第７章　システム導入後の保守作業の検討

章　内　目　次

7. システム導入後の保守作業の検討

システムを長期的・安定的に稼動させるため、システム導入後の保守作業について検討した。

システムの安定稼動のためには、システムの情報セキュリティ（機密性、完全性、可用性）が確保される必要がある。そこで、システムの稼動要件を整理するとともに、想定されるリスクを整理し、情報セキュリティ対策を検討した。さらに、情報セキュリティ対策を実現するためのシステム保守作業の内容及び役割分担、実施体制を検討し、保守運用仕様案を作成した。

7.1 システム稼働に関する要件

7.1.1 システムの特徴

本システムは、外環の各 JCT・IC における工事関係交通を一元管理し、円滑な車両運行を支援するとともに、搬出入されるシールド発生土のトレーサビリティを確保するものである。

本システムでは、東名 JCT、中央 JCT、大泉 JCT、青梅 IC に発着する発生土および資機材等の運搬車両の関東地方内での運行を対象とする。運用体制としては、外環国道事務所、NEXCO 中日本、NEXCO 東日本による 3 事業者会議のもとに、事業者が各 JCT の統括管理者として、需要調整会議の主催や JV への指示等を行う。

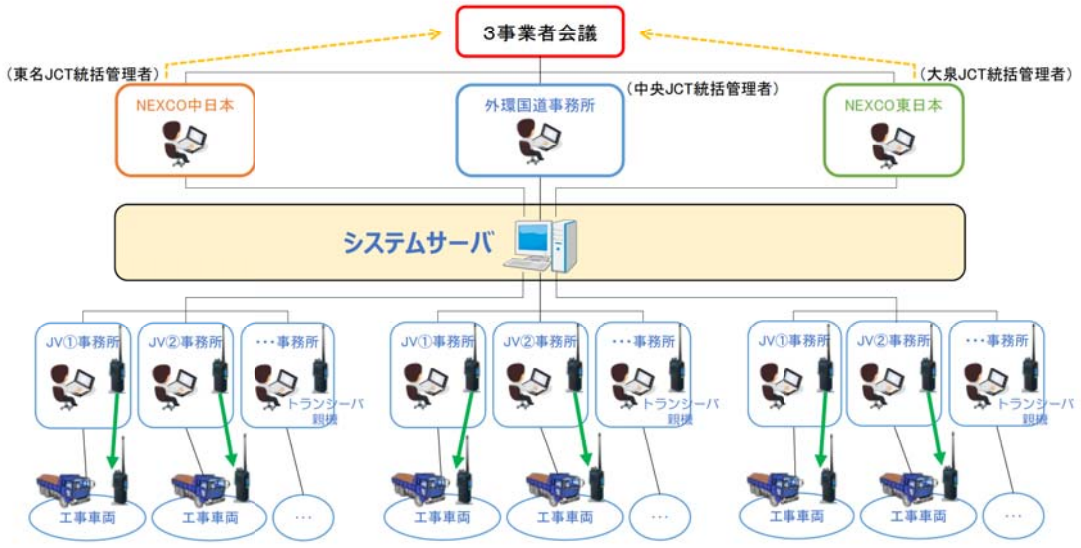


図 7-1　システム運用体制イメージ

本システムのシステム構成イメージを図 7-2 に示す。

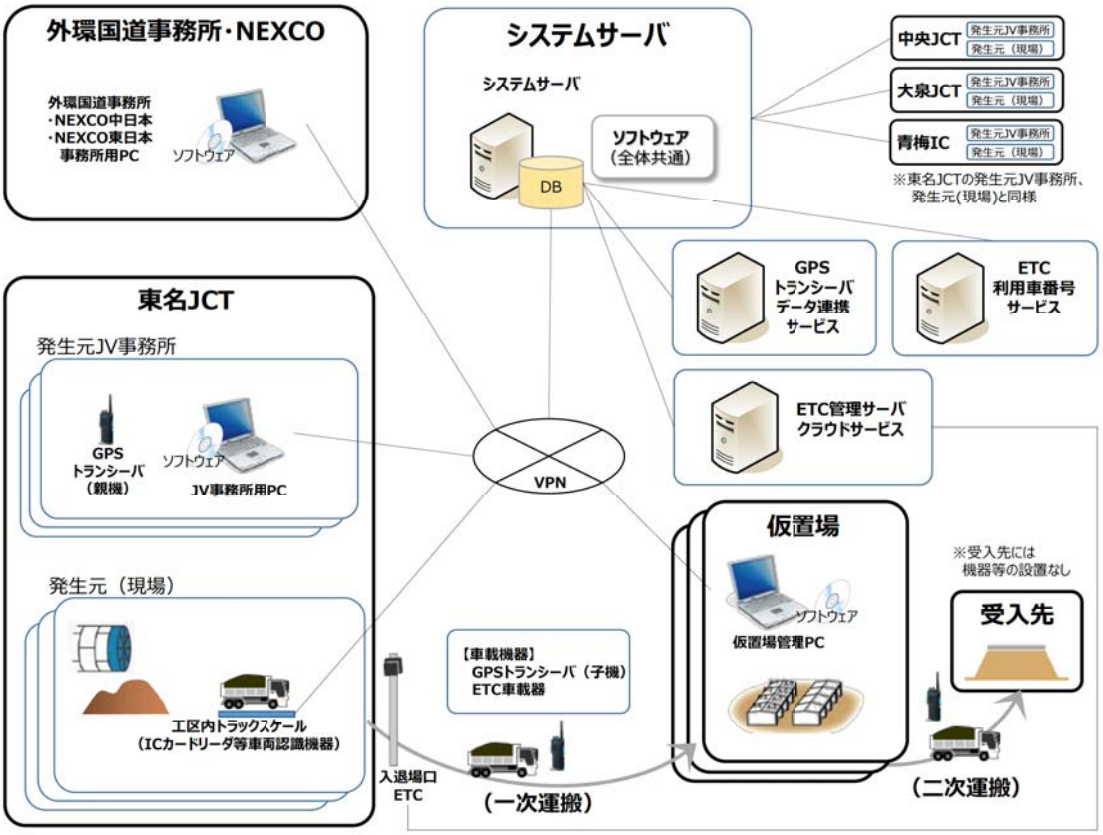


図 7-2　システム構成イメージ

本システムはクライアント/サーバ方式である。システムサーバは以下のとおり機器・サービスと連携を行う。

・クライアント端末：クライアント/サーバシステム（VPN 接続）
・トラックスケール：計量情報を取得（VPN 接続）
・GPS トランシーバデータ連携サービス
　：GPS トランシーバの位置情報を取得（SSL 接続）
・ETC 管理サーバクラウドサービス：ETC 路側機の車両通過情報を取得（SSL 接続）
・ETC 利用車番号サービス：ETC 利用車番号照会（SSL 接続）

7.1.2 システム稼動要件

(1) システム稼動時間

本システムは 24 時間稼動する。

(2) システム停止期間

通常時は 24 時間無停止とする。

本システムが停止しても、工事自体が停止することはないため、障害発生時は平日 1 日以内の復旧を目標とする。

(3) 障害発生後の復旧時点

障害発生前日夜までのデータを自動復旧する。

前日夜から復旧までのデータは、手作業により修復または、システム外で別途記録を保管する。

7.2 運用時想定されるリスクと情報セキュリティ対策の検討

7.2.1 情報資産の格付け

本システムは外環の各 JCT における工事関係交通を一元管理し、発生土等の運搬結果を蓄積する。本システムで取り扱う情報資産は、公共事業に係る情報であると同時に、複数の JV の施工情報を含む。

本システムで取り扱う情報資産を、「政府機関の情報セキュリティ対策のための統一基準（平成 28 年度版）」（サイバーセキュリティ戦略本部）より格付けする。

表 7-1　情報の格付けの定義

分類		定義	取扱い方法
機密性	機密性 3	秘密文書に相当する機密性を要する情報	特定の者だけがアクセスできる状態を厳密に確保する
	機密性 2	不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、「機密性 3 情報」以外の情報	行政事務従事者（※）以外がアクセスできない状態を最低限確保する
	機密性 1	不開示情報に該当すると判断される蓋然性の高い情報を含まない情報	
完全性	完全性 2	改ざん、誤びゅう又は破損により、国民の権利が侵害され又は行政事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報	情報が改ざん、誤びゅう又は破損されていない状態を確保する
	完全性 1	完全性2情報以外の情報	
可用性	可用性 2	滅失、紛失又は当該情報が利用不可能であることにより、国民の権利が侵害され又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報	情報が滅失又は紛失されていない状態及び情報へのアクセスを認められた者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保する
	可用性 1	可用性2情報以外の情報	

※本システムでは工事受託者を含む

本システムでは秘密文書に相当する情報は取り扱わないが、車両運転者について個人情報を含む可能性があり、また工事契約上の情報も含むため、一部の情報について、工事発注者および受託者以外がアクセスできない状態を確保する必要がある。また、情報の改ざんや紛失等によりシステム機能を発揮できない、またトレーサビリティ要件を満たせないおそれがあるため、完全性・可用性の確保が必要である。

表 7-2　システムで取り扱う情報の格付け

分類	データ名	機密性			完全性		可用性		備考
		3	2	1	2	1	2	1	
需要調整情報	工事車両運行計画ファイル		○		○		○		
	適正化需要ファイル		○		○		○		
	工事車両運行計画確定値ファイル		○		○		○		
運行管理情報	トランシーバ搭載車両		○		○		○		車両番号を含む、備考に運転者氏名等を含む可能性あり(個人情報)
	拠点通過実績			○	○		○		
	運搬経路判定用			○	○		○		
	仮置場搬入出管理			○	○		○		
	中継地搬入出管理			○	○		○		
	JCT 別拠点内車両台数			○	○		○		
車両動態情報	地図表示用 GPS			○	○		○		
	GPS 履歴			○	○		○		
運搬実績情報	車両運搬実績		○		○		○		備考に運転者氏名等を含む可能性あり(個人情報)
	その他の運搬実績		○		○		○		備考に個人情報を含む可能性あり
	仮置場区画添付資料		○		○		○		添付資料の内容は規定しない
	仮置場区画判定結果			○	○		○		
アラート台数情報	JCT アラート台数			○	○		○		
	JV アラート台数			○	○		○		
マスタ情報	工事情報		○		○		○		契約情報を含む
	拠点情報		○		○		○		契約情報を含む
	仮置場区画情報			○	○		○		
	トランシーバ情報			○	○		○		
	ユーザ情報			○	○		○		
	車両情報		○		○		○		車両番号を含む(個人情報)
	トラックスケール情報			○	○		○		

7.2.2 システム運用時に想定されるリスク

セキュリティに関する問題の種類により、機密性・完全性・可用性に対して及ぼす影響は異なる。このため、それぞれのインシデント特性を考慮したセキュリティ対策を考える必要がある。

表 7-3　インシデントの種類とその影響

インシデント	機密性	完全性	可用性
ウィルス感染	中	大	小
不正アクセス	大	大	小
サービス不能(Dos)攻撃	－	－	大
情報漏洩	大	－	－
システム障害	小	中	大

出典　https://www.nic.ad.jp/ja/materials/security-seminar/20031105/ikai.pdf

(1) 機密性に関するリスク

本システムは、システムサーバに対してクライアント端末、トラックスケール等の各種機器がクライアント/サーバ方式で接続される。また、GPS トランシーバデータ連携サービス、ETC 管理サーバクラウドサービス、ETC 利用車番号サービスとの連携を行う。このため、機密性に関するリスクとして、通信経路での情報漏洩（通信経路の盗聴）が想定される。

本システムは機密性２（秘密情報には該当しないが、関係者以外がアクセスできない状態を最低限確保するべき情報）の情報資産を含む。このため、通信経路の盗聴を防ぐ対策が必要となる。

(2) 完全性に関するリスク

本システムはシステムサーバにデータベースを搭載し、全てのデータを一括管理する。このため、完全性に関するリスクとして、システムサーバへの不正アクセスが想定される。

また、サーバ及びクライアント端末はインターネットに接続可能であるほか、クライアント端末はユーザが USB 等を接続することが可能である。このため、ウィルス感染によるデータ改ざんのリスクが想定される。

加えて、本システムでは GPS 等によりデータの自動取得を行っており、システム障害が起きた場合は、障害発生中のデータが失われる恐れがある。

データ改ざんや紛失等によりシステム機能を発揮できず、またトレーサビリティ要件を満たせないおそれがあるため、不正アクセス、ウィルス感染、システム障害を防ぐ対策が必要である。

(3) 可用性に関するリスク

サーバ及びクライアント端末はインターネットに接続可能である。このため、悪意ある第三者が通常の範囲を超えたアクセスを行うことで、システムを停止させる（Dos 攻撃）リスクがある。

また、システム障害が起きた場合は、システム機能を使用できなくなるリスクがある。

本システムは 24 時間稼動のシステムであり、システム機能を安定的に使用し続けるため、Dos 攻撃やシステム障害を防ぐ対策が必要である。

障害発生箇所別に、本システムで障害が発生した際の影響を表 7-4 に示す。本システムは外環工事の車両を取り扱う 24 時間稼動のシステムであるが、もし障害が起きた場合でも、工事自体がストップすることはない。ただし、障害発生期間中のデータが失われるおそれがあることから、障害発生中は、人手による記録作業等が必要となる。また、復旧後は、人手で記録していた情報をシステムに入力したり、帳票に取りまとめたりする作業が発生する。

表 7-4　システム障害による影響

障害発生箇所	障害による影響	障害時/復旧後の対応（案）		備考
システムサーバ	システム全体が停止する	以下の全ての対応が必要		・サーバが停止しても、GPSトランシーバでの通話はできる ・サーバが停止しても、ETC通過データは後日復旧できる
ETCデータ連携部分	・ETC路側機のパトランプが点灯しない ・発生元への車両入退場をリアルタイムに検知できない ・発生元を出発する発生土運搬実績データを正しく作成できず、運搬実績帳票が出力されない	障害時	・ETC利用車番号未登録車をパトライトで判別できないため、入場口でガードマンが全車両の入場をチェックする ・地図上に表示される車両アイコンの色で積載/空荷を区別できないため、車両の位置・進行方向から判断して運行指示する	・ETC通過データは、初めにETC管理サーバクラウドサービスに蓄積される ・ETC管理サーバからシステムサーバへETC通過データを送信できなかった場合は、**復旧後にまとめて送信される**
		復旧後	・発生元、仮置場、受入先への入退場記録（拠点通過履歴）より、必要に応じて手作業で帳票を作成する	
GPSデータ連携部分	・車両の位置を地図上に表示できない ・仮置場、受入先への車両入退場を検知できない ・仮置場、受入先を発着する発生土運搬実績データを正しく作成できず、運搬実績帳票が出力されない ・車両の走行履歴が残らない	障害時	・仮置場の入場口でガードマンが全車両の入場を記録する ・受入先の入場口でガードマンが全車両の入場を記録する ・地図を使用せずに運行指示する	・GPSデータ連携に不具合が生じても、GPSトランシーバでの通話はできる ・GPSデータは、初めにGPSトランシーバデータ連携サービスに蓄積される ・GPSデータ連携サーバには、障害発生中のデータを**復旧後に自動送信する仕組みがないため**、障害発生中の各車両の走行履歴（GPS点群）は取得できない
		復旧後	・発生元への入退場記録（拠点通過履歴）のみが自動作成されるため、仮置場、受入先の入場記録を加えて手作業で帳票を作成する	
トラックスケールデータ連携部分	・計量結果をシステムに保存できない ・運搬実績帳票に計量結果が反映されない	障害時	・トラックスケール側で保管できる場合は、計量データを蓄積しておく ・トラックスケール側に保管できない場合は、計量結果を手作業で別途保存しておく	・トラックスケールは、障害発生中のデータを**復旧後に自動送信する仕組みがないため**、障害発生中の計量データは別途登録が必要
		復旧後	・全体共用部分の保守作業員により、トラックスケール計量データを手作業でデータベースに登録する	
ETC利用車番号オンライン申請部分	・車両を新規登録しても、ETC利用車番号申請ができないため、ETC通過時に「未登録」扱いになる	障害時	・全体共用部分の保守作業員により、手作業で申請を行う	・ITS-TEAの受付時間は、自動化/手動にかかわらず、平日昼間のみ
		復旧後	・対応なし	
PCアプリケーション（JV事務所用PC、仮置場管理PC、JCT統括管理者事務所用PC）	・システム画面が操作できない ・発生元等の場内台数が超過しても、アラートが出ない	障害時	・需要調整は、エクセルファイルをメールで授受して実施する ・地図を使用せずに運行指示する ・仮置場の区画への搬入出時刻登録、区画の試験結果入力、運搬実績の修正、各種帳票出力等の作業は復旧まで延期する	・GPSトランシーバでの通話はできる ・サーバ側の機能（ETCデータ連携、GPSデータ連携、トラックスケールデータ連携）は稼動できる
		復旧後	・障害時に延期していた作業を実施する	

● システムが停止した場合に発生する費用（例）

システムが　8時間　全停止した場合に発生する主な費用を試算する。

1. 障害時
・発生元での入場チェック
・仮置場での入場チェック
・受入先での入場チェック
・計量結果の記録
（シールドJVのみ）

※運行指示を行う職員は増員しないと想定

[redacted]

2. 復旧後
・トレーサビリティ帳票作成
（シールドJVのみ、1JVあたり半日程度の作業とする）

※延期した作業の担当者は増員しないと想定

7.2.3 情報セキュリティ対策

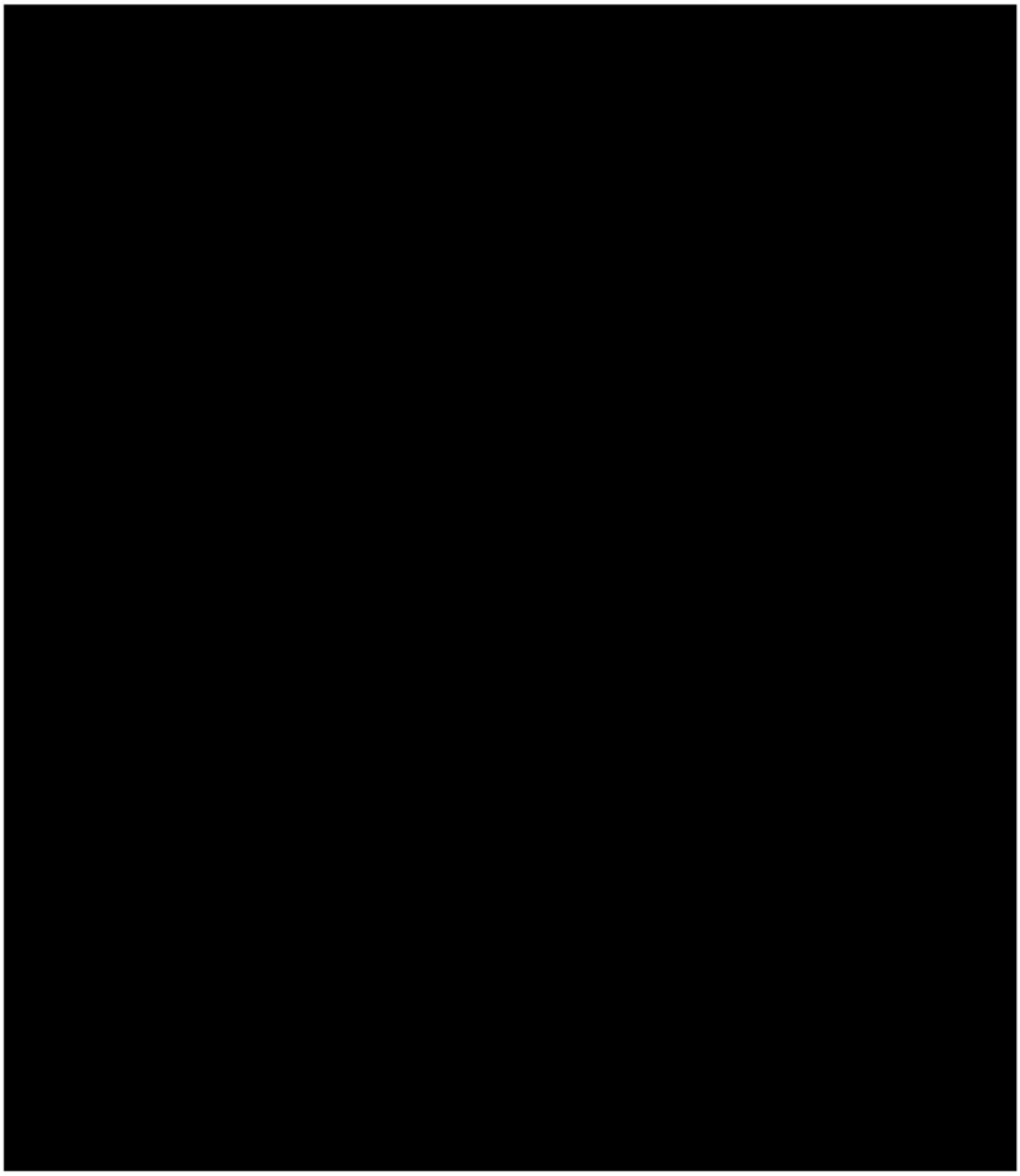
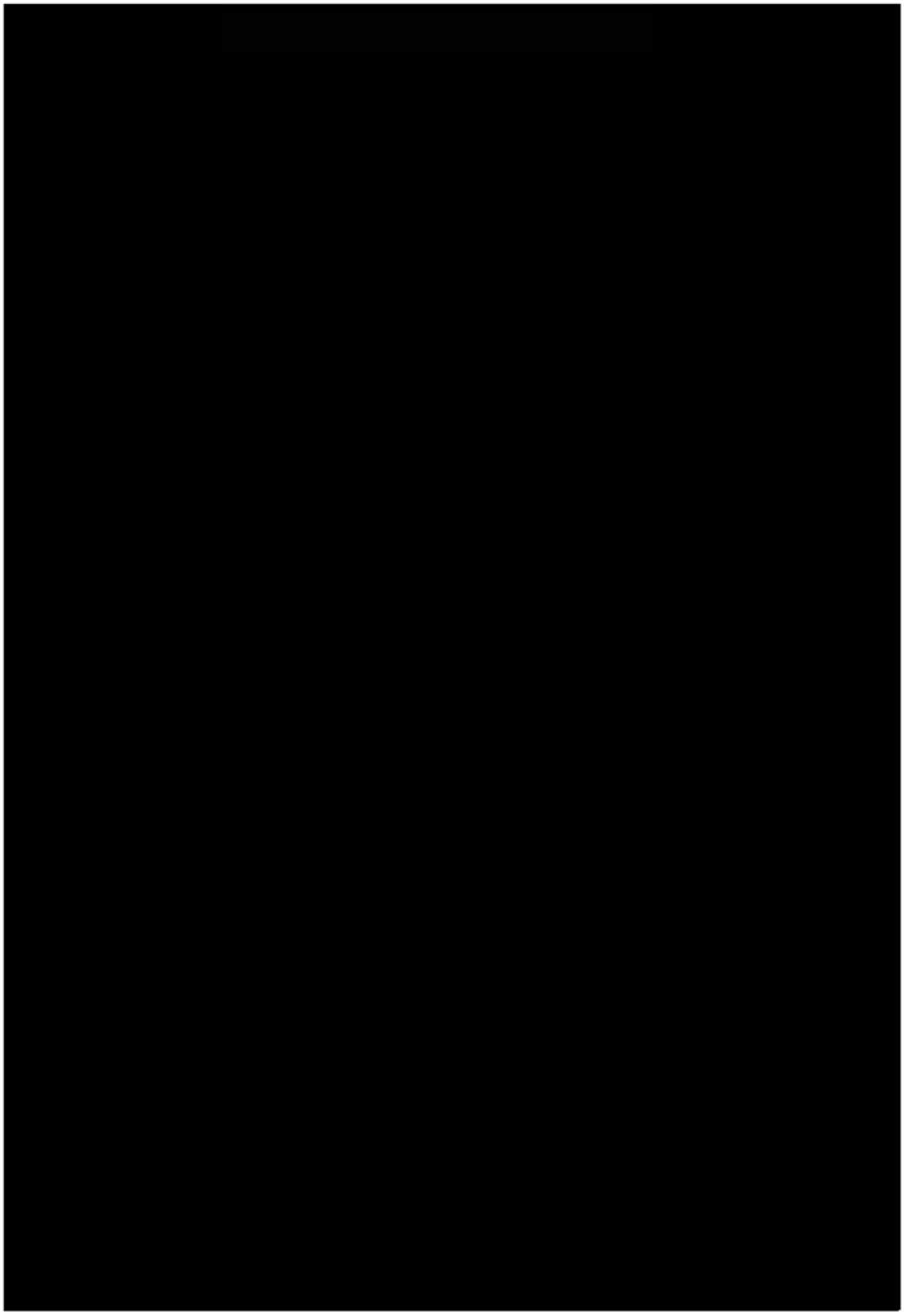


表 7-5　ユーザ別のデータ閲覧・編集権限



(4) システム障害に関する対策

③ ネットワークの冗長化

■参考：Arcstar Universal One の冗長化

Q6：アクセス回線標準二重化とはどういうことですか？メリットは何ですか？

Arcstar Universal Oneは、メインのアクセス回線に加えてバックアップのアクセス回線を標準でご提供しています。「Universal Oneターミナル」も、アクセス回線の二重化に対応しており、面倒な設計は不要。万が一の回線故障時にも自動でバックアップ側の回線に切り替わり、安心して ご利用いただけます。

Q24：VPN網内は冗長化されていますか？

冗長化しています。中継ルーターについては、装置および中継線を二重化・二面化、お客さま収容ルーターについては、共有部（電源など）の二重化を行っています。

出典：Arcstar Universal One よくあるご質問

http://www.ntt.com/business/services/network/vpn/vpn/faq.html

④ 試験環境の整備

7.3　システム保守作業の内容及び役割分担、実施体制の検討

システムの稼動要件及び情報セキュリティ要件を踏まえ、本システムの保守作業の内容、役割分担、実施体制を検討した。

7.3.1 保守作業の内容及び役割分担

本システムの機器等は、全体共用部分、JCT 共用部分、個別工事担当部分、仮置場担当部分に分けて調達されている。システム保守においても調達時の担当を踏襲し、各調達を行った事業者が、適切な作業担当者へ保守作業を発注することを想定する。

表 7-6　保守作業項目及び役割分担

7.3.2 保守作業の実施体制

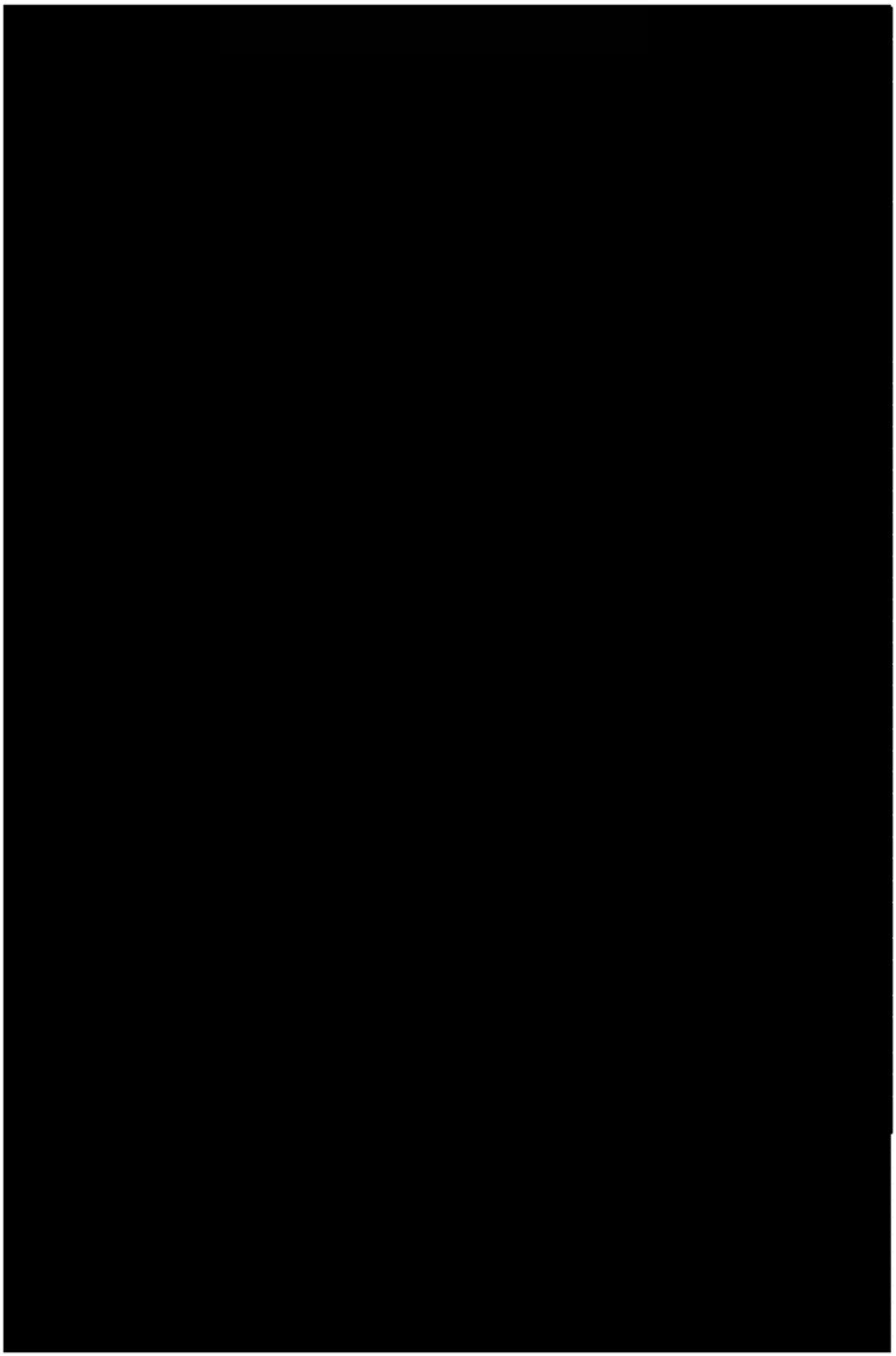
(1) 障害対応時間

本システムは24時間稼動するため、障害対応時間を平日昼間だけに限定するか、24時間365日対応するかを比較検討した。比較表を表 7-7 に示す。

本システムが停止しても、工事自体が停止することはないため、まずは案 1（平日 9～18 時）にて稼動を開始することとした。

なお今後、システム利用者及び車両運行台数が増えた場合にも十分な体制を確保できているかどうか、JV や事業者へのヒアリング等を通じて継続的にモニタリングしていく必要がある。

表 7-7　障害対応時間による影響範囲と費用



(2) ヘルプデスク対応時間

本システムは 24 時間稼動するため、ヘルプデスク対応時間を平日昼間だけに限定するか、24 時間 365 日対応するかを比較検討した。比較表を表 7-8、表 7-7 に示す。

ヘルプデスクは対応時間中、常時待機している必要があり、問合せが少なければヘルプデスク要員が無為に待機することとなる。このため、まずは案 1（平日 9～18 時）にて稼動を開始することとした。

なお今後、システム利用者及び車両運行台数が増えた場合にも十分な体制を確保できているかどうか、JV や事業者へのヒアリング等を通じて継続的にモニタリングしていく必要がある。

表 7-8　ヘルプデスク対応時間による影響範囲と費用

比較項目	案1	案2
選択肢	平日9～18時	24時間　365日
影響範囲	△　障害発生の第一報が遅れる △　夜間に操作方法が分からなくなった場合、ヘルプデスク開始時刻まで作業できない	○　障害発生の第一報が早い △　夜間は問合せが少ないため、ヘルプデスク要員は待機状態が多くなる
[redacted]		

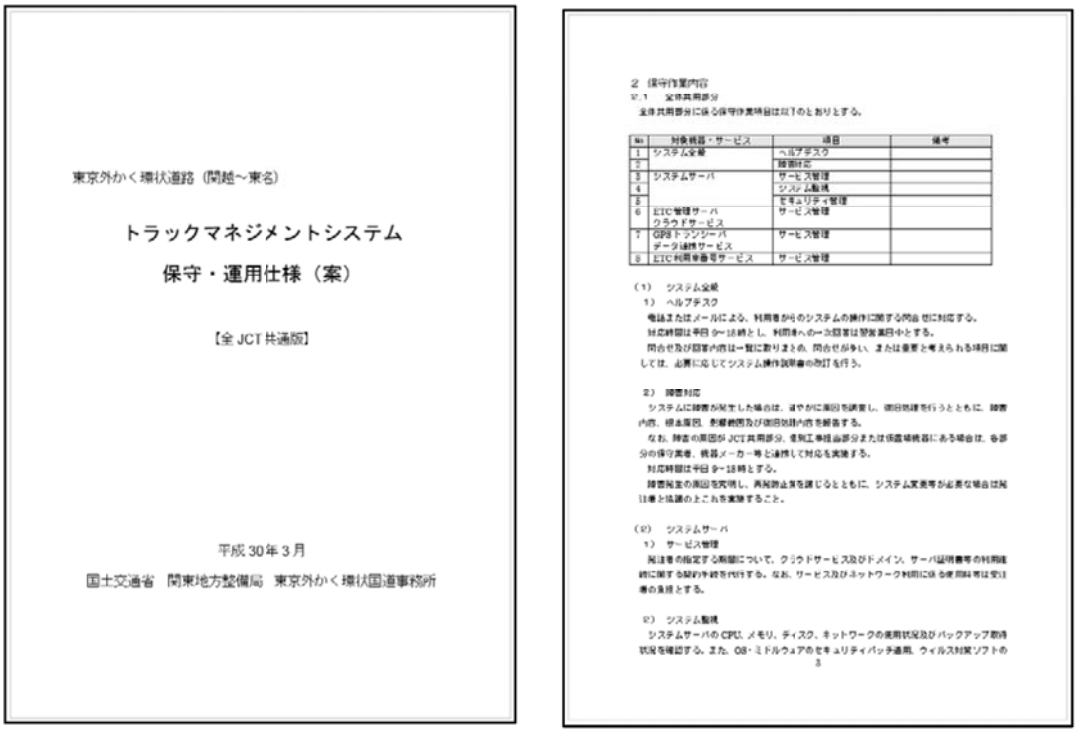
＜概算費用の算出方法＞

・時間帯による割増率を以下のように設定した。

種別	労働時間	割増率
平日	9～18時	100%
	5時～9時 18～22時	125%
	22～5時	160%
休日	5～22時	150%
	22～5時	185%

7.3.3 保守運用仕様案の作成

前項までの検討内容を踏まえ、トラックマネジメントシステム保守・運用仕様（案）を作成した。



東京外かく環状道路（関越～東名）

トラックマネジメントシステム
保守・運用仕様（案）

【全 JCT 共通版】

平成 30 年 3 月
国土交通省　関東地方整備局　東京外かく環状国道事務所

2　保守作業内容

2.1　全体共用部分

全体共用部分に係る保守作業時間は以下のとおりとする。

No	対象機器・サービス	項目	備考
1	システム全般	ヘルプデスク	
2		障害対応	
3	システムサーバ	サービス管理	
4		システム監視	
5		セキュリティ管理	
6	ETC管理サーバ クラウドサービス	サービス管理	
7	GPSトランシーバ データ連携サービス	サービス管理	
8	ETC利用申番号サービス	サービス管理	

（1）　システム全般

1）　ヘルプデスク

電話またはメールにより、利用者からのシステムの操作に関する問合せに対応する。

対応時間は平日 9～18 時とし、利用者へのメール回答は翌営業日中とする。

問合せ及び回答内容は一覧に取りまとめ、問合せが多い、または重要と考えられる項目に関しては、必要に応じてシステム操作説明書の改訂を行う。

2）　障害対応

システムに障害が発生した場合は、速やかに原因を調査し、切り分けを行うとともに、障害内容、根本原因、影響範囲及び復旧見込みの内容を報告する。

なお、障害の原因が JCT 共用部分、受託工事担当部分または搭載機器にある場合は、各部分の保守業者、機器メーカー等と連携して対応を実施する。

対応時間は平日 9～18 時とする。

障害発生の原因を究明し、再発防止策を講じるとともに、システム変更等が必要な場合は関係者と協議の上これを実施すること。

（2）　システムサーバ

1）　サービス管理

発注者の指定する期間について、クラウドサービス及びドメイン、サーバ証明書等の利用期間に関する契約手続を代行する。なお、サービス及びネットワーク利用に係る使用料等は受注者の負担とする。

2）　システム監視

システムサーバの CPU、メモリ、ディスク、ネットワークの使用状況及びバックアップ取得状況を確認する。また、OS・ミドルウェアのセキュリティパッチ適用、ウィルス対策ソフトの

3

図 7-3　トラックマネジメントシステム保守・運用仕様（案）イメージ

7.4　今後の課題

7.4.1 試験環境の整備

本格運用の開始当初は、システムサーバの試験環境がない状態である。今後、システム改良等を行う場合に、本番と同等の環境で改良プログラムの試験を行えるようにするため、試験環境を整備することが望ましい。

7.4.2 保守作業の実施体制のモニタリング

本格運用の開始当初は、障害対応時間及びヘルプデスク対応時間を平日 9～18 時としている。今後、システム利用者及び車両運行台数が増えた場合にも十分な体制を確保できているかどうか、JV や事業者へのヒアリング等を通じて継続的にモニタリングしていく必要がある。