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7回

第8編：具体的な構築・運用の実践

東京都産業労働局

講師紹介

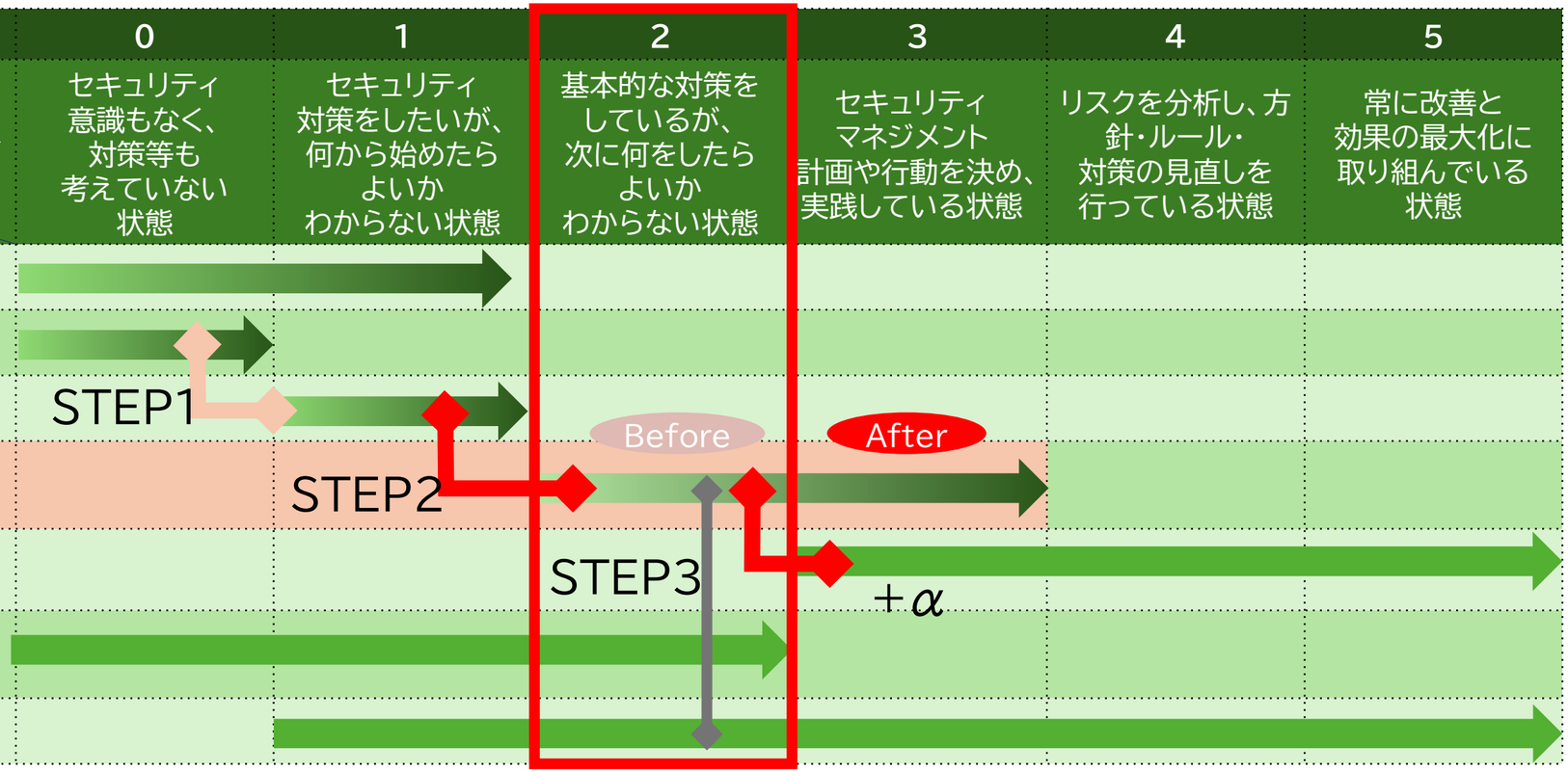
氏名	矢野　泰広（やの　よしひろ）
業務経歴	26年（セキュリティ経験：15年）
専門分野	情報セキュリティ、DX、ICT、クラウド技術、 ネットワーク技術、DB設計・構築、プロジェクト マネジメント、WEBシステム設計・構築、 サーバ設計・構築
保有資格	情報処理安全確保支援士（第004005号） 経済産業省認定 情報処理技術者試験 プロジェクトマネージャ、 情報処理技術者第一種、情報処理技術者第二種 インターネット検定 .com Master ADVANCE★★ 生成AIパスポート 家電製品アドバイザー（AV情報家電・生活家電）
コメント	中小企業を中心にDX、ネットワーク、クラウド技術お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

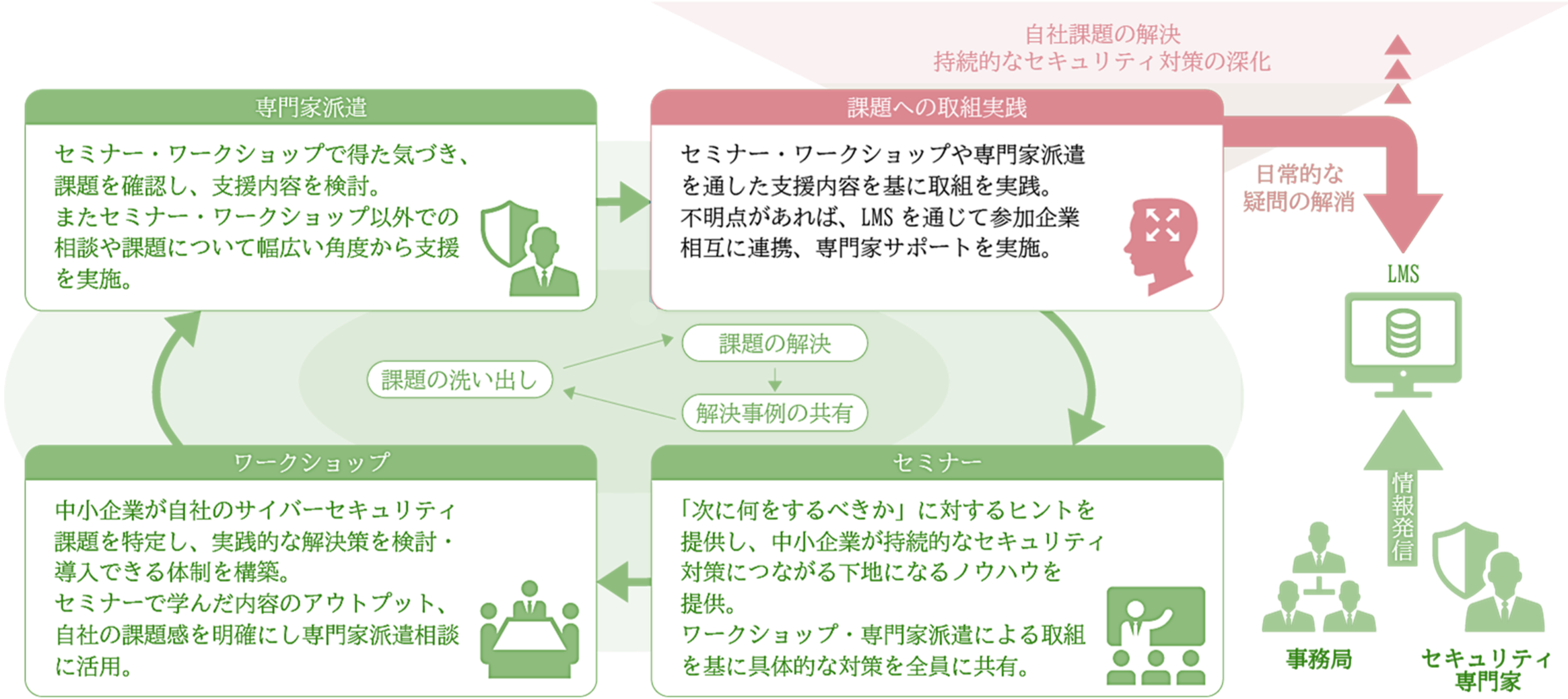
- 継続的なセキュリティ対策の実施を支援する。
- 人材の育成と実践的な課題解決を通じて、サプライチェーン全体のセキュリティ強化を図る。

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	全体総括

第20章. セキュリティ機能の実装と運用

セキュリティ機能の実装と運用

セキュリティ機能の実装と運用

【参照：第6回テキスト20-1-1.】
P56～P63

デジタル・ガバメント推進標準ガイドライン

1. プロジェクトの管理
2. 予算および執行
3. サービス・業務企画
4. 要件定義
5. 調達
6. 設計・開発
7. サービス・業務の運営と改善
8. 運用および保守
9. システム監査

プロジェクトの管理

【参照：第6回テキスト20-1-2.】
P63～P70

プロジェクト管理活動の全体の流れ

1. プロジェクトの立ち上げ、初動
2. プロジェクト計画書などの作成
3. プロジェクトのモニタリング
4. プロジェクトの終結

プロジェクトの目標設定におけるポイント

- 顧客が困っていること（受領連絡までの時間）への対応を優先
- 顧客や注文内容の異なりを捉え、個々のニーズへ対応（大量注文）
- 顧客目線で事前、事後の作業も改善（顧客確認）
- 小さく始める。そして、軌道修正しながら最終目標へ到達する
（段階的なKPI）

プロジェクトの管理

【参照：第6回テキスト20-1-2.】
P63～P70

「KGI」「CSF」「KPI」の定義と関係

- 重要目標達成指標（KGI：Key Goal Indicator）
- 重要成功要因（CSF：Critical Success Factor）
- 重要成果指標（KPI：Key Performance Indicator）

セキュリティ機能を実装・運用するためのポイント

- 多数の事業者間をまたいだシステム障害が発生するリスクへの対応
- 個人情報などの重要情報が漏えいするリスクへの対応

予算および執行

【参照：第6回テキスト20-1-3.】
P70～P78

予算活動の全体の流れ

1. 予算のための稟議（予算要求）の事前準備
2. 見積り依頼
3. 見積りの精査
4. 予算のための稟議（予算要求）に必要な資料の準備
5. 概要要求に向けた調整
6. 予算執行について

セキュリティ機能を実装・運用するためのポイント

- 情報システムを構成する製品のサポート終了に付随する経費の考慮
- 人事異動時の引続き不足を防ぐこと

サービス・業務企画

【参照：第6回テキスト20-1-4.】
P78～P83

サービス・業務企画の全体の流れ

1. サービス・業務企画の開始準備
2. 利用者視点でのニーズ把握
3. 業務の現状把握
4. サービス・業務企画内容の検討
5. 軌道修正
6. 新しい業務要件の定義

セキュリティ機能を実装・運用するためのポイント

- デジタル技術を徹底的に活用する

要件定義

【参照：第6回テキスト20-1-5.】
P83～P91

要件定義の全体の流れ

1. 要件定義の事前準備
2. RFIの実施
3. 要件定義の全体像
4. 機能要件の定義
5. 新しい非機能要件の定義
6. 要件定義終了後の対応

要件定義プロセスにおけるFit＆Gap分析

1. 業務要件の整理
2. パッケージソフトやSaaSの機能確認
3. フィット部分の特定（Fit）
4. ギャップ部分の特定（Gap）
5. コストとリスクの評価

要件定義

【参照：第6回テキスト20-1-5.】
P83～P91

Fit＆Gap分析結果に基づく決定

決定	条件
そのまま導入	フィット部分が大きくカスタマイズ不要な場合
部分的にカスタマイズして導入	小規模なギャップがあり、一部カスタマイズやプロセス変更で対応可能な場合
大幅なカスタマイズまたは導入中止	キャップが大きく、コストやリスクが許容範囲を超えるような場合

セキュリティ機能を実装・運用するためのポイント

- 非機能要件における、情報セキュリティに関する事項について
- 想定されるリスクの概要と対策について
- 最低限記載すべき情報セキュリティ対策要件

調達

【参照：第6回テキスト20-1-6.】
P91～P95

調達の全体の流れ

1. 調達の事前準備
2. 調達仕様書の作成
3. 調達仕様書以外のドキュメント作成
4. 調達手続きとプロジェクト管理
5. 検収

セキュリティ機能を実装・運用するためのポイント

- 再委託先の情報セキュリティ対策に係る規定を確認すること

設計・開発

【参照：第6回テキスト20-1-7.】
P95～P104

設計・開発の全体の流れ

1. 設計・開発を開始するための事前準備
2. 設計・開発の計画
3. 設計・開発・テストの管理
4. 見落としがちな活動に注意
5. 新業務の運営を円滑に行うための準備

セキュリティ機能を実装・運用するためのポイント

- テスト計画の策定
- テストのレベルと種類
- テストツールの活用

サービス・業務の運営と改善

【参照：第6回テキスト20-1-8.】
P104～P109

サービス・業務の運営と改善の全体の流れ

1. 新しいサービス・業務の事前準備
2. 業務の定着と次の備え
3. 業務の改善

セキュリティ機能を実装・運用するためのポイント

- 業務を外部委託する際の注意
- インシデントの優先度づけ

運用および保守

【参照：第6回テキスト20-1-9.】
P109～P117

運用および保守の全体の流れ

1. 運用・保守を開始するための事前準備
2. 運用・保守の計画
3. 運用・保守の定着と次の備え
4. 運用・保守の改善と業務の引継ぎ

セキュリティ機能を実装・運用するためのポイント

- セキュリティ関連作業を定期的に確実に実施すること
- セキュリティ対策会議の実施
- 情報システムのアカウントの管理

システム監査

【参照：第6回テキスト20-1-10.】
P117～P120

システム監査の全体の流れ

1. システム監査の理解
2. システム監査計画と監査実施計画
3. システム監査の実施
4. 指摘事項を踏まえた改善

セキュリティ機能を実装・運用するためのポイント

- 情報セキュリティ監査

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

ECサイトの構築とセキュリティ機能の実装と運用

ECサイトの構築とセキュリティ機能の実装と運用

【参照：テキスト21-1.】
P2～P3

ECサイト導入における全体概要

デジタル・ガバメント推進標準ガイドラインに準拠させた場合

ステップ	概要
1.　サービス・業務企画	事業目的とサービスの具体的な方向性を決める
2.　要件定義	サービスの実現に必要な機能／非機能の要件を定義する
3.　調達	開発に必要なリソースの調達
4.　設計・開発	プロジェクトの計画立案と管理
5.　サービス・業務の運営と改善	運営しながら改善
6.　運用および保守	安定稼動の維持と継続的改善

※セキュリティ要件は、「要件定義」のフェーズで決定する。

サービス・業務企画

【参照：テキスト21-1-1.】
P3～P7

利用者視点でのニーズ把握

ペルソナ分析を活用し、仮想顧客の特徴を具体化することで、利用者が抱える課題等を浮き彫りにし、具体性の高いアイデアを創出する。

ペルソナ分析を活用した、サービス・業務企画のステップ

1. ターゲットとなる利用者に関する情報を収集する
2. 収集した情報を分析し、グルーピングする
3. グルーピングした情報から利用者像を具現化、ペルソナを作成
4. 業務の現状把握
5. サービス・業務企画内容の検討

サービス・業務企画

【参照：テキスト21-1-1.】
P3～P7

業務の現状分析とフロー作成の重要性

現状把握の目的

複数の関係者が理解しやすい形で業務の状況を共有する。

業務フローとは

誰が、何を、どの順番で実施しているかを視覚的に示すツール

- 現行フロー（AsIs）：現在の業務内容を可視化
- 将来フロー（ToBe）：企画後の業務の変化点を明記
- ポイント：関係者にわかりやすい形式で表記する

業務フローの例：

1. 実店舗での購入フロー（テキスト P6 図84 参照）
2. ECサイトでの購入フロー（テキスト P7 図85 参照）

要件定義

【参照:テキスト21-1-2.】
P7～P53

一貫性を持った要件定義書の作成

- プロジェクト管理や契約合意の基盤となる。
- 誤った定義や曖昧な表現は後続工程に重大な影響が出る。

要件定義のポイント

- 用語の統一
- 業務要件の整合性
- 箇条書きで簡潔に

機能要件の定義

- 機能
- 画面
- 帳票
- データ
- 外部インターフェース

要件定義

【参照:テキスト21-1-2.】
P7～P53

機能に関する事項

- 機能とは、システムが何をしてくれるか。

＜テキスト P8 参照＞

画面に関する事項

- 画面とは、システムとやり取りをするための「窓口」のこと。

＜テキスト P9 参照＞

帳票に関する事項

- 帳票とは、システムから出力される書類のこと。

＜テキスト P9 参照＞

要件定義

【参照:テキスト21-1-2.】
P7～P53

データに関する事項

- データとは、システムが扱う情報のこと。

＜テキスト P10 参照＞

外部インターフェースに関する事項

- 外部インターフェースとは、システム同士が連携し情報をやり取りする仕組みのこと。

＜テキスト P10～11 参照＞

要件定義

【参照:テキスト21-1-2.】
P7～P53

非機能要件の定義

- 情報セキュリティに関する事項
- ユーザビリティおよびアクセシビリティに関する事項
- システム方式に関する事項
- 規模に関する事項
- 性能に関する事項
- 信頼性に関する事項
- 拡張性に関する事項
- 上位互換性に関する事項
- 中立性に関する事項
- 継続性に関する事項
- 情報システム稼動環境に関する事項
- データマネジメントに関する事項
- テストに関する事項
- 移行に関する事項
- 引継ぎに関する事項
- 教育に関する事項
- 運用に関する事項
- 保守に関する事項

要件定義

【参照:テキスト21-1-2.】
P7～P53

情報セキュリティに関する事項

- 情報セキュリティとは、システムに保存されたデータや情報を守るための仕組みやルールのこと。
- セキュリティ要件の決める流れ
  1. リスクアセスメントを実施する。
  2. 必要な管理策を決定する。
  3. セキュリティ要件を決める。
     - IPAが提供しているガイドラインでは、次の3つのレベルで定めている。
       1. 必須
       2. 必要
       3. 推奨
- セキュリティ対策要件（構築時）は、テキストP14～P22参照。

※ P20 要件6.中の「クレジットカード・セキュリティガイドライン」がVer6.0に改訂されました。
変更点：EC加盟店のシステム及びWebサイトの「脆弱性対策」の実施など（2025/03/05）

要件定義

【参照:テキスト21-1-2.】
P7～P53

ユーザビリティおよびアクセシビリティに関する事項

ユーザビリティとは？

- 使いやすさのこと。

アクセシビリティとは？

- 誰でも目的の情報にたどり着けるか。

＜テキスト P22～23 参照＞

システム方式に関する事項

システム方式とは？

- システムがどのように動作するか、そのために必要なツールや技術をどう使うかを決めるもの。

＜テキスト P23～24 参照＞

要件定義

【参照:テキスト21-1-2.】
P7～P53

規模に関する事項

規模とは？

- システムがどれくらいのユーザーに使われるか。
- どれくらいの情報量を扱うか。

＜テキスト P24 参照＞

性能に関する事項

性能とは？

- システムが快適に利用できるか。

＜テキスト P24～25 参照＞

信頼性に関する事項

信頼性とは？

- システムがどれだけ安定して動くか。

＜テキスト P25～26 参照＞

要件定義

【参照:テキスト21-1-2.】
P7～P53

拡張性に関する事項

拡張性とは？

- 性能低下を感じた時に、どのように拡張を実施し、性能を確保するか。

＜テキスト P26 参照＞

上位互換性に関する事項

上位互換性とは？

- ソフトウェアの新しいバージョンが、古いバージョンの機能やデータを問題なく使えるか。

＜テキスト P26～27 参照＞

中立性に関する事項

中立性とは？

- システムが特定の会社や製品に依存しないようにすること。

＜テキスト P27 参照＞

要件定義

【参照:テキスト21-1-2.】
P7～P53

継続性に関する事項

継続性とは？

- システムが問題や災害が起こったときにも、できるだけ早く復旧して再び使えるようにするための能力のこと。

＜テキスト P27～28 参照＞

情報システム稼働環境に関する事項

情報システム稼働環境とは？

- システムが実際に動くために必要なすべての要素のこと。

＜テキスト P28～29 参照＞

テストに関する事項

テストとは？

- システムが設計通りに動作するか、不具合がないかチェックすること。

＜テキスト P29～30 参照＞

要件定義

【参照:テキスト21-1-2.】
P7～P53

移行に関する事項

移行とは？

- 現在使っているシステムやデータを新しいシステムに引き継いで移動させる作業のこと。

＜テキスト P30 参照＞

引継ぎに関する事項

引継ぎとは？

- 現在の担当者や事業者が行っている作業や業務を、次の担当者や事業者にスムーズに渡すための作業のこと。

＜テキスト P30～32 参照＞

要件定義

【参照:テキスト21-1-2.】
P7～P53

教育に関する事項

教育とは？

- システムの利用者がそのシステムを正しく理解し、効率的に使うために行う研修やトレーニングのこと。

＜テキスト P32 参照＞

運用に関する事項

運用とは？

- 情報システムが常に正常に動き続けるように維持・管理すること。

＜テキスト P33～38 参照＞

保守に関する事項

保守とは？

- システムの現状の機能を維持しつつ問題を修正する作業のこと。

＜テキスト P38～40 参照＞

要件定義

【参照:テキスト21-1-2.】
P7～P53

SaaS型サービスの選定基準と利用時に必要となる対策

SaaS型サービスとは？

- SaaS（Software as a Service）は、インターネットを通じて使うソフトウェアのことです。

＜テキスト P40 参照＞

Fit&Gap 分析

Fit&Gap分析とは？

- SaaSやパッケージソフトを導入する際に、自社の業務要件にどれだけ合っているかと、どこが合わないかを認識するためのプロセスのこと。

＜テキスト P40 参照＞

要件定義

【参照:テキスト21-1-2.】
P7～P53

Fit&Gap分析の実施方法(例)

1. 現状分析
   ＜テキスト P42 参照＞
2. SaaS,パッケージソフトウェアの機能調査
   ＜テキスト P42～43 参照＞
3. 比較分析
   ＜テキスト P43～49 参照＞
4. ギャップへの対応検討
   ＜テキスト P49～50参照＞
5. 費用対効果の分析
   ＜テキスト P50～51 参照＞
6. 実施計画の策定
   ＜テキスト P51参照＞

調達

【参照:テキスト21-1-3.】
P53～P58

調達仕様書の作成方法

- 調達仕様書とは？
  プロジェクトに必要な製品やサービスを外部の事業者から調達するときに、発注者側（自分たち）が何を求めているか、どんな条件があるかを詳しくまとめたドキュメントのこと。

調達仕様書を作成するときに、特に注意が必要なポイント

1. 調達の意図や目的を正しく伝える
2. 作業内容・納品物を関連付けて網羅的に記載する
3. 外部事業者の具体的な作業内容を明確にする
4. 作業の実施体制を明確にする
5. 成果物の取扱いに注意する（知的財産権）
6. 再委託に関する事項を定める
7. 納品後に不具合が発覚したときの責任を明確にする（契約不適合責任）

調達

【参照:テキスト21-1-3.】
P53～P58

適正な価格で最適な業者の選定

- 調達仕様書の明確化
- 透明性と公平性の維持
- 複数の見積り取得

3点見積りとは

プロジェクトやタスクの時間やコストを予測するための方法の一つ。
3つの異なるシナリオに基づいて予測を行います。それぞれのシナリオは以下の通り

シナリオ	概要
楽観値	最も良い条件がそろった場合の最低コスト
最頻値	一般的な条件で進行した場合の予測コスト
悲観値	最悪の状況が発生した場合の最高コスト

設計・開発

【参照:テキスト21-1-4.】
P58～P60

設計・開発の計画

- 「設計・開発実施要領」の作成
- 「設計・開発実施計画書」の作成

＜テキスト P58～60 参照＞

設計・開発・テストの管理

- 単体テスト
- 結合テスト
- 総合テスト
- 受入テスト

＜テキスト P60 参照＞

サービス・業務の運営と改善

【参照:テキスト21-1-5.】
P61～P66

業務の定着と次の備え

業務の定着とは？

- 新しい情報システムが導入された後、そのシステムを実際の業務でスムーズに使えるようにすること。
- システムのリリースが近づいたら、従業員向けに教育を行い、業務マニュアルを使ってシステムの使い方や業務の流れなどの説明を実施する。

＜テキスト P61 参照＞

業務の改善

業務の改善とは？

- サービスや業務を運営していく中で発生する問題や新しい情報をもとに、より良い運営方法を見つけていくプロセスのこと。

＜テキスト P64～65 参照＞

運用および保守

【参照:テキスト21-1-6.】
P66～P69

運用・保守の計画

運用・保守の計画とは？

- システムが安定して動作し続けるように、日々の運用や修理・メンテナンスをどう進めるかを決める計画のこと。

＜テキスト P66～67 参照＞

運用・保守の改善と業務の引継ぎ

運用・保守の改善とは？

- システムやその運用方法をより効率的に、より安全にするための取り組みのこと。

＜テキスト P67 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