JAHIS

JAHIS標準 25-×××

Japanese

Association of

Healthcare

Information

Systems Industry

JAHIS
ヘルスケア分野における
監査証跡の
メッセージ標準規約
Ver.2.2

2025 年 X 月

一般社団法人

保健医療福祉情報システム工業会

医療システム部会　セキュリティ委員会

JAHIS ヘルスケア分野における監査証跡の
メッセージ標準規約 Ver.2.2
ま え が き

2005 年 4 月の個人情報保護法完全施行に伴い、保健医療福祉分野において2つのガイドライン（「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」*1、「医療情報システムの安全管理に関するガイドライン」）が出された。これらの中では医療機関に対して、個人情報の取り扱いに関する「説明責任」が求められている。これを果たすためには、システムが適切に運用されていることを証拠として示すことが重要であり、そのためには第三者が検証可能なレベルの監査証跡を残すことが重要である。医療機関に医療情報システムを提供しているベンダとしては、技術的対策としてシステムに監査証跡を残す機能を実装し、医療機関の運用において余計な負荷がかからないようにする必要がある。そこで JAHIS としては、日本の現状および国際的な監査証跡の標準化の動向を踏まえ、RFC3881 をベースとした標準的な監査証跡のメッセージ規約の必要最小限の基準を 2006 年 3 月に制定した。

その後、ISO や IHE 等で検討されている規格や標準化の内容を踏まえ、より詳細で効率的な監査を可能にするために、監査ログ出力イベントを追加したものに 2010 年 2 月に改訂を行った。

2014 年 3 月には、これまで引用規格としてきた DICOM Supplement95（その時点では Frozen Draft）が標準となった際に内容が変更されたことと、ISO で検討されていた ISO27789 が出版されたことを受け、それらとの整合をとるようにメッセージ内容の改訂を行った。

2021 年 5 月には、引用規格である DICOM PS3.15 の改訂が行われ、複数のイベント ID とイベントタイプコードが追加され、ISO27789 でもそれに応じた改定が進んでいることに対応したメッセージ内容の改訂を行った。

今回は、引用規格である DICOM PS3.15 の改訂が行われ、項目のオプションの変更が行われたので、それに対応した改訂を行った。

本ガイドラインが、医療情報の普及・推進に多少とも貢献できれば幸いである。

*1:2017 年 4 月 14 日に「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」として発行

2025 年月

一般社団法人 保健医療福祉情報システム工業会
医療システム部会 セキュリティ委員会

目　次

1. 目的と適用範囲

1.1. 目的

本規約においては監査証跡のうち「医療情報システムの安全管理に関するガイドライン」において求められている業務アプリケーションの監査ログのログメッセージ規約を策定する。本規約において規定する監査ログは以下の目的で利用されることを想定している。

(1)　個人情報へのアクセス履歴の確認
(2)　医療機関が説明責任を果たすために利用
(3)　副次的効果としての目的外アクセスの抑止
(4)　情報システムのセキュリティ監査

「個人情報へのアクセス履歴の確認」は、医療機関として管理責任を果たすために必要な管理を実施する際に行われるもので、問題の発生を検知するための利用や、セキュリティ対策の改善を検討するための利用などを想定している。

「医療機関が説明責任を果たすために利用」は、患者からの自己の情報の利用についての問い合わせに答える際にその証拠として利用する場合や、情報セキュリティ監査を受ける際に運用状況を説明するための証拠として利用する場合などを想定している。

「副次的効果としての目的外アクセスの抑止」は監査証跡を取得していることを関係者に周知することで、不正行為や犯罪行為などの目的外行為を行った場合にそれが管理者に把握されやすいことを認識させ、目的外行為を心理的に抑止するなどの効果を狙っている。

「情報システムのセキュリティ監査」は、情報システムが施設ごとのセキュリティポリシにしたがって適正に運用されているかどうかを確認する監査業務における証拠を収集することを想定している。

1.2. 策定方針

本規約は、監査証跡に関し、システムが技術的に担保しなければならない監査ログメッセージの規約を定めたものであり、メッセージの生成タイミングや通信手段などの実装方式については規定しない。また、監査イベントについては、必要最小限の基準とオプションを定めている。特に配慮したのは以下の二点である。

(1)　技術で担保する部分を明確にし、運用も含めた監査手法の確立を補助する。
(2)　監査証跡の粒度を明確にし、運用に余計な負荷がかからないようにする。

また、本規約の策定に当たっては、標準的な形式を採用し、ユーザ側に不必要な手間が発生しないようにすることを重視し、以下の二点に注意して策定を行った。

(1)　マルチベンダのシステムでも統一された監査証跡の管理が可能であること。
(2)　最低限の要件を明確にした上で、将来の拡張に対する自由度を持たせること。

メッセージ形式としては、医用画像と通信の標準規格である DICOM Part15 Security and System Management Profiles で規定されている Audit Trail Message Format Profile を採用した。

1.3. 適用範囲

1.3.1. 対象モデル

ここでは、本規約において対象とする情報システムのモデルを図1. 3-1 のように定義する。

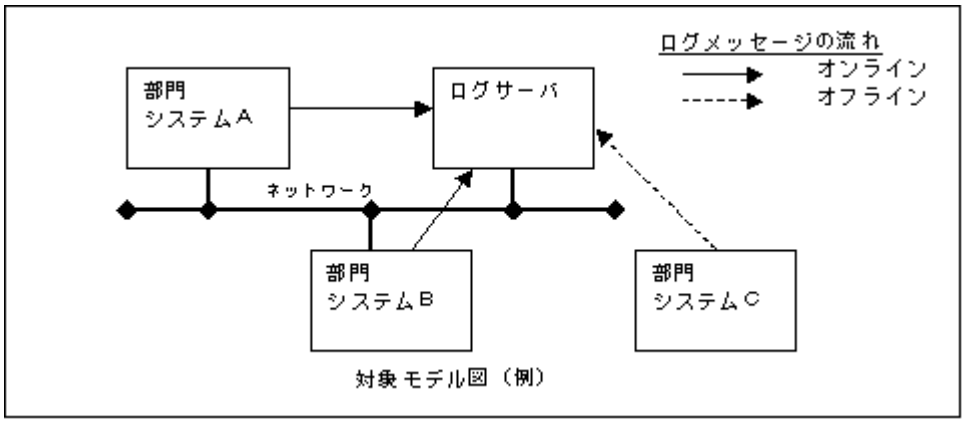

図1.3-1 対象モデル図

(1)　機能的に独立した2つ以上の情報システムから構成された、複合型の情報システムであること

補足説明

本規約の目的は監査ログのメッセージを策定することにあるので、ここではメッセージの標準化が必要な2つ以上の情報システムからなる複合システムを対象とする。もちろん、単一の情報システムで構成されるシステムにおいても、将来のシステム拡張を考慮したり、監査ログの標準化を考慮したりすると、本規約に従った監査ログを収集することは有意義であり、実装を妨げるものではない。

(2)　複合型の情報システムが、任意のシステム形態(トポロジ)の情報システムから構成されること。

補足説明

ここでいうシステム形態とは、いわゆるスタンドアロン型、クライアント・サーバ型、ホスト・端末型(Web 型もこの範疇のバリエーションと考えてよい)など、情報システムを構成する要素の物理的・論理的な配置を意味している。

(3)　それぞれの情報システムを構成する機能要素(端末、サーバ等)の物理的配置が、当該の医療機関の敷地内で閉じていることを前提としないこと。

補足説明

医療機関の敷地外からのシステム利用、いわゆる遠隔利用を行なう場合、システム形態によっては、遠隔地にある端末側で監査ログを収集するケースが想定される。本規約は、そのような場合も対象とする。

(4)　それぞれの情報システムにおいて、保護対象となる情報へのアクセスが行われた際に、それぞれの情報システムが監査ログを生成すること。

補足説明

本規約では、監査ログの生成を調停、または代行するような機能の存在は想定しておらず、複合システムを構成する個々の情報システムが、それぞれ独自に監査ログを生成することを前提とする。それぞれの情報システムにおいて、どの機能要素(装置、ソフトウェアのプロセス等)が監査ログを出力するかは、その形態によって変わってくる。ここでは、参考として代表的なシステム形態における監査ログの出力場所の例を示す。

スタンドアロン型の場合(図1. 3-2)

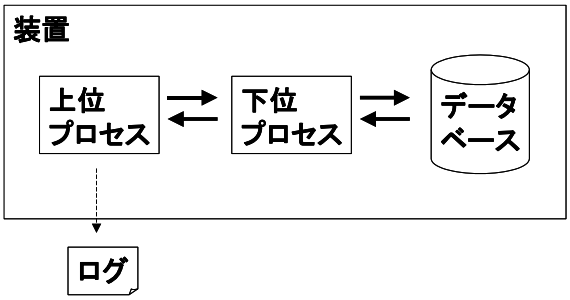

図1.3-2 スタンドアロン型

・上位プロセスが下位プロセスに指示して保護対象情報アクセスするケースでは、上位プロセス側で監査ログを生成する。
・ただし、これは下位プロセスからの監査ログ出力を妨げるものではない。

クライアント・サーバ型の場合(図1.3-3)

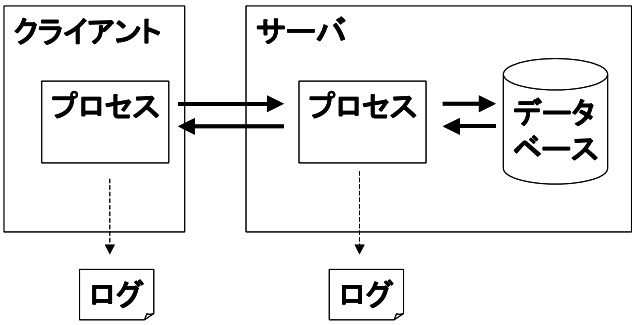

図1.3-3 クライアント・サーバ型

・原則的にはクライアントとサーバ両方が監査ログを出力する。
・クライアントが出力できない場合はサーバだけが監査ログを出力する。
・サーバが出力する監査ログが有用でない場合(監査ログから利用者等が特定できない場合など)は、クライアントだけが出力する。

ホスト・端末型(Web 型)の場合(図1.3-4)

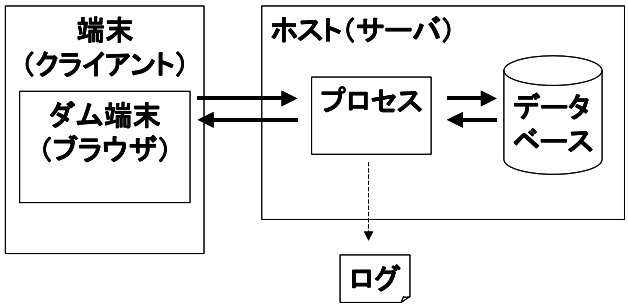

図1.3-4 ホスト・端末(Web)型

・ホスト(サーバ)でのみ監査ログを出力する。

(5) 監査ログを生成した情報システム(以下、ログクライアントと呼ぶ)が、その内容を機能的に独立した情報保存用装置(以下、ログサーバと呼ぶ)に、何らかの方法を用いて伝達すること。

補足説明

ログクライアントからログサーバに監査ログを渡す方法は、どのようなものであってもよい。オンライン処理(通信)によるメッセージ伝達でもよいし、オフラインで人の手を介したファイル渡しでもよい。オンラインであれば、ログクライアントからログサーバに送りつけてもよいし、逆にログサーバがログクライアントから回収してもよい。

(6)　すべてのログクライアントとログサーバ間で、時刻同期が行われていること

補足説明

本規約では、複数のログクライアントで生成された監査ログをログサーバに集め、蓄積することを想定している。この蓄積された監査ログを調べて、何らかの事実を導き出すためには、任意の監査ログの時間的な前後関係が正確に保全されている必要がある。情報システムを構成する機器間での時刻同期については、「医療情報システムの安全管理に関するガイドライン」でも言及されており、本規約ではこのガイドラインに沿った精度での時刻同期が行われていることを前提条件とする。

1.3.2. 適用範囲外

ここでは本規約において適用範囲外とする項目を規定する。これらを規約の対象とすることについて、一定の意義を見出すこともできるが、現時点で実装を考えた場合、あまり制約が多いと普及を阻害する要因となることが懸念される。いずれ普及した時点で順次規格化を目指すものとする。

(1)　ログクライアントとログサーバ間での情報伝達の方法
(2)　ログサーバでのデータ保存方法、およびその形式
(3)　監査手法
(4)　オペレーティングシステムやミドルウェア(DBMS 等)が生成するログ
(5)　装置間での時刻同期の方法

2. 引用規格・引用文献

(1)　医療情報システムの安全管理に関するガイドライン　第 6.0 版

厚生労働省から令和 5 年 5 月に出されたガイドライン。医療情報システムの導入及びそれに伴う情報の外部保存を行う場合の取扱いについてのもの。

(2)　DICOM Part 15:Security and System Management Profiles

米国放射線学会(ACR)と北米電機工業会(NEMA)が開発した医用画像と通信の標準規格である DICOM (Digital Imaging and Communications in Medicine)は、病院内外で異なった製造業者の異なった種類、所謂「マルチベンダ」と「マルチモダリティ」のデジタル画像機器をネットワークまたは保存媒体をもって相互に接続し、患者の画像検査情報の送受信や、画像データの伝送を可能とすることを目指している。

DICOM Part 15 では、DICOM 規格に準じた装置が、監査証跡の収集およびロギングを行なうアプリケーションに監査メッセージを送るためのメカニズムについて説明している。セキュリティ管理者が各個別のノードから監査情報を抽出するのではなく、各ノードが監査情報を収集ポイントに送ることをモデル化しており、その目的は監査証跡メッセージの収集を標準化するためである。

Part 15 にて定義されている監査証跡に関するコードについては、DICOM Part 16 "Content Mapping Resource"に記載されている。

現時点での最新は、DICOM2025a 版である。

(3)　ISO 27789 Audit Trails for EHR

ISO 27789 は、EHR(Electric Health Record)に対するデータアクセスを、すべてのドメインのすべての情報システムに渡って監査可能にしておくためのフレームワークを提供するものである。監査イベントと監査デー

タの形式は、DICOMとの互換性を考慮し、EHRに特化した拡張を行っている。
ISO 27789 は複数ドメインでの横断的なアクセスを対象としているが、本規約は基本的に院内に閉じた単一ドメインでの利用を前提としているところに違いがある。

3. 用語の定義

(1)(患者の)個人情報
当該情報に含まれる氏名、生年月日、その他の記述等により特定の個人を識別することができるもの(他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。)をいう。医療分野においては、死者に関する情報が、同時に、遺族等の生存する個人に関する情報でもある場合には、当該生存する個人に関する情報となる。
医療機関で利用される情報システムは、一般に患者の個人情報を含むと考えてよい。この考え方からすると、情報システム内のすべての情報に対するアクセスの際に監査ログを収集することでシステムの安全性と信頼性を高めることができる。

(2)説明責任
医療機関が、外部の利害関係者(患者など)に、自身の行動について事前・事後に説明する責任のこと。

(3)管理責任
運用面の管理を施設が行う責任のこと。

(4)結果責任
発生した問題点や損失に対する責任のこと。

(5)監査証跡
監査対象システムの入力から出力に至る過程を追跡できる一連の仕組みと記録のこと。

(6)監査ログ
「いつ」「誰が」「誰の」情報にアクセスしたかを記録した情報のこと。「何の」や「何故」、「どこから」も重要な情報であるが、これらを記録することでシステムの負荷が高まることが予想され、本規約ではこれらを適用範囲外とする。

(7)ログクライアント
監査ログを生成した情報装置・プログラムのこと。利用者の識別と、アクセスする情報単位を認識しており、その単位で監査証跡を生成する実体をさすものとする。

(8)ログサーバ
ログクライアントから監査ログを受け取り、保存する情報装置・プログラムのこと。

(9)セキュリティポリシ
医療機関における情報セキュリティに関する基本方針のこと。

4. 記号および略語

本規約では、次の記号および略語の表記を用いる。

DBMS	Database Management System
DICOM	Digital Imaging and Communications in Medicine
OS	Operating System
PHI	Protected Health Information
RFC	Request for Comments

5. 監査ログの生成

5.1. 概要

監査ログを生じさせるきっかけとなる監査イベント(トリガイベント)は、各々の医療情報システムの規模や用途、関係するスタッフ、セキュリティポリシの内容によって定義される。本規約では、個人情報へのアクセスの履歴の確認と、患者に対して医療機関が説明責任を果たすことができることを監査証跡の主たる目的としているため、一般的な情報セキュリティが扱うシステム全体のセキュリティ監査のための監査証跡の範囲すべてを網羅するものではない。また、対象を業務アプリケーションに限定している。

「医療情報システムの安全管理に関するガイドライン」が要求する「いつ」「誰が」「誰の」情報にアクセスしたかを満たす監査メッセージを生成するために、以下の2つの監査イベントを必須とする。

① 個人情報へのアクセスイベント
② 個人情報への検索イベント

また、より詳細な監査を可能にするためにオプションとして以下の監査イベントを定義する。

③ 業務アプリケーションの起動および停止のイベント
④ 利用者認証のイベント
⑤ 個人情報のアプリケーション外部との入出力のイベント
⑥ 個人情報以外の情報へのアクセスイベント
⑦ 業務アプリケーションにおけるセキュリティに関するイベント
⑧ 業務アプリケーションの保存している監査ログへのアクセスイベント

なお、本書の適用範囲外のイベントを以下に例示する。

(1) OS やミドルウェアレベルでの各種イベント
(2) システムユーティリティを用いてのアクセスイベント
(3) 装置のネットワークへの物理的な接続、切断のイベント
(4) ウイルス対策システムなどの保護システムの作動や停止のイベント
(5) 修正パッチの適用のイベント

5.2.　イベント種類と内容の解説

5.2.1. 個人情報へのアクセスイベント(必須)

個人情報へのアクセスイベントを監査イベントとする。アクセスとは、データの作成、読み取り、更新、削除のことである。当該の保護データに対して「いつ」「誰が」「誰の情報にアクセスしたか」の情報がログの内容となる。(表 5.2-1、図 5.2-1)

表 5.2-1 個人情報へのアクセスイベント

イベント	内容
個人情報へのアクセスイベント	いつ、 誰が、 誰の情報にアクセスしたか

個人情報へのアクセスイベント

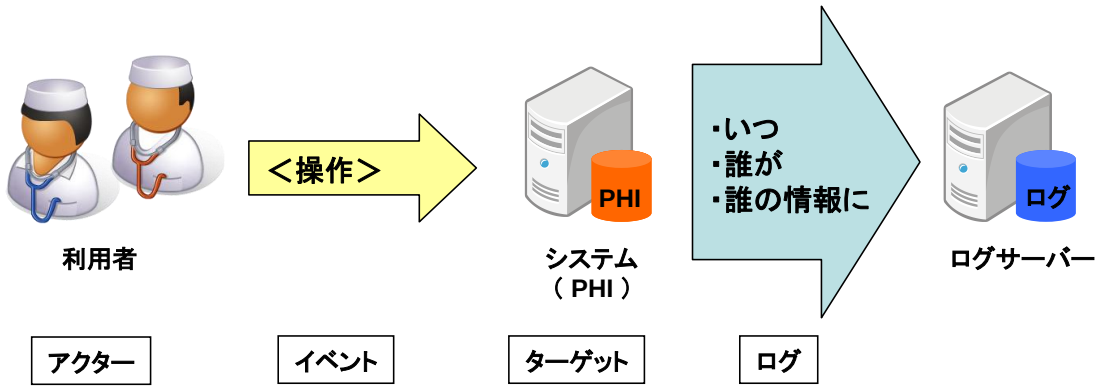

図 5.2-1 個人情報へのアクセスイベント

5.2.2. 個人情報への検索イベント(必須)

個人情報へのアクセスを目的としたDB等への検索イベントを監査イベントとする。検索イベントとは、検索行為そのものであり、検索結果として得られた個人情報の参照については個人情報へのアクセスイベントとする。当該の検索イベントについて「いつ」「誰が」「どのような条件で検索したか」の情報がログ内容となる。(表 5.2-2、図 5.2-2)

表 5.2-2 個人情報への検索イベント

イベント	内容
個人情報への検索イベント	いつ、 誰が、 どのような条件で検索したか

個人情報への検索イベント

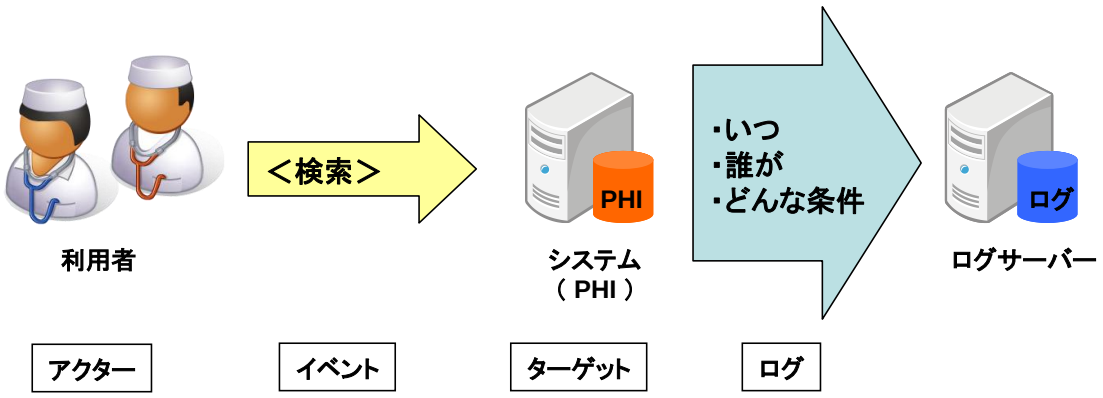

図 5.2-2 個人情報への検索イベント

5.2.3. 業務アプリケーションの起動および停止のイベント(オプション)

業務アプリケーションの起動および停止イベントを監査イベントとする。「いつ」「どの業務アプリケーションが」「開始あるいは停止したか」の情報がログの内容となる。(表 5.2-3、図 5.2-3)

表 5.2-3 業務アプリケーションの起動および停止のイベント

イベント	内容
業務アプリケーションの起動および停止のイベント	いつ、 どの業務アプリケーションが、 開始あるいは停止したか

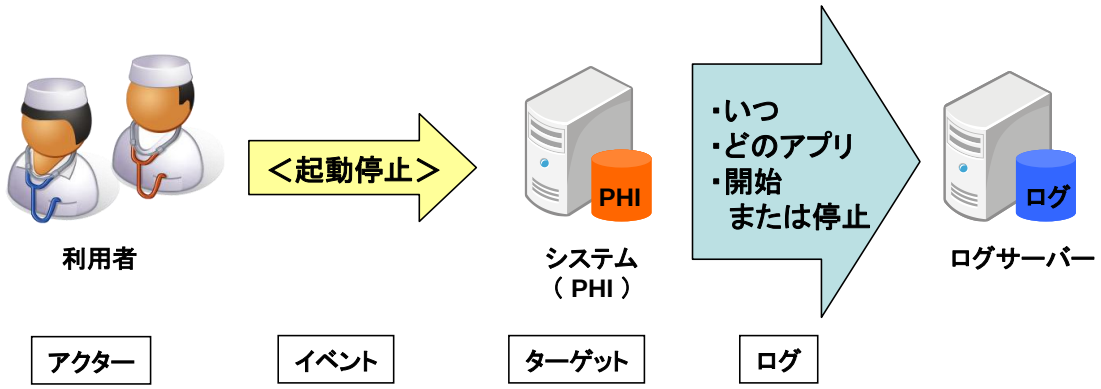

図 5.2-3 業務アプリケーションの起動および停止のイベント

5.2.4. 利用者認証のイベント(オプション)

利用者認証のイベントを監査イベントとする。「いつ」「誰が認証されたか」の情報がログの内容となる。(表5.2-4、図5.2-4)

表5.2-4 利用者認証のイベント

イベント	内容
利用者認証のイベント	いつ、 誰が認証されたか

利用者認証のイベント

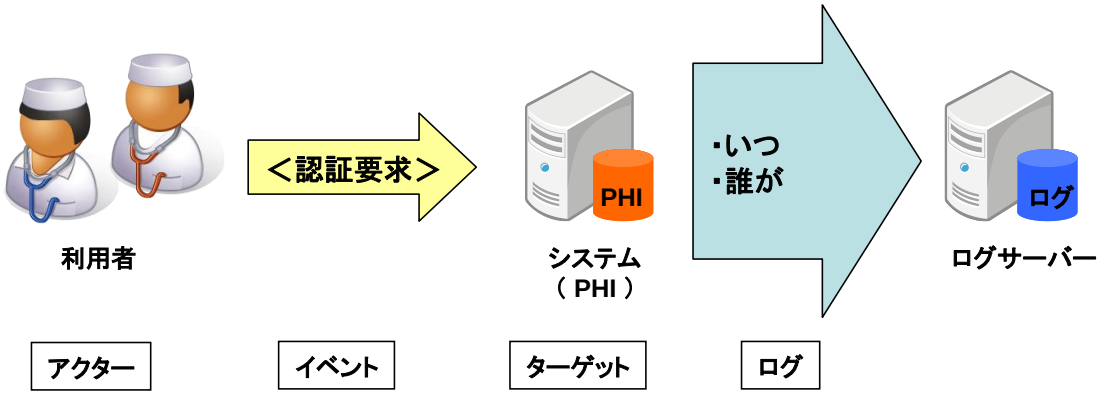

図5.2-4 利用者認証のイベント

5.2.5. 個人情報の外部への出力のイベント(オプション)

個人情報を外部へ出力するイベントを監査イベントとする。外部への出力とは、正当な利用者がアプリケーションの機能を使って当該アプリケーション以外の利用目的のために個人情報を出力すること。例えば、紙への印刷、ファイルへの出力、他システムへのデータ通信などである。

「いつ」「誰が」「どの媒体に」「誰の情報を取り出ししたか」の情報がログの内容となる。(表 5.2-5、図 5.2-5)

表 5.2-5 個人情報の外部への出力のイベント

イベント	内容
個人情報の外部への出力のイベント	いつ、 誰が、 どの媒体に 誰の情報を取り出ししたか

個人情報の外部への出力のイベント

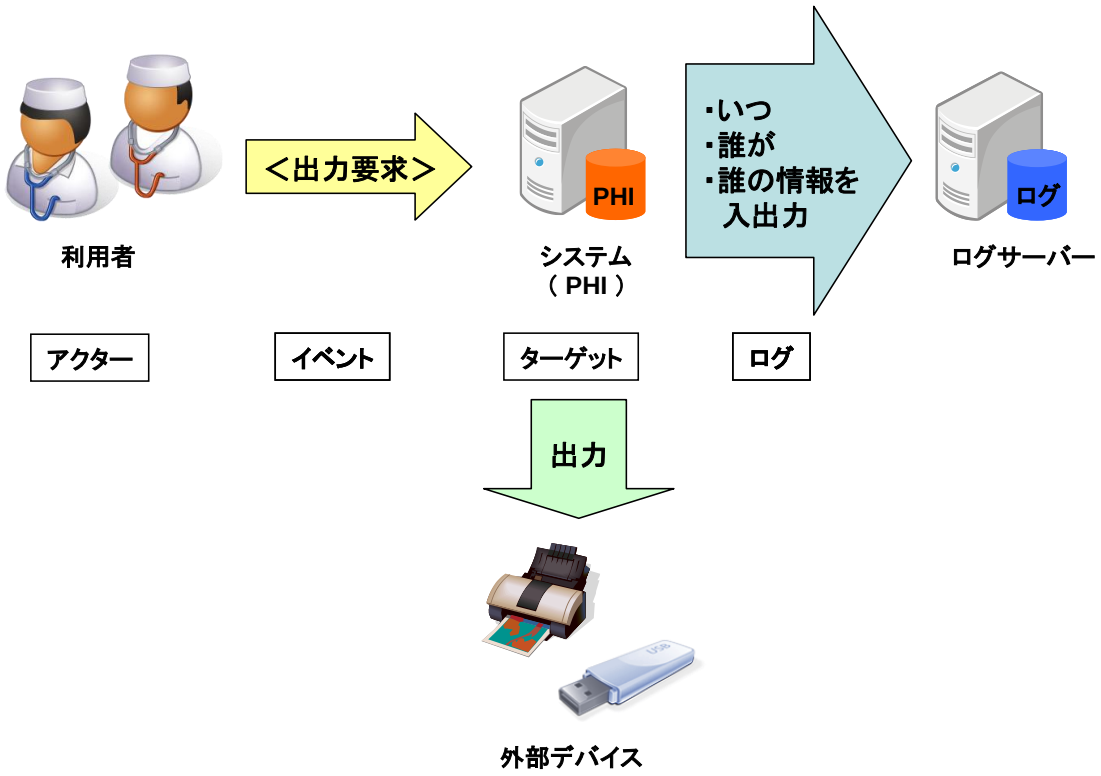

図 5.2-5 個人情報の外部への出力のイベント

5.2.6. 個人情報の外部からの入力のイベント(オプション)

個人情報を外部から入力するイベントを監査イベントとする。外部からの入力とは、正当な利用者がアプリケーションの機能を使って個人情報を入力することである。

「いつ」「誰が」「どの媒体から」「誰の情報を取り込んだか」の情報がログの内容となる。(表 5.2-6、図 5.2-6)

表 5.2-6 個人情報の外部からの入力のイベント

イベント	内容
個人情報の外部からの入力のイベント	いつ、 誰が、 どの媒体から 誰の情報を取り込んだか

個人情報の外部からの入力のイベント

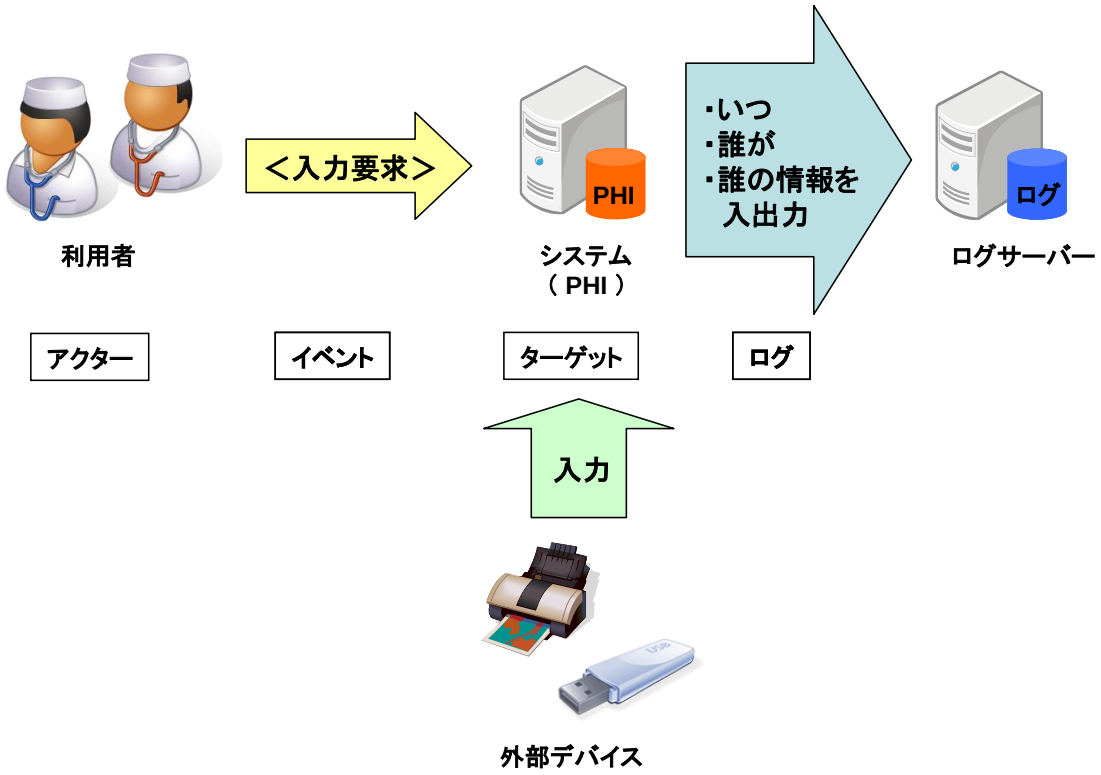

図 5.2-6 個人情報の外部からの入力のイベント

5.2.7. 個人情報以外の情報へのアクセスイベント(オプション)

本規約では、個人情報以外の情報へのアクセスイベントを監査イベントとする。個人情報以外の情報資産に対するアクセスを対象とする。例えば、

・権限管理テーブルへのアクセス
・検査コードマスタへのアクセス
・経営分析データへのアクセス
・匿名化データへのアクセス

などである。当該のデータに対して「いつ」「誰が」「何の情報にアクセスしたか」の情報がログの内容となる。(表5.2-7、図5.2-7)

表5.2-7 個人情報以外の情報へのアクセスイベント

イベント	内容
個人情報以外の情報への アクセスイベント	いつ、 誰が、 何の情報にアクセスしたか

個人情報以外の情報へのアクセスイベント

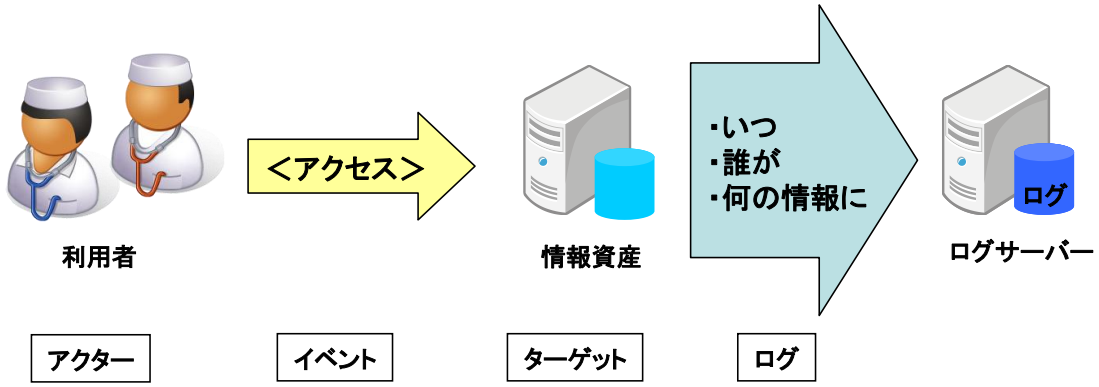

図5.2-7 個人情報以外の情報へのアクセスイベント

5.2.8. 業務アプリケーションにおけるセキュリティ警告イベント(オプション)

業務アプリケーションにおけるセキュリティ警告イベントを監査イベントとする。セキュリティ警告イベントとは、例えば、

・ファイルの入出力エラー
・異常終了
・リソース不足

などである。

「いつ」「どの業務アプリケーションが」「どのようなセキュリティ警告を発したか」の情報がログの内容となる。(表 5.2-8、図 5.2-8)

表 5.2-8 セキュリティ警告イベント

イベント	内容
業務アプリケーションにおけるセキュリティ警告イベント	いつ、 どの業務アプリケーションが、 どのようなセキュリティ警告を発したか

セキュリティ警告イベント

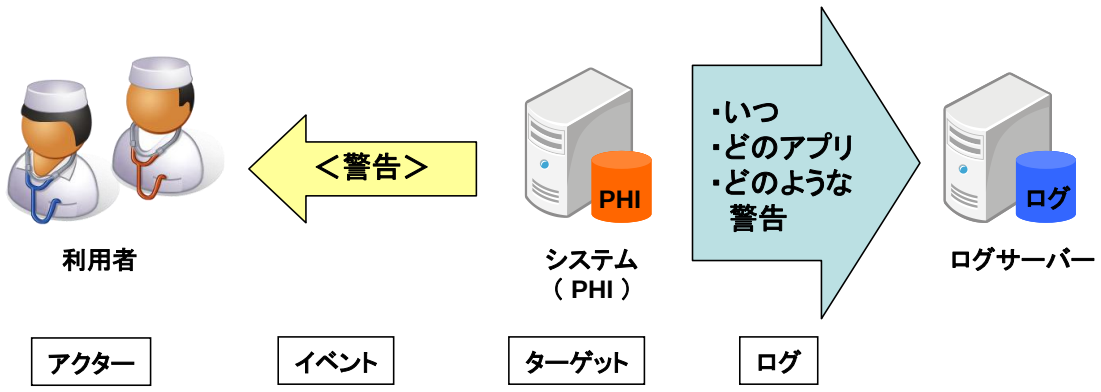

図 5.2-8 セキュリティ警告イベント

5.2.9. 業務アプリケーションの保存している監査ログへのアクセスイベント(オプション)

業務アプリケーションの保存している監査ログへのアクセスイベントを監査イベントとする。当該アプリケーションの機能以外でのアクセスは対象としない。「いつ」「誰が」「どの監査ログにアクセスしたか」の情報がログの内容となる。(表 5.2-9、図 5.2-9)

表 5.2-9 監査ログへのアクセスイベント

イベント	内容
業務アプリケーションの保存している監査ログへのアクセスイベント	いつ、 誰が、 どの監査ログにアクセスしたか

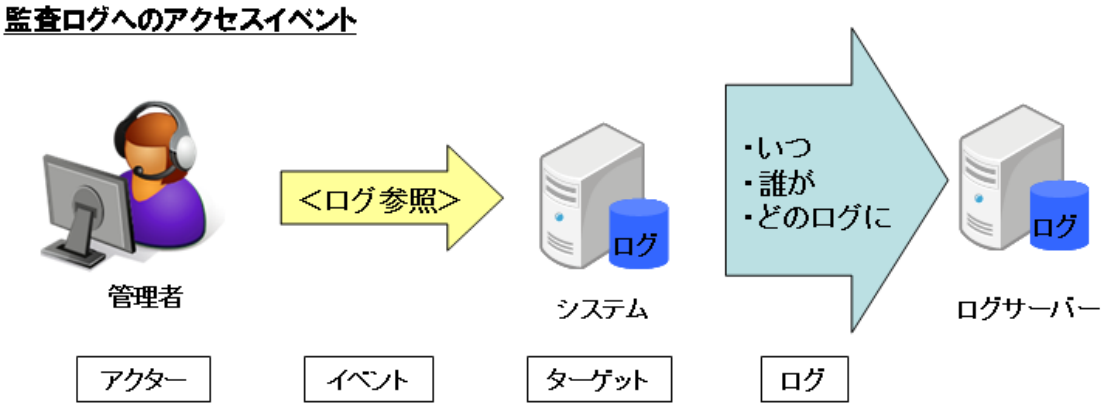

図 5.2-9 監査ログへのアクセスイベント

6. メッセージ内容

6.1. メッセージの一般的な書式

本節では、監査ログのメッセージの一般的な書式について説明する。イベントごとのメッセージ内容については「7.イベント別メッセージ」を参照のこと。メッセージ形式は、DICOM に準拠しており Part15 のスキーマを使用できる。

表 6.1-1 の見方について以下に説明する。(以降、表に分類、オプションの列がある場合は同様の見方とする)

・分類の存在数の表記について。なお、「イベント関連」は常に 1 個のみ存在する

(1) :1 個のみ存在する
(0..1) :0 個または 1 個存在する
(1..2) :1 個または 2 個存在する
(0..N) :0 個から N 個存在する

・オプションの表記について

M:必須(Mandatory)
MC:条件つき必須(Conditional Mandatory)
U:オプション(User Option)

表 6.1-1 メッセージの一般的な書式

分類	フィールド名	オプション	説明	追加情報
イベント関連	EventID	M	監査イベントの ID	6.1.1 を参照のこと
	EventActionCode	M	イベントで実行されたアクション	以下の値が入る。 C 生成 R 読む/見る/印刷/検索 U 更新 D 削除 E 実行 DICOM ではオプション U だが JAHIS では M とする。
	EventDateTime	M	イベントの発生した時刻	6.1.1 を参照のこと
	EventOutcomeIndicator	M	イベントの成功、失敗を示す	
	EventTypeCode	U	イベントのタイプ	DICOM PS3.16 CID401 参照。
ユーザ関連	UserID	M	人またはプロセスの ID	6.1.2 を参照のこと
	AlternativeUserID	U	人またはプロセスの別の ID	
	UserName	U	人またはプロセスの名前	
	UserIsRequestor	M	要求者か否かが入る	
	RoleIDCode	U	人またはプロセスの役割	DICOM PS3.16 CID402 参照
	PurposeOfUse	U	データにアクセスした目的	ISO27789 の規定に従う DICOM では未定義(追加予定)
	NetworkAccessPointTypeCode	U	ネットワークアクセスポイントのタイプ	6.1.3 を参照のこと
	NetworkAccessPointID	U	ネットワークアクセスポイントに対する ID	
発生源	AuditEnterpriseSiteID	U	発生源システムの場所	6.1.4 を参照のこと

システム関連	AuditSourceID	M	発生源システムのユニークな ID	
	AuditSourceTypeCode	U	発生源システムのタイプ	
関係者オブジェクト関連	ParticipantObjectTypeCode	M	関係者オブジェクトのタイプコード	6.1.5 を参照のこと ParticipantObjectTypeCode および ParticipantObjectTypeCodeRole のオプションは DICOM では U だが、JAHIS では M とする。
	ParticipantObjectTypeCodeRole	M	関係者オブジェクトの役割を示すコード	
	ParticipantObjectDataLifeCycle	U	関係者オブジェクトのデータライフサイクルステージの ID	
	ParticipantObjectIDTypeCode	M	ParticipantObjectID に含まれるタイプ	
	ParticipantObjectPolicySet	U	ParticipantObjectID に対するポリシー	ISO27789 の規定に従う。 DICOM では未定義(追加予定)
	ParticipantObjectSensitivity	U	ParticipantObjectID に対するポリシーで定義された機微性	6.1.5 を参照のこと
	ParticipantObjectID	M	関係者オブジェクトの ID	
	ParticipantObjectName	MC	関係者オブジェクトの名前	
	ParticipantObjectQuery	MC	検索内容	
	ParticipantObjectDetail	U	関係者オブジェクトの詳細情報	
	ParticipantObjectDescription	U	関係者オブジェクトの説明	

6.1.1 EventID, EventDateTime, EventOutcomeIndicator

EventID には、その監査イベントの内容に適合する ID が入る。この項目は必須である。使用が許されているのは、DICOM Part16 ”Content Mapping Resource” にて規定された監査イベントと JAHIS によって独自に定義された監査イベントのみである。使用が許されている値は7. 10の「CID(ccc1) 監査イベント ID」に示されているので参照のこと。

EventDateTime には、その監査イベントの発生した時刻が入る。この項目は必須である。ISO8601 に規定された世界標準時(UTC: Coordinated Universal Time)の形式を使用すること。

EventOutcomeIndicator には、その監査イベントが成功したか/失敗したかが入る。この項目は必須である。表 6.1-2 の値を使用すること。

表 6.1-2 EventOutcomeIndicator の値

値	意味
0	成功
4	小さい失敗　アクションを再実行(例:最初の誤入力によるパスワード無効)
8	重大な失敗　アクションを中断(例:過度の誤入力によるパスワード無効)
12	主要な失敗　アクションによる実行不可(例:過度の無効ログオンの試みによるアカウント無効)

6.1.2 UserID, AlternativeUserID, UserName, UserIsRequestor

UserIDには、その監査イベントを発生させた人、プロセス、ノード、出力先、入力元のIDが入る。この項目は必須である。これは発生源(AuditSourceID)においてユニークである必要がある。出力先の場合は、出力先の URL、送信先のメールアドレス、出力先のメディアコードなどが入る。入力元の場合は、入力元の URL、入力元のメールアドレス、入力元のメディアコードなどが入る。

AlternativeUserID には、その監査イベントを発生させた人、プロセス、ノード、出力先、入力元の別の ID が

入る。この項目はオプションである。

UserName には、その監査イベントを発生させた人、プロセス、ノード、出力先、入力元の名前が入る。この項目はオプションである。

UserIsRequestor には、その監査イベントの要求者かどうかの論理値が入る。この項目は必須である。省略時は「真」となる。

6.1.3 NetworkAccessPointTypeCode, NetworkAccessPointID

NetworkAccessPointTypeCode には、その監査イベントの発生したネットワークアクセスポイントの種類が入る。この項目はオプションである。表 6.1-3 の値が入る。

表 6.1-3 NetworkAccessPointTypeCode の値

値	意味
1	マシン名(DNS 名を含む)
2	IP アドレス
3	電話番号
4	Email アドレス
5	URI

NetworkAccessPointID には、その監査イベントの発生したネットワークアクセスポイントの ID が入る。この項目はオプションである。

6.1.4 AuditEnterpriseSiteID, AuditSourceID, AuditSourceTypeCode

AuditEnterpriseSiteID には、その監査イベントの発生した組織内ネットワークの論理的な発生源の ID が入る。この項目はオプションである。

AuditSourceID には、その監査イベントの発生した発生源の ID が入る。この項目は必須である。少なくとも監査される組織内でユニークである必要がある。

AuditSourceTypeCode には、その監査イベントの発生した発生源のタイプが入る。この項目はオプションである。表 6.1-4 の値が入る。

表 6.1-4 AuditSourceTypeCode の値

値	意味
1	End-user interface(エンドユーザ・インターフェース)
2	Data acquisition device or instrument(データ収集装置または機器)
3	Web server process tier in a multi-tier system(多層システムにおける WEB サーバプロセス層)
4	Application server process tier in a multi-tier system(多層システムにおけるアプリケーションサーバプロセス層)
5	Database server process tier in a multi-tier system(多層システムにおけるデータベースサーバプロセス層)*
6	Security server, e.g., a domain controller(ドメインコントローラ等のセキュリティサーバ)
7	ISO level 1-3 network component(ISO レベル 1-3 のネットワークコンポーネント)
8	ISO level 4-6 operating software(ISO レベル 4-6 のオペレーティングソフトウェア)
9	External source, other or unknown type(外部ソース、別のまたは不明のタイプ)

*DICOM では誤植で 4 と同じ“Application server ～”と記載されていたものを JAHIS では修正した。

6.1.5 ParticipantObjectTypeCode, ParticipantObjectTypeCodeRole, ParticipantObjectDataLifeCycle, ParticipantObjectIDTypeCode, ParticipantObjectPolicySet, ParticipantObjectSensitivity, ParticipantObjectID, ParticipantObjectName, ParticipantObjectQuery, ParticipantObjectDetail, ParticipantObjectDescription

ParticipantObjectTypeCode には、関係者オブジェクトのタイプのコードが入る。この項目は必須である。表 6.1.-5 の値が入る。

表 6.1-5 ParticipantObjectTypeCode の値

値	意味
1	人
2	システムオブジェクト
3	組織
4	その他

ParticipantObjectTypeCodeRole には、関係者オブジェクトのタイプコードの役割が入る。この項目は必須である。表 6.1-6 の値が入る。

表 6.1-6 ParticipantObjectTypeCodeRole の値

値	意味	ParticipantObjectTypeCode
1	Patient(患者)	1－人
2	Location(場所)	3－組織
3	Report(報告書)	2－システムオブジェクト
4	Resource(リソース)	1－人、3－組織
5	Master File(マスタファイル)	2－システムオブジェクト
6	User(ユーザ)	1－人、2－システムオブジェクト(人間のユーザでない)
7	List(リスト)	2－システムオブジェクト
8	Doctor(医師)	1－人
9	Subscriber(加入者)	3－組織
10	Guarantor(保証人)	1－人、3－組織
11	Security User Entity(セキュリティユーザエンティティ)	2－システムオブジェクト
12	Security User Group(セキュリティユーザグループ)	2－システムオブジェクト
13	Security Resource(セキュリティリソース)	2－システムオブジェクト
14	Security Granularity Definition(セキュリティレベルの定義)	2－システムオブジェクト
15	Provider(提供者)	1－人、3－組織
16	Data Destination(データ送信先)	2－システムオブジェクト
17	Data Repository(データ保存先)	2－システムオブジェクト
18	Schedule(スケジュール)	2－システムオブジェクト
19	Customer(顧客)	3－組織
20	Job(ジョブ)	2－システムオブジェクト
21	Job Stream(ジョブストリーム)	2－システムオブジェクト

22	Table(表)	2－システムオブジェクト
23	Routing Criteria(ルーティング基準)	2－システムオブジェクト
24	Query(問い合わせ)	2－システムオブジェクト
25	Data Source(データソース)	2－システムオブジェクト
26	Processing Element(処理要素)	2－システムオブジェクト

ParticipantObjectDataLifeCycle には、関係者オブジェクトのライフサイクルが入る。この項目はオプションである。表 6.1-7 の値が入る。

表 6.1-7ParticipantObjectDataLifeCycle の値

値	意味
1	Origination or Creation(発生または作成)
2	Import or Copy from original(原本からの入力またはコピー)
3	Amendment(修正)
4	Verification(検証)
5	Translation(翻訳)
6	Access or Use(アクセスまたは使用)
7	De-identification(匿名化、非識別化)
8	Aggregation, summarization, derivation(統合、要約、派生)
9	Report(報告書)
10	Export or Copy to target(対象先への出力またはコピー)
11	Disclosure(開示)
12	Receipt of Disclosure(開示の受け取り)
13	Archiving(保管)
14	Logical Deletion(論理的削除)
15	Permanent erasure or physical destruction(永久抹消または物理的破壊)

ParticipantObjectIDTypeCode には、関係者オブジェクトの ID のタイプコードが入る。この項目は必須である。表 6.1-8 の値が入る。

表 6.1-8 ParticipantObjectIDTypeCode の値

値	意味	ParticipantObjectTypeCode
1	Medical Record Number(カルテ番号)	1－人
2	Patient Number(患者番号)	1－人
3	Encounter Number(受付番号)	1－人
4	Enrollee Number(登録番号)	1－人
5	Social Security Number(社会保障番号)	1－人
6	Account Number(会計番号)	1－人、3－組織
7	Guarantor Number(保証人番号)	1－人、3－組織
8	Report Name(報告書名)	2－システムオブジェクト
9	Report Number(報告書番号)	2－システムオブジェクト
10	Search Criteria(検索基準)	2－システムオブジェクト
11	User Identifier(ユーザ ID)	1－人、2－システムオブジェクト
12	URI	2－システムオブジェクト

ParticipantObjectSensitivity には、関係者オブジェクトの機微性が入る。この項目はオプションである。

ParticipantObjectID には、関係者オブジェクトのユニークな ID が入る。関係者オブジェクトとはアクセスされた患者の情報、問い合わせ内容、入出力情報等が入る。この項目は必須である。具体的には関係者オブジェクトが患者情報の場合、該当患者の患者 ID が入る。患者情報ではない場合は、検索の種類を示す ID（システムで定義されるもの）、URI、ファイル名、データベーステーブル名等が入る。

ParticipantObjectName には、関係者オブジェクトの名前が入る。この項目は ParticipantObjectQuery がないと必須である。具体的には関係者オブジェクトが患者情報の場合、該当患者の患者氏名が入る。

ParticipantObjectQuery には、検索内容を base64 で符号化した文字列が入る。イベントが個人情報への検索の場合、あるいは、ParticipantObjectName がなければ必須である。

ParticipantObjectDetail には、関係者オブジェクトの詳細情報が入る。この項目はオプションである。

ParticipantObjectDescription には、関係者オブジェクトの説明が入る。この項目はオプションである。

7. イベント別メッセージ

本章ではイベント別の監査ログのメッセージの内容について記述する。記述するイベントは、

(1)　個人情報へのアクセスイベント
(2)　個人情報への検索イベント
(3)　業務アプリケーションの起動および停止のイベント
(4)　利用者認証のイベント
(5)　個人情報の外部への出力のイベント
(6)　個人情報の外部からの入力のイベント
(7)　個人情報以外の情報へのアクセスイベント
(8)　業務アプリケーションにおけるセキュリティに関するイベント
(9)　業務アプリケーションの保存している監査ログへのアクセスイベント

である。

また、メッセージ内で記述されるイベントIDおよびコードについて表 7.10-1 でまとめて記述する。

7.1. 個人情報へのアクセスイベントメッセージ

このメッセージでは、個人情報の作成、読み取り、変更、または削除に関するイベントの内容を記述する。表 7.1-1 に内容を示す。

表 7.1-1 個人情報へのアクセスイベントメッセージ

分類	フィールド名	オプション	値の制限
イベント関連	EventID	M	監査イベントの ID。以下の値が入る。 EV (110110, DCM, "Patient Record")
	EventActionCode	M	監査ログを生成したイベントで実行されたアクション。以下の値が入る。 EV:"C" (作成) "R" (読み取り) "U" (更新) "D" (削除)
	EventDateTime	M	イベントが発生した時刻。
	EventOutcomeIndicator	M	イベントの成功、失敗を示す。
	EventTypeCode	U	イベントのタイプ。 DT (110145, DCM, "Session start") DT (110146, DCM, "Session stop")
ユーザ関連(1..2)	UserID	M	データを操作した人またはプロセスの ID。両方ともわかっている場合は、人とプロセスの両方を含める。これは発生源(AuditSourceID)においてユニークな値である。
	AlternativeUserID	U	データを操作した人またはプロセスの別の ID。
	UserName	U	データを操作した人またはプロセスの名前。
	UserIsRequestor	M	データを操作した人またはプロセスが本イベントの要求者か否かを示す。以下の値が入る。 EV TRUE DICOM 規格ではオプション U だが JAHIS では M とする。
	RoleIDCode	U	イベントを実行するときのデータを操作した人またはプロセスの役割。
	PurposeOfUse	U	ISO27789 の規定に従う
	NetworkAccessPointTypeCode	U	ネットワークアクセスポイントのタイプ。

	NetworkAccessPointID	U	ネットワークアクセスポイントに対する ID。
発生源システム関連(1) *	AuditEnterpriseSiteID	U	ネットワーク中の論理的な発生源システムの場所。AuditSourceID を修飾するために使う。
	AuditSourceID	M	発生源システムのユニークな ID。
	AuditSourceTypeCode	U	発生源システムのタイプ。
関係者オブジェクト関連(アクセスされた患者情報)(1)	ParticipantObjectTypeCode	M	関係者オブジェクトのタイプコード。以下の値が入る。 EV 1 (人)
	ParticipantObjectTypeCodeRole	M	関係者オブジェクトの役割を示すコード。以下の値が入る。 EV 1 (患者)
	ParticipantObjectDataLifeCycle	U	関係者オブジェクトのデータライフサイクルステージの ID。
	ParticipantObjectIDTypeCode	M	ParticipantObjectID に含まれるタイプ。以下の値が入る。 EV 2 (患者 ID)
	ParticipantObjectPolicySet	U	ISO27789 の規定に従う
	ParticipantObjectSensitivity	U	ParticipantObjectID に対するポリシー定義の機微性。
	ParticipantObjectID	M	関係者オブジェクトのインスタンス ID。患者 ID が入る。
	ParticipantObjectName	M	関係者オブジェクトのインスタンスの名前。患者名が入る。
	ParticipantObjectDetail	U	関係者オブジェクトのインスタンスの詳細情報。
	ParticipantObjectDescription	U	関係者オブジェクトのインスタンスの説明

＊DICOM では、General Message Format にのみ記載されているが、JAHIS では個々のメッセージにも記載した。

7.2. 個人情報への検索イベントメッセージ

このメッセージでは、個人情報へのアクセスを目的としたDB等への検索の発行および受信に関するイベントを記述する。メッセージには、検索に対する応答は記録されず、検索が発行された事実のみを記録する。表 7.2-1 に内容を示す。

表 7.2-1 個人情報への検索イベントメッセージ

分類	フィールド名	オプション	値の制限
イベント関連	EventID	M	監査イベントのID。以下の値が入る。 EV (110112, DCM, "Query")
	EventActionCode	M	監査ログを生成したイベントで実行されたアクション。以下の値が入る。 EV "E" (実行)
	EventDateTime	M	イベントが発生した時刻。
	EventOutcomeIndicator	M	イベントの成功/失敗を示す。
	EventTypeCode	U	イベントのタイプ。
問合せ元関連(1)	UserID	M	検索を発行したプロセスのID。これは発生源(AuditSourceID)において ユニークな値である。
	AlternativeUserID	U	検索を発行したプロセスの別のID。
	UserName	U	検索を発行したプロセスの名前。
	UserIsRequestor	M	検索を発行したプロセスが本イベントの要求者か否かを示す。
	RoleIDCode	M	イベントを実行するときの検索を発行したプロセスの役割。以下の値が入る。 EV (110153, DCM, "Source Role ID")
	NetworkAccessPointTypeCode	U	ネットワークアクセスポイントのタイプ。
	NetworkAccessPointID	U	ネットワークアクセスポイントに対するID。
問合せ先関連(1)	UserID	M	検索に応答するプロセスのID。これは発生源(AuditSourceID)において ユニークな値である。
	AlternativeUserID	U	検索に応答するプロセスの別のID。
	UserName	U	検索に応答するプロセスの名前。
	UserIsRequestor	M	検索に応答するプロセスが本イベントの要求者か否かを示す。
	RoleIDCode	M	イベントを実行するときの検索に応答したプロセスの役割。以下の値が入る EV (110152, DCM, "Destination Role ID")
	NetworkAccessPointTypeCode	U	ネットワークアクセスポイントのタイプ。
	NetworkAccessPointID	U	ネットワークアクセスポイントに対するID。
他の関係者関連(0..N)	UserID	M	関係しており認識されている他の関係者のID。特に要求者である人あるいはプロセスのID。これは発生源(AuditSourceID)において ユニークな値である。
	AlternativeUserID	U	他の関係者の別のID。
	UserName	U	他の関係者の名前。
	UserIsRequestor	M	他の関係者が本イベントの要求者か否かを示す。
	RoleIDCode	U	他の関係者の役割。
	NetworkAccessPointTypeCode	U	ネットワークアクセスポイントのタイプ。
	NetworkAccessPointID	U	ネットワークアクセスポイントに対するID。
発生源関連(1)	AuditEnterpriseSiteID	U	ネットワーク中の論理的な発生源の場所。AuditSourceIDを修飾するために使う。
	AuditSourceID	M	発生源のユニークなID。
	AuditSourceTypeCode	U	発生源のタイプ。
関係者オブジェクト関連(問い合わせ内容)(1)	ParticipantObjectTypeCode	M	関係者オブジェクトのタイプコード。以下の値が入る。 EV 2 (システム)

	ParticipantObjectTypeCodeRole	M	関係者オブジェクトの役割を示すコード。以下の値が入る。 EV(3,報告書)
	ParticipantObjectDataLifeCycle	U	関係者オブジェクトのデータライフサイクルステージのID。
	ParticipantObjectIDTypeCode	M	ParticipantObjectIDに含まれるタイプ。 EV(10,検索基準)
	ParticipantObjectSensitivity	U	ParticipantObjectIDに対するポリシー定義の機微性
	ParticipantObjectID	M	関係者オブジェクトのインスタンスのID。
	ParticipantObjectQuery	M	base64で符号化された検索内容。本内容は各装置開発ベンダにて内容が分析できなければならない。
	ParticipantObjectDetail	U	関係者オブジェクトのインスタンスの詳細情報 DICOM規格ではオプションMCだがJAHISではUとする。
	ParticipantObjectDescription	U	関係者オブジェクトのインスタンスの説明

7.3. 業務アプリケーションの起動および停止のイベントメッセージ

このメッセージでは、業務アプリケーションの起動および停止のイベントを記述する。表 7.3-1 に内容を示す。

表 7.3-1 業務アプリケーションの起動および停止のイベントメッセージ

分類	フィールド名	オプション	値の制限
イベント関連	EventID	M	監査イベントの ID。以下の値が入る。 EV (110100, DCM, "Application Activity")
	EventActionCode	M	監査ログを生成したイベントで実行されたアクション。以下の値が入る。 EV "E" (実行)
	EventDateTime	M	イベントが発生した時刻。
	EventOutcomeIndicator	M	イベントの成功、失敗を示す。
	EventTypeCode	M	起動あるいは停止。以下の値が入る。 DT (110120, DCM, "Application Start") DT (110121, DCM, "Application Stop")
起動/停止したアプリケーション関連(1)	UserID	M	起動あるいは停止したプロセスの ID。これは発生源(AuditSourceID)においてユニークな値である。
	AlternativeUserID	MC	起動あるいは停止したプロセスの別の ID。DICOM 装置ならば AE タイトルが入る。
	UserName	U	起動あるいは停止したアプリケーションの名前。
	UserIsRequestor	M	EV FALSE
	RoleIDCode	M	以下の値が入る。 EV (110150, DCM, "Application")
	NetworkAccessPointTypeCode	U	ネットワークアクセスポイントのタイプ。
	NetworkAccessPointID	U	ネットワークアクセスポイントに対する ID。
アプリケーションを起動/停止させたユーザまたはプロセス関連(0..N)	UserID	M	起動あるいは停止させた人またはプロセスの ID。これは発生源(AuditSourceID)においてユニークな値である。
	AlternativeUserID	U	起動あるいは停止させた人またはプロセスの別の ID。
	UserName	U	起動あるいは停止させた人またはプロセスの名前。
	UserIsRequestor	M	EV TRUE
	RoleIDCode	M	以下の値が入る EV (110151, DCM, "Application Launcher")
	NetworkAccessPointTypeCode	U	ネットワークアクセスポイントのタイプ。
	NetworkAccessPointID	U	ネットワークアクセスポイントに対する ID。
発生源システム関連(1)	AuditEnterpriseSiteID	U	ネットワーク中の論理的な発生源システムの場所。AuditSourceID を修飾するために使う。
	AuditSourceID	M	発生源システムのユニークな ID。
	AuditSourceTypeCode	U	発生源システムのタイプ。

7.4. 利用者認証のイベントメッセージ

このメッセージでは、利用者認証に関するイベントを記述する。表 7.4-1 に内容を示す。

表 7.4-1 利用者認証のイベントメッセージ

分類	フィールド名	オプション	値の制限
イベント関連	EventID	M	監査イベントの ID。以下の値が入る。 EV (110114, DCM, "User Authentication")
	EventActionCode	M	監査ログを生成したイベントで実行されたアクション。以下の値が入る。 EV "E" (実行)
	EventDateTime	M	イベントが発生した時刻。
	EventOutcomeIndicator	M	イベントの成功、失敗を示す。
	EventTypeCode	M	イベントのタイプ。以下の値が入る。 EV (110122, DCM, "Login") EV (110123, DCM, "Logout")
ユーザ関連(1)	UserID	M	認証されたユーザの ID。あるいは認証されなかったユーザの ID。これは発生源(AuditSourceID)においてユニークな値である。
	AlternativeUserID	U	認証されたユーザの別の ID。あるいは認証されなかったユーザの別の ID。
	UserName	U	認証されたユーザの名前。あるいは認証されなかったユーザの名前。
	UserIsRequestor	M	EV TRUE
	RoleIDCode	U	イベントを実行するときのプロセスの役割。
	NetworkAccessPointTypeCode	M	ネットワークアクセスポイントのタイプ。
	NetworkAccessPointID	M	ネットワークアクセスポイントに対する ID。
ノード関連(0..1)	UserID	M	認証を行ったノードの ID。これは発生源(AuditSourceID)においてユニークな値である。
	AlternativeUserID	U	認証を行ったノードの別の ID。
	UserName	U	認証を行ったノードの名前。
	UserIsRequestor	M	EV FALSE
	RoleIDCode	U	認証を行ったノードの役割。
	NetworkAccessPointTypeCode	U	ネットワークアクセスポイントのタイプ。
	NetworkAccessPointID	U	ネットワークアクセスポイントに対する ID。
発生源システム関連(1)	AuditEnterpriseSiteID	U	ネットワーク中の論理的な発生源システムの場所。AuditSourceID を修飾するために使う。
	AuditSourceID	M	発生源システムのユニークな ID。
	AuditSourceTypeCode	U	発生源システムのタイプ。

7.5.個人情報の外部への出力のイベントメッセージ

このメッセージでは、個人情報の外部への出力のイベントに関するイベントの内容を記述する。表 7.5-1 に内容を示す。

表 7.5-1 個人情報の外部への出力のイベントメッセージ

分類	フィールド名	オプション	値の制限
イベント関連	EventID	M	監査イベントの ID。以下の値が入る。 EV (110106, DCM, “Export”)
	EventActionCode	M	監査ログを生成したイベントで実行されたアクション。以下の値が入る。 EV:“R”（読み取り）
	EventDateTime	M	イベントが発生した時刻。
	EventOutcomeIndicator	M	イベントの成功、失敗を示す。
	EventTypeCode	U	イベントのタイプ。
リモート入力者またはプロセス関連(0..N)	UserID	M	リモートでデータを受け取った人またはプロセスの ID。両方ともわかっている場合は、人とプロセスの両方を含める。これは発生源(AuditSourceID)においてユニークな値である。
	AlternativeUserID	U	リモートでデータを受け取った人またはプロセスの別の ID。
	UserName	U	リモートでデータを受け取った人またはプロセスの名前。
	UserIsRequestor	M	リモートでデータを受け取った人またはプロセスが本イベントの要求者か否かを示す。以下の値が入る。 EV FALSE
	RoleIDCode	M	イベントを実行するときのリモートでデータを受け取った人またはプロセスの役割。以下の値が入る。 EV (110152, DCM, “Destination Role ID”)
	NetworkAccessPointTypeCode	U	ネットワークアクセスポイントのタイプ。
	NetworkAccessPointID	U	ネットワークアクセスポイントに対する ID。
出力者またはプロセス関連(1..2)	UserID	M	データを操作した人またはプロセスの ID。両方ともわかっている場合は、人とプロセスの両方を含める。これは発生源(AuditSourceID)においてユニークな値である。
	AlternativeUserID	U	データを操作した人またはプロセスの別の ID。
	UserName	U	データを操作した人またはプロセスの名前。
	UserIsRequestor	M	データを操作した人またはプロセスが本イベントの要求者か否かを示す。以下の値が入る。 EV TRUE
	RoleIDCode	M	イベントを実行するときのデータを操作した人またはプロセスの役割。 EV (110153, DCM, “Source Role ID”)
	NetworkAccessPointTypeCode	U	ネットワークアクセスポイントのタイプ。
	NetworkAccessPointID	U	ネットワークアクセスポイントに対する ID。
出力先関連(1)	UserID	M	データの出力先の ID。 出力先 URL,送信先メールアドレス、出力先メディアコード等
	AlternativeUserID	U	データの出力先の別の ID。
	UserName	U	データの出力先の名前。
	UserIsRequestor	M	データの出力先が本イベントの要求者か否かを示す。以下の値が入る。 EV FALSE

	RoleIDCode	M	イベントを実行するときのデータを操作した人またはプロセスの役割。 EV (110154, DCM, “Destination Media”)
	NetworkAccessPointTypeCode	MC	ネットワークアクセスポイントのタイプ。
	NetworkAccessPointID	MC	ネットワークアクセスポイントに対する ID。
	MediaIdentifier	MC	メディアのボリューム ID、URI あるいは他の識別子。 デジタルメディアの場合必須。
	MediaType	M	メディアのタイプ。 DICOM PS3.16 CID 405. Media Type Code の値を使用すること。
発生源システム関連(1)	AuditEnterpriseSiteID	U	ネットワーク中の論理的な発生源システムの場所。AuditSourceID を修飾するために使う。
	AuditSourceID	M	発生源システムのユニークな ID。
	AuditSourceTypeCode	U	発生源システムのタイプ。
出力情報 (0..N)	ParticipantObjectTypeCode	M	関係者オブジェクトのタイプコード。以下の値が入る。 EV 1 (人)
	ParticipantObjectTypeCodeRole	M	関係者オブジェクトの役割を示すコード。以下の値が入る。 EV 1 (患者)
	ParticipantObjectDataLifeCycle	U	関係者オブジェクトのデータライフサイクルステージの ID。
	ParticipantObjectIDTypeCode	M	ParticipantObjectID に含まれるタイプ。以下の値が入る。 EV 2 (患者 ID)
	ParticipantObjectSensitivity	U	ParticipantObjectID に対するポリシー定義の機微性。
	ParticipantObjectID	M	関係者オブジェクトのインスタンス ID。患者 ID が入る。
	ParticipantObjectName	M	関係者オブジェクトのインスタンスの名前。患者名が入る。
	ParticipantObjectDetail	U	関係者オブジェクトのインスタンスの詳細情報。
	ParticipantObjectDescription	U	関係者オブジェクトのインスタンスの説明。

7.6.個人情報の外部からの入力のイベントメッセージ

このメッセージでは、個人情報の外部からの入力のイベントに関するイベントの内容を記述する。表 7.6-1 に内容を示す。

表 7.6-1 個人情報の外部からの入力のイベントメッセージ

分類	フィールド名	オプション	値の制限
イベント関連	EventID	M	監査イベントの ID。以下の値が入る。 EV (110107, DCM, “Import”)
	EventActionCode	M	監査ログを生成したイベントで実行されたアクション。以下の値が入る。 EV:“C” (作成) “U” (更新) DICOM 規格では、”C”のみだが、JAHIS では、“U”を追加した。
	EventDateTime	M	イベントが発生した時刻。
	EventOutcomeIndicator	M	イベントの成功、失敗を示す。
	EventTypeCode	U	イベントのタイプ。
入力者またはプロセス関連(1..N)	UserID	M	データを入力した人またはプロセスの ID。両方ともわかっている場合は、人とプロセスの両方を含める。これは発生源(AuditSourceID)においてユニークな値である。
	AlternativeUserID	U	データを入力した人またはプロセスの別の ID。
	UserName	U	データを入力した人またはプロセスの名前。
	UserIsRequestor	M	データを操作した人またはプロセスが本イベントの要求者か否かを示す。以下の値が入る。 EV TRUE
	RoleIDCode	M	イベントを実行するときのデータを操作した人またはプロセスの役割。 EV (110152, DCM, “Destination Role ID”)
	NetworkAccessPointTypeCode	U	ネットワークアクセスポイントのタイプ。
	NetworkAccessPointID	U	ネットワークアクセスポイントに対する ID。
入力元関連(1)	UserID	M	データを入力した人またはプロセスの ID。両方ともわかっている場合は、人とプロセスの両方を含める。これは発生源(AuditSourceID)においてユニークな値である。
	AlternativeUserID	U	データを入力した人またはプロセスの別の ID。
	UserName	U	データを入力した人またはプロセスの名前。
	UserIsRequestor	M	データを操作した人またはプロセスが本イベントの要求者か否かを示す。以下の値が入る。 EV FALSE
	RoleIDCode	M	イベントを実行するときのデータを操作した人またはプロセスの役割。 EV (110155, DCM, “Source Media”)
	NetworkAccessPointTypeCode	U	ネットワークアクセスポイントのタイプ。
	NetworkAccessPointID	MC	ネットワークアクセスポイントに対する ID。ネットワークアクセスポイントのタイプが存在するならば必須。
	MediaIdentifier	M	メディアのボリューム ID、URI あるいは他の識別子。
	MediaType	M	メディアのタイプ。 DICOM PS3.16 CID 405. Media Type Code の値を使用すること。

入力元関連(0..N)	UserID	M	データの入力元の ID。これは発生源(AuditSourceID)においてユニークな値である。 入力元 URL,入力元メールアドレス、入力元メディアコード等
	AlternativeUserID	U	データの入力元の別の ID。
	UserName	U	データの入力元の名前。
	UserIsRequestor	M	以下の値が入る。 EV FALSE
	RoleIDCode	M	イベントを実行するときの役割。 EV (110153, DCM, “Source Role ID”)
	NetworkAccessPointTypeCode	U	ネットワークアクセスポイントのタイプ。
	NetworkAccessPointID	MC	ネットワークアクセスポイントに対する ID。ネットワーク経由の場合は必須
発生源システム関連(1)	AuditEnterpriseSiteID	U	ネットワーク中の論理的な発生源システムの場所。AuditSourceID を修飾するために使う。
	AuditSourceID	M	発生源システムのユニークな ID。
	AuditSourceTypeCode	U	発生源システムのタイプ。
入力情報 (0..N)	ParticipantObjectTypeCode	M	関係者オブジェクトのタイプコード。以下の値が入る。 EV 1 (人)
	ParticipantObjectTypeCodeRole	M	関係者オブジェクトの役割を示すコード。以下の値が入る。 EV 1 (患者)
	ParticipantObjectDataLifeCycle	U	関係者オブジェクトのデータライフサイクルステージの ID。
	ParticipantObjectIDTypeCode	M	ParticipantObjectID に含まれるタイプ。以下の値が入る。 EV 2 (患者 ID)
	ParticipantObjectSensitivity	U	ParticipantObjectID に対するポリシー定義の機微性。
	ParticipantObjectID	M	関係者オブジェクトのインスタンス ID。患者 ID が入る。
	ParticipantObjectName	M	関係者オブジェクトのインスタンスの名前。患者名が入る。
	ParticipantObjectDetail	U	関係者オブジェクトのインスタンスの詳細情報。
	ParticipantObjectDescription	U	関係者オブジェクトのインスタンスの説明。

7.7. 個人情報以外の情報へのアクセスイベントメッセージ

このメッセージでは、個人情報以外の情報へのアクセスに関するイベントの内容を記述する。表 7.7-1 に内容を示す。

表 7.7-1 個人情報以外の情報へのアクセスイベントメッセージ

分類	フィールド名	オプション	値の制限
イベント関連	EventID	M	監査イベントの ID。以下の値が入る。 EV (110100 JAHIS, “Non-PatientRecords”)
	EventActionCode	M	監査ログを生成したイベントで実行されたアクション。以下の値が入る。 EV:“C”（作成） “R”（読み取り） “U”（更新） “D”（削除）
	EventDateTime	M	イベントが発生した時刻。
	EventOutcomeIndicator	M	イベントの成功、失敗を示す。
	EventTypeCode	U	イベントのタイプ。 DT (110145, DCM, “Session start”) DT (110146, DCM, “Session stop”)
ユーザ関連(1..2)	UserID	M	データを操作した人またはプロセスの ID。両方ともわかっている場合は、人とプロセスの両方を含める。これは発生源(AuditSourceID)においてユニークな値である。
	AlternativeUserID	U	データを操作した人またはプロセスの別の ID。
	UserName	U	データを操作した人またはプロセスの名前。
	UserIsRequestor	M	データを操作した人またはプロセスが本イベントの要求者か否かを示す。以下の値が入る。 EV TRUE
	RoleIDCode	U	イベントを実行するときのデータを操作した人またはプロセスの役割。
	PurposeOfUse	U	ISO27789 の規定に従う
	NetworkAccessPointTypeCode	U	ネットワークアクセスポイントのタイプ。
	NetworkAccessPointID	U	ネットワークアクセスポイントに対する ID。
発生源システム関連(1)	AuditEnterpriseSiteID	U	ネットワーク中の論理的な発生源システムの場所。AuditSourceID を修飾するために使う。
	AuditSourceID	M	発生源システムのユニークな ID。
	AuditSourceTypeCode	U	発生源システムのタイプ。
関係者オブジェクト関連(アクセスされた情報)(1)	ParticipantObjectTypeCode	M	関係者オブジェクトのタイプコード。以下の値が入る。 EV 2(システム)
	ParticipantObjectTypeCodeRole	M	関係者オブジェクトの役割を示すコード。以下の値が入る。 EV 5 (マスタ),3(報告書)
	ParticipantObjectDataLifeCycle	U	関係者オブジェクトのデータライフサイクルステージの ID。
	ParticipantObjectIDTypeCode	M	ParticipantObjectID に含まれるタイプ。以下の値が入る。 EV 12(URI)
	ParticipantObjectPolicySet	U	ISO27789 の規定に従う
	ParticipantObjectSensitivity	U	ParticipantObjectID に対するポリシー定義の機微性。
	ParticipantObjectID	M	関係者オブジェクトの URI。マスタ名、テーブル名、ファイル名等

	ParticipantObjectName	M	関係者オブジェクトのインスタンスの名前。 マスタ名、テーブル名、ファイル名等
	ParticipantObjectDetail	U	関係者オブジェクトのインスタンスの詳細情報。
	ParticipantObjectDescription	U	関係者オブジェクトのインスタンスの説明。

7.8. 業務アプリケーションにおけるセキュリティに関するイベントメッセージ

このメッセージでは、業務アプリケーションにおけるセキュリティに関するイベントを記述する。表 7.8-1 に内容を示す。

表 7.8-1 業務アプリケーションにおけるセキュリティに関するイベントメッセージ

分類	フィールド名	オプション	値の制限
イベント関連	EventID	M	監査イベントの ID。以下の値が入る。 EV (110113, DCM, "Security Alert")
	EventActionCode	M	監査ログを生成したイベントで実行されたアクション。以下の値が入る。 EV "E" (実行)
	EventDateTime	M	イベントが発生した時刻。
	EventOutcomeIndicator	M	イベントの成功、失敗を示す。
	EventTypeCode	M	イベントのタイプ。DICOM PS3.16 CID401 参照。
レポートユーザ関連(1..2)	UserID	M	イベントを発行した人またはプロセスの ID。これは発生源(AuditSourceID)においてユニークな値である。
	AlternativeUserID	U	イベントを発行したプロセスの別の ID。
	UserName	U	イベントを発行したプロセスの名前。
	UserIsRequestor	M	セキュリティに関するプロセスが本イベントの要求者か否かを示す。 EV TRUE
	RoleIDCode	U	イベントを発行したプロセスの役割。
	NetworkAccessPointTypeCode	U	ネットワークアクセスポイントのタイプ。
	NetworkAccessPointID	U	ネットワークアクセスポイントに対する ID。
アクティブな関係者情報(0..N)	UserID	M	セキュリティアラートの要因となった人、プロセス、ノードの ID。これは発生源(AuditSourceID)においてユニークな値である。
	AlternativeUserID	U	イベントに応答するプロセスの別の ID。
	UserName	U	イベントに応答するプロセスの名前。
	UserIsRequestor	M	イベントに応答するプロセスが本イベントの要求者か否かを示す。 EV FALSE
	RoleIDCode	U	イベントが発行されたときのプロセスの役割。
	NetworkAccessPointTypeCode	U	ネットワークアクセスポイントのタイプ。
	NetworkAccessPointID	U	ネットワークアクセスポイントに対する ID。
発生源システム関連(1)	AuditEnterpriseSiteID	U	ネットワーク中の論理的な発生源システムの場所。AuditSourceID を修飾するために使う。
	AuditSourceID	M	発生源システムのユニークな ID。
	AuditSourceTypeCode	U	発生源システムのタイプ。
警告サブジェクト関連 (0..N)	ParticipantObjectTypeCode	M	警告サブジェクトのタイプコード。以下の値が入る。 EV 2 (システム)
	ParticipantObjectTypeCodeRole	U	警告サブジェクトの役割を示すコード。以下の値が入る。 EV 5(マスタファイル) EV 13(セキュリティリソース)
	ParticipantObjectDataLifeCycle	U	警告サブジェクトのデータライフサイクルステージの ID。
	ParticipantObjectIDTypeCode	M	ParticipantObjectID に含まれるタイプ。 DT 12(URI) DT (110182, DCM, "Node ID")

	ParticipantObjectSensitivity	U	ParticipantObjectID に対するポリシー定義の機微性。
	ParticipantObjectID	M	警告サブジェクトのインスタンスの ID。 ParticipantObjectIDTypeCode が 12(URI)の場合は、この値はアラートの対象となるファイルまたは他のリソースの URI。 ParticipantObjectIDTypeCode が(110182, DCM, "Node ID")の場合は、この値はアラートの対象となるノード ID (node_name @ domain_name の形式または IP アドレス)。
	ParticipantObjectName	M	警告サブジェクトのインスタンスの名前。 ParticipantObjectIDTypeCode が 12(URI)の場合は、この値はアラートの対象となるファイルまたは他のリソースの名称。 ParticipantObjectIDTypeCode が(110182, DCM, "Node ID")の場合は、この値はアラートの対象となるノード名称(node_name または IP アドレス)。
	ParticipantObjectDetail	M	警告サブジェクトのインスタンスの詳細情報。
	ParticipantObjectDescription	U	警告サブジェクトのインスタンスの説明。

7.9. 業務アプリケーションの保存している監査ログへのアクセスイベントメッセージ

このメッセージでは、業務アプリケーションが保存している監査ログへのアクセスイベントの内容を記述する。表 7.9-1 に内容を示す。

表 7.9-1 業務アプリケーションが保存している監査ログへのアクセスイベントメッセージ

分類	フィールド名	オプション	値の制限
イベント関連	EventID	M	監査イベントの ID。以下の値が入る。 EV (110101, DCM, “Audit Log Used”)
	EventActionCode	M	監査ログを生成したイベントで実行されたアクション。以下の値が入る。 EV:“R”（読み取り）
	EventDateTime	M	イベントが発生した時刻。
	EventOutcomeIndicator	M	イベントの成功、失敗を示す。
	EventTypeCode	U	イベントのタイプ。
ユーザ関連(1..2)	UserID	M	監査ログにアクセスした人またはプロセスの ID。両方ともわかっている場合は、人とプロセスの両方を含める。これは発生源(AuditSourceID)においてユニークな値である。
	AlternativeUserID	U	監査ログにアクセスした人またはプロセスの別の ID。
	UserName	U	監査ログにアクセスした人またはプロセスの名前。
	UserIsRequestor	M	監査ログにアクセスした人またはプロセスが本イベントの要求者か否かを示す。以下の値が入る。 EV TRUE
	RoleIDCode	U	イベントを実行するときの監査ログにアクセスした人またはプロセスの役割。
	NetworkAccessPointTypeCode	U	ネットワークアクセスポイントのタイプ。
	NetworkAccessPointID	U	ネットワークアクセスポイントに対する ID。
発生源システム関連(1)	AuditEnterpriseSiteID	U	ネットワーク中の論理的な発生源システムの場所。AuditSourceID を修飾するために使う。
	AuditSourceID	M	発生源システムのユニークな ID。
	AuditSourceTypeCode	U	発生源システムのタイプ。
関係者オブジェクト関連(アクセスされた監査ログ)(1)	ParticipantObjectTypeCode	M	関係者オブジェクトのタイプコード。以下の値が入る。 EV 2(システム)
	ParticipantObjectTypeCodeRole	M	関係者オブジェクトの役割を示すコード。以下の値が入る。 EV 13(セキュリティリソース)
	ParticipantObjectDataLifeCycle	U	関係者オブジェクトのデータライフサイクルステージの ID。
	ParticipantObjectIDTypeCode	M	ParticipantObjectID に含まれるタイプ。以下の値が入る。 EV 12(URI)
	ParticipantObjectSensitivity	U	ParticipantObjectID に対するポリシー定義の機微性。
	ParticipantObjectID	M	関係者オブジェクトのインスタンス ID。URI(ファイル名、テーブル名等)
	ParticipantObjectName	M	関係者オブジェクトのインスタンスの名前。ファイル名、テーブル名等
	ParticipantObjectDetail	U	関係者オブジェクトのインスタンスの詳細情報。
	ParticipantObjectDescription	U	関係者オブジェクトのインスタンスの説明。

7.10. イベントIDおよびコード表

CID(ccc1) 監査イベント ID
コンテキスト ID(ccc1)
監査イベント ID
タイプ: 拡張可能　　バージョン: 20201105

表 7.10-1 イベント ID およびコード表

符号化体系指定子	コード値	コード意味
JAHIS	110110	Patient Record(患者レコード)*1
DCM	110100	Application Activity
DCM	110101	Audit Log Used
DCM	110106	Export
DCM	110107	Import
DCM	110110	Patient Record(患者レコード)
DCM	110112	Query(問合せ)
DCM	110113	Security Alert
DCM	110114	User Authentication
JAHIS	110100	Non-PatientRecords

*1 Ver.2.0 で規定していた(JAHIS,110110,"Patient Record")は廃止。(DCM,110110,"Patient Record")を使用のこと。

付録―1. 参考文献

（1）個人情報の保護に関する法律
個人情報保護委員会の以下の URL を参照のこと。
https://www.ppc.go.jp/personalinfo/legal/

（2）医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス
厚生労働省の以下の URL を参照のこと。
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000027272.html

（3）一般社団法人日本画像医療システム工業会（JIRA） DICOM の世界
一般社団法人日本画像医療システム工業会（JIRA） の以下の URL を参照のこと。
https://www.jira-net.or.jp/index.html

付録―2. 作成者名簿

作成者(社名五十音順)

有馬　一閣	株式会社 NTT データ
下野　兼揮	株式会社グッドマン
西田　慎一郎	株式会社島津製作所
梶山　孝治	富士フイルム株式会社
村田　公生	富士フイルム株式会社
茗原　秀幸	三菱電機株式会社

改定履歴		
日付	バージョン	内容
2006/12	1.0	初版
2008/10	1.1	●章立てを JAHIS 標準テンプレートに従うように変更 ●メッセージの一般書式説明を追加 ●以下のトリガイベントを追加し、それぞれのメッセージ仕様を規定 ・業務アプリケーションの起動および停止のイベント ・利用者認証のイベント ・個人情報の外部への出力のイベント ・個人情報の外部からの入力のイベント ・個人情報以外の情報へのアクセスイベント ・業務アプリケーションにおけるセキュリティに関するイベント ・業務アプリケーションの保存している監査ログへのアクセスイベント
2014/2	2.0	●引用規格を最新のものに対応するように改定 ●メッセージの一般書式説明に以下の項目を追加。 ・AccessPurposeCode ・ParticipantObjectPolicySet ●患者情報へのアクセスイベントの EventID を変更
2021/5	2.1	●最新の DICOM、ISO27789 と整合するように改定 ●RFC3881 への参照を削除 ●引用規格を最新のものに対応するように改定 ●メッセージの一般書式説明に以下の項目を追加。 ・ParticipantObjectDescription ●項目名 AlternateUserID を AlternativeUserID に修正
2025/X	2.2	●以下の項目名のオプション性の変更に対応するように改訂。 ・ParticipantObjectName ・ParticipantObjectQuery

（JAHIS標準　25-）
2025 年 X 月発行

ヘルスケア分野における監査証跡のメッセージ標準規約 Ver.2.2

発行元　一般社団法人　保健医療福祉情報システム工業会
〒105－0004　東京都港区新橋2丁目5番5号
（新橋2丁目MTビル5階）

電話　03-3506-8010　　FAX　03-3506-8070