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10回
第10編：全体総括

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26章. エグゼクティブサマリー

第27章. 各章のポイント

第26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26-1.】
P3～P4

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）

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）

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）

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9章）

全体要旨

【参照：テキスト26-1.】
P4

テキストの概要

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）

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）

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）

第８編　具体的な構築・運用の実践【レベル３】
（第20章～第21章）

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）

テキスト活用のポイント

【参照：テキスト26-2.】
P5～P9

1. ポイントの再認識
   - DX推進の考え方の把握：＜テキストP5～P6参照＞
   - セキュリティ対策の全容の認識：＜テキストP6参照＞
   - 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P7参照＞
   - 自組織としての実践準備：＜テキストP7～P8参照＞
2. 関係者との共有
   ＜テキストP8参照＞
3. 社内体制の確立
   ＜テキストP8～P9参照＞
4. セキュリティ対策の実践
   ＜テキストP9参照＞

第27章. 各章のポイント

第1章～第25章

第１章 デジタル時代の社会とIT情勢

【参照：テキスト27-1.】
P11～P12

要旨

1-1. デジタル時代の社会変革とIT情勢の関係性

- 社会の現状と今後の同行（Society5.0）
- DXとは
- 生成AIとは

第１章 デジタル時代の社会とIT情勢

【参照：テキスト27-1.】
P11～P12

認識していただきたい実施概要

1. 中小企業のDX推進とビジネス発展の重要性
   - 中小企業は限られたリソースの中でDXを推進し、新たなサービスを創造することで、急速に変化するビジネス環境に対応し、ビジネスを発展させることが重要です。
2. デジタル技術活用とセキュリティ対策の必要性
   - データやデジタル技術を効果的に活用するためには最新技術の知識と専門人材が必要であり、安全に利用するために適切なセキュリティ対策を実施することが重要です。
3. 生成AI利用時の情報漏えいリスク管理
   - 生成AIは業務効率化に役立ちますが、パブリックな生成AIでは情報漏えいのリスクがあるため、機密情報を入力しないように注意して活用することが重要です。

第２章 サイバーセキュリティの基礎知識

【参照：テキスト27-2.】
P13～P15

要旨

2-1. 導入済みと想定するセキュリティ対策機能
- UTM（Unified Threat Management）
- EDR（Endpoint Detection and Response）

2-2. SECURITY ACTION（セキュリティ対策自己宣言）
- 情報セキュリティ5か条
- 情報セキュリティ自社診断
- 情報セキュリティ基本方針

2-3. サイバーセキュリティアプローチ方法
- Lv1. クイックアプローチ
- Lv2. ベースラインアプローチ
- Lv3. 網羅的アプローチ

第２章 サイバーセキュリティの基礎知識

【参照：テキスト27-2.】
P13～P15

認識していただきたい実施概要

1. 「SECURITY ACTION」制度の活用
   - 中小企業が情報セキュリティ対策に取り組む宣言として「SECURITY ACTION」を導入し、従業員の意識向上と対外的信頼の向上に有効である。
2. サイバーセキュリティ脅威への3つのアプローチ
   - サイバーセキュリティの脅威に対処するために、効果的な3種類のアプローチが存在する。

第３章 デジタル社会の方向性と現実に向けた国の方針

【参照：テキスト27-3.】
P16～P18

要旨

3-1. 国の基本方針および実施計画の要約

- （さまざまな分野における）DXの推進
- デジタル・ガバメントの強化
- サイバーセキュリティの強化

3-2. 政府機関が目指す社会の方向性とサイバーセキュリティ課題

- デジタル社会を実現していくための7つの戦略的な政策
- 各分野における基本的な施策
- Society5.0
- DXの推進
- 中小企業がDX推進における優位な点

第３章 デジタル社会の方向性と現実に向けた国の方針

【参照：テキスト27-3.】
P16～P18

認識していただきたい実施概要

1. 政府の基本方針や社会実現計画を通じたIT・デジタル・サイバーセキュリティの学習
   - 国の基本方針や社会実現計画を通じて、IT、デジタル、サイバーセキュリティの方向性や課題を学ぶ。
2. 中小企業の優位性を活かした積極的なDXの重要性
   - 中小企業特有の強みを理解し、積極的にデジタルトランスフォーメーション（DX）に取り組むことが組織の成長に不可欠である。

第４章 サイバーセキュリティ戦略および関連法令

【参照：テキスト27-4.】
P19～P21

要旨

4-1. NISC：サイバーセキュリティ戦略
- サイバーセキュリティ戦略
- サイバーセキュリティ2024

4-2. 企業経営に重要なDX推進とセキュリティ確保の両立
- 企業経営のためのサイバーセキュリティの考え方
- DX with Cybersecurity

4-3. 関連法令
- 個人情報保護法
- GDPR（EU一般データ保護規則）

第４章 サイバーセキュリティ戦略および関連法令

【参照：テキスト27-4.】
P19～P21

認識していただきたい実施概要

1. 国家レベルのサイバーセキュリティ戦略の理解
   - サイバーセキュリティ戦略によって、国家レベルでのサイバーセキュリティの確保に向けた方針や目標が設定されていることを理解する。
2. サイバーセキュリティ対策を経営理念と位置付ける重要性
   - サイバーセキュリティ対策の支出を経営に必要な投資と捉え、積極的に取り組むことが重要である。
3. 専門知識がなくてもセキュリティ意識を持つことの重要性
   - DX推進と並行して、ITやセキュリティの専門知識がなくても、業務遂行時にセキュリティを意識し、必要な対策能力を身につけること（プラス・セキュリティ）が重要である。
4. 個人情報の適切な取扱いに関する法令遵守
   - 個人情報保護法やGDPRなどのサイバーセキュリティ関連法令に基づき、個人情報をセキュリティレベルの高い情報として適切に取扱うこと。

第５章 事例を知る：重大なインシデント発生から課題解決まで

【参照：テキスト27-5.】
P22～P24

要旨

5-1. 情報セキュリティの概要
- 情報セキュリティ白書
- 情報セキュリティ10大脅威

5-2. 重大インシデント事例から学ぶ課題解決
- IoTデバイスへの攻撃
- サプライチェーンを介した標的型メール攻撃
- テレワーク環境での情報漏えい
- ランサムウェアへの感染

5-3. 実際の被害事例から見るケーススタディー
- インシデント事例を通じたベストプラクティスの紹介

第５章 事例を知る：重大なインシデント発生から課題解決まで

【参照：テキスト27-5.】
P22～P24

認識していただきたい実施概要

1. 情報セキュリティ白書や10大脅威の活用
   - 最新の脆弱性や脅威情報、攻撃の傾向・手法を把握し、適切な予防策や対策を講じることができる。
2. 過去インシデント事例からの学び
   - 過去の事例をもとに脅威対応策を策定し、リスク戦略の改善やセキュリティ意識の向上を図り、将来のインシデントに適切に対応できる。

第６章 企業経営で重要となるIT投資と投資としてのサイバーセキュリティ対策

【参照：テキスト27-6.】
P25～P27

要旨

6-1. これからの企業経営で必要な観点：社会の動向
- 現実社会とサイバー空間のつながり
- IT活用における課題

6-2. 守りのIT投資と攻めのIT投資
- 守りのIT投資と攻めのIT投資
- 次世代技術を活用したビジネス展開

6-3. 経営投資としてのサイバーセキュリティ対策
- サイバーセキュリティの確保

第６章 企業経営で重要となるIT投資と投資としてのサイバーセキュリティ対策

【参照：テキスト27-6.】
P25～P27

認識していただきたい実施概要

1. 現実社会とサイバー空間の連携および社会動向の把握
   - 現実社会とサイバー空間のつながりやSociety5.0などの社会動向を理解することが、今後の企業経営において重要な視点となる。
2. 「攻め」のIT投資の重要性の理解と実施
   - IT投資には「攻め」と「守り」があり、特に「攻め」のIT投資の重要性が増しているため、それを理解し積極的に取り組むことが重要である。
3. DX推進とサイバーセキュリティ対策の同時実施
   - デジタルトランスフォーメーション（DX）の推進に伴いデータやデジタル技術の活用が進む中で、サイバー攻撃の被害を防ぐために同時にサイバーセキュリティ対策を行うことが重要である。

第７章 セキュリティ対策の概要（全容）

【参照：テキスト27-7.】
P28～P30

要旨

7-1. 対策基準の策定

- セキュリティ対策基準の概要
  - 基本方針
  - 対策基準
  - 実施手順・運用規則など
- 対策基準策定のアプローチ方法
  - Lv.1 クイックアプローチ
  - Lv.2 ベースラインアプローチ
  - Lv.3 網羅的アプローチ

第７章 セキュリティ対策の概要（全容）

【参照：テキスト27-7.】
P28～P30

認識していただきたい実施概要

1. 対策基準の外部公開による説明責任の果たし方
   - セキュリティ対策を外部に公開することで、内外に対して対策の実施状況を示し、説明責任を果たすことができる。
2. 対策基準に基づく実施手順の作成
   - 策定した対策基準に従い、具体的な実施手順を作成することが重要である。
3. 対策基準策定時のアプローチ選択と推奨
   - 企業の現状や目標に応じて「Lv.1 クイックアプローチ」や「Lv.2 ベースラインアプローチ」を用いて対策基準を策定できるが、網羅的なフレームワークであるISMSを参考にする「網羅的アプローチ」が推奨される。

第８章 用語定義および関係性と識別方法

【参照：テキスト27-8.】
P31～P33

要旨

8-1. 用語の定義、脅威・脆弱性の識別

- 用語の定義と関係性
  - 脅威
  - 脆弱性
  - 情報資産
  - セーフガード（管理策）
  - リスク
- 脅威の識別
  - 人為的脅威
  - 環境的脅威
- 脆弱性の識別

第８章 用語定義および関係性と識別方法

【参照：テキスト27-8.】
P31～P33

認識していただきたい実施概要

1. リスク増大の要因
   - 「脅威」「脆弱性」「資産の価値」のいずれかが増加すると、リスクが増大する。
2. リスク減少のための対応策
   - 「脅威」、「脆弱性」、「資産の価値」を識別し、リスクに対する保護要求事項を明確にし、それに合致するセーフガード（管理策）を適切に実施することでリスクを減少させる。

第９章 具体的な手順の作成（Lv.1 クイックアプローチ）

【参照：テキスト27-9.】
P34～P35

要旨

9-1. 【Lv.1 クイックアプローチ】の概要

9-2. セキュリティインシデント事例を参考とした実施手順

認識していただきたい実施概要

1. Lv.1 クイックアプローチの特徴
   - 実際のセキュリティインシデント事例をもとに自社での発生可能性や被害規模を検討し、対策基準や実施手順を策定することで、社会的に影響の大きいまたは緊急性の高い事象への対策が容易になる。

第10章 具体的な手順の作成（Lv.2 ベースラインアプローチ）

【参照：テキスト27-10.】
P36～P37

要旨

10-1. 【Lv.2 ベースラインアプローチ】の概要

10-2. ガイドラインを参考とした実施手順

認識していただきたい実施概要

1. Lv.2 ベースラインアプローチの特徴
   - ガイドラインやひな型などの既存手法を参考に対策基準や実施手順を策定するため、自社に適した参考元があれば、それをもとに簡易な手順で策定しやすい。

第11章 セキュリティフレームワーク

【参照：テキスト27-11.】
P38～P40

要旨

11-1. セキュリティフレームワークの概要

11-2. 情報セキュリティマネジメントシステム（ISMS）

11-3. NISTサイバーセキュリティフレームワーク（CSF）

11-4. サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）

11-5. サイバーセキュリティ経営ガイドライン

第11章 セキュリティフレームワーク

認識していただきたい実施概要

【参照：テキスト27-11.】
P38～P40

1. フレームワークに沿ったセキュリティ対策の有効性
   - 効果的なセキュリティ対策の実施や取引先・顧客からの信頼向上のために、フレームワークに基づいて対策を進めることが有効である。
2. ISMSを基盤としたフレームワークの選択と補完
   - セキュリティ対策用フレームワークは複数存在するが、まずは業種業態を問わずセキュリティ対策の全体枠組みと網羅的な対策項目を提供するISMSを基盤とし、必要に応じて業種や重点領域に特化した各種フレームワークで補完することが有効である。

第12章 リスクマネジメント

【参照：テキスト27-12.】
P41～P43

要旨

12-1. リスクマネジメント：概要

- リスクマネジメントプロセス（ISO 31000）
- 情報セキュリティリスクマネジメント（ISO/IEC 27005）
- ISO/IEC 27001におけるリスクマネジメント手順

12-2. リスクマネジメント：リスクアセスメント

12-3. リスクマネジメント：リスク対応

第12章 リスクマネジメント

【参照：テキスト27-12.】
P41～P43

認識していただきたい実施概要

1. リスクマネジメントプロセスにおけるリスクアセスメントの必須性
   - リスク対応を行うためには、リスクマネジメントプロセスの中でリスクアセスメントを実施することが不可欠である。
2. リスクアセスメントの実施項目
   - リスクアセスメントでは、「リスク特定」、「リスク分析」、「リスク評価」を順に実施する。
3. リスク対応の選択肢
   - リスクアセスメントの結果に基づき、「リスク回避」、「リスク低減」、「リスク移転」、「リスク受容」の中から適切な対応策を選択する。

第13章 ISMSの要求事項と構築（LV.3 網羅的アプローチ）

【参照：テキスト27-13.】
P44～P47

要旨

13-1. 【Lv.3 網羅的アプローチ】の概要
- Lv.3 網羅的アプローチ

13-2. フレームワークを参考とした実施手順

13-3. ISMS文書体系（ISMS構築・導入に必要な文書と記録）
- 文書体系のポイント

13-4. ISO/IEC27001の審査準備と審査内容
- 認証機関の選定と申し込み
- 審査事前準備
- 第一段階・第二段階審査
- 維持審査・再認証審査

第13章 ISMSの要求事項と構築（LV.3 網羅的アプローチ）

認識していただきたい実施概要

【参照：テキスト27-13.】
P44～P47

1. 必要なドキュメント作成手順の理解
   - 「4.組織の状況」から「10.改善」までの7項目に基づき、必要なドキュメントの作成手順を理解する。
2. ISMSマネジメントプロセスの導入とPDCAサイクルの実施
   - ISMSマネジメントプロセスを取り入れ、計画（Plan）、実行（Do）、評価（Check）、改善（Act）のPDCAサイクルを回す。

第14章 ISMSの管理策

【参照：テキスト27-14.】
P48～P50

要旨

14-1. 管理策の分類と構成

- 管理策：ISO/IEC 27002
- 管理策のテーマと属性
- 策定手順
  - 管理策の決定
  - 管理策の検証
  - 適用宣言書の作成
  - 実施手順の作成

第14章 ISMSの管理策

【参照：テキスト27-14.】
P48～P50

認識していただきたい実施概要

1. 管理策としての対策とISO/IEC 27002:2022の項目数
   - ISMSにおけるリスク対応のための対策として管理策が存在し、ISO/IEC 27002:2022では合計93項目が示されている。
2. ISO/IEC 27002:2022の管理策のテーマと属性の活用
   - ISO/IEC 27002:2022で示される管理策は4つのテーマと5つの属性に分類されており、これらを参考にして組織に適したセキュリティ対策を選択することが重要である。

第15章 組織的対策

【参照：テキスト27-15.】
P51～P53

要旨

15-1. 作成する候補となる実施手順書類について

15-2. 組織的対策として重要となる実施項目

- 37項目の管理策

第15章 組織的対策

【参照：テキスト27-15.】
P51～P53

認識していただきたい実施概要

1. 組織的管理策の選択と対策基準の策定
   - リスクアセスメントの結果に基づき、必要な組織的管理策を選択し、対策基準を策定する。
2. 公開可能な対策基準の策定
   - 対策基準を基本方針とともに公開可能なものとして策定する。
3. 対策基準実行のための実施手順の策定
   - 決定した対策基準を実行に移すための実施手順を策定する。
4. わかりやすい実施手順の作成
   - 実施手順を組織の内部文書として、従業員に対してわかりやすく策定するよう心掛ける。

第16章 人的対策

【参照：テキスト27-16.】
P54～P55

要旨

16-1. 作成する候補となる実施手順書類について

16-2. 人的対策として重要となる実施項目

- 8項目の管理策

第16章 人的対策

【参照：テキスト27-16.】
P54～P55

認識していただきたい実施概要

1. 人的管理策の選択と対策基準の策定
   - リスクアセスメントの結果に基づき、必要な人的管理策を選択し、対策基準を策定する。
2. 公開可能な対策基準の策定
   - 対策基準を基本方針とともに公開可能なものとして策定する。
3. 対策基準実行のための実施手順の策定
   - 決定した対策基準を実行に移すための実施手順を策定する。
4. わかりやすい実施手順の作成
   - 実施手順を組織の内部文書として、従業員に対してわかりやすく策定するよう心掛ける。

第17章 物理的対策

【参照：テキスト27-17.】
P56～P58

要旨

17-1. 作成する候補となる実施手順書類について

17-2. 物理的対策として重要となる実施項目

- 14項目の管理策

17-3. BYOD、MDM

- BYOD（Bring Your Own Device）
- MDM（Mobile Device Management）

第17章 物理的対策

【参照：テキスト27-17.】
P56～P58

認識していただきたい実施概要

1. 物理的管理策の選択と対策基準の策定
   - リスクアセスメントの結果に基づき、必要な物理的管理策を選択し、対策基準を策定する。
2. 公開可能な対策基準の策定
   - 対策基準を基本方針とともに公開可能なものとして策定する。
3. 対策基準実行のための実施手順の策定
   - 決定した対策基準を実行に移すための実施手順を策定する。
4. わかりやすい実施手順の作成
   - 実施手順を組織の内部文書として、従業員に対してわかりやすく策定するよう心掛ける。
5. BYODおよびMDMの概要と運用手順の理解
   - BYOD（Bring Your Own Device）およびMDM（Mobile Device Management）の概要とその運用手順を理解する。

第18章 技術的対策

【参照：テキスト27-18.】
P59～P62

要旨

18-1. 作成する候補となる実施手順書類について

18-2. 技術的対策として重要となる実施項目

- 34項目の管理策

18-3. 実施手順を適用するセキュリティ概念

- Security by Design
- ゼロトラストモデル
- SASE（Secure Access Service Eddge）
- ネットワーク制御（Network as a Service）
- セキュリティ統制（Security as a Service）

18-4. インシデント対応

第18章 技術的対策

【参照：テキスト27-18.】
P59～P62

認識していただきたい実施概要

1. 技術的管理策の選択と対策基準の策定
   - リスクアセスメントの結果に基づき、必要な技術的管理策を選択し、対策基準を策定する。
2. 公開可能な対策基準の策定
   - 対策基準を基本方針とともに公開可能なものとして策定する。
3. 対策基準実行のための実施手順の策定
   - 決定した対策基準を実行に移すための実施手順を策定する。
4. わかりやすい実施手順の作成
   - 実施手順を組織の内部文書として、従業員に対してわかりやすく策定するよう心掛ける。
5. 各種テーマごとの概要理解と実施手順の策定
   - 各種テーマごとの概要を理解し、自社に適した実施手順を策定する。

第19章 セキュリティ対策状況の有効性評価

【参照：テキスト27-19.】
P63～P64

要旨

19-1. 内部監査

19-2. 外部監査

認識していただきたい実施概要

1. 外部監査の実施とその効果
   - 外部監査を行うことで、第三者の視点から企業が保有する情報資産を守るための体制や環境が整っているかをチェックできる。
2. 内部監査の実施とその効果
   - 内部監査を行うことで、セキュリティのルールや文書の内容が適切で有効かどうかをチェックできる。

第20章 セキュリティ機能の実装と運用（IT環境構築・運用実施手順）

【参照：テキスト27-20.】
P65～P66

要旨

20-1. セキュリティ機能の実装と運用

- Fit＆Gap分析

20-2. アジャイル開発

認識していただきたい実施概要

1. 「デジタル・ガバメント推進標準ガイドライン」を参考にしたシステム導入と留意点の理解
   - 中小企業にも適用可能なシステム導入工程や実践時の留意点を理解する。
2. 情報システム構築と運用工程でのセキュリティ機能の実装
   - 各工程においてセキュリティ機能を実装する。
3. アジャイル開発の重要性の理解
   - アジャイル開発の重要性を理解する。

第21章 人的、組織的、技術的、物理的対策の実施手順に基づいた実施

【参照：テキスト27-21.】
P67～P68

要旨

21-1. ECサイトの構築とセキュリティ機能の実装と運用

- 「デジタル・ガバメント推進標準ガイドライン」に準拠した手順

認識していただきたい実施概要

1. 「デジタル・ガバメント推進標準ガイドライン」を参考にしたセキュリティ機能の実装
   - 情報システムを導入する際に「デジタル・ガバメント推進標準ガイドライン」を参考にし、セキュリティ機能を実装する。
2. 要件定義におけるセキュリティ要件の決定
   - 要件定義では、適用宣言書をもとに情報資産のリスクを考慮し、適切なセキュリティ要件を決定する。

第22章 サイバーセキュリティ対策を実践するための知識とスキル

【参照：テキスト27-22.】
P69～P71

要旨

22-1. デジタルスキル標準（DSS）

- DXリテラシー標準
- DX推進スキル標準

22-2. ITスキル標準（ITSS）

22-3. ITSS＋（プラス）

- データサイエンス領域
- アジャイル領域
- IoTソリューション領域
- セキュリティ領域

第22章 サイバーセキュリティ対策を実践するための知識とスキル

【参照：テキスト27-22.】
P69～P71

要旨

22-4. ｉコンピテンシディクショナリ（iCD）

- タスクディクショナリ
- スキルディクショナリ

認識していただきたい実施概要

1. サイバーセキュリティ対策に必要なスキル・知識の体系的理解
   - デジタルスキル標準やITスキル標準など各種フレームワークをもとに、サイバーセキュリティ対策を実践するために必要なスキルや知識を体系的に理解する。
2. IT知識・スキルを持つ人材の育成と確保
   - 各種スキル標準のフレームワークを活用し、効果的なセキュリティ対策を実践するために必要なIT全般の知識やスキルを持つ人材を育成・確保する。

第23章 人材の知識とスキルの認定制度

【参照：テキスト27-23.】
P72～P73

要旨

23-1. Di-Lite

- IT・ソフトウェア領域
- 数理・データサイエンス領域
- 人工知能（AI）・ディープラーニング領域

23-2. 情報処理技術者試験

23-3. 国際セキュリティ資格

第23章 人材の知識とスキルの認定制度

【参照：テキスト27-23.】
P72～P73

認識していただきたい実施概要

1. ITおよびデジタル人材のスキル・知識の認定制度の理解
   - ITおよびデジタル人材のスキルと知識を認定する制度を理解する。
2. 認定制度を活用した人材育成の推進
   - 情報処理技術者試験や国際資格などのITおよびデジタル人材のスキル・知識の認定制度を活用し、人材育成に取り組む。

第24章 各種人材育成カリキュラム

【参照：テキスト27-24.】
P74～P76

要旨

24-1. プラス・セキュリティ知識補充講座 カリキュラム例

- 経営層向けカリキュラム
- デジタル化推進部門の部課長級マネジメント層向けカリキュラム

24-2. 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）】

24-3. マナビDX

第24章 各種人材育成カリキュラム

【参照：テキスト27-24.】
P74～P76

認識していただきたい実施概要

1. セキュリティ関連カリキュラム内容の把握
   - 「プラス・セキュリティ知識補充講座 カリキュラム例」や「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）」など、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内容を把握する。
2. 実施計画および実施内容の検討
   - カリキュラム内容を参考にし、具体的な実施計画や実施内容を検討する。
3. マナビDXの活用によるデジタルスキル向上
   - マナビDXを活用して、デジタルスキルの向上を図る。

第25章 スキルと知識を持った人材育成・人材確保方法

【参照：テキスト27-25.】
P77～P78

要旨

25-1. 「プラス・セキュリティ」の実施計画例

- プラス・セキュリティ知識補充講座カリキュラム例

25-2. 「リスキリング」「チェンジマインド」の実施計画例

認識していただきたい実施概要

1. 関係機関公表カリキュラムを活用した実施計画および教育・研修内容の作成と実施
   - 関係機関が公表しているカリキュラムを活用し、チェンジマインドやリスキリングを含めた実施計画を策定します。さらに、具体的な教育・研修内容を作成し、実施することで、組織全体のデジタルスキル向上を図ります。

第28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28-1.】
P80～P89

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28-1.】
P80～P89

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28-1.】
P80～P89

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28-1.】
P80～P89

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）	○	－	○	－
情報セキュリティ委員会	－	○	○	－
情報システム管理者	－	－	○	○
一般社員	－	-	○	－

今後のアクション

【参照：テキスト28-1.】
P80～P89

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

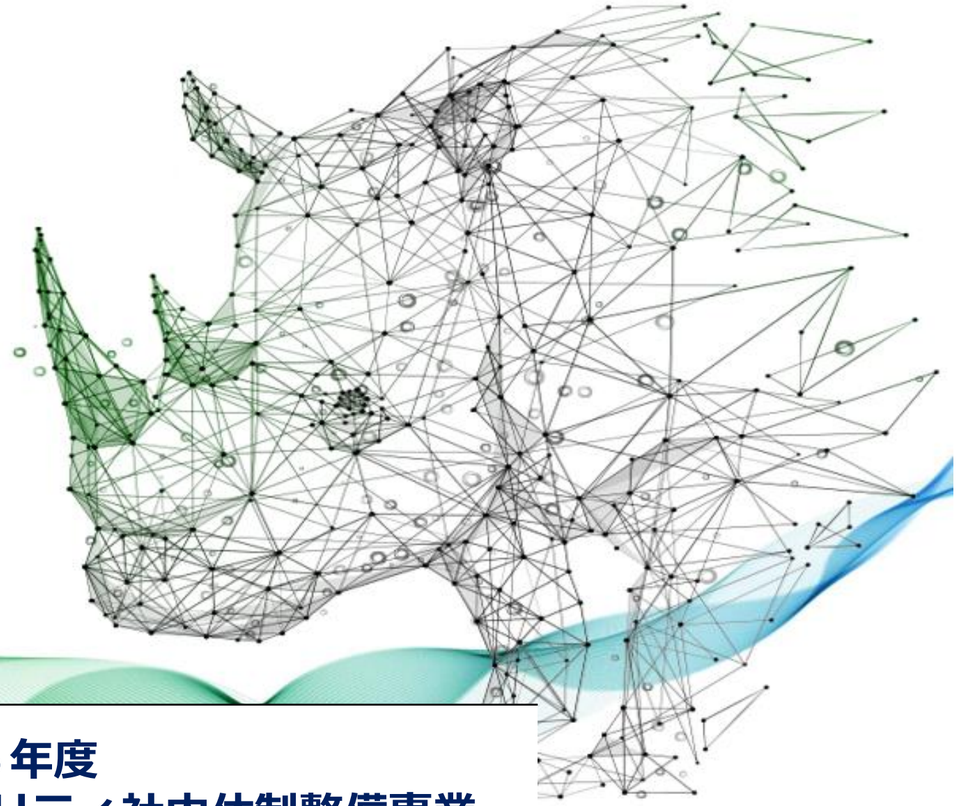
＜テキストP85～86参照＞

継続的な情報収集

＜テキストP86～88参照＞

人材育成を実施するために参考となる文献

＜テキストP88～89参照＞



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