往訪閲覧・縦覧のデジタル化に関する技術カタログ掲載技術の応募フォームにおける質問事項一覧

【募集する技術】

本公募では「申請者が規制所管省庁等で管理している情報をオンラインで閲覧・縦覧することを可能とする、往訪閲覧・縦覧のデジタル化を実現することができる製品・サービス」を募集します。

なお、申請者が閲覧・縦覧に使用する端末は、規制所管省庁等が所有・管理する閲覧・縦覧専用の共同利用型端末や、申請者が所有・管理する個人用端末を想定しています。それぞれでオンラインでの閲覧・縦覧を実現する方法が異なる場合がありますので、御留意ください。

【募集期間】

2023年10月６日（金）～2023年11月６日（月）

本フォームへの回答をもとに、「技術カタログ」を取りまとめ、デジタル庁ホームページで公表予定です。回答いただいた内容は、原則としてそのまま技術カタログの内容として公表します。

（全84問）

【募集対象】

往訪閲覧・縦覧のデジタル化後の業務は「データ保存」、「申請受付」、「情報開示」、「開示完了」の４つのプロセスに分けられます。

今回募集する技術については、「情報開示」プロセスにおける以下２つの機能を必須とします。

・　閲覧・縦覧開始時の本人認証機能

-なりすまし防止機能

・　開示情報に係るセキュリティ対策機能

-個人情報の保護機能

-のぞき見防止機能

-複写抑止・防止機能

なお、上記全ての機能を有している技術であることが望ましいですが、一部の機能のみを有している技術でも応募いただくことは可能です。

【御回答いただくにあたっての留意点】

諸手続きの都合上、回答内容の変更には時間を要しますため、回答内容の誤り等に十分に御留意の上で御回答ください。

なお、回答提出後の回答内容の変更につきましては、以下の【連絡先】まで御連絡ください。

また、複数の製品・サービスの申請を行う場合には、応募する製品・サービスごとに申請ください。

募集要領に記載の応募条件は、今後見直す可能性があります。

【連絡先】

株式会社三菱総合研究所（再委託先：KPMGコンサルティング株式会社）

〒100－8141　東京都千代田区永田町二丁目10番３号

デジタル庁技術カタログ公募担当

E-mail：catalog-inquiry_atmark_ml.mri.co.jp

迷惑メール防止のため、「@」を「_atmark_」と表示しています。メールをお送りになる際には、「_atmark_」を「@」（半角）に直してください。

E-mailでのお問合せをお願いいたします。

お電話・御来訪等でのお問合せは受け付けておりませんので御了承ください。

法人情報

1. 法人名（正式名称）【必須】

個人事業主・フリーランス等の法人に属さない方は屋号や氏名を記載してください。

（例）

株式会社三菱総合研究所

2. 法人名のフリガナ【必須】

法人名のフリガナを全角カタカナで記載してください。

なお、法人格のフリガナは不要です。

（例）

ミツビシソウゴウケンキュウショ

3. 法人設立国【必須】

法人の設立国を選択してください。設立が日本国以外の場合は、「その他」を選択の上、国名を記載してください。

個人事業主・フリーランス等の法人に属さない方は「日本国」を選択してください。

□ 日本国

□ その他

4. 法人番号【必須】

法人番号を半角数字（13桁）で記載してください。

個人事業主・フリーランス等の法人に属さない方は「0000000000000」を記載してください。

（例）

8000012010038

5. 従業員数【必須】

個人事業主・フリーランス等の法人に属さない方は「法人に属していない」を選択してください。

○ 50人以下
○ 50人超100人以下
○ 100人超300人以下
○ 300人超
○ 法人に属していない

6. 資本額【必須】

個人事業主・フリーランス等の法人に属さない方は「法人に属していない」を選択してください。

○ 5,000万円以下
○ 5,000万円超１億円以下
○ １億円超３億円以下
○ ３億円超
○ 法人に属していない

7. 所在地【必須】

本社所在地を記載してください。

個人事業主・フリーランス等の法人に属さない方は事業所又は自宅住所を記載してください。

なお、自宅住所は都道府県市区町村までの記載でも問題ございません。また一

切の自宅住所の公表を望まない方は「非公表」と記載してください。

（例）

東京都千代田区丸の内XX丁目XX-XX

8. 法人の概要がわかるホームページ・SNS等のURL【必須】

個人事業主・フリーランス等の法人に属さない方でホームページ・SNS等をお持ちでない方は、事業活動や経歴等の参考Webサイト（researchmap等）を記載してください。いずれもお持ちでない方は「無し」と記載してください。

（例）

https(:)//www.xxxx.xxxxx.xxxx

9. 公共調達における事業者登録【必須】

公共調達における事業者登録について、登録済みのものを全て選択してください。「都道府県」、「市区町村」について、１団体でも登録済みのものがありましたら選択してください。

事業者登録をお持ちでない方は「無し」を選択してください。

- □ 中央省庁（全省庁統一資格）
- □ 都道府県
- □ 市区町村
- □ 無し

10. 製品・サービスのサポートエリア【必須】

製品・サービスの販売時及び販売後のサポートエリアを全て選択してください。全国をサポートしている場合は「全国」を選択し、一部の都道府県のみでサポートしている場合は、該当する地方を選択してください。

- □ 全国
- □ 北海道地方

- ☐ 東北地方
- ☐ 関東地方
- ☐ 中部地方
- ☐ 近畿地方
- ☐ 中国地方
- ☐ 四国地方
- ☐ 九州地方

11. 日本における担保的責任財産の概要【必須】

万一、事業者側の過失によってデータ漏洩・破損等の回復不能な損害が生じた際の、損害賠償を実現するために、日本国内に保有している担保的な資産について概要・状況を記載してください。

なお、非公開を希望される場合は「非公開」と回答してください。

（例）

賠責保険：XXXX円相当

不動産：XXXX円相当

現金：XXXX円程度

債権：XXXX円相当

有価証券：XXXX円相当

12. 損害賠償額上限規定の概要【必須】

万一、事業者側の過失によってデータ漏洩・破損等の回復不能な損害が生じた際の、損害賠償に係る製品・サービスの契約上における事業者側の損害賠償額の上限規定について概要を記載してください。

（例）

最後の料金支払いの1年分を上限とする。特別損害は一切補償しない。

製品・サービス情報

13. 製品・サービス名【必須】

（例）

XXXX情報開示・閲覧システム

14. 製品・サービスの型番【任意】

15. 製品・サービスの概要紹介（簡潔に100字まで）【必須】

16. 製品・サービスに関連するホームページ・SNS等のURL【必須】

製品・サービスに関連するホームページ・SNS等がありましたら記載してください。

お持ちでない方は「無し」と記載してください。

（例）

https(:)//www.xxxx.xxxxx.xxxx

17. 製品・サービスの製造業者【必須】

前のセクション「法人情報」で回答いただいた法人が、製品・サービスの製造業者であるかについて選択してください。

○ はい

○ いいえ

18. 製品・サービスの製造業者名【必須】

前の設問で「いいえ」を回答いただいた場合、製品・サービスの製造業者名を記載してください。

（例）

株式会社三菱総合研究所

19. 製品・サービスの製造業者名のフリガナ【必須】

製品・サービスの製造業者名のフリガナを全角カタカナで記載してください。

なお、法人格のフリガナは不要です。

（例）

ミツビシソウゴウケンキュウショ

20. 製品・サービスの製造業者の法人番号【必須】

製品・サービスの製造業者の法人番号を半角数字（13桁）で記載してください。

個人事業主・フリーランス等の法人に属さない場合は「0000000000000」を記載してください。

（例）

8000012010038

21. 製品・サービスの製造業者の所在地【必須】

製品・サービスの製造業者の本社所在地を記載してください。

個人事業主・フリーランス等の法人に属さない場合は事業所又は自宅住所を記載してください。

なお、自宅住所は都道府県市区町村までの記載でも問題ございません。また一切の自宅住所の公表を望まない場合は「非公表」と記載してください。

（例）

東京都千代田区丸の内XX丁目XX-XX

22. 製品・サービスが準拠しているガイドライン・ガイドブック等【任意】

製品・サービスが準拠しているガイドライン・ガイドブック等がありましたら、それらの名称及び発行体を記載してください。

（例）

・製品安全に関する事業者ハンドブック（経済産業省発行）

・協調的なデータ利活用に向けたデータマネジメント・フレームワーク（経済産業省発行）

・IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）（経済産業省発行）

23. 製品・サービスが取得している第三者認証等【任意】

製品・サービスが取得している第三者認証等がありましたら、それらの名称を記載してください。

なお、サイバーセキュリティに係る認証については別途設問を設けておりますので、サイバーセキュリティ以外の取得認証について御回答ください。

（例）

SOCレポート（AICPA/CICA）

必須機能１．閲覧・縦覧開始時の本人認証機能

24. 「閲覧・縦覧開始時の本人認証機能」を有しますか？【必須】

「無」を選択した場合は、次のセクション「必須機能2．開示情報に係るセキュリティ対策機能」に進みます。

○ 有
○ 無

25. どのような方法で閲覧・縦覧開始時の本人認証を行いますか？【必須】

該当する選択肢を選択してください。
なお、１つの製品・サービスで複数の方法を組み合わせて閲覧・縦覧開始時の本人認証機能を実現している場合は、複数選択してください。
該当する方法が選択肢にない場合は、「その他」を選択し、方法を記載してください。

□ 申請者の知識情報（ID・パスワード、PINコード、秘密の質問、等）を利用し本人を認証する
□ 申請者の所持情報（ICカード、ワンタイムパスワード、携帯電話番号（SMS）、等）を利用し本人を認証する
□ 申請者の生体情報（顔、指紋、静脈、等）を利用し本人を認証する
□ その他

26. 方法を実現する技術の成熟度【必須】

前設問で回答いただいた方法を実現する技術について、該当する成熟度レベルを選択してください。
なお、方法を実現する技術が複数あり、かつ、技術ごとに成熟度レベルが異なる場

合は、「その他」を選択し、それぞれのレベルを記載してください。

○　レベル3：実装（製品・サービスとして提供されている）
○　レベル2：応用（製品・サービスとしての提供に向けて実証試験段階である）
○　レベル1：基礎（製品・サービスとしての提供に向けて研究調査段階である）
○　その他

27.　方法を実現する技術の詳細【必須】

２つ前の設問で回答いただいた方法を実現する技術について、詳細を記載してください。
特に、どのような技術を活用して、どのように本人認証をしているのかを具体的に記載してください。技術内容に関するエビデンス等が公表されている場合は、参考URL等も併せて記載してください。
（例）
ICカード認証と指紋認証を組み合わせた二要素認証により本人認証を実施している。

必須機能２．開示情報に係るセキュリティ対策機能

28. 「開示情報に係るセキュリティ対策機能」を有しますか？【必須】

「機能①：個人情報の保護機能」、「機能②：のぞき見防止機能」、「機能③：複写抑止・防止機能」といった開示情報に係るセキュリティ対策機能を有しますか？いずれかの機能を有する場合は「有」を、いずれの機能も有しない場合は「無」を選択してください。なお、「無」を選択した場合は、次のセクション「その他募集の対象とする機能１．紙媒体を電子媒体として変換する機能」に進みます。

○ 有
○ 無

機能①：個人情報の保護機能

29. 「個人情報の保護機能」を有しますか？【必須】

「無」を選択した場合は、次のセクション「機能②：のぞき見防止機能」に進みます。

○ 有
○ 無

30. どのような方法で個人情報の保護を行いますか？【必須】

該当する選択肢を選択してください。
なお、閲覧・縦覧の対象となる情報に含まれる個人情報については、AI等を用いて検出することを想定しています。
１つの製品・サービスで複数の方法を組み合わせて個人情報の保護機能を実現している場合は、複数選択してください。
該当する方法が選択肢にない場合は、「その他」を選択し、方法を記載してください。

□ 検出された個人情報を自動で閲覧・縦覧の対象から除外する（非開示にする）
□ 検出された個人情報を自動で墨塗り等により見えなくする
□ 検出された個人情報を自動で別の文字列に変換（仮名化、匿名化）する
□ 個人情報を検出し、自動で規制所管省庁等の管理者に通知する
□ その他

31. 方法を実現する技術の成熟度【必須】

前設問で回答いただいた方法を実現する技術について、該当する成熟度レベルを選択してください。
なお、方法を実現する技術が複数あり、かつ、技術ごとに成熟度レベルが異なる場合は、「その他」を選択し、それぞれのレベルを記載してください。

○ レベル3：実装（製品・サービスとして提供されている）

○　レベル2：応用（製品・サービスとしての提供に向けて実証試験段階である）

○　レベル1：基礎（製品・サービスとしての提供に向けて研究調査段階である）

○　その他

32.　方法を実現する技術の詳細【必須】

２つ前の設問で回答いただいた方法を実現する技術について、詳細を記載してください。

特に、どのような技術を活用して、どのような電子媒体を対象に、どのような個人情報を検出できるのか、検出された個人情報に対してどのような処理を行うのかを具体的に記載してください。技術内容に関するエビデンス等が公表されている場合は、参考URL等も併せて記載してください。

（例）

AIを活用し、データベースやCSVファイルに含まれる以下の個人情報を自動検出することが可能。検出された個人情報を自動で閲覧・縦覧の対象から除外、又は別の文字に変換（仮名化）することが可能。

＜保護可能な個人情報＞

- 人名情報（氏名、姓、名、ふりがな/フリガナ）
- 住所情報（郵便番号、都道府県、市区町村、番地、ふりがな/フリガナ）
- その他個人情報（生年月日、年齢、性別、電話番号、メールアドレス）

機能②：のぞき見防止機能

33. 「のぞき見防止機能」を有しますか？【必須】

「無」を選択した場合は、次のセクション「機能③：複写抑止・防止機能」に進みます。

○ 有
○ 無

34. どのような方法でのぞき見防止を行いますか？【必須】

該当する選択肢を選択してください。
なお、１つの製品・サービスで複数の方法を組み合わせてのぞき見防止機能を実現している場合は、複数選択してください。
該当する方法が選択肢にない場合は、「その他」を選択し、方法を記載してください。

□ 閲覧・縦覧に使用している端末のカメラ等で申請者以外の人物の顔を検知した場合や申請者の顔を一定時間以上検知できない場合に、自動で閲覧・縦覧に使用している端末の画面をスクリーンセーバー表示に切り替える、ブラックアウトさせる等の処理を行う
□ 閲覧・縦覧に使用している端末のカメラ等で申請者以外の人物の顔を検知した場合や申請者の顔を一定時間以上検知できない場合に、自動で規制所管省庁等の管理者に通知する
□ 閲覧・縦覧に使用している端末の画面ミラーリングを検知し、自動で閲覧・縦覧に使用している端末の画面をスクリーンセーバー表示に切り替える、ブラックアウトさせる等の処理を行う
□ 閲覧・縦覧に使用している端末の画面ミラーリングを検知し、自動で規制所管省庁等の管理者に通知する
□ 閲覧・縦覧に使用している端末の画面ミラーリング機能を制限する
□ その他

35. 方法を実現する技術の成熟度【必須】

前設問で回答いただいた方法を実現する技術について、該当する成熟度レベルを選択してください。

なお、方法を実現する技術が複数あり、かつ、技術ごとに成熟度レベルが異なる場合は、「その他」を選択し、それぞれのレベルを記載してください。

○ レベル3：実装（製品・サービスとして提供されている）
○ レベル2：応用（製品・サービスとしての提供に向けて実証試験段階である）
○ レベル1：基礎（製品・サービスとしての提供に向けて研究調査段階である）
○ その他

36. 方法を実現する技術の詳細【必須】

２つ前の設問で回答いただいた方法を実現する技術について、詳細を記載してください。

特に、どのような技術を活用して、どのようなのぞき見リスクに対応できるのかを具体的に記載してください。技術内容に関するエビデンス等が公表されている場合は、参考URL等も併せて記載してください。

（例）

顔認識技術を活用し、申請者側端末のカメラで申請者以外の人物の顔を検知した場合や申請者の顔を一定時間以上検知できない場合に、自動で閲覧・縦覧に使用している端末の画面をブラックアウトさせることで、閲覧・縦覧中の背後からののぞき見や離席中ののぞき見を防止することが可能。

機能③：複写抑止・防止機能

37. 「複写抑止・防止機能」を有しますか？【必須】

「無」を選択した場合は、次のセクション「その他募集の対象とする機能１．紙媒体を電子媒体として変換する機能」に進みます。

○ 有
○ 無

38. どのような方法で複写抑止・防止を行いますか？【必須】

該当する選択肢を選択してください。

なお、１つの製品・サービスで複数の方法を組み合わせて複写抑止・防止機能を実現している場合は、複数選択してください。

該当する方法が選択肢にない場合は、「その他」を選択し、方法を記載してください。

□ 申請者等が閲覧・縦覧している画面を撮影しようとする、意図的にカメラ等を手で遮ろうとする等の不正行為を、閲覧・縦覧に使用している端末のカメラ等で検知し、自動で閲覧・縦覧に使用している端末の画面をスクリーンセーバー表示に切り替える、ブラックアウトさせる等の処理を行う
□ 申請者等が閲覧・縦覧している画面を撮影しようとする、意図的にカメラ等を手で遮ろうとする等の不正行為を、閲覧・縦覧に使用している端末のカメラ等で検知し、自動で規制所管省庁等の管理者に通知する
□ 閲覧・縦覧に使用している端末のプリントスクリーンや画面キャプチャ、テキストのコピー及びペースト等の機能を制限する
□ 閲覧・縦覧の対象となる情報に電子透かし等を付与する
□ その他

39. 方法を実現する技術の成熟度【必須】

前設問で回答いただいた方法を実現する技術について、該当する成熟度レベルを選

択してください。

なお、方法を実現する技術が複数あり、かつ、技術ごとに成熟度レベルが異なる場合は、「その他」を選択し、それぞれのレベルを記載してください。

○　レベル3：実装（製品・サービスとして提供されている）
○　レベル2：応用（製品・サービスとしての提供に向けて実証試験段階である）
○　レベル1：基礎（製品・サービスとしての提供に向けて研究調査段階である）
○　その他

40.　方法を実現する技術の詳細【必須】

２つ前の設問で回答いただいた方法を実現する技術について、詳細を記載してください。

特に、どのような技術を活用して、どのような複写リスクに対応できるのかを具体的に記載してください。技術内容に関するエビデンス等が公表されている場合は、参考URL等も併せて記載してください。

（例）

行動認識技術を活用し、申請者等がカメラやスマートフォン、スマートグラス等のデバイスで閲覧画面を撮影しようとする、カメラを手で遮ろうとする等の不正行為を、閲覧・縦覧に使用している端末のカメラで検知し、自動でその端末の画面をブラックアウトさせることで、閲覧画面の撮影による複写を防止することが可能。

その他募集の対象とする機能１．紙媒体を電子媒体として変換する機能

41.　「紙媒体を電子媒体として変換する機能」を有しますか？【必須】

「無」を選択した場合は、次のセクション「その他募集の対象とする機能２．申請者以外の閲覧を制限する機能」に進みます。

○　有
○　無

42.　どのような方法で紙媒体を電子媒体に変換しますか？【必須】

該当する選択肢を選択してください。

なお、１つの製品・サービスで複数の方法を組み合わせて紙媒体を電子媒体に変換する機能を実現している場合は、複数選択してください。

該当する方法が選択肢にない場合は、「その他」を選択し、方法を記載してください。

□　複写機やカメラ等を用いて、紙媒体を読み取りデジタル画像に変換する
□　複写機やカメラ等を用いて、紙媒体を読み取りデジタル画像に変換し、更にOCR等により記載されている文字を認識し、デジタル情報に変換する
□　OCR等により記載されている文字を認識するにあたり、AI等を活用し、文字認識率の向上、手書き文字の高精度な認識を可能としている
□　その他

43.　方法を実現する技術の成熟度【必須】

前設問で回答いただいた方法を実現する技術について、該当する成熟度レベルを選択してください。

なお、方法を実現する技術が複数あり、かつ、技術ごとに成熟度レベルが異なる場合は、「その他」を選択し、それぞれのレベルを記載してください。

○　レベル3：実装（製品・サービスとして提供されている）

○　レベル2：応用（製品・サービスとしての提供に向けて実証試験段階である）

○　レベル1：基礎（製品・サービスとしての提供に向けて研究調査段階である）

○　その他

44.　方法を実現する技術の詳細【必須】

２つ前の設問で回答いただいた方法を実現する技術について、詳細を記載してください。

特に、どのような技術を活用して、どのように紙媒体を電子媒体に変換しているのか、どのように文字認識率を向上させているのかを具体的に記載してください。技術内容に関するエビデンス等が公表されている場合は、参考URL等も併せて記載してください。

（例）

複写機やカメラ等を用いて、紙媒体を読み取りデジタル画像に変換し、更にOCRにより記載されている文字を認識し、デジタル情報に変換する。またAIを活用することにより、一度認識間違いをした文字を学習することで、文字認識率を向上することが可能。手書き文字も高精度に認識し、デジタル情報に変換することが可能。

その他募集の対象とする機能２．申請者以外の閲覧を制限する機能

45. 申請者にのみファイル閲覧を許可し、申請者以外の閲覧を制限する機能を有しますか？【必須】

「無」を選択した場合は、次のセクション「サイバーセキュリティ」に進みます。

（例）

・IRM（Information Rights Management）

・文書に対するパスワード保護

・証明書による文書の保護

○ 有

○ 無

46. 機能を実現する技術の成熟度【必須】

前設問で回答いただいた機能を実現する技術について、該当する成熟度レベルを選択してください。

○ レベル3：実装（製品・サービスとして提供されている）

○ レベル2：応用（製品・サービスとしての提供に向けて実証試験段階である）

○ レベル1：基礎（製品・サービスとしての提供に向けて研究調査段階である）

47. 機能を実現する技術の詳細【必須】

２つ前の設問で回答いただいた機能を実現する技術について、詳細を記載してください。

特に、どのような技術を活用して、どのように申請者にのみファイル閲覧を許可しているのか、どのように申請者以外の閲覧を制限しているのかを具体的に記載してください。技術内容に関するエビデンス等が公表されている場合は、参考URL等も併せて記載してください。

サイバーセキュリティ

セキュリティ認証取得や脆弱性対策、データの取扱い、及びソフトウェアサプライチェーン管理等の製品・サービスに関する網羅的なセキュリティ情報について御回答ください。

なお、選択肢に記載されている各認証の概要や特徴等については、「（参考資料）サイバーセキュリティに関する設問の趣旨と概要」を参照ください。

48. 組織/法人のサイバーセキュリティ管理に関する認証について、以下の４つのうち取得しているものを全て選択してください。【必須】

該当しない場合は「取得していない」を選択してください。

- □ ISO/IEC 27001認証
- □ ISO/IEC 27017認証
- □ ISO/IEC 27701認証
- □ JIS Q 15001認証
- □ 取得していない

49. 製品・サービスについて「ISO/IEC 15408認証」、「CCDS認証」の取得状況を以下より選択してください。【必須】

- ○ 両方取得している
- ○ 「ISO/IEC 15408認証」のみ取得している
- ○ 「CCDS認証」のみ取得している
- ○ 両方取得していない

50. 「ISO/IEC 15408認証」について、取得しているCCのレベル（EAL）及び対象のProtection Profile（PP）を記載してください。【必須】

PPについては、Security Target（ST）がPPを参照している場合に回答してください。

51. **「CCDS認証」について、下記のサイバーセキュリティ認証で取得しているものを全て選択してください。【必須】**

□ 2019年版認証（CCDS-GR01-2019）
□ 2021年版認証（CCDS-GR01-2021）
□ 2023年版認証（CCDS-GR01-2023）

52. **その他製品・サービスに関する認証【任意】**

「ISO/IEC 15408認証」、「CCDS認証」以外で、サイバーセキュリティの観点から取得している認証がありましたら、その名称を記載してください。

（例）

RBSS（優良防犯機器認定制度）

53. **サイバーセキュリティにおける脆弱性検査の実施状況を以下より選択してください。【必須】**

○ 国内外発刊のガイドラインに準拠した脆弱性検査を実施している
○ 準拠するガイドラインはないが、独自に脆弱性検査を実施している
○ 脆弱性検査の実施を検討中
○ 脆弱性検査を実施していない

54. **国内外発刊のガイドラインに準拠した脆弱性検査について、準拠するガイドラインの情報（発行元、名称など）を記載してください。【必須】**

55. **国内外発刊のガイドラインに準拠した脆弱性検査について、具体的な内容を記載してください。【必須】**

56. **独自に実施している脆弱性検査について、具体的な内容を記載してください。【必須】**

57. **取扱い業務データの保存国【必須】**

全ての取扱い業務データがどの国のデータセンタに保存されるか、該当する選択肢を選択してください。日本国内以外の場合は、「その他」を選択し、その内容を記載してください。

○　日本国内のデータセンタ
○　その他

58. **取扱い業務データの機密性確保に関する対策【任意】**

前設問「取扱い業務データの保存国」の回答に関し、データの機密性を確保するための具体的な技術等の対策を記載してください。

（例）

・「CRYPTREC 暗号リスト(電子政府推奨暗号)」に掲載されている暗号化アルゴリズムによって暗号化されている

・暗号化鍵がクラウドサービス内の耐タンパー装置（ハードウェアセキュリティモジュール）等の仕組みによって安全に管理され、その暗号化鍵の使用可否が利用者側の管理下に置かれる等、利用者側の意に反した復号を行うことができない仕組みが確立されている

59. **保存した取扱い業務データに係る紛争発生に際し、裁判管轄権**

の所在地について以下より選択してください。【必須】

○ 日本の裁判所に裁判管轄権がある
○ 海外の裁判所に裁判管轄権がある

60. **保存した取扱い業務データに係る紛争発生に際し、適用される準拠法を回答してください。【必須】**

日本法以外に準拠する場合は、「その他」を選択の上、準拠する国の法律を記載してください。

○ 日本法に準拠する
○ その他

61. **ソフトウェアが有している機能【必須】**

ソフトウェア※について、下記に示す機能を有している場合は、以下より該当する機能を選択してください。
※サービス提供目的のために購入または導入され、運用目的で使用される全ての形式（スタンドアロンソフトウェア、クラウドベースのソフトウェア等）を対象とする。

□ 権限昇格機能（一時的に管理者権限を得る）の実行や、権限管理に関する機能を有している
（例）ネットワーク管理システム、ネットワーク構成管理ツール、ネットワークトラフィック監視ツール、等
□ ネットワークやコンピュータリソースへ直接アクセスするか、アクセス可能な権限を有する機能を有している
（例）Webブラウザ、ルーティングプロトコル、DNSリゾルバやDNSサーバー、SDN制御プロトコル、VPN、等
□ ソフトウェアデータまたは制御系システムへのアクセスを管理する機能を有している
（例）ID管理システム、バックアップサービスシステム、リカバリーマネー

ジャー、NAS、SAN、等

□ ネットワーク制御、エンドポイントセキュリティ等におけるセキュリティ機能のような、信頼性が不可欠な機能を有している
（例）OS、ハードディスク暗号化ソフトウェア、パスワードマネージャー、EDR、ファイアウォール、IDS/IPS、等

□ 特権アクセスにより、セキュリティ対策が行われている信頼された境界の外で動作する機能を有している
（例）SIEM、リモート型脆弱性スキャンツール、パッチ管理ツール、アプリケーション構成管理ツール、等

□ いずれの機能も有していない

62. ソフトウェア及びソフトウェアを実行するためのプラットフォームに対する保護対策【必須】

ソフトウェア及びソフトウェアを実行するためのプラットフォーム※について、不正なアクセスや不正利用から保護する対策を実施している場合は、該当する対策を全て選択してください。また、選択肢に該当する対策が無い場合は「その他」を選択し、対策内容を記載してください。対策を実施していない場合は、「対策を実施していない」を選択し、その理由を「その他」に記載してください。
※エンドポイントの端末、サーバー、クラウドサービスのリソース等のソフトウェアが動作するプラットフォームを意味する。

□ ソフトウェア及びプラットフォームのユーザーに対し認証機能を使用し、ユーザーごとに扱うデータのトランザクションに係るリスクを踏まえ、アクセス権限を管理している
（例）SSO、MFA、等

□ ソフトウェア及びプラットフォームにアクセスするサービスごとに識別・認証し、システム内での通信や情報のやり取りが正当なサービスやアプリケーションとの間で行われ不正なアクセスや通信を防止するよう管理している

□ ソフトウェア及びプラットフォームへのアクセス権はユーザーごとに必要最低限の範囲で付与し、重要な資産への不正アクセスを防止している
（例）アクセス権管理専用のプラットフォームを使用し個々の管理者を

識別している、管理セッションへのアクセスを制御・記録している、等

- □ ソフトウェア、プラットフォーム及び関連データへの直接アクセスを最小限に抑えるため、ネットワークを保護している
  （例）ネットワーク分離、プロキシの利用、SDP、ファイアウォール、リモートアクセス管理、等
- □ 対策を実施していない
- □ その他

63. ソフトウェアを実行するためのプラットフォームで使用されるデータに対する対策【必須】

ソフトウェアを実行するためのプラットフォームで使用されるデータについて、機密性、完全性、可用性を保護する対策を実施している場合は、該当する対策を全て選択してください。また、選択肢に該当する対策が無い場合は「その他」を選択し、対策内容を記載してください。

対策を実施していない場合は、「対策を実施していない」を選択し、その理由を「その他」に記載してください。

- □ データ資産の特定、重要度と影響で分類、管理ポリシーの策定を実施の上、データ侵害への対応（例：暗号化制御、データ難読化対応等）、攻撃時の回復手順策定を実施している
- □ データ資産への不正なアクセスを防止するため、ユーザーに必要最小範囲へのアクセス権の付与や職掌権限にもとづく適切なアクセスレベルの設定を実施している
  （例）属性情報ベースのアクセス権制御（ABAC）、等
- □ ローカルストレージ上で保存され外部へ送信されるデータに対して、不正アクセスを防止するための認証、暗号化を施している。また、デバイスへの物理的なセキュリティの確保、損傷ファイルのリカバリ手順の策定、構成管理などを実施している
- □ ネットワークに対する不正な接続を防止するための適切な対策を実施している。また、ネットワーク上のデータが脆弱性の少ないプロトコルで安全に送受信している

（例）TLS 1.3プロトコルの利用、等

□ 障害発生時、迅速な復旧作業が可能となるよう障害時対応計画を策定し、その有効性を確認している。また、データ消失等の事態に備え、バックアップ及びリストアの仕組みを実装し、その有効性を確認している

□ 対策を実施していない

□ その他

64. ソフトウェアの特定と維持管理による保護対策【必須】

ソフトウェアを実行するためのプラットフォームと、それらのプラットフォームに展開されている全てのソフトウェアを特定して維持管理し、ソフトウェアが悪用されないよう保護するための対策を実施している場合は、該当する対策を全て選択してください。また、選択肢に該当する対策が無い場合は「その他」を選択し、対策内容を記載してください。

対策を実施していない場合は、「対策を実施していない」を選択し、その理由を「その他」に記載してください。

□ プラットフォーム上の全てのソフトウェア（サードパーティ製ソフトウェア、OSSを含む）のソフトウェア・コンポーネントのインベントリを作成し、作成したインベントリの最新性、完全性、正確性、及び可用性を維持している

（例）ソフトウェア部品表（SBOM：software bill of materials）、等

□ プラットフォーム上の全てのソフトウェア（サードパーティ製ソフトウェア、OSSを含む）に対してパッチ管理プロセスを適用し、継続的な脆弱性の監視・スキャンが行われ、適切なタイミングでのパッチ適用を実施している

（例）既知の脆弱性を迅速に特定し文書化している、ネットワーク帯域幅の制約を考慮しデバイスへのタイムリーなパッチ適用に影響がないようにしている、等

□ プラットフォーム上の全てのソフトウェア（サードパーティ製ソフトウェア、OSSを含む）のセキュアなベースライン構成（構成設定、ソフトウェアロード、パッチレベル、情報システムの物理的または論理的な配置等）を実装し、ベースラインを維持するための変更プロセスが構築さ

れ、かつ誤った構成や脆弱性及び未承認の変更への適切な対処がなされるよう監視している
（例）Active Directoryによる実装、等

- □ プラットフォーム上の全てのソフトウェア（サードパーティ製ソフトウェア、OSSを含む）について、提供された SBOM やコンポジションアナリシスを実施して、脆弱性や OSS ライセンスなどのリスクを評価している
- □ プラットフォーム上の全てのソフトウェア（サードパーティ製ソフトウェア、OSSを含む）について、SBOM データを標準フォーマットで管理している
（例）SPDX（Software Package Data Exchange）、CycloneDX、SWID タグ（Software Identification タグ）、等
- □ ソフトウェア製品の SBOM データを、必要に応じて社内外の関係者に適切な方法で共有している
- □ 対策を実施していない
- □ その他

65. ソフトウェアを実行するためのプラットフォームに対するインシデントに関する対策【必須】

ソフトウェアを実行するためのプラットフォームに関連する脆弱性やインシデントを早急に検出、対応、回復する対策を実施している場合は、該当する対策を全て選択してください。また、選択肢に該当する対策が無い場合は「その他」を選択し、対策内容を記載してください。
対策を実施していない場合は、「対策を実施していない」を選択し、その理由を「その他」に記載してください。

- □ 監査記録やログ記録がポリシーに従って決定、文書化され、ログ収集機能を実装している。また、その収集記録をレビューし、日常監視やセキュリティインシデント検知、運用改善等に活用している
- □ 管理・許可されていないソフトウェア、権限のない人員・デバイスの接続を監視・検知し、これに対応するためのポリシーと仕組みを実装している

□ データの漏洩・改ざんを防止するため、悪質なコードの実行等の攻撃についてモニタリングを実施している。また、検知したイベントを分析し、攻撃の標的及び手法を理解するために活用している

□ 不正侵入等を防ぐため、ネットワークデバイスの脆弱性に対してセキュリティ対策を実施している
（例）ファイアウォールの設定、境界保護、トラフィックの監視、暗号化された新型プロトコルの利用、等

□ セキュリティインシデントの発生時を想定して、対応方針・手順の策定、人材育成を実施している
（例）対応計画や復旧計画の策定・評価、緊急時対応訓練、セキュリティ管理人材の育成研修プラットフォーム上のソフトウェアのセキュリティイベントを監視している、等

□ 対策を実施していない

□ その他

66. ユーザー及び管理者のセキュリティの理解を促進する対策【必須】

ソフトウェアや、当該ソフトウェアを実行するためのプラットフォームに関するユーザー及び管理者のセキュリティの理解を促進する対策を実施している場合は、該当する対策を全て選択してください。また、選択肢に該当する対策が無い場合は「その他」を選択し、対策内容を記載してください。
対策を実施していない場合は、「対策を実施していない」を選択し、その理由を「その他」に記載してください。

□ ソフトウェア及び当該ソフトウェアを実行するためのプラットフォームを利用する全てのユーザー（管理・監督者及び契約業者を含む）に対し、それぞれの役割と責任に基づいて、安全に利用するためのセキュリティとプライバシーに関するリテラシートレーニングを実施している
（例）実際の出来事やインシデントをシミュレートするリテラシートレーニングの実践的な演習を実施している、等

□ ソフトウェア及び当該ソフトウェアを実行するためのプラットフォームの管理において、何らかの役割を持つ全ての人に対し、それぞれの役割

と責任に基づいて、安全に管理するためのロールベースでのトレーニングを実施している

（例）個人を特定できる情報になり得る情報の種類やその処理に関連するリスク・考慮事項・義務について学習している、インシデント発生時にシステム管理者が代替の処理及びストレージサイトでシステムを設定する方法を学習している、等

□ ソフトウェア及び当該ソフトウェアを実行するためのプラットフォームに関わる全てのユーザーと管理者に対するトレーニングの継続的な改善を目的とした活動を実施している

（例）セキュリティトレーニング結果を定量的な数値等で把握し結果を踏まえたトレーニング内容の改善等を実施している、内部または外部のセキュリティインシデント等からの教訓をロールベースのトレーニングに組み込んでいる、等

□ 対策を実施していない

□ その他

67. ソフトウェア開発におけるベストプラクティスな手法の実施状況【必須】

当該ソフトウェアの開発時において、以下に示すベストプラクティスな手法に従ってソフトウェアの設計、構築、検証を行っている場合は、該当する項目を全て選択してください。
いずれも実施していない場合は、「いずれも実施していない」を選択し、その理由を「その他」に記載してください。

□ 脅威モデリング手法を用いて設計レベルのセキュリティに関する問題を特定し、主要なテスト対象または見落とされる可能性のあるテスト対象を特定している

□ テスト自動化ツールを採用することで、テストの一貫した実行と結果の正確な確認を実施しつつ、テストに掛かる工数を最小化している

□ 静的解析（コードベースでの分析）を実施している

（例）コードスキャナーを使用して主要なバグを検出している、ハードコードされたパスワードや暗号鍵等がないかを確認している、等

□ 動的解析（テストケースでプログラムを実行し分析）を実施している
（例）テストケースに基づきブラックボックステストを実施している、リグレッションテストを実施している、ソフトウェアがWebサービスを提供する場合はWeb アプリケーションスキャナーなどを使用して脆弱性を検出している、等

□ ソフトウェアに含まれているコンポーネント（OSS等の外部ソース含む）について、脆弱性データベース等を活用し脆弱性を継続的に監視している

□ 検証の結果見つかったバグを修正し、かつ開発プロセスの早い段階でバグを発見し修正するために必要なプロセスの改善を実施している

□ いずれも実施していない

□ その他

製品・サービスの導入実績

68. 日本国内での導入実績【必須】

日本国内での公的機関、企業等における導入件数を記載してください。

実績をお持ちでない方は「０件」と記載してください。

（例）

500件以上

69. 公的機関での導入実績【必須】

前設問「日本国内での導入実績」のうち、公的機関での導入件数を記載してください。

実績をお持ちでない方は「０件」と記載してください。

（例）

10件以上

70. 主な導入事例①【必須】

主な導入事例の概要について御紹介ください。

導入事例をお持ちでない方は「無し」と記載してください。

概要は、「①発注者」、「②概要」、「③参考URL（あれば）」、「④投資対効果（あれば）」について記載してください。

「①発注者」については「●●県」のように具体的な発注者名でなくても問題ございません。「④投資対効果（あれば）」については、具体的な数値を用いて記載してください。難しい場合には、定性的な記載（例えば、閲覧・縦覧の対面監視等に要する人件費を削減できた、等）でも問題ございません。

（例）

① 発注者

●●県

② 概要

●●県が実施する●●に関する閲覧業務では、閲覧業務のデジタル化にあたり、●●が課題とされていた。本サービスでは、●●といった技術の活用により、●●に関する技術的課題を解決し、現在では年間●●人が本サービスを活用し、オンラインでの閲覧を利用している。

③ 参考URL

https(:)//www.xxxx.xxxxx.xxxx

④ 投資対効果：

- 年間の閲覧・縦覧の対面監視等に係る人件費が前年比●●%削減された。
- 年間の閲覧・縦覧の対面監視等に要する時間が前年比●●%削減された。
- 費用便益比※●●の費用対効果が得られた。

※「実際に要した費用の総計」に対する「得られた便益の総計」の比率。一般的にその値が１以上であれば、その事業は妥当なものと評価される。

71. 主な導入事例②【任意】

導入事例①と同様の形式で記載してください。

72. 主な導入事例③【任意】

導入事例①と同様の形式で記載してください。

その他製品・サービス情報

73. 製品・サービスの導入・維持に係る費用【任意】

製品・サービスの導入・維持にあたり、規制所管省庁等に必要となる費用を記入してください。また、月額やアカウント数に応じた料金体系がある場合はそちらも記載してください。

なお、料金体系がホームページ・SNS等で公表されている場合は、当該ホームページ・SNS等のURLを記載してください。

（例）

・初期導入費用：XXXX円（税抜）

・月額利用料：XXXX円（税抜）

・ホームページ：https(:)//www.xxxx.xxxxx.xxxx

74. 特許登録【任意】

製品・サービスに関連する発明の名称及び特許番号を最大３つ記載してください。

（例）

① 発明の名称：XXXX

特許番号：特許第XXXXXXX号

② 発明の名称：XXXX

特許番号：特許第XXXXXXX号

75. 規制所管省庁等が製品・サービスを利用するにあたって準拠・参照すべきガイドライン・ガイドブック等【任意】

規制所管省庁等が製品・サービスを利用するにあたって準拠・参照すべきガイドライン・ガイドブック等がありましたら、その名称及び発行体を記載してください。

（例）

AIプロダクト品質保証ガイドライン（AIプロダクト品質保証コンソーシアム）

76. 製品・サービスを利用するにあたっての制限事項や使用上の注意点【任意】

製品・サービスを利用するにあたっての制限事項や使用上の注意点があれば記載してください。もし改善の見通し等がありましたら、可能な限りで差し支えございませんので、記載してください。

（例）

・閲覧・縦覧申請者の本人の認証にあたっては、申請者側で特定のアプリケーションをスマートフォンにダウンロードしてもらう、ないしは特定のデバイスを準備してもらうことが必要。

・閲覧・縦覧申請者がダウンロードするアプリケーションはAndroidのみに対応。2025年度にはiOSにも対応予定。

・現製品・サービスでは本人認証に数分以上の時間を要するが、製品・サービスの改善を行っており、改善によって時間短縮が可能になる見込み。

77. 製品・サービスに関連するアピール情報等【任意】

製品・サービスの特徴やアピール情報（導入のしやすさ、運用のしやすさ、等）があれば記載してください。

なお、受賞歴、メディア掲載、論文掲載等の実績があれば、それらも記載してください。

問合せ先情報

技術カタログへの掲載及び事務局等との連絡に利用する連絡先を御回答ください。

78. 担当部署・担当者名【必須】

担当部署・担当者名を記載してください。

どちらか一方の記載でも問題ございません。

（例）

セーフティ＆インダストリー本部　山田太郎

79. 担当部署・担当者名のフリガナ【必須】

前設問で回答いただいた担当部署・担当者名のフリガナを全角カタカナで記載してください。

（例）

セーフティアンドインダストリーホンブ　ヤマダタロウ

80. 連絡先【必須】

電話番号及び電話受付時間、メールアドレスを記載してください。

電話番号及び電話受付時間、メールアドレスのどちらか一方は必ず御回答ください。

（例）

000-0000-0000　平日XX:XX~XX:XX

xxxx@xxxxx.com

81. 個人情報の取扱いへの同意【必須】

・ 本公募は、デジタル庁の業務委託を受けた株式会社三菱総合研究所及び再委託先のKPMGコンサルティング株式会社が実施するものです。
・ 応募フォーム等に御記入の個人情報のお取扱いについては、「募集要領及び参考資料」に掲載する、デジタル庁にて2022年９月30日に策定された「技術カタログへの登録における個人情報の取扱いについて」のとおり、株式会社三菱総合研究所及び再委託先のKPMGコンサルティング株式会社において適切に管理致します。

○　　個人情報の取扱いに同意する

その他

82. 著作権の取扱いに対する同意【必須】

この応募フォームを通じて収集された技術情報については、「募集要領及び参考資料」に掲載する「著作権について」に記載された条件に従って、デジタル庁の管理するウェブサイトにて公表される予定のため、内容をよくお読みいただいた上で、御同意いただけますと幸いです。「同意する」ボタンをクリックした場合、この条件に従ってデジタル庁の管理するウェブサイトにて公表されます。

○　著作権の取扱いに同意する

83. 技術カタログの利用規約に対する同意【必須】

この応募フォームを通じて収集された技術情報については、「募集要領及び参考資料」に掲載する「テクノロジーマップ及び技術カタログ利用規約」に記載された条件に従ってデジタル庁の管理するウェブサイトにて公表される予定のため、内容をよくお読みいただいた上で、御同意いただけますと幸いです。「同意する」ボタンをクリックした場合、この条件に従ってデジタル庁の管理するウェブサイトにて公表されます。なお、「テクノロジーマップ及び技術カタログ利用規約」は、今後変更される可能性があります。

○　同意する

84. 回答内容についての御確認【必須】

諸手続きの都合上、回答内容の変更には時間を要しますため、今一度、回答内容に誤り等ないか御確認ください。

○　確認しました