別紙
付紙様式

情報セキュリティ対策実施確認書

1　下請負者名又は開示先事業者名等

(1) 事業者名：

(2) 対象部門等名：

(3) 請負又は開示予定年月日：

(4) 業務の実施予定場所※：

※（請負事業者又は開示先事業者の業務の実施予定場所を記入）

2　防衛省による情報セキュリティ実地監査の受査状況

(1) 下請負者又は開示先事業者

ア　監査年月日：

イ　監査結果：

ウ　監査結果の文書番号及び年月日：

(2) 下請負者又は開示先事業者の業務実施場所を管理する事業者（(1)の下請負者又は開示先事業者と同じ場合は省略可）

ア　監査年月日：

イ　監査結果：

ウ　監査結果の文書番号及び年月日：

3　下請負者又は開示先事業者に対する確認事項（上記２における監査年月日が請負年月日の属する年度又はその前年度の場合は、下線を引いた事項を除き確認を省略することができる。）

番号	確認事項	実施／未実施	実施状況の確認方法　又は　未実施の理由
1	**5(1)情報セキュリティ基本方針及び情報セキュリティ基準** ・保護すべき情報を取り扱う可能性のある全ての者に周知することを定めていること。 ・必要に応じて下請負者へ周知することを定めていること。		
2	**5(2)情報セキュリティ基本方針等の見直し** ・情報セキュリティ基本方針等を定期的並びに重大な変化及び事故が発生した場合、見直しを実施し、必要に応じて変更することを定めていること。		
3	**6(1)ア　情報セキュリティに対する経営者等の責任** ・経営者等が情報セキュリティ基本方針等を承認することを定めていること。 ・取扱者以外の役員（持分会社にあっては社員を含む。以下同じ。）、管理職員等を含む従業員その他の全ての構成員について、取扱者以外の者は保護すべき情報に接してはならないことを定めていること。 ・職務上の下級者等に対して、保護すべき情報の提供を要求してはならないことを定めていること。		
4	**6(1)イ　責任の割当て** ・総括責任者を置くことを定めていること。 ・管理責任者を置くことを定めていること。		
5	**6(1)ウ　守秘義務** ・取扱者との間で守秘義務を定めた契約又は合意をすることを定めていること。 ・定期的並びに状況の変化及び事故が発生した場合、要求事項の見直しを実施し、必要に応じて修正することを定めていること。		
6	**6(1)エ　情報セキュリティの実施状況の監査** ・情報セキュリティの実施状況について、定期的及び重大な変化が発生した場合、監査を実施し、必要に応じて是正措置をとることを定めていること。 ・定期的及び重大な変化が発生した場合において、監査を適切に実施していること。 ・監査の実施に関し、その結果を保存していること。 ・監査の結果、必要な是正措置が適切にとられていること。		
7	**6(2)　保護すべき情報を取り扱う下請負者** ・保護すべき情報を請け負わせる場合には、契約上の義務に本基準に基づいた実施を含めるとともに、確認を実施し、防衛省へ届け出ることを定めていること。		

番号	確認事項	実施／未実施	実施状況の確認方法　又は　未実施の理由
8	**6(3)ア　第三者への開示の禁止** ・第三者（法人又は自然人としての防衛省と直接契約関係にある者以外の全ての者をいい、親会社、地域統括会社、ブランド・ライセンサー、フランチャイザー、コンサルタントその他の防衛省と直接契約関係にある者に対して指導、監督、業務支援、助言、監査等を行うものを含む。以下同じ。）への開示又は漏えいをしてはならないことを定めていること。 ・保有し、又は知り得た情報を第三者との契約において伝達、交換、共有その他提供する約定があるときは、保護すべき情報をその対象から除く措置を定めていること。 ・やむを得ない場合は、あらかじめ書面による防衛省の許可を得ることを定めていること。		
9	**6(3)イ　第三者に関係したリスクの管理** ・第三者の取扱施設への立入りを許可する場合、リスクを明確にした上対策を定めていること。		
10	**6(3)ウ　第三者に対する立入りの許可** ・第三者へ立入りを許可する場合の手順を定めていること。		
11	**7(1)　分類の指針** ・保護すべき情報を明確に分類できる分類体系を定めていること。		
12	**7(2)ア　保護すべき情報の目録** ・目録の作成及び維持することを定めていること。 ・目録が適切に維持されていること。		
13	**7(2)イ　取扱いの管理策** ・取扱施設で取り扱うことを定めていること。 ・接受等を記録することを定めていること。 ・個人が所有する情報システム及び可搬記憶媒体で取り扱ってはならないことを定めていること。 ・（やむを得ない場合）事前に防衛省の許可を得る手続を定めていること。 ・防衛省の指示に従い、返却、提出、破棄等必要な措置をとることを定めていること。 ・防衛省から、保護すべき情報の破棄を求められた場合であって、当該情報を引き続き保有する必要がある場合には、その理由を添えて、発注者(防衛省との直接契約関係にある防衛関連企業をいう。以下同じ。)を経由して防衛省(調達要求元)に協議を求めることができることを定めていること。 ・接受等が適切に記録されていること。		
14	**7(2)ウ　保護すべき情報の保管等** ・保護すべき情報は、施錠したロッカー等において保管することを定めていること。 ・ロッカー等の鍵を適切に管理（無断での使用を防止）することを定めていること。 ・施錠したロッカー等において保管していること。 ・ロッカー等の鍵を適切に管理していること。		
15	**7(2)エ　保護すべき情報の持ち出し** ・持ち出しに伴うリスクを回避することができると判断する場合の判断基準を定めていること。 ・持ち出しする場合は記録することを定めていること。 ・持ち出しを記録していること。		
16	**7(2)オ　保護すべき情報の破棄** ・復元できない方法による破棄を定めていること。 ・破棄したことを記録することを定めていること。 ・破棄を記録していること。		
17	**7(2)カ　該当部分の明示** ・保護すべき情報を作成、製作又は複製した場合、保護すべき情報である旨の表示を行う事を定めていること。 ・契約の目的物が保護すべき情報を含むものである場合には、当該契約の履行の一環として収集、整理、作成等した一切の情報について、防衛省が当該情報を保護すべき情報には当たらないと確認するまでは、保護すべき情報として取り扱うことを定めていること。 ・防衛関連企業は、保護すべき情報の指定を解除する必要がある場合には、その理由を添えて、発注者を経由して防衛省（調達要求元）に協議を求めることができることを定めていること。 ・保護すべき情報を記録する箇所を明示する及び明示の方法を定めていること。 ・適切に表示及び明示されていること。		
18	**8(1)　経営者等の責任** ・経営者等は取扱者の指定の範囲を必要最小限とするとともに、ふさわしいと認める者を充て、情報セキュリティ基本方針等を遵守させることを定めていること。 ・防衛省との契約に違反する行為を求められた場合に、これを拒む権利を実効性をもって法的に保障されない者を当該ふさわしい者と認めないことを定めていること。		
19	**8(2)　取扱者名簿** ・取扱者名簿を作成し、又は更新したときは、発注者を経由して各取扱者について防衛省に届け出て同意を得ることを定めていること。 ・取扱者名簿には、取扱者の氏名、生年月日、所属する部署、役職、国籍等が記載されていること。 ・取扱者名簿には、保護すべき情報に接する全ての者（保護すべき情報に接する役員（持分会社にあっては社員を含む。以下同じ。）、管理職員、派遣社員、契約社員、パート、アルバイト等を含む。この場合において、当該者が、自らが保護すべき情報に接しているとの認識の有無を問わない。）が記載されていること。		
20	**8(3)　情報セキュリティ教育及び訓練** ・定期的な教育及び訓練の実施を定めていること。 ・定期的に行う教育には、組織の方針、取扱手順、関連する法令その他なりすましメール等による悪意のあるコードへの感染を防止するための対策及び感染した場合の対処手順等に関する内容が含まれていること。 ・定期的に教育及び訓練を実施していること。 ・教育及び訓練の実施状況を記録し、保管していること。		

番号	確認事項	実施／未実施	実施状況の確認方法　又は　未実施の理由
21	**8(4)　違反者への対処方針** ・情報セキュリティ基本方針等に違反した取扱者に対する対処方針及び手続を定めていること。		
22	**8(5)　取扱者の責任** ・在職中及び離職後においても、知り得た保護すべき情報を第三者に漏えいしてはならないことを定めていること。		
23	**8(6)　保護すべき情報の返却** ・保護すべき情報に接する必要が無くなった場合は、管理者へ返却することを定めていること。 ・保護すべき情報は、管理者へ返却されていること。		
24	**9(1)ア　取扱施設の指定** ・取扱施設を定めていること。		
25	**9(1)イ　物理的セキュリティ境界** ・物理的セキュリティ境界を用いることを定めていること。		
26	**9(1)ウ　物理的入退管理策** ・取扱施設への立入りは、許可された者だけに制限することを定めていること。 ・第三者の立入りを記録することを定めていること。 ・立入記録の保管を定めていること。 ・第三者の立入りを記録し、保管していること。		
27	**9(1)エ　取扱施設での作業** ・機密性に配慮し作業することを定めていること。 ・通信機器及び記録装置を利用する場合は、経営者等の許可を得ることを定めていること。		
28	**9(2)ア　保護システムの設置及び保護** ・保護システムへの保護措置を実施することを定めていること。 ・保護システムへ保護措置が実施されていること。		
29	**9(2)イ　保護システムの持ち出し** ・持ち出しに伴うリスクを回避することができると判断する場合の基準を定めていること。 ・持ち出しする場合は記録することを定めていること。 ・持ち出しを記録していること。		
30	**9(2)ウ　保護システムの保守及び点検** ・第三者による保守及び点検を行う場合は、必要な処置を実施することを定めていること。 ・第三者による保守及び点検時において、必要な処置が実施されていること。		
31	**9(2)エ　保護システムの破棄又は再利用** ・保護すべきデータが復元できない状態であることを点検し、物理的に破壊したのち、破棄し、その旨を記録することを定めていること。 ・復元できない状態であることを点検した後、再利用することを定めていること。 ・破棄を記録していること。		
32	**10(1)　操作手順書** ・操作手順書を整備し、維持することを定めていること。 ・操作手順書には、□ ①可搬記憶媒体へ保存時の手順②可搬記憶媒体及び保護システムの破棄又は再利用の手順③電子メール等での伝達の手順④セキュリティに配慮したログオン手順についての記述又は引用が引用がなされていること。		
33	**10(2)　悪意のあるコードからの保護** ・保護システムを最新の状態に更新されたウイルス対策ソフト等を用いて、少なくとも週1回以上フルスキャンを行うことなどにより、悪意のあるコードから保護することを定めていること。（なお、1週間以上電源の切られた状態にあるサーバ又はパソコンについては、再度の電源投入時に当該処置を行うことで可。） ・ウイルス対策ソフト等を最新の状態に更新していること。 ・保護システムをウイルス対策ソフト等により、少なくとも週1回以上フルスキャンしていること。（1週間以上電源の切られた状態にあるサーバ及びパソコンについては、再度の電源投入時に当該処置を行うことで可。）		
34	**10(3)　保護システムのバックアップの管理** ・可搬記憶媒体へのバックアップを実施する場合、調達における情報セキュリティ基準7(2) 及び10(4) に添った取扱いをすることを定めていること。		
35	**10(4)ア　可搬記憶媒体の管理** ・保護すべき情報を保存した可搬記憶媒体を施錠したロッカー等により集中保管することを定めていること。 ・ロッカー等の鍵を適切に管理することを定めていること。 ・保護すべき情報とそれ以外を容易に区別できる処置をすることを定めていること。 ・施錠したロッカー等において集中保管していること。 ・ロッカー等の鍵を適切に管理していること。 ・保護すべき情報とそれ以外を容易に区別できる処置がされていること。		
36	**10(4)イ　可搬記憶媒体への保存** ・可搬記憶媒体へ保存する場合、暗号技術を用いることを定めていること。		
37	**10(4)ウ　可搬記憶媒体の破棄又は再利用** ・保護すべきデータが復元できない状態であることを点検し、物理的に破壊したのち、破棄し、その旨を記録することを定めていること。 ・復元できない状態であることを点検した後、再利用することを定めていること。 ・破棄を記録していること。		

番号	確認事項	実施／未実施	実施状況の確認方法　又は　未実施の理由
38	**１０(5)ア　保護すべき情報の伝達** ・伝達に伴うリスクから保護できると判断する場合の基準を定めていること。		
39	**１０(5)イ　伝達及び送達に関する合意** ・保護すべき伝達及び送達は、守秘義務を定めた契約又は合意した相手に対してのみ行うことを定めていること。		
40	**１０(5)ウ　送達中の管理策** ・保護すべき文書等を送達する場合、許可されていないアクセス及び不正使用等から保護する方法を定めていること。		
41	**１０(5)エ　保護すべきデータの伝達** ・保護すべきデータを伝達する場合には、保護すべきデータが既に暗号技術を用いて保存されている、通信事業者の回線区間に暗号技術を用いる又は電子メール等に暗号技術を用いることのいずれかによって、保護すべきデータを保護しなければならないことを定めている。(漏えいのおそれのない取扱施設内で有線での伝達をする場合を除く。) ・電子メール等による伝達など、暗号技術を用いるに当たって個人の操作を要するものについて、その旨の教育を行うなど、確実な実施のための方策がとられていること。		
42	**１０(6)　外部からの接続** ・外部からの接続を許可する場合は、利用者の認証を行い、及び暗号技術を用いることを定めていること。		
43	**１０(7)　電子政府推奨暗号等の利用** ・暗号技術を用いる場合には、電子政府推奨暗号等を用いることを定めていること。 ・やむを得ず電子政府推奨暗号等を使用できない場合は、その他の秘匿化技術を用いることを定めていること。		
44	**１０(8)　ソフトウェアの導入管理** ・導入するソフトウェアの安全性を確認することを定めていること。		
45	**１０(9)　システムユーティリティの使用** ・システムユーティリティの使用を制限することを定めていること。		
46	**１０(10)　技術的脆弱性の管理** ・脆弱性に関する情報を取得すること及び適切に対処することを定めていること。		
47	**１０(11)ア　監査ログ取得** ・利用者の保護すべき情報へのアクセス及び例外処理を記録した監査ログを取得することを定めていること。		
48	**１０(11)イ　監査ログの保管** ・取得した監査ログを記録のあった日から少なくとも３か月以上保存すると□ともに、定期的に点検することを定めていること。 ・監査ログを記録のあった日から３か月以上保存していること。		
49	**１０(11)ウ　監査ログの保護** ・監査ログを改ざん及び許可されていないアクセスから保護することを定めていること。		
50	**１０(11)エ　クロックの同期** ・保護システム及びネットワークを通じて保護システムにアクセス可能な情報システムの日付及び時刻を定期的に合わせることを定めていること。		
51	**１０(11)オ　保護すべきデータの監視** ・保護システムが共有ネットワーク（インターネット等）へ物理的に接続されている場合は、共有ネットワークを通じた保護すべきデータの社外漏えいを未然に防止することを可能とする常時監視を行わなければならない。 ・保護すべきデータが、共有ネットワークを通じて社外へ漏えいすることを未然に防止することを可能とする常時監視を行っていること。		
52	**１１(1)　アクセス制御方針** ・職務内容に応じて、保護すべき情報、取扱施設及び保護システムへのアクセス制御方針を定めていること。 ・定期的並びに重大な変化及び事故が発生した場合、見直しを実施し、必要に応じて修正することを定めていること。		
53	**１１(2)ア　利用者の登録管理** ・保護システムの利用者の登録及び登録削除をすることを定めていること。		
54	**１１(2)イ　パスワードの割当て** ・初期又は仮パスワードは、容易に推測されないものとするとともに、機密性を配慮した方法で配布することを定めていること（パスワードより強固な手段を併用又は採用している場合はこの限りでない。）。		
55	**１１(2)ウ　管理者権限の管理** ・管理者権限の利用は必要最低限とすることを定めていること。		
56	**１１(2)エ　アクセス権の見直し** ・保護システムの利用者のアクセス権の割当てを定期的及び必要に応じて見直すことを定めていること。		
57	**１１(3)ア　パスワードの利用** ・保護システムの利用者は、容易に推測されないパスワードを選択しなければならないことを定めていること（パスワードより強固な手段を併用又は採用している場合はこの限りでない。）。		
58	**１１(3)イ　無人状態にある保護システム対策** ・保護システムが無人状態に置かれる場合、機密性を配慮した措置を実施することを定めていること。 ・無人状態にある保護システムへ機密性を配慮した措置が実施されていること。		

番号	確認事項	実施／未実施	実施状況の確認方法　又は　未実施の理由
59	**１１(4)ア　機能の制限** ・保護システムの利用者の職務内容に応じて、利用できる機能を制限することを定めていること。		
60	**１１(4)イ　ネットワークの接続制御** ・保護システムを共有ネットワークへ接続する場合、接続に伴うリスクから保護することを定めていること（FW設置など）。		
61	**１１(5)ア　セキュリティに配慮したログオン手順** ・保護システムの利用者は、セキュリティに配慮した手順でログオンすることを定めていること。 ・セキュリティに配慮した手順でログオンしていること。		
62	**１１(5)イ　利用者の識別及び認証** ・保護システムの利用者ごとに一意な識別子（ユーザーID、ユーザー名等）を保有させることを定めていること。		
63	**１１(5)ウ　パスワード管理システム** ・保護システムは、パスワードの不正使用を防止する機能を有さなければならないことを定めていること。		
64	**１２(1)、(2)　情報セキュリティの事故の報告** ・情報セキュリティ事故等に関する下記のそれぞれの事項について、発注者（防衛省との直接契約関係にある防衛関連企業をいう。以下同じ。）への報告要領を定めているとともに、当該報告要領に以下のことが規定されていること。 ①　情報セキュリティ事故が発生したときは、適切な措置を講じるとともに、直ちに把握し得る限りの全ての内容を、その後速やかにその詳細を発注者に報告しなければならない。 ②　ア）保護すべき情報が保存されたサーバ又はパソコン（以下「サーバ等」という。）に悪意のあるコードへの感染又は不正アクセスが認められた場合、及びイ）保護すべき情報が保存されているサーバ等と同一のイントラネットに接続されているサーバ等に悪意のあるコードへの感染が認められた場合において、適切な措置を講じるとともに、直ちに把握し得る限りの全ての内容を、その後速やかにその詳細を発注者に報告しなければならない。 ③　情報セキュリティ事故の疑い又は事故につながるおそれのある場合は、適切な措置を講じるとともに、速やかに、その詳細を発注者に報告しなければならない。 ④　前記①から③までに規定する報告のほか、保護すべき情報の漏えい、紛失、破壊等の事故が発生した可能性又は将来発生する懸念について防衛関連企業の内部又は外部から指摘があったときは、防衛関連企業は、直ちに当該可能性又は懸念の真偽を含む把握し得る限りの全ての背景及び事実関係の詳細を速やかに防衛省に報告しなければならない。 ・報告に当たっての責任者及び連絡担当者等を明らかにした連絡系統図を作成している（異動等のあった場合には更新している）とともに、直ちに発注者に報告する場合の責任者及び連絡担当者を明示していること。		
65	**１２(3)ア　対処体制及び手順** ・情報セキュリティ事故（情報セキュリティ事故の疑いのある場合を含む。以下同じ。）及び事象に対処するため、対処体制、責任及び手順を定めていること。		
66	**１２(3)イ　証拠の収集** ・情報セキュリティ事故が発生した場合（保護すべき情報が保存されたサーバ等に悪意のあるコードへの感染が認められた場合を含む。）、証拠を収集し、速やかに発注者を理由して防衛省へ提出することを定めていること。		
67	**１２(3)ウ　情報セキュリティ基本方針等への反映** ・情報セキュリティ基本方針等の見直しに、情報セキュリティ事故及び事象を反映することを定めていること。		
68	**１３(1)ア　遵守状況の確認** ・管理者の責任の範囲において、情報セキュリティ基本方針等の遵守状況の確認を定めていること。		
69	**１３(1)イ　技術的遵守の確認** ・保護システムの管理者の責任の範囲において、情報セキュリティ基本方針等への技術的遵守状況を確認することを定めていること。		
70	**１３(2)　情報セキュリティの記録** ・保護すべき情報に係る重要な記録の保管期間を定めていること。 ・重要な記録は、施錠したロッカー等において保管又は暗号技術を用いる等厳密に保護することを定めていること。 ・適切に鍵を管理することを定めていること。 ・重要な記録は、施錠したロッカー等において保管又は暗号技術を用いる等厳密に保護されていること。 ・適切に鍵が管理されていること。		
71	**１３(3)　監査ツールの管理** ・保護システムの監査に用いるツールは、悪用を防止するため、必要最低限の使用にとどめることを定めていること。		

確認年月日：＿＿＿＿＿＿＿＿＿＿

確認者（企業名、所属、役職、氏名）：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

注：未実施の理由については、実施する必要がないと認められる合理的な理由を記すこと。