Vol.2021-IS-155 No.14
2021/3/9

通常業務を妨げないパッシブ認証の検討

柿崎 淑郎[1,a)]　土井根 礼音[1]　桑名 健太[1]　吉田 美香子[2]

概要：医療現場等で医療機器の運用管理にあたっては，使用状況の管理や故障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，認証は基本的に，利用者の能動的な行為によって行われることがほとんどであるので，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，認証がなおざりになっている．本研究は，そのような状況下において，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する．本稿では，産科業務においてパッシブ認証を導入するにあたっての検討結果を報告する．

1. はじめに

業務において，誰が何をしたかは，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）を適切に実施しなくてはならない．その上で，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，可監査性が達成される．これらが正しく適切に機能しない場合，不正アクセスや内部不正が発生し，業務の信頼性が損なわれる．結果として，厳しい業務ルールが課せられたり，職場内での不信感が高まったりして，業務効率が低下し，最終的には組織の機能不全に至る．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極めて重要である．

一方で，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る．そのため，認証を行う行為は，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．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，共用アカウントが利用されていたり，離席中でもログインしっぱなしだったりすることも珍しくない．このような状況下においては，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，誰が何をしたかを検証することが困難になる．

本研究では，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する．本稿では，産科業務をケーススタディとしてリスク分析を行い，認証精度とリスクのバランスについて検討し，業務における受容性を考慮した議論を行う．

[1] 東京電機大学
[2] 東北大学大学院
[a)] kakizaki@mail.dendai.ac.jp

2. 認証の三要素

2.1 知っていることによる認証

知っていること（Something You Know; SYK）による認証は，広く一般的に用いられており，パスワードや暗証番号など，被認証者の知識による認証である．

盗聴や推測，あるいは辞書攻撃や全数探索などによって，パスワードを第三者に知られたとしても，本人はその事実に気づきにくい．また，パスワードを探索するコンピュータの性能は年々向上するため，安全なパスワードには十分な長さが必要となるが，パスワードを記憶する人間の記憶力は飛躍的に向上しないので，被認証者の負担となっている．

パスワードは複雑性を増したり，パスワード長を長くすれば，安全性は向上する一方で，十分に長いパスワードは覚えるのが困難であったり，入力に時間がかかったり，入力を誤る危険性が増したりする．また，認証時にはキーボードなどからパスワードを入力するため，被認証者の負担は必ず発生する．

2.2 持っているものによる認証

持っているもの（Something You Have; SYH）による認証は，IC カードや物理的な鍵など，被認証者の所有物による認証である．

IC カードをカードリーダーにかざしたり，鍵を鍵穴に挿入するなど，被認証者の能動的な行動を必要とするもの

ⓒ 2021 Information Processing Society of Japan

もあるが，ビーコン等の自ら電波を発信することで，被認証者の能動的な行動を必要としない認証もある．知識による認証に比べて，パスワード等の記憶や入力が必要ないため，利便性が高い．一方では，所有物の貸し借りや紛失，盗難などによって，真正な所有者以外がなりすまして利用することもできる．

2.3 本人の特徴による認証

本人の特徴（Something You Are; SYA）による認証は，指紋認証や顔認証などの，生体情報に基づく生体認証である．近年では，多くのスマートフォンで生体認証が採用されており，広く一般的に利用されるようになってきた．

知識による認証ではパスワードを忘れてしまったり，所有物による認証では所有物をなくしてしまったりするが，生体認証では被認証者本人の生体情報を用いるため，そのような問題はなく，利便性が高い．一方では，手袋をしたり，マスクをしたりすると，生体情報を正しく読み取ることができず，認証が行えない問題がある．また，指紋認証器など専用のデバイスが必要であるなど，実装コストが比較的高い上に，本人拒否率や他人受入率によって，本人であっても認証精度が 100%にならない不安定さがある．

3. ケーススタディ：産科業務

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 [1,2]．そのため，産科業務は多忙であり，身体的に自立してる褥婦や，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 [3]．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，事故防止等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，新生児体重計測についてケーススタディをする．

3.1 新生児体重計測

新生児は，取り違えを防ぐために，図 1 に示すようなネームバンドを足首などにつけて，識別されている．業務の電子化が進んでいる場合，ネームバンドに ID が付与されていたり，バーコードが付与されたりすることもある．

新生児は生後 2, 3 日の間は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 1 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．そのため，出生後から退院までの間，体重管理が重要になっている．

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，

図 1 新生児のネームバンド装着例

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．この際も，看護師は新生児から目を離すことはできないうえに，転落等の事故防止のために両手は常にフリーにしておく必要がある．そのため，計測した体重は看護師が暗記しておくか，一瞬新生児から目を離してメモに記録するので，記録の正確性が損なわれたり，新生児の安全性が損なわれたりする．計測結果は最終的に検温表に転記されるが，全新生児の計測終了後に行われるため，体重変化の経過を授乳量にすぐに反映することができず，転記時に誤りが生じることもある．また，体重計測のみである場合は，2, 3 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る．

ここで，正期産であり治療を必要としない新生児の場合，出生後から退院までの入院は褥婦に付随するものであり，入院患者とみなされないため新生児のカルテが作成されず，記録のみに留められていることも少なくない．この場合の記録は，褥婦のカルテに記録されたり，電子カルテシステムとは別のシステムに記録されたりしており，その扱いは分娩施設によって異なる．

3.2 記録作業の低減

このような産科業務において，我々の研究グループでは，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，記録システムとする）を提案している [4]．この記録システムでは，図 2 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を設置し，ベビースケールから計測体重を取得する．また，新生児と看護師は UHF タグを所持しており，記録デバイスは計測時に周辺にいた新

ⓒ 2021 Information Processing Society of Japan

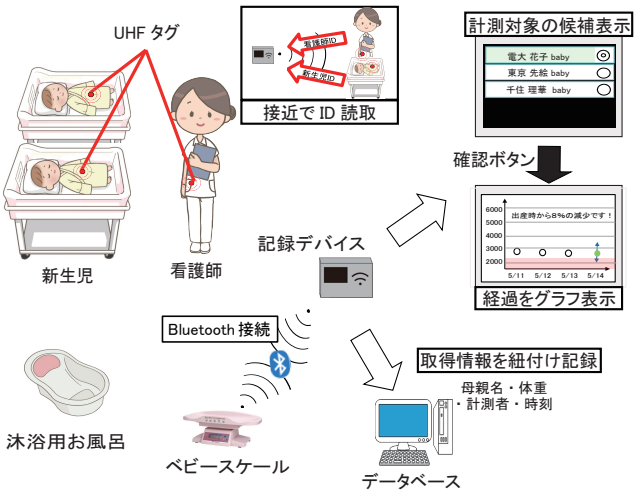

図 2 新生児体重経過記録システムの概要（文献 [4] より引用）

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，新生児の計測体重を記録者と紐づけて，データベースに記録する．記録デバイスは計測体重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，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．

このシステムでは，計測対象である新生児と記録者である看護師を，それぞれが所持する UHF タグを用いた所有物認証を行っている．本稿では，産科業務において本記録システムを利用する上で，所有物によるパッシブ認証を用いることによるリスクとその対応について議論を行う．

4. 通常業務を妨げないパッシブ認証の検討

4.1 検討の目的

記録システムの主たる目的は，通常業務を妨げることなく，計測体重を記録することにある．記録の信頼性を確保するためには，計測対象者である新生児を識別し，計測している記録者である看護師を識別し，それらを合わせて記録することが求められる．

この際には，対象者の認証を行うことになるが，通常業務を妨げる方式では，産科業務における安全性を損ない，業務負担が増加すれば，使われないシステムとなる．そのため，通常業務において，さらなる負担を与えることなく，安全性と利便性を確保することが必要となる．

安全性と利便性が確保されれば，通常業務の一部を電子化することができる．また，記録の電子化によって，紙から電子カルテ等への転記が不要になり，また転記の際の誤入力もなくなり，結果として看護師の業務負担が軽減できる．

認証には 2 章で挙げた三要素が用いられるが，知っていることによる認証は，パスワードや暗証番号などにより認証するため，被認証者はキーボード入力やタッチパネル操作などの何らかの能動的な動作を必要とする．

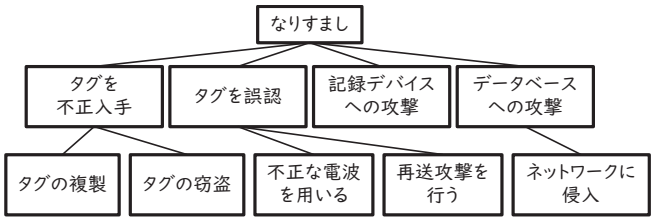

図 3 なりすましのアタックツリー分析

本人の特徴による認証は，指紋認証や顔認証などの生体認証であり，知っていることによる認証よりは通常業務を妨げにくい．しかしながら，医療従事者である看護師は，マスクや手袋を付けていることが少なくないため，指紋認証や顔認証を利用できない場面が少なくない．

持っているものによる認証では，ビーコン等の電波を自ら発信するものを利用すれば，被認証者の能動的な行動を必要としないパッシブ認証が可能である．

よって，本稿では，産科業務における新生児の体重計測時に，UHF タグを用いたパッシブ認証が許容できるかどうかをリスク分析を行い，考察する．

4.2 リスク分析

記録システムにおいては，以下のリスクがあげられる．

(1) 誤った計測値を記録する
(2) 記録を改ざんする
(3) 記録を削除する
(4) 異なる新生児として記録する
(5) 異なる記録者として記録する
(6) 第三者が記録を閲覧する
(7) 記録システムを使用不能にする

上記のリスクのうち，“記録を改ざんする”，“記録を削除する”，“記録システムを使用不能にする” は，新生児の体重計測とその記録時に発生するリスクではなく，記録システム自体のリスクである．本稿では，新生児の体重計測とその記録時において，新生児や看護師の認証にパッシブ認証を適用可能かどうかのリスク分析であるため，“異なる新生児として記録する” と “異なる記録者として記録する” および “第三者が記録を閲覧する” を対象として分析する．また，これらは “なりすまし” としてまとめることができるため，“なりすまし” のアタックツリー分析 [5] による脅威分析を行う．“なりすまし” のアタックツリー分析の結果を図 3 に示す．

まず，“タグを不正入手” する攻撃を考える．この攻撃方法としては，“タグの複製” あるいは “タグの窃盗” が考えられる．UHF タグから出力される電波は暗号化されていないため，タグの複製は難しくない．一方で，入院患者

の取り間違いを防ぐために，手首や足首などに識別用のタグを用いることは一般的であり，また，そのタグに付いたバーコードを読み取って，患者を識別することも一般的に行われている．そのため，このような識別用タグに電波を発する機能が付加されたとしても，“タグを不正入手” する攻撃としては，従来と同様であり，従来と同じ対策で対応可能である．

次に，“タグを誤認” させる攻撃について，考える．攻撃方法の一つとして，“不正な電波を用いる” 方法がある．この方法では，平文の正規な通信から，一部を変更した不正な通信によって，その場には存在しないタグと同じ電波を発信することで，タグを誤認させる．対策としては，暗号によって通信路を暗号化する対策が考えられるが，UHF タグでは，電波のブロードキャストであるため，暗号化は期待できない．Bluetooth など暗号化可能な通信で置き換えることで，この攻撃を防ぐことができるが，ビーコンの送信側の電力供給や稼働可能時間などを考慮する必要がある．

もう一つの攻撃方法として，“再送攻撃を行う” 方法がある．この方法は，平文通信でも暗号化通信でも，正規の通信をそのまま再送する攻撃である．正規の通信を再送するので，再送された通信かどうかを識別できなければ，再送攻撃を受け入れてしまう．暗号化通信であれば，通信内容にタイムスタンプや乱数を含め，同じタイムスタンプや乱数が含まれた通信は再送であると判別することができる．

暗号化されていない平文通信では，“不正な電波を用いる” 方法も “再送攻撃を行う” 方法も防ぐことは難しい．一方で，タグから記録デバイスまでの通信で重要なのは，UHF タグの ID である．記録システムでは，UHF タグから発信される ID を元に，その ID に対応した記録対象者である新生児をデータベースから取得する．そのため，データベースに存在しない ID を記録デバイスが受信しても，記録対象者が存在しないので，記録は行われない．データベースに存在する ID の場合，記録デバイスが記録を開始しようとするが，図 2 に示すように，記録対象者の候補が画面に表示されて確認ができるため，看護師が誤認しなければ，なりすましは行われない．

攻撃者が看護師になりすます場合，看護師が行うべき確認が行われないため，新生児のなりすましも防ぐことができない．そのため，看護師のなりすましは十分に効果的な対策を行う必要がある．

近年では，防犯や医療事故防止などの観点から，病棟に監視カメラが導入されていることも少なくない．監視カメラは，入院患者の見守り，侵入者の監視などの常時監視に加えて，なんらかの事故があった際に，看護師等の医療従事者を守るための証拠としても利用される．プライバシー問題から，病室に設置されることは少ないものの，廊下に設置されていることは多い．この監視カメラの映像を活用することで，沐浴室に入室した看護師と記録デバイスが認証した看護師が異なっている場合，看護師がなりすましを行っていることを特定することができる．

4.3 考察

リスク分析の結果から，記録システムをパッシブ認証で利用する際には，以下の点に注意することが求められる．

(1) 記録デバイスはベビースケールの周辺でのみ利用する
(2) 看護師は計測対象の新生児と記録デバイスが認証した新生児が同一であることを確認する
(3) パッシブ認証で利用中は，新生児の計測体重を記録するデータベース以外の業務システムには接続しない
(4) 安全性を高めるために，監視カメラ等の周辺情報を活用し，パッシブ認証の結果を検証する

1 は，記録デバイスからの不正アクセスを防ぐために，正規の場所でのみ使われるために必要である．記録デバイスはベビースケールと Bluetooth でペアリングされており，ベビースケールの周辺に記録デバイスがあるのであれば，記録デバイスは正規の場所である沐浴室で利用されていると推定できる．

2 は，記録の信頼性のために必要である．立て続けに新生児の体重計測を行う場合，記録デバイス周辺に複数に新生児がいることがある．その際には，記録デバイスのディスプレイには，計測対象の候補が複数表示される．看護師は表示された候補の中から，記録対象者を正しく選ぶことが必要である．これは，体重計測時のみならず，取り違えを防ぐために必要な通常業務であり，正規の看護師であれば正確に実施することが期待できる．また，記録デバイスとベビースケール，コットの位置関係を適切にすることで，電波強度が最も強い記録対象者を強調するなどによって，看護師が記録対象者を正しく選ぶ際に，手助けをすることも可能と考えられる．

3 と 4 は，パッシブ認証のリスクを低減するために必要である．リスク分析の結果より，UHF タグでのパッシブ認証では，なりすましのリスクは無視できないため，なりすましが行われた場合における影響を最小限にする必要性がある．記録デバイスは新生児の計測体重を記録するために，データベースに接続するが，それ以外の業務システムに接続しないようにアクセス制御することで，なりすましによる業務システムへの影響を防ぐことが重要である．また，監視カメラの映像から，パッシブ認証された看護師と沐浴室にいる看護師が同一であるかを確かめることで，なりすましのリスクを低減することができる．このように，パッシブ認証だけでは認証結果の信頼性に不安がある場合でも，監視カメラ等の周辺情報を活用することで，パッシブ認証の結果を検証し，安全性を高めることができる．

4.4 責任追跡性と可監査性

記録システムの記録に問題が見つかった場合，その記録

ⓒ 2021 Information Processing Society of Japan

を行った看護師を特定できるかどうかは，責任追跡性において重要な要素である．

先に考察したように，UHF タグでのパッシブ認証では，なりすましのリスクは無視できないが，監視カメラ等の周辺情報を活用することで，パッシブ認証の結果を検証することができる．また，沐浴室以外にもビーコンなどが設置されていたり，周辺に看護師がいたりする場合，それらの情報を合わせて記録することで，記録が行われた位置の推定や周辺にいた看護師からのヒアリングなどで，記録の正当性を検証することも考えられる．

もし，監視カメラの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，記録デバイスが行うパッシブ認証に組み入れることで，映像から検知した人物と記録デバイスが UHF タグから認識した人物が同一でなかった場合に，データベースへの接続を遮断するアクセス制御が行え，記録システムとしての認証精度が向上し，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 UHF タグから読み取られた ID と電波強度を記録することで，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，パッシブ認証に加えて，いくつか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. おわりに

本稿では，多忙を極める参加業務の中でも，電子化や自動化によって看護師の業務負担軽減が期待できる，新生児体重計測について，UHF タグを用いたパッシブ認証の採用におけるリスク分析を行った．新生児の体重計測結果を記録するデータベースを電子カルテシステムなどの業務システムとは別に分離すれば，なりすましのリスクがあるパッシブ認証であっても，その影響は許容範囲内である．また，監視カメラや周辺のビーコンなどを活用することで，パッシブ認証の結果を検証することができ，責任追跡性と可監査性を確保することも可能である．

謝辞

本研究は公益財団法人立石科学技術振興財団研究助成の助成によるものである．

参考文献

[1] 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).

[2] 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 (オンライン), DOI: 10.24462/jnse.7.0_130 (2020).

[3] 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 (2019). https://www.igaku-shoin.co.jp/paper/archive/y2019/PA03331_01.

[4] 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.

[5] Schneier, B.: Attack trees, Dr. Dobb's journal, Vol. 24, No. 12, pp. 21–29 (1999).

ⓒ 2021 Information Processing Society of Japan