NIST Special Publication 800-64 Revision 2

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

情報システム開発ライフサイクルにおけるセキュリティの考慮事項

Richard Kissel
Kevin Stine
Matthew Scholl
Hart Rossman
Jim Fahlsing
Jessica Gulick

情報セキュリティ

米国立標準技術研究所
情報技術研究所
コンピュータセキュリティ部門

Gaithersburg, MD 20899-8930

2008 年 10 月

米国商務省 長官
Carlos M. Gutierrez, Secretary

NIST 副所長
Patrick D. Gallaghe

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

コンピュータシステム技術に関する報告書

米国国立標準技術研究所（NIST: National Institute of Standards and Technology、以下、NIST と称す）の情報技術ラボラトリ（ITL:Information Technology Laboratory）は、国家の測定および標準に関する基盤において技術的リーダーシップを提供することにより、米国の経済と公共福祉に貢献している。情報技術ラボラトリは、テストの実施、テスト技法の開発、参照データの作成、実装によるコンセプト実証、技術的分析を通じて、情報技術の開発と生産的利用の発展に努めている。情報技術ラボラトリの責務は、連邦政府の情報システムにおいて、費用対効果の高いセキュリティを施し、国家安全保障にかかわらない情報のプライバシーを確保するための、技術的、物理的、管理的および運用のための標準とガイドラインを策定することにある。NIST Special Publication 800 シリーズでは、情報システムセキュリティにおける情報技術ラボラトリの調査、ガイドライン、普及活動ならびに産業界、政府機関および教育機関との共同活動について報告する。

作成機関

米国国立標準技術研究所（NIST: National Institute of Standards and Technology、以下 NIST と称する）は、2002 年施行の連邦情報セキュリティマネジメント法（FISMA: Federal Information Security Management Act、以下 FISMA と称す）、公法 107-347 に基づくその法的責任を推進するために、この文書を作成した。

NIST は、すべての連邦政府機関の運営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、最低限の要求事項を含んだ標準およびガイドラインを作成する責務があるが、このような標準およびガイドラインは国家安全保障にかかわる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、『政府機関の情報システムの保護（Securing Agency Information Systems）』の要求事項に一致しており、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政府機関が使用する目的で作成されている。非政府組織が自由意志で使用することもでき、著作権の制約はない（翻訳者注:著作権に関するこの記述は、SP800-64 の英語の原文のことを言っており、日本語へ翻訳した本書の著作権は、独立行政法人情報処理推進機構および NRI セキュアテクノロジーズ株式会社に帰属する）。

本文書における一切は、商務長官が法的権威に基づき連邦政府に対して義務および拘束力を与えた標準および指針を否定するものではない。また、これらの指針は、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に変更を加えたり、これらに取って代わるものと解釈してはならない。

本文書中で特定される商業的組織、装置、資料は、実験手順または概念を適切に説明するためのものである。したがって、NIST による推薦または保証を意味するものではなく、これらの組織、資料、または装置が、その目的に関して得られる最善のものであると意味しているわけでもない。

謝辞

本書執筆陣であるRichard Kissel、Kevin StineおよびMatthew Schollは、本書のアップデート、ドラフトの作成、および資料のレビューに貢献してくれた同僚(Science Applications International Corporation (SAIC)のHart Rossman氏、Jim Fahlsing氏およびJessica Gulick氏)に感謝の意を表する。また、本書の原作者および本書の作成に大いに寄与してくれた校閲者(Arnold Johnson氏、John Garguilo氏、Marianne Swanson氏および Elizabeth Lennon氏)に、とりわけ感謝の意を表する。さらに、公共および民間部門からいただいた数多くの貢献にも心より感謝の意を表する。彼らの建設的で思慮深いコメントによって、本書の質と実用性が高められた。

目次

図

要旨

NIST SP800-64『情報システム開発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 System Development Life Cycle) 』は、連邦政府機関が、重要な IT セキュリティ手順を IT システム開発ライフサイクル(SDLC: System Development Life Cycle、以下 SDLC と称す)に組み込む際に役立つ資料として、作成された。このガイドラインは、国家安全保障にかかわるシステムを除く、すべての連邦政府システムに適用できる。本書は、チュートリアルではなく、リファレンスとして利用することを意図しており、SDLC を通して必要に応じて、他の NIST 文書と併用することが望ましい。

本書は、情報システムのオーナー、情報のオーナー、情報システム開発者およびプログラムマネージャなど、情報システムに携わる連邦政府の職員および情報セキュリティ専門家にとって有用なものである。

最も効果的な情報セキュリティを実現するためには、SDLC の初期段階で情報セキュリティを組み込むことが求められる。SDLC の早い段階で情報セキュリティを組み込みによって、セキュリティプログラム投資に対する費用対効果を最大にすることができる。以下に、その理由を示す。

- セキュリティの脆弱性と誤った構成を早期に発見し、軽減することで、セキュリティ管理策の実施および脆弱性の軽減にかかる費用が少なくなる。
- 必須のセキュリティ管理策の実施にかかわる、エンジニアリング上の問題(engineering challenge)への意識が高まる。
- 共有セキュリティサービスを特定し、セキュリティ戦略とツールを再利用することで、開発費を削減し、スケジュールを短縮できると同時に、実績がある手法と技の利用により、セキュリティ状態を向上することができる。
- 包括的なリスク管理をタイムリーに行うことで、経営者は、十分な情報を得た上で、意思決定を行うことができる。

本書は、SDLC の情報セキュリティコンポーネントに焦点を置く。まず、ほとんどのシステム開発で必要とされるセキュリティ上の重要な役割と責任について説明する。次に、SDLC プロセスになじみのないユーザが情報セキュリティと SDLC との関係を理解できるよう、SDLC に関する十分な情報を提供する。

本書では、セキュリティ手順を SDLC(ウォーターフォールモデルとも呼ばれる)に組み込む。本書記載の SDLC の 5 つのステップは、開発手法の一例であり、必ずしもこの手法を用いる必要はない。

最後に本書では、SDLC ベースの開発のように明確に定義されない IT プロジェクトやイニシアティブに対する洞察を行う。これらのプロジェクトやイニシアティブには、サービス指向型アーキテクチャ、組織をまたがるプロジェクト、および IT 施設開発などがある。

第 1 章

はじめに

組織内のすべての IT 資産に対するリスクを管理するための、包括的な戦略を実施、統括するためには、SDLC におけるセキュリティを考慮することが不可欠である。NIST SP800-64 は、連邦政府機関が、重要なセキュリティ活動を自身の SDLC ガイドラインに組み込む際に役立つ資料として、作成された。

1.1 目的および適用範囲

本書の目的は、連邦政府機関による、情報セキュリティの IT 開発プロセスへの組み込みを支援することにある。結果として政府機関は、リスクベースの費用効果に優れたセキュリティ管理策を特定、開発し、テストすることができる。本書は、SDLC の情報セキュリティコンポーネントに焦点を置く。システムの導入および開発全般に関しては、本書が扱う範囲外とする。また、組織の情報システムガバナンスプロセスについても、本書が扱う範囲外とする。

まず、ほとんどのシステム開発で必要とされるセキュリティ上の重要な役割と責任について説明する。次に、SDLC プロセスになじみのないユーザが情報セキュリティと SDLC との関係を理解できるよう、SDLC に関する十分な情報を提供する。

本書が扱う範囲は、ウォーターフォール SDLC 方法論の範囲内で生じるセキュリティ活動である。本書が扱う内容は、政府機関が採用しうる他の SDLC 方法論にも流用できるようになっている。

1.2 対象読者

本書は、情報システムおよび情報セキュリティに関わる連邦政府の職員にとって有用なものである。これらの職員には (i) 情報システムおよび情報セキュリティを管理、監督する者（最高情報責任者(CIO)、上級情報セキュリティ責任者(SAISO)、運用認可権限者(AO)など）(ii) 組織の任務遂行に強い関心を持つ組織の責任者 (ミッションおよびビジネスエリアのオーナー、情報のオーナーなど) (iii) 情報システム開発責任者(プログラムマネージャ、プロジェクトマネージャ、情報システム開発者など) (iv) 情報セキュリティの導入および運用責任者(情報システムのオーナー、情報のオーナー、情報システムセキュリティ責任者など) が含まれる。

1.3 組織の任務、セキュリティプログラム、および IT マネジメントに対する情報セキュリティの価値

連邦政府機関は、重要な任務を達成するために、情報および情報システムに大きく依存している。情報システムへの依存度が高まり、システムがより複雑になると同時に、リスク環境が絶えず変化することから、情報セキュリティは、いまや組織の任務遂行になくてはならない機能となった。この機能を実施することによって、政府機関が扱う情報へのリスク、政府機関の総体的な任務へのリスク、および政府機関が事業を遂行しアメリカ国民に仕える能力を脅かすリスクが軽減されるようでなければならない。情報セキュリティは、情報の機密性、完全性および可用性へのリスクが適切かつ効果的に管理された場合に、業務遂行の立役者となる。

政府機関は、自身の SDLC にセキュリティを組み込むことによって、次のようなさまざまな効果が得られることに気づくであろう。

- セキュリティの脆弱性と誤った構成を早期に発見し、軽減することで、セキュリティ管理策の実施および脆弱性の軽減にかかる費用が少なくなる。
- 必須のセキュリティ管理策の実施にかかわる、エンジニアリング上の問題(engineering challenge)への意識が高まる。
- 共有セキュリティサービスを特定し、セキュリティ戦略とツールを再利用することで、開発費を削減し、スケジュールを短縮できると同時に、実績がある手法と技の利用により、セキュリティ状態を向上することができる。
- 包括的なリスク管理をタイムリーに行うことで、経営者は、十分な情報を得た上で、意思決定を行うことができる。
- システム開発段階における重要なセキュリティ決定事項を文書化することにより、すべての開発フェーズにおいてセキュリティが十分に考慮されたことを、経営層に納得させることができる。
- 組織と顧客が自信をもってセキュリティの導入と利用を促進できるようになる。また、政府が自信をもってセキュリティへの投資を継続できるようになる。
- システム間の相互運用性が向上し、システムの統合が容易になる(さもないと、それらのシステムをさまざまなシステムレベルでセキュアにする必要があるため、統合性が損なわれてしまう)。

1.4 本書の構成

本文書は以降、次のように構成されている。

- **第 2 章**(Overview of Information Security and the System Development Life Cycle)では、SDLC と他の IT 分野の関係について簡単に述べる。また、SDLC に関する共通の理解を確立し、情報セキュリティの SDLC への組み込みにかかわる役割と責任について論じる。
- **第 3 章**(Incorporating Security into the Information System Development Life Cycle)では、情報セキュリティを SDLC のそれぞれのフェーズに組み込む際に役立つ考慮事項について述べる。
- **第 4 章**(Additional Security Considerations)では、サービス指向型アーキテクチャや仮想化などの開発シナリオに対するセキュリティ考慮事項について考察する。これらの開発にあたっては、従来のシステム開発努力とは異なるセキュリティ組込みアプローチが必要となる。

本書は、7 つの付録を含む。付録 A には、用語集を示す。付録 B には、略語の包括的なリストを示す。付録 C には、参考文献のリストを示す。付録 D には、NIST publications と SDLC セキュリティ活動のマッピングを示す。付録 E では、他の SDLC 方法論の概要を述べる。付録 F では、SDLC の開発／調達フェーズにおける、セキュリティ計画作成に関する追加考慮事項について論じる。付録 G では、SDLC へのセキュリティの統合に関する追加のグラフ図を示す。

第 2 章

情報セキュリティの概要と SDLC の原理

システムセキュリティプロセスと活動により、IT システムの管理と開発に役立つ有力な入力情報が生成され、リスクの特定、計画作成および軽減が可能になる。リスクマネジメントアプローチ[1]には、政府機関の情報と資産を保護する必要性と、セキュリティ管理策の実施およびリスク軽減戦略にかかる費用とのバランスを、SDLC 全体を通して適切に保つことが含まれる(図 2-1 を参照)。リスク管理を最も効果的に行うには、重要な資産と業務、および政府機関全体にかかわる脆弱性を特定しなければならない。リスクは共有されるものであり、組織、財源またはトポロジに特化しているわけではない。重要な資産と業務およびそれらの相互接続の特定と確認は、システムセキュリティ計画プロセスを通じて、また、CPIC(資本計画および投資管理)プロセスと EA(エンタープライズアーキテクチャ)プロセスが生成する情報の編集によって成し遂げられる。CPIC プロセスと EA プロセスが生成する情報は、政府機関の極めて重要な業務、それらの業務を支える資産、および既存の相互依存性と関係に対する洞察を与えてくれる。組織は、重要な資産と業務を特定した後に、BIA(Business Impact Analysis:ビジネス影響解析)を実施すべきである。BIA の目的は、組織のシステムと資産と、それらのシステムと資産によって提供される重要なサービスを関連づけること、また、それらのシステムや資産が損なわれた場合に被る被害をアセスメントすることにある。これらのシステムを特定することによって、政府機関は、(システムの)優先順位付けを行い、セキュリティを効果的に管理できるようになる。結果として、セキュリティオフィスは、IT プログラムを費用対効果が高くなるような形で実施できるようになり、IT プログラムが政府機関の業務にもたらす影響と価値を明確に示すことができる。

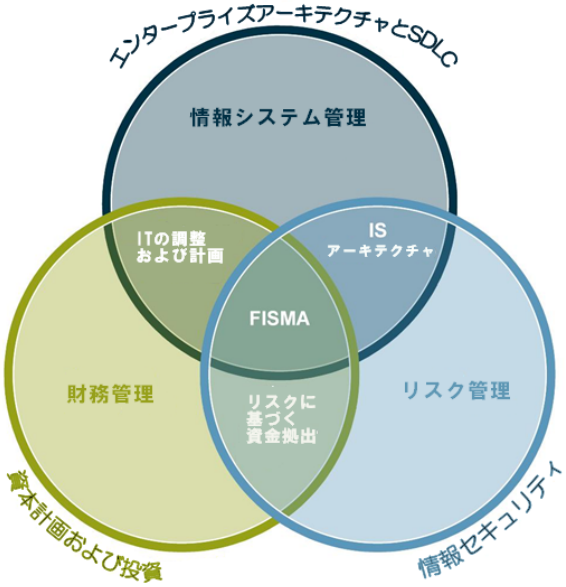

図 2-1. セキュリティ考慮事項の位置づけ

システムとプロジェクトに対するリスクマネジメントベースのアプローチを実施することは、セキュリティを政府機関のシステムと CPIC ライフサイクルに早い段階で組み入れて、かつサイクル全体を通してセキュリティを実施することを意味する。セキュリティをプロジェクトまたはシステムのライフサイクルに組み入れることで、組織は、セキュリティを、それらのプロジェクトやシステムにとって欠かすことのできない要素として、計画、調達、導入し、展開することができる。これにより、ライフサイクルのすべてのフェーズにおいて、セキュリティ要件が満たされているかを確認し、実施を促すことができる。

ライフサイクルマネジメントは、セキュリティ関連の決定事項の文書化を支援し、経営層に対して、ライフサイクルのすべてのフェーズにおいてセキュリティが十分に考慮されたことを保証する。システム管

1 NIST SP 800-39 (ドラフト)『情報システムのリスク管理 (Managing Risk from Information Systems: An Organizational Perspective) 』では、システムセキュリティリスクマネジメントプログラムの枠組みを記載している。

理者は、文書化された情報を利用して、なぜそのような決定が下されたかを確認することができる。(これにより、環境の変化がもたらす影響を、よりはやくアセスメントできるようになる。) 監視グループと第三者監査グループは、この情報をレビューすることによって、システム管理者が仕事を十分にこなしたかを確認し、セキュリティが考慮されていないエリアを特定することができる。レビューには、作成されたドキュメントの内容が、システムの実際の運用状況および管理状況を反映しているかを確認することが含まれる。

組織が、情報システムを効率的に開発するために使用できる方法は、数多く存在している。ウォーターフォールモデルと呼ばれる従来の SDLC では、システムが SDLC の最終段階で引き渡されると仮定する。別の SDLC 方法では、プロトタイプモデルを使用する。この方法は、実際には最終的な運用システムを開発せずに、システム要件の理解を深めるために使用される場合が多い。システムが複雑になるほど、より反復の多い開発モデルが必要になる。情報システムが大規模になり設計が複雑になるにつれ、より複雑なモデルが開発され、適用されてきた。このような複雑なモデルとしては、高速アプリケーション開発(RAD)モデル、共同アプリケーション開発(JAD)モデル、プロトタイプモデル、およびスパイラルモデルなどがある。システムの予想規模と複雑さ、開発スケジュール、およびシステムの寿命は、使用する SDLC モデルの選択に影響する。ほとんどの場合、SDLC の選択は、組織の調達ポリシーによって定められる。付録 E では、他の SDLC 方法論の概要を述べる。

このガイドでは、ウォーターフォールモデルを例として使用し、セキュリティを SDLC へ組み込んでいく。このモデルは、さまざまなモデルの中でも最も単純なものなので、この議論に適している。ただし、この項で論じる概念は、あらゆる SDLC モデルに適用できる。

2.1 共通の理解を確立する

2.1.1 連邦政府機関の SDLC ポリシーおよびガイドライン

各政府機関は、組織のビジネスニーズを支援し、組織の特異な文化を補うための、文書化されていて繰り返し利用可能な SDLC ポリシーとガイドラインを備えるべきである。政府機関の SDLC ガイドラインは、その機関の IT マネジメントスタイル、ニーズの複雑さ、および調達に関するプリファランス(preference)によっては、おおざっぱで客観的になることもある。たとえば、システムを開発し維持するための活動を自身で行う政府機関もあれば、それらの活動(開発のみならずメンテナンスも含まれることがある)を外注する機関もある。前者の場合、より詳細な手順を要する場合がある。一方で、調達中心の業務では、調達目的、サービスレベル、および調達物の詳細があれば事が足りる。調達中心の業務では、なじみがなく管理が行き届かないサプライチェーンを利用することもあり、このような場合、業務特有の脆弱性が存在すると考えられる。組織は、これらの脆弱性を理解し、考慮したうえで、リスクベースの決定を行うべきである。

典型的な SDLC は、「開始」、「開発／調達」[2]、「インプリメンテーション／アセスメント」、「運用／保守」、「廃止」の 5 つのフェーズからなる。それぞれのフェーズには、セキュリティを SDLC に効果的に組み込むためのセキュリティタスクが含まれている。なお、これらのフェーズは、システムが廃止されるまで繰り返えされることがある。

2 本書では、調達プロセスについては、あまり詳しく説明しない。調達に関する詳細情報については、FAR(連邦調達規則)と、組織独自のポリシーおよび手続きを参照のこと。

- 開発 – このフェーズでは、システムのニーズを明らかにし、システムの目的を文書化する。
- 開発／調達 – このフェーズでは、システムを設計、調達、プログラミング、開発、または構築する。
- インプリメンテーション／アセスメント。このフェーズでは、受け入れ検査後に、システムをインストールまたは配置する。
- 運用／保守。このフェーズでは、システムを稼動する。導入されたシステムは、ハードウェアやソフトウェアの追加を含め、数々のイベントの発生によって修正されることが多い。
- 廃止。このフェーズでは、システムの秩序だった終了、極めて重要なシステム情報の保護、システムが処理したデータの新システムへの移行、または適用可能な記録管理規定およびポリシーに従ったデータの保存などを確実にするための活動が行われる。

SDLC ガイドラインは、以下のものを文書化することによって、読者に有用性をもたらす。

- 主要な活動とマイルストーンに対する洞察
- 判断点またはコントロールゲート
- システム設計にとって極めて重要な情報を提供するアウトプット
- プロジェクトの成果
- システムの保守、セキュリティおよび運用に関する考慮事項

本書は、政府機関のミッションプロセス、エンタープライズアーキテクチャおよびファイナンシャルプロセスをサポートするものであり、また、それらによってサポートされるべきものである。

2.1.2 セキュリティの統合について

システムとプロジェクトに対するリスクマネジメントアプローチを実施することは、セキュリティを政府機関の SDLC と CPIC ライフサイクルに組み入れることを意味する。リスクマネジメントを扱うセキュリティコンポーネント群(マイルストーン、成果物、コントロールゲート、および相互依存性などで構成される)を備えることで、セキュリティが、プロジェクトやシステムにとって欠かすことのできない要素として計画、調達開発され、展開されるようになる。また、これによりライフサイクルのすべてのフェーズにおいて、セキュリティ要件が満たされているかを確認し、実施を促すことができる。セキュリティを SDLC に完全かつ効果的に組み込むことにより、セキュリティの専門家は、CPIC、IT および EA の代表と協力して、SDLC 全体を通して、セキュリティ考慮事項を効果的に管理、監視できるようになる。

プロジェクトの初期段階で情報セキュリティを実施することで、セキュリティ要件を必要に応じて統括的かつコスト効率よく成熟させることができる。製品の開始フェーズにおいてセキュリティを組み込むと、セキュリティ技術を後から組み込むよりもコストが少なくてすむ。なぜならば、セキュリティ技術を後から追加すると、システムの再構築やカスタマイズが必要となり、セキュリティ管理策も必要以上に多くなる(または少なくなる)ことがあるからである。すべてのプロジェクトにおいて、セキュリティは、システム要

件を策定する際に、それらの要件に含めるべきである。セキュリティを考慮したソリューションを考案することで、セキュリティ管理策を追加する必要性が大幅に減少することもある（たとえば、ドアが 2 つの家を設計する場合と、ドアが 4 つの家を設計する場合を比べてみよう。前者は、後者よりもドアの数が少ないため、エントリーポイント(家の入り口)のセキュリティが少なくてすむ。また、セキュリティシステムと電流を導入している家の周りにワイヤーを張ることで、家の壁に穴が開くことを防ぐことができる。）また、これにより、企業レベルでセキュリティ計画を策定し、セキュリティの再利用、コストの削減、スケジュールの短縮、およびセキュリティの信頼性の向上を図ることができる。

実装に関するヒント

セキュリティ活動は、個々に存在する補完的な文書またはセキュリティライフサイクルにて管理するのではなく、政府機関の SDLC ポリシーとガイドラインに物理的かつ論理的に組み込まなければならない。これにより、それらのポリシーとガイドラインの読者層が広がり、読者にとっては、不必要に多くの文書を参照しなくてもよくなる。当然のことながら SDLC へのセキュリティの統合では、より詳細な情報を提供する補足文書を参照することも必要となる。

SDLC にセキュリティを確実に組み込むための最も有効な方法は、包括的なリスクマネジメントプログラムを計画し、実施することである。（セクション 2.1.5 を参照） これにより、セキュリティコストと要件の統合化と、政府機関内の IT 投資家および IT 開発者にリスク情報を提供するための組込み式で繰り返し利用可能な認可プロセスを実現できる。

2.1.3 資本計画および投資管理プロセス

それぞれの政府機関は、OMB Circular A-11 に準拠して確立し文書化した CPIC プロセスを備えている。NIST SP800-65『IT セキュリティの資本計画及び投資管理プロセスへの統合(Integrating IT Security into the Capital Planning and Investment Control Process) 』では、セキュリティの統合と価値について詳しく述べている。本書では、SDLC へのセキュリティの統合に焦点をあてて、セキュリティの統合と価値について考察している。

以下に、本書を読む際に考慮すべき、NIST SP 800-65 の主要概念を示す。

- OMB Circular A-130 によると、CPIC プロセスとは、「情報資源に対する投資を継続的に特定、選択、管理し評価するための管理プロセス。このプロセスは、予算の編成と施行を結びつけるものであり、政府機関の任務および特定のプログラムの目的達成に焦点を置く。」と定義されている。セキュリティを CPIC プロセスに組み込むことによって、情報資源を完全かつ規律ある方法で計画、提供することができ、IT 投資に対するセキュリティを向上できる。

- CPIC プロセスへのセキュリティの組み込みは、組織の任務およびセキュリティ要件が、投資ライフサイクル全体を通して満たされることを確実にするための、7 段階の方法論から成る。

- それぞれのステップの役割と責任は、政府機関ごとに異なるが、これらのステップが CPIC プロセス全体を通して企業レベルまたは作業単位レベルで関与することによって、政府機関が資本計画および情報セキュリティの目標と目的を達成できるようになる。

- 政府機関は、OMB 資本計画と NIST ガイドラインに従って、GAO(会計検査院:Government Accountability Office)の最優良事例、および連邦政府による IT 投資のための三相投資ライフサイクルモデル)を適用することが求められる。

- 資本計画プロセスでは、情報セキュリティ管理策の実施と評価にかかる費用と、IT 資源の効果的な保護にかかる費用も、計上しなければならない。

2.1.4 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は、NIST SP 800-53 に記載の、連邦政府情報と情報システムの機密性、完全性および可用性を保護することためのセキュリティ管理策ファミリーに準拠すべきである。包括的なセキュリティアーキテクチャでは、現行のセキュリティサービス、ツールおよび専門知識を認識すること、予測されるビジネスニーズおよび要件を概説すること、および政府機関の文化と戦略計画に沿った実施計画を明確に述べることが求められる。通常、セキュリティアーキテクチャは、期待される結果（徴候と、さらなる調査/調整を必要とする要因）の特定、プロジェクトスケジュールの作成、必要なリソースの推定、およびプロジェクトの主要な依存関係の明確化などのタスクを遂行するための、統合スケジュールによって補足される。

2.1.5 NISTリスクマネジメントフレームワークにおける役割

本書は、セキュリティ機能と保証を SDLC に組み込むたの、サンプルロードマップを提供することによって、NIST リスクマネジメントフレームワークを補足する。本書はまた、それぞれの政府機関が独自の文化を持ち、システムの特性もそれぞれに異なることを考慮したうえで、追加活動として考えられる活動について詳しく述べている。これらの追加活動は、NIST リスクマネジメントフレームワークを補足する。NIST リスクマネジメントフレームワークに関する詳細は、NIST SP 800-39 (ドラフト),『情報システムのリスク管理 (Managing Risk from Information Systems: An Organizational Perspective) 』に記載されている。

2.2 レガシーシステムに対する考慮事項

多くの場合に組織は、情報セキュリティライフサイクルにおける考慮事項を、長期にわたって運用されてきたレガシーシステムにも適用している。レガシーシステムの中には、リスクマネジメントに関する決定事項(現在採用されているセキュリティ管理策を含む)を包括的に記述した、優れたセキュリティ計画を備えたものもある。また、中には、利用できるドキュメントが少ないシステムもある。いずれにせよセキュリティ考慮事項は、レガシーシステムにとっても重要であり、正しく適用し文書化すべきである。このようにすることで、管理策が実施されて効果的に機能することを確実にし、情報と情報システムを適切に保護できるようになる。

実装に関するヒント

セキュリティ要件と期待値の効果的な伝達は、極めて重要な、かつ、骨の折れるステップである。重要なのは、セキュリティ要件を具体的かつ理解しやすい用語を使って文書化することで、誰がどのような責任と説明義務を有するかを明確に把握できるようにすることである。媒体(メモ、契約書または期待に関する文書など)および内容の詳細さと複雑さは、扱いやすいレベルでなくてはならず、また、費用対効果も高くなければならない。これは、本書全体を通して取り扱う議題である。

2.3 SDLC における重要な役割と責任

情報システム開発では、多くの参加者が、一つ以上の役割を担う。これらの役割と肩書きの名称は、組織によって異なる。すべての参加者が、あるフェーズのあらゆる活動に関わるわけではない。それぞれのフェーズで、どの参加者の判断を仰ぐ必要があるかは、開発によっても組織によっても異なる。どの開発でも、情報セキュリティ担当者が、できるだけ早く、なるべく初期フェーズで関与することが重要である。以下に、重要な役職のリストを示す。組織によっては、単一の個人が複数の役割を担う場合もある。

表 2-1. SDLC におけるセキュリティ上の重要な役割と責任

役職	責任
運用認可権限者 (AO; Authorizing Official)	情報システムの運用に対する責任を負う、政府機関の責任者。運用を認可するにあたっては、システムの利用により生じる政府機関の業務や資産、個人、他の組織、および国家へのリスクが、受容可能なレベルであることが条件となる。任務遂行にあたって運用認可権限者は、(i) 完成したセキュリティ計画 (ii) セキュリティアセスメントレポート、および (iii) 情報システムの脆弱性を軽減または除去するための行動計画とマイルストーンに依存する。
最高情報責任者 (CIO; Chief Information Officer)	CIO は、組織の情報システムの計画、予算設定、投資、パフォーマンス、および調達を担当する。したがって、組織のエンタープライズアーキテクチャに適合する、最も効率的で効果的な情報システムを調達する際に、CIO は組織のトップに対してアドバイスし支援する。
設定管理者 (CM; Configuration Management Manager)	CM マネージャは、情報システムまたはネットワーク構成の変化に伴う影響を管理する。したがって、変更管理プロセスを合理化し、システムのセキュリティ状態に害を与える可能性がある変更を検知し、未然に防ぐ。
契約担当者 (Contracting Officer)	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担当者である。
契約担当者の技術代表者 (COTR; Contracting Officer's Technical Representative)	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。
情報システムセキュリティ担当者 (Information System Security Officer)	情報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。
IT 投資委員会(またはそれに相当するもの) (Information Technology Investment Board (or equivalent))	IT(情報テクノロジ)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。
法律顧問/契約代理人 (Legal Advisor/Contract Attorney)	調達プロセス中の法的問題に関して、チームへのアドバイスを担当する。
プライバシー担当者 (Privacy Officer)	調達中のサービスまたはシステムが、保護、流布(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確実に適合するようにする。
プログラムマネージャ/プログラム担当者 (情報のオーナー) (Program Manager / Official (Information Owner))	この担当者は、SDLC プロセス中に、情報システムのビジネスおよびプログラム関係者を代表する。プログラムマネージャは、セキュリティにおいて重要な役割を果たし、理想的にはシステムの機能要件を詳細に認識する。

役職	責任
QA/テストディレクター (QA/Test Director)	QA/テストディレクターは、システムテストと評価を担当する。QA/テストディレクターは、種々のプログラムのリソースとして機能し、プログラムマネージャおよび顧客と連携して、テスト計画の策定と実施を支援する。また、システムの仕様をレビューし、テストのニーズを決定し、プログラムマネージャと協力して、フィールドテストに向けた活動を計画する。
政府機関の上級情報セキュリティ責任者 (Senior Agency Information Security Officer (SAISO))	最高情報セキュリティ責任者(CISO)とも呼ばれる SAISO は、SDLC へのセキュリティの組込みに関するポリシーの普及と、情報セキュリティのための企業基準(enterprise standards)の策定を担当する。SAISO は、組織の情報セキュリティリスクを特定、評価し、最小限に抑えるための、適切な構造化方法論を組織に導入する際に、中心的な役割を果たす。
ソフトウェア開発者 (Software Developer)	ソフトウェア開発者は、アプリケーション、ソフトウェア、およびインターネット/イントラネットサイトのプログラムのコーディング(「セキュアなコーディング」を含む)を担当する。また、設定管理者(CM manager)と協力して、設定管理(CM)問題を特定、解決し、管理策を実施する。
システム設計者 (System Architect)	システム設計者は、アプリケーション全体のデザイナー兼インテグレータとして、全体的な設計アーキテクチャを策定し、そのアーキテクチャの概念的統合性を、プロジェクトのライフサイクル全体を通して維持する役割を担う。システム設計者は、プロジェクトチームによる技術的作業の成果物(設計、仕様、手順およびドキュメントを含む)の品質を保証しなければならない。
システムオーナー (System Owner)	システムオーナーは、情報システムの調達、開発、統合、修正、運用および保守を担当する。
その他の参加者 (Other Participants)	情報システム開発における役職の数は、情報システムの複雑さに伴って増大する可能性がある。ゆえに、開発を確実に成功へ導くためには、開発チームの全メンバーの協力が欠かせない。情報セキュリティ担当者は、開発プロセス全体にわたり重要な決定を行う必要があるので、プロセスのできるだけ早い時期に関与する必要がある。システムユーザは、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開発を支援する。参加者には、IT、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ことがある。

第 3 章

SDLC へのセキュリティの組み込み

本セクションでは、SDLC へのセキュリティの組込みに役立つ考慮事項について述べる。セキュリティ考慮事項は、SDLC の個々のフェーズにおいて特定される。これにより組織は、ビジネスアプリケーションとセキュリティ要件を共に発展させることができ、システム開発におけるバランスのとれたアプローチを実現できるようになる。図 3-1 に、開発フェーズによって構成される、プロセスの全体図を示す。

図 3-1 SDLC の概念図

読者に対して明確で簡潔なガイダンスを提供するために、次のセクションでは以下の様式で、ライフサイクルの各フェーズを記述する。

- そのフェーズを簡単に説明する。
- 一般的なコントロールゲート、つまり、ライフサイクルにおいて、システムをいつ評価するか、また、プロジェクトの継続、方向転換、中断を経営陣がいつ決定するかを示すポイントを記述する。コントロールゲートは、組織ごとに調整できるよう、柔軟でなければならない。コントロールゲートは、組織に対して、システム開発がライフサイクルの次のフェーズに移る前に、セキュリティ考慮事項がシス

テムに反映されていること、十分なセキュリティが組み込まれていること、特定されたリスクが十分に理解されていることを確認するための機会を与えてくれるため、有用である。

- そのフェーズの主なセキュリティ活動を特定し、記述する。また、それぞれの活動について、以下の領域ごとに定義を加える。

  — 解説 。活動を詳細に記述し、活動を実施するにあたって考慮すべき事項を説明する。

  — 期待される結果。共通タスクによって生成される結果とアーチファクトを、これらの成果物の SDLC への前方統合/後方統合に関する提案とともに、リスト形式で示す。

  — 同時化。SDLC が柔軟に実施され、各フェーズのタスクと成果が適切かつ一貫して関係者に伝えられ、調整されることを確実にするための、フィードバックループ。

  — 相互依存性。他のタスクとの主な相互依存性を示す。これは、セキュリティ統合活動が、他の IT プロセスによって悪影響を受けないようにするためにも、重要である。

3.1 SDLC フェーズ: 開始

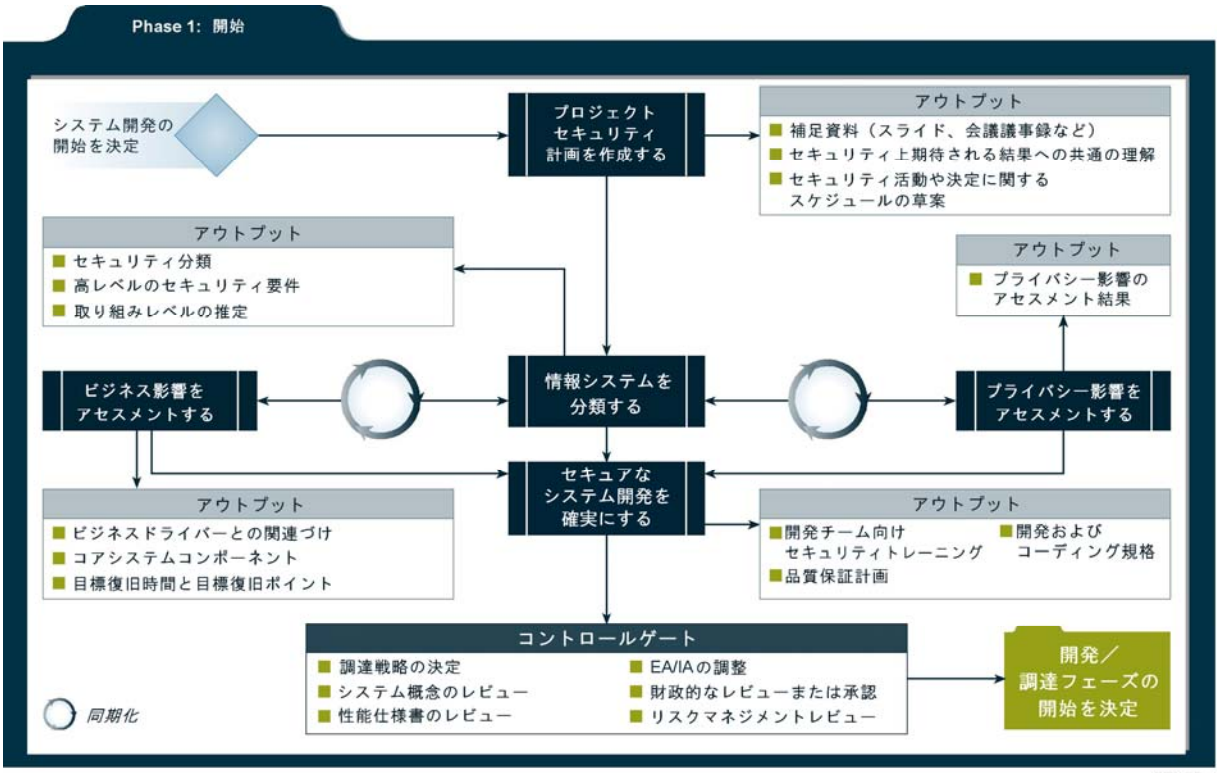

図 3-2 セキュリティ考慮事項の開始フェーズへの関連づけ

3.1.1 解説

SDLC の 1 番目のフェーズであるこのフェーズでは、セキュリティ考慮事項が、セキュリティの入念な、かつ早い段階での統合の鍵となる。また、これにより組織は、脅威、要件、および機能性と統合に関する制約を考慮するようになる。この時点においてセキュリティは、情報セキュリティオフィスからの入力情報をもとに、ビジネスリスクの観点でとらえられる。たとえば、政府機関が、(自身が運営する)著名なウェブサイトが改変されたり、重要なビジネスの最中に利用できなくなることによって、国民の信頼を失うといったリスクを特定することも考えられる。本フェーズの主なセキュリティ活動には、以下のものが含まれる:

- 機密性、完全性および可用性に関するビジネス要件を概説する。
- 情報分類を決定し、個人情報などの取り扱いに注意を要する情報を伝送、保存または作成する際に適用される、特殊取り扱い要件(special handling requirement)を特定する。
- プライバシーにかかわるすべての要件を定義する。

適切なリスクマネジメント計画を早い段階で作成し、役職員の意識向上を図ることで、組織は、コストを削減し、時間を節約できる。セキュリティに関する議論は、開発プロジェクトから切り離すのではなく、プロジェクトの一環として行うべきである。これは、プロジェクト担当者が、ビジネス決定事項、およびそれらの決定が開発プロジェクト全体に及ぼすリスクを的確に理解するためにも、重要である。

3.1.2 コントロールゲート

本フェーズの一般的なコントロールゲートには、以下のものが含まれる:

- **調達戦略の決定** 残りの開発プロセスを通して用いる調達戦略を決定する。
- **システム概念のレビュー** システム概念が、実現性があって、完全で、達成可能であるか、また、組織の使命目的と予算上の制約を満たしているかをレビューする。
- **性能仕様書のレビュー** 現在定義されているすべてのセキュリティ要件が、システムの初期設計に反映されることを確実にするために、性能仕様書をレビューする。
- **エンタープライズアーキテクチャの調整とセキュリティサービスの調整** IT ビジョン、標準およびビジネス要件を調和させるためにエンタープライズアーキテクチャを調整する。また、現在実施されている(または、これから実施する予定である)セキュリティサービスを調整する。
- **財政的なレビュー** システムが、CPIC アーチファクトとガイダンスに適合するかを確認する。この際、リスクマネジメントに要する費用とのバランスを考慮すること。
- **リスクマネジメントのレビュー** NIST リスクマネジメントフレームワークガイドラインに準拠するレビュー活動であり、システムリスクを管理する上での曖昧さを減らすために行う。これには、情報システムのセキュリティ分類結果(情報の種類、影響レベル、および最終的なシステムセキュリティ分類など)のレビューが含まれる。

3.1.3 主なセキュリティ活動

3.1.3.1 セキュリティ計画作成を開始する

説明:	開始フェーズにおけるセキュリティ計画作成では、次のようなことから着手する。 • システム開発におけるセキュリティ上の重要な役割を特定する。 • セキュリティ要件の元となるもの(関連する法律、規定および基準など)を特定する。 • すべての主要関係者が、セキュリティ上の意味合い、考慮事項および要求事項などに関して、共通の理解を持てるようにする。 • キーセキュリティマイルストーンの草案を策定する。これには、タイムフレームや、セキュリティ手順の実施が迫っていることを示す開発トリガー(development trigger)が含まれる。 このように早い段階で着手することで、システム開発者は、セキュリティ要件と関連する制約を(早い段階で)定義し、プロジェクトに組み込むことができる。また、このような取り組みは、プロジェクトリーダーに対して、多くの決定事項にはセキュリティ上の意味合いがあり、プロジェクトの進行中に正しく評価しなければならないことを思い出させてくれる。 **セキュリティ上の役割を明確化する** 情報システムセキュリティ担当者(ISSO)を決定することは、重要なステップである。この担当者を決定する際には、担当者が当該業務を遂行するために割く時間、職務の遂行に必要なスキル、担当者が責任を効果的に果たすための能力をどの程度有しているかなどを考慮しなければならない。プロセスの初めに ISSO を決定することで、プロセスの初めにリスクをもとに決定した事項に対する重要な洞察がもたらされ、チームメンバーがセキュリティをシステム開発に組み込む際に、ISSO の支援を得ることができるようになる。 **セキュリティの統合に関する関係者の意識を向上させる** ISSO は、ビジネスオーナーや開発者が、セキュリティ手順、要件および期待される結果を早い段階で理解することを支援し、セキュリティ計画が SDLC の初期段階で作成されることを確実

	にする。トピックスには、以下のものが含まれる: • セキュリティ上の責任 • セキュリティ報告メトリクス • 共通セキュリティ管理策(存在する場合のみ) • 承認および運用認可プロセス • セキュリティテストおよびアセスメントテクニック • セキュリティに関するドキュメントと要件に関するドキュメント • セキュアなデザイン、アーキテクチャ、およびコーディング慣行 • セキュリティ調達に関する考慮事項 • 開発スケジュールおよびリソース影響を扱う主な活動(実環境におけるテスト、運用認可、およびトレーニングなど) **プロジェクト計画を作成する** (開発プロジェクトスケジュールに組み込まれる)セキュリティマイルストーンのためのプロジェクト概要を策定することにより、変更が生じた場合でも、適切な計画作成を行うことができる。この段階で行う活動は、セキュリティ活動に先立つ意思決定活動であることもある。
期待されるアウトプット:	• 補足資料(スライド、会議議事録など)。 • セキュリティ上期待される結果(security expectation)への共通の理解。 • セキュリティ活動や決定に関するスケジュールの草案。
同期化:	マイルストーンまたはセキュリティ会議を複数回にわたって計画し、各セキュリティ考慮事項がシステム開発全体を通して討議されるようにする。
相互依存関係:	プロジェクトスケジュールには、セキュリティ活動を含めるようにし、スケジュールやリソースに関する将来の決定に備えるようにする。
実施に関するヒント	
• 開始フェーズのセキュリティ計画には SDLC 全体に対する準備を含めること。これには、セキュリティに関わる主要マイルストーンと成果物、ツールおよび技術の明確化が含まれる。調達を要するアイテム(テストツールやアセスメントツールなど)に関しては、特別な配慮が必要となる。 • プロジェクトのアーチファクト(会議議事録、ブリーフィング、役割を明確に示した資料など)の多くは、標準化が可能であり、開発者が適切なレベルの活動計画を作成できるよう、開発者に提供することができる。 • 実際に会って行う会議は、参加者の理解と意識を評価する機会を与えてくれる。 • 政府機関が、同一の ISSO に、複数のシステムを割り当てている場合、計画中のアプローチによって、それらのシステムの多重処理機能も向上する。(たとえば、共通システムまたは共通組織に所有権を付与するなど)。 • SDLC の初期段階において、政府機関の記録管理担当者、プライバシー担当者、および情報公開法(FOIA)担当者のアドバイスを受けることで、該当する法律や政府機関のポリシーに準拠できるようにすること。	

3.1.3.2 情報システムを分類する

説明:	NIST リスクマネジメントフレームワークのステップ 1 に該当するセキュリティ分類は、政府機関のビジネスおよび IT 管理機能にセキュリティを組み込むための重要なステップを提供し、情報システム間のセキュリティ標準化基盤の確立を支援する。セキュリティ分類は、EA によって定義され、NIST SP800-60『情報および情報システムの タイプとセキュリティ分類のマッピングガイド(Guide for Mapping Types of Information and Information Systems to Security Categories)』に記述されているように、どの情報が、政府機関のどの事業部門をサポートするかを特定することから始まる。以降のステップでは、機密性、完全性および可用性の観点から、セキュリティを評価する。このような評価を行うことで、政府機関のミッション、情報および情報システムと、費用効率が高い情報セキュリティを強く結びつけることができる。 FIPS 199『連邦政府の情報および情報システムに対するセキュリティ分類規格(Standards for Security Categorization of Federal Information and Information Systems) 』は、組織の情報と

	情報システムのセキュリティ分類を確立するための、標準化されたアプローチを提供する。FIPS 199 と姉妹関係にある NIST SP 800-60 は、情報および情報システムを分類するためのプロセスロードマップと、情報分類法を提供する。セキュリティの分類は、情報システムに悪影響を及ぼす特定のイベントが発生した場合に、そのイベントが組織に与える潜在的影響に基づいて分類される。つまり、情報システムは、割り当てられたミッションの完遂、資産の保護、法的責任の履行、日常機能の維持、および個人の保護などの機能があり、それが損なわれた場合の影響に基づいて分類されるのである。また、組織が必要とするセキュリティの分類は、情報システムの運用による組織に対するリスクを査定する場合に、脆弱性および脅威の情報とともに使用する必要がある。 FIPS 199 はセキュリティ違反があった場合(機密性、完全性、可用性の損失)に、組織または個人に影響する可能性について、3 つのレベル(低、中、高)を定めている。セキュリティの分類基準と手引きは、情報システム用のセキュリティ管理策を、組織が適切に選択する場合に役立つ。
期待されるアウトプット:	• セキュリティ分類 – セキュリティ分類プロセスにとって重要なことは、調査結果、重要な決定事項、および情報システムのセキュリティ分類プロセスを裏付ける根拠(システムセキュリティ計画に含まれるもの)を文書化することである。 • 高レベルのセキュリティ要件。 • 取り組みレベルの推定 – 取り組みレベルは、セキュリティ分類の結果を、NIST SP 800-53 の最低限のセキュリティ管理策と、NIST SP 800-53A『連邦政府情報システムのためのセキュリティ管理策アセスメントガイド(Guide for Assessing the Security Controls in Federal Information Systems)』のアセスメント手順に適用することによって、引き出すことができる。
同期化:	システムに重要な変更が加えられた場合や、ビジネスインパクト分析が更新された場合には、セキュリティ分類を再度実施する。
相互依存関係:	• ビジネスインパクト分析: 政府機関の担当者は、各タスク活動のパフォーマンスの評価に、セキュリティ分類情報とビジネスインパクト分析情報を相互利用することを、考慮すべきである。セキュリティ分類とビジネスインパクト分析には共通の目的があり、政府機関は、これらの活動を個々のシステムに対して実施し、結果を利用してセキュリティの正確さを確保すべきである。 • CPIC と EA: ビジネス認可のアーキテクチャ(business-approved architecture) [3]なしには IT 投資が行われないのと同様に、セキュリティライフサイクルの初期段階でセキュリティ分類を実施することは、ビジネスを可能とする活動であり、EA プロセスや CPIC プロセス、マイグレーションやアップグレードに関する決定に必要な情報を提供する。 • システム設計: 様々な影響レベルを念頭においてシステムアーキテクチャーを理解し、設計することによって、企業内の共通セキュリティゾーンを利用したセキュリティサービスと保護による、「規模の経済(economies of scale)」を実現できる。この種のアプローチでは、セキュリティ分類プロセスによって得ることができる政府機関の情報の種類およびデータの種類を、的確に理解することが求められる。 • 緊急時/災害時復旧計画作成: 緊急時/災害時復旧計画作成担当者は、データの種類が複数あり、その影響レベルもそれぞれに異なる情報システムをレビューすべきである。また、アプリケーションを類似の影響レベルごとにグループ化し、グループごとに十分に保護されたインフラを確立することを検討すべきである。これにより、適切な緊急時/災害時保護管理策を効果的に適用することができ、低い影響システムに過剰な保護を施こすことを回避できる。 • 情報共有とシステム相互接続に関する契約書: 政府機関の担当者は、諸機関間の接続を評価する際に、集約された個々のセキュリティ分類情報を利用すべきである。
実施に関するヒント	
• 政府機関は、適切なレベルのミッションサポートと、現行および将来のセキュリティ要件の入念な実施を確実にするためにも、システムレベル分類の有効性を、政府機関の優先事項の観点から評価するための、正式なプロセスを確立しな	

3 2006 年 12 月発行の FEA Consolidated Reference Model Document, Version 2.1.

ければならない。これにより、システムに対する比較可能な評価を促進できると同時に、共通セキュリティ管理策を導入し、多重防護を確立することができるなど、多くの便益がもたらされる。

- 政府機関の担当者は、システムに暫定的に割り当てられた影響レベルが適切であるかをレビューし、必要な場合は調整を行うべきである。この際、レビュー対象システムを使用する組織、システムが使用される環境、その組織のミッション、システムをどのように使用するか、および接続性などを考慮すること。具体的には、以下のものが含まれる: 組織のミッションの重要性、ライフサイクルとタイミング上の意味合い、設定およびセキュリティポリシー関連の情報、特殊取り扱い要件など。
- システム全体のセキュリティ分類が中位または高位レベルに分類される場合であっても、機密性、完全性、および／または可用性を保護するための SP800-53 の各セキュリティ管理策には、高水位マーク(それぞれのセキュリティ目的への影響レベルの中で、最も高いレベルをシステムの影響レベルとする)の考えが適用される場合がある。これは、それらの管理策が完全に独立していて、コストや他の懸念事項によって、高水位マークを適用すべきであることが推奨される場合に相当する。システム分類が完了すると、リスクマネジメントアプローチによる管理策の選択が行われる。また、正当と認められる相違(justifiable variance)に関しては、文書化されて、システムのセキュリティ計画に記載される。
- 政府機関は、システムが扱う情報の種類を集約するうえで、考慮すべき要素がいくつか存在することを認識すべきである。これらの要素を考慮するとき、システムの機密性、完全性、および／または可用性への影響の分類結果を揺るがすような、以前には見えなかった懸念事項が浮上することがある。これらの要素には、データの集約、システムにとって不可欠な機能、酌量すべき事情、およびシステムに関する他の要因が含まれる。

3.1.3.3 ビジネス影響をアセスメントする

説明:	政府機関の事業部門へのシステムインパクトの評価によって、特定のシステムコンポーネントと、システムが提供する重要なビジネスサービスが関連づけられる。その情報は、システムコンポーネントに障害が発生した場合のビジネスおよびミッションへの影響を特定するために利用される。ライフサイクルの初期段階に生成されるこの草案によって、関係者は、IT とセキュリティに関する重要な決定事項を知ることができる。このタスクでは、セキュリティ分類において特定された可用性への影響レベルも考慮しなければならない。ビジネス影響アセスメントテンプレートに関しては、NIST SP 800-34 『IT システムにおける緊急時対応計画ガイド(Contingency Planning Guide for Information Technology Systems)』を参照のこと。
期待されるアウトプット:	• このシステムがサポートする事業部門と、それらの部門が受ける影響を特定することができる。 • 必要最低限の機能を維持するために必要な、(システムの)コアコンポーネントを特定することができる。 • ビジネスに影響が及ぶまでの、システムの許容ダウン時間 (システムの)コアコンポーネントを特定することができる。(目標復旧時間の割り出しに役立つ)。 • データの損失に対するビジネストレランス(business tolerance)を特定することができる。(目標復旧時間の割り出しに役立つ)。
同期化:	• ビジネス影響アセスメント結果は、定期的にレビューし、主要な開発決定が行われた場合(新しい機能の追加)や、システムの目的と範囲が大幅に変更された場合に、更新すべきである。 • システムが成熟するにつれて、主要 IT コンポーネントをより詳しく評価できるように、ビジネス影響アセスメントを拡張すべきである。
相互依存関係:	• ビジネス影響アセスメントは、緊急時対応計画プロセスにおける主要なステップである。ビジネス影響アセスメントによって、システム要件、プロセス、およびの相互依存性の特徴づけを、より正確に行えるようになる。また、ビジネス影響アセスメントが生成する情報を使用して、緊急時対応要件と軽減方法を決定することができる。 • ビジネス影響アセスメントのインプットと目的は、FIPS 199 のセキュリティ分類活動のインプットと目的に類似している。結果としてビジネス影響アセスメントは、ビジネス上のすべてのドライバー(driver、誘因)が適切に取り上げられるようにするための、抑制と均衡を提供する補足活動となる。
実施に関するヒント	
• この情報の一部は、イニシアティブの投資対効果検討書の原本から引き出すことができる。	

- より規模が大きく複雑な開発では、関係者会議を開いて、考えられる関連と影響をブレーンストーミングすることを検討すること。
- 可能な場合は、データと情報を多目的に再生利用すること。分類結果は、ビジネス影響アセスメント(BIA)、災害復旧（DR）、緊急時対応計画（CP）と事業継続（COOP）に関する決定に再生利用できる。分類は、災害復旧のプライオリティーを反映したものでなければならない。そうでないとすると、分類が適切なレベルで行われなかったか、あるいは、災害復旧プライオリティーが正しく設定されていないと考えられる。
- ビジネス影響アセスメント結果は、サービスプロバイダとの間で交わすサービス内容合意書の要件や目標を定めるために利用できる。

3.1.3.4 プライバシー影響をアセスメントする

説明:	新しいシステムを開発するとき、そのシステムがプライバシーにかかわる情報を伝送、格納、作成するかどうかを考えることが重要である。これは、通常、セキュリティ分類プロセスにおいて情報の種類を特定する際に、特定される。開発中のシステムがプライバシーにかかわる情報を扱うと考えられる場合は、システムのオーナーが、適切な保護対策とセキュリティ管理策を特定し実施しなければならない。これには、プライバシー情報インシデントへの対応要件と報告要件が含まれる。政府機関の多くは、プライバシーに関する考慮事項に対処するためのワンテップモデルまたはツーステップモデルを使用している。ワンステップモデルは、政府機関のシステム一覧に記載されているすべてのシステムが、プライバシーインパクトアセスメントを策定することを求めている。プライバシーインパクトアセスメントには、プライバシー情報であるかどうかを判別するための基準と、情報を適切に保護するためのセキュリティ管理策を文書化したものが含まれる。これとは対照的にツーステップモデルは、すべてのシステムに対して限界値分析を行い、それぞれのシステムのプライバシーインパクトアセスメントを実施すべきか否かを判断する。正の答えがでた場合、プライバシデータと管理策に対するより詳細な評価を、プライバシーインパクトアセスメントの形式で実施する。どちらのモデルであっても結果は文書化され、システムセキュリティ計画に盛り込まれて、適切に維持される。
期待されるアウトプット:	プライバシー情報がどこで、どの程度収集、格納、作成されるかについて、詳細を提供する、プライバシーインパクトアセスメント。
同期化:	重要な決定が行われた場合や、システムの目的と範囲が大幅に変更された場合に、レビューし、更新する。
相互依存関係:	• FIPS199 のセキュリティ分類は、情報の種類(プライバシー情報など)を特定するための最初のステップである。 • セキュリティ管理策を特定しアセスメントすることによって、プライバシー情報を保護するための管理策追加の必要性を判断できる。 • これは、システムのセキュリティ計画、緊急時対応計画、およびこれらの文書に含めることもあるビジネス影響分析に影響を及ぼす。

実施に関するヒント

- プライバシー情報ガバナンス(Governance for Privacy Information): 1974 施行のプライバシー法, 5 U.S.C. § 552A。
- 2002 年施行の電子政府法は、1974 施行のプライバシー法のプライバシー保護要件を強化したものである。 これらの公法によると、連邦政府機関は、個人に関する情報の収集、普及または開示について、特定の責任を持つとされている。
- 2003 年 9 月 29 日に発行された OMB 覚書「2002 年施行の電子政府法のプライバシー規定の実施に関する OMB ガイダンス(OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002)」により、電子政府法のプライバシー規定が発効された。このガイダンスは、このガイダンスは、(人間が認識できる形で)個人を特定できる情報に適用される。これには、名前、住所、電話番号、社会保障番号、電子メールアドレスなどが含まれる。
- OMB M-06-16 と OMB M-07-17。

3.1.3.5 セキュアな情報システム開発プロセスを確実に使用する

説明:	初期段階におけるアプリケーションセキュリティの主な責任は、開発チームが負うことになる。彼らは、アプリケーションの詳細な機能について、最も深く理解しており、機能的挙動およびビジネスプロセスロジックにおけるセキュリティ上の欠陥を特定する能力を備えている。彼らは、第 1 レベルの防御となり、セキュリティ構築の機会を提供する。重要なことは、彼らの役割が他の者によって肩代わりされたり、軽減されないようにすることである。彼らに期待されることを伝えることは、コードレベルにいたるまでの保護環境を計画して、実現するための鍵となる。考慮すべき事項には、以下のものが含まれる: ***開発のためのセキュアな運用概念(Secure Concept of Operations (CONOPS) for Development)。*** 組織は、自身の環境におけるセキュアな開発のための CONOPS ドキュメントを作成し、コードリポジトリ用の緊急時対応計画を実施すべきである。なぜならば、ソースコードは、ソフトウェアとシステム開発の主要な作業生産物であり、開発環境への妨害が発生した場合に、適切に保持しなければならないからである。 ***規格とプロセス。*** システム開発は、セキュアな慣行を考慮した標準プロセスを用いて実施すべきである。その標準プロセスは、文書化されていて、繰り返し利用可能であることが求められる。 これを達成するためには、システムが要求する保証レベルを満たすための適切なセキュリティプロセスを決定し、文書化しなければならない。システムの保証要件が高い場合には、追加の管理策を開発プロセスに組み入れることもある。 ***開発チーム向けのセキュリティトレーニング。*** 主要な開発者に対して、追加的なセキュリティトレーニングが必要な場合がある。このようなトレーニングは、開発者が現存の脅威を理解し、考えられる製品の悪用方法を把握すると同時に、セキュアな設計とコーディング技法を身につけることを支援するために行われる。また、これにより開発者は、よりセキュアなデザインを作成し、開発プロセスの早い段階で重要問題に対処できるようになる。 ***品質管理。*** 品質管理(計画作成、保証および管理を含む)は、情報システムの欠陥を最小限にとどめ、システムを適切に実行するための鍵となる。また、品質管理によって、システムの悪用や誤使用(意図的であるなしにかかわらず)につながるギャップ(セキュリティホール)を少なくすることができる。 ***セキュアな環境。*** SP800-53 の記述のとおり、システム開発環境は、FISMA の最低限の順守基準を満たさなければならない。これには、ワークステーション、サーバー、ネットワークデバイスおよびコードリポジトリが含まれる。他の運用システムや環境と同様に、開発環境も運用認可を受けなければならない。セキュアな開発環境は、セキュアなソフトウェアとシステムの開発につながる。 ***セキュアなコード慣行とリポジトリ。*** コードリポジトリに対しては、特に、チェックイン/チェックアウト機能による分散型コードコントリビューションをサポートするシステムについては、特別な注意を払わなければならない。コードリポジトリへのアクセスには、役割ベースのアクセスを使用する。アクセスログは、セキュアな開発プロセスの一環として、定期的にレビューする。コードは、標準的技法を用いて開発する。前述の CONOPS の中で重要なのは、セキュアなコーディングパターンとコンポーネントを確立し、維持することである。セキュアなコーディングパターンには、セキュリティ上の要件を満たしつつ特定の機能要件を満たす方法を示す、コードレベルの例と関連文書が含まれる。開発者は、これらのパターンを再利用して、すべてのソフトウェアコンポーネントを安全に開発することができる。また、これによりすべてのコンポーネントが、組織による綿密な検査を経た後に、採用されるようになる。可能な場合、セキュリティ検定に合格したソフトウェアコンポーネントを、将来のソフトウェア開発とシステム統合に再使用できるコンポーネントとして、保持すべきである。 システム開発者とセキュリティ代表者は、一つのチームとして、セキュアな開発環境に対する有用で費用対効果に優れた貢献を実現するためのステップについて、合意を得るべきである。
期待されるアウトプット:	• 開発フェーズにおけるセキュリティトレーニング計画。 • 計画された品質保証技術と、その技術がもたらす成果物、およびマイルストーン。 • 開発およびコーディング規格(開発環境を含む)。

同期化:	完了品テストとセキュリティテストから学んだ教訓が、製品に欠陥が含まれるのを防ぐための、開発プロセスおよび開発標準の調整に適しているかどうかを評価する。
相互依存関係:	• IT 開発標準には、セキュリティを損なわせることなく、開発プロセスに付加価値を付けるような、適切な方法論を含めるべきである。 • システム開発トレーニングおよびオリエンテーションには、基本的なセキュリティ意識向上プログラム、トレーニングおよび教育と、環境に特化した専門の意識向上プログラム、トレーニングおよび教育を含めるべきである。

実施に関するヒント

- 最新のアプリケーションセキュリティ欠陥と攻撃方法を理解することは、それらの欠陥や攻撃からシステムを保護するためには不可欠である。開発チームとテストチームに対するアプリケーションセキュリティトレーニングの実施は、前述の問題や技術への理解を向上させると同時に、よりセキュアなシステムの開発を可能にする。開発者が、開発フェーズにおいて何を求め、何をテストすべきかを理解していれば、品質保証（QA）にリリースされるセキュリティ欠陥の数が少なくなる。また、QA テストチームがアプリケーションセキュリティについてしっかりとした教育を受けていれば、製品が次のテストフェーズに移行する前に、セキュリティ問題を特定できる可能性が高まる。そのようなトレーニングは、システム全体のセキュリティへの信頼の向上につながる。また、アプリケーションセキュリティに関するトレーニングを実施することによって、QA テストチームがアプリケーションセキュリティの重要性をしっかりと認識できるようになる。
- 開発チームが気づいている欠点に関しては、早期に対処すべきである。システムの内部の仕組みについて十分な理解を要する複雑な攻撃が、悪意のある攻撃者のレベルでは実施できないと仮定すべきではない。システムオーナーが「隠れた情報」とみなしていた情報が、攻撃者によって「発見」されるという事件が、一度ならず、複数回にわたって発生している。
- システムのセキュリティ欠陥の可能性を減らすためには、セキュリティに焦点を当てた追加要素を検証した後に、既存のコーディング規格または開発手引き文書に取り入れるべきである。これらの規格は、C++、Java、HTML、JavaScript および SQL など、組織が使用しているすべてのソフトウェア開発言語を網羅していなければならない。

3.2 SDLC フェーズ: 開発／調達

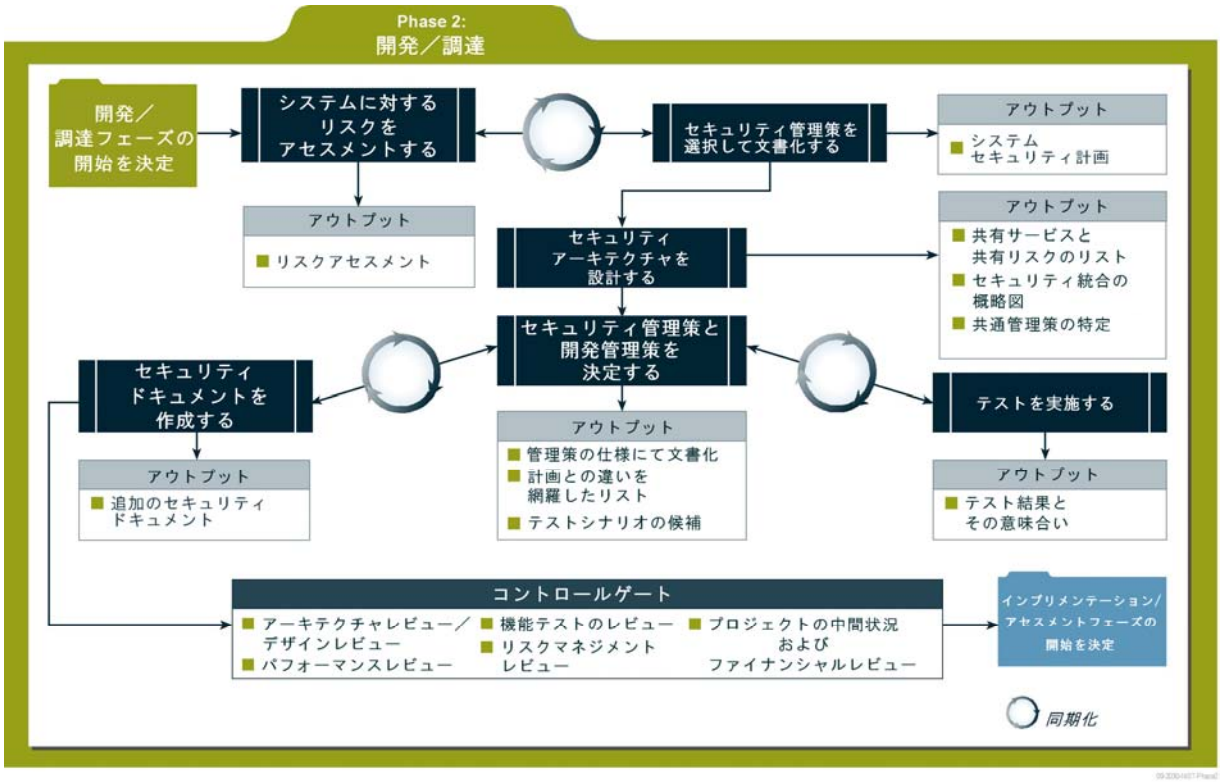

図 3-3 セキュリティ考慮事項の開発／調達フェーズへの関連づけ

3.2.1 解説

本セクションでは、SDLC の 2 番目のフェーズに特化したセキュリティ考慮事項を取り扱う。本フェーズの主なセキュリティ活動には、以下のものが含まれる:

- リスクアセスメントを行い、その結果を使ってベースラインセキュリティ管理策を補足する。
- セキュリティ要件を分析する。
- 機能的テストおよびセキュリティテストを実施する。
- システム承認と運用認可のドキュメントを用意する。
- セキュリティアーキテクチャを設計する。

本セクションでは、情報セキュリティコンポーネントを連続したトップダウン形式で示しているが、必ずしもこの順番で進める必要はない。複雑なシステムのセキュリティ分析は、一貫性と完全性が達成されるまで、繰り返し実施されることになる。

3.2.2 コントロールゲート

本フェーズの一般的なコントロールゲートには、以下のものが含まれる:

- **アーキテクチャ/デザインレビュー**　計画されたシステム設計と、他のシステムとの統合の可能性を評価し、共有サービスや共通セキュリティ管理策（認証、災害復旧、侵入検知、インシデント報告など）のシステムへの組み込みを検討する。
- **システムパフォーマンスレビュー**　システムが、文書化されたオーナーの期待を満たしているか(あるいは満たすことが可能か)を評価し、システムが不適切に使用された場合に、予想可能な形で動作するかをチェックする。（たとえば、リソースが予想されるレベルで大量にロードされた場合に、可用性とデータの完全性を、システムがどの程度まで維持できるか。）
- **システム機能のレビュー**　機能要件が詳細に定義されていて、テストできる状態であるかをチェックする。
- **プロジェクトの中間状況およびファイナンシャルレビュー**　推定努力レベルの大きな変動を検出するためのレビュー。これは、費用便益率を監視し、効果的な決定を継続して行うためにも重要である。
- **リスクマネジメントに関する決定事項の継続的なレビュー**　これは、上述のレビューのために必要となることもあれば、システム／システムのセキュリティ管理策／システム要件の変更に伴い実施されることもある。

3.2.3 主なセキュリティ活動

3.2.3.1 システムに対するリスクをアセスメントする

説明:	リスクアセスメントの実施に関しては、NIST SP 800-30『IT システムのためのリスクマネジメントガイド（Risk Management Guide for Information Technology Systems）』を参照のこと。 リスクアセスメントの目的は、システムデザイン、システム要件、および(セキュリティ分類プロセスから導き出される)必要最低限のセキュリティ要件に対する担当者の現在の知識を評価して、予想されるリスクを軽減するための彼らの能力を測定することにある。アセスメント結果によって、当該セキュリティ管理策が適切な保護を提供することが示されるか、あるいは、更なる計画が必要な分野がハイライトされるようでなければならない。アセスメントを成功裏に行うためには、システムドメイン内の各分野に精通している者（ユーザ、技術者、オペレーションエキスパート）の参加が必要である。 セキュリティリスクアセスメントは、設計仕様の承認が行われる前に実施すべきである。なぜならば、このアセスメントを行った結果、仕様の追加または調整が必要となることがあるからである。 組織は、開発／調達中のシステムのセキュリティについて考慮することに加えて、そのシステムに直接または間接的に接続される他のシステムへの影響についても考慮しなければならない。たとえば、接続される他のシステムから継承した共通管理策が存在する場合や、軽減すべき追加のリスクが存在する場合などへの対処が考えられる。このような場合、脅威と脆弱性に対するより包括的な見解を得るために、エンタープライズレビューを実施することが考えられる。
期待されるアウトプット:	洗練されたリスクアセスメント。このアセスメントは、システムへの潜在的リスク、設計上の既知の欠点、特定されたプロジェクト制約、およびビジネスと IT コンポーネントに対する既知の脅威をより正確に反映した、成熟したシステム設計にもとづくものである。前述の要件は、この時点で、システムに特化した管理策に移行する。

同期化:	このリスクアセスメントは、システム開発のより成熟した段階で実施されるため、(そこにたどり着くまでに)先に完了したセキュリティス手順(ビジネス影響分析またはセキュリティ分類など)を再実行することも考えられる。開発が計画どおりに進むことは稀であり、要件は変化するものである。
相互依存関係:	• セキュリティ分類は、情報の種類にもとづくリスクアセスメント情報を提供する。 • 情報と情報システムに必要な保護を施すために、リスクアセスメントにもとづき、追加のセキュリティ管理策または補足管理策を計画(または修正)することがある。

実施に関するヒント

- どのような組織であっても、内部ソースによる脅威が発生する確率は極めて高い。システムの使用が認められた職員やシステム開発者によるシステムの不適切な使用は、実際に脅威となる。そのような職員はシステムに対するアクティブなアカウントを持つと考えられるため、なおさらである。セキュリティ慣行には、システムおよびシステムをサポートするプロセスに対する、第三者の監査が含まれなければならない。内部ソースを継続的に監視し、完全性ベースツールを使用してシステム設定の監視と管理を行うことは、有用である。これにより、監査ログを自動的に、かつ、一括して収集、関連づけ、分析できるツールが提供される。
- 既知のコンポーネントの脆弱性に関しては、NVD (National Vulnerability Database)(http://nvd.nist.gov)を参照し、それらの情報をもとに、脆弱性を軽減するための管理策を策定すると良い。策定した管理策は、テストが必要になる。
- 複数のオーナーを持つシステム(異なる複数のドメインにまたがることもある)を扱う上で重要なことは、受け継がれた共有のリスクを特定し、それらのリスクに対処することである。
- システムに必要な厳格さとシステムの複雑さによっては、第1インターフェース以上(第 2 インターフェース、第 3 インターフェース、...)のデータフロー／情報共有を行う必要がある。そうしないと、未知の脆弱性を継承しかねない。
- それ以外の継承されたリスクは、システムに関する資料を供給するによって評価されることもある。サプライチェーンのリスクは、正しく理解、評価し、偽造した資料、違法コピーした資料、ライセンスのない資料、または意図的に盗んだ資料を使用することがないようにする。

3.2.3.2 セキュリティ管理策を選択して文書化する

説明:	セキュリティ管理策の選択と文書化は、NIST リスクマネジメントフレームワーク のステップ 2 に相当する。セキュリティ管理策の選択は、次の 3 つの活動から成る:(i) ベースラインセキュリティ管理策(共通セキュリティ管理策を含む)を選択する (ii) 管理策の調整ガイダンスを適用して、ベースラインを調節する (iii)リスクアセスメント結果とローカルな状況にもとづき、調整済みのベースラインに管理策を追加して、補足する。(補足するかどうかは、判断する。) セキュリティ管理策の選択プロセスでは、組織全体的な見解が不可欠である。このような見解によって、すべてのミッション／ビジネスプロセスと、それらのプロセスを支援する情報システムおよび組織的インフラに対するリスクを、適切に軽減できるようになる。 セキュリティ管理策の選択プロセスには、セキュリティ管理策の詳細を定義する法律および規定(FISMA、OMB circulars、授権法、政府機関独自の統治法、FIPS や NIST Special Publications、およびそのほかの法律および連邦規定など)の分析が含まれなければならない。 セキュリティの他の側面と同様に、目標は、組織の情報資産の保護要件を満たす、費用効率が高い管理策を実施することである。それぞれ状況において、システムセキュリティがミッションパフォーマンスにもたらす利点と、システムの運用により生じるリスクとのバランスがとれていなければならない。 NIST SP 800-18 に記述されているように、個々の情報システムに割り当てられたセキュリティ管理策は、システムセキュリティ計画にて文書化される。セキュリティ計画は、組織内の情報システムのセキュリティ要件を概説し、それらの要件を満たすために実施中の(または計画中の)セキュリティ管理策を記述する。セキュリティ計画は、セキュリティ分類、調整、および補足活動に関する根拠、個々の管理策が組織の環境においてどのように実施されるか、リスクが大きいために適用される使用制限についても記述する。セキュリティ計画には、管理策の選択プロセスにおける決定事項と、それらの決定にする根拠が記述されるため、重要な資料となる。セキュリティ計画は、組織内の適切な担当者によって承認され、システム運用認可決定を支援するセキュリティ認可パッケージのキードキュメントの一つとして、提出される。

期待されるアウトプット:	• システムセキュリティ計画 – どのセキュリティ管理策が、どこに、どのように適用されるかを示すセキュリティ管理策の仕様。
同期化:	• セキュリティ管理策と、それらの管理策に対応する仕様は、セキュリティ管理策選択基準に沿った、適切なレベルの保護を反映したものでなければならない。 • 重要な決定では、二次的リスクも考慮する。ここでいう二次的リスクとは、決定事項が、リスクアセスメントにおいて特定されたセキュリティ管理策と保護に影響を及ぼす場合にもたらされるリスクである。
相互依存関係:	• 管理策の要件が明確化された後は、システムセキュリティ計画に盛り込まれる。 • リスクアセスメントは、調整済みのセキュリティ管理策が効果的であり、組織のリスク許容度を満たしていることを確認するための、主要なツールとなる。

実施に関するヒント

- マトリックスフォーマットのセキュリティ要件に取り組むことによって、開発者とセキュリティエンジニアは、主要システムコンポーネントごとの実施状況をレビューできるようになる。また、ギャップ分析が楽になると同時に、適切なリスク分析と管理策の実施が可能になる。
- セキュリティ要件は、具体的に述べること。複合なシステムでは、要件分析の繰返しが必要になることもある。もしそうならば、計画的なレビューを主要 SDLC マイルストーンに沿って行うべきである。
- 新しい機能要件は、セキュリティ上の意味合いを持つことがある。追加された個々の機能要件に対して、セキュリティ分析を実施しないと、さらなるリスクが発生したり、既存のセキュリティ管理策が弱まる可能性が高くなる。このような状況では、文書化されていないリスクがシステムに導入される可能性がある。
- より詳細な「攻撃防止」要件が用意されていれば、セキュリティ管理策とメソッドがリリースされる前に、テストされるようになる。文書化された要件が存在する場合、テストケースの作成と実施が必要になると考えられる。
- セキュリティ管理策は一次元ではなく、システム内の複数コンポーネントにおいて、適切な管理策が適用されるべきである。たとえば、システムが SQL サーバー、Web Sphere およびメインフレームで構成されている場合、アセスメントをすべての構成要素に対して実施する、または、一部の構成要素に対して実施する、あるいは、どの構成要素に対しても実施しない、といった選択を行うことが考えられる。 このような事柄をこの段階で文書化することによって、テストに要する労力を減らすことができる。
- 政府機関は、このフェーズにおいて、廃棄計画の作成に着手し、ライフサイクルのすべてのフェーズを通した廃棄／移行計画を立てなければならない。この活動は、要件フェーズの一環として実施することが好ましい。このようにすることで、廃棄に必要なすべてのリソースを把握し、リソースの確保を計画することができる。ハードウェアやソフトウェアは、他のフェーズにおいて、不要になったり、損傷することもあるため、廃棄手順は、ライフサイクル全体を通して有用な手順となる。

3.2.3.3 セキュリティアーキテクチャを設計する

説明:	政府機関における共有サービスプロバイダの利用の増加と主要セキュリティサービスの一元化に伴い、これらのサービスを計画し、サービスがシステムにどのように統合されるかを理解することが重要になってきている。 システムに対する企業レベルの調整によって、イニシアティブが政府機関の将来計画に適合することと、矛盾が生じないこと、または、必要以上に冗長なサービスを提供しないことが保証されなければならない。また、システムが成熟し、利用するサービスに関する決定事項が増えるにつれ、最適な統合に向けたエンタープライズアーキテクチャのレビューが必要となる。 システムレベルのセキュリティは、設計後に、システム設計に組み込まれる。これは、サービスのゾーン化(またはクラスタ化)によってサービスを集約または分散化し、冗長的な(または追加の)保護層を設けることによって、実現できることもある。システムレベルのセキュリティ設計は、外部から調達するサービス、計画されたシステム相互接続、およびシステムユーザの関心の違い(たとえば、カスタマーサービス対システム管理者)などを考慮しなければならない。 もう一つの例としては、すべてのプライオリティーとリスクの大きい作業の流れを正確に追跡または再構築するためのシステム監査戦略がある。監査戦略には、いくつかの異なるコンポーネント(ウェブアプリケーション、データベース、メインフレーム、ウェブサーバなどを含むが、これらに限定されるわけではない)からの監査記録を含めなければならない。目標は、できるだけ多

	くの監査情報を取得することではなく、セキュリティ違反やシステム障害の可能性を調査するのに必要な情報のみを取得することにある。 この活動は、既知のボトルネックと単一障害点を、IT 開発の観点からレビューする際に実施されると考えられる。 必要最低限のセキュリティ要件と、本プロセスの初期段階に特定された要件と制約は、設計者に対して、設定すべき一連の前提条件と制約を提供する。 この活動によって、セキュリティを考慮したシステムコアコンポーネント計画が可能になり、オーナーシップの総コストを下げることができる。
期待されるアウトプット:	• セキュリティ統合の概略図 － セキュリティがシステム内のどこで実施され共有されるかを示す。セキュリティアーキテクチャは、コアセキュリティ管理策がどこに、どのように適用されているかが読者に分かるように、図解する。 • 共有サービスと、サービスの利用により生じる共有リスクのリスト。 • システムが利用する共通管理策のリスト。
同期化:	• セキュリティアーキテクチャは、システムドキュメントのキーコンポーネントになる。システムドキュメントは、大きな変更が発生した場合や、重要なコントロールゲート（マイルストーン）に達した場合に、レビューを行い更新する。 • アセスメント、セキュリティテスト、およびレビューの結果が有意である場合は、有効性に関するフィードバックの可能性を検証する。
相互依存関係:	• エンタープライズアーキテクチャは、最適な統合を実現した類似システムまたはサービスへの見識をもたらしてくれる。 • システムセキュリティ計画には、セキュリティアーキテクチャの取り組みや戦略の要約を記述する。 • セキュリティ要件分析が生成する情報の大半は、詳細な情報である。設計者は、この情報をレビューし、システムレベルで理論的に適用して、管理策が意図したとおりに機能するか、あるいはギャップ(不必要な冗長性)が存在するかどうかを特定することができる。
実施に関するヒント	
• セキュリティアーキテクチャは、当該システムの設計仕様に対して、最低限のセキュリティ要件を実施することが問題となる場合に、効果的な補足管理策を提供する。また、セキュリティアーキテクチャによって、システムが継承する共通管理策と、それらの管理策に責任を持つ者が明確になる。 • そのシステムのセキュリティの背後にある論理を示すことによって、（政府機関が）追加の管理策が必要かどうかを判断しやすくなる。 • ダウンストリームを有するシステムによって受容されたリスクと、組織への悪影響は、セキュリティアーキテクチャのレビュー時に特定され、問題として取り上げられることがある。個々のシステムリスクの結集ともいえるエンタープライズリスクは、政府機関のエンタープライズアーキテクチャプロセス全体を通して明示し、追跡すべきである。	

3.2.3.4 セキュリティ管理策と開発管理策を設計する

説明:	本段階では、セキュリティ管理策が実施され、システムの一部になる。開発中の管理策の適用は、慎重に検討し、論理的に計画しなければならない。目的は、管理策を組み入れることによって、システムパフォーマンス上の問題を早期に知ることにある。また、管理策の中には、通常の開発活動を制限または妨害するものもある。 新しいシステムの場合、システムセキュリティ計画に記載されているセキュリティ要件は、本段階で設計、開発、実施される。運用中のシステムのセキュリティ計画が、組織に対して、追加の管理策を策定して現在実施中の管理策を補足するか、あるいは、効果的でない管理策を修正することを求めることもある。 本タスクにおいて、セキュリティをシステムに組み込むうえでの問題点とトレードオフをもとに、いくつかの決定が下される。ここで重要なのは、主要な決定事項と、そのような決定に至ったビジネス／技術上の誘因について、文書化することである。計画された管理策の適用が可能でない(または望ましくない)場合は、補足管理策の使用を検討し、文書化すべきである。

期待されるアウトプット:	• 実施された管理策と、それらの管理策の仕様を文書化したもの。(その内容はセキュリティ計画に含まれる)。 • 開発に関する決定とトレードオフによってセキュリティ管理策がどのように変化したか、を示すリスト。 • 既知の脆弱性または限界をテストするための、アセスメントシナリオの候補。
同期化:	セキュリティ管理策の適用は、機能テストおよびユーザテストの結果に応じて変更されることがある。変更に関しては、文書として残すこと。
相互依存関係:	• セキュリティ要件分析は、必要に応じてレビュー、更新する。 • セキュリティアーキテクチャ戦略は、必要に応じてレビュー、更新する。 • 具体的の構成は文書化するか、システムセキュリティ計画に記載する。
実施に関するヒント	
本段階で、初期のセキュリティ要件からの逸脱を文書化することによって、しっかりしたリスクプラニングが可能となり、後に、ビジネス上の判断に後戻りすることによる時間の浪費を回避できる。また、これにより、リスク計画の根拠が示される。	

3.2.3.5 セキュリティドキュメントを作成する

説明:	システムセキュリティ計画は、最も重要な資料である。これをサポートするドキュメントには、以下のものが含まれる: • 構成管理計画 • 緊急時対応計画(ビジネス影響分析を含む) • 継続的な監視計画 • セキュリティの意識向上、トレーニングおよび教育(SATE)計画 • インシデント対応計画 • プライバシー影響アセスメント(PIA) これらのドキュメントを作成する際は、文書化されるセキュリティサービスの成熟度を考慮しなければならない。これらのドキュメントには、既知の要件、共通管理策、およびテンプレートのみが含まれることもある。これらのドキュメントの記入は、プロジェクトの早い段階で開始すべきである。 本段階で重要なことは、セキュリティアプローチと適切な範囲を決定し、それぞれの責任をしっかりと理解することである。たとえば、災害復旧計画は、接続された一般支援システム(General Support System)があれば、事が足りる場合もある。また、セキュリティの意識向上、トレーニングおよび教育(SATE)は、共有サービスプロバイダに委託することもできる。この場合、それらの計画はシステム固有の部分に焦点を当てて、キーポイントは現場のサービス内容合意書から参照する、といったことも考えられる。 システム開発の進捗に伴うドキュメントの作成は、コストの削減と、ギャップを早期に発見するための包括的なアプローチによる意思決定能力の向上につながる。
期待されるアウトプット:	• システムセキュリティ計画をサポートする追加のセキュリティドキュメント。
同期化:	これらのドキュメントは、ユーザが受け入れるまで更新される。これにより、ドキュメントが正確なものとなる。
相互依存関係:	セキュリティドキュメントは、以下のものを反映しなければならない: ● セキュリティ要件分析 ● セキュリティアーキテクチャ ● ビジネス影響アセスメント ● セキュリティ分類

実施に関するヒント
● セキュリティオペレーションは、コンプライアンスの文書化によって先導されるべきではない。このオペレーションは、システムのニーズにもとづくものでなければならないと同時に、(組織の)セキュリティガイダンスに従って記述されなければならない。 ● 規模が大きく、設計が複雑で、政治的に慎重を期する主要システムでは、ドキュメントごとに連絡先(POC)を割り当てた後に、ドキュメントの範囲、期待される内容、および詳細レベルに関するミーティングによって、システム開発を開始すると良い。

3.2.3.6 開発テスト、機能テストおよびセキュリティテストを実施する

説明:	開発中のシステム、またはソフトウェア、ハードウェアおよび／またはコミュニケーションの修正を実施中のシステムは、システムが実施される前に、テスト、評価しければならない。テストと評価の目的は、開発されたシステムが機能要件とセキュリティ要件を満たしていることを確認することにある。セキュリティ管理策のテストは、NIST SP 800-53A『連邦政府情報システムのためのセキュリティ管理策アセスメントガイド(Guide for Assessing the Security Controls in Federal Information Systems)』に記載のアセスメント手順によって補足される管理策のための、技術的セキュリティ仕様にもとづくものとする。 テストおよび評価プロセスは、特殊性(specificity)、再現性(repeatability)、および反復(iteration)に焦点を置いている。特殊性(specificity)とは、テストの範囲を調整して、その環境での使用を意図したセキュリティ要件のみをテストできることを意味する。再現性(repeatability)とは、情報システムに対する一連のテストを複数回実施(または類似システムを平行してテスト)した結果、毎回同じような結果が得られることを意味する。反復(iteration)とは、システムの全体的、または部分的な機能テストを複数回連続して実施できることを意味する。これにより組織は、受入可能なレベルのシステム要件へ準拠を達成するまで、テストを繰り返し実施できる。このような特性を実現するためには、機能テストをできる限り自動化し、テストケースの詳細を公表することが求められる。これにより、繰り返し使用できる再現性のあるテストプロセスを確立することが可能になる。自動テストツールの使用とNIST SCAP (Security Content Automation Protocol)の統合は、セキュリティ管理策のテストおよび評価活動を開始する前に、完了していなければならない。機能テストまたは自動化されたテストにおいてテストされなかったセキュリティ機能は、要件への準拠を確実にするためにも、管理策の明示的なテストおよび評価において、慎重にチェックされる。 システムの開発中は、テストデータ(スタブデータ)のみを使用する。システムまたはソフトウェアの開発中には、運用データ、セキュリティ関連データ、または個人情報(PII)がそのシステムまたはソフトウェア上に存在しないようにする。
期待されるアウトプット:	テスト結果を文書化したもの。これには、テスト中に発見された予想外の変動(variation)が含まれる。
同期化:	すべてのテスト結果は、構成管理されたアップデートが実施できるよう、開発者に戻される。予想外の結果が示された場合、顧客に対して要件の性質の明確化が求められることもある。
相互依存関係:	• セキュリティ要件分析が影響を受けて、更新が必要となることもある。 • セキュリティアーキテクチャが変更による影響を受けて、更新が必要となることもある。 • 現行の軽減措置を反映するために、システムリスクアセスメントの更新が必要となることもある。

実施に関するヒント
• 冗長な機能テストとセキュリティテスト活動を減らすために、機能テスト計画に一般的なセキュリティ機能のテストを(可能な限りの多く)含めることが奨励される。 • 機能テストにおいて、基本管理策(必須のアクセスコントロール、セキュアなコード開発、およびファイアウォールなど)の予備テストを実施することによって、開発サイクルの早い段階で問題を軽減または除去できる。予備テストは、承認および運用認可(C&A)のテストではなく、開発レベルのテストであると考えられている。しかしながら、予備テスト後に変

更がない場合には、テスト結果を C&A に最大限に利用する。

- 注目度が高く、取り扱いに注意を要するシステムの場合、第三者による開発テストが奨励されることもある。
- 予備テストを実施することによって、コストとスケジュール上のリスクを軽減できる。
- 予備テストは、コンポーネントレベルまたはセキュリティゾーンレベルで実施することができる。これにより、個々のコンポーネントまたはセキュリティゾーンを、一つのエンティティとして、確実にセキュアにすることができる。
- ライフサイクル全体を通して実施されるすべてのセキュリティテストのプロセスと結果を捕え、評価、問題の特定、および再利用に利用する。
- ソースコードは、自動化されたツールを使って、または、手動の抜き取り検査によってレビューし、システムセキュリティに有害な影響を及ぼす一般的なプログラミングエラーを特定する。有害な影響を及ぼすプログラミングエラーには、以下のものが含まれる：クロスサイトスクリプティング脆弱性、バッファーオーバーフロー、競合状態、オブジェクトモデル違反、ユーザ入力データの検証の甘さ、エラーハンドリングの甘さ、セキュリティパラメータの露出, プレーンテキストで表示されるパスワード、およびソフトウェア開発品質保証プロセスの一環として定められた、セキュリティポリシー、モデルまたはアーキテクチャへの違反。

3.3 SDLC フェーズ: インプリメンテーション／アセスメント

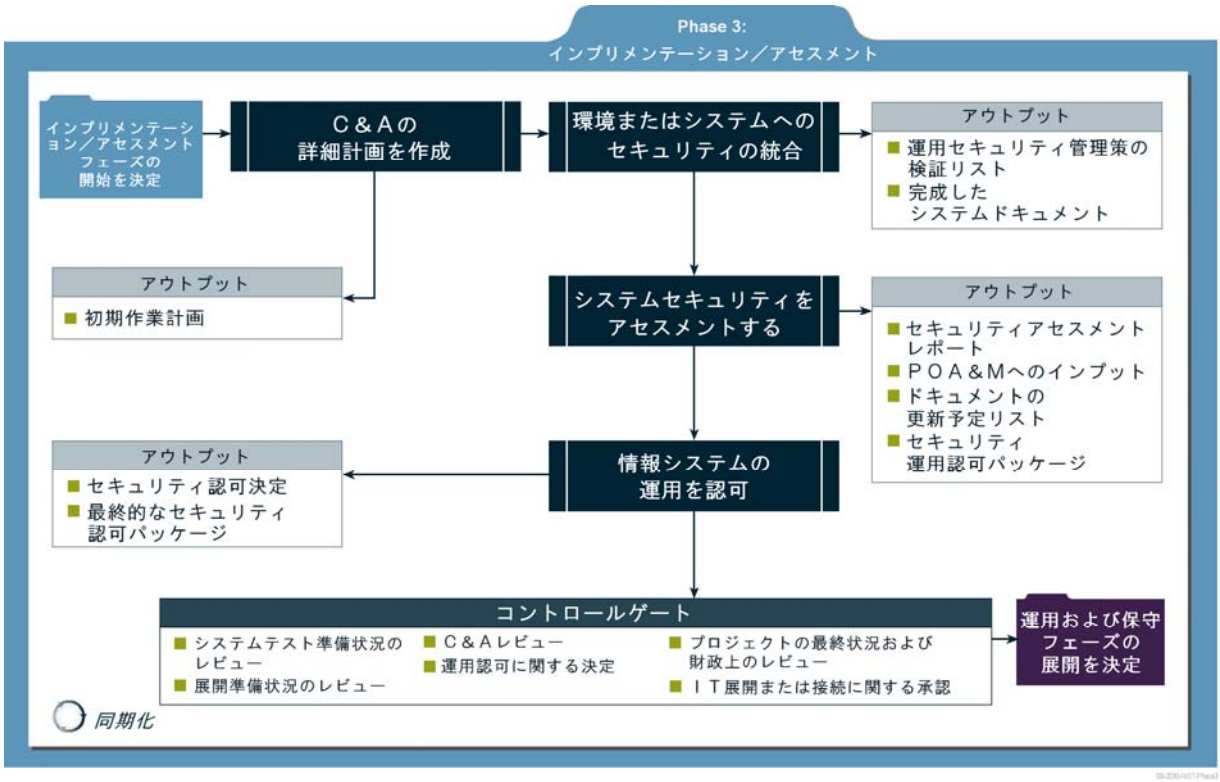

図 3-4 セキュリティ考慮事項のインプリメンテーション／アセスメントフェーズへの関連づけ

3.3.1 解説

インプリメンテーション／アセスメントは、SDLC の 3 番目のフェーズである。本フェーズでは、組織の運用環境にて、システムをインストールし、評価する。

本フェーズの主なセキュリティ活動には、以下のものが含まれる:

- 情報システムを、そのシステム用の環境に統合する。
- システム承認活動を計画し、実施する。この際、セキュリティ管理策のテストと同期が取れるようにする。
- システム運用認可活動を完了させる。

3.3.2 コントロールゲート

本フェーズの一般的なコントロールゲートには、以下のものが含まれる:

- システムテスト準備状況のレビュー (System Test Readiness Review)

- C&A レビュー (C&A Review)
- プロジェクトの最終状況および財政上のレビュー (Final Project Status and Financial Review)
- 展開準備状況のレビュー (Deployment Readiness Review)
- 運用認可権限者 (AO)による決定 (Authorizing Official (AO) Decision)
- IT 展開または接続に関する承認 (IT Deployment or Connection Approval)

3.3.3 主なセキュリティ活動

3.3.3.1 セキュリティ承認と運用認可(C&A)の詳細計画を作成する

説明:	運用認可権限者(AO)は、システム運用でのリスクを承認する責任がある。ゆえにシステムの最終的な運用に関連したリスクが受容できないように思われる場合には、開発チームにアドバイスできる。仕様によっては、受容可能な残余リスクがわからない場合に、過度の負担とコストを必要とする場合もある。受容可能な残余リスクの判断には、AO の関わりが必要になる。システム調達の計画段階中に要件の変更を組み入れた方が、要請、ソース選択、または契約管理の段階中に組み入れるよりも簡単である。 開発チームと運用認可権限者は、証拠の形式について話し合うべきである(最終的な決定は、運用認可権限者が行う。) この証拠には、システムテスト結果と、そのほかの関連データが含まれることがある。また、調達責任者と運用認可権限者は、システムの変更とシステム環境の変化への対処方法について話し合うべきである。セキュリティ専門調査委員会の設立の可能性についても、話し合うべきである。そのようなグループは、次のようなメンバーで構成されることが考えられる:ユーザ、プログラムマネージャとアプリケーションスポンサー;システム／セキュリティ／データベースの管理者;セキュリティ担当者またはセキュリティ専門家(C&A の代表者を含む);システムアナリストまたはアプリケーションアナリスト。 適切なテストを行い、テスト中に要件の変更がないようにするためには、セキュリティ運用認可の範囲を明確にすべきである。これにより、実施パフォーマンスの測定の前に作成、承認されるテスト計画の、基盤を築くことができる。この時点で承認パッケージは、あらかた完成していなければならない。 また、準拠に関する政府機関指定の初期レビューも実施されていなければならない。
期待されるアウトプット:	• 初期作業計画:キープレーヤー、プロジェクトの制約、コアコンポーネント、テストの範囲、および期待される厳格さ(rigor)を記載した計画ドキュメント。承認パッケージは、あらかた完成していて、準拠に関する政府機関指定の初期レビューも、実施されていなければならない。
同期化:	情報システムセキュリティ担当者は、システムオーナーに対して、C&A の実施に必要なドキュメントを提供する。運用認可権限者には、その旨が伝えられる。
相互依存関係:	セキュリティ管理策アセスメント計画は、本計画文書／セッションから、基礎的な情報を得る。
実施に関するヒント	
• テストの 4～6 週間前に計画セッションを開くか、または、プロジェクト予備計画を作成することによって、リソースの確保と適切な計画作成のための、十分な時間が与えられる。 • 承認パッケージの簡単なレビューを行うことによって、考えられる問題が明らかになる。 • アクティブなテストは開発に影響を与えるため、本ミーティングが始まる前に、時間的な余裕を持って計画すべきである。 • 計画プロセスの早い段階(フェーズ 1 からでも良い)で運用認可権限者を参加させることによって、C&A の予想結果を立てることができ、C&A コントロールゲートにたどり着く前に不足の事態が起きるのを防ぐことができる。	

3.3.3.2 確立した環境またはシステムにセキュリティを統合する

説明:	システムインテグレーションは、運用サイトにおいて、システムが展開される時に実施される。インテグレーションテストおよび受け入れテストは、システムが納品されインストールされた後に、実施される。セキュリティ管理策の設定は、メーカーの指示、利用可能なセキュリティ実施ガイダンス、および文書化されたセキュリティー仕様に従って、実施する。
期待されるアウトプット:	• 運用セキュリティ管理策の検証リスト。 • 完成したシステムドキュメント。
同期化:	• インストール中に遭遇した問題については、評価を行い、再発の可能性がある場合には、緊急時対応計画に含める。 • 情報システムセキュリティ担当者は、インストールされたシステムをレビューし、管理策が実施されていること、適切な設定が行われていること、管理策の検証リストがシステムオーナーと運用認可権限者に提供されることを確実にする。
相互依存関係:	変更点については、主要なセキュリティドキュメントに反映すること。
実施に関するヒント	
• テスト環境と開発環境をクリアにして、データが残らないようにする。 • システムを運用環境または他のシステムに組み込む場合には、重要なオペレーションに支障をきたさないよう、細心の注意を払うこと。	

3.3.3.3 システムセキュリティをアセスメントする

説明:	開発中のシステム、またはソフトウェア、ハードウェアおよび／またはコミュニケーションの修正を実施中のシステムについては、正式な運用認可を受ける前に、正式な評価を実施する。セキュリティアセスメントプロセスの目的は、システムが機能要件とセキュリティ要件を満たしていることと、システム運用環境における残存セキュリティリスクが許容範囲内であることを確認することにある。セキュリティ管理策のテストは、NIST SP 800-53A『連邦政府情報システムのためのセキュリティ管理策アセスメントガイド(Guide for Assessing the Security Controls in Federal Information Systems)』に記載のアセスメント手順に基づくものとする。 組織は、システムの初期運用を開始する前に、セキュリティ承認を実施して、管理策がどの程度正しく導入されているか、どの程度意図したとおりに運用されているか、システムのセキュリティ要求事項に対する適合性の観点から望まれる結果をどの程度産出しているかを評価しなければならない。また、情報システムのセキュリティ管理策の定期的なテストと評価を実施し、管理策の有効性が維持されるようにする。セキュリティ管理策の有効性の検証に加えて、セキュリティ承認を行うことにより、情報システムの実際の脆弱性が明らかになることもある。 セキュリティ管理策の有効性とシステムの脆弱性を特定することによって、信頼できるリスクベースのセキュリティ運用認可決定を支援する重要な情報が、運用認可権限者に提供される。
期待されるアウトプット:	• セキュリティ運用認可パッケージ。これには、セキュリティアセスメントレポート、行動計画とマイルストーン(POA&M)、およびシステムセキュリティ計画が含まれる。
同期化:	• 承認者は、書面による承認パッケージ結果をシステムオーナー、情報システムセキュリティ担当者およびシステム管理者に提供する。 • アセスメント結果は、システムオーナー、情報システムセキュリティ担当者、システム管理者および開発者との間で共有される。
相互依存関係:	前述のすべてのステップ。
実施に関するヒント	

• すべてのドキュメントをレビューできる段階まで完成させて、レビュー時にシステムの現状を把握できるようにする。 • 承認パッケージを CD/DVD または他の電子メディアにコピーすることによって、構成を管理し、アーカイブを最新に保つことができる。 • 主要な関係者の代表によるチームを編成し、テストが完了するまで定期的に集まるようにすることで、コミュニケーションが進むと同時に、不測の事態を減らすことができる。 • C&A プロセスを関係者全員に明示して、テストの厳格さ(rigor)と範囲について合意を得ることは、スムーズな承認活動を確実にするうえで、非常に重要である。 • リスクと費用効率をもとにして、継続監視の優先順位付けを行う。 • 以前に実施されたもので、関連性のあるアセスメントの結果を、できるだけ多く再利用する。

3.3.3.4 情報システムを認可する

説明:	OMB Circular A-130 は、情報を処理、格納、伝送するシステムに対して、セキュリティ認可を受けることを求めている。政府機関の上級職員によって与えられるこの認可(セキュリティ運用認可として知られている)は、検証された管理策の有効性にもとづくものである。管理策の有効性の検証では、その管理策が合意を得たレベルの保証を満たしているか、(管理策を実施することによって)政府機関の資産や業務(ミッション、機能、イメージ、評判を含む)への残存リスクが許容範囲内に収まっているか、などをチェックする。 セキュリティ認可決定は、リスクベースの決定であり、セキュリティ管理策の検証プロセスにおいて生成されるセキュリティテストおよび評価結果に大きく依存する(その情報だけに依存するわけではないが)。運用認可権限者は、セキュリティ運用認可の決定(システムの運用を許可し、政府機関の資産や業務へ残存リスクを明示的に受け入れるかどうか)を下す際に、主に、以下のものに依存する: (i) 完成したシステムセキュリティ計画 (ii) セキュリティテストおよび評価結果 (iii) システムの脆弱性を軽減または除去するための行動計画とマイルストーン。
期待されるアウトプット:	• セキュリティ認可決定。この決定は文書化されて、運用認可権限者からシステムオーナーと情報システムセキュリティ担当者に送られる。 • 最終的なセキュリティ認可パッケージ。
同期化:	• システム一覧と報告統計を更新して、運用認可ステータスが反映されるようにする。 • 資本計画および投資管理(CPIC)活動も、システムの運用が認可された場合に更新する。
相互依存関係:	• セキュリティと予算に関わるドキュメントも、結果として示されたステータスをもとに更新する。 • 情報システムの承認ステートメント。
実施に関するヒント	
運用認可権限者は、システムに対するリスクだけではなく、システムの運用により生じる組織全体へのリスクについても判断する。	

3.4 SDLC フェーズ: 運用および保守

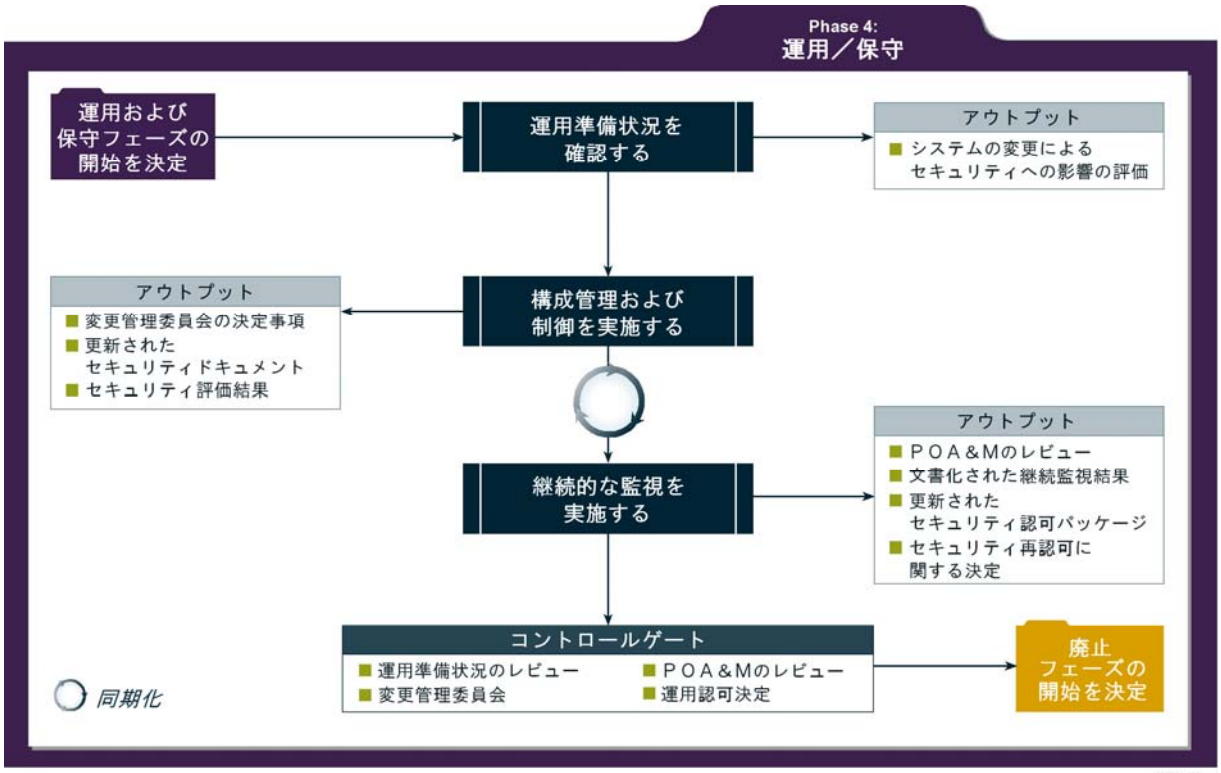

図 3-5 セキュリティ考慮事項の運用／保守フェーズへの関連づけ

3.4.1 解説

運用および保守は、SDLC の 4 番目のフェーズである。本フェーズでは、以下の作業を行う: (i) システムを導入、運用し、システムへの強化や修正を開発、テストし、ハードウェアやソフトウェアを追加または置き換える。(ii) システムのパフォーマンスを継続的に監視し、セキュリティ要件が満たされているかどうかをチェックする。また、システムに必要な変更を実施する。(iii) 運用システムを定期的に評価して、システムをより効果的で効率的、かつセキュアなものにするための方法を模索する。システムが効果的に運用され、合意を得たリスクレベルの維持と、組織のニーズへの対応がしっかりと行われている間は、システムの運用は続く。必要な場合は、システムの修正または変更の特定が行われ、システムが本フェーズよりも前のフェーズに再投入されることもある。

本フェーズの主なセキュリティ活動には、以下のものが含まれる:

- 運用準備状況のレビュー(operational readiness review)を実施する。
- システム構成を管理する
- システムのセキュリティ管理策の安全な運用と継続監視のための手順と手続きを確立する。
- 必要に応じて再運用認可を実施する。

3.4.2 コントロールゲート

本フェーズの一般的なコントロールゲートには、以下のものが含まれる:

- 運用準備状況のレビュー
- 変更案に対する変更管理委員会(Change Control Board)による レビュー
- 行動計画とマイルストーンのレビュー
- 運用認可決定 (3 年ごと、または大きな変更が行われた場合)

3.4.3 主なセキュリティ活動

3.4.3.1 運用準備状況を確認する

説明:	多くの場合、システムが本番環境に移行すると、システムに対する予想外の変更が発生する。重大な変更が行われた場合は、セキュリティ管理策の完全性を確保するために、管理策のテストを修正(構成など)して、テストを実施することもある。 本ステップは、必ずしも必要であるわけではない。しかしながら、リスクを軽減し、土壇場の番狂わせに効果的に対処するためのステップとして、実施を考慮すべきである。
期待されるアウトプット:	システムの変更によるセキュリティへの影響の評価。
同期化:	• システム管理者と情報システムセキュリティ担当者が、システムオーナーに対して、システムが通常に運用されているか、また、セキュリティ要件に準拠しているか、を確認する。 • 土壇場の変更が発生し、その変更によってシステムのリスクレベルが根本的に変わる場合には、システムオーナーは再承認を検討すべきである。(これは、稀なケースである)。.
相互依存関係:	• 運用準備状況のレビューは、C&A プロセスを補足する活動であり、変更をレビューして、リスクの可能性を調査する。 • 管理策に対する変更は、セキュリティドキュメントに反映する。
実施に関するヒント	
• アプリケーションが強化または変更された場合は、回帰テストを実施することによって、追加の脆弱性が導入されるのを回避することができる。たとえば、ソースコードを加えることで、別の箇所にエラーが導入され、既存の安定した機能に負の影響がもたらされることがしばしばある。 • データフィールドの追加を含む変更は、メモを残し、分析を行って、システムのセキュリティ状態が低下していないか、追加の管理策を導入すべきか、などを判断する。 • 新しい IT システムを本番環境に展開する前に、ユーザに対して、セキュリティ意識とセキュリティ慣行に関する十分なトレーニングを実施する。	

3.4.3.2 構成管理および制御を実施する

説明:	構成管理および制御に関する効果的な方針と手順は、情報システム、またはシステムを取り巻く環境に特定の変更があった場合に生じる、セキュリティ上の影響を十分に考慮するうえで重要である。 構成管理およびコントロール手順は、情報システムのハードウェア、ソフトウェアおよびファームウェアコンポーネントの初期ベースラインを確立するうえで、また、システムへの変更点の正確な目録を管理、維持するうえで、きわめて重要である。システムのハードウェア、ソフトウェアまたはファームウェアへの変更は、重大なセキュリティ影響をもたらすことがある。

	システムへの変更を文書化して、セキュリティ上の影響を継続的に評価することは、セキュリティ認可を維持するうえで、重要である。 このようなステップを効果的に実施することによって、システムの継続監視能力に対する、極めて重要な入力が提供される。これにより、システムのセキュリティ状態と管理策の有効性を低下させる重大な変更の、特定能力が向上し、適切な評価およびテストを実施できるようになる。 注: SCAP は、特定の標準を用いて、自動化された脆弱性管理、測定とポリシーコンプライアンス評価（FISMA コンプライアンスなど)を行うための、手段である。政府機関の構成管理手順には、再現性と一貫性を確保するために、本活動を組み込まなければならない。これは、プロフィールへの変更の定期レビューを必要とする、反復プロセスである。
期待されるアウトプット:	• 変更管理委員会(CCB)の決定事項。 • 更新されたセキュリティドキュメント(システムセキュリティ計画、行動計画とマイルストーン(POA&M)など)。 • 文書化されたシステムの変更に対するセキュリティ評価。
同期化:	• システムアップデートは、少なくとも年 1 回、または重要な変更が生じた場合に、セキュリティドキュメントに含めなければならない。 • 構成管理システムドキュメントは、システムの継続監視計画に入力を提供するものでなければならない。
相互依存関係:	• セキュリティアーキテクチャは、コンポーネントレベルのセキュリティサービスに関する重要な詳細を提供するものでなければならない。コンポーネントレベルのセキュリティサービスは、計画された変更がもたらす影響を評価するためのベンチマークを提供する。たとえば、データベースソフトウェアを新バージョンにアップグレードする予定で、新バージョンのソフトウェアの監視能力が旧バージョンよりも劣るとする。この場合、そのレベルの監視能力が当該コンポーネントに必要かどうかを判断するための情報が、セキュリティアーキテクチャまたはセキュリティ管理策ドキュメントによって提供されなければならない。最終的な分析によって、更なるレビューが実現の前に必要かどうかを判断できるようになる。
実施に関するヒント	
• 構成管理に関するアーチファクトを見てセキュリティ上の意味合いを捕らえることは、必ずしも容易でない。レビュー者は、機密性、完全性および可用性に直接、または間接的に影響を与えるあらゆる変更について、留意すべきである。 • 新しいデータを加えるようなシステム強化は、システムセキュリティ分類および関連セキュリティ管理策への影響のレビューを必要とすることもある。 • 独自の緊急事態を考慮に入れた、省略された構成管理プロセスを、緊急時対応のために用意しておくべきである。このような独自の緊急事態への対処は、時間が許す限り、徹底的にレビューする。	

3.4.3.3 継続的な監視を実施する

説明:	継続監視の最終的な目的は、システムおよびシステムが運用される環境へのやむをえない変更があっても、管理策の有効性が維持されることを確認することにある。 綿密に設計され管理が行き届いた継続監視プロセスは、管理策アセスメントとリスク決定プロセスを、静的なものから動的なものに変えることができる。この動的プロセスは、組織内の適切な担当者に対して、重要なセキュリティステータス情報をほぼリアルタイムで提供する。組織は、この情報を使用して、適切なリスク軽減活動を行うことができ、システムの継続運用を認可してリスクを明示的に受け入れるか否かについて、信頼できるリスクベースの決定を下すことができる。 管理策の有効性の継続監視は、さまざまな方法で実現できる。たとえば、セキュリティレビュー、セルフアセスメント、構成管理、アンチウィルス管理、パッチ管理、セキュリティテストおよび評価、または監査などが挙げられる。可能な場合は、自動化を導入して、労力を減らし、再現性を確保する。 継続監視に含まれる活動として、再運用認可がある。これは、システムのセキュリティに影響を及ぼすような重大なシステム変更があった場合や、連邦政府または政府機関ポリシーが規定する期間が経過した場合に、実施される。
期待されるアウト	• 文書化された継続監視結果

プット:	• 行動計画とマイルストーン(POA&M) のレビュー。 • セキュリティレビュー、メトリクス、対策と傾向変動分析。 • 更新されたセキュリティドキュメントとセキュリティ再認可決定(必要な場合)。
同期化:	継続監視は、リスクレベルが大幅に変動して、管理策が修正、追加または廃止された場合に、調整する。
相互依存関係:	継続監視は、システムのオーナーに対して、システムセキュリティ計画、セキュリティアセスメントレポート、および行動計画とマイルストーン(POA&M)ドキュメントを継続的に更新するための、効果的なツールを提供する。

実施に関するヒント

- 政府機関は、費用効率が高い継続監視プログラムを実行するよう努めなければならない。継続監視プログラムでは、利用可能である場合には、共通サービスを活用して、より頻繁な監視と、重要なセキュリティ管理策に対するシステム固有の監視を行うべきである。
- システムのすべての管理策を継続的に監視することが現実的ではなく、かつ、費用効率が高いわけでもない場合には、管理策の監視スケジュールを立てることを検討すべきである。このようなスケジュールは、より頻繁な監視を必要とする管理策が、要求される頻度で監視されること、また、すべての管理策がそれぞれの運用認可決定の間に、すくなくとも一度は評価されるようにするためにも重要である。
- 継続監視プロセスは定期的に評価し、脅威の変化をレビューし、それらの変化がシステムを保護するための管理策の能力にどのような影響を及ぼすかを特定しなければならない。脅威がアップデートされることによって、リスクに関する決定が更新され、既存の管理策が変更されることもある。
- 進行中のもので継続監視に役立つ活動を信頼し活用すること。AV DAT ファイルアップデート、日常保守、物理的セキュリティ防火訓練、ログレビューなどは、すべて特定し、継続監視フェーズに取り入れるようにする。
- リスクを軽減するうえでの管理策の重要性、クローズされた POA&M アイテムの有効性、単一障害点をもとに、継続監視を優先付けすること。
- システム承認の有効期間に一致する監視サイクルを特定し、再承認に再利用できるテスト手順と結果を抽出する。
- 継続監視活動は、セキュリティパフォーマンス計画およびセキュリティ投資収益率の測定を支援するデータを、提供することもある。
- 再運用認可を実施すべきか否かを判断するための政府機関独自の基準を定義することによって、意思決定者が情報を十分に得ることができ、関係者が共通の理解を持つことができる。基準には、独自の状況にも対応できるよう、ある程度の自由度を持たせるべきである。

3.5 SDLC フェーズ: 廃止

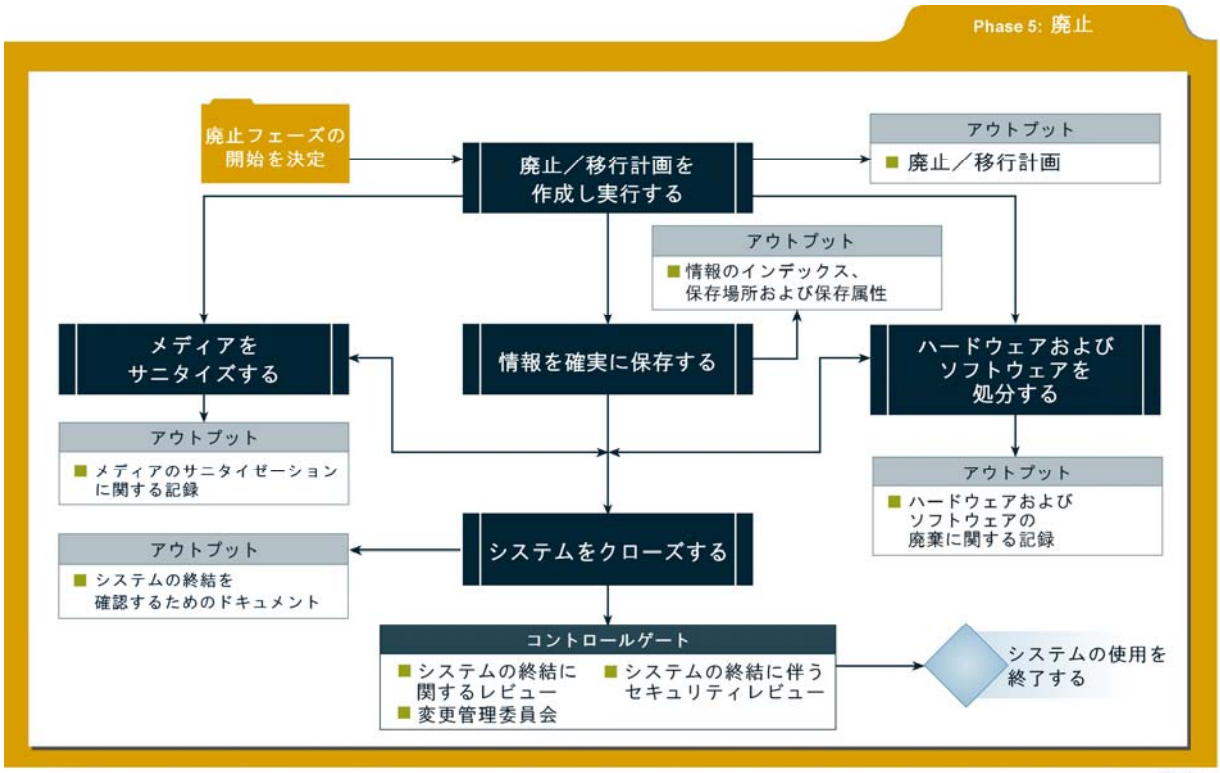

図 3-6 セキュリティ考慮事項の廃棄フェーズへの関連づけ

3.5.1 解説

SDLC の最終フェーズである「廃棄」では、システムを廃棄し、実施中のすべての契約を完了する。情報とシステムの廃棄に関連する情報セキュリティ問題には、明確に対処する必要がある。情報システムが交換されたり、旧式になったり、もはや役立たなくなった場合、連邦政府のリソースや資産を確実に保護することが重要である。

通常、システムには、はっきりとした終わりというものがない。システムは、要件の変更または技術の改善の結果として、次世代へ進化または移行するからである。セキュリティ計画は、システムとともに絶えず進化する必要がある。(現行のシステムの)環境、管理、および運用上の情報の多くは、後続のシステムのセキュリティ計画の開発時にも利用でき、かつ有効であるべきである。

廃止活動は、システムの秩序だった終了を確保し、情報の一部またはすべてが将来必要になった場合に再利用できるように、システムに関する重要な情報を保存する。廃止活動では、システムが処理したデータを適切に保存することに重きが置かれる。データを適切に保存することで、データを別のシステムに効果的に移行したり、将来予想されるアクセスを可能にするために、適用可能な記録管理規定およびポリシーに従ってデータをアーカイブすることができる。

本フェーズの主なセキュリティ活動には、以下のものが含まれる:

- 廃棄／移行計画を作成し、実施する。
- 重要な情報をアーカイブする 。
- メディアをサニタイズ(データを完全に消去)する。
- ハードウェアとソフトウェアを廃棄する。

3.5.2 コントロールゲート

本フェーズの一般的なコントロールゲートには、以下のものが含まれる:

- システムの終結に関するレビュー
- 変更管理委員会
- システムの終結に伴うセキュリティレビュー

3.5.3 主なセキュリティ活動

3.5.3.1 廃止／移行計画を作成し実施する

説明:	廃棄/移行計画を作成することによって、すべての関係者が、システムとその情報の将来計画について知るようになる。この計画には、重要なコンポーネント、サービス、および情報の廃棄/移行ステータスを記述する。 この計画は、作業計画と同様に、システムまたはその情報を正しく終結、伝送、または移行するために必要なステップ、決定、およびマイルストーンを特定する。 多くの場合、廃止されたシステムまたはシステムコンポーネントは、休止中であるが、システムインフラに接続されたままである。結果として、これらのコンポーネントは、見落とされたり、使途不明となったり、最適でないセキュリティ保護レベルで維持されることになり、システムインフラや接続されているすべてのシステムへの追加のリスクが発生することになる。移行計画は、このような結果の軽減を支援する。
期待されるアウトプット:	システムおよびシステムの情報をクローズし移行するための、文書化された廃止／移行計画。
同期化:	セキュリティ決定事項と資金調達が変更になる、または、廃止に関する決定により影響を受ける場合には、保留中の計画も、セキュリティドキュメントに反映する。
相互依存関係:	セキュリティ計画やセキュリティ管理策要件などのセキュリティドキュメントの更新が、必要となることもある。
実施に関するヒント	
• システムの廃止を実施する前に、政府機関の記録管理担当者、プライバシー担当者、および情報公開法(FOIA)担当者のアドバイスを受けることで、これらの法律や政府機関のポリシーに準拠できるようにすること。 • 廃棄/移行計画は、廃棄フェーズを待たずに作成するようにする。ライフサイクルのすべてのフェーズを通して、廃棄/移行を計画すること。この活動は、要件フェーズの一環として実施することが好ましい。このようにすることで、廃棄/移行に必要なすべてのリソースを把握し、リソースの確保を計画することができる。また、この活動は、ハードウェアやソ	

フトウェアが不要になったり、損傷した場合に実施することもある。他のフェーズにおける、廃棄/移行活動も、このフェーズで明らかにする。

3.5.3.2 情報を確実に保存する

説明:	情報を保存する場合、組織は、将来情報を取得するために必要な方法を考慮する必要がある。記録の取得に使用する技術は、将来も簡単に利用できるとはかぎらない。また、システムの廃止の際には、記録保持に関する法的要件も考慮する必要がある。
期待されるアウトプット:	保存された情報のインデックスと、保存されている場所および保存属性。
同期化:	記録管理、プライバシー、および情報公開法を考慮する。
相互依存関係:	プライバシーに関する考慮および活動は、情報公開法(FOIA)を遵守うえで重要となることもある。
実施に関するヒント	
• 組織の FOIA オフィスと緊密な調整を行うことによって、この活動を計画しやすくなる。 • 組織は、National Archives and Records Administration Information System Security Oversight Office からも、ヒント(助言)を得ることができる。	

3.5.3.3 メディアをサニタイズする

説明:	システムのオーナーは、セキュリティ分類の結果に基づいて、NIST SP 800-53『連邦政府情報システムにおける推奨セキュリティ管理策(Recommended Security Controls for Federal Information Systems)』を参照すべきである。SP800-53 では、次のように規定している。「組織は、承認された機器、技術および手順を使用して、情報システムデジタルメディアをサニタイズにする。」 組織は、メディアのサニタイズと破壊活動を追跡、文書化、検証し、サニタイズ用の機器／手順を定期的にテストして、それらの機器／手順が正しく機能することを確実にする。組織は、情報システムデジタルメディアを廃棄、または組織外で再利用する前に、それらのメディアをサニタイズ、または破壊し、権限のない個人がメディアに含まれる情報にアクセスし利用することを防ぐ。 NIST SP 800-88『(Guidelines for Media Sanitization)』では、メディアのサニタイゼーションを、廃止、消去、除去、破壊の 4 つのカテゴリーに分類している。また、この文書は、システムオーナーが、情報を分類し、その情報が記録されている媒体の性質を見極め、その機密性に対するリスクを見積もり、その媒体に関する将来の計画を決定したうえで、適切なサニタイズ方法を決めることを推奨している。選択したプロセスについては、コスト、環境への影響などについて評価するとともに、機密性へのリスクを最も軽減し、プロセスに課せられるそのほかの制約を最大限に満たす意志決定を行うべきである。 サニタイズに関する意志決定を行うときは、システムの機密性の分類とともに、いくつかの要素を考慮すべきである。最終的な決定の前に、媒体サニタイズプロセスのコストとメリットを理解すべきである。たとえば、フロッピーディスクなどの安価な媒体を消磁するのは、費用対効果が高くない可能性がある。
期待されるアウトプット:	メディアのサニタイゼーションに関する記録。
同期化:	なし
相互依存関係:	セキュリティ分類によって、システム情報が特定され、関連リスクレベルが明確になる。
実施に関するヒント	

• 消去または除去が推奨される方法ではあるが、媒体を破壊するほうが（訓練、追跡、検証などを考慮すると）ほかのいずれかの方法よりも費用対効果が高い場合もある。 • 各組織は、妥当であり、かつ既存のリスクのアセスメントによって示唆される場合は、適用するサニタイズのレベルをいつでもあげることができる。

3.5.3.4 ハードウェアおよびソフトウェアを処分する

説明:	ハードウェアおよびソフトウェアは、適用可能な法律または規制の定めるところに従って、売却、譲渡、または廃棄することができる。ソフトウェアの処分は、ライセンスまたは開発者とのその他の契約、および連邦政府の規制に従う必要がある。ハードウェアを破壊する必要はめったに生じないが、機密を要する情報が含まれ、破壊する以外には処分できない保存メディアについてはこの限りではない。保存メディアを適切に処分できない場合、残りのハードウェアを売却または譲渡できるように、メディアを撤去してから物理的に破壊することもできる。システムの中には、保存メディアを取り外した後でも、機密を要する情報が残っている場合がある。機密を要する情報がシステムに残っているかどうか定かではない場合、システムの処分前に、ISSO に意見を求めるべきである。また、ベンダに相談して、廃棄の選択肢がほかにはないかを確認したり、リスクを確認することもできる。
期待されるアウトプット:	• ハードウェアおよびソフトウェアの廃棄に関する記録。これらの記録には、（売却、廃棄、または贈与のために）手元から離れたハードウェアとソフトウェアのリストや、組織内の他のプロジェクトやタスクに再投入されたハードウェアとソフトウェアのリストが含まれることもある。
同期化:	システムおよびコンポーネント一覧を更新したもの。
相互依存関係:	ハードウェアおよびソフトウェア一覧は、適宜、更新する。
実施に関するヒント	
• システムを廃棄する際には、資産説明責任要件を忘れないこと。可能な場合、使用済みの IT の寄付や危険物のeサイクリング(e-cycling)を検討する。 • 合衆国法典第 40 編は、余剰設備が「教育の分野で有用」であり、「連邦政府の設備は重要な国家資産である」ことをシステムオーナーや管理者に忠告している。余剰設備や媒体は、法律の許す範囲内で、できるだけ学校や非営利組織が利用できるようにすべきである。 • 一部の政府機関は、コストを節減するために、かなり古い部品を緊急時対応のために維持している。たとえば、使われなくなったラップトップを在宅勤務者との連絡に使用して、インターネット通信または電子メール通信などの、簡単な処理のみを行うことが考えられる。	

3.5.3.5 システムをクローズする

説明:	情報システムは、通常、この時点で正式に終結され、分解される。
期待されるアウトプット:	• システムの終結を確認するためのドキュメント。これには、承認および運用認可権限者、構成管理者、システムオーナー、ISSO、およびプログラムマネージャに対する、最終的な終結通知が含まれる。
同期化:	なし
相互依存関係:	• セキュリティドキュメントのアーカイブ（必要に応じて）。 • 継続監視サービスが提供されている場合は、プロバイダに、システムの終結を通知する（CM(構成管理)、AV(ウィルス対策)、IR(インシデント対応)、CCB(変更管理委員会)を含むこと

	がある)。 • FISMA 報告とエンタープライズアーキテクチャのためのインベントリの更新。
実施に関するヒント	
• システムの正式な終結と適切な措置を明示した文書。この文書は、主要なすべての関係者に配布され、正式な終結を行うための最も単純なアプローチを提供する。	

第 4 章

セキュリティに関する追加的な考慮事項

セキュリティの組み込みは、セキュリティを管理するための技術であり、これにより、SDLC フェーズにおける特定のセキュリティ考慮事項の実施が可能になる。しかしながら IT プロジェクトとイニシアティブは、システム開発やアプリケーション開発のように明確に範囲を絞ることができないことがある。一部のイニシアティブは、サービスベースのクロス IT プラットフォーム(場合によっては、複数の組織をまたぐもの)であったり、データセンタ、ホットサイトの建物など施設ベースであったりする。これらのプロジェクトでは、できる限り、確立された審査委員会に従い、必要なセキュリティ考慮事項を認識し、それらの事項に対処しなければならない。このセクションでは、一般的な例をもとに、セキュリティ上の考慮事項をいくつか示す。このセクションで示す、セキュリティを SDLC に組み込むための主要な要素は、上述の分野において、共通に適用できる。ソリューションをセキュアにするために、関係者同士の関係を伝えて文書化することは、プロジェクトを成功に導くための鍵となる。

4.1 サプライチェーンとソフトウェア保証

サプライチェーン[4]とソフトウェア保証を確保するためには、民間の努力によって、ハードウェアとソフトウェアのコード作成における完全性、セキュリティおよび信頼性を促進するための最優良事例と方法論が、普及されるようでなければならない。これには、開発時に誤ったコード、悪意のあるコード、落とし穴が導入されないようにするためのプロセスと手順が含まれる。この分野は、成長し続けているため、将来にわたっては、より具体的な情報を提供するガイドラインが作成されるであろう。一般に、これらのプロセスと手順は、以下の 3 つの目標を達成するために用いられる:

- **信頼性** – 悪意をもって、または、意図せずに挿入された、利用可能な脆弱性が存在しないこと。また、資料が、偽物、著作権侵害、または知的財産権の侵害にあてはまらない、正規の文書であること。

- **予測可能な実施** – ハードウェアとソフトウェアが意図したとおりに機能することへの確信が得られること。

- **準拠** –ハードウェアとソフトウェアのプロセスと製品が、要件、標準および手順に確実に準拠するための、計画され体系化された多専門的活動を実施すること。

これらの目標を達成するために調達マネージャと情報セキュリティマネージャは、サプライチェーンにより生じるリスクをリスク軽減活動に含めなければならない。具体的には、以下のものが含まれる:

- 供給元の処理能力(ビジネス実践)に関する情報を利用して、供給元の製品とサービスの利用による、調達プロジェクトとシステムによってなされる業務へのリスクを特定する。

- 評価された製品に関する情報は、利用できるようにして、レビューを行うことで、悪用される可能性のある脆弱性を発見し、製品のセキュアな設定を行ってから製品を利用できるようにする。

4 サプライチェーンとは、製品の販売チャネルのことを言う。これには、製品の部品調達から、末端消費者への製品の引渡しまでが含まれる。

4.2 サービス指向型アーキテクチャ

サービス指向型アーキテクチャ(SOA)は、情報システム構造上のスタイルの一種であり、既存の、または新規の機能をサービスとして実装できる。これらのサービスは、1 つのサービスから別のサービスにデータを受け渡すことによって、または、一つ以上のサービス間で活動を調整することによって、コミュニケーションをはかる。NIST SP 800-95『(Guide to Secure Web Services)』は、SOA のセキュリティ考慮事項に関する詳細な情報を提供する。

SOA のセキュリティ管理に関する主な課題には、セキュリティ境界のスコーピング、適切なリスクレベルの割り当て、複数関係者のセキュリティ上の期待と責任を管理し、関係者の同意を得ること、などが含まれる。認可に関する戦略を考案することも、スケジュールと資源の観点からすれば、難題となることもある。従来の SDLC プロセスを適用できない場合であっても、ここで示すセキュリティ考慮事項のほとんどを適用することができる。政府機関は、費用効率が高く扱いやすい運用認可、継続監視、および再運用認可を可能にするアプローチを計画すべきである。

従来の解析ツール(スキャナ、侵入検知システム[IDSs]、パケットクラフティング／分析ツールなど)の多くが、サービス指向型アーキテクチャの総合的なセキュリティ状況を効果的に評価することができないため、このような評価はセキュリティアナリストにゆだねられる。セキュリティアナリストは、解析ツールを利用して、独自の SOA テストケースを適用し、脆弱性とリスクを分析するためのセキュリティ環境の合成モデルを推定する。

利用可能な自動化されたテストに加えて、以下に示す SOA 独自の側面に焦点をあてたレビューが推奨される。

- 追跡記録の承認と相関。
- サービス指向型アーキテクチャインテグレーションに関する記述(Service-Oriented Architecture Interaction Description)。これには、ポートレット、SAML (Security Assertions Markup Language)、SOAP(Simple Object Access Protocol)、UDDI(Universal Description, Discovery, and Integration)、WSDL(Web Services Description Language)、XACML(Extensible Access Control Markup Language)、および多くの WS-*標準(WS-Security 、WS-Policy、WS-Interoperability など)が含まれる。(この記述は、それぞれのアイテムのセキュリティ機能と便益にハイライトを当てたものである。)
- アクセス制御 (自由裁量および役割ベース)。
- コアエンタープライズサービスの構成および利用。
- 堅牢なメタデータの作成、保護および処理

4.3 セキュリティモジュールの再利用のための認定

アプリケーションと情報システムのオブジェクト指向化とコンポーネントベース化が進むにつれ、セキュリティ上の意味合いと、複数のプロジェクト(おそらく、複数の組織間で)でソフトウェアモジュールを再利用するコストを考慮しなければならない。コンポーネントとソフトウェアモジュールは、再利用を念頭において作成することが推奨される。特に、広範なプロジェクトにセキュリティ機能を提供するためのコードの作成には、このことが重要になってくる。これらのモジュールの承認と運用認可は、機能評価のための単体テストに類似するものであり、開発者、設計者およびエンジニアに対して、すぐに使える、信

頼できるコードから成るツールボックスを提供する。このようなツールボックスは、情報システムの開発段階におけるセキュリティコンプライアンスとリスクマネジメントを確実に実現するためのものであり、必要に応じて実施でき、費用も少なくてすむ。

認定されたモジュールに関しては、モジュールの特徴と機能を詳細に記述する。運用認可に関するドキュメントは、モジュールと一緒に保存する。運用認可を無効にするといったことがないような、使用事例と実施慣行にスポットを当てた開発者向けドキュメントも、利用できるようにする。モジュールとドキュメントは、開発者（または開発チーム）によるデジタル署名によって、運用認可の完全性と真正性を保持できるようにする。複雑なモジュール(独自のアプリケーションと考えられる)には、NIST SP 800-37 に記載のプロセスと本質的に同じプロセスを採用することがある。

4.4 組織をまたぐソリューション

組織をまたぐソリューションは、協定書またはサービス内容合意書に基づく、情報アプリケーションへのアクセスを必要とする。このようなアクセスが与えられることで、両組織(または複数の組織)に価値と便益がもたらされる。組織をまたがって利用できるアプリケーションは、対象の消費者に基づき 2 つのケースに分類される。最初のケースでは、「エンタープライズ」が対象となる。エンタープライズは、組織全体であり、独立したリソース(人、組織、および技術など)が含まれる。これらのリソースには、機能の調整と情報の共有によって、共通のミッション(または関連するミッション一式)を支援する。第 2 のケースでは、利益共同体(COI)が予測対象となる。COI は、共有ミッション、ビジネスプロセスおよび目的を支持するために、共通の語彙を使って情報を交換し合う、人々の集まりである。このコミュニティは、情報交換に参加するユーザ/オペレータ、これらのユーザのためのサービス、アプリケーション、機能およびシステムを開発する者、要件を定義し、ユーザに代わってリソースを確保する機能的な支持者から成る。

組織をまたぐソリューションを開発する際には、指針に関する草案文書を作成する(協定書やサービス内容合意書など)。これらの文書には、すべての関係者を適切に保護するための、セキュリティ機能と要件、および期待されるパフォーマンスレベルを記述する。さらに、将来のリスクを十分に管理するための、テストと有効性の検証に対する責任、インシデント対応手順、および監視と運用ポリシーに対する合意を得なければならない。ユーザとコード/アプリケーションの認証と承認には、特別な配慮が必要である。これには、ユーザ基盤の拡張計画、組織間の認証および承認システムの相互依存性、共通アクセス環境、および登録/登録抹消手順が含まれる。

4.5 テクノロジの進歩とメジャーな移行

情報技術が早いペースで進化し、これにともない情報技術が選択的に旧式化するにつれ、新システムにおけるセキュリティの SDLC への統合と他システムの統合に加えて、技術の進化に対処するためのシステムのオーバーホール、アップグレードまたは移行も考慮しなければならなくなった。情報技術が進化することによって、エンタープライズセキュリティにおける新たな課題が浮上し、欠陥のある実施／統合慣行を通じて、よく知られている脆弱性が再導入されるリスクが発生する。情報技術の相乗効果は、既存の問題をさらに深刻化させるようなリスクの相乗効果をもたらす。

組織が、情報技術の進化が持つセキュリティ上の意味合いを把握する場合や、システムの大掛かりな移行を計画する際には、情報システムセキュリティに関して、以下のような経験をすると考えられる:

- 組織が、組織のミッションを果たすために(またはミッションの変更に対処するために)、あるいは、ビジネス上の深刻な問題を解決するために初めて情報技術を導入する際には、セキュリティ要件のベースラインを緩和または除去することで、プロセスの進行を速めることがしばしばある。

- レガシーシステムの最終的な承認および運用認可においては、情報システムの既存のセキュリティ管理策の妥当性が評価される。レガシー基盤においては、通常、管理策によってセキュリティが実施される。それらの管理策は、承認され、運用認可を受けたものであり、リスクを適切に軽減できると判断されたものである。

- 最終的に、情報システムは成熟し、採用は増加し、脆弱性、リスク、その技術のリスク軽減戦略、および環境への理解は深まると考えられる。結果として、レガシーシステムに対する新技術のリスクマネジメント計画が、経営陣にとって納得のいくものとなり、システムの高機能が実証されることによって、システムへの信頼も高まることであろう。

情報技術の進歩とこれらの組織的行動の組み合わせによって、従来の技術から新しい技術へのセキュアな移行を計画し資本を投下する機会が、組織に与えられる。

また、これらの行動パターンは、先進技術や新しい技術に限られたものではない。10 年以上前に開発された情報技術が脚光をあびることは、よくあることである。このような技術は、時間の経過とともに、セキュリティがあまくなることがある。また、過去に、脆弱性が発見されて、それら脆弱性を克服するためのアクティブなパッチが適用されたと考えられる。

4.6 データセンタまたは IT 施設の開発

データセンタまたは IT 施設における開発上のセキュリティでは、物理セキュリティソリューションに重きを置いているが、重要なのは、以下のことを認識することである:データセンタは、アプリケーショを構築するための、大量の演算能力とストレージを収容する倉庫であり、データセンタの設備を利用するすべての顧客が適切に保護されていることを確実にするために、特別な注意を払わなければならない。

典型的な大規模組織は、データセンタを複数有することがある。それぞれデータセンタは、特定の顧客とミッションをサポートすることに責任を負うが、互いに連携することによって、高い可用性を提供する。また、このような連携によって、業務の継続と災害復旧に関する要件(多くの場合、データをオフサイトに格納できること、または、データを処理するための代替サイトを用意することが求められる)を、費用効率が高くなる形で満たせるようになる。データセンタは責任を共有し、冗長性のメトリクスを提供しなければならない。これらの条件下では、休止中のデータに加えて送受信中のデータも、データの分離を維持する必要がある。特に、データセンタスタッフの管理機能の職務と監査能力の分離は、確実に実施する。これによって、管理トラフィックとアプリケーションに対して別々の LAN や VLANs を使う必要性が正当化されることが多い。

この(技術上および運用上の)セキュリティの統合は、データセンタの仮想化が進み、仮想化されたオペレーションシステム環境全体を、データセンタ内の独立した個々のハードウェアプラットホームに移行する能力が高まるにつれて、より重要になる。

データセンタに特化した考慮事項の一つに、文脈上の環境データ(contextual environmental data)のセキュリティがある。このデータは、物理セキュリティシステム(カメラや運動センサーなど)の監視と、演

算を行うハードウェアの温暖な作業環境を保つための環境システムの監視から得ることができる。このデータは、ネットワークを介してアクセスできるデジタルメディアに追加保存される。このデータは、機密性が高く、攻撃者にコア情報システムへのアクセスを与える可能性があるため、慎重な取り扱いを要する。組織は、これらのシステムを適切に保護し、最終的なデータをオフサイトまたは帯域外にて保管する。帯域外の例としては、データセンタに設置されている顧客情報システムや、そのシステムが使用するネットワークを除く、ネットワーク／情報システムがある。

4.7 仮想化

仮想マシンとアプリケーションを使用することで実現できる仮想化は、コスト削減の機会を与えてくれる手法として、近年ますます利用される傾向にある。仮想化は、隔離と復旧の観点から追加のセキュリティを提供する一方で、仮想の実装に伴う固有のセキュリティリスクに対処するための、追加のセキュリティ計画を必要とする。このようなセキュリティリスクには、共有クリップボード、仮想マシンにおけるキーストロークロギング、および当該ホストのリソースへのサービス拒否などがある。

従来の物理プラットフォームのセキュリティ管理策のうち、仮想化の実装で一般的に見落とされる管理策には、以下のもの含まれる:

- 仮想マシンとホストにおけるマルウェア対策
- ホストとバージョンの管理業務の分離
- 監査に関するログを取ること、および仮想環境外への監査ログのエクスポートと格納
- 仮想マシンとホストにおける構成およびパッチ管理
- 仮想マシンとホスト間のネットワークトラフィックの暗号化
- 侵入検知システム(IDS)と侵入防止システム(IPS)による監視

仮想化が分散形ネットワークを利用することと、その実装が複雑であることから、仮想化を実装することによって、セキュリティ上の一般的な懸念事項がさらに深刻化することがある。このような懸念事項には、マルウェア、情報漏洩、パッチ管理、アクセス制御のあまさなどがある。

最高の結果を得るためには、セキュリティ(選択基準)を政府機関の選択基準に含めること、また、セキュアな配備およびメンテナンス計画を仮想ソリューションを実施する前に作成し、文書化することが求められる。

付録A – 用語集

用語	定義
Acceptance: 受け入れ	認定された政府担当者による行為。これにより政府は、自組織または別の省庁の代理として、入札済みの既存の特定供給品（サプライ）の管理または所有を引き継ぐ、または契約の一部または完全な履行によって提供される特定のサービスを承認する。受け入れは、設備やシステムが所定の技術および性能基準を満たすかに関する最終的な判断である。
Acquisition: 調達、取得	資産やサービスを調達するプロセスのすべての段階を含む。資産またはサービスの必要性を判断するプロセスに始まり、契約の完了および終結で終わる。
Business Impact Analysis (BIA): ビジネス影響分析	ITシステムの要件、プロセスおよび相互依存性を分析すること。組織は、BIAを利用して、システムの緊急時対応要件を具体化し、重大な障害が発生した際の優先順位付けを行うことができる。 情報源: *SP 800-34*
Certification and Accreditation – (C&A): 承認および運用認可	情報システムのセキュリティ管理策(管理、運用、技術上の管理策)の包括的なアセスメント。C&Aは、管理策がどの程度正しく導入されているか、どの程度意図したとおりに運用されているか、システムのセキュリティ要求事項に対する適合性の観点から望まれる結果をどの程度産出しているかを評価することで、セキュリティ認可を支援する。情報システムの運用の可否、および合意済みのセキュリティ管理策の導入を前提に、政府機関の業務（ミッション、機能、イメージまたは評判を含む）や資産、または個人に対するリスクを明示的に容認するか否かに関する、公式な意思決定。決定は、政府機関の上級責任者によって下される。 情報源*: SP 800-37*
Clinger-Cohen Act of 1996: 1996 年施行の Clinger–Cohen 法	「Information Technology Management Reform Act」とも呼ばれる。IT リソースを管理および調達する方法を大幅に変更した法律。各省庁が、価値を最大限に引き上げ、IT 投資のリスクを評価および管理するプロセスを構築し、実施するための要件を含む。
Closeout: 終結	すべての最終的な契約活動を含む（たとえば、あらゆる要件が完遂したことの確認や、最終支払いの実行など）。
Commercial off-the-shelf (COTS): 市販標準製品	既存の市販されているソフトウェアおよびハードウェア。Off–the–shelf（即納品）とも呼ばれる。

用語	定義
Contract administration: 契約の管理	設定された価格や予定内で、政府が契約書に既定された高品質の製品やサービスを受領できるようにする、政府による契約の管理。
Contracting Officer (CO):契約担当者	契約を締結、管理、および/または終了する権限を持ち、関連する判断や調査を行う人物
Contracting Officer's Technical Representative: 契約担当者の技術代理人	通常は、技術的指示および受け入れに関連して、CO が所定の契約管理責任を委任する人物。
Control Gate: コントロールゲート	システム開発活動をいつ評価するか、また、プロジェクトの継続、方向転換、中断を経営陣がいつ決定するかを示すポイント。
Deliverable: 成果物	契約条件に基づいて、政府向けに用意され、納入される製品またはサービス。
Environment: 環境	情報システムの開発、運用および保守に影響を及ぼす外部プロシージャ、状況とオブジェクトの集合。 情報源*: FIPS 200; CNSSI-4009*
Federal Acquisition Regulation (FAR): 連邦調達規則	執行機関で一貫した調達方針および手順を制定する規則。
Federal Information Processing Standards: 連邦情報処理基準	情報技術ラボラトリによって開発され、米国商務省の一部であるNISTによって発行された、政府機関向けの標準。FIPSは、共通レベルの品質、または一定レベルの相互接続性を確保するための情報技術に関する議題をいくつか取り扱う。
Federal Information Processing Standards Publications: FIPS 刊行物	FIPS PUB(刊行物)は、商務長官の承認後、NISTによって発行される。一部のFIPS PUBは、連邦政府の調達活動で必須とされている。
Federal Information Security Management Act (FISMA): 連邦情報セキュリティマネジメント法	FISMAは、政府機関に対して、ITセキュリティを資金計画およびエンタープライズアーキテクチャプロセスに組み込むこと、すべてのプログラムとシステムのITセキュリティのレビューを毎年実施すること、それらのレビューの結果をOMBに報告することを義務づけている。 情報源: *SP 800-65*
Information Resources: 情報資源	情報および関連資源。これには、人、設備、資金、情報技術などがある。 情報源: *44 U.S.C., Sec. 3502*

用語	定義
Information Security: 情報セキュリティ	機密性、完全性、可用性を確保するために、情報および情報システムを不正なアクセス、使用、開示、妨害、改ざん、または破壊から保護すること 情報源*: 44 U.S.C., Sec. 3542*
Information System: 情報システム	情報の収集、処理、保守、利用、共有、普及、または廃棄のために体系化された情報資源のセット。 情報源*: 44 U.S.C., Sec. 3502; OMB Circular A-130, App. III*
Information System Owner: 情報システムオーナー	情報システムの調達、開発、統合、修正または運用と保守に対して責任を有する者 情報源*: FIPS 200; CNSSI-4009 Adapted*
Information System Security Officer (ISSO): 情報システムセキュリティ担当者	上級情報セキュリティ責任者、運用認可権限者、管理職職員、または情報システムオーナーによって任命された個人であり、情報システムやプログラムの運用上の適切なセキュリティ状態を維持することに責任を持つ。 情報源*: SP 800-53; CNSSI-4009 Adapted*
Information Technology (IT) : 情報技術	データや情報の自動調達、保存、操作、管理、移動、制御、表示、切り替え、交換、送信、または受信に使用する装置または相互接続されたシステム。一般に、コンピュータ、付属装置、ソフトウェア、ファームウェア、同様の手順、サービス、および関連するリソースを含む。
Plan of Action and Milestones (POA&M): 行動計画とマイルストーン	このドキュメントには、計画の要素を達成するためのリソース、タスクを果たすためのマイルストーン、およびマイルストーン達成予定日について、詳細に記述する。このドキュメントには、計画の要素を達成するためのリソース、タスクを果たすためのマイルストーン、およびマイルストーン達成予定日について、詳細に記述する。このPOA&Mの目的は、政府機関が、発見されたプログラム上の、または、システム上の欠陥を是正するための活動の進捗を、特定、評価、優先順位付け、監視できるようにすることにある。 情報源*: OMB Memorandum 02-01*
Privacy Impact Assessment (PIA): プライバシー影響アセスメント	情報の取り扱いに関する分析であり、以下の目的で実施される: 1)情報の取扱いが、該当する法律上の要件、規制上の要件、および政策要件に確実に準拠するようにする。2)電子情報システムによって特定可能な形式で情報を収集、維持、普及する際の、リスクと影響を判断する。3)潜在的なプライバシーリスクを軽減するための、情報の取り扱いに関する保護対策と代替プロセスを検証し、評価する。 情報源: OMB Memorandum 03-22

用語	定義
Residual Risk: 残存するリスク	すべてのITセキュリティ対策が適用された後に残っている、潜在的リスク。個々の脅威には、関連する残存リスクが存在する。 情報源*: SP 800-33*

付録 B - 略語

AO	Authorizing Official(運用認可権限者)
AV	Anti-Virus(ウェルス対策)
BIA	Business Impact Assessment(ビジネス影響アセスメント)
C&A	Certification and Accreditation(承認と運用認可)
CCB	Change Control Board(変更管理委員会)
CIO	Chief Information Officer(最高情報責任者)
CISO	Chief Information Security Officer(最高情報セキュリティ責任者)
CM	Configuration Management(構成管理)
COI	Community of Interest(利益共同体)
CONOPS	Concept of Operations(運用概念)
COOP	Continuity of Operations(業務の継続)
COTR	Contracting Officer's Technical Representative(契約担当者の技術代理人)
COTS	Commercial Off-The-Shelf(市販標準製品)
CP	Contingency Plan(緊急時対応計画)
CPIC	Capital Planning and Investment Control(資本計画および投資管理)
DR	Disaster Recovery(災害時復旧)
EA	Enterprise Architecture(エンタープライズアーキテクチャ)
FAR	Federal Acquisition Register(連邦調達レジスタ)
FIPS	Federal Information Processing Standard(連邦情報処理基準)
FISMA	Federal Information Security Management Act(連邦情報セキュリティマネジメント法)
FOIA	Freedom of Information Act(情報公開法)
GAO	Government Accountability Office(会計検査院)
IDS	Intrusion Detection System(侵入検知システム)
IPS	Intrusion Prevention System(侵入防止システム)
IR	Incident Response(インシデント対応)
ISSO	Information System Security Officer(情報システムセキュリティ担当者)
IT	Information Technology (情報技術)
ITL	Information Technology Laboratory(情報技術ラボラトリ)
JAD	Joint Application Development(共同アプリケーション開発)
LAN	Local Area Network(ローカルエリアネットワーク)
NIST	National Institute of Standards and Technology(米国国立標準技術研究所)
OMB	Office of Management and Budget(行政管理予算局)
PIA	Privacy Impact Assessment(プライバシー影響アセスメント)
PII	Personally Identifiable Information(個人情報)
POA&M	Plan of Action and Milestones(行動計画とマイルストーン)
QA	Quality Assurance(品質保証)
RAD	Rapid Application Development(高速アプリケーション開発)
RFP	Request for Proposal(提案依頼書)
SAISO	Senior Agency Information Security Officer(上級情報セキュリティ責任者)
SAML	Security Assertion Markup Language(エスエーエムエル)
SATE	Security Awareness, Training, and Education(セキュリティ

	の意識向上、トレーニングおよび教育）
SCAP	Security Content Automation Protocol(SCAP)
SDLC	System Development Life Cycle（システム開発ライフサイクル）
SLA	Service-Level Agreement（サービス内容合意書）
SOA	Service-Oriented Architecture（サービス指向型アーキテクチャ）
SOAP	Simple Object Access Protocol（シンプルオブジェクトアクセスプロトコル）
SOW	Statement of Work（作業指示書）
SP	Special Publication（特別刊行物）
SSP	System Security Plan（システムセキュリティ計画）
ST&E	Security Test and Evaluation（セキュリティテストおよび評価）
UDDI	Universal Description, Discovery, and Integration（ユニバーサルディスクリプションディスカバリー＆インテグレーション）
USC	United States Code（合衆国法律集）
VLAN	Virtual Local Area Network(仮想 LAN)
WSDL	Web Services Description Language（ウェブサービス記述言語）
XACML	Extensible Access Control Markup Language（拡張可能なアクセス制御マークアップ言語）

付録 C - 参考文献

Clinger-Cohen Act, 40 United States Code (U.S.C.) 1401 and following, 1996.

Computer Security Act of 1987, Public Law (P.L.) 100-235.

National Technology Transfer and Advancement Act of 1995 (P.L. 104-113).

Privacy Act of 1974, 5 U.S.C. 552a.

E-Government Act, P.L. 107-347, December 2002.

Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. Chapter 35, Subchapter III, 2002.

OMB Circular A-130, *Management of Federal Information Resources*, November 2000.

GSA publication, *A Guide to Planning, Acquiring, and Managing Information Technology Systems*, Version 1, December 1998.

Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, June 2001.

FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

NIST SP 800-18 Revision 1, *Guide for Developing Security Plans for Information Technology Systems*, February 2006.

NIST SP 800-30,[5] *Risk Management Guide for Information Technology Systems*, January 2002.

NIST SP 800-33, *Underlying Technical Models for Information Technology Security*, December 2001.

NIST SP 800-37 Revision 1, Draft *Guide for Security Authorization of Federal Information Systems: A Security Lifecycle Approach*, August 2008.

NIST SP 800-39, Draft *Managing Risk from Information Systems: An Organizational Perspective*, April 2008

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, December 2007.

5 NIST SP 800-30 は、現在改訂中である。この改訂によって SP 800-30 の内容は、SP 800-39 に記載のリスクマネジメントフレームワークのさまざまなステップにおける、リスクアセスメントに焦点が置かれた内容になる。

NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, June 2008.

NIST SP 800-60 Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categorization Levels*, August 2008.

NIST SP 800-65, *Integrating Security into the Capital Planning and Investment Control Process*, January 2005.

NIST Interagency Report (NISTIR) 7298, *Glossary of Key Information Security Terms*, April 2006.

付録 D - NIST 参考文献マトリックスおよびウェブサイト

さらなる調査を支援するために、下記のメトリクスでは、SDLC におけるセキュリティ活動と、関連する NIST 刊行物の対応を記載している。詳細な情報は下記のウェブサイトから入手できる: http://csrc.nist.gov と http://nvd.nist.gov/scap.

セキュリティ活動	参考になる NIST Publications
フェーズ 1 – 開始	
1. セキュリティ計画作成を開始する	SP 800-64, -100, -37, -53
2. 情報システムを分類する	SP 800-60, FIPS 199
3. ビジネス影響をアセスメントする	SP 800-34
4. プライバシー影響をアセスメントする	SP 800-37
5. セキュアな情報システム開発プロセスを確実に使用する	SP 800-64, -16
フェーズ 2 – 開発／調達	
1. システムに対するリスクをアセスメントする	SP 800-30
2. セキュリティ管理策を選択して文書化する	SP 800-53
3. セキュリティアーキテクチャを設計する	SP 800-30
4. セキュリティ管理策と開発管理策を設計する	SP 800-53, FIPS 200
5. セキュリティドキュメントを作成する	SP 800-18
6. 開発テスト、機能テストおよびセキュリティテストを実施する	FIPS 140-2; SCAP website (see above)
フェーズ 3 – インプリメンテーション／アセスメント	
1. C&A セキュリティ承認と運用認可(C&A)の詳細計画を作成する	SP 800-37
2. 確立した環境またはシステムにセキュリティを統合する	SP 800-64
3. システムセキュリティをアセスメントする	SP 800-37, -53A
4. 情報システムを認可する	SP 800-37
フェーズ 4 – 運用／保守	
1. 運用準備状況を確認する	SP 800-70, -53A
2. 構成管理を実施する	SP 800-53A, -100
3. 継続的な監視を実施する	SP 800-53A, -100
フェーズ 5 – 廃止	
1. 廃止／移行計画を作成し実施する	None
2. 情報を確実に保存する	SP 800-12, -14
3. メディアをサニタイズする	SP 800-88
4. ハードウェアおよびソフトウェアを処分する	SP 800-35

セキュリティ活動	参考になる NIST Publications
フェーズ 1 – 開始	
5. システムをクローズする	None

付録 E – 他の SDLC 方法論

本書で論じているウォーターフォールモデル以外にも、多くの SDLC 方法論が存在する。組織は、それらの方法論を用いることによって、情報システムを効果的に開発できる。システムの予想規模と複雑さ、開発スケジュール、およびシステムの寿命は、使用する SDLC モデルの選択に影響する。ほとんどの場合、SDLC の選択は、組織の調達ポリシーによって定められる。採用される方法論、または開発プロセスの形式や期間にかかわらず、重要なのは、セキュリティ要件と考慮事項(重要なセキュリティドキュメントを含む)をライフサイクル全体を通して計画し、取り扱うことである。

共同アプリケーション開発

伝統的なウォーターフォールモデルでは、開発チームが、アプリケーションの開発に着手する前に要件を収集する(多くの場合、顧客に対する一連のインタビューを通して)。共同アプリケーション開発(JAD)方法論を用いることで、顧客とエンドユーザと開発者が JAD セッションを通して協力して、アプリケーションを設計、開発できるようになる。開発プロセスは顧客の大きな関与を必要とするため、この方法論を用いることで、開発を短期間で終えることができ、顧客の満足度も向上する。

プロトタイプモデル

プロトタイプモデルは、いったん要件分析が完了すると、プロトタイプタイプの設計と開発にすぐにとりかかることができるという点で、ウォータフォールモデルに似ている。作成されたプロトタイプは、顧客によって評価され、フィードバックが開発者に提供される。その後開発者は、顧客の期待に沿えるように、製品を改良する。

高速アプリケーション開発

高速アプリケーション開発(RAD)は、アプリケーションを短期間で作成するための開発方法論である。RAD では、使用する形式的方法論の数を少なくして、ソフトウェアコンポーネントを再利用するなど、アプリケーションの開発速度を速めるための技法が用られる。高速な開発と引きかえに、機能性とパフォーマンスに関しては、ある程度の妥協が必要となることもある。しかしながら重要なのは、短期間での製品の納入と引きかえに、セキュリティ面での妥協が生じないようにすることである。具体的には、情報と情報システム、およびそれらが提供するミッション機能を適切に保護するためのセキュリティ管理策の選択と仕様において、妥協が生じないようにする。

スパイラルモデル

スパイラルモデルは、プロトタイプとウォーターフォールモデルの特徴を組み合わせた開発技法である。スパイラルモデルは規模が大きくて費用がかかる、複雑なプロジェクトに好んで採用されることが多い。スパイラルモデルプロセスには、通常、要件定義と初期設計の考案、および最初のプロトタイプの作成と評価が含まれる。その後、プロトタイプが洗練されて望まれる製品に仕上がるまで、後続のプロトタイプに対して同じプロセスが繰り返される。最終的なシステムは最終的なプロトタイプに基づいて構築され、実稼働環境にて評価、維持される。

付録 F – さらなる調達に関する考慮事項

本書は、政府機関が重要な情報セキュリティ手順を IT システム開発ライフサイクル(SDLC)に組み込む際に役立つ資料として、作成された。本付録は、調達計画作成に関する追加の考慮事項について論じている。これらの考慮事項は、SDLC の開発／調達フェーズにおける情報セキュリティの確立に寄与する。

- **契約のタイプ**

  契約のタイプ（たとえば、確定価格、時間-材料契約、実コストと確定費用など）は、セキュリティ上の重要な意味を持つことがある。仕様を開発している情報セキュリティ技術専門家と契約担当者は協力して、組織にとって最も有利になる契約タイプを選択する必要がある。

- **他の機能グループによる検討**

  システムの規模と範囲に応じて、さまざまな機能グループの参加者から構成されるグループ（たとえば法務、人事、物理的セキュリティ、記録管理など）が役立つ場合がある。これらの機能グループは、機密性、完全性、および可用性の保証要件に対する見識を持っている必要がある。早くからこれらのグループが計画プロセスに関わることが重要なのは、ライフサイクルコストを減らす結果となり、また初期段階では要件を変更しやすいからである。

- **承認エージェントと運用認可権限者による検討**

  OMB Circular A-130、付録 III は、システムが、特定の環境でデータを処理できるように承認または認可されることを要求している。システムを保護するために、管理上、運用上、および技術上のセキュリティ管理策を導入する必要がある。管理および運用上のセキュリティ管理策は、契約の範囲から外れることがある。理由としては、組織でこれらのセキュリティ管理策を実施する責任が、開発者にないことが挙げられる。さらに、技術的セキュリティ機能および保証セキュリティ仕様を、開発者との契約に含めなければならない。これらのセキュリティ管理策は、技術仕様の開発に織り込む必要がある。運用認可権限者（AO）は、残余リスクを受容できるレベルまで低減するために、セキュリティ管理策全体が適切かどうかを判断する際に、これらの前提を考慮する。

  C&A テストには、組織が実装した管理および運用上のセキュリティ管理策も含まれる。組織が実装したこれらのセキュリティ管理策の有効性を判断することは、セキュリティ管理策アセスメントの役割である。アセスメントプロセスは、システムセキュリティ計画における想定が、想定どおりにインプリメントされており、またセキュリティコントロール全体が、残余リスクを受容可能なレベルまで低減するために適切であることを確認する必要がある。契約者が開発したシステムのセキュリティ属性の受け入れテストは、C&A プロセスの一部としてセキュリティテストの前提条件になる。

  AO は、システム運用でのリスクを承認する責任がある。ゆえにシステムの最終的な運用に関連したリスクが受容できないように思われる場合には、開発チームにアドバイスできる。仕様によっては、受容可能な残余リスクがわからない場合に、過度の負担とコストを必要とする場合もある。受容可能な残余リスクの判断には、AO の関わりが必要になる。システム調達の計画段階中に要件の変更を組み入れた方が、要請、ソース選択、または契約管理の段階中に組み入れるよりも簡単である。

- **プロセスの循環的な性質**

開発／調達フェーズでのセキュリティ手順は、循環的に取り組む必要がある。これらの手順は相互関連しており、互いに依存している。システムの規模と複雑さに応じて、これらの手順は、しばしば考えが精緻化されるに従って実行されることがある。

- **評価と受け入れ**

  システム評価計画と適切な受け入れ基準が、調達/開発フェーズで開発される。要請は、評価にあわせて設計される必要があり、評価はテストと分析を含む必要がある。インプリメントされたシステムが仕様に準拠しているかどうかを明確に判断できるように仕様を作成する。一般に、2 つの別々の活動、つまり契約の受諾と C&A でセキュリティテストが必要になる。

  契約の受諾は、通常、開発者との契約に含まれる機能および保証セキュリティ仕様だけを扱う。C&A テストには、組織が実施した管理および運用上のセキュリティ管理策も含まれる。開発者が責任を負うこともある管理策の導入と正しい運用は、システムセキュリティ要件に前提として含められていることもある。組織でインプリメントするセキュリティ管理策の適切な判断は、C&A テストの役割である。開発したシステムのセキュリティ属性の受け入れテストは、C&A プロセス下でのセキュリティテストの前提条件になる。

- **提案要求書の作成**

  提案要求書（RFP；Request for Proposal）によって、連邦政府は、提供者の提案に基づいて、最も価値の高い決定を行うことができる。RFP プロセスの長所は、連邦政府のニーズに最も適合する契約を取り決めるときに、連邦政府と提供者に柔軟性が与えられる点である。

  連邦政府は、必要な情報セキュリティの機能、手続き、および保証をさまざまに特定できる。また、RFP は柔軟なドキュメントにもなりうる。調達の代替案に関するガイダンスは、組織の調達オフィスまたは契約担当者に確認する必要がある。

- **セキュリティ仕様および作業ステートメントの開発**

  セキュリティ仕様および作業ステートメント（SOW；Statement of Work）は要件分析に基づく。仕様は、システムが行うことになっている作業に関する詳細を提供する。また、仕様は、インプリメントのメカニズム、戦略、および設計とは独立して作成する必要もある。つまり、仕様ではシステムが行う方法ではなく、行うべきことを記述する。

  SOW は、開発者が契約を実施するときに行う必要がある作業について詳述する。たとえば、契約下で開発されるドキュメントは、SOW で指定される。セキュリティ保証要件は、開発者が従うプロセスの多くの側面について、また、プロセスが正しく完全に遂行されていることを組織に保証するために調達する必要のある証拠について詳述している。セキュリティ保証要件も SOW で指定されることがある。

  セキュリティ機能要件が、セキュリティ仕様に対応付けられるという一般規則には例外がある。セキュリティ機能をインプリメントするためのメカニズムの選択は、提案の準備中ではなく、システム運用ライフサイクル中に行われることがある。テクノロジまたはセキュリティ環境の変更に対応するために、このような決定はシステム運用ライフサイクルに委ねられる。たとえば、ライフサイクル中に、認証メカニズムが、再利用可能な記憶方式のパスワードから、バイオメトリクス技術によるトークンに変更されることがある。システム運用ライフサイクル中にセキュリティ機能を実装するためのメカニズムを選択する場合、組織は、SOW において、研究を行い単一のメカニズムまたはメカニズムの組み合わせを推奨する作業を開発者に割り当てることができる。単一のメカニズムまたはメカニズムの組み合わせの選択は、依然として、調達している組織の役割になっている。

セキュリティ仕様と作業ステートメントがシステムのセキュリティ属性を完全および明確に表していない場合、そのシステムは必要なレベルのセキュリティを確保できないことは、これまでの例でも明らかである

以降の項では、一般的な仕様と連邦規定の仕様という、情報セキュリティ仕様の 2 つのソースについて説明する。調達責任者は必要なものに焦点を当て、契約担当者と協力して、その要求に最も適した方法を判断する必要がある。

- **一般的な仕様**

  一般的な情報セキュリティ仕様には、NIST ガイドライン、商用ソース、および業界団体のガイダンスなど、多くのソースを利用できる。

  一般的な情報セキュリティ仕様は、レビューを実施して、調達するシステムへの適合性を確認する。これらの仕様は、見落としがちな領域に関する情報を提供する。また、これらの仕様は直接使用できる言語を提供するため、時間の節約にもなる。しかしながら、これらのソースをもとに、機能、手順および保証事項を選択する際には、注意が必要である。これらのアイテムは、アイテム間の相互依存性に応じて、一般的な情報セキュリティ仕様にグルーピングされることもある。機能、手順、保証事項、およびグルーピングの有無をしっかりと理解したうえで、これらのアイテムを指定する必要がある。

  各仕様は、要件分析、特にリスクアセスメントに照らして正当化されていなければならない。一般的なソースが推奨する保護は考慮する必要があるが、リスクアセスメントがサポートしていない場合は、RFP に含めてはならない。

- **連邦規定の仕様**

  連邦機関は、法の定めるところにより、RFP に追加仕様も含めなければならない。これらは、指定仕様と呼ばれることがある。すべての連邦機関は、該当する連邦政府政策と FIPS 刊行物にシステムが準拠するように徹底させなければならない。政府機関は、組織の法律担当者と調達責任者の同意を得て発布された公的なポリシーである、指定仕様を要求できる。

  指定仕様は、調達されているシステムが指定仕様の基準に一致している場合、RFP や他の該当する調達ドキュメントに取り入れる必要がある。指定仕様を意識することは、非常に重要である。

  該当する法律、規制、およびポリシーを RFP に取り入れることは、システムを調達する連邦機関の責任になる。全体の行政機関に影響する指令に加え、各部門および独立機関は、独自の一連の通達、命令、および基準を持っている。

  技術仕様とは別に要件を列挙するだけでは不十分である。ポリシーの解釈を開発契約者に任せたままではうまくいかない。むしろ、関連するポリシーとガイダンスを解釈するか、少なくとも技術セキュリティ仕様で参照する必要がある。

  FIPS 刊行物は、NIST コンピュータセキュリティリソースセンター（http://csrc.nist.gov）で入手できる。該当する OMB Circular、覚書、およびポリシードキュメントは、http://www.whitehouse.gov/omb で入手できる。

  1995 年施行の国家技術移転促進法(National Technology Transfer and Advancement Act)（公法[P.L.]104-113）では、連邦政府の部局および機関に対して、実用的な場合は、

自発的で合意に基づく標準化団体によって開発された技術産業基準を使用することを命じている。

調達されているシステムにどの連邦規定の仕様が適用されるかを把握しておくことは、調達責任者の責務になる。多くの人々が、この取り組みに責任があるのは契約担当者であると間違って信じている。しかし、これらは技術的な問題なので、この責任は調達責任者にある。

- **提案の評価**

提案の評価プロセスでは、オファーが、RFP に記載された最低の要件を満たしているかどうかを判断し、提供者が予想される契約を十分遂行できるかどうかを査定する。この取り組みには、提案のメリットに関する技術的分析が含まれる。調達/開発フェーズの一部として、調達責任者は契約担当者と協力して、評価の基準とその実施方法を判断するための評価計画を開発する。評価自体は、調達のソース選択フェーズ中に実行される。情報セキュリティは、連邦政府に対するセキュリティの重要性に注意を促すために、評価基準で取り扱う必要がある。提供者は RFP（特に RFP L および M 項）を研究し、連邦政府が最も重要とみなしているものを理解する。

- **評価計画の策定**

情報セキュリティ機能を評価するとき、オファーが最低要件を満たしているか、予想される契約を十分に遂行できるかどうかを査定することが難しい場合がある。したがって、提供者は、情報セキュリティ機能に関するハードウェアとソフトウェアの説明が間違いないこと、提供者が提案のサービスを提供できることを、連邦政府に保証する必要がある。しかし、情報セキュリティは、コンピュータシステムの他の側面と同様に、複雑で重要な問題であるので、提供者の主張は、十分な保証とはならない可能性がある。

保証の提供の仕方によっては、連邦政府がそれを適切に査定できるかどうかに関わることがある。SOW は、保証要件など、システムの開発に関する連邦政府の要件を指定する。一般に、保証仕様には、連邦政府によって検討されるドキュメントが含まれている。裁定後、保証がさらに必要だと連邦政府が判断した場合、システムを十分に開発するために追加資金が必要になることがある。

提供者がどの程度の保証を提供する必要があるかに関する判断は、評価計画の策定時に考慮しなければならない。この計画は、提供者に対する指示や提案の評価方法およびソース選択の実行方法に関する情報を提供する RFP 条項の作成段階で使用される。

このプロセスの一部として、セキュリティの受け入れテストの判断を行う必要がある。C&A と同様にセキュリティテストおよび評価（ST&E；Security Testing and Evaluation）を承認の一部として調整し、連邦政府の取り組みを効果的に管理することは重要である。

一定のテストと評価が、提案の評価の一部として行われることがあり、ベンチマークと機能実証を導入できる。ベンチマークにはストレステスト（レスポンス時間、スループットなど）が含まれ、セキュリティテストと類似している。このようなベンチマークの範囲とレベルの選択はビジネス上の判断によって決められる。また、購入者としての連邦政府と提供者の両者がコストを負担する。いずれかの当事者が、コストが非常に高いと判断する場合もある。徹底した ST&E を受ける提案の数を制限するために、提案の評価を構造化できる。たとえば、セキュリティ機能実証はすべての提供者に対して要求し、保証およびペネトレーションテスト（侵入テスト）は明確に選択した提供者にのみ適用することができる。

既存の製品、開発されるシステム、およびサービスの ST&E の間には大きな違いがある。組織は、開発されるシステムとサービスに関してあいまいな部分がある。1 つのアプローチは、提案されたセキュリティ機能、保証、およびサービスが提供されなかった場合、これを、さまざまな法的

制裁が設けられた契約違反とみなすことである。連邦政府は、評価のために有意義で一貫した結果がもたらされるように、契約前の機能実証を構成することができる。

セキュリティへの脅威とセキュリティポリシーへの組織の取り組みをはっきりと明確化すること、および提案されたセキュリティ手段が意図された目的にとって明らかに十分であることが重要である。保証は、信頼することになる製品または情報システムの評価（積極的調査）に基づく必要がある。ドキュメントと結果として生じる IT 製品またはシステムの妥当性は、範囲、深さ、および厳格さに重点を置いて、専門の評価者が測定する必要がある。

アーキテクチャと設計は、脆弱性とテストに大きな影響を与える。優れた設計には、基準としてテスト容易性が含まれている。未知のセキュリティ属性を持つシステムとサービスの導入によるセキュリティへの影響を軽減するための、アーキテクチャと設計を使用することによって、ST&E の費用を最小限に抑えることができる。セキュリティのアーキテクチャと設計には、脆弱性およびリスクを軽減し、ST&E のコストを下げるテクニック（カプセル化や隔離など）を採用する必要がある。

対応策を組み込んだセキュリティアーキテクチャを考慮する必要がある。これらの対応策には、個々のネットワーク用のポイントソリューション（ファイアウォールや侵入検知システム[IDS]など）、セキュリティ情報管理（SIM）、セキュアネットワーク管理（SNM；Secure Network Management）システムとの SIM 統合などがある。

- **評価計画で考慮すべき項目**

この項の残りの部分では、評価計画の情報セキュリティ関連部分の開発に役立つ概念について説明する。

評価計画を開発するときに、機能代替案とセキュリティ代替案が互いに矛盾することがある。たとえば、情報セキュリティをもたらす機能が、簡単な操作性をもたらす機能と矛盾する場合がある。どのように提供者が異なる構成を提案し、矛盾するオプションとトレードオフを示せばよいかを、連邦政府は明確にする必要がある。ただし、検討を容易にし、提案の準備費用を最小限に抑えるために、提案を手頃なサイズにとどめておくように注意すべきである。

テストは、提案されたシステムまたは製品が、情報セキュリティ要件を満たせるかどうかを判断する 1 つの方法である。テストは、システムの性質に応じて、実際のテスト実証またはベンチマークの形式で、提案の評価に組み入れることも、契約後の受け入れテストに組み入れることもできる。評価プロセス中、テストは、費用、技術、および調達の完全性の考慮事項に応じて、いろいろな場合に使用できる。しかし、提供者の提案の準備費用を抑制するため、費用のかかるテストは最小限にとどめておくべきである。費用のかかる提案は、競争を抑制するだけでなく、最終的にはその費用は契約費用の高騰となって連邦政府に回されることになるからだ。

情報システムテスト、特にパフォーマンステストは、情報セキュリティ機能を有効にして実行すべきである。

調達責任者の市場に関する認識が高いほど、評価計画の開発に伴う負荷が軽減される。ただし、市場調査には提案を使用できない。また、提案を受領した後では、評価計画を変更できない。さらには、他の提案からの追加情報を使用して、評価計画を修正することもできない。しかし、連邦政府の真の優先順位を反映した評価方法を確実に開発するために提供された代替案を調査することは有用である。

- **特別契約要件**

RFP における要素の中には、情報セキュリティに関連していても、SOW または評価基準に含まれないものがある。これらの要素は通常、契約の当事者に割り当てられる権利、責任、および賠償を扱っている。多くの場合、このような義務は、契約の実際の遂行期間（POP；Period of

Performance）を通じて効力を持つ。したがって、こうした要素は、特別契約条項または要件で対処すればよい。契約期間中に取得した情報の非開示の要件が一例になる。

付録 G - SDLC 内セキュリティの追加グラフ図