模擬サイバー攻撃試験サービス　提案依頼書

・対応可否「必須」の仕様は必ず満たすこと。
・対応可否が空欄の項目は、当該欄に〇または×を入力すること。〇の場合、所定の配点を加算する。

仕様番号				仕様内容
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。
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。
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。
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。
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。
1	5	3		報告会を実施する。
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。
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。
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。

仕様番号				仕様内容
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。
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。）
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。）
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等を試験できる。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。
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。
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。
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。
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
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。
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。

仕様番号				仕様内容
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。
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。
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。
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。
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。
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。
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。
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	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	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	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	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	1	1	6	ファイルタイプが偽装されたファイル
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	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。
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。
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。
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。
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	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	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	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	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	6	ファイルタイプが偽装されたファイル
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。

仕様番号				仕様内容
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。
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。
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。
2	3	1	1	PowerShellコマンドを利用した試験用マルウェア
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	3	1	3	.Net Framework、Visual Basicを利用した試験用マルウェア
2	3	1	4	DLL等を利用した試験用マルウェア
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。
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	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	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	**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
2	4	1	2	HTTPSによる送信
2	4	1	3	DNSプロトコルによる送信
2	4	1	4	FTPによる送信
2	4	1	5	SMTPによる送信
2	4	1	6	SMBプロトコルによる送信
2	4	1	7	ICMPによる送信
2	4	1	8	Telnetによる送信
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
2	4	1	10	Google Driveへのアップロード
2	4	1	11	One Driveへのアップロード
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。
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。
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。
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。

仕様番号				仕様内容
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。
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。
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。
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。
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。
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。
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。
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。
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。
2	5	3		試験の結果、侵入できた端末、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形式のファイルで提出すること。
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。
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。
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：〇を入力し、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：x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。
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。
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	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こと。 ・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	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。
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。
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。

仕様番号				仕様内容
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。
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。
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。
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。
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こと。