令和８年度 障害者委託訓練業務

「知識・技能習得訓練コース（集合訓練)」　仕様書

1 業務の目的

障害のある方の就職を支援するため、障害者の態様に応じた多様な訓練を実施することが目的である。受託者は事業の趣旨を踏まえ、障害者の就職の促進及び雇用の継続を目的として、地域の障害者雇用ニーズに対応した職業訓練を実施し、就職に必要な知識・技能の習得を図ること。

2 業務の内容

（１）訓練の実施

（２）訓練受講生の就職支援及び定着支援

（３）訓練及び就職支援の実施に伴う業務

3 企画提案を募集するコース（プロポーザル企画提案募集）

知識・技能習得訓練コース（集合訓練）

訓練区分	訓練開始月	定員	訓練実施地域	集合訓練	訓練時間
自由提案コース１	10 月～12 月	10 名以内	広島市	３か月	標準：１００時間／月 下限：８０時間／月 訓練開始時間は午前９時以降を目安とする。

※ 訓練時間には、入校式と修了式、職業能力講座の時間数は含めない。

4 訓練開始月

広島障害者職業能力開発校と協議の上、決定する。

5 訓練対象者

ハローワークの求職登録者で、精神障害（高次脳機能障害・発達障害を含む）や身体障害・知的障害・特定疾患があり、受講あっせんを受けた方。

6 委託費の上限額

区 分	１人１月あたりの上限額(税込)
委託訓練費（集合訓練）	７０，４００円

※中途退所等により、委託費が減額される場合がある。

7 就職支援経費

就職支援の実施に係る経費相当額として、就職者１人あたり２２，０００円(税込)を訓練月数に応じて支給する。

※就職支援経費の対象となる就職者は、修了者または中退者のうち訓練修了後３か月以内に雇用保険の被保険者（障害者の日常生活及び社会生活を総合的に支援するための法律における障害福祉サービス（就労継続支援事業Ａ型等）により雇用される被保険者及び日雇労働被保険者は除く。）として雇用された者である。

8 職業能力講座委託費の上限額

区 分	１人１日あたりの上限額(税込)	上限額(税込)
職業能力講座	２，２００円	８，８００円（４日間分）

※中途退所等により、委託費が減額される場合がある。

9 訓練内容

自由提案コースは、提案したコースで想定している職種で働くために必要となるスキルを習得することによって就職の促進を目指す訓練内容とする。

なお、過去２年間（令和５年４月１日から令和７年３月 31 日の間に実施･終了したもの）に、当校の障害者委託訓練を実施した機関においては、就職率の平均値が 30%を下回っている場合は、同内容での提案は認めない。受託希望機関は、より効果的な訓練が実施されるよう、訓練内容の見直しを行った上で提案を行うものとする。

（１）職業能力講座

４日間の基礎的なビジネスマナー等を内容とする講座を実施することができる。

ア 主な内容

働くことの意義や目的の理解、基礎的なビジネスマナー等の習得が不十分であるために、直ちに就職することが困難な状態である受講生を想定し、基礎的なビジネスマナー等を内容とする。

イ 職業能力講座の期間等について

職業能力講座の時間は１２時間以上、日数は４日間とする。この日数が４日間を超える場合でも、委託費の支給は４日間分とする。

なお、集合訓練又は職場実習と同日に行うことはできないものとする。

（２）集合訓練

座学及び実技による訓練を実施するものとし、個々の障害特性及び地域の企業ニーズに即した効果的な訓練内容とする。

なお、職業能力講座又は職場実習と同日には行うことはできないものとする。

10 訓練スケジュール

（１）月数の設定及び月の下限時間

ア 月数の単位

１か月の単位は訓練開始日を起算日とし、翌月の起算日と同日の前日までとする。ただし、最終月については、前日よりも前に訓練を終了する日程も認める。

なお、翌月に起算日の前日が暦上ない場合その月は、前々日とし、前々日がない場合は

前々々日とする。

イ 訓練時間の下限時間

訓練時間は１か月８０時間を下限とし、これを下回るカリキュラムは認めない。

また、職業能力講座は、集合訓練と分けて設定するため、職業能力講座を含めて８０時間となるカリキュラムは認めない。

（２）訓練時間の設定（標準）

週５日、１日あたり５時間の訓練カリキュラムを標準とするが、訓練受講生の障害の態様や訓練内容によっては変更することができる。

※ １単位時間を４５分以上６０分未満とする場合は、１単位時間を１時間とみなす。

（３）入校式及び修了式

訓練開始日と最終日に実施すること。（ただし、訓練時間数には含まない。）

（４）就職活動日

原則、訓練期間中に１回以上（可能であれば、月に１回以上）設定すること。ただし、土・日・祝日に設定することは不可とする。ハローワークにおける職業相談や就職試験の受験日として設定するよう周知すること。

なお、就職活動日は訓練受講生の自主的な就職活動の実施を目的とするため、訓練時間に含まない。

（５）適宜、就職相談等を実施し、訓練修了後の早期就職に向けた支援を行うこと。

11 訓練の実施

（１）提案書類の内容をもとにして契約締結した内容を誠実に実施すること。

（２）募集締切日翌日時点で受講申込者が最少開講人数以上の場合は、必ず訓練を実施すること。

※ 選考後に受講申し込みの辞退等があり、最少開講人数を下回った場合でも訓練を実施すること。

（３）受講申込者が最少開講人数を下回った場合は、訓練実施について広島障害者職業能力開発校と協議を行い、訓練の実施（又は中止）を決定すること。

※ 訓練の実施を決定した場合は、いかなる場合においても訓練を実施すること。

（４）訓練の実施にあっては、施設、設備関係等の基準を次のとおりとすること。

ア 施設

・教室の面積は、受講者１人当たり 1.65 ㎡以上とする。
・交通手段又は駐車場が確保されていること。
・教室、実習場、昼食・休憩場所、その他訓練環境が確保されていること。

イ 設備

・訓練実施に必要な機器があること。
・教室には、訓練に必要な机、椅子、訓練用提示機材（ホワイトボード等）が整備されていること。
・実技を行う場所には、訓練を適切かつ効果的かつ安全に実施できる設備、機器、器具等が必要数整備されていること。
・パソコンを使用する訓練においては、パソコンは１人１台で、十分な性能を有していること。
・情報機器を使った作業を行う場合は、「情報機器作業における労働衛生管理のためのガ

イドライン」に準じること。

ウ 訓練

・講師は、訓練関連の有資格者又は、実務経験、指導経験を有する者であること。
・訓練生が欠席した場合、可能な範囲で若干の補講の実施に努めること。
・訓練開始日の約２週間後及び最終日の約１か月前に、訓練生と委託先職員、当校職員で個別面談を実施する。なお、個別面談は訓練時間内で実施することとし、時間割等、訓練カリキュラムに組み込むこと。
・聴覚障害者が入校した場合は、可能な範囲で手話通訳、要約筆記、筆談等の対応に努めること。

12 訓練及び就職支援の実施に伴う業務

障害者委託訓練事務処理マニュアルに基づき、次の業務を実施すること。

（１）募集要項の作成（配布資料により作成～完成まで及び印刷）

（２）訓練生の募集・広報

訓練受講希望者及び受講申込者からの訓練内容や施設・設備等に関する問合せ、施設見学要望等については、適切かつ真摯に対応すること。

（３）入校式、修了式の開催

（４）訓練に係る雇用保険の事務手続き

（５）求職者支援制度等の事務手続き

（６）訓練生の出欠席の管理、指導及び報告

（７）訓練生の訓練生活指導及び報告

（８）訓練実施状況の把握及び報告

（９）訓練生の能力習得状況の把握及び報告

(10) 訓練生へのアンケート調査の実施、改善対策及び報告

(11) 災害発生時の対応及び連絡

(12) 訓練生の中途退校に係る事務処理

(13) 各種資格試験に係ること

(14) 訓練生の就職支援、定着支援

職務経歴書・履歴書の作成指導、面接指導、キャリア・コンサルティング、職業相談、求人開拓、求人情報の提供等、就職に関する状況把握や就職率向上のための分析等を行うこと。また、定着支援のため、各種支援機関と密に連携を図ること。

(15) 個人情報の管理

別紙「委託先事業者向け個人情報の漏えい等に係る対応・対策ガイド」、「機密情報取扱特記事項」、「情報セキュリティに関する特記事項」及び「受託者向け情報セキュリティ遵守事項」に基づき、訓練生募集の段階から業務完了まで、適切に個人情報を管理すること。

(16) その他、協議の上、必要と認める業務

(17) 本仕様書に定めのないものについては、広島障害者職業能力開発校の指示に従うこと。

別紙

委託先事業者向け個人情報の漏えい等に係る対応・対策ガイド

第一部　個人情報の漏えい・紛失の事案発生時の対応

個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「法」という。）第 66 条第２項の規定により、行政機関等から委託を受けた者及び指定管理者について、行政機関等と同じ安全管理措置が求められるとともに、個人情報保護委員会規則で定められた漏えい等が発生した場合には、行政機関等を通じて個人情報保護委員会に報告する必要があります。

漏えい等が発生した場合又は発生した可能性がある場合には、直ちに委託契約等を行った行政機関等の担当課に報告を行ってください。

１　速やかな報告

次のような場面に遭遇したら、直ちに報告してください。

□ 個人情報を含む書類や記憶媒体、ＰＣ等の紛失・盗難が発覚
□ 個人情報を保管していたキャビネットの鍵、入館証等の紛失・盗難が発覚
□ 別人宛ての個人情報をメールやＦＡＸで誤送信、誤発送
□ 情報システムの設定ミス等によりインターネット上で保有個人情報の閲覧が可能な状態となっていた場合
□ 個人情報が記録された帳票等を誤って廃棄した場合
□ 暗号化処理された個人情報の復元キーを喪失したことにより復元できなくなった場合
□ 不正アクセス・不正持ち出しの形跡を発見
□ ランサムウェア等により保有個人情報が暗号化され、復元できなくなった場合
□ サイバー攻撃を受け、何らかの漏えい等が発生したおそれがある場合
□ 県民、報道機関、警察等から情報漏えい等に関する苦情や問合せ
□ インターネット掲示板等で個人情報の漏えい等に関する書込みを発見
□ 再委託先等の関係業者から上記について通報

※　上記以外にも、個人情報の漏えいのおそれがある事態に遭遇した場合には、できるだけ早く委託契約等を行った行政機関等の担当課に連絡してください。

２　被害拡大防止措置

事実関係の調査・確認を行い、事案の性質に即した、適切な被害拡大防止措置を講じてください。

区分	応急措置例	二次被害防止策例
紛失・盗難	○ 紛失物の捜索、回収 ○ 警察への届出 ○ 流出したアカウントの	○(口座番号、ＩＤパスワード等が含まれていた場合) 本人に通知し、口座停止、ＩＤ停止などを促す。

	停止、パスワード変更	
誤送信・ＨＰでの誤公開	○ 受信者への連絡と情報の削除依頼 ○ 誤ってＨＰに公開した情報の削除	○(口座番号、ＩＤパスワード等が含まれていた場合) 本人に通知し、口座停止、ＩＤ停止などを促す。 ○ ＷＥＢ検索サイトからのキャッシュ削除 ○ ＷＥＢサイトの停止
不正プログラム(ウイルス、スパイウェア等)	○ ウイルス感染したパソコンの特定 ○ ウイルス感染したパソコンのネットワークからの切り離し	○(口座番号、ＩＤパスワード等が含まれていた場合) 本人に通知し、口座停止、ＩＤ停止などを促す。 ○ ウイルス名の特定と駆除 ○ 漏えいした情報の回収

第二部　個人情報の漏えい・紛失防止策

取扱う個人情報の秘匿性等その内容に応じて、次の事例を参考に、個人情報の漏えい・紛失防止のための対策を講じてください。

1　送付・交付・送信の際の漏えい

文書等を郵送したり、窓口で交付したり、メールで送信したりした際に、他人の個人情報が目に触れる状態になることにより、個人情報が漏えいするケースがあります。

(1) 紙文書の送付・交付

紙文書の送付や交付に伴って漏えい等が発生するものとしては、次の類型があります。

ア【記載内容の誤り】

そもそも送付・交付した文書自体に誤りやミスがあり、そこに記載された他人の個人情報が漏えいするケース。

No.	事　　例
1	以前作成したA宛ての文章を上書きして、新たにB宛ての文章を作成し、Bに送付したところ、文章の中にAの氏名の記載が残っていた。
2	表面と裏面でそれぞれ異なる個人の個人情報を記載したデータを印刷し、そのまま配布した。
3	個人データを記載した用紙の裏紙を利用して、資料等を印刷し、第三者にそのまま配布してしまった。

《防止策》

□ 個人情報を含む文章の内容は、複数人で「読み合わせ」をして確認する。

□ 既存のファイルの上書きではなく、差込印刷機能を使用して作成する。(事例１)

イ【誤封入】

個人情報を含む文書の封入を誤り、他人に送付してしまうケース。

No.	事　　例
4	封筒の取違いにより、A宛ての封筒の中にB宛ての書類を封入して郵送してしまい、Bの個人情報が漏えいしてしまった。
5	A宛ての書類の封入作業中に、Bの個人情報が記載された書類が紛れ込むことにより、Bの個人情報が漏えいしてしまった。

《防止策》

□ 大量の個人情報の封入作業は、個人の作業机とは別の場所で行う。

□ 封入作業スペースの周辺を整理整頓する。

□ 書類を封入する作業と、封かんする作業は別工程の作業として実施し、それぞれが確認する。

□ 少数分の書類の封入・封かん作業でも、二人で確認を行う。やむを得ず一人で作業を行う場合には、書類の封入時には、「声出し」「指さし確認」を行う。

□ 書類作成時にプリンタやコピー機など、複数人が扱う機器を利用する場合、他の書類の紛れ込みがないことを確認する。（事例５）

□ 封入前に、封筒と内容物の数を合わせておき、封入後に封筒と内容物の残数が一致するかを確認する。（事例５）

この種の事案を防止するには、担当者個人が注意するだけではなく、組織的に事務処理の流れの中に個人情報の確認を組み込む必要があります。ダブルチェックがシステム的に行われるように、事務処理の分析及びマニュアルの見直しを検討してください。

ウ【誤交付】

窓口等で、他人の個人情報を含む文書を渡したケース。

No.	事　　例
6	窓口でAに対して、同姓同名であるBの名前が記載された文書を渡した。
7	他人の書類が混入したまま交付してしまい、個人情報が漏えいしてしまった。

《防止策》（イ【誤封入】も参照）

□ 交付書類を作成する際は、他者の書類が混在しないように分けて保管する。

□ 利用者と対面するスペースを整理整頓する。

□ 交付時には、名前や写真など本人が確認できるものの提示を受けた上で交付を行う。

□ 交付書類の種類、枚数を確認してから交付する。

□ 同姓同名の者がいることを前提とした書類作成・交付時の本人確認手順（氏名に加え、生年月日や住所等も確認する等）を実施する。

エ【送付過程での書類紛失】

個人情報を含む文書が、送付中に封筒ごと行方不明になったケース。

No.	事　　例
8	相手方に関係書類を送付し、意見書とともに返送するよう依頼していたが、返送

	期限までに届かなかったので問い合わせたところ、返送したと言われた。
9	個人情報が含まれた書類をＡ社に送付したところ、Ａ社は受け取っていないと言っている。
10	同じ会社内の部署間で書類をやり取りする過程で所在不明となった。

《防止策》

□ 個人情報の含まれる書類を郵送する際に、可能な場合には、簡易書留、特定記録等の普通郵便とは別の方法を利用する。

□ 送付する際には、送付先に電話等により一報する。また、必要に応じ、届いた時には送付先から連絡をもらうようにする。

□ 封筒に赤字で「○○関係書類在中」などと記載し、注意喚起する。

□ 可能な限り、郵送による送付・回収から、直接手渡しによる依頼・回収に変更する。また、送付確認簿を作成し、受領印の押印を受け、受け渡しについて双方確認できるようにする。（事例８）

□ なるべく相手方に届きやすい日時に到達するように発送する。

※ 事例９が発生したケースでは、土曜日に相手方に到達したと考えられるため、休み中に相手方に届かないように金曜日の発送を避けているという。

(2) 電子メール送信、ＨＰ掲載

電子メールやＨＰ掲載に伴って漏えい等が発生するものとしては、次の類型があります。

ア【送信先・送信方法の誤り】

メール送付の際に、送信先・送信方法を誤って送信してしまうケース。

No.	事　　例
11	メールを多人数に一斉送信する際に、メールアドレスを「宛先」又は「ＣＣ」で送ったため、受信者に全員のメールアドレスが丸見えになった。
12	個人情報ファイルを含むメールをＡ送信しようとしたところ、誤ってＢへ送付してしまった。

メールアドレスを「宛先」又は「ＣＣ」で送れば、受信者は同時に送信した全員のメールアドレスが見える形で送付されます。個人が識別できる（誰のものか分かる）メールアドレスは個人情報のため、「宛先」又は「ＣＣ」で一斉送信した時点で個人情報の漏えいとなります。

また、メールマガジンの登録者に一斉送信した場合には、誰がメールマガジンに登録されているかという個人情報も漏えいしたことになります。

《防止策》

□ 外部の複数の者に電子メールを送信する際には、内容や送信先に応じて「宛先」「ＣＣ」「ＢＣＣ」を適切に選択する。送信先が知らない者同士であれば、必ず「ＢＣＣ」で送付する。（多数宛に送信する際は、２人で確認する。）

□ 電子メール送信前に、宛先（To、CC、BCC）、件名、添付ファイル、コメントを「声出し」、「指差し」等で確認することも有効。

□ 一斉送信時には、メーリングリストを活用し、個別のアドレスは使用しない。

□ メール送信先が正しいか、送信前に再度確認する。

イ【添付ファイル・ＨＰ掲載情報の誤り】

メールに添付したファイルやHPに公開したファイルが誤っているケース。

No.	事　　例
13	メールに参考資料Ａを添付して送付しようとして、誤って名簿Ｂを添付して送付してしまった。
14	行事の参加申込書の様式をＨＰに掲載したところ、掲載したファイルの別シートに前年度の参加者名簿が載っていた。
15	団体の実態調査の結果をＨＰに掲載したが、誤って団体の代表者の氏名、住所、電話番号を掲載した。

《防止策》

□ 誤ったファイルを添付してメールすることを防止するため、添付したファイルを送信前に一度開いて確認する。

□ 紛らわしいファイル名を付けない、送付用のファイルは別ホルダーで保存するなどして、間違えにくいファイル管理をする。

□ 添付ファイルが誤りでなくても、重要な個人情報や機密情報が含まれる場合には、誤送信等に備えて、ファイルにパスワードを設定する。

(3) ＦＡＸ送信

ＦＡＸ送信に伴って漏えい等が発生するケース。

No.	事　　例
16	ＦＡＸ番号を手打ちした際に、打ち込んだ数字を１つ誤り、全く知らない番号に送信してしまった。
17	特定の団体にＦＡＸで書類を送信する際、誤って多くの団体に一斉送信した。
18	Ａ宛てのＦＡＸ送信の書類の中に、Ｂに関する個人情報が含まれる書類が混ざったまま、Ａに書類を送信した。

《防止策》（(1)イ【誤封入】も参照）

□ 送信する書類の誤りや誤混入を防止するため、送付票に枚数を記載する際に、改めて送信する書類に誤りがないか、他の書類が混入していないかを確認する。

□ ＦＡＸを送信する際、他の書類が混入していないことを確認する。

□ ＦＡＸを送信する前に、ＦＡＸ番号が正しいか再確認する。

□ 定型的なＦＡＸ送信の際は、短縮ダイヤルを利用する。

□ ＦＡＸ送信時には二人で宛先を確認する。

□ ＦＡＸ送信後、送信記録の確認や電話等で受信確認を行うことも併せて実施する。

※最新のＦＡＸ機器では、誤ダイヤルを防ぐための機能（送信先を２回ダイヤルしないとＦＡＸ送信されない設定等）を備えているものがあり、そうした機能がある場合には、積極的に活用してください。

２　利用・保管に関する漏えい

個人情報へのアクセス、持ち出し、出力、複製等に伴って漏えい等が発生するものとしては、次の類型があります。

(1) 持ち出し時の紛失・盗難

個人情報が含まれる書面や電磁的媒体を持ち出した際に、紛失や盗難にあうケース。

No.	事　　例
19	個人情報が含まれる資料を持ち帰って帰宅後に残業を行う予定だったが、途中で立ち寄った店の駐車場で、車から盗まれた。
20	委託業務に関して、個人の風貌がわかる形で動画・写真を撮影したビデオカメラを新幹線での移動中に紛失した。
21	道路を歩いていたところ、個人情報が入ったカバンを背後から盗まれた。 自宅駐車場に停めた自家用車に仕事用のカバンを乗せたまま施錠していたが、ガラスを割られ、個人情報が入ったカバンを盗まれた。
22	個人情報が書かれたメモ等の入ったバッグを外出中に紛失した。

《防止策》

□ 個人情報が記載された書面や電磁的媒体の持ち出しは原則禁止とし、やむを得ず持ち出す場合には、管理者の許可を得る。（できれば台帳に持ち出し・返却を記録する。）

□ 紛失・盗難に備えて、持ち出す個人情報は小分けにして、最小限のものとする。

□ 重要な個人情報を持ち出した際には、必要な場所にしか立ち寄らない。

□ 外部での検討などの目的で個人情報を含む資料を持ち出す場合は、匿名化等、個人が識別できないような措置を講じる。

□ 外出先では、個人情報や重要な情報が入ったカバン等は常時携帯する。

(2) 施設内での紛失・盗難・誤廃棄

施設内での管理が不十分であるために紛失・盗難・誤廃棄が発生するケース。

No.	事　　例
23	社内で保管していたはずの個人情報を含む書類が所在不明となった。
24	社内で受付担当課から事務担当課に交付した後、所在不明となった。
25	部屋の施錠・鍵の管理等が不十分で、個人情報が含まれるパソコンが盗難に遭った。
26	個人情報を含む書類を保存年限満了前に廃棄した。

《防止策》

□ 個人情報を含む書類等を扱う作業を行う場合には、他の書類との混入がないよう、机上を整理する。

□ 個人情報を含む書類を保管する際は、正しい保管場所（例えば、重要な個人情報は施錠可能な書庫に保管する等）であることを十分に確認する。

□ 個人情報の利用後は、速やかに所定の保管場所に戻すようにする。

□ 書類を保管する際には、保存期間が明確に分かるようにする。

□ 個人情報にアクセス可能なパソコンがある執務室に部外者を立ち入らせないようにする。

□ 個人情報の入ったファイル等を机の上に放置したまま離席あるいは帰宅しない。
□ 離れた場所にあるプリンタに出力した書類はすぐに取りに行く。
□ 起動中のパソコンを他の人が利用できる状態で長時間離席しない（パスワードによりロックする。）
※〔パソコンのロックの仕方〕
「Ctrl＋Alt＋Delete」、「Windows キー＋Ｌ」
□ 紛失等を防止するため、原則、原本により作業することとし、コピーやメモを作成しない。

３　不完全な方法による廃棄処理

個人情報の含まれる書類又は電磁的記録媒体の廃棄に伴って生じた個人情報の漏えいとしては、次のケースがあります。

No.	事　　例
27	個人情報が記載された廃棄対象の文書等が路上で見つかり、警察署から拾得物として届けられているとの連絡があった。
28	電磁的媒体を破棄する際に、単純に中のデータを削除しただけで、そのまま廃棄したが、電磁的媒体が転売され、データ復元されたことにより個人情報が流出した。

《防止策》
□ 複数の書面や電磁的媒体を廃棄する際には、すべてが廃棄対象であることを再確認する。
□ 個人情報を含む紙文書の廃棄は、シュレッダーによる裁断処理や業者による溶解処理等の方法によって、確実に処理する。
□ 個人情報を記載した電磁的媒体を廃棄する際には、専用の消去ソフトを使用するか、物理的に破壊する。
□ 廃棄業者を利用する際には、コストだけではなく、情報の管理体制や実績等を踏まえ、信頼のおける業者を選ぶ。
□ 廃棄した記録を台帳等に残す。

４　その他

その他、思わぬところから個人情報が漏えいすることも考えられるので、勤務時間内外を問わず、十分な注意をしてください。

No.	事　　例
29	特定の疾病に関する情報を行う業務で、知人の申請があることを発見し、その内容を家庭内でうっかり口にしてしまったため、家族が悪気なく関係者にお見舞いの意を伝えて、漏えいが発覚した。
30	同僚同士で昼食を食べている際に、個人情報を含む業務の話題を話してしまい、周辺に居た第三者が SNS に投稿して、漏えいが発覚した。
31	仕事風景を SNS に写真で投稿し、写り込んだ書類に個人情報が記載されていたため、漏えいした。
32	担当者の本名で登録している SNS で、相手方の実名を伏せて業務に関する話を発信したが、担当者や発信した内容を元に、容易に相手方が特定できてしまい、個

	人情報の漏えいとなった。

《防止策》

□ 公共交通機関、エレベータ、食堂、飲食店、家庭内などで、職務上知り得た個人情報に関する会話は慎む。（携帯電話の使用も要注意）

□ 電車（新幹線）等の中で個人情報を扱う仕事をしたり、資料の予習、復習をしたりして、個人情報が他人の目に触れるおそれのあることはしない。

□ 業務に関係のない SNS や掲示板に、仕事中の写真や仕事に関する話をアップしない。

機 密 情 報 取 扱 特 記 事 項

第１章　基本的事項

（機密情報）

第１　受注者は、この契約による業務（以下「業務」という。）を行うに当たっては、提供方法及び媒体を問わず、本件業務を行うために発注者から提供を受け、又は受注者自らが取得若しくは作成した情報（公になっている情報及び本契約後に公になった情報を除く。以下「機密情報」という。）を適正に取り扱わなければならない。

（秘密の保持）

第２　受注者は、業務に関して知り得た機密情報の内容をみだりに他人に知らせ、又は不当な目的に使用してはならない。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。

（目的外利用・提供の禁止）

第３　受注者は、機密情報を本件業務の履行のために必要な範囲において利用できるものとし、発注者の指示又は承諾があるときを除き、利用目的以外の目的に利用し、又は第三者に提供してはならない。

（複製又は加工）

第４　受注者は、発注者が禁止している場合を除き、本件業務の履行のために必要な範囲において機密情報を複製又は加工することができるものとし、複製又は加工により生じた情報についても本契約に基づく機密情報として取り扱うものとする。

（安全管理措置）

第５　受注者は、機密情報の漏えい、滅失又は毀損（以下「漏えい等」という。）の防止その他の安全管理のために必要かつ適切な措置（以下「安全管理措置」という。）を講じなければならない。

（従事者への周知及び監督）

第６　受注者は、業務に従事している者（正社員のほか、派遣労働者（労働者派遣事業の適正な運営の確保及び派遣労働者の保護等に関する法律（昭和60年法律第88号）第２条第２号に規定する派遣労働者をいう。以下同じ。）、契約社員その他の正社員以外の労働者を含む。以下「従事者」という。）に対し、在職中及び退職後において、機密情報の内容をみだりに他人に知らせ、又は不当な目的に使用してはならないことを周知するとともに、業務を処理するために取り扱う機密情報の安全管理が図られるよう、従事者に対して必要かつ適切な監督を行わなければならない。

（教育の実施）

第７　受注者は、機密情報の情報セキュリティに対する意識の向上及び漏えい等の防止のため、従事者に対し適切な教育及び研修を行わなければならない。

（機密情報の持ち出しの禁止）

第８　受注者は、発注者の指示又は承諾を得た場合を除き、機密情報が記録された資料等をこの契約に定める実施場所その他発注者が定める場所の外に持ち出してはならない。

（再委託等に当たっての留意事項）

第９　受注者は、発注者の書面による承諾を得て業務の全部又は一部を第三者に委託（二以上の段階にわたる委託をする場合及び受注者の子会社（会社法（平成17年法律第86号）第２条第３

号に規定する子会社をいう。）に委託をする場合を含む。以下「再委託等」という。）する場合には、再委託等の相手方に対し、発注者及び受注者と同様の安全管理措置を講じなければならないことを周知するとともに、この契約に基づく機密情報の取扱いに関する一切の義務を遵守させるものとする。

（再委託等に係る連帯責任）

第10　受注者は、再委託等の相手方の行為について、再委託等の相手方と連帯してその責任を負うものとする。

（再委託等の相手方に対する管理及び監督）

第11　受注者は、再委託等をする場合には、再委託する業務における機密情報の適正な取扱いを確保するため、再委託等の相手方に対し適切な管理及び監督をするとともに、発注者から求められたときは、その管理及び監督の状況を報告しなければならない。

（機密情報の返還、消去又は廃棄）

第12　受注者は、機密情報及び機密情報が記録された媒体等について、業務完了後、発注者の指定した方法により、直ちに返還、消去又は廃棄しなければならない。また、発注者から求められた場合にはその状況を報告しなければならない。

（取扱状況の報告及び調査）

第13　発注者は、必要があると認めるときは、受注者に対して、業務を処理するために取り扱う機密情報の取扱状況を報告させ、又は調査を行うことができる。また、機密情報の適切な管理を確保するため必要と認められる場合には、受注者に対し必要な指示を行うことができる。

（漏えい等の発生時における報告）

第14　受注者は、業務に関し機密情報の漏えい等若しくは機密情報の安全の確保に係る事態が発生し、又は発生したおそれがあること（再委託等の相手方により発生し、又は発生したおそれがある場合を含む。）を知ったときは、直ちに発注者に報告し、発注者の指示に従わなければならない。

（契約解除）

第15　発注者は、受注者が本特記事項に定める義務を履行しない場合又は法令に違反した場合には、この契約を解除することができる。

（損害賠償）

第16　受注者が本特記事項に違反したことにより発注者又は第三者に損害を及ぼした場合には、発注者が必要と認める措置を直ちに講ずるとともに、発注者又は第三者に対して生じた損害を賠償するものとする。

（存続期間）

第17　本特記事項の効力は本件業務に係る契約期間の満了まで有効とする。ただし、第２（秘密の保持）、第12（機密情報の返還、消去又は廃棄）、第14（漏えい等の発生時における報告）及び第16（損害賠償）の規定については、契約期間の満了後も有効に存続するものとする。

（協議事項）

第18　本特記事項に定めのない事項に関しては、別途発注者と誠実に協議の上、円満な解決を図るものとする。

第２章　個人情報の取扱いに係る特約

（趣旨）

第１　受注者は、業務を行うために発注者から提供を受け、又は受注者自らが取得又は作成した機密情報について、個人情報の保護に関する法律（平成15年法律第57号。以下「個人情報保護法」という。）第２条第１項に規定する個人情報が含まれる場合には、個人情報保護法に基づき個人情報を取り扱うとともに、本特記事項第１章の規定に加えて、本章の規定を遵守しなければならない。

（個人情報の取扱い）

第２　受注者は、業務を行うに当たっては、個人情報保護法に基づき、個人の権利利益を侵害することのないよう個人情報を適正に取り扱わなければならない。

（取得の制限）

第３　受注者は、業務を行うに当たって個人情報を取得する場合には、業務を遂行するために必要な範囲として発注者が指定した範囲を超えて、個人情報の取得及び保有を行ってはならない。

（利用目的の明示）

第４　受注者は、業務を行うに当たって本人から直接書面（電磁的記録を含む。）に記録された当該本人の個人情報を取得するときは、発注者の指示に従い、個人情報保護法第62条に規定する利用目的の明示等の必要な措置を行うものとする。

（安全管理措置）

第５　受注者は、個人情報保護法第66条第２項の規定に従い、個人情報の漏えい、滅失又は毀損の防止その他の保有個人情報の安全管理のために必要かつ適切な措置を講じなければならない。

（教育の実施）

第６　受注者は、個人情報取扱作業責任者及び従事者に対して、個人情報の保護及び個人情報取扱業務の適切な遂行のために必要な教育及び研修を実施しなければならない。

（再委託等）

第７　受注者は、発注者の書面による承諾を得て再委託等を行う場合には、再委託等の相手方に対し、本章の規定に基づく個人情報の取扱いに関する一切の義務を遵守させるものとし、再委託等の相手方の行為について、再委託等の相手方と連帯してその責任を負うものとする。

情報セキュリティに関する特記事項

（総則）

第１　この特記事項は、受注者が業務を行うに当たって、機密情報取扱特記事項第１章第１に規定する「機密情報」が含まれた電磁的記録を取り扱う場合の特則を定めるものであり、受注者は、機密情報取扱特記事項と合わせて本特記事項を遵守しなければならない。

（基本的事項）

第２　受注者は、業務を行うに当たっては、別紙「受託者向け情報セキュリティ遵守事項」に基づき、情報を適正に取り扱わなければならない。

（安全管理措置）

第３　受注者は、機密情報を含む電磁的記録（以下「機密データ」という。）の取扱いに当たっては、機密データの漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等の防止のために、必要かつ適正な管理（以下「安全管理措置」という。）を行うものとする。

（作成、複製又は加工）

第４　受注者が、機密データを作成、複製又は加工（以下「作成等」という。）しようとする場合には、本件業務の履行のために必要な範囲において行うものとし、作成等の途上で生成される情報についても、第３と同等の安全管理措置を講じなければならない。また、作成等の途上で不要となった情報については、随時消去するものとする。

（機密データの保存等に係る届出）

第５　受注者はあらかじめ、業務の遂行において取り扱う機密データの保存先等の情報（オンラインストレージ等のクラウドサービスを使用している場合に当たっては、利用契約先の情報等を含む。）を別記様式により発注者に届け出るとともに、内容に変更が生じた場合には、速やかに再度の届出を行うものとする。

（機密データの持出等の禁止）

第６　受注者は、あらかじめ発注者の承認を得た場合を除き、機密データの社外への持出及び第５により届出を行っていないオンラインストレージ等のクラウドサービス上に保存する行為を行ってはならない。

（目的外利用・提供の禁止）

第７　受注者は、機密データの業務遂行の目的以外の目的による利用及び第三者（会社法（平成17年法律第 86 号）第２条第３号の２に規定する子会社等及び同条第４号の２に規定する親会社等を含む。）への提供を行ってはならない。

（生成ＡＩの利用）

第８　受注者は、本契約に基づく業務遂行のため、生成ＡＩ（文章、画像、プログラム等を生成できるＡＩモデルをいう。以下同じ。）又は生成ＡＩを利用したサービス（以下「生成ＡＩ等」という。）において機密データを取り扱う場合には、次の事項を遵守しなければならない。

１　受注者は、本業務に関して入力した内容が生成ＡＩ等の学習に利用されない生成ＡＩ等を使用すること。

２　生成ＡＩ等を利用して作成した納品成果物については、生成ＡＩ等を利用している旨を発注者に明示して納品すること。

３　利用する生成ＡＩ等に関する情報をあらかじめ別記様式により発注者に届け出るとともに、内

容に変更が生じた場合には、速やかに再度の届出を行うこと。

（教育の実施）

第９　受注者は、機密データを取り扱う従事者に対し、別紙「受託者向け情報セキュリティ遵守事項」を理解し、実践するために必要な情報セキュリティに係る教育及び訓練を実施するものとする。

（再委託等に当たっての留意事項）

第 10　受注者は、発注者の書面による承諾を得て業務の全部又は一部を第三者に委託（二以上の段階にわたる委託をする場合及び受注者の子会社（会社法第２条第３号に規定する子会社をいう。）に委託をする場合を含む。以下「再委託等」という。）する場合には、再委託等の相手方にこの特記事項及び別紙「受託者向け情報セキュリティ遵守事項」を遵守させなければならない。

（再委託等に係る連帯責任）

第 11　受注者は、再委託等の相手方の行為について、再委託等の相手方と連帯してその責任を負うものとする。

（機密データの返還等）

第 12　受注者は、本契約による業務を遂行するために利用又は作成した機密データについて、業務完了後直ちに、返還又は消去を行うものとする。ただし、発注者が別に指示したときは当該方法によるものとする。

（再委託等の相手方からの回収等）

第 13　受注者が発注者の承認を得て再委託等の相手方に機密データを提供した場合において、受注者は、業務終了後直ちに再委託等の相手方から機密データを回収し、又は再委託等の相手方に消去させるものとする。ただし、発注者が別に指示したときは当該方法によるものとする。

（報告等）

第 14　報告等については、次のとおりとする。

１　発注者は、必要があると認めるときは、受注者又は再委託等の相手方に対して、この特記事項の遵守状況その他のセキュリティ対策の状況について、定期的又は随時に報告を求めることができる。

２　受注者は、この特記事項に違反する行為が発生した場合、又は発生するおそれがあると認められる場合（再委託等の相手方により発生し、又は発生するおそれがある場合を含む。）は、直ちに発注者にその旨を報告し、その指示に従わなければならない。

３　受注者は、この特記事項への違反の有無にかかわらず、本契約に係る業務で取り扱う情報資産に対して、情報セキュリティインシデントが発生した場合、又は発生するおそれがあると認められる場合は、直ちに発注者にその旨を報告し、その指示に従わなければならない。

（立ち入り検査）

第 15　発注者は、この特記事項の遵守状況の確認のため、受注者又は再委託等の相手方に対して立ち入り検査（発注者による検査が困難な場合にあっては、第三者や第三者監査に類似する客観性が認められる外部委託事業者の内部監査部門による監査、検査又は国際的なセキュリティの第三者認証(ISO/IEC27001 等)の取得等の確認）を行うことができる。

（情報セキュリティインシデント発生時の公表）

第 16　発注者は、本契約に係る業務に関して、情報セキュリティインシデントが発生した場合（再委託等の相手方により発生した場合を含む。）は、必要に応じて、当該情報セキュリティインシデントを公表することができるものとする。

（情報セキュリティの確保）

第 17　発注者は、本契約に係る受注者の業務の遂行に当たって、前項までに定めるもののほか、必要に応じて、情報セキュリティを確保する上で必要な対策を実施するよう指示することができ、受注者はこれに従わなければならない。

（損害賠償）

第 18　受注者が本特記事項に違反したことにより発注者又は第三者に損害を及ぼした場合には、発注者が必要と認める措置を直ちに講ずるとともに、発注者又は第三者に対して生じた損害を賠償するものとする。

（存続期間）

第 19　本特記事項の効力は本件業務に係る契約期間の満了まで有効とする。ただし、第 12（機密データの返還等）、第 13（再委託等の相手方からの回収等）、第 14（報告等。ただし、第１項の規定を除く。）及び第 18（損害賠償）の規定については、契約期間の満了後も有効に存続するものとする。

（協議事項）

第 20　本特記事項に定めのない事項に関しては、別途発注者と誠実に協議の上、円満な解決を図るものとする。

受託者向け情報セキュリティ遵守事項

1　趣旨

この受託者向け情報セキュリティ遵守事項は、情報セキュリティに関する特記事項（以下「特記事項」という。）に基づき、受注者が業務を行う際の細則及び具体的な手順を定めたものであり、受注者は特記事項と合わせて遵守する義務を負う。

2　機密データの管理・保管及び持出

(1)　管理・保管

受注者は、本契約に係る業務の遂行に当たって入手した資料、データ、記録媒体等について、常に適正な管理を行うとともに、特に個人情報等の重要な情報について、暗号化、パスワードの設定、個人情報の匿名化、アクセス制限等、厳重に管理し、使用しない場合には、施錠ができる書庫等に保管しなければならない。

(2)　持出

受注者は、特記事項第６（機密データの持出等の禁止）に基づき、あらかじめ発注者の承認を得て機密データを社外へ持ち出す場合には、機密データを出力又は保存した機器又は媒体について盗難及び紛失が発生しないよう十分な対策を講じるとともに、機密データの暗号化又は電子ファイルを開くためのパスワードを設定するなど第三者への漏えい等を防ぐための安全管理措置を講じること。

3　クラウドサービスの利用

(1)　事前の届出

受注者は、オンラインストレージ等のクラウドサービス（以下「クラウドサービス」という。）を利用して機密データを取り扱う場合には、特記事項第５（機密データの保存等に係る届出）に基づき事前に届出を行ったクラウドサービスを利用するものとする。また、利用するクラウドサービスを変更しようとする場合には、あらかじめ再度の届出を行うものとする。

(2)　提供事業者によるアクセス等

受注者がクラウドサービスにおいて機密データを取り扱う場合には、当該クラウドサービスの提供事業者による機密データのアクセス若しくは利用等が可能な契約又は利用規約とされているクラウドサービスを使用してはならない。ただし、発注者から承諾がある場合にはこの限りではない。

(3)　機密データの消去等

受注者は、業務中にクラウドサービスにおいて取り扱う機密データについて、不要となった時点で随時に機密データの消去を行うとともに、業務完了後はデータの消去又は暗号鍵を削除する等の対応により、保存した機密データが復元困難となる措置を講じること。

4　情報機器等の管理

(1)　情報機器

受注者は、機密データを取り扱う機器（ノートPC及びタブレット等の端末、サーバ等）をネットワークに接続して使用する場合には、セキュリティ対策ソフトの導入等により外部から

の侵入及び漏えい等を防止するための必要な対策を講じるとともに、OS 及びソフトウェアを最新の状態に更新するなど、セキュリティの脆弱性に関する対策を講じなければならない。

(2)　ネットワーク接続

機密データを取り扱う機器又は情報システムを外部のネットワークと接続して利用する場合には、取り扱う機密情報の重要性に応じて、適正なセキュリティ対策を講じること。

5　パスワード管理

機密情報の保管・管理、電子ファイルの閲覧制限、情報システムの管理その他のセキュリティ対策のため、パスワードによる管理を行う場合は、次に掲げる事項を遵守すること。

(1)　従事者個人に割り当てられたパスワードは当該従事者以外の者に漏れることがないよう適切に管理すること。

(2)　パスワードが流出したおそれがある場合には、受注者におけるセキュリティ管理者に速やかに報告するとともに、パスワードを変更する対応を行うこと。

6　情報の送受信

受注者が、発注者又は発注者が送付先として指定した者を送り先として機密データを含む情報を送受信する場合には、次に掲げる事項を遵守すること。

(1)　電子メール

ア　宛先、メール本文、添付ファイルの中身について、送信前に確認すること。

イ　発注者が送付先として指定したメールアドレスが複数ある場合の送信については、送付先のメールアドレスを BCC に入れる又は個別送付が可能なソフトウェアを利用するなど、送付先のメールアドレスの漏えいを防ぐための適切な対策を講じること。

(2)　ファイル交換・転送サービス

ファイル交換・転送サービスによる送受信を行う場合は、発注者が指定したサービスとすること。

(3)　オンラインストレージ

オンラインストレージを利用して送受信を行う場合には、発注者が指定したオンラインストレージを利用すること。

7　従事者の教育

特記事項第９（教育の実施）に基づき、受注者は次の事項を遵守すること。

(1)　従事者の教育状況の管理

受注者において、本業務の従事者が適切な教育及び訓練を受けた者であるか確認すること。また、業務の履行期間中であっても、教育状況が不十分と思われる事案が生じた場合は、追加の教育及び訓練を実施すること。

(2)　教育状況の報告

受注者は、本契約の期間中に発注者が従事者の教育状況の確認を求めた場合には、教育及び訓練の内容、実施日時並びに受講状況等を報告すること。

(3)　再委託先等の従事者

再委託先等の従事者の教育状況について発注者が確認を求めた場合には、(2)の報告に代えて、受注者が再委託先等の教育状況を確認した方法及び内容について報告すること。

8　機密情報の漏えい・紛失の防止策の徹底

受注者は、機密情報の漏えい・紛失を防止するため、次の事項に留意するとともに、機密情報を取り扱う従事者に対し適切な指示及び監督を行うこと。

(1)　ノートPC等のモバイル端末の社外利用

ノートPC等のモバイル端末を社外で使用する場合には次の事項を遵守すること。

ア　ノートPC等のモバイル端末を第三者が使用することがないよう、利用認証等の適切なセキュリティ対策を行うこと。

イ　ノートPC等のモバイル端末に直接機密データを保存する場合には、データ暗号化等による紛失・盗難時の対策をとること。

ウ　飲食店、公共施設、休憩所など、本件業務と関わりのない不特定多数の者が利用する場所において、ノートPC等のモバイル端末を利用しての業務を行わないこと。

エ　公衆Wi-Fi等の不特定多数の者が利用可能なネットワークに接続しないこと。

オ　ノートPC等のモバイル端末の紛失及び盗難に十分注意するとともに、短時間であっても部外者が立ち入る恐れのある共用スペースや車内に放置しないこと。

カ　盗難及び紛失の防止のため、酒席へのノートPC等のモバイル端末の持込みを行わないこと。

(2)　書類の取扱いについて

機密データを印刷した書類については、次のとおり取り扱うこと。

ア　機密データを書類として出力する場合には、情報の流出防止のため、必要最低限の範囲に限るものとし、不要となった時点でシュレッダー等による廃棄を行うこと。

イ　飲食店、公共施設、休憩所など、本件業務と関わりのない不特定多数の者が利用する場所において、当該書類を用いた業務を行わないこと。

ウ　発注者の承諾がある場合を除き、第三者への閲覧、複写又は提供を行わないこと。

エ　盗難及び紛失の防止のため、酒席へ当該書類の持込みを行わないこと。

(3)　その他の禁止事項

ア　不特定多数の者が立ち入る場所で携帯電話等の通話手段を利用する場合には、機密情報が含まれる内容を話してはならない。

イ　部外者が聞き取る可能性がある場所（公共交通機関、エレベータ、食堂、飲食店、家庭内など）で本件業務に係る内容を話してはならない。

ウ　発注者の承諾がある場合を除き、ソーシャルメディアにおいて本業務に係る内容及び本業務を推察できる内容の発信を行なってはならない。

9　セキュリティ事案発生時の連絡・対応

受注者は、本業務に関し情報セキュリティインシデントが発生した場合の連絡・管理体制をあらかじめ定めるとともに、情報セキュリティインシデントの発生又は発生したおそれがある場合には次の対応を行わなければならない。

(1)　一報

受注者は、発注者が指定した連絡窓口に、最初に事案を認識した時点から60分以内に一報の連絡をすること。

(2)　続報

一報後、発注者が求める事項について、速やかに続報の連絡を行うこと。

(3) 受注者による公表

情報セキュリティインシデント事案の発生について受注者が公表する場合には、事前に発注者に対して公表を行う旨の連絡をするものとする。ただし、損害の発生が生じる可能性があり急を要するなど、やむを得ない事情がある場合はこの限りではない。