# 令和6年度
# 中小企業サイバーセキュリティ
# 社内体制整備事業

**第9回**

**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】**

# セミナー内容

| 編 | テーマ |
| --- | --- |
| 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

| 編 | テーマ |
| --- | --- |
| 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7編 | ISMSの構築と対策基準の策定と実施手順 |
| 第8編 | 具体的な構築・運用の実践 |
| 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 |
| 第10編 | 全体総括 |

# セミナー内容

## 第24章. 各種人材育成カリキュラム

## 第25章. スキルと知識を持った人材育成・人材確保方法

# 第24章. 各種人材育成カリキュラム

## プラス・セキュリティ知識補充講座 カリキュラム例
## ITスキル標準モデルカリキュラム【ITスキル標準V3（レベル1）】
## マナビDX

# プラス・セキュリティ知識補充講座

【参照：テキスト24-1.】
P3

## カリキュラム構成と目標

### 経営層（経営層全体）

- サイバーセキュリティ動向が自社リスクに与える影響を正確に把握する
- リスクを考慮して、セキュリティ体制や投資を適切に決定・指示する
- インシデント時に迅速で適切な経営判断と指示を行う

### デジタル化推進部門の部課長級マネジメント層

- サイバーセキュリティの動向が自部署や事業に与える影響を正確に理解する
- 自部署で実施中のセキュリティ対策の状況を把握する
- 経営層が適切な判断をできるよう、影響と現状を説明・報告する
- 社内外（情報システム部門やベンダー）とスムーズにコミュニケーションを取る

# プラス・セキュリティ知識補充講座

【参照：テキスト24-1.】
P4

## 対象別の目標・到達レベル

| | 理解 | コミュニケーション | 評価・分析 | 判断 |
|---|---|---|---|---|
| 高 | 自らの役割に必要な知識を概ね網羅的に習得し、理解している | 自ら把握すべきことを洗い出し、専門家を含む適切な対象者に回答を求めることができる | 脅威や脆弱性が自組織に及ぼす影響を評価できる | 自らの知識のみで、自組織での対応に関する適切な判断ができる |
| **中** | **自らの役割に必要な知識の全体像を把握した上で、その一部について理解していることを自覚している** | **専門家との意見交換ができる** | **脅威や脆弱性がどのように自組織に影響を及ぼすのかを理解できる** | **専門家の判断について、根拠を理解して合意を与えることができる** |
| 低 | サイバーセキュリティ関連文書に用いられる用語の意味を理解している | 専門家からの説明を概ね理解することができる | 脅威や脆弱性とは何かを理解している | 自らの知識のみでは判断に関与することが困難 |

# プラス・セキュリティ知識補充講座

【参照：テキスト24-1-1.】
P5～P7

## 経営層向けカリキュラム例

| 単元 | 目標 | 到達レベル |
|---|---|---|
| 1．基礎知識 | 経営層として、提案や施策の妥当性を判断するために必要な知識を習得する | 関係者との円滑なコミュニケーションができる程度の概念と用語を理解する |
| 2．脅威と対策 | 主要な脅威を事業リスクとして適切に把握する能力を身につける | 脆弱性が完全に排除できないことを理解し、最新の脅威への対応と被害想定を行う力を養う |
| 3．投資 | セキュリティリスクが企業価値に与える影響を理解し、適切な対策と投資を判断する | • リスクを特定し、優先順位を設定して、必要な体制や人材を確保・育成する<br>• 提示されたセキュリティ対策案の妥当性を経営層として判断する |
| 4．ステークホルダーとの関係 | インシデント対応を理解し、企業価値を守るための準備を具体的にイメージする | 対策方針について外部と意見交換や説明ができるレベルの理解を持つ |

# プラス・セキュリティ知識補充講座

【参照：テキスト24-1-2.】
P7～P9

## 部課長向けカリキュラム例

| 単元 | 目標 | 到達レベル |
|---|---|---|
| １．基礎知識（初級編） | 部門管理者として必要なデジタル化推進に関する最低限の知識を学ぶ | デジタルシステムやインターネットのセキュリティ対策に関する基本知識を身につける |
| １．基礎知識（中級編） | 部門管理者として適切な判断を行うために必要な知識を認識する | サイバーセキュリティに関する基本的な用語と概念を習得し、ベンダーと実務的な対話ができるレベルに達する |
| ２．脅威と対策 | 主要な脅威を事業リスクとして適切に理解する能力を身につける | 脆弱性を完全には排除できないことを理解し、最新の脅威への対応と被害の想定を行えるようになる |

# プラス・セキュリティ知識補充講座

【参照：テキスト24-1-2.】
P7～P9

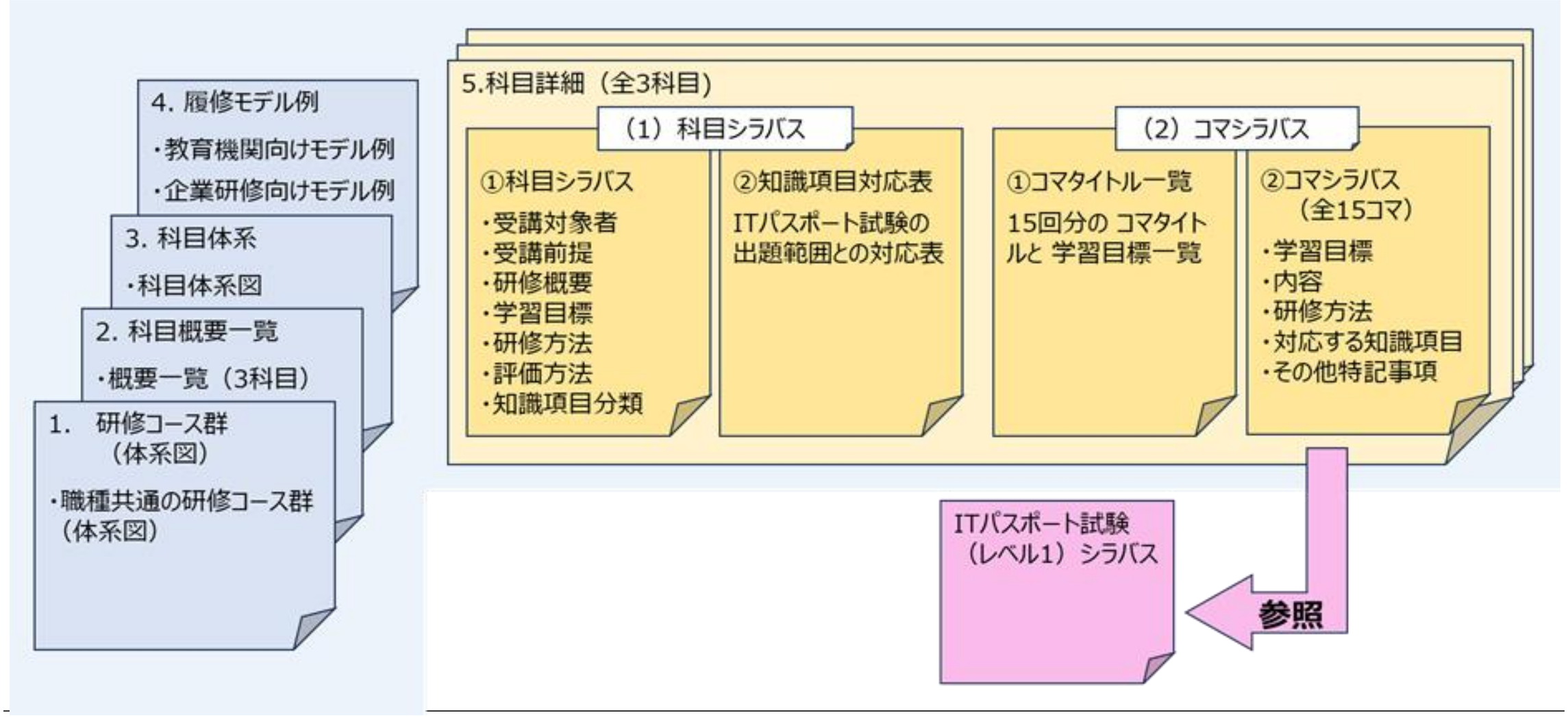
## 部課長向けカリキュラム例

| 単元 | 目標 | 到達レベル |
|---|---|---|
| ３．投資 | サイバーセキュリティリスクの管理に必要な概念と具体的な行動を理解する | • 部署のリスクを特定し、優先順位を設定し、体制や要員の確保・育成を進める<br>• 提示されたセキュリティ対策案の妥当性を判断する能力を持つ |
| ４．ステークホルダーとの関係 | サイバーセキュリティ対策やインシデント対応を理解し、情報開示や連絡を効果的に実践する | 自部署の対策に関する社内外の情報収集や協議を実務レベルで実施できるようになる |
| ５．関連法令 | サイバーセキュリティに関する法律や基準を実用的に理解する | デジタル化における取組で必要な法律や基準を意識して対応する |

# ITスキル標準モデルカリキュラム

【参照：テキスト24-2.】
P10

## ITスキル標準モデルカリキュラムの構成



# ITスキル標準モデルカリキュラム

【参照：テキスト24-2.】
P10～P11

## ITスキル標準モデルカリキュラムの構成

| | |
|---|---|
| **対象人材** | ① 本格的な就業経験のない学生<br>② IT に関する基本的な知識を持たない社会人 |
| **対象場面** | ① 企業：IT 系企業を含め企業などの内定者の入社前研修など<br>② 教育機関：情報系、非情報系のすべての学部、学科における教育。ただし、情報系専門学科においては一般教養課程における教育 |
| **特徴** | ● 特定の製品や分野に偏らない知識と体系的なパーソナルスキルを修得できます。<br>● IT パスポート試験の出題範囲と整合し、科目およびコマシラバスごとに知識項目との対応が明らかになっているので、「IT パスポート試験（レベル 1）シラバス」と併用することでより一層の研修効果を図ることができます。 |

# プラス・セキュリティ知識補充講座

【参照：テキスト24-2.】
P11～P14

## コース概要

| 科目名 | 概要 | 受講対象者／受講前提 | シラバス |
|---|---|---|---|
| IT入門（１） | 経営戦略、システム開発ライフサイクル、プロジェクト・サービスマネジメント、システム監査の基礎を学ぶ | ITスキル標準レベル1を目指す者 | テキストP12参照 |
| IT入門（２） | デジタル化、アルゴリズム、ハードウェア、ソフトウェア、ネットワーク、データベース、セキュリティの基礎知識を学ぶ | ITスキル標準レベル1を目指し、「IT入門（1）」修了または同等の知識を有する者 | テキストP13参照 |
| パーソナルスキル入門 | チームワーク、コミュニケーション、プレゼン、論理的思考、ビジネスマナー、IT活用に必要なスキルを学ぶ | ITスキル標準レベル1を目指し、高校卒業程度の知識を有する者（前提科目なし） | テキストP14参照 |

# マナビDX

【参照：テキスト24-3.】
P15～P16

## 紹介されている講座

- 厳選された信頼できる講座
- 種類が豊富
- 受講料支援のある講座も掲載
- リスキリングにも活用
- デジタルリテラシー講座
- デジタル実践講座
- サイバーセキュリティ関連講座
- 特定のスキルに特化した講座

# マナビDX

【参照：テキスト24-3.】
P16～P17

## 講座のレベル

| | |
|---|---|
| レベル 4 | **DX 推進スキル標準・ITSS・ITSS+**<br>一つまたは複数の専門を獲得したプロフェッショナルとして、専門スキルを駆使し、業務上の課題を発見と解決をリードするレベル。プロフェッショナルとして求められる、経験の知識化とその応用（後進育成）に貢献する。 |
| レベル 3 | **DX 推進スキル標準・ITSS・ITSS+**<br>要求された作業をすべて独力で遂行するレベル。専門を持つプロフェッショナルを目指し、必要となる応用的知識・技能を有する。 |
| レベル 2 | **DX 推進スキル標準・ITSS・ITSS+**<br>要求された作業について、上位者の指導の下、その一部を独力で遂行するレベル。プロフェッショナルに向けて必要となる基本的知識・技能を有する。 |
| レベル 1 | **DX リテラシー標準**<br>要求された作業について、上位者の指導を受けて遂行するレベル。プロフェッショナルに向けて必要となる基本知識・技能を有する。 |

# マナビDX

【参照：テキスト24-3.】
P17～P18

## マナビDXでの学び方

- Point1 キーワードやカテゴリで検索可能
  - キーワードから探す
  - スキルやロールから探す
  - マナビＤＸオススメから探す
- Point2 自分の「お気に入り」や「学習プラン」の作成が可能
  - 「お気に入り」への登録
  - 「学習プラン」による計画的な学習の実現
- Point3 講座は「デジタルスキル標準（DSS）」と紐づけ
  - 「デジタルスキル標準（DSS）」を理解し活用する
- Point4 最先端の新技術にも対応

# 第25章. スキルと知識を持った人材育成・人材確保方法

## 「プラス・セキュリティ」の実施計画例
## 「リスキリング」「チェンジマインド」の実施計画例

# 「プラス・セキュリティ」の実施計画例

【参照：テキスト25-1.】
P21～P23

前提条件
　中小企業を対象とし、セキュリティ専門家が社内に存在しない。

1. 目標の明確化　　＜テキストP21参照＞

2. 学習方法の検討　＜テキストP22参照＞
   - 専門家の活用
   - オンライン学習の活用
   - 内部研修の実施

3. 受講者の準備　　＜テキストP22参照＞
   - 受講の要否判定
   - 事前アンケートの実施

# 「プラス・セキュリティ」の実施計画例

【参照：テキスト25-1.】
P23～P28

4. カリキュラムの実施　＜テキストP23参照＞
   - オンライン研修の実施
   - 集合講習の実施
   - 演習の実施

5. 結果の評価と報告　　＜テキストP24参照＞
   - 結果のフィードバック
   - 最終報告書の作成

6. ガントチャートの作成＜テキストP24参照＞
   - 進捗確認とスケジュール管理
   - リソースの効率的な活用と調整
   - リスクの早期特定と対応策の準備

# 「リスキリング」「チェンジマインド」の実施計画例

【参照：テキスト25-2-1.】
P29～P34

## 「ITスキル標準」の実施計画例

1. 目標の明確化
   <テキストP29参照>
2. 目標達成に必要な作業を洗い出す
   <テキストP29参照>
3. 学習内容の詳細化
   <テキストP30参照>
4. 学習方法の選定
   <テキストP33参照>
5. 学習の進行と進捗管理
   <テキストP34参照>
6. フィードバック収集とフォローアップの実施
   <テキストP34参照>

# 「リスキリング」「チェンジマインド」の実施計画例【参照：テキスト25-2-2-1.】P35～P40

## 「デジタルスキル標準」の実施計画例

## DXリテラシー標準

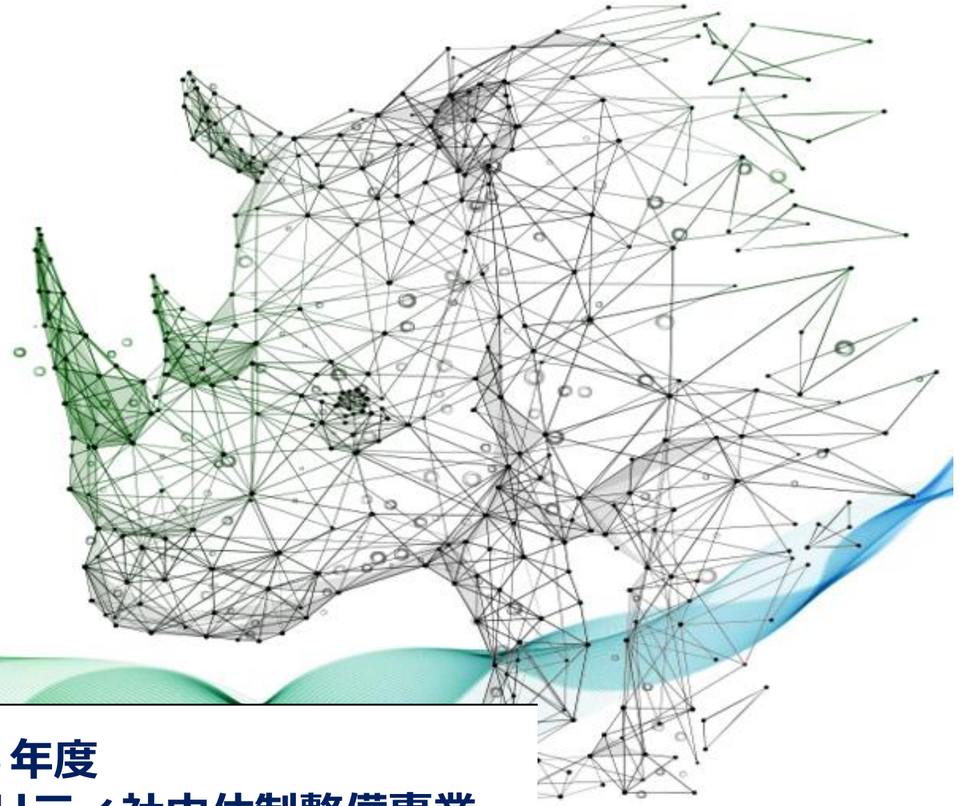
1. 学習内容の検討
   <テキストP35参照>
2. 学習方法の選定
   <テキストP37参照>
3. 学習計画の策定
   <テキストP38参照>
4. 学習の実施
   <テキストP39参照>
5. フィードバックの収集とフォローアップ
   <テキストP39参照>

# 「リスキリング」「チェンジマインド」の実施計画例【参照：テキスト25-2-2-2.】P40～P51

## 「デジタルスキル標準」の実施計画例

### DX推進スキル標準

1. 現状分析と目標設定
   <テキストP42参照>
2. 学習計画の作成
   <テキストP44参照>
3. 学習計画の周知と実施準備
   <テキストP50参照>
4. 学習の実行
   <テキストP50参照>
5. フィードバックと進捗管理
   <テキストP50参照>
6. 学習プランの調整
   <テキストP50参照>
7. 成果の評価とフィードバック
   <テキストP51参照>
8. フォローアップと継続学習
   <テキストP51参照>



# 令和６年度
# 中小企業サイバーセキュリティ社内体制整備事業