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7回

第8編：具体的な構築・運用の実践【レベル3】

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	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10編	全体総括

セミナー内容

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

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.】
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.】
P4～P6

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.】
P6～P8

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

例

1. 実店舗での購入フロー（テキスト P7 図83 参照）
2. ECサイトでの購入フロー（テキスト P8 図84 参照）

要件定義

【参照：テキスト21-1-2.】
P8～P9

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.】
P9～P11

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 P9 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 P10 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 P10 参照＞

要件定義

【参照：テキスト21-1-2.】
P11～P12

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 P11 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 P11 参照＞

要件定義

【参照：テキスト21-1-2.】
P12～P13

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
- 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.】
P13～P24

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P17～P24参照。

要件定義

【参照：テキスト21-1-2.】
P24～P26

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 P24 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 P25 参照＞

要件定義

【参照：テキスト21-1-2.】
P26～P28

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 P26 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 P26 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 P27 参照＞

要件定義

【参照：テキスト21-1-2.】
P28～P29

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 P28 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 P28 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 P29 参照＞

要件定義

【参照：テキスト21-1-2.】
P29～P32

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 P29 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 P30 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 P31 参照>

要件定義

【参照：テキスト21-1-2.】
P32～P34

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 P32 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 P33 参照＞

要件定義

【参照：テキスト21-1-2.】
P34～P42

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 P34 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 P35 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 P41 参照＞

要件定義

【参照：テキスト21-1-2.】
P42～P57

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 P42 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 P43 参照＞

要件定義

【参照：テキスト21-1-2.】
P43～P57

Fit&Gap分析の実施方法（例）

1. 現状分析
   <テキスト P44 参照>
2. SaaS,パッケージソフトウェアの機能調査
   <テキスト P45 参照>
3. 比較分析
   <テキスト P46 参照>
4. ギャップへの対応検討
   <テキスト P53 参照>
5. 費用対効果の分析
   <テキスト P54 参照>
6. 実施計画の策定
   <テキスト P54 参照>

調達

【参照：テキスト21-1-3.】
P57～P61

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.】
P61～P63

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.】
P63～P65

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 P63 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 P64 参照＞

サービス・業務の運営と改善

【参照：テキスト21-1-5.】
P65～P71

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 P65 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 P69 参照＞

運用および保守

【参照：テキスト21-1-6.】
P71～P74

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。

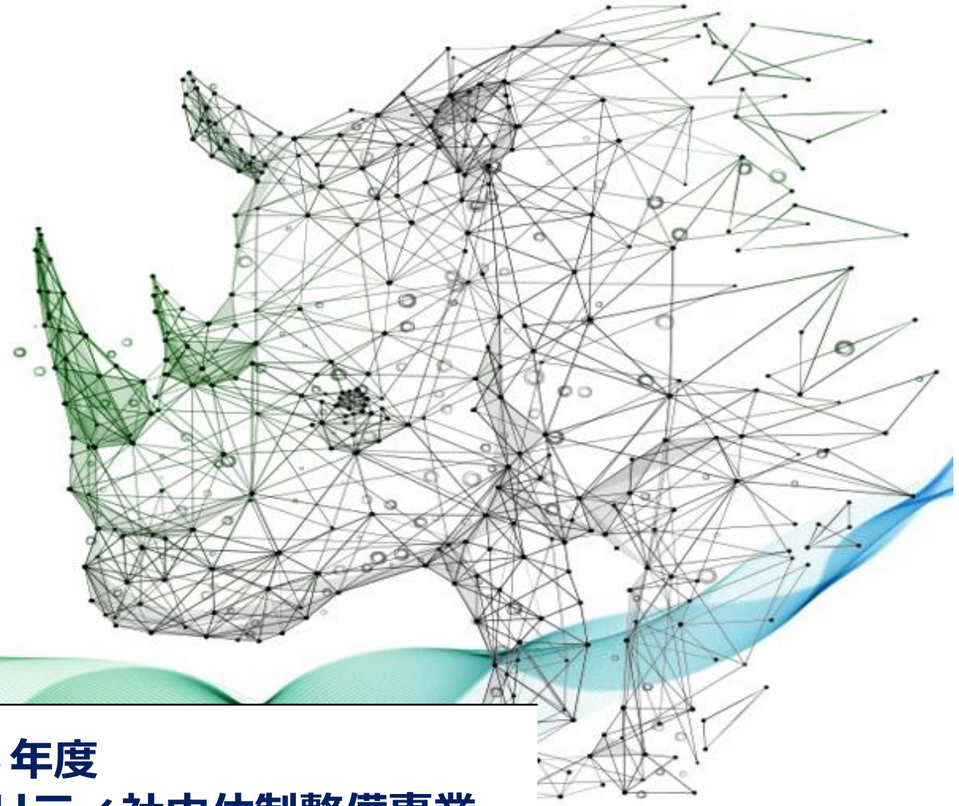
＜テキスト P71 参照＞

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 P72 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