.UNJUST_SOFTWARE の達成によって P.UNJUST_SOFTWARE が実装される。

P.RECOMMEND（勧告）

この組織のセキュリティ方針は、不正な使用に対する事前の勧告的警告メッセージに関するものである。有効な対策方針について以下に述べる。

a. TOE を使用する前に、すべての操作員に対し勧告的警告メッセージを表示する。

TOE を使用する前には、すべての操作員に対して、勧告的警告メッセージを表示することにより、不正な使用に対して注意喚起する。この対策に応じるためのセキュリティ対策方針は、O.RECOMMEND である。

したがって、この要求に応じる対抗策として該当する、O.RECOMMEND の達成によって P.RECOMMEND が実装される。

5. 拡張コンポーネント定義

5.1. 拡張機能コンポーネント

CC パート 2 に定義された、セキュリティ機能コンポーネントの拡張コンポーネントとして FPT_TST.2 を定義する。このコンポーネントは FPT（TSF の保護）クラス、FPT_TST（TSF 自己テスト）ファミリの拡張コンポーネントとして定義される。また、本コンポーネントは完全性を検証する範囲を TSF 実行コード、もしくは TSF 実行コードの一部から選択が可能であり、さらに TSF データの完全性の検証のみを行うことも可能であり、TSF 実行コード全体を完全性検証の範囲（TSF データに関しては一部の選択も可）としている FPT_TST.1 の簡易版（下位階層）という位置付けとして定義される。

以下に、CC パート 2 で定義される FPT_TST ファミリに対して、変更が生じる箇所を示す。

TSF 自己テスト（FPT_TST）

コンポーネントのレベル付け

FPT_TST.2　簡易 TSF テストは、TSF の正しい運用をテストする能力を提供する。これらのテストは、作動すべき条件が満たされた時に実行することができる。また、このテストは、（一部もしくは全ての）TSF 実行コードの完全性を検証する能力、および（一部もしくは全ての）TSF データの完全性を検証する能力を提供する。

管理：FPT_TST.2
以下のアクションは FMT における管理機能と考えられる:

- TSF 自己テストが動作する条件の管理

監査：FPT_TST.2
FAU_GEN1 セキュリティ監査データ生成が PP／ST に含まれていれば、以下のアクションを監査対象にすべきである：
- 最小：TSF 自己テストが成功した場合のテスト結果
- 基本：TSF 自己テストの実行とテスト結果
- 詳細：自己テストが作動すべき条件の変更

FPT_TST.2　簡易 TSF テスト
下位階層：　なし
依存性：　FPT_AMT.1 抽象マシンテスト

FPT_TST.2.1　TSF は、[割付：自己テストが作動すべき条件]下で、自己テストを実行しなければならない。
FPT_TST.2.2　TSF は、自己テストを行うことによって、選択：[割付：TSF の一部]、TSF 全体、[割付：TSF データの一部]、TSF データ全体]の完全性を検証することができなければならない。

6. セキュリティ要件

本章では、セキュリティ要件を記述する。

6.1. セキュリティ機能要件

TOE が提供するセキュリティ機能要件を記述する。

○セキュリティ監査（FAU）

FAU_ARP.1 セキュリティアラーム

下位階層： なし

FAU_ARP.1.1 TSF は、セキュリティ侵害の可能性が検出された場合、[割付: アクションのリスト]を実行しなければならない。

[割付：アクションのリスト]：サーバ管理者、監査者へのアラート通知

依存性： FAU_SAA.1 侵害の可能性の分析

FAU_GEN.1 監査データ生成

下位階層： なし

FAU_GEN.1.1 TSF は、以下の監査対象事象の監査記録を生成できなければならない：

- 監査機能の起動と終了；
- 監査の[選択：最小、基本、詳細、指定なし：から一つのみ選択]レベルのすべての監査対象事象；及び
- [割付：上記以外の個別に定義した監査対象事象]。

[選択：最小、基本、詳細、指定なし：から一つのみ選択]：基本

各機能要件を選択した場合に監査対象とすべき基本レベル以下のアクション（CC における規定）と、それに関連する TOE の監査対象事象（表 6-1）と、個別に定義した監査対象事象を示す。

表 6-1 監査対象とすべき基本レベル以下のアクション（CC における規定）と関連する監査対象事象

機能要件	監査対象とすべきアクション	監査対象事象
FAU_ARP.1	1) 最小: 切迫したセキュリティ侵害によってとられるアクション	1) サーバ管理者、 監査者へのアラートイベントの通知
FAU_GEN.1	なし	なし
FAU_GEN.2	なし	なし
FAU_SAA.1	1) 最小: すべての分析メカニズムの活性化/非活性化 2) 最小: ツールによって実行される自動応答	1) 監査機能の起動と停止 2) サーバ管理者、監査者へのアラートイベントの通知
FAU_SAR.1	1) 基本: 監査記録からの情報の読み出し	1) 監査証跡参照機能の起動と停止
FAU_SAR.2	1) 基本: 監査記録からの成功しなかった情報読み出し	1) アクセスの拒否
FAU_SAR.3	なし	なし
FAU_STG.1	なし	なし
FAU_STG.3	1) 基本: 閾値を超えたためにとられるアクション	1) 監査証跡領域枯渇の警告（サーバ管理者、監査者への通知） 1) 監査証跡領域枯渇、監査証跡削除（サーバ管理者、監査者への通知）
FAU_STG.4	1) 基本: 監査格納失敗によってとられるアクション	1) 最も古くに格納された監査記録への上書きと、サーバ管理者及び監査者への通知
FCS_CKM.1	1) 最小: 動作の成功と失敗 2) 基本: オブジェクト属性及び機密情報(例えば	1) 鍵生成・変更の成功と失敗 2) 生成・変更した暗号鍵の情報（鍵長、有効

機能要件	監査対象とすべきアクション	監査対象事象
	共通あるいは秘密鍵)を除くオブジェクトの値	期間)
FCS_CKM.4	1) 最小: 動作の成功と失敗 2) 基本: オブジェクト属性及び機密情報(例えば共通あるいは秘密鍵)を除くオブジェクトの値	1) 鍵変更・削除の成功と失敗 2) 変更・削除した暗号鍵の情報（鍵長、有効期間)
FCS_COP.1	1) 最小: 成功と失敗及び暗号操作の種別 2) 基本: すべての適用可能な暗号操作のモード、サブジェクト属性、オブジェクト属性	1) 暗号操作の成功と失敗、暗号操作の種別（暗号化／復号)、暗号アルゴリズム 2) サブジェクトに関連付けられる操作員 ID、操作員種別、暗号操作を行う権限リスト
FDP_ACC.1a	なし	なし
FDP_ACC.1b	なし	なし
FDP_ACF.1a	1) 最小: SFP で扱われるオブジェクトに対する操作の実行における成功した要求 2) 基本: SFP で扱われるオブジェクトに対する操作の実行におけるすべての要求	1), 2) 個人データレコードの生成、更新、参照、削除 1), 2) 個人データの提供・預託データレコードの生成、削除 1), 2) 個人データの加工データレコードの生成、更新、参照、削除 1), 2) 承認依頼レコードの生成、参照、削除 1), 2) 未登録個人データレコードの参照、削除
FDP_ACF.1b	1) 最小: SFP で扱われるオブジェクトに対する操作の実行における成功した要求 2) 基本: SFP で扱われるオブジェクトに対する操作の実行におけるすべての要求	1), 2) 個人データの提供・預託データレコードのエクスポートの成功と失敗 1), 2) バックアップデータレコードのエクスポート・インポートの成功と失敗
FDP_ETC.2	1) 最小: 情報エクスポート成功 2) 基本: 情報をエクスポートするすべての試み	1), 2) バックアップデータのエクスポートの成功と失敗
FDP_ITC.2	1) 最小: 任意のセキュリティ属性を含む、利用者データの成功したインポート 2) 基本: 任意のセキュリティ属性を含む、利用者データをインポートするすべての試み	1), 2) バックアップデータのインポートの成功と失敗
FIA_AFL.1	1) 最小: 不成功の認証試行に対する閾値への到達及びそれに続いてとられるアクション(例えば端末の停止)、もし適切であれば、正常状態への復帰(例えば端末の再稼動)	1) 不成功の認証試行回数の閾値到達、それに続いてとられるアクション（アカウントの一定時間の無効化、アカウントのロック） 1) 無効化されたアカウントの認証試行（サーバ管理者における不成功の認証試行回数の閾値到達後、再び認証が成功すると不成功認証試行回数がクリアされ、正常状態に復帰する）クライアント操作員のアカウントがロックされた場合には正常状態には戻らない。
FIA_ATD.1	なし	なし
FIA_SOS.1	1) 最小: TSF による、テストされた秘密の拒否 2) 基本: TSF による、テストされた秘密の拒否または受け入れ	1), 2) 操作員の登録／編集の成功と失敗
FIA_UAU.1a	1) 最小: 認証メカニズムの不成功になった使用 2) 基本: 認証メカニズムのすべての使用	1), 2) 最小、基本 : クライアント操作員の認証（成功及び失敗)
FIA_UAU.1b	1) 最小: 認証メカニズムの不成功になった使用 2) 基本: 認証メカニズムのすべての使用	1), 2) 最小、基本 : サーバ管理者の認証（成功及び失敗)
FIA_UID.1a	1) 最小: 提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用 2) 基本: 提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用	1), 2) クライアント操作員の識別（成功及び失敗)
FIA_UID.1b	1) 最小: 提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用 2) 基本: 提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用	1), 2) サーバ管理者の識別（成功及び失敗)
FIA_USB.1	1) 最小: 利用者セキュリティ属性のサブジェクトに対する不成功結合(例えば、サブジェクトの生成) 2) 基本: 利用者セキュリティ属性のサブジェクトに対する結合の成功及び失敗(例えば、サブジェ	1), 2) 操作員の識別と認証（成功及び失敗)

機能要件	監査対象とすべきアクション	監査対象事象
	クトの生成の成功及び失敗)	
FMT_MSA.3	1) 基本: 許可的あるいは制限的規則のデフォルト設定の改変 2) 基本: セキュリティ属性の初期値の改変すべて	1) なし（改変されることはない） 2) なし（改変されることはない）
FMT_MTD.1	1) 基本: TSF データの値におけるすべての改変	1) セキュリティ侵害の可能性の判断に用いる監査証跡の重要度の変更 1) 操作員の登録、削除 1) パスワードの変更 1) 不成功認証試行回数の定義の変更 1) バナー表示メッセージの管理 1) 操作員種別毎のセション確立許可時間帯の変更 1) 各暗号鍵の生成、削除 1) 監査証跡の削除、エクスポート、インポート
FMT_SMF.1	1) 最小: 管理機能の使用	1) セキュリティ侵害の可能性の判断に用いる監査証跡の重要度の管理 1) 提供・預託先公開鍵のインポート 1) 不成功の認証試行に対する閾値の管理 1) 操作員の登録／編集／削除 1) 操作員種別の付与 1) バナー表示メッセージの管理 1) 操作員種別毎のセション確立許可時間帯の管理
FMT_SMR.2	1) 最小: 役割の一部をなす利用者のグループに対する改変 2) 最小: 役割に対して与えられた条件のために成功しなかった、その役割を使用する試み	1) なし（改変されることはない） 2) アクセスの拒否
FTA_SSL.3	1) 最小: セションロックメカニズムによる対話セションの終了	1) セションロックメカニズムによる対話セションの終了
FTA_TAB.1	なし	なし
FTA_TSE.1	1) 最小: セション確立メカニズムによるセション確立の拒否 2) 基本: 利用者セション確立におけるすべての試み	1) セション確立の拒否 2) ・クライアント端末用パッケージの正当性検証 ・セション鍵の生成 ・クライアント操作員の識別と認証 ・勧告的警告メッセージの表示
FPT_TST.2	1) 最小 : TSF 自己テストが成功した場合のテスト結果 2) 基本 : TSF 自己テストの実行とテスト結果	1) クライアント端末用パッケージの正当性を検証して一致した事象 2) クライアント端末用パッケージの正当性を検証した結果
FPT_STM.1	1) 最小： 時間の変更;	なし（OS の機能を使用）

[割付：上記以外の個別に定義した監査対象事象]：
・サーバサブシステムで発生したエラー
・サーバサブシステムのセットアップ
・基本機能の起動と停止
・未登録個人データのインポートの成功と失敗

FAU_GEN.1.2 TSF は、各監査記録において少なくとも以下の情報を記録しなければならない：

- 事象の日付・時刻、事象の種別、サブジェクト識別情報、事象の結果（成功または失敗）；及び
- 各監査事象の種別に対して、PP／ST の機能コンポーネントの監査対象事象の定義に基づいた、[割付：その他の監査関連情報]

[割付：その他の監査関連情報]：

・プロセス ID
・重要度（なし、低、中、高）

依存性： FPT_STM.1 高信頼タイムスタンプ

FAU_GEN.2 利用者識別情報の関連付け

下位階層： なし

FAU_GEN.2.1 TSF は、各監査対象事象を、その原因となった利用者の識別情報に関連付けられなければならない。

依存性： FAU_GEN.1 監査データ生成
FIA_UID.1 識別のタイミング

FAU_SAA.1 侵害の可能性の分析

下位階層： なし

FAU_SAA.1.1 TSF は、監査事象の監視に規則のセットを適用し、これらの規則に基づき SFR 実施の侵害の可能性を示すことができなければならない。

FAU_SAA.1.2 TSF は、監査された事象を監視するための以下の規則を実施しなければならない:

- セキュリティ侵害の可能性を示すものとして知られている[割付：定義された監査対象事象のサブセット]をすべて合わせた、あるいは組み合わせたもの;
- [割付：その他の規則]。

[割付：定義された監査対象事象のサブセット]：
すべての監査対象事象に関して、監査者の定めた重要度以上の重要度を含む監査証跡が生成された場合に、セキュリティ侵害の可能性があると判断する。セキュリティ侵害の可能性を判断するために選択可能な重要度は低、中、高のいずれか一つである。

[割付：その他の規則]：なし

依存性： FAU_GEN.1 監査データ生成

FAU_SAR.1 監査レビュー

下位階層： なし

FAU_SAR.1.1 TSF は、[割付：許可利用者]が、[割付：監査情報のリスト]を監査記録から読み出せるようにしなければならない。

[割付：許可利用者]：サーバ管理者、監査者

[割付：監査情報のリスト]：
{プロセス ID、サブジェクト識別情報、事象の種別、事象の結果（成功または失敗）、事象の日付・時刻、重要度}

FAU_SAR.1.2 TSF は、利用者に対し、その情報を解釈するのに適した形式で監査記録を提供しなければならない。

依存性： FAU_GEN.1 監査データ生成

FAU_SAR.2 限定監査レビュー

下位階層： なし

FAU_SAR.2.1 TSF は、明示的な読み出しアクセスを承認された利用者を除き、すべての利用者に監査記録への読み出しアクセスを禁止しなければならない。

依存性： FAU_SAR.1 監査レビュー

FAU_SAR.3 選択可能監査レビュー

下位階層： なし

FAU_SAR.3.1 TSF は、[割付：論理的な関連の基準]に基づいて、監査データを[選択：検索、分類、並べ替え]する能力を提供しなければならない。

[割付：論理的な関連の基準]：
検索、並べ替えには以下の条件を指定できる。
・プロセス ID
・サブジェクト識別情報
・事象の種別
・事象の日付・時刻
・事象の結果（成功または失敗）
・重要度

[選択：検索、分類、並べ替え]：検索、並べ替え

依存性： FAU_SAR.1 監査レビュー

FAU_STG.1 保護された監査証跡格納

下位階層： なし

FAU_STG.1.1 TSF は、監査証跡に格納された監査記録を不正な削除から保護しなければならない。

[詳細化]：格納された → サーバ端末の DB に格納された

FAU_STG.1.2 TSF は、監査証跡内の監査記録への不正な改変を[選択：防止、検出：から一つのみ選択]できねばならない。

[詳細化]：監査証跡内の → サーバ端末の DB に格納された監査証跡内の

[選択：防止、検出：から一つのみ選択]：防止

依存性： FAU_GEN.1 監査データ生成

FAU_STG.3 監査データ損失の恐れ発生時のアクション

下位階層： なし

FAU_STG.3.1 TSF は、監査証跡が[割付：事前に定義された限界]を超えた場合、[割付：監査格納失敗の恐れ発生時のアクション]をとらなければならない。

[詳細化]：監査証跡 → サーバ端末の DB に格納された監査証跡

[割付：事前に定義された限界]：
サーバ管理者がサーバサブシステムのセットアップ時に指定した容量の 80%

[割付：監査格納失敗の恐れ発生時のアクション]：
サーバ管理者、監査者への通知

依存性： FAU_STG.1 保護された監査証跡格納

FAU_STG.4 監査データ損失の防止

下位階層: FAU_STG.3 監査データ消失の恐れ発生時のアクション

FAU_STG.4.1 TSF は、監査証跡が満杯になった場合、[選択: 監査対象事象の無視、特別な権利を持つ許可利用者に関わるもの以外の監査対象事象の抑止、最も古くに格納された監査記録への上書き: から 1 つのみ選択]及び[割付: 監査格納失敗時にとられるその他のアクション]を行わなければならない。

[詳細化]: 監査証跡 → サーバ端末の DB に格納された監査証跡

[選択: 監査対象事象の無視、特権を持つ許可利用者に関わるもの以外の監査対象事象の抑止、最も古くに格納された監査記録への上書き: から一つのみ選択]: 最も古くに格納された監査記録への上書き

[割付: 監査格納失敗時にとられるその他のアクション]:
サーバ管理者、監査者への通知

依存性: FAU_STG.1 保護された監査証跡格納

○暗号サポート（FCS）

FCS_CKM.1 暗号鍵生成

下位階層： なし

FCS_CKM.1.1 TSF は、以下の[割付：標準のリスト]に合致する、指定された暗号鍵生成アルゴリズム[割付：暗号鍵生成アルゴリズム]と指定された暗号鍵長[割付：暗号鍵長]に従って、暗号鍵を生成しなければならない。

[割付：標準のリスト]：表 6-2 に示す。
[割付：暗号鍵生成アルゴリズム]：表 6-2 に示す。
[割付：暗号鍵長]：表 6-2 に示す。

表 6-2 暗号鍵と生成アルゴリズム

鍵の種類	標準	暗号鍵生成アルゴリズム	暗号鍵長
サーバ共通鍵	X 社暗号仕様標準	X 社暗号鍵生成アルゴリズム	168bit
処理連携サーバ共通鍵	X 社暗号仕様標準	X 社暗号鍵生成アルゴリズム	168bit
サーバ秘密鍵	PKCS#1	RSA	2048bit
サーバ公開鍵	PKCS#1	RSA	2048bit
セション鍵	X 社暗号仕様標準	X 社暗号鍵生成アルゴリズム	168bit

依存性： [FCS_CKM.2 暗号鍵配付
または
FCS_COP.1 暗号操作]
FCS_CKM.4 暗号鍵破棄
FMT_MSA.2 セキュアなセキュリティ属性

FCS_CKM.4 暗号鍵破棄

下位階層： なし

FCS_CKM.4.1 TSF は、以下の[割付：標準のリスト]に合致する、指定された暗号鍵破棄方法[割付：暗号鍵破棄方法]に従って、暗号鍵を破棄しなければならない。

[割付：標準のリスト]：なし

[割付：暗号鍵破棄方法]：
すべての暗号鍵は、ダミーデータ（乱数やゼロデータなどの実質的な意味のないデータ）で上書きしてから削除する暗号鍵破棄方法

依存性： [FDP_ITC.1 セキュリティ属性なし利用者データのインポート
または
FDP_ITC.2 セキュリティ属性付き利用者データのインポート
または
FCS_CKM.1 暗号鍵生成]
FMT_MSA.2 セキュアなセキュリティ属性

FCS_COP.1 暗号操作（暗号化・復号・署名）

下位階層： なし

FCS_COP.1.1 TSF は、[割付: 標準のリスト]に合致する、特定された暗号アルゴリズム[割付: 暗号アルゴリズム]と暗号鍵長[割付: 暗号鍵長]に従って、割付: 暗号操作のリスト]を実行しなければならない。

[割付：標準のリスト]：表 6-3 に示す。
[割付：暗号アルゴリズム]：表 6-3 に示す。
[割付：暗号鍵長]：表 6-3 に示す。
[割付：暗号操作のリスト]：表 6-3 に示す。

表 6-3 暗号鍵生成アルゴリズムと暗号操作

鍵の種類	標準	暗号アルゴリズム	暗号鍵長	暗号操作
サーバ共通鍵	FIPS PUB 46-3	Triple DES	168bit	・サーバ端末内 DB のバックアップデータの暗号化・復号
処理連携サーバ共通鍵	FIPS PUB 46-3	Triple DES	168bit	・処理連携サーバ端末内 DB のバックアップデータの暗号化・復号
サーバ秘密鍵	PKCS#1	RSA	2048bit	・サーバ端末ークライアント端末間通信データのセション鍵の復号
サーバ公開鍵	PKCS#1	RSA	2048bit	・サーバ端末ークライアント端末間通信データのセション鍵の暗号化
提供・預託先共通鍵	FIPS PUB 46-3	Triple DES	168bit	・提供・預託データの暗号化
セション鍵	FIPS PUB 46-3	Triple DES	168bit	・サーバ端末ークライアント端末間通信データの暗号化・復号
標準		暗号アルゴリズム		暗号操作
FIPS PUB 180-1		SHA-256		・バックアップデータのハッシュ操作（生成・比較） ・提供・預託データのハッシュ操作（生成）

依存性： [FDP_ITC.1 セキュリティ属性なし利用者データのインポート、または
FDP_ITC.2 セキュリティ属性付き利用者データのインポート、または
FCS_CKM.1 暗号鍵生成]
FCS_CKM.4 暗号鍵破棄
FMT_MSA.2 セキュアなセキュリティ属性

○利用者データ保護（FDP）

FDP_ACC.1a サブセットアクセス制御（個人情報処理メイン機能）

下位階層： なし

FDP_ACC.1.1.a TSF は、[割付: サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト]に対して[割付: アクセス制御 SFP]を実施しなければならない。

[割付：サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト]：

＜サブジェクト＞
・オペレータプロセス
・個人情報利用者プロセス
・個人情報管理者プロセス

＜オブジェクト＞
・個人データレコード
・未登録個人データレコード
・個人データの提供データレコード
・個人データの預託データレコード
・個人データの加工データレコード
・個人データに関する承認依頼（登録用）レコード
・個人データに関する承認依頼（更新用）レコード
・個人データに関する承認依頼（削除用）レコード
・個人データに関する承認依頼（提供用）レコード
・個人データに関する承認依頼（預託用）レコード

＜SFP で扱われるサブジェクトとオブジェクト間の操作＞
・個人データレコードの生成、参照、更新、削除、印刷、保存
・未登録個人データレコードの参照、削除、印刷、保存
・個人データの提供･預託データレコードの生成、削除、印刷、保存
・個人データの加工データレコードの生成、参照、更新、削除、印刷、保存
・個人データに関する承認依頼（登録用）レコードの生成、参照、削除、印刷、保存
・個人データに関する承認依頼（更新用）レコードの生成、参照、削除、印刷、保存
・個人データに関する承認依頼（削除用）レコードの生成、参照、削除、印刷、保存
・個人データに関する承認依頼（提供用）レコードの生成、参照、削除、印刷、保存
・個人データに関する承認依頼（預託用）レコードの生成、参照、削除、印刷、保存

[割付：アクセス制御 SFP]：
個人情報処理メイン機能アクセス制御方針

依存性： FDP_ACF.1 セキュリティ属性によるアクセス制御

FDP_ACC.1b サブセットアクセス制御（外部入出力）

下位階層： なし

FDP_ACC.1.1.b TSF は、[割付: サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト]に対して[割付: アクセス制御 SFP]を実施しなければならない。

[割付：サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト]：

＜サブジェクト＞
・サーバ管理者プロセス
＜オブジェクト＞
・個人データの提供･預託データテーブル
・バックアップデータテーブル
＜SFP で扱われるサブジェクトとオブジェクト間の操作＞
・個人データの提供･預託データテーブルのエクスポート
・バックアップデータテーブルのエクスポート、インポート

[割付：アクセス制御 SFP]：外部入出力アクセス制御方針

依存性： FDP_ACF.1 セキュリティ属性によるアクセス制御

FDP_ACF.1a セキュリティ属性によるアクセス制御（個人情報処理メイン機能）

下位階層： なし

FDP_ACF.1.1.a TSF は、以下の[割付: 示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ]に基づいて、オブジェクトに対して、[割付: アクセス制御 SFP]を実施しなければならない。

[割付：示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ] ：
以下のとおり、表に示す。

・示された SFP 下において制御されるサブジェクト及び対応する SFP 関連セキュリティ属性・・・表 6-4 に示す。

表 6-4 サブジェクト及び対応するセキュリティ属性

制御されるサブジェクト	対応する SFP 関連セキュリティ属性
オペレータプロセス 個人情報利用者プロセス 個人情報管理者プロセス	操作員種別

・示されたSFP下において制御されるオブジェクト及び対応するSFP関連セキュリティ属性・・・表 6-5 に示す。

表 6-5 オブジェクト及び対応するセキュリティ属性

制御されるオブジェクト	対応する SFP 関連セキュリティ属性
個人データレコード 未登録個人データレコード 個人データの提供データレコード 個人データの預託データレコード 個人データの加工データレコード 個人データに関する承認依頼（登録用）レコード	個人データ種別

制御されるオブジェクト	対応する SFP 関連セキュリティ属性
個人データに関する承認依頼（更新用）レコード 個人データに関する承認依頼（削除用）レコード 個人データに関する承認依頼（提供用）レコード 個人データに関する承認依頼（預託用）レコード	

[割付：アクセス制御 SFP]：個人情報処理メイン機能アクセス制御方針

FDP_ACF.1.2.a TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうかを決定するために、次の規則を実施しなければならない: [割付: 制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]。

[割付：制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]： 表 6-6 に示す。

表 6-6 個人情報処理メイン機能へのアクセスを管理する規則

制御されたサブジェクト	サブジェクトのセキュリティ属性（操作員種別）	制御されたオブジェクト	オブジェクトのセキュリティ属性（個人データ種別）	制御された操作
オペレータプロセス	オペレータ	個人データに関する承認依頼（登録用）レコード	個人データに関する承認依頼（登録用）	生成
		個人データに関する承認依頼（更新用）レコード	個人データに関する承認依頼（更新用）	
		個人データに関する承認依頼（削除用）レコード	個人データに関する承認依頼（削除用）	
		未登録個人データレコード	未登録個人データ	参照 削除
個人情報利用者プロセス	個人情報利用者	個人データレコード	個人データ	参照
		個人データの加工データレコード	個人データの加工データ	
		個人データに関する承認依頼（提供用）レコード	個人データに関する承認依頼（提供用）	生成
		個人データに関する承認依頼（預託用）レコード	個人データに関する承認依頼（預託用）	
		個人データの加工データレコード	個人データの加工データ	生成 更新 削除
個人情報管理者プロセス	個人情報管理者	個人データレコード	個人データ	参照
		個人データの加工データレコード	個人データの加工データ	
		個人データに関する承認依頼（登録用）レコード	個人データに関する承認依頼（登録用）	参照 削除
		個人データに関する承認依頼（更新用）レコード	個人データに関する承認依頼（更新用）	
		個人データに関する承認依頼（削除用）レコード	個人データに関する承認依頼（削除用）	

制御された サブジェクト	サブジェクトの セキュリティ属性（操作員種別）	制御された オブジェクト	オブジェクトのセキュリティ属性（個人データ種別）	制御された操作
		個人データに関する承認依頼（提供用）レコード	個人データに関する承認依頼（提供用）	
		個人データに関する承認依頼（預託用）レコード	個人データに関する承認依頼（預託用）	
		個人データレコード	個人データ	生成 更新 削除
		個人データの提供データレコード	個人データの提供データ	生成 削除
		個人データの預託データレコード	個人データの預託データ	

表 6-6 で示された操作員種別を有する制御されたサブジェクトは、制御されたオブジェクトに対して、制御された操作のみを行うことができる。

FDP_ACF.1.3.a TSF は、次の追加規則、[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に許可する規則]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に許可しなければならない。

[割付：セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則]： なし

FDP_ACF.1.4.a TSF は、[割付：セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。

[割付：セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則]： 表 6-6 に挙げるサブジェクトは、制御されたオブジェクトに対し、制御された操作（印刷、クライアント端末への保存）を行えない。

依存性： FDP_ACC.1 サブセットアクセス制御
FMT_MSA.3 静的属性初期化

FDP_ACF.1b セキュリティ属性によるアクセス制御（外部入出力）

下位階層： なし

FDP_ACF.1.1.b TSF は、以下の[割付：示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ]に基づいて、オブジェクトに対して、[割付：アクセス制御 SFP]を実施しなければならない。

[割付：示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ] ：
以下のとおり、表に示す。

・示された SFP 下において制御されるサブジェクト及び対応する SFP 関連セキュリティ属性・・・表 6-7 に示す。

表 6-7 サブジェクト及び対応するセキュリティ属性

制御されるサブジェクト	対応する SFP 関連セキュリティ属性
サーバ管理者プロセス	操作員種別

・示されたSFP下において制御されるオブジェクト及び対応するSFP関連セキュリティ属性・・・表 6-8 に示す。

表 6-8 オブジェクト及び対応するセキュリティ属性

制御されるオブジェクト	対応する SFP 関連セキュリティ属性
個人データの提供･預託データレコード バックアップデータレコード	個人データ種別

[割付：アクセス制御 SFP]：外部入出力アクセス制御方針

FDP_ACF.1.2.b TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうか決定するために、次の規則を実施しなければならない：[割付：制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]

[割付：制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]： 表 6-9 に示す。

表 6-9 外部入出力を管理する規則

制御されたサブジェクト	サブジェクトのセキュリティ属性（操作員種別）	制御されたオブジェクト	オブジェクトのセキュリティ属性（個人データ種別）	制御された操作
サーバ管理者プロセス	サーバ管理者	個人データの提供･預託データレコード	個人データの提供･預託データ	エクスポート
		バックアップデータレコード	バックアップデータ	エクスポート インポート

表 6-9 で示された操作員種別を有する制御されたサブジェクトは、制御されたオブジェクトに対して、制御された操作のみを行うことができる。

FDP_ACF.1.3.b TSF は、以下の追加規則に基づいて、オブジェクトに対するサブジェクトのアクセスを明示的に承認しなければならない：[割付：セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則]。

[割付：セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則]： なし

FDP_ACF.1.4.b TSF は、[割付：セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。

[割付：セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則]：なし

依存性： FDP_ACC.1 サブセットアクセス制御
FMT_MSA.3 静的属性初期化

FDP_ETC.2 セキュリティ属性付き利用者データのエクスポート（バックアップデータ）
下位階層： なし

FDP_ETC.2.1 TSF は、SFP 制御下にある利用者データを TOE の外部にエクスポートするとき、[割付: アクセス制御 SFP 及び/または情報フロー制御 SFP]を実施しなければならない。

[詳細化]： 利用者データ → バックアップデータ

[割付：アクセス制御 SFP(s)及び／または情報フロー制御 SFP(s)]：
外部入出力アクセス制御方針

FDP_ETC.2.2 TSF は、利用者データに関係したセキュリティ属性と共に利用者データをエクスポートしなければならない。

[詳細化]： 利用者データ → バックアップデータ

FDP_ETC.2.3 TSF は、セキュリティ属性が TSC の外部にエクスポートされるとき、それがエクスポートされる利用者データに曖昧さなく関係付けられることを保証しなければならない。

[詳細化]： 利用者データ → バックアップデータ

FDP_ETC.2.4 TSF は、利用者データが TSC からエクスポートされるとき、以下の規則を実施しなければならない：[割付：追加エクスポート制御規則]。

[詳細化]： 利用者データ → バックアップデータ

[割付：追加エクスポート制御規則]： なし

依存性： [FDP_ACC.1 サブセットアクセス制御、または
FDP_IFC.1 サブセット情報フロー制御]

FDP_ITC.2 セキュリティ属性付き利用者データのインポート（バックアップデータ）

下位階層： なし

FDP_ITC.2.1 TSF は、SFP 制御下にある利用者データを TOE の外部からインポートするとき、[割付: アクセス制御 SFP 及び/または情報フロー制御 SFP]を実施しなければならない。

[詳細化]： 利用者データ → バックアップデータ

[割付：アクセス制御 SFP(s)及び／または情報フロー制御 SFP(s)]：
外部入出力アクセス制御方針

FDP_ITC.2.2 TSF は、インポートされる利用者データに関連付けられたセキュリティ属性を使用しなければならない。

[詳細化]： 利用者データ → バックアップデータ

FDP_ITC.2.3 TSF は、使用されるプロトコルが、受け取るセキュリティ属性と利用者データ間の曖昧さのない関連性を備えていることを保証しなければならない。

[詳細化]： 利用者データ → バックアップデータ

FDP_ITC.2.4 TSF は、インポートされる利用者データのセキュリティ属性の解釈が、利用者データの生成元によって意図されたとおりであることを保証しなければならない。

[詳細化]： 利用者データ → バックアップデータ

FDP_ITC.2.5 TSF は、SFP に従って制御され、利用者データを TSC 外からインポートするときは、以下の規則を実施しなければならない：[割付：追加のインポート制御規則]。

[詳細化]： 利用者データ → バックアップデータ

[割付：追加のインポート制御規則]： なし

依存性： [FDP_ACC.1 サブセットアクセス制御、または
FDP_IFC.1 サブセット情報フロー制御]
[FTP_ITC.1 TSF 間高信頼チャネル、または
FTP_TRP.1 高信頼パス]
FPT_TDC.1 TSF 間基本 TSF データ一貫性

○識別と認証（FIA）

FIA_AFL.1 認証失敗時の取り扱い

下位階層： なし

FIA_AFL.1.1 TSF は、[割付：認証事象のリスト]に関して、[選択：[割付：正の整数値], 「[割付：許容可能な値の範囲]内における管理者設定可能な正の整数値」] 回の不成功認証試行が生じたときを検出しなければならない。

[割付：認証事象のリスト] ：
・最後に成功した認証以降の各クライアント操作員の認証
・最後に成功した認証以降の各サーバ管理者の認証

[選択：[割付：正の整数値], 「[割付：許容可能な値の範囲]内における管理者設定可能な正の整数値」]：「1～5 回内における管理者設定可能な正の整数値」

FIA_AFL.1.2 不成功の認証試行が定義した回数に達するか上回ったとき、TSF は、[割付：アクションのリスト]をしなければならない。

[割付：アクションのリスト]：表 6-10 に示す。

表 6-10 TOE へのアクセスを管理する規則

認証事象	アクション
最後に成功した認証以降の各クライアント操作員の認証	アカウントをロックし、解除不可能にする。
最後に成功した認証以降の各サーバ管理者の認証	アカウントを 5 分間無効化する。その後、不成功認証試行回数を 0 にする。

＜注釈＞
ロックされたアカウントを復旧する場合は、個人情報管理者もしくはサーバ管理者が当該アカウントを削除し、再度アカウントを作成する。
・個人情報管理者が復旧できるアカウント：オペレータ、個人情報利用者
・サーバ管理者が復旧できるアカウント：個人情報管理者、監査者

依存性： FIA_UAU.1 認証のタイミング

FIA_ATD.1 利用者属性定義

下位階層： なし

FIA_ATD.1.1 TSF は、個々の利用者に属する以下のセキュリティ属性のリストを維持しなければならない。：[割付: セキュリティ属性のリスト]

[割付：セキュリティ属性のリスト]：

{操作員種別（オペレータ、個人情報利用者、個人情報管理者、サーバ管理者、監査者）}

依存性： なし

FIA_SOS.1 秘密の検証

下位階層： なし

FIA_SOS.1.1 TSF は、秘密が[割付：定義された品質尺度]に合致することを検証するメカニズムを提供しなければならない。

[割付：定義された品質尺度]： 以下の品質尺度

＜品質尺度＞

・操作員のパスワードは 6 文字以上 10 文字以下の、以下の範囲の ASCII 文字が使用できる。

・アルファベットは、大文字[A-Z]の 26 文字、小文字[a-z]の 26 文字の合計 52 文字。

・数字は、[0-9]の合計 10 文字。

・記号は、!"#$%&'()*+,-./:;<=>?@[¥]^_`{|}~ の 32 文字。

・1 文字以上の数字または記号を含む。

・2 文字以上のアルファベットを含む（大文字、小文字は区別される）。

・新しいパスワードは、直前のパスワードと同一であってはならない。

依存性： なし

FIA_UAU.1a 認証のタイミング（クライアント操作員）

下位階層： なし

FIA_UAU.1.1.a TSF は、利用者が認証される前に利用者を代行して行われる[割付：TSF 仲介アクションのリスト]を許可しなければならない。

[詳細化]：利用者 → クライアント操作員

[割付：TSF 仲介アクションのリスト]：

・勧告的警告メッセージの表示

・セション鍵生成

・クライアント端末用パッケージの正当性検証

・クライアント操作員の識別

FIA_UAU.1.2.a TSF は、その利用者を代行する他の TSF 仲介アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

[詳細化]： 利用者 → クライアント操作員

依存性： FIA_UID.1 識別のタイミング

FIA_UAU.1b 認証のタイミング（サーバ管理者）

下位階層： なし

FIA_UAU.1.1.b TSF は、利用者が認証される前に利用者を代行して行われる[割付：TSF 仲介アクションのリスト]を許可しなければならない。

[詳細化]： 利用者 → サーバ管理者

[割付：TSF 調停アクションのリスト]：

・勧告的警告メッセージの表示

・サーバ管理者の識別

FIA_UAU.1.2.b TSF は、その利用者を代行する他の TSF 仲介アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

[詳細化]： 利用者 → サーバ管理者

依存性： FIA_UID.1 識別のタイミング

FIA_UID.1a 識別のタイミング（クライアント操作員）

下位階層： なし

FIA_UID.1.1a TSF は、利用者が識別される前に利用者を代行して実行される[割付：TSF 仲介アクションのリスト]を許可しなければならない。

[詳細化]： 利用者 → クライアント操作員

[割付：TSF 仲介アクションのリスト]：
・勧告的警告メッセージの表示
・セション鍵生成
・クライアント端末用パッケージの正当性検証

FIA_UID.1.2a TSF は、その利用者を代行する他の TSF 仲介アクションを許可する前に、各利用者に識別が成功することを要求しなければならない。

[詳細化]： 利用者 → クライアント操作員

依存性： なし

FIA_UID.1b 識別のタイミング（サーバ管理者）

下位階層： なし

FIA_UID.1.1b TSF は、利用者が識別される前に利用者を代行して実行される[割付：TSF 仲介アクションのリスト]を許可しなければならない。

[詳細化]：利用者 → サーバ管理者

[割付：TSF 仲介アクションのリスト]：
・勧告的警告メッセージの表示

FIA_UID.1.2b TSF は、その利用者を代行する他の TSF 調停アクションを仲介する前に、各利用者に識別が成功することを要求しなければならない。

[詳細化]： 利用者 → サーバ管理者

依存性： なし

FIA_USB.1 利用者・サブジェクト結合

下位階層： なし

FIA_USB.1.1 TSF は、以下の利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトに関連付けなければならない。：[割付: 利用者セキュリティ属性のリスト]

[割付：利用者セキュリティ属性のリスト]： 操作員種別

FIA_USB.1.2 TSF は、利用者を代行して動作するサブジェクトと利用者セキュリティ属性の最初の関連付けに関する次の規則を実施しなければならない：[割付：属性の最初の関連付けに関する規則]

[割付：属性の最初の関連付けに関する規則]： 表 6-11 に示す。

表 6-11 属性の最初の関連付けに関する規則

利用者	利用者を代行して動作するサブジェクト	利用者セキュリティ属性（操作員種別）
サーバ管理者	サーバ管理者プロセス	サーバ管理者
監査者	監査者プロセス	監査者
個人情報管理者	個人情報管理者プロセス	個人情報管理者
オペレータ	オペレータプロセス	オペレータ
個人情報利用者	個人情報利用者プロセス	個人情報利用者

FIA_USB.1.3 TSF は、TSF は、以下の利用者セキュリティ属性への変更を管理する規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。:[割付： 属性の変更に関する規則]
[割付：属性の変更に関する規則]：
操作員種別を変更する役割は存在しない。

依存性： FIA_ATD.1 利用者属性定義

○セキュリティ管理（FMT）

FMT_MSA.3 静的属性初期化（個人データ種別）

下位階層： なし

FMT_MSA.3.1 TSF は、その SFP を実施するために使われるセキュリティ属性として、[選択：制限的、許可的：から一つのみ選択、[割付：その他の特性]]デフォルト値を与える[割付：アクセス制御 SFP、情報フロー制御 SFP]を実施しなければならない。

[選択：制限的、許可的：から一つのみ選択、[割付：その他の特性]]：
その他の特性

[割付：その他の特性]：表 6-12 に示す。

表 6-12 オブジェクトに関連付けられるセキュリティ属性

オブジェクト	オブジェクトに関連付けられるセキュリティ属性（個人データ種別）
個人データレコード	個人データ
未登録個人データレコード	未登録個人データ
個人データの提供データレコード	個人データの提供データ
個人データの預託データレコード	個人データの預託データ
個人データの加工データレコード	個人データの加工データ
個人データに関する承認依頼（登録用）レコード	個人データに関する承認依頼（登録用）
個人データに関する承認依頼（更新用）レコード	個人データに関する承認依頼（更新用）
個人データに関する承認依頼（削除用）レコード	個人データに関する承認依頼（削除用）
個人データに関する承認依頼（提供用）レコード	個人データに関する承認依頼（提供用）
個人データに関する承認依頼（預託用）レコード	個人データに関する承認依頼（預託用）
バックアップデータレコード	バックアップデータ

[割付：アクセス制御 SFP、情報フロー制御 SFP] ：
個人情報処理メイン機能アクセス制御方針
外部入出力アクセス制御方針

FMT_MSA.3.2 TSF は、オブジェクトや情報が生成されるとき、[割付：許可された識別された役割]が、デフォルト値を上書きする代替の初期値を指定することを許可しなければならない。

[割付：許可された識別された役割]： なし

依存性： FMT_MSA.1 セキュリティ属性の管理
FMT_SMR.1 セキュリティの役割

FMT_MTD.1 TSF データの管理

下位階層： なし

FMT_MTD.1.1 TSF は、[割付: TSF データのリスト]を[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]する能力を[割付: 許可された識別された役割]に制限しなければならない。

[割付：TSF データのリスト]：表 6-13 に示す。

[選択：デフォルト値変更、問い合わせ、改変、削除、消去、[割付：その他の操作]]：表 6-13 に示す。

[割付：その他の操作]：表 6-13 に示す。

[割付：許可された識別された役割]：表 6-13 に示す。

表 6-13 TSF データの管理

TSF データ	選択：デフォルト値変更、問い合わせ、改変、削除、消去、その他の操作	許可された識別された役割
セキュリティ侵害の可能性を判断するために用いる監査証跡の重要度	改変	監査者
サーバ管理者の操作員 ID	問い合わせ、削除、作成	サーバ管理者
サーバ管理者のパスワード	作成	サーバ管理者
監査者、個人情報管理者の操作員 ID	問い合わせ、削除、作成	サーバ管理者
監査者、個人情報管理者のパスワード	削除、作成	サーバ管理者
オペレータ、個人情報利用者の操作員 ID	問い合わせ、削除、作成	個人情報管理者
オペレータ、個人情報利用者のパスワード	削除、作成	個人情報管理者
操作員自身のパスワード	改変	オペレータ 個人情報利用者 個人情報管理者 サーバ管理者 監査者
サーバ共通鍵	問い合わせ、改変、削除、作成	サーバ管理者
処理連携サーバ共通鍵	問い合わせ、改変、削除、作成	サーバ管理者
サーバ秘密鍵	問い合わせ、改変、削除、作成	サーバ管理者
サーバ公開鍵	問い合わせ、改変、削除、作成	サーバ管理者
	問い合わせ	オペレータ 個人情報利用者 個人情報管理者 監査者
提供・預託先共通鍵	問い合わせ、削除、インポート	サーバ管理者
	問い合わせ	個人情報管理者
セション鍵	問い合わせ、削除、作成	オペレータ 個人情報利用者 個人情報管理者 監査者

TSF データ	選択：デフォルト値変更、問い合わせ、改変、削除、消去、その他の操作	許可された識別された役割
操作員の最後に成功した認証以降の不成功認証試行回数の定義	問い合わせ、改変	サーバ管理者
バナー表示メッセージ	問い合わせ、改変、作成	サーバ管理者
操作員種別毎のセション確立許可時間帯	問い合わせ、改変、作成	サーバ管理者
監査証跡	問い合わせ、削除、エクスポート、インポート	監査者
	問い合わせ	サーバ管理者

表 6-13 で示された許可された識別された役割は、制御された TSF データに対して、制御された操作のみを行うことができる。

依存性： FMT_SMF.1 管理機能の特定
FMT_SMR.1 セキュリティ役割

FMT_SMF.1 管理機能の特定

下位階層： なし

FMT_SMF.1.1 TSF は、以下の管理機能を実行することができなければならない。: [割付: TSF によって提供される管理機能のリスト]

[割付：TSF によって提供されるセキュリティ管理機能のリスト]：
表 6-14 に示す。

表 6-14 セキュリティ管理機能の特定

機能要件	管理要件	管理項目
FAU_ARP.1	1) アクションの管理(追加、除去、改変)。	なし（アクションは固定であり、管理対象とならない）
FAU_GEN.1	なし	なし
FAU_GEN.2	なし	なし
FAU_SAA.1	1) 規則のセットから規則を(追加、改変、削除)することによる規則の維持。	セキュリティ侵害の可能性の判断に用いる監査データの重要度の管理
FAU_SAR.1	1) 監査記録に対して読み出し権のある利用者グループの維持(削除、改変、追加)。	なし（アクションは固定であり、管理対象とならない）
FAU_SAR.2	なし	なし
FAU_SAR.3	なし	なし
FAU_STG.1	なし	なし
FAU_STG.3	1) 閾値の維持; 2) 監査格納失敗が切迫したときにとられるアクションの維持(削除、改変、追加)。	なし（閾値、アクションは固定であり、管理対象とならない）
FAU_STG.4	1) 監査格納失敗時にとられるアクションの維持（削除、改変、追加)。	なし（アクションは固定であり、管理対象とはならない）
FCS_CKM.1	1) 暗号鍵属性の変更の管理。鍵の属性の例としては、鍵種別(例えば、公開、秘密、共通)、有効期間、用途(例えば、ディジタル署名、鍵暗号化、鍵交換、データ暗号化)などがある。	なし（アクションは固定であり、管理対象とならない）
FCS_CKM.4	1) 暗号鍵属性の変更の管理。鍵の属性の例としては、鍵種別(例えば、公開、秘密、共通)、有効期間、用途(例えば、ディジタル署名、鍵暗号化、鍵交換、データ暗号化)などがある。	なし（アクションは固定であり、管理対象とならない）
FCS_COP.1	なし	なし
FDP_ACC.1a	なし	なし
FDP_ACC.1b	なし	なし
FDP_ACF.1a	1) 明示的なアクセスまたは拒否に基づく決定に使われる属性の管理。	なし （変更不可のため管理項目はない）

機能要件	管理要件	管理項目
FDP_ACF.1b	1) 明示的なアクセスまたは拒否に基づく決定に使われる属性の管理	なし （変更不可のため管理項目はない）
FDP_ETC.2	なし	なし
FDP_ITC.2	1) インポートに対して使用される追加の制御規則の改変。	なし（アクションは固定であり、管理対象とならない）
FIA_AFL.1	1) 不成功の認証試行に対する閾値の管理 2) 認証失敗の事象においてとられるアクションの管理	1) 不成功の認証試行に対する閾値の管理 2) なし（アクションは固定であり、管理対象とならない）
FIA_ATD.1	1) もし割付に示されていれば、許可管理者は利用者に対する追加のセキュリティ属性を定義することができる	なし（アクションは固定であり、管理対象とならない）
FIA_SOS.1	1) 秘密の検証に使用される尺度の管理	なし（アクションは固定であり、管理対象とならない）
FIA_UAU.1a	1) 管理者による認証データの管理 2) 関係する利用者による認証データの管理 3) 利用者が認証される前にとられるアクションのリストを管理すること	1) クライアント操作員のパスワードの登録 2) クライアント操作員のパスワードの改変 3) なし（アクションは固定であり、管理対象とならない）
FIA_UAU.1b	1) 管理者による認証データの管理 2) 関係する利用者による認証データの管理 3) 利用者が認証される前にとられるアクションのリストを管理すること	1) サーバ管理者のパスワードの登録 2) サーバ管理者のパスワードの改変 3) なし（アクションは固定であり、管理対象とならない）
FIA_UID.1a	1) 利用者識別情報の管理 2) 許可管理者が、識別前に許可されるアクションを変更できる場合、そのアクションリストを管理すること	1) クライアント操作員 ID の作成、問い合わせ、削除 2) なし（アクションは固定であり、管理対象とならない）
FIA_UID.1b	1) 利用者識別情報の管理 2) 許可管理者が、識別前に許可されるアクションを変更できる場合、そのアクションリストを管理すること	1) サーバ管理者 ID の作成、問い合わせ、削除 2) なし（アクションは固定であり、管理対象とならない）
FIA_USB.1	1) 許可管理者は、デフォルトのサブジェクトのセキュリティ属性を定義できる 2) 許可管理者は、デフォルトのサブジェクトのセキュリティ属性を変更できる	1) サーバ管理者はサーバ管理者、監査者、個人情報管理者の操作員種別を付与でき、個人情報管理者はオペレータと個人情報利用者の操作員種別を付与できる 2) なし（許可する役割はない）
FMT_MSA.3	1) 初期値を特定できる役割のグループを管理すること 2) 所定のアクセス制御 SFP に対するデフォルト値の許可的あるいは制限的設定を管理すること	1) なし（初期値を特定できる役割は存在しない） 2) なし（管理する役割はない）
FMT_MTD.1	1) TSF データと相互に影響を及ぼし得る役割のグループを管理すること	なし（TSF データと相互に影響を及ぼし得る役割のグループは固定）
FMT_SMF.1	なし	なし
FMT_SMR.2	1) 役割の一部をなす利用者のグループを管理すること 2) 役割が満たさなければならない条件を管理すること	なし（役割の一部をなす利用者のグループ、役割が満たさなければならない条件は固定）
FTA_SSL.3	1) 個々の利用者に対し対話セションの終了を生じさせる利用者が非アクティブである時間の特定 2) 対話セションの終了を生じさせる利用者が非アクティブであるデフォルト時間の特定	なし（アクションは固定であり、管理対象とならない）
FTA_TAB.1	1) 許可管理者によるバナーの維持	1) バナー表示メッセージの管理
FTA_TSE.1	1) 許可管理者によるセション確立条件の管理	1) 操作員種別毎のセション確立許可時間帯の管理
FPT_TST.2	1) TSF 自己テストが動作する条件の管理	なし（アクションは固定であり、管理対象とはならない）
FPT_STM.1	1) 時間の管理	なし（システム内時刻の管理は、OS により行われるため、管理対象とならない）

依存性： なし

FMT_SMR.2 セキュリティ役割における制限

下位階層： FMT_SMR.1

FMT_SMR.2.1 TSF は、役割[割付：許可された識別された役割]を維持しなければならない。

[割付：許可された識別された役割]：
・オペレータ
・個人情報利用者
・個人情報管理者
・サーバ管理者
・監査者

FMT_SMR.2.2 TSF は、利用者を役割に関連付けなければならない。

FMT_SMR.2.3 TSF は、条件[割付：異なる役割に対する条件]が満たされていることを保証しなければならない。

[割付：異なる役割に対する条件]：
一つの操作員アカウントは、オペレータ、個人情報利用者、個人情報管理者、サーバ管理者、監査者を兼ねられない。

依存性： FIA_UID.1 識別のタイミング

○TOE アクセス（FTA）

FTA_SSL.3 TSF 起動による終了

下位階層： なし

FTA_SSL.3.1 TSF は、[割付：利用者が非アクティブである時間間隔]後に対話セションを終了しなければならない。

[割付：利用者が非アクティブである時間間隔]：
TOE への最後の操作から 15 分

依存性： なし

FTA_TAB.1 デフォルト TOE アクセスバナー

下位階層： なし

FTA_TAB.1.1 利用者セション確立前に、TSF は、TOE の不正な使用に関する勧告的警告メッセージを表示しなければならない。

依存性： なし

FTA_TSE.1 TOE セション確立

下位階層： なし

FTA_TSE.1.1 TSF は、[割付：属性]に基づきセション確立を拒否できなければならない。

[割付：属性]： セション確立要求時刻、操作員種別

依存性： なし

○TSF の保護（FPT）

FPT_TST.2 簡易 TSF テスト

下位階層： なし

FPT_TST.2.1 TSF は、[割付：自己テストが作動すべき条件]下で、自己テストを実行しなければならない。

[割付：自己テストが作動すべき条件]：
クライアント操作員がクライアント端末を利用してサーバ端末に対しアクセスする時の、識別認証が行われる前

FPT_TST.2.2 TSF は、自己テストを行うことによって、[選択：[割付：TSF の一部]、TSF 全体、[割付：TSF データの一部]、TSF データ全体]の完全性を検証することができなければならない。

[選択：[割付：TSF の一部]、TSF 全体、[割付：TSF データの一部]、TSF データ全体]：

[割付：TSF の一部]：個人情報処理システムクライアント用アプリケーションパッケージ

依存性： FPT_AMT.1 抽象マシンテスト

6.2. セキュリティ保証要件

TOE セキュリティ保証要件を示す。
本 TOE の評価保証レベルは EAL3 である。全てのセキュリティ保証要件は CC パート 3 に規定されているセキュリティ保証コンポーネントを直接使用する。

(1) 開発（ADV）
- ADV_ARC.1 : セキュリティアーキテクチャ記述
- ADV_FSP.3 : 完全な要約を伴う機能仕様
- ADV_TDS.2 : アーキテクチャ設計

(2) ガイダンス文書（AGD）
- AGD_OPE.1 : 利用者操作ガイダンス
- AGD_PRE.1 : 準備手続き

(3) ライフサイクルサポート（ALC）
- ALC_CMC.3 : 許可の管理
- ALC_CMS.3 : 実装表現の CM 範囲
- ALC_DEL.1 : 配付手続き
- ALC_DVS.1 : セキュリティ手段の識別
- ALC_LCD.1 : 開発者によるライフサイクルモデルの定義

(4) セキュリティターゲット評価（ASE）
- ASE_CCL.1 : 適合主張
- ASE_ECD.1 : 拡張コンポーネント定義
- ASE_INT.1 : ST 概説
- ASE_OBJ.2 : セキュリティ対策方針
- ASE_REQ.2 : 派生したセキュリティ要件
- ASE_SPD.1 : セキュリティ課題定義
- ASE_TSS.1 : TOE 要約仕様

(5) テスト（ATE）
- ATE_COV.2 : カバレージの分析
- ATE_DPT.1 : テスト：基本設計
- ATE_FUN.1 : 機能テスト
- ATE_IND.2 : 独立テスト – サンプル

(6) 脆弱性評定（AVA）
- AVA_VAN.2 : 脆弱性分析

6.3. セキュリティ要件根拠

6.3.1. セキュリティ機能要件根拠

セキュリティ機能要件と TOE セキュリティ対策方針の対応関係を表 6-15 に示す。この表で示す通り、各セキュリティ機能要件が、少なくとも 1 つの TOE セキュリティ対策方針に対抗している。

表 6-15 セキュリティ機能要件とセキュリティ対策方針の対応関係

	O.I&A	O. ACCESS_CONTROL	O.TAKE_OUT	O.AUDIT	O.ALERT	O.RECOMMEND	O.AUTO_LOGOUT	O.USERDATA_PROTECTION	O.BACKUP_RECOVERY	O.AVAILABLE_TIME_RESTRICTION
FAU_ARP.1					×					
FAU_GEN.1				×						
FAU_GEN.2				×						
FAU_SAA.1					×					
FAU_SAR.1				×						
FAU_SAR.2				×						
FAU_SAR.3				×						
FAU_STG.1				×						
FAU_STG.3				×						
FAU_STG.4				×						
FCS_CKM.1								×		
FCS_CKM.4								×		
FCS_COP.1								×		
FDP_ACC.1a		×	×							
FDP_ACC.1b		×							×	
FDP_ACF.1a		×	×							
FDP_ACF.1b		×							×	
FDP_ETC.2									×	
FDP_ITC.2									×	
FIA_AFL.1	×									
FIA_ATD.1	×	×								
FIA_SOS.1	×									
FIA_UAU.1a	×									
FIA_UAU.1b	×									
FIA_UID.1a	×									
FIA_UID.1b	×									
FIA_USB.1	×	×								
FMT_MSA.3		×	×							
FMT_MTD.1		×		×				×		
FMT_SMF.1		×								
FMT_SMR.2		×								
FTA_SSL.3							×			
FTA_TAB.1						×				
FTA_TSE.1										×
FPT_TST.2			×							

次に、各 TOE セキュリティ対策方針が、セキュリティ機能要件により実現できることを説明する。

各セキュリティ対策方針に対し、必要な対策の詳細を分析する。次に、それぞれの対策に対し、要求される機能を示し、それがすべて満たされることでセキュリティ対策方針を実現することができることを示す。なお、要求される機能については、一つ以上のセキュリティ機能要件がそれを満たし、セキュリティ対策方針に対する機能要件として必要であることを示す。

O.I&A（識別認証）

この TOE セキュリティ対策方針は、正当な操作員が TOE を利用するための、利用者の制限を求めている。この要求に対し、必要な対策の詳細と、求められる機能は以下のとおりである。

a. TOE 利用前に、操作員を識別する。

操作員が TOE を利用する前には、利用を許可されている者であることが識別されなければならない。よって、操作員が識別される前に実行が許可される TSF は、操作員を識別するための TSF のみである。ただし、クライアント操作員の識別時には、勧告的警告メッセージの表示、セション鍵生成、及びクライアント端末用パッケージの正当性検証も許可される。また、サーバ管理者の識別時には、勧告的警告メッセージの表示も許可される。この要件に該当するセキュリティ機能要件は、FIA_UID.1a、及び FIA_UID.1b である。

b. TOE 利用前に、操作員を認証する。

操作員が TOE を利用する前には、利用を許可されている者であることが認証されなければならない。よって、操作員が認証される前に実行が許可される TSF は、操作員を認証するための TSF のみである。この要件に該当するセキュリティ機能要件は、FIA_UAU.1a、及び FIA_UAU.1b である。

c. 認証情報の品質を検証する。

識別認証の機能強度を確保するためには、利用者認証情報が、利用者本人以外に予測されることが困難でなければならない。予測されることが困難であるためには、利用者認証情報に対し、必要なレベルの品質を明確に定義し、その品質が満たされていることを検証しなければならない。この要件に該当するセキュリティ機能要件は、FIA_SOS.1 である。

d. 識別認証に成功した時に、TOE の利用を許可する。

識別認証に成功した操作員は、同じく成功した端末を用いて TOE を利用できなければならない。TOE 利用に際しては、TOE は操作員を代行するサブジェクトを生成し、操作員は TSF を実施するために使用するセキュリティ属性を関連付けられる。この要件に該当するセキュリティ機能要件は、FIA_ATD.1、及び FIA_USB.1 である。

e. 指定回数以内に識別・認証に成功しない場合、TOE の利用を無効とする。

識別認証に失敗した操作員は、TOE の正当な利用者ではないとみなす必要がある。TOE は指定した回数識別認証に失敗した操作員に対し、あらかじめ定義されたアクション(アカウントのロック、または一定期間の無効化)を実施しなければならない。この要件に該当するセキュリティ機能要件は、FIA_AFL.1 である。

以上、a、b、c、d、e すべての対策を満たすことは、O.I&A を満たすことである。したがって、それぞれの対策に必要な機能要件として該当する、FIA_AFL.1、FIA_ATD.1、FIA_SOS.1、FIA_UAU.1a、FIA_UAU.1b、FIA_UID.1a、FIA_UID.1b、及び FIA_USB.1 の達成により、O.I&A を実現できる。

O. ACCESS_CONTROL （アクセスコントロール）

この TOE セキュリティ対策方針は、操作員または操作員を代行するプロセスが、あ

らかじめ決定された保護資産に対するアクセス権限に応じて、アクセスが許可されることを求めている。この要求に対し、必要な対策の詳細と、求められる機能は以下のとおりである。

a. アクセス制御を規定し、実施する。

各操作員に対して許可する操作と対象を決定し、そのとおりに実施しなければならない。よって、操作員を代行して動作するサブジェクトと、操作対象（オブジェクト）の操作リストを定義し、それらに付与されるセキュリティ属性に従ってアクセス制御を実施する。この要件に該当するセキュリティ機能要件は、FDP_ACC.1a、FDP_ACC.1b、FDP_ACF.1a、及び FDP_ACF.1b である。

b. 操作員をプロセスに関連付ける。

操作員に応じてアクセスを制限するためには、TOE 利用に際し各操作員が持つ利用者セキュリティ属性が自分を代行して動作するプロセス（サブジェクト）に関連付けられなければならない。よって、操作員は、それぞれの利用者セキュリティ属性である操作員種別を持ち、操作員を代行して動作するサブジェクトに操作員種別が関連付けられる。この要件に該当するセキュリティ機能要件は、FIA_ATD.1、及び FIA_USB.1 である。

c. 意図したとおりアクセス制御が行われるために、TOE の動作に重大な影響を及ぼす操作を管理者に制限し、各操作員に必要な操作権限を与える。

アクセス制御の対象となるオブジェクトには、セキュリティ属性である個人データ種別が付与される。その付与されたセキュリティ属性の値に応じて、各操作員のアクセスの可否が決定される。同種のオブジェクトに対し、アクセス制御規則が変動することはないため、個人データ種別は同種のオブジェクトに対して固定されていなければならず、デフォルト値から改変されることなく、その役割を持つ操作員も存在しない。この要件に該当するセキュリティ機能要件は、FMT_MSA.3 である。

また、TOE の動作に影響を及ぼす設定について、管理する権限を持つ者を制限しなければならない。よって、サーバ管理者、及びクライアント操作員に対し、それぞれに許可された役割を定義することで許可されていない操作を禁止し、各操作員は必要なセキュリティ機能の管理を行う。この要件に該当するセキュリティ機能要件は、FMT_MTD.1、及び FMT_SMF.1 である。

これらの許可された操作は各操作員に応じて決められ、異なる操作員の権限を兼ねることを許可しない。よって、許可された役割を定義し、各操作員はその役割に関連付けられることで、操作の権限を持つ。また、複数の役割を兼任することはできない。この要件に該当するセキュリティ機能要件は、FMT_SMR.2 である。

以上、a、b、c すべての対策を満たすことは、O.ACCESS_CONTROL を満たすことである。したがって、それぞれの対策に必要な機能要件として該当する、FIA_ATD.1、FIA_USB.1 、 FDP_ACC.1a 、 FDP_ACC.1b 、 FDP_ACF.1a 、 FDP_ACF.1b 、FMT_MSA.3、FMT_MTD.1、FMT_SMF.1、及び FMT_SMR.2 の達成により、O.ACCESS_CONTROL を実現できる。

O.TAKE_OUT（クライアント端末を経由した TOE 外への利用者データの持出し）

この TOE セキュリティ対策方針は、クライアント端末を経由した利用者データの TOE 外への持ち出し（保存、印刷）の禁止について求めている。この要求に対し、必要な対策の詳細と、求められる機能は以下のとおりである。

a. クライアント端末への保存、クライアント端末からの印刷を禁止する。

クライアント端末を経由した TOE 外への持ち出しは、クライアント端末から外部記憶媒体への保存、または印刷が考えられる。これらを制限することで、TOE 外部への持ち出しを禁止しなければならない。この要件に該当するセキュリティ機能要件は、FDP_ACC.1a、及び FDP_ACF.1a である。

そして、これを実現するためには、クライアント操作員がクライアント端末を利用

する前に、持ち出しを制限するソフトウェアがクライアント端末にインストールされていることを検証し、満たした場合のみクライアント端末がサーバ端末にアクセスすることを許可する必要がある。そのために、クライアント端末用 TSF の正当性を検証する。この要件に該当するセキュリティ機能要件は、FTP_TST.2 である。
また、アクセス制御の対象となるオブジェクトには、セキュリティ属性である個人データ種別が付与され、その付与されたセキュリティ属性の値に応じて、各操作員のアクセスの可否が決定される。同種のオブジェクトに対し、アクセス制御規則が変動することはないため、個人データ種別は同種のオブジェクトに対して固定されていなければならず、デフォルト値から改変されることなく、その役割を持つ操作員も存在しない。この要件に該当するセキュリティ機能要件は、FMT_MSA.3 である。

以上、a の対策を満たすことは、O.TAKE_OUT を満たすことである。したがって、それぞれの対策に必要な機能要件として該当する、FDP_ACC.1a、FDP_ACF.1a、FPT_TST.2、及び FMT_MSA.3 の達成により、O.TAKE_OUT を実現できる。

O.AUDIT（監査）

このTOEセキュリティ対策方針は、監査証跡の取得とその保護について求めている。
監査証跡は TOE に対するセキュリティ侵害の状況を後日確認するための証拠となる情報であり、必要となった時点で利用できなければならない。このため、監査証跡の保護では、監査証跡の確実な取得、監査証跡の改ざんを考慮する。この要求に対し、必要な対策の詳細と、求められる機能は以下のとおりである。

a. 監査証跡として必要な情報を取得する。

TSF による監査対象とすべき事象について、必要な情報を記録しなければならない。利用者セキュリティ属性管理機能を使用しようとするすべての試みについて、事象の日付・時刻、プロセス ID、及びサブジェクト識別情報を含む監査証跡を生成する。つまり、セキュリティメカニズムに対するあらゆる使用についての監査（監査レベル：基本）を求める。この要件に該当するセキュリティ機能要件は、FAU_GEN.1 である。
監査証跡の取得において、事象を起こした主体を明らかにしなければならない。よって、監査対象事象を、その原因となった識別情報に関連付ける。この要件に該当するセキュリティ機能要件は、FAU_GEN.2 である。

b. すべての監査証跡を取得する。

監査の対象とする事象は、すべて監査証跡として取得されなければならない。このため、監査証跡の取得が不可能となる前にこれを検知し、必要な処置を行わなければならない。よって、監査証跡が事前に定義された限界値を超えると、これをサーバ管理者・監査者に対し通知する。また、監査証跡を格納する領域が枯渇した場合は、最も古くに格納された監査証跡を上書きすることで、最新の事象を監査証跡として取得し、これをサーバ管理者・監査者に対し通知する。なお、セキュリティ侵害については、別途警告を発することが要求されているため、古い監査証跡より最新の監査証跡が優先される。また、監査証跡退避機能が TOE により提供されているため、古い監査証跡は定期的に TOE 外へ退避されることができ、監査証跡の事実上の損失の可能性は低い。この要件に該当するセキュリティ機能要件は、FAU_STG.3、FAU_STG.4 である。

c. 監査証跡の改ざんを防御し、検出する。

監査証跡は TOE の動作を後日検証するための証拠となる情報であるため、改ざんを防御し、これを検出しなければならない。DB 内の監査証跡の保護に該当するセキュリティ機能要件は、FAU_STG.1 である。

d. 取得した監査証跡の利用者、及び利用内容を制限する。

監査証跡を読み出すことを、許可された者のみに制限する。監査証跡を読み出して

利用することについて、サーバ管理者と監査者のみに利用を許可し、それ以外の者の利用を禁止する。この要件に該当するセキュリティ機能要件は、FAU_SAR.1、及び FAU_SAR.2 である。

監査証跡の利用においては、検索、及び並べ替えができなければならない。監査証跡の利用にあたっては、指定された条件を用いた検索、及び並べ替えを提供する。この要件に該当するセキュリティ機能要件は、FAU_SAR.3 である。

監査証跡の削除を、許可された者のみに制限する。これらの作業は監査者のみに許可し、それ以外の者の作業を禁止する。この要件に該当するセキュリティ機能要件は FMT_MTD.1 である。

監査証跡の退避（エクスポート、及びインポート）を、許可された者のみに制限する。これらの作業は監査者のみに許可し、それ以外の者の作業を禁止する。この要件に該当するセキュリティ機能要件は FMT_MTD.1 である。

以上、a、b、c、d すべての対策を満たすことは、O.AUDIT を満たすことである。したがって、それぞれの対策に必要な機能要件として該当する、FAU_GEN.1、FAU_GEN.2、FAU_SAR.1、FAU_SAR.2、FAU_SAR.3、FAU_STG.1、FAU_STG.3、FAU_STG.4、及び FMT_MTD.1 の達成により、O.AUDIT を実現できる。

O.ALERT（アラート）

この TOE セキュリティ対策方針は、セキュリティ侵害の可能性を検出した際のアラート通知について求めている。この要求に対し、必要な対策の詳細と、求められる機能は以下のとおりである。

a. セキュリティ侵害の可能性を検出する。

取得した監査証跡から、セキュリティ侵害の可能性について検出しなければならない。よって、監査対象事象の発生に際し、あらかじめ決められた閾値を監査証跡に付加し、閾値に応じてセキュリティ侵害の可能性を検出する。すべての監査対象事象に関して、監査者が定めた重要度を含む監査証跡が生成された場合に、セキュリティ侵害の可能性があると判断する。この要件に該当するセキュリティ機能要件は、FAU_SAA.1 である。

b. 検出したセキュリティ侵害の可能性について通知する。

セキュリティ侵害の可能性が検出された時、自動的な応答を返さなければならない。よって、セキュリティ侵害の可能性の検出によって、サーバ管理者と監査者に対するアラート通知を行う。この要件に該当するセキュリティ機能要件は、FAU_ARP.1 である。

以上、a、b すべての対策を満たすことは、O.ALERT を満たすことである。したがって、それぞれの対策に必要な機能要件として該当する、FAU_ARP.1、及び FAU_SAA.1 の達成により、O.ALERT を実現できる。

O.RECOMMEND（勧告）

この TOE セキュリティ対策方針は、操作員に対する勧告的警告メッセージの表示について求めている。この要求に対し、必要な対策の詳細と、求められる機能は以下のとおりである。

a. 操作員に勧告的警告メッセージを表示する。

操作員が不正な操作を試みた際には、勧告的警告メッセージを表示しなければならない。利用者セッション確立前に、不正な利用に関する勧告的警告メッセージを表示する。この要件に該当するセキュリティ機能要件は、FTA_TAB.1 である。

以上、a の対策を満たすことは、O.RECOMMEND を満たすことである。したがって、その対策に必要な機能要件として該当する、FTA_TAB.1 の達成により、O.RECOMMEND を実現できる。

O.AUTO_LOGOUT（自動ログアウト）

この TOE セキュリティ対策方針は、TOE と操作員との対話セションの自動終了について求めている。この要求に対し、必要な対策の詳細と、求められる機能は以下のとおりである。

a. 対話セションを終了する。

操作員が一定時間 TOE を操作しない状態が続くと、TOE と操作員との対話セションを終了しなければならない。操作員が TOE を操作しない時間があらかじめ決められた時間間隔を超えると、TOE と操作員との対話セションを切断する。この要件に該当するセキュリティ機能要件は、FTA_SSL.3 である。

以上、a の対策を満たすことは、O.AUTO_LOGOUT を満たすことである。したがって、その対策に必要な機能要件として該当する、FTA_SSL.3 の達成により、O.AUTO_LOGOUT を実現できる。

O.USERDATA_PROTECTION（利用者データの保護）

この TOE セキュリティ対策方針は、利用者データの保護について求めている。その対策として暗号操作を用いて利用者データを保護する必要がある。この要求に対し、必要な対策の詳細と、求められる機能は以下のとおりである。

a. 暗号鍵を生成する。

バックアップデータ、及び通信データを暗号化するための暗号鍵を生成しなければならない。よって、それぞれの暗号化／復号に必要な暗号鍵を生成するための暗号アルゴリズムと暗号鍵長を決定する。この要件に該当するセキュリティ機能要件は、FCS_CKM.1 である。

b. 暗号操作を行う。

決められた暗号鍵、及び暗号アルゴリズムに従って、暗号操作を行わなければならない。よって、それぞれに該当する暗号操作について決定する。この要件に該当するセキュリティ機能要件は、FCS_COP.1 である。

c. 暗号鍵を安全に破棄する。

使用された暗号鍵は、不正に再利用されないように安全に破棄されなければならない。よって、暗号鍵の破棄の方法を決定する。この要件に該当するセキュリティ機能要件は、FCS_CKM.4 である。

d. TOE 外部から暗号鍵を受領する。

TOE 外部へ利用者データを取り出すものとして、提供・預託データのエクスポートが存在する。この提供・預託データについても暗号化によるデータの保護を行うが、暗号化に利用する鍵は、TOE で生成せず、提供・預託データの受信者から暗号化に使用する公開鍵を受領する。よって、TOE 外部で生成した暗号鍵を利用するために TOE 内部へインポートするものをサーバ管理者のみに制限する。この要件に該当するセキュリティ機能要件は、FMT_MTD.1 である。

また、インポートした暗号鍵の取り扱いを許可する者をサーバ管理者、及び個人情報管理者に制限する。この要件に該当するセキュリティ機能要件は、FMT_MTD.1 である。

e. 暗号鍵の利用権限を管理する。

暗号化／復号の動作に影響を及ぼす暗号鍵について、管理する権限を持つ者を制限しなければならない。よって、サーバ管理者、及びクライアント操作員に対し、それぞれに許可された役割を定義することで、暗号鍵の許可されていない操作（暗号化/復号）を禁止し、各操作員は必要な暗号鍵のみ管理を行う。この要件に該当するセキュリティ機能要件は、FMT_MTD.1 である。

以上、a、b、c、d、e すべての対策を満たすことは、O.USERDATA_PROTECTION を満たすことである。したがって、その対策に必要な機能要件として該当する、

FCS_CKM.1、FCS_CKM.4、FCS_COP.1、FDP_ACC.1b、FDP_ACF.1b、及び FMT_MTD.1 の達成により、O.USERDATA_PROTECTION を実現できる。

O.BACKUP_RECOVERY（バックアップ／リカバリ）

この TOE セキュリティ対策方針は、TOE の保護資産を TOE 外部にバックアップすることと、そのデータを再度 TOE 内にリカバリすることについて求めている。この要求に対し、必要な対策の詳細と、求められる機能は以下のとおりである。

a. 対象データをバックアップする。

TOE の保護資産を TOE の外部にバックアップしなければならない。また、バックアップしたデータは障害時などの必要に応じて TOE にリカバリされるので、セキュリティ属性付きのバックアップデータを取得する。よって、TOE からデータをセキュリティ属性付きでエクスポートする機能を提供する。この要件に該当するセキュリティ機能要件は、FDP_ETC.2 である。

b. バックアップしたデータをリカバリする。

TOE の外部から、TOE の保護資産としてデータをリカバリしなければならない。リカバリするデータは、ハッシュ操作による改ざん検知の仕組みがとられ、物理的に保護された室内に保存されるため、正確なセキュリティ属性付きのバックアップデータのリカバリを行う。よって、TOE 外部からデータをセキュリティ属性付きでインポートする機能を提供する。この要件に該当するセキュリティ機能要件は、FDP_ITC.2 である。

c. バックアップ／リカバリを許可する者を制限する。

エクスポート／インポートするするデータについて、取り扱いを許可する者を制限する。よって、操作員を代行して動作するサブジェクトと、操作対象（オブジェクト）の操作リストを定義し、その定義に従ってアクセス制御を実施する。この要件に該当するセキュリティ機能要件は、FDP_ACC.1b、及び FDP_ACF.1b である。

以上、a、b、c すべての対策を満たすことは、O.BACKUP_RECOVERY を満たすことである。したがって、その対策に必要な機能要件として該当する、FDP_ACC.1b、FDP_ACF.1b、FDP_ETC.2、及び FDP_ITC.2 の達成により、O.BACKUP_RECOVERY を実現できる。

O.AVAILABLE_TIME_RESTRICTION（利用時間制限）

この TOE セキュリティ対策方針は、セション確立の時間的な制限について求めている。この要求に対し、必要な対策の詳細と、求められる機能は以下のとおりである。

a. セション確立を拒否する。

あらかじめ決められたアクセスが可能な時間帯を除き、利用者データへのアクセスを拒否できなければならない。よって、セション確立が許可された時間帯を除き、TOE への操作員からのセション確立を拒否する。この要件に該当するセキュリティ機能要件は、FTA_TSE.1 である。

以上、a の対策を満たすことは、O.AVAILABLE_TIME_RESTRICTION を満たすことである。したがって、その対策に必要な機能要件として該当する、FTA_TSE.1 の達成により、O.AVAILABLE_TIME_RESTRICTION を実現できる。

6.3.2. 依存性の検証

セキュリティ要件のコンポーネントの依存性を表 6-16 に示す。

表 6-16 セキュリティ要件のコンポーネントの依存性

項番	セキュリティ要件	CC パート 2 で規定されている依存コンポーネント	TOE の依存コンポーネント	依存性が満たされないコンポーネント	妥当性
1	FAU_ARP.1	FAU_SAA.1	FAU_SAA.1	なし	
2	FAU_GEN.1	FPT_STM.1	なし	FPT_STM.1	*5
3	FAU_GEN.2	FAU_GEN.1	FAU_GEN.1	なし	
		FIA_UID.1	FIA_UID.1a FIA_UID.1b	なし	
4	FAU_SAA.1	FAU_GEN.1	FAU_GEN.1	なし	
5	FAU_SAR.1	FAU_GEN.1	FAU_GEN.1	なし	
6	FAU_SAR.2	FAU_SAR.1	FAU_SAR.1	なし	
7	FAU_SAR.3	FAU_SAR.1	FAU_SAR.1	なし	
8	FAU_STG.1	FAU_GEN.1	FAU_GEN.1	なし	
9	FAU_STG.3	FAU_STG.1	FAU_STG.1	なし	
10	FAU_STG.4	FAU_STG.1	FAU_STG.1	なし	
11	FCS_CKM.1	[FCS_CKM.2、または FCS_COP.1]	FCS_COP.1	なし	
		FCS_CKM.4	FCS_CKM.4	なし	
		FMT_MSA.2	なし	FMT_MSA.2	*1
12	FCS_CKM.4	[FDP_ITC.1、または FDP_ITC.2、または FCS_CKM.1]	FCS_CKM.1	なし	
		FMT_MSA.2	なし	FMT_MSA.2	*1
13	FCS_COP.1	[FDP_ITC.1、または FDP_ITC.2、または FCS_CKM.1]	FCS_CKM.1	なし	
		FCS_CKM.4	FCS_CKM.4	なし	
		FMT_MSA.2	なし	FMT_MSA.2	*1
14	FDP_ACC.1a	FDP_ACF.1	FDP_ACF.1a	なし	
15	FDP_ACC.1b	FDP_ACF.1	FDP_ACF.1b	なし	
16	FDP_ACF.1a	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1a FMT_MSA.3	なし	
17	FDP_ACF.1b	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1b FMT_MSA.3	なし	
18	FDP_ETC.2	[FDP_ACC.1、あるいは FDP_IFC.1]	FDP_ACC.1b	なし	
19	FDP_ITC.2	[FDP_ACC.1、または FDP_IFC.1]	FDP_ACC.1b	なし	
		[FTP_ITC.1、または FTP_TRP.1]	なし	[FTP_ITC.1、または FTP_TRP.1]	*2
		FPT_TDC.1	なし	FPT_TDC.1	*2
20	FIA_AFL.1	FIA_UAU.1	FIA_UAU.1a FIA_UAU.1b	なし	
21	FIA_ATD.1	なし	なし	なし	
22	FIA_SOS.1	なし	なし	なし	
23	FIA_UAU.1a	FIA_UID.1	FIA_UID.1a	なし	
24	FIA_UAU.1b	FIA_UID.1	FIA_UID.1b	なし	
25	FIA_UID.1a	なし	なし	なし	
26	FIA_UID.1b	なし	なし	なし	
27	FIA_USB.1	FIA_ATD.1	FIA_ATD.1	なし	
28	FMT_MSA.3	FMT_MSA.1	なし	FMT_MSA.1	*3
		FMT_SMR.1	なし	FMT_SMR.1	*3
29	FMT_MTD.1	FMT_SMF.1	FMT_SMF.1	なし	
		FMT_SMR.1	FMT_SMR.2 (左記の上位階層)	なし	
30	FMT_SMF.1	なし	なし	なし	

項番	セキュリティ要件	CC パート 2 で規定されている依存コンポーネント	TOE の依存コンポーネント	依存性が満たされないコンポーネント	妥当性
31	FMT_SMR.2	FIA_UID.1	FIA_UID.1a FIA_UID.1b	なし	
32	FTA_SSL.3	なし	なし	なし	
33	FTA_TAB.1	なし	なし	なし	
34	FTA_TSE.1	なし	なし	なし	
35	FPT_TST.2	FPT_AMT.1	なし	FPT_AMT.1	*4

表 6-16 より、TOE セキュリティ機能要件は後述する例外を除きそれぞれの必要な依存関係をすべて満たしている。すべての例外について、依存関係は満たされなくても問題がない根拠を以下に示す。

*1) FCS_CKM.1、FCS_CKM.4、FCS_COP.1 → FMT_MSA.2

FCS_CKM.1、FCS_CKM.4、及び FCS_COP.1 で取り扱うセキュリティ属性は、各暗号鍵に関するものである。それぞれが標準化されたアルゴリズムに従って、属性の値が決定されており、操作員が設定・改変する値を受け入れることはない。よって、これらの依存関係は不要である。

*2) FDP_ITC.2 → FTP_ITC.1、FTP_TRP.1、FPT_TDC.1

リムーバブル媒体は、物理的に保護された室内に保管され、攻撃者によるデータの改ざんに対する脅威は想定されないため、インポートされるデータは正確なものである。また、インポートされるデータは暗号化されて保存されており、通信路上において完全性が満たされていることを、ハッシュ値を用いて確認することができる。よって、この依存関係は不要である。

*3) FMT_MSA.3a、FMT_MSA.3b → FMT_MSA.1、FMT_SMR.1

FMT_MSA.3a、及び FMT_MSA.3b の対象となるセキュリティ属性は、TOE により管理されており、操作員に対しデフォルト値変更・問い合わせ・改変・削除などの役割は存在せず、役割を維持する必要性もない。よって、この依存関係は不要である。

*4) FPT_TST.2 → FPT_AMT.1

本 TOE では、TSF(個人情報処理システムクライアント用アプリケーションパッケージ）が正当なものであることの検証を要求している。その検証においては、本 TOE における下層の抽象マシン(クライアント端末における OS やハードウェア）の動作は依存しない。よって、この依存関係は不要である。

*5) FAU_GEN.1 → FPT_STM.1

4.2 運用環境のセキュリティ対策方針 に示されるとおり、OE.TIME_STAMP の実現により、本 TOE が監査証跡を生成する際に利用する高信頼タイムスタンプは、TOE の運用環境によって提供される。よって、この依存関係は不要である。

6.3.3. セキュリティ保証要件根拠

本システムは、個人データを登録、閲覧・検索、提供、預託、加工、更新、及び削除するためのシステムである。2005 年 4 月には、個人情報の保護に関する法律（平成 15 年 5 月 30 日法律第 57 号）が完全施行されて社会の意識も高まり、個人情報に関する事故は、故意・ミスを問わず、大きな社会的・経営的問題に発展するケースがある。このため、本システムのセキュリティ機能には高い信頼性が要求される。EAL3 は TOE における開発段階のセキュリティ対策の分析(系統だったテストの実施と分析、及び開発環境や開発生産物の管理状況の評価）を含み、セキュリティ機能を安全に使用するための十分なガイダンス情報が含まれていることの分析が含まれるので妥当な選択であるといえる。

7. TOE 要約仕様

本章では、TOE が提供するセキュリティ機能の要約仕様について述べる。

7.1. TOE セキュリティ機能

表 7-1 に EA 1 について示す。

ここで示される通り、本節で説明するセキュリティ機能は、6.1 節に記述される全ての SFR を満たすものである。

表 7-1 TOE セキュリティ機能とセキュリティ機能要件の対応関係

	FAU_ARP.1	FAU_GEN.1	FAU_GEN.2	FAU_SAA.1	FAU_SAR.1	FAU_SAR.2	FAU_SAR.3	FAU_STG.1	FAU_STG.3	FAU_STG.4	FCS_CKM.1	FCS_CKM.4	FCS_COP.1	FDP_ACC.1a	FDP_ACC.1b	FDP_ACF.1a	FDP_ACF.1b	FDP_ETC.2	FDP_ITC.2	FIA_AFL.1	FIA_ATD.1
SF.Audit	×	×	×	×	×		×		×	×											
SF.ACC					×	×		×						×	×	×	×	×	×		×
SF.I&A																				×	
SF.Crypto											×	×	×								
SF.Import_Export																		×	×		

	FIA_SOS.1	FIA_UAU.1a	FIA_UAU.1b	FIA_UID.1a	FIA_UID.1b	FIA_USB.1	FMT_MSA.3	FMT_MTD.1	FMT_SMF.1	FMT_SMR.2	FTA_SSL.3	FTA_TAB.1	FTA_TSE.1	FPT_TST.2
SF.Audit									×					
SF.ACC						×	×	×	×	×				
SF.I&A	×	×	×	×	×				×		×	×	×	×
SF.Crypto														
SF.Import_Export														

以下では各 TOE セキュリティ機能に関して、その概要および対応する SFR の具体的な実現方法について説明する。

7.1.1. 監査機能（SF.Audit）

監査機能は、TOE がセキュアに運用されていることを監査するために必要な情報の採取及び管理を行う機能である。本機能では、監査の対象となる事象が発生した場合に、当該事象を監査証跡として採取する。また、サーバ管理者及び監査者向けの機能として、監査証跡参照機能、及び監査証跡管理機能を提供する。ただし、監査証跡を生成するのに必要な高信頼タイムスタンプは、OS により提供される。以下では監査機能について、SFR の実現方法という観点から説明する。

7.1.1.1. 対応する SFR の実現方法

(1) FAU_ARP.1 セキュリティアラーム

TOE は、監査証跡管理機能において下記機能を提供する。

- TOE は、すべての監査対象事象に関して、監査者の定めた重要度以上の重要度を含む監査証跡が生成された場合に、セキュリティ侵害の可能性があると判断し、サーバコンソールへの表示、及び監査者へのメールにより、サーバ管理者、及び監査者へのアラート通知を行う。セキュリティ侵害の可能性を判断するために選択可能な重要度は低、中、高のいずれか一つである。

この機能の実装により、FAU_ARP.1 を実現する。

(2) FAU_ GEN.1 監査データ生成

監査証跡は以下の監査対象事象の発生時に採取し、サーバ端末の DB にすべて格納する。

- 監査機能の起動と終了
  - 監査証跡参照機能の起動と停止
  - 監査証跡管理機能の起動と停止
  - 監査証跡の削除
  - 監査証跡領域枯渇の警告
  - セキュリティ侵害の可能性の判断に用いる監査証跡の重要度の管理と通知
- 監査証跡退避機能の起動と終了
  - 監査証跡のエクスポート、インポート
- サーバサブシステムのセットアップ
- サーバ管理者、監査者へのアラートイベントの通知
- 基本機能の起動と停止
- システム環境設定
  - セキュリティ侵害の可能性の判断に用いる監査証跡の重要度の管理
  - 不成功認証試行回数の管理
  - バナー表示メッセージの管理
  - 操作員種別毎のセション確立許可時間帯の管理
- アクセスの拒否
- 操作員の登録・編集・削除
- 操作員種別の付与
- 操作員の識別と認証
- クライアント端末用パッケージの正当性検証
- パスワードの変更
- 不成功の認証試行回数の閾値到達
（それに続いてとられるアクションを併せて記録する）
- 無効化されたアカウントの認証試行
- セションロックメカニズムによる対話セションの終了
- 鍵生成・変更・削除（生成・変更・削除した暗号鍵の情報を併せて記録する）

・暗号操作（暗号アルゴリズム、関連する操作員 ID、操作員種別、
暗号操作対象の権限リストを併せて記録する）
・個人データレコードの生成、更新、参照、及び削除
・個人データの提供・預託データレコードの生成、及び削除
・個人データの加工データレコードの生成、更新、参照、及び削除
・承認依頼レコードの生成、参照、及び削除
・未登録個人データレコードの参照、及び削除
・提供・預託先共通鍵のインポート
・バックアップデータレコードのエクスポート、及びインポート
・サーバサブシステムで発生したエラー
・提供・預託データレコードのエクスポートの成功と失敗
・未登録個人データレコードのインポートの成功と失敗

また、TOE が生成する監査証跡は以下の項目で構成される。

・プロセス ID　　：プロセスを一意に識別する番号
・サブジェクト識別情報　　：（セション鍵生成のみ）端末 ID
（それ以外の場合）登録されている操作員 ID
・事象の種別　　：事象の分類を表すもの
・重要度　　：なし、低、中、高の 4 種類
・事象の結果　　：成功／失敗
・事象の日付・時刻：OS から取得したタイムスタンプ情報を使用

この機能の実装により、FAU_GEN.1 を実現する。

(3) FAU_GEN.2 利用者識別情報の関連付け

上記監査証跡の項目中に示されているサブジェクト識別情報（端末 ID、または操作員 ID）により、各監査対象事象とその原因となった端末または操作員の識別情報との関連付けが可能となる。この機能の実装により、FAU_GEN.2 を実現する。

(4) FAU_SAA.1 侵害の可能性の分析

監査機能は、上記監査証跡の項目に示す通り、なし・低・中・高いずれかの値をとる重要度を監査証跡として取得し、この値をセキュリティ侵害の可能性を判断する際のパラメータとして使用する（監査者が予め定めた重要度以上の重要度を含む監査証跡が生成された場合にセキュリティ侵害の可能性があると判断する）。
これにより、ある規則に基づく侵害の可能性の分析を要求する FAU_SAA.1 を実現する。

(5) FAU_SAR.1 監査レビュー

TOE は、監査証跡参照機能において下記機能を提供する。

・ 取得した上記項目（プロセス ID、サブジェクト識別情報、事象の種別、重要度、事象の結果、事象の日付・時刻）により構成される監査証跡を、サーバ端末、監査者端末のコンソール上に、利用者が解釈可能な形式で表示する

この機能の実装および、後述するアクセス制御機能（SF.ACC）により、FAU_SAR.1 を実現する。

(6) FAU_SAR.3 選択可能監査レビュー

TOE は、監査証跡参照機能において下記機能を提供する。

・ 監査証跡の各項目（プロセス ID、サブジェクト識別情報、事象の種別、事象の結果（成功/失敗）、事象の日付・時刻、及び重要度）をキーにした監査証跡の検索、及び並べ替え

この機能の実装により、FAU_SAR.3 を実現する。

(7) FAU_STG.3 監査データ損失の恐れ発生時のアクション

TOE は、監査証跡管理機能において下記機能を提供する。

- 取得した監査証跡が、サーバサブシステムのセットアップ時に確保された DB 上の監査格納領域の 80%を超えた場合、監査格納領域の枯渇の恐れがある旨をサーバコンソールへの表示、監査者へのメール送信により、サーバ管理者、及び監査者に通知する

この機能の実装により、FAU_STG.3 を実現する。

(8) FAU_STG.4 監査データ損失の防止

TOE は、監査証跡管理機能において下記機能を提供する。

- 取得した監査証跡が、サーバサブシステムのセットアップ時に確保された DB 上の監査格納領域の 100%に達したとき、TOE は、領域の枯渇、及び作成日時が古い監査証跡から順番に削除する旨をサーバコンソールに通知するとともに、監査者へメールにより通知する。その上で、監査証跡の作成日時が古いものから順番に削除し、最新の監査証跡を生成する

この機能の実装により、FAU_STG.4 を実現する。

(9) FMT_SMF.1 管理機能の特定

TOE は、監査証跡管理機能においてセキュリティ侵害の可能性の判断に用いる、監査証跡の重要度を管理する。これは FMT_SMF.1 で要求される管理機能の一部であり、従って、この機能の実装および後述の識別認証機能、操作員管理・アクセス制御機能の実装により、FMT_SMF.1 を実現する。

7.1.2. 識別認証機能（SF.I&A）

識別認証機能は、TOE にアクセスする操作員を識別し、登録されている操作員本人であることを確認するための機能を提供する。また本機能は、操作員の識別認証に加え、操作員が使用するクライアント端末にインストールされたソフトウェアの正当性検証を行う機能を提供する。以下では識別認証機能について、SFR の実現方法という観点から説明する。

7.1.2.1. 対応する SFR の実現方法

(1) FIA_UID.1a 識別のタイミング、FIA_UAU.1a 認証のタイミング
（クライアント操作員）

TOE は、クライアント操作員の識別認証に関して以下の機能を提供する。

- TOE は、クライアント操作員の識別認証前に勧告的警告メッセージの表示、セション鍵生成、及びクライアント端末用パッケージの正当性検証のみを許可する
- 下記処理が 1→2→3→4 の順番ですべて成功した場合のみ、クライアント操作員の識別認証成功となる
    1. 勧告的警告メッセージの表示
    2. セション鍵の生成
    3. クライアント端末用パッケージの正当性検証
    4. クライアント操作員の識別認証

上記機能の実装により、FIA_UID.1a および FIA_UAU.1a を実現する。

(2) FIA_UID.1b 識別のタイミング、FIA_UAU.1b 認証のタイミング
（サーバ管理者）

TOE は、サーバ管理者の識別認証に関して以下の機能を提供する。

- TOE は、サーバ管理者の識別認証前に勧告的警告メッセージの表示のみを許可する
- 下記処理が 1→2 の順番ですべて成功した場合のみ、サーバ管理者の識別認証成功となる
    1. 勧告的警告メッセージの表示
    2. サーバ管理者の識別認証

上記機能の実装により、FIA_UID.1b および FIA_UAU.1b を実現する。

(3) FIA_SOS.1 秘密の検証

TOE は、ID・パスワード方式を用いるクライアント操作員、及びサーバ管理者の識別認証において下記機能を提供する。

- TOE は、操作員のパスワードが以下の条件を満たしていることを検証する
    - 6 文字以上 10 文字以下の、以下の範囲の ASCII 文字である
        - アルファベットは、大文字[A-Z]の 26 文字、小文字[a-z]の 26 文字の合計 52 文字
        - 数字は、[0-9]の合計 10 文字
        - 記号は、!"#$%&'()*+,-./:;<=>?@[¥]^_`{|}~ の 32 文字
    - 1 文字以上の数字または記号を含む
    - 2 文字以上のアルファベットを含む（大文字、小文字は区別される）
    - 新しいパスワードは、直前のパスワードと同一ではない
- TOE は、操作員の登録時及びパスワードの変更時において、新たなパスワードの候補として入力された文字列が上記の基準を満たさない場合には、パスワードの候補の再入力を要求する

この機能の実装により、FIA_SOS.1 を実現する。

(4) FIA_AFL.1 認証失敗時の取り扱い

TOE は、クライアント操作員、及びサーバ管理者の識別認証に関して以下の機能を提供する。

- 操作員が入力した ID に対するパスワードが異なる場合、操作員 ID 毎にパスワード誤り回数をカウントする
- 連続パスワード誤り回数が、サーバ管理者によって指定される最後の認証以降の不成功認証試行回数（1～5 回）に達すると、そのアカウントがサーバ管理者のものである場合には、当該アカウントを 5 分間無効化する（無効化が解除されると、不成功認証試行回数は 0 回に変更される）
- アカウントがクライアント操作員のものである場合には、当該アカウントをロックし、解除不可能とする
- 上記クライアント捜査員のアカウントを再び使用するためには、個人情報管理者もしくはサーバ管理者が当該アカウントを一度削除し再度アカウントを作成する

上記機能の実装により、FIA_AFL.1 を実現する。

(5) FPT_TST.2 簡易 TSF テスト

TOE は、クライアント操作員の識別認証に関して以下の機能を提供する。

- 上記「クライアント端末用パッケージの正当性検証」において、クライアント端末がサーバ端末に対し、自身にインストールされる個人情報処理システムクライアント用アプリケーションパッケージが正当なものであることを証明する

上記機能の実装により、FPT_TST.2 を実現する。

(6) FTA_TAB.1 デフォルト TOE アクセスバナー

TOE は、クライアント操作員、及びサーバ管理者の識別認証処理において、TOE 利用の前に、不正な利用に関する勧告的警告メッセージを表示する。
この機能の実装により、FIA_TAB.1 を実現する。
また、勧告的警告メッセージの作成、更新は、操作員管理・アクセス制御機能の実装により、サーバ管理者に限定される。

(7) FTA_SSL.3 TSF 起動による終了

TOE は、クライアント端末、サーバ端末間に確立するセションに関して以下の機能を提供する。

- TOE は、操作員 ID 毎に TOE への最後の操作時間を保持し、現在時刻との差が 15 分になるとセションを切断する
- 操作時間は、セションの切断により、0 に再設定される

上記機能の実装により、FTA_SSL.3 を実現する。

(8) FTA_TSE.1 TOE セション確立

TOE は、クライアント端末、サーバ端末間に確立するセションに関して以下の機能を提供する。

- TOE は、セション確立前に、セション確立要求時刻を、操作員種別毎のセション確立許可時間帯と照合する
- セション確立時刻が操作員種別毎のセション確立許可時間帯外の場合、セション確立を拒否する

上記機能の実装により、FTA_TSE.1 を実現する。
また、セション確立許可時間帯の設定、更新は、操作員管理・アクセス制御機能の実装により、サーバ管理者に限定される。

(9) FMT_SMF.1 管理機能の特定

TOE は、識別認証機能において表 7-2 に示すセキュリティ管理機能を提供する。

表 7-2 提供セキュリティ管理機能

特定されたセキュリティ管理項目	セキュリティ管理機能
不成功の認証試行回数の管理	不成功の認証試行に対する閾値の管理
バナー表示メッセージの管理	バナー表示メッセージの管理
操作員種別毎のセション確立許可時間帯の管理	操作員種別毎のセション確立許可時間帯の管理
操作員管理 自身によるパスワードの改変	クライアント操作員のパスワードの登録 クライアント操作員のパスワードの改変 クライアント操作員 ID の作成、問い合わせ、削除 サーバ管理者のパスワードの登録 サーバ管理者のパスワードの改変

これは FMT_SMF.1 で要求される管理機能の一部であり、従って、この機能の実装および監査機能、操作員管理・アクセス制御機能の実装により、FMT_SMF.1 を実現する。

7.1.3. 暗号機能（SF.Crypto）

暗号機能は、サーバ端末とクライアント端末間通信の暗号化、バックアップデータの暗号化・復号化、及び個人データの提供データ・預託データの暗号化を行う機能を提供する。また暗号鍵の生成・インポート・破棄を行う機能を提供する。以下では操作員管理・アクセス制御機能について、SFR の実現方法という観点から説明する。

7.1.3.1. 対応する SFR の実現方法

(1) FCS_CKM.1 暗号鍵生成

TOE は、暗号操作を行う際、表 7-3 に示す暗号鍵を用いる。

表 7-3 暗号鍵と生成アルゴリズム

鍵の種類	標準	暗号鍵生成アルゴリズム	暗号鍵長
サーバ共通鍵	A 社暗号鍵運用標準	A 社共通鍵生成アルゴリズム	168bit
処理連携サーバ共通鍵	A 社暗号鍵運用標準	A 社共通鍵生成アルゴリズム	168bit
サーバ秘密鍵	PKCS#1	RSA	2048bit
サーバ公開鍵	PKCS#1	RSA	2048bit
セション鍵	A 社暗号鍵運用標準	A 社共通鍵生成アルゴリズム	168bit
標準		暗号アルゴリズム	
FIPS PUB 180-1		SHA-256	

これらの鍵は下記のタイミングで生成される。

- サーバ端末セットアップ時、またはサーバ端末内 DB のバックアップデータを取得するまでの任意のタイミングで、サーバ共通鍵を生成する
- 処理連携サーバ端末セットアップ時、または処理連携サーバ端末内 DB のバックアップを取得するまでの任意のタイミングで、処理連携サーバ共通鍵を生成する
- サーバ端末セットアップ時にサーバ端末にて、サーバ公開鍵・秘密鍵ペアを生成する
- サーバ端末、クライアント端末間の通信発生時にクライアント端末にてセション鍵を生成する

この機能の実装により、FCS_CKM.1 を実現する。

(2) FCS_CKM.4 暗号鍵破棄

TOE は、格納している暗号鍵を破棄する場合には、暗号鍵を格納していた領域をダミーデータ（乱数やゼロデータなどの意味のないデータ）で上書きした後、領域を解放する。

この機能の実装により、FCS_CKM.4 を実現する。

(3) FCS_COP.1 暗号操作

TOE は、表 7-3 に示す暗号鍵を使用した、下記暗号操作機能を提供する。

- サーバ端末内 DB バックアップデータ暗号操作
  - サーバ端末内 DB のバックアップデータのハッシュ値を生成し、サーバ共通鍵を用いてサーバ端末内 DB のバックアップデータを暗号化する
  - 暗号アルゴリズムは FIPS PUB 46-3 に適合した Triple DES を使用する
  - 復号時には、ハッシュ値を比較することで改ざんの有無を検出する
- 処理連携サーバ端末内 DB バックアップ暗号操作
  - 処理連携サーバ端末内 DB のバックアップデータのハッシュ値を生成し、処理連携サーバ共通鍵を用いて、処理連携サーバ端末内 DB のバックアップデータを暗号化する

- 暗号アルゴリズムは FIPS PUB 46-3 に適合した Triple DES を使用する
- 復号時には、ハッシュ値を比較することで改ざんの有無を検出する

・ クライアント端末、サーバ端末間通信データ暗号操作
- サーバ端末とクライアント端末間の通信発生時には、クライアント端末が生成したセション鍵を、予めクライアント端末にインストールされたサーバ公開鍵を使用して暗号化しサーバ端末に送付する
- 通信データのハッシュ値を生成し、セション鍵を使用して通信データを暗号化する
- 暗号アルゴリズムは FIPS PUB 46-3 に適合した Triple DES を使用する
- 通信データの復号時には、同時に受信したハッシュ値を比較することで改ざんの有無を検出する

・ 提供・預託データ暗号操作
- 個人データの提供・預託データを生成する都度サーバ端末において、提供・預託データのハッシュ値を生成する
- ハッシュ値と提供・預託データの双方を提供・預託先から受領した提供・預託先共通鍵を用いて暗号化する
- 暗号アルゴリズムは FIPS PUB 46-3 に適合した Triple DES を使用する

上記機能の実装により、FCS_COP.1 を実現する。

(4) FCS_CKM.4 暗号鍵破棄

TOE は、格納している暗号鍵を破棄する場合には、暗号鍵を格納していた領域をダミーデータ（乱数やゼロデータなどの意味のないデータ）で上書きした後、領域を解放する。

この機能の実装により、FCS_CKM.4 を実現する。

7.1.4. バックアップ／リカバリ機能（SF.Import_Export）

バックアップ／リカバリ機能は、TOE の正常動作のためにサーバ端末上の必要な利用者データ及び TSF データをバックアップデータとしてエクスポート／インポートする。また、処理連携サーバ端末上の未登録個人データをバックアップデータとしてエクスポート／インポートする。各端末のバックアップデータは外部出力、外部からのインポートの際に、暗号機能（SF.Crypto）により暗号、復号処理が行われる。以下ではバックアップ／リカバリ機能について、SFR の実現方法という観点から説明する。

7.1.4.1. 対応する SFR の実現方法

(1) FDP_ETC.2 セキュリティ属性付き利用者データのエクスポート

TOE は、バックアップ機能において下記機能を提供する。

- TOE 正常動作のためにサーバ端末上の必要な利用者データ及び TSF データをバックアップデータとしてエクスポートする
- 処理連携サーバ端末上の未登録個人データをバックアップデータとしてエクスポートする
- バックアップデータに含まれる TSF データは対応する利用者データに対して、曖昧さなく正確に対応付けられ、共にリムーバブル媒体に格納され、物理的に保護された室内に保管される

この機能の実装、及び操作員管理・アクセス制御機能が提供する、エクスポート処理に関する権限管理機能の実装により、FDP_ETC.2 を実現する。

(2) FDP_ITC.2 セキュリティ属性付き利用者データのインポート

TOE は、リカバリ機能において下記機能を提供する。

- バックアップデータをインポートする際には、エクスポート処理で作成されたバックアップデータが格納されたリムーバブル媒体を用い、セキュリティ属性付きでインポートされる
- インポートされたバックアップデータは、関係付けられているセキュリティ属性と共に、DB に格納される
- インポートに際し、暗号機能によりバックアップデータの復号処理が行われると共に、ハッシュ値を確認する事により、改ざんの有無、およびセキュリティ属性の正確な対応を確認する

この機能の実装、及び操作員管理・アクセス制御機能が提供する、インポート処理に関する権限管理機能の実装により、FDP_ITC.2 を実現する。

7.1.5. 操作員管理・アクセス制御機能（SF.ACC）

操作員管理・アクセス制御機能は、TOE にアクセスする操作員の登録・削除・情報管理を行う機能と、各操作員が持つ属性である操作員種別に対して付与される権限に基づき、TOE に対する全ての操作を制御する機能を提供する。以下では操作員管理・アクセス制御機能について、SFR の実現方法という観点から説明する。

7.1.5.1. 対応する SFR の実現方法

(1) FMT_SMR.2 セキュリティ役割における制限

TOE は、操作員登録に関して以下の機能を提供する。

・ 操作員は、登録時に以下のセキュリティ属性を持つ

（セキュリティ属性）

- 操作員 ID
- パスワード
- 操作員種別

・ 以下の操作員種別を定義する

（操作員種別）

- オペレータ
- 個人情報利用者
- 個人情報管理者
- サーバ管理者
- 監査者

・ すべての操作員は、登録時に上記のいずれかの操作員種別に分類される

・ 一つの操作員を複数の操作員種別に重複して分類できない

この機能の実装により、FMT_SMR.2 を実現する。

(2) FIA_ATD.1 利用者属性定義

TOE は、上記の操作員種別を定義し、識別認証機能（SF.I&A）によって識別及び認証された操作員の操作員 ID から、当該操作員の操作員種別を認識し、ログアウトするまで操作員種別の情報を維持する。

この機能の実装により、FIA_ATD.1 を実現する。

(3) FIA_USB.1 利用者・サブジェクト結合

TOE は、識別認証機能（SF.I&A）で識別及び認証が終了した後、操作員 ID を、操作員を代行して動作するサブジェクトである独立した操作員プロセスに関連付ける。各操作員に付与される操作員種別および操作員プロセスの関係を表 7-4 に示す。

表 7-4 操作員に付与されるセキュリティ属性の対応

操作員	操作員を代行して動作するサブジェクト	付与されるセキュリティ属性（操作員種別）
サーバ管理者	サーバ管理者プロセス	サーバ管理者
監査者	監査者プロセス	監査者
個人情報管理者	個人情報管理者プロセス	個人情報管理者
オペレータ	オペレータプロセス	オペレータ
個人情報利用者	個人情報利用者プロセス	個人情報利用者

この機能の実装により、FIA_USB.1 を実現する。

(4) FMT_MSA.3 静的属性初期化

TOE は、表 7-5 に示すオブジェクトが新規に生成される際に、セキュリティ属性である個人データ種別を付与する。また、これらの個人データ種別は、すべての操作員において改変することが禁止される。

各オブジェクトに付与されるセキュリティ属性である個人データ種別を表 7-5 に示す。

表 7-5 オブジェクトに関連付けられるセキュリティ属性

オブジェクト	オブジェクトに関連付けられるセキュリティ属性（個人データ種別）
個人データレコード	個人データ
未登録個人データレコード	未登録個人データ
個人データの提供データレコード	個人データの提供データ
個人データの預託データレコード	個人データの預託データ
個人データの加工データレコード	個人データの加工データ
個人データに関する承認依頼（登録用）レコード	個人データに関する承認依頼（登録用）
個人データに関する承認依頼（更新用）レコード	個人データに関する承認依頼（更新用）
個人データに関する承認依頼（削除用）レコード	個人データに関する承認依頼（削除用）
個人データに関する承認依頼（提供用）レコード	個人データに関する承認依頼（提供用）
個人データに関する承認依頼（預託用）レコード	個人データに関する承認依頼（預託用）
バックアップデータレコード	バックアップデータ

この機能の実装により、FMT_MSA.3 を実現する。

(5) FDP_ACC.1a サブセットアクセス制御、FDP_ACF.1a セキュリティ属性によるアクセス制御（個人情報処理メイン機能）

TOE は、表 7-6 に示す個人情報処理メイン機能アクセス制御方針に従った、個人データに関するアクセス制御機能を提供する。

表 7-6　個人情報処理メイン機能アクセス制御方針

制御された サブジェクト	サブジェクトのセキュリティ属性（操作員種別）	制御された オブジェクト	オブジェクトのセキュリティ属性（個人データ種別）	制御された操作
オペレータ プロセス	オペレータ	個人データに関する承認依頼（登録用）レコード	個人データに関する承認依頼（登録用）	生成
		個人データに関する承認依頼（更新用）レコード	個人データに関する承認依頼（更新用）	
		個人データに関する承認依頼（削除用）レコード	個人データに関する承認依頼（削除用）	
		未登録個人データレコード	未登録個人データ	参照 削除
個人情報利用者 プロセス	個人情報利用者	個人データレコード	個人データ	参照
		個人データの加工データレコード	個人データの加工データ	
		個人データに関する承認依頼（提供用）レコード	個人データに関する承認依頼（提供用）	生成
		個人データに関する承認依頼（預託用）レコード	個人データに関する承認依頼（預託用）	
		個人データの加工データレコード	個人データの加工データ	生成 更新 削除
個人情報管理者 プロセス	個人情報管理者	個人データレコード	個人データ	参照
		個人データの加工データレコード	個人データの加工データ	
		個人データに関する承認依頼（登録用）レコード	個人データに関する承認依頼（登録用）	参照 削除
		個人データに関する承認依頼（更新用）レコード	個人データに関する承認依頼（更新用）	
		個人データに関する承認依頼（削除用）レコード	個人データに関する承認依頼（削除用）	
		個人データに関する承認依頼（提供用）レコード	個人データに関する承認依頼（提供用）	
		個人データに関する承認依頼（預託用）レコード	個人データに関する承認依頼（預託用）	
		個人データレコード	個人データ	生成 更新 削除
		個人データの提供データレコード	個人データの提供データ	生成 削除
		個人データの預託データレコード	個人データの預託データ	

この機能の実装により、FDP_ACC.1a、および FDP_ACF.1a を実現する。

(6) FDP_ACC.1b サブセットアクセス制御、FDP_ACF.1b セキュリティ属性によるアクセス制御（外部入出力）

TOE は、表 7-7 に示す外部入出力に関する管理規則に従った、提供・預託データエクスポート、バックアップデータエクスポート、インポートに関するアクセス制御機能を提供する。

表 7-7 外部入出力アクセス制御方針

制御されたサブジェクト	サブジェクトのセキュリティ属性（操作員種別）	制御されたオブジェクト	オブジェクトのセキュリティ属性（個人データ種別）	制御された操作
サーバ管理者プロセス	サーバ管理者	個人データの提供・預託データレコード	個人データの提供・預託データ	エクスポート
		バックアップデータレコード	バックアップデータ	エクスポート インポート

。

この機能の実装により、FDP_ACC.1b、および ADP_ACF.1b を実現する

(7) FAU_SAR.1 監査レビュー

TOE は、監査証跡の参照権限管理に関して下記機能を提供する。
- 操作員種別を定義し、すべての操作員をいずれか一つの操作員種別に分類する
- サーバ管理者及び監査者に対して、監査証跡を参照するための権限を付与することで明示的に監査証跡の読み出しアクセスを許可する

この機能の実装および監査機能により、FAU_SAR.1 を実現する。

(8) FAU_SAR.2 限定監査レビュー

TOE は、監査証跡の参照権限管理に関して下記機能を提供する。
- 操作員種別を定義し、すべての操作員をいずれか一つの操作員種別に分類する
- サーバ管理者及び監査者に対してのみ、監査証跡を参照するための権限を付与することで明示的に監査証跡の読み出しアクセスを許可する
- その他の操作員種別に対しては、読み出しアクセスを禁止する。

この機能の実装により、FAU_SAR.2 を実現する。

(9) FAU_STG.1 保護された監査証跡保管

TOE は、監査証跡のアクセス権限管理に関して下記機能を提供する。
- 操作員種別を定義し、すべての操作員をいずれか一つの操作員種別に分類する
- 監査者とサーバ管理者に対してのみ監査証跡へのアクセス権限を付与する
- サーバ管理者に対しては、参照権限のみ付与する
- 監査証跡の削除権限は、監査者のみに付与し、エクスポート実施後にのみ削除処理が可能とする

この機能の実装により、FAU_STG.1 を実現する。

(10) FDP_ETC.2 セキュリティ属性付き利用者データのエクスポート(バックアップデータ)

TOE は、表 7-7 に示す外部入出力アクセス制御方針に従い、バックアップデータのエクスポート操作をサーバ管理者に限定する。
この機能の実装、およびバックアップ／リカバリ機能により、FDP_ETC.2 を実現する。

(11) FDP_ITC.2 セキュリティ属性付き利用者データのインポート(バックアップデータ)

TOE は、表 7-7 に示す外部入出力アクセス制御方針に従い、バックアップデータのインポート操作をサーバ管理者に限定する。
この機能の実装、およびバックアップ／リカバリ機能により、FDP_ITC.2 を実現する。

(12) FMT_MTD.1 TSF データの管理

TOE は、表 7-8 に示す通り、左列に示す各 TSF データに対して、右列に示された対応する各操作員が、中列に示された各操作を実行する事のみを許可する。
この機能の実装により、FMT_MTD.1 を実現する。

表 7-8 TSF データに対する操作と役割

TSF データ	操作	許可された識別された役割
セキュリティ侵害の可能性を判断するために用いる監査証跡の重要度	改変	監査者
サーバ管理者の操作員 ID	問い合わせ、削除、作成	サーバ管理者
サーバ管理者のパスワード	作成	サーバ管理者
監査者、個人情報管理者の操作員 ID	問い合わせ、削除、作成	サーバ管理者
監査者、個人情報管理者のパスワード	削除、作成	サーバ管理者
オペレータ、個人情報利用者の操作員 ID	問い合わせ、削除、作成	個人情報管理者
オペレータ、個人情報利用者のパスワード	削除、作成	個人情報管理者
操作員自身のパスワード	改変	オペレータ 個人情報利用者 個人情報管理者 サーバ管理者 監査者
サーバ共通鍵	問い合わせ、改変、削除、作成	サーバ管理者
処理連携サーバ共通鍵	問い合わせ、改変、削除、作成	サーバ管理者
サーバ秘密鍵	問い合わせ、改変、削除、作成	サーバ管理者
サーバ公開鍵	問い合わせ、改変、削除、作成	サーバ管理者
	問い合わせ	オペレータ 個人情報利用者 個人情報管理者 監査者
提供・預託先共通鍵	問い合わせ、削除、インポート	サーバ管理者
	問い合わせ	個人情報管理者
セション鍵	問い合わせ、削除、作成	オペレータ 個人情報利用者 個人情報管理者 監査者
操作員の最後に成功した認証以降の不成功認証試行回数の定義	問い合わせ、改変、作成	サーバ管理者
バナー表示メッセージ	問い合わせ、改変、作成	サーバ管理者
操作員種別毎のセション確立許可時間帯	問い合わせ、改変	サーバ管理者
監査証跡	問い合わせ、削除、エクスポート、インポート	監査者
	問い合わせ	サーバ管理者

(13) FMT_SMF.1 管理機能の特定

TOE は、操作員の登録に関連して、以下の機能を提供する。

- サーバ管理者は、個人情報処理システムサーバ用アプリケーションパッケージのセットアップ時に最初に登録される
- サーバ管理者は、操作員登録時にサーバ管理者、監査者、及び個人情報管理者のいずれかを選択する
- 個人情報管理者は、操作員登録時にオペレータ、及び個人情報利用者のいずれかを選択する

これは FMT_SMF.1 で要求される管理機能の一部であり、従ってこの機能の実装、および監査機能、識別認証機能の実装により、FMT_SMF.1 を実現する。

8. 用語・参考資料

8.1. 個人情報保護法における用語とその定義内容

用語	定義内容
[個人情報保護法]	
個人情報	この法律において「個人情報」とは、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。
個人情報データベース等	個人情報を含む情報の集合物であって、次に掲げるものをいう。 一特定の個人情報を電子計算機を用いて検索することができるように体系的に構成したもの 二前号に掲げるもののほか、特定の個人情報を容易に検索することができるように体系的に構成したものとして政令で定めるもの
個人情報取扱事業者	個人情報データベース等を事業の用に供している者をいう。ただし、次に掲げる者を除く。 一国の機関 二地方公共団体 三独立行政法人等（独立行政法人等の保有する個人情報の保護に関する法律（平成十五年法律第五十九号）第二条第一項に規定する独立行政法人等をいう。以下同じ。） 四地方独立行政法人（地方独立行政法人法（平成十五年法律第百十八号）第二条第一項に規定する地方独立行政法人をいう。以下同じ。） 五その取り扱う個人情報の量及び利用方法からみて個人の権利利益を害するおそれが少ないものとして政令で定める者。 （政令第２条） 法第２条第３項第５号の政令で定める者は、その事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定の個人の数（当該個人情報データベース等の全部又は一部が他人の作成に係る個人情報データベース等で個人情報として氏名又は住所若しくは居所（地図上又は電子計算機の映像面上において住所又は居所の所在の場所を示す表示を含む。）若しくは電話番号のみが含まれる場合であって、これを編集し、又は加工することなくその事業の用に供するときは、当該個人情報データベース等の全部又は一部を構成する個人情報によって識別される特定の個人の数を除く。）の合計が過去６月以内のいずれの日においても５０００を超えない者とする。
個人データ	個人情報データベース等を構成する個人情報をいう。
保有個人データ	個人情報取扱事業者が、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことのできる権限を有する個人データであって、その存否が明らかになることにより公益その他の利益が害されるものとして政令で定めるもの又は一年以内の政令で定める期間以内に消去することとなるもの以外のものをいう。

8.2. 本STにおける用語

用語	定義内容
個人情報処理 メイン機能	個人データに関する操作（登録、更新、削除、閲覧・検索、提供、預託、加工）及び操作の承認を行う機能。
未登録個人データ 外部入力機能	顧客から送信されたデータを Web サーバで未登録個人データとして生成し、この未登録個人データの処理連携サーバ端末へのインポートを行う機能。
提供・預託データ 外部出力機能	暗号化された提供・預託データのエクスポートを行う機能。
監査証跡退避機能	監査証跡のエクスポート、及びインポートを行う機能。
基本機能	個人情報処理メイン機能、未登録個人データ外部入力機能、提供・預託データ外部出力機能、及び監査証跡退避機能を総称していう。
個人情報処理 メイン機能利用者	オペレータ、個人情報利用者、及び個人情報管理者を総称していう。
オペレータ	個人データの登録、更新、及び削除を行う権限を与えられた操作者。
個人情報利用者	個人データの閲覧・検索、提供、預託、及び加工を行う権限を与えられた操作者。
個人情報管理者	個人情報の管理を行うため、個人データの閲覧・検索、オペレータ・個人情報利用者の操作の承認、及び操作員管理（オペレータ・個人情報利用者の管理）を行う権限を与えられた操作者。
サーバ管理者	個人情報処理システムの管理者として、基本機能の起動／停止、鍵管理、システム環境設定（第 2.2 節(2)参照）、バックアップ／リカバリ、個人データの提供・預託データの外部出力、監査証跡参照、操作員管理（サーバ管理者、監査者、個人情報管理者の管理）を行う権限を有する操作者。
監査者	監査証跡の検査、管理、及び退避を行う権限を与えられた操作者。
操作員	オペレータ、個人情報利用者、個人情報管理者、サーバ管理者、及び監査者を総称していう。
クライアント 操作員	オペレータ、個人情報利用者、個人情報管理者、及び監査者を総称していう。
組織の責任者	TOE に対し、直接操作は行わない。サーバ管理者、監査者、及び個人情報管理者を任命する者であり、A 社通信教育事業部長を指す。
サーバ端末	個人データが格納される端末。
処理連携サーバ端末	個人データが格納され、DMZ 上の Web サーバと、サーバ端末との中継を行うための端末。メールサーバも兼ねる。
オペレータ端末	個人データの登録、更新、削除を行うために、オペレータが使用する端末。
個人情報利用者端末	個人データの閲覧・検索、提供、預託、及び加工を行うために、個人情報利用者が使用する端末。
個人情報管理者端末	オペレータと個人情報利用者の操作を承認するために、個人情報管理者が使用する端末。
監査者端末	監査証跡の参照、及び管理を行うために、監査者が使用する端末。
クライアント端末	オペレータ端末、個人情報利用者端末、個人情報管理者端末、及び監査者端末を総称していう。

8.3. 略語・用語

<CC 関連略語>
CC（Common Criteria）: コモンクライテリア
EAL（Evaluation Assurance Level）: 評価保証レベル
IT（Information Technology）: 情報技術
PP（Protection Profile）: プロテクションプロファイル
SF（Security Function）: セキュリティ機能
ST（Security Target）: セキュリティターゲット
TOE（Target Of Evaluation）: 評価対象
TSF（TOE Security Functions）: TOE セキュリティ機能
SFR（Security Functional Requirements）: セキュリティ機能要件

<TOE 関連略語>
DAT（Digital Audio Tape）: 音声をディジタル化して録音、再生するテープカセット
DB（Database）: データベース
DBMS（Database Management System）: データベース管理システム
DDS（Digital Data Storage）: DAT の技術をベースに開発された磁気テープを利用した大容量記憶装置の一つ
DES（Data Encryption Standard）: IBM 社によって開発された秘密鍵暗号化アルゴリズム。Triple DES は、DES を三重に適用するようにした秘密鍵暗号化アルゴリズム。
DMZ（DeMilitarized Zone）: 外部ネットワーク（例：インターネット）に対してサービスを提供する公開サーバを設置する LAN のセグメント。ファイアウォールにより、外部ネットワークからも内部ネットワーク（例：社内 LAN）からも隔離される。
FIPS（Federal Information Processing Standard）: 米国政府調達基準。暗号モジュールの安全性に関する標準を含む。
HDD（Hard Disk Drive）: 磁気記憶メディアのハードディスクに対し、読み書きをするための装置。
ID（IDentification）: 識別番号
OS（Operating System）: 基本ソフト
PKCS（Public Key Cryptography Standards）: RSADSI 社が定める、公開鍵暗号技術をベースとした各種の規格群。
RSA（Rivest Shamir Adleman）: Ronald Rivest 氏、Adi Shamir 氏、Leonard Adleman 氏の 3 人が 1978 年に開発した公開鍵暗号方式
SSL（Secure Socket Layer）: Netscape Communications 社が開発した、インターネット上で情報を暗号化して送受信するプロトコル。
Web : WWW（World Wide Web）と同義。主に HTML（Hyper Text Markup Language）と呼ばれるマークアップ言語で記述された Web ページを Web サーバから読み出し、Web ブラウザで閲覧する技術。

8.4. 参考資料

・Common Criteria for Information Technology Security Evaluation
Part 1:Introduction and general model September 2006 Version3.1 Revision1
CCMB-2006-09-001

・Common Criteria for Information Technology Security Evaluation
Part 2:Security functional components September 2006 Version3.1 Revision1
CCMB-2006-09-002

・Common Criteria for Information Technology Security Evaluation
Part 3:Security assurance components September 2006 Version3.1 Revision1
CCMB-2006-09-003

・Common Methodology for Information Technology Security Evaluation
Evaluation Methodology September 2006 Version3.1 Revision1
CCMB-2006-09-04

・情報技術セキュリティ評価のためのコモンクライテリア
パート 1：概説と一般モデル 2006 年 9 月 バージョン 3.1 改訂第 1 版
CCMB-2006-09-001
平成 19 年 3 月翻訳第 1.2 版
独立行政法人情報処理推進機構セキュリティセンター情報セキュリティ認証室

・情報技術セキュリティ評価のためのコモンクライテリア
パート 2：セキュリティ機能コンポーネント 2006 年 9 月 バージョン 3.1 改訂第 1 版
CCMB-2006-09-002
平成 19 年 3 月翻訳第 1.2 版
独立行政法人情報処理推進機構セキュリティセンター情報セキュリティ認証室

・情報技術セキュリティ評価のためのコモンクライテリア
パート 3：セキュリティ保証コンポーネント 2006 年 9 月 バージョン 3.1 改訂第 1 版
CCMB-2006-09-003
平成 19 年 3 月翻訳第 1.2 版
独立行政法人情報処理推進機構セキュリティセンター情報セキュリティ認証室

・情報技術セキュリティ評価のための共通方法
評価方法 2006 年 9 月 バージョン 3.1 改訂第 1 版 CCMB-2006-09-004
平成 19 年 3 月翻訳第 1.2 版
独立行政法人情報処理推進機構セキュリティセンター情報セキュリティ認証室

・JIS Q 15001:2006 個人情報保護マネジメントシステムー要求事項

・[個人情報保護法] 個人情報の保護に関する法律（平成十五年法律第五十七号）

・[ガイドライン] 個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン 平成 19 年 3 月 経済産業省

付録Ｃ　研究業績一覧

（2014 年 3 月現在）

1. コアアイデアを含む研究業績

学術論文

＜ジャーナル（査読採録）＞

・　アクタ関係表に基づくセキュリティ要求分析手法（SARM）を用いたスパイラルレビューの提案，情報処理学会論文誌（ジャーナル）Vol.52 No.9，2011

＜ジャーナル（条件付採録）＞

・　CC-Case～コモンクライテリア準拠のアシュアランスケースによるセキュリティ要求分析・保証の統合手法，情報処理学会論文誌（ジャーナル）セキュリティ特集号 2014

・　International Journal of Cyber-Security and Digital Forensics

＜国際会議(査読採録)＞

・　A Spiral Review Method for Security Requirements，ProMAC2010 P1227-1238

・　Specification of Whole Steps for the Security Requirements Analysis Method (SARM) - From Requirement Analysis to Countermeasure Decision –，ProMAC2011

・　Proposal on Countermeasure Decision Method Using Assurance Case And Common Criteria，ProMAC2012

・　A Proposal on Security Case based on Common Criteria，AsiaARES2013

・　Efficient Use of Assurance Case against System Risk in the Project Management，ProMAC2013

・　CC-Case for the System Development over Life-cycle Process, ComSec2014

2.これら以外の発表

- アクタ関係表に基づくセキュリティ要求分析手法（ＳＡＲＭ）の提案，情報処理学会 CSS2009 富山 P721-726

- アクタ関係表に基づくセキュリティ要求分析手法（ＳＡＲＭ）の改良提案，情報処理学会創立 50 周年記念（第 72 回）全国大会　講演論文集（３）3-639, 2010

- アクタ関係表に基づくセキュリティ要求分析手法(SARM)の提案と活用, 2011 年ＰＭ学会春季研究発表大会

- セキュリティ要求分析手法（SARM）の適用法について，2012 年ＰＭ学会春季研究発表大会

- セキュリティ保証ケースを用いた対策立案方法の提案，SCIS2013

- プロジェクトマネジメントの要求リスクを考慮した保証ケースの提案，2013 年ＰＭ学会春季研究発表大会

- CC-Case～コモンクライテリア準拠のアシュアランスケースによるセキュリティ要求分析・保証の統合手法 Assurance Case And Common Criteria，CSS2013

- CC に対応したセキュリティ要求分析手法 SARM の考察，SCIS2014