IPA NEWS vol.69 11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 組織のセキュリティ戦略を牽引するリーダーへ

「実戦力」と「人脈」を磨け！ 中核人材育成プログラムの1年

- セキュリティのすゝめ 18〈フィッシング詐欺の手口と対策〉
  情報窃取や金銭被害の危険も！
  「フィッシング詐欺」にご用心
- IPAの最新情報をまとめてお届け！
  Hot & New Topics

阪急阪神ホールディングス
株式会社
リスクマネジメント推進室
情報セキュリティ推進部
課長補佐
久保貴司さん（中央）

阪急阪神ホールディングス
株式会社
リスクマネジメント推進室
情報セキュリティ推進部長
松本寿也さん（右）

IPA
産業サイバーセキュリティセンター
調査分析部
サイバーインシデント調査室 室長
中山顕さん（左）

特集

組織のセキュリティ戦略を牽引するリーダーへ

「実戦力」と「人脈」を磨け！ 中核人材育成プログラムの1年

企業の制御システムのセキュリティ施策を担う人材を育てるIPAの「中核人材育成プログラム」。その第7期（2023年度）に参加した受講者・久保貴司さんの1年に密着し、講義の内容や成長の様子、業界を超えた人脈が形成されるプロセスなどをレポートします。久保さんの派遣を決めた上司の方やIPAのコーディネーターにも話をうかがいました。

開講～プライマリー

まるで大学の講義のよう。学ぶのが面白い！

「中核人材育成プログラム」（以下、本プログラム）は、企業などの経営層と現場担当者をつなぐ「中核人材」の育成を目的とした1年間のフルタイム・プログラムです（図表）。各業界の現場を想定した模擬プラントを使用してOT（制御技術）とIT（情報技術）のスキルを習得できるだけでなく、グループワークを通じた業務推進能力やリーダーシップも身につき、さらに業界を超えた人脈を築けるのも大きな魅力。2017年の開講以来、400名以上の中核人材を育成・輩出してきました。

第7期（2023年7月～2024年6月実施）は鉄道や航空、電力、ガスなどの重要インフラ事業者や産業基盤事業者などから65名が参加。その一人が阪急阪神ホールディングス株式会社の久保貴司さんです。「セキュリティは門外漢で、講義についていけるか不安」といいつつ、「会社の期待に応えるため、また鉄道業界のセキュリティ水準を底上げするためにもがんばります。当社から本プログラムへの派遣は初めてで、後進に道を開く意味でもたくさんの知見や経験を持ち帰れたら」と意気込みを語ります。

プログラムの幕開けは、OTとITの基礎を座学中心で学ぶ「プライマリー」。「大学の講義のようでついていくのに必死ですけれども、新しいことを学ぶのは面白いです」と久保さん。受講者間のレベル合わせを行うと同時に親睦を図る期間でもあり、「飲み会もあって、まるで学生時代に戻ったかのよう。みなさんとスムーズに馴染めています。特に同じ鉄道業界の受講者6名とは会ってすぐ打ち解けました」と笑顔が弾けました。

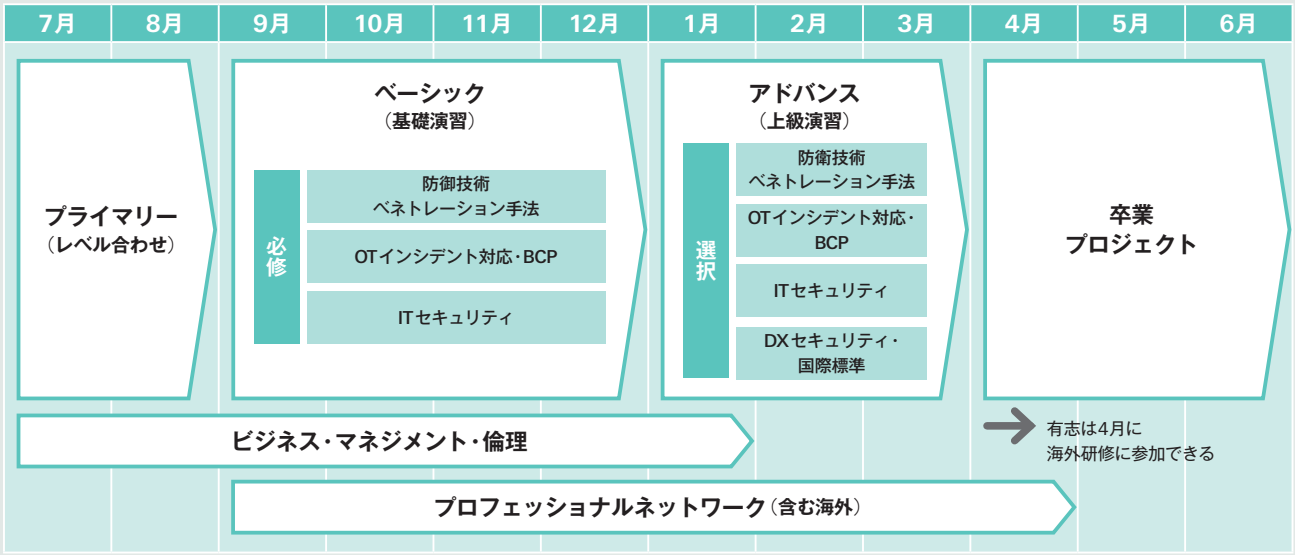
ベーシック

模擬プラントに攻撃が！上司の「授業参観」に緊張

9月からはOTやITのセキュリティ、BCPなどの考え方を網羅的に習得する「ベーシック（基礎演習）」期間がスタート。演習を主体に、次の3つのテーマを学んでいきます。

【防衛技術・ペネトレーション手法】施設管理やスマートグリッド、工場などの実設備に近い模擬プラ

図表　中核人材育成プログラムの年間カレンダー



ントに講師がサイバー攻撃を仕掛け、それにグループで対処。「多様な業界のセキュリティを学べると同時に、他グループの対処も勉強になります」と久保さん。鉄鋼や精密機器の工場も見学し、現場の物理的対策の考え方を体感しました。

【OTインシデント対応・BCP】シナリオに沿って模擬プラントにサイバー攻撃を再現。防衛策や検知方法をグループで討議します。「社内向け教育訓練やインシデント対応の演習では、セキュリティ対策を従業員にどう周知し、インシデント発生時にどうコミュニケーションを取ればよいか、具体的なヒントを得ることができました」

【ITセキュリティ】OTセキュリティ実現のためのIT設計やインシデント発生時の対応を学びます。講師が仕掛けたサイバー攻撃を解析し、社の上層部に報告するという設定で演習を2回実施。1回目は受講者の実際の責任者の方々に報告をしました。久保さんは「授業参観のようで緊張しました（笑）。報告では、事業への影響や今後の対策など意思決定に資する情報の提供を心がけました。有事に活きる貴重な経験ができました」と語ります。また、修了者コミュニティである叶会（かなえかい）の情報交換会や、課外活動としてセキュリティのスキルと知識を問う外部の競技会にも参加。学びと人脈に磨きをかけました。

アドバンス

鉄道業界の防衛技術を探求。海外関連機関での演習も

12月中旬から、より高度なトレーニングや演習を通じて知見の向上を目指す「アドバンス（上級演習）」期間へ突入。コースはベーシック期間の3テーマに、AIや産業向けIoT、商用クラウドなどのセキュリティ課題や国際標準を学ぶ**【DXセキュリティ・国際標準】**を加えた4テーマで、久保さんは防衛技術とITセキュリティを選びました。

防衛技術では鉄道メンバー6名でチームを組み、OTとITを組み合わせた業務に近い環境で防衛策を探求しました。「他の鉄道会社の方と協働できる貴重な機会」と、久保さんは目を輝かせます。また、別のメンバーとは、セキュリティ製品について攻撃の検知機能を比較する研究も行いました。ITセキュリティコースでは、グループ内で攻撃と防御に分かれて競う演習などを行い、実戦力を強化できたといいます。さまざまな演習を重ね、中核人材としての力量を着実に高めてきた久保さん。「OTシステムのどこが危険か、どう防ぎ、どう上司へ報告すべきかなどがわかってきました」と手ごたえを語ります。

イギリスとフランスへの海外派遣演習にも参加。政府系機関や研究施設を訪れ、見聞を広げました。

演習を重ね、OTシステムの防御の勘どころがわかってきた

卒プロ～修了

ここで得た知識や人脈はかけがえのない財産

4月、習得した知識や経験の集大成となる卒業プロジェクトが開始。企業や業界のセキュリティをテーマとした課題にグループで取り組みます。受講者が持ち寄った約20のテーマのうち、久保さんは次の4つに参加しました。

■ **鉄道の運行管理システムのセキュリティ対策**……久保さんがリーダーとなって、鉄道メンバーが集結。リスク分析から対策までを体系化したマニュアルと、サイバー攻撃の検知のしくみの高度化策を

まとめたドキュメントの2つの成果物を制作しました。

■ **脅威インテリジェンス導入・運用ガイドラインの作成**……攻撃の動向や危険性の高い情報を把握するサービスやツールの活用ガイドラインを作成しました。

■ **スタートアップ企業のセキュリティ強化**……啓発動画「Visionary Security ～Zeroから始めるセキュリティ対策～」の作成や大学起業部での講演を行いました。

■ **セキュリティ啓発コンテンツの開発**……ゲームを通じて従業員のセキュリティ意識を高めることを目的に、「コミュニケーションで乗り切れ！ サイバーインシデント対応24時」と「セキュリティホライゾン ここから始めるIoTセキュリティ」を制作しました。

目を見張る成長をみせた久保さん。修了式では修了者代表としてあいさつを述べました。苦楽をともにした同期生ともお別れ。「ここで得た知識や人脈はかけがえのない財産になりました」

帰任後

卒プロを部会に。同期生との交流はこれからも

7月、阪急阪神ホールディングスに帰任した久保さんは、新設されたリスクマネジメント推進室の情報セキュリティ推進部で新たな一歩を踏み出しました。グループのセキュリティ施策のとりまとめやインシデント対応、教育訓練などを担う部署で、まさに久保さんに最適な業務といえそうです。

帰任後も同期生とはオンラインで交流し、一部の卒業プロジェクトを部会にする動きもあるとか。叶会の関西部会にも入会し、1～7期の縦のつながりもできました。

グループのセキュリティ強化に貢献したい

OTのセキュリティについて業界横断で連携体制を築くことは本プログラムの目的のひとつ。「獲得した実戦力と人脈を業務に還元し、グループのセキュリティレベルの向上に貢献していきたい。第8期にも当社から人材を派遣しているので、共通言語で話せる仲間をグループ全体に増やす橋渡し役になれたらと思います」と久保さん。

阪急阪神ホールディングスグループと鉄道業界のさらなるセキュリティ強化に向け、久保さんの活躍が期待されます。

たくましく成長した久保さんを頼りにしています

久保さんの派遣を決めた上司 **松本さん**

セキュリティが経営課題のひとつとなる中、当社としてもセキュリティに取り組む中核人材を育成していく方針を掲げ、その一環として本プログラムを利用しました。

久保さんに白羽の矢を立てたのは、鉄道事業で重要インフラの整備に携わったり、本社の管理部門でリスクマネジメントに携わったりといった業務経験から。1年しっかり学んで、セキュリティに関する幅広い知識を身につけたという印象ですね。卒業プロジェクトでリーダーとしてメンバーの方々をまとめた経験も業務に生きると思います。

久保さんにはグループ全体のセキュリティを高める、まさに中核人材として活動していただきたい。万が一、セキュリティインシデントがあった場合には、ホールディングスの中心となるのはもちろんのこと、現場に赴いて対処を指揮することも望まれます。たくましく成長した久保さんを頼りにしています。

リピート利用の多さも特徴。価値ある人材が育つ場

プログラムのコーディネーター **中山さん**

コーディネーターとして、また卒業プロジェクトの副メンターとして、受講者はみんな教え子のようなもの。必死に勉強して成長していく姿を見守ることが一番のやりがいです。

久保さんは生来の人柄のよさに加え、知識やスキルも養い、この1年で人材として磨きがかかりました。困難を突破する力もありますね。よい仲間もたくさん得ましたし、壁にぶつかったとしても乗り越えていけると信じています。

本プログラムの修了者の中には、現在セキュリティ部門の管理職として本プログラムに人材を送り出す側になっている方もおられます。参加企業・組織と長期的な関係を維持できていることは、本プログラムへの評価の表れでもあるでしょう。叶会は貴重な人脈形成の場でもあり、価値ある人材が育つことは、これまでの実績からみて間違いのないこと。経者者や管理職の方には、ぜひ本プログラムの利用を検討いただければと思います。

- **プログラムに対する評価や人材を送り出すことの意義を松本さんが語るウェブ限定記事はこちら**
  https://www.ipa.go.jp/about/ipanews/ipanews202411.html#specialissue_weblimited
- **中核人材育成プログラムの詳しい内容はこちら。各期の卒業プロジェクトも紹介しています。**
  https://www.ipa.go.jp/jinzai/ics/core_human_resource/index.html

メールやSMSから巧妙に偽サイトへ誘導

情報窃取や金銭被害の危険も！「フィッシング詐欺」にご用心

不正なメール送信など、さらなる攻撃の踏み台にも

実在する組織やサービスをかたってメールやSMSを送り付け、その中に偽のウェブサイトへのリンクを仕込んで誘導し重要情報をだましとる「フィッシング詐欺」の相談が、IPAへ継続的に寄せられています。この手法で詐取される情報は大きく2つ。ひとつが「個人情報」です。住所・氏名などの基礎情報のほか、身分証明書に関する情報は本人になりすまして契約行為などに悪用される可能性があり、クレジットカード情報や銀行口座の暗証番号などが盗み取られた場合は不正な決済や送金につながる危険があります。もうひとつの重要情報がウェブサービスのログインに必要な「IDやパスワード」です。不正ログインされ、さらなる情報の窃取を招くばかりか、不正なメールの送信など、さらなる攻撃の踏み台として悪用される危険があります。

金融庁の発表では、2023年11月末でフィッシング詐欺によるとみられるインターネットバンキングの預金不正送金は被害件数5,147件、被害額約80.1億円と、いずれも過去最多を更新。フィッシング対策協議会の発表（下図）でも2024年7月のフィッシング報告件数は17万7,855件と、前月比約23.4%増となり、対策が必要です。

実物のデザインを盗用。真偽の見極めは困難

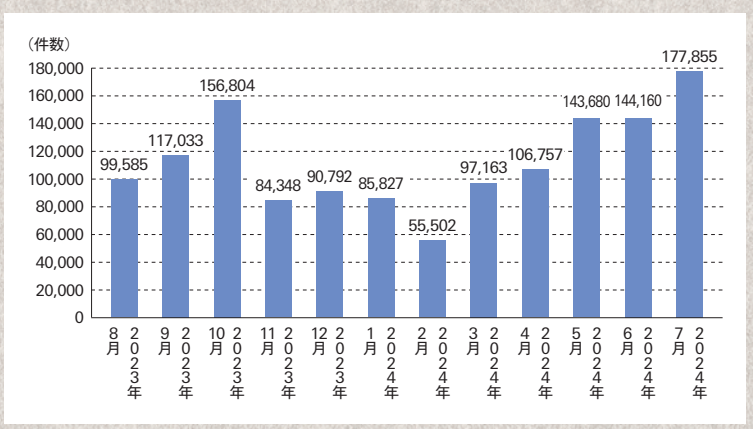
フィッシング詐欺でかたられるのは宅配・通販・銀行・カードなどの事業者が多いものの、最近はかたられる事業者が多様化しているうえ、リアルタイムフィッシングやQRコードを悪用したフィッシングなど手口の進化もみられます（詳細は下記URLより参照ください）。事業者が発行する実際のメールの文面や本物のサイトのデザインが盗用されることもあり、見た目で真偽を見抜くことは困難です。対策として、以下を徹底しましょう。

まずは、メールフィルタなどのセキュリティ対策サービスを導入すること。攻撃のすべてをブロックすることはできませんが、基本的な対策として有効です。また、少しでも不審に思ったらメールやSMSを開封しないこと。開封したとしても、添付ファイルやURLリンクはクリックしないでください。迷う場合は、そのメールやSMSのリンクからウェブサイトへアクセスするのではなく、ブラウザのブックマーク（お気に入り）や検索結果から正規のサイトにアクセスしましょう。

組織に所属していて、不審なメールやSMSを受信した際の対応マニュアルがあれば、それに従ってください。フィッシングサイトにアクセスしてしまった場合も、定められた連絡先へ迅速に報告・相談することが重要です。

IPAの情報セキュリティ安心相談窓口でも相談を受け付けています。

フィッシング対策協議会に寄せられたフィッシング報告件数（海外含む）



フィッシング対策協議会の下記URL掲載データをもとにIPAが作図
https://www.antiphishing.jp/report/monthly/202407.html

＋ 対策のポイント ＋

1. メールフィルタなどセキュリティ対策サービスを導入する
2. 不審なメールやSMSは不用意にURLリンクをクリックしない
3. サイトへのアクセスは正規のURLから行う
4. 所属組織で対応が決まっている場合はそれに従う

- 最新のフィッシング詐欺の手口についてはこちら　https://www.ipa.go.jp/about/ipanews/ipanews202411.html#security_weblimited
- IPA安心相談窓口だより　https://www.ipa.go.jp/security/anshin/attention/2021/mgdayori20210831.html
- 情報セキュリティ安心相談窓口　https://www.ipa.go.jp/security/anshin/about.html
- フィッシングに関するサイトやメールの報告はフィッシング対策協議会で受け付けています。　https://www.antiphishing.jp/

IPAの最新情報をまとめてお届け！

Hot & New Topics

サポート詐欺の手口・状況をまとめたレポート公開

サポート詐欺は偽の警告画面でユーザーをだまし、サポート料金と称した金銭をだまし取る手口です。IPAの情報セキュリティ安心相談窓口に寄せられた、偽セキュリティ警告（サポート詐欺）の相談内容や、独自の調査・検証などにより把握した内容をまとめたレポートを公開しました。サポート詐欺の相談件数は2022年ごろから増加し続けており、手口も変化しています。広告枠やブラウザ通知機能を利用した典型例、偽オペレータとのやりとり事例、対処としての画面の閉じ方などを、実際の画面の例を掲載し解説しています。

最近は右記事例に限らず、さまざまな企業を詐称する偽の警告画面が出現していますのでいっそうの注意をお願いします。

https://www.ipa.go.jp/security/anshin/measures/supportscam_report.html

● サポート詐欺の画面例

※詐欺画面の例であり、マイクロソフト社が配信しているものではありません

デジタル時代のスキル変革等に関する調査（2023年度）

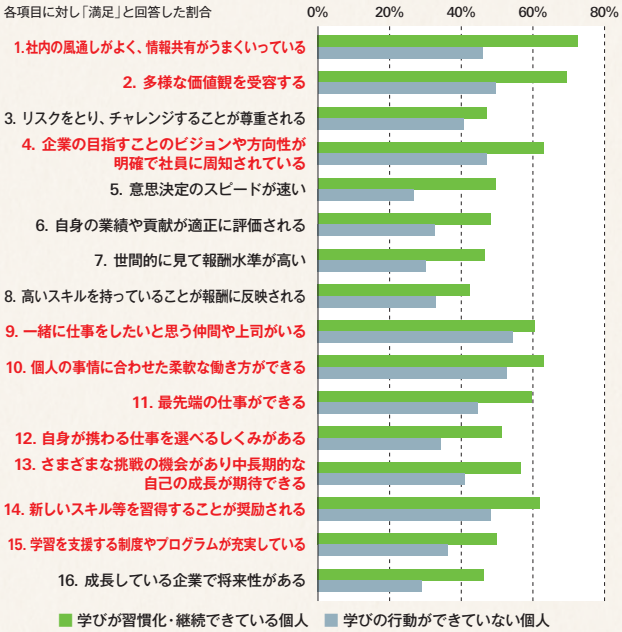
デジタル化の進展に伴い、DXを推進する人材の獲得・育成が急務となっています。本調査でも人材育成では社員の「スキル向上・獲得へのマインドシフト」が48.3％で最多の課題となり、企業は個人が自律的に学ぶことを求めているのがわかります。

右図の通り、会社員個人としてみると、自律的な学びが習慣化・継続している人（全体の約33%）はそうでない人に比してエンゲージメントが高い傾向にあります。特に、赤文字の項目は、学びが習慣化・継続できている人の50％以上が「満足」と回答しています。

企業と個人の相互的な発展につながる“自律的な、学び”――これを促進する10個の施策と4つの要素（ドライバー）を具体的事例から抽出し記載しています。これらの考察が自律的な学びによる人材育成に貢献することを希望しています。

https://www.ipa.go.jp/pressrelease/2024/press20240722.html

● 「自律的な学び」とエンゲージメント（個人調査）



ワンスオンリー入門ガイド　申請・証明手続の抜本改善

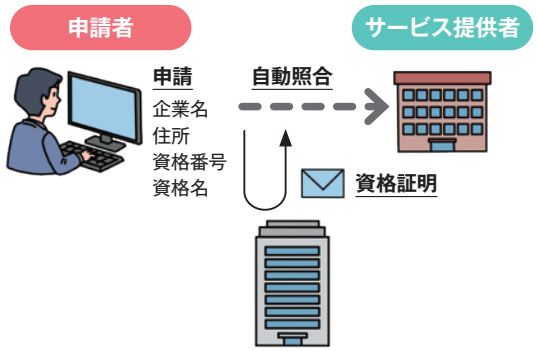
ワンスオンリーとは、申請や届出を一度行えば、初回登録データが再利用され次回以降の手続きが円滑に進むサービスです。ネットショッピングではよくあるものの日本の行政手続きではまだ実際の適用例は少ないのが現実です。

一方、EU域内では、それぞれの国内や、国境を越えた行政手続き（転居時の車両登録、教育申請等）でもワンスオンリーシステムをすでに実現しています。

本ガイドでは、先進事例としてEUのOnce-Only Technical System（OOTS）の概要をご紹介するとともに、申請手続きのシステム設計者・運用者の方々向けに設計方針を入門編としてご説明しています。ぜひ手にとってみてください。

https://www.ipa.go.jp/digital/data/data-spaces-academy.html#once-only_beginners-guide

● **ワンスオンリーサービスのイメージ**
（資格証明が必要な申請の例）



・申請時、証明書添付の手間やコストが減る
・審査が自動化され短時間になる
・証明書の偽造が防げる

Just Information

脆弱性体験学習ツール「AppGoat」で学ぼう！

脆弱性の概要や対策方法など、脆弱性に関する基礎的な知識を実習形式で体系的に学べるツールAppGoat。ウェブアプリケーションの脆弱性対策に必要なスキルを習得したい開発者やウェブサイトの管理者におすすめです。攻撃者の視点、開発者の視点の双方から脆弱性を学べます。個人学習用教材としてはもちろん集合学習（最大40人）においても使えます。

今回、AppGoatを利用してみたい方々に向けたナビゲーション用動画を作成しました。AppGoatの概要から始まり、利用申請から学習の進め方までを説明しています。本動画を参考に、AppGoatを試してみませんか？

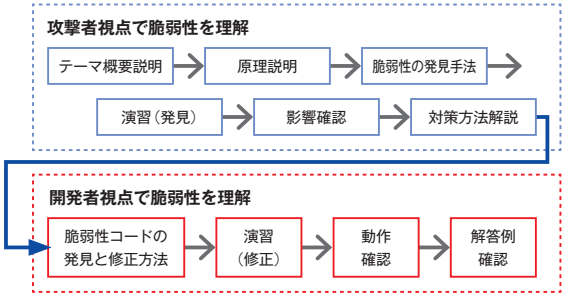
「AppGoat」で学べる12種類のテーマ

学べる脆弱性	
クロスサイト・スプリクティング	認証制御や認可制御の欠落
SQLインジェクション	HTTPヘッダ・インジェクション
クロスサイト・リクエスト・フォージェリ	バッファオーバーフロー
ディレクトリ・トラバーサル	クリックジャッキング
OSコマンド・インジェクション	メールヘッダ・インジェクション
セッション管理の不備	その他の脆弱性 （システム情報漏えいなど）

https://www.ipa.go.jp/security/videos/list.html#zeitai_new

学習の流れ

左記の全12種類の脆弱性につき、各脆弱性内の学習テーマごとに、前半は攻撃者の視点で脆弱性を攻撃する演習から始め、後半は開発者の視点で実際にソースコードを修正し脆弱性対策を学びます。



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6年度・問1】

マーケティングオートメーション（MA）に関する記述として，最も適切なものはどれか。

ア　企業内に蓄積された大量のデータを分析して，事業戦略などに有効活用する。

イ　小売業やサービス業において，販売した商品単位の情報の収集・蓄積及び分析を行う。

ウ　これまで人間が手作業で行っていた定型業務を，AIや機械学習などを取り入れたソフトウェアのロボットが代行することによって自動化や効率化を図る。

エ　見込み顧客の抽出，獲得，育成などの営業活動を効率化する。

問2　マネジメント系【令和6年度・問50】

ソフトウェア製品の品質特性を，移植性，機能適合性，互換性，使用性，信頼性，性能効率性，セキュリティ，保守性に分類したとき，RPAソフトウェアの使用性に関する記述として，最も適切なものはどれか。

ア　RPAが稼働するPCのOSが変わっても動作する。

イ　RPAで指定した時間及び条件に基づき，適切に自動処理が実行される。

ウ　RPAで操作対象となるアプリケーションソフトウェアがバージョンアップされても，簡単な設定変更で対応できる。

エ　RPAを利用したことがない人でも，簡単な教育だけで利用可能になる。

問3　テクノロジ系【令和6年度・問82】

ISMSクラウドセキュリティ認証に関する記述として，適切なものはどれか。

ア　一度認証するだけで，複数のクラウドサービスやシステムなどを利用できるようにする認証の仕組み

イ　クラウドサービスについて，クラウドサービス固有の管理策が実施されていることを認証する制度

ウ　個人情報について適切な保護措置を講ずる体制を整備しているクラウド事業者などを評価して，事業活動に関してプライバシーマークの使用を認める制度

エ　利用者がクラウドサービスへログインするときの環境，IPアドレスなどに基づいて状況を分析し，リスクが高いと判断された場合に追加の認証を行う仕組み

正解：問1 エ　問2 エ　問3 イ

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」最新号の公開をお知らせするメール配信サービスをご提供しています。お申込み、配信先の変更・配信停止につきましてはウェブページをご覧ください。

IPAニュース　検索

https://www.ipa.go.jp/about/ipanews/index.html

● 「IPA NEWS」アンケートはこちら

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.69
発行日　令和6年11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/