別表

「装備品等及び役務の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」の一部改正表

改正前	改正後
装備品等及び役務の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 第１条～第８条　［略］ （適用の特例） 第９条　［略］ ２～３　［略］ ４　甲は、第２項の規定により提出された事業計画（第２項ただし書の規定により届出があった場合には、その内容）を確認し、防衛装備庁長官と協議を行ったうえでこれを適当と認めたときは、その旨を乙に通知するものとする。 ５　乙は、前項の通知を受けた場合には、甲が適当と認めた事業計画が完了するまでの間は、装備品等及び役務の調達における情報セキュリティの確保について（防経装９２４６号。２１．７．３１）の規定を適用することができる。 別紙 装備品等及び役務の調達における情報セキュリティ基準 第１　［略］ 第２　定義 (1)～(10)　［略］ (11) 第三者とは、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・サイセンサー、フランチャイザー、	装備品等及び役務の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 第１条～第８条　［略］ （適用の特例） 第９条　［略］ ２～３　［略］ ４　甲は、第２項の規定により提出された事業計画（第２項ただし書の規定により届出があった場合には、その内容）を確認し、これを適当と認めたときは、その旨を乙に通知するものとする。 ５　乙は、前項の通知を受けた場合には、甲が適当と認めた事業計画が完了するまでの間は、装備品等及び役務の調達における情報セキュリティの確保について（防経装第９２４６号。２１．７．３１）の規定を適用することができる。 別紙 装備品等及び役務の調達における情報セキュリティ基準 第１　［略］ 第２　定義 (1)～(10)　［略］ (11) 第三者とは、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・サイセンサー、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。	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、監査等を行う者を含む。
(12)～(41)　［略］	(12)～(41)　［略］
第３　対象	第３　対象
１　［略］	１　［略］
２　対象者 対象者は、防衛関連企業において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。）、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。）とする。	２　対象者 対象者は、防衛関連企業において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。）、管理職員、派遣社員、契約社員、パート、アルバイト等を含む。）とする。
第４　［略］	第４　［略］
第５　組織のセキュリティ	第５　組織のセキュリティ
１　［略］	１　［略］
２　経営者等及び取扱者の責務	２　経営者等及び取扱者の責務
(1)　取扱者の指定等	(1)　取扱者の指定等
ア～ウ　［略］	ア～ウ　［略］
エ　管理者は、取扱者として指定した個人の氏名、生年月日、所属する部署、役職及び国籍等を記載したリスト（以下「取扱者名簿」という。）を作成又は更新し、取扱者に保護すべき情報を取り扱わせる前に、防衛省の確認を受けるものとする。	エ　管理者は、取扱者として指定した個人の氏名、生年月日、所属する部署、役職及び国籍等を記載したリスト（以下「取扱者名簿」という。）を作成又は更新し、取扱者に保護すべき情報を取り扱わせる前に、防衛省に届け出なければならない。 なお、保護すべき情報の取扱いの開始については、防衛省の指示によるものとする。
オ　［略］	オ　［略］
(2)～(3)　［略］	(2)～(3)　［略］
３～４　［略］	３～４　［略］
第６　保護すべき情報の管理	第６　保護すべき情報の管理
１　［略］	１　［略］

2　保護すべき情報の目録の作成等	2　保護すべき情報の目録の作成等
(1)　目録の作成 管理者は、保護すべき情報を保管した場所、保存した保護システム、可搬記憶媒体等、保護すべき情報の管理状況を記載した目録を作成するものとする。	(1)　目録の作成 管理者は、保護すべき情報を保管した場所、保存した保護システム、可搬記憶媒体等、保護すべき情報の管理状況を記載した目録を作成するものとする。 なお、目録の作成は、保護すべき情報の取扱いに関するシステムログの記録により代用することができるものとする。
(2)　目録の更新 ア　管理者は、下記の（ｱ）から（ｳ）までに掲げる措置（以下「接受等」という。）を実施する場合は、保護すべき情報の目録を更新するものとする。	(2)　目録の更新 ア　管理者は、下記の（ｱ）から（ｳ）までに掲げる措置（以下「接受等」という。）を実施する場合は、保護すべき情報の目録を更新するものとする。 なお、目録の更新は、保護すべき情報の取扱いに関するシステムログの記録により代用することができるものとする。
(ｱ)～(ｳ)　［略］	(ｱ)～(ｳ)　［略］
イ　目録には、接受等を行った者の氏名、所属、所在等を記載するものとする。 ただし、保護システムにおける保護すべきデータの閲覧については、システムログの記録により代用することができる。	イ　目録には、接受等を行った者の氏名、所属、所在等を記載するものとする。 ただし、保護すべき情報の取扱いに関するシステムログの記録により代用する場合は、アカウントの識別子を記載するものとする。
(3)　［略］	(3)　［略］
３～４　［略］	３～４　［略］
5　保護システムにおける可搬記憶媒体の使用制限	5　保護システムにおける可搬記憶媒体の使用制限
(1)　使用できる可搬記憶媒体及びその用途などを記載した目録を作成し、保護システム管理者の承認を得ること。	(1)　使用できる可搬記憶媒体及びその用途などを記載した目録を作成し、保護システム管理者の承認を得ること。 なお、目録の作成は、保護すべき

	情報の取扱いに関するシステムログの記録により代用することができるものとする。
(2)　前号に規定する目録は、定期的に、及び保護システムにおいて使用できる可搬記憶媒体、その用途等に変更があった場合など必要があると認められる場合にはその都度精査し、必要に応じ、更新すること。	(2)　前号に規定する目録は、定期的に、及び保護システムにおいて使用できる可搬記憶媒体、その用途等に変更があった場合など必要があると認められる場合にはその都度精査し、必要に応じ、更新すること。 なお、目録の更新は、保護すべき情報の取扱いに関するシステムログの記録により代用することができるものとする。
(3)～(6)　［略］	(3)～(6)　［略］
６～９　［略］	６～９　［略］
第７　［略］	第７　［略］
第８　物理的及び環境的セキュリティ	第８　物理的及び環境的セキュリティ
１　［略］	１　［略］
２　取扱施設等に対する物理的セキュリティ対策	２　取扱施設等に対する物理的セキュリティ対策
(1)　取扱施設等の指定	(1)　取扱施設等の指定
ア　経営者等は、自社のセキュリティ水準を維持する物理的範囲を画定するため、保護すべき情報の取扱施設に加え、関係施設を指定するものとする。	ア　経営者等は、自社のセキュリティ水準を維持する物理的範囲を画定するため、取扱施設に加え、関係施設を指定するものとする。
イ　［略］	イ　［略］
	ウ　管理責任者は、取扱施設等、取扱施設等に講じた物理的セキュリティ対策及び入退管理機器の設置状況について図面等により管理するものとする。
ウ　管理責任者は、取扱施設等への立ち入り許可に関する手順を作成し、許可した者の名簿（以下「取扱施設等立入名簿」という。）を作成し、保護システム管理者の同意を得ることとする。	エ　管理責任者は、取扱施設等への立ち入り許可に関する手順を作成し、許可した者の名簿（以下「取扱施設等立入名簿」という。）を作成し、保護システム管理者の同意を得ることとする。

エ　管理責任者は、取扱施設等立入名簿に基づき取扱施設等への立ち入りを許可する証明書を発行するものとし、当該立ち入りを許可する者については、業務の遂行上必要最小限に制限するものとする。	オ　管理責任者は、取扱施設等立入名簿に基づき取扱施設等への立ち入りを許可する証明書を発行するものとし、当該立ち入りを許可する者については、業務の遂行上必要最小限に制限するものとする。
オ　管理責任者は、取扱施設等立入名簿を定期的に見直し、必要に応じて更新するものとする。	カ　管理責任者は、取扱施設等立入名簿を定期的に見直し、必要に応じて更新するものとする。
(2)　［略］	(2)　［略］
ア　取扱施設と関係施設の境界に入退口を設置し、入退管理機器又は警備員等により、入退する者が当該入退を許可された者であることを管理（識別及び認証を含む。以下この号において同じ。）すること。	ア　取扱施設と関係施設の境界に入退口を設置し、入退管理機器又は警備員、受付係その他管理責任者が指定した者（以下「警備員等」という。）により、入退する者が当該入退を許可された者であることを管理（識別及び認証を含む。以下この号において同じ。）すること。
イ　［略］	イ　［略］
ウ　取扱施設への入退をＩＤカードにより管理する場合は、当該入退の記録を電子的に取得すること。	ウ　取扱施設への入退をＩＤカード（社員証、身分証明書その他入退する者の個人識別が可能なものをいう。以下同じ。）により管理する場合は、当該入退の記録を電子的に取得すること。
エ～カ　［略］	エ～カ　［略］
キ　取扱施設の入退をＩＣカードのみで管理する場合は、当該施設の境界を警備員等、センサー装置又は監視カメラによる監視など必要な措置を講じること。	キ　取扱施設の入退をＩＣカード（一時的に貸与した入退カード、複数の者が共用するカードその他入退する者の個人識別ができないものをいう。）のみで管理する場合は、当該施設の境界を警備員等、センサー装置又は監視カメラによる監視など必要な措置を講じること。
ク　［略］	ク　［略］
(3)～(5)　［略］	(3)～(5)　［略］
	(6)　取扱施設等が自然災害等の非常事態により使用できない場合は、経

	営者等が指定する取扱施設等を代替する施設において、総括者が当該事態の状況を踏まえつつ、取扱者のみが当該保護すべき情報に接することができるようにするために必要な物理的セキュリティ対策を講じることで、保護すべき情報を扱うことができる。
３～５　［略］	３～５　［略］
第９　［略］	第９　［略］
第１０　情報セキュリティ事故等への対応	第１０　情報セキュリティ事故等への対応
１　［略］	１　［略］
２　情報セキュリティ事故等への対処テスト	２　情報セキュリティ事故等への対処テスト
(1)　防衛関連企業は、情報セキュリティ事故等に対する保護システムの対処能力の有効性を検証し、潜在的な弱点又は欠陥を発見するため、情報セキュリティ事故等対処テストを定期的に実施するものとする。	(1)　防衛関連企業は、情報セキュリティ事故等対処計画の有効性を検証し、潜在的な弱点又は欠陥を発見するため、情報セキュリティ事故等対処テストを第７第１項の規定による訓練に含めるなど、定期的に実施するものとする。
(2)　［略］	(2)　［略］
第１１　情報セキュリティ事故等発生時の対応	第１１　情報セキュリティ事故等発生時の対応
１　［略］	１　［略］
２　防衛省への報告	２　防衛省への報告
(1)　総括者は、前項第１号及び第２号に掲げる情報セキュリティ事故等の報告を受けた場合は、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防衛省（契約担当官等又は防衛装備庁長官が別に定めた部署の職員。以下同じ。）に報告するものとする。	(1)　総括者は、前項第１号に掲げる情報セキュリティ事故等の報告を受けた場合は、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防衛省（契約担当官等又は防衛装備庁長官が別に定めた部署の職員。以下同じ。）に報告するものとする。
(2)～(4)　［略］	(2)～(4)　［略］
第１２　［略］	第１２　［略］

第１３　セキュリティ監査	第１３　セキュリティ監査
１　セキュリティ監査計画の作成	１　セキュリティ監査計画の作成等
(1)　防衛関連企業は、情報セキュリティ基本方針等に基づく措置の実施状況の確認及び有効性の評価を客観的に行うため、監査部門を設置し、同部門には原則として最低１名は監査を受ける部署以外の取扱者を含むものとする。	(1)　防衛関連企業は、情報セキュリティ基本方針等に基づく措置の実施状況の確認及びその措置が継続的に有効であることの評価を客観的に行うため、監査部門を設置し、同部門には原則として最低１名は監査を受ける部署以外の者を含むものとする。この場合において、セキュリティ監査の項目が保護すべき情報に関する事項である場合は、当該保護すべき情報の取扱者を含むものとする。
(2)　［略］	(2)　［略］
ア～イ［略］	ア～イ　［略］
ウ　情報セキュリティ基本方針等に基づく措置に係る実施状況の確認及び有効性の評価を行うための手順及び方法	ウ　情報セキュリティ基本方針等に基づく措置に係る実施状況の確認及びその措置が継続的に有効であることの評価を行うための手順及び方法
(3)～(4)　［略］	(3)～(4)　［略］
２　セキュリティ監査の実施	２　セキュリティ監査の実施
総括者は、１年に１回以上及び自社の情報セキュリティに重大な変化が生じた場合など必要と認めた場合に、監査部門に、前項に規定するセキュリティ監査計画に基づくセキュリティ監査を実施させるものとする。	総括者は、１年に１回以上及び自社の情報セキュリティに重大な変化が生じた場合など必要と認めた場合に、監査部門に、前項に規定するセキュリティ監査計画に基づくセキュリティ監査（情報セキュリティ基本方針等に基づく措置が継続的に有効であることの評価を含む。）を実施させるものとする。
３　セキュリティ監査結果の報告等	３　セキュリティ監査結果の報告等
(1)　［略］	(1)　［略］
(2)　［略］	(2)　［略］
ア　情報セキュリティ基本方針等に基づく措置の実施状況及び有効性に係る問題点の有無及びその内容	ア　情報セキュリティ基本方針等に基づく措置の実施状況及びその措置が継続的に有効であることに係る問題点の有無及びその内容

イ～ウ　［略］ (3)～(5)　［略］ 第１４　防衛省による監査 １　［略］ ２　監査への協力 防衛関連企業は、防衛省が監査を実施する場合は、防衛省の求めに応じ必要な協力（監査官の取扱施設等への立入り、及び監査官による書類の閲覧等への協力）を行うものとする。	イ～ウ　［略］ (3)～(5)　［略］ 第１４　防衛省による監査 １　［略］ ２　監査への協力 防衛関連企業は、防衛省が監査を実施する場合は、防衛省の求めに応じ必要な協力（監査官の取扱施設等への立入り、監査官による書類の閲覧、保護すべき情報の取扱いに関するシステムログの記録の確認等への協力）を行うものとする。
付紙 装備品等及び役務の調達における情報セキュリティの確保に関するシステムセキュリティ実施要領 第１　［略］ 第２　システムセキュリティ実装計画書 １　システムセキュリティ実装計画書の作成 (1)　防衛関連企業は、自社の保有又は使用する保護システムについて、セキュリティ基準に規定する措置を適切に実施し、本基準に適合していることを証明する資料として、システムセキュリティ実装計画書を作成するものとする。 (2)　［略］ ２～３　［略］ ４　システムセキュリティ実装計画書の周知 保護システム管理者は、システムセキュリティ実装計画書を作成又は変更した場合は、これを周知するとともに、システム管理業務	付紙 装備品等及び役務の調達における情報セキュリティの確保に関するシステムセキュリティ実施要領 第１　［略］ 第２　システムセキュリティ実装計画書 １　システムセキュリティ実装計画書の作成 (1)　防衛関連企業は、自社の保有又は使用する保護システムについて、本基準に規定する措置を適切に実施し、本基準に適合していることを証明する資料として、システムセキュリティ実装計画書を作成するものとする。 (2)　［略］ ２～３　［略］ ４　システムセキュリティ実装計画書の周知 保護システム管理者は、システムセキュリティ実装計画書を作成又は変更した場合は、これを周知するとともに、システム管理業務に従事

に従事する者以外にシステムセキュリティ実装計画書を配布又は閲覧させないものとする。	する者以外にシステムセキュリティ実装計画書（操作手順書を除く。）を配布又は閲覧させないものとする。
５　［略］	５　［略］
第３　構成管理	第３　構成管理
１　セキュリティエンジニアリングの原則の適用 防衛関連企業は、保護システムの設計、開発、導入及び変更する場合において、セキュリティエンジニアリングの原則を適用するものとする。	１　セキュリティエンジニアリングの原則の適用 防衛関連企業は、保護システムの設計、開発、導入及び変更する場合において、セキュリティエンジニアリングの原則（情報システムの企画から設計、開発、運用に至るまでのすべての工程において、セキュリティを確保する方策をいう。）を適用するものとする。
２～４　［略］	２～４　［略］
第４～第５　［略］	第４～第５　［略］
第６　識別及び認証　［略］	第６　識別及び認証　［略］
１　識別及び認証等の実施	１　識別及び認証等の実施
(1)～(2)　［略］	(1)～(2)　［略］
(3)　パスワードによる認証の実施	(3)　パスワードによる認証の実施
ア～ウ　［略］	ア～ウ　［略］
エ　［略］	エ　［略］
(ｱ)　大文字英字、小文字英字、数字及び特殊文字をそれぞれ１文字以上使用した１４文字以上であり容易に推測されないものであること	(ｱ)　大文字英字、小文字英字、数字及び特殊文字のうち３種類以上使用した１０文字以上であり、容易に推測されないものであること。
(ｲ)　定められた期間以内に変更すること。	削除
(ｳ)　世代にわたって同じパスワードを使用しないこと。	削除
(ｴ)　紙等への記載又は記憶媒体への保存（オに規定する場合を除く。）が行われていないこと。	(ｲ)　紙等への記載又は記憶媒体への保存（オに規定する場合を除く。）が行われていないこと。
オ～カ　［略］	オ～カ　［略］
２　［略］	２　［略］
第７～第１２　［略］	第７～第１２　［略］