令和8年11月20日　　支担官第４８６号

支出負担行為担当官
防衛省大臣官房会計課
会計管理官　廣瀬　和希
（公　印　省　略）

公　　告

下記により入札を実施するので、入札心得及び契約条項等を了承の上、参加されたい。

記

１．入札に付する事項

調達番号	件名	内容	履行場所	履行期間
R8-S-0756	サイバー攻撃対処業務における官民連携に係る調査・研究役務	仕様書のとおり	仕様書のとおり	自：契約締結日 至：令和９年３月３１日

２．入札方式　　一般競争入札（総合評価落札方式、電子調達システム（政府電子調達（ＧＥＰＳ））対象案件）

３．入札日時　　令和８年１２月１８日(金)（１１：００）

４．入札場所　　防衛省市ヶ谷庁舎Ｅ２棟３階入札室

５．参加資格　（１）予算決算及び会計令第７０条の規定に該当しない者であること。なお、未成年者、被保佐人又は被補助人であって、契約締結のために必要な同意を得ている者は、同条中、特別の理由がある場合に該当する。
（２）予算決算及び会計令第７１条の規定に該当しない者であること。
（３）令和07・08・09年度防衛省競争参加資格（全省庁統一資格）「役務の提供等」のＣ等級以上に格付けされ、関東・甲信越地域の競争参加資格を有するもの。
（４）防衛省から「装備品等及び役務の調達に係る指名停止等の要領」に基づく指名停止の措置を受けている期間中の者でないこと。
（５）前号により、現に指名停止を受けている者と資本関係又は人的関係のある者であって、当該者と同種の物品の売買又は製造若しくは役務請負について防衛省と契約を行おうとする者でないこと。
（６）上記（３）の等級かかわらず、防衛省所管契約事務取扱細則（平成１８年防衛庁訓令第１０８号）第１８条第４項各号のいずれかに該当する者（具体的には、以下ア～キのいずれかに該当する者）であること。なお、要件に該当する者で入札に参加しようとするものについては、　令和８年１２月３日（木）　１２：００　までに下記ア～キに記載する書類等を防衛省大臣官房会計課契約係へ提出すること。

ア　当該入札に係る物品と同等以上の仕様の物品を製造した実績等を証明できる者

イ　資格審査の統一基準により算定された総合審査数値に以下の技術力の評価の数値を加算した場合に、当該入札に係る等級に相当する数値となる者

項　目	基　準	数　値
入札物品等（訓令第１８条第４項に規定する契約の対象となる物品又は役務をいう。以下同じ）に関連する特許保有件数	３件以上 ２件 １件	15 10 5
入札物品の製造等（訓令第１８条第４項に規定する契約の対象となる物品の製造又は役務の提供等をいう。以下同じ）に携わる技術士資格保有者数	９人以上 ７～８人 ５～６人 ３～４人 １～２人	15 12 9 6 3
入札物品の製造等に携わる技能認定者数（特級、一級、単一級）	11人以上 ９～10人 ７～８人 ５～６人 ３～４人 １～２人	6 5 4 3 2 1

注：１　特許には、海外で取得したものを含む。
　　２　技術士には、技術士と同等以上の科学技術に関する外国の資格のうち文部科学省

令で定めるものを有する者であって、技術士の業務を行うのに必要な相当の知識及び能力を有すると文部科学大臣が認めたものを含む。

ウ　ＳＢＩＲ制度の特定新技術補助金等の交付先中小企業者等であり、当該入札に係る物品又は役務に関する分野における技術力を証明できる者

エ　株式会社産業革新投資機構、独立行政法人中小企業基盤整備機構、株式　会社地域経済活性化支援機構、株式会社農林漁業成長産業化支援機構、株式会社民間資金等活用事業推進機構、官民イノベーションプログラム、株式会社海外需要開拓支援機構、一般社団法人環境不動産普及促進機構における耐震・環境不動産形成促進事業、株式会社日本政策投資銀行における特定投資業務、株式会社海外交通・都市開発事業支援機構、国立研究開発法人科学技術振興機構、株式会社海外通信・放送・郵便事業支援機構、一般社団法人グリーンファイナンス推進機構における地域脱炭素投資促進ファンド事業及び株式会社脱炭素化支援機構の支援対象事業者又は当該支援対象事業者の出資先事業者であり、当該競争に係る物品又は役務に関する分野における技術力を証明できる者

オ　国立研究開発法人（科学技術・イノベーション創出の活性化に関する法律（平成２０年法律第６３号）第２条第９項に規定する研究開発法人のうち、同法別表第３に掲げるものをいう。）が同法第３４条の６第１項の規定により行う出資のうち、金銭出資の出資先事業者又は当該出資先事業者の出資先事業者であり、当該競争に係る物品又は役務に関する分野における技術力を証明できる者

カ　国立研究開発法人日本医療研究開発機構による「創薬ベンチャーエコシステム強化事業（ベンチャーキャピタルの認定）」又は国立研究開発法人新エネルギー・産業技術総合開発機構による「研究開発型スタートアップ支援事業（ベンチャーキャピタル等の認定）」において採択された者の出資先事業者であり、当該競争に係る物品又は役務に関する分野における技術力を証明できる者

キ　グローバルに活躍するスタートアップを創出するための官民による集中プログラム（Ｊ－Ｓｔａｒｔｕｐ又はＪ－Ｓｔａｒｔｕｐ地域版）に選定された事業者であり、当該競争に係る物品又は役務に関する分野における技術力を証明できる者

６．入札方法　　落札決定に当たっては、入札書に記載された金額に当該金額の１０％に相当する額を加算した額（当該金額に１円未満の端数があるときは、その端数金額を切り捨てるものとする。）をもって落札価格とするので、入札者は、消費税等に係る課税事業者であるか免税業者であるかを問わず、見積もった契約金額の１１０分の１００に相当する金額を入札書に記載すること。

７．入札保証金及び契約保証金　　免　除

８．入札の無効　　５の参加資格のない者のした入札または入札に関する条件に反した入札は無効とする。

９．契約書作成の要否　　要

10．適用する契約条項　　役務等契約条項、談合等の不正行為に関する特約条項、
暴力団排除に関する特約条項、

11．その他
（１）細部入札要領については別途配布する「一般競争入札の案内について」（以下、入札案内）のとおり。
（２）入札案内受領の際、資格審査結果通知書（全省庁統一資格）の写しを提示すること。
（３）原則、現に指名停止を受けている者の下請負については認めないものとする。ただし、真にやむを得ない事由を防衛省が認めた場合には、この限りではない。
（４）この一般競争（総合評価落札方式）に参加を希望するものは、応札資料作成要領に定める提出物を　令和８年　１２月　７日（月）　１２：００　までに提出しなければならない。
（５）本案件は、府省共通の「電子調達システム」（https://www.p-portal.go.jp）を利用した応札及び入開札手続により実施するものとする。ただし、電子調達システムによりがたい者は、「紙」による入札書等の提出も可とするが、郵便入札については、令和８年　１２月　１６日（水）までに、下記担当者必着分を有効とする。
（６）落札者が、１０に掲げる契約条項のほか、中小企業信用保険法第２条第１項に規定する中小企業者である場合は、「債権譲渡制限特約の部分的解除のための特約条項」を別途適用する。
（７）入札案内の交付場所、契約条項を示す場所及び問合せ先
〒162-8801　東京都新宿区市谷本村町５－１　（庁舎Ａ棟10階）※顔写真付の身分証明書を持参すること。

受付時間　９：３０～１８：１５（１２：００～１３：００までの間を除く）

また、入札案内のメール配布を希望する者は、以下のとおりメールを送信すること。

メールアドレス：naikyoku_chotatsu_mailmagazine@ib.dss.mod.go.jp
メール件名　　：「件名：○○○」　入札案内送信依頼
添付ファイル　：資格審査結果通知書（全省庁統一資格）の写し
防衛省大臣官房会計課契約係　柴崎　電話　03-3268-3111　内線20824

仕　様　書		
件名	**サイバー攻撃対処業務における官民連携に係る調査・研究役務**	作成年月日　令和８年１１月　９日
		整備計画局サイバー整備課

1　総則

1.1　適用範囲

この仕様書は、防衛省・自衛隊（以下「官」という。）と平成２５年７月に設置したサイバーディフェンス連携協議会の参加企業等（以下「ＣＤＣ参加企業等」という。）によるサイバー攻撃対処業務における官民連携に係る調査・研究役務（以下「本役務」という。）について規定する。

1.2　引用文書等

この仕様書に引用する次の文書は、この仕様書に規定する範囲内において、この仕様書の一部を構成するものであり、入札書又は見積書の提出時における最新版を適用する。

なお、引用文書が定める事項がこの仕様書の内容と異なる場合は、この仕様書の内容が優先する。

a)　引用文書

1)　著作権法（昭和４５年法律第４８号）
2)　サイバーセキュリティ基本法（平成２６年法律第１０４号）
3)　自衛隊法（昭和２９年法律第１６５号）
4)　警察官職務執行法（昭和２３年法律第１３６号）
5)　重要電子計算機に対する不正な行為による被害の防止に関する法律（令和７年法律第４２号。以下「サイバー対処能力強化法」という。）
6)　重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律（令和７年法律第４３号。以下「整備法」という。）
7)　環境物品等の調達の推進に関する基本方針（令和８年２月３日変更閣議決定）
8)　都民の健康と安全を確保する環境に関する条例（平成１２年東京都条例第２１５号）

b)　関連文書

1)　個人情報の保護に関する法律（平成１５年法律第５７号）
2)　防衛省の情報保証に関する訓令（平成１９年防衛省訓令第１６０号）

2　役務の実施に関する要求

2.1　本役務の目的

令和８年１０月１日のサイバー対処能力強化法及び整備法の一部施行を踏まえ、サイバー脅威動向にあわせたサイバー攻撃対処業務を実施することとされている。この際、防衛省・自衛隊を含めた政府全体及び防衛産業の官民連携に寄与する情報提供、報告、共同対処実施要領の整備を行うためのサイバー攻撃対処演習及びワークショップを実施し、課題等について分析、評価及び総括を実施するとともに、欧米主要国の官民連携施策を調査し、これを踏まえた改善提案を行う。

また、国内はもとより、欧米各国等で報告されている攻撃キャンペーンの動向や脅威アクターの攻撃手法への対処方法について、本役務を通して官民で情報共有を行う。

なお、訓練の終了後に最新のサイバー脅威動向（ＡＩ含む）を踏まえた総括を行う。

2.2　実施場所

官の指定する場所とする。

2.3　契約期間

契約締結日から令和９年３月３１日(水)まで

2.4　役務実施事項

2.4.1　実施計画書の作成

契約相手方は、官と調整の上、契約締結後速やかに本役務に係る実施計画書を作成し、官に提出する。実施計画書には本役務の実施体制を記載するものとする。

2.4.2　官側への定期報告

契約相手方は、官と調整の上、実施内容等について、官に本役務の進捗等を適宜報告し、指示を受けること。具体的な報告内容については実施計画書で定める。

2.4.3　サイバー攻撃対処演習の事前教育の実施

契約相手方は、サイバー攻撃対処演習用のプラットフォーム（以下「プラットフォーム」という）をオンプレミス又はクラウド上に準備する。その際、ＣＤＣ参加企業等に対し本番演習の前にサイバー演習の専門家によるプラットフォームの操作教育、教育コンテンツの受講支援及び質疑応答を適宜適切に実施する。また、演習参加者が本番演習においてＡＩの支援を受けた脅威ハンティングを円滑に実施できるよう、事前教育にはプラットフォームの基本操作に加え、ＡＩ機能の利用方法を含む脅威ハンティングの基本操作に関する教育を含めるものとし、全ての演習参加者に対し、演習前にプラットフォームへのログイン及び当該機能の利用ができる環境を整備すること。

2.4.4　サイバー攻撃対処演習の実施

官、ＣＤＣ参加企業等及びその他の公的機関の担当者（以下「演習参加者」という。）を対象としたサイバー攻撃対処演習（参加者は、約５０名程度を基準とし、ＣＤＣ参加企業等に加えて公的機関等の聴講者（見学者）等（２０名程度）が参加するものとする。また、チーム分けは行わないものとする。）を２日間にわたり実施する。なお、当日は円滑な演習進行を図るため支援員（４名以上）を配置するものとする。

また、プラットフォームの安定的な稼働を保証するため、別途プラットフォームの開発元技術者（１名以上）を現地に同席させるものとする。

さらに、演習の実施に当たっては、ＡＩを活用した攻撃（Red チーム機能）及びＡＩの支援を受けた脅威ハンティング（Blue チーム機能）に関する説明を演習参加者及び聴講者（見学者）に対して実施するとともに、演習参加者は実際に当該ＡＩ機能を操作できるものとする。なお、演習の終了後、プラットフォーム開発元の専門家による演習シナリオの解説及び各演習参加者の取組に対する総評（良かった点を含む。）を実施し、必要に応じて通訳を付すものとする。

2.4.5　ＣＤＣ参加企業等に対する事前の資料送付

契約相手方は、官と調整の上、サイバー攻撃対処演習の実施前までに、概要説明資料を演習参加者に送付するものとする。

2.4.6　サイバー攻撃対処演習シナリオの作成

契約相手方は、官と調整の上、サイバー攻撃対処演習において官民の情報共有及び連携、事案対処能力向上に資するシナリオを用意するものとする。この際、サイバー対処能力強化法のほか、整備法の施行によるサイバーセキュリティ基本法、自衛隊法、及び自衛隊法の規定により準用する警察官職務執行法の改正に留意すること。

なお、シナリオについて最新の攻撃キャンペーン（別表に掲げる内容）を参考に、ＡＩを活用した攻撃(Red チーム機能)を必ず含めること。ＡＩの支援を受けた脅威ハンティング（Blue チーム機能）においては、官民連携の演習を主眼とし、国内はもとより米国や欧州各国で報告されている最新の攻撃キャンペーン（別表に掲げる内容）を全て自動で実施できるプラットフォームを使用すること。なお、シナリオの作成にあたっては、官側と事前にと方針について調整すること。

また、企画段階の検討のため、最新の技術動向を反映した複数のシナリオ案（ＡＩによる攻撃や制御系システムに対する攻撃を含む）を企画提案するものとする。

さらに、演習の実効性を高めるため、最新の技術動向を踏まえ、ＡＩを活用

した攻撃（Red チーム機能）の実演及びＡＩの支援を受けた脅威ハンティング（Blue チーム機能）を取り入れたシナリオとし、次に掲げるとおり実施するものとする。

（１）ＡＩを活用した攻撃の実演 演習用プラットフォーム上での攻撃実証実績を有するＡＩ攻撃サービス（Vulnetic 等）又は同等の機能を有し検証済みのツールを用い、脆弱性のあるウェブサーバー等の演習用環境に対する侵害を実演するものとする。

（２）ＡＩの支援を受けた脅威ハンティング 演習参加者は、チーム分けを伴わず、自動攻撃が完了した環境を調査対象として、ＡＩの支援を受けながら、脅威の検知・分析等を実施するものとする。

（３）演習の実施構成 ①１日目は、ＡＩを活用した攻撃の実演を行うとともに、ＡＩの支援を受けた脅威ハンティングに関するハンズオン形式のレクチャー（講義及び操作実習）を実施する。②２日目は、１日目のレクチャーをもとに、演習参加者がＡＩの支援を受けた脅威ハンティングを実践するものとし、調査対象環境は、１日目とは異なる自動攻撃シナリオ又はＡＩによる攻撃が完了した環境とする。

なお、本演習は、リアルタイムで進行する攻撃への即時的対処を求めるものではなく、攻撃が完了した環境を対象として、ＡＩの支援を受けながら脅威の検知・分析・対処に係る実践能力の向上を図ることを目的とする。

2.4.7　サイバー攻撃対処演習の環境

a)　演習用プラットフォーム及びプラットフォーム側ネットワークは、仮想マシンや仮想ネットワーク等の仮想化技術によって構成するものとする。その際、１００台（基準）の仮想マシンでシステムを構築できるものとする。

b)　演習会場並びに演習会場側の端末及びネットワークは官が別途調達する役務（以下「演習支援役務」という。）により準備させたものを使用する。契約相手方は、演習支援役務事業者と密接に連携し、適切な演習環境構築に協力するよう努めること。

なお、端末上に仮想マシンでクライアント環境を構築する場合であっても上記 a)の基準台数に含めないこととする。

c)　プラットフォームをオンプレミスに準備した場合、プラットフォームと演習会場間双方の機器の接続点を責任分界点とする。クラウドに準備した場合、各役務のインターネット接続点を責任分界点とする。

なお、外部のＡＩサービスを利用する場合についても同様に、当該サービスの利用に係るインターネット接続点を責任分界点とし、演習に必要な通信が安定的に確保されるよう努めるものとする。

2.4.8　参加者の意見聴取

官側が主催するワークショップの実施に当たり、ＣＤＣ参加企業等から官民の情報共有及び連携、事案対処能力向上に対しての課題、およびニーズ（ＡＩの利活用に関する課題及びニーズを含む。）について聴取することを目的としたアンケートを官側と調整のうえ作成する。

2.4.9　欧米主要国の官民連携施策の調査

アメリカ合衆国、イギリス、オーストラリア、イタリア、フランス、カナダ及びドイツを含む北大西洋条約機構加盟国のうち３か国以上の官民連携施策を15 事例以上調査すること。また、ＡＩを活用したサイバーセキュリティ施策（ＡＩを活用した脆弱性検査などのサイバーセキュリティ施策に加え、ＡＩからの攻撃を想定した防御の枠組みなどもＡＩ活用が前提とされたサイバーセキュリティ施策として含める)を 10 事例以上調査すること。これら調査結果を次項の改善提案の資とすること。

2.4.10　演習及びワークショップの評価分析

前記2.4.3～2.4.8の実施結果を踏まえ、課題、問題点、改善点の分析を実施するとともに、官民連携に必要な情報提供、報告、共同対処実施要領等の作成及び改善提案を行う。

なお、この際は欧米主要国で実施している官民連携施策について留意し、実効性のある要領となることに努めること。

2.4.11　報告書の作成

契約相手方は、官と調整の上、次年度以降の情報共有の更なる活性化を図るため、官民の情報共有及び連携、事案対処能力向上のための提案等並びにアンケート分析結果の報告を記載した役務実施報告書を作成するものとする。

なお、３月下旬までに報告会を実施し、役務実施報告書について官の承認を得ること。報告会の開催に当たっては、官の指定する場所又は官の指定するＷｅｂ会議システムを使用することとする。

2.5　実施形態

契約相手方は、官と調整の上、官が指定する場所に参加する形態で、サイバー攻撃対処演習を実施することとする。

2.6　費用負担

本役務において用いる資料及び資機材等は、契約相手方の負担とする。

2.7　言語

本役務において作成する資料は、日本語で記載するものとし、日本語以外のものが含まれる場合には、参考文献及び引用文献を除き日本語訳を付けるものとする。

3　契約相手方の要件等

契約相手方は、本役務の実施に当たって次の体制を確保し、これを変更する場合には事前に官側と協議することとする。

3.1　契約相手方の要件

a) 契約相手方は、直近３年以内にＩＴおよびＯＴセキュリティの訓練実績があること。

b) 契約相手方は、直近３年以内に防衛省におけるサイバーレンジを使用したサイバー攻撃対処訓練の実績等を有すること。

c) 契約相手方は、直近３年以内に防衛省以外の官公庁及び独立行政法人を含む公的機関におけるサイバーレンジを使用したサイバー攻撃対処訓練の実績を有すること。

d) 契約相手方は、入札書又は見積書の提出時において有効な情報セキュリティマネジメントシステム（ISO/IEC 27001 又は JIS Q 27001）の第三者認証を有すること。

3.2　役務員の要件

a) 契約相手方は、契約の履行に必要な業務に従事する者（以下「業務従事者」という。）を確保すること。

b) 業務従事者のうち１名以上は、過去１年以内に、防衛省及び防衛省以外の官公庁及び独立行政法人を含む公的機関におけるサイバーレンジに関する教育・演習等の役務に責任者又は責任者に準ずる立場で従事した実績を有すること。

c) 業務従事者のうち１名以上は、防衛省及び防衛省以外の官公庁及び独立行政法人を含む公的機関におけるサイバーレンジに関する教育・演習等の役務に従事した実績を有すること。

d) 上記の業務従事者は、履行に必要若しくは有用な、又は背景となる経歴、知見、資格、語学（母語及び外国語能力）及び業績等を有すること。なお、業務従事者が他の手持ち業務等との関係において履行に必要な業務所要に対応できる態勢にあること。

3.3　第三者に係る取扱い

a) 契約相手方は、本役務に第三者（以下「下請事業者」という。）を従事させる必要がある場合には、あらかじめ、下請事業者の事業者名及び従事者等を届け出た上で、官側の承認を得るものとする。

b) 契約相手方は、本契約の履行に当たり知り得た知識を第三者（下請事業者を除く。）に漏洩又は他に転用しないこと。

4　提出資料等

契約相手方は、**表１**に示す提出資料を防衛省整備計画局サイバー整備課に提出することとする。

表１　提出資料

番号	名称	提出時期	媒体（※）
１	実施計画書	契約締結後速やかに	書面１部、電子媒体１部
２	サイバー攻撃対処演習の概要説明資料（サイバー攻撃対処演習シナリオ含む）	サイバー攻撃対処演習の実施まで（官側との調整による）	書面１部、電子媒体１部
３	役務実施報告書	契約納期まで	書面１部、電子媒体１部

※　電子媒体は、Microsoft Office（Word、Excel 又は Power Point）を用いて作成し、作成したファイルをＰＤＦファイルとしたものと合わせ、契約相手方が用意する電子媒体に保存して提出すること。

5　著作権等

著作権その他の権利は、**別紙**のとおり取り扱うこととする。

6　情報保全

a)　契約相手方は、資料及び物件の取扱いに当たっては細心の注意を払い、官から貸付を受けた資料等について、当該作業後、速やかに返却するものとする。

b)　業務従事者は、業務従事者名簿に記載された者に限定するものとする。

7　その他

7.1　検査

検査は、この仕様書に基づき支出負担行為担当官補助者が行う。

7.2　疑義事項

この仕様書の内容について疑義を生じた場合は、契約担当官等と協議するものとする。

7.3　環境要件

a)　本役務において使用する物品は、環境物品等の調達の推進に関する基本方針（令和８年２月３日変更閣議決定）の基準を満たすものを使用すること。ただし、基本方針の改定があった場合には、これに従うものとする。

b)　本役務において使用する物品の輸送を行うに当たっては、環境に配慮したものとし、自動車を用いる場合は、都民の健康と安全を確保する環境に関する条例（平成１２年東京都条例第２１５号）のディーゼル車規制に適合する

自動車を用いること。なお、官から求められた場合、速やかに自動車検査証を提示すること。

別表

演習用サイバー攻撃が模擬する内容

項	サイバー攻撃者グループ名	参考にする既知の事件	攻撃に使用する技術や行動(実行順は適宜で良い。) ※詳細を調べたい場合、 MITRE ATT&CK (https://attack.mitre.org/)を参照のこと。
1	Volt Typhoon	米国の重要インフラを標的とした一連の攻撃 ※特定の事案ではなく、左記グループによる長期間にわたる一連の事案を指す。.	a)スピアフィッシングリンク:標的型メールに悪意のあるリンクを記載し、当該リンクをユーザーにクリックさせる。 b)システム所有者・ユーザーの検出:攻撃者は、主たる利用者、現在ログイン中のユーザー、当該システムを常用するユーザーの集合、又はユーザーが現在システムを利用しているか否かの特定を試みることがある。例えば、アカウントのユーザー名の取得や資格情報のダンプによってこれを行う。ユーザー及びユーザー名の情報は、実行中プロセスの所有権、ファイル及びディレクトリの所有権、セッション情報、システムログなどシステム全体に広く存在するため、他の検出技術を用いて様々な方法で収集され得る。攻撃者は、自動検出の過程で得た本情報を利用して、標的への感染を完遂するか否か、又は特定の行動を試みるか否かなど、その後の行動を決定することがある。 c)システム情報の検出:攻撃者は、バージョン、パッチ、修正プログラム、サービスパック、アーキテクチャなど、オペレーティングシステム及びハードウェアに関する詳細な情報の取得を試みることがある。攻撃者は、自動検出の過程で得た本情報を利用して、標的への感染を完遂するか否かなど、その後の行動を決定することがある。 d)システムネットワーク構成の検出:攻撃者は、アクセス先のシステム又はリモートシステムの情報収集を通じて、当該システムのネットワーク構成及び設定の詳細を探る可能性が高い。この情報の収集には、Arp、ipconfig/ifconfig、nbtstat、route など、各種のオペレーティングシステム管理ユーティリティが利用され得る。 e)システムネットワーク接続の検出:攻撃者は、現在アクセスしている侵害済みシステム又はリモートシステムについて、ネットワーク経由の問い合わせにより、接続の一覧の取得を試みることがある。 f)権限グループ検出(ローカルグループ):攻撃者は、ローカルシステム又はドメインレベルのグループ及び権限設定の特定を試みることがある。 g)権限グループ検出(ドメイングループ):攻撃者は、ローカルシステム又はドメインレベルのグループ及び権限設定の特定を試みることがある。 h)クエリレジストリ:攻撃者は、Windows レジストリにアクセスし、システム、構成、インストールされているソフトウェアに関する情報を収集することがある。 i)プロセス検出:攻撃者は、システム上で実行されているプロセスに関する情報の取得を試みることがある。取得した情報は、ネットワーク内のシステムで動作している一般的なソフトウェアを把握するために利用され得る。攻撃者は、自動検出の過程で得た本情報を利用して、標的への感染を完遂するか否かなど、その後の行動を決定することがある。 j)セキュリティソフトウェアの検出:攻撃者は、システムにインストールされているセキュリティソフトウェア、構成、防御ツール及びセンサーの一覧の取得を試みることがある。これには、ローカルのファイアウォール規則やアンチウイルスなどが含まれ得る。攻撃者は、自動検出の過程で得た本情報を利用して、標的への感染を完遂するか否かなど、その後の行動を決定することがある。 k)ファイルおよびディレクトリの検出:攻撃者は、ホスト又はネットワーク共有の特定の場所において、ファイルシステム内のファイル及びディレクトリを列挙し、特定の情報を検索することがある。攻撃者は、自動検出の過程で得た本情報を利用して、標的への感染を完遂するか否かなど、その後の行動を決定することがある。

			l)Windows Management Instrumentation(WMI):Windows Management Instrumentation(WMI)は、Windows システムコンポーネントへのローカル及びリモートアクセスのための統合環境を提供する Windows の管理機能である。ローカル及びリモートアクセスには WMI サービス、リモートアクセスにはサーバーメッセージブロック(SMB)及びリモートプロシージャコールサービス(RPCS)を利用し、RPCS はポート 135 で動作する。 m)正当なアカウント(ドメインアカウント):攻撃者は、資格情報アクセスの技術を用いて特定のユーザー又はサービスアカウントの資格情報を窃取したり、初期アクセスを得る手段として、偵察段階でソーシャルエンジニアリングにより資格情報を取得したりすることがある。 n)イベントトリガー実行(WMI イベントサブスクリプション):Windows Management Instrumentation(WMI)は、Windows システムコンポーネントへのローカル及びリモートアクセスのための統合環境を提供する Windows の管理機能である。ローカル及びリモートアクセスには WMI サービス、リモートアクセスにはサーバーメッセージブロック(SMB)及びリモートプロシージャコールサービス(RPCS)を利用し、RPCS はポート 135 で動作する。 o)Web サービスを介した流出(PowerShell 経由):データの流出は、主要なコマンドアンドコントロール(C2)のプロトコル又はチャネルとは異なるプロトコルで行われる。データは、主要な C2 サーバーとは別のネットワーク上の場所へ送信される可能性が高い。別のプロトコルには、FTP、SMTP、HTTP/S、DNS、SMB など、主要な C2 チャネルとして使用されていない任意のネットワークプロトコルが含まれる。異なるチャネルには、クラウドストレージなどのインターネット上の Web サービスも含まれ得る。 p)ツールの持ち込み(イングレスツール転送):攻撃者が使用するツールその他のファイルは、作戦期間中、あるシステムから別のシステムへコピーして配置されることがある。ファイルは、C2 チャネルを通じて外部の攻撃者管理システムから被害者のネットワーク内へ持ち込まれたり、FTP など別のツールによる代替プロトコルを通じて持ち込まれたりすることがある。また、Mac や Linux では scp、rsync、sftp などのネイティブツールを用いてコピーすることもできる。 q)データ操作:攻撃者は、エンドユーザーがデータにアクセスし表示する際のデータを操作するため、システムを改変することがある。実行時データを操作することで、攻撃者は業務プロセス、組織の認識及び意思決定に影響を与えることが可能となる。
2	MirrorFace	日本国内の政治団体・報道機関等を標的とした一連の攻撃 ※特定の事案ではなく、左記グループによる長期間にわたる一連の事案を指す。	a)スピアフィッシングリンク:標的型メールに悪意のあるリンクを記載し、当該リンクをユーザーにクリックさせる。 b)保護されていない資格情報:ソフトウェアの脆弱性の悪用は、攻撃者がプログラム、サービス、又はオペレーティングシステムのソフトウェア若しくはカーネル自体のプログラミングエラーを利用して、攻撃者が制御するコードを実行する場合に発生する。資格情報や認証の仕組みは、有用な資格情報の入手やシステムへのアクセス手続きの回避を目的として、攻撃者の標的となることがある。その一例として、Kerberos を標的とし、ドメインユーザーの権限を用いて Kerberos チケットを偽造できる MS14-068 がある。資格情報アクセスを目的とした脆弱性悪用は、対象となるプロセスや取得した資格情報によっては、権限昇格につながることもある。 c)正当なアカウント(ドメインアカウント):攻撃者は、資格情報アクセスの技術を用いて特定のユーザー又はサービスアカウントの資格情報を窃取したり、初期アクセスを得る手段として、偵察段階でソーシャルエンジニアリングにより資格情報を取得したりすることがある。 d)ツールの持ち込み(イングレスツール転送):攻撃者が使用するツールその他のファイルは、作戦期間中、あるシステムから別のシステムへコピーして配置されることがある。ファイルは、C2 チャネルを通じて外部の攻撃者管理システムから被害者のネットワーク内へ持ち込まれたり、FTP など別のツールによる代替プロトコルを通じて持ち込まれたりすることがある。また、Mac や Linux では scp、rsync、sftp などのネイティブツールを用いてコピーすることもできる。 e)悪意のあるファイル:攻撃者は、実行を得るためにユーザーの特定の操作に依存することがある。

			これは、文書ファイルのアイコンと拡張子を模した実行ファイルを標的型メールの添付ファイルとして送付し、ユーザーに開かせるなど、直接的なコード実行である場合がある。また、標的型メールに記載されたリンクをユーザーがクリックし、ブラウザやアプリケーションの脆弱性の悪用を通じてクライアント実行が行われるなど、他の実行技術につながることもある。攻撃者は、.doc、.pdf、.xls、.rtf、.scr、.exe、.lnk、.pif、.cpl など、ユーザーに実行させる必要がある複数の種類のファイルを用いることがある。 f)DLL サイドローディング:Windows システムは、プログラムに読み込むために必要な DLL を探す共通の方法を使用している。攻撃者は、Windows の DLL 検索順序や、DLL を曖昧に指定しているプログラムを悪用して、権限昇格及び永続化を図ることがある。 g)スケジュールされたタスク/ジョブ(永続化):at や schtasks などのユーティリティ及び Windows タスクスケジューラを用いて、指定した日時に実行されるプログラムやスクリプトをスケジュールすることができる。RPC の利用に必要な認証が満たされ、ファイル及びプリンター共有が有効であれば、リモートシステム上にもタスクをスケジュールできる。リモートシステム上でのタスクのスケジュールには、通常、当該リモートシステムの管理者グループのメンバーであることが必要である。 h)システム情報の検出:攻撃者は、バージョン、パッチ、修正プログラム、サービスパック、アーキテクチャなど、オペレーティングシステム及びハードウェアに関する詳細な情報の取得を試みることがある。攻撃者は、自動検出の過程で得た本情報を利用して、標的への感染を完遂するか否かなど、その後の行動を決定することがある。 i)正当なアカウント(ドメインアカウント):攻撃者は、資格情報アクセスの技術を用いて特定のユーザー又はサービスアカウントの資格情報を窃取したり、初期アクセスを得る手段として、偵察段階でソーシャルエンジニアリングにより資格情報を取得したりすることがある。 j)システム所有者・ユーザーの検出:攻撃者は、主たる利用者、現在ログイン中のユーザー、当該システムを常用するユーザーの集合、又はユーザーが現在システムを利用しているか否かの特定を試みることがある。例えば、アカウントのユーザー名の取得や資格情報のダンプによってこれを行う。ユーザー及びユーザー名の情報は、実行中プロセスの所有権、ファイル及びディレクトリの所有権、セッション情報、システムログなどシステム全体に広く存在するため、他の検出技術を用いて様々な方法で収集され得る。攻撃者は、自動検出の過程で得た本情報を利用して、標的への感染を完遂するか否か、又は特定の行動を試みるか否かなど、その後の行動を決定することがある。 k)プロセス検出:攻撃者は、システム上で実行されているプロセスに関する情報の取得を試みることがある。取得した情報は、ネットワーク内のシステムで動作している一般的なソフトウェアを把握するために利用され得る。攻撃者は、自動検出の過程で得た本情報を利用して、標的への感染を完遂するか否かなど、その後の行動を決定することがある。 l)パスワードストアからの資格情報(Windows 資格情報マネージャー):ソフトウェアの脆弱性の悪用は、攻撃者がプログラム、サービス、又はオペレーティングシステムのソフトウェア若しくはカーネル自体のプログラミングエラーを利用して、攻撃者が制御するコードを実行する場合に発生する。資格情報や認証の仕組みは、有用な資格情報の入手やシステムへのアクセス手続きの回避を目的として、攻撃者の標的となることがある。その一例として、Kerberos を標的とし、ドメインユーザーの権限を用いて Kerberos チケットを偽造できる MS14-068 がある。資格情報アクセスを目的とした脆弱性悪用は、対象となるプロセスや取得した資格情報によっては、権限昇格につながることもある。 m)画面キャプチャ:攻撃者は、作戦期間中に情報を収集するため、デスクトップの画面キャプチャの取得を試みることがある。画面キャプチャ機能は、侵害後の活動で使用されるリモートアクセスツールの機能として含まれていることがある。 n)Web サービスを介した流出(PowerShell 経由):データの流出は、主要なコマンドアンドコントロール(C2)のプロトコル又はチャネルとは異なるプロトコルで行われる。データは、主要な C2 サーバー

			とは別のネットワーク上の場所へ送信される可能性が高い。別のプロトコルには、FTP、SMTP、HTTP/S、DNS、SMB など、主要な C2 チャネルとして使用されていない任意のネットワークプロトコルが含まれる。異なるチャネルには、クラウドストレージなどのインターネット上の Web サービスも含まれ得る。 o)スタートアップフォルダによる永続化:レジストリの「run キー」やスタートアップフォルダにエントリを追加すると、ユーザーのログイン時に参照先のプログラムが実行される。これらのプログラムは当該ユーザーのコンテキストで実行され、当該アカウントに関連付けられた権限レベルを持つ。 p)ファイルの削除(PowerShell 経由):攻撃者によってシステム上に投入又は作成されたマルウェア、ツールその他の非ネイティブファイルは、ネットワーク内で何がどのように行われたかの痕跡を残すことがある。攻撃者は、痕跡を小さく保つため、又は侵害後の後処理の一環として、侵入期間中にこれらのファイルを削除することがある。 q)Windows イベントログの消去:悪意のあるツールが検知され、隔離その他の措置が取られた場合、攻撃者は当該ツールが検知された理由(インジケータ)を特定し、そのインジケータを除去するようツールを改変して、標的の防御システムや類似システムを使用する後続の標的に検知されない更新版を使用することがある。 r)OS 資格情報のダンプ:資格情報のダンプとは、通常はハッシュ又は平文パスワードの形式で、オペレーティングシステム及びソフトウェアからアカウントのログイン情報及びパスワード情報を取得するプロセスである。取得した資格情報は、横展開や制限された情報へのアクセスに利用され得る。 s)既知の資格情報を用いた SSH による横展開:攻撃者は、正当なアカウントを用いて、telnet、SSH、VNC など、リモート接続を受け付けるよう設計されたサービスにログインすることがある。その後、攻撃者はログインしたユーザーとして行動することができる。 t)サーバーソフトウェアコンポーネント(Web シェルのアップロード):攻撃者は、サーバーアプリケーションの正当な拡張開発機能を悪用して、システムへの永続的なアクセスを確立することがある。エンタープライズサーバーアプリケーションには、アプリケーション開発者がソフトウェアを記述及びインストールして主要なアプリケーションの機能を拡張できる機能が含まれることがある。攻撃者は、悪意のあるソフトウェアコンポーネントをインストールして、サーバーアプリケーションを拡張及び悪用することが可能となる。
3	Silk Typhoon	Microsoft Exchange Server に対する攻撃 ※特定の事案ではなく、左記グループによる長期間にわたる一連の事案を指す。	a)スピアフィッシングリンク:標的型メールに悪意のあるリンクを記載し、当該リンクをユーザーにクリックさせる。 b)インターネット接続の検出:攻撃者は、現在アクセスしている侵害済みシステム又はリモートシステムについて、ネットワーク経由の問い合わせにより、接続の一覧の取得を試みることがある。 c)システム所有者・ユーザーの検出:攻撃者は、主たる利用者、現在ログイン中のユーザー、当該システムを常用するユーザーの集合、又はユーザーが現在システムを利用しているか否かの特定を試みることがある。例えば、アカウントのユーザー名の取得や資格情報のダンプによってこれを行う。ユーザー及びユーザー名の情報は、実行中プロセスの所有権、ファイル及びディレクトリの所有権、セッション情報、システムログなどシステム全体に広く存在するため、他の検出技術を用いて様々な方法で収集され得る。攻撃者は、自動検出の過程で得た本情報を利用して、標的への感染を完遂するか否か、又は特定の行動を試みるか否かなど、その後の行動を決定することがある。 d)プロセス検出:攻撃者は、システム上で実行されているプロセスに関する情報の取得を試みることがある。取得した情報は、ネットワーク内のシステムで動作している一般的なソフトウェアを把握するために利用され得る。攻撃者は、自動検出の過程で得た本情報を利用して、標的への感染を完遂するか否かなど、その後の行動を決定することがある。 e)ファイルおよびディレクトリの検出:攻撃者は、ホスト又はネットワーク共有の特定の場所において、ファイルシステム内のファイル及びディレクトリを列挙し、特定の情報を検索することがあ

			る。攻撃者は、自動検出の過程で得た本情報を利用して、標的への感染を完遂するか否かなど、その後の行動を決定することがある。 f)システムネットワーク構成の検出:攻撃者は、アクセス先のシステム又はリモートシステムの情報収集を通じて、当該システムのネットワーク構成及び設定の詳細を探る可能性が高い。この情報の収集には、Arp、ipconfig/ifconfig、nbtstat、route など、各種のオペレーティングシステム管理ユーティリティが利用され得る。 g)自動収集:システム又はネットワーク内に侵入すると、攻撃者は内部データを収集するための自動化された技術を用いることがある。この技術の実行方法には、スクリプトを用いて、ファイル種別、場所、名前などの一定の基準に合致する情報を特定の時間間隔で検索及びコピーする方法が含まれ得る。この機能はリモートアクセスツールに組み込まれていることもある。 h)ローカルシステムからのデータ:機密データは、流出の前に、システム上に存在するファイルシステムや情報のデータベースなど、ローカルシステムの情報源から収集され得る。 i)リモートシステム検出:攻撃者は、現在のシステムからの横展開に使用され得る、ネットワーク上の他のシステムを IP アドレス、ホスト名その他の論理識別子によって一覧化しようとすることがある。この機能はリモートアクセスツールに含まれ得るが、オペレーティングシステムで利用可能なユーティリティも使用され得る。また、攻撃者はローカルの hosts ファイルを用いて、リモートシステムのホスト名と IP アドレスの対応を発見することもある。 j)ブルートフォース(パスワード):攻撃者は、パスワードが不明な場合やパスワードハッシュを取得した場合に、アカウントへのアクセスを試みるため、ブルートフォース技術を用いることがある。 k)正当なアカウント(ドメインアカウント):攻撃者は、資格情報アクセスの技術を用いて特定のユーザー又はサービスアカウントの資格情報を窃取したり、初期アクセスを得る手段として、偵察段階でソーシャルエンジニアリングにより資格情報を取得したりすることがある。 l)OS 資格情報のダンプ:資格情報のダンプとは、通常はハッシュ又は平文パスワードの形式で、オペレーティングシステム及びソフトウェアからアカウントのログイン情報及びパスワード情報を取得するプロセスである。取得した資格情報は、横展開や制限された情報へのアクセスに利用され得る。 m)正当なアカウント(ローカルアカウント):攻撃者は、資格情報アクセスの技術を用いて特定のユーザー又はサービスアカウントの資格情報を窃取したり、初期アクセスを得る手段として、偵察段階でソーシャルエンジニアリングにより資格情報を取得したりすることがある。 n)リモート電子メールの収集:攻撃者は、標的から機密情報を収集するため、ユーザーの電子メールを標的とすることがある。 o)コマンドアンドコントロールを介した流出:データの流出は、コマンドアンドコントロール(C2)チャネルを介して行われる。データは、C2 通信と同じプロトコルを用いて通常の通信チャネルに符号化される。 p)Windows イベントログの消去:悪意のあるツールが検知され、隔離その他の措置が取られた場合、攻撃者は当該ツールが検知された理由(インジケータ)を特定し、そのインジケータを除去するようツールを改変して、標的の防御システムや類似システムを使用する後続の標的に検知されない更新版を使用することがある。 q)リモートサービス(管理共有の割り当て):攻撃者は、正当なアカウントを用いて、telnet、SSH、VNC など、リモート接続を受け付けるよう設計されたサービスにログインすることがある。その後、攻撃者はログインしたユーザーとして行動することができる。 r)RoboCopy によるリモートファイルコピー:攻撃者は、正当なアカウントを用いて、telnet、SSH、VNC など、リモート接続を受け付けるよう設計されたサービスにログインすることがある。その後、攻撃者はログインしたユーザーとして行動することができる。 s)スケジュールされたタスク:攻撃者は、正当なアカウントを用いて、telnet、SSH、VNC など、リモート接続を受け付けるよう設計されたサービスにログインすることがある。その後、攻撃者はログ

			インしたユーザーとして行動することができる。 t)スケジュールされたタスクの実行:at や schtasks などのユーティリティ及び Windows タスクスケジューラを用いて、指定した日時に実行されるプログラムやスクリプトをスケジュールすることができる。RPC の利用に必要な認証が満たされ、ファイル及びプリンター共有が有効であれば、リモートシステム上にもタスクをスケジュールできる。リモートシステム上でのタスクのスケジュールには、通常、当該リモートシステムの管理者グループのメンバーであることが必要である。 u)ツールの持ち込み(イングレスツール転送):攻撃者が使用するツールその他のファイルは、作戦期間中、あるシステムから別のシステムへコピーして配置されることがある。ファイルは、C2 チャネルを通じて外部の攻撃者管理システムから被害者のネットワーク内へ持ち込まれたり、FTP など別のツールによる代替プロトコルを通じて持ち込まれたりすることがある。また、Mac や Linux では scp、rsync、sftp などのネイティブツールを用いてコピーすることもできる。 v)リモートサービス(管理共有の割り当て):攻撃者は、正当なアカウントを用いて、telnet、SSH、VNC など、リモート接続を受け付けるよう設計されたサービスにログインすることがある。その後、攻撃者はログインしたユーザーとして行動することができる。 w)RoboCopy によるリモートファイルコピー:攻撃者は、正当なアカウントを用いて、telnet、SSH、VNC など、リモート接続を受け付けるよう設計されたサービスにログインすることがある。その後、攻撃者はログインしたユーザーとして行動することができる。 x)スケジュールされたタスク:攻撃者は、正当なアカウントを用いて、telnet、SSH、VNC など、リモート接続を受け付けるよう設計されたサービスにログインすることがある。その後、攻撃者はログインしたユーザーとして行動することができる。 y)システムバイナリのプロキシ実行(Rundll32):rundll32.exe プログラムは、任意のバイナリを実行するために呼び出され得る。攻撃者は、Windows が通常の操作で rundll32.exe を使用することによるホワイトリストや誤検知のため、当該プロセスの実行を監視していない可能性のあるセキュリティツールの検知を回避する目的で、この機能を悪用してコードの実行を代理させることがある。 z)OS 資格情報のダンプ(NTDS):ソフトウェアの脆弱性の悪用は、攻撃者がプログラム、サービス、又はオペレーティングシステムのソフトウェア若しくはカーネル自体のプログラミングエラーを利用して、攻撃者が制御するコードを実行する場合に発生する。資格情報や認証の仕組みは、有用な資格情報の入手やシステムへのアクセス手続きの回避を目的として、攻撃者の標的となることがある。その一例として、Kerberos を標的とし、ドメインユーザーの権限を用いて Kerberos チケットを偽造できる MS14-068 がある。資格情報アクセスを目的とした脆弱性悪用は、対象となるプロセスや取得した資格情報によっては、権限昇格につながることもある。 aa)アカウントの作成(ドメインアカウント):攻撃者は、資格情報アクセスの技術を用いて特定のユーザー又はサービスアカウントの資格情報を窃取したり、初期アクセスを得る手段として、偵察段階でソーシャルエンジニアリングにより資格情報を取得したりすることがある。 ab)アカウントの操作:アカウントの操作は、攻撃者が環境内の資格情報及び特定の権限レベルへのアクセスを維持するのに役立つことがある。操作には、権限の変更、資格情報の変更、権限グループの追加又は変更、アカウント設定の変更、認証方法の変更などが含まれ得る。また、パスワード有効期間ポリシーを回避するためにパスワードを繰り返し変更し、侵害した資格情報の寿命を延ばすなど、セキュリティポリシーを無効化することを目的としたアカウント活動も含まれ得る。アカウントを作成又は操作するには、攻撃者は既にシステム又はドメイン上で十分な権限を有している必要がある。 ac)収集データのアーカイブ:収集したデータは、流出の前に中央の場所又はディレクトリに集められる。データは、別々のファイルとして保持されるか、データの圧縮や暗号化などの技術によって 1 つのファイルに結合され得る。 ad)コマンドアンドコントロールを介した流出:データの流出は、コマンドアンドコントロール(C2)チャネルを介して行われる。データは、C2 通信と同じプロトコルを用いて通常の通信チャネルに符

			号化される。
4	Salt Typhoon	米国の通信事業者を標的とした一連の攻撃 ※特定の事案ではなく、左記グループによる長期間にわたる一連の事案を指す。	a)スピアフィッシングリンク:標的型メールに悪意のあるリンクを記載し、当該リンクをユーザーにクリックさせる。 b)ネットワーク共有検出:ネットワークには、ユーザーがネットワーク上の様々なシステムのファイルディレクトリにアクセスできるようにする、共有ネットワークドライブやフォルダが含まれていることが多い。 c)RoboCopy によるリモートファイルコピー:ネットワークドライブやその他の共有場所に保存されたコンテンツは、正当なファイルに悪意のあるプログラム、スクリプト又はエクスプロイトコードを追加することで汚染され得る。ユーザーが共有された汚染コンテンツを開くと、悪意のある部分が実行され、リモートシステム上で攻撃者のコードが動作する可能性がある。攻撃者は、汚染された共有コンテンツを横展開に利用することがある。 d)保護されていない資格情報:ソフトウェアの脆弱性の悪用は、攻撃者がプログラム、サービス、又はオペレーティングシステムのソフトウェア若しくはカーネル自体のプログラミングエラーを利用して、攻撃者が制御するコードを実行する場合に発生する。資格情報や認証の仕組みは、有用な資格情報の入手やシステムへのアクセス手続きの回避を目的として、攻撃者の標的となることがある。その一例として、Kerberos を標的とし、ドメインユーザーの権限を用いて Kerberos チケットを偽造できる MS14-068 がある。資格情報アクセスを目的とした脆弱性悪用は、対象となるプロセスや取得した資格情報によっては、権限昇格につながることもある。 e)正当なアカウント(ドメインアカウント):攻撃者は、資格情報アクセスの技術を用いて特定のユーザー又はサービスアカウントの資格情報を窃取したり、初期アクセスを得る手段として、偵察段階でソーシャルエンジニアリングにより資格情報を取得したりすることがある。 f)プロセス検出:攻撃者は、システム上で実行されているプロセスに関する情報の取得を試みることがある。取得した情報は、ネットワーク内のシステムで動作している一般的なソフトウェアを把握するために利用され得る。攻撃者は、自動検出の過程で得た本情報を利用して、標的への感染を完遂するか否かなど、その後の行動を決定することがある。 g)システムネットワーク構成の検出:攻撃者は、アクセス先のシステム又はリモートシステムの情報収集を通じて、当該システムのネットワーク構成及び設定の詳細を探る可能性が高い。この情報の収集には、Arp、ipconfig/ifconfig、nbtstat、route など、各種のオペレーティングシステム管理ユーティリティが利用され得る。 h)ローカルデータステージング:収集したデータは、流出の前に中央の場所又はディレクトリに集められる。データは、別々のファイルとして保持されるか、データの圧縮や暗号化などの技術によって 1 つのファイルに結合され得る。 i)Web サービスを介した流出(PowerShell 経由):データの流出は、主要なコマンドアンドコントロール(C2)のプロトコル又はチャネルとは異なるプロトコルで行われる。データは、主要な C2 サーバーとは別のネットワーク上の場所へ送信される可能性が高い。別のプロトコルには、FTP、SMTP、

			HTTP/S、DNS、SMB など、主要な C2 チャネルとして使用されていない任意のネットワークプロトコルが含まれる。異なるチャネルには、クラウドストレージなどのインターネット上の Web サービスも含まれ得る。 j)スケジュールされたタスク/ジョブ(永続化):at や schtasks などのユーティリティ及び Windows タスクスケジューラを用いて、指定した日時に実行されるプログラムやスクリプトをスケジュールすることができる。RPC の利用に必要な認証が満たされ、ファイル及びプリンター共有が有効であれば、リモートシステム上にもタスクをスケジュールできる。リモートシステム上でのタスクのスケジュールには、通常、当該リモートシステムの管理者グループのメンバーであることが必要である。 k)ツールの持ち込み(イングレスツール転送):攻撃者が使用するツールその他のファイルは、作戦期間中、あるシステムから別のシステムへコピーして配置されることがある。ファイルは、C2 チャネルを通じて外部の攻撃者管理システムから被害者のネットワーク内へ持ち込まれたり、FTP など別のツールによる代替プロトコルを通じて持ち込まれたりすることがある。また、Mac や Linux では scp、rsync、sftp などのネイティブツールを用いてコピーすることもできる。 l)DLL サイドローディング:Windows システムは、プログラムに読み込むために必要な DLL を探す共通の方法を使用している。攻撃者は、Windows の DLL 検索順序や、DLL を曖昧に指定しているプログラムを悪用して、権限昇格及び永続化を図ることがある。 m)時間ベースの回避:システム時刻は、エンタープライズネットワーク内のシステム及びサービス間の時刻同期を維持するため、ドメイン内の Windows Time サービスによって設定及び保存される。 n)キーロギング:攻撃者は、正当なアカウントのための資格情報の取得及び情報収集の手段として、キーロギングやユーザー入力フィールドの傍受など、ユーザー入力を取得する方法を用いることができる。 o)OS 資格情報のダンプ:資格情報のダンプとは、通常はハッシュ又は平文パスワードの形式で、オペレーティングシステム及びソフトウェアからアカウントのログイン情報及びパスワード情報を取得するプロセスである。取得した資格情報は、横展開や制限された情報へのアクセスに利用され得る。 p)Windows Management Instrumentation(WMI):Windows Management Instrumentation(WMI)は、Windows システムコンポーネントへのローカル及びリモートアクセスのための統合環境を提供する Windows の管理機能である。ローカル及びリモートアクセスには WMI サービス、リモートアクセスにはサーバーメッセージブロック(SMB)及びリモートプロシージャコールサービス(RPCS)を利用し、RPCS はポート 135 で動作する。 q)Windows Remote Management(WinRM):Windows Remote Management(WinRM)は、ユーザーがリモートシステムと対話(実行ファイルの実行、レジストリの変更、サービスの変更など)できるようにする、Windows のサービス及びプロトコルの名称である。winrm コマンドや、PowerShell など各種プログラムから呼び出され得る。 r)システムネットワーク接続の検出:攻撃者は、現在アクセスしている侵害済みシステム又はリモートシステムについて、ネットワーク経由の問い合わせにより、接続の一覧の取得を試みることがある。 s)リモートシステム検出:攻撃者は、現在のシステムからの横展開に使用され得る、ネットワーク上の他のシステムを IP アドレス、ホスト名その他の論理識別子によって一覧化しようとすることがある。この機能はリモートアクセスツールに含まれ得るが、オペレーティングシステムで利用可能なユーティリティも使用され得る。また、攻撃者はローカルの hosts ファイルを用いて、リモートシステムのホスト名と IP アドレスの対応を発見することもある。 t)ドメイントラストの検出:攻撃者は、Windows のマルチドメイン/フォレスト環境において横展開の機会を特定するために用いられ得る、ドメイントラスト関係に関する情報の収集を試みることがある。ドメイントラストは、あるドメインが別のドメインの認証手続きに基づいてリソースへのアク

			セスを許可する仕組みであり、トラストされたドメインのユーザーは、トラストするドメインのリソースにアクセスできる。発見した情報は、攻撃者が SID 履歴の挿入、パスザチケット、Kerberoasting を行うのに役立つことがある。ドメイントラストは、DSEnumerateDomＡＩnTrusts() Win32 API 呼び出し、.NET メソッド、LDAP を用いて列挙できる。Windows ユーティリティの Nltest は、攻撃者がドメイントラストの列挙に使用することが知られている。 u)ドメインアカウントの検出:攻撃者は、ローカルシステム又はドメインのアカウントの一覧の取得を試みることがある。 v)防御機能の低下(インジケータのブロック):攻撃者は、センサーが通常取得するインジケータやイベントが収集及び分析されるのを妨害しようとすることがある。これには、イベントテレメトリの収集及び流れを制御する設定を改ざんすることにより、Event Tracing for Windows(ETW)などのホストベースのセンサーを悪意を持ってリダイレクトしたり無効化したりすることが含まれ得る。これらの設定は、システム上の構成ファイルやレジストリに保存されているほか、PowerShellやWindows Management Instrumentation などの管理ユーティリティを介してアクセスできることもある。 w)保護されていない資格情報:ソフトウェアの脆弱性の悪用は、攻撃者がプログラム、サービス、又はオペレーティングシステムのソフトウェア若しくはカーネル自体のプログラミングエラーを利用して、攻撃者が制御するコードを実行する場合に発生する。資格情報や認証の仕組みは、有用な資格情報の入手やシステムへのアクセス手続きの回避を目的として、攻撃者の標的となることがある。その一例として、Kerberos を標的とし、ドメインユーザーの権限を用いて Kerberos チケットを偽造できる MS14-068 がある。資格情報アクセスを目的とした脆弱性悪用は、対象となるプロセスや取得した資格情報によっては、権限昇格につながることもある。 x)既知の資格情報を用いたSSHによる横展開:攻撃者は、正当なアカウントを用いて、telnet、SSH、VNC など、リモート接続を受け付けるよう設計されたサービスにログインすることがある。その後、攻撃者はログインしたユーザーとして行動することができる。 y)防御機能の低下(コマンド履歴ログの妨害):攻撃者は、自身のツールや活動の検知を回避するため、セキュリティツールを無効化することがある。これは、セキュリティソフトウェアやイベントログ処理プロセスの停止、実行時にツールが起動しないようレジストリキーを削除するなど、セキュリティスキャンやイベント報告を妨害する方法で行われることがある。 z)アカウントの操作:アカウントの操作は、攻撃者が環境内の資格情報及び特定の権限レベルへのアクセスを維持するのに役立つことがある。操作には、権限の変更、資格情報の変更、権限グループの追加又は変更、アカウント設定の変更、認証方法の変更などが含まれ得る。また、パスワード有効期間ポリシーを回避するためにパスワードを繰り返し変更し、侵害した資格情報の寿命を延ばすなど、セキュリティポリシーを無効化することを目的としたアカウント活動も含まれ得る。アカウントを作成又は操作するには、攻撃者は既にシステム又はドメイン上で十分な権限を有している必要がある。 aa)システム情報の検出:攻撃者は、バージョン、パッチ、修正プログラム、サービスパック、アーキテクチャなど、オペレーティングシステム及びハードウェアに関する詳細な情報の取得を試みることがある。攻撃者は、自動検出の過程で得た本情報を利用して、標的への感染を完遂するか否かなど、その後の行動を決定することがある。 ab)内部プロキシ:攻撃者は、システム間のネットワークトラフィックを転送したり、コマンドアンドコントロール(C2)サーバーへのネットワーク通信の中継として機能させ、自身のインフラへの直接接続を避けたりするために、接続プロキシを使用することがある。プロキシやポートリダイレクトによるトラフィック転送を可能にするツールは多数存在し、HTRAN、ZXProxy、ZXPortMap などが含まれる。攻撃者はこれらのプロキシを、C2 通信の管理、同時外向き接続数の削減、接続断に対する耐性の確保、被害者間の既存の信頼された通信路への便乗による疑念の回避などのために使用する。 ac)ファイルの削除:攻撃者によってシステム上に投入又は作成されたマルウェア、ツールその他の

			非ネイティブファイルは、ネットワーク内で何がどのように行われたかの痕跡を残すことがある。攻撃者は、痕跡を小さく保つため、又は侵害後の後処理の一環として、侵入期間中にこれらのファイルを削除することで、フォレンジック調査を困難にすることが可能となる。

5	ー	ランサムウェアを用いた攻撃全般 ※特定のグループによる特定の事案ではなくランサムウェアを使用した攻撃の一例とする。	a)ローカルシステムからのデータ:ファイルシステムや構成ファイル、ローカルデータベースなどのローカルシステムソースを検索し、流出を実行する前に、関心のあるファイルや機密データを見つけようとする。 b)リモートシステム検出:横展開に使用される可能性のあるネットワーク上の IP アドレス、ホスト名などを収集して他のシステムのリストを収集しようとする。 c)リモートサービス:リモートデスクトップや Windows 管理共有など、リモートサービスを悪用して正規のアカウントへのログインを試みる。 d)難読化:システム上、または窃取のための転送データを暗号化やエンコード等、難読化することによって、ファイルの検知やセキュリティ分析を困難にしようとする。 e)バイナリバディング:バイナリバディングを使用して、ファイルの動作に影響しないゴミデータを大量に追加して、マルウェアをセキュリティ機材が処理できる容量よりも大きくしようとする。 f)プロセス検出:システム上で実行されているアプリケーションを把握するなどの目的で、システム上で実行中のプロセスの一覧を取得する。 g)コマンド及びスクリプトインタープリター:コマンドラインや PowerShell など、コマンドやスクリプトインタープリターを悪用しコマンド、スクリプト、バイナリなどを実行しようとする。 h)データステージング:収集したデータを流出させる際、ローカルのとあるディレクトリや、システム上のとある端末など、どこか 1 ヶ所に集め、圧縮ファイルに変換する等の準備を行う。 i)人力ツール転送:攻撃に使用するツールを外部から侵害中のシステムへ転送したり、侵害中のシステム内部で転送や拡散したりする。 j)ブルートフォース:アカウントへのアクセスのため、パスワードを総当たり、辞書攻撃、またはパスワードハッシュなどの過去に取得した資格情報をチェックする等の手法によりログインしようとする。 k)ユーザー実行:悪意のあるリンクや添付ファイルの付いたメールを送信し、ユーザーにそれらを実行させようとする。 I)標的への悪影響のための暗号化:標的のシステム破壊や、金銭目的の脅迫のため、標的のシステムやネットワーク上の多数のデータを暗号化し、標的の可用性を損ねる。 m)防御機能の低下: Windows の監査ログやファイアウォールのルール改ざんなど、各種の監視、セキュリティ機能や機材を無効化、もしくは設定変更を行う。 n)アーティファクトの非表示・検出の回避のため、ファイルやディレクトリ、ユーザー、ウインドウなど、各種の非表示機能を悪用しようとする。 o)フィッシング:悪意のあるリンクや添付メールを含むバラマキ型メールや、標的型メールを送付する。
6	ー	内部犯行による攻撃全般 ※特定のグループによる特定の事案ではなく、内部犯行による攻撃の一例とする。	a)システムサービス検出:システム上で動作中のサービスの一覧を取得する。 b)アプリケーションウインドウの検出:侵害中のシステムの利用方法の推測に役立てるため、開いているアプリケーションウインドウのリストを取得しようとする。 c)クエリレジストリ:各種の手段で Windows レジストリにアクセスし、システム、構成、インストールされているソフトウェア、セキュリティなど、システムやネットワークの現状を把握するのに役立つ様々な情報を収集しようとする。 d)システムネットワーク構成の検出: IP アドレスや MAC アドレス、リモートシステムの検出、インターネットへの出口の特定など、攻撃するシステムのネットワーク構成や設定に関する情報を収集する。 e)リモートシステム検出:横展開に使用される可能性のあるネットワーク上の IP アドレス、ホスト名などを収集して他のシステムのリストを収集しようとする。 f)システムネットワーク接続検出:侵入済みネットワークの IP アドレスの一覧取得など、ネットワーク接続の一覧を把握しようとする。 g)プロセス検出:システム上で実行されているアプリケーションを把握するなどの目的で、システム上で実行中のプロセスの一覧を取得する。 h)権限グループ検出(ローカルグループ) :端末のローカルのアカウントの一覧と管理者権限のアカウントを見つけようとする。

			i)アプリケーション層プロトコル(Web プロトコル) :外部との通信を検知や遮断されないため、 HTTP など、Web トラフィックに紛れて指令サーバーとの接続やデータの流出などの通信を行う。 j)システム情報の検出:窃取した大量のデータを圧縮ファイルにして外部へ流出させる準備をする前に、使用可能な空き領域を確認するなど、OS やハードウェア等に関する詳細な情報を取得する。 k)ドメインアカウントの検出:PowerShell のコマンドなどを使用して、ドメインアカウントの一覧を取得する。 l)周辺機器の検出:コンピュータに接続されている周辺機器及びコンポーネントに関する情報を収集しようとする。 m)システム時刻検出:被害者のロケーションの把握、攻撃の自動実行時間の決定、あるいはセキュリティ機材による解析のためのマルウェアの実行の有無を把握するため、システム時刻を収集しようとする。 n)ネットワーク共有検出:収集する情報のソースの特定、横展開の対象となるシステムを特定するため、リモートシステムで共有されているフォルダとドライブを把握しようとする。 o)ドライブバイ攻撃:初期アクセス確立などの目的で、 Web サイト訪問者をマルウェアに感染させる等の攻撃をする。 p)ユーザー実行:悪意のあるリンクや添付ファイルの付いたメールを送信し、ユーザーにそれらを実行させようとする。 q)仮想マシン/サンドボックス回避:セキュリティ機材やマルウェア解析者による解析を回避するため、マルウェアにマルウェア自身が実行されているシステム環境を検出するための機能を埋め込む。

別紙

著作権その他の権利

１　契約相手方は、役務実施報告書を作成する場合は、第三者が有する著作権等を侵害することのないよう、必要な処置を講ずること。

２　この契約において作成した役務実施報告書が第三者の権利を侵害しているとして、官側に対して、第三者が何らかの請求・主張を行ったときには、契約相手方が自己の費用にて当該第三者と交渉・訴訟を行い、弁護士費用、その他の費用を含む損害賠償責任は全て契約相手方が負担すること。

３　この契約において創作され納入物となる役務実施報告書の著作物において著作権等が発生する場合、その権利は次によること。ただし、官側は納入された著作物を自ら利用するために必要と認められる範囲において、翻案、複製及び貸与することができる。

(1)　契約相手方が従来から有していた著作権等は、契約相手方に留保される（以下「留保著作権等」という。）。

(2)　契約相手方は、この契約で新たに契約相手方が著作した役務実施報告書の著作権を官側に譲渡することとし、役務実施報告書の納入時に**付紙第１**「役務実施報告書に関する著作権譲渡証明書」を作成し、提出すること。

(3)　契約相手方は、提出書類及び納入物に関し、著作権法に規定する著作者人格権を行使しないこととし、役務実施報告書の納入時に**付紙第２**「役務実施報告書に関する著作者人格権不行使証書」を作成し、提出すること。

(4)　契約相手方は、役務実施報告書に関する著作権等の留保を主張する場合は「役務実施報告書に関する著作権譲渡証明書」の附属書として**付紙第３**「役務実施報告書に関する留保著作権等内訳書」を作成し、提出すること。契約相手方は、提出後速やかに留保部分について官側と協議を行った上で、確認を受けること。また、確認を受けた留保部分に関する詳細資料を官側に提出すること。

４　契約相手方は、著作権等の帰属等に関し疑義が発生した場合は、その都度官側と協議して解決すること。また、協議において取決めを行った場合、契約相手方は、取り決めた文書を速やかに官側に提出し、確認を受けること。

付紙第１

役務実施報告書に関する著作権譲渡証明書

令和　　年　　月　　日

甲

殿

乙　住　　所
会 社 名
代表者名

統制番号 （調達要求番号）			
品名			
契約金額		納入先部隊等名 （納入場所）	
数量・単位			
単価		契約番号及び年月日	

乙は、上記契約により作成した役務実施報告書に関する著作権（著作権法（昭和４５年法律第４８号）第２１条から第２８条に定める全ての権利を含む。）を令和　　年　　月　　日に甲に対して譲渡したことに相違ありませんので、本証明書を提出いたします。ただし、甲及び乙の協議の下、乙への留保が認められた著作権は除くものといたします。

付紙第２

役務実施報告書に関する著作者人格権不行使証書

令和　　年　　月　　日

甲

殿

乙　住　　所
会 社 名
代表者名

統制番号 （調達要求番号）			
品名			
契約金額		納入先部隊等名 （納入場所）	
数量・単位			
単価		契約番号及び年月日	

乙は、上記契約により作成した役務実施報告書に関する著作者人格権（著作権法（昭和４５年法律第４８号）第１８条から第２０条に定める全ての権利を含む。）を行使しないことを約束し、本証書を提出いたします。

なお、著作者人格権を行使しようとする場合には、甲の承認を得るものとします。

付紙第３

附属書

役務実施報告書に関する留保著作権等内訳書

役務実施報告書に関する著作権譲渡証明書のただし書により、乙に留保される著作権等の内訳は、次のとおりです。

該当範囲	
該当箇所	
理由	

サイバー攻撃対処業務における官民連携に係る調査・研究役務

総合評価実施要領

令和８年（2026 年）１０月

防　　衛　　省

1　総則

1.1　適用範囲

本要領は、「**サイバー攻撃対処業務における官民連携に係る調査・研究役務**」に係る総合評価実施要領について規定する。

1.2　引用文書

本要領は、「**サイバー攻撃対処業務における官民連携に係る調査・研究役務**」に係る次の文書を引用する。

a)　**仕様書**

b)　**応札資料作成要領**

c)　**評価手順書**

d)　**評価基準表**

2　総合評価の実施方針

2.1　本調達における総合評価実施の基本的な考え方

「公共調達の適正化について（財計第２０１７号。１８．８．２５）」（以下「財務大臣通知」という。）において、行政補助的な業務に係る役務等の契約のうち、本業務のように価格競争による一般競争入札により難い場合は、総合評価落札方式により実施することとされている。

本調達は、高度な専門知識及び経験を必須とすることから、財務大臣通知を受け、更なる調達の公正化・透明化のため、総合評価落札方式により実施するものである。

総合評価は、応札者からの提案事項のうち、仕様書及び応札資料作成要領に定める要件を全て満たしたものについて、それぞれの要件が、提案どおり実現可能であるか、また、適切に実施されるかどうかを判断するために実施するものである。

2.2　評価項目

a)　**仕様書から評価対象事項を抽出し、提案要求項目として整理した上で、応札資料作成要領の別添「評価基準表」にとりまとめた。**

b)　**必須項目及び任意項目に対する評価の観点**

必須項目及び任意項目に対する評価の考え方は次のとおり。

1)　**必須項目：最低限必要な契約相手方の条件。**

2)　**任意項目：有していることが望まれる契約相手方の条件。**

2.3　得点配分及び配点

a)　**提案要求項目の得点配分**

価格と同等に評価できる項目を必須項目「基礎点」とし、価格と同等に評価できない項目を任意項目「加点」として、それぞれの得点配分は、１対１とする。

b)　**提案要求項目の配点**

提案要求項目の配点については、提案要求項目の分類ごとに以下のとおりとする。

提案要求項目	得点配分	参考（全体比）
1　業務の実施方針等	340	約 55%
2　実施体制	200	約 35%
3　賃上げの表明	20	約 3%
4　ワーク・ライフ・バランスの推進	20	約 3%
5　マイナンバーカード普及等の推進に対する評価	10	約 2%
6　デジタル・スタートアップの公共調達参入機会拡大に係る事項	10	約 2%
計	600	100%

3　総合評価の実施手順

総合評価（技術評価）は、以下の手順により実施する。

順	区分	実施者	内容
1	技術評価の実施	技術評価者	技術評価により、技術点の評価を実施する。評価にあたっては、評価手順書の別添「評価基準表」の各［提案要求項目］について評価する。それぞれの評価者が実施した評価をもとに平均点を算定し、評価者の平均点をもって技術点の評価とする。ただし、基礎点の対象となる要件については１名の評価者が評価を実施することとし、一つでも要求事項を満たしていない場合は、その応札者は不合格とする。
2	技術評価結果の報告	サイバー整備課担当者	技術評価の結果については、「技術評価実施報告書」（別紙第２）に取りまとめた上で、会計課担当者に提出する。
3	落札者の決定	会計課	開札により、価格が予定価格を下回ったものについて、価格点を算定し、技術点との合算により、落札者を決定する。 なお、技術評価の対象が１者のみの場合は、価格点の算出及び技術点との合算は行わない。

4　技術評価の実施

技術評価の実施要領は、以下のとおりとする。

a)　評価者（基準）

整備計画局サイバー整備課員　５名

b)　評価対象

提案書

c)　評価基準

評価基準は、別添「評価基準表」とする。

d) **評価方法**

1) 技術評価者は、提案書を対象に評価を実施する。

2) 技術評価の実施に当たっては、以下の基準に基づき、それぞれの評語を用いて評価を実施する。

(必須項目の評価)

評価事項	評語	配点比率	備考
要求事項を満たしている	A	100%	
要求事項を満たしていない	D	0%	

(任意項目 (ただし(12)及び(15)から(18)を除く。) の評価)

評価事項	評語	配点比率
優れている(非常に合理的又は実績に基づいた優れた提案であり、評価できる点が多数)	A	100%
やや優れている(標準的だが、評価できる点が、いくつか見られる)	B	70%
やや劣っている (過不足はないが、(スケジュール、実施方法、実現性等に)懸念がある)	C	40%
劣っている又は提案なし	D	0%

(任意項目 (12) の評価)

評価事項		評語	配点	備考
次の配点に応じて ITSS レベル等に応じて最も高いレベルの資格を本項目の評価とする。		―	―	
	①CISSP、CISA、CISM、CRISC、CGEIT、GIAC、CEH、OSCP、CIA、PMP、技術士 (情報工学部門又は情報工学を選択科目とする総合技術監理部門)、博士 (サイバーセキュリティ又は教育学に関する研究を専攻分野とするもの)、情報処理安全確保支援士、高度情報処理技術者試験及びその他 ITSS レベル４に位置づけられる資格のいずれかを有する者	A	30 点	
	②SSCP、CAPM、応用情報技術者試験、その他の ITSS レベル３に位置づけられる資格及び修士 (サイバーセキュリティ又は教育学に関する研究を専攻分野とするものであって専門職学位を含む)	B	15 点	

	③基本情報技術者試験、情報セキュリティマネジメント試験、その他の ITSS レベル２に位置づけられる資格及び学士（工学、理学、法学、教育学に関するもの）	C	10 点	
	④上記資格のいずれも有していない。	D	0 点	

（任意項目の評価）（15）

評価事項	評語	配点比率
該当	A	100%
該当なし	D	0%

（任意項目の評価）（16）

評価事項	評語	配点比率
①または②に該当	A	100%
該当なし	D	0%

（任意項目の評価）（17）

評価事項	評語	配点比率
すべて該当	A	100%
②のみ該当	B	70%
①のみ該当	C	40%
該当なし	D	0%

（任意項目の評価）（18）

評価事項	評語	配点比率
①～③すべて該当	A	100%
該当なし	D	0%

3) 技術評価者は、評価結果を「技術評価実施結果表（全項目）」（別紙第３）又は「技術評価実施結果表（任意項目のみ）」（別紙第４）に記載する。

4) サイバー整備課担当者は、3)で記載された実施結果を取りまとめ、「技術評価実施報告書」（別紙第２）を作成する。

5) 4)の作成に当たり、提案要求項目の評価点配分を基に、技術評価者の評語に基づく配点比率を乗じて得た点数を評価点とし、技術評価者ごとに、提案要求項目に対する評価点を算出する。

6) サイバー整備課担当者は、提案要求項目ごとに、技術評価者のうち最上位者の者と最下位者の者を各一名除外した３名の者の得点の平均点（小数点以下第３位を四捨五入する。）を算定し、その合計点から技術点を算出する。

7) サイバー整備課担当者は、6)の技術点から「総合評価実施結果」（別紙第１）を作成する。

e) 留意事項

評価員は、入札公告等を行ったときから落札者が決定するまでの間、入札者と思われる者に接触しないものとし、入札者の提案内容について疑義がある場合等は、契約担当官等を通じて

書面により問い合わせる。ただし、当該案件に関係しない用務のために、やむを得ず入札者と思われる者と接触するときは、案件、単価等にかかわらず、「調達等関係業務に従事している職員が防衛省の退職者を含む業界関係者等と接触する場合における対応要領について」（防経装第８３０３号。１９．８．３０）の例により適切に接触及び報告書を作成する。

別紙第１

令和 年　月　日

総合評価実施結果

件名：　サイバー攻撃対処業務における官民連携に係る調査・研究役務

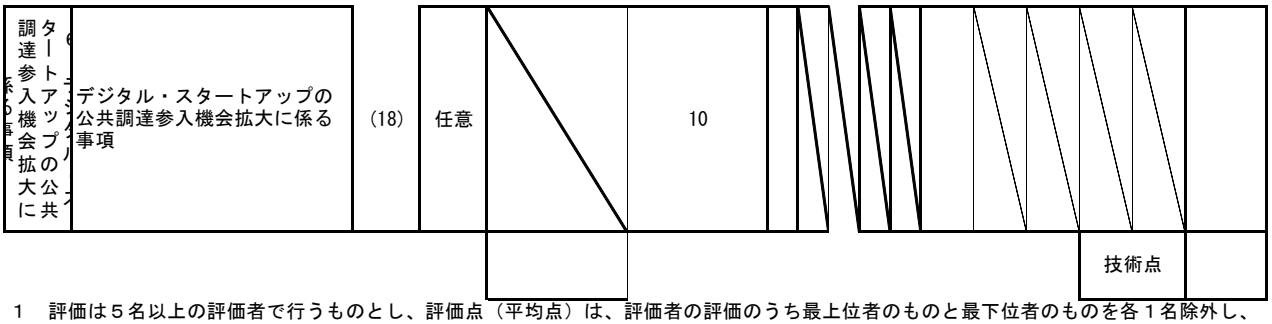
番号	応札者名	技術点	評価実施日	備考
1				
2				
3				
4				
5				

別紙第２

技術評価実施報告書

件名：　サイバー攻撃対処業務における官民連携に係る調査・研究役務

項番	提案要求項目		番号	評価区分	技術点		評価者					評価点					
					基礎点（価格と同等に評価できる項目）	加点（価格と同等に評価できない項目）	評価者１	評価者２	評価者３	評価者４	評価者５	評価者１	評価者２	評価者３	評価者４	評価者５	平均
１　業務の実施方針等	役務内容の妥当性、独創性		(1)	必須	70												
			(2)	任意		10											
			(3)	任意		40											
			(4)	任意		60											
			(5)	任意		80											
			(6)	任意		10											
			(7)	任意		10											
	役務計画の妥当性、効率性		(8)	必須	60												
２　実施体制	組織の経験・能力	類似調査業務の経験（組織）	(9)	必須	30												
		ISMS認証	(10)	必須	30												
		調査業務に当たっての管理・バックアップ体制	(11)	必須	30												
	業務従事者の経験・能力	調査業務への適性	(12)	任意		30											
			(13)	必須	50												
		類似調査業務の経験（業務従事者）	(14)	必須	30												
３　賃上げの表明	賃上げ表明の実施及び表明書の提出		(15)	任意		20											
４　ワーク・ライフ・バランス等の推進に関する指標	認定の取得		(16)	任意		20											
５　マイナンバーカード普及等の推進に対する評価	マイナンバーカード普及等の推進に対する評価		(17)	任意		10											



1　評価は５名以上の評価者で行うものとし、評価点（平均点）は、評価者の評価のうち最上位者のものと最下位者のものを各１名除外し、３名以上の評価点を平均して算出する。
2　評価点(平均点）は、小数点第３位を四捨五入し小数点第２位とする

別紙第３

技術評価実施結果表（全項目）

実施年月日	令和　　年　　月　　日
評価実施者	

件名：　サイバー攻撃対処業務における官民連携に係る調査・研究役務

業者名＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

項番	提案要求項目		番号	評価区分	評価結果	備考 （評価の観点）
１ 役務の実施内容	役務内容の妥当性、独創性		(1)	必須		本役務の実施にあたり、本役務の目的及び制約事項を理解した提案になっているか。役務実施事項について、全く記述されていない、仕様書に則った具体的な手法について記述されていない、あるいは記述された内容の実現が明らかに望めないと認められる場合には要求事項を満たさないものとする。
			(2)	任意		仕様書2.4.3項に掲げるサイバー攻撃対処演習用の事前教育プログラムが優れている。
			(3)	任意		仕様書2.4.4項に掲げるサイバー攻撃対処演習の実施について、要求事項を満たす提案がなされ、要求元や本役務に関連する事業を理解した提案となっている。
			(4)	任意		仕様書2.4.6項の演習シナリオを作成するに当たり、十分な攻撃キャンペーンの攻撃手法を取り入れるとともに、ＡＩを十分に活用した上で、実効性があるシナリオを策定できる提案となっている。
			(5)	任意		仕様書2.4.7項のサイバー攻撃対処演習の環境について、2.4.6項のシナリオを考慮し、実現性のある環境構築が可能な提案となっている。
			(6)	任意		仕様書2.4.9項の欧米主要国の官民連携施策を調査するに当たり、実現性のある調査手法や調査先を示しているか。
			(7)	任意		仕様書に示した内容以外の独自性のある優れた提案がされているか。仕様書に示した内容以外の手法を提案している場合、それが仕様書に示した内容より優れていると言える根拠が示されているか。
	調査計画の妥当性、効率性		(8)	必須		調査、演習の手法、日程等に無理がなく、目的に沿った実現性のあるものか。
２ 実施体制	組織の経験・能力	類似役務業務の経験（組織）	(9)	必須		契約の相手方は、3.1項a)～c)記載の要件を満たす実績を有しているか。有している場合には、その概要について具体的に記載されているか。
		ISMS認証	(10)	必須		契約の相手方は、情報セキュリティマネジメントシステム（ISO/IEC 27001又はJIS Q 27001）の第三者認証を有しているか。
		調査業務に当たっての管理・バックアップ体制	(11)	必須		契約の相手方は、役務を遂行可能な人員（2.4.4項を参照）を確保しているか。 契約の相手方は、円滑な事業遂行のための人員補助体制を組んでいるか。 契約の相手方の管理者は、調査業務に関する経験や知見はあるか。
	業務従事者の経験・能力	調査業務への適性	(12)	任意		業務従事者は、3.2項d）に示す資格について、次に掲げるITSS等のレベルの高い資格を有する場合、そのレベルに応じて加点する。 ・ＣＩＳＳＰ、ＧＩＡＣ、ＣＩＳＡ、ＣＩＳＭ、ＣＲＩＳＣ、ＣＥＨ、ＰＭＰ、技術士（情報工学）、情報処理安全確保支援士、高度情報処理技術者試験等。
			(13)	必須		業務従事者が他の手持ち業務等との関係において履行に必要な業務所要に対応できる態勢にあることが記載されているか。（必要工数確保及び名義の流用の防止）
		類似調査業務の経験（業務従事者）	(14)	必須		業務従事者は、3.2項b)～c)に記載の要件を満たす実績を有しており、その概要について具体的に記載されているか。
３　賃上げの表明						
	賃上げ表明の実施及び表明書の提出		(15)	任意		令和８年度における対前年度比、又は令和８年における前年比で給与総額を2.5%以上増加させる旨、従業員に表明していること【中小企業等】

4　ワーク・ライフ・バランス等の推進に関する指標					
	認定の取得	(16)	任意		次の要件のいずれかを満す事業者であるか。 ①ワーク・ライフ・バランスを推進する企業として、女性活躍推進法、次世代育成支援対策推進法（平成15年法律第120号。以下「次世代法」という。）、青少年の雇用の促進等に関する法律（昭和45年法律第98号。以下「若者雇用促進法」という。）その他関係法令に基づく認定（認定の基準が複数あるものにあっては、労働時間等の働き方その他のワーク・ライフ・バランスに関する基準を満たすものに限る。以下同じ。）を受けていること。 ②女性活躍推進法第８条に基づく一般事業主行動計画（計画期間が終了していないものに限る。）を策定していること。（常時雇用する労働者の数が100人以下のものに限る。）
5　マイナンバーカード普及等の推進に対する評価					
	マイナンバーカード普及等の推進に対する評価	(17)	任意		次の要件のいずれかを満す事業者であるか。 ①電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律（平成14年法律第153 号。）第17条第１項第4号、第5号若しくは第6号の規定に該当する事業者であって、同条第4項に規定する取決めを地方公共団体情報システム機構と締結した事業者又は電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律施行規則（平成15年総務省令第120号）第29条第１項の定めにより、総務大臣の認定を受けたものとみなされた事業者であるか。 ②官民データ活用推進基本法第10条第２項に規定する電子情報処理組織を使用して入札に参加する事業者であって、公的個人認証法第3条第1項に定める署名用電子証明書又は第22条に定める利用者証明用電子証明書を用いて入札に参加する事業者であるか。
5　デジタル・スタートアップの公共調達参入機会拡大に係る事項					
	デジタル・スタートアップの公共調達参入機会拡大に係る事項	(18)	任意		次の要件のすべてを満す事業者であるか。 ①　中小企業基本法（昭和38年法律第154号）第２条第１項に規定する中小企業者（みなし大企業を除く）であること ②　設立から15年未満であること ③　情報システムに関連した先進技術やアイデアをもって当該事業に主体的に取り組み、今回の調達を実績として今後事業拡大することが期待できる事業者であること

別紙第３

技術評価実施結果表（任意項目）

実施年月日	令和　　年　　月　　日
評価実施者	

件名：　サイバー攻撃対処業務における官民連携に係る調査・研究役務

業者名＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

項番	提案要求項目		番号	評価区分	評価結果	備考（評価の観点）
１　役務の実施内容	役務内容の妥当性、独創性		(1)	必須		本役務の実施にあたり、本役務の目的及び制約事項を理解した提案になっているか。役務実施事項について、全く記述されていない、仕様書に則った具体的な手法について記述されていない、あるいは記述された内容の実現が明らかに望めないと認められる場合には要求事項を満たさないものとする。
			(2)	任意		仕様書2.4.3項に掲げるサイバー攻撃対処演習用の事前教育プログラムが優れている。
			(3)	任意		仕様書2.4.4項に掲げるサイバー攻撃対処演習の実施について、要求事項を満たす提案がなされ、要求元や本役務に関連する事業を理解した提案となっている。
			(4)	任意		仕様書2.4.6項の演習シナリオを作成するに当たり、十分な攻撃キャンペーンの攻撃手法を取り入れるとともに、ＡＩを十分に活用した上で、実効性があるシナリオを策定できる提案となっている。
			(5)	任意		仕様書2.4.7項のサイバー攻撃対処演習の環境について、2.4.6項のシナリオを考慮し、実現性のある環境構築が可能な提案となっている。
			(6)	任意		仕様書2.4.9項の欧米主要国の官民連携施策を調査するに当たり、実現性のある調査手法や調査先を示しているか。
			(7)	任意		仕様書に示した内容以外の独自性のある優れた提案がされているか。仕様書に示した内容以外の手法を提案している場合、それが仕様書に示した内容より優れていると言える根拠が示されているか。
	調査計画の妥当性、効率性		(8)	必須		調査、演習の手法、日程等に無理がなく、目的に沿った実現性のあるものか。
２　実施体制	組織の経験・能力	類似役務業務の経験（組織）	(9)	必須		契約の相手方は、3.1項a)～c)記載の要件を満たす実績を有しているか。有している場合には、その概要について具体的に記載されているか。
		ISMS認証	(10)	必須		契約の相手方は、情報セキュリティマネジメントシステム（ISO/IEC 27001又はJIS Q 27001）の第三者認証を有しているか。
		調査業務に当たっての管理・バックアップ体制	(11)	必須		契約の相手方は、役務を遂行可能な人員（2.4.4項を参照）を確保しているか。 契約の相手方は、円滑な事業遂行のための人員補助体制を組んでいるか。 契約の相手方の管理者は、調査業務に関する経験や知見はあるか。
	業務従事者の経験・能力	調査業務への適性	(12)	任意		業務従事者は、3.2項d）に示す資格について、次に掲げるITSS等のレベルの高い資格を有する場合、そのレベルに応じて加点する。 ・ＣＩＳＳＰ、ＧＩＡＣ、ＣＩＳＡ、ＣＩＳＭ、ＣＲＩＳＣ、ＣＥＨ、ＰＭＰ、技術士（情報工学）、情報処理安全確保支援士、高度情報処理技術者試験等。
			(13)	必須		業務従事者が他の手持ち業務等との関係において履行に必要な業務所要に対応できる態勢にあることが記載されているか。（必要工数確保及び名義の流用の防止）
		類似調査業務の経験（業務従事者）	(14)	必須		業務従事者は、3.2項b)～c)に記載の要件を満たす実績を有しており、その概要について具体的に記載されているか。
３　賃上げの表明						
	賃上げ表明の実施及び表明書の提出		(15)	任意		令和８年度における対前年度比、又は令和８年における前年比で給与総額を2.5%以上増加させる旨、従業員に表明していること【中小企業等】

4　ワーク・ライフ・バランス等の推進に関する指標					
	認定の取得	(16)	任意		次の要件のいずれかを満す事業者であるか。 ①ワーク・ライフ・バランスを推進する企業として、女性活躍推進法、次世代育成支援対策推進法（平成15年法律第120号。以下「次世代法」という。）、青少年の雇用の促進等に関する法律（昭和45年法律第98号。以下「若者雇用促進法」という。）その他関係法令に基づく認定（認定の基準が複数あるものにあっては、労働時間等の働き方その他のワーク・ライフ・バランスに関する基準を満たすものに限る。以下同じ。）を受けていること。 ②女性活躍推進法第８条に基づく一般事業主行動計画（計画期間が終了していないものに限る。）を策定していること。（常時雇用する労働者の数が100人以下のものに限る。）
5　マイナンバーカード普及等の推進に対する評価					
	マイナンバーカード普及等の推進に対する評価	(17)	任意		次の要件のいずれかを満す事業者であるか。 ①電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律（平成14年法律第153 号。）第17条第１項第4号、第5号若しくは第6号の規定に該当する事業者であって、同条第4項に規定する取決めを地方公共団体情報システム機構と締結した事業者又は電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律施行規則（平成15年総務省令第120号）第29条第１項の定めにより、総務大臣の認定を受けたものとみなされた事業者であるか。 ②官民データ活用推進基本法第10条第２項に規定する電子情報処理組織を使用して入札に参加する事業者であって、公的個人認証法第3条第1項に定める署名用電子証明書又は第22条に定める利用者証明用電子証明書を用いて入札に参加する事業者であるか。
5　デジタル・スタートアップの公共調達参入機会拡大に係る事項					
	デジタル・スタートアップの公共調達参入機会拡大に係る事項	(18)	任意		次の要件のすべてを満す事業者であるか。 ①　中小企業基本法（昭和38年法律第154号）第２条第１項に規定する中小企業者（みなし大企業を除く）であること ②　設立から15年未満であること ③　情報システムに関連した先進技術やアイデアをもって当該事業に主体的に取り組み、今回の調達を実績として今後事業拡大することが期待できる事業者であること

サイバー攻撃対処業務における官民連携に係る調査・研究役務

応札資料作成要領

令和８年（2026 年）１１月

防　　衛　　省

1　総則

1.1　適用範囲

本書は、サイバー攻撃対処業務における官民連携に係る調査・研究役務（以下「本役務」という。）の調達における応札資料の作成要領について規定する。

2　防衛省が応札者に提示する資料及び応札者が提出すべき資料

防衛省は、応札者に**表１**に示す資料を提示する。応札者は、それらを受けて、**表２**に示す応札資料を作成し、防衛省へ提出すること。

表１　防衛省が応札者に提示する資料

資料名称	資料内容
仕様書	本役務の仕様を記載したもの。
応札資料作成要領	提案書に記載する項目の概要を記載したもの。
評価手順書	応札者の提案を評価する場合に用いる評価方式、総合評価点の算出方法及び評価基準等を記述したもの。
評価基準表	仕様書に記述された事項のうち、業務内容を中心に提案要求項目として整理し、評価区分、評価の観点、評価配分等を記述したもの。

表２　応札者が防衛省に提示する資料

番号	資料名称	資料内容
1	提案書	評価基準表に記載された評価の観点を踏まえ、仕様書に記載された仕様の実現方法を記載したもの
2	提案書記述箇所対応表	評価基準表の提案書ページ番号欄に、対応する提案書の記載箇所のページ番号を付記したもの。

※　上記以外の補足資料等の提出は原則として認めない。

2.1　提案書作成要領

a)　提案書は、日本語で作成し、必要に応じて用語の解説等を添付すること。

b)　提案書は、評価基準表に掲げられた評価項目の番号順につづること。

c)　提案書は、専門家以外の者にも理解できるよう、日本語で十分に分かりやすい記述とすること。なお、必要に応じて、用語解説などを添付すること。

d)　提案書は、日本産業規格Ａ４版縦に横書き（文字数、行数は任意）で作成することとし、特別に大きな図表等が必要な場合のみ、同規格Ａ３版横にて作成すること。

e)　提案書には、作成した応札者が類推されないよう、会社名を容易に想像できる文言等を記載しないこと。

2.2　提案書記載箇所対応表の作成要領

応札者は、防衛省から提示された別添「評価基準表」の提案書ページ番号欄に、対応する提案書記載箇所のページ番号を記入することにより、対応表を作成すること。

評価基準表の各項目の説明を**表３**に示す。

表３　「評価基準表」の各項目の説明

項目名	項目説明・記入要領	記入者
項目	提案要求事項の分類	防衛省
提案要求項目	応札者に提案を求める事項	防衛省
評価区分	必須事項・任意事項の区分	防衛省
基礎点・加点	各項目における基礎点・加点	防衛省
提案書ページ番号	作成した提案書における該当ページ番号を記載し、該当する提案書のページが存在しない場合には空欄とすること。評価者は各提案要求事項について、本欄に記載されたページのみを対象として採点を行う。	応札者

2.3　提出要領

応札者は、**表４**に示す提出物を令和８年●月●日（●）12 時までに、防衛省大臣官房会計課契約係に提出すること。ただし、提出物のうち２部のみに、会社名を記載すること。

表４　提出物

番号	提出物の名称	提出形式	数量
1	提案書	電子データ	２部（うち１部のみ会社名を記載）
2	提案書記述箇所対応表	電子データ	２部（うち１部のみ会社名を記載）

3　その他

3.1　留意事項

a)　提出物の作成に当たり、質問等を行う必要がある場合には、別紙様式「質問状」に必要事項を記載し、3.2 に示す連絡先にあらかじめ電話連絡した上で、電子メールにて提出すること。

※質問状の提出期限

令和８年●月●日（●）17 時までとする。

b)　前記の提案書に係る内容の作成要領にしたがった提案書ではないと防衛省が判断した場合には、提案書の評価を行わないことがある。

c) 応札者が提出した提案書（特に作業工数に係る）は、低入札価格調査を行う場合の資料とする。
d) 本役務で知り得たいかなる情報(公知の事実を除く。)については、その保全を徹底し、官側の同意を得ることなく無断で第三者に漏洩してはならない。
e) 本役務の成果物については、その著作権も付属して防衛省に移転するものとする。ただし、本役務の以前から所有している著作権及び第三者が所有している著作権については、この限りではない。
f) 提出する提案書等の作成に掛かる経費については支払われない。
g) 提出された提案書等は返却されない。
h) 提出された提案書等について説明を求められた時は、これに応じること。
i) 他の者（法人又は個人）に関する説明内容及び審査状況について、その者の利益を損なう恐れがあると認められる場合には、非開示情報として保護されるものとする。
j) 提案資料等は、契約の一部を構成するものとする。

3.2 質問状に関する連絡先

防衛省大臣官房会計課管理班物品管理係
電話番号：03-3268-3111　内線 20815、20816、20820

サイバー攻撃対処業務における官民連携に係る調査・研究役務

応札資料作成要領

令和８年（2026 年）１１月

防　　衛　　省

1　総則

1.1　適用範囲

本書は、サイバー攻撃対処業務における官民連携に係る調査・研究役務（以下「本役務」という。）の調達における応札資料の作成要領について規定する。

2　防衛省が応札者に提示する資料及び応札者が提出すべき資料

防衛省は、応札者に**表１**に示す資料を提示する。応札者は、それらを受けて、**表２**に示す応札資料を作成し、防衛省へ提出すること。

表１　防衛省が応札者に提示する資料

資料名称	資料内容
仕様書	本役務の仕様を記載したもの。
応札資料作成要領	提案書に記載する項目の概要を記載したもの。
評価手順書	応札者の提案を評価する場合に用いる評価方式、総合評価点の算出方法及び評価基準等を記述したもの。
評価基準表	仕様書に記述された事項のうち、業務内容を中心に提案要求項目として整理し、評価区分、評価の観点、評価配分等を記述したもの。

表２　応札者が防衛省に提示する資料

番号	資料名称	資料内容
1	提案書	評価基準表に記載された評価の観点を踏まえ、仕様書に記載された仕様の実現方法を記載したもの
2	提案書記述箇所対応表	評価基準表の提案書ページ番号欄に、対応する提案書の記載箇所のページ番号を付記したもの。

※　上記以外の補足資料等の提出は原則として認めない。

2.1　提案書作成要領

a)　提案書は、日本語で作成し、必要に応じて用語の解説等を添付すること。

b)　提案書は、評価基準表に掲げられた評価項目の番号順につづること。

c)　提案書は、専門家以外の者にも理解できるよう、日本語で十分に分かりやすい記述とすること。なお、必要に応じて、用語解説などを添付すること。

d)　提案書は、日本産業規格Ａ４版縦に横書き（文字数、行数は任意）で作成することとし、特別に大きな図表等が必要な場合のみ、同規格Ａ３版横にて作成すること。

e)　提案書には、作成した応札者が類推されないよう、会社名を容易に想像できる文言等を記載しないこと。

2.2　提案書記載箇所対応表の作成要領

応札者は、防衛省から提示された別添「評価基準表」の提案書ページ番号欄に、対応する提案書記載箇所のページ番号を記入することにより、対応表を作成すること。

評価基準表の各項目の説明を**表３**に示す。

表３　「評価基準表」の各項目の説明

項目名	項目説明・記入要領	記入者
項目	提案要求事項の分類	防衛省
提案要求項目	応札者に提案を求める事項	防衛省
評価区分	必須事項・任意事項の区分	防衛省
基礎点・加点	各項目における基礎点・加点	防衛省
提案書ページ番号	作成した提案書における該当ページ番号を記載し、該当する提案書のページが存在しない場合には空欄とすること。評価者は各提案要求事項について、本欄に記載されたページのみを対象として採点を行う。	応札者

2.3　提出要領

応札者は、**表４**に示す提出物を令和８年１２月７日（月）12 時までに、防衛省大臣官房会計課契約係に提出すること。ただし、提出物のうち２部のみに、会社名を記載すること。

表４　提出物

番号	提出物の名称	提出形式	数量
1	提案書	電子データ	２部（うち１部のみ会社名を記載）
2	提案書記述箇所対応表	電子データ	２部（うち１部のみ会社名を記載）

3　その他

3.1　留意事項

a)　提出物の作成に当たり、質問等を行う必要がある場合には、別紙様式「質問状」に必要事項を記載し、3.2 に示す連絡先にあらかじめ電話連絡した上で、電子メールにて提出すること。

※質問状の提出期限

令和８年１１月３０日（月）17 時までとする。

b)　前記の提案書に係る内容の作成要領にしたがった提案書ではないと防衛省が判断した場合には、提案書の評価を行わないことがある。

c) 応札者が提出した提案書（特に作業工数に係る）は、低入札価格調査を行う場合の資料とする。
d) 本役務で知り得たいかなる情報(公知の事実を除く。)については、その保全を徹底し、官側の同意を得ることなく無断で第三者に漏洩してはならない。
e) 本役務の成果物については、その著作権も付属して防衛省に移転するものとする。ただし、本役務の以前から所有している著作権及び第三者が所有している著作権については、この限りではない。
f) 提出する提案書等の作成に掛かる経費については支払われない。
g) 提出された提案書等は返却されない。
h) 提出された提案書等について説明を求められた時は、これに応じること。
i) 他の者（法人又は個人）に関する説明内容及び審査状況について、その者の利益を損なう恐れがあると認められる場合には、非開示情報として保護されるものとする。
j) 提案資料等は、契約の一部を構成するものとする。

3.2 質問状に関する連絡先

防衛省大臣官房会計課管理班物品管理係
電話番号：03-3268-3111　内線 20815、20816、20820

技術評価基準表

別添

件名： サイバー攻撃対処業務における官民連携に係る調査・研究役務

項番	提案要求項目		番号	評価区分	評価の観点	得点配分		提案書ページ番号
						基礎点	加点	
1	業務の実施方針等							
	調査及び演習等の内容、方法及び計画	調査内容の妥当性、独創性	(1)	必須	本役務の実施にあたり、本役務の目的及び制約事項を理解した提案になっているか。役務実施事項について、全く記述されていない、仕様書に則った具体的な手法について記述されていない、あるいは記述された内容の実現が明らかに望めないと認められる場合には要求事項を満たさないものとする。	70	－	
			(2)	任意	仕様書2.4.3項に掲げるサイバー攻撃対処演習用の事前教育プログラムが優れている。	－	10	
			(3)	任意	仕様書2.4.4項に掲げるサイバー攻撃対処演習の実施について、要求事項を満たす提案がなされ、要求元や本役務に関連する事業を理解した提案となっている。	－	40	
			(4)	任意	仕様書2.4.6項の演習シナリオを作成するに当たり、十分な攻撃キャンペーンの攻撃手法を取り入れるとともに、ＡＩを十分に活用した上で、実効性があるシナリオを策定できる提案となっている。	－	60	
			(5)	任意	仕様書2.4.7項のサイバー攻撃対処演習の環境について、2.4.6項のシナリオを考慮し、実現性のある環境構築が可能な提案となっている。	－	80	
			(6)	任意	仕様書2.4.9項の欧米主要国の官民連携施策を調査するに当たり、実現性のある調査手法や調査先を示しているか。		10	
			(7)	任意	仕様書に示した内容以外の独自性のある優れた提案がされているか。仕様書に示した内容以外の手法を提案している場合、それが仕様書に示した内容より優れていると言える根拠が示されているか。	－	10	
		調査計画の妥当性、効率性	(8)	必須	調査、演習の手法、日程等に無理がなく、目的に沿った実現性のあるものか。	60	－	
2	実施体制							
	組織の経験・能力	類似業務の経験（組織）	(9)	必須	契約の相手方は、3.1項a)～c)記載の要件を満たす実績を有しているか。有している場合には、その概要について具体的に記載されているか。	30	－	
		ISMS認証	(10)	必須	契約の相手方は、情報セキュリティマネジメントシステム（ISO/IEC 27001又はJIS Q 27001）の第三者認証を有しているか。	30	－	
		調査業務に当たっての管理・バックアップ体制	(11)	必須	契約の相手方は、役務を遂行可能な人員（2.4.4項を参照）を確保しているか。 契約の相手方は、円滑な事業遂行のための人員補助体制を組んでいるか。 契約の相手方の管理者は、調査業務に関する経験や知見はあるか。	30	－	
	業務従事者の経験・能力	調査業務への適性	(12)	任意	業務従事者は、3.2項d）に示す資格について、次に掲げるITSS等のレベルの高い資格を有する場合、そのレベルに応じて加点する。 ・ＣＩＳＳＰ、ＧＩＡＣ、ＣＩＳＡ、ＣＩＳＭ、ＣＲＩＳＣ、ＣＥＨ、ＰＭＰ、技術士（情報工学）、情報処理安全確保支援士、高度情報処理技術者試験等。	－	30	
			(13)	必須	業務従事者が他の手持ち業務等との関係において履行に必要な業務所要に対応できる態勢にあることが記載されているか。（必要工数確保及び名義の流用の防止）	50	－	
		類似調査業務の経験（業務従事者）	(14)	必須	業務従事者は、3.2項b)～c)に記載の要件を満たす実績を有しており、その概要について具体的に記載されているか。	30		
3	賃上げの表明							
	賃上げ表明の実施及び表明書の提出		(15)	任意	令和８年度における対前年度比、又は令和８年における前年比で給与総額を2.5%以上増加させる旨、従業員に表明していること【中小企業等】	－	20	
4	ワーク・ライフ・バランス等の推進に関する指標							
	認定の取得		(16)	任意	次の要件のいずれかを満す事業者であるか。 ①ワーク・ライフ・バランスを推進する企業として、女性活躍推進法、次世代育成支援対策推進法（平成15年法律第120号。以下「次世代法」という。）、青少年の雇用の促進等に関する法律（昭和45年法律第98号。以下「若者雇用促進法」という。）その他関係法令に基づく認定（認定の基準が複数あるものにあっては、労働時間等の働き方その他のワーク・ライフ・バランスに関する基準を満たすものに限る。以下同じ。）を受けていること。 ②女性活躍推進法第８条に基づく一般事業主行動計画（計画期間が終了していないものに限る。）を策定していること。（常時雇用する労働者の数が100人以下のものに限る。）	－	20	
5	マイナンバーカード普及等の推進に対する評価							
	マイナンバーカード普及等の推進に対する評価		(17)	任意	次の要件のいずれかを満す事業者であるか。 ①電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律（平成14年法律第153 号。）第17条第１項第4号、第5号若しくは第6号の規定に該当する事業者であって、同条第4項に規定する取決めを地方公共団体情報システム機構と締結した事業者又は電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律施行規則（平成15年総務省令第120号）第29条第１項の定めにより、総務大臣の認定を受けたものとみなされた事業者であるか。 ②官民データ活用推進基本法第10条第２項に規定する電子情報処理組織を使用して入札に参加する事業者であって、公的個人認証法第3条第1項に定める署名用電子証明書又は第22条に定める利用者証明用電子証明書を用いて入札に参加する事業者であるか。	－	10	

6　デジタル・スタートアップの公共調達参入機会拡大に係る事項								
	デジタル・スタートアップの公共調達参入機会拡大に係る事項		(18)	任意	次の要件のすべてを満す事業者であるか。 ①　中小企業基本法（昭和38年法律第154号）第２条第１項に規定する中小企業者（みなし大企業を除く）であること ②　設立から15年未満であること ③　情報システムに関連した先進技術やアイデアをもって当該事業に主体的に取り組み、今回の調達を実績として今後事業拡大することが期待できる事業者であること	－	10	
					合計	300	300	

別紙様式

質　問　状

令和　　年　　月　　日

社名			
住所			
TEL		FAX	
E-mail			
質問者			
質問に関連する文書名及びページ			
質問内容			

サイバー攻撃対処業務における官民連携に係る調査・研究役務

評価手順書

令和８年（2026 年）１１月

防　　衛　　省

1　総則

1.1　適用範囲

本書は、サイバー攻撃対処業務における官民連携に係る調査・研究役務における評価手順について規定する。

2　落札方式及び得点配分

2.1　落札方式

次の要件を全て満たす者のうち、2.2 の総合評価点が最も高い者を落札者とする。

a)　入札価格が予定価格の範囲内であること。

b)　評価基準表に記載される要件のうち、「評価区分」が「必須」とされる「提案要求項目」を全て満たしていること。

2.2　総合評価点の計算

技術点は、評価基準表の提案要求項目ごとに、複数の技術評価者が付与した点数の平均点を算出（小数点以下第３位を四捨五入とする。）し、その合計とする。

総合評価点　＝　技術点　＋　価格点

a)　技術点の配分上限値は６００点（基礎点：３００点、加点：３００点）

基礎点：「評価区分」が「必須」に設定される評価点

加　点：「評価区分」が「任意」に設定される評価点

b)　価格点は、入札価格を予定価格で除して得た値を１から減じて得た値に入札価格に対する評価点配分を乗じて得た値（小数点以下第３位を四捨五入）とする。

価格点 ＝ （１－入札価格÷予定価格）× 価格点の配分

c)　技術点の配分と価格点の配分は２：１とし、価格点の配分上限値は３００点とする。

3　評価の手続き

3.1　技術評価

技術点により技術評価を行う。なお、技術点の評価方法は、後述の「**4 技術点の評価方法**」に示すところによる。

3.2　総合評価

3.1 を通過した応札者について、総合評価点を算出し、最も高い応札者を落札者とする。

4　技術点の評価方法

4.1　提案要求項目における得点配分

評価基準表のとおり。

4.2　基礎点評価

基礎点評価は、評価基準表に示す「評価の観点」に従って行い、技術評価者から１名選出して評価を実施するものとし、要件が満たされている場合は、4.1 に示す評価点を配分し、１項目でも満たされていない場合は、不合格とする。

4.3　加点評価

加点評価は、評価基準表に示す「評価の観点」に従って行い、技術評価者の全員が実施するものとし、要件の充足度合いに応じて、4.1 に示す評価点を上限とし、配分する。

5　落札者の決定

a)　入札者の入札価格が予算決算及び会計令（昭和 22 年勅令第 165 号）第 79 条の規定に基づいて作成された予定価格の制限の範囲内であり、かつ、「2.2　総合評価点の計算」によって得られた総合評価点の最も高い者を落札者とする。ただし、予算決算及び会計令第 84 条の規定に該当する場合は、予算決算及び会計令第 85 条の基準（予定価格に 10 分の６を乗じて得た額）を適用するので、基準に該当する入札が行われた場合は入札の結果を保留する。この場合において、入札参加者は当省の行う事情聴取等の調査に協力しなければならない。

b)　a)の調査の結果、会計法（昭和 22 年法律第 35 号）第 29 条の６第１項ただし書きの規定に該当すると認められるときは、その定めるところにより、予定価格の制限の範囲内の価格をもって入札をした他の者のうち、総合評価点の最も高い者を落札者とすることがある。

c)　落札者となるべき者が２人以上あるときは、直ちに当該入札者又はその代理人にくじを引かせ、落札者を決定するものとする。また、入札者又はその代理人がくじを引くことができないときは、入札執行事務に関係のない職員がこれに代わってくじを引き、落札者を決定するものとする。

d)　契約担当官等は、落札者を決定したときには、その氏名（法人の場合はその名称）及び金額を書面で通知する。また、落札できなかった入札者は、落札の相対的な利点に関する情報（当該入札者と落札者のそれぞれの入札価格及び技術の得点）の提供を要請することができる。

技術評価基準表

別添

件名： サイバー攻撃対処業務における官民連携に係る調査・研究役務

項番	提案要求項目		番号	評価区分	評価の観点	得点配分		提案書ページ番号
						基礎点	加点	
1	業務の実施方針等							
	調査及び演習等の内容、方法及び計画	調査内容の妥当性、独創性	(1)	必須	本役務の実施にあたり、本役務の目的及び制約事項を理解した提案になっているか。役務実施事項について、全く記述されていない、仕様書に則った具体的な手法について記述されていない、あるいは記述された内容の実現が明らかに望めないと認められる場合には要求事項を満たさないものとする。	70	－	
			(2)	任意	仕様書2.4.3項に掲げるサイバー攻撃対処演習用の事前教育プログラムが優れている。	－	10	
			(3)	任意	仕様書2.4.4項に掲げるサイバー攻撃対処演習の実施について、要求事項を満たす提案がなされ、要求元や本役務に関連する事業を理解した提案となっている。	－	40	
			(4)	任意	仕様書2.4.6項の演習シナリオを作成するに当たり、十分な攻撃キャンペーンの攻撃手法を取り入れるとともに、ＡＩを十分に活用した上で、実効性があるシナリオを策定できる提案となっている。	－	60	
			(5)	任意	仕様書2.4.7項のサイバー攻撃対処演習の環境について、2.4.6項のシナリオを考慮し、実現性のある環境構築が可能な提案となっている。	－	80	
			(6)	任意	仕様書2.4.9項の欧米主要国の官民連携施策を調査するに当たり、実現性のある調査手法や調査先を示しているか。		10	
			(7)	任意	仕様書に示した内容以外の独自性のある優れた提案がされているか。仕様書に示した内容以外の手法を提案している場合、それが仕様書に示した内容より優れていると言える根拠が示されているか。	－	10	
		調査計画の妥当性、効率性	(8)	必須	調査、演習の手法、日程等に無理がなく、目的に沿った実現性のあるものか。	60	－	
2	実施体制							
	組織の経験・能力	類似業務の経験（組織）	(9)	必須	契約の相手方は、3.1項a)～c)記載の要件を満たす実績を有しているか。有している場合には、その概要について具体的に記載されているか。	30	－	
		ISMS認証	(10)	必須	契約の相手方は、情報セキュリティマネジメントシステム（ISO/IEC 27001又はJIS Q 27001）の第三者認証を有しているか。	30	－	
		調査業務に当たっての管理・バックアップ体制	(11)	必須	契約の相手方は、役務を遂行可能な人員（2.4.4項を参照）を確保しているか。 契約の相手方は、円滑な事業遂行のための人員補助体制を組んでいるか。 契約の相手方の管理者は、調査業務に関する経験や知見はあるか。	30	－	
	業務従事者の経験・能力	調査業務への適性	(12)	任意	業務従事者は、3.2項d）に示す資格について、次に掲げるITSS等のレベルの高い資格を有する場合、そのレベルに応じて加点する。 ・ＣＩＳＳＰ、ＧＩＡＣ、ＣＩＳＡ、ＣＩＳＭ、ＣＲＩＳＣ、ＣＥＨ、ＰＭＰ、技術士（情報工学）、情報処理安全確保支援士、高度情報処理技術者試験等。	－	30	
			(13)	必須	業務従事者が他の手持ち業務等との関係において履行に必要な業務所要に対応できる態勢にあることが記載されているか。（必要工数確保及び名義の流用の防止）	50	－	
		類似調査業務の経験（業務従事者）	(14)	必須	業務従事者は、3.2項b)～c)に記載の要件を満たす実績を有しており、その概要について具体的に記載されているか。	30		
3	賃上げの表明							
	賃上げ表明の実施及び表明書の提出		(15)	任意	令和８年度における対前年度比、又は令和８年における前年比で給与総額を2.5%以上増加させる旨、従業員に表明していること【中小企業等】	－	20	
4	ワーク・ライフ・バランス等の推進に関する指標							
	認定の取得		(16)	任意	次の要件のいずれかを満す事業者であるか。 ①ワーク・ライフ・バランスを推進する企業として、女性活躍推進法、次世代育成支援対策推進法（平成15年法律第120号。以下「次世代法」という。）、青少年の雇用の促進等に関する法律（昭和45年法律第98号。以下「若者雇用促進法」という。）その他関係法令に基づく認定（認定の基準が複数あるものにあっては、労働時間等の働き方その他のワーク・ライフ・バランスに関する基準を満たすものに限る。以下同じ。）を受けていること。 ②女性活躍推進法第８条に基づく一般事業主行動計画（計画期間が終了していないものに限る。）を策定していること。（常時雇用する労働者の数が100人以下のものに限る。）	－	20	
5	マイナンバーカード普及等の推進に対する評価							
	マイナンバーカード普及等の推進に対する評価		(17)	任意	次の要件のいずれかを満す事業者であるか。 ①電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律（平成14年法律第153 号。）第17条第１項第4号、第5号若しくは第6号の規定に該当する事業者であって、同条第4項に規定する取決めを地方公共団体情報システム機構と締結した事業者又は電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律施行規則（平成15年総務省令第120号）第29条第１項の定めにより、総務大臣の認定を受けたものとみなされた事業者であるか。 ②官民データ活用推進基本法第10条第２項に規定する電子情報処理組織を使用して入札に参加する事業者であって、公的個人認証法第3条第1項に定める署名用電子証明書又は第22条に定める利用者証明用電子証明書を用いて入札に参加する事業者であるか。	－	10	

6　デジタル・スタートアップの公共調達参入機会拡大に係る事項								
	デジタル・スタートアップの公共調達参入機会拡大に係る事項		(18)	任意	次の要件のすべてを満す事業者であるか。 ①　中小企業基本法（昭和38年法律第154号）第２条第１項に規定する中小企業者（みなし大企業を除く）であること ②　設立から15年未満であること ③　情報システムに関連した先進技術やアイデアをもって当該事業に主体的に取り組み、今回の調達を実績として今後事業拡大することが期待できる事業者であること	－	10	
					合計	300	300	

付紙

ワーク・ライフ・バランス等推進企業の評価基準

評価項目	評価等の区分※1		評価（評価配分に対する配点比率）
ワーク・ライフ・バランス等推進企業に対する評価	女性活躍推進法に基づく認定（えるぼし認定企業・プラチナえるぼし認定企業）等	プラチナえるぼし ※2	A（100％）
		えるぼし3段階目 ※3	B（70％）
		えるぼし2段階目 ※3	B（70％）
		えるぼし1段階目 ※3	B（70％）
		行動計画※4	C（40％）
	次世代法に基づく認定（くるみん認定企業・プラチナくるみん認定企業）	プラチナくるみん※5	A（100％）
		くるみん（令和4年4月1日以降の基準）※6	B（70％）
		くるみん（平成29年4月1日～令和4年3月31 日までの基準） ※7	B（70％）
		トライくるみん※8	B（70％）
		くるみん（平成29年3月31日までの基準） ※9	C（40％）
	若者雇用促進法に基づく認定（ユースエール認定企業）		B（70％）
	該当なし		D（0％）

※1 複数の認定等に該当する場合は、最も配点が高い区分により加点を行うものとする。
※2 女性の職業生活における活躍の推進に関する法律等の一部を改正する法律（令和元年法第24 号）による改正後の女性活躍推進法第12 条の規定に基づく認定
※3女性活躍推進法第9条の規定に基づく認定。なお、労働時間等の働き方に係る基準は満たすことが必要。
※4 常時雇用する労働者の数が100 人以下の事業主に限る（計画期間が満了していない行動計画を策定している場合のみ）。
※5 次世代法第15 条の2の規定に基づく認定
※6 次世代法第13 条の規定に基づく認定のうち、次世代育成支援対策推進法施行規則の一部を改正する省令（令和3年厚生労働省令第185 号。以下「令和3年改正省令」という。）による改正後の次世代育成支援対策推進法施行規則（以下「新施行規則」という。）第4条第1項第1号及び第2号の規定に基づく認定
※7 次世代法第13 条の規定に基づく認定のうち、令和3年改正省令による改正前の次世代育成支援対策推進法施行規則第4条又は令和3年改正省令附則第2条第2項の規定に基づく認定（ただし、※9 の認定を除く。）
※8 次世代法第13 条の規定に基づく認定のうち、新施行規則第4条第1項第3号及び第4号の規定に基づく認定
※9 次世代法第13 条の規定に基づく認定のうち、次世代育成支援対策推進法施行規則等の一部を改正する省令（平成29 年厚生労働省令第31 号。以下「平成29 年改正省令」という。）による改正前の次世代育成支援対策推進法施行規則第4条又は平成29 年改正省令附則第2条第3項の規定に基づく認定