案件番号:120126004

令和８年度

CONPAS 保守･運用業務

特 記 仕 様 書

令和８年１月

国土交通省　関東地方整備局

1．業務概要

本業務は、国土交通省関東地方整備局において構築した CONPAS[※1] を保守・運用するものである。

2．履行期間

令和8年4月1日から令和9年3月31日までとする。

3．業務内容

業務名称	業務内容	数量	摘要
計画・準備			
	計画・準備	1 式	
業務打合せ			
	事前協議	1 回	
	最終報告	1 回	
保守・運用			
	システム運用・監視	1 式	
	データセンター保守	1 式	
	ソフトウェア保守	1 式	
	ハードウェア保守	1 式	
	データ取得・整理	1 式	
成果物			
	業務完成図書	1 式	

4．提供資料及び貸与物件

4－1　提供資料

令和7年度　CONPAS 保守・運用業務　報告書

4－2　貸与物件

品　　名	規　　格	単位	数量
ｼｽﾃﾑ（ﾌﾟﾛｸﾞﾗﾑ）	ｼｽﾃﾑ（ﾌﾟﾛｸﾞﾗﾑ）	式	1
ﾃﾞｰﾀｾﾝｻ側ｻｰﾊﾞｰ機器	VPN ﾙｰﾀｰ	式	1
ﾀｰﾐﾅﾙ側ｻｰﾊﾞｰ機器	無停電電源装置、ﾃﾞｰﾀ交換用 NAS、ﾌｧｲﾔｳｫｰﾙ、VPN ﾙｰﾀｰ、ﾚｲﾔ２ｽｲｯﾁ	式	1

5．業務仕様

5－1　総則

機器の保守及びシステムの運用にあたっては「デジタル・ガバメント推進標準ガイドライン」（令和 7 年 5 月 27 日第 19 回デジタル社会推進会議幹事会決定）に定める規定を参考にするものとする。その他、本特記仕様書に定めのない事項については、「港湾設計・測量・調査等業務共通仕様書」（国土交通省港湾局　令和 7 年 4 月）の定めによるものとする。

[※1] CONPAS：関東地方整備局がコンテナターミナルゲートにおけるコンテナ搬出入手続の効率化を目的に設計・構築した港湾情報システム（特許取得）

５－２ 計画・準備

業務を行うにあたって、事前に業務内容を把握し、業務の手順及び遂行に必要な事項を整理し、業務実施計画書を作成する。なお、計画書の中には、運用体制、スケジュール、作業内容を必ず記載するものとする。

５－３ 業務打合せ

本業務の履行にあたっては、調査職員と十分な打合せを行うものとし、事前協議 1 回、最終報告 1 回の計 2 回行うものとする。

なお、中間報告は未計上としているが、変更が生じる場合は調査職員と協議の上、決定することとし、これに係る変更契約は履行期限の末日までに行うものとする。

５－４ 保守・運用

（機能概要）

国土交通省関東地方整備局が構築した CONPAS を安定的に稼働させ、かつ、システム障害時に迅速に対応するための保守・運用を行う。なお、調査職員、利用者からのシステム操作に関する問い合わせへの対応も本業務に含まれる。

本業務の対象となるシステムは、関東地方整備局が保有する CONPAS システム(データセンター1式、データ連携用の中立 LAN 一式 （コンテナターミナル事業者等のターミナルオペレーションシステムは除く））、及び Colins※2 とのデータ通信環境である。

① Colins 連携

実入りコンテナ搬出について、TOS から Colins に登録された情報を CONPAS に取り込む。登録された情報は、陸運事業者からの WEB 登録内容の誤りチェックに利用する。

② 港湾情報 WEB

CY 業務：事前登録時間枠、事前登録可能本数を登録する。

陸運業務：事前登録枠の範囲内で、予約情報を登録する。

なお、運転手名、車両 No は後追いでの追加入力を可能とする。

予約情報は該当 CY の中継サーバへ送信する。

③ PS カード連携

ゲートでの PS カード読み取りのタイミングで出入管理情報システムより PS カード情報を取得する。搬出入作業が予約された運転手（PS カード ID）を検知した場合、該当 CY のゲートシステムへ PS カード読取情報（予約情報を含む）を送信する。

（運用体制等）

運用体制

受注者は、以下の体制で運用を行うものとする。

・保守連絡窓口の受付時間は、原則平日 9:00-17:00 とする。

・平日 9:00-17:00 以外においても、対象コンテナターミナルの搬出入ゲートが運用されている間は連絡可能な体制とすること。

・運用体制については、事前に調査職員に書面にて通知し、承認を受けること。

・運用体制を変更しようとする場合は、事前に調査職員に変更内容を記載した書面をもって通知し、承認を受けること。

※2 国土交通省港湾局が港湾利用者にリアルタイムなコンテナ物流情報を一元化して提供している WEB サイト

運用期間、対象ターミナル及び対象者

運用期間　　　　:令和 8 年 4 月から令和 9 年 3 月までを想定している。

対象ターミナル :横浜港南本牧ふ頭コンテナターミナル
東京港大井ふ頭1・2号コンテナターミナル
東京港大井ふ頭3・4号コンテナターミナル
コンテナターミナル①
コンテナターミナル②

対象者　　　　　:陸運事業者、ターミナル事業者

なお、対象とするコンテナターミナル①、②は想定としているため、費用に関しては未計上としている。運用期間、対象ターミナル等に変更が生じる場合は調査職員と協議の上、決定することとし、これに係る変更契約は履行期限の末日までに行うものとする。

(1)システム運用・監視

① 運用スケジュール・サービス時間帯

受注者は、対象コンテナターミナルの搬出・搬入ゲートが運用されている期間は、CONPAS を継続的に稼働できるように、必要なシステム操作及び監視を行うこと。

② 手動操作

受注者は、CONPAS のサーバ障害時に、リモートからプロセスの再起動、OS の再起動等のコマンド操作を行えるようにすること。また、サーバのスイッチのオン／オフの操作がリモートで行える、又は、手動でのサーバのスイッチのオン／オフが、依頼により即時に実行できる体制とすること。さらに、仮想環境によりサーバ機能を提供する場合はデータセンターへの連絡によりサーバの OS 稼働の復旧が可能とすること。

③ 運用管理ツール

受注者は、データセンターの機能もしくは受注者の用意する監視ソフトウェア等で障害の検知を行うことを可能とし、障害を検知した場合は、メール等にて即時に障害検知の連絡を受けられるようにすること。

④ システム・ネットワーク監視

受注者は、CONPAS の稼動に関する障害の検知を行うこと。
なお、監視対象は、ネットワーク障害、トラフィックの輻輳、HTTP サーバ、FTP サーバ、メールサーバ等のサイトの稼動に必須のプロセス、サーバのハードウェア障害とすること。

⑤ 障害の一次切り分け

受注者は、障害発生の連絡を受けてから、速やかに復旧対応のための障害箇所の一次切り分け作業を開始すること。また、受注者は、障害の一次切り分け後、原因に応じて、障害の復旧作業に着手もしくは、回線・稼働環境提供者への復旧指示を行うこと。

なお、障害の復旧にあたっては、(2)、(3)、(4)の復旧条件に従うこと。

⑥ 障害対応

障害の復旧に当たっては、調査職員と連携すること。障害の発生に際しては、調査職員に対して、障害の原因・内容・復旧状況について速やかに報告を行うこと。また、受注者が障害を確認した後、受注者は、直ちに対応状況の報告を調査職員に電話とメールにて連絡すること。

⑦ 運用業務

受注者は、CONPAS の運用に関する以下の作業を実施すること。

・ターミナルの受付時間枠、受付本数の登録

・利用者からのシステム操作に関する問い合わせへの対応

⑧ 運用状況報告

受注者は、毎月運用状況について調査職員に報告を行うこと。

⑨ ターミナルオペレーションシステムからのデータ受信

受注者は、接続するターミナルオペレーションシステムからのデータ受信状況を確認し、不具合を認めた場合は速やかに調査職員に報告するとともに、原因を調査すること。不具合が CONPAS 又は中立 LAN 側で対応可能な原因による場合は、受注者が復旧を行うこと。ただし、原因がハードウェアにあると判断される場合には、受注者が復旧の計画を立てること。また、ターミナルオペレーションシステム側での対応が必要と判断される場合は、ターミナルオペレーションシステムの管理者と連携して、受注者が復旧の計画を立てること。

⑩ Colins からのデータ受信

受注者は、接続する Colins からのデータ受信状況を確認し、不具合を認めた場合は速やかに調査職員に報告するとともに、原因を調査すること。不具合が CONPAS で対応可能な原因による場合は、受注者が復旧を行うこと。また、Colins 側での対応が必要と判断される場合は、Colins の管理者と連携して、受注者が復旧の計画を立てること。

（2）データセンター保守

① 稼働時間帯

24 時間稼働できるデータセンターを利用すること。

② 運用体制

受注者は、ネットワーク障害に対して速やかな復旧体制を確保すること。なお、ネットワーク障害時には速やかに障害発生の検知を行い、受注者が障害発生を速やかに把握することができるような体制であること。また、常時センター内で有人の監視が行える体制を整えているデータセンターを利用すること。（リブートやインジケーター確認、手動による。）

（3）ソフトウェア保守

① 保守対応時間帯

受注者は、ソフトウェア障害を 24 時間検知できる体制とすること。障害を検知した場合には、直ちに復旧作業に着手できるようにすること。

② 保守担当者の復旧許容時間

受注者は、ソフトウェアの障害を検知した場合は、直ちに復旧を行う体制を確保すること。

③ ソフトウェア保守の対応方法

受注者が保守担当者による対応可能な環境を提供し、遠隔保守での対応を想定して

いる。

④ オペレーティングシステム（OS）及びミドルウェア等のパッチ適用

受注者は、OS 及びミドルウェアでセキュリティの観点でのバージョンアップ等が行われた場合には、適用の影響を検討・確認の上、速やかに適用を行うこと。

アプリケーションに影響があった場合は、適用の是非を調査職員と協議の上で決定すること。

⑤ 定期保守

受注者は、毎月定期保守を実施すること。定期保守を実施した際は、速やかに調査職員に点検結果の報告を行うこと。

（4）ハードウェア保守

① 対象ハードウェア（詳細は別紙 1、別紙 2 を参照すること）

CONPAS を司る WEB サーバ、TOS 連携用サーバ、管理サーバ、DB サーバ、中継サーバ（ターミナル毎）、データ交換用 NAS サーバ、バックアップデータ保存用機器等を対象とする。

② 保守体制の確保

受注者は、ハードウェアの障害を検知した場合は、直ちに復旧を行う体制を確保すること。

③ 保守担当者の復旧許容時間

受注者は、ハードウェア障害を検知した場合は、概ね 3 日以内（土日・祝日を除く）に復旧を行うものとし、これによらない場合は調査職員と協議するものとする。また、ハードウェアの交換・修理の必要が生じた場合は、調査職員と協議の上で決定すること。

④ 定期保守

受注者は、毎月定期保守を実施すること。定期保守を実施した際は、速やかに調査職員に点検結果の報告を行うこと。

（5）データ取得・整理

CONPAS の運用に伴い得られたデータの取得・整理を行うこと。また、取得するデータ及び整理方法については、事前に調査職員に報告し、承諾を得ること。

6．成果物

業務の成果物は、実施した保守・運用の内容を業務完成図書として取りまとめ、以下に基づき提出するものとする。

（1）電子納品とは、特記仕様書、図面、業務計画書、報告書、写真、取得データ等全ての最終成果（以下「業務完成図書」という。）を「土木設計業務等の電子納品要領」（R06.03）（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電子データで作成し納品するものである。なお、電子化の対象書類及び書面における署名又は押印の取り扱いについては、調査職員と協議のうえ決定する。また、電子納品の運用にあたっては、「地方整備局（港湾空港関係）の事業における電子納品運用ガイドライン【業務編】」(R07.03)を参考にする。

（2）「業務完成図書」は、「要領」に基づいて作成した電子データを電子媒体（CD－R又はDVD－R）で2部提出するものとする。なお、「要領」に記載がない項目の電子化については、調査職員と協議のうえ決定する。

（3）「紙」による報告書は製本１部とする。なお、報告書製本の体裁は黒表紙金文字製本のA4 判とし、図面は縮小A3判折り込みを標準とする。

（4）図面は「CAD製図基準」（平成 29 年 3 月）に基づいて作成しなければならない。
また、図面作成の運用にあたっては、「地方整備局（港湾空港関係）の事業における電子納品運用ガイドライン【資料編】」を参考とする。

（5）納入場所
横浜市中区北仲通５－５７　横浜第二合同庁舎１４階
国土交通省　関東地方整備局　港湾空港部　クルーズ振興・港湾物流企画室

７．守秘義務

業務の実施過程で知った一切の情報を第三者に漏洩しないこと。本特記仕様書に基づく全ての作業において、発注者が提供した業務上の情報を第三者に開示し、又は漏洩しないこと。また、そのために必要な措置を講ずること。

発注者が提供する資料は、原則として貸し出しによるものとし、履行期限までに返却すること。また、当該資料の複写及び第三者への提供はしないこと。

やむを得ず第三者に開示することが必要である場合は、事前に調査職員と協議のうえ、承認を得ること。本調達に従事する者は原則として受注者の社員であることとし、社員以外の者が従事する場合は、身元を保証するとともに、身元を明らかにする書面を発注者に提出し、承認を受けること。

８．検査

本特記仕様書のとおり実施されたことの確認をもって検査とする。

９．情報セキュリティに関する事項

以下に示す情報セキュリティ対策の実施にあたっては、事前に調査職員と協議を行うものとする。本事項は「国土交通省情報セキュリティポリシー」に基づいたものであるが、「政府機関等の情報セキュリティ対策のための統一基準群」に準拠しているため、必要に応じて参照するものとする。なお、「国土交通省情報セキュリティポリシー」は非公開資料のため、閲覧場所は当局内に限定し、その内容を秘密にしなければならない。閲覧を希望する場合には、契約締結後、受注者が調査職員に守秘義務の誓約書を提出する。

（1） 一般的事項

【情報の取扱】

1）業務の実施過程で知った一切の情報を第三者に漏洩しないこと。本特記仕様書に基づく全ての作業において、発注者が提供した業務上の情報を第三者に開示し、又は漏洩しないこと。また、そのために必要な措置を講ずること。

2）発注者が提供する資料は、原則として貸し出しによるものとし、履行期間までに返却すること。また、当該資料の複写及び第三者への提供はしないこと。

やむを得ず第三者に開示することが必要である場合は、事前に調査職員と協議のうえ、承認を得ること。

3）本業務に従事する者は原則として受注者の社員であることとし、社員以外の者が従事する場合は、身元を保証するとともに、身元を明らかにする書面を調査職員に提出し、承認を受けるものとする。
4）本業務に従事するすべての者と個別に退職後も有効な守秘義務契約を締結していること。
5）電磁的記録媒体を廃棄する場合は、情報が保存された媒体の種類（紙媒体、磁気媒体、フラッシュメモリ等）や動作可否などの状況を考慮した上で、全ての情報を復元できないように抹消すること。

【情報の管理体制】

本業務を行う事業者は、当該業務の実施において情報セキュリティを確保するための体制を整備する。

・情報へアクセスする主体の識別とアクセスの制御について、「政府機関等の情報セキュリティ対策のための統一基準群」を参照して実施することとする。
・受注者は、当該業務の実施において意図せざる変更が加えられないための管理体制を整備する。
・受注者は、資本関係・役員の情報、本業務の実施場所、本業務従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報を提示すること。
・本業務の運用に係る要員を限定すること。また、全ての要員の所属、専門性（資格等）、実績及び国籍について掲示すること。本業務の実施期間中に要員を変更する場合は、事前に調査職員へ連絡し、確認を得ること。
・運用に係る者の所属（契約社員、派遣社員等の雇用形態は問わず、本業務に従事する全ての要員）、実績（経験年数、資格等）及び国籍について、調査職員にあらかじめ提出し、確認を得ること。
・再委託を行う場合、受注者は、再委託先の資本関係・役員等の情報、業務の実施場所、作業要員の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績・国籍等に関する情報の提供を行うとともに、再委託した事業に対して意図せざる変更が加えられないための十分な管理体制がとられることを調査職員に報告し、確認を得ること。

【セキュリティ対策の実施体制】

1）本業務に係る情報システムにおいて以下のセキュリティ機能を具体化し、実装する。
（ア）本業務に係る情報システムへのアクセスを業務上必要な者に限るための機能
（イ）本業務に係る情報システムに対する不正アクセス、ウイルス・不正プログラム感染等、インターネットを経由する攻撃、不正等への対策機能
（ウ）本業務に係る情報システムにおけるセキュリティ事故及び不正の原因を事後に追跡するための機能
2）本業務に係る情報システムの構築における以下の脆弱性対策を提案する。
（ア）構築する情報システムを構成する機器及びソフトウェアの中で、脆弱性対策を実施するものを適切に決定すること。
（イ）脆弱性対策を行うとした機器及びソフトウェアについて、公表されている脆弱性情報及び公表される脆弱性情報を把握すること。
（ウ）把握した脆弱性情報について、対処の要否、可否を判断すること。対処したものに関して対処方法、対処しなかったものに関してその理由、代替措置及び影響を納品時に調査職員に報告すること。
3）本業務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又はそのおそれがある

場合には、速やかに調査職員に報告する。これに該当する場合には、以下の事象を含む。
（ア）受注者に提供し、又は受注者によるアクセスを認める国土交通省の情報の外部への漏えい及び目的外利用
（イ）受注者の者による国土交通省のその他の情報へのアクセス
4）下表に示す項目について、月次及び年次で報告書を作成すること。なお、サービスレベルが目標に満たない場合はその要因分析を行うとともに、達成状況の改善に向けた対策を提案すること。

表　月次報告・年次報告項目一覧

項　目	月次報告	年次報告
実施した作業概要・状況	○	
サービスレベルの達成状況	○	○
定期点検の実施状況	○	○
システムリソースの消費状況で特筆すべき事項	○	
インシデント一覧	○	○
問い合わせ及び対応状況と特筆すべき問い合わせ及び対応記録	○	
対応すべき課題及びリスクの一覧とその対応状況	○	○
業務における情報セキュリティ対策の実施状況	○	
運用、保守の改善提案（ある場合）	○	○
職員が指示する事項	○	○

5）運用・保守対象機器について、メーカーの情報公開等により、OS 等ソフトウエアのセキュリティホール、バグ等の情報を得た場合には、速やかに調査職員に伝達すること。また、運用・保守対象機器に監視、ハードウェアメーカーソフトウェアメーカー等からバージョンアップ情報、サポート切れ情報、製品に関する不具合方法等、運用・保守対象機器に対して有益と判断できる技術情報については、その情報の公開後、速やかに調査職員に報告すること。
6）本業務の遂行において、受注者における情報セキュリティ対策の履行が不十分である可能性を発注者が認める場合には、管理技術者は、調査職員の求めに応じこれと協議を行い、合意した対応を採る。

【インシデント対応】
1）コンピュータウイルスの感染や、不正アクセス等のセキュリティイベントを検知した場合、速やかに調査職員に報告すること。
2）本システムにおいて、セキュリティ上の問題発生時、調査職員が「緊急」と判断する事態の場合は、通常業務時間後も継続して対応を求めることがある。
3）業務遂行における情報セキュリティ対策の履行状況について、調査職員が本特記仕様書において求める情報セキュリティ対策の実績の報告を求めた場合には、速やかに報告書を書面にて提出すること。
4）保守業務として障害及びインシデント発生時の復旧作業並びに障害及びインシデント発生を予防する目的で行う非定型業務全般を行うこと。なお、いずれも実施に当たっては

その妥当性を確認すること。ただし、受注者の責によらない大規模インシデントにより、通常業務の想定を大幅に上回る事象が発生した場合には、調査職員と協議すること。

【セキュリティリスクへの対応】

1）本システムが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログを取得すること。

2）本システムに含まれる構成要素（サーバー機器、ネットワーク機器等）のうち、時刻設定が可能なものについては、システムにおいて基準となる時刻に当該構成要素の時刻を同期させ、ログに時刻情報も記録されるよう設定すること。

3）本システムで取得するログについて、「政府機関等の情報セキュリティ対策のための統一基準群」を参考にログを取得する情報項目を定め管理すること。なお、情報の取得が難しい場合には調査職員と協議し除外とすること。

4）本システムで取得するログの保存期間について、調査職員と合意すること。

5）取得したログに対する不正な消去、改ざん及びアクセスを防止するため、適切なアクセス生後を含む、ログ情報の保全方法を定め、調査職員と合意すること。

6）ログが取得できなくなった場合の対処方法を定め、調査職員と合意すること。

7）機器等の盗難及び不正な持ち出しを防止するため、対策を講ずること。

8）本業務において、守るべき情報資産（打合せ資料、設計書及び設定値等）を示した上で、これらの情報資産に対する不正アクセス、滅失及びき損等に対処するため実施する対策（例：ネットワークの分離、ウイルス対策等）を提示すること。

9）本業務で取り扱う情報及び当該情報を取り扱うシステムの完全性の保護にあたり、下記の完全性の要件を満たすこととする。

（ア）機器の故障に起因するデータの滅失や改変を防止する対策を講ずること。

（イ）理結果を検証可能とするため、ログ等の証跡を残すこと。

（ウ）保管するログ情報は滅失しないように対策すること。

（エ）保管するログ情報は暗号化すること。これによらない場合は、データへのアクセス制御等により完全性を担保すること。

（2） 情報システム構築、運用・保守に係る事項

【通信回線対策】

・通信プロトコル及びポートの利用を必要最低限に制限するとともに、不正アクセス及び許可されていない通信を検知・遮断する機能を備えること。

・サーバの正当性を検証できる機能を備えること。

・サービス不能攻撃の影響を排除又は低減するための対策装置やサービスの導入等、サービス停止の脅威を軽減する対策を行うこと。

【不正プログラム対策】

・感染や感染拡大を防止する機能を備えるとともに、既知及び未知の不正プログラムの検知及びその実行の防止の機能を有するソフトウェアを導入すること。

・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、当該機能の導入状況及び更新状況を把握すること。

【不正監視】

サービス不能攻撃を受け、サーバ装置、通信回線装置又は通信回線が過負荷状態に陥り利用できない場合を想定し、攻撃への対処を効率的に実施可能な以下を例とする手段及び連絡体制の確保について検討すること。

（ア） サービス不能攻撃を受けているサーバ装置、通信回線装置及びそれらを保護するための装置を操作できる手段を確保する
（イ） 災害情報等の緊急性が高く、国民の生命や財産に著しく影響を及ぼし得るような重要情報については、サービス不能攻撃を受けた際にも発信を可能とする

【アクセス制限・利用制限】
アクセス権限の管理のため、以下のとおり設定すること。
1）本システムに権限管理機能を導入するにあたり、管理者権限の特権を持つ主体の識別コード及び主体認証情報が悪意ある第三者によって、不正に窃取された際の被害を最小化するための措置及び内部からの不正操作や誤操作を防止するための措置として、以下のいずれかの措置を講ずること。
（ア）業務上必要な主体のみに限定する。
（イ）必要最小限の権限のみ付与する。
（ウ）デュアルロック機能を導入する。
（エ）管理権限を行使できる端末をシステム管理者等の専用端末とする。
2）管理者権限を持つ識別コードを付与する場合は以下の措置を講ずること。
（ア）業務上必要な場合に限定する。
（イ）初期設定の識別コードを変更できる場合には、識別コードを初期設定以外のものに変更する。
（ウ）初期設定の主体認証情報を変更できる場合には、主体認証情報を初期設定以外のものに変更する。
（エ）ネットワーク経由のログインを制限する。
（オ）管理者権限を有する識別コードの利用は権限を必要とする業務に限定し、一般の業務として使用させない。
3）識別コードの付与にあたり、以下のいずれかの措置を講ずること。
（ア）本システムを利用する主体ごとに個別に付与する。ただし、やむを得ず、複数の主体で共用する識別コードを付与する必要がある場合には、利用者を特定できる仕組みを設けた上で、発注者の合意を得ること。
（イ）識別コードの付与に関する記録及び当該記録を消去する場合の情報セキュリティ責任者からの事前の許可
（ウ）ある主体に付与した識別コードを別の主体に対して付与することの禁止

【物理対策】
1） 情報の漏えいを防止するため、施錠可能なサーバラック等により物理的な対策を講じること。
2） 物理的な手段によるセキュリティ侵害に対抗するため、重要情報を扱う情報システムの構成装置については、外部からの侵入対策が講じられた場所に設置すること。

【障害対策（事業継続対応）】
1）情報セキュリティインシデントの発生時に迅速に対処するため、情報システムの構成が記載された文書※を管理・更新すること。
※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（情報システム名、システム構成、種別、機種、ソフトウェアの種類、バージョン、構成、識別コード等）に関する文書
2）情報システムを構成する機器等の関連文書を整備するとともに、構成要素ごとの情報セキュリティ水準を維持するための実施手順を整備すること。

3）サービスの継続性を確保するため、システムの異常停止を防止するとともに、障害時の復旧手順を整備すること。

【サプライチェーン・リスク対応】

1）情報セキュリティ対策の履行状況を確認するために、発注者が情報セキュリティ監査の実施を必要と判断した場合は、受注者は監査を受け入れること。

2）情報セキュリティ監査で問題点の指摘または改善案の提示を受けた場合には、対応案を調査職員と協議し、指示された期間までに是正を図ること。

【利用者保護対策】

1）情報セキュリティ水準を低下させる設定変更を利用者に要求することがないよう配慮した上で、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）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提供されないようにすること。

（3） 再委託に関する事項

1）本業務の一部を他の事業者に再委託させる場合には、受注者は、発注者が受注者に求めるものと同水準の情報セキュリティを確保するための対策を契約に基づき再委託先に行わせる。再委託先に行わせた情報セキュリティ対策及びこれを行わせた結果に関する報告を、受注者に求める場合がある。

2）業務の一部を再委託等（再々委託等、更なる再委託を含み、最終的に委託を受けた者までを含む。以下同じ）する場合においては、再委託等の相手方（以下「再委託先等」という。）の商号又は名称、法人番号、住所並びに再委託等を行う契約の範囲、再委託等の必要性及び契約金額等について記載した再委託等申請書を作成し、発注者の承認を得ること。

3）再委託先等については、発注者によるサプライチェーン・リスク等の確認の結果、変更を求めることがあることに留意すること。

4）再委託先等が更に再委託を行うことについて把握できるよう、再委託先等との契約文書等において明文化しそれらの報告等を義務づけること。

5）契約者は再委託先等の行為について本件に関する一切の責任を負うものとする。また、再委託先等において、本調達仕様書に定める事項に関する義務違反又は義務を怠った場合には、発注者は当該再委託先等への再委託等の中止を請求することができる。

6）再委託等を行う場合、再委託先等が本特記仕様書に示す要件を満たすこと。なお、本特記仕様書に示す要件を満たさない場合、それに準ずる対策等について記載した書面を提出し、発注者の承認を得ること。

7）再委託先等について、追加・変更が発生した場合は、その都度、修正内容を報告すること。変更等がない場合は、その旨確認したことを毎月報告すること。発注者の承認を得ずに再委託等が判明した場合は、指名停止等を含め厳しい対応を行う。

10．その他

（1） 本特記仕様書に記載なき事項について疑義が生じた場合は、調査職員と協議し決定すること。

（2） 本業務に必要な資料で、調査職員により提供可能なものは、その都度、これを貸与する。

（3） 本業務を遂行するにあたり取り扱うこととなる文書、情報の管理を徹底すること。

（4） 中立LANを経由してターミナルオペレーションシステムへの侵入を行わないこと。なお、中立LANを経由したターミナルオペレーションシステムへの侵入・攻撃等によるシステム障害に

ついては、本業務の受注者が一切の責任を負うこと。

（5） 本業務の履行期間中に、本システムのプログラムに改修を加えた場合においても、本システムの保守・運用に関しては、本業務の受注者が一切の責任を負うこと。

（6） 本業務を掌握するために本システム等の設計書を閲覧することが出来る。

（7） 暴力団員等による不当介入を受けた場合の措置

1）受注者は、暴力団員等による不当介入を受けた場合は、断固としてこれを拒否すること。

2）1）により警察に通報又は捜査上必要な協力を行った場合には、速やかにその内容を記載した書面により発注者に報告しなければならない。

3）1）及び2）の行為を怠ったことが確認された場合は、指名停止等の措置を講じることがある。

4）暴力団員等による不当介入を受けたことにより工程に遅れが生じる等の被害が生じた場合は、発注者と協議しなければならない。

（8） 本業務は、別件発注予定業務等（CONPAS システム改修及び検討業務、Cyber Port、出入管理情報システム、Colins）と密接な関係があることにより、関係者で協力するとともに必要に応じ調査職員と緊密に協議し、その指示に従わなければならない。

（9）作業体制及び作業従事者に関する事項

1）作業体制図及び担当者名簿を含む作業計画書を作成し、発注者の承認を得ること。

2）作業体制図には、品質保証の管理に係る管理体制及び本件で利用する端末の機器リストを含めること。

3）担当者名簿には、要員計画及び業務に関わる者の所属（契約社員、派遣社員等の雇用形態は問わず、委託事業に従事する全ての要員）、氏名、生年月日、住所（都道府県のみ）及び国籍を記載すること。

4）利用端末や要員については、発注者によるサプライチェーン・リスク等の確認の結果、変更を求めることがあることに留意すること。

5）業務の一部を再委託等する場合においては、その再委託先等についても作業体制図及び作業員名簿に含めること。

6）追加・変更が発生した場合は、その都度、修正内容について発注者の承認を得ること。変更等がない場合は、その旨確認したことを毎月報告すること。発注者の承認を得ずに作業実施等が判明した場合は、指名停止等を含め厳しい対応を行う。