

現場技術業務委託共通仕様書 新旧対照表

※赤字下線部：改定箇所

改正後		改正前		備考
<p>現場技術業務委託共通仕様書 (令和8年2月)</p> <p>目次</p>		<p>現場技術業務委託共通仕様書 (令和7年2月)</p> <p>目次</p>		(変更)
第1章	総則	第1章	総則	
第1条	適用	第1条	適用	
第2条	用語の定義	第2条	用語の定義	
第3条	提出書類	第3条	提出書類	
第4条	受発注者の責務	第4条	受発注者の責務	
第5条	設計図書の支給及び点検	第5条	設計図書の支給及び点検	
第6条	業務計画書	第6条	業務計画書	
第7条	業務の着手	第7条	業務の着手	
第8条	監督員	第8条	監督員	
第9条	管理技術者	第9条	管理技術者	
第10条	現場技術員	第10条	現場技術員	
第11条	打合せ等	第11条	打合せ等	
第12条	地元関係者との交渉等	第12条	地元関係者との交渉等	
第13条	土地への立ち入り等	第13条	土地への立ち入り等	
第14条	成果物の提出	第14条	成果物の提出	
第15条	検査	第15条	検査	
第16条	修補	第16条	修補	
第17条	条件変更等	第17条	条件変更等	
第18条	契約変更	第18条	契約変更	
第19条	履行期間の変更	第19条	履行期間の変更	
第20条	一時中止	第20条	一時中止	
第21条	部分使用	第21条	部分使用	
第22条	再委託	第22条	再委託	
第23条	安全等の確保	第23条	安全等の確保	
第24条	守秘義務	第24条	守秘義務	
第25条	機密保持及び個人情報保護	第25条	機密保持及び個人情報保護	
第26条	行政情報流出防止対策の強化	第26条	行政情報流出防止対策の強化	
第27条	暴力団等の契約からの排除	第27条	暴力団等の契約からの排除	(変更)
第28条	暴力団員等による不当介入を受けた場合の措置	第28条	暴力団員等による不当介入を受けた場合の措置	
第2章～第3章	(略)	第2章～第3章	(略)	(略)

改正後	改正前	備考
<p style="text-align: center;"><b>現場技術業務委託共通仕様書</b></p> <p style="text-align: center;">第1章 総 則</p> <p>第1条～第24条 (略)</p> <p>第25条 機密保持及び個人情報保護</p> <p>1. 基本的事項</p> <p>受注者は、機密情報（発注者から提供を受ける技術情報及び行政の運営上の情報等で秘密である旨を示されたもの。）及び個人情報（<u>個人情報</u>の保護に関する法律第2条第1項に規定する個人情報をいう。）（以下「機密情報・個人情報」という。）の保護の重要性を認識し、業務を行うに当たっては、人の生命、身体、財産その他の権利利益を害することのないよう、機密情報・個人情報の取扱いを適正に行わなければならない。</p> <p>2～5 (略)</p> <p>6. 安全管理措置</p> <p>(1) 受注者は、業務を処理するため収集、作成した機密情報・個人情報又は発注者から引き渡された機密情報・個人情報を漏えい、き損及び滅失（以下「漏えい等」という。）することのないよう、機密情報・個人情報の安全な管理に努めなければならない。</p> <p>(2)～(7) (略)</p> <p>(8) 受注者は、機密情報・個人情報を、その秘匿性等その内容に応じて、次の各号に定めるところにより管理しなければならない。</p> <p><u>ア</u> 金庫、保管庫又は施錠若しくは入退室管理の可能な保管室に保管すること。</p> <p><u>イ</u> 電子データとして、保存及び持ち出す場合は、可能な限り暗号化処理又はこれと同等以上の保護措置をとること。</p> <p><u>ウ</u> 業務を処理するために情報システムを使用する場合は、次に掲げる措置を講ずること。</p> <p><u>（ア）</u> 認証機能を設定する等の情報システムへのアクセスを制御するために必要な措置</p> <p><u>（イ）</u> 情報システムへのアクセスの状況を記録し、その記録を1年間以上保存し、及びアクセス記録を定期的に分析するために必要な措置</p> <p><u>（ウ）</u> 情報システムへの不正なアクセスの監視のために必要な措置</p> <p><u>エ</u> 保管・管理するための台帳を整備し、機密情報・個人情報の受け渡し、使用、複写又は複製、保管、持ち出し、廃棄等の取り扱いの状況等を記録すること。</p> <p><u>オ</u> 盗難・漏えい・改ざんを防止する適切な措置を講ずること。</p> <p><u>カ</u> バックアップを定期的に行い、機密情報・個人情報が記載された文書及びそのバックアップに対して定期的に保管状況及びデータ内容の正確性について点検を行うこと。</p>	<p style="text-align: center;"><b>現場技術業務委託共通仕様書</b></p> <p style="text-align: center;">第1章 総 則</p> <p>第1条～第24条 (略)</p> <p>第25条 機密保持及び個人情報保護</p> <p>1. 基本的事項</p> <p>受注者は、機密情報（発注者から提供を受ける技術情報及び行政の運営上の情報等で秘密である旨を示されたもの。）及び個人情報（<u>生存する個人に関する情報であつて、特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより、特定の個人を識別することができることとなるものを含む。）をいう。</u>）（以下「機密情報・個人情報」という。）の保護の重要性を認識し、業務を行うに当たっては、人の生命、身体、財産その他の権利利益を害することのないよう、機密情報・個人情報の取扱いを適正に行わなければならない。</p> <p>2～5 (略)</p> <p>6. 安全管理措置</p> <p>(1) 受注者は、業務を処理するため収集、作成した機密情報・個人情報又は発注者から引き渡された<u>電子媒体に記録された</u>機密情報・個人情報を漏えい、き損及び滅失（以下「漏えい等」という。）することのないよう、機密情報・個人情報の安全な管理に努めなければならない。</p> <p>(2)～(7) (略)</p> <p>(8) 受注者は、機密情報・個人情報を、その秘匿性等その内容に応じて、次の各号に定めるところにより管理しなければならない。</p> <p><u>①</u> 金庫、保管庫又は施錠若しくは入退室管理の可能な保管室に保管すること。</p> <p><u>②</u> 電子データとして、保存及び持ち出す場合は、可能な限り暗号化処理又はこれと同等以上の保護措置をとること。</p> <p><u>③</u> 業務を処理するために情報システムを使用する場合は、次に掲げる措置を講ずること。</p> <p>ア 認証機能を設定する等の情報システムへのアクセスを制御するために必要な措置</p> <p>イ 情報システムへのアクセスの状況を記録し、その記録を1年間以上保存し、及びアクセス記録を定期的に分析するために必要な措置</p> <p>ウ 情報システムへの不正なアクセスの監視のために必要な措置</p> <p><u>④</u> 保管・管理するための台帳を整備し、機密情報・個人情報の受け渡し、使用、複写又は複製、保管、持ち出し、廃棄等の取り扱いの状況等を記録すること。</p> <p><u>⑤</u> 盗難・漏えい・改ざんを防止する適切な措置を講ずること。</p> <p><u>⑥</u> バックアップを定期的に行い、機密情報・個人情報が記載された文書及びそのバックアップに対して定期的に保管状況及びデータ内容の正確性について点検を行うこと。</p>	<p>(略)</p> <p>(変更)</p> <p>(略)</p> <p>(変更)</p> <p>(略)</p> <p>(変更)</p>

現場技術業務委託共通仕様書 新旧対照表

※赤字下線部：改定箇所

del>

改正後	改正前	備考
<p>7～13 (略)</p> <p>14. 対象外</p> <p>(1) 発注者及び受注者は、次の<del>い</del>ずれかに該当する情報は、機密情報として扱わないことを確認する。ただし、機密情報に該当しないことはこれを主張する側において明らかにしなければならないものとする。</p> <p><del>ア</del> 提供時点で既に公知であった情報、又は既に保有していた情報</p> <p><del>イ</del> 提供後、受領者の責めに帰すべからざる事由により公知となった情報</p> <p><del>ウ</del> 正当な権限を有する第三者から適法に入手した情報</p> <p><del>エ</del> 機密情報を利用することなく独自に開発した情報</p> <p><del>オ</del> 保持義務を課すことなく第三者に提供した情報</p> <p>(2) (略)</p> <p>15～16 (略)</p> <p>17. 監査、調査等</p> <p>(1)～(2) (略)</p> <p>(3) 発注者は、<del>次</del>の<del>い</del>ずれかに該当する場合は、<del>実</del>地検査を<del>書</del>面報告に代えることができる。なお、受注者から提出された<del>書</del>面報告の内容に疑義がある場合は、原則として<del>実</del>地検査をするものとする。</p> <p><del>ア</del> 受注者がプライバシーマーク又は ISMS (JISQ27001 (ISO/IEC27001)) の認証を取得している場合</p> <p><del>イ</del> 受注者の作業場所について、セキュリティ対策として<del>受注者</del>の従業員以外の立ち入りを禁止している場合</p> <p><del>ウ</del> 受注者の作業場所が<del>県</del>外等の遠隔地にある場合</p> <p><del>エ</del> 発注者から受注者に提供した個人情報について氏名を番号に置き換える等、容易に照合することができない程度の匿名化処置を講じている場合</p> <p><del>オ</del> 受注者が要配慮個人情報が含まれる個人情報又は特定個人情報を取り扱わず、かつ、取り扱う個人情報の人数が100人未満の場合</p> <p><del>カ</del> 契約期間が1箇月以内、かつ、発注者が<del>実</del>地検査を行うと納期の遅延をもたらすおそれがある場合</p> <p>第26条～第28条 (略)</p> <p>(以下、省略)</p>	<p>7～13 (略)</p> <p>14. 対象外</p> <p>(1) 発注者及び受注者は、次の<del>各</del>号に該当する情報は、機密情報として扱わないことを確認する。ただし、機密情報に該当しないことはこれを主張する側において明らかにしなければならないものとする。</p> <p>①提供時点で既に公知であった情報、又は既に保有していた情報</p> <p>②提供後、受領者の責めに帰すべからざる事由により公知となった情報</p> <p>③正当な権限を有する第三者から適法に入手した情報</p> <p>④機密情報を利用することなく独自に開発した情報</p> <p>⑤保持義務を課すことなく第三者に提供した情報</p> <p>(2) (略)</p> <p>15～16 (略)</p> <p>17. 監査、調査等</p> <p>(1)～(2) (略)</p> <p>(3) 発注者は、<del>以下</del>の<del>各</del>号に該当する場合は、<del>実</del>地検査を<del>書</del>面報告に代えることができる。なお、受注者から提出された<del>書</del>面報告の内容に疑義がある場合は、原則として<del>実</del>地検査をするものとする。</p> <p>①受注者がプライバシーマーク又は ISMS (JISQ27001 (ISO/IEC27001)) の認証を取得している場合</p> <p>②受注者の作業場所について、セキュリティ対策として<del>乙</del>の従業員以外の立ち入りを禁止している場合</p> <p>③受注者の作業場所が<del>県</del>外等の遠隔地にある場合</p> <p>④発注者から受注者に提供した個人情報について氏名を番号に置き換える等、容易に照合することができない程度の匿名化処置を講じている場合</p> <p>⑤受注者が要配慮個人情報が含まれる個人情報又は特定個人情報を取り扱わず、かつ、取り扱う個人情報の人数が100人未満の場合</p> <p>⑥契約期間が1箇月以内、かつ、発注者が<del>実</del>地検査を行うと納期の遅延をもたらすおそれがある場合</p> <p>第26条～第28条 (略)</p> <p>(以下、省略)</p>	<p>(略)</p> <p>(変更)</p> <p>(略)</p> <p>(略)</p> <p>(略)</p> <p>(変更)</p> <p>(略)</p>

現場技術業務委託共通仕様書関連様式 新旧対照表

※赤字下線部：改定箇所

改正前

備考

現場技術業務委託共通仕様書関連様式

様式1～13 (略)

様式14 (共通仕様書第25条17項関係)

機密情報・個人情報を取り扱う委託契約に係る実地検査(書面)報告書

業務名： 委託

点検項目	確認事項	点検結果	点検内容又は「否」の場合の措置内容
1. 機密情報・個人情報の取得、利用			
(ア)機密情報・個人情報の取得の範囲と手段	・取得するときは、利用目的を明示し県の同意を得ているか ・利用目的に必要な範囲内で適法かつ公正な手段で取得しているか	適・否	
(イ)目的外利用及び提供の制限	・県が提供した機密情報・個人情報は、契約の目的のみに利用しているか	適・否	
(ウ)提供した機密情報・個人情報の複写	・県の承諾なしに機密情報・個人情報が記録された資料等を複写していないか	適・否	
2. 機密情報・個人情報の安全管理措置			
(ア)業務を処理する事業所	・県の同意なしに、機密情報・個人情報を事業所内から持ち出していないか ・機密情報・個人情報に関するデータの保管場所を日本国内に限定しているか	適・否	
(イ)機密情報・個人情報を取り扱う場所(作業場所)	・作業場所を特定し、あらかじめ県に届け出ているか ・作業場所を変更するときも同様になされているか	適・否	
(ウ)業務処理のためのパソコン及び電子媒体			
①パソコン等の台帳管理	・パソコン及び電子媒体を台帳で管理し、県が承諾した場合以外は作業場所から持ち出していないか	適・否	
②私用パソコン等の使用禁止	・私用のパソコン等を使用していないか	適・否	
③パソコン等のソフトウェア	・パソコン等に導入されたソフトウェアは脆弱性のないものに更新されているか。また、ファイル交換ソフト等個人情報の漏えいにつながるおそれのあるソフトウェアがインストールされていないか。	適・否	
(エ)機密情報・個人情報の管理等			
①機密情報・個人情報の金庫等での保管	・金庫等又は入退室管理可能な保管室で保管しているか	適・否	
②電子データの保存及び持ち出し	・電子データとして保存及び持ち出す場合、暗号化処理等の保護措置をとっているか	適・否	
③業務処理のための情報システム使用	・業務処理のための情報システムについて、以下の措置が講じられているか。 認証機能によるシステムへのアクセス制御 アクセス状況の記録、保存、分析 不正アクセス監視	適・否	
④保管・管理のための台帳	・保管・管理するための台帳を整備し、機密情報・個人情報の受け渡し、使用、複写、保管、持ち出し、廃棄等の状況が記録されているか	適・否	
⑤盗難等の防止	・盗難、漏えい、改ざんを防止する適切な措置が講じられているか	適・否	
⑥バックアップ	・バックアップが定期的に行われ、機密情報・個人情報が記録された文書及びそのバックアップに対して定期的な点検が行われているか	適・否	
3. 機密情報・個人情報の廃棄及び消去			
(ア)機密情報・個人情報の廃棄・消去	・電子媒体を物理的に破壊する等、判読、復元できないようしているか ・パソコン等にデータ消去用ソフトウェアを使用し、判読、復元できないようしているか	適・否	
(イ)機密情報・個人情報の廃棄証明	・機密情報・個人情報を廃棄又は消去した旨の証明書が提出されているか	適・否	
4. 責任体制の整備			
(ア)業務責任者、業務従事者	・業務責任者及び業務従事者を定め、書面による報告がなされているか ・内部における監督、指示に基づく責任体制が構築されているか	適・否	
(イ)派遣労働者	・業務を派遣労働者に行わせている場合、労働者派遣契約書に所定の事項を記載しているか	適・否	
(ウ)教育の実施	・業務責任者及び業務従事者に対して必要な教育が実施されているか	適・否	
5.再委託の有無	・再委託を禁止している場合、契約に反して再委託が行われていないか(契約書等で再委託を認めている場合は、事前承認が必要であるにもかかわらず、事前承認なく再委託が行われていないか) ・再委託の条件等について契約書、仕様書に記載がある場合、その内容を満たしているか	適・否	

年 月 日  
(発注者又は受注者名)  
(報告書作成者職・氏名)

現場技術業務委託共通仕様書関連様式 新旧対照表

※赤字下線部：改定箇所

改正後

備考

現場技術業務委託共通仕様書関連様式

様式1～13 (略)

(略)

様式14 (共通仕様書第25条17項関係)

(変更)

機密情報・個人情報を取り扱う委託契約に係る 実地 書面 検査報告書

業務名： 委託

点検項目	確認事項	点検結果	点検内容又は「否」の場合の措置内容
1. 機密情報・個人情報の取得、利用			
(ア)機密情報・個人情報の取得の範囲と手段	・取得するときは、利用目的を明示し県の同意を得ているか ・利用目的に必要な範囲内で適法かつ公正な手段で取得しているか	適・否	
(イ)目的外利用及び提供の制限	・県が提供した機密情報・個人情報は、契約の目的のみに利用しているか	適・否・ <u>対象外</u>	
(ウ)提供した機密情報・個人情報の複写	・県の承諾なしに機密情報・個人情報が記録された資料等を複写していないか	適・否・ <u>対象外</u>	
2. 機密情報・個人情報の安全管理措置			
(ア)業務を処理する事業所	・県の同意なしに、機密情報・個人情報を事業所内から持ち出していないか ・機密情報・個人情報に関するデータの保管場所を日本国内に限定しているか	適・否	
(イ)機密情報・個人情報を取り扱う場所(作業場所)	・作業場所を特定し、あらかじめ県に届け出ているか ・作業場所を変更するときも同様になされているか	適・否	
(ウ)業務処理のためのパソコン及び電子媒体			
④パソコン等の台帳管理	・パソコン及び電子媒体を台帳で管理し、県が承諾した場合以外は作業場所から持ち出していないか	適・否	
⑤私用パソコン等の使用禁止	・私用のパソコン等を使用していないか	適・否	
⑥パソコン等のソフトウェア	・パソコン等に導入されたソフトウェアは脆弱性のないものに更新されているか。また、ファイル交換ソフト等機密情報・個人情報の漏えいにつながるおそれのあるソフトウェアがインストールされていないか。	適・否	
(エ)機密情報・個人情報の管理等			
⑦機密情報・個人情報の金庫等での保管	・金庫等又は入退室管理可能な保管室で保管しているか	適・否	
⑧電子データの保存及び持ち出し	・電子データとして保存及び持ち出す場合、暗号化処理等の保護措置をとっているか	適・否	
⑨業務処理のための情報システム使用	・業務処理のための情報システムについて、以下の措置が講じられているか。 認証機能によるシステムへのアクセス制御 アクセス状況の記録、保存、分析 不正アクセス監視	適・否	
⑩保管・管理のための台帳	・保管・管理するための台帳を整備し、機密情報・個人情報の受け渡し、使用、複写、保管、持ち出し、廃棄等の状況が記録されているか	適・否	
⑪盗難等の防止	・盗難、漏えい、改ざんを防止する適切な措置が講じられているか	適・否	
⑫バックアップ	・バックアップが定期的に行われ、機密情報・個人情報が記録された文書及びそのバックアップに対して定期的な点検が行われているか	適・否	
3. 機密情報・個人情報の廃棄及び消去			
(ア)機密情報・個人情報の廃棄・消去	・電子媒体を物理的に破壊する等、判読、復元できないようしているか ・パソコン等にデータ消去用ソフトウェアを使用し、判読、復元できないようしているか	適・否	
(イ)機密情報・個人情報の廃棄証明	・機密情報・個人情報を廃棄又は消去した旨の証明書が提出されているか	適・否	
4. 責任体制の整備			
(ア)業務責任者、業務従事者	・業務責任者及び業務従事者を定め、書面による報告がなされているか ・内部における監督、指示に基づく責任体制が構築されているか	適・否	
(イ)派遣労働者	・業務を派遣労働者に行わせている場合、労働者派遣契約書に所定の事項を記載しているか	適・否・ <u>対象外</u>	
(ウ)教育の実施	・業務責任者及び業務従事者に対して必要な教育が実施されているか	適・否	
5.再委託の有無	・再委託を禁止している場合、契約に反して再委託が行われていないか(契約書等で再委託を認めている場合は、事前承認が必要であるにもかかわらず、事前承認なく再委託が行われていないか) ・再委託の条件等について契約書、仕様書に記載がある場合、その内容を満たしているか	適・否・ <u>対象外</u>	

年 月 日  
(発注者又は受注者名)  
(報告書作成者職・氏名)

(供覧) 調査職員又は監督員(正・副)