JAHIS 標準 09-003

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 Ver1.1

2010年02月

保健医療福祉情報システム工業会

セキュリティ委員会

監査証跡ＷＧ

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 Ver1.1

ま　え　が　き

平成 17 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つのガイドラインが出された。これらの中で医療機関に対して、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が本規約である。また、従来規格で定義が曖昧と思われる項目の記述を見直した。

本ガイドラインが、医療情報のの普及・推進に多少とも貢献できれば幸いである。

2010 年 02 月

保健医療福祉情報システム工業会
セキュリティ委員会
監査証跡ＷＧ

＜＜ 告知事項 ＞＞

本ガイドラインは関連団体の所属の有無に関わらず、ガイドラインの引用を明示することで自由に使用することができるものとします。ただし一部の改変を伴う場合は個々の責任において行い本ガイドラインに準拠する旨を表現することは厳禁するものとします。

本ガイドラインならびに本ガイドラインに基づいたシステムの導入・運用についてあらゆる障害や損害について、本ガイドライン作成者は何らの責任を負わないものとします。ただし、関連団体所属の正規の資格者は本ガイドラインについての疑義を作成者に申し入れることができ、作成者はこれに誠意をもって協議するものとします。

改定履歴		
日付	Ver	内容
2006/12	1.0	初版
2009/10	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

目次

第１章　適応範囲

１．１　目的

本規約においては監査証跡のうち「医療情報システムに関する安全管理のガイドライン」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

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。

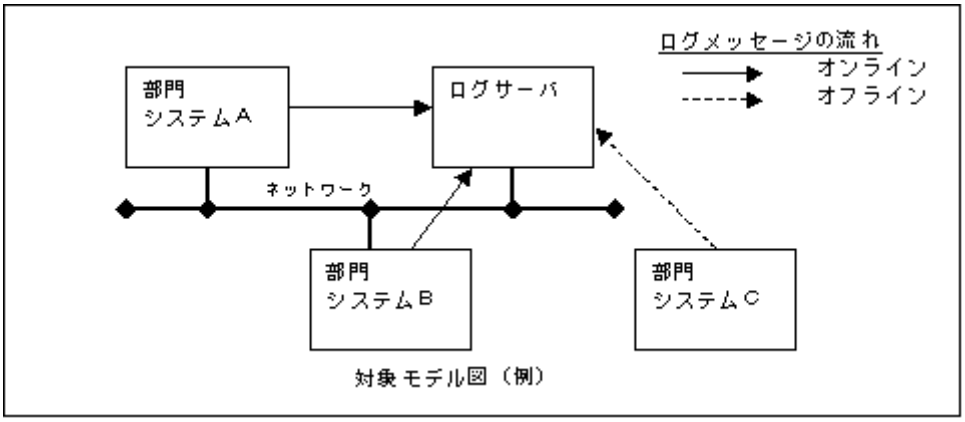
また、規約の策定に当たっては、標準的な形式を採用し、ユーザ側に不必要な手間が発生しないようにすることを重視し、以下の二点に注意して策定を行った。

（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

１．３　適応範囲

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下記のように定義する。



対象モデル図（例）

（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

この規格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、この規格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。

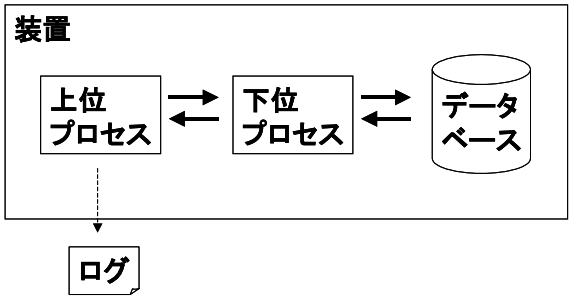
（４）　それぞれの情報システムにおいて、保護対象となる情報へのアクセスが行われた際に、それぞれの情報システムが監査ログを生成すること

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

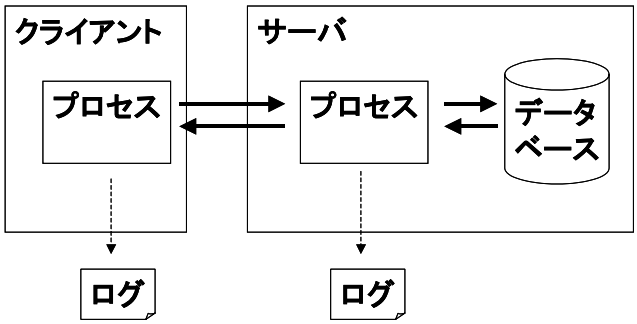
アのプロセス等）が監査ログを出力するかは、その形態によって変わってくる。ここでは、参考として代表的なシステム形態における監査ログの出力場所の例を示す。

スタンドアロン型の場合



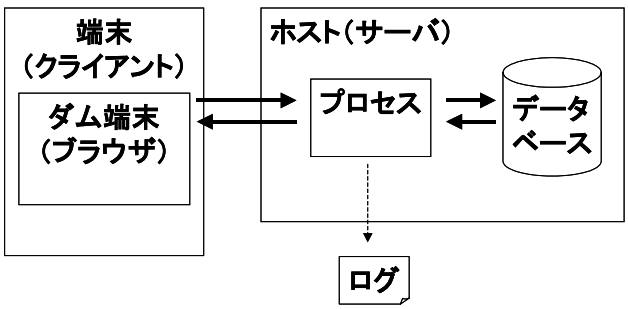
・上位プロセスが下位プロセスに指示して保護対象情報アクセスするケースでは、上位プロセス側で監査ログを生成する
・ただし、これは下位プロセスからの監査ログ出力を妨げるものではない

クライアント・サーバ型の場合



・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



・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

この規約では、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、本規格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

第２章　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４版

厚生労働省から平成 21 年 3 月 31 日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 Supplement 95：Audit Trail Messages

米国放射線学会（ACR）と北米電子機器工業会（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 Communication 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 の監査証跡に関する技術文書として、「Supplement 95 : Audit Trail Messages（以下「Supplement 95」という。）」 が提唱されているが、現時点では Frozen Draft となっている。しかし、医療に特化したセキュリティとプライバシーの全体的なシステムの一部として監査機能を扱っており、監査メッセージの交換に関しての規定としては大変有効である。

Supplement 95 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簡素にするためである。

（３） RFC3881 : Security Audit & Access Accountability XML Data Definitions for Healthcare Applications

Supplement 95 基本メッセージフォーマットは「RFC 3881 : Security Audit & Access Accountability XML Data Definitions for Healthcare Applications（以下「RFC 3881」という。）」で規定される XML スキーマを拡張させ、DICOM アプリケーションが XML ベースの監査証跡メッセージを設定するために必要な語彙（DICOM 固有の監査メッセージ）を定義している。具体的には、医療データに誰が、いつ、どのような操作に対して、どこからアクセスし、どの患者のレコードが関係するかが監査メッセージに含まれる。また、監査メッセージの伝送メカニズムは「RFC 3195 : Reliable Delivery for syslog」で規定される SYSLOG を使用して伝送ポイントに伝送される仕組みとなっており同時に、信頼できる伝送、バッファリング、確認応答、認証、識別、および暗号化のメカニズムを提供する。

第３章　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フェイルセーフとしてよい。

（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。

第４章　記号および略語

このガイドラインでは、次の記号および略語の表記を用いる。

DBMS	Database Management System
DICOM	Digital Imaging and Communication in Medicine
OS	Operation System

PHI	Protected Healthcare Information
RFC	Request for Comments

第５章　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

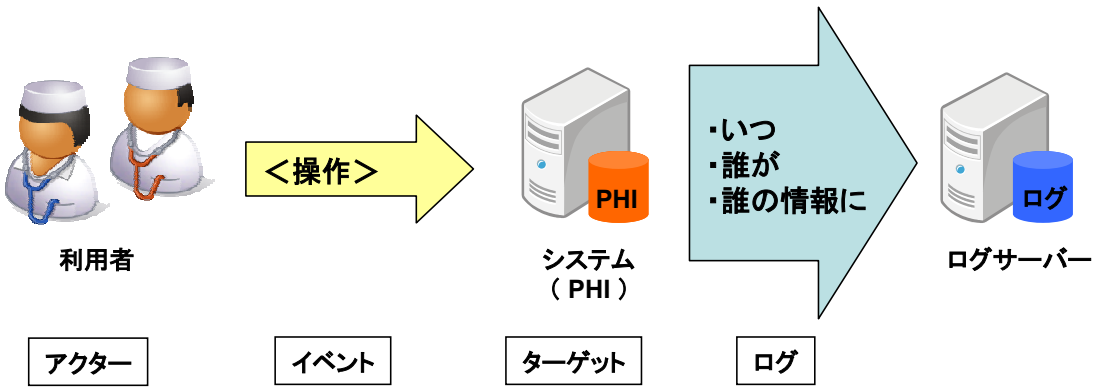
５．２　イベント種類と内容の解説

５．２．１　個人情報へのアクセスイベント（必須）

本規約では、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。

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

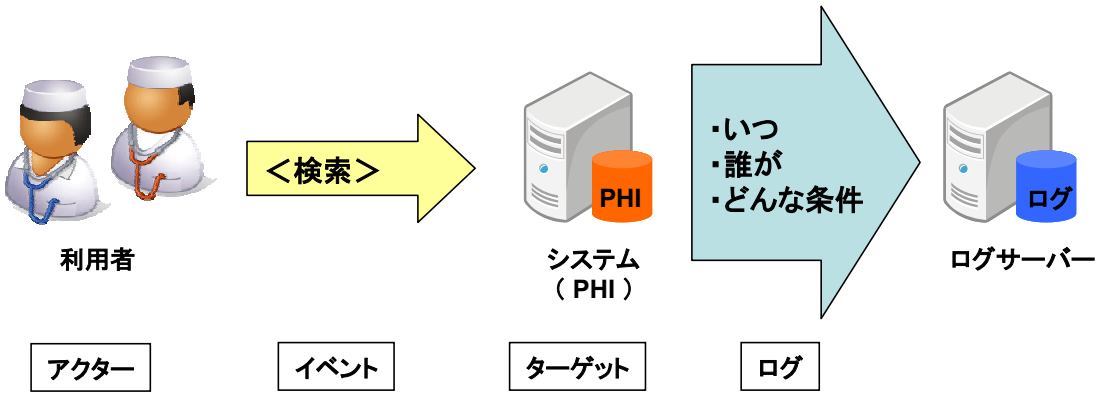


５．２．２　個人情報への検索イベント（必須）

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。

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

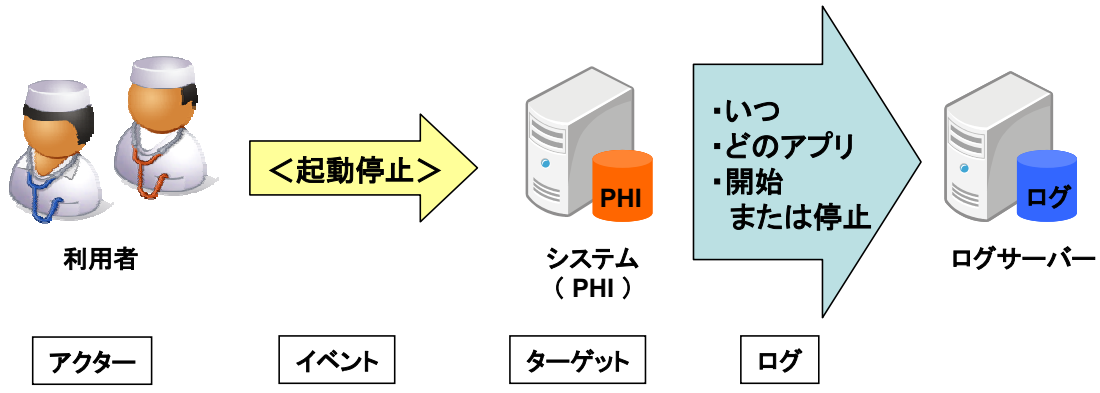


５．２．３　業務アプリケーションの起動および停止のイベント（オプション）

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。

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

業務アプリケーションの起動および停止



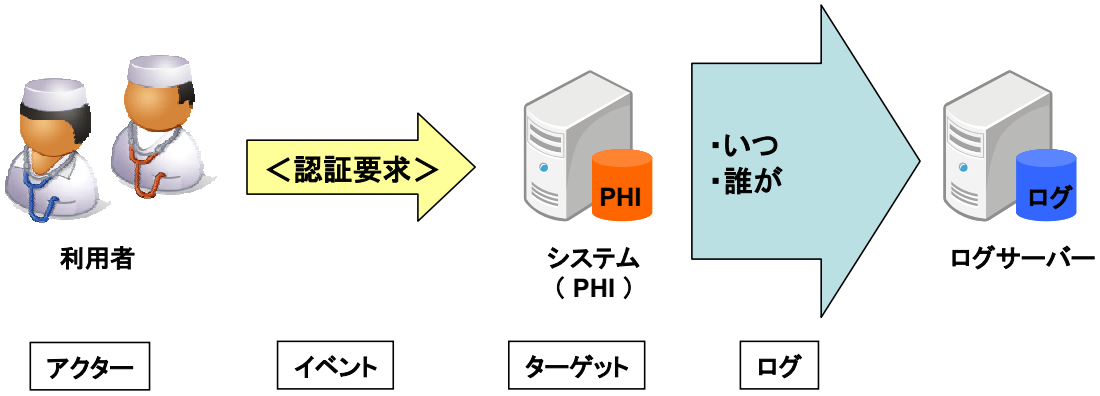
５．２．４　利用者認証のイベント（オプション）

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。

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



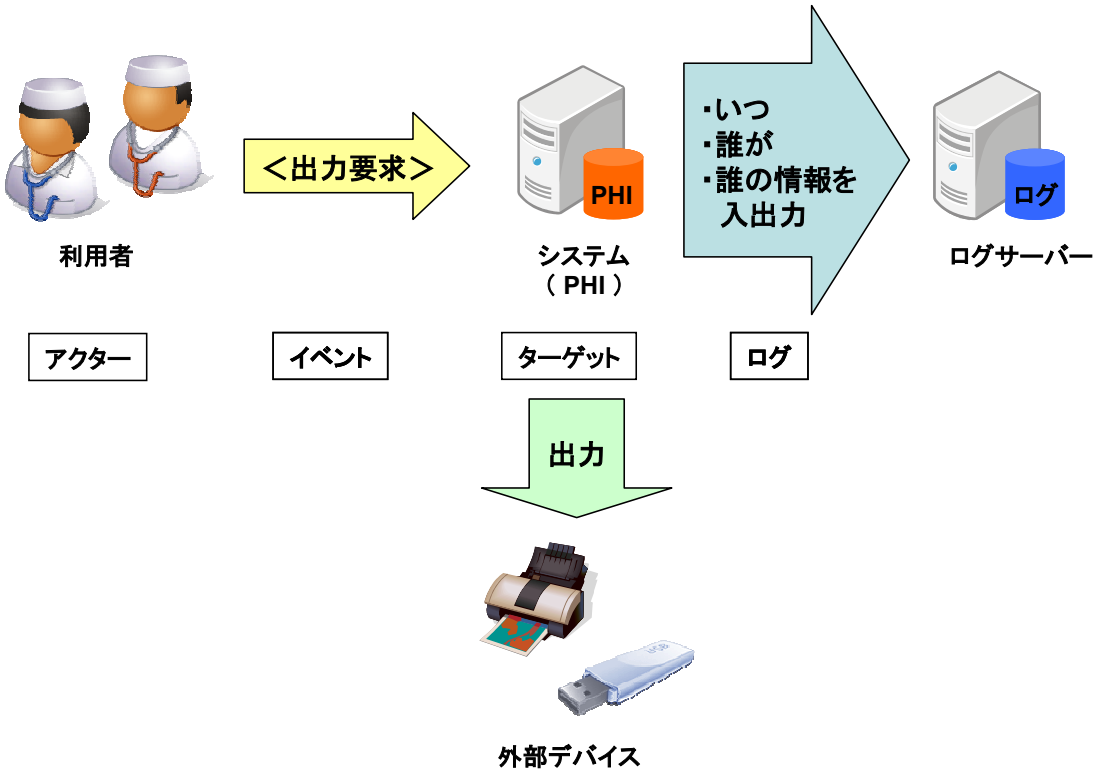
５．２．５　個人情報の外部への出力のイベント（オプション）

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。

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



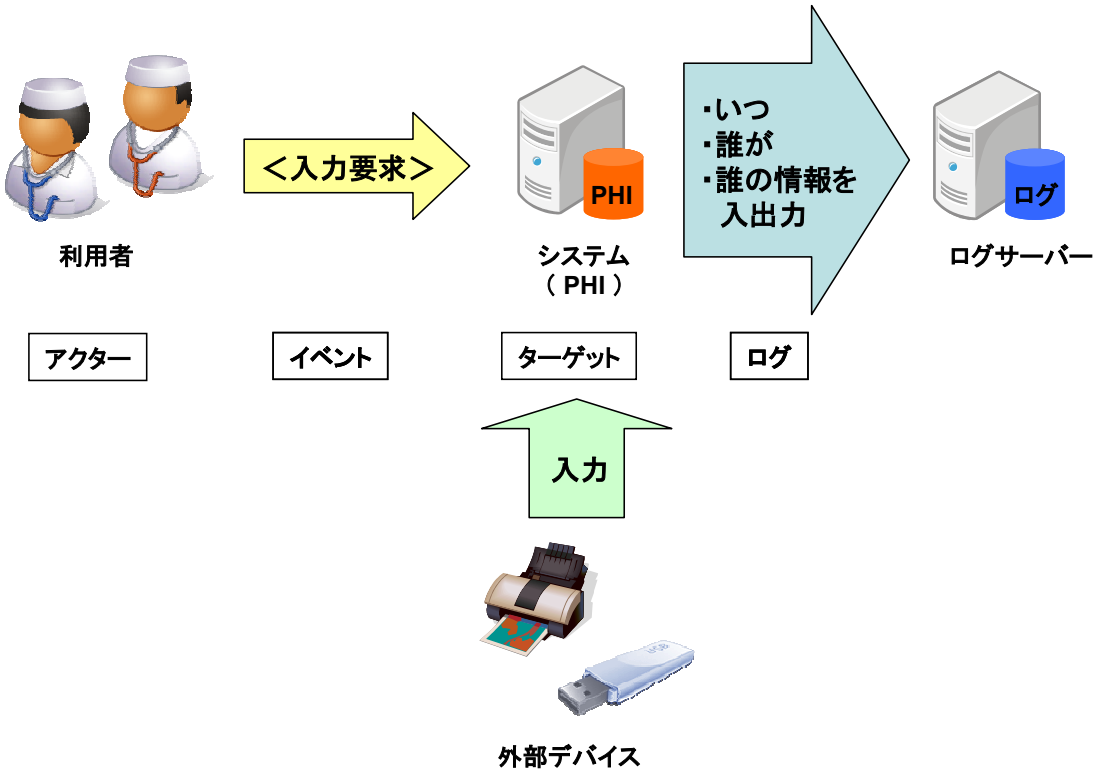
５．２．６　個人情報の外部からの入力のイベント（オプション）

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。

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



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）

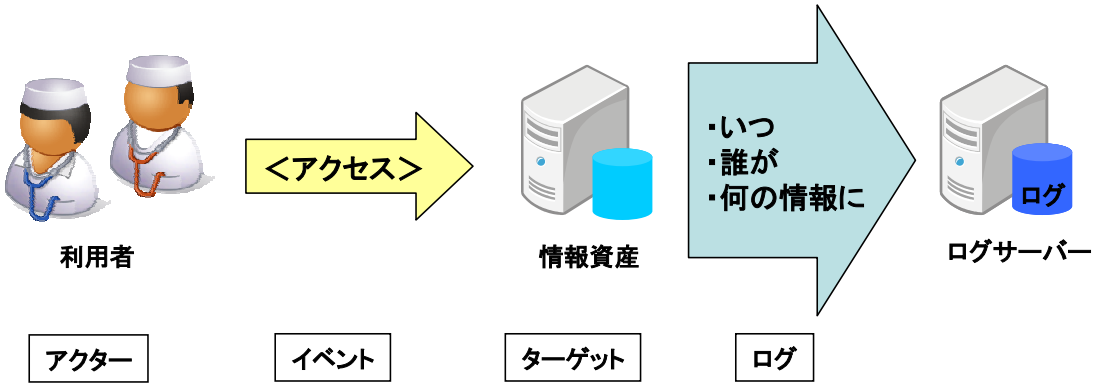
本規約では、個人情報以外の情報へのアクセスイベントを監査イベントとする。個人情報以外の情報資産に対するアクセスを対象とする。例えば、

・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。

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



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、

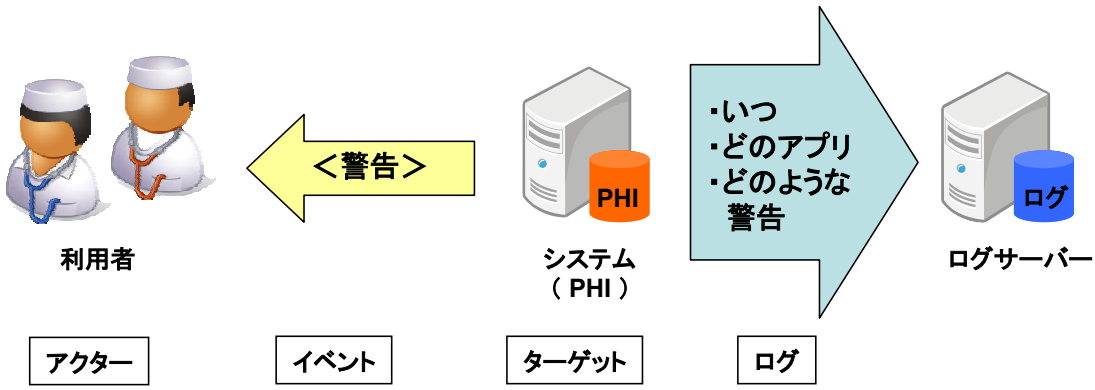
・ファイルの入出力エラー
・異常終了
・リソース不足

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。

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

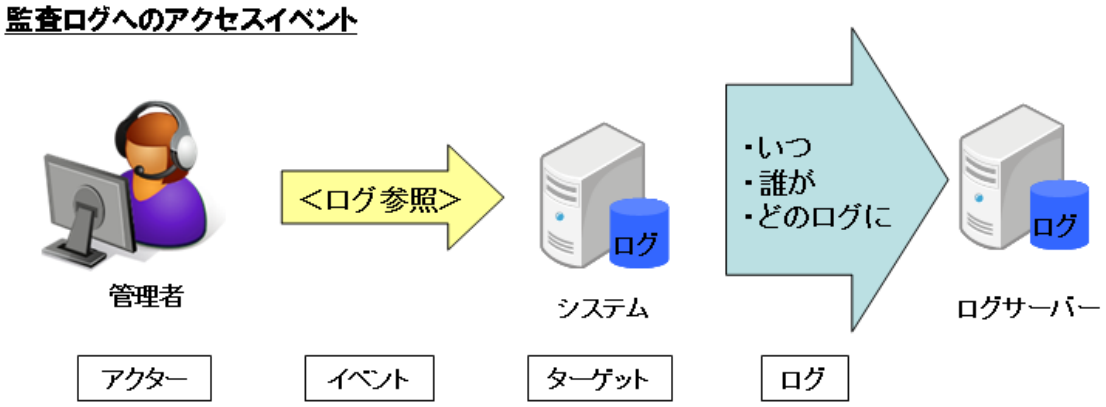
セキュリティ警告イベント



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。

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



第６章　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第７章を参照のこと。メッセージ形式は RFC3881 に準拠したものである。RFC3881 の内容については一部翻訳したものを附属書 A に付けているので参考にしていただきたい。

表の見方について以下に説明する。

・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)

M/U：イベントにより必須またはオプション

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	DICOMおよびJAHIS標準で拡張。 DCID(ccc1)参照。
	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
	EventDateTime	M	イベントの発生した時刻	RFC3881の規定に従う
	EventOutcomeIndicator	M	イベントの成功､失敗を示す	RFC3881の規定に従う
	EventTypeCode	U	イベントのタイプ	DICOMおよびJAHIS標準で拡張。 DCID(ccc2)参照。

ユーザ関連	UserID	M	人またはプロセスのID	6.1.1を参照のこと
	AlternateUserID	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	U	要求者か否かが入る	RFC3881の規定に従う
	RoleIDCode	U	人またはプロセスの役割	DICOMおよびJAHIS標準で拡張。 DCID(ccc3)参照
	NetworkAccessPointTypeCode	U	ネットワークアクセスポイントのタイプ	RFC3881の規定に従う
	NetworkAccessPointID	U	ネットワークアクセスポイントに対するID	RFC3881の規定に従う
発生源システム関連	AuditEnterpriseSiteID	U	発生源システムの場所	RFC3881の規定に従う
	AuditSourceID	M	発生源システムのユニークなID	RFC3881の規定に従う
	AuditSourceTypeCode	U	発生源システムのタイプ	RFC3881の規定に従う
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	RFC3881の規定に従う
	ParticipantObjectTypeCodeRole	M	関係者オブジェクトの役割を示すコード	RFC3881の規定に従う
	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	RFC3881の規定に従う
	ParticipantObjectIDTypeCode	M	ParticipantObjectIDに含まれるタイプ	RFC3881の規定に従う
	ParticipantObjectSensitivity	U	ParticipantObjectIDに対するポリシーで定義された機微性	RFC3881の規定に従う
	ParticipantObjectID	M	関係者オブジェクトのID	6.1.2を参照のこと
	ParticipantObjectName	U	関係者オブジェクトの名前	
	ParticipantObjectQuery	M/U	検索内容	

	ParticipantObjectDetail	U	関係者オブジェクトの詳細情報	

６．１．１　UserID, AlternateUserID, UserName

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。

AlternameUserID 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。

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。

６．１．２　ParticipantObjectID, ParticipantObjectName, ParticipantObjectQuery, ParticipantObjectDetail

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、入出力情報等のことである。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。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に必須。

ParticipantObjectDetail には、関係者オブジェクトの詳細情報が入る。

第７章　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。

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。 RFC3881の規定に従う。
	EventOutcomeIndicator	M	イベントの成功、失敗を示す。 RFC3881の規定に従う。
	EventTypeCode	U	イベントのタイプ。 Start End CID(ccc2)を使用してJAHISにより拡張した値が入る。
ユーザー関連 (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。
	AlternateUserID	U	データを操作した人またはプロセスの別のID。 RFC3881の規定に従う。
	UserName	U	データを操作した人またはプロセスの名前。 RFC3881の規定に従う。

	UserIsRequestor	U	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。 RFC3881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。 RFC3881の規定に従う。
	NetworkAccessPointID	U	ネットワークアクセスポイントに対するID。 RFC3881の規定に従う。
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。 RFC3881の規定に従う。
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。 RFC3881の規定に従う。
	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。 RFC3881の規定に従う。
	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	U	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。 RFC3881の規定に従う。

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。

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。 RFC3881の規定に従う。
	EventOutcomeIndicator	M	イベントの成功、失敗を示す。 RFC3881の規定に従う。
	EventTypeCode	U	イベントのタイプ。 RFC3881の規定に従う。
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。
	AlternateUserID	U	検索を発行したプロセスの別のID。 RFC3881の規定に従う。
	UserName	U	検索を発行したプロセスの名前。 RFC3881の規定に従う。
	UserIsRequestor	U	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。 RFC3881の規定に従う。
	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”)
	NetworkAccessPointTypeCode	U	ネットワークアクセスポイントのタイプ。 RFC3881の規定に従う。
	NetworkAccessPointID	U	ネットワークアクセスポイントに対するID。 RFC3881の規定に従う。
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。
	AlternateUserID	U	検索に応答するプロセスの別のID。 RFC3881の規定に従う。
	UserName	U	検索に応答するプロセスの名前。 RFC3881の規定に従う。
	UserIsRequestor	U	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。 RFC3881の規定に従う。
	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”)

	NetworkAccessPointTypeCode	U	ネットワークアクセスポイントのタイプ。 RFC3881の規定に従う。
	NetworkAccessPointID	U	ネットワークアクセスポイントに対するID。 RFC3881の規定に従う。
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。
	AlternateUserID	U	他の関係者の別のID。 RFC3881の規定に従う。
	UserName	U	他の関係者の名前。 RFC3881の規定に従う。
	UserIsRequestor	U	他の関係者が本イベントの要求者か否かを示す。 RFC3881の規定に従う。
	RoleIDCode	U	他の関係者の役割。 RFC3881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。 RFC3881の規定に従う。
	NetworkAccessPointID	U	ネットワークアクセスポイントに対するID。 RFC3881の規定に従う。
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。 RFC3881の規定に従う。
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 (レポート)
	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。 RFC3881の規定に従う。
	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。 RFC3881の規定に従う。
	ParticipantObjectID	M	関係者オブジェクトのインスタンスのID。 RFC3881の規定に従う。
	ParticipantObjectName	U	関係者オブジェクトのインスタンスの名前。 RFC3881の規定に従う。
	ParticipantObjectQuery	M	base64で符号化された検索内容。本内容は本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。 RFC3881の規定に従う。

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。

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。 RFC3881の規定に従う。
	EventOutcomeIndicator	M	イベントの成功、失敗を示す。 RFC3881の規定に従う。
	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。
	AlternateUserID	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。 RFC3881の規定に従う。
	UserName	U	起動あるいは停止したアプリケーションの名前。 RFC3881の規定に従う。
	UserIsRequestor	U	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。 RFC3881の規定に従う。
	NetworkAccessPointID	U	ネットワークアクセスポイントに対するID。 RFC3881の規定に従う。
アプリケーションを起動/停止させたユーザm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。
	AlternateUserID	U	起動あるいは停止させた人またはプロセスの別のID。 RFC3881の規定に従う。
	UserName	U	起動あるいは停止させた人またはプロセスの名前。 RFC3881の規定に従う。
	UserIsRequestor	U	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。 RFC3881の規定に従う。
	NetworkAccessPointID	U	ネットワークアクセスポイントに対するID。 RFC3881の規定に従う。
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。 RFC3881の規定に従う。

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。

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。 RFC3881の規定に従う。
	EventOutcomeIndicator	M	イベントの成功、失敗を示す。 RFC3881の規定に従う。
	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。
	AlternateUserID	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。 RFC3881の規定に従う。
	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。 RFC3881の規定に従う。
	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。 RFC3881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。 RFC3881の規定に従う。
	NetworkAccessPointID	U	ネットワークアクセスポイントに対するID。 RFC3881の規定に従う。
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。
	AlternateUserID	U	認証を行ったノードの別のID。 RFC3881の規定に従う。
	UserName	U	認証を行ったノードの名前。 RFC3881の規定に従う。
	UserIsRequestor	M	EV FALSE
	RoleIDCode	U	認証を行ったノードの役割。 RFC3881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。 RFC3881の規定に従う。
	NetworkAccessPointID	U	ネットワークアクセスポイントに対するID。 RFC3881の規定に従う。

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。 RFC3881の規定に従う。

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。

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。 RFC3881の規定に従う。
	EventOutcomeIndicator	M	イベントの成功、失敗を示す。 RFC3881の規定に従う。
	EventTypeCode	U	イベントのタイプ。 RFC3881の規定に従う。
出力者関連 (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。
	AlternateUserID	U	データを操作した人またはプロセスの別のID。 RFC3881の規定に従う。
	UserName	U	データを操作した人またはプロセスの名前。 RFC3881の規定に従う。
	UserIsRequestor	U	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”)
	NetworkAccessPointTypeCode	U	ネットワークアクセスポイントのタイプ。 RFC3881の規定に従う。
	NetworkAccessPointID	U	ネットワークアクセスポイントに対するID。 RFC3881の規定に従う。
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
	AlternateUserID	U	データの出力先の別のID。 RFC3881の規定に従う。
	UserName	U	データの出力先の名前。 RFC3881の規定に従う。
	UserIsRequestor	U	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。 RFC3881の規定に従う。

	NetworkAccessPointID	MC	ネットワークアクセスポイントに対するID。 RFC3881の規定に従う。
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。 RFC3881の規定に従う。
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。 RFC3881の規定に従う。
	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。 RFC3881の規定に従う。
	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	U	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。 RFC3881の規定に従う。

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。

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)
	EventDateTime	M	イベントが発生した時刻。 RFC3881の規定に従う。
	EventOutcomeIndicator	M	イベントの成功、失敗を示す。 RFC3881の規定に従う。
	EventTypeCode	U	イベントのタイプ。 RFC3881の規定に従う。
入力者関連 (1..2)	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。
	AlternateUserID	U	データを入力した人またはプロセスの別のID。 RFC3881の規定に従う。
	UserName	U	データを入力した人またはプロセスの名前。 RFC3881の規定に従う。
	UserIsRequestor	U	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”)
	NetworkAccessPointTypeCode	U	ネットワークアクセスポイントのタイプ。 RFC3881の規定に従う。
	NetworkAccessPointID	U	ネットワークアクセスポイントに対するID。 RFC3881の規定に従う。
入力元関連(1)	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
	AlternateUserID	U	データの入力元の別のID。 RFC3881の規定に従う。
	UserName	U	データの入力元の名前。 RFC3881の規定に従う。
	UserIsRequestor	U	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 (110155, DCM, “Source Media”)
	NetworkAccessPointTypeCode	U	ネットワークアクセスポイントのタイプ。 RFC3881の規定に従う。

	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 RFC3881の規定に従う。
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。 RFC3881の規定に従う。
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。 RFC3881の規定に従う。
	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。 RFC3881の規定に従う。
	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	U	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。 RFC3881の規定に従う。

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。

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。 RFC3881の規定に従う。
	EventOutcomeIndicator	M	イベントの成功、失敗を示す。 RFC3881の規定に従う。
	EventTypeCode	U	イベントのタイプ。 Start End CID(ccc2)を使用してJAHISにより拡張した値が入る。
ユーザー関連 (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。
	AlternateUserID	U	データを操作した人またはプロセスの別のID。 RFC3881の規定に従う。
	UserName	U	データを操作した人またはプロセスの名前。 RFC3881の規定に従う。
	UserIsRequestor	U	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。 RFC3881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。 RFC3881の規定に従う。
	NetworkAccessPointID	U	ネットワークアクセスポイントに対するID。 RFC3881の規定に従う。
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。 RFC3881の規定に従う。
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 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(レポート)

	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。 RFC3881の規定に従う。
	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。 RFC3881の規定に従う。
	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	U	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。 RFC3881の規定に従う。

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。

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。 RFC3881の規定に従う。
	EventOutcomeIndicator	M	イベントの成功、失敗を示す。 RFC3881の規定に従う。
	EventTypeCode	M	イベントのタイプ。 RFC3881の規定に従う。
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。
	AlternateUserID	U	イベントを発行したプロセスの別のID。 RFC3881の規定に従う。
	UserName	U	イベントを発行したプロセスの名前。 RFC3881の規定に従う。
	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。 RFC3881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。 RFC3881の規定に従う。
	NetworkAccessPointID	U	ネットワークアクセスポイントに対するID。 RFC3881の規定に従う。
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。
	AlternateUserID	U	イベントに応答するプロセスの別のID。 RFC3881の規定に従う。
	UserName	U	イベントに応答するプロセスの名前。 RFC3881の規定に従う。
	UserIsRequestor	U	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。 RFC3881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。 RFC3881の規定に従う。

	NetworkAccessPointID	U	ネットワークアクセスポイントに対するID。 RFC3881の規定に従う。
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。 RFC3881の規定に従う。
警告サブジェクト関連 (1)	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(マスターファイル） 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。 RFC3881の規定に従う。
	ParticipantObjectIDTypeCode	M	ParticipantObjectIDに含まれるタイプ。 EV 12(URI)
	ParticipantObjectSensitivity	U	ParticipantObjectIDに対するポリシー定義の機微性。 RFC3881の規定に従う。
	ParticipantObjectID	M	警告サブジェクトのインスタンスのID。 ファイル名、テーブル名など（URI）、 RFC3881の規定に従う。
	ParticipantObjectName	U	警告サブジェクトのインスタンスの名前。 RFC3881の規定に従う。
	ParticipantObjectQuery	U	警告サブジェクトの実際のQuery情報 RFC3881の規定に従う。
	ParticipantObjectDetail	U	警告サブジェクトのインスタンスの詳細情報。 RFC3881の規定に従う。

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。

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。 RFC3881の規定に従う。
	EventOutcomeIndicator	M	イベントの成功、失敗を示す。 RFC3881の規定に従う。
	EventTypeCode	U	イベントのタイプ。 RFC3881の規定に従う。
ユーザー関連 (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。
	AlternateUserID	U	監査ログにアクセスした人またはプロセスの別のID。 RFC3881の規定に従う。
	UserName	U	監査ログにアクセスした人またはプロセスの名前。 RFC3881の規定に従う。
	UserIsRequestor	U	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。 RFC3881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。 RFC3881の規定に従う。
	NetworkAccessPointID	U	ネットワークアクセスポイントに対するID。 RFC3881の規定に従う。
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。 RFC3881の規定に従う。
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。 RFC3881の規定に従う。
	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。 RFC3881の規定に従う。
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	U	関係者オブジェクトのインスタンスの名前。
ParticipantObjectDetail	U	関係者オブジェクトのインスタンスの詳細情報。 RFC3881の規定に従う。

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: 20091001

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

CID(ccc2) 監査イベントタイプコード

コンテキストID(ccc2)
イベントタイプコード

タイプ: 拡張可能　　バージョン: 20091001

符号化体系指定子	コード値	コード意味
JAHIS	110120	Start（アクセス開始）
JAHIS	110121	End（アクセス終了）
DCM	110120	Application Start
DCM	110121	Application Stop
DCM	110122	Login
DCM	110123	Logout

CID(ccc1) 役割ID

コンテキストID(ccc3)
役割 ID

タイプ: 拡張可能　　バージョン: 20091001

符号化体系指定子	コード値	コード意味
DCM	110152	Destination(送信先)
DCM	110153	Source(送信元)
DCM	110150	Application
DCM	110151	Application Launcher

DCM	110154	Destination Media
DCM	110155	Source Media

附属書 A 「RFC3881：Security Audit & Access Accountability XML Data Definitions for Healthcare Applications」　５章 Data Definitions　翻訳

本附属書は、「RFC3881：Security Audit & Access Accountability XML Data Definitions for Healthcare Applications」における「５章　データ定義」を翻訳したものである。監査ログメッセージ解釈の参考にしていただきたい。

5. データ定義

このセクションは XML スキームでデータを定義し記述する。

データ要素は、下記のように分類される：

1）イベント識別　　-何が行われたか
2）アクティブな関係者識別　　-誰によって
3）ネットワーク・アクセスポイント識別　-どこで始められたか
4）発生源識別　　-どのサーバを使用したか
5）関係オブジェクト識別　　-どの記録に対して

5.1. イベント識別

次のデータは名前、アクション・タイプ、時間、そして監査されたイベントの配列を識別する。

イベント識別データは、監査イベント毎に 1 つのセットが存在する。

5.1.1. イベント識別

説明

特定の監査されたイベント(例えばメニュー項目、プログラム、ルール、ポリシー、機能コード、アプリケーション名、URL)のための識別子であり、実行された機能を識別する。

オプション性：　必須

形式 / 値

システム実装者によって定義されたか標準的な用語集を参照するためのコード化された値。「コード」属性は少なくとも発生源識別内で、曖昧なことなくユニークでなければならない（セクション 5.4 参照）。イベント識別の例はプログラム名、メソッド名あるいは関数名である。

コードとして定義、または標準の参照のため、XML スキーマは以下のオプション属性を定義する。

属性	値
CodeSystem	OID 参照。
CodeSystemName	コード化するシステムの名前；ローカルに定義されたコードセットのための値であることを強く推奨する。
DisolayName	表示と報告書の中で使用される値
OriginalText	コードに変換される入力値

あいまいでないイベント識別要求のサポートのため、複数の値の定義は禁止である。

原理

これは監査された機能を識別する。“実行”というイベント･アクション･コード監査記録については、これがアプリケーション関数が実行されたことを示す。

5.1.2. イベント･アクション･コード

説明

監査を生成するイベント実行中のアクション･タイプの指標

オプション性： オプション

形式 / 値

一覧表：

値	意味	例
C	生成	あるオーダーを発行したときのような、新しいデータベースオブジェクトの生成
R	読む/見る/印刷/検索	医者監査のような、データの表示や印刷
U	更新	患者情報の改訂のような、データの更新
D	削除	医師マスター･ファイルのレコードのような、項目の削除
E	実行	ログオン、プログラム実行、オブジェクト・メソッドの使用のような、システムやアプリケーション機能の実行

原理

これは、関連オブジェクト上でどのような種類のアクションが行われたかを明示する。

注

上記に列挙されていないアクションは、特定の機能か、オブジェクト間メソッド、あるいは２つ以上の別個のイベントの実行と見なされる。

認可のようなアプリケーション･アクションは実行機能であり、イベント識別は機能を示す。

放射線画像のようなアプリケーションにとって、検索アクションはデータ自体にはアクセスせず、データの存在のみを確認します。監査は明確に区別する必要はない。

“移動”のような合成アクションは、読む・生成・削除のそれぞれの操作、または、関数やメソッドの実行によって監査データの生成により監査される。

5.1.3. イベント日付/時間

説明

世界標準時(UTC：Universal coordinated time)

例：現地時間の不明瞭性をなくすための日時の仕様

オプション性: 必須

形式/値

世界標準時(UTC)を明確に伝えるために、ISO8601 標準に従って形式化された日時の表現

原理

イベントを特定の日時に関連付ける。特にセキュリティ監査では、地理分布により発生する時間差問題を排除するために、一貫した時間基準（例：UTC）を必要とする。

注

分散システムでは、幾つかの共通の時間基準（例：NTP[RFC1305] サーバー）を利用するのが良い実装の方策である。

5.1.4. イベント結果インジケータ

説明

イベントが成功したか、または失敗したかを表示する。

オプション性: 必須

形式／値

一覧表：

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：ユーザによる過度の無効ログオンの試みによるアカウント無効）

原理

いくつかの監査イベントが、成功または失敗インジケータによって判定される。例えば、なぜログインが失敗したかを表示するために、このフラグにゼロでない値をセットする。

注

いくつかの場合、放射線検査の不完全又は中断した転送のように、「成功」は部分的な可能性がある。責任を明確にするため、これらの区別は関係しない。

5.1.5. イベントタイプコード

説明

イベントのカテゴリのための識別子。

オプション性: オプション

形式／値

システムの実装者により定義された、または標準的な用語集に対する参照として定義された、コード化された値の一覧。

定義されたコード、または標準に対する参照を実装するため、XML スキーマが下記の任意の属性を定義する。

属性	値
CodeSystem	OID 参照
CodeSystemName	コードシステムの名前。 ローカルで定義されたコードセットに意義を持たせる

ために強く推奨する。

DisplayName　表示とレポートに利用するために必要。

OriginalText　コードに変換された入力値

イベントが 1 つ以上の方法で分類される可能性があるため、複数の値が指定されることがある。

原理

このフィールドは、実装で定義されたイベントカテゴリによって、メッセージの検索を可能にする。

5.2.　実使用者識別

以下のデータは、監査イベント記録を目的のためにユーザを識別する。ユーザは、人もしくは、人以外により起動された装置、あるいはソフトウェアプロセスである。　オプションとして、ユーザのネットワークアクセスの場所が特定化される。

１つのイベントに対して複数のユーザが想定される。例えば、あるユーザが別の複数のユーザを起動したり、複数のユーザや装置、プロセスが関連するイベントがある。しかしながら、そのイベントを起動もしくは要求するのは単一のユーザであろう。

5.2.1.　ユーザ ID

説明

そのイベントに実際に関係するユーザのユニークな ID

オプション性:　必須

形式／値

認証システムから提供される文字列としてのユーザ識別子。これは、発生源識別（5.4 参照）に含まれるユニークな値である。

原理

この項は監査イベントと特定のユーザを関連づける。

注

システム間の監査に対しては、特に長期間の保存の場合、このユーザ識別子は永久的に

ユニークなキーを用いることにより、監査イベントと特定ユーザとの関連付けを永久に行う。

ノード単位の認証に対しては、人間以外の装置やプロセスを識別する場合に限り、ユーザ ID としてノード名が使われる。

5.2.2.　代理ユーザ ID

説明

ユーザに対する代わりのユニークな識別子

オプション性:オプション

形式／値

認証システムから提供される文字列としてのユーザ ID。この ID は、可能であれば、共通の認証システム（SSO など）によるものであろう。

原理

いくつかの状況では、ユーザは 1 つの ID で認証されるが、特定のアプリケーションシステムにアクセスするために、同義の ID を使うこともある。例えば、いくつかの SSO の実装ではこうなるであろう。この代理識別子は、オリジナル識別子として認証に用いられ、ユーザ ID は、アプリケーションによって知られ使用される。

5.2.3.　ユーザ名

説明

ユーザに対する人にとって意味のある名前

オプション性:　オプション

形式／値

文字列

原理

ユーザ ID と代理ユーザ ID は、内部的なものかどうか不明瞭な値である。この項目は、監査人に実際のユーザを識別させる役目をはたす。

5.2.4.　ユーザは要求者

説明

ユーザが、監査されるイベントの要求者もしくは起動者であるかどうかの指標。

オプション性：オプション

形式／値

論理値、省略時解釈は「真」

原理

この値は、要求側ユーザと受容側ユーザとの識別に用いる。例えば、ある者が他のユーザへ送信されるレポート出力を起動する。

5.2.5.　役割 ID コード

説明

イベントを実施する際のユーザの役割の仕様であり、役割ベースのアクセス制御のセキュリティのために割り当てられる。

オプション性：　オプション；複数値

形式／値

認証システムからの役割コードもしくは文字列が付与された「コード」属性を持つコード値。複数の値を使用できる。

コードは実装において定義されるか標準的な用語集を参照する。実装における定義コードもしくは標準への参照に対して、XML スキーマはそれらのオプションの属性を定義する。

属性	値の説明
CodeSystem	OID の参照
CodeSystemName	コーディングシステムの名称；局所的に定義されたコードセットを尊重することを強く推奨する
Display Name	ディスプレイとレポートで使用される値
Original Text	コードに変換される入力値

原理

この値は、監査イベントとユーザの役割を結びつける。ユーザの機能的役割カテゴリーを用いてイベントの集合を解析するためのオプションの値である。

注

多くのセキュリティシステムではこのデータを生成することができないため、これはオプションとなる。

共通のメッセージに対して、可能であれば、この識別子は共通の認証システムにとって知られたものとなる。あるいは、これは発生源ＩＤ（4.4 節参照）に含まれるユニークな値である。複数のシステムから収集される監査データの曖昧さを防ぐために、役割に関連する広域でのユニークな識別子の採用を検討せよ。

役割 ID は、個人の説明責任の代わりにはならない。

複合的な役割と複数の役割を持つユーザにより曖昧さが生じる、例えば、複合的な中のどの役割が使用されたか、あるいは、どの権限を用いたのか？

5.3.　ネットワークアクセスポイント識別

ネットワークアクセスポイントは、アプリケーション動作時にネットワークの論理的位置を識別する。これらのデータは１：１に実使用者識別データと対応する。

5.3.1.　ネットワークアクセスポイント種類コード

説明

ネットワークアクセスポイントの種類、つまり監査イベントによってもたらされる識別子である。

オプション性：オプション

形式／値

一覧表：

値	意味
1	マシン名、DNS 名を含む
2	IP アドレス

3　電話番号

原理

このデータは監査イベントにおけるユーザデバイスのネットワークアクセスポイント識別子の種類を示す。この値はオプションであり、複数のサーバに記録されたイベント群を、ネットワークアクセスポイントの種類ごとに分析する場合などに用いられる。

5.3.2.　ネットワーク・アクセスポイントＩＤ

説明

監査イベントのための、ユーザデバイスのネットワーク・アクセスポイントの識別子である。これは装置 ID、IP アドレス、または装置に関連した幾つかの識別子である。

オプション性：オプション

形式／値

与えられたネットワーク・アクセスポイントの種類が特定されていれば、テキストは有効な値のみに規定される。特定に関しては、なるべく多くのオプションが使えることが望ましい。

原理

このデータはユーザのネットワーク・アクセスポイントを識別し、実行したサーバのネットワーク・アクセスポイントを明確にする。この値はオプションであり、複数のサーバに記録されたイベント群に対して、特定のネットワーク・アクセスポイントのデータアクセスを分析する場合などに用いられる。

注

ネットワークアクセスポイント ID は個人の説明責任の代りにはならない。特にインターネット IP アドレスは、変り易く、特に短い時間の中で 1 人以上に割り当てられる可能性がある。

例

```
Network Access Point ID: SMH4WC02
Network Access Point Type: 1 = Machine Name

Network Access Point ID: 192.0.2.2
```

Network Access Point Type: 2 = IP address

Network Access Point ID: 610-555-1212
Network Access Point Type: 3　= Phone Number

5.4.　発生源識別

以下のデータは主としてアプリケーション・システムとプロセスに必要である。多層、分散、あるいは複合アプリケーション群は発生源識別が曖昧となるので、そのイベントに実際に係った各アプリケーションやプロセスによるフィールド収集が必要となる。　例えば、複数のセットされた値は、複数層に分散されたアプリケーションを構成しているウェブサーバ、アプリケーションプロセスやデータベースサーバ処理を特定することができる。低レベルのネットワーク転送等の受動的イベントは特定される必要はない。

実装戦略によって、多層、分散、あるいは複合アプリケーションを構成するコンポーネントが、一つのアプリケーションイベントに対し一つ以上の監査メッセージを生成することは可能である。その後のデータ整理は必要ではあるが、監査メッセージ内のさまざまなデータはそのようなケースの識別に利用されます。このドキュメントは、リポジトリと報告メカニズムにより必要時にデータ整理をされることを前提とするが、それらのメカニズムを特定しない。

5.4.1.企業サイト ID の監査

説明
ヘルスケア企業ネットワークの中の論理的な発生源の位置。例えば、複合企業の中の病院または他のプロバイダー位置。

オプション性：　オプション

形式／値
ヘルスケア事業体の中のユニークな識別テキストストリング。監査データを生成するアプリケーションが発生源ＩＤによって唯一特定されるときは、値なしでよい。

原理
この値はマルチサイト企業健康情報システムのサイトの中で区別される。

注

これは監査記録を生成するアプリケーションで定義される。 それは、その企業とわかるビジネス組織（データ所有者）が識別できるユニークコードを含む。その値は、更に発生源ＩＤを特定し、曖昧さを除く。業種により、値は異なるかもしれない。 組織の中において、レベルの差があるかもしれない。

5.4.2. 発生源ＩＤの監査

説明

イベントの起源となる発生源の識別子。

オプション性：必須

形式／値

少なくとも監査される企業サイトＩＤの内のユニークな識別子テキストストリング

原理

このフィールドはイベントを特定の発生源システムに結びつける。それは、発生場所によりイベントのグループ化の分析ために使用されるかもしれない。

注

いくつかの構成では、負荷分散機能は処理を 2 つまたはそれ以上の重複サーバに配分する。 このようにしてこのフィールドに定義された値は特定の発生源システムというよりむしろサーバのグループのための発生源識別子であるとみなされるかもしれない。

5.4.3. 発生源タイプコードの監査

説明

イベントの起源となる発生源のタイプを識別するコード

オプション性：オプション

形式／値

コード化された一覧表であり、任意にシステム実装者により定義されるか、標準用語集で参照される。 定義されていないか、参照される場合、「コード」属性のデフォルト値は以下の通りである。

値	意味
1	エンドユーザーインターフェース
2	データ収集デバイスまたは端末
3	多層システムにおけるウェブサーバープロセス層
4	多層システムにおけるアプリケーションサーバー層
5	多層システムにおけるデータベースサーバー層
6	セキュリティサーバー、例）ドメインコントローラー
7	ISO level 1-3 ネットワークコンポーネント
8	ISO level 4-6 オペレーティングソフトウェア
9	外部発生源、または、その他

定義されたコードか標準の参照の実装のために、XML スキーマはこれらの任意の属性を定義する:

属性	値
CodeSystem	OID 参照
CodeSystemName	コーディングシステムの名前; ローカル定義コードの値を強く推奨する
DisplayName	ディスプレイやレポートの中で使われる値
OriginalText	コードに変換された入力値

発生源は 1 つ以上の方法で分類されるかもしれないので、指定された複数の値があるかもしれない。

原理

このフィールドは、どのタイプの発生源が発生源ＩＤによって特定されるかを示す。イベントが起こった発生源のタイプに従って分析の為に使われるイベントグループは任意の値かもしれない。

5.5. 関係オブジェクト識別

アクセスされたデータもしくはオブジェクトの特定のインスタンスを示すことにより、以下のデータが監査プロセスを補助する。

イベント識別の値を除いて、これらのデータは必須である。アクティブな関係者識別と監査元識別は監査可能なイベント全体を証明することができる。ヘルスケア組織のポリシーや規制に従ってこれらのデータが含まれる監査レコードの生成が行われたり、抑止されたりする。

イベントは１つ以上の関係オブジェクトを持つので、このグループは繰り返し型の値をとることができる。例えば、施設のポリシーと実装上の選択。

- ２つの関係者オブジェクト値のセットは医療記録番号と患者に対する特定のヘルスケアの発生や出来事で患者データへのアクセス確認をすることに使うことができる。

- 患者の関係者と患者の承認を受けた代理人は同時に識別される。

- 主治医と紹介先医師は同時に識別される。

- ワークリストで確認されるすべての患者は、識別される。

- 放射線検査において、受付番号や撮影番号により識別される一連の関係者オブジェクトが識別される。

注

それぞれの監査メッセージは、そのような関係者オブジェクトの関係の１つの使い方を立証するだけで、存在するかあるいは可能であるすべての関係を立証するものではない。

5.5.1.　関係するオブジェクトタイプコード

説明

監査された関係者オブジェクトタイプのコード。この値は、ユーザのロールや関係者オブジェクトに対するどんなユーザ関係とも区別される。

オプション性：オプション

形式／値

一覧：

値	意味
-----	----------

1　人
2　システムオブジェクト
3　組織
4　その他

原理

行為が行われるオブジェクトを記述するために、監査可能なイベントにおいて、行為の主題への照会を追加し、行為のオブジェクトタイプを問い合わせが可能であることも重要である。

5.5.2.　関係者オブジェクトコードの役割

説明

コードは監査された関係者オブジェクトの機能アプリケーションの役割を表す。

オプション性：オプション

形式／値

関係者オブジェクトタイプコードの一覧と仕様

値	意味	関係者オブジェクトタイプコード
1	患者	1－人
2	場所	3－組織
3	レポート	2－システムオブジェクト
4	情報源	1－人 3－組織
5	ﾏｽﾀﾌｧｲﾙ	2－システムオブジェクト
6	ユーザ	1－人 2－システムオブジェクト（人間のユーザではない）
7	リスト	2－システムオブジェクト
8	医師	1－人
9	署名者	3－組織
10	保証人	1－人 3－組織
11	ｾｷｭﾘﾃｨﾕｰｻﾞｴﾝﾃｨﾃｨ	1－人 2－システムオブジェクト

12：ｾｷｭﾘﾃｨﾕｰｻﾞｸﾞﾙｰﾌﾟ	2－システムオブジェクト
13：ｾｷｭﾘﾃｨ資源	2－システムオブジェクト
14：ｾｷｭﾘﾃｨ粒度定義	2－システムオブジェクト
15：ﾌﾟﾛﾊﾞｲﾀﾞｰ	1－人
	3－組織
16：ﾃﾞｰﾀ送付先	2－システムオブジェクト
17：ﾃﾞｰﾀ収納場所	2－システムオブジェクト
18：スケジュール	2－システムオブジェクト
19：顧客	3－組織
20：仕事	2－システムオブジェクト
21：仕事の流れ	2－システムオブジェクト
22：テーブル	2－システムオブジェクト
23：ルート基準	2－システムオブジェクト
24：検索	2－システムオブジェクト

ｾｷｭﾘﾃｨ資源は、抽象的な機密オブジェクトであり、画面、インターフェース、文書、プログラム等。監査ﾃﾞｰﾀｾｯﾄや収納先なども。

原理

詳細な監査分析のため、業務の役割に沿った関係者のより粒度の細かいタイプ表現をする必要がある。

5.5.4.　関係者オブジェクトＩＤのタイプコード

説明

関係者オブジェクトＩＤに含まれる識別子について記述する。

オプション性：　必須

形式/ 値

属性名“コード”を使用して、特定の関係者オブジェクトタイプコードへの対応付けを以下の一覧表で示す。下のコードはデフォルトである。

値	意味	関係者オブジェクトタイプコード
1	カルテ番号	1－人
2	患者番号	1－人
3	受付番号	1－人
4	登録番号	1－人
5	社会保障番号	1－人
6	会計番号	1－人
		3－組織
7	保証人番号	1－人
		3－組織
8	レポート名	1－組織
9	レポート番号	2－システムオブジェクト
10	検索基準	2－システムオブジェクト
11	ユーザーID	1－人
		2－システムオブジェクト
12	発生源識別形式(URI)	2－システムオブジェクト

セキュリティ管理のトリガーイベントは実行されたオブジェクトを識別するためにユーザ識別子とテキストベースの URI が使用される。

このコードは上に示されたようなデフォルトであり、それは実装上定義されたもの、または、HL7 バージョン 2.4 の 207 表や DICOM のメディアタイプという標準用語集を参照している。定義されたコードまたは標準を参照した実装に対して、XML スキーマは以下のオプションとなる属性を定義している。

属性	値
CodeSystem	OID 参照
CodeSystemName	コーディングシステム名；ローカルに定義された値をとることを強く推奨
DisplayName	ディスプレイ、レポートに使用される値
OriginalText	コードに変換された値

原理

関係者オブジェクトを同義的に識別する様々な識別子を区別する必要がある。

5.5.6.関係者オブジェクトＩＤ

説明

関係者オブジェクトの特定の物を識別する

オプション性：　必須

形式／値

文字列。関係者オブジェクトタイプコード と関係者オブジェクトＩＤタイプコードに依存する値の形式。

原理

このフィールドは、例えば患者の様な、一つのオブジェクトを識別する特定のもので、プライバシーやセキュリティ問題を探し追跡する。

注

これは、オブジェクトを識別する主要なユニーク識別キーで、そのため、実装に際しては合成データフィールドとなろう。

5.5.7.　関係者オブジェクト名

説明

監査された関係者オブジェクトＩＤを特定の実体として記述するもので、氏名の様なもの。

オプション性：オプション

形式／値
　文字列

原理
　このフィードは監査の際に問合せや報告の中で特定の人物を識別するために使われる。例えば、複数の同義の関係者オブジェクトＩＤ（患者番号、診療録番号、受付番号、その他）が使われる。

5.5.8.　関係者オブジェクト検索

説明
　検索タイプの関係者オブジェクトによる実際の検索

オプション性：　オプション

形式／値
　Base64 コード化データ

原理
　検索イベントでは、特定のイベントを識別するため、検索処理に実際に入力された値を把握することが必須であろう。それらの検索処理の実装とデータのコード化の差異のため、これは Base64 でコード化される。そのため、その後、監査データ分析処理によって、復号や翻訳がなされる。

5.5.9.　関係者オブジェクト詳細

説明
　特定のアクセス又は使用されたオブジェクトの詳細に関する実行定義データ。

オプション性：オプション

形式
　タイプと値の組合せ。“タイプ”の属性は実行定義の文字列。“値”の属性は Base64 コード化データ。

原理

特定の監査の遂行において、アクセスされたオブジェクトから特定の詳細情報や値が導出されることが望ましい。タイプと値の組合せにより、実行定義や局所的に拡張できるオブジェクトタイプ識別子や値の使用が可能となる。例えば、診療上の診断オブジェクトは多様な検査結果を含み、この要素はタイプや数字や結果のタイプを文書化する。

多数のデータのコード化がこの要素にはあり得る。従って、その値 Base64 のコードデータとなる。それは、その後、監査データ分析処理で、デコードまたは翻訳される。

付録 1：参考文献

（1） 個人情報の保護に関する法律

個人情報の適正な取扱いに関し、国及び地方公共団体の責務等を明らかにするとともに、個人情報を取り扱う事業者の遵守すべき義務等を定めることにより、個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする法律。平成 15 年 5 月 30 日に公布、平成 17 年 4 月 1 日より完全施行された。

（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ドライン

厚生労働省から平成 16 年 12 月 24 日に出されたガイドライン。上記個人情報保護法の対象となる病院、診療所、薬局、介護保険法に規定する居宅サービス事業を行う者等の事業者等が行う個人情報の適正な取扱いの確保に関する活動を支援するためのものであり、厚生労働大臣が法を執行する際の基準となるもの。

（3） 経済産業省「情報セキュリティ管理基準」（平成２０年改正版）

経済産業省から平成２０年に出された情報セキュリティマネジメントの基本的な枠組みと具体的な管理項目を規定した基準となるもの。効果的な情報セキュリティマネジメント体制を構築し、適切な管理策の整備と運用を行うための手本となる。なお、この管理基準は、日本国内の認証制度である ISMS 適合性評価制度における適合性評価の尺度と整合をとっている。

（4） 経済産業省「情報セキュリティ監査基準 ver1.0」

経済産業省から平成１５年に出された情報セキュリティ監査を行う際の指針となる基準を示すもの。「情報セキュリティ管理基準（平成２０年版）」と対になる基準として、監査人が監査上の判断の尺度として用いることが期待される。

付録 2：作成者名簿

作成者（五十音順）

石川　尊之　　（日本電気株式会社）
岡田　康　　（東芝住電医療情報システムズ株式会社）
島　成佳　　（日本電気株式会社）
西田　慎一郎　（株式会社島津製作所）
深尾　卓司　　（セコム株式会社）
松本　義和　　（サイバートラスト株式会社）
茗原　秀幸　　（三菱電機株式会社）

（JAHIS 標準 09-003）

2010 年 02 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
Ver1.1～

発行元 保健医療福祉システム工業会
〒105-0001 東京都港区虎ノ門 1 丁目 19－9
（虎ノ門 TB ビル 6F）
電話　03-3506-8010　　FAX　03-3506-8070