

大多喜浄水場監視制御設備点検業務委託

特記仕様書

令和 8 年度

大多喜浄水場

第1章 総 則

1 適用範囲

本仕様書は、委託者の発注する次の業務委託（以下「本業務委託」という。）に適用するものとし、特に定めなき事項については業務委託契約約款によるものとする。

(1) 業務委託番号：浄委 2026 第 2 号

(2) 業務委託名：大多喜浄水場監視制御設備点検業務委託

(3) 業務委託場所：夷隅郡大多喜町小谷松 500 番地 大多喜浄水場
いすみ市須賀谷1, 293番地2 須賀谷配水池
いすみ市岬町大字鴨根字桑ノ木谷1, 438番地 第 2 配水池
いすみ市大字新田1, 486番地 大原配水池
いすみ市下布施1, 754番地 1 大寺配水池
夷隅郡大多喜町新丁279番地 大多喜配水場
夷隅郡大多喜町八声1, 352番地の 4 八声配水場
夷隅郡大多喜町大字西部田字川島892番地
水資源機構導水制御工

(4) 業務委託期間：契約日から令和 9 年 3 月 3 1 日まで

2 業務委託目的

本業務委託は、大多喜浄水場及び 7 箇所の場外施設に設置されている監視制御設備の機能及び性能維持を図るため、点検を実施するものである。

3 業務実施上の留意事項

(1) 業務実施上の基準及び解釈

受託者は、業務委託契約書、業務委託契約約款及び本仕様書に基づき業務を実施するものとするが、本仕様書に記載されていない事項であっても、業務実施上当然必要と思われるものについては、委託者と協議のうえ実施するものとし、解釈に疑義が生じた場合は相互の協議によるものとする。

(2) 損害

受託者は、業務実施に当たり委託者施設に損傷、又は浄水場等業務に支障を与えないよう十分に注意しなければならない。万一損傷を与えた場合は、直ちに委託者に報告するとともに、その指示に基づき受託者の責任において速やかに原形に復するものとする。

(3) 点検員及び施設の安全確保

受託者は、本業務委託の対象設備に精通した作業員を派遣しなければならない。

受託者は、作業の実施に当たり、委託者と工程の打合せを行い、浄水場等の運転に支障を与えないように作業の工程を計画するとともに、点検員と施設の安全確保を図らなければならない。特に、作業上対象設備の機能停止を必要とする場合は、図面等での確認を行うとともに十分な打合せを行うものとし、不用意に稼働中の装置の電源を断としてはならない。

(4) 作業実施計画

受託者は、事前の打ち合わせ結果に基づき作業実施計画書を作成し、委託者の承諾を得るものとする。また、作業は、開始前に委託者の許可を得て実

施し、終了後に報告するものとする。

(5) 作業時間

本業務委託の作業は、土曜日、日曜日、祝日を除く平日の午前9時から午後5時までの間に実施するものとし、時間を延長する場合は事前に委託者の許可を得なければならない。

(6) 点検員の衛生管理

受託者は水道法に定める定期及び臨時の健康診断並びに委託者の指定する健康診断を受託者の負担で行い、その結果を報告しなければならない。

(7) 作業上の衛生管理

受託者は、本業務委託の作業場所が用水供給施設内であることを認識し、衛生には十分注意しなければならない。また、油脂や薬剤等飲料水に不適なものは、取扱いに特に注意をするとともに、池内及びその上部での油脂類の使用は避けなければならない。

(8) 異常発生時の体制

受託者は、本業務委託の対象設備に故障等の異常が発生した場合に備え、速やかに保守に応じられる体制を常時整えておくものとする。

(9) 工器具及び測定器等

本業務委託に必要な工器具、測定器等は受託者の負担で用意するものとする。なお、使用する計測機器等は、十分な性能及び精度を有するものとし、仕様及び個体を特定できるよう報告書等に記載しなければならない。

但し、電源は設備に支障のない範囲で使用できるものとする。

(10) 軽油

本業務委託で使用する軽油について、JIS規格軽油を使用しなければならない。また、受託者は県税事務所がその他の機関と合同で行う建設機械及び本業務委託に係る車両等を対象とする燃料の抜き取り調査に対しては、委託者の指示により協力しなければならない。

(11) 個人情報

個人情報の取扱いについては、「個人情報等取扱特記事項」により適切に行わなければならない。

4 業務監督職員

- (1) 委託者は、本業務委託における業務監督職員を定め、受託者に通知するものとする。
- (2) 業務監督職員は、受託者に対する指示、承諾、協議等の職務を行うものとする。

5 業務責任者

- (1) 受託者は、契約後直ちに業務責任者を選任し委託者に通知するものとする。
- (2) 業務責任者は、本業務委託全般について、連絡調整に当たるものとする。
- (3) 業務責任者は、業務委託の実施中は現場に常駐しなければならない。

6 業務計画書

- (1) 受託者は、本業務委託の委託後14日以内に業務計画書を作成し、委託者

に提出するものとする。

(2) 業務計画書には、原則として、下記事項を記載するものとする。

- ア 業務内容（目的・概要）
- イ 点検方法等
- ウ 業務分担表
- エ 業務工程表
- オ 安全対策
- カ 緊急時の対応及び体制表
- キ 業務連絡体制表
- ク データの保護及び管理、マルウェア対策について
ただし委託者が指定する委託のみ記載することとする。
- ケ その他、必要事項

7 作業要領書

- (1) 受託者は、設備の重要性を十分理解したうえで、稼働設備機能に支障をきたさぬよう、点検作業を行う前に作業要領書を委託者に提出し、14日前までに承諾を得なくてはならない。
- (2) 作業要領書には、原則、下記事項を記載するものとする。

- ア 作業内容（対象設備・内容）
- イ 作業工程表
- ウ 作業体制
- エ 設備養生箇所・範囲
- オ 設備養生手順

8 腸内細菌検査の実施

浄水場、浄水池その他これらに準ずる水道施設に工事、委託等で延べ30日以上立ち入り作業に従事する者、ろ過池以降の施設で直接水に触れる作業をする者、その他業務監督職員が特に指示する者は、腸内細菌検査を受託者の負担で実施し、その結果を庁舎立入許可申請書とともに業務監督職員に提出しなければならない。

9 提出書類

- | | |
|---|----|
| (1) 業務着手届（着手時） | 2部 |
| (2) 業務責任者等選任通知書（着手時） | 2部 |
| (3) 同上経歴書（着手時） | 2部 |
| (4) 同上直接的かつ恒常的な雇用関係にあることを証明する書類の写し（社会保険証の写し等） | 2部 |
| (5) 業務工程表（着手時、全体工程、変更時） | 2部 |
| (6) 業務計画書（契約後14日以内） | 2部 |
| (7) 作業要領書（点検日の14日前まで） | 2部 |
| (8) 作業日誌・点検結果表（点検時） | 1部 |
| (9) 点検結果報告書 | 2部 |

本業務委託の点検内において部品、機器等に交換又は更新が必要と認められる場合は、交換推奨部品、更新推奨品等を報告書に明記すること。

- (10) 業務完了報告書（完了時） 2 部
(11) 業務記録写真（完了時、黒板に作業日記入） 1 部
写真撮影は、作業前、作業中、作業後を工程毎に鮮明に撮影したデジタル記録とし、C D 及び印画紙相当に印刷する。
データ形式は JPEG とし、サイズは原則として 1,280×960（約 120 万画素）、容量は 300KB 程度とする。
(12) その他、委託者の指定するもの。

1 0 電子納品

- (1) 本業務委託は電子納品対象委託業務とする。電子納品とは、調査、設計、委託などの各業務段階の最終成果を電子データで納品することを言う。ここでいう電子成果品とは、「工事完成図書の電子納品等要領電気通信設備編：（以下、「要領」という。）」に示されたファイルフォーマットに基づいて作成されたものを指す。
(2) 成果品は、「要領」に基づいて作成した電子成果品を電子媒体で正副 2 部提出する。「要領」で特に記載の無い項目については、原則として電子データを提出する義務はないが、「要領」の解釈に疑義がある場合は業務監督職員と協議のうえ、電子化の是非を決定する。
なお、電子納品の運用にあたっては、「千葉県企業局電子納品運用ガイドライン（案）平成 31 年 4 月改訂」等を参考にするものとする。
(3) 委託完成図書の提出の際には、国土交通省の電子納品チェックシステムによるチェックを行い、事前協議でエラーチェックの対象から除外された以外の項目についてエラーが無いことを確認した後、ウィルス対策を実施した上で提出すること。

1 1 データの保護

本業務委託の実施にあたり、データの取扱いについては、別記「データ保護及び管理に関する特記仕様書」を守らなければならない。ただし委託者が指定する委託のみ該当することとする。

1 2 マルウェア対策

本業務委託の実施にあたり、外部記録媒体等によるデータを持ち込んで作業を行う場合は、事前にマルウェア対策を実施しなければならない。また作業員の身分が確認できるようにしなければならない。

1 3 業務委託料の支払方法

委託料の支払いは業務完了後、一括支払いとする。

第2章 業務内容

1 概要

本業務委託は、大多喜浄水場及び7箇所の場合外施設に設置されている監視制御設備の機能及び性能維持を図るため、点検を実施するものである。

(1) 中央監視制御設備点検

分散型制御用計算機設備巡回点検 . . . 2回/年
分散型制御用計算機設備精密点検 . . . 1回/年
ウイルス検査 1回/年
リモート接続 一式
年間保守業務 一式

(2) 遠方監視制御設備点検

親局 . . . 一式 (大多喜浄水場)
子局 . . . 7箇所 (須賀谷配水池、第2配水池、大原配水池、大寺配水池、
大多喜配水池、八声配水池、水資源機構導水制御工)

2 対象設備

代表機器のみを記す。記載なき盤内の実装機器についても点検対象とする。

(1) 中央監視制御設備

ア 二重化フィールドコントロールユニット (AFV30D) . . . 5台
イ ESBバス二重化用ノードユニット
ANB10D . . . 12台
ANB11D . . . 3台
ウ 監視操作装置
HTHIS6555 . . . 3台 (内1台保守用PC)
HTHIS6545 . . . 1台
エ 帳票用PC (HJ6555) . . . 1台
オ Vnet/IP用ネットワークスイッチ (GRVSW) . . . 8台 (内2台予備品)
カ プリンタ
帳票用 (LBP442) . . . 1台
監視用 (LBP842C) . . . 1台
キ タイムサーバ (TS-2210) . . . 1台

(2) 遠方監視制御設備 (基本構成)

ア 親局 (インターフェース盤 (2)、(3)) 2面
(ア) テレメータ TL500-BS1S-01 21台
(イ) 外付け電話呼び出しユニット TL500-AU2S-20 1台
(ウ) 専用電話器 ELTEL FT-4W 1台
(エ) 通信用避雷器 TL500-SF112 21台
イ 子局7箇所
(ア) テレメータ TL500-BS1S-01 7台
(イ) 外付け電話呼び出しユニット TL500-AU2S 7台
(ウ) 専用電話器 ELTEL FT-4W 7台
(エ) 通信用避雷器 TL500-SF112 7台

- (オ) アナログ入力モジュール FL100-AT71S-08/10・・・7 台
- (カ) アナログ出力モジュール FL100-AR71S-04/20・・・12 台
- (キ) デジタル入力モジュール FL100-DT71S-16・・・25 台
- (ク) デジタル出力モジュール FL100-DR71S-16・・・6 台
- (ケ) アイソレータ YJH1-017-AAN0・・・32 台

3 点検内容

1 中央監視制御設備 分散型制御用計算機設備 巡回点検内容

原則として機器を停止せずに作業を実施する。契約期間内に 2 回の点検を実施する。

点検内容は製造者標準の点検要領とし、業務監督職員の承諾を得て実施すること。

点検表には基準値を記載し、合わせて基準値の根拠を添付すること。点検報告書には各機器の総合所見を記載すること。また、点検報告書は点検後速やかに提出すること。

(1) 共通検査項目

ア 設置環境調査

設置状態等について、システムが動作するのに十分な環境であることを確認する。また、損傷や欠陥（特に結露跡や腐食）がないことを目視により点検する。システムの設置環境にとって好ましくない状態を見出した場合、処置方法、改善方法等について業務監督職員に提示すること。

イ 稼働状態確認

システム稼働状態画面にてステータス表示が正常であることを確認する。
また、ステータスランプが付いているカード・機器ではステータス表示が正常であることを確認する。

ウ 盤共通部確認

照明消光、ファン動作、異音の有無等の各部の確認、フィルタの清掃を行う。

エ 各端子、コネクタの増し締め

システム構成盤機器内の各端子の増し締めを行う。

(2) 対象機器毎の点検項目

ア 二重化フィールドコントロールユニット (AFV30D)

(ア) 稼働状態確認

各カードが所定の位置に実装され、RDY ランプが点灯していることを確認する。また、ステータスランプが付いているカードでは、ステータス表示が正常であることを確認する。

(イ) 総合検査

システム稼働状態画面にて、各部の異常がないこと、CPU アイドルタイムに問題がないことを確認する。

(ロ) 機器の稼働情報及び設置環境情報の確認

CPU 使用率、CPU 温度を確認する。

イ ESB バス二重化ノードユニット (ANB10D・ANB11D)

(ア) 稼働状態確認

各カードが所定の位置に実装され、RDY ランプが点灯していることを確認する。また、ステータスランプが付いているカードでは、ステータス表示が正常であることを確認する。

(イ) 総合検査

システム稼働状態画面にて、各部の異常がないことを確認する。

ウ 監視操作装置 (HTHIS6545・HTHIS6555)

(ア) 稼働状態確認

ステータスランプが付いているカードでは、ステータス表示が正常であることを確認する。

(イ) 各部清掃

本体（フィルタ含む）・モニタの外観清掃を実施する。

(ウ) 冷却ファン検査

ファンの回転状況・異音の有無を確認する。

(エ) モニタ機能検査

画面に表示された文字・表示色等について、歪み・輝度の劣化、焼き付き・ドット抜け等が目視にて認められないことを検査する。色ずれが発生している場合は、画面調整を実施する。また、タッチパネル機能を有する物は、操作に応じた入力ができることを確認し、ずれが生じている場合は調整を行う。

(オ) ハードディスク検査

使用率、空き容量の確認を行う。また、エラーログを収集し機器に問題がないことを確認する。

(カ) 総合検査

ソフトウェアのアプリケーション設定を確認する。

各種ログに異常がないこと及び操作監視機能に問題がないことを確認する。

(キ) 機器の稼働情報及び設置環境情報の確認

CPU 使用率、DISK 使用率、物理メモリ使用率、ネットワーク使用率、イベントログを確認する。

エ 帳票用 PC (HJ6555)

(ア) 稼働状態確認

ステータスランプが付いているカードでは、ステータス表示が正常であることを確認する。

(イ) 各部清掃

本体（フィルタ含む）・モニタの外観清掃を実施する。

(ウ) 冷却ファン検査

ファンの回転状況・異音の有無を確認する。

(エ) モニタ機能検査

画面に表示された文字・表示色等について、歪み・輝度の劣化、焼き付き・ドット抜け等が目視にて認められないことを検査する。色ずれが発生している場合は、画面調整を実施する。

(オ) ハードディスク検査

使用率、空き容量の確認を行う。また、エラーログを収集し機器に問題

がないことを確認する。

(カ) 総合検査

各種ログに異常がないこと及び他の接続機器と正常に通信ができること、帳票(Trifellows)機能に問題がないことを確認する。

(キ) 機器の稼働情報及び設置環境情報の確認

CPU 使用率、DISK 使用率、物理メモリ使用率、ネットワーク使用率、イベントログを確認する。

オ V-net/IP ネットワークスイッチ (GRVSW)

(ア) 稼働状態確認

ハードウェアランプの点灯状態を確認し、異常がないことを確認する。

(イ) 外観清掃

外観清掃を実施し、損傷や欠陥がないことを目視により点検する。

ケーブル接続状態を目視・触手により確認する。

カ プリンタ (LBP442・LBP842 C)

(ア) 稼働状態確認

損傷や欠陥がないことを目視により点検し、ステータス表示が正常であることを確認する。

(イ) 各部清掃

プリンタ本体の外観、内部清掃を行う。

(ウ) 印字機能検査

テスト印字により印刷品質を確認し、必要に応じて適宜調整を行う。

オンラインで他の接続機器から正常に印刷ができることの確認を行う。

また、ステータスプリントにより各種状態・設定の確認を行う。

キ タイムサーバ (TS-2210)

(ア) 稼働状態確認

ハードウェアランプの点灯状態及び LCD パネル表示を確認し、異常がないことを確認する。

(イ) 外観清掃

外観清掃を実施し、損傷や欠陥がないことを目視により点検する。

ケーブル接続状態を目視・触手により確認する。

2 中央監視制御設備 分散型制御用計算機設備 精密点検基準

この点検実施基準は、分散型制御用計算機設備等に対する精密点検に適用する。

点検内容は製造者標準の点検要領とし、業務監督職員の承諾を得て実施すること。点検表には基準値を記載し、合わせて基準値の根拠を添付すること。点検報告書には各機器の総合所見を記載すること。また、点検報告書は点検後速やかに提出すること。

(1) 対象装置
【制御装置関係】

盤			主な機器		
設置場所	名称	COMP	型式	STN	COMP
管理本館 1 階 電気室	管理本館分散型制御装置盤	100	AFV30D	301	101
			ANB10D	－	102
	管理本館 No. 1 中継リレー盤	110	ANB10D	－	111
	管理本館 No. 2 中継リレー盤	120	－	－	－
薬注棟電気室	薬注 No. 1 中継リレー盤	130	ANB11D	－	131
			ANB10D	－	132
	薬注 No. 2 中継リレー盤	140	ANB10D	－	141
			ANB10D	－	142
薬注 No. 3 中継リレー盤	薬注 No. 3 中継リレー盤	150	－	－	－
			－	－	－
	粉末活性炭注入 No. 1 中継リレー盤	160	ANB11D	－	161
			ANB10D	－	171
ろ過池電気室	沈殿池分散型制御装置盤	200	AFV30D	302	201
			GRVSW	－	202
沈殿池電気室	沈殿池 No. 1 中継リレー盤	210	ANB11D	－	211
	沈殿池 No. 2 中継リレー盤	220	ANB10D	－	221
ろ過池電気室	ろ過池分散型制御装置盤	300	AFV30D	303	301
			GRVSW	－	302
	ろ過池 No. 1 中継リレー盤	310	ANB10D	－	311
	ろ過池 No. 2 中継リレー盤	320	ANB10D	－	321
送水ポンプ棟 電気室	送水ポンプ分散型制御装置盤	400	AFV30D	304	401
			GRVSW	－	402
			GRVSW	－	403
	送水ポンプ No. 1 中継リレー盤	410	ANB10D	－	411
	送水ポンプ No. 2 中継リレー盤	420	ANB10D	－	421
管理本館 2F 計算機室	場外監視用分散型制御装置盤	500	AFV30D	305	501
			ANB10D	－	502
	遠方インターフェース盤(1)	510	－	－	－
	遠方インターフェース盤(2)	520	－	－	－
	遠方インターフェース盤(3)	530	－	－	－
	光・電変換器盤	600	GRVSW	－	601
			GRVSW	－	602
			GRVSW	－	予備
			GRVSW	－	予備
			TS(タイムサーバ)	－	604
	電源分電盤	700	－	－	－
	汎用 UPS (表示確認)	－	BM15K-30FNF	－	－

【監視装置関係】 ※ 専用デスク (G DESK2 8 台) を含む。

設置場所	機器名称	STN	COMP	型式
管理本館 2F 中央管理室	監視制御装置 (1) 工業用	3. 6	62	HTHIS6555
	監視制御装置 (2) 工業用	3. 6	63	HTHIS6555
	帳票用 PC 工業用	3. 4	41	HTHIS6555
	監視制御装置 (3) 工業用	3. 3	230	HTHIS6545
	監視用プリンタ	－	605	LBP842 C
	帳票用プリンタ	－	606	LBP442
管理本館 2F 計算機室	監視制御装置保守用	3. 6	64	HTHIS6555

(2) 精密点検内容

機器停止を行い、契約期間中に 1 回の作業を実施する。機器停止により稼働施設に影響を及ぼすことが考えられる場合は停止を伴わない点検とするが、作業要領書等にて業務監督職員の承諾を得ること。

ア 共通検査項目

(ア) 設置環境調査

設置状態等について、システムが動作するのに十分な環境であることを確認する。

また、損傷や欠陥（特に結露跡や腐食）がないことを目視により点検する。システムの設置環境にとって好ましくない状態を見出した場合、処置方法、改善方法等について業務監督職員に提示すること。

(イ) 状態の確認

a 稼働状態確認

システム稼働状態画面にてステータス表示が正常であることを確認する。また、ステータスランプが付いているカード・機器ではステータス表示が正常であることを確認する。

b 機器情報確認

ハードウェア型式、製造番号、製造年月、レビジョンやソフトウェアのインストール情報、レビジョンの確認を行う。

c ソフトウェアのバックアップ

点検前にシステムアプリケーションソフトウェア、各種設定情報のバックアップを取得する。

(ロ) 各部清掃

盤内外及びシステム構成機器外観に付着している塵埃や汚れを除去するための清掃作業を行う。

(ハ) 盤共通部確認

ブレーカー遮断機能、ヒューズ溶断・挿入状態、照明消光、ファン動作・異音の有無等各部の確認を行う。

(ニ) 各部スイッチ動作確認

操作、切替（選択）スイッチの作動確認を行う。

(ホ) 電源電圧検査

a 供給電源電圧検査

機器に供給される AC 電源電圧を測定し、許容範囲内であることを確認する。

b 電源装置電圧検査

各機器の電源装置電圧を測定し、許容範囲内であることを確認する。

(キ) 各端子、コネクタの増し締め

システム構成盤機器の各端子の増し締めを行う。また、プラグイン・カードコネクタ、ヒューズホルダ、ネジ止め部の損傷や欠陥、内部ケーブルのねじれ、破損がないことを目視確認する。

イ 対象機器毎の点検項目

(ア) 二重化フィールドコントロールユニット (AFV30D)

a 稼働状態確認

各カードが所定の位置に実装され、RDY ランプが点灯していることを確認する。また、ステータスランプが付いているカードでは、ステータス表示が正常であることを確認する。点検前にチューニングパラメータのセーブを実施する。

b 各部分解清掃

構成機器、構成機器内の実装カードについて清掃を実施し、損傷や欠陥がないことを目視により点検する。プラグイン・カードコネクタ、ヒューズホルダ、ネジ止め部の損傷や欠陥、内部ケーブルのねじれ、破損がないことを目視・触手により確認する。

c 電源電圧検査

・供給電源電圧検査

機器に供給される AC 電源電圧を測定し、許容範囲内であることを確認する。

・電源装置電圧検査

各機器の電源装置電圧を測定し、許容範囲内であることを確認する。

・バッテリー検査

バッテリーの充電電圧を測定し、規定範囲内であることを確認する。
また、有効期限が切れていないことを併せて確認する。

d CPU 機能検査

自己診断プログラム及びテストプログラムにて機能検査を行い、正常であることを確認する。

e メモリ機能検査

テストプログラムにて機能検査を行い、全領域に対する読込動作が正常であることを確認する。

f V-net/IP 通信検査

監視操作装置 (HTHIS6545・HTHIS6555) によりロード・セーブが正常に行えることを確認する。

g ESB/ER バス通信検査

モジュールに内蔵されている自己診断プログラム及びシステムプログラムにより検査を行い、任意のノードユニットに対して正常に通信することを確認する。

h 冗長化機能検査

システムにて制御権が正常に切り替わることを確認する。

i 警報接点機能 (外部インターフェースユニット) 検査

CPU 異常又はユニット電源断にて警報出力接点が正常に動作することを確認する。

j 入出力精度検査

テストプログラムにより全点検査を行う。なおアナログ入出力については、信号入出力ネスト(D E、MHC)と組合せで行う。

・アナログ入力検査

各モジュールのハードウェアの入力仕様に合わせ入力信号を印可し、読込誤差が入力信号精度定格以下であることを確認する。(3点試験)

・アナログ出力検査

各モジュールのハードウェアの出力仕様に合わせ出力信号を設定し、出力値が出力信号精度定格以下であることを確認する。(3点試験)

・デジタル入力検査

各入力点に対して接点による入力信号を印可し、そのときの入力値が正常であることを確認する。

・デジタル出力検査

各出力点に対して出力信号を設定し、そのときの出力値が正常であることを確認する。

・パルス入力検査

各入力点に対してパルス信号を印可し、入力パルス数とカウントした値が同じことを確認する。

k 通信検査

通信インターフェースユニット(FA-M3)等のサブシステムとのデータ送受信を行い、正常に通信ができることを確認する。

l 総合検査

システム稼働状態画面にて、各部の異常がないこと、CPU アイドルタイムに問題がないことを確認する。

m 機器の稼働情報及び設置環境情報の確認

CPU 使用率、CPU 温度を確認する。

(イ) ESB バス二重化ノードユニット(ANB10D・ANB11D)

a 稼働状態確認

各カードが所定の位置に実装され、RDY ランプが点灯していることを確認する。また、ステータスランプが付いているカードでは、ステータス表示が正常であることを確認する。

b 各部分解清掃

構成機器、構成機器内の実装カードについて清掃を実施し、損傷や欠陥がないことを目視により点検する。プラグイン・カードコネクタ、ヒューズホルダ、ネジ止め部の損傷や欠陥、内部ケーブルのねじれ、破損がないことを目視・触手により確認する。

c 電源電圧検査

・供給電源電圧検査

機器に供給される AC 電源電圧を測定し、許容範囲内であることを確認する。

- ・電源装置電圧検査
各機器の電源装置電圧を測定し、許容範囲内であることを確認する。
- d ESB/ER バス通信検査
モジュールに内蔵されている自己診断プログラム及びシステムプログラムにより検査を行い、任意のノードユニットに対して正常に通信することを確認する。
- e 冗長化機能検査
システムにて制御権が正常に切り替わることを確認する。
- f 入出力精度検査
テストプログラムにより全点検査を行う。なおアナログ入出力については、信号入出力ネスト(D E、MHC)と組合せで行う。
 - ・アナログ入力検査
各モジュールのハードウェアの入力仕様に合わせ入力信号を印可し、読込誤差が入力信号精度定格以下であることを確認する。(3点試験)
 - ・アナログ出力検査
各モジュールのハードウェアの出力仕様に合わせ出力信号を設定し、出力値が出力信号精度定格以下であることを確認する。(3点試験)
 - ・デジタル入力検査
各入力点に対して接点による入力信号を印可し、そのときの入力値が正常であることを確認する。
 - ・デジタル出力検査
各出力点に対して出力信号を設定し、そのときの出力値が正常であることを確認する。
 - ・パルス入力検査
各入力点に対してパルス信号を印可し、入力パルス数とカウントした値が同じことを確認する。
- g 通信検査
通信インターフェースユニット(FA-M3)等のサブシステムとのデータ送受信を行い、正常に通信ができることを確認する。
- h 総合検査
システム稼働状態画面にて、各部の異常がないことを確認する。
- (ウ) 監視操作装置(HTHIS6545・HTHIS6555)
 - a 稼働状態確認
ステータスランプが付いているカードでは、ステータス表示が正常であることを確認する。併せてウィルス感染の有無を検査し、ハードディスク構成情報やOSを含むディスクイメージのフルバックアップを行う。ウィルスが発見された場合、即時、業務監督職員に報告しその対応について協議する(3 ウィルス検査を参照)。
 - b 各部分解清掃
構成機器、構成機器内の実装カードやキーボード・マウス・モニタ・UPSについて清掃を実施し、損傷や欠陥がないことを目視により点検す

る。プラグイン・カードコネクタ、ヒューズホルダ、ネジ止め部の損傷や欠陥、内部ケーブルのねじれ、破損がないことを目視・触手により確認する。

c 電源電圧検査

・供給電源電圧検査

機器に供給される AC 電源電圧を測定し、許容範囲内であることを確認する。

・バッテリー検査

バッテリーの充電電圧を測定し、規定範囲内であることを確認する。

また、有効期限が切れていないことを併せて確認する。

・冷却ファン検査

ファンの回転状況・異音の有無を確認する。

・モニタ機能検査

画面に表示された文字・表示色等について、歪み・輝度の劣化、焼き付き・ドット抜け等が目視にて認められないことを検査する。色ずれが発生している場合は、画面調整を実施する。また、タッチパネル機能を有する物は、操作に応じた入力ができることを確認し、ずれが生じている場合は調整を行う。

d キーボード検査

全てのキーを操作し、それぞれのキーに対応する入力が入ることを確認する。また、オペレータキーボードについては、ランプ点灯、ブザー鳴動することも確認する。

e マウス検査

マウス装置を操作し、それに対応した入力が入ることを確認する。

f UPS 機能検査

通電稼働中に UPS 供給電源を停止させ、正常に自動シャットダウンすることを確認する。

g 光学ドライブ検査

DVD-RAM の書き込み・読み出しが正常に行えることを確認する。また、ドライブのクリーニングを行うこと。

h ハードディスク検査

ディスク装置メディア領域内に対して、正常に書き込み・読み出し動作が行えることを検査する。使用率、空き容量の確認を行う。また、エラーログを収集し機器に問題がないことを確認する。

i CPU 機能検査

自己診断プログラム及びテストプログラムにて機能検査を行い、正常であることを確認する。

j メモリ機能検査

テストプログラムにて機能検査を行い、全領域に対する読込動作が正常であることを確認する。

k V-net/IP 通信検査

二重化フィールドコントロールユニット (AFV30D) にロード・セーブが正常に行えること、他監視操作装置 (HTHIS6545・HTHIS6555) と正常に通信できることを確認する。

1 総合検査

ソフトウェアのアプリケーション設定を確認する。各種ログに異常がないこと及び操作監視機能に問題がないことを確認する。

m 機器の稼働情報及び設置環境情報の確認

CPU 使用率、DISK 使用率、物理メモリ使用率、ネットワーク使用率、イベントログを確認する。

(エ) 帳票用 PC (HJ6555)

a 稼働状態確認

ステータスランプが付いているカードでは、ステータス表示が正常であることを確認する。併せてウィルス感染の有無を検査し、ハードディスク構成情報や OS を含むディスクイメージのフルバックアップを行う(3 ウィルス検査を参照)。

ウィルスが発見された場合、即時、業務監督職員に報告し、その対応について協議する。

b 各部分解清掃

構成機器、構成機器内の実装カードやキーボード・マウス・モニタ・UPS について清掃を実施し、損傷や欠陥がないことを目視により点検する。プラグイン・カードコネクタ、ヒューズホルダ、ネジ止め部の損傷や欠陥、内部ケーブルのねじれ、破損がないことを目視・触手により確認する。

c 電源電圧検査

・供給電源電圧検査

機器に供給される AC 電源電圧を測定し、許容範囲内であることを確認する。

・バッテリー検査

バッテリーの充電電圧を測定し、規定範囲内であることを確認する。
また、有効期限が切れていないことを併せて確認する。

d 冷却ファン検査

ファンの回転状況・異音の有無を確認する。

e モニタ機能検査

画面に表示された文字・表示色等について、歪み・輝度の劣化、焼き付き・ドット抜け等が目視にて認められないことを検査する。色ずれが発生している場合は、画面調整を実施する。

f キーボード検査

全てのキーを操作し、それぞれのキーに対応する入力が入ることを確認する。

g マウス検査

マウス装置を操作し、それに対応した入力が入ることを確認する。

h UPS 機能検査

通電稼働中に UPS 供給電源を停止させ、正常に自動シャットダウンすることを確認する。

i 光学ドライブ検査

DVD-RAM の書き込み・読み出しが正常に行えることを確認する。また、ドライブのクリーニングを行うこと。

- j ハードディスク検査
ディスク装置メディア領域内に対して、正常に書き込み・読み出し動作が行えることを検査する。使用率、空き容量の確認を行う。また、エラーログを収集しシステムに問題がないことを確認する。
- k CPU 機能検査
自己診断プログラム及びテストプログラムにて機能検査を行い、正常であることを確認する。
- l メモリ機能検査
テストプログラムにて機能検査を行い、全領域に対する読込動作が正常であることを確認する。
- m 総合検査
各種ログに異常がないこと及び他の接続機器と正常に通信ができること、帳票(Trifellows)機能に問題がないことを確認する。
- n 機器の稼働情報及び設置環境情報の確認
CPU 使用率、DISK 使用率、物理メモリ使用率、ネットワーク使用率、イベントログを確認する。
- (オ) V-net/IP 用ネットワークスイッチ (GRVSW)
 - a 稼働状態確認
ハードウェアランプの点灯状態を確認し、異常がないことを確認する。
 - b 外観清掃
外観清掃を実施し、損傷や欠陥がないことを目視により点検する。ケーブル接続状態を目視・触手により確認する。
 - c 供給電源電圧検査
機器に供給される AC 電源電圧を測定し、許容範囲内であることを確認する。
 - d システム状態検査
ログ内容を検査し、異常がないことを確認する。また、設定内容をバックアップする。
 - e 総合検査
自己診断（電源 Off/On）にて正常に起動することを確認し、システム稼働状態画面にて通信が正常であることを確認する。
- (カ) プリンタ (LBP442・LBP842 C)
 - a 稼働状態確認
損傷や欠陥がないことを目視により点検し、ステータス表示が正常であることを確認する。
 - b 各部清掃
プリンタ本体の外観、内部清掃を行う。
 - c 総合検査
自己診断（電源 Off/On）にて正常に起動することを確認する。
 - d 印字機能検査
テスト印字により印刷品質を確認し、必要に応じて適宜調整を行う。オンラインで他の接続機器から正常に印刷ができることの確認を行う。また、ステータスプリントにより各種状態・設定の確認を行う。

(キ) タイムサーバ(TS-2210)

a 稼働状態確認

ハードウェアランプの点灯状態及び LCD パネル表示を確認し、異常がないことを確認する。また、保管情報（統計情報・中継情報・ログ）を確認し、保管設定情報を保存・エクスポートする。

b 外観清掃

外観清掃を実施し、損傷や欠陥がないことを目視により点検する。
ケーブル接続状態を目視・触手により確認する。

c 供給電源電圧検査

機器に供給される AC 電源電圧を測定し、許容範囲内であることを確認する。

d 総合検査

自己診断（電源 Off/On）にて正常に起動すること、時刻合わせが正常に行えることを確認する。

3 ウィルス検査

契約期間内に 1 回、精密点検時に CENTUM-VP システムの HIS について、ウィルス検査及びシステムのバックアップを行う。

(1) ウィルス検査

オフライン環境でウィルス検索ソフトを使用し、ウィルスの検査を行う。

ウィルスが発見された場合、即時業務監督職員に報告しその対応について協議する。

(2) システムバックアップ

オフライン環境でバックアップソフトを起動する。ハードディスクの内容全てをイメージとして外付けハードディスクにバックアップし、もう 1 台のハードディスクにコピーする。

4 リモート接続

電話回線を使用してオンラインにて常時接続する。異常発生時には障害情報収集、障害箇所の切り分け及び特定等を行う。

(1) 計算機の保護

本業務委託では、リモート接続に伴い計算機による通信を使用するが、コンピュータウィルス等が計算機に障害を発生させる汚染をもたらさないよう十分な注意・対策を実施しなければならない。これにより、設備に損害を与えた場合は、速やかに業務監督職員に連絡の上、受託者の負担で復旧するものとする。

5 年間保守業務

制御用計算機設備に故障・不具合等が発生した場合及び調整が必要な場合、業務監督職員から異常の連絡を受けた場合は、原因の如何に関わらず速やかに業務監督職員と協議の上、迅速に技術者を派遣し正常に復旧させるものとする。この場合、本業務委託の点検に起因する軽微なものについては本業務委託

の役務に含むものとし、その他については協議するものとする。

6 遠方監視制御設備 点検内容

遠方監視制御装置（親局、子局）について、以下の項目の点検を行うと共に各部の清掃及び調整を実施するものである。

- (1) 内外観目視点検
- (2) 各部清掃
- (3) スイッチの設定確認
- (4) LED 状態表示の確認
- (5) 電源電圧確認/リップル波形測定
- (6) ビス締付/コネクタ接続確認
- (7) 送信/受信レベルの測定/良否判定
- (8) 対向試験（親局～子局間）
- (9) 呼び出し確認（専用電話器）
- (10) 入出力試験
- (11) 総合機能確認

個人情報等取扱特記事項

第1 基本的事項

受託者は、個人情報等の保護の重要性を認識し、この契約による事務の実施に当たっては、個人の権利利益を侵害することのないよう、個人情報等の取扱いを適正に行う。

第2 事務従事者への周知及び監督

(事務従事者への監督)

- 1 受託者は、この契約による事務を行うために取扱う個人情報等の適切な管理が図られるよう、事務従事者に対して必要かつ適切な監督を行う。

(事務従事者への周知)

- 2 受託者は、事務従事者に対して、次の事項等の個人情報等の保護に必要な事項を周知させるものとする。
 - (1) 事務従事者又は事務従事者であった者は、その事務に関して知り得た個人情報等をみだりに他人に知らせてはならないこと
 - (2) 事務従事者又は事務従事者であった者は、その事務に関して知り得た個人情報等を不当な目的に使用してはならないこと

第3 個人情報等の取扱い

(収集の制限)

- 1 受託者は、この契約による事務を行うために個人情報等を収集するときは、当該事務の目的を達成するために必要な範囲内で、適法かつ公正な手段によりこれを行う。

(秘密の保持)

- 2 受託者は、この契約による事務に関して知り得た個人情報等をみだりに他人に知らせてはならない。この契約が終了し、又は解除された後においても、同様とする。

(漏えい、滅失及びき損の防止等)

- 3 受託者は、この契約による事務に関して知り得た個人情報等について、個人情報等の漏えい、滅失及びき損の防止その他の個人情報等の適切な管理のために必要な措置を講じる。

(持ち出しの制限)

- 4 受託者は、委託者が承諾した場合を除き、この契約による事務を委託者が指定した場所で行い、個人情報等が記録された機器、記録媒体、書類等（以下「機器等」という。）を当該場所以外に持ち出してはならない。

(目的外利用及び提供の制限)

- 5 受託者は、委託者の指示がある場合を除き、個人情報等をこの契約の目的以外の目的のために利用し、又は委託者の承諾なしに第三者に対して提供してはならない。

(複写又は複製の制限)

- 6 受託者は、この契約による事務を処理するために委託者から引渡された個人情報等が記録された機器等を委託者の承諾なしに複写又は複製してはならない。

第4 再委託の制限

受託者は、委託者が承諾した場合を除き、この契約による事務については自ら行い、第三者にその取扱いを委託してはならない。

第5 事故発生時における報告

受託者は、この契約に違反する事態が生じ、又は生じるおそれのあることを知ったときは、速やかに委託者に報告し、委託者の指示に従うものとする。

第6 情報システムを使用した処理

受託者は、情報システムを使用してこの契約による事務を行う場合には、この特記事項のほか、最高情報セキュリティ責任者（総務部デジタル改革推進局デジタル推進課が所管する千葉県情報セキュリティ対策基準（平成14年3月15日制定）5（1）アに規定する職にある者をいう。）の定める「データ保護及び管理に関する特記仕様書」等を遵守する。

第7 機器等の返還等

受託者は、この契約による事務を処理するために、委託者から提供を受け、又は受託者自らが収集し、若しくは作成した個人情報等が記録された機器等は、この契約完了後直ちに委託者に返還し、又は引渡すものとする。ただし、委託者が別に作業の方法を指示したときは、当該方法によるものとする。

第8 委託者の調査、指示等

（調査、指示等）

- 1 委託者は、受託者がこの契約により行う個人情報等の取扱状況を随時調査し、又は監査することができる。この場合において、委託者は、受託者に対して、必要な指示を行い、又は必要な事項の報告若しくは資料の提出等を求めることができる。
（公表）
- 2 委託者は、受託者がこの契約により行う事務について、情報漏えい等の個人情報等を保護する上で問題となる事案が発生した場合には、個人情報等の取扱いの態様、損害の発生状況等を勘案し、受託者の名称等の必要な事項を公表することができる。

第9 契約の解除及び損害の賠償

- 1 委託者は、次の各号のいずれかに該当するときは、この契約を解除し、及び受託者に対して損害の賠償を請求することができる。
 - （1）受託者又は受託者の委託先（順次委託が行われた場合におけるそれぞれの受託者を含む。）の責めに帰すべき事由による情報漏えい等があったとき
 - （2）受託者がこの特記事項に違反し、この契約による事務の目的を達成することができないと認められるとき

注

- 1 委託に係る事務の実態に則して、適宜必要な事項を追加し、不要な事項は省略することとする（例：仮名加工情報、行政機関等匿名加工情報等及び匿名加工情報を取り扱う事務を委託しない場合には、「個人情報等」の「等」の記述を削除する）

データ保護及び管理に関する特記仕様書

第1 目的

本契約において取扱う各種データについて、適正なデータ保護・管理方策及び情報システムのセキュリティ方策について明確にすることを目的とする。

第2 適用範囲

本契約を履行するに当たり、出版、報道等により公にされている情報を除き、委託者が交付若しくは使用を許可し、又は契約の相手方（以下「受託者」という。）が作成若しくは出力したものであって用紙に出力されたものを含む全ての情報（以下「電子データ等」という。）を対象とする。

第3 対象とする脅威

本書において対象とする脅威は、次に掲げる情報セキュリティが侵害された又はそのおそれがある場合とする。

- (1) 不正プログラムへの感染（受託者におけるものを含む。）
- (2) サービス不能攻撃によるシステムの停止（受託者におけるものを含む。）
- (3) 情報システムへの不正アクセス（受託者におけるものを含む。）
- (4) 書面又は外部記録媒体の盗難又は紛失（受託者におけるものを含む。）
- (5) 機密情報の漏えい・改ざん（受託者におけるものを含む。）
- (6) 異常処理等、予期せぬ長時間のシステム停止（受託者におけるものを含む。）
- (7) 委託者が受託者に提供した又は受託者にアクセスを認めた委託者の電子データ等の目的外利用又は漏えい
- (8) アクセスを許可していない委託者の電子データ等への受託者によるアクセス
- (9) 意図しない不正な変更等（受託者におけるものを含む。）

第4 本契約を履行する者が遵守すべき事項

受託者は、本契約の履行に関して、以下の項目を遵守すること。

4.1 業務開始前の遵守事項

受託者は、以下の(1)から(6)までの各項目に定める事項及び契約内容を一部再委託する場合は(7)に定める事項を取りまとめた「データ管理計画書」を作成し、業務開始前までに委託者の承認を得ること。

なお、行政手続きにおける特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）による個人番号及び特定個人情報等（以下「特定個人情報等」という。）を取扱う業務の場合は、他の電子データ等と明確に区分して管理することとし、特定個人情報等の適正な取扱いに関するガイドラインに基づく安全管理措置について、「データ管理計画書」の各事項へ、追加で記載すること。

(1) データ取扱者等の指定

受託者は、電子データ等を取扱う者（以下「データ取扱者」という。）及び、データ取扱者を統括する者（以下「データ取扱責任者」という。）を指定し、その所属、役職及び氏名等を記入した「データ取扱者等名簿」を作成すること。

また、特定個人情報等を扱う業務の場合は、特定個人情報等を明確に管理するため、特定個人情報等を取扱う者（以下「特定個人情報等ファイル取扱者」という。）及び特定個人情報等ファイル取扱者を統括する者（以下「特定個人情報等ファイル取扱責任者」という。）についても併せて指定し、「データ取扱者等名簿」に記載すること。

なお、データ取扱者、データ取扱責任者、特定個人情報等ファイル取扱者及び特定個人情報等ファイル取扱責任者（以下「データ取扱者等」という。）

は、守秘義務等のデータの取扱いに関する社内教育、又はこれに準ずる講習等を受講した者とし、その受講実績も併せて「データ取扱者等名簿」に記入すること。

(2) データ取扱者等への教育・周知計画

受託者は、データ取扱者等を対象とした、本契約での電子データ等の取扱いや漏えい防止等の教育及び周知に関する「データ取扱者等への教育・周知計画」を作成すること。

(3) 電子データ等の取扱いにおける情報セキュリティ確保の措置計画

受託者は、本契約に係る電子データ等の取扱いに関し、電子データ等の保存、運搬、複製及び破棄並びに電子データ等の保管場所を変更する場合において実施する措置を記載した「データ取扱計画」を作成すること。「データ取扱計画」には、以下に示す措置を含めること。

ア 本契約の作業に係る電子データ等を取扱うサーバ、パソコン、モバイル端末について、アクセス制御及び脅威に関する最新の情報を踏まえた不正プログラム対策及び脆弱性対策を行うこと。

イ 機密性2以上の電子データ等の取扱いは、委託者又は受託者のいずれかの管理下でない情報システム等（データ取扱者等の個人所有物であるパソコン及びモバイル端末を含む。）を用いることを原則として禁止し、必要がある場合は委託者の許可を得て用いること。

ウ 電子データ等名称、データ取扱者名、授受方法、使用目的、使用場所、保管場所、保管方法、返却方法、授受日時、返却日時、特定個人情報等々の有無等を記録する「データ管理簿」を整備すること。

エ 機密性2以上の電子データ等の保存に、委託者又は受託者のいずれかの管理下でない情報システム等又は電磁的記録媒体（データ取扱者等が私的に契約しているサービス及びデータ取扱者等の個人所有物である電磁的記録媒体を含む。）を用いることを原則として禁止し、必要がある場合は委託者の許可を得て用いること。

オ データ取扱責任者又は特定個人情報等ファイル取扱責任者が、データ取扱者又は特定個人情報等ファイル取扱者の作業に立ち会うなど適切な管理を行うこと。

カ データ取扱責任者又は特定個人情報等ファイル取扱責任者が、データ取扱者又は特定個人情報等ファイル取扱者が作業を終了し作業場所を離れる際は、データの持ち出しの有無を厳重に検査すること。

キ 機密性2以上の電子データ等を電子メールにて送信する場合には、暗号化を行うこと。

(4) 外部設置における情報セキュリティ確保の措置計画

受託者は、委託者が指定する場所以外に情報システム機器を設置（外部設置）し、本契約に係る電子データ等を取扱う場合は、情報セキュリティ確保のために、部外者の侵入等の意図的な情報漏えい等を防止する措置を記載した「外部設置における情報セキュリティ措置計画」を作成すること。「外部設置における情報セキュリティ措置計画」には以下に示す措置を含めること。

ア 情報システムにアクセス（一般向けに提供されているウェブページへのアクセスを除く。）する作業は、受託者の管理下であり、部外者の立入りが制限された場所において行うこと。

イ 電子データ等を取扱うパソコン、モバイル端末等について、盗難、紛失、表示画面ののぞき見等による漏えいを防ぐための措置を講ずること。また、それらの措置を講じていないパソコン、モバイル端末等を用いた作業を制限すること。

ウ 入退室記録、作業記録等を蓄積し、不正の検知、原因特定に有効な管理機能を備えること。

(5) 外部接続における情報セキュリティ確保の措置計画

受託者は、委託者が指定するネットワーク以外のネットワークへ接続（以下「外部接続」という。）し、本契約に係る電子データ等を取扱う場合は、情報セキュリティ確保のために、外部のネットワークからの侵入や改ざんを防御する措置を記載した「外部接続におけるセキュリティ措置計画」を作成すること。「外部接続におけるセキュリティ措置計画」には、以下に示す措置を含めること。

ア 外部接続箇所にファイアウォールを設置し、不要な通信の遮断を行うこと。

イ 外部接続箇所に侵入検知システムを設置し、ネットワークへの不正侵入の遮断を行うこと。

ウ 外部接続箇所で不正な通信を検出した場合、委託者へ通報を行うこと。

(6) 情報セキュリティが侵害された又はそのおそれがある場合における対処手順

受託者は、本契約に係る業務の遂行において情報セキュリティが侵害された又はそのおそれがある場合に備え、事前に連絡体制を整備し、発生した場合の対処手順を記載した「情報セキュリティ侵害時対処手順」を作成すること。

「情報セキュリティ侵害時対処手順」には、以下に示す対処を含めること。

ア 作業中に、情報セキュリティが侵害された又はそのおそれがあると判断した場合には、直ちに、委託者に、口頭にてその旨第一報を入れること。委託者への第一報は、情報セキュリティインシデントの発生を認知してから1時間以内に行うこと。

イ 当該第一報が行われた後、発生した日時、場所、発生した事由、関係するデータ取扱者等を明らかにし、平日の午前9時から午後5時の間は1時間以内に、それ以外の時間帯は3時間以内に委託者に報告すること。また、当該報告の内容を記載した書面を遅延なく委託者に提出すること。

ウ 委託者の指示に基づき、対応措置を実施すること。

エ 委託者が指定する期日までに、発生した事態の具体的内容、原因、実施した対応措置を内容とする報告書を作成の上、委託者に提出すること。

オ 再発を防止するための措置内容を策定し、委託者の承認を得た後、速やかにその措置を実施すること。

(7) 再委託における情報セキュリティの確保の措置計画

受託者は、本契約内容について一部再委託（更に順次行われる再委託を含む。）する場合、受託者が業務を実施する場合に求められる水準と同一水準の情報セキュリティ対策を再委託先において確保させる必要があり、再委託先における情報セキュリティの十分な確保を受託者が担保するとともに、再委託先の情報セキュリティ対策の実施状況を確認するため、「再委託における情報セキュリティ措置計画」を作成すること。なお、特定個人情報等を取扱う業務を再委託したときは、委託者が行う再委託先の管理状況等の確認について、受託者は必要な協力を行うこと。

4.2 業務実施中における遵守事項

(1) 「データ管理計画書」に基づく情報セキュリティ確保

「データ管理計画書」に記載した、データ取扱者等への教育・周知、電子データ等の取扱い及び作業場所等の情報セキュリティ確保のための措置を実施すること。

(2) データ管理簿への記録

受託者は、データ取扱者等が電子データ等を取扱う場合、「データ管理簿」に記録し、データ取扱責任者に確認させること。また、特定個人情報等を扱う業務の場合、特定個人情報等ファイル取扱責任者に併せて確認させること。

(3) 「データ管理計画書」の変更

ア 受託者は、本契約に基づく請負作業中に、次の事項について作業開始前に提出した「データ管理計画書」の内容と異なる措置を実施する場合は、事前に「データ管理計画書」の変更について委託者に提出し、承認を得ること。また、承認された変更の内容を記録し保存すること。

- ・データ取扱者等の異動を行う場合
- ・データ取扱者等に対する教育・周知の計画を変更する場合
- ・電子データ等の取扱いに関する計画又は作業場所等の情報セキュリティ確保のための措置を変更する場合
- ・再委託先及び再委託先の情報セキュリティ対策を変更する場合

イ 一時的に「データ管理計画書」とは異なる措置を実施する場合は、原則として事前にその旨を委託者へ提出し、承認を得ること。ただし、情報セキュリティが侵害された又はそのおそれがある場合など緊急を要する場合等の場合、受託者は、実施内容について事後速やかに委託者へ報告すること。

(4) 業務の報告・監査等

ア 受託者は、委託者へ業務実施中の「データ管理計画書」の遵守状況について定期的に報告すること。

イ 受託者は、委託者が「データ管理計画書」に係る管理状況について監査を要請した時は、定期・不定期にかかわらず、これを受け入れること。

ウ 受託者は、「データ管理計画書」の評価、見直しを行うとともに、必要な改善策等について、委託者へ提案すること。

(5) 情報セキュリティ対策の履行が不十分であった場合の対応

受託者の本契約に係る作業における情報セキュリティ対策の履行が不十分であると委託者が判断した場合、受託者は委託者と協議の上、必要な是正措置を講ずること。

また、是正措置の内容を「データ管理計画書」に反映させること。

4.3 業務完了時の遵守事項

(1) データ返却等処理

受託者は、本契約に基づく業務が完了したときは、「データ管理簿」に記録されている全てのデータについて、返却、消去、廃棄等の措置を行うものとし、処理の方法、日時、場所、立会者、作業責任者等の事項を記した、「データ返却等計画書」を事前に委託者へ提出し、承認を得た上で処理を実施すること。

また、特定個人情報等を扱う業務の場合は、特定個人情報等であることを「データ返却等計画書」に明示すること。

(2) 作業後の報告

受託者は、「データ返却等計画書」に基づく処理が終了したときは、その結果を記載した「データ管理簿」を委託者へ提出すること。

(3) 情報セキュリティ侵害の被害に関する記録類の引渡し

受託者は、本契約の業務遂行中に情報セキュリティが侵害された又はそのおそれがある事象が発生した場合、4.1(6)に基づいて取得し保存している記録類を委託者に引渡すこと。

4.4 記憶装置の修理及び廃棄等におけるデータ消去

受託者は、契約により委託者が利用する情報システム機器の修理及び廃棄、リース返却（以下、「廃棄等」という。）の場合、記憶装置から、全ての電子データ等を消去の上、復元不可能な状態にする措置（以下、「抹消措置」という。）を実施すること。

(1) 抹消措置計画の作成

受託者は、「データ管理計画書」へ作業予定日時、作業予定場所、実施予定

者氏名、データ完全消去区分、使用機材名・数量、データ消去対象記憶装置リスト、立会者などを記載した「抹消措置作業計画」を追加するとともに、必要に応じてその他の措置内容を変更した上、抹消措置実施日（賃貸借契約の場合は賃貸借期間満了日）の30日前までに委託者に提出し、承認を得ること。

また、賃貸借契約の場合は賃貸借期間満了日から30日以内に抹消措置実施日を設定すること。

(2) 抹消措置実施方法

ア マイナンバー利用事務系の領域において住民情報を保存する記憶媒体の抹消措置の方法

(ア) 当該媒体を分解・粉砕・溶解・焼却・細断などによって物理的に破壊し、確実に復元を不可能とすること。なお、対象となる機器について、リース契約による場合においても、リース契約終了後、当該機器の記憶媒体については、物理的に破壊を行うこと。

(イ) 職員が抹消措置の完了まで立ち会いによる確認を行う。ただし、庁舎外で抹消措置を行う場合は、庁舎内において、一般的に入手可能な復元ツールの利用によっても情報の復元が困難な状態までデータの消去を行い、職員が作業完了を確認した上で、委託事業者等に引渡しを行い、委託事業者等が物理的な破壊を実施し、当該破壊の証拠写真が添付された完了証明書により確認できること。

イ 機密性2以上に該当する情報を保存する記憶媒体（上記アに該当するものを除く。）の抹消措置の方法

(ア) 一般的に入手可能な復元ツールの利用を超えた、いわゆる研究所レベルの攻撃からも耐えられるレベルで抹消を行うこと。

(イ) 庁舎内において、一般的に入手可能な復元ツールの利用によっても情報の復元が困難な状態までデータの消去を行い、職員が作業完了を確認した上で、委託事業者等に引渡しを行い、抹消措置の完了証明書により確認できること。

ウ 機密性1に該当する情報を保存する記憶媒体の抹消措置の方法

(ア) 一般的に入手可能な復元ツールの利用によっても情報の復元が困難な状態に消去すること。

(イ) 庁舎内においてデータの消去を実施し、職員が作業完了を確認するなど適正な方法により確認できること。

エ IoT機器を含む特殊用途機器の抹消措置の方法

(ア) デジタル複合機などのIoT機器を含む特殊用途機器に保存された電子データ等の漏えいの対策について、国際標準に基づくセキュリティ要件と同等以上のセキュリティ要件とその要件に適合した第三者認証（「IT製品の調達におけるセキュリティ要件リスト」適合製品など）を取得している機能を有する場合は、当該機能によるデータ消去をもって抹消措置とすることができる。

(イ) 庁舎内においてデータの消去を実施し、職員が作業完了を確認するなど適正な方法により確認できること。

(3) 抹消措置の報告

受託者は、抹消措置実施日から30日以内に、作業日時、実施者氏名、データ完全消去区分、使用機材名・数量、データ消去対象記憶装置リスト、立会者及び全ての記憶装置について抹消措置前後の写真を添付した「抹消措置完了報告書」を委託者へ提出し、承認を得ること。

第5 情報システムの情報セキュリティ要件

受託者は、本契約により情報システムを導入する場合は、対象となる以下の項目

を遵守すること。

5.1 侵害対策

(1) 通信回線対策

ア 通信経路の分離

不正の防止及び発生時の影響範囲を限定するため、外部との通信を行うサーバ装置及び通信回線装置のネットワークと、内部のサーバ装置、端末等のネットワークを通信回線上で分離するとともに、業務目的、所属部局等の情報の管理体制に応じて内部のネットワークを通信回線上で分離すること。

イ 不正通信の遮断

通信回線を介した不正を防止するため、不正アクセス及び許可されていない通信プロトコルを通信回線上にて遮断する機能を備えること。

ウ 通信のなりすまし防止

情報システムのなりすましを防止するために、サーバの正当性を確認できる機能を備えるとともに、許可されていない端末、サーバ装置、通信回線装置等の接続を防止する機能を備えること。

エ サービス不能化の防止

サービスの継続性を確保するため、情報システムの負荷がしきい値を超えた場合に、通信遮断や処理量の抑制等によってサービス停止の脅威を軽減する機能を備えること。

(2) 不正プログラム対策

ア 不正プログラムの感染防止

不正プログラム（ウイルス、ワーム、ボット等）による脅威に備えるため、想定される不正プログラムの感染経路の全てにおいて感染を防止する機能を備えるとともに、新たに発見される不正プログラムに対応するために機能の更新が可能であること。

イ 不正プログラム対策の管理

システム全体として不正プログラムの感染防止機能を確実に動作させるため、当該機能の動作状況及び更新状況を一元管理する機能を備えること。

(3) 脆弱性対策

ア 構築時の脆弱性対策

情報システムを構成するソフトウェア及びハードウェアの脆弱性を悪用した不正を防止するため、開発時及び構築時に脆弱性の有無を確認の上、運用上対処が必要な脆弱性は修正の上で納入すること。

イ 運用時の脆弱性対策

運用開始後、新たに発見される脆弱性を悪用した不正を防止するため、情報システムを構成するソフトウェア及びハードウェアの更新を効率的に実施する機能を備えるとともに、情報システム全体の更新漏れを防止する機能を備えること。

5.2 不正監視・追跡

(1) ログ管理

ア ログの蓄積・管理

情報システムに対する不正行為の検知、発生原因の特定に用いるために、情報システムの利用記録、例外的事象の発生に関するログを蓄積し、委託者が指定する期間保管するとともに、不正の検知、原因特定に有効な管理機能（ログの検索機能、ログの蓄積不能時の対処機能等）を備えること。

イ ログの保護

ログの不正な改ざんや削除を防止するため、ログに対するアクセス制御機能及び消去や改ざんの事実を検出する機能を備えるとともに、ログのアーカイブデータの保護（消失及び破壊や改ざんの脅威の軽減）のための措置を含む設計とすること。

ウ 時刻の正確性確保

情報セキュリティインシデント発生時の原因追及や不正行為の追跡において、ログの分析等を容易にするため、システム内の機器を正確な時刻に同期する機能を備えること。

(2) 不正監視

ア 侵入検知

不正行為に迅速に対処するため、情報システムで送受信される通信内容の監視及びサーバ装置のセキュリティ状態の監視等によって、不正アクセスや不正侵入を検知及び通知する機能を備えること。

イ サービス不能化の検知

サービスの継続性を確保するため、大量のアクセスや機器の異常による、サーバ装置、通信回線装置又は通信回線の過負荷状態を検知する機能を備えること。

5.3 アクセス・利用制限

(1) 主体認証

情報システムによるサービスを許可された者のみに提供するため、情報システムにアクセスする主体の認証を行う機能として、ID／パスワードの方式を採用し、主体認証情報の推測や盗難等のリスクの軽減を行う機能として、パスワードの複雑性及び指定回数以上の認証失敗時のアクセス拒否などの条件を満たすこと。

(2) アカウント管理

ア ライフサイクル管理

主体のアクセス権を適切に管理するため、主体が用いるアカウント（識別コード、主体認証情報、権限等）を管理（登録、更新、停止、削除等）するための機能を備えること。

イ アクセス権管理

情報システムの利用範囲を利用者の職務に応じて制限するため、情報システムのアクセス権を職務に応じて制御する機能を備えるとともに、アクセス権の割り当てを適切に設計すること。

ウ 管理者権限の保護

特権を有する管理者による不正を防止するため、管理者権限を制御する機能を備えること。

5.4 機密性・完全性の確保

(1) 通信経路上の盗聴防止

通信回線に対する盗聴行為や利用者の不注意による情報の漏えいを防止するため、通信内容を暗号化する機能を備えること。

(2) 保存情報の機密性確保

情報システムに蓄積された情報の窃取や漏えいを防止するため、情報へのアクセスを制限できる機能を備えること。また、保護すべき情報を利用者が直接アクセス可能な機器に保存できないようにすることに加えて、保存された情報を暗号化する機能を備えること。

(3) 保存情報の完全性確保

情報の改ざんや意図しない消去等のリスクを軽減するため、情報の改ざんを検知する機能又は改ざんされていないことを証明する機能を備えること。

5.5 情報窃取・侵入対策

(1) 情報の物理的保護

情報の漏えいを防止するため、記憶装置のパスワードロック、暗号化等によって、物理的な手段による情報窃取行為を防止・検知するための機能を備える

こと。

(2) 侵入の物理的対策

物理的な手段によるセキュリティ侵害に対抗するため、情報システムの構成装置（重要情報を扱う装置）については、外部からの侵入対策が講じられた場所に設置すること。

5.6 障害対策（事業継続対応）

(1) システムの構成管理

情報セキュリティインシデントの発生要因を減らすとともに、情報セキュリティインシデントの発生時には迅速に対処するため、構築時の情報システムの構成（ハードウェア、ソフトウェア及びサービス構成に関する詳細情報）が記載された文書を提出するとともに文書どおりの構成とし、加えて情報システムに関する運用開始後の最新の構成情報及び稼働状況の管理を行う方法又は機能を備えること。

(2) システムの可用性確保

サービスの継続性を確保するため、情報システムの各業務の異常停止時間が復旧目標時間として 1 日を超えることのない運用を可能とし、障害時には迅速な復旧を行う方法又は機能を備えること。

5.7 サプライチェーン・リスク対策

(1) 受託者（再委託先含む）において不正プログラム等が組み込まれることへの対策

情報システムの構築において、委託者が意図しない変更や機密情報の窃取等が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。当該品質保証体制を証明する書類（例えば、品質保証体制の責任者や各担当者がアクセス可能な範囲等を示した管理体制図）を提出すること。

(2) 調達する機器等に不正プログラム等が組み込まれることへの対策

機器等の製造工程において、委託者が意図しない変更が加えられないよう適切な措置がとられており、当該措置を継続的に実施していること。また、当該措置の実施状況を証明する資料を提出すること。

5.8 利用者保護

(1) 情報セキュリティ水準低下の防止

情報システムの利用者の情報セキュリティ水準を低下させないように配慮した上でアプリケーションプログラムやウェブコンテンツ等を提供すること。

(2) プライバシー保護

情報システムにアクセスする利用者のアクセス履歴、入力情報等を当該利用者が意図しない形で第三者に送信されないようにすること。

電気取扱い作業マニュアル

1 目的

浄水場、給水地点、事務所等の施設に係わる電気設備の設置、点検、修理、撤去等の電気工事の計画、作業を行う場合における作業の安全を図るため、千葉県企業局自家用電気工作物保安規程第14条第4項の規定により、本マニュアルを定めるものとする。

2 作業計画及び準備

- (1) 作業は停電をして行うことを原則とする。やむをえず全停電が困難な場合で、停電範囲が限られる場合には、充分なる安全対策を施すものとする。
- (2) 同一室内において、作業が、重複しないよう、予め工程を調整する。
- (3) 「作業手順書」を作成し、所属長及び主任者の承認を得るものとする。

作業手順書内容

ア 作業の目的

イ 作業責任者及び体制

ウ 作業の内容、作業時刻、作業場所、作業者等

エ 停電時刻及び停電範囲を示す図面等

- (4) 作業の実施に先立ち、工事箇所又は配電盤等への電源ケーブルにつき、現地調査を行い図面と現物が一致することを確認する。

調査したケーブルにはペイントによる識別、若しくは表示札を取付け、確実に判別できるようにする。

例 撤去ケーブル・・・黄色

3 作業前打合せ

工事实施の当日、管理室の操作職員（浄水場、給水地点等の施設に関わる作業を行う場合）、業務監督職員、受託者による合同打合せを行い、業務の安全に努める。

打合せ内容

- (1) 業務の目的
- (2) 業務の内容
- (3) 当日の工程
- (4) 相互の連絡体制及び指揮命令系統

なお、打合せ記録を書面にて作成する。

4 作業

- (1) 作業に先立ち、安全区画ネット、赤テープ等により危険区域を表示する。
- (2) 電源側開閉器を開路し、開路した開閉器は施錠し、断路位置にし、若しくは「通電禁止（操作禁止）」の表示を取付け又は監視人を置く。
- (3) 開路した電路の残留電荷を安全な方法で確実に放電させる。
- (4) 開路した電路が高圧であったものについては、検電後、短絡接地器具を用いて確実に短絡接地する。
- (5) 作業に当たっては、必要な保護具を着用し、必要な防具を装着する。
- (6) ケーブルを撤去・切断等する場合には、前項までの安全処置を確認した後、

ケーブルに、「作業許可」の表示を取付ける。

5 復電作業及び復電以後の操作

- (1) 作業終了し、開路した電路に通電しようとするときは、作業者の安全及び短絡接地器具を取外したことを確認した後、これを行う。
- (2) 復電作業中に同一室内においては他の作業を行わない。
- (3) 重故障により遮断器がトリップした場合にはその機器の操作スイッチに、「操作禁止」の銘板を取付けたマグネット式のスイッチガード等を取付ける。
スイッチガードの取外しは現場確認を行った後、浄水場、給水地点等にあつては主任者等がこれを行い、事務所等にあつては所属職員がこれを行うこととする。
これにより現場確認の徹底と誤認の防止を図る。

6 設計時の配慮等

- (1) 配線や機器の設置について単純にする。
コンデンサについては、母線一括として設置する方法、若しくはポンプと同一盤内又は専用盤とする。
- (2) 同一盤内に異系統の電源が混在する場合は取扱注意の旨の表示を取付ける。
- (3) 増設、改造工事完了後は、工事箇所のみならず全体図等の関連図面の整備を行い常に最新の状態の図面を備えつけ、関係職員に対し教育を行う。

7 備考

- (1) 電気工作物の工事、維持及び運用に当たっては、本マニュアルの内容を遵守すること。
- (2) 電気工作物の「施工計画書」、「作業手順書」の作成においても同様とする。
- (3) 本マニュアルの内容を点検業務委託に準用する。