仕　様　書

1.件名：医療データのための匿名化暗号ソフトウェアのプロトタイプ実装

2.研究の概要

2-1. 概要・目的

国立研究開発法人産業技術総合研究所サイバーフィジカルセキュリティ研究部門(以下、「産総研」という。)では，経済安全保障重要技術育成プログラム（K Program）の「セキュアなデータ流通を支える暗号関連技術（高機能暗号)」のサブ課題「医療ＩＣＴの高度化を促進する高機能暗号の開発とその汎用化」を実施している。その課題の一つに、患者情報等を暗号化したまま匿名加工を施すことが可能な匿名化暗号があり（以下、「本課題」という。)、特に電子カルテを匿名化して複数の機関で共有する機能の実現を目指している。

3.ソフトウェアの概要

本件は、匿名化された電子カルテ共有システムのコアとなる暗号エンジンの開発である。今後、本課題で開発される匿名化された電子カルテの共有システムに組み込むことを念頭に、入力される電子カルテに対する汎用性を維持した開発を行うこととする。

4.ソフトウェアの構成

本業務において開発すべき匿名化暗号ソフトウェアのプロトタイプは、以下の3つの機能群で構成される。これらの機能を実現するソースコード、バイナリ、設計書を作成すること。

4-1：匿名化された医療データの暗号化機能
4-2：暗号化機能で暗号化されたデータの保持機能

4-3：暗号化されたデータサーバからのデータ取得機能

各機能の詳細仕様については、「5. 構成別開発仕様詳細」で記載する。

5. 構成別開発仕様詳細

以下では各プログラムの詳細な仕様について述べるが、まず本開発で扱われる「匿名化された医療データ」について記載する。

＜匿名化された医療データ＞

以下では、医療機関が所有する患者ひとりひとりの電子カルテのデータを生データと呼び、生データに含まれる情報は、通常の電子カルテに含まれる情報（氏名・年齢・住所・既往歴等）とする。生データに含まれる情報は 100 種類程度を想定する。本開発で用いる生データはテストデータであり、実際の患者データは扱わない。開発時に用いるテストデータは、開発時に受注者が 4 万件程度用意するものとする。生データの例を表 1 に記す。

表 1：生データの例。

氏名	年齢	住所	病傷名	既往歴	・・・
産総研　太郎	53	東京都港区..	高血圧	水疱瘡...	・・・
産総研　花子	32	大阪府堺市..		糖尿病...	・・・

匿名化とは、生データに含まれる情報を加工し、個人が一意に特定できないよう加工する処理である。一つの情報に対して複数のパターンの匿名化を施すことがある。(例：生データの年齢 54 歳に対して、「50 代」「40 歳以上」などと加工する)。そのため、一つの情報（電子カルテ)に対し、複数のパターンの匿名化を施すことがある。また、基本的に必ず匿名化する情報（名前、住所、生年月日など)と、通常匿名化するが場合によっては匿名化しない項目（家族構成、病歴等)、基本的に匿名化しない項目（経過記録等）を想定する。現状 3～4 パターンを想定するが、詳細については別途協議する。このように作成したデータを匿名化データと呼ぶ。

匿名化データは、csv などの表形式で表現されるものとする。行は一人の患者を表し、列は一つの情報を表す。先述の通り、一つの情報に対して複数のパタ

ーンの匿名化を施しているため、一人の患者に対して様々なパターンの匿名化データが存在し得る。（つまり、これらの匿名化のパターンごとに列が存在する。）なお、生データの情報がそのまま含まれる列も存在する。この表における一つのセルを項目と呼ぶ。匿名化データの例を表 2 に記す。

表 2：匿名化データの例。「年代」「閾値」は年齢を匿名化した項目である。

氏名	匿名氏名	年齢	年代	閾値	・・・
産総研　太郎	S. T.	53	50 代	40 歳以上	・・・
産総研　花子	S. H.	32	30 代	40 歳未満	・・・

匿名化データは、固定されたものを扱い、更新等の処理は行われないものとする。また、生データを匿名化する機能の開発は、本開発では求めない。

5-1：匿名化されたデータの暗号化機能

本機能は、匿名化されたデータを入力として受けとり、そのデータを暗号化する。

5-1-1：動作環境

暗号化機能は、ECIES などの国際標準化された Key Encapsulation Mechanism (KEM)を用いて実現することとし、暗号化機能は、開発言語として Python を用いて実装され、Windows10 以降の Windows OS 上で動作するものとする。KEM は、以下の三つ組のアルゴリズムで定義される。

KeyGen$(1^{\lambda})\rightarrow$(PK, SK) ：セキュリティパラメタ 1^{λ} を入力とし、公開鍵 PK と秘密鍵 SK を出力する。

Encap(PK)→(k, E)：公開鍵 PK を入力とし、共通鍵 k と、k をカプセル化した E（以下「カプセル E」という）を出力する。特に k を用いてデータ m を暗号化して暗号文 C を生成することを Enc(k, m)→C と表す。

Decap(SK, E)→k：秘密鍵 SK とカプセル E を入力とし、共通鍵 k を出力する。特に k を用いて暗号文 C を復号してデータ m を出力する処理を Dec(k,C)→m と表す。

5-1-2：実装仕様

- 入力：匿名化データ（CSV 形式)、KEM 公開鍵 PK
- 出力：暗号化データの集合 {(C_i, E_i)}
- 機能要件：
  本機能は、以下の処理を順に実行する。
  a) データ取得機能の鍵を、KeyGen(1$^{\lambda}$)→(PK, SK)に基づいて生成する。暗号化機能は、データ取得機能の KEM 公開鍵 PK のみを所持しているとする。
  b) 暗号化は、暗号化データの項目（これを m_i とする）ごとに以下の動作を行う：Encap(PK)→(k_i, E_i)、 Enc(k_i, m_i)→C_i。項目の定義については、「匿名化された医療データ」を参照すること。
  c) 暗号化機能は、全ての項目 m_i について、(C_i, E_i)をデータサーバに送信する。これらの情報に基づいて作られるものを暗号化データと呼称する。

5-2：暗号化機能で暗号化されたデータの保持機能

本機能は、匿名化されたデータの暗号化機能から送信されたデータを保持し、クライアントからの取得要求に応答する。また、暗号化データを（あらかじめ用意された）データベースに保持する機能を備える。

5-2-1：動作環境

本機能は、(Ubuntu24.04 以上のバージョンの)Linux OS 上で動作するものとする。

5-2-2：実装仕様

入力：暗号化データ {(C_i, E_i)}

出力：クライアントからの指定に応じたデータセット

機能要件：

- データの永続化機構を持ち、整合性・完全性を保つこと。
- アクセス要求に対して指定項目のデータを適切に返すこと。

5-3：暗号化されたデータサーバからのデータ取得機能

本機能は，データサーバから暗号化データを取得し、KEM 復号によって元の匿名化データを復元する。

5-3-1：動作形態

本機能は、web API として実現し、コマンドラインから操作するものとする。また、本機能については、クライアント側の処理は、Python を用いて実装され Windows10 以降の Windows OS 上で動作し、サーバ側の処理は、(Ubuntu24.04 以上のバージョンの)Linux OS 上で動作するものとする。

5-3-2：実装仕様

- 本機能は、取得したいデータをデータサーバに要求する。その際には、所望する項目を項目名（カラム名）で指定しなければならない。
- データ取得機能を持つクライアントは、秘密鍵 SK を所持しているものとする。クライアントは、秘密鍵 SK を使用して、データサーバからの応答で得た暗号文を適切に処理（具体的には、Decap(SK, E_i)→k_i, Dec(k_i, c_i)→m_i を実行）し、(匿名化された）データ m_i を取得する。

6.特記事項

作業者は上記作業の実施にあたり、以下の要件を満たしていること。

- 匿名加工の製品を提供可能であること。
- 楕円曲線のペアリングを利用した高機能暗号の実装実績があること。
- CRYPTREC での活動経験のあるメンバーが含まれていること。
- 匿名加工技術、属性ベース暗号等の開発実績があること。
- IACR 主催国際会議において発表された高機能暗号に関する当該発表論文およびその他一般的な公開情報のみに基づく高機能暗号方式の実装実績、さらに、同高機能暗号方式に基づく情報セキュリティシステム開発実績を有すること。

7.完成品の試験・確認

産総研担当者の立ち会いのもと、受注者は「9. 納入物品」で示されたプログラム設計書およびプログラムの使用方法に関する取扱説明書に記載されている操作手順を実際に実行し、仕様書に記載されている機能・性能が実現されていることおよびドキュメント類の内容・品質を確認すること。

8.支給品・貸与品

なし

9.納入物品（提出文書、電子ファイル、ソースコード等）

納入物品は、原則として安全なファイル共有サービスを用いて電子データで納入すること。

9-1：4-1～4-3 の機能のソースコード、バイナリ、設計書　一式

9-2：9-1 に関する取扱説明書　１部

9-3：データの暗号化や取得等にかかる時間等を評価した性能評価書　１部

10.納入場所

東京都江東区青海 2-3-26

国立研究開発法人産業技術総合研究所

サイバーフィジカルセキュリティ研究部門

臨海副都心センター　本館 1104 室

11.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「7. 完成品の試験・確認」に従って確認して、納入の完了とする。受注者は確認にかかる作業を支援すること。

12.納入期限

2025 年 10 月 31 日（金）

13.成果の取扱い

13-1: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。）は、受注者がプログラム作成により得られた技術上の成果のうち産総研が指示するもの（以下「成果」という。）についての利用及び処分に関する権利を専有するものとする。

13-2:受注者は、成果に係るソフトウェアの著作権（著作権法第 27 条及び第 28 条に規定する権利を含む。）及び意匠登録を受ける権利を産総研に譲渡するものとし、著作者人格権を行使しないものとする。ただし、パッケージ製品に係るものは除く。

13-3:受注者は、産総研に対し、納品した成果品が第三者の知的財産権を侵害しないことを保証するものとする。なお、納品した成果品について、第三者の権利侵害の問題が生じ、その結果、産総研又は第三者に費用や損害が生じた場合は、受注者は、その責任と負担においてこれを処理するものとする。

14. セキュリティ要件

14-1:情報セキュリティポリシーに関する要件

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(別途定める読み替え条項に従うものとする。以下同じ。)を遵守するとともに、情報セキュリティポリシーにおいて産総研に求められる水準の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受注者決定後に提示する。

【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

② 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、見直しの内容に応じ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担当者に事前に報告し承認を得ること。

14-2: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貸与品は産総研担当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、産総研担当者に提出すること。なお、契約終了後、速やかに返却又は廃棄し、産総研担当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産総研担当者に提出すること。
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、産総研担当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、事前に産総研担当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。

⑫産総研担当者より、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。

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産総研担当者と協議の上、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、当該成果物を産総研担当者の許可を得て、抹消すること。また、受注者は、産総研担当者の指示に従い、当該成果物の抹消の確認を受けること。

15.付帯事項

15-1:受注者は、産総研担当者の求めにより、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。

15-2:納入時には、本プログラムの操作について講習を行うこと。

15-3:納入されたプログラム等における発注側の責めによらない納入の完了後1年以内の動作不良等不具合については、その補修、調整等責任をもって無償で速やかに行うこと。

15-4:本仕様書の技術的内容及び知り得た情報に関しては、守秘義務を負うものとする。

15-5: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。また、本仕様書に定めのない事項及び疑義が生じた場合は、調達担当者と協議のうえ決定する。

15-6: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。

別紙

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）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、又は知り得るべきソースコード、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産総研担当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、又は知り得るべきソースコード等の埋込み又は組込みその他産総研担当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、又は知り得るべきものに限り、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、本業務に産総研担当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産総研担当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するものとする。

②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の対応は不要。

5. 受注者の業務責任者等

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提出された資料等により産総研担当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、調達担当者は

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。

②産総研は、受注者の責めに帰すべき事由により、本情報システムに産総研担当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。