原議保存期間	5年(令和10年3月31日まで)
有 効 期 間	一種(令和10年3月31日まで)

庁内各部局課長
各附属機関の長
各地方機関の長
各都道府県警察の長
殿

警察庁丁会発第369号、丁技企発第33号
令和４年４月４日
警察庁長官官房会計課長
警察庁長官官房技術企画課長

調達における情報セキュリティの確保に関する特約条項について（通達）

国の安全に関する重要な情報を国以外の者に扱わせることを内容とする売買、貸借、請負その他の契約を行う際の調達における情報セキュリティの確保については、「調達における情報セキュリティ要件の記載について」（平成24年１月24日付け内閣官房副長官通知）により、調達仕様書及びこれに基づき作成する契約書において、当該契約の履行に当たって必要な情報セキュリティ要件を記載することなどが求められてきたところである。

この点、契約相手方における情報管理の更なる徹底を図るため、「調達における情報セキュリティの確保に関する特約条項について（通達）」（令和３年３月11日付け警察庁丁会発第248号ほか。以下「旧通達」という。）により示していた情報セキュリティの確保に関する特約条項のモデルを、この度の組織改正に伴い改めて示すこととしたので、情報セキュリティの確保を必要とする契約を行う場合は、引き続き、同条項を活用されたい。

なお、旧通達は廃止する。

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。

一　甲が秘密区分の指定をした秘密に属する文書、図面、図書等（電磁的記録を含む。）

二　甲が秘密区分の指定をした秘密に属する物件

三　一号又は二号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。）又は物件のうち、甲が指定したもの

（下請負の禁止）

第２条　乙は、本契約の全部又は一部を第三者に下請負させてはならない。ただし、やむを得ず下請負をさせるときは、その下請負先、契約内容等を記した書面を添え、甲の許可を得るものとする。

２　前項ただし書により乙が下請負をさせる場合、乙は乙と下請負者との間で締結する契約において、下請負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項の許可を与えないことができる。

４　第１項ただし書により乙が下請負させる場合の下請負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「下請負者等」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（乙及び下請負者等における、派遣社員、契約社員、パート及び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、同名簿を甲に通知しなければならない。

４　乙は、契約締結後速やかに、情報セキュリティ確保のため、取扱者に対し作業内容に応じた教育計画を作成し、甲の承認を得るものとする。

なお、乙が予め当該計画を有する場合には、これに代えることができる。

5　甲は乙に対し、第４項の教育計画の実施状況について、報告を求めることができる。

（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　乙又は下請負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許可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、方法の如何にかかわらず複製・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。

（脆弱性対策等の実施）

第６条　乙は、本件業務を実施するにあたり、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、コンピューター・ウイルス、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、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７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、下請負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８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。

一　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

二　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

三　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コンピューター・ウイルスの感染が認められた場合

四　一号から三号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９条　乙は、乙の従業員又は下請負者等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１０条　乙は、本契約の履行に際し、第８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８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８条に規定する事故が下請負者等において発生した場合、乙は甲が当該下請負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８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８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。

（情報セキュリティ監査）

第１１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、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　甲が下請負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１２条　甲は、第８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た場合において、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

（１）事業者名：

（２）対象部門等名：

（３）契約開始年月日：

（４）前回確認実施年月日：

【留意事項】

確認対象者が下請負者等の場合は、（１）欄に事業者名を記載し、その末尾に「(下請負者等)」と記載すること。この場合、（３）欄には、下請負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	実施／未実施	実施状況（詳細）又は 未実施の理由
１	２．１ 本契約の全部又は一部を第三者に下請負させていない。		
２	２．１ （１が未実施の場合） やむを得ず下請負をさせるときは、その下請負先、契約内容等を記した書面を添え、甲の許可を得ている。		
３	３．２ 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。		
４	３．２ 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。		
５	３．３ 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。		
６	３．３ 取扱者の名簿を作成し､甲に通知している。		
７	３．４ 教育計画を作成し、甲の承認を得ている。		
８	３．１ 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。	※	※
９	４．１ 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。		
１０	４．２ 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または漏えいしないよう、措置を講じている。		
１１	４．３ （１及び２が未実施の場合） 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許可を得ている。	※	※
１２	５．１ 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。		
１３	５．２ （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。	※	※
１４	５．２	※	※

	（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。		
１５	５．３ 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。		
１６	５．４ 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。		
１７	５．５ 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。	※	※
１８	５．６ 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。		
１９	５．７ 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。	※	※
２０	６．１ （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。	※	※
２１	６．２ （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、コンピューター・ウィルス、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。	※	※
２２	６．２ （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、コンピューター・ウィルス、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。	※	※
２３	７．１ （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。	※	※
２４	７．５ 報告した確認結果について、甲の承認を得ている。		
２５	１０．１ （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。	※	※
２６	１０．４ （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。	※	※
確認年月日： 確認者（事業者名、所属、役職、氏名）：　　印			

【留意事項】
※欄については、該当がある場合に記載する。