

模擬サイバー攻撃試験業務提案競技実施要領

1 趣旨

模擬サイバー攻撃試験業務を委託する相手方を選定するに当たって、優れた提案を求めるため、提案競技を実施するものである。

2 業務内容

別紙「模擬サイバー攻撃試験サービス 提案依頼書」（以下「提案依頼書」という。）のとおり

3 業務委託期間

契約締結の日から令和7年3月31日まで

4 契約価格の上限

金6,000千円（契約締結の日から令和7年3月31日までにおける、提案依頼書に示される業務の過程で発生する総費用の上限であり、消費税及び地方消費税を含む。）

5 参加資格要件

次に掲げる要件の全てを満たす者とする。

- (1) 地方自治法施行令（昭和22年政令第16号）第167条の4第1項及び第2項に規定する者に該当しない者であること。
- (2) 提出書類の提出期限の日から契約締結の時までの間に、青森県から指名停止の措置を受けていない者であること。
- (3) 令和6年2月13日青森県告示第86号（物品等の競争入札参加資格）の規定により、役務の提供を受ける契約で電子計算組織に係るものについてAの等級に格付けされた者で、業務委託の営業種目を有する者であること。
- (4) 日本国内の病院・官公庁・銀行等での試験業務実施実績を有すること。

6 スケジュール

参加資格確認申請書提出期限	令和6年9月13日	16時45分まで
質問受付期限	令和6年9月13日	16時45分まで
企画提案書等提出期限	令和6年10月4日	16時45分まで
プレゼンテーション・ヒアリング	令和6年10月中旬予定	
契約締結	令和6年10月下旬予定	

7 手続等

(1) 提出先・問合せ先

〒030-8553 青森市東造道2-1-1 病院局運営部情報管理課 担当：平野、東
電話 017-726-8221 FAX 017-726-8409
E-mail kazuho_hirano@med.pref.aomori.jp, yohei_higashi@med.pref.aomori.jp

(2) 提案依頼書等の交付

ア 交付期間

令和6年8月29日から令和6年10月4日まで

イ 交付方法

青森県立中央病院ホームページに掲載する。

<https://aomori-kenbyo.jp/posts/23178/>

(3) 参加資格確認申請書の提出

ア 提出期限 令和6年9月13日 16時45分まで

イ 提出場所 7(1)と同じ

ウ 提出方法

参加資格確認申請書(様式第1号)及び競争入札参加資格審査の結果通知書の写しを持参又は郵送で1部提出すること。なお、競争入札参加資格審査の申請をしたが、提出期限までに結果通知書の写しを提出できない場合は、結果通知書を入手次第、速やかに提出するものとする。

エ 辞退

参加資格確認申請書の提出後、辞退する場合には、速やかに提案辞退届(様式任意)を7(1)に持参又は郵送すること。

(4) 参加資格審査結果の通知及び企画提案書等の提出要請

参加資格確認申請書提出者の参加資格を審査した後、令和6年9月20日までに審査結果を書面により通知する。併せて、参加資格を満たす者に対しては、企画提案書等の提出を要請する。

(5) 質問の受付等

ア 受付期限 令和6年9月13日 16時45分まで

イ 受付場所 7(1)と同じ

ウ 質問方法

質問書(様式第2号)を持参、郵送、FAX又は電子メールで提出すること。

エ 回答

令和6年9月20日までに企画提案書等の提出を要請された者全員の参加資格確認申請書に記載された電子メールアドレスに対して7(1)の電子メールアドレスから回答する。

(6) 企画提案書等の提出

ア 提出期限 令和6年10月4日 16時45分まで

イ 提出場所 7(1)と同じ

ウ 提出方法 持参又は郵送で提出すること。

エ 作成要領 別紙「模擬サイバー攻撃試験業務提案競技企画提案書等作成要領」のとおり

(7) その他

ア 手続きに関する書類を持参する場合の受付時間は、土、日、祝日を除く平日8時15分から16時45分までとする。

イ 手続きに関する書類を郵送する場合は、配達証明付き書留郵便に限り、提出期限日又は受付期限日必着とする。

8 審査の概要

(1) 評価基準

別紙「模擬サイバー攻撃試験業務提案競技評価基準」のとおり

(2) プレゼンテーション及びヒアリングの実施

企画提案書、提案価格及び対応可否表について、プレゼンテーション及びヒアリングを実施する。対面による実施を原則とし、時間及び場所については、別途通知する。

(3) 審査方法

企画提案書、提案価格、対応可否表、プレゼンテーション及びヒアリングについて、評価基準に基づいて審査する。

(4) 候補者の選定方法

審査の結果、最も評価点の高かった提案者を、契約の相手方の候補者として選定する。最高点の者が複数の場合は、最高点の者の中で提案価格の金額が最も安価な者を契約の相手方の候補者として選定する。なお、金額も同額の場合については、当該者は当初提案の金額の範囲内で提案価格を再作成し、再提出された提案価格の金額が最も安価な者を契約の相手方の候補者として選定する。

(5) 審査結果の通知

審査結果は、全ての提案者に対して書面により通知する。

9 契約手続

(1) 契約交渉の相手方に選定された者と協議を行い、委託内容、経費等について再度調整を行った上、契約を締結する。

(2) 最も評価点の高かった提案者との協議により契約に至らなかった場合には、次点の者を契約の相手方の候補者として選定し契約の協議を行う。

(3) 契約は、採用された提案内容によることを原則とするが、協議によりその内容を変更する場合がある。

(4) 再委託は県の事前承認を必要とするが、業務の全部又は主たる部分を一括して第三者に委託し、又は請け負わせることはできない。

(5) 契約代金の支払いについては、精算払いとする。

10 その他

(1) 企画提案書及び提案価格については、1者につき1提案とする。

提出書類の作成、提出、ヒアリング及びプレゼンテーション等本提案競技への参加に要する経費については、参加者の負担とする。

(2) 書類等の作成に用いる言語、通貨及び単位は、日本語、日本円、日本の標準時及び計量法（平成4年法律第51号）に定める単位とする。

(3) 失格の要件

次に掲げる事項に該当する者は、失格とする。

ア 提出した書類に虚偽の内容を記載した場合

イ 本要領に示した企画提案書等の作成及び提出に関する条件に違反した場合

- ウ 提案価格の金額が4の契約価格の上限額を超える場合
- エ 記載すべき事項の全部又は一部が記載されていない場合
- オ 対応可否表で「必須」とされている仕様を満たさない場合
- カ 対応可否表における各項目の得点が評価基準に定める最低点数未満である場合
- キ 審査の公平性に影響を与える行為があった場合
- ク 審査に係る構成員に対して、直接、間接を問わず故意に接触を求めた場合
- ケ その他選定結果に影響を及ぼすおそれのある不正行為を行った場合

(4) 提出された書類の取扱い

- ア 提出期限後の書類の追加・修正には原則として応じない。又、提出書類に記載された業務責任者及び技術者は、特別な理由があると認められる場合を除き、変更することができない。
- イ 提出された書類は返却しない。
- ウ 提出された書類は、選定を行う作業に必要な範囲において、複製を作成することがある。
- エ 企画提案書等は、他の提案者に対して非公開とする。

(様式第1号)

令和6年 月 日

青森県立中央病院 殿

住 所

商号又は名称

代表者職氏名

印

模擬サイバー攻撃試験業務提案競技参加資格確認申請書

令和6年8月29日付けで公募のありました標記に係る提案競技に参加したいので、関係書類を添えて申請します。

なお、次の事項に該当しないこと並びにこの申請書及び添付書類のすべての記載事項については、事実と相違ないことと誓約いたします。

- (1) 地方自治法施行令（昭和22年政令第16号）第167条の4第1項及び第2項に規定する者に該当しない者であること。
- (2) 青森県から指名停止の措置を受けていない者であること。

(添付書類)

- 1 提案者概要表（別紙1）
- 2 本業務に係る実施体制（様式任意）
- 3 試験業務実施実績申告書（別紙2）

本件に係る連絡先

所 属

担当者名

電 話

F A X

e-mail

提 案 者 概 要 表

1 提案者の状況（令和6年4月1日現在）

(1) 本社

商号又は名称	
住所	
代表者氏名	
電話番号	
資本金	
従業員数	
営業年数	

(2) 青森県内に本店を有しない場合、青森県最寄りの支店・営業所

名称	
住所	
代表者名	
電話番号	

(3) 入札参加資格

等級	業種	営業種目
	U 電子計算組織に係るもの	U01 システム開発 U02 システム維持管理 U03 業務委託 U04 ソフトウェア賃貸借 U99 その他（ ）

※等級を記入し、営業種目として届出していないものを消去すること

2 本業務に係る実施体制

(組織体制、業務担当者を明示するものとし、様式は任意とする。)

(別紙2)

令和6年 月 日

青森県立中央病院 殿

住 所
商号又は名称
代表者職氏名

印

試験業務実施実績申告書

試験業務実施実績について、下表のとおり申告します。

No.	事業所名	所在地	従業員数	実施年月日
1				
2				
3				
4				
5				

- ※ 日本国内の病院、官公庁、金融機関等での試験業務実施実績を1つ以上記載すること。
- ※ 契約書の写し等の実績を証明できる資料を添付すること。
- ※ 事業所名や所在地を公開できない場合は、「X病院」「近畿地方」等と記載してよい。
この場合、契約書の写し等は、「■■■病院」等のように、事業所を特定できる情報を黒塗りにしてよい。

(様式第2号)

令和6年 月 日

青森県立中央病院 殿

住 所

商号又は名称

代表者職氏名

模擬サイバー攻撃試験業務提案競技に係る質問書

模擬サイバー攻撃試験業務提案競技について、次のとおり質問があるので提出します。

資 料 名	
条項又はページ	
内 容	

※ 電子メールにより送付する場合は、押印が不要であること

資料名は、配布した資料の名称を記載すること

本件に係る連絡先

所 属

担当者名

電 話

F A X

e-mail

(様式第3号)

令和6年 月 日

青森県立中央病院 殿

住 所

商号又は名称

代表者職氏名

印

模擬サイバー攻撃試験業務提案競技に係る企画提案書等

模擬サイバー攻撃試験業務提案競技について、次のとおり企画提案書等を提出いたします。

【提出物】

- | | | |
|---------------|------|------|
| ・企画提案書 | 正本1部 | 副本8部 |
| ・提案価格（様式第4号） | 正本1部 | 副本8部 |
| ・対応可否表（様式第5号） | 正本1部 | 副本8部 |

青森県立中央病院 殿

住 所
商号又は名称
代表者職氏名 印

提 案 価 格

業務名 模擬サイバー攻撃試験業務

億	千	百	十	万	千	百	十	円

- 1 上記費用には、消費税及び地方消費税を含んでいます。
- 2 費用内訳は別紙のとおりです。

(様式第5号)

令和6年 月 日

模擬サイバー攻撃試験サービス 対応可否表

- ・対応可能である仕様内容に「○」、対応不可である仕様内容に「×」をつけること。
- ・「必須」と記載された仕様内容は必ず満たすこと。

仕様番号			仕様内容	対応可否	配点
1			基本要件		
1	1		実施目的		
1	1	1	国内の医療機関においてサイバー攻撃の脅威が高まっているため、自施設の院内ローカルエリアネットワーク（以下、LAN）に対し、現実のサイバー攻撃シナリオを模した試験（以下、試験）を実施することで、当院のセキュリティ基盤の脆弱性を明らかにし、今後の基盤整備に資する知見を得る。また、各試験の痕跡を収集し、インシデント対応技術の向上に役立つ資料を得る。		
1	2		調達範囲		
1	2	1	模擬サイバー攻撃試験サービス 一式		
1	3		実施期限		
1	3	1	令和6年11月1日から30日の間の平日に試験を実施すること。		5
1	3	2	試験終了から令和7年1月31日までの間に試験結果の報告会を実施すること。		5
1	3	3	令和7年3月28日までの間、試験結果についての問い合わせ等を受け付けること。		5
1	4		用語の定義		
1	4	1	【LAN】発注者の組織内のローカルエリアネットワーク		
1	4	2	【WAN】外部ワイドエリアネットワーク		
1	4	3	【試験用マルウェア】現実に存在するマルウェアまたはそれを加工したファイルで、試験環境下で安全に実行でき、試験後は除去できることが保証されたもの。		
1	4	4	【試験用サーバ】試験の実施及び評価を行うサーバで、受注者がWAN上に置く。		
1	4	5	【評価用端末】攻撃試験の対象及び起点となる端末。LAN上のWindows端末の中から、発注者が指定する。		
1	5		実施概要		
1	5	1	模擬サイバー攻撃試験を実施する。	必須	
1	5	2	試験で得られた各種データを含む、評価レポートを提出する。	必須	
1	5	3	報告会を実施する。	必須	
1	5	4	評価レポート及び報告会の内容についての問い合わせに一定期間対応する。	必須	
1	5	5	問い合わせ期間の終了後、受注者は試験で取得した全てのデータを破棄し、その旨を書面で報告する。	必須	
1	6		実施環境		
1	6	1	試験は発注者の組織内LANに対して実施する。LANには約3,000台の各種端末（Windows10、Windows11、WindowsServer、CentOS、MacOS、iOS、Android等）が接続されている。		
1	6	2	発注者が指定するWindows端末を「評価用端末」として用いる。評価用端末は次の役割を担う。 ・1.7.1 メール攻撃試験において、WANからの模擬メール攻撃を受ける対象端末となる。 ・1.7.2 試験用マルウェアのダウンロード試験において、試験用マルウェア等のダウンロードの可否を当該端末上で試験する。 ・1.7.3 マルウェア実行試験において、当該端末上で試験用マルウェアの実行を試みる。 ・1.7.4 情報流出試験において、外部への情報流出試験の基点となる。 ・1.7.5 横展開試験を実行する際の基点となる。		
1	6	3	試験の実施のため、外部に試験用サーバを置く場合、同サーバと通信できるのは評価用端末のみとすること。	必須	

仕様番号			仕様内容	対応可否	配点
1	6	4	評価用端末として、条件の異なる2台の端末（A、B）を指定して試験ができること。この場合、受注者は、AとBそれぞれについて1.7.1～1.7.5に示す試験を実施し、AとBの成績の比較を報告書に含めることとする。 （注：受注者が提示する見積金額内で、2台の評価用端末について試験を実施し報告書を作成できる場合は「○」と回答する。1台までの場合は「×」と回答する。）		20
1	6	5	評価用端末の性能は次のとおりとする。 ・ Windows11 pro 64bit（直近のアップデート済み） ・ 4コア CPU ・ RAM 8GB ・ ディスク空き容量 100GB ・ 1NIC ・ メールソフト：Outlook ・ Webブラウザ：Edge （注：この性能の端末で全ての試験が実施できる場合は「○」と回答する。より高い性能が必要な場合は「×」と回答する。）		5
1	7		基本機能		
1	7	1	「メール攻撃試験」として、外部から評価用端末へ、試験用マルウェアを添付したEメールが到達できるかを試験できる。詳細は 2.1. 参照。		
1	7	2	「試験用マルウェアのダウンロード試験」として、外部から評価用端末へ、模擬マルウェアのダウンロードが可能かを試験できる。詳細は 2.2. 参照。		
1	7	3	「マルウェア実行試験」として、評価用端末上で、試験用マルウェアの実行の可否を試験できる。詳細は 2.3. 参照。		
1	7	4	「情報流出試験」として、評価用端末から外部への情報流出の可否を試験できる。詳細は 2.4. 参照。		
1	7	5	「横展開試験」として、評価用端末からLAN上の到達可能な端末への横展開が可能かを試験できる。詳細は 2.5. 参照。		
1	7	6	各攻撃の実施時刻及び実施内容のタイムラインログをCSVまたはxlsx形式のファイルで提出できる。		
1	7	7	試験した攻撃手段を、MITRE ATT&CK（v15.1以降とする）に準拠した ATT&CK ID別に整理して報告書に含めることができる。（以下、「T～」は ATT&CK IDを示す）		
1	8		安全対策		
1	8	1	受注者は攻撃試験の実施にあたり安全対策責任者を置くこと。	必須	
1	8	2	安全対策責任者は、試験の実施中、オンサイトで立ち会うこと。		10
1	8	3	安全対策責任者は、評価用端末を除く、LAN上のすべての機器（端末、サーバ、ネットワーク機器、その他）に対し、設定変更や既存データの上書き等、復元困難な障害を及ぼす恐れのある機能が、攻撃試験用のツールに含まれていないことを確認すること。	必須	
1	8	4	安全対策責任者は、試験中に何らかの障害が生じた場合、並びに発注者からの指示があった場合、直ちに試験を中断すること。	必須	
1	8	5	安全対策責任者は、試験に起因することが疑われる、次に例示する悪影響が発生した場合、関係ベンダーと連携して、調査報告を行い、復旧に努めること。 ・ LAN上の端末の不具合 ・ 医療情報システム（電子カルテシステム、医事システム、各部門システム等）の不具合 ・ ファイル等の上書きや消失 ・ その他利用者に影響のある不具合	必須	
1	9		機密保持		
1	9	1	当院セキュリティポリシー（青森県情報セキュリティ基本方針、青森県情報セキュリティ対策基準）を遵守すること。	必須	
1	9	2	受注者は、業務によって知り得た発注者の業務上の機密及び業務の履行過程で生じた成果物に関する情報を業務の目的以外に使用し、または外部に開示し、若しくは漏洩しないこと。	必須	
1	9	3	受注者は、業務員に対し、前項を遵守するよう指導、監督すること。また、機密事項が記録された資料、電磁的記録媒体等（以下「機密資料等」という。）を適正に管理すること。	必須	
1	9	4	受注者は、機密資料等を保管する場合は、室内の施錠のできる場所に厳重に保管すること。	必須	

仕様番号				仕様内容	対応可否	配点
1	9	5		受注者は、機密資料等の利用等が完了した場合は、速やかに発注者に返還し、または発注者からの指示により責任を持って廃棄すること。	必須	
1	9	6		受注者は、機密資料等を取り扱った者が退職する場合、受注者所定の機密保持に関する規則等により、当該者に対する業務に関する機密保持を適正に実施すること。	必須	
1	9	7		受注者は、上記事項について、県が開示する情報セキュリティポリシーの内容を十分理解した上で、業務従事者及びその他すべての関係者に遵守を徹底すること。	必須	
1	9	8		発注者は、受注者が情報セキュリティポリシーに基づき適切な管理を行っているか、業務期間中、随時確認を行い、その結果に基づく指摘等を行うことができるものとする。指摘等があった場合、受注者はその内容に従うこと。	必須	
2				サービス要件		
2	1			メール攻撃試験		
2	1	1		試験用マルウェアが添付されたEメールを、外部から評価用端末に送信し、受信可否を検査する。試験用マルウェアの種類は枝番の通りとする。	必須	
2	1	1	1	ランサムウェア等、暗号化を行う機能が含まれた試験用マルウェア		2
2	1	1	2	評価用端末の認証情報等を窃取する機能が含まれた試験用マルウェア		2
2	1	1	3	Excel、Word等のアプリケーションの脆弱性をつくコードが含まれた試験用マルウェア		2
2	1	1	4	評価用端末から別端末への横展開を行う機能が含まれた試験用マルウェア		2
2	1	1	5	偽警告等、悪意のあるコードが実行されたかのように振る舞う機能が含まれた試験用マルウェア		2
2	1	1	6	ファイルタイプが偽装されたファイル		2
2	1	2		1,000種類以上の試験用マルウェアの送信を試験できること。		2
2	1	3		外部から評価用端末に送信したEメールの件名、送信日時、添付ファイル名を含むリストを、CSVまたはxlsx形式のファイルで提出できること。		4
2	1	3	1	試験に使用したマルウェア検体のファイルハッシュ値を、2.1.3のリストに含めることができること。		1
2	1	3	2	試験に使用したマルウェア検体に含まれるエクスプロイトコードのCVE識別子を、2.1.3のリストに含めることができること。		1
2	2			試験用マルウェアのダウンロード		
2	2	1		外部から評価用端末へ、試験用マルウェアのダウンロードを発生させ、ダウンロードの可否を検査する。試験用マルウェアの種類は枝番の通りとする。	必須	
2	2	1	1	ランサムウェア等、暗号化を行う機能が含まれた試験用マルウェア		2
2	2	1	2	評価用端末の認証情報等を窃取する機能が含まれた試験用マルウェア		2
2	2	1	3	Excel、Word等のアプリケーションの脆弱性をつくコードが含まれた試験用マルウェア		2
2	2	1	4	評価用端末から別端末への横展開を行う機能が含まれた試験用マルウェア		2
2	2	1	5	偽警告等、悪意のあるコードが実行されたかのように振る舞う機能が含まれた試験用マルウェア		2
2	2	1	6	ファイルタイプが偽装されたファイル		2
2	2	2		ダウンロードを試みた相手先のURL、IPアドレス、ポート番号、セッション開始時刻、ファイル名、ファイルサイズを含むタイムラインログデータを、CSVまたはxlsx形式のファイルで提出する。		6
2	2	2	1	試験に使用した模擬マルウェア検体のファイルハッシュ値を、2.3.2のデータに含めることができる。		1
2	2	2	2	試験に使用した模擬マルウェア検体に含まれるエクスプロイトコードのCVE識別子を、2.3.2のデータに含めることができる。		1
2	3			試験用マルウェアの実行		
2	3	1		評価用端末上で、本項の枝番に例示する試験用マルウェアを起動し、マルウェアとしての一連の動作を完了できるかどうかを試験する。	必須	
2	3	1	1	PowerShellコマンドを利用した試験用マルウェア		2

仕様番号				仕様内容	対応可否	配点
2	3	1	2	Windowsコマンドシェルを利用した試験用マルウェア		2
2	3	1	3	.Net Framework、Visual Basicを利用した試験用マルウェア		2
2	3	1	4	DLL等を利用した試験用マルウェア		2
2	3	2		実行した試験用マルウェアのファイル名、実行時刻（時:分:秒形式）が含まれたタイムラインログデータを、CSVまたはxlsx形式のファイルで提出すること。		6
2	3	2	1	試験に使用した模擬マルウェア検体のファイルハッシュ値を、2.4.2のデータに含めることができる。		2
2	3	2	2	試験に使用した模擬マルウェア検体に含まれるエクスプロイトコードのCVE識別子を、2.4.2のデータに含めることができる。		2
2	3	3		評価用端末上で、一連の模擬マルウェアの実行が済んだ直後に、ファストフォレンジックデータを収集できること。収集は発注者が行い、サイバーディフェンス社CDIR-Collectorを用いる。		2
2	4			情報流出試験		
2	4	1		評価用端末から外部へ、本項の枝番に例示する送信方法で、情報流出を模したテストデータ送信を試み、送信の可否を試験する。		
2	4	1	1	HTTPによる送信		1
2	4	1	2	HTTPSによる送信		1
2	4	1	3	DNSプロトコルによる送信		1
2	4	1	4	FTPによる送信		1
2	4	1	5	SMTPによる送信		1
2	4	1	6	SMBプロトコルによる送信		1
2	4	1	7	ICMPによる送信		1
2	4	1	8	Telnetによる送信		1
2	4	1	9	オープンポートの探索及び同ポートを利用したTCPによる送信		1
2	4	1	10	Google Driveへのアップロード		1
2	4	1	11	One Driveへのアップロード		1
2	4	2		それぞれの試験送信を試みた際の、送信方法、宛先IPアドレス、ポート番号、送信開始時刻を含むタイムラインログデータをCSVまたはxlsx形式のファイルで提出すること。		4
2	5			横展開試験		
2	5	1		次の要領で横展開試験を行う。 ・あらかじめ発注者が「除外対象」をIPアドレス単位またはセグメント単位で指定する。 ・受注者は、評価用端末から、除外対象を除く、LAN上のできるだけ多くの端末に対し、本項の枝番に例示する手段を含む各種技術的手段を複合的に利用して横展開を試みる。	必須	
2	5	1	1	LAN内の利用可能なリモートサービス（T1021、T1210）の検索及びこれを利用した横展開を試験する。		1
2	5	1	2	LAN内の利用可能なソフトウェア展開ツール（T1072）の検索及びこれを利用した横展開を試験する。		1
2	5	1	3	内部スピアフィッシング（T1534）を利用した横展開を試験する。		1
2	5	1	4	パスワードハッシュ、Kerberosチケット、アプリケーションアクセストークンなどの代替認証情報（T1550）を利用した横展開を試験する。		1
2	5	1	5	既存のリモートサービスセッションの乗っ取り（T1563）を利用した横展開を試験する。		1
2	5	1	6	横展開用のツールや端末内の既存のツール（T1570）を利用した横展開を試験する。		1
2	5	1	7	LLMNR/NBT-NS Poisoning等、AiTM攻撃（T1557）を利用した認証突破による横展開を試験する。		1
2	5	1	8	Password Spraying等、ブルートフォース攻撃（T1110）を利用した認証突破による横展開を試験する。		1

仕様番号				仕様内容	対応可否	配点
2	5	1	9	LSASSメモリ等、OS認証情報のダンプ（T1003）を利用した認証突破による横展開を試験する。		1
2	5	1	10	アクセストークンの操作（T1134）を利用した権限昇格による横展開を試験する。		1
2	5	2		横展開試験の実施及び評価のため、外部ワイドエリアネットワーク（以下、WAN）上のサーバとの通信を確立する必要がある場合、同サーバと通信できるのは評価用端末のみとすること。	必須	
2	5	3		試験の結果、侵入してきた端末、侵入時刻、侵入に利用した手段（Mitre IDと関連付けること）、侵入ルートの評価レポートに含めるとともに、タイムラインログをCSVまたはxlsx形式のファイルで提出すること。		5
2	5	4		試験の結果、ネットワーク内の探索により収集できた情報として、発見した端末、認証情報、トークン情報、共有フォルダ等、収集時刻を評価レポートに含めるとともに、タイムラインログをCSVまたはxlsx形式のファイルでも提出すること。		5
2	5	5		横展開試験の実施及び評価のため、外部のサーバとの通信を確立する必要がある場合、同サーバと通信できるのは評価用端末のみとすること。	必須	
2	5	6		横展開の対象となる端末上にテンポラリファイルまたはテンポラリフォルダが作成されるか。 作成されない場合：○を入力し、枝番1～3は空欄とすること。この場合、5点とする。 作成される場合：×を入力し、枝番1～3にも回答を入力すること。この場合、枝番1～3の配点はそれぞれ1点、2点、2点とする。		5
2	5	6	1	テンポラリフォルダの作成は1端末につき1つまでとし、すべてのテンポラリファイルはその配下に置くこと。テンポラリフォルダを作成しない場合、テンポラリファイルの作成は1端末につき1つまでとすること。		(1)
2	5	6	2	作成したテンポラリフォルダ及びテンポラリファイルは、試験終了までに削除すること。試験中に利用者が偶然端末をオフラインにするなど、何らかの事由で削除できなかった場合は、次項の提出リスト内に削除未完了フラグを立てて明示すること。		(2)
2	5	6	3	作成したテンポラリフォルダ及びファイルのリストを評価レポートに含めるとともに、CSVまたはxlsx形式で提出すること。当該リストは、次の情報を含むものとする。 ・ 端末識別情報（ホスト名、MACアドレス等） ・ 端末のIPアドレス ・ 作成場所のフルパス ・ 作成したフォルダ名及びファイルの名称 ・ ファイルサイズ ・ 作成日時 ・ 最終更新日時 ・ 削除完了日時（削除できなかった場合は空欄） ・ 削除未完了フラグ		(2)
2	5	7		横展開を受けた端末からファストフォレンジックデータを抽出するため、横展開に成功した端末のホスト名、IPアドレス等の情報を、試験終了後に直ちに発注者に報告できること。		5
2	6			評価レポート		
2	6	1		評価レポートは日本語主体で作成すること。添付資料として英文を含んでよいが、発注者がその内容について問い合わせた場合は日本語で回答すること。	必須	
2	6	2		評価レポートに含まれる、当院の情報に関する表やリストは、別途、二次利用可能なファイル形式（CSV形式、xlsx形式等）のファイルで添付すること。		
2	6	3		成功した攻撃に対応する有効な対策についての提案が含まれていること。		10
2	6	4		成功した攻撃に対応する MITRE ATT&CK IDを記載し、技術及び緩和策の概要を日本語でレポート内に含めること。		5
2	7			報告会及び問い合わせ対応		
2	7	1		概ね2時間程度の報告会を実施すること。開催形式はオンライン、オンサイトのいずれでもよい。	必須	
2	7	2		試験内容、評価レポート、報告会の内容に関する発注者からの問い合わせに対し、概ね3営業日以内に回答すること。回答はEメールで行うこと。	必須	
3				その他		
3	1			疑義取り扱い		
3	1	1		本提案依頼書に定めのない事項及び疑義が生じた場合は、発注者と受注者で協議の上、決定するものとする。	必須	