令和7年度
中小企業サイバーセキュリティ
実践力強化プログラム

第10回

第11編：　生成AIおよびAIマネジメントシステム
第12編：　全体総括

東京都産業労働局

講師紹介

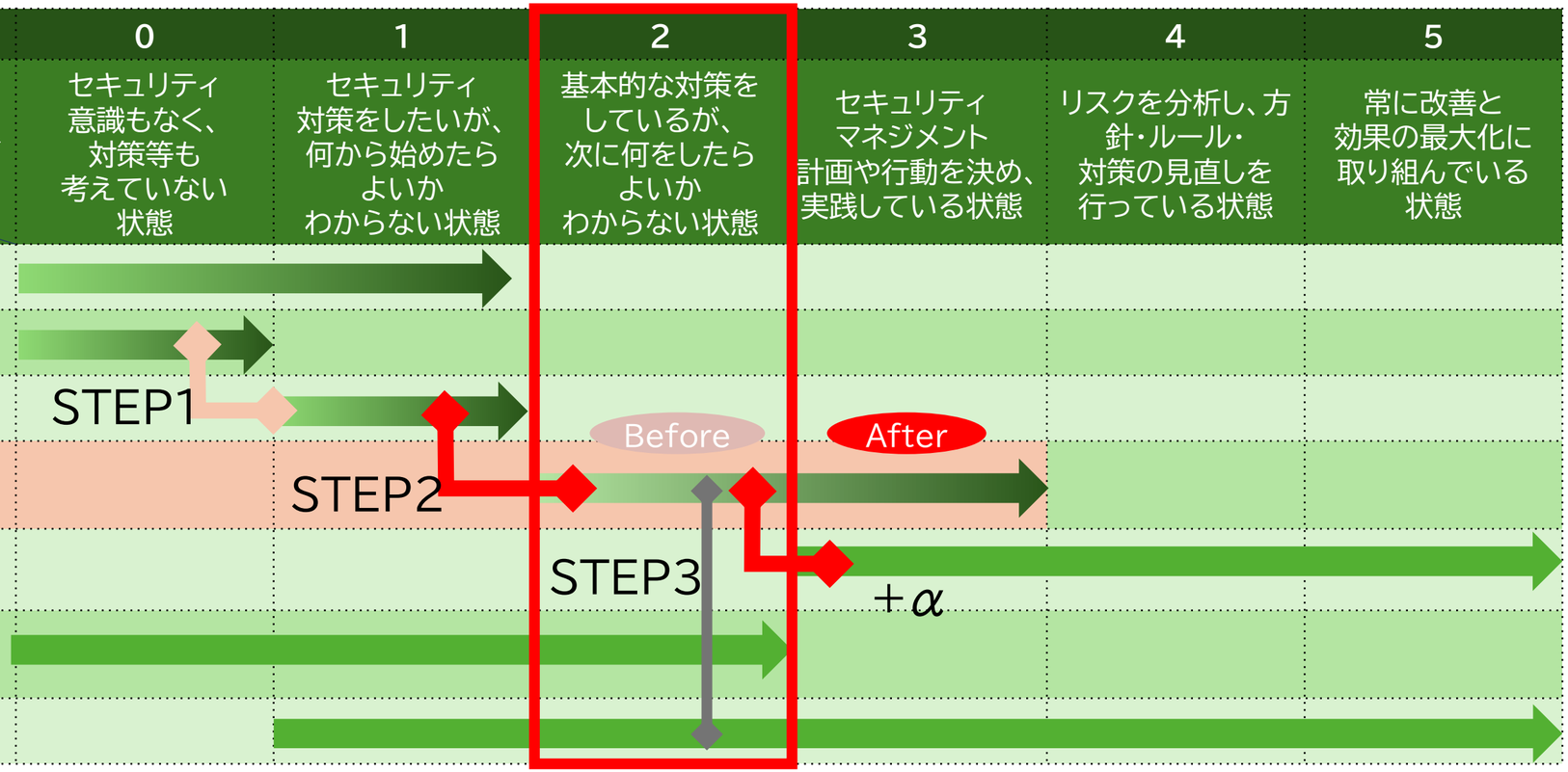
氏名	矢野　泰広（やの　よしひろ）
業務経歴	26年（セキュリティ経験：15年）
専門分野	情報セキュリティ、DX、ICT、クラウド技術、 ネットワーク技術、DB設計・構築、プロジェクト マネジメント、WEBシステム設計・構築、 サーバ設計・構築
保有資格	情報処理安全確保支援士（第004005号） 経済産業省認定 情報処理技術者試験 プロジェクトマネージャ、 情報処理技術者第一種、情報処理技術者第二種 インターネット検定 .com Master ADVANCE★★ 生成AIパスポート 家電製品アドバイザー（AV情報家電・生活家電）
コメント	中小企業を中心にDX、ネットワーク、クラウド技術および情報セキュリティに関する構築や導入支援やコンサルティングの経験が豊富。併せて長年にわたり大手通信事業者のSE（技術営業）を対象に指導を行ってきた事から、幅広い業種、業態の企業の状況を認識しており、中小企業の課題点を的確に捉え、各企業が取り組みやすい解決策を提示する対応力に定評がある。

目的

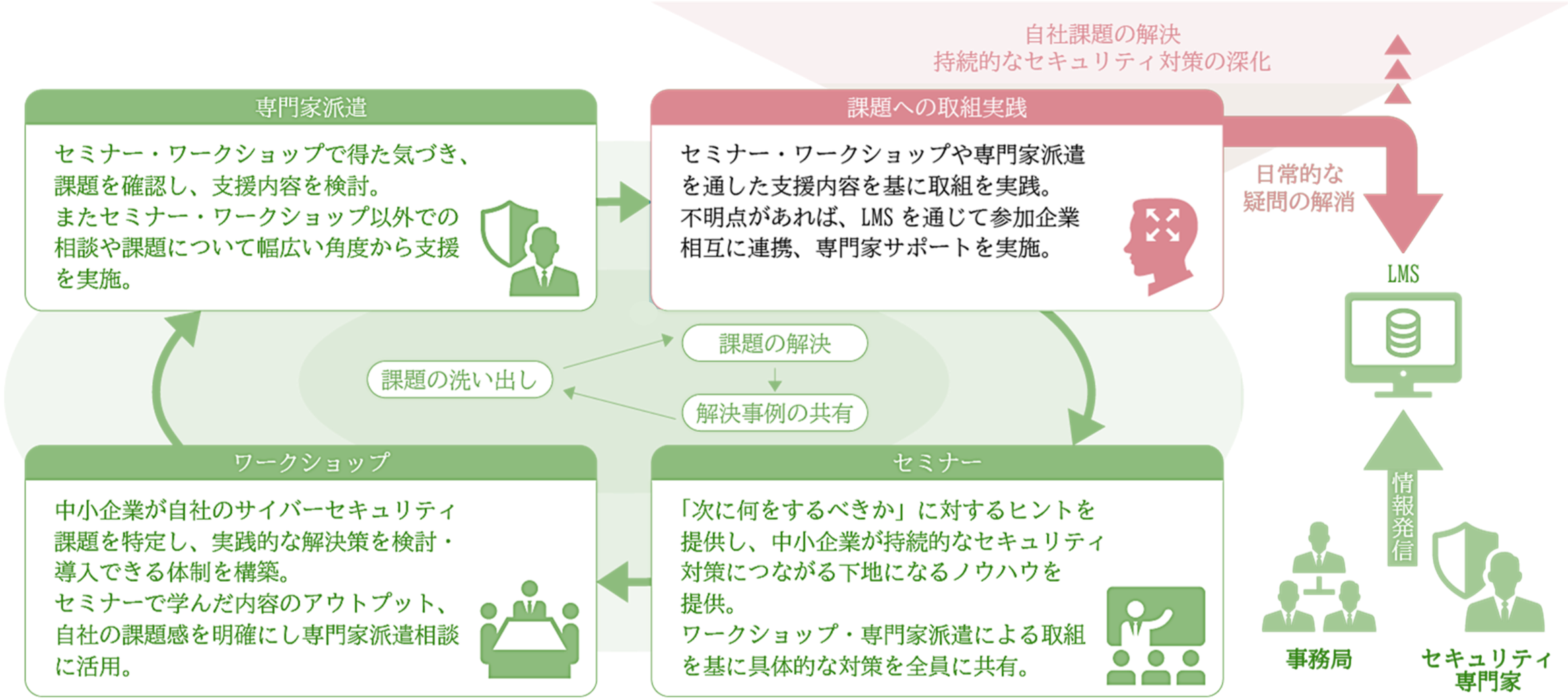
- 継続的なセキュリティ対策の実施を支援する。
- 人材の育成と実践的な課題解決を通じて、サプライチェーン全体のセキュリティ強化を図る。

東京都他事業と本事業の位置づけ

成熟度レベル　※COBITを援用し設定	0	1	2	3	4	5
ステータス / 事業と主な支援領域	セキュリティ意識もなく、対策等も考えていない状態	セキュリティ対策をしたいが、何から始めたらよいかわからない状態	基本的な対策をしているが、次に何をしたらよいかわからない状態	セキュリティマネジメント計画や行動を決め、実践している状態	リスクを分析し、方針・ルール・対策の見直しを行っている状態	常に改善と効果の最大化に取り組んでいる状態
中小企業サイバーセキュリティの極意						
中小企業サイバーセキュリティ 啓発事業						
中小企業サイバーセキュリティ 基本対策事業						
中小企業サイバーセキュリティ実践力強化プログラム（本事業）						
中小企業サイバーセキュリティインシデント対応力強化						
Tcyss（東京中小企業サイバーセキュリティ支援ネットワーク）						
サイバーセキュリティ対策促進助成金						



支援内容の全体像


自社課題の解決
持続的なセキュリティ対策の深化
専門家派遣
セミナー・ワークショップで得た気づき、課題を確認し、支援内容を検討。
またセミナー・ワークショップ以外での相談や課題について幅広い角度から支援を実施。
課題への取組実践
セミナー・ワークショップや専門家派遣を通した支援内容を基に取組を実践。
不明点があれば、LMS を通じて参加企業相互に連携、専門家サポートを実施。
日常的な
疑問の解消
LMS
課題の解決
課題の洗い出し
解決事例の共有
ワークショップ
中小企業が自社のサイバーセキュリティ課題を特定し、実践的な解決策を検討・導入できる体制を構築。
セミナーで学んだ内容のアウトプット、自社の課題感を明確にし専門家派遣相談に活用。
セミナー
「次に何をするべきか」に対するヒントを提供し、中小企業が持続的なセキュリティ対策につながる下地になるノウハウを提供。
ワークショップ・専門家派遣による取組を基に具体的な対策を全員に共有。
情報発信
事務局
セキュリティ専門家

スケジュール

支援内容	7月	8月	9月	10月	11月	12月	1月	2月	3月
セミナー・ワークショップ（全10回）	7/25（金）	8/8（金）	8/27（水）	9/11（木）	9/25（木）	10/10（金）	10/27（月）	11/17（月）	12/12（金）	1/16（金）		
専門家派遣（全4回）	1回目		2回目		3回目			4回目				
事例集								ご参加いただいた企業様への取材	事例集作成期間	公表3月下旬～		

セミナー内容

実施回	編	テーマ
第1回 7/25 （金）	第0編	はじめに
	第1編	サイバーセキュリティを取り巻く背景
	第2編	中小企業に求められるデジタル化の推進とサイバーセキュリティ対策
第2回 8/8 （金）	第3編	これからの企業経営に必要なIT活用とサイバーセキュリティ対策
	第4編	セキュリティ事象に対応して組織として対策すべき対策基準と具体的な実施
	第5編	各種ガイドラインを参考にした対策の実施

セミナー内容

実施回		編	テーマ
第3回	8/27(水)	第6編	ISMSなどのフレームワークの種類と活用法の紹介
第4回 第5回	9/11(木) 9/25(木)	第7編	ISMSの構築と対策基準の策定と実施手順
第6回 第7回	10/10(金) 10/27(月)	第8編	具体的な構築・運用の実践
第8回	11/17(月)	第9編	中小企業が組織として実践するためのスキル・知識と人材育成
第9回	12/12(金)	第10編	サイバーレジリエンス能力の育成
第10回	2026年 1/16(金)	第11編	生成AIおよびAIマネジメントシステム
		第12編	全体総括

第28章. IT-BCPの一環としてのインシデントに対応する体制

情報システム継続計画（IT-BCP）の基本要素と体制
インシデント対応体制の確立と初動対応の具体的手順
復旧・回復プロセスと教訓の反映（継続的改善）
サイバーレジリエンス能力向上のための実践的な演習と訓練

サイバーレジリエンス能力向上のための実践的な演習と訓練

【参照:テキスト28-4.】 P2～P4

サイバーレジリエンス能力向上のための演習と訓練

　文書化された IT-BCP／IRP を実効的にするには、定期的な訓練・演習が必須であり、訓練は、計画の有効性検証、役割の明確化、習熟度向上に直結する。

対象別の訓練の推奨

- 経営層向け:　　サイバーリスク判断や対外説明のシミュレーション訓練
- 実務担当者向け:　CYDER・RPCIなどの実践的演習で封じ込め・復旧手順を習得

人材育成の統合

- 非専門人材も初期対応（報告・連絡・封じ込め補助）を行えるよう、「プラス・セキュリティ」などの基礎教育を継続する
- 中小企業では、これが外部専門家との橋渡し役として重要である

サイバーレジリエンス能力向上のための実践的な演習と訓練

【参照:テキスト28-4.】P2～P4

IT-BCPにおけるインシデント対応(IR)体制の実践ステップと教訓の反映

ステップ	実践内容の概要 (サイバーレジリエンス視点)	サイバーレジリエンス能力への貢献
準備・計画 (Plan)	IT-BCP/IRP策定、RTO/RPO設定、体制構築、演習実施	事態発生時の対応能力と迅速性の確保
検知・分析 (Detect/Analyze)	脅威の早期検知と影響範囲の特定、ログ保全	被害拡大の防止(封じ込め)
復旧・回復 (Recover)	システムの復元、サービス再開、恒久対策の実施	タイムリーな事業の再開
改善・教訓 (Improve)	事後評価に基づく再発防止策の実施、ポリシー改訂、訓練見直し	組織全体のレジリエンス向上と適応性の獲得

サイバーレジリエンス能力向上のための実践的な演習と訓練

【参照:テキスト28-4.】P2～P4

訓練・教育のおける定着のための実践的な手順

訓練・教育の実施方法

- 組織の成熟度に合わせて 机上 → 模擬 → 外部演習 を段階的に導入する
- 訓練目的・対象・頻度(年1回以上)を明確化する

訓練結果の活用

- 訓練後は評価表で改善点(連絡体制・判断・文書整合性)を整理する
- 結果を IT-BCP に添付し、次回改善サイクルへ反映 → レジリエンス向上に直結する

外部支援の活用

- IPA:サイバー演習教材・CYDER
- NCO:演習モデル・訓練シナリオ
- 地域組織:商工会等との合同訓練

外部支援の活用で、小規模でも現実的な訓練環境を構築できる。

第29章.生成AIおよびAIマネジメントシステム

AIの進化とガバナンス・リスクマネジメントの喫緊性
AIガバナンスの国際標準：ISO/IEC 42001の全貌
AIに特有のリスクの特定と体系的な管理
ISO/IEC 42001に基づくAIマネジメントシステムの構築と運用
認証取得の動向と先進企業の事例
AI時代の持続可能な成長に向けた戦略的活用

AIの進化とガバナンス・リスクマネジメントの喫緊性

【参照：テキスト29-1.】
P7～P8

AI普及に伴うリスク

　AIにはバイアス、プライバシー侵害、セキュリティリスク、倫理問題が内在しており、自動判断の不透明性や説明困難性は、従来技術より高度な管理を必要としている。また、生成AIでは、誤情報生成、著作権侵害、機密漏洩、攻撃者による悪用といった具体的リスクが顕在化している状況である。

世界的な規制動向とISOの役割

- 欧州AI法（EU AI Act）、NIST AI RMF、米国大統領令など、AI関連規制が各国で急速に整備されている
- ISO/IECは、AIリスク管理と信頼性向上のため国際規格（ISO/IEC 42001）を策定した
- 国際標準は、共通理解の形成と国際取引の円滑化に寄与する

AIの進化とガバナンス・リスクマネジメントの喫緊性

【参照：テキスト29-1.】
P7～P8

AI普及に伴うリスク

AIリスクの複雑性と企業が直面する課題

- AIリスクは技術にとどまらず、社会・倫理・経済など及ぼす効果が多面的である
- 統一的な国際規制は未整備で、各国が異なるリスクアプローチを採用している
- 技術進化が規制を上回るため、企業は 複数の規制への同時対応が必要である

ISO/IEC 42001の意義

- 多様な規制環境下において「AIのガバナンス」「リスク管理」「倫理的配慮」を体系化した国際規格である
- AI導入では、技術力に加え、どの規制に準拠し、どの社会的影響を考慮するかという高度なガバナンス戦略が不可欠である

AIガバナンスの国際標準：ISO/IEC 42001の全貌

【参照：テキスト29-2.】
P9～P11

ISO/IEC 42001とは：AIマネジメントシステム（AIMS）の目的と特徴

2023年に発行された世界初のAIマネジメントシステム規格であり、AIの設計・開発・運用におけるリスク最小化と倫理的・安全なAI活用を目的とした枠組みとなっている。また、企業がAIを「信頼性・透明性・安全性」をもって運用するための国際基準になる。

導入によるメリット（ポイント）

- 信頼性向上：　国際標準準拠を示し、顧客・取引先の信頼を獲得できる
- リスク管理強化：　バイアス・プライバシー・セキュリティなどAI特有リスクを体系的に管理できる
- 規制対応の容易化：EU AI Act 等、多様な国際規制への適合性を高める
- 競争力強化：　認証取得が差別化要因となり、先行優位を確保できる
- ガバナンス確立：　AIの責任体制・プロセスが組織に浸透させられる
- コスト最適化：　効率的な開発とリスク回避で長期的な費用を削減できる

AIガバナンスの国際標準：ISO/IEC 42001の全貌

【参照：テキスト29-2.】
P9～P11

既存のマネジメントシステム規格（ISO 9001など）との整合性

ISO/IEC 42001は ハイレベルストラクチャー（HLS） を採用し、ISO 9001、ISO/IEC 27001、ISO 27701 などと構造が共通であるため、既存のISOを持つ組織は、統合しやすく導入負荷が低いと言える。
※次ページにて図示

▼ 特筆すべきISO/IEC 27001との相乗効果

- 情報セキュリティ管理とAIガバナンスを一体化でき、プロセスの合理化ができる
- 既存の管理手順・文化・専門知識を AIガバナンスに直接応用できる

組織へのメリット（整合性がもたらす効果）

- AI管理を既存の体制に統合することで、効率的なAIガバナンス強化を実現できる
- 部門間の分断を防ぎ、組織全体で一貫したリスクマネジメントを構築できる
- AI導入における国際競争力や信頼性向上に寄与する

AIに特有のリスクの特定と体系的な管理

【参照：テキスト29-3.】
P12～P16

AIがもたらす主なリスクの種類と影響

AIには バイアス、プライバシー侵害、セキュリティ、透明性、責任、教育、競争、公正性、環境など多面的なリスクが存在する。

日本の「AI事業者ガイドライン」は「人間中心のAI社会原則（7つの原則）」をもとに、AIで想定されるリスクを10の原則に細分化しており、項目は次の通りである。

①人間中心	②安全性	③公平性	④プライバシー保護
⑤セキュリティ確保	⑥透明性	⑦アカウンタビリティ	
⑧教育・リテラシー	⑨公正競争確保	⑩イノベーション	

生成AIの追加リスク

- 著作権侵害
- 機密情報漏えい
- 攻撃者の悪用（フィッシング・マルウェア生成）

AIに特有のリスクの特定と体系的な管理

【参照：テキスト29-3.】
P12～P16

ISO/IEC 42001におけるリスクベースアプローチの原則

ISO/IEC 42001は、AIを安全に活用するためのリスクベースアプローチを中核とする国際規格である。

組織に求められる体系的な実施

- AIリスクの特定・分析・評価
- 適切な管理策の選択と実施
- 38の管理策・10の管理目標に基づく統合的管理

  38の管理策・10の管理目標に基づく統合的管理は、AIの特性（用途・影響度）に応じて柔軟に管理策を適用するため、過剰規制を避けつつ高リスクを重点管理できる。

AIに特有のリスクの特定と体系的な管理

【参照:テキスト29-3.】
P12～P16

AIリスクアセスメントと影響度評価の具体的な実践

- AIリスクアセスメント
  バイアス、誤判断、プライバシー侵害、外部要因を分析する
- 影響度評価
  個人・社会・経済への影響(人権・情報漏えい・雇用など)を判断する
- 定性・定量手法を組み合わせ、不確実な領域にも対応している
- 対応策は回避・低減・共有・保有などから選択できる

ISO 31000(リスクマネジメントの指針)との連携と活用

- ISO 31000はリスクマネジメントの国際指針(原則・枠組み・プロセス)である
- 「リスク特定→分析→評価→対応→モニタリング」の一連の流れが体系化されている
- AIリスクに対する事前管理・損失最小化・文書化が強化できる
- ISO/IEC 42001の実践において、ISO 31000は包括的な基盤として機能する

ISO/IEC 42001に基づくAIマネジメントシステムの構築と運用

【参照:テキスト29-4.】 P17～P22

主要な要求事項と管理策(Annex Aの活用)

ISO/IEC 42001はAIマネジメントシステム(AIMS)の要求事項を定義しているおり、主な要求事項は以下の通り。

- 組織の文脈:　内部・外部環境、利害関係者ニーズ、AI目的の整理
- リーダーシップ:　責任・権限・AI文化の推進
- 計画:　AIリスク・機会の特定、リスク対応計画
- サポート:　要員・スキル・認識・文書化
- 運用:　AIシステム導入・データ管理・モニタリング・リスク管理
- パフォーマンス評価:　監視・測定・レビュー
- 改善:　評価結果に基づく継続的改善

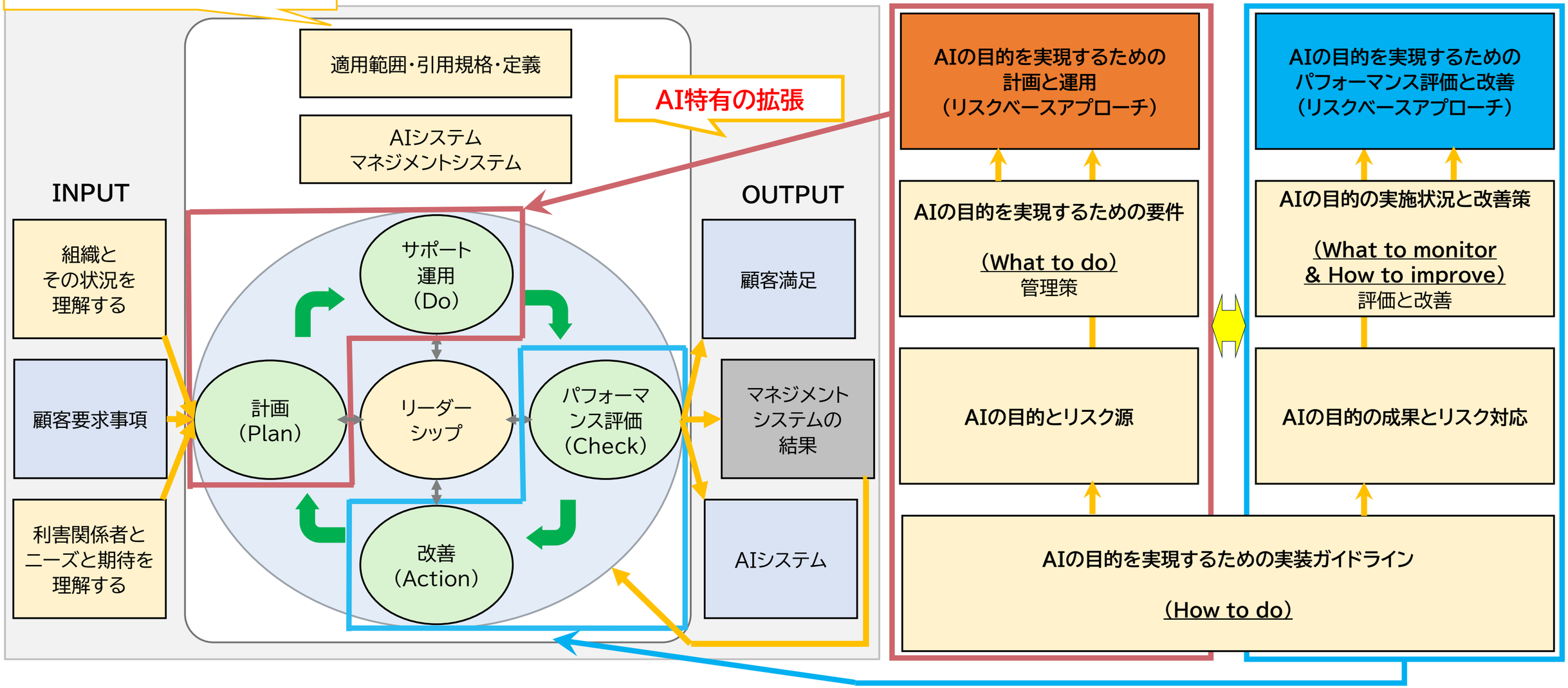
また、Annex Aでは具体的な管理策の一覧を示し、ガバナンス、リスク管理、データ・アルゴリズム管理、透明性・説明責任、監視・改善といった観点で、AIの安全・公正・説明可能な運用を支える指針となっている。

図：AIマネジメントシステムの構成

本文の基本構成とアプローチは
他のマネジメントシステムと同様

【参照：テキスト29-4.】P17～P22

図1. AIマネジメントシステムの構成
経済産業省「AIマネジメントシステムの国際規格が発行されました　安全・安心なAIシステムの開発と利活用を目指して（ISO/IEC 42001）」をもとに作成



ISO/IEC 42001に基づくAIマネジメントシステムの構築と運用

【参照:テキスト29-4.】P17～P22

導入プロセスと実践的なステップ

ISO/IEC 42001導入の一般的な流れ

- ギャップ分析
  現状のAI利用と管理レベルを把握し、不足点を洗い出す
- AIMSの設計・統合
  既存プロセス上にAIマネジメントの枠組みを構築する
- リスク・影響度評価の定期実施
  AIリスクと影響を継続的に評価する
- AI方針・手順の制定
  倫理・プライバシー・データ保護などを網羅する
- プロセスの文書化
  要求事項への適合を示せる記録を整備する
- 外部監査への準備・認証取得
  その後も法令・規制の変化に応じて更新し、内部監査・教育を継続する

ISO/IEC 42001に基づくAIマネジメントシステムの構築と運用

【参照:テキスト29-4.】 P17～P22

既存システムとの統合と効率的な導入

- ISO 9001、ISO/IEC 27001と構造が共通(HLS)で統合しやすい
- プロセスの重複を削減し、コスト・期間の短縮が可能である
- 部分導入(AIリスクアセスメントのみ等)も柔軟に実施できる

導入における課題と解決策

課題

- コスト・専門人材不足、継続運用に対する負荷、柔軟性低下の懸念

解決策

- 段階的導入:リスクアセスメント等、重要要素から順に導入
- 既存ISOシステムとの統合で負荷軽減
- 外部専門家の活用及び経営層コミットメントの強化

第30章. エグゼクティブサマリー

全体要旨

テキストの活用ポイント

全体要旨

【参照:テキスト30-1.】
P25～P27

テキストの概要

第1編　サイバーセキュリティを取り巻く背景【レベル共通】

（第1章～第4章）

サイバーセキュリティを取り巻く背景として、デジタル化が進む社会と情報技術（IT）活用の動向を解説し、基本的なサイバーセキュリティ知識やUTM・EDRの活用を振り返りました。また、サイバーセキュリティの脅威に対処する段階的なアプローチ方法を明確にするとともに、サイバーセキュリティ戦略に関連する国の方針と関連法令、セキュリティ確保とDX推進の両立の必要性について解説しました。

第2編　中小企業に求められるデジタル化の推進とサイバーセキュリティ対策【レベル共通】

（第5章～第6章）

実際のインシデント事例を通して、近年のサイバー攻撃の傾向や対策などを紹介しました。これからの企業経営で必要な観点となる社会の動向、「守りのIT投資」や「攻めのIT投資」などのIT投資や、経営投資としてのセキュリティ対策の重要性を説明しました。

全体要旨

【参照:テキスト30-1.】
P25～P27

テキストの概要

第3編　これからの企業経営で必要なIT活用とサイバーセキュリティ対策【レベル共通】（第7章～第8章）

ISMS認証を前提としたセキュリティ対策における基準を3段階にレベル分けし、それぞれのアプローチ手法について解説しました。さらに、ISO/IEC 27000に記述されている「リスク」、「脅威」、「脆弱性」、「管理策」といった用語の定義とそれらの関係性、脅威や脆弱性の識別方法を説明しました。

第4編　セキュリティ事象に対応して組織として策定すべき対策基準と具体的な実施【レベル1】（第5章～第6章）

実際のセキュリティインシデントの事例を踏まえ、自社での発生可能性や被害規模を慎重に検討し、対策基準や実施手順を策定していく手法である、Lv.1クイックアプローチについて解説しました。

第5編　各種ガイドラインを参考にした対策の実施【レベル2】（第10章）

ガイドラインやひな型など既存の手法を参考にして対策基準や実施手順を策定する手法である、Lv.2ベースラインアプローチについて解説しました。

全体要旨

【参照:テキスト30-1.】
P25～P27

テキストの概要

第6編　ISMSなどのフレームワークの種類と活用法の紹介【レベル3】

（第11章～第12章）

サイバーセキュリティ対策における代表的なフレームワーク（ISMS、CSF2.0、CPSFなど）の概要と、リスクマネジメントやリスクアセスメントの手法、リスク対応の考え方について説明しました。

第7編　ISMSの構築と対策基準の策定と実施手順【レベル3】

（第13章～第19章）

ISMSのフレームワークを用いて、体系的・網羅的にセキュリティ対策基準、実施手順を作成するLv.3網羅的アプローチについて説明しました。ISMSの管理策（組織的、人的、物理的、技術的管理策）をもとに、対策基準を策定する手順と、策定した対策基準をもとに具体的な実施手順を策定する方法を説明しました。最後に、内部・外部監査によるセキュリティ対策の有効性評価について解説しました。

全体要旨

【参照:テキスト30-1.】
P25～P27

テキストの概要

第8編　具体的な構築・運用の実践【レベル3】

（第20章～第21章）

デジタル・ガバメント推進標準ガイドラインなどが示すサービスシステム構築と運用の工程を参考に、中小企業においても有効な情報システムを導入する流れと、セキュリティ対策の実装と運用ポイントを説明しました。ECサイトを例にとり、企画から要件定義、調達、設計・開発、運用保守までの流れと、セキュリティ機能の実装方法を解説しました。

第9編　組織として実践するためのスキル・知識と人材育成【レベル共通】

（第22章～第25章）

各種スキル標準のフレームワークをもとに、必要とされる新しいスキルや知識、ITおよびデジタル人材のスキル、知識の認定制度について解説するとともに、必要な知識やスキルを備えた人材の育成・確保のために、関係機関が公表しているセキュリティ関連のカリキュラムを紹介しました。また紹介したカリキュラムなどを活用して教育・研修計画を作成する方法を解説しました。

全体要旨

【参照:テキスト30-1.】
P25～P27

テキストの概要

第10編　サイバーレジリエンス能力の育成【レベル共通】

（第26章～第28章）

サイバー攻撃やシステム障害などの事態が発生した場合でも事業を継続し、速やかに復旧・改善するために必要となるサイバーレジリエンス能力について解説しました。従来の侵入防止を中心とした対策に加え、インシデント対応計画やIT-BCPを含めた対応・復旧・改善の考え方を整理し、中小企業において段階的に取り組むための実践的な方向性を解説しました。

第11編　生成AIおよびAIマネジメントシステム

（第29章）

生成AIの利活用が進展する中で、企業が留意すべきリスクとガバナンスの考え方について解説しました。ISO/IEC 42001などの国際標準を参考に、情報セキュリティ、法令遵守、倫理を含めたAIマネジメントシステムの基本的な枠組みを整理し、組織として適切に生成AIを管理・運用するための方向性を説明しました。

テキスト活用のポイント

【参照:テキスト30-2.】
P28～P32

1. ポイントの再認識
   - DX推進の考え方の把握:＜テキストP28～29参照＞
   - セキュリティ対策の全容の認識:＜テキストP29参照＞
   - 自組織でのセキュリティ対策の実施項目の認識:＜テキストP30参照＞
   - 自組織としての実践準備:＜テキストP30～31参照＞

2. 関係者との共有
   ＜テキストP31参照＞
3. 社内体制の確立
   ＜テキストP31～32参照＞
4. セキュリティ対策の実践
   ＜テキストP32参照＞

第31章. 各章のポイント

各章のポイント

各章のポイントを整理し、具体的な知識やスキルを振り返ることを目的としています。

＜テキストP34～P112参照＞

第32章. 今後実施すべきこと

今後のアクション

今後のアクション

【参照:テキスト32-1.】
P114～P123

本テキストの内容を実践するために行うべき事項

**テキストに記載された各章の理解を深め、
経営者を含めた関係者と共有すること**

- 各章のポイントの理解
- DX推進の考え方の把握
- セキュリティ対策全容の認識
- 自組織でのセキュリティ対策の実施項目の認識

1. リスクアセスメントによって自組織の現状のリスクを把握する。
2. リスクアセスメントの結果を踏まえ、管理策の中から自組織として実施すべき項目を選定する。
3. 実施する管理策に関して、自組織としての実施手順を策定する。

今後のアクション

【参照:テキスト32-1.】
P114～P123

経営者のリーダーシップによって、社内体制を整備すること

- 実施手順の実行準備
- 実施手順の実行
  1. 組織体制と役割の決定
  2. 年間を通して実行すべき事項の例示

- リスクアセスメントの実施、リスク対応のための計画作成、管理策の検討
- 資産台帳の見直し
- 事業継続に関する試験
- 内部監査
- マネジメントレビュー
- 不適合及び是正処置のレビュー
- 定期教育
- 外部審査
- 情報セキュリティのための方針群のレビュー
- 秘密保持契約書の確認
- 「関係当局との連絡」体制の見直し
- 法令規制一覧表の確認
- 運用チェックリストによる確認
- 入退記録の確認
- など

実施するための年間計画を作成する

今後のアクション

【参照:テキスト32-1.】
P114～P123

Fit&Gap分析

1. 現状分析
2. SaaS、パッケージソフトウェアの機能調査
3. 比較分析
4. ギャップへの対応策検討
5. 費用対効果の分析
6. 実施計画の策定

非機能要件におけるセキュリティ要件の決め方

1. 情報システムで取扱う情報資産に対し、リスクアセスメントを実施する。
2. リスクアセスメントの結果をもとに、必要な管理策を決定する。
3. セキュリティ要件を決定する。

今後のアクション

【参照:テキスト32-1.】
P114～P123

管理策を実施するための参考となる情報

- ISO/IEC 27002:2022対応 情報セキュリティ管理策実践ガイド
- ISMS推進マニュアル－活用ガイドブック ISO/IEC 27001:2022対応
- JISC「JIS Q 27000 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語」
- ISO/IEC 27002:2022

取組例

対策基準（例）	5.2情報セキュリティの役割及び責任	5.5関係当局との連絡	6.7リモートワーク	8.15ログ取得
実施手順（例）	情報セキュリティ委員会を設置する。	関係当局およびその連絡先を「連絡先一覧表」に特定し、必要時に容易に連絡がとれる体制を確立・維持する。	社内ネットワークへはVPNにて接続する。	バックアップが確実に行われており、障害時に復元が可能かどうかを月に1度チェックする。
トップマネジメント（経営層）	○	ー	○	ー
情報セキュリティ委員会	ー	○	○	ー
情報システム管理者	ー	ー	○	○
一般社員	ー	-	○	ー

今後のアクション

【参照:テキスト32-1.】
P114～P123

セキュリティ対策を考慮した情報システムを導入するために参考となる情報

＜テキストP119～120参照＞

継続的な情報収集

＜テキストP120～P122参照＞

人材育成を実施するために参考となる文献

＜テキストP122～P123参照＞

令和7年度
中小企業サイバーセキュリティ
実践力強化プログラム

東京都産業労働局