交通安全施設用パーソナルコンピュータ仕様書

北 海 道 警 察 釧 路 方 面 本 部 交 通 課

1　適用範囲

本仕様書は、北海道警察釧路方面本部の交通安全施設用パーソナルコンピュータの賃貸借契約に適用する。

2　機器の構成等

(1)　賃貸借契約する機器構成等は次のとおりとする。

交通安全施設用パソコン（ソフトウェアを含む。）

(2)　機器の構成及び数量は次のとおりとする。

	品　　名		構　　成	数量	単位	設置場所
パソコン	パーソナルコンピュータ		本体	2	台	釧路方面本部 交通課
			セキュリティワイヤー	2	個	
			マウス（マウスパッド含む）	2	個	
			キーボード	2	個	
	ソフトウェア	統合ソフトA		2	式	
		統合ソフトB		2	式	
		製図ソフト		2	式	
		図形ソフト		2	式	
		地図ソフト		2	式	
		ログ管理ソフト		2	式	
		ウイルス対策ソフト		2	式	
周辺機器等	ディスプレイ		ディスプレイケーブル含む	2	台	
	プリンタ		プリンタケーブル含む	1	台	

3　使用条件

(1)　電源

本機器は、交流電源（100V±10V、50Hz）で安定した動作をすること。

(2)　温湿度

本機器は、温度10℃～30℃、相対湿度30～80%の範囲において安定した動作をすること。

4 各種機器仕様

パソコン

項　目		機 能 及 び 性 能
本体 パーソナルコンピュータ		デスクトップ型
	OS	Windows 11Pro（日本語版 64bit）であること。
	CPU	インテル Core i5-8500 プロセッサー (3.0GHz) 同等あるいは、それ以上の中央処理装置であること。
	メインメモリ	16 GB以上を、実装すること。
	ストレージ	データ容量が500GB以上、磁気ディスクドライブ又はSSDで暗号化機能付きであること。
	光学ドライブ装置	DVDスーパーマルチドライブ以上を、本体に内蔵すること。
	ディスプレイカード	GPUが2GB以上であること。
	インターフェイス	次のインターフェイスを有すること。 ・USB：USB3.0対応、4個以上（内一つは前面）
	その他	無線LAN機能を搭載している場合は、その機能を無効化できること。 LANインターフェイス機能を搭載している場合は、その機能を無効化できること。
セキュリティワイヤー		パソコン本体に取り付け可能なシリンダー錠タイプ又は南京錠タイプであること。 長さ1.8m以上、太さ3.0mm以上5.0mm以下であること。
マウス		USB光学式またはレーザー式のホイール付き2ボタンであること。
キーボード		テンキー付きでUSB接続であること。

ソフトウエア

項　目	機 能 及 び 性 能
統合ソフトA	Microsoft Office Personal 2021同等品以上であること。
統合ソフトB	Just System社 Just Police 5 であること。 契約時における最新版のバージョンであること。
製図ソフト	Ijcad STD シングル 期間ライセンス（5年）であること。
図形ソフト	Adobe Reader （無償）の最新版をインストールすること。
地図ソフト	昭文社 SuperMapple デジタル24 東日本版であること。
ログ管理ソフト	RUNEXY社製 MylogStar 4 Desktop であること。
ウィルス対策ソフト	トレンドマイクロ社 ウイルスバスター コーポレートエディションPLUS（最新版）と同等に、不正アクセスや不正プログラム等の検知・駆除が可能であること。 契約時における最新版のバージョンであること。 契約期間中の更新権を有すること。
その他	上記ソフトウエアはすべて日本語版とすること。 OSを含めたすべてのソフトウエアについては、すべて最新の修正モジュール、若しくはサービスパックを適用することとし、北海道警察の指示によりアップデート（オフラインでの手動更新）を行うこと。 障害発生対策としてソフトウエアについてはすべて再インストール用の媒体を添付すること（統合ソフトA及び製図ソフト、図形ソフトを除く。）。

周辺機器等

項　目	機 能 及 び 性 能
ディスプレイ	ワイド液晶パネル21．5インチ以上かつ16bitカラー対応であること。 解像度 1920×1080ドット以上であること。
プリンタ	A3版用紙にカラー印刷が可能なレーザー式であること。 2以上の給紙トレイを有すること。パソコンとUSBで接続可能なこと。 オフラインで使用するため、無線LAN機能及びWifi機能を有しないこと又は停止できること。

5　注意事項

⑴　4に掲げる機器及びソフトウエアについては、Microsoft Windows 11 Pro 64ﾋﾞｯﾄ で正常に動作すること。

⑵　機器の保守については、別紙 1「特記事項」のとおり。

⑶　北海道グリーン購入基本方針の判断基準に適合していること。

6　その他

⑴　当該調達に関し、特に定める事項については、別紙1「特記事項」による。

⑵　本仕様書を、当該調達手続に関係ない第三者に譲渡、閲覧及び交付してはならない。

別紙１

特　記　事　項

１　納入条件

⑴　機器の使用に必要な搬入、設置及び調整等の作業を行うこと。

⑵　機器の搬入、設置及び調整作業や、ソフトウエア及びプリンタドライバ等のインストール作業は北海道警察（以下「甲」という。）と協議の上、指示に従うこと。

⑶　機器の納入に伴うソフトウエアのインストール作業等、事前準備に要する場所は、契約の相手方（以下「乙」という。）が確保すること。

⑷　機器やソフトウエアのユーザ登録等は、乙が行うこと。

⑸　機器の梱包材等は、乙の責任において処分すること。

⑹　設置及び設定等の作業に従事するため庁舎内に立ち入る要員の氏名等について、別途指示する様式により事前に甲に申し出ること（搬入作業にのみ従事する者を除く。）。

⑺　上記経費は、機器の賃貸借料に含まれるものとする。

⑻　契約物品は同一機器とする。

⑼　乙は甲の求めにより設置場所において操作説明を行うこと。必要な説明書類等は乙が用意すること。

⑽　ログイン時に主体認証を行う機能の設定を行うこと（管理者ユーザー・一般ユーザーの登録、一定回数認証に失敗した際に認証を一定時間停止させる設定等）。

２　保守要領

⑴　乙は、機器の正常な動作を確保するため、次に掲げる機器の保守点検業務を行うものとする。

保　守　対　象　機　器	数量	摘　　要
○交通安全施設用パーソナルコンピュータ	２式	パーソナルコンピュータとこれに接続するマウス及びキーボード並びに各種ケーブルを含む。
○ソフトウエア（甲がインストールしたソフトを除く。）	２式	また、各機器に内蔵する電池（二次電池を含む）の劣化についても、保守の対象とする。
○プリンタ	１式	プリンタケーブルを含む

保守体制は、平日８時間（午前９時から午後５時まで）とし、甲の口頭による通知後当該機器設置場所において障害状況を確認し、修理を行うものとする。

⑵　保守の都合上、やむを得ず修理対象機器を機器設置場所以外で修理をする場合には、事前に甲の了解を得ること。

なお、当該機器が電磁的記録装置を内蔵する場合、甲の指示に従い乙が用意するデータ消去機能を有する装置で、所要の措置を講じてから修理に着手すること。データ消去が困難な場合には、北海道警察職員立会のもと乙が磁気ディスク等を再利用できない状態にすること。

また、修理完了までの間、当該機器と同等又は同等以上の性能を有する機器を、乙の責任において必要なソフトウエアのインストール及び設定等を行い設置すること。

⑶　保守作業に従事するため甲の指示する場所に立ち入る要員の氏名等について、別途指示する様式により事前に申し出ること。保守要員が異動等により変更となった場合には、その都度届け出ること。

⑷　甲は、保守作業の遂行につき保守要員が著しく不適当であると認めた場合は、乙に対して当該理由を通知し、必要な措置をとるべきことを求めることができるものとする。

⑸　保守に要する経費は、機器の賃貸借料に含まれるものとする（但し、天災その他不可抗力、または使用者側の故意若しくは重大な過失による場合を除く。）。

⑹　保守用部品は、令和12年２月28日まで確保しなければならない。

３　遵守事項

乙は、別紙２「情報セキュリティの確保に関する特約条項」の各事項を遵守すること。

４　サプライチェーン・リスク対策

⑴　本仕様書で調達するソフトウェア及びハードウェアの候補となる機器等については、あらかじめ甲に機器等リストを提出し、甲がサプライチェーン・リスクに係る懸念が払拭されないと判断した場合には、甲と迅速かつ密接に連携し、代替品選定等を行うこと。

⑵　本仕様書で調達するソフトウェア及びハードウェアについて、不正な変更（機器等の製造工程、流通過程で不正プログラムを含む予期しない又は好ましくない特性を組み込むことをいう。）が疑われると甲が判断した場合は、乙において調査及び必要な措置を講じること。

⑶　機器等の製造工程において意図しない変更が加えられないよう適切な措置が執られており、当該措置を継続的に実施していること。

⑷　機器等の製造工程の履歴に関する記録を含む製造工程の管理体制が適切に整備されていること。

⑸　機器等に対して不正な変更が加えられないように製造者等が定めたセキュリティ確保のための基準等が整備されており、その基準等が機器等に適応されていること。

⑹　機器等の設計から部品検査、製造、完成品検査に至る工程について、不正な変更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。機器に不正が見つかったときに、追跡調査や立入検査等により原因を調査し、排除できる体制を整備している生産工程による製品であること。

⑺　機器を構成する要素（ソフトウエア、ハードウエア）に対して不正な変更があった場合に識別できる構成管理体制が確立していること。

⑻　乙が機器を構成する要素（ソフトウエア、ハードウエア）として採用した機器等について、不正な変更が加えられていないことを検査する体制が乙において確立していること。

⑼　前記⑶から⑻については、甲が必要と認める場合には、証明又は確認できる資料等の提出を求めることがある。

５　機器の撤去

⑴　契約期間満了後、乙は機器の設置場所から当該機器を撤去すること。

⑵　当該機器が電磁的記録装置を内蔵する場合は、記録データをいかなる手段及び方法によっても復元不可能な方法で確実に消去し、甲の確認を受けること。

⑶　上記の経費は、機器の賃貸借料に含まれるものとする。

６　責任の所在

納入物品の稼働及び保守については、物品の製造者及び保守業者のいかんにかかわらず、乙が最終責任を負うこと。

別紙２

情報セキュリティの確保に関する特約条項

（目的）

第１条　乙は、本契約に係る業務（以下「本件業務」という。）の実施のために、甲から提供する情報その他本件業務の実施において知り得た情報（以下「保護すべき情報」という。）の機密性、完全性及び可用性を維持すること（以下「情報セキュリティ」という。）に関して、この特約条項に定めるところにより、その万全を期さなければならない。

２　保護すべき情報の範囲は次の各号とする。

⑴　甲が管理対象にするものとした文書、図面、図書等（電磁的記録を含む。）

⑵　甲が管理対象にするものとした物件

⑶　⑴又は⑵に掲げるものを基に、乙が作成（複製及び写真撮影を含む。）した文書、図面、図書等（電磁的記録を含む。）又は物件

（再委託の禁止）

第２条　乙は、本契約の全部又は一部を第三者に再委託させてはならない。ただし、やむを得ず再委託をしようとするときは、その再委託を受ける者、契約内容等を記した書面を添え、甲の承認を得るものとする。

２　前項ただし書により乙が再委託をする場合、乙は、乙と再委託を受ける者との間で締結する契約において、再委託を受ける者において本特約条項と同等の情報セキュリティの確保が行われるよう定めなければならない。

３　甲は、前項の契約について、情報セキュリティの確保が十分満たされていないと認められる場合、第１項の承認をしないことができる。

４　第１項ただし書により乙が再委託をする場合の再委託を受ける者その他本契約の履行に係る作業に従事する乙以外の事業者（以下「再委託を受ける者等」という。）における情報セキュリティの確保について、乙は本特約条項に従い、必要な通知、申請、確認等を行うものとする。

（情報セキュリティ確保のための体制等の整備）

第３条　乙は、保護すべき情報に係る情報セキュリティを確保するために必要な体制を整備しなければならない。

２　乙は、乙の代表者又は代表者から代理権限を与えられた者を情報セキュリティに係る責任者（以下「情報セキュリティ責任者」という。）とし、情報セキュリティ責任者の下に、保護すべき情報の管理に係る管理責任者を指定し甲に通知するものとする。

３　乙は、保護すべき情報に接する者（乙及び再委託を受ける者等における、派遣社員、契約社員、パート、アルバイト等を含む。以下「取扱者」という。）から情報セキュリティの確保に関する誓約書を徴収するとともに、取扱者の名簿を作成し、同名簿を甲に提出しなければならない。

（守秘義務）

第４条　乙は、保護すべき情報を本契約の履行期間中のほか、履行後においても第三者に開示又は漏えいしてはならない。

２　取扱者は、在職中及び離職後においても、保護すべき情報を第三者に開示又は漏えいしてはならない。

３　乙又は再委託を受ける者等がやむを得ず保護すべき情報を第三者に開示しようとする場合には、乙はあらかじめ、書面により甲に申請し承諾を得なければならない。

（管理）

第５条　乙は、本契約に基づき、甲が乙に提供する情報（以下「業務情報」という。）及び甲が乙に貸与する仕様書その他の資料（以下「業務資料」という。）については、特に厳重な取扱いを行うものとし、その保管管理について一切の責任を負うものとする。

２　乙が甲の指定する場所において個別業務を行う場合に持ち込む物品、業務情報及び業務資料は適正に管理するものとする。

　また、甲の承諾なくしては、その場所から物品、業務情報及び業務資料を持ち出してはならない。

３　乙は、第１項及び第２項の業務情報及び業務資料の管理について、甲の承認を得るものとする。

４　乙は、業務情報及び業務資料について、本契約の履行その他甲の指定した目的以外に使用してはならない。

５　乙は、業務情報について、本契約が終了したとき、又は甲から廃棄を求められたときは、これを直ちに甲が認める方法により廃棄するものとする。

６　乙は、業務情報及び業務資料を、甲の承諾なくしては、方法のいかんにかかわらず複製・複写してはならない。

７　乙は、業務資料について、本契約が終了したとき、又は甲から返還を求められたときは、これを直ちに甲に返還するものとする。

８　乙が作成（複製及び写真撮影を含む。）した文書、図面、図書等（電磁的記録を含む。）又は物件のうち、乙から甲に所有権が移転したものは全て甲の認める方法により廃棄しなければならない。

（作業責任者の選出）

第６条　乙が甲の指定する場所において個別業務を行う場合、乙は業務実施に関する乙の作業責任者を定め、書面をもって甲に通知するものとする。

２　前項により選任された作業責任者は、作業場所における乙の個別業務の実施を統括し、乙の定める規則に基づき就業管理を行い、個別業務の遂行に関する一切の事項を処理し、個別業務の遂行につき乙を代理する権限を有するものとする。

３　乙が作業責任者の権限に関し制限を設けた場合若しくは作業責任者を変更する場合は、乙は当該内容を書面により事前に甲に通知するものとする。

４　甲は、個別業務の遂行について作業責任者又は作業員が著しく不適当であると認めた場合は、乙に対して当該理由を通知し、必要な措置を執るべきことを求めることができるものとする。

（作業員名簿の提出）

第７条　乙が甲の指定する場所において個別業務を行う場合、乙は業務実施に関する乙の作業員名簿を作成し、書面をもって甲に通知するものとする。

（脆(ぜい)弱性対策等の実施）

第８条　乙は、本件業務を実施するに当たり、情報システムを使用する場合について、当該情報システムのアクセス権の付与を業務上必要な者に限るとともに、保護すべき情報へのアクセスを記録する措置を講ずるものとする。

２　前項の場合に、乙は、情報システムに対する不正アクセス、不正プログラム感染等情報システムの脆(ぜい)弱性に係る情報を収集し、これに対処するための必要な措置を講ずるものとする。

（情報セキュリティの対策の履行状況の確認）

第９条　乙は、契約締結後速やかに、本特約条項が定める項目を含む情報セキュリティ対策の履行状況（以下「情報セキュリティ対策履行状況」という。）を確認するとともに、確認結果について甲に報告するものとする。

２　乙は、契約締結後、少なくとも１年に１回、情報セキュリティ対策履行状況を確認するとともに、確認結果について甲に報告するものとする。

３　前各項の確認については、別記様式「情報セキュリティ対策履行状況確認書」によるものとする。ただし、別記様式の様式により難い場合は、この限りではない。

４　乙は、再委託を受ける者等における情報セキュリティ対策履行状況について、前各項に準じた確認の結果を甲に対して報告するものとする。

５　乙は、甲に報告した確認結果について、甲の承認を得るものとする。

（情報セキュリティ侵害事案等事故）

第10条　情報セキュリティ侵害事案等事故（以下「事故」という。）とは次の各号のことをいう。

⑴　保護すべき情報のほか、契約に係る情報について、外部への漏えい又は目的外利用が行われた場合

⑵　保護すべき情報のほか、契約に係る情報について、認められていないアクセスが行われた場合

⑶　保護すべき情報を取り扱い又は取り扱ったことのある電子計算機又は外部記録媒体に不正プログラム感染が認められた場合

⑷　⑴から⑶までに掲げるもののほか、甲又は乙の保護すべき情報のほか契約に係る情報の

侵害、紛失、破壊等の事故が発生し、又はそれらの疑い若しくはおそれがある場合

（情報セキュリティ侵害事案等事故に関する乙の責任）

第11条　乙は、取扱者の故意又は過失により前条に規定する事故があったときでも、契約上の責任を免れることはできない。

（情報セキュリティ侵害事案等事故発生時の措置）

第12条　乙は、本契約の履行に際し、第10条に規定する事故があったときは、適切な措置を講ずるとともに、速やかにその詳細を甲に報告しなければならない。

２　甲は、第10条に規定する事故が発生した場合、必要に応じ乙に対し調査を実施することとし、乙は甲が行う当該調査について、全面的に協力しなければならない。

３　第10条に規定する事故が再委託を受ける者等において発生した場合、乙は甲が当該再委託を受ける者等に対して前項の調査を実施できるよう、必要な協力を行うものとする。

４　乙は、第10条に規定する事故の損害・影響等の程度を把握するため、必要な業務資料等を契約終了時まで保存し、甲の求めに応じて甲に提出するものとする。

５　第10条に規定する事故が乙の責めに帰すべき事由による場合、当該措置に必要な経費については乙の負担とする。

６　前項の規定は、甲の損害賠償請求権を制限するものではない。

（意図しない変更が加えられないための体制の整備）

第13条　乙は、甲より委託された業務の実施において、情報システムに対し甲の意図しない変更が加えられないことを保証する管理を行うこと。また、甲の求めに応じて具体的な品質保証体制を証明する書類を提出することとする。

２　情報システムに対し甲の意図しない変更が加えられる不正が判明した際には、追跡調査や立ち入り検査等により原因を調査し、排除するための体制を構築するものとする。

（情報セキュリティ監査）

第14条　甲は必要に応じ、乙に対して情報セキュリティ対策に関する監査を行うものとし、監査の実施のために、甲の指名する職員を乙の事業所その他関係先に派遣することができる。この場合、乙は、監査を受け入れる部門、場所、時期、条件等を記載した、「情報セキュリティ監査対応計画書」を事前に甲に提出することとする。

２　甲は、前項の規定にかかわらず、情報セキュリティ対策に関し特段の必要が生じた場合、緊急に監査を実施することができる。

３　乙は、甲が情報セキュリティ対策に関する監査を実施する場合、甲の求めに応じ、必要な協力（甲の指名する職員による取扱施設への立ち入り及び関係書類の閲覧等）をしなければならない。

４　甲が再委託を受ける者等に対して情報セキュリティ対策に関する監査を行うことを求める場合、乙は当該監査の実施のために必要な協力を行うこととする。

５　乙は、自ら情報セキュリティ対策に関する監査を行った場合は、その結果を甲に報告することとする。
６　甲は、監査の結果、情報セキュリティ対策が十分満たされていないと認められる場合は、その是正のための必要な措置を講ずるよう乙に求めることができる。
７　乙は、前項の規定により、甲から求めがあったときは、速やかにその是正措置を講じなければならない。

（契約の解除）
第15条　甲は、第10条に規定する事故が、乙の責めに帰すべき事由により発生し、本契約の目的を達することができなくなった場合は、この契約の全部又は一部を解除することができる。
２　前項の規定により甲がこの契約を解除した場合において、主たる契約条項の契約の解除に関する規定を準用する。

別記様式

情報セキュリティ対策履行状況確認書

1　確認対象者

⑴　事業者名：

⑵　対象部門等名：

⑶　契約開始年月日：

⑷　前回確認実施年月日：

【留意事項】

確認対象者が再委託を受ける者等の場合は、⑴に事業者名を記載し、その末尾に「(再委託を受ける者等)」と記載すること。

この場合、⑶には、再委託契約等の開始年月日を記載すること。

2　確認事項

番号	確認事項	確認結果	実施状況（詳細）、未実施等の理由
第２条関係			
1	本契約の全部又は一部を第三者に再委託していない。	□している □していない	
2	（再委託している場合） やむを得ず再委託をしようとするときは、その再委託を受ける者、契約内容等を記した書面を添え、甲の承諾を得ている。	□承諾あり □承諾なし	
第３条関係			
3	代表者又は代表者から代理権限を与えられた者を情報セキュリティ責任者としている。	□している □していない	
4	情報セキュリティ責任者の下に、保護すべき情報の管理に係る管理責任者を指定し、甲に通知している。	□している □していない	
5	取扱者から情報セキュリティの確保に関する誓約書を徴収している。	□している □していない	
6	取扱者の名簿を作成し、甲に提出している。	□している □していない	
~~7~~	~~教育計画を作成し、甲の承認を得ている。~~	□承認あり □承認なし	
8	その他、情報セキュリティを確保するために必要な体制を整備している。	□該当あり □該当なし	※
第４条関係			
9	保護すべき情報を第三者に開示又は漏えいしていないことを確認している。	□確認あり □確認なし	
10	取扱者が、在職中又は離職後においても、保護すべき情報を第三者に開示又は漏えいしないよう、措置を講じている。	□措置あり □措置なし	
11	（第三者への開示がある場合） やむを得ず保護すべき情報を第三者に開示しようとする場合には、あらかじめ、書面により甲に申請し承諾を得ている。	※ □承諾あり □承諾なし	※
第５条関係			
12	業務情報及び業務資料について、特に厳重な取扱いを行っている。	□行っている □行っていない	
13	（甲の指定する場所において個別業務を行う場合） 持ち込む物品、業務情報及び業務資料を適正に管理している。	※ □適正 □不適正	※
14	（甲の指定する場所において個別業務を行う場合） 甲の承諾なくして、その場所から物品、業務情報及び業務資料を持ち出していないか確認している。	※ □確認あり □確認なし	※
15	業務情報及び業務資料の管理について、甲の承認を得ている。	□承認あり □承認なし	
16	業務情報及び業務資料について、甲の指定した目的以外に使用しないよう、措置を講じている。	□措置あり □措置なし	
17	業務情報について、甲から廃棄を求められたとき、直ちに甲が認める方法により廃棄している。	※ □実施 □未実施	※

18	業務情報及び業務資料を、甲の承諾なくして、複製・複写していないか確認している。	□確認あり □確認なし	
19	甲から返還を求められた資料を、甲に直ちに返還している。	※ □実施 □未実施	※
第８条関係			
20	（情報システムを使用する場合） 当該情報システムのアクセス権の付与を業務上必要な者に限るとともに、保護すべき情報へのアクセスを記録する措置を講じている。	※ □措置あり □措置なし	※
21	（情報システムを使用する場合） 情報システムに対する不正アクセス、不正プログラム感染等情報システムの脆弱性に係る情報を収集している。	※ □実施 □未実施	※
22	（情報システムを使用する場合） 情報システムに対する不正アクセス、不正プログラム感染等情報システムの脆弱性に対処するための必要な措置を講じている。	※ □措置あり □措置なし	※
第９条関係			
23	（情報セキュリティ対策の履行状況の確認が２回目以降の場合） 前回の確認及び甲に対する報告から、１年以上を経過していない。	※ □１年以内 □１年以上	※
24	報告した確認結果について、甲の承認を得ている。	□承認あり □承認なし	
第12条関係			
25	（情報セキュリティ侵害事案等事故が発生した場合） 事故発生時に適切な措置を講じるとともに、速やかに甲に報告を行った。	※ □実施 □未実施	※
26	（情報セキュリティ侵害事案等事故が発生した場合） 事故の損害・影響等の程度を把握するため、必要な業務資料を保存している。	※ □保存あり □保存なし	※
確認年月日： 確認者（事業者名、所属、役職、氏名）：			

※欄については、該当がある場合に記載する。