NIST Special Publication 800-55 Revision 1

情報セキュリティ
パフォーマンス測定ガイド

Elizabeth Chew, Marianne Swanson, Kevin Stine,
Nadya Bartol, Anthony Brown, and Will Robinson

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

情報セキュリティ

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

2008 年 7 月

米国商務省長官
Carlos M. Gutierrez, Secretary

米国立標準技術研究所 副所長
James M. Turner, Deputy Director

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レポート

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）、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、行政管理予算局による通達（OMB Circular: Office of Management and Budget Circular、以下OMB Circular と称す）の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、SP800-55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。

本文書は、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、完全に正確であること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

本書執筆陣は、本書のドラフトをレビューし作成に貢献してくれた Joan Hash (NIST)、Arnold Johnson (NIST) 、Elizabeth Lennon (NIST) 、Karen Scarfone (NIST) 、Kelley Dempsey (NIST), および Karen Quigg (MITRE)に感謝の意を表する。また、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

表

要旨

本書は、システムレベルとプログラムレベルの測定指標（measures）の策定、選択、実装を支援するための手引である。これらの測定指標は、システムとセキュリティプログラムに適用されているセキュリティ管理策の有効性を評価するためのものである。測定指標は、パフォーマンスに関連する適切なデータの収集、分析、報告を通じて、意思決定を促進し、パフォーマンスや説明責任を改善することを目的として設計されたツールである。また、これにより政府機関の任務を成功裏に果たすうえで、システムとセキュリティプログラムに適用されているセキュリティ管理策の効率と有効性を確保することがいかに重要であるかを示すことができる。本書に記載のパフォーマンス測定指標の策定プロセスは、政府機関において情報セキュリティを実施する者が、与えられた権限と組織の任務にもとづいて、情報システムとセキュリティ活動との関連性を確立するのに役立つ。また、情報セキュリティの重要性を組織に示すうえでも有用である。

現在ある法律、規定、規制の多くにおいて、パフォーマンスの測定、特に情報セキュリティパフォーマンスの測定が要求条件とされている。そのような法律には、クリンガー・コーエン法(Clinger-Cohen Act)、政府業績成果法(GRPA : Government Performance and Results Act)、政府事務書類制限法(GPEA : Government Paperwork Elimination Act)、連邦情報セキュリティマネジメント法(FISMA : Federal Information Security Management Act)などがある。法律を遵守することに加えて政府機関は、パフォーマンス測定指標を、内部改善のための管理ツールとして使用することができる。これは、セキュリティプログラムの実施を政府機関レベルの戦略計画に関連づけるうえで、有用である。

以下に、情報セキュリティ測定プログラム（information security measurement program） の策定および実施において考慮すべき事項を示す。

- ●測定指標により、定量化可能な情報(割合、平均、数値)が得られること
- ●測定指標の根拠となるデータは容易に入手できること
- ●測定指標の対象は、繰り返し可能なセキュリティプロセスのみとすること
- ●測定指標は、パフォーマンスの追跡やリソースの割り当てに役立つものでなければならない

本書で述べる測定指標作成手順に従えば、パフォーマンスが低いことの原因が明確化され、それによって適切な是正措置が示されるような測定指標を作成することができる。

本書では、以下の 3 種類の測定指標の策定と収集に焦点を当てている。

- ●セキュリティポリシーの実施状況を評価する測定指標
- ●セキュリティサービスの提供結果を評価する効率／有効性測定指標
- ●セキュリティイベントがビジネスまたはミッションに与える影響を評価する影響測定指標

実際に取得可能でパフォーマンスの向上に役立つような測定指標のタイプは、組織のセキュリティプログラムの成熟度と、システムのセキュリティ管理策の実装に依存する。同時に異なるタイプの測定指標を使用することは可能だが、セキュリティ測定指標の主な焦点は、セキュリティ管理策の実施が進展するにつれて変化する。

1. はじめに

セキュリティパフォーマンスの測定は、規制上の理由、財政上の理由、および組織上の理由により必要とされることが多い。現在ある法律、規定、規制の多くにおいて、パフォーマンスの測定、特にセキュリティパフォーマンスの測定が要求条件とされている。そのような法律には、クリンガー・コーエン法(Clinger-Cohen Act)、政府業績成果法(GRPA : Government Performance and Results Act)、政府事務書類制限法(GPEA : Government Paperwork Elimination Act)、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)などがある。

これらの法律、規定、規制が、情報セキュリティ測定（information security measurement） を促す主な要因となる一方で、そのような情報セキュリティパフォーマンスの測定が組織にもたらす利益も、パフォーマンス測定を実施する強い動機となる。政府機関は、パフォーマンス測定指標(performance measures)を、内部改善のための管理ツールとして使用することができる。これは、セキュリティプログラムの実施を政府機関レベルの戦略計画に関連づけるうえで、有用である。情報セキュリティ測定指標は、パフォーマンスに関連する適切なデータの収集、分析、報告を通じて、意思決定を促進し、パフォーマンスや説明責任を改善することを目的として設計されたツールである。測定指標によって、管理策の実施、効率および有効性が、極めて重要な活動を成功裏に行ううえでいかに重要であるかを示すことができる。本書に記載のパフォーマンス測定指標の策定プロセスは、政府機関において情報セキュリティを実施する者が、与えられた権限と組織の任務にもとづいて、情報システムとセキュリティ活動との関連性を確立するのに役立つ。また、情報セキュリティの重要性を組織に示すうえでも有用である。

1.1 目的および適用範囲

本書は、セキュリティ管理策の実施状況、管理策の効率と有効性、および管理策がもたらす影響と、そのほかのセキュリティ関連活動に関する情報を示す、システムレベルとプログラムレベルの測定指標の策定、選択、実装に関する手引きである。本書では、測定指標を使って現在実施中のセキュリティ管理策、ポリシー、手順が適切であるかを確認する方法を示している。また、マネジメント層が追加のセキュリティリソースをどこに割り当てるかを決定し、生産的でない管理策を特定、評価し、継続的監視の対象となる管理策の優先順位付けを行うのに役立つアプローチを説明する。さらに、測定指標を策定して実施する手順と、測定指標を使用してセキュリティ管理策の投資を十分に正当化し、リスクにもとづく判断を支援する方法についても説明する。効果的な情報セキュリティ測定プログラムが作成できれば、セキュリティリソースの割り当てを決めるために役立つデータが得られ、パフォーマンスに関する報告の準備が容易になる。そのようなプログラムをうまく実現できれば、セキュリティプログラムの状況を毎年報告することを求める行政管理予算局(OMB: Office of Management and Budget、以下 OMB と称す)の要件を満たすことができる。

NIST SP800-55 Revision1 は、セキュリティ測定指標に関する既存の NIST 文書を拡張したものであり、プログラムレベルでセキュリティパフォーマンスを定量化するための手引きとなる。（これにより組織の戦略目標が支援される。）本書に記載の手順と方法論は、政府機関レベルの戦略計画作成プロセスを通じて、システムセキュリティパフォーマンスと政府機関のパフォーマンスを関連づけるものである。また、これらの手順と方法論によって、情報セキュリティがどのような形で組織の戦略目標と目的の達成に貢献するかを示すことができる。本書のガイドラインに沿って策定したパフォーマンス測定指標を使用することで、組織は、政府機関に義務付けられた種々の要求事項や方策(FISMA を含む)への対応能力を高めることができる。

本書は、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)』に記載のセキュリティ管理策を、情報セキュリティプログラムの評価を支援する測定指標の策定に利用している。本書では、測定指標の策定に関するガイドラインに加えて、政府機関が調整、拡張したり、ほかの測定指標を策定する際のモデルとして利用できる測定指標のリストを記載している。[1] 本書に記載の NIST SP 800-53 のセキュリティ管理策に関する情報は、NIST SP 800-53 に含まれないセキュリティ管理策に対する政府機関独自の測定指標の作成にも適用できる。

本書に記載の情報セキュリティ測定プログラムは、法的な要求事項を満たすために役立つ。このプログラムは、データ収集、分析、報告の基盤を提供する。このような基盤は、以下のものを支援するために、組織が調整できるようになっている ー FISMA パフォーマンス測定指標、連邦エンタープライズアーキテクチャ(FEA: Federal Enterprise Architecture、以下 FEA と称す)の業績測定参照モデル(PRM)の要求事項、セキュリティパフォーマンスに関する定量化可能情報の報告を義務付ける組織固有の要件。

1.2 対象とする読者

本書は主に、最高情報責任者、上級情報セキュリティ責任者(最高情報責任者と呼ばれることが多い)、および情報システムセキュリティ責任者向けに書かれたものである。本書は、NIST SP 800-53 に記載のセキュリティ管理策に精通している者を対象としている。本書が示す概念、手順および測定指標は、政府機関および産業界において使用できる。

1.3 これまでの経緯

セキュリティ管理策の有効性を測定するアプローチは、長年にわたって検討されてきた。NIST SP 800-55『情報技術システムのためのセキュリティメトリクスガイド(Security Metrics Guide for Information Technology System)』と NIST SP 800-80(ドラフト) 『Guide to Developing Performance Metrics for Information Security』は、両方ともセキュリティ測定指標を扱っている。本書は、これらの文章をベースにしたものであり、これらの文章で紹介しているアプローチを、NIST SP 800-53 に記載のセキュリティ管理策に適用している。また、NIST SP 800-55 の原本の概念とプロセスを拡張した文書でもあり、組織によるセキュリティプログラム実装の評価を支援することを目的としている。

情報システムと情報セキュリティプログラムのためのセキュリティ管理策の実施に関しては、2002 年施行の電子政府法(Electronic Government Act)に従って毎年レビューを行い、OMB に報告する。電子政府法には、FISMA が含まれ、この法令では、各部門や機関が、該当するセキュリティ要件を満たしていることを証明し、年次のプログラムレビューを元に実際のパフォーマンスレベルを文書化することを義務付けている。

1 本書が提供する測定指標の候補は必須ではない。むしろ、本書の読者がサンプルとして使用できることを意図したものである。

1.4　重要な成功要因

組織内の情報セキュリティ測定プログラムには、互いに依存する 4 つの要素が含まれる(図 1-1 参照)。

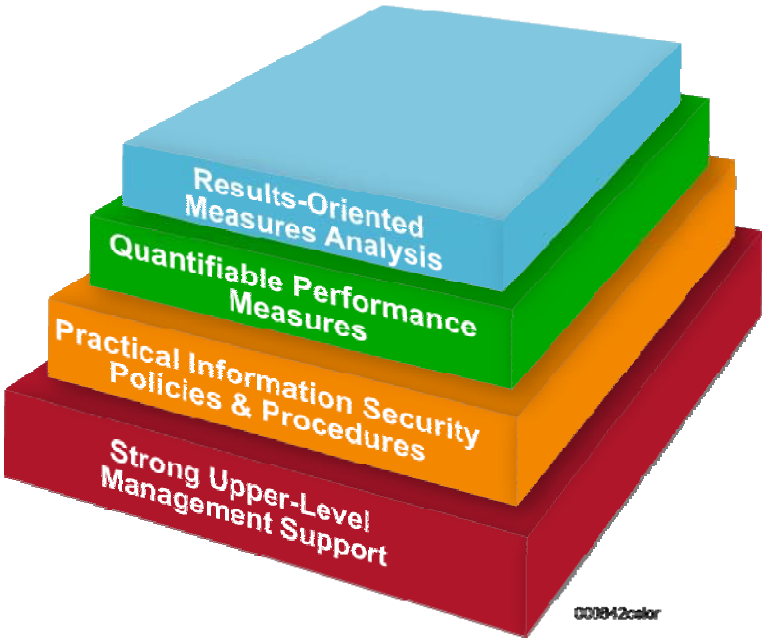

図1-1 情報セキュリティ測定プログラム構造

上級マネジメント層の強力なサポートという基盤は、情報セキュリティプログラムの成功だけでなく、プログラムの実施にとっても必要不可欠である。このサポートがあってこそ、組織の最上位レベルにおいてセキュリティにフォーカスする風土が形成できる。堅牢な基盤(つまり、情報資源を管理する地位にいる人の積極的なサポート)がないと、政策上の制約や予算上の制約による圧力が加わった場合に、情報セキュリティ測定プログラムが有効に機能しなくなる可能性がある。

有効な情報セキュリティ測定プログラムの2つ目の要素は、強制的に従わせるのに必要な権限に後押しされた、実務的なセキュリティポリシーと手順の存在である。セキュリティポリシーは、セキュリティマネジメント構造を概説し、情報セキュリティに関する各担当者の責任を明らかにし、進展と遵守を確認するための基盤を提供する。セキュリティ手順は、セキュリティ管理策の実施に関するマネジメント層の責任と立場と、それらの管理策をどのレベルまで適用するかを文書化する。測定に必要なデータを用意するための手順が規定されていない場合、測定指標を容易に得ることはできない。

3つ目の要素は、意味のあるパフォーマンスデータを捕捉・収集できるような、定量化可能なパフォーマンス測定指標を策定して定着させることである。意味のあるデータを得るためには、定量化可能な情報セキュリティ測定指標がセキュリティのパフォーマンス目標と目的に基づいたものであり、容易に取得可能かつ評価可能なものでなくてはならない。また、繰り返しが可能で、パフォーマンスの経時的な傾向を提供し、パフォーマンスの追跡とリソースの管理に役立つものでなければならない。

最後に、情報セキュリティ測定プログラムで非常に重要なことは、定期的に一貫した測定データ分析の実施である。分析結果は、その結果から得た教訓を生かし、既存のセキュリティ管理策の有効性を向上させ、新しいセキュリティ上の要件が出てきた時に備えた将来的な管理策を計画するために使用する。収集したデータがセキュリティプログラム全体の改善にとって意味のある有用なデータとなることを確実にするためには、データを正確に収集することが不可欠であり、このことが利害関係者と利用者にとっての再優先事項とならなければならない。

セキュリティプログラムの実施の成否は、どの程度意味のある結果が得られたかで判断されるべきである。総合的な情報セキュリティ測定プログラムは、組織のセキュリティに対する姿勢に直接影響を与えるような意思決定のための、本質的な根拠を提供する。この意思決定には予算と要員の要求、手持ちのリソースの割り当てが含まれる。情報セキュリティ測定プログラムは、提出が義務付けられているセキュリティパフォーマンス報告書を準備する際に役立つ。

1.5 他の NIST 文書との関係

本書は、NIST special publications シリーズの文書で、情報管理者と情報セキュリティ要員による情報セキュリティプログラムの策定、実装、維持を支援することを目的としている。本書は、さまざまな情報セキュリティ活動の結果に基づき、セキュリティパフォーマンスを定量化することに焦点を当てる。このアプローチは、多くの情報源に依存する。これらの情報源には以下のものが含まれる。

- **●情報セキュリティアセスメントおよびテストに関する取り組み** 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)』に記載されているような取り組み。
- **●情報セキュリティリスクアセスメントに関する取り組み** NIST SP800-30『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)』に記載されているような取り組み。
- **●必要最低限の推奨セキュリティ管理策** NIST SP800-53『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)』が奨励するセキュリティ管理策。

NIST SP800-55 Revision 1 は、セキュリティ管理策の実施状況と有効性をシステムレベルとプログラムレベルで測定、分析するための、定量的アプローチを提供する点で、NIST SP 800-53A と異なる。このようなアプローチは、複数の取り組みによって実現される。本書はまた、複数のシステムから情報を収集し、企業レベルでセキュリティを測定、分析するためのアプローチを提供する。NIST SP 800-53A は、管理策が、システムのセキュリティ計画に沿って意図したとおりに導入され、運用されているかを評価するための、手順を提供する。NIST SP800-53A のアセスメント手順を適用することで得たアセスメント結果は、情報セキュリティを評価するためのデータとして使用できる。

本書に記載の情報セキュリティ測定結果は、いくつかの NIST publication に記載のセキュリティプログラム活動に対する入力を提供する。それらの NIST publication には次のようなものがある。

- NIST SP 800-100『 情報セキュリティハンドブック ― マネジメント層向けガイド(Information Security Handbook: A Guide for Managers)』

- NIST SP 800-65『IT セキュリティの資金計画および投資管理プロセスへの統合(Integrating IT Security into the Capital Planning and Investment Control Process)』

これらの測定指標は、セキュリティ管理策の継続的監視の優先順位付けを支援するために利用できる。(セキュリティ管理策の継続的監視に関しては、NIST SP 800-37『連邦政府情報システムに対するセキュリティ承認と運用認可ガイド (Guide for the Security Certification and Accreditation of Federal Information Systems)』を参照のこと。)

1.6 本文書の構成

以降の章では、次の内容について説明する。

●第 2 章「役割と責務」

情報セキュリティプログラムの成功と、情報セキュリティ測定プログラムの確立に直接関わる職員の役割と責務について説明する。

●第 3 章「セキュリティ測定指標の背景」

情報セキュリティ測定指標の背景と定義に関する手引き、実施のメリット、各種情報セキュリティ測定指標、情報セキュリティ測定プログラムの成功に直接影響する要因について説明する。

●第 4 章「法律および戦略上の動因(Driver)」

情報セキュリティと戦略計画を、関連する法律と手引きをもとに結び付ける。

●第 5 章「測定指標策定プロセス」

情報セキュリティ測定指標を策定するためのアプローチと手順を説明する。

●第 6 章「セキュリティ測定の実施」

情報セキュリティ測定プログラムの実施に影響を与える要因について説明する。.

本書には、4 つの付録が含まれている。付録 A「測定指標の候補」には、組織がそのまま使用したり、組織特有の要件に合うように修正できるような、情報セキュリティ測定指標の実例を記載している。付録 B には、本書で使用する略語の一覧を記載している。付録 C には、参考文献の一覧を記載している。付録 D には、FIPS 200『連邦政府の情報および情報システムに対する最低限のセキュリティ要求事項(Minimum Security Requirements for Federal Information and Information Systems)』から抜粋した最低限のセキュリティ要求事項を記載している。

2. 役割と責務

この章では、情報セキュリティ測定指標の策定と実装における主な役割と責務について説明する。情報セキュリティに関しては、組織内のすべての者が責任を負うべきではあるが、セキュリティ意識を組織全体に渡って浸透させることに関しては、セクション2.1～2.6に記載の者が重要な役割を担う。

2.1 部局長（Agency Head）

部局長は、情報セキュリティ測定に関連して、以下の責務を履行する。

- ●情報セキュリティ測定指標が、政府機関の任務を果たすことを目的として、組織の戦略計画および運用計画策定プロセスを支援するために使用されることを確実にする。
- ●情報セキュリティ測定指標が、(最高情報責任者(CIO)による)政府機関のセキュリティプログラムの有効性に関する年次報告に組み込まれることを確実にする。
- ●情報セキュリティ測定指標の策定と実施へのサポートを示し、当該政府機関に対して正式なサポートを申し出る。
- ●情報セキュリティ測定活動を成功させるために十分な資金と人的資源を割り当てる。
- ●政府機関全体のセキュリティパフォーマンスの改善を推進するための最も重要な要素として、情報セキュリティ測定を積極的に普及させる。
- ●正式に測定指標収集を開始するためのポリシーを承認する。

2.2 最高情報責任者（CIO）[2]

最高情報責任者(CIO)は、情報セキュリティ測定に関連して、以下の責務を履行する。

- ●情報セキュリティ測定指標を使用して、適用されるセキュリティ要件が満たされているかどうかを監視する。
- ●情報セキュリティ測定指標を使用して、政府機関のセキュリティプログラムの有効性を評価し、部局長に対して年次報告を行う。
- ●正式な指揮を通じて、マネジメント層が情報セキュリティ測定指標の策定と実施に積極的であることを表明する。
- ●セキュリティプログラムの全体的な健全性を監視し、該当する規定を遵守するためには、情報セキュリティ測定指標が重要であるということを正式に伝える。
- ●情報セキュリティ測定プログラムの策定と実施が確実に行われるようにする。
- ●情報セキュリティ測定プログラムに十分な資金と人的資源を割り当てる。

2 政府機関が正式な最高情報責任者(CIO)を任命していない場合は、これに相当する地位にいる者が CIO の業務を行うべきである。このことは、FISMA によって義務付けられている。

●情報セキュリティ測定指標を定期的にレビューし、情報セキュリティ測定データを活用して、ポリシーのサポート、リソースの割り当て、予算の裁定、セキュリティプログラムの状況および情報システムに対する運用上のリスクの評価を行う。

●測定指標の分析を通じて見つかった問題に対処し、セキュリティ手順を見直したり、スタッフに対して追加のセキュリティ訓練を実施するなどの是正対策をとるためのプロセスを確実に実施する。

●測定指標を公式に策定、導入、実施するためのポリシー、手順および手引きを発行する。

2.3 上級情報セキュリティ責任者

政府機関によっては、上級情報セキュリティ責任者(SAISO)のことを、最高情報セキュリティ責任者(CISO)と呼ぶこともある。本書の中では、SAISO という用語を SAISO と CISO の両方の意味で使用している。SAISO は、情報セキュリティ測定に関連して、以下の責務を履行する。

●セキュリティポリシー、手順および慣行上のあらゆる欠陥を是正するための活動を計画、実施、評価、文書化するためのプロセスに、情報セキュリティ測定を組み込む。

●情報セキュリティ測定プログラムの策定と実施に十分な資金と人的資源を割り当てる。

●情報セキュリティ測定指標に関連する内部の手引きやポリシーの策定を指揮する。

●情報セキュリティ測定指標を使用して、(最高情報責任者(CIO)による)政府機関のセキュリティプログラムの効果に関する年次報告(是正措置の進展状況を含む)を支援する。

●情報セキュリティ測定指標を策定し、実施する。

●情報セキュリティ測定指標を策定、収集、分析、報告する際に、機関全体で標準的な手順が使われるようにする。

●情報セキュリティ測定指標を使用して、ポリシーの作成、リソースの割り当て、予算の裁定などを行う。

2.4 プログラム管理者／システムオーナー

プログラム管理者とシステムオーナーは、情報および情報システムの機密性、完全性、可用性を確保するために、適切なセキュリティ管理策が実施されることを確実にする責務がある。プログラム管理者とシステムオーナーは、情報セキュリティ測定に関連して、以下の責務を履行する。

●情報セキュリティ測定プログラムの策定と実施に参加し、データ収集の実現性に関して意見を述べ、データソースとその格納場所を明確にする。

●情報セキュリティ測定指標の策定、収集、分析、報告方法と、測定指標がセキュリティポリシー、要件、リソース割り当て、予算裁定にどのように影響するかについて担当者を教育する。

●測定指標データが一貫してかつ正確に収集され、データの分析と報告を行う担当者に提供されるようにする。

●必要に応じて、担当者の十分な参加と協力を指示する。

●情報セキュリティ測定データを定期的にレビューし、ポリシーの作成、リソースの割り当て、予算の裁定において活用する。

●セキュリティパフォーマンスの測定を通じて明確化された是正措置の実施をサポートする。

2.5 システムセキュリティ責任者

システムセキュリティ責任者(ISSO)は、情報セキュリティ測定に関連して、以下の責務を履行する。

●情報セキュリティ測定プログラムの策定と実施に参加し、データ収集の実現性に関して意見を述べ、データソースとその格納場所を明確にする。

●データを収集する、あるいは、データの収集、分析、報告を行う担当者に測定データを提供する。

2.6 その他の関連する役割

情報セキュリティ測定は、インシデント対応、IT オペレーション、プライバシー、エンタープライズアーキテクチャ、人的資源、物理的セキュリティなど、組織にかかわるさまざまな構成要素および関係者からの入力を要することがある。セクション 5.1 には、利害関係者の追加リストを記載している。

3. 情報セキュリティ測定の背景

この章では、情報セキュリティ測定指標とは何か、なぜセキュリティのパフォーマンスを測定すべきなのかといった、基本的な情報を説明する。さらに、評価に使用できる測定指標の種類を定義し、情報セキュリティ測定プログラムを成功に導くための重要な側面について説明するとともに、測定指標を管理、報告、意思決定において利用する方法を明確にする。

3.1 定義

情報セキュリティ測定指標は、パフォーマンスに関連する適切なデータの収集、分析、報告を通じて、意思決定を促進し、パフォーマンスや説明責任を改善することを目的として設計されたツールである。パフォーマンスを測定する目的は、評価された活動の状態を監視し、測定結果に基づいて是正措置を講じることによってそれらの活動を改善することにある。

情報セキュリティ測定指標は、組織内のさまざまなレベルで収集することができる。詳細な測定指標はシステムレベルで収集され、組織の規模や複雑度に応じて集約されて徐々に上位レベルへと渡されていくことになる。より詳細な項目や集約された項目に対してメトリクス（metrics）や測定指標（measures）といった用語を使用することもできるが、本書ではデータ収集、分析および報告の結果を示す用語として、測定指標（measures）を標準で使用している。また、データ収集、分析および報告プロセスには、測定（measurement）を使用している。（訳者注：metrics と measures は、同様の意味で使われており、NIST SP800-55 では metrics を、NIST SP800-55 rev.1 では measures を使っている。NIST SP800-55 rev.1 の訳では、measures を測定指標、measurement を測定と訳している。）

情報セキュリティ測定指標は、セキュリティのパフォーマンス目標と目的をもとに策定される。情報セキュリティのパフォーマンス目標は、「すべての職員が適切な情報セキュリティ意識向上トレーニングを受講する」といった、情報プログラムまたはセキュリティプログラムを実施することにより得られる望ましい結果を明言する。セキュリティパフォーマンスの目標を設定すると、セキュリティポリシーにより定義された行動および、組織全体でセキュリティ管理策が一貫して実施されるようになるための手続きが明確になるため、目標の達成が可能となる。上記の目標例に対応するセキュリティパフォーマンスの目的の例としては、「すべての新人職員は新人研修を受講する」、「社員研修に行動規範の概要を組み入れる」、「社員研修には組織のセキュリティポリシーと手続きの概要や参考資料を組み入れる」などがあげられる。

情報セキュリティ測定指標は、セキュリティ管理策の実施度合いや、セキュリティ管理策の効率と有効性を定量化し、セキュリティ活動の妥当性を分析し、可能な是正措置を明確にすることで、目標や目的を達成したかどうかを監視する。測定指標を策定する過程で、政府のガイドライン、法律、規制、およびエンタープライズレベルのガイダンスに端を発する目標や目的が明確になり、優先順位が付けられる。これにより、セキュリティパフォーマンスの評価可能な側面と組織運営上の優先順位が一致することが保証される。

情報セキュリティ測定指標は、結果の比較、分析のための数式の適用、同じ参照点を使った変化の追跡などを行うための定量化可能な情報が得られるものでなければならない。割合や平均が最も一般的であるが、評価対象の活動によっては絶対数が適している場合もある。

測定指標を計算するのに必要なデータは容易に取得できることが必要であり、対象となる手順は測定可能である必要がある。測定においては、繰り返し可能で変化しない手順のみを検討すべきである。ただし、手順が繰り返し可能で変化しないものであっても、その手順とパフォーマンスが文書化されていないと、測定可能なデータの収集が難しい場合もある。本来他の目的に必要なリソースまで占有することにより、測定の目的よりも測定による負担が大きくなってしまうことがないよう、測定指標は容易に取得できるデータを使用しなければならない。測定のためのデータを提供できる情報セキュリティ活動には、リスクアセスメント、ペネトレーションテスト、セキュリティアセスメント、および継続的監視などがある。その他のアセスメント活動(セキュリティトレーニングおよび意識向上プログラムの有効性のアセスメントなど)の結果も、定量化し、測定の元データとして使用することができる。

測定指標をパフォーマンスの追跡やリソースの割り当てを目的として活用するためには、測定指標からパフォーマンスの経時的な傾向が得られ、問題領域に適用することのできる是正措置が明確になる必要がある。マネジメント層は、測定指標の傾向をレビューする、是正措置を明確にして優先順位を付ける、リスク軽減要因や利用できるリソースに基づいてこれらの是正措置の適用を指示するといった方法を用いてパフォーマンスをレビューするための手段として測定指標を使用するべきである。第 5 章で述べる測定指標策定手順に従えば、パフォーマンスが低いことの原因や、適切な是正措置を明らかにするという目的に沿って測定指標を作成することができる。

3.2 測定指標を使うことのメリット

情報セキュリティ測定プログラムには組織や財政面でも数多くのメリットがある。まず、情報セキュリティ測定指標を策定することにより、セキュリティパフォーマンスに対する説明責任を改善し、セキュリティ活動の有効性を向上させ、法律、規定、規制への準拠を示し、リソース割り当を決定する際に必要となる定量化されたインプットを提供することが可能である。

説明責任の改善 情報セキュリティ測定指標は、セキュリティ管理策のうち、実施されていないもの、実施方法が間違っているもの、あるいは有効でないものを特定するために役立つ。これにより組織は、情報セキュリティに対する説明責任を改善することができる。また、データ収集と解析プロセスにより、組織の特定構成要素または特定情報システムに適用されているセキュリティ管理策の実施に責任を持つ担当者を、容易に特定できるようになる。

情報セキュリティの有効性の向上 情報セキュリティ測定プログラムを使用することで、組織は、情報システムのセキュリティ改善の度合いを定量化し、政府機関の戦略目標と目的がどの程度達成できたかを示すことができる。また、情報セキュリティ活動結果とイベント結果(インシデントデータ、サイバー攻撃による収益の損失など)を対応するセキュリティ管理策とセキュリティ投資に関連づけることで、現在実施されているセキュリティ手順や、手続き、管理策の有効性の判断を支援する。

法律への準拠を明示 組織は、情報セキュリティ測定プログラムを実施、維持することによって、適用される法律、規則、規定に準拠していることを明示することができる。FISMA の年次報告は、過去および現在の会計年度に対するパフォーマンス報告を義務付けているが、それを満たすうえでも情報セキュリティ測定指標が役に立つ。さらに、情報セキュリティ測定指標を GAO(会計検査院)や IG(監察官)による監査に対するデータとしても活用することができる。情報セキュリティ測定プログラムを実施することは、事前のセキュリティ対策に対して政府機関が前向きであることを示すことにもなる。さらに、GAO や IG の監査とその後の更新においては、GAO や IG から定期的にデータが要求されるが、このデータを収集する手間を大幅に削減することができるだろう。

リソース割り当を決定する際に必要となる定量化されたインプットの提供　財政上の制約や市場の状況により、政府や企業は限られた予算で活動せざるを得ない。そのような状況では、情報セキュリティインフラに対する広範囲な投資の妥当性を示すことは困難である。情報セキュリティへの投資の割り当ては、包括的なリスク管理プログラムに沿って行うべきである。情報セキュリティ測定指標を使用することで、組織は、定量化されたデータをリスク管理プロセスに提供することができ、リスクにもとづく意思決定を行うことができる。また、過去および現在のセキュリティ投資の成否を評価することができ、将来の投資に向けたリソース割り当ての根拠となる定量化されたデータを得ることができる。プログラムマネージャーやシステムオーナーは、測定指標の分析結果を用いて問題を切り離し、収集したデータを使って投資要求の妥当性を示すことで、投資対象をさらなる改善が必要な領域に絞ることができる。測定指標を使ってセキュリティ投資の対象を定めれば、手持ちのリソースから最高の価値を引き出すことが可能になるだろう。

3.3　測定指標のタイプ

組織のセキュリティプログラムの成熟度により、首尾よく収集できる測定指標のタイプが決まる。プログラムの成熟度は、手順や手続きが定められているか、また、慣習化しているか、といった要素によって決まる。セキュリティプログラムが発達するに従い、ポリシーはより詳細になり、より詳しく文書化されるようになる。また、そこで使われる手順はより標準化され慣習化したものになり、パフォーマンスの評価で使用するデータがより多く得られるようになる。

図 3-1 に、この流れを示す。図 3-1 では、セキュリティプログラムの測定に関する考慮事項を図解している。図 3-1 が示すように、成熟していないセキュリティプログラムを使って効果的な測定を行うためには、事前にプログラムの目標と目的を策定する必要がある。より成熟したプログラムは、実施測定指標を使用してパフォーマンスを測定し、最も成熟したプログラムは、効率／有効性測定指標およびビジネス影響測定指標を使用して、セキュリティ手順と手続きの効果を特定する。

セキュリティプログラムの目標と目的を定めるうえで、上級マネジメント層のサポートは必要不可欠である。これらの目標と目的は、プログラムの初期段階でセキュリティポリシーと手順によって明示されるか、あるいは他のさまざまなソースによって明確になると考えられる。（目標と目的の詳細は、Sections 4.1 と 5.2 を参照のこと）プログラムが実施され成熟するにつれて、セキュリティポリシーが文書化され、セキュリティ手順が決まってくる。有用な情報セキュリティ測定指標の策定には、文書化された手順と、セキュリティ管理策の実施に関するなんらかのデータが存在することが求められる。

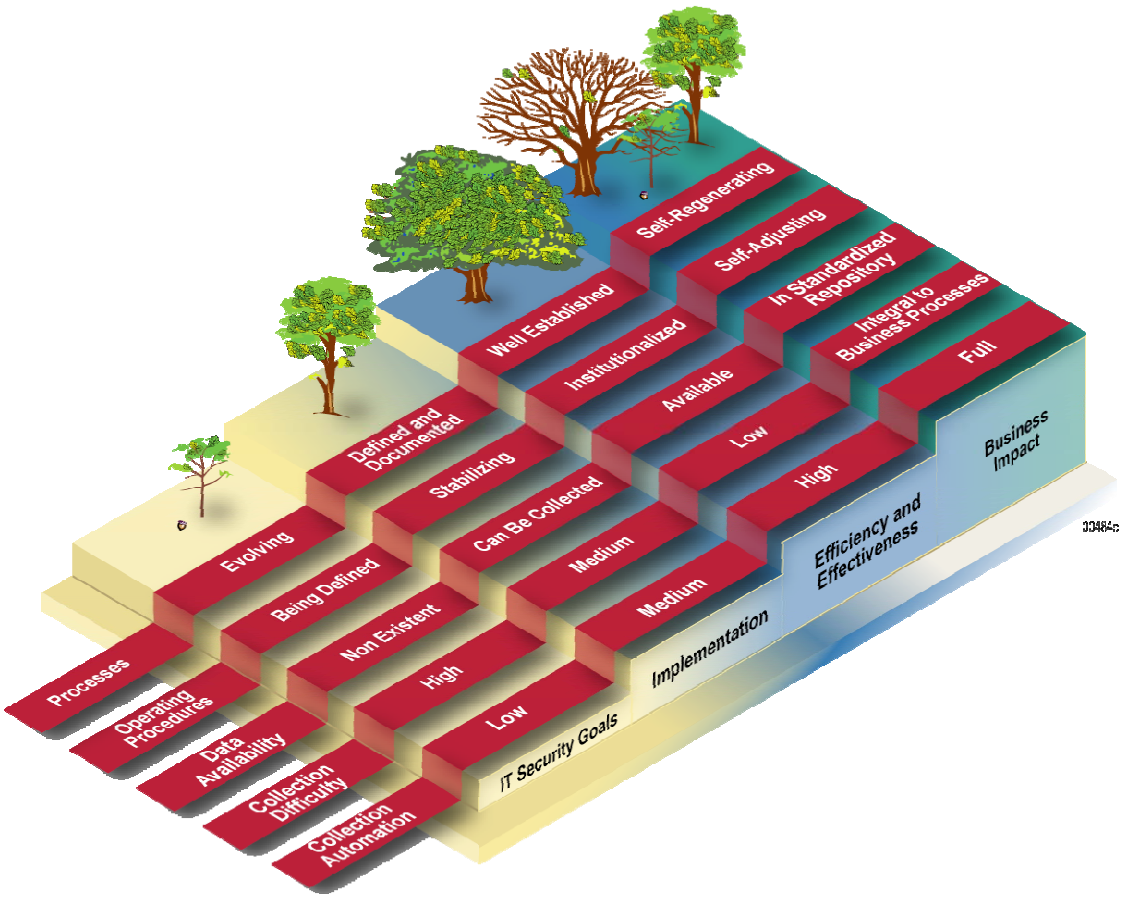

図 3-1 情報セキュリティプログラムの成熟度と測定の種類

成熟したプログラムでは、通常、複数の追跡機構を使ってパフォーマンスのさまざまな面を文書化し定量化するようになっている。より多くのデータが利用できるようになるに従い、測定の難しさが減少し、データ収集をより自動化できるようになる。データ収集の自動化は、人間から集めるデータと比較して、自動化されたデータソースから収集できるデータがどれだけあるかにかかっている。手動でのデータ収集では、アンケートを作成し、組織のスタッフに対してインタビューや意識調査を行うことになる。セキュリティプログラムが成熟するに従い、自己診断ツール、セキュリティ承認と運用認可(C&A)データベース、事故報告対応データベースなどの半自動化あるいは自動化されたデータソースから、より多くの有用なデータが入手できるようになる。すべてのデータが、人間の関与や介在がない自動化されたデータソースから収集できるようになると、測定データの収集は完全に自動化されたとみなされる。

どのようなタイプの測定指標(実施、効率／有効性、影響)が実際に収集可能でパフォーマンスの改善に役立つかは、セキュリティ管理策の実施の度合いに依存する。異なるタイプの測定指標を同時に使用することは可能だが、セキュリティプログラムの実施の度合いが向上するにつれ、情報セキュリティ測定指標の主な焦点も変化する。セキュリティプログラムの目標と戦略計画が文書化され実施されると、実施の結果を確実に収集できる能力も向上する。組織のセキュリティプログラムが進化して、パフォーマンスデータがより容易に入手できるようになると、測定指標の焦点は、プログラムの効率／有効性と、セキュリティ管理策を実施したことによる運用面での結果に移行する。そして、セキュリティが組織

の業務手順に統合されると、その手順は繰り返し利用可能となり、データ収集は完全に自動化され、セキュリティ関連の行動やイベントがミッションやビジネスに与える影響を、データ相関分析により特定できるようになる。付録 A に、実施測定指標、効率／有効性測定指標および影響測定指標の例を示す。

3.3.1 実施測定指標

実施測定指標は、セキュリティプログラム、特定のセキュリティ管理策、および対応するポリシーと手順の実施状況を示すのに用いられる。セキュリティプログラムに関わる実施測定指標の例としては、承認されたセキュリティ計画が組み込まれたシステムの割合や、要求通りのパスワードポリシーが組み込まれたシステムの割合などがある。これらの測定指標の結果は、始めは 100 パーセント未満になるかもしれない。しかし、セキュリティプログラムおよび対応するポリシーと手順が成熟するにつれて、結果は 100 パーセントに達するべきであり、その状態が維持されるべきである。この段階で組織は、測定指標の焦点を、実施測定指標から効率／有効性測定指標と影響測定指標に置き換えるべきである。

実施測定指標は、システムレベルでの検証も可能である(たとえば、システム内で標準構成を使用しているサーバーの割合など)。この測定指標の結果は、始めは、おそらく 100 パーセント未満になるであろう。実施測定指標の結果が 100 パーセントに達し、その状態が維持されるようになると、この測定指標の対象となっているセキュリティ管理策が情報システムによって十分なレベルで実施されているとみなされ、改善が求められる管理策に測定指標の焦点が置かれるようになる。大部分の実施測定指標の結果が 100 パーセントに達し、その状態が維持されるようになった段階で、組織は、測定指標の焦点を、実施測定指標から効率／有効性測定指標と影響測定指標に置き換えるべきである。ただし、実施測定指標は改善が必要なセキュリティ管理策を特定するうえで有用であるため、実施測定指標をまったく実施しないという選択は避けるべきである。測定プログラムの焦点とリソースは、組織の成長とともに、実施測定指標から効率／有効性測定指標と影響測定指標に移行すべきである。

実施測定指標は、以下のドキュメントまたは手段により簡単に得られるデータを必要とする － セキュリティアセスメントレポート、年 1 回および四半期ごとに FISMA に提出するレポート、行動計画とマイルストーン（POA&M）、セキュリティ活動を文書化、追跡するために一般的に使われるそのほかの手段。

3.3.2 効率／有効性測定指標

効率／有効性測定指標は、プログラムレベルのプロセスと、システムレベルのセキュリティ管理策が、正しく導入され、意図したとおりに運用され、望まれる結果を産出しているか監視するために使用できる。効率／有効性測定指標は、アセスメントの証拠と結果に焦点をあてたものである。この測定指標は、セキュリティ管理策の実施の度合い、および組織のセキュリティ状況への影響を定量化した、複数のデータポイントを要することもある。たとえば、エンタープライズオペレーティングシステムの脆弱性のうち、パッチがあてられたものの割合、または、脆弱性が軽減されたものの割合は、実施と有効性に関する測定指標である。このような測定指標は、脆弱性がパッチなどの手段によって軽減されたかどうかを示すため、NIST SP 800-53 のセキュリティ管理策 SI-2(Flaw Remediation:欠陥の修正)の実施の評価に利用できる。また、この測定指標が管理策 SI-5(Security Alerts and Advisories:セキュリティ警報と勧告）の有効性を示すこともある。たとえば、この測定指標を使用して組織の管理策 SI-5 の実施状況を評価した結果が目標を下回る場合、組織において警告を受ける能力と、それらの警告をもとに脆弱性を首尾よく軽減するための能力が十分に備わっていないことが判明する。

効率／有効性測定指標は、セキュリティ管理策実施結果の 2 つの側面、すなわち、結果自体のロバストネス(「***有効性***」といわれる)と、結果の適時性(「***効率***」といわれる)を扱う。たとえば、アクセスコントロールの設定が誤っていたために発生したインシデントの割合を特定するための効率／***有効性***測定指標は、セキュリティ管理策 IR-5(Incident Monitoring:インシデントの監視)、AU-6(Audit Monitoring, Analysis, and Reporting: 監査記録の監視、分析および報告)、および CM-4(Monitoring Configuration Changes: 構成変更の監視)の実施と***有効性***に関する情報に依存する。

また、スケジュールどおりにメンテナンスを受けるシステムコンポーネントの割合を特定するための***効率***／有効性測定指標は、セキュリティ管理策 MA-2 (Periodic Maintenance: 定期的な保守)および SA-3 (Life Cycle Support: ライフサイクルサポート)の***効率***に関する情報に依存する。

効率／有効性測定指標は、前回のポリシーと調達の決定に関する重要な情報を、セキュリティの意思決定者に提供する。また、このような測定指標を使用することで、セキュリティプログラムのパフォーマンスを向上させるために何をすべきかが見えてくる。さらに、効率／有効性測定指標は、セキュリティ管理策の有効性の特定を支援するため、継続的監視のためのデータソースとして利用できる。効率／有効性測定指標の結果は、選択されたセキュリティ管理策が正しく機能しているかどうか、是正措置の優先順位付けを助成しているかどうかを確認するためにも利用できる。

効率／有効性測定指標では、セキュリティプログラム活動から得られるデータと、自動化された監視・評価ツールから得られるデータを、セキュリティ管理策の実施に直結するような形で組み合わせることが求められることもある。

3.3.3 影響測定指標

影響測定指標は、情報セキュリティが組織のミッションにもたらす影響を、明確にするために用いられる。組織のミッションは組織ごとに異なるため、影響測定指標は、本質的に組織に特化したものとなる。 影響測定指標は、組織のミッションに応じて、以下のものを定量化するために利用できる。

- ●セキュリティプログラムの実施またはセキュリティイベントへの対処により、コストをどれだけ削減できるか
- ●セキュリティプログラムを実施することにより、国民の信頼をどの程度得られるか
- ●情報セキュリティが組織ミッションにもたらす、そのほかの影響

影響測定指標は、セキュリティ管理策の実施に関する評価結果を、リソースに関するさまざまな情報と組み合わせる。影響測定指標は、情報セキュリティが組織にとっていかに重要であるかを直に示すものであり、また、組織の幹部が求める測定指標でもある。たとえば、政府機関の情報システム関連予算のうち、何割を情報セキュリティに割り当てるかは、NIST SP 800-53 のセキュリティ管理策 SA-2(Allocation of Resources:リソースの割り当て)と SA-4(Acquisitions:調達)の実施状況、有効性および実施結果に関する情報に依存する。予算関連の影響測定指標のより一般的な例として、提示資料 300(OMB の予算申請書式)を使って OMB に報告される、セキュリティ投資報告の数がある。この測定指標は、セキュリティ管理策の影響を調べるためではなく、セキュリティ投資のポートフォリオと予算プロセスの関係を評価するために使用される。

影響測定指標では、組織全体にわたるさまざまな情報資源から得た情報を、セキュリティ活動とイベントに直接結びつける形で追跡することが求められる。

3.4 測定に関する留意事項

情報セキュリティパフォーマンス測定に着手している組織は、プログラムを成功に導くためのいくつかの考慮事項を知っておくべきである。これらの考慮事項には、組織の構造と業務手順に加えて、必要な予算、人員、時間に対する理解が含まれる。

3.4.1 組織上の留意事項

情報セキュリティ測定指標の策定とプログラムの実施に際しては、適切な関係者が参加しなければならない。セキュリティが主な任務ではなくても、定期的にセキュリティとやり取りする部門(教育部門、リソース管理部門、法務部門)も、このプロセスに参加する必要がある。(関係者の詳細は、セクション 5.1 を参照のこと。) パフォーマンスの評価一般に対して責任を持つ部門があるなら、情報セキュリティ測定プログラムの策定と実施に際し、その組織とすりあわせを行うべきである。組織全体のデータ呼び出しと操作に関する承認プロセスがすでにある場合には、情報セキュリティ測定プログラムの策定と実施に当たっては、そのプロセスに準拠すべきである。

3.4.2 管理のしやすさ

どんな情報セキュリティ測定プログラムであっても、組織にとって扱いやすいものでなければならない。セキュリティ活動の結果には、定量化してパフォーマンス評価に使用できるものが多数あるが、リソースは限られており、リソースの大部分はパフォーマンスのギャップを埋める作業に当てるべきであることから、評価の必要性に優先順位を付けて、収集する測定指標の数を制限するべきである。各関係者が担当する測定指標の数は、最小限(通常 2～3)にとどめるべきである。こうすることで、収集された測定指標が意味のあるものとなり、影響と結果に関する所見がもたらされ、結果をもとにしてパフォーマンスのギャップを埋めるための作業時間が、関係者に与えられる。プログラムが成熟して目標レベルに到達したら、古い測定指標を段階的に廃止し、より新しい項目の達成度や有効性を評価するための新しい測定指標を採用するべきである。また、組織のミッションが再定義されたり、セキュリティポリシーやガイドラインに変更が生じた場合にも、新しい測定指標が必要となる。

3.4.3 データ管理上の留意事項

データの品質や妥当性を確実なものにするために、測定データの収集や報告に使用するデータ収集方法やデータリポジトリは、直接的に使用するかデータソースとして使用するかによらず、標準化されている必要がある。主要なデータソースが、組織のどこかの部門が報告した情報だけが保管されたインシデント報告のデータベースであったり、組織ごとに報告手順が一貫していなかったりした場合、データの妥当性が疑われる。標準化された報告手順の重要性は、いくら強調しても足りないほどである。情報セキュリティ測定プログラムへの入力となる可能性がある業務手順を策定し、実施しようとしているのであれば、データ収集と報告の方法を明確に規定して、有効なデータを容易に収集できるようにする必要がある。

セキュリティデータは大量に収集できるかもしれないが、評価プログラムのある時点では、すべてのデータが有用なわけではないことを理解する必要がある。データ収集、特に情報セキュリティ測定のためのデータ収集は、できるだけ業務の邪魔にならないようにするとともに、集めたデータを最大限に活

用して、手持ちのリソースをデータの収集ではなく問題の解決に当てることが必要である。測定プログラムを定着させるためには、十分な投資を行って、正しくプログラムを実装し、最大限の利益が得られるようにすることが必要である。測定プログラムがもたらす利益は、プログラムを維持するためのリソースへの投資費用を上回ると考えられる。

最後に、セキュリティデータリポジトリに含まれる情報は、運営上のデータおよび脆弱性データの重要なコレクションであることを覚えておこう。このデータは、取り扱いに注意を要するため、セキュリティデータリポジトリは適切に保護されるべきである。

3.4.4 測定データ収集の自動化

測定データ収集を自動化できれば、データ管理を効果的に行うことができる。また、データ収集と報告の標準化、および評価活動のビジネスプロセスへの統合による評価活動の慣行化を促進できる。さらに、人的エラーの機会を最小限にとどめることができ、より正確なデータが利用可能になる。データの可用性も、標準化されたデータ収集と報告により向上することがある。(たとえばコレクションが、集中データベース(centralized database)または類似のデータリポジトリに保持される場合など。)

パフォーマンス測定の自動化に加えて、組織は、そのような自動化によって他の自動化されたセキュリティタスクがどのように補足されるかを考慮すべきである。例えば、組織が使用する構成チェックリストが XML(Extensible Markup Language)フォーマットの場合、一般商用 (COTS: Commercial Off-The-Shelf)ツール、政府調達向け(GOTS: Government Off-The-Shelf)ツール、またはオープンソースツールを使用して、自動的にセキュリティ構成をチェックし、その結果と技術的コンプライアンス要求を照合することができる。これらのチェックリストは主に、FISMA などの規制に準拠するために使用できるが、特定の技術管理策の設定を NIST SP 800-53 に記載のセキュリティ管理策に対応づけるためにも使用できる。これにより、コンプライアンスの確認を、より効率的で一貫した方法で行うことができる。たとえば、チェックリストを使用してシステム上のパスワード強度設定を検証し、それらの設定が NIST SP800-53 が規定する要件を満たしているかどうかを報告することができる。自動化されたデータ収集により、政府機関のセキュリティパフォーマンス測定指標がダイナミックに更新され、情報セキュリティの目標が達成されているかどうかを確認し、是正措置や軽減活動が必要な箇所を特定できるようになる。

3.5 情報セキュリティ測定プログラムのスコープ

情報セキュリティ測定プログラムは、さまざまな環境やニーズに合わせて対象範囲を調整できる。たとえば、

- ●稼動中のシステムのシステムレベルのセキュリティパフォーマンスを定量化する
- ●情報システムおよびソフトウェア開発プロセスにおいて、情報セキュリティが情報システム開発ライフサイクル（SDLC）にどの程度統合されたかを定量化する
- ●企業全体のセキュリティパフォーマンスを定量化する

など。

情報セキュリティ測定指標は、組織の構成概念(部門、サイトなど)ごとに適用することができる。組織は、特定の関係者のニーズ、戦略目標と目的、運用環境、リスクの優先度、およびセキュリティプログラムの成熟度にもとづいて、情報セキュリティ測定プログラムのスコープを決定すべきである。

3.5.1 個々の情報システム

組織は、情報セキュリティ測定指標をシステムレベルで適用し、必要な(または望ましい)セキュリティ管理策の実施の有無、有効性/効率、または影響に関して定量化されたデータを得ることができる。システムオーナーは、測定指標を使用して、システムのセキュリティ状態を確認し、組織の要件を満たしていることを示し、改善が必要な領域を特定できる。情報セキュリティ測定指標は、セキュリティ承認と運用認可(C&A)活動(リスクアセスメント、システムセキュリティ計画、および継続的監視など)、FISMA報告活動、または資金計画を支援する。

3.5.2 システム開発ライフサイクル(SDLC)

情報セキュリティ測定指標は、対象のセキュリティ管理策の実施を監視するために、システム開発ライフサイクル全体を通して使用すべきである。システム開発ライフサイクルにおいて形式化された情報セキュリティ測定指標は、プロジェクトマネージャに対して、情報セキュリティがどの程度システム開発ライフサイクルに組み込まれていて、システムにどの程度の脆弱性が存在するかを把握するための、重要な情報を提供する。プロジェクト活動によっては、異なる測定指標が有効な場合もある。以下の表に、さまざまなプロジェクト活動の開発ライフサイクルにおいて利用できる測定指標の例を示す。

表 1 システム開発における測定指標[3]

システム開発ライフサイクルフェーズ	関連測定指標	目的	意義
調達／開発	• システムのセキュリティ状態に悪影響を及ぼす製品上の欠陥の割合	• 将来利用される可能性があるソフトウェア欠陥を特定する	• ライフサイクルプロセスの有効性と開発者向けセキュリティトレーニングの有効性を確認できる • 追加のセキュリティ管理策が必要かどうかを確認できる
調達／開発	• デザインにマップされるセキュリティ要件(実施されているセキュリティ管理策など)の割合	• セキュリティ要件が計画、実施されているかを確認する	• リリースの初期段階でセキュリティ要件が包含されているかどうかを確認できる • セキュリティ実施の複雑さを確認できる • 追加のセキュリティ管理策に関する短期ニーズと長期ニーズが明らかになる
調達／開発	• モジュールに対するエントリポイントの数(エントリポイントの数は、必要最低限に抑えるべきである)	• エントリポイントを少なくすることで、監視の量を減らす。	• 本来備わっている脆弱性の可能性と、エンタープライズリスクの増加の可能性が明らかになる

[3] これらの測定指標は、国土安全保障省のソフトウェア品質保証プログラム(Department of Homeland Security Software Assurance Program)との連携により、策定された。

システム開発ライフサイクル フェーズ	関連測定指標	目的	意義
調達／開発	• ソフトウェアの脆弱性として知られる欠陥（バッファオーバフローやクロスサイトスクリプトなど）が発見された数 • デザイン、コードおよび要件からの逸脱の数 • 欠陥の数とコード内でそれらの欠陥が見つかった箇所(コンポーネント間、ユニットシーム(unit seam)間、またはその他のインターフェース間に欠陥がある場合、リスクが高くなる) • 発見された脆弱性のうち、軽減された脆弱性の割合	• テストと実施に先立って、セキュリティ上の欠陥に対処する	• 開発とメンテナンスの手直しに掛かる費用を最小限に抑えることができる
調達／開発	• 各種セキュリティ活動のコスト/スケジュールの差異	• セキュリティ活動の計画と実施を監視する	• プロジェクトを成功させるためのコストとスケジュールに関するリスクが明らかになる • 未来プロジェクトの計画策定をより正確に行えるようになる
インプリメンテーション／アセスメント	• 脆弱性を含むモジュールの割合 • 満たされなかった管理策要件の割合	• 将来利用される可能性があるソフトウェア欠陥を特定する	• システム実施時に利用されるシステムリスクが明らかになる • 追加のセキュリティ管理策に関するニーズが明らかになる

これらの種類の測定指標を収集して分析することは、プロジェクトマネージャにとって以下の点で役に立つ。

●情報セキュリティに影響を及ぼす可能性のあるソフトウェア欠陥が、システム開発ライフサイクルの早い段階で、かつ、(欠陥の是正による)費用対効果が最も高くなるようなタイミングで特定されているかを確認できる。

●ソフトウェアの潜在的脆弱性を特定、除去し、よりセキュアな設計実践を確立できる。

●是正措置(訓練の実施、分かりにくい手順の改定など)を必要とする傾向を特定して調査することができる。

●必要なセキュリティ管理策がシステムに正しく導入されるかを確認できる。

●システム開発ライフサイクル全体を通してセキュリティリスクの傾向を追跡できる。

システム開発ライフサイクルにおいて適切な情報セキュリティ測定指標を収集、分析、報告することにより、情報セキュリティをより確実にシステム開発努力に統合することができる。これにより、システムセキュリティ要件を後で追加するのではなく、現段階で組み入れることができる。

3.5.3 エンタープライズレベルの測定プログラム

組織は、情報セキュリティ測定指標をエンタープライズ全体に適用し、セキュリティ管理策の実施状況、有効性／効率、およびセキュリティ活動への影響を監視できる。エンタープライズレベル測定指標は、複数のシステムレベル測定指標の集合によって構成されることもあれば、企業全体を対象に策定することもできる。

効果的なエンタープライズレベル測定を実現するには、測定が依存する手順が一貫していること、繰り返し利用可能なこと、企業全体にわたって利用可能であることが保証されるよう、組織がある程度熟したレベルで事業を運営していることが求められる。

4. 法律および戦略上の動因(Driver)

この章では、政府機関の総合パフォーマンス測定報告書と、セキュリティパフォーマンス測定報告書の関係を説明し、これらの2つの活動をリンクするためのガイドラインを示す。これらの2つの活動を正しくリンクすることによって、政府機関は、自身のミッション、目標および目的を達成できるようになる。セクション 4.1 と 4.2 では、GPRA(Government Performance Results Act)、FISMA、連邦エンタープライズアーキテクチャ(Federal Enterprise Architecture)を、パフォーマンス測定の観点から概説し、対応するパフォーマンス管理要件を記述する。セクション 4.3 では、企業戦略計画策定と情報セキュリティの関係について論じる。

4.1 法律上の留意事項

執行規則に加えて GPRA や FISMA のような法律は、政府機関によるパフォーマンスの管理、定量化、報告を強く促す要因となっている。これらの活動の目的は、米国政府の業務の合理化を促進し、サービスの向上を図り、これらのサービスの価値を市民に示すことにある。政府機関は、戦略的に方策をたてて、それらの方策および対応するパフォーマンス測定指標を市民が利用できるようにしなければならない。行政機関も、組織に対してパフォーマンス測定指標の収集と報告を義務付ける方策を策定すべきである。

4.1.1 GPRA (Government Performance Results Act: 政府業績評価法)

GPRA は、プログラム目標を明確にし、プログラムパフォーマンスに関する情報を提供することで、プログラム有効性と効率の改善を図る。プログラムの改善を体系化して促進するために、GPRA は、政府機関に対して、多年にわたる戦略計画を作成し、それらの計画に対するパフォーマンスを毎年報告するよう義務づけている。

以下に、GPRA の目的を示す。

- ●系統的な手段によってプログラム目標達成に関する責任を政府機関に負わせることで、連邦政府の能力に対するアメリカ国民の信頼を向上させる。
- ●具体的には、プログラム目標を設定し、これらの目標に対する実際のパフォーマンスを測定し、進展状況を公表するための一連の試験計画を通じて、プログラムパフォーマンスを改善する。
- ●結果、サービス品質、およびユーザ満足度に政府機関の目を向けさせることによって、連邦政府プログラムの有効性と公に対する説明責任を向上させる。
- ●連邦政府の管理者に対して、プログラム目的を達成するための計画作成を促し、プログラム結果とサービス品質に関する情報を提供することによって、(管理者による)サービスの向上を支援する。
- ●連邦議会に対して、法律上の目的達成に関する客観的な情報を提供し、連邦政府プログラムと出費の相対的有効性と効率を報告することによって、議会の意思決定能力を向上させる。
- ●連邦政府の内部管理を改善する。[4]

[4] Public Law 103-62、1993 年施行の政府業績成果法(Government Performance and Results Act)。

GPRA は、政府機関に対して、戦略計画とパフォーマンス計画を作成することを義務付けている。作成した戦略計画とパフォーマンス測定報告書は、毎年提出することになっている。GPRA は、この計画作成を、「プログラムを通じて何が達成されるか、また、その成果がプログラムの目的をどの程度満たすものであるか」といった結果を管理するためのものであるとし、政府機関の全体的な資金計画および投資管理(CPIC)プロセスの一環としてとらえている。[5]

政府機関は、戦略計画とパフォーマンス計画作成の一環として、以下に示す事項を実施すべきである。

- ●長期および年間の目標と目的を明確にする。
- ●適度のパフォーマンス目標を立てる。
- ●目標と目的に対するパフォーマンスを四半期ごとに OMB に報告する。

このパフォーマンス測定報告書は、政府機関目標と目的、およびパフォーマンス上の目標に対するパフォーマンスを追跡する手段を提供するものであり、GPRA を直接支援する。政府機関は、情報セキュリティパフォーマンス測定指標と自身のセキュリティ目標と目的を照らし合わせることによって、情報セキュリティが組織のミッションにもたらす影響を示すことができる。

GPRA は、OMB Circular A-11,「予算の準備、提出、執行(Preparation, Submission, and Execution of the Budget)」のパート 6 によって実施される。

4.1.2 FISMA

FISMA は、連邦政府政府機関に対して、自身の情報システムが処理、伝送、保存する情報の機密度に応じて情報を適切に保護するための、包括的な情報セキュリティプログラムを実施することによって、自身のリソースを保護することを義務付けている。FISMA はまた、政府機関が、情報セキュリティプログラムを実施、管理するうえでのパフォーマンスを評価、報告することを義務付けている。

以下に FISMA の目的を示す。

- ●連邦政府の業務と資産をサポートする情報資源に対するセキュリティ管理策が、有効であることを確実にするための、包括的なフレームワークを提供する。
- ●連邦政府の現行のコンピュータ環境の、高度にネットワーク化された性質を認識し、関連するセキュリティリスクを組織全体で効果的に管理、監視できるようにする。(これには、一般国民、国家安全保障に関わる者、および法執行コミュニティ間における情報セキュリティ活動の調整が含まれる。)
- ●連邦政府情報と情報システムを保護するために最低限必要なセキュリティ管理策を開発、維持できるようにする。
- ●連邦政府機関の情報セキュリティプログラムに対する監視を強化するためのメカニズムを提供する。

[5] OMB Circular A-11、2005 施行の「予算の準備、提出、執行(Preparation, Submission, and Execution of the Budget)」のセクション 15.5.

●商用に開発された情報セキュリティ製品は、民間部門が設計、構築、運営する情報インフラであり、かつ国防および経済安全保障にとって重要な情報インフラを保護するための、先進的でダイナミック、かつ堅牢で効果的なセキュリティソリューションを提供することを認識させる。

●ハードウェア／ソフトウェア情報セキュリティの技術的なソリューションは、個々の政府機関が、商用に開発された製品から選択すべきでることを認識させる。[6]

FISMA はまた、NIST に対して、連邦政府の情報システムに関する規準とガイドラインを策定し公布することを義務づけている。

FISMA は、政府機関に対して、自身の情報システムへのリスクを特定、アセスメントして、適切なセキュリティ管理策を定義、実施することによって情報資源を保護することを義務づけている。また、政府機関が自身のセキュリティプログラムの状況を四半期ごとに、および毎年報告することを義務づけている。慣習化された情報セキュリティパフォーマンス測定プログラムを使用することで、政府機関は、関連する FISMA パフォーマンス指標を収集し、報告できる。たとえば、保有するすべての情報システムのうち、承認および運用認可が与えられたシステムの割合や、すべての職員のうち、必須のセキュリティトレーニングを受けた者の割合、および他の FISMA 報告要件への準拠などを、迅速に調べることが可能となる。また、成熟した情報セキュリティ測定プログラムを使用することで、政府機関は、セキュリティデータの収集、分析、定量化、および報告に対する根拠を提供し、内部的または外部的に要求される新規のセキュリティパフォーマンス測定報告要件を満たすことができる。

OMB は、FISMA の年次報告および四半期ごとの報告の、手順および要素に関するガイドラインを毎年発行している。

4.2 連邦政府のエンタープライズアーキテクチャ

情報セキュリティパフォーマンス測定に関する法律上の要求事項に加えて、行政機関は、連邦政府機関の有効性を監視、改善するための方策を、定期的に実施する。情報セキュリティ測定指標に依存する行政機関の方策として、FEA(連邦政府のエンタープライズアーキテクチャ)がある。FEA の参照モデルの一例としては、業績測定参照モデルがある。業績測定参照モデルは、主要 IT 投資のパフォーマンスと、それらの投資がプログラムパフォーマンスにもたらす便益を評価するための、標準フレームワークである。

組織は、データ収集の重複を減らし、情報セキュリティのエンタープライズアーキテクチャへの統合を容易にするために、情報セキュリティ測定指標の開発と実施を FEA 活動に結びつけることを考慮すべきである。

4.3 エンタープライズ戦略計画と情報セキュリティのつながり

連邦政府機関は、GPRA の要件に従って、戦略計画作成プロセスの一環として、長期の戦略目標を策定する。通常は、5～6 つの戦略目標が設定され、それぞれの目標に対して、いかにして目標を達成するかを示すいくつかのパフォーマンス目標が用意される。このプロセスの一環として、政府機関は、

[6] Public Law 107-347, 2002 施行の電子政府法(E-Government Act)のタイトル III

四半期ごとの、および年間の目標と目的を設定し、その周期ごとに目標と目的の達成度を定量化するためのパフォーマンス測定指標を策定する。

情報セキュリティパフォーマンス測定指標は、政府機関のセキュリティプログラムおよび関連するパフォーマンス測定の実施を監視、報告するための手段を提供する。このような活動は、FISMA にて義務付けられている。これらの測定指標を使用することで、政府機関は、自身のミッションを支援する情報資源を保護するための、セキュリティ管理策の有効性をアセスメントできるようになる。

最終的に全ての活動は、戦略計画作成活動の中で定義され毎年リアセスメントされる政府機関の全体的な目標と目的を支援するものでなければならない。情報セキュリティは、戦略計画作成プロセスにおいて、少なくても 1 つの目標または目的に明示的に結びつくようにすべきである。そうすることによって情報セキュリティが、政府機関のミッションを達成するうえでいかに重要であるかを示すことができる。このような結び付けは、政府機関の全体的なミッションを考慮したセキュリティ要件を明確に示す目標と目的を特定することによって、実現できる。政府機関の目標および目的の達成度は、適切な情報セキュリティパフォーマンス測定指標を実装することによって監視できる場合がある。

情報セキュリティパフォーマンス測定指標は、組織内の複数レベル(政府機関全体、局ごと、または個別のセキュリティプログラム)で策定し使用できる。セクション 3.6 で論じたように、パフォーマンス測定指標はさまざまな活動に合わせて対象範囲を調整できる。組織内の異なるレベルで策定した測定指標は、内部管理とプロセス改善のために使用すべきである。それらの測定指標を政府機関レベルのセキュリティプログラムパフォーマンス測定指標に統合することもできる。政府機関レベルの測定指標は、組織の幹部に報告されるか、または、GPRA や FISMA などの外部への報告に利用される。

5. 測定指標策定プロセス

早い段階でセキュリティパフォーマンス測定指標プログラムの準備に時間を裂くことは、システム開発段階で要件定義に時間を裂くことと同様のメリットがある。開発プロセスの初めに要件定義に時間を注ぐことは、プロセスの進行中にそのつど要件を改定する場合に比べてより効果的である。以下に、パフォーマンス測定指標プログラムの策定にあたって考慮すべき重要な事項を示す。

- ●組織の戦略とビジネス環境(ミッションおよび情報セキュリティにおけるプライオリティー、環境、要件を含む)に最も適した管理策を選択する。
- ●すべての関係者から時間をかけてインプットを収集し、彼らの賛同を得たうえで、彼らに教育を施す。
- ●適切な技術およびプロセス基盤(データ収集、分析および報告ツールの作成/修正を含む)の構築を確実にする。

情報セキュリティ測定プログラムの確立および運用は、測定指標の策定と実施という 2 つのプロセスによって導かれる。測定指標の策定プロセスでは、測定指標の初期セットを作成し、その中からある時点で組織にとって適切な測定指標を選択する。情報セキュリティ測定プログラムの実施プロセスは元来反復可能であり、セキュリティの適切な側面が、特定の期間に渡って測定されていることを保証する。この章では、測定指標の策定プロセスについて説明する。(実施プロセスについては、第 6 章で説明する。)

図 5-1 に、より大きな組織における情報セキュリティ測定指標の位置づけを示す。ここに示すように、情報セキュリティ測定指標を使うことによって、組織や特定のシステムにおいてセキュリティ活動が実施されているか、その効率や有効性はどうか、ビジネスへの影響があるかといった点を漸進的に評価することができる。

情報セキュリティ測定指標の策定プロセスでは、主に次の 2 つのことを行う。

- ●現在の情報セキュリティプログラムの明確化と定義
- ●セキュリティ管理策の実装、効率、有効性、影響を評価するための特定の測定指標の策定と選択

図 5-1 で示した 2 つの作業は、順番に実行する必要はない。このプロセスは、測定指標について検討するための枠組みであり、このプロセスを通じて特定の組織、または、組織内のさまざまな利害関係者グループに合わせて調整できる測定指標を特定することができる。

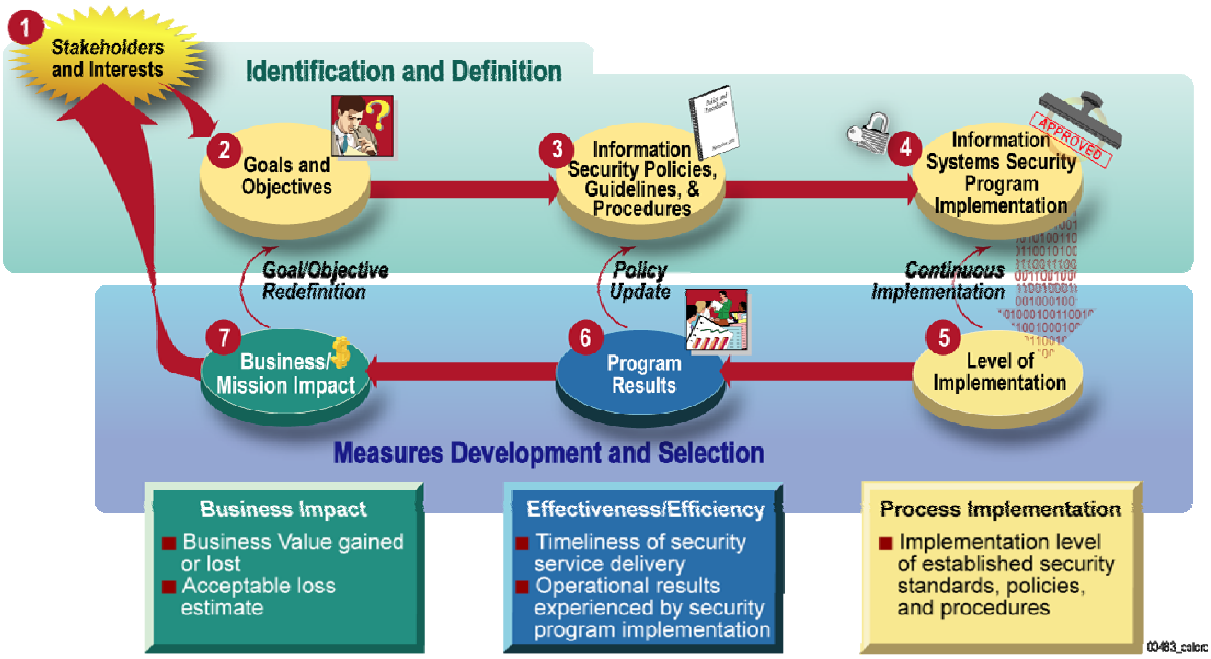

図 5-1 情報セキュリティ測定指標策定プロセス

5.1 関係者の利害の明確化

測定指標策定プロセス(図 5-1)のフェーズ 1 は、利害関係者と情報セキュリティ測定指標に対する彼らの関心事を示している。組織のだれもが情報セキュリティの関係者になりうる(ある人またはグループが、他の人またはグループよりも、より深くセキュリティに関与することはあるにせよ)。以下に、情報セキュリティに関する主な関係者を示す。

●部局長

●最高情報責任者(CIO)

●上級情報セキュリティ責任者(SAISO) ／最高情報セキュリティ責任者(CISO)

●情報システムセキュリティ責任者(ISSO)

●プログラムマネージャー／システムオーナー

●システム管理者／ネットワーク管理者

●セキュリティ担当者

●情報システムサポート担当者

次に重要なセキュリティ関係者は組織のメンバーで、セキュリティが主なミッションではないものの、業務上何らかの形でセキュリティに関わるメンバーである。これには、以下の者が含まれる可能性がある。

●最高財務責任者(CFO)

●教育部門

●人事部門

●監察官(IG)

●個人情報保護管理責任者(CPO)および個人情報保護に責任をもつ他の担当者

組織階層の中での関係者の役割におけるセキュリティの性格や地位に応じて、関係者それぞれの利害は異なる。関係者には、自分の責務範囲内での組織のセキュリティのパフォーマンスがわかるような、カスタマイズされた測定指標が必要になる場合がある。関係者の利害関係がどうなっているかは、インタビュー、ブレインストーミング、ミッション宣言のレビューなど、複数の場面を通じて決定することができる。関係者の関心事は、法律や規制への準拠にあることが多い。セクション 3.4.2 で述べたように、各関係者が受け持つ測定指標の数は、一人あたり 2～3 個とすべきである。組織がセキュリティプログラムを確立している段階では、一人あたりの測定指標の数をより少なくすることをお勧めする。測定指標の数は、セキュリティプログラムと測定プログラムの成熟に合わせて、徐々に増やしていけばよい。

関係者には情報セキュリティ測定指標策定の各段階に参加してもらい、セキュリティパフォーマンスを評価するという考えを確実に浸透させるべきである。関係者が参加することで、システム情報セキュリティ測定指標が他人事ではないという意識が組織のさまざまなレベルで生まれ、プログラム全体が成功に向かう。

情報セキュリティの 3 つの評価可能な側面(ビジネスへの影響、効率／有効性、実施の有無)が、それぞれ異なる関係者の興味を引く。経営者はビジネスやミッションへのセキュリティ活動の影響(最新の事故による財政上の損害や社会的な信用上の損害、有力紙に自分たちに関する記事が載るかなど)に興味を持つが、セキュリティマネージャーやプログラムマネージャーは、セキュリティプログラムの効率と有効性(事故を防ぐことはできたか、どれだけ迅速に対応できたかなど)に興味を持つ。一方で、システム管理者やネットワーク管理者は、何がいけなかったのか(事故を防止するため、あるいは事故の影響を最小限に食い止めるために必要なことをすべて行ったか)を知りたがる。

5.2 目標と目的の定義

測定指標策定プロセス(図 5-1 参照)のフェーズ 2 では、情報システムのセキュリティプログラムで定めたセキュリティ管理策の実装を左右する、システムセキュリティパフォーマンスの目標と目的を明確にして文書化する。連邦政府組織に対するシステムセキュリティの目標と目的は、高レベルのポリシーや要件、法律、規制、ガイドラインおよびガイダンスの形で表される。[7]

セキュリティプログラムの目標と目的は、政府機関全体のミッションを支援するエンタープライズレベルの目標と目的(通常は政府機関の戦略計画およびパフォーマンス計画で明示されるもの)から導き出すこともできる。適用可能なセキュリティパフォーマンスの目標や目的を明確化し抽出するために、該当するドキュメントをレビューするべきである。抽出された目標や目的は関係者とともに検証し、確実に関係者が目標や目的を受け入れて測定指標策定プロセスに参加するようにする。

[7] 要件、法律、規制、ガイドラインおよびガイダンスの詳細は、セクション 4 を参照のこと。

FIPS 200『連邦政府の情報および情報システムに対する最低限のセキュリティ要求事項(Minimum Security Requirements for Federal Information and Information Systems) 』は、必要最低限のセキュリティ要件の仕様を提供する。NIST SP 800-53 では、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) 』が規定する低位、中位および高位の影響レベルの情報システムに対する、最低限必要なセキュリティ管理策を記載している。政府機関は、自身の情報システムが処理、保存、伝送するデータの機密度に応じて、最低限必要なセキュリティ管理策を定義、実施すべきである。このように政府機関のセキュリティプログラムには、これらのセキュリティ管理策の実施と有効性に関する計画、実施、監視、および報告を含めなければならない。政府機関は、セキュリティ活動と政府機関レベルの戦略計画作成を首尾よくリンクするために、FIPS 200 に記載の最低限のセキュリティ要求事項の仕様を情報セキュリティパフォーマンス測定指標の開発目的への入力として使用できる。(本仕様は、NIST SP 800-53 の 17 のセキュリティ管理策ファミリに対応するものであり、詳細は付録 D に記載している。) 付録 A に、プログラムレベルとシステムレベルの情報セキュリティ測定指標と、それに対応する目標や目的の例を記載している。

5.3 セキュリティポリシー、手引き、手続きのレビュー

測定指標策定プロセス(図 5-1 参照)のフェーズ 3 では、組織ごとのセキュリティ上の慣例に焦点を当てる。セキュリティ管理策をどのように実装すべきかに関する詳細は、通常は組織ごとのポリシーや手続きに明記される。ポリシーや手続きには、システムに対して規定されたセキュリティ上の慣例のベースラインが定義されているが、特に、セキュリティ管理策、セキュリティ要件、およびセキュリティ技術を実施することが、どのような形でセキュリティパフォーマンスの目標や目的の達成につながるかを記載している。最初に測定指標を策定する時や、将来、初期の測定指標が使い尽くされて他の測定指標で置き換える必要が生じた場合には、これらの文書を検証する必要がある。組織は、適用されるドキュメントをレビューし、適切なセキュリティ管理策、適用可能な手順、およびパフォーマンス目標を設定しなければならない。

5.4 セキュリティプログラムの実施レビュー

測定指標策定プロセス(図 5-1 参照)のフェーズ 4 では、測定データを抽出するのに使用できる可能性のある既存の測定指標とデータリポジトリをすべてレビューする。レビュー後に実際にそれらの情報を取り出し、それを使って、測定指標の策定やデータ収集の基となる実施証拠を明確化する。[8] 実施証拠とは、セキュリティパフォーマンス目標が満たされているか、または少なくとも将来的にパフォーマンス目標の達成につながるような活動が行われているかを示す、セキュリティ管理策の側面を指す。既に実施されたシステムセキュリティ要件、手順、手続きは、ドキュメント、インタビュー、観察といった複数の情報源から抽出することが可能である。

測定データの生成に必要な情報は、以下の情報源に含まれていることがある。

●システムセキュリティ計画 [9]

---

8 実施証拠とは情報セキュリティパフォーマンス測定指標を支援するために収集したデータのことをいう。実施証拠に関しては、セクション 5.6 の表 2 で詳しく説明している。

9 NIST SP 800-18 は、システムセキュリティ計画作成に関するガイドラインを提供する。

●行動計画とマイルストーン(POA&M)レポート

●最新の GAO や IG の調査結果

●セキュリティ関連活動の記録(事故対応と報告、テスト、ネットワーク管理、監査ログ、ネットワークとシステムの課金など)

●リスクアセスメントとペネトレーションテストの結果

●承認および運用認可(C&A)文書(セキュリティアセスメントレポートなど)

●継続監視結果

●緊急時対応計画

●構成管理計画

●トレーニングの結果と統計

システムセキュリティ活動が進化し、それを記述した文書が変化するに従い、既存の測定指標が廃止されて新しい測定指標が策定されることになる。新しく策定された測定指標が適切なものになるように、これらのドキュメントや他の同様のドキュメントを調査して、測定指標に盛り込むべき新しい領域を明確化することが必要となる。

5.5 測定指標の策定と選択

測定指標策定プロセス(図 5-1 参照)のフェーズ 5、6、7 は、プロセスの実施、有効性と効率、ミッションへの影響を評価する測定指標の策定に関連するものである。この章で紹介する測定指標策定プロセスは、これらの 3 つの分野の測定指標を作成する方法を示すものである。(付録 A に、NIST SP 800-53 のセキュリティ管理策ファミリに対応する測定指標を含めた測定指標の候補を記載している。) このプロセスでは、システムセキュリティとプログラムセキュリティの継続的改善を支援することを目的として、パフォーマンス測定指標を策定、使用し、セキュリティ活動を組織の戦略目標に明示的に結びつける。このアプローチは、組織が複数の戦略目標を持つこと、また、一つの目標が複数の測定指標からの入力を必要とする可能性があることを前提としている。

5.5.1 測定指標の策定アプローチ

情報セキュリティ測定指標の策定では、測定活動の範囲に応じて、特定の管理策の評価、管理策グループの評価、またはセキュリティプログラムの評価のいずれかに焦点を合わせるべきである。このようなアプローチにより、戦略目的支援に対する組織のスタンスを確認するための測定指標を策定することができる。また、このアプローチを複数の管理策やセキュリティプログラム全体の測定に使用することによって、セキュリティパフォーマンスを大局的に見ることができる。

管理策ファミリ、または個々の管理策に対応する測定指標は、以下に示す事項を満たさなければならない。

●当該管理策(または管理策ファミリ)に直接マッピングされること。

●セキュリティ管理策の実施(状況)を表すデータを使って、行動計画とマイルストーン(POA&M)、テスト、プロジェクト追跡などの、必要な測定指標を策定すること。

●測定指標を低位、中位、高位影響レベルの情報システムのいずれかに割り振ること。

セキュリティプログラムの全体的なパフォーマンスを扱う測定指標は、以下に示す事項を満たさなければならない。

●対象となるすべてのセキュリティ管理策の全体的なセキュリティパフォーマンスを包含していることもあるセキュリティ目標と目的にマッピングされること。

●セキュリティプログラムパフォーマンスを表すデータを使って、必要な測定指標を策定すること。

5.5.2 測定指標の優先順位付けと選択

既存のポリシーや手続きに基づいて考えられる測定指標は非常に多くある。測定指標に優先順位を付けることにより、初回の実施に向けて選択された最終的な測定指標が、以下の性質を満たすようにする。

●リスクベースのアプローチを使って定められた、優先度の高いセキュリティ管理策の実装を強化できること。優先度の高い項目は、最新の GAO または IG のレポート、継続監視の一環として実施するリスクアセスメントの結果、または組織の内部的な目的などによって決定される。

●既存の情報源やデータリポジトリ(システム一覧、トレーニングデータベース、行動計画とマイルストーン（POA&M）など)から実際に取得可能なデータを使用すること。

組織は、自身が評価するものを管理する。関係者一人につき、優先度が高い測定指標を 2～3 個選択して割り当てるとよい。優先順位付けには、リスクベースのアプローチを使用すること。

●既存の確立されたプロセスを評価するものであること。一貫性のないプロセスを評価しても、セキュリティパフォーマンスに関して意味のある情報を得ることはできず、パフォーマンスのある側面を対象とするために活用することはできない。ただし、そのような評価を行うことによって、継続的なアセスメントによる厳密な監視が必要なベースラインを特定し、セキュリティ状態を改善するための新しい測定指標を得られる場合もあるため、まったく意味がないというわけではない。

組織は、選択された測定指標の重要度に差異を設け、結果が既存のセキュリティプログラムの優先度を正確に反映するようにするために、重み付けがされた尺度(scale)を使ってもよい。その場合には、セキュリティプログラム全体の中でのその測定指標の重要度に基づいて、各測定指標に対して値を割り当てる。測定指標の重み付けは、全体的なリスク緩和目標に基づいて行われるべきであり、そうすることによって、相対的に規模が小さなイニシアチブではなく、より重要度の高いエンタープライズレベルのイニシアチブを反映できるようになる。測定指標の重み付けは、情報セキュリティ測定指標を部門の資金計画プロセスへと統合するための有効なツールとなる。

5.5.3 パフォーマンス目標の設定

パフォーマンス目標を設定することは、情報セキュリティ測定指標を定義するうえで重要な要素となる。パフォーマンス目標により、成功の度合いを判断するための基準が確立される。成功の度合いは、測定指標の結果が、記述されたパフォーマンス目標にどれだけ近いかによって決まる。パフォーマンス目標を設定する仕組みは、実施測定指標とその他 2 種類の測定指標(効率／有効性と影響)とで異なる。実施測定指標では、目標は、特定のタスクが 100% 達成された状態に設定する。

効率／有効性測定指標と影響測定指標に対するパフォーマンス目標の設定は、より複雑である。なぜならマネジメント層は、定性的論証や主観的な論証を用いてセキュリティの有効性と効率の適切なレベルを定め、それらのレベルを適用可能な測定指標に対するパフォーマンス目標として使用する必要があるからである。どんな組織でも、セキュリティ管理策の効果的な実装、セキュリティサービスの効率的な提供、セキュリティ関連の事故がミッションに与える影響の最小化を望むものであるが、関連する評価項目は、システムごとに異なる。これらの測定指標に対するパフォーマンス目標を設定しておき、実際の評価結果が得られた後に、その結果を元にして目標を調整してもかまわない。また、パフォーマンスのベースラインとして使えるような最初の評価結果が得られるまでは、これらの測定指標に対する目標を設定しなくてもよい。つまり、ベースラインが得られ、改善にむけた活動が明確になった段階で、特定のシステム環境にとって現実的な、適切なパフォーマンス目標と実施のマイルストーンを定義する。ベースラインが得られた後でもパフォーマンス目標を設定できないようであれば、マネジメント層は、評価した活動とそれに対応する測定指標から組織が期待する価値が得られているかどうかを検討する必要がある。

有効性／効率測定指標と影響測定指標のベースラインとパフォーマンス目標の設定は、これらの測定指標に関係する履歴データがあると容易になる場合がある。過去の傾向を観察することにより、これまでのパフォーマンスの範囲がどの程度であったかがわかり、将来に対する実際的な目標を設定できるようになる。将来的には、専門家による推奨事項や業界標準が公開され、目標設定の手段を提供することになるかもしれない。図 5-2 に、承認された情報セキュリティ計画の割合に関する実施測定指標の例を示す。

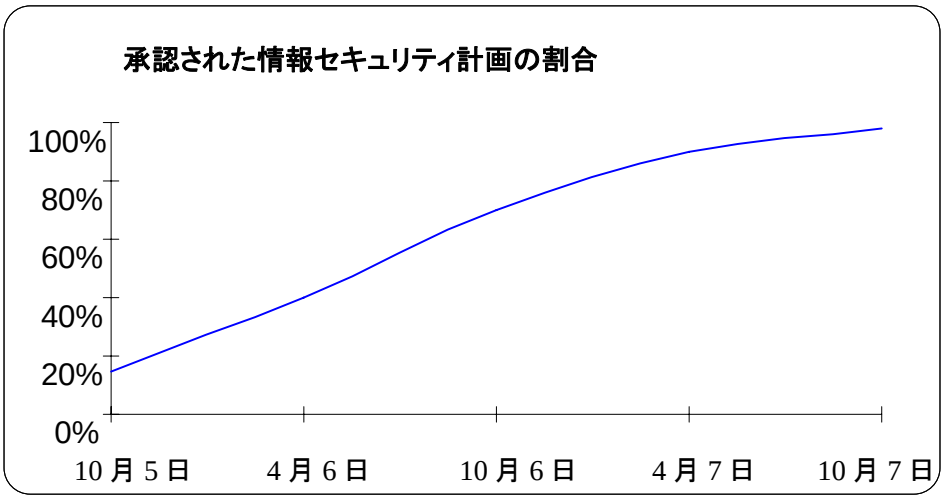

図 5-2 情報セキュリティ測定指標傾向の例

5.6 測定指標策定用テンプレート

組織は、測定指標の開発、調整、収集、および報告活動が繰り返し利用できることを確実にするために、パフォーマンス測定指標を標準書式で文書化しなければならない。測定指標を標準書式で文書化することにより、

本テンプレートおよび付録Aに記載の測定指標の候補は、あくまでも例であり、組織のニーズに合わせて調整できるようになっている。

測定指標の収集、分析および報告活動の手引きとなる詳細を得ることができる。表 2 の測定指標テンプレートは、そのような標準書式の例を示すものである。

測定指標テンプレートは、測定指標のための推奨アプローチを提供するが、組織内部の慣行や手順によっては、組織がテンプレートを調整する必要がある場合がある。テンプレートの調整は、当該フィールドのサブセットを使用したり、組織の環境や要件にもとづきフィールドを追加することによって実施できる。

表 2 測定指標テンプレートとインストラクション

フィールド	データ
測定指標 ID	測定指標の追跡および並べ替えに利用できる一意の識別子を記述する。これらの識別子は、組織の命名規約によって割り当てることもできるし、そのほかのソースを参照して割り当ててもよい。
目的	戦略目標および／またはセキュリティ目標を記述する。システムレベル測定指標では、目標を達成することが、当該システムの管理策を実施することにつながる。プログラムレベル測定指標には、戦略目標とセキュリティ目標の両方が含まれることがある。たとえばセキュリティ目標は、組織のミッションを支援するエンタープライズレベルの目標から導き出すことができる。これらの目標は通常、戦略計画およびパフォーマンス計画で明示される。可能な場合、政府機関のドキュメントから抽出したエンタープライズレベルの目標と具体的なセキュリティ目標も記述するか、もしくは、選択された戦略目標の達成を助成するセキュリティプログラム目標を記述する。
測定指標	測定指標の定義を記述する。「割合」、「数」、「頻度」、「平均」など、数量を表す単語で始まる言葉を使用する。 . 可能であれば、評価対象の NIST SP 800-53 の管理策を記述する。評価結果を裏付ける情報を提供する管理策は、「実施証拠」欄に記述する。測定指標が FIPS 199 の影響レベル(高位、中位、低位)のいずれかに当てはまる場合は、そのレベルも記述すること。
種類	測定指標の種類(実施、有効性／効率、影響)を記述する。
数式	数値による測定指標を得るために実行する計算を記述する。実施証拠のリストアップを通じて収集した情報は、測定指標を求めるための数式に対する入力となる。
達成目標	測定指標が満足できるものであるかどうかを判断するための閾値。(マイルストーンの達成の度合いや統計測定指標など。) 達成目標は、割合、時間、ドル、または他の適切な単位で表わすことができる。達成目標には、達成期限を含めることができる。最終目的と臨時目標を設定し、目標が達成されるまでの進捗を追跡できるようにする。
実施証拠	実施証拠は、測定指標を算定し、活動が実施されたことを立証し、特定の測定指標が満足できない結果をもたらした原因を特定するために使用する。 ●手動によるデータ収集では、測定指標公式の計算に必要なデータを得るための質問とデータ要素を特定し、測定指標が受容できるかを確認し、取得した情報が有効であるかを確認すること。 ●各質問またはクエリー に関して、情報提供元となった NIST SP 800-53 管理策の番号を記述すること。(可能な場合のみ) ●測定指標が FIPS 199 の影響レベルのいずれかに当てはまる場合は、そのレベルも記述すること。 ●自動化されたデータ収集では、測定指標公式の計算に必要なデータの要素を特定し、測定指標が受容できるかを確認し、取得した情報が有効であるかを確認すること。
頻度	データの収集、分析、報告を行う頻度を記述する。データを収集する頻度は、評価対象のセキュリティ管理策の変化率をもとに決定すること。データを報告する頻度は、外部への報告要件と内部顧客の好みをもとに決定すること。

フィールド	データ
責任を負う利害関係者	以下に示すような主要な関係者を記述する。 ●情報のオーナー: 組織において、(自身に)必要な情報を所有する構成要素および個人を特定すること。 ●情報の収集者: 組織において、データの収集に責任を持つ構成要素および個人を特定すること。(注:情報の収集は、可能な場合に別の者に任せるか、あるいは、別の組織の代表者に任せるべきである。これにより、利害の対立を避け、職務の分離を確実に実施できる。小規模企業の場合、これらの 2 つの職務を分離することが可能かどうかを見極める必要がある) ●情報の受領者: 組織において、データを受信する構成要素および個人を特定すること。
データソース	測定指標を求めるために使うデータがある場所を記述する。これには、必要な情報を提供するデータベース、追跡ツール、組織、組織内の特定の役職などを含むようにする。
報告フォーマット	測定指標がどのような形式(円グラフ、折れ線グラフ、棒グラフ、または他の書式)で報告されるかを記述する。フォーマットのタイプを記述するか、あるいは、サンプルを示すこと。

付録Aに記載の測定指標候補は、あくまでも測定指標の例であり、ある時点において、規制に関する報告や組織に関する報告を行うために必要となる場合もあれば(FISMA など)、そうでない場合もある。 これらの測定指標をリストアップする目的は、以下の条件を満たす測定指標の例を示すことにある。

●記述されているとおりに使用できる。

●組織の要件に合わせて修正し、調整できる。

●他の情報セキュリティ測定指標を策定するためのテンプレートとして使用できる。

組織は、これらの測定指標を、自身の測定活動の開始点として自由に使用できるが、これらの測定指標は必須ではない。

5.7 測定指標策定プロセス内のフィードバック

最終的に実施するために選択された測定指標は、パフォーマンスの評価、満足のいかない評価結果の原因の特定、改善領域の特定だけでなく、一貫したポリシーの実施、セキュリティポリシーの変更の実施、目標や目的の再定義、パフォーマンスの継続的な向上などにも役立つ。この関係は、図 5-1 の「目標／目的の再定義」、「ポリシーのアップデート」、「継続的な向上」と書かれたフィードバックの矢印で示されている。いったんセキュリティ管理策の実施の評価が開始されると、その後の評価は、パフォーマンスの傾向を明らかにし、実施の割合が適正かどうかを判断するために使用することができる。また、各測定指標をどの程度の頻度で収集すべきかは、評価対象となる事象のライフサイクルに依存する。完了または更新されたセキュリティ計画の割合に関する測定指標は、年 2 回よりも多い頻度で収集すべきではない。クラック可能なパスワードに関する測定指標は、より頻繁に収集すべきである。継続的な評価は、適用されるセキュリティ管理策が継続的に実装されることにつながる。有効性／効率測定指標が実装されると、セキュリティポリシーと手続きで設定したセキュリティ管理策のパフォーマンス目標が現実的かどうか、また、適切かどうかが理解しやすくなる。

たとえば、セキュリティポリシーで特定のパスワード設定が定義されている場合、ポリシーへの準拠の度合いは、ポリシーに従って設定されているパスワードの割合を測ることでわかる。これは、セキュリティ管理策の実装レベルを測るものである。すべてのパスワードをポリシーに準拠して設定することにより、パスワードが破られてシステムが不正に使用されることが完全には無くならないにせよ、かなりの程度減ると考えられる。既存のパスワードポリシーの実施の有効性を測るには、クラック可能なパスワードの割合を測ればよい(これには、パスワードを破るための一般的なツールを使用する)。これは、実装されたセキュリティ管理策の有効性を測るものである。必要なパスワードポリシーを実施した後もクラック可能なパスワードがかなりの割合で残っている場合には、論理的な帰結として、パスワード破りを防ぐという目的においては、そのポリシーは有効ではないということになる。その場合には、ポリシーを強化するか、他の緩和策の実施を検討する必要がある。さらに、パスワードポリシーを現在のままにしておくか、強化するか、それともパスワード認証を他の手法で置き換えるかについて、コストとメリットを見極める必要がある。費用便益分析を行うことにより、ビジネス影響測定指標が得られる。このビジネス影響測定指標により、システムの特定や認証の目標を再定義し、これらの目標とシステムのミッションとを適切に整合させるという問題に対処することができる。

6. 情報セキュリティ測定の実施

情報セキュリティ測定を実施する際には、情報セキュリティ測定指標を使ってセキュリティ管理策のパフォーマンスを監視し、監視結果を使ってパフォーマンスを向上させるための行動を起こす。この反復的なプロセスは 6 つのフェーズから構成され、すべてのフェーズが実行された場合に、情報セキュリティ測定指標を継続的に使用することによる、セキュリティ管理策のパフォーマンスの監視と改善が可能になる。図 6-1 に、情報セキュリティ測定プログラムの実施プロセスを示す。

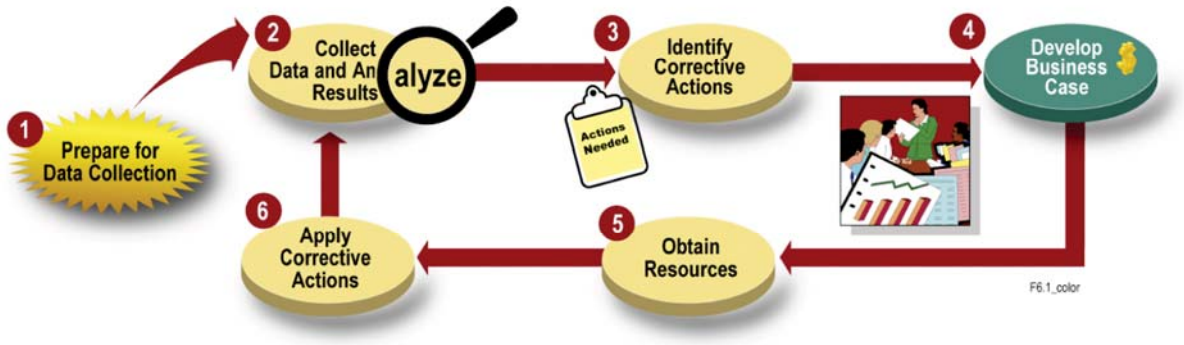

図 6-1 情報セキュリティ測定プログラムの実施プロセス

6.1 データ収集の準備

プロセスのフェーズ 1、「データ収集の準備」は、総合的な情報セキュリティ測定プログラムを確立するうえでの主要な活動であり、情報セキュリティ測定指標の明確化、定義、策定、選択が含まれる。次のステップは、情報セキュリティ測定プログラムの実施計画の策定である。[10]

具体的な実施手順は、測定用のデータをどのように収集、分析、報告するかにもとづいて決定する。これらの手順は「測定プログラム実施計画書」として文書化する。計画書には、以下の項目が含まれることがある。

- 計画の読者
- データ収集(依頼側と提供側)、分析、報告の責務を含む、測定指標の役割と責務

[10] 情報セキュリティ測定プログラムの実施計画は、組織のニーズに応じて文語体(formal)であったり、口語体(informal)であったりする。

●測定指標の収集、分析、報告プロセス(特定の組織構造、手順、ポリシー、手続きに合うように調整されたもの)

●リスクアセスメント、C&A、FISMA 報告活動といった、CIO 室の内部での調整内容の詳細

●測定データを効率的かつ妨害されずに収集することを確実にするための、SAISO(上級情報セキュリティ責任者)と組織内の SAISO 以外の機能との間での調整内容の詳細

●データの収集と追跡を行うツールの作成や選定

●データの収集と追跡を行うツールの変更

●測定指標の要約報告フォーマット

情報セキュリティ測定指標の実施計画には、セキュリティプログラムの継続監視に関する規定を含まなければならない。継続監視活動には、構成管理、情報システムに変更が加わることにより生じるセキュリティへの影響の分析、セキュリティ管理策のサブセットのアセスメント、およびステータスに関する報告が含まれる。堅実な継続監視慣行により、組織は、継続監視を目的としてシステムに導入する管理策を選択するための、選択基準を確立することができる。NIST SP 800-37 は、継続監視プロセスに関する手引きである。NIST SP 800-53A は、セキュリティ管理策のアセスメントに関する手引きである。継続監視の結果から、フェーズ 2 で収集するデータを補足、支援するためのデータを得ることができる。また、継続監視の結果を使用することで、フェーズ 3 の是正措置の優先順位付けが楽になる。

6.2 データ収集と結果分析

フェーズ 2「データ収集と結果分析」では、収集した測定指標を使ってシステムセキュリティの理解を深め、適切な是正措置を明確にするのに不可欠な活動を行う。フェーズ 2 には以下の活動が含まれる。

●「測定プログラム実施計画書」で規定された手順に基づいて測定データを収集する

●測定指標を適宜統合し、高レベルの測定指標を得る。(たとえば、システムレベルの測定指標をロールアップすることで、プログラムレベルの測定指標を得る。)

●収集データの整理と、データ分析や報告に適したフォーマット(データベースやスプレッドシートなど)での保管

●ギャップ分析の実施 － 収集した測定指標を、(定義されている場合には)目標に照らし合わせ、実際のパフォーマンスと期待されるパフォーマンスとのギャップを明確にする

●パフォーマンスが良くない場合の原因の特定

●改善が必要な領域の特定

パフォーマンスが思わしくない場合の原因は、複数の測定指標から得たデータを使って特定できることがよくある。たとえば、承認されたセキュリティ計画の割合が許容できないほど低いということを突き止めたとしても、それだけでは(セキュリティ計画への準拠の度合いが低いといった)問題の改善方法を見いだすことはできない。準拠の度合いが低い原因を特定するためには、承認されたセキュリティ計画の割合が低い理由に関する情報を収集する必要がある(手引きがない、経験不足、優先順位の衝突など)。この情報は、別個の測定指標として収集することも、承認済みのセキュリティ計画の割合に対する実施証拠として収集することも可能である。この情報を収集して整理した後、問題の原因に対して是正措置を実行することになる。

以下に、セキュリティ管理策の実装や有効性の確保がうまくいかない原因の例を示す。

●リソース －人的資源、財源などのリソース不足

●訓練－ システムの設置、管理、維持、使用を行う要員に対し、適切な訓練が行われていない

●システムのアップグレード－セキュリティパッチのうち、以前に削除されていて、オペレーティングシステムのアップグレードの際に含まれなかったものがある

●構成管理の実施－新しいシステムやアップグレードしたシステムに、必要なセキュリティ設定やパッチが適用されていない

●ソフトウェアの互換性－セキュリティパッチやアップグレードに、システムがサポートするソフトウェアアプリケーションとの互換性がない

●認識とコミットメント－マネジメント層にセキュリティに対する認識がない／マネジメント層のコミットメントがない

●ポリシーと手続き－必要なセキュリティ機能の組み込み、使用、監査を保証するために必要なポリシーや手続きがない

●アーキテクチャーシステムアーキテクチャやセキュリティアーキテクチャが貧弱なために、システムが脆弱である

●プロセスの非効率性－計画プロセスおよび実施プロセスが非効率なために測定に影響が出ている(組織的な行動を指示するために必要なコミュニケーションプロセスも含む)

6.3 是正措置の明確化

プロセスのフェーズ 3「是正措置の明確化」では、実施におけるギャップ(フェーズ 2 で明確化されたもの)を埋めるためのロードマップとなる、計画を作成する。これには以下の活動が含まれる。

●是正措置の範囲の決定－結果と原因要素に基づき、各パフォーマンスの問題に対して適用し得る是正措置を明確にする。是正措置には、システム設定の変更や、セキュリティ要員･システム管理要員･正規利用者の訓練、セキュリティツールの購入、システムアーキテクチャの変更、新しい手順と手続きの作成、セキュリティポリシーの更新などがある。

●全体的なリスク緩和目標に基づく是正措置の優先順位づけ－ひとつのパフォーマンスに関わる問題に適用できる是正措置はいくつかあるが、問題の大きさと釣り合わなかったり、費用がかかりすぎたりして、適切でないものがある。適用可能な是正措置には、パフォーマンスに関わる問題ごとに、コストの低い順、効果が大きい順に優先順位を付ける。是正措置に優先順位をつける際には、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)』で説明されているリスク管理プロセス、または NIST SP 800-65『IT セキュリティの資金計画および投資管理プロセスへの統合(Integrating IT Security into the Capital Planning and Investment Control Process)』で説明されている是正措置の優先順位付けプロセスを使用すべきである。「データ収集の準備」フェーズで各測定指標に対して重みを割り当てた場合には、これらの重みを用いて是正措置に優先順位を付ける。そうでない場合には、本フェーズ「是正措置の明確化」において、特定の是正措置の実施の重要度、是正措置のコスト、是正措置が組織のセキュリティ状況に与える影響の度合いに基づいて、是正措置に重みを割り当てるこ

ともできる。是正措置は、対応するシステムまたは組織の POA&M に記述し、継続監視プロセスの一環として追跡すべきである。

●最も適切な是正措置を選択－優先順位をつけた是正措置のリストから、実行可能な是正措置を選び、十分な費用便益分析を実施する。

6.4 ビジネスケース（投資対効果検討書）の策定とリソースの獲得

フェーズ 4 と 5 はそれぞれ「ビジネスケースの作成」と「リソースの獲得」で、フェーズ 3 で明確になった改善措置の実施に必要な、リソースを獲得するための予算策定サイクルについて言及する。ビジネスケースの開発に関わる手順は業界の慣例や義務化されたガイドライン(OMB Circular A-11、クリンガー・コーエン法(Clinger-Cohen Act)、GPRA を含む)を基にする。これより前の 3 つのフェーズの結果は、補強証拠としてビジネスケースに含まれる。

以下に、ビジネスケース分析の一環として通常実施される活動を示す。これらの活動は、是正措置の実施に必要なリソースを獲得するための、政府機関固有のプロセスの範囲内で実施される。

●測定指標策定プロセスのフェーズ 2 で明確化したミッションとその目標を記述。

●現状を維持するのに必要なコストを算出し、リスクを評価して、他の投資と比較する際の基準として使用。

●測定プログラム実施プロセスのフェーズ 2 で明確化した、パフォーマンス目標と現在の評価結果とのギャップを記述。

●測定プログラム実施プロセスのフェーズ 3 で明確化した、各是正措置に対するライフサイクルコストまたは代替投資の評価。

●感度分析を行って、どの変数が最もコストに影響するかを見極める。[11]

●改善されたパフォーマンスによってもたらされる、定量化可能な利点と定量化不可能な利点の特徴を記述する。その際、測定プログラム実施プロセスのフェーズ 3 で付与した是正措置に対する優先順位を元にする。

●特定の代替手段に付随する障害やプログラム上のリスクの可能性を考慮に入れるためにリスク分析を行う。

●ビジネスケースの利点を正確に表現するために、ビジネスケースの要点を要約して、予算提出の準備を行う。[12]

各政府機関は、このフェーズでは、政府機関独自のビジネスケースガイドラインに従わなければならない。政府機関は、通常、独自のビジネスケースプロセスと、ライフサイクルにおける支出に関する閾値を備えており、これらのプロセスと閾値を使って、どの投資および予算要求がフォーマルなビジネスケースを要するかを判断する。一般に、ビジネスケースの策定に要する労力は、資金要請の規模と範

11 変数の値を少しだけ変化させることによって計算結果が大きく変わる場合、結果はそのパラメータや前提に対して感度が高いということになる。

12 是正措置の実施に必要な予算を要求するための、情報の準備に関する詳細は、NIST SP 800-65『IT セキュリティの資金計画および投資管理プロセスへの統合(Integrating IT Security into the Capital Planning and Investment Control Process)』を参照のこと。

囲に相応するものでなければならない。たとえば、災害復旧サイトを設置、維持するためのビジネスケースは、アカウントレビュープロセスを確立するためのビジネスケースよりも綿密になる。

ビジネスケースの範囲と複雑さにかかわらず、ビジネスケースの要素や分析を用いることで、内部予算や外部予算のリクエストをより容易に行うことができる。ビジネスケースを入念に調べることで、リソースを獲得しやすくなる。リソース獲得フェーズには、以下の活動が含まれる。

- ●予算審査のための質問への回答
- ●割り当てられた予算の受領
- ●利用可能なリソースの優先順位付け(要求したリソースがすべて割り当てられなかった場合)
- ●是正措置を実行するためのリソースの割り当て

6.5 是正措置の適用

プロセスのフェーズ 6「是正措置の適用」では、セキュリティプログラムに対する是正措置、または、セキュリティ管理策の技術面、管理面、運用面の各領域における是正措置を行う。組織は、行動計画とマイルストーン(POA&M)プロセスにより、是正措置の状態を文書化、監視する。

反復的にデータ収集、分析、報告を行うことにより、是正措置の進展状況の追跡、改善状況の評価、さらなる改善が必要な領域の明確化を行うことができる。サイクルを反復的に実施することによって、進展状況が監視され、是正措置がセキュリティ管理策の実装に意図したとおりに作用することが保証される。頻繁にパフォーマンスを測定することにより、是正措置が計画通りに実施されない場合や、期待した効果が現れなかった場合でも、組織内部で迅速な軌道修正が可能となる。これにより、外部の監査、C&A、その他の同様な活動において問題が発覚することを防止することができる。

付録 A: 測定指標の候補

十分な時間をかけてセキュリティパフォーマンス測定指標を確立することは、セキュリティパフォーマンスを評価することによって得られる効果を最大限にするためにも重要である。

この章では、プログラムレベルとシステムレベルの測定指標のサンプルを示す。サンプル測定指標には、セキュリティプログラム測定指標と、FIPS 200『連邦政府の情報および情報システムに対する最低限のセキュリティ要求事項(Minimum Security Requirements for Federal Information and Information Systems) 』に対応する測定指標が含まれる。FIPS 200 の最低限のセキュリティ要求事項は、NIST SP 800-53 の 17 の管理策ファミリに対応するものである。これらの測定指標は、完全セットとして使用できることを意図したものではなく、あくまでも例を示すものであり、組織は、これらの測定指標を調整し、セキュリティプログラムのパフォーマンスの評価に使用することができる。調整の例には、タイムフレーム、実施証拠、データソース、計算式、報告書式、頻度、責任を有する関係者、およびテンプレートへのフィールドの追加などが含まれている。

読者は、これらの測定指標が FIPS 200 の最低限のセキュリティ要求事項のすべてを扱っているわけではなく、それらの要求事項の単一または複数の重要な側面を扱っていることに留意する必要がある。組織は、本章記載の測定指標のサンプルが自身のニーズに合わない場合は、追加の測定指標を策定し、これらの測定指標を補足、または、置き換えることを検討すべきである。

これらの測定指標の候補は、プログラムレベルまたはシステムレベルで実施できるセキュリティ管理策の例である。これらにはすべての種類の測定指標(実施測定指標、有効性／効果測定指標、影響測定指標)が含まれる。

測定指標 1: セキュリティ予算(プログラムレベル)

フィールド	データ
測定指標 ID	セキュリティ予算測定指標 1
目標	• *戦略目標*: 人員、施設と製品のための包括的なセキュリティおよび説明責任環境を確保する。 • *セキュリティ目的*: 政府機関の情報と情報システムを適切に保護するためのリソースを確保する。
測定指標	政府機関の情報システム予算に対する、セキュリティ予算の割合(%)。 NIST SP 800-53 管理策: SA-2 (リソースの割り当て)
測定指標の種類	影響
計算式	(セキュリティに特化した予算 ／ IT に関わる予算の総額) × 100
達成目標	組織が定めた割合に達していること。
実施証拠	1. 政府機関のすべてのシステムに対するセキュリティ予算の総額はいくらになりますか (SA-2)? _____ 2. 政府機関のすべてのシステムに対する IT 予算の総額はいくらになりますか (SA-2)? _____
頻度	測定指標を収集する頻度: 組織が定めた頻度 (例: 年 1 回) 測定指標を報告する頻度: 組織が定めた頻度 (例: 年 1 回)
責任を有する関係者	• 情報のオーナー: 最高情報責任者(CIO)、最高財務責任者(CFO)、上級情報セキュリティ責任者(SAISO) (例: 最高情報セキュリティ責任者[CISO]) • 情報収集者: システム管理者 または情報システムセキュリティ責任者(ISSO)、予算担当者 • 情報の受領者: 最高情報責任者(CIO)、上級情報セキュリティ責任者(SAISO) (例: 最高情報セキュリティ責任者[CISO])、外部監査管 (例: OMB)
データソース	提示資料 300 および 53、政府機関の予算に関する文書 。
報告書式	IT 予算の総額に対するセキュリティ予算の割合(%)を示す円グラフ。

測定指標 2: 脆弱性管理(プログラムレベル)

フィールド	データ
測定指標 ID	脆弱性測定指標 1
目標	• *戦略目標*: 人員、施設と製品のための包括的なセキュリティおよび説明責任環境を確保する。 • *セキュリティ目的*: すべての脆弱性が特定、軽減されることを確実にする。
測定指標	発見された高い脆弱性[13] のうち、組織が定めた期間内に軽減された脆弱性の割合(%)。 NIST SP 800-53 管理策: RA-5 (脆弱性のスキャン(走査))
測定指標の種類	有効性／**効率**
計算式	(発見後、組織が定めた期間内に軽減された脆弱性の数 ／ 発見された脆弱性の数) × 100
達成目標	組織が定めた割合に達していること。
実施証拠	1. その期間内に発見された高い脆弱性はいくつありますか? (RA-5)? _____ 2. 上記の脆弱性のうち、組織が定めた期間内に軽減された脆弱性はいくつありますか? (RA-5)? _____
頻度	測定指標を収集する頻度: 組織が定めた頻度 (例: 四半期ごと) 測定指標を報告する頻度: 組織が定めた頻度 (例: 四半期ごと)
責任を有する関係者	• 情報のオーナー: 最高情報責任者(CIO)、上級情報セキュリティ責任者(SAISO) (例: 最高情報セキュリティ責任者[CISO])、システムオーナー • 情報収集者: システム管理者または情報システムセキュリティ責任者(ISSO) • 情報の受領者: 最高情報責任者(CIO)、上級情報セキュリティ責任者(SAISO) (例: 最高情報セキュリティ責任者[CISO])
データソース	脆弱性走査ソフト、監査ログ、脆弱性管理システム、パッチ管理システム、変更管理記録。
報告書式	発見された脆弱性のうち、組織が定めた期間内に軽減された脆弱性の割合(%)を、報告期間別に示す積重ね棒グラフ。

13 NVD(National Vulnerability Database)は、データベース上のすべての CVE(Common Vulnerabilities and Exposures)に対して、「低位」「中位」および「高位」のランク付けを行うように設計されている。 NVD は、http://nvd.nist.gov. からアクセスできる。

測定指標 3: アクセス制御(AC) (システムレベル)

フィールド	データ
測定指標 ID	リモートアクセス制御測定指標 1 (または組織指定の一意の識別子)
目標	• *戦略目標*: 人員、施設と製品のための包括的なセキュリティおよび説明責任環境を確保する。 • *セキュリティ目的*: 情報、システムおよびコンポーネントに対するアクセスを、信頼できる個人またはコンピュータに限定する。これらの個人またはコンピュータは、特定可能であること、既知のものであること、適切な権限を持つことが求められる。
測定指標	不正アクセスに利用されるリモートアクセスポイントの割合(%) NIST SP 800-53 管理策: AC-17 (リモートアクセス)
測定指標の種類	**有効性**／効率
計算式	(不正アクセスに利用されたリモートアクセスポイントの数／リモートアクセスポイントの総数) × 100
達成目標	組織が定めた割合を上回らないこと。
実施証拠	1. あなたの組織は、自動化ツールを使って、すべてのリモートアクセスポイントを特定するためのネットワーク図を最新に保っていますか (CM-2)? □ はい □ いいえ 2. ネットワーク上のリモートアクセスポイントはいくつありますか? _____ 3. あなたの組織は、侵入検知システム(IDS)を使って、リモートアクセスポイントを往来するトラフィックを監視していますか (SI-4)? □ はい □ いいえ 4. あなたの組織は、すべてのリモートアクセスポイントに関する監査ログを収集、レビューしていますか (AU-6)? □ はい □ いいえ 5. あなたの組織は、各インシデントを標準化されたカテゴリ別に分類する機能を持つセキュリティインシデントデータベースを備えていますか (IR-5)? □ はい □ いいえ 6. インシデントデータベース、IDS が生成するログと警告、および／またはリモートアクセスポイントに関するログファイルをチェックした結果、報告期間内に不正アクセスを許したアクセスポイントはいくつありますか? _____
頻度	測定指標を収集する頻度: 組織が定めた頻度 (例: 月 1 回) 測定指標を報告する頻度: 組織が定めた頻度 (例: 四半期ごと)
責任を有する関係者	• 情報のオーナー: コンピュータセキュリティインシデント対応チーム (CSIRT) • 情報収集者: システム管理者または情報システムセキュリティ責任者(ISSO) • 情報の受領者: 最高情報責任者(CIO)、上級情報セキュリティ責任者(SAISO) (例: 最高情報セキュリティ責任者[CISO])
データソース	インシデントデータベース、監査ログ、ネットワーク図、IDS が生成するログと警告。
報告書式	すべてのリモートアクセスポイントのうち、不正アクセスに利用されたアクセスポイントの割合(%)を、月別に示す積重ね棒グラフ。

測定指標 4: 意識向上およびトレーニング (AT) (プログラムレベル)

フィールド	データ
測定指標 ID	セキュリティトレーニング測定指標 1 (または組織指定の一意の識別子)
目標	• *戦略目標*: 最新でセキュアなインフラと運用能力を備えることによって、高品質の労働力を確保する。 • *セキュリティ目的*: 組織の人員に対し、適切な訓練を施すことで、自身が担当する情報セキュリティ関連の任務や責任を果たせるようにする。
測定指標	セキュリティに関する責務についている職員のうち、セキュリティトレーニングを受けた者の割合 (%)。 NIST SP 800-53 管理策: AT-3 (セキュリティトレーニング)
測定指標の種類	実施
計算式	(過去 1 年以内にセキュリティトレーニングを受けたセキュリティ担当者の数 ／ セキュリティ担当者の総数) × 100
達成目標	組織が定めた割合に達していること。
実施証拠	1. セキュリティに関する重要な責務は、資格条件によって定義され、ポリシーにて文書化されていますか (AT-1 と PS-2)? □ はい □ いいえ 2. どの職員がセキュリティに関する重要な責務を負うかについて記録をとっていますか(AT-3)? □ はい □ いいえ 3. あなたの組織(または組織の構成部門)の中で、セキュリティに関する重要な責務を負う職員は何人いますか (AT-3)? _____ 4. トレーニング記録は維持されていますか(AT-4)? (トレーニング記録には、特定の職員が受けたトレーニングを記録します。) □ はい □ いいえ 5. セキュリティに関する重要な責務を負う職員のうち、必要なトレーニングを受けた者は何人いますか (AT-4)? 6. すべての職員がトレーニングを受けたわけではない場合、その理由を選択(または記述)してください (AT-4)。 □ 資金不足 □ 時間不足 □ コースがない □ 従業員が登録されていない □ その他(具体的に記述) _____
頻度	測定指標を収集する頻度: 組織が定めた頻度 (例: 四半期ごと) 測定指標を報告する頻度: 組織が定めた頻度 (例: 年 1 回)

フィールド	データ
責任を有する関係者	• 情報のオーナー: 組織が定めた者(例: トレーニングマネージャー) • 情報収集者: 組織が定めた者(例: 情報システムセキュリティ責任者[ISSO]、トレーニングマネージャー) • 情報の受領者: 最高情報責任者(CIO)、情報システムセキュリティ責任者(ISSO)、上級情報セキュリティ責任者(SAISO) (例: 最高情報セキュリティ責任者[CISO])
データソース	トレーニングおよび意識向上の追跡記録。
報告書式	トレーニングを受けたセキュリティ担当者と、受けていない担当者の割合を示す円グラフ。パフォーマンスが目標を下回る場合は、目標に達しなかった原因が示される。

測定指標 5: 監査および責任追跡性(AU) (システムレベル)

フィールド	データ
測定指標 ID	監査記録レビュー測定指標 1 (または組織指定の一意の識別子)
目標	• *戦略目標*: 人員、施設と製品のための包括的なセキュリティおよび説明責任環境を確保する。 • *セキュリティ目的*: システムの監査記録を適切なレベルで作成、保護、維持することで、非合法的な活動、不正な活動、または不適切な活動を監視、分析、調査、報告できるようにする。
測定指標	不適切な活動を確認するために実施する、監査記録レビューおよび分析の平均実施頻度。 NIST SP 800-53 管理策: AU-6 (監査記録の監視、分析および報告)
測定指標の種類	有効性／**効率**
計算式	報告期間における平均実施頻度。
達成目標	組織が定めた頻度に達していること。
実施証拠	各システムについて: 1. システム上でログ取得は有効になっていますか (AU-2)? □ はい □ いいえ 2. あなたの組織は、システム監査ログの内容から「不適切」な活動を特定するための判断基準を明確に定義していますか? □ はい □ いいえ 3.以下の期間内に、不適切な活動を確認するためにレビューを行った監査ログは、いくつありますか (AU-3 and AU-6)? (各システムについて最も近い期間を選択してください。) ここ数日間 _____ ここ 1 週間 _____ ここ 2 週間～1 ヶ月間 _____ ここ 1～ 6 ヶ月 _____ 過去 6 ヶ月以上 _____
頻度	測定指標を収集する頻度: 組織が定めた頻度 (例: 1 日 1 回) 測定指標を報告する頻度: 組織が定めた頻度 (例: 四半期ごと)
責任を有する関係者	• 情報のオーナー: 組織が定めた者(例: システムオーナー) • 情報収集者: 組織が定めた者(例: システム管理者) • 情報の受領者: 最高情報責任者(CIO)、情報システムセキュリティ責任者(ISSO)、上級情報セキュリティ責任者(SAISO) (例: 最高情報セキュリティ責任者[CISO])
データソース	監査ログレポート。
報告書式	実施証拠フィールドに記載の 5 つの期間ごとに、平均実施頻度(またはそれ以上の頻度)でレビューを実施したシステムの数を示す棒グラフ。

測定指標 6: 承認、運用認可、セキュリティ評価(CA) (プログラムレベル)

フィールド	データ
測定指標 ID	C&A を取得するための測定指標 1 (または組織指定の一意の識別子)
目標	• *戦略目標*: 人員、施設と製品のための包括的なセキュリティおよび説明責任環境を確保する。 • *セキュリティ目的*: すべての情報システムが必要に応じて承認され、運用が認可されることを確実にする。
測定指標	新しいシステムのうち、システムの実施に先立ち、運用認可権限者による承認および運用認可(C&A)を取得したシステムの割合(%) NIST SP 800-53 管理策: CA-6 (セキュリティの運用認可)
測定指標の種類	**有効性**／効率
計算式	(システムの実施に先立ち承認および運用認可(C&A)を取得した新システム) ／ (新システムの総数) × 100
達成目標	組織が定めた割合に達していること。
実施証拠	1. あなたの組織(または組織の構成部門)では、システムに関する資産目録を最新かつ完全な状態に維持していますか? □ はい □ いいえ 2. あなたの組織内には正式な C&A プロセスが存在していますか? □ はい □ いいえ 3. 質問 2 に対する回答が「はい」の場合、システム開発プロジェクトを実施する前に C&A を取得することが必須になりますか (CA-1)? □ はい □ いいえ 4. 報告期間内に実施された新システムはいくつありますか? _____ 5. 報告期間内に実施された新システム(質問 4 で回答)のうち、実施前に運用認可を取得したシステムはいくつありますか (CA-6)? _____
頻度	測定指標を収集する頻度: 組織が定めた頻度 (例: 四半期ごと) 測定指標を報告する頻度: 組織が定めた頻度 (例: 年 1 回)
責任を有する関係者	• 情報のオーナー: 組織が定めた者 (例: 運用認可権限者) • 情報収集者: 組織が定めた者 (例: システムオーナー) • 情報の受領者: 最高情報責任者(CIO)、情報システムセキュリティ責任者(ISSO)、上級情報セキュリティ責任者(SAISO) (例: 最高情報セキュリティ責任者[CISO])
データソース	システム資産目録、C&A 記録
報告書式	新しいシステムのうち、C&A のパッケージを提出して運用認可権限者による運用認可を得たシステムと、そうでないシステムの割合を示す円グラフ。

測定指標 7: 構成管理(CM) (プログラムレベル)

フィールド	データ
測定指標 ID	構成管理測定指標 1(または組織指定の一意の識別子)
目標	• *戦略目標*: 電子情報インフラの開発と利用を促進する。 • *セキュリティ目的*: 組織の情報システム(ハードウェア、ソフトウェア、ファームウェア、およびドキュメントを含む)の基本的な構成とその一覧表を、それぞれのシステムの開発ライフサイク全体について設定し、維持する。
測定指標	最新のベースライン構成情報から特定された変更点のうち、事前に承認を得てから変更されたものの割合(%)。 NIST SP 800-53 管理策– CM-2 (ベースライン構成)、CM-3 (構成変更管理)
測定指標の種類	実施
計算式	(自動スキャンによって発見された変更点のうち、事前に承認を得てから変更されたものの数 ／ 自動スキャンによって発見された変更点の総数) × 100
達成目標	組織が定めた割合に達していること。
実施証拠	1. あなたの組織は、組織が承認するプロセスを使用して、システムへの構成変更を管理していますか (CM-3)? □ はい □ いいえ 2. あなたの組織は、自動スキャンによって、システムやネットワークに対する構成変更を特定していますか (CM-2 管理強化策 2)? □ はい □ いいえ 3.「はい」と答えた場合、前回の報告期間内に自動スキャンによって発見された構成変更はいくつありますか (CM-3)? _____ 4. 前回の報告期間内に承認を得てから実施された変更管理要件は、いくつありますか (CM-3)? _____
頻度	測定指標を収集する頻度: 組織が定めた頻度 (例: 四半期ごと) 測定指標を報告する頻度: 組織が定めた頻度 (例: 年 1 回)
責任を有する関係者	• 情報のオーナー: 組織が定めた者 (例: 構成管理者) • 情報収集者: 組織が定めた者 (例: 情報システムセキュリティ責任者(ISSO)、システムオーナー、システム管理者) • 情報の受領者: 最高情報責任者(CIO)、情報システムセキュリティ責任者(ISSO)、上級情報セキュリティ責任者(SAISO) (例: 最高情報セキュリティ責任者[CISO])、運用認可権限者[AO]、構成管理委員会(Configuration Control Board)
データソース	システムセキュリティ計画、構成管理データベース、セキュリティツールが生成するログ
報告書式	最新のベースライン構成(資料)に文書化されているもので、承認を得て実施された構成変更と、文書化されていない構成変更の割合を比較するための円グラフ。

測定指標 8: 緊急時対応計画(CP) (プログラムレベル)

フィールド	データ
測定指標 ID	緊急時対応計画テスト測定指標 1 (または組織指定の一意の識別子)
目標	• *戦略目標*: 人員、施設と製品のための包括的なセキュリティおよび説明責任環境を確保する。 • *セキュリティ目的*:緊急時対応、バックアップ処理、災害後のシステム復旧に関する計画を作成、維持し、効果的に実施することによって、緊急事態が発生した場合であっても、重要な情報資源の可用性を確保し、業務を継続できるようにする。
測定指標	緊急時対応計画テストを毎年実施しているシステムの割合 (%) NIST SP 800-53 管理策: CP-4 (緊急時対応計画のテストと実習)
測定指標の種類	**有効性**／効率
計算式	(システム一覧に記載されているシステムのうち、緊急時対応計画テストを毎年実施しているシステムの数 ／ システム一覧に記載されているシステムの数) × 100
達成目標	組織が定めた割合に達していること。
実施証拠	1. システム一覧に記載されているシステムはいくつありますか? _____ 2. それらのシステムのうち、承認された緊急時対応計画を備えているシステムはいくつありますか (CP-2)? _____ 3. 過去 1 年間でテストを実施した緊急時対応計画はいくつありますか (CP-4)? _____
頻度	測定指標を収集する頻度: 組織が定めた頻度 (例: 年 1 回) 測定指標を報告する頻度: 組織が定めた頻度 (例: 年 1 回)
責任を有する関係者	• 情報のオーナー: 組織が定めた者 (例: 緊急時対応計画管理者) • 情報収集者: 組織が定めた者 (例: システムオーナー、システム管理者) • 情報の受領者: 最高情報責任者(CIO)、情報システムセキュリティ責任者(ISSO)、上級情報セキュリティ責任者(SAISO) (例: 最高情報セキュリティ責任者[CISO])
データソース	緊急時対応計画テストの結果
報告書式	緊急時対応計画テストを毎年実施しているシステムと、そうでないシステムの割合を比較するための円グラフ。

測定指標 9: 識別および認証(IA) (システムレベル)

フィールド	データ
測定指標 ID	ユーザカウント測定指標 1 (または組織指定の一意の識別子)
目標	• *戦略目標*: 人員、施設と製品のための包括的なセキュリティおよび説明責任環境を確保する。 • *セキュリティ目的*: 情報セキュリティポリシーに従ってすべてのシステムユーザを識別し、認証する。
測定指標	共有アカウントへのアクセスを許可されているユーザの割合(%) NIST SP 800-53 管理策– AC-2 (アカウント管理)、AC-3(アクセス制御の実施)、および IA-2(ユーザ識別および認証)
測定指標の種類	**有効性**／効率
計算式	(共有アカウントへのアクセスを許可されているユーザの数 ／ ユーザの総数) × 100
達成目標	組織が定めた割合を上回らないこと。
実施証拠	1. そのシステムへのアクセスを許可されているユーザは何人いますか (IA-2)? _____ 2. それらユーザのうち、共有アカウントへのアクセスを許可されているユーザは何人いますか (AC-2)? _____
頻度	測定指標を収集する頻度: 組織が定めた頻度 (例: 月 1 回) 測定指標を報告する頻度: 組織が定めた頻度 (例: 月 1 回)
責任を有する関係者	• 情報のオーナー: 組織が定めた者 (例: システムオーナー、システム管理者) • 情報収集者: 組織が定めた者 (例: システム管理者) • 情報の受領者: 最高情報責任者(CIO)、情報システムセキュリティ責任者(ISSO)、上級情報セキュリティ責任者(SAISO) (例: 最高情報セキュリティ責任者[CISO])
データソース	構成管理データベース、アクセス制御リスト、システムが生成したユーザ ID リスト
報告書式	共有アカウントへのアクセスを許可されているユーザと、そうでないユーザの割合を比較するための円グラフ。

測定指標 10: インシデント対応(IR) (プログラムレベル とシステムレベル)

フィールド	データ
測定指標 ID	インシデント対応測定指標 1 (または組織指定の一意の識別子)
目標	• *戦略目標*: 組織のプログラムとサービスに関する正確な情報を、タイムリーに利用できるようにする。 • *セキュリティ目的*: インシデントを追跡し文書化したものを、適切な組織の関係者および／または承認権限のある者に報告する
測定指標	報告期間内に報告されたインシデントの割合(%)を、実施証拠に記載のカテゴリ別に算出。 NIST SP 800-53 管理策 – IR-6 (インシデントの報告)
測定指標の種類	**有効性**／効率
計算式	それぞれのカテゴリにおいて (報告期間内に報告されたインシデントの数 ／報告されたインシデントの総数) × 100
達成目標	組織が定めた割合に達していること。
実施証拠	1. その期間内に報告されたインシデントはいくつありますか (IR-6)? カテゴリ 1 – 不正アクセス? _____ カテゴリ 2 – サービス拒否? _____ カテゴリ 3 –悪意のあるコード? _____ カテゴリ 4 – 不正利用? _____ カテゴリ 5 –走査/プローブ/アクセスの試み? _____ カテゴリ 6 – 調査? _____ 2. その報告期間内に報告された個人情報関連インシデントはいくつありますか (IR-6)? _____ 3. 報告されたインシデントのうち、US-CERT が定める報告期間内(カテゴリ別に設定されている)に報告されたインシデントはいくつありますか (IR-6)? カテゴリ 1 – 不正アクセス? _____ カテゴリ 2 – サービス拒否? _____ カテゴリ 3 –悪意のあるコード? _____ カテゴリ 4 – 不正利用? _____ カテゴリ 5 –走査/プローブ/アクセスの試み? _____ カテゴリ 6 – 調査? _____ 4. 報告された個人情報関連インシデントのうち、US-CERT および／または OMB 覚書（Memorandum）が定める報告期間内(カテゴリ別に設定されている)に報告されたインシデントはいくつありますか (IR-6)? _____
頻度	測定指標を収集する頻度: 組織が定めた頻度 (例: 月 1 回) 測定指標を報告する頻度: 組織が定めた頻度 (例: 年 1 回)
責任を有する関係者	• 情報のオーナー: 組織が定めた者 (例: コンピュータセキュリティインシデント対応チーム [CSIRT]) • 情報収集者: 組織が定めた者 (例: システムオーナー、情報システムセキュリティ責任者 [ISSO]、CSIRT) • 情報の受領者: 最高情報責任者(CIO)、上級情報セキュリティ責任者(SAISO) (例: 最高情報セキュリティ責任者[CISO])
データソース	インシデントログ、インシデント追跡データベース（利用できる場合のみ)

フィールド	データ
報告書式	ワンタイム(一度きりの)スナップショット　－　期間内に報告されたインシデントの割合をカテゴリ別に示す積重ね棒グラフ。 傾向 －カテゴリ別の割合と 100 パーセントを示す折れ線グラフ。

測定指標 11: 保守(MA) (システムレベル)

フィールド	データ
測定指標 ID	保守測定指標 1 (または組織指定の一意の識別子)
目標	• *戦略目標*: 電子情報インフラの開発と使用を促進する。 • *セキュリティ目的*: 組織の情報システムに対する定期的かつタイムリーな保守を実施し、情報システムの保守に用いるツール、技術、メカニズムや人員を効果的に管理する。
測定指標	正式なメンテナンススケジュールどおりにメンテナンスを受けるシステムコンポーネントの割合 (%)。 NIST SP 800-53 管理策– MA-2 (定期的な保守) および MA-6 (時宜を得た保守)
測定指標の種類	有効性／**効率**
計算式	(正式なメンテナンススケジュールどおりにメンテナンスを受けるシステムコンポーネントの数 ／システムコンポーネントの総数) × 100
達成目標	組織が定めた割合に達していること。
実施証拠	1. そのシステムには、正式なメンテナンススケジュールが備わっていますか (MA-2)? □ はい □ いいえ 2. そのシステム内のコンポーネントはいくつありますか (CM-8)? _____ 3. それらのコンポーネントのうち、正式なメンテナンススケジュールどおりにメンテナンスを受けたコンポーネントはいくつありますか (MA-6)? _____
頻度	測定指標を収集する頻度: 組織が定めた頻度 (例: 四半期ごと) 測定指標を報告する頻度: 組織が定めた頻度 (例: 年 1 回)
責任を有する関係者	• 情報のオーナー: 組織が定めた者 (例: システムオーナー) • 情報収集者: 組織が定めた者 (例: システム管理者) • 情報の受領者: 最高情報責任者(CIO)、情報システムセキュリティ責任者(ISSO)、上級情報セキュリティ責任者(SAISO) (例: 最高情報セキュリティ責任者[CISO])
データソース	メンテナンススケジュール、メンテナンスログ
報告書式	その期間において、正式なメンテナンススケジュールどおりにメンテナンスを受けたシステムコンポーネントと、そうでないコンポーネントの割合を比較するための円グラフ。

測定指標 12: 記録媒体の保護(MP) (プログラムレベル とシステムレベル)

フィールド	データ
測定指標 ID	媒体上のデータの消去測定指標 1 (または組織指定の一意の識別子)
目標	• *戦略目標*: 人員、施設と製品のための包括的なセキュリティおよび説明責任環境を確保する。 • *セキュリティ目的:*情報システムの媒体を廃棄または再利用する前に、その内容を完全に消去または物理的に破壊する。
測定指標	FIPS199 規定の高位影響システムに対するサニタイズテストに合格したメディアの割合（%） NIST SP 800-53 管理策 – MP-6 (媒体上の記録の抹消と媒体の廃棄)
測定指標の種類	**有効性**／効率
計算式	(サニタイズテストに合格したメディアの数 ／ テストを実施したメディアの総数) × 100
達成目標	組織が定めた割合に達していること。
実施証拠	1. あなたの組織は、メディアを廃棄または再利用する前にメディアの内容を消去する、といったことに関するポリシーを備えていますか (MP-1)? □ はい □ いいえ 2. あなたの組織は、メディアに対して、FIPS199 規定の高位影響システムに対するサニタイズテストを実施していますか (MP-6 管理強化策 2)? □ はい □ いいえ 3. テストに合格したメディアはいくつありますか (MP-6 管理強化策 2)? _____ 4. テストを受けたメディアはいくつありますか (MP-6 管理強化策 2)? _____
頻度	測定指標を収集する頻度: 組織が定めた頻度 (例: 四半期ごと) 測定指標を報告する頻度: 組織が定めた頻度 (例: 年 1 回)
責任を有する関係者	• 情報のオーナー: 組織が定めた者 (例: 施設セキュリティ責任者) • 情報収集者: 組織が定めた者 (例: システムオーナー、情報システムセキュリティ責任者 (ISSO]) • 情報の受領者: 最高情報責任者(CIO)、上級情報セキュリティ責任者(SAISO) (例: 最高情報セキュリティ責任者[CISO])
データソース	サニタイズテスト結果
報告書式	特定の期間において、サニタイズテストに合格したメディアと、そうでないメディアの割合(%)を比較するための円グラフ。

測定指標 13: 物理的および環境的な保護(PE) (プログラムレベル)

フィールド	データ
測定指標 ID	物理的セキュリティーインシデント測定指標 1 (または組織指定の一意の識別子)
目標	• *戦略目標*: 人員、施設と製品のための包括的なセキュリティおよび説明責任環境を確保する。 • *セキュリティ目的*: 物理的保護メカニズムと情報セキュリティ保護メカニズムを統合することで、組織の情報資源を適切に保護する。
測定指標	物理的セキュリティインシデントのうち、情報システムを設置している施設に対する未許可の入場を許してしまったインシデントの割合(%) NIST SP 800-53 管理策– PE-6 (物理的アクセスの監視)
測定指標の種類	**有効性**／効率
計算式	(物理的セキュリティインシデントのうち、情報システムを設置している施設への無断進入を許してしまったインシデントの数 ／物理的セキュリティインシデントの総数) × 100
達成目標	組織が定めた割合を上回らないこと。
実施証拠	1. その期間内に起きた物理的セキュリティインシデントはいくつありますか (PE-6)? _____ 2. それらのインシデントのうち、情報システムを設置している施設への無断進入を許してしまったインシデントはいくつありますか (PE-6)? _____
頻度	測定指標を収集する頻度: 組織が定めた頻度 (例: 四半期ごと) 測定指標を報告する頻度: 組織が定めた頻度 (例: 四半期ごと)
責任を有する関係者	• 情報のオーナー: 組織が定めた者 (例: 物理的セキュリティ担当者) • 情報収集者: 組織が定めた者 (例: コンピュータセキュリティインシデント対応チーム [CSIRT]) • 情報の受領者: 最高情報責任者(CIO)、情報システムセキュリティ責任者(ISSO)、上級情報セキュリティ責任者(SAISO) (例: 最高情報セキュリティ責任者[CISO])
データソース	物理的セキュリティインシデントレポート、物理アクセス制御ログ
報告書式	物理的セキュリティインシデントのうち、情報システムを設置している施設への無断進入を許してしまったインシデントの割合(%)を示す円グラフ。

測定指標 14: 計画(PL) (プログラムレベル とシステムレベル)

フィールド	データ
測定指標 ID	計画測定指標 1 (または組織指定の一意の識別子)
目標	• *戦略目標*: 人員、施設と製品のための包括的なセキュリティおよび説明責任環境を確保する。 • *セキュリティ目的*: セキュリティ計画を作成、文書化し、定期的な更新を行い、計画を実施する。セキュリティ計画には、組織の情報システムに対する既存または計画中のセキュリティ管理策と、情報システムにアクセスする個人の行動規範を記載する。
測定指標	システムへのアクセスに関して、行動規範を読んで理解したことが署名によって示された場合のみ、アクセスを許可している職員の割合(%)。 NIST SP 800-53 管理策– PL-4 (行動規則) および AC-2 (アカウント管理)
測定指標の種類	実施
計算式	(行動規範の同意書に署名後に、システムへのアクセスを許可されたユーザの数 ／システムにアクセスできるユーザの総数) × 100
達成目標	組織が定めた割合に達していること。
実施証拠	1. システムにアクセスできるユーザは何人いますか (AC-2)? _____ 2. それらのユーザのうち、行動規範の同意書に署名したユーザは何人いますか (PL-4)? _____ 3. 同意書に署名後に、はじめてシステムへのアクセスを許可されたユーザは何人いますか? _____
頻度	測定指標を収集する頻度: 組織が定めた頻度 (例: 四半期ごと) 測定指標を報告する頻度: 組織が定めた頻度 (例: 年 1 回)
責任を有する関係者	• 情報のオーナー: 組織が定めた者 (例: システムオーナー、情報システムセキュリティ責任者[ISSO]) • 情報収集者: 組織が定めた者 (例: システム管理者、システムオーナー) • 情報の受領者: 最高情報責任者(CIO)、情報システムセキュリティ責任者(ISSO)、上級情報セキュリティ責任者(SAISO) (例: 最高情報セキュリティ責任者[CISO])
データソース	行動規範に関するレコードを保持しているリポジトリ。
報告書式	行動規範の同意書に署名後にシステムへのアクセスを許可されたユーザと、署名しなくてもシステムにアクセスできたユーザの割合(%)を比較するための円グラフ。

測定指標 15: 人的セキュリティ (PS) (プログラムレベル とシステムレベル)

フィールド	データ
測定指標 ID	人的セキュリティ 検査測定指標 1 (または組織指定の一意の識別子)
目標	• *戦略目標*: 人員、施設と製品のための包括的なセキュリティおよび説明責任環境を確保する。 • *セキュリティ目的*: 組織内で責任のある地位を与えられている個人が、信頼のおける人物であり、その地位について設定されたセキュリティ基準を満たしていることを確実にする。
測定指標	審査を受けた後に、組織の情報と情報システムへのアクセスを許可されたユーザの割合（%） NIST SP 800-53 管理策– AC-2 (アカウント管理) および PS-3 (要員に対する審査)
測定指標の種類	実施
計算式	(審査を受けたユーザの数 ／ システムにアクセスできるユーザの総数) × 100
達成目標	組織が定めた割合に達していること。
実施証拠	1. 組織の情報と情報システムへのアクセスを許可されたユーザは何人いますか (AC-2)? _____ 2. それらのユーザのうち、審査を受けたユーザは何人いますか (PS-3)? _____
頻度	測定指標を収集する頻度: 組織が定めた頻度 (例: 四半期ごと) 測定指標を報告する頻度: 組織が定めた頻度 (例: 年 1 回)
責任を有する関係者	• 情報のオーナー: 組織が定めた者 (例: 人事担当者) • 情報収集者: 組織が定めた者 (例: システム管理者、システムオーナー, 情報システムセキュリティ責任者[ISSO]) • 情報の受領者: 最高情報責任者(CIO)、情報システムセキュリティ責任者(ISSO)、上級情報セキュリティ責任者(SAISO) (例: 最高情報セキュリティ責任者[CISO])
データソース	クリアランスレコード、アクセス制御リスト
報告書式	すべてのユーザのうち、審査を受けたユーザの割合(%)を示す円グラフ。

測定指標 16: リスクアセスメント (RA) (システムレベル)

フィールド	データ
測定指標 ID	リスクアセスメント脆弱性測定指標 1 (または組織指定の一意の識別子)
目標	• *戦略目標*: 人員、施設と製品のための包括的なセキュリティおよび説明責任環境を確保する。 • *セキュリティ目的*: 情報システムの運用によって生じる、組織の業務(ミッション、機能、イメージおよび評判を含む)や資産、および個人へのリスクを、定期的に評価する。
測定指標	組織指定の期間内に軽減された脆弱性の割合(%) NIST SP 800-53 管理策– RA-5 (脆弱性のスキャン(走査)) および CA-5(行動計画とマイルストーン(PoA&M))
測定指標の種類	有効性／**効率**
計算式	(PoA&M のスケジュールどおりに軽減された脆弱性の数 ／PoA&M に文書化されている脆弱性(脆弱性走査によって発見されたもの)の総数) × 100
達成目標	組織が定めた割合に達していること。
実施証拠	1. あなたの組織は、脆弱性走査を定期的に実施していますか (RA-5)? □ はい □ いいえ 2. 脆弱性走査は、どれくらいの周期で実施していますか? □ 週 1 回 □ 月 1 回 □ 四半期ごと □ その他_____ 3. あなたの組織の POA&M 手順では、脆弱性走査によって発見された脆弱性を、適切なシステム POA&M に文書化することを義務づけていますか (CA-5)? □ はい □ いいえ 4. 脆弱性走査によって発見された脆弱性のうち、適切な POA&M に文書化された脆弱性はいくつありますか (CA-5)? _____ 5. 文書化された脆弱性のうち、POA&M のスケジュールどおりに軽減された脆弱性はいくつありますか (CA-5)? _____
頻度	測定指標を収集する頻度: 組織が定めた頻度 (例: 月 1 回) 測定指標を報告する頻度: 組織が定めた頻度 (例: 月 1 回)
責任を有する関係者	• 情報のオーナー: 組織が定めた者 (例: システムオーナー、情報システムセキュリティ責任者[ISSO]) • 情報収集者: 組織が定めた者 (例: システム管理者、システムオーナー、情報システムセキュリティ責任者[ISSO]) • 情報の受領者: 最高情報責任者(CIO)、情報システムセキュリティ責任者(ISSO)、上級情報セキュリティ責任者(SAISO) (例: 最高情報セキュリティ責任者[CISO])
データソース	POA&M、脆弱性走査報告

フィールド	データ
報告書式	スケジュールどおりに軽減された脆弱性と、そうでない脆弱性の割合を比較するための円グラフ。

測定指標 17: システムおよびサービスの調達(SA) (プログラムレベル とシステムレベル)

フィールド	データ
測定指標 ID	サービスの調達契約測定指標 1 (または組織指定の一意の識別子)
目標	• *戦略目標:* 電子情報インフラの開発と利用を促進する。 • *セキュリティ目的:* 組織が外部委託する際の情報、アプリケーションおよび／またはサービスを保護するために、外注先のプロバイダが適切なセキュリティ対策を行うことを確実にする。
測定指標	セキュリティ要件や仕様を含む、システムおよびサービス調達契約の割合（%） NIST SP 800-53 管理策 – SA-4 (調達)
測定指標の種類	実施
計算式	(セキュリティ要件や仕様を含む、システムおよびサービス調達契約の数 ／システムおよびサービス調達契約の総数) × 100
達成目標	組織が定めた割合に達していること。
実施証拠	1. 組織が現在抱えているサービス調達契約は、いくつありますか? _____ 2. それらの契約のうち、セキュリティ要件や仕様を含む契約はいくつありますか (SA-4)? _____
頻度	測定指標を収集する頻度: 組織が定めた頻度 (例: 四半期ごと) 測定指標を報告する頻度: 組織が定めた頻度 (例: 年 1 回)
責任を有する関係者	• 情報のオーナー: 組織が定めた者 (例: 契約責任者) • 情報収集者: 組織が定めた者 (例: 契約責任者の技術代表者、システムオーナー) • 情報の受領者: 契約責任者の技術代表者、システムオーナー、調達責任者、最高情報責任者(CIO)、情報システムセキュリティ責任者(ISSO)、上級情報セキュリティ責任者(SAISO) (例: 最高情報セキュリティ責任者[CISO])
データソース	サービス調達契約
報告書式	セキュリティ要件や仕様を含むシステムおよびサービス調達契約と、そうでない契約の割合を比較するための円グラフ。

測定指標 18: システムおよび通信の保護(SC) (プログラムレベル)

フィールド	データ
測定指標 ID	システムおよび通信の保護測定指標 1 (または組織指定の一意の識別子)
目標	• *戦略目標*: 電子情報インフラの開発と利用を促進する。 • *セキュリティ目的*:電子情報インフラを適切に保護するために、十分な資源を割り当てる。
測定指標	(承認されたオペレーションモードで動作する)FIPS 140-2 認定暗号化モジュール(以下、FIPS 140-2 認定モジュールと称す)を、すべての暗号処理に使用しているモバイルコンピュータとデバイスの割合(%)。 NIST SP 800-53 管理策 – SC-13 (暗号化の利用)
測定指標の種類	実施
計算式	(すべての暗号処理に FIPS 140-2 認定モジュールを使用しているモバイルコンピュータとデバイスの数 ／モバイルコンピュータとデバイスの総数) × 100
達成目標	組織が定めた割合に達していること。
実施証拠	1. 組織において使用されているモバイルコンピュータとデバイスはいくつありますか (CM-8)? _____ 2. それらのモバイルコンピュータとデバイスのうち、暗号技術を使用しているものは、いくつありますか (CM-8)? _____ a. FIPS 140-2 認定モジュールを採用しているモバイルコンピュータとデバイスはいくつありますか (SC-13)? _____ b. それらのモバイルコンピュータとデバイスのうち、すべての暗号処理に FIPS 140-2 認定モジュールを使用しているモバイルコンピュータとデバイスはいくつありますか (SC-13)? _____ 3. 暗号技術の実装を免除されているモバイルコンピュータとデバイスはいくつありますか (CM-8)? _____
頻度	測定指標を収集する頻度: 組織が定めた頻度 (例: 四半期ごと) 測定指標を報告する頻度: 組織が定めた頻度 (例: 年 1 回)
責任を有する関係者	• 情報のオーナー: 組織が定めた者 (例: システムオーナー、情報システムセキュリティ責任者[ISSO]) • 情報収集者: 組織が定めた者 (例: システム管理者、システムオーナー、情報システムセキュリティ責任者[ISSO]) • 情報の受領者: 最高情報責任者(CIO)、情報システムセキュリティ責任者(ISSO)、上級情報セキュリティ責任者(SAISO) (例: 最高情報セキュリティ責任者[CISO])
データソース	システムセキュリティ計画
報告書式	すべてのモバイルコンピュータとデバイスのうち、すべての暗号処理に FIPS 140-2 認定モジュールを使用しているモバイルコンピュータとデバイスの割合(%)を示す円グラフ。

測定指標 19: システムおよび情報の完全性(SI) (プログラムレベル とシステムレベル)

フィールド	データ
測定指標 ID	システムおよび情報の完全性 1 (または組織指定の一意の識別子)
目標	• *戦略目標*: 電子情報インフラの開発と利用を促進する。 • *セキュリティ目的*: 組織の情報システムの適切な箇所に悪意のあるコードからの保護策を備えること。また、情報システムのセキュリティ警告やアドバイザリを監視し、それに対応する適切な活動を行うこと。
測定指標	オペレーティングシステムの脆弱性のうち、パッチが適用されたもの、または、パッチが適用できればリスクが軽減できたと考えられるものの割合(%)。 NIST SP 800-53 管理策– SI-2 (欠陥の修正)
測定指標の種類	実施、**有効性**／効率
計算式	警告やアドバイザリ、および脆弱性走査によって特定された脆弱性のうち、パッチが適用された(または、パッチが適用可能でないと判断された／パッチの適用やその他の処置が免除された)脆弱性の数 ／ 警告やアドバイザリ、および脆弱性走査によって特定された脆弱性の総数) × 100
達成目標	組織が定めた割合に達していること。
実施証拠	1. あなたの組織は、警告やアドバイザリを組織内に配布していますか (SI-5)? □ はい □ いいえ 2. それらの警告やアドバイザリを分析した結果、特定された脆弱性はいくつありますか (SI-5)? _____ 3. 脆弱性走査によって特定された脆弱性はいくつありますか (RA-5)? _____ 4. 特定された脆弱性のうち、パッチが適用された(または、なんらかの処置が講じられた) 脆弱性はいくつありますか (SI-2)? _____ 5. パッチが適用可能でないと判断された脆弱性はいくつありますか (SI-2)? _____ 6. パッチを適用する(または、なんらかの処置を講じる)ことによって軽減できない脆弱性であるがゆえに、パッチの適用やその他の処置が免除された脆弱性はいくつありますか? _____
頻度	測定指標を収集する頻度: 組織が定めた頻度 (例: 週 1 回) 測定指標を報告する頻度: 組織が定めた頻度 (例: 月 1 回)
責任を有する関係者	• 情報のオーナー: 組織が定めた者 (例: コンピュータセキュリティインシデント対応チーム [CSIRT]) • 情報収集者: 組織が定めた者 (例: 情報システムセキュリティ責任者[ISSO]、システムオーナー) • 情報の受領者: 最高情報責任者(CIO)、情報システムセキュリティ責任者(ISSO)、上級情報セキュリティ責任者(SAISO) (例: 最高情報セキュリティ責任者[CISO])
データソース	脆弱性走査、POA&M、警告やアドバイザリのリポジトリ、リスクアセスメント
報告書式	警告やアドバイザリ、および脆弱性走査によって特定された脆弱性の総数と、それらの脆弱性のうち、パッチが適用された(または、パッチが適用可能でないと判断された／パッチの適用やその他の処置が免除された)脆弱性の割合(%)を示す、積重ね棒グラフ。

付録 B: 略語

AC	アクセス制御 (Access Control)
AO	運用認可権限者 (Authorizing Official)
AT	意識向上およびトレーニング (Awareness and Training)
AU	監査および責任追跡性 (Audit and Accountability)
C&A	承認および運用認可 (Certification and Accreditation)
CFO	最高財務責任者 (Chief Financial Officer)
CIO	最高情報責任者 (Chief Information Officer)
CISO	最高情報セキュリティ責任者 (Chief Information Security Officer)
CM	構成管理 (Configuration Management)
COTS	一般商用の (Commercial Off-The-Shelf)
CP	緊急時対応計画 (Contingency Planning)
CPIC	資金計画および投資管理 (Capital Planning and Investment Control)
CSIRT	コンピュータセキュリティインシデント対応チーム(Computer Security Incident Response Team)
FEA	連邦政府のエンタープライズアーキテクチャ (Federal Enterprise Architecture)
FIPS	連邦情報処理基準 (Federal Information Processing Standards)
FISCAM	連邦情報システム管理監査マニュアル (Federal Information System Controls Audit Manual)
FISMA	連邦情報セキュリティマネジメント法 (Federal Information Security Management Act)
FY	会計年度 (Fiscal Year)
GAO	会計検査院 (Government Accountability Office)
GOTS	政府調達向け (Government Off-The-Shelf)
GPEA	政府事務書類制限法(Government Paperwork Elimination Act)
GPRA	政府業績成果法 (Government Performance and Results Act)
ID	身分証明書 (Identification)
IG	監察官 (Inspector General)
IR	インシデント対応 (Incident Response)
ISSEA	国際システムセキュリティ技術協会 (International Systems Security Engineering Association)
ISSO	情報システムセキュリティ責任者 (Information System Security Officer)
ITL	情報技術ラボラトリ (Information Technology Laboratory)
MP	記録媒体の保護 (Media Protection)
NIST	米国国立標準技術研究所 (National Institute of Standards and Technology)
OMB	行政管理予算局 (Office of Management and Budget)
PE	物理的および環境的 (Physical and Environmental)
PL	計画 (Planning)
POA&M	行動計画とマイルストーン (Plan of Action and Milestones)
PRM	業績測定参照モデル (Performance Reference Model)
PS	物理的セキュリティ (Physical Security)
RA	リスクアセスメント (Risk Assessment)
SA	システムおよびサービスの調達 (System and Services Acquisition)
SAISO	上級情報セキュリティ責任者 (Senior Agency Information Security Officer)

SC　　システムおよび通信の保護 (System and Communications Protection)
SDLC　　システム開発ライフサイクル (System Development Life Cycle)
SI　　システムおよび情報の完全性 (System and Information Integrity)
SP　　特別刊行物 (Special Publication)
USC　　合衆国法律集 (United States Code)
US-CERT　　米国のコンピュータ緊急事態対策チーム (United States Computer Emergency Readiness Team)
XML　　拡張マークアップ言語 (Extensible Markup Language)

付録 C: 参考文献

Bartol N., Givans N., *Measuring the "Goodness" of Security*, 2nd International Systems Security Engineering Association (ISSEA) Conference Proceedings, February 2001.

Bartol N., *Information Security Performance Measurement: Live*, 3rd ISSEA Conference Proceedings, March 2002.

Clinger-Cohen Act of 1996 (formerly known as the Information Technology Management Reform Act), February 10, 1996.

E-Government Act, Title III—Federal Information Security Management Act (P.L 107-347), December 2002.

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

Federal Information Processing Standards (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems,* March 2006.

Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 (P.L. 106-398).

General Accounting Office, *Federal Information System Controls Audit Manual (FISCAM),* GAO/AIMD-12.19.6, January 1996.

Government Performance and Results Act of 1993 (PL. 103-62).

National Institute of Standards and Technology Interagency Report 7298, *Glossary of Key Information Security Terms,* April, 2006.

National Institute of Standards and Technology Special Publication 800-18, *Guide for Developing Security Plans and Information Technology Systems,* February 2006.

National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems,* June 2001.

National Institute of Standards and Technology Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems,* May 2004.

National Institute of Standards and Technology Special Publication 800-53, *Recommended Security Controls for Federal Information Systems,* December 2007..

National Institute of Standards and Technology Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems,* June 2008.

National Institute of Standards and Technology Special Publication 800-65, *Integrating Security into the Capital Planning and Investment Control Process,* January 2005.

National Institute of Standards and Technology Special Publication 800-100, *Information Security Handbook: A Guide for Managers*, October 2006.

Office of Management and Budget, "Security of Federal Automated Information Resources," Appendix III to OMB Circular A-130, *Management of Federal Information Resources*, February 8, 1996.

Office of Management and Budget Circular A-11, *Preparation, Submission, and Execution of the Budget, Part 6, Preparation and Submission of Strategic Plans, Annual Performance Plans, and Annual Program Performance Reports* (updated annually).

付録 D: 最低限のセキュリティ要求事項の詳述 [14]

- **アクセス制御（AC: Access Control）:** 組織は、情報システムへのアクセスを、権限を付与されたユーザ、権限を付与されたユーザの業務を代行するプロセス、権限を付与されたデバイス（他の情報システムを含む）、権限を付与されたユーザが実施することを許可されたトランザクション（処理）や機能に限定すべきである。
- **意識向上およびトレーニング（AT: Awareness and Training）:** 組織は、次の 2 項目を確実に行わなければならない。(i)組織の情報システムの管理者やユーザに対し、自らの活動に関連するセキュリティリスクと、組織の情報システムのセキュリティに関して適用される法律、大統領令、指令、方針、基準、指示、規定または手順を認識させること。(ii) 組織の人員に対し、適切な訓練を施すことで、自身が担当する情報セキュリティ関連の任務や責任を果たせるようにすること。
- **監査および責任追跡性（AU: Audit and Accountability）:** 組織は、次の 2 項目を確実に行わなければならない。(i)システムの監査記録を適切なレベルで作成、保護、維持することで、非合法的な活動、不正な活動、または不適切な活動を監視、分析、調査、報告できるようにすること。(ii)それぞれの情報システムのユーザ活動を一意に追跡し、ユーザが自身の活動に対する説明責任を果たすように仕向けること。
- **承認、運用認可、セキュリティ評価（CA: Certification, Accreditation and Security Assessments）:** 組織は、次の 4 項目を確実に行わなければならない。(i)組織の情報システムのセキュリティ管理策を定期的に評価し、それらの管理策の適用が効果的であるかを判断すること。(ii)組織の情報システムの欠陥の修正と脆弱性の軽減または除去のための行動計画を作成し実施すること。(iii)組織の情報システムの運用と、その他の関連情報システムとの接続を承認すること。(iv)情報システムのセキュリティ管理策を継続的に監視することにより、それらの管理策が引き続き有効となることを確実にすること。
- **構成管理（CM: Configuration Management）:** 組織は、次の 2 項目を確実に行わなければならない。(i)組織の情報システム（ハードウェア、ソフトウェア、ファームウェア、およびドキュメントを含む）の基本的な構成とその一覧表を、それぞれのシステムの開発ライフサイク全体について設定し、維持すること。(ii)組織の情報システムに採用されている IT 製品のセキュリティ設定を決定し、(社員に)実施させること。
- **緊急時対応計画（CP: Contingency Planning）:** 組織は、緊急時対応、バックアップ処理、災害後のシステム復旧に関する計画を作成、維持し、効果的に実施することによって、緊急事態が発生した場合であっても、重要な情報資源の可用性を確保し、業務を継続できるようにする。
- **識別および認証（IA: Identification and Authentication）:** 組織は、組織の情報システムへアクセスを許可する前提条件として、情報システムのユーザ、ユーザの業務を代行するプロセス、またはデバイスを識別し、認証しなければならない。
- **インシデント対応(IR: Incident Response):** 組織は、次の 2 項目を確実に行わなければならない。(i)情報システムのインシデント対応運用能力(適切な準備、検知、分析、隔離、回復および

[14] FIPS200『連邦政府の情報および情報システムに対する最低限のセキュリティ要求事項(Minimum Security Requirements for Federal Information and Information Systems)』は、2006 年 3 月に発行された。

ユーザの対応活動を含む)を構築すること。(ii)インシデントを追跡し、文書化したものを、適切な組織の関係者および／または承認権限のある者に報告すること。

- **保守(MA: Maintenance):** 組織は、次の 2 項目を確実に行わなければならない。(i)組織の情報システムに対する定期的かつタイムリーな保守を実施すること。(ii)情報システムの保守に用いるツール、技術、メカニズムや人員を効果的に管理すること。
- **記録媒体の保護(MP: Media Protection):**組織は、次の 3 項目を確実に行わなければならない。(i)紙と電子ベース双方の情報システムの媒体を保護すること。(ii)情報および情報システムの媒体へのアクセスを、権限を付与されたユーザに限定すること。(iii)情報システムの媒体を廃棄または再利用する前に、その内容を完全に消去または物理的に破壊すること。
- **物理的および環境的な保護(PE: Physical and Environmental Protection):**組織は、次の 5 項目を確実に行わなければならない。(i)情報システム、機器および各オペレーション環境への物理的アクセスを、権限を付与された個人に限定すること。(ii)物理的な施設を保護し、情報システムのためのインフラを支援すること。(iii)情報システムの支援ユーティリティを整備すること。(iv)環境的な危険から情報システムを保護すること。(v)情報システムが設置されている施設に対して、適切な環境管理策を実施すること。
- **計画(PL: Planning):** 組織は、セキュリティ計画を作成、文書化し、定期的な更新を行い、計画を実施しなければならない。セキュリティ計画には、組織の情報システムに対する既存または計画中のセキュリティ管理策と、情報システムにアクセスする個人の行動規範を記載すること。
- **人的セキュリティ(PS:Personal Security):**組織は、次の 3 項目を確実に行わなければならない。(i)組織内で責任のある地位を与えられている個人(第三者サービスプロバイダを含む)が、信頼のおける人物であり、その地位について設定されたセキュリティ基準を満たしていること。(ii)解雇または、異動などの人事的措置中に、組織の情報や情報システムが保護されていること。(iii)組織のセキュリティ方針や、手順に順守できなかった人員に対する正式な罰則が採用されていること。
- **リスクアセスメント(RA:Risk Assessment):**組織は、情報システムの運用、および組織の情報の処理、格納または伝送によって生じる組織の業務(ミッション、機能、イメージおよび評判を含む)や資産、および個人へのリスクを、定期的に評価しなければならない。
- **システムおよびサービスの調達(SA: System and Services Acquisition):** 組織は、次の 4 項目を確実に行わなければならない。(i)組織の情報システムを適切に保護するために、十分な資源を割り当てること。(ii)情報セキュリティの検討事項を盛り込んだシステム開発のライフサイクルを採用すること。(iii)ソフトウェアの利用やインストールに関する制限を設けること。(iv)組織が外部委託する際の情報、アプリケーションおよび／またはサービスを保護するために、外注先のプロバイダが適切なセキュリティ対策を行っていること。
- **システムおよび通信の保護(SC: System and Communications Protection):**組織は、次の 2 項目を確実に行わなければならない。(i)情報システムの外部との境界および、主要な内部との境界における組織的な通信(例:組織の情報システムによって発信または、受信した情報)を監視、管理および保護すること。(ii)組織の情報システムにおける効果的な情報セキュリティを促進する構造設計、ソフトウェア開発技術とシステムエンジニアリングの原則を採用すること。
- **システムおよび情報の完全性(SI: System and Information integrity):**組織は、次の 3 項目を確実に行わなければならない。(i)情報や情報システムの欠陥をタイムリーに特定し、報告お

よび訂正すること。（ii）組織の情報システムの適切な箇所に悪意のあるコードからの保護策を備えること。（iii）情報システムのセキュリティ警告やアドバイザリを監視し、それに対応する適切な活動を行うこと。