4　現在の状況等

保護すべき情報の取扱い（現状）	□　取り扱っていない。 （取扱開始予定時期：＿＿＿年＿＿＿月） □　紙媒体のみで取り扱っている。 □　スタンドアロン端末で取り扱っている。 □　外部ネットワーク（防衛セキュリティゲートウェイを除く。以下同じ。）や社内の情報システムに接続しないＬＡＮ環境で取り扱っている。 □　外部ネットワークや社内の情報システムに接続したＬＡＮ環境で取り扱っている。
保護すべき情報の取扱い（特定取組実施後の予定）	□　スタンドアロン端末で取り扱う。 □　外部ネットワークや社内の情報システムに接続しないＬＡＮ環境で取り扱う。 □　外部ネットワークや社内の情報システムに接続したＬＡＮ環境で取り扱う。
システムセキュリティ実装計画書（注１）	□　防衛省に提出済み （提出日：＿＿年＿＿月＿＿日・提出先機関：　　） □　防衛省に提出予定 （提出予定時期：＿＿＿年＿＿＿月）
サイバーセキュリティ強化を行うための脆弱性の調査結果概要等（注２）	
防衛セキュリティゲートウェイの利用状況	□　利用している。 □　利用予定である。（予定時期：＿＿＿年＿＿＿月頃） □　利用の申込みをしている。 □　利用の申込みを検討又は予定している。 □　利用予定はない。 利用しない理由： （　　）

（注１）「システムセキュリティ実装計画書」とは、装備品製造等事業者が、自社が保有し、又は使用する保護システム（保護すべき情報を取り扱う情報システムをいう。）について、自社の情報セキュリティ基本方針等に規定する措置を適切に実施し、防衛省が定めた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「防衛産業サイバーセキュリティ基準」という。）に適合していることを証明する資料として、当該事業者が作成したものを指す。

（注２）脆弱性調査の結果概要とサービス名称を記載し、必要に応じパンフレット等を添付すること。

5　特定取組の目的、見込まれる効果等

特定取組の目的（注１）	「防衛産業サイバーセキュリティ基準」において関連する項番号（注２）
□　組織的セキュリティの強化 □　物理的及び環境的セキュリティの強化 □　システムセキュリティの強化 □　脆弱性調査 □　その他	

見込まれる効果等（注３）

（注１）該当する項目全てにチェックをすること。

（注２）「防衛産業サイバーセキュリティ基準」において関連する項番号を全て記載すること。

（注３）取組の詳細（具体的取組、導入する機器・ソフトウェア、サービス等）・規模（取組の対象となる端末・アカウント・職員等の数）、実施体制等を明記すること（別添を可とする。）。

（注４）防衛セキュリティゲートウェイの利用に係る特定取組を実施する場合は、申請者自身の負担で実施するものについてのみ記載すること。

（注５）保護システム領域を防衛事業・民間事業共用で利用する場合は、経済合理性その他の理由を明記すること。

（注６）特定取組の内容を補足する参考資料がある場合は、当該資料を添付すること。