独立行政法人情報処理推進機構
平成30年度計画

独立行政法人

情報処理推進機構

（平成31年2月27日変更）

目次

独立行政法人情報処理推進機構平成30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30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セキュリティ対策の強化

1－1．平成30年度における重点事項

（1）重要インフラ関連企業におけるサイバーセキュリティ対策強化

① 事業内容

サイバー情報共有イニシアティブ（J－CSIP）への参加業界・組織の拡大、共有情報の充実を図るとともに、関係省庁や機構の産業サイバーセキュリティセンターと連携し、リスク分析実施支援等を行うことにより、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さらなる推進を図る。

② 成果指標

平成30年度において、機構が提供・共有する情報や支援等を通じて、情報セキュリティ対策強化に向けた新規・追加の取組を実施した重要インフラ関連企業数を100社以上とする。

（2）中小企業におけるセキュリティ対策意識の向上

① 事業内容

中小企業が関連する様々な団体や制度等との連携を図りつつ、セキュリティ対策に関する情報提供やセミナー開催支援等を通じて、対策実施の重要性の理解促進を図り、中小企業の自発的な取組を推進する。

② 成果指標

平成30年度終了時点において、「SECURITY ACTION 制度」に参画する中小企業数を5，000社以上とする。

（3）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 事業内容

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) 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。

(e) 企業や産業における具体的な取組が着実に行われていくように、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、上述の事業内容について情報発信を行う。

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)情報収集分析環境構築を完了し本格的な調査分析業務を開始、受講者等へのサイバーセキュリティに関する最新情報等を提供する。

② 成果指標

平成30年度に実施する人材育成プログラムについて、社会インフラ・産業基盤における産業サイバーセキュリティの状況を踏まえながら、プログラムの改修・新規開発等による受講者数拡大への取組を進めつつ、平成29年7月開講の第一期中核人材育成プログラムを超える受講者数として76名以上を確保する。

また、平成30年6月に第一期中核人材育成プログラムが閉講することを踏まえ、同プログラムを始め、産業サイバーセキュリティセンターの人材育成プログラムの受講者コミュニティの形成を進めつつ、企業や産業における演習実施、ポリシー策定、組織変更その他及びこれらに関する企画・提案等の取組の実施状況を把握および促進するためのフォローアップの仕組みを構築しつつ、少なくとも第一期中核人材育成プログラムの受講者76名の約2／3が年度内に具体的なアクションを起こすと想定し平成30年度において当センターの人材育成プログラムの受講者によって50件の具体的な取組がなされることを目標とする。

1－2. 着実に取り組む事項

（1）あらゆるデバイス、システム、媒体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）サイバーセキュリティ上の脅威への対応

① 深刻化、増大する標的型攻撃や新種のマルウェア等によるサイバー攻撃に対して、攻撃情報の共有体制を強化・拡大させる。また、被害発生時における初動対応措置や対応策検討の支援を行うとともに、脅威やサイバー攻撃の傾向を予測し、被害の未然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）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、サイバー攻撃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継続し、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継続する。

c. 「標的型サイバー攻撃の特別相談窓口」の運営を通じ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）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. 脅威やサイバー攻撃の傾向を予測し、被害の未然防止のための措置等高度な対策等の提案、中長期的に発生し得る事象の発信等を図るため、被害組織、攻撃ツール、攻撃者情報などの脅威情報の収集チャネルを拡大し、わが国に対する脅威や被害傾向の分析能力の向上を図る。

f. 分析した結果得られるわが国に対するサイバー脅威情報や被害傾向は、J－CRATの助言品質及び即応性の向上、J－CRAT及び機構から発信する注意喚起情報等に活用する。

② 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、インター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、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い、国民一般に対しタイムリーな情報提供を行う。

③ 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、機構以外の相談組織との連携も含め、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②bで得られたノウハウをもとに、適切な解説を伴った「安心相談窓口だより」を発信する。

（1－2）システムの脆弱性に対する適切な対策の実施

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必要とする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. JPCERT／CCとの連携の下、「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、情報の優先提供の運用を開始するとともに、提供先の拡大について検討する。

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 iPediaJVN iPedia」（脆弱性対策情報データベース）及び「My JVN」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 ますます重要性が増大する組込み機器等の脆弱性に関する対策の提示等を行い、対策推進及び普及啓発を行う。

④ 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するとともに、外部組織との連携について調査・検討を行い、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。また、注意喚起のスピード及び質を高めるため、外部組織との連携を含めた注意喚起体制の強化を図る。

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ているという課題を解決するため、国内ウェブサイトの脆弱性をプロアクティブに検出するためのツール開発に向けた検討を行う。

（1－3）社会的に重要な情報システム等に関する対策支援

① 社会的に重要な情報システム等について、関係府省等の求めに応じて、セキュリティ対策状況の確認、サイバーセキュリティ強化等のための調査、各種情報提供、インシデント発生時の原因究明調査等の協力を行う。

② 我が国の社会インフラ・産業基盤に係る制御システムについて、関係府省等の求めに応じて、リスク分析の実施支援を行うとともに、分析手法の浸透を図る。（1－1（1）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、平成29年度に公開した「制御システムのセキュリティリスク分析ガイド」の第2版の作成及び同ガイドの普及活動を実施する。

b. 平成29年度に2業界で実施した制御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ガイド」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（再掲　1－1（3）①）

① 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. 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。

e. 企業や産業における具体的な取組が着実に行われていくように、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、上述の事業内容について情報発信を行う。

② 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。

③ サイバー攻撃情報の調査・分析事業

a. 情報収集分析環境構築を完了し本格的な調査分析業務を開始、受講者等へのサイバーセキュリティに関する最新情報等を提供する。

（3）非技術的要因を踏まえた調査、分析

① 企業・組織・サプライチェーン全体の情報セキュリティリスク管理に関して、経営者やCISO等が取り組むべき事項の実態、事例等を調査、分析・評価し、情報発信する。

a. 企業経営層やCISO、事業部門等が連携し、脅威に柔軟に対応できるセキュリティリスク管理を行うため、既存のセキュリティガイドライン等の活用状況について調査を行い、具体的な実践事例（プラクティス）を提示するとともに、セキュリティ対策状況を可視化するための検討を行う。

b. ICTシステム・サービス調達に関するサプライチェーンのセキュリティリスク管理を企業が効果的に行うための共通なサプライチェーンセキュリティ指針について調査を実施する。

② 新しいIT基盤の活用やデータ利活用における情報セキュリティ確保、データ利用倫理の確立等の社会的要請に応じるため、情報セキュリティ対策、データ利活用における情報保護、プライバシーに関する技術・市場・意識等の調査・分析を行い、情報提供を行う。

a. 「情報セキュリティ白書2018」を編集、作成、出版するとともに、PDF版を公開する。

b. 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。

c. 他者との共有を前提に一定の条件下で利用可能な情報の利活用及び保護・管理方法に関する調査・分析を行い、情報提供を行う。

③ 新しいIT基盤や脅威の傾向を把握し、中長期的に生じうる重大脅威を適切に予測するための基礎的な調査・分析を行う。

a. 情報セキュリティリスク・インシデント被害を適切に把握し、可視化するためのリスク評価手法、指標について既存方式・研究動向の調査を行う。

b. IoT、AI等の急速に普及しているIT基盤に関し、その潜在的なリスク要因が社会基盤への活用等によりどのように増幅されうるかなどの脅威予測に向けた検討を行う。

（4）セキュリティ対策に関する普及啓発、情報提供

① 広く企業及び国民一般に情報セキュリティ対策の重要性を知らしめるため、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う。

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. 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。

c. 関係機関、全国の民間団体等の協力の下、標語、ポスター等の作品制作、学校全体としての取組事例に関するコンクールの実施等により児童・生徒への情報セキュリティの普及啓発、情報モラル向上の啓発に取り組む。

d. 全国の民間団体や関係機関との連携を図りつつ、スマートフォン・SNS・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。

e. 情報セキュリティ啓発サイト及び情報セキュリティ対策支援システムを引き続き運営し、企業内で研修等に活用できる学習コンテンツや資料、自社の対策実施状況を確認できる分析ツールを継続して提供し、広く普及啓発を行う。

② 中小企業による自発的な対策実施の促進を目的に、中小企業と関連する様々な団体や制度との連携を図りつつ、以下の活動に取り組む。（1－1（2）参照）

a. 「SECURITY ACTION 制度」の周知を図り参画企業の拡大に取り組む。

b. 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」の情報を提供し普及を図るとともに、組織内指導者の育成等に取り組む。

c. セキュリティプレゼンター制度を運用し、登録したセキュリティ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、自主的普及活動の拡大を図る。

d.「中小企業の情報セキュリティ対策ガイドライン」について、実用性、実効性の向上に向けた改訂の検討を行い、必要に応じ改訂を実施する。

③ 教育関係者や警察など、個々の現場に近い団体等との連携を拡大させ、機構が提供する情報が必要とされる現場に届き、有効に活用されるように情報提供チャネルの拡大を図る。

④ 国内外のセキュリティ関連機関との連携、国際会議への参加、セキュリティ関連規格の調査等を通じて、情報セキュリティに関する最新情報の収集や技術共有等に取り組むとともに、得られた情報について、機構が行う事業への反映や情報発信等に活用する。

（5）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の利活用推進と評価品質の向上に向けた以下の施策を行う。

a. 認証作業を着実に実施する。また、制度運営において発生する技術面及び手続面の課題については、関係各者と調整し早期の解決を図る。

b. 評価品質の均質化及び評価作業の効率化のため、製品評価におけるテスト手法や脆弱性評定について、国内外の関連団体からの情報を収集し制度関係者との共有を図る。

c. 制度の利用促進のため、政府調達の動向を見据えた新たな製品分野に対するセキュリティ評価に関する試行・情報収集及び情報公開を行う。

d. 制度利用者の視野に立った評価・認証手続の改善を行う。

② 政府調達におけるIT機器等のセキュリティ確保等に資するため、IT機器等のセキュリティ要件、その要件を満たす認証取得製品、その他調達要件等の情報提供を行う。

a. 政府機関や民間企業、組織等がIT製品を調達する際に考慮すべきセキュリティ上の脅威とそれに対抗するためのセキュリティ要件を製品分野毎に定めた「IT製品の調達における要件リスト」の改訂案を策定するとともに、当該リストに掲載する国際標準に基づくセキュリティ要件については翻訳等を行った上で、情報提供を行う。

b. 国際的に共同開発中のセキュリティ要件について、検討を行う会議に機構職員を派遣し日本の意見を反映させる。また、当該セキュリティ要件に基づき認証された製品についても情報提供を行う。

（6）暗号技術の調査・評価

① CRYPTREC暗号リストの適切な維持・管理のため、CRYPTRECの事務局を引き続き務めるとともに、CRYPTREC暗号リストに掲載されている暗号アルゴリズムの危殆化監視活動や暗号技術の適切な利用／運用を促進するための情報提供等を行う。

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、国際会議等に参加し、調査を行う。
b. 暗号アルゴリズムの危殆化監視活動の一環として、大阪大学／JAISTと国際学会ECC2018を共催し、暗号技術に関する最新の研究成果について公開・情報提供を行う。
c. 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（SSL／TLS暗号設定ガイドライン）の改定版を発行・公開し、普及啓発のためCRYPTREC統一WEBサイトや各種展示会等（情報セキュリティExpo等）にて情報提供を行う。
d. 暗号技術の安全な利用を促進するための普及啓発活動として、一般を対象とした暗号技術に関する運用ガイドラインの作成を行う。具体的には、平成30年度は「鍵管理」に関するガイドラインの作成に着手する。
e. 暗号技術の適切な利用／運用を促進するため、これまでCRYPTREC統一WEBサイトにて公開してきた各種ドキュメント類の文書番号を一般に判り易く分類・整理する形でCRYPTREC統一WEBサイトを改訂し、広く一般に公開・情報提供を行う。

② 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を推進する。
a. 業務管理ソフトウェア及び暗号アルゴリズム実装試験ツールの調整を継続し、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. 暗号実装の脆弱性評価、対策技術に関する情報収集、欧米関連団体と連携し、関連技術文書の作成等を行う。
d. 暗号実装の脆弱性評価ツールを活用して、日本国内の開発者、評価機関、大学等の関係者と、暗号実装の脆弱性評価に係る情報共有を図る。
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。

（7）独法等に対する不正な通信の監視、監査等

① NISCの監督の下、独法等の情報システムの監視を実施する。
② サイバーセキュリティ戦略本部からの委託により、独法等の情報セキュリティ監査を実施する。具体的には、マネジメント監査及びペネトレーションテストを実施すると共に、これまでに情報セキュリティ監査を実施した法人に対するフォローアップ監査を実施する。
③ 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。

【平成30年度の評価指標】

中期計画に掲げる指標について、平成30年度においては、以下に定める評価指標を達成しているか否かを総合的に勘案して評価を行う。

① 重要インフラ関連企業におけるセキュリティ対策の強化【基幹目標】（再掲 1－1（1）②）

平成30年度において、機構が提供・共有する情報や支援等を通じて、情報セキュリティ対策強化に向けた新規・追加の取組を実施した重要インフラ関連企業数を100社以上とする。

［重要度高・優先度高・難易度高］

② 中小企業におけるセキュリティ意識の向上【基幹目標】（再掲 1－1（2）②）

平成30年度終了時点において、「SECURITY ACTION 制度」に参画する中小企業数を5，000社以上とする。

［重要度高・優先度高・難易度高］

③ 情報セキュリティ対策の企業への普及促進

平成30年度において、機構が整備、提供する対象者別（一般企業、中小企業、重要インフラ関連企業向け）のガイドライン等の累計普及数を50，000件以上とするとともに、当該ガイドライン等に対する役立ち度について、4段階評価で上位2つの評価を得る割合を3分の2以上確保する。

④ 国民に対するサポート体制構築

平成30年度において、機構が運営する「情報セキュリティ安心相談窓口」との連携組織を1組織以上拡大する。

⑤ 社会インフラ・産業基盤のサイバーセキュリティに係る人材育成プログラムの提供（再掲 1－1（3）②）

平成30年度に実施する人材育成プログラムについて、社会インフラ・産業基盤における産業サイバーセキュリティの状況を踏まえながら、プログラムの改修・新規開発等による受講者数拡大への取組を進めつつ、平成29年7月開講の第一期中核人材育成プログラムを超える受講者数として76名以上を確保する。

⑥ 社会インフラ・産業基盤のサイバーセキュリティリスクに対する取組促進【基幹目標】（再掲 1－1（3）②）

平成30年6月に第一期中核人材育成プログラムが閉講することを踏まえ、同プログラムを始め、産業サイバーセキュリティセンターの人材育成プログラムの受講者コミュニティの形成を進めながら、企業や産業における演習実施、ポリシー策定、組織変更その他及びこれらに関する企画・提案等の取組の実施状況を把握および促進するためのフォローアップの仕組みを構築しつつ、少なくとも第一期中核人材育成プログラムの受講者76名の約2／3が年度内に具体的なアクションを起こすと想定し平成30年度において当センターの人材育成プログラムの受講者によって50件の具体的な取組がなされることを目標とする。

［重要度高・優先度高・難易度高］

2. 高度な能力を持つIT人材の発掘・育成・支援及びネットワーク形成とIT人材の裾野拡大に向けた取組の強化

2－1. 平成30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

① 事業内容

未踏育成期間中にプロジェクトマネージャーによる技術的指導・助言に加え、法務・財務等の起業・事業化に必要な専門知識や知的財産権確保に必要な専門知識等の修得を支援する講義の場を設け、IT人材の経営力の強化を支援する。さらに、プロジェクトマネージャーの助言や紹介等をうけて、企業や投資家等との共同研究や事業マッチング等の機会を提供し、また積極的に活用させ、新たな社会価値創出への行動を支援する。

② 成果指標

未踏関係事業の修了生による新たな社会価値創出を、新技術の創出数（知的財産権に関する出願・登録数や企業等との共同研究・開発テーマ設定数）、新規起業・事業化の資金確保数、ビジネスマッチング成立件数で総合的に捉え、合わせて10件以上とする。

（2）セキュリティ・キャンプ事業

① 事業内容

セキュリティ・キャンプ実施協議会と連携して講師、修了生のネットワーク形成を図るとともに、講師等の候補生をベテラン講師がコーチ、フォローする仕組みを形成し、全国大会および地方大会からの将来有為な人材の活躍を支援する。

② 成果指標

セキュリティ・キャンプ修了者による全国大会及び地方大会の講師・チューター数、各種講演会・勉強会での講師数を合わせて45名以上とする。

2－2. 着実に取り組む事項

（1）優れたIT人材の発掘・育成・支援の実施と活躍の機会の提供

（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（2－1（1）参照）

① ソフトウェア関連分野においてイノベーションを創出することのできる独創的なアイディア、技術を有するとともに、これらを活用していく能力を有する優れた個人を、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う「未踏事業」を実施する。

② 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う「未踏アドバンスト事業」を実施する。

③ 基礎技術や領域横断的技術革新に取り組む未踏的 IT 人材が自らのアイディアや技術力を最大限に活かし将来の経済発展への貢献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う「未踏ターゲット事業」を実施する。

④ IT 人材の早期起業、事業化を加速するため、教育機会・啓発創発機会・人材交流機会を、有機的に連動し

て設ける。

（1－2）若年層の優秀なセキュリティ人材の発掘・育成（2－1（2）参照）

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、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、1～2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。

② 全国大会および地方大会ともに、セキュリティ・キャンプ修了生の中から適切な人材を講師やチューターに登用し、継続的な自己研鑽の場として、また指導者としての経験を深める場としての活用を図る。

（1－3）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 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、情報セキュリティの最新動向や効果的なカリキュラム・研修手法を反映した教材を用いて、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継続して努める。

② 情報処理安全確保支援士の登録者公開情報について、登録情報の取得を容易にするなど更に利便性を高めるため、情報処理安全確保支援士公開システム（仮称）を公開する。

③ 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、情報処理安全確保支援士が担う役割や活躍の場などに関して企業訪問等から事例収集を行い、セミナー開催やSNSによる情報発信等にて公開するとともに、情報処理安全確保支援士が効果的な講習を継続受講できるよう、カリキュラムや研修手法等の調査と教材への展開を行う。

（1－4）優れたIT人材の交流の場の提供等による人的ネットワーク活性化促進

① 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・事業化に向けた講習会や交流の場を提供するなど、コミュニティ活動の強化を図る。

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するセキュリティ人材ネットワークの活性化を図る。

（2）社会の第一線での活躍が見込まれるIT人材の発掘を通じたIT人材の裾野の拡大

（2－1）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30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、サイバーセキュリティ人材を始めとするIT人材の高度化と裾野の拡大、技術の複雑化、利用者ニーズの多様化などITを取り巻く環境変化を踏まえて、試験問題を作成する。また、情報処理安全確保支援士試験の一部免除制度における学科等の審査・認定業務を着実に実施するとともに、本制度の普及に努め、サイバーセキュリティ人材の裾野の拡大と育成に貢献する。

② 産業界・教育界等に対して積極的な広報活動を展開し、情報セキュリティマネジメント試験及びiパスを始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・定着化を推進することで、試験の活用の促進と収益の維持を目指す。

③ 平成30年度における評価指標である「企業における情報処理技術者試験の活用割合」（後掲）の達成状況を確認するため、調査を実施する。

（2－2）情報処理技術者試験のアジア展開

① 情報処理技術者試験のアジア各国試験との同等性に関する相互認証及び相互認証に基づくアジア共通統一試験については、IT人材の拡充策の重要性が増す中、着実に実施する。特にアジア共通統一試験については、更なる定着を図るべく問題作成やプロモーション等の支援を行う。

【平成30年度の評価指標】

中期計画に掲げる指標について、平成30年度においては、以下に定める評価指標を達成しているか否かを総合的に勘案して評価を行う。

① 未踏事業修了生の成果【基幹目標】（再掲　2－1（1）②）

未踏関係事業の修了生による新たな社会価値創出を、新技術の創出数（知的財産権に関する出願・登録数や企業等との共同研究・開発テーマ設定数）、新規起業・事業化の資金確保数、ビジネスマッチング成立件数で総合的に捉え、合わせて10件以上とする。

［重要度高・優先度高・難易度高］

② セキュリティ・キャンプ修了生の活動【基幹目標】（再掲　2－1（2）②）

セキュリティ・キャンプ修了生による全国大会及び地方大会の講師・チューター数、各種講演会・勉強会での講師数を合わせて45名以上とする。

全国大会修了生の中から選定して全国大会および地方大会の講師として講義ができるようにする。チューターには講義補助の機会を通じて、勉強会講師や講演者としての活動へのチャレンジを促す。実施に際してはセキュリティ・キャンプ実施協議会との連携により、修了生講師をベテラン講師がフォローするなど講義の質が担保できるよう考慮する。また、各種講演会や勉強会においてはイベント情報の共有や適時の参加を促すなどの支援を行う。

［重要度高・優先度高・難易度高］

③ 情報処理安全確保支援士の活動

情報処理安全確保支援士（RISS）が保有している知識やスキルを発揮して、情報セキュリティに関連する業務遂行がなされたとする値について、情報処理安全確保支援士（RISS）の登録のきっかけに関する調査結果より20%と仮置きし、平成30年度は30%を達成できるよう活動を推進する。

また、平成30年度中に情報処理安全確保支援士（RISS）に対するアンケートを実施しRISS活躍指標の基礎数値の取得・再設定を行った上で、情報処理安全確保支援士（RISS）の役割や活躍の場などの事例収集を通じて、企業・組織や個人向けの普及策を検討する。その上で必要に応じて平成30年度の目標値を修正し、各年度の達成割合を設定する。

④ 情報処理技術者試験制度の活用

IT人材の裾野拡大を図るため、ITを提供する側だけでなく、ITを利用する側も含めた企業における情報処理技術者試験の活用割合について、平成30年度においては55%以上を目指す。

3. ICTに関する新しい流れを常に捉え、発信していく機能の強化

3－1. 平成30年度における重点事項

（1）Society 5．0 の実現に向けたICTに関する新たな技術動向の調査・発信（～新技術等の社会実装の促進～）

① 事業内容

「未来投資戦略2017[1]」において示された第4次産業革命（IoT、ビッグデータ、人工知能（AI）、ロボット、シェアリングエコノミー等）のイノベーションを、あらゆる産業や社会生活に取り入れることにより、様々な社会課題を解決する「Society 5．0」の実現を推進するために、ICTに関する技術動向（ビッグデータやAI等の新技術）を調査・分析し、社会実装の促進等につながる情報発信を効果的に実施する。

具体的には、新技術として大きく進展しているAIについては、一般企業のAIに対する適切な理解と導入を促進し、社会実装を進めることが重要であり、機構で調査・分析した内容を基に、技術者にとどまらず経営層も視野に入れた有用な情報を発信する。

また、ブロックチェーンやビッグデータ技術等の新たなICTに関する技術を社会実装していく際の課題を抽出し、解決の方向性を提言するために、情報の調査・分析を行う。

② 成果指標

新技術として大きく進展しているAIについて、平成29年度調査事業として実施した「AIの社会実装における課題と対策の動向調査」の結果を基に、経営者に向けた分かりやすいAIの解説や、一般企業の関心が高い、AIの動向、社会実装上の課題と対策などを盛り込んだ、「AI白書2018」（仮称）を発行する。

また、新たなICTに関する技術の社会実装を推進するために委員会等を設置し、技術領域を特定した上で、実装課題の抽出及び課題解決に向けて当該技術領域に対する評価の考え方を整理する。

（2）IoT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（～つながる世界の安全安心と国際標準化の推進～）

① 事業内容

「未来投資戦略2017[2]」において示されたIoTシステムの設計・開発・運用に係る概念等について、国際標準化を積極的に推進するとともに、「日本再興戦略2016」の工程表[3]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」を様々な産業分野に展開するための活動を行う。

具体的には、様々な製品やシステムがつながるIoT社会においては、そのセーフティやセキュリティが重要であるが、特にIoT社会で関心の高いセキュリティに着目し、遵守すべきセキュリティの基本的な枠組みの国際標準化を日本主導で進めることにより、我が国産業界の競争力を強化するとともに、国際的なIoTのセキュリティレベルの向上を目指す。

また、「つながる世界の開発指針[4]」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[5]」（IoT推進

---

1 「未来投資戦略 2017」の第１ ポイント　基本的な考え方　http://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/miraitousi2017_t.pdf

2 「未来投資戦略 2017」の６．サイバーセキュリティの確保　（２）新たに講ずべき具体的施策 http://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/miraitousi2017_t.pdf

3 「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

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

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

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企業の開発現場に適用させるべく、「つながる世界の品質確保に向けた手引き」等を用いて、積極的な普及活動を実施する。

さらに、IoT時代の製品やシステムの高信頼化に向けて、独国フラウンホーファー研究機構実験ソフトウェアエンジニアリング研究所（IESE[6]）と製造分野の IoT 高信頼化に関する実証実験を計画し、その準備を行う。

② 成果指標

IoT製品やシステムのセーフティやセキュリティを確保するために、開発時に特に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、ISO/IEC JTC1[7]/SC27[8]に、「IoTセキュリティガイドライン」を基本としたセキュリティ確保の考え方を提案し、正式なプロジェクトとして成立させる。併せて、ISO/IEC JTC1/SC41[9]に、「安全なIoTシステムのためのセキュリティに関する一般的枠組」を基本としたセキュリティ確保のための方法論も提案し、正式なプロジェクトとして成立させる。

また、「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」を様々な産業分野に展開するために、「つながる世界の品質確保に向けた手引き」等を用いて、個別訪問による説明及び外部団体主催や機構主催セミナー等での講演を実施することにより、IoT時代の製品開発の高信頼化が重要であることを100以上の団体や企業に広く周知する。併せて、当該開発指針や当該手引き等の開発現場での適用推進における課題を把握・整理するため、企業等が自ら開発指針の実施状況を確認できるように指針とポイントを具体的にまとめた「つながる世界の開発指針チェックリスト」、あるいはIoT機器・システムの品質を確保し、維持・改善するという側面から、IoTの品質に係わる考慮事項とポイントをまとめた「つながる世界の品質確保チェックリスト」の適用事例を5件以上確保する。

さらに、IESEと製造分野のIoT高信頼化に関する実証実験の実施計画書を取りまとめる。

3－2. 着実に取り組む事項

（1）ICTの新たな技術等に関する調査分析及び発信

（1－1）ICTに関する技術動向やIT人材に関する動向等の調査・分析及び社会実装の促進等につながる情報発信の強化

① 新技術として大きく進展しているAIについて、平成29年度調査事業として実施した「AIの社会実装における課題と対策の動向調査」の結果を基に、経営者に向けた分かりやすいAIの解説や、一般企業の関心が高い、AIの動向、社会実装上の課題と対策などを盛り込んだ、「AI白書2018」（仮称）を発行する。また、新たなICTに関する技術の社会実装を推進するために委員会等を設置し、技術領域を特定した上で、実装課題の抽出及び課題解決に向けて当該技術領域に対する評価の考え方を整理する。（3－1（1）参照）

② 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」を発行する。また、対象とする開発手法を拡大して新たに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・分析を強化する。

③ 「情報セキュリティ白書2018」を編集、作成、出版するとともに、PDF 版を公開する。（再掲 1－2（3）②）

④ 2017年度のIT人材動向調査を取りまとめた「IT人材白書2018」を発行する。

---

6 IESE : Institute for Experimental Software Engineering の略

7 SO/IEC JTC1（International Organization for Standardization/ International Electrotechnical Commission Joint Technical Committee 1）：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。

8 SC27 は JTC1 傘下の Sub Committee の一つでセキュリティ技術に関する規格の標準化活動を行っている。

9 SC41 は JTC1 傘下の Sub Committee の一つで IoT と関連技術に関する規格の標準化活動を行っている。

また、情報技術の革新や産業界におけるデジタル化が急速に進展してきていることを踏まえ、IT人材を取り巻く動向把握等についての検討を行う。

その他、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の情報発信や新事業支援機関からの要請に基づく機構の成果普及や講師の派遣等を行う。

（1－2）ICTの安全性・信頼性等の脅威となる情報収集・調査・分析

① 新しいIT基盤や脅威の傾向を把握し、中長期的に生じうる重大脅威を適切に予測するための基礎的な調査・分析を行う。（再掲　1－2（3）③）

a. 情報セキュリティリスク・インシデント被害を適切に把握し、可視化するためのリスク評価手法、指標について既存方式・研究動向の調査を行う。

b. IoT、AI等の急速に普及しているIT基盤に関し、その潜在的なリスク要因が社会基盤への活用等によりどのように増幅されうるかなどの脅威予測に向けた検討を行う。

（1－3）組込みソフトウェア産業の抱える課題、開発技術動向、人材育成状況等の調査・分析

① 経済産業省と協力して、「未来投資戦略2017」の工程表[10]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を図るために、組込みソフトウェア産業の実態調査を実施し、アンケート調査により150社以上から適正な回答を得るとともに、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って、分析結果を取りまとめる。

（1－4）IoTによる地域課題の解決や新事業創出に関する取組支援及び地域におけるIoTやICTの技術等の社会実装の推進

① 経済産業省と連携して、地域におけるIoTプロジェクト創出のための取組みを支援するべく「地方版IoT推進ラボ」としてこれまで74地域選定しており、本取組みの展開に向けて新たな地域を選定する。選定地域への人的支援、広報の支援、活動に資する情報の提供・共有を行う。

a. 地域におけるIoTの知見を向上させるため、セミナーへの講師を派遣するとともに新事業創出に向けたメンターを派遣するなど、各地域のニーズに応じて支援を実施する。

b. 選定地域の取組み成果を広く一般に普及するために、ポータルサイトを運営するとともに全国及び地域に根ざした各種イベントに出展する。また、地域間連携を促進するために、選定地域間の交流の場の提供や機会を作る。

c. 地方版IoT推進ラボ事務局及び地域未来投資促進法機構窓口として、各地域とのネットワークを構築し、プロジェクト創出に向けた地域間の情報連携を促進する。

② IoTによる地域課題の解決や新事業創出に向けて、地域団体、公的機関等と連携をして、意見交換会等を実施することにより、IoTやICTの技術等の実装に当たって地域の抱える課題やニーズを把握する。さらに、課題の解決の一助とすべく、地域の特性、関係機関の体制等を踏まえて重点化を図り、計画的にIoTやICTの技術等に関するセミナーへの講師派遣等を行って機構が整備した指針・ガイドライン等を普及展開することで、効果的に地域におけるIoTやICTの技術等の社会実装を推進する。

（2）ICTの新たな技術等に関する客観的な基準・指針・標準の整備及び情報発信

（2－1）ICTに関する新しい技術の社会実装に必要な指針・ガイドラインの整備・見直し及び普及

① IoTの進展等に伴うシステムの高度化に対応するとともにその生産性・信頼性の向上を目指し、現状でも強

10 「未来投資戦略 2017」の工程表　中短期工程表「人材の育成・活用力の強化」⑭
http://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/miraitousi2017_t.pdf

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いて、平成29年度までに整備した「ユーザのための要件定義ガイド」、「システム再構築を成功に導くユーザガイド」等のガイドブック類や改訂した「非機能要求グレード[11]」の普及促進を図る。また、その過程で明らかになる要件定義等の諸課題について更に検討を行い、ガイドブック等に反映する。

（2－2）IoTシステムや組込みソフトウェア等の高度化、生産性・信頼性向上に向けた指針・ガイドライン等の整備及び普及

① IoT製品やシステムのセーフティやセキュリティを確保するために、「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」を様々な産業分野に展開するために、「つながる世界の品質確保に向けた手引き」等を用いて、個別訪問による説明及び外部団体主催や機構主催セミナー等での講演を実施することにより、IoT時代の製品開発の高信頼化が重要であることを100以上の団体や企業に広く周知する。併せて、当該開発指針や当該手引き等の開発現場での適用推進における課題を把握・整理するため、企業等が自ら開発指針の実施状況を確認できるように指針とポイントを具体的にまとめた「つながる世界の開発指針チェックリスト」、あるいはIoT機器・システムの品質を確保し、維持・改善するという側面から、IoTの品質に係わる考慮事項とポイントをまとめた「つながる世界の品質確保チェックリスト」の適用事例を5件以上確保する。さらに、IoT時代の製品やシステムの高信頼化に向けて、IESEと製造分野のIoT高信頼化に関する実証実験の実施計画書を取りまとめる。（3－1（2）参照）

② 「つながる世界の開発指針」の実装に向けて、安全安心なシステムの設計・開発に係る実践的なIT人材を大学等の教育機関で育成するための教材等を開発し、それらを用いた講座を実施して評価し、教材等を改良する。

（2－3）製品・サービスの生産性や信頼性を向上させるための手法・技術の活用及び普及

① IoTやAIなどの技術が進展し、複雑化、多様化してきた近年のシステム開発においては、従来にも増して、システム俯瞰アプローチ（目的指向[12]と全体俯瞰[13]、多様な専門分野の統合[14]などを考慮するシステム開発アプローチ）が重要となる。そのため、システム俯瞰アプローチに対応できる人材育成に寄与するために、目指すべき人材像を明らかにし、その育成に必要となる教材として、「システム俯瞰アプローチの実践演習」（仮称）を作成する。加えて、産業界でのシステム俯瞰アプローチの推進を促すために平成29年度までに整備した「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」、「技術者のためのシステムズエンジニアリング導入の薦め」、「成功事例に学ぶシステムズエンジニアリング」を用いて普及展開を行い、100以上の団体や企業にシステム俯瞰アプローチの重要性を広く周知する。

② ICTシステムの安全性解析や事故分析の手法として米国等で実績があるSTAMP[15]（システム理論に基づく事故モデル）について、平成29年度に開発したSTAMP支援ツールや日本の産業構造や開発プロセスの特徴に配慮して取りまとめた「はじめてのSTAMP／STPA」等のガイドブック等を活用し、幅広い産業分野への普及拡大を図る。

③ ソフトウェア開発の生産性・信頼性の向上を目指し、ソフトウェア開発データ白書を始めとする各種ガイドブック類の活用促進を図るために、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、定量的プロジェ

---

11 システム基盤の可用性や拡張性などの非機能の要求を明確化し、システムを発注する側（ユーザ企業）とシステムを開発する側（開発企業）で合意形成するための手法やツール、ガイド類。

12 解決策を考える前に本来の目的を明確に定義し、常に目的を意識しながら考えるアプローチを指す。

13 視点と視野を変えながら全体を俯瞰して対象を捉えるアプローチを指す。

14 多様な分野（技術、事業、領域、環境、文化、社会など）の知見を統合。

15 Systems-Theoretic Accident Model and Processes の略

クト管理の一層の普及を推進する。

（2－4）重要性の高い基準・指針等の国際標準化への取組

① IoT製品やシステムのセーフティやセキュリティを確保するために、開発時に特に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、ISO/IEC JTC 1/SC27 に、「IoTセキュリティガイドライン」を基本としたセキュリティ確保の考え方を提案し、正式なプロジェクトとして成立させる。併せて、ISO/IEC JTC 1/SC41 に、「安全なIoTシステムのためのセキュリティに関する一般的枠組」を基本としたセキュリティ確保のための方法論も提案し、正式なプロジェクトとして成立させる。（3－1（2）参照）

（2－5）IT スキル標準の継続改善

① デジタルトランスフォーメーション（DX）に向けたスキル変革に資する新たなITスキル標準の拡充を図るため、有識者によるWGを運営し、ITエンジニアの学び直し領域に関するアジャイル領域のDevOpsへの拡充、IoT領域のIT－OTの橋渡し部分の内容検討、DXを推進する人材類型の検討、及び当該人材が必要とする観点からスキル・知識の内容の再構築とメンテナンスを行う。

② ITスキル標準の検討を通じた専門的な知見を活用し、経済産業省が行う「第四次産業革命スキル取得講座認定制度」（通称：「Reスキル講座」）の制度運用に対して必要な支援を行う。

（2－6）官民データの利活用促進のための技術標準等の整備及び普及

① 政府CIO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、官民データ連携のため、情報の共有や活用を円滑に行うための情報共有基盤事業IMI(Infrastructure for Multilayer Interoperability:)を進める。

a. 基礎データ、基礎技術の検討・開発

基礎データとなるコア語彙の改良・分野別語彙の整理、基礎技術となる語彙記法・DMDについて検討・整備を実施。必要に応じた文字規格のメンテナンスを行う。

b. 基本サービスの提供

IMIをユーザーに有効活用してもらうため、機構で整備するガイドラインなどのコンテンツ、基礎データや基礎技術の成果物等の情報を、オープンデータ作成者・官民データ利活用者に向けて「imi.go.jp」サイトから提供する。

IMIユーザーの拡大に向けて、地方セミナーを実施する。また、「imi.go.jp」から公開中の、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利用者を拡大するため、定期的に操作説明会を実施する。合わせてユーザーからの意見を集約し、機能強化に向けて準備を進める。

IMIパートナー企業や自治体にデータ構築の支援をしながら、パートナーや自治体の課題・知見を収集、協力体制を強化、分野横断的な展開に向けた環境整備を進める。

以上の取組の成果として、共通語彙基盤・文字情報基盤を調達要件とする自治体数を、全自治体の8%とするよう、普及を図る。（平成29年度現在で文字基盤は3%、語彙基盤は1%であり、平成30年度は倍増を目指す。）

c. 標準化終了後の文字情報基盤についてフォローアップを継続する。

d. 自治体調査の実施

自治体の公共データの対応状況やIMIについての認知度等を調査する。

（3）海外機関との連携の促進

① 米国商務省国立標準技術研究所（NIST[16]）、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[17]）、IESE等の海外機関との連携を通じて、ICT等に関する技術等の最新情報の交換や技術共有等に取り組む。

【平成30年度の評価指標】

中期計画に掲げる指標について、平成30年度においては、以下に定める評価指標を達成しているか否かを総合的に勘案して評価を行う。

① ICTに関する技術動向等の調査・分析・情報発信

機構が取りまとめたICTに関する技術動向等の白書及びICTに関する調査等の報告書について、普及件数の年間総数につき、第三期中期目標期間中における年間平均値以上を達成する。（参考値：第三期中期目標期間（平成28年度まで）の普及件数の年間平均159，661件）

② ICTに関する指針やガイドラインの提供及び普及促進【基幹目標】

機構が整備したICTに関する指針やガイドラインについて、普及件数の年間総数につき、第三期中期目標期間における年間平均値以上を達成する。さらに、当該指針やガイドラインの利用者又は想定される利用予定者に対し、セミナー等において役立ち度（見込）を調査し、4段階評価で上位2つの評価を得る割合を3分の2以上確保する。（参考値：第三期中期目標期間（平成28年度まで）の普及件数の年間平均435，663件）

［重要度高・優先度高・難易度高］

③ ITスキル標準の浸透

IoT、ビッグデータ、AI等の進展による今後のIT人材の在り方に影響を及ぼし得る産業動向や技術等の調査、並びにスキル変革に求められる指標として整備・発信する新たなITスキル標準に関する情報アクセス数について、毎年度、平成25年度～平成28年度の年度当たり平均アクセス数（※）以上を達成する。（※基準値：平成25年度～平成28年度の年度当たり平均アクセス数29，269件）

16 ＮＩＳＴ：National Institute of Standards and Technology の略

17 ＳＥＩ：Software Engineering Institute の略

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．機動的・効率的な組織及び業務の運営

（1）PDCAサイクルに基づく業務運営の不断の見直し

① 機構の各事業について、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、改善のPDCAサイクル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 業務運営の見直しに当たっては、機構内部における自己評価結果に加え、主務大臣による評価結果やその過程で得られた経営に関する有識者、評価に関する有識者からの意見・助言等、第三者からの客観的な評価・意見等を踏まえ、その結果を事業選択や業務運営の効率化に反映させる。また、ITを巡る内外の情勢変化等も見据えつつ、業務効率向上のための最適な組織体制を柔軟かつ機動的に構築できるよう、継続的な見直しを実施する。

③ 上期終了時点において、平成30年度計画において掲げた事業の進捗状況の把握を行うとともに、自己評価や主務大臣の評価等により抽出された課題等への対応状況についてフォローアップを行い、それを踏まえた「平成30年度下期実行計画」を策定することにより、PDCAサイクルに基づく業務運営の見直しの実効性を確保する。また、予算の適切な執行に向け、「中間仮決算」を実施する。

（2）機動的・効率的な組織及び業務の運営

① 組織内外の課題や組織横断的な課題に対して適切に対応するため、各部署の業務を総括的に把握している職員等からなる常設の会議体を設置し、当該課題に対して機構全体の視点から議論・検討を行い、組織全体としての最適効率を目指す組織・業務運営を行う体制を構築する。

② 限られた人員で効果的・効率的に事業を実施するため、部署間の連携促進、縦割り排除を目的とした情報共有を行う常設の会議体を設置し、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、組織全体として最適かつ効果的・効率的な業務運営を行う。

③ 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する。各界の外部意見の把握に努めるとともに、トップマネジメント相互の経験の共有を通じて、より実効性のある業務運営方針の立案につなげる。

④ 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、組織内への知識の習得や蓄積を図ることを通じて組織のパフォーマンス向上に努める。

⑤ 情報システム開発・運用業務、プロモーション業務、全国レベルの大規模業務等、業務内容や専門性に応じて効果的なアウトソーシングを実施するとともに、中核業務へのリソース集中を通じて組織の資源配分効率の向上に努める。また、可能な限り競争的な方法により事業者等を選定する。

2．業務経費等の効率化

運営費交付金を充当して行う業務については、新規に追加されるもの、拡充分及び特別事業費を除き、一般管理費（人件費及びその他の所要額計上を必要とする経費を除く。）について前年度比3%以上、業務経費（人件費及びその他の所要額計上を必要とする経費を除く。）について前年度比1%以上の効率化を行う。

3．人件費管理の適正化

役職員の給与水準については、国家公務員の給与水準を踏まえ、検証したうえで適切な見直しを実施することにより適正化に取り組むとともに、ラスパイレス指数、役員報酬、給与規程及び総人件費を公表する。

4. 調達の合理化

（1） 公正かつ透明な調達手続による適切で迅速かつ効果的な調達を実現する観点から、「独立行政法人における調達等合理化の取組の推進について（平成27年5月25日総務大臣決定）」を踏まえ、引き続き、毎年度策定する「調達等合理化計画」に基づく取組を着実に実施する。

また、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、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。）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。

5. 業務の電子化等による業務運営の効率化

（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） システムが安全に稼働できるための環境整備を目的としたシステム構築やサービス等の検討・導入を進める。

（3） 給与計算に関する業務の効率化を図るため、当該業務についてアウトソースの検討を行う。

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. 運営費交付金の適正化

（1） 事務事業については不断の見直しを行いつつ、必要性等に応じた財源の最適配分（人員、予算等）を行うとともに、執行状況を役員会でチェックする等、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、予期せぬ運営費交付金債務残高の発生を抑制する。

（2） 「独立行政法人会計基準」（平成12年2月16日独立行政法人基準研究会、平成27年1月27日改訂）等により、運営費交付金の会計処理として、業務達成基準による収益化が原則とされたことを踏まえ、引き続き、収益化単位の業務ごとに予算と実績を適切に把握し、適正な予算執行管理を行う。

（3） 機構の財務内容等の透明性を確保する観点から、決算情報の公表の充実等を図る。

2. 自己収入の拡大

機構が行う業務のうち、受益者が特定でき、受益者に応分の負担能力があり、負担を求めることで事業目的が損なわれない業務については、経費を勘案して、適切な受益者負担を求めることとし、自己収入の増加に努める。

3. 試験勘定の採算性の確保

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持続的な運営を可能とするため、応募者の増加に資する取組を実施するとともに、事務の活性化・効率化及び収益の維持・改善を図るものとする。

4. 地域事業出資業務（地域ソフトウェアセンター）

（1） 地域事業出資業務については、繰越欠損金を減少させるため、平成30年度の経常収益合計で2千万円以上確保する。

そのために、地域ソフトウェアセンターの経営状況について、中間決算及び年度決算見込等の資料提出を求めることにより的確に把握し、また、様々な機会をとらえて経営者との情報交換を密に行うことにより指導・助言等を積極的に行い、センターの経営改善を図るとともに、適切な配当を求めるものとする。

（2） 以下の基準に該当するものは、他の出資者等との連携の下に、抜本的な改善策について協議を進め、当該期間中に解散に向けた取組を促すものする。

①経営改善を行っても、繰越欠損金が増加（3期連続を目安）又は増加する可能性が高い場合

②主要株主である地方自治体・地元産業界からの支援が得られない場合

5. 債務保証管理業務

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。

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）の発生により資金不足が生じた場合、短期借入金の限度額（20億円）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

剰余金が発生したときは、業務の推進及び拡充、広報活動の充実、職員の研修の充実、施設・設備の整備に係る経費に充てる。

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） 事業や組織の見直しに合わせた人員体制の整備等

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、就職情報サイトの積極的活用や採用説明会の開催頻度を高めること等により、新卒採用者の確保に向けた採用活動の強化を図る。

② 新卒採用者に対して、トレーナー及びメンター制度を充実させることにより、職員の自立化及び職場環境への早期定着化を図る。

③ 事業遂行に係る必要性に応じて、専門性を有する人材やセキュリティ人材の採用を図る。

④ 中途採用にあたって、業務のミスマッチ防止の観点から、ジョブディスクリプションを作成する。

⑤ 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、組織内への知識の習得や蓄積を図ることを通じて組織のパフォーマンス向上に努める。

（2） 職員の中長期的な育成を図るため、研修実施計画を策定し、同計画に基づく階層別研修、職員全般に必要とされる知識や行動を習得するための基本研修や、職員のニーズ等を踏まえた目的別・テーマ別研修を実施する。

（3） 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を行うとともに、能力評価の評価結果を昇給・昇格に反映させる。加えて、多角的な評価（360度評価）を実施することにより、人事評価の信頼性を高める取組を行う。

3. 中期目標期間を超える債務負担

中期目標期間を超える債務負担については、当該債務負担行為の必要性及び資金計画への影響を勘案し、合理的と判断されるものについて行う。

4. 積立金の処分に関する事項

前中期目標期間の最終事業年度における積立金残高のうち、主務大臣の承認を受けた金額については、情報処理促進法第43条に規定する業務の財源に充てる。

5. その他独立行政法人通則法第29条に規定する中期目標を達成するために必要な事項

（1）内部統制の充実・強化

平成29年度に実施したリスク調査、コンプライアンスに係る取組を踏まえ、適宜コンプライアンスに係る研修を実施するなど、平成30年度以降の継続的活動を計画し、引き続き内部統制活動の定着を図る。

（2）機構における情報セキュリティの確保

① 独法等における情報システムの監視業務や情報セキュリティ監査業務について、自らが実施側の立場であることを十分に認識しつつ、適切に業務を実施するとともに、得られた知見については、必要に応じ、機構自身のセキュリティ確保に活用する。

② 「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ことにより、情報セキュリティの維持・向上に努める。

③ 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。

（3）戦略的広報の推進

① 第四期中期計画における新生IPAおよび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。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、新しい組織構成に伴う構成変更を実施。また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29年度に開発・導入した新たな受付サービスを開始する。

③ 積極的な報道発表を実施し、個別取材にも対応する等、事業成果の認知度向上に努める。

④ 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、広報冊子の制作・配布を行う。

⑤ 機構が公開するセキュリティ対策情報及び実施するイベント・セミナー情報、公募・入札情報等について、「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」にまとめて発信する。

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。

⑦ これらの情報発信活動を通じて平成30年度に新たに12，000名の登録者を追加する。

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	7，030
国庫補助金	1，377
受託収入	506
業務収入	5，041
その他収入	10
計	13，964
支　出	
業務経費	13，191
受託経費	506
一般管理費	1，066
計	14，762

［人件費の見積り］

平成30年度には2，215百万円を支出する。

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	0

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	3，301
その他収入	3
計	3，304
支　出	
業務経費	3，003
一般管理費	194
計	3，197

［人件費の見積り］

平成30年度には431百万円を支出する。

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	金　額		
	情報セキュリティ	IT人材育成	社会基盤
収　入			
運営費交付金	4，013	905	1，241
国庫補助金	1，377	0	0
受託収入	461	0	45
業務収入	1，735	0	4
その他収入	0	0	0
計	7，586	905	1，289
支　出			
業務経費	7，582	905	1，696
受託経費	461	0	45
一般管理費	0	0	0
計	8，043	905	1，741

区　別	債務保証業務	法人共通	合　計
収　入			
運営費交付金	0	872	7，030
国庫補助金	0	0	1，377
受託収入	0	0	506
業務収入	1	0	1，740
その他収入	3	0	3
計	4	872	10，656
支　出			
業務経費	4	0	10，187
受託経費	0	0	506
一般管理費	0	872	872
計	4	872	11，565

［人件費の見積り］

平成30年度には1，783百万円（情報セキュリティ745百万円、IT人材育成146百万円、社会基盤427百万円、法人共通466百万円）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	4
計	4
支　出	
計	0

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	15，237
業務費用	12，147
受託経費	506
一般管理費	1，066
減価償却費	1，518
収益の部	
経常収益	15，170
運営費交付金収益	7，030
補助金収益	1，377
受託収入	506
業務収入	5，041
その他収入	22
資産見返負債戻入	1，190
財務収益	4
純利益（△純損失）	△　66
前中期目標期間繰越積立金取崩額	184
目的積立金取崩額	0
総利益（△総損失）	117

［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	
経常収益	0
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	0
目的積立金取崩額	0
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	3，215
業務費用	2，948
一般管理費	194
減価償却費	73
収益の部	
経常収益	3，312
業務収入	3，301
その他収入	3
資産見返負債戻入	8
財務収益	0
純利益(△純損失)	97
前中期目標期間繰越積立金取崩額	0
目的積立金取崩額	0
総利益(△総損失)	97

別紙2－4

収支計画（一般勘定）

（単位:百万円）

区　別	金　額		
	情報セキュリティ	IT人材育成	社会基盤
費用の部			
経常費用	8，867	905	1，291
業務費用	7，046	905	1，244
受託経費	461	0	45
一般管理費	0	0	0
減価償却費	1，360	0	2
収益の部			
経常収益	8，684	905	1，291
運営費交付金収益	4，013	905	1，241
補助金収益	1，377	0	0
受託収入	461	0	45
業務収入	1，735	0	4
その他収入	0	0	0
資産見返負債戻入	1，097	0	2
財務収益	0	0	0
純利益（△純損失）	△　184	0	0
前中期目標期間繰越積立金取崩額	184	0	0
目的積立金取崩額	0	0	0
総利益（△総損失）	0	0	0

区　別	債務保証業務	法人共通	合　計
費用の部			
経常費用	4	955	12，022
業務費用	4	0	9，199
受託経費	0	0	506
一般管理費	0	872	872
減価償却費	0	83	1，445
収益の部			
経常収益	4	955	11，839
運営費交付金収益	0	872	7，030
補助金収益	0	0	1，377
受託収入	0	0	506
業務収入	1	0	1，740
その他収入	3	0	3
資産見返負債戻入	0	83	1，182
財務収益	0	0	0
純利益（△純損失）	0	0	△　184
前中期目標期間繰越積立金取崩額	0	0	184
目的積立金取崩額	0	0	0
総利益（△総損失）	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	
経常収益	20
その他収入	16
財務収益	4
純利益(△純損失)	20
前中期目標期間繰越積立金取崩額	0
目的積立金取崩額	0
総利益(△総損失)	20

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	20，828
業務活動による支出	13，984
投資活動による支出	1，044
翌年度への繰越	5，801
資金収入	20，828
業務活動による収入	13，964
運営費交付金による収入	7，030
国庫補助金による収入	1，377
受託収入	506
業務収入	5，041
その他収入	10
投資活動による収入	2，100
当年度期首資金残高	4，764

［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	5，492
業務活動による支出	3，142
投資活動による支出	55
翌年度への繰越	2，296
資金収入	5，492
業務活動による収入	3，304
業務収入	3，301
その他収入	3
投資活動による収入	1，100
当年度期首資金残高	1，088

別紙3－4

資金計画（一般勘定）

（単位:百万円）

区　別	金　額		
	情報セキュリティ	IT人材育成	社会基盤
資金支出	9，835	905	3，549
業務活動による支出	7，670	905	1，289
投資活動による支出	537	0	452
翌年度への繰越	1，628	0	1，808
資金収入	9，835	905	3，549
業務活動による収入	7，586	905	1，289
運営費交付金による収入	4，013	905	1，241
国庫補助金による収入	1，377	0	0
受託収入	461	0	45
業務収入	1，735	0	4
その他収入	0	0	0
投資活動による収入	1，000	0	0
当年度期首資金残高	1，248	0	2，260
区　別	債務保証業務	法人共通	合　計
資金支出	53	951	15，292
業務活動による支出	27	951	10，842
投資活動による支出	0	0	989
翌年度への繰越	25	0	3，461
資金収入	53	951	15，292
業務活動による収入	4	872	10，656
運営費交付金による収入	0	872	7，030
国庫補助金による収入	0	0	1，377
受託収入	0	0	506
業務収入	1	0	1，740
その他収入	3	0	3
投資活動による収入	0	0	1，000
当年度期首資金残高	49	79	3，636

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	43
翌年度への繰越	43
資金収入	43
業務活動による収入	4
その他収入	4
当年度期首資金残高	39