「ECサイトセキュリティ対策のための調査業務」に係る一般競争入札

（総合評価落札方式）

入札説明書

2022年3月25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3月25日付け公告）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　　ECサイトセキュリティ対策のための調査業務
(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) 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。

なお、入札金額は、別紙入札内訳書に基づき各単価に予定数量を乗じた総価とする。また、本業務の履行のための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」又は「B」の等級に格付けされ、関東・甲信越地域の資格を有する者であること。
(4) 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。
(5) 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。
(6) 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。

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．入札説明会の日時及び場所

(1) 入札説明会の日時
2022年4月11日（月） 11時00分
(2) 入札説明会の実施方法
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.(4)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7日（木）17時00分までに申し込むこと。
② 電子メールの件名に「【ECサイトセキュリティ対策のための調査業務】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。

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11日（月）から2022年5月9日（月）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.(4)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5月13日（金）から2022年5月16日（月）。
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5月16日（月） 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.(4)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	－	５部
④	評価項目一覧	－	５部
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	提案書受理票	様式４	１通
⑦	③と④の電子ファイル		

(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.(4)の担当者名）を記載するとともに「ECサイトセキュリティ対策のための調査業務　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.(4)の担当者名）を記載し、かつ、「ECサイトセキュリティ対策のための調査業務　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17時までに14.(4)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「ECサイトセキュリティ対策のための調査業務　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.(4)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.(4)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 ヒアリングを次の日程で実施する。

日時：2022年5月19日（木）10時30分～17時30分の間（1者あたり1時間を予定）

感染症予防対策のため、オンラインまたは電子メールや電話等の手段によるヒアリングを行う場合があるので、その際はIPAの指示に従うこと。

なお、ヒアリングについては、提案内容を熟知した実施責任者等が対応すること。

7. 開札の日時及び場所

(1) 開札の日時

2022年5月23日（月）　11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（案）を参照）

なお、落札者より提出された別紙入札内訳書により、単価契約とする。

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、機構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)　落札者は、契約締結時までに別紙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。

(4)　入札説明会への参加申込み、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16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 セキュリティ対策推進部
脆弱性対策グループ　担当：板橋、土屋（昭）
TEL：03-5978-7527
E-mail：isec-vm-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。

(5)　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: 吉中、中尾
TEL：03-5978-7502
E-mail：fa-bid-kt@ipa.go.jp

別紙

年　　月　　日

入札内訳書

独立行政法人情報処理推進機構
理事長　富田　達夫　殿

住所
法人名
代表者名　　印

件名： EC サイトセキュリティ対策のための調査業務

項　目	予定数量	単位	単価（円）	金額（円）
下記を除く本事業に係る全作業（※１）	1	式		
仕様書 3.2.2(2)～(5)および(7)診断の実施（※２）	30	脆弱性診断先の EC サイト数		
			合計（税抜）	（※３）

※１　本事業に係る全作業には、
Ⅲ.仕様書のうち「3.2.2(2)～(5)および(7)」以外の全ての作業に要する費用を含めること。

※２　実際の数量は予定数量よりも減少する場合があるが、その場合も単価の変更はできない。

※３　同欄に算出された金額を入札書に記載すること。
なお、落札者の決定に当たっては、入札金額に 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。

※４　各金額について、1 円未満の端数は認めない。

（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（案）

○○○○情財第○○号

契　約　書

独立行政法人情報処理推進機構（以下「甲」という。）と○○○○○（以下「乙」という。）とは、次の条項により「EC サイトセキュリティ対策のための調査業務」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「EC サイトセキュリティ対策のための調査業務」（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。

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及び契約単価は、次のとおりとする。

(1)EC サイトに対する個別調査を除く業務

業務	契約金額（税抜）	数量
仕様書 3.2.2(2)～(5)及び(7)診断の実施以外	円	一式

(2)EC サイトに対する個別調査実施業務

業務	一件あたりの単価（税抜）	予定数量
仕様書 3.2.2(2)～(5)及び(7)診断の実施	円	30 件

2　甲が本契約の対価として乙に支払うべき金額は、前項第 1 号の契約金額と、前項第 2 号に定める単価に調査の実績件数を乗じて得た金額との合計金額に、消費税額及び地方消費税額（消費税法第 28 条第 1 項及び第 29 条並びに地方税法第 72 条の 82 及び第 72 条の 83 の規定に基づき算出した額）を加えた額とする。

3　第 1 項の契約単価には、当該業務の履行のための一切の費用が含まれるものとする。

（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 10 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、第 5 条に規定する契約金額、単価及び予定数量に基づき、同様の計算によって得られる対価としての金額から、既済部分に相当する金額を控除した額の 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。）を違約金として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、契約書本文第5条に規定する契約金額、単価及び予定数量に基づき、同様の計算によって得られる対価としての金額（本契約締結後、契約金額又は単価の変更があった場合には、変更後の契約金額又は単価から得られる金額）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。

20〇〇年〇月〇日

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

「EC サイトセキュリティ対策のための調査業務」

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

EC サイトセキュリティ対策のための調査業務

2. 背景・目的

2.1. 背景

B to C の越境 EC（電子商取引）市場が世界的に急速に拡大している中、日本が世界の EC 市場参入に取り残されないためにも、海外展開を目指す中小企業者等に対して、越境 EC 市場参入のための支援をすることが重要である。

一方、報道で頻繁に取り上げられるように、EC サイト改ざんによる個人情報・クレジットカード情報等の流出事件が後を絶たず、越境 EC 市場参入のためには EC サイトのセキュリティ対策強化が必須である。

しかし、EC サイトを運営する中小企業等はサイバーセキュリティに対する意識が一般的に高くなく、何をすべきかがわからない状況であり、これら中小企業等に対し、適切な指針を作成することが重要である。

本背景の中、中小企業者等が運営する EC サイトについて、システムベンダー等との契約・運営保守状況や脆弱性に関する調査を行い、サイト運営事業者が特に陥りやすいセキュリティの誤解や実施すべき対策を明らかにし、EC サイト構築時・運営時に留意すべき事項をまとめたガイドラインを策定・普及する必要がある

2.2. 目的

本事業では、海外展開を目指す中小企業者等の安全な越境 EC 市場参入を支援するため、中小企業者等が運営する EC サイトについて、脆弱性等に関する調査を行うことで、EC サイト構築時・運営時に留意すべき事項をまとめたガイドライン等の策定および普及を目的とする。

3. 業務内容

3.1. 業務概要

中小企業等が運営する EC サイト等へのヒアリングや脆弱性診断等を実施調査し得られた結果を踏まえてガイドライン等の作成を行う。

- EC サイトへのサイバー攻撃による被害企業の被害実態調査
- EC サイトのセキュリティ対策状況調査
- EC サイトセキュリティ対策ガイドラインの作成
- 委員会の運営支援作業
- 調査実施報告書等の作成

3.2. 業務内容

3.2.1. EC サイトへのサイバー攻撃による被害企業等の被害実態調査

過去、EC サイトがサイバー攻撃を受け、個人情報、クレジットカード情報等の漏洩被害が発生した中小企業等に対しヒアリングを実施し、被害の内容、被害の原因、EC サイト構築時のセキュリティ対策、被害時のセキュリティ対策状況（運用・保守契約の締結状況、運営体制、脆弱性診断の頻度、修正すべき脆弱性のモニタリング・対策状況）および EC サイト運営体制、被害後に実施した技術・運用・契約面での対策内容およびその十分性等を把握する。

本情報を EC サイト運営者の使用パッケージ、サイト構築・運用形態の差異等により分析し、EC サイト構築、運用、契約時におけるセキュリティ対策強化に資する教訓を抽出する。

(1) ヒアリング調査

【対象と件数】

① 被害企業：20 社

・中小企業が運営する EC サイト

・ヒアリング対象に関しては IPA が企業リストを提示するので、請負者は当該企業にコンタクトの上ヒアリングに協力いただける 20 社を選定し、IPA の承認のもとアポイントを開始し、了承を得た企業のヒアリングを実施すること。

・企業リストに関し IPA は、ヒアリングできないケースも考慮して選定に十分な企業数を提供する。

・ヒアリング企業の選定においては、被害企業の状況と心情を考慮し、誠意をもってヒアリングの了解を頂く様に努力すること。

② EC サイト構築事業者等：以下合計 10 社
EC サイト構築時のセキュリティ対策の実施状況の確認、および運用・保守契約におけるセキュリティ対策の実施状況や、提供しているセキュリティに関するサービス内容等を把握し、その結果を、EC サイト構築、運用、契約時におけるセキュリティ対策強化に資する対策ガイドラインに反映する。

・パッケージベンダ：EC-CUBE、WelCart、その他含め計 3 社
・EC-CUBE のインテグレートパートナーで構築事例のコンピテンシーを持つプラチナ、ゴールド、シルバーのランク所有事業者：3 社（各 1 社）
・その他のパッケージの EC 構築事業者：4 社
・ヒアリング対象に関しては請負者が上記対象に沿い IPA に提案し、IPA の承認のもとアポイントを開始し、了承を得た企業のヒアリングを実施すること。
・ヒアリング対象の 10 社の対象件数については、アポイントメント状況等により、IPA の承認のもと変更を可能とする。

③ ショッピングカート ASP 事業者（以下、ASP 事業者）：5 社
EC サイト構築時にショッピングカードの利用におけるセキュリティ対策の実施状況の確認、および運用・保守契約におけるセキュリティ対策の実施状況や、提供しているセキュリティに関するサービス内容等を把握し、その結果を、EC サイト構築、運用、契約時におけるセキュリティ対策強化に資する対策ガイドラインに反映する。

・ヒアリング対象に関しては請負者が上記対象に沿い IPA に提案し、IPA の承認のもとアポイントを開始し、了承を得た企業のヒアリングを実施すること。

上記に記載をしている①、②、③のヒアリング件数を変更する場合は、IPA と協議の上変更をすること。

【ヒアリング項目例】
項目例を以下に示す。請負者はこの内容を元に改めて整理し、IPA の承認のもと確定させること。

① 被害企業
・被害概要：概要／現在の状況／背景／調査方法／公表状況
・被害内容：個人情報流出／クレジットカード情報流出／暗号化／破壊／脅迫
・被害原因：一次的な原因（脆弱性／設定不備／…）、二次的な原因（バックドアが設置された事により情報が窃取された／…）
・被害時の対応：被害当時の対応、復旧までの経緯、被害損失（金額換算）
・被害時のセキュリティ対策状況：運用時のセキュリティ対策内容、運用・保守契約の有無（セキュリティ対応、脆弱性情報提供、脆弱性パッチ対応）
・被害時のサイト運営体制(自組織人員の有無等)、サイバーセキュリティ関連保険への加入状況
・構築時のセキュリティ対策：セキュリティ設計、セキュアコーディング、脆弱性診断等の有無
・根本対策：実施に実施した対策（例えば、ASP サービスに移行した場合そう判断した理由等）
・改善内容：ベンダ選定、アプリケーション改修（セキュアプログラミング）／脆弱性診断／PCI-DSS
・「たられば」（教訓）:こうやっておけばよかった等
・そもそもセキュリティの重要性は理解していたと思われるが、実施しなかった理由
・その他、業界団体等に対する要望等

② EC サイト構築事業者
・EC サイト運営者（EC サイト構築事業者のお客様）の運用・保守契約の締結状況（契約率が低い場合は、その理由と対策案）
・運用・保守契約を締結している場合の保守内容の状況（特に費用支出に関して）
・契約書上でのセキュリティ関連の実施項目の記載状況
・脆弱性診断の提案状況及び提案をする上での制約状況
・セキュリティの運用・保守コストの算出方法と内訳
・業界としての改善策
・（EC-CUBE 社の場合）インテグレートパートナーのランキングを算出する基準等（セキュリティの観点が含まれているか）

③　ASP 事業者

・ASP 事業者のセキュリティ対策内容（PCI-DSS 準拠状況や脆弱性診断やセキュリティ監視等）
・お客様によるカスタマイズにおけるセキュリティ上の懸念（脆弱性の入り込む余地等）
・お客様コンテンツに問題があった場合、ASP 事業者責任が生じる可能性の有無
・お客様におけるセキュリティ事件・事故等

【調査方法】

・請負者はヒアリング調査に向け事前に「ヒアリング主旨説明」資料を作成し IPA からの承認を得ること。「ヒアリング主旨説明」資料には、ヒアリング主旨説明文、ヒアリング概要（件名、主な内容、実施日、実施場所、訪問者、問合せ先等）、ヒアリング調査詳細項目を記載すること。
・請負者はヒアリング対象組織に対し、「ヒアリング主旨説明」資料を同報のうえアポイントを取ること。
・ヒアリング前に可能な範囲でヒアリング対象組織からヒアリング項目に関する回答を得ること。
・請負者は、ヒアリング調査を実施し、ヒアリング調査結果を取り纏めた資料を作成すること。

【ヒアリング方法】

被害企業に対し被害内容や根本的な問題点等を伺うことは嫌がれることが多い。しかしながら本質的な対策を検討するためには、深く真実を伺う必要がある。そのため、ヒアリング方法の原則は以下の通りとする。

・訪問によるヒアリングの方がより多く深く情報を伺える可能性が高いため、ヒアリングは基本訪問とする。その際、新型コロナウイルス対策を十分に配慮すること。
・請負者が訪問でのヒアリングを望む旨の理由を添えたうえでもヒアリング対象組織がオンラインでのヒアリングを望む場合はオンラインでのヒアリングも可とする。
・ヒアリング時間は基本 1 時間とすること。

(2)　ヒアリング結果の分析

3.2.1(1)の調査結果を元に EC サイトが受けた攻撃による被害の状況や原因や考えられる対策等、また EC 構築事業者や ASP 事業者からの側面で運用・保守契約の締結状況や構築時も含めたセキュリティ観点での契約の記載状況を分析し取り纏め、調査報告書に記載するともに EC サイトセキュリティ対策ガイドラインにも結果を盛り込むこと。

3.2.2.　EC サイトのセキュリティ対策状況調査

パッケージ、OSS 等を使用し構築された中小企業等の EC サイトに対して、EC サイト運営者自身によるセルフチェックや専門家による脆弱性診断を実施することにより、現在の EC サイトのセキュリティ対策状況を把握し、脆弱性診断結果の報告及び対策の助言を実施する。

(1)　調査全体

【対象と件数】

・セキュリティ対策状況調査の対象は中小企業が運営する EC サイトで、オンプレミス環境や AWS 等の IaaS・PaaS（リモートからの脆弱性診断が許されるサイト）上の自社構築サイト。
・対策状況調査対象に関しては以下の HP で募集し、IPA が提示する。なお IPA から提示するセキュリティ対策状況調査対象企業は事前に対策状況調査の了承を得ている企業である。
https://www.ipa.go.jp/security/vuln/ec-site/vuln-ec-site2022.html
・調査対象 EC サイト：最小 20 サイト以上、最大 30 サイト
・上記調査対象 EC サイトを対象に 3.2.2(2)～3.2.2(5)および 3.2.2(7)を実施する。
・調査対象 EC サイト数に関しては契約締結以降、かつ、請負者が作業に必要なリソースを開始必要となる前に決定する。

(2)　セルフチェック調査

【セルフチェック項目例】

項目例を以下に示す。請負者はこの内容を元に改めて整理し、IPA の承認のもと確定させること。

・EC サイト全般のセキュリティ対策内容
・EC サイトの構築や運用におけるセキュリティの契約事項
・サイト構築時のセキュリティ対策状況（公開時の脆弱性診断も含む）

・運用段階での対策状況（運用環境「ステージングの有無等」、情報収集、脆弱性パッチ、インシデント体制）

【調査方法】

・請負者はセルフチェック調査に向け事前に「セルフチェック主旨説明及びセルフチェック項目」資料を作成し IPA からの承認を得ること。「セルフチェック主旨説明及びセルフチェック項目」には、セルフチェック主旨説明文、セルフチェック概要（件名、主な内容、注意事項、回収日、問合せ先など）、セルフチェック内容を記載すること。

・請負者はセルフチェック調査後のヒアリング調査に向け事前に「ヒアリング主旨説明」資料を作成し IPA からの承認を得ること。「ヒアリング主旨説明」資料には、ヒアリング主旨説明文、ヒアリング概要（件名、主な内容、実施日、実施場所、訪問者、問合せ等）、ヒアリング調査詳細項目を記載すること。

・請負者はセキュリティ対策状況調査対象組織に対し、以下を送付すると共にセルフチェックを依頼し、併せてヒアリングのアポイントも取ること。

- 「セルフチェック主旨説明及びセルフチェック項目」資料
- 「ヒアリング主旨説明」資料
- ヒアリングでの確認のため診断対象情報（IP アドレス・ネットワーク構成図等）提供依頼書

・請負者は、ヒアリング前までにセルフチェック結果を対策状況調査対象組織から回収のうえ分析し不明点や理解を深める点を事前に取り纏めヒアリングを充実させること。

(3) ヒアリング調査

セルフチェックで確認した以下の内容を深堀し、新たな情報を引き出すこと。また追加の項目例を以下に記すが請負者はこの内容を元に改めて整理し、IPA の承認のもと確定させること。

【ヒアリング項目例】

・EC サイト全般のセキュリティ対策内容
・EC サイトの構築や運用におけるセキュリティの契約事項
・サイト構築時（公開時のセキュリティ診断も含む）の対策状況
・運用段階での対策状況（運用環境（ステージングの有無等）、脆弱性情報収集、脆弱性パッチの適用、インシデント体制）
・契約内容に関して、セキュリティ対策に関する事項が含まれていない、または不足している場合は、含まれていないまたは、不足した理由を確認すること。
・契約に関する内容に、セキュリティ対策を含める事は可能であったか、委託先との契約においては含める事が不可能であったかを確認すること。

【ヒアリング方法】

・訪問によるヒアリングの方がより多くかつ深く診断対象情報を含めた情報を伺える可能性が高いため、ヒアリングは基本訪問とする。その際新型コロナウイルス対策を十分に配慮すること。
・請負者が訪問でのヒアリングを望む旨の理由を添えたうえでもセキュリティ対策状況調査対象組織がオンラインでのヒアリングを望む場合に関してはオンラインでのヒアリングも可とする。
・ヒアリング時間は基本 1 時間とすること。
・セルフチェックでの内容も併せて深掘りし、新たな情報を引き出すこと。

(4) 脆弱性診断

【脆弱性診断の実施方法】

・事前に受け取っている診断対象情報をもとにした脆弱性診断実施に関する確認・決定をすること。

- ネットワーク診断（診断対象となるネットワーク、診断対象 IP 数、禁止事項の確認）
- ウェブアプリケーション診断（指定のウェブサイトに対する事前確認、事前確認結果から診断対象範囲の決定）

・脆弱性診断は、ネットワーク診断とウェブアプリケーション診断の両方を実施すること。
・ウェブアプリケーション診断の対象画面は、10 画面を対象とすること。
・各脆弱性診断において実施する項目については、IPA の承認を得て決定すること。
・検査対象プラットフォーム （例） Linux, Apatch、EC-Cube, My SQL 等を対象とする。
・ネットワーク診断は、リモートから公開サーバに対して診断を行うこと。
・ウェブアプリケーション診断は、公開している動作中のサイトに対して行うこと。

・診断実施時の免責事項については、申込時に IPA が承諾を得る。

【脆弱性診断実施内容】
・ネットワーク診断内容
- ネットワーク調査（TCP･UDP･サービススキャン、OS 推測、ホスト名調査）、各種サービスの脆弱性スキャン、FTP 調査、SSH 調査、TELNET 調査、SMTP 調査、POP 調査、DNS 調査、HTTP/HTTPS 調査、SNMP 調査、NTP 調査、バックドア調査（ポートスキャン）

・ウェブアプリケーション診断内容
－「OWASPTOP10」に掲載の項目
SQL インジェクション、NoSQL インジェクション、OS コマンド・インジェクション、LDAP インジェクション、認証の不備、機微な情報の露出、XML 外部エンティティ参照(XXE)、アクセス制御の不備、不適切なセキュリティ設定、クロスサイト・スクリプティング(XSS)、安全でないデシリアライゼーション、既知の脆弱性のあるコンポーネントの使用等

－「安全なウェブサイトの作り方」の「セキュリティ実装 チェックリスト」に掲載の項目
SQL インジェクション、OS コマンド・インジェクション、パス名パラメータの未チェック／ディレクトリ・トラバーサル、セッション管理の不備、クロスサイト・スクリプティング、CSRF（クロスサイト・リクエスト・フォージェリ）、HTTP ヘッダ・インジェクション、メールヘッダ・インジェクション、クリックジャッキング、バッファオーバーフロー、アクセス制御や認可制御の欠落等

－「OWASP アプリケーションセキュリティ検証標準 4.0」に掲載の項目
認証の検証要件、セッション管理の検証要件、アクセス制御検証要件、バリデーション、無害化とエンコーディング検証要件、保存時の暗号化の検証要件、データ保護の要件、通信の検証要件、悪性コードの検証要件、ビジネスロジックの検証要件、ファイルとリソースの検証要件、API、Web サービスの検証要件、構成の検証要件等
※上記記載の各要件に含まれている項目で、レベル 1、レベル 2、レベル 3 の全てがチェックされている項目を想定

－ その他の項目
最近の EC サイトへのサイバー攻撃事例を把握し、極力それらへの対策がなされているかを確認すること。また、脆弱性が存在していた場合、その脆弱性が悪用できるかについて可能な範囲で確認をすること。

ネットワーク診断、ウェブアプリケーション診断の診断実施内容について、診断対象の個々のウェブサイトの状況等により、変更が発生する可能性がある。請負者は、診断対象の全 EC サイトに関して、事前に診断実施内容の一覧を作成し、IPA の承認を受けること。また、契約締結時点での計画した診断内容と、実際の診断内容との差分を把握する為、提案内容に契約締結時点で計画する診断内容の内訳を示すこと。

(5) 脆弱性診断結果の報告及び対策の助言
対策状況調査対象組織に対して脆弱性診断をした結果について報告すると共に対策の助言について、訪問もしくはオンラインで実施すること（基本 1 時間）。

(6) EC サイトの対策状況の分析
3.2.2(2)～3.2.2(5)の調査結果を元に分析し取り纏め、調査報告書に記載するともに EC サイトセキュリティ対策ガイドラインにも結果を盛り込むこと。

(7) 脆弱性診断後の対策状況の確認
対策状況調査対象組織に対して脆弱性診断から 3 カ月後を目安に、脆弱性診断で検出された問題の対策状況や対策予定をメールで確認すること。

3.2.3. EC サイトセキュリティ対策ガイドラインの作成

3.2.1 や 3.2.2 で得られた教訓、および、中小企業等が EC サイトを構築する際に技術・運用・契約面で考慮すべき事項等を、EC サイトセキュリティ対策ガイドラインとしてまとめること。ガイドライン作成にあたっては中小企業等の経営者も読者であることを配慮すること。

(1) ガイドラインの作成

【作成内容】

・形状としては、A4 サイズ縦、Microsoft Word で作成すること。

・EC 業界において既に公開されている各種ガイドライン等の資料との整合性を考慮して作成すること。

・3.2.1、3.2.2 のヒアリングで得た結果（生の声、具体事例、グッドプラクティス等、ASP サービスへの移行等のメリット／デメリット等）を最大限に取り込み、中小企業等の経営者に響く内容とすること。

・EC サイトセキュリティ対策ガイドライン骨子案を以下に示す。

以下目次をベースラインとし、ヒアリング、脆弱性診断の結果を基に、効果的な業界レベルへの対策に資するよう改良を図ること。

第一部　EC サイトにおけるセキュリティ対策

① はじめに

② EC サイトが狙われている（EC サイト攻撃からの被害事例、調査結果を踏まえて）

③ なにが問題なのか（EC サイトの脆弱な点、調査結果を踏まえて）

④ 攻撃に対しどのように向き合うべきか（対策に対する指針）

⑤ 対策をしないと何が起きるのか？（サイトおよび事業停止、お客様への迷惑）

第二部　EC サイト構築の各フェーズにおける対策

① 具体的な対策

（ア）組織的な対策

（イ）サイト計画時における対策

（ウ）サイト構築時における対策

（エ）サイト公開時における対策

（オ）サイト運用時における対策

※自社による EC サイト構築と、ショッピング ASP カートによる EC サイト構築の両方式におけるのメリット・デメリットを定量的に記載すること。

② EC サイト開発時・運用時における外部発注契約上の注意事項

契約に係る問題点、契約のあり方、注意事項

③その他

実際に被害にあった際の対応、対策

現在の自組織のセキュリティ状況確認のチェックリスト

参考資料

---

(2) 内容の妥当性確認

作成した EC サイトセキュリティ対策ガイドラインの内容の妥当性を確認するため、EC サイトやそのセキュリティに精通する委員による委員会で意見を聴取した内容を EC サイトセキュリティ対策ガイドラインに反映し、現実も考慮された実用的なものとし品質を高めること。

(3) ガイドラインの作成に当たって遵守すること

3.2.5.(3)に沿うこと。

3.2.4. 委員会の運営支援作業

IPA が主催する委員会における IPA 事務局支援作業を以下の内容に基づいて行う。委員会は、IPA が選定する有識者、専門家等 4～5 名程度で構成し、1 回当たり約 2 時間、3 回以上開催する。なお、委員会はリモート形式での開催を想定しているが、実施形式については開催の都度 IPA との協議の上決定するものとする。

	開催時期	議題（案）
第 1 回	2022 年 7 月頃	ガイドラインの概要の説明、対応方針の確認
第 2 回	2022 年 9 月頃	制作中ガイドラインの説明、チラシの作成に関する意見聴取
第 3 回	2022 年 11 月頃	制作中ガイドラインの説明、チラシの作成に関する意見聴取
第 4 回	2022 年 12 月頃	最終段階のガイドラインの説明、効果的な普及啓発ルート・方法に関する意見聴取

請負者は第 1 回の委員会にて項目 3.2.1～3.2.2 の調査を実施している旨について説明するための説明資

料を作成して説明する。また作成する EC サイトセキュリティ対策ガイドラインに関しての概要について説明し、委員からあがった意見を踏まえ EC サイトセキュリティ対策ガイドラインの作成にあたる。

請負者は各委員会前後に、IPA 事務局会合（IPA 及び請負者等が参加）を 1 回当たり約 2 時間、計 6 回以上、リモート形式もしくは集合形式で行うものとする。集合形式の場合は、新型コロナウイルス対策を行った上で IPA 会議室において行うものとする。

委員会委員に対する委嘱手続き、謝金・交通費等の支払いは IPA が行う。

委員会を集合形式で行う場合は、新型コロナウイルス対策を行った上で基本 IPA の会議室で実施し、飲み物の費用は IPA が負担する。委員の都合により外部会議室を利用しても良い。その費用の支払いは、請負者が負担すること。

請負者は以下の作業を行う。

1. 委員会日程調整
   委員会開催に向け、IPA 事務局や IPA 会議室も含め委員会委員との日程調整を行う。具体的な日程は IPA と協議の上、決定する。
2. 委員会での議論を進めるための資料作成
   上記表の議題（案）に関する資料や委員会で議論するための論点等を纏めた資料を作成し、各回の委員会開催の 2 週間前までに完成版を IPA に提出すること。
3. リモート形式での開催のための準備とサポート
   リモート会議ツールを IPA と協議し決定した上で委員会の開催準備を行うとともに、リモート形式の会議がスムーズに進行するように委員会出席者へのサポート等を行うこと。また、リモート会議ツールは、請負者が準備すること。
4. 議事進行表の作成
   委員会の議事運営がスムーズに進行できるよう、委員会事務局向けの資料として、議事進行表を作成し、各回の委員会開催の 2 週間前までに完成版を IPA に提出すること。
5. 議事録作成
   1 枚に纏めた要約版と発言の詳細版を各回の委員会開催後 3 営業日以内に IPA に提出すること。

3.2.5. 調査実施報告書等の作成

3.2.1～3.2.3 の調査結果について取り纏め調査実施報告書を作成すること。また 3.2.3 にて作成した EC サイトセキュリティ対策ガイドラインに関する紹介チラシも作成すること。

(1) 調査実施報告書の作成

本事業に関する調査内容・調査経緯に関して全情報を報告書としてまとめること。

【調査実施報告書内容】

以下に調査実施報告書の内容に関する内容例を示す。IPA と協議のうえで作成すること。

- ・各事業工程にて調査した内容
- ・被害企業を対象とした専門家によるヒアリング内容と結果
- ・EC サイトの脆弱性診断内容と結果
- ・汎用的なリストによるセルフチェック内容と結果
- ・専門家によるヒアリング内容と結果
- ・専門家による脆弱性診断内容と結果
- ・対策ガイドラインの概要・普及方法

(2) 紹介チラシの作成

EC サイトセキュリティの重要性等の概要を含め、EC サイトセキュリティ対策ガイドラインにその対処方法が記載されている旨の配布用チラシ原文を作成すること。

【作成方法】

- ・形状としては、A4 サイズ縦、裏表の 2 ページ
- ・作成ソフト（フォーマット）は IPA と協議のうえ決めること。

【作成内容】

- ・セキュリティ対策の必要性を経営者が認識することを目的とし、経営者の心に響く説得力のある内容とすること。
- ・例えば、表は経営者向け、裏は管理者向けもしくは、冗長を省いて表裏で一連の説明とする等、効果的内容とすること。

(3) 調査実施報告書の作成に当たって遵守すること

- 日本語で作成すること(ただし、固有名詞や文献参照等に外国語表記を用いることは可能。ただし、その場合は日本語での解説も併記すること)。
- アルファベット等の略語については初出箇所のページ下部に脚注を挿入し、説明すること。
- 誤記・誤植を含まないこと。
- 図表を用い、理解し易いよう配慮の上、体系的に整理された記述にすること。
- 文章や図、写真等を引用する際には、引用部分それぞれにおいて出典元を明記すること。
- IPA からの依頼(説明の追記や、独自の図表作成)を反映すること。
- 予め記述項目、記載内容及び記載水準に対して IPA の合意を得ること。
- IPA に帰属できない他者の著作物は除くこと。
- 目次を作成すること。
- 五十音順・アルファベット順の用語集、略語集を含めること。
- 一般公開に資する内容とし、図表を用いた分かりやすい記述とすること。

3.2.6. 全体スケジュール

参考として、全体のスケジュール(案)を以下に記載するが、請負者にて詳細なスケジュールを提案すること。

	2022年								2023年	
	～5月	6月	7月	8月	9月	10月	11月	12月	1月	2月
被害企業の被害実態調査	準備	1次募集	ヒアリング	2次募集	ヒアリング	ヒアリング結果纏め				
セキュリティ対策状況調査	選定・通知	セルフチェック	ヒアリング	診断	診断	診断	診断結果纏め			
ガイド・普及啓発・調査報告書										
委員会			第1回		第2回		第3回	第4回		
納品										

4. 事業の実施体制

4.1. 実施体制に関する要件

本調査を実施するにあたっては、次の業務実施体制を整えること。

(1) 事業の実施体制及び役割を、事業実施内容と整合させること。
(2) 要員数、体制、役割分担を明確にすること。
(3) IPA との円滑なコミュニケーションと遅滞なきプロジェクト管理を図るために、プロジェクトマネージャ(正・副)を設置した管理体制とすること。
(4) 実施担当者は、情報セキュリティに関する知識を有した調査経験者で構成すること。
(5) 4.2.1.(2)及び 4.2.2.(2)の要件を全て満たす担当者を、少なくとも 3 名は実施担当者に入れること。
(6) 業務の役割を定めた実働可能な人数を確保すること。
(7) 組織として適切な管理・バックアップ体制を整えること。
(8) 作成するドキュメント類が正確かつ明確に記述されるよう、請負者内での事前レビュー体制を万全のものとすること。この体制により、用語・用法の不統一、誤字脱字、論理的矛盾等、調査の本質に直接関わりのない修正については、請負者の責任において IPA への納入前に修正すること。
(9) 3.2.1～3.2.2 のヒアリング時の臨場感がガイドラインの作成担当者へ正しく伝わるよう、十分なコミュニケーションが取れる体制とすること。

4.2. 実績及びスキルに関する要件

4.2.1. 3.2.1～3.2.5 の実施するにあたっては、次の実績及びスキル要件を満たすこと。

(1) 法人としての実績
- 本業務に関係する産学官の有識者へのコネクションを有していること。
- 過去に脆弱性や脆弱性情報の公表および情報セキュリティに関する調査の実施があること。
- 過去に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があること。
- 過去に企業におけるセキュリティに関する実態調査(インタビュー調査等)を実施した経験があること。
- 過去にセキュリティ人材(CISO 等を含む)の役割や育成を扱った検討会等で活動した経験があること。

(2) 担当者としての実績及びスキル
- 脆弱性および情報セキュリティに関する専門的知識を有し、過去に脆弱性および情報セキュリティに関する調査を少なくとも 3 回行った実績があること。
- 過去に制度の策定や改善に関する委員会を少なくとも 3 回運営した実績があること。
- 過去に政府機関において情報セキュリティ政策の立案・遂行の担当をした経験があること。
- 調査内容(脆弱性や情報セキュリティ)に関する人的ネットワークを有していること。
- 調査内容(脆弱性や情報セキュリティ)に関する専門的知識・知見に基づいたデータ分析及びレポーティング能力を有していること。

4.2.2. 3.2.3 の実施するにあたっては、次の実績及びスキル要件を満たすこと。

(1) 法人としての実績
- 過去に脆弱性や脆弱性情報の公表および情報セキュリティに関する調査の実施があること。
- 過去に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があること。
- 過去に企業におけるセキュリティに関する実態調査(インタビュー調査等)を実施した経験があること。
- ネットワーク診断、ウェブアプリケーション診断をサービスとして提供していること。
- 情報セキュリティサービス基準適合サービスリストに登録されていることが望ましい。

(2) 担当者としての実績及びスキル
- 脆弱性および情報セキュリティに関する専門的知識を有し、過去に脆弱性および情報セキュリティに関する調査を少なくとも 3 回行った実績があること。
- 調査内容(脆弱性や情報セキュリティ)に関する専門的知識・知見に基づいたデータ分析及びレポーティング能力を有していること。
- ネットワーク診断、ウェブアプリケーション診断に関する専門的知識・経験を有し、過去にネットワーク診断、ウェブアプリケーション診断を実施した実績があること。

5. 調査に関する留意事項
- 以下の作業の打合せには国内出張が伴うことが予定される。契約締結時点での国内出張の予定比率を以下に示す。なお、請負者および IPA 双方の協議の結果、実際に発生する国内出張旅費が本比率と大幅に乖離した場合には、国内出張旅費に関する実費精算も可能とする。
  - ・3.2.1(1)① :40%
  - ・3.2.1(1)② :30%
  - ・3.2.1(1)③ :20%
  - ・3.2.2(3) :30%
  - ・3.2.2(5) :30%

  (注)国内出張の定義:出張の起点駅から 100 キロメートル以上の地域、又は宿泊を伴う出張
- 契約後直ちにキックオフミーティングを開催し、全体的な計画を提示し、IPA と意識をすり合わせ、調査を開始すること。
- 調査を効率的に進めるため、調査の手法・方法を工夫すること。
- プロジェクト管理により、作業計画を明確に定め、作業項目ごとの工程管理を行うこと。
- 2 週間に一回は、ミーティングにおいて、各調査に関する進捗状況の報告を行い、作業の遅延等が生じた場合にはその対策案を IPA 担当者に報告するとともに、リカバリーに努めること。ミーティングの資料は、ミーティング開催日の 3 営業日前までに、IPA に送付すること。なお、IPA と協議のうえ、ミーティングを実施しない週があるとしても、各調査に関する進捗状況の報告はメールで実施すること。
- 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こと。
- 各ミーティングの形式はリモート形式を主とするが、必要に応じて集合形式でも行うものとする。集合形

式で行う場合は、新型コロナウイルス対策を行った上で実施するものとする。
- 各調査項目について、調査状況を定期的に IPA へ報告すること。
- IPA からの調査に関する報告要求があった際には、速やかに対応すること。
- IPA との打合せ等で必要となる全ての会話は日本語を用いること。
- 各ヒアリングは、ヒアリング先にて 1 時間程度のものとし、IPA も同行するので IPA を含めヒアリング先との日程調整をすること。
- ヒアリングを進めるための資料として、ヒアリングの主旨やヒアリング項目などを記載した「ヒアリング対象者向け主旨説明」「ヒアリング実施概要」と、必要に応じてヒアリングを効率的に実施するための資料を用意しヒアリング先に持参する。これらの資料はヒアリング開催 1 週間前迄に IPA に提出し了承をとること。
- ヒアリング先でのヒアリングにあたっては、ヒアリング先でのコロナウイルス対策に応じた対策を採った上で臨むこと。
- ヒアリング実施にあたっては、あらかじめヒアリング相手に対しヒアリング内容の取扱い方法など注意事項を説明すること。
- ヒアリング後、議事録として 1 枚にまとめた要約版と発言の詳細版を、ヒアリング実施後 3 営業日以内に IPA に提出すること。ただし、諸般の事情により 3 営業日以内の共有が困難になる場合は、事前に IPA に許可を取って対応すること。
- 脆弱性診断後、診断結果を脆弱性診断実施後 20 営業日以内に IPA に提出すること。ただし、諸般の事情により 20 営業日以内の共有が困難になる場合は、事前に IPA に許可を取って対応すること。
- 対策状況調査対象組織の対策状況または対策予定については、定期的に回答状況を IPA に報告すること。
- 仕様書に定めのない事項等については、IPA と請負者が協議の上、決定すること。

6. セキュリティに関する要件

(1) 請負者は本調査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、当機構に対し「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、住所、生年月日、所属部署、役職等が記載されたもの）を契約前に提出し、同意を得ること。（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、本調査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。また、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、予め当機構へ届出を行い同意を得ること。

（確保すべき履行体制）

契約を履行する一環として請負者が収集、整理、作成等した一切の情報が、当機構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

当機構が個別に承認した場合を除き、情報取扱者以外の者に対して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

(2) 請負者は請負者の資本関係・役員等の情報、本調査の実施場所、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、資格（情報セキュリティに係る資格等）、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) 本調査の過程で得た一切の情報（ヒアリング内容、会議内容等）は、当機構の許可なく情報取扱者以外の者に開示又は漏えいしないものとし、他に利用しないこと。

(4) 請負者は秘密情報や個人情報の取り扱いに留意し適切に管理を行うこと。また、情報漏えい防止対策や情報の暗号化、脆弱性への対応等適切に情報セキュリティ対策を実施すること。さらに、本調査の一部業務を再委託する場合、請負者は再委託先が十分な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。

(5) 情報セキュリティインシデントが発生した場合、ただちに当機構に報告し当機構の指示に基づき適切に対応すること。

(6) 保護すべき情報はパスワードの設定等、安全な方法で受け渡しをすること。また、契約中／契約終了後の如何に依らず、一時的に当機構から提示する未公開情報や個人情報等は、不要になった段階で適切に削除するとともに、当機構に確認を取ること。

(7) 請負者の情報セキュリティ対策の履行状況を確認する必要が生じた場合、対応すること。

(8) 情報セキュリティ対策が不十分であることが判明した場合、当機構と調整し、適切に対処すること。

7. 納入関連

7.1. 納入期限・納入場所

2023 年 2 月 17 日(金)
〒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 16 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 セキュリティ対策推進部 脆弱性対策グループ

7.2. 納入物件

以下の報告書を収めた、電子媒体(CD-R 等)を納入すること。
(1) EC サイトセキュリティ対策ガイドライン
(2) 調査実施報告書
(3) 紹介チラシ

以上の納入物件に併せて、調査の過程で入手したデータ、文献、資料、委員会の議事録、ヒアリング記録、脆弱性診断結果、結果報告書も提出すること。

検収のため、上記(1)～(3)に記載した納入物件については、バインダーに収納した印刷物を 1 部提出すること。

7.3. 検収条件

納入物件の内容に関しては、調査内容及び対象に関して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。

以上

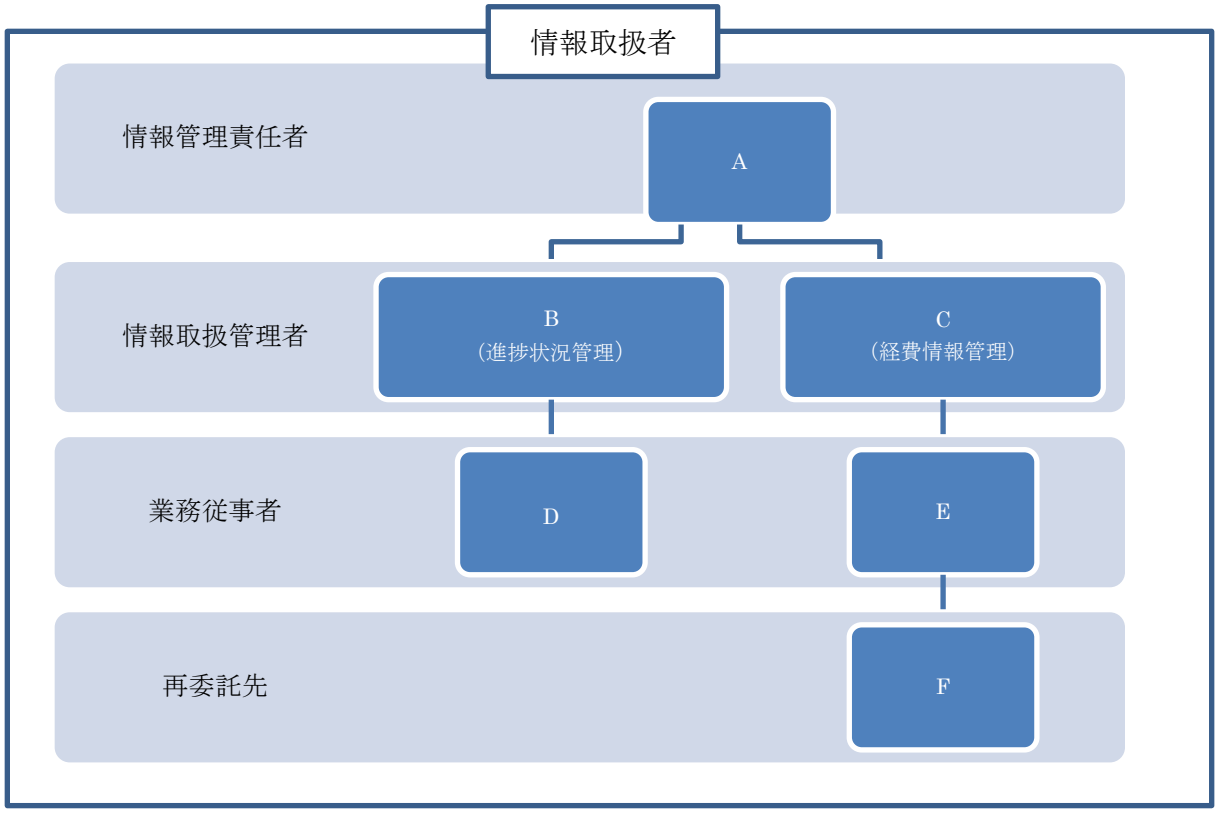
情報取扱者名簿

		(しめい) 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 (※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						

(※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) 本調査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、本調査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) 本調査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。

情報管理体制図（例）



【情報管理体制図に記載すべき事項】

- 本調査の遂行にあたって保護すべき情報を取り扱う全ての者。（再委託先も含む。）
- 本調査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。

「ECサイトセキュリティ対策のための調査業務」

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、「ECサイトセキュリティ対策のための調査業務」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「ECサイトセキュリティ対策のための調査業務」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	「ECサイトセキュリティ対策のための調査業務」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○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	調査業務の実施方針等	目標設定、実施作業内容、実施スケジュール及び事業の実現性等。 仕様書の実施方法の他に、より適切な方法など事業の効果・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	本事業実施の、体制、環境及び類似事業の実績、業務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 Office2013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。

「ECサイトセキュリティ対策のための調査業務」

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	調査実施報告書等は日本語で作成し、図表等は本文中に挿入すること（ただし、固有名詞や文献参照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「4.事業の実施体制」に記載している実施要員に関する要件を満たすこと。	
	0.4 スケジュール	作業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　調査業務の実施方針等								
	1.1 調査内容の妥当性		・仕様書の調査内容について、全て記載されているか。	必須	10	－	10	
	1.2 調査方法の妥当性	1.2.1 EC サイトへのサイバー攻撃による被害企業の被害実態調査	・仕様書 3.2.1（1）【対象と件数】に記載のヒアリング調査を実施することになっているか。	必須	5	－	35	
			・上記のヒアリング先について、名称、選定理由、基準などが記載されており、客観的な根拠や妥当性が、示されているか。	任意		5		
			・仕様書 3.2.1（1）ヒアリング先選定にあたっての具体的な手順が記載されているか。また、【ヒアリング項目例】に記載の項目についてヒアリングすることになっているか。	必須	5	－		
			・上記のヒアリング項目の他、有効となる項目が提案されているか。	任意	－	5		
			・仕様書 3.2.1（1）に記載のヒアリング調査を実施するにあたって、具体的な調査方法、提案が記載されているか。	任意	－	5		
			・仕様書 3.2.1（1）に記載のヒアリング調査を効率的に進めるための工夫が記載されており、それが妥当である事が客観的な根拠とともに説明されているか。	任意	－	5		
			・仕様書 3.2.1(2)に記載のヒアリング調査結果の分析にあたって、その整理/分析の仕方が、提案されており、それについての根拠が説明されているか。	任意	－	5		

		1.2.2 EC サイトのセキュリティ対策状況調査	・仕様書 3.2.2（1）【対象と件数】に記載の調査を実施することになっているか。	必須	5	－	165	
			・仕様書 3.2.2（1）【対象と件数】に記載の調査について、具体的な調査方法、提案が記載されているか。	任意	－	5		
			・仕様書 3.2.2(2)【セルフチェック項目例】に記載の項目についてチェックすることになっているか。	必須	5	－		
			・仕様書 3.2.2（2）に記載のセルフチェック調査結果の分析にあたって、その整理/分析の仕方が、提案されており、それについての根拠が説明されているか。	任意	－	5		
			・仕様書 3.2.2（2）に記載のセルフチェック調査結果を実施するにあたって、具体的な調査方法、提案が記載されているか。	任意	－	5		
			・仕様書 3.2.2（2）に記載のセルフチェック調査を効率的に進めるための工夫が記載されており、それが妥当である事が客観的な根拠とともに説明されているか。	任意	－	5		
			・仕様書 3.2.2(3)【ヒアリング項目例】に記載の項目についてチェックすることになっているか。	必須	5	－		
			・仕様書 3.2.2（3）に記載のヒアリング調査結果の分析にあたって、その整理/分析の仕方が、提案されており、それについての根拠が説明されているか。	任意	－	5		
			・仕様書 3.2.2（3）に記載のヒアリング調査結果を実施するにあたって、具体的な調査方法、提案が記載されているか。	任意	－	5		
			・仕様書 3.2.2（3）に記載のヒアリング調査を効率的に進めるための工夫が記載されており、それが妥当である事が客観的な根拠とと	任意	－	5		

			もに説明されているか。				
			・仕様書 3.2.2(4)【脆弱性診断の実施方法】に記載の調査を実施することになっているか。	必須	5	-	
			・上記の脆弱性診断内容の他、最近の EC サイトの被害で多く使用されている攻撃手法及び対応する脆弱性が診断内容として提案されているか。	任意	-	20	
			・仕様書 3.2.2（4）に記載の脆弱性診断の実施にあたって、具体的な診断実施方法（仕様ツール等）、提案が記載されているか。	任意	-	20	
			・仕様書 3.2.2（4）に記載の脆弱性診断の実施にあたって、存在していた脆弱性が悪用できるかについての確認するための手動等による調査手順が記載されているか。	任意	-	20	
			・仕様書 3.2.2（4）に記載の脆弱性診断の実施を効率的に進めるための工夫が記載されており、それが妥当である事が客観的な根拠とともに説明されているか。	任意	-	20	
			・仕様書 3.2.2(5)に記載の診断結果の報告及び対策の助言について実施することになっているか。	必須	5	-	
			・仕様書 3.2.2(5)に記載の診断結果の報告及び、対策の助言について、効率的に進めるための工夫が記載されているか。	任意	-	5	
			・仕様書 3.2.2(6)に記載の対策状況の分析について実施することになっているか。	必須	5	-	
			・仕様書 3.2.2(6)に記載の対策状況の分析について、効率的に進めるための工夫が記載されており、それが妥当である事が客観的な根拠とともに説明されているか。	任意	-	5	

			・仕様書 3.2.2 (7) に記載の対策状況の確認について実施することになっているか。	必須	5	－		
			・仕様書 3.2.2(7)に記載の対策状況の確認について、具体的な調査方法、提案が記載されているか。	任意	－	5		
		1.2.3 EC サイトセキュリティ対策ガイドラインの作成	・仕様書 3.2.3 に記載されたガイドラインの作成作業の作業内容について、すべて記載されているか。	必須	5	－	55	
			・仕様書 3.2.3(1)の自社による EC サイト構築と、ショッピング ASP カートの定量的比較作成する具体的手順が記載されているか。	任意	－	20		
			・仕様書 3.2.3 に記載されたガイドラインの作成内容について、想定している読者である中小企業の経営者に有益となる内容とするため記載内容が提案されているか。	任意	－	20		
			・仕様書 3.2.3 に記載のガイドライン作成作業について具体的な作成方法、提案が記載されているか。	任意	－	5		
			・仕様書 3.2.3 に記載のガイドライン作成作業を効率的に進めるための工夫が記載されており、それが妥当である事が客観的な根拠とともに説明されているか。	任意	－	5		
		1.2.4 委員会の運営支援作業	・仕様書 3.2.4 に記載された支援作業事項の内容について、全て記載されているか。	必須	5	－	10	
			・運営支援作業や委員会の進行について、独自の知見や経験に基づきどのような方法で実施するのが効果的か提案されているか。	任意	－	5		
		1.2.5 調査実施報告書等の作成	・仕様書 3.2.5 に記載された報告書等を全て作成することになっているか。	必須	5	－	15	
			・仕様書 3.2.5 に記載の支援作業を効率的に進めるための工夫が記載されており、それが妥当である事が客観的	任意	－	5		

		な根拠とともに説明されているか。					
		・調査実施報告書の作成指針について提案がなされており、それが有効であることが説明されているか。	任意	－	5		
	1.3 作業計画の妥当性、効率性	・調査の手法、日程等に無理がなく、目的に沿った実現性はあるか。 ・全体作業スケジュールが具体的に提案されているか。	必須	5	－	10	
		・調査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	－	5		
2　組織の経験・能力							
	2.1 調査実施能力	・業務の役割を定めた実動可能な人数が確保されているか。 ・組織として適切な管理・バックアップ体制となっているか。 ・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	5	－	50	
		・プロジェクトマネージャ(正・副)を設置した管理体制となっているか。	必須	5	－		
		・ドキュメント類が正確かつ明確に記述されるよう、請負者内での事前レビュー体制は万全なものとなっているか。	必須	5	－		
		・実施担当者は、情報セキュリティに関する知識を有した調査経験者で構成されているか。	必須	5	－		
		・仕様書 4.2.1(2)に記載されている担当者の要件を全て満たす者が、少なくとも 3 名は実施体制に含まれているか。	必須	5	－		
		・仕様書 4.2.2(2)に記載されている担当者の要件を全て満たす者が、少なくとも 3 名は実施体制に含まれているか。	必須	5	－		

		・仕様書 4.2.2(1)に記載されている、情報セキュリティサービス基準適合サービスリストに登録されているか。（脆弱性診断を再委託先が行う場合にはその企業名（複数でも可）を記載すること。	任意		20		
	2.2 類似業務の経験	・本業務に関係する産学官の有識者へのコネクションを有しているか。	必須	5	－	25	
		・過去に企業におけるセキュリティに関する実態調査（インタビュー調査等）を実施した経験があること。	必須	5	－		
		・ 過去にセキュリティ人材（CISO 等を含む）の役割や育成を扱った検討会等で活動した経験があること。	必須	5	－		
		・過去に組織として、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。	必須	5	－		
		・過去に脆弱性や脆弱性情報の公表および情報セキュリティに関する調査の実績があるか。	必須	5	－		
3　業務従事者の経験・能力							
	3.1 類似調査業務の経験	・担当者は、脆弱性および情報セキュリティに関する専門知識を有し、過去に脆弱性及び情報セキュリティに関する調査を少なくとも 3 回行った経験はあるか。	必須	5	－	40	
		・担当者は、過去に制度の策定や改善に関する研究会を少なくとも 3 回運営した経験はあるか。	必須	5	－		
		・担当者は、調査内容（脆弱性や情報セキュリティ）に関する人的ネットワークを有しているか。	必須	5	－		
		・過去に政府機関において、情報セキュリティ政策の立案・遂行の担当をした経験は含まれているか。	必須	5	－		
		3.2.1(1)①②③および 3.2.2(3)(5)を実際に行う担当者の経歴が記載	任意		20		

		され、本業務実施に十分なスキルを持つことが説明されているか。					
	3.2 調査内容に関する専門知識・適格性	・担当者は、調査内容（脆弱性や情報セキュリティ）に関する専門的知識・知見に基づいたデータ分析及びレポーティング能力を有しているか。	必須	5	－	50	
		・脆弱性情報の取扱いおよび情報セキュリティに関する専門知識・知見を持っていることが説明されているか。	必須	5	－		
		・脆弱性診断に関わる担当者は過去にウェブサイトの脆弱性診断を実施した実績を持つことが説明されているか。（実績件数等を記載すること）	任意	－	20		
		・実施要員に、以下に該当する者のいずれかが含まれるか。 - 情報処理安全確保支援士の登録を受けている者もしくは情報処理安全確保支援士試験に合格した者もしくは情報処理安全確保支援士の試験と同等レベルの試験の合格者 - CISSP、CISA あるいは相当の資格を有する者	任意	－	20		
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	－	15	15	

160	320	480

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 実施体制及び担当者略歴	・入札者の概要の分かる資料	任意	
		・本調査履行のための体制図	任意	
		・各業務従事者の経歴（氏名、所属、役職、学歴、職歴、業務経験、研修実績その他経の経歴、資格（情報セキュリティに係る資格等）、母語及び外国語能力、国籍等がわかる資料）	必須	
		・受託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「情報取扱者名簿」を契約時に提出できることを確約する。（仕様書中に提示）	必須	
	5.2 会社としての実績	・本調査の類似案件実績	任意	
		・本調査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、調査実施における前提条件等	任意	

「ECサイトセキュリティ対策のための調査業務」

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、「ECサイトセキュリティ対策のための調査業務」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196点、価格点の配分を98点とする。

技術点	480点
価格点	240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、複数の評価者で各項目を評価し、各評価者の評価結果（得点）の平均値（小数点第2位以下切捨て）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。	20	5
A	通常想定される提案としては最適な内容である。	12	3
B	概ね妥当な内容である。	6	1
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・プラチナえるぼし認定企業）	プラチナえるぼし（※1）	15
	認定基準○（5）（※2）	12
	認定基準○（3～4）（※2）	10
	認定基準○（1～2）（※2）	6
	行動計画（※3）	3
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	13
	くるみん認定企業（新基準）（※4）	10
	くるみん認定企業（旧基準）（※5）	7
若者雇用促進法に基づく認定（ユースエール認定企業）		13

※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　○○○○○　担当者殿

質　問　書

「EC サイトセキュリティ対策のための調査業務」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、「EC サイトセキュリティ対策のための調査業務」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　　￥＿＿＿＿＿＿＿＿＿＿＿＿

（※別紙入札内訳書に基づき算出された下記件名に係る費用の総価（税抜）を記載すること）

件　名　「EC サイトセキュリティ対策のための調査業務」

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：「EC サイトセキュリティ対策のための調査業務」

【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	5 部		④	評価項目一覧	5 部	
⑤	資格審査結果通知書の写し	1 通		⑥	提案書受理票	（本紙）	
⑦	③と④の電子ファイル	1 式					

---------- 切り取り ----------

提案書受理番号＿＿＿＿＿＿＿＿＿＿＿＿

提案書受理票

年　　月　　日

件　名　「EC サイトセキュリティ対策のための調査業務」

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
セキュリティ対策推進部 脆弱性対策グループ

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。