# IPA 情報発信第 167 号（2018 年 3 月）

2018 年 4 月 3 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 167 号の内容＞

## 今月のトピックス

### １．未踏事業スペシャルイベント「未踏会議 2018」を開催

未踏 IT 人材の起業・事業化を支援するスペシャルイベントを開催し、未踏事業の統括プロジェクトマネージャーである夏野剛氏の講演や次世代コンピュータ、AI、ロボティクスをテーマとしたパネルディスカッション等を行いました。また、未踏事業の支援者・支援機関、IT 人材活用を進めている企業等を対象とした未踏 IT 人材との交流イベント「未踏 Night」を行いました。

### ２．産業サイバーセキュリティに関する CISO 向け短期プログラムにて、元米国国家安全保障局（NSA）長官らが講演

CISO 向けの「業界共通トレーニング」において、キース・アレキサンダー氏（元米国国家安全保障局（NSA）長官兼サイバー軍司令官）、中西宏明産業サイバーセキュリティセンター長（日立製作所取締役会長兼代表執行役）らが講演を行いました。

### ３．IoT 製品・サービス開発者のセキュリティ対策と意識の調査結果を発表 -IoT 製品におけるセキュリティ意識の低さが明らかに-

IoT 製品の脆弱性の取扱いのあり方やその開発における脆弱性対策の啓発について検討するため、アンケート調査を実施した結果、製品開発段階でセキュリティ方針や基準があると答えた割合が 4 割に満たないことなどが明らかになりました。調査結果報告書に加え、対策ガイドも公開しました。

### ４．「漢字 6 万文字の国際標準化」が「デジタル・コンテンツ・オブ・ジ・イヤー’17」等を受賞

15 年間に渡り実施してきた「漢字 6 万文字の国際標準化」が、野田総務大臣ご臨席の一般社団法人デジタルメディア協会「デジタル・コンテンツ・オブ・ジ・イヤー’17」授賞式において、年間コンテンツ賞「優秀賞」を受賞するなどしました。

## Ⅰ．安全な IT 社会の実現

６．ENISA「ICS/SCADA システムの通信ネットワークの相互依存性」概要の公開
７．「SECURITY ACTION」自己宣言者サイトで受付開始
８．不正ログイン被害への対策特設ページの公開
９．「サイバーレスキュー隊（J-CRAT）技術レポート 2017 インシデント発生時の初動調査の手引き～WindowsOS 標準ツールで感染を見つける～」を公開
１０．重要なセキュリティ情報（3 月）

## 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．「つながる世界の品質確保に向けた手引き」を発表
２．STAMP 支援ツール「STAMP Workbench」を公開
３．「システムズエンジニアリング導入実施の一事例　報告書」を公開
４．「ソフトウェア開発データが語るメッセージ 2017」を公開
５．「成功事例に学ぶシステムズエンジニアリング」を公開
６．「制御システム セーフティ・セキュリティ要件検討ガイド」を公開
７．「情報処理システム高信頼化教訓集（IT サービス編）2017 年度版」を公開
８．「家づくりで理解する要求明確化の勘どころ」を公開
９．「はじめての STAMP/STPA（活用編）」を公開
１０．「SEC journal」第 52 号を発行
１１．「組込みソフトウェア開発向けコーディング作法ガイド ESCR［C 言語版］Ver.3.0」の英語版を公開
１２．SEC セミナー開催報告（3 月）
１３．「第 11 回地方自治体における情報システム基盤の現状と方向性の調査」の結果の公開

## 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

１．2018 年度未踏アドバンスト事業の公募を開始
２．「セキュリティ・キャンプフォーラム 2018」を開催
３．「セキュリティ・ミニキャンプ in 四国 2017（徳島）」を開催
４．「日経 BP IoT Japan 関西 2018」への出展
５．平成 30 年度春期「情報処理安全確保支援士（登録セキスペ）試験」及び「情報処理技術者試験」の応募者数について

## 今月のトピックス

### 1.未踏事業スペシャルイベント「未踏会議 2018」を開催

（担当：イノベーション人材センター）

IPA は、未踏 IT 人材の起業・事業化を支援するスペシャルイベント「未踏会議 2018」を 3 月 9 日（金）に浅草橋ヒューリックホール&カンファレンス（東京都台東区）で開催しました。

4 回目となる今回は、「過去にすがるな。未来をつかめ。」をキャッチフレーズに、「第 1 部 未踏 Keynote」、「第 2 部 未踏 Deep-Dive」、「第 3 部 未踏 Night」の三部構成で、未踏 IT 人材の活動内容を紹介し認知を広げることで、彼らの産業界等での更なる活躍を促進することを目的に行いました。

「第 1 部 未踏 Keynote」では、未踏事業の統括プロジェクトマネージャーである夏野剛氏を招いて、未踏事業の実績と今後の計画を紹介いただくとともに、3 名の未踏 IT 人材のショートプレゼンテーションを実施しました。

「第 2 部 未踏 Deep-Dive」では、次世代コンピュータ、AI、ロボティクスの 3 つのテーマについて、それぞれのフィールドで活躍している未踏 IT 人材とゲストによるパネルディスカッションを行いました。

「第 3 部 未踏 Night」では、未踏 IT 人材が自身の研究成果や事業について未踏事業の支援者・支援機関、IT 人材活用を進めている企業等に対し紹介するプレゼンテーションを実施し、併せて未踏 IT 人材の成果出展や書籍紹介ブース設置を行いました。

当日は、260 名以上の方々に参加いただき、ニコニコ生放送では 1 万 5 千以上の視聴数となりました。

「未踏会議 2018」の詳細については、次の URL をご覧ください。

https://www.ipa.go.jp/jinzai/mitou/2017/mitoukaigi2018.html

https://www.ipa.go.jp/jinzai/mitou/mitoukaigi/2018/

### 2.産業サイバーセキュリティに関する CISO 向け短期プログラムにて、元米国国家安全保障局（NSA）長官らが講演

（担当：産業サイバーセキュリティセンター）

IPA は、2018 年 3 月 2 日（金）～3 日（土）に、サイバーセキュリティ対策を統括する CISO を対象とした「業界共通トレーニング」を実施しました。トレーニングには、電力、製薬、食料品、電気機器、電子部品等の業界から 12 名の受講者が集まりました。

本トレーニングは、産業サイバーセキュリティセンターのアドバイザーであ

るキース・アレキサンダー氏（元米国国家安全保障局（NSA）長官兼サイバー軍司令官）が CEO を務める米国アイアンネット・サイバーセキュリティ社の協力を得て行われているものです。今年度最終回となる今回は、キース・アレキサンダー氏も講師として登壇しました。

2 日間の日程では、中西宏明産業サイバーセキュリティセンター長（日立製作所取締役会長兼代表執行役）の特別講演や、米国電力会社のセキュリティ対策責任者等も歴任したスティーブ・ザルースキー氏（リーバイス社チーフセキュリティアーキテクト）らによる CISO の在り方に関する講義が行われました。ほかにも、受講者が CISO 及びその連携すべきメンバーの役割でインシデント対応を模擬体験する机上演習（ウォーゲーム・セッション）が行われ、講師及び受講者の経験談も交えながら、活発なディスカッションが行われました。

## 3.IoT 製品・サービス開発者のセキュリティ対策と意識の調査結果を発表
## － IoT 製品におけるセキュリティ意識の低さが明らかに －

（担当：セキュリティセンター）

IPA は、3 月 22 日（木）に「情報システム等の脆弱性情報の取扱いに関する研究会」における IoT 製品・サービス開発者のセキュリティ対策と意識の調査結果報告書及びガイド等を発表しました。

IoT 製品の普及に伴い、組み込まれたソフトウェアの脆弱性に起因する脅威が現実のものとなっていることを背景に、「情報システム等の脆弱性情報の取り扱いに関する研究会」では、IoT 製品の脆弱性の取扱いのあり方やその開発における脆弱性対策の啓発について検討するため、アンケート調査を実施しました。その結果、次のような結果が得られました。

1. 製品・サービスの開発段階でセキュリティ方針、基準が「ある」と回答した割合：35.6%
2. 開発段階において脆弱性対策を考慮している割合：68.3%
3. 2.で実施している対策のうち、実施率が低かった対策：セキュアプログラミングの適用が 41.4%、コーディング規約の利用が 36.4%

さらに同研究会では、本調査を踏まえ、IoT 製品・サービスの提供におけるセキュリティ対応に対する企業の責任の考え方や、脆弱性対策が必要な理由等を解説し、セキュリティ対策に企業として取り組んでもらうことを目的とした IoT 製品・サービス脆弱性対応ガイドを作成しました。

また、併せて、「情報システム等の脆弱性情報の取扱いに関する研究会」の活動成果をまとめた報告書を公開しました。

IoT 製品・サービス開発者のセキュリティ対策と意識の調査結果の詳細については、次の URL をご覧ください。

https://www.ipa.go.jp/security/fy29/reports/vuln_handling/index.html

## 4.「漢字 6 万文字の国際標準化」が「デジタル・コンテンツ・オブ・ジ・イヤー'17」等を受賞

（担当：国際標準推進センター）

IPA は、3 月 12 日（月）に「漢字 6 万文字の国際標準化」について野田総務大臣ご臨席の一般社団法人デジタルメディア協会（AMD）「デジタル・コンテンツ･オブ・ジ・イヤー '17／第 23 回 AMD アワード」授賞式において、年間コンテンツ賞「優秀賞」を受賞しました。

IPA では、行政の実務で求められる人名や地名等の正確な表記をコンピュータで可能にするために、文字のデザイン、文字コードとの対応付け等を整備しながら国際標準化作業を進め、昨年 12 月に約 6 万文字の漢字が国際規格（ISO/IEC）となりました。

これら漢字の統一規格化の調査から完了までの 15 年間に渡る「漢字 6 万文字の国際標準化」事業の功績が、評価されたものです。

また、3 月 6 日（火）には、一般社団法人オープン＆ビッグデータ活用・地方創生推進機構の「勝手表彰[1]」において、スポンサー賞のうち「日本マイクロソフト賞」を受賞しました。

受賞事業に関連する「「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」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

[1] オープンデータに関する優れた取り組みを、勝手に選んで表彰。2013 年度から始まり、2017 年度で 5 回目を迎える。

## Ⅰ．安全な IT 社会の実現

### １．「IT サプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査」報告書を発表

（担当：セキュリティセンター）

IPA は、3 月 26 日（月）に「IT サプライチェーン[2]の業務委託におけるセキュリティインシデント及びマネジメントに関する調査」の報告書を発表しました。

近年、ウイルス感染や不正アクセス等により、ウェブサイトの運営委託先から大量の個人情報が漏洩した、というような報道を目にすることは珍しいものではなくなりました。このような IT サプライチェーン上のインシデントの影響は、直接の被害組織だけでなく、複数の関係者に影響を及ぼす可能性があり、看過できない課題となっています。

そこで、IPA では、IT サプライチェーンにおける対策状況、及びインシデント発生事例等について調査を実施しました。本調査の中でユーザ企業 499 社、IT システム・サービス提供企業 620 社にアンケート調査を実施した結果、次のようなことが明らかになりました。

1. 情報通信業以外の委託元の過半数が、実施すべき情報セキュリティ対策を仕様書等で委託先に明示していない。特に、製造業では 71.1%、卸売・小売業で 74.2%が明記しておらず、顕著。
2. 委託契約におけるセキュリティ上の課題を質問したところ、「情報セキュリティ上の責任範囲（責任分界点）がわからない」と回答する割合が、委託元、委託先とも最多。

今後、調査結果を受け、IT サプライチェーンの業務委託におけるセキュリティ対策の状況把握や対策実施が推進されるよう、関連する調査・分析を予定しています。

「IT サプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査」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/about/press/20180326.html

2　IT システム・サービスに関する業務を系列企業やビジネスパートナー等に外部委託し、その委託が連鎖する形態。

## ２．「CISO 等セキュリティ推進者の経営・事業に関する役割調査」報告書の公開

（担当：セキュリティセンター）

IPA は、3 月 28 日（木）に「CISO 等セキュリティ推進者の経営・事業に関する役割調査」報告書を公開しました。

経済産業省及び IPA が共同で策定した「サイバーセキュリティ経営ガイドライン[3]」の経営者が認識すべき 3 原則の一つに、経営層はサイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要というものがあります。

一方、サイバーセキュリティ戦略本部が公開した「サイバーセキュリティ人材育成プログラム[4]」では、経営層自らがサイバーセキュリティ対策を企画・立案し、実務者層を動かすことは困難であるとしています。そのため、同プログラムは、経営戦略とサイバーセキュリティに関する業務課題を理解した上で、様々な役割を持った実務者層を指揮し、経営層の補佐的な役割を担う「橋渡し人材」が必要であるとしています。

本報告書では経営層、CISO[5]及びその補佐役となる橋渡し人材等のセキュリティ推進者が担う役割、特にセキュリティへの取組みが経営と事業に貢献するようマネジメントする役割について、その実態や期待されている内容について解説しています。

「CISO 等セキュリティ推進者の経営・事業に関する役割調査」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/index.html

## ３．「第四次産業革命を踏まえた秘密情報の管理と利活用におけるリスクと対策に関する調査」報告書の公開

（担当：セキュリティセンター）

IPA は、3 月 22 日（木）に「第四次産業革命を踏まえた秘密情報の管理と利活用におけるリスクと対策に関する調査」報告書を公開しました。

第四次産業革命を視野に入れたデータの利活用の推進等を背景に、クラウドサービスを利用して社外環境で自社の情報を管理する、あるいは複数者間でデータを共有するといった機会も増加し、情報の利活用・管理の手法が多様化しています。

---

[3] 2015 年 12 月公開、2017 年 11 月改訂（http://www.meti.go.jp/policy/netsecurity/mng_guide.html）

[4] 2017 年 4 月公開（https://www.nisc.go.jp/active/kihon/pdf/jinzai2017.pdf）

[5] Chief Information Security Officer、最高情報セキュリティ責任者

こうした新たな社会動向を踏まえ、今般、営業秘密を含む秘密情報の漏えい、その被害の拡大を引き起こす管理上の課題及び想定されるリスクを抽出し、これらの課題・リスクに対応した情報漏えい対策に関する調査を行いました。

本報告書では秘密情報の管理・利活用におけるリスク・課題、対策に関するポイントを企業における秘密情報管理の構造から整理しています。また、データ利活用等の重要性増大に伴う秘密情報管理上の新たなリスク・課題についても解説しています。我が国におけるデータ利活用の推進において、各者が適切に秘密情報を管理・利活用する上での一助となることを期待します。

「第四次産業革命を踏まえた秘密情報の管理と利活用におけるリスクと対策に関する調査」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/ts_research/20180322.html

## ４．「データ利活用における重要情報共有管理に関する調査」報告書の公開

（担当：セキュリティセンター）

IPA は、3 月 29 日（木）に「データ利活用における重要情報共有管理に関する調査」報告書を公開しました。

AI、ビッグデータ解析等の IT 技術を用いたデータ利活用による新しいビジネスが注目されています。このようなビジネスを立ち上げる場合、企業内、企業間、あるいは産学官等で重要情報（営業秘密情報、知財情報等）を共有してそれらデータを利活用しながら、それらの保護にも注意して事業を推進する必要性が我が国でも広く認識されつつあります。

今般、新しい IT 基盤でのデータ利活用に関して先進的な事例の多い海外（米国）における重要情報の共有や管理状況の調査を行いました。

本報告書では主に、「米国における企業・政府機関・大学間の連携」、「企業、政府機関、大学それぞれのデータ共有管理の特徴」について解説しています。これからの産学官の連携に当たり適切にデータを管理、利活用する上での一助となることを期待します。

「データ利活用における重要情報共有管理に関する調査」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/ts_research/20180329.html

## ５．「情報セキュリティ 10 大脅威 2018」の解説資料の公開

（担当：セキュリティセンター）

IPA は、3 月 30 日（金）に「情報セキュリティ 10 大脅威 2018」[6]の解説を記載した資料を公開しました。本資料は、次の 3 章構成となっています。

・第 1 章 情報セキュリティ対策の基本 IoT 機器(情報家電)編
IoT 機器を利用する上で、実施しておくべき情報セキュリティ対策の基本について解説しています。

・第 2 章 情報セキュリティ 10 大脅威 2018
2017 年において社会的影響が大きかったセキュリティ上の脅威について、「10 大脅威選考会」の投票結果に基づき、「個人」、「組織」における脅威を 1 位から 10 位に順位付けして解説しています。

・第 3 章 注目すべき脅威や懸念
社会に影響を与えるおそれがあり、現時点で注目しておきたい脅威や懸念等について解説しています。

IPA は、本資料が、読者自身のセキュリティ対策への理解と、各企業・組織の研修やセキュリティ教育等に活用されることにより、セキュリティ対策の普及の一助となることを期待しています。

「情報セキュリティ 10 大脅威 2018」解説資料の詳細については、次の URL をご覧ください。

https://www.ipa.go.jp/security/vuln/10threats2018.html

## ６．ENISA「ICS/SCADA システムの通信ネットワークの相互依存性」概要の公開

（担当：セキュリティセンター）

IPA は、3 月 30 日（金）に ENISA[7]発行文書の概訳「ICS/SCADA システムの通信ネットワークとセキュリティ[8]」を公開しました。

本概訳は、長距離通信、とりわけインターネットの活用によって変革を果たした産業制御システム（ICS）／遠隔監視制御（SCADA）システムを、ネットワ

---

6 2017 年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、IPA が脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者等からなる「10 大脅威選考会」が脅威候補に対して審議・投票を行い、決定したもの。

7 欧州ネットワーク情報セキュリティ機関

8 原題「Communication network dependencies for ICS/SCADA Systems」

ーク化がもたらした新たな脅威から守るため、ICS/SCADA システムを構成する機器をつなぐネットワークに着目し、脅威、攻撃シナリオ、対策等を知見として示し、ICS/SCADA システムのセキュリティ及びレジリエンスの向上を支援することを目的としたものです。本概訳では、対象読者、モデルとするアーキテクチャ、ICS/SCADA の相互依存性、脅威と脆弱性、攻撃シナリオ、対策、提言の計 7 項目について、概要を日本語でまとめています。

ENISA 発行文書の概訳「ICS/SCADA システムの通信ネットワークの相互依存性」の詳細については、次の URL の「海外における取組み」をご覧ください。

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

## 7.「SECURITY ACTION」自己宣言者サイトで受付開始

（担当：セキュリティセンター）

IPA は、3 月 1 日（木）に「SECURITY ACTION」自己宣言者サイトでの SECURITY ACTION の登録受付を開始しました。

「SECURITY ACTION」は、中小企業自らが情報セキュリティ対策に取組むことを自己宣言する制度です。

「SECURITY ACTION」自己宣言者サイトでは、以下のサービスを提供しています。

・「SECURITY ACTION」の新規/変更/中止の申込み
・「SECURITY ACTION」ロゴマークのダウンロード
・「SECURITY ACTION」自己宣言企業の検索/一覧ダウンロード

「SECURITY ACTION」自己宣言者サイトでの詳細については、次の URL をご覧ください。

https://security-shien.ipa.go.jp/security/index.html

## 8. 不正ログイン被害への対策特設ページの公開

（担当：セキュリティセンター）

IPA は、3 月 8 日（木）に不正ログイン被害への対策特設ページを公開しました。

スマートフォンの普及及びインターネットサービスの拡大に伴い、情報セキュリティ安心相談窓口には、インターネットサービスへの不正ログイン被害に関する相談が継続して多く寄せられています。そこで、不正ログイン対策につ

いて情報提供を行う特集ページを開設することとしました。
本ページでは不正ログイン被害への対策として、「パスワードの作成・管理方法」と「2 段階認証の設定」について情報提供を行っています。「2 段階認証の設定」については、下記 2 種類の設定手順書を公開しました。

1. Apple ID 編　「2 ファクタ認証」
2. Google アカウント編　「2 段階認証プロセス」

今後も、SNS、ショッピングサイト、クラウドサービス等の主要なサービスについて、順次追加していく予定です。

不正ログイン被害への対策特設ページの詳細については、次の URL をご覧ください。

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

## ９．「サイバーレスキュー隊（J-CRAT[9]）技術レポート 2017 インシデント発生時の初動調査の手引き～WindowsOS 標準ツールで感染を見つける～」を公開

（担当：セキュリティセンター）

IPA は、3 月 29 日（木）に「サイバーレスキュー隊（J-CRAT）レポート 2017 インシデント発生時の初動調査の手引き～WindowsOS 標準ツールで感染を見つける～」を公開しました。
本レポートは、組織内でセキュリティインシデントが発生した際に、マルウェア感染の検証、被害把握を実践するための手引きです。J-CRAT のレスキュー活動の初動段階でのノウハウや手順を解説し、各組織のシステム担当者が適切な対応をとれるようになることを目的としています。
今回は、J-CRAT のレスキュー活動で実際に行っている初動対応の一部である WindowsOS 標準ツールで感染を見つける方法を解説しています。

サイバーレスキュー隊（J-CRAT）レポート 2018　～インシデント発生時の初動調査の手引き～ の詳細については、次の URL をご覧ください。

https://www.ipa.go.jp/security/J-CRAT/report/20180329.html

[9] J-CRAT：Cyber Rescue and Advice Team against targeted attack of Japan

### １０．重要なセキュリティ情報（3 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「重要なセキュリティ情報[10]」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す。当該情報をご参照いただき、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。

3 月は、「緊急」0 件、「注意」3 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

## 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．「つながる世界の品質確保に向けた手引き」を発表

（担当：ソフトウェア高信頼化センター）

IPA は、3 月 22 日（木）に「つながる世界の品質確保に向けた手引き～IoT 開発・運用における妥当性確認・検証の重要ポイント～」を発表しました。

本ガイドブックは、今後ますます普及が進む IoT[11]の品質確保を目的に、検証の立場における考慮事項を示したガイドブックであり、2016 年 3 月に公開した「つながる世界の開発指針[12]」の品質に関する事項を具体化したものです。

開発者、保守者、品質保証者、運用者等、品質に携わるすべての担当者を対象として、開発、保守及び運用における IoT の品質確保、維持及び改善のために最低限考慮してほしいポイントを 13 の視点としてまとめています。

本ガイドブックを活用することで、IoT 機器及び IoT システムの開発及び運用時に考慮すべき品質を理解、確認することができます。また、開発及び運用の現場で活用できる「つながる世界の品質確保チェックリスト」も併せて公開

---

10 「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。

11 IoT(Internet of Things) ：さまざまなモノがインターネットに接続し、情報をやり取りすること。

12 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。
https://www.ipa.go.jp/sec/publish/tn16-002.html

しました。
IPA では、本ガイドブックを実際の現場で活用していただくために、セミナーや展示会等で周知を行い、利用者が安心して利活用できる品質の IoT 機器・システムの実現に貢献していきます。

「『つながる世界の品質確保に向けた手引き』を発表」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/20180322.html

## ２．STAMP 支援ツール「STAMP Workbench」を公開

（担当：ソフトウェア高信頼化センター）

IPA は、3 月 30 日（金）に STAMP[13]支援ツール「STAMP Workbench」を公開しました。
近年の IoT の進展に伴い大規模・複雑化するシステムでは、アクシデントの原因として複数の要素間の相互作用による要因も考える必要があります。STAMP/STPA[14]は、システムを構成するハードウェアやソフトウェアだけではなく、システムと連携する他のシステムや人間系、環境までも含めて複数の要素間の相互作用による要因を捉える新しい安全性解析手法で、欧米を中心に宇宙、航空、鉄道等、幅広い産業界で注目されています。
しかし、日本においては活用方法の理解不足と本解析手法の特徴である思考作業と図表を含む資料の作成、修正作業の繰り返しによる手順の煩雑さが普及の阻害となっています。このため、利用者が思考作業に専念できるように、以下の機能を実装したツールを開発しました。

1. STAMP/STPA 初心者に対する解析基本手順支援機能
2. 解析用資料における図表の自動生成・修正機能

IPA では、開発した STAMP 支援ツール「STAMP Workbench」の普及活動を通じて、システムの安全性向上に貢献していきます。

「STAMP 支援ツール『STAMP Workbench』を公開」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/20180330.html

---

13 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。

14 STAMP/STPA(STAMP/System Theoretic Process Analysis) ：STAMP の理論に基づいたハザード(事故要因)解析手法。

## ３.「システムズエンジニアリング導入実施の一事例　報告書」を公開

（担当：ソフトウェア高信頼化センター）

IPA は、2017 年 4 月から 8 か月間、「システム開発の上流設計工程にシステムズエンジニアリング[15]の考え方を導入する取組み」を、三菱重工機械システム株式会社と共同で実施し、「システムズエンジニアリング導入実施の一事例　報告書」として 3 月 1 日（木）に公開しました。

近年、サービスや社会インフラが複雑化・多様化し、多数の専門領域にまたがるシステム開発が増加しており、システム全体を最適化する開発やビジネス設計が必要となってきています。

そこで IPA では、欧米を中心に、高度な専門性を要する複雑なシステム開発に適用されているシステムズエンジニアリングのアプローチを訴求することが有効であると考え、三菱重工グループの高度道路交通システム[16]系の新たなシステム開発の取組みを対象に、システム開発の現場へのシステムズエンジニアリングのアプローチの導入を試行しました。

本取組みにより、次のような知見が得られました。

1. 「システムライフサイクルのプロセス」を理解し、開発標準と比較することで、自部門の有識者の暗黙知を整理評価して、新たな開発標準の運用に活用できる。
2. 上流工程で、プロジェクト本来の目的とシステムの設計内容の整合性を確認することで、問題の早期発見につなげられる。

IPA は、本取組みを通じ、IoT システムの開発など、市場拡大が期待される分野において、システムズエンジニアリングの考え方が普及することを期待しています。

「『システムズエンジニアリング導入実施の一事例　報告書』を公開」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/20180301.html

## ４.「ソフトウェア開発データが語るメッセージ 2017」を公開

（担当：ソフトウェア高信頼化センター）

IPA は、3 月 6 日（火）に「ソフトウェア開発データが語るメッセージ 2017」を公開しました。

---

15 複数の専門領域にまたがる多様な価値を考慮しつつ全体最適を実現するためのアプローチのこと。

16 高度道路交通システム（ITS：Intelligent Transport Systems）：人と道路と自動車の間で情報の受発信を行い、道路交通が抱える事故や渋滞、環境対策など、様々な課題を解決するためのシステムのこと。

本書では、IPA が保有するソフトウェア開発プロジェクトデータを分析して導き出された、「ソフトウェア生産性は全体的に低下傾向にあること」、「ソフトウェアに対する品質要求は高まっていること」、「生産性を低下させないポイントは上流工程強化であること」について説明しています。

IPA は、上記分析結果を踏まえてソフトウェア開発者向けに次のようなメッセージを記載しています。

1. 定量的管理を推進し、生産性の経年推移を踏まえて生産性目標の設定を。
2. 定量的管理を推進し、品質要求レベルに見合った生産性目標の設定を。
3. 業務分野経験等のスキルが高い要員の育成を。

IPA は、本書が活用されることでソフトウェア開発現場の品質マネジメントが改善され、ソフトウェアの信頼性がより一層向上していくことを期待しています。

「『ソフトウェア開発データが語るメッセージ 2017』を公開」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/20180306.html

## ５．「成功事例に学ぶシステムズエンジニアリング」を公開

（担当：ソフトウェア高信頼化センター）

IPA は、3 月 15 日（木）に「成功事例に学ぶシステムズエンジニアリング～IoT 時代のシステム開発アプローチ～」を公開しました。

本資料では、日本国内 5 社の成功事例を基に、システムズエンジニアリングのアプローチが「どのような場面で」、「どのような効能を発揮するのか」を具体的に説明しています。さらに、問題解決にシステムズエンジニアリングを利用しようとした場合の注意ポイントや、適用に向けてのヒントも紹介しています。

IPA では、本資料がシステムズエンジニアリングの現場への適用を促進する「入門書」として幅広く活用されることを期待して、積極的な普及活動を展開していきます。

「『成功事例に学ぶシステムズエンジニアリング』を公開」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/20180315.html

## ６.「制御システム セーフティ・セキュリティ要件検討ガイド」を公開

（担当：ソフトウェア高信頼化センター）

IPA は、3 月 19 日（月）に制御システムの安全関連システムに関するセキュリティ向上を目的とした「制御システム セーフティ・セキュリティ要件検討ガイド」を公開しました。

本ガイドは、制御システムに関わる事業者やインテグレータが、システムのライフサイクルを通じて、セーフティを確保しながら制御システムのセキュリティ検討を行う際に参考となる検討の基本的な考え方及び手順の概要を示しています。また、本ガイドを参考に理解を深められるように、ケーススタディによる解説も掲載し、脅威分析を実施する際の分析シートのテンプレートも併せて公開しました。

「『制御システム セーフティ・セキュリティ要件検討ガイド』を公開」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/20180319.html

## ７.「情報処理システム高信頼化教訓集（IT サービス編）2017 年度版」を公開

（担当：ソフトウェア高信頼化センター）

IPA は、3 月 26 日（月）に重要インフラに関わるシステムにおける類似障害の発生防止と影響範囲の縮小を目指し、障害情報とその対策をそれぞれ普遍化した「情報処理システム高信頼化教訓集（IT サービス編）2017 年度版」を公開しました。

本教訓集は、2014 年 5 月に初版を公開後、毎年新たな「教訓」を追加して最新化を行っています。4 回目の改訂となる 2017 年度版では、新たに 8 件の教訓を追加し累計 50 件の教訓を収録しています。また、教訓及び IPA で蓄積している報道された障害事例を容易に検索できるように、IPA が導出した 99 種の「注意すべき観点[17]」のうち特に重要な 10 種についても掲載しています。

IPA は、本教訓集の公開を通して、「教訓」が業界・分野を越えて幅広く共有され、国民生活や社会・経済基盤を支えるシステムの信頼性向上につながることを期待しています。

---

[17] 2018 年 1 月 31 日に教訓及び IPA で蓄積している報道された障害事例について、短い時間でポイントや全体像をつかめるよう、99 種の「注意すべき観点」として IPA が取りまとめ、公開したもの。また、その観点に基づいて分類した障害事例の一覧表も併せて公開した。
https://www.ipa.go.jp/sec/system/index.html#shougaijirei

「『情報処理システム高信頼化教訓集（IT サービス編）2017 年度版』を公開」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/20180326.html

## ８.「家づくりで理解する要求明確化の勘どころ」を公開

（担当：ソフトウェア高信頼化センター）

IPA は、3 月 27 日（火）に小冊子「家づくりで理解する要求明確化の勘どころ～システム構築を成功させる要件定義のポイント～」を公開しました。

昨今、IT システムの大規模化・複雑化に伴い、ビジネス要求が高度化しています。ユーザ企業から開発企業に要求が正しく伝わっていないと、開発プロジェクトの現場で実装する機能は要求を正しく反映したものになりません。この問題を解決するには、ユーザ企業が要求を抜け漏れなく定義するために実施すべきことを明確にすることが重要です。

本小冊子では、「システム開発の要件定義」と「家づくりの要件定義」が非常によく似ていることから、システム開発の要件定義のポイントを家づくりに例えて分かりやすく解説しています。

IPA では、本小冊子の普及とともに、これを通じて 2017 年 3 月に公開した「ユーザのための要件定義ガイド～要求を明確にするための勘どころ～」の普及を図り、システム開発の要件定義時の不備に伴うトラブルの防止に向けた活動を継続していきます。

「『家づくりで理解する要求明確化の勘どころ』を公開」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/20180327.html

## ９.「はじめての STAMP/STPA（活用編）」を公開

（担当：ソフトウェア高信頼化センター）

IPA は、3 月 28 日（水）に「はじめての STAMP/STPA（活用編）」を公開しました。

本資料は、2016 年 4 月に公開した「はじめての STAMP/STPA[18]」、2017 年 3 月に公開した「はじめての STAMP/STPA（実践編）[19]」から一歩踏み込み、STAMP/STPA を「やってみる」から「当たり前に行う」レベルに読者を引き上げ

18 https://www.ipa.go.jp/sec/reports/20160428.html
19 https://www.ipa.go.jp/sec/publish/tn17-001.html

ることを目的に作成しました。産業界での実施事例を中心にSTAMP/STPAによる定性的分析からシミュレーションによる定量的分析につなげた事例、セキュリティ分析への応用事例、また新しい安全理論であるSafety2.0[20]の実現に向けてFRAM[21]をはじめとする安全解析手法について解説しています。

IPAでは、本資料を含む「はじめてのSTAMP/STPA」シリーズの普及を推進し、安全・安心なIoT社会の実現に貢献していきます。

「『はじめてのSTAMP/STPA（活用編）』を公開」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/20180328_2.html

## １０.「SEC journal」第52号を発行

（担当：ソフトウェア高信頼化センター）

IPAは、3月1日（木）に「SEC journal」第52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回発行しており、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52号の主な掲載記事は、以下のとおりです。

・所長対談：システム思考の重要性について考える
　　慶應義塾大学大学院システムデザイン・マネジメント研究科
　　教授　白坂　成功　氏
・特集：複雑システムの安全性分析法STAMP
・事例紹介：システムズエンジニアリングを活用したITSのセキュリティ機能設計の取り組み
・報告：SEC journal 論文賞　受賞論文発表[22]

本号では「複雑システムの安全性分析法STAMP」を特集しています。複雑化するシステムに対応するためには、従来型の安全性分析手法では限界があり、新たな分析手法としてSTAMPに注目が集まっています。STAMPの概要、ツール紹介、国内外での適用事例等、最新の動向をお伝えします。

「SEC journal』第52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

---

20 人と機械と周辺環境をつないで情報をやりとりし、協調して安全を確保する取組みのこと。

21 FRAM(Functional Resonance Analysis Method) ：機能共鳴分析手法

22 IPAでは、ソフトウェア開発現場で役立つ論文を募集しており、SEC journalへ掲載された論文の中から毎年1回「SEC journal 論文賞」を選定し、表彰している。

## １１．「組込みソフトウェア開発向けコーディング作法ガイド ESCR [C 言語版] Ver.3.0」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、3 月 28 日（水）に「組込みソフトウェア開発向けコーディング作法ガイド ESCR[23]［C 言語版］Ver.3.0」の英語版を公開しました。

ESCR とは、自動車や家電製品をはじめとする多くの製品の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ルール集としてまとめたものです。

本資料は、2 月 15 日（木）に Web 公開した「ESCR［C 言語版］Ver.3.0[24]」を、オフショア開発[25]や海外企業でも利用できるように日本語版の内容をそのまま英訳したものです。

IPA では、本資料を用いた普及活動を通じて、安全・安心な組込みソフトウェアを効率的に開発できる環境づくりに貢献するとともに、海外への IPA の活動紹介や研究機関との連携強化を図っていきます。

「『組込みソフトウェア開発向けコーディング作法ガイド ESCR［C 言語版］Ver.3.0』の英語版を公開」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/20180328_1.html

## １２．SEC セミナー開催報告（3 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。

3 月は、次の日程で実施しました。

・事例から学ぶ IT サービス高信頼化へのアプローチ（第 4 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～（3 月 7 日）

https://sec.ipa.go.jp/seminar/20180307.html

・IoT 時代のシステム開発の課題に立ち向かう～システムズエンジニアリン

23 ESCR(Embedded System development Coding Reference)

24 https://www.ipa.go.jp/sec/reports/20180215.html

25 システム開発などの業務を海外企業や海外の現地法人などに委託すること。

グ導入の薦め～（3 月 15 日）
https://sec.ipa.go.jp/seminar/20180315.html

・上流工程強化セミナー in 大阪～システム再構築を成功に導くために～（3 月 17 日）
https://sec.ipa.go.jp/seminar/20180317.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～基本となる考え方（ベンチマーキング）と企業での導入事例を紹介～（3 月 23 日）
https://sec.ipa.go.jp/seminar/20180323.html

・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～（3 月 28 日）
https://sec.ipa.go.jp/seminar/20180328.html

## １３.「第 11 回地方自治体における情報システム基盤の現状と方向性の調査」の結果の公開

（担当：国際標準推進センター）

IPA は、3 月 16 日（金）に「第 11 回地方自治体における情報システム基盤の現状と方向性の調査」を実施し、その結果を公開しました。

本調査は、地方自治体における情報システムの利活用状況の現状を把握することを目的に、2007 年度より継続して実施しています。また、一昨年度から、「世界最先端 IT 国家創造宣言」に基づき、電子行政分野におけるオープンな利用環境整備に向けたオープンデータの取り組み状況を主に調査を実施しています。

「世界最先端 IT 国家創造宣言・官民データ活用推進基本計画」(2017 年 5 月 30 日閣議決定)では、「官民データを相互につなげて共有し、利活用が容易になるよう、国と各地方公共団体等が一体となって環境整備を行う」ことが求められています。

本調査[26]の結果、IPA が事業を進める「文字情報基盤」の認知度は 66.3%、「共通語彙基盤」の認知度は 58.1%にとどまっており、認知度の向上に引き続き取り組む必要があることが明らかになりました。

IPA は、「文字情報基盤」や「共通語彙基盤」の各自治体における活用状況、各自治体でのオープンデータの取り組みなど、本調査結果の活用を通じて、地方自治体における IT プラットフォームの整備やオープンデータの利活用が一層推進されることを期待します。

26 アンケート調査を実施し、706 自治体が回答。

「第 11 回地方自治体における情報システム基盤の現状と方向性の調査」の詳細については、次の URL をご覧ください。

https://www.ipa.go.jp/osc/research/jichitai.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. 2018 年度未踏アドバンスト事業の公募を開始

（担当：イノベーション人材センター）

IPA は、3 月 8 日（木）～4 月 24 日（火）の期間で 2018 年度未踏アドバンスト事業の公募を開始しました。

未踏アドバンスト事業は、IT を駆使してイノベーションを創出できる優れたアイディア・技術力を持つ“未踏的 IT 人材”が、自らのアイディアや技術力を最大限に活かし、起業や自らが実施主体者となる事業化につなげていけるよう、優れた能力と実績を持ち合わせたプロジェクトマネージャー・ビジネスアドバイザ等による指導・助言、活動実績（育成従事実績）に応じた活動費提供を行います。従来の未踏事業とは異なり、年齢制限がなく、起業又は事業化に強い関心を持つ未踏的 IT 人材を対象としています。

2018 年度は、市場性、開発実現性、事業性を兼ね備えた IT を活用した革新的なアイディア・プロトタイプ（製品・サービスの企画・構想を練っている段階、製品・サービスのプロトタイプ開発を継続している段階）を有し、起業又は事業化に強い関心を持つ未踏的 IT 人材からプロジェクトを募集します。

また、本事業の公募に関する説明会を 3 月 14 日（水）に IPA（東京都文京区）で開催しました。当日は本事業に関する詳細な説明を行い、応募を目指す方に本事業の理解を深めていただきました。

「2018 年度未踏アドバンスト事業」公募の詳細については、次の URL をご覧ください。

https://www.ipa.go.jp/about/kobo/kobo20180308.html

https://www.ipa.go.jp/jinzai/advanced/2018/koubo_index.html

## 2.「セキュリティ・キャンプフォーラム 2018」を開催

（担当：イノベーション人材センター）

IPA は、3 月 16 日（金）にセキュリティ・キャンプ実施協議会と共同で「セキュリティ・キャンプフォーラム 2018」をフクラシア東京ステーション（東京都千代田区）で開催しました。

本フォーラムは、セキュリティ・キャンプ修了生の年度を超えた交流、産業界での認知度向上と活動支援を目的に、毎年開催しているものです。

当日の来場者数は、修了生やセキュリティ・キャンプ実施協議会の会員企業の方を中心に 71 名あり、セキュリティ・キャンプ実施協議会の会員企業や、セキュリティ・キャンプ事業の修了生からの講演などがありました。

「セキュリティ・キャンプフォーラム 2018」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/forum2018.html

## 3.「セキュリティ・ミニキャンプ in 四国 2017（徳島）」を開催

（担当：イノベーション人材センター）

IPA は、3 月 3 日（土）に国立大学法人徳島大学と共同で「セキュリティ・キャンプ in 四国 2017（徳島）」を開催しました。

徳島県でのセキュリティ・キャンプ地方大会の開催は初めてで、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 17 名）では、用意されたサーバに対してオープンソースのログ管理ソフトウェアを用いてログを収集し、過負荷の原因調査や可視化を学習する講義などが行われました。

「セキュリティ・ミニキャンプ in 四国 2017（徳島）」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/minicamp2018_tokushima.html

## 4.「日経 BP IoT Japan 関西 2018」への出展

（担当：イノベーション人材センター）

IPA は、3 月 8 日(木)～9 日(金)に開催された日経 BP 社主催の「IoT Japan 関西 2018」（会場：グランフロント大阪（大阪府大阪市））にて、「地方版 IoT 推進ラボ」の展示及びセミナーを実施しました。

近畿・中国・四国 6 地域（滋賀県、大阪府、大阪府大阪市、奈良県、広島県、徳島県美波町）が取組内容を展示し、3 地域（大阪府大阪市、奈良県、徳島県美波町）の代表者が新たな IoT ビジネスを創出するプロジェクトの成果や今後の可能性等についてパネル討論を行いました。

展示には多くの来場者があり、セミナー会場の参加者も定員を超え、盛況のうちに終了しました。

「地方版 IoT 推進ラボ」の「IoT Japan 2018」出展の詳細については、次の URL をご覧ください。

https://iotlab.jp/local/office-iot-6/

## ５．平成 30 年度春期「情報処理安全確保支援士（登録セキスペ）試験」及び「情報処理技術者試験」の応募者数について

（担当：情報処理技術者試験センター）

IPA は、3 月 9 日（金）に平成 30 年度春期「情報処理安全確保支援士（登録セキスペ）試験」及び「情報処理技術者試験」（所管：経済産業省、4 月 15 日（日）実施）の応募者数を公表しました。

■「情報処理安全確保支援士（登録セキスペ）試験」の応募者数について

平成 30 年度春期「情報処理安全確保支援士（登録セキスペ）試験」の応募者数は、以下のとおりです。

| | 今回の応募者数 | 前年同期応募者数 | 前年同期比 |
|---|---|---|---|
| 情報処理安全確保支援士（登録セキスペ）試験 | 23,180 | 25,130 | 92.2% |

■「情報処理技術者試験」の応募者数について

平成 30 年度春期「情報処理技術者試験」の応募者数は、前年同期比 101.8%の 186,380 人となりました。

なお、基本情報技術者試験は前年同期比 108.6%となり、応募者の属性別の内訳（アンケート結果の無記入を除く）は、社会人 108.6%、学生 102.0%でした。

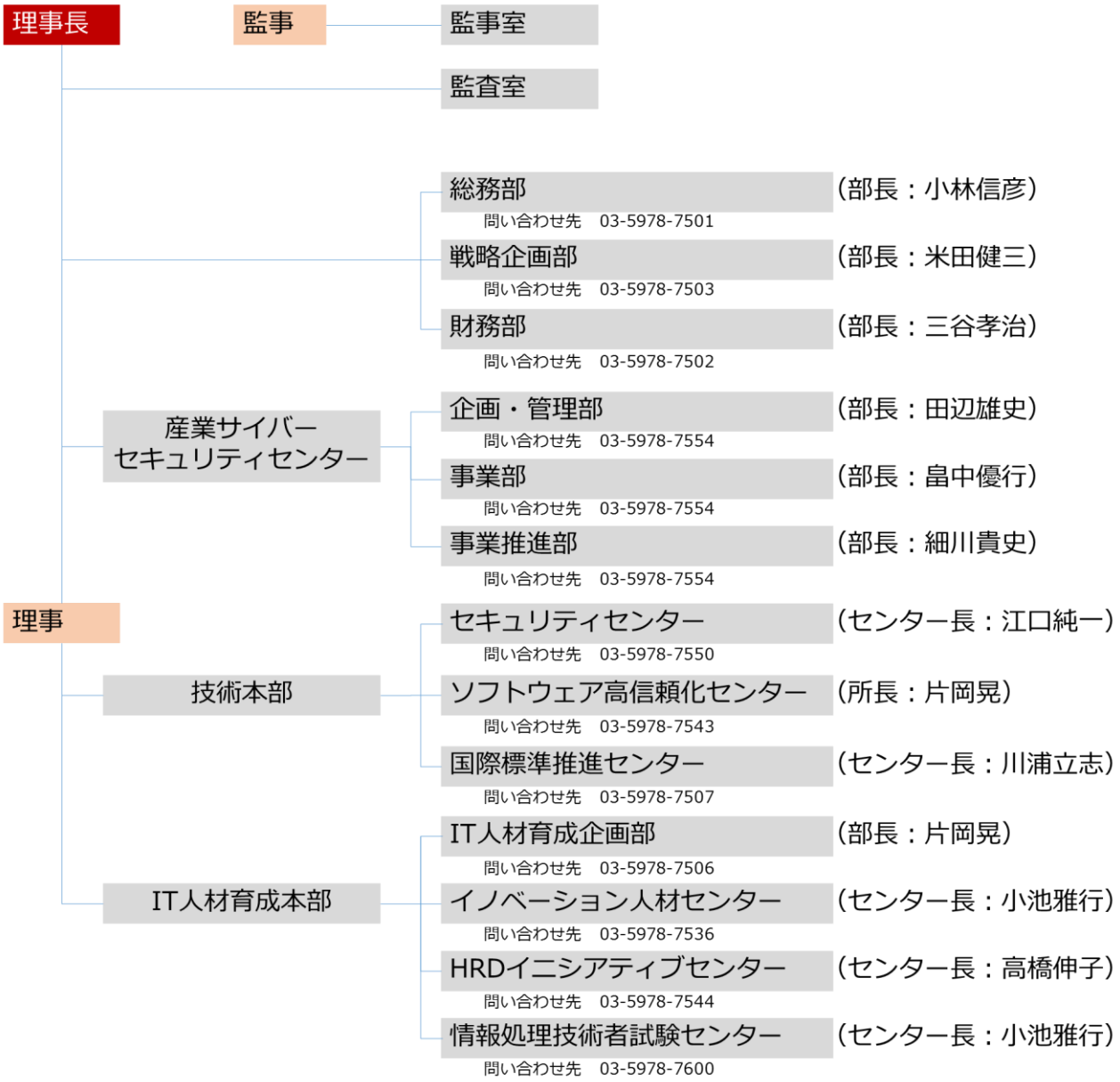
各試験区分の応募者数は、以下のとおりです。

| | 今回の応募者数 | 前年同期応募者数 | 前年同期比 |
|---|---|---|---|
| 情報処理技術者試験　合計 | 186,380 | 183,017 | 101.8% |
| 情報セキュリティマネジメント試験 | 19,300 | 21,162 | 91.2% |
| 基本情報技術者試験 | 73,581 | 67,784 | 108.6% |
| 応用情報技術者試験 | 49,223 | 49,333 | 99.8% |
| 高度試験　合計 | 44,276 | 44,738 | 99.0% |
| プロジェクトマネージャ試験 | 18,212 | 18,291 | 99.6% |
| データベーススペシャリスト試験 | 17,165 | 17,706 | 96.9% |
| エンベデッドシステムスペシャリスト試験 | 4,646 | 4,590 | 101.2% |
| システム監査技術者試験 | 4,253 | 4,151 | 102.5% |

応募者の詳しい統計については、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