セキュリティ製品の有効性検証における
対象製品の募集

公 募 要 領

2022 年 1 月 11 日

独立行政法人**情報処理推進機構**

目 次

1. 概要

1.1. 背景・目的

経済産業省の産業サイバーセキュリティ研究会 WG3 において、信頼できるセキュリティ製品（サービスを含む。以下、単に製品と呼ぶ。）と隠れたニーズを掘り起こし、ビジネスマッチングの場を提供することにより、セキュリティ産業の発展を目指すとしている[1]。新型コロナウイルス感染拡大を契機に急速にデジタル化・IT化への期待が進む一方で、サイバー攻撃の脅威も日々洗練されており、セキュリティ製品への期待も高まっている。成熟したセキュリティ製品市場において海外製の製品が高いシェアを有している現在、日本で開発された新たなセキュリティ製品の市場参入を促進するためには、サイバー攻撃の脅威や対策動向等を踏まえ、これから重要性が高くなると考えられる製品分野を明らかにする必要があるとしている。また、その分野に該当する日本で開発されたセキュリティ製品について、有効性検証・実環境における試行導入検証を実施し、その内容を発信することで、ユーザが日本で開発された製品を選定しやすい環境を構築するとしている。

これを受けて独立行政法人情報処理推進機構（以下「IPA」という。）は、実際にセキュリティ製品を検証し、結果を公表する「セキュリティ製品の有効性検証」の仕組みの構築に資する情報の整理を行う予定である。これに向けて、2019 年 9 月に立ち上げた「サイバーセキュリティ検証基盤構築に向けた有識者会議[2]（以下「有識者会議」という。）」において、検証の具体的な試行を行うこととし、検証対象となる製品分野、検証方法などについて検討を進めてきた。2019 年度の事業では、製品の有効性検証体制や手続き、評価結果の公開などにおける課題やあるべき姿を抽出することを目的に試行的な検証を行った。また、2020 年度の事業では、ここまでに得られた知見に基づいて、公平性を確保しながら製品公募・対象製品選定を実施する仕組み、効率的な有効性検証の仕組み及び検証結果公表等の仕組みから成るサイバーセキュリティ検証基盤を構築した。またこの基盤を試行的に運用して、検証対象候補の製品を公募しその中から対象製品を選定して検証を行った。加えて、本基盤で検証するセキュリティ製品の市場参入促進に有効な仕組みの検討を行い、また 2019 年度に作成した「試行導入・導入実績公表の手引き」を改良した。

今年度は、昨年度構築した基盤を運用して検証対象候補製品を公募し、その中から対象製品を選定して検証を行う。今般、検証の題材としてご協力いただける製品を募集することとなった。

1.2. 公募の内容

今年度の試行的な検証の題材としてご協力いただける製品を募集する。製品に対して、別途選定した検証者が製品の有効性を検証し、検証結果を公表する。

1.3. スケジュール概観

本公募のスケジュール概観を表 1 に示す。

表 1 スケジュール概観

イベント	スケジュール
公募期間	2022 年 1 月 11 日（火） ～ 2022 年 1 月 21 日（金）
質問の受付 ※詳細は 4.5 を参照のこと。	2022 年 1 月 11 日（火） ～ 2022 年 1 月 14 日（金） 17 時 00 分まで
応募書類の受付期間 ※詳細は 4.4 を参照のこと。	2022 年 1 月 17 日（月） ～ 2022 年 1 月 21 日（金） 17 時 00 分まで
審査期間	2022 年 1 月 24 日（月） ～ 2022 年 1 月 31 日（月）
ヒアリング	2022 年 1 月 27 日（木） ～ 2022 年 2 月 1 日（火） （1 者あたり 15～30 分程度を予定） ※ IPA が必要と判断した応募者に対してのみ実施する。
採択結果の通知	2022 年 2 月 1 日（火）頃（予定）
検証実施期間	2022 年 2 月上旬 ～ 2022 年 3 月上旬 （予定）

[1] https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/pdf/004_03_00.pdf
[2] https://www.ipa.go.jp/security/economics/kensyokiban2019.html

2. 応募資格

検証製品の応募者は、以下の要件を満たすものとする。

(1) 法人格を有していること。
(2) 日本国内に開発拠点を有していること。さらに、応募製品はこの拠点で製品開発(あるいは技術開発、製品企画等)されたものであること。
(3) 応募製品は2017年1月以降に新規に市販された製品であること。ただし、販売元の関係会社等への移転、製品名称の変更、製品のバージョンアップなどは新規の市販とは認めない。
(4) 効率的な試行検証の実施のために、検証者及びIPAとの連絡体制を構築すること。試行検証に関わるメンバーのリストを作成し、連絡の情報伝達順位を明確化すること。
(5) 応募製品の技術・機能等を正しく理解したうえで検証方式を策定することを目的として、検証者及びIPAに対して、応募製品の技術責任者、開発責任者等を知らせ、必要に応じて相談できるようにすること。
(6) 別紙2暴力団排除に関する誓約事項について、誓約する者であること。

3. 応募書類作成要領

応募者は、仕様書(別紙 1)に基づいて応募書類を作成すること。

3.1. 応募用紙への記載事項

応募者は、仕様書(別紙1)の項目内容について、要求内容を十分に咀嚼した上で記載及び応募すること。

3.2. その他留意事項

(1) 応募用紙及び添付資料を、電子ファイルで提出すること。電子ファイルは Microsoft Office 互換形式、もしくは PDF 形式で作成すること。ただし、これに拠りがたい場合は 4.3 の担当部署まで申し出ること。
(2) 記入にあたっては日本語で正確に記述すること。
(3) 文字の大きさは 10 ポイント以上とする。
(4) 書式設定は、用紙サイズは A4 縦置き、横書き、左右に 19mm 以上の余白を設けること。
(5) 文中の特殊な造語、略語、専門用語については、正式名称がある場合はそれとともに、判りやすい定義を初出の箇所に記述すること。

4. 応募要領

応募者は、この公募要領に基づいて応募書類を作成し、これを提出期限内に提出しなければならない。また、採択決定日前日までの間において IPA 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。

4.1. 提出書類

(1) 提出する書類

応募に際して提出する書類(以下、応募書類と略記。)は以下のとおりとする。なお、所定の様式に従って作成すること。

No.	提出書類		部数
①	応募用紙(電子媒体)	【様式 1】(別ファイル参照)	1 部
②	応募用紙添付資料(電子媒体)		1 部

(2) 提出された応募書類に係る秘密の保持

応募書類は検証製品の採択及び採択後の検証作業の為にのみ用い、IPA 及び委託事業者において厳重に管理する。

取得した個人情報については、採択のために利用するが、特定の個人を識別しない状態に加工した統計資料等に利用することがある。

提供された個人情報は、上記の目的以外で利用することはない。(ただし、法令等により提供を求められた場合を除く。)

（注意事項）
提出された応募書類の作成に要した経費については支払わない。また、受理した応募書類は採択結果に関わらず返却しない。

4.2. 提出期限
提出書類の受付期間及び提出期限は次のとおり。
（1）受付期間
2022 年 1 月 17 日(月)から 2022 年 1 月 21 日(金)
（2）提出期限
2022 年 1 月 21 日（金） 17 時 00 分必着。
上記期限を過ぎた応募用紙等はいかなる理由があっても受け取らない。

4.3. 提出先
本事業の委託事業者である三菱総合研究所の下記担当部署に、4.4 の提出方法で提出すること。
[担当部署]
〒100-8141
東京都千代田区永田町 2-10-3
株式会社三菱総合研究所
デジタル・イノベーション本部 サイバーセキュリティ戦略グループ 担当：篠原、江連、須田
E-mail：ipa-kensyo_kiban@ml.mri.co.jp
TEL：03-6858-3578

4.4. 提出方法
応募用紙及び添付書類の電子媒体を以下の方法で提出すること。
（1）ファイル転送サービスによる提出
応募用紙及び添付書類の電子媒体は、委託事業者である株式会社三菱総合研究所が用意するファイル転送サービスによる提出を行うこと。

応募用紙及び添付書類の提出に際して必要となる情報は、事前に応募希望者に対して連絡する。提出に必要な情報を事務局から連絡するために、4.3 の担当部署まで電子メールによりファイル転送サービスの情報を希望する旨を連絡すること。この際、電子メールの件名を「ファイル転送サービスの希望」とし、本文に担当者の所属・氏名・電子メールアドレス・連絡先電話番号を記入すること。

4.5. 応募に関する質問の受付等
（1）質問の方法
質問書（別紙 3)に所定事項を記入の上、4.3 の担当部署まで電子メールにより提出すること。
（2）受付期間
2022 年 1 月 11 日(火)から 2022 年 1 月 14 日(金)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。

5. 審査方法等
5.1. 審査方法
採択にあたっては、以下の手順に従い応募内容の審査を実施し決定する。
（1）書類審査
応募内容について、応募用紙等の書類審査を事務局にて実施し、検証対象候補製品を選定する。
（2）ヒアリング
IPA が必要と判断した応募者に対してヒアリングを実施する。ヒアリングには、事務局のほか別途設置した有識者会議の構成員が参加する。ヒアリングでは、応募内容に関する説明の後、質疑応答に対応すること。
日時：2022 年 1 月 27 日（木） ～ 2022 年 2 月 1 日（火）（1 者あたり 15～30 分程度を予定）
※ ヒアリング日時は事務局より別途指定する。

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、応募内容を熟知した実施責任者等が対応すること。

(3) 採択結果の決定及び通知について
(1)で選定された検証対象候補製品について、別途設置した有識者会議にて厳正に審査の上、検証対象製品を採択する。

いずれの応募についても応募内容が要件を満たさない場合は、採択を見合わせる場合がある。
採択結果については、2022 年 2 月 1 日(火)頃に各応募者に通知する。

なお、下記を含む審査に係る情報の公開・公表、審査に関しての問合せには応じない。
(1) 書類審査の審査基準
(2) 検証対象候補製品の審査基準、検証対象製品の採択基準
(3) 応募製品に関する情報
(4) 応募者に関する情報
(5) 検証対象候補製品に関する情報
(6) 採択製品に関する情報

5.2. 採択件数
種別 A と種別 B で合計 2 製品を採択予定である。

6. その他

(1) 応募者は、提出した応募用紙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) 製品選定にあたって、必要に応じて応募者に対してヒアリング等を実施する場合がある。
(3) 応募できる製品は 1 企業・団体について 1 製品とする。
(4) 1 企業・団体から複数の応募があった場合、応募製品とする 1 製品について事務局から問合せる。
(5) 本試行検証において新たに作成された成果物は原則、IPA に帰属するものとする。
(6) 本試行検証にて発生した事故・トラブル・機器の破損やその他の損害については、IPA の責めに帰す場合を除き、IPA は責任を負いかねる。
(7) 本試行検証における個人情報の取扱いについては、下記「個人情報の取扱いについて」、(別添 1)個人情報の取扱いに関する特則、(別添 2)特定個人情報の取扱いに関する特則に準ずるものとする。

個人情報の取扱いについて

- 株式会社三菱総合研究所は、2003 年 1 月 8 日にプライバシーマークの付与・認定を受けております。応募者及び質問者の個人情報は、株式会社三菱総合研究所が定める「個人情報保護方針」に則り、適切な保護措置を講じ、厳重に管理いたします
- 応募者及び質問者の個人情報は IPA 事業「2021 年度サイバーセキュリティ検証基盤の運用」の一環として、検証業務の管理及び諸連絡のために利用させていただきます。それ以外の目的で個人情報を利用する場合は、改めて目的をお知らせし、同意を得るものといたします。
- 株式会社三菱総合研究所にご提供頂いた個人情報は、製品選定及び事務連絡のために、IPA に提供します。
- 当該業務終了後は、株式会社三菱総合研究所管理分においては、株式会社三菱総合研究所が責任を持って廃棄します。
- 個人情報に関する株式会社三菱総合研究所の連絡先
  ・個人情報保護管理者：株式会社三菱総合研究所　取締役執行役員　野邊　潤
  （連絡先：03-5157-2111、E-mail：privacy@mri.co.jp）
  ・個人情報の取扱いに関するご連絡先、苦情・相談窓口
  ※開示、訂正、利用停止等のお申し出は、下記窓口までご連絡ください。

株式会社三菱総合研究所　広報部　　電話：03-6705-6004　FAX：03-5157-2169
E-mail：prd＠mri.co.jp　URL：https://www.mri.co.jp/request/
お問い合わせ番号：PMS001365

7.　本事業の実施主体

本事業は、以下の IPA 担当部署が実施主体である。

[IPA 担当部署]
〒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 17 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　セキュリティ分析グループ　担当：島田、白石
TEL：03-5978-7530

（別添 1）

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

（別添2）

特定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、以下に掲げる用語の意義は、次の各号に定めるところによるものとする。

一「個人情報」とは、乙が取扱う個人情報（「個人情報の保護に関する法律」（平成 15 年法律第 57 号、以下「個人情報保護法」という。）第2条第1項に規定する個人情報であって、生存する個人に関する情報であり、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。）をいう。

二「個人番号」とは、請負業務において謝礼金受領者の個人番号（「行政手続における特定の個人を識別するための番号の利用等に関する法律」（平成 25 年法律第 27 号。以下「番号法」という。）第7条第1項又は第2項の規定により、住民票コードを変換して得られる番号であって、当該住民票コードが記載された住民票に係る者を識別するために指定されるものをいう。）をいう。

三「特定個人情報」とは、個人番号をその内容に含む個人情報をいう。

四「従業員」とは、乙の組織内にあって直接又は間接に乙の指揮監督を受けて乙の業務に従事している者をいい、雇用関係にある従業者（正社員、契約社員、嘱託社員、パート社員、アルバイト社員等）のみならず、乙との間の雇用関係にない者（取締役、監査役等）を含む。

五「第三者」とは、甲及び乙（甲及び乙の役員・従業員、及び本件業務に係る乙の再請負先組織を含む。）以外の全てのものをいう。

（責任者の選任）

第 2 条　乙は、特定個人情報を取扱う場合において、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。

（特定個人情報の収集）

第 3 条　乙は、請負業務遂行のため特定個人情報を収集するときは、「個人情報保護法」及び「番号法」その他の法令に従い、適切か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、特定個人情報の開示・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、請負業務に従事する従業員以外の者に、特定個人情報を取り扱わせてはならない。

3　乙は、請負業務に従事する従業員のうち特定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、特定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。

（持ち出しの禁止）

第 5 条　乙は、特定個人情報を、乙の事務所の外へ持ち出してはならない。ただし、請負業務実施にあたり、必要な手続きを経て再請負契約を締結する場合を除く。

（目的外使用の禁止）

第 6 条　乙は、特定個人情報を請負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 7 条　乙は、甲の事前の書面による承諾を得ることなしに、特定個人情報を複写又は複製してはならない。ただし、請負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。

（特定個人情報の管理）

第 8 条　乙は、特定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、特定個人情報に対する不正アクセスまたは特定個人情報の紛失、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、乙における特定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特定個人情報について、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。

（再請負の取扱い）
第 9 条 乙が甲の承諾を得て請負業務を第三者に再請負する場合は、十分な特定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特定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。又、乙は、甲から要求を受けたときは、当該契約書の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逃れない。乙は自らの責任において、再請負先に対して、本契約で定められている乙の義務と同等の義務を課すとともに、必要かつ適切な監督を行わなければならない。

（報告、資料の提出及び監査）
第 10 条 甲は、乙における本特則の遵守状況を確認するために必要な限度において、乙に対する書面による事前の通知により、報告、資料の提出又は監査の受入れを求めることができる。この場合、乙は、請負業務の遂行に支障が生ずるときその他の正当な理由がある場合を除き、甲の求めに応じるものとする。
2 前項の報告、資料の提出又は監査の受入れにあたり、乙は甲に対して、乙の営業秘密（不正競争防止法第2条第6項に定める営業秘密をいう。）に関する秘密保持義務等について定めた秘密保持契約の締結を求めることができるものとする。
3 甲は、監査のために乙の事業所又はコンピュータセンター等への入館が必要となる場合、乙所定の事務処理及び入退館等に関する規則に従うものとする。

（改善の指示）
第 11 条 甲は、前条による報告、資料の提出を受け、又は監査を実施した結果、乙において特定個人情報の安全管理措置が十分に講じられていないと認めたときは、乙に対し、その理由を書面により通知かつ説明した上で、安全管理措置の改善を要請することができるものとする。
2 乙は、前項の要請を受けたときは、安全管理措置の改善について甲と協議を行わなければならない。

（事故発生時の対応）
第 12 条 乙において特定個人情報に対する不正アクセス又は特定個人情報の紛失、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乙に提示しなければならない。
2 前項の場合において、甲及び乙が講ずべき措置については、安全管理措置の実施状況、事故によって特定個人情報の本人が被る権利利益の侵害の状況、事故の内容及び規模等に鑑み、甲乙協議の上、定めるものとする。
3 第 1 項の事故が乙の本契約の違反に起因する場合において、甲が、被害を被った本人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。
4 第 1 項の事故が乙の本契約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 2 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わなければならない。

（特定個人情報の返却等）

第 13 条　乙は、甲から要請があったとき、又は、請負業務が終了（本契約解除の場合を含む。）したときは、特定個人情報（その複製物を含む。）の全部を本人に返却し、記録媒体から削除し、復元できない状態にしなければならない。

2　乙は、前項による特定個人情報の削除を実施した場合には、その証明書を本人に提出することとする。

以上

【別紙 1】

仕様書

セキュリティ製品の有効性検証における
対象製品の募集

実施内容（仕様書）

独立行政法人**情報処理推進機構**

実施内容（仕様書）

1. 件名

セキュリティ製品の有効性検証における対象製品の募集

2. 背景・目的

経済産業省の産業サイバーセキュリティ研究会 WG3 において、信頼できるセキュリティ製品（サービスを含む。以下、単に製品と呼ぶ。）と隠れたニーズを掘り起こし、ビジネスマッチングの場を提供することにより、セキュリティ産業の発展を目指すとしている[3]。新型コロナウイルス感染拡大を契機に急速にデジタル化・IT化への期待が進む一方で、サイバー攻撃の脅威も日々洗練されており、セキュリティ製品への期待も高まっている。成熟したセキュリティ製品市場において海外製の製品が高いシェアを有している現在、日本で開発された新たなセキュリティ製品の市場参入を促進するためには、サイバー攻撃の脅威や対策動向等を踏まえ、これから重要性が高くなると考えられる製品分野を明らかにする必要があるとしている。また、その分野に該当する日本で開発されたセキュリティ製品について、有効性検証・実環境における試行導入検証を実施し、その内容を発信することで、ユーザが日本で開発された製品を選定しやすい環境を構築するとしている。2019 年度の事業では、製品の有効性検証体制や手続き、評価結果の公開などにおける課題やあるべき姿を抽出することを目的に試行的な検証を行った。また、2020 年度の事業では、ここまでに得られた知見に基づいて、公平性を確保しながら製品公募・対象製品選定を実施する仕組み、効率的な有効性検証の仕組み及び検証結果公表等の仕組みから成るサイバーセキュリティ検証基盤を構築した。またこの基盤を試行的に運用して、検証対象候補の製品を公募しその中から対象製品を選定して検証を行った。加えて、本基盤で検証するセキュリティ製品の市場参入促進に有効な仕組みの検討を行い、また 2019 年度に作成した「試行導入・導入実績公表の手引き」（以降、「手引き」）を改良した。

今年度は、昨年度構築した基盤を運用して検証対象候補製品を公募し、その中から対象製品を選定して検証を行う。今般、検証の題材としてご協力いただける製品を募集することとなった。

3. 公募する製品について

以下の 2 種類の製品種別（種別 A ／ 種別 B）を募集する。応募者は、どちらの製品種別に対して応募するか、応募用紙で明記すること。

[種別 A]

日本の市場において新規性の高いセキュリティに関する機能を有する製品とする。
種別 A に応募する応募者は応募書類の中で、上記に該当する機能があることを説明するものとする。

種別 A の製品は、上記に該当する機能が応募書類等の説明内容通りであることを検証する対象とする。

[種別 B]

セキュリティ機能に関する優れたユーザビリティ[4]を備えた製品とする。種別 B に応募する応募者は応募書類の中で、該当するユーザビリティを明記するものとする。

種別Bの製品は、上記に該当するユーザビリティが応募書類の説明内容通りであることを、検証する対象とする。この検証のための導入環境（IT 環境）は、民間事業者等のオフィス等を想定した実環境とする。なお、種別Bの製品が想定するユーザであって、ユーザビリティの検証に協力する者（以降、「検証協力ユーザ」）は、種別Bに応募するセキュリティ製品ベンダが用意すること。

種別Bの検証では、検証項目・検証方法・検証実務・検証結果等の検討に、検証協力ユーザの意見を

[3] https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/pdf/004_03_00.pdf
[4] 種別Bの検証で取り上げるユーザビリティは、本仕様書末尾の「7.補足」を参照のこと。

反映すること。応募する製品ベンダは、検証協力ユーザから、下記協力について事前に同意を得たうえで応募すること。

・種別 B の製品を利用する具体的な業務タスクを想定し、そのタスクで検証したいユーザビリティの以下の項目（詳細は、本仕様書 7.補足を参照）について、意見を出すこと。

機能充足性／機能正確性／効率性・運用操作性／習得性／ユーザエラー耐性／その他のユーザビリティの項目

・策定途中の検証項目を確認し、意見を出すこと

・検証途中の結果等を確認し、意見を出すこと

・検証結果の公表に際し、公表内容の選択・表現等の調整に協力すること

なお、種別 A・種別 B の両方において、有識者会議にて重要分野と選定した下記の分野(1)～(4)に該当し、日本国内にて製品開発（あるいは技術開発、製品企画等）された製品を検証対象とする。

(1) 脅威の可視化

エンドユーザーやシステム管理者などが晒されているセキュリティ上の脅威を可視化することに資する製品。下記の機能等を想定する。

① マルウェアの感染などによる不審な内部通信の発生を捉え、通知する

② 通信フローを監視し、定常時とは異なる状況を検知した場合に通知する

本重要分野に関する製品で種別 A に対して応募する場合、以下に示されるような検証項目について検証を実施することが想定される。なお、以下は例示であり、これに限るものではない。応募用紙において、応募製品に対して実施すべき検証項目を説明すること。

- 検知できる脅威や不正通信の種類に関する検証項目
- 検知した脅威や不正通信に関する情報の質・量に関する検証項目
- 脅威や不正通信の検知タイミングに関する検証項目
- 検知した脅威や不正通信の遮断に関する検証項目
- 検知した脅威や不正通信の情報の通知に関する検証項目
- 脅威や不正通信への対応管理機能に関する検証項目

本重要分野に関する製品で種別 B に対して応募する場合、以下に示されるような機能のユーザビリティについて検証を実施することが想定される。なお、以下は例示であり、これに限るものではない。応募用紙において、応募製品に対して検証すべきユーザビリティを説明すること。

- 脅威や通信フローの自動監視・自動検知機能に関するユーザビリティ
- 検知した脅威や不正通信の自動分析機能に関するユーザビリティ
- 脅威分析の結果の優先度付けの機能に関するユーザビリティ

(2) リスクの可視化・緩和

OS、ファームウェア、ソフトウェア等に含まれるリスクを検出し、検出したリスクに対する緩和策の提案や対策の優先度付けを実施することで、リスクの可視化・緩和に資する製品。下記の機能等を想定する。

① 製品を構成しているオープンソースソフトウェア（以下、OSS)に内在する脆弱性の検出とリスク評価を自動で行い、リスクに対する緩和策や対策の優先度を表示する

② 検出されたリスクが内在する OSS を含んだシステム、アプリケーションなどの対策状況を組織単位、ソフトウェア単位などで表示・管理する

本重要分野に関する製品で種別 A に対して応募する場合、以下に示されるような検証項目について検証を実施することが想定される。なお、以下は例示であり、これに限るものではない。応募用紙において、応募製品に対して実施すべき検証項目を説明すること。

- 検出できるリスクの種類に関する検証項目
- 検出したリスクに関する情報の質・量に関する検証項目
- 検出したリスクに対する対策の優先度付けに関する検証項目
- 検出したリスクに関する情報の通知に関する検証項目
- 検出したリスクへの対応管理機能に関する検証項目

- 新たな脆弱性が検出できるまでの期間に関する検証項目

本重要分野に関する製品で種別 B に対して応募する場合、以下に示されるような機能のユーザビリティについて検証を実施することが想定される。なお、以下は例示であり、これに限るものではない。応募用紙において、応募製品に対して実施すべき検証項目を説明すること。

- リスクの自動検出機能に関するユーザビリティ
- 検出したリスクの自動分析機能に関するユーザビリティ
- 検出したリスクの優先度付けの機能に関するユーザビリティ

(3) データ保護

IT 資産上の様々なデータを、漏えい、改ざん、盗聴等のセキュリティ脅威から保護する製品。下記の機能等を想定している。

① IT 資産上のデータを自動的に暗号化し、保護する
② IT 資産上のデータを自動的にバックアップし、必要な時にバックアップデータを即座に復元する

本重要分野に関する製品で種別 A に対して応募する場合、以下に示されるような検証項目について検証を実施することが想定される。なお、以下は例示であり、これに限るものではない。応募用紙において、応募製品に対して実施すべき検証項目を説明すること。

- 保護できるデータの種類に関する検証項目
- 保護できるデータの単位に関する検証項目
- データ保護のタイミングに関する検証項目
- 保護データの管理機能に関する検証項目

本重要分野に関する製品で種別 B に対して応募する場合、以下に示されるような機能のユーザビリティについて検証を実施することが想定される。なお、以下は例示であり、これに限るものではない。応募用紙において、応募製品に対して検証すべきユーザビリティを説明すること。

- データの自動保護機能に関するユーザビリティ
- データの暗号化・復号化に係る機能に関するユーザビリティ

(4) ID/アクセス管理

IT 資産に対するアクセスに対して、利用者の ID や関連する情報（端末情報、OS、アプリ、バージョン、セキュリティパッチ等）に基づいてその信頼性を判断し、認証する製品。下記の機能等を想定している。

① アクセスした端末の真正性（正当性）を判断し、不正な端末の接続を拒否・通知する
② IT 資産におけるアクセスログや操作ログ等を自動で収集し、動作の正当性を検証する
③ 利用者IDを登録・修正・削除する
④ 利用者のアクセス権を設定・修正する
⑤ 利用者を認証（認証の支援も含む）する

本重要分野に関する製品で種別 A に対して応募する場合、以下に示されるような検証項目について検証を実施することが想定される。なお、以下は例示であり、これに限るものではない。応募用紙において、応募製品に対して実施すべき検証項目を説明すること。

- 検出できるアクセスの種類に関する検証項目
- 不正アクセスの検出・接続拒否に関する検証項目
- 検出した不正アクセスに関する情報の質・量に関する検証項目
- 検出した不正アクセスに対する対策の優先度付けに関する検証項目
- 検出した不正アクセスに関する情報の通知に関する検証項目
- 正当な ID や IT 資産情報の管理に関する検証項目

本重要分野に関する製品で種別 B に対して応募する場合、以下に示されるような機能のユーザビリティについて検証を実施することが想定される。なお、以下は例示であり、これに限るものではない。応募用紙において、応募製品に対して検証すべきユーザビリティを説明すること。

- 不正アクセスの自動検出機能に関するユーザビリティ
- 検出した不正アクセスの自動分析機能に関するユーザビリティ
- 検出した不正アクセスの優先度付け機能に関するユーザビリティ

なお、当該製品は、有識者会議にて選定した下記のキーワードに関連するものであることが望ましい。

① ゼロトラスト対応
② IoT

また本事業の主旨から、商用利用可能な OSS や無償ツール等は応募の対象外とする。既に市販しているものに限る。なお、種別Aと種別Bのいずれも当該製品を他の製品と比較する検証は行わない。

4. 実施内容

4.1 検証について

(1) 検証の目的

過年度事業において構築した基盤を運用して検証対象候補製品を公募し、その中から対象製品を選定して有効性検証を行う。

(2) 検証で応募者が実施すべき作業内容

① 検証方法の調整

- 別途選定した検証者と、どのような検証項目をどのような方法で検証するか協議し、検証方法について合意を得る。
- 【種別 B の製品のみ】検証協力ユーザの意見も確認し、検証協力ユーザの利用を想定した業務タスクで検証すること。また、検証項目の設定においては「試行導入・導入実績公表の手引き」を参照して行うこと。

② 検証の実施

- 応募者は検証者が指定する環境に、指定された期間対象製品を設置・導入し、検証実施に必要な設定・調整作業を実施する。
- 【種別 B の製品のみ】検証協力ユーザの意見も確認すること。なお、検証環境は民間事業者等のオフィス等の IT 環境を想定した実環境とすること。

③ 検証結果の公表内容の調整

- ②の検証結果の評価については、有識者会議が行う。
- 検証結果は応募者にフィードバックされる。有識者会議・検証者、応募者及び検証協力ユーザ（種別 B の製品のみ）が同意した内容についてのみ公表する。
- 上記調整した公表内容の公表の仕方、応募者の広報活動への利用方法などについては別途協議の上決定する。
- 【種別 B の製品のみ】検証結果のまとめにおいては「手引き」を参照して行うものとし、併せて検証項目の設定等の作業において「手引き」がどの程度有用であったか、意見を出すこと。

(3)【種別 B の製品のみ】検証で検証協力ユーザが実施すべき作業内容

① 検証方法の調整

- 別途選定した検証者及び製品ベンダとともに、策定途中の検証項目を確認して、自らが利用したい環境や業務タスク等について意見を出す。

② 検証の実施

- 検証途中の結果等を確認し、意見を出す。

③ 検証結果の公表内容の調整

- 検証結果の公表に際し、その内容調整に協力する。

5. 応募者に求める協力事項

応募者は本検証の実施にあたって、下記事項について協力すること。

(1) 対象製品、付属物、検証用データ、利用環境等、検証に関して検証者が必要とする物品等を無償で提供すること。

(2) 製品のインストール、初期設定、操作・利用の指導、検証作業中に判明する不明事項への問合せ、検証作業に対する支援などの役務を、検証期間中（2022 年 2 月から 2022 年 3 月上旬 （予定））の間、無償で、

必要に応じて即座に提供すること。
(3) 本検証を効率的に実施するために、検証者及び IPA との連絡体制を構築すること。
(4) 応募製品の技術・機能等を正しく理解したうえで検証方式を策定することを目的として、検証者及び IPA に対して、応募製品の技術責任者、開発責任者等を知らせ、必要に応じて相談できるようにすること。
(5) 本検証の実施にあたって、応募者と検証者、IPA との間で秘密保持契約の締結を求めないこと。
(6)【種別 B の製品のみ】検証協力ユーザを用意し、検証協力ユーザから協力の合意を得ること。また、検証項目・検証方法・検証実務・検証結果等の検討に、検証協力ユーザの意見を反映すること。

6. 検証実施期間
2022 年 2 月から 2022 年 3 月上旬（予定）

7. 補足
種別Bのユーザビリティ検証は、検証協力ユーザの具体的な業務タスクを設定したうえで、特定のセキュリティ機能について検証する。また検証は、
・その製品の使用環境
（例）一般事務部門のオフィス環境／サーバールーム／SOC、など
・対象ユーザ
（例）一般事務部門の社員／ITシステム運用部門のオペレータ／SOC 等セキュリティ部門の技術者、など
を想定したうえで行う。
取り上げるユーザビリティの項目は次の 6 項目であり、応募の際に応募ベンダが選択（複数選択可）するものとする。
①機能充足性
設定した業務タスクを実施するために必要なセキュリティ機能が、その製品によってすべて提供されており不足がないこと。それによって、対象製品を用いることで対象ユーザが業務タスクを完了できること。
②機能正確性
設定した業務タスクを実施する上で、対象製品の提供するセキュリティ機能が正しく（必要な精密さで）動作すること（例：脅威の見逃しや誤検知がないこと）。また、機能の選択、設定、運用が正しくできる、こと。それによって、対象ユーザが正確に業務タスクを実施できること。
③効率性・運用操作性
設定した業務タスクを実施するために対象製品の提供するセキュリティ機能を利用することで、ユーザに過度な負担が掛からないこと。例えば十分な自動化、機能の統合、状態の可視化、操作ガイドの呈示、ヘルプデスクへのリンク等が提供されており、対象ユーザが操作に時間を掛けずとも、効率的に業務タスクが実施できること。
④習得性
設定した業務タスクを実施するためのセキュリティ機能の操作方法は、理解・習得が容易であること。それによって、対象ユーザがすぐに操作できるようになること。
⑤ユーザエラー耐性
ユーザのエラー操作（誤操作）に対し耐性があり、例えば、誤操作の可能性を警告する／状態の復旧が容易である／影響を最小限に抑える、などの機能を備えていること。それによって、対象ユーザが誤操作を起こしても、被るロス（時間、業務中断等）が最小限に抑えられること。
⑥その他のユーザビリティの項目
対象製品は、対象ユーザに上記①～⑤以外の便益を提供すること。

【別紙 2】

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、応募書類の提出をもって誓約します。

【別紙 3】

2022 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　セキュリティ対策推進部　セキュリティ分析グループ　担当者宛

株式会社三菱総合研究所
デジタル・イノベーション本部　サイバーセキュリティ戦略グループ　担当者宛

質 問 書

「セキュリティ製品の有効性検証における対象製品の募集」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。