

# 独立行政法人情報処理推進機構 平成28年度計画

独立行政法人  
情報処理推進機構

# 目次

I. 国民に対して提供するサービスその他業務の質の向上に関する目標を達成するためとるべき措置.....	2
1. 新たな脅威への迅速な対応等の情報セキュリティ対策の強化～誰もが安全なITを安心して利用できる 経済社会のための情報セキュリティ基盤の確立を目指して～.....	2
1-1. 平成28年度における重点事項.....	2
1-2. 着実に取り組む事項.....	3
2. 社会全体を支える情報処理システムの信頼性向上に向けた取組の推進～重要インフラ分野等にお ける情報処理システムの信頼性・安全性の向上～.....	8
2-1. 平成28年度における重点事項.....	8
2-2. 着実に取り組む事項.....	9
3. IT人材育成の戦略的推進～若い突出したIT人材の発掘・育成及び高度IT人材育成の体系・客観的な能 力基準の普及等～.....	12
3-1. 平成28年度における重点事項.....	12
3-2. 着実に取り組む事項.....	13
II. 業務運営の効率化に関する目標を達成するためとるべき措置.....	16
III. 財務内容の改善に関する目標を達成するためとるべき措置.....	19
IV. 予算(人件費見積もりを含む。)、収支計画及び資金計画.....	20
V. 短期借入金の限度額.....	20
VI. 重要な財産の譲渡・担保計画.....	20
VII. 不要財産又は不要財産となることが見込まれる財産がある場合には、当該財産の処分に関 する計画.....	21
VIII. 剰余金の使途.....	21
IX. その他主務省令で定める業務運営に関する事項.....	21
(別紙)	
別紙1 予算	
別紙2 収支計画	
別紙3 資金計画	

# 独立行政法人情報処理推進機構平成28年度計画

独立行政法人通則法第31条第1項に基づき、独立行政法人情報処理推進機構(以下、「機構」という。)の平成28年度の事業運営に関する計画を次のように定める。

## I. 国民に対して提供するサービスその他業務の質の向上に関する目標を達成するためとるべき措置

### 1. 新たな脅威への迅速な対応等の情報セキュリティ対策の強化～誰もが安全なITを安心して利用できる経済社会のための情報セキュリティ基盤の確立を目指して～

#### 1-1. 平成28年度における重点事項

##### (1) 独法等<sup>1</sup>に対するサイバー攻撃を監視するシステムの構築・保守運用

① 事業内容

NISC<sup>2</sup>の監督の下、独法等の情報システムの監視体制を構築し、政府機関全体としてのサイバーセキュリティの強化に資する。

② 成果指標

NISCの監督の下、独法等の情報システムの監視体制構築を行う。

##### (2) 情報セキュリティ監査の実施

① 事業内容

サイバーセキュリティ戦略本部からの委託に基づき、独法等の情報セキュリティ対策の実態把握と改善に資するため、助言型の情報セキュリティ監査を行う。

② 成果指標

サイバーセキュリティ戦略本部との委託契約に基づいて、独法等に対する情報セキュリティ監査を実施する。

##### (3) 重要インフラにおけるサイバーセキュリティ対策強化

① 事業内容

重要インフラ事業者の対策状況調査やサイバーセキュリティリスク分析等を通じて、重要インフラにおけるサイバーセキュリティ対策強化を推進する。

② 成果指標

経済産業省や重要インフラ産業を所管する省庁と協議のうえ選定した3業界4事業者に対して実施する。

##### (4) 中小企業向けのサイバーセキュリティ対策強化

① 事業内容

中小企業における情報セキュリティ対策の自発的な取り組みを促すため、全国に会員企業を有する中小企業関連団体と一体となり情報セキュリティ対策を呼びかける「共同宣言」を行う。

<sup>1</sup> 独立行政法人及びサイバーセキュリティ戦略本部が指定する特殊法人等

<sup>2</sup> National center of Incident readiness and Strategy for Cybersecurity (内閣サイバーセキュリティセンター)

## ② 成果指標

商工三団体<sup>3</sup>を含む中小企業関連団体と共同宣言を行う。

## 1-2. 着実に取り組む事項

### (1)あらゆるデバイス、システムを対象としたサイバー攻撃等に関する情報の収集、分析、提供、共有

#### (1-1)ウイルス等の脅威への対応

- ① 急速に変化しつつある脅威を的確に把握し、ウイルスや不正アクセス等の情報を積極的に収集・分析し、広く国民一般に対し、傾向や対策等の情報提供を行う。
  - a. 経済産業省の告示に基づき、コンピュータウイルス及び不正アクセス被害の届出受付を行いつつ、定期的に受付状況を公表する。
  - b. スマートデバイスやパソコンに関するウイルスや不正アクセス等の解析・検証環境を整備するとともに、情報の収集、現象の分析及びノウハウの蓄積、情報発信活動を行う。
- ② ユーザからの相談・問い合わせ対応については、自動応答システム等の活用により効率的に行う。
  - a. 「問合せ対応システム」による対応事例の共有や活用を行うことにより、業務の効率化を図る。
- ③ 深刻化、増大する標的型攻撃や新種のコンピュータウイルス等のサイバー攻撃に対して、注意喚起・情報共有のみならず、未然発生防止のための措置等高度な対策等の提案を行う。
  - a. サイバー情報共有イニシアティブ(J-CSIP<sup>4</sup>)の運用を着実に継続し、より有効な活動に発展させるよう参加組織の拡大、共有情報の充実等を図る。
  - b. 「標的型サイバー攻撃の特別相談窓口」の運営を通して情報収集を行いつつ、ウイルス検体の収集・解析・分析・アドバイスや対策情報発信等をタイムリーに実施する。
  - c. 公的組織や重要関連組織に対する標的型サイバー攻撃の被害低減を目的としたサイバーレスキュー隊(J-CRAT<sup>5</sup>)を運用し、組織への標的型サイバー攻撃対応等の支援を実施する。また、サイバーセキュリティ戦略本部から委託があった場合、当該委託に基づき、独法等の情報システムに対するサイバー攻撃の原因究明調査を実施する。
  - d. 標的型サイバー攻撃の解析において、独立行政法人情報通信研究機構(NICT<sup>6</sup>)等と連携して攻撃防御の技術に関する知見交換を行い、解析手法の高度化を行う。

#### (1-2)情報システムの脆弱性に対する適切な対策の実施(情報処理促進法第43条第3項の規定に基づく情報の公表に係るものを含む。)

- ① 「脆弱性関連情報届出受付制度」を引き続き着実に実施するとともに、関係者との連携を図りつつ、脆弱性関連情報をより確実に利用者に提供する手法を検討する。
  - a. 経済産業省の告示に基づき、脆弱性関連情報の届出受付を行いつつ、四半期毎に届出の受付状況を公開する。
  - b. JPCERT/CC<sup>7</sup>との連携を図りつつ、脆弱性関連情報をウェブサイト運営者、ソフトウェア製品開発者に

<sup>3</sup> 日本商工会議所、全国商工会連合会及び全国中小企業団体中央会

<sup>4</sup> J-CSIP: Initiative for Cyber Security Information sharing Partnership of Japan<sup>5</sup> J-CRAT: Cyber Rescue and Advice Team against targeted attack of Japan

<sup>5</sup> J-CRAT: Cyber Rescue and Advice Team against targeted attack of Japan

<sup>6</sup> NICT: National Institute of Information and Communication Technology

<sup>7</sup> JPCERT/CC: Japan Computer Emergency Response Team Coordination Center

提供する。

- c. 脆弱性対策を促進するためのツールを提供する。
  - d. 「情報システム等の脆弱性情報の取扱いに関する研究会」において脆弱性対策の問題点とその解決策を検討するとともに、届出制度の改善策を策定する。
  - e. 情報処理の促進に関する法律(情報処理促進法)の改正に伴い、「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」等の関連規定に求められる変更について、ステークホルダーとなる関係団体とも連携して検討し、また、必要な合意形成を図る。
  - f. 上記e.の関連規定の変更にあわせ、機構が実施する脆弱性対策等の業務について、その設計や体制に必要な見直しを検討する。
- ② 統合的な脆弱性対策情報の提供環境を整備し、開発者、運用者及びエンドユーザに対して、脆弱性対策の普及啓発を推進する。
- a. 「JVN iPedia」(脆弱性対策情報データベース)及び「MyJVN<sup>8</sup>」の運用を引き続き行う。
  - b. 情報システムの脆弱性対策を普及・啓発するためにセミナー等を開催する。
- ③ 最新の脆弱性情報やインシデント情報を収集・分析し、注意喚起による危険回避や対策の徹底を図り、情報セキュリティリスクの低減を促進する。
- a. 情報セキュリティ上の最新情報を適宜収集しつつ、特に必要とされる場合には注意喚起等による対策情報等の公表を行う。

### (1-3)社会的に重要な情報システムに関する対策支援

- ① 重要インフラ分野や制御システム等の社会的に重要な情報システムについて、関係府省等の求めに応じて、情報セキュリティ強化のための調査、協力を行う。(1-1(3)参照)
- a. 制御システムのセキュリティについて、標準化動向、業界動向等に関する情報を収集するとともに、国内での普及を行う。
  - b. 制御システムの評価支援業務を実施する。
- ② 我が国の競争力の源泉となる組込み機器の脆弱性に関する対策の提示等を行う。
- a. 組込み機器の脆弱性に対する調査、検討及び普及啓発を行う。
  - b. 組込み機器の脆弱性の検出技術の普及啓発を行う。
- ③ 平成29年度に機構に設置する「産業系サイバーセキュリティ推進センター(仮称)」の効率的、効果的な設置等に資するため、機構の関係部署が有するサイバーセキュリティに関する知見を共有・活用する。(3-1(5)参照)

### (1-4)技術的レポート等の提供と満足度調査

- ① 技術情報の収集・分析結果を技術的なレポート等として年間20回以上提供する。
- ② 機構から情報を提供・共有した企業、個人等に対し、その提供時等に200者以上のアンケートを行うほか、共有相手先等へ30者以上のインタビュー、ウェブサイトを用いた意見の収集等を行い、提供・共有した情報に関するニーズや課題を把握する。それらを元に提供・共有する情報について、内容の充実、手段の改善等のフィードバックを行う。また、意見の収集とフィードバックは、的確な対応ができるよう担当を一元化して実施する。

---

<sup>8</sup> セキュリティ上問題となるPCやサーバの脆弱性の対策を促進するために、対策情報を効率的に収集し、簡単な操作で最新情報に基づいたチェックを行うことができる仕組み(フレームワーク)の総称。

## (2) 情報セキュリティ対策に関する普及啓発

- ① 広く企業及び国民一般に情報セキュリティ対策を周知するため、地域で開催される情報セキュリティに関するセミナーへの講師派遣等の支援、各種イベントへの出展、普及啓発資料の配布、啓発サイトの運営等を行い、更なる啓発活動を実施する。
  - a. サイバー攻撃等に関する情報の収集・分析や提供・共有に対するフィードバックをもとに、広く企業及び国民一般に、効果的・効率的に情報セキュリティ対策を普及啓発するためのコンテンツを作成するとともに、普及啓発活動で活用する。
  - b. 地域で開催される情報セキュリティに関するセミナーへの講師派遣等の支援を行う。
  - c. 情報セキュリティ啓発サイトの運営を行い、広く普及啓発を行う。
  - d. 小中高等学校の児童・生徒を対象とした情報セキュリティに関するコンクールを開催する。実施に当たっては、全国の小中高等学校に対して応募依頼を行うとともに、機構の成果物を紹介する。
  - e. 一般ユーザ、経営層を含む一般企業、セキュリティ専門職等に向けて情報セキュリティに関する普及啓発を行うため、各種イベントへの参加、普及啓発資料の制作・配布等を行う。
  - f. 全国の民間団体の協力を得て、スマートフォン・SNS<sup>9</sup>・インターネット利用者に対し情報セキュリティ対策等の普及啓発を行うとともに、情報セキュリティの普及啓発を行う民間団体の連携の強化を図る。
  - g. 中小企業の情報セキュリティ人材不足の解消に向けて指導者を育成するとともに、セキュリティプレゼンター制度を運用し、関連団体等への協力を得て、セキュリティプレゼンター登録数を100名以上増加させる。
  - h. 商工三団体の傘下団体等の協力を得つつ脆弱性対策情報等の定期的周知先の拡大を図る。
  - i. 中小企業向けセキュリティガイドラインについて、経営者向けパート、最新脅威への対策等を追加し、改定する。また、国や中小企業関連団体等が共同して情報セキュリティの重要性を訴える取り組みに参画する。更に、セミナー等の機会を通じて中小企業に同ガイドラインの情報を提供し、必要な支援を行う。(1-1(4)参照)
- ② 情報セキュリティに関する脅威を分析・評価し、IT利用企業や国民一般に向けた積極的な情報セキュリティ対策を図るため、必要な情報提供を行う。
  - a. 企業経営に情報セキュリティ対策を有効に取り入れるため、情報セキュリティ対策や情報セキュリティリスク管理に関する組織の取り組みについて調査する。
  - b. 情報セキュリティに関連する事象に対して、社会科学的な観点からの取組、情報セキュリティリスクの対応についての動向および情報セキュリティエコノミクスの動向について調査した結果を踏まえ、サイバーセキュリティ経営ガイドラインの解説書を作成する。
  - c. インターネット利用者を対象に、情報セキュリティ脅威に対する意識調査を実施する。
- ③ 社会的要請に応じ、情報セキュリティ対策・プライバシーに関する状況の調査・分析を行い、情報提供を行う。
  - a. 「情報セキュリティ白書2016」を編集、作成、出版するとともに、電子書籍版を作成する。
  - b. 組織における内部不正防止ガイドラインの普及に資するため、関連する事例収集及びガイドライン改定を行う。
- ④ 米国商務省国立標準技術研究所(NIST<sup>10</sup>)、韓国インターネット振興院(KISA<sup>11</sup>)等の各国の情報セキュ

<sup>9</sup> SNS : Social Networking Service の略

<sup>10</sup> N I S T : National Institute of Standards and Technology の略

<sup>11</sup> K I S A : Korea Internet & Security Agency の略

リティ機関との連携を通じて、情報セキュリティに関する最新情報の交換や技術共有等に取り組む。

- a. 米国商務省国立標準技術研究所(NIST)、韓国インターネット振興院(KISA)等と、各国のサイバー攻撃の現状や各国の対応状況について情報収集、意見交換を行う。

### **(3)国際標準に基づくIT製品等のセキュリティ評価及び認証制度の着実な実施**

- ① ITセキュリティ評価及び認証制度において、制度利用者の視点に立った評価・認証手続きの改善、評価等に関する人材の育成、積極的な広報活動等を実施する。特に、認証書発行までにかかる期間を成果指標とし適切な期間内とする。また、認証取得後、認証取得者に対してアンケート調査を実施し業務改善を図る。
  - a. 認証を通じ、国内で使用される製品のセキュアな開発環境の整備及びセキュアな製品調達の推進を図る。
  - b. ITセキュリティ評価及び認証制度の利用促進と評価品質向上のため、政府調達製品におけるセキュリティ確保のための調査や開発、情報提供を実施する。
  - c. ITセキュリティ評価及び認証制度の関係者(調達者、開発者等)からの制度への要望や運営上の課題を踏まえた申請手続きの改善や内部処理の短縮に努める。
- ② 暗号・セキュリティ製品やモジュールの認証、暗号技術等広範に亘る情報セキュリティ対策の国際標準化や新たな手法の開発に係わる国際会議等に参加し、貢献する。
  - a. 情報セキュリティ分野と関連の深い国際標準化活動であるISO/IEC JTC1/SC27<sup>12</sup>が主催する国際会合(年2回)等へ、機構職員を派遣し、活動成果の国際規格への反映を働きかけるとともに、収集した国際規格動向を踏まえ、今後の事業への反映を行う。
  - b. CCRA<sup>13</sup>会議に出席し、認証に係る情報交換や相互承認の取組について検討を行う。
  - c. 脆弱性対策に関する国際的な標準化等に参画し、情報システム等のグローバルな安全性の確保に向けた活動に寄与する。
- ③ 暗号モジュール試験及び認証制度(JCMVP)について、試験等に関する人材の育成を図るとともに、暗号モジュールセキュリティ要求事項の国際標準ISO/IEC 19790に基づく認証制度の運営準備を推進する。
  - a. CMVP<sup>14</sup>(NIST)との共同認証制度の検討を進める。
  - b. 暗号モジュール試験及び認証制度(JCMVP)並びにITセキュリティ評価及び認証制度(JISEC)ハードウェア分野の認証を推進する。
  - c. ハードウェア評価・認証に関連して脆弱性評価、対策技術に関する情報収集、欧米関連団体との連携強化を図る
  - d. 最先端の脆弱性評価ツールを、日本国内のハードウェア開発者、評価機関、大学等の関係者に利用させることにより、ハードウェアの脆弱性評価に係る人材の育成を図る。
- ④ 政府調達等における情報セキュリティの確保に資するため、政府及び地方公共団体の調達担当者等に対して「政府機関の情報セキュリティ対策のための統一基準」を満たすように、調達する機器等のセキュリティ

<sup>12</sup> ISO/IEC JTC1/SC27 (International Organization for Standardization/ International Electrotechnical Commission Joint Technical Committee 27) : ISO は非電気分野、IEC は電気分野の国際標準化機関であり、両機関が情報処理分野を担当する合同委員会 JTC1 を設けている。SC27 は JTC1 傘下の Sub Committee の 1 つでセキュリティ技術を担当。

<sup>13</sup> C C R A (Common Criteria Recognition Arrangement) : Common Criteria (情報技術セキュリティを評価するための国際規格) にもとづいたセキュリティ評価・認証の相互承認に関する国際的な協定。

<sup>14</sup> C M V P (Cryptographic Module Validation Program) : N I S T が運営する北米の暗号モジュール認証制度。

イ要件及びその要件を満たす認証取得製品等の情報提供や普及啓発を行う。

- a. 「IT製品の調達におけるセキュリティ要件リスト」について、改定等の要否を検討し、検討結果に応じて経済産業省と共に改定案を策定するとともに、当該要件リストの効果的活用を施すためのガイドブックを引き続き提供する。
- b. IT製品の技術分野ごとに作成したプロテクションプロファイル<sup>15</sup>の情報提供を実施する。
- c. 情報システムを調達する際にセキュリティ要件の確認を支援するツール等を提供する。

#### **(4)暗号技術の調査・評価**

- ① 電子政府推奨暗号リストの適切な維持・管理を行うため、CRYPTREC<sup>16</sup>の事務局を引き続き務めるとともに、電子政府推奨暗号の危殆化をフォローするため、国際会議へ出席し、調査を行う。また、民間セクターにおける暗号利用システムの円滑な移行を図るための情報提供を行う。
  - a. 暗号技術評価委員会の活動において、情報システム等のセキュリティ技術の基礎となる暗号アルゴリズムの安全性監視活動を実施するため、国際会議等に年間7回以上参加し、調査を行う。
  - b. 暗号技術活用委員会の活動において、CRYPTREC暗号リスト小改定についての検討及び暗号の普及促進や暗号プロトコル安全性評価を実施するための課題についての検討を行う。
  - c. 暗号技術を安全に利用してもらうための普及啓発活動として、一般を対象とした運用ガイドラインの作成に着手する。
  - d. CRYPTRECの1年間の活動成果を報告するため、NICTと共同でCRYPTRECシンポジウム2016を開催する。
- ② 技術的評価能力の向上に資する最新技術動向の情報収集等を行うため、NIST及びJIWG<sup>17</sup>と毎年定期協議を行う。

<sup>15</sup> Protection Profile：IT製品等のセキュリティ要件をISO/IEC 15408に基づいて記述した要求仕様書

<sup>16</sup> C R Y P T R E C (Cryptography Research and Evaluation Committees)：電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査検討するプロジェクト。

<sup>17</sup> J I W G (Joint Interpretation Working Group)：欧州における、スマートカード等のセキュリティ認証機関からなる技術ワーキンググループ。



## 2. 社会全体を支える情報処理システムの信頼性向上に向けた取組の推進～重要インフラ分野等における情報処理システムの信頼性・安全性の向上～

### 2-1. 平成28年度における重点事項

#### (1)IoT<sup>18</sup>時代のシステム開発におけるセーフティ・セキュリティの実現(～つながる世界の開発指針の実装と普及～)

##### ① 事業内容

「日本再興戦略2016」の工程表<sup>19</sup>において示された第4次産業革命を支える環境整備を推進するため、機構が平成27年度に取りまとめた「つながる世界の開発指針」を政府の政策や様々な産業分野に展開する。具体的には、IoT推進コンソーシアム<sup>20</sup>IoTセキュリティワーキンググループが策定する「IoTセキュリティガイドライン」や様々な産業分野や団体の標準仕様等に反映させるべく開発指針の積極的な提案活動を実施する。

さらに、産業分野への開発指針の普及に向けて、積極的な普及活動に努めるとともに、産業界における実装を推進する。

加えて、異なる産業分野が連携する場合においても開発指針を適用することができるよう、様々な製品とつながるIoT製品の信頼性を高めていくために必要となるセーフティ・セキュリティ要件について、外部有識者の知見を得て明確化を行う。

##### ② 成果指標

IoT推進コンソーシアムIoTセキュリティワーキンググループが策定する「IoTセキュリティガイドライン」に、「つながる世界の開発指針」の記載内容を反映させる。また、産業分野間における情報連携を促進するため、第三期中期計画期間の終了までに、「つながる世界の開発指針」を4以上の産業分野や団体の標準仕様等に反映させる。

さらに、個別訪問による説明及び外部団体主催やIPA主催のセミナー等での講演を実施し、200以上の団体・企業等に対して当該開発指針を広く周知するとともに、開発指針を適用できているかどうかの確認を企業等が自ら行えるようにするための要件確認リスト等を整備し、開発指針を異なる産業分野の2以上の団体または企業に適用する。

加えて、セーフティ・セキュリティに関する要件を取りまとめた技術要件書等を作成する。

#### (2)システム構築における上流工程の強化(～IoT環境に対応したシステム開発の促進～)

##### ① 事業概要

IoTの進展によって様々な製品同士がつながり、それにより従来想定していなかった事態が起きる可能性があることから、こうした状況変化に対応しつつ効果的なシステム構築が行えるよう、上流工程を強化していく必要がある。そのため、システムズエンジニアリング<sup>21</sup>の導入が先行している欧州の適用事例等を調査・分析し、有効領域を明らかにすることを通じて、広く産業界にIoT時代のシステム構築に有用な考え方やアプローチ手法の導入を推進する。

<sup>18</sup> Internet of Things(モノのインターネット)

<sup>19</sup> 「日本再興戦略2016」の工程表 中短期工程表「第4次産業革命の実現⑨」[http://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/2016\\_kouteihyo.pdf](http://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/2016_kouteihyo.pdf)

<sup>20</sup> 産学官が参画・連携し、IoT推進に関する技術の開発・実証や新たなビジネスモデルを創出・推進するために2015年に設立された組織。

<sup>21</sup> 様々な要件を俯瞰的・系統的に把握し、複数の製品やサービスが連携するようなシステムの複雑化に対応した開発方法

## ② 成果指標

システムズエンジニアリングに関する10件以上の適用事例を収集し、分析結果や有効性を解説した報告書等を公開する。導入推進に係る指標については平成29年度計画において設定する。

### **(3) 組込みソフトウェア産業の構造転換に向けた取組**

#### ① 事業概要

経済産業省と協力して、「日本再興戦略2016」の工程表<sup>22</sup>にて示された組込みソフトウェア産業に関する取組みを推進する。具体的には、組込みソフトウェア産業の抱える課題、開発技術動向、人材育成状況等を把握するため、我が国における組込みソフトウェア産業の実態を調査・分析し、その結果を我が国の組込みソフトウェア産業育成策に反映させる。

#### ② 成果指標

組込みソフトウェア産業に係る実態調査については、国内の組込みソフトウェア関連企業15社以上にヒアリングを行うとともに、アンケート調査も行い100社以上から適正な回答を得て、分析結果を取りまとめる。さらに、分析結果を関係省庁等で策定予定の「組込みソフトウェア産業戦略(仮称)」骨子案に反映させる。

## **2-2. 着実に取り組む事項**

### **(1) 重要インフラ分野の情報処理システムに係るソフトウェア障害情報の収集・分析及び対策**

#### **(1-1) 重要インフラシステム等のソフトウェア障害情報の収集・分析、及びソフトウェア障害の再発防止の導入促進や事例に対する対策支援**

- ① 平成27年度までに取りまとめた障害事例情報の分析に基づく教訓や、障害事例情報の教訓化ノウハウ及び教訓の活用方法に関するガイド等を提供し、新たに2以上の産業分野において、自律的な障害情報収集・共有の体制を構築する。
- ② 平成27年度までの成果を活用し、産業ごとに自律的に障害情報共有が進むように必要な情報提供、情報共有基盤の整備等の支援を進めるとともに、社会に深刻な影響を及ぼした情報処理システムの障害事例情報の分析活動の強化を図る。
- ③ 重要インフラシステム等のソフトウェア障害防止に向けて、平成27年度までに整理した教訓、及び教訓の作成・活用ガイドや活用事例等の普及展開を図る。
- ④ ソフトウェア開発データの活用による情報処理システムの信頼性向上を目指し、過去2年間に収集・分析したデータを加え、「ソフトウェア開発データ白書」を出版する。また、新たに200プロジェクト以上の開発データを収集し、分析を行う。さらに、組込み系の開発データ収集・分析を強化する。
- ⑤ 情報処理システムの信頼性の向上に係る成果の有効性(役立ったと回答する者の割合)を平成27年度と同程度またはそれ以上とする。(中期目標:50%以上、平成26年度実績:78%)また、情報処理システムの信頼性の向上に係るガイドライン等の機構の成果について、企業等への導入率を平成27年度と同程度またはそれ以上とする。(中期目標:35%以上、平成26年度実績:45%)

### **(2) 利用者視点でのソフトウェア信頼性の見える化の促進**

#### **(2-1) ソフトウェア品質説明力の強化の促進**

- ① 製品・サービス等の異なる20の業界団体・機関等に対し、情報処理システムの信頼性の向上に関する利

<sup>22</sup> 「日本再興戦略 2016」の工程表 中短期工程表「第4次産業革命の実現③」

用者や業界等のニーズや課題の把握を継続して行う。さらに、業界団体・機関等と継続的な意見交換を行う関係を構築し、ガイドライン等の企業等への導入を促進する。

### **(2-2)ソフトウェア信頼性の見える化促進のための環境整備**

- ① IoT時代に求められる情報処理システムを実現するソフトウェアについて、その高信頼性を確保するため、先進的な設計技術の効果的な適用事例を10件収集し、分析・整理する。また、ソフトウェアの信頼性検証のための先進技術及びその活用手法に関する内外の最新動向を収集する。
- ② IoTの進展により、様々な組込みシステムやITシステム等が接続されるようになることから、IoT環境(つながる世界)におけるセーフティ・セキュリティを確保するため「つながる世界の開発指針」の普及展開を図り、異なる産業分野の2以上の団体又は企業に適用する。また、普及展開の段階で出てきた新たな要件をこの開発指針に反映する。(2-1(1)参照)
- ③ IoT時代の産業分野間での情報連携において、セーフティ・セキュリティを確保するための高信頼化機能の実証実験を行う。
- ④ 大学等におけるソフトウェア工学分野の研究提案(RISE<sup>23</sup>)を公募し、選考・採択した研究を支援するとともに、得られた成果を産業界へ展開するための活動を行う。

### **(3)公共データの利活用など政府方針に基づく電子行政システムの構築支援**

- ① 政府CIO<sup>24</sup>室、経済産業省と連携して「情報共有基盤推進委員会」を運営し、電子行政システム構築支援に係る事業(オープンデータ構築支援及び文字情報基盤の活用)について事業を進める。
  - a. 共通語彙基盤  
電子行政システムにおけるオープンデータ提供や情報連携に不可欠な基本語彙「コア語彙」の整備を継続しながら、共通語彙基盤の活用について検討を進める。また、共通語彙基盤の利便性をさらに強化し、より広く語彙の構築や活用を効率的に行えるようにするため、情報連携用基本語彙データベースの構築を進めるとともに、語彙データベースを活用する利用者に対して、使いやすいインターフェースを提供するツールの構築を開始する。
  - b. 文字情報基盤  
行政機関が情報処理をするために必要となる人名漢字等の文字情報を国際標準に適合した基盤に整備し、利便性の高い公共サービスとして提供する。また、国際標準化作業の推進を図るとともに、事業内容の普及に努める。
  - c. 自治体調査の実施  
自治体の公共データの対応状況や共通語彙基盤、文字情報基盤についての認知度等を調査する。

### **(4)ソフトウェアの信頼性に関する海外有力機関との国際連携**

- ① 米国商務省国立標準技術研究所(NIST<sup>25</sup>)、米国カーネギーメロン大学ソフトウェアエンジニアリング研究所(SEI<sup>26</sup>)、独国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<sup>27</sup>)等の海外の代表的

<sup>23</sup> RISE : Research Initiative on Advanced Software Engineering の略

<sup>24</sup> CIO : Chief Information Officer の略

<sup>25</sup> NIST : National Institute of Standards and Technology の略

<sup>26</sup> S E I : Software Engineering Institute の略

<sup>27</sup> IESE : Institute for Experimental Software Engineering の略

機関との意見交換を行う。

- ② ソフトウェアの信頼性に関して、特に重要性の高いものについては、国際標準化に向けた活動を行う。

#### **(5)システム構築における上流の機能強化(2-1(2)参照)**

- ① IoT環境下で、様々な組み込みシステムやITシステム等を一体として考える新たな開発手法として、システムズエンジニアリングを位置づけて、その有効領域を明らかにする。また、新たな開発手法の普及展開に向けて、ソフトウェア高信頼化センターをシステムズエンジニアリングの産学連携の拠点とする整備を進める。
- ② 複合原因障害のリスク要因評価(ハザード分析)に関する手法として米国等で実績があるSTAMP<sup>28</sup>(システム理論に基づく事故モデル)について、日本国内での適用法を検討する。また、検討した手法は、実産業界分野の題材による適用試験を行うとともに、普及展開を図る。
- ③ IoTの進展により想定される情報システムの開発要件の不確実性の拡大等に対応するため、現状でも強化が求められているシステム開発プロセスの上流工程における諸作業を適切に行うために必要な知識・経験(ノウハウ)を収集し、分析を行う。また、収集・分析した知識・経験(ノウハウ)をガイドブック等に整理し、普及展開を図る。

---

<sup>28</sup> Systems-Theoretic Accident Model and Processes の略

### 3. IT人材育成の戦略的推進～若い突出したIT人材の発掘・育成及び高度IT人材育成の体系・客観的な能力基準の普及等～

#### 3-1. 平成28年度における重点事項

##### (1)若い突出したIT人材の発掘・育成と産業界全体への活用の啓発(未踏IT人材発掘・育成事業)

###### ① 事業概要

現プロジェクトマネジャー(PM)が有する専門性と異なる専門性を有するPM2名を増員し、発掘する人材の多様化を拡げるとともに、PMの独自の指導のもと、若い突出したIT人材を引き続き育成する。

U-22プログラミングコンテスト、ETロボコン等と引き続き連携するとともに、平成28年度は関西地区を重点地区として大学等における個別説明会を開催するなどして、応募件数の増加に努める。

###### ② 成果指標

平成28年度においては応募件数130件以上を目指す。また、関西地区において大学等の個別説明会を10回以上(平成27年度実績:5回)開催し、関西地区からの応募件数40件以上(平成27年度実績:25件)を目指す。

##### (2)ITによる新事業創出起業家支援(IoTプロジェクト支援事業)

###### ① 事業概要

我が国のイノベーション加速に向けて、ITによる新事業を創出する起業家を支援する体制を構築し、新たな価値創造を担う人材を育成する「先進的IoTプロジェクト支援事業」を実施する。先進的なIoTプロジェクトを公募により採択し、採択された案件に対して、資金支援やメンターによる伴走型支援を実施する。平成27年度中に行った第1回公募において採択した案件について、資金支援やメンターによる伴走型支援を実施するとともに新たに公募を行う。

また、自治体が企業等と一体となって、地方での取り組みを通じて地方課題の解決に資するIoTビジネスの創出を目指す人材の発掘・育成の取り組みを推進するために経済産業省が実施する「地方版IoT推進ラボ」の取り組みに対して第1弾、第2弾選定の審査協力を行うとともに、第1弾選定 IoT 推進ラボに職員を派遣して各ラボの進捗状況、現場ニーズを把握し適切な支援等を行う。

###### ② 成果指標

先進的IoTプロジェクト支援事業については、平成28年度中に公募を行い、8件程度の採択を目標とする。平成29年度途中まで支援を実施することから、支援結果に係る指標については平成29年度計画において設定する。

地方版IoT推進ラボについては、経済産業省と連携しつつ、経済産業省が行う採択審査においてIoT推進の観点から参画するとともに関係機関と連携しつつ支援体制を構築する。第1弾選定 IoT 推進ラボについては、支援内容を明確化し、順次メンター派遣等の支援を行う。

##### (3)特定の優れた技術を持ったIT人材の発掘・育成(セキュリティ・キャンプ)

###### ① 事業概要

セキュリティ・キャンプの開催を通じて、高度なIT人材を全国幅広く育成し、高度IT人材の裾野を拡げる。

具体的には、サイバーセキュリティ分野への関心と技術ポテンシャルの高い全国の22歳以下の精鋭を一堂に会した「セキュリティ・キャンプ全国大会」を、賛同企業会員により構成された「セキュリティ・キャン

プ実施協議会」と共同開催する。

また、サイバーセキュリティ人材の発掘とセキュリティ・キャンプ修了生の継続的育成のために、「セキュリティ・キャンプ実施協議会」と共同して、セキュリティ・キャンプ地方大会を開催する。セキュリティ・キャンプ地方大会の開催にあたっては、既に開催実績のある地方においては自立的な運営を促し、初めて開催する地方においてはノウハウ移転に注力するなど、メリハリをつけた形で実施する。

② 成果指標

セキュリティ・キャンプ全国大会及び地方大会を延べ10回程度開催し、修了生180名以上の輩出を目指す。(平成27年度実績162名)

#### **(4) 新国家資格の準備及び着実な実施(情報処理安全確保支援士)**

① 事業概要

新国家資格「情報処理安全確保支援士」制度(平成28年10月創設)における試験、登録及び講習事務の実施機関として、事前準備及び実施体制の整備を進める。情報処理促進法の改正後、速やかに登録申請の受付を開始するとともに、平成29年度から開始する情報処理安全確保支援士試験に係る問題作成や情報処理安全確保支援士向けの講習の準備等を行う。また、企業等における本制度の認知度向上、活用促進に向けたプロモーション活動を実施する。

② 成果指標

企業等における経営層や人事・教育担当者等に本制度の活用を訴求するため、業界団体や教育事業者等と連携した説明会等を10回以上実施する。

#### **(5) 産業系サイバーセキュリティ推進センター(仮称)の設立準備**

① 事業内容

重要インフラや我が国経済・社会の基盤を支える産業における、サイバー攻撃に対する防護力を強化するため、平成29年度に機構に産業系サイバーセキュリティ推進センター(仮称)を設置し、官民が共同してサイバーセキュリティ対策の中核となる人材を育成する。

② 成果指標

平成29年度に産業系サイバーセキュリティセンター(仮称)を設立するために必要なカリキュラム作成等の準備を行う。

### **3-2. 着実に取り組む事項**

#### **(1) イノベーションを創出する若いIT人材の発掘・育成と産業界全体への活用の啓発**

##### **(1-1) 若い突出したIT人材の発掘・育成と産業界全体への活用の啓発**

- ① 重点地区を定めて人材の発掘を促進し、平成28年度に実施される公募(平成29年度公募)において応募件数を130件以上とする。(3-1(1)参照)
- ② 現プロジェクトマネージャー(PM)と専門性の異なるPM2名を増員し、発掘する若い突出したIT人材の多様性を高めるとともに、PMの独自の指導のもと、引き続き育成する。(3-1(1)参照)
- ③ 一般社団法人未踏等の外部団体と連携し、若い突出したIT人材による成果等をイベントや交流会を通じて産業界に周知するとともに、起業・事業化に向けたネットワーク作りを行う。

##### **(1-2) ITによる新事業創出起業家支援(3-1(2)参照)**

- ① 我が国のイノベーション加速に向けて、ITによる新事業を創出する起業家を支援する体制を構築し、新た

な価値創造を担う人材を育成する「先進的IoTプロジェクト支援事業」を実施する。

- ② メンター（PM、アドバイザー）による伴走支援を行う。メンター（PM、アドバイザー）による伴走支援を通じて、起業家やクリエイター等によるITを中心とした日本のイノベーション加速のためのIT人材育成支援体制を構築・運営する。実施にあたっては、有識者による推進委員会を設置し、事業運営の助言・評価を受ける。

### (1-3) 特定の優れた技術を持ったIT人材の発掘・育成

- ① セキュリティ・キャンプの開催を通じて、高度なIT人材を全国幅広く育成し、高度IT人材の裾野を広げる。  
(3-1(3)参照)
- ② キャンプフォーラムの開催など修了生に対するフォローアップの強化を図る。
- ③ サイバーセキュリティ分野でのイノベーションを起こすために未踏事業とのコラボレーションを図る。

## (2) IT融合人材と情報セキュリティ人材に関する客観的な能力基準の整備及び情報発信

### (2-1) IT融合人材のスキル指標等の提示と活用の促進等

- ① 平成27年度までの事業成果であるIT融合人材スキル指標や組織能力評価指標（成熟度モデル）等について、「iコンピテンシ デクシヨナリ(iCD)」の情報発信基盤である「iCDポータル」を通じ、より利用しやすい形で提供する。

### (2-2) 情報セキュリティ人材のスキル指標等の提示と活用の促進

- ① マネジメント面からの情報セキュリティ対策を担う人材（情報セキュリティマネジメント人材）について、「情報セキュリティマネジメント試験」と連携したプロモーション活動を実施する。
- ② 情報セキュリティに関する高度なスキルを有する人材（高度情報セキュリティ人材）について、業界団体等の取り組みと連携し、経営者視点や業界ニーズ等（IoT、AI<sup>29</sup>、データ活用等の新たなIT活用領域への対応を含む。）の観点から、同人材が活躍する代表的な役割参照モデルを構築するとともに、スキルを維持、向上させていくための教育プログラム構築に向けた検討を行う。
- ③ 新国家資格「情報処理安全確保支援士」制度（平成28年10月創設）における試験、登録及び講習事務の実施機関として、事前準備及び実施体制の整備を進める。情報処理促進法の改正後、速やかに登録申請の受付を開始するとともに、平成29年度から開始する情報処理安全確保支援士試験に係る問題作成や情報処理安全確保支援士向けの講習の準備等を行う。また、企業等における本制度の認知度向上、活用促進に向けたプロモーション活動を実施する。（3-1(4)参照）

### (2-3) IT人材をめぐる動向等の情報発信と新事業支援機関に対する取組

- ① IT人材の現状や新たな動向及びこれまでのIT人材動向の分析結果を踏まえ、「IT人材白書2017」を取りまとめるための調査を実施する。また、IT人材育成に取り組む産業界や教育界、ITを活用する人材に対して「IT人材白書」の普及を図り、IT人材育成に関する動向等の情報発信を行う。
- ② 情報関連人材育成事業を行う新事業支援機関等に対して、機構の成果について積極的に情報発信を行う。また、新事業支援機関からの要請に基づき、機構の成果普及や講師の派遣等を行う。

## (3) 情報処理技術者の技術力及び国民のIT利活用力の向上を目指した情報処理技術者試験の実施等

<sup>29</sup> AI：Artificial Intelligence（人工知能）

- ① 平成28年度情報処理技術者試験として春期試験(4月)、秋期試験(10月)及びCBT<sup>30</sup>方式によるiパス(ITパスポート試験(随時))を実施する。その際、情報セキュリティ人材をはじめとするIT人材の多様化と高度化、新たな情報技術の進歩・変化を反映しつつ、共通キャリア・スキルフレームワークに準拠した試験問題を作成する。また、試験問題の品質を維持するため、試験委員会の体制を強化する。
- ② 産業界・教育界への広報活動を強化し、情報セキュリティマネジメント試験をはじめとする情報処理技術者試験、iパス、平成29年度から開始する情報処理安全確保支援士試験の更なる普及・定着化を推進するとともに、不断のコスト削減に努め、試験の活用促進と収益の改善を目指す。
- ③ 情報処理技術者試験のアジア各国との相互認証の維持、アジア共通統一試験の定着に向けた支援を行う。

#### (4) スキル標準及び産学連携に関する事業の民間を含めた実施体制の構築

##### (4-1) 民間を含めた実施体制の構築に向けたスキル標準の統合

- ① 平成27年度に正式版を公開した「iコンピテンシ デクシヨナリ(iCD)」について、タスク・スキルの追加、改訂を行い「iCD2016」として公開する。また、iCDをより活用しやすくするため、目標達成度合いの管理や経年データの分析、研修・資格との連携機能等を追加した活用システムを併せて提供する。

##### (4-2) 民間を含めたスキル標準運営体制の検討とスキル標準活用推進

- ① iCDの普及・活用促進の民間移管を視野に入れ、情報発信基盤となる「iCDポータル」を公開し、iCDの認知度や活用方法の理解度向上に向けたプロモーション活動を実施する。また、スキル標準活用促進団体等による自主的な活動に対し積極的な支援を行う。
- ② グローバル展開を図る国内企業が安心してiCDを活用できるよう、欧米を中心とした国際的スキル体系の関連団体との協力関係を構築し、相互参照の強化を図る。

##### (4-3) 産学連携に関する情報ハブ機能の民間を含めた実施体制の継続的運営

- ① 産業界及び教育界における自立的産学連携IT人材育成活動に資するノウハウ、コンテンツを蓄積したIT人材育成iPediaを運用する。

---

<sup>30</sup>CBT：Computer Based Testing（コンピュータを利用して実施する試験方式）



## Ⅱ. 業務運営の効率化に関する目標を達成するためとるべき措置

### (1) 出口戦略を意識した業務運営の不断の見直し

- ① 各事業について実施の妥当性及び出口戦略を意識し、計画の策定、実行、評価、改善等に基づき業務運営の不断の見直しを行い、リソースを適切に配分する。
- ② 外部有識者及び第三者の意見・評価、フォローアップ調査、アウトカム分析等により、各事業の厳格かつ客観的な評価・分析を実施し、その結果を事業選択や業務運営の効率化に反映させることにより見直しの実効性を確保する。
- ③ 機構内の検討機能を強化するため事業実施前に部門横断的に方針の情報共有や意見交換会を行う等、事業の運営方法等が有効かつ効率的なものであるか検証する。
- ④ 機構に設置した各種審議委員会による事業評価や有識者・利用者に対するヒアリング(100者以上)等を行い、その結果を事業運営に反映させる。
- ⑤ 平成28年度計画を着実に実施するため、上期終了時点において事業の進捗状況の把握を行うとともに、それを踏まえた「平成28年度下期実行計画」を策定する。また、予算の適切な執行に向け、「中間仮決算」を実施する。
- ⑥ 機構の業務について、監査法人による外部監査のほかに、監事監査や監査室による内部監査を実施する。具体的には、監事監査については、平成28年度「監事監査計画」に基づき監査を実施し、監査室監査については、平成28年度「内部監査計画」に基づき、情報セキュリティ対策の状況に関する監査、ITセキュリティ認証業務に関する監査及び暗号モジュール認証業務に関する監査等の業務監査を実施し、監査結果を業務にフィードバックする。また、昨年度の監査結果に対するフォローアップを併せて行う。

### (2) 機動的・効率的な組織及び業務の運営

- ① 業務運営の見直しの結果を反映させるとともに、ITを巡る内外の情勢変化等を踏まえ、運営効率向上のための最適な組織体制に向けて不断の見直しを図る。
- ② 組織内外の課題に対応するため、部署を越えた横断的な連携を図り、外部専門人材も含めたワーキンググループやタスクフォースの設置等を行うことにより、機動的・効率的な組織・業務運営を行う。
- ③ 業務内容や専門性に応じて柔軟に活用できる多様な外部専門人材や先端的なセキュリティ人材を機動的・積極的に活用し、情勢の変化への対応力を高めるとともに、知識の習得や蓄積を通じて組織のパフォーマンス向上に努める。
- ④ 組織内の個々人が最大限のパフォーマンスを発揮できるよう、業績評価制度とそれに基づく処遇の徹底や外部研修の活用等を積極的に行い、職員の業務遂行能力の向上を図る。
- ⑤ 能力評価を実施し、評価結果を昇給・昇格に適正に反映させる。
- ⑥ 職員の中長期的な育成のため、キャリアステップに応じた階層別研修、高度な専門知識や実践的技能を習得させるテーマ別研修等を実施する。その他、職員の説明能力向上と職員間の知識の共有を目指した「1hourセミナー」を適宜、実施する。
- ⑦ 機構における専門性・特殊性の高い業務を継続していく観点から、就職情報サイトの積極的活用や採用説明会の充実等、新卒採用者の確保に向けた採用活動を強化する。
- ⑧ 行政改革における人件費削減の要請に応えつつ、限られた人員で効果的・効率的に事業を実施するため、

相乗効果をもたらすような部署間連携の強化を図るとともに、課題解決に対応した最適な組織体制を柔軟に整備する。

- ⑨ 機構の内部統制の推進として、内部統制委員会で策定した「行動計画」に基づき、コンプライアンス意識調査、リスクの抽出・分類・評価・対応及びコンプライアンス研修を実施するとともに、リスク管理委員会及び内部統制委員会を開催する。

### **(3) 運営費交付金の計画的執行**

- ① 運営費交付金の執行状況について、毎月財務部にて取りまとめ、役員会に報告することによりチェック機能の強化を図る等、運営費交付金の執行管理体制を強化することにより、事業の性質上やむを得ない案件を除き年度内での計画的執行を徹底し、予期せぬ運営費交付金債務残高の発生を抑制する。また、予期せぬ交付金債務残高についてはその発生要因を分析した上で、次年度以降の適正かつ計画的執行に努める。

### **(4) 戦略的な情報発信の推進**

#### **(4-1) ITに係る情報収集・発信等(シンクタンク機能の充実)**

- ① ユーザーニーズ等に関する市場動向、ITの技術動向、国際標準化動向等の調査を国内外に亘って行い、情報サービス・ソフトウェア産業に係る各種情報を収集し、積極的な情報発信を実施する。
- ② 海外関連機関との連携強化や国際会議への積極的な参加等を通じ、国際的な情報発信及び国際動向の把握に努める。
- ③ ITの安全性・信頼性向上に資する基準・標準の策定及び事業成果の活用に向けたツール化、データベース構築、ガイドブック作成等を行い、利便性の高い情報提供を行う。
- ④ 高度な情報サービスの利用を通じた我が国の国民生活の向上及び産業の発展のために、研究会等により数年先の市場動向及び技術動向を見据え今後注力していくべき技術分野等の抽出を行う。
- ⑤ 機構のニューヨーク事務所を活用し、米国におけるITの最新動向の把握に努める。
- ⑥ 機構と関連のある情報サービス産業関係団体との間で、トップレベルでの定期的な意見交換会を開催し、ユーザーニーズやIT関連の市場動向の把握に努める。
- ⑦ 最先端の分野における知見を高めるため、専門家を招いた勉強会等を定期的に開催する。

#### **(4-2) 戦略的広報の実施**

- ① ITに関する最新情報を発信することを目的として有識者等による講演等で構成するシンポジウムを開催するとともに、機構の事業内容及び成果の発信に適する展示会に出展する。また、開催結果の分析を行い、その内容を踏まえ翌年度の行事についての具体的な開催計画の策定に取り組む。
- ② 機構ウェブサイトについてコンテンツの充実を図り、有益かつ迅速な情報提供に努めるとともに、事業成果の主要なものについては、遅滞なく掲載する。また、利用者の利便性向上を図るため、ウェブサイトの画面構成の改善等に努めるほか、コンテンツ・マネジメント・システム(CMS)の更新及びアクセス解析手法等の検討を行う。さらに、機構が主催するセミナー、シンポジウム等の円滑な受付業務を実施することを目的に、平成27年度に廃止したイベント・セミナー受付システムに代わる新たな受付サービスを導入する。
- ③ 機構の事業活動への理解及び事業成果の利用促進等を図ることを目的として、広報誌「IPA NEWS」を定期的に発行するほか、広報用冊子の制作・配布を行う。

- ④ 第三期中期計画に掲げた500件以上の報道発表の実現に向け、積極的に報道発表を実施する。また、個別取材対応を積極的に行う等、事業成果の認知度向上に努める。
- ⑤ 機構の行う公募、入札、イベント・セミナー情報及びセキュリティ対策情報等について、「メールニュース」等を通じた積極的な情報提供を行うとともに、毎月の事業成果について、「情報発信」として広報する。またメールニュース配信システムについては、従来よりも一層の安全・安心なサービスを利用者に提供するため、新たに電子メール証明書を付加するなど適切なセキュリティ対応を実施する。
- ⑥ 動画共有サイト、SNS等外部サービスを活用し、より広範な事業成果の普及を図る。

### **(5)業務・システムの最適化**

- ① 役職員等の作業を円滑かつ迅速に行うことができるよう、共通基盤システム及び基幹業務システムの運用管理・維持管理業務を確実に遂行する。
- ② 法律や制度改正及び社会環境の変化に柔軟に対応できるよう、基幹業務システムの高度化と業務の効率化の観点から、基幹業務システムの見直しを行う。
- ③ 執務環境における利便性の向上とコスト削減を目指し、執務環境の環境整備を図る。
- ④ 情報資産に対するリスク分析を踏まえ、システム障害時においても縮退運転可能な環境整備を目的としたシステムの構築・サービスの導入に着手する。

### **(6)業務経費等の効率化**

- ① 厳密な予算執行管理を継続して実施し、適正な執行を図る。運営費交付金を充当して行う業務においては、第三期中期目標期間中、一般管理費(人事院勧告を踏まえた給与改定分、退職手当を除く。)及び業務経費(新規分、拡充分を除く。)について、毎年度平均で前年度比3%以上の効率化を行う。
- ② 役職員の給与水準については、国家公務員の給与構造改革等を踏まえた適切な見直しを実施するとともに、ラスパイレス指数、役員報酬、給与規程及び総人件費を公開する。また、給与水準についての検証を行い、これを維持する合理的な理由がない場合には必要な措置を講じることにより、給与水準の適正化に取り組み、その検証結果や取組状況を公開する。

### **(7)調達最適化**

- ① 調達等合理化計画に基づき、契約の適正化を推進することとし、また、財務部内に設置した契約相談窓口による事前確認により、事業の目的に合致した入札・契約方法の選択及び手続きの適正化を推進しやむを得ない案件を除き、一般競争入札等(競争入札、企画競争及び公募をいう。以下同じ。)によるものとする。  
 具体的には、財務部内に設置した契約相談窓口による事前確認により、事業の目的に合致した入札・契約方法の選択及び手続きの適正化を推進し、やむを得ない案件を除き、一般競争入札等により調達を行うとともに、これら契約状況を適時適切に公開する。  
 結果として、一者応札・一者応募となった場合には事後調査を行い、問題点を把握し、今後の調達において改善に努める。
- ② 入札・契約の実施方法及び一者応札・一者応募となった契約案件について、契約監視委員会を2回以上開催して点検を行う。また、入札・契約の適正な実施について、監事等の監査を受ける。
- ③ 契約事務マニュアル、入札説明書ひな型等を活用することとし、事務処理の一層の標準化・効率化を図

る。

なお、当該マニュアル等の内容について、必要に応じて、適切に改訂を行う。

- ④ 役職員等に対して契約業務全般における知識の習得を図るため、定期的な研修を2回以上実施する。

## **(8) 機構のセキュリティ対策の強化**

- ① 「情報セキュリティ対策推進計画」に基づき、教育・訓練・自己点検・リスクアセスメント等の人的対策を実施する。機構の情報セキュリティ対策に係わる内部規程等の遵守状況を確認すると共に、継続的な遵守を目的とした対策を講じる。
- ② 役職員等が安全に業務を遂行できるよう、標的型攻撃メールやマルウェアなど、外部からの侵入の試みや感染による機密情報の流出などを予防・防止するための環境設定・運用監視を行なう。
- ③ 情報資産に対するリスク分析を踏まえ、適切な情報セキュリティ対策(主に物理的対策・技術的対策)を検討・実施する。

## **III. 財務内容の改善に関する目標を達成するためとるべき措置**

### **1. 自己収入拡大への取組み**

- (1) ITセキュリティ評価及び認証制度、暗号モジュール試験及び認証制度について、積極的な広報活動を通じて、その利用拡大を図る。
- (2) 機構主催のセミナー、印刷製本物及び出版物等について適切な受益者負担を求めていく。

### **2. 決算情報・セグメント情報の公表の充実等**

- (1) 機構の財務内容等の一層の透明性を確保する観点から、決算情報・セグメント情報の公開の充実等を図る。

### **3. 地域事業出資業務(地域ソフトウェアセンター)**

- (1) 地域ソフトウェアセンターの経営状況を的確に把握するため、決算ヒアリング等を行い、経営改善を目的とした積極的な指導・助言等を行う。  
また、地域ソフトウェアセンターに対する直接的、間接的な支援について、主要株主である地方自治体・地元産業界との意見交換を行う。
- (2) 地域ソフトウェアセンター全国協議会が毎年度3回以上開催されるよう開催計画についての助言等を行う。  
また、機構の活動内容の紹介等により、地域ソフトウェアセンター間の情報交換を促進し、地域ソフトウェアセンターの経営改善を図る。

### **4. 債務保証管理業務**

- (1) 保証債務の残余管理については、保証先への往訪や代表者との面談並びに決算書の徴求等を適宜行うとともに、金融機関とも連携して債権の保全を図る等適切に実施する。

## **5. 資産の健全化**

(1)保有する資産について自主的な見直しを行い、効率的な業務運営を担保するため不断の見直しを実施する。また、資産の実態把握に基づき、機構が保有し続ける必要があるかを厳しく検証し、支障のない限り、国への返納を行う。さらに、情報処理技術者試験の持続的な運営を可能とするため、応募者数増加に資する取り組みと不断のコスト削減に努め、財政基盤の確保を図ることにより、円滑な事業運営を目指す。

## **IV. 予算(人件費見積もりを含む。)、収支計画及び資金計画**

### **1. 予算(別紙参照)**

総表(別紙1-1)

事業化勘定(別紙1-2)

試験勘定(別紙1-3)

一般勘定(別紙1-4)

地域事業出資業務勘定(別紙1-5)

### **2. 収支計画(別紙参照)**

総表(別紙2-1)

事業化勘定(別紙2-2)

試験勘定(別紙2-3)

一般勘定(別紙2-4)

地域事業出資業務勘定(別紙2-5)

### **3. 資金計画(別紙参照)**

総表(別紙3-1)

事業化勘定(別紙3-2)

試験勘定(別紙3-3)

一般勘定(別紙3-4)

地域事業出資業務勘定(別紙3-5)

## **V. 短期借入金の限度額**

運営費交付金の受入等の遅延、その他の事故等(例えば天災による情報処理技術者試験の中止や延期等)の発生により生じた資金不足が生じた場合、短期借入金の限度額(15億円)の範囲内で借入を行う。

## **VI. 重要な財産の譲渡・担保計画**

なし

## **VII. 不要財産又は不要財産となることが見込まれる財産がある場合には、当該財産の処分に関する計画**

なし

## **VIII. 剰余金の使途**

平成28年度で各勘定に剰余金が発生したときには、翌年度の後年度負担に考慮しつつ、各々の勘定の負担に帰属すべき次の使途に充当する。

- ・ソフトウェアの安全性・信頼性向上に関する業務等の充実
- ・短期の任期付職員の新規採用
- ・人材育成及び能力開発研修等
- ・広報、成果発表会等
- ・情報処理技術者試験の充実・改善、質の向上

## **IX. その他主務省令で定める業務運営に関する事項**

### **1. 施設及び設備に関する計画**

なし

### **2. 人事に関する計画**

- (1) 機構における専門性・特殊性の高い業務を継続していく観点から、ジョブローテーションの実施や職員のキャリアパス形成等を通じ、中長期的視点に立った人材の育成を図る。
- (2) 就職情報サイトの積極的活用や採用説明会の充実等、新卒採用者の確保に向けた採用活動を強化する。

### **3. 中期目標期間を超える債務負担**

- (1) 中期目標期間を超える債務負担については、情報処理技術者試験業務等において当該業務が中期目標期間を超える場合で、当該債務負担行為の必要性・適切性を勘案し合理的と判断されるものについて予定している。

### **4. 積立金の処分に関する事項**

- (1) 主務大臣の承認を受けた積立金については、情報処理技術者試験の制度改正等に係る経費の支出及び第二期中期目標期間中に自己収入財源で取得し第三期中期目標期間へ繰り越した固定資産の減価償却費等に要する費用に充てることとする。

別紙1 予算

別紙1-1

予算(総表)

(単位:百万円)

区別	金額
収入	
運営費交付金	7,247
国庫補助金	798
受託収入	194
業務収入	2,869
その他収入	36
計	11,145
支出	
業務経費	11,653
受託経費	194
一般管理費	1,090
計	12,937

[人件費の見積り]

平成28年度には1,554百万円を支出する。

但し、上記の額は、役員報酬、職員基本給、職員諸手当、超過勤務手当、諸支出金(法定福利費を除く。)等に相当する範囲の費用である。

[注記]

各別表の「金額」欄の計数は、原則としてそれぞれ四捨五入によっているので、端数において合計とは一致しないものがある。

## 別紙1-2

## 予算(事業化勘定)

(単位:百万円)

区別	金額
収入	
その他収入	0
計	0
支出	
計	-



## 別紙1-3

## 予算(試験勘定)

(単位:百万円)

区別	金額
収入	
業務収入	2,826
その他収入	2
計	2,828
支出	
業務経費	2,478
一般管理費	208
計	2,686

[人件費の見積り]

平成28年度には305百万円を支出する。

但し、上記の額は、役員報酬、職員基本給、職員諸手当、超過勤務手当、諸支出金(法定福利費を除く。)等に相当する範囲の費用である。

## 別紙1-4

## 予算(一般勘定)

(単位:百万円)

区別	プログラム開 発普及業務	情報技術セキュリティ 評価・認証業務	信用保証業務	事業運営業務	合計
収入					
運営費交付金	6,258	107	-	882	7,247
国庫補助金	798	-	-	-	798
受託収入	194	-	-	-	194
業務収入	5	38	-	-	43
その他収入	27	-	7	-	34
計	7,283	145	7	882	8,317
支出					
業務経費	9,023	145	7	-	9,175
受託経費	194	-	-	-	194
一般管理費	-	-	-	882	882
計	9,217	145	7	882	10,251

## [人件費の見積り]

平成28年度には1,249百万円を支出する。

但し、上記の額は、役員報酬、職員基本給、職員諸手当、超過勤務手当、諸支出金(法定福利費を除く。)等に相当する範囲の費用である。

## 別紙1-5

## 予算(地域事業出資業務勘定)

(単位:百万円)

区別	金額
収入	
その他収入	0
計	0
支出	
計	-

別紙2 収支計画

別紙2-1

収支計画(総表)

(単位:百万円)

区別	金額
費用の部	
経常費用	9,066
業務費用	7,413
受託経費	194
一般管理費	1,090
減価償却費	369
収益の部	
経常収益	9,222
運営費交付金収益	5,061
補助金収益	798
受託収入	194
業務収入	2,869
その他収入	7
資産見返負債戻入	292
財務収益	29
純利益(△純損失)	184
前中期目標期間繰越積立金取崩額	-
目的積立金取崩額	-
総利益(△総損失)	184

[注記]

各別表の「金額」欄の計数は、原則としてそれぞれ四捨五入によっているもので、端数において合計とは一致しないものがある。

## 別紙2-2

## 収支計画(事業化勘定)

(単位:百万円)

区別	金額
費用の部	-
収益の部	
財務収益	0
純利益(△純損失)	0
前中期目標期間繰越積立金取崩額	-
目的積立金取崩額	-
総利益(△総損失)	0

## 収支計画(試験勘定)

(単位:百万円)

区別	金額
費用の部	
経常費用	2,651
業務費用	2,358
一般管理費	208
減価償却費	85
収益の部	
経常収益	2,834
業務収入	2,826
その他収入	1
資産見返負債戻入	8
財務収益	1
純利益(△純損失)	184
前中期目標期間繰越積立金取崩額	-
目的積立金取崩額	-
総利益(△総損失)	184

## 収支計画(一般勘定)

(単位:百万円)

区別	プログラム開 発普及業務	情報技術セキュリティ 評価・認証業務	信用保証業務	事業運営業務	合計
費用の部					
経常費用	5,206	157	7	1,045	6,413
業務費用	4,903	145	7	-	5,020
受託経費	194	-	-	-	194
一般管理費	-	-	-	882	882
減価償却費	108	13	-	163	284
収益の部					
経常収益	5,181	157	4	1,045	6,387
運営費交付金収益	4,072	107	-	882	5,061
補助金収益	798	-	-	-	798
受託収入	194	-	-	-	194
業務収入	5	38	-	-	43
その他収入	2	-	4	-	6
資産見返負債戻入	108	13	-	163	284
財務収益	25	-	3	-	28
純利益(△純損失)	0	0	0	0	0
前中期目標期間	-	-	-	-	-
繰越積立金取崩額	-	-	-	-	-
目的積立金取崩額	-	-	-	-	-
総利益(△総損失)	0	0	0	0	0

## 別紙2-5

## 収支計画(地域事業出資業務勘定)

(単位:百万円)

区別	金額
費用の部	-
収益の部	
財務収益	0
純利益(△純損失)	0
前中期目標期間繰越積立金取崩額	-
目的積立金取崩額	-
総利益(△総損失)	0



別紙3 資金計画

別紙3-1

資金計画(総表)

(単位:百万円)

区別	金額
資金支出	15,405
業務活動による支出	10,883
投資活動による支出	2,054
翌年度への繰越	2,469
資金収入	15,378
業務活動による収入	11,405
運営費交付金による収入	7,247
国庫補助金による収入	798
受託収入	194
業務収入	2,869
その他収入	36
投資活動による収入	1,934
当年度期首資金残高	2,324

[注記]

各別表の「金額」欄の計数は、原則としてそれぞれ四捨五入によっているもので、端数において合計とは一致しないものがある。

## 別紙3-2

## 資金計画(事業化勘定)

(単位:百万円)

区別	金額
資金支出	1
翌年度への繰越	1
資金収入	1
業務活動による収入	0
その他収入	0
当年度期首資金残高	1

## 資金計画(試験勘定)

(単位:百万円)

区別	金額
資金支出	3,936
業務活動による支出	2,566
投資活動による支出	120
翌年度への繰越	1,250
資金収入	3,936
業務活動による収入	2,828
業務収入	2,826
その他収入	2
当年度期首資金残高	1,109

## 資金計画(一般勘定)

(単位:百万円)

区別	プログラム開 発普及業務	情報技術セキュリティ 評価・認証業務	信用保証業務	事業運営業務	合計
資金支出	10,128	145	317	882	11,472
業務活動による支出	7,283	145	7	882	8,317
投資活動による支出	1,934	-	-	-	1,934
翌年度への繰越	911	0	310	0	1,222
資金収入	10,128	145	317	882	11,472
業務活動による収入	7,282	145	10	882	8,319
運営費交付金による収入	6,258	107	-	882	7,246
国庫補助金による収入	798	-	-	-	798
受託収入	194	-	-	-	194
業務収入	5	38	-	-	43
その他収入	25	-	10	-	35
投資活動による収入	1,934	-	-	-	1,934
当年度期首資金残高	911	0	308	0	1,219

## 別紙3-5

## 資金計画(地域事業出資業務勘定)

(単位:百万円)

区別	金額
資金支出	25
翌年度への繰越	25
資金収入	25
業務活動による収入	0
その他収入	0
当年度期首資金残高	25