独立行政法人情報処理推進機構
平成29年度計画

独立行政法人

情報処理推進機構

（平成30年2月28日変更）

目次

独立行政法人情報処理推進機構平成29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29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．我が国の経済・社会を支える重要インフラや産業基盤のサイバー攻撃に対する防御力の強化

1－1．平成29年度における重点事項

（1）産業サイバーセキュリティセンターの設立

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いてサイバー攻撃に対する防護力を強化するため、平成29年4月に機構に産業サイバーセキュリティセンターを設立し、官民が共同してサイバーセキュリティ対策の強化を図る。

模擬システムを用いた演習や、攻撃・防御の経験、最新のサイバー攻撃情報の調査・分析などを通じて、社会インフラ・産業基盤へのサイバーセキュリティリスクに対応する人材・組織・システム・技術を生み出していく。

a. 人材育成事業

(a) 社会インフラ・産業基盤をもつ企業・機関において、所有するシステムのリスクを認識しつつ、サイバーセキュリティ対策だけでなく、所有する個人情報の保護や物理的セキュリティ対策などをも含めた幅広いセキュリティ対策を判断できる人材を育成するプログラムを提供する。

(b) 情報システムから制御システムまでを想定した模擬システム等を使用し、専門家と共に安全性・信頼性の検証や早期復旧の演習を行う。

(c) 制御システム及び情報システムのセキュリティに関する最新の技術・ノウハウを学び、他の業界のセキュリティ責任者や専門家、海外のセキュリティ専門家及び企業・機関との連携を促進するコミュニティを創出し、海外の有益な知見を得る。

(d) 企業などの経営層に対して、サイバー攻撃の実態やセキュリティ対策の必要性を啓発するための機会を提供するとともに、情報発信を行う。

(e) 各種セミナー・短期プログラムの開催を通じて、サイバーセキュリティ経営ガイドライン等を活用した組織強化を促す。

b. 実際の制御システムの安全性・信頼性検証事業

(a) 機構のセキュリティセンターと連携し、我が国の社会インフラ・産業基盤に係る制御システムの安全性・信頼性に関するリスク評価を行う。

c. サイバー攻撃情報の調査・分析事業

(a) 機構のセキュリティセンターと連携し、最新のサイバー攻撃情報を収集する体制を構築する。

② 成果指標

社会インフラ及び産業基盤をもつ事業者等においてサイバーセキュリティの総合的な戦略立案を担う人材を育成するため、100名程度に対し教育と啓発を実施する。
また、運営費交付金及び受講料による収入を財源に当該事業を運営し、事業継続の仕組みを作る。
センターが各事業を実施するにあたっては、利用企業のニーズを把握しつつ、利用企業や関係省庁と協議を行いながら実施する。

2. 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. 平成29年度における重点事項

（1）情報収集・分析手法の拡大

① 事業内容

新たな脅威への対応スピードを高めて、効果的なセキュリティ対策が実施できる体制構築を図るため、他の情報共有体とのインジケータ情報の授受等連携範囲の拡大、グローバルに収集した脅威情報からわが国に対するサイバー脅威や被害傾向を分析、注意喚起情報の効果的な伝達・実行に向けての方策検討などを開始する。

② 成果指標

取組みに応じた成果を、今年度内に公表する。

（2）独法等[1]に対する監視及び監査の実施

① 事業内容

NISC[2] の監督の下、独法等の情報システムの監視を行うとともに、サイバーセキュリティ戦略本部からの委託に基づく助言型の情報セキュリティ監査を行う。

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の運用を行う。
サイバーセキュリティ戦略本部の委託に基づいて、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

重要インフラにおけるサイバーセキュリティ対策強化の更なる推進を図るため、機構の産業サイバーセキュリティセンターと連携し、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上、引き続き重要インフラシステムのリスク分析を行う。

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事業者に対してリスク分析を実施する。

（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

[1]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

[2] 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）

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の共同宣言に基づき、情報セキュリティ対策を呼びかける。具体的には、中小企業自身による自己宣言を証する「Security Action」制度を開始し、また、定期的な呼びかけコンテンツを作成し中小企業関連団体を通じて配信などを行う。

② 成果指標

第1四半期内に「Security Action」制度の受付を開始する。年4回程度、中小企業向けの呼びかけコンテンツを作成し、共同宣言賛同団体を通じて中小企業に配信する。

2－2. 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等の解析・検証環境を整備するとともに、ネット上の情報の収集を行い、「安心相談窓口」に寄せられる情報も併せて、インターネット上で起きている現象の分析及び事例の解析・検証を行うことにより、ノウハウの蓄積を行う。

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. 国民一般からの情報セキュリティ関連相談や問い合わせ対応を、的確にかつ効率的に行う。

b. 「問合せ対応システム」を活用し「情報セキュリティ安心相談窓口」の運用を着実に行い、蓄積した対応事例を問い合わせ対応へ活用しつつ、上記①bで得られたノウハウを元に、適切な解説を伴った「安心相談窓口だより」を発信する。

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[3]）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。また、標的型メールに関連する情報だけでなく、海外の業界動向や標準、ガイドライン等に関する情報共有を開始し、業界ごとの自主的活動を促す。

b. J-CSIPの活動においては、情報提供元の意思を尊重しつつ、他の情報共有体とのインジケータ情報の授受等の連携範囲の拡大について検討を開始する。

c. 「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。

d. 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[4]）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。

e. 従来の手法に加えて、被害組織、攻撃ツール、攻撃者情報などの脅威情報をグローバルに収集し活用

[3] J－CSIP：Initiative for Cyber Security Information sharing Partnership of Japan

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

することにより、わが国に対するサイバー脅威情報や被害の傾向を分析することにより、サイバー攻撃被害の低減、拡大防止、傾向予測等を行う。

f. 被害の報告があった組織だけでなく、連鎖的な攻撃の対象となっている組織、さらには攻撃が予想される組織に対するレスキュー・アドバイスが可能となるよう、情報の収集と分析、情報の管理と活用を高度化するスキームの検討を開始する。

g. 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等の原因究明調査を実施する。

（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[5]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、製品開発者(ソフトウェア製品及び組込み機器)に提供する。

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検討する。

e. 改訂後の「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」に基づき、適切かつ迅速な処理を進め、情報の優先提供の試行を開始する。

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[6]」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。

b. 脆弱性対策情報の公開にもかかわらず攻撃被害が少なからず生じえるという課題の解決を図るため、実際の対策実施への連携方策の可能性について検討する。

（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。（2－1（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、制御システムのリスク評価業務の実施とその手法の業界への普及を図る。

b. 平成28年度に3業界で実施した重要インフラシステムのリスク分析、セキュリティテストを通じて抽出した

---

[5] Japan Computer Emergency Response Team Coordination Center（一般社団法人 JPCERT コーディネーションセンター）

[6] 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。

ノウハウを文書化し、当該各業界で共有可能な「業界向けリスク分析用標準テンプレート」を作成する。

c. 産業サイバーセキュリティセンターと連携し、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上、引き続き重要インフラシステムのリスク分析を行う。

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。

（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。

（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及び調査結果等をもとに、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、各種イベントへの参加、セミナーの開催等を行い、更なる普及啓発に取り組む。

b. 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名以上増加させるとともに、登録したプレゼンターが活躍する地域で自主的に開催するセミナー等を支援することにより、自主的普及活動の新規開拓を図る。

c. 公的機関、団体及び地域等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。

d. 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。

e. 児童・生徒への情報セキュリティの普及啓発を目的に標語、ポスター等の作品制作、学校全体としての取り組み事例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、教育委員会等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。

f. 全国の民間団体の協力を得て、スマートフォン・SNS[7]・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。また、海外からの旅行者に向けた情報セキュリティに関する注意点についての検討を開始する。

g. 中小企業における情報セキュリティ対策の自発的な実施の促進のため、共同宣言参加団体等関連各団体との連携を図りつつ、以下の活動に取り組む。（2－1（4）参照）

(a) 自己宣言制度の周知を図り宣言企業の拡大に取り組む。

(b) 情報セキュリティに関する情報の定期的周知先の拡大を図る。また、セミナー等の機会を通じて中小企業に対し、「中小企業の情報セキュリティ対策ガイドライン[8]」の情報を提供し普及を図るとともに、組織内

[7] ＳＮＳ：Social Networking Service の略

[8] https://www.ipa.go.jp/files/000055520.pdf

指導者の育成等に取り組む。

(c) 中小企業の情報セキュリティの取り組み事例を収集し、模範となる先進的な事例について普及を図る方策について検討する。

h 情報セキュリティ支援システムを運営し、企業内で研修等に活用できる学習ツール、自社の状況を確認できる分析ツールを整備・提供する。

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、情報セキュリティ対策や、サプライチェーンリスク等新たなリスクへの対応を含む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を実施する。

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及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、今後起こりうる新たなサイバーセキュリティ脅威に関する調査を実施する。

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及び倫理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2017」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、ガイドラインの適用範囲拡大に関する調査を実施する。

c. 世界の公的な研究機関においてどのような情報管理およびセキュリティ管理を実施しているかについて調査を実施する。

④ 米国商務省国立標準技術研究所(NIST[9])、韓国インターネット振興院(KISA[10])等の各国の情報セキュ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. NIST、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。

⑤ 各種相談窓口、情報共有の仕組などにより収集した情報を分析し、効果的な活用を検討する。また、政策目標や社会課題に資するために必要な情報の収集・分析を行う。また、外部に対する発信機能の強化を図るべく、平成29年度は体制や仕組みの検討に着手する。

(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。

[9] NIST：National Institute of Standards and Technology の略

[10] KISA：Korea Internet & Security Agency の略

c. ITセキュリティ評価及び認証制度の関係者へのヒアリング結果や過去の認証実績の分析結果を踏まえた認証機関の短縮や手続きの改善に努める。

d. 海外のITセキュリティ評価及び認証制度について、関連する法律及び政府の施策も含め、制度の現状、動向、効果等について調査する。

② セキュリティ製品や暗号モジュールの認証、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[11]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[12]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。

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. 業務管理ソフトウェアの調整を継続し、NISTとの共同認証の環境整備を進める。同時に普及策を検討するためにJCMVPの利用状況・課題などを整理・調査する。

b. JCMVP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、欧米関連団体と連携し、関連技術文書を作成する。

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。

e. 海外の暗号モジュール試験及び認証制度について、関連する法律及び政府の施策も含め、制度の現状、動向、効果等について調査する。

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[13]」を満たすように、調達する機器等のセキュリティ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[14]」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[15]の情報提供を実施する。

（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[16]の事務局を引き続き務めるとも

---

[11] 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。

[12] ＣＣＲＡ（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。

[13] http://www.nisc.go.jp/active/general/pdf/kijyun28.pdf

[14] http://www.meti.go.jp/policy/netsecurity/cclistmetisec2014.pdf

[15] プロテクションプロファイル：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

[16] CRYPTREC（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。

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、既作成の暗号に関する運用ガイドラインの改定案を作成する。また、新たに整備すべき暗号の運用ガイドラインの検討を行う。

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を継続実施する。

d. NICT[17]と共同でCRYPTRECシンポジウム2017を開催しCRYPTRECの活動成果を報告する等、暗号に関する成果の普及を行う。

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[18]と毎年定期協議を行う。

3. 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～

3－1. 平成29年度における重点事項

（1）IoT[19] 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[20]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[21]」を様々な産業分野に展開する。具体的には、「つながる世界の開発指針」そのもの、あるいはこれを参考とした「IoTセキュリティガイドライン[22]」（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）を様々な産業分野や団体の標準仕様等に反映させるべく積極的な提案活動を実施する。

また、様々な製品とつながる IoT 製品やシステムのセーフティやセキュリティを担保することを主眼とする国際規格を策定すべく、日本からの標準化提案に向けた準備作業を行う。

さらに、IoT 時代の製品やシステムの高信頼化に向けて、開発した製品やシステムが開発指針に沿っているかを試験時に確認する際の考慮すべき事項について、外部有識者の知見を得て取りまとめる。

② 成果指標

「つながる世界の開発指針」を様々な産業分野に展開するために、平成28年度においては首都圏を中心に活動したが、平成29年度においては地域・中小の100以上の団体や企業に対して「『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）」、「つながる世界の開発指針チェックリスト」及び「つながる世界の利用時の品質」を用いて、個別訪問による説明及びセミナー等での講演を実施することにより、

---

17 National Institute of Information and Communication Technology（国立研究開発法人情報通信研究機構）

18 JIWG（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

19 Internet of Things(モノのインターネット)

20 「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

21 http://www.ipa.go.jp/files/000054906.pdf

22 http://www.meti.go.jp/press/2016/07/20160705002/20160705002-1.pdf

同開発指針及び同ガイドラインを広く周知する。併せて、平成28年度に計画した「当該開発指針を第3期中期目標期間終了までに4以上の産業分野や団体の標準仕様等に反映させる」という目標は平成28年度に達成したところであるが、平成29年度においては重要インフラ分野等にも注力しつつ、さらに2以上の産業分野や団体の標準仕様等に反映する。

また、IoT 製品やシステムの利用時のセーフティやセキュリティを確保するために、開発時にセーフティやセキュリティを担保することを主眼とする国際規格の策定に向けて、提案内容の素案を作成する。

さらに、開発した製品やシステムが開発指針に沿っているかを試験時に確認する際に考慮すべき事項を取りまとめ、「IoT 時代の製品・システムの試験確認のためのガイド」（仮称）として公開する。

（2）システム構築能力の強化（～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、要求が複雑化する、あるいは従来想定していないリスクの発生等の課題が生まれてくる。例えば、システムの設計当初に製品同士をつなげる際の要件の想定不足や、つながった際の影響の想定不足などの課題があり、こうした変化に対応しつつ効果的なシステム構築が行えるよう、複雑なシステム全体を俯瞰できる手法や多様な要求をもれなく効果的に仕様に落とし込む手法等の導入を通じ上流工程に重点を置いてシステム構築能力を強化していく必要がある。そのため、システムの設計当初の想定不足を最小化するために、システム全体を俯瞰し、上流工程からシステムの動作を検証しつつ品質を作りこむことができるシステムズエンジニアリング [23] について、平成28年度に企業・団体の経営層に認知と重要性の認識を促すために作成した「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」や「開発者のためのシステムズエンジニアリング導入の薦め」を用いて、それを導入するための提案活動を行う。

また、我が国の開発現場の実務者がシステムズエンジニアリングの導入にあたって直面する障壁をあらかじめ取り除いておく必要があることから、開発現場でのシステムズエンジニアリングの有効性確認や課題発掘を行うことを通じて、我が国企業等がシステムズエンジニアリングを導入する際の課題や解決策を明確化するとともに、システムズエンジニアリングの実践に向けて、企業等への導入を推進すべく、実務に役立つ教材を作成する。

さらに、人工知能、ブロックチェーン [24] やビッグデータ [25] 技術等、新たな情報技術が登場しているところであるが、それらの技術導入がもたらすセキュリティ・セーフティ・信頼性向上のインパクト、コストや利便性の影響等について評価を行うことが困難であることが、導入の大きな障壁となっていると考えられることから、システム構築能力強化の一環として、上述の評価の実現可能性について検討を行う。

② 成果指標

個別訪問による説明及び外部団体主催や機構主催のセミナー等での講演を実施し、100以上の団体や企業等に対して「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」や「開発者のためのシステムズエンジニアリング導入の薦め」を用いて、システムの上流工程の強化及びシステムズエンジニアリングの導入の必要性を周知する。

また、システムズエンジニアリングを適用したパイロットプロジェクトを実施してその有効性評価を行い、実

[23] 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

[24] 分散しているコンピュータにデータを分散することで、中央集権的な第三者機関を置かずに、安全に破壊・改ざんが困難なネットワークを作る技術 (http://www.meti.go.jp/meti_lib/report/2016fy/000323.pdf 平成 27 年度総合調査研究グローバル財務戦略に関する調査研究報告書)

[25] 広く、深く、速いデータ処理とそれに伴うアクションを可能にする、インターネット上にあるデータ、またはセンサー、無線タグ、SNS 等から生じる膨大なデータ

践上の課題とその解決策を検討して報告書として取りまとめるとともに、システムズエンジニアリングの教材として「システムズエンジニアリング解説書（入門編）」（仮称）を作成する。
さらに、新技術の評価体制構築に向け、技術領域を特定した上で、評価指標または評価方法の検討を行う。

（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 [26] にて示された組込みソフトウェア産業に関する構造転換を促進するための技術者の能力向上等の取組を促進する。
具体的には、組込みソフトウェアの組み込まれた製品やシステムを開発において必要とする技術手法等の活用促進の観点から、組込みセキュリティ・セーフティ設計方策、組込みスキル標準、コーディング規約策定、定量データ収集等の活動を推進する。
また、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、平成28年度に引き続き、我が国における組込みソフトウェア産業の実態を調査・分析する。

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、その結果が関係省庁等における政策の検討資料となることを目指す。

3－2. 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28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28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28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、平成28年度までに収集したデータに加えて、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・分析の強化を継続するとともに、その結果を取りまとめた「組込みソフトウェア開発データ白書」を発行する。（3－1（3）参照）

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28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27年度実績：83%）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28年度と同程

[26] 「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⑧」

度またはそれ以上とする。（中期目標：35%以上、平成27年度実績：52%）

（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 「つながる世界の開発指針」を様々な産業分野に展開するために、地域・中小の100以上の団体や企業に対して「『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）」、「つながる世界の開発指針チェックリスト」及び「つながる世界の利用時の品質」を用いて、個別訪問による説明及びセミナー等での講演を実施することにより、「つながる世界の開発指針」及び「IoTセキュリティガイドライン」を周知する。また、重要インフラ分野等にも注力しつつ、さらに2以上の産業分野や団体の標準仕様等に反映する。さらに、開発した製品やシステムが開発指針に沿っているかを試験時に確認する際に考慮すべき事項を、取りまとめ、「IoT時代の製品・システムの試験確認のためのガイド」（仮称）として公開する。（3－1（1）参照）

（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時代には、短時間でのシステム開発やシステムの柔軟な変更に容易に対応できる開発手法が必要である。これを具現化した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。

② ソフトウェア工学の振興、産業振興に寄与するため、大学等に対して安全安心なシステムの設計・開発に係る実践的なIT人材育成のための教材等開発を公募し、「つながる世界の開発指針」の実装に向けた実践的な教材等を開発し、それらを用いた講座を実施することで教材等を評価する。

（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[27]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」の整備を継続するとともに、分野別語彙の開発を進める組織と協調し、共通語彙基盤の適用分野拡大と普及を図る。情報連携用基本語彙データベースと、その活用を支援するツールの構築を進め、自治体等を現場とする実証実験等で検証し運用を開始する。これら成果を “imi.go.jp”サイトから統合的に提供し、情報連係に不可欠な基本情報を安定的に提供する基盤として整備を進めるとともに、セミナー等の普及活動を行う。

b. 文字情報基盤

行政機関が情報処理をするために必要な人名漢字等の文字情報を提供するデータベースの機能強化を実施し、情報連携に不可欠な基本情報として”imi.go.jp”サイトから統合的に提供する。漢字・変体仮名の符号化に係る国際標準化作業を完了させ、そのフォローアップと成果普及を推進する。

[27] CIO : Chief Information Officer の略

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 NIST、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[28]）、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[29]）、欧州MISRA[30]等の海外の代表的機関との意見交換を行う。

② IoT製品やシステムの利用時のセーフティやセキュリティを確保するために、開発時にセーフティやセキュリティを担保することを主眼とする国際規格の策定に向けて、提案内容の素案を作成する。（3－1（1）参照）

（5）システム構築における上流の機能強化（3－1（2）参照）

① 個別訪問による説明及び外部団体主催や機構主催のセミナー等での講演を実施し、100以上の団体や企業等に対して「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」や「開発者のためのシステムズエンジニアリング導入の薦め」を用いて、システムの上流工程の強化及びシステムズエンジニアリングの導入の必要性を周知する。

また、システムズエンジニアリングを適用したパイロットプロジェクトを実施し、その有効性評価を行うとともに、実践上の課題とその解決策を検討し、報告書として取りまとめる。
さらに、システムズエンジニアリングの教材として、「システムズエンジニアリング解説書（入門編）」（仮称）を作成する。

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[31]（システム理論に基づく事故モデル）について、セキュリティへの適用対象拡大を検討する。また、これまでの検討結果を取りまとめた、STAMPを実践していくための具体的な手順や技法を日本の開発現場に合わせて解説した「はじめてのSTAMP／STPA」の産業界への普及拡大を図る。

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、平成28年度に整理した、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）をまとめたガイドブックの普及促進を図る。また、システム再構築パターンの追加や非機能要件定義などのノウハウの収集・分析を継続し、ガイドブックの改訂等を行う。

④ 従来セーフティを中心に確保してきた制御システム等へのセキュリティ要求の高まりに対応するため、セーフティとセキュリティの両面から当該システムに求められる要件をすり合わせ、整理していく等の設計における検討手順を取りまとめたガイドブック等を作成する。（3－1（3）参照）

---

[28] ＳＥＩ：Software Engineering Institute の略

[29] IESE : Institute for Experimental Software Engineering の略

[30] MISRA：Motor Industry Software Reliability Association の略

[31] Systems-Theoretic Accident Model and Processes の略

4. 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～

4－1. 平成29年度における重点事項

（1）未踏IT人材発掘・育成事業及び未踏アドバンスト事業の実施

① 事業概要

若く突出した才能を有するIT 人材が、その有する独創性やポテンシャルの高いアイデアを、担当プロジェクトマネジャー（担当PM）から独自の指導を受けながら実現化していく「未踏事業」の実施を通じ、引き続き若く突出したIT人材の育成を目指す。未踏事業への応募を拡大するため、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29年度においては、大学教員等への未踏事業の個別説明を定常的に実施するなど、未踏事業への応募件数増加に努める。

また、技術シード（製品・サービスのプロトタイプ等）をビジネスにつなげたいという強い志を持つ未踏事業を修了したIT 人材等に対して、専属プロジェクトマネージャー（専属PM）と各分野の専門家による指導を行い、起業・事業化を支援する新たな取り組みとして未踏アドバンスト事業を実施する。

② 成果指標

大学等の個別説明会を30回以上（平成28年度実績：25回）開催し、これまで応募がなかった大学等からの応募も目指しつつ未踏事業への応募件数130件以上を目指す。また、未踏アドバンスト事業においては、2件以上の支援を行う。

（2）セキュリティ・キャンプの開催

① 事業概要

学生を対象とした情報セキュリティ人材の発掘・育成のため、4泊5日の合宿形式でセキュリティ・キャンプ全国大会を開催するとともに、1日間の専門講座等の形式でセキュリティ・キャンプ地方大会を開催する。

特に全国大会では、セキュリティを意識したプログラミングの講義を新設することで、開催規模の拡充（50名→80名）を図る。

② 成果指標

セキュリティ・キャンプ全国大会及び同地方大会の開催を通じて、延べ210名以上の修了生の輩出を図る。

（3） 国家資格「情報処理安全確保支援士」制度の着実な運営及び活用促進

① 事業概要

平成28年10月に創設された国家資格「情報処理安全確保支援士」制度の実施機関として、情報処理安全確保支援士試験の実施（年2回）及び問題作成、登録申請の受付・審査、登録簿への登録、登録情報の公開を行うとともに、情報処理安全確保支援士向けの講習を行い、制度の着実な運営に努める。

また、登録者数の更なる増加及び企業等における制度活用促進に向け、制度概要に加え、情報処理安全確保支援士が担う役割モデルや活躍の場などに関するプロモーション活動を実施する。

② 成果指標

情報処理安全確保支援士が担う代表的な役割モデルを3種以上構築するとともに、本制度の企業認知度50%以上を達成する。

4－2. 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 若く突出した才能を有するIT人材を育成する観点から、引き続き「未踏事業」を実施する。（4－1（1）参照）

② 技術シード（製品・サービスのプロトタイプ等）をビジネスにつなげたいという強い志を持つ未踏事業を修了したIT人材等を公募により採択し、専属PMと各分野の専門家による指導と技術シードの磨き上げに要した作業時間を資金援助し、起業・事業化を支援する新たな取り組みとして、未踏アドバンスト事業を実施する。（4－1（1）参照）

③ 一般社団法人未踏等の外部団体と連携し、または独自に取り組み、若い突出したIT人材による成果等をイベント、交流会、ビジネスマッチング等を通じて産業界に発信するとともに、起業・事業化に向けたコミュニティ活動の強化を図る。

（1－2） 特定の優れた技術を持ったIT人材の発掘・育成

① 学生を対象とした情報セキュリティ人材の発掘・育成のためにセキュリティ・キャンプ全国大会及びセキュリティ・キャンプ地方大会を開催する。（4－1（3）参照）

② 情報セキュリティに関する講演会の開催等を通じて、セキュリティ・キャンプの修了生に対して、参加後のフォローアップを図る。

（1－3） ITによる新事業創出起業家支援（先進的IoTプロジェクト支援事業）

① ITの利活用による新事業を創出する起業家・事業家支援を引き続き実施し、新たな価値創造を担う人材を育成する。

② 公募採択した先進的なIoTプロジェクトに対して資金支援およびメンター（PM、専門アドバイザ）による伴走支援によるサポートを行い、各プロジェクトがモデル事業[32]として設定した成果目標を達成することを目指す。事業実施にあたっては、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。

（1－4） 地域の IT ビジネス創出人材の育成支援（地方版IoT推進ラボ支援事業）

① 経済産業省が実施する地方版 IoT 推進ラボの選定に協力するとともに、選定された地方版 IoT 推進ラボのプロジェクト [33]（以下「ラボプロジェクト」という。）において行う、IoT に関する知見を向上させるために行われるセミナーへの講師派遣や、新ビジネス創出に向けてのメンター派遣などを、各ラボプロジェクトの支援ニーズに応じて実施する。

② 支援に際しては、各ラボプロジェクトの情報発信・情報共有を目的としたポータルサイトの運用、ラボプロジェクト間の交流・連携を目的としたイベントの開催等、各ラボプロジェクトの活動を活性化させる仕組みを併せて構築し、各ラボプロジェクトが設定した成果目標を達成するようサポートする。

（2） 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

[32] 製品・サービスの展開地域または時期等を模範的に事業化して展開し、その効用を確認し評価する事業

[33] IT の利活用により地域課題の解決に資する人材を発掘・育成する、自治体を中心とした地域連携組織

（2－1）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 情報セキュリティ人材（情報処理安全確保支援士を含む。）の育成及び活用促進に向け、業界団体等の取組と連携し、企業等におけるセキュリティに関する業務とそれに対応する役割の明確化、セキュリティ人材の育成モデル、教育プログラム構築に向けた検討を行うとともに、その成果を活用したプロモーション活動を実施する。

②平成28年10月に創設された国家資格「情報処理安全確保支援士」制度の実施機関として、登録申請の受付・審査、登録簿への登録、登録情報等の公開を行うとともに、情報処理安全確保支援士向けの講習を行い、制度の着実な運営に努める。また登録者数の更なる増加及び企業等における制度活用促進に向け、制度概要に加え、情報処理安全確保支援士が担う役割モデルや活躍の場などに関するプロモーション活動を実施する。（4－1（3）参照）

（2－2） 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 2016年度のIT人材動向調査を取りまとめた「IT人材白書2017」を発行するとともに、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等を踏まえ、「IT人材白書2018」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）情報処理技術者試験及び情報処理安全確保支援士試験の実施等

① 平成29年度情報処理技術者試験、情報処理安全確保支援士試験として春期試験（4月）、秋期試験（10月）及びCBT[34]方式によるiパス（ITパスポート試験（随時））を着実に実施する。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、試験委員会の体制強化に伴い、新たに委嘱した試験委員と、知見や意識等の共有を図る。

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及びiパスをはじめとする情報処理技術者試験、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、試験の活用の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 「iコンピテンシ ディクショナリ（iCD）」について、昨年度に引き続きタスク・スキルの追加、改訂を行い「iCD 2017」として公開する。また、iCD活用システムについては、5年計画の最終年度分（データアップロード機能、別冊管理機能等）の設計・構築を完了させ、第4期中期計画での継続運用に向けた運用計画策定と運用に必要な機能の開発等を行う。

[34]ＣＢＴ：Computer Based Testing（コンピュータを利用して実施する試験方式）

（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 平成30年4月に設立を予定している「民間主体による新協会（仮称）」への活用促進業務移行を踏まえ、平成29年度は移行対象業務を整理し移行準備を整える。

② 平成28年度において、欧州におけるiCDを活用した新たなフレームワークの実験的な構築や、米国で開発された知識体系（BOK）との相互参照など海外連携が急速に進展したことから、平成29年度においても引き続き、国内企業のグローバル展開の際のiCD活用を目的として、米欧を中心とした海外関連機関との連携を図る。

③ 第4次産業革命に対応した新たなスキル標準の策定及び継続的な拡充を図るための運営体制の整備に向けた検討を行う。具体的には、新たなスキル標準に関する実証調査の実施、調査結果を踏まえた改訂を行うといった継続サイクルを構築する。

（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 産学連携による高等教育機関における実践的なIT人材育成支援事業については、民間を含めた情報ハブ機能の実施体制として、産学の主体的な活動による「高度IT人材育成産学連絡会」への参画を引き続き行う。

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29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29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29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29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。また、新任職員向けの研修を強化する。

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開催等により、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 平成28年度に実施したリスク管理、コンプライアンスの取組を整理し、機構全体の内部統制活動として体系化の上、平成29年度以降の継続的活動として計画し、内部統制活動の定着を図る。

（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、年度内での計画的執行を徹底し、予期せぬ会計基準第81条第4項の振替額の発生を抑制する。

（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開発・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件以上の報道発表を実現したことを受け、引き続き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。

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。また、第4期中期目標期間に向けてマスメディアに加えた新たな情報発信手段を踏まえた広報戦略を立案する。

（5）業務・システムの最適化

① 役職員等の作業を円滑かつ安全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 業務効率の更なる向上を目的とした、基幹業務システムの機能強化を進める。

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。

（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）調達の適正化

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 高度サイバー攻撃などによる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。

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、保証先の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29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開催等により、新卒採用者の確保に向けた採用活動の強化を図るとともに、事業推進の観点から専門知識等のスキルを有する者の中途採用を行う。

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

なし

別紙

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	5,712
国庫補助金	848
受託収入	433
業務収入	5,892
その他収入	18
計	12,903
支出	
業務経費	13,107
受託経費	433
一般管理費	1,126
計	14,666

［人件費の見積り］

平成29年度には2，239百万円を支出する。

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	3,386
その他収入	2
計	3,388
支出	
業務経費	3,007
一般管理費	209
計	3,216

［人件費の見積り］

平成29年度には400百万円を支出する。

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	4,673	123	－	916	5,712
国庫補助金	848	－	－	－	848
受託収入	433	－	－	－	433
業務収入	2,485	22	－	－	2,507
その他収入	9	－	7	－	16
計	8,448	145	7	916	9,516
支出					
業務経費	9,949	145	7	－	10,100
受託経費	433	－	－	－	433
一般管理費	－	－	－	916	916
計	10,382	145	7	916	11,450

［人件費の見積り］

平成29年度には1，839百万円を支出する。

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	15,203
業務費用	11,111
受託経費	433
一般管理費	1,126
減価償却費	2,533
収益の部	
経常収益	15,369
運営費交付金収益	5,712
補助金収益	848
受託収入	433
業務収入	5,892
その他収入	5
資産見返負債戻入	2,479
財務収益	13
純利益（△純損失）	179
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）	179

［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

別紙2－3

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	3,216
業務費用	2,944
一般管理費	209
減価償却費	62
収益の部	
経常収益	3,394
業務収入	3,386
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)	179
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)	179

別紙2－4

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	10,900	146	7	934	11,986
業務費用	8,015	145	7	－	8,166
受託経費	433	－	－	－	433
一般管理費	－	－	－	916	916
減価償却費	2,452	1	－	17	2,471
収益の部					
経常収益	10,891	146	4	934	11,974
運営費交付金収益	4,673	123	－	916	5,712
補助金収益	848	－	－	－	848
受託収入	433	－	－	－	433
業務収入	2,485	22	－	－	2,507
その他収入	－	－	4	－	4
資産見返負債戻入	2,452	1	－	17	2,471
財務収益	9	－	3	－	12
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	28,226
業務活動による支出	12,732
投資活動による支出	13,736
翌年度への繰越	1,758
資金収入	28,226
業務活動による収入	12,906
運営費交付金による収入	5,712
国庫補助金による収入	848
受託収入	433
業務収入	5,892
その他収入	20
投資活動による収入	1,934
当年度期首資金残高	13,387

［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

別紙3－3

資金計画(試験勘定)

(単位:百万円)

区別	金額
資金支出	4,638
業務活動による支出	3,216
投資活動による支出	－
翌年度への繰越	1,421
資金収入	4,638
業務活動による収入	3,388
業務収入	3,386
その他収入	2
当年度期首資金残高	1,250

別紙３－４

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	22,184	145	317	916	23,562
業務活動による支出	8,448	145	7	916	9,516
投資活動による支出	13,736	－	－	－	13,736
翌年度への繰越	0	0	310	0	310
資金収入	22,184	145	317	916	23,562
業務活動による収入	8,448	145	10	916	9,518
運営費交付金による収入	4,673	123	－	916	5,712
国庫補助金による収入	848	－	－	－	848
受託収入	433	－	－	－	433
業務収入	2,485	22	－	－	2,507
その他収入	9	－	10	－	19
投資活動による収入	1,934	－	－	－	1,934
当年度期首資金残高	11,802	0	308	0	12,110

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