

# 独立行政法人情報処理推進機構 令和2年度計画

独立行政法人  
情報処理推進機構

(令和3年2月15日変更)

# 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.....	3
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.....	3
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.....	10
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.....	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.....	17
1. 機動的・効率的な組織及び業務の運営.....	17
2. 業務経費等の効率化.....	17
3. 人件費管理の適正化.....	18
4. 調達合理化.....	18
5. 業務の電子化等による業務運営の効率化.....	18
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.....	18
1. 運営費交付金の適正化.....	18
2. 自己収入の拡大.....	19
3. 試験勘定の採算性の確保.....	19
4. 地域事業出資業務(地域ソフトウェアセンター).....	19
5. 債務保証管理業務.....	19
IV. 予算(人件費見積もりを含む。)、収支計画及び資金計画.....	19
1. 予算(別紙参照).....	19
2. 収支計画(別紙参照).....	20
3. 資金計画(別紙参照).....	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.....	20
VIII. 剰余金の使途.....	20
IX. その他主務省令で定める業務運営に関する事項.....	20
1. 施設及び設備に関する計画.....	20
2. 人事に関する計画.....	21
3. 中期目標期間を超える債務負担.....	21
4. 積立金の処分に関する事項.....	21
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.....	21

別紙.....	24
別紙1 予算.....	24
別紙2 収支計画.....	29
別紙3 資金計画.....	34

# 独立行政法人情報処理推進機構令和2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。)の令和2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) 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。
  - 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分析能力の強化、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、国内外の業界動向等の情報共有も継続する。
  - b. J-CSIPの活動においては、情報提供元的意思を尊重しつつ、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. 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。また、東京オリンピック・パラリンピック競技大会に向け、要請に応じて関連団体・省庁等からの支援要請に対応する。
- ② 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、情報収集チャネルを拡大し、情報の量及び質を高める。
  - a. 被害組織、攻撃ツール、攻撃者情報などの脅威情報を用いてわが国における脅威情報や被害傾向の分析能力の向上を図るとともに、有識者との連携チャネルの拡大に努め、助言品質の向上、機構から発信する注意喚起情報等に活用する。
- ③ 国民からの相談・問合せに対応するための相談窓口を引き続き運営するとともに、急速に変化しつつある脅威を的確に把握し、コンピュータウイルス等のマルウェアや不正アクセス等の情報を積極的に収集・分析し、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、届出状況を公表する。
  - b. 「情報セキュリティ安心相談窓口」を引き続き運営するとともに、さらに広く国民一般に対するサービス及びサポートする体制を強化する。
  - c. 国民の手元で起きている現象を把握した上でタイムリーな情報提供を行うため、スマートデバイスやパン

コンにまつわるインターネットトラブルに関して検証・分析できる環境の維持、外部組織との連携の活性化や情報収集チャネル拡大等により、相談対応品質および問題解決能力の向上を図る。

- d. 相談対応や各所との情報共有で得られた脅威情報や被害状況の収集および分析に努め、手口の検証を実施し、対策ノウハウの蓄積に努めるとともに、国民への情報提供を行う。

### (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. 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JPCERT/CCとの連携を図りつつ提供する。
  - c. 「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。
  - d. 「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、特定の組織に対して脆弱性関連情報を優先的に提供する。
- ② 統合的な脆弱性対策情報の提供環境を整備することにより、開発者、運用者及びエンドユーザーに対して、脆弱性対策情報の活用を促す。
  - a. 「JVN 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と共に、地域で開催されるセミナーへの講師派遣等の支援を行う。
  - c. 脆弱性対策を促進するための各種ツールを提供する。
- ③ 組込み機器等の脆弱性に関する対策の提示等を行う。
  - a. 組込み機器等に対する脆弱性対策のためのガイドラインを提供する。
  - b. 組込み機器等に対する脆弱性対策に関する普及啓発を行う。
- ④ 最新の脆弱性情報や攻撃・被害情報を収集・分析し、注意喚起による危険回避や対策の徹底を図り、サイバーセキュリティ上のリスクの低減を促進する。
  - a. 「(1-1)サイバーセキュリティ上の脅威への対応」で得られた情報に加え、サイバーセキュリティに関わる最新状況等を適宜収集し、必要に応じてタイムリーに注意喚起等による対策情報等を公表する。

### (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 重要インフラ分野等(データ活用に積極的に取り組む企業・組織を含む。)の社会的に重要な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、インシデント発生時の原因究明調査等の協力を行う。
  - a. 生産性向上特別措置法に基づくデータ共有事業の安全確認審査におけるセキュリティ対策状況等の確認を要請に応じて行う。
  - b. 経済産業省からの依頼により、経済産業省が策定した「情報セキュリティサービス基準」に適合する情報セキュリティサービスの提供状況について調査を行い、その結果を「情報セキュリティサービス基準適合サービスリスト」として公開する。
  - c. サイバーセキュリティ基本法及び生産性向上特別措置法に基づく原因究明調査を要請に応じて実施す

る。

- d. 経済産業省が進めている「サイバー・フィジカル・セキュリティ対策フレームワーク」の策定・普及活動に協力し、必要に応じて改訂等に向けた検討を行う。

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。

- 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調査するとともに、「制御システムのセキュリティリスク分析ガイド」の実践研修開催等による普及活動を実施する。
- b. 重要インフラシステムのリスク分析等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個別業界向けリスク分析ガイドを作成する。
- c. 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、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**

① 人材育成事業

- a. 社会インフラ・産業基盤を有する企業・機関において、OTやITシステムのリスクを認識しつつ、必要なサイバーセキュリティ対策を総合的に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に係る演習を行う。
- c. 国内外の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・機関と連携し、海外の有益な知見を得る。
- d. 第3期中核人材育成プログラムの受講生に対し、平成30年度に立ち上げた中核人材育成プログラムの修了者コミュニティへの参画を促しつつ、同コミュニティの活動が円滑に推進するよう継続して支援する。
- e. 各種セミナーや責任者に対する人材育成プログラムの開催等を通じて、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的な対策強化を促す。
- f. 産業サイバーセキュリティセンターが提供する人材育成プログラムの講義の一部をIPA職員等が担当する取組を継続する。
- g. 企業や産業におけるサイバーセキュリティ対策が着実に行われていくように、経営層に対して、各種セミナー等を通じて、セキュリティ対策の必要性を啓発するとともに、上述の事業内容について情報発信を行う。
- h. 産業サイバーセキュリティセンターが提供する人材育成プログラムの修了者を継続して輩出するため、同プログラムの普及策及び受講者獲得の方策を策定する。
- i. 送配電事業者などエネルギー・リソース・アグリゲーション・ビジネス(ERAB)に参画する事業者向けにERABサイバーセキュリティガイドラインに準拠する人材育成トレーニングプログラムの開発等を行う。

② 実際の制御システムの安全性・信頼性検証事業

- a. 機構内関係部署間で連携し、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. 情報収集分析環境を活用し、調査分析結果を社会に還元しつつ分析環境の改善及び充実を図る。また、人材育成プログラムの受講者等へ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 経営層等に対して情報セキュリティ対策の重要性を訴え、企業や組織における情報セキュリティ対策の取組を促進させるため、企業・組織・サプライチェーン全体で見逃されがちな脅威、課題等を掘り起こし、分析・評価及び必要な情報提供を行う。
  - a. ガイドラインのさらなる普及に向けたプラクティスの拡充に関する調査検討を行う。
  - b. ICTシステムやサービスの業務委託契約における条件等について国内外の実態調査を行う。
- ② ICT利用企業や国民一般に向けて積極的な情報セキュリティ対策の浸透を促すため、社会的要請等に応じ、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・情報セキュリティ倫理に対する意識等に関する状況調査・分析及び必要な情報提供を行う。
  - a. 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。
  - b. データ利活用における重要情報の共有に必要な保護・管理方法に関する調査・検討を行う。
  - c. サイバーセキュリティに対する意識の醸成とセキュリティビジネスの活性化に向けて、最新動向や政策等の情報発信とユーザー、ベンダー等との交流等を促進する。また、地方の関係機関・組織と連携して、地方での交流促進に向けた取組を進める。
  - d. 「情報セキュリティ白書2020」を作成する。
- ③ 潜在的な情報セキュリティ上の脅威や攻撃の傾向を技術動向や社会動向、利用者・攻撃者の心理等から多面的に分析し、中長期的に発生し得る重大事象やそれに対する対策等の予測的な情報発信や、セキュリティリスク・対策状況を可視化・評価する手法提供の可能性について検討する。
  - a. 「サイバーセキュリティ経営ガイドライン可視化ツール」の実証評価及び改訂に向けた調査検討を行う。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新しいIT基盤に関し、それらの潜在的な脆弱性、信頼の欠如等のリスクがどのように発現・拡大しうるか等の脅威予測に向けた調査・検討を行う。
  - c. セキュリティ対策に係る製品・サービスの効果、性能等を評価し、評価結果の公表を行う仕組みの在り方について調査・検討する。

### **(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、講師の派遣等を行い、更なる普及啓発に取り組む。
  - b. 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り組み事例に関するコンクールの効率的実施等により児童・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。
  - c. 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。
- ② 中小企業が情報セキュリティ対策を身近な課題としてとらえ自発的に対策を行う気運を高めるべく、中小企

業が関連する様々な団体や制度との連携を図りつつ、ガイドライン、自己宣言制度等の普及を行う。

- a. 「中小企業の情報セキュリティ対策ガイドライン」を普及させるため、中小企業支援機関向けの周知・講師派遣、ガイドラインの実践に関する指導ができる者の拡大等を行う。
  - b. 情報処理安全確保支援士等を活用し、中小企業向けセキュリティマネジメント体制強化支援等を行いつつ、「SECURITY ACTION 制度」の更なる周知を図り、参加企業数の拡大に取り組む。中小企業におけるセキュリティ対策の更なる普及に向けて、ニーズや宣言内容等について検討する。
  - c. 中小企業が自発的に対策を行う気運をより一層高めるため、中小企業のセキュリティ対策に有益な診断／教育ツール等の提供及びこれらの普及を自主的に行う「セキュリティプレゼンター」と中小企業をマッチングする場の提供を行う。
  - d. 中小企業のセキュリティ対策支援サービス等の実証を行うとともに、関係機関・団体、民間企業等との連携により、中小企業のセキュリティ対策支援サービス等の普及に向けた検討を行う。
- 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)IT製品等のセキュリティ評価、認証等の着実な実施**

- ① 「IT製品のセキュリティ評価及び認証制度」を引き続き着実に実施するとともに、評価・認証手続の改善、評価に関する技術の維持・向上、現状・動向の調査、情報提供を実施する。
  - a. 「IT製品のセキュリティ評価及び認証制度」に係る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き面での課題については、関係各者と調整して解決を図る。
  - 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価について、国内外の関連団体・組織等からの情報収集、脆弱性評価ツール等を通じて制度関係者との情報共有及び国内の技術力維持・向上を図る。
  - c. 制度の利用促進のため、政府機関によるIT関連調達動向を見据え、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・情報収集及び情報提供を行う。
  - d. 「IT製品のセキュリティ評価及び認証制度」の維持に関連し、相互承認アレンジメント(CCRA)の運営に参画するとともに、国際的に共同で策定中のセキュリティ要件(cPP)についても要請に応じて参画する。
  - e. 「IT製品のセキュリティ評価及び認証制度」における新たな評価項目検討の一環として、ハードウェアへの新たな攻撃手法に対する評価手法を確立するために、認証試験に活用可能な攻撃手法の調査及び有効性の検証を行う。
- 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. 「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。
- ③ クラウドサービスの安全性評価に係る制度運営・審査業務を開始し、登録が認められたクラウドサービスのリストを公表する。また、評価の枠組みや管理基準等についてクラウドサービスに係る最新の技術的動向や海外動向の調査を行い、制度所管省庁に対して効果的な改善の提案を行う。



## **(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等の情報提供を行う。
  - a. CRYPTREC暗号リストの信頼性維持のため、国際会議等への参加を通じて暗号アルゴリズムの安全性／危殆化を監視する。また、昨年度調査の結果等を踏まえたCRYPTREC暗号リスト改定方針を策定する。
- ② 情報システムのセキュリティ確保の根幹である暗号技術の適切な利用／運用を促進するため、暗号技術の利用／運用面での現状・動向等の調査を行い、ガイドライン等により、情報提供を行う。
  - a. 既作成の暗号技術の適切な利用／運用に関するガイドラインについて、普及を行うとともに、利用環境の変化等に応じた改定の要否について検討する。
- ③ 「暗号モジュール試験及び認証制度」を着実に実施するとともに、評価・認証手続の改善、評価に関する技術の維持・向上、現状・動向の調査、情報提供等を実施する。
  - a. 「暗号モジュール試験及び認証制度」に係る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き面での課題については、関係各者と調整して解決を図る。
  - b. 認証機関としての環境維持のため、業務管理システム及び暗号アルゴリズム実装試験ツール維持管理を行う。
  - c. 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 NISCの監督の下、複雑化・巧妙化しているサイバー攻撃に対応するため、最新の技術を用いて監視・分析等の機能強化を図る。
- ③ 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。

### **【令和2年度の評価指標】**

中期計画に掲げる指標について、令和2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】

令和2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】

「SECURITY ACTION 制度」に参加する中小企業数について、関連団体等との協力関係を強化する等により該当地域における本制度の普及拡大に努め、3大都市圏を除く36道県にて令和2年度終了時点で累計で48,000社以上とする。

[重要度高・優先度高・難易度高]

(参考値:一つ星から二つ星へのステップアップ数)

③ 情報セキュリティ対策の企業への普及促進

令和2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

令和2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

令和2年度に実施する人材育成プログラムにおいて、既存プログラムの運営から得られた知見及び産業サイバーセキュリティの現状を踏まえ、各プログラムの改修等により受講者数の拡大を図り、産業サイバーセキュリティセンターが提供する人材育成プログラムの受講者数100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】

産業サイバーセキュリティセンターが提供する人材育成プログラムの修了者により、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・提案等の具体的な取組が150件実施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

### (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) 突出したIT人材の発掘・育成と社会価値創出の促進

- 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ア、技術を有する優れた個人を、優れた能力と実績を持つプロジェクトマネージャーのもとに発掘・育成を行う「未踏IT人材発掘・育成事業」を実施する。
- ② 革新的なアイデア等を有する人材が、自らのアイデアや技術力を最大限に活かし、ビジネスや社会課題の解決につなげていけるよう、優れた能力と実績を持つプロジェクトマネージャー等による指導・助言を行う「未踏アドバンス事業」を実施する。
- ③ 次世代ITを活用する先進分野において、基礎技術や領域横断的技術革新に取り組む優れた人材が自らのアイデ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つプロジェクトマネージャー等による指導・助言を行う「未踏ターゲット事業」を実施する。また、経済産業省と連携して、当該事業に係る今後の実施分野拡充の可能性について検討に着手する。

#### (1-2) 若年層の優秀なセキュリティ人材の発掘・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、4泊5日の合宿形式でセキュリティ・キャンプ全国大会とセキュリティ・ネクストキャンプ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 セキュリティ・キャンプ全国大会、セキュリティ・ネクストキャンプおよびセキュリティ・キャンプ地方大会において、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。  
また、セキュリティ・キャンプ修了生に対する情報セキュリティに関する講演会の開催・修了生の組織化への取組等(セキュリティ・キャンプフォーラムの実施を含む)を通じて、セキュリティ人材ネットワークの活性化を図る。

#### (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 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、及び登録資格の更新を行うとともに、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た情報処理安全確保支援士向けの講習、及び同等以上の効果を有すると認められる講習(特定講習)に関する業務(特定講習を認定するための基準の整理を含む)を行い、制度の着実な運営に継続して努める。
- ② 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、関連団体等との協働によるセミナーや制度説明会等の開催、ウェブやメール、情報処理安全確保支援士ポータルサイト等による情報処理安全確保支援士のニーズに合った情報発信等を行う。

#### (1-4) 優れたIT人材の人的ネットワーク活性化促進

- ① 外部団体と連携し、または独自に取り組み、未踏関係事業の成果等をイベント、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、社会価値創出に向けた講習や交流の場を提供する。

## **(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 令和2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、AI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、ITパスポート試験については、政府の「AI戦略2019」(令和元年6月11日 統合イノベーション戦略推進会議決定)の記載に対応するため、令和4年度からの実施に向けて、出題範囲・シラバス・出題内容の見直しに着手する。
- 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。また、現状の試験に係る全体的な実施方法等の見直しを含めた中期的な対策について検討し、試験の活用の促進と収益の維持を目指す。
- ③ 令和2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。
- ④ 経済産業省が実施する情報処理技術者試験の今後の方向性に関する検討に協力する。

### **(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他、外部資金を活用し、試験に向けた各国の指導者を育成する研修の調整等を行う。また、新規国の要望等に対しては、相手国との関係に留意しながら、適宜必要な対応をとる。

## **【令和2年度の評価指標】**

中期計画に掲げる指標について、令和2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】**

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】**

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。

全国大会等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)に対するアンケートを実施し、60%を達成する。

### 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、令和2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

#### (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 ICTに関する新技術の社会実装の推進、デジタルトランスフォーメーション(DX)の進展を加速させるための有用な情報を提供することを目的として、市場の潮流や政策・制度の影響を踏まえ、AI、IoT、ブロックチェーン、量子コンピューティング等の新技術領域における国内外のビジネス動向、技術動向、政策動向についての調査・分析を実施する。また、DXの担い手であるユーザー企業に対する示唆等を盛り込んだレポート等のコンテンツを作成し、社会のニーズに合った形でタイムリーに発信する。
- ② 民間企業のDXの進展を支える情報提供を目的として、社会や産業の実態を把握するための情報、新たな潮流を踏まえ具体的な行動に移すための情報と分析結果を取りまとめた新たな白書の発刊に向けた検討を行う。経済産業省が推進するDX関連施策との整合性を図るとともに、新型コロナウイルスがビジネスに与えた影響等を含め、新白書で取り上げるべきテーマや対象領域の検討を行い、これらに関する最新動向等を把握するための調査を実施する。
- ③ IT企業、ユーザー企業及びデジタルビジネス推進部門を対象として実施したIT人材動向調査の結果を取りまとめ、「IT人材白書2020」として発行する。
- ④ 「情報セキュリティ白書2020」を発行する。

##### (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(再掲)

- ① 潜在的な情報セキュリティ上の脅威や攻撃の傾向を技術動向や社会動向、利用者・攻撃者の心理等から多面的に分析し、中長期的に発生し得る重大事象やそれに対する対策等の予測的な情報発信や、セキュリティリスク・対策状況を可視化・評価する手法提供の可能性について検討する。
  - a. 「サイバーセキュリティ経営ガイドライン可視化ツール」の実証評価及び改訂に向けた調査検討を行う。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新しいIT基盤に関し、それらの潜在的な脆弱性、信頼の欠如等のリスクがどのように発現・拡大しうるか等の脅威予測に向けた調査・検討を行う。

##### (1-3)組込み/IoT 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 経済産業省と連携して、組込み/IoT産業のDX推進施策に資することを目的に、ステークホルダー毎にDXへの取組状況や技術導入等の動向、また、これらの経年変化を把握するための調査を実施する。

##### (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/ICTプロジェクト創出のための取組を支援するべく次の取組を実施する。
  - a. 地域における更なる取組の拡大に向け、「地方版IoT推進ラボ」として前年度までに選定した101地域に加え、新たな地域を選定するとともに、選定したラボに対して、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人的支援、広報の支援、活動に資する情報の提供・共有支援を実施する。
- b. 地方版 IoT 推進ラボの更なる発展に向け、経済産業省とともに地域の有力推進者による検討会議や全国担当者会議を開催し、他の施策との連携や地方版 IoT 推進ラボの今後の方向性等について検討を行うとともに、当該検討結果を踏まえ、各ラボの特徴を考慮した各種施策の展開に向けた取組を実施する。
- ② デジタル化による地域課題の解決や経済活性化に向けて、「地方版IoT推進ラボ」や地域団体、公的機関等とのネットワークを強化し、これらの組織との連携を通じ、機構の推進施策の展開を行う。

## (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 ユーザー企業とベンダー企業とが良好な関係を保ちつつDX推進のためのシステム開発を行えるようにするため、前年度に公開した「モデル取引・契約書」について、システム再構築等における企画プロセス等の観点からの見直しを行うとともに、見直した「モデル取引・契約書」の普及を行う。
- ② 企業競争力の向上、及び業界全体の効果的なIT投資の促進のため、以下の取組を実施する。
- a. 各企業の DX の取組状況を自己診断することを可能にする「DX 推進指標」の運用方法の検討、DX 推進に関連する国内外の最新事例やシステム開発技術・方法論等の動向調査を行うとともに、IT システムを構築する際に参考となる情報を集約した手引書やその運用の助けとなる指標を策定する。
- b. 経済産業省が行うデジタル経営に係る認定制度の運用開始に向け、経済産業省と連携して制度設計及び認定手順の整理を行うとともに、申請受付を開始し、着実に制度を運用する。また、認定を受けた事業者に対するフィードバックの実施や、認定事業者情報の対外発信を行うとともに、企業及び関係者が認定制度を活用し企業の DX をさらに進められるように、必要な調査・検討を行う。
- c. 企業・業界の非競争領域における共通的なプラットフォームの構築に向けた検討を開始し、前年度実施したニーズ調査、課題整理の結果を踏まえつつ、経済産業省と連携して取組分野の選定を行うとともに、選定した分野の共通プラットフォーム構築方針に関するステークホルダー間の合意形成に向けた調整を行う。
- ③ 各種ステークホルダーや専門家間の共通認識・共通理解を図り、データ連携等を通じた新たな付加価値創造を促進するため、以下の取組を実施する。
- a. 透明性・公平性が担保された形で中立的なアーキテクチャの設計を行うために必要な機能・体制(主要な民間・大学組織等を含む)を有する「産業アーキテクチャ・デザインセンター(仮称)」を発足する。
- b. 各省各庁又は事業者の依頼に応じて、既存の調査等を踏まえ、アーキテクチャ設計、標準化を含む実装・管理・運用方法等に関する調査研究の方針の検討及び当該作業への着手、並びに、当該調査研究結果の報告・公表の方法の検討を行う。
- c. アーキテクト人材の育成に向けた教育プログラム開発等に関する検討や、将来的にアーキテクチャ設計が必要となる可能性のある領域に関する実現可能性調査等に着手する。
- d. 上記の取組みについて、国内外への積極的な発信を行うとともに、関係機関(米 NIST、独 Industrie4.0、印 iSPIRT 等を含む)の有識者等と、本取組に関する連携方法の検討・情報交換等を行う。

### (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 安全安心なIoTシステム開発のための「つながる世界の開発指針」の実装に向け、開発した教材等の教育機関等における利用促進を図る。
- ② 前年度に実施した組込み/IoT産業の動向把握や製造業のDX推進事例等に関する調査結果を踏まえ、中小規模製造業のOT分野向けのDX推進のための課題や導入技術、進め方等について検討し、ガイドブック等に取りまとめて公開するとともに、その普及を行う。

### (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 これまで取組みを行ってきたシステムズエンジニアリング、事故分析・安全性解析手法やソフトウェア開発の定量的なプロジェクト管理等について、外部からの要請に応じ、講師派遣やセミナー開催等の協力を行う。また、前年度までに収集したソフトウェア開発のプロジェクトデータを活用し、開発スタイルに依存しない普遍的な品質の指標である信頼性に焦点を当てた分析を実施し、分析データ集として公開する。

### (2-4) 重要性の高い基準・指針等の国際標準化への取組

- ① 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ため、日本主導で進めている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引き続き推進し、「IoTのセキュリティとプライバシーのガイドライン」及び「ISO/IEC/IEEE 15288システムエンジニアリングプロセスへのトラストワージネス活動の統合」の国際規格案の作成について、(一社)情報処理学会情報規格調査会に協力する。

### (2-5) ITスキル標準の継続改善

- ① 第四次産業革命への対応に向けて求められる新たな領域の“学び直し”の指針として策定・提供しているITSS+について、各領域の専門的知見を有する有識者及び関連団体と連携し、内容の改善及び情報発信を行う。また、産業動向や技術動向を踏まえた、今後の見直しの方向性に関する検討を行う。
- ② IT産業等におけるプレーヤー構造の変化や、ユーザー企業を含めた組織・人材マネジメントの変化等、前年度までの調査の成果等から浮き彫りとなった課題を踏まえ、人材の学び直しの状況や、取組促進における阻害要因等を調査し、スキル習得の更なる加速化に向けた対応策の検討を行う。
- ③ 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習得講座認定制度」(通称:「Reスキル講座」)の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 前年度に作成・公開したデータ活用に関するガイドの利用者から評価、フィードバックを得て、必要に応じてガイドの改定を行うとともにガイドの活用を促進するための普及策を検討する。
- ② 共通語彙基盤の有効活用に向け、機構が整備したコア語彙、ガイド等のコンテンツを提供する「imi.go.jp」サイトの維持・管理を行う。また、当該業務の外部移管を視野に入れ、既存コンテンツの再整理を行うとともに、移管先、移管方法等を検討する。
- ③ 漢字一覧表やIPAフォント等の文字情報基盤コンテンツの継続的な維持・管理業務の民間移管に向け、前年度に引き続き、当該業務を実施可能な移管先候補の選定及び調整を行い、移管に係る契約手続き等を進める。



### **(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)をはじめ、機構が行う業務に関する海外関連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。

#### **【令和2年度の評価指標】**

中期計画に掲げる指標について、令和2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、人工知能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)

- ④ 企業におけるデジタル経営改革の推進

デジタル経営改革に向け、DX推進指標による自己診断実施組織数について、令和2年度中に120組織以上増加させる。

- ⑤ アーキテクチャ設計に関する機能の強化

各省各庁又は事業者の依頼に応じて、特定の技術、製品、企業、業界等に偏りがない中立的なアーキテクチャについて、2分野以上で取組を開始し、ステークホルダーを含めた検討体制の整備及び調査に着手する。

## 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及び機動的・効率的な業務の運営

- 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。

業務運営の見直しに当たっては、前年度の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外部有識者からの意見・助言等、第三者からの客観的な評価・意見等を踏まえ、必要に応じて既存事業の改廃や新規事業の開始も検討する。また、当該見直しを踏まえ、リソース配分を弾力的に行うことにより、必要な組織体制の柔軟かつ機動的な構築に努める。

また、追加された業務の的確な執行に向けて組織を整備するとともに、必要な予算及び人員の配分、既存の組織の見直しを行う。

- ② 事業の実施に際しては、常にアウトカムを意識した業務遂行を推進する。上期終了時点において、令和2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、前年度の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う。また、それを踏まえて下期において実施すべき取組を取りまとめ、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。

予算の計画的かつ効率的執行に向けて、適正な予算執行管理を行う。

#### (2) 機動的・効率的な組織及び業務の運営

- ① 機構全体に関係する重要課題や業務運営の進め方について、戦略企画委員会をはじめとする会議において、全体の視点から議論・検討を行い、組織横断的な課題に適切に対応する。

また、機構が行う事業について、関係する部署間での情報共有や共通する課題の検討を行うセンター間調整会議等を活用し、部門間の連携、縦割りの排除、事業の相乗効果発揮等を促進する。

これらの取組により、機構全体としての業務運営の最適効率化を図る。

- ② 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。併せて、各界の情勢把握及び連携に向けて、情報交換を行う団体の拡大を図る。
- 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、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。
- ④ 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。

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。また、事前確認の際、予定額の考え方等について聞き取り・助言を行う。

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並びに過去の一者応札案件の改善状況について、契約監視委員会を2回以上開催して、委員の点検を受ける。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、当該業務について外部サービスの利用を開始する。

(4) 機構における更なる働き方改革に向けて各種制度を見直すなど、テレワーク制度の導入やフレックスタイム勤務などの導入に向けた検討を進め、効率的かつ柔軟な業務運営を図る。また、新たなシステムを活用した法人文書管理の徹底を図る。

(5) 役員会等の機構内で開催する会議の審議結果について、組織内に共有する仕組みを明確化する。

(6) 機構業務のデジタルトランスフォーメーション(DX)について、内部の業務改革推進の観点及び国民へのサービス向上の観点から課題を抽出し、取り組む体制を新たに整備して実行に移す。

## **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、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、計画的かつ効率的執行に向けて、配分予算の執行状況を定期的に把握・計画調整等を行い、役員会に報告する等、引き続き適正な執行管理に努めることにより、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」等に基づき、引き続き、業務達成基準を原則とし、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。  
「独立行政法人会計基準」改訂に基づき、「行政コスト計算書」、「純資産変動計算書」を新たに作成する。また、「独立行政法人の事業報告書に関するガイドライン」に基づき事業報告書を作成する。

## **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、令和2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・助言等を積極的にいき、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とする。
- 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**

地域SCに係る清算分配金を受領した場合には、速やかに処分手続きに着手する。

## **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 事業拡大への対応、安定的な事業実施等を目的として、人材の確保・育成に係る方針の策定及び組織の人員構成等の在り方の見直しに着手し、人員体制の増強を図る。
  - ② 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。
  - ③ 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。
  - ④ 情報セキュリティ対策の実現、IT社会の動向調査・分析・基盤構築、IT人材の育成等の事業を実施するうえで必要となる専門性等を有する人材の採用を図る。
  - ⑤ 中途採用・企業出向者の採用にあたって、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。
  - ⑥ 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。
  - ⑦ 情報セキュリティ等専門性を有する職員について、適性を踏まえたローテーション施策を実施することにより、組織のパフォーマンス向上を図る。
  - ⑧ 労働時間管理の徹底等による長時間労働の削減や年次有給休暇の取得促進など、働き方改革に向けた取組を推進する。
- (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、多角的な評価の実施等により、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51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**

- ① 令和元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、令和2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。特にリスク調査については、リスクの適切な把握を目的として、業務の可視化を行うとともに、効果的なモニタリングが実施されるための取組を行う。併せて、インシデントの取りまとめや共有体制の整備を図る。
- ② 天災や突発的な事故等の非常事態や海外渡航における安全確保に備え、既存の安全管理に関する規程やマニュアル等について、拡充を図る。
- ③ 内部統制活動の一環として、内部(外部)通報やハラスメント等に関する相談に関してより適切に対応するため、相談窓口の外部委託の検討や相談員の増員など環境整備を図るとともに、関連規程の整備などを行い、組織として適切な対応を行えるようにする。
- ④ 機構の業務について、監査法人による外部監査のほかに、監事監査の補助及び内部監査部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、令和2年度「監事監査計画」に基づき内部統制システム(リスク管理)に関する監査等を実施する。また、内部監査については、令和2年度「内部監査計画」に基づき、法人文書管理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。なお、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。  
監事監査及び内部監査の有効性を高めるため、認識されている課題についてフォローアップを行い、課題の解決に対する組織的な取組を促進させる。

## **(2)機構における情報セキュリティの確保**

- ① 機構が保有する個人情報や法人文書の開示請求等に対して、法律に基づき適切な対応を行う。
- ② 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適切に実施するとともに、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。
- ③ 「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。
- ④ 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・運用監視を行う。

## **(3)戦略的広報の推進**

- ① マーケティング・コミュニケーション志向に基づき、目的と対象に適った広報を実施するため、広報戦略の立案・PDCAサイクルを定着させる。ITの活用が拡大する中、これまでリーチできていない新たな層を含めて広くIPAを認知させる手段・戦略を検討し、効果を測定しながら広報施策の継続的な見直しを実施する。機構全体としての広報施策に取り組み、職員へのコミュニケーションを高めて、組織としての一体的な活動を実施する。
- ② 機構ウェブサイトおよびコンテンツ・マネジメントシステム(CMS)について、利用者のアクセスしやすさと管理しやすさの両面に関する実態調査に基づき、刷新に向けた設計を実施する。
- 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を広め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。また、有識者へ広報実績レポートの発行を行う。

- 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。
- ⑦ これらの情報発信活動について、リーチする客層やアクセスの解析を踏まえて戦略的に実施することにより、令和2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	13, 147
国庫補助金	2, 200
受託収入	649
業務収入	7, 590
その他収入	10
計	23, 596
支 出	
業務経費	22, 795
受託経費	649
一般管理費	1, 218
計	24, 661

#### [人件費の見積り]

令和2年度には3, 011百万円を支出する。

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ため、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	-

## 予算(試験勘定)

(単位:百万円)

区 別	金 額
収 入	
業務収入	3,927
その他収入	3
計	3,930
支 出	
業務経費	3,778
一般管理費	212
計	3,990

## [人件費の見積り]

令和2年度には384百万円を支出する。

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	8,999	782	2,460
国庫補助金	2,200	—	—
受託収入	649	—	—
業務収入	3,659	—	4
その他収入	0	—	—
計	15,507	782	2,464
支 出			
業務経費	15,315	782	2,916
受託経費	649	—	—
一般管理費	—	—	—
計	15,964	782	2,916
区 別	債務保証業務	法人共通	合 計
収 入			
運営費交付金	—	906	13,147
国庫補助金	—	—	2,200
受託収入	—	—	649
業務収入	1	—	3,663
その他収入	3	—	3
計	4	906	19,662
支 出			
業務経費	4	—	19,017
受託経費	—	—	649
一般管理費	—	1,006	1,006
計	4	1,006	20,671

## [人件費の見積り]

令和2年度には2,628百万円(情報セキュリティ978百万円、IT人材育成211百万円、社会基盤888百万円、法人共通551百万円)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	—

## 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	17,928
業務費用	14,638
受託経費	649
一般管理費	1,118
減価償却費	1,523
収益の部	
経常収益	19,417
運営費交付金収益	7,780
補助金収益	2,200
受託収入	649
業務収入	7,590
その他収入	22
資産見返負債戻入	1,172
財務収益	4
純利益(△純損失)	1,490
前中期目標期間繰越積立金取崩額	277
目的積立金取崩額	—
総利益(△総損失)	1,767

#### [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	
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	—
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	4,075
業務費用	3,778
一般管理費	212
減価償却費	85
収益の部	
経常収益	3,935
業務収入	3,927
その他収入	3
資産見返負債戻入	5
財務収益	—
純利益(△純損失)	△ 140
前中期目標期間繰越積立金取崩額	6
目的積立金取崩額	—
総利益(△総損失)	△ 134



## 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	9,624	782	2,466
業務費用	7,610	782	2,464
受託経費	649	—	—
一般管理費	—	—	—
減価償却費	1,365	0	2
収益の部			
経常収益	11,234	782	2,466
運営費交付金収益	3,632	782	2,460
補助金収益	2,200	—	—
受託収入	649	—	—
業務収入	3,659	—	4
その他収入	—	—	—
資産見返負債戻入	1,094	0	2
財務収益	0	—	—
純利益(△純損失)	1,610	—	—
前中期目標期間繰越積立金取崩額	271	—	—
目的積立金取崩額	—	—	—
総利益(△総損失)	1,881	—	—
区 別	債務保証業務	法人共通	合 計
費用の部			
経常費用	4	977	13,853
業務費用	4	—	10,860
受託経費	—	—	649
一般管理費	—	906	906
減価償却費	—	72	1,438
収益の部			
経常収益	4	977	15,463
運営費交付金収益	—	906	7,780
補助金収益	—	—	2,200
受託収入	—	—	649
業務収入	1	—	3,663
その他収入	3	—	3
資産見返負債戻入	—	72	1,167
財務収益	0	—	0
純利益(△純損失)	—	—	1,610
前中期目標期間繰越積立金取崩額	—	—	271
目的積立金取崩額	—	—	—
総利益(△総損失)	—	—	1,881

## 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	—
目的積立金取崩額	—
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	29,306
業務活動による支出	16,405
投資活動による支出	8,257
翌年度への繰越	4,645
資金収入	29,306
業務活動による収入	23,596
運営費交付金による収入	13,147
国庫補助金による収入	2,200
受託収入	649
業務収入	7,590
その他収入	10
投資活動による収入	200
当年度期首資金残高	5,510

#### [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	6,139
業務活動による支出	3,990
翌年度への繰越	2,149
資金収入	6,139
業務活動による収入	3,930
業務収入	3,927
その他収入	3
当年度期首資金残高	2,209

## 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	16,878	782	3,820
業務活動による支出	8,259	782	2,464
投資活動による支出	7,705	—	452
翌年度への繰越	914	—	904
資金収入	16,878	782	3,820
業務活動による収入	15,507	782	2,464
運営費交付金による収入	8,999	782	2,460
国庫補助金による収入	2,200	—	—
受託収入	649	—	—
業務収入	3,659	—	4
その他収入	0	—	—
投資活動による収入	—	—	—
当年度期首資金残高	1,371	—	1,356
区 別	債務保証業務	法人共通	合 計
資金支出	429	1,207	23,116
業務活動による支出	4	906	12,415
投資活動による支出	—	100	8,257
翌年度への繰越	425	201	2,444
資金収入	429	1,207	23,116
業務活動による収入	4	906	19,662
運営費交付金による収入	—	906	13,147
国庫補助金による収入	—	—	2,200
受託収入	—	—	649
業務収入	1	—	3,663
その他収入	3	—	3
投資活動による収入	200	—	200
当年度期首資金残高	225	301	3,253

## 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	51
翌年度への繰越	51
資金収入	51
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	47