

IPA 情報発信第 164 号 (2017 年 12 月)

2017 年 12 月 28 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 164 号の内容>

今月のトピックス

1. 「文字情報基盤整備事業」で推進していた漢字 6 万文字の国際規格化が完了

文字情報基盤事業として推進してきた漢字 6 万文字の国際規格化が完了しました。行政機関や会社ごとで作成していた外字を同規格に定めるコードに置き換えることで、共通の文字を相互に利用できます。それにより、大幅なコストダウンになり、また、ビッグデータの解析等も容易になります。

2. 「情報セキュリティに対する意識調査」等で、悪意ある SNS 投稿者の心理が判明

「2017 年度情報セキュリティに対する意識調査」等を実施した結果、SNS の利用に対する倫理観について、セキュリティの脅威に関する質問から、悪意ある投稿経験者の心理で最も多いのは「気が済んだ、すっとした」であるなどの調査結果が明らかになりました。

3. イスラエル人講師による産業サイバーセキュリティに関する講義を実施

世耕経済産業大臣が本年 5 月にイスラエルと合意した「日イスラエル・イノベーション・パートナーシップ」等に基づき、イスラエル電力公社 CEO 等が産業サイバーセキュリティセンターの受講生に対して講義および演習を行いました。

4. 西銘恒三郎経済産業副大臣が IPA に来訪

西銘恒三郎経済産業副大臣が IPA に来訪され、産業サイバーセキュリティセンターの講義風景、情報セキュリティ対策、人材育成の取組等を視察されました。

I. 安全な IT 社会の実現

1. 「ネットワークカメラシステムにおける情報セキュリティ対策要件チェックリスト」を公開
2. 「制御システムのセキュリティリスク分析ガイドの早分かり 活用の手引き」を公開
3. 第 13 回 IPA「ひろげよう情報モラル・セキュリティコンクール」2017 の受賞作品、受賞校を決定
4. 年末年始における情報セキュリティ対策」の公開
5. 重要なセキュリティ情報 (12 月)
6. 「セキュリティ・ミニキャンプ in 北陸 2017 (金沢)」を開催
7. 「セキュリティ・ミニキャンプ in 沖縄 2017」を開催

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. 「『つながる世界の開発指針』の実践に向けた手引き[IoT 高信頼化機能編]」の英語版を公開
2. 「安全性解析手法 STAMP/STPA セミナー@大阪」を開催
3. 「SEC journal」第 51 号を発行
4. SEC セミナー開催報告（12 月）と SEC セミナー開催案内（1 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. 平成 29 年度秋期「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」（応用情報技術者試験、高度試験）の合格者を発表

今月のトピックス

1. 「文字情報基盤整備事業」で推進していた漢字 6 万文字の国際規格化が完了

(担当：国際標準推進センター)

12月22日(金)に、ISO(国際標準化機構)から文字コード国際規格のISO/IEC 10646(Universal Coded Character Set)第5版が発行され、IPAが文字情報基盤事業として推進してきた漢字6万文字の国際規格化が完了しました。

これまでは、ある行政機関や会社が人名漢字をコンピュータで正確に表記しようとする場合、外字作成の必要があり、それぞれで文字コードを登録していました。外字のコードには一貫性が無いため、行政機関や会社のシステムを越えた電子文書の共有は困難でした。

そこで、IPAでは、内閣官房IT総合戦略室、経済産業省と共に、文字情報基盤整備事業を2010年9月から推進してきました。この事業は、行政の実務で使用されている人名や地名等約6万文字の漢字について、コンピュータで用いる文字フォントや文字コードを統一し、国際規格化等するものです。

今後は、同規格を参照することで、官民双方で外字作成やデータ変換に係るコストが削減され、コンピュータ上における漢字の利便性が大きく向上し、ひいてはビッグデータの解析等、今まで利活用が困難とされていた分野において、漢字の利活用がより進むことが期待されます。

「文字情報基盤整備事業」で推進していた漢字6万文字の国際規格化についての詳細については、次のURLをご覧ください。

<https://www.ipa.go.jp/about/press/20171225.html>

2. 「情報セキュリティに対する意識調査」等で、悪意ある投稿者の心理が判明

(担当：セキュリティセンター)

IPAは、情報セキュリティに関する対策情報の発信、普及啓発等の活動に役立てることを目的として、「2017年度 情報セキュリティの脅威に対する意識調査」および「2017年度 情報セキュリティの倫理に対する意識調査」を実施し、その報告書を12月14日(木)に公開しました。

本調査は2005年から毎年、パソコンおよびスマートデバイス利用者を対象に、情報セキュリティ対策の実施状況、情報発信に際しての意識、および法令遵守に関する意識についてアンケートを実施・集計しているもので、今回で16回目となります。

今回の調査結果の主なポイントは以下のとおりです。

- ・悪意ある投稿経験者の投稿後の心理で、最も多いのは、「気が済んだ、すっ

とした」で 35.6%、前年比 4.3%増。特に 10代は 45.5%、20代は 40.5%と他世代より高い傾向。

- ・恋人等、相手が非常に近い間柄であれば、「自身の性的な姿を撮影した写真や動画」を SNS で共有しても構わないと考えるスマートデバイス利用者は 7.4%、パソコン利用者が 5.3%。
- ・一方、「SNS で自身の性的な写真や動画を撮影して投稿した」ことを問題があると認識している回答割合は 1 割程度増加。

「2017 年度 情報セキュリティに対する意識調査」報告書等の詳細については、次の URL をご覧ください。

<https://www.ipa.go.jp/security/fy29/reports/ishiki/index.html>

3. イスラエル人講師による産業サイバーセキュリティに関する講義を実施

(担当：産業サイバーセキュリティセンター)

IPA では、11 月 28 日（火）に、イスラエルから来日した 5 名の講師が産業サイバーセキュリティセンターの中核人材育成プログラム受講者に対し集中的に講義および演習を行う国際スピーカーデーを実施しました。

これは、世耕経済産業大臣が本年 5 月にイスラエルを訪問した際に合意した「日イスラエル・イノベーション・パートナーシップ」において産業分野のサイバーセキュリティ強化に向けた協力を促進するとしたこと、および同訪問時に両国の経済産業省の間で署名された「サイバーセキュリティ協力覚書

(MOC)」に基づき、イスラエルの Eli Cohen 経済産業大臣およびサイバーセキュリティ関係者が多数来日し多くのイベントが行われる中で実現したものです。

当日は、イスラエル国家サイバー局の新サイバー技術ユニット代表責任者である Yigal Unna 氏によるイスラエルにおける重要インフラ向けサイバーセキュリティ戦略に関する講義のほか、イスラエルの官民有識者による世界の最新動向を踏まえた講義、さらには、イスラエル電力公社の CEO がモデレーターを務める机上演習も行われ、受講生 8 名が仮想企業の CEO や CISO の役割を与えられ、サイバークライシスマネジメントを体験しました。

4. 西銘恒三郎経済産業副大臣が IPA に来訪

(担当：戦略企画部)

西銘恒三郎経済産業副大臣が 12 月 12 日（火）に、IPA の視察に来訪されました。

我が国のセキュリティ中核人材を育成する産業サイバーセキュリティセンターにて講義風景や演習設備等をご見学いただくとともに、標的型サイバー攻撃に対処するための取り組みである「サイバー情報共有イニシアティブ (J-CISI

P)、「サイバーレスキュー隊 (J-CRAT)」をはじめ、「セキュリティ・キャンプ」、「未踏」、「情報処理安全確保支援士」等についての説明を行いました。

<https://www.ipa.go.jp/about/news/20171227.html>

I. 安全な IT 社会の実現

1. 「ネットワークカメラシステムにおける情報セキュリティ対策要件チェックリスト」を公開

(担当：セキュリティセンター)

IPA は、12 月 7 日 (木) に政府機関や自治体をはじめネットワークカメラシステムの調達者が活用できる「ネットワークカメラシステムにおける情報セキュリティ対策要件チェックリスト」を公開しました。

近年、公共の場に設置されたネットワークカメラの映像が不特定多数に閲覧できる状態にあったことが指摘されており、国の機関等がネットワークカメラシステムを調達する際には、その運用において想定される脅威への対策を講ずることが「政府機関の情報セキュリティ対策のための統一基準¹」で求められています。

そこで、IPA ではより安全な国民サービスを提供するための政府調達推進の一環として、ネットワークカメラシステムの機能と運用におけるセキュリティ上の対策を確認できるチェックリストを作成しました。

本チェックリストの特徴は、実現が難しいセキュリティの要件を推奨するものではなく、調達者にとって解りやすく、かつ、市場調達の観点からも現実的な要件のみを記載していることです。

本チェックリストの詳細については、次の URL をご覧ください。

<https://www.ipa.go.jp/about/press/20171207.html>

2. 「制御システムのセキュリティリスク分析ガイドの早分かり 活用の手引き」を公開

(担当：セキュリティセンター)

IPA は、12 月 19 日 (火) に「制御システムのセキュリティリスク分析ガイドの早分かり 活用の手引き」を公開しました。

本手引きは、10 月に公開した「制御システムのセキュリティリスク分析ガイド²」が本文・別冊合計で 420 ページと分量が多いため、どこにどのような記

¹ 2016 年 8 月 31 日サイバーセキュリティ戦略本部決定。

² IPA が 2008 年から実施してきた制御システムにおけるセキュリティ対策等に関する調査、および 2014 年以降に

載・内容があるか分かりやすくなるよう簡潔に示しています。同ガイドの目次に沿ってリスク分析の作業手順を解説し、該当ページも記載しているため、効率的に同ガイドを参照することができます。また、セキュリティ対策を推進する担当者にとって、経営層に対する説明資料としても活用でき、自組織のセキュリティ対策推進に役立ちます。

本手引きにより、制御システムのセキュリティリスク分析ガイドの活用が広がり、制御システムおよび重要インフラの事業者において適切なセキュリティ対策の策定が進展することを期待しています。

「制御システムのセキュリティリスク分析ガイドの早分かり 活用の手引き」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/20171219.html>

3. 第13回 IPA「ひろげよう情報モラル・セキュリティコンクール」2017の受賞作品、受賞校を決定

(担当：セキュリティセンター)

IPAは、第13回 IPA「ひろげよう情報モラル・セキュリティコンクール」2017の各受賞作品を12月25日(月)に決定し、公開しました。

今年度は、児童・生徒が制作した標語55,744作品、ポスター5,493作品、4コマ漫画6,720作品、書写(硬筆)2,292作品の中から、最優秀賞3作品、優秀賞9作品、書写賞6作品、文部科学大臣賞1作品を決定したほか、本コンクールの協力組織、団体の選出による各賞も併せて決定しました。

第13回 IPA「ひろげよう情報モラル・セキュリティコンクール」2017の受賞作品、受賞校の詳細については、次の URL をご覧ください。

<https://www.ipa.go.jp/security/event/hyogo/>

4. 「年末年始における情報セキュリティ対策」の公開

(担当：セキュリティセンター)

IPAは、12月21日(木)に「年末年始における情報セキュリティ対策」を公開しました。

長期休暇の時期は、「システム管理者が長期間不在になる」、「友人や家族と旅

実施したセキュリティリスク分析から得られた知見の集大成。「リスク分析の具体的な手法や手順がわからない」「リスク分析には膨大な工数を要するので回避したい」という事業者の悩み、課題に応えるため、その手法・手順を記載。これに加え、リスク分析シートや特定対策に関するチェックシート等、実践にかなう素材を提供しているのも特徴。

行に出かける」等、いつもとは違う状況になりやすく、ウイルス感染や不正アクセス等の被害が発生した場合に対処が遅れてしまったり、SNS への書き込み内容から思わぬ被害が発生したり、場合によっては関係者に対して被害が及ぶ可能性があります。

また、ここ数ヶ月の間、実在の企業を騙った不審なメールに関する相談が多く寄せられています。長期休暇明けはメールが溜まっていることが想定されますので、誤って不審なメールの添付ファイルを開いたり、本文中の URL にアクセスしたりしないように注意してください。

なお、2017 年に起きたサイバー攻撃の中から、標的型サイバー攻撃に関する活動の概要とそのトピックもご紹介しています。

「年末年始における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。

<https://www.ipa.go.jp/security/topics/alert291221.html>

5. 重要なセキュリティ情報（12 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³」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、ご自身のパソコン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。

12 月は、「緊急」0 件、「注意」2 件を公開しました。

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>

6. 「セキュリティ・ミニキャンプ in 北陸 2017（金沢）」を開催

（担当：イノベーション人材センター）

IPA は、金沢工業大学、金沢大学大学院自然科学研究科電子情報科学専攻、北陸先端科学技術大学院大学、セキュリティ・キャンプ実施協議会と共同で

³ 「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。

「セキュリティ・ミニキャンプ in 北陸 2017（金沢）」を12月2日（土）～3日（日）に開催しました。

石川県でのセキュリティ・ミニキャンプ地方大会の開催は3回目で、一般講座と専門講座の2講座を実施しました。

一般講座（参加者78名）では、セキュリティ・キャンプの面白さや得られたもの、応募のためのアドバイスに関する講演等が行われました。

また、専門講座（参加者24名）では、具体的な拡張機能の脆弱性を確認し、考えられる被害や脆弱性のない拡張機能の作り方を考察する講義等が行われました。

「セキュリティ・ミニキャンプ in 北陸 2017（金沢）」の詳細については、次のURLをご覧ください。

https://www.ipa.go.jp/jinzai/camp/2017/minicamp2017_kanazawa.html

7. 「セキュリティ・ミニキャンプ in 沖縄 2017」を開催

（担当：イノベーション人材センター）

IPAは、セキュリティ・ミニキャンプ沖縄実施協議会、セキュリティ・キャンプ実施協議会と共同で「セキュリティ・ミニキャンプ in 沖縄 2017」を12月16日（土）～17日（日）に2日間開催しました。

沖縄県でのセキュリティ・ミニキャンプ地方大会の開催は5回目で、セキュリティ専門の学生向けに専門講座を実施しました。

専門講座（参加者30名）では、ものづくりとセキュリティの融合について、グループで考察する講義等が行われました。

「セキュリティ・ミニキャンプ in 沖縄 2017」の詳細については、次のURLをご覧ください。

https://www.ipa.go.jp/jinzai/camp/2017/minicamp2017_okinawa.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. 「『つながる世界の開発指針』の実践に向けた手引き[IoT 高信頼化機能編]」の英語版を公開

（担当：ソフトウェア高信頼化センター）

IPAは、12月26日（火）に「『つながる世界の開発指針』の実践に向けた手引き[IoT 高信頼化機能編]」の英語版を公開しました。

本手引きは、IoT時代に向けて、「つながる世界の開発指針⁴」のうち、技術面での対策が必要になる部分を更に具体化し、安全安心なIoT機器や関連システムを開発する際に求められる機能と実装上の考慮事項を解説したものです。

英語版の公開により、海外への開発委託や事業展開に利用され、IoT製品の世界的な信頼性向上やIoT分野における日本企業の競争力向上の一助となることを期待しています。また、IPAでは本資料を用いた普及活動等を行い、海外へのIPAの活動の紹介や研究機関との連携強化を図ります。

IPAは、今後、策定が見込まれるIoTの国際標準を見据え、本手引きをベースとしたテクニカルリファレンスの提案も視野に入れて活動していきます。

『「つながる世界の開発指針」の実践に向けた手引き [IoT 高信頼化機能編]』の英語版の詳細については、次のURLをご覧ください。

<https://www.ipa.go.jp/sec/reports/20171226.html>

2. 「安全性解析手法 STAMP/STPA セミナー@大阪」を開催

(担当：ソフトウェア高信頼化センター)

IPAは、12月16日(土)に大阪市立総合生涯学習センター(大阪府大阪市)にて、「安全性解析手法 STAMP/STPA セミナー@大阪」をソフトウェア技術者協会(SEA⁵) 関西支部と一般社団法人組込みシステム技術協会(JASA⁶)との共同で開催しました。

本セミナーでは、複雑化するシステムの安全性を向上するために、欧米を中心に産業界で注目されているSTAMP⁷の解説やSTAMPに基づくシステムの安全性解析手法(STAMP/STPA⁸)の適用事例の解説等が行われました。

当日は47名の方に参加いただき、盛況のうちに終了しました。

今後もIoTの普及によって複雑化する社会システムに対応するため、IPAでは新たな安全性解析手法の提案・普及活動を継続し、システムの安全性向上に貢献していきます。

「安全性解析手法 STAMP/STPA セミナー@大阪」の詳細については、次のURL

⁴ IoT製品の開発者が開発時に考慮すべきリスクや対策を指針として明確化したものでIPAが2016年3月に公開。<https://www.ipa.go.jp/sec/reports/20160324.html>

⁵ SEA(Software Engineers Association) :ソフトウェアハウス、コンピューターメーカー、計算センター、エンドユーザ、大学、研究所等それぞれ異なった環境に置かれているソフトウェア技術者あるいは研究者が、そうした社会組織の壁を越えて、各自の経験や技術を自由に交流しあうための「場」として設立。

⁶ JASA(Japan Embedded Systems Technology Association) :組込みシステムにおける応用技術に関する調査研究、標準化の推進、普及および啓発等を行うことにより、組込みシステム技術の高度化および効率化を図り、それにより日本の産業の健全な発展と国民生活の向上に寄与することを目的とした一般社団法人。

⁷ STAMP(System Theoretic Accident Model and Processes) :マサチューセッツ工科大学(MIT)の Nancy Leveson 教授が提唱した「アクシデントはシステム構成要素間の相互作用から創発的に発生する」という理論。

⁸ STPA(System Theoretic Process. Analysis) :STAMP の理論に基づく、相互作用する機能単位でハザード要因を考える新しいハザード分析手法。

をご覧ください。

<https://sec.ipa.go.jp/seminar/20171216.html>

3. 「SEC journal」第51号を発行

(担当：ソフトウェア高信頼化センター)

IPAは、12月1日(金)に「SEC journal」第51号を発行しました。

「SEC journal」は、2005年1月に創刊号発刊以来、毎年4回発刊しており、SECの活動成果やソフトウェア開発に関する事例や論文を掲載しています。

「SEC journal」第51号の主な掲載記事は、以下の通りです。

- ・ 所長対談：企業のデジタル化を推進するために～CDO⁹の役割とは～
一橋大学商学研究科 教授/CDO Club Japan 顧問 神岡太郎 氏
- ・ 論文：提案依頼書に含まれる無理難題の分類
(2017年 SEC journal 論文賞 所長賞受賞論文)
- ・ 特集：ソフトウェア開発の定量的管理
- ・ 報告：ソフトウェア高信頼化センターの地域支援活動について

本号ではソフトウェア開発定量的管理を特集しています。SECでは2004年の設立当初より定量データを収集しており、2017年11月には「組込みソフトウェア開発データ白書2017¹⁰」を発行しました。

IPAでは、今後も定期的な情報発信活動を通じて、広く事業成果の普及を推進し、安全・安心なIoT社会の実現に貢献していきます。

「SEC journal」第51号の詳細については、次のURLをご覧ください。

<https://www.ipa.go.jp/sec/secjournal/index.html>

4. SECセミナー開催報告(12月)とSECセミナー開催案内(1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等を紹介する特別セミナーをそれぞれ実施しています。

12月は、次の日程で実施しました。

⁹ CDO(Chief Digital Officer) :最高デジタル責任者。企業内のデジタル戦略を取りまとめる役職。

¹⁰ 定量データを活用したプロジェクト管理の推進を目的に、様々な企業から組込みソフトウェア開発におけるプロジェクトデータを収集・分析して、その結果を取りまとめた書籍。

- ・失敗しない要件定義の勘どころ～ビジネス要求を正しくシステム化要件として定義するポイントの解説～（12月5日）
<https://sec.ipa.go.jp/seminar/20171205.html>
- ・システムの信頼性向上に向けたソフトウェア開発定量管理の勧め～定量的データに基づくソフトウェア開発のプロセス改善を目指して～（12月13日）
<https://sec.ipa.go.jp/seminar/20171213.html>
- ・事例から学ぶITサービス高信頼化へのアプローチ（第3回）～障害事例から根本原因を分析し教訓化するプロセスを学習～（12月14日）
<https://sec.ipa.go.jp/seminar/20171214.html>
- ・システム再構築を成功に導くための手法選択と計画立案～再構築におけるリスクの正確な把握と対策の合意手順の解説～（12月19日）
<https://sec.ipa.go.jp/seminar/20171219.html>

1月は、次の日程で開催を予定しています。

- ・ソフトウェア開発力強化セミナーin仙台～要件定義と定量的マネジメントの勘どころ～（1月30日）
<https://sec.ipa.go.jp/seminar/20180130-01.html>
- ・SEC先進事例応用セミナー ソフトウェア品質事例最前線～ソフトウェア品質シンポジウム AWARD 受賞者から学ぶ～（1月30日）
<https://sec.ipa.go.jp/seminar/20180130-02.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. **平成29年度秋期「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」（応用情報技術者試験、高度試験）の合格者を発表**
（担当：情報処理技術者試験センター）

IPAは、平成29年度秋期「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」のうち応用情報技術者試験・高度試験（いずれも経済産業省所管、10月15日（日）実施）の合格者を12月20日（水）に発表しました。

■ 情報処理安全確保支援士（登録セキスペ）試験

合格者に関する主な情報は以下のとおりです。なお、今回の最年長合格者は76歳であり、前回の最年長（65歳）を大幅に更新しました。

	応募者数	受験者数	合格者数	合格率	合格者平均年齢
情報処理安全確保支援士（登録セキスペ）試験	23,425	16,218	2,767	17.1%	35.5

合格者は、IPAに申請し、登録を受けることによって、名称独占の国家資格である「情報処理安全確保支援士（登録セキスペ）」を取得することができます。登録手続き等に関する詳しい情報は、次のURLをご覧ください。

<https://www.ipa.go.jp/siensi/index.html>

■ 情報処理技術者試験（応用情報技術者試験、高度試験）

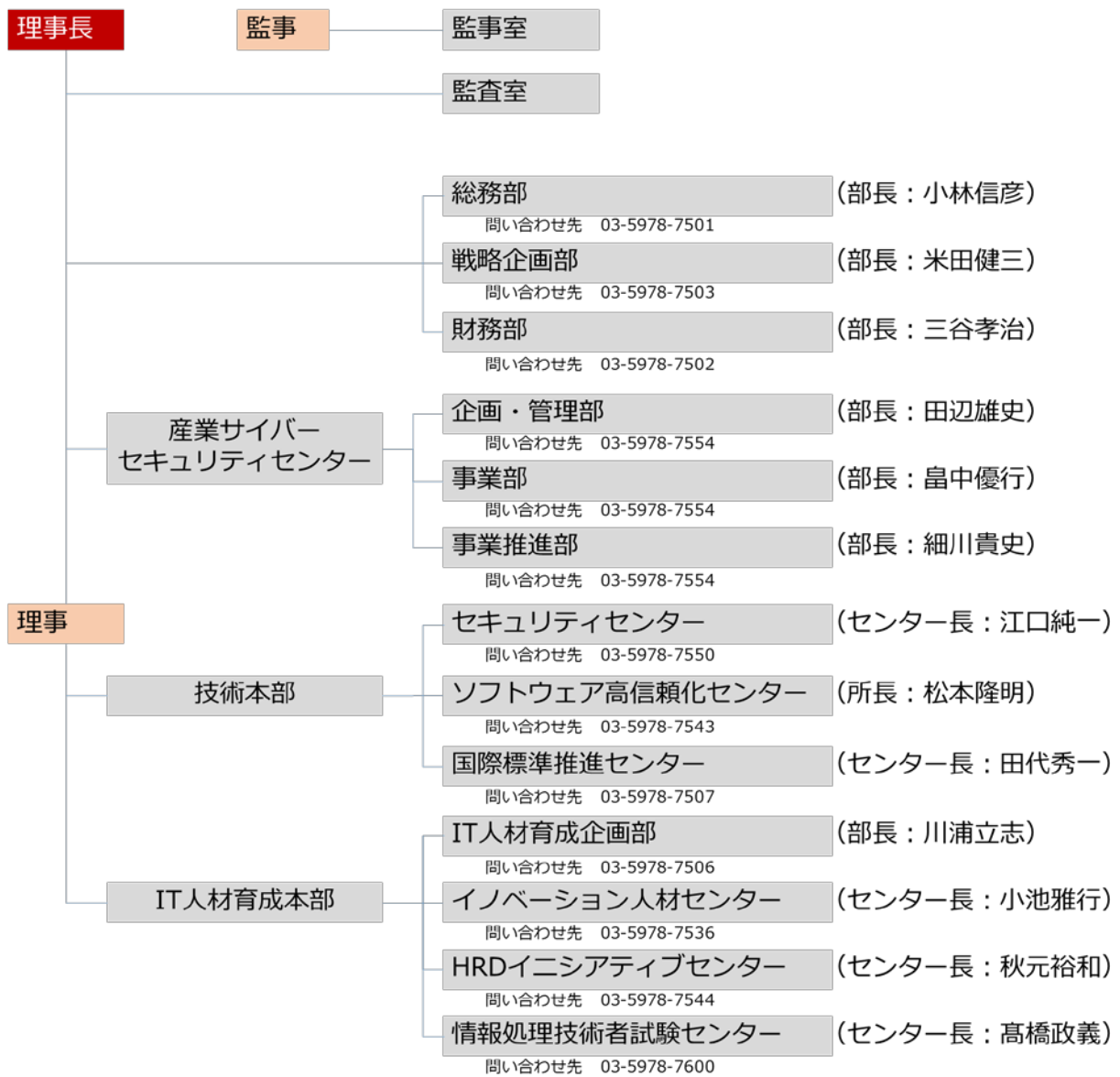
合格者に関する主な情報は以下のとおりです。なお、今回の「ネットワークスペシャリスト試験」の最年長合格者は67歳であり、これまでの最年長（66歳）を更新しました。

		応募者数	受験者数	合格者数	合格率	合格者平均年齢
応用情報技術者試験		50,969	33,104	7,216	21.8%	28.7
高度試験	ITストラテジスト試験	6,984	4,747	700	14.7%	39.0
	システムアーキテクト試験	8,678	5,539	703	12.7%	36.6
	ネットワークスペシャリスト試験	19,556	12,780	1,736	13.6%	33.5
	ITサービスマネージャ試験	5,779	3,932	535	13.6%	39.0

統計に関する詳しい情報については、次のURLをご覧ください。

https://www.jitec.ipa.go.jp/1_07toukei/_index_toukei.html

●IPA 組織図



本書に関するお問合せ先
 戦略企画部 広報G 山北・稲垣
 〒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 : pr-inq@ipa.go.jp