

## <IPA 情報発信第 155 号の内容>

### 今月のトピックス

#### 1. 「CeBIT 2017」へ出展

日独首脳などが参加し、IoT/インダストリー4.0に関するサイバーセキュリティ等の日独協力の枠組みを定めた「ハノーバー宣言」がなされるなどした国際イベント「CeBIT 2017」に出展し、「つながる世界の開発指針」を始めとした安全・安心な IoT システム開発や IoT 人材育成に役立つコンテンツを紹介しました。

#### 2. 未踏事業スペシャルイベント「未踏会議 2017」を開催

未踏 IT 人材の起業・事業化を支援する「未踏会議 2017」を開催しました。シンポジウムでは、未踏 IT 人材がプレゼンやパネルディスカッションを行い、交流イベントの「未踏ナイト」では、世耕経済産業大臣が来場し、未踏事業の発展につながる力強いご挨拶をいただきました。

#### 3. 「企業における営業秘密管理に関する実態調査」報告書を公開

企業における営業秘密の漏えいや管理に係る対策状況について、実態の把握と傾向の分析を行い、報告書を公開しました。漏えいリスクを感じる社会動向変化の要因、様々な対策への取り組みが進んでいる企業に共通する要因などを明らかにしています。

#### 4. 大分県とサイバーセキュリティ対策等に関する連携協定を締結

今後 5 年間で、県内の情報セキュリティマネジメント試験合格者 1,000 人、情報処理安全確保支援士登録者 100 人の輩出を目標とする大分県と相互に連携協力することを目的に、広瀬大分県知事と連携協定の締結を行いました。都道府県レベルとこのような連携協定を締結したのは初めてです。

### I. 安全な IT 社会の実現

1. 「セキュリティ・キャンプフォーラム 2017」の開催
2. 「自動車の情報セキュリティへの取組みガイド」第 2 版を公開～製品のライフサイクル（製造工程、配送を含む）をカバーするセキュリティへの対応～
3. 「偽警告で、また新たな手口が出現」～パソコンが正常に操作できなくなったと錯覚させる多数の狡猾な細工～
4. 「2016 年度中小企業における情報セキュリティ対策の実態調査」を公開
5. 「情報セキュリティ 10 大脅威 2017」解説資料を公開
6. 「情報システム等の脆弱性情報の取扱いに関する研究会」2016 年度報告書を公開
7. 「情報セキュリティに関するサプライチェーンリスクマネジメント調査」報告書を公開
8. 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. 「International Conference on Software Testing, Verification and Validation 2017 (ICST2017)」へ出展
2. 「つながる世界の『利用時の品質』～IoT時代の安全と使いやすさを実現する設計～」を公開
3. 「経営者のためのシステムズエンジニアリング導入の薦め」を公開
4. 第10回要求シンポジウム「要求定義の今と未来 ～イノベーション/モダナイゼーション時代の要求定義のヒントを事例から探る～」を開催
5. 「はじめての STAMP/STPA (実践編) ～システム思考に基づく新しい安全性解析手法～」を公開
6. ソフトウェア開発データが語るメッセージ「設計レビュー・要件定義強化のススメ」を公開
7. 「大規模・複雑化した組込みシステムのための障害診断手法 ～ 事後 V&V の体系と要素技術 ～ 」を公開
8. 「障害未然防止のための設計知識の整理手法ガイドブック (組込みシステム編)」を公開
9. 「情報処理システム高信頼化教訓集 (IT サービス編) 2016 年度版」を公開
10. 「先進的な設計・検証技術の適用事例報告書 2016 年度版」を公開
11. 「第10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」を公開
12. 「コア語彙 バージョン 2.4」を公開
13. 「SEC journal」第48号を発行

## 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. アジア共通統一試験推進コア人材育成事業「Top Gun プログラム」を実施
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」の応募者数について

## 今月のトピックス

### 1. 「CeBIT 2017」へ出展

(担当：ソフトウェア高信頼化センター、HRD イニシアティブセンター)

IPA は、3月20日(月)～3月24日(金)までハノーバー国際見本市会場にて開催された「国際情報通信技術見本市 (CeBIT 2017)」に出展しました。

本イベントは、ドイツメッセ社の主催による、IoT、ビッグデータ、クラウド、セキュリティなど、IT ビジネスに特化した専門展示会で、毎年70ヶ国から約3,000社が出展し、100ヶ国から約200,000名が参加しています。本年は、日独首脳が参加したほか、高市総務大臣及び世耕経済産業大臣とドイツのツィプリス経済エネルギー大臣との間で、IoT/インダストリー4.0に関するサイバーセキュリティ、国際標準化、研究開発分野等での日独協力の枠組みを定めた「ハノーバー宣言」に署名がされました。

IPA は、「つながる世界の開発指針<sup>1</sup>」、「組込みソフトウェア向けコーディング作法ガイド (ESCR)<sup>2</sup>」、「はじめての STAMP/STPA<sup>3</sup>」、「i コンピテンシディクショナリ<sup>4</sup>」といった安全・安心な IoT システムの開発や IoT 時代を担う人材育成に役立つコンテンツを紹介しました。

当日、ブース来場者からは「英語版の資料があるのはありがたい」「IoT セキュリティガイドラインに関心がある」「欧州支社での人材育成に活用したい」といったご意見をいただきました。

IPA は、これらのご意見を基に今後も IoT の信頼性向上や人材育成に関する国際的な情報発信を強化してまいります。

「CeBIT 2017」の詳細については、次の URL をご覧ください。

---

<sup>1</sup> IPA が 2016 年 3 月に公開した、自動車や家電等のさまざまなモノがインターネットを通じて相互に接続する「IoT 社会」におけるセーフティ・セキュリティ等のリスクに対処するための業界横断的な開発指針。

日本語版：<http://www.ipa.go.jp/sec/reports/20160324.html>

英語版：<http://www.ipa.go.jp/english/sec/reports/20160729-02.html>

<sup>2</sup> 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。

日本語版：<http://www.ipa.go.jp/sec/reports/20161018.html>、<http://www.ipa.go.jp/sec/reports/20140307.html>

英語版：[http://www.ipa.go.jp/english/sec/quality\\_assurance/esxr.html](http://www.ipa.go.jp/english/sec/quality_assurance/esxr.html)

<sup>3</sup> 大規模で複雑なシステムの事故のリスクやセキュリティ上の脆弱性を効率的に漏れなく見つけるための安全性解析手法 STAMP/STPA について、踏切システムを題材に解説した入門書

(<http://www.ipa.go.jp/sec/reports/20160428.html>)。なお、STAMP(System Theoretic Accident Model and Processes)とは、マサチューセッツ工科大学(MIT)の Nancy G. Leveson 教授が、文献“Engineering a Safer World”(2012 年)の中で提唱したシステム理論に基づく事故モデル。STPA(System Theoretic Process Analysis)とは、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。

<sup>4</sup> 企業において IT を利活用するビジネスに求められる業務(タスク)と、それを支える IT 人材の能力や素養(スキル)を「タスクディクショナリ」、「スキルディクショナリ」として体系化したもの。

日本語版：[http://www.ipa.go.jp/jinzai/hrd/i\\_competency\\_dictionary/icd.html](http://www.ipa.go.jp/jinzai/hrd/i_competency_dictionary/icd.html)

英語版：<http://www.ipa.go.jp/english/humandev/icd.html>

ドイツメッセ日本代表部：<http://www.jma.or.jp/dms/search/detail/4>

公式サイト（英語ページ）：<http://www.cebit.de/en/>

## 2. 未踏事業スペシャルイベント「未踏会議 2017」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 2017」を3月10日（金）にアクトスクエア（東京都渋谷区）で開催しました。

3回目となる今回は、「加速するITの、その先へ。」をキャッチフレーズに、様々なフィールドで活躍している未踏IT人材の考え・想いや、具体的な活動内容を紹介することで、彼らの産業界等における活用が促進され、更なる活躍のフィールドが広がることを目的に行いました。

「第一部 未踏会議（シンポジウム）」では、起業・事業化を進める方を含む未踏IT人材6名がショートプレゼンテーション及び「日本からAppleやGoogleは生まれるか？」「日本に未来はあるか？」をテーマにパネルディスカッションを行いました。

「第二部 未踏ナイト（交流イベント）」では、冒頭に世耕経済産業大臣から未踏事業の発展につながる力強いご発言を含むご挨拶を頂戴した後、未踏IT人材が自身の研究成果や事業について紹介する招待プレゼンテーションを実施しました。また、未踏IT人材や、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の方等を対象とした懇親会を行いました。

当日は、未踏会議、未踏ナイト合わせて、延べ200名程度の方々に参加いただき、ニコニコ生放送では約1万5千アクセスもの視聴をいただきました。また、参加された方のアンケートでは、「未踏IT人材を“起業環境”につなぐことが極めて重要」や、「AI、ビッグデータ、IoTの海外の人材と未踏の人材とのやり取りを聞きたい」など、未踏IT人材への期待を感じられるコメントが多数寄せられました。

「未踏会議 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/mitou/2016/mitoukaigi2017.html>

<http://www.ipa.go.jp/jinzai/mitou/mitoukaigi/2017/>

## 3. 「企業における営業秘密管理に関する実態調査」報告書を公開

（担当：セキュリティセンター）

IPAは、企業における営業秘密の漏えいや管理に係る対策状況について調査し、実態の把握と傾向の分析を行い、3月17日（金）に調査報告書を公開しま

した。

営業秘密漏えい事案は、報道等で明らかになった大きな事件のみならず、様々な業種・規模の企業で発生しており、その漏えいのルート・手段も多様であることから企業側も対策に苦慮している状況です。

企業における営業秘密の管理実態については、経済産業省が2012年度に「人材を通じた技術流出に関する調査研究」で調査していますが、IPAは、その後の法改正や社会動向変化等を踏まえ、アンケート調査、インタビュー調査及び判例調査を通じて実態の把握を行い、次のような分析を行いました。

- ・漏えいリスクを感じる社会動向変化の上位3項目は、「標的型攻撃の増加」、「スマートフォン・タブレット機器等の急速な普及」、「データの活用機会の増加」。
- ・情報区分がしっかりとできている企業ほど、具体的な漏えい対策に関する取り組みも進んでいる。
- ・漏えい検知活動を実施している企業の方が、様々な対策への取り組みが進んでいる他、漏えい行為を行った者への処罰・法的対応ができている。

「企業における営業秘密管理に関する実態調査」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/fy28/reports/ts\\_kanri/index.html](https://www.ipa.go.jp/security/fy28/reports/ts_kanri/index.html)

#### 4. 大分県とサイバーセキュリティ対策等に関する連携協定を締結

(担当：戦略企画部)

IPAは、大分県（知事：広瀬 勝貞）とサイバーセキュリティ対策などに関する連携協定を3月27日（月）に締結しました。IPAとして、都道府県レベルとこのような連携協定は初めてのものとなります。

大分県では、「ラグビーワールドカップ2019」を控え、県内の情報分野の安全・安心の向上を図り、地域の活性化に取り組むことにより、「情報セキュリティ先進県」を目指しています。また、今後5年間で、県内の情報セキュリティマネジメント試験合格者1,000人、情報処理安全確保支援士登録者100人の輩出を目標としています。

これを受けて、IPAと大分県は、共に公的機関としてその保有する経験と知見等に基づいて可能な限り、相互に連携協力することを目的に、IPAで両トップによる連携協定の締結式を行いました。

「大分県とサイバーセキュリティ対策等に関する連携協定を締結」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/20170327.html>

## I. 安全な IT 社会の実現

### 1. 「セキュリティ・キャンプフォーラム 2017」の開催

(担当：イノベーション人材センター)

IPA は、セキュリティ・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 2017」を 3 月 17 日（金）に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躍支援を目的に、毎年開催しているものです。

当日は、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 83 名が来場し、基調講演では東京工業大学の首藤一幸准教授より、セキュリティ技術者が目指すべきキャリアについて講演いただきました。また、修了生より、セキュリティ・キャンプ修了後の技術的な活動状況について講演いただきました。

「セキュリティ・キャンプフォーラム 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/2016/forum2017.html>

### 2. 「自動車の情報セキュリティへの取組みガイド」第 2 版を公開～製品のライフサイクル（製造工程、配送を含む）をカバーするセキュリティへの対応～

(担当：セキュリティセンター)

IPA は、自動車製品のライフサイクル（企画、開発、運用、廃棄）の各フェーズにおけるセキュリティに対する取組みの考え方を解説する「自動車の情報セキュリティへの取組みガイド」第 2 版を 3 月 23 日（木）に公開しました。

現在、様々な安全機能の実用化やネットと接続した高付加価値なサービスの提供が実現されるようになってきています。一方で、自動車に対するサイバー攻撃の手法の検討が数多く行われ、脆弱性が公表されたことにより製品リコールにつながるなど、セキュリティ上の問題やそれらへの取組みなども大きく取り上げられるようになってきています。

この度の改訂にあたっては、第 1 版では触れられなかった、開発時の製造工程における脅威への対応や、所有者や利用者に製品が届けられるまでの運送工程におけるセキュリティの確保に関する項目を加筆しています。

IPA は、自動車業界において、セーフティに加え、セキュリティ面でもより品質の高い製品が消費者に提供されることを期待します。

「自動車の情報セキュリティへの取組みガイド」第 2 版の詳細については、次の URL をご覧ください。

### 3. 「偽警告で、また新たな手口が出現」～パソコンが正常に操作できなくなったと錯覚させる多数の狡猾な細工～

(担当：セキュリティセンター)

IPAは、マウスのポインターが勝手に動いているようなアニメーションやマイクロソフトのURLにアクセスしているようなアドレスバーの画像を表示させるといった、偽警告の新たな手口を確認し、3月29日（水）に公表しました。

去る1月には、マイクロソフト社のウェブサイトと酷似した画面上に警告メッセージを表示させ、同社を騙って電話に誘導するという手口が確認されており、続々と新たな手口が出現しているといえます。

今後も、異なる画面やメッセージを表示させ、電話に誘導する手口が巧妙に変化していくことが予想されます。

そのため、インターネット利用中に“ウイルスに感染”“個人情報の流出”などといった警告メッセージと共に電話番号が表示された際には、その電話番号に電話はせずに、IPAなどの公的機関の相談窓口にご相談することをおすすめします。

「偽警告で、また新たな手口が出現」の詳細については、次のURLをご覧ください。

<http://www.ipa.go.jp/security/anshin/mgdayori20170329.html>

### 4. 「2016年度中小企業における情報セキュリティ対策の実態調査」を公開

(担当：セキュリティセンター)

IPAは、中小企業、とりわけ小規模企業者における情報セキュリティ対策の実情を把握するため、経営者・IT担当者・従業員を対象とした調査を実施し、分析結果を3月30日（木）に公表しました。

結果を見ると、規模が小さい企業ほど情報セキュリティ対策の不備が浮き彫りとなりました。今回の調査結果の主なポイントは以下のとおりです。

- (1) 情報漏えい等のインシデント又はその兆候を発見した場合の対応方法を規定しているのは、小規模企業では13.7%。

また、セキュリティポリシーの文書化を実施している小規模企業の割合は8.2%であり、中小企業（100人以下：17.8%、101人以上：46.6%）に比べて実施率が低い傾向。

- (2) 社内の情報セキュリティに関するルールから逸脱した場合の措置につい

て、就業規則等で規定していると回答した企業の割合は、小規模企業では 17.6%、100 人以下の中小企業では 38.1%、101 人以上の中小企業では 61.3%となっており、企業規模による差が顕著。

「2016 年度中小企業における情報セキュリティ対策の実態調査」の詳細については、次の URL をご覧ください。

<https://www.ipa.go.jp/security/fy28/reports/sme/>

## 5. 「情報セキュリティ 10 大脅威 2017」解説資料を公開

(担当：セキュリティセンター)

IPA は、「情報セキュリティ 10 大脅威 2017」<sup>5</sup>の解説を記載した資料を 3 月 30 日（木）に公表しました。

本資料は、下記の 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 スマートフォン編
- 第 2 章 情報セキュリティ 10 大脅威 2017
- 第 3 章 注目すべき脅威や懸念

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 2017」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/10threats2017.html>

## 6. 「情報システム等の脆弱性情報の取扱いに関する研究会」2016 年度報告書を公開

(担当：セキュリティセンター)

IPA は、「情報システム等の脆弱性情報の取扱いに関する研究会」の活動として報告書をまとめ、3 月 30 日（木）に公開しました。

昨年度の「情報システム等の脆弱性情報の取扱いに関する研究会」（座長：土居 範久慶應義塾大学名誉教授）でとりまとめた「新たな情報セキュリティ早期警戒パートナーシップの基本構想」のロードマップに沿って、今年度は以下の

---

<sup>5</sup> 2016 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、決定したものの。



事項を検討しました。また、これらを踏まえた情報セキュリティ早期警戒パートナーシップガイドラインの改訂などに取り組みました。

- ・「重要インフラ事業者への優先情報提供の実現に向けた検討」
- ・「脆弱性情報の取扱い判断基準と取扱いルールの方策に関する検討」
- ・「ソフトウェア開発者やウェブサイト運営者による脆弱性対応」
- ・「調整不能案件公表」
- ・「EoL 製品の脆弱性」
- ・「IoT の脆弱性」
- ・新たな課題である「フルディスクロージャ型の脆弱性公表サイト」や「現行パートナーシップ改善」

IPA は、これらの調査報告書が有効利用され、ソフトウェアの脆弱性対策の普及が進むことを期待しています。

「情報システム等の脆弱性情報の取扱いに関する研究会」2016 年度報告書の詳細については、次の URL をご覧ください。

[http://www.ipa.go.jp/security/fy28/reports/vuln\\_handling/index.html](http://www.ipa.go.jp/security/fy28/reports/vuln_handling/index.html)

## 7. 「情報セキュリティに関するサプライチェーンリスクマネジメント調査」報告書を公開

(担当：セキュリティセンター)

IPA は、サプライチェーンにおける情報セキュリティリスクマネジメントの取組みへの課題を整理するための調査を実施し、結果を 3 月 30 日（木）に公表しました。

今日、IT システムや提供する製品・サービスにおいて、設計・開発・製造、及び運用・保守・廃棄に至るまでのプロセス（サプライチェーン）の一部を外部委託することは一般的となっていますが、系列企業やビジネスパートナー等の外部委託者が関与するサプライチェーンにおける情報セキュリティリスクの把握やマネジメントは容易ではありません。

今回の調査の概要及び主なポイントは以下の通りです。

- (1) 委託元にとって、委託が連鎖するほど情報セキュリティ対策状況の把握は困難になる。
- (2) 大企業は、委託先に求める情報セキュリティについて「統一されたルール」を策定する傾向にある。
- (3) 中小企業は大企業よりも「委託先における情報セキュリティ管理の確認頻度が低い」傾向にある。

「情報セキュリティに関するサプライチェーンリスクマネジメント調査」報告書の詳細については、次の URL をご覧ください。

<http://www.ipa.go.jp/security/fy28/reports/scrm/index.html>

## 8. 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対象に「重要なセキュリティ情報<sup>6</sup>」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 月より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

3 月は、「緊急」4 件、「注意」1 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. 「International Conference on Software Testing, Verification and Validation 2017 (ICST2017)」へ出展

（担当：ソフトウェア高信頼化センター）

IPA は、3 月 13 日（月）～3 月 17 日（金）、早稲田大学西早稲田キャンパス（東京都新宿区）にて開催された「International Conference on Software Testing, Verification and Validation 2017 (ICST2017)」に出展しました。

本イベントは、米国電気電子学会（IEEE）、特定非営利活動法人ソフトウェアテスト技術振興協会、早稲田大学の共催による、ソフトウェアテストに関する

---

<sup>6</sup> 「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。

国際会議です。

IPA は会期中、「つながる世界の開発指針」および「i コンピテンシディクシヨナリ」を紹介するポスター展示を行いました。また、IPA 理事長より「Aiming to Realize a “Reliable IT Society”」、技術本部ソフトウェア高信頼化センター所長より「Systematic Approach toward Dependable System Development」という 2 つの講演を行いました。聴講された方からは「IoT のガイドラインを製品開発時の検証方針の参考としたい」といったご意見をいただきました。

IPA は、今後も IoT の信頼性向上や人材育成に関する国際的な情報発信を強化してまいります。

「International Conference on Software Testing, Verification and Validation 2017 (ICST2017)」の詳細については、次の URL をご覧ください。

<http://aster.or.jp/conference/icst2017/japanese/>

## 2. 「つながる世界の『利用時の品質』～IoT 時代の安全と使いやすさを実現する設計～」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 (木)、さまざまなモノ同士がつながる IoT (Internet of Things) 時代に向けて、利用者の特性や利用状況を考慮して IoT デバイス/サービスを開発するポイントを紹介した報告書、「つながる世界の『利用時の品質』～IoT 時代の安全と使いやすさを実現する設計～」を公開しました。

本報告書には、今後の IoT 時代でつながっていくことが予想される家電・自動車・モバイル製品などを対象に、「利用時の品質」を考慮しなかったために発生した失敗事例および利用者目線で開発できたことによる成功事例を合わせて 26 件収録しています。さらに、事例の分析から利用時の品質向上に必要な 15 個の視点を抽出し、それぞれの視点において開発時に注意すべき点を解説しています。

IPA は、本報告書がマーケティングやデザインなどの担当者とソフトウェア開発者の意識合わせのために利用され、あらゆる利用者が安心して製品やサービスを利用できる環境作りに貢献できることを期待しています。

「つながる世界の『利用時の品質』～IoT 時代の安全と使いやすさを実現する設計～」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/20170330.html>

### 3. 「経営者のためのシステムズエンジニアリング導入の薦め」を公開

(担当：ソフトウェア高信頼化センター)

IPA は、IoT 時代の複雑なシステムの企画や品質の確保に有効とされている「システムズエンジニアリング」の普及を目的に「経営者のためのシステムズエンジニアリング導入の薦め」を3月29日(水)に公開しました。

本資料では、「鉄道・列車制御システムの更新とサービス継続」、「次世代静脈注入ポンプの開発」などの5件の事例の分析を通してシステムズエンジニアリングの有効性や利用可能な場面を紹介しています。

IPA は、本資料が、企業のシステム開発へのシステムズエンジニアリング導入のきっかけとなり、IoT 時代のシステム開発に関わる様々な問題の解決に貢献することを期待しています。

「経営者のためのシステムズエンジニアリング導入の薦め」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/20170329.html>

### 4. 第10回要求シンポジウム「要求定義の今と未来 ～イノベーション/モダナイゼーション時代の要求定義のヒントを事例から探る～」を開催

(担当：ソフトウェア高信頼化センター)

IPA は、3月10日(金)にNTT DATA 駒場研修センター(東京都目黒区)にて第10回要求シンポジウム「要求定義の今と未来 ～イノベーション/モダナイゼーション時代の要求定義のヒントを事例から探る～」を株式会社NTT データ、富士通株式会社と共同で開催しました。

本シンポジウムでは、IT システム開発における企画や要求定義<sup>7</sup>といった上流工程強化のための IPA の取り組みを紹介しました。また、IT システムを企画・調達するユーザ企業の方々の上流工程に関する課題認識と取り組みについて発表いただきました。当日は約260名の方にご参加いただき、参加者からは「イノベーションに関する講演は大変刺激になりました」、「事例は生の内容であり身近でわかりやすく、ためになります」といったご意見をいただきました。

IPA では、これらのご意見を基に、今後も上流工程の強化による IT システムの信頼性向上の取り組みを継続していきます。

「第10回要求シンポジウム」の詳細については、次の URL をご覧ください。

<http://sec.ipa.go.jp/seminar/20170310.html>

---

<sup>7</sup> IT システムの利用者が求める機能、性能、安全性、セキュリティ等の条件を漏れなく文書化すること。

## 5. 「はじめての STAMP/STPA（実践編）～システム思考に基づく新しい安全性解析手法～」を公開

（担当：ソフトウェア高信頼化センター）

IPA は、IoT のような複雑なシステムのハザード分析手法である STAMP/STPA を現場で実践するための手引書「はじめての STAMP/STPA（実践編）～システム思考に基づく新しい安全性解析手法～」を 3 月 24 日（金）に公開しました。

本書では、STAMP/STPA の活用事例として、分析が難しいと思われる踏切の「とりこ<sup>8</sup>」検知事例、人や組織が直接的な分析対象となる工事事例、安全設計に馴染まないと思われがちなインターネット通販システム事例などを取り上げ、分析において行った工夫や、新たに発見された効果などを紹介しています。

IPA は、本書がシステムの安全性確保の責務を負うシステム開発者、ソフトウェア開発者の間で利用され、幅広いシステムの安全性が向上することを期待しています。

「はじめての STAMP/STPA（実践編）～システム思考に基づく新しい安全性解析手法～」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/20170324.html>

## 6. ソフトウェア開発データが語るメッセージ「設計レビュー・要件定義強化のススメ」を公開

（担当：ソフトウェア高信頼化センター）

IPA は、保有する 4,067 件のソフトウェア開発プロジェクトデータを分析した結果を、「ソフトウェア開発データが語るメッセージ「設計レビュー・要件定義強化のススメ」」として 3 月 31 日（金）に公開しました。

本書では、「上流工程の不具合摘出比率を高めることで、信頼性向上が期待できる」ことと、「要件定義を強化することによって、信頼性向上が期待できる」ことを定量的に示しています。IPA は、上流工程の不具合摘出作業（設計レビューなど）や要件定義にかかる時間とコストを増やすよう、ソフトウェア開発企業の経営者や現場の責任者へ働きかけるための根拠資料として本書が使われることを想定しています。

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「設計レビュー・要件定義強化

---

<sup>8</sup> 踏切の遮断機が下りた際、何らかの理由で線路上に人や自動車を取り残されてしまうこと。

のススメ」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/20170331.html>

## 7. 「大規模・複雑化した組込みシステムのための障害診断手法 ～ 事後 V&V の体系と要素技術 ～」を公開

(担当：ソフトウェア高信頼化センター)

IPA は、大規模で複雑な組込みシステムの障害原因究明と再発防止に有効な手法である事後 V&V<sup>9</sup>の普及を目的に「大規模・複雑化した組込みシステムのための障害診断手法 ～ 事後 V&V の体系と要素技術 ～」を 3 月 21 日（火）に公開しました。

本書では、事後 V&V に利用できる STAMP/STPA などの分析手法を、化学プラントシミュレーターなどの具体的なシステムの分析例を通して紹介しています。

IPA は、本書の普及を通して、組込みシステムの障害防止に貢献していくとともに、今後はセキュリティ侵害の検出や機能間のつながりが動的に変化する IoT システムの障害追跡にも対応できるよう、障害原因診断手法の発展に努めてまいります。

「大規模・複雑化した組込みシステムのための障害診断手法 ～ 事後 V&V の体系と要素技術 ～」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/20170321\\_2.html](http://www.ipa.go.jp/sec/reports/20170321_2.html)

## 8. 「障害未然防止のための設計知識の整理手法ガイドブック（組込みシステム編）」を公開

(担当：ソフトウェア高信頼化センター)

IPA は、組込みシステムを開発・運用する企業が保有する「過去トラ DB（過去トラブルデータベース）」を活用するための「障害未然防止のための設計知識の整理手法ガイドブック（組込みシステム編）」を 3 月 21 日（火）に公開しました。

本ガイドブックでは、ベテラン技術者の経験やノウハウが埋蔵された「過去トラ DB」の障害情報記録から抽出した「設計知識<sup>10</sup>」を構造化・一般化し、検索のための分類タグを設定する手順を紹介しています。

IPA は、本書の普及を通して、今後、新たに開発される組込みシステムの設計段階から障害リスクが低減されていくことを期待しています。

<sup>9</sup> 設計段階で考慮漏れやミスを防ぐために用いられる「検証と妥当性確認 (V&V: Verification and Validation)」と同じ考え方で、障害発生後に原因究明を行う手法。

<sup>10</sup> 障害を未然防止するための対策をシステムの設計に反映するための知識。

「障害未然防止のための設計知識の整理手法ガイドブック（組込みシステム編）」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/20170321\\_1.html](http://www.ipa.go.jp/sec/reports/20170321_1.html)

## 9. 「情報処理システム高信頼化教訓集（IT サービス編）2016 年度版」を公開 （担当：ソフトウェア高信頼化センター）

IPA は、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）2016 年度版」を 3 月 27 日（月）に公開しました。

本教訓集は、2015 年 3 月に公開した同教訓集 2015 年度版の内容を拡充したもので、今年度は新たに 6 件の教訓を追加し、今年度発生した障害の原因として目立っていた「ヒューマンエラー」と「システムの高負荷／過負荷」に着目した対策についても解説しています。

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。

「情報処理システム高信頼化教訓集（IT サービス編）2016 年度版」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/20170327.html>

## 10. 「先進的な設計・検証技術の適用事例報告書 2016 年度版」を公開 （担当：ソフトウェア高信頼化センター）

IPA は、「先進的な設計・検証技術の適用事例報告書」に、新たに 19 件の事例を 3 月 2 日（木）に追加しました。

本報告書は、複雑化・高度化するシステムを迅速、かつ高信頼に開発するための先進的な「設計・検証手法」を開発現場で実践した成功事例（ベストプラクティス）を集めたものです。

IPA は、今後も実用性の高い技術情報を継続して収集し、広く一般へ提供することにより、先進的な技術・手法を導入する開発現場において、自社の状況と事例を比較するなど、本報告書を「参考書」として活用いただき、利用者にとって信頼性の高いソフトウェア開発につながることを期待しています。

「先進的な設計・検証技術の適用事例報告書 2016 年度版」の詳細については、次の URL をご覧ください。

## 1 1. 「第 10 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」を公開

(担当：国際標準推進センター)

IPA は、「第 10 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、調査結果を 3 月 31 日（金）に公開しました。

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、昨年度から、閣議決定「世界最先端 IT 国家創造宣言<sup>11</sup>」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。

本調査結果には、IPA が進めている「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状況など、地方自治体の IT 化推進のヒントが多く含まれています。

IPA は、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ています。

本調査の詳細については、次の URL をご覧ください。

<http://www.ipa.go.jp/osc/research/jichitai.html>

## 1 2. 「コア語彙 バージョン 2.4」を公開

(担当：国際標準推進センター)

IPA は、共通語彙基盤「コア語彙 バージョン 2.4」を 3 月 31 日（金）に公開しました。

「コア語彙」は、共通語彙基盤の基礎をなすもので、氏名、住所、組織等、あらゆる社会活動で共通的に使用される中核的な用語の集合です。多くのシステム間で情報交換のための基礎となる語彙で、データ交換、オープンデータの二次利用等の効率化に役立つものであり、継続して見直しを行っています。

今回の見直しは、データ表現の容易性や汎用性の向上のため、「サービス型」、「制限型」などのクラス用語を新たに導入するとともに、語彙全体の構造を見直し、「参照」といった項目を、多くのクラスで共通に使えるようにしました。

なお、公開後に一定の周知期間を経た後、上位互換性のある本バージョンと旧版との入れ替えを行うこととしています。

<sup>11</sup> 2013 年 6 月 14 日閣議決定、2015 年 6 月 30 日改訂「世界最先端 IT 国家創造宣言」(内閣官房 IT 総合戦略室)  
(<https://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20150630/siryou1.pdf>)



「コア語彙 バージョン 2.4」の詳細については、次の URL をご覧ください。

<https://imi.go.jp/core/240/>

### 1.3. 「SEC journal」第 48 号を発行

(担当：ソフトウェア高信頼化センター)

IPA は、「SEC journal」第 48 号を 3 月 1 日（水）に発行しました。

「SEC journal」は、2005 年 1 月に創刊号発行以来、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 48 号の主な掲載記事は、以下のとおりです。

- ・ 所長対談：IoT 時代におけるシステムズエンジニアリングの重要性  
ドイツ フラウンホーファー研究機構 実験的ソフトウェア工学研究所（IESE） イェンス・ハイドリッヒ氏、マーティン・ベッカー氏
- ・ 論文：自動運転車を取り巻く System of Systems の安全性要求の妥当性確認と検証
- ・ 特集：システムズエンジニアリング
- ・ 解説：GQM+Strategies による組織目標と戦略の整合化及び目標定量管理の実践と拡張-SEC WG 及び早稲田大学ゴール指向経営研究会の活動より-
- ・ 連載：情報システムの障害状況 2016 年後半データ

「SEC journal」の詳細については、次の URL をご覧ください。

<http://www.ipa.go.jp/sec/secjournal/index.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. アジア共通統一試験推進コア人材育成事業「Top Gun プログラム」を実施

(担当：IT 人材育成企画部)

IPA は 2 月 20 日から 3 月 1 日までの 10 日間、アジア共通統一試験（ITPEC 試験）のトップ合格者など 14 名を招聘し「Top Gun プログラム」を実施しました。

「Top Gun プログラム」は、アジア各国の優秀な人材が日本の IT 企業などで

のワークショップ参加を通じ、日本の IT 企業特有の商慣習、開発現場の課題及び解決法などを学ぶとともに、日本企業との交流を図りました。本プログラムは、ITPEC 試験における特に優秀な人材を、同試験のさらなる発展に向けた推進リーダーとして育成するとともに、ITPEC 各国の試験実施機関と日本の IT 企業との連携体制構築などに係る協力者や推進役として育成することを目的としています。

プログラム最終日には、IPA 理事長より「ITPEC アンバサダー」の任命証及び徽章が授与されました。

本事業を通じて ITPEC 試験合格者、ITPEC 試験実施機関及び我が国 IT 企業との連携が進むことを期待します。

## 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」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、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、4 月 16 日（日）実施）の応募者数を 3 月 13 日（月）に公表しました。

### (1) 「情報処理安全確保支援士（登録セキスペ）試験」

平成 29 年度春期試験から開始する「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、25,130 人となりました。

### (2) 「情報処理技術者試験」

平成 29 年度春期「情報処理技術者試験」の応募者数は、前年同期比 110.9%<sup>12</sup>の 183,017 人<sup>13</sup>となりました。

各試験区分の応募者数は、基本情報技術者試験、応用情報技術者試験、高度試験の合計それぞれが、いずれも前年同期比 110%を超える増加となり、特に、高度試験のうち、「データベーススペシャリスト試験」の応募者数が前年同期比 126.7%と大幅に増加しました。また、「情報セキュリティマネジメント試験」は 21,162 人と、平成 28 年度春期の試験開始以来 3 期連続で 2 万人以上の受験申込みがありました。

各試験区分の応募者数は、以下のとおりです。

<sup>12</sup> 旧試験区分である「情報セキュリティスペシャリスト試験」を除く。

<sup>13</sup> 平成 28 年度春期試験 平成 28 年熊本地震での試験中止等の措置として、平成 29 年度春期試験を振替で受験する方を含む。( [http://www.jitec.ipa.go.jp/1\\_00topic/topic\\_20160509.html](http://www.jitec.ipa.go.jp/1_00topic/topic_20160509.html) )

	今回 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（旧試験区分を除く合計）	183,017	165,067	110.9%
情報セキュリティマネジメント試験	21,162	21,691	97.6%
基本情報技術者試験	67,784	61,281	110.6%
応用情報技術者試験	49,333	44,102	111.9%
高度試験（旧試験区分を除く合計）	44,738	37,993	117.8%
プロジェクトマネージャ試験	18,291	16,173	113.1%
データベーススペシャリスト試験	17,706	13,980	126.7%
エンベデッドシステムスペシャリスト試験	4,590	4,205	109.2%
システム監査技術者試験	4,151	3,635	114.2%
【旧】情報セキュリティスペシャリスト試験	-	26,864	-

「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」の応募者の詳細については、次の URL をご覧ください。

[http://www.jitec.ipa.go.jp/1\\_07toukei/\\_index\\_toukei.html](http://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 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