「防衛装備品製造過程等におけるサイバーセキュリティ対策強化事業」への参加希望企業における情報セキュリティ体制の強化に係る事業計画書の作成要領

令和４年７月

公益財団法人　防衛基盤整備協会

1　はじめに

「防衛装備品製造過程等におけるサイバーセキュリティ対策強化事業」とは、防衛関連中小企業の情報セキュリティ対策の強化策等の試行・評価等を行うことで、防衛装備品に関する情報漏えい防止及びサイバーセキュリティ対策の負担が大きいサプライチェーン維持のため、新情報セキュリティ基準の適用を見据えた効果的な施策の導入の資を得ることを目的とするものです。本事業に参加を希望する企業は、自社の情報セキュリティ体制の現状と課題、当該事業への協力のために本年度において実施を計画する情報システムに係る強化策の試行や従業員に対する教育訓練、５年度以降において実施する見込みの対応策等について記載した「事業計画書」を作成し、参加申込書と併せて提出していただく必要があります。本ペーパーは、「事業計画書」の作成の仕方について説明したものです。

（1）対象：

防衛省との間で防衛装備品の調達等に係る契約の実績がある企業又は今後新たに防衛省との契約に参入することを検討している企業のうち、防衛装備品の製造、維持・整備に携わる中小企業に該当するもの（原則として「日本標準産業分類（平成 25 年 10 月改訂）」の分類上の製造業に属するもので、その他（自動車整備、機械等修理、技術サービス等）の場合は個別に判定いたします）。

（中小企業基本法における中小企業者の定義
製造業その他：　資本金の額又は出資の総額が３億円以下の会社又は常時使用する従業員の数が３００人以下の会社及び個人）

（2）申請期間：

募集要領に記載の募集開始から参加企業が事業の予算上の上限に達するまで（終了時には当協会のウェブサイトで公表）

（3）応募手続：

所定の申込書に必要事項を記載し、事業計画書（本ペーパー別紙様式１）及び所要の添付資料とともに、当協会にメール又は郵送で提出する。

（4）相談窓口（事業計画書の作成に関するお問い合わせはこちらにお願い致します。）：

公益財団法人防衛基盤整備協会　情報セキュリティ部内　事務局
（営業時間：　８：３０～１７：１５（土日、祝日除く））
メールアドレス：　csa2022@bsk-z.or.jp、　電話番号：　03-3358-8704
担　当：　岡田、六畑、小島

Ⅱ　記入要領

（1）企業名（業種）

○　貴社の名称を記入してください。

○　（業種）は、【　　】内に「日本標準産業分類（平成２５年１０月改訂）」の分類項目名により該当するものを記入の上で、防衛省・自衛隊の装備品関連の製造実績がある場合は（　　）内にその内容を簡単に記入してください。

○　［防衛省との情報セキュリティ特約の付された契約締結の実績］は、実績がある場合は、その直近の年度を記入し、無い場合は「なし」と記入してください。

（2）情報セキュリティ体制の現状

①　情報セキュリティ規則類の有無

部内の役職員等を対象とした、情報セキュリティの基本方針、情報の管理方法、物理的・環境的・技術的情報セキュリティ対策、情報セキュリティ事故への対応等につき規定した規則類（規則、規程、通達、要領等、名称は問わず）を定めている場合はその名称を、定めていない場合は「無し」と記入してください。

②　情報セキュリティ体制

社内の情報セキュリティに係る管理及び運用についての責任者として、次のような役割を担う者を任命している場合は、その者の組織上における役職名（例：情報担当取締役、総務部長、システム課長、ネットワーク管理室長等）を、任命していない場合は「無し」と記入してください。

・情報セキュリティ総括責任者：　社内の全ての情報セキュリティに係る管理及び運用についての総括的な責任者
・情報システム管理責任者：　社内における全ての情報システムに係る管理及び運用についての責任者
・情報資産管理責任者：　貴社が保有する全ての情報資産に係る管理及び運用についての責任者
・その他（特別な役割を担う者を任命している場合に記載）：（例）ネットワーク管理責任者（社内の情報ネットワークの管理及び運用についての責任者）

③　情報セキュリティ教育訓練の実績

役職員を対象とした以下のような情報セキュリティに係る教育訓練を実施している場合は直近における実施内容を簡単に、実施していない場合は「無し」と記入してください。

教育	情報セキュリティ責任者・担当者	情報システム管理や情報セキュリティ事案対処等に係る専門的な教育（部外委託を含む）
	一般の役職員	情報セキュリティに関する基礎的な注意事項等の教育（採用時教育の一環、部外委託のｅラーニング等）
訓練	情報セキュリティ責任者・担当者	情報セキュリティ事案への対処要領等に係る実地訓練（部外委託を含む）
	一般の役職員	標的型攻撃メール訓練（部外委託を含む）

④　情報セキュリティに関する監査の実績

情報セキュリティに関して部内の監査員による又は部外の監査組織に委託しての監査（情報セキュリティ規則類の遵守状況、情報システムの運用状況、情報セキュリティインシデントの有無等）につき、実施している場合は、「部内の監査員により業務監査の一部として実施」、「部内の監査員により特別監査として実施」、「部外の監査組織により業務監査の一部として実施」、「部外の監査組織により特別監査として実施」等のように記入し、実施していない場合は、「未実施」と記入してください。

（3）情報セキュリティ上の課題として認識している事項

一般的に企業における情報セキュリティ上の課題としては、以下のようなものが想定されます。これを参考にして、貴社における情報セキュリティ上の課題で特に重要と考えられるものを３点（可能であれば、複数の分野の課題に係るもの）を目途として記入してください。

組織的課題	○情報セキュリティに係る基本方針や規則類が定められていない（内容が古くて最新の情勢に対応できていない） ○情報セキュリティに係る責任者や担当部署が明確に定められていない。 ○情報セキュリティ対策のためにかけられる資源（経費、人材等）が不十分である。
人的課題	○情報セキュリティに係る専任の担当者がいない（専任の担当者はいるが、必ずしも十分な専門的知識を有していない又は業務が多忙で十分な対応ができていない）。 ○従業員に対して、就業規則や個別契約を通じて十分な守秘義務を課していない（知り得た秘密の取扱いにつき制約なし、制約はあるが罰則による担保なし等）。 ○従業員に対して、情報セキュリティに係る必要事項等について適時の教育を実施していない（一般の従業員は入社時以降教育の機会なし、座学のみで実際の対応を体験する訓練の機会無し等）。
物理的・環境的課題	○就業場所への立入状況の管理（入退出者及び日時の記録、第三者の立入制限等）ができていない。 ○重要な情報の保管・取扱場所が指定されていない。 ○重要な情報や情報システムの保管・設置場所について、特段のアクセス制限が実施されていない（無関係の者が自由に近づける、個人所有の情報機器の持ち込み・仕様が無制限である等）

技術的課題	○情報システムに関するアクセス管理が不十分である（アクセス制御方針が決められていない、アクセス権限の付与状況が統一的に把握されていない、退職・異動に伴うアクセス権限の変更が随時実施されていない等） ○システム利用者によるパスワード設定ルールが定められていない（設定の文字数・種類、変更周期、再使用可能な世代数等）。 ○セキュリティ対策機能やソフトウェア等を最新の状態に維持することがルール化されていない。 ○情報システムにおける防護措置（ＵＴM機器の設置、端末へのウイルス対策ソフトの導入等）が実施されていない。 ○情報システムの状況について、定期的なログの取得・分析や脆弱性診断等によって監視・確認する態勢ができていない。 ○無許可の情報システム機器や個人所有の情報システム機器の社内情報ネットワークへの接続の有無が把握できていない。 ○社外で情報システム機器を使って業務を行う場合（テレワーク等）のルールが定められていない。
その他の課題	○重要情報の取扱いを委託する委託先企業との間で、その取扱い要領や守秘義務、漏えい時の賠償責任等について規定した契約を結んでいない。 ○情報セキュリティに係るインシデント（重要情報の漏えい、紛失、棄損等）が発生した場合の対応手順や関係者の役割等が明確に定められていない。 ○業務継続計画の中に情報セキュリティインシデント発生後の対応について定められていない。

（4）情報システムに係る強化策の実証

○　５年度から施行される予定である防衛省の「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（「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」（以下「新情報セキュリティ基準」という。）への対応を見据えて、情報セキュリティ体制を強化するため、情報システムに係る強化策の実証として実施を計画している施策について記入していただきます。

○　対象となる強化策は、次のいずれかになります。

①　当協会があらかじめ準備した次の４種類の施策の中から選択する場合（各施策の細部については別添の資料を参照。）

ア　ＥＤＲ（Endpoint Detection and Response）用機器及び監視等サービスの導入：　ＣＹＢＥＲＧＹM社の「Ｘ－ＳＯＣ」サービスを導入して、ネットワークに接続されている端末機器（PC、サーバー、スマートフォン等）の操作や動作の常時監視を行い、サイバー攻撃の兆候を早期に発見して不審なプログラムやプロセスの停止、ネットワークの切断等の初動対処を速やかに実施し、被害の拡大を防ぐ。	マルウェア等の内部ネットワークへの侵入を前提とした防護策 ←新基準「保護システムの基本的防御」に対応
イ　高度な手法を活用可能なウイルス対策ソフトウェアの導入：　米海軍で使用実績のあるウイルス対策ソフトウェアである「AppGuard」を対象企業のエンドポイント（ＰＣ）に導入することで、アプリケーション等の動作を監視し、不正な命令の可能性があると判断した場合はその実効を阻止することで、情報漏えい等の問題の発生を防止する。	マルウェア等の内部ネットワークへの侵入を前提とした防護策 ←新基準「保護システムの基本的防御」に対応

ウ　セキュアなクラウドサービスの活用：　新情報セキュリティ基準が参考にしている米国の情報セキュリティ基準である NIST　SP800-171 に対応した機能を有する Exostar 社のアプリケーション（FedRAMP 中位レベルと同等）を活用した富士通（株）のクラウドサービスである「ＦＵＪＩＴＳＵ　ＮＩＳＴ対応トラステッドコネクトサービス」を導入し、新情報セキュリティ基準に適応した形で安全かつ円滑に重要情報の処理・格納・伝送を実施する。	クラウドサービスの利用拡大を前提とした防護を含む対応策 ←新基準「アクセス制御、構成管理、識別及び認証、通信制御、システム監視、セキュリティ監査等」に対応
エ　ファイルの暗号化：　DataClasys 社の中小企業向けファイルセキュリティシステムである「DataClasys」を導入し、サーバーやＰＣ中のファイルを暗号化して保存するとともにその利用権限を管理し、権限のあるユーザーにそのままでのアプリケーション等の利用を可能とすることで可用性を維持しつつ、仮にファイルが流出しても権限のない第三者がファイルを開くことができないため重要情報の漏えいを防止する。	ファイル流出の可能性を前提とした防護策　←新基準「保護システムの基本的防御」に対応

上記の４つの中から、実施を希望するものを原則１つ選択（特に希望する場合は２つまで選択可）して、記入してください。（書き方は、「○○○○○○（導入する施策の名称）を試行的に導入し、●●●●●●●●●●●●●●●●（検証する内容）を検証する。」という形式のイメージです。下記のサンプルを参考にしてください。）

○　端末へのＥＤＲ用機器及び監視サービスを試行的に導入して、サイバー攻撃の兆候を早期に発見して初動対処を速やかに実施する体制の社内における有効性及び継続運用の実施可能性につき検証する。 ○　高度な手法を活用可能なウイルス対策ソフトウェアを試行的に導入し、サイバー攻撃の実行を阻止して情報漏えい等の発生を未然に防止する体制の社内における有効性及び継続運用の実施可能性につき検証する。 ○　セキュアなクラウドサービスを試行的に導入し、オンプレミスの場合に比して情報の処理・格納・伝送等や情報セキュリティに係る対応等に係る運用上の効果・効率性や負担の程度等につき検証する。 ○　ファイルの暗号化システムを試行的に導入し、サイバー攻撃に対するその有効性、暗号化されたファイルの運用上の可用性及び社内における継続運用の実施可能性につき検証する。

② ①以外の施策で実施を希望する場合

新情報セキュリティ基準に対応して情報セキュリティ体制を強化するための施策として、次に列記する項目に係るもので①以外のものの実施を希望される場合は、以下のア及びイの要件を満たすことが必要となります。これらの要件を満たした上で①以外の施策の実施を希望される場合は、具体的な施策の内容及び期待される効果について記入してください。

【対象項目】

○設備・機器の導入、　　○ソフトウェアの導入、　　○データ暗号化サービスの利用、 ○ＮＯＣ（Network Operation Center）やＳＯＣ（Security Operation Center）等のデータ・トラフィック／ネットワーク・ログ監視サービス利用、 ○セキュアクラウドサービスｎ利用、　　○その他サイバーセキュリティ対策強化に有用と認められるもの

【必要要件】

ア　本事業における実証の一つとして実施する場合は、①の事業と同様に、当協会が同施策のための器材やサービスの提供事業者と契約して、貴社内においてそのご協力の下で必要な機材やサービスを用いた実証試験として実施いたします。この場合は、あくまで防衛省の調査研究事業の一環として実施しますので、本年度末に事業が終了する時点で、使用していた器材等は全て撤去いたします。(経費的に全てを貴社の自己資金で実施する場合は、そのような制約はなく、試行のために導入したツール及びその成果物は全て参加企業に帰属いたします。その場合は、本事業の実施成果をとりまとめる際の参考とするため実施成果について情報提供頂ければ幸いです。)

イ　施策については、新情報セキュリティ基準への対応に資するものであることが必要であり、基本的に次の【対象となり得る施策】のいずれかに該当するものとします（これらに該当しないもの、例えば、基本ソフト（ＯＳ）のアップデートや一般的なインターネットセキュリティ対策ソフトのインストール等、防衛関連企業に通常求められてきた一般的な強化策にとどまるようなものについては対象外とし、疑義があるものについては当協会でヒアリング等を実施の上で個別に適否を審査いたします。)。

【対象となり得る施策】

高度な手法を活用可能なウイルス対策ソフトウェアの導入	特定・防御だけでなく検知・対応機能まで備えたものであれば可とする
イントラネット、外部ネットワークとの境界で保護システムを防護する境界防護機器（ＵＴＭ等）の導入	保護システムを外部と接続するためにその境界に新たに設置されたものであれば可とする
電子政府推奨暗号等を採用し、暗号鍵を厳格に管理可能なデータ暗号化ツールの導入	可とする
多要素認証ツールの導入（ネットワークアクセス時は、加えてリプレイ攻撃に耐性のある方式）	可とする
許可された通信以外を拒否するプロキシサーバ等の導入	新基準対応との関係が説明できれば可とする
不正なアクセス等への速やかな対応を可能にするシステム常時監視サービス等の導入	可とする
脆弱性スキャンツールの導入	可とする
取扱施設への入退管理がＩＤカードのみの場合、取扱施設へのアクセス制御機器（監視カメラ等）の導入	可とする
役割と責任に応じた取扱者等への教育訓練の実施	新基準対応のために一般の教育訓練と区別された内容であれば可とする
情報セキュリティ事故等対処テストの実施	新基準対応のために新たに取り入れられた内容であれば可とする

○　なお、希望されました施策（②を全て自己資金で実施する場合を除く。）の実施の可否については、その目的である実施成果の検証の可否や期待される効果（施策の組み合わせによっては効果の検証が困難となる場合があるため）、全体の予算の制約、参加企業間の公平性等を考慮して、当協会内の選定委員会で審議の上で決定いたしますので、必ずしも希望どおりにならない場合がありますことをご承知おきください。

（5）人材の育成・確保のための施策

①　本協会は参加企業の全てを対象として次のような教育訓練の実施を計画しております。（各施策の細部については別添の資料を参照。）

区　分	実　施　内　容	対象者
集合教育	情報セキュリティの責任者及び情報システム管理者・利用者を対象として、サイバー攻撃の現状やインシデント発生時における対応等についての集合教育及び理解度確認テストを実施し、必要な一般的及び専門的な知識を付与するとともに、爾後に実施する管理者訓練の効果の向上を図る。	各責任者等
ｅラーニング	参加象企業の一般従業員に対して、標的型メール訓練の実施後に、ＧＳＸ社の IT セキュリティｅラーニングサービスを利用して、情報セキュリティ上の留意事項等について教育を実施し、同訓練の有効性の確認及びセキュリティ意識の向上による知識の習熟度の向上を図る。	一般従業員
システム管理者訓練	参加企業のＩＴ部門、セキュリティ部門、セキュリティアナリストを対象として CyberGym 社が提供する「セキュリティ部門・IT 部門向けトレーニング」を実施し、実際のサイバー攻撃を体験して、複数の検出・監視ツールを駆使してサイバーインシデントを検出し、その初期分析を行うためのスキルを修得する。	各責任者等
標的型メール訓練	全ての従業員を対象としてＧＳＸ社の標的型メール訓練をｅラーニングの実施前後に実施し、一般従業員のセキュリティ意識レベルを確認するとともに、弱点となる部門や教育を強化すべき部門等のリスクの可視化により、爾後の情報セキュリティ対策を強化すべきターゲットを明確化して対策に反映する。	一般従業員

②　一般従業員に対して、情報セキュリティに関する意識向上や基礎的な知見を付与するため、あらためて所要の教育訓練（①の教育訓練を含む。）を実施する計画がある場合は、それについて具体的に記入してください。

計画がない場合（①を実施する必要がないと判断される場合を含む）は、その理由を記入してください。

（記入例）

- 既に全従業員に対して定期的に情報セキュリティに係る教育を実施する態勢をとっており、あらためて新しい制度を実施する必要性があるとは考えない。
- 業務が極めて多忙で、教育を受けさせている時間的余裕がない。

③　情報セキュリティ担当者や情報システム管理者の要員を、ア．社内において既存の従業員の中から新たに任命し、所要の教育訓練（①の教育訓練を含む。）を実施する等により育成する、イ．部外から新たに専門的知見を有する者を採用する等によりあらためて育成・確保する計画がある場合は、それについて具体的に記入してください。

計画がない場合は、その理由を記入してください。

（記入例）

・　情報セキュリティ担当者３名、情報システム管理者及びその補助者２名を確保しており、いずれも十分な専門的知見を有するため、あらためて特段の措置を実施する必要性はないと考えている。

・　情報セキュリティ担当者も情報システム管理者も、人員が限られる中で業務が極めて多忙で、教育訓練を受けさせている時間的余裕がない。

（６）その他の対応

①　現状把握・評価

本協会は参加企業の全てを対象として、情報セキュリティ体制の現状把握・評価のため、次の措置を実施することを予定しております。

ア　参加企業から提供を受けた文書類（情報セキュリティ規則、組織図、取扱施設図面、情報セキュリティ教育実施結果、情報セキュリティ監査結果等）を審査するとともに、情報システム管理者や情報セキュリティ担当者等からヒアリングを行い、並行して関係者を対象としたアンケートによる意識調査を実施することで、主に組織的・人的・物理的なセキュリティ上の問題点（リスク）を洗い出す。

イ　技術的なセキュリティ上の問題点を可視化するため、専用のツール及び専門家によるセキュリティ診断（以下の２種類）を実施して、参加企業の情報システムに内在する脆弱性を明らかにする。

・ＣＹＢＥＲＧＹＭ社の「脆弱性診断サービス」により参加企業の情報システムのネットワークやプラットフォーム、Ｗｅｂアプリケーションにつき不具合の有無を診断する。

・コーネットソリューションズ者による Picus 社製の「セキュリティデバイス防御診断サービス」を実施し、参加企業のネットワークに接続されているセキュリティデバイスがどの程度サイバー脅威を防御できるかをシミュレーションする。

これら以外に情報セキュリティ体制の現状把握のために、次のいずれかの施策の実施を希望される場合は、その旨（及び（iii）を希望する場合には具体的な施策の内容及び期待される効果）を記入してください。

（ｉ）情報資産リスク評価（(漏えい・滅失した場合による影響度の深刻度や、損害賠償対応や訴訟費用等の金銭的な影響度を含む。）

これを実施する場合は、保有する情報資産の洗い出し及び「情報資産管理台帳」台帳への記載（名称、管理者、保管場所、利用者、媒体等）を貴社に実施していただく必要がございます。

（ii）ペネトレーションテスト（侵入テスト）

（iii）その他、情報セキュリティ体制の現状評価に有用と認められるもの

②　その他

（４）（５）及び（６）①以外に情報セキュリティ体制の強化のため本年度に実施を計画している施策がございましたら、具体的に記入してください（事例として一般的に想定されるものは、以下のようなものが考えられますので、ご参考にしてください）。

特段実施する計画がなければ、「無し」と記入してください。

【想定される事例】

○　情報セキュリティ規則類を見直し、防衛省の新情報セキュリティ基準に対応するように改正を行う。

○　社内に情報セキュリティについての専門部署を設立する。

○　情報システムにおける脆弱性診断の結果を踏まえて、システム管理業者に委託してセキュリティホールの解消等のための改修措置を実施する。

（7）経費見積り

①（4）（5）で記入した施策関連

ア　当協会が準備して提供するものについては、下記のとおり記入してください。

・端末へのＥＤＲ用機器及び監視サービスの導入の実証:　サービス導入初度経費及び対象期間中の運営経費　約〇〇〇万円（本事業で負担予定）

・高度な手法を活用可能なウイルス対策ソフトウェアの導入の実証：　導入初度経費及び対象期間中の運営経費　約〇〇〇万円（本事業で負担予定）

・セキュアなクラウドサービスの導入の実証：　導入初度経費及び対象期間中の運営経費　約△△△万円（本事業で負担予定）

・ファイルの暗号化システムの導入の実証：　導入初度経費及び対象期間中の運営経費　約△△△万円（本事業で負担予定）

・ｅラーニング及び標的型メール訓練、集合教育及びシステム管理者訓練の実施経費：　実施経費　約□□万円（本事業で負担予定）

この他、集合教育及びシステム管理者訓練への参加者旅費について、当協会が指定する実施予定場所までの見積り金額（概数）を計算して記入してください。

イ　ア以外の施策で実施を希望するものについては、その機器・サービスの提供事業者から見積りを取得し、その金額を記入するとともに、当該見積りを添付してください（見積りを取得することが困難な場合は、当協会の相談窓口に御相談してください）。

（記入例）

・ウイルス対策ソフトウェアの更新：16,000 円／３台・３年　×５セット＝　80,000 円

・脆弱性スキャンツールの導入：50,000 円×10ＩＰ分＝500,000 円

②（6）で記入した施策関連

ア　当協会が準備して提供するものについては、下記のとおり記入してください。

・脆弱性診断サービスの実施　：　準備及び実施経費　約〇〇万円（本事業で負担予定）

・セキュリティデバイス防御診断サービスの実施　：　準備及び実施経費　約△△万円（本事業で負担予定）

イ　脆弱性診断結果を踏まえてシステム管理業者にシステム改修を委託する場合は、既に管理を依頼している業者がいる場合は、相談して仮置きの見込み額を記入してください。定まった業者がいない場合は、使用している情報システムがオンプレミスのサーバー＋端末でネットワークを構成しているシステムの場合は「約 500,000 円（仮置き）」と、スタンドアロンのシステムの場合は「約 100,000 円（仮置き）」と記入してください。

ウ　その他の施策で経費（人件費を除く）が発生するものは、その内容及び見込み金額（見積りが取れないものは仮置きのもので可）を記入してください。

③　人件費関連

貴社の人件費の標準単価（〇〇〇〇〇円／人日）に次の人数及び日数を掛けて算出した金額の合計額を記入してください。

ア　事業に係る協力業務の担当者分

〇人　×　１８日（説明会参加１日、ヒアリング・アンケート対応（準備含む）４日、脆弱性診断等対応（準備含む）６日、実証用機器等の設置対応（準備含む）３日、機器の撤収対応（準備含む）２日、成果報告２日）

イ　集合教育・システム管理者訓練への参加者分

□人　×　３日（集合教育１日、システム管理者訓練２日）

④　合計

①から③の合計金額を記入し、更に企業負担分がある場合は、その後に（うち企業負担分）として、①アの本事業が負担予定の金額を除いた金額を記入してください。

（８）５年度以降において実施する見込みの対応策

①　本年度において本事業の経費負担で実施する対策（（４）の情報システムに係る強化策の実証及び（５）の教育訓練）のうちで、実施結果により有効性が確認された場合には５年度以降において自社負担で引き続き実施することを想定しているものがある場合は、その旨を記入してください（記入の仕方のイメージは、以下のとおりです。）。

〇　端末へのＥＤＲ用機器及び監視サービス（高度な手法を活用可能なウイルス対策ソフトウェア、セキュアなクラウドサービス、ファイルの暗号化システム）の導入について、４年度における実証の結果、その有効性が確認されかつ自社での運用が可能と判断された場合には、同種のサービスを自社負担で継続して実施する。 〇　一般社員を対象としたｅラーニング及び標的型メール訓練については、４年度の実施によりその有効性が確認できた場合は、経費的に対応可能なサービスを選定しかつ対象者を限定して、自社負担で継続して実施する。 〇　情報システム管理者及び同補助者に対するシステム管理者訓練については、４年度の実施によりその有効性が確認できた場合は、各年度の参加人数を限定して、自社負担で継続して実施する。

②　本年度において自社負担で実施する施策で、実施結果により有効性が確認された場合は、５年度以降において引き続き実施することを想定しているものがある場合は、その旨を記入してください。

（９）添付資料

○　令和３年度決算に係る貸借対照表及び損益計算書（決算期が９月期の場合は、令和２年度決算に係るものを御提出ください。）

○　本事業に関する宣誓・同意書（代表者本人が自署したもの）（本ペーパー別紙様式２を使用）

（別紙様式１）

情報セキュリティ体制の強化に係る事業計画書

１　企業名（業種）	
２　情報セキュリティ体制の現状	
３　情報セキュリティ上の課題として認識している事項	
４　情報システムに係る強化策の試行	
５　人材の育成・確保のための施策	
６　その他の対応	
７　経費見積り	
８　５年度以降において実施する見込みの対応策	
９　添付資料	

情報セキュリティ体制の強化に係る事業計画書（記入のイメージ）

1　企業名（業種）	株式会社○○○○【電子回路基板製造業（自衛隊航空機用電子回路の製造)】 ［防衛省との情報セキュリティ特約の付された契約締結の実績：　無し］
2　情報セキュリティ体制の現状	①　情報セキュリティ規則類の有無（名称：○○○○情報セキュリティ管理規則） ②　情報セキュリティ体制（総括責任者：有（総務部長)、情報システム管理者：有（○○課長)、情報資産管理者：無し） ③　情報セキュリティ教育訓練の実績：入社時教育の一環として実施 ④　情報セキュリティに係る監査の実績：部内の監査員による業務監査の一部として実施
3　情報セキュリティ上の課題として認識している事項	○　情報システムに関する知見を有する社員が１名しかいないため、平素はシステム管理業務全般に追われて多忙であり、情報セキュリティに関して十分な時間を割けない。また、情報セキュリティに係る最新の知見を修得する時間的余裕もないため、最新の脅威に対応できる十分な能力があるかは疑問である。 ○　情報セキュリティに係る最新の対応策を導入するだけの経費的余裕がなく、端末のＰＣに市販のウイルス対策ソフトをインストールしているだけで、パッチ処理も完全にできているとはいえない。 ○　新入社員時以降は各社員に情報セキュリティに係る教育を実施する機会がなく、個々の社員が情報セキュリティに係る高い意識を持っているとは言い難い状況にある。
4　情報システムに係る強化策の試行	○　端末へのＥＤＲ用機器及び監視サービスを試行的に導入して、サイバー攻撃の兆候を早期に発見して初動対処を速やかに実施する体制の社内における有効性及び継続運用の実施可能性につき検証する。 ○　可能であればセキュアなクラウドサービスを導入し、オンプレミスの場合に比して情報の処理・格納・伝送等や情報セキュリティに係る対応等に係る運用上の効果・効率性や負担の程度等につき検証する。 ○　保護情報を取り扱う場合に保護システムとして運用する予定の情報システムの端末のウイルス対策ソフトウェアを更新する。
5　人材の育成・確保のための施策	○　防衛基盤整備協会（以下「協会」という。）が計画する全社員を対象としたｅラーニング及び標的型メール訓練を受講し、情報セキュリティに係る意識の向上及び必要な知識の付与を図る。 ○　現在の情報システム管理者の他にその補助者２名を指定し、協会が計画する情報セキュリティに係る集合教育及びシステム管理者訓練に参加させて、情報セキュリティ体制のコアとなる人材として育成する。

6　その他の対応	○　情報システムにおける脆弱性診断及びセキュリティデバイス防御診断を実施して、現状把握・評価を行う。 ○　情報システムにおける脆弱性診断の結果を踏まえて、システム管理業者に委託してセキュリティホールの解消等のための改修措置を実施する。 ○　情報セキュリティ規則を見直し、協会の指摘を踏まえ防衛省の新情報セキュリティ基準に対応するよう改正する。
7　経費見積り	○　端末へのＥＤＲ用機器及び監視サービスの導入の試行：　サービス導入初度経費及び対象期間中の運営経費　約○○○万円（本事業で負担予定） ○　セキュアなクラウドサービスの導入の試行：　導入初度経費及び対象期間中の運営経費　約△△△万円（本事業で負担予定） ○　ウイルス対策ソフトウェアの更新：　16,000 円／３台・３年　×５セット＝　80,000 円 ○　ｅラーニング及び標的型メール訓練、集合教育及びシステム管理者訓練の実施経費：　実施経費　約□□　万円（官側が負担予定）、参加者旅費　約 120,000 円 ○　人件費：　30,000 円／人日　×　２１日（説明会参加、ヒアリング・アンケート対応、機器の設置・撤収対応、教育訓練参加等）＝630,000 円 ○　脆弱性診断結果への対応：　システム管理業者へのシステム改修委託経費　約 500,000 円（仮置き） 合計　約○○○万円（うち企業負担分　約 1,130,000 円）
8　５年度以降において実施する見込みの対応策	○　端末へのＥＤＲ用機器及び監視サービスの導入及びセキュアなクラウドサービスの導入について、４年度における試行の結果、その有効性が確認されかつ自社での運用が可能と判断された場合には、同種のサービスを自社負担で継続して実施する。 ○　全システム利用者を対象としたｅラーニング及び標的型メール訓練については、４年度の実施によりその有効性が確認できた場合は、経費的に対応可能なサービスを選定しかつ対象者を限定して、自社負担で継続して実施する。 ○　情報システム管理者及び同補助者に対するシステム管理者訓練については、４年度の実施によりその有効性が確認できた場合は、各年度の参加人数を限定して、自社負担で継続して実施する。
9　添付資料	○令和３年度決算に係る貸借対照表及び損益計算書 ○本事業に関する宣誓・同意書（代表者本人が自署したもの）

（別紙様式２）

令和４年度「防衛装備品製造過程等におけるサイバーセキュリティ対策強化事業」への参加に関する宣誓・同意書

次の１から４までのいずれにも宣誓し、次の５から９までのいずれにも同意します。また、虚偽の宣誓を行った場合又は同意した事項に違反した場合は、防衛基盤整備協会（以下「協会」という。）が本事業への参加企業として採択する前であれば、本事業への参加申請を取り下げ、既に採択して事業を開始していた場合は、協会が当社のために実施した情報セキュリティ体制の現状把握、同体制の強化策の実証や当社の社員を対象とした教育訓練等の実施のために要した経費に相当する金額を返還します。

１　本事業の応募要件を満たしていること。
２　本事業への応募及び採択後の事業への参加の過程で協会の情報セキュリティ強化事業事務局（以下「事務局」という。）からの求めに応じて提供した情報に虚偽のないこと。
３　「暴力団排除に関する特約条項」及び「談合等の不正行為に関する特約条項」について遵守すること。
４　協会が当社に対して本事業に基づく情報セキュリティ体制の現状把握、同体制の強化策の試行、当社の社員を対象とした教育訓練等を実施した後においても、事業を実施する上で求められる情報セキュリティに関する措置を実施する意思があり、必要な措置を継続的に行うこと。
５　本事業における当社と協会との契約内容及び当社において実施された個別具体的な施策の内容が確認できる書類等その他事務局が定める書類等を電磁的記録等により３年間保存するとともに、当該書類のうち事務局が必要と認めるものについて事務局の依頼に応じて速やかに提出すること。
６　事務局が本事業に係る精算行為のために行う関係書類の提出及び関係者へのヒアリング等の依頼に応じること。
７　本事業に不正又は不適当な手段により参加して利得を得た場合は、当該利得に相当する金額の返還等を遅滞なく行う義務を負うこと。
８　本事業の終了後における精算手続等に必要な範囲に限り、提供された情報（個人情報を含む。）や書類等が第三者に提供される場合があること。
９　本事業への参加に関し事務局と締結する契約に従うこと。

令和４年　　月　　日

法人名：　　株式会社　〇〇〇〇〇〇 〇〇〇

代表者の氏名（自署）：　　〇　〇　〇　〇