

出題範囲とシラバスの一部改訂（iパス 6.3）の情報

IT パスポート試験（iパス）の出題範囲とシラバスの改訂が、IPA（独立行政法人 情報処理推進機構）より発表されています。

ここでは、改訂のポイントと追加用語などについて解説します。

【改訂のポイント】

◆改訂の目的

今回の改訂は、情報処理技術者試験を企業の DX（デジタルトランスフォーメーション）推進を担う人材育成に活用するための見直しとされています。

◆改訂の内容

具体的には、主に以下の内容が追加されています。

- ・ ビジネス変革、デザイン、データ利活用、AI 利活用などの知識
- ・ 数理・データサイエンス・AI モデルカリキュラムに関する用語
- ・ 情報セキュリティ管理分野における用語
- ・ すでに出題されている用語の取り込み など

iパスのシラバスについては、企業の環境問題への関わり、ソフトウェア開発技術の傾向、情報セキュリティに関する用語など、近年の環境変化や技術動向などを踏まえた情報の追加がみられます。

新シラバスに沿った出題は 2024 年 10 月試験から適用されます。なお、試験時間や出題数、採点方式、合格基準は従来どおりで変更はありません。

【試験対策】

出題内容が大幅に変更されたわけではなく、すでに過去の試験に出題された用語があとからシラバスに追加されたケースも含まれます。そのため、まずはこれまでの教材の範囲と過去問題によりしっかりと対策しておくことが重要です。

ただし、今回追加された用語や項目は、今後、出題頻度が高まることが考えられますので、用語や項目の意味はひとつと理解しておきましょう。

【追加された主な用語・項目】

以下に今回、シラバスに追加された用語の中から、主に企業と環境問題との関わりについての分野と、アジャイルを中心としたソフトウェア開発技術の知識、情報セキュリティ管理分野に含まれる用語・項目を中心に取り上げて解説します。

◆ストラテジ分野

カーボンニュートラル

地球温暖化対策として、二酸化炭素（CO₂）などの温室効果ガスの排出を抑えつつ吸収量を増やし、排出量と吸収量を均衡させることを目指す国際的な取り組みです。具体的には、再生可能エネルギーといった温室効果ガスの排出の少ないエネルギーへの置き換え、植林による緑化の促進などがあります。国や企業がそれぞれ目標を掲げて取り組んでいます。

グリーントランスフォーメーション（GX）

温室効果ガスの排出を抑制するカーボンニュートラル実現のため、石油や石炭などの化石燃料から太陽光や風力などのクリーンエネルギーに置き換えていく社会的な活動を指します。GX 実現には、国や企業から消費者までを含めた経済社会全体での取り組みが必要とされます。

GX 推進法

2023 年に成立した「脱炭素成長型経済構造への円滑な移行の推進に関する法律」の略称です。GX 推進と経済成長とを両立させるための基本方針と戦略、政策などが定められています。「GX 実現に向けた基本方針」に基づき、(1) GX 推進戦略の策定・実行、(2) GX 経済移行債の発行、(3) 成長志向型カーボンプライシング（次項参照）の導入、(4) GX 推進機構の設立、(5) 進捗評価と必要な見直し、を法定しています。

カーボンプライシング

企業などが排出する CO₂ に価格を付け、CO₂ 排出へのコストを負担させることで、排出抑制を促す政策手法です。石油や石炭などの化石燃料の使用に課税する「炭素税」や、企業ごとに CO₂ 排出量の上限を決め、それを超過する企業と下回る企業との間で CO₂ の排出量を取引する「排出量取引制度」などの手法があります。

カーボンフットプリント（CFP）

個々の製品やサービスについて、そのライフサイクル全体における温室効果ガスの排出量を CO₂ 排出量に換算し、製品やサービスに表示するしくみです。原材料調達から流通、廃棄、リサイクルなどに至る過程全体での温室効果ガスの排出量を可視化したものであり、その数値を明らかにすることで、消費者が脱炭素・低炭素な製品やサービスを選びやすくなります。

適格請求書等保存方式（インボイス制度）

2023 年から開始された、複数税率に対応した仕入税額の控除方式です。10%と 8%の 2 種類の税率を区分し、適格請求書（インボイス）に記載することで、消費税を正確に納付さ

せることを目的とします。

適格請求書には、売り手（適格請求書発行事業者）の登録番号と、適用税率と消費税額が記載されます。買い手は売り手から交付を受けた適格請求書を一定期間保存することで、仕入税額の控除を受けられます。

デジュレスタンダード

ISO や ITU、IEEE といった標準化団体が規定する公的規格の総称です。デファクトスタンダード（事実上の標準）と対義的な意味をもちます。

◆マネジメント分野

スクラム

アジャイル型ソフトウェア開発の代表的なフレームワークです。数人でスクラムチーム（次項参照）を組み、開発する機能の計画から実装までを細切れ（スプリント）にして短期間で行い、これを繰り返しながら継続的なリリースを続ける開発手法です。

スクラムチーム

スクラムによる開発の基本単位となるチームです。主にプロダクトオーナー 1 人、スクラムマスター 1 人、開発者 6～9 人程度で構成されます。

プロダクトオーナー（PO）	開発の方向性や結果などに対する最終責任者。チームに必要な情報の提供や意思決定などを行い、ステークホルダ※との調整も担う。プロダクトバックログ（次項参照）の作成・管理、優先順位の決定などに責任をもつ
スクラムマスター	チームが円滑に活動できるようメンバーを支援する役割。チーム活動の有効性に責任をもつ
開発者	スプリントバックログの開発を担うメンバー。さまざまなスキルをもつ人がチームを組み、自律的に行動する

※ステークホルダ：製品やサービス（プロダクト）の利用者、出資者、管理職などの利害関係者

スプリント

スクラムによる開発の基本単位となる小規模なプロジェクトです。1つのスプリントは1か月程度の期間であり、その中で計画や設計、開発、検査などの工程を繰り返し、リリース可能と評価できる成果物（インクリメント）をつくり上げます。1つのスプリントが完了したら、次のスプリントへ移行します。

スプリントでは、開発作業と並行して次の4つのイベントを行います。

スプリント プランニング	スプリント開始時に行う、チーム全体で作業計画（スプリントバックログ）を策定する会議。スプリントで開発する成果物をプロダクトバックログから選んで優先順位を決め、スプリントバックログに落とし込む
デイリースクラム	毎日 15 分ほどで行う、開発者を中心とした小会議。作業の調整や進捗の確認などを実施する
スプリントレビュー	スプリント中に作業した成果物の検査を行う。チームメンバーとともにステークホルダも参加する
スプリント レトロスペクティブ	スプリントの最後に行う、振り返りの会議。今回のスプリントの問題点とその原因、解決策などについて、チーム内で話し合い、次につなげる

プロダクトバックログ

スクラムで開発する製品やサービス（プロダクト）において、実現が必要な要素をリスト化したものです。プロダクトで提供すべき価値や機能などを、ステークホルダがプロダクトを利用する理由や目的を文章で表した「ユーザストーリー」などの形式で書き出し、挙げた項目を優先順位によって並べ替えます。

スプリントバックログ

各スプリントで行う作業をリスト化したものです。今回のスプリントで実現する要素をプロダクトバックログから選び、その実現に必要な作業を優先順位によって並べ替えます。開発者にとってはスプリントのスケジュールになります。

◆テクノロジー分野

リスクベース認証

ユーザ認証の方式の 1 つで、ユーザがシステムにアクセスする際の行動を分析してリスク評価を行い、その結果に応じて認証を行うものです。日頃の行動パターンから外れる行動を検知することで、利便性が損なわれることがなく、より確実な本人認証を行えるようになります。なりすましや不正ログインなどを防ぐ効果も期待できます。

一般的にはアクセスする場所や時間帯、利用デバイス、IP アドレスなどの情報をもとにリスク評価を行い、その結果に応じて認証の強度を決めます（パッシブ認証）。海外からのアクセスなど、日頃と異なる行動はリスクが高いと判断し、追加認証などを求めます。追加認証には、あらかじめ登録した秘密の質問に答えさせる、メールで送付した URL から再アクセスさせるなどの方法があります（アクティブ認証）。リスクが低いと判断した場合は、追加認証を行わないので、利便性とセキュリティ性を両立しやすいという特長があります。

認証の3要素

「知識情報」「所持情報」「生体情報」の3つの情報を指して「認証の3要素」といいます。

知識情報	ユーザが知識としてもっている情報による認証。文字や数字からなるパスワードなど
所持情報	ユーザがもっている物による認証。USB 認証器やハードウェアトークン、スマートフォンアプリで生成するワンタイムパスワードなど
生体情報	ユーザの指紋、顔、虹彩、声紋といった身体的特徴や、筆跡、キーストロークといった行動的特徴による認証

パスワードレス認証

ユーザ認証の方式の1つで、パスワードを使わずに本人を認証するものです。

パスワードの代わりに、認証器などによる所持情報、本人の身体的特徴などを使う生体情報、ユーザが登録したメールアドレス宛にシステムがメールを送信し、メールに記載されたリンクをユーザがクリックすることでアクセス権を付与する「マジックリンク」など、またはその組み合わせを使って認証します。

本人拒否率（FRR） / 他人受入率（FAR）

生体認証は、採取したサンプルとあらかじめ登録されたデータとを照合し、その類似度で本人かどうかを判断します。生体認証の精度は、本人拒否率（FRR）と他人受入率（FAR）という2つのエラー率を指標として表されます。

本人拒否率（FRR）	本人の生体情報を、本人ではないと誤って認証する割合
他人受入率（FAR）	他人の生体情報を、本人と誤って認識する割合

本人拒否率が高くなると利便性を害することになり、他人受入率が高くなると安全性を脅かす結果となるため、どちらの値も低くなるように設定するのが望ましいとされます。