

令和 2 年 10 月 30 日

(独) 高齢・障害・求職者雇用支援機構
システム総括管理室

民間競争入札実施事業
基幹ネットワークシステム
保守・運用管理の委託業務の実施状況について（案）

1. 事業の概要

「競争の導入による公共サービスの改革に関する法律」（平成 18 年法律第 51 号、以下「公共サービス改革法」という。）に基づく民間競争入札を行い、平成 29 年度から（独）高齢・障害・求職者雇用支援機構基幹ネットワークシステムに係る保守・運用管理業務を実施している。

（1）業務内容の概要（詳細は別紙 1）

- ① インシデント管理
- ② 障害時対応
- ③ 問題管理
- ④ 変更・リリース管理
- ⑤ 構成管理
- ⑥ リソース監視
- ⑦ 稼働監視
- ⑧ ログ管理
- ⑨ 情報セキュリティ監視及び管理
- ⑩ バックアップ及びリストア
- ⑪ 情報システムの操作と管理
- ⑫ 申請書等の業務管理
- ⑬ 機構本部計画停電対応
- ⑭ 監査等への対応
- ⑮ 技術支援
- ⑯ 日次報告
- ⑰ 月次報告と会議
- ⑱ 文書と記録の管理
- ⑲ 保守業務
- ⑳ 基幹ネットワークシステム及び各業務システムの変更等に伴う付随業務
及び技術支援等

(2) 契約期間

平成29年5月1日から令和4年4月30日

(3) 受託事業者

株式会社日立システムズ

(4) 実施状況評価期間

平成29年5月1日から令和2年3月31日

(5) 受託事業者決定の経緯

入札参加者（4者）から提出された基幹ネットワークシステムに係る保守・運用管理業務における提案書等を審査した結果、当機構が定めた評価項目が全て満たされていることを確認した。

平成29年2月17日に開札を行い、総合評価を行った結果、株式会社日立システムズが落札者となった。

2. 確保されるべきサービスの質の達成状況概要（詳細は別紙2）

(1) 確保されるべきサービスの質

ア 業務内容

民間競争入札実施要項「2（1）機構基幹ネットワークシステムに係る保守・運用管理の概要」に示す運用業務を適切に実施すること。

イ 本業務のサービスレベル

本業務の効率化と品質向上並びに円滑化を図るため、予め請負者と機構間においてサービスレベルアグリーメント（SLA）を締結する。

ウ ヘルプデスク利用者アンケート調査結果

年に1回の割合でヘルプデスク利用者に対して、満足度についてアンケートを実施（問合せをした利用者に当該案件に係る満足度について直接記載を依頼し、回収できたものののみ採点対象とする）し、その結果の基準スコア（65点以上）を維持すること。

各質問とも、「満足」（配点100点）、「ほぼ満足」（同80点）、「普通」（同60点）、「やや不満」（同40点）、「不満」（同0点）で採点し、各利用者の回答の平均スコア（100点満点）を算出する。

(2) 達成状況概要

ア 業務内容

受託事業者は、本事業を適切に実施した。

イ 本業務のサービスレベル（詳細は別紙2）

	評価事項	基準値	達成の有無
1	基幹ネットワークサービス提供時間	稼動率95%以上	達成 平均99%
2	サービスレベル報告	月に1度	達成
3	サービスレベルの見直し	6ヶ月に1度	達成
4	満足度調査	65点以上	達成 平均91点
5	インシデント受付第一報対応時間	2時間以内	達成
6	インシデント対応状況報告時間	状況が変化する毎	達成
7	障害検知第一報報告時間	15分以内	達成
8	障害復旧時間	4時間以内	達成
9	障害時進捗連絡時間	4時間毎	達成
10	障害復旧時の報告時間	24時間以内	達成
11	ログ情報提供時間	4時間以内	達成
12	ログ解析頻度	月に1度	達成
13	情報セキュリティ対策の報告	1週間に1度	達成
14	申請受付連絡時間	2時間以内	達成
15	申請処理及び連絡時間	1日以内	達成
16	法定停電計画書提出	実施日の通知から1ヶ月以内	達成
17	法定停電連絡	実施日の3週間前までに連絡	達成
18	日次報告	当日中を取りまとめ翌業務日の午前中までに報告	達成
19	月次報告	当月中を取りまとめ翌月の10日までに報告	達成
20	定例会議	月に1度	達成
21	文書と記録の最新版の確認	1日以内	達成
22	改善報告	月に1度	達成

23	保守業務情報提供	情報入手後から3業務日以内	達成
24	セキュリティ上の重大障害件数	月に0件	達成
25	機構基幹ネットワークシステム運用上の重大障害件数	月に0件	達成

ウ ヘルプデスク利用者アンケート調査結果

上記イ第4項のとおり、平成29年度から令和元年度の満足度調査の結果は平均91点であり、達成すべき質を確保した。

3. 実施経費の状況及び評価

(1) 実施経費（税抜）

単年度あたり：83,604,000円

平成29年5月から令和4年4月まで、418,020,000円

(2) 従来経費（税抜）

単年度あたり：103,304,348円

平成27年6月から平成29年4月まで、198,000,000円

(3) 経費削減効果

「平成27年度契約の実施経費」－「平成29年度契約の実施経費」

従来経費103,304,348円－実施経費83,604,000円
=19,700,348円（単年度あたり）

削減率19.1%

(4) 評価

平成27年度契約と比較して、単年度あたり19,700,348円(19.1%)削減することができた。また、今回の調達では4者応札となったことから、競争性についても改善されたと評価する。

4. 民間事業者からの改善提案による改善実施事項

民間事業者から提出される報告書等において、セキュリティ対策の強化、運用の効率化、利便性の向上等の観点から隨時改善提案がなされ、実施されている。

主な改善事項を以下に示す。（詳細は別紙3）

- ・ インシデント管理 : 2件
- ・ 障害時対応 : 1件
- ・ 構成管理 : 1件
- ・ ログ管理 : 1件
- ・ 情報システムの操作と管理 : 1件
- ・ 申請書等の業務管理 : 1件
- ・ 機構本部計画停電対応 : 1件
- ・ 保守業務 : 2件

5. 機構で設置した外部有識者を含む評価委員会における意見について

（1）評価

「確保されるべきサービスの質及び達成状況」、「実施経費の状況及び評価」及び「民間事業者からの改善提案に関する実施状況」については全て認められる。

（2）意見

市場化テストの終了は妥当と思慮される。なお、市場化テストにより改善された内容について、その要因を分析し、今後に活かし、市場化テスト終了後も更なるサービスの質の向上及びコスト削減がなされることを期待する。

6. 全体的な評価

本業務入札においては、4者からの応札があり、競争性は確保された。これは、市場化テスト実施により、委員等から多くの意見が出され、これまでの運用管理業務の実績に基づく具体的な業務内容の開示等の調達仕様の改善が行われ、新規参入の妨げとなっていた内容が取り払われたためである。

また、民間競争入札実施要項（以下「実施要項」という。）において設定したサービスの質は上記2のとおり確保されており、基幹ネットワークシステム保守・運用管理の委託業務は、全国約170施設の機構職員が効果的かつ円滑に業務を遂行するため、本システムを適正かつ安定的に稼働させるという目的を達成しているものと評価できる。

7. 今後の事業

（1）事業の実施状況

本事業の実施状況は以下のとおりである。

- ① 実施期間中に受託事業者が業務改善命令を受ける又は業務に係る法令違反

行為等を行った事案はなかった。

- ② 実施状況について、月次報告において総括情報セキュリティ管理者及びCIO補佐官からチェックを受けている。また、3ヶ月ごとに行われるSLA評価委員会においては、総括情報セキュリティ管理者及びCIO補佐官に加え、各地方施設の業務を管理する課の長からチェックを受けており、今後も同様のチェックを受ける予定である。
- ③ 入札において、4者からの応札があり、競争性は確保されている。
- ④ 経費について、市場化テスト導入前と比較し、約19.1%の削減効果があった。
- ⑤ 対象公共サービスの確保されるべきサービスの質について、全項目の基準値を達成しており、サービスの質は確保されている。

（2）次期事業の実施

（1）のとおり、本事業については良好な実施結果が得られていることから、次期事業においては、「市場化テスト終了プロセス及び新プロセス運用に関する指針」（平成26年3月19日官民競争入札等監理委員会決定。平成31年3月8日一部改正。）に基づき、終了プロセスに移行した上で、自ら公共サービスの質の維持・向上及び経費削減を図っていくこととしたい。

なお、終了後も公共サービス改革法の民間競争入札のプロセスを通じて進めてきた公共サービスの質、実施期間、入札手続き及び情報開示に関する事項を踏まえた上で、サービスの質の維持向上及びコスト削減を図っていくこととしたい。

【業務内容の詳細】

①インシデント管理

- ・ ヘルプデスクとして、機構役職員及びシステム担当者からの連絡（電話、電子メール、書面、口頭）を受け付ける。
- ・ 保守事業者からの情報や受託事業者が自ら検知した障害等の情報についても、インシデントとして受け付ける。
- ・ 受け付けたインシデントに対応する。
- ・ インシデントを受理したときは、その旨を発信者及びシステム担当者へ通知する。
- ・ 情報セキュリティインシデント発生時においては、上記手順に加えて、機構が定める情報セキュリティインシデント対処手順書等の手順・手続きに従って対処する。

②障害時対応

- ・ 障害対応の体制を整備する。
- ・ 障害状況を把握し、発生時刻、対象機器、障害内容、影響度、影響範囲、想定復旧時刻等を機構のシステム担当者へ報告する。
- ・ 障害箇所を切り分け、サポート業者、保守業者等へエスカレーションする。
- ・ 障害復旧作業を実施する。
- ・ 障害発生から解決に至るまでの進捗状況を、定期的にシステム担当者に報告する。
- ・ 障害復旧時には、障害発生状況、対処方法等をまとめて、システム担当者に書面で報告する。
- ・ 障害発生原因の分析と再発予防・改善等を行う。
- ・ 障害発生時対応の手順をあらかじめ文書化し、システム担当者の承認を得た上で、受託事業者で共有する。

③問題管理

- ・ インシデント（障害を含む）を、発生原因が判明しているものと原因が不明であるものとに分類し、管理する。
- ・ 問題の調査を行い、原因、是正策を特定する。
- ・ 全ての問題について、問題の状態（オープン、クローズ、対応状況等）、原因、是正策等を記録する。

④変更・リリース管理

- ・ 基幹ネットワークシステムに関するすべての変更要求について、効果、優先度、リスクの観点から評価し、変更要求を実現するための最適な実装方

- 法を特定する。
- ・ 変更が失敗した場合に備え、切り戻し手順を変更前にあらかじめ特定する。
 - ・ 変更要求には、変更を要する問題、原因、是正または予防策、リスク評価の結果、実装方法、切り戻し手順を含めることとし、機構が定める導入申請書兼導入実施報告書に記載の上、受託事業者内での承認プロセスを経て、システム担当者に提出し、承認を得る。
 - ・ 承認済みの変更要求を実施（リリース）する。
 - ・ リリースの結果（成功、失敗、失敗した場合の措置等）を記録する。
 - ・ リリース後、変更が有効であったか否かの評価を行い、システム担当者へ報告する。

⑤構成管理

- ・ 基幹ネットワークシステムのハードウェア、ソフトウェアを特定するための情報及びそれらに関連する設定情報、運用手順書などの文書を管理する。
- ・ 基幹ネットワークシステム内の各システムについて、運用管理業務開始時における構成情報を取得し、記録する。
- ・ リリース等により基幹ネットワークシステムの構成が変更された場合は、構成情報を最新の状態に改定し、改訂履歴を維持する。
- ・ 構成情報及び構成情報から参照される設定情報や手順書等は、破損や不正アクセスなどの脅威から適切に保護し、必要な時に直ちに使用できる状態で管理する。
- ・ 構成情報をシステム担当者から求められた場合は、速やかに提供する。

⑥リソース監視

- ・ 管理対象機器のうち、サーバのハードディスク容量・メモリ容量等、各種サーバ構成要素を常時監視する。
- ・ 監視に当たっては、監視方法、監視体制及び閾値を定める。
- ・ 閾値を超えるなどの状況を検知した場合は、上記①及び②の手順により対処する。

⑦稼働監視

- ・ 回線、ネットワーク機器及びサーバの稼働状況をあらかじめ定めた一定の間隔で監視し、監視対象項目の値があらかじめ定めた閾値を超えた場合には、他の関連する項目についても確認・把握し、システム担当者に報告する。
- ・ 監視にはSNMPを利用し、アラートが発生した場合は、目視による確認や他の関連する機器の状態についても状況を把握したうえで、システム

担当者に連絡する。

- ・ 監視により異常を検知した場合は、上記①及び②の手順により対処する。

⑧ログ管理

- ・ 運用手順書において、バックアップ対象データに指定されたログを取得する。
- ・ 取得したログは、適切なアクセス制限管理の下、すべてのログを保管する。
- ・ 取得したログは、システム担当者の求めに応じて、速やかに提出する。

⑨情報セキュリティ監視及び管理

- ・ インターネットメール、WEBサーバ等を含むサーバ、運用管理対象端末に係るマルウェアの感染の監視を行う。
- ・ 基幹ネットワークシステムに不適切なパソコン及びサーバが接続されないよう、検疫システムを利用して監視する。
- ・ JPCERTやIPA等のセキュリティ情報を定期的に取得し、システム担当者に報告する。
- ・ ハードウェアベンダ及びソフトウェアベンダの脆弱性情報、セキュリティパッチ情報を定期的に取得し、システム担当者に報告する。
- ・ 取得した情報を分析し、必要に応じて情報セキュリティ機器（マルウェア対策、スパムメール対策、検疫、標的型攻撃対策、ファイアウォール等）の設定を最適に保つよう、設定変更を行う。
- ・ サーバ及び運用管理対象機器に係るパターンファイル及びセキュリティパッチを常に最適なものに更新し、適切なマルウェア対策ソフトウェアの稼働を確認する。
- ・ 脆弱性診断により脆弱性が指摘された場合は、対象機器に対して、その対策を講じる。
- ・ 情報セキュリティ監査の実施時に、システム担当者からの協力依頼に応じる。
- ・ 情報セキュリティ監査での指摘事項については、システム担当者と協議のうえ、可能な限りの対策を講じる。

⑩バックアップ及びリストア

- ・ バックアップ対象機器に示すサーバを対象とした、バックアップを実施する。
- ・ バックアップが正常に完了しているかを確認し、システム担当者に報告する。
- ・ 障害等が発生した場合は、システム担当者の指示により、最適な方法を検討の上、データのリストア（復元）を行う。

⑪情報システムの操作と管理

- ・ 管理対象機器のO S、パッチ、設定等を最適に維持管理する。設定の変更は、業務影響を最小限にとどめるよう留意する。
- ・ 各システムのアカウントを管理する
- ・ ファイルサーバのアクセス権の管理・設定やディスククォータの設定を行う。
- ・ 旅費計算で使用するソフトウェア（駅すぱあと）のデータ更新。
- ・ 職員用端末のキッティング、送付、在庫管理等を行う。
- ・ 各種管理用帳票（機器台帳、機構LAN構成図等）の維持・管理。
- ・ グループウェアの管理。
- ・ 外部メール（インターネットメール）システムの管理。
- ・ その他、資産管理。
- ・ 人事異動に係るアカウント更新作業及び機構本部端末移設・設定変更作業。

⑫申請書等の業務管理

- ・ ネットワーク機器接続・停止申請に係る対応。
- ・ 施設計画停電申請に係る対応。
- ・ WEBフィルタリング解除申請及びメールブロック解除申請に係る対応。
- ・ 各種アカウント（Windows、グループウェア、外部メールシステム等）申請に係る対応。
- ・ ソフトウェア導入申請に係る対応。

⑬機構本部計画停電対応

- ・ 機構本部の計画停電（年2回）に対応して、事前に計画書を提出のうえ、バックアップや起動・停止作業を適切に実施する。

⑭監査等への対応

- ・ 会計検査院・会計監査法人等の監査、内部監査、情報セキュリティ監査等への対応については、資料作成のほか、必要に応じて当日の立ち合いを行う。

⑮技術支援

- ・ セキュリティ対策作業に係る技術的な提案を行う。
- ・ 基幹ネットワークシステムに係る技術的な提案を行う。

⑯日次報告

- ・ インシデントの発生状況及びその対応状況を報告する。
- ・ 問題管理における特定した問題とは正、予防策、改善策を報告する。
- ・ 申請書等の業務管理における申請受付及びその対応状況を報告する。

⑰月次報告と会議

- ・ 月次報告書を毎月末締めで取りまとめ、運用管理状況報告として、システム担当者に提出する。
- ・ 運用管理業務の報告・説明を行う。また、議事録を作成し、提出、保管する。
- ・ システム担当者の指示に基づき、必要な都度開催される検討会議に出席し、意見や提案を行う。

⑯文書と記録の管理

- ・ 運用管理手順書を整備し、運用手順に変更が生じた場合は、速やかに手順書を改定する。

⑰保守業務

- ・ ハードウェアについては、名称、台数、設置場所を管理し、その一部が追加、変更、撤去された場合及び設置場所が変更となった場合には、運用管理業務に係る手順書、台帳等について必要な変更を適用する。
- ・ ソフトウェアについては、日々の運用で行う、更新、アップグレード、バージョンアップ等を把握し、一元的に管理する。
- ・ ソフトウェアのライセンスに関しては、資産管理のインベントリ情報をを利用して、管理に係る支援業務を行う。
- ・ ハードウェア及びソフトウェアの定期的な保守点検や速やかな障害対応等を実施するため、保守事業者と緊密な連絡体制を整える。
- ・ 障害対応時は、保守事業者と連携し、部品交換等の場合は、保守事業者の作業をサポートする。
- ・ 管理対象機器等に関して、ソフトウェアメーカー、ハードウェアメーカー等からのバージョンアップ情報、サポート切れ情報、不具合情報、脆弱性情報等を収集し、システム担当者に提供する。

⑱基幹ネットワークシステム及び各業務システムの変更等に伴う付随業務及び技術支援等

- ・ 基幹ネットワークシステム及び各業務システムの変更等に伴う技術的な支援、提案等を行う。
- ・ 基幹ネットワークシステム及び各業務システムの各種変更に対する検証、報告等を行う。
- ・ 基幹ネットワークシステム及び各業務システムの変更等に係る打合せ等へ出席する。
- ・ 機構施設ネットワーク及び各業務システムの変更等に伴う回線に係る技術的な支援等を行う。

【確保されるべきサービスの質の達成状況及び評価の詳細】

項目番号	評価事項	内容	基準値※1、※2	評価
1	基幹ネットワークサービス提供時間	利用者が基幹ネットワークを利用できる時間（稼働率）。	稼働率95%以上。ただし、法定停電等、機構と事前に合意された時間を除く。	期間中の稼働率は平均99%であり、サービスの質は確保されている。
2	サービスレベル報告	S LA項目の達成状況及び運用指標の状況報告の頻度。	月に1度。	サービスレベルの達成状況は毎月の定例会で報告されており、サービスの質は確保されている。
3	サービスレベルの見直し	S LA項目及びその値の見直しの頻度。	6ヶ月に1度及び機構及び業務従業者が合意した時。	サービスレベルの見直しについては、6ヶ月に1度行われており、サービスの質は確保されている。
4	満足度調査	運用管理業務の品質の満足度について、利用者及びシステム担当者について調査・分析する。	機構が定める様式を用いたユーザへのアンケートにおいて満足度の平均が100点満点中65点以上。	平均91点であり、サービスの質は確保されている。
5	インシデント受付第一報対応時間	インシデントを受け付けてから、発信者へ受領確認を通知する時間。	電話、口頭（メールを伴う場合もある）による場合は、受け付けた時点で、同時に受領確認通知を行う。 メールのみによる場合は、受け付けか	インシデントの受け付けから発信者へ通知をするまでの時間は基準値を達成しており、サービスの質は確保されている。

			ら、2時間以内に受領確認通知を行う。	
6	インシデント対応状況報告時間	インシデントの対応状況を発信者(システム総括管理室含む)へ定期的に連絡する頻度。	状況が変化する毎に連絡を行うこと(クローズするまで)。	インシデントの対応状況について、状況が変化する毎に連絡が行われており、サービスの質は確保されている。
7	障害検知第一報報告時間	障害を検知した場合、第一報としてシステム担当者へ報告するまでの時間。	15分以内。	15分以内に障害検知の第一報がされており、サービスの質は確保されている。
8	障害復旧時間	障害検知から障害復旧作業を完了するまでの時間。	4時間以内。	障害検知から復旧作業を完了するまでの時間は、4時間以内であり、サービスの質は確保されている。
9	障害時進捗連絡時間	障害発生からクローズまで、状況をシステム担当者に連絡する頻度。	4時間毎。	障害発生からクローズまで、状況をシステム担当者に連絡する頻度は、4時間毎を達成しており、サービスの質は確保されている。

10	障害復旧時の報告時間	障害発生時から書面にて報告を行う時間。	24時間以内。	障害復旧から書面による報告は、24時間以内に行われており、サービスの質は確保されている。
11	ログ情報提供時間	システム担当者の請求からログ情報の提出までの時間。	4時間以内。	ログ情報の提出は、4時間以内に行われており、サービスの質は確保されている。
12	ログ解析頻度	ログの解析を行う頻度。	月に1度。	ログの解析は、月に1度行われており、サービスの質は確保されている。
13	情報セキュリティ対策の報告	情報を入手してからシステム担当者に報告を行う頻度。	1週間に1度。	日々の情報確認結果は日報で報告されており、サービスの質は確保されている。
14	申請受付連絡時間	各種申請書の申請を受け付けた旨を申請者に通知する時間。	受付後、2時間以内。	申請を受け付けた旨の通知は、2時間以内に行われており、サービスの質は確保されている。
15	申請処理及び連絡時間	申請を受け付けてから設定を完了し、申請者に連絡を行うまでの時間。	1日以内。	連絡は1日以内に行われており、サービスの質は確保されている。

16	法定停電計画書提出	法定停電実施日に先立ち、計画書をシステム担当者に提出する時間。	実施日の通知から1ヶ月以内。	計画書の提出は、実施日の通知から1ヶ月以内に行われており、サービスの質は確保されている。
17	法定停電連絡	法定停電実施日に先立ち、関係する施設等へ連絡する時間。	実施日の3週間前までに連絡。	施設等への連絡は実施日の3週間前までに行われており、サービスの質は確保されている。
18	日次報告	日次報告の頻度。	当日中を取りまとめ翌業務日の午前中。	日次報告は期限内に行われており、サービスの質は確保されている。
19	月次報告	月次報告の頻度。	当月中を取りまとめ翌月の10日までに報告。	月次報告は期限内に行われており、サービスの質は確保されている。
20	定例会議	定例会の頻度。	月に1度。	定例会は毎月開催されており、サービスの質は確保されている。
21	文書と記録の管理（最新版の確認）	運用保守手順の変更が承認されてから手順書に反映するまでの時間。	1日以内。	手順書の変更は1日以内に行われており、サービスの質は確保されている。
22	改善報告	継続的改善の状況をシステム担	月に1度。	状況は毎月の定例会で報告されており、サービ

		当者に報告する頻度。		スの質は確保されている。
23	保守業務情報提供	保守におけるソフトウェアメーカー、ハードウェアメーカー等からのバージョンアップ情報、サポート切れ情報、不具合情報、脆弱性情報等を入手してシステム担当者に報告するまでの時間。	情報入手後から3業務日以内。	保守業務情報提供は日報で報告されており、サービスの質は確保されている。
24	セキュリティ上の重大障害件数	個人情報、当機構等に関する情報その他の契約履行に際し知り得た情報漏えいの件数が0件であること。	月に0件であること。ただし、運用業者の責めに帰さない場合を除く。	情報漏えいは発生しておらず、サービスの質は確保されている。
25	機構基幹ネットワークシステム運用上の重大障害件数	長期にわたり正常に稼動できない事態・状況及び保有するデータの喪失等により、業務に多大な支障が生じるような重大障害の件数が0件であること。	月に0件であること。	運用上の重大障害は発生しておらず、サービスの質は確保されている。

※1 基準値に記載する時間については業務時間外、日については業務日外を除く。

※2 基準値に記載する時間については、ハードウェア・ソフトウェア保守事業者の作業時間等、運用管理業者の責に帰さない時間については除く。

【民間事業者からの改善提案による改善実施事項の詳細】

①インシデント管理の改善1

ウィルス対策機能等の通知を受け取った際の対応について、通知ごとの対応手順書を整備することで、対応内容や確認事項をより具体的なものに改善し、インシデント発生時の対応を強化した。

②インシデント管理の改善2

利用者がログインパスワードを失念した場合に、電話によるパスワードリセットの依頼が行われる場合があったが、他者がなりすましてパスワードを初期化する可能性があった。そこで、パスワード初期化についても、申請ツールにより行うこととし、改善した。

③障害時対応の改善

第二 GSOC 及び機構が別途調達する SOC (SHIELD SOC) が導入され、不審通信の監視を行うこととなった。システム導入当初は対応方法が属人化しており、対応に個人差が生じる可能性や作業漏れが生じる可能性があった。そこで、第二 GSOC 及び SHIELD SOC の検知パターンと各パターンに対する手順書を整備した。

④構成管理の改善

機器の更新等に係る作業を別途調達した際に、設計書の更新が正常に行われていない問題が生じた。そこで、運用規則を改善し、設計書を一元管理することで、障害対応やシステム更改時に誤った資料を参照することができるように改善した。

⑤ログ管理の改善

これまで、ユーザのログイン、ログオフ等に係るセキュリティログは確認に時間を要するものであったことから、AD サーバにログオン又はログオフした際に識別用ログを出力する仕組みと、ログを保持する仕組みを整備し、セキュリティインシデント等が発生した際に、ユーザのログイン履歴を迅速に調査することを可能とした。また、この機能を活用し、深夜のログイン状況を調査し、不正ログインがないか確認を行う運用へ改善した。

⑥情報システムの操作と管理の改善

退職等により不要となったアカウントの削除が定期的に行われていなかったため、定期的な不要アカウントの洗い出し及び削除作業を行うことで改善した。

⑦申請書等の業務管理の改善

申請管理ツールについて、「申請書を作業実施日等でソートする機能がない」、「作業進捗の記載欄がない」等の問題があり、作業遅延が発生する可能性があった。そこで、申請書のデータを管理するツールを用意し、改善した。

⑧機構本部計画停電対応の改善

計画停電に係る作業手順書について、対象機器及びチェック項目を見直すことで、作業をより効率化し、短時間に実施できるよう改善した。また、この改善を日時チェックに用いられる確認表にも適用し、改善した。

⑨保守業務の改善 1

一部施設において、端末を管理する機器台帳が独自に整備されていたことから、機器や I P アドレス、利用者等の把握が円滑に行えない問題があった。そこで、共通の機器台帳を整備することで、迅速な対応を可能とした。

⑩保守業務の改善 2

各ソフトウェアの保守サポート期限を確認することが運用上定められていなかったことから、サポート期限切れによる障害が発生する可能性があった。そこで、各機能の主要ソフトウェア、保守サポート期限、確認する U R L リスト等を一覧にまとめ、チェックリストに記載し、定常業務とすることで、ソフトウェアの状態を最適に保つように改善した。