装装保第１３５８４号
令和７年７月１４日

（宛先別記）　殿

防衛装備庁装備政策部装備保全管理課長
（公印省略）

装備品等及び役務の調達における情報セキュリティ確保のための措置に係るシステムセキュリティ実装計画書及び事業計画の提出様式について（通知）

標記について、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のための措置の細部事項について（装装保第４２０８号。令和５年３月１４日）第１２項の規定に基づき、システムセキュリティ実装計画書及び事業計画の提出様式を別紙様式第１及び別紙様式第２のとおり定め、令和７年９月１日から適用することとしたので通知する。

添付書類：別紙様式第１、別紙様式第２
配布区分：長官官房総務官、長官官房人事官、長官官房会計官、長官官房監察監査・評価官、長官官房各装備開発官、長官官房艦船設計官、装備政策部装備政策課長、プロジェクト管理部事業計画官、技術戦略部技術戦略課長、調達管理部調達企画課長、調達事業部需品調達官、航空装備研究所管理部総務課長、陸上装備研究所総務課長、艦艇装備研究所総務課長、新世代装備研究所総務課長、防衛イノベーション科学技術研究所総務・会計ユニット長、各試験場副場長

宛先

大臣官房会計課長
防衛大学校総務部会計課長
防衛医科大学校事務局経理部経理課長
防衛研究所企画部総務課長
統合幕僚監部総務部総務課長
統合幕僚監部指揮通信システム部指揮通信システム企画課長
陸上幕僚監部監理部会計課長
陸上幕僚監部装備計画部装備計画課長
海上幕僚監部総務部経理課長
海上幕僚監部装備計画部装備需品課長
航空幕僚監部総務部会計課長
航空幕僚監部装備計画部装備課長
情報本部総務部総務課長
情報本部総務部会計課長
防衛監察本部総務課長
北海道防衛局総務部会計課長
北海道防衛局調達部調達計画課長
東北防衛局総務部会計課長
東北防衛局郡山防衛事務所長
北関東防衛局総務部総務課長
北関東防衛局総務部会計課長
北関東防衛局装備部装備企画課長
北関東防衛局宇都宮防衛事務所長
南関東防衛局総務部会計課長
南関東防衛局調達部装備課長
近畿中部防衛局総務部総務課長
近畿中部防衛局総務部会計課長
近畿中部防衛局調達部装備課長
近畿中部防衛局舞鶴防衛事務所長
東海防衛支局会計課長
東海防衛支局装備課長
東海防衛支局岐阜防衛事務所長
中国四国防衛局総務部総務課長
中国四国防衛局総務部契約課長
中国四国防衛局総務部会計課長
中国四国防衛局調達部装備課長

中国四国防衛局玉野防衛事務所長
九州防衛局総務部総務課長
九州防衛局総務部会計課長
熊本防衛支局総務課長
長崎防衛支局総務課長
沖縄防衛局総務部総務課長
沖縄防衛局総務部会計課長
沖縄防衛局調達部調達計画課長

別紙様式第１

システムセキュリティ実装計画書

20　　年　　月　　日提出

企業名

基本情報

（　　年　月　日現在）

提出企業名	
本社所在地	
資本金	
従業員数	
事業内容	
事業計画で申請した新基準切替日	無　　・　　有　　（新基準対応完了見込時期：　　年　月　日）
規則類の承認	無　　・　　有　　（確認通知番号･発簡日　又は予定日：　　号　年　月　日）
基盤強化法の申請	申請有　・　申請無　（経費率適用：有　・　無）
ＤＳＧの利用	無　　・　　有　　（　　年　月　日 以降）
保護システム名	システム （稼働開始予定　　：　　年　月　日 ） （保護すべき情報の取扱開始予定：　　年　月　日※）

※稼働開始予定日と異なる場合は分けて記載

改版履歴

版数	日付	作成・更新箇所	作成・更新理由	作成・改版者 （保護システム管理者）	承認者 （総括者）	承認者 （経営者等）

1. 本書の目的

当社は、本書において、当社の保有する保護システム（　　システム）の利用開始にあたり、当該システムが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（以下「セキュリティ基準」という。）および同・第９（保護システムについての管理策）で規定する付紙であるシステムセキュリティ実施要領（以下「実施要領」という。）第２に基づくシステムセキュリティ実装を実施し、セキュリティ基準に適合していることを防衛省に証明する。

2. 企業情報

ア　当社

企業名	
住所	
電話番号	

イ　下請負者に該当する企業

下請負企業名	
住所	
電話番号	

3. 責任者情報

ア　経営者等

氏名	
会社名	
所属	
役職名	
住所（勤務先）	
電話番号	
メールアドレス	

イ　総括者

氏名	
会社名	
所属	
役職名	
住所（勤務先）	
電話番号	
メールアドレス	

ウ　管理者

氏名	
会社名	
所属	
役職名	
住所（勤務先）	
電話番号	
メールアドレス	

エ　保護システム管理者

氏名	
会社名	
所属	
役職名	
住所（勤務先）	
電話番号	
メールアドレス	

オ　管理責任者

氏名	
会社名	
所属	
役職名	
住所（勤務先）	
電話番号	
メールアドレス	

4. 保護システムの概要

(1) 基本情報

保護システム名	用途

(2) 取扱環境区分

取扱環境区分		該当する取扱環境（✓を入力）
①	外部ネットワーク接続あり環境	
②	外部ネットワーク接続なし環境（企業内ネットワーク等）	
③	スタンドアロン	
④	DSG	

(3) 構成要素

付紙様式第１_ハードウェア・ソフトウェア一覧のとおり。

(4) ネットワーク構成概要

5. 保護すべきデータの取り扱い概要

（1）基本情報

業務内容	説明

（2）データフロー図概要

6. 情報セキュリティ特約の各要求事項への適合状況

付紙様式第２_適合チェックリストのとおり。

7．実施要領　第 2 に規定する文書等について

実施要領の第 2.1（2）に規定する文書等の作成状況 **7．実施要領　第 2 に規定する文書等について**

第 2.1 （2）に規定する文書等	文書等の名称
ア．ベースライン構成設定	
イ．ブラックリスト又はホワイトリスト	
ウ．構成設定目録	
エ．操作手順書	
オ．アクセス制御方針	
カ．保護システムにおけるモバイルコード及び VoIP 技術の利用に係る要件	
キ．保護システムにおける各種のオフィス機器の利用に係る要件	
ク．保護システムのセキュリティを確保するための組織体制図	
ケ．保護システムのネットワーク構成図	
コ．保護すべきデータのデータフロー図	

□　上記文書等は、防衛省の求めがあった場合には提出可能な状態で当社にて保管しています。

８．取扱施設等について

取扱施設等の概要は以下のとおり。

以　上

【保護システム名】

ハードウェア・ソフトウェア一覧

改版履歴

Revision	日付	更新内容			
		対象シート	更新内容	更新者(保護システム管理者)	承認者(総括者)

ハードウェア一覧

ハードウェア情報						
No.	種別	用途	メーカー名称	機種、型番	OS（端末、サーバー等）	機器名称
1						
2						
3						
4						
5						

ソフトウェア一覧

ソフトウェア情報							ソフトウェア 管理情報		ソフトウェア ユーザ登録情報		
No.	ソフトウェア名称	種別	用途	メーカー名称	バージョン	インストール機器	管理部署	管理者氏名	登録者氏名	登録区分 (法人/個人)	ライセンス数
1											
2											
3											
4											
5											

【保護システム名】

適合チェックリスト

改版履歴

Revision	日付	更新内容			
		対象シート	更新内容	更新者(保護システム管理者)	承認者(総括者)

保護システム_基準・実施要領の適合チェックリスト（Ver1.0）

取扱環境区分　：

→ **企業記入欄（白抜きの行）**

No.	防・規則	条項	防・情報セキュリティ基準に関する解説①②の該当箇所 https://www.mod.go.jp/atla/cybersecurity.html	確認項目・ポイント（以下に示す要求を達成するためのルール、手順、体制、環境を整備しているか）（カッコ内に記載される数字＜必要な期間等＞は目安として記載：解説を参照）	対応ステータス	対応箇所（システム実装計画書）	対応箇所（J列：社内ドキュメントの名称、またはJ列以外のシステム実装計画書）	対応内容（システム実装計画以外の場合は、記載内容を抜粋または要約）	入力日	最終更新日	備考
	情報セキュリティ基準	第4 情報セキュリティ基本方針等									
	情報セキュリティ基準	第4.1	第4 情報セキュリティ基本方針等	企業は、情報セキュリティ基本方針等の作成及び変更について、以下のことを定め、実施していること。							
1	情報セキュリティ基準	第4.1	解説①-p1	情報セキュリティ基本方針等（情報セキュリティ基本方針、同規則、同実施手順）を作成した後、防衛省による提出・確認まで終わっているか（防衛省から確認済みである旨の発簡文書を受領したか）。							
2	情報セキュリティ基準	第4.1	解説①-p1	情報セキュリティ基本方針等は、経営者等が承認しているか（同基本方針は総括者、同規則は管理者、同実施手順は保護システム管理者が作成する事を想定）。							
	情報セキュリティ基準	第6 保護すべき情報の管理									
	情報セキュリティ基準	第6.1	第6 保護すべき情報の管理	企業は、保護すべき情報の分類について以下のことを定め、実施していること。							
3	情報セキュリティ基準	第6.1	解説①-p6	保護すべき情報やデータとそれ以外の情報等を明確に区別できるように分類して管理しているか。							
	情報セキュリティ基準	第8 物理的及び環境的セキュリティ									
	情報セキュリティ基準	第8.2	物理的及び環境的セキュリティ	経営者等および管理責任者は、取扱施設等に対する物理的セキュリティ対策について以下のことを定め、実施していること。							
4	情報セキュリティ基準	第8.2	解説①-p14	経営者等は、保護すべき情報を取り扱える物理的範囲を画定し、取扱施設と関係施設を指定しているか。							
5	情報セキュリティ基準	第8.2	解説①-p14	経営者等は、取扱施設内に保護システムを設置し、取扱施設内で保護すべき情報を取扱うようにしているか。							
6	情報セキュリティ基準	第8.2	-	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しているか。							
	情報セキュリティ基準	第8.4	物理的及び環境的セキュリティ	保護システム管理者は、保護システムに対する物理的セキュリティ対策について以下のことを定め、実施していること。							
7	情報セキュリティ基準	第8.4	解説①-p18	保護システムを構成するハードウェア及び記憶媒体の不正な移動及び持ち出しを防止する措置を講じているか（施錠したラック等に設置、ワイヤーでの固定、入退の境界の金属探知器等）。							
8	情報セキュリティ基準	第8.4	解説①-p18	保護システムに接続された送配線は、情報窃取を目的とした加工や切断を防ぐための対策をしているか。							
	情報セキュリティ基準	第9 保護システムの管理策									
	情報セキュリティ基準	第9	保護システムについての管理策	企業は、保護システムの管理策について以下のことを定め、実施していること。							
9	情報セキュリティ基準	第9	解説①-p20	本基準及びシステムセキュリティ実施要領から保護システムに必要な管理策を盛り込んだ、情報セキュリティ実施手順を作成しているか。							
	情報セキュリティ基準	第10 情報セキュリティ事故等への対応									
	情報セキュリティ基準	第10.1	情報セキュリティ事故等への対応	企業は、情報セキュリティ事故等対処計画について以下のことを定め、実施していること。							
10	情報セキュリティ基準	第10.1	解説①-p21	保護システムと接続可能な全ての情報システムを分析・精査（システムログ等）し、原因特定しているか（または、できるようにしているか）。							
	システムセキュリティ実施要領	第2 システムセキュリティ実装計画書									
	システムセキュリティ実施要領	第2	第2 システムセキュリティ実装計画書	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の作成等について以下のことを定め、実施していること。							
11	システムセキュリティ実施要領	第2	解説②-p1	**b. 保護システムで実装すべき本チェックリストの該当項目（非該当を除く項目）が全て対応済になっているか。**							
12	システムセキュリティ実施要領	第2	解説②-p2	e. 経営者等の承認を得ているか。また、変更時は経営者等の承認を得ることにしているか（総括者を介して承認を得ているか）。							
	システムセキュリティ実施要領	第3 構成管理									
	システムセキュリティ実施要領	第3.2	第3 構成管理	保護システム管理者は、ベースライン構成設定について以下のことを定め、実施していること。							
13	システムセキュリティ実施要領	第3.2	解説②-p3	保護システムの構成要素（ハード、ソフト、記憶媒体、ネットワーク）のベースライン構成設定（基準となる設定内容）は、保護システム管理者が定め、総括者の承認を得ているか。							
14	システムセキュリティ実施要領	第3.2	解説②-p3	ベースライン構成設定は、情報セキュリティ基本方針等と整合的であり、保護システム構成要素の機能及び動作を業務遂行上の必要最小限に制限したうえで、保護システムのセキュリティを確保しているか。							
15	システムセキュリティ実施要領	第3.2	解説②-p4	構成設定を実施するための物理・論理的なアクセス権限は、必要最小限に限定し、必要最小限のふさわしい者に限定して使用することにしているか。							
16	システムセキュリティ実施要領	第3.2	解説②-p4	構成設定は、安全でない、もしくは不要なプログラム、ポート、プロトコルを実行不可（無効化含む）としているか。							
17	システムセキュリティ実施要領	第3.2	解説②-p5	ブラックリスト又はホワイトリストは、構成要素毎に作成しているか。保護システム管理者とユーザで利用するソフトが異なる場合は、ユーザー権限毎に禁止/許可しているソフトが分かるようにリストを作成しているか。ブラックリストは実行不可、ホワイトリストは該当プログラムのみ実行可としているか。定期的（年１回以上）または構成要素に変化・変更が生じた場合に精査、更新しているか。							
	システムセキュリティ実施要領	第3.3	第3 構成管理	保護システム管理者は、ベースライン構成設定の変更等の手順を作成し、以下のことを定め、実施していること。							
18	システムセキュリティ実施要領	第3.3	解説②-p6	ベースライン構成設定の変更、および、特別（例外的）な構成設定は、当該構成設定の内容が本基準や情報セキュリティ基本方針等に反しないことを保護システムのセキュリティに及ぼす影響を事前に分析し、確認してから実施しているか。							
	システムセキュリティ実施要領	第3.4	第3 構成管理	企業および保護システム管理者は、構成設定に係る記録及び保存について以下のこと定めていること。							
19	システムセキュリティ実施要領	第3.4	解説②-p7	保護システム管理者は、構成要素・設定に係る現状（最新の状態）を確認・証明できるよう構成設定目録を作成しているか。							
20	システムセキュリティ実施要領	第3.4	解説②-p7	構成設定目録には構成要素ごとに保護システム管理者が指定した責任者等を記載しているか。							
	システムセキュリティ実施要領	第4 保護システムの基本的防御									
	システムセキュリティ実施要領	第4.1	第4 保護システムの基本的防御	企業は、保護システムの領域の確定について、以下のことを定め、実施していること。							
21	システムセキュリティ実施要領	第4. 1	解説②-p8	保護システムにおける保護すべき情報を扱う領域を定め、企業内ネットワーク（イントラネット）、外部ネットワークとの境界に物理的又は論理的に制御可能な措置を行っているか。							
	システムセキュリティ実施要領	第4.2	第4 保護システムの基本的防御	保護システム管理者は、保護システムの操作手順書について以下のことを定め、実施していること。							
22	システムセキュリティ実施要領	第4.2	解説②-p8	保護システムの利用者向けの手順、セキュリティ上の遵守事項を記載した操作手順書を作成し、総括者の承認を得ているか。							
23	システムセキュリティ実施要領	第4.2	解説②-p8	操作手順書は、保護システム利用者が保護システムを利用する際はいつでも参照が可能であるか。							
	システムセキュリティ実施要領	第4.3	第4 保護システムの基本的防御	企業は、保護すべきデータの暗号化について以下のことを定め、実施していること。							
24	システムセキュリティ実施要領	第4.3	解説②-p9	保護すべきデータを保護システム及び可搬記憶媒体に保存する場合は、暗号化しているか。							
25	システムセキュリティ実施要領	第4.3	解説②-p9	データの暗号化は電子政府推奨暗号等を使用しているか（防衛省から指示があればそれに従う）。							
26	システムセキュリティ実施要領	第4.3	解説②-p9	暗号鍵を厳格に管理しているか（時間の経過等によって関係者外に鍵が漏洩しない対策が採られていること。鍵を扱う利用者の制限、定期的な鍵の変更および過去の鍵の管理等が十分であること等）。							
	システムセキュリティ実施要領	第4.4	第4 保護システムの基本的防御	保護システム管理者は、その他の基本的防御対策について以下のことを定め、実施していること。							
27	システムセキュリティ実施要領	第4.4	解説②-p10	保護システムにソフトウェアをインストール又はアップデートする場合は、予め有効性・副作用の可能性を分析・評価し、セキュリティ上必要かつ適切な場合に限り実施しているか。特に、セキュリティ上のアップデートが必要な場合は速やかにアップデートしているか（アップデートが可能になってから30日以内を目安）。							
28	システムセキュリティ実施要領	第4.4	解説②-p10	保護システムにおけるアプリケーション等の機能は、システム管理者用・利用者用で分離しているか。							
29	システムセキュリティ実施要領	第4.4	解説②-p10	管理者機能の不正利用の防止策を講じているか（管理者権限以外では読み取りや実行ができないように設定等）。							
30	システムセキュリティ実施要領	第4.4	解説②-p11	仮想化技術を利用する場合は、仮想マシン間でのデータの不正又は意図しない移動やデータリソースへのアクセスを防止する措置及び対策をしているか。							
31	システムセキュリティ実施要領	第4.4	解説②-p11	保護システムを外部システムと接続する場合は、接続・使用の安全性を検証し、業務上アクセス権限のない者による意図しないまたは不正な接続、システムの使用、データの漏洩を排除するための管理・制限をしているか。							
	システムセキュリティ実施要領	第5 アクセス制御									
	システムセキュリティ実施要領	第5.1	第5 アクセス制御	企業および保護システム管理者は、アクセス制御方針について以下のことを定め、実施していること。							
32	システムセキュリティ実施要領	第5.1	解説②-p12	保護すべきデータ及び保護システムの論理的アクセスの制御内容（どのユーザがどのデータにどのような操作内容でアクセスする必要があるか等）を明記しているか。							
33	システムセキュリティ実施要領	第5.1	解説②-p12	保護すべきデータ、保護システムにアクセス権限を有する者を、業務上必要最小限に限定しているか。							
	システムセキュリティ実施要領	第5.2(1)	第5 アクセス制御	保護システム管理者およびアカウント管理者は、アカウント管理について以下のことを定め、実施していること。							
34	システムセキュリティ実施要領	第5.2(1)	解説②-p13	アカウント管理者は、業務(一般利用者、システム管理者等の遂行する業務の責任範囲)ごとにアカウントを分離して用意し、それぞれに必要最低限の機能を割当て、適切な使用者にアカウント付与するための計画を作成し、保護システム管理者の承認を得ているか。							
35	システムセキュリティ実施要領	第5.2(1)	解説②-p13、14	アカウント（管理者権限を含む）が付与される者を必要最小限にしているか。また、管理者権限（局所的な管理権限を含む）は、必要なときのみ使用するようになっているか。							
36	システムセキュリティ実施要領	第5.2(1)	解説②-p13	アカウント管理者は、利用者を識別（特定）できるようにアカウントを付与・管理し、利用状況（利用者名、利用開始日時）を記録しているか。							

No.	防・規則	条項	防・情報セキュリティ基準に関する解説①②の該当箇所 https://www.mod.go.jp/atla/cybersecurity.html	確認項目・ポイント（以下に示す要求を達成するためのルール、手順、体制、環境を整備しているか） （カッコ内に記載される数字＜必要な期間等＞は目安として記載；解説を参照）	対応ステータス	対応箇所 （システム実装計画書）	対応箇所 （J列：社内ドキュメントの名称、またはJ列以外のシステム実装計画書）	対応内容（システム実装計画以外の場合は、記載内容を抜粋または要約）	入力日	最終更新日	備考
	システムセキュリティ実施要領	第5.2(2)	第5 アクセス制御	保護システム管理者は、ログオンの管理について以下のことを定め、実施していること。							
37	システムセキュリティ実施要領	第5.2(2)	解説②-p15	保護システムへの連続したログオン失敗を許容する上限回数を設定し、上限を超えた場合の不正アクセス防止対策をしているか（15分以内に4回連続して失敗したら自動的にアカウントロック、自動ロック後30分を目安にロック解除、等）。							
38	システムセキュリティ実施要領	第5.2(2)	解説②-p15	ログオン失敗時にパソコン画面等に不要な情報（ログオン失敗理由等の不正アクセスに有益な情報）を出力表示してないか。							
	システムセキュリティ実施要領	第5.2(3)	第5 アクセス制御	保護システム管理者は、保護システムにログオンしたユーザセッションの管理について以下のことを定め、実施していること。							
39	システムセキュリティ実施要領	第5.2(3)	解説②-p15	非アクティブ（未使用）状態を許容する上限時間（最長30分）を設定し、上限を超えた場合、ユーザセッションをロックするようにしているか（ユーザセッションが不当に奪取されないよう操作画面をロック、スタンバイモードにする、等）。							
40	システムセキュリティ実施要領	第5.2(3)	解説②-p15	保護システム利用者が保護システムから一時的に離れる際は、操作ディスプレイをスクリーンセーバ等で保護する運用としているか。							
41	システムセキュリティ実施要領	第5.2(3)	解説②-p15	保護システム利用者がユーザセッションのロックを解除（利用再開）する際は多要素認証を利用することとしているか。							
42	システムセキュリティ実施要領	第5.2(3)	解説②-p15	保護システム利用者が、ログオフを要求すると自動的にユーザセッションを終了するようにしているか。							
43	システムセキュリティ実施要領	第5.2(3)	解説②-p15	保護システム利用者が、実行していたセッションを終了する場合は、全てのプログラムを終了しているか（常時立ち会うことが困難な長時間の継続実行を要する計算処理等のプログラムは、不正アクセスができない状態で実行しているか）。							
	システムセキュリティ実施要領	第5.2(4)	第5 アクセス制御	保護システムへのリモートアクセス管理について以下のことを定め、実施していること。							
44	システムセキュリティ実施要領	第5.2(4)	解説②-p16	保護システムへのリモートアクセス（ワイヤレス含む）利用は、保護システム管理者が事前に承認する手順になっているか。							
45	システムセキュリティ実施要領	第5.2(4)	解説②-p16	保護システムへのリモートアクセス（ワイヤレス含む）は、必要最小限に制限しているか。							
46	システムセキュリティ実施要領	第5.2(4)	解説②-p16	保護システムへのリモートアクセス（ワイヤレス含む）の通信を、暗号化しているか。							
47	システムセキュリティ実施要領	第5.2(4)	解説②-p16	保護システムへの入り口となる外部との境界を必要最小限としているか。また境界を構成する各機器（VPNゲートウェイサーバ等）でアクセスを必要最小限に制限する設定にしているか（当該境界部分の監視は第8に沿って行う）。							
48	システムセキュリティ実施要領	第5.2(4)	解説②-p16	保護システムへのリモートアクセス（ワイヤレス含む）利用中の端末で、異なる宛先への同時接続をできないようにしているか（スプリットトンネリングの禁止）。							
49	システムセキュリティ実施要領	第5.2(4)	解説②-p16	リモートアクセス（ワイヤレス含む）時の管理者権限の使用を原則禁止しているか。							
	システムセキュリティ実施要領	第6 識別及び認証									
	システムセキュリティ実施要領	第6.1	第6 識別及び認証子	保護システム管理者およびアカウント管理者は、保護システムの識別及び認証等について以下のことを定め、実施していること。							
50	システムセキュリティ実施要領	第6.1	解説②-p17	アカウント管理者は、保護システムの構成機器等の要素に識別可能な識別子（機器や利用者を一意に特定できるホスト名、機器名、ユーザID等）を付与しているか。また保護システム管理者の承認を得ているか。							
51	システムセキュリティ実施要領	第6.1	解説②-p17、18	保護システム利用者の代理として操作する処理（識別子を付与された本人ではない者が業務上の理由で当該識別子＜管理者権限を含む＞を一時利用して代行する作業、処理）は利用証跡（代行した者、内容）を管理しているか。代行する者が正当であることを確認、認証しているか。							
52	システムセキュリティ実施要領	第6.1	解説②-p18	保護システムへのログオンは多要素認証になっているか。							
53	システムセキュリティ実施要領	第6.1	解説②-p18	保護システムへのリモートアクセス時の多要素認証はリプレイ攻撃に耐性があるか（ワンタイムトークン、ワンタイムパスワード等）。							
54	システムセキュリティ実施要領	第6.1	解説②-p18	ログオンする機器が識別子を付与した正当な機器であることを確認、認証しているか。							
55	システムセキュリティ実施要領	第6.1	解説②-p19	アカウント管理者は、保護システム利用者に付与するアカウントの初期パスワードを、アカウント毎に異なる推測されにくい内容で割り当てているか。							
56	システムセキュリティ実施要領	第6.1	解説②-p19	アカウントと初期パスワードの交付は機密性に配慮して配付しているか。初期パスワードを直ちに変更させる措置を講じているか。							
57	システムセキュリティ実施要領	第6.1	解説②-p19	パスワードは、以下の要件を充たしているか。 (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) 紙等への転記、又は記憶媒体への保存が行われていないこと。							
58	システムセキュリティ実施要領	第6.1	解説②-p19	保護システム内で保存・伝送する必要があるパスワード（埋め込みパスワード）は、容易に他者に漏洩しない措置を講じているか（暗号化、ハッシュ化等）。							
59	システムセキュリティ実施要領	第6.1	解説②-p19	パスワードを忘失した際は、無効化・パスワードの再発行の措置を講じているか。							
60	システムセキュリティ実施要領	第6.2	解説②-p20	保護システム管理者は、パスワード以外（IDカード、USBトークン、生体認証など）のその他の認証子による認証についても、十分な強度による方法とし、認証子を格納する機器（IDカード、USBトークン等）は紛失や修理・交換時には無効化する等、不正アクセスがないよう厳格に管理しているか。							
	システムセキュリティ実施要領	第7 通信の制御									
	システムセキュリティ実施要領	第7.1	第7 通信制御	企業および保護システム管理者は、通信の制御について以下の措置及び手順を定めていること。							
61	システムセキュリティ実施要領	第7.1	解説②-p21	保護システムが外部ネットワークと通信する場合は、これらの境界に機器を設置し、必ず当該境界を経由して通信しているか。							
62	システムセキュリティ実施要領	第7.1	解説②-p21、22	外部との境界に設置した機器（FW等）で、必要な通信以外を拒否する設定としているか。							
63	システムセキュリティ実施要領	第7.1	解説②-p21	外部との境界にサブネットワーク（DMZ)を設置し、ネットワークを分断する設定としているか。また、外部から保護システム向けの通信が必要な場合は、当該サブネットワーク内に外部向けに保護システムを代理するサーバ（プロキシサーバ）を設置して、外部から保護システムが直接アクセスされないように通信を遮断しているか（不特定多数の者がアクセス可能なWebサーバーを保有する場合等）。							
64	システムセキュリティ実施要領	第7.1	解説②-p21	外部との境界にインターフェース（VPNゲートウェイ等）を設置し、リモートアクセス（ワイヤレス含む）を管理しているか。							
	システムセキュリティ実施要領	第7.2	第7 通信制御	企業および保護システム管理者は、通信データ及び通信セッションの保護について以下の措置及び手順を定めていること。							
65	システムセキュリティ実施要領	第7.2	解説②-p22	保護すべきデータの通信は、実施要領に沿ってセキュリティが確保され、業務上必要最小限に制限しているか。							
66	システムセキュリティ実施要領	第7.2	解説②-p22	保護すべきデータは保護システム以外との通信を禁止しているか。やむを得ず通信が必要な場合は、防衛省の許可を得ることとしているか。							
67	システムセキュリティ実施要領	第7.2	解説②-p22	取扱施設外との通信は全て暗号化しているか（データまたは通信経路の暗号化）。							
68	システムセキュリティ実施要領	第7.2	解説②-p23	保護システムの通信セッションを保護しているか（セッション終了時は関係するネットワーク接続等の処理を全て終了しているか、非アクティブ時はの30分を目安に自動切断しているか）。							
69	システムセキュリティ実施要領	第7.2	解説②-p23	保護システムと外部システムとの通信セッションは、電子証明書等で通信相手が正当であることを確認（なりすまし防止）しているか。							
	システムセキュリティ実施要領	第7.3	第7 通信制御	保護システム管理者は、通信機能の利用制限について以下のことを定め、実施していること。							
70	システムセキュリティ実施要領	第7.3	解説②-p24	保護システムでモバイルコードの利用が必要な場合、悪用されないよう利用条件を定めて適切に制限しているか（保護システム管理者による利用条件の設定、利用承認）。							
71	システムセキュリティ実施要領	第7.3	解説②-p24	保護システムでVoIP技術の利用が必要な場合、悪用されないよう利用条件を定めて適切に制限しているか（保護システム管理者による利用条件の設定、利用承認）。							
72	システムセキュリティ実施要領	第7.3	解説②-p24	保護システムでオフィス機器の利用が必要な場合、悪用されないよう利用条件を定めて適切に制限しているか（保護システム管理者による利用条件の設定、利用承認）。また、以下a.b.の措置を講じているか。 a. リモートアクセス（遠隔やワイヤレス経由のオフィス機器の接続・起動・操作）を不許可としているか。 b. オフィス機器が起動していることが外形的に分かる表示をしているか。							
	システムセキュリティ実施要領	第8 システム監視									
	システムセキュリティ実施要領	第8.1	第8 システム監視	企業は、システム監視実施について以下のことを定め、実施していること。							
73	システムセキュリティ実施要領	第8.1	解説②-p25	保護システムの内部、保護システムと外部ネットワークとの境界、それぞれにおいて異常検知のためのシステム監視をしているか。以下a.～d.の必須監視項目を監視対象としているか。 a. 不正な相手方、不正な方法等によるアクセス b. 利用者権限、管理者権限の不正な使用 c. 保護システム内部、保護システムを宛先／送信元とする不正な通信 d. 悪意のあるコードの保護システムへの侵入							
	システムセキュリティ実施要領	第8.2	第8 システム監視	企業および保護システム管理者は、システム監視の実施方法について以下のことを定め、実施していること。							
74	システムセキュリティ実施要領	第8.2	解説②-p26	システムログ（第9）を利用し、システム上の挙動を常時監視して不正を検知しているか。							
75	システムセキュリティ実施要領	第8.2	解説②-p26	不正アクセスを検知した場合は、アラートを保護システム管理者、担当者に通知するよう保護システムに設定しているか。							
76	システムセキュリティ実施要領	第8.2	解説②-p26	内部の兆候、外的な状況変化に関する情報を収集・分析し、システム監視体制や監視範囲を適切に調整しているか。							
77	システムセキュリティ実施要領	第8.2	解説②-p27	不正な通信の監視では、保護システムを宛先／送信元とする通信トラフィックを常時監視して不正を検知しているか。							
78	システムセキュリティ実施要領	第8.2	解説②-p27	不正な通信の監視では、保護システムへのローカル接続を常時監視して不正を検知しているか。							

No.	防・規則	条項	防・情報セキュリティ基準に関する解説①②の該当箇所 https://www.mod.go.jp/atla/cybersecurity.html	確認項目・ポイント（以下に示す要求を達成するためのルール、手順、体制、環境を整備しているか） （カッコ内に記載される数字＜必要な期間等＞は目安として記載；解説を参照）	対応ステータス	対応箇所 （システム実装計画書）	対応箇所 （J列：社内ドキュメントの名称、またはJ列以外のシステム実装計画書）	対応内容（システム実装計画以外の場合は、記載内容を抜粋または要約）	入力日	最終更新日	備考
79	システムセキュリティ実施要領	第8.2	解説②-p27	不正な通信の監視では、保護システムへのネットワーク接続を常時監視して不正を検知しているか。							
80	システムセキュリティ実施要領	第8.2	解説②-p27	不正な通信の監視では、保護システムへのリモート接続（デバイス接続）を常時監視して不正を検知しているか。							
81	システムセキュリティ実施要領	第8.2	解説②-p27	不正な通信の監視では、保護システムへのリモートアクセス（ログイン接続）を常時監視して不正を検知しているか。							
82	システムセキュリティ実施要領	第8.2	解説②-p27	悪意のあるコードの検知では、パターンマッチング手法やヒューリスティックエンジン等を利用したマルウェア対策ソフトウェアをインストールしているか。							
83	システムセキュリティ実施要領	第8.2	解説②-p27	悪意のあるコードの検知では、不正／脆弱性検知ソフトウェア（パターンファイル等）を速やかにアップデートしているか。							
84	システムセキュリティ実施要領	第8.2	解説②-p27	悪意のあるコードの検知では、マルウェア対策ソフトウェアで保護システムを定期的にフルスキャン)をしているか（1週間に1回以上、1 週間以上電源が切られていた場合は起動時直後）。							
85	システムセキュリティ実施要領	第8.2	解説②-p27	悪意のあるコードの検知では、マルウェア対策ソフトウェアで保護システムのファイル操作をリアルタイムスキャンしているか。							
	システムセキュリティ実施要領	第8.4	第8 システム監視	企業および保護システム管理者はシステム監視により取得した情報の利用及び保管について以下のことを定め、実施していること。							
86	システムセキュリティ実施要領	第8.4	解説②-p28	システム監視で取得した情報（ログ、記録等）は、改ざん・漏洩・盗取・消失防止のために暗号化・施錠等の措置をとったうえで、間断のない証跡を十分な期間保管しているか（契約履行後少なくとも3年）。							
	システムセキュリティ実施要領	第9 システムログ									
	システムセキュリティ実施要領	第9.1	第9 システムログ	保護システム管理者は、システムログの取得及び分析について以下のことを定め、実施していること。							
87	システムセキュリティ実施要領	第9.1	解説②-p29	保護すべきデータに対する操作証跡ログを保護システム利用者毎に自動的に取得しているか。							
88	システムセキュリティ実施要領	第9.1	解説②-p29	保護システム担当者は、取得するログの対象・内容・方法について保護システム管理者の承認を得ているか。							
89	システムセキュリティ実施要領	第9.1	解説②-p29	ログ取得に失敗した場合は保護システム担当者等にアラートを発報しているか。							
	システムセキュリティ実施要領	第9.2	第9 システムログ	保護システム管理者は、システムログの管理について以下のことを定め、実施していること。							
90	システムセキュリティ実施要領	第9.2	解説②-p31	システムログ取得・分析のために保護システムの設定を行う者を限定してアクセス権限を付与しているか。							
	システムセキュリティ実施要領	第9.3	第9 システムログ	保護システム管理者は、システムログにタイムスタンプを付与する要領に関し以下のことを定め、実施していること。							
91	システムセキュリティ実施要領	第9.3	解説②-p32	システムクロックを利用して、ログにタイムスタンプを付与しているか。							
92	システムセキュリティ実施要領	第9.3	解説②-p32	システムログのタイムスタンプの時刻表記を日本標準時を基準として統一しているか（JSTが困難である場合はUTC、GMT等で統一し、保護システム内・保護システム間で時刻の誤認・混同がないようにしているか）。							
93	システムセキュリティ実施要領	第9.3	解説②-p32	保護システムのシステムクロックは、外部機関が提供する正確な時刻を同期することで、時刻ずれが起きないようにしているか。							
	システムセキュリティ実施要領	第10 脆弱性スキャン等									
	システムセキュリティ実施要領	第10.1	第10 脆弱性スキャン等	保護システム管理者は、脆弱性スキャンについて以下のことを定め、実施していること。							
94	システムセキュリティ実施要領	第10.1	解説②-p33	定期的（月1回以上）に保護システム全体に脆弱性スキャンを実施しているか。							
	システムセキュリティ実施要領	第11 バックアップ									
	システムセキュリティ実施要領	第11	第11 バックアップ	保護システム管理者は、バックアップの手順において以下のことを定め、実施していること。							
95	システムセキュリティ実施要領	第11	解説②-p35	バックアップは、全ての保護すべきデータ及び必要なシステムデータを対象としているか。							
96	システムセキュリティ実施要領	第11	解説②-p35	バックアップデータは少なくとも次回のバックアップまで保存しているか。							
97	システムセキュリティ実施要領	第11	解説②-p35	バックアップの頻度は、定期的に実施し、自社の定める目標復旧時間を考慮して設定しているか。							
98	システムセキュリティ実施要領	第11	解説②-p35	バックアップデータの機密性・完全性、可用性を保護しているか（バックアップデータを保管する拠点や場所を保護しているか）。							
99	システムセキュリティ実施要領	第11	解説②-p35	バックアップ手順を定めているか（バックアップデータを利用した復旧手順を含むこと）。							
	システムセキュリティ実施要領	第12 システムメンテナンス等									
	システムセキュリティ実施要領	第12.1	第12 システムメンテナンス等	保護システム管理者は、システムメンテナンス等計画について以下のことを定め、実施していること。							
100	システムセキュリティ実施要領	第12.1	解説②-p36	定期的ないしは必要に応じ保護システムのメンテナンス（保守、点検、アップグレード等）を行っているか。また、保護システムのメンテナンス計画は管理責任者と調整して作成し、総括者の承認を得ているか。							
101	システムセキュリティ実施要領	第12.1	解説②-p36	保護システムをメンテナンスのために取扱施設外に持ち出す場合、保護システムから取外す場合、それぞれの手順を定めているか（必要な承認、保護すべきデータを削除・退避しておく措置・手順を用意しているか）。							
102	システムセキュリティ実施要領	第12.1	解説②-p36	保護システムのリモートメンテナンス時が必要な場合について、メンテナンス体制や手法に応じて保護すべきデータを保全する措置・手順を用意しているか。							
	システムセキュリティ実施要領	第12.2	第12 システムメンテナンス等	保護システム管理者は、システムメンテナンス等の実施について以下のことを定め、実施していること。							
103	システムセキュリティ実施要領	第12.2	解説②-p37	メンテナンス要員は、保護システム管理者が保護システム利用者の中から、必要最小限に制限して指定しているか。							
	システムセキュリティ実施要領	第12.3	第12 システムメンテナンス等	保護システム管理者は、システムメンテナンスの記録について以下のことを定めていること。							
104	システムセキュリティ実施要領	第12.3	解説②-p39	システムメンテナンスの監督者は、メンテナンス作業内容（日時、事業者の名称・所在、作業員、作業内容等）を記録し、管理責任者、保護システム管理者はこれらを確認しているか。							

別紙様式第２

事業計画

20　　年　　月　　日提出

企業名

１．本書の目的

当社は、保護すべき情報を取り扱うために「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」が付された契約を履行するに際して、「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」（以下「本基準」という。）に従って必要な措置を取るべきところ、自らが保有する設備等の改修に時間を要する等の理由により直ちに本基準に従って保護すべき情報を取り扱うことが困難であるため、その理由及び本基準に従った取扱いを行うことができる時期について申請する必要があり、その際に、本基準に従って保護すべき情報を取り扱うために必要な設備等の改修等に係る事業の計画について、本書をもって確認いただくものである。

２．責任者情報

ア　契約責任者

氏名	
会社名	
所属	
役職名	
住所（勤務先）	
電話番号	
メールアドレス	

イ　事業計画責任者

氏名	
会社名	
所属	
役職名	
住所（勤務先）	
電話番号	
メールアドレス	

３．契約内容、旧基準適用の理由、新基準の適用時期等

契約名	
要求元	
契約担当官	
契約期間	
保護情報取扱開始時期	
取扱事業所名等	
契約内容	
旧基準適用の理由 **(特約条項第９条第１項)**	
新基準の適用時期	令和　年　　月　　日
経費率算定企業	
防衛生産基盤強化法申請	
ＤＳＧ加入	

４．保護すべき情報（対象契約の情報セキュリティ指定書から転記）

保護すべき情報	保護すべき情報の詳細	企業で取り扱う際の留意事項	備考

５．契約履行に必要な保護システム

取扱環境区分　（現状）

①		紙媒体のみ閲覧
②		スタンドアロン
③		外部ネットワーク接続なし
④		外部ネットワーク接続あり
⑤	―	ＤＳＧ

（新基準適用後）

―	紙媒体のみ閲覧
	スタンドアロン
	外部ネットワーク接続なし
	外部ネットワーク接続あり
	ＤＳＧ

（１）現状（旧基準適用）

（２）新基準適用後

６．契約履行に必要な施設

（１）現状（旧基準適用）

現状での施設実態を記入する（旧基準適用状況を✓で確認する）	
	取扱施設があること
	取扱施設について入退管理できること
	「保護すべき情報」は取扱施設の中でのみ利用･保管すること

（２）新基準適用後

新基準対応で求める施設の条件を満たすこと（✓で確認する）		
	取扱施設と関係施設があること（隣接または同範囲内にある）	
		保護情報を取り扱う全ての場所が特定されていること
		取扱施設の全ての出入口を特定していること
		関係施設の全ての出入口を特定していること
		これらの出入口が詳細レイアウトに明記されていること
	取扱施設について入退管理で個人を特定すること	
		入退者を入退管理機器等で許可された者のみに制限すること
		入退時に監視カメラで個人特定を補完できること
		これらの入退管理が全ての出入口について行われていること
	関係施設の外側境界に入退口を設置し、必要な管理措置により入退者を制限すること	
	「保護すべき情報」は取扱施設の中でのみ利用･保管すること	
	外部から「保護すべき情報」を覗かれないこと	
	外部から入退室口以外から侵入できないこと	

７．新基準適用までのスケジュール

８．概算費用

規　則		
取扱施設		
システム		

以 上