東海大学紀要情報通信学部
Vol.17,2024,pp.1-6

論文

Intel SGX を用いた新生児体重経過記録システムの実装

柿崎 淑郎[*1]，村瀬 友哉[*2]，森澤 辰哉[*2]，西平 侑磨[*3]，大東 俊博[*4]

Implementation of a Neonatal Weight Progress Recording System using Intel SGX

by

Yoshio KAKIZAKI[*1], Tomoya MURASE[*2], Tatsuya MORISAWA[*2], Yuma NISHIHIRA[*3] and Toshihiro OHIGASHI[*4]

(received on Oct.24,2024 & accepted on Jan.30,2025)

あらまし

医療現場等で医療機器の運用管理にあたっては，使用状況の管理や事後の責任追及のために状況の把握が求められており，セキュリティを確保するためには，誰が何をしているのかを適切に記録しなければならない．そのために重要な役割を果たすのが，認証と認可であるが，認証は利用者の能動的な行為によって行われることが基本であり，被認証者の負担になり，通常業務に影響を与える場合も少なくないため，認証を行うこと自体がなおざりになっている．本研究では，パッシブ認証を導入することで，通常業務を妨げることなく，責任追跡性と可監査性を達成することを目的として，新生児体重経過記録システムを提案し，Intel SGX を用いた実装を行う．

Abstract

In the medical field, managing medical devices requires tracking usage to ensure accountability after incidents. To enhance security, it is crucial to record user actions properly. Authentication and authorization are important for this purpose, but user-driven authentication can burden staff and disrupt workflows. In this study, we propose and implement a neonatal weight progress recording system in maternity services using Intel SGX. By applying passive authentication, our approach aims to achieve traceability and auditability without interrupting normal operations, ensuring security while minimizing the impact on staff and maintaining seamless workflow integration.

キーワード：産科業務，新生児体重経過記録，Intel SGX，属性ベース暗号

Keywords: *Maternity Services, Neonatal Weight Progress Recording, Intel SGX, Attribute-based Encryption*

1. はじめに

業務において，誰が何をしたかを記録することは，責任追跡性（Accountability），可監査性（Auditability）の観点から，重要である．責任追跡性を確保するためには，業務の行為者が誰であるかを明確にする必要があり，認証（Authentication）が適切に実施されなくてはならない．さらに可監査性は，業務の行為者が何をしたかを記録したログなどによって達成される．これらが適切に機能することで，不正アクセスや内部不正を防止し，業務の信頼性が保たれる．そのため，組織の健全性を保つためにも，認証や業務ログの取得は重要な要素である．

一方，認証は被認証者の能動的な行為によって行われることが基本であり，認証を行う行為自体が被認証者の負担になり，通常業務の遂行に少なからず影響を与えている．特に，業務が多忙であったり，セキュリティリテラシーが低かったりすると，認証がなおざりになり，離席中でもログインしっぱなしだったり，共用アカウントが利用されていたりすることも珍しくない．このような状況下では，認証結果に信頼性がないため，事故発生後にログを調べたとしても，誰が何をしたかを確信をもって検証することが困難になる．

このような現状を背景として，被認証者の負担にならない受動的な認証であるパッシブ認証を導入することで，通常業務を妨げることなく，責任追跡性と可監査性を達成することを目的として，産科業務における新生児の体重経過記録業務を対象としたシステムが，池田らによって提案され[1),2)]，柿崎らがリスク分析を行い[3),4)]，森澤を中心に著者らによって試作が行われている．

本研究では，森澤らの試作で用いられている共用デバイス上の秘密鍵が，悪意ある第三者に利用されることを防ぐために，Intel SGX（以下，SGX）[5)]を用いたシステムの提案と実装[6)]を行う．これによって，通常業務を妨げることなく，パッシブ認証によって責任追跡性と可監査性を達成するとともに，悪意ある第三者による不正利用を防ぎ，システムの完全性を実現する．

*1 情報通信学部情報通信学科 准教授
Department of Information and Telecommunication Engineering, Associate Professor
*2 情報通信学部通信ネットワーク工学科 卒業生
Department of Communication and Network Engineering, Former Student
*3 情報通信学研究科情報通信学専攻 修了生
Graduate School of Information and Telecommunication Engineering, Former Student
*4 情報通信学部情報通信学科 教授
Department of Information and Telecommunication Engineering, Professor

2. 準備

2.1 産科業務と新生児体重計測

日本の総合病院では，産科の 7 割以上が婦人科やその他内科・外科患者も対象にする混合病棟である [7), 8)]．産科業務は多忙であり，身体的に自立している褥婦や，日本の診療報酬では保険対象外となる健康な新生児へのケアが後回しにされている [9)]．また，混合病棟であるため，看護師は産科業務のみならず様々な業務を行う必要があり，その業務負担を減らすことは，事故防止の観点からも必要な措置である．そこで，産科業務の中でも，重要な業務の一つでありながら，電子化や自動化によって看護師の業務負担軽減が強く期待できる,新生児の体重計測について説明する．

産科業務において重要な業務の一つに，新生児の体重計測がある．

新生児は，生後数日間で一時的に体重が減少し，出生時体重を下回る．これを生理的体重減少といい，生後一週間程度で出生時体重に戻る．生理的体重減少は，一般的に出生時体重の 5〜10%程度の範囲で減少するが，それ以上に減少しないように，モニタリングと適切な対応が必要となる．

新生児の体重測定は沐浴時に実施されることが多いため,新生児用の体重計であるベビースケールは沐浴室に設置されていることが多い．体重測定の際は，新生児が寝ているコットからベビースケールに移して行うが，転落等の事故防止のため，看護師は細心の注意を払って作業を行う．体重計測後は，そのまま沐浴を行うか，沐浴をせずにコットに戻るかのいずれかであるが，この際も，看護師は新生児から目を離すことはできない．そのため， 沐浴を伴う体重計測時においては，沐浴が終わり，計測体重を記録することができるまでの間，看護師が暗記しておく必要がある．最終的に計測結果は検温表に転記されるが，沐浴室から出た後に行われるため，体重変化の経過を直ちに授乳量へ反映することが困難である．また，体重計測のみで沐浴を行わない場合は，数名の新生児を一人の看護師で立て続けに対応することがあり，記録の正確性に問題が生じ得る．

2.2 Intel SGX

Intel Software Guard Extensions (SGX)[5)] は，Intel が開発した CPU レベルのセキュリティ技術であり,信頼性の高い実行環境（Trusted Execution Environment，TEE）を提供することを目的としている．SGX では，プログラムコードとデータを保護された領域であるエンクレーブと呼ばれる特定のメモリ領域内で実行することで，悪意のあるソフトウェアやハードウェアからの攻撃に対して耐性を有する．この技術により，アプリケーションの一部が暗号化されたメモリ内で実行され，オペレーティングシステムやハイパーバイザといった高特権のソフトウェアであっても，エンクレーブ内のデータにアクセスできないというセキュリティモデルが実現されている．

エンクレーブ内のデータは，メモリ外への出力時には，CPU に内蔵されている鍵から導出される派生鍵によって，Sealing され，プロセッサ外部に保存される場合でもデータの機密性と整合性が保たれる．これにより，アプリケーションが信頼できない環境，例えば，クラウドや共用環境などで実行される場合でも，データの漏洩や改ざんを防止することが可能になる．

SGX は，リモートアテステーションを通じて，外部の第三者に対してエンクレーブが正しく設定されていることを証明することができる．リモートアテステーションの証明プロセスでは，エンクレーブが正当に生成され，要求されたセキュリティ条件を満たしているかどうかを確認するために，プロセッサが特別な証明データを生成し，この証明データを用いて，リモートの第三者はエンクレーブが適切に動作していることを検証でき，これによって，クラウドや分散コンピューティング環境での安全な実行を保証することができる．

SGX の活用範囲は幅広く，データのプライバシ保護や機密情報の管理，またはセキュアな計算プロトコルの実装に利用される．例えば，医療データや金融データの保護，クラウド上での機密データ処理などに利用されることが多い.これらの用途では，通常の実行環境では実現が困難な高い機密性を保持したまま計算を行う必要があり，SGX によってそれが可能となっている．

3. 新生児体重経過記録システムの試作

このような産科業務において，池田らは，看護師の記録作業を低減する新生児の体重経過記録システム（以下，記録システム）を提案しており [1), 2)]，森澤を中心に著者らがプロトタイプ実装を行っている．この記録システムでは，Fig. 1 に示すように，ベビースケールと無線接続された記録デバイスが，ベビースケールから計測結果を取得する．新生児と看護師は個別の Bluetooth ビーコンを所持しており，記録デバイスは体重計測時に周辺にいる新生児と看護師を識別し，計測対象となる新生児の候補を表示する．看護師が計測対象の新生児を選択し，確認ボタンを押すことで，新生児の計測結果を記録者（看護師）と紐づけて，データベースに記録する．記録デバイスは計測結果をデータベースに記録するとともに，計測対象新生児の経過記録をデータベースから取得し，体重の経過をグラフ化し，ディスプレイに表示することで，看護師は新生児の生理的体重減少の状態を一目で確認することができる.これによって，看護師の暗記を要することなく，体重計測記録が自動で行え，業務負荷を軽減するとともに，正確な記録を可能とする．

なお，本研究においては，正規産であり治療を必要としない新生児の体重経過管理を対象としている．このような新生児は，出産後から退院までの間の入院は，褥婦に付随するものと見做されており，入院患者とは見做されない．そのため，新生児のカルテは作成されないのが一般的であり，退院までの記録については，医療機器としての認証を取得しないものであっても，利用可能である．

プロトタイプ実装したシステムの前提条件は以下の通りである．

- すべての新生児と看護師は，それぞれに Bluetooth ビーコンが割り当てられており,ビーコン送信されている識別番号でそれぞれを識別可能である．
- 看護師はいくつかのグループに分けられており,所属するグループの新生児のみを担当する．
- すべての新生児はいずれかのグループに所属する．

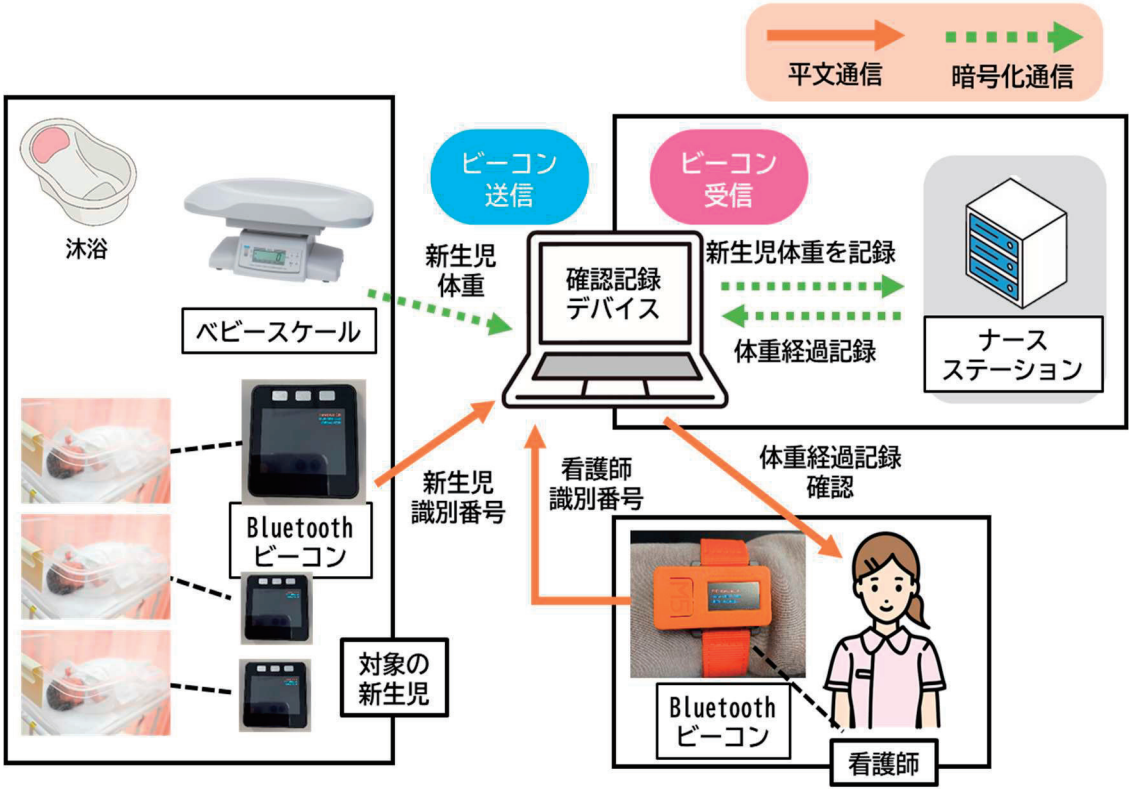

Fig. 1　System Configuration Diagram.

- 看護師は役職，担当業務，所属グループなどの属性を持ち，その属性による属性ベース暗号の秘密鍵（以下，属性鍵）がナースステーション上の KGC で生成され，割り当てられ，確認記録デバイス（以下，記録デバイス）内に保存している．
- 新生児の体重経過記録（以下，体重 DB）はグループの看護師だけが復号できるように属性ベース暗号で暗号化されている．

ここで，属性ベース暗号[10]は，ユーザの属性を秘密鍵（属性鍵）とし，その属性に合致した暗号文を復号できる公開鍵暗号方式の一つである．なお，ここでは復号条件（ポリシー）を暗号文に関連付ける暗号文ポリシー属性ベース暗号（CP-ABE）を単に属性ベース暗号と呼ぶ．KGC は鍵生成センタ（Key Generation Center）のことであり，属性ベース暗号に用いられる属性鍵を生成する信頼できる第三者機関である．

体重計測時においては，Bluetooth ビーコンの信号強度から，ベビースケール上の新生児と，記録デバイスのもっとも近くにいる看護師を識別し，識別された新生児の体重 DB を看護師の属性鍵によって記録デバイス上で復号し，復号された体重 DB を確認するとともに，ベビースケールで計測した記録を追記し，再暗号化して，保存する．もし，看護師と新生児が異なるグループであった場合，復号条件が合わないため，新生児の体重 DB は復号されない．

しかしこの方法では，属性鍵を記録デバイス上に保管する必要があるが，記録デバイスを複数の看護師が利用する共用デバイスのため，もし他人の属性鍵を不正に利用することができた場合，権限のない新生児の体重 DB を閲覧および改ざんができる問題がある．

4. 提案方式

4.1 システム概要

本研究では，記録デバイス内の SGX を用いて，属性ベース暗号による体重 DB の復号と再暗号化を行う．これによって，新生児体重経過記録システムのプロトタイプ実装における，記録デバイスでの属性鍵管理の問題を解決する．

プロトタイプ実装では，新生児の体重計測を行う看護師が共用利用する記録デバイスにおいて，属性ベース暗号による復号と再暗号化を行っており，またそれらに用いる看護師の属性鍵を保管していた．そのため，記録デバイスにアクセス可能な攻撃者（正規利用者が不正を行う場合も含む）が，看護師の属性鍵を不正に利用することができた場合に，体重 DB を復号したり，改ざんしたりすることができてしまっていた．

提案方式では，看護師の属性鍵を記録デバイスの SGX 内に格納し，また SGX 内で属性ベース暗号による復号と再暗号化の処理を実行することで，安全ではない記録デバイスにおいても，属性鍵の不正利用ができないように対策を行う．なお，提案方式の実装にあたって，属性ベース暗号は，複数の KGC に対応した Multi-authority 型の属性ベース暗号（MA-ABE）[11]を用いる．別の研究グループによる SGX 内で利用可能な属性ベース暗号の実装として，MA-ABE がすでにあったため，本来は MA-ABE を必要としないが，特段の影響はないため，提案方式の実装に採用する．

4.2 実装環境

記録デバイスは，CPU は Intel Core i5-10400H （SGX 対応），OS は Ubuntu16.04 のマシンを用いた．ナースステー

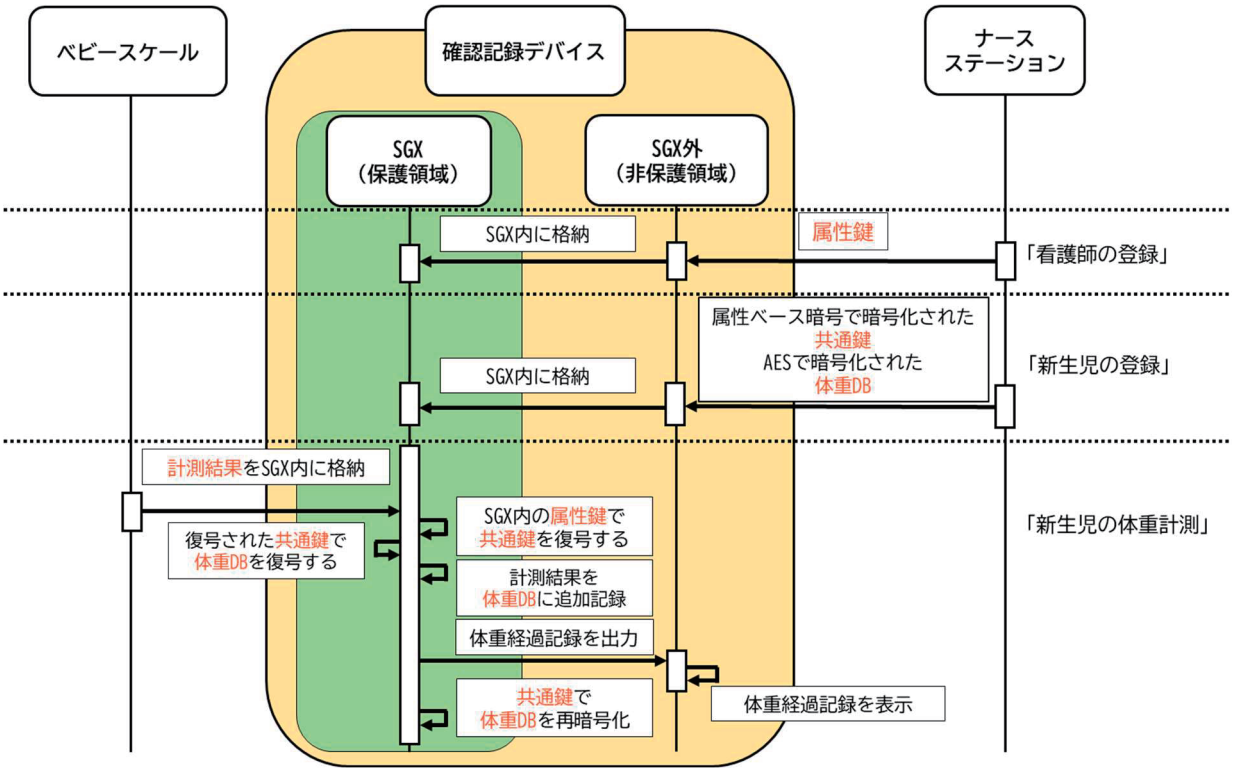

Fig. 2　System Sequence Diagram.

ションは，SGX を必要としないが，属性ベース暗号を利用するため，記録デバイスとナースステーションは，実装上は同一マシン上の別アプリケーションとして実装した．また，ベビースケールでの体重計測を模擬するために，記録デバイス上で，適当な値を出力することとした．看護師と新生児の Bluetooth ビーコンとして，それぞれ M5StickC と M5Stack を用いた．

4.3 処理手順

提案方式の処理手順について説明する．提案方式では，SGX を適用したことにより，その処理手順を 3 つのフェーズに分けて行われる．提案方式の処理手順を Fig. 2 に示す．

4.3.1 看護師の登録

看護師が持つ Bluetooth ビーコンと，看護師の属性に基づいた属性鍵の生成と，それらを関連付ける“看護師の登録”フェーズを行う．

役職や担当業務，所属グループなどの看護師の属性は，病院の職員管理システム，ナースステーションにおける勤務簿などから取得する．ナースステーションの KGC において，看護師の属性に基づいた属性鍵を生成する．生成した属性鍵と看護師の Bluetooth ビーコンの識別番号を，リモートアテステーションを用いて安全に記録デバイス内の SGX に格納する．

4.3.2 新生児の登録

新生児の Bluetooth ビーコンと新生児の体重 DB との関連付け，および体重 DB を暗号化する“新生児の登録”フェーズを行う．

新生児が産まれたら，Bluetooth ビーコンを割り当て，適切なグループに割り当てる．また，空の体重 DB を作成し，体重 DB と Bluetooth ビーコンの識別番号を関連付ける．体重 DB を共通鍵暗号である AES で暗号化し，グループの看護師だけが復号できるように，AES の共通鍵を属性ベース暗号で暗号化する．属性ベース暗号で暗号化された共通鍵，AES で暗号化された体重 DB，新生児の識別番号を，リモートアテステーションを用いて安全に記録デバイス内の SGX に格納する．

なお，提案方式の純粋な実装にあたっては，共通鍵暗号は不要であるが，体重 DB が膨大になった場合も考慮し，属性ベース暗号に比べて高速に暗号化/復号が行える共通鍵暗号を併用したハイブリッド暗号化を採用している．

4.3.3 新生児の体重計測

新生児の Bluetooth ビーコンと看護師の Bluetooth ビーコン，およびベビースケールからの体重計測結果を体重 DB に登録する“新生児の体重計測”フェーズを行う．

看護師が新生児の体重計測を開始すると，
確認デバイスは Bluetooth ビーコンの信号強度から，測定者である看護師と被測定者である新生児を識別し，特定する．ベビースケールでの体重計測結果は，リモートアテステーションを用いて安全に記録デバイス内の SGX に格納する．確認デバイスの SGX 内で，特定された看護師の属性鍵を用いて，共通鍵を復号する．また，復号した共通鍵を用いて，特定された新生児の体重 DB を復号する．このとき，新生児が所属するグループと看護師が所属するグループが一致していれば，体重 DB は復号されるが，一致していなければ復号されない．確認デバイスの SGX 内で，復号された体重 DB に計測結果を追記し，記録デバイスの SGX 外に体重経過記録を出力し，SGX 外のディスプレイに表示する．最後に，復号した共通鍵を用いて，体重 DB を再暗号化するとともに，復号した共通鍵は消去する．

これらの復号および再暗号化に係る処理はすべて記録デバイスの保護領域である SGX 内で行われるため，不特定

多数が利用する記録デバイスにおいても高い機密性が維持されており，安全に利用することができる．

5. 考察

5.1 看護師と新生児の識別

本システムでは,看護師と新生児の識別に Bluetooth ビーコンの識別番号を用いている．Bluetooth ビーコンは無線信号であるため，誤識別が生じる可能性がある．池田らが予備実験を実施しており [1]，無線の受信信号強度（RSSI）によって距離推定ができることを確認しており，ベビースケールで体重計測中の新生児は，Bluetooth ビーコン受信機の直上にいるため，RSSI が非常に強く，誤識別の可能性はほぼなかった．ただし，看護師は新生児の近くで体重計測を行うため，RSSI が強く，誤識別の可能性は低かったが，沐浴室に複数の看護師がいる場合，どちらがよりベビースケールに近いかについては，誤識別が考えられた [4]．そのため，看護師については，体重計測している一定時間の平均 RSSI を用いることにより,誤識別を避けることが可能となった．

以上より，沐浴室内に複数の看護師および複数の新生児がいたとしても，Bluetooth ビーコンの識別信号で測定者および被測定者を識別することが可能である．

5.2 責任追跡性と可監査性

何らかの事故が発生した場合に，誰がいつ何をしたのかを業務記録から確認できることは，責任追跡性の観点から重要である．これは責任を追及するのみならず，正しい業務手順で業務を行っていたことの証明や，故意ではなく過失であることを証明する上で，必要となる．また，責任追跡性に必要となる業務記録が，信用できるものであり，改ざんされていないことは，可監査性を達成する上で，重要である．

5.1 節で考察したように，Bluetooth ビーコンの識別番号では，本人によるアクティブな認証ではなく，パッシブ認証であるため，誤識別の可能性が排除しきれないが，業務スケジュールや勤務実態などのコンテキスト情報と突合することで，高い確度で信頼できる記録が作成できる [3]．

もし，沐浴室の監視カメラ映像をリアルタイムに利用でき，映像から人物検知が行えたとすれば，映像から検知した人物と記録デバイスが識別した人物が同一であるかどうかを検証することが可能であり，責任追跡性が高まる．

記録システムは計測体重の記録のみならず，新生児体重計測の開始から終了まで，周辺の新生児や看護師の Bluetooth ビーコンの識別番号と RSSI を記録することで，事後に時系列を検証することができる．これにより，記録デバイス周辺に誰がいて，どのような順序で体重計測を行ったかを検証することができ，可監査性に耐えうるログを残すことができる．

このように，本システムにおいていくつかの運用上の対策を組み合わせることで，責任追跡性と可監査性は十分に確保できる．

5.3 看護師の作業時間の軽減

池田らが標準的な動作時間に基づいた作業時間の軽減について考察しており [2]，新生児一人あたりの計測時間として，標準的な動作では 53.4 秒であるところ，本システムでは 5.4 秒であり，およそ 90%の作業時間短縮が見込まれると試算している．この試算では，ベビースケールからの体重計測結果が自動で記録されるため，標準的な動作で必要となるメモ，メモから検温表への転記などが不要となっている．そのため，これらの動作における人為的ミスの可能性も排除されており,記録の正確性が高まっており,また，記録が即時に反映されることから，ナースステーションの看護師が体重 DB を参照すれば，沐浴後の授乳量に即座に反映させられる効果もある．

5.4 記録デバイスの安全性

4.1 節で説明したように,新生児体重経過記録システムのプロトタイプ実装においては，共用デバイスである記録デバイスにおいて,属性ベース暗号の復号/再暗号化を行っており，またそれに用いる属性鍵も保管されていた．本システムでは，記録デバイスの SGX を用いて，SGX 内で属性ベース暗号の処理を行うことで，この問題への対応を行っている．

Fig. 2 に示したように，体重 DB を復号するために必要な共通鍵は，リモートアテステーションを用いて安全に記録デバイス内の SGX に格納する．また,属性ベース暗号で暗号化された共通鍵を復号するために必要な属性鍵も，リモートアテステーションを用いて安全に記録デバイス内の SGX に格納する．体重 DB の復号/再暗号化は SGX 内で行われ，また，その際に必要となる共通鍵，属性鍵のいずれもが SGX 内にのみ存在し，非保護領域である SGX 外には露出しない．

そのため，記録デバイスにおいては，被測定者である新生児と測定者である看護師が同じグループでなければ，体重 DB は復号されることがない．また，記録デバイスにおいて，看護師が体重経過記録を確認するために，復号された体重 DB の内容が,非保護領域である SGX 外に出力されるが，このデータを改ざんしたとしても，SGX 内に入れる手段はなく，また再暗号化もできないため，改ざんは実現しない．

このように，属性ベース暗号の処理を SGX 内で行うことで，プロトタイプ実装において存在した問題を解決し，複数の看護師が利用する共用デバイスであっても，安全に利用することができる．

6. おわりに

本研究では,産科業務における新生児体重計測について，計測・記録の自動化による看護師の作業負担軽減を目的とした新生児体重経過記録システムを作成し，共用デバイスにおいても安全に利用できるように,Intel SGX を用いて実装を行った．本システムでは，Bluetooth ビーコンによる測定者と被測定者の識別により,通常業務を妨げることなく，責任追跡性と可監査性を達成することができる．また，新生児の体重計測および記録業務が自動化できることで，多忙を極める看護師の業務負担を軽減することができ，業務効率化が期待できる．

謝辞

本研究の一部は，公益財団法人立石科学技術振興財団研究助成，JSPS 科研費（課題番号 22K12034）の助成を受けたものである．

参考文献

1) 池田彰希，吉田美香子，柿崎淑郎，土井根礼音，桑名健太：看護師の記録作業を低減する出生後入院中の新生児の体重経過記録システムの提案，第 8 回看護理工学会学術集会 (2020). P8-08.
2) 池田彰望，吉田美香子，柿崎淑郎，土井根礼音，桑名健太：看護師の記録作業を低減する新生児の体重経過記録システムの計測対象の認識特性評価，ライフサポート学会 第 31 回フロンティア講演会 (2022). 1A04.
3) 柿崎淑郎，土井根礼音，桑名健太，吉田美香子： 通常業務を妨げないパッシブ認証の検討, 情報処理学会研究報告, pp. 1–5 (2021). Vol.2021-IS-155 No.14.
4) Kaikizaki, Y., Doine, R., Kuwana, K. and Yoshida, M.: Implementing passive authentication with enhanced risk-based security, Proc. of 2022 16th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), IEEE, pp. 78–83 (online), DOI: 10.1109/SITIS57111.2022.00020 (2022).
5) Intel: Intel Software Guard Extensions, https://software.intel.com/en-us/sgx/details. （閲覧日 2024 年 10 月 19 日）
6) 村瀬友哉，森澤辰哉，西平侑磨，大東俊博，柿崎淑郎： Intel SGX を用いた新生児体重経過記録システムの提案と実装, 2024 年電子情報通信学会総合大会 (2024). A-19-05.
7) Otaki, C., Saito, I., Izumi, S. and Osawa, K.: Analysis of night-shift nurses' locations and durations using information communication equipment: A prospective observational study of a mixed obstetric ward with severe patients in Japan, Journal of Nursing Science and Engineering, Vol. 7, pp. 13–24 (online), DOI: 10.24462/jnse.7.0 13 (2020).
8) Otaki, C., Saito, I., Izumi, S. and Osawa, K.: Analysis of day shift nurses' and midwives' locations and durations using information communication equipment: A prospective observational study of a mixed obstetric ward with critical patients in Japan, Journal of Nursing Science and Engineering, Vol. 7, pp. 130‐140, DOI: 10.24462/jnse.7.0 130 (2020).
9) 木下勝之，齋藤いずみ，井本寛子，松永智香： 産科混合病棟で十分なケアを, https://www.igaku-shoin.co.jp/paper/archive/y2019/PA03331_01 (2019).
10) Sahai, A. and Waters, B.: Fuzzy Identity-Based Encryption, EUROCRYPT 2005, Springer Berlin Heidelberg, pp. 457–473 (2005).
11) Rouselakis, Y. and Waters, B.: Efficient Statically-Secure Large-Universe Multi-Authority Attribute-Based Encryption, Financial Cryptography and Data Security, Springer, pp. 315–332 (2015).