「新たなサイドチャネル攻撃に関する実機調査と評価手順の作成」に係る一般競争入札

（総合評価落札方式）

入札説明書

2021年7月27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（2021年7月27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　　新たなサイドチャネル攻撃に関する実機調査と評価手順の作成
(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、「新たなサイドチャネル攻撃に関する実機調査と評価手順の作成」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1・2・3年度（平成31・32・33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開催方法

(1) 入札説明会の日時
2021年8月11日（水）　15時00分
(2) 入札説明会の開催方法
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、2021年8月10日（火）17時00分までに申し込むこと。
② 電子メールの件名に「【新たなサイドチャネル攻撃に関する実機調査と評価手順の作成】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
2021年8月11日（水）から2021年8月31日（火）　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
2021年9月2日（木）から2021年9月6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
2021年9月6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	－	4 部
④	評価項目一覧	－	4 部
⑤	令和 1・2・3 年度（平成 31・32・33 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（CD-R 又は DVD-R 提出）	－	1 部

(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「新たなサイドチャネル攻撃に関する実機調査と評価手順の作成　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、「新たなサイドチャネル攻撃に関する実機調査と評価手順の作成　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.(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「新たなサイドチャネル攻撃に関する実機調査と評価手順の作成　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-R 又は DVD-R 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
IPAが必要と判断した入札者に対して実施する。
日時：2021年9月9日（木）9時30分～14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
2021年9月10日（金）　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A

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）

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、契約締結時までに入札内訳書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　セキュリティ技術評価部

暗号グループ　　担当：神田、橋本、佐藤

TEL：03-5978-7545

E-mail：isec-jisech-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:中尾、関

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（案）

2021 情財第〇〇号

契　約　書

独立行政法人情報処理推進機構（以下「甲」という。）と〇〇〇〇〇（以下「乙」という。）とは、次の条項により「新たなサイドチャネル攻撃に関する実機調査と評価手順の作成」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「新たなサイドチャネル攻撃に関する実機調査と評価手順の作成」（以下、「請負業務」という。）の完遂を乙に注文し、乙は本契約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 49 条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 2 第 18 項又は第 21 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 2 第 18 項又は第 21 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（損害賠償額の予定）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損害賠償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、前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（損害賠償額の予定）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損害賠償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。

2021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

「新たなサイドチャネル攻撃に関する実機調査と評価手順の作成」

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

「新たなサイドチャネル攻撃に関する実機調査と評価手順の作成」

2. 背景・目的

従来、セキュリティの観点では、ソフトウェアへの攻撃に比べて、ハードウェアへの攻撃はノウハウが必要なだけでなく、一部のハードウェア解析装置そのものが非常に高価であったり、またターゲットとなるハードウェアデバイスの技術的情報や攻撃の知見を持つ攻撃者も限定的であったりすることから、サイドチャネル攻撃のハードルが高く一般にセキュリティが高いと思われていた。しかしながら、最近では、ハードウェア解析装置の低廉化・高度化も進んでおり、また攻撃ノウハウを覚え込ませた人工知能で解析させるなど、サイドチャネル攻撃のリスクは格段に高まっている。

今後はサイドチャネル攻撃がより一般的な攻撃手法となる可能性があるため、市販品に搭載されるハードウェアへのサイドチャネル攻撃に対する脆弱性の検証が重要になる。そのため、サイドチャネル攻撃に対するセキュリティ検証に活用可能な技術を調査・追試し、評価手法として確立することが必要である。特に、人工知能技術の利用によるサイドチャネル解析手法の進化[1]、無線通信インターフェースからの漏洩による新たなサイドチャネル攻撃[2]などについて、その脅威が無視できなくなって来ており、今後の動向に注意を払わなければならない状況である。

そのため、独立行政法人情報処理推進機構（以下「IPA」という。）では、上記の脅威が増加する恐れのある新たなサイドチャネル攻撃に関する評価手順を明らかにするための実機調査を実施する。なお、本調査は関連する先行調査「フォトエミッション等のサイドチャネル攻撃に関する調査」における参考文献調査及び机上検討を引き継いで、実機を使用した侵入試験／解析試験を試行することで机上検討を超える知見を得て、実証された評価手順／解析手順を作成することを目的とする。

本調査によって得られた新たな知見や調査結果は、最終的にはハードウェア攻撃手法を含むハイレベルな検証サービスを行う際の評価手法及び評価基準の開発、並びに IT セキュリティ評価及び認証制度[3]における新たな評価基準の提案などに活用する。

3. 事業概要

・無線通信インターフェースからの漏洩によるサイドチャネル攻撃の実機調査と評価手順[4]の作成
・人工知能技術によるサイドチャネル解析手法の実機調査と解析手順の作成
・成果報告書等の作成
・成果報告会の開催

4. 業務内容

---

[1] 人工知能技術の利用によるサイドチャネル解析手法の進化：従来は熟練した技術者にのみ可能であった攻撃の最適なポイントの選択などが人工知能技術の利用によって容易になりつつある。
参考文献①[AI-1]：Breaking cryptographic implementations using deep learning techniques. SPACE 2016
参考文献②[AI-2]：Convolutional Neural Networks with Data Augmentation Against Jitter-Based Countermeasures. CHES 2017
参考文献③[AI-3]：Non-Profiled Deep Learning-Based Side-Channel Attacks CHES 2019

[2] 無線通信インターフェースからの漏洩によるサイドチャネル攻撃：BlueTooth や WiFi などを傍受することによって、接続しているデバイスへのサイドチャネル攻撃を実施するもの。
参考文献①[SC-1]：Screaming Channels BlackHat USA 2018 https://i.blackhat.com/us-18/Wed-August-8/us-18-Camurati-Screaming-Channels-When-Electromagnetic-Side-Channels-Meet-Radio-Tranceivers-wp.pdf
参考文献②[SC-2]： “Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers,” in Proc. of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp. 163-177, Jan. 2018.
参考文献③[SC-3]： “Understanding Screaming Channels: From a Detailed Analysis to Improved Attacks,” in IACR Transactions on Cryptographic Hardware and Embedded Systems (CHES), 2020.

[3] IT セキュリティ評価及び認証制度：IPA は、IT 製品について調達者が求めるセキュリティ機能やセキュリティ保証が満たされていることを情報セキュリティの国際標準 ISO/IEC 15408 に基づいて第三者が評価し、その結果を公的に検証する制度として JISEC を運営している。https://www.ipa.go.jp/security/jisec/index.html

[4] 評価手順：特定の製品や機能などについて、ある脆弱性を悪用した攻撃が成功するかを評価するための手順。この手順に従った攻撃 が IT セキュリティ製品に対して成功しない場合には、「この脆弱性はその製品に対して悪用可能では無い」と評価する 。 攻撃が成功してしまう場合であっても、攻撃のコストが非常に高い場合には、「この脆弱性の悪用は現実的では無い」として製品は不合格とならない。合格基準となる攻撃のコストは、 スマートカード及び類似デバイスのサポート文書 (([JIL https://www.sogis.eu/documents/cc/domains/sc/JIL Application of Attack Potential to Smartcards v3 1.pdf に基づき国際連携している。

4.1　業務概要

サイドチャネル攻撃においては、新たな攻撃機器や解析手法が採用されたり、新たな攻撃パスが発見されたりと活発な動きが続いている。それらの状況に対応するためには、具体的に侵入試験を実施したり、従来の攻撃方法との比較を行ったりして、新たなサイドチャネル攻撃を予め調査し、攻撃方法や解析方法として有効なものについて評価手順及び解析手順を作成する必要がある。このため、以下の実機調査の業務を行う。

①無線通信インターフェースからの漏洩によるサイドチャネル攻撃の実機調査と評価手順の作成

Bluetooth、Wifi 等の無線通信インタフェース機能を実装したマイクロプロセッサ上の以下の機能/実装に対して、無線通信を傍受するサイドチャネル攻撃を試行し、内部情報を取得できるかを調査する。そして、取得されてしまうことが今後[5]は現実的になると判断される有効な攻撃シナリオ[6]を作成して、レーティング表を作成する。また、その実施方法を IT セキュリティ評価及び認証制度において再現できるように評価手順としてまとめる。

- ソフトウェア実装された DES 暗号又は AES 暗号

②人工知能技術によるサイドチャネル解析手法の実機調査と解析手順の作成

研究用に公開されている以下の種別の電力波形を、ニューラルネットワークによる深層学習モデルに基づいて GPU 上で試行解析し、「内部情報を取得する解析能力」及び「サイドチャネル攻撃への対抗手段を無力化する能力」を調査する。そして、従来のサイドチャネル解析より優れた点がある解析シナリオ[7](以降、有効な解析シナリオと称する)を作成して、レーティング表を作成する。また、その実施方法を IT セキュリティ評価及び認証制度において再現できるように解析手順としてまとめる。

- ジッタの有る電力波形
- マスキングされていない電力波形
- マスキングされた電力波形

③成果報告書等の作成
④成果報告会の開催

4.2　業務内容

4.2.1　無線通信インターフェースからの漏洩によるサイドチャネル攻撃の実機調査と評価手順の作成

本業務は表 1 の手順で行なうこと。なお、手順を変更する必要がある場合には IPA と協議し承諾を得ること。

表 1【無線通信インターフェースからの漏洩によるサイドチャネル攻撃の実機調査と評価手順の作成の業務の手順】

No.	手順	説明
1	侵入試験準備	・侵入試験を実施するために以下の準備を行う。 □実施体制の構築 □試験機器の用意と試験環境の構築 □試験対象のマイクロプロセッサの準備

[5] 今後：本節 4 .1 業務概要においての「今後」は、 現時点での知見から 2~5 年程度先を想定している。
[6] 攻撃シナリオ：本文書ではターゲットとするデバイスに対して攻撃者が実行する一連のアクションを具体的かつ明確に記述したものを指す。第三者が再現できる程度に各ステップの目的、 準備や設定、そして使用するテクニックや結果の判断内容が詳細で、 担当 者による差異が発生しないものを想定する。
[7] 解析シナリオ：本文書ではターゲットとする電力波形に対して解析者が実行する一連のアクションを具体的かつ明確に記述したものを指す。第三者が再現できる程度に各ステップの目的、準備や設定、そして使用するテクニックや結果の判断内容が詳細で、担当者による差異が発生しないものを想定する。

2	実機による測定(その 1)	・表 3 の試験項目について、以下の作業を行う。 □マイクロプロセッサに試験項目の動作をさせる。 □オシロスコープ、プローブ等の測定機器をマイクロプロセッサに接続/近接させて、従来の測定方法による消費電力波形又は放射電磁波を測定し、内部情報を取得するサイドチャネル攻撃を行う。
3	周波数候補の特定	・表 3 の試験項目について、以下の作業を行う。 □No.2 の結果を分析して、以下のように内部情報の取得に適している(周波数、時刻)[8]を測定候補として 3 セット特定する。 〇(周波数、時刻)×3 セット
4	実機による測定(その 2)	・表 3 の試験項目について、以下の作業を行う。[9] □マイクロプロセッサが無線通信によって放射する電磁波を測定する外部の測定機器について、測定機器、設置場所の観測条件を変えて無線通信の搬送波の電磁波を測定する。 □設置場所はマイクロプロセッサから 1～3m 程度の一定の距離において、方角と仰角を任意に変化させて測定する。 □搬送波の受信状況が最も良い方角と仰角を、以下のように最低 1 セット観測位置として特定する。 〇（方角、仰角）×1 セット
5	攻撃シナリオの作成	・表 3 の試験項目について、以下の作業を行う。 □解析アルゴリズムを検討して、最低 2 つを選択する。 □No.3 で特定した周波数候補 3 つ、No.4 で特定した観測位置 1 つ、選択した解析アルゴリズム 2 つを組合わせて、最低 6 つの攻撃シナリオを作成する。
6	実機による測定(その 3)	・表 3 の試験項目について、以下の作業を行う。 □No.5 で作成した攻撃シナリオを試行して、実際の内部情報取得の効率と達成される取得率を調査する。 □試行結果から実際に内部情報の取得が現実的であると判定された攻撃シナリオを、表 3 の試験項目に対する「有効な攻撃シナリオ」とする。 ・有効な攻撃シナリオが 1 つも無い場合には、手順 No.5 に戻り作成方針を再検討する。
7	評価手順の作成	・表 3 の試験項目について、以下の作業を行う。 □No.6 で「有効な攻撃シナリオ」と判定されたものに対応する評価手順とレーティング表を作成する。
8	本節に関する報告書作成	本節の作業内容と結果を成果報告書の対応する章に記載する。

以下に、上記表 1 の各手順について説明及び注意を記述する。

①手順 No.1【侵入試験準備】

[実施体制の構築]

・本節で実施する「無線通信インターフェースからの漏洩によるサイドチャネル攻撃の実機調査と評価手順の作成」の業務について以下の実施体制を構築すること。

〇「Bluetooth、WiFi 等の無線 LAN、又は ISO/IEC 14443 等のコンタクトレス通信」に関連する調査、研究、評価、認証、あるいは関連する業務や類似する業務のいずれかをおこなった経験のある要員を含むこと。

〇サイドチャネル攻撃に関連する調査、研究、評価、認証、あるいは関連する業務や類似する業務のいずれかをおこなった経験のある要員を含むこと。

〇ハードウェア侵入試験機器、あるいは類似の機器を業務として利用した経験を持つ要員を含むこと。

[8] 測定結果に応じて、周波数は周波数区間や範囲の意味で使用されることがある。そして、搬送波のサイドバンドの場合は、両側の領域で 1 つとカウントする。また、時刻は時間範囲の意味で使用されることがある。

[9] 有線接続による侵入試験においては、本手順は省略しても良い。

〇IT セキュリティ評価及び認証制度に関する知見のある要員を含むこと。

[試験機器の用意と試験環境の構築]

・侵入試験で使用する機器には、無線通信インターフェースからの電磁波を観測するための「無線受信機能」と受信した電磁波を測定する「高周波測定機能」が含まれること。そして 3 つの参考文献([SC-1]、[SC-2]、[SC-3])と少なくとも同等の再現実験ができる表 2 の仕様／性能の要求事項を満たす機器を使用すること。

表 2【電磁波測定機器の仕様／性能】

機能	機器	仕様／性能	要求事項
無線受信	アンテナ／プローブ	受信周波数	2.4GHz～5GHz を含むこと
高周波測定	オシロスコープ	サンプリング周波数	5GS/s 以上

・無線通信インターフェースからの電磁波測定環境は外来からの電磁波ノイズ等の防止に努めること。また、高周波の測定に適した関連測定機器を使用すること。

[試験対象のマイクロプロセッサの準備]

・侵入試験の対象となるデバイスは、表 3 の試験項目の暗号演算を行うデジタル回路と無線通信インターフェースを同一チップ内に実装したものを用意する。

・侵入試験の対象となるデバイスについては、名称及び仕様の概要を明らかにすること。また、実際の選択については、IPA と協議し承諾を得ること。

・攻撃の対象とする無線通信方式には、BlueTooth、WiFi 等から最低 1 つの無線 LAN 規格の通信方式を含める。なお、BlueTooth は IEEE 802.15 シリーズ及び BlueTooth LE から、Wifi は IEEE 802.11 シリーズから任意に選択して構わないが、名称及び仕様の概要を明らかにすること。また、本事業実施前に IPA と協議し承諾を得ること。

・受託事業者自身が用意するターゲットデバイスの無線通信インタフェースからの電磁波観測を有利にする物理加工等の前処理が有る場合は受託事業者自身で実施する。

表 3【侵入試験項目】

No.	試験項目
1	ソフトウェア実装された DES 暗号又は AES 暗号 [10]

②手順 No.2【実機による測定(その 1)】

[通常手法による測定]

・マイクロプロセッサにオシロスコープ、プローブ等の測定機器を接続又は近接させて、消費電力又は放射電磁波を測定する環境を作り、通常のサイドチャネル攻撃を実施する体制を作る。

・マイクロプロセッサに表 3 の試験項目に関連する一連の動作を繰り返し実行させてサイドチャネル測定を行う。

・測定の継続に伴い、内部情報である暗号鍵情報の取得効率を分析する。

③手順 No.3【周波数候補の特定】

・手順 No.2 の測定結果を周波数の観点で分析して、内部情報の取得に適した周波数と時刻のセットを以下のように周波数候補として 3 セット [11]特定する。

〇[周波数候補 3 セット]

(周波数 A1、時刻 A1)、(周波数 A2、時刻 A2)、(周波数 A3、時刻 A3)

・この手順の分析においては、内部情報の取得効率の推移や達成された取得率を総合的に評価して候補を選択する。

[10] DES 暗号又は AES 暗号から 1 つ選択すること。

[11] 一般的な観点として第 3 高調波までを含める意図があるが、測定の結果に応じてより良い取得の可能な周波数を選択して良い。

・2.背景・目的で挙げた 3 つの参考文献([SC-1]、[SC-2]、[SC-3])を参考とする。

④手順 No.4【実機による測定(その 2)】

[無線通信による搬送波測定]

・無線通信によって放射する搬送波を測定するために、アンテナ/プローブとオシロスコープを設置して測定を行う。

・マイクロプロセッサには任意の動作をさせて測定を行う。

・アンテナ/プローブをマイクロプロセッサから 1～3m 程度の一定距離の球面上に配置しながら、方角と仰角を様々に変化させて、最も搬送波の受信レベルが高い（方角、仰角）を観測位置として以下のように 1 セット特定する。

○[観測位置 1 セット]
（方角、仰角）

⑤手順 No.5【攻撃シナリオの作成】

・マイクロプロセッサに表 3 の試験項目に関連する動作に対する攻撃シナリオを作成する。

・攻撃シナリオは、相関電力解析(CPA:Correlation Power Analysis)、差分電力解析(DPA:Differential Power Analysis)、相互情報量解析(MIA:Mutual Information Analysis)、テンプレート攻撃(Template Attack)、CRA(Correlation Radio Analysis)、TRA(Template Radio Analysis)等の解析アルゴリズム、あるいは更にこれらを複号させた解析アルゴリズムから、最低 2 つの解析アルゴリズムを選択して、攻撃シナリオ[12]を作成すること。

・攻撃シナリオは、選択した解析アルゴリズム 2 つ、手順 No.4 で特定した観測位置 1 つ、そして手順 No.3 で特定した周波数候補 3 つを組合わせて、最低 6 つの攻撃シナリオを作成する。

・攻撃シナリオの例をサンプル として 以下に参考情報として示す。これは、あくまでイメージの提示のための概要 の記述であり、かつ一部の抽出であることに留意すること。

表 4【攻撃シナリオの例】

※攻撃シナリオの例は、以下のとおり。なお、攻撃シナリオの記述としては一部分の抜粋であることに注意。

項目	記述
名称	AES 暗号に対する差分電力解析による暗号鍵の取得
攻撃目標	暗号鍵
機能	AES 暗号
動作	暗号化
攻撃テクニック	差分電力解析
攻撃シナリオ	・ターゲットデバイスに暗号演算の実行をさせる制御環境を設定 ・ターゲットデバイスの無線 LAN 通信インターフェース（802.11a）が放出する電磁波を観測するように測定機器をセットアップ ・AES 暗号プログラムに 0x3DF8～A14B を入力し、暗号化を実施 … ・AES 暗号プログラムに 0xF2AE～6E3C を入力し、暗号化を実施 ・保存した電磁波測定データから特定の周波数成分を抽出する等の前処理を実施し…。 ・差分電力解析を適用 …
補足情報	・ターゲットデバイスの CK 周波数：… ・オシロスコープのサンプリング周波数：… …

・2.背景・目的で挙げた 3 つの参考文献([SC-1]、[SC-2]、[SC-3])を参考とすること。

[12] 解析アルゴリズムが異なる場合は、それに関係しない他の部分の内容が同じである攻撃シナリオも、異なる攻撃シナリオとして扱う。

⑥手順 No.6【実機による測定（その 3)】

［無線通信によるサイドチャネル測定］

・アンテナ/プローブをマイクロプロセッサから手順 No.6 で特定した観測位置に配置し、マイクロプロセッサに表 3 の試験項目の動作を実行させて、無線通信の搬送波を受信して、手順 No.3 で特定された周波数候補を測定する環境を作り、無線通信によるサイドチャネル攻撃を実施する体制を作る。そして、手順 No.5 で作成した攻撃シナリオをすべて試行して、実際の内部情報取得の効率と達成される取得率を調査する。

・測定の継続に伴い、内部情報である暗号鍵情報の取得効率を分析する。

・サイドチャネル攻撃単独で内部情報を 100%すべて取得することは一般的に困難であるため、測定の継続に伴う取得率の推移を調べたり、あるいは既知鍵解析等において正解値がランキングの何番目にあるかの推移を調べることが傾向の判断に必要である。このような推移をグラフにマッピングして取得の効率が鈍化した点を見極めて、総当たり攻撃など他の攻撃手法を補助的に組合わせるなどの対応を考慮する。総当たり攻撃等の補助的な作業を実際に実施完了することは不要であり、総当たり攻撃の手法の説明と攻撃の完了に要する期間を計算すること。

・攻撃シナリオの実施開始から総当たり攻撃等の補助的な攻撃手法の完了までの期間が、5 年 [13]以内である場合には、内部情報の取得が現実的に可能である攻撃シナリオと判定すること。

・総当たり攻撃などの補助的な攻撃手法の所要期間は、専用ハードウェアエミュレータやクラウドコンピューティングの利用も考慮して完了までの最短所要期間を推測すること。

・試行結果が実際に内部情報の取得が現実的であると判定された攻撃シナリオを表 3 の試験項目の「有効な攻撃シナリオ」とする。

・「すべての攻撃シナリオが有効な攻撃シナリオでは無い。」と判定された場合には、手順 No.5 に戻り攻撃シナリオの作成方針を再検討する。周波数候補と解析アルゴリズムが、優先順位の次点であったものを繰り上げて新たな攻撃シナリオを作成し、本手順 No.6 を再実行する。その際には実機検証で得られた知見からの攻撃シナリオの修正も考慮に含める。それでも、「有効な攻撃シナリオ」に到達しない場合は再度、再検討と再実行を行う。そして、トータルで最低 2 回の再検討と再実行を経てもなお、「有効な攻撃シナリオ」への到達が 1 つも無い場合は、攻撃の完了までの期間が最も短い攻撃シナリオ上位 3 件を「有効な攻撃シナリオ」とみなして、以降の手順を実施する。

⑦手順 No.7【評価手順の作成】

・手順 No.6 で「有効な攻撃シナリオ」と判定されたものに対応する評価手順とレーティング表を作成する。ISO/IEC15408[14] にある独立テストの試験計画の項目を報告書として記述する際の要求仕様を参考にし、第三者による再現実験が可能な詳細度で、攻撃シナリオにおいて実施される手順を評価手順として取りまとめること。記述内容に関して判断に迷う場合は IPA に相談すること。

・総当たり攻撃等の補助的な攻撃手法を組合わせた場合は、総当たり攻撃方法の具体的なアルゴリズム等の手順と使用を想定する機器についても記述すること。また、総当たり攻撃が完了する期間の計算についても記述すること。専用ハードウェアエミュレータやクラウドコンピューティングの利用を想定した場合は、具体的な使用手順や利用の申請方法までは不要であり、利用を想定した機器の名称、仕様/機能やサービスの概要が分かる記述で良い。

・有効な攻撃シナリオのレーティング表を作成すること。レーティング表の作成においては、スマートカード及び類似デバイスのサポート文書([JIL AAP]) [15]に適合させること。

⑧手順 No.8【本節に関する報告書作成】

・「手順 No.2【実機による測定(その 1)】」、「手順 No.4【実機による測定(その 2)】」、そして「手順 No.6【実機による測定(その 3)】」で使用した「アンテナ/プローブ」と「オシロスコープ」及び関連するオプション、関連測定機器について仕様／性能を記述すること。また、これら機器の接続や初期化の手順などについても記述すること。

・試験環境の構築として、電磁波ノイズなどの防止について対策した事項を記述すること。また、高

[13] この判定基準は、IT セキュリティ評価及び認証制度における「現実的な攻撃シナリオ」の判定基準ではないことに留意すること。本文書では将来の脅威に備えるための調査業務として特別な判定基準を採用している。

[14] ISO/IEC 15408：情報技術セキュリティ評価のための共通方法評価方法2017年4月バージョン3.1改訂第5版
AVA_VAN.4-7、AVA_VAN.4-10 https://www.ipa.go.jp/security/jisec/cc/documents/CEMV3.1R5-J1.0.pdf

[15] [JIL AAP] (Joint Interpretation Library Application of Attack Potential to Smartcards and Similar Devices)：JILが作成したハードウェアへの攻撃に関する評価認証をサポートする文書であり、攻撃者の攻撃ポテンシャル等について記述。
https://www.sogis.eu/documents/cc/domains/sc/JIL-Application-of-Attack-Potential-to-Smartcards-v3-1.pdf

周波の測定に適した関連測定機器を使用したことに関する事項を記述すること。
・本節の侵入試験において、使用したターゲットデバイスについて記述すること。また、その仕様等の情報を記述すること。ターゲットデバイスの無線通信インタフェースからの電磁波観測を有利にする物理加工等の前処理が有った場合は、その概要を記述すること。
・2.背景・目的で挙げた 3 つの参考文献([SC-1]、[SC-2]、[SC-3])以外の文献を参考にした場合は、文献の一覧と各文献の概要を記述すること。
・「No.2 実機による測定(その 1)」において実施した実機測定の内容と結果を記述すること。また、測定の継続に伴う内部情報の取得効率の推移の分析についても記述すること。そして、通常のサイドチャネル攻撃の測定方法として各機能やオプションに採用した設定、測定手順、そして結果について記述すること。
・「No.3 周波数候補の特定」において、周波数候補の特定のために実施した分析と特定結果について記述すること。
・「No.4 実機による測定(その 2)」において、観測位置の特定において実施した実機測定の内容と結果を記述すること。
・「No.5 攻撃シナリオの作成」において、最も効率的で取得率が高いと想定する攻撃シナリオを作成するために実施した分析と判断について記述すること。また、作成した攻撃シナリオと想定される結果を記述すること。そして、作成した攻撃シナリオの背景となる技術的な知見や情報、あるいは戦略が有る場合には、それについても記述すること。
・「No.6 実機による測定(その 3)」において実施したすべての侵入試験の内容と結果を記述すること。また、測定の継続に伴う取得率の推移や既知鍵解析等の分析の内容についても記述すること。そして、総当たり攻撃等の補助的な攻撃手法を組み合わせた場合は、その手法の内容や使用を想定した機器の名称、仕様/機能やサービスの概要についても記述し、攻撃の完了までの期間の計算方法と計算結果を記述すること。
・「No.6 実機による測定(その 3)」において実施した侵入試験のすべてについて、攻撃の完了までの期間が 5 年以内と判定された攻撃シナリオを「有効な攻撃シナリオ」として報告すること。
・「No.6 実機による測定(その 3)」において、「すべての攻撃シナリオが現実的では無い。」と判断された際の、攻撃シナリオの再検討、実機試験の再実行について、再検討の内容、実機検証による知見、再作成された攻撃シナリオ、再実行された結果について記述すること。また、最終的に「有効な攻撃シナリオ」とみなす判断があった場合は、その過程についても記述すること。
・「No.7 評価手順の作成」において作成した評価手順は、ISO/IEC15408 にある独立テストの試験計画の項目を報告書として記述する際の要求仕様を参考にし、第三者による再現実験が可能な詳細度で、攻撃シナリオにおいて実施された手順を評価手順として取りまとめること。記述内容に関して判断に迷う場合は IPA に相談すること。また、レーティング表を記述すること。レーティング表の各ファクタには点数の根拠を記述すること。
・本節全体を通して得られた結果を俯瞰する視点からの分析や取りまとめを記述すること。

4.2.2 人工知能技術によるサイドチャネル解析手法の実機調査と解析手順の作成

本業務は表 5 の手順で行なうこと。なお、手順を変更する必要がある場合には IPA と協議し承諾を得ること。

表 5【人工知能技術によるサイドチャネル解析手法の実機調査と解析手順の作成の業務の手順】

No.	手順	説明
1	侵入試験準備	・解析試験を実施するために以下の準備を行う。 □実施体制の構築 □解析機器の用意と解析環境の構築 □解析対象の波形データの準備
2	従来のサイドチャネル解析の実施	・表 7 の試験項目について、以下の作業を行う。 □人工知能技術によらない従来のサイドチャネル解析を実施する。
3	解析シナリオの作成	・表 7 の試験項目について、以下の作業を行う。 □2.背景・目的の人工知能の参考文献([AI-3])の再現をする 2

		つの解析シナリオを作成する。[16]
4	人工知能技術によるサイドチャネル解析の実施	・表 7 の試験項目について、以下の作業を行う。 □手順 No.3 で作成した 2 つの解析シナリオを試行する。
5	実施結果比較	・表 7 の試験項目について、以下の作業を行う。 □手順 No.2 と手順 No.4 の試行結果比較から、人工知能技術によるサイドチャネル解析に優れた点があると判定された解析シナリオを「有効な解析シナリオ」とする。 ・有効な解析シナリオが 1 つも無い場合には、手順 No.3 に戻り作成方針を再検討する。
6	解析手順の作成	No.5 で有効な解析シナリオとされたものについて解析手順を作成し、レーティング表を作成する。
7	本節に関する報告書作成	本節の作業内容と結果を成果報告書の対応する章に記載する。

以下に、上記表 5 の各手順について説明及び注意を記述する。

①手順 No.1【侵入試験準備】

[実施体制の構築]

・本節で実施する「人工知能技術によるサイドチャネル解析手法の実機調査と解析手順の作成」の業務について以下の実施体制を構築すること。

〇人工知能技術に関連する調査、研究、評価、認証、あるいは関連する業務や類似する業務のいずれかをおこなった経験のある要員を含むこと。
〇IT セキュリティ評価及び認証制度に関する知見のある要員を含むこと。

[解析機器の用意と解析環境の構築]

・解析試験で使用するシミュレーション環境においては、2.背景・目的で挙げた 3 つの参考文献([AI-1]、[AI-2]、[AI-3])におけるシミュレーションと少なくとも同等の解析実験ができる表 6 の機器以上の性能の機器を使用すること。

表 6【人工知能技術のシミュレーション実施機器】

機能	機器
GPU	NVIDIA GeForce GTX 1080 GPU
CPU	Intel Xeon E5-2687W CPU

・Keras、TensorFlow、Python 等のオープンソースニューラルネットワークライブラリや、MATLAB 等のソフトウェアツールを使用するための用意をする。そして、ニューラルネットワークをシミュレーションできる環境を構築する。
・以下のようなニューラルネットワークの一種である MLP(Multi Layer Percetion:多層パーセプトロン)、CNN(Couvolutional Neural Network : 畳み込みニューラルネット)、そしてこれらに基づいた DLPA(Deep Learning Power Analysis : 深層学習電力解析)をシミュレーショする環境を構築する。

〇MLP(Multi Layer Percetion:多層パーセプトロン):ニューラルネットワークの一種であり、入力層、隠れ層、出力層が全結合であるもの。
〇CNN(Couvolutional Neural Network : 畳み込みニューラルネット) : ニューラルネットワークの一種であり、全結合していない順伝搬型であるもの。

[解析対象の波形データの準備]

[16] 少なくとも 1 つの解析シナリオは[AI-3]の再現として非プロファイル型を採用すること。より良い結果が得られる場合には、もう 1 つの解析シナリオとして[AI-3]の再現で無いものやプロファイル型であるものを作成して良い。

・解析試験の対象となる電力波形は、シミュレーションによって生成したものではなく、実際のデバイスが生成したものを用意すること。
・DPA contest v4.2 等において公開されている AES 等の電力波形を解析の入力として用意する。
・解析試験の対象となる電力波形については、名称及び概要を明らかにすること。また、本事業実施前に IPA と協議し承諾を得ること。
・解析対象の波形データは、表 7 の試験項目をすべてカバーするように、それぞれ最低１つ選択すること。

表 7【解析試験項目】

試験項目
ジッタの有る波形
マスキングされていない電力波形
マスキングされた電力波形

②手順 No.2【従来のサイドチャネル解析の実施】
［人工知能技術に依らない解析］
・表 7 の試験項目について、以下の作業を行う。

□従来の手法によるサイドチャネル解析を実施する。解析対象の波形データの仕様に応じて、例えば主成分分析等による前処理、アラインメント、解析アルゴリズム(SPA/SEMA、CPA/CEMA、DPA/DEMA、MIA 等)による解析、そして補助的な攻撃手法を実施する。2.背景・目的で参照された参考文献 [AI-3] において人工知能技術と比較されている従来手法、あるいは類似の解析手法を候補に含めて選択し実施すること。実施が可能な波形データであれば、プロファイルド／ノンプロファイルドによらず広くサイドチャネル解析の手法を候補に含めること。判断に迷う場合は IPA に相談すること。
□サイドチャネル攻撃単独で攻撃目標を 100%すべて取得することは一般的に困難であることに留意すること。電力波形データの解析数を増やすことによって取得率がどのような推移をたどるかを調べたり、あるいは既知解解析において正解値がランキングの何番目にあるかの推移を調べること。このような推移をグラフにマッピングして取得のペースが鈍化した点を見極めて、総当たり攻撃など他の攻撃手法を補助的に組合わせるなどの対応を考慮する。総当たり攻撃等の補助的な作業を実際に実施完了することは不要であり、総当たり攻撃の手法の説明と攻撃の完了に要する期間を計算すること。
□総当たり攻撃などの補助的な攻撃手法の所要期間は、専用ハードウェアエミュレータやクラウドコンピューティングの利用も考慮して完了までの最短所要期間を推測すること。
□総当たり攻撃等の補助的な攻撃手法を組合わせた場合は、総当たり攻撃方法の具体的なアルゴリズム等の手順と使用を想定する機器についても記述すること。また、総当たり攻撃が完了する期間の計算についても記述すること。専用ハードウェアエミュレータやクラウドコンピューティングの利用を想定した場合は、具体的な使用手順や利用の申請方法までは不要であり、利用を想定した機器の名称、仕様/機能やサービスの概要が分かる記述で良い。

③手順 No.3【解析シナリオの作成】
・表 7 の試験項目について、以下の作業を行う。

□2.背景・目的で参照された参考文献([AI-3])の Non-Profiled-Deep Learning Side Channel Attack に従って解析する以下の 2 タイプのアプローチの解析シナリオを各 2 つ作成する。(計 4 つ)

〇タイプ 1：MLP をシミュレーションする解析環境において、2.背景・目的の人工知能の参考文献([AI-3])の Algorithm1,2 等を実施する MLP-DLPA を適用する解析シナリオ
〇タイプ 2：CNN をシミュレーションする解析環境において、2.背景・目的の人工知能の参考文献([AI-3])の Algorithm1,2 等を実施する CNN-DLPA を適用する解析シナリオ

□2.背景・目的で参照された参考文献([AI-1]、[AI-2]、[AI-3])を参考にし、同等レベル以上の解析試験を再現するための解析シナリオを作成する。

④手順 No.4【人工知能技術によるサイドチャネル解析の実施】

・表 7 の試験項目について、以下の作業を行う。

□手順 No.3 で作成された解析シナリオを解析環境を実際に使用して調査する。
□サイドチャネル攻撃単独で攻撃目標を 100%すべて取得することは一般的に困難であることに留意すること。電力波形データの解析数を増やすことによって取得率がどのような推移をたどるかを調べたり、あるいは既知解解析において正解値がランキングの何番目にあるかの推移を調べること。このような推移をグラフにマッピングして取得のペースが鈍化した点を見極めて、総当たり攻撃など他の攻撃手法を補助的に組合わせるなどの対応を考慮する。総当たり攻撃等の補助的な作業を実際に実施完了することは不要であり、総当たり攻撃の手法の説明と攻撃の完了に要する期間を計算すること。
□総当たり攻撃などの補助的な攻撃手法の所要期間は、専用ハードウェアエミュレータやクラウドコンピューティングの利用も考慮して完了までの最短所要期間を推測すること。
□総当たり攻撃等の補助的な攻撃手法を組合わせた場合は、総当たり攻撃方法の具体的なアルゴリズム等の手順と使用を想定する機器についても記述すること。また、総当たり攻撃が完了する期間の計算についても記述すること。専用ハードウェアエミュレータやクラウドコンピューティングの利用を想定した場合は、具体的な使用手順や利用の申請方法までは不要であり、利用を想定した機器の名称、仕様/機能やサービスの概要が分かる記述で良い。

⑤手順 No.5【実施結果比較】

・表 7 の試験項目について、以下の作業を行う。

□手順 No.2 の実施結果と手順 No.4 の実施結果を比較し、「内部情報を取得する解析能力」、あるいは「サイドチャネル攻撃への対抗手段を無力化する能力」の観点で、手順 No.4 の方が優れている点があった解析シナリオは、「有効な解析シナリオ」と判定する。結果の一部や一連のステップの一部であっても優れている点があればポジティブに判定する。判断に迷う場合は IPA に相談すること。

・「すべての試験項目の解析シナリオが有効な解析シナリオでは無い。」と判定された場合には、手順 No.3 に戻り解析シナリオの作成方針を再検討する。電力波形等のデータの解析数増加に伴う取得率や正解値ランキングの推移を考慮し、2.背景・目的の人工知能の参考文献([AI-3])の Algorithm1,2 等の改変を含めて検討して新たな解析シナリオを作成する。そして、手順 No.4 及び手順 No.5 を再実行する。その際には解析試行で得られた知見からの解析シナリオの修正も考慮に含める。それでも、「有効な解析シナリオ」に到達しない場合は再度、再検討と再実行を行う。そして、トータルで最低 2 回の再検討と再実行を経てもなお「有効な解析シナリオ」への到達が 1 つも無い場合は、攻撃の完了までの期間が最も短い解析シナリオ上位 3 件を「有効な解析シナリオ」とみなして、以降の手順を実施する。

⑥手順 No.6【解析手順の作成】

・表 7 の試験項目について、以下の作業を行う。

□手順 No.5 で「有効な解析シナリオ」と判定されたものについて解析手順を作成する。作成は、ISO/IEC15408 にある独立テストの試験計画の項目を報告書として記述する際の要求仕様を参考にし、第三者による再現実験が可能な詳細度で、解析シナリオにおいて実施される手順を解析手順として取りまとめること。記述内容に関して判断に迷う場合は IPA に相談すること。また、有効な解析シナリオのレーティング表を作成する。レーティング表の作成においては、スマートカード及び類似デバイスのサポート文書([JIL AAP])に適合させること。

⑦手順 No.7【本節に関する報告書作成】

・「手順 No.2【従来のサイドチャネル解析の実施】」及び「手順 No.4【人工知能技術によるサイドチャネル解析の実施】」で使用したソフトウェア、GPU、CPU 及び関連するオプション、関連機器について仕様／性能を記述すること。また、これら機器の接続や初期化などがある場合には、それらの手順につ

いても記述すること。
・「手順 No.1【解析機器の用意と解析環境の構築】」において、解析環境の構築として、効率的な解析を目的に対策した事項があれば記述すること。
・本節の解析試験において、使用した解析ターゲットの波形データについて記述すること。また、その仕様等の情報を記述すること。
・2.背景・目的で挙げた 3 つの参考文献([AI-1]、[AI-2]、[AI-3])以外の文献を参考にした場合は、文献の一覧と各文献の概要を記述すること。
・「No.2 従来のサイドチャネル解析の実施」において実施したすべての解析試験の内容と結果を記述すること。また、波形数の増加に伴う内部情報の取得効率の推移の分析についても記述すること。そして、総当たり攻撃等の補助的な攻撃手法を組み合わせた場合は、その手法の内容や使用を想定した機器の名称、仕様/機能やサービスの概要についても記述し、攻撃の完了までの期間の計算方法と計算結果を記述すること。
・「No.3 解析シナリオの作成」において、作成した解析シナリオと想定される結果を記述すること。
・「No.4 人工知能技術によるサイドチャネル解析の実施」において実施したすべての解析試験の内容と結果を記述すること。また、波形数の増加に伴う取得率の推移や既知鍵解析等の分析の内容についても記述すること。そして、総当たり攻撃等の補助的な攻撃手法を組み合わせた場合は、その手法の内容や使用を想定した機器の名称、仕様/機能やサービスの概要についても記述し、攻撃の完了までの期間の計算方法と計算結果を記述すること。
・「No.4 人工知能技術によるサイドチャネル解析の実施」において実施した解析試験のすべてについて、手順 No.3 において想定した結果と得られた結果との比較を行い、差異がある場合は理由の分析を記述すること。
・「No.5 実施結果比較」において判定された解析シナリオを「有効な解析シナリオ」とそうでない解析シナリオとして報告すること。「有効な解析シナリオ」と判定されたものについては、手順 No.2 の結果との比較において優れていると判断された内容を記述するここと。
・「No.5 実施結果比較」において、「すべての試験項目の解析シナリオが現実的では無い。」と判断された際の、解析シナリオの再検討、実機解析の再実行について、再検討の内容、解析試験による知見、再作成された解析シナリオ、再実行された結果について記述すること。また、最終的に「有効な解析シナリオ」とみなす判断があった場合は、その過程についても記述すること。
・「No.6 解析手順の作成」において作成した解析手順を記述すること。作成は、ISO/IEC15408 にある独立テストの試験計画の項目を報告書として記述する際の要求仕様を参考にし、第三者による再現実験が可能な詳細度で、解析シナリオにおいて実施された手順を解析手順として取りまとめること。
記述内容に関して判断に迷う場合は IPA に相談すること。また、レーティング表を記述すること。レーティング表の各ファクタには点数の根拠を記述すること。
・本節全体を通して得られた結果を俯瞰する視点からの分析や取りまとめを記述すること。

4.2.3　成果報告書等の作成

4.2.1～4.2.2 で実施された作業結果について、成果報告書として取り纏める。全体の記述の詳細度のレベルが十分であることに留意すること。また、4.2.4 に掲げる成果報告会で使用するプレゼンテーション資料も作成すること。作成にあたっては、以下の条件を満たすこと。

- 成果報告書
  a. A4 版の Microsoft Word 形式とし、300 ページ以上で取りまとめること。
  b. 目次を作成すること。
  c. 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。
  d. 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。
  e. 根拠となる実験結果及びデータは、補足資料に加えること。
  f. 4.2.1、4.2.2 において実施された作業結果については、それぞれ１つの章に取りまとめて報告すること。
  g. それぞれの業務内容において、以下の観点にしたがって記載すること。
     ・【4.2.1 表 1No.8 についての報告内容】
     ・【4.2.2 表 5No.7 についての報告内容】
  h. 4.2.4 において開催する成果報告会における IPA からの意見等を反映すること。

- プレゼンテーション資料
  a. 横書き（16:9 サイズ）の Microsoft PowerPoint 形式とし、本事業の要点（全体概要、実施内容、結果、考察等）を 60～80 シートで取りまとめること。

- 共通の注意事項
  a. 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。その場合は日本語での解説も併記すること）。
  b. 誤記・誤植を含まないこと。
  c. IPA からの依頼を反映すること。
  d. 予め記述項目、記載内容及び記載水準に対して IPA の了解を得ること。
  e. これらの要件をすべて満たす成果報告書、プレゼンテーション資料を作成して IPA と協議し承諾を得た期限までに提出すること。

4.2.4　成果報告会の開催

実施期間終了前に、本事業全体について、Zoom を除く Web 会議ツールによるオンライン形式の報告会を 1 回開催する。報告会の開催日程は IPA 担当者と協議し開催の 2 ヶ月前までに決定すること。また、アジェンダ及び使用するプレゼンテーション資料は事前に IPA 担当者に提出し、開催の 2 週間前までに承諾を得ること。報告会は最大 20 人の IPA 聴衆の接続を想定し少なくとも総計 3 時間以上のプレゼンテーションに加えて質疑応答の時間をそれぞれの業務内容ごとに設けること。

・4.2.1 の報告には担当した「無線 LAN 通信又はコンタクトレス通信」の知見を持つ実施要員、サイドチャネル攻撃の知見を持つ実施要員が参加して説明すること。

・4.2.2 の報告には担当した人工知能技術に知見を持つ実施要員が参加して説明すること。

・上記 4.2.1、4.2.2 の報告には、プロジェクトリーダ及び IT セキュリティ評価及び認証制度に知見がある実施要員も参加し、報告及び質疑応答を支援すること。

5.　事業の実施体制

(1) 業務の役割を定めた実働可能な人数を確保すること。
(2) プロジェクトリーダを定めること。プロジェクトリーダ（複数人可）は過去に IT セキュリティ分野に関連する調査、研究、評価、認証、あるいは関連する業務や類似する業務のいずれかの経験があること。
(3) 4.2.1 について、①手順 No.1【侵入試験準備】の[実施体制の構築] の条件を満たす実施体制を構築すること。
(4) 4.2.2 について、①手順 No.1【侵入試験準備】の[実施体制の構築] の条件を満たす実施体制を構築すること。
(5) 業務に当たる者に欠員が生じた場合は、速やかに同等又はそれ以上の経歴を有する代替者を充てられる体制が整えられていること。
(6) 組織として IT 製品の脆弱性の調査や攻撃手法の再現の実績があること。

6.　情報管理体制

（１）情報管理体制

①受託事業者は本業務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、IPA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、役職等が記載されたもの）を契約前に提出し、IPA担当者の同意を得ること。（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IPA担当者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受託事業者が収集、整理、作成等した一切の情報が、目的外の用途に利用されないこと。また、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こと。そして、IPAが提供する情報及び委託事業が生成する情報が、受託

事業者又はその従業員、再委託先、若しくはその他の者による意図せざる変更が加えられないための管理体制を構築すること。

②委託業務に携わる者を特定し本委託業務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。ただし、IPA担当者の承認を得た場合は、この限りではない。

③①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IPA担当者へ届出を行い、同意を得なければならない。

（２）委託業務従事者の経歴
委託業務従事者の氏名、所属、役職、業務経験、その他略歴（学歴、職歴、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）を提出すること。
※経歴提出のない委託業務従事者の人件費は計上不可。

（３）情報の受渡及び履行完了後の情報の取扱い
IPAとの情報の受渡方法やIPAから提供した資料又はIPAが指定した資料の取扱い（返却・抹消等）については、IPA担当者の指示に従い定められた手順により情報を取扱うこと。また、抹消の際にIPAからの求めがあった場合は、抹消されたことに関する確認に対応すること。業務日誌を始めとする経理処理に関する資料については適切に保管すること。

7. 情報セキュリティ対策遵守方法

（１）情報セキュリティ対策
①受託事業者は本委託業務で取り扱う情報を保護し適切に管理するため委託業務に携わる者が実施する具体的な情報セキュリティ対策の内容及び管理体制を明らかにし、ＩＰＡの承諾を得るために、以下②～⑩の情報セキュリティ対策の遵守方法を実装する 「情報管理に対する社内規則」を契約前に提出し、IPA担当者の同意を得ること。有しない場合は代わりとなるものでも良い。

②委託業務の役務内容を一部再委託する場合は、事前にIPA担当者に報告し承認を得ること。そして、再委託されることにより生ずる脅威に対して情報セキュリティが確保されるように以下の(a)、(b)の措置の実施を担保させること。また、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報をIPAに提供し、IPAの承認を受けること。
(a)以下の内容を含む情報セキュリティ対策を再委託先に実施させること。
（ア）再委託先に提供する情報の目的外利用の禁止
（イ）再委託先における情報セキュリティ対策の実施及び管理体制
（ウ）再委託先企業又はその従業員、若しくはその他の者による意図せざる変更が加えられないための管理体制
（エ）再委託先の資本関係・役員等の情報、再委託事業の実施場所、再委託事業従事者の所属・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提供
（オ）情報セキュリティインシデントへの対処方法
（カ）情報セキュリティ対策その他の契約の履行状況の確認方法
（キ）情報セキュリティ対策の履行が不十分な場合の対処方法
(b)再委託する業務において取り扱う情報の格付等を勘案し、必要に応じて以下の内容を再委託仕様に含めること。
（ア）情報セキュリティ監査の受入れ
（イ）サービスレベルの保証

③①の情報セキュリティ対策の実施を確保するために定めた書面に変更がある場合、あるいは②の再委託先の情報に変更が有る場合は、予めIPA担当部門へ届出を行い、同意を得なければならない。

④委託事業における情報セキュリティ対策の履行状況のIPAによる確認に対応するために、IPAが提供する情報及び委託事業が生成する情報の保護及び取扱に係る情報セキュリティ対策その他の契約の履行状況をIPAと合意した定期毎に報告すること。そして、IPAが求める場合は、履行状況の確認のための情報セキュリ

ティ監査を受け入れること。また、IPAが提供する情報及び委託事業が生成する情報の保護及び取扱に係る情報セキュリティ対策の履行が不十分であるとIPAが判断した場合は、情報セキュリティ対策の実施についてIPAの求める改善を行うこと。

⑤IPAが提供する情報及び委託事業で生成された情報を取扱した情報システムの更改又は廃棄を行う場合は、当該情報システムに保存されている情報について、当該情報の格付及び取扱制限を考慮した上で、以下の措置を適切に講ずること。
(ア)情報システム更改時の情報の移行作業における情報セキュリティ対策
(イ)情報システム廃棄時の不要な情報の抹消
(ウ)端末及びサーバ装置の電磁的記録媒体の全ての情報の抹消

⑥委託業務の内容を勘案し、適切な場合には情報処理安全確保支援士の資格を有する者、情報処理技術者試験のうち情報セキュリティに関する資格を有する者、又はこれらと同等の知識及び技能を有する者を情報取扱者に含めること。

⑦受託事業者は、資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・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提供すること。

⑧IPAが提供する情報及び委託事業で生成された情報を取扱する情報システムのセキュリティ機能において定める主体認証・アクセス制御・権限管理・ログ管理等の機能面での対策、ソフトウェアに関する脆弱性対策、不正プログラム対策、サービス不能攻撃対策、IPv6通信回線において定める遵守事項のうちサーバ装置に関係するもの、電子メールサーバ、ウェブサーバ、DNS サーバ及びデータベース、ウェブ等において遵守事項を定めて実施すること。

⑨IPAが提供する情報及び委託事業で生成された情報を取扱する複合機及び特定用途機器が備える機能、利用方法、設置環境並びに取り扱う情報の格付及び取扱制限に応じ、適切なセキュリティ要件を策定し、適切な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講ずること。また、運用を終了する際に、複合機及び特定用途機器の電磁的記録媒体の全ての情報を抹消すること。

⑩本事業の作業においてクラウドサービスを利用する場合は「クラウドサービス利用のための情報セキュリティマネジメントガイドライン[17]」 に記載されている情報セキュリティ対策を行うこと。

（２）情報セキュリティインシデント等の報告
受託事業者は、IPAが提供する情報及び委託事業が生成する情報の権限外のアクセスあるいは第三者への漏洩などの情報セキュリティインシデントに対する適切な対処方法を予め手順として構築すること。そして、受託事業者は本委託業務において、情報セキュリティインシデント、情報の目的外利用等を認知した場合は、速やかにIPAに報告し、IPA担当者の指示に従い、委託事業を一時中断するなどの必要な措置と共に契約に基づく対処を行うこと。

8. 留意事項

- 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こと。
- 受託事業者は、契約後、具体的な作業計画を立案し、IPA 担当者の承認を得ること。
- 受託事業者は、各調査項目について、調査が一定程度終了したものから随時 IPA に報告すること。
- IPA から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。
- プロジェクト管理等により、作業計画を明確に定め、作業項目ごとの工程管理を行い、もし作業の遅延等が生じた場合には IPA に報告すること。

[17] https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf

9. 納入関連

9.1 納入期限・納入場所

2022 年 3 月 4 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 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 セキュリティ技術評価部 暗号グループ

9.2 納入物件

以下の報告書を収めた電子媒体（CD-R 又は DVD-R）を納入すること。

(1) 成果報告書 一式
(2) プレゼンテーション資料 一式

＜注＞

・調査の過程で作成したデータには、IPA と行った打合せの議事録と使用した資料、成果報告会の議事録等を含む。
・その他、本調査内で入手したデータ、文献、資料等も併せて提出すること。

10. 検収関連

検収条件

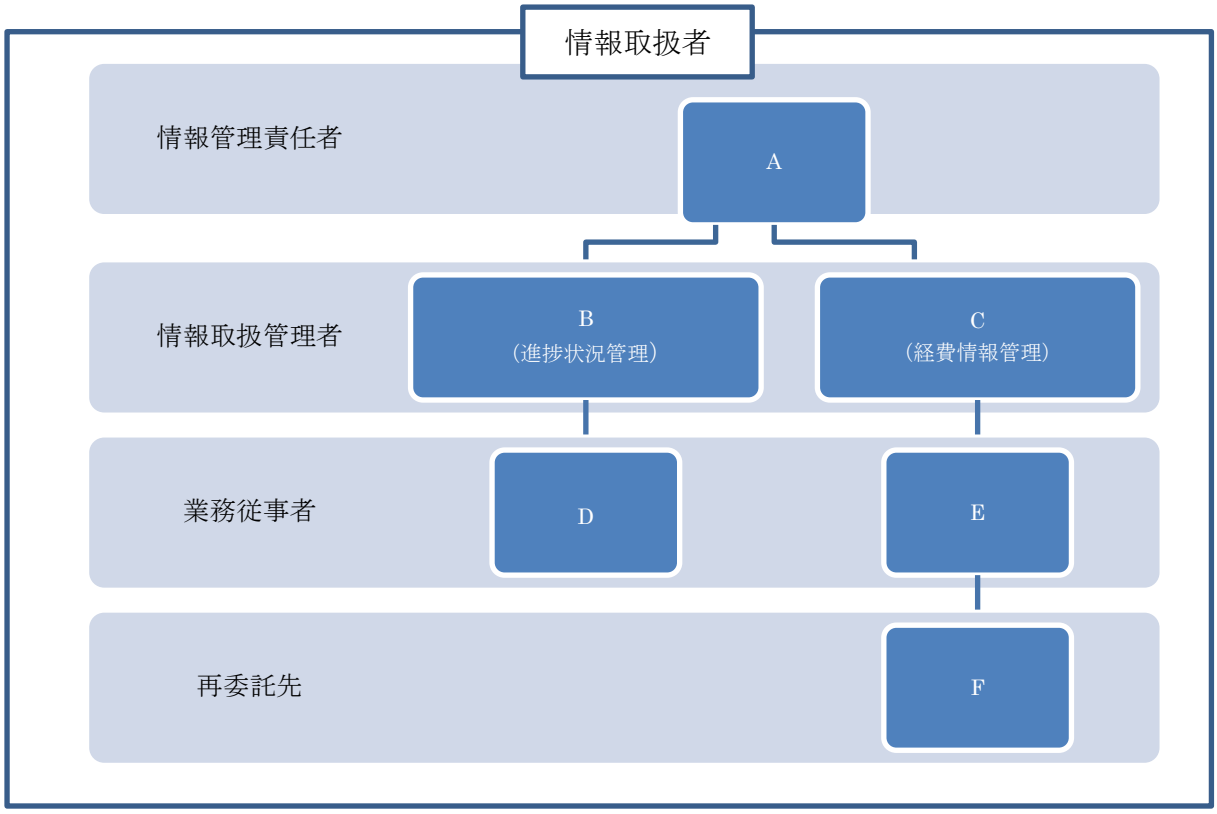
納入物件の内容に関しては、調査内容及び対象に関して本仕様書に示された条件、項目を満たしているかについて確認を行う。また、品質については「2.背景・目的」で示された目的を満たすに十分か否かを基準に判断する。

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) 受託事業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) 本委託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、本委託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) 本委託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。(再委託先も含む)
(※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は、下記のとおり

- 本委託業務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設定し記載すること。

「新たなサイドチャネル攻撃に関する実機調査と評価手順の作成」

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、「新たなサイドチャネル攻撃に関する実機調査と評価手順の作成」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「新たなサイドチャネル攻撃に関する実機調査と評価手順の作成」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、 ・攻撃手法/解析手法の概要 ・実機試験/実機解析の計画概要 ・侵入試験環境/解析試験環境の概要と仕様／性能 ・攻撃シナリオ概要/解析シナリオ概要のサンプル ・攻撃シナリオ/解析シナリオの作成方針 ・無線通信方式 ・成果報告書作成手法と日程 ・成果報告会の開催手法と日程 ・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	「新たなサイドチャネル攻撃に関する実機調査と評価手順の作成」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	サイドチャネル攻撃等の実機調査と評価手順の作成の実施方針等	・中項目1.1【無線通信インターフェースからの漏洩によるサイドチャネル攻撃の実機調査と評価手順の作成】 □小項目1.1.1【攻撃手法の概要】：仕様書4.2.1の業務に関連するサイドチャネル攻撃について、入札者の認識する攻撃手法の概要を記載すること。 □小項目1.1.2【実機試験の計画概要】：仕様書4.2.1の業務の実機試験における試験環境構築（表1手順No.2、手順No.4及び手順No.6それぞれ）、ターゲットデバイスの用意、実施期間等の計画概要について記載すること。 □小項目1.1.3【無線通信方式】：仕様書4.2.1の業務における無線通信方式がIEEE 802.15シリーズ、BlueTooth LE等、IEEE 802.11シリーズより１つ以上選択され記載されていること。（仕様書4.2.1 ①手順No.1【侵入試験準備】[試験対象のマイクロプロセッサの準備] 3番目の・を参照） □小項目1.1.4【侵入試験環境】：仕様書4.2.1の業務における実機による侵入試験環境（表1手順No.2、手順No.4及び手順No.6それぞれ）の概要を記載すること。 □小項目1.1.5【攻撃シナリオのサンプル例示】：仕様書4.2.1 表3【侵入試験項目】から1つ選択して攻撃シナリオ概要のサンプルを最低１つ例示すること。 □小項目1.1.6【攻撃シナリオの作成方針】：仕様書4.2.1の業務の表1手順No.5における攻撃シナリオの作成方針を記載すること。作成方針には、解析アルゴリズムを選択する知見に基づいた説明が含まれていること。 ・中項目1.2【人工知能技術によるサイドチャネル解析手法の実機調査と解析手順の作成】 □小項目1.2.1【解析手法の概要】：仕様書4.2.2の業務に関連するサイドチャネル解析について、入札者の認識する解析手法の概要を記載すること。 □小項目1.2.2【実機解析の計画概要】：仕様書4.2.2の業務の実機解析における解析環境構築（表5手順No.2及

		び手順No.4それぞれ）、解析ターゲットの用意、実施期間等の計画概要について記載すること。 □小項目1.2.3【解析試験環境】：仕様書4.2.2の業務における実機による解析試験環境（表5手順No.2及び手順No.4それぞれ）の概要を記載すること。 □小項目1.2.4【解析シナリオのサンプル例示】：仕様書4.2.2 表7【解析試験項目】の解析シナリオ概要のサンプルを最低１つ例示すること。 □小項目1.2.5【解析シナリオの作成方針】：仕様書4.2.2の業務の表5手順No.3における解析シナリオの作成方針を記載すること。作成方針には、ニューラルネットワークの深層学習の進め方に関する知見に基づいた説明が含まれていること。 ・中項目1.3【成果報告書等の作成の妥当性】 □小項目1.3.1【成果報告書の作成】：成果報告書等の作成手法（構成、作成手順、日程、共通の注意事項への対処方針等）を記載すること。 □小項目1.3.2 【成果報告会の開催】：成果報告会の開催手法（アジェンダ、開催方式、日程、プレゼン資料の提供方法等）を記載すること。
2	組織の経験・能力	・中項目2.1【業務実施能力】 本事業の実施体制及び役割を定めた体制、要員数、役割分担、環境等について記載すること。 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。）を記載すること。 業務に当たる者に欠員が生じた場合に、速やかに同等又はそれ以上の経歴を有する代替者を充てられる体制が整えられているか記載すること。 IT製品の脆弱性の調査や攻撃手法の再現についての実績を有するか記載すること。 本事業を円滑に遂行するためのアカデミア等の外部組織との人的ネットワークや情報源等を有しているかそのネットワークの概要と共に記載すること。
3	業務従事者の経験・能力	・中項目3.1【類似業務管理の経験】 プロジェクトリーダ（複数人可）は過去にITセキュリティに関連する調査、研究、評価、認証、あるいは関連する業務や類似する業務のいずれかの経験があるかを

		経験の概要（分野、時期及び期間、担当の概要等）と共に記載すること。 ・中項目3.2【業務内容に関する専門知識・適格性】 □小項目3.2.1【サイドチャネル攻撃】：「中項目1.1の業務業務」の実施要員にサイドチャネル攻撃に関連する調査、研究、評価、認証、あるいは関連する業務や類似する業務のいずれかをおこなった経験のある要員を含んでいるかを経験の概要と共に記載すること。 □小項目3.2.2【ハードウェア侵入試験】：「中項目1.1の業務」の実施要員にハードウェア侵入試験機器、あるいは類似の機器を業務として利用した経験を持つ要員を含んでいるかを経験の概要と共に記載すること。 □小項目3.2.3【無線LAN等】：「中項目1.1の業務」の実施要員に「Bluetooth、WiFi等の無線LAN、又はISO/IEC 14443等のコンタクトレス通信」等に関連する調査、研究、評価、認証、あるいは関連する業務や類似する業務のいずれかをおこなった経験のある要員を含んでいるかを経験の概要と共に記載すること。 □小項目3.2.4【人工知能技術】：「中項目1.2の業務」の実施要員に人工知能技術に関連する調査、研究、評価、認証、あるいは関連する業務や類似する業務のいずれかをおこなった経験のある要員を含んでいるかを経験の概要と共に記載すること。 □小項目3.2.5【ITセキュリティ評価及び認証制度】:「中項目1.1の業務及び中項目1.2の業務」の実施要員にITセキュリティ評価及び認証制度に知見がある要員を含んでいるかを経験の概要と共に記載すること。
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。

「新たなサイドチャネル攻撃に関する実機調査と評価手順の作成」

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	成果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「4.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.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．サイドチャネル攻撃等の実機調査と評価手順の作成の実施方針等								
	1.1 無線通信インターフェースからの漏洩によるサイドチャネル攻撃の実機調査と評価手順の作成（仕様書 4.2.1）	1.1.1 攻撃手法の概要	中項目 1.1 の業務に関連する攻撃手法の概要が記載されているか。 それは、2.背景・目的の参考文献[SC-1]、[SC-2]、[SC-3]に一貫する内容となっているか。	必須	5		80	
			攻撃手法の概要は、業務の目的達成に効果的か。	任意		10		
		1.1.2 実機試験の計画概要	中項目 1.1 の業務における侵入試験の実施計画が記載されており、実機試験（仕様書 4.2.1 表 1 手順 No.2、手順 No.4 及び手順 No.6 それぞれ）の進め方が説明されているか。	必須	5			
			侵入試験の実施計画における実機試験の進め方は、試験環境構築（仕様書 4.2.1 表 1 手順 No.2、手順 No.4 及び手順 No.6 それぞれ）、ターゲットデバイスの用意、実施期間の点で、業務の目的達成に効果的か。	任意		10		
		1.1.3 無線通信方式(仕様書 4.2.1 ①手順 No.1【侵入試験準備】[試験対象のマイクロプロセッサの準備] 3 番目の・参照)	中項目 1.1 の業務の無線通信方式が IEEE 802.15 シリーズ、BlueTooth LE 等、IEEE 802.11 シリーズより 1 つ以上選択され、名称及び仕様の概要が記載されており、業務の目的に合致するか。	必須	5			
		1.1.4 侵入試験環境	中項目 1.1 の業務の侵入試験環境（仕様書 4.2.1 表 1 手順 No.2、手順 No.4 及び手順 No.6 それぞれ）の概要が記載されており、侵入試験で使用する機器は、仕様書 4.2.1 表 2 の要求する仕様／性能を満たすか。	必須	5			
		1.1.5 攻撃シナリオのサンプル例示	中項目 1.1 の業務の攻撃シナリオ概要のサンプルが記載されており、業務の目的に合致しているか。	必須	5			
			攻撃シナリオ概要が具体的に記載されており、そのシナリオが効果的であることが説明されているか。	任意		15		
		1.1.6 攻撃シナリオの作成方針	中項目 1.1 の業務における攻撃シナリオの作成方針が記載されており、解析アルゴリズムを選択する方針が説明されているか。	必須	5			
			解析アルゴリズムの選択の方針は、解析アルゴリズムの選択に有用な知見に基づいて説明されており、業務の目的達成に効果的か。	任意		15		
	1.2 人工知能技術によるサイドチャネル解析手法の実機調査と解析手順の作成（仕様書 4.2.2）	1.2.1 解析手法の概要	中項目 1.2 の業務に関連する解析手法の概要が記載されているか。 それは、2.背景・目的の参考文献[AI-1]、[AI-2]、[AI-3]に一貫する内容となっているか。	必須	5		75	
			解析手法の概要は、業務の目的達成に効果的か。	任意		10		

		1.2.2 実機解析の計画概要	中項目 1.2 の業務における解析試験の実施計画が記載されており、実機解析環境（仕様書 4.2.2 表 5 手順 No.2 及び手順 No.4 それぞれ）による解析試験の進め方が説明されているか。	必須	5			
			解析試験の実施計画における実機解析の進め方は、解析環境構築（仕様書4.2.2表5手順No.2及び手順No.4それぞれ）、解析ターゲットの用意、実施期間の点で、業務の目的達成に効果的か。	任意		10		
		1.2.3 解析試験環境	中項目 1.2 の業務の解析試験環境（仕様書 4.2.2 表 5 手順 No.2 及び手順 No.4 それぞれ）の概要が記載されており、仕様書 4.2.2 表 6 の要求する機器の性能を満たすか。	必須	5			
		1.2.4 解析シナリオのサンプル例示	中項目 1.2 の業務の解析シナリオ概要のサンプルが記載されており、業務の目的に合致しているか。	必須	5			
			解析シナリオ概要が具体的に記載されており、そのシナリオが効果的であることが説明されているか。	任意		15		
		1.2.5 解析試験の実施方針	中項目 1.2 の業務における解析シナリオの作成方針が記載されており、ニューラルネットワークによる深層学習の方針が説明されているか。	必須	5			
			ニューラルネットワークによる深層学習の方針は、深層学習を進めることに有用な知見に基づいて説明されており、業務の目的達成に効果的か。	任意		15		
	1.3 成果報告書等の作成の妥当性	1.3.1 成果報告書の作成	成果報告書の作成手法が記載されているか。	必須	5		20	
			作成手法、日程等に無理がなく、実現性はあるか。	任意		5		
		1.3.2 成果報告会の開催	成果報告会の開催手法が記載されているか。	必須	5			
			開催手法、日程等に無理が無く、実現性はあるか。	任意		5		

2 組織の経験・能力								
	2.1 業務実施能力	・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。 ・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。）が提出されているか。	必須	5		20	
		・業務に当たる者に欠員が生じた場合は、速やかに同等又はそれ以上の経歴を有する代替者を充てられる体制が整えられているか。	必須	5			

			・IT 製品の脆弱性の調査や攻撃手法の再現についての実績を有する旨が記載されているか。	必須	5			
			・本事業を円滑に遂行するためのアカデミア等の外部組織との人的ネットワークや情報源等を有している旨が記載されているか。	任意		5		
3　業務従事者の経験・能力								
	3.1 類似業務管理の経験		プロジェクトリーダ(複数人可)は過去に IT セキュリティ分野に関連する調査、研究、評価、認証、あるいは関連する業務や類似する業務のいずれかの経験がある旨が記載されているか。	必須	5		20	
			プロジェクトリーダ(複数人可)の管理経験はサイドチャネル攻撃、ハードウェア侵入試験、暗号アルゴリズム実装に関連する業務の遂行管理に有効であることが経験した分野や最近の技術動向への対応の観点など、具体的に記載されているか。	任意		15		
	3.2 業務内容に関する専門知識・適格性	3.2.1 サイドチャネル攻撃	中項目 1.1 の業務の実施要員において、サイドチャネル攻撃に関連する調査、研究、評価、認証、あるいは関連する業務や類似する業務のいずれかをおこなったことのある要員の経験について記載されているか。	必須	5		100	
			中項目 1.1 の業務の実施要員のサイドチャネル攻撃に関連する経験は最近の技術動向を反映して業務を遂行するのに有効であることが、過去 3 年以内の経験など、具体的に記載されているか。	任意		15		
		3.2.2 ハードウェア侵入試験	中項目 1.1 の業務の実施要員において、ハードウェア侵入試験機器、あるいは類似の機器を業務として利用したことのある要員の経験について記載されているか。	必須	5			
			中項目 1.1 の業務の実施要員のハードウェア侵入試験機器、あるいは類似の機器の利用経験は最近の技術動向を反映して業務を遂行するに有効であることが、過去 3 年以内の経験など、具体的に記載されているか。	任意		15		
		3.2.3 無線 LAN 等	中項目 1.1 の業務の実施要員において、「Bluetooth、WiFi 等の無線 LAN、又は ISO/IEC 14443 等のコンタクトレス通信」等に関連する調査、研究、評価、認証、あるいは関連する業務や類似する業務のいずれかをおこなったことのある要員の経験について記載されているか。	必須	5			
			中項目 1.1 の業務の実施要員の「Bluetooth、WiFi 等の無線 LAN、又は ISO/IEC 14443 等のコンタクトレス通信」等に関連する経験は最近の技術動向を反映して業務を遂行するに有効であることが、過去 3 年以内の経験など、具体的に記載されているか。	任意		15		
		3.2.4 人工知能技術	中項目 1.2 の業務の実施要員において、人工知能技術に関連する調査、研究、評価、認証、あるいは関連する業務や類似する業務のいずれかをおこなったことのある要員の経験について記載されているか。	必須	5			

			中項目 1.2 の業務の実施要員の人工知能技術に関連する経験は最近の技術動向を反映して業務を遂行するに有効であることが、過去 3 年以内の経験など、具体的に記載されているか。	任意		15		
		3.2.5 IT セキュリティ評価及び認証制度	中項目 1.1 及び中項目 1.2 の業務の実施要員において、IT セキュリティ評価及び認証制度に知見がある要員の経験が記載されているか。	必須	5			
			中項目 1.1 及び中項目 1.2 の業務の実施要員の IT セキュリティ評価及び認証制度に関する知見は最近の技術動向を反映して業務を遂行するに有効であることが、過去 3 年以内の経験など、具体的に記載されているか。	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		11	11	
					110	216	326	

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 各業務従事者の略歴	各業務従事者の略歴（氏名、所属、役職、学歴、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	
	5.2「情報管理体制図」及び「情報取扱者名簿」	5.2 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文書。 （「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情報取扱者名簿（31 ページ）、情報管理体制図（例）（32 ページ）を参照）	必須	
	5.3 情報管理に対する社内規則	情報セキュリティ対策の遵守方法を実装することを説明する文書（仕様書 7. 情報セキュリティ対策遵守方法を参照）	必須	
	5.4 入札者の概要	・ 入札者の概要の分かる資料	任意	
	5.5 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	
	5.6 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	

VI. 評価手順書

「新たなサイドチャネル攻撃に関する実機調査と評価手順の作成」

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、「新たなサイドチャネル攻撃に関する実機調査と評価手順の作成」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326点、価格点の配分を163点とする。

技術点	326点
価格点	163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	5
A	通常想定される提案としては最適な内容である。	9	6	3
B	概ね妥当な内容である。	4	3	1
C	内容が不十分である。	0	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）	11
	認定基準○（5）（※2）	7
	認定基準○（3～4）（※2）	7
	認定基準○（1～2）（※2）	4
	行動計画（※3）	2
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）	7
	くるみん認定企業（旧基準）（※5）	4
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　セキュリティ技術評価部
暗号グループ　担当者殿

質　問　書

「新たなサイドチャネル攻撃に関する実機調査と評価手順の作成」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、「新たなサイドチャネル攻撃に関する実機調査と評価手順の作成」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　「新たなサイドチャネル攻撃に関する実機調査と評価手順の作成」

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：「新たなサイドチャネル攻撃に関する実機調査と評価手順の作成」

【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	提案書受理票	（本紙）	
⑦	③と④の電子ファイル（CD-R又はDVD-R提出）	1部					

---------- 切り取り ----------

提案書受理番号＿＿＿＿＿＿＿＿＿＿＿＿

提案書受理票

年　　月　　日

件　名　「新たなサイドチャネル攻撃に関する実機調査と評価手順の作成」

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　セキュリティ技術評価部
暗号グループ

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。