目指せ！ 情報処理のエキスパート!!

国家試験に挑戦！ ～ITパスポート試験編～

ITパスポート試験（iパス）は、IT社会で働くすべての社会人が備えておくべきITに関する基礎的な知識が証明できる国家試験です。

問1　ストラテジ系【令和4年度・問24】

教師あり学習の事例に関する記述として，最も適切なものはどれか。

ア　衣料品を販売するサイトで，利用者が気に入った服の画像を送信すると，画像の特徴から利用者の好みを自動的に把握し，好みに合った商品を提案する。

イ　気温，天候，積雪，風などの条件を与えて，あらかじめ準備しておいたルールベースのプログラムによって，ゲレンデの状態がスキーに適しているか判断する。

ウ　麺類の山からアームを使って一人分を取り，容器に盛り付ける動作の訓練を繰り返したロボットが，弁当の盛り付けを上手に行う。

エ　録音された乳児の泣き声と，泣いている原因から成るデータを収集して入力することによって，乳児が泣いている原因を泣き声から推測する。

問2　マネジメント系【令和4年度・問44】

ITサービスマネジメントにおけるインシデント管理の目的として，適切なものはどれか。

ア　インシデントの原因を分析し，根本的な原因を解決することによって，インシデントの再発を防止する。

イ　サービスに対する全ての変更を一元的に管理することによって，変更に伴う障害発生などのリスクを低減する。

ウ　サービスを構成する全ての機器やソフトウェアに関する情報を最新，正確に維持管理する。

エ　インシデントによって中断しているサービスを可能な限り迅速に回復する。

問3　テクノロジ系【令和4年度・問68】

無線LANルータにおいて，外部から持ち込まれた端末用に設けられた，“ゲストポート”や“ゲストSSID”などと呼ばれる機能によって実現できることの説明として，適切なものはどれか。

ア　端末から内部ネットワークには接続をさせず，インターネットにだけ接続する。

イ　端末がマルウェアに感染していないかどうかを検査し，安全が確認された端末だけを接続する。

ウ　端末と無線LANルータのボタン操作だけで，端末から無線LANルータへの接続設定ができる。

エ　端末のSSIDの設定欄を空欄にしておけば，SSIDが分からなくても無線LANルータに接続できる。

正解：問1 エ　問2 エ　問3 ア

IPAとは

独立行政法人情報処理推進機構（IPA）は、経済産業省所管の政策実施機関です。
デジタル基盤の構築・提供、デジタル人材の育成、
サイバーセキュリティ対策の普及促進などの事業に取り組んでいます。

● 「IPA NEWS」定期送付のお申込み、送付先の変更、送付停止は、下記のメールアドレスにご連絡くださいますようお願い致します。
メール　**spd-ipanews@ipa.go.jp**

● 「IPA NEWS」アンケートはこちら

● IPAのSNS公式アカウント、メールニュースの配信登録はこちら
https://www.ipa.go.jp/

IPA 独立行政法人 情報処理推進機構
Information-technology Promotion Agency, Japan

VEGETABLE OIL INK
リサイクル適性Ⓐ この印刷物は、印刷用の紙へリサイクルできます。
R70 古紙パルプ配合率70％再生紙を使用

IPA NEWS vol.62
発行日　令和5年8月
独立行政法人情報処理推進機構
〒113-6591 東京都文京区本駒込二丁目28番8号　文京グリーンコートセンターオフィス
URL●https://www.ipa.go.jp/

IPA NEWS vol.62　8月号

「IPA NEWS」はIPAの日々の活動をわかりやすくご紹介する広報誌です。

特集　新理事長が語る「Society 5.0」と機構の役割

新生IPA、始動！

■ **セキュリティのすゝめ 11〈ECサイトを標的にしたサイバー攻撃が増加〉**
IPAのガイドラインで始める！
ECサイトのセキュリティ対策

■ **IPAの最新情報をまとめてお届け！**
Hot & New Topics

IPA
理事長
デジタルアーキテクチャ・
デザインセンター
センター長
齊藤裕さん

特集

新理事長が語る「Society 5.0」と機構の役割

新生IPA、始動！

IPAは今春就任した齊藤裕新理事長のもと、日本のデジタル競争力強化に向け、力強い一歩を踏み出しています。日本の産業界を取り巻く課題を踏まえ、新たな体制で何を目指すのか。デジタルエコシステム形成への戦略、Society 5.0が描く未来の社会像、そしてそれを実現するためのIPAの役割と第5期中期計画について齊藤新理事長が語ります。

日本の名目GDPはGAMAに劣るという現実

近年のデジタル技術の革新はすさまじく、データ駆動型ビジネスをベースとした新たな産業革命が勃興しているといえます。しかしながら、デジタル化の遅れる日本はこれに追随できていません。

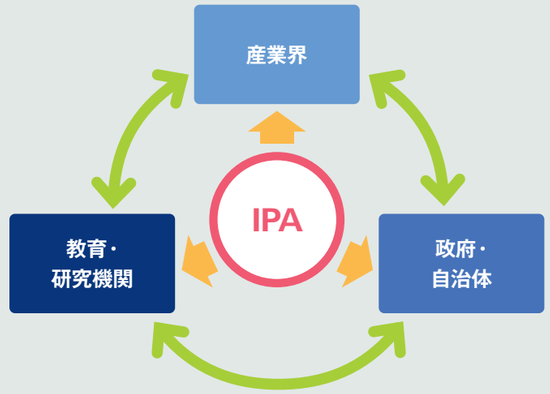
日本のデジタル競争力は世界63ヶ国中29位と過去最低を記録（IMD「世界デジタル競争力ランキング2022」）。この不振がGDPにも反映され、欧米や中国、韓国などデジタル化の進む国がGDPを右肩上がりで高めているのに対し、日本のGDP成長は20年以上低迷の一途をたどっているのです。いまや日本の名目GDPは、巨大プラットフォーマーであるGAMA（Google、Apple、Meta、Amazon）の合計時価総額にも及ばないという嘆かわしい状況です。事態の改善に乗り出さなければ、日本の産業競争力は衰退するばかりです。また、日本が海外勢のプラットフォームの大口顧客になっているということでいえば、支出の増大、雇用基盤の弱体化、データの流出、ひいては国力の地盤沈下までもが懸念されます。日本のデジタル競争力の底上げは、待ったなしで取り組むべき課題といえるでしょう。

複数サービスの連携がプラットフォーマーの手法

GAMAのようなプラットフォーマーの強みは、さまざまなパートナー企業がデジタル経済圏を築いて共存共栄する仕組み、すなわち“デジタルエコシステム”を形成している点です。参加するプレイヤーがデジタルの力でデータを効率よく収集・共有・利活用し、さらにこれらワークフローの全体最適を実現することで複数のサービスを連携させ、顧客に最大の付加価値を提供していく。それが今、世界を席巻するデジタルプラットフォーマーのビジネスモデルなのです。

翻って、日本ではそうしたエコシステムがつくられていません。企業が技術や知見を囲い込む高度成長期のような風潮が未だ根強くありますし、また業界を横断して特定の企業がリーダーシップを取ろうとしても公平性や信頼性の面で障壁が大きく、実現に至らないといった背景があるからです。つまり、企業や団体に連携を働きかけつつ、全体を見渡せる調整役がいないということです。

図表1　IPAが目指すデジタルエコシステムの形



IPAが調整役を担って協調領域をデザインする

ここにこそ、IPAの新たな存在意義があると考えます。世界に肩を並べるデジタルエコシステムの形成に向けて、「産業界」「政府・自治体」「教育・研究機関」の間を取り持つのは、経済産業省のIT政策実施機関であり、かつ企業や研究機関とも関係の深いIPAが適切であろうと思います。多彩なスキルや知見を持つ各界の人材をつなぐ場を創出し、共通資産としてデータを共有・活用して、データから社会価値を創出し再びデータに還元、さらなる活用を図るべく、IPAがハブとなるということです（図表1）。

協調領域をしっかりデザインすることで多くの企業が参入しやすくなり、健全な競争が促され、なおかつ社会的コストも抑えられます。日本の企業が力を結集できる形を整えることで、海外勢に負けない技術革新がもたらされるのではないでしょうか。

この延長線上に実現するのが、政府が描く未来像である「Society 5.0」にほかなりません。AIやIoT、ロボットなどを活用してルーチンの自動化・効率化を図り、人間の創造性をいっそう拡大する豊かな社会を多くのキープレイヤーとともにつくり上げる――。そんなビジョンを掲げ、IPAではデジタル社会のアーキテクチャを設計する官民連携の場として、2020年にデジタルアーキテクチャ・デザインセンター（DADC）を創設しました。私はそのセンター長を務め、理事長となった今も兼務しています。IPAでは同センターのこれまでの実績や知見を踏まえつつ、設計したアーキテクチャを実装する際に必要な基盤の構築・運用を担うデジタル基盤センターをこのたび新設しました。官と民の中間で相互運用性を担保する基盤を確立するのが狙いです。

第5期中期計画における事業の3つの柱

官民連携で価値を創出する調整役としてIPAは新たなスタートを切り、日本のデジタル競争力向上に邁進していきます。具体的には、第5期中期計画における事業の3つの柱を次の通り策定しました。

①デジタル基盤の提供

前述の通り、エコシステムを形成するには関係各所が広く活用できる協調領域の整備が欠かせません。Society 5.0の実現に向けたアーキテクチャの設計、インフラの標準化、データモデルの統合化など、デジタル化に必要なさまざまな要素を官民で連携しながら取り揃え、提供していきます。

②デジタル人材の育成

デジタル化やDX（デジタルトランスフォーメーション）を推進するには、当然ながらデジタル人材を増やす必要があります。IPAではこれまでも試験制度の運用等を通じてデジタル人材の育成に貢献してきました。今後、人材の育成をいっそう加速するため、デジタル人材に適した評価（アセスメント）も視野に入れていきたいと考えています。

③サイバーセキュリティの確保

Society 5.0は現実空間とサイバー空間が融合するサイバーフィジカルシステムであるため、サイバー攻撃が現実社会に与える影響が甚大となります。従って、サイバーセキュリティを遺漏なく確保しなければなりません。これまでIPAが取り組んできたサイバーセキュリティは、「不審な動きやインシデントなど、何かが起きてからの対処」が主でした。しかし、今やサイバー攻撃は地政学リスク、経済安全保障リスクとして認識されるようになり、取り組みのパラダイム転換が世界的に求められています。今後は、サイバー攻撃の意図を地政学的な見地から読み取る「サイバー状況把握力」の強化によって予見性を高めつつ、これに加えてシステムの設計段階から脆弱性をあらかじめ排除する「セキュリティバイデザイン」の発想も問われることで

人間の創造性を拡大する豊かな社会を、多くのプレイヤーと共創する

しょう。状況把握とシステムの両面からリスクマネジメントを先回りする視点もこれからの事業に必要だと考えています。

また、これら3つの柱を実現するには、IPAの内部にさまざまな知見や専門性が問われることになります。機構職員自らがデジタル人材となり、社会に対してその価値を体現することが重要で、「業務運営の効率化」も事業に共通の課題ととらえています（図表2）。

人に寄り添ったデジタル化を実現

日本は現状では精彩を欠いているものの、優れた技術力や知見、ノウハウの蓄積があります。社会の至るところに散らばるそうした宝を横断的に連携してデジタルエコシステムを築くことで、世界に類を見ないサイバーフィジカルシステムを編み出すことは決して夢ではありません。そして、それを海外に展開すればGAMAのような世界標準となるプラットフォームを日本起点でつくることができるのではないでしょうか。

注意したいのは、これからのビジネスで鍵を握るのがデータであるということ。GAMAのような巨大IT企業を日本に1社つくるのではなく、さまざまな企業や組織が持つデータをみんなが活用できるようにすれば、それだけ強いエコシステムを生み出すことができますし、それは日本の競争力の回復にもつながることでしょう。

私自身、製造現場のエンジニアとして長く経験を積んできました。「ジャパン・アズ・ナンバーワン」といわれた時代は、ものづくりで世界トップを目指そうという機運が現場にみなぎっていたものです。そうした現場の力が、企業の成長を牽引する原動力のひとつになっていたことは間違いありません。

サイバーフィジカルシステムではデジタルとモノがつながりますから、日本のものづくりの技術が再び脚光を浴びるはずです。環境を整えることで日本の競争力のV字回復を側面から支援し、かつてのような世界トップを目指せる環境を次世代のエンジニアに提供していきたいと思っています。世界で活躍できるエンジニアを増やし、産業界を活性化することで、今の日本を覆う閉塞感も取り払われていくのではないでしょうか。

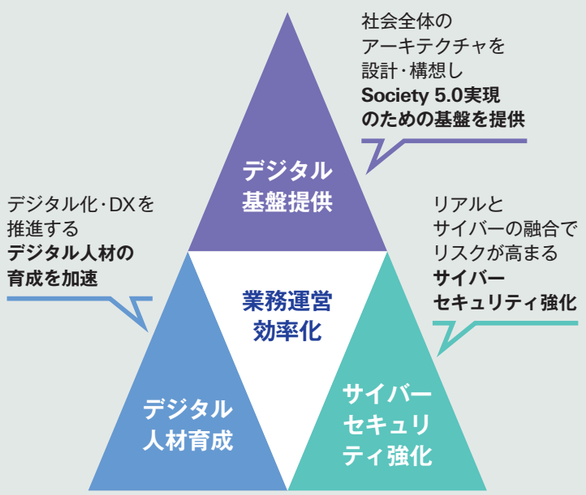
Society 5.0は、テクノロジーを活用して人間中心の社会を実現するものです。年齢や住む地域による情報格差がなくなれば、誰もがいきいきと暮らせる社会になりますし、さらにデジタル化でルーチンワークが自動化されることで、働き手は個々の持ち味を存分に生かせるようにもなるでしょう。

いわば、人に寄り添ったデジタル化を実現すること――。その究極の目標に向け、私たちIPAはさらに力を尽くしていきます。

人に寄り添ったデジタル化を実現するために、さらに力を尽くす

「人に寄り添ったデジタル化を実現するために尽力したい」と齊藤理事長

図表2　第5期中期計画における事業の3つの柱



齊藤理事長がIPAのミッション・ビジョン・バリューとともに、IPAが求める人材像について語った
ウェブ限定記事はこちら… https://www.ipa.go.jp/about/ipanews/ipanews202308.html#specialissue_weblimited

中小企業の自社開発サイトに被害が多数発生

IPAのガイドラインで始める！ ECサイトのセキュリティ対策

! 事故対応費用に約1億円かかった会社も

通販サイトなどECサイトを標的としたサイバー攻撃が増え、ユーザーの個人情報やクレジットカード情報を窃取されたり、クレジットカードを不正利用されたりする被害が後を絶ちません。国内発行クレジットカードにおける年間不正利用被害総額は、2016年が142億円だったのに比べ、2022年は約436億円へと3倍以上に達しています（日本クレジット協会調べ）。

被害の大半を占めるのは、中小企業が独自に構築したサイトです。「売上が少ないので狙われるはずがない」という思い込みが、危機意識の低下につながっているとみられます。そして、それが構築プログラムのアップデートを怠る、単純なID・パスワードを設定する、開発・運用の委託先とのセキュリティ契約に不備が生じるなど、ECサイトの脆弱性が放置される結果となっているのです。

しかし、ひとたび事故や被害が発生すると、サイト閉鎖に伴う売上の減少、信用の失墜、原因調査や補償といった事故対応費用の支出など、甚大な損失を生みかねません。実際、被害に遭ってECサイトを閉鎖した場合の売上高の平均損失額は約5,700万円。事故対応費用の平均額は約2,400万円（いずれも1社あたり）にも上ります。中には事故対応費用に約1億円かかった会社もあり、事前のセキュリティ対策の重要性がうかがえます。

! “初めの一歩”として役立つガイドライン

顧客やカード会社からの指摘で初めて被害に気づき、それまで数年にわたって情報を抜き取られていたことが明らかになったケースもあります。「自社のECサイトもすでに攻撃を受けているかもしれない」という緊張感をもって早急に対策をとりましょう。

IPAではECサイト構築・運用時のセキュリティ対策をまとめた「ECサイト構築・運用セキュリティガイドライン」を2023年3月に公開しました。ECサイトを持つ中小企業への調査を踏まえつつ、専門家の知見もふんだんに盛り込んで、ECサイト構築・運用時に必要なセキュリティ対策をわかりやすく解説。「経営者編」と「実践編」から成る構成で、最低限取り組むべきセキュリティ対策を示しており、全社での取り組みの“初めの一歩”を踏み出す際に役立ちます。

ECサイトを新規で立ち上げる事業者やECサイトを運営している事業者の経営者、実務担当者はぜひ活用してください。具体的なセキュリティ対策の一部を図に示しました。

また、必要な対策の全項目および「ECサイト構築・運用セキュリティガイドライン」は下記のリンクから参照できます。経営者と担当者で一緒にチェックを行い、安心・安全なECサイトの構築、運用にチーム一丸となって取り組みましょう。

ECサイト構築＆運用時におけるセキュリティ対策要件（抜粋）

〈構築時〉
- □ サーバ及び管理端末等で利用しているソフトウェアをセキュリティパッチ等により最新の状態にする。
- □ 管理者画面や管理用ソフトウェアへ接続する端末を制限する。
- □ サイト利用者情報の登録時及びパスワード入力時における、不正ログイン対策を実施する。

〈運用時〉
- □ ECサイトへの脆弱性診断を定期的及びカスタマイズを行った際に行い、見つかった脆弱性を対策する。
- □ システムの定期的なバックアップの取得及びアクセスログの定期的な確認を行い不正アクセス等があればアクセスの制限等の対策を実施する。

※いずれの項目も、自社で対応困難な場合は外部委託先の活用により対策を実施する。

＋ 対策のポイント ＋

1. 「自分たちは大丈夫」という慢心は禁物！
2. サイバー攻撃は重大な経営リスクと認識する。
3. 対策を徹底し、ECサイトの脆弱性を放置しない。
4. ガイドラインを活用し、全社レベルの取り組みに。

- **対策の全項目を見たい方は…** https://www.ipa.go.jp/about/ipanews/ipanews202308.html#security_weblimited
- **ガイドラインを見たい方は…** https://www.ipa.go.jp/security/guide/vuln/guideforecsite.html

IPAの最新情報をまとめてお届け！

Hot & New Topics

重要インフラ業界の事故原因究明調査のための施設を開設

近年、重要インフラや社会基盤を狙ったサイバー攻撃が、国内のライフラインなどに被害を及ぼす事案が増えています。こうした中、日本では2022年6月に高圧ガス保安法等が改正され、電力、ガス、高圧ガス分野のプラントなどで重大な事故等が発生した場合にサイバーセキュリティの観点から原因究明の調査を行うことが規定されました。この調査事業を担うIPAでは、本法案の施行（2023年12月頃）に向けた体制整備の一環として新施設を立ち上げました。欧米各国ではサイバーセキュリティに関する事故調査の法整備が進む一方、日本では対応の遅れが課題となっています。国内初のサイバーセキュリティに関する調査機関としてIPAが機能し、事故原因が明らかになることで重要インフラ業界におけるサイバーリスクへの対応方針の検討やガイドラインの策定などが可能になり、防護力の向上につながることが期待されます。

6月に開催された関係者向け施設見学会

産業用制御システム向け侵入検知製品等の導入手引書を公開

近年、重要インフラや工場の製造ラインなどを支える産業用制御システムでもインターネットの活用が進み、これによってサイバー攻撃の被害を受けるリスクが高まっています。これらのリスクへの有効な対策のひとつが、産業用制御システムや制御ネットワークへの不正侵入を検知する製品等の活用です。本手引きは、産業用制御システムを有する企業のシステム運用者や管理者などを対象に、産業用制御システム向け侵入検知製品等の導入や運用の方法を解説したもので、製品タイプの類型的な特長や導入の各フェーズにおける検討のポイント、有効な運用方法などを紹介しています。初めて製品を活用する場合でも製品の選定や導入・運用を円滑に進めることができます。

https://www.ipa.go.jp/security/controlsystem/icsidshandbook.html

● 本手引きの全体構成

第1章 手引き作成の背景と目的
第2章 侵入検知製品等の基本事項
第3章 侵入検知製品等の導入の進め方
第4章 侵入検知製品等の導入後の留意点
付録 本手引きで用いている主な用語の説明

● 侵入検知製品等を使う際の導入検討から本格運用まで

❶ 導入検討フェーズ
- 導入目的の明確化
- 目的を達成するための取り組み方針の決定
- 製品等への投資判断

❷ 構築フェーズ
- 現状の把握
- 最適な構築・運用方針の検討
- 製品等の選定
- 製品等の設置

❸ 試験運用フェーズ
- 体制の整備
- 機能検証
- 検知ポリシーの設定・チューニング
- （必要に応じて）カスタマイズ

❹ 本格運用フェーズ
- アラート・ログの監視と脅威の検出・判定
- 検出された脅威への対処
- 経営層への報告

「未踏ターゲット事業」に新たなターゲット分野を追加

先進分野のIT人材を発掘・育成する「未踏ターゲット事業」は、2018年度の事業開始以降、「量子コンピューティング技術を活用したソフトウェア開発」をターゲット分野に据えてプロジェクトを募集し、その支援によってIT人材の育成に寄与してきました。今年度からは「リザバーコンピューティング技術を活用したソフトウェア開発」を新たに加え、先進分野の人材育成を推進します。リザバーコンピューティングは時系列情報処理に適した機械学習の枠組みのひとつで、少量のデータでの高速学習が可能な技術として研究開発の進展が期待される分野です。IPAでは採択したプロジェクトに対して今年10月から約5ヶ月間のサポートを行う予定です。

https://www.ipa.go.jp/pressrelease/2023/press20230703.html

● リザバーコンピューティング技術を活用したソフトウェア開発

募集プロジェクトの要件（一部抜粋）

【ニューラルネットワークリザバーに関する対象領域例】
- モデル・アーキテクチャの高性能化・高効率化に関する開発・性能評価
  （例：他の機械学習モデルや脳情報処理の仕組みを活用するもの）
- アプリケーションに適した学習アルゴリズムの開発・性能評価
  （例：予測、分類、異常検知、制御）

【物理リザバーに関する対象領域例】
- 自然・物理現象を用いたリザバーの開発・性能評価
  （すでにリザバーとして機能しうる物理系の準備があることが望ましい）
- 自然・物理現象を用いたリザバーのシミュレータ開発・性能評価

公募・審査：2023年7月上旬～9月上旬
採択：2023年9月下旬～10月上旬
サポート内容：
- PMによる技術的なアドバイスや助言
- 開発資金（上限200万円）の提供

Just Information

制御システムのセキュリティ演習プログラムを開催！

制御システムを有する企業の皆さまを対象にした2つの演習プログラムを開催します。いずれもグループワークを中心とした構成で、制御システムを狙うサイバー攻撃への対応スキルを習得することができます。また、参加者同士のコミュニケーションから他業界や他社とのつながりを深め、新たな視点での知見を得ることもできます。両プログラムは情報処理安全確保支援士の実践講習としても参加いただけますので、ぜひお申込みください。

【責任者向け】

業界別サイバーレジリエンス強化演習（CyberREX）

サイバー攻撃を受けた際の被害を最小化し、素早いリカバリーを行うための対応力・回復力である「サイバーレジリエンス」を強化し、組織全体のセキュリティレベルの向上を目指す2日間のプログラムです。各業界の特性を踏まえたインシデント対応演習で、攻撃検知から一次対応、回復までの一連の流れに関する知識・ノウハウを習得できます。

開催日：2023年9月21日（木）・22日（金）
対象：石油、素材、化学、製薬、金属、鉄鋼、電力、ガス、ビル、医療業界のCISO相当やマネジメント層の方
会場：IPA（秋葉原UDX：東京都千代田区）
申込み期限：2023年8月25日（金）

https://www.ipa.go.jp/jinzai/ics/short-pgm/cyberrex/2023-2.html

【実務者向け】

制御システム向けサイバーセキュリティ演習（CyberSTIX）

産業用制御システムを狙ったサイバー攻撃とその攻撃への対処方法を学習する2日間のプログラム。制御システムへのサイバー攻撃と攻撃によるオペレーションの混乱を体験しながら、攻撃の分析や防御手法などについて学んでいきます。模擬システムを用いたハンズオン演習で、現場でも役立つ実践的な対応スキルを習得できます。

開催日：2023年9月25日（月）・26日（火）
対象：制御システムのサイバーセキュリティ担当者
会場：IPA（東京都文京区）
申込み期限：2023年8月25日（金）

https://www.ipa.go.jp/jinzai/ics/short-pgm/cyberstix/2023-2.html