NIST Special Publication 800-50

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

IT セキュリティの意識向上および トレーニングプログラムの構築

Mark Wilson, Joan Hash

コンピュータ 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 20899-8933

2003 年 10 月

米国商務省 長官

Donald L. Evans

技術管理局 技術担当商務次官

Phillip J. Bond

国立標準技術研究所 所長

Arden L. Bement, Jr.

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

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

コンピュータシステム技術に関する報告書

米国立標準技術研究所（NIST; National Institute of Standards and Technology）のITL（Information Technology Laboratory）は、国家の評価基準および標準化インフラストラクチャの技術的なリーダーシップを提供し、米国の経済および公共福祉を推進する機関である。ITLは、テスト、テスト技法、参照データの開発、概念実装、技術的分析の検証を行い、情報技術の開発と生産的な利用の発展に努めている。ITLの責務には、技術的、物理的、および管理上の標準を開発し、連邦政府のコンピュータシステム内の、取り扱いに注意を要する非機密扱い情報のセキュリティとプライバシーの対費用効果的なガイドラインの作成が含まれる。本特別刊行物800シリーズでは、コンピュータセキュリティにおけるITLの調査、ガイダンス、成果および、産業界、政府機関および教育機関との共同活動についての報告を行う。

米国政府印刷局
WASHINGTON: 2003

政府刊行物管理局、米国政府印刷局監督指導により販売
インターネット: bookstore.gpo.gov — 電話: (202) 512-1800 — Fax: (202) 512-2250
郵送: Stop（私書箱） SSOP, Washington, DC 20402-0001

権限

本文書は、米国立標準技術研究所（NIST; National Institute of Standards and Technology）が、一般法 107-347 および、2002 年の連邦情報セキュリティ管理法（FISMA; Federal Information Security Management Act）に基づくその法的責任を推進するために作成された。

NIST は、すべての政府機関のオペレーションおよび情報資産に適切な情報セキュリティに係る最小限要件を含む標準およびガイドラインを作成する責任を負う。当該標準およびガイドラインは、国家のセキュリティシステムには適用されない。本ガイドラインは、行政管理予算局（OMB; Office of Management and Budget）Circular A-130、第 8b(3)項、『機関の情報システムの保護（Securing Agency Information Systems）』の要件に一致しており、これは A-130 の付録 IV「主要箇所の分析」で分析されているとおりである。補足情報は、A-130、付録 III に記述する。

本ガイドラインは、連邦諸機関による使用を目的として作成されたものである。非政府組織が任意に使用することもでき、著作権によって制約されることはない（ただし帰属性を明らかにすることが望ましい）。

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諸機関に対して義務および拘束力を与えた標準およびガイドラインを否定するものではない。また、本ガイドラインは、商務長官、行政管理予算局長、または他のすべての連邦政府当局者の既存の権威を改変したものまたは、これらに優先するものと解釈してはならない。

本文書では、試行的な手順および概念を的確に記述するために、商業行為を行う特定の事業体、設備、または資料に言及することがある。特定される商業事業体、設備および資料は、NIST による推奨または支持を意味するものではなく、またその事業体、資料、設備が目的に最適であることを示すものでもない。

目次

図

謝辞

国防総省の George Bieber 氏、NIST IT セキュリティ部門の Carolyn Schmidt 女史、国立衛生研究所（NIH; National Institutes of Health）の Jaren Doherty 氏、米国海洋大気庁（NOAA; National Oceanographic and Atmospheric Administration）の Becky Vasvary 女史、内国歳入庁（IRS; Internal Revenue Service）の Richard Stone 氏、および NIST の Pauline Bowen 女史、Richard Kissel 氏、Tanya Brewer-Joneas 女史に、感謝の意を表したい。また、NIST 技術担当編集者の Elizabeth Lennon 女史にも、本文書を編集していただいたことに感謝の意を表する。

厚生省（DHHS; Department of Health and Human Services）インディアン衛生局の Ann L. Brown 女史、DHHS/プログラムサポートセンター（PSC; Program Support Center）の Carolyn O'Connor 女史、および DHHS/PSC の Charles A. Filius 氏の方々にも、特筆すべき貢献をいただいた。

最後に、連邦情報システムセキュリティ教育者協会（FISSEA; Federal Information Systems Security Educators' Association）の執行委員会の各委員である、社会保障局（SSA; Social Security Administration）の Barbara Cuffie 女史、財務省の Patricia Black 女史、および DHHS/PSC の Dara Murray 女史に感謝の意を表する。

要旨

NIST 特別刊行物 800-50『IT セキュリティの意識向上およびトレーニングプログラムの構築（Building An Information Technology Security Awareness and Training Program）』では、効果的な情報技術（IT）セキュリティプログラムの構築に向けたガイダンスを提供し、2002 年の連邦情報セキュリティ管理法（FISMA）と行政管理予算局（OMB）Circular A-130 付録 III で規定される要件の裏付けを行う。強力な IT セキュリティプログラムを実現するには、様々な管理、運用、および技術的コントロールを整備し、IT リソースの保護に役立てるだけではなく、セキュリティポリシー、手順、および技術に関して IT ユーザをトレーニングしなければならない。さらに、組織における IT インフラストラクチャの管理職各位は、割り当てられた責務を効果的に果たすために必要なスキルを身につける必要がある。組織のリソースに対するセキュリティは、技術的な問題であると同時に人的な問題でもあるため、セキュリティトレーニングの領域に目を向けなければ、多大なリスクを組織が抱えることになってしまう。

セキュリティ意識向上およびトレーニングプログラムでは、全員が何らかの役割を担っているが、組織の幹部、最高情報責任者（CIO; Chief Information Officer）、プログラム担当者、および IT セキュリティプログラムマネージャは、組織全体に効果的なプログラムを確立する上で重要な責任を担っている。プログラムの目的と内容は、既存のセキュリティプログラムでの指示と既存の組織のセキュリティポリシーと関連していなければならない。組織の IT セキュリティプログラムポリシーでは、意識向上およびトレーニングプログラムの必要要件を明確に規定する必要がある。

本文書では、IT セキュリティ意識向上およびトレーニングプログラムのライフサイクルにおいて、次の 4 つの重要なステップを確認する。

・ 意識向上およびトレーニングプログラムの設計（第 3 項）:
本ステップでは、組織全体にわたるニーズアセスメントを実施し、トレーニング方針の作成および承認を行う。本方針文書では、組織のセキュリティトレーニングの設定目標の裏付けのための実施タスクを特定する。

・ 意識向上およびトレーニングマテリアルの作成（第 4 項）:
本ステップでは、利用可能なトレーニングの情報資源、目的、内容、およびトレーニングマテリアルの作成に焦点を定め、必要に応じて契約ベースでの支援要請も行われる。

・ プログラムの実施（第 5 項）:
本ステップでは、意識向上およびトレーニングプログラムの効果的な連絡方法および展開を扱う。また、意識向上およびトレーニングマテリアルの配布方法（ウェブ、遠隔教育、ビデオ、現地教育など）も扱う。

・ プログラム実施後の評価（第 6 項）:
本ステップでは、プログラムを最新の状態に保ち、その効果を監視するためのガイダンスを提供する。効果的なフィードバック方法について説明する（アンケート調査、フォーカスグループ、ベンチマークなど）。

本文書では、セキュリティトレーニング機能を管理するために使用する、一般的な 3 つのモデルについても説明している。

・ 中央集約化: すべての責任が中央職権（CIO（最高情報責任者や IT セキュリティプログラムマネージャなど）に属する。

・ 部分的分散化: 中央職権はトレーニングポリシーおよび方策について責任を持ち、プログラム実施の責任について分散化を行う。

・ 完全分散化: 中央職権は方針作成のみ担当し、他のすべての責任は個々の組織の構成要員に委嘱する。

どのタイプのモデルに該当するかは、予算およびその他の情報資源の配分、組織の規模、任務の整合性、組織の地理的分散度などをどう把握し評価するかで異なってくる。

本文書は、NIST 特別刊行物 800-16『情報技術セキュリティトレーニングの要件: 役割および実施ベースモデル（Information Technology Security Training Requirements: A Role- and Performance-Based Model）』の姉妹版である。この 2 つの刊行物は補完関係にある。SP 800-50 が、高度なレベルで、いかに IT セキュリティ意識向上およびトレーニングプログラムを構築するかを記述する一方、SP 800-16 では、低い戦術レベルで、役割ベースの IT セキュリティトレーニングのアプローチについて記述する。

1. 序論

連邦機関および組織は、IT の使用と管理に関わるすべての人員に対して次の点を確保しないかぎり、高度にネットワーク化した今日のシステム環境において、情報の機密性、完全性、および可用性を保護することはできない。

- 組織の任務に関連した各自の役割と責任を把握する。

- 組織の IT セキュリティポリシー、手続きおよび実務を理解する。

- 各自が責任を持つ IT 資源を保護するために必要でかつ利用可能な様々な管理方法、運用、および技術的コントロールについて、最低限必要な知識を身につけている。

システムおよびネットワークの保護の取り組みで人的要素が最も弱い部分であるということは、監査レポート、定期刊行物、および各種カンファレンスでのプレゼンテーションで言及されているので、IT セキュリティ専門家のコミュニティでは広く理解されている。技術を介さない「人的要因」が、妥当かつ適切なレベルのセキュリティを提供するためには重要なのである。人的要素が重要である反面、弱い部分でもあるならば、より慎重にこの「資産」に対して目を向けなければならない。IT セキュリティに関する各自の責任、組織のポリシー、各自に任された IT リソースの適切な使用および保護方法を、確実に理解させるためには、組織に共通の堅固な意識向上およびトレーニングプログラムが最重要になるのである。

1.1 目的

本文書では、組織の IT セキュリティプログラムの一部として、包括的な意識向上およびトレーニングプログラムを構築し管理するためのガイドラインを提供する。本ガイドラインでは、ライフサイクルにおける意識向上およびトレーニングプログラムの設計（第 3 項）、作成（第 4 項）、実施（第 5 項）から、プログラムの実施後の評価（第 6 項）までを提示している。本文書には、いかに IT セキュリティ専門家が意識向上およびトレーニングのニーズを特定し、トレーニング計画を作成し、意識向上およびトレーニングの資金調達に対する組織の賛同を得るかについてのガイダンスが含まれている。また、本文書には、以下についても記述する。

- 意識向上およびトレーニングトピックの選択

- 意識向上およびトレーニングマテリアルの情報源の取得

- 様々な方法を使用した、意識向上およびトレーニングマテリアルの実施

- プログラムの有効性の評価

・ 技術および組織上の優先事項の変更に伴う焦点の更新および改善

1.2 対象とする読者

本ガイダンスは、CIO、IT セキュリティプログラムマネージャ[1]およびスタッフ、管理職（システムおよびアプリケーションの所有者を含む）およびその契約者、組織のトレーニングコーディネーターなど（ただしこれらに限定するものではない）、組織における重要な読者層を対象としている。組織の意識向上およびトレーニングプログラムと IT セキュリティプログラム全体が成功をおさめるどうかは、こうした人々が組織の情報および IT 関連のリソースの保護という共通目標を目指して取り組んでいけるかどうかにかかっている。

1.3 目的

本ガイダンスでは、組織において、IT セキュリティ意識向上およびトレーニングプログラムを設計、作成、インプリメント、および管理するために、IT セキュリティプログラムの一環として行う必要のある作業を取り上げている。本目的には、従業員からスーパバイザおよび職務マネージャ、幹部レベルのマネージャまで、組織の IT ユーザーすべての意識向上およびトレーニングニーズが含まれる。本ガイドラインでは、専門的能力開発（つまり、専門化」）と認証の問題（組織での継続的な承認）についても説明する。ここでは IT セキュリティ教育について言及し定義を行うが、詳しくは取り上げない。

本文書は、NIST 特別刊行物 800-16『情報技術セキュリティトレーニング要件: 役割ベースモデルとパフォーマンスベースモデル（Information Technology Security Training Requirements: A Role- and Performance-Based Model）』の姉妹版である。この 2 つの刊行物は補完関係にある。SP 800-50 では、高度なレベルで、いかに IT セキュリティ意識向上およびトレーニングプログラムの構築するかを記述する一方、SP 800-16 では、低い戦術レベルで、役割ベースの IT セキュリティトレーニングのアプローチについて説明している。

[1] 連邦情報セキュリティ管理法（FISMA）では、この職位は組織の上級情報セキュリティ担当者に相当する。本ガイダンスでは「IT セキュリティプログラムマネージャ」を用いているが、部署または組織の IT セキュリティプログラム担当者の名称は、組織によって様々である。たとえば、「情報システムセキュリティマネージャ」、「情報システムセキュリティ担当者」、「自動データ処理（ADP; Automated Data Processing）セキュリティ担当者」、「自動情報システム（AIS; Automated Information System）セキュリティ担当者」、「情報保障セキュリティ担当者」などの名称を使用している組織もある。どのような名称でも、説明されている職位（役割）は、組織の企業共通の IT セキュリティプログラムに対して責任を担う担当者を説明しているものである。

1.4 ポリシー

OMB Circular A-130、付録 III では、全体のサポートシステムに対するトレーニングをシステムセキュリティ計画の要素、主要アプリケーションに対するトレーニングをアプリケーションセキュリティ計画の要素として扱う。[2] 本 Circular では、システムセキュリティ計画のトレーニング要素に関して、次のように述べている。「システムへのアクセスを許可する前に、すべての個々人は、セキュリティ上の各自責任を果たすために適切なトレーニングを受ける必要がある。このようなトレーニングでは、従業員がシステムのルールに精通できるように、利用可能な技術的支援を受け、技術的なセキュリティ製品および手段を判断できる必要がある。システムのルールに則った行動と定期的なトレーニングは、システムに継続的にアクセスする場合に必要である」。

本 Circular では、アプリケーションセキュリティ計画の一環として、次のように述べている。「個々人にアプリケーションへのアクセスを許可する前に、すべての個々人が、各自の責任とアプリケーションの規則に焦点を当てた専門的なトレーニングを受ける必要がある。本トレーニングは、システムへのアクセスに必要なトレーニングに加えられる場合もある。このようなトレーニングは様々であり、情報取得アプリケーションを使用する一般ユーザーのメンバーに対するアクセス時の通知もあれば、リスクの高いアプリケーションを使用する従業員に対する公式的なトレーニングもある」。

さらに、2002 年の連邦情報セキュリティ管理法（FISMA）では、各組織の幹部に、「これらの要件および関連するポリシー、手順、標準、およびガイドラインに基づいて、組織を支援するのに十分なトレーニングを積んだ人員を確保する責任」を課している。FISMA ではまた、求められる「組織に共通の情報セキュリティプログラム」には、「情報システムのオペレーションおよび、組織の資産をサポートする契約者および他のユーザーを含む人員に対して下記の(i),(ii)を通知するセキュリティ意識向上トレーニング含めること」と述べている。

⑴ 各自の活動に関連した情報セキュリティリスク

⑵ このようなリスクを軽減するように設計された組織のポリシーおよび手順を遵守する各自の責任

組織の IT セキュリティプログラムポリシーには、組織全体にわたる意識向上およびトレーニングプログラム要件に対する明確かつ明瞭な項目が存在しなければならない。意識向上およびトレーニングプログラムのポリシーの中で記されるトピックスには、役割と責任、プログラム方針とプログラム計画の作成、計画されたプログラムの実施、意識向上およびトレーニングプログラムの管理が含まれなければならない。

---

[2] ユーザー、システム/ネットワーク管理者、システムまたはアプリケーションのマネージャにとって必要なセキュリティトレーニングを認知することによって、システムまたはアプリケーションの所有者/マネージャは、セキュリティ関連のニーズに適切な予算組みができる。

1.5 役割と責任

意識向上およびトレーニングの作成と実施を組織に要求するポリシーを理解することは重要だが、誰が IT セキュリティ意識向上およびトレーニングの責任を担うのかを組織が理解することが不可欠である。本項では、IT セキュリティ意識向上およびトレーニングの責任を担う組織内の担当者を特定し説明する。

中には完成度の高い IT セキュリティプログラムを備えている組織もあるが、基本的な要員確保、資金調達、およびサポートの実現に頭を痛めている組織もある。意識向上およびトレーニングプログラムの形式は、組織ごとに大幅に異なる可能性がある。これは、一部には、そのプログラムの完成度による。[3] プログラムの完成度を上げるために役立つひとつの方法は、プログラムの成功を左右する重要な職位についての IT セキュリティ意識向上およびトレーニングの責任を作成し文書化することである。[4]

1.5.1 組織の幹部

組織の幹部は、全従業員に対する効果的なセキュリティ意識向上およびトレーニングの実施が確実に最優先されていることを確認しなければならない。これには、強力な意識向上およびトレーニング内容を伴う、実行可能な IT セキュリティプログラムの実施が含まれる。組織の幹部は次の責務を果たす必要がある。

- CIO（最高情報責任者）を任命する。
- IT セキュリティの責任を割り当てる。
- 組織共通の IT セキュリティプログラムが実施され、十分な資源と予算が割り当てられ、効果的であることを保証する。
- 組織に IT 資源を保護するために十分なトレーニングを受けた人員がいることを保証する。

[3] 組織文化における相違は、IT セキュリティプログラムの配備、資金の調達方法、管理者へのアクセスと管理職によるサポートに表れる。（単独）組織（内）で実施可能な意識向上およびトレーニングプログラムの異なるモデルの例については、第 3.1 項を参照のこと。

[4] IT セキュリティ意識向上およびトレーニングの責任は、組織のポリシー、職位記述書、および適宜、パフォーマンスまたは個別開発計画において文書化することが可能である。

1.5.2 最高情報責任者（CIO）

FISMA では、最高情報責任者（CIO）が、トレーニングを管理し、情報セキュリティに対し重大な責任が伴う人員の監視を課している。CIO は、組織の IT セキュリティプログラムマネージャと協力して、次の責務を果たす必要がある。

・ IT セキュリティ意識向上およびトレーニングプログラムの全体的な方針を策定する。

・ 組織の幹部、上級管理職、システムおよびデータの所有者、およびその他の人員が、セキュリティ意識向上およびトレーニングプログラムの概念と方針を理解していることおよび、プログラムの実施の進捗を知らせる。

・ 組織の IT セキュリティ意識向上およびトレーニングプログラムの資金調達を保証する。

・ セキュリティ上重要な責任を担う組織担当者のトレーニングを保証する。

・ セキュリティ上に関する各自の責任について、全ユーザーが十分にトレーニングされていることを保証する。

・ 効果的な追尾性および報告手段を保証する。

1.5.3 IT セキュリティプログラムマネージャ

IT セキュリティプログラムマネージャは、意識向上およびトレーニングプログラムの戦術レベルでの責任を担う。本役割において、プログラムマネージャは次の責務を果たさなければならない。

・ 作成された意識向上およびトレーニングマテリアルが、対象読者にとって適切であることを保証する。

・ 意識向上およびトレーニングマテリアルを効果的に配し、目的とする対象読者に届けられることを保証する。

・ 意識向上およびトレーニングマテリアルとそのプレゼンテーションに関するフィードバックを提供するための効果的な方法を、ユーザーとマネージャが習得していることを保証する。

・ 意識向上およびトレーニングマテリアルは定期的に見直しを行い、必要に応じて更新することを保証する。

・ 効果的な追尾性および報告手段の設定を支援する。

1.5.4 マネージャ

マネージャは、そのユーザーが設定されたITセキュリティ意識向上およびトレーニング要件を遵守しているかについて責任を負う。マネージャは次の責務を果たす必要がある。

・ CIO と IT セキュリティプログラムマネージャと協力して、共通の責任を達成する。

・ 適宜、システム所有者やデータ所有者の役割を果たす。[5]

・ セキュリティ上重要な責任を持った役割を担うユーザーを対象とした個別開発計画（IDP; Individual Development Plan）の作成を検討する。

・ IT セキュリティプログラムスタッフ、常勤または非常勤のセキュリティ担当者、およびセキュリティ上重要な責任を担うその他の担当者の専門能力開発と認定を促進する。

・ アクセスを許可する前に、システム（一般サポートシステムおよび主要アプリケーション）の全ユーザー（契約者を含む）に、セキュリティ上の各自の責任を果たす方法について、適切なトレーニングを受けていることを確実にする。

・ ユーザー（契約者を含む）に、各自が使用する各システムおよびアプリケーション固有のルールを理解していることを確実にする。

・ 意識向上またはトレーニングあるいはその両方の欠如に帰因するユーザーのエラーおよび手抜かりを軽減するように努める。

[5] 一般的なサポートシステムおよび主要アプリケーションの所有者として従事するマネージャは、全ユーザーが適切なトレーニングを受けていることを確実とすることを含め、そのシステムおよびアプリケーションのITセキュリティ全体に対しての責任を担う。

1.5.5 ユーザー

ユーザーは、どの組織でも最大の対象者であり、故意でないエラーや IT 脆弱性の軽減に貢献できる単独かつ最も重要な集団である。ユーザーには、アクセスを必要とする従業員、契約者、海外または自国の客員研究者、他の組織の人員、訪問者、招待客、およびその他の協力者や提携先が含まれる。ユーザーは次の責務を果たす必要がある。

- 組織のセキュリティポリシーおよび手順を理解し、これを遵守する。
- アクセス権を持つシステムおよびアプリケーションの行動規範について適切なトレーニングを受けている。
- トレーニングニーズを達成するために管理職に協力する。
- ソフトウェア/アプリケーションをセキュリティパッチを適用することで最新の状態を維持する。
- 組織の情報をより有効に保護するために取れる行為を認識する。こういった行動には、パスワードの適切な使用、データのバックアップ、適切なウイルス対策、疑わしいインシデントまたはセキュリティポリシー違反の報告、ソーシャルエンジニアリング攻撃を回避するために設定された規則の遵守、スパムまたはウイルスやワームの蔓延を阻止するための規則の遵守などが含まれるが、これらに限定されるものではない。

2. コンポーネント: 意識向上、トレーニング、教育

効果的な IT セキュリティプログラムが作成できるどうかは、下記の要素にかかっている。

1) 既知のリスクによって緩和されたビジネスニーズが反映される IT セキュリティポリシーを作成する。
2) 組織のセキュリティポリシーや手続きが文書化されている、IT セキュリティに関する責任をユーザーに通知する。
3) プログラムの監視とレビューのためのプロセスを設定する。[6]

セキュリティ意識の向上およびトレーニングは、組織の全ユーザーに焦点を当てる必要がある。管理職は、組織内で適切な IT セキュリティ行動の例を定めなければならない。意識向上プログラムは、様々な方法で設定および実施することが可能で、上級管理職や幹部を含む組織のすべてのユーザーレベルを対象として開始する必要がある。こういった取り組みの有効性が通常、意識向上およびトレーニングプログラムの有効性を判断する。これは、IT セキュリティプログラムにもあてはまる。

意識向上およびトレーニングプログラムは、管理職を含むユーザーが各自の責務の遂行に必要とする情報の伝達手段という点で非常に重要である。IT セキュリティプログラムの場合、これは、企業全体にセキュリティ要件を伝え

る手段となる。

効果的なIT セキュリティ意識向上およびトレーニングプログラムでは、組織のIT システムおよび情報の使用に関する適切な行動規範を明確にしている。本プログラムは、遵守すべきIT セキュリティポリシーおよび手順を伝達する。これは最も重要なことであり、遵守違反に対して課されるあらゆる制裁のもととなるものである。

ユーザーには最初に遵守事項を知らせる必要がある。アカウンタビリティ（責任）は、全面的に通知され、適切なトレーニングを受けた意識の高い従業員によってもたらされなければならない。

この項では、意識向上、トレーニング、および教育の関係、意識向上 - トレーニング - 教育の継続性について説明する。

2.1 継続性

学習は継続である：意識向上から始まり、トレーニングとなり、教育へと発展していくものである。この継続性を図2-1 に示す。この継続性は、NIST 特別出版物800-16『情報技術セキュリティトレーニングの必要要件: 役割ベースモデルとパフォーマンスベースモデル（Information Technology Security Training Requirements: A Role- and Performance-Based Model）』の第2 章で詳しく説明する。
（http://csrc.nist.gov/publications/nistpubs/index.html）[7]

[6] 効果的なIT セキュリティ意識向上およびトレーニングプログラムは、プログラムで使用するマテリアルが、組織のIT セキュリティプログラムポリシーおよびIT 問題別ポリシーに、しっかりと根ざしたものによって成功することが可能となる。ポリシーが明確かつ簡潔に作成されていれば、（ポリシーに基づいた）意識向上およびトレーニングマテリアルは、しっかりとした基礎にもとづき構築されることになる。

[7] ここで述べ、図2－1で示す本継続性は、NIST 特別刊行物 800-16 に記述されるように、意識向上、トレーニングおよび、教育の関連を示すものである。本ガイドラインの目的のために、3 つの学習方法について、明確な境界線が設定されている。

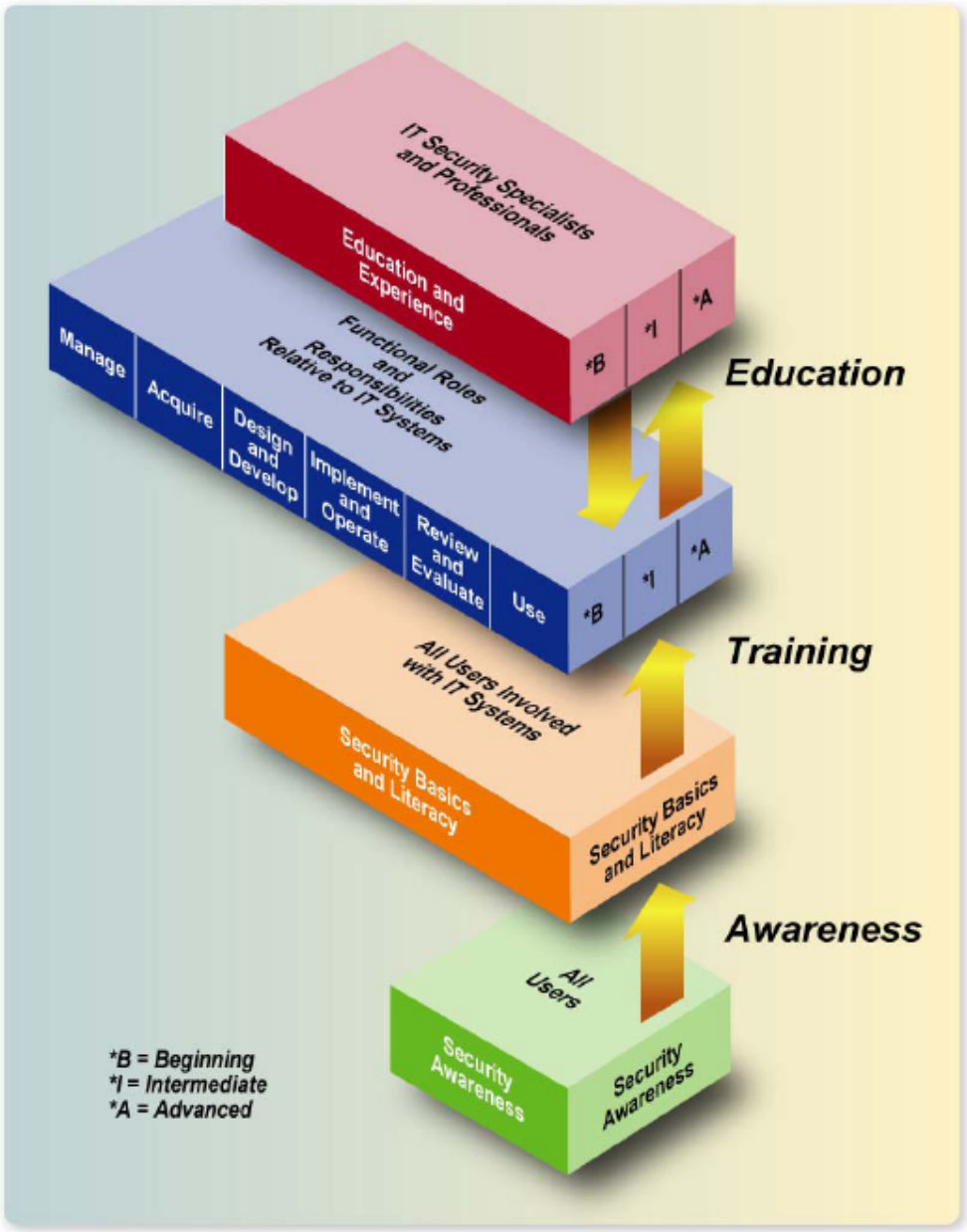

図 2-1: IT セキュリティラーニングの継続性

2.2 意識向上

セキュリティ意識向上への取り組みは、セキュリティに関連する行動の変化や、有効なセキュリティ実践を目的として設計される。意識向上は、NIST 特別刊行物 800-16 で次のように定義されている。

『意識向上はトレーニングではない。意識向上を掲げる目的は、単純にセキュリティへ意識を向けることである。意

識向上の表示は、各自が IT セキュリティの問題を認識し、適切な対応を行うことを意図したものである。

> 意識向上はトレーニングではない。意識向上を掲げる目的は、単純にセキュリティへ意識を向けることである。意識向上は、各自が IT セキュリティの問題を認識し、適切な対応を行うことを意図したものである。

意識向上活動では、学習者は情報の受け手であり、一方、トレーニング環境での学習者は、より積極的な役割を担っている。意識向上は、魅力的なパッケージング手法を使用して、幅広い対象者に働きかけられるかどうかにかかっている。トレーニングは、職務遂行能力を促進する知識や技術を構築する目的を持つより公式的なものである。』

意識向上講座のトピックスの例は（または、意識向上マテリアルの配布）、ウイルス対策である。この問題への対処は単純明快である。ウイルスとは何か、ユーザーのシステムがウイルスに感染した場合どうなるか、システムを保護するためにユーザーは何をすべきか、ウイルスが検出された場合にユーザーは何をすべきかを記述し、単純かつおおまかに扱われる。第 4.1.1 項に、考えうる意識向上トピックスをリストする。

意識向上とトレーニングとの移行段階は、NIST 特別刊行物 800-16 で「セキュリティの基本と教育（リテラシー）」から構成されている。この基本および学習用（リテラシー）マテリアルは、用語、トピックス、および概念を中心に構成したものである。一端、組織がセキュリティの意識向上と警戒意識の全体的なレベルを向上させるプログラムを確立すると、基本およびリテラシーマテリアルに基づいて、より堅固な意識向上プログラムを作成または展開が可能となる。また、本プログラムはトレーニングプログラムに基礎を提供することも可能となる。

2.3 トレーニング

トレーニングは、NIST 特別刊行物 800-16 で次のように定義されている。

『学習継続性におけるトレーニングのレベルでは、IT セキュリティ以外の職能的専門分野（マネジメント、システム設計および開発、調達、監査部門など）の実務者によって、関連性のある必要なセキュリティスキルおよび能力を生み出すように努める。』

トレーニングと意識向上の最も重要な相違点は、トレーニングが特定の機能を実行する人員に対する指導力を模索するのに対し、意識の向上ではある問題または、一連の問題に個々の意識を向けようとしていることである。トレーニングで取得されたスキルは、意識の向上、特にセキュリティの基本および学習（リテラシー）マテリアルの上に構築される。トレーニングカリキュラムは、必ずしもより高度な学習を行う機関からの正式な学位をもたらすものではないが、証書または、学位取得を目的としたカレッジまたは、大学のプログラムのコースにも、トレーニングコースと同様の学習（リテラシー）マテリアル含まれることが多い。

> トレーニングでは、関連性のある必要なセキュリティスキルおよび能力を生み出すように努める。

トレーニングの一例に、システム管理者用のITセキュリティコースがある。本コースには、実施すべき管理コントロール、運用コントロール、および技術的コントロールを詳述に扱う。管理コントロールには、ポリシー、IT セキュリティプログラム管理、リスク管理、およびライフサイクルセキュリティが含まれる。運用コントロールには、人的およびユーザーの問題、緊急時対応計画、インシデントハンドリング、意識向上およびトレーニング、コンピュータサポートおよび運用、物理的および環境的セキュリティ問題が含まれる。技術的コントロールには、識別および認証、論理的アクセスコントロール、監査証跡、および暗号化が含まれる（これらのコントロールの詳細については、NIST 特別刊行物 800-12『コンピュータセキュリティ入門: NIST ハンドブック』（http://csrc.nist.gov/publications/nistpubs/index.html）を参照）。

2.4 教育

教育は、NIST 特別刊行物 800-16 で次のように定義されている。

『教育のレベルは、様々な職能的専門分野のセキュリティスキルおよび能力のすべてを、共通の知識体系に統合し、概念、問題、および原則についての多面的な学習を追加し、洞察能力と予防的対応能力のある IT セキュリティ専門家の育成を目指している。』

教育は、様々な職能的専門分野のセキュリティスキルおよび能力のすべてを、共通の知識体系に統合し、洞察能力と予防的対応能力のある IT セキュリティ専門家の育成を目指している。

教育の一例は、カレッジまたは、大学での学位プログラムである。人々の中には、特定の専門分野において自己のスキル開発または向上のために、1つまたは複数のコースを受講する。これは教育とは相反するトレーニングである。多くのカレッジや大学では認定プログラムを提供しており、本プログラムでは、学生は、関連する専門分野のクラスを、たとえば 2 つ、6 つ、または 8 つ取り、終了時には証書が交付される。しばし、こういった認証プログラムは、学校とソフトウェアまたはハードウェアベンダー共同で実施される。こういったプログラムは、教育よりもトレーニングとしての特徴が顕著である。セキュリティトレーニングの責任を担う担当者は、両方のタイプのプログラムを評価して、特定したニーズをどちらがより効果的に扱うかを判断する。

2.5 専門的能力開発

専門的能力開発は、初心者からセキュリティ専門家に至るユーザーが、それぞれの役割に必要なレベルの知識および能力を確実に習得できるようにすることを目指している。専門的能力開発は、認証によりそのスキルを証明する。このような開発と適切な認証は、「専門化」と呼ぶことが可能である。このような認定テストの予備作業には、通常、所定の知識体系または技術的カリキュラムの学習が含まれ、実際の職務経験で補足されることもある。

IT セキュリティ担当者、IT セキュリティ監査者、IT 請負業者、およびシステム/ネットワーク管理者の中には、IT セ

キュリティ分野での専門化への移行傾向が見られ、発展傾向にある。認証には一般的認定と技術的認定の 2 つのタイプがある。一般的認定は、IT セキュリティ専門職の多くの側面に関する知識基盤の構築に焦点を当てている。技術的認定では、特定のプラットフォーム、オペレーティングシステム、ベンダー製品などに関連した、セキュリティ上の技術的問題に主な焦点を当てている。

IT セキュリティ専門家を採用基準として、IT セキュリティ専門家の認証に焦点をあてる連邦機関、組織がある。その他の組織では、認定を受けたユーザーを保有するために昇給やボーナスを提供し、IT セキュリティ分野のその他のユーザーには認定を取得するように奨励している。

3. 意識向上およびトレーニングプログラムの設計

IT セキュリティ意識向上およびトレーニングプログラムの作成には、プログラムの設計（IT セキュリティ意識向上およびトレーニングプログラム計画の作成を含む）、意識向上およびトレーニングマテリアルの作成、およびプログラムのインプリメント、の 3 つの主要ステップがある。IT セキュリティ意識向上およびトレーニングを少しでも実践すれば、IT セキュリティに関する組織の姿勢と組織内の警戒意識の改善への第一歩となる。この項では、意識向上およびトレーニングプログラムの作成における最初のステップである、プログラムの設計について説明する。

意識向上およびトレーニングプログラムは、組織の任務を念頭に設計しなければならない。意識向上およびトレーニングプログラムが組織のビジネスニーズを裏付け、組織の文化と IT アーキテクチャに関連であることが重要である。最も優秀なプログラムとは、ユーザーが対象であると感じる問題が提示されるプログラムである。

IT セキュリティ意識向上およびトレーニングプログラムの設計は、「既存の指示に整合している意識向上およびトレーニング機会の作成と実施計画とはどのようなものか」という疑問に対する回答となる。[8] プログラムの設計段階では、組織の意識向上およびトレーニングニーズが特定され、組織全体の効果的な意識向上およびトレーニング計画が作成され、組織による賛同が求められ、優先順位[9]が設定される。

この項では次の項目について説明する。

・ 意識向上およびトレーニング活動の構築方法

・ ニーズアセスメントの実施方法（および実施理由）

・ 意識向上およびトレーニング計画の作成方法

・ 優先順位の設定方法

・ 適切な「難易度の設定」（問題の複雑さレベルの設定）方法

・ 意識向上およびトレーニングプログラムの資金調達方法

3.1 組織の意識向上およびトレーニングプログラムの構築

意識向上およびトレーニングプログラムでは、様々な方法で設計、作成、および実施が行うことができる。3つの一般的なアプローチまたはモデルは次のとおりである。

・ モデル 1: ポリシー、方策、および実施の集中化

・ モデル 2: ポリシーおよび方策の集中化、実施の分散化

・ モデル 3: ポリシーの集中化、方策および実施の分散化

意識向上およびトレーニングプログラムの活動を監視するために包含または、構築されるモデルは、次の要因により異なる。

・ 組織の規模と地理的分散状況

・ 定義される組織的役割と責任

・ 予算割り当てと権限

[8] 意識向上およびトレーニング計画には、意識向上およびトレーニングプログラムの責任の達成を目的とする組織方針を反映させなければならない。

[9] 優先順位には、どの意識向上およびトレーニングマテリアルを最初に作成するか、誰が最初にそのマテリアルを受け取るかが含まれる。

モデル 1: 集中化プログラム管理モデル (集中化されたポリシー、方策および、実施)

本モデルでは、組織全体の IT セキュリティの意識向上およびトレーニングプログラムに対する責任と予算は、中央組織に与えられる。すべての指示、方策作成、計画、スケジュール設定は、この「セキュリティ意識向上およびトレーニング」権限 (者) によって調整される。

図 3-1: モデル 1: プログラム管理の集中化

意識向上およびトレーニング方策は中央組織によって作成されるため、方策決定に役立つニーズアセスメントも、中央組織によって行われる。中央組織は、意識向上および、トレーニングマテリアルのみならず、トレーニング計画も作成する。組織全体にマテリアルを行き渡らせる方法は、中央組織が定め、遂行する。一般的に、このような組織では、CIO と IT セキュリティプログラムマネージャの両者が組織的に、この中央権限に位置付けられる。

中央権限と組織ユニットとの伝達は相互間で行われる。中央権限は、IT セキュリティ意識向上およびトレーニングに関する組織のポリシーの指示、プログラム実施の方針、マテリアルおよび、その実施方法を組織ユニットに伝達する。組織ユニットは、中央権限から要求された情報を提供する。たとえば、中央組織は、その責任を果たすために、意識向上セッションの参加者数、特定のトピックスに関してトレーニングを受けた人数、および意識向上およびトレーニングセッションにまだ参加していない人数に関するデータを収集する場合がある。組織ユニットは、意識向上およびトレーニングマテリアルの有効性およびマテリアルの内容を実施する際に使用する方法の適切性に関して、フィードバックを提供することもできる。これによって、中央組織は、マテリアルの手直し、追加、または削除または、実施方法を修正することができる。

こういった集中化モデルは、頻繁に、次のような組織で展開される。

・ 比較的小規模であるか、大部分の IT 機能を高度に構造化し中央管理している組織

・ 必要なリソース、専門知識、ユニットレベルの任務および業務についての知識を、本部レベルで保有している組織

・ 任務と業務上の目標が、すべての構成ユニットにわたり非常に類似している組織

モデル 2: プログラム管理の部分的分散化モデル (集中化されたポリシーおよび方策、分散化されたプログラム実施)

本モデルでは、セキュリティ意識向上およびトレーニングのポリシーと方策は中央組織によって定められるが、プログラムの実施は組織のライン部門管理担当者に委ねられる。意識向上およびトレーニングの予算割り当て、マテリアル作成、およびスケジュール設定は、これらの担当者の責任となる。

意識向上およびトレーニングプログラムの方策は、依然として中央組織が決定するので、ニーズアセスメントは中央組織が行う。ポリシー、方策、および予算は、中央組織から組織単位へ渡される。この方策に基づいて、組織単位は、独自のトレーニング計画を作成する。組織単位は、自身の意識向上およびトレーニングマテリアルを作成し、自組織ユニット内におけるマテリアルの展開方法を決定する。

プログラム管理の集中化モデル (モデル 1) と同様に、このモデルでも、中央組織と組織単位との間の伝達は相互間で行われる。中央組織は、IT セキュリティ意識向上およびトレーニングに関する組織のポリシーの指示、プログラム実施の方策、組織単位ごとの予算を伝達する。また、中央組織は組織単位がトレーニング計画の作成とプログラムのインプリメントに責任があることを助言し、その責任を果たせるように、組織単位にガイダンスまたはトレーニングを提供することもある。

中央組織は各組織単位に対して、定期的な報告、予算支出のレポーティング、組織単位のトレーニング計画の状態、および意識向上およびトレーニングマテリアルの実装に関する進捗レポートを求めることがある。中央組織は、意識向上セッションの参加者数、特定のトピックスに関してトレーニングを受けた人数、および意識向上およびトレーニングセッションにまだ参加していない人数を報告するように、組織単位に要求することもある。組織単位は、中央組織が他の組織単位に効果的なガイダンスを提供できるように、学んだ教訓を記述するように求められる場合もある。

図 3-2: モデル 2 - プログラム管理の部分的分散化

本プログラム管理の部分的分散化モデルは、多くの場合、次のような組織で展開される。

・ 比較的大規模な組織、または、本部（中央）と組織単位の両方のレベルに明確な責任が割り当てられている、分散のかなり進んだ構造を持つ組織

・ 機能が広範な地域に分散している組織

・ 組織単位それぞれに異なった任務があり、組織単位固有のニーズに基づくと意識向上およびトレーニングプログラムが大幅に異なる組織

モデル 3: プログラム管理の完全分散化モデル（集中化されたポリシー、分散化された方策およびプログラム実施）

本モデルでは、中央のセキュリティ意識向上およびトレーニングの組織（CIO/IT セキュリティプログラムマネージャ）は、セキュリティ意識向上およびトレーニング要件に関する広範なポリシーと要求事項を配布するが、プログラム全体を実行する責任は他の組織単位に与える。こういったモデルでは通常、中央組織が統括する分散組織によって

指示が出される。これは通常、中央の CIO および IT セキュリティ担当者に従属するサブシステムの CIO および IT セキュリティプログラムマネージャが設けられることを意味する。

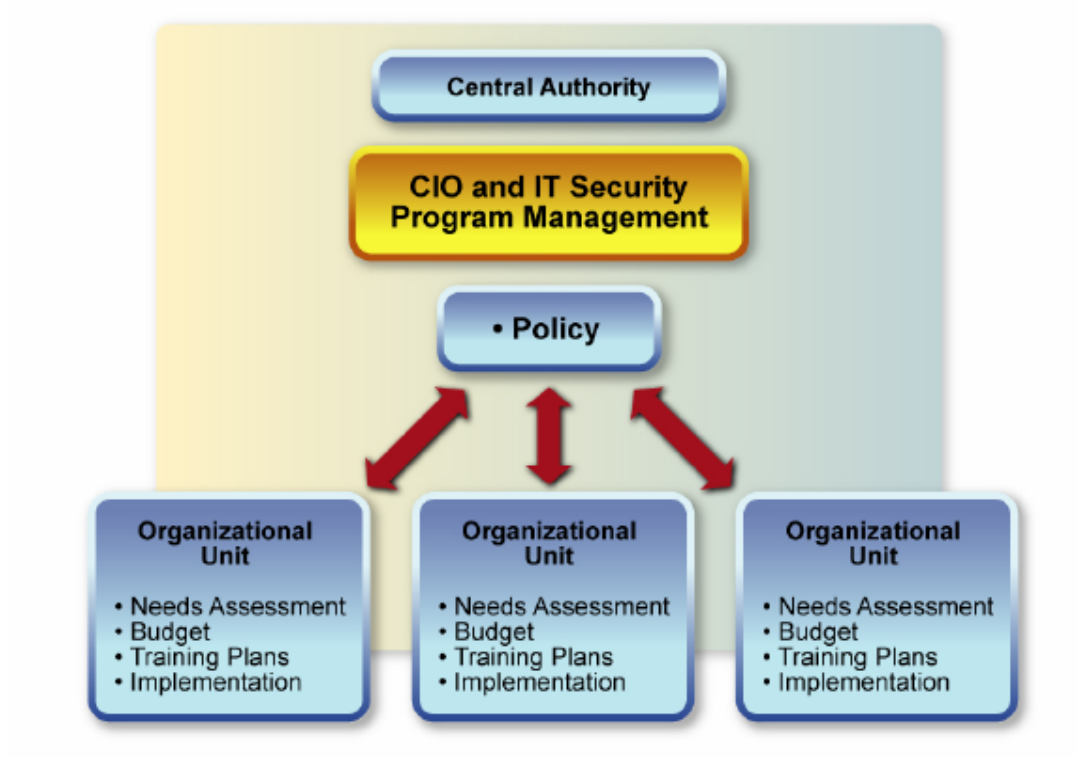

図 3-3: モデル 3: プログラム管理の完全分散化

本モデルでは、組織単位が意識向上およびトレーニングプログラムの方策を決定するので、ニーズ（査定または、必要性査定）アセスメントは各組織単位によって行われる。ポリシーおよび予算は、中央組織から組織単位へ渡される。この方策に基づいて、組織単位は、自身のトレーニング計画を作成する。組織ユニットは、自身の意識向上およびトレーニングマテリアルを作成し、自組織内においてマテリアルを展開する方法を決定する。

プログラム管理の集中化モデル（モデル 1）およびプログラム管理の部分的分散化モデル（モデル 2）と同様に、このモデルでも、中央組織と組織ユニット間における伝達は相互間において行われる。中央組織は、IT セキュリティ意識向上およびトレーニングに関する組織のポリシーの指示と組織単位ごとの予算を通達する。中央組織はまた、組織単位独自のニーズ（査定または、必要性査定）アセスメントの実行、独自の方策の作成、トレーニング計画の作成、およびプログラムの実施に責任があることを、組織ユニットに助言することもある。中央組織は、組織単位が各自の責任を果たせるように、組織単位にガイダンスまたはトレーニングを提供することもできる。

中央組織が、ポリシーおよびプログラム要件を実施するための優れた戦略を持っておらず、組織単位レベルでのパフォーマンスおよび業務上の問題を考慮できない場合、プログラム管理の完全分散化モデルを用いることは、わずかな責任、または責任が全くない状態で、「IT セキュリティプログラムを放棄する」ことになる。

中央組織は、各組織ユニットからの定期的な報告、予算支出のレポーティング、ニーズアセスメントの状態と結果、組織単位が選択した方策、トレーニング計画の状態、意識向上およびトレーニングマテリアルの実装に関する進捗レポートを求めることがある。また、中央組織は、意識向上セッションの参加者数、特定のトピックに関してトレーニングを受けた人数、および意識向上およびトレーニングセッションにまだ参加していない人数を報告するように、組織単位に求めることもある。

このプログラム管理の完全分散モデルは、多くの場合、次のような組織で展開される。

- 比較的大規模な組織
- 一般的な責任は本部（中央）に割り当て、特定の責任は組織単位レベルに割り当てた、非常に分散の進んだ構造を持つ組織
- 機能が広範な地域に分散している組織
- 分離された異なる任務を持つ準自立的な組織単位を持つため、大幅に異なる意識向上およびトレーニングプログラムが必要となる組織

採用するモデルが特定すると、選択した組織のモデルに整合した、ニーズアセスメント実施への取り組み方法を定めなければならない。

3.2 ニーズアセスメントの実施

ニーズアセスメントは、組織の意識向上およびトレーニングのニーズを判断するために使用するプロセスである。ニーズアセスメントの結果は、特定した意識向上およびトレーニングニーズに見合った適切なリソースの割り当てを、管理職に確信させる正当な根拠の提供が可能でる。

ニーズアセスメントの実施では、主要な人員による関与が重要である。最低限、以下の役割は、特別なトレーニングニーズという観点で扱われなければならない。

- 幹部管理職

  組織のリーダーは、セキュリティプログラムの基礎を形成する指示および法律について、十分に理解する必要がある。また、自組織ユニット内のユーザーによる全面的な遵守を確実にする、自らの指導的役割を理解する必要もある。

- セキュリティ要員（セキュリティプログラムマネージャおよびセキュリティ担当者）

  セキュリティ要員はおのおの、自組織の専門分野のコンサルタントとして行為する。したがって、セキュリティポリ

シーと一般に認められている模範事例について、十分に教育を受けていなければならない。

・ システム所有者

所有者は、セキュリティポリシーの広範な理解と、自身の管理するシステムに適用されるセキュリティコントロールおよび要件に関する高度な理解を保有していなければならない。

・ システム管理者および IT サポート要員

これらの要員は、セキュリティプログラムの成功にとって不可欠なサポート業務に関して、高度な権限を与えられているので、効果的なセキュリティの実践方法と実装についての高度な技術的知識を習得する必要がある。

・ 運用マネージャおよびシステムユーザー

これらの要員は、業務の遂行に使用するシステムのセキュリティコントロールおよびふるまいの規則に関する高度なセキュリティ意識向上およびトレーニングが必要である。

組織の様々な情報源は、IT セキュリティ意識向上およびトレーニングニーズを決定するために用いることが可能であり、そういった情報の収集方法も様々である。図 3-4 では、ニーズアセスメントの一環として情報収集の技術を提案する。[10]

[10] ニーズアセスメントのプロセスは、組織の意識向上およびトレーニングプログラムのニーズを特定するために必要とされるプロセスと同様に複雑である。同様に、こうしたニーズを特定する技術は、組織の規模、労働力の複雑さ、任務の類似性または多様性についての知識だけでなく、組織の文化および慣習を理解し、選択しなければならない。たとえば、1 つの任務または類似した任務だけを抱える小規模な組織では、IT セキュリティプログラムのレビューまたは非公式調査やアンケートの結果が、意識向上およびトレーニングプログラムのニーズの特定に有効であることが多い。一方、多種多様なユーザーと任務を抱える大規模な組織では、プログラムニーズの特定のために分析される情報を収集するために、より複雑なアンケートを作成しなければならない。

- 特定されるすべての主要グループおよび組織とのインタビュー
- 組織全体にわたる調査
- 現在の意識向上およびトレーニングマテリアル、トレーニングスケジュール、参加者リストなどの利用可能なリソースマテリアルのレビューとアセスメント（精査および、査定）
- 意識向上およびトレーニングに関連するメトリック（測定基準）の分析（必要な意識向上のセッションまたは体験を終えたユーザーのパーセンテージまたは、その残存数パーセンテージ、セキュリティ上重要な責任を担い、役割特有マテリアルでトレーニングを受けたユーザーのパーセンテージなど）
- システムおよびアプリケーションの所有者と任命されたセキュリティ代表者を特定するための、一般サポートシステムおよび主要アプリケーションのセキュリティ計画のレビュー（精査）
- アクセス権を持つ全ユーザーを判断するための、システムインベントリおよびアプリケーションユーザーID のデータベースのレビュー
- 監督機関（会議での質疑、監査官、内部レビュー/監査、内部コントロールプログラムなど）による所見および／または、推奨の精査または、IT セキュリティプログラムに関するプログラム精査
- 管理者、一般サポートシステムおよび主要アプリケーションの所有者、IT に依存したビジネス機能を保有する他組織のスタッフとの対話およびインタビュー
- 事象（サービス拒否攻撃、Web サイトの改ざん、連続攻撃に用いられるシステムのハイジャック、首尾の良いウイルス攻撃）の分析は、特定グループ要員のトレーニング（または追加のトレーニング）の必要性を示す場合がある。
- 技術またはインフラストラクチャに対する変更が行われた場合のレビュー
- 業界、学界、または政府の刊行物やトレーニング/教育機関によってはじめて特定された傾向の研究。これらの「早期警戒システム」の使用は、まだ問題として捉えていない組織内での課題に対する見識を提供することが可能である。

図 3-4: ニーズアセスメントの一環としての情報収集手段

付録 A には、ニーズアセスメントのインタビューとアンケートの例を記載している （記載されている例には、システム管理者の一般的な職務指向型アンケートの一環として、いくつかの IT セキュリティ関連の質問が含まれている。一般的な職務トレーニング要件がわかっている場合、このアンケートでは、その職務のセキュリティ意識向上およびトレーニングニーズに焦点を当てることができる）。

測定基準は、組織の IT セキュリティ意識向上およびトレーニングニーズの判断を行うために用いることが可能な、重要かつ効果的な手段である。測定基準は、意識向上およびトレーニングの実施レベルと、意識向上およびトレーニングの有効性および効率性を定量化し、意識向上およびトレーニングの取り組みの適切さを分析し、改善できる点を特定することによって、意識向上およびトレーニングプログラムの最終目標と達成目標の実現を監視する。測定基準の論考については、NIST 特別刊行物 800-55『IT システムのセキュリティメトリクスガイド（Security Metrics Guide for Information Technology Systems）』を参照のこと。意識向上およびトレーニングのメトリックの例は、本文書

に付録 B として収録する。

図 3-5 では、ニーズアセスメントの開始時に理解しておくべき、組織特有の重要な問題を図示する。図 3-4 に示す手段は、こういった問題に対する見識および、理解するための情報を提供する。こういった問題から、必要な情報がニーズアセスメントのプロセスに投入されなければならない。これを理解することが、IT セキュリティ意識向上およびトレーニングプログラムの方策と設計の形成の一助となる。[11]

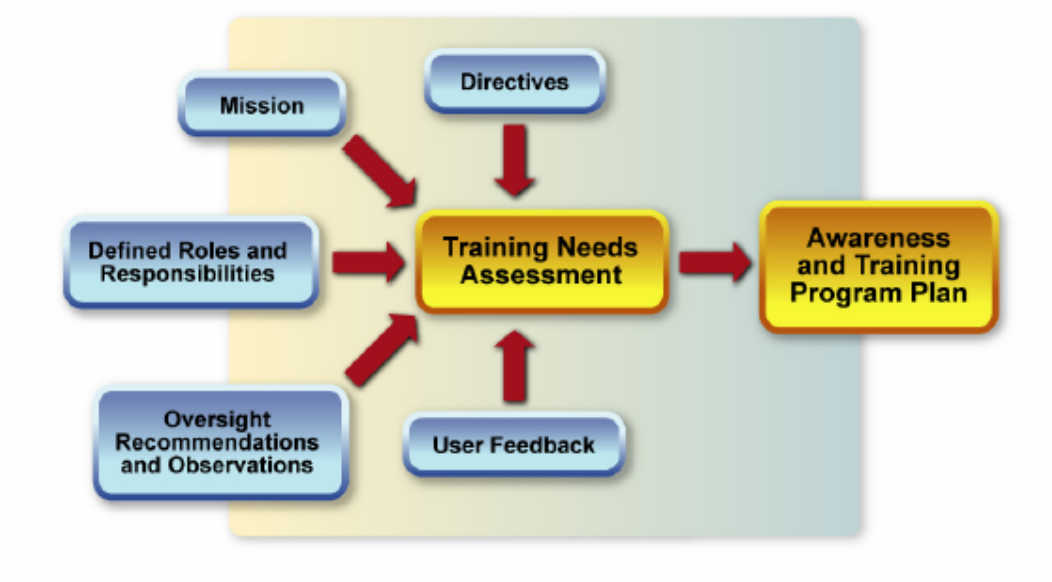

図 3-5: 組織特有の重要な問題の理解

収集した情報の分析は、図 3-6 に示すような主要な疑問に回答することができる。

- どのような意識向上、トレーニングおよび／または、教育が必要なのか（つまり、何が求められているのか）。
- こういったニーズを満たすために、現在どのようなことが行われているのか。
- こういったニーズをいかに扱うかに関し、現在はどのような状態か（つまり、現在の取り組み方により、どの程度効を奏しているか）。
- ニーズと現在行われていることとのギャップはどこにあるか（つまり、どのニーズへの対処がさらに必要か）。
- どのニーズが最も重要か。

図 3-6: ニーズアセスメントの実施における主要な質問への回答

図 3-7 は、意識向上およびトレーニングの要件と組織の現在の取り組みとの関係を示したものである。網掛け部分は、実施する必要のある追加の IT セキュリティ意識向上およびトレーニングを示す。ニーズアセスメントは、こういった追加ニーズ、つまり現在の取り組みと求められる取り組みとのギャップを特定するために役立つ。

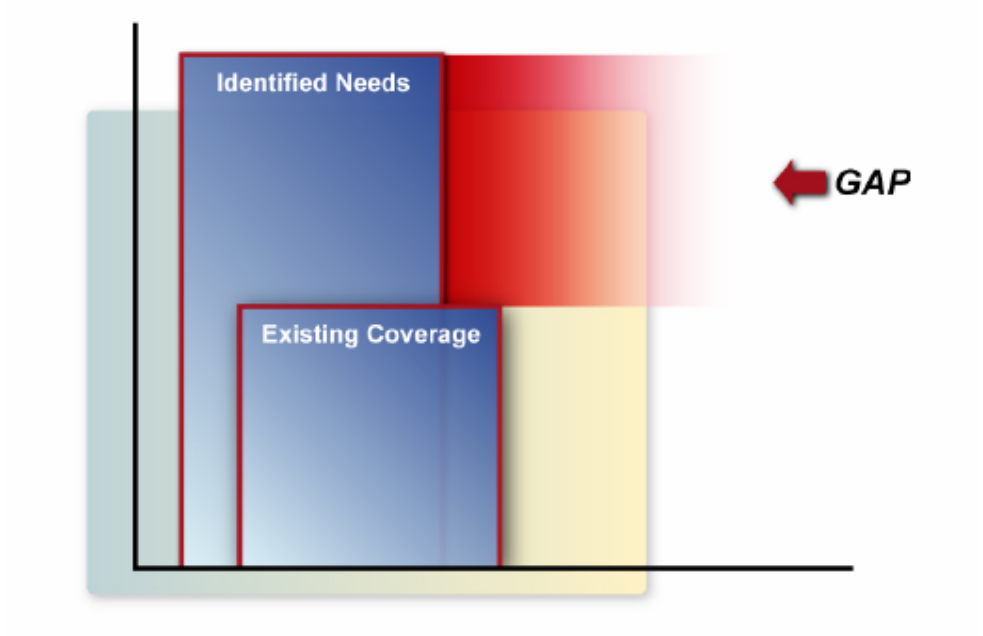

図 3-7: 求められる意識向上およびトレーニング vs. 現在の取り組み

ニーズ（査定または、必要性査定）アセスメントのもう一方の重要な側面は、関連 IT セキュリティ意識向上およびトレーニングプログラム要件である。たとえば、意識向上およびトレーニングマテリアルが、コンピュータベーストレーニング（CBT; Computer-Based Training）テクノロジを用いて提示される場合、既存の環境が新規または拡張した意識向上およびトレーニングプログラムをサポートするかどうかを判断するために、組織の処理プラットフォーム（ローカルエリアネットワーク、ワークステーション、ビデオカード、スピーカーなど）上で、技術アセスメントが行われなければならない。同様に、組織がクラスルームトレーニングを計画している場合、ニーズアセスメントでは、効果的な学習環境のための十分なスペースが確保されているかどうかを確認しなければならない。また、障害が伴い、特別な対応が必要な従業員を含む人的資源の問題があることもある。労働組合の問題でも、以前は組合が扱わなかったものが生じることもある。

ニーズアセスメントがいったん完了すると、意識向上およびトレーニング計画の作成に必要な情報が利用可能になる。本計画では、組織全体を包含し、ニーズアセスメントで特定された優先順位を組み込まれなければならない。

[11] ニーズアセスメントにおいて、扱うべきもう 1 つの問題は、セキュリティ上の重要な責任として特定されている役割である。こういった既存の役割は、現在もセキュリティ上重要な責任を担っているかどうか見直さなければならない。以前にはセキュリティ上わずかな責任を担っていた、または全く担っていなかった他の役割についても見直さなければならない。組織における組織上および技術上の変更は、担っている役割とそのセキュリティ上の責任に影響が及ぶことがある。

3.3 意識向上およびトレーニングの戦略と計画の作成

ニーズ（査定または、必要性査定）アセスメントが完了すると、組織は、IT セキュリティ意識向上およびトレーニングプログラムの作成、実施、および維持方針の作成に取りかかる。本計画は、方針を構成する要素が搭載された作業文書である。当該計画では次の要素を検討しなければならない。

- 意識向上およびトレーニングの遂行を求める既存の国家および地域の政策
- 意識向上およびトレーニングプログラムの目的
- 意識向上およびトレーニングマテリアルを誰が設計、作成、実施、および管理を行うかおよび、適切なユーザーが参加または、適切なマテリアルを閲覧することを保証する組織の担当者の役割と責任
- プログラムの各段階（意識向上、トレーニング、教育、専門的能力開発[認証]など）ごとの達成目標
- プログラムの各段階の対象者
- それぞれの対象者に応じた必須（適用可能な場合は選択）コースまたはマテリアル
- プログラムの各段階の学習目標
- 各セッションまたはコースで扱うトピックス
- プログラムの各段階で用いられる展開方法
- プログラムの各段階での学習の文書化、フィードバック、および証拠 [12]
- プログラムの各段階のマテリアルの評価および更新
- それぞれの対象者へのマテリアル提示の頻度 [13]

付録 C には、意識向上およびトレーニングプログラム計画のテンプレートのサンプルを収録する。

3.4 優先順位の設定

セキュリティ意識向上およびトレーニングの方針と計画が完了したら、実施スケジュールを設定しなければならない。こういった状況が段階ごとに発生する場合（予算の制約やリソースの可用性などのため）、どちらを最初にスケ

ジュールし、どの順番で行うかの判断に用いる要因を決定することが重要である。考慮すべき主な要因は次のとおりである。

マテリアル/リソースの可用性

意識向上およびトレーニングマテリアルと必要なリソースが簡単に利用できる場合、計画の主要項目を早期にスケジュールすることができる。ただし、コースマテリアルを作成する必要がある場合、またはインストラクターを特定しスケジュールを設定しなければならない場合、これらの要件は、集合優先順位として考えなければならない。

役割と組織への影響

組織的役割および、リスクに関し優先順位を付けて扱うことが一般的である。企業全体にわたる指令を取り扱う広範な意識向上の率先項目は、優れたセキュリティの実践規則を迅速に従業員に配布できるため、高い優先順位が与えられる。また、信頼性が高く影響力の大きい職位（組織における高い機密性を持っていると判断れる IT セキュリティプログラムマネージャ、セキュリティ担当者、システム管理者、およびセキュリティ管理者としての職位）に注目して、これらの職位に展開方針での高い優先順位を保証することも一般的である。こういった類の職位は、一般的に、ユーザーが所有するアクセス権のタイプ（および何のシステムにアクセスするか）に批准する。

現在の整合性の状態

これには、意識向上およびトレーニングプログラムにおける重大な格差に注目すること（ギャップ分析など）と、初期の展開に不十分な領域を対象とすることが含まれる。

重要なプロジェクトの従属関係

システムが関与する（新しいオペレーティングシステム、ファイアウォール、仮想プライベートネットワーク[VPN]など）の必要要件を作成するため、セキュリティトレーニングの一部に依存するプロジェクトがある場合、トレーニングスケジュールでは、これらの従属関係を扱うために必要な規定の時間枠内でのトレーニングが行われなければならない。

---

[12] 意識向上およびトレーニング計画のこの要素では、誰がトレーニングを受け、誰がまだトレーニングを必要としているかを組織が追跡する方法、参加者がマテリアルの適切さについてコメントを残すための方法、参加者が意識向上またはトレーニングマテリアルを経験して利益を得られたかどうかを組織が判断する方法を文書化しなければならない。

[13] 最低年に 1 度は、従業員全員が意識向上マテリアルに触れなければならない。年間を通じ様々な方法で配布されたマテリアルを使用し意識向上プログラムを続けることは、非常に効果的であると言えよう。セキュリティ上の重要な責任を担うユーザーグループ（システムおよびネットワーク管理者、マネージャ、セキュリティ担当者など）に対するセキュリティトレーニングは、必要に応じて、継続的な職能トレーニングに組み込まれなければならない。

3.5 難易度の設定

「難易度の設定」は、作成するマテリアルの複雑さに関して設定しなければならない判断を意味する。複雑さは、学習を受ける人員の役割に比例しなければならない。マテリアルは、
1) 対象の参加者の組織内での職位
2) その職位に必要なセキュリティスキルの知識
という 2 つの重要な基準に基づいて作成しなければならない。マテリアルの複雑さは、作成開始前に決定しなければならない。難易度の設定は、意識向上、トレーニング、教育という学習の 3 つのタイプすべてに適用する。

意識向上活動に関して難易度を設定する場合、システムの使用において期待されるふるまいの規則に焦点を当てなければならない。こういった規則は、組織のポリシーから直接引用され、組織の全員に適用される。したがって、この規則は、混同または誤解の余地を残すことなく、十分明確に説明される必要がある。組織の意識向上プログラムの完成に従い、最初のマテリアルがほとんどのユーザーに触れられたならば、この難易度をさらに高く設定することができる。基礎および学習コースを含む難易度設定の引き上げの方法が沢山存在することが NIST 特別刊行物 800-16 の第 3 章のガイダンスに記載されている。難易度の引き上げについては、第 6 項で詳しく説明する。

「バーの設定」は、作成するマテリアルの複雑さに関する判断を行う必要があることを意味している。これは、意識向上、トレーニング、教育という学習の 3 つのタイプすべてに適用される。

正確な難易度の設定は、時にトレーニングマテリアルの作成よりも重要である。トレーニングの最終目標は、適切で必要なスキルと能力を算出するため、ニーズアセスメントによって、IT セキュリティ上重要な責任を担う担当者を特定し、その能力を査定し、トレーニングニーズを特定することが重要である。トレーニングマテリアルは、参加者が各自の職務に関連したセキュリティ上の責任を達成するために必要な、一連のスキルが提供されるように作成しなければならない。IT セキュリティトレーニングマテリアルは、これから訓練を受けようとしている人員（システム管理者、Web または電子メールサーバーの管理者、監査人など）にあわせて、初級レベルで作成することができる。マテリアルは、訓練経験がより豊富でより責任の重い人員にあわせて、中級レベルで作成することもできる。上級用マテリアルは、高度な信頼と、IT セキュリティ責務が伴う職務に従事する「中核組織」に位置する人員または、組織級の問題を扱う専門家のために開発されるものである。NIST 特別刊行物 800-16 の第 4 章では、トレーニングコースの作成者に役立つように、3 つのレベルのそれぞれでの学習目標を含め、これらの 3 つのレベルの複雑さに合わせたトレーニングマテリアル作成のガイダンスを提供している。[14]

[14] 組織は、より高度な、またはより複雑なトレーニングが必要なスタッフに見合った市販（COTS; Commercial Off-the-Shelf）のトレーニングマテリアルを用いることもできる。組織はこの場合でも、役割またはグループごとに学習目標を定め、複雑さのレベルごとにも学習目標を定める必要がある。利用可能な COTS トレーニングマテリアルは、次いで、それぞれの役割に対し何が求められているかを判断するために、組織のニーズに見合っているかどうかの比較がされる。ベンダー提供のトレーニングの問題については、第 4 項で詳細に取り上げる。

教育レベルの学習の場合、カリキュラムがカレッジや大学で作成されるので、難易度の設定はより難しくなることがあるが、短期間に組織固有のニーズに影響されることはあまりない。いったん組織内（通常、IT セキュリティ担当部署内）で教育ニーズが特定されれば、必要な学習を提供するスクールを見出すことができる。組織は、ニーズに見合った認証または学位プログラムを持つ地域の大学を、または通信教育によって同様のプログラムを提供しているスクールの「買い取り」を検討することができる。トレーニングマテリアルの場合と同様に、カレッジまたは大学は、そのカリキュラムが組織の要員のセキュリティニーズに見合っているという理由から選択されなければならない。

3.6 セキュリティ意識向上およびトレーニングプログラムの資金調達

いったん意識向上およびトレーニング方針についての合意がなされ、優先順位が定められたら、資金調達の要件が計画に追加されなければならない。第 3.1 項で説明した実施モデルに基づいて割り当てられた資金調達サポートの範囲を判断しなければならない。組織の CIO は、本件において整合である期待値（期待額）を明確な意思と共に伝えなければならない。資金調達源の判断に用いるアプローチ法は、現在の予算または期待できる予算と他の組織の優先順位に基づき組織が扱わなければならない。セキュリティ意識向上およびトレーニング計画は、合致すべき最小要件の集合として見なされ、これらの必要要件は、予算または契約の観点から見て、サポート可能なものでなければならない。契約上のトレーニング要件は、拘束力のあるドキュメント（了解事項覚書（MOU; Memos of Understanding）、契約書など）で特定しなければならない。資金調達要件を示すために使用するアプローチには、次の項目を含めることがある。

・トレーニングの総予算に占めるパーセンテージ

・役割別のユーザー1 人あたりの割り当て（たとえば、主要セキュリティ要員およびシステム管理者のトレーニングは、組織においてセキュリティ専門職務を遂行していない人員の一般的なセキュリティトレーニングよりもコストがかかる）

・「IT 総予算に占めるパーセンテージ」 または 「プログラムの実施総コストに基づいた、コンポーネント別の明確な割り当て額」

セキュリティ意識向上およびトレーニング構想が、組織の他の構想よりも優先順位が低いとみなされる場合、セキュリティ意識向上およびトレーニング計画の実施の問題が生じることがある。競合する優先順位を評価し、既存のセキュリティトレーニング要件に準ずる組織の能力に影響を及ぼすと思われる資金調達におけるあらゆる不足を対処する方策を作成する責任は CIO にある。このことは、予算内での意識向上およびトレーニング方針を調整したり、追加の資金調達を要請したり、現在のリソースの再割り当ての指図を意味する。また、資金調達が可能になるとした所定の期間が経過した時点で、段階的に実施計画を実施することも意味する。

4. 意識向上およびトレーニング資料の作成

意識向上およびトレーニングプログラムの設計がいったん終了すると、サポートマテリアルの作成が可能になる。マテリアルは、次の点を考慮して作成しなければならない。[15]

「どのようなふるまいを強化すべきか？」(意識向上)

「対象者に対して、どのような単一または複数のスキルを学習および適用させるか？」(トレーニング)

いずれの場合でも、参加者(対象者)が自らの職務に取り入れるべき特定のマテリアルに焦点が置かれなければならない。参加者(対象者)は、マテリアルが自らの職務に向けて作成されていると思えば、セッションで見聞きすることに注意を払い、取り入れるであろう。決まり切った(個別的ではない一般的で、どの対象者にも広く適用される)と「思われる」プレゼンテーションはどれも、年に 1 度の「決められているので出席している」という他のセッションと同じ程度のものとして頭の中に仕舞い込まれてしまう。ただし、マテリアルが興味深く新しいものであれば、意識向上およびトレーニングプログラミングは効果的なものとなる。[16]

ある時点で、「自分は意識向上マテリアルを作成しているのか、それともトレーニングマテリアルを作成しているのか」と尋ねられる。一般に、意識向上マテリアルの目標は、優秀なセキュリティの実践に注意を払っているため、意識向上へ取り組みで伝えられる概念は短く簡単なものである。このような概念では 1 つのトピックスを取り上げることも、対象者が認識すべき複数のトピックスを取り上げることもできる。

---

[15] 意識向上およびトレーニングマテリアルは、組織内で作成することも、他の組織または専門組織のマテリアルを自組織用に調整することも、契約者/ベンダーから購入することもできる。サービスおよび製品の契約の詳細については、NIST 特別刊行物 800-35『情報技術セキュリティサービスへのガイド(Guide to Information Technology Security Services)』(草案)、NIST 特別刊行物 800-36『情報技術セキュリティ製品の選択ガイド(Guide to Selecting Information Technology Security Products)』(草案)を参照のこと。契約問題に関するより広範なガイドラインについては、NIST 特別刊行物 800-4A『連邦政府の情報技術調達におけるセキュリティの考慮事項 - 調達開始者、契約担当者、および IT セキュリティ担当者用ガイド(Security Considerations in Federal Information Technology Procurements - A Guide for Procurement Initiators, Contracting Officers, and IT Security Officials)』(草案)を参照のこと。

[16] IT セキュリティに関する人員の姿勢やふるまいを変えることは、やりがいのある職務である。新たなセキュリティポリシーは、ユーザーが長年にわたって各自の職務を果たしてきた方法と相対することが多い。たとえば、かつてはすべての情報をオープンな形で共有して業務を行ってきた部署や組織は、この情報へのアクセスおよび配布を制限するように求められている。こうした必要な変化にユーザーを順応させる場合に使用される優れた手法は、個人的な生活体験(なりすまし(個人情報の盗難詐欺)、個人の健康状態や財務データへの不正アクセス、ハッキング(不正侵入))に照らしながら IT セキュリティ問題を論じることから、意識向上モジュール(構成部分)またはセッションを開始するというものである。

意識向上プログラム対象者には、組織の全ユーザーが包含されなければならない。意識向上プログラムまたはキャンペーン [17] で伝えらる概念では、IT セキュリティ上の共通した責任を、個々がそれぞれ認識しなければならない。一方、トレーニングクラスでの概念は特定の対象者に向けられる。トレーニングマテリアルでの概念には、参加者（対象者）が各自の職務を果たすために知っておく必要のある、セキュリティ関連のあらゆる知識が含まれなければならない。トレーニングマテリアルは、通常、意識向上セッションまたはキャンペーンで使用されるマテリアルよりもはるかに詳細である。

4.1 意識向上マテリアルの作成

組織規模の意識向上プログラムまたはキャンペーンのマテリアル作成の開始に際して尋ねられる質問は、「組織の全従業員に、IT セキュリティに関して、何を認識させるべきか？」というものである。意識向上およびトレーニング計画には、一連のトピックスを含めなければならない。電子メール速報、IT セキュリティに関するオンラインの日刊ニュース Web サイト、および定期刊行物は、考え方およびマテリアルを得るための優れた情報源である。その他にも、組織のポリシー、プログラムレビュー、内部監査、内部コントロールプログラムレビュー、自己評価、および抜き打ち検査からも、取り扱うべきトピックスを特定することができる。

4.1.1 意識向上トピックの選択

どのような意識向上セッションまたはキャンペーンでも言及し簡単に論じることのできるトピックスは、非常に多く存在する。[18] 次のようなトピックスが存在する。

・ パスワードの使用と管理 - 作成、変更頻度、保護など

・ ウイルス、ワーム、トロイの木馬などの不正プログラムからの保護 - スキャン、定義の更新

・ ポリシー - 不履行の含意

・ 未知な（不審な）メール／添付ファイル

---

[17] 組織は、特定の問題に焦点を当てて、セキュリティ意識向上キャンペーンを実施することがある。たとえば、ユーザーが、ソーシャルエンジニアリング攻撃または特定のウイルスのターゲットになっている場合、「当該情報を公開する」ために、様々な意識向上手法を使用した意識向上キャンペーンを迅速に実施する必要がある。このようなキャンペーンは、特定の 1 つまたは複数のトピックに関する情報を適時に伝達する必要性があるため、通常の意識向上プログラムの実施とは異なる。

[18] 管理、運用および技術的制御としてまとめられたトピックスの全容は、刊行物 800-12, 800-18 および 800-26 に掲載する。

・ ウェブの利用 ― ウィルスの流行、ユーザのふるまいの監視

・ スパム（迷惑メール）

・ データのバックアップと格納ストレージ ― 集中化または分散化アプローチ

・ ソーシャルエンジニアリング

・ 事故対応 – 誰に？どうすればよいか？の連絡先

・ ショルダーサーフィン（肩越しの盗み見）

・ システム環境における変更 - システムおよびデータへのリスクの増加（水害、火災、ホコリやチリ、物理的なアクセス）

・ 在庫および財物の移送 - 責任のある組織とユーザー責任の特定（媒体の消去など）

・ 個人的利用および利益の問題 - 職場と自宅でのシステム

・ 携帯端末のセキュリティ問題 - 物理的および無線状態でのセキュリティ問題の双方を取り上げる。

・ 暗号化の使用とインターネットを介した重要／機密情報の送信 - 組織ポリシー、手順、および技術的サポートの連絡先を取り上げる。

・ 出張時のラップトップ型コンピュータのセキュリティ - 物理的および、情報セキュリティ問題の双方を取り上げる。

・ 個人所有のシステムおよび職場のソフトウェア - 許可されているかどうかを記述する（著作権など）。

・ システムパッチの時機的な適用 - 設定管理の一部

・ ソフトウェアライセンス制限の問題 - コピーが許可されている時または、されていない時を取り上げる。

・ 組織のシステムにおいてサポート／許可されているソフトウェア - 設定管理の一部

・ アクセス制御の問題 – 最小特権および職務分離を扱う。

・ 個々の責任 – 個々の責任が組織において何を意味しているかを説明する。

- 承認ステートメントの使用 - パスワード、システムおよびデータへのアクセス、個人的利用および利益

- 訪問者の管理と区域への物理的アクセス - 適用可能な物理的セキュリティポリシーおよび手順（不審者の厳密な調査、例外的な活動の報告）を検討する。

- デスクトップセキュリティ - スクリーンセーバーの使用、訪問者に対して画面上の情報の閲覧の制限（「盗み見」の防止/制限）、システムへのアクセスを許可するバッテリバックアップシステム

- 機密問題の対象となる情報の保護 - システム内での保護、履歴の保護、バックアップ媒体での保護、ハードコピー形式での保護、破壊されるまでの保護

- メーリングリストのエチケット - ファイルの添付やその他の規則

4.1.2 意識向上マテリアルの情報源

意識向上プログラムに組み込むことのできる、セキュリティ意識向上マテリアルのソースには様々なものがある。マテリアルは、特定の問題を扱うことも、場合によっては、全体の意識向上プログラム、セッション、またはキャンペーンの作成をいかに開始するか記述することもできる。時機的なマテリアルの情報源には次のものがある。

- 業界主催のニュースグループ、学術組織、または組織の IT セキュリティ担当部署が発行した電子メールの使用に係る助言
- 専門組織およびベンダー
- IT セキュリティに関するオンラインの日刊ニュース Web サイト
- 定期刊行物
- 会議、セミナー、およびコース

意識向上マテリアルは、一度に 1 つのテーマを使用して作成することも、複数のテーマやメッセージを組み合わせたプレゼンテーションとして作成することもできる。

たとえば、意識向上ツール（技法）に関するポスターやスローガンでは 1 つのテーマを含むべきだが、インストラクター指導のセッションや Web ベースのプレゼンテーションでは複数のテーマを含むことができる（配布方法については、第 5 項で詳細に取り上げる）。どのアプローチを選択した場合も、情報量が対象者を圧倒することがあってはならない。必要要件（ポリシー）の簡単な言及、改善のために設計された要件での問題点、取るべき行為は、一般的な意識向上プレゼンテーションに包含されるべき主要なトピックスである。[19]

[19] NIST コンピュータセキュリティ部門の Web サイトにある意識向上、トレーニング、教育、および専門的能力開発のページ（http://csrc.nist.gov/ATE）には、意識向上とトレーニングの両方のマテリアルを提供または販売している政府サイト、業界サイト、および学術サイトへのリンクが多数記載されている。

基本およびリテラシー（技能）マテリアルが組み込まれたより複雑な意識向上プレゼンテーション（NIST 特別刊行物 800-16 の第 3 章を参照）では、特定の目的についてより深く追求する。なぜならば、基本およびリテラシー（技能）は、意識向上とトレーニングとの間の媒介であるため、こういった付加レベルでの詳述さおよび、複雑さのが適切である。

4.2 トレーニングマテリアルの作成

特定のトレーニングコースのマテリアル作成の開始当初に尋ねられる質問は、「対象者に、どの単一または複数のスキルを学習してもらいたいか？」というものである。意識向上およびトレーニング計画では、自らの IT セキュリティ責務を扱うために、トレーニングを受ける単独jのまたは、複数の対象者を特定しなければならない。NIST 特別刊行物 800-16 『情報技術セキュリティトレーニングの必要要件: 役割ベースモデルとパフォーマンスベースモデル（Information Technology Security Training Requirements: A Role- and Performance-Based Model）』(http://csrc.nist.gov/publications/nistpubs/index.html) には、大勢の異なる対象者に合わせたトレーニングコースの構築方法が記載されている。本項では、当該 NIST 刊行物での技法について記述する。その他のトレーニングコースおよびマテリアルの情報源も取り上げ、記述する。

4.2.1 トレーニングコースの構築のためのモデル: NIST 特別刊行物 800-16

NIST 特別刊行物 800-16 の技法では、IT セキュリティトレーニングコースの作成に有効な技法を提供する。この項では、この刊行物の発刊目的となった背景を提供し、この方法を使用したトレーニングコースの作成方法について記述する。

目的と技法:

特別刊行物 800-16 では、1980 年代中期から後期のメインフレーム志向の環境とは相反する、現在の分散化コンピューティング環境における IT セキュリティトレーニングニーズが示されている。本文書では、IT セキュリティ上のある程度の責任を担う 26 の役割を取り上げている。特別刊行物 800-16 では、将来のテクノロジおよび組織的役割に対応するため、役割やその他のパラメータを拡張する技法に自在性を付与する。この技法では、初級、中級、および上級レベルでトレーニングコースを作成できるようにもなっている。コースの作成者に役立つように、それぞれのレベルに合わせた学習目標の例も用意されている。組織は、本物を使用して、IT セキュリティ上重要な責任を担う新規および既存の役割に、必要なトレーニングの対応を検討しなければならない。

特別刊行物を使用したトレーニングコースの作成:

NIST 特別刊行物 800-16 には、多数の情報源が記載されており、コース作成者がトレーニングコースの構築に使用することができる。この情報源とは、IT セキュリティの学習継続性モデル、26 の役割と役割ベースの表、46 の個々のトレーニング表、12 の一連の知識トピックスおよび概念、3 つの基本的トレーニング内容のカテゴリ、および 6 つの機能的専門分野である。

いったんITセキュリティトレーニングが必要とする対象者が特定されたら、コース選択にはNIST特別刊行物の付録Eが用いられる。[20] 組織は、自組織で使用される特定の職位に基づき、取り組み方の調整ができる。付録Eには、この刊行物で取り上げられる26の役割のそれぞれに1つずつ、合計26の表が記載されている。図4-1は、システム管理者用のコースの表例である。

IT Security Training Matrix - *System Administrator*

Training Areas	Functional Specialities						
	A Manage	B Acquire	C Design and Develop	D Implement and Operate	E Review and Evaluate	F Use	G Other
1. Laws and Regulations				1D ✓			
2. Security Program							
2.1. Planning							
2.2. Management				2.2D ✓			
3. System Life Cycle Security							
3.1 Initiation				3.2D ✓			
3.2. Development				3.3D ✓			
3.3. Test and Evaluation				3.4D ✓			
3.4. Implementation			3.4C ✓	3.4D ✓			
3.5. Operations	3.5A ✓		3.5C ✓	3.5D ✓			
3.6. Termination				3.6D ✓			
4. Other							

図 4-1: IT セキュリティトレーニングマトリクスの例

[20] いったんトレーニングニーズが特定されると、組織によっては、カリキュラムビルダー（トレーニング作成の専門家）に依頼してトレーニングマテリアルを作成してもらうこともある。トレーニング作成の専門家は、普通、IT セキュリティの専門家ではないため、専門家は、マテリアルの正確性はもとより、複雑化の正確性を期すため、IT セキュリティスタッフと緊密に協力する。

それぞれの表には、コースマテリアルの作成に使用される多数のセルが存在する。合計で 46 のセルがあるが、各コースには特定のセルだけが使用される。コースマトリクス（表）によっては 2 つのセルしかないこともあり、IT セキュリティ担当者およびマネージャのコースマトリクス（表）では、46 すべてのセルを使用する。ほとんどのマトリクス（表）では 7 から 10 のセルを使用する。

本マトリクス（表）は、3 つの基本的トレーニング内容のカテゴリ、またはトレーニング分野（つまり、法と規制、セキュリティプログラム、およびシステムライフサイクルセキュリティ）に関連の 6 つの役割カテゴリ（または機能的専門分野）によって構成される。6 つの役割カテゴリまたは機能的専門分野は次のとおりである。

- 管理 - 本カテゴリは、組織での IT ベースの機能を管理する担当者に該当する。

- 取得 - 本カテゴリは、IT 製品および／またはサービスの取得に関わる（ベンダーの IT システムの提案を評価する情報源選択委員会に従事するなど）担当者に該当する。これは、契約担当者の技術代表者（COTR; Contracting Officer's Technical Representative）として従事するものにとって特に重要である。

- 設計および作成 - 本カテゴリは、システムおよびアプリケーションの設計と作成を行う担当者に該当する。

- 運用 - このカテゴリは、IT システム（Web サーバー、電子メールサーバー、ファイルサーバー、LAN、WAN、メインフレームなど）を運用（管理）する担当者に該当する。

- レビューと評価 - このカテゴリは、組織の内部コントロールプログラム、内部レビュー、または外部監査プログラムの一部として、IT 機能のレビューと評価（監査）を行う担当者に該当する（監査官など）。

- 使用 - このカテゴリは、職務を遂行するために IT リソースにアクセスしたり、IT を使用する人員に該当する。

カテゴリ（または機能的専門分野）は、各マトリクス（表）の上部に左から右へ並べられている。さらに役割カテゴリを追加したり、機能的専門分野を作成できるように、「その他」と名付けられた代替セルが、7 番目の列に用意されている。これらの 6 つのカテゴリは、対象者に合わせて調整され、ある役割における特定の機能を扱うコースを可能にするものである。たとえば、システム管理者が機能を管理するまたは、単独または複数のシステムを運営（運用）することもある。トレーニングコースマテリアルは、組織内での役割ごと（個々の職務機能によって）に構成されなければならない。

図 4-1 のシステム管理者コースのマトリクス（表）例では、コースマテリアルは 10 個のセルから作成される。各セルは、コースマテリアルの構成要素とみなすことができる。この例では、ほとんどのセルが、「インプリメントおよび運用」の専門分野または列に該当している。これは、システム管理者が単独または複数のシステムを実行（運用）することが想定されるからである。このコースはシステムの管理、設計、および開発を扱うため、10 のうちのいくつかのセルが、これらの専門分野または列に現れている。

4.2.2 トレーニングコースおよびマテリアルの情報源

コース作成にあたり、トレーニングマテリアルの情報源を決定する最初のステップは、マテリアルを組織内で作成するのか、外部委託するのかを決めることである。組織が内部に専門知識を蓄積しており、トレーニングマテリアルおよびコースの作成に必要な情報源を割りあてることが可能な場合は、NIST 特別刊行物 800-16 を用いることができる。

図 4-2 には、コースマテリアルを内部で作成するか、外部委託するかを決定する際に考慮すべき、いくつかの重要な問題が記載されている。

- この職務を遂行するための内部リソースが揃っているか。このリソースには、適切なスキルを持った人員と、作業を行うのに十分な人員が含まれる。
- 内部でマテリアルを作成した場合、外部委託する場合よりも対費用効果的か。
- 資金調達手段が整えられているか（予算）。
- 契約担当者の技術代表者（COTR）の役割を担い、契約者の行為を効果的に監視できるスタッフがいるか。
- 組織は、契約者がマテリアルの作成を行う場合、マテリアル維持に必要な情報源が揃っているか（資金調達および必要な専門知識を持ったスタッフなど）。
- コース内容の機密性では、契約者がマテリアルを使用することを排除するのか。
- 外部委託は、重要なトレーニングの配信スケジュールに対応できるか。

図 4-2: 主要な質問 - トレーニングマテリアルを内部で作成するか、外部委託するか

組織が、トレーニングコースの作成を外部委託することを決定した場合、特定の対象者にあわせて作成できる、既製のコースを提供するベンダーは多数存在する。特定のベンダーを選択する前に、組織は、トレーニングニーズについて全面的に理解し、候補として有望なベンダーのマテリアルが組織のニーズに見合っているかどうかの判断ができなければならない。

パートナーシップの最大活用:

組織は、トレーニングコースマテリアルを既存の情報源を使用して作成するか、外部委託するかを単に決定するだけではなく、多くのオプションも選択できる。組織は、マテリアルを作成したり、IT セキュリティトレーニングニーズを満たすトレーニングイベントを調整するために、他の組織とのパートナーシップを確立する（または既存のパートナーシップを最大活用する）ことができる。たとえば、複数の組織がリソースと専門知識を組み合わせ、特定の対象者に向けたトレーニングコースを作成することもできる。作成したマテリアルの大部分が組織の固有のマテリアルとしてト

レーニングコースに含まれ、その構成要素として限定される場合、関与するすべての組織は、その大部分を使用することができる。この場合、諸組織は、組織固有のマテリアルを含む構成要素の修正または調整のみを行わなければならない。

同様に、組織は、IT セキュリティのディ、年次または。地域カンファレンスを編成し、当該カンファレンスが他の組織の人員にも公開されていることを公表することがある。一方、提供されるマテリアルは、両方の組織が必要とするものと正確には一致していないこともあるが、コストをかなり抑えた、特定の対象者のトレーニングニーズのいくつかと見合う、方法となることが可能である。このような調整を行う場合、各参加組織の出欠を追跡し、トレーニングマテリアルの適用性を確実にし、責任の判断を行い、他の運営および管理上の問題を扱うことを許可するプロセスを構築しなければならない。

まったく新しいコースを作成するのではなく、他の組織が作成した、低コストで編集可能なトレーニングマテリアルの使用も検討することが可能である。利用可能なマテリアルが目的とする対象者に適用できるかどうか、参加予定者が IT セキュリティ上の責任を満たすために知る必要のある内容がマテリアルで取り上げられているかどうかに留意しなければならない。

組織内で、IT セキュリティプログラムマネージャは、組織のトレーニング機能との、または自身のトレーニングを調整または実施する職務マネージャとの新しいパートナーシップの構築または、既存のパートナーシップを強化することができる。内部で作成された職能トレーニング（財務アプリケーション、人事管理など）では、関連するITセキュリティ問題の適切な討議が欠けてしまうことが多い。パートナーシップを通じ、IT セキュリティプログラムマネージャは、トレーニングマテリアルのセキュリティに対する既存の参考文献の精査を提案し、完全性と正確性を調べることができる。IT セキュリティプログラムマネージャは、トレーニングまたはセキュリティの要素を含まない職能マテリアルのセキュリティ構成箇所を作成することで、職務マネージャを補佐することもできる。IT セキュリティプログラムマネージャは、外部委託される職能トレーニングの作成についての契約内容を精査し、該当するセキュリティ問題が、目的とする対象者にとって十分な詳述さおよび、複雑さを扱っていることを確認することも可能である。

5. 意識向上およびトレーニングプログラムの実施

IT セキュリティ意識向上およびトレーニングプログラムは、次の項目が終了した後にのみ実施しなければならない。

・ ニーズ（査定または必要性査定）アセスメントを実施した。

・ 方策を作成した。

・ この方策を実施するための意識向上およびトレーニングプログラム計画を完成した。

・ 意識向上およびトレーニングマテリアルを作成した。

図 5-1 には、意識向上およびトレーニングプログラムの実施を先導する主要な段階を示す。

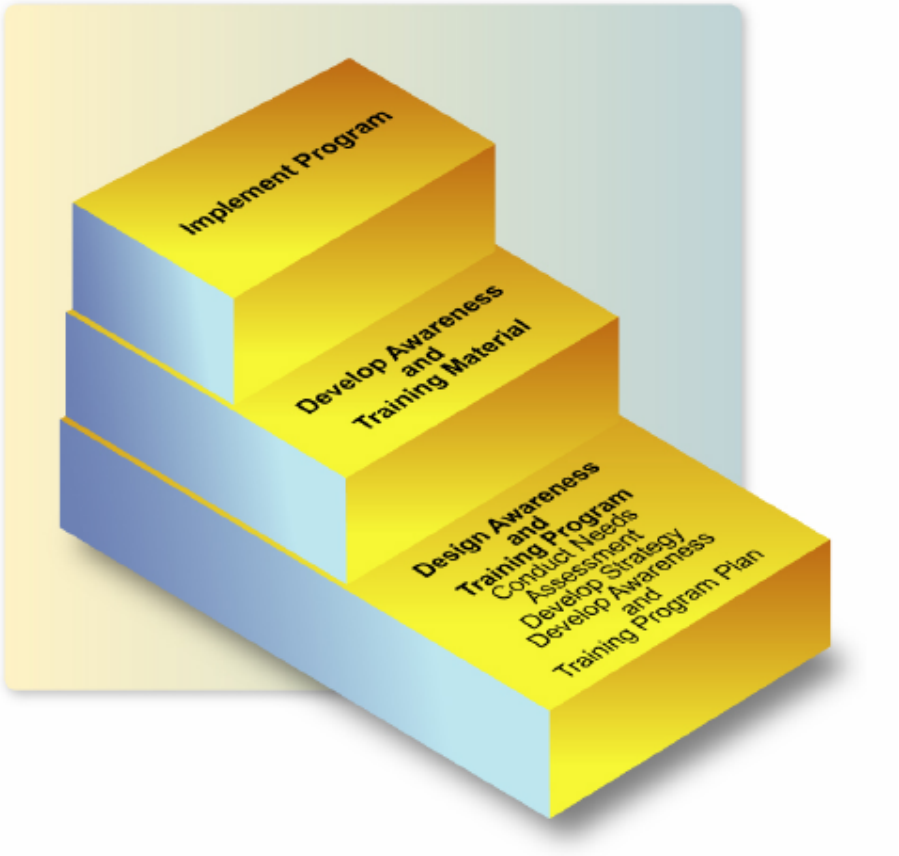

図 5-1: プログラムの実施に至るまでの主要ステップ

5.1 計画についての連絡

必要な情報源の実施と委託に対する組織からのサポートを得るため、プログラムの実施について十分な説明がされなければならない。この説明には、プログラム実施の期待予想値と組織に対する利益はもとより、組織の管理職およびスタッフのサポートの期待予想値が含まれる。資金調達の問題も扱われなければならない。たとえば、管理職は、意識向上およびトレーニングプログラムの実施に係る費用がすべて、CIO または IT セキュリティプログラム予算による資金調達なのか、プログラムの実施費用の予算に占める割合を補うために自らの予算に影響が及ぶか否かを知らなければならない。プログラムの実施に関与する全員がその役割と責任を理解しておくことが不可欠である。さらに、スケジュールと完成要件の連絡が行われなければならない。

計画の連絡は、第 3 項で述べた 3 つの実施モデルへ位置づけることができる。一般的なシナリオ（計画）は以下である。

プログラムの集中化モデルの通信シナリオ（計画）:

本モデルでは、CIO および／または IT セキュリティプログラムマネージャが、組織のすべての IT セキュリティ意識向上およびトレーニングポリシーを作成し、方策とプログラム計画を作成し、プログラムを実施する。したがって、マテリアル作成と実施に必要なすべての資金調達は、CIO および IT セキュリティプログラムマネージャによって管理され、提供される。プログラムの実施までに、ニーズ（査定または、必要性査定）アセスメントを実施し、トレーニング計画を作成し、意識向上およびトレーニングマテリアルの作成が終了している。CIO および／または IT セキュリティプログラムマネージャは、組織の幹部と上級管理職に、実施計画の概要を説明し、組織全体へ通達するための承認を得る。いったん実施計画が承認されたら、CIO および／または IT セキュリティプログラムマネージャは、組織の部門管理者に計画を通達し、意識向上およびトレーニング提供のスケジュールを伝え、適宜、それぞれの部門のセッション枠への割り当てを行う。。次いで部門マネージャは、その計画を自部門スタッフに伝え、求められる意識向上およびトレーニングを特定し、参加者のスケジュールを設定し、それぞれのスロットに対する候補者を CIO または IT セキュリティプログラムマネージャへの要求事項として提出する。

プログラムの部分的分散化モデルの通信シナリオ（計画）:

本モデルでは、CIO および／または IT セキュリティプログラムマネージャが、組織のすべての IT セキュリティ意識向上およびトレーニングポリシーを作成し、方策を作成する。また、方策を導き出すためのニーズ（査定または、必要性査定）アセスメントも行う。続いて部門マネージャは、意識向上およびトレーニングの予算を与えられ、自部門のトレーニング計画を作成し、プログラムを実施する。部門マネージャは、要求事項として CIO および／または IT セキュリティプログラムマネージャに、（プログラムの）状況を報告しなければならない。

プログラムの分散化モデルの通信シナリオ（計画）:

本モデルでは、CIO および／または IT セキュリティプログラムマネージャが、IT セキュリティ意識向上およびトレーニングプログラムに関する広範なポリシーと期待効果を通達する。プログラムの残余部分の実行は、組織部門の責任である。組織部門のマネージャは、ニーズ（査定または、必要性査定）アセスメントの実施、方策の策定、ト

レーニング計画の作成、意識向上およびトレーニングマテリアルの作成、意識向上およびトレーニングプログラムの実施を行うことが期待される。必要に応じて、CIO および／または、IT セキュリティプログラムマネージャに、状況レポートを提出しなければならない。

意識向上およびトレーニングプログラムを実施する計画について、組織の管理職に説明が行われ、(承認されることにより)、意識向上および、トレーニングプログラムの実施が可能となる。意識向上マテリアルと連絡事項を組織全体に提示し、広める方法は多数存在する。

5.2 意識向上マテリアルの配布手段

IT セキュリティ意識向上に関するメッセージを組織全体に広める手法は多数ある。選択される手段は、情報源とメッセージ:方針の複雑さによる。

組織が検討するであろう手法には次のものがあるが、これに限定されるものではない。

- 意識向上の手段(ペン、キーチェーン、付箋紙、メモ帳、救急箱、(デスク回り)クリーンアップキット、メッセージ付きディスク、しおり、フリスビー、時計、「了解」カードなど)でのメッセージ
- ポスター、「やること、やってはいけないことリスト」、またはチェックリスト
- スクリーンセーバーおよび警告バナー/メッセージ
- ニュースレター
- デスク間警告(組織のメールシステムを通じて配信される明色刷りハードコピーの 1 ページもの掲示板
  - デスクつき 1 部または、オフィスで回覧)
- 組織全体にわたる電子メールメッセージ
- ビデオテープ
- Web ベースのセッション
- コンピュータベースのセッション
- 遠隔会議セッション

・ インストラクター直接指導のセッション

・ IT セキュリティの日または類似したイベント

・ 手弁当セミナー

・ セキュリティ連絡先情報や月間セキュリティのヒント／コツなどを記したポップアップカレンダー

・ マスコット

・ クロスワードパズル

・ 表彰プログラム（盾、マグ、感謝状など）

単独のメッセージの配布に向いている手法は、意識向上ツール、ポスター、アクセスリスト、スクリーンセーバーおよび警告バナー、各デスクへの警告、組織全体の電子メールメッセージ、手弁当セミナー、表彰プログラムである。

複数のメッセージをより簡単に組み込める手法には、「やること、やってはいけないことリスト」、ニュースレター、ビデオテープ、Web ベースのセッション、コンピュータベースのセッション、遠隔会議セッション、インストラクターの直接指導のセッション、手弁当セミナーがある。

あまり費用をかけずに、メッセージを込める手段には、意識向上ツールでのメッセージ、ポスター、アクセスリスト、「許可および禁止事項リスト」、チェックリスト、スクリーンセーバーおよび警告バナー、各デスクへの警告、組織全体の電子メールメッセージ、インストラクターの直接指導のセッション、自費セミナー、表彰プログラムがある。付録 D には意識向上ポスターを例に挙げる。

さらに情報源を必要とする手段には、ニュースレター、ビデオテープ、Web ベースのセッション、コンピュータベースのセッション、遠隔会議セッションがある。

意識向上マテリアルを関心を引く最新のものにし、意識向上メッセージを繰り返し、様々な方法で表現することによって、より多くのユーザーの意識向上レッスンや問題（意識）の維持を大いに高めることができる。たとえば、ソーシャルエンジニアリング攻撃の犠牲になることを回避するためのセッションは、ポスター、定期的に配信される組織全体への電子メールメッセージ、ユーザーに配布される意識向上ツールのメッセージなどによる強化が可能である。

5.3 トレーニングマテリアル配布の手段

トレーニングマテリアルを効果的に配布するための手段は、次の特徴を裏付けるテクノロジを活用すべきである。

- 使いやすさ（アクセスしやすい、更新/管理しやすいなど）
- 拡張性（様々な対象者規模や様々な場所で使用できるなど）
- 責任（完成度合いの把握および、統計データの使用など）
- 広範な業界サポート（適性数の見込みベンダー、アフターサポートを調達できる十分な機会など）

組織が採択する最も一般的な手段は、次のとおりである。

- **相互ビデオトレーニング（IVT; Interactive Video Training；インタラクティブビデオトレーニング）**

  IVT は、トレーニングマテリアルの配信に利用できる、遠隔学習手段の 1 つである。本テクノロジは、送受信両用の相互的オーディオおよびビデオ指導を裏付けるものである。相互性は、非相互的トレーニングよりもテクノロジを効果的にする一方、費用も割高である。

- **Web ベースのトレーニング**

  本テクノロジは配信環境では、現在、最も一般的なものである。Web ベースセッションの「出席者」は単独で学習し、独自のペースで学ぶことができる。パフォーマンスを評価するために、テストおよびアカウンタビリティ機能を組み込むことができる。本手段法を取り入れたトレーニングモデルは、インストラクターと受講生との間、または受講生間における（付加的）相互便益性の提供を始めている。

- **Web を使用しないコンピュータベースのトレーニング**

  本手段は、Web が利用できるようになっても一般的に用いられている。本手段は、依然としてトレーニングマテリアルの配信に効果的な方法であり、特に Web ベースのマテリアルにアクセスできない場合に有効である。Web ベースのトレーニングとは異なり、この手段は、インストラクターと受講生との間、または受講生間でのやり取りはできない。

- **現場でのインストラクター指導のトレーニング（仲間同士（受講生同士）のプレゼンテーションおよび指導を含む）**

  本手段は最も古いものの一つであるが、対象者へのトレーニングマテリアルを配布する最も一般的な手段の一つである。本手段の最大の利点は、相互的な指導を行えるところにある。ただし、本手段にはいくつかの欠点がある。大規模な組織では、すべての対象者が出席できるように、十分なクラスのスケジュールを設定することが困難な場合がある。従業員が広い地域に分散する組織では、インストラクターと受講生の移動費用が膨大になってしまう可能性が生じる。こういった分散組織の場合は困難ではあるが、他の方法よりもこの伝統

的な方法を好む学習者もいる。

様々なトレーニング配信手法を 1 つのセッションに融合することは、マテリアルを提示し、対象者を惹きつけるために効果的な方法である。たとえば、インストラクター指導のセッション中のビデオの上映は、対象者を、異なる情報源に注意を向けさせることができる。ビデオの上映はまた、インストラクターが提示している内容を補強することもできる。IVT、Web ベースのトレーニングおよび、Web を使用しないコンピュータベースのトレーニングも、インストラクター指導のトレーニングセッションの一部として用いることができる。

6. プログラムの実施後

IT セキュリティ意識向上トレーニングプログラムは、テクノロジの変化、IT インフラストラクチャ、組織の変化、組織の任務および優先度の変化に十分な注意が払われていなければ、すぐに時代遅れになってしまう。CIO と IT セキュリティプログラムマネージャは、こういった潜在的な問題を認識し、本プログラムが全体的な目的に意義を持って対応し続けることを確実とする方針にメカニズムを組み入れる必要がある。

たゆまぬ向上は、常にセキュリティ意識向上トレーニングの第一歩である。なぜならば、本領域に関しては、「十分に行った」と言えることがないからである。

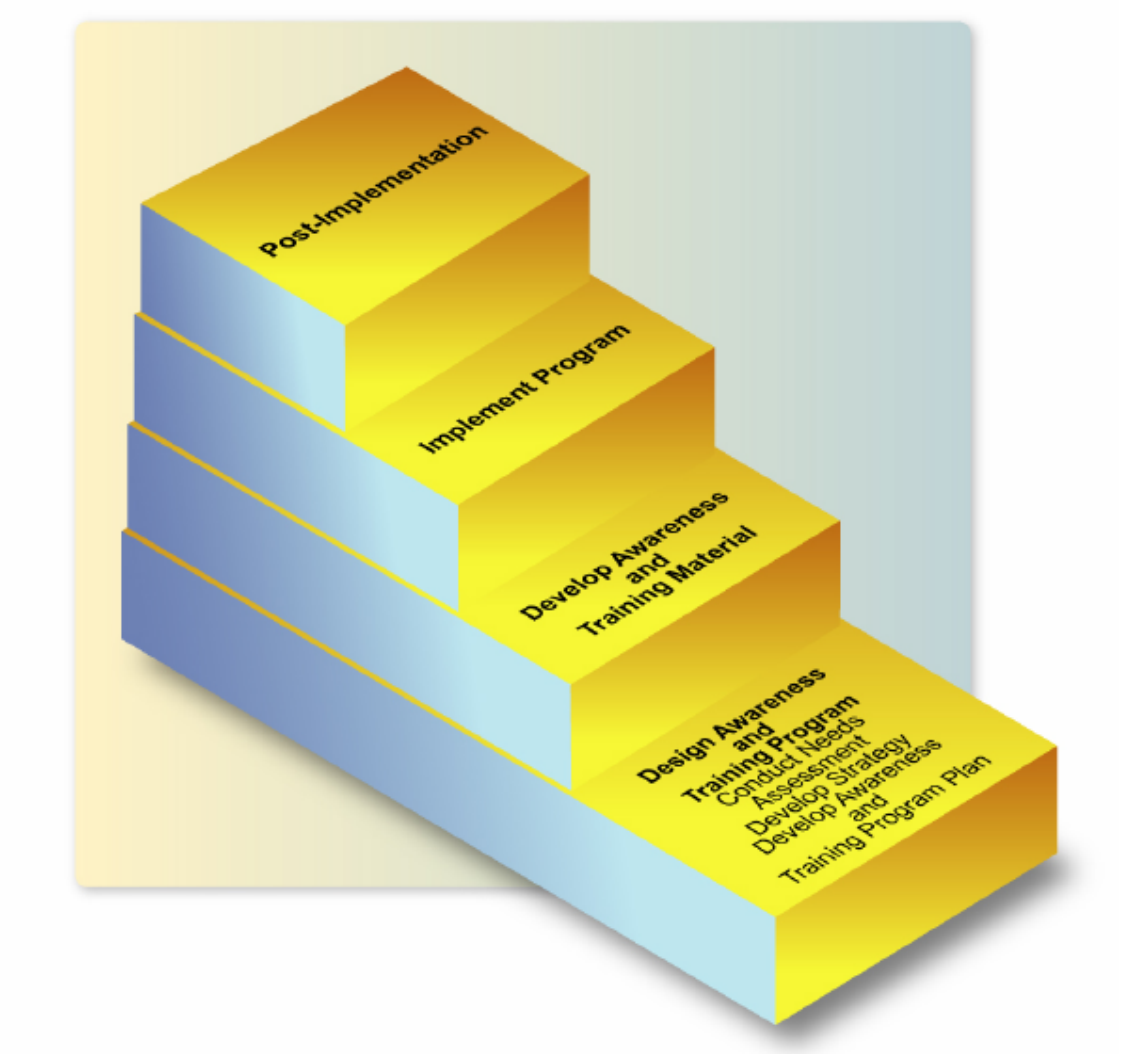

図 6-1: プログラムの実施後までの主なステップ(段階)

6.1 整合性の監視

プログラムがいったん実施されると、整合性および有効性を監視する手続きが導入されなければならない。プログラム活動に関する主な情報（コース、日付、対象者、コスト、ソースなど）を把握できるように、自動追跡システムを設計しなければならない。当該追跡システムでは、組織レベルでこういったデータが把握されるため、組織全体における分析、意識向上、トレーニングおよび教育の第一歩に関する報告を行うために用いられる。データベースの必要要件には、すべての対象ユーザーのニーズを盛り込む必要がある。こういったデータベースの一般的なユーザーは次のとおりである。

- **CIO** - 戦略的な計画を裏付け、組織の幹部およびその他の上級管理職に、IT セキュリティ意識向上トレーニングプログラムの状態について通知し、自組織におけるセキュリティ要員の能力と重要な必要性を特定し、プログラム分析を実行し、企業規模での活動を特定し、セキュリティおよび IT の予算調達の助力となり、プログラム改善の必要性を特定し、整合性を査定するためにデータベースを使用する。

- **IT セキュリティプログラムマネージャ** - セキュリティ計画を裏付け、CIO や他の管理職およびセキュリティ要員へ状況を報告し、資金調達にかかる要求を判断し、組織が設定した最終目的と達成目標との整合性を立証し、ベンダーと他のトレーニング情報源を特定し、セキュリティ関連の問い合わせに対応し、現在の（対象）範囲を特定し、重要な欠落に対する調整を行うためにデータベースを使用する。

- **人事部門** - すべてのセキュリティ関連のトレーニングを調達するための効果的なメカニズムが存在することを確認し、IT セキュリティトレーニング関連の費用を特定し、職位記述書の作成、状況報告を助力し、トレーニングの問い合わせに対応し、専門的能力開発の援助にデータベースを使用する。

- **組織のトレーニング部門** - 組織全体のトレーニング方針の作成に助力し、セキュリティ指示に結びついたトレーニングデータベース要件を設定し、可能なトレーニング情報源を特定し、トレーニング要求を裏付け、コースの適切さと一般性を特定し、資金計画を裏付け、問い合わせへの対応にデータベースを使用する。

- **職務マネージャ** - ユーザートレーニングの進捗を監視し、必要に応じユーザートレーニング計画の調整を行い、状況報告書を入手し、部門内のセキュリティトレーニングに関する問い合わせに対応し、予算および、提案の予算の助力となるトレーニングの情報源および、費用の特定のためにデータベースを使用する。

- **監査人** - セキュリティ指示と組織のポリシーが伴う整合性を監視するため、データベースの情報を使用する。

- **最高財務責任者（CFO; Chief Financial Officer）** - 予算の問い合わせに対応し、財務計画を助力し、セキュリティトレーニングにおける資金調達活動に関する報告書を組織の幹部および上級管理職に提出するためにデータベースの情報を使用する。

整合性の追跡には、データベースの情報によって示されたプログラムの状況を査定し、組織によって設定された標準に対応するプログラムの状況が関与する。報告書は格差または問題を特定するために生成し、用いられる。次いで、是正措置と必要なフォローアップが行なわれる。意識向上、トレーニングまたは教育の提供および／または完成予定日程は、管理職への正式なリマインダの形式をとることがある。

6.2 評価とフィードバック

正式な評価とフィードバックの仕組みは、すべてのセキュリティ意識向上、トレーニング、および教育プログラムの重要な要素である。既存のプログラムの働きの良識がなければ、継続的な改善が発生することはない。さらに、フィードバックの仕組みは、当初設定されたプログラムの目標に対処するために設計しなければならない。ベースラインの必要要件がいったん確定したら、フィードバックの方針を設計、実施する。図 6-2 は、意識向上トレーニングプログラム計画の更新に用いられる、様々な評価およびフィードバックのメカニズムを示したものである。[21]

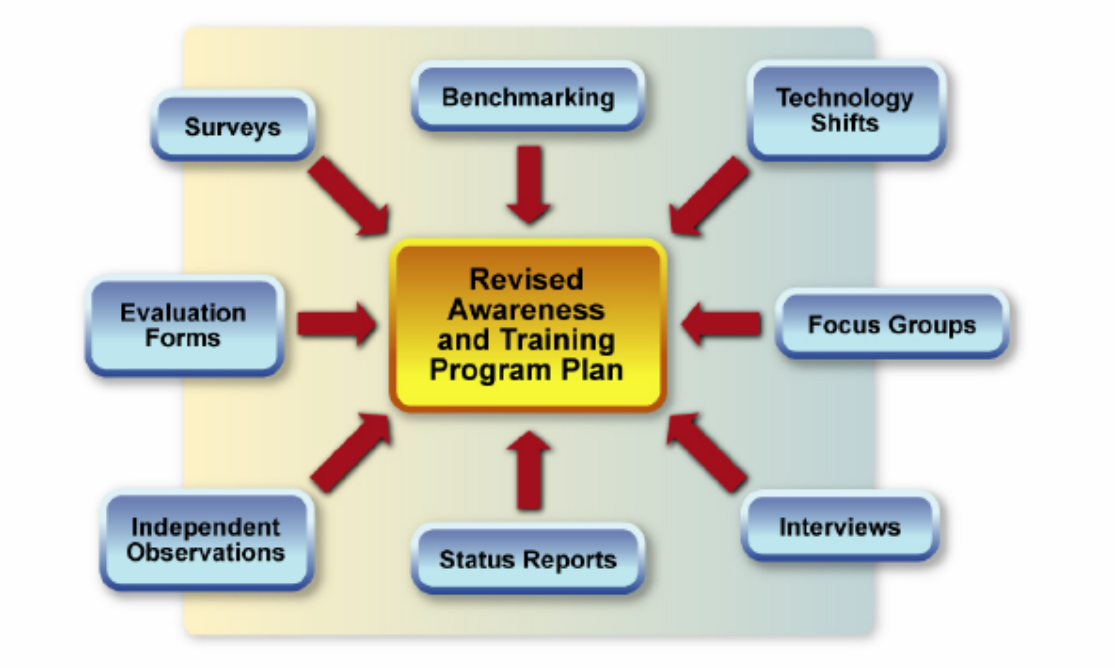

図 6-2: 評価およびフィードバック手法

[21] 意識向上トレーニングプログラム計画は、意識向上およびトレーニングプログラムの設計フェーズの結果を表したものである。設計フェーズとは、意識向上トレーニングプログラムのライフサイクルにおける、4 つの主要フェーズ（プログラムの設計、マテリアルの作成、プログラムの実施、プログラムの管理）の最初のフェーズである。評価およびフィードバック手段では、意識向上トレーニングプログラム計画の更新の結果となる洞察を提供する。ニーズアセスメントの実施に従い、ニーズアセスメントは組織が意識向上およびトレーニングプログラム計画を決定に役立つため、評価およびフィードバック手法から得られた見識を考慮することが重要である。

フィードバック方針では、品質、目的、展開方法（Web ベース、オンサイト、オフサイト）、困難さのレベル、使いやすさ、セッションの期間、関連性、流通性、修正にかかる提案を扱う要素を組み込む必要がある。

フィードバックを求めるため、多くの方法を適用することが可能である。最も一般的な方法は次のとおりである。

- **評価フォーム/アンケート**

  様々な形式を用いることができる。優れたデザインは、記入する側の多くの記述をする必要性を解消する。その秘訣は、できるだけ「ユーザーフレンドリー（ユーザーの側に立った）」なフォームのデザインである。このような評価手段の設計技術に精通した内部の専門家または、外部の専門家に援助を求め、作業を行う。

- **フォーカスグループ**

  （トレーニングの）対象者を集め、公開討論会において、IT セキュリティトレーニングプログラムの有効性についての観点を討論し、改良のためのアイデアを求める。

- **選抜インタビュー**

  本アプローチ手段ではじめに、インパクト、優先度、または他に設定された基準に基づき、トレーニングの対象グループを特定し、フィードバックのための具体的な分野を特定する。このアプローチは、通常、1 対 1 のインタビューもしくは、小規模で同等レベルのグルーピング（通常、10 人または、以下）で行われるため、フォーカスグループのそれより個別的なアプローチとなるため、参加者は、プログラムの評価をより積極的に仕向けることができる。

- **独立した観察/分析**

  フィードバックを求めるためのもう1つのアプローチは、組織主導の監査の一部として、外部契約者またはその他の第三者による、IT セキュリティ意識向上およびトレーニングプログラムのレビューを組み込むことである。組織は、プログラムの効果に関する公平な意見を得るために、通常の監視行為（OIG、GAO など）に加えてこれを行う。

- **公式な状況レポート**

  組織全体にわたるセキュリティ意識向上およびトレーニング要件に焦点を当て続けるために有効な方法は、職務マネージャによる定期的な状況報告要件を実施することである。

- **セキュリティプログラムのベンチマーク（外観）**

  多くの組織では、継続的な改善およびさらなる向上のための方針の一環として、「セキュリティプログラム」ベンチマークを組み入れている。こういった類のベンチマークでは、「自分は、どのように同僚の中で評価されているのか」という自問に焦点が当てられる。外部に焦点を当てた形式のセキュリティベンチマークでは、組織のパフォーマンスを多くの他の組織と比較し、現在利用できるデータと共に、組織全体にわたって観察されたベースラインに基づいたレポートが戻される。こういったベンチマークの要素には、セキュリティ意識向上およ

びトレーニングが含まれなければならない。こういったベンチマークは、通常、かなり長い期間（5 年またはそれ以上）、組織の広範囲にわたる膨大な情報（データ）を持つベンチマーク手法の専門家の手によって作成される。

6.3 変更の管理

プログラムは、新しいテクノロジや関連するセキュリティ問題が登場したときに、その構造に従い継続的に更新を行うことが必要である。新たな構造および、手法の変化に対応するために、トレーニングニーズは新たなスキルおよび、能力へと推移することが必要になる。組織の任務および／または、目的における変更も、トレーニングの場やその内容をいかに効果的に設計するかのアイディアに影響を及ぼす。国防といった新たな問題の発生も、最新の搾取法やその対策をユーザーへの通知／教育を継続するために必要なセキュリティ意識向上行為の性質および、その範囲に影響が及ぶ。新たな法律および、法廷での判決も、意識向上および、トレーニングマテリアルの作成および／または、実施に影響を及ぼすことがあり、次いで、組織のポリシーにも影響が及ぶことがある。最後に、セキュリティ指示の変更や更新に従い、意識向上およびトレーニングマテリアルはこういった変更を反映しなければならない。

変更の管理は、トレーニング/意識向上/教育の展開が停滞せずに、したがって、組織が直面する実際に明らかになった問題に対して不適切にならないように設計されたプログラムのコンポーネントである。それは、組織文化に反映するセキュリティポリシーおよび、手順の変更にも対応するように設計されている。

6.4 継続的な改良（「難易度の引き上げ」）

プログラムの本段階では、組織におけるセキュリティの普及度が、セキュリティの意識向上および、優秀さのレベル作成に到達することに焦点を置く。従業員への意識向上、トレーニング、および教育に関するプロセスの配布は、全体的なビジネス方針に統合しなければならない。完成されたセキュリティの意識向上および、トレーニングプログラムでは、本領域に係る一連の測定基準を定義し、自動化システムは、定量的データを把握し、関係責任者への定期的なあらかじめ定義されたサイクルでの管理情報の発信を援助するために配備がされなければならない。

監視、フォローアップ、および修正手順は途切れなく、適切に定義されている。最後に、本段階で組織は、先進テクノロジ、優れた実践方法、およびベンチマークの機会といった分野の継続的な調査に、その意識向上およびトレーニングプログラムの正式なメカニズムを組み込んでいる。

6.5 プログラム成功のための指標

CIO、プログラム担当者、および IT セキュリティプログラムマネージャは、継続的な改良および、組織のセキュリティ意識向上、トレーニング、教育プログラムのサポートを、第一に主導しなければならない。組織内で自らに割り当てられたセキュリティ上の役割を、全員が果たすことができ、遂行しようとする意思を持つことが重要である。セキュリ

ティでは、「最も弱い部分が強さを決定する」という言葉は真実である。組織の情報およびインフラストラクチャを確保することは、チームの努力の賜物である。以下は、プログラムをサポートし、プログラム容認の目安となる主な指標である。

- 合意を得た方針を実施するための十分な資金調達
- 主な責任者（CIO,プログラム担当者、IT セキュリティプログラムマネージャ）が当該戦略の効果的な実施を可能にする適切な組織的配置
- ウェブ、電子メール、TV などを通じての広範な配布サポートおよびセキュリティ意識向上アイテムの掲示
- 幹部／上級管理者レベル関係者のセキュリティに関するスタッフへの言葉（スタッフミーティング、組織の幹部による全ユーザーへの放送など）
- 測定基準の使用（セキュリティ事故または、違反の下降 [22]、既存の意識向上およびトレーニングの対象と特定される必要性における格差の縮小、意識向上マテリアルを体験したユーザーのパーセンテージの増加、適切なトレーニングを受け、セキュリティ上の重要な責任を持つユーザーのパーセンテージの増加を示すメトリックス（測定基準）など）
- 管理者は、その地位および、ファイルによって整合性が遵守されるセキュリティ管理を回避するために、組織における自らの地位を用いてはならない。
- 必須セキュリティフォーラム/ブリーフィングの出席水準
- セキュリティに対する貢献度の認定（賞金/賞品、コンテストなど）
- セキュリティプログラムの管理/調整における重要な役割を担うことによって立証される意欲

[22] セキュリティ行為が改善されると、セキュリティインシデントあるいは、セキュリティ違反の数は減少する一方で、潜在的なインシデントの報告は、ユーザーが強い警戒心を抱くため増加することがある。

付録 A ニーズアセスメントのインタビューとアンケート

現在の任務（組織/担当部署）:

所属組織（部署/組織）:
地位または等級: _____
現在の任務の日付（月/年）: _____
肩書き: _____

このアンケートは、あなたの組織の自動情報システムとネットワークを管理するために使用する知識、スキル、経験を明らかにするように設計されています。あなたが行っている職務、それらを遂行するために学習した方法、任務を果たす上で最大のメリットと思われるトレーニングの種類について質問しています。提供していただく情報は、（組織名）システム管理者のニーズに適合したセキュリティトレーニングの設計に使用されます。アンケートの回答にかかる時間はおよそ 30 分です。

第 1 部 背景:

1. 現在、システム管理者としての職務を行っていますか。…… はい いいえ

1a.「はい」の場合、終日勤務ですか。…… はい いいえ

1b. 常勤でない場合、システム管理の職務に費やす時間は何パーセントですか。
……_____%

2. システム管理者としてどのくらいの期間勤務していますか。 ____年____か月

3. あなたの下で働くシステム管理者がいますか。…… はい いいえ

4. システム管理者の下で働いていますか。…… はい いいえ

5. システム管理の公式トレーニングを受けたことがありますか。……。…… はい いいえ

（「はい」の場合、下に具体的に記入してください）

_____

（学校またはベンダー）　コースのタイトル/名称　（期間 - 日数）（年）

_____

（学校またはベンダー）　コースのタイトル/名称　（期間 - 日数）（年）

6. システムセキュリティについての公式トレーニングを受けたことがありますか。(「はい」の場合、下に具体的に記入してください) ...はい いいえ

_____

(学校またはベンダー) コースのタイトル/名称 (期間 - 日数) (年)

_____

(学校またはベンダー) コースのタイトル/名称 (期間 - 日数) (年)

7. 終了した学校教育の年数を記入してください。(たとえば、高卒 = 12 年、文学士/理学士 = 16 年など) : _____

8. 昨年、システム管理または情報システムセキュリティに関連したセミナーまたは会議に何回出席しましたか。

9. コンピュータ/ネットワーキング/ソフトウェアのジャーナルまたは雑誌を定期購読していますか。(「はい」の場合、下に具体的に記入してください) .....はい いいえ

_____

第 2 部 タスクのパフォーマンスとトレーニング:

列 A の各タスクごとに、タスク遂行の頻度を示す列 B の文字を丸で囲んでください。 **O**－なし **L**－ひと月に 1 回以下 **M**－毎月 **W**－毎週 **D**－毎日		このタスクの主なトレーニング方法にチェックを付けてください。「その他」の場合は、具体的に記入してください（ワークショップ、試行錯誤など）。	各タスクについて、必要だと思われるトレーニングのレベルを、初級（E）、中級（I）、上級（A）から選び（□）を付けてください。
A	**B**		
システムハードウェアの管理:			
ハードウェアのインストールの計画	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A ____
ハードウェアの取得	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A ____
ネットワークのインストールの調整	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A ____
予防保守のスケジュール設定	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A ____
ハードウェア修理の調整	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A ____
ハードウェアのインストール	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A ____
システムの起動	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A ____
システムハードウェアの一覧の管理	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A ____
消耗品の注文	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A ____
診断の実行	O L M W D	__クラスルーム ___ OJT（オンザジョブ）	E ____ I____

		__ 独学 ___ その他 _____	A____
ハードウェアの再配置	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E____ I____ A____
システムソフトウェアの管理：			
オペレーティングシステムパラメータの最適化	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E____ I____ A____
システム変更の計画	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E____ I____ A____

列 A の各タスクごとに、タスク遂行の頻度を示す列 B の文字を丸で囲んでください。 **O**－なし **L**－ひと月に 1 回以下 **M**－毎月 **W**－毎週 **D**－毎日		このタスクの主なトレーニング方法にチェックを付けてください。「その他」の場合は、具体的に記入してください（ワークショップ、試行錯誤など）。	各タスクについて、必要だと思われるトレーニングのレベルを、初級（E）、中級（I）、上級（A）から選び（□）を付けてください。
A	**B**		
システムデフォルトの設定	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E____ I____ A____
新しいオペレーティングシステムカーネルの生成	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E____ I____ A____
システム起動/シャットダウン手順の管理	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E____ I____ A____
コマンドファイルの管理	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E____ I____ A____
更新の有効性のテスト	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E____ I____ A____
システムソフトウェアのインストール	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E____ I____ A____

システムのシャットダウン	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
システムの再起動	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
ソフトウェア一覧の管理	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
システム変更のインストール	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
ベンダー固有のハードウェアのインストール	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
システム更新プログラムまたはパッチのインストール	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
ドキュメントの管理	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
データストレージの管理			
データストレージレイアウトの計画	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____

列 A の各タスクごとに、タスク遂行の頻度を示す列 B の文字を丸で囲んでください。 **O**－なし **L**－ひと月に 1 回以下 **M**－毎月 **W**－毎週 **D**－毎日		このタスクの主なトレーニング方法にチェックを付けてください。「その他」の場合は、具体的に記入してください（ワークショップ、試行錯誤など）。	各タスクについて、必要だと思われるトレーニングのレベルを、初級（E）、中級（I）、上級（A）から選び（□）を付けてください。
A	**B**		
バックアップ手順の計画	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
バックアップ手順のインプリメント	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他	E ____ I____ A____

		_____	
データストレージの使用状況の監視	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
ファイルシステムの完全性の管理	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
ファイルシステムのセキュリティの監査	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
不要なファイルの削除	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
ログファイルの管理	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
データストレージレイアウトの計画管理	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
ストレージメディアの初期化	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
ディスクのパーティション	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
ファイルシステムの作成	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
データのロード	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
バックアップからのデータの回復	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
アプリケーションソフトウェアの管理:			

ソフトウェアパッケージの効果の評価	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E____ I____ A____

列 A の各タスクごとに、タスク遂行の頻度を示す列 B の文字を丸で囲んでください。 **O**－なし **L**－ひと月に 1 回以下 **M**－毎月 **W**－毎週 **D**－毎日		このタスクの主なトレーニング方法にチェックを付けてください。「その他」の場合は、具体的に記入してください（ワークショップ、試行錯誤など）。	各タスクについて、必要だと思われるトレーニングのレベルを、初級（E）、中級（I）、上級（A）から選び（□）を付けてください。
A	**B**		
アプリケーションパラメータの最適化	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E____ I____ A____
アプリケーション変更の計画	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E____ I____ A____
アプリケーション間の互換性の保証	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E____ I____ A____
インストール前のアプリケーションの完全性の検証	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E____ I____ A____
ソフトウェアインストールの有効性のテスト	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E____ I____ A____
アプリケーションソフトウェアのインストール	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E____ I____ A____
一覧管理	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E____ I____ A____
アプリケーションドキュメントの管理	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E____ I____ A____
アプリケーション更新プログラムのインストール	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E____ I____ A____

ネットワーク接続の計画	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
ホスト間接続の要求	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
インターネットアドレスの取得	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
ネットワークケーブルの接続	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
TTY ラインの設定	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
周辺回線の設定	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
列 A の各タスクごとに、タスク遂行の頻度を示す列 B の文字を丸で囲んでください。 **O**－なし **L**－ひと月に 1 回以下 **M**－毎月 **W**－毎週 **D**－毎日		このタスクの主なトレーニング方法にチェックを付けてください。「その他」の場合は、具体的に記入してください（ワークショップ、試行錯誤など）。	各タスクについて、必要だと思われるトレーニングのレベルを、初級（E）、中級（I）、上級（A）から選び（□）を付けてください。
A	**B**		
ファイルサーバーとクライアントの設定	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
ファイアウォールの設定	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
ネットワーク活動の監視	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
ネットワークサービスの管理	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____

ネットワークブリッジとルータの管理	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
プリントサーバーの管理	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
ターミナルサーバーの管理	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
ネットワークトポロジの管理	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
ノードへのアドレスの割り当て	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
ネットワークソフトウェアのインストール	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
アクセス許可の設定	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
ネットワークソフトウェアの起動	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
通信の接続性のテスト	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
ネットワークソフトウェアの停止	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
ホスト接続の再確立	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____

列 A の各タスクごとに、タスク遂行の頻度を示す列 B の文字を丸で囲んでください。 **O**－なし **L**－ひと月に 1 回以下 **M**－毎月 **W**－毎週 **D**－毎日		このタスクの主なトレーニング方法にチェックを付けてください。「その他」の場合は、具体的に記入してください（ワークショップ、試行錯誤など）。	各タスクについて、必要だと思われるトレーニングのレベルを、初級（E）、中級（I）、上級（A）から選び（□）を付けてください。
A	**B**		
監査ガイドライン確立の補佐	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A ____
ユーザーセキュリティガイドラインの策定の補佐	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A ____
システムセキュリティ計画立案の補佐	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A ____
ホストネットワーク認定における補佐	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A ____
出力ラベル処理手順の確認	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A ____
データラベル処理手順の確認	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A ____
セキュリティメカニズムのテストの補佐	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A ____
監査証跡の分析の補佐	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A ____
インシデントハンドリングの補佐	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A ____
セキュリティ手順の実施	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A ____

システムの物理的セキュリティ管理の補佐	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
デバイスのアクセスコントロール管理の補佐	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
セキュリティインシデントのレポート	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
アカウントの管理:			
アカウント管理方針の計画	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
列 A の各タスクごとに、タスク遂行の頻度を示す列 B の文字を丸で囲んでください。 **O**－なし **L**－ひと月に 1 回以下 **M**－毎月 **W**－毎週 **D**－毎日		このタスクの主なトレーニング方法にチェックを付けてください。「その他」の場合は、具体的に記入してください（ワークショップ、試行錯誤など）。	各タスクについて、必要だと思われるトレーニングのレベルを、初級（E）、中級（I）、上級（A）から選び（□）を付けてください。
A	**B**		
ユーザログイン環境の確立	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
必須アクセスコントロール管理における ISSO の補佐	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
アカウント権限の管理	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
アカウント活動の監査	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
アカウントが使用するリソースの管理	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
新しいアカウントの追加	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他	E ____ I____ A____

		_____	
アカウントのアクセスコントロールリストの設定における補佐	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
基本的な運用手順の説明	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
パスワードの変更の補佐	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
アカウントの削除	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
問題のトラブルシューティング：			
問題シナリオの再現	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
エラーメッセージの解釈	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
コンポーネントのテスト	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
問題の隔離	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
問題とソリューションのログの管理	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
システムのクラッシュからの回復	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
ユーザー定義の問題に対する対応	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____

トラブルシューティング情報の収集	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
診断ツールの使用	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
是正措置の開始	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____

第 2 部 タスクのパフォーマンスとトレーニング（続き）：

下の表を使用して、上記で扱われていない他のシステム管理機能で、あなたが行っているものをすべて記入してください。それぞれについて、タスクの実行頻度、任務を遂行するための訓練の主要方法、およびさらなるトレーニングがタスクの遂行に役立つと考えられるかどうかを入力してください。

列 A の各タスクごとに、タスク遂行の頻度を示す列 B の文字を丸で囲んでください。 **O**－なし **L**－ひと月に 1 回以下 **M**－毎月 **W**－毎週 **D**－毎日		このタスクの主なトレーニング方法にチェックを付けてください。「その他」の場合は、具体的に記入してください（ワークショップ、試行錯誤など）。	各タスクについて、必要だと思われるトレーニングのレベルを、初級（E）、中級（I）、上級（A）から選び（□）を付けてください。
A	**B**		
	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____
	O L M W D	__クラスルーム ___ OJT（オンザジョブ） __ 独学 ___ その他 _____	E ____ I____ A____

第 3 部 任務におけるタスクディスカッション:

1. 次の作業が必要ですか。
___ファイアウォールのインストール
___ファイアウォールの運用
___ファイアウォールの管理

2. 質問 1 のいずれかにチェックを付けた場合、具体的に記入してください。
ファイアウォールの数 _____、
ハードウェアの種類 _____、および
ファイアウォールで使用するソフトウェア_____

3. 次のコンポーネントをインストールする必要がありますか。
___ネットワークケーブル
___PC/ワークステーション
___ルータ/ブリッジ Bridges
___セキュリティ関連のハードウェア
___セキュリティ関連のソフトウェア
___その他のソフトウェア

4. あなたの任務では、シェルスクリプトのプログラム方法または記述方法を理解している必要がありますか。
はい　　いいえ
どの言語ですか。_____

5. 昨年、どのような機能/プログラムを作成しましたか。
___ クローンジョブ
___ ログイン機能
___ バックアップ
___ リストア
___ アカウンティング機能
___ その他（具体的に記入してください）_____

6. どのようなスクリプトまたはプログラムを管理していますか。
___ クローンジョブ
___ ログイン機能
___ バックアップ
___ リストア
___ アカウンティング機能
___ その他（具体的に記入してください）_____

7. システムに関する責務を、次の担当者の誰かと分担していますか（それぞれの人数を入力してください）。
___ネットワーク管理者
___データベース管理者
___その他のシステム管理者
___ISSO/ISSM

8. 複数のネットワークを管理していますか。…….. はい　　いいえ

9. システムでは、どのバージョンのどのオペレーティングシステムを使用していますか（Solaris 2.5.1 など）
_____

10. システムセキュリティの責任を担っていますか。…….. はい　　いいえ
「はい」の場合、どのような指示またはポリシーによってその責務が定められていますか。
_____
_____

11. 次のそれぞれに対して、どのような具体的なプログラムを使用していますか。（それぞれについて、その使用があなたの指示または組織によって、オプション（O）か必須（R）かを入力してください）。
ネットワークマッピング_____
侵入検知_____
システムロギング_____
監査機能_____
パスワードチェックまたは強化_____

12. システム管理者として認定されていますか。…….. はい いいえ
「はい」の場合、認定を取得するために受けたトレーニングコースを具体的に記入してください（クラスルーム、CD、CBT など ）。

_____
_____
_____

13. あなたにとって上位5つの情報システムセキュリティトレーニングニーズを挙げてください（それぞれについて、ニーズが初級、中級、上級のどのトレーニングに該当するかを記してください）。

A. _____
B. _____
C. _____
D. _____
E. _____

追加コメント:

_____
_____
_____
_____
_____
_____
_____

アンケートにご協力いただきありがとうございました。

付録 B 意識向上およびトレーニングメトリックの例

重要な要素	13.1 従業員は、セキュリティ上の責任を果たすために適切なトレーニングを受けたことがあるか
部下への質問	13.1.2 従業員のトレーニングおよび専門的能力開発は、文書化され監視されているか。
メトリック	セキュリティ上重要な責任を担う従業員のうち、専門的なトレーニングを受けた従業員のパーセンテージ
目的	組織内の特定のシステムについて、指定されたセキュリティ上の役割およびセキュリティ上の責任を担う従業員の専門知識のレベルを評価するため
プログラム実施の証拠	1. セキュリティ上重要な責任が資格基準で定義され、文書化されているか。 □はい　□いいえ 2. どの従業員がセキュリティ上の専門的な責任を担っているかを記録しているか。 □はい　□いいえ 3. 組織（適用できる場合は組織の構成要素）の中で、何人の従業員が、セキュリティ上重要な責任を担っているか。_____ 4. トレーニング記録がつけられているか（トレーニング記録は特定の従業員が受けたトレーニングを示す）。 □はい　□いいえ 5. トレーニング計画では、専門的なトレーニングが必要であると記されているか。 □はい　□いいえ 6. セキュリティ上重要な責任を持つ担当者のうち何人が、トレーニング計画で述べられた必要なトレーニングを受けたか。_____ 7. トレーニングを受けていない担当者がいる場合、次の中で該当する理由をすべて記入すること。 □資金調達の不足 □時間の不足 □コース利用不可 □従業員の未登録 □その他（具体的に）_____
頻度	最低限年に 1 回
公式	セキュリティ上重要な責任を担う従業員のうち、必要なトレーニングを受けた人数（質問 6）/セキュリティ上重要な責任を担う従業員数（質問 3）

データソース	従業員トレーニング記録またはデータベース、コース終了認定
指標	このメトリックの目標は 100 パーセントである。セキュリティ担当者が適切なトレーニングを受けていない場合、組織には、最新の脅威と脆弱性を撲滅するための準備が整っていない可能性がある。特定のセキュリティコントロールオプションおよびツールは、急速に変化し進化している。継続的なトレーニングによって、必要なセキュリティ情報の可用性を強化できる。 このメトリックは、トレーニングを受けたセキュリティスタッフの増加が、特定のタイプのインシデントおよび無防備な脆弱性の軽減に関連し、この軽減に役立っているかどうかを判断するために、セキュリティインシデント数および対策済みの脆弱性の数との相関関係を調べることができる。

コメント: 質問1と2は、このメトリックの情報の信頼性を測るために使用される。役割と責任は、ポリシーおよび手順で定義する必要があり、その役割を遂行するため担当者を特定する必要がある。質問4と5は、担当者が修了する必要のある専門的トレーニングすべてを明確にするために役立つ情報を提供する。

担当者に十分なトレーニングが行われていない場合、質問7によってその理由が明らかになる。トレーニング不足の原因が不明な場合、管理職はこの不備を正すための是正処置を定めることができる。

付録 C 意識向上およびトレーニングプログラム計画のテンプレート例

概要
背景 ・ OMB A-130、付録 III ・ 連邦情報セキュリティ管理法（FISMA） ・ 特定の部署または連邦機関あるいはその両方のポリシー（意識向上およびトレーニングのプログラムと計画を推進する他の関連情報または基本原理）
組織の IT セキュリティポリシー 最終目標 達成目標 役割/責任
意識向上 対象者（管理職および全従業員） 活動および目標期日 スケジュール マテリアルおよび方法のレビューと更新
トレーニング/教育 役割 1: 幹部およびマネージャ 学習目標 対象領域 方法/活動 スケジュール 評価基準 役割 2: IT セキュリティスタッフ 学習目標 対象領域 方法/活動 スケジュール 評価基準 役割 3: システム/ネットワーク管理者 学習目標 対象領域 方法/活動 スケジュール 評価基準 . . . および IT セキュリティ上重要な責任を担うその他の役割

専門的認定

役割 1:　IT セキュリティスタッフ
- 学習目標
- 対象領域
- 方法/活動
- スケジュール
- 評価基準

役割 2:　システム/ネットワーク管理者
- 学習目標
- 対象領域
- 方法/活動
- スケジュール
- 評価基準
- . . . および IT セキュリティ上重要な責任を担うその他の役割

リソース要件	**コスト**
要員確保	$ xxx
契約サポート	$ xxx
設備（トレーニングルーム、遠隔会議設備など）	$ xxx
メディア（Web ベースおよびコンピュータベースのマテリアル用のサーバー）	$ xxx

付録 D 意識向上ポスターの例