IPA 情報発信第 156 号（2017 年 4 月）

2017 年 5 月 1 日
独立行政法人情報処理推進機構（IPA）
理事長 富田　達夫

＜IPA 情報発信第 156 号の内容＞

今月のトピックス

１．「産業サイバーセキュリティセンター発足記念シンポジウムおよび式典」を開催

4 月発足の産業サイバーセキュリティセンターの紹介や企業内の体制整備などについての重要性を啓発するためのシンポジウムを開催しました。中西センター長から設立趣旨を説明し、受講生を派遣予定の自動車・鉄道・電気・ガス・放送等企業の経営層のご参列に加えて、世耕大臣、丸川大臣、藤井政務官、勝野電事連会長からご挨拶を頂きました。

２．4,172 名の「情報処理安全確保支援士（登録セキスペ）」が誕生

国家資格「情報処理安全確保支援士（登録セキスペ）」4,172 名の登録を行いました。また、登録番号、氏名、勤務先などを含む登録者公開情報を公表しました。

３．「セキュリティ領域」「データサイエンス領域」に関するスキル標準を取りまとめ、“ITSS+”（プラス）として公開

第 4 次産業革命に向けた IT 人材の育成を推進するための新たなスキル標準を策定する一環として、「セキュリティ領域」「データサイエンス領域」に関するスキル標準を取りまとめ、“ITSS+（プラス）”として公開しました。

Ⅰ．安全な IT 社会の実現

Ⅱ．IT システムの安心・安全の確保と開発・利活用の効率化

１．SEC セミナー「コーディング技法で守るモビリティ社会のセキュリティ」を開催
２．2015 年度のソフトウェア工学分野の先導的研究支援事業の成果を公開
３．SEC セミナー開催案内（5 月）

Ⅲ．未来の IT 社会を担う人材の育成とビジネス支援・技術開発促進

１．「IT 人材白書 2017」を発行
２．平成 29 年度春期「情報処理安全確保支援士（登録セキスペ）試験」および「情報処理技術者試験」を実施

今月のトピックス

１.「産業サイバーセキュリティセンター発足記念シンポジウムおよび式典」を開催

（担当：産業サイバーセキュリティセンター）

IPA は、「産業サイバーセキュリティセンター発足記念シンポジウムおよび式典」を 4 月 24 日（月）に開催しました。

当シンポジウムでは、4 月 1 日に発足した産業サイバーセキュリティセンターの設立経緯や講義概要の紹介を行うとともに、重要な社会インフラに対するサイバーセキュリティ上の脅威を踏まえて、企業内におけるサイバーセキュリティ人材のキャリアパス構築や、社内体制整備についての重要性を啓発することを目的に講演やパネルディスカッションを実施しました。

当日は、中西センター長からセンターの設立趣旨を説明しました。また、世耕経済産業大臣から、人材に対する投資についての経営層への期待を込めたご挨拶を頂いたほか、丸川東京オリンピック競技大会・東京パラリンピック競技大会担当大臣（サイバーセキュリティ戦略本部　副本部長）及び藤井国土交通大臣政務官、受講生派遣企業の代表として勝野電気事業連合会会長（中部電力株式会社代表取締役社長）からもご挨拶を頂きました。また、総務省及び厚生労働省の審議官、受講生派遣を予定する化学、石油、鉄鋼、自動車、鉄道、電気、ガス、放送等の企業の経営層、当センターの第一期生となる受講生を含む約 300 名の参加者にご来場いただき、盛況のうちに終了しました。

IPA は、今後もサイバーセキュリティ人材確保に向けた制度・施策、グローバルな最新の脅威と対策を企業や国民に広く周知していきます。

２．4,172 名の「情報処理安全確保支援士（登録セキスペ）」が誕生

（担当：HRD イニシアティブセンター）

IPA は、4 月 1 日（土）付けで 4,172 名の「情報処理安全確保支援士（登録セキスペ）」の登録を行いました。

登録者には IPA 理事長名の登録証を交付するとともに、IPA ウェブサイトにて登録番号、氏名、勤務先などを含む登録者公開情報を公表しております。

登録者の平均年齢は 40.5 歳となり、地域別では関東地方が約 7 割を占め、また全ての都道府県に登録セキスペが誕生しました。

IPA は、登録セキスペが企業や組織における情報セキュリティ対策の推進力となり、サイバーセキュリティの確保のための取組みに貢献し、今後活躍の場を広げて行くことを期待します。

本件の詳細については、次の URL をご覧ください。

http://www.ipa.go.jp/about/press/20170403.html

３．「セキュリティ領域」「データサイエンス領域」に関するスキル標準を取りまとめ、“ITSS+”（プラス）として公開

（担当：HRD イニシアティブセンター）

IPA は、第 4 次産業革命に向けた IT 人材の育成を推進するための新たなスキル標準を策定する一環として、「セキュリティ領域」「データサイエンス領域」に関するスキル標準を取りまとめ、“ITSS+（プラス）”として 4 月 7 日（金）に公開しました。

ITSS+は、「セキュリティ領域」「データサイエンス領域」のそれぞれについて、具体的な専門分野や業務活動（タスク）、必要なスキルを体系化した指標であり、主に従来の IT スキル標準（ITSS）が対象としている情報サービスの提供やユーザ企業の情報システム部門に関わっている既存の人材が、スキル強化を図るための“学び直し”の指針として活用されることを想定しています。

IPA では、今後もデジタル変革で求められる人材のスキル類型について検討を続け、政府の第 4 次産業革命の推進に対応した新たなスキル標準の策定を行う予定です。

本件の詳細については、次の URL をご覧ください。

http://www.ipa.go.jp/about/press/20170407.html

Ⅰ．安全な IT 社会の実現

１．「企業の CISO[1]や CSIRT[2]に関する実態調査 2017」報告書を公開

（担当：セキュリティセンター）

IPA は、4 月 13 日（木）に「企業の CISO や CSIRT に関する実態調査 2017」報告書を公開しました。

本調査は昨年から実施しているもので、経営者の情報セキュリティに対する関与と、企業の組織的な対策状況についての現状を把握するため、文献調査・アンケート調査を行っています。アンケート調査では日・米・欧の従業員 300 人以上の企業を対象に実施し、その結果を比較しました。主なトピックは以下のとおりです。

(1) 現在、CISO に期待されている役割やスキルは、セキュリティを偏重している。セキュリティ部門と経営層をつなぐ橋渡しとしての役割は、まだ企

1 Chief Information Security Officer：最高情報セキュリティ責任者。

2 Computer Security Incident Response Team の略。サイバー攻撃による情報漏えいや障害など、コンピュータセキュリティにかかわるインシデントに対処するための組織。

業では認知されていない。
(2) 日本では、CISO が任命されている組織の割合は 6 割程度で、欧米と 20 ポイント以上の差がある。また、日本では多くの CISO が他の役職と兼任であり、専任 CISO の多い欧米とは異なる。
(3) 日本では、CISO の半数以上(58.7%)がセキュリティ要員（人数）は十分だと回答している。一方、現場では不足感が半数を超えている。
(4) 日本では、CSIRT を設置したものの、期待したレベルを満たしていると解釈していない。
(5) 日本では、経営層の情報セキュリティへの関与は、重要インフラ企業でも 6 割～7 割程度に留まる。

「企業の CISO や CSIRT に関する実態調査 2017」報告書の詳細については、次の URL をご覧ください。

https://www.ipa.go.jp/security/fy29/reports/ciso-csirt/index.html

２.「安心相談窓口に寄せられた相談の分析（2016 年）～被害の未然防止と拡大防止対策に向けての考察～」報告書を公開

（担当：セキュリティセンター）

IPA は、4 月 26 日（水）に「安心相談窓口に寄せられた相談の分析（2016 年）～被害の未然防止と拡大防止対策に向けての考察～」報告書を公開しました。

本レポートは、今後の被害予防と被害拡大防止に有効な対策の手がかりを探るため、当窓口に寄せられた相談情報をもとに、相談内容の動向、相談種別ごとの相談者の属性傾向、また、被害に巻き込まれた原因や相談内容などを類型化し、分析を行ったものです。分析結果としては以下のような点が明らかとなっています。

・相談件数が最も多かった「ワンクリック請求」事案では、請求画面を表示させる手口の変化と被害状況の推移に一定の相関関係が見られた。また、相談者の年齢・性別に顕著な偏りが見られた。
・次いで相談件数が多かった「偽警告」事案では、悪意のある者によりパソコンが遠隔操作される前か後かによる、相談者の不安の変化の状況が分かった。
・未成年者に限定して分析してみたところ、相談件数こそ少ないものの、相談内容の部分ではスマートフォン向けの様々なアプリやサービスに分散していることが分かり、この世代特有の傾向をうかがい知ることができた。

また、これらの分析結果に基づき、現時点で見えてきた課題と、それらを解決するために有効と思われる対策案についても解説しています。

「安心相談窓口に寄せられた相談の分析（2016 年）～被害の未然防止と拡大防止対策に向けての考察～」の詳細は、次の URL をご覧ください。

https://www.ipa.go.jp/security/anshin/info/2016soudan-analysis-report.html

３．注意喚起　偽口座への送金を促す“ビジネスメール詐欺”の手口

（担当：セキュリティセンター）

IPA は、“ビジネスメール詐欺”に関する注意喚起を行うとともに、レポート「ビジネスメール詐欺『BEC[3]』に関する事例と注意喚起」を 4 月 3 日(月)に公開しました。

“ビジネスメール詐欺”は巧妙に細工したメールのやりとりにより、企業の担当者を騙し、攻撃者の用意した口座へ送金させる詐欺の手口です。金銭被害が多額になる傾向があり、手口の悪質さ・巧妙さは、諜報活動等を目的とする“標的型サイバー攻撃”とも通じるところがあります。2 月には国内でも逮捕者が出たとの報道がありました。被害を防止するためには、特に企業の経理部門等が、このような手口の存在を知ることが重要です。

このレポートでは、“ビジネスメール詐欺”の 5 つのタイプを説明し、4 件の実事例の概要を紹介するとともに、それら事例で使われた攻撃手口を解説し、対策を述べています。また、レポートの添付資料では、4 件の事例で使われた攻撃の手口について、更に詳しく紹介しています。ビジネスメール詐欺の対策のための参考としてください。

「偽口座への送金を促す“ビジネスメール詐欺”の手口」の詳細については、次の URL をご覧ください。

https://www.ipa.go.jp/about/press/20170403_2.html

４．日本国内で接続されている IoT 機器数および「SHODAN[4]」および「Censys[5]」を使った機器の検索方法の公開

（担当：セキュリティセンター）

IPA は、「SHODAN」および「Censys」を用いて、インターネットに接続されて

---

3 BEC：Business E-mail Compromise

4 2009 年に John Matherly 氏によって開発された検索エンジン。インターネットに接続されている機器の情報を検索できる。

5 2015 年にミシガン大学の研究者によって開発された検索エンジン。インターネットに接続されたサーバー、ルーター、IP 電話等の機器を検索でき、無償で利用可能。

いる機器を検索し、日本国内で接続されている IoT 機器数を 4 月 17 日（月）に公開しました。
機器が有するサーバ機能ごとの検索結果と、その過程で用いた検索式も公開しております。

「日本国内で接続されている IoT 機器数」については、次の URL をご覧ください。

http://www.ipa.go.jp/security/iot/20170417.html

５．情報セキュリティ啓発映像「偽警告」「標的型サイバー攻撃の組織的な対策」「中小企業向け情報セキュリティ対策」の３本を公開

（担当：セキュリティセンター）

IPA は、YouTube 内の「IPA Channel[6]」に標的型攻撃対策をテーマとした 3 本の新作映像を 4 月 3 日（月）に追加しました。

- 「その警告メッセージ、信じて大丈夫？ ブラウザの“ 偽警告”にご用心！」
- 「見えざるサイバー攻撃 -標的型サイバー攻撃の組織的な対策-」
- 「あなたの会社のセキュリティドクター -中小企業向け情報セキュリティ対策の基本-」

情報セキュリティ啓発映像「偽警告」「標的型サイバー攻撃の組織的な対策」「中小企業向け情報セキュリティ対策」の詳細については、次の URL をご覧ください。

http://www.ipa.go.jp/security/keihatsu/videos/index.html

６．安心相談窓口だより「被害低減のための偽警告の手口と対策を紹介する映像コンテンツを公開」

（担当：セキュリティセンター）

IPA は、被害低減のための偽警告の手口と対策を紹介する映像コンテンツを公開しました。
2016 年度に IPA に寄せられた偽警告に関する相談件数は 2,624 件でした。339 件だった 2015 年度に比べ、相談件数は 7.7 倍に増加しています。
偽警告の画面で表示される内容は、電話をかけさせるための何の根拠もない「単なる騙し」に過ぎません。警告の内容は鵜呑みにせず、画面を閉じるだけで問題ありません。しかし、その手口は狡猾、かつ巧妙です。偽警告の被害低

6 情報セキュリティに関する脅威や対策などを学ぶための映像コンテンツを配信する IPA の公式チャンネル。

減の特効薬は、警告の内容が単なる騙しであることを知り、決して電話をかけないことです。

「被害低減のための偽警告の手口と対策を紹介する映像コンテンツ」の詳細については、次の URL をご覧ください。

https://www.ipa.go.jp/security/anshin/mgdayori20170411.html

7．安心相談窓口だより「Windows サーバーを狙ったランサムウェア感染被害が発生」

（担当：セキュリティセンター）

IPA は、Windows サーバーを狙ったランサムウェア感染被害の発生を確認し、4 月 27 日（木）に公表しました。

2017 年 1 月から「Windows サーバー内のファイルが暗号化された」というランサムウェア感染被害と考えられる相談や届出が寄せられています。寄せられた情報から、原因には、パスワード設定の不備があり、その結果 Windows サーバーに不正ログインされてしまい、ランサムウェアに感染させられてしまったと考えられます。

また、寄せられた相談、届出では被害に遭ったサーバーすべてが Windows OS でしたが、原因は不正アクセスであり、Windows サーバーという特定の OS だけが被害に遭うものではありません。よって、業務の都合等で外部からのリモートアクセスを許可するサーバーを運用している場合は、“適切なパスワード管理を徹底する”“サーバーへのアクセス制限を設定する”ことを改めて確認し、対策をしてください。

「Windows サーバーを狙ったランサムウェア感染被害が発生」の詳細については、次の URL をご覧ください。

https://www.ipa.go.jp/security/anshin/mgdayori20170427.html

8．コンピュータウイルス・不正アクセスの届出状況及び相談受付状況 [2017 年第 1 四半期（1 月～3 月）]

（担当：セキュリティセンター）

IPA は、2017 年第 1 四半期（1 月～3 月）のコンピュータウイルス・不正アクセスの届け出及び相談の状況をまとめ、4 月 24 日（月）に公開しました。公開内容の概要は、以下のとおりです。

（1） コンピュータウイルス届出状況

今期のウイルス届出件数は 480 件でした。

不正プログラム検出数は 124,230 個、ウイルス検出数は 9,317 個でした。

(2) コンピュータ不正アクセス届出状況

今期の届出件数は 26 件で、そのうち被害があったのは 21 件でした。

(3) 情報セキュリティ安心相談窓口の相談状況

今期のウイルス・不正アクセス関連の相談件数は 3,553 件でした。

コンピュータウイルス・不正アクセスの届出状況及び相談受付状況の詳細については、次の URL をご覧ください。

https://www.ipa.go.jp/security/txt/2017/q1outline.html

９．脆弱性対策情報データベース JVN iPedia の登録状況 [2017 年第１四半期（1 月～3 月）]

（担当：セキュリティセンター）

IPA は、2017 年第１四半期（1 月～3 月）の脆弱性対策情報データベース「JVN iPedia」（ジェイブイエヌ　アイ・ペディア）の登録状況を「脆弱性対策情報データベース JVN iPedia に関する活動報告レポート」としてまとめ、4 月 25 日（火）に公開しました。

今期に、脆弱性対策情報データベース「JVN iPedia」日本語版に登録された脆弱性対策情報は 267 件で、2007 年 4 月 25 日の公開開始からの登録件数は累計 7,160 件となりました。

脆弱性対策情報データベース JVN iPedia の登録状況の詳細については、次の URL をご覧ください。

https://www.ipa.go.jp/security/vuln/report/JVNiPedia2017q1.html

１０．ソフトウェア等の脆弱性関連情報に関する届出状況 [2017 年第１四半期（1 月～3 月）]

（担当：セキュリティセンター）

IPA は、2017 年第１四半期（1 月～3 月）の脆弱性関連情報の届出状況を「ソフトウェア等の脆弱性関連情報の取り扱いに関する活動報告レポート」としてまとめ、4 月 26 日（水）に公開しました。

今期の脆弱性情報の届出件数は 145 件でした。内訳は、ソフトウェア製品に関するものが 88 件で累計 3,520 件、ウェブサイトに関するものが 57 件で累計 9,541 件でした。これにより、2004 年 7 月の届出受付開始からの累計は 13,061 件となりました。

ソフトウェア等の脆弱性関連情報に関する届出状況の詳細については、次のURL をご覧ください。

https://www.ipa.go.jp/security/vuln/report/vuln2017q1.html

１１．サイバー情報共有イニシアティブ（J-CSIP）運用状況 [2017 年 1 月～3 月]

（担当：セキュリティセンター）

IPA は、2017 年第 1 四半期（1 月～3 月）の「サイバー情報共有イニシアティブ」（J-CSIP）の活動内容をまとめ、4 月 27 日（木）に公表しました。

4 月 26 日、新たに「クレジット業界 SIG[7]」が発足し、J-CSIP は、8 業界 115 組織の体制となりました。

今期の情報提供件数は 73 件であり、うち標的型攻撃メールとみなした情報は 0 件でした。また、IPA による分析を経て、IPA が独自に入手した情報も含む 9 件の情報共有を傘下組織へ行いました。

本レポートでは、四半期の運用状況に加え、2016 年度全体を含む、過去 5 年分の情報提供および情報共有等の実施件数を掲載しています。

J-CSIP の運用状況の詳細については、次の URL をご覧ください。

https://www.ipa.go.jp/security/J-CSIP/index.html

１２．重要なセキュリティ情報（４月）

（担当：セキュリティセンター）

IPA では、インターネットを使っている多くの利用者が影響を受けるセキュリティ対策情報を対象に「重要なセキュリティ情報[8]」として公開しています。

「重要なセキュリティ情報」とは、放っておくと不正アクセスやデータが盗まれるなどの危険性が高いセキュリティ上の問題と対策についてお伝えするもので、IPA 情報発信では 2013 年 12 月から広く啓発するため記載しています。発信情報から、ご自身の PC やシステムへの影響を判断の上、速やかな対策を心がけてください。

4 月は、「緊急」1 件、「注意」4 件を公開しました。

---

7 SIG：Special Interest Group の略。J-CSIP では、情報共有を目的に業界を軸にした組織をグループ化しており、SIG と呼んでいる。

8 「重要なセキュリティ情報」は、次の基準で対策の緊急度を表しています。
「緊急」･･･影響度の高いセキュリティ上の問題があると公表された情報でかつ、当該問題を悪用した攻撃が実際に行われているケース。
「注意」･･･影響度の高いセキュリティ上の問題があると公表された情報又は、当該問題を悪用した攻撃が行われる可能性があるケース。

重要なセキュリティ情報の詳細については、次の URL をご覧ください。

https://www.ipa.go.jp/security/announce/alert.html

Ⅱ．IT システムの安心・安全の確保と開発・利活用の効率化

１．SEC セミナー「コーディング技法で守るモビリティ社会のセキュリティ」を開催

（担当：ソフトウェア高信頼化センター）

IPA は、4 月 24 日（月）に SEC セミナー「コーディング技法で守るモビリティ社会のセキュリティ」を開催しました。

本セミナーでは、「MISRA[9] C/C++[10]」を活用したセキュリティへの取組みや、欧州のコーディング技法の状況、セキュリティ対応について英国 LDRA 社[11]から紹介するとともに、IPA から「組込みソフトウェア向けコーディング作法ガイド（ESCR）[12]」の最新状況を紹介しました。

参加者からは「コーディングスタンダードは育成に使えそうだ」といったご意見を頂きました。

IPA では、これらのご意見を基に、今後もコーディング技法の普及活動を通して IT システムの信頼性向上の取組みを継続していきます。

「コーディング技法で守るモビリティ社会のセキュリティ」の詳細については、次の URL をご覧ください。

http://sec.ipa.go.jp/seminar/20170424.html

２．2015 年度のソフトウェア工学分野の先導的研究支援事業の成果を公開

（担当：ソフトウェア高信頼化センター）

IPA は、4 月 20 日（木）に 2015 年度のソフトウェア工学分野の先導的研究支援事業（RISE）の研究成果を公開しました。

---

9 MISRA(The Motor Industry Software Reliability Association)：自動車メーカ、部品メーカ、研究者からなる欧州の自動車業界団体。

10 MISRA C/C++言語による安全で信頼性のあるソフトウェアを開発するためのコーディングガイドライン。自動車業界を中心に広範に運用されている標準技法。

11 LDRA 社は、30 年以上にわたって、安全な生活に関わるソフトウェアアプリケーションの自動解析・検証ツールを提供。航空宇宙、原子力、自動車分野等の企業が、セーフティクリティカルな国際標準に準拠するためのテストツールとして利用。

12 組込みソフトウェア開発において、読みやすくエラーが発生しにくいソースコードを書くために、コーディングする際の注意事項やノウハウをまとめたルール集。

C++言語版：http://www.ipa.go.jp/sec/reports/20161018.html

C 言語版：http://www.ipa.go.jp/sec/reports/20140307.html

本事業は、大学等の学術分野におけるソフトウェアに関する研究成果を産業界に普及・展開することを目的に、ソフトウェア工学分野の先導的研究やソフトウェアの経済的効果に関する研究を公募し、支援する取組みです。

IPA では 2012 年度より本事業を開始し、2015 年度は 6 つの研究テーマを採択しこれを支援してきました。このうち研究が終了した 2 件の成果報告書を以下のとおり公開しました。

組織名	研究期間	研究テーマ名
国立大学法人電気通信大学	2 年間	D-Case に基づく議論構造可視化支援ツールの開発と、スマートコミュニティにおける合意形成の実証
学校法人早稲田大学　早稲田大学	2 年間	測定評価と分析を通じたソフトウェア製品品質の実態定量化および総合的品質評価枠組みの確立

「2015 年度のソフトウェア工学分野の先導的研究支援事業の成果」の詳細については、次の URL をご覧ください。

http://www.ipa.go.jp/sec/reports/20170420.html

３．SEC セミナー開催案内（5 月）

（担当：ソフトウェア高信頼化センター）

IPA は、事業成果を広く普及・啓発することを目的としたセミナー、ソフトウェア・エンジニアリングに関する国内外の最新動向などを紹介する特別セミナーをそれぞれ実施しています。

5 月は、次の日程で開催を予定しています。

・デジタル時代に向けた大分イノベーション
～OITA4.0 の実現に向けて～（5 月 19 日）

http://sec.ipa.go.jp/seminar/20170519.html

・激動の IoT 時代を見据えた組込みシステム価値向上とは？
～2016 年度 製品・制御システム高信頼化部会成果報告～　@JAIST 品川（5 月 29 日）

http://sec.ipa.go.jp/seminar/20170529.html

・つながる世界に求められる利用時の品質
～安全安心を実現するためにソフトウェア設計者が考慮すべきこと～（5 月 31 日）

http://sec.ipa.go.jp/seminar/20170531.html

Ⅲ. 未来の IT 社会を担う人材の育成とビジネス支援・技術開発促進

1.「IT 人材白書 2017」を発行

（担当：IT 人材育成企画部）

IPA は、『IT 人材白書 2017 デジタル大変革時代、本番へ　～IT エンジニアが主体的に挑戦できる場を作れ～』を 4 月 24 日（月）に公開しました。

本書は、IT 人材育成事業の一環として最新の IT 人材の動向や実態を網羅的に調査し、まとめたもので、IT 人材の育成を考えるすべての経営者、実務・政策担当者、人事担当者を読者層として想定しています。

今回の調査では、デジタル変革の中心となる「IT 企業」や「ユーザー企業の IT 部門」、及びデジタルビジネスを実施する「ネットサービス実施企業」に対して、デジタル変革[13]への認識や対応状況等を調査しました。また、先駆的なサービスを展開している米国の情報処理・通信に携わる人材との比較や育成状況について調査を行いました。

主なポイントは次の通りです。

- デジタル変革に対する認識や対応状況
- 変革を主導すべき者とその役割
- 新事業を担うリーダー的人材の特徴や育成環境
- 日本と米国の情報処理・通信に携わる人材の動向比較
- 国内企業における IT 人材の「量」に対する過不足感の変化

なお、「IT 人材白書 2017」は、Amazon、全国官報販売協同組合販売所から購入できます。

発行：独立行政法人情報処理推進機構（IPA）
ISBN：978-4-905318-50-7
定価：本体 1,389 円（税別）
A4 変形版/299 頁

「IT 人材白書 2017」の詳細については、次の URL をご覧ください。

http://www.ipa.go.jp/jinzai/jigyou/about.html

[13]ここでは、IoT やビッグデータ、AI など技術の進展等によって、社会や産業、企業、人のあり方や働き方が大きく変化することを指している。

２．平成 29 年度春期「情報処理安全確保支援士（登録セキスペ）試験」および「情報処理技術者試験」を実施

（担当：情報処理技術者試験センター）

IPA は、平成 29 年度春期「情報処理安全確保支援士（登録セキスペ）試験」および「情報処理技術者試験」（所管：経済産業省）を 4 月 16 日（日）に実施しました。

合格発表は、「情報セキュリティマネジメント試験」および「基本情報技術者試験」が 5 月 17 日（水）正午、その他の試験が 6 月 21 日（水）正午の予定です。

平成 29 年度春期「情報処理安全確保支援士（登録セキスペ）試験」および「情報処理技術者試験」の合格発表スケジュールについては、次の URL をご覧ください。

http://www.jitec.ipa.go.jp/1_00topic/topic_20170416_schedule.html

同試験の「問題冊子・解答例」については、次の URL をご覧ください。

http://www.jitec.ipa.go.jp/1_04hanni_sukiru/mondai_kaitou_2017h29.html

●IPA 組織図

本書に関するお問合せ先
戦略企画部 企画・調査Ｇ　笛木・野村
〒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
TEL：03-5978-7503
E-mail：spd-plan@ipa.go.jp