NIST Special Publication 800-35

National Institute of
Standards and Technology
Technology Administration
U.S. Department of Commerce

IT セキュリティサービスガイド

米国立標準技術研究所による勧告

Tim Grance
Joan Hash
Marc Stevens
Kristofor O'Neal
Nadya Bartol

この文書は下記団体によって翻訳監修されています
IPA 独立行政法人 情報処理推進機構 INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN
NRI SECURE TECHNOLOGIES

コンピュータセキュリティ

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

2003 年 10 月

米国商務省 長官

Donald L. Evans

技術管理局 技術担当商務次官

Phillip J. Bond

米国立標準技術研究所 所長

Arden L. Bement, Jr.

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

謝辞

本書執筆陣である米国立標準技術研究所（NIST）の Tim Grance および Joan Hash、Booz Allen Hamilton 社（BAH）の Marc Stevens、Kristofor O'Neal、Nadya Bartol は、本書の多くの草案を校閲し、技術的内容に貢献してくれた同僚に対し感謝の意を表す。また、公共ならびに民間部門の読者からは、本書の質と実用性を高める上で貴重な洞察を与える多くのコメントをいただき非常に感謝している。特に、環境保護局、財務省、テネシー川流域開発公社、および Electronic Data Systems 社をはじめとする、主要組織からいただいた広範なフィードバックは、本書の作成に大いに寄与してくれた。また、NIST の Ron Ross 氏、Gary Stoneburner 氏、Curtis Barker 氏、Ron Tencati 氏、Marianne Swanson 女史、および Bill Burr 氏、BAH の Alexis Feringa 氏、Don Ottinger 氏、Skip Hirsh 氏、および Robert Young 氏、ならびに Shirley Radack 女史には、多大なレビューとコメントをいただき、本書の執筆全体にわたって鋭く洞察に満ちた助言をしてくれた。

市販製品の記述または民間組織に対する言及は、参考までに書かれているにすぎない。したがって、NIST による推薦または公認を意味するものではなく、言及された製品が最も有効だと意味しているわけでもない。

エグゼクティブサマリ

組織では、しばしば、その情報技術（IT）セキュリティプログラムやエンタープライズアーキテクチャ全体を保持し、改善していくために、さまざまな IT セキュリティサービスを評価および選択する必要が生じる。セキュリティポリシーの作成から侵入検知のサポートに至る IT セキュリティサービスは、組織内部の IT グループから提供されることもあれば、また多くのベンダーからも提供されることもある。組織にとって、サービスおよびサービスプロバイダの選択肢が増えれば、競争が促進し、市場に新機軸がもたらされ、組織はその利益を享受することができるようになる。しかし、組織がサービスプロバイダの能力を判断し、サービスの信頼性を測定し、セキュリティサービス契約に関わる多くの複雑さに対処していくことは、困難で厳しいものである。組織の IT セキュリティサービスの選択、インプリメント、および管理を担う担当者は、与えられた選択肢を注意深く評価してから、独自の IT セキュリティプログラムの要件を満たすと信じることができるリソースを選択する必要がある。

IT セキュリティサービスを選択、インプリメント、および管理するときに考慮すべき要素には、(1) サービスアレンジメントのタイプ、(2) サービスプロバイダの適性、運用上の要件と能力、経験、および実行能力、(3) サービスプロバイダの従業員の信頼性、(4) 組織のシステム、アプリケーション、およびデータに適切な保護を施せるだけのサービスプロバイダの能力がある。これらの事項は、考慮されるサービスのサイズ、タイプ、複雑さ、コスト、および重要性と、サービスをインプリメントまたは契約する組織の特定のニーズとに応じて、すべてのサービスに（さまざまな程度で）適用される。

本書『情報技術セキュリティサービスのガイド』特別刊行物 800-35 は、組織に IT セキュリティサービスのライフサイクルのさまざまなフェーズを紹介し、IT セキュリティサービスの選択、インプリメント、および管理を支援する。このライフサイクルは、IT セキュリティの意志決定者が IT セキュリティを開始し終了するまでの活動を計画するためのフレームワークを提供する。IT セキュリティサービスプロセスの系統だった管理は、非常に重要である。関係する多くの問題を考慮せず、組織的なリスクを管理できなければ、深刻な影響が組織に及ぶことがある。IT セキュリティの意志決定者は、関連するコストと基本的なセキュリティ要件だけでなく、組織の使命、運用、戦略的機能、人員、およびサービスプロバイダアレンジメントに対し、決定が及ぼす影響についても考慮する必要がある。

IT セキュリティのライフサイクルの 6 つのフェーズは次のとおりである。

- **フェーズ 1: 開始**
  IT セキュリティサービスのインプリメントによって組織の IT セキュリティプログラムに対し効果が得られるかを調査する必要性を判断する。

- **フェーズ 2: アセスメント**
  メトリクスを使用して現在の環境におけるセキュリティ状態を判断し、必要要件とそれに対する有効なソリューションを特定する。

・**フェーズ 3: ソリューション決定**

意志決定者が、候補となるソリューションを評価し、ビジネスケースを作成し、利用可能な選択肢の中から許容できるサービスアレンジメントソリューションの重要な特徴を決定する。

・**フェーズ 4: インプリメント**

サービスプロバイダを選択し、契約を結んで、サービスアレンジメントを作成し、ソリューションをインプリメントする。

・**フェーズ 5: 運用**

サービスプロバイダおよび定義した要件に対するセキュリティパフォーマンスを継続的に監視し、組織に対するリスクおよび脅威の変化を定期的に評価し、許容できるセキュリティ状態を維持できるようにセキュリティソリューションに対し必要な調整を行うことによって、運用を確実に行う。

・**フェーズ 6: 終了**

サービスを終了または打ち切る際にスムーズな移行を行う。

このガイドは、IT セキュリティサービスを取り巻く多くの問題に対し、組織の取り組みを支援するライフサイクルについて記述している。しかしながら、このガイドは、特定の IT セキュリティサービス、IT セキュリティサービスアレンジメント、IT セキュリティサービス契約、または IT セキュリティサービスプロバイダを指定、および推奨するものではない。各組織は、自身でニーズの分析を行い、そのニーズに最も適切に対処できるように、IT セキュリティサービスの評価、選択、インプリメント、および管理を実施しなければならない。

このガイドは、NIST SP 800-64『情報システム開発のライフサイクルにおけるセキュリティの考慮事項（Security Considerations in the Information System Development Life Cycle）』や NIST SP 800-36『情報技術セキュリティ製品の選択ガイド（Selecting Information Technology Security Products）』など、IT システムの調達に焦点を当てた他の NIST 特別刊行物（SP）と併せて使用する必要がある。NIST 800-55『情報技術システム用のセキュリティメトリクスガイド（Security Metrics Guide for Information Technology Systems）』では、メトリクスの使用とメトリクスプログラムの開発の重要性について説明している。

次に挙げるその他の NIST 特別刊行物には、具体的なサービスおよび技術に関する情報が記されている。

・ SP 800-30:『情報技術システム用のリスク管理ガイド（Risk Management Guide for Information Technology Systems）』
・ SP 800-32:『公開鍵技術および連邦政府の PKI インフラストラクチャ入門（Introduction to Public Key Technology and the Federal PKI Infrastructure）』
・ SP 800-33:『情報技術セキュリティ用の基本技術モデル（Underlying Technical Models for Information Technology Security）』
・ SP 800-34:『情報技術システム用の緊急時対応計画ガイド（Contingency Planning Guide for Information

Technology Systems)』

- SP 800-41:『ファイアウォールおよびファイアウォールポリシー入門 (An Introduction to Firewalls and Firewall Policy)』
- SP 800-42:『ネットワークセキュリティテストのガイドライン (Guideline on Network Security Testing)』
- SP 800-48:『ワイヤレスネットワークセキュリティ: 802.11、ブルートゥース、携帯端末 (Wireless Network Security: 802.11, Bluetooth, and Handheld Devices)』
- SP 800-50:『情報技術セキュリティの意識向上およびトレーニングプログラムの構築 (Building an Information Technology Security Awareness and Training Program)』
- SP 800-53:『連邦情報システム用の推奨セキュリティコントロール (Recommended Security Controls for Federal Information Systems)』

IT セキュリティサービスの利用を検討している組織は、次の点を考慮することを勧める。

- 客観的なビジネスケースを慎重に作成する。IT セキュリティサービスのニーズは、組織のビジネスニーズに基づいている必要がある。提案されたソリューションの分析、コスト見積もり、利益分析、プロジェクトリスク分析、および他の比較対象の代替案の評価を含んだビジネスケースがあれば、組織のビジネスニーズを定め、サポートしていくのに必要なドキュメントを作成することができる。

- 必要となる各セキュリティコントロールついて期待するパフォーマンス値を定め、結果を測定可能な形で表現し、不履行とみなされるあらゆる事態に対する是正措置と対応方法を定義した、行使力のある具体的なサービス契約書を作成する。

- IT セキュリティのライフサイクル全体にわたりメトリクスを使用する。メトリクスは、アセスメントフェーズにおいてサービスが基準に達しているか評価するために客観的なデータを提供し、運用フェーズにおいてサービスプロバイダのパフォーマンスを査定するのにも必要となる客観的なデータを提供する。可能な限り、組織の基本的なニーズを満たしているセキュリティ状態の達成または維持における進捗を示すことができるメトリクスを選択する。

- 組織内で様々な IT セキュリティサービスが利用される間、それらに適用されるサービス契約書やメトリクスを効果的に追跡できるプロセスや実施手順を作成する。

- 既存のサービスプロバイダまたは機能と新しいサービスプロバイダとの間で、適切な移行期間を設ける。

- 提供されるセキュリティサービスを理解および管理し、組織のミッションにとって重要なデータを保護するために必要な技術的専門知識を保持する。

- 戦略/ミッション、予算/資金、技術/アーキテクチャ、組織、人員、およびポリシー/プロセスの 6 つの問題領域に十分な注意を払う。

目次

図目次

表目次

1. はじめに

1.1 作成機関

米国立標準技術研究所（NIST; National Institute of Standards and Technology）は、2002 年の連邦情報セキュリティ管理法（FISMA; Federal Information Security Management Act）、公法 107-347 に基づくその法的責任を推進するために、このドキュメントを作成した。

NIST は、すべての連邦機関の業務および資産に適切な情報セキュリティをもたらすために、最低要件を含んだ標準およびガイドラインを作成する責任があるが、このような標準およびガイドラインは国家のセキュリティシステムには適用されない。このガイドラインは、行政管理予算局（OMB; Office of Management and Budget）Circular A-130、第 8b(3)項、『連邦機関の情報システムの保護（Securing Agency Information Systems）』の必要要件に一致しており、これは A-130 の付録 IV「重要部門の分析」で分析されているとおりである。補足情報は、A-130、付録 III に記載されている。

このガイドラインは、連邦機関が使用する目的で用意されている。非政府組織が自己責任において使用することもでき、出自を明らかにすることが望ましいが、著作権の制約はない。

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

1.2 目的

組織ではしばしば、その IT セキュリティプログラム全体を保持および改善するために、さまざまな IT セキュリティサービスを評価、選択、および導入する必要が生じる。IT セキュリティサービス（セキュリティポリシー作成、侵入検知サポートなど）は、組織内部の IT グループやベンダーによって提供されている。組織の IT セキュリティサービスの選択、インプリメント、および管理を担う担当者は、必要なプロセスと手順を注意深くレビューし、利用可能な多数の選択肢を比較し、IT セキュリティプログラムの必要要件を最も満たしていると確信できるリソースを選択する必要がある。

IT セキュリティサービスを選択、インプリメント、および管理するときに考慮すべき要素には、
⑴ サービスアレンジメントのタイプ
⑵ サービスプロバイダの適性、必要要件、経験、および実行能力
⑶ サービスプロバイダの従業員の信頼性
⑷ 組織のシステム、アプリケーション、およびデータに対する保護

がある。これらの考慮事項は、対象となるサービスのサイズ、タイプ、複雑さ、コスト、および重要性に応じて（さまざまな程度で）適用される。

このガイドの目的は、組織にITセキュリティサービスのライフサイクルのさまざまなフェーズを紹介して、ITセキュリティサービスの選択、インプリメント、および管理を支援することである。IT セキュリティサービスのライフサイクルは、IT セキュリティの意志決定者が IT セキュリティの活動を開始から終了まで計画するためのフレームワークを提供する。ITセキュリティサービスプロセスの系統だった管理は、非常に重要である。関与する複雑な多くの問題を考慮せず、対処できない場合、深刻な影響が組織に及ぶことがある。IT セキュリティの意志決定者は、コストとセキュリティ要件だけでなく、組織のミッションおよび戦略的機能、人員、およびサービスプロバイダアレンジメントについても考慮しなければならない。

このガイドは、IT セキュリティサービスのライフサイクルの各フェーズについて述べ、信頼できるセキュリティ方法を評価および選択を始める上での重要なポイントを提供する。このガイドで述べることは、多種多様な IT セキュリティ要件を抱えるさまざまな組織を対象としている。このガイドは、サービスプロバイダのサービスレベルを定める契約作成の重要性などの一般的なトピックについて取り上げてはいるが、組織のニーズに最も適合したサービスまたはサービスレベルを規定するものではない。このガイドで示すプロセスとコンセプトを適用するときには、各組織特有のニーズを常に考慮する必要がある。最後に、NIST はこの刊行物で、意志決定者とその他の関係者に対し、IT セキュリティサービスの調達でのセキュリティおよびポリシーの問題について、情報およびアドバイスを提供する。

1.3 制限

このドキュメントの第 5 項では、IT セキュリティサービスのサンプルを挙げているが、網羅的なリストは記していない。組織では、明確に特定した IT セキュリティサービスに加え、システム管理などの重要なセキュリティコンポーネントを含んだサービスを調達したい場合もあるかもしれない。このガイドでは、このようなサービスを取り上げていないが、このガイドに記された情報は、その他の関連サービスにも拡大して適用することができる。

このガイドは、IT セキュリティサービスの外部アレンジメント（外部委託など）の作成に、賛成と反対のどちらかの立場を支持するものではない。読者は、OMB Circular A-76『商業事業体のパフォーマンス（Performance of Commercial Activities）』を参照して、商業事業体と契約した上で活動を行うべきか、政府の施設および人員を使用して組織内で行うべきかの判断基準を定める必要がある。

1.4 対象とする読者

このガイドは、組織内で手配するか、外部プロバイダから調達するかにかかわらず、IT セキュリティサービスを利用しようとしている組織を対象としている。このガイドの目標は、IT セキュリティの意志決定者およびマネージャが、組織のミッションおよびニーズの達成に最も適切な IT セキュリティサービス、サービスレベル、および

サービスアレンジメントをインプリメントおよび管理していくことを支援することである。

1.5 本ドキュメントの構成

次章以降、このドキュメントは次のように構成されている。

第 2 章では、IT セキュリティのライフサイクルの選択、インプリメント、および管理に関わるさまざまな人員の役割と責任について説明する。

第 3 章では、セキュリティサービスのライフサイクルの概要や選択した IT セキュリティサービスの概要など、IT セキュリティサービスについて概説する。この章では、セキュリティサービスのライフサイクルのフレームワーク、ライフサイクルを通じて対処すべき問題の概要、IT セキュリティの意志決定者が考慮できるさまざまなサービスアレンジメントの概要、および、セキュリティサービスのライフサイクルにおいて IT セキュリティの意志決定者にとって役立つツールの概観について説明する。

第 4 章では、IT セキュリティサービスの調達に関連した問題を詳細に論じる。セキュリティサービスのライフサイクルとの関連では、この章は、セキュリティサービスの開始、現在の環境を見積もり、新しいサービスが必要かどうかを判断するために必要となる材料、サービス契約で扱うべき内容、およびサービス契約を終了または打ち切る方法について説明する。

第 5 章では、これまでの情報の適用例として、いくつかの具体的な IT セキュリティサービスについて詳しく説明する。

以上の章に加え、次の 5 つの付録も添えられている。

付録 A では参考文献の一覧を記している。

付録 B では略称の一覧を記している。

付録 C では、IT セキュリティプロバイダとのサービス契約の概要例を記している。

付録 D では、組織のサービス契約で使用できる文言例を記している。この文言は、組織の具体的なニーズに適切に合わせて修正した後、サービス契約、作業別計算書（SOW; statement of work）などの契約書、または同意覚書および了解事項覚書（MOA/MOU; memorandums of agreement/understanding）を作成する場合に使用できる。

付録 E はよくある質問とその回答の一覧である。

2. 役割と責任

あるサービスの選択、インプリメント、および管理に携わる参加者の選出は、サービスのタイプと範囲、サービスアレンジメント、および組織のタイプとサイズなどに依存する。多数の IT セキュリティ機能に関して外部組織と契約しようとしている大規模な連邦機関は、範囲の限られた従業員用 IT セキュリティトレーニングプログラムを求めている零細企業とは、まったく異なる要件を持つ。したがって、参加者のリストも零細企業に比べて多大になる。以下に挙げる役割は、多くの異なるサービスにも当てはまる。組織が実際に作成する参加者のリストは、下に示すリストよりも小さくなることもあれば、大きくなることもある。たとえば、組織内の内部グループがセキュリティサービスを提供する場合は、契約担当者と契約担当者の技術担当者（COTR; Contracting Officer's Technical Representative）の役割は必要ない。

2.1 最高情報責任者

最高情報責任者（CIO; Chief Information Officer）は、組織の IT 計画、予算設定、投資、パフォーマンス、および取得を担当する。したがって CIO は、効率的で効果的な IT セキュリティサービスの取得において、組織の上級職員を監督する。

2.2 契約担当者

契約担当者は、契約の締結、処理、および終了に関する権限を持ち、関連する判断と認定を行う。

2.3 契約担当者の技術代表者

契約担当者の技術代表者（COTR）は、契約担当者によって任命された適格な社員であり、特定の契約での技術的側面を扱う技術代表者として行動する。

2.4 投資委員会（またはそれに相当するもの）

IT 投資委員会またはそれに相当するものは、1996 年の Clinger-Cohen 法（第 5 項）によって定められた資産計画および投資管理プロセスの運用を担当する。

2.5 IT セキュリティプログラムマネージャ

IT セキュリティプログラムマネージャは、IT セキュリティに関するエンタープライズスタンダードの作成または適用を担当する。この担当者は、組織に対する IT セキュリティリスクの特定、評価、最小化に役立つ、構造化された適切な方法論を導入する際に主導的役割を果たす。IT セキュリティプログラムマネージャは、システムリスク分析を調整および実行し、リスク軽減の代替案を分析し、実際に脅威に直面した場合にミッションの遂行を保証するセキュリティソリューションを取得する上で必要となるビジネスケースを構築する。また、組織のニーズを

満たすためにセキュリティ管理活動が必要になると、この活動が確実に行われるように、上級管理職をサポートする。

2.6 システムセキュリティ担当者

IT システムセキュリティ担当者は、情報システムのライフサイクル全体を通じて、そのセキュリティの確保を担当する。

2.7 プログラムマネージャ（データの所有者）/取得開始者

このプログラムマネージャは、IT セキュリティサービスのライフサイクル中のプログラミング可能な分野に責任を持つ。プログラムマネージャは、IT セキュリティサービスの戦略的計画構想に関わっており、サービスの機能要件を詳細に把握しているので、セキュリティにおいて不可欠な役割を果たす。

2.8 プライバシー担当者

プライバシー担当者は、サービスまたはサービスアレンジメントが、保護、配信（情報の共有と交換）、および情報開示に関して、既存のプライバシーポリシーに適合するように取り計らう。

2.9 その他の参加者

IT システムの取得と管理が複雑になれば、サービス取得に必要になる役割の数も増える可能性がある。取得を確実に成功へ導くには、取得チームの全メンバーの協力が欠かせない。システム認証者および認定者は、調達プロセスが終わりに近づいたときに重要な決定を行うので、迅速に重大な問題に対処できるように、早い時期から彼らを関与させると効果的である。システムユーザーは、ニーズの判断、要件の精緻化、および引き渡されたシステムの点検と承認の際に、プログラムマネージャに協力して取得を支援する。その他の参加者として、情報技術、設定管理、設計およびエンジニアリング、施設の各グループの代表者も含まれる場合がある。

3. IT セキュリティサービス

この章では、IT セキュリティサービス、サービスアレンジメント、サービスにおける諸問題、およびサービス管理ツールの概要について説明する。これらの概要は、第 4 章で述べる IT セキュリティサービスのライフサイクルの導入部分にあたる。IT セキュリティサービスのライフサイクル自体は、サービスを実施するために内部リソースを使用するか、外部サービスプロバイダを使用するかという組織の決定に左右されない。誰がセキュリティサービスを実施しようとも、最終的には、組織自身があらゆるセキュリティ侵害に対する責任を保有し、その影響を受けるのである。

3.1 IT セキュリティサービスの概要

セキュリティサービスは、3 つのカテゴリのいずれかに分類される（表 3-1）。

表 3-1 IT セキュリティのカテゴリ

管理サービス	組織のコンピュータセキュリティプログラムの管理者が日常的に取り扱うテクニックおよびデバイス。コンピュータセキュリティプログラムと組織内のリスクの管理に焦点が当てられる。
運用サービス	（システムではなく）人の手によってインプリメントし実行しなければならないコントロールに焦点を当てたサービス。このサービスは多くの場合、専門技術や専門知識を必要とし、管理活動と技術コントロールに依存する。
技術サービス	コンピュータシステムで実行するセキュリティコントロールに焦点を当てた技術サービス。このサービスの効果は、システムの機能が適切かどうかに依存している。

セキュリティサービスのライフサイクルは、セキュリティサービスが属するカテゴリに関わらず、すべてのセキュリティサービスに適用され、時には IT セキュリティ全体にも適用されることがある。マネージャは、どの IT セキュリティサービスをインプリメント、査定、または打ち切る必要があるかを判断するときに、他の IT セキュリティサービスに対する影響を考慮しなければならない。

第 5 章では、各タイプの IT セキュリティサービスについてさらに詳しく説明している。NIST 特別刊行物（SP）800-12『コンピュータセキュリティ入門: NIST コンピュータセキュリティハンドブック（An Introduction to Computer Security: The NIST Computer Security Handbook）』でも、コンピュータセキュリティ、セキュリティコントロール、およびサービスの包括的な概要と入門が提供されている。

運用例 - 組織は、組織内のファイアウォールのプログラム監視を保持しているが、毎日の監査ログの監視を外部グループに任せている。

セキュリティアレンジメントは、人員の役割によって異なって見えることがある。この例では、外部グループが監査レビューサービスを実行するので、ファイアウォールマネージャは、このアレンジメントを外的なものとみなす。ファイアウォールサービスは内部でインプリメントされるので、組織のトップレベルのビジネスマネージャは、これを内部アレンジメントとみなす。組織の IT セキュリティ担当者は、内部のファイアウォールサービスとその外部の監査レビューコンポーネントの両方を認識するため、これを両方の真ん中あたりにある混成したアレンジメントとみなすことができる。

3.2 IT セキュリティサービスアレンジメントの概要

最も適切なサービス、サービスの組み合わせ、およびサービスレベルを選択することは、誰が必要なサービスを提供するかを決定するのと同様に複雑な判断が必要になる。この決定の複雑さは大部分、組織が選択できるアレンジメントの範囲が広いことから生じているが、第 3.4 項で論じる組織、人員、およびその他の問題も、この決定が簡単ではなくより複雑になっている原因である。

可能性のあるサービスアレンジメントは幅広く存在している。組織は、必要なサービスを提供するために、内部の従業員およびチームを選択することも、外部のサービスプロバイダへサービスを完全に任せることもできる。この外部のサービスプロバイダはどのような組織でもかまわない。なぜなら、この用語は、外部の商用サービスプロバイダだけを意味しているわけではないからである。たとえば、組織は、系列組織、事業体、または商用サービスプロバイダから、外部グループを採用できる。

3.3 IT セキュリティサービス管理ツールの概要

不十分なセキュリティから危害が生じる可能性があるため、IT セキュリティマネージャと意志決定者は、効果的な管理ツールを使用して、成功の可能性を高める必要がある。2 つの重要なツールは、メトリクスとサービス契約である。

メトリクスの概要

メトリクスとは、実際の関連データの収集、データ分析、およびパフォーマンスデータレポートを通じて、意志決定とアカウンタビリティ（責任追跡）を容易にする管理ツールである。メトリクスプログラムの重要性は、NIST SP 800-55『情報技術システム用のセキュリティメトリクスガイド（Security Metrics Guide for Information Technology Systems）』で述べられている。コンピュータセキュリティメトリクスについて語り尽くすことは、このドキュメントの範囲外であるが、IT セキュリティサービスマネージャは、少なくともどのメトリクスをいつ使用する必

要があるかを理解しておかなければならない。

たとえば、トレーニングや意識向上プログラムのような管理サービスのためのメトリクスとしては、就業後 30 日以内に IT セキュリティトレーニングを受ける新人の比率がある。このデータを繰り返し時間をかけて収集すれば、マネージャは、現在のトレーニングサービスプロバイダが、現時点でその責務をどれだけ達成しているかを査定でき、そのサービスプロバイダに対する将来の目標を定め、その後、所期の目標をどれだけ達成しているかを査定することができる。メトリクスプロセスについては、次章で説明する。

サービス契約の概要

サービス契約は、サービスプロバイダと、サービスを必要とする組織との間の契約である。サービスアレンジメントが複雑になり、商用サービスプロバイダを導入するようになると、契約を結ぶ機会も増加する。たとえば、商用事業体にすべてを外部委託したサービスアレンジメントでは、マネージャが、サービスプロバイダに対しその行動に責任を負わせるようにするために、正式な契約が必要となる。すべてを内部で行うサービスアレンジメントでは、正式な契約はあまり必要でなく、おそらく、同意報告プロセスまたは同意覚書が必要になる。アレンジメントとは無関係に、すべての当事者はその役割と責任を認識する必要がある。第 4.4.1 項では、サービス契約の重要性について説明する。

3.4 IT セキュリティサービス課題の概要

セキュリティサービスとサービスアレンジメントのインプリメントは複雑になることがある。各セキュリティサービスには、それぞれのコストとリスクが伴うが、各サービスアレンジメントも同様である。1 つの課題に対する意志決定は、他の領域において組織に大きな影響を与えることがある。意志決定者は、近い将来のコスト/価値、新しい脆弱性、人員削減、従業員の生産性/士気と内部機能スキルの低下の可能性、その他の影響に伴う長期的なリスクとの間でバランスをとる必要がある。考慮すべき要因や課題についてどの程度書き出すかは組織によって異なるが、この要因と課題はどの組織においても、表 3-2 に示すように 6 つのカテゴリに分類することができる。

表 3-2 IT セキュリティサービス問題のカテゴリ

戦略/使命	意志決定者は、ある決定の影響について考えるときに、戦略的観点から見て組織にとって何が最善であるか、組織がその使命を達成するために何が最も役立つかを自問自答しなければならない。セキュリティサービスは、適切に適用されれば、使命の機能を損なうことなく、使命の効果を高める結果になる。
予算/資金	コストを考慮する場合、価値とライフサイクル全体のコストに焦点を当てる必要がある（第 4.2.1.2 項参照）。
技術/アーキテクチャ	IT サービスは、それが管理サービスの場合でも、技術的な側面を持つ。IT セキュリティマネージャは、ライフサイクル全体にわたって、技術的な課題と組織のエンタープライズアーキテクチャに対する影響を考慮しなければならない。
組織	組織に関する課題は、組織のイメージや評判に対するダメージ、中核能力に対する焦点の変更、組織の回復力など、組織の形として見えない要素に関連している。多くの場合、長期間受け入れられてきた内部コントロールや、自然な事業単位分担や法的要件によって時を経て形成されてきた商慣習を、IT セキュリティサービスプロバイダを導入する際に再考する必要がある。
人員	人員に関する課題は、組織の契約者と従業員に関係する。マネージャは、従業員に対する決定の影響を、常に認識している必要がある。インプリメントするサービスアレンジメントによっては、現在の従業員にとって、大きな派生的影響が生じることもある。可能性のあるこれらの影響についての理解が、内部サービスと外部サービスとの適切な役割分担をもたらすための基本要素である。この課題に早期に対処できれば、従業員は組織にとって重要なリソースであり続けることができる。
ポリシー/プロセス	効果的なセキュリティは強固なポリシーから始まるのであり、しかるべき決定が行われ、適切な移行とインプリメントが行われるようにするために、ポリシーおよびプロセスの意味を考慮しなければならない。

以上に挙げた、課題、ツール、およびアレンジメントは、IT セキュリティサービスを提供していく上で重要であるため、このガイドでも繰り返し取り上げる。

3.5 IT セキュリティサービスの一般的な考慮事項

組織のニーズに最も適合したサービスプロバイダを特定するために、意志決定者が答えなければならないいくつかの一般的な質問を以下に挙げている。これらの質問は、第 3.4 項で述べたさまざまな課題のカテゴリに従って分類されている。

これらの質問をガイドとして使用し、それぞれの組織は、どの質問がそれぞれの具体的なニーズに関連しているかを判断する必要がある。質問は網羅されているわけではなく、組織が追加の質問を作成する必要が生じることもある。場合によっては、サービスプロバイダではなく、組織の方が質問の回答者として適切なこともある

だろう。

表 3-3 サービスプロバイダに関する質問 [1]

戦略/使命	1. 「サービスプロバイダ」の使命はどのようなものか。 2. 「サービスプロバイダ」は組織の使命を理解しているか。 3. 「サービスプロバイダ」の使命とサービス内容は、”組織の目的”に合致するように、どのようにしてその整合性が調整され、また、どのように組織の能力を向上させることができるのか。 4. スタッフ数、顧客数、拠点数、および事業収益を具体的に述べ、「サービスプロバイダ」ビジネスについて説明せよ。「サービスプロバイダ」は、実行期間中に、何らかの主要な戦略/使命の変更を計画しているか、または予算/資金の実現性の問題を予想しているか。 5. 「サービス」は本質的に政府機関に適したものか。
予算/資金	1. どれだけのコストで、「サービスプロバイダ」はサービスを提供するのか。 2. サービスレベルが上がるとサービスコストはどれだけかかるか。サービスレベルが下がるとどれだけになるか。 3. どのようにして「サービスプロバイダ」は予算超過を防止するのか。 4. 「サービスプロバイダ」は予算超過に対してどのような是正措置を施すのか。
技術/アーキテクチャ	1. どのようにして「サービスプロバイダ」は、IT セキュリティサービスを実行するのか。 2. 誰が、必要となるハードウェアおよびソフトウェアを提供する、もしくは所有するのか。 3. 「サービスプロバイダ」は、どのレベルでサービスを提供するのか（可用率、メトリクスレポート、保守、ハードウェアおよびソフトウェアの回復など）。 4. どのようにして「サービスプロバイダ」は、このサービスレベルを確保するのか。 5. 「サービスプロバイダ」は、サービス目標を達成できなかった場合に、どのような是正措置を妥当と考えているか（つまりサービスクレジット）。 6. 早期終了および延長に対する「サービスプロバイダ」要件はどのようなものか。 7. 拡大縮小の問題はどのように対処されるか。 8. 「サービスプロバイダ」はこれまで、この種の組織に対して、このタイプのサービスをこのレベルで提供した経験があるか。「サービスプロバイダ」は、過去の実績に対して参考資料を提供できるか。 9. 「サービスプロバイダ」の IT セキュリティ環境はどのようなものか。 10. 「サービスプロバイダ」は緊急事態にどのように対処するか。

[1] この質問の発行主体は、セキュリティサービスをサービスプロバイダから取得し最終的に受け入れる部門である。

組織	1. 「サービスプロバイダ」の作業環境はどのようなもので、組織の環境と互換性があるか。 2. 「サービスプロバイダ」は、どれだけ組織の環境に適合できるか。 3. 「サービスプロバイダ」の評判（市場において、コストおよびサービス目標の達成に関して）はどのようなものか。「サービスプロバイダ」は競合他社と比べてどのように優れているか。
人員	1. 「サービスプロバイダ」のスタッフは、現場に出向するのか、現場に出向しないのか、それともそれらの組み合わせか。 2. 「サービスプロバイダ」のスタッフには、適切な人物保証および能力保証があるか、または確保できるのか。 3. 「サービスプロバイダ」は、どのスタッフをこの業務に割り当てるのか。そのスタッフのスキルはどのようなものか。「サービスプロバイダ」のスタッフは、組織の一員としての要件を満たしているか。 4. どのようにして「サービスプロバイダ」は、スタッフが技術およびサービスの分野で時流に遅れないように取り計らっているのか。
ポリシー/プロセス	1. 「サービスプロバイダ」は、組織のポリシーまたはプロセス、あるいはその両方に対する変更を予測しているか。 2. 「サービスプロバイダ」のセキュリティポリシー（緊急時対応計画など）は、組織のポリシーとどのような点で異なっているか。組織のポリシーがより高い基準に設定されている場合、「サービスプロバイダ」のポリシーは、この高い基準への対応に苦労することがないか。低い場合、「サービスプロバイダ」は、より厳しい組織のポリシーに従うのか。 3. どのようにして「サービスプロバイダ」は、そのデータと、別の組織のデータとの混合に対処するのか。組織のデータを確実に保護できるプロセスが用意されているか。

3.6 組織の利害の衝突

過去、現在、または将来に実行された（または実行される）作業に関する利害を、契約を結んだサービスプロバイダが持つ場合、組織的な利害衝突（OCI; conflict of interest）が存在する可能性がある。利害衝突が存在する場合、サービスプロバイダが公平で、技術的に適切で、且つ客観的なサービスを提供する能力が減衰したり、競争上不公平な優位性をもたらすことがある。もちろん、組織的な利害衝突が起きる前に回避できれば一番よい。連邦取得規則（FAR; Federal Acquisition Regulation）（下位区分9.5）では、OCIの回避が重要である理由について、2つの根本的な原則を挙げている。

・[サービスプロバイダの]判断を偏らせる原因となる、対立する二つの役割が共存するのを防ぐ

・競争上不公平な優位性が生じるのを防ぐ

FAR では、[サービスプロバイダ]が、すべての競争者が利用できるわけではない機密情報を、契約に関連した適切な認可や供給業者選定情報なしに政府担当者から手に入れており、こうした情報が、契約獲得時にその[サービスプロバイダ]に有利に働くような場合に、競争上不公平な優位性が存在することがあるとしている。

FARは連邦政府の契約にのみ適用される規則であるが、どの組織おいても、OCIがITセキュリティサービスのライフサイクルの全てのフェーズで起こる可能性があり、競争上不公平な優位性がもたらされるかもしれないことを認識しておかなければならない。

・組織が、OCI の影響を回避、無力化、または最小化するために行えるいくつかの方法がある。たとえば、合意書、作業別計算書、契約などで差し障りのある部分を修正または消去するという方法がある。

・サービスプロバイダが要件の作成で重要な役割を果たした後で、入札に参加することを禁止する。

・サービスプロバイダがアクセスできる機密情報または権限の必要な情報の使用を禁止する。

・作業の実行への関与を防止し、作業に影響する立場にならないように、サービスプロバイダ内で作業を区分する。

・サービスプロバイダが、自身の作業を検査するように求められた場合など、結果としてOCIになるかもしれない行為をしないよう要求する。サービスプロバイダは、その関係を開示し、その作業の実行から自らを不適格にしなければならない。

・権限の必要なドキュメントをそれを必要とするすべての者に公開する（OCIの無効化）。

OCI が存在しているが回避できないと判断し、続行したいと考えた場合、組織の首脳は続行して、OCI を放

棄することもできる。

OCI の存在を特定し、OCI の効果を許容レベルまで緩和し、または OCI を無効にすることは、IT セキュリティサービスのライフサイクルを管理する場合に重要であるが、複雑な法的問題や規制上の問題が発生することがあるため、組織の法務部門の綿密な助言なしに検討すべきではない。

4. IT セキュリティサービスのライフサイクル

IT セキュリティサービスのライフサイクルは、IT セキュリティの意志決定者とマネージャに、IT セキュリティサービスの選択、インプリメント、および管理に使用できる 6 フェーズプロセスを提供する。この章では、ライフサイクルのさまざまなフェーズと、各フェーズ内での課題および決定事項について詳細に説明する。図 4-11 に示すように、セキュリティサービスのライフサイクルは、直線的と反復的の両方の要素を併せ持つ。開始、インプリメント、終了までは直線的に進行するが、アセスメント、ソリューション、運用のフェーズは、IT セキュリティサービスを成功させるために、継続的に行われなければならない。

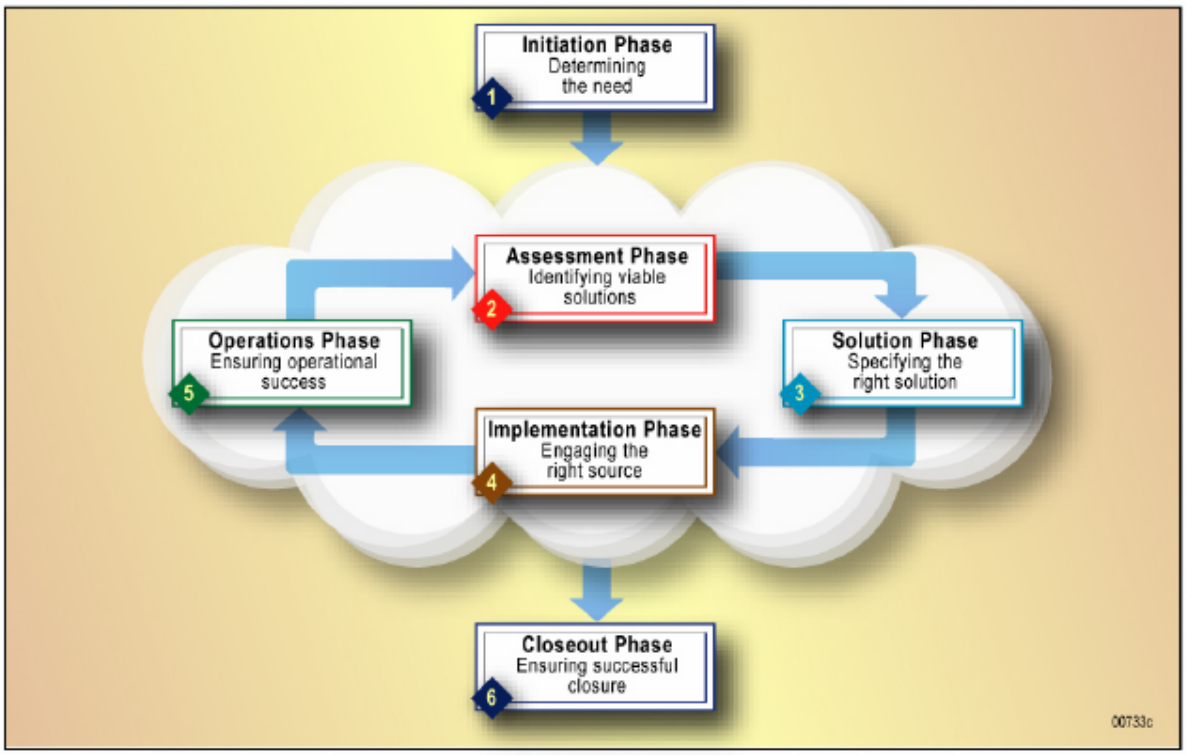

図 4-1 IT セキュリティサービスのライフサイクル

6 つのフェーズは次のとおりである。

- **フェーズ 1: 開始**

  サービスのライフサイクルを開始する必要性について認識する。第 4.1 項では、このフェーズでのトリガーについて説明する。

・ **フェーズ 2: アセスメント**

意志決定者はサービスをインプリメントし、サービスプロバイダを選択する前に、現在の環境を正確に描写する必要がある。第4.2項では、フェーズ2と、適切なメトリクスの作成および収集の重要性について説明する。

・ **フェーズ 3: ソリューション**

意志決定者は、アセスメントフェーズ中に特定した実行可能な選択肢の中から、適切なソリューションを選択する。第 4.3 項では、ビジネスケースとインプリメント計画について説明する。

・ **フェーズ 4: インプリメント**

サービスとサービスプロバイダは、インプリメントフェーズの中でインプリメントされる。第 4.4 項では、サービス契約の作成とサービスインプリメントについて、意志決定者を対象に説明する。

・ **フェーズ 5: 運用**

サービスは運用され、サービスプロバイダは完全に組み込まれ、サービスレベルおよびパフォーマンスの監査が定期的に行われる。第 4.5 項では、サービスレベルおよびパフォーマンスの監視におけるメトリクスの重要性について説明する。

・ **フェーズ 6: 終了**

環境が変化することで、サービスが不要となったり、パフォーマンスの低下が顕著な場合は、IT セキュリティサービスの交換または終了が必要になる。第 4.6 項では、フェーズ 3 で作成した終了計画を使用して、サービスまたはサービスプロバイダ、あるいはその両方の終了および引き上げる方法について説明する。

4.1 フェーズ 1: 開始

図 4-2 では、IT セキュリティサービスのライフサイクルのフェーズ 1 開始を表している。このフェーズは一つのステップだけで構成される：組織が現在の環境を評価し、実施可能なサービスソリューションを特定する引き金となるイベントの発生である。このイベントの定義を満たす具体的なトリガーは、組織によって異なる。トリガーは、第 3.4 項で挙げた 6 つの領域、戦略/使命、予算/資金、技術/アーキテクチャ、組織、人員、およびポリシー/プロセスのいずれかに該当する。表 4-1 は、各課題領域においてトリガーとなるイベントの例を示している。

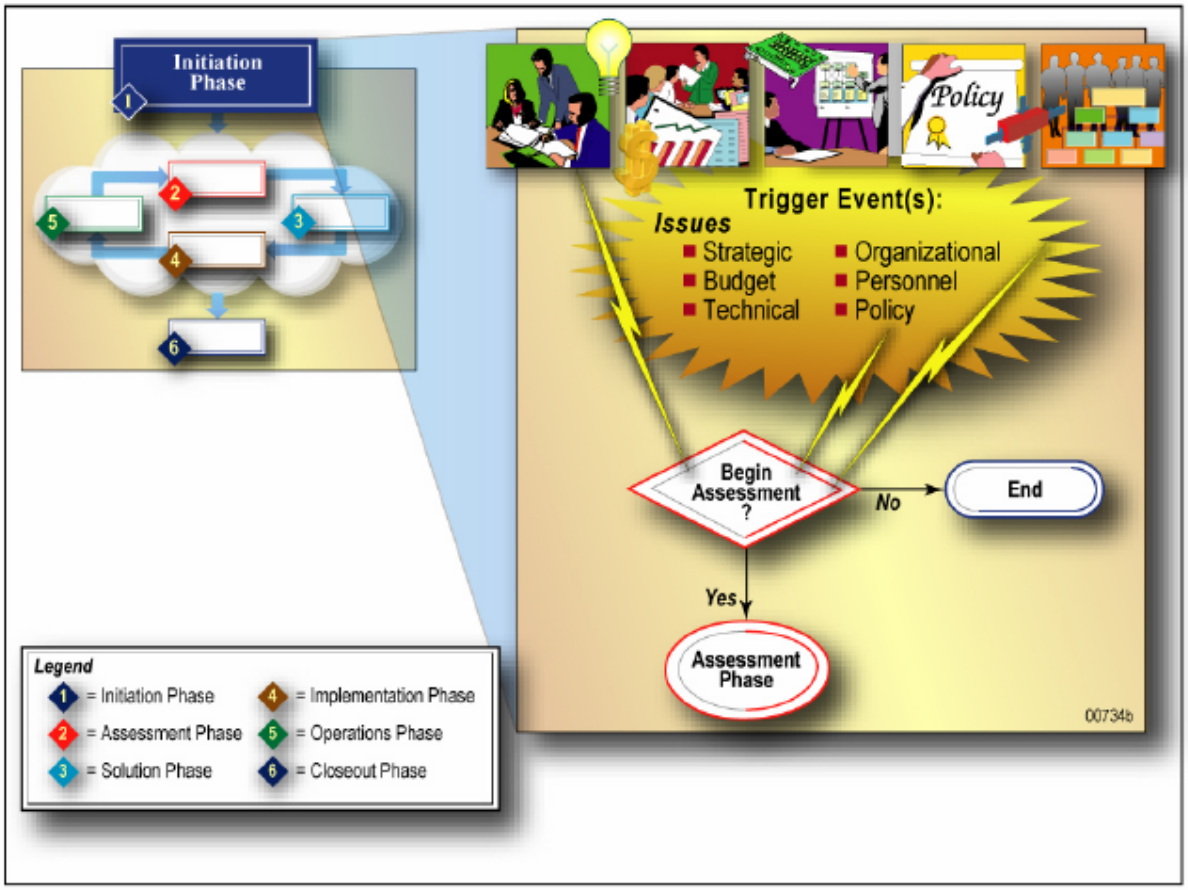

図 4-2 開始フェーズ

ビジネスマネージャ、IT マネージャ、および IT セキュリティマネージャが、サービスライフサイクルを開始する。セキュリティサービスの決定においては、ビジネス機能のサポートに最適なサービスアレンジメントで、最適なレベルで、最適なセキュリティサービスを獲得するように行う必要がある。ライフサイクルの次のフェーズ、アセスメントでは、最適なサービスが、内部で実行されるか外部で実行されるかを判断する。

1 つの IT セキュリティサービスのライフサイクルが開始されると、多くの場合、別のライフサイクルが終了する。円滑な移行を行うには、マネージャは、終了するサービスと開始するサービスとの間で起こりうる相互作用と影響について認識する必要がある。

表 4-1 IT セキュリティ問題とライフサイクルトリガの例

戦略/使命	・ ビジネスモデルの変更 ・ 組織の使命およびビジネス機能により適応するための、新しいサービスアレンジメントへの投資
予算/資金	・ より充実したセキュリティサービスを実現するための IT セキュリティ予算の増加 ・ コスト削減手段として妥当な場合の IT セキュリティ予算の削減
技術/アーキテクチャ	・ インプリメントする必要のある新しい技術 ・ 新しい技術へのアップグレード
組織	・ 成功していない現在の組織の環境および従業員の組み合わせ（すでに外部のサービスプロバイダを使用している場合） ・ 組織によるサービスアレンジメントアプローチの変更
人員	・ 数人の専門家の辞職、およびセキュリティサービス領域における専門知識の欠如
ポリシー/プロセス	・ 組織のセキュリティニーズに適合しなくなった現在使用中のポリシーやプロセス

4.2 フェーズ 2: アセスメント

フェーズ 2 アセスメントは、図 4-3 に示すように、開始フェーズに続く。このフェーズでのステップには、既存の環境のベースラインの確立、機会と障害の分析、オプションとリスクの特定がある。既存の環境のベースラインを理解するために、意志決定者は、メトリクスと総所有コスト（TCO; total cost of ownership）の原則を使用して、意志決定に利用される最も正確なデータを確保する必要がある。これらのデータは、後のフェーズのサービス契約で使用するパフォーマンス目標と予想されるコストの決定にも利用する。

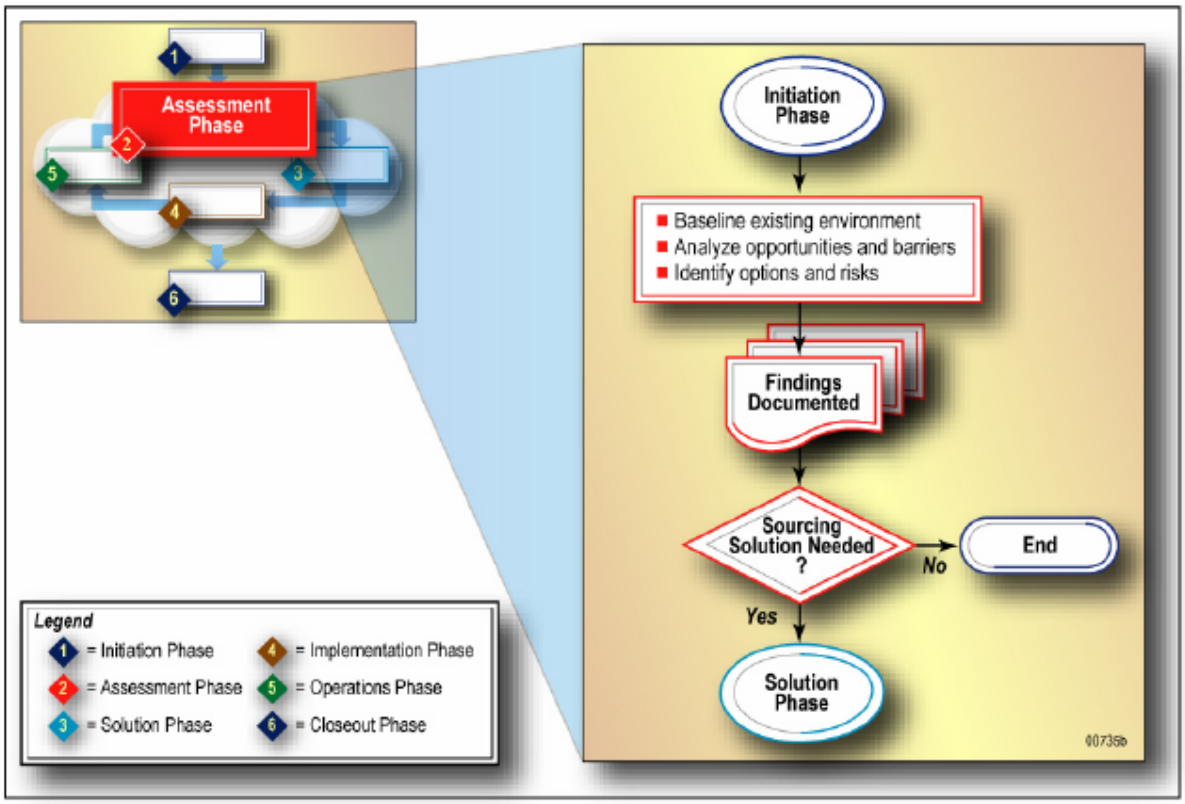

図 4-3 アセスメントフェーズ

意志決定者は、サービスメトリクスと総コストに留意しながら、機会と障害の検討を開始する。第 3.4 項で述べた IT セキュリティサービス課題のほか、市場や顧客などの外部要因も、機会と障害を分析するためのフレームワークを形成する。最終的に、既存の環境、機会、または障害に応じて、マネージャには選択肢とリスクが与えられる。これらの選択肢の中から、マネージャは、フェーズ 3 でソリューションを選ぶことになる。

4.2.1 既存の環境のベースラインの確立

マネージャは、IT セキュリティのライフサイクルを開始した後、現在の環境の基本ベースラインを確立する必要がある。このベースラインは、現在のアレンジメントがセキュリティ要件をどれだけ満たしており、どれだけのコストがかかっているかをマネージャに提示する。マネージャは、複数のサービスアレンジメントにおける利益や複数のサービスプロバイダ間における提案を比較するために、これらの 2 つの測定値が必要になる。

ここでの作業範囲は、セキュリティコントロールの性質またはその組み合わせに依存する。コントロールまたはコントロールの組み合わせに関する全ての領域がカバーされなければならない。たとえば、もし組織がファイアウォールサービスを評価するのであれば、組織はファイアウォールポリシーやその他のポリシー、ファイアウォールアーキテクチャの効果、ここでの作業に関係するその他の問題についても評価する必要がある。

ベースラインの確立に使用するデータは、客観的で、公平で、包括的な方法で収集する必要がある。現在の環境の利害関係者は、サービスレベルの決定や調達するソリューションの選択に使用されるデータの提供、またはデータの収集の支援を要求されることがある。現在の利害関係者は特別な利害を有しているために、彼らが用いるデータ収集テクニックやレポート方式には、意図的かどうかにかかわらず、この利害が反映されてしまうことがある。メトリクスや TCO などの公式なツールを使用すれば、データ収集作業において不本意に利害が偏るのを最小限に抑えることができる。さらに、過去のメトリクスとデータを再検討すれば、現在の環境のベースラインの確立において利害の偏りをなくすことができる。

4.2.1.1 メトリクスの作成、収集、分析

メトリクスは、意志決定者に、客観的に定量化できるデータを提供する。メトリクスの重要性は、このフェーズから始まり、ライフサイクル全体にわたって存続する。

メトリクスの作成は測定する「対象」を定めることから始まる。メトリクスは、組織の全体の機能とセキュリティ目標に対応付けられ、サービスが提供する所期の結果に連動している必要がある。どのサービスに対するメトリクスでも、次の点に関連したデータを含む必要がある。

- **インプリメントレベル**
  インプリメントレベルのメトリクスは、同意された必要な活動が同意された時間枠内でどの程度完了しているかを定量化する。

- **サービスレベル**
  このメトリクスは、サービス提供の適時性を定量化する（つまり、運用を回復するまでの平均時間や、ファイアウォールの再設定にかかる時間）。

- **効果**

効果のメトリクスは、サービスがどの程度適切に提供されたか、およびその有効性（つまり、顧客サービス評価、セキュリティ侵入および遮断レベル、コンピュータウィルスに感染したシステム数）を表した結果要素である。

・ **ビジネスの影響**

ビジネスの影響メトリクスは、財源および運用資源などのビジネスパラメータに対する影響を定量化する（ウィルス攻撃による金銭的損失、サーバー停止による作業時間の損失）。

メトリクスの作成に関するその他の考慮事項には、次の点がある。

・ 実際に収集できるメトリクスだけを考慮する。

・ 取得可能で定量化できるイベントのみを、メトリクスの基盤とする。

・ 技術的機能から問題解決手順、人員の適性まで、IT セキュリティサービスのすべての側面を考慮する。

・ ビジネスの運用目標をメトリクスの基盤とする。

・ 提供される IT セキュリティサービスのレベルの評価を十分に洞察し、サービスオプションを適切に比較する。

・ 結果だけでなく原因を評価できるようにメトリクスを収集する。

・ 傾向を追跡できるようにメトリクスを収集する。

NIST SP 800-55『情報技術システム用のセキュリティメトリクスガイド（Security Metrics Guide for Information Technology Systems）』では、有用なメトリクスの特性に関する詳細と、練り上げられた（練り上げられている）メトリクスプログラムを用意することの重要性について述べられている。フェーズ 3、4、5 において、組織が目標を設定し、サービス契約を作成し、サービスプロバイダのパフォーマンスを監視する IT セキュリティサービスのライフサイクルを経ることで、IT セキュリティに対する反復可能で一貫したメトリクスアプローチの重要性が明らかになってくるだろう。

4.2.1.2 総所有コスト

メトリクスプログラムと関連して、IT セキュリティサービスの意志決定者は、サービスの総コストを特定する必要がある。メトリクスは、さまざまな活動におけるコストの判断に役立つので、この作業に組み込むことができる（たとえば、ダウンタイムのコスト、ウィルス攻撃のコスト）。総コストの原則は一般に、TCO と呼ばれている。TCO には、インプリメントコストと運用コストだけでなく、関連コストも含まれる（間接費、給料、給付金、技術のアップグレード、ソフトウェアサポート、および保守など）。意志決定者は、これらの情報を使用して、ソリューショ

ンフェーズでのビジネスケースの作成中に、他のサービスアレンジメントのコストと既存の環境のコストとを比較することができる。総コストを特定すれば、意志決定者は、あるサービスオプションが他のオプションに比べてどれくらい価値があるかを正確に説明できるようになる。

4.2.2 機会と障害の分析

パフォーマンスとコストの観点から現在の環境を理解できれば、組織は、機会と障害の分析を開始することができる。機会と障害を分析すると、組織は、変更できる機能と領域、変更できない機能と領域、およびそれぞれの理由を特定できるようになる。IT セキュリティの利害関係者はプロセスに参加して、分析結果を承認する必要がある。適切に実施された分析には、次の点が含まれる。

戦略/ミッション

・ サービスおよび機能がビジネスにとってどれだけ重要かを特定する。

予算/資金

・ 予算委員会による承認と資金を確保するために、すべての該当する規制や法規に従って、合理的で実行可能な財政計画を明確にする。

技術/アーキテクチャ

・ 組織の技術能力の保持が重要かどうかを判断し理解する。

組織

・ どのサービスアレンジメントが、組織の作業環境と価値にとって適切かを判断する。
・ 管理職が、すべての利害関係者にとっての無形利益（たとえば、従業員の士気の改善や組織のイメージなど）を、これから作成するビジネスケースに組み入れることができるようにする。

人員

・ すべての利害関係者が、何より重要なパフォーマンスの目標と特定のニーズを特定し、提案要求書（RFP; Request for Proposal）/SOW/サービスレベル契約（SLA; Service Level Agreement）の要件など、特定のサービスレベル要件に変換できるようにする。

ポリシー/プロセス

・ 将来の所期のサービスアレンジメント戦略に向けて、統合と移行に取り組み始める。

4.2.3 選択肢とリスクの特定

アセスメントフェーズの最後のステップでは、意志決定者は、選択肢とリスクの特定を開始する必要がある。ベースラインでは現在の環境を示し、機会と障害のステップでは期待する目標を描き始めた。このステップでは

「その方法（ハウツー）」をより明確にする。

この「方法」ステップでは、サービスアレンジメントを決定する。第 3 章で説明したように、組織は、内部チームとスタッフだけを使用する場合から、セキュリティサービスの完全な外部委託まで、さまざまなセキュリティサービスアレンジメントを使用して、セキュリティサービス要件を実行できる。このライフサイクルフェーズでは、多くの組織はまだ、多くの選択肢とさまざまなサービスアレンジメントを考慮する必要がある。これらの 1 つ 1 つについて、組織は、利益とリスクを特定する必要がある。

場合によっては、既存のアレンジメントとサービスレベルが効果的であり適切であることが明らかになることもある。ビジネス機能、顧客、および効果的なセキュリティに焦点を当てることが非常に重要である。選択されたアレンジメントやサービスレベルは、これらの 3 つの点を最も適切に満たしていなければならない。ビジネスおよび IT プロセスを改善することは、おそらく、サービスアレンジメントを変更するよりも効果的でリスクも少ない。組織は、サービス、サービスアレンジメント、またはサービスプロバイダを変更することによってのみ改善できる領域が、アセスメントの実施によって明確にならないかぎり、現在の環境を変更しようとしてはならない。

4.3 フェーズ 3: ソリューション

図 4-4 では、IT セキュリティサービスのライフサイクルのフェーズ 3 ソリューションを示している。

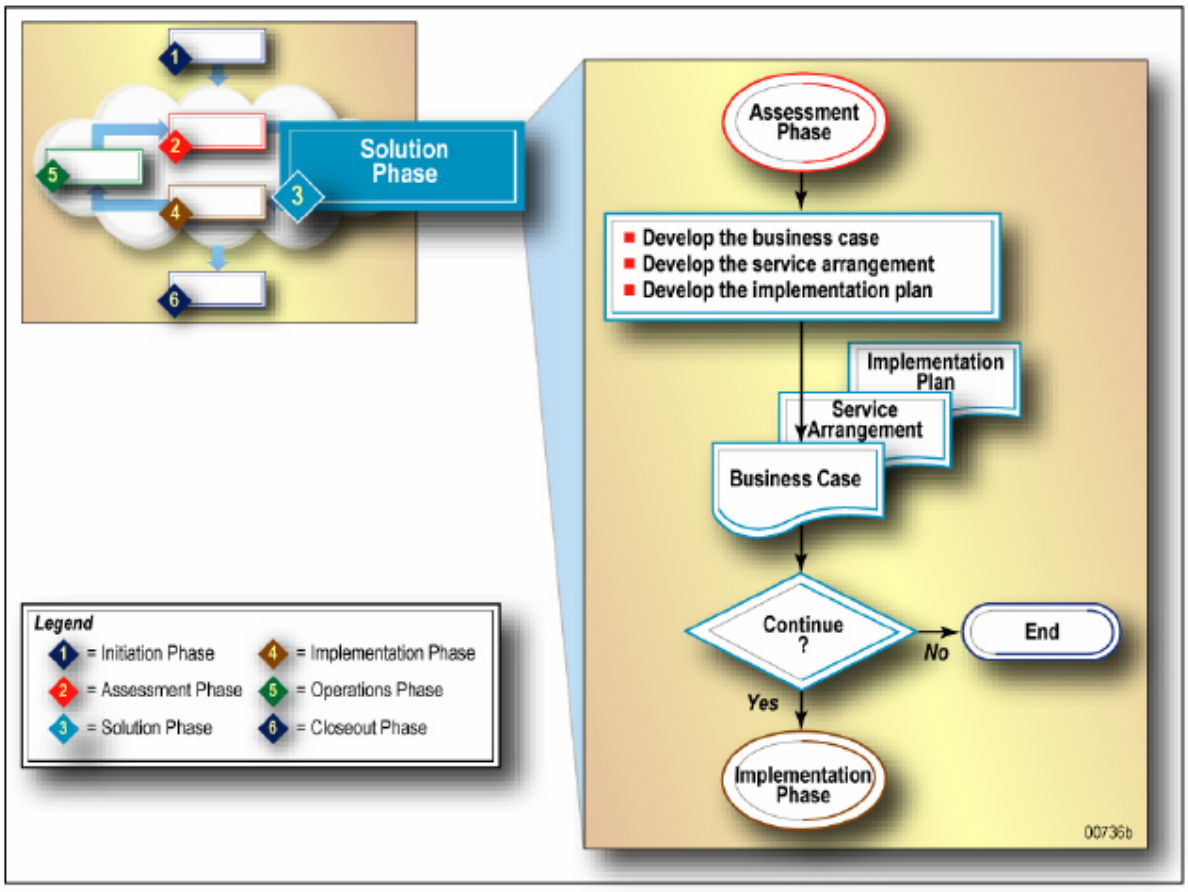

図 4-4 ソリューションフェーズ

サービスアレンジメントとサービスレベルに関するソリューションの選択が、このフェーズの唯一の要素である。ソリューションを指定する前に、意志決定者は、考慮すべき個々の可能性について、詳細なビジネスケースを練り上げる必要がある。

ビジネスケースは、マネージャに、個々の代替案に対する、コスト、利益、および組織に対するリスクを予想する材料を提供する。コスト、利益、および組織に対するリスクを比較すると、マネージャは、好ましいソリューションを特定できるようになる。インプリメント計画は、サービスプロバイダを特定する方法とサービスのインプリメント手段を、マネージャに与える。

4.3.1 ビジネスケースの作成

アセスメントフェーズの中で、意志決定者は現在の環境を明確にした。このソリューションフェーズでは、将来に期待する状態を特定するために、ビジネスケースを作成する必要がある。ビジネスケースは、代替案の中で最も適切なソリューションを特定するのに必要な情報を提供する。大抵の場合、組織はビジネスケースを作成するための独自の方法論を持つようになるが、次の 5 つの要素は、ほとんどのビジネスケースの作成に共通している。

- **代替案分析** [2]
  組織は、利用可能なすべての選択肢を検討する必要がある。組織は、正式なコスト見積もり、利益分析、および組織に対するリスクの分析を作成するのに十分実行可能と考えられる選択肢を最終的に決定する。

- **コスト見積もり**
  組織は、個々の代替案について TCO 見積もりを作成する必要がある。個々の代替案と現在の環境の見積もりには一貫性があり、同様のコスト要素を含み、同じ仮定に基づいている必要がある。

- **利益分析**
  組織は、個々の代替案の利益を正式に特定する必要がある。これらは、可能な場合は必ず、定量化する必要がある（コスト節減、コスト回避など）。たとえば、（アセスメントフェーズ中に収集されたメトリクスに基づいて）新しいサービスのインプリメントによって、セキュリティインシデント率を 50%引き下げるには、インシデントごとに x ドルかかると見積もった場合、組織はコスト回避の可能性を特定できるようになる。また、使命や顧客に対する影響といった質的な利益を考慮することも重要になる。

- **プロジェクトリスク分析**

各代替案の利益とともに、プロジェクトリスクも特定する必要がある。OMB では、組織および変更管理のリスク、ビジネスリスク、データ/情報リスク、技術的リスク、戦略的リスク、セキュリティリスク、プライバシーリスク、プロジェクトリソースリスクの 8 つの標準的なリスクカテゴリを定めている [3]。これらのリスクには、予算超過、スケジ

ュールの遅れ、ベンダーに関する不確定要因、プライバシーに対する懸念などが含まれることもある。リスクの分析は、すべての代替案を同じリスク要因に対して評価し、発生する確率と発生した場合の影響を判断する必要がある。組織は、その後、それぞれの代替案のリスク調整コストを決定する必要がある。

---

[2] たいていの場合、このステップはアセスメントフェーズ中に完了している。[3] OMB Circular A-11、Exhibit 300

- **代替案の評価**

  最後に、組織は、コスト、利益、およびリスクに基づいて、個々の代替案を格付けする必要がある。この分析から、組織は適切な代替案を特定できる。

4.3.2 サービスアレンジメントの作成

データ収集、分析、選択肢の比較という面倒な作業がすでに終了しているので、サービスアレンジメントの作成は比較的短いステップになる。ビジネスケースを利用しても、意志決定が簡単にいかない、または明確にならないこともあるが、ビジネスケースは意志決定者が組織のニーズに適したサービスアレンジメントを比較検討、考慮、選択するために必要となるデータを提供していなければならない。意志決定者の間で議論や意見の相違が見られる可能性もあるが、最終的に選択には合意が必要である。ビジネスマネージャや IT セキュリティマネージャ全員が、インプリメントするソリューションに完全に賛同している場合にのみ、サービスアレンジメントは成功する。

4.3.3 インプリメント計画の作成

この時点で、関係者は、サービスアレンジメントの予算と範囲を決定し、インプリメント計画の作成を開始しなければならない。インプリメント計画は、現在の環境から将来の所期の環境へ移行するためのロードマップを、組織に提供する。インプリメント計画では、次の点に対処する必要がある。

- **プロジェクト管理の役割と責任**

  インプリメント計画は、インプリメントフェーズと運用フェーズの両方におけるプロジェクト管理の役割と責任に、個人の役割と責任を関連付ける。

- **予算と範囲**

  IT セキュリティマネージャは、サービスアレンジメントの予算と範囲を定める。この取り組みは、次のフェーズでのサービスプロバイダの特定、依頼、評価にとって重要になる。

- **インプリメントプロセス**

  プログラムマネージャは、IT セキュリティサービスのインプリメントに関する自身のビジョンを明確にする。たとえば、プログラムマネージャが、テストグループやパイロットプログラムから開始しようと考える、またはサービスの移行期間を設けようと考える場合、その作業を遂行するプロセスを、ここで詳細に取り決める。

・ **リスク移行計画**

IT セキュリティプログラムマネージャは、アセスメントフェーズとソリューションフェーズで特定したそれぞれのリスクを移行させる自身の計画を具体化する。

・ **終了計画**

終了計画は、組織内の他の業務を阻害せずにサービスアレンジメントを確実に終了するために作成する。終了計画は、サービス契約満了などの通常の予定された終了、サービスプロバイダの倒産などの予定外の終了、およびサービスプロバイダ能力不足などの緊張に満ちた終了に対する行動計画を提供する。

・ **移行管理**

移行管理計画では、現在の環境から将来の所期の環境への移行を管理する組織の取り組みについて、文書化する。マネージャは、配置転換した従業員の応対、変更に対する抵抗への対処、組織の焦点の転換、および従業員への変更に関する明確な説明を行うための計画を作成する。あるサービスアレンジメントから別のサービスアレンジメントへの移行する際には、おそらくかなりの額の移行コストが生じることになる。これらのコストは、ライフサイクルコストおよび代替案の分析に織り込んでおく必要がある。また、これらのコストは、移行計画の作成時にも検討されるべきである。

4.4 フェーズ 4: インプリメント

サービスアレンジメントとサービスプロバイダの選択は、実際、IT セキュリティのライフサイクルの中でも簡単な部分である。メトリクスの作成とデータの収集は、特にメトリクスプログラムがまだ用意されていなければ、かなりの作業が必要になる。様々なサービスを組み合わせることは大変な作業だと思うかもしれないが、客観的なデータと体系的な分析によって最適な方針は明確になっているはずである。こうした決定を行うには、準備と注意が必要になる。マネージャは、明確なサービス契約を作成して、インプリメント計画が慎重に実行されるようにしておかなければならない。慎重な計画と実行は成功確率を高めるが、サービスが運用フェーズに移れば、マネージャはサービスに求める期待レベルを管理していく必要がある。どのサービスアレンジメントも一夜で問題を修正するわけではなく、どのサービスプロバイダも完全な状態で登場するとは限らない。図 4-5 では、IT セキュリティサービスのライフサイクルのフェーズ 4 インプリメントを示している。

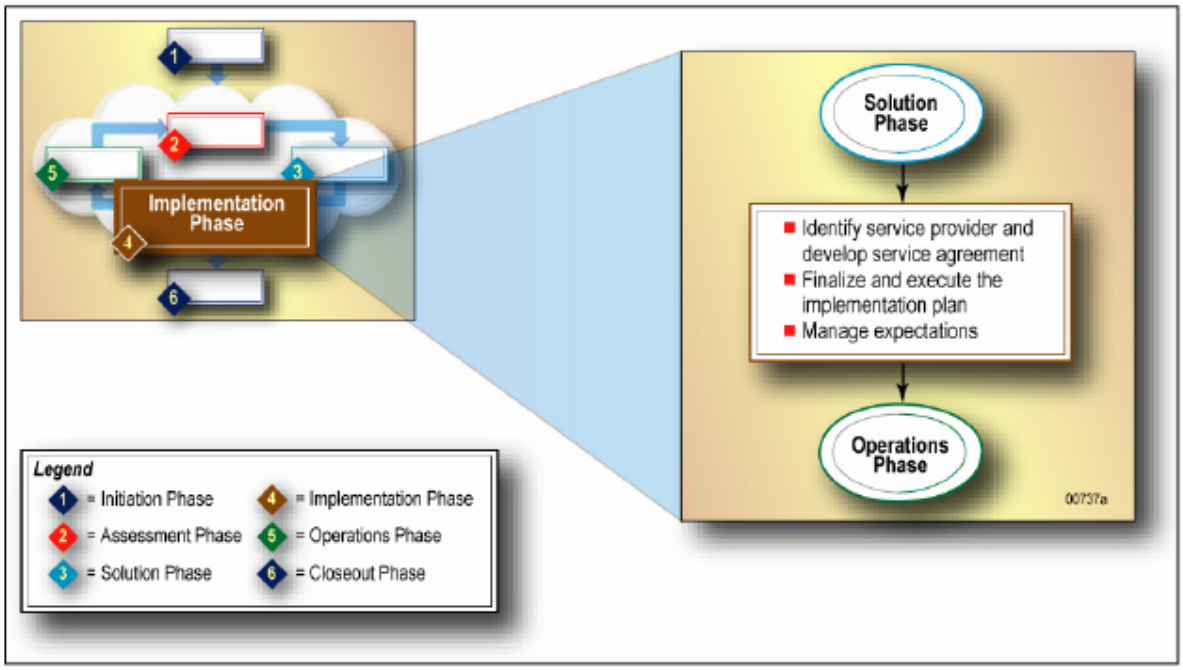

図 4-5 インプリメントフェーズ

4.4.1 サービスプロバイダの特定とサービス契約の作成

ソリューションフェーズの間、セキュリティ意志決定者は、サービスアレンジメントを選択する。このフェーズでは、サービスプロバイダを特定する必要がある。サービスプロバイダを特定する方法は、組織、サービス契約、およびサービスアレンジメントのタイプによって異なる。内部のリソースを使ったサービスアレンジメントでは、すでにサービスプロバイダは決まっているかもしれない。外部調達によるサービスアレンジメントまたは混合したアレンジメントでは、組織は、複数のサービスプロバイダを特定して、提案を引き出すことができる。大規模の政府組織では、RFP を公開して、外部調達によるサービスアレンジメントの公式な提案を受け付けることもある。組織がどの特定の契約方法を選択するかにかかわらず、次の基本的なステップがほとんどの場合に適用される。

パフォーマンスベースの取得が、多くのアレンジメントで外部サービスプロバイダを導入する望ましい方法として使用されている。パフォーマンスベースの取得では、サービスプロバイダが適切なソリューションを提案する際に、より柔軟に提案できるようになっている。ジョブポジション、従業員要件、および方法を指定した RFP に回答するように、サービスプロバイダに要求するのではなく、組織は、コスト効率のよい方法を提供するようにサービスプロバイダに要求するのである。たとえば、これまでのフェーズで特定されたメトリクスは、競合するサービスプロバイダが自身の SOW と目標達成のコストを記して返答する目的記述書に換えることができる。この方法は、組織が SOW を作成し、サービスプロバイダがその作業の実行に要するコストを記して返答していた従来の取得方法とは対照的である。サービスプロバイダにより重い責任を負わせることにより、組織は、はるかに広範かつ綿密にソリューションを評価でき、適切なサービスプロバイダを見つける確率が高まる。

・ **サービスプロバイダのサービスレベル目標の設定**

ベースラインフェーズで関連データを特定し取得しているので、IT セキュリティマネージャは、サービスプロバイダが満たすべきパフォーマンス目標を決定する必要がある。これらのサービスレベルは、サービスプロバイダと交渉を重ね、サービス契約で正式に文書化する。

・ **サービスプロバイダからの提案の募集**

組織は、さまざまな方法でサービスプロバイダを特定することができる。サービス領域に少数のプロバイダしかいない、または新規市場である場合、組織は、その分野の全サービスプロバイダに、見積もりとサービス内容を要求できる。組織は、RFP を告知して、コスト提案を提供するように利害関係者に指示することもできる。組織は、方法とは無関係に、できるだけ多くのサービスプロバイダを検討し、競争を促進させる必要がある。組織は、このガイドの第 3.5 項で挙げた質問のいくつかに答えるように、サービスプロバイダに求めることもできる。

・ **提案とサービスプロバイダの評価**

組織は、さまざまなサービスプロバイダの提案、コスト見積もり、または管理計画、あるいはそれらの組み合わせを評価して、各プロバイダについて慎重に検討する必要がある。提案されたコストが最も重要な要因になるかもしれないが、マネージャは、価値、サービスプロバイダの評判、サービスプロバイダの過去の業績、および組織が持つ使命をサポートする上でのサービスプロバイダの能力などについても、コストに比較してバランスを取る必要がある。組織は、方法体系、サービスレベル、およびコストが、組織の予想に一致しており、それらが実現可能であるかを確認する必要もある。たとえば、コストとサービスレベルが競合他社の水準をはるかに超えている提案は、疑いの目を持って、さらなる調査を実施した方がよい。

・ **サービスプロバイダの選択**

サービスプロバイダを評価した後、意志決定者は、ニーズ、目標、対象に最も適合したサービスプロバイダを選択する。

・ **サービス契約の作成**

価格とサービスレベルのさらなる交渉が必要になることもあるが、価格とサービスレベルが合意に達すると、サービス契約を作成する必要がある。サービスアレンジメントによっては、このプロセスはある程度公式的なものになる。たとえば、内部調達によるサービスアレンジメントでは、同意されたプロセス、報告内容、MOA から構成される。外部調達によるサービスアレンジメントでは、正式な契約内容を文書化する必要がある。サービス契約書として使用されるドキュメントのタイプに関わらず、契約内容は内部調達と外部調達のサービスプロバイダ共に同じでなければならない。

契約では、契約のタイプに関わらず、次の内容を指定する必要がある。

・ 組織の役割および責任とサービスプロバイダの役割および責任の両方の明確な定義（人物保証のレベルやスタッフの身元調査など）

・ 場所や施設のセキュリティ要件などを含めたサービス環境、ポリシー、手順、標準、契約、ライセンスの説明

・ 定められたサービスレベルとサービスレベルのコスト。サービス契約におけるサービスレベルの選択では、顧客のタイプもしくは価格レベルに応じて異なるサービスレベルを規定し、実施期間に応じて異なるサービスレベルを規定することができる。たとえば、契約の 1 年目は 2 年目よりも高いサービスレベルを要求できる。

・ サービスレベルと期日目標、規則、その他の契約条件をサービスプロバイダが遵守しているかどうかについて、マネージャが査定する方法を定めたプロセス

・ サービスプロバイダによる不履行または損害に対する具体的な是正措置（金銭、法的など）

・ 実施期間または納入期日、あるいはその両方

・ 組織の管理職に対するサービスプロバイダの窓口

・ サービスプロバイダが情報およびリソースを利用できるようにすることに関する組織の責任
・ 組織およびサービスプロバイダのデータの混在に対する手順および保護

・ 機密データの取り扱いの明示的な規則

以上のうち 1 つまたは複数の項目が考慮されなかったために、サービスアレンジメントがうまくいかないことが非常に多い。組織はニーズを明確に定義し、サービスプロバイダは期待されていることを明確に理解しておく必要がある。

4.4.2 インプリメント計画の完了と実行

これまでの活動によって、サービスプロバイダとサービスレベルが確定したので、組織は、インプリメント計画を完了し、計画の実行に移すことができる。いくつかの詳細は、サービスアレンジメントの交渉中に変更でき、マネージャはどのように計画が変更されるかについて認識しておく必要がある。

4.4.3 期待レベルの管理

新しいサービス、サービスアレンジメント、サービスプロバイダが稼動すると、すべての関係者はサービスに対する期待レベルを管理する必要がある。それぞれの関係者が新しいセキュリティと組織の環境に適応し、運用を始めると、いくつかの矛盾が生じることがある。綿密な監視と協力を確保するために、マネージャとサービ

スプロバイダとの間で通信回線を開き続けておく必要がある。

重要なガイドラインとして次の点が挙げられる。

・ 組織内部での衝突か、内部グループと外部のサービスプロバイダとの間の衝突かに関わらず、隠し立てせず問題に対処する。

・ まだアカウンタビリティが確保されている間に、サービスプロバイダがその責務を行えるようにする。

・ セキュリティサービスのライフサイクルを保持する。

4.5 フェーズ 5: 運用

運用フェーズは、サービスプロバイダとサービスのインプリメントが完全に終わってから開始する。このフェーズの間、サービスアレンジメントが現場のニーズに最も適合していることを確認するために、組織、そのセキュリティ、セキュリティサービスプロバイダが監視される。このアセスメントは、稼動中のライフサイクルの終了と新しいライフサイクルの開始を引き起こすトリガーが発生するまで続けられる。組織とサービスプロバイダは、発生した問題に対処できるように、通信回線を開いておく必要がある。

運用フェーズ全体を通じて、組織のプロジェクトマネージャは、サービスプロバイダが、その規定されたサービスレベルを満たし、内部のセキュリティ手順およびポリシーを遵守していることを確認する必要がある。たとえば、組織では、外部のサービスプロバイダが機密を要する資料（人的、プライバシー、ミッションの機密にかかわらず）を取り扱う場合、内部のサービスプロバイダと同じようには徹底できないことが多い。内部のサービスプロバイダが人物保証を必要とする場合、外部のサービスプロバイダも人物保証を必要とする可能性は非常に高いのである。図 4-6 では、IT セキュリティサービスのライフサイクルのフェーズ 5 運用を示している。

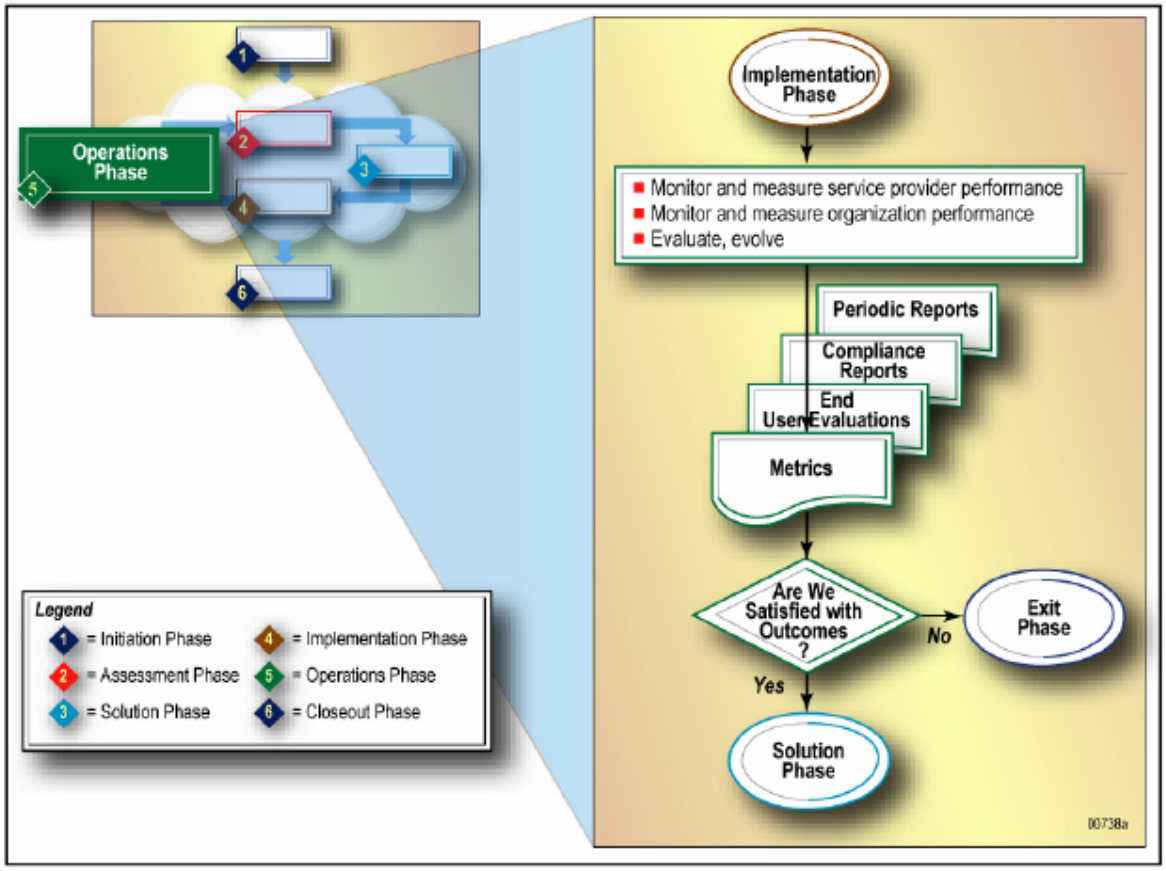

図 4-6 運用フェーズ

4.5.1 サービスプロバイダのパフォーマンスの監視

運用フェーズは、アセスメントフェーズと似ている。アセスメントフェーズで収集したデータは、この新しいサービスプロバイダのパフォーマンスレベルを掴むために利用される。運用フェーズでは、アセスメントフェーズで定義した将来の所期のアレンジメントが、現在のアレンジメントとなる。

サービス契約で規定した目標は、収集したメトリクスと比較する必要がある。メトリクスはサービスレベル目標を提供するが、組織は、エンドユーザーの評価や顧客満足レベル調査を使用して、パフォーマンスを評価することもできる。IT セキュリティマネージャは、他の運用マネージャ（顧客サービスマネージャなど）と協力して、サービスプロバイダがサービス目標を達成していることを確認しなければならない。IT セキュリティマネージャはまた、サービスプロバイダが、IT セキュリティポリシーやプロセスだけでなく、該当する法や規制を遵守していることも確認する必要がある。IT セキュリティマネージャは、サービスプロバイダが、プライベートなデータ、機密データ、人的データ、または組織の使命に関わるデータを危険にさらしていないことを、運用フェーズ中に確認する必要がある。遵守性に関するレポートが、この作業に役立つ。サービス契約は、不履行に対するペナルティ、是正措置、あるいはその両方を指定した条項を含んでいなければならず、管理する側は、サービスプロバイダが契約での指示どおりに実行していない場合、これらを適用しなければならない。

4.5.2 組織のパフォーマンスの監視と測定

サービスプロバイダはサービス契約で規定された目標を達成する必要があるが、IT セキュリティマネージャは、サービスとサービスプロバイダだけでなく、IT セキュリティ機能や組織全体に目を向ける必要がある。IT セキュリティ機能には、さまざまなレベルの IT サービス（管理、運用、技術）が複数混在しており、サービスアレンジメントには、技術、ポリシー、文化、人員などに対する影響が伴う。したがって、マネージャは、サービスアレンジメントが、サービスの実行中に他の領域に悪影響を及ぼしていないことを確認しなければならない。

4.5.3 評価と改善

サービスは成熟するにつれ進化していく。サービスプロバイダや組織の監視・測定を行うことにより、IT セキュリティの利害関係者は、組織のパフォーマンスを評価でき、目標が達成されたときでも改善の余地を求めることができる。IT セキュリティサービスの世界は絶えず変化し続け、セキュリティアレンジメントおよび契約も変更していく必要がある。

4.6 フェーズ 6: 終了

開始フェーズで述べたように、複数のライフサイクルが重なり合うこともある。1 つの IT セキュリティサービス、サービスアレンジメント、または契約が終了すると、別のものが開始する。サービスを終了する理由によっては、管理上、困難な状況が発生することがある。打ち切られたサービスプロバイダが必ずしも、組織に最善の利益をもたらすことを留意しているとはかぎらず、プロバイダの変更が簡単にはいかない場合もある。したがって、IT セキュリティマネージャは必ず、適切な終了計画を選択し、それをインプリメントしておく必要がある。

図 4-7 では、IT セキュリティサービスのライフサイクルのフェーズ 6 終了を示している。

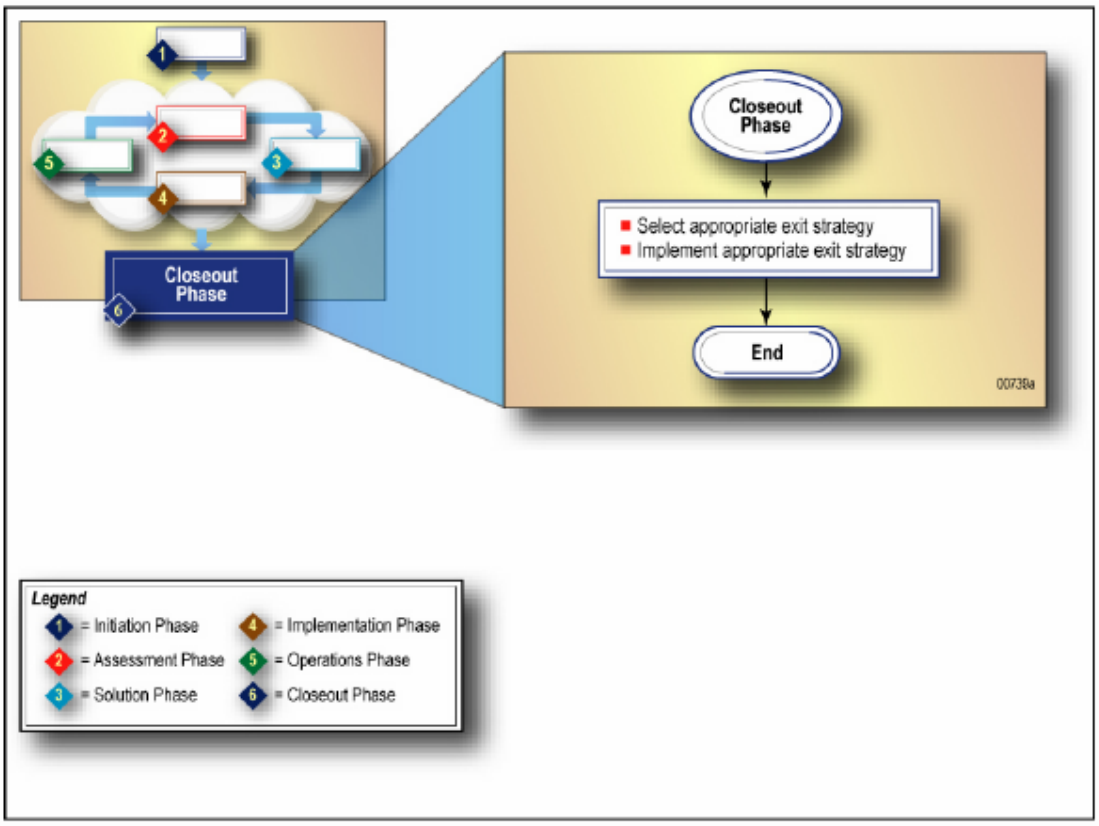

図 4-7 終了フェーズ

4.6.1 適切な終了計画の選択

終了計画の作成で述べたように、組織は、いくつかの終了計画を用意して、実施できるようにしていなければならない（第 4.3.3 項）。多くの場合、組織は前もって終了を予定することができる。たとえば、サービスプロバイダと組織が 6 か月後に失効する同意契約を結ぶことができる。ただし、これは常に当てはまるわけではない。サービスアレンジメントがマネージャの望むようにはうまくいかなかったり、サービスプロバイダが目標を達成できなかったり、新しい技術が登場したり、またはサービスプロバイダが突然破産申請をすることもある。マネージャは、このようなさまざまなシナリオを想定して、終了計画を速やかに実施できるように整えておく必要がある。

4.6.2 適切な終了計画の実施

サービス、サービスアレンジメント、またはサービスプロバイダを打ち切るために、適切な終了計画が決まると、プロジェクトマネージャは終了計画を実施に移す必要がある。終了計画があれば、綿密な終結が確実に行え、将来の所期の IT セキュリティサービスのインプリメントに対する教訓が得られる。

5. サービスのタイプ

効果的なITセキュリティプログラムには、複数の階層からなる防御手段が含まれている必要がある。組織は、その情報システムの価値と重要度を評価し、リスクレベルに適したセキュリティコントロールを決定しなければならない。組織のシステムレベルでも個人のシステムレベルでも、セキュリティプログラムは、管理、運用、技術のセキュリティコントロールを適切に組み合わせている必要がある[4]。管理または運用コントロールによって補完することなく、技術的リソースにのみ依存しているのでは不十分である。

この項では、このドキュメントで説明している管理、運用、および技術サービスの例を提示する。表 5-1 には、これから説明する IT セキュリティサービスを挙げている。それぞれのセキュリティサービスを定義し、サービス提供の性質が説明されている。この後に、それぞれのセキュリティサービスに固有の課題と考慮事項が記される。

表 5-1 カテゴリごとのセキュリティサービス

セキュリティサービス	カテゴリ
セキュリティプログラム	管理
セキュリティポリシー	管理
リスク管理	管理
セキュリティアーキテクチャ	管理
認証および認定	管理
IT 製品のセキュリティ評価	管理
緊急時対応計画	運用
インシデントハンドリング	運用
テスト	運用
トレーニング	運用
ファイアウォール	技術
侵入検知	技術
公開鍵基盤（PKI）	技術

[4] 管理、運用、技術のコントロールについては、NIST SP 800-12『コンピュータセキュリティ入門: NIST ハンドブック（An Introduction to Computer Security: The NIST Handbook）』、NIST SP 800-18『情報技術システム用セキュリティ計画の作成ガイド（Guide for Developing Security Plans for Information Technology Systems）』、および SP 800-53『連邦政府の情報システム用の推奨セキュリティコントロール（Recommended Security Controls for

Federal Information Systems)』で取り上げられている。

ここでは、利用可能なすべてのセキュリティサービスの網羅的なリストは記していない。セキュリティサービスプロバイダは、これらの複数のサービス要素を組み合わせ、独自の名称で独自のサービス内容を作り上げている。技術が進歩するにつれて、新しいセキュリティサービスが生み出される。多くの場合、このガイドで示すサービスに関する課題と考慮事項は、他のセキュリティサービスに合わせて使用することも、修正することもできるであろう。

5.1 管理セキュリティサービス

5.1.1 IT セキュリティプログラムの作成

IT セキュリティプログラムは、セキュリティコントロールを組み合わせたものであり、これらは管理、運用、技術という用語に基づいて分類できる。2002 年の連邦情報セキュリティ管理法（FISMA）、OMB Circular A-130『連邦政府の自動情報リソースのセキュリティ』、および OMB、NIST などの連邦機関によって公表されたその他の政府全般のポリシー、標準、手順をはじめとする連邦法や規制によって、連邦諸組織のポリシー、標準、手順が定められている。

通常ポリシーは適用範囲の広いレベルで作成されているので、組織は、従業員がポリシーを遵守する上での明確な方針となる標準、ガイドライン、手順も作成する必要がある。標準とガイドラインでは、システムを保護するために使用する技術や方法を指定する。手順は、特定のセキュリティに関連した作業を遂行する上で従わなければならない詳細なステップである。標準、ガイドライン、手順は、ハンドブック、規約、またはマニュアルを通じて組織全体に行き渡せることができる。これらのドキュメントが一緒になって、従業員が IT セキュリティにおける自身の役割を認識し、IT セキュリティプログラムを遵守できるようになる。

IT セキュリティプログラムサービス

サービスプロバイダは、セキュリティプログラムの効果を保証し、組織の主だったコンポーネントを評価し、セキュリティ関して重要な責任を持つ組織の従業員に対して適切なセキュリティトレーニングを提供することで、組織の意思決定者が組織全体に渡るセキュリティプログラムの構築とその維持を進めていくことを支援することができる。サービスプロバイダは、また、組織の IT セキュリティプログラムを独自に評価および監査できる。

包括的な IT セキュリティプログラムサービスは、組織の特定のニーズおよび IT セキュリティプログラムの相対的な成熟度に応じて異なる多くの要素から構成される。IT セキュリティプログラムサービスには、次の要素が含まれる。

・ 組織の制御下にある業務や資産に対するリスクの評価

・ 組織の業務や資産の保護に適切なセキュリティレベルの決定

・組織の制御下にある業務や資産をサポートする各システムに関する現在のセキュリティ計画の改善･維持
・セキュリティインシデントハンドリング手順の作成

・外部レポートの手順の説明など、共通の脆弱性に関連した情報を共有するためのプロセスの作成

・一連の効果的なセキュリティコントロールやテクニックの作成

・セキュリティコントロールを IT 投資に適切に組み入れられるようにするための資金計画や投資管理プロセスの作成

・組織が、利用中のセキュリティコントロール、ポリシー、手順の適切性を効果的に評価し、セキュリティコントロール投資の適切な根拠を示すための一連の IT セキュリティメトリクスの作成

・組織の重要なインフラストラクチャの保護（CIP; Critical Infrastructure Protection）の責務に、その IT セキュリティプログラムを組み入れる程度に関する分析

5.1.2 IT セキュリティポリシー

このガイドの中では、IT セキュリティポリシーは、「IT セキュリティの決定事項のドキュメント」と定義される。IT セキュリティポリシーは、NIST SP 800-12『コンピュータセキュリティ入門: NIST ハンドブック（An Introduction to Computer Security: The NIST Handbook）』で詳細に説明されている。NIST SP 800-12 では、IT セキュリティポリシーを次の 3 つの基本タイプに分類している。

・プログラムポリシー
組織の IT セキュリティプログラムの作成、組織内でのその適用範囲の定義、実施時の責務の割り当て、戦略的方針の確立、および実施するためのリソース割り当てに使用される高度なポリシー

・問題別のポリシー
緊急時対応計画、システムのリスク管理に対する個別の方法の使用、新しい規制または法の適用などの組織の個々の問題に対処する。これらのポリシーは多くの場合、技術や関連要因における変化が生じるたびに頻繁に改訂する必要がある。

・システム固有のポリシー
どのシステムアクションが許可されているかに関して、アクセスコントロールリストを作成したり、ユーザーをトレーニングするなど、個々のシステムに対処する。これらのポリシーは、同じ組織内でもシステムごとに異なることがある。さらに、ここでのポリシーは、組織の電子メール（e メール）やファックスのセキュリティポリシーを巡る経営上の決定といった、システムとはまったく異なる事項に関連することもある。

IT セキュリティポリシーサービス

サービスプロバイダは、組織が、既存および新規に作成されたセキュリティポリシー、標準、ガイドライン、手順の分析を支援することができる。ポリシーを承認する権限は本質的に組織の中核となる機能であり、したがってポリシーの最終的な承認は、組織で行う必要がある。この制約があるため、組織は、内外関わらずサービスプロバイダが支援やサポートだけを提供するように制限しなければならない。包括的な IT セキュリティポリシーサービスは、組織の特定のニーズや IT セキュリティプログラムの相対的な成熟度に応じて異なる多くの要素から構成される。

IT セキュリティポリシーには、次の要素が含まれる。

・ 組織の運用環境の高度な分析

・ 新しく登場した技術

・ ガバナンスプロセス [5]

・ 手順

・ 適用可能なガイダンスと規制に対する遵守性の判断

・ 現在のポリシーと将来の所期のポリシーとの違いを評価する組織またはプログラムのギャップ分析

・ セキュリティプログラムポリシーと詳細な問題固有およびシステム固有のポリシーを統合した組み合わせの作成

・ 作業、リソース、優先順位、所有権を特定する、短期、中期、長期のインプリメント計画の作成

・ IT セキュリティメトリクスの作成

[5] ガバナンスは、戦略およびポリシーの決定をどのように行い、配布し、実施するかに関するものである。ガバナンスは最上位の管理を表し、IT セキュリティプログラムのさまざまなマネージャが実行する、連邦機関またはプログラムの運用の大枠を定義する。ガバナンスは、人員（つまり役割）、組織構造、プロセス、および決定サポートツールから構成され、これらの多くは、ポリシーで定義する必要がある（必ずしも IT セキュリティポリシー

ではない)。

5.1.3 リスク管理

リスク管理は、NIST SP 800-30『情報技術システム用のリスク管理ガイド(Risk Management Guide for Information Technology Systems)』で包括的に説明されている。NIST SP 800-30 では、リスク管理の主要目的を、「防御手段の運用コストと経済的コストのバランスをとり、IT システムおよびデータを保護することによって利益を達成する」ことと記している。

リスク管理サービス

サービスプロバイダは、リスク管理活動をサポートするサービスパッケージを、さまざまに組み合わせて提供している。サービスプロバイダは、組織のリスク管理プログラムをサポートするリスク管理ガイダンスを作成することもできる。サービスプロバイダがリスク管理プログラム全体を管理するが、組織が常に、そのプログラムに対する責任を持つ。サービスプロバイダは、リスクアセスメントを実行したり、リスク移行計画を作成することもできる。成熟し実用的なリスク管理プログラムが、組織で既に使用されている場合、サービスプロバイダはそのプログラムの有効性を監査できる。

5.1.4 IT セキュリティアーキテクチャ

セキュリティアーキテクチャとは、組織の使命およびセキュリティ目標をサポートする IT インフラストラクチャの戦略的な計画と作成のことを意味する。これは、サポートのためにセキュリティ要件分析が行われた後に、セキュリティ設計フェーズで作成されるプロセスである。

IT セキュリティアーキテクチャサービス

組織が新しいセキュリティアーキテクチャの設計をサービスプロバイダに依頼する場合、サービスプロバイダが組織の現在のアーキテクチャの技術やセキュリティベースラインにアクセスできるようにしておかなければならない。サービスプロバイダは、組織がまだベースラインの確立を行っていない場合、ベースラインの確立を行うことができる。ベースラインの確立サービスには、ビジネスニーズ、機能要件、セキュリティ要件、リスクアセスメントのほか、適切なセキュリティコントロールの特定が含まれる。サービスプロバイダは、セキュリティコントロールを特定し、組織のセキュリティポリシーを強化する技術を特定・評価することができる。サービスプロバイダは、組織のニーズを最も満たす技術アーキテクチャを形成するセキュリティソリューションの選択手法を作成することができる。最後に、サービスプロバイダは、セキュリティアーキテクチャを文書化する必要がある。

5.1.5 認証および認定

認定とは、リスクを許容範囲に収めるための所定の技術、管理、運用の防護策が利用されている環境内で、システムが許容されるリスクレベルで運用されていることを、認定担当者が公式に宣言したものである。認定は

通常、技術的セキュリティ評価、リスクアセスメント、緊急時対応計画、署名入りの行動規範によってサポートされる。認証は、認定プロセスをサポートするために行われる IT システムの技術的セキュリティ評価であり、特定の設計やインプリメントが、一連の指定されたセキュリティ要件をどの程度満たしているかを定める。
NIST SP 800-37（草案）『情報技術システムのセキュリティ認証および認定の連邦ガイドライン（Federal Guidelines for the Security Certification and Accreditation of Information Technology Systems）』では、情報システムを認証および認定するために設計された標準的なプロセス、活動および一般作業、管理アプローチを定めている。

認証および認定サービス

認証活動における複雑さと厳格さは、システムの重大度、情報の機密性、システムの危険度、および関心のレベルに応じて異なる。認証と認定（C&A; Certificaion and Accreditation）サービスプロバイダは、認証における全体的な管理や実施を行い、また、最終的に認定者に承認を求めて提出される最終認証パッケージの個々のドキュメントについて準備や評価を行うことができる。

C&A サービス活動には、次のいずれかの作業が含まれる。

・ セキュリティテストおよび評価（ST&E; security test and evaluation）計画とテスト手順の作成

・ ST&E の実施

・ テスト結果の分析とレポート

・ 脆弱性評価の作成/実施

・ 最終的な脆弱性評価レポートの作成

・ 認証者または認定者に対する技術的サポート

5.1.6 IT セキュリティ製品の評価

現在、市販（COTS; commercial off-the-shelf）製品のセキュリティ機能および保証レベルを評価するため、2つの著名なセキュリティテスト、評価プログラムが整えられている。
・ 全米情報保証パートナーシップ[6]（NIAP; National Information Assurance Partnership）共通基準－コモンクライテリア[7]（CC; Common Criteria）評価および検証方法（CCEVS; CC Evaluation and Validation Scheme）
・ NIST 暗号鍵管理モジュール検証プログラム[8]（CMVP; Cryptographic Module Validation Program）
である。

[6] http: //niap.nist.gov を参照。

[7] その他の製品評価サービスには、共通基準保護プロファイルの作成と評価がある。

[8] http: //csrc.nist.gov を参照。

両方のプログラムでは、政府機関が、民間研究機関により実施されたテストや評価プロセスの結果を確証し、セキュリティ標準が正しく一貫して適用されていることを検証している。製品が既存の検証済み製品リストに見つからない場合、他の連邦機関が個々の製品を評価している可能性もある。多くの場合、1 度しか使用されない IT セキュリティ製品のために包括的なセキュリティ評価を実施することは、その製品が組織全体で広く使用されるようにならない限り、費用対効果があるとは言えない。したがって、(このような評価を行う場合、) 評価機関によって検証済み製品リストに挙げられている製品は、選択肢の一つとして見なすべきである。セキュリティ保証に関する追加情報は、NIST SP 800-23『セキュリティ保証と取得/テスト済みおよび評価済み製品の使用に関する連邦組織向けガイドライン (Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products)』で得られる。

IT セキュリティ製品評価サービス

NIAP CCEVS では、国際標準である国際標準化機構/国際電気標準会議 (ISO/IEC) 15408『IT セキュリティ評価の共通基準 (Common Criteria for IT Security Evaluation)』の一連のセキュリティ要件と仕様に対して、さまざまな主要技術領域における商用セキュリティ製品を独自に評価するために、民間部門の評価機関によって構成されるネットワークを活用している。CMVP でも民間部門の独立認定評価機関を使って、FIPS 140-2、『暗号鍵管理モジュールのセキュリティ要件 (Security Requirements for Cryptographic Modules)』および関連の暗号化アルゴリズムの連邦規格に対する暗号鍵管理モジュールの適合試験を中心に行っている。

5.2 運用セキュリティサービス

5.2.1 緊急時対応計画

近年のネットワークコンピューティング環境では、緊急時対応計画の作成において大きな課題に直面している。ネットワークコンピューティングの出現により、これまではローカル問題として取り扱われてきたことの範囲と焦点に変化が生じてきている。緊急時対応計画は、データやインフラストラクチャの損失による影響を軽減するように設計される。緊急時対応計画では、組織の人員が、重要な IT 機能と接続性を迅速で、効果的に、かつ安全に回復できるようにする。緊急時対応計画は、広範なイベントに対応する回復アクションを実行するために必要となる、手順、リソース、作業、情報を定義する。また、適切に作成・試験された緊急時対応計画は、重要なリソースが必要なときに利用できることを保証し、緊急事態における組織の業務継続をサポートする。この計画は成長していくドキュメントであり、システムの構成および運用における変更を反映するように、定期的に更新する必要がある。緊急時対応計画の追加情報は、NIST SP 800-34『情報技術システム用の緊急時対応計画ガイド (Contingency Planning Guide for Information Technology Systems)』に記されている。このガイドでは、緊急事態後に重要な IT サービスを維持し回復するためのさまざまな緊急時対応計画が説明されている。

緊急時対応計画では、少なくとも、サポート情報、通知/活性化、回復、再構築、参考資料の 5 つの主要コンポーネントを取り扱う必要がある。

・**サポート情報** - 計画作業の概要やコンセプトの紹介

・**通知/活性化** - 通知手順、損害アセスメント、計画の活性化などの項目

・**回復** - 一連の回復活動、回復手順などの項目

・**再構築** - 一連の回復活動、システムのテスト、作業の終了などの項目

・**計画の参考資料** - 契約情報、設備リスト、サービス契約、他の関連する緊急時対応計画などの項目

緊急時対応計画サービス

サービスプロバイダは、緊急時対応計画ライフサイクルのさまざまなフェーズに応じたサービスを提供している。緊急時対応計画サービスを外部委託するかどうか検討する場合、組織は、サービス提供の明細（緊急時対応計画の作成、更新とテスト、実行など）ごとに費用対効果分析を行うことができる。

・**作成**

サービスプロバイダは組織の緊急時対応計画を作成できる。このサービスは、多数の機能領域から情報を収集する必要がある。ベンダーは最初にビジネスインパクト評価（BIA; business impact assessment）を実施して、システムの内部と外部の依存関係、許容可能な停止期間、回復優先順位を判断する必要がある。BIA は、緊急時対応計画の中核を構成する具体的な回復戦略や手順を作成するための基礎となる。

・**更新とテスト**

緊急時対応計画は成長していくドキュメントなので、必要に応じて計画を更新することは、緊急時対応計画を成功させる上で重要である。計画を作成した同じサービスプロバイダに更新とテストを任せるのが一般的である。システムに組み込まれた人員、手順、資産、またはその他のリソースが変更されたとき、計画の更新を行う必要がある。

サービスプロバイダはまた、計画が必要になる前に、その計画を必ずテストする。このテストは、計画のすべての側面を網羅したリハーサルまたはシミュレーションドリルや完全操業演習である。このテスト演習の結果は、緊急時対応計画で文書化され、管理職によって討議される。この結果により、緊急時対応計画手順の効果が判断され、すべての欠陥が明らかになる。予想外のイベントによって運用が中断されたときに、より早期に回復でき、人員が期待されている行動を認識できるように、スタッフは緊急事態関連の責務に対する訓練を受けなければならない。

・ **実行**

緊急時対応計画の実行フェーズに対する責任は組織にあるが、サービスプロバイダは実行フェーズにおける特定の側面をサポートすることができる。たとえば、サービスプロバイダがシステムやデータリカバリ用のホットサイト（本番と平行して稼動し続ける予備サイト）またはモバイルサイトを準備しているため、組織はデータリカバリを外部に委託することもある。プロバイダは、計画とその中での役割について、組織の人員に対して定期的に訓練を行うことができる。

5.2.2 インシデントハンドリング

IT セキュリティインシデントとは、セキュリティメカニズムの障害や、これらのメカニズムの失敗またはセキュリティ侵害によって引き起こされるコンピュータシステムまたはネットワークでの有害事象のことである。インシデントハンドリング機能は、通常処理での混乱に対して迅速かつ効果的に反応できる能力を提供する。準備、識別、封じ込め、除去、回復、フォローアップという、インシデントレスポンスの 6 つのフェーズの効果的なプロセスと手順を作成し定めることにより、効果的なインシデントハンドリングが実現する。このインシデントハンドリングプロセスは、組織が重要な証拠の適切な取り扱いを確実に行うために必要となる法的処置サービスとも整合性が取れている必要がある。

インシデントハンドリングサービス

インシデントハンドリング機能は、24 時間 365 日利用可能でなければならない。サービスプロバイダは、次に挙げるサービスの 1 つまたは組み合わせを提供できる。

インシデントハンドリングサービスには、次のサービスが含まれる。

・ インシデントハンドリングプログラムの作成

・ システム構成プロファイルの作成と管理

・ 法的処置機能の提供

・ インシデントハンドリング手順のテストと更新

・ インシデントハンドリング手順の管理と実行

インシデントハンドリング手順サービスには、次のサービスが含まれる。

・ 影響を受けたシステムやプラットフォームの隔離

・障害システムの選別

・レポートアセスメント（ログファイルの解釈、優先順位の決定、分析）

・識別/検証（インシデントの性質と範囲の特定）
・分類（損なわれた情報、システム、インシデントの機密性の特定）

・内部と外部の調整（情報適格性に応じて、該当する内部や外部の関係者に通知し調整する）

・解決

・技術的支援（発生した原因や適切に機能しなくなった項目など、イベントの詳細な分析の提供）

・除去（インシデントの原因と影響の消去）

・回復（通常運用へのシステムの復帰）

・予防サポート

・IDS の運用、保守、監視（IDS に直接結びついたインシデントレスポンス）

・トレーニング

・インシデント後のコンサルティング

・第三者分析、除去と回復の検証、是正と移行処置、レポート

5.2.3 テスト

情報システムやネットワークにおけるセキュリティ状態のテストは、システムを保護する上で重要なコンポーネントである。しかし、テストに関する完全かつ徹底した説明は、このドキュメントの範囲を超えているので行わない [9]。テストは、セキュリティ手段と手順が目的どおりに機能していることを確認できる唯一の方法である。テストはまた、これまで不明であった弱点や脆弱性を識別する場合にも役立つ。すべてのテスト活動は、手動であれ自動であれ、人間の関与が必要になり、したがってサービスとして提供される。

テストの結果は次のように使用できる。

・ あらゆる是正処置の基準点として

---

[9] セキュリティテストの各カテゴリおよびタイプに関する詳細については、NIST 特別刊行物 800-42『ネットワークセキュリティテストのガイドライン（Guideline on Network Security Testing）』を参照されたい。

・組織の進展を把握するためのベンチマークツールとして

・システムセキュリティ要件のインプリメントの評価のため

・費用便益分析のため

・リスクアセスメント、機能要件分析、C&A、パフォーマンス向上作業などの、より上位のライフサイクル活動への入力値として

テストのカテゴリには、次の項目が含まれる。

・ネットワークマッピング

・ログレビュー

・脆弱性スキャニング

・完全性チェッカー

・侵入テスト

・ウィルス検知

・ST&E

・ウォーダイアリング

・パスワード解析

テストサービス

非常に専門的で技術的な性質のため、テストは、多くの場合、外部サービスプロバイダ向きと考えられているセキュリティ活動の 1 つである。ただし、非常に立ち入った測定になるので、サービスプロバイダが有能であり、組織にとって信頼できるということが重要になる。テストは、個別の活動として行うことも、リスク管理プログラムの一部としてリスクアセスメントの下で行うこともできる。サービスプロバイダは、管理職からの明確で明瞭な指示（書面による「提携規則」）、一連のインターネットプロトコル（IP）アドレス、明確に定められたテスト範囲を必要とするほか、計画とアセスメント、要件分析、テストの実行、分析結果とドキュメントに必要なものについてのデータも必要とする。

5.2.4 トレーニング

トレーニングは、稼動しているシステムのセキュリティ状態を維持する上で最も重要なコンポーネントの1つである。どのような組織の IT システムの保護においても、熟練し、知識が豊富で、あらゆるレベルの訓練を受けた人員がいなければ達成できない。セキュリティトレーニングと教育は、ビジネスを遂行する上で不可欠な継続的な取り組みと考える必要がある。絶えず進化する技術を取り扱う場合、特にセキュリティの領域においては、教育は終わることのない変化と進歩に対応していく必要がある。マネージャは、情報に基づいた判断と投資を行い、許容可能なレベルまでリスクを適切に緩和するために、セキュリティプログラムおよびコントロールの現状を理解しなければならない。IT システムのすべてのユーザーは、情報と IT リソースの保護に対する責任を認識しておく必要がある。

NIST SP 800-16『情報技術セキュリティトレーニング要件（Information Technology Security Training Requirements）』の IT セキュリティ学習の段階は、図 5-1 に示したように、IT セキュリティの認識、トレーニング、および教育プログラムの指導ガイダンスを示している。このモデルは、OMB Circular A-130 などの複数の連邦規制の要件に基づいて作成されている。

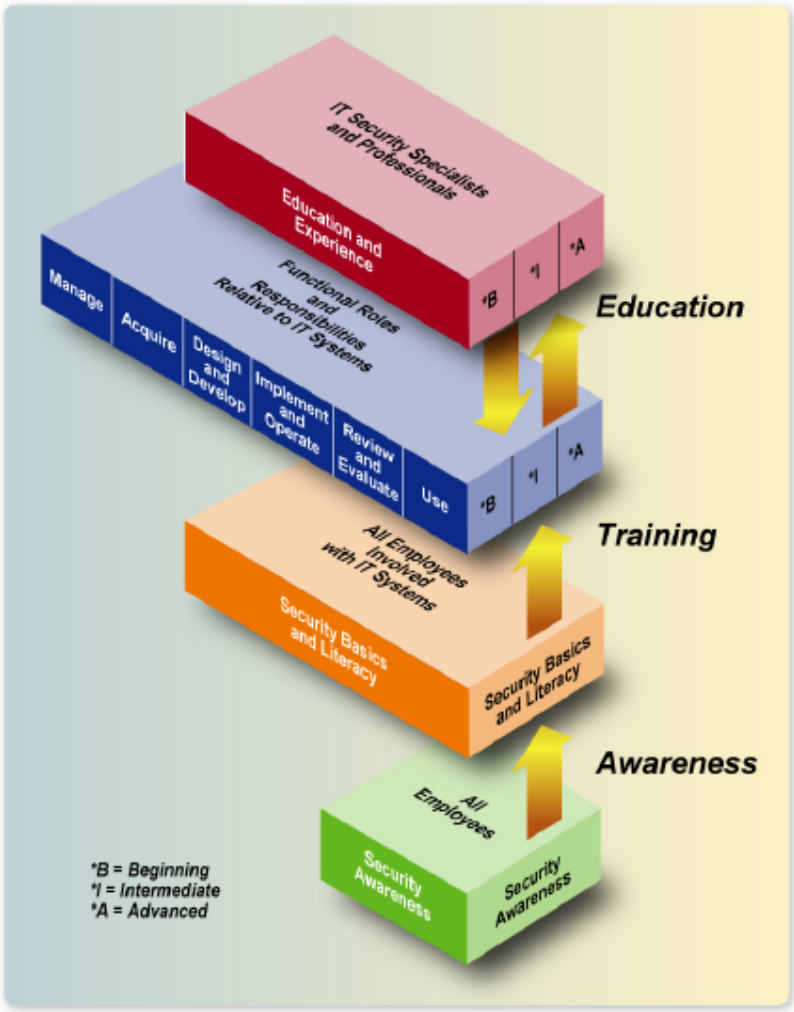

図 5-1 情報技術セキュリティ学習の段階

このモデルは、次の要素を統合した 3 次元配列を図示している。

・**3 つのタイプのトレーニング** – 意識向上、トレーニング、教育

・**6 つのセキュリティの機能的役割** - 管理、取得、設計と作成、インプリメントと運用、レビューと評価、使用

・**3 レベルのトレーニング** - 初級、中級、上級

NIST SP 800-50『情報技術セキュリティの意識向上およびトレーニングプログラムの構築（Building an Information Technology Security Awareness and Training Program）』では、組織の IT セキュリティプログラム内で、意識向上とトレーニングプログラムを設計、作成、実施、保守するための詳細なガイダンスを提供している。このガイドでは、NIST SP 800-16 に基づいて、IT セキュリティトレーニングと意識向上プログラムの設計･実施における次の 4 つのステップについて説明する。

・意識向上とトレーニングプログラムの設計

・意識向上とトレーニング資料の作成

・プログラムの実施

・実施後

トレーニングサービス

IT セキュリティトレーニングサービスプロバイダは、「総合的な」セキュリティ意識向上やトレーニングプログラムをサポートする、広範なサービスを提供できる。プロバイダは組織に代わってプログラムの設計、作成、実施、および保守を行えるが、組織のトレーニングおよび意識向上プログラムの特定の要素の支援をすることもできる。サービスプロバイダは、次のサービスを提供できる。

・プログラムレベルのサポート

・コースレベルのサポート

・トレーニングサポートサービス

5.3 技術的セキュリティサービス

5.3.1 ファイアウォール

ファイアウォールは、故意または故意でない侵入からネットワークを守るために、ネットワークを防御するアプリケーションをインストールしたデバイスである。ファイアウォールは、2 つのネットワーク（通常はプライベートネットワークとインターネットなどのパブリックネットワーク）間の接続点またはゲートウェイに置かれる。「ファイアウォール」という用語は、ファイアウォールが、一つのネットワークを複数の物理的サブネットワークに分割することによって、あるサブネットから別のサブネットへ拡大する可能性のある被害を抑えるプロセスが、自動車における防火ドアまたは防火壁と同じように機能していることに由来している。

ファイアウォールサービス

サービスプロバイダは、次のファイアウォール機能の一部またはすべてを実行できる。

・ 単一または複数のファイアウォールを組み込んだファイアウォールソリューションを設計する。

・ 新しいネットワークおよび既存のネットワークへファイアウォールの導入および統合する。

・ インシデントレスポンスまたは侵入検知システム（IDS）などの他の技術的コントロールとの統合および可用性を確保するためにファイアウォールサービスを監視する。

・ 定期的なアップグレードなど、組織のファイアウォールを管理する。

組織は、信頼できる自社製品シリーズを揃えた特定のサービスプロバイダを選択することも、外部ベンダーの製品とコンポーネントを使用しながら幅広いセキュリティサービスの提供を専門とした全般的なサービスプロバイダを選択することもできる。

5.3.2 侵入検知

侵入とは、リソースの完全性、機密性、または可用性を損ねようとする一連の行動のことである。侵入検知とは、ネットワークまたは選択したホスト上に配備されたパッシブな（受身的な）セキュリティ活動のことである。IDS に組み込まれるデバイスは、侵入を検知し、情報を中央管理コンソールに提供するために使用される。セキュリティスタッフはこの情報を調べて、深刻なセキュリティ侵害が行われたかどうかを判断する。IDS は次のようなさまざまな機能を実行する。

・ ユーザーとシステムの活動の監視

・ システム構成と脆弱性の監査
・ 重要なシステムおよびデータファイルの完全性の評価

・ 既知の攻撃を反映した活動パターンの認識

・ 異常な活動パターンに対する統計分析の実行

・ ポリシー違反を示すユーザー活動を意識した、オペレーティングシステム監査証跡管理の提供

・ カスタマイズレポートの提供

この継続的な監視および監査活動は、セキュリティアーキテクチャ全体にとって不可欠な要素である。IDS は通常、考えられる攻撃の具体的な兆候を識別し、防御方法を再検討させることによって、情報セキュリティインフラストラクチャの各部分の完全性を改善する。これらは多くの場合、ユーザーの活動についてネットワークに入ってきた時点から出ていく時点まで追跡することができる。IDS は、特定のタイプの攻撃を認識でき、適切なスタッフに警告を発することができる（このように設定されている場合）。

侵入検知サービス

侵入検知が効果を発揮するには、IDS でその検出事項を照合するための、攻撃シグニチャの豊富な知識ベースが必要になる。脅威と脆弱性は本質的に静的なものではなく、絶えず変化し進化していく。攻撃シグニチャデータベースは、IDS が最新の脅威を検知できるように、頻繁に更新する必要がある。サービスプロバイダは、単一の IDS 製品用データベースの管理費用を複数の顧客の間で分担できるので、少ないコストでこれを達成できる。IDS を運用し管理するには、高度な専門知識が必要になる。IDS やサービスプロバイダでは解決できない侵入が発生した場合や、サービスプロバイダによる問題解決が契約に含まれていない場合、サービスプロバイダは組織に連絡し、続いて組織がその事態の解決を図る。

5.3.3 公開鍵基盤

近代のセキュリティアーキテクチャでは、広範に分散した環境の中で必要とされる情報を配信し、且つ保護している。こうした環境では、ユーザー、リソース、利害関係者は、そのすべてが違った時間の違った場所に存在する可能性がある[10]。PKI では、こうしたセキュリティのニーズに対処し、拡張性が高く、分散している PKI の特性を活用したアプローチ（製品、サービス、設備、ポリシー、手順、契約、人員から構成まで）を取っている。PKI によって、組織は電子的に以下の点を保証しながらビジネスを遂行することができる。

[10] PKI に関するこの項は、NIST SP 800-32『公開鍵技術および連邦政府の PKI 入門（Introduction to Public Key Technology and the Federal PKI）』および NIST SP 800-25『連邦機関での電子署名および本人確認に対する公開鍵技術の使用（Federal Agency Use of Public Key Technology for Digital Signatures and Authentication）』か

ら大幅に引用している。

・トランザクションの送信側であると識別された人員またはプロセスが、本当に発信元であること（否認防止）

・トランザクションを受信した人またはプロセスが目的とする受信側であること（識別と認証）

・データの完全性が損なわれていないこと（完全性）

上記の 3 つのサービスに加え、PKI は鍵回復と権限/承認の 2 つのサービスも実現することができる。

・鍵回復 ： 組織は従業員が暗号化したデータを回復できなければならないが、暗号化鍵が利用できない場合、この鍵を回復しなければデータを回復できない[11]。

・権限/承認 ： 証明書はユーザーの身元を保証し、また、ユーザーが認められている権限を指定できる。

公開鍵基盤の機能要素には、認証局（CA; certification authority）、登録局（RA; registration authority）、リポジトリ、アーカイブがある。PKI の特性は、非常に技術的なセキュリティコントロールであるということである。次の NIST 刊行物では、さらに詳しく PKI について説明している。

・NIST SP 800-32『公開鍵技術および連邦政府の PKI 入門（Introduction to Public Key Technology and the Federal PKI）』

・NIST SP 800-25『連邦機関での電子署名および本人確認に対する公開鍵技術の使用（Federal Agency Use of Public Key Technology for Digital Signatures and Authentication）』

PKI サービス

PKI の設計、開発、導入、保守は、複雑な技術的課題であり、以下に挙げる多くの要素を含む。[12]

・相互運用性

・拡張性

・高額なコスト（PKI の導入とソフトウェアアプリケーションの利用）

・複雑なポリシー作成

[11] 鍵回復の原因はさまざまであり、暗号化したファイルを復号化するパスワードを従業員が忘れた場合、情報

を暗号化した従業員が死去した場合、誰かが捜査当局者から犯罪活動を隠そうとした場合などがある。

[12] GAO レポート 01-277『公開鍵基盤技術の導入における進歩と残存する問題（Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology）』、2001 年 2 月

・ 難解で理解しにくい技術に対するトレーニングの問題

PKI サービスはさまざまな形でパッケージ化することができる。全体の PKI プロセスをサービスプロバイダが実行することも、セキュリティプロバイダが内部で PKI を管理することも、PKI 要素を部分的にプロバイダが実行することもできる（ハイブリッド）。次のリストには、サービスプロバイダが実行できる PKI の要素 [13] の例を示している。

表 5-2 PKI サービス要素の例

証明書検証	アプリケーションがアクセスしようとしている人の本人確認を要求したときに、随時、証明書を発行したサービスプロバイダとともに証明書を検証チェックする。
証明書の発行	身元証明がサービスプロバイダによって正しく行われた、または組織によって保証された場合に、利用者に証明書を発行する。
補完的 PKI サービス	PKI 関連のプログラミング、システム統合、テレコミュニケーションインターフェースサポート
技術の更新	新しいアルゴリズム、フォーマット、技術、メカニズム、メディアの導入
アドホックデータの収集、分析、配布	PKI サービスに関連したその場限りのデータ収集、分析、配布サービス
ハードウェアトークン	鍵ペアを生成し、秘密鍵を保管するハードウェアトークン

[13] http: //hydra.gsa.gov/aces/order.pdf、2001 年 9 月 5 日

付録 A - 参考文献

NIST Special Publication (SP) 800-12, *An Introduction to Computer Security: The NIST Computer Security Handbook*, February 7, 1996.
NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, April 1998.
NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*, December 1998.
NIST SP 800-23, *Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*, August 2000.
NIST SP 800-25, *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*, October 2000.
NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, January 2002.
NIST SP 800-31, *Intrusion Detection Systems*, November 2001.
NIST SP 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, February 2001.
NIST SP 800-33, *Underlying Technical Models for Information Technology Security*, December 2001.
NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002.
NIST SP 800-36, *Guide to Selecting Information Technology Security Products*, October 2003.
NIST SP 800-37, *Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems*, draft.
NIST SP 800-42, *Guideline on Network Security Testing*, October 2003.
NIST SP 800-48, *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*, November 2002
NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003.
NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, draft
NIST SP 800-55, *Security Metrics Guide for Information Technology Systems*, July 2003.
NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle*, October 2003.
NIST Publication, *Introduction to Public Key Introduction to Public Key Technology and the Federal Technology and the Federal PKI*, February 26, 2001.
A-1
NIST Interagency Report (NISTIR) 4749, *Sample Statements of Work for Federal Computer Security Services: For Use In House or Contracting Out*, June 26, 1992.
FIPS 140-2, *Security Requirements for Cryptographic Modules*, June 2001.
Federal Information Security Management Act of 2002, 44 U.S.C. Chapter 35, Subchapter III. 2002.
Federal Financial Institutions Examination Council (FFIEC), *Guidance on the Risk Management of Outsourced Technology Services*, SR Letter 00–17, November 2000.
Gartner Research, *The Price of Information Security* Gartner Group, June 1, 2001.
General Service Administration, Information System Security Managers and Information System Security

Officers Training, September 2000.
Lessons Learned from the Federal Computer Incident Response Capability (FEDCIRC) Pilot: http://csrc.nist.gov/topics/incidentNIST/sanspaper.htm, August 1998.
MIS Training Institute, *Auditing your Information Security Program*, Class Notes (Personnel Security), September 2003.
OMB Circular A-11, *Planning, Budgeting, and Acquisition of Capital Assets*, June 2002.
OMB Circular A-76, *Performance of Commercial Activities*, May 2003.
OMB Circular A-130, *Management of Information Resources*, November 2000.

Web Sites

http://csrc.nist.gov
http://niap.nist.gov
http://www.cert.org/security-improvement/modules/omss/index.html

付録 B - 略称リスト

BIA	ビジネス影響アセスメント (Business Impact Assessment)
C&A	認証および認定 (Certification and Accreditation)
CA	認証局 (Certification Authority)
CIO	最高情報責任者 (Chief Information Officer)
CIP	重要なインフラストラクチャの保護 (Critical Infrastructure Protection)
COTR	契約担当者の技術代表者 (Contracting Officer's Technical Representative)
e-mail	電子メール (Electronic Mail)
FIPS	連邦情報処理規格 (Federal Information Processing Standard)
FISMA	連邦情報セキュリティ管理法 (Federal Information Security Management Act)
IDS	侵入検知システム (Intrusion Detection System)
IP	インターネットプロトコル (Internet Protocol)
ISP	インターネットサービスプロバイダ (Internet Service Provider)
IT	情報技術 (Information Technology)
MOA	同意覚書 (Memorandum of Agreement)
MOU	了解事項覚書 (Memorandum of Understanding)
NIST	米国立標準技術研究所 (National Institute of Standards and Technology)
NISTIR	NIST 連邦機関相互レポート (NIST Interagency Report)
OMB	行政管理予算局 (Office of Management and Budget)
OPM	人事管理局 (Office of Personnel Management)
PKI	公開鍵基盤 (Public Key Infrastructure)
PUB	刊行物 (Publication)
RA	登録局 (Registration Authority)
RFP	提案要求書 (Request for Proposal)
SDLC	システム開発のライフサイクル (System Development Life Cycle)
SLA	サービスレベル契約 (Service Level Agreement)
SOW	作業別計算書 (Statement of Work)
ST&E	セキュリティテストおよび評価 (Security Test and Evaluation)
TCO	総所有コスト (Total Cost of Ownership)
U.S.C.	合衆国法律集 (United States Code)

付録 C - サービス契約の概要

サービス契約は、サービスのタイプと範囲、サービスアレンジメント、組織のタイプに応じて、多種多様な形態を取りうる。この付録に収録したサービス契約の概要例は、もっぱらガイドとして利用されることを想定している。個々の書式、条項、および条件は、各組織ごとに異なる。IT セキュリティマネージャは、サービスプロバイダとの交渉が終了してはじめて、そのサービス契約を作成する必要があるが、組織の法律顧問や契約専門家と相談しながら進めることが最も重要である。

1. 序 - 目的、参加者、およびサービスを紹介する。

   1.1. 目的
   1.2. 参加者
   1.3. サービスの全般的な説明

2. サービス環境 - 実際の場所から、使用するハードウェアおよびソフトウェア、サービスプロバイダが遵守する必要のあるポリシーおよび手順まで、組織がサービスを実行する環境について説明する。

   2.1. 機器
   2.2. 施設
   2.3. 事業体および場所
   2.4. ポリシー、手順、および標準
   2.5. 契約およびライセンス

3. 役割と責任 - 主要参加者全員の役割と責任を記述する。サービスプロバイダの責任は、サービス業務だけでなく、サービスの文書化、活動のレポート、およびサポート機能についても明記する必要がある（たとえば、新しいサービスによって苦情電話が起きた場合、誰がどのようにこれらの電話に対処するのかを、サービス契約で明記する必要がある）。

   3.1. サービスプロバイダの責任

      3.1.1. サービス業務
      3.1.2. 文書化
      3.1.3. サービスサポート
      3.1.4. レポート要件

   3.2. クライアント組織の責任

4. サービスレベル - メトリクス、サービスレベル、およびサービスレベルの評価方法を特定する。メトリクス作

成の詳しいガイダンスについては、NIST 特別刊行物 800-55『情報技術システムのセキュリティメトリクスガイド（Security Metrics Guide for Information Technology Systems）』を参照すると、メトリクスの作成および収集に関するガイダンスのほか、IT セキュリティメトリクス例が得られる。組織は、許容可能なレベルから、中間レベル、目標レベルまでサービスレベルを明記することも、さまざまなユーザーグループまたはスケジュール時間ごとに異なるサービスレベルを設定することもできる。後者の場合、それぞれのサービスレベルを明記する必要がある。

4.1. 目標
4.2. メトリクス
4.3. サービスレベル
4.4. サービスレベルアセスメント

5. 条件および調停 - サービスレベルの実施コストおよび期間と、前項で明記された役割および責任を規定するほか、サービス契約での紛争の解決、不履行の対処、および要件変更に伴う契約の修正を行うプロセスを規定する。

5.1. コスト
5.2. 実施期間
5.3. 紛争の解決
5.4. 不履行に対する是正措置
5.5. 契約の保守

付録 D - 取得文言の例

D.1 序

この付録では、このドキュメントで挙げたサービスに対応する情報技術（IT）セキュリティサービスの作業別計算書（SOW）、または他の形式のサービスプロバイダ契約の作成に適した文言[14]を示す。この文言は優れたITセキュリティ管理に代わるものではないが、組織のスタッフおよび政府のサービスプロバイダは、規定された各活動について一般的な理解を促す土台としてこの付録を使用できる。文言例は、整合性と品質の高い IT セキュリティサービスをより簡単に実現するために役立つ。この記述は、サービスの契約を行う場合、または組織内からサービスを調達する場合に適用される。繰り返しになるが、取得担当者と法律顧問は複雑で難解な専門領域における専門家であるので、彼らと綿密な相談やガイダンスを実施することが望ましい。

D.2 取得文言の例

ここで示す文言はサンプルであり、「定型文」として用意されたものではない。それぞれの組織は、特有のニーズを分析し、機能、リソース、スケジュール要件、制約を判断する必要がある。この文言を適切に修正すれば、さまざまなレベルの組織（部局、連邦機関、事務局、地域局、支局、出張所）で使用できる。その他の取得文言は、NIST 特別刊行物（SP）800-64『情報システム開発のライフサイクルにおけるセキュリティの考慮事項（Security Considerations in the Information System Development Life Cycle）』を参照されたい。

このドキュメントでは、不等記号（<>）を使用して、組織が入力する情報を示している。この部分に適切な情報を入力しやすくするために、一般的な用語や説明を使用している（組織名など）。文言を修正または改善する担当者への指示は注記として示され、[注]と記されている。

この付録の文言を修正する担当者にとって、他の NIST 刊行物が大いに役立つ。これらの作業を実行する担当者にとっても、他の NIST 特別刊行物が有用である。

このガイドで説明してきたサービスの（すべてではないが）多くが、この付録に登場している。多くの場合、この付録で記述される文言は、他のセキュリティサービスに適合するように修正できる。文言内で述べられている成果物はサンプルであり、組織の特定のニーズに適合するように修正する必要がある。

このガイドで説明してきたサービスに関する取得文言以外にも、IT セキュリティ製品や一般的な IT セキュリティサービス契約管理を評価するためのサービスに関する取得文言も収録している。

---

[14] この項は、NISTIR 4749『連邦政府のコンピュータセキュリティサービス用の作業別計算書サンプル: 内部調達または外部委託（Sample Statements of Work for Federal Computer Security Services: For Use In House or Contracting Out）』（1991 年 12 月）に基づいている。付録 D の文言は、当初、SOW の文言として作成された。

内部の MOA で使用する場合は、修正が必要である。

D.3 管理セキュリティサービス

D.3.1 IT セキュリティプログラムの開発

D.3.1.1 現在の IT セキュリティ状況のレビュー

契約者は、<IT セキュリティ担当者、最高情報責任者（CIO）、プログラムマネージャ、または他の指定要因>の支援を受け、連邦情報技術セキュリティ評価フレームワークをガイドとして使用して、現在の IT セキュリティプログラムの状況を判断する。契約者は、どの IT セキュリティプログラム要素およびドキュメントが存在しているかを判断する。存在している要素およびドキュメントに対し、契約者はレビューを行う。契約者は、どの要素またはドキュメントが存在しているかに注目する。このレビューでは、次の観点からドキュメントを検討する。

・ アプリケーションシステムの検定、レビュー、リスク分析

・ IT 設備のレビュー

・ 技術的ソフトウェア評価

・ 緊急時と障害回復の計画およびテスト

・ 人的セキュリティ

・ IT セキュリティ意識向上とトレーニング

・ セキュリティ管理および調整契約者は、<組織名>の IT セキュリティプログラムを評価するために、およそ<N>回、現地設置場所に出向くものとする。

契約者はまた、次の点もレビューする。

・ 既存のポリシーと手順

・ 適用可能な連邦規制

・ 組織のミッションステートメント（使命宣言書）

・ 組織の情報管理リソースポリシーステートメント

・IT セキュリティの目標、ポリシー、手順、標準

・IT セキュリティとプライバシーの計画

・その他の関連ドキュメント

契約者は、存在しない要素またはドキュメントを含め、この作業の所見を文書化したレポートを用意する。契約者は、契約担当者の技術代表者（COTR）に、現在の IT セキュリティ状況のレポートを提出する。

D.3.1.2 IT セキュリティプログラム用フレームワークの作成

契約者は、IT セキュリティプログラム用のフレームワークを作成する。このフレームワークには、IT セキュリティポリシーステートメントの草案が含まれる。フレームワークは、少なくとも次の要素を含めて、主要プログラム要素を特定する。

・リスク管理

・セキュリティコントロールのレビュー

・ライフサイクル

・承認を与える処理（認証と認定）

・システムセキュリティ計画

・人的セキュリティ

・物理的および環境的保護

・緊急時対応計画

・ハードウェアとシステムソフトウェアの保守

・生産、入力/出力コントロール

・データの完全性

・文書化

・セキュリティの意識向上、トレーニング、教育

・インシデントレスポンス能力

・識別と認証

・論理アクセスコントロール

・監査証跡

レポートでは、スタッフ、予算、機器など、利用可能または必要となるリソースを特定する。

契約者は、<組織名>IT セキュリティ目標およびポリシーステートメントの草案を<作成/改訂>する。この目標には、連邦規制および組織のミッションを反映させる。ポリシーには、IT セキュリティ目標を反映させる。

契約者は、IT セキュリティプログラム構造レポートとポリシーステートメントを COTR に提出する。

D.3.1.3 管理手順およびコントロールプログラムアセスメントのレビュー

契約者は、セキュリティをサポートする管理手順を検証する。これには、組織のガバナンス構造、権威者と責任者、および機能分担の分析が含まれる。契約者はまた、各領域（全般、物理的、データ、システム、アプリケーションソフトウェア）においてレビューする管理コントロールのリストを提供する。このリストには少なくとも次の項目を含める。

・書面によるポリシーと運用手順

・エラーや不一致のレポーティング手順

・適切な義務の分担を含む組織と報告階層

・セキュリティ意識向上とトレーニングの作成と実施

・契約者は、管理手順およびコントロールレポートを COTR に提出する。

D.3.1.4 プログラムアセスメントレポートの準備

契約者は、プログラムアセスメントレポートを作成する。ここでは、セキュリティプログラム全体が、適切な連

邦、州、地域の法およびポリシーのほか、内部ポリシーおよび手順を遵守しているかどうかについて要約する。このレポートでは、修正や救済を必要とする主要なセキュリティの弱点を詳述する。レビューする領域ごとの要約、所見、セキュリティにおける弱点の影響（存在する場合）、および管理職が採用できる推奨アクション（存在する場合）を提供する。このレポートはまた、より詳細な分析を必要とする領域も特定する。契約者は、プログラムアセスメントレポートを COTR に提出する。

D.3.2 IT セキュリティポリシーの作成とレビュー

D.3.2.1 IT セキュリティプログラムの詳細と戦略の作成

契約者は、次の項目を含めて、一連の IT セキュリティプログラムのトピックまたは戦略、あるいはその両方を作成する。

・ セキュリティポリシーと計画

・ リスク管理

・ セキュリティコントロール

・ 行動規範

・ ライフサイクル管理

・ 認証および認定

・ 人的、物理的、環境セキュリティ

・ コンピュータサポートと運用

・ 緊急時対応計画

・ トレーニング

・ インシデントレスポンス

・ アクセスコントロール

・ 監査証跡

・ ログファイル

それぞれの戦略には次の項目を含める。

・ 権威者と責任者を含む職位記述書草案

・ スタッフ配置理由

・ リソース要件見積もり

・ 予算見積もり

・ マイルストーン（通過的達成目標）とそのスケジュール

それぞれの戦略ごとに、契約者は、ポリシー、手順、標準の草稿を作成するか、既存のものを特定する。契約者はまた、上記の要素を組み込んだ戦略ごとにドキュメントを用意する。

D.3.2.2 人的セキュリティ戦略の作成

契約者は、ポリシー、手順、メカニズムを取り上げた人的セキュリティ戦略を作成する。契約者は、<組織名>の人事部や情報セキュリティ部と連携する。これは、作成された戦略が、職位機密性分類、人的セキュリティ選別、情報機密性について、<組織名>のポリシーや手順と同調するために行われる。契約者は、コンピュータシステムへのアクセス、システムの設計･開発･保守、あるいはハードコピーやコンピュータ処理された形式での機密情報の取り扱いなどの義務を有するすべての従業員と契約者に、この戦略が確実に適用されるようにする、契約者は、人的セキュリティ戦略を COTR に提出する。

D.3.2.3 システムセキュリティ戦略の作成

契約者は、情報を処理する上で必要となるコントロールを取り扱うシステムセキュリティ戦略を作成する。重要な考慮事項は、システムの不適切な運用や作為的な操作から生じる損失･損害のリスクとその規模である。

セキュリティおよびコントロール目標をこの戦略に含める。

契約者はまた、該当する連邦法、規制、OMB 実施指示に準拠した IT セキュリティおよびプライバシー計画を準備するためのガイダンスを作成する。契約者は、システムセキュリティ戦略を COTR に提出する。

D.3.2.4 IT 物理的セキュリティ戦略の作成

契約者は、リスクアセスメントの実行と、<組織名>の IT システムの緊急時対応計画の確保を含んだ IT 物理的セキュリティ戦略を作成する。この戦略では、<組織名>独自の環境、ネットワーク、情報機密性のニーズを取り扱う。この戦略には、重要なシステムとアプリケーションの特定が含まれる。戦略ではまた、リスクアセスメントの方法やテクニック、バックアップ戦略を取り扱う。

契約者は、IT 物理的セキュリティ戦略を COTR に提出する。

D.3.2.5 物理的手順およびコントロールのレビュー

契約者は、人的、施設、IT 資産の物理的セキュリティ手順とコントロールをレビューする。契約者は、用意された物理的セキュリティ手順とコントロールのリストを作成する。このリストには、各領域へのアクセスに対する認可を含み、少なくとも次の項目を含む。

・ 物理的アクセスコントロールとその効果

・ 施錠と入館手順

・ 妥当かつ適切な保守のための空調設備、無停電電源装置、消火装置、ポンプ装置

・ ハードウェアやソフトウェアの盗難、その他の人間と機械に関係する脅威に対する保護

・ データとソフトウェアのオフサイトストレージに関する手順

・ 洪水、火災、地震、台風、竜巻などの自然災害やその他の自然に基づく施設への脅威に対する対応手順

・ パーソナルコンピュータの使用およびソフトウェア著作権使用許諾のポリシー

契約者は、物理的セキュリティ手順とコントロールレポートを COTR に提出する。

D.3.2.6 IT セキュリティのレビュー

契約者は、機密を要し重要な IT システムやデータファイルを吟味する。契約者は、データセキュリティテクニックと方法をレビューするためのリストを作成する。これには次の項目が含まれる。

・ アクセスコントロール、完全性コントロール、バックアップ手順

・ 機密データを取り扱う手順とインプリメント

・ 既存のプライバシーポリシーとその保護方法

・ 情報アクセス（承認とインプリメント）

・ 開発中のシステムとシステムを本番環境に移行する方法

・ 情報やシステムの管理に対して明文化されたユーザーの責任

契約者は、データセキュリティテクニックと方法レポートを COTR に提出する。

D.3.2.7 人的セキュリティのレビュー

契約者は、ポジションに関連した情報の扱い区分(クラシフィケーション)、人に対するセキュリティスクリーニング、情報の機密性、セキュリティトレーニングおよび意識向上などの要素に関する、連邦および<組織名>の人事的セキュリティポリシーや手順に対する準拠性を評価するレポートを作成する。このレポートでは、ポリシーや手順が、機密データにアクセスできる全てのポジションにいる人員を扱っているかどうかを検討する。契約者は、人的セキュリティレポートを COTR に提出する。

D.3.3 リスク管理

D.3.3.1 リスクアセスメントとセキュリティ計画のレビュー

契約者は、この SOW で取り上げる機密を要するシステムの適切な<組織名>のリスクアセスメントと<組織名>のセキュリティ計画をレビューする。契約者は、このレビューを文書化したレポートを用意する。レポートでは、計画で概説するコントロールや手順、基準となる規制や通達要件を取り上げる。契約者は、<組織名>のリスクアセスメントとセキュリティ計画レポートを COTR に提出する。

D.3.3.2 システムのリスクアセスメント方法の選択

[注：組織は、使用する特定のリスクアセスメント方法またはツールを指定できる。組織が方法またはツールを指定しない場合、この作業を実行する必要がある。]

<契約者または組織名>は、オペレーティングシステムのリスクを評価するテクニックを選択する。選択したリスクアセスメント方法は、NIST SP 800-30『情報技術システム用のリスク管理ガイド（Risk Management Guide for Information Technology Systems）』と合致する必要がある。

契約者は、方法選択の理由を説明した方法選択レポートを COTR に提出する。

D.3.3.3 リスクアセスメントの実行

契約者は、リスクアセスメント方法のサポートに必要なデータを収集し、リスクアセスメントを実行する。リスクアセスメント作業に必要な要件は次のとおりである。

・ システムの特性決定

・ 脅威の特定

・ 脆弱性の特定

・ コントロール分析

・ 蓋然性の判断

・ 影響の分析

・ リスクの判断

・ コントロールの推奨

・ 結果の文書化

D.3.3.4 リスク低減計画の作成

契約者は、リスクアセスメントで特定されたリスクを低減する計画 [15] を作成する。計画には次の項目を含める。

・ アクションの推奨優先順位

・ 推奨コントロールオプションの評価

・ 費用対効果分析

・ 保護インプリメント計画

・ 残余リスクの判断

契約者は、リスク低減レポートを COTR に提出する。

[15] リスク低減プロセスのある重要なステップは、組織が排他的に行う必要があるため、この項から排除されている。これらのステップには、最終的なコントロールの選択、コントロールのインプリメントの担当の割り当て、選択したコントロールの実際のインプリメントなどがある。

D.3.4 認証と認定

D.3.4.1 セキュリティ要件の決定

契約者は、システム、そのユーザー、機能要件、セキュリティ要件全体を理解するために、システムについて研究する。

D.3.4.2 システムセキュリティ要件の準備とレビュー

契約者は、システムセキュリティ要件のリストを用意する。契約者は、システムセキュリティ要件のリストを COTR に提出する。

D.3.4.3 システムのセキュリティテストと評価 [16] の実行

契約者は、セキュリティテストと評価を実行し、適切な検証テクニック、検証手順、手順の改良を使用して、IT システムの管理、運用、技術的セキュリティコントロールが、適切にインプリメントされ、効果的に使用されていることを実証する。

契約者は、ST&E 活動の結果に基づいた最終 ST&E レポートを用意し、これを COTR に提出する。

D.3.4.4 セキュリティ検定レポートの準備

契約者は、検定作業の結果を要約したセキュリティ検定レポートを準備する。このステートメントでは、実施中または作成中のセキュリティとコントロールの適性を取り上げる。契約者は、セキュリティ検定レポートとステートメントを COTR に提出する。

[16] NIST SP 800-37（草案）では、開発用の ST&E と運用用の ST&E とを区別している。ST&E のタイプは、システムが新規か、大幅な変更を受けているか、またはすでに配信され装備されているかにより異なる。この SOW パラグラフは一般的な場合を示しており、開発用の ST&E と運用用の ST&E とを区別していない。

契約者は、製品のセキュリティ機能に関するレポートの草案を作成し、セキュリティ製品レポートを COTR に提出する。

D.3.5 IT セキュリティ製品の選択と評価

NIST SP 800-23『セキュリティ保証と取得/テスト済みおよび評価済み製品の使用に関する連邦組織向けガイドライン（Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products）』には、セキュリティ関連の IT 製品の取得と使用に関する、連邦組織向けのガイダンスが記述されている。NIST SP 800-23 では、全米情報保証パートナーシップの共通規則－コモンクライテリア－（CC）評価とその検証プログラムと、NIST の暗号鍵管理モジュール検証プログラム（CMVP：Cryptographic Module Validation Program）を紹介している。組織が CC または CMVP プログラムの範囲外から製品を選択する場合、次の SOW パラグラフが提供される。ただし、機密情報を保護するために暗号法を使用する必要があると判断した連邦機関については、NIST 認定研究所で試験済みの関連 FIPS 標準に適合した FIPS 認定の暗号法を使用しなければならない。

D.3.5.1 セキュリティ機能を判断するための製品の評価

契約者は、<製品名>のセキュリティ機能またはシステムの他のセキュリティ製品とのインターフェース、あるいはその両方を判断する。該当する場合、これには、<製品名>ベンダーの代表者との直接の連絡が必要になることがある。製品の購入が必要なこともあるが、試用ベースでの評価版を試用することが望ましい。

D.3.5.2 推奨事項およびインプリメント計画の提供

契約者は、<製品名>が組織の要件に適合しているかどうかに関する推奨事項レポートを提供する。推奨事項は、コスト、レスポンス時間、使いやすさ、インプリメントと運用のしやすさ、顧客サポート、ドキュメントの品質に基づく。推奨事項が明白である場合、契約者は、組織のセキュリティ目標をサポートする<製品名>をインプリメントする計画を準備する。この計画では、インプリメントプロセス全体を通じて、どのように目標を達成するかを記述する。

契約者は、推奨事項およびインプリメント計画レポートを COTR に提出する。

D.3.5.3 組織の要件と利用可能な製品のレビュー

直接的な IT セキュリティ機能を実行するハードウェアとソフトウェア製品の評価

契約者は、組織の IT セキュリティ計画と<IT セキュリティ製品のタイプ> IT セキュリティ製品の要件とをレビューする。このレビューでは、組織のニーズに最も適切に適合する機能について文書化する。契約者はまた、これらのニーズに合わせて設計された製品のタイプのリストを作成する。このリストには、各製品の簡潔で全般的な説明を含める。

契約者は、製品要件レポートと製品候補リストを COTR に提出する。

[注：組織が、特定のタイプの IT セキュリティ製品を考えている場合、次の手順が必要になる。レポートが承認されると、契約者は、評価される製品のリストを提出して承認してもらう。<組織名>は、さらに評価できるように、<N>個の製品を選択する。

利用可能な製品の評価

追加評価が必要と判断された製品ごとに、契約者はその製品の実働版またはデモ版を取得して、その機能をテストする。該当する場合、これには、<IT セキュリティ製品名>ベンダーの代表者との直接の連絡が必要になることがある。製品の購入が必要なこともあるが、試用ベースでの評価版を試用することが望ましい。契約者はまた、その製品が関連する既存の連邦標準に準拠していることを確認する。

このレポートでは、<IT セキュリティ製品>によって実行される IT セキュリティ機能を取り上げる。また、データ収集機能、実用性（使いやすさ、エラーメッセージ、ドキュメントの品質など）、セキュリティコントロール、レポート機能、製品サポート、組織の他の IT セキュリティ製品や手順との互換性についても取り上げる。契約者は、各製品の長所と短所を文書化したレポートを用意する。

契約者は、製品評価レポートを COTR に提出する。

デモンストレーションの実施と推奨事項の提供

契約者は、特定した IT セキュリティ製品ごとにデモンストレーションを行い、評価レポートでその長所と短所を強調する。契約者は、インプリメントに適した製品を 1 つまたは複数推奨する。推奨事項は、特定の組織のセキュリティ要件に対する製品の達成能力に基づき、コスト、レスポンス時間、使いやすさ、インプリメントと運用のしやすさ、顧客サポート、ドキュメントの品質、出力レポートに基づく。

契約者は、推奨事項レポートを COTR に提出する。

[注：特定した IT セキュリティ製品それぞれの長所と短所を特定することが必要であるが、各製品のデモンストレーションはオプションである。]

D.4 運用セキュリティサービス

D.4.1 緊急時対応計画

D.4.1.1 緊急時対応計画のレビュー

契約者は、ユーザーの関与、実際の運用、完全さ、正確さについて、緊急時対応計画 [17] をレビューする。契約者は、特定された欠陥と計画に組み込まれている是正措置に注目しながら、最新のテスト計画やテスト結果をレビューする。契約者は、緊急時対応計画レビューレポートを COTR に提出する。

D.4.1.2 現在の緊急時対応計画手順のレビュー

契約者は、現在の緊急時対応計画手順をレビューし、<組織名>システムによる機密データ処理の継続的運用に与える影響を評価する。このレビューでは、計画されたレスポンスを逐次調べ、生命を保護し、損害を抑え、基本的サービスと運用を行える能力を保持する上で適切かどうかを検討する。契約者はまた、使用されるシナリオを含め、最新の緊急時対応計画手順のテスト結果もレビューする。契約者は、このレビューから得られた所見をレポートに文書化する。契約者は、緊急時対応計画手順レビューレポートを COTR に提出する。

D.4.1.3 損害アセスメント方法の評価

契約者は、セキュリティに対する影響を含め、損害アセスメントの実行に使用される方法を評価し、所見をレポートに文書化する。このレポートでは、損害アセスメントに使用される方法を取り上げる。契約者は、損害アセスメント方法に、緊急事態または混乱の原因、さらなる混乱または損害の可能性、緊急事態により影響を受ける領域、物理的インフラストラクチャの状態、IT 機器の在庫や機能状態、IT 機器またはデータへの損害のタイプ、交換の必要な項目、サービス回復にかかる推定時間が含まれているかどうかを評価する。契約者は、損害アセスメント方法評価レポートを COTR に提出する。

D.4.1.4 バックアップ手順のレビュー

契約者は、最新の緊急時対応計画テスト手順書を含んだバックアップ手順をレビューし、プロセス全体にわたって手順の適切性とシステムのセキュリティを査定する。契約者はまた、テストに使用されたシナリオを含む最新のバックアップ手順のテスト結果もレビューする。このテスト結果には、バックアップの輸送、ストレージ、各システムをサポートする特定の手順を含める。契約者は、バックアップ手順レビューレポートを COTR に提出する。

---

[17] この作業では、緊急時対応計画が存在していると想定している。このような計画が存在していない場合、ま

たは不完全な場合、別の作業で計画を作成する。

D.4.1.5 緊急時対応計画の評価

契約者は、緊急時対応計画を評価して、想定された期間中に継続的な運用を提供できるかどうかを判断する。レビューでは、セキュリティの必要なレベルを取り上げ、回復プロセス、一時的な運用、元のサイトへ復帰または新しいサイトへ移行することで、このレベルが有効であり続けることを確認する。契約者はまた、使用されるシナリオを含め、最新の緊急時対応計画のテスト結果もレビューする。契約者は、このレビューをレポートに文書化する。契約者は、緊急時対応計画評価レポートを COTR に提出する。

D.4.2 インシデントハンドリング

D.4.2.1 インシデントレスポンスチームの確立

契約者は、インシデントレスポンスチーム（チーム）を結成し、直接的な技術的支援を提供する。この支援には、<組織名>の現場からの要求に応じた現場出向を含める。目標は、チームが、インシデントにより発生した技術的問題を解決するために十分なサポートを、支援を要求している全ての現場に対して提供することである。

チームは、チーム活動を行う中心となる<組織名>の本部にオフィスを構え維持する。このセンターには、他のサイトと通信するために必要となるコンピュータやその他のハードウェアも収容する。

D.4.2.2 インシデント追跡システムの確立

チームは、<組織名>が、以前のインシデントに関する関連情報、既知のウィルスやその他の有害コードのドキュメントへのリンク、システムの既知の脆弱性、重要な連絡担当者を見つけるためのシステムを開発する。チームはインシデント追跡システムを開発する。

COTR がこの追跡システムをレビューする。

D.4.2.3 協力手順の作成

組織の判断で、チームは、<組織名>とその他の連邦組織との間で協力手順を作成する。チームの作業の一部として、インシデントレポートの手順を作成する。これらの手順では、インシデント中に連絡する人物、共有する情報の種類、特定の作業を実行する人物、さまざまなタイプのインシデントとその状況下でのサブタスクの分担方法について定める。チームは、ベンダーとの協力関係を構築し、セキュリティの脆弱性と修復方法について学習する。チームはまた、ベンダーと協力して、問題を確実に修復する。契約者は、これらの協力手順を文書化し、インシデントハンドリングガイドラインに含める。

契約者は、協力手順レポートを COTR に提出する。

D.4.2.4 インシデントハンドリングの手順およびポリシーの作成

チームは、チームと<組織名>の現場の技術担当者の両方が遵守できる、インシデントハンドリングの手順とポリシーを作成する。これらのガイドラインには、イベントハンドリングのための管理と技術ガイダンス、作業3で作成した協力手順レポートを含める。チームは、発生したインシデントやチームが関わっている状況を定義する。これらのガイドラインは、<組織名>のポリシーに一致する。これらのガイドラインには、技術的問題を解決し、組織的な作業を行い、証拠を保持するために必要な詳細も含める。

最後に、これらのガイドラインは、インシデントハンドリングの関係者が、イベントを分類し、インシデントやイベントに対応する優先順位を付ける場合に役立つ。

契約者は、インシデントハンドリングガイドラインを COTR に提出する。

D.4.2.5 セキュリティで保護された電気通信機能の開発

チームは、<組織名>の現場との間で、セキュリティで保護された通信機能を確立する。これによってチームは、複数の現場から電子メールを送受信し、パッチや技術データなどを相互に交換できるようになる。これは、チームが、機密性が高く、アクセスするのに権限が必要となる情報を配信するには、コントロールが必要であることを示唆している。

D.4.2.6 インシデントハンドリングのソフトウェアツールの特定

チームのメンバーは、インシデントハンドリングプロセスを容易にするソフトウェアツールのタイプを決定する。ツールには、侵入監視、検知やそれを記録する機能、インシデント分析やリバースエンジニアリングを行うツール、リアルタイム通知を含む。契約者はツールの機能についてのレポートを作成する。このレポートには、もし手に入るのであれば、最もコスト効率がよく、<組織名>によるインシデントハンドリングに役立つツールの推奨を含める。

契約者は、インシデントハンドリングに使用するソフトウェアツールに関するレポートを COTR に提出する。

D.4.2.7 トレーニングおよび意識向上活動の実施

チームは、<組織名>と協力して、<トピック名>に関するワークショップまたはトレーニングセミナーを実施する。これらの活動では、チームは、<トピック名>の方法のデモンストレーションを作成する必要がある。チームは、<トピック名>で役立つ有用なソフトウェアツールに関する情報も提供する。

COTR はワークショップまたはトレーニングセミナーの概要およびスケジュールを受け取る。契約者は、ワークショップまたはトレーニングセミナーの日時と場所を COTR と取り決める。

D.4.3 トレーニング

D.4.3.1 コースの概要とレッスンのマスタープランの作成

契約者は、組織内の受講者カテゴリごとのレッスンのマスタープランとコース資料を作成する。この作業のガイドラインは作業の説明の項に記載している。

契約者は、コースの概要とレッスンのマスタープランを IT セキュリティスタッフに提示する。

D.4.3.2 受講者カテゴリごとのレッスンプランの作成

契約者は、組織内の受講者カテゴリごとのレッスンプランとコース資料を作成する。

契約者は、受講者カテゴリごとのレッスンプランとコース資料を IT セキュリティスタッフに提示する。

D.4.3.3 パイロットクラスの実施

契約者は、作成したコースごとにパイロットクラスを実施し、組織が承認した評価方法を使用して、コース資料とプレゼンテーションの有効性を評価する。

契約者は、最終的なインストラクターガイドと参加者資料のパッケージを COTR に提出する。この提出には、上記の作業で作成されたすべての資料を含める。

D.5 技術的セキュリティサービス

D.5.1 <IT システム名>のシステムセキュリティサポート

契約者は、組織の現場における<システム名>デバイスの交換設置、アップグレード、統合のサポートを提供する。契約者は次のサポートを提供する。

・インストール後サポート

契約者は、インストール後に<システム名>のサポートを提供する。このサポートには、<システム名>の維持と緊急事態時の復元または交換が含まれる。

・現場設置

契約者は、<組織>の承認のもと、指定した場所での<システム名>製品の現場での交換設置を行う。

・文書化

契約者は、今後の保守と拡張のライフサイクル運用を高めるために、教訓を含み、すべての現場設置の結果を要約した出張報告書を作成する。契約者はまた、システムのインストールの承認を得るために要求されている文書化サポートの調整も行う。

・運用上の影響

契約者は、重要な中心機能に影響を与えずに、上記のサポートを実施する。この影響アセスメントは、顧客サポート要件などの既存の利用可能なリソースと、すべての重大なインシデント、イベント、活動、または現在の運用に基づく。<組織>と<ベンダー>のチームは、影響全体を評価し、既存の要件をサポートする適切な推奨事項を作成する。

・現場要件分析

契約者は、現場に対し、現場要件分析を要求し、参加し、調整する。この分析は、それぞれの現場設置中に、実行されるべき作業レベルと、必要になる機器や接続の数量・タイプを決定するために使用される。

D.6 契約管理

次の SOW パラグラフは、特定の IT セキュリティサービスには関連していない。むしろ、必要なサービスの取得をサポートする場合に使用される。

D.6.1 契約者要員の要件

この活動に割り当てられる契約者要員は、<審査レベル>までの適切な<経歴審査>を受ける。

契約者は、提供されたスキルカテゴリを使用して、この活動を担当するスタッフを推薦する。

[注：経歴審査の基準は、情報の機密を守る任命内容と要求されている身元調査の種類と一貫性が取れている必要がある。]

D.6.2 人的資格要件

契約者の現場リーダー、技術的リーダー、およびセキュリティ代表者は、6 か月以内に<認定>またはそれに相当するものを取得するか [18] [19]、<等級名>またはそれに相当するものを得ている。

契約者は、提供されたスキル要件を使用して、この活動を担当するスタッフを推薦する。

D.6.3 契約者要員のセキュリティ要件

契約者は、<組織名>のセキュリティプログラムで運用される情報へのアクセス権を持つ契約者、下請け契約者、ベンダー要員（以下「契約者要員」）と、この契約に基づいて作成され、受理されたシステムが、<組織の要件>を満たしていることを保証する。

プログラムマネージャは、各作業要求書で身元調査要求を特定する。

<組織名>は、必要に応じて、契約者にセキュリティ質問表フォームの提出を求める。それぞれの情報へのアクセスが認められる前に、すべてのフォームを記入して提出し、プログラムマネージャから承認を受ける必要がある。

身元調査を受けた契約者要員の適性に関する質問がある場合、その旨を通知し、回答する機会をその要員に与える。この要員が不適切と判断した場合、<組織名>は、契約者と契約担当者に通知する。アクセス拒否の通知があった場合、契約者は、アクセスコントロールシステムを通じたアクセスの無効化、システムアクセス権限の無効化、およびアクセス ID およびメディアの返却など、以降のアクセスを排除するための行動が迅速に行われるようにする。

---

[18] 業界認定は、IT セキュリティ要員が資格を備えていること、または技術的に適切であることを保証しない。特定の認定を取得するように全要員に対して一律に要求することは、高額になり、組織の利益を高めることなく、利用可能な選択肢を不必要に制限する場合がある。認定は、IT セキュリティのスキルレベルの理解を得るために、他の手段とともに使用される。一般的なセキュリティ認定は、セキュリティプログラムマネージャやシステムアドミニストレータなどのポジションには役立つが、プロトコルや暗号エンジニアなどの専門的なスキルを必要とするポジションにはあまり役立たない。このような領域では、専門的な認定が有効である。一般的な認定と専門的な認定だけでは、必ずしも能力または有効性の保証にはならず、概してその他の証明が必要となる。

[19] セキュリティ認定の総合的なリストは、次のサイトに用意されている。
searchsecurity.techtarget.com/tip/1,289483,sid14_gci900920,00.html

付録 E - よくある質問とその回答

1. このガイドはどのような読者を対象としているか。

情報技術セキュリティサービスのガイドは、IT セキュリティサービスの開始、管理、実施、または終了を担当する IT セキュリティのすべての利害関係者を対象としている。さらに、このドキュメントは、組織が、現在のサービスおよびサービスプロバイダのパフォーマンスを評価し、代替案が投資回収率を向上させるかどうかを定めるためのするためのフレームワークを提供しているので、ビジネスマネージャにも有用である。

2. このガイドはどのような目的で作成されたのか。

このガイドは、IT セキュリティの利害関係者に、IT セキュリティサービスの開始、管理、実施、および終了を行うためのライフサイクルフレームワークを提供するために作成された。組織は、セキュリティやその他の IT 投資の投資回収率を最大化しようとしている。組織が適切なサービスプロバイダや効果的なセキュリティサービスを見つけようとするときに、IT セキュリティサービスの開始、管理、実施、終了を行うためのフレームワークが必要であった。

3. IT セキュリティサービスとはどのようなものか。

IT セキュリティサービスはさまざまに分類できる。このドキュメントでは、管理、運用、または技術サービスのいずれかに分類されている。管理 IT セキュリティサービスは、組織内の IT セキュリティプログラムおよびリスクの管理を中心としたサービスであり、たとえばセキュリティポリシーの作成やリスク管理などがある。運用セキュリティサービスは、〔システムではなく〕人間が実施し実行するセキュリティコントロールに焦点を当てたものであり、ネットワークテストやトレーニングおよび意識向上などがある。最後の技術サービスは、IT システムによって実行されるセキュリティコントロールに焦点を当てたサービスであり、ファイアウォールや侵入検知などがある。このドキュメントでは、実現可能な IT セキュリティサービスのサンプルを提供している。

4. IT セキュリティサービスのライフサイクルとはどのようなものか。

IT セキュリティサービスのライフサイクルは、IT セキュリティサービスを開始、管理、実施、および終了するための、6 つのフェーズから成るアプローチである。この 6 つのフェーズは次のとおりである。

・ 開始
・ アセスメント
・ ソリューション
・ インプリメント

・運用
・終了

5. IT セキュリティサービスのライフサイクルでは、どのような人物が役割を割り当てられているか。

IT セキュリティサービスの選択、アセスメント、インプリメント、および管理を行う参加者は、サービスのタイプと範囲、サービスアレンジメント、および組織のタイプにより異なる。重要な役割としては、特に、最高情報責任者（CIO）、契約担当者、契約担当者の技術代表者、IT 投資委員会、IT セキュリティプログラムマネージャ、IT システムセキュリティ担当者、プログラムマネージャ/調達開始者、およびプライバシー担当者がある。

6. IT セキュリティアレンジメントとはどのようなものか。

IT セキュリティアレンジメントとは、IT セキュリティサービス要件を特定した結果であり、組織がこのサービス要件を実施する方法に対する決定である。IT セキュリティマネージャが選択できるサービスアレンジメントは無数にある。組織は、その内部の従業員とチームを選択して必要なサービスを実現することも、外部サービスプロバイダを全面的に使用することも、外部および内部の両方の従業員に IT セキュリティサービスの役割を割り当てることもできる。

7. この IT セキュリティサービスガイドは、IT セキュリティサービスの「外部委託」を推奨しているのか。

このガイドでは、特定のサービス、サービスレベル、サービスの組み合わせ、サービスアレンジメント、サービス契約、またはサービスプロバイダを規定していない。むしろ、各組織に適切な IT セキュリティサービスを評価、分析、選択するための方法を提供している。どのドキュメントでも、所与の組織にとって何が最適かを規定するには、非常に多くの問題と非常に多くの変数がある。IT セキュリティマネージャとその他の上級担当者は、各代替案のリスクと利益を査定し、組織にとって最も適切な代替案を選択する必要がある。

8. マネージャが IT セキュリティサービスの管理に使用できるツールにはどのようなものがあるか。

このガイドでは、IT セキュリティサービスのライフサイクルフレームワーク、メトリクス、サービス契約など、マネージャが IT セキュリティサービスの管理に使用できるいくつかのツールを取り上げている。

9. メトリクスとはどのようなものか。

メトリクスとは、実際の関連データの収集、データ分析、およびパフォーマンスデータレポートを通じて、意志決定とアカウンタビリティを容易にする管理ツールである。トレーニングや意識向上プログラムなどの管理サービスのメトリクスの例としては、就業後 30 日以内に IT セキュリティトレーニングを受ける新人の人数が挙げられる。このメトリクスを繰り返し時間をかけて収集すれば、マネージャは、現在のトレーニングサービスプロバイダが、現時点でその責務をどれだけ達成しているかを査定し、そのサービスプロバイダに対する将来の目標を定め、その後、所期の目標をどれだけ達成しているかを査定することができる。

10. IT セキュリティサービスの決定に影響する問題および要因にはどのようなものがあるか。

IT セキュリティサービスの決定に影響する要因は無数にあり、サービス、サービスアレンジメント、および組織のタイプにより異なる。一般的に言えば、要因と問題は次のカテゴリに分類できる。

・ 戦略/使命 - 組織の使命とビジネス機能に関連

・ 予算/資金 - IT セキュリティのコスト、資金、価格に関連

・ 技術/アーキテクチャ - 組織の技術とアーキテクチャ環境に関連

・ 組織/文化 - イメージ、評判、回復力などの組織の無形要素に関連

・ 人員 - 組織の契約者と従業員に関連

・ ポリシー/プロセス - 組織のビジネス、IT セキュリティポリシー、手順に関連

11. 組織は、そのサービスがライフサイクルのどのフェーズに該当するかをどのようにして把握するのか。

IT セキュリティサービスのライフサイクルは、IT セキュリティサービスが継続的に査定および評価される、反復的なプロセスである。組織が IT セキュリティサービスをまだインプリメントしておらず、それらを必要としている場合は、開始フェーズに該当する。その他の場合はすべて、おそらく運用フェーズに該当し、サービスプロバイダと組織のパフォーマンスを評価する。

12. どのような要因がライフサイクルをトリガするのか。

トップレベルの管理職が現在の IT セキュリティ機能を評価することにした場合から、新しい IT セキュリティサービス要件まで、ライフサイクルをトリガする要因はいくつもある。このトリガは、おそらく、質問 10 で記した問題のカテゴリのいずれかに該当するが、すべてのトリガには、「現在の IT セキュリティ環境を評価し、実行可能なサービスソリューションを特定する理由が十分にあるイベント」という 1 つの共通した特性がある。

13. 組織は、現在のサービスが適切かどうかをどのようにして判断するのか。

IT セキュリティサービスのライフサイクルの 2 番目のフェーズは、アセスメントフェーズである。このフェーズでは、IT セキュリティマネージャは、メトリクスの使用や総所有コスト（TCO）の原則を通じて、既存の IT セキュリティ環境を評価する。これらをともに使用することで、マネージャは現在のサービスレベルとコストを評価できる。ただし、このサービスレベルおよびコストが許容できるかどうかは、このドキュメントの範囲外である。このことは、IT セキュリティマネージャが組織それぞれの IT セキュリティおよびビジネス要件に基づいて、独自に判断する

必要がある。

14. 組織は IT セキュリティソリューションをどのようにして選択するのか。

組織は、現在の環境のアセスメントと、現在のサービスに照らして実行可能な代替案のビジネスケース作成に基づいて、IT セキュリティソリューションを選択する。ビジネスケースでは、意志決定が簡単または明確にならないこともあるが、意志決定者が組織のニーズに適したサービスアレンジメントを比較検討、考慮、選択するために必要なデータを提供する必要がある。意志決定者の間で議論や意見の相違が見られる可能性もあるが、最終的に選択には合意が必要である。ビジネスマネージャおよび IT セキュリティマネージャ全員が、インプリメントするソリューションに完全に賛同している場合にのみ、サービスはうまくいくのである。

15. 組織はサービスプロバイダをどのように選択するのか。

組織がサービスプロバイダを選択する方法は、サービス、サービスアレンジメント、および組織のタイプにより異なる。サービスアレンジメントが内部のものである場合、サービスを提供する 1 つの内部グループしか存在しない。サービスが新しい分野のものである場合、または高度に専門的な経験を必要とする場合、選択できるサービスプロバイダはわずかしかない。規模の大きな政府機関では公式の RFP を公表することもある。どの場合でも、組織は、サービスプロバイダ評価基準を特定し、提案を募集し、基準に照らして候補のプロバイダを評価する必要がある。

16. サービス契約にはどのような内容を含めるべきか。

サービス契約では少なくとも次の内容を指定する必要がある。

・ 組織の役割および責任とサービスプロバイダの役割および責任の両方に関する明確な定義

・ 実施期間または納入期日

・ 定められたサービスレベルとサービスレベルのコスト。

・ サービスレベルと期日目標、規則、およびその他の契約条件をサービスプロバイダが遵守しているかどうかを、マネージャが査定する方法に関して確定したプロセス

・ サービスプロバイダによる不履行または損害に対する具体的な是正措置（金銭、法的など）

・ 機密データの取り扱いの明示的な規則

17. 組織はサービスのパフォーマンスをどのように監視するのか。

組織は、IT セキュリティサービスのライフサイクルの運用フェーズで、サービスプロバイダのパフォーマンスと組織のパフォーマンスを監視する必要がある。これらのメトリクスを収集する頻度と方法は、IT セキュリティプロバイダとクライアント組織との間のサービス契約で指定する必要がある。フェーズ 2（現在の環境の評価）で収集したメトリクスが、運用中に収集したメトリクスと同じになる可能性が高い。なぜなら、将来のサービスアレンジメントがその後、現在の環境になるからである。

18. IT セキュリティサービスのライフサイクルはいつ終了するのか。

IT セキュリティサービスのライフサイクルのトリガが無数に存在するように、サービスプロバイダの破産、契約の終了、要件の変更、サービスプロバイダの不十分なパフォーマンス、新しい技術要件など、IT セキュリティが終了する理由も多数存在する。サービスの終了すべてに共通する特性は、別のセキュリティソリューションのインプリメントが必要になるほど重大なイベントということである。