「2022年度ペネトレーションテストによる独立行政法人等の情報システムに対するセキュリティ対策状況調査（その1）」に係る一般競争入札

（総合評価落札方式）

入札説明書

2022年4月8日

独立行政法人情報処理推進機構

目　　次

Ⅰ．入札説明書

独立行政法人情報処理推進機構の請負契約に係る入札公告（2022年4月8日付け公示）に基づく入札については、関係法令並びに独立行政法人情報処理推進機構会計規程及び同入札心得に定めるもののほか、下記に定めるところにより実施する。

記

1．競争入札に付する事項

(1) 作業の名称　2022年度ペネトレーションテストによる独立行政法人等の情報システムに対するセキュリティ対策状況調査（その1）

(2) 作業内容等　別紙仕様書のとおり。

(3) 履 行 期 限　別紙仕様書のとおり。

(4) 作 業 場 所　別紙仕様書のとおり。

(5) 入 札 方 法　落札者の決定は総合評価落札方式をもって行うので、

① 入札に参加を希望する者（以下「入札者」という。）は「6.(4)提出書類一覧」に記載の提出書類を提出すること。

② 上記①の提出書類のうち提案書については、入札資料作成要領に従って作成、提出すること。

③ 上記①の提出書類のうち、入札書については仕様書及び契約書案に定めるところにより、入札金額を見積るものとする。入札金額は、「2022年度ペネトレーションテストによる独立行政法人等の情報システムに対するセキュリティ対策状況調査（その1）」に関する総価とし、総価には本件業務に係る一切の費用を含むものとする。

④ 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パーセントに相当する額を加算した金額（当該金額に1円未満の端数が生じたときは、その端数金額を切捨てるものとする。）をもって落札価格とするので、入札者は、消費税及び地方消費税に係る課税事業者であるか免税事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。

⑤ 入札者は、提出した入札書の引き換え、変更又は取り消しをすることはできないものとする。

2．競争参加資格

(1) 予算決算及び会計令（以下「予決令」という。）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) 予決令第71条の規定に該当しない者であること。

(3) 令和4・5・6年度競争参加資格（全省庁統一資格）において「役務の提供等」で、「A」、「B」又は「C」の等級に格付けされている者であること。

(4) 「情報セキュリティサービス基準適合サービスリスト[1]」の脆弱性診断サービス分野に掲載されている者であること（新規又は更新の手続き中を含む）。

(5) 各省各庁及び政府関係法人等から取引停止又は指名停止処分等を受けていない者（理事長が特に認める場合を含む。）であること。

(6) 経営の状況又は信用度が極度に悪化していないと認められる者であり、適正な契約の履行が確保される者であること。

(7) 過去3年以内に情報管理の不備を理由に機構から契約を解除されている者ではないこと。

[1] 経済産業省が策定した「情報セキュリティサービス基準」への適合性を審査登録機関により審査し、認められた、事業者の情報セキュリティサービスのリストで、IPA により公開している。

3. 入札者の義務

(1) 入札者は、当入札説明書及び独立行政法人情報処理推進機構入札心得を了知のうえ、入札に参加しなければならない。

(2) 入札者は、当機構が交付する仕様書に基づいて提案書を作成し、これを入札書に添付して入札書等の提出期限内に提出しなければならない。また、開札日の前日までの間において当機構から当該書類に関して説明を求められた場合は、これに応じなければならない。

4. 入札説明会の日時・実施方法及び参加方法

(1)入札説明会の日時

2022年4月13日（水）15時00分

(2) 入札説明会実施方法

オンラインによる説明会とする。

(3) 入札説明会参加方法

入札説明会（オンライン）への参加を希望する場合は、14.(5)の担当部署まで、以下のとおり電子メールにより申し込むこと。

① オンラインによる説明会は会議招待メールを送信する必要があるため、2022年4月11日（月）17時00分までに申し込むこと。

② 電子メールの件名に「【2022年度ペネトレーションテストによる独立行政法人等の情報システムに対するセキュリティ対策状況調査（その1）】入札説明会申し込み」と明記し、入札説明会に参加する者の所属名・氏名及びメールアドレスを記載の上申し込むこと。

※ 本入札説明会は、「2022年度ペネトレーションテストによる独立行政法人等の情報システムに対するセキュリティ対策状況調査（その1）～（その3）」合同で開催する。

5. 入札に関する質問の受付等

(1) 質問の方法

質問書（様式1）に所定事項を記入の上、電子メールにより提出すること。

(2) 受付期間

2022年4月13日（水）から2022年4月21日（木） 17時00分まで。

なお、質問に対する回答に時間がかかる場合があるため、余裕をみて提出すること。

(3) 担当部署

14.(5)のとおり

6. 入札書等の提出方法及び提出期限等

(1) 受付期間

2022年4月26日（火）から2022年4月28日（木）

持参の場合の受付時間は、月曜日から金曜日(祝祭日は除く)の10時00分から17時00分(12時30分～13時30分の間は除く）とする。

(2) 提出期限

2022年4月28日（木） 17時00分必着。

上記期限を過ぎた入札書等はいかなる理由があっても受け取らない。

(3) 提出先

14.(5)のとおり。

(4) 提出書類一覧

No.	提出書類		部数
①	委任状（代理人に委任する場合）	様式２	１通
②	入札書（封緘）	様式３	１通
③	提案書	－	各１部
④	評価項目一覧	－	
⑤	令和４・５・６年度競争参加資格（全省庁統一資格）における資格審査結果通知書の写し	－	１通
⑥	「情報セキュリティサービス基準適合サービスリ	－	１通

	スト」の申請書の写し（リスト掲載の手続き中の場合）		
⑦	③と④の電子ファイル	－	各1部
⑧	提案書受理票	様式4	1通

(5) 提出方法

① 入札書等提出書類を持参により提出する場合

入札書を封筒に入れ封緘し、封皮に氏名（法人の場合は商号又は名称）、宛先（14.(5)の担当者名）を記載するとともに「2022年度ペネトレーションテストによる独立行政法人等の情報システムに対するセキュリティ対策状況調査（その1）　一般競争入札に係る入札書在中」と朱書きし、その他提出書類一式と併せ封筒に入れ封緘し、その封皮に氏名（法人の場合はその商号又は名称）、宛先（14.(5)の担当者名）を記載し、かつ、「2022年度ペネトレーションテストによる独立行政法人等の情報システムに対するセキュリティ対策状況調査（その1）　一般競争入札に係る提出書類一式在中」と朱書きすること。なお、入札書等提出書類を持参により提出する場合は、持参日の前営業日18時までに14.(5)の担当部署宛に電子メールで連絡すること。連絡なしで持参する場合は受け取れない場合がある。

② 入札書等提出書類を郵便等（書留）により提出する場合

二重封筒とし、表封筒に「2022年度ペネトレーションテストによる独立行政法人等の情報システムに対するセキュリティ対策状況調査（その1）　一般競争入札に係る提出書類一式在中」と朱書きし、中封筒の封皮には直接提出する場合と同様とすること。

なお、提出書類一覧（6.(4)）の「⑦：③と④の電子ファイル」の提出は、感染症予防対策のため、CDに収録して提出する方法の他、電子メールによる提出を可能とする。その場合、件名に「提案書及び評価項目一覧の提出」と記載した電子メールに電子ファイルを添付し、14.(5)の担当部署へ送付すること。その際、添付する電子ファイルにはパスワードを付与すること。電子ファイルの容量が2MBを超える場合は、送付方法を別途案内するので、余裕をもって14.(5)の担当部署に電子メールで連絡すること。

(6) 提出後

① 入札書等提出書類を受理した場合は、提案書受理票を入札者に交付する。なお、受理した提案書等は評価結果に関わらず返却しない。

②ヒアリングを行う場合は、次の日程で実施する。

日時：2022年5月10日（火）10時30分～17時30分の間（1者あたり1時間を予定）

場所：独立行政法人情報処理推進機構　会議室B

なお、ヒアリングについては、提案内容を熟知した、Ⅲ.仕様書「5.実施体制」のプロジェクト責任者又はペネトレーションテスト責任者が対応すること。また、電子メールやWeb会議等の手段によるヒアリングを行う場合がある。

7. 開札の日時及び場所

(1) 開札の日時

2022年5月16日（月）　14時00分

(2) 開札の場所

東京都文京区本駒込2-28-8　　文京グリーンコートセンターオフィス13階

独立行政法人情報処理推進機構　会議室B

8. 入札の無効

入札公告に示した競争参加資格のない者による入札及び入札に関する条件に違反した入札は無効とする。

9. 落札者の決定方法

独立行政法人情報処理推進機構会計規程第29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、当機構が入札説明書で指定する要求事項のうち、必須とした項目の最低限の要求をすべて満たしている提案をした入札者の中から、当機構が定める総合評価の方法をもって落札者を定めるものと

する。ただし、落札者となるべき者の入札価格によっては、その者により当該契約の内容に適合した履行がなされないおそれがあると認められるとき、又はその者と契約することが公正な取引の秩序を乱すこととなるおそれがあって著しく不適当であると認められるときは、予定価格の範囲内の価格をもって入札をした他の者のうち、評価の最も高い者を落札者とすることがある。

10. 入札保証金及び契約保証金　　全額免除

11. 契約書作成の要否　　要（Ⅱ．契約書　契約書（案）を参照）

12. 支払の条件
　契約代金は、業務の完了後、当機構が適法な支払請求書を受理した日の属する月の翌月末日までに支払うものとする。

13. 契約者の氏名並びにその所属先の名称及び所在地
〒113-6591　東京都文京区本駒込2-28-8　　文京グリーンコートセンターオフィス16階
独立行政法人情報処理推進機構　理事長　富田　達夫

14. その他
(1)　入札者は、提出した証明書等について説明を求められた場合は、自己の責任において速やかに書面をもって説明しなければならない。
(2)　契約に係る情報については、当機構のウェブサイトにて機構会計規程等に基づき公表（注）するものとする。
(3)　本件の落札者は、「2022年度ペネトレーションテストによる独立行政法人等の情報システムに対するセキュリティ対策状況調査（その2）」には応札できないため注意すること。
(4)　落札者は、契約締結時までに入札内訳書及び提案書の電子データを提出するものとする。なお、本請負業務の一部を、第三者（以下「再請負先」という。）に請け負わせる場合、再請負先との契約金額（複数の再請負先がいる場合はその合計額）が、本業務の契約金額の4割を超えてはならない。
(5)　仕様書に関する照会先、入札に関する質問の受付、入札書類の提出先
〒113-6591
東京都文京区本駒込2-28-8　　文京グリーンコートセンターオフィス15階
独立行政法人情報処理推進機構　セキュリティセンター　公共セキュリティ部
セキュリティ監査グループ　担当：益子、入来
TEL：03-5978-7563
E-mail：isec-audit-kobo@ipa.go.jp
　なお、直接提出する場合は、文京グリーンコートセンターオフィス13階の当機構総合受付を訪問すること。
(6)　入札行為に関する照会先
独立行政法人情報処理推進機構　財務部　契約・管財グループ　担当: 田埜入、中尾
TEL：03-5978-7502
E-mail：fa-bid-kt@ipa.go.jp

（注） 独立行政法人の事務・事業の見直しの基本方針（平成 22 年 12 月 7 日閣議決定）
に基づく契約に係る情報の公表について

独立行政法人が行う契約については、「独立行政法人の事務・事業の見直しの基本方針」（平成22年12月7日閣議決定）において、独立行政法人と一定の関係を有する法人と契約をする場合には、当該法人への再就職の状況、当該法人との間の取引等の状況について情報を公開するなどの取組を進めるとされているところです。

これに基づき、以下のとおり、当機構との関係に係る情報を当機構のウェブサイトで公表することとしますので、所要の情報の当方への提供及び情報の公表に同意の上で、応札若しくは応募又は契約の締結を行っていただくよう御理解と御協力をお願いいたします。

なお、案件への応札若しくは応募又は契約の締結をもって同意されたものとみなさせていただきますので、ご了知願います。

（1）公表の対象となる契約先

次のいずれにも該当する契約先

① 当機構において役員を経験した者（役員経験者）が再就職していること又は課長相当職以上の職を経験した者（課長相当職以上経験者）が役員、顧問等として再就職していること

② 当機構との間の取引高が、総売上高又は事業収入の3分の1以上を占めていること

※ 予定価格が一定の金額を超えない契約や光熱水費の支出に係る契約等は対象外

（2）公表する情報

上記に該当する契約先について、契約ごとに、物品役務等の名称及び数量、契約締結日、契約先の名称、契約金額等と併せ、次に掲げる情報を公表します。

① 当機構の役員経験者及び課長相当職以上経験者（当機構OB）の人数、職名及び当機構における最終職名

② 当機構との間の取引高

③ 総売上高又は事業収入に占める当機構との間の取引高の割合が、次の区分のいずれかに該当する旨

3分の1以上2分の1未満、2分の1以上3分の2未満又は3分の2以上

④ 一者応札又は一者応募である場合はその旨

（3）当方に提供していただく情報

① 契約締結日時点で在職している当機構OBに係る情報（人数、現在の職名及び当機構における最終職名等）

② 直近の事業年度における総売上高又は事業収入及び当機構との間の取引高

（4）公表日

契約締結日の翌日から起算して原則として72日以内（4 月に締結した契約については原則として 93 日以内）

（5）実施時期

平成23年7月1日以降の一般競争入札・企画競争・公募公告に係る契約及び平成23年7月1日以降に契約を締結した随意契約について適用します。

なお、応札若しくは応募又は契約の締結を行ったにもかかわらず情報提供等の協力をしていただけない相手方については、その名称等を公表させていただくことがあり得ますので、ご了知願います。

Ⅱ．契約書

2022 情財第〇〇号

契　約　書（案）

独立行政法人情報処理推進機構（以下「甲」という。）と〇〇〇〇〇（以下「乙」という。）とは、次の条項により「2022 年度ペネトレーションテストによる独立行政法人等の情報システムに対するセキュリティ対策状況調査（その 1)」に関する請負契約を締結する。

（契約の目的）

第1条　甲は、別紙仕様書記載の「契約の目的」を実現するために、同仕様書及び提案書記載の「2022年度ペネトレーションテストによる独立行政法人等の情報システムに対するセキュリティ対策状況調査（その1）」（以下、「請負業務」という。）の完遂を乙に注文し、乙は本契約及び関係法令の定めに従って誠実に請負業務を完遂することを請け負う。

2　乙は、本契約においては、請負業務またはその履行途中までの成果が可分であるか否かに拘わらず、請負業務が完遂されることによってのみ、甲が利益を受け、また甲の契約の目的が達成されることを、確認し了解する。

（再請負の制限）

第 2 条　乙は、請負業務の全部を第三者に請負わせてはならない。

2　乙は、請負業務の一部を第三者（以下「再請負先」という。）に請負わせようとするときは、事前に再請負先、再請負の対価、再請負作業内容その他甲所定の事項を、書面により甲に届け出なければならない。その場合、再請負先との契約金額（複数の再請負先がいる場合はその合計額）が、請負業務の契約金額の 4 割を超えてはならない。

3　前項に基づき、乙が請負業務の一部を再請負先に請負わせた場合においても、甲は、再請負先の行為を全て乙の行為とみなし、乙に対し本契約上の責任を問うことができる。

（責任者の選任）

第 3 条　乙は、請負業務を実施するにあたって、責任者（乙の正規従業員に限る。）を選任して甲に届け出る。

2　責任者は、請負業務の進捗状況を常に把握するとともに、各進捗状況について甲の随時の照会に応じるとともに定期的または必要に応じてこれを甲に報告するものとする。

3　乙は、第 1 項により選任された責任者に変更がある場合は、直ちに甲に届け出る。

（納入物件及び納入期限）

第 4 条　納入物件、納入期限及びその他納入に関する事項については、別紙仕様書のとおりとする。

（契約金額）

第 5 条　甲が本契約の対価として乙に支払うべき契約金額は、金〇〇，〇〇〇，〇〇〇円（うち消費税及び地方消費税〇，〇〇〇，〇〇〇円）とする。

（権利義務の譲渡）

第 6 条　乙は、本契約によって生じる権利又は義務を第三者に譲渡し、又は承継させてはならない。

（実地調査）

第 7 条　甲は、必要があると認めるときは、乙に対し、自ら又はその指名する第三者をして、請負業務の実施状況等について、報告又は資料を求め、若しくは事業所に臨んで実地に調査を行うことができる。

2　前項において、甲は乙に意見を述べ、補足資料の提出を求めることができる。

（検査）

第 8 条　甲は、納入物件の納入を受けた日から 30 日以内に、当該納入物件について別紙仕様書及び提案書に基づき検査を行い、同仕様書及び提案書に定める基準に適合しない事実を発見したときは、当該事実の概要を書面によって遅滞なく乙に通知する。

2　前項所定の期間内に同項所定の通知が無いときは、当該期間満了日をもって当該納入物件は同項所定の検査に合格したものとみなす。
3　請負業務は、当該納入物件が本条による検査に合格した日をもって完了とする。
4　第1項及び第2項の規定は、第1項所定の通知書に記載された指摘事実に対し、乙が適切な修正等を行い甲に再納入する場合に準用する。

（契約不適合責任）
第9条　甲は、請負業務完了の日から1年以内に納入物件その他請負業務の成果に種類、品質又は数量に関して仕様書及び提案書の記載内容に適合しない事実（以下「契約不適合」という。）を発見したときは、相当の催告期間を定めて、甲の承認または指定した方法により、その契約不適合の修補、代品との交換又は不足分の引渡しによる履行の追完を乙に請求することができる。但し、発見後合理的期間内に乙に通知することを条件とする。
2　前項において、乙は、前項所定の方法以外の方法による修補等を希望する場合、修補等に要する費用の多寡、甲の負担の軽重等に関わらず、甲の書面による事前の同意を得なければならない。この場合、甲は、事情の如何を問わず同意する義務を負わない。
3　第1項において催告期間内に修補等がないときは、甲は、その選択に従い、本契約を解除し、またはその不適合の程度に応じて代金の減額を請求することができる。ただし、次の各号のいずれかに該当する場合は、第1項に関わらず、催告なしに直ちに解除し、または代金の減額を請求することができる。
一　修補等が不能であるとき。
二　乙が修補等を拒絶する意思を明確に表示したとき。
三　契約の性質又は当事者の意思表示により、特定の日時又は一定の期間内に修補等をしなければ契約の目的を達することができない場合において、乙が修補等をしないでその時期を経過したとき。
四　前各号に掲げる場合のほか、甲が第1項所定の催告をしても修補等を受ける見込みがないことが明らかであるとき。
4　第1項で定めた催告期間内に修補等がなされる見込みがないと合理的に認められる場合、甲は、前項本文に関わらず、催告期間の満了を待たずに本契約を解除することができる。
5　前各項において、甲は、乙の責めに帰すべき事由による契約不適合によって甲が被った損害の賠償を、別途乙に請求することができる。
6　本条は、本契約終了後においても有効に存続するものとする。

（対価の支払及び遅延利息）
第10条　甲は、請負業務の完了後、乙から適法な支払請求書を受理した日の属する月の翌月末日までに契約金額を支払う。なお、支払いに要する費用は甲の負担とする。
2　甲が前項の期日までに対価を支払わない場合は、その遅延期間における当該未払金額に対して、財務大臣が決定する率(政府契約の支払遅延に対する遅延利息の率（昭和24年12月12日大蔵省告示第991号））によって、遅延利息を支払うものとする。
3　乙は、請負業務の履行途中までの成果に対しては、事由の如何を問わず、何らの支払いもなされないことを確認し了解する。

（遅延損害金）
第11条　天災地変その他乙の責に帰すことができない事由による場合を除き、乙が納入期限までに納入物件の納入が終らないときは、甲は遅延損害金として、延滞日数1日につき契約金額の1,000分の1に相当する額を徴収することができる。
2　前項の規定は、納入遅延となった後に本契約が解除された場合であっても、解除の日までの日数に対して適用するものとする。

（契約の変更）
第12条　甲及び乙は、本契約の締結後、次の各号に掲げる事由が生じた場合は、甲乙合意のうえ本契約を変更することができる。
一　仕様書及び提案書その他契約条件の変更（乙に帰責事由ある場合を除く。）。
二　天災地変、著しい経済情勢の変動、不可抗力その他やむを得ない事由に基づく諸条件の変更。
三　税法その他法令の制定又は改廃。
四　価格に影響のある技術変更提案の実施。

2　前項による本契約の変更は、納入物件、納期、契約金額その他すべての契約内容の変更の有無・内容等についての合意の成立と同時に効力を生じる。なお、本契約の各条項のうち変更の合意がない部分は、本契約の規定内容が引き続き有効に適用される。

（契約の解除等）

第13条　甲は、第9条による場合の他、次の各号の一に該当するときは、催告の上、本契約の全部又は一部を解除することができる。但し、第4号乃至第6号の場合は催告を要しない。

一　乙が本契約条項に違反したとき。

二　乙が天災地変その他不可抗力の原因によらないで、納入期限までに本契約の全部又は一部を履行しないか、又は納入期限までの納入が見込めないとき。

三　乙が甲の指示に従わないとき、その職務執行を妨げたとき、又は談合その他不正な行為があったとき。

四　乙が破産手続開始の決定を受け、その他法的整理手続が開始したこと、資産及び信用の状態が著しく低下したと認められること等により、契約の円滑な履行が困難と認められるとき。

五　天災地変その他乙の責に帰すことができない事由により、納入物件を納入する見込みがないと認められるとき。

六　乙が、甲が正当な理由と認める理由により、本契約の解除を申し出たとき。

2　乙は、甲がその責に帰すべき事由により、本契約上の義務に違反した場合は、相当の期間を定めて、その履行を書面で催告し、その期間内に履行がないときは、本契約を解除することができる。

3　乙の本契約違反の程度が著しく、または乙に重大な背信的言動があった場合、甲は第1項にかかわらず、催告せずに直ちに本契約を解除することができる。

4　甲は、第1項第1号乃至第4号又は前項の規定により本契約を解除する場合は、違約金として契約金額の100分の10に相当する金額（その金額に100円未満の端数があるときはその端数を切り捨てる。）を乙に請求することができる。

5　前項の規定は、甲に生じた実際の損害額が同項所定の違約金の額を超える場合において、甲がその超える部分について乙に対し次条に規定する損害賠償を請求することを妨げない。

（損害賠償）

第14条　乙は、乙の責に帰すべき事由によって甲又は第三者に損害を与えたときは、その被った損害を賠償するものとする。ただし、乙の負う賠償額は、乙に故意又は重大な過失がある場合を除き、第5条所定の契約金額を超えないものとする。

2　第11条所定の遅延損害金の有無は、前項に基づく賠償額に影響を与えないものとする。

（違約金及び損害賠償金の遅延利息）

第15条　乙が、第13条第4項の違約金及び前条の損害賠償金を甲が指定する期間内に支払わないときは、乙は、当該期間を経過した日から支払をする日までの日数に応じ、年3パーセントの割合で計算した金額の遅延利息を支払わなければならない。

（秘密保持及び個人情報）

第16条　甲及び乙は、相互に本契約の履行過程において知り得た相手方の秘密を他に漏洩せず、また本契約の履行に必要な範囲を超えて利用しない。ただし、甲が、法令等、官公署の要求、その他公益的見地に基づいて、必要最小限の範囲で開示する場合を除く。

2　乙は、契約締結後速やかに、情報セキュリティを確保するための体制を定めたものを含み、以下に記載する事項の遵守の方法及び提出を求める情報、書類等（以下「情報セキュリティを確保するための体制等」という。）について、甲に提示し了承を得た上で確認書類として提出すること。ただし、別途契約締結前に、情報セキュリティを確保するための体制等について甲に提示し了承を得た上で提出したときは、この限りでない。また、契約期間中に、甲の要請により、情報セキュリティを確保するための体制及び対策に係る実施状況を紙媒体又は電子媒体により報告すること。加えて、これらに変更が生じる場合は、事前に甲へ案を提出し、同意を得ること。

なお、報告の内容について、甲と乙が協議し不十分であると認めた場合、乙は、速やかに甲と協議し対策を講ずること。

3　乙は、本契約遂行中に得た本契約に関する情報（紙媒体及び電子媒体）について、甲の許可なく当機構外で複製してはならない。また、作業終了後には、複製した情報が電子計算機等から消去されていること

を甲が確認できる方法で証明すること。
4　乙は、本契約を終了又は契約解除する場合には、乙において本契約遂行中に得た本契約に関する情報（紙媒体及び電子媒体であってこれらの複製を含む。）を速やかに甲に返却又は廃棄若しくは消去すること。その際、甲の確認を必ず受けること。
5　乙は、契約期間中及び契約終了後においても、本契約に関して知り得た当機構の業務上の内容について、他に漏らし又は他の目的に利用してはならない。ただし、甲の承認を得た場合は、この限りではない。
6　乙は、本契約の遂行において、情報セキュリティが侵害され又はそのおそれがある場合の対処方法について甲に提示すること。また、情報セキュリティが侵害され又はそのおそれがあることを認知した場合には、速やかに甲に報告を行い、原因究明及びその対処等について甲と協議の上、その指示に従うこと。
7　乙は、本契約全体における情報セキュリティの確保のため、「政府機関等の情報セキュリティ対策のための統一基準」等に基づく、情報セキュリティ対策を講じなければならない。
8　乙は、当機構が実施する情報セキュリティ監査又はシステム監査を受け入れるとともに、指摘事項への対応を行うこと。
9　乙は、本契約に従事する者を限定すること。また、乙の資本関係・役員の情報、本契約の実施場所、本契約の全ての従事者の所属、専門性（情報セキュリティに係る資格・研修実績等）、実績及び国籍に関する情報を甲に提示すること。なお、本契約の実施期間中に従事者を変更等する場合は、事前にこれらの情報を甲に再提示すること。
10　個人情報に関する取扱いについては、別添「個人情報の取扱いに関する特則」のとおりとする。
11　本条は、本契約終了後も有効に存続する。

（知的財産権）
第 17 条　請負業務の履行過程で生じた著作権（著作権法第 27 条及び第 28 条に定める権利を含む。）、発明（考案及び意匠の創作を含む。）及びノウハウを含む産業財産権（特許その他産業財産権を受ける権利を含む。）（以下「知的財産権」という。）は、乙又は国内外の第三者が従前から保有していた知的財産権を除き、第 8 条第 3 項の規定による請負業務完了の日をもって、乙から甲に自動的に移転するものとする。なお、乙は、甲の要請がある場合、登録その他の手続きに協力するものとする。
2　乙は、請負業務の成果に乙が従前から保有する知的財産権が含まれている場合は、前項に規定する移転の時に、甲に対して非独占的な実施権、使用権、第三者に対する利用許諾権(再利用許諾権を含む。)、その他一切の利用を許諾したものとみなし、第三者が従前から保有する知的財産権が含まれている場合は、同旨の法的効果を生ずべき適切な法的措置を、当該第三者との間で事前に講じておくものとする。なお、これに要する費用は契約金額に含まれるものとする。
3　乙は、甲及び甲の許諾を受けた第三者に対し、請負業務の成果についての著作者人格権、及び著作権法第 28 条の権利その他“原作品の著作者／権利者”の地位に基づく権利主張は行わないものとする。

（知的財産権の紛争解決）
第 18 条　乙は、請負業務の成果が、甲及び国内外の第三者が保有する知的財産権（公告、公開中のものを含む。）を侵害しないことを保証するとともに、侵害の恐れがある場合、又は甲からその恐れがある旨の通知を受けた場合には、当該知的財産権に関し、甲の要求する事項及びその他の必要な事項について遅滞なく調査を行い、これを速やかに甲に書面で報告しなければならない。
2　乙は、知的財産権に関して甲を当事者または関係者とする紛争が生じた場合（私的交渉、仲裁を含み、法的訴訟に限らない。）、その費用と責任において、その紛争を処理解決するものとし、甲に対し一切の負担及び損害を被らせないものとする。
3　第 9 条の規定は、知的財産権に関する紛争には適用しない。また、本条は、本契約終了後も有効に存続する。

（成果の公表等）
第 19 条　甲は、請負業務完了の日以後、請負業務の成果を公表、公開及び出版（以下「公表等」という。）することができる。
2　甲は、乙の承認を得て、請負業務完了前に、予定される成果の公表等をすることができる。
3　乙は、成果普及等のために甲が成果報告書等を作成する場合には、甲に協力する。
4　乙は、甲の書面による事前の承認を得た場合は、その承認の範囲内で請負業務の成果を公表等することができる。この場合、乙はその具体的方法、時期、権利関係等について事前に甲と協議してその了解を得

なければならない。なお、甲の要請がある場合は、甲と共同して行う。
5　乙は、前項に従って公表等しようとする場合には、著作権表示その他法が定める権利表示と共に「独立行政法人情報処理推進機構が実施する事業の成果」である旨を、容易に視認できる場所と態様で表示しなければならない。
6　本条の規定は、本契約終了後も有効に存続する。

（協議）
第 20 条　本契約の解釈又は本契約に定めのない事項について生じた疑義については、甲乙協議し、誠意をもって解決する。

（その他）
第 21 条　本契約に関する紛争については、東京地方裁判所を唯一の合意管轄裁判所とする。

特記事項

（談合等の不正行為による契約の解除）
第 1 条　甲は、次の各号のいずれかに該当したときは、契約を解除することができる。
一　本契約に関し、乙が私的独占の禁止及び公正取引の確保に関する法律（昭和 22 年法律第 54 号。以下「独占禁止法」という。）第 3 条又は第 8 条第 1 号の規定に違反する行為を行ったことにより、次のイからハまでのいずれかに該当することとなったとき
イ　独占禁止法第 61 条第 1 項に規定する排除措置命令が確定したとき
ロ　独占禁止法第 62 条第 1 項に規定する課徴金納付命令が確定したとき
ハ　独占禁止法第 7 条の 4 第 7 項又は第 7 条の 7 第 3 項の課徴金納付命令を命じない旨の通知があったとき
二　本契約に関し、乙の独占禁止法第 89 条第 1 項又は第 95 条第 1 項第 1 号に規定する刑が確定したとき
三　本契約に関し、乙（法人の場合にあっては、その役員又は使用人を含む。）の刑法（明治 40 年法律第 45 号）第 96 条の 6 又は第 198 条に規定する刑が確定したとき

（談合等の不正行為に係る通知文書の写しの提出）
第 2 条　乙は、前条第 1 号イからハまでのいずれかに該当することとなったときは、速やかに、次の各号の文書のいずれかの写しを甲に提出しなければならない。
一　独占禁止法第 61 条第 1 項の排除措置命令書
二　独占禁止法第 62 条第 1 項の課徴金納付命令書
三　独占禁止法第 7 条の 4 第 7 項又は第 7 条の 7 第 3 項の課徴金納付命令を命じない旨の通知文書

（談合等の不正行為による損害の賠償）
第 3 条　乙が、本契約に関し、第 1 条の各号のいずれかに該当したときは、甲が本契約を解除するか否かにかかわらず、かつ、甲が損害の発生及び損害額を立証することを要することなく、乙は、契約金額（本契約締結後、契約金額の変更があった場合には、変更後の契約金額）の 100 分の 10 に相当する金額（その金額に 100 円未満の端数があるときは、その端数を切り捨てた金額）を違約金として甲の指定する期間内に支払わなければならない。
2　前項の規定は、本契約による履行が完了した後も適用するものとする。
3　第 1 項に規定する場合において、乙が事業者団体であり、既に解散しているときは、甲は、乙の代表者であった者又は構成員であった者に違約金の支払を請求することができる。この場合において、乙の代表者であった者及び構成員であった者は、連帯して支払わなければならない。
4　第 1 項の規定は、甲に生じた実際の損害額が同項に規定する違約金の金額を超える場合において、甲がその超える分について乙に対し損害賠償金を請求することを妨げるものではない。
5　乙が、第 1 項の違約金及び前項の損害賠償金を甲が指定する期間内に支払わないときは、乙は、当該期間を経過した日から支払をする日までの日数に応じ、年 3 パーセントの割合で計算した金額の遅延利息

を甲に支払わなければならない。

（暴力団関与の属性要件に基づく契約解除）

第4条　甲は、乙が次の各号の一に該当すると認められるときは、何らの催告を要せず、本契約を解除することができる。

一　法人等（個人、法人又は団体をいう。）が、暴力団（暴力団員による不当な行為の防止等に関する法律（平成3年法律第77号）第2条第2号に規定する暴力団をいう。以下同じ。）であるとき又は法人等の役員等（個人である場合はその者、法人である場合は役員又は支店若しくは営業所（常時契約を締結する事務所をいう。）の代表者、団体である場合は代表者、理事等、その他経営に実質的に関与している者をいう。以下同じ。）が、暴力団員（同法第2条第6号に規定する暴力団員をいう。以下同じ。）であるとき

二　役員等が、自己、自社若しくは第三者の不正の利益を図る目的又は第三者に損害を加える目的をもって、暴力団又は暴力団員を利用するなどしているとき

三　役員等が、暴力団又は暴力団員に対して、資金等を供給し、又は便宜を供与するなど直接的あるいは積極的に暴力団の維持、運営に協力し、若しくは関与しているとき

四　役員等が、暴力団又は暴力団員であることを知りながらこれと社会的に非難されるべき関係を有しているとき

（再請負契約等に関する契約解除）

第5条　乙は、本契約に関する再請負先等（再請負先（下請が数次にわたるときは、すべての再請負先を含む。）並びに自己、再請負先が当該契約に関連して第三者と何らかの個別契約を締結する場合の当該第三者をいう。以下同じ。）が解除対象者（前条に規定する要件に該当する者をいう。以下同じ。）であることが判明したときは、直ちに当該再請負先等との契約を解除し、又は再請負先等に対し解除対象者との契約を解除させるようにしなければならない。

2　甲は、乙が再請負先等が解除対象者であることを知りながら契約し、若しくは再請負先等の契約を承認したとき、又は正当な理由がないのに前項の規定に反して当該再請負先等との契約を解除せず、若しくは再請負先等に対し契約を解除させるための措置を講じないときは、本契約を解除することができる。

（損害賠償）

第6条　甲は、第4条又は前条第2項の規定により本契約を解除した場合は、これにより乙に生じた損害について、何ら賠償ないし補償することは要しない。

2　乙は、甲が第4条又は前条第2項の規定により本契約を解除した場合において、甲に損害が生じたときは、その損害を賠償するものとする。

3　乙が、本契約に関し、第4条又は前条第2項の規定に該当したときは、甲が本契約を解除するか否かにかかわらず、かつ、甲が損害の発生及び損害額を立証することを要することなく、乙は、契約金額（本契約締結後、契約金額の変更があった場合には、変更後の契約金額）の100分の10に相当する金額（その金額に100円未満の端数があるときは、その端数を切り捨てた金額）を違約金として甲の指定する期間内に支払わなければならない。

4　前項の規定は、本契約による履行が完了した後も適用するものとする。

5　第2項に規定する場合において、乙が事業者団体であり、既に解散しているときは、甲は、乙の代表者であった者又は構成員であった者に違約金の支払を請求することができる。この場合において、乙の代表者であった者及び構成員であった者は、連帯して支払わなければならない。

6　第3項の規定は、甲に生じた実際の損害額が同項に規定する違約金の金額を超える場合において、甲がその超える分について乙に対し損害賠償金を請求することを妨げるものではない。

7　乙が、第3項の違約金及び前項の損害賠償金を甲が指定する期間内に支払わないときは、乙は、当該期間を経過した日から支払をする日までの日数に応じ、年3パーセントの割合で計算した金額の遅延利息を甲に支払わなければならない。

（不当介入に関する通報・報告）

第7条　乙は、本契約に関して、自ら又は再請負先等が、暴力団、暴力団員、暴力団関係者等の反社会的勢力から不当要求又は業務妨害等の不当介入（以下「不当介入」という。）を受けた場合は、これを拒否し、又は再請負先等をして、これを拒否させるとともに、速やかに不当介入の事実を甲に報告するとともに警察への通報及び捜査上必要な協力を行うものとする。

本契約の締結を証するため、本契約書 2 通を作成し、双方記名押印の上、甲、乙それぞれ 1 通を保有する。

2022 年〇月〇日

甲　東京都文京区本駒込二丁目 28 番 8 号
　　独立行政法人情報処理推進機構
　　理事長　富田　達夫

乙　〇〇県〇〇市〇〇町〇丁目〇番〇〇号
　　株式会社〇〇〇〇〇〇〇
　　代表取締役　〇〇　〇〇

（別添）

個人情報の取扱いに関する特則

（定義）

第１条　本特則において、「個人情報」とは、業務に関する情報のうち、個人に関する情報であって、当該情報に含まれる記述、個人別に付された番号、記号その他の符号又は画像もしくは音声により当該個人を識別することのできるもの（当該情報のみでは識別できないが、他の情報と容易に照合することができ、それにより当該個人を識別できるものを含む。）をいい、秘密であるか否かを問わない。以下各条において、「当該個人」を「情報主体」という。

（責任者の選任）

第２条　乙は、個人情報を取扱う場合において、個人情報の責任者を選任して甲に届け出る。

２　乙は、第１項により選任された責任者に変更がある場合は、直ちに甲に届け出る。

（個人情報の収集）

第３条　乙は、業務遂行のため自ら個人情報を収集するときは、「個人情報の保護に関する法律」その他の法令に従い、適切且つ公正な手段により収集するものとする。

（開示・提供の禁止）

第４条　乙は、個人情報の開示・提供の防止に必要な措置を講じるとともに、甲の事前の書面による承諾なしに、第三者（情報主体を含む）に開示又は提供してはならない。ただし、法令又は強制力ある官署の命令に従う場合を除く。

２　乙は、業務に従事する従業員以外の者に、個人情報を取り扱わせてはならない。

３　乙は、業務に従事する従業員のうち個人情報を取り扱う従業員に対し、その在職中及びその退職後においても個人情報を他人に開示・提供しない旨の誓約書を提出させるとともに、随時の研修・注意喚起等を実施してこれを厳正に遵守させるものとする。

（目的外使用の禁止）

第５条　乙は、個人情報を業務遂行以外のいかなる目的にも使用してはならない。

（複写等の制限）

第６条　乙は、甲の事前の書面による承諾を得ることなしに、個人情報を複写又は複製してはならない。ただし、業務遂行上必要最小限の範囲で行う複写又は複製については、この限りではない。

（個人情報の管理）

第７条　乙は、個人情報を取り扱うにあたり、本特則第４条所定の防止措置に加えて、個人情報に対する不正アクセスまたは個人情報の紛失、破壊、改ざん、漏えい等のリスクに対し、合理的な安全対策を講じなければならない。

２　乙は、前項に従って講じた措置を、遅滞なく甲に書面で報告するものとする。これを変更した場合も同様とする。

３　甲は、乙に事前に通知の上乙の事業所に立入り、乙における個人情報の管理状況を調査することができる。

４　前三項に関して甲が別途に管理方法を指示するときは、乙は、これに従わなければならない。

５　乙は、業務に関して保管する個人情報（甲から預託を受け、或いは乙自ら収集したものを含む）について甲から開示・提供を求められ、訂正・追加・削除を求められ、或いは業務への利用の停止を求められた場合、直ちに且つ無償で、これに従わなければならない。

（返還等）

第８条　乙は、甲から要請があったとき、又は業務が終了（本契約解除の場合を含む）したときは、個人情報が含まれるすべての物件（これを複写、複製したものを含む。）を直ちに甲に返還し、又は引き渡すとともに、乙のコンピュータ等に登録された個人情報のデータを消去して復元不可能な状態とし、その旨を甲に報告しなければならない。ただし、甲から別途に指示があるときは、これに従うものとする。

２　乙は、甲の指示により個人情報が含まれる物件を廃棄するときは、個人情報が判別できないよう必要な

処置を施した上で廃棄しなければならない。

（記録）

第 9 条　乙は、個人情報の受領、管理、使用、訂正、追加、削除、開示、提供、複製、返還、消去及び廃棄についての記録を作成し、甲から要求があった場合は、当該記録を提出し、必要な報告を行うものとする。

2　乙は、前項の記録を業務の終了後 5 年間保存しなければならない。

（再請負）

第 10 条　乙が甲の承諾を得て業務を第三者に再請負する場合は、十分な個人情報の保護水準を満たす再請負先を選定するとともに、当該再請負先との間で個人情報保護の観点から見て本特則と同等以上の内容の契約を締結しなければならない。この場合、乙は、甲から要求を受けたときは、当該契約書面の写しを甲に提出しなければならない。

2　前項の場合といえども、再請負先の行為を乙の行為とみなし、乙は、本特則に基づき乙が負担する義務を免れない。

（事故）

第 11 条　乙において個人情報に対する不正アクセスまたは個人情報の紛失、破壊、改ざん、漏えい等の事故が発生したときは、当該事故の発生原因の如何にかかわらず、乙は、ただちにその旨を甲に報告し、甲の指示に従って、当該事故の拡大防止や収拾・解決のために直ちに応急措置を講じるものとする。なお、当該措置を講じた後ただちに当該事故及び応急措置の報告並びに事故再発防止策を書面により甲に提示しなければならない。

2　前項の事故が乙の本特則の違反に起因する場合において、甲が情報主体又は甲の顧客等から損害賠償請求その他の請求を受けたときは、甲は、乙に対し、その解決のために要した費用（弁護士費用を含むがこれに限定されない）を求償することができる。なお、当該求償権の行使は、甲の乙に対する損害賠償請求権の行使を妨げるものではない。

3　第 1 項の事故が乙の本特則の違反に起因する場合は、本契約が解除される場合を除き、乙は、前二項のほか、当該事故の善後策として必要な措置について、甲の別途の指示に従うものとする。

以上

Ⅲ．仕様書

「2022 年度ペネトレーションテストによる独立行政法人等の情報システムに対するセキュリティ対策状況調査（その 1)」

事業内容（仕様書）

独立行政法人**情報処理推進機構**

事業内容（仕様書）

1. 件名

「2022 年度ペネトレーションテストによる独立行政法人等の情報システムに対するセキュリティ対策状況調査（その 1)」

2. 背景・目的

サイバーセキュリティに対する脅威は、年々複雑化・巧妙化しており、サイバー攻撃による被害は、行政機関や民間企業といったあらゆる組織において確認されている。また、行政機関と密接に連携して業務を遂行している独立行政法人及び指定法人[2]（以下「独立行政法人等」という。）も、同様のサイバー攻撃の脅威に晒されている。

このような状況を受け、我が国においてはサイバーセキュリティ基本法の下、サイバーセキュリティの確保に向けた取り組みが推進されている。本業務では、その一環として、独立行政法人情報処理推進機構（以下「IPA」という。）が独立行政法人等の情報システム（以下「調査対象システム」という。）に対して、情報システム内部への侵入可否及び侵入後の被害状況について、攻撃者が実際に行う最新の攻撃手法を用いて客観的に検証するペネトレーションテストを実施する。その検証結果に基づき、セキュリティ対策上の問題点について評価及び助言等を行い、独立行政法人等全体の情報セキュリティ水準を向上させることを本業務の目的とする。

3. 業務内容

3.1. 業務概要

本業務は、調査対象システムに対してペネトレーションテストを実施し、セキュリティ対策上の問題点について評価及び助言等を行う。具体的な業務内容は 3.2 に記載する。また、本仕様書で使用する「ペネトレーションテスト」に係る定義及び条件等について、以下に記載する。

なお、本仕様書中で「ペネトレーションテスト」を「テスト」又は「調査」と表記する場合がある。

(1) ペネトレーションテストに係る定義及び条件等

IPA が想定しているペネトレーションに係る定義等は以下のとおりであり、テスト実施観点の作成及びペネトレーションテストの実施にあたっては、これらを参考とした上で実施すること。

① ペネトレーションの定義

ア 管理者権限を持つアカウントによる OS・ミドルウェア等へのログイン

イ 一般ユーザ権限を持つアカウントによる OS・ミドルウェア等へのログイン

ウ 認証を回避しての OS に対するコマンドの実行

エ ア～ウ以外での対象ホスト内の情報の窃取

② 本業務におけるペネトレ―ションテストの内容

いわゆる脆弱性診断は、システムが悪用された場合に侵害可能性のある脆弱性を検出・優先付けして報告するものであるが、本業務におけるペネトレーションテストは、攻撃者の視点に立ち、検出された複数の脆弱性や設定不備などを単独又は組み合わせにより疑似攻撃を行い、前段階の疑似攻撃で得られた情報をさらに次の疑似攻撃に利用したりすることで、システムのセキュリティを実際に迂回・突破した結果を報告することを意味する。

本業務におけるペネトレーションテストは、システム情報及び脆弱性情報等の収集、対象ホストへの侵入可否の調査及び分析、侵入可能な攻撃の実行、侵入後の攻撃活動（情報収集や攻撃の結果により判明した対象機器の脆弱性等を利用し、他の更に重要なホストへの侵入を試行すること等）を網羅するものとする。なお、ソーシャルエンジニアリングやテスト対象への物理的な攻撃は、原則として実施しない。

一般的なペネトレーションテストのための方法論や疑似攻撃の手法には、NIST SP800-115 や Penetration Testing Execution Standard (PTES) などに示されたものがあるが、請負者は、近年のサイバー攻撃の動向や最新の攻撃手法を勘案し、攻撃者の視点に立ったより実践的なテストとなるよう攻撃手法や使用するツールを採用し、本業務を遂行すること。

[2] 特殊法人及び認可法人のうち、サイバーセキュリティ戦略本部が指定するものをいう。

③ ペネトレーションテストの終了条件

テスト対象とする各種サーバ、端末、通信回線装置（以下「ホスト」という。）に対し、上記①に示す侵入を達成できる可能性のある攻撃手法をすべて実施すること。ただし、多数の攻撃手法が存在するなど、実施期間内にすべての攻撃手法を実施することが困難であると想定される場合には、独立行政法人等及び IPA と協議の上、実施する攻撃手法数を調整してもよい。

なお、調整により実施しない攻撃手法のうち、脆弱性が確認されたものについては、個別調査結果報告書に脆弱性に関する情報を記載すること。

④ 調査期間

1 システムあたりの調査期間は 2 日～5 日程度（原則として移動時間を含む。）で実施すること。なお、調査期間は、テスト対象システムに対して侵入を試みる作業を行う期間であり、ペネトレーションテストの実施結果に関する分析及び評価を行う期間は含まない。

また､3.2(3)②オに記載するテスト実施観点作成のための事前ポートスキャン等を実施するための現地での作業期間は、当該調査期間の範囲に含めないものとする。

さらに、テスト当日にテスト対象システムとの通信の疎通が取れないなどの不測の事態が発生した場合も、調査対象組織と協議の上、予定していたテストが実施できるよう、必要に応じてスケジュールを調整すること。

⑤ ペネトレーションテストの攻撃手法

調査において使用する攻撃手法は、稼動中のサービスに支障を与える可能性がある場合、その影響について独立行政法人等に事前に説明すること。また、独立行政法人等から承認が得られた場合には、調査を実施すること。

3.2. 業務内容

(1) 調査対象

① 独立行政法人等が運用する IP 通信が可能な情報システムのうち、1 法人あたり 1 システム（15～30IP 程度)、合計 14 法人 14 システム程度を対象とし、IP アドレス数は全体で 285IP 以内とする。ただし、調査対象となる情報システム等の詳細については、契約締結後に別途 IPA より指示する。

② ①の 285IP に含む IP アドレスとは、テスト対象とする情報システムの各ホストに付与され、テストを実施する対象として選定したものとする。
なお、IPv6 アドレスも対象となる場合があることに留意すること。

③ 調査実施場所は原則首都圏とするが､調査対象システムが地方に設置されている場合はこの限りではない（首都圏以外に 2 地域程度を想定)。

④ 調査対象ホストの選定では、調査対象システム担当者及び IPA と協議の上、資料の確認、選定支援及び調整等を行うこと。

(2) 全体実施計画書の作成

請負者は、次の事項を含む全体実施計画書を IPA と協議の上で作成すること。

① 記載内容

ア 全体スケジュール
イ 事前説明会及びヒアリング内容
ウ ペネトレーションテスト方法（使用する機材やツール等の内容を含む。）
エ ペネトレーションテストの実施完了条件
オ ペネトレーションテストの実施結果に関する分析、評価方法及び評価観点
カ 本業務に係る管理者（プロジェクト責任者とペネトレーションテスト責任者）及び作業従事者に関する役割及び氏名を含む体制図
キ 業務体制、管理者及び作業従事者の所属、氏名及び経歴の一覧表
業務体制として、本業務に係る管理者（プロジェクト責任者（1 名）とペネトレーションテスト責任者（1 名以上））及び作業従事者（3 名以上）を必ず配置すること。なお、プロジェクト責任者とペネトレーションテスト責任者は兼務できないものとする。

② 期限

IPA と協議するための全体実施計画書案は契約締結日からおおむね 1 週間以内に提出すること。

(3) ペネトレーションテストの実施等

① 事前説明会及びヒアリングの実施

ア 請負者は、IPA と協議の上、法人ごとに事前説明会及びヒアリングの時期について調整すること。

イ 事前説明会は原則として法人ごとに 1 回開催することとし、調査対象システム担当者又は IPA の指定する場所で実施すること。

ウ 事前説明会では、調査日程、調査内容、依頼事項、調査実施における注意点等について説明すること。ヒアリングシートは 、以下の事項を含み、事前説明会及びヒアリングに先立って記入を依頼しておくこと。

(ア)テスト対象システムの概要
(イ)システム利用形態
(ウ)インターネット接続状況
(エ)インターネット以外のテスト対象組織外ネットワークの接続状況
(オ)OS 及びサーバ用途
(カ)事前ポートスキャン等やペネトレーションテストの実施時における連絡先及び連絡方法
(キ)Web アプリケーションを監視対象とする侵入防御装置やウェブアプリケーションファイアウォールの有無（※）

（※）テストの実施にあたり、侵入検知（または、防御）装置やウェブアプリケーションファイアウォールが有の場合は、当該機器等の状態を防御、検知のどちらの状態でテストを実施するのか検討が必要となる旨を、ヒアリングシートに記載すること。

エ 請負者は、回答されたヒアリングシートに基づき、調査対象システムに係るヒアリングを行うこと。

オ ヒアリングにおける調査対象ホストの選定では、請負者のこれまでの経験や知見を活用し効果的なペネトレーションテストが実施できるよう、必要な資料の閲覧（例えば、ネットワーク構成図等）や確認、助言等を行うこと。

カ 請負者は、調査対象システム側で必要となる事前準備・確認事項（例えば、データのバックアップの取得や、通信監視を委託している業者を始めとする関係先への連絡、調査実施時においてサービス障害等が発生した場合の技術的な対応、必要に応じた復旧支援態勢等）について、調査対象システム担当者及び IPA へ説明すること。

キ 事前説明会及びヒアリング終了後、3 営業日を目処に議事録を作成し IPA に提出すること。

② 個別実施計画書の作成

ア 請負者は、調査対象システムごとに、以下の事項を含めた個別実施計画書を作成すること。

（ア） ペネトレーションテストの概要
（イ） ペネトレーションテストの実施方法（攻撃方法、使用するツール等の内容を含む。詳細は次項イを参照）
（ウ） テスト実施観点（次項ウを参照）
（エ） ペネトレーションテスト期間中の作業スケジュール
（オ） 業務体制、管理者及び調査対象システムのテストに従事する作業従事者の役割、所属、氏名の一覧表
(カ)事前説明会及びヒアリング等で決定した事項のうち、テスト実施に当たり共有すべき事項

イ ペネトレーションテストの実施における手続きの流れに沿って、テストの実施内容の観点をとりまとめた実施観点を作成し、個別実施計画書に含めること。IPA において想定するテスト実施観点を表 1 に示す。

表 1 テスト実施観点（想定）

項目	
1	システム情報、脆弱性情報等の収集 ・ネットワーク情報の収集 ・システム情報の収集 ・脆弱性情報の収集 ・ユーザ情報の収集
2	対象ホストへの侵入可否の調査・分析 ・OS、ミドルウェアその他システム上に内在する脆弱性の調査

	・認証サービスの稼働状況の調査 ・ユーザ情報の調査 ・プロダクト固有のデフォルトユーザ情報の調査
3	侵入可能な攻撃の実行 ・ユーザ ID、パスワードを使用したログイン試行 ・OS、ミドルウェア、その他のシステム上の脆弱性を利用したコマンドの実行 ・OS、ミドルウェア、その他のシステム上の脆弱性を利用した情報の窃取
4	侵入後の活動 ・一般ユーザから管理者への権限昇格の実行 ・システム内部の情報収集 ・侵入に成功したホストと同様の手法で他ホストへの侵入 ・侵入に成功したホストを踏み台にした他ホストへの侵入

ウ　想定する侵入経路を簡易なネットワーク図等を用いて作成すること。テスト実施観点には、以下の２つを含めること。

(ア)外部起点（リモート）

インターネットからの攻撃を想定し、公開サーバ及び Web アプリケーション等に対する侵入を模擬

(イ)内部起点（オンサイト）

標的型攻撃等により職員用端末等が感染したことを想定し、内部ネットワークを起点としたサーバ、ネットワーク機器類（公開セグメントを含む）及び Web アプリケーションに対する侵入を模擬

また、個別実施計画書の内容は、事前ポートスキャン等の結果を踏まえ、必要に応じて追記又は修正すること。

エ　個別実施計画書については、調査対象システム担当者と協議の上で作成し、調査実施までに IPA 及び調査対象システム担当者の承認を得ること。ただし、承認が得られなかった場合は、個別実施計画書の問題点について意見聴取した上で再設計し再協議すること。

オ　テスト実施観点を作成する上で、事前に調査対象ホストへのポートスキャン等が必要な場合は、対象ホスト、実施方法、実施希望日について調査対象システム担当者と協議の上、事前に調査対象システム担当者の承認を得ること。

なお、当該作業を調査対象システムの拠点で行い、端末の持込み、接続及びログ情報の持ち出しに当たって、申請書の提出等が必要な場合、調査対象システム担当者の指示に従うこと。

カ　調査において脆弱性等を利用して攻撃するためのプログラム(以下「調査用プログラム」という。)を利用する場合は、当該プログラムを利用することによって判明する問題点の詳細及び利用した際に想定されるリスクについて、IPA 及びテスト対象組織に説明し、それぞれの承認を得ること。

キ　テストにおいて使用する攻撃手法が、稼動中のサービスに支障を与える可能性がある場合、その影響について IPA 及びテスト対象組織に説明し、それぞれの承認が得られた場合にテストを実施すること。

ク　調査対象法人又は調査対象法人が利用する共通基盤等からテスト手法等について情報提供を求められた場合、IPA 又は調査対象システム担当者の指示に従うこと。

③　ペネトレーションテストの実施

請負者は、承認が得られた個別実施計画書及び以下の事項に基づきペネトレーションテストを実施すること。

ア　調査は原則として、月曜日から金曜日（祝祭日を除く。）の午前 10 時から午後 5 時までの時間帯で実施すること。ただし、全体で 10 日間程度は休日又は平日の夜間に調査することを想定している。その際は、調査対象システム担当者と調整の上、体制を整備すること。

イ　内部起点での調査は現地で実施することを基本とする。なお、内部起点の調査を遠隔で実施する場合、個別実施計画書を作成する段階で、その手法、実績について IPA 及び対象組織に提示し承認を得ること。また、現地での作業は新型コロナウイルス感染症対策を行った上で実施すること。

ウ　調査期間の各日の作業開始時及び作業終了時には、調査対象システム担当者及び IPA に連絡すること。また、各日の作業終了後、作業進捗報告書（実施した作業内容及び調査対象ホストがわかるもの）を作成し、調査対象システム担当者及び IPA に提出すること。また、計画より早く調査

を終了する場合は、その理由を IPA に報告し、承認を得ること。

エ　調査において、検出した問題を利用して侵入できた場合、調査対象システム担当者及び IPA に対して、その旨を速やかに連絡すること。その後、調査対象システム担当者から情報提供依頼や状況の再現を求められた場合は協力すること。なお、当該問題点がテスト対象組織に重大な影響を及ぼす可能性があると請負者が判断した場合、IPA にも報告すること。

オ　作業中は、調査対象システムを含む独立行政法人等が運用しているシステムのサービスを停止させたり、又は阻害したりしていないか常に状況を確認すること。

カ　調査対象システムを含む独立行政法人等が運用しているシステムのサービスを停止させ、又は阻害した場合は、直ちに作業を中止し、調査対象システム担当者及び IPA へ連絡すること。具体的な報告基準は以下の通りとする。

・ 調査を実施した結果、調査対象システムの全部又は一部の機能やサービスについて、利用者視点での何らかの影響が発生したことを認識した場合（サービス停止、無応答、性能劣化等）

・ 上記に示した事象が軽微なものであっても、当該事象を調査対象システム担当者が認識するに至った場合

また、サービス復旧の際に協力を求められた場合には、調査対象システム担当者及び IPA の指示に従うこと。

なお、中止した調査の再開については、調査対象システム担当者と再開に伴う影響も含め、十分に調整し、サービスへの影響が生じない対策を講じること。

キ　調査対象システム担当者からの指示及び問い合わせに速やかに対応できる体制を整備すること。

ク　現地での調査において、端末の持込み・接続及びログ情報の持ち出しに当たって、調査対象の法人に対して申請書等の提出が必要な場合、調査対象システム担当者及び IPA の指示に従うこと。

ケ　蔵置した調査用プログラム、起動したプロセス及び作成したダンプファイルその他のペネトレーションテスト中に調査対象システムに加えた影響は、これを残留させないよう適切に処理（以下「残留物の除去処理」という。）すること。なお、請負者のみで残留物の除去処理が出来ない場合にあっては、ペネトレーションテスト実施期間終了後直ちに IPA 及び調査対象システム担当者に報告した上で、調査対象組織に残留物の除去処理を依頼すること。また、必要に応じて除去処理に係る対応を現地にて実施すること。

(4) ペネトレーションテストの実施結果に関する分析及び評価

① 調査対象システムごとの個別調査結果報告書の作成

ア　記載内容

A) 請負者は、調査結果から調査対象システムのセキュリティ対策の実施状況の分析・評価を行い、その結果について以下の項目を含めた個別調査結果報告書を作成すること。併せて、IP アドレス等の機密情報をマスクしたバージョンも作成すること。

(ア)調査の内容

・調査で用いた調査実施手順・方法とテスト実施観点

・調査対象システムについて調査を実施した範囲

(イ)調査の実施結果

・検出した問題の内容及び危険度の一覧

※一覧については、IPA と調整の上、別表も作成すること

・検出した問題を再現する方法

・検出した問題に対して推奨する具体的な対策方法

なお、根本的な対策方法が、期間及びコスト等の面から早期の実施が現実的に困難と想定される場合は、暫定的な対策についても併せて示すこと。

(ウ)調査結果全体の評価

・全体的な調査結果のまとめ及び総論

(エ)問い合わせ窓口

・質問対応連絡先（メールアドレス、電話番号）

B) 個別調査結果報告書の内容は、図表やイメージ等を用いるなど、調査対象システム担当者が理解し、調査の再現が可能となるよう読み易さについて工夫すること。また、調査対象システム担当者がセキュリティ対策水準の向上に努められるよう、必要に応じて請負者の知見、助言等を適宜追加すること。

C) 侵入できた問題点については、問題点の重要性の認識が容易となるよう危険度のレベルを用いて

説明すること。また、侵入できた問題点については侵入が成功するまでの攻撃の流れが把握できるように、利用した脆弱性や設定の不備も含めて記載すること。

D) 調査対象システムの評価の認識が容易となるよう、検出した問題点のほか、侵入の過程において検出した脆弱性情報等を総合的に評価し、レベルを用いて説明すること。

イ　期限

請負者は、調査対象システムに対するペネトレーションテスト終了後、概ね 3 週間以内に個別調査結果報告書案を IPA に提出すること。

② 調査対象システムごとの個別調査結果の説明

請負者は、必要に応じて、調査対象システム担当者及び IPA と調整の上、個別調査結果報告書について説明すること。また、質疑応答を含む議事録を作成し、終了後 1 週間以内を目処に IPA に提出すること。

③ 全体調査結果報告書の作成

ア　実施内容

請負者は、次の事項を含む全体調査結果報告書を IPA と協議の上作成すること。

(ア)上記(4)①において作成した個別調査結果報告書を取りまとめたもの

(イ)ペネトレーションテスト結果の全体を俯瞰し、国内外のサイバー攻撃の動向等を考慮したうえで、独立行政法人等全体の情報セキュリティ水準を向上させるための IPA に対する助言

(ウ)今後のペネトレーションテストを実施するに当たっての助言

(エ)総評

イ　期限

別途指定する期日までに全体調査結果報告書案を IPA に提出すること。

(5) 付随作業

① 進捗管理及び課題管理

請負者は、作業の実施に当たり、IPA と密に連絡を取るとともに、進捗管理表を作成して臨むこと。また、1 ヵ月に 1 回は情報を集約し、作業の進捗状況について報告を行うこと。

なお、本業務の実施に当たり疑義や問題が生じた際には、速やかに IPA と協議して決定・解決すること。

② 問い合わせ等への対応

請負者は、本業務に係る IPA からの問い合わせ等があった場合には速やかに対応すること。

また、調査対象システム担当者からの問い合わせ等についても同様とし、必要に応じて IPA と協議の上、対応すること。

③ 打合せにおける記録の作成

請負者は、調査対象システム担当者との打合せ終了後、3 営業日を目処に議事録を作成し、調査対象システム担当者及び IPA に提出すること。議事録には、決定事項、宿題事項、共有あるいは記録すべき議論内容を記載すること。

4. 業務期間及びスケジュール

4.1 業務期間

契約締結日から 2023 年 2 月 28 日

4.2 スケジュール

本業務では、表2の作業スケジュールを想定している。具体的なスケジュールについては、本仕様書の業務内容を踏まえ、IPAと協議の上、決定すること。

表2 作業スケジュール

時期	主な作業内容
2022年5月	・キックオフ ・全体実施計画書の作成 ・体制、役割分担及びスケジュール等の確認 ・事前説明会及びヒアリングの日程調整 ・ペネトレーションテストの実施時期調整
2022年5月～2023年1月	・事前説明会及びヒアリングの実施 ・調査対象システムの情報収集・攻撃手法等の検討 ・個別実施計画書の作成 ・ペネトレーションテストの実施 ・個別調査結果報告書の作成及び提出 ・調査結果の質疑対応
2023年2月	・全体調査結果報告書の作成及び報告

5. 実施体制

本業務を実施するための請負者の体制について、請負者の資本関係・役員等の情報、当該作業の実施場所、全ての業務従事者の所属、雇用形態、実績（経験年数、資格等）及び国籍についての情報を明らかにすること。

(1) 請負者の資格等

① 「情報セキュリティサービス基準適合サービスリスト[3]」の脆弱性診断サービス分野に掲載されている者であること（手続き中を含む）。

② 過去 3 年間において、情報システムにおけるペネトレーションテスト、プラットフォーム診断、ウェブアプリケーション診断のセキュリティ診断の実績を毎年 3 件以上有することとし、うち年間 1 件以上はペネトレーションテストの実績を含むこと。

(2) 業務従事者の経歴

業務従事者の経歴（氏名、所属、役職、学歴、職歴、業務経験、研修実績その他の経歴、専門的知識その他の知見、母語及び外国語能力、国籍等がわかる資料）を提出すること。

※経歴提出のない業務従事者の人件費は計上不可。

(3) 業務従事者の役割

業務従事者として、プロジェクト責任者、ペネトレーションテスト責任者及び作業従事者を配置すること。なお、作業従事者については、必ず３名以上配置すること。プロジェクト責任者、ペネトレーションテスト責任者及び作業従事者の役割については以下のとおり。

① プロジェクト責任者（1 名）

本業務の全体を統括・管理し、本業務におけるに係る全ての進捗管理、成果物の品質管理、ステークホルダー・マネジメント、要員管理及びコミュニケーション管理等、本業務を成功させるために必要な管理事項について、適切に監視・監督を行う。

② ペネトレーションテスト責任者（1 名以上）

本業務において実施する調査全体を統括・管理し、ペネトレーションテストの実施、事前説明会やヒアリング、個別報告会の実施にあたって必要となる進捗管理、成果物（個別実施計画書、個別結果一覧、個別調査結果報告書等）の品質管理等テストを問題なく完了させるために必要な事項について、適切に管理・監督を行う。

③ 作業従事者（3 名以上）

本業務において実際にテスト等を実施するほか、プロジェクト責任者及びペネトレーションテス

[3] 経済産業省が策定した「情報セキュリティサービス基準」への適合性を審査登録機関により審査し、認められた、事業者の情報セキュリティサービスのリストで、IPA により公開している。

ト責任者の管理・監督の下、本業務遂行のために必要な作業を行う。

(4) 業務従事者の資格等

業務従事者の資格等の要件については、次のとおりとする。ただし、①プロジェクト責任者と②ペネトレーションテスト責任者は兼務できないものとする。

① プロジェクト責任者（1 名）

過去 3 年間において、情報システムに係るプロジェクトマネジメント業務の責任者としての経験を有すること。

② ペネトレーションテスト責任者（1 名以上）

ア 情報セキュリティに係る業務の経験年数を 5 年以上有し、かつペネトレーションテストの責任者としての経験を有すること。

イ 情報処理技術者試験、他の民間団体が認定するセキュリティ資格のうち、以下のいずれかの資格を有しているか、又は資格を有することと同等以上の技術を保持していることが証明できること。

- 情報処理安全確保支援士
- CISSP

③ 作業従事者（3 名以上）

ア 作業従事者のうち少なくとも 3 名は、3 年以上のペネトレーションテストの経験を有すること。

イ 作業従事者のうち、少なくとも 1 名以上は、以下のいずれかの資格を有しているか、又は資格を有することと同等以上の技術を保持していることが証明できること。

- 情報処理安全確保支援士
- CISSP

ウ 以下の資格条件、実績を満たす者が含まれていることが望ましい。

- CEH（Certified Ethical Hacker）
- GIAC（Global Information Assurance Certification）
- OSCP（Offensive Security Certification Professional）
- 作業従事者の実績として報告した共通脆弱性識別子 CVE(Common Vulnerabilities and Exposures)番号や、情報セキュリティに関するカンファレンスでの講演や CTF(Capture The Flag)等のコンテストで上位入賞実績

(5) 業務従事者の知識

業務従事者は、以下の内容を把握していること。

① 内閣官房内閣サイバーセキュリティセンター：「政府機関等の情報セキュリティ対策のための統一基準」

② IPA：「安全なウェブサイトの作り方」、「安全な SQL の呼び出し方」、「セキュア・プログラミング講座 Web アプリケーション編」、「セキュア・プログラミング講座 C/C++言語編」、「「高度標的型攻撃」対策に向けたシステム設計ガイド」

③ 不正アクセス行為の禁止等に関する法律

④ MITRE ATT&CK で示されている戦術や技術に関する考え方

⑤ OWASP TOP 10 で示されている Web アプリケーションにおける脆弱性とその攻撃手法

(6) 体制

① 請負者は、本業務を円滑に遂行するための体制を整備すること。円滑に遂行するための体制には最低限、以下の項目を含めること。

ア 遅滞なく本業務を遂行するための調査対象システム担当者との調整体制

イ 当該業務の実施において情報セキュリティを確保するための体制（情報セキュリティ管理体制、事故発生時の対処体制及び対処方法、実施場所のセキュリティ確保方法）

ウ 本業務にかかる作業工程及びその進捗状況を管理する体制

エ 調査対象システムに関し、個人・組織の不正等により意図せざるシステムや情報の変更、調査対象に関する情報の漏えいが行われないための十分な管理体制

② 請負者は、情報管理体制について以下とすること。

ア 請負者は本事業で知り得た情報を適切に管理するため、次の履行体制を確保し、発注者に対し「情報セキュリティを確保するための体制を定めた書面（情報管理体制図」」及び「情報取扱者名簿」（氏名、個人住所、生年月日、所属部署、役職、パスポート番号及び国籍等が記載された

もの）を契約前に提出し、担当部門の同意を得ること。（個人住所、生年月日については、必ずしも契約前に提出することを要しないが、その場合であっても担当部門から求められた場合は速やかに提出すること。）なお、情報取扱者名簿は、委託業務の遂行のため最低限必要な範囲で情報取扱者を掲載すること。

（確保すべき履行体制）

契約を履行する一環として契約相手方が収集、整理、作成等した一切の情報が、IPA が保護を要さないと確認するまでは、情報取扱者名簿に記載のある者以外に伝達又は漏えいされないことを保証する履行体制を有していること。

イ　本事業で知り得た一切の情報について、情報取扱者以外の者に開示又は漏えいしてはならないものとする。「情報取扱者名簿」以外の者に情報を提供等することは重大な契約違反となるため注意すること。

ウ　本事業において知り得た全ての情報について、受注者が自ら利用、又は第三者に開示する際は IPA の承認を得ること及び受注者が第三者と包括的に情報提供を行う契約を締結している等の場合があることにも留意すること。

エ　アの情報セキュリティを確保するための体制を定めた書面又は情報取扱者名簿に変更がある場合は、予め担当部門へ届出を行い、同意を得なければならない。

オ　　有している場合には情報管理に関する社内規則を提出すること。有しない場合は代わりとなるものでもよい。

③　請負者は、契約締結後、全作業従事者の機密保持に関する誓約書をとりまとめ、体制図を含めた「担当者名簿」と併せて、速やかに IPA へ提出すること。

④　本業務を遂行する上で不適当と認められる管理者及び作業従事者について、IPA は請負者に対し、交代を求めることができるものとする。ただし、交代の際は交代前と同等以上の技能等を有すると IPA が認めた者に限る。

⑤　本業務の契約期間中に請負者の事情により管理者又は作業従事者を変更する場合は相応の期間をもって事前に IPA へ通知し、許可を得ること。

⑥　請負者の作業実施場所は日本国内の拠点のみとし、作業エリアは本業務の業務従事者以外の者が立ち入ることができないように措置を講ずること。また、作業に用いる機材等について作業実施中以外においては、業務従事者以外が取り扱うことができないように措置を講ずること。

6. 情報セキュリティに関する要件

⑴ 取り扱う情報に対する措置及び本業務範囲外の利用の禁止

本業務の実施のために IPA から提供する情報その他当該業務の実施において知り得た情報については、その秘密を保持し、漏えい・紛失・盗難等が起こらぬように必要な措置を講じ、当該業務の目的以外に利用しないこと。

作業場所においての作業の実施方法及び受領した文書等の作業中における取り扱い方法や、本業務で利用する端末、メールシステムやストレージなどの情報システムのセキュリティ対策の技術的要件等は、別添に掲げる要件（本業務の性質等に照らして、セキュリティ上同等以上と認められる要件である場合を含む。）を満たすこと 。本業務の一部を再委託する場合、請負者は再委託先が同等の情報セキュリティ対策を実施していることを担保し、当機構の求めがあれば再委託先の情報セキュリティ対策の実施状況を確認・報告すること。

⑵ 本業務範囲外の操作の禁止

請負者は、本業務に必要な範囲を超えて、情報システム内の情報の閲覧・取得や調査対象外の情報システムへの侵入等を行わないこと。

⑶ 作業履歴等の記録

本業務における情報システムの操作ログや作業履歴等を記録すること。

なお、記録すべき具体的なログ・情報等については調査対象システムごとに IPA と協議し、IPA が要求した場合は提出すること。

⑷ 情報の保管

ペネトレーションテスト実施中に得られた情報、操作ログ等の一切のデータ等については、日本国内のみで取扱うこととし、クラウドサービス等のインターネット上のサービスにて取扱わず、必ず請負者

の責任において専用の端末内又は外部電磁的記録媒体に暗号化するなどして厳重に保管すること。

(5) 情報セキュリティ対策実施の報告

本業務の遂行において、1ヵ月に1回情報セキュリティ対策の履行状況をIPAへ報告するとともに、情報セキュリティインシデントの発生、情報の目的外利用、情報セキュリティ対策の履行が不十分であること等を認知した場合は、直ちにIPAへ報告すること。また、被害の程度を把握するため、請負者は必要な記録類を契約終了時まで保存し、IPAの求めに応じて納入物件と共にIPAへ提出すること。

(6) 情報の廃棄

請負者は、本業務の契約終了後1カ月以内にIPAが指示するタイミングで、本業務の納入物件を除き、全ての情報は、請負者において責任のある者の管理の下で廃棄すること。また、廃棄した情報及びその方法をIPAへ報告し、確認を受けること。

なお、ここでいう「廃棄」とは、全ての者による情報入手、復元及び内容の判読ができない状況にすることを意味する。納入物件の保管は契約不適合期間の終了時までとし、書面及びCD-R等媒体についても、契約不適合期間終了後、前述と同様に廃棄を行うこと。

(7) 監査の受け入れ

本業務の遂行における情報セキュリティ対策の履行状況を確認するために、IPAが情報セキュリティ監査の実施を必要と判断した場合は、情報セキュリティ監査を受け入れること。

なお、その実施については、請負者とIPAで事前に協議を行うものとする。

7. その他

(1) 作業はIPAの指示に基づき行うものとし、必要に応じて適宜ミーティング等により作業内容の調整を行うものとする。
(2) 提出書類の作成に当たっては、Microsoft Officeを使用して作成することとし、これ以外の形式を使用する場合は、事前にIPAに相談すること。
(3) 使用言語は日本語とし、独立行政法人等の職員が読解可能な平易な文章で記載すること。ただし、専門用語や固有名詞等に外国語表記を用いることは可能とする。
(4) リモートで打合せを行う場合、第三者に会議内容が漏洩しないよう十分な対策を施したWeb会議システム及びそれらを使用するための機材を準備すること。

8. 納入関連

8.1 納入期限・納入場所

2023年2月28日
〒113-6591
東京都文京区本駒込2丁目28番8号　文京グリーンコートセンターオフィス15階
独立行政法人情報処理推進機構 セキュリティセンター 公共セキュリティ部 セキュリティ監査グループ

8.2 納入物件

以下の資料の電子データを収めた記録媒体（CD-R又はDVD-R）　一式
(1) 全体実施計画書
(2) 個別実施計画書
(3) 個別調査結果報告書
(4) 全体調査結果報告書

＜注＞

・本業務の実施過程で作成した文書等も併せて提出すること。当該文書等には、作業進捗報告書、進捗管理表、会議資料、議事録等を含む。

9. 検収条件

納入物件の内容に関しては、本仕様書に示された条件、項目を満たしているかについて確認を行う。また、品質については「2.背景・目的」で示された目的を満たすに十分か否かを基準に判断する。

（別添）

情報セキュリティ対策に関する技術的要件等

本業務に係る要機密情報（以下、「業務情報」という。）を取り扱うために請負者が利用する情報システム（端末、ストレージ、メールシステム、Web 会議システム等）等は、以下のセキュリティ対策に係る技術的要件等を満足すること（※本要件の各項目に記載した方法以外のセキュリティ対策により、本業務の性質等に照らして、同等以上のセキュリティ上の効果があると認められる場合を含む。ただし、その場合は、具体的かつ明確に、同等以上のセキュリティ上の効果があることを証明すること。）

１　シャドーIT の禁止

業務情報を取り扱う情報システムは、請負者により管理又は明示的に利用が許可された情報システムに限ること。

２ 認証機能

(1)　業務従事者が業務情報を取り扱うために情報システムを利用する場合、当該業務従事者が正当であることを検証するため主体認証を用いた機能を情報システムに設けること。

(2)　主体認証情報としてパスワードを使用し、かつ、業務従事者自らがパスワードを設定することを可能とする場合には、強固なパスワードに必要な桁数や複雑さ（例えばログインパスワードにあっては 10 文字以上（業務情報を含むファイルを保護する主体認証情報にあってはログインパスワードよりさらに十分強固な文字数）を基本とし、かつ、英語大文字・小文字・数字・特殊文字といった複数文字種の混在など）を業務従事者に守らせる機能を設けること。ただし、やむを得ず機能を設けることができない場合は、十分に強固なパスワードを業務従事者に遵守させることやパスワードの使いまわしの禁止など、強固な主体認証情報を設定するに当たってのルールを定め、業務従事者に徹底させること。

(3) 業務情報や業務情報を取り扱う情報システムへの不正アクセスから保護するための主体認証情報が、第三者に対して明らかにならないよう、主体認証情報を送信又は保存する場合にはその内容を暗号化し、主体認証情報に対するアクセス制限を設けて適切に管理すること。

(4)　インターネットを通じて接続試行可能なメールシステムやテレワークシステム等の情報システムに業務情報が保管されている場合は、当該情報システムの主体認証機能の設定において、知識（パスワード等、業務従事者本人のみが知り得る情報）による認証、所有（電子証明書を格納する IC カード、ワンタイムパスワード生成器、業務従事者本人のみが所有する機器等）による認証、生体（指紋や静脈等、本人の生体的な特徴）などの主体認証方式を２つ以上の組み合わせた多要素主体認証方式を用いること。それが困難な場合は、パスワードが万一第三者に漏洩、推知された場合でも、正当な業務従事者のみが接続試行可能な措置を講ずること。

３ アクセス権限設定

(1)　情報システムの特性、情報システムが取り扱う情報の取扱制限等に従い、業務情報に対して正当な権限を有する業務従事者のみがアクセス制御の設定等を行うことができる機能を設けること。

(2)　業務情報を扱う情報システム及び業務情報へのアクセスが許可される主体が、当該業務情報を扱うことが認められる正当な業務従事者のみに確実に制限されるように、アクセス制御機能を適切に運用すること。

４ 不正プログラム等への対策

(1)　想定される不正プログラムの感染経路（少なくとも端末）において、不正プログラム対策ソフトウェア等により対策を講ずること。

(2)　不正プログラム対策ソフトウェア等に定義ファイルを用いる場合、その定義ファイルが常に最新の状態になるように構成すること。

(3)　不正プログラム対策ソフトウェア等により、定期的に全てのファイルを対象としたスキャンを実施するように構成すること。

５　ソフトウェアに関する脆弱性対策

(1)　請負者が脆弱性対応に責任を有する業務情報を扱う情報システムを構成するサーバ装置、端末及び

通信回線装置上で利用するソフトウェアの脆弱性に関する情報は、製品ベンダや脆弱性情報提供サイト等を通じて適時調査を行うこと。

(2)　請負者が脆弱性対応に責任を有する業務情報を扱う情報システムを構成するサーバ装置、端末及び通信回線装置上で利用するソフトウェアにおける脆弱性対策の状況を定期的に確認すること。

(3)　脆弱性対策が講じられていない状態が確認された場合並びにサーバ装置、端末及び通信回線装置上で利用するソフトウェアに関連する脆弱性情報を入手した場合は、セキュリティパッチの適用又はソフトウェアのバージョンアップ等による情報システムへの影響を考慮した上で、ソフトウェアに関する措置を講ずること。

6 保存する情報の暗号化

情報システムのストレージなどの記憶装置に業務情報を保存する場合は、ファイル暗号化等のセキュリティ機能を持つアプリケーションを用いる方法、ハードディスク全体又はファイル単体を暗号化するソフトウェアの導入、OS が備えている暗号化機能などの方法で業務情報が暗号化の対応ができるようにすること。

7 通信回線

(1)　請負者が接続許可を与えた通信回線（支給された Wi-Fi やテザリング用のスマートフォン、一定のセキュリティ要件を満たした通信回線など）以外から業務情報を扱う情報システムを接続させないこと。

(2)　業務情報を扱う情報システムへのリモートアクセス環境を構築する場合は VPN 回線を整備するなどして、通信経路及びアクセス先の情報システムのセキュリティを確保すること。その VPN 回線等のアクセス認証には 2(4)に掲げた多要素認証等の措置を講ずること。

(3)　業務情報を扱う情報システムのリモートアクセスにおいて、無線経路の秘匿性や安全性が不明なものや接続経路の管理状況が不明な無料のインターネット接続サービス等の情報セキュリティ水準が不明な通信回線を利用しないこと。

8　業務従事者端末（PC、スマートフォン等）

(1)　業務情報を扱う業務従事者端末の利用状況（シリアルナンバー、OS 種別・バージョン情報、使用アプリケーション、パッチ適用状況、当該端末を扱っている業務従事者の氏名等）について、最新の状態を把握すること。

(2)　請負者が利用を許可したソフトウェアのみを、業務情報を扱う端末で利用させること。また、許可していないソフトウェアのインストールや利用をさせないこと。

(3)　業務情報を取り扱う端末については、端末の盗難、不正な持ち出し、第三者による不正操作の対策として、少なくとも①から④に挙げる対策を講じること。

①端末で利用する電磁的記録媒体に保存されている業務情報の暗号化
②不要な業務情報を端末に保存しないこと
③端末の放置の禁止
④利用時以外のシャットダウン及びネットワークの切断

なお、業務従事者の作業環境などに応じて表示用デバイスの盗み見等の物理的な脅威から保護するための対策（のぞき見防止フィルタの利用、パーテーションの設置など）が必要な場合は、あわせて講ずること。

(4) 請負者の許可を受けた業務従事者端末を使用すること。

(5)　USB ポートの無効化、未登録の外部電磁的記録媒体の接続を制御・管理する製品やサービスの導入など、請負者が利用を許可していない USB メモリ等の外部電磁的記録媒体へ情報を保存できない対策を講じること。技術的措置を講じることができない場合はルール整備等のマネジメント上の措置を講じていること。

(6)(1)から(5)までのほか、１から７まで及び 11 に求める情報セキュリティ要件（業務従事者端末に関するもの）を満たすこと。

9　メール

原則として、SMTP によるサーバ間通信について TLS（1.2 以上）による保護を利用した、電子メールの盗聴防止策に対応ができるようにすること。技術的対応が困難な場合は、機密性を保持して業務情報をやりとりする適切な代替措置が提案されていること。

10　外部サービス

(1)　情報の保管を行う場合、クラウドサービス等のインターネット上のサービスにて取り扱わず、上記１から６及び 11 の対策を行い、請負者の責任において保管すること。

(2)　(1)に該当する場合（業務情報を直接保管する場合）以外において、外部サービス(請負者以外の者が一般向けに情報システムの一部又は全部の機能を提供するものをいう。以下同じ。))を用いて業務情報を取り扱う場合は、当該外部サービスの利用を通じて請負者が取り扱う業務情報に対して国内法以外の法令及び規制が適用されるリスクを評価して外部サービス提供者を選定し、必要に応じて業務情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を、原則として選定条件に含めていること、または「ISMAP クラウドサービスリスト」に掲載されている外部サービスであること。ただし、当該選定条件を含めることが困難な外部サービスを利用する場合は、これらリスクに対する適切な技術的対抗措置や利用ルールの整備したうえで利用するなど、請負者において可能な限り代替措置を講じていること。

(3)　請負者内での外部サービスを用いた Web 会議サービスで業務情報を取り扱う場合は、可能な限りエンドツーエンド（E2E）の暗号化を行い、議事録作成機能、自動翻訳機能、録画機能など、E2E の暗号化を利用できなくなる機能を使用しないこと。

(4) 請負者が利用を認めていない外部サービスで業務情報を取り扱わないこと。

11　その他

(1)　業務情報を取り扱う情報システムが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログを可能な限り取得すること。

(2)　業務上不要となった業務情報は、速やかに復元できないように抹消すること。

(3)　被監査法人から受領した要機密情報を含む文書等についての取り扱い、持ち出しにおける取り扱い手順を定めること。

「2022年度ペネトレーションテストによる独立行政法人等の情報システムに対するセキュリティ対策状況調査（その1）」

入札資料作成要領

独立行政法人**情報処理推進機構**

目　　次

本書は、「2022年度ペネトレーションテストによる独立行政法人等の情報システムに対するセキュリティ対策状況調査（その1）」に係る入札資料の作成要領を取りまとめたものである。

第1章　独立行政法人情報処理推進機構が入札者に提示する資料及び入札者が提出すべき資料

独立行政法人情報処理推進機構（以下「機構」という。）は入札者に以下の表1に示す資料を提示する。入札者はこれを受け、以下の表2に示す資料を作成し、機構へ提出する。

［表1　機構が入札者に提示する資料］

資料名称	資料内容
① 仕様書	本件「2022年度ペネトレーションテストによる独立行政法人等の情報システムに対するセキュリティ対策状況調査（その1）」の仕様を記述（目的・内容等）。
② 入札資料作成要領	入札者が、評価項目一覧及び提案書に記載すべき項目の概要等を記述。
③ 評価項目一覧	提案書に記載すべき提案要求事項一覧、必須項目及び任意項目の区分、得点配分等を記述。
④ 評価手順書	機構が入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。

［表2　入札者が機構に提出する資料］

資料名称	資料内容
① 評価項目一覧の遵守確認欄及び提案書頁番号欄に必要事項を記入したもの	仕様書に記述された要件一覧を遵守又は達成するか否かに関し、遵守確認欄に○×を記入し、提案書頁番号欄に、該当する提案書の頁番号を記入したもの。
② 提案書	仕様書に記述された要求仕様をどのように実現するかを提案書にて説明したもの。主な項目は以下のとおり。 ・入札者が提案する、調査内容、調査方法。 ・実施体制、スケジュール ・調査・報告書作成者のスキル ・補足資料(入札者の関連する実績の詳細)等

第2章　評価項目一覧に係る内容の作成要領

2.1　評価項目一覧の構成

評価項目一覧の構成及び概要説明を以下表3に示す。

［表3 評価項目一覧の構成の説明］

評価項目一覧における項番	事項	概要説明
0	遵守確認事項	「2022年度ペネトレーションテストによる独立行政法人等の情報システムに対するセキュリティ対策状況調査（その1）」を実施する上で遵守すべき事項。これら事項に係る具体的内容の提案は求めず、全ての項目についてこれを遵守する旨を記述する。
1～4	提案要求事項	提案を要求する事項。これら事項については、入札者が提出した提案書について、各提案要求項目の必須項目及び任意項目の区分け、得点配分の定義に従いその内容を評価する。
5	添付資料	入札者が作成した提案の詳細を説明するための資料。これら自体は、直接評価されて点数が付与されることはない。 例：担当者略歴、会社としての実績、実施条件等

2.2　遵守確認事項

遵守確認事項における各項目の説明を以下に示す。

入札者は、別添「評価項目一覧の遵守確認事項」における「遵守確認」欄に必要事項を記載すること。遵守確認事項の各項目の説明に関しては、以下表4を参照すること。

［表4 遵守確認事項上の各項目の説明］

項目名	項目説明・記入要領	記入者
大項目～小項目	遵守確認事項の分類	機構
内容説明	遵守すべき事項の内容	機構
遵守確認	入札者は、遵守確認事項を実現・遵守可能である場合は〇を、実現・遵守不可能な場合（実現・遵守の範囲等について限定、確認及び調整等が必要な場合等を含む）には×を記載する。	入札者

2.3　提案要求事項

提案要求事項における各項目の説明を以下に示す。

入札者は、別添「評価項目一覧の提案要求事項」における「提案書頁番号」欄に必要事項を記載すること。提案要求事項の各項目の説明に関しては、以下表5を参照すること。

［表5 提案要求事項上の各項目の説明］

項目名	項目説明・記入要領	記入者
大項目～小項目	提案書の目次(提案要求事項の分類)	機構
提案要求事項	入札者に提案を要求する内容	機構
評価区分	必ず提案すべき項目(必須)又は必ずしも提案する必要は無い項目(任意)の区分を設定している。 各項目について、記述があった場合、その内容に応じて配点を行う。	機構
得点配分	基礎点及び各項目に対する最大加点	機構
提案書頁番号	作成した提案書における該当頁番号を記載する。該当する提案書の頁が存在しない場合には空欄とする。評価者は各提案要求事項について、本欄に記載された頁のみを対象として採点を行う。	入札者

2.4　添付資料

添付資料における各項目の説明を以下表6に示す。

［表6 添付資料上の各項目の説明］

項目名	項目説明・記入要領	記入者
大項目～小項目	提案書の目次(提案要求事項の分類)	機構
資料内容	入札者が提案の詳細を説明するための資料	機構
提案の要否	必ず提案すべき項目(必須)又は必ずしも提案する必要は無い項目(任意)の区分を設定している。	機構
提案書頁番号	作成した提案書における該当頁番号を記載する。該当する提案書の頁が存在しない場合には空欄とする。	入札者

第3章　提案書に係る内容の作成要領及び説明

3.1　提案書の構成及び記載事項

以下に、別添「評価項目一覧」から[提案書の目次]の大項目を抜粋したもの及び求められる提案要求事項を表7に示す。提案書は、表7の項番、項目内容に従い、提案要求内容を十分に咀嚼した上で記述及び提案すること。なお、詳細は別添「評価項目一覧」を参照すること。

[表7 提案書目次及び提案要求事項]

提案書 目次項番	大項目	求められる提案要求事項
1	業務の実施方針等	目的を達成するための実施作業内容、実施スケジュール及び本業務の実現性等に加え、以下を記載すること。 ・全体実施計画書の作成方針 ・事前説明会及びヒアリング実施項目 ・個別実施計画書の作成方針 ・個別調査結果報告書の作成方針 ・全体調査結果報告書の作成方針 ・業務の実施体制及び作業実施場所での情報管理方針 ・実施体制に含まれる全ての業務従事者の所属、雇用形態、実績（経験年数、資格等）及び国籍 なお、仕様書に記載した業務内容の他に、より適切な方法など、本業務の効果・効率を高める工夫があれば提案すること。
2	組織の経験・能力	本業務の実施に要求される、体制、環境及び類似業務の実績、ノウハウの蓄積等の実施能力。
3	業務従事者の経験・能力	過去の経験、業務遂行上有効な資格や知識の有無等。
4	ワーク・ライフ・バランス等の推進に関する指標	ワーク・ライフ・バランス等の推進に関する認定又は行動計画の策定状況。 ※本項目を提案書に含める場合は、認定通知書等の写しを添付すること。
5	添付資料	提案した内容の詳細を説明するための資料。例としては、実施担当者の専門知識、関連する資格や実施組織の類似事業の実績の詳細など。

3.2　提案書様式

① 提案書及び評価項目一覧はA4判カラーにて印刷し、特別に大きな図面等が必要な場合には、原則としてA3判にて提案書の中に折り込む。

② 提案書は、電子媒体の提出を求める場合がある。その際のファイル形式は、原則として、Microsoft Office2016互換またはＰＤＦ形式のいずれかとする（これに拠りがたい場合は、機構まで申し出ること）。

3.3 留意事項

① 提案書を評価する者が特段の専門的な知識や商品に関する一切の知識を有しなくても評価が可能な提案書を作成する。なお、必要に応じて用語解説などを添付する。

② 提案に当たって、特定の製品を採用する場合は、当該製品を採用する理由を提案書中に記載するとともに、記載内容を証明及び補足するもの（製品紹介、パンフレット、比較表等）を添付する。

③ 入札者は提案の際、提案内容についてより具体的・客観的な詳細説明を行うための資料を、添付資料として提案書に含めることができる(その際、提案書本文と添付資料の対応が取れるようにする)。

④ 機構から連絡が取れるよう、提案書には連絡先（電話番号、FAX番号、及びメールアドレス）を明記する。

⑤ 上記の提案書構成、様式及び留意事項に従った提案書ではないと機構が判断した場合は、提案書の評価を行わないことがある。また、補足資料の提出や補足説明等を求める場合がある。

⑥ 提案書、その他の書類は、本件における総合評価落札方式（加算方式）の技術評価に使用する。

⑦ 提案書は契約書に添付し、その提案遂行が担保されるため、実現可能な内容を提案すること。

⑧ 提案内容の一部を外注する場合は、その作業内容を明記すること。

「2022年度ペネトレーションテストによる独立行政法人等の情報システムに対するセキュリティ対策状況調査（その1）」

評価項目一覧

独立行政法人**情報処理推進機構**

１．評価項目一覧－遵守確認事項－

大項目	小項目	内容説明	遵守確認
0　遵守確認事項			
	0.1 納入物件	報告書等の各種資料は日本語で作成し、平易な文章で記載すること（ただし、専門用語や固有名詞等に外国語表記を用いることは可能）。	
	0.2 調査の範囲	Ⅲ.仕様書「3.業務内容」に記載している項目を一括して受託すること（部分についての提案は認めない）。	
	0.3 業務従事者の経験・能力	Ⅲ.仕様書「5.実施体制」に記載している業務従事者に関する要件を満たすこと。	
	0.4 スケジュール	業務実施計画（全体実施計画・個別実施計画）を明確に定めた上で工程管理を行い、納入期限を守ること。	

2．提案要求事項

提案書の目次			提案要求事項	評価区分	得点配分			提案書頁番号
大項目	中項目	小項目			基礎点	加点	合計	
1　業務の実施方針等								
	1.1 業務内容の妥当性		・ Ⅲ.仕様書の内容について、全て記載されているか。	必須	11	－	11	
	1.2 業務方法の妥当性、独創性	1.2.1 全体実施計画書の作成	・ Ⅲ.仕様書に基づき、調査対象システム数や作業内容を踏まえた全体実施計画書の項目が具体的に記載されているか。	必須	10	－	130	
		1.2.2 ペネトレーションテストの実施等	・ 事前説明会及びヒアリングの実施項目が具体的に記載されているか。	必須	5	－		
			・ 効果的なペネトレーションテストを実施するための方策（調査対象ホストの選定方法、収集すべき情報や事前調整内容など）が記載されているか。	任意	－	10		
			・ 個別実施計画書の項目が具体的に記載されているか。	必須	5	－		
			・ Ⅲ.仕様書の目的を満たすために有効なテスト実施観点が記載されているか。	任意	－	15		
			・ ペネトレーションテストに用いる手法やツール等が効率的であることが記載されているか。	任意	－	10		
			・ ペネトレーションテスト実施時における課題及び解決方法が具体的に記載されているか。	任意	－	15		
		1.2.3 ペネトレーションテストの実施結果に関する分析及び評価	・ 個別調査結果報告書の構成が具体的に記載されているか。	必須	5	－		
			・ 調査対象システムへの侵入可否を検証するために有効な分析方法が具体的に記載されているか。	任意	－	10		
			・ 検出した問題の危険度等による評価の判断基準が記載されているか。	任意	－	10		
			・ 検出した問題に対し、有効な対処策を助言するための方策が記載されているか。	任意	－	15		
			・ 調査対象システム担当者が情報セキュリティ対策水準の向上に活用できる参考情報等が具体的に記載されているか。	任意	－	15		
			・ 全体調査結果報告書の構成が具体的に記載されているか。	必須	5	－		

	1.3 業務実施計画の妥当性、効率性	・ 業務を効率的に進めるための工夫がなされており、それが妥当である事が説明されているか。	任意	－	10	20	
		・ Ⅲ.仕様書に示された項目以外に、本業務の目的を達成するために必要な作業や留意点等が記載されているか。	任意	－	10		
2 組織の経験・能力							
	2.1 業務の実施能力	・ Ⅲ.仕様書「5.実施体制(1)、(6)①～⑤」に記載した組織としての資格、実績及び体制を有しているか。 ・ 事業の実施体制及び役割が、実施内容と整合しているか。 ・ 要員数、体制、役割分担が明確にされているか。 ・ 事業を遂行可能な人数が確保されているか。 ・ 適切な情報管理体制が確保されているか。また、情報取扱担当者以外の者が、情報に接することがないか。 ・以下の資料が提出されているか。 情報管理に対する社内規則等（社内規則がない場合は代わりとなるもの。）	必須	10	－	40	
		・ 作業実施場所としての請負者の事務所は、日本国内にあり、Ⅲ.仕様書「5.実施体制(6)⑥を満たす情報セキュリティ管理が施されているか。	必須	10	－		
		・Ⅲ.仕様書「6.情報セキュリティに関する要件」に記載した情報セキュリティに関する技術的要件等を満たしていることが説明されているか。また、本要件の各項目に記載した方法以外のセキュリティ対策を実施する場合、同等以上のセキュリティ上の効果があることを、具体的かつ明確に説明しているか。	必須	10	－		
		・ スケジュールの遅延が予測される場合等へ対応するため、人員補助体制が組み込まれた体制が整備されているか。	任意	－	10		
	2.2 類似業務の経験	・ 組織として、官公庁に対するペネトレーションテストや情報セキュリティに関するコンサルティング業務を実施した経験はあるか。	任意	－	15	15	
3 業務従事者の経験・能力							
	3.1 類似業務の専門知識・経験	・ 業務従事者に、Ⅲ.仕様書「5.実施体制(5)」に記載した知識を有した者を含めているか。	必須	10	－	20	
		・ 本業務の実施にあたり有効な経験を有していることが説明されているか。	任意	－	10		
	3.2 業務内容に関する資格・適格性	・ 業務従事者に、Ⅲ.仕様書「5.実施体制(4)（③ウを除く）」に記載した資格等を有した者を含めているか。	必須	10	－	25	

		・ 業務従事者に、Ⅲ.仕様書「5.実施体制(4)③ウ」に記載した資格保有者を含める等、本業務の実施にあたり有効な高度な情報セキュリティに関する専門知識・知見を有していることが説明されているか。	任意	－	15		
4 ワーク・ライフ・バランス等の推進に関する指標							
		・企業として、以下のいずれかに該当するワーク・ライフ・バランスの取組を推進しているか。 ①女性の職業生活における活躍の推進に関する法律（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） ②次世代育成支援対策推進法（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） ③青少年の雇用の促進等に関する法律（若者雇用促進法）に基づく認定（ユースエール認定企業）	任意	－	9	9	
				91	179	270	

３．添付資料

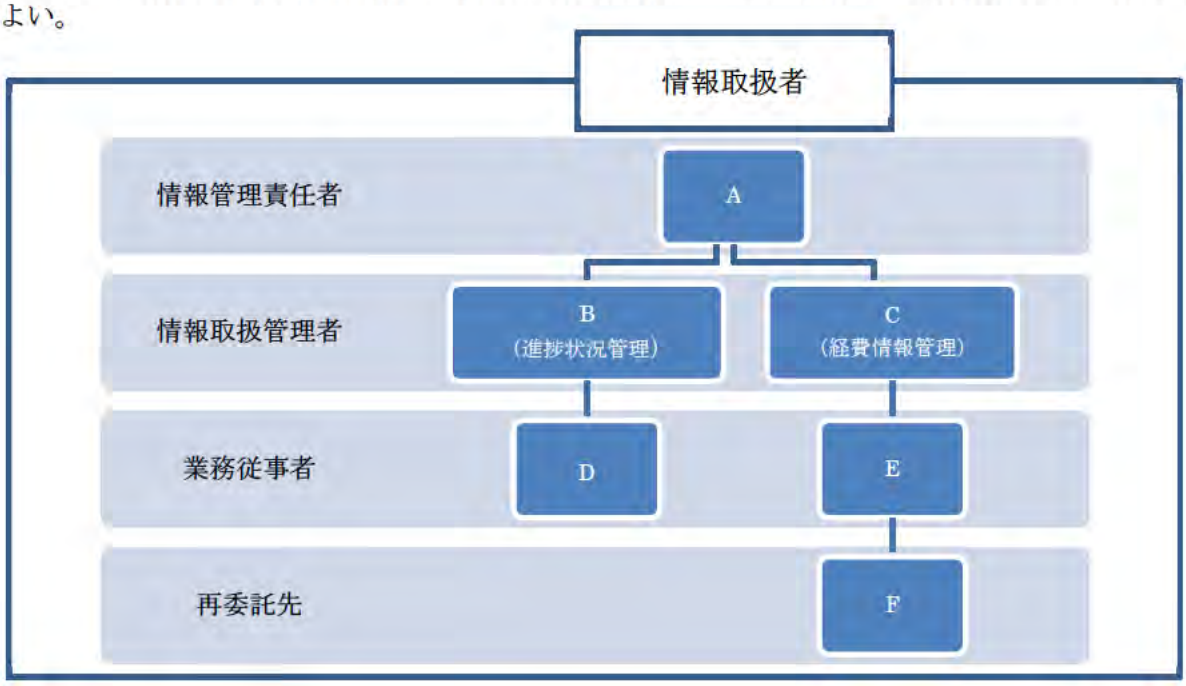
提案書の目次		資料内容	提案の要否	提案書頁番号
大項目	小項目			
5　添付資料				
	5.1 実施体制及び調査・作成者略歴	・ 入札者の概要の分かる資料	任意	
		・ 本業務履行のための体制図	必須	
		・ 各業務担当者の略歴（氏名、所属、役職、職歴、業務経験、研修実績その他経歴、専門的知識その他の知見、母語及び外国語能力、国籍等）	必須	
		・ 請負者の情報管理体制がわかる「情報管理体制図」、情報を取扱う者の氏名・住所・生年月日・所属部署・役職等がわかる「情報取扱担当者名簿」を契約前に提出できることを確約する。 （「情報管理体制図」及び「情報取扱者名簿」に記載すべき事項等は次ページを参照）	必須	
	5.2 会社としての実績	・ 本業務の類似案件実績	任意	
		・ 本業務に有用な領域での資格、実績等	任意	
		・ ワーク・ライフ・バランス等の推進に関する認定通知書等の写し	任意	
	5.3 その他	・ その他提案内容を補足する説明、業務実施における前提条件等	任意	

※情報管理体制図に記載すべき事項

a）本業務の遂行に当たって保護すべき情報を取り扱うすべての者。（再請負先も含む。）

b）本業務の遂行のため最低限必要な範囲で情報取扱者を設定し記載すること。

c）有している場合には情報管理に関する社内規則を提出すること。有しない場合は代わりとなるものでもよい。



※情報取扱者名簿に記載すべき事項等

（※１）請負者としての情報取扱の全ての責任を有する者。必ず明記すること。

（※２）本業務の遂行にあたって主に保護すべき情報を取り扱う者ではないが、本業務の進捗状況などの管理を行うもので、保護すべき情報を取り扱う可能性のある者。

（※３）本業務の遂行にあたって保護すべき情報を取り扱う可能性のある者。

（※４）日本国籍を有する者及び法務大臣から永住の許可を受けた者（入管特例法の「特別永住者」を除く。）以外の者は、パスポート番号等及び国籍を記載。

（※５）個人住所、生年月日については、必ずしも契約前に提出することを要しないが、その場合であっても担当部門から求められた場合は速やかに提出すること。

情報取扱者名簿

		（しめい） 氏名	個人住所 （※5）	生年月日 （※5）	所属部署	役職	パスポート番号及び 国籍（※4）
情報管理責任者（※1）	A						
情報取扱管理者（※2）	B						
	C						
業務従事者（※3）	D						
	E						
再委託先	F						

「2022年度ペネトレーションテストによる独立行政法人等の情報システムに対するセキュリティ対策状況調査（その1）」

評価手順書(加算方式)

独立行政法人**情報処理推進機構**

本書は、「2022年度ペネトレーションテストによる独立行政法人等の情報システムに対するセキュリティ対策状況調査（その1）」に係る評価手順を取りまとめたものである。落札方式、評価の手続き及び加点方法等を以下に示す。

第1章　落札方式及び得点配分

1.1　落札方式

次の要件を共に満たしている者のうち、「1.2 総合評価点の計算」によって得られた数値の最も高い者を落札者とする。

①　入札価格が予定価格の制限の範囲内であること。

②「Ⅴ.評価項目一覧」の遵守確認事項及び評価項目の必須区分を全て満たしていること。

1.2　総合評価点の計算

総合評価点　＝　技術点　＋　価格点

技術点 ＝ 基礎点 ＋ 加点

価格点 ＝ 価格点の配分　×　（ 1　－ 入札価格 ÷ 予定価格）

※小数点第2位以下切捨て

1.3　得点配分

技術点に関し、必須及び任意項目の配分を270点、価格点の配分を135点とする。

技術点	270点
価格点	135点

第2章　評価の手続き

2.1　一次評価

一次評価として、「Ⅴ.評価項目一覧」の各事項について、次の要件をすべて満たしているか審査を行う。一次評価で合格した提案書について、次の「2.2二次評価」を行う。

①「1.遵守確認事項」の「遵守確認」欄に全て「○」が記入されていること。

②「2.提案要求事項」の「提案書頁番号」欄に、提案書の頁番号が記入されていること。

③「3.添付資料」の提案が必須となっている資料の「提案書頁番号」欄に頁番号が記入されていること。

2.2　二次評価

上記「2.1 一次評価」で合格した提案書に対し、次の「第3章 評価項目の加点方法」に基づき技術評価を行う。なお、ヒアリングを実施した場合には、ヒアリングにより得られた評価を加味するものとする。

評価に当たっては、複数の審査員の合議によって各項目を評価し、評価に応じた得点の合計をもって技術点とする。

2.3　総合評価点の算出

以下の技術点と価格点を合計し、総合評価点を算出する。

①「2.2 二次評価」により算定した技術点

②「1.2 総合評価点の計算」で定めた計算式により算定した価格点

第3章　評価項目の加点方法

3.1　評価項目得点構成

評価項目（提案要求事項）毎の得点については、評価区分に応じて、必須項目は基礎点、任意項目は加点として付与する。

なお、評価項目毎の基礎点、加点の得点配分は「Ⅴ．評価項目一覧」の「2.評価項目一覧-提案要求事項-」を参照すること。

3.2　基礎点評価

提案内容が、必須項目を満たしている場合に基礎点を付与し、そうでない場合は0点とする。従って、一つでも必須項目を満たしていないと評価（0点）した場合は、その入札者を**不合格**とし、価格点の評価は行わない。

3.3　加点評価

任意項目について、提案内容に応じて下表の評価基準に基づき加点を付与する。

評価ランク	評価基準	項目別得点	
S	通常の想定を超える卓越した提案内容である。	15	10
A	通常想定される提案としては最適な内容である。	9	6
B	概ね妥当な内容である。	4	3
C	内容が不十分である。	0	0

ただし、「4 ワーク･ライフ・バランス等の推進に関する指標」については、下表の評価基準に基づき加点を付与する。複数の認定等が該当する場合は、最も配点が高い区分により加点を付与する。

認定等の区分		項目別得点
女性活躍推進法に基づく認定（えるぼし認定企業・プラチナえるぼしに認定企業）	プラチナえるぼし（※1）	9
	認定基準○（5）（※2）	7
	認定基準○（3～4）（※2）	6
	認定基準○（1～2）（※2）	3
	行動計画（※3）	1.5
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）	プラチナくるみん認定企業	7
	くるみん認定企業（新基準）（※4）	6
	くるみん認定企業（旧基準）（※5）	3
若者雇用促進法に基づく認定（ユースエール認定企業）		7

※1　改正後女性活躍推進法（令和2年6月1日施行）第12条に基づく認定
※2　女性活躍推進法第9条に基づく認定
　　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。

※3　常時雇用する労働者の数が300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）。
※4　新くるみん認定（改正後認定基準（平成29年4月1日施行）により認定）
※5　旧くるみん認定（改正前認定基準又は改正省令附則第2条第3項の経過措置により認定）

Ⅶ. その他関係資料

独立行政法人情報処理推進機構入札心得

（趣　旨）
第１条　独立行政法人情報処理推進機構（以下「機構」という。）の契約に係る一般競争又は指名競争（以下「競争」という。）を行う場合において、入札者が熟知し、かつ遵守しなければならない事項は、関係法令、機構会計規程及び入札説明書に定めるもののほか、この心得に定めるものとする。

（仕様書等）
第２条　入札者は、仕様書、図面、契約書案及び添付書類を熟読のうえ入札しなければならない。
２　入札者は、前項の書類について疑義があるときは、関係職員に説明を求めることができる。
３　入札者は、入札後、第１項の書類についての不明を理由として異議を申し立てることができない。

（入札保証金及び契約保証金）
第３条　入札保証金及び契約保証金は、全額免除する。

（入札の方法）
第４条　入札者は、別紙様式による入札書を直接又は郵便等で提出しなければならない。

（入札書の記載）
第５条　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 パーセントに相当する額を加算した金額をもって落札価格とするので、入札者は消費税に係る課税事業者であるか免税事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。

（直接入札）
第６条　直接入札を行う場合は、入札書を封筒に入れ、封緘のうえ入札者の氏名を表記し、予め指定された時刻までに契約担当職員等に提出しなければならない。この場合において、入札書とは別に提案書及び証書等の書類を添付する必要のある入札にあっては、入札書と併せてこれら書類を提出しなければならない。
２　入札者は、代理人をして入札させるときは、その委任状を持参させなければならない。

（郵便等入札）
第７条　郵便等入札を行う場合には、二重封筒とし、入札書を中封筒に入れ、封緘のうえ入札者の氏名、宛先、及び入札件名を表記し、予め指定された時刻までに到着するように契約担当職員等あて書留で提出しなければならない。この場合において、入札書とは別に提案書及び証書等の書類を添付する必要のある入札にあっては、入札書と併せてこれら書類を提出しなければならない。
２　入札者は、代理人をして入札させるときは、その委任状を同封しなければならない。

（代理人の制限）
第８条　入札者又はその代理人は、当該入札に対する他の代理をすることができない。
２　入札者は、予算決算及び会計令（昭和 22 年勅令第 165 号、以下「予決令」という。）第 71 条第１項各号の一に該当すると認められる者を競争に参加することが出来ない期間は入札代理人とすることができない。

（条件付きの入札）
第９条　　予決令第 72 条第１項に規定する一般競争に係る資格審査の申請を行ったものは、競争に参加する者に必要な資格を有すると認められること又は指名競争の場合にあっては指名されることを条件に入札書を提出することができる。この場合において、当該資格審査申請書の審査が開札日までに終了しないとき又は資格を有すると認められなかったとき若しくは指名されなかったときは、当該入札書は落札の対象としない。

（入札の取り止め等）

第 10 条　入札参加者が連合又は不穏の行動をなす場合において、入札を公正に執行することができないと認められるときは、当該入札者を入札に参加させず又は入札の執行を延期し、若しくは取り止めることがある。

（入札の無効）

第 11 条　次の各号の一に該当する入札は、無効とする。

(1) 競争に参加する資格を有しない者による入札
(2) 指名競争入札において、指名通知を受けていない者による入札
(3) 委任状を持参しない代理人による入札
(4) 記名押印（外国人又は外国法人にあっては、本人又は代表者の署名をもって代えることができる。）を欠く入札
(5) 金額を訂正した入札
(6) 誤字、脱字等により意思表示が不明瞭である入札
(7) 明らかに連合によると認められる入札
(8) 同一事項の入札について他人の代理人を兼ね又は 2 者以上の代理をした者の入札
(9) 入札者に求められる義務を満たすことを証明する必要のある入札にあっては、証明書が契約担当職員等の審査の結果採用されなかった入札
(10) 入札書受領期限までに到着しない入札
(11) 暴力団排除に関する誓約事項（別記）について、虚偽が認められた入札
(12) その他入札に関する条件に違反した入札

（開　札）

第 12 条　開札には、入札者又は代理人を立ち会わせて行うものとする。ただし、入札者又は代理人が立会わない場合は、入札執行事務に関係のない職員を立会わせて行うものとする。

（調査基準価格、低入札価格調査制度）

第 13 条　工事その他の請負契約（予定価格が 1 千万円を超えるものに限る。）について機構会計規程細則第 26 条の 3 第 1 項に規定する相手方となるべき者の申込みに係る価格によっては、その者により当該契約の内容に適合した履行がされないこととなるおそれがあると認められる場合の基準は次の各号に定める契約の種類ごとに当該各号に定める額（以下「調査基準価格」という。）に満たない場合とする。

(1) 工事の請負契約　その者の申込みに係る価格が契約ごとに 3 分の 2 から 10 分の 8.5 の範囲で契約担当職員等の定める割合を予定価格に乗じて得た額
(2) 前号以外の請負契約　その者の申込みに係る価格が 10 分の 6 を予定価格に乗じて得た額

2　調査基準価格に満たない価格をもって入札（以下「低入札」という。）した者は、事後の資料提出及び契約担当職員等が指定した日時及び場所で実施するヒアリング等（以下「低入札価格調査」という。）に協力しなければならない。

3　低入札価格調査は、入札理由、入札価格の積算内訳、手持工事等の状況、履行体制、国及び地方公共団体等における契約の履行状況等について実施する。

（落札者の決定）

第 14 条　一般競争入札最低価格落札方式（以下「最低価格落札方式」という。）にあっては、有効な入札を行った者のうち、予定価格の制限の範囲内で最低の価格をもって入札した者を落札者とする。また、一般競争入札総合評価落札方式（以下「総合評価落札方式」という。）にあっては、契約担当職員等が採用できると判断した提案書を入札書に添付して提出した入札者であって、その入札金額が予定価格の制限の範囲内で、かつ提出した提案書と入札金額を当該入札説明書に添付の評価手順書に記載された方法で評価、計算し得た評価値（以下「総合評価点」という。）が最も高かった者を落札者とする。

2　低入札となった場合は、一旦落札決定を保留し、低入札価格調査を実施の上、落札者を決定する。

3　前項の規定による調査の結果その者により当該契約の内容に適合した履行がされないおそれがあると認められるとき、又はその者と契約を締結することが公正な取引の秩序を乱すこととなるおそれがあって著しく不適当であると認められるときは、次の各号に定める者を落札者とすることがある。

(1) 最低価格落札方式　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、最低の価格をもって入札した者
(2) 総合評価落札方式　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、総合評価点が最も高かった者

（再度入札）
第 15 条　開札の結果予定価格の制限に達した価格の入札がないときは、直ちに再度の入札を行う。なお、開札の際に、入札者又はその代理人が立ち会わなかった場合は、再度入札を辞退したものとみなす。
2　前項において、入札者は、代理人をして再度入札させるときは、その委任状を持参させなければならない。

（同価格又は同総合評価点の入札者が二者以上ある場合の落札者の決定）
第 16 条　落札となるべき同価格又は同総合評価点の入札をした者が二者以上あるときは、直ちに当該入札をした者又は第 12 条ただし書きにおいて立ち会いをした者にくじを引かせて落札者を決定する。
2　前項の場合において、当該入札をした者のうちくじを引かない者があるときは、これに代わって入札事務に関係のない職員にくじを引かせるものとする。

（契約書の提出）
第 17 条　落札者は、契約担当職員等から交付された契約書に記名押印（外国人又は外国法人が落札者である場合には、本人又は代表者が署名することをもって代えることができる。）し、落札決定の日から 5 日以内（期終了の日が行政機関の休日に関する法律（昭和 63 年法律第 91 号）第 1 条に規定する日に当たるときはこれを算入しない。）に契約担当職員等に提出しなければならない。ただし、契約担当職員等が必要と認めた場合は、この期間を延長することができる。
2　落札者が前項に規定する期間内に契約書を提出しないときは、落札はその効力を失う。

（入札書に使用する言語及び通貨）
第 18 条　入札書及びそれに添付する仕様書等に使用する言語は、日本語とし、通貨は日本国通貨に限る。

（落札決定の取消し）
第 19 条　落札決定後であっても、この入札に関して連合その他の事由により正当な入札でないことが判明したときは、落札決定を取消すことができる。

以上

（別記）

暴力団排除に関する誓約事項

当社（個人である場合は私、団体である場合は当団体）は、下記の「契約の相手方として不適当な者」のいずれにも該当しません。

この誓約が虚偽であり、又はこの誓約に反したことにより、当方が不利益を被ることとなっても、異議は一切申し立てません。

記

1. 契約の相手方として不適当な者

(1) 法人等（個人、法人又は団体をいう。）が、暴力団（暴力団員による不当な行為の防止等に関する法律（平成 3 年法律第 77 号）第 2 条第 2 号に規定する暴力団をいう。以下同じ。）であるとき又は法人等の役員等（個人である場合はその者、法人である場合は役員又は支店若しくは営業所（常時契約を締結する事務所をいう。）の代表者、団体である場合は代表者、理事等、その他経営に実質的に関与している者をいう。以下同じ。）が、暴力団員（同法第 2 条第 6 号に規定する暴力団員をいう。以下同じ。）であるとき

(2) 役員等が、自己、自社若しくは第三者の不正の利益を図る目的又は第三者に損害を加える目的をもって、暴力団又は暴力団員を利用するなどしているとき

(3) 役員等が、暴力団又は暴力団員に対して、資金等を供給し、又は便宜を供与するなど直接的あるいは積極的に暴力団の維持、運営に協力し、若しくは関与しているとき

(4) 役員等が、暴力団又は暴力団員であることを知りながらこれと社会的に非難されるべき関係を有しているとき

上記事項について、入札書の提出をもって誓約します。

（様　式　1）

年　　月　　日

独立行政法人情報処理推進機構　セキュリティセンター　公共セキュリティ部
セキュリティ監査グループ　担当者殿

質 問 書

「2022 年度ペネトレーションテストによる独立行政法人等の情報システムに対するセキュリティ対策状況調査（その 1)」に関する質問書を提出します。

法人名	
所属部署名	
担当者名	
電話番号	
E-mail	

質問書枚数
枚中 枚目

＜質問箇所について＞

資料名	例）　○○書
ページ	例）　P○
項目名	例）　○○概要
質問内容	

備考
1. 質問は、本様式1 枚につき1 問とし、簡潔にまとめて記載すること。
2. 質問及び回答は、IPA のホームページに公表する。（電話等による個別回答はしない。）また、質問者自身の既得情報（特殊な技術、ノウハウ等)、個人情報に関する内容については、公表しない。

（様　式　2）

年　　月　　日

独立行政法人情報処理推進機構　理事長　殿

所　在　地

商号又は名称

代 表 者 氏 名　　印
（又は代理人）

委　任　状

私は、下記の者を代理人と定め、「2022 年度ペネトレーションテストによる独立行政法人等の情報システムに対するセキュリティ対策状況調査（その 1)」の入札に関する一切の権限を委任します。

代 理 人(又は復代理人)

所　在　地

所属・役職名

氏　　名

使 用 印 鑑

（様　式　3）

年　　月　　日

独立行政法人情報処理推進機構　理事長　殿

所　在　地

商号又は名称

代表者氏名　　印

（又は代理人、復代理人氏名）

印

入　札　書

入札金額　　￥＿＿＿＿＿＿＿＿＿＿＿＿

（※　下記件名に係る費用の総価を記載すること）

件　名　「2022年度ペネトレーションテストによる独立行政法人等の情報システムに対するセキュリティ対策状況調査（その1）」

契約条項の内容及び貴機構入札心得を承知のうえ、入札いたします。

（様　式　4）

提案書受理票（控）

提案書受理番号＿＿＿＿＿＿＿＿＿＿＿＿

件名：「2022 年度ペネトレーションテストによる独立行政法人等の情報システムに対するセキュリティ対策状況調査（その 1）」に関する提案書

【入札者記載欄】

提出年月日：　　年　　月　　日
法 人 名：
所 在 地：　〒
担 当 者：　所属・役職名
氏名
TEL　　FAX
E-Mail

【ＩＰＡ担当者使用欄】

No.	提出書類	部数	有無	No.	提出書類	部数	有無
①	委任状（委任する場合）	1 通		②	入札書（封緘）	1 通	
③	提案書	4 部		④	評価項目一覧	4 部	
⑤	資格審査結果通知書の写し	1 通		⑥	「情報セキュリティサービス基準適合サービスリスト」申請書の写し（手続き中の場合）	1 通	
⑦	③と④の電子ファイル（CD または電子メールで提出）	各 1 部		⑧	提案書受理票	（本紙）	―

切り取り

提案書受理番号＿＿＿＿＿＿＿＿＿＿＿＿

提案書受理票

年　　月　　日

件　名　「2022 年度ペネトレーションテストによる独立行政法人等の情報システムに対するセキュリティ対策状況調査（その 1）」

法人名（入札者が記載）：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

担当者名（入札者が記載）：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿殿

貴殿から提出された標記提案書を受理しました。

独立行政法人情報処理推進機構　セキュリティセンター　公共セキュリティ部
セキュリティ監査グループ
担当者名：　　㊞

（参　考）

予算決算及び会計令【抜粋】

（一般競争に参加させることができない者）

第 70 条　契約担当官等は、売買、貸借、請負その他の契約につき会計法第二十九条の三第一項の競争（以下「一般競争」という。）に付するときは、特別の理由がある場合を除くほか、次の各号のいずれかに該当する者を参加させることができない。

一　当該契約を締結する能力を有しない者

二　破産手続開始の決定を受けて復権を得ない者

三　暴力団員による不当な行為の防止等に関する法律（平成三年法律第七十七号）第三十二条第一項各号に掲げる者

（一般競争に参加させないことができる者）

第 71 条　契約担当官等は、一般競争に参加しようとする者が次の各号のいずれかに該当すると認められるときは、その者について三年以内の期間を定めて一般競争に参加させないことができる。その者を代理人、支配人その他の使用人として使用する者についても、また同様とする。

一　契約の履行に当たり故意に工事、製造その他の役務を粗雑に行い、又は物件の品質若しくは数量に関して不正の行為をしたとき。

二　公正な競争の執行を妨げたとき又は公正な価格を害し若しくは不正の利益を得るために連合したとき。

三　落札者が契約を結ぶこと又は契約者が契約を履行することを妨げたとき。

四　監督又は検査の実施に当たり職員の職務の執行を妨げたとき。

五　正当な理由がなくて契約を履行しなかつたとき。

六　契約により、契約の後に代価の額を確定する場合において、当該代価の請求を故意に虚偽の事実に基づき過大な額で行つたとき。

七　この項（この号を除く。）の規定により一般競争に参加できないこととされている者を契約の締結又は契約の履行に当たり、代理人、支配人その他の使用人として使用したとき。

2　契約担当官等は、前項の規定に該当する者を入札代理人として使用する者を一般競争に参加させないことができる。