

仕 様 書

1. 件名

AI チップ設計拠点 Web サイトを半導体設計 Cloud に導入する作業

2. 研究の概要・作業の目的

国立研究開発法人産業技術総合研究所 AI チップデザインオープンイノベーションラボラトリ (AIDL) (以下、「産総研」という。) では、共用施設の AI チップ設計拠点 (以下、「AIDC」という。) を活用したチップレット設計基盤構築に向けた技術開発を進めている。本技術開発において、設計ガイドラインや画像データも機密情報となる。しかしながら、AI チップ設計拠点 Web サイト (以下、「拠点 Web」という[*1]) はさくらインターネット上で運用されており (以下、「拠点さくら Web」という)、設計ガイドラインや画像データが第三者に共有されるリスクを十分に防ぐことができず、これはセキュリティ的に重大な懸念となる。これに対処するため、拠点さくら Web の一部を AIDC 内の半導体設計 Cloud 内に移動した拠点 Web (以下、「Cloud 内 Web」という) を構築することが必要である。

[*1] <https://ai-chip-design-center.org/>

3. 作業項目

- (1) Cloud 内 Web 仕様書の作成
- (2) Cloud 内 Web の構築
- (3) システム検証

4. 作業項目別仕様

(1) Cloud 内 Web 仕様書の作成

受注者は Cloud 内 Web の仕様書を作成するにあたって、拠点さくら Web の構成を把握する必要がある。本作業の契約前に拠点さくら Web の構成を開示するにあたっては、事前に産総研と秘密保持契約(NDA)の契約が必要となる。

- ① 拠点さくら Web は、拠点利用者の契約形態に応じた複数の Web ページ、ユーザ登録、利用申請、管理運営ページを提供している。Cloud 内 Web でも同様の機能を設定すること。
- ② 拠点さくら Web では、半導体利用契約形態 (最大 1024 契約形態) をサポートし、形態毎に表示するページやコンテンツを制御している。Cloud 内 Web でも同様の機能を設定すること。
- ③ セキュリティ機能強化方式を Cloud 内 Web 仕様書に記載すること。
- ④ 拠点さくら Web は、一般に公開している部分があり、それを Cloud 内 Web に移動することはセキュリティ上好ましくない。この部分は拠点さくら Web に残すこと。この構成を Cloud 内 Web 仕様書に記載すること。
- ⑤ 拠点さくら Web に掲載された設計ガイドラインや画像データのうちセキュリティ強化すべきコンテンツ (ページ) がある。これらのページおよび拠

点の管理運営ページは Cloud 内 Web に移動すること。この構成を Cloud 内 Web 仕様書に記載すること。

- ⑥ 拠点さくら Web とセキュリティを強化した Cloud 内 Web との通信機能を開発する必要がある。この通信機能には、現在の拠点さくら Web 以外の少なくとも 1 つ以上のさくらネットワーク上の Web サイト（今後設定する可能性あり）と通信する機能を有すること。
- ⑦ 拠点さくら Web と Cloud 内 Web の同期を取る部分の通信手段方式を Cloud 内 Web 仕様書に記載すること。
- ⑧ 拠点さくら Web と Cloud 内 Web 間の通信機能は、Cloud 内 Web のセキュリティ機密度を保てること。
- ⑨ Cloud 内 Web が動作するサーバの OS 仕様を Cloud 内 Web 仕様書に記載すること。
- ⑩ 受注後早期に Cloud 内 Web 仕様書を調達請求者に提出し、承認を得ること。

(2) Cloud 内 Web の構築

- ① Cloud 内 Web 仕様書の内容を拠点 Cloud 内に構築すること。
- ② 拠点さくら Web と Cloud 内 Web の通信手段を構築すること。

(3) システム検証

- ① Cloud 内 Web の動作検証を行うこと。Cloud 内 Web で拠点の管理運営ページの動作確認を行うこと。拠点さくら Web と Cloud 内 Web の通信手段の動作確認を行うこと。動作確認結果を報告し、調達請求者の承認を得ること。
- ② 拠点さくら Web と Cloud 内 Web の全体の動作確認を行うこと。動作確認結果を報告し、2025 年 3 月 31 日までに承認を得ること。

5. 貸与品

- (1) さくらインターネットへのログイン情報。
- (2) 拠点 Web サイトへのログイン情報。
- (3) 半導体設計 Cloud へのログイン情報。

6. 特記事項

受注者は、以下の要件を有すること。

- (1) 本拠点の web システムは、半導体設計に特化した web システムである。受注者は半導体設計に特化した web システムの構築・運用・改良の業務について複数年以上の経験があること。確認の為にその Web サイトの URL と半導体設計に必要な米国輸出管理や諸契約形態を考慮した部分について説明すること。
- (2) 本拠点の web システムは、利用しやすさと米国輸出管理を考慮した半導体業界独自の契約形態に基づくセキュリティの両立を図っている。このため契約形態に則した Authority code を利用者に割り振り、半導体設計に関する契約

を前提にしたセキュアな環境を Authority code ごとに構築している。受注者には、このようなセキュリティを前提にした Web ページを対象にしていること
の理解を求める。確認のため、技術審査時に Authority code による制御の
意味(必要性)を説明すること。

- (3) 本作業項目 4. 項について、Web 構造、データベース構造、その実現方法、お
よび制限すべき機能などを具体的に説明した資料を技術審査時に提出するこ
と。
- (4) 本拠点の web システムは、さくらインターネット上にあり、すでに利用され
ているため、動作が確認できたものだけを本拠点 Web ページに掲載する方式
などを具体的に説明した資料を技術審査時に提出すること。
- (5) 本作業は、Redmine[*2]による進捗管理を行うこと。
 - ① 全ての報告や質問は、その内容、原因箇所、対策方法と指示先を記載した
チケットを本拠点が整備した Redmine に登録すること。(※ チケットとは、
Redmine のタスク管理に使用されるタスクを記述したもの)
 - ② 登録したチケットが完了した場合は、終了処理を Redmine で行うこと。
 - ③ 期限を過ぎて 5 営業日以上応答のないチケットは、本拠点に報告すること。

[*2] Redmine システムはプロジェクト管理ツールのひとつ。本拠点で整
備している Redmine を使用すること。受注者には契約後にアクセス権を
設定する。具体的な利用方法については後日、本拠点より案内する。

7. 納入前確認試験

- (1) 受注者は本拠点担当者とともに、公開された Web サイトで動作確認を行い、
仕様内容を満たしていることを確認する。その結果を動作確認報告書として
提出すること。動作確認報告書には、本仕様書に記載された内容と実施内容
を対比させた仕様項目チェックリストと、各項目の動作テスト結果を掲載す
ること。

8. 守秘義務

- (1) 「13. セキュリティ要件」を遵守すること。
- (2) 本項の規定は、本契約による履行が完了した後、又は解除した後も 3 年間、
なおその効力を有するものとする。

9. 納入物品

- (1) Cloud 内 web 仕様書 [4. (1)]
 - ・ 契約後早期に Web 仕様書を作成し、調達請求者から仕様書の内容について

承認を得ること。

- ・仕様書の提出は、調達請求者の指示する Redmine 上にファイルをアップロードすること。

(2) 作業成果が反映された web システム 一式 [4. (2)]

- ・修正した拠点さくら Web: 本拠点 Web サイトとして掲載しているさくらインターネット上にインストールすること。
- ・作成した Cloud 内 Web: 本拠点の半導体設計 Cloud 上にインストールすること。

(3) 動作確認報告書 [4. (3)]

- ・動作確認報告書には、仕様項目チェックリスト、動作テスト結果を含めること。
- ・動作確認報告書の提出は、調達請求者の指示に従い、さくらインターネット上、半導体設計 Cloud 上、Redmine 上などにファイルをアップロードすること。
- ・全体確認に先立って拠点さくら Web、Cloud 内 Web 個別の動作検証を行い、動作確認報告書の内容について承認を得ること。
- ・2025 年 3 月 31 日までに拠点さくら Web と Cloud 内 Web の全体の動作確認を行い、動作確認報告書の内容について承認を得ること。

10. 納入の完了

本件は「9 納入物品」に記載された納入物品が過不足なく納入され、仕様書を満たしていることを確認して、納入の完了とする。

11. 納入期限及び納入場所

納入期限：2025 年 3 月 31 日

納入場所：〒113-0032 文京区弥生 2-11-16

東京大学 本郷地区浅野キャンパス 武田先端知ビル 203 号室

AI チップ設計拠点

12. 成果の取扱い

- (1) 産総研は、受注者が本業務で作成した設計データ、検証環境、ドキュメント（以下「成果」という。）についての利用及び第三者への開示、公開に関する権利を有するものとする。
- (2) 受注者は、成果のうち受注者が著作権を有するものについては著作権を産総研に開発委託代金支払いの対価として譲渡するものとし、著作者人格権を行使しないものとする。
- (3) 受注者は、検収終了後、直ちに別紙様式による著作者財産権譲渡証書及び著作者人格権不行使証書を提出するものとする。

13. セキュリティ要件

- (1)本業務の遂行に当たっては、産総研の情報セキュリティポリシーを準拠した情報セキュリティ対策を講じること。産総研の情報セキュリティ規程については、下記 URL を参照のこと。その他の情報セキュリティポリシーの詳細については契約締結後に提示する。

【国立研究開発法人産業技術総合研究所情報セキュリティ規程】

https://www.aist.go.jp/Portals/0/resource_images/aist_j/outline/comp-legal/pdf/securitykitei.pdf

産総研の情報セキュリティポリシーの見直しが行われた場合は、その内容を準拠した情報セキュリティ対策を講じること。なお、対応内容については産総研に事前に報告し承認を得ること。

(2)その他セキュリティに関する要件

- ① 受注者は、本業務の履行に際して、秘密である旨を示されて貸与を受けた秘密情報を秘密として適切に保持することとし、第三者に開示又は漏洩してはならない。
- ② 受注者は、本業務の履行によって知った一切の情報を本業務の履行以外の目的に利用してはならない。契約終了後も同様とする。
- ③ 貸与品は調達請求者の了解なしに所外に持ち出しまたは複製してはならない。
- ④ 産総研の所外へ持ち出しまたは複製した貸与品については一覧表を作成し、調達請求者に提出すること。なお、契約終了後、速やかに返却又は廃棄し、調達請求者の確認を得たうえで一覧表からの削除を行うこと。
- ⑤ 受注者は、契約締結後、情報セキュリティ管理体制を記載したドキュメントを調達請求者に提出すること。
- ⑥ 受注者は、本業務において、受注者の従業員若しくはその他の者によって、意図せざる変更が加えられない管理体制とすること。
- ⑦ 受注者は、産総研の求めに応じて、資本関係、役員等の情報、委託事業の実施場所並びに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を行うこと。
- ⑧ 本業務にかかる情報に関する情報セキュリティインシデントが生じた場合、速やかに報告の上、原因の分析を実施し、調達請求者と対処内容及び再発防止策を検討すること。当該インシデントへの対処を実施するにあたっては、事前に調達請求者の確認を得ること。
- ⑨ 情報セキュリティインシデントが生じたことで、受注者の作業環境等の確認が必要となった場合には、産総研の調査に協力を行うこと。
- ⑩ 産総研で情報セキュリティインシデントが発生した場合、速やかに調査及び復旧に協力を行うこと。

- ⑪ 本業務の遂行における情報セキュリティ対策の履行状況を確認するため、産総研が提示するチェックリストの内容に基づき、適宜情報セキュリティ対策の履行状況を報告すること。※2
- ⑫ 調達請求者より、情報セキュリティ対策の履行が不十分であると指摘された場合は、速やかに是正処置を講ずること。
- ⑬ 本業務の遂行における情報セキュリティ対策の履行状況を確認するために、産総研が情報セキュリティ監査の実施を必要と判断した場合、受注者は、産総研が定めた実施内容（監査内容、対象範囲、実施者等）に基づく情報セキュリティ監査を受け入れること。
- ⑭ 受注者は、産総研の許可なく、本業務の一部又は全部を第三者（再委託先）に請け負わせてはならない。ただし、受注者に求めている情報セキュリティ対策を、再委託先が実施することを再委託先に担保させるとともに、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産総研に提供し、承認申請書を提出して、事前に産総研の書面による承認を受けた場合はこの限りではない。※3
- ⑮ 本業務の履行においては、十分な秘密保持を行うこと。
- ⑯ サプライチェーン・リスクに係る情報セキュリティ上の事象が発生した場合、受注者は原因調査などについて調達請求者と協議の上、主導的に解決を図ること。
- ⑰ 受注者は、受注先及び再委託先において作成した委託事業に係る成果物（システム構成・設定情報、等を含む。産総研に帰属しない著作物を除く。）の納入の完了後速やかに、当該成果物を調達請求者の許可を得て、抹消すること。また、受注者は、調達請求者の指示に従い、当該成果物の抹消の確認を受けること。

14. 付帯事項

- (1) 作業場所は日本国内であること。
- (2) 調達請求者の求めにより、作業の進捗状況及び作業内容について報告しなければならない。
- (3) 本仕様書の技術的内容に関する質問等については、調達請求者と協議すること。
本仕様書に定めのないこと項及び疑義が生じた場合は、調達担当者との協議のうえ決定する。
- (4) サプライチェーン・リスクに対応するため、別紙に記載する事項に従って契約を履行しなければならない。

以上

別紙様式

年 月 日

著 作 者 財 産 権 譲 渡 証 書

国立研究開発法人産業技術総合研究所 殿

請 負 者
住 所
会 社 名
代表者氏名

印

請負契約 (年 月 日 契約)
件 名

上記契約により作成したソフトウェアのうち、受注者が著作権を有するものについての所有権及び著作権（著作権法第 27 条及び第 28 条に規定する権利を含む）は、国立研究開発法人産業技術総合研究所に譲渡したことに相違ありません。ただし、自己所有していた権利は除くものとします。

著作者人格権不行使証書

国立研究開発法人産業技術総合研究所 殿

請負者
住 所
会 社 名
代表者氏名

印

請負契約 (年 月 日 契約)
件 名

上記契約により作成したソフトウェアのうち、受注者が著作権を有するものについての著作権（著作権法第 27 条及び第 28 条に規定する権利を含む）に係わる著作者人格権を行使しないことを約束します。

なお、著作者人格権を行使しようとする場合は、国立研究開発法人産業技術総合研究所の承認を得るものとします。

サプライチェーン・リスク対応に係る特記事項

1. サプライチェーン・リスクへの対応

受注者は、機器等の意図的な不正改造及び情報システム又はソフトウェアに不正なプログラムを埋め込むなど、国立研究開発法人産業技術総合研究所(以下、「産総研」という。)の意図しない変更が加えられたときに生じ得る情報の漏えい若しくは破壊又は機能の不正な停止、暴走その他の障害等の情報セキュリティ上のリスク(以下「サプライチェーン・リスク」という。)に対応するため、受注者は「IT 調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ」(平成 30 年 12 月 10 日関係省庁申合せ)及び指示書に基づく対応を図らねばならない。

2. 意図しない変更に対する対策

- ①受注者は、本業務の履行に際して、サプライチェーン・リスクが潜在すると知り、又は知り得べきソースコード、プログラム等(以下「ソースコード等」という。)の埋込み又は組込みその他調達請求者の意図しない変更を行ってはならない。
- ②受注者は、本業務の履行に際して、サプライチェーン・リスクが潜在すると知り、又は知り得べきソースコード等の埋込み又は組込みその他調達請求者の意図しない変更が行われないように相応の注意をもって管理しなければならない。
- ③受注者は、本業務の履行に際して、情報の窃取等により研究所の業務を妨害しようとする第三者から不当な影響を受けるおそれのある者が開発、設計又は製作したソースコード等(受注者がその存在を認知し、かつ、サプライチェーン・リスクが潜在すると知り、又は知り得べきものに限り、主要国において広く普遍的に受け入れられているものを除く。)を直接又は間接に導入し、又は組み込む場合には、これによってサプライチェーン・リスクを有意に増大しないことを調査、試験その他の任意の方法により確認又は判定するものとする。

3. サプライチェーン・リスクにかかる調査の受入れ体制

- ①受注者は、本業務に調達請求者の意図しない変更が行われるなど不正が見つかったときは、追跡調査や立入検査等、産総研と連携して原因を調査し、サプライチェーン・リスクを排除するための手順及び体制を整備し、当該手順及び体制を示した書面を調達請求者に提出しなければならない。

4. サプライチェーン・リスクを低減するための対策

- ①受注者は、サプライチェーン・リスクを低減する対策として、本業務の設計、構築、運用・保守の各工程における不正行為の有無について定期的または必要に応じて監査を行う体制を整備するとともに、本業務により産総研に納入する納入物品に対して意図しない変更が行われるリスクを回避するための試験を行わなければならない。当該試験の項目は、情報セキュリティ技術の趨勢、対象の情報システムの特性等を踏まえ、受注者において適切に設定し、少なくとも以下の6項目については必ず実施しなければならない。

- (1) 環境設定されたパラメータの再確認
 - (2) 製造中に利用したアカウントの削除の確認
 - (3) ウイルスチェック
 - (4) 不要なソフトウェアパッケージの削除の確認
 - (5) 使用ソフトウェアのバージョン管理の確認
 - (6) ソフトウェアのインストール手順書(インストールソフトウェアの名称及び設定パラメータ内容を含む手順書をいう。)の完成度の確認
- ②受注者は、前項の試験に関し、試験毎に試験チェックリストを作成し、調達請求者に提出しなければならない。
- ③機器の納入であり、かつ、設計、構築、運用・保守の各工程が存在しない場合は、4. ①及び②の対応は不要。

5. 受注者の資本関係・役員等の情報等に関する情報提供等

- ①受注者は、本業務の履行に従事する業務責任者及び業務従事者(契約社員、派遣社員等の雇用形態を問わず、本業務の履行に従事する全ての従業員をいう。以下同じ。)を必要最低限の範囲に限るものとする。
- ②受注者は、サプライチェーン・リスクの注意喚起と提出書類の指示書に基づき書面で提出する以下の情報に従い、本業務を履行しなければならない。なお、当該情報に変更がある場合は、変更の内容を記載した申請書を産総研に提出し、書面による事前承認を受けなければならない。
- (1) 受注者及び本業務の一部を再委託する者の資本関係及び役員等の情報
 - (2) 本業務に係る各工程の実施場所(産総研及び産総研以外のそれぞれの場所)
 - (3) 本業務の履行に従事する業務責任者及び業務従事者の氏名、所属、役職、専門性(特に、情報セキュリティに係る資格、研修実績、情報セキュリティ業務での経験年数)
 - (4) 本業務の履行に従事する業務責任者及び業務従事者の国籍(雇用対策法(昭和41年法律第132号)第28条第1項に基づき事業主が厚生労働大臣に届け出る事項として、雇用対策法施行規則(昭和41年労働省令第23号)第10条第1項第3号に規定される国籍の属する国等をいう。以下同じ。)別の人数
- ③機器納入であり、かつ、設計、構築、運用・保守の各工程が存在しない場合は、5. ①及び②の対応は不要。

6. 再委託

6.1 本業務の第三者への委託の制限

受注者は、産総研の許可なく、本業務の一部又は全部を第三者(再委託先)に請け負わせてはならない。ただし、6.2 に定める事項を遵守する場合はこの限りではない。

6.2 第三者への委託に係る要件

- ①受注者は、本業務の一部又は全部を第三者に再委託するときは、再委託先の事業者名、住所、再委託対象とする業務の範囲、再委託する必要性について記載した承認申請書を、委託元である産総研に提出し、書面による事前承認を受けなければならない。

- ②受注者は、本業務の一部又は全部を第三者に再委託するときは、再委託した業務に伴う再委託者の行為について、全ての責任を負わなければならない。
- ③受注者は、知的財産権、情報セキュリティ(機密保持を含む。)及びガバナンス等に関して、本仕様書が定める受注者の責務を再委託先も負うよう、必要な処置を実施し、その内容について委託元である産総研の承認を得なければならない。
- ④受注者は、受注者がこの仕様書の定めを遵守するために必要な事項について本仕様書を準用して、再委託者と約定しなければならない。
- ⑤受注者は、前号に掲げる情報の提供に加えて、再委託先において本委託事業に関わる要員の所属、専門性(情報セキュリティに係る資格・研修実績等)、実績及び国籍についての情報を委託元である産総研へ提出すること。
- ⑥受注者は、再委託先において、産総研の意図しない変更が加えられないための管理体制について委託元である産総研に報告し、許可又は確認(立入調査)を得ること。

7. その他

- ①別表に掲げる資料、書面及び指示書に基づき提出された資料等により調達請求者に報告された内容について、サプライチェーン・リスクが懸念され、これを低減するための措置を講じる必要があると認められる場合に、会計担当者は受注者に是正を求めることがあり、受注者は相当の理由があると認められるときを除きこれに応じなければならない。なお、機器の納入であり、かつ、設計、構築、運用・保守の各工程が存在しない場合は、7. ①の対応は不要。
- ②産総研は、受注者の責めに帰すべき事由により、本情報システムに調達請求者の意図しない変更が行われるなど不正が見つかった場合は、契約条項に定める契約の解除及び違約金の規定を適用し、本業務契約の全部又は一部を解除することができる。

(別表)

番号	名称		資料、書面等の内容	提出時期	様式
1	納入物品に対して意図しない変更が行われるリスクを回避するための試験チェックリスト		受注者の納入物品に対して意図しない変更が行われるリスクを回避するための試験項目が記載された書面	試験実施前まで	任意
2	履行に従事する従業員等		資本関係・役員等の情報等に関する情報が記載された書面	契約の締結後遅滞なく	任意