仕　様　書

1.件名：医療データのための空間ベース暗号ソフトウェアのプロトタイプ実装

2.研究の概要

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、ある医療施設が患者情報を暗号化し、近隣施設等のみが復号できる暗号化方式（空間ベース暗号）があり、特に緊急時に必要最低限の施設のみが、患者の受け入れ可否などを確認するための情報を得られ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、緊急時等の医療情報共有システムのコアとなる空間ベース暗号エンジンの開発である。今後、本課題で開発される緊急時等の医療情報共有システムに組み込むことを念頭に、入力される医療データ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空間ベース暗号ソフトウェアのプロトタイプは、以下の四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：医療機関の鍵生成局機能
4-2：位置情報に関する鍵生成局機能

4-3：時刻情報に関する鍵生成局機能
4-4：医療データの暗号化機能

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、まず本開発の概要を述べる。本開発では、「属性ベース暗号（Attribute-Based Encryption, ABE)」並びに「階層型 ID ベース暗号（Hierarchical Identity-Based Encryption, HIBE)」という暗号技術を用いる。これらの技術に関する説明は、各プログラムの詳細な仕様の中で行う。本開発の全体像を図 1 に示す。

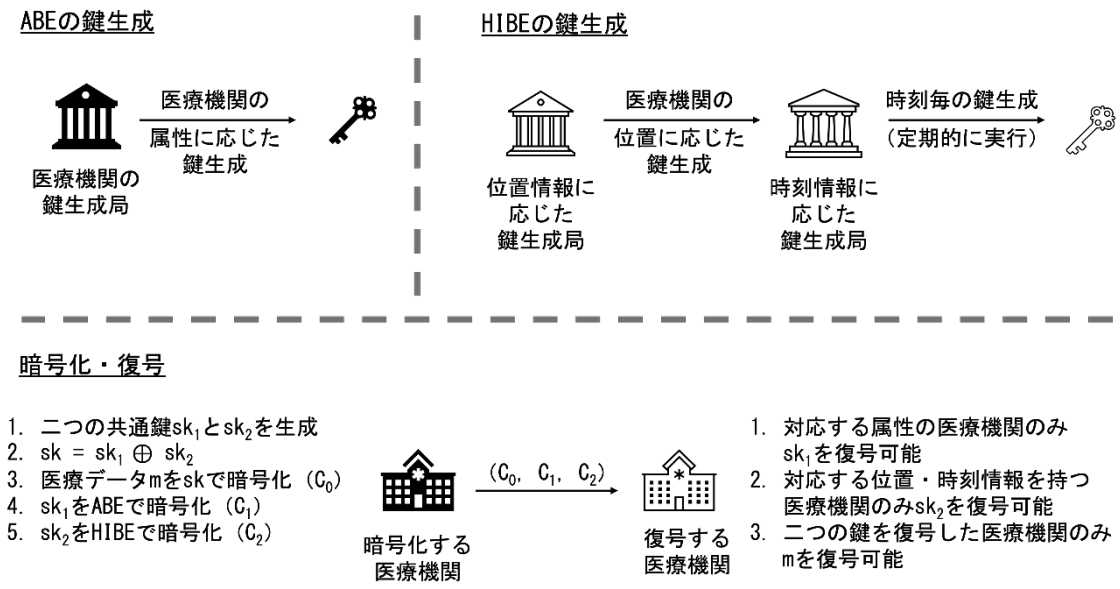

図 1：本開発の全体像

(4-1)医療機関の鍵生成局機能は、医療機関の外部にある信頼できる第三者機関が実行するものであり、ABE による鍵生成を行う。各医療機関の属性に応じた秘密鍵を生成し、送信する。この鍵は医療機関の初期設定時に一度だけ発行されるものである。また、ABE の公開鍵を本鍵生成局初期設定時に発行しており、各医療機関は初期設定時に公開鍵を取得する。

(4-2)位置情報に関する鍵生成局機能は、医療機関の外部にある信頼できる第三者機関が実行するものであり、位置情報を HIBE の第一層とみなした鍵生成

を行う。各医療機関の位置情報に基づく秘密鍵を生成し、送信する。位置情報は市区町村程度の粒度を想定しており、この鍵はある位置情報（市区町村）に医療機関が初めて加わる際の初期設定時に一度だけ発行されるものである。また HIBE の公開パラメタを本鍵生成局機能の初期設定時に発行しており、各医療機関の初期設定時に一度だけ HIBE 秘密鍵と公開パラメタを取得する。

(4-3)時刻情報に関する鍵生成局機能は、医療機関が実行することを想定した機能であり、時刻情報を HIBE の第二層とみなした鍵生成を行う。医療機関の初期設定時に取得した HIBE 秘密鍵と公開パラメタを用いて、時刻に基づく秘密鍵を、あらかじめ定められたタイミングで定期的に生成する。あらかじめ定められたタイミングとは、例えば 1 日を 6 時間ごとに四分割したもので、医療機関が次の 0～6 時の間は患者が受け入れられると判断した場合その時間帯の秘密鍵を生成する。

(4-4)医療データの暗号化機能は医療機関が担う。暗号化の方法については図 1 を参照すること。医療機関はまず共通鍵 sk_1 と sk_2 を生成し、$sk = sk_1 \oplus sk_2$ を計算する。患者の医療データを sk を用いて暗号化し、さらに sk_1 と sk_2 をそれぞれ ABE と HIBE で暗号化する。ABE で指定する属性は、医療機関の専門性や救急医療の度合いなどである（属性に関しては 5-1-2 節を参照のこと）。例えば内科の二次救急を指定して ABE 暗号文が作成された場合、内科を持つ二次救急指定病院のみがこの暗号文を復号し，sk_1 を得られる。HIBE は所望する搬送先の位置情報と現在時刻を指定して暗号文を作成する。例えば 13 時に A 市を指定した場合、A 市にあってかつ 12～18 時に受け入れ可能という秘密鍵を生成した医療機関のみが、HIBE 暗号文を復号し，sk_2 を得られる。このように sk_1 と sk_2 を復号できた医療機関のみが、$sk = sk_1 \oplus sk_2$ を求めることができ、従って患者の医療データを復号できる。

5-1：医療機関の鍵生成局機能

本機能は、医療機関の属性ごとに ABE の秘密鍵を生成する。

5-1-1：動作環境

ABE の方式は、文献[1]の 3 章に記述されている暗号文ポリシー型の方式を用いる。本機能は、Linux および Windows OS 上で動作するものとする。ABE は以下の四つのアルゴリズムで定義される。ただし、これらのアルゴリズムは一般的な記述であることに留意すること。方式の実装時に用いるペアリングの曲線のタイプやパラメータは協議の上、決定するものとする

ABE.Setup(U)→(PK,MSK)：属性集合全体 U を入力として受け取り、公開鍵 PK とマスター秘密鍵 MSK を出力する。

ABE.KeyGen(MSK,S)→sk_S：マスター秘密鍵 MSK と属性集合 S ⊆ U を入力として受け取り、この属性に対する秘密鍵 sk_S を出力する。

ABE.Enc(PK, γ, m)→C：公開鍵 PK、アクセス構造 γ、メッセージ m を入力として受け取り、暗号文 C を出力する。

ABE.Dec(sk_S, C) = m：秘密鍵 sk_S と暗号文 C を入力として受け取る。もし S が C を作成する際のアクセス構造 γ に対して γ(S)=1 を満たすならば m を出力する。

[1] Waters, B. Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization. PKC 2011.

5-1-2：属性集合

属性集合は以下の項目を含むものとする。

- 救急医療機関としての指定（三段階）
  - 一次救急・二次救急・三次救急
- 専門分野（六つ）
  - 内科・外科・循環器科・脳神経系・整形外科・マイナー
- 入院ベッドの有無

なお、医療機関が一次救急かつ二次救急として指定されることもあるため、ABE の属性全体集合は U = {一次救急, 二次救急, 三次救急, 内科, 外科, 循環器科, 脳神経系, 整形外科, マイナー, 入院ベッド有}という 10 個の項目を含むものとする。

属性集合 S は、「5-4：医療データの暗号化機能」で説明する暗号化機能で主に活用される情報である。ただし、S は U の部分集合であり、例えば S = {一次救急, 二次救急, 内科, 整形外科, 入院ベッド有}のような値を取る。つまり救急医療機関としての指定や専門分野は必ずしも一つに限定されないことに留意すること。医療データを暗号化する（つまり緊急搬送先を決定する）際に、受け入れ可能な医療機関のみが復号できるようにするために、ABE で属性を指定して暗号文を作成する。

5-1-3：実装仕様

- 入力：属性集合 $S \subseteq U$
- 出力：秘密鍵 sk_S
- 機能要件：本機能は、以下の処理を順に実行する。
  a) 公開鍵 PK とマスター秘密鍵 MSK を、ABE.Setup(U)→(PK,MSK)に基づいて生成し、PK を公開する。ただしこの処理は初期設定時のみ行われる。
  b) 秘密鍵 sk_S を、ABE.KeyGen(MSK,S)→sk_S に基づいて生成する。

5-2：位置情報に関する鍵生成局機能

本機能は、医療機関の位置ごとに HIBE の秘密鍵を生成する。

5-2-1：動作環境

HIBE の方式は、文献[2]または文献[3]に記述されている暗号文ポリシー型の方式を用いる。本機能は、Linux および Windows OS 上で動作するものとする。ABE は以下の四つのアルゴリズムで定義される。ただし、これらのアルゴリズムは一般的な記述であることに留意すること。方式の実装時に用いるペアリングの曲線のタイプやパラメータは協議の上、決定するものとする。

HIBE.Setup(t)→(pp,SK)：ユーザの最大階層数 t を入力として受け取り、公開パラメタ pp とルート秘密鍵 SK を出力する。

HIBE.KeyGen(ID,d_{j-1})→d_j：ユーザの ID = (I_1, ..., I_j)と、j-1 階層の秘密鍵 d_{j-1} を入力として受け取り、j 階層の秘密鍵 d_j を出力する。特に d_0 = SK である。

HIBE.Enc(pp,ID,m)→C：公開パラメタ pp、ユーザの ID、メッセージ m を入力として受け取り、暗号文 C を出力する。

HIBE.Dec(d_{ID},C)→m：ある ID の秘密鍵 d_{ID} と暗号文 C を入力として受け取る。C が ID に対して作られたものならば m を出力する。

5-2-2：階層と ID に関する設定

本件では階層が二つ、つまり t = 2 の HIBE を扱う。第一階層は位置情報であり、市区町村程度の粒度の位置情報を扱うこととする。第二階層は時刻情報である。第二階層については「5-3：時刻情報に関する鍵生成局機能」で説明する。

5-2-3：実装仕様

- 入力：位置情報 P
- 出力：位置情報に対する秘密鍵 d_P
- 機能要件：本機能は、以下の処理を順に実行する。
  a) 公開パラメタ pp とルート秘密鍵 SK を、HIBE.Setup(2)→(pp,SK)に基づいて生成し、pp を公開する。ただし、この処理は初期設定時のみ行われる。
  b) 秘密鍵 d_P を、HIBE.KeyGen(P,SK)→d_P に基づいて生成する。

[2] Gentry, C., Silverberg, A. Hierarchical ID-Based Cryptography. ASIACRYPT 2002.

[3] Boneh, D., Boyen, X. Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles. EUROCRYPT 2004.

5-3：時刻情報に関する鍵生成局機能

本機能は、時刻ごとにHIBEの秘密鍵を生成する。

5-3-1：動作環境

HIBEの方式は、「5-2：位置情報に関する鍵生成局機能」と同様のものとすること。本機能は、LinuxおよびWindows OS上で動作するものとする。方式の実装時に用いるペアリングの曲線のタイプやパラメータは協議の上、決定するものとする。

5-3-2：時刻情報

まず、本機能は医療機関等が担うものとする。医療機関は、位置情報に関する鍵生成局機能が生成したHIBE第一階層の秘密鍵を保有しており、定期的（6時間ごと等）に自組織が患者を受け入れられるかどうかを確認し、問題なければその時間の情報を含んだHIBE秘密鍵を生成する。ただし患者を受け入れられるかどうかの確認は運用によるところであり、本開発の対象外とする。また、時刻をどう具体的に設定するかについては今後協議の上、決定するものとする。

5-3-3：実装仕様

- 入力：位置情報P、時刻情報T、位置情報に対する秘密鍵 d_P
- 出力：位置・時刻情報に対する秘密鍵 d_{PT}
- 機能要件：本機能は、以下の処理を実行する。
  a) 位置・時刻情報に対する秘密鍵 d_{PT} をHIBE.KeyGen((P,T),d_P)→d_{PT}に基づいて生成する。

5-4：医療データの暗号化機能

本機能は、（緊急医療時の患者受け入れ可否の確認のために）医療データを共通鍵暗号（Symmetric Key Encryption, SKE）・ABE・HIBEを用いて暗号化する。また復号動作についてもここで記述する。

5-4-1：動作環境

ABE の方式は「5-1：医療機関の鍵生成局機能」と、HIBE の方式は「5-2：位置情報に関する鍵生成局機能」と同様のものとすること。本機能は Linux および Windows OS 上で動作するものとする。SKE は AES などの標準的なもので、特に共通鍵として（定められた長さの）ランダムビット列を用いる方式とする。
SKE は以下の二つのアルゴリズムで定義される。ただしこれらのアルゴリズムは一般的な記述であることに留意すること。方式の実装時に用いるペアリングの曲線のタイプやパラメータは協議の上、決定する。また、鍵生成アルゴリズムは陽に記述していない点にも留意すること。

SKE.Enc(sk,m)→c：共通鍵 sk とメッセージ m を入力として受け取り、暗号文 c を出力する。

SKE.Dec(sk,c)→m:共通鍵 sk と暗号文 c を入力として受け取り、m を出力する。

5-4-2：医療データ

医療データには以下のような情報が含まれる。

- 年齢
- 性別
- 発症状況
- バイタルサインや身体所見
- 既往歴やアレルギー、家族の付き添いの有無
- 服薬情報
- 蘇生処置の希望

これらは機微情報であるためみだりに配布できない一方で、緊急医療の際には具体的な受信者を指定せず配布する必要がある。この条件を達成するために、ある属性を満たす医療機関であり、かつある時刻にある場所に存在するもののみが情報にアクセスできるような方法が求められる。そのために、ABE で医療機関の属性を指定した暗号文を、HIBE で位置情報と時刻を指定した暗号文を作成する。

5-4-3：実装仕様（暗号化）

- 入力：医療データ m、位置情報 P、時刻情報 T、ABE の公開鍵 PK、アクセス構造 γ、HIBE の公開パラメタ pp
- 出力：医療データの暗号文$(C_0,\ C_1,\ C_2)$
- 機能要件：本機能は、以下の処理を順に実行する。
  a) あらかじめ定められた長さの二つビット列 sk_1 と sk_2 をランダムに生成する。さらに $sk = sk_1 \oplus sk_2$ を計算する。
  b) 暗号文を$(C_0,\ C_1,\ C_2)$を以下のように生成する。SKE.Enc(sk,m)→C_0、
  ABE.Enc(PK, γ, sk_1)→C_1、HIBE.Enc(pp, (P,T), sk_2)→C_2。

5-4-4：実装仕様（復号）

- 入力：医療データの暗号文$(C_0,\ C_1,\ C_2)$、ABE 秘密鍵 sk_S、HIBE 秘密鍵 d_{ID}、時刻情報 T、ABE の公開鍵 PK、アクセス構造 γ、HIBE の公開パラメタ pp
- 出力：医療データ m
- 機能要件：本機能は、以下の処理を順に実行する。
  a) ABE.Dec$(sk_S, C_1)=sk_1$、HIBE.Dec$(d_{ID}, C_2)=sk_2$ を求め、$sk_1 \oplus sk = sk$ を計算する。
  b) SKE.Dec(sk,C_0) = m を出力する。

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。

- 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 に代表される暗号技術に関する公的なプロジェクトで委員や技術報告活動経験のあるメンバーが含まれていること。
- 暗号アルゴリズムに関する学術論文などの文書を読解し、その内容を適切にソフトウェア実装を行う業務経験として、1 年以上の実務経験を有するメンバーが 2 名以上参画できること。

7. 完成品の試験・確認

産総研担当者の立ち合いのもと、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 11 月 28 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。