

PS3.15

DICOM PS3.15 2017c - セキュリティおよび システム管理プロファイル

Published by
National Electrical Manufacturers Association
1300 N. 17th Street
Rosslyn, Virginia 22209 USA

© Copyright 2017 by the National Electrical Manufacturers Association. All rights including translation into other languages, reserved under the Universal Copyright Convention, the Berne Convention for the Protection of Literacy and Artistic Works, and the International and Pan American Copyright Conventions.

Disclaimer 免責事項

DICOM is the worldwide Standard for medical imaging and related information. It is published and copyright by the National Electrical Manufacturers Association (NEMA). The normative DICOM Standard is published in English, and is available free on the official website at <http://dicom.nema.org/standard.html>.

This document is a translation prepared by the Japan Medical Imaging and Radiological Systems Industries Association (JIRA) under agreement with NEMA, with the intention to help Japanese readers understand the DICOM Standard more readily.

This translation represents a “best effort”; however, differences in meaning may exist between this translation and the normative DICOM Standard. Further, the DICOM Standard is under continuous maintenance and extension, so readers should expect that there are changes that are not reflected in this translation.

In the event of any difference between this translation and the DICOM Standard published in English by NEMA, the English version is normative and takes precedence.

Implementations shall claim conformance to the normative DICOM Standard. Users are advised to obtain the most current documents of the DICOM Standard directly from the official website.

DICOM は医用画像と関連する情報に関する国際標準規格です。DICOM 規格は米国電機工業会（NEMA）が発行し著作権を有します。DICOM 規格の規範文書は英語で出版され、公式サイト <http://dicom.nema.org/standard.html> から無償でダウンロードが可能です。

この文書は日本語を好む読者がDICOM 規格をより容易に理解するための手助けを意図して、NEMA の許可を得て一般社団法人日本画像医療システム工業会（JIRA）が提供する翻訳です。

この翻訳は最善の努力を以て提供されていますが、この翻訳と規範DICOM 規格の間に意味の違いが存在するかもしれません。更に、DICOM 規格は継続的な保守と拡張が施されているので、読者はこの翻訳に反映されていない変更が存在することに留意する必要があります。

この翻訳とNEMA が発行する英語版のDICOM 規格との間に差が生じた場合は、英語版が規範であり優先します。

実装は規範DICOM 規格への適合性を宣言しなければなりません。使用者はDICOM 規格の最新の文書を公式サイトから直接入手することが要望されます。

注意と免責事項

この出版物に含まれる情報は、それを開発していた時点において、文書の開発や承認に従事していた人々の合意および文書の承認によって技術的に理にかなっていると考えられた。合意とはこの文書の開発に参加したすべての人の間で満場一致があることを必ずしも意味しない。

NEMA 規格および指針出版物は、ここに含まれている文書はその一つであるが、自発的に合意された規格開発手続きに従って開発される。このプロセスは有志者を集めて、そして / または、この出版によってカバーされる論題に関心を持つ人々の見解を捜し出す。NEMA は手続きを管理し、合意の開発における公平さを推進する規則を確立しているが、NEMA は文書を執筆しない、またその規格および指針出版物に含まれている任意の情報の正確さまたは完全性、あるいは任意の判断についての正当性を、独自に試験、評価、または検証しない。

NEMA は、特別か、間接か、重大か、補償かにかかわらず、この文書の出版、使用、応用、あるいは信頼に、直接あるいは間接的に起因する、いかなる性質のいかなる身体傷害、財産あるいは他の損害に対する責任を放棄する。NEMA は、明示的か暗黙的かを問わず、ここに出版されるすべての情報の正確さあるいは完全性に関して責任を放棄し保証しない、またこの文書の中の情報が読者の特定の目的あるいはニーズを満たすことに関して責任を放棄し、保証をしない。NEMA は、この規格または指針による、個々の製造業者あるいは販売業者の製品またはサービスの性能を保証することを引き受けない。

この文書を出版し利用可能にするにあたって、NEMA は、任意の個人あるいは団体のために、あるいはそれらに代わって、専門または他のサービスを与えることを引き受けない、または、NEMA は、任意の個人あるいは組織によって誰か他の人に負わされたいかなる義務も引き受けない。この文書を使用する人は誰でも、自分自身の独立した判断に頼るべきである、または必要に応じて、与えられる環境における合理的な行為の決定において有能な専門家の助言を求めべきである。この出版物によってカバーされたテーマに関する情報と他の規格は、他の情報源から入手可能なことがある、そして利用者は、この出版によってカバーされない追加の見解あるいは情報に関してその情報源を調べたいと思うかもしれない。

NEMA はこの文書の内容への遵守を監視する力または強制する力をもっていないし、それを引き受けない。NEMA は安全あるいは健康目的のために、製品、設計または設置を、認証、試験、または検査しない。この文書中のいかなる健康あるいは安全関連情報への遵守に関するいかなる証明書あるいは他の宣言書も、NEMA に帰することはなく、そしてそれはたまたま宣言書の証明者または製造業者の責任である。

PS3.15: DICOM PS3.15 2017c - セキュリティおよびシステム管理プロファイル

Copyright © 2017 NEMA

目次

注意と免責条項	13#
まえがき	15#
1# 適用範囲と適用分野	17#
1.1# セキュリティ方針およびメカニズム	17#
1.2# システム管理プロファイル	17#
2# 引用規格	19#
3# 定義	21#
3.1# 参照モデル定義	21#
3.2# 参照モデルセキュリティアーキテクチャ定義	21#
3.3# ACSE サービス定義	21#
3.4# セキュリティ定義	21#
3.5# DICOM 序文と概要定義	22#
3.6# DICOM 適合性定義	22#
3.7# DICOM 情報オブジェクト定義	22#
3.8# DICOM サービスクラス定義	22#
3.9# DICOM 通信サポート定義	22#
3.10# DICOM セキュリティプロファイル定義	22#
4# 記号と省略形	23#
5# 規約	25#
6# セキュリティおよびシステム管理プロファイルの概要	27#
6.1# セキュア使用プロファイル	27#
6.2# セキュアトランスポートコネクションプロファイル	27#
6.3# デジタル署名プロファイル	27#
6.4# 媒体保存セキュリティプロファイル	28#
6.5# ネットワークアドレス管理プロファイル	28#
6.6# 時間同期プロファイル	28#
6.7# アプリケーション構成管理プロファイル	28#
6.8# 監査証跡プロファイル	28#
7# 構成プロファイル	31#
7.1# アクタ	32#
7.2# トランザクション	32#
A# セキュア使用プロファイル（規格）	35#
A.1# オンライン電子保存セキュア使用プロファイル	35#
A.1.1# SOP インスタンス状態	35#
A.2# 基本デジタル署名セキュア使用プロファイル	36#
A.3# ビット保存デジタル署名セキュア使用プロファイル	37#
A.4# 基礎的 SR デジタル署名セキュア使用プロファイル	37#
A.5# 監査証跡メッセージフォーマットプロファイル	37#
A.5.1# DICOM 監査メッセージスキーマ	38#
A.5.1.1# 監査メッセージスキーマ	38#
A.5.1.2# スキーマ内で使用するコード	42#
A.5.1.2.1# Audit Source Type Code	42#
A.5.1.2.2# Participant Object Type Code Role	42#
A.5.1.2.3# Participant Object Data Life Cycle	43#
A.5.1.2.4# Participant Object ID Type Code	44#
A.5.2# 一般的なメッセージフォーマット規約	44#
A.5.2.1# UserID	48#
A.5.2.2# AlternativeUserID	48#
A.5.2.3# Username	49#
A.5.2.4# Multi-homed Nodes	49#
A.5.2.5# EventDateTime	49#
A.5.2.6# ParticipantObjectTypeCodeRole	49#
A.5.3# DICOM 固有の監査メッセージ	50#
A.5.3.1# アプリケーション活動	51#
A.5.3.2# 監査ログの使用	51#
A.5.3.3# DICOM インスタンスの転送を開始する	52#

A.5.3.4#	データの書き出し	54#
A.5.3.4.1#	UserIsRequestor	56#
A.5.3.5#	データの読み込み	56#
A.5.3.6#	アクセスされた DICOM インスタンス	58#
A.5.3.7#	転送された DICOM インスタンス	59#
A.5.3.8#	削除された DICOM スタディ	61#
A.5.3.9#	ネットワークエントリ	62#
A.5.3.10#	問い合わせ	63#
A.5.3.11#	セキュリティアラート	64#
A.5.3.12#	ユーザー認証	66#
A.5.3.13#	オーダーレコード	67#
A.5.3.14#	患者レコード	68#
A.5.3.15#	手続きレコード	69#
A.6#	監査証跡メッセージ送信プロファイル—SYSLOG-TLS	70#
A.7#	監査証跡メッセージ送信プロファイル—SYSLOG-UDP	71#
B#	セキュアトランスポートコネクションプロファイル (規格)	73#
B.1#	基本 TLS セキュアトランスポートコネクションプロファイル	73#
B.2#	ISCL セキュアトランスポートコネクションプロファイル	73#
B.3#	AES の TLS セキュアトランスポート接続プロファイル	74#
B.4#	基礎的ユーザーID アソシエーションプロファイル	75#
B.5#	ユーザーID プラス パスワードアソシエーションプロファイル	75#
B.6#	ケルベロス ID 折衝アソシエーションプロファイル	76#
B.7#	統合 SAML アサーション ID 折衝アソシエーションプロファイル	76#
B.8#	電子メールトランスポートのセキュア使用	76#
C#	デジタル署名プロファイル (規格)	79#
C.1#	基本 RSA デジタル署名プロファイル	79#
C.2#	作成者 RSA デジタル署名プロファイル	79#
C.3#	認可 RSA デジタル署名プロファイル	80#
C.4#	構造化レポート RSA デジタル署名プロファイル	81#
D#	媒体保存セキュリティプロファイル (規格)	83#
D.1#	基本 DICOM 媒体セキュリティプロファイル	83#
D.1.1#	セキュア DICOM ファイルの中の DICOM ファイルのカプセル化	83#
E#	属性機密性プロファイル	85#
E.1#	アプリケーションレベル機密性プロファイル	85#
E.1.1#	匿名化(De-identifier)	85#
E.1.2#	再識別化(Re-identifier)	103#
E.1.3#	適合要求事項	103#
E.2#	基礎アプリケーションレベル機密性プロファイル	104#
E.3#	基礎アプリケーションレベル機密性オプション	104#
E.3.1#	ピクセルデータ消去オプション	105#
E.3.2#	認識視覚特徴消去オプション	105#
E.3.3#	グラフィックス消去オプション	106#
E.3.4#	構造化内容消去オプション	106#
E.3.5#	ディスクリプタ消去オプション	107#
E.3.6#	保持経時時間情報オプション	107#
E.3.7#	保持患者特性オプション	108#
E.3.8#	保持装置識別オプション	108#
E.3.9#	保持 UID オプション	109#
E.3.10#	保持安全個人オプション	109#
F#	ネットワークアドレス管理プロファイル	115#
F.1#	基本ネットワークアドレス管理プロファイル	115#
F.1.1#	ホスト名を解決する	115#
F.1.1.1#	適用範囲	115#
F.1.1.2#	ユースケース/役割	115#
F.1.1.3#	参照される標準	116#
F.1.1.4#	DNS セキュリティ考察 (参考)	116#
F.1.1.5#	DNS 実装考察 (参考)	117#
F.1.1.6#	サービス発見の支援	117#

F.1.2# DHCP サーバを構成する	117#
F.1.2.1# 適用範囲	117#
F.1.2.2# ユースケース/役割	117#
F.1.2.3# 参照される標準	118#
F.1.3# DHCP サーバを見つけて使用する	118#
F.1.3.1# 適用範囲	118#
F.1.3.2# ユースケース/役割	118#
F.1.3.3# 参照される標準	118#
F.1.3.4# 相互作用図	119#
F.1.4# リースを維持する	120#
F.1.4.1# 適用範囲	120#
F.1.4.2# ユースケース/役割	120#
F.1.4.3# 参照される標準	120#
F.1.4.4# 正常な相互作用	120#
F.1.5# DDNS 協調	120#
F.1.5.1# 適用範囲	120#
F.1.5.2# ユースケース/役割	121#
F.1.5.3# 参照される標準	121#
F.1.5.4# イベントの基礎コース	121#
F.1.6# DHCP セキュリティ考察 (参考)	121#
F.1.7# DHCP 実装考察 (参考)	122#
F.1.8# 適合	122#
G# 時間同期プロファイル	123#
G.1# 基本時間同期プロファイル	123#
G.1.1# NTP サーバを見つける	123#
G.1.1.1# 適用範囲	123#
G.1.1.2# ユースケース/役割	124#
G.1.1.3# 参照される標準	124#
G.1.1.4# イベントの基礎コース	124#
G.1.1.5# 代替パス	124#
G.1.1.6# 仮定	124#
G.1.1.7# 事後条件	125#
G.1.2# 時間を維持する	125#
G.1.2.1# 適用範囲	125#
G.1.2.2# ユースケース/役割	125#
G.1.2.3# 参照される標準	125#
G.1.2.4# イベントの基礎コース	125#
G.1.3# NTP セキュリティ考察 (参考)	125#
G.1.4# NTP 実装考察 (参考)	126#
G.1.5# 適合	126#
H# アプリケーション構成管理プロファイル	127#
H.1# アプリケーション構成管理プロファイル	127#
H.1.1# データモデルコンポーネントオブジェクト	127#
H.1.1.1# 装置	128#
H.1.1.2# ネットワークアプリケーションエンティティ	129#
H.1.1.3# ネットワーク接続	130#
H.1.1.4# 転送能力	131#
H.1.1.5# DICOM 構成ルート	131#
H.1.1.6# 装置ルート	132#
H.1.1.7# 一意的 AE タイトル登録簿ルート	132#
H.1.1.8# 一意的 AE タイトル	132#
H.1.2# アプリケーション構成データモデル階層	133#
H.1.3# オブジェクトおよび属性用の LDAP スキーマ	134#
H.1.4# トランザクション	147#
H.1.4.1# LDAP サーバを見つける	147#
H.1.4.1.1# 適用範囲	147#
H.1.4.1.2# ユースケース/役割	147#
H.1.4.1.3# 参照される標準	147#

H.1.4.1.4# 相互作用図.....	147#
H.1.4.1.5# 代替パス.....	148#
H.1.4.2# LDAP サーバを問い合わせる.....	148#
H.1.4.2.1# 適用範囲.....	148#
H.1.4.2.2# ユースケース/役割.....	148#
H.1.4.2.3# 参照される標準.....	148#
H.1.4.2.4# 相互作用記述.....	148#
H.1.4.3# LDAP サーバを更新する.....	149#
H.1.4.3.1# 適用範囲.....	149#
H.1.4.3.2# ユースケース/役割.....	149#
H.1.4.3.3# 参照される標準.....	149#
H.1.4.3.4# 相互作用記述.....	149#
H.1.4.3.5# ネットワーク AE 生成のための特別更新.....	149#
H.1.4.4# LDAP サーバを維持する.....	150#
H.1.5# LDAP セキュリティ考察 (参考).....	150#
H.1.5.1# 脅威の評価.....	150#
H.1.5.2# 利用可能な LDAP セキュリティメカニズム.....	151#
H.1.5.3# 推奨 (参考).....	151#
H.1.6# 実装考察 (参考).....	152#
H.1.7# 適合.....	152#
H.2# DNS サービス発見.....	152#
H.2.1# 適用範囲.....	152#
H.2.2# ユースケース/役割.....	153#
H.2.3# 参照される標準.....	153#
H.2.4# 例.....	154#

図一覧

7-1. トランザクションおよびアクタ	34#
F.1-1. ホスト名を解決する	115#
F.1-2. DNS 参照標準	116#
F.1-3. DHCP サーバを構成する	117#
F.1-4. DHCP サーバを見つけて使用する	118#
F.1-5. DHCP 相互作用	119#
F.1-6. リースを維持する	120#
F.1-7. DDNS 協調	121#
G.1-1. NTP サーバを見つける	124#
G.2-1. 時間を維持する	125#
H.1-1. アプリケーション構成データモデル	127#
H.1-2. DICOM 構成階層	133#
H.1-3. LDAP サーバを見つける	147#
H.1-4. LDAP サーバを選ぶ	147#
H.1-5. LDAP サーバを問い合わせる	148#
H.1-6. LDAP サーバを更新する	149#
H.2-1. Find DICOM サービス	153#

表一覧

A.5.1.2.1-1. Audit Source Type Code の値	42#
A.5.1.2.2-1. Participant Object Type Code Roles	42#
A.5.1.2.3-1. Participant Object Data Life Cycle の値	43#
A.5.1.2.4-1. Participant Object ID Type Code の値	44#
A.5.2-1. 一般的なメッセージフォーマット	45#
A.5.2.6-1. ParticipantObjectTypeCodeRole	49#
A.5.3.1-1. アプリケーション活動メッセージ	51#
A.5.3.2-1. 監査ログ使用のメッセージ	52#
A.5.3.3-1. DICOM インスタンスの転送を開始するための監査メッセージ	53#
A.5.3.4-1. データ書き出しのための監査メッセージ	54#
A.5.3.5-1. データ読み込みのための監査メッセージ	56#
A.5.3.6-1. DICOM インスタンスへのアクセスのための監査メッセージ	58#
A.5.3.7-1. DICOM インスタンスの転送のための監査メッセージ	59#
A.5.3.8-1. DICOM スタディの削除のための監査メッセージ	61#
A.5.3.9-1. ネットワークエントリのための監査メッセージ	62#
A.5.3.10-1. 問い合わせのための監査メッセージ	63#
A.5.3.11-1. セキュリティアラートのための監査メッセージ	65#
A.5.3.12-1. ユーザー認証のための監査メッセージ	66#
A.5.3.13-1. オーダーレコードのための監査メッセージ	67#
A.5.3.14-1. 患者レコードのための監査メッセージ	68#
A.5.3.15-1. 手続きレコードのための監査メッセージ	69#
B.1-1. TLS 機能のための最小メカニズム	73#
B.2-1. ISCL 機能のための最小メカニズム	74#
B.3-1. TLS 機能のための最小メカニズム	74#
B.4-1. DICOM アソシエーション折衝機能のための最小メカニズム- 基礎的ユーザーID アソシエーションプロファイル	75#
B.5-1. ユーザーID プラス パスコードアソシエーションプロファイル -DICOM アソシエーション折衝機能のための最小メカニズム	76#
B.6-1. ケルベロス ID 折衝アソシエーションプロファイル -DICOM アソシエーション折衝機能のための最小メカニズム	76#
B.7-1. 統合 SAML アサーション ID 折衝アソシエーションプロファイル - DICOM アソシエーション折衝機能のための最小メカニズム	76#
E.1-1. アプリケーションレベル機密性プロファイル属性	89#
E.3.10-1. 安全なプライベート属性	110#
F.1-1. 基本ネットワークアドレス管理プロファイル	115#
F.1-2. DHCP パラメータ	119#
G.1-1. 基本時間同期プロファイル	123#
H.1-1. アプリケーション構成管理プロファイル	127#
H.1-2. 装置オブジェクトの属性	128#
H.1-3. 装置オブジェクトの子オブジェクト	129#
H.1-4. ネットワーク AE オブジェクトの属性	129#
H.1-5. ネットワーク AE オブジェクトの子オブジェクト	130#
H.1-6. ネットワーク接続オブジェクトの属性	130#
H.1-7. 転送能力オブジェクトの属性	131#
H.1-8. DICOM 構成ルートオブジェクトの属性	131#
H.1-9. DICOM 構成ルートオブジェクトの子オブジェクト	132#
H.1-10. 装置ルートオブジェクトの属性	132#
H.1-11. 装置ルートオブジェクトの子オブジェクト	132#
H.1-12. 一意的 AE タイトル登録簿ルートオブジェクトの属性	132#
H.1-13. 一意的 AE タイトル登録簿ルートオブジェクトの子オブジェクト	132#
H.1-14. 一意的 AE タイトルオブジェクトの属性	132#
H.1-15. LDAP セキュリティパターン	151#

注意と免責条項

この出版物での情報は、開発当時は、文書の開発および承認に従事していた人のコンセンサスによって技術的に正常であると考えられた。コンセンサスは、この文書の開発に参加するすべての人による満場一致を必ずしも意味しない。

NEMA 規格およびガイドライン出版物は、自発的なコンセンサス規格開発プロセスを通じて開発されている。本書もその一つである。このプロセスではボランティアを集め、この出版物の対象となるトピックに関心をもつ人の見解を求める。NEMA は手続きを管理し、合意の開発における公平さを推進する規則を確立しているが、NEMA は文書を執筆しない、またその規格および指針出版物に含まれている任意の情報の正確さまたは完全性、あるいは任意の判断についての正当性を、独自に試験、評価、または検証しない。

NEMA は、特別、間接、必然か補償にかかわらず、直接的または間接的にこの出版物、この文書の使用、適用または依存に起因する身体傷害、財産または他の損害に対し免責とする。NEMA は、明示的か暗黙的かを問わず、ここに出版された情報の正確さと完全性について免責とし保証はしない。またこの文書中の情報が読者の特定の目的またはニーズを満たすことは免責とし保証はしない。NEMA は、個々のメーカーまたは販売業者の製品または役務の性能を、この規格またはガイドにより保証することを試みない。

この文書を出版し利用可能にする際に、NEMA は、個人または組織のために、またはそれらを代表して専門的その他の役務を与えることを試みていない。また NEMA は個人または組織が他の者に対し負う義務を行うものではない。この文書を使用する人は誰でも、自分自身の判断に頼るべきである。または、適切な場合、所定のコンテキストでの合理的な行為を決定する際に有能な専門家に対し助言を求めるべきである。この出版物の対象のトピックについての情報および他の規格は、他の情報源から入手できることがある。この出版物の対象でない追加の見解または情報を求めて、ユーザーは他の情報源を調べる必要がある。

NEMA はこの文書の内容への適合を監視または強制する権限をもっていない。NEMA は安全または健康の目的のために、製品、設計または設置を認証しないし、試験しないし、または検査しない。この文書の健康または安全関連の情報への適合の認証または他の言明は、いかなるものにも NEMA は免責とし、その言明を認証し実行した者が全責任を負う。

まえがき

この DICOM 規格は、DICOM 規格委員会の手続きに従って開発された。

DICOM 規格は、[ISO/IEC Directives, Part 2]に確立された指針を用いた複数の巻の文書として構成される。

DICOM® は National Electrical Manufacturers Association (NEMA) の医療情報のデジタル通信に関する規格文献のための登録商標であり、不許複製・禁無断転載である。

HL7® および CDA® は Health Level Seven International の登録商標である。不許複製・禁無断転載。

SNOMED®, SNOMED Clinical Terms®, SNOMED CT® は International Health Terminology Standards Development Organisation (IHTSDO)の登録商標である。不許複製・禁無断転載。

LOINC® は Regenstrief Institute, Inc.の登録商標である。不許複製・禁無断転載。

1 適用範囲と適用分野

DICOM 規格のこの巻は実装が適合性を主張することがあるセキュリティおよびシステム管理プロファイルを明記する。セキュリティおよびシステム管理プロファイルは、TLS、ISCL、DHCP および LDAP などの、外部で開発された規格プロトコルを参照し、DICOM 規格プロトコルを情報の相互交換に使用するシステムにおいてこれらを使用することを配慮しながら定義されている。

1.1 セキュリティ方針およびメカニズム

DICOM 規格はセキュリティ方針の問題に対処してないが、セキュリティのレベルに応じて適切なセキュリティ方針を遵守する必要なことは明らかである。規格は、応用エンティティ間の DICOM オブジェクトの相互交換に関するセキュリティ方針を実装するために使用できるメカニズムを単に提供する。例えば、セキュリティ方針は、アクセス制御のある水準を指示することがある。この規格はアクセス制御方針を考慮しないが、関与した応用エンティティに対してアクセス制御方針を実装するための十分な情報を交換するための技術的手段を提供する。

この規格は、DICOM 相互交換に関与する応用エンティティが、アクセス制御、監査証跡、物理的保護、データの機密性と完全性の維持、および利用者とデータにアクセスする彼らの権利を識別するメカニズムを含むが、しかしそれらに制限されないで、適切なセキュリティ方針を実装していると仮定する。本質的に、各応用エンティティは、他の応用エンティティとのセキュア通信を試みる前に彼ら自身の局所環境が安全であると保証しなければならない。

応用エンティティがアソシエーション折衝によって DICOM 経由で情報を相互交換することに合意する場合、それらは本質的に、他の応用エンティティにおける信用の何らかの水準に同意している。元来、応用エンティティは、彼らの通信相手が彼らの管理下でデータの機密性と完全性を維持するだろうと期待する。もちろん、信頼のそのレベルは局所的なセキュリティおよびアクセス制御方針によって指示されることがある。

応用エンティティは、それらが他の応用エンティティと通信する通信路を信頼しないことがある。したがって、この規格は、応用エンティティに対して、安全に互いを認証するための、交換されたメッセージへの任意の改ざんまたは変造を検知するための、または、通信チャンネルを通過するときにそれらのメッセージの機密性を保護するためのメカニズムを提供する。応用エンティティは、彼らが通信チャンネルに置く信頼の水準に依存して、自由にこれらのメカニズムの何れかを利用できる。

この規格は、応用エンティティが応用エンティティの局所利用者、およびその利用者の役割またはライセンスを安全に識別できると仮定する。利用者が人である場合、または、組織または数台の装置のような抽象的エンティティである場合があることに注意すること。応用エンティティが DICOM 経由で情報の交換に同意する場合、さらに、それらは、セキュア通信路をセットする際に交換される証明書によって応用エンティティの利用者に関する情報を交換することがある。その後、応用エンティティは、アクセス制御方針を実装する際に、または監査証跡を作成する際に、局所または遠隔の利用者に関する証明書に含まれる情報を考慮することがある。

さらにこの規格は、情報の「所有者」（例えば、患者、施設）が特定利用者、または情報にアクセスする利用者の特定クラスに権限を与えたかどうかを決定する手段を、応用エンティティがもっていると仮定する。さらにこの規格は、応用エンティティによって提供されるアクセス制御の中でそのような許可が考慮されることがあると仮定する。現時点では、この規格は、そのような許可を応用エンティティ間で通信する方法は考慮されていないが、これは将来の検討の対象となるかもしれない。

さらにこの規格は、TLS を使用する応用エンティティが、応用エンティティの利用者のための X.509 鍵証明書にセキュアなアクセスを有するか、または安全に得ることができることを前提とする。さらにこの規格は、応用エンティティが受け取る X.509 証明書を検証する手段をもっていることを前提とする。検証メカニズムは局所的に管理された管理局、公に利用可能な管理局または何らかの信頼された第三者を使用することがある。

この規格は、ISCL を使用する応用エンティティが適切な鍵管理および配布メカニズム（例えばスマートカード）にアクセスすることを前提とする。そのような鍵管理と配布メカニズムの性質と使用は、特定現場で使用されるセキュリティ方針の一部である可能性があるけれども、DICOM の適用範囲外である。

1.2 システム管理プロファイル

この巻で指定されたシステム管理プロファイルは、構成管理プロセスのオートメーションをサポートすることを目指している。このプロセスは、DICOM 規格プロトコルを情報交換に使用するシステムを操作するのに必要である。

この巻は、応用エンティティが、複雑さの異なる様々なネットワーク環境の中で作動するかもしれないと仮定する。これらの環境の範囲は、孤立ネットワーク上で作動する少数のユニットに始まり、限定的な中央集中ネットワークサポート活動を備えたデパートメントレベルネットワークがあり、さらに十分なネットワーク管理サービスを備えた企業レベルネットワークまでの範囲に及ぶ。

かもしれない。システム管理プロファイルは、一般に、実装に対してアドレスされるが、応用エンティティにはアドレスされないことに注意。同じプロファイルが、ネットワーク上の異なる応用によってサポートされる必要がある。

2 引用規格

次の規格は、このテキストの中で引用することによって、この規格の規定を構成する規定を含む。出版の時点で、示された版は有効であった。全ての規格は改訂の対象であり、この規格に基づいた協定の当事者は次に示した規格の最新の版を適用する可能性について調査することを推奨される。

[ISO/IEC Directives, Part 2] ISO/IEC.2016/05. 7.0. *国際規格の構成および作成の規則*
http://www.iec.ch/members_experts/refdocs/iec/isoiecdir-2%7Bed7.0%7Den.pdf .

ANSI X9.52 American National Standards Institute. ANSI X9.52-1998, Triple Data Encryption Algorithm Modes of Operation. 1998.

ECMA 235, The ECMA GSS-API Mechanism

FIPS PUB 46 Data Encryption Standard

FIPS PUB 81 DES Modes of Operation

IETF Internet X.509 Public Key Infrastructure; Time Stamp Protocols; March 2000

ISO/IEC 10118-3:1998 Information technology - Security techniques - Hash-functions - Part 3: Dedicated hash-functions (RIPEMD-160 reference)

注：草案の RIPEMD-160 仕様およびサンプルコードは右記からも入手可能。 <ftp://ftp.esat.kuleuven.ac.be/pub/bosselaer/ripemd>

ISO 7498-1, Information Processing Systems - Open Systems Interconnection - Basic Reference Model

ISO 7498-2, Information processing systems - Open Systems Interconnection - Basic reference Model - Part 2: Security Architecture

ISO/TR 8509, Information Processing Systems - Open Systems Interconnection - Service Conventions

ISO 8649:1987, Information Processing Systems - Open Systems Interconnection - Service Definition for the Association Control Service Element

Integrated Secure Communication Layer V1.00 MEDIS-DC

ITU-T Recommendation X.509 (03/00) "Information technology - Open Systems Interconnection - The directory: Public-key and attribute certificate frameworks"

注

ITU-T Recommendation X.509 は ISO/IEC 9594-8 1990 に類似している。しかしながら ITU-T recommendation はよりよく知られている形式であり、また 1993 と 2000、2 組の補正を含めて 2001 に改訂された。ITU-T は、以前は CCITT として知られていた。

RFC1035 Domain Name System (DNS)

RFC1305 Network Time Protocol (Version 3) Specification, Implementation

RFC2030 Simple Network Time Protocol (SNTP) Version 4

RFC2131 Dynamic Host Configuration Protocol

RFC2132 Dynamic Host Configuration Protocol Options

RFC2136 Dynamic Updates in the Domain Name System (DNS UPDATE)

RFC2181 Clarifications to the DNS Specification

RFC2219 Use of DNS Aliases for Network Services

RFC2246, Transport Layer Security (TLS) 1.0 Internet Engineering Task Force

注

TLS は SSL 3.0 に由来し、それと大部分は互換性をもつ。

RFC2251 Lightweight Directory Access Protocol (v3)

RFC2313 PKCS #1: RSA Encryption, Version 1.5, March 1998.

RFC2563 DHCP Option to Disable Stateless Auto-Configuration in IPv4 Clients

RFC2782 A DNS RR for specifying the location of services (DNS SRV)

RFC2849 The LDAP Data Interchange Format (LDIF)

RFC2898 PKCS #5: Password-Based Cryptography Specification Version 2.0, September 2000

RFC3211 Password-based Encryption for CMS, December 2001

RFC3268 Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS), June 2002.

RFC3447 PKCS #1 RSA Cryptography Specifications Version 2.1, February 2003

注

RSA Encryption Standard は ISO/IEC 9796 の Informative Annex A (付属書 (参考)) および CEN/TC251 European Prestandard prENV 12388:1996 の Normative Annex A (付属書 (規定)) に同様に定義されている。

RFC3852 Cryptographic Message Syntax, July 2004

RFC3370 Cryptographic Message Syntax (CMS) Algorithms, August 2002

RFC3565 Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS), July 2003

SHA-1 National Institute of Standards and Technology, FIPS Pub 180-1: Secure Hash Standard, 17 April 1995

SHA-2 National Institute of Standards and Technology, FIPS Pub 180-2: Secure Hash Standard, 1 August 2002

RFC3851 Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification

RFC3853 S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP)

RFC5424 The Syslog Protocol

RFC5425 Transport Layer Security (TLS) Transport Mapping for Syslog

RFC5426 Transmission of Syslog Messages over UDP

注

規定の RFC は、しばしばその後の RFC の発行によって更新される。オリジナルの旧 RFC は、新しい RFC への参照を含めるために修正されない。

3 定義

この規格の目的のために、次の定義が適用される。

3.1 参照モデル定義

規格のこの巻は、ISO 7498-1の中で定義された次の用語を使用する：

- a. 応用エンティティ Application Entity
- b. プロトコルデータ単位または層プロトコルデータ単位 Protocol Data Unit or Layer Protocol Data Unit
- c. トランスポートコネクション Transport Connection

3.2 参照モデルセキュリティアーキテクチャ定義

規格のこの巻は、ISO 7498-2の中で定義された次の用語を使用する：

- a. データ機密性 Data Confidentiality

注

定義は、「情報が、利用可能にならないか、権限外の個人、エンティティ、またはトランザクションに開示されない特性」である。

- b. データ発信元認証 Data Origin Authentication

注

定義は「受信データの発信元が主張されたとおりである認証」である。

- c. データ完全性 Data Integrity

注

定義は「データが無許可の方法で変更されなかったか破壊されなかったという特性」である。

- d. かぎ管理 Key Management

注

定義は「セキュリティ方針に従ったかぎの作成および保存、配布、削除、保管、応用」である。

- e. デジタル署名 Digital Signature

注

定義は、「データ単位の受け取り人がその単位の発信元および完全性を証明することと、偽造に対して保護することとを可能にするところの、例えば受け取り人によって、データ単位に追加されたデータ、またはデータ単位の暗号変換」である。

3.3 ACSE サービス定義

規格のこの巻は、ISO 8649の中で定義された次の用語を使用する：

- a. アソシエーションまたは応用アソシエーション Association or Application Association

3.4 セキュリティ定義

規格のこの巻は、ECMA 235の中で定義された次の用語を使用する：

- a. セキュリティコンテキスト Security Context

注

定義は「形成したか、形成することを試みている起動側または受動側へのセキュリティアソシエーションを代表するセキュリティ情報」である

3.5 DICOM 序文と概要定義

規格のこの巻は、PS 3.1 の中で定義された次の用語を使用する：

- a. 属性 Attribute

3.6 DICOM 適合性定義

規格のこの巻は、PS 3.2 の中で定義された次の用語を使用する：

- a. セキュリティプロファイル Security Profile

3.7 DICOM 情報オブジェクト定義

規格のこの巻は、PS 3.3 の中で定義された次の用語を使用する：

- a. モジュール Module

3.8 DICOM サービスクラス定義

規格のこの巻は、PS3.4 の中で定義された次の用語を使用する：

- a. サービスクラス Service Class
b. サービス - オブジェクト対 (SOP) インスタンス Service-Object Pair (SOP) Instance

3.9 DICOM 通信サポート定義

規格のこの巻は、PS3.8 の中で定義された次の用語を使用する：

- a. DICOM 上位層 DICOM Upper Layer

3.10 DICOM セキュリティプロファイル定義

次の定義は、DICOM 規格のこの巻の中で一般に使用される：

セキュアトランスポートコネクション	Secure Transport Connection 改ざん、盗聴、擬装からの保護の何らかの水準を提供するトランスポートコネクション。
メッセージ認証コード	Message Authentication Code データ要素の部分集合に由来したダイジェストまたはハッシュコード。
証明書 Certificate	当事者とその当事者の公開暗号アルゴリズムおよびパラメータ、かぎを識別する電子文書。証明書は、その他の物の中に、証明書を作成したエンティティからの識別 (identity) とデジタル署名を含む。証明書の内容および書式は ITU-T Recommendation X.509 によって定義される。

4 記号と省略形

次の記号および省略形が、規格のこの巻の中で使用される。

ACR	American College of Radiology
AE	Application Entity
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CEN TC251	Comite European de Normalisation-Technical Committee 251-Medical Informatics
CBC	Cipher Block Chaining
CCIR	Consultative Committee, International Radio
CN	Common Name
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DICOM	Digital Imaging and Communications in Medicine
DN	Distinguished Name
DNS	Domain Name System
DDNS	Dynamic Domain Name System
ECMA	European Computer Manufacturers Association
EDE	Encrypt-Decrypt-Encrypt
HL7	Health Level 7
IEC	International Electrical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IOD	Information Object Definition
ISCL	Integrated Secure Communication Layer
ISO	International Standards Organization
JIRA	Japan Medical Imaging and Radiological Systems Industries Association
LDAP	Lightweight Directory Access Protocol
LDIF	LDAP Interchange Format
MAC	Message Authentication Code
MD-5	Message Digest - 5
MEDIS-DC	Medical Information System Development Center
MTU	Maximum Transmission Unit
NEMA	National Electrical Manufacturers Association
NTP	Network Time Protocol

OID	Object Identifier (analogous to UID)
PDU	Protocol Data Unit
RDN	Relative Distinguished Name
RFC	Request For Comment (used for standards issued by the IETF)
RR	Resource Record (when used in the context of DNS)
RSA	Rivest-Shamir-Adleman
SCP	Service Class Provider
SCU	Service Class User
SHA	Secure Hash Algorithm
SNTP	Simple Network Time Protocol
SOP	Service-Object Pair
SSH	Secure Shell
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UID	Unique Identifier
UTC	Universal Coordinated Time

5 規約

セクション 3 の定義の中で記載された用語は文書の全体にわたって大文字で書かれる。

6 セキュリティおよびシステム管理プロファイルの概要

実装は、セキュリティおよびシステム管理プロファイルのどれに対しても適合を個々に主張することがある。さらにそれは、2 つ以上のセキュリティまたはシステム管理プロファイルへの適合を主張することがある。それはその適合性宣言の中で、与えられたトランザクションに対してそれがプロファイルをどのように選択するかを示す。

6.1 セキュア使用プロファイル

実装は、1 つ以上のセキュア使用プロファイルへの適合を主張することがある。そのようなプロファイルは、属性と特定方法での他のセキュリティプロファイルの使用法を概説する。

セキュア使用プロファイルは付属書 A の中で明記される。

6.2 セキュアトランスポートコネクションプロファイル

実装は、1 つ以上のセキュアトランスポートコネクションプロファイルへの適合を主張することがある。

セキュアトランスポートコネクションプロファイルは次の情報を含む：

- a. プロトコルフレームワークと折衝メカニズムの記述
- b. 実装がサポートするエンティティ認証の記述
 1. 認証されるエンティティの識別
 2. エンティティが認証されるメカニズム
 3. 監査ログサポートに対するすべての特別の考慮
- c. 実装がサポートする暗号メカニズムの記述
 1. セッションかぎを配布する方法
 2. 暗号プロトコルと関係するパラメータ
- d. 実装がサポートする完全性検査メカニズムの記述

セキュアトランスポートコネクションプロファイルは付属書 B の中で明記される。

6.3 デジタル署名プロファイル

実装は、1 つ以上のデジタル署名プロファイルへの適合を主張することがある。

デジタル署名プロファイルは下記の情報から構成される：

- a. 下記を含む、デジタル署名が果たす役割：
 1. デジタル署名がだれをまたはどんなエンティティを表すか。
 2. デジタル署名の目的の記述。
 3. データ集合の中にデジタル署名が含まれる条件。
- b. デジタル署名の中に含まれる属性のリスト。
- c. 下記を含めた、デジタル署名を作成するか確認するために使用されるメカニズム：
 1. MAC アルゴリズム (0400,0015) 属性のために使用される値を含む MAC またはハッシュコードを作成するために使用されるアルゴリズムと関連するパラメータ。

2. デジタル署名を作成するときに、MAC またはハッシュコードを暗号化するために使用される暗号アルゴリズムと関連するパラメータ。
 3. 証明書タイプ (0400,0110) 属性に対して使用される値を含めて、使用される証明書タイプまたはかぎ配布メカニズム。
 4. 証明されたタイムスタンプタイプ (0400,0305) および証明されたタイムスタンプ (0400,0310) 属性のためのすべての要求事項。
- d. 署名者を識別するためのすべての特別な要求事項。
 - e. ある場合は、他のデジタル署名との関係。
 - f. デジタル署名を作成し、確認し、解釈するために必要な他の要素。

デジタル署名プロファイルは付属書 C の中で明記される。

6.4 媒体保存セキュリティプロファイル

実装は、1 つ以上の媒体保存セキュリティプロファイルへの適合を主張する、言い換えると、1 つ以上の媒体保存応用プロファイルへの適合を必要とすることがある。

注

実装は、媒体保存応用プロファイルへの適合を主張しないで、媒体保存セキュリティプロファイルへの適合を主張しないことがある。

媒体保存セキュリティプロファイルは下記の仕様を含む：

- a. セキュリティのどの様相がプロファイルによって取り扱われるか。
- b. ある場合は、安全にすることができる DICOM ファイルのタイプへの制限。
- c. DICOM ファイルをカプセルに入れて、それを安全にする方法。

媒体保存セキュリティプロファイルは付属書 D の中で明記される。

6.5 ネットワークアドレス管理プロファイル

実装は、1 つ以上のネットワークアドレス管理プロファイルへの適合を要求するかもしれない。そのようなプロファイルは、実装のためにネットワークアドレスを得るために非 DICOM ネットワークプロトコルの使用を概説する。

ネットワークアドレス管理プロファイルは付属書 F の中で明記される。

6.6 時間同期プロファイル

実装は、1 つ以上の同期プロファイルへの適合を要求するかもしれない。そのようなプロファイルは、実装のために現在の時刻をセットするために非 DICOM プロトコルの使用を概説する。

時間同期プロファイルは付属書 G の中で明記される。

6.7 アプリケーション構成管理プロファイル

実装は、1 つ以上のアプリケーション構成管理プロファイルへの適合を要求するかもしれない。そのようなプロファイルは、他の装置の性状、アドレスおよび能力を得るために非 DICOM ネットワークプロトコルの使用を概説する。それによって、実装は DICOM プロトコルを使用して通信するかもしれない。また、そのようなプロファイルは、実装がその性状、アドレスおよび能力を公表するか発表するために、それらの非 DICOM プロトコルの使用も指定する。さらに、そのようなプロファイルは、実装固有構成情報が装置によってどのように得られるかも指定する。

アプリケーション構成管理プロファイルは付属書 H の中で明記される。

6.8 監査証跡プロファイル

実装は、1 つ以上の監査証跡プロファイルへの適合を要求するかもしれない。そのようなプロファイルは、セキュリティおよび個人情報保護方針施行のための監査メッセージの作成およびトランスポートを概説する。

監査証跡プロファイルは、付属書 A の中で明記される。

7 構成プロファイル

構成管理サポートは、DICOM 規格以外の規格に定義されたプロトコルによって実行される。これらのプロトコルは、アクタ、トランザクションおよびプロファイルの点からここで記述される。

アクタは DICOM プロファイル内に使用される応用エンティティと類似している。アクタは、特別の役割を行うハードウェアとソフトウェアのプロセスの集合である。装置がサービスを提供するか利用する時、装置は、適切なネットワーク活動を扱うアクタを含む。DICOM 構成アクタは装置上の他の応用エンティティと共存してもよい。いくつかの DICOM 構成アクタは、一般的な使用 IT 設備の部品として存在する。アクタの仕様は、応用エンティティのように、実際の実装の詳細に関して何も意味しない。

アクタ相互作用はトランザクションの点から定義される。トランザクションはそれぞれ名前が与えられる。その結果トランザクションは様々な活動を含む。トランザクションはすべて、通信しているアクタの点から定義される。トランザクションでのアクタの関係は、DICOM 活動中の単純な SCU および SCP 役割より複雑かもしれない。トランザクションが人との対話を含む場合、トランザクションはユーザーインターフェース、取外し可能な媒体、および他のメカニズムによって実行されるかもしれない。人は、トランザクションユースケースモデルの観点からアクタであると記述される。トランザクションは、より典型的には、特定のオペレーションを行う一連のネットワーク活動である。

トランザクションは必須成分と選択成分の両方を含む。トランザクションを実行しているアクタは、必須成分をすべて実装することを要求される。

いくつかのトランザクションはトランザクション定義に人間のアクタを含む。これらのアクタは、他のところにアクタとして定義されず、また、プロファイル説明の中に含まれない。これらのアクタは、これらの人々がコンピュータアクタと対話することを可能にするために、ある種のメカニズムが提供されなければならないことを明示するために存在する。そのユーザーインターフェースがどのように提供されるかについての他の詳細は、この規格によって明示されない。例については、Configure DHCP トランザクションの定義を参照すること。

適合は、プロファイルによって更に管理される。プロファイルは、どのトランザクションがアクタに必要なか、どのトランザクションがオプションかの点から定義される。特定のアクタの実装は、どのオプションのトランザクションおよびどのトランザクション成分が実行されたかを明示することにより文書化される。要求されるトランザクションまたは成分を省略する実装は、どんな実装もそのアクタの実装であることを主張できない。

例えば、ネットワークアドレス管理プロファイルでは、DHCP サーバは、DHCP サーバを構成し、DHCP サーバを見つけて使用し、DHCP リースを維持するという 3 つのトランザクションを行うことを要求される。さらに、それは、DDNS 協調により DNS サーバを更新するトランザクションをサポートするかもしれない。

プロファイルは、2 つ以上のアクタのための定義を含む。それは、機能を行うように協力するアクタのすべてのためのトランザクションを指定する。例えば、ネットワークアドレス管理プロファイルは DHCP サーバアクタ、DHCP クライアントアクタおよび DNS サーバアクタをカバーする。システムが有用になるため少なくとも 1 つの DHCP サーバおよび 1 つの DHCP クライアントが存在しなければならない。DHCP サーバが DDNS 協調トランザクションを実行する必要はないので、DNS サーバはそれ自身オプションである。DNS サーバがシステムの一部ならば、DDNS 協調が必要であり、DHCP サーバが DDNS 協調トランザクションに参加すると期待される。

注

DHCP サーバと同じネットワーク上で存在する DNS サーバがあるかもしれない。しかし、その DNS サーバが、このプロファイルからの DNS サーバアクタを提供していない場合、それは DICOM 構成活動の一部ではない。

プロファイル、アクタおよびトランザクションは次のセクションの中で要約される。個々の特定のプロファイルのためのアクタおよびトランザクションの詳細な性状は、各プロファイルの付属書に述べられている。そのトランザクションは、それらのオリジナルの規格文書、例えば、インターネットプロトコル用の RFC からのパラメータおよび用語の点から文書化される。トランザクションの全詳細が付属書に述べられてはいない。そのトランザクションの DICOM 応用に適切な特定の詳細だけ述べられている。これらの外部プロトコルのための完全な詳細は、外部プロトコルのための適切な規格文書の中で文書化される。特定のプロファイルの要求事項への適合は、これらの外部プロトコル文書への適合を含まなければならない。

7.1 アクタ

DHCP サーバ

DHCP サーバは、ネットワーク構成記述が提供されているコンピュータ/ソフトウェア機能であり、さらに、DHCP プロトコルに従って操業開始構成サービスを提供する特徴がある。

DHCP クライアント

DHCP クライアントは、コンピュータの操業開始の間に TCP/IP パラメータを得るために使用されるソフトウェア機能である。それは、これらのパラメータの妥当性を維持するオペレーションを継続する。

DNS サーバ

DNS サーバは、DNS プロトコルを利用するクライアントからの問い合わせに応じて IP 関連情報を提供するコンピュータ/ソフトウェア機能である。それはアソシエーションしたデータベース機能の一部であり、IP アドレス情報に機械名を関連づける現在のデータベースを維持する。DNS サーバは世界的な連結データベースからも孤立させられ、ローカル DNS サービスだけを提供するかもしれない。

DNS クライアント

コンピュータ/ソフトウェア機能としての DNS クライアントは、DNS プロトコルを利用し、ホスト名を与えられた時に IP 情報を得る。ホスト名は、明示的な IP アドレスの代りに、構成ファイルまたは他のファイル中にあるかもしれない。必要な場合、ホスト名はダイナミックに IP アドレスに変換される。DNS クライアントは、必要な情報を提供するために DNS サーバを使用する。

NTP サーバ

NTP サーバは、NTP または SNTP プロトコルに従ってタイムサービスを提供するコンピュータ/ソフトウェア機能である。

NTP クライアント

NTP クライアントは、NTP サーバから時間情報を得て、NTP サーバからの時報と同期してクライアント時間を維持するソフトウェアである。

SNTP クライアント

SNTP クライアントは、NTP サーバから時間情報を得て、NTP サーバからの時報とほぼ同期してクライアント時間を維持するソフトウェアである。SNTP クライアント同期は、NTP が提供する正確さまたは精密さでもって維持されない。

LDAP サーバ

LDAP サーバは、様々なディレクトリ情報の内部データベースを維持するコンピュータ/ソフトウェア機能である。このディレクトリ情報のうちのいくらかは DICOM 構成スキーマに相当する。LDAP サーバは、ディレクトリ情報を読み更新するためにネットワークアクセスを提供する。LDAP サーバはディレクトリ情報の外部ローディング、アンローディングおよびバックアップに対しメカニズムを供給する。LDAP サーバは、サーバのアソシエーションしたネットワークの一部かもしれない。それが提供するものは、LDAP プロトコルの規則に従ってアソシエーションしたディレクトリデータベースについての統合された見方である。

LDAP クライアント

LDAP クライアントは、LDAP サーバへの問い合わせを行うために LDAP プロトコルを利用する。LDAP サーバはデータベースを維持し、このデータベースの内容に基いたこれらの問い合わせに回答する。

7.2 トランザクション

次のトランザクションは、1 つ以上 DICOM 構成プロトコルに従うアクタ間の通信を提供するために使用される。

DHCP サーバを構成する

このトランザクションは、このネットワーク用に定められた IP パラメータに対する追加、削除、および変更を反映するために DHCP サーバの構成を変更する。

DHCP サーバを見つけて使用する

このトランザクションは、DHCP プロトコルの規則に従うネットワークメッセージのシーケンスである。このトランザクションにより、DHCP クライアントは、利用可能な DHCP サーバを見つけて、そのクライアントに適切なサーバを選ぶことができる。このトランザクションは、必須な IP パラメータ情報を DHCP サーバから得て、追加のオプションのパラメータを DHCP サーバから得る。

クライアントを構成する

サービススタッフは、クライアントのための最初の構成を設定するためにこのトランザクションを使用する。

リースを維持する

このトランザクションは、その IP リースが更新されない場合、DHCP クライアントがどのように振る舞うべきかを扱う。

DDNS 協調

このトランザクションが文書化するのは、DHCP サーバが DNS サーバと協調し、DHCP クライアントに割り当てられたホスト名を使用して DHCP クライアントへのアクセスを維持できるようにするか否かである。

ホスト名を解決する

このトランザクションは、ホスト名を与えられた時、コンピュータ用に IP アドレスを得る。

時間を維持する

これらのトランザクションは、マスタータイムサービスと時間同期を維持するために NTP または SNTP のクライアントに必要とされた活動である。

NTP サーバを見つける

このトランザクションは、NTP のために定義された自動発見手続きである。これはブロードキャスト方法または DHCP サポート方法のいずれかを使用するかもしれない。

LDAP サーバを見つける

このトランザクションでは、DNS サーバは LDAP サーバの IP アドレス、ポートおよび名前を得るために問い合わせられる。

問い合わせ LDAP サーバ

このトランザクションでは、LDAP サーバは LDAP データベースの内容に関して問い合わせられる。

クライアント最新版 LDAP サーバ

このトランザクションは、構成されているクライアントからの LDAP 最新版指示を使用して、構成データベースを更新する。

LDAP サーバを維持する

このトランザクションは、LDAP サーバのローカルサービスを使用して、構成データベースを更新する。

図 7-1 はアクタとそれらのトランザクションを示す。通常の装置は、NTP クライアント、DHCP クライアントおよび LDAP クライアントを、他の応用アクタに追加してもつ。トランザクション、「DHCP サーバを構成する」、「クライアントを構成する」および「LDAP サーバを維持する」は、これらのトランザクションはソフトウェアアクタと人間のアクタとの間にあるため、示されない。DICOM は、手段やユーザーインタフェースを指定しない。DICOM は、ある能力がサポートされることを単に必要とするだけである。

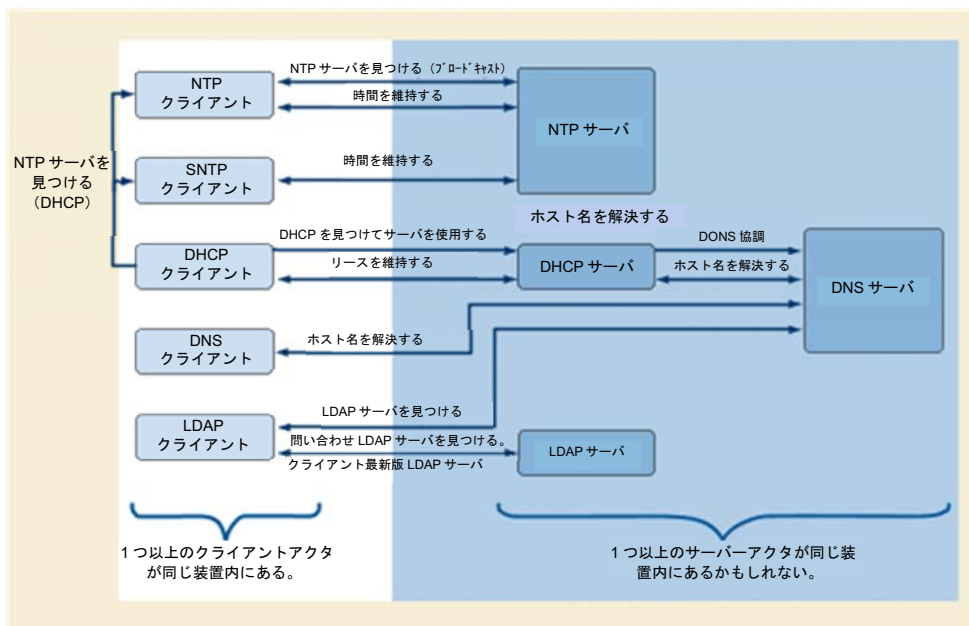


図 7-1. トランザクションおよびアクタ

A セキュア使用プロファイル（規格）

A.1 オンライン電子保存セキュア使用プロファイル

オンライン電子保存セキュア使用プロファイルは、局所セキュリティ方針がオリジナルのデータ集合とそれに続く複写の追跡を必要とするそのような場合に、応用エンティティが SOP インスタンスの状態を追跡し確認することを可能にする。

適合性宣言は、システムは遠隔アクセスを制限する方法を示す。

A.1.1 SOP インスタンス状態

オンライン電子保存セキュア使用プロファイルに適合する実装は、保存サービスクラスを使用して転送される SOP インスタンスをもつ SOP インスタンス状態 (0100,0410) 属性の使用に関する次の規則に従う：

- a. オンライン電子保存セキュア使用プロファイルをサポートし、オンライン電子保存での診断用途を意図した SOP インスタンスを作成する応用エンティティは：
 1. SOP インスタンス状態をオリジナル (OR) にセットする。
 2. 次の属性を含める：
 - i. SOP クラス UID (0008,0016) および SOP インスタンス UID (0008,0018)
 - ii. 知られている場合、インスタンス作成日付 (0008,0012) およびインスタンス作成時刻 (0008,0013)
 - iii. SOP インスタンス状態
 - iv. SOP 許可日時 (0100,0420)
 - v. ある場合は、SOP 許可コメント (0100,0424)
 - vi. 許可装置証明番号 (0100,0426)
 - vii. 検査インスタンス UID (0020,000D) およびシリーズインスタンス UID (0020,000E)
 - viii. 知られている一般装置モジュールの任意の属性
 - ix. 存在する任意のオーバーレイデータ
 - x. 存在する任意の画像データ
- b. SOP インスタンス状態がオリジナル (OR) のとき、SOP インスタンスを保持する応用エンティティは、次の規則に従う限り、オーソライズドオリジナル (AO) に SOP インスタンス状態を変更することがある：
 1. 応用エンティティは、許可されたエンティティが診断の目的に使用可能なものとして SOP インスタンスを保証したと断定する。
 2. 応用エンティティは SOP インスタンス状態をオーソライズドオリジナル (AO) に変更する。SOP インスタンス UID は変わらない。
 3. 応用エンティティは SOP 許可日時 (0100,0420) および許可装置証明番号 (0100,0426) 属性を適切な値に設定する。さらに、それは適切な SOP 許可コメント (0100,0424) 属性を加えることがある。
- c. SOP インスタンス状態がオリジナル (OR) か、オーソライズドオリジナル (AO) である場合、SOP インスタンスを保持する1つの応用エンティティだけがある。そのような SOP インスタンスを保持する応用エンティティはそれを削除しない。
- d. オンライン電子保存をサポートする応用エンティティと通信する場合、SOP インスタンス状態がオリジナルか (OR)、オーソライズドオリジナル (AO) である場合、SOP インスタンスを保持する応用エンティティは、次の規則に従う限り、オンライン電子保存セキュア使用プロファイルと同様に適合する別の応用エンティティにその SOP インスタンスを転送することがある：

1. 転送がセキュアトランスポートコネクションで生じる。
 2. 転送に関与する2つの応用エンティティは互いを確認する、そして、他がオンライン電子保存セキュア使用プロファイルをサポートすることを認証経由で確認する。
 3. 転送後に行ったデータ完全性検査が、SOP インスタンスが伝送中に変更されたことを示す場合、受信側応用エンティティは保存要求を拒絶し、受信した SOP インスタンスを廃棄する。
 4. 転送は保存委託サービスクラスのプッシュモデルを使用して確認される。この確認を終えるまで、受信側応用エンティティは他の任意の応用エンティティへ SOP インスタンスまたは SOP インスタンスのオーソライズドコピーを転送しない。
 5. 受信側応用エンティティが記憶装置に SOP インスタンスを成功裡に委ねたことを確認すると、送信側応用エンティティは、SOP インスタンスのその局所コピーに下記の1つを行う：
 - i. SOP インスタンスを削除する、
 - ii. 無指定 (NS) に SOP インスタンス状態を変更する、
 - iii. SOP インスタンス状態がオーソライズドオリジナル (AO) だった場合は、オーソライズドコピー (AC) に SOP インスタンス状態を変更すること。
- e. オンライン電子保存をサポートする応用エンティティと通信する場合、SOP インスタンス状態がオーソライズドオリジナル (AO) またはオーソライズドコピー (AC) である SOP インスタンスを保持する応用エンティティは、次の規則に従う限りは、別の応用エンティティに SOP インスタンスのオーソライズドコピーを送ってもよい：
1. 転送がセキュアトランスポートコネクションで生じる。
 2. 転送に関与する2つの応用エンティティは互いを確認する、そして、他がオンライン電子保存セキュア使用プロファイルをサポートすることを認証経由で確認する。
 3. 送信側応用エンティティは、送信するコピーの中で、SOP インスタンス状態を無指定 (NS) またはオーソライズドコピー (AC) にセットする。SOP インスタンス UID は変わらない。
 4. 転送後に行われたデータの完全性検査が、SOP インスタンスが伝送中に変更されたことを示す場合、受信側応用エンティティは保存要求を拒絶し、コピーを廃棄する。
- f. オンライン電子保存セキュア使用プロファイルをサポートしないシステムと通信する場合、または通信がセキュアトランスポートコネクションで行われない場合、
1. このセキュリティプロファイルに適合する送信側応用エンティティは、無指定 (NS) に SOP インスタンス状態をセットするか、または送信側応用エンティティがセキュアでないトランスポートコネクション上にまたはオンライン電子保存セキュア使用プロファイルをサポートしないシステムに発送する任意の SOP インスタンスの SOP インスタンス状態および関連するパラメータを省略する。
 2. このセキュリティプロファイルに適合する受信側応用エンティティは、セキュアでないトランスポートコネクション上で、またはオンライン電子保存セキュア使用プロファイルをサポートしないシステムから受信した任意の SOP インスタンスの SOP インスタンス状態を無指定 (NS) へセットする。
- g. 保存委託保存サービスクラスによって必要とされるように、受信側応用エンティティは保存サービスクラスに定義される水準 2 に従って (即ち、私的属性を含むすべての属性) SOP インスタンスを保存する、そして SOP インスタンス状態、SOP 許可日時、許可装置証明番号および SOP 許可コメントの他の属性を強制しない。
- h. 上に概説された SOP インスタンス状態、SOP 許可日時、許可装置証明番号、および SOP 許可コメント属性への変更、または前述の変更に伴うグループ長さ属性への変更以外は、応用エンティティは如何なる属性値も変更しない。

A.2 基本デジタル署名セキュア使用プロファイル

デジタル署名を有効にして作成する実装は、基本デジタル署名セキュア使用プロファイルへの適合性を主張することがある。このセキュリティプロファイルへの適合性を主張する実装は、デジタル署名を扱うときに次の規則に従う：

- a. 実装は、それが SOP インスタンスのいかなる無許可の不正な変更を加えることに対して警戒するのと同じ方法で、それが受け取るすべての SOP インスタンスを保存する。

- b. 可能な場合どこでも、その実装は、それが受け取るすべての SOP インスタンス内のデジタル署名を有効にする。
- c. 実装が SOP インスタンスを別の応用エンティティに送る場合、それは下記を行う：
 - 1. 属性値のフォーマットへの任意の許可された変形により無効になったかもしれないすべてのデジタル署名を削除する。(例えばパディングの削除、数の代替表現)。
 - 2. SOP インスタンスが受信されたときに実装が確認することができたデータ要素をカバーする 1 つ以上の新しいデジタル署名を作成する。

A.3 ビット保存デジタル署名セキュア使用プロファイル

SOP インスタンスを保存し転送する実装は、ビット保存するデジタル署名セキュア使用プロファイルへの適合性を主張することができる。このセキュリティプロファイルへの適合性を主張する実装は、デジタル署名を扱うときに次の規則に従う：

- a. SOP インスタンスが別の応用エンティティへ転送される場合、すべての属性の値領域は最初に受信した領域のビットに対するビットの複製であるような方法で、実装は、それが受信するすべての SOP インスタンスを保存する。
- b. 実装は、シーケンスの中の項目の順序を変更しない。
- c. 実装は、DICOM 経由で別の応用エンティティ上へのその SOP インスタンスを送る場合、それが受信するすべての SOP インスタンスのいかなるデータ要素も削除しないか変更しない。これは、受信したいいかなるデジタル署名も含む。

注

実装は、いかなる既存のデジタル署名も変更しない新しいデータ要素を追加することがある。

- d. 実装は明示的 VR 転送構文を利用する。

注

暗黙の VR 転送構文で受信したデジタル署名を確認することができないことがあるので、明示的 VR 転送構文を使用することができない実装は、このセキュア使用プロファイルに適合することができない。

- e. 実装は、別の応用エンティティにそのオブジェクトを送信する場合、それが受け取るいかなるデータ要素の VR も変更しない。

A.4 基礎的 SR デジタル署名セキュア使用プロファイル

このセキュリティプロファイルへの適合を主張する実装は何れも、デジタル署名を含む構造化レポートまたはキーオブジェクト選択文書を作成する場合、次の規則に従わなければならない：

- a. 実装が構造化レポートまたはキーオブジェクト選択文書 SOP インスタンスに署名する場合、デジタル署名は、構造化レポート RSA デジタル署名プロファイルに従って作成されなければならない。
- b. 作成されたすべての署名された構造化レポートまたはキーオブジェクト選択文書 SOP インスタンスの中で、現在の参照手続き証拠シーケンス(0040,A375)の参照 SOP シーケンスアイテムおよび適切な他の証拠シーケンス(0040,A385)の中にリストされる参照された SOP インスタンスはすべて、参照デジタル署名シーケンスまたは参照 SOP インスタンス MAC シーケンスの何れかを含まなければならない。その参照は両方を含むかもしれない。

適合を主張する実装は、その適合性宣言書の中で、それが構造化レポートまたはキーオブジェクト選択文書に署名するか否かの条件を概説しなければならない。

A.5 監査証跡メッセージフォーマットプロファイル

自動システムでのヘルスケアプライバシーおよびセキュリティを保証するのをサポートするために、使用法のデータを集める必要がある。これらのデータは、管理職員によって、ヘルスケアデータの使用が医療サービス提供者のデータセキュリティ要求事項に従うことを検証するため、かつデータ使用の責任能力を確立するために調査される。このデータ収集と調査のプロセスはセキュリティ監査と呼ばれ、また、データはそれ自体監査証跡を含む。監査証跡は、より進んだ調査をするのが妥当であると思われる興味あるイベントが起っているかもしれない時を検知するために、査察目的に使用できる。

このプロファイルは、集められるデータのフォーマット、および調査適用による事後の使用のためのヘルスケアアプリケーションシステムによって捕えられる属性の最小のセットを定義する。データには、ヘルスケアデータにアクセスしたのは誰か、いつか、どんなアクションのためか、どこからか、そしてどの患者記録が関係したかについての記録を含む。いつ監査メッセージが作成されるか、またはどのアクションがそれらの受け取りのため講じられるかに関して、どんな行動の要求事項も指定されない。これら

は局所方針決定および法的要求事項に従う。

このセキュリティプロファイルへの適合を主張する実装はすべて、以下のことをしなければならない：

- a. 監査証跡メッセージを、セクション A.5.1 の中で指定された XML スキーマに従うようにフォーマットする。それによりそれらのメッセージが XML スキーマに対して妥当性確認され、セクション A.5.2 に指定された規約に従う。
- b. このプロファイルに述べられてたイベントのために、このプロファイルによってセクション A.5.3 に指定された制限に適合し、その適合性宣言書に国内拡張を記述する。

注

上記の条件が満たされる限り、実装は実装に特有の拡張を含むかもしれない。

- c. その適合性宣言書にそれが検知し報告できるイベントについて記述する。
- d. その適合性宣言書にそれがメッセージの受信をもって実行できる処理について記述する。
- e. その適合性宣言書にイベント報告およびイベント処理の設定方法について記述する。

注

他のプロファイルは、監査メッセージの送信を指定する。

A.5.1 DICOM 監査メッセージスキーマ

このプロファイルへの適合を主張する実装は、監査証跡メッセージをフォーマットするために次の XML スキーマを使用しなければならない。このスキーマの出典は、RFC3881 の IETF 草案のインターネット規格の中で指定されたスキーマである。つまり「ヘルスケアアプリケーションの安全監査およびアクセス責任能力 XML メッセージデータ定義」であって、W3C 勧告「XML スキーマ第 1 部：構造」バージョン 1.0、2001 年 5 月に従うものであり、またセクション A.5.2 に概説された DICOM 拡張および制限を組込む。

このスキーマは Relax NG のコンパクトなフォーマットの中で提供される。

注

このスキーマは等価な XML スキーマまたは他の電子フォーマットに変換できる。このスキーマは、RFC 3881 スキーマへのいくつかの修正を含んでいるが、それは監査メッセージ要求事項についての現場経験を反映している。このスキーマは RFC3881 スキーマを拡張する。

A.5.1.1 監査メッセージスキーマ

監査スキーマの内容は以下のとおり：

```
datatypes xsd = "http://www.w3.org/2001/XMLSchema-datatypes"
```

```
# This defines the coded value type. The comment shows a pattern that can be used to further
# constrain the token to limit it to the format of an OID. Not all schema software
# implementations support the pattern option for tokens.
other-csd-attributes =
  (attribute codeSystemName { token } | # OID pattern="[0-2](\.\d)(\.[1-9][0-9]*)*"
   attribute codeSystemName { token }, # This makes clear that codeSystemName is
   # either an OID or String
  attribute displayName { token }?,
  attribute originalText { token } # Note: this also corresponds to DICOM "Code Meaning"
CodedValueType =
  attribute csd-code { token },
  other-csd-attributes
```

Define the event identification, used later

```

EventIdentificationContents =
  element EventID { CodedValueType },
  element EventTypeCode { CodedValueType }*, # Note: DICOM/IHE defines and uses this
      # differently than RFC-3881
  attribute EventActionCode {          # Optional action code
    "C" |      ## Create
    "R" |      ## Read
    "U" |      ## Update
    "D" |      ## Delete
    "E" |      ## Execute
  }?,

  attribute EventDateTime { xsd:dateTime },
  attribute EventOutcomeIndicator {
    "0" |      ## Nominal Success (use if status otherwise unknown or ambiguous)
    "4" |      ## Minor failure (per reporting application definition)
    "8" |      ## Serious failure (per reporting application definition)
    "12" |     ## Major failure, (reporting application now unavailable)
  },

  element EventOutcomeDescription { text }?

```

Define AuditSourceIdentification, used later

```

AuditSourceIdentificationContents =
  attribute AuditEnterpriseSiteID { token }?,
  attribute AuditSourceID { token },
  element AuditSourceTypeCode { AuditSourceTypeCodeContent }*

# Define AuditSourceTypeCodeContent so that an isolated single digit
# value is acceptable, or a token with other csd attributes so that
# any controlled terminology can also be used.

```

```

AuditSourceTypeCodeContent =
  attribute csd-code {
    "1" |      ## End-user display device, diagnostic device
    "2" |      ## Data acquisition device or instrument
    "3" |      ## Web Server process or thread
    "4" |      ## Application Server process or thread
    "5" |      ## Database Server process or thread
    "6" |      ## Security server, e.g., a domain controller
    "7" |      ## ISO level 1-3 network component
    "8" |      ## ISO level 4-6 operating software
    "9" |      ## other
  token },      ## other values are allowed if a codeSystemName is present
  other-csd-attributes? ## If these are present, they define the meaning of code

```

Define ActiveParticipantType, used later

```

ActiveParticipantContents =
  element RoleIDCode { CodedValueType }*,
  element MediaIdentifier {
    element MediaType { CodedValueType }
  }?,
  attribute UserID { text },
  attribute AlternativeUserID { text }?,
  attribute UserName { text }?,

```

```

attribute UserIsRequestor { xsd:boolean },
attribute NetworkAccessPointID { token }?,
attribute NetworkAccessPointTypeCode {
  "1" |      ## Machine Name, including DNS name
  "2" |      ## IP Address
  "3" |      ## Telephone Number
  "4" |      ## Email address
  "5" }?    ## URI (user directory, HTTP-PUT, ftp, etc.)

```

```

# The BinaryValuePair is used in ParticipantObject descriptions to capture parameters.
# All values (even those that are normally plain text) are encoded as xsd:base64Binary.
# This is to preserve details of encoding (e.g., nulls) and to protect against text
# contents that contain XML fragments. These are known attack points against applications,
# so security logs can be expected to need to capture them without modification by the
# audit encoding process.

```

```

ValuePair =
# clarify the name
attribute type { token },
attribute value { xsd:base64Binary } # used to encode potentially binary, malformed XML text, etc.

```

```

# Define ParticipantObjectIdentification, used later

```

```

# Participant Object Description, used later

```

```

DICOMObjectDescriptionContents =
  element MPPS {
    attribute UID { token } # OID pattern="[0-2](\.\.0)(\.[1-9][0-9]*)*"
  }*,
  element Accession {
    attribute Number { token }
  }*,
  element SOPClass { # SOP class for one study
    element Instance {
      attribute UID { token } # OID pattern="[0-2](\.\.0)(\.[1-9][0-9]*)*"
    }*,
    attribute UID { token }?, # OID pattern="[0-2](\.\.0)(\.[1-9][0-9]*)*"
    attribute NumberOfInstances { xsd:integer }
  }*,
  element ParticipantObjectContainsStudy {
    element StudyIDs {
      attribute UID { token }
    }*
  }?,
  element Encrypted { xsd:boolean }?,
  element Anonymized { xsd:boolean }?

```

```

ParticipantObjectIdentificationContents =
  element ParticipantObjectIDTypeCode { CodedValueType },
  (element ParticipantObjectName { token } | # either a name or
  element ParticipantObjectQuery { xsd:base64Binary }), # a query ID field,
  element ParticipantObjectDetail { ValuePair }*, # optional details, these can be extensive
  # and large
  element ParticipantObjectDescription { DICOMObjectDescriptionContents }*,
  attribute ParticipantObjectID { token }, # mandatory ID
  attribute ParticipantObjectTypeCode { # optional type
    "1" | ## Person
    "2" | ## System object
    "3" | ## Organization
    "4" | ## Other
  }

```



```

}?,

attribute ParticipantObjectTypeCodeRole {    ## optional role
"1" |    ## Patient
"2" |    ## Location
"3" |    ## Report
"4" |    ## Resource
"5" |    ## Master File
"6" |    ## User
"7" |    ## List
"8" |    ## Doctor
"9" |    ## Subscriber
"10" |   ## Guarantor
"11" |   ## Security User Entity
"12" |   ## Security User Group
"13" |   ## Security Resource
"14" |   ## Security Granularity Definition
"15" |   ## Provider
"16" |   ## Data Destination
"17" |   ## Data Archive
"18" |   ## Schedule
"19" |   ## Customer
"20" |   ## Job
"21" |   ## Job Stream
"22" |   ## Table
"23" |   ## Routing Criteria
"24" |   ## Query
"25" |   ## Data Source
"26" |   ## Processing Element
}?,

attribute ParticipantObjectDataLifeCycle {    # optional life cycle stage
"1" |    ## Origination, Creation
"2" |    ## Import/ Copy
"3" |    ## Amendment
"4" |    ## Verification
"5" |    ## Translation
"6" |    ## Access/Use
"7" |    ## De-identification
"8" |    ## Aggregation, summarization, derivation
"9" |    ## Report
"10" |   ## Export
"11" |   ## Disclosure
"12" |   ## Receipt of Disclosure
"13" |   ## Archiving
"14" |   ## Logical deletion
"15" }?, ## Permanent erasure, physical destruction

attribute ParticipantObjectSensitivity { token }?

# The basic message
message =
element AuditMessage {
(element EventIdentification { EventIdentificationContents }, # The event must be identified
element ActiveParticipant { ActiveParticipantContents }+, # It has one or more active
                    # participants
element AuditSourceIdentification {                # It is reported by one source
    AuditSourceIdentificationContents
},
element ParticipantObjectIdentification {          # It may have other objects involved

```

```

    ParticipantObjectIdentificationContents
  })
}

```

And finally the magic statement that message is the root of everything.
start = message

A.5.1.2 スキーマ内で使用するコード

上記の監査スキーマには以下の値セットが定義されている。これらはコード化された用語ではない。メッセージ内の適切な位置での使用に応じて意味が決まる値である。

A.5.1.2.1 Audit Source Type Code

Audit Source Type Code（監査ソースタイプコード）の値は、イベントの発生元（ソース）の種類を明記するものである。コード化された用語からのコードおよび処理系定義のコードも AuditSourceTypeCode に使用できる。

表 A.5.1.2.1-1. Audit Source Type Code の値

値	意味
1	エンドユーザーのインターフェイス
2	データを取得する装置または機器
3	多層システムのウェブサーバプロセス層
4	多層システムのアプリケーションサーバプロセス層
5	多層システムのアプリケーションサーバプロセス層
6	ドメインコントローラ等のセキュリティサーバ
7	ISO レベル 1-3 ネットワーク構成要素
8	ISO レベル 4-6 オペレーティングソフトウェア
9	外部ソース、その他または認識されていないタイプ

A.5.1.2.2 Participant Object Type Code Role

Participant Object Type Code Role（参加者オブジェクトタイプコードロール）は ParticipantObjectIdentification の属性であり、拡張性はない。この属性は省略されるか、あるいはアサインされた以下の値のうちの一つかもしれない。コード化された用語はサポートされない。

表 A.5.1.2.2-1. Participant Object Type Code Roles

値	意味	関連すると思われる Participant Object Type Code
1	患者	1 - 個人
2	ロケーション	3 - 組織
3	報告書	2 - システムオブジェクト
4	リソース	1 - 個人、または 3 - 組織
5	マスターファイル	2 - システムオブジェクト
6	ユーザー	1 - 個人、または 2 - システムオブジェクト
7	リスト	2 - システムオブジェクト
8	医師	1 - 個人

値	意味	関連すると思われる Participant Object Type Code
9	加入者	3 - 組織
10	保証人	1 - 個人, または 3 - 組織
11	セキュリティユーザーエンティティ	1 - 個人, または 2 - システムオブジェクト
12	セキュリティユーザーグループ	2 - システムオブジェクト
13	セキュリティリソース	2 - システムオブジェクト
14	セキュリティレベルの定義	2 - システムオブジェクト
15	提供者	1 - 個人, または 3 - 組織
16	データ送信先	2 - システムオブジェクト
17	データレポジトリ	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	ジョブ	2 - システムオブジェクト
21	ジョブストリーム	2 - システムオブジェクト
22	表	2 - システムオブジェクト
23	ルーティング基準	2 - システムオブジェクト
24	問い合わせ	2 - システムオブジェクト

A.5.1.2.3 Participant Object Data Life Cycle

Participant Object Data Life Cycle (参加者オブジェクトデータライフサイクル) は ParticipantObjectIdentification の属性であり、拡張性はない。この属性は省略されるか、あるいはアサインされた以下の値のうちの一つかもしれない。コード化された用語はサポートされない。

表 A.5.1.2.3-1. Participant Object Data Life Cycle の値

値	意味
1	発生または作成
2	オリジナルを読み込みまたはコピー
3	修正
4	検証
5	翻訳
6	アクセスまたは使用
7	匿名化(De-identifier)
8	統合, 要約, 派生
9	報告書
10	対象先へ書き出しましたまたはコピー
11	開示
12	開示の受け取り
13	アーカイブ
14	論理削除

値	意味
15	永久抹消または物理的破壊

A.5.1.2.4 Participant Object ID Type Code

Participant Object ID Type Code (参加者オブジェクト ID タイプコード) は参加者オブジェクト ID に含まれる ID について記述する。コード化された用語からのコードおよび処理系定義のコードも ParticipantObjectTypeCodeRole に使用できる。

表 A.5.1.2.4-1. Participant Object ID Type Code の値

値	意味	関連すると思われる Participant Object Type Code
1	カルテ番号	1 - 個人
2	患者番号	1 - 個人
3	エンカウンター番号	1 - 個人
4	登録者番号	1 - 個人
5	社会保障番号	1 - 個人
6	登録番号	1 - 個人, または 3 - 組織
7	保証人番号	1 - 個人, または 3 - 組織
8	報告書名	2 - システムオブジェクト
9	報告書番号	2 - システムオブジェクト
10	検索条件	2 - システムオブジェクト
11	ユーザー ID	1 - 個人, または 2 - システムオブジェクト
12	URI	2 - システムオブジェクト

A.5.2 一般的なメッセージフォーマット規約

次の表は、A.5.1 の中で指定されたメッセージスキーマから主要なフィールドをリストする。それに追加して、DICOM アプリケーションがどのようにフィールド値を満たすかについての指示、規約および制約をリストする。これらのフィールド名は DICOM 監査メッセージスキーマにあるリーフ要素および属性である (セクション A5.1 参照)。スキーマによって明記されるように、これらのフィールドが他の XML 要素で囲まれるかもしれないことに注意すること。

注

当スキーマ、コード、コンテンツは元は RFC3881 から導出したものである。IETF は RFC3881 のメンテナンスや更新を行っていないため、DICOM のスキーマおよびコードとは徐々に相違が生じてきている。根底となる規格として RFC3881 を参照している文書は他にも存在する。2004 年以降、RFC3881 には監査スキーマへの修正や追加がない。

以降の諸表では、オプション性の項目に以下の表示を使用する：

- M** 必須の要素または属性。
- U** ユーザーオプションの要素または属性。作成者はこれを含めてもよいし省略してもよい。
- MC** 所定の条件に当てはまる場合は必須となる要素または属性。
- UC** 所定の条件に当てはまる場合、ユーザーが含まれることにした場合のみ当要素または属性は表示される。

表 A.5.2-1. 一般的なメッセージフォーマット

	フィールド名	オプション性	概要	フィールド形式/値の追加条件
イベント	EventID	M	特別の監査されたイベントのための ID	イベントのファミリーのための ID。例えば、「ユーザー認証」。 DCID 400 「監査イベント ID」
	EventActionCode	U	監査を作成したイベント中に行われたアクションのタイプのための指標。	C 発注等, データベースオブジェクトの新規作成。 R 医師センサス等の表示/閲覧/印刷/照会画面またはデータ印刷 U 患者の修正情報等のデータ更新 D マスターファイルレコード等のアイテム削除 E ログオン, プログラム実行, オブジェクトメソッドの使用等のシステム機能またはアプリケーション機能の実施
	EventDateTime	M	統合調整時間 (UTC), つまり現地時間帯に関して明白な日付/時間明細。	監査されたイベントが生じた時。セクション A.5.2.5 参照。
	EventOutcomeIndicator	M	イベントが成功したか失敗したかどうかを示す。	0 成功 1 軽微な失敗, アクション再開。例えば無効なパスワードにより初回再試行 2 深刻な失敗, アクション終了。例えば無効なパスワードで試行回数超過 3 重大な失敗, アクション利用不可に。例えばログオン失敗回数が最大数を超えたためユーザーアカウントが無効化 特別のイベントが一部は成功し, 一部は失敗した場合, 1つのメッセージが成功したアクションに対し作成され, 1つのメッセージが失敗したアクションに対し作成されなければならない (つまり, 混合結果をもつ単一のメッセージではない)。
	EventTypeCode	U	イベントのカテゴリのための ID。	イベントに適用可能なファミリー内の特定のタイプ。例えば「ユーザーログイン」 DCID 401 「監査イベントタイプコード」
活発な参加者 (多重値)	UserID	M	イベントに活発に参加するユーザーのための一意的な ID。	セクション A.5.2.1 を参照。
	AlternativeUserID	U	ユーザーのための代替の一意的な ID。	セクション A.5.2.2 を参照。
	UserName	U	人間に意味の分かる, ユーザーのための名前。	セクション A.5.2.3 を参照

	フィールド名	オプション性	概要	フィールド形式/値の追加条件
	UserIsRequestor	M	ユーザーが、監査されているイベントの要求者または開始者か否かの指標。	どの参加者が、監査されているトランザクションを始めたか識別するために使用される。どの参加者が要求者であるかを監査ソースが決めることができない場合、フィールドはすべての参加者の中で値 FALSE で存在しなければならない。 システムは多数の参加者を UserIsRequestor であると確認してはならない。数人の既知の要求者がある場合、報告制度は UserIsRequestor として 1 人だけを取り上げなければならない。
	RoleIDCode	U	イベントを行う場合、ユーザーが果たす役割の明細。これは役割に基いたアクセス制御セキュリティで割当てられる。	DCID 402 「積極的な監査参加者の役割 ID コード」 注 このフィールドの使用法は、個々のメッセージ性状の中で下記のように洗練される。これが多重値のフィールドであるので、他の追加の役割も存在するかもしれない。
	NetworkAccessPointTypeCode	U	ネットワークアクセスポイントのタイプの ID	セクション A.5.2.4 を参照。
	NetworkAccessPointID	U	ユーザー装置のネットワークアクセスポイントのための ID。これは装置 id, IP アドレスまたは装置に関連した他の ID であり得る。	
監査ソース	AuditEnterpriseSiteID	U	ヘルスケア企業ネットワーク内の論理的なソース位置。例えば、病院、多重エンティティ供給者グループ内の他の供給者位置。	監査ソース ID は、全体的に一意的であることは要求されないので、監査ソース ID を更に規定する役目をする。
	AuditSourceID	M	ソースの ID。	監査可能なイベントを検知し、この監査メッセージを作成したシステムの識別。しばしば、監査ソースは参加者のうちの 1 人であるが、さらに、それは参加者の活動を監視している外部システムであり得る（例えば、アドオン監査作成装置）。
	AuditSourceTypeCode	U	ソースのタイプを指定するコード	セクション A.5.1.2.1 を参照。 例えば、収集装置は「2」（データ収集装置）を使用するかもしれない。PACS/RIS システムは「4」（アプリケーションサーバトランザクション）を使用するかもしれない。
参加者オブジェクト（多重値）	ParticipantObjectTypeCode	U	監査されている参加者オブジェクトタイプのためのコード。この値は、ユーザーの役割から、または参加者オブジェクトに対するユーザー関係から区別される。	1 個人 2 システムオブジェクト 3 組織 4 その他
	ParticipantObjectTypeCodeRole	U	監査されている参加者オブジェクトの機能的な適用役割を表すコード。	セクション A.5.1.2.2 を参照。

	フィールド名	オプション性	概要	フィールド形式/値の追加条件
	ParticipantObjectDataLifeCycle	U	参加者オブジェクト用のデータライフサイクルステージのための ID。これは時間経過のデータの監査証跡を提供するために使用できる。それはシステムを通じて経過する。	セクション A.5.1.2.3 を参照。
	ParticipantObjectIDTypeCode	M	参加者オブジェクト ID に含まれている ID について記述する。	セクション A.5.1.2.4 および CID 404 「監査参加者オブジェクト ID タイプコード」を参照。 注 このフィールドの使用法は、個々のメッセージ性状の中で下記のように洗練される。これは多重値のフィールドであるため、役割も複数存在するかもしれない。
	ParticipantObjectSensitivity	U	参加者オブジェクト ID の方針定義感度を表示する。例えば、VIP、HIV ステータス、メンタルヘルスステータスまたは同様のトピック。	ローカルで定義された用語。
	ParticipantObjectID	M	参加者オブジェクトの特定のインスタンスを識別する。	個々のメッセージ性状によって洗練された使用法
	ParticipantObjectName	U	監督される参加者オブジェクト ID のインスタンス特有ディスクリプタ。例えば、人の名前。	個々のメッセージ性状によって洗練された使用法
	ParticipantObjectQuery	U	問い合わせタイプの参加者オブジェクトのための実際の問い合わせ。	個々のメッセージ性状によって洗練された使用法
	ParticipantObjectDetail	U	実装定義されたデータであって、オブジェクトの特定の詳細に関しアクセスされたか使用されたもの。	当要素はタイプ/値のペアである。「タイプ」の属性は実装定義されたテキスト文字列である。「値」の属性はベース 64 を使用してコード化されたデータである。当値はバイナリーデータの送信に適している。
	SOPClass	MC		SOP クラスの UID であってこの参加者オブジェクトの中で引用されるもの。 ParticipantObjectIDTypeCode が (110180, DCM, "Study Instance UID") であり、またオプションのフィールド (AccessionNumber, ContainsMPPS, NumberOfInstances, ContainsSOPInstances, Encrypted, Anonymized) の何れかがこの参加者オブジェクトの中にある場合に必要。任意のフィールドが一つも存在していない場合でも ParticipantObjectIDTypeCode が (110180, DCM, "Study Instance UID") である場合、存在してもよい。
	Accession	U		受入番号はこの参加者オブジェクトと提携した。
	MPPS	U		MPPS インスタンス UID はこの参加者オブジェクトと提携した。
	NumberOfInstances	U		SOP の数はこの参加者オブジェクトによって引用される。

	フィールド名	オプション性	概要	フィールド形式/値の追加条件
	Instance	U		SOP インスタンス UID 値 注 SOP インスタンスのリストを含むことにより、かなり大きな監査メッセージを作成できる。ほとんどの状況の下で、SOP インスタンス UID のリストは監査目的に必要とされない。
	Encrypted	U		真実か誤りを示す単一の値。データが暗号化されたか否かを示す。 注 暗号化データおよび非暗号化データの混合があった場合、2つのイベント報告書を作成すること。
	Anonymized	U		真実か誤りを示す単一の値。患者識別情報がすべてデータから取り除かれたか否かを示す。
	ParticipantObjectContainsStudy	U		Study InstanceUID。これは、ParticipantObjectTypeCode が (110180, DCM, "Study Instance UID") でない場合、使用されるかもしれない。

A.5.2.1 UserID

参加者が人ならば、ユーザーIDは、この特定システム上でその人のために使用されたIDでなければならない。形式は loginName@domain-name である。

参加者が識別可能なプロセスならば、選択された UserID は、内部システムログの中で使用されるIDのうちの一つでなければならない。例えば、ユーザーIDは、ローカルシステムログの中でローカルのオペレーティングシステム内に使用されるプロセスIDかもしれない。参加者がノードならば、ユーザーIDはノード名であってシステム管理者によって割当てられたものかもしれない。他の参加者、例えば、スレッド、再配置可能なプロセス、ウェブサービス終了点、ウェブサーバ実行可能スレッドは、適切なIDをもつであろう。その実装は、適合性宣言書中で、使用されたIDを文書化しなければならない、セクション A.6 参照。この要求事項の目的は、監査ログIDが報告制度の内部システムログと一致できるようにすることである。

データの読み込みまたは書き出し中に（例えば、媒体により）、UserID フィールドは、人々の識別および媒体それ自体の識別の両方に使用される。役割IDコードが EV(110154, DCM, "Destination Media") または EV(110155, DCM, "Source Media") である場合、UserID は次のとおりかもしれない：

- ソースか目的地を識別する URI（好ましい形式）、
- 電子メールアドレス。形式は「mailto: user@address」
- 媒体のタイプの性状（例：DVD）、およびその識別ラベルの性状、自由なテキストフィールドとしてのもの、
- 媒体のタイプの性状（例：紙、フィルム）、および媒体作成者の位置の性状（つまり、プリンタ）。

媒体のための UserID フィールドは高度に柔軟である必要がある。使用されるかもしれない媒体およびトランスポートの種類が多いからである。

A.5.2.2 AlternativeUserID

参加者が人ならば、代替のユーザーIDは、その人に企業内で認証目的に使用されたIDでなければならない。例えば、Kerberos Username (user@realm) である。参加者が DICOM アプリケーションならば、代替のユーザーIDは、イベントに参加した1つ以上の AE タイトルでなければならない。多数の AE タイトルは次のようにコード化されなければならない：

AE タイトル= aetitle1;aetitle2;...

データの読み込みまたは書き出し中に（例えば、媒体により）、代替 UserID フィールドは、人々の識別および媒体それ自体の識別の両方に使用される。役割 ID コードが（110154, DCM, “Destination Media”）、または（110155, DCM, “Source Media”）であるとき、代替 UserID は、媒体上の機械可読の識別かもしれない。例えば、媒体通し番号、ボリュームラベル、または DICOMDIR SOP インスタンス UID である。

A.5.2.3 Username

参加者についての人間に判読可能な識別。参加者が人ならば、人の名前が使用されなければならない。参加者がプロセスならば、プロセス名が使用されなければならない。

A.5.2.4 Multi-homed Nodes

NetworkAccessPointTypeCode と NetworkAccessPointID は、多数の物理的なネットワーク接続をしているシステムには曖昧になり得る。これらのマルチホームノードについては、監査のイベントを報告する場合、単一の DNS 名または IP アドレスが選択され使用されなければならない。DICOM は、識別に使用されるネットワーク接続を選択する特定方法の使用を要求しない。しかし、それは、そのノードに関するイベントのために作成された監査メッセージのすべてに対し同じでなければならない。

A.5.2.5 EventDateTime

EventDateTime は、報告されているイベントが行われた日付および時間である。いくつかのイベントには重要な継続がある。これらの場合、日付と時間は、報告されているイベントと一貫し、かつ、適切な方法によって選ばれなければならない。

EventDateTime は時間帯情報を含まなければならない。

監査メッセージの作成者は閏秒をサポートしてもよいが、要求はされない。監査メッセージの受け手は、閏秒情報を用いてメッセージを処理できなければならない。

A.5.2.6 ParticipantObjectTypeCodeRole

ParticipantObjectTypeCodeRole は報告中のイベントにてオブジェクトが果たした役割を識別する。イベントの多くは複数の参加オブジェクトを伴う。ParticipantObjectTypeCodeRole はイベントにおいてどのオブジェクトがどの役割を果たしたかを識別する。また、エージェント、多目的エンティティ、マルチ役割エンティティも対象として含む。イベントの目的には主な役割が 1 つ選ばれる。

表 A.5.2.6-1. ParticipantObjectTypeCodeRole

コード	簡略説明	概要
1	患者	当オブジェクトはこのイベントに関連する治療を受ける患者である。患者 ID またはこれに相当するもので特定可能である。患者は人でも動物でもよい。
2	ロケーション	イベントに関連するとして特定された場所。通常はそのイベントが行われた場所のことである。配送の場合、通常のイベントは場所への到着または場所からの出発であることに注意。
3	報告書	当オブジェクトはイベントの結果として作成された種類を問わない保存文書である。例えば紙面での報告書、フィルム、電子報告書、DICOM スタディ等がある。カルテライフサイクル管理に関する課題は他へ通達される。
4	リソース	(推奨せず)
5	マスターファイル	文書作成や挙動の管理に使用する、設定可能なファイル。例えば、HL7 マスターファイルトランザクション、値セット等で保持されるオブジェクトなどである。
6	ユーザー	他のカテゴリで特定されない限り、人である参加者
7	リスト	(推奨せず)
8	医師	イベントに関連した治療を提供または実施する人。通常は内科医。医師と提供者の主な違いは、どのような形で参加するか、である。医師はその作業を実際に行う人である。一方、提供者はその作業に対し責任を負う人または組織である。
9	加入者	イベントの一環として通知された人またはシステム。イベント実施時に自動システムが他者に通知するような状況でこれは有意義である。

コード	簡略説明	概要
10	保証人	ヘルスケアイベントの支払責任を引き受ける保険会社やその他の組織。
11	セキュリティユーザーエンティティ	イベントに関与する、セキュリティの役割を担った人またはアクティブなシステム。
12	セキュリティユーザーグループ	(推奨せず)
13	セキュリティリソース	役割表等、イベントに関する受動的オブジェクト
14	セキュリティレベルの定義	(推奨せず) 所定の RBAC セキュリティ方法論に関連
15	提供者	治療提供について責任を負う人または組織これにはすべての形態の治療、認可済みあるいはその逆、そしてすべての種類のチームおよび治療グループが含まれる。提供者と医師とでは、患者へ実際に治療を施したかどうかという点で違いがあることに注意。
16	データ送信先	他の役割が適切でない場合のデータ転送先
17	データアーカイブ	アーカイブやデータベース等などの役割を果たすデータ転送元またはデータ転送先
18	スケジュール	スケジュール情報を保持するオブジェクト。予定表や空き時間情報など。
19	顧客	サービスを受け取る組織または個人。患者向けのサービスを受け取る組織や、動物向けのサービスを受け取る個人など。
20	ジョブ	オーダー、タスク、ワークアイテム、手順ステップ等、実施するワークの概要例：MPPS の特定インスタンス
21	ジョブストリーム	ジョブリストまたはジョブリストを提供するシステム。例：NWL SCP など。
22	表	(推奨せず)
23	ルーティング基準	アイテムのルーティングや送付を特定または管理するオブジェクト。例えばメールのルーティング基準である配信リストなど。送付対象はドキュメント、ジョブといったオブジェクトである。
24	問い合わせ	問い合わせ内容。種類を問わず、問い合わせ内容の取得に使用する。セキュリティ監視対策として、実際の問い合わせを知ることは大変重要である。
25	データソース	合致する役割が他にない場合はデータの源または起点。
26	処理要素	当イベントの一環としてデータを作成、分析、修正、操作するデータ処理要素。

A.5.3 DICOM 固有の監査メッセージ

次のサブセクションは、メッセージ特殊化を定義する。これは DICOM 監査証跡プロファイルへの適合を主張する実装により使用される。次の表で特記されないフィールド（つまり、XML 要素および関連する属性）は、A.5.1 および A.5.2 の中で指定された規約に従わなければならない。

このプロファイルへの適合を主張する実装で、このプロファイルにより定義された監査メッセージの1つでカバーされる活動を報告するものは、このプロファイルに定義されたメッセージフォーマットを使用しなければならない。しかしながら、このプロファイルへの適合を主張するシステムは、その監査メッセージによって報告された活動が生じる度ごとにメッセージを送るようには要求されない。期待されることは、監査メッセージのトリガーが個別基準で構成可能であり、ネットワーク負荷対脅威の厳しさの平衡を、ローカルのセキュリティポリシーに従って保つことである。

注

- どのエンティティが実際に監査のイベントをいつ送るかは、DICOM の範囲外のシステム設計問題である。例えば、問い合わせメッセージを作成するのは、問い合わせに結局応答するエンティティにより問い合わせが作成される場合のエンティティ、または問い合わせに直接関連しないモニタリングエンティティである。しかしそれは、モニタされたネットワークトラフィックに基いた監査メッセージを作成する。
- ここで記述したイベントに似ているイベントを報告するため、これらの定義はスキーマを拡張する根拠として使用できる。

以降の諸表で、情報エンティティカラムが示すのは、実世界エンティティと、メッセージヘコード化された情報要素との関係である。

A.5.3.1 アプリケーション活動

この監査メッセージは、応用エンティティの開始または停止のイベントについて記述する。これは、どんな種類のアプリケーションの開始またはシャットダウンの、より一般的な場合にも密接な関係があり、それらの目的にも適しているかもしれない。

表 A.5.3.1-1. アプリケーション活動メッセージ

実世界エンティティ	フィールド名	オプション性	値の制約
イベント	EventID	M	EV(110100, DCM, " Application Activity")
	EventActionCode	M	列挙値 E = Execute
	EventDateTime	M	規定されていない
	EventOutcomeIndicator	M	規定されていない
	EventTypeCode	M	DT (110120, DCM, " Application Start ") DT (110121, DCM, " Application Stop ")
活発な参加者： アプリケーション開始 済み (1)	UserID	M	開始または停止のプロセスの識別は、A.5.2.1 の中で明記されるようにフォーマットされる。
	AlternativeUserID	MC	プロセスが DICOM をサポートする場合、AE タイトルは A.5.2.2 の中で明記されたようになる。
	UserName	U	規定されていない
	UserIsRequestor	M	規定されていない
	RoleIDCode	M	EV (110150, DCM, " Application ")
	NetworkAccessPointTypeCode	U	規定されていない
	NetworkAccessPointID	U	規定されていない
活発な参加者： アプリケーションを開 始した人またはプロセ ス (0.. N)	UserID	M	アプリケーションを始めるか停止する人またはプロセス
	AlternativeUserID	U	規定されていない
	UserName	U	規定されていない
	UserIsRequestor	M	規定されていない
	RoleIDCode	M	EV (110151, DCM, " Application Launcher ")
	NetworkAccessPointTypeCode	U	規定されていない
	NetworkAccessPointID	U	規定されていない

参加者オブジェクトはこのメッセージに必要とされない。

A.5.3.2 監査ログの使用

このメッセージは、監査証跡情報のログを読む人またはプロセスのイベントについて記述する。

注

例えば、監査情報のローカルキャッシュを維持する実装であって、情報が中央の収集ポイントに転送されなかった場合、ローカルキャッシュがユーザーによってアクセスされるならば、実装はこのメッセージを作成するかもしれない。

表 A.5.3.2-1. 監査ログ使用のメッセージ

実世界エンティティ	フィールド名	オプション性	値の制約
イベント	EventID	M	EV (110101, DCM, "Audit Log Used")
	EventActionCode	M	列挙値でなければならない： R = read
	EventDateTime	M	規定されていない
	EventOutcomeIndicator	M	規定されていない
	EventTypeCode	U	規定されていない
活発な参加者： アプリケーションを開始した人またはプロセス (1..2)	UserID	M	監査証跡にアクセスする人またはプロセス。両方が既知の場合、2つの活発な参加者が含まなければならない (人とプロセスの両方)。
	AlternativeUserID	U	規定されていない
	UserName	U	規定されていない
	UserIsRequestor	M	規定されていない
	RoleIDCode	U	規定されていない
	NetworkAccessPointTypeCode	U	規定されていない
	NetworkAccessPointID	U	規定されていない
参加オブジェクト： 監査ログの ID (1)	ParticipantObjectTypeCode	M	次のとおりでなければならない：2 = システム
	ParticipantObjectTypeCodeRole	M	次のとおりでなければならない：13 = セキュリティリソース
	ParticipantObjectDataLifeCycle	U	規定されていない
	ParticipantObjectIDTypeCode	M	次のとおりでなければならない：12 = URI
	ParticipantObjectSensitivity	U	規定されていない
	ParticipantObjectID	M	監査ログの URI
	ParticipantObjectName	U	次のとおりでなければならない：" Security Audit Log "
	ParticipantObjectQuery	U	規定されていない
	ParticipantObjectDetail	U	規定されていない
	ParticipantObjectDescription	U	規定されていない
	SOPClass	U	セクション A.5.2 を参照
	Accession	U	セクション A.5.2 を参照
	NumberOfInstances	U	セクション A.5.2 を参照
	Instances	U	セクション A.5.2 を参照
	Encrypted	U	セクション A.5.2 を参照
	Anonymized	U	セクション A.5.2 を参照
ParticipantObjectContainsStudy	U	セクション A.5.2 を参照	

A.5.3.3 DICOM インスタンスの転送を開始する

このメッセージは、あるノードから別のノードまで、システムのセキュリティ領域の管理内で、システムが1セットの DICOM インスタンスの転送を開始するイベントを記述する。このメッセージは、単に1人の患者に関する情報を含むかもしれない。

注

別の Instances Transferred メッセージが、転送完了のために定義される。したがって、送られるべく意図されたものと、実際に送られたものとを比較できる。

表 A.5.3.3-1. DICOM インスタンスの転送を開始するための監査メッセージ

実世界エンティティ	フィールド名	オプション性	値の制約
イベント	EventID	M	EV (110102, DCM, " Begin Transferring DICOM Instances ")
	EventActionCode	M	次のとおりでなければならない : E = Execute
	EventDateTime	M	規定されていない
	EventOutcomeIndicator	M	規定されていない
	EventTypeCode	U	規定されていない
活発な参加者 : データ送信プロセス (1)	UserID	M	データを送るプロセスの ID
	AlternativeUserID	U	規定されていない
	UserName	U	規定されていない
	UserIsRequestor	M	規定されていない
	RoleIDCode	M	EV (110153, DCM, " Source Role ID ")
	NetworkAccessPointTypeCode	U	規定されていない
	NetworkAccessPointID	U	規定されていない
活発な参加者 : データ受信プロセス (1)	UserID	M	データを受け取るプロセスの ID
	AlternativeUserID	U	規定されていない
	UserName	U	規定されていない
	UserIsRequestor	M	規定されていない
	RoleIDCode	M	EV (110152, DCM, "Destination Role ID")
	NetworkAccessPointTypeCode	U	規定されていない
	NetworkAccessPointID	U	規定されていない
活発な参加者 : 他の参加者 (0..N)	UserID	M	深く関わり合っただけ既知かもしれない他の参加者の ID, 特に要求者である第三者の ID
	AlternativeUserID	U	規定されていない
	UserName	U	規定されていない
	UserIsRequestor	M	規定されていない
	RoleIDCode	U	規定されていない
	NetworkAccessPointTypeCode	U	規定されていない
	NetworkAccessPointID	U	規定されていない
参加オブジェクト : 転送中のスタディ (1..N)	ParticipantObjectTypeCode	M	次のとおりでなければならない : 2 = システム
	ParticipantObjectTypeCodeRole	M	次のとおりでなければならない : 3 = 報告書
	ParticipantObjectDataLifeCycle	U	規定されていない
	ParticipantObjectIDTypeCode	M	EV (110180, DCM, "Study Instance UID")
	ParticipantObjectSensitivity	U	規定されていない
	ParticipantObjectID	M	スタディインスタンス UID
	ParticipantObjectName	U	規定されていない
	ParticipantObjectQuery	U	規定されていない
	ParticipantObjectDetail	U	1 つ以上の SOP クラス UID 値をもつ要素 「ContainsSOPClass」
	ParticipantObjectDescription	U	規定されていない
	SOPClass	MC	規定されていない

実世界エンティティ	フィールド名	オプション性	値の制約
	Accession	U	規定されていない
	NumberOfInstances	U	規定されていない
	Instances	U	規定されていない
	Encrypted	U	規定されていない
	Anonymized	U	規定されていない
参加オブジェクト： 患者 (1)	ParticipantObjectTypeCode	M	次のとおりでなければならない：1 = 個人
	ParticipantObjectTypeCodeRole	M	次のとおりでなければならない：1 = 患者
	ParticipantObjectDataLifeCycle	U	規定されていない
	ParticipantObjectIDTypeCode	M	次のとおりでなければならない：2 = 患者 ID
	ParticipantObjectSensitivity	U	規定されていない
	ParticipantObjectID	M	患者 ID
	ParticipantObjectName	U	患者の名前
	ParticipantObjectQuery	U	規定されていない
	ParticipantObjectDetail	U	規定されていない
	ParticipantObjectDescription	U	規定されていない

A.5.3.4 データの書き出し

このメッセージは、データがシステムのセキュリティ領域の管理から離れることを意味するシステムからデータの書き出しをするイベントを記述する。書き出しの例は、紙への印刷、フィルムへの記録、別のフォーマットへの転換による EHR 内の保存、取外し可能な媒体への書き込み、または電子メールによる送信である。多くの患者を 1 つのイベントメッセージ中で記述してもよい。

表 A.5.3.4-1. データ書き出しのための監査メッセージ

実世界エンティティ	フィールド名	オプション性	値の制約
イベント	EventID	M	EV (110106, DCM, "Export")
	EventActionCode	M	次のとおりでなければならない：R = Read
	EventDateTime	M	規定されていない
	EventOutcomeIndicator	M	規定されていない
	EventTypeCode	U	規定されていない
活発な参加者： リモートユーザーおよび プロセス (0..n)	UserID	M	データを受け取る遠隔のユーザーまたはプロセスの ID
	AlternativeUserID	U	規定されていない
	UserName	U	規定されていない
	UserIsRequestor	M	セクション A.5.3.4.1 を参照
	RoleIDCode	M	EV (110152, DCM, "Destination Role ID")
	NetworkAccessPointTypeCode	U	規定されていない
NetworkAccessPointID	U	規定されていない	

実世界エンティティ	フィールド名	オプション性	値の制約
活発な参加者： データの書き出しをする ユーザーまたはプロセス (1..2)	UserID	M	データの書き出しをするローカルユーザーまたはプロセスの ID。両方が既知の場合、2つの活発な参加者が含まなければならない（人とプロセスの両方）。
	AlternativeUserID	U	規定されていない
	UserName	U	規定されていない
	UserIsRequestor	M	セクション A.5.3.4.1 を参照
	RoleIDCode	M	EV (110153, DCM, " Source Role ID ")
	NetworkAccessPointTypeCode	U	規定されていない
	NetworkAccessPointID	U	規定されていない
活発な参加者： 媒体 (1)	UserID	M	セクション A.5.2.3 を参照
	AlternativeUserID	U	セクション A.5.2.4 を参照
	UserName	U	規定されていない
	UserIsRequestor	M	FALSE でなければならない
	RoleIDCode	M	EV (110154, DCM, "Destination Media")
	NetworkAccessPointTypeCode	MC	物理的な媒体以外に書き出しされる場合、例えば、目的地がネットワークであり、フィルム、紙または CD ではない場合に、要求される。そうでなければ存在してもよい。
	NetworkAccessPointID	MC	ネットワークアクセスポイントタイプコードが存在する場合に要求される。そうでなければ存在してもよい。
	MediaIdentifier	MC	ボリューム ID、URI または媒体用の他の ID。 デジタル媒体である場合に要求される。そうでなければ存在してもよい。
Media Type	M	DCID 405 "Media Type Code"から選ばれた値	
参加オブジェクト： スタディ (0..N)	ParticipantObjectTypeCode	M	次のとおりでなければならない：2 = システム
	ParticipantObjectTypeCodeRole	M	次のとおりでなければならない：3 = 報告書
	ParticipantObjectDataLifeCycle	U	規定されていない
	ParticipantObjectIDTypeCode	M	EV (110180, DCM, "Study Instance UID")
	ParticipantObjectSensitivity	U	規定されていない
	ParticipantObjectID	M	スタディインスタンス UID
	ParticipantObjectName	U	規定されていない
	ParticipantObjectQuery	U	規定されていない
	ParticipantObjectDetail	U	規定されていない
	ParticipantObjectDescription	U	規定されていない
	SOPClass	MC	表 A.5.2-1 を参照
	Accession	U	規定されていない
	NumberOfInstances	U	規定されていない
	Instances	U	規定されていない
	Encrypted	U	規定されていない
Anonymized	U	規定されていない	
参加オブジェクト： 患者 (1..N)	ParticipantObjectTypeCode	M	次のとおりでなければならない：1 = 個人
	ParticipantObjectTypeCodeRole	M	次のとおりでなければならない：1 = 患者
	ParticipantObjectDataLifeCycle	U	規定されていない
	ParticipantObjectIDTypeCode	M	次のとおりでなければならない：2 = 患者 ID

実世界エンティティ	フィールド名	オプション性	値の制約
	ParticipantObjectSensitivity	U	規定されていない
	ParticipantObjectID	M	患者 ID
	ParticipantObjectName	U	患者の名前
	ParticipantObjectQuery	U	規定されていない
	ParticipantObjectQuery	U	規定されていない
	ParticipantObjectDetail	U	規定されていない
	ParticipantObjectDescription	U	規定されていない

A.5.3.4.1 UserIsRequestor

1人のユーザー（ローカルかまたは遠隔の）は要求者であると確認されなければならない。つまり UserIsRequestor であり、TRUE の値をもたなければならない。これによりプッシュブルの転送モデルを媒体のために受け入れる。

A.5.3.5 データの読み込み

このメッセージは、今システムを入力しているデータはこの組織のセキュリティ領域の管理下になかったことを暗示する、データの組織への読み込みイベントを記述する。組織内の媒体による転送は、データ読み込みのイベントというよりはむしろ、データ転送としてしばしば考えられる。読み込みの例は、データから新しいローカルのインスタンスを、取外し可能な媒体上に作成することである。多くの患者を1つのイベントメッセージ中で記述してもよい。

1人のユーザー（ローカルかまたは遠隔の）は要求者であると確認されなければならない。つまり UserIsRequestor であり、TRUE の値をもたなければならない。これによりプッシュブルの転送モデルを媒体のために受け入れる。

表 A.5.3.5-1. データ読み込みのための監査メッセージ

実世界エンティティ	フィールド名	オプション性	値の制約
イベント	EventID	M	EV (110107, DCM, "Import")
	EventActionCode	M	次のとおりでなければならない： C = Create
	EventDateTime	M	規定されていない
	EventOutcomeIndicator	M	規定されていない
	EventTypeCode	U	規定されていない
活発な参加者： データの読み込みをするユーザーまたはプロセス (1..n)	UserID	M	データの読み込みをするローカルユーザーかプロセスの ID
	AlternativeUserID	U	規定されていない
	UserName	U	規定されていない
	UserIsRequestor	M	セクション A.5.3.5 を参照
	RoleIDCode	M	EV (110152, DCM, "Destination Role ID")
	NetworkAccessPointTypeCode	U	規定されていない
	NetworkAccessPointID	U	規定されていない
活発な参加者： ソース媒体 (1)	UserID	M	セクション A.5.2.3 を参照
	AlternativeUserID	U	セクション A.5.2.4 を参照
	UserName	U	規定されていない
	UserIsRequestor	M	FALSE でなければならない
	RoleIDCode	M	EV (110155, DCM, " Source Media ")
	NetworkAccessPointTypeCode	U	規定されていない

実世界エンティティ	フィールド名	オプション性	値の制約
	NetworkAccessPointID	MC	正味のアクセスポイントタイプコードが存在する場合、存在しなければならない。
	MediaIdentifier	M	ボリューム ID, URI または媒体用の他の ID。
	MediaType	M	DCID 405 “媒体タイプコード”から選ばれた値
活発な参加者 : ソース (0..n)	UserID	M	セクション A.5.2.3 を参照
	AlternativeUserID	U	セクション A.5.2.4 を参照
	UserName	U	規定されていない
	UsersRequestor	M	セクション A.5.3.5 を参照
	RoleIDCode	M	EV (110153, DCM, " Source Role ID ")
	NetworkAccessPointTypeCode	U	規定されていない
	NetworkAccessPointID	MC	正味のアクセスポイントタイプコードが存在する場合、存在しなければならない。
参加オブジェクト : スタディ (0..N)	ParticipantObjectTypeCode	M	次のとおりでなければならない : 2 = システム
	ParticipantObjectTypeCodeRole	M	次のとおりでなければならない : 3 = 報告書
	ParticipantObjectDataLifeCycle	U	規定されていない
	ParticipantObjectIDTypeCode	M	EV (110180, DCM, "Study Instance UID")
	ParticipantObjectSensitivity	U	規定されていない
	ParticipantObjectID	M	スタディインスタンス UID
	ParticipantObjectName	U	規定されていない
	ParticipantObjectQuery	U	規定されていない
	ParticipantObjectDetail	U	規定されていない
	ParticipantObjectDescription	U	規定されていない
	SOPClass	MC	表 A.5.2-1 を参照
	Accession	U	規定されていない
	NumberOfInstances	U	規定されていない
	Instances	U	規定されていない
	Encrypted	U	規定されていない
Anonymized	U	規定されていない	
参加オブジェクト : 患者 (1..N)	ParticipantObjectTypeCode	M	次のとおりでなければならない : 1 = 個人
	ParticipantObjectTypeCodeRole	M	次のとおりでなければならない : 1 = 患者
	ParticipantObjectDataLifeCycle	U	規定されていない
	ParticipantObjectIDTypeCode	M	次のとおりでなければならない : 2 = 患者 ID
	ParticipantObjectSensitivity	U	規定されていない
	ParticipantObjectID	M	患者 ID
	ParticipantObjectName	U	患者の名前
	ParticipantObjectQuery	U	規定されていない
	ParticipantObjectDetail	U	規定されていない
ParticipantObjectDescription	U	規定されていない	

A.5.3.6 アクセスされた DICOM インスタンス

このメッセージは、DICOM SOP インスタンスが観察、利用、更新、または削除されるメッセージを記述する。このメッセージは、単に1人の患者に関する情報を含まなければならない。またその患者のためのいくつかのスタディ活動をすべて要約するために使用できる。このメッセージは、インスタンスが属するスタディを記録するが、個々のインスタンスは記録しない。

スタディ内のインスタンスがすべて削除される場合、EV(110105, DCM, "DICOM Study Deleted")イベントが使用されなければならない。セクション A.5.3.8 を参照。

表 A.5.3.6-1. DICOM インスタンスへのアクセスのための監査メッセージ

実世界エンティティ	フィールド名	オプション性	値の制約
イベント	EventID	M	EV (110103, DCM, " DICOM Instances Accessed ")
	EventActionCode	M	列挙値 : C = create R = read U = update D = delete
	EventDateTime	M	規定されていない
	EventOutcomeIndicator	M	規定されていない
	EventTypeCode	U	規定されていない
	活発な参加者 : データを操作する人および (または) プロセス (1..2)	UserID	M
	AlternativeUserID	U	規定されていない
	UserName	U	規定されていない
	UserIsRequestor	M	規定されていない
	RoleIDCode	U	規定されていない
	NetworkAccessPointTypeCode	U	規定されていない
	NetworkAccessPointID	U	規定されていない
参加オブジェクト : スタディ (1..N)	ParticipantObjectTypeCode	M	次のとおりでなければならない : 2 = システム
	ParticipantObjectTypeCodeRole	M	次のとおりでなければならない : 3 = 報告書
	ParticipantObjectDataLifeCycle	U	規定されていない
	ParticipantObjectIDTypeCode	M	EV (110180, DCM, "Study Instance UID")
	ParticipantObjectSensitivity	U	規定されていない
	ParticipantObjectID	M	スタディインスタンス UID
	ParticipantObjectName	U	規定されていない
	ParticipantObjectQuery	U	規定されていない
	ParticipantObjectDetail	U	規定されていない
	ParticipantObjectDescription	U	規定されていない
	SOPClass	MC	表 A.5.2-1 を参照
	Accession	U	規定されていない
	NumberOfInstances	U	規定されていない
	Instances	U	規定されていない
	Encrypted	U	規定されていない
	Anonymized	U	規定されていない

実世界エンティティ	フィールド名	オプション性	値の制約
参加オブジェクト： 患者 (1)	ParticipantObjectTypeCode	M	次のとおりでなければならない：1 = 個人
	ParticipantObjectTypeCodeRole	M	次のとおりでなければならない：1 = 患者
	ParticipantObjectDataLifeCycle	U	規定されていない
	ParticipantObjectIDTypeCode	M	次のとおりでなければならない：2 = 患者 ID
	ParticipantObjectSensitivity	U	規定されていない
	ParticipantObjectID	M	患者 ID
	ParticipantObjectName	U	患者の名前
	ParticipantObjectQuery	U	規定されていない
	ParticipantObjectDetail	U	規定されていない
	ParticipantObjectDescription	U	規定されていない

A.5.3.7 転送された DICOM インスタンス

このメッセージが記述するのは、DICOM SOP インスタンスの転送が2つの応用エンティティ間で完了したイベントである。このメッセージは、単に1人の患者に関する情報を含むかもしれない。

注

このインスタンスメッセージに先行して「インスタンスの転送を始める」メッセージがあるかもしれない。「インスタンスの転送を始める」メッセージは SOP インスタンスを保存する意図を伝える。その一方で「転送されたインスタンス」メッセージは、転送の完成を記録する。何らかの不一致が2つのメッセージ間にあると、機密漏洩の可能性がある。

表 A.5.3.7-1. DICOM インスタンスの転送のための監査メッセージ

実世界エンティティ	フィールド名	オプション性	値の制約
イベント	EventID	M	EV (110104, DCM, " DICOM Instances Transferred ")
	EventActionCode	M	列挙値： 受け取り手が転送されたインスタンスのコピーを保持していなかった場合は C = (create : 作成) 受け取り手が転送された SOP インスタンスのコピーをすでに保持しており、そのコピーに変更は不要と判断している場合は R = (read : 読み込み) 保持しているコピーと受け取ったコピーとの差異を調整するため保持しているコピーを変更する場合は U = (update : 更新) 監査ソースが受け取り手ではない、またはインスタンスがかつて受け取りノードで保持されていたか不明である場合は R = (Read : 読み込み) を使用する。
	EventDateTime	M	転送が完了した時でなければならない
	EventOutcomeIndicator	M	規定されていない
	EventTypeCode	U	規定されていない

実世界エンティティ	フィールド名	オプション性	値の制約
活発な参加者 : データを送ったプロセス (1)	UserID	M	規定されていない
	AlternativeUserID	U	規定されていない
	UserName	U	規定されていない
	UserIsRequestor	M	規定されていない
	RoleIDCode	M	EV (110153, DCM, " Source Role ID ")
	NetworkAccessPointTypeCode	U	規定されていない
	NetworkAccessPointID	U	規定されていない
活発な参加者 : データを受け取ったプロセス (1)	UserID	M	規定されていない
	AlternativeUserID	U	規定されていない
	UserName	U	規定されていない
	UserIsRequestor	M	規定されていない
	RoleIDCode	M	EV (110152, DCM, " Destination Role ID ")
	NetworkAccessPointTypeCode	U	規定されていない
	NetworkAccessPointID	U	規定されていない
活発な参加者 : 他の既知の参加者, 特に 要求者である第三者 (0..N)	UserID	M	規定されていない
	AlternativeUserID	U	規定されていない
	UserName	U	規定されていない
	UserIsRequestor	M	規定されていない
	RoleIDCode	U	規定されていない
	NetworkAccessPointTypeCode	U	規定されていない
	NetworkAccessPointID	U	規定されていない
参加オブジェクト : 転送中のスタディ (1..N)	ParticipantObjectTypeCode	M	次のとおりでなければならない : 2 = システム
	ParticipantObjectTypeCodeRole	M	次のとおりでなければならない : 3 = 報告書
	ParticipantObjectDataLifeCycle	U	規定されていない
	ParticipantObjectIDTypeCode	M	EV (110180, DCM, "Study Instance UID")
	ParticipantObjectSensitivity	U	規定されていない
	ParticipantObjectID	M	スタディインスタンス UID
	ParticipantObjectName	U	規定されていない
	ParticipantObjectQuery	U	規定されていない
	ParticipantObjectDetail	U	規定されていない
	ParticipantObjectDescription	U	規定されていない
	SOPClass	MC	表 A.5.2-1 を参照
	Accession	U	規定されていない
	NumberOfInstances	U	規定されていない
	Instances	U	規定されていない
	Encrypted	U	規定されていない
	Anonymized	U	規定されていない

実世界エンティティ	フィールド名	オプション性	値の制約
参加オブジェクト： 患者 (1)	ParticipantObjectTypeCode	M	次のとおりでなければならない：1 = 個人
	ParticipantObjectTypeCodeRole	M	次のとおりでなければならない：1 = 患者
	ParticipantObjectDataLifeCycle	U	規定されていない
	ParticipantObjectIDTypeCode	M	次のとおりでなければならない：2 = 患者 ID
	ParticipantObjectSensitivity	U	規定されていない
	ParticipantObjectID	M	患者 ID
	ParticipantObjectName	U	患者の名前
	ParticipantObjectQuery	U	規定されていない
	ParticipantObjectDetail	U	規定されていない
	ParticipantObjectDescription	U	規定されていない

A.5.3.8 削除された DICOM スタディ

このメッセージが記述するのは、1 つ以上のスタディおよびすべての関連する SOP インスタンスを単一の行為中に削除するイベントである。このメッセージは、単に 1 人の患者に関する情報を含まなければならない。

表 A.5.3.8-1. DICOM スタディの削除のための監査メッセージ

実世界エンティティ	フィールド名	オプション性	値の制約
イベント	EventID	M	EV (110105, DCM, " DICOM Study Deleted ")
	EventActionCode	M	次のとおりでなければならない：D=Delete
	EventDateTime	M	規定されていない
	EventOutcomeIndicator	M	規定されていない
	EventTypeCode	U	規定されていない
活発な参加者： スタディを削除する人またはプロセス (1..2)	UserID	M	規定されていない
	AlternativeUserID	U	規定されていない
	UserName	U	規定されていない
	UserIsRequestor	M	規定されていない
	RoleIDCode	U	規定されていない
	NetworkAccessPointTypeCode	U	規定されていない
	NetworkAccessPointID	U	規定されていない
参加オブジェクト： 転送中のスタディ (1..N)	ParticipantObjectTypeCode	M	次のとおりでなければならない：2 = システム
	ParticipantObjectTypeCodeRole	M	次のとおりでなければならない：3 = 報告書
	ParticipantObjectDataLifeCycle	U	規定されていない
	ParticipantObjectIDTypeCode	M	EV (110180, DCM, "Study Instance UID")
	ParticipantObjectSensitivity	U	規定されていない
	ParticipantObjectID	M	スタディインスタンス UID
	ParticipantObjectName	U	規定されていない
	ParticipantObjectQuery	U	規定されていない
	ParticipantObjectDetail	U	規定されていない
	ParticipantObjectDescription	U	規定されていない
SOPClass	MC	表 A.5.2-1 を参照	

実世界エンティティ	フィールド名	オプション性	値の制約
	Accession	U	規定されていない
	NumberOfInstances	U	規定されていない
	Instances	U	規定されていない
	Encrypted	U	規定されていない
	Anonymized	U	規定されていない
参加オブジェクト： 患者 (1)	ParticipantObjectTypeCode	M	次のとおりでなければならない：1 = 個人
	ParticipantObjectTypeCodeRole	M	次のとおりでなければならない：1 = 患者
	ParticipantObjectDataLifeCycle	U	規定されていない
	ParticipantObjectIDTypeCode	M	次のとおりでなければならない：2 = 患者 ID
	ParticipantObjectSensitivity	U	規定されていない
	ParticipantObjectID	M	患者 ID
	ParticipantObjectName	U	患者の名前
	ParticipantObjectQuery	U	規定されていない
	ParticipantObjectDetail	U	規定されていない
	ParticipantObjectDescription	U	規定されていない

A.5.3.9 ネットワークエントリ

このメッセージは、システム、例えばモバイルの装置が、ネットワークに故意に出入りするイベントを記述する。

注

機械は、分離前にこのメッセージを送ることを試みるのが望ましい。これが可能でない場合、機械は、後でそれを送ることができるようにするために、ローカルのバッファ中にメッセージを保持するのが望ましい。その後、モバイルの機械は、安全な領域外にある間、ローカルのバッファ中の監査メッセージを捕えることができる。機械が安全な領域に再度接続される場合、それは分離メッセージ（もしバッファされれば）を送ることができ、次にバッファされたメッセージ、次に安全な領域と再結合するためのモバイルの機械メッセージが続く。これらのメッセージ上のタイムスタンプは、イベントが生じたと気づかれた時であり、メッセージが送られる時ではない。

表 A.5.3.9-1. ネットワークエントリのための監査メッセージ

実世界エンティティ	フィールド名	オプション性	値
イベント	EventID	M	EV (110108, DCM, " Network Entry")
	EventActionCode	M	次のとおりでなければならない：E = Execute
	EventDateTime	M	規定されていない
	EventOutcomeIndicator	M	規定されていない
	EventTypeCode	M	EV (110124, DCM, " Attach ")EV (110125, DCM, " Detach ")
活発な参加者： ネットワークに出入りする ノードまたはシステム (1)	UserID	M	規定されていない
	AlternativeUserID	U	規定されていない
	UserName	U	規定されていない
	UserIsRequestor	M	FALSE でなければならない
	RoleIDCode	U	規定されていない
	NetworkAccessPointTypeCode	U	規定されていない
	NetworkAccessPointID	U	規定されていない

参加者オブジェクトはこのメッセージに必要とされない。

A.5.3.10 問い合わせ

このメッセージは、問い合わせが出されるかまたは受け取られるイベントを記述する。メッセージは、問い合わせに対する反応を記録せず、問い合わせが出されたという事実を単に記録する。例えば、これは DICOM SOP クラスを使用して、問い合わせを報告するだろう：

- a. モダリティワークリスト
- b. UPS プル
- c. UPS 監視
- d. 合成インスタンス問い合わせ

注

1. 問い合わせに対する反応は、どんなイベントが問い合わせ後に起きるかにより、1つ以上の Instances Transferred メッセージまたは Instances Accessed メッセージに帰着するかもしれない。もしセキュリティ関連の故障、例えば、アクセス違反が問い合わせの処理中に起きれば、それらの故障は他の監査メッセージ、例えば、SecurityAlert メッセージ中に現れることが望ましい。
2. 非 DICOM 問い合わせもこのメッセージによって捕えられるかもしれない。参加者オブジェクト ID タイプコード、参加者オブジェクト ID および問い合わせフィールドは、そのような非 DICOM 問い合わせと関係する値をもっているかもしれない。

表 A.5.3.10-1. 問い合わせのための監査メッセージ

実世界エンティティ	フィールド名	オプション性	値の制約
イベント	EventID	M	EV (110112, DCM, " Query ")
	EventActionCode	M	次のとおりでなければならない : E = Execute
	EventDateTime	M	規定されていない
	EventOutcomeIndicator	M	規定されていない
	EventTypeCode	U	規定されていない
活発な参加者 : 問い合わせ発行プロセス (1)	UserID	M	規定されていない
	AlternativeUserID	U	規定されていない
	UserName	U	規定されていない
	UserIsRequestor	M	規定されていない
	RoleIDCode	M	EV (110153, DCM, " Source Role ID ")
	NetworkAccessPointTypeCode	U	規定されていない
	NetworkAccessPointID	U	規定されていない
活発な参加者 : 問い合わせに対応するプロセス (1)	UserID	M	規定されていない
	AlternativeUserID	U	規定されていない
	UserName	U	規定されていない
	UserIsRequestor	M	規定されていない
	RoleIDCode	M	EV (110152, DCM, " Destination Role ID ")
	NetworkAccessPointTypeCode	U	規定されていない
	NetworkAccessPointID	U	規定されていない

実世界エンティティ	フィールド名	オプション性	値の制約
活発な参加者： 他の既知の参加者，特に問い合わせを要求した第三者 (0..N)	UserID	M	規定されていない
	AlternativeUserID	U	規定されていない
	UserName	U	規定されていない
	UserIsRequestor	M	規定されていない
	RoleIDCode	U	規定されていない
	NetworkAccessPointTypeCode	U	規定されていない
	NetworkAccessPointID	U	規定されていない
参加オブジェクト： 問い合わせされた SOP および問い合わせ (1)	ParticipantObjectTypeCode	M	次のとおりでなければならない：2 = システム
	ParticipantObjectTypeCodeRole	M	次のとおりでなければならない：3 = 報告書
	ParticipantObjectDataLifeCycle	U	規定されていない
	ParticipantObjectIDTypeCode	M	DT (110181, DCM, "SOP Class UID")
	ParticipantObjectSensitivity	U	規定されていない
	ParticipantObjectID	M	ParticipantObjectIDTypeCode が (110181, DCM, "SOP Class UID") である場合，このフィールドは問い合わせられている SOP クラスの UID を保持しなければならない。
	ParticipantObjectName	U	規定されていない
	ParticipantObjectQuery	M	ParticipantObjectIDTypeCode が (110181, DCM, "SOP Class UID") ある場合，このフィールドは DICOM 問い合わせのデータセット，xs:base64Binary encoded を保持しなければならない。そうでなければ，それは使用されるプロトコルのフォーマットでの問い合わせでなければならない。
	ParticipantObjectDetail	MC	ParticipantObjectIDTypeCode が (110181, DCM, "SOP Class UID") の場合，要求される。 XML 属性「TransferSyntax」を備えた ParticipantObjectDetail 要素が存在しなければならない。転送構文属性の値は問い合わせの転送構文の UID でなければならない。要素内容は xs:base64Binary encoding でなければならない。転送構文は DICOM 転送構文でなければならない。
	ParticipantObjectDescription	U	規定されていない
	SOPClass	U	表 A.5.2-1 を参照
	Accession	U	規定されていない
	NumberOfInstances	U	規定されていない
	Instances	U	規定されていない
	Encrypted	U	規定されていない
Anonymized	U	規定されていない	

A.5.3.11 セキュリティアラート

このメッセージは，ノードがそのためにセキュリティアラート体制，例えば，セキュア通信チャネルを確立する場合のノード認証失敗を報告する必要のあるあらゆるイベントについて記述する。

注

ノード認証のイベントは成功と失敗の両方を報告するために使用できる。成功の報告が終わる場合、すべての確認された DICOM アソシエーション、HL7 トランザクションおよび HTML 接続が成功したノード認証に帰着するに違いないので、これは非常に多くの監査メッセージを作成するかもしれない。ほとんどの状況で、失敗だけが報告されることが期待される。

表 A.5.3.11-1. セキュリティアラートのための監査メッセージ

実世界エンティティ	フィールド名	オプション性	値の制約
イベント	EventID	M	EV (110113, DCM, " Security Alert ")
	EventActionCode	M	次のとおりでなければならない : E = Execute
	EventDateTime	M	規定されていない
	EventOutcomeIndicator	M	成功は有益なアラート体制を意味する。他の失敗値は、アラートの厳しさを示す、警告するコードを意味する。軽微な失敗または深刻な失敗は、緩和努力がシステムセキュリティを維持するのに有効だったことを示す。重大な失敗は、緩和努力が有効でないかもしれないし、かつ、セキュリティシステムが危険にさらされたかもしれないことを示す。
	EventTypeCode	M	DCID 403 "Security Alert Type Code"から選ばれた値。
活発な参加者 : 報告する人および/ またはプロセス (1..2)	UserID	M	規定されていない
	AlternativeUserID	U	規定されていない
	UserName	U	規定されていない
	UsersRequestor	M	規定されていない
	RoleIDCode	U	規定されていない
	NetworkAccessPointTypeCode	U	規定されていない
	NetworkAccessPointID	U	規定されていない
活発な参加者 : 行う人またはプロセス (0..N)	UserID	M	規定されていない
	AlternativeUserID	U	規定されていない
	UserName	U	規定されていない
	UsersRequestor	M	FALSE でなければならない
	RoleIDCode	U	規定されていない
	NetworkAccessPointTypeCode	U	規定されていない
	NetworkAccessPointID	U	規定されていない
参加オブジェクト : アラートサブジェクト (0..N)	ParticipantObjectTypeCode	M	次のとおりでなければならない : 2 = システム
	ParticipantObjectTypeCodeRole	U	定義語 : 5 = master file 13 = security resource
	ParticipantObjectDataLifeCycle	U	規定されていない
	ParticipantObjectIDTypeCode	M	定義語 : 12 = URI(110182, DCM, "Node ID") = ノード ID
	ParticipantObjectSensitivity	U	規定されていない

実世界エンティティ	フィールド名	オプション性	値の制約
	ParticipantObjectID	M	12 (URI) の ParticipantObjectTypeCode については、その後、この値は、アラートの主題であるファイルまたは他のリソースの URI でなければならない。 (110182, DCM, "Node ID ") の ParticipantObjectTypeCode については、その後、値は、node_name@domain_name の形をしているアラート、または IP アドレスとしてのアラートのいずれかの主題であるノードの ID を含まなければならない。 そうでなければ、値は、アラートの主題の ParticipantObjectTypeCode によって指定されたタイプの ID でなければならない。
	ParticipantObjectName	U	規定されていない
	ParticipantObjectQuery	U	規定されていない
	ParticipantObjectDetail	M	「アラート概要」と等しい属性「タイプ」を備えた要素は、値としてアラートの性質の自由なテキスト性状で存在しなければならない。
	ParticipantObjectDescription	U	規定されていない
	SOPClass	U	表 A.5.2-1 を参照
	Accession	U	規定されていない
	NumberOfInstances	U	規定されていない
	Instances	U	規定されていない
	Encrypted	U	規定されていない
	Anonymized	U	規定されていない

A.5.3.12 ユーザー認証

このメッセージは、ユーザーがログオンまたはログオフを試みたイベントを記述する。この報告は試みが成功したか否かにかかわらず行うことができる。参加者オブジェクトはこのメッセージに必要とされない。

注

ユーザーは通常 UserIsRequestor TRUE をもっている。しかし、ログアウトタイマーの場合、ノードは UserIsRequestor であるかもしれない。

表 A.5.3.12-1. ユーザー認証のための監査メッセージ

実世界エンティティ	フィールド名	オプション性	値の制約
イベント	EventID	M	EV (110114, DCM, "User Authentication")
	EventActionCode	M	次のとおりでなければならない : E = Execute
	EventDateTime	M	規定されていない
	EventOutcomeIndicator	M	規定されていない
	EventTypeCode	M	定義語 : EV (110122, DCM, "Login") EV (110123, DCM, "Logout")

実世界エンティティ	フィールド名	オプション性	値の制約
活発な参加者： 認証または要求された人 (1)	UserID	M	規定されていない
	AlternativeUserID	U	規定されていない
	UserName	U	規定されていない
	UserIsRequestor	M	規定されていない
	RoleIDCode	U	規定されていない
	NetworkAccessPointTypeCode	M	規定されていない
	NetworkAccessPointID	M	規定されていない
活発な参加者： 認証を行うノードまたはシステム (0..1)	UserID	M	規定されていない
	AlternativeUserID	U	規定されていない
	UserName	U	規定されていない
	UserIsRequestor	M	規定されていない
	RoleIDCode	U	規定されていない
	NetworkAccessPointTypeCode	U	規定されていない
	NetworkAccessPointID	U	規定されていない

A.5.3.13 オーダーレコード

このメッセージは作成中、修正中、アクセス中、または削除中のオーダーのイベントについて記述する。このメッセージは、単に1人の患者に関する情報を含むかもしれない。

注

オーダーレコードは一般に非 DICOM システムが管理する。ただし、DICOM アプリケーションはしばしばオーダーレコードを操作するため、監査ログにそのようなイベントを記録するようサイトセキュリティ方針にて義務付けてもよい。

表 A.5.3.13-1. オーダーレコードのための監査メッセージ

実世界エンティティ	フィールド名	オプション性	値の制約
イベント	EventID	M	EV (110109, DCM, "Order Record")
	EventActionCode	M	列挙値： C = create R = read U = update D = delete
	EventDateTime	M	規定されていない
	EventOutcomeIndicator	M	規定されていない
	EventTypeCode	U	規定されていない
	ユーザー (1..2)	UserID	M
AlternateUserID		U	規定されていない
UserName		U	規定されていない
UserIsRequestor		U	規定されていない

実世界エンティティ	フィールド名	オプション性	値の制約
	RoleIDCode	U	規定されていない
	NetworkAccessPointTypeCode	U	規定されていない
	NetworkAccessPointID	U	規定されていない
患者 (1)	ParticipantObjectTypeCode	M	EV 1 (個人)
	ParticipantObjectTypeCodeRole	M	EV 1 (患者)
	ParticipantObjectDataLifeCycle	U	規定されていない
	ParticipantObjectIDTypeCode	M	EV 2 (患者 ID)
	ParticipantObjectSensitivity	U	規定されていない
	ParticipantObjectID	M	患者 ID
	ParticipantObjectName	U	患者の名前
	ParticipantObjectQuery	U	規定されていない
	ParticipantObjectDetail	U	規定されていない
	ParticipantObjectDescription	U	これ以上規定なし

A.5.3.14 患者レコード

このメッセージは作成中、修正中、アクセス中、または削除中の患者レコードのイベントについて記述する。

注

DICOM および非 DICOM システムの両方が管理する患者レコードにはいくつかの種類がある。DICOM アプリケーションはあらゆるシステムが管理する患者レコードをしばしば操作するため、監査ログにそのようなイベントを記録するようサイトセキュリティ方針にて義務付けてもよい。特定の DICOM SOP インスタンスが関与しない患者レコードのアクセスまたは操作を記録するのにこの監査イベントを使用することができる。

表 A.5.3.14-1. 患者レコードのための監査メッセージ

実世界エンティティ	フィールド名	オプション性	値の制約
イベント	EventID	M	EV (110110, DCM, "Patient Record")
	EventActionCode	M	列挙値 : C = create R = read U = update D = delete
	EventDateTime	M	規定されていない
	EventOutcomeIndicator	M	規定されていない
	EventTypeCode	U	規定されていない
ユーザー (1..2)	UserID	M	データを操作する人またはプロセスの ID 両方が既知の場合、2つの活発な参加者が含まなければならない (人とプロセスの両方)。
	AlternateUserID	U	規定されていない

実世界エンティティ	フィールド名	オプション性	値の制約
	UserName	U	規定されていない
	UserIsRequestor	U	規定されていない
	RoleIDCode	U	規定されていない
	NetworkAccessPointTypeCode	U	規定されていない
	NetworkAccessPointID	U	規定されていない
患者 (1)	ParticipantObjectTypeCode	M	EV 1 (個人)
	ParticipantObjectTypeCodeRole	M	EV 1 (患者)
	ParticipantObjectDataLifeCycle	U	規定されていない
	ParticipantObjectIDTypeCode	M	EV 2 (患者 ID)
	ParticipantObjectSensitivity	U	規定されていない
	ParticipantObjectID	M	患者 ID
	ParticipantObjectName	U	患者の名前
	ParticipantObjectQuery	U	規定されていない
	ParticipantObjectDetail	U	規定されていない
	ParticipantObjectDescription	U	これ以上規定なし

A.5.3.15 手続きレコード

このメッセージは作成中、アクセス中、修正中、アクセス中または削除中の手続きレコードのイベントについて記述する。このメッセージは、単に 1 人の患者に関する情報を含むかもしれない。

注

- DICOM アプリケーションは MPPS 更新等でしばしば手続きレコードを操作する。モダリティワークリストの問い合わせイベントは問い合わせイベントメッセージにて記述される。
- 同一の受入番号が複数のオーダー番号と共に表示される場合もある。そのような多対多の関係を取得するためスタディ参加者フィールドまたは全体メッセージが繰り返されることもある。

表 A.5.3.15-1. 手続きレコードのための監査メッセージ

実世界エンティティ	フィールド名	オプション性	値の制約
イベント	EventID	M	EV (110111, DCM, "Procedure Record")
	EventActionCode	C	列挙値 : C = create R = read U = update D = delete
	EventDateTime	M	規定されていない
	EventOutcomeIndicator	M	規定されていない
	EventTypeCode	U	規定されていない

実世界エンティティ	フィールド名	オプション性	値の制約
ユーザー (1..2)	UserID	M	データを操作する人またはプロセスの ID 両方が既知の場合、2つの活発な参加者が含まれなければならない (人とプロセスの両方)。
	AlternateUserID	U	規定されていない
	UserName	U	規定されていない
	UserIsRequestor	U	規定されていない
	RoleIDCode	U	規定されていない
	NetworkAccessPointTypeCode	U	規定されていない
	NetworkAccessPointID	U	規定されていない
スタディ (0..N)	ParticipantObjectTypeCode	M	EV 2 (システム)
	ParticipantObjectTypeCodeRole	M	EV 3 (報告書)
	ParticipantObjectDataLifeCycle	U	規定されていない
	ParticipantObjectIDTypeCode	M	EV (110180, DCM, "Study Instance UID")
	ParticipantObjectSensitivity	U	規定されていない
	ParticipantObjectID	M	スタディインスタンス UID
	ParticipantObjectName	U	規定されていない
	ParticipantObjectQuery	U	規定されていない
	ParticipantObjectDetail	U	これ以上規定なし
	ParticipantObjectDescription	U	これ以上規定なし
	SOPClass	MC	これ以上規定なし
	Accession	U	これ以上規定なし
	NumberOfInstances	U	これ以上規定なし
	Instances	U	これ以上規定なし
	Encrypted	U	これ以上規定なし
Anonymized	U	これ以上規定なし	
患者 (1)	ParticipantObjectTypeCode	M	EV 1 (個人)
	ParticipantObjectTypeCodeRole	M	EV 1 (患者)
	ParticipantObjectDataLifeCycle	U	規定されていない
	ParticipantObjectIDTypeCode	M	EV 2 (患者 ID)
	ParticipantObjectSensitivity	U	規定されていない
	ParticipantObjectID	M	患者 ID
	ParticipantObjectName	U	患者の名前
	ParticipantObjectQuery	U	規定されていない
	ParticipantObjectDetail	U	規定されていない
	ParticipantObjectDescription	U	これ以上規定なし

A.6 監査証跡メッセージ送信プロファイル—SYSLOG-TLS

このプロファイルは、監査証跡メッセージの送信を定義する。Syslog (RFC5425) のためのトランスポート層セキュリティ (TLS) トランスポート写像は、信頼できるトランスポート、バッファリング、認識、認証、識別および暗号化のためのメカニズムを提供する。RFC5424 は、使用される TLS は、TLS のバージョン 1.2 で「なければならない」と述べる。この DICOM プロファイルのためには、TLS が使用され「なければならない」。またバージョン 1.2 またはそれ以降が「推奨される」。

注

「なければならない」および「推奨される」という単語は、規定要求事項のための IETF 仕様書に従って使用されている。

このプロファイルへの適合を要求するどんな実装も、監査証跡メッセージフォーマットプロファイルに適合しなければならない。XML 監査証跡メッセージの作成が、監査証跡メッセージフォーマットプロファイルに定義されたフォーマットを使用して行われた場合、それは、RFC5425 に定義されている TLS メカニズムに関する syslog を使用して、収集ポイントに送信されなければならない。このプロファイルに適合するシステムは、少なくとも 32768 オクテットのメッセージサイズをサポートしなければならない。

注

1. 他の目的のための監査メッセージも同じ syslog 接続で転送されるかもしれない。これらのメッセージは監査証跡メッセージフォーマットに適合しないかもしれない。
2. RFC5425 は、2KB メッセージの必須なサポートを指定し、少なくとも 8KB のサポートを強く推奨し、最大サイズを制限しない。
3. 受信メッセージが受信アプリケーションサポートより長い場合、メッセージは廃棄されるか切詰められるかもしれない。送信アプリケーションは通知されない。

XML 監査証跡メッセージは、RFC5424 「Syslog プロトコル」に規定のとおり、Syslog メッセージの SYSLOG-MSG 要素の MSG 部に挿入されなければならない。XML 監査メッセージには UTF-8 で符号化されたユニコード文字が含まれてもよい。

注

UTF-8 は、syslog プロトコルによって保留される制御文字の利用を避ける。しかし、システムは UTF-8 のために準備されていないと、これらのメッセージを正確に表示できないかもしれない。

PRI フィールドの設定は、10 の設備値を使用して行われなければならない（セキュリティ/認可メッセージ）。ほとんどのメッセージは 5 の厳しさ値をもっていることが望ましい（正常であるが重要な）。もっともそれが監査メッセージ中の、より詳細な情報に適切な場合、アプリケーションは他の値を選ぶかもしれない。この意味は、ほとんどの監査メッセージのため、PRI フィールドは値「<85>」を含むということである。

SYSLOG-MSG の HEADER 中の MSGID フィールドは設定されなければならない。値「DICOM+RFC3881」は、このプロファイルに適合するメッセージに使用されてもよい。

SYSLOG-MSG の MSG フィールドは存在しなければならない。また DICOM 監査メッセージスキーマに従う XML 構造でなければならない（セクション A.5.1 を参照）。

syslog メッセージは、RFC5424 に述べるように作成および送信されなければならない。

このセキュリティプロファイルへの適合を要求するどんな実装も、その適合性宣言書に次項を記述しなければならない：

- a. RFC5424 および RFC5425 に関連する任意の構成パラメータ。
- b. 作成されるか処理されるあらゆる STRUCTURED-DATA。
- c. 監査メッセージのための任意の実装スキーマまたはメッセージ要素拡張。
- d. 送受信が可能なメッセージの最大サイズ。

A.7 監査証跡メッセージ送信プロファイル—SYSLOG-UDP

このプロファイルは、監査証跡メッセージの送信を定義する。Syslog メッセージを UDP (RFC5426) 上で送信すると、監査メッセージの迅速なトランスポートのメカニズムを提供する。それは参考規格「BSD syslog プロトコル (RFC3164)」の標準化された後継者であり、RFC3164 は様々な設定中で広く使用される。

syslog ポート番号は構成可能であり、ポート番号 (514) が初期設定である。

根本的な UDP トランスポートは、MTU サイズ引く UDP ヘッダー長より長いメッセージを受理しなくてもよい。この結果、より長い syslog メッセージは切詰められるかもしれない。これらのメッセージが切詰められる場合、結果として生じる XML は正しくないかもしれない。切詰められたメッセージおよび他のセキュリティ上の懸念があるために、syslog メッセージは TLS 上で送信す

ることが好まれるかもしれない（セクション A.6 を参照）。

PRI フィールドの設定は、10 の設備値を使用して行われなければならない（セキュリティ/認可メッセージ）。ほとんどのメッセージは 5 の厳しさ値をもっていることが望ましい（正常であるが重要な）。もっとも、それが監査メッセージ中の、より詳細な情報に適切な場合、アプリケーションは 4（警告条件）の値を選ぶかもしれない。この意味は、ほとんどの監査メッセージのため、PRI フィールドは値「<85>」を含むということである。監査保存庫は、入って来る PRI 値すべてに適切に対処する準備ができなければならない。

SYSLOG-MSG の HEADER 中の MSGID フィールドは設定されなければならない。値「DICOM+RFC3881」は、このプロファイルに適合するメッセージに使用されてもよい。

SYSLOG-MSG の MSG フィールドは存在しなければならない。また DICOM 監査メッセージスキーマに従う XML 構造でなければならない（セクション A.5.1 を参照）。

syslog メッセージは、RFC5424 に述べるように作成および送信されなければならない。

このセキュリティプロファイルへの適合を要求するどんな実装も、その適合性宣言書に次項を記述しなければならない：

- a. RFC5424 および RFC5426 に関連する任意の構成パラメータ。
- b. 作成されるか処理されるあらゆる STRUCTURED-DATA。
- c. 監査メッセージのための任意の実装スキーマまたはメッセージ要素拡張。
- d. 送受信が可能なメッセージの最大サイズ。

B セキュアトランスポートコネクションプロファイル（規格）

B.1 基本 TLS セキュアトランスポートコネクションプロファイル

基本 TLS セキュアトランスポートコネクションプロファイルをサポートする実装は、トランスポート層セキュリティ版 1.0 プロトコルによって明記されたフレームワークと折衝メカニズムを利用する。表 B.1-1 は、TLS 内の対応する機能が応用エンティティにサポートされる場合、サポートされなければならないメカニズムを指定する。このプロファイルは、TLS の機能（エンティティ認証、暗号化、完全性検査）をすべてサポートすることを実装に要求しない。もし TLS チャネルの設立中に折衝によって同意されれば、他のメカニズムも使用されてもよい。

表 B.1-1. TLS 機能のための最小メカニズム

サポートする TLS 機能	最小メカニズム
エンティティ認証 Entity Authentication	RSA based certificates
マスタシークレットの交換 Exchange of Master Secrets	RSA
データ完全性 Data Integrity	SHA
プライバシー Privacy	Triple DES EDE, CBC

実装が TLS 接続を受理する IP ポート、またはこのポート番号が選択若しくは構成されるメカニズムは、適合性宣言書で指定されなければならない。このポートは、他のタイプトランスポートコネクション（セキュアまたはセキュアでない）のために使用されたポートとは異なる。

注

基本 TLS セキュアトランスポートコネクションプロファイルをサポートするシステムは、彼らのポートとして TLS 上の DICOM 上位層プロトコルのための登録済ポート番号「2762 dicom-tls」（10 進）を使用することを強く推奨される。

さらに適合性宣言は、かぎ管理のために実装がサポートするメカニズムを示す。

プロファイルは、TLS セキュアトランスポートコネクションを確立する方法、または、同位エンティティ認証の間に交換された任意の証明書的重要性を明記しない。これらの問題は、何らかの現場で指定されたセキュリティ方針に多分従っている応用エンティティに任される。証明書所有者の ID は、応用エンティティによって監査ログサポートに使用できる。またはいくつかの外部アクセス権管理枠組に基いたアクセスを制限するために使用できる。一旦応用エンティティがセキュアトランスポートコネクションを確立した場合、上位層アソシエーションはそのセキュア通信路を使用できる。

注

PDU サイズと TLS 記録サイズとの間に相互作用があり、これはトランスポートの効率に影響する。許される最大 TLS 記録サイズは、許される最大 PDU サイズより小さい。

完全性検査が失敗する場合、実装特有の供給者理由で上位層へ A-P-ABORT 指示を発行することを送信側および受信側の両方に起こさせて、接続は TLS プロトコルによって中断される。使用される供給者理由は、適合性宣言の中で文書化される。

注

完全性検査失敗は、通信路のセキュリティが危険にさらされたことがあることを示す。

B.2 ISCL セキュアトランスポートコネクションプロファイル

ISCL トランスポートコネクションプロファイルをサポートする実装は、統合セキュア通信層（V1.00）によって明記されたフレームワークおよび折衝メカニズムを利用する。応用エンティティは、表 B.2-1 の中で指定されたメカニズムを選択するために ISCL を使用する。応用エンティティは、最小として、エンティティ認証メカニズムおよびデータ完全性検査を使用する。応用エンティティは自由選択でプライバシーメカニズムを使用することがある。

表 B.2-1. ISCL 機能のための最小メカニズム

サポートする ISCL 機能	最小メカニズム
エンティティ認証 Entity Authentication	Three pass (four-way) authentication(ISO/IEC 9798-2)
データ完全性 Data Integrity	Either MD-5 encrypted with DES, or DES-MAC (ISO 8730)
プライバシー Privacy	DES (注を参照)

注

オンライン電子保存に対してプライバシーのための DES の使用は任意選択である。

データの完全性検査について、実装は、MD-5 を適用する前に乱数を暗号化するか、または MD-5 の出力を暗号化することがある。その順序はプロトコルの中で指定される。受信側は順序にかかわらずメッセージ上で完全性検査を実行できる。

実装が ISCL 接続を受諾する IP ポート、またはこのポート番号が選択されるか構成されるメカニズムは、適合性宣言の中で指定される。このポートは、他のタイプトランスポートコネクション（セキュアまたはセキュアでない）のために使用されたポートとは異なる。

注

ISCL セキュアトランスポートコネクションプロファイルをサポートするシステムは、それらのポートとして ISCL 上の DICOM 上位層プロトコルのための登録済ポート番号「2761 dicom-iscl」を使用することを強く推奨される。

さらに適合性宣言は、かぎ管理のために実装がサポートするメカニズムを示す。

プロファイルは、ISCL セキュアトランスポートコネクションを確立する方法を明記しない。これらの問題は、何らかの現場で指定されたセキュリティ方針に多分従っている応用エンティティに任される。一旦応用エンティティがセキュアトランスポートコネクションを確立した場合、上位層アソシエーションはそのセキュア通信路を使用できる。

注

トランスポートの効率に影響を与える PDU サイズと ISCL 記録サイズの間には相互作用があることがある。

完全性検査が失敗する場合、実装特有の供給者理由で上位層へ A-P-ABORT 指示を発行することを送信側および受信側の両方に起こさせて、接続は ISCL プロトコルによって中断される。使用される供給者理由は、適合性宣言の中で文書化される。

注

完全性検査失敗は、通信路のセキュリティが危険にさらされたことがあることを示す。

B.3 AES の TLS セキュアトランスポート接続プロファイル

AES の TLS セキュアトランスポート接続プロファイルをサポートする実装は、トランスポート層セキュリティバージョン 1.0 プロトコルによって指定されたフレームワークおよび折衝メカニズムを利用しなければならない。表 B. 3-1 は、TLS 内の対応する機能が応用エンティティにサポートされる場合、サポートされなければならないメカニズムを指定する。このプロファイルは、TLS の機能（エンティティ認証、暗号化、完全性検査）をすべてサポートすることを実装に要求しない。もし TLS チャネルの設立中に折衝によって同意されれば、他のメカニズムも使用されてもよい。

表 B.3-1. TLS 機能のための最小メカニズム

サポートする TLS 機能	最小メカニズム
エンティティ認証 Entity Authentication	RSA based Certificates

2 つの暗号 (cyphersuite) オプションが、このプロファイルに適合するアプリケーションによって TLS 折衝の間に提示されなければならない：

TLS_RSA_WITH_AES_128_CBC_SHA

TLS_RSA_WITH_3DES_EDE_CBC_SHA

そのアプリケーションは両方のオプションを提示しなければならない。AESバージョンの方が好まれないと見なされる。予備として3DESが、このプロファイルが、3DES cyphersuiteだけをサポートするアプリケーションと容易に相互作用できるようにするために提示される。

実装が TLS 接続を受理する IP ポート、またはこのポート番号が選択若しくは構成されるメカニズムは、適合性宣言書で指定されなければならない。このポートは、他のタイプトランスポートコネクション（セキュアまたはセキュアでない）のために使用されたポートとは異なる。

注

強く勧められることは、システムが、AES の TLS セキュアトランスポート接続プロファイルをサポートする場合、システムのポートとして、公認のポート番号「2762 dicom-tls」を DICOM 上部層プロトコルのため TLS 上で使用することである（10 進）。

さらに適合性宣言は、かぎ管理のために実装がサポートするメカニズムを示す。

プロファイルは、TLS セキュアトランスポートコネクションを確立する方法、または、同位エンティティ認証の間に交換された任意の証明書的重要性を明記しない。これらの問題は、何らかの現場で指定されたセキュリティ方針に多分従っている応用エンティティに任される。証明書所有者の ID は、応用エンティティによって監査ログサポートに使用できる。またはいくつかの外部アクセス権管理枠組に基いたアクセスを制限するために使用できる。一旦応用エンティティがセキュアトランスポートコネクションを確立した場合、上位層アソシエーションはそのセキュア通信路を使用できる。

注

PDU サイズと TLS 記録サイズとの間に相互作用があり、これはトランスポートの効率に影響する。許される最大 TLS 記録サイズは、許される最大 PDU サイズより小さい。

完全性検査が失敗する場合、実装特有の供給者理由で上位層へ A-P-ABORT 指示を発行することを送信側および受信側の両方に起こさせて、接続は TLS プロトコルによって中断される。使用される供給者理由は、適合性宣言の中で文書化される。

注

完全性検査失敗は、チャネルのセキュリティが侵害されている可能性があることを示す。

B.4 基礎的ユーザーID アソシエーションプロファイル

実装は、基礎的ユーザーID アソシエーションプロファイルをサポートする場合、1 または 2 のユーザーID タイプのために、ユーザーID アソシエーション折衝サブアイテムを受理しなければならない。それはパスワードを確認する必要はない。肯定応答が要求される場合、実装はアソシエーションレスポンスサブアイテムで答えなければならない。

主要フィールドからのユーザーID は、実装内でユーザー識別として使用されなければならない。そのような用途は、ユーザー識別を監査メッセージ中に記録することを含む。

表 B.4-1. DICOM アソシエーション折衝機能のための最小メカニズム- 基礎的ユーザーID アソシエーションプロファイル

サポートするアソシエーション折衝機能	最小メカニズム
ユーザーID User Identity	Username

B.5 ユーザーID プラス パスコードアソシエーションプロファイル

実装は、ユーザーID プラス パスコードアソシエーションプロファイルをサポートする場合、ユーザーID アソシエーション折衝サブアイテムを 2 のユーザーID タイプのために送受信しなければならない。肯定応答が要求される場合、アソシエーションアクセプタ実装はアソシエーションレスポンスサブアイテムで答えなければならない。パスワード情報は内部または外部認証システムに利用可能にならなければならない。ユーザーID はパスワードおよび認証システムによって認証されなければならない。認証が失敗する場合、アソシエーションは拒絶されなければならない。

主要フィールドからのユーザーID は、実装内でユーザー識別として使用されなければならない。そのような用途は、ユーザー識別を監査メッセージ中に記録することを含む。

表 B.5-1. ユーザーID プラス パスコードアソシエーションプロファイル -DICOM アソシエーション折衝機能のための最小メカニズム

サポートするアソシエーション折衝機能	最小メカニズム
ユーザーID User Identity	Username and Passcode

B.6 ケルベロス ID 折衝アソシエーションプロファイル

実装は、ケルベロス ID 折衝アソシエーションプロファイルをサポートする場合、ユーザーID アソシエーション折衝サブアイテムを、3のユーザーID タイプのために、送受信しなければならない。肯定応答が要求される場合、アソシエーションアクセプタ実装は、ケルベロスサーバチケットを含むアソシエーションレスポンスサブアイテムで答えなければならない。ケルベロスサーバチケット情報は、内部または外部ケルベロス認証システムに利用可能にならなければならない。ユーザーID はケルベロス認証システムによって認証されなければならない。認証が失敗する場合、アソシエーションは拒絶されなければならない。

主要フィールドからのユーザーID は、実装内でユーザー識別として使用されなければならない。そのような用途は、ユーザー識別を監査メッセージ中に記録することを含む。

表 B.6-1. ケルベロス ID 折衝アソシエーションプロファイル -DICOM アソシエーション折衝機能のための最小メカニズム

サポートするアソシエーション折衝機能	最小メカニズム
ユーザーID User Identity	Kseberos

B.7 統合 SAML アサーション ID 折衝アソシエーションプロファイル

実装は、統合 SAML アサーション ID 折衝アソシエーションプロファイルをサポートする場合、ユーザーID アソシエーション折衝サブアイテムを、4のユーザーID タイプのために、送受信しなければならない。肯定応答が要求される場合、アソシエーションアクセプタ実装は SAML レスポンスを含むアソシエーションレスポンスサブアイテムで答えなければならない。SAML アサーション情報は、内部または外部認証システムに利用可能にならなければならない。ユーザーID は、SAML アサーションを使用する認証システムによって認証されなければならない。認証が失敗する場合、アソシエーションは拒絶されなければならない。

主要フィールドからのユーザーID は、実装内でユーザー識別として使用されなければならない。そのような用途は、ユーザー識別を監査メッセージ中に記録することを含む。

表 B.7-1. 統合 SAML アサーション ID 折衝アソシエーションプロファイル - DICOM アソシエーション折衝機能のための最小メカニズム

サポートするアソシエーション折衝機能	最小メカニズム
ユーザーID User Identity	SAML Assertion

B.8 電子メールトランスポートのセキュア使用

DICOM ファイルセットは、電子メールトランスポート上でこのプロファイルに従って送られる場合、次の規則に従わなければならない：

- ファイルセットは、電子メール本文への添付でなければならない。
- 電子メール全体（本文、ファイルセット添付および他の添付）は、AES を使用して RFC3851 および RFC3853 に従って暗号化されなければならない。
- 電子メール本文および添付は、RFC3851 に従って圧縮されてもよい。
- 電子メールは、送り手によってデジタル署名されなければならない。署名は暗号化の前後に適用してもよい。このデジタル署名は、この電子メール中の情報を受け手に開示する送り手の権限を送り手が証明していることを意味すると解釈されなければならない。

電子メール署名が存在するのは、最小の送り手情報を提供し、かつ電子メール（本文内容、添付など）送信の完全性を確認するためである。電子メール署名は、電子メールに添付されたファイルセットに含む DICOM 報告書およびオブジェクト中に存在する他

の署名とは別である。それらの署名は臨床の用途の点から定義される。どんな臨床の内容証言も、電子メール署名としてではなく、DICOM SOP インスタンス中のデジタル署名としてコード化されなければならない。電子メールは、臨床証言をすることができない人によって作成されるかもしれない。電子メール署名の使用を通じて、構成者は、データを受け手に送信する権限をもつことを証明する。

注

1. このプロファイルは、ZIP ファイルの内在使用または電子メール上の他のファイルセットパッケージングとは別である。
2. 個人情報が伝えられている場合、ほとんどの国の規制は暗号化または等価な保護の使用を要求する。このプロファイルは規制の中で最も一般的な要求事項を満たす。しかし、追加のローカルの要求事項があるかもしれない。追加の要求事項は、電子メール本文中の必須なステートメント、および患者プライバシーを防御するための電子メール本文の内容禁止を含むかもしれない。

C デジタル署名プロファイル（規格）

C.1 基本 RSA デジタル署名プロファイル

基本 RSA デジタル署名プロファイルは、デジタル署名を作成するために MAC の RSA 暗号の使用を概説する。このプロファイルは、署名するデータ要素のいかなる特定集合も指定しない。他のデジタル署名プロファイルは、どのデータ要素に署名するべきかの仕様または他のカスタム化を加えて、このプロファイルを参照することがある。

デジタル署名の作成者は、その後、それは私的 RSA かぎを使用して暗号化される MAC を作成するために RIPEMD-160, MD5, SHA-1, または SHA-2 ファミリー (SHA256, SHA384, SHA512) ハッシュ関数の 1 つを使用する。デジタル署名の確認者は、指定されたハッシュ関数 (RIPEMD-160, MD5, SHA-1, SHA256, SHA384, SHA512) のいずれによって作成された MAC も使用できる。

注

MD5 の使用はその発明者、RSA によって推奨されない。ftp://ftp.rsasecurity.com/pub/pdfs/bulletn4.pdf を参照。

RFC2437 (PKCS#1) の中で指示されるように、署名される MAC は、RSA かぎサイズと一致するブロックサイズにパディングされる。MAC アルゴリズム (0400,0015) の値は、「RIPEMD160」、「MD5」、「SHA1」、「SHA256」、「SHA384」、「SHA512」のいずれかにセットされる。RSA かぎ対を所有する応用エンティティまたは装置製造者の識別 (identity) と同様に秘密かぎに関連した公開かぎは、X.509 (1993) 署名証明書の中で送信される。証明書タイプ (0400,0110) 属性値は「X509_1993_SIG」に設定する。サイト特有の方針は X.509 証明書の生成、認証、配布方法を定めている。サイトは X.509 証明書を直接発行し配布することがある、または認証機関のサービスを利用することがあるが、証明書作成および検証のあらゆる合理的方法を使用することがある。

実装がタイムスタンプを利用する場合、それは「CMS_TSP」の保証されたタイムスタンプタイプ (0400,0305) を使用する。保証されたタイムスタンプ (0400,0310) は「Internet X.509 Public Key Infrastructure; Time Stamp Protocols; March 2000」の中で記述されるように作成される。

C.2 作成者 RSA デジタル署名プロファイル

DICOM SOP インスタンスの作成者は、作成者 RSA デジタル署名プロファイルを使用して、署名を作成することがある。このプロファイルによって作成されたデジタル署名は、SOP インスタンスの画素データがその最初の作成以来変更されていないことを確認するために使用できる、生涯データ安全性チェックとして、貢献する。作成者 RSA デジタル署名プロファイルをサポートする実装は、それが作成するすべての SOP インスタンスで作成者 RSA デジタル署名を含むことがある；しかしながら、その実装はそうすることは要求されない。

最低、実装は作成者 RSA デジタル署名を作成する際に次の属性を含む：

- a. SOP クラスおよびインスタンス UID
- b. 存在する場合は、SOP 作成日および時刻
- c. 検査およびシリーズインスタンス UID
- d. 存在する一般装置モジュールのすべての属性
- e. 存在するオーバーレイ面モジュール、カーブモジュール、またはグラフィック注釈モジュールのすべての属性
- f. 存在する一般画像モジュールおよび画像画素モジュールのすべての属性
- g. 存在する SR 文書一般モジュールおよび SR 文書内容モジュールのすべての属性
- h. 存在する波形モジュールおよび波形注釈モジュールのすべての属性
- i. 存在するマルチフレーム機能グループモジュールのすべての属性
- j. 存在する拡張 MR 画像モジュールのすべての属性
- k. 存在する MR 分光法モジュールのすべての属性
- l. 存在する生データモジュールのすべての属性

- m. 存在する拡張 CT 画像モジュールのすべての属性
- n. 存在する拡張 XA/XRF 画像モジュールのすべての属性
- o. 存在する区分画像モジュールのすべての属性
- p. 存在するカプセル化文書モジュールのすべての属性
- q. 存在する X 線 3D 画像モジュールのすべての属性
- r. 存在する拡張 PET 画像モジュールのすべての属性
- s. 存在する拡張 US 画像モジュールのすべての属性
- t. 存在する表面区分モジュールのすべての属性
- u. 存在する表面メッシュモジュールのすべての属性
- v. 存在する構造化ディスプレイモジュール, 構造化ディスプレイ注釈モジュール, および構造化ディスプレイ画像ボックスモジュールのすべての属性
- w. 存在するインプラントテンプレートモジュールのすべての属性
- x. 存在するインプラントアセンブリーテンプレートモジュールのすべての属性
- y. 存在するインプラントテンプレートグループモジュールのすべての属性
- z. 存在するポイントクラウドモジュールのすべての属性
- aa. 存在する拡張マンモグラフィ画像モジュールのすべての属性
- bb. 存在するトラクトグラフィ結果モジュールのすべての属性
- cc. 存在する体積グラフィック注釈モジュールのすべての属性

デジタル署名は、基本 RSA デジタル署名プロファイルに記述された方法論を用いて作成される。典型的に、作成者 RSA デジタル署名を作成するために使用される証明書と関連する秘密かぎは、サービスまたは据付技術者によってセットされる応用エンティティの構成パラメータである。

作成者 RSA デジタル署名は、他のデジタル署名との直接の関係をもたない。しかしながら、許可デジタル署名のような他のデジタル署名は、作成者 RSA デジタル署名のタイムスタンプと協同するために使用されることがある。

C.3 認可 RSA デジタル署名プロファイル

使用するために DICOM SOP インスタンスを承認する技術者または医師は、認可 RSA デジタル署名プロファイルを使用して署名を作成することを応用エンティティに要求することがある。作成されたデジタル署名は、SOP インスタンスの中の画素データが、技術者または医師が承認した時に見たものと同一であることを確認するために使用できる、生涯データ保全性チェックとして役立つ。

最低、実装は認可 RSA デジタル署名を作成する際に次の属性を含む：

- a. SOP クラスおよびインスタンス UID
- b. 検査およびシリーズインスタンス UID
- c. この値が技術者か医師によって証明可能なすべての属性（例えば、それらの値が技術者または医師に表示される）
- d. 存在するオーバーレイ面またはカーブ、グラフィック注釈モジュールのすべての属性
- e. 存在する一般画像および画像画素モジュールのすべての属性
- f. 存在する SR 文書一般および SR 文書内容モジュールのすべての属性
- g. 存在する波形および波形注釈モジュールのすべての属性

- h. 存在するマルチフレーム機能グループモジュールのすべての属性
- i. 存在する拡張 MR 画像モジュールのすべての属性
- j. 存在する MR 分光法モジュールのすべての属性
- k. 存在する生データモジュールのすべての属性
- l. 存在する拡張 CT 画像モジュールのすべての属性
- m. 存在する拡張 XA/XRF 画像モジュールのすべての属性
- n. 存在する区分画像モジュールのすべての属性
- o. 存在するカプセル化文書モジュールのすべての属性
- p. 存在する X 線 3D 画像モジュールのすべての属性
- q. 存在する拡張 PET 画像モジュールのすべての属性
- r. 存在する拡張 US 画像モジュールのすべての属性
- s. 存在する表面区分モジュールのすべての属性
- t. 存在する表面メッシュモジュールのすべての属性
- u. 存在する構造化ディスプレイ、構造化ディスプレイ注釈、および構造化ディスプレイ画像ボックスモジュールのすべての属性
- v. 存在するインプラントテンプレートモジュールのすべての属性
- w. 存在するインプラントアセンブリテンプレートモジュールのすべての属性
- x. 存在するインプラントテンプレートグループモジュールのすべての属性
- y. 存在するポイントクラウドモジュールのすべての属性
- z. 存在する拡張マンモグラフィ画像モジュールのすべての属性
- aa. 存在する体積グラフィック注釈モジュールのすべての属性

デジタル署名は、基本 RSA デジタル署名プロファイルに記述された方法論を用いて作成される。応用エンティティは、ログインメカニズムまたはスマートカードのようなサイト特有の手続きを通じて、技術者または医師の ID を決定し、彼らの証明書を取得する。

認可 RSA デジタル署名は、他のデジタル署名との直接の関係をもたない。しかしながら、作成者デジタル署名のような他のデジタル署名は、認可 RSA デジタル署名のタイムスタンプと協同するために使用されることがある。

C.4 構造化レポート RSA デジタル署名プロファイル

このプロファイルは、確認観察者が 1 人だけの場合、デジタル署名を構造化レポートまたはかぎオブジェクト選択文書に追加するメカニズムを定義する。このデジタル署名プロファイルに従うインスタンスは、データセットのトップのレベルで少なくとも 1 つのデジタル署名を含まなければならない。

このプロファイルに従うデジタル署名はすべて、デジタル署名目的コードシーケンス属性を含まなければならない(0400, 0401)。

実装は、このプロファイルによって要求されるデジタル署名を作成する際に、最小限、次の属性を含まなければならない：

- a. SOP クラス UID
- b. 検査およびシリーズインスタンス UID
- c. 存在する一般的な設備モジュールのすべての属性
- d. 現在の要求される手続き証拠シーケンス

- e. 適切な他の証拠シーケンス
- f. 前任者文書シーケンス
- g. 観察日付時間
- h. 存在する SR 文書内容モジュールのすべての属性

検証フラグが「VERIFIED」に設定された（また、SOP インスタンス UID はもはや変えられない）場合、デジタル署名プロファイルの少なくとも 1 つは、(5, ASTM-sigpurpose, 「検証署名」) の目的を持ち、さらに次の属性を上記属性に追加して含まなければならない：

- a. SOP インスタンス UID
- b. 検証フラグ
- c. 検証する観察者シーケンス
- d. 検証日付時間

注

システムはさらに作成者 RSA デジタル署名を追加するかもしれない。それは、機械が検証できる他の属性をカバーすることがある。

参照 SOP インスタンス MAC シーケンス(0400, 0403)の発生はすべて、「RIPEMD160」、「MD5」、「SHA1」、「SHA256」、「SHA384」または「SHA512」の何れかに設定された、MAC アルゴリズム(0400,0015)の値をもたなければならない。

デジタル署名は、基本 RSA デジタル署名プロファイルに記述された方法論を用いて作成される。応用エンティティは、署名者の ID を決定し、アプリケーション特有の手続き、例えば、ログインメカニズムまたはスマートカードを通じてそれらの証明書を得なければならない。適合性宣言書は、アプリケーションがどのように署名者を識別し、証明書を得るか明示しなければならない。

注

構造化レポート RSA デジタル署名は、他のデジタル署名と直接関係しない。しかしながら、他のデジタル署名、例えば、作成者 RSA デジタル署名は、構造化レポート RSA デジタル署名のタイムスタンプを確証するために使用されてもよい。

D 媒体保存セキュリティプロファイル（規格）

D.1 基本 DICOM 媒体セキュリティプロファイル

基本 DICOM 媒体セキュリティプロファイルは、セキュリティの次の局面に取り組むようなセキュア DICOM ファイルへ DICOM ファイルのカプセル化を可能にする：

- 機密性、
- 完全性、
- データ発信元認証（オプション）。

このプロファイルは、内容暗号化および RSA またはパスワードベースの暗号化用の AES または Triple-DES のどちらか、または内容暗号化かぎのかぎ移送のための AES 若しくは Triple-DES のどちらかの使用を規定する。暗号化された内容は下記のいずれかであることができる DICOM ファイルである。

- ダイジェストアルゴリズムとして SHA-1, SHA256, SHA384, SHA512 を使用し、署名アルゴリズムとして RSA を使用して、1つ以上のデジタル署名で署名される DICOM ファイル、または
- デジタル署名のアプリケーションなしで、ダイジェストアルゴリズムとして SHA-1, SHA256, SHA384, SHA512 でダイジェストされる DICOM ファイル。

注

ダイジェストアルゴリズム要求事項は脅威が発展するように発展する。ダイジェスト要求事項が変更されれば、このプロファイルは追加の要求事項を含むために変更される。

D.1.1 セキュア DICOM ファイルの中の DICOM ファイルのカプセル化

このセキュリティプロファイルに一致するセキュア DICOM ファイルは、RFC3852, RFC3370, RFC3565 に定義された暗号メッセージ構文の包まれたデータ内容タイプを含む。包まれたデータは、かぎ派生アルゴリズム用に RSA[RFC3447]または PBKDF2 [RFC2898]を使用するパスワードベースの暗号化を、そして内容暗号かぎのかぎトランスポート用には AES または Triple-DES [RFC3211]のどちらかを使用しなければならない。このセキュリティプロファイルに一致するセキュア DICOM ファイルの作成者は、内容暗号化用に AES または Triple-DES を使用してもよい。このプロファイルへの適合を要求する読者は、AES または Triple-DES のどちらかを使用してセキュア DICOM ファイルを解読することができなければならない。AES かぎの長さは、RFC によって許可された長さならどれでもよい。Triple-DES かぎの長さは、ANSI X9.52 によって定義されるように 168 ビットである。符号化は次の仕様書に従って行われなければならない。つまり RFC3370 中の RSA かぎトランスポートおよび Triple-DES 内容暗号化の仕様、並びに RFC3565 中の AES 内容暗号化の仕様である。

包まれたデータ内容タイプの暗号化された内容は、下記の選択でなければならない：

- 署名データ内容タイプ（Signed-data content type）；
- ダイジェストデータ内容のタイプ（Digested-data content type）。

両方の場合で、SHA-1[SHA-1], SHA256, SHA384, SHA512 [SHA-2] はダイジェストアルゴリズムとして使用される。署名データ内容タイプの場合、署名アルゴリズムとして RSA[RFC2313]が使用される。

パスワードに基づいた暗号化が PBKDF2 を使用する場合、8 ビットの文字列であってかぎの作成に使用されるパスワードを含むものは、初期設定文字レパートリによって定義された符号化および図形文字表現に制限されなければならない。

注

1. 内容暗号化かぎの RSA かぎ移送は、欧州予備（暫定）規格 ENV 13608-2: Health Informatics - Security for healthcare communication - Part 2: Secure data objects の中で要求として明示される。
2. RSA かぎ移送に使用された非対称かぎ対のサイズ上の要求は、このプロファイルに定義されない。

3. 署名データ内容タイプの署名者情報 (SignerInfo) 構造の署名属性要素の使用に対する要求または制限は、このプロファイルの中で定義していない。署名属性は、ENV 13608-2 によって要求されるように、例えば、署名時間が SMIME 能力を明示するために使用されることがある。
4. パスワードベースの暗号化は、内容暗号かぎのかぎトランスポートのため使用する場合、証明書ベースの暗号化ほど恐らく安全ではない可能性がある。しかし、受け手のリストが事前に未知であるとき、または公開かぎインフラストラクチャーがないときには有用かもしれない。そのセキュリティは、パスワードのエントロピーに依存し、もしユーザー選択されれば全く低くなり得る。RFC3211 は、単一のワードではなく単一のパス「フレーズ」の使用を強く勧めており、また、RFC2898 は実際の長さ制限は課していない。さらに、パスワードかパスフレーズの交換に使用される方法も、セキュリティのレベルに重要な影響を及ぼすことがある。
5. PBKDF2 は RFC2898 の中で定義され、「テキストストリングとしての解釈は無指定の任意の長さのオクテット文字列」であるパスワードを指定する。送り手と受け手との間の相互運用性のために、文字コード体系および図形文字表現の両方を定義する必要がある。ISO IR6 (US-ASCII)、すなわち DICOM の初期設定文字レパートリ (PS3.5 を参照) が、他の文字セット (例えば、UTF-8) の使用による曖昧さを避けるために指定されている。他の文字セットは、特定の図形文字表現に対し同じ 2 進法数値に必ずしも帰着しない。

ISO IR6 中の記号の図形文字表現は、たとえ同じ 2 進法表現が他の 7 ビットのスキームで異なる図形文字表現をもつ場合でも、明示的に定義される。例えば、日本で使用される ISO 646 のバージョン (ISO-IR 14 ローマ字) では、05/12 は「¥」として表現されバックslash「\」ではない。アプリケーションの責任として、ユーザーへのそのような記号の入力方式および表示は、正確な符号化に写像されることを保証することである。これはローカルに無関係である。つまり、もしパスワードが「123\\$/」であれば、それは 03/01、03/02、03/03、05/12、02/04 としてコード化されるべきである。これはユーザーが、バックslash「\」(U+005C) を日本のキーボードまたは米国のキーボードでタイプするかどうかには無関係である。「¥」(U+00A5) が日本のキーボード上にタイプされることを予想しない方がよい。またパスワードがテキストとして表示される場合、05/12 が「¥」として表示しない方がよい。

ISO IR6 符号化および図形文字表現に対する制約 (例えば、UTF-8 の最小の符号化ではなく) により、同綴異義語 (同じに見えるがコード化が異なる文字) および同じ意味の代替符号化による曖昧さを除去する。例えば、1 文字のドイツ文字「ß」(U+00DF) に対する 2 文字の「ss」(U+0073 U+0073)、表音文字に対する同じ意味の表意文字、例えば、日本の平仮名「ぞう」(U+305E U+3046) に対する漢字「像」(U+50CF) である。

表現できない文字を使用してユーザーがパスワードを作成するのを防止することはアプリケーションの責任である。例えば、西欧のキーボード上で、ユーザーはアクセント付文字の入力を許されない方がよい。例えば「é」(U+00E9) または「ö」(U+00F6) である。なぜならそのような文字の ISO IR 6 文字への写像が定義されていないからである (例えば、「e」または「o」)。

E 属性機密性プロファイル

この付属書は、収集に関与する患者または他の個人若しくは組織に関する個人識別可能な情報（III: Individually Identifiable Information）の漏洩になる恐れがある DICOM データセット内の属性の削除および置換に取り組むプロファイルおよびオプションについて記述する。

プロファイルは、データセットがそれらの意図した目的に役立つようにするために、情報削除と情報保持の必要性との間のバランスに取り組むために提供される。

異なるプロファイルの組合せの拡張を防ぐために、オプションがプロファイルに追加して使用される。

E.1 アプリケーションレベル機密性プロファイル

アプリケーションレベル機密性プロファイルは、セキュリティの次の様相を扱う：

- 応用層のデータ機密性。

これらのプロファイルでは扱わないが、規格のどこか他のところが扱う、セキュリティの他の様相は次のとおり：

- DICOM モデルの他の層の中の機密性；
- データ完全性。

これらのプロファイルの目標は、特殊目的の、既存のデータセットの匿名版の作成である。それは匿名化(De-identifier)SOP インスタンスを作成する元となったオリジナルの SOP インスタンスを置換する意図はないし、また、画像アーカイブの臨床データセットの主要な表現の機能を果たす意図はない。匿名化(De-identifier)SOP インスタンスが有用であるのは、例えば、教育または研究ファイルの作成、治験の実装、または登録への提出など、患者など個人の身元を保護することが必要な場合である。場合によっては、権限を有する者により匿名を識別可能に戻す手段を提供することも必要である。

E.1.1 匿名化(De-identifier)

アプリケーションは、このプロファイルおよびオプションで指定されるすべての属性を保護し保持する場合、匿名化(De-identifier)としてアプリケーションレベル機密性プロファイルおよびオプションへの適合を主張できる。この文脈でいう保護とは次のプロセスとして定義される：

1. アプリケーションは、暗号化属性データセットの1つ以上のインスタンスを作成し、保護すべき属性を、1つ以上の暗号化属性データセットインスタンスの修正属性シーケンス(0400,0550)の（単一）アイテムにコピーしてもよい。

注

1. オリジナルデータセットを完全に再構築することは難しいかも知れない。しかし、暗号化属性データセットの修正属性シーケンス中の属性（例えば、SOP インスタンス UID）は、オリジナルデータセットを保持するオリジナル SOP インスタンスに戻って参照してもよい。
 2. 暗号化された属性データセットが作成されることは必要とされない。確かに、データセットの長期保管が期待され、無許可の識別回復に対する長期保護を提供するのに今の暗号化技術は不適当かもしれないような状況があるかもしれない。
 3. 識別回復または置換された UID または日付および時間の長期的一貫性を助けるための他のメカニズムは、推奨されない。それよりも暗号化属性データセットのメカニズムであってこの目的を意図するものの方がよい。例えば、それが患者名の暗号化ハッシュを含むことが望まれる場合、その目的のため実装される別の個人属性に符号化されることは望ましくないが、しかし、暗号化属性データセットに含まれ、標準メカニズムを使用して符号化されることが望ましい。これにより異なる実装間の互換性が可能となり、暗号化かぎの品質および管理に基づいたセキュリティを提供する。非暗号化ハッシュは安全性がかなり低いので避ける方がよいことにも注意すること。なぜならトリビアル辞書に基づく攻撃に対し弱いからである。
2. 保護されるべき属性はそれぞれデータセットから取り除かれるか、またはその値を患者を特定できない別の「置換値」で置き換えなければならない。

注

1. このプロセスが情報オブジェクト定義の完全性に悪影響を与えぬよう保証することが匿名化(De-identifier)の責任である。つまりダミー値が、保護されるタイプ 1 属性にとって必要かもしれないが、ゼロリングスで送られないかもしれない。そしてセキュリティメカニズムに気づかないアプリケーションによって、暗号化された形式で保存または交換されることになっている。
 2. 規格は、特定のダミー値の使用を義務付けていない。また、確かに、例えば、教育用のデータセットでは何らかの意味をもってよい。そこでは実際の患者識別情報が後日の検索のために暗号化される。しかし有効な代替方法で識別される。例えば、ダミー患者の名前(0010,0010)は、教育の場合で病理学のタイプを伝えてもよい。ダミー値が患者を識別するために使用できないことを保証するのは、匿名化(De-identifier)ソフトウェアかまたは操作者の責任である。
 3. 属性、例えば、スタディインスタンス UID(0020,000D)または評価基準系 UID(0020,0052)に対するダミー値の一貫性を保証することが、匿名化(De-identifier)の責任である。これは多数の関連する SOP インスタンスを保護する場合である。確かに、インスタンスレベルに関するすべてのエンティティの属性は、保護されるすべてのインスタンスに対し一貫することが望ましい。例えば、患者エンティティ用の患者 ID、スタディエンティティ用のスタディ ID、シリーズエンティティ用のシリーズ番号である。
 4. いくつかのプロファイルは、アイテムのシーケンスの部分を選択的には保護できない。保護される属性がアイテムのシーケンスに含まれている場合、アイテムのシーケンス全体を保護する必要があるかもしれない。
 5. 匿名化(De-identifier)は、識別情報を画像ピクセルデータに焼き付けけないことを保証することが望ましい。なぜならモダリティはそのような焼き付け識別を第一に生成しないからである。またはピクセルデータ消去オプションの使用を通じて識別情報を削除する；セクション E.3 を参照。もし非ピクセルデータグラフィックスまたはオーバーレイが識別を含んでいれば、匿名化(De-identifier)は識別情報を削除または消去するよう要求される。これはグラフィックス消去オプションが支援されている場合である。セクション E.3.3 を参照。焼き付けまたはグラフィックの識別情報を探し出して削除する手段は、この規格の範囲外である。
3. 保持されるべく指定された属性はそれぞれ保持されなければならない。匿名化(De-identifier)の裁量により、保護されるデータセットに属性を追加してもよい。

注

例として、属性患者年齢(0010,1010)は、患者生年月日(0010,0030)の置換として導入されてもよい。これは患者の年齢が重要であり、また、プロファイルが置換を許す場合である。

4. もし使用されれば、暗号化された属性データセットのインスタンスはすべて DICOM 転送構文で符号化され、暗号化され、そして保護されるべきデータセット内に、暗号化された属性シーケンスのアイテムとして保存されなければならない(0400,0500)。暗号化は、RSA[RFC2313]を使用して行われなければならない。内容暗号化かぎの暗号かぎをトランスポートするためである。このセキュリティプロファイルに適合する匿名化(De-identifier)は、AES または Triple-DES の何れかを内容暗号化に使用してもよい。AES かぎの長さは、RFC によって許可された長さならどれでもよい。Triple-DES かぎの長さは、ANSI X9.52 によって定義されるように 168 ビットである。符号化は次の仕様書に従って行われなければならない。つまり RFC3370 中の RSA かぎトランスポートおよび Triple-DES 内容暗号化の仕様、並びに RFC3565 中の AES 内容暗号化の仕様である。

注

1. 暗号化された属性シーケンス(0400,0500)のアイテムは、それぞれ、2つの属性から成る。一つは、暗号化属性データセットのインスタンスを符号化するために使用された転送構文の UID を含む暗号化された内容転送構文 UID(0400,0510)である。他の一つは、暗号化属性データセットインスタンスの暗号化の結果としてのデータブロックを含む暗号化内容(0400,0520)である。
 2. 内容暗号化かぎの RSA かぎ移送は、欧州予備(暫定)規格 ENV 13608-2: Health Informatics - Security for healthcare communication – Part 2: Secure data objects の中で要求として明示される。
5. RSA かぎトランスポートに使用される非対称のかぎペアのサイズ上の要求事項は、この機密性スキームの中で定義されていない。実装は、基礎アプリケーションレベル機密性プロファイルへの適合を、匿名化(De-identifier)として主張する場合、常に SOP インスタンス UID(0008,0018)属性、および他の SOP インスタンスへのすべての参照を保護（例えば、暗号化および置換）されなければならない。これは主なデータセットに含まれているか、または、アイテムのシーケンスのアイテムに埋込まれているかを問わない。何れも無許可のエンティティによって患者を識別するため使用される恐れがある。

注

シーケンスのアイテムに埋込まれた SOP インスタンス UID の場合、この意味は、トップレベルのデータセット中の
 包囲属性は全体が暗号化されなければならないということである。

6. 属性患者識別削除(0012,0062)は置換されるか、またはデータセットに YES の値を用いて追加されなければならない。また CID 7050「匿名化(De-identifier)方法」からの 1 つ以上のコードであって、使用されるプロファイルおよびオブションに対応するものは、匿名化(De-identifier)方法コードシーケンス(0012,0064)に追加されなければならない。使用される方法を記述するテキスト文字列は、匿名化(De-identifier)方法(0012,0063)に挿入または追加されてもよいが、要求はされない。
7. 匿名化(De-identifier)されるデータセットが DICOM ファイル内に保存されている場合、128 バイトの前文を含むファイルメタ情報は、存在する場合、匿名化(De-identifier)アプリケーションの記述と取り替えられなければならない。そうでなければ、識別情報が未修正のファイルメタ情報または前文を通じて漏れるかもしれないというリスクがある。PS 3.10 を参照。

表 E.1-1 に各プロファイルに対し列記された属性は、標準 IOD に含まれ、または標準拡張 IOD に含まれているかもしれない。実装が、アプリケーションレベル機密性プロファイルへの適合を匿名化(De-identifier)として主張する場合、表 E.1-1 に列記された属性のインスタンスをすべて保護するか保持されなければならない。これはインスタンスが主なデータセットに含まれていたか、アイテムのシーケンスのアイテムに埋込まれていたかを問わない。次のアクションコードが表の中で使用される：

- D-ゼロでない長さの値と置換する。それはダミー値であり VR と一致しているかもしれない
- Z-ゼロの長さの値またはゼロでない長さの値と置換する。それはダミー値であり VR と一致しているかもしれない
- X-削除する。
- K-キープする（非シーケンス属性には不変、シーケンスは消去される）。
- C-消去する。識別情報を含まず VR と一致する同様の意味の値に取り替える。
- U-セットのインスタンス内で内部的に一貫しているゼロでない長さの UID に取り替える。
- Z/D-もし D が IOD 適合を維持するように要求されなければ、Z（タイプ 2 対タイプ 1）
- X/Z-もし Z が IOD 適合を維持するように要求されなければ、X（タイプ 3 対タイプ 2）
- X/D-もし D が IOD 適合を維持するように要求されなければ、X（タイプ 3 対タイプ 1）
- X/Z/D-もし Z または D が IOD 適合を維持するように要求されなければ、X（タイプ 3 対タイプ 2 対タイプ 1）
- X/Z/U*-もし Z または含まれるインスタンス UID（U）の置換が IOD 適合を維持するように要求されなければ、X（タイプ 3 対タイプ 2 対 UID 参照を含むタイプ 1 シーケンス）

これらのアクションコードは、シーケンス属性および非シーケンス属性の両方に適用可能である；シーケンスの場合、アクションはシーケンスおよびその内容のすべてに適用可能である。シーケンスを消去する（「C」アクション）と、シーケンス内の属性の値を変更する。これは IOD でのその使用の文脈内のシーケンスの意味が理解される場合である。またはシーケンスの各アイテム中の各データセットに再帰的にプロファイル規則を適用する。シーケンスをキープする（「K」アクション）と、シーケンスの各アイテム中の各データセットに再帰的にプロファイル規則を適用することを要求する（例えば、そのシーケンス内に含まれる UID を再配置するためである）。

オブションのための要求事項は、実装された時、下層のプロファイルのための要求事項に優先する。

注

1. 表 E.1-1 に列記された属性は、患者識別の機密性を保証するのには十分ではないかもしれない。特に、識別情報は、規格合成 IOD（PS3.3 の中で定義されもの）の中にはないが、規格拡張 SOP クラスの中で使用される、個人属性、新規格属性、廃止規格属性および追加規格属性に含まれるかもしれない。表 E.1-1 が示すのは、規格合成 IOD に使用される属性および廃止属性である。さらに表 E.1-1 に含むのは、データセットで通常見つからないが、コマンド、ディレクトリおよびメタ情報ヘッダーの中で使用されるいくつかの要素である。しかし、個人のシーケンス内で誤用されることがある。構造化した報告書の本文内容アイテム、表示状態の本文の注釈、カーブおよびオーバーレイは、特にアドレスされる。識別情報はすべて削除されることを保証することは匿名化(De-identifier)の責任である。

2. アプリケーションレベル機密性プロファイルへの適合が必ずしも機密性を保証しないことは注目されるべきである。例えば、もし攻撃者がオリジナル画像に既にアクセスしていれば、ピクセルデータが一致するかもしれない。もっともそのような脅威の可能性および影響は無視できると考えられるかもしれない。もし暗号化属性シーケンスが使用されるならば、暗号化スキームは攻撃に対し脆弱かもしれないことが理解されるべきである。さらに、組織のセキュリティ方針およびかぎ管理方針は、保護の有効性にはるかに大きな影響を及ぼすと認識される。
3. 全国および地方規制は、変わるかもしれないが、追加属性が匿名化(De-identifier)されることを要求する。もっともプロファイルとオプションの設計は、既知の規制を十分に満足し、意図する目的に対する匿名化(De-identifier)インスタンスの有効性を損なわないよう行われた。
4. 表 E.1-1 は規定であるが、しかし、DICOM 規格が進化し、他の同様の属性が IOD に追加されるとともに、表は拡張される。匿名化(De-identifier)はこの拡張性を考慮するかもしれない、例えば、すべての日付および時間を、DT、DA または TM の値表現に基づき扱うことを考慮する。単なる日付および時間属性ではない。
5. プロファイルとオプションは、匿名化(De-identifier)設計が次のことをすべきか否か指定しない。つまり識別漏洩のリスクとして既知のものを削除し、安全であるとして既知のものだけ保持することである。一方で、前者のアプローチは、規格が拡張されるか、ベンダーが予想外の標準またはプライベート属性を加える場合、失敗する。他方で、後者は、各インスタンスを PS3.3 中の情報オブジェクト定義と、完全ではないが広範に比較することを要求する。必要または有用な情報を廃棄することを避けるためである。表 E.1-1 は、適合に必要な最小限のアクションを定義する。
6. 個人の SOP クラスの匿名化(De-identifier)は定義されない。
7. 「C」(消去)アクションは文字列 VR だけでなくコードシーケンスのためにも指定される。なぜなら個人コードまたはローカルコード、および非標準のコード意味を使用すると、識別漏洩を引き起すかもしれないからである。
8. デジタル署名シーケンスは削除される必要がある。なぜならそれが署名者の証明書を含むからである；理論上、署名は検証でき、オブジェクトは匿名化(De-identifier)自身によりそれ自身の証明書で再署名される。しかしこれは規格によって要求されない。
9. 一般に、この表に CS VR 属性はない。なぜなら符号列は識別情報を含まないと仮定することが通常安全であるからである。
10. 一般に、個人のコードを含む、符号化されたシーケンスエントリが識別情報を含まないと仮定することが通常安全であるので、この表にコードシーケンス属性はない。例外は供給者とスタッフのためのコードである。
11. ピクセルデータ消去および認識視覚特徴消去オプションは、この表に列記されない。なぜならそれらは、ピクセルデータ自体に対するオペレーションの記述によって定義されるからである。ピクセルデータ消去オプションは、アイコン画像シーケンス内のピクセルデータに適用されるかもしれない。または、一旦主なデータセットのピクセルデータが消去されたならば、アイコン画像シーケンスは再生成される可能性が高い。アイコン画像シーケンスは削除されることになっている。これはそのピクセルデータが消去できない場合である。
12. オリジナル属性シーケンス(0400,0561) (それは修正属性シーケンス(0400,0550)を含む) は、一般に削除される必要がある。なぜならそれが他の属性の解読されたコピーを含み、属性は修正されていたかもしれない (例えば、外国の画像のインポート中にローカルの確認者および名前を使用することを強制された)；代替アプローチはその内容を選択的に修正することである。これは、暗号化属性シーケンス内で、修正属性シーケンス(0400,0550)を使用することとは異なる(0400,0500)。
13. 表 E.1-1 は、PS3.3 の中で定義された規格合成 IOD の中の属性と、そうでない属性とを区別する；いくつかの属性は PS3.3 の中で他の IOD のため定義されているか、または合成 IOD のトップレベルデータセットの中以外の特定使用方法をもつ。しかし、実装者により、規格拡張 SOP クラスとしてのインスタンス中で、規格によって定義された以外のレベルにおいて (誤って) 使用される。遭遇したそのような属性は削除してもよい。インスタンスの規格 IOD への適合は損なわれない。例えば、検証観察者シーケンス(0040,A073)は、構造化した報告書 IOD の中で単に定義されている。したがって表 E.1-1 では D として述べられている。なぜならそれはタイプ 1C であるからである；もし画像インスタンスの中で遭遇すれば、それは単に削除されることが望ましい (X として扱われる)。

表 E.1-1. アプリケーションレベル機密性プロファイル属性

属性名	タグ	廃止 (PS 3.6か ら)	規格合 成 IOD (PS 3.3か ら)	基礎プ ロファ イル	保持安 全個人 オプシ ョン	保持 UID オ プショ ン	保持装 置識別 オプシ ョン	保持患 者特性 オプシ ョン	保持経 時フル 日付オ プショ ン	保持経 時修正 日付オ プショ ン	記述消 去オプ ション	構造化 目次消 去オプ ション	グラフ 消去オ プショ ン
受入番号	(0008,0050)	N	Y	Z									
収集コメント	(0018,4000)	Y	N	X							C		
収集文脈シー ケンス	(0040,0555)	N	Y	X								C	
収集日	(0008,0022)	N	Y	X/Z					K	C			
収集日付時間	(0008,002A)	N	Y	X/D					K	C			
収集装置処理 記述	(0018,1400)	N	Y	X/D							C		
収集プロトコ ル記述	(0018,9424)	N	Y	X							C		
収集時間	(0008,0032)	N	Y	X/Z					K	C			
実際の間人実 行者シーケ ンス	(0040,4035)	N	N	X									
追加の患者の 履歴	(0010,21B0)	N	Y	X							C		
アドレス (試 行)	(0040,A353)	Y	N	X									
入院 ID	(0038,0010)	N	Y	X									
入院日付	(0038,0020)	N	N	X					K	C			
入院診断コー ドシーケンス	(0008,1084)	N	Y	X							C		
入院診断記述	(0008,1080)	N	Y	X							C		
入院時間	(0038,0021)	N	N	X					K	C			
影響を受けた SOP インス タンス UID	(0000,1000)	N	N	X		K							
アレルギー	(0010,2110)	N	N	X				C			C		
任意	(4000,0010)	Y	N	X									
著者観察者シ ーケンス	(0040,A078)	N	Y	X									
サービスの分 岐	(0010,1081)	N	N	X									
カセット ID	(0018,1007)	N	Y	X			K						

属性名	タグ	廃止 (PS 3.6 から)	規格合 成 IOD (PS 3.3 から)	基礎プ ロファ イル	保持安 全個人 オプシ ョン	保持 UID オ プシ ョン	保持装 置識別 オプシ ョン	保持患 者特性 オプシ ョン	保持経 時フル 日付オ プシ ョン	保持経 時修正 日付オ プシ ョン	記述消 去オプ ション	構造化 目次消 去オプ ション	グラフ 消去オ プシ ョン
実装処理手順に関するコメント	(0040,0280)	N	Y	X							C		
連結 UID	(0020,9161)	N	Y	U		K							
患者データ記述に関する機密性の制約	(0040,3001)	N	N	X									
顧問医師の識別シーケンス	(0008,009D)	N	Y	X									
顧問医師の名前	(0008,009C)	N	Y	Z									
内容作成者の名前	(0070,0084)	N	Y	Z									
内容作成者の識別コードシーケンス	(0070,0086)	N	Y	X									
内容日付	(0008,0023)	N	Y	Z/D					K	C			
内容シーケンス	(0040,A730)	N	Y	X								C	
内容時間	(0008,0033)	N	Y	Z/D					K	C			
造影ボーラス剤	(0018,0010)	N	Y	Z/D							C		
寄与記述	(0018,A003)	N	Y	X							C		
居住する国	(0010,2150)	N	N	X									
現在の観察者 (試行)	(0040,A307)	Y	N	X									
現在の患者位置	(0038,0300)	N	N	X									
カーブデータ	(50xx,xxxx)	Y	N	X									C
カーブ日付	(0008,0025)	Y	Y	X					K	C			
カーブ時間	(0008,0035)	Y	Y	X					K	C			
保管組織シーケンス	(0040,A07C)	N	Y	X									
データセットトレーリングパディング	(FFFC,FFFC)	N	Y	X									
派生記述	(0008,2111)	N	Y	X							C		

属性名	タグ	廃止 (PS 3.6 から)	規格合 成 IOD (PS 3.3 から)	基礎プ ロファ イル	保持安 全個人 オプシ ョン	保持 UID オ プシ ョン	保持装 置識別 オプシ ョン	保持患 者特性 オプシ ョン	保持経 時フル 日付オ プシ ョン	保持経 時修正 日付オ プシ ョン	記述消 去オプ ション	構造化 目次消 去オプ ション	グラフ 消去オ プシ ョン
検出器 ID	(0018,700A)	N	Y	X/D			K						
装置製造番号	(0018,1000)	N	Y	X/Z/D			K						
装置 UID	(0018,1002)	N	Y	U		K	K						
デジタル署名 UID	(0400,0100)	N	Y	X									
デジタル署名 シーケンス	(FFFA,FFFA)	N	Y	X									
ディメンジョン 組織 UID	(0020,9164)	N	Y	U		K							
退院診断記述	(0038,0040)	Y	N	X							C		
配布アドレス	(4008,011A)	Y	N	X									
配布名	(4008,0119)	Y	N	X									
服用量参照 UID	(300A,0013)	N	Y	U		K							
収集終了日付 時間	(0018,9517)	N	Y	X/D					K	C			
エスニックグ ループ	(0010,2160)	N	Y	X				K					
完了予想日時	(0040,4011)	N	N	X					K	C			
失敗した SOP インス タンスの UID リスト	(0008,0058)	N	N	U		K							
規格の UID	(0070,031A)	N	Y	U		K							
実施者オーダ ー番号/画像 化サービスリ クエスト	(0040,2017)	N	Y	Z									
フレームコメ ント	(0020,9158)	N	Y	X							C		
評価基準系 UID	(0020,0052)	N	Y	U		K							
架台 ID	(0018,1008)	N	Y	X			K						
発生器 ID	(0018,1005)	N	Y	X			K						
グラフィック 注釈シーケン ス	(0070,0001)	N	Y	D									C

属性名	タグ	廃止 (PS 3.6 から)	規格合 成 IOD (PS 3.3 から)	基礎プ ロファ イル	保持安 全個人 オプシ ョン	保持 UID オ プシ ョン	保持装 置識別 オプシ ョン	保持患 者特性 オプシ ョン	保持経 時フル 日付オ プシ ョン	保持経 時修正 日付オ プシ ョン	記述消 去オプ ション	構造化 目次消 去オプ ション	グラフ 消去オ プシ ョン
人間実行者名前	(0040,4037)	N	N	X									
人間実行者組織	(0040,4036)	N	N	X									
アイコン画像シーケンス (注 12 を参照)	(0088,0200)	N	Y	X									
識別コメント	(0008,4000)	Y	N	X							C		
画像コメント	(0020,4000)	N	Y	X							C		
画像表示コメント	(0028,4000)	Y	N	X									
画像サービスリクエストコメント	(0040,2400)	N	N	X							C		
印象	(4008,0300)	Y	N	X							C		
インスタンス強制日時	(0008,0015)	N	Y	X					K	C			
インスタンス作成者 UID	(0008,0014)	N	Y	U		K							
施設アドレス	(0008,0081)	N	Y	X									
施設コードシーケンス	(0008,0082)	N	Y	X/Z/D									
施設名	(0008,0080)	N	Y	X/Z/D									
施設部門名	(0008,1040)	N	Y	X									
保険計画識別	(0010,1050)	Y	N	X									
結果の指定受信者識別シーケンス	(0040,1011)	N	N	X									
解釈承認シーケンス	(4008,0111)	Y	N	X									
解釈著者	(4008,010C)	Y	N	X									

属性名	タグ	廃止 (PS 3.6 から)	規格合 成 IOD (PS 3.3 から)	基礎プ ロファ イル	保持安 全個人 オプシ ョン	保持 UID オ プシ ョン	保持装 置識別 オプシ ョン	保持患 者特性 オプシ ョン	保持経 時フル 日付オ プシ ョン	保持経 時修正 日付オ プシ ョン	記述消 去オプ ション	構造化 目次消 去オプ ション	グラフ 消去オ プシ ョン
解釈診断記述	(4008,0115)	Y	N	X							C		
解釈 ID 発行者	(4008,0202)	Y	N	X									
解釈記録者	(4008,0102)	Y	N	X									
解釈テキスト	(4008,010B)	Y	N	X							C		
解釈 トラン スクリャパー	(4008,010A)	Y	N	X									
照射イベント UID	(0008,3010)	N	Y	U		K							
入院 ID の発 行者	(0038,0011)	N	Y	X									
患者 ID の発 行者	(0010,0021)	N	Y	X									
サービスエピ ソード ID の 発行者	(0038,0061)	N	Y	X									
大きなパレット カラーlookup アップテー ブル UID	(0028,1214)	Y	N	U		K							
最後の月経日 付	(0010,21D0)	N	N	X					K	C			
MAC	(0400,0404)	N	Y	X									
媒体保存 SOP インス タンス UID	(0002,0003)	N	N	U		K							
医療警報	(0010,2000)	N	N	X							C		
カルテロケー タ	(0010,1090)	N	N	X									
軍隊階級	(0010,1080)	N	N	X									
修正属性シー ケンス	(0400,0550)	N	N	X									
修正画像記述	(0020,3406)	Y	N	X									
修正装置 ID	(0020,3401)	Y	N	X									
修正装置メー カー	(0020,3404)	Y	N	X									
スタディを読 影する医師の 名前	(0008,1060)	N	Y	X									

属性名	タグ	廃止 (PS 3.6 から)	規格合 成 IOD (PS 3.3 から)	基礎プ ロファ イル	保持安 全個人 オプシ ョン	保持 UID オ プシ ョン	保持装 置識別 オプシ ョン	保持患 者特性 オプシ ョン	保持経 時フル 日付オ プシ ョン	保持経 時修正 日付オ プシ ョン	記述消 去オプ ション	構造化 目次消 去オプ ション	グラフ 消去オ プシ ョン
結果の、意図された受け手の名前	(0040,1010)	N	N	X									
観察日付 (試 行)	(0040,A192)	Y	N	X					K	C			
観 察 対 象 の UID (試行)	(0040,A402)	Y	N	U		K							
観察時間 (試 行)	(0040,A193)	Y	N	X					K	C			
観察 UID	(0040,A171)	N	Y	U		K							
占有	(0010,2180)	N	Y	X							C		
オペレータの 識別シーケ ンス	(0008,1072)	N	Y	X/D									
オペレータの 名前	(0008,1070)	N	Y	X/Z/D									
オリジナル属 性シーケンス	(0400,0561)	N	Y	X									
オーダーコー ルバック電話 番号	(0040,2010)	N	N	X									
オーダーコー ルバックテレ コム情報	(0040,2011)	N	N	X									
オーダー入力 者	(0040,2008)	N	N	X									
オーダー入力 者の位置	(0040,2009)	N	N	X									
他の患者 ID	(0010,1000)	N	Y	X									
他の患者 ID シーケンス	(0010,1002)	N	Y	X									
他の患者名前	(0010,1001)	N	Y	X									
オーバレイコ メント	(60xx,4000)	Y	N	X									C
オーバレイデ ータ	(60xx,3000)	N	Y	X									C
オーバレイ日 付	(0008,0024)	Y	Y	X					K	C			
オーバレイ時 間	(0008,0034)	Y	Y	X					K	C			
パレットカラ ールックアッ プテーブル UID	(0028,1199)	N	Y	U		K							

属性名	タグ	廃止 (PS 3.6 か ら)	規格合 成 IOD (PS 3.3 か ら)	基礎プ ロファ イル	保持安 全個人 オプシ ョン	保持 UID オ プショ ン	保持装 置識別 オプシ ョン	保持患 者特性 オプシ ョン	保持経 時フル 日付オ プショ ン	保持経 時修正 日付オ プショ ン	記述消 去オプ ション	構造化 目次消 去オプ ション	グラフ 消去オ プショ ン
参加者シーケンス	(0040,A07A)	N	Y	X									
患者アドレス	(0010,1040)	N	N	X									
患者コメント	(0010,4000)	N	Y	X							C		
患者 ID	(0010,0020)	N	Y	Z									
患者性別中性化	(0010,2203)	N	Y	X/Z				K					
患者の州	(0038,0500)	N	N	X				C			C		
患者輸送準備	(0040,1004)	N	N	X									
患者の年齢	(0010,1010)	N	Y	X				K					
患者の生年月日	(0010,0030)	N	Y	Z									
患者の出生名	(0010,1005)	N	N	X									
患者の誕生時間	(0010,0032)	N	Y	X									
患者の施設住居	(0038,0400)	N	N	X									
患者の保険計画コードシーケンス	(0010,0050)			X									
患者の母の出生名	(0010,1060)	N	N	X									
患者の名前	(0010,0010)	N	Y	Z									
患者の一次言語コードシーケンス	(0010,0101)			X									
患者の一次言語修飾語コードシーケンス	(0010,0102)			X									
患者の宗教の好み	(0010,21F0)	N	N	X									
患者の性別	(0010,0040)	N	Y	Z				K					
患者のサイズ	(0010,1020)	N	Y	X				K					
患者のテレコム情報	(0010,2155)	N	N	X									

属性名	タグ	廃止 (PS 3.6 から)	規格合 成 IOD (PS 3.3 から)	基礎プ ロファ イル	保持安 全個人 オプシ ョン	保持 UID オ プシ ョン	保持装 置識別 オプシ ョン	保持患 者特性 オプシ ョン	保持経 時フル 日付オ プシ ョン	保持経 時修正 日付オ プシ ョン	記述消 去オプ ション	構造化 目次消 去オプ ション	グラフ 消去オ プシ ョン
患者の電話番号	(0010,2154)	N	N	X									
患者の体重	(0010,1030)	N	Y	X				K					
実施場所	(0040,0243)	N	N	X									
実施処理手順 記述	(0040,0254)	N	Y	X							C		
処理手順終了 日付	(0040,0250)	N	Y	X					K	C			
処理手順終了 日時	(0040,4051)	N	N	X					K	C			
処理手順終了 時間	(0040,0251)	N	Y	X					K	C			
実装処理手順 ID	(0040,0253)	N	Y	X									
実施処理手順 開始日	(0040,0244)	N	Y	X					K	C			
実施処理手順 開始日時	(0040,4050)	N	N	X					K	C			
実施処理手順 開始時刻	(0040,0245)	N	Y	X					K	C			
実施ステー ション AE タイ トル	(0040,0241)	N	N	X			K						
実施ステー ション地理的 地域コードシー ケンス	(0040,4030)	N	N	X			K						
実施ステー ション名前	(0040,0242)	N	N	X			K						
実施ステー ションネームコ ードシーケ ンス	(0040, 4028)	N	N	X			K						
実施医師の識 別 シーケ ンス	(0008,1052)	N	Y	X									

属性名	タグ	廃止 (PS 3.6 か ら)	規格合 成 IOD (PS 3.3 か ら)	基礎プ ロファ イル	保持安 全個人 オプシ ョン	保持 UID オ プショ ン	保持装 置識別 オプシ ョン	保持患 者特性 オプシ ョン	保持経 時フル 日付オ プショ ン	保持経 時修正 日付オ プショ ン	記述消 去オプ ション	構造化 目次消 去オプ ション	グラフ 消去オ プショ ン
実施医師の名前	(0008,1050)	N	Y	X									
人のアドレス	(0040,1102)	N	Y	X									
人の識別コードシーケンス	(0040,1101)	N	Y	D									
人名	(0040,A123)	N	Y	D									
人のテレコム情報	(0040,1104)	N	Y	X									
人の電話番号	(0040,1103)	N	Y	X									
解釈を承認した医師	(4008,0114)	Y	N	X									
医師読影スタディ識別シーケンス	(0008,1062)	N	Y	X									
記録の医師	(0008,1048)	N	Y	X									
記録の医師識別シーケンス	(0008,1049)	N	Y	X									
発行オーダー番号/画像化サービスリクエスト	(0040,2016)	N	Y	Z									
プレート ID	(0018,1004)	N	Y	X			K						
前投薬	(0040,0012)	N	N	X				C					
妊娠の有無	(0010,21C0)	N	N	X				K					
プレゼンテーション表示収集 UID	(0070,1101)	N	Y	U		K							
プレゼンテーションシーケンス収集 UID	(0070,1102)	N	Y	U		K							
手順ステップキャンセル日時	(0040,4052)	N	N	X					K	C			
プライベート属性	(gggg,eeee) ここで gggg は奇数	N	N	X	C								

属性名	タグ	廃止 (PS 3.6 から)	規格合 成 IOD (PS 3.3 から)	基礎プ ロファ イル	保持安 全個人 オプシ ョン	保持 UID オ プシ ョン	保持装 置識別 オプシ ョン	保持患 者特性 オプシ ョン	保持経 時フル 日付オ プシ ョン	保持経 時修正 日付オ プシ ョン	記述消 去オプ ション	構造化 目次消 去オプ ション	グラフ 消去オ プシ ョン
プロトコル名	(0018,1030)	N	Y	X/D							C		
省略理由の記述	(300C,0113)	N	Y	X							C		
画像化サービ スリクエスト の理由	(0040,2001)	Y	N	X							C		
スタディの理 由	(0032,1030)	Y	N	X							C		
参照されたデ ジタル署名シ ーケンス	(0400,0402)	N	Y	X									
参照 UID の参 照されたフレ ーム	(3006,0024)	N	Y	U		K							
参照された一 般目的予定処 理ステップト ランザクシ ョン UID	(0040,4023)	Y	N	U		K							
参照された画 像シーケンス	(0008,1140)	N	Y	X/Z/U*		K							
参照された観 察 UID (試 行)	(0040,A172)	Y	N	U		K							
参照された患 者別名シー ケンス	(0038, 0004)	N	N	X									
参照された患 者写真シー ケンス	(0010,1100)	N	Y	X									
参照された患 者シーケ ンス	(0008,1120)	N	Y	X		X							
参照された実 施処理手順シ ーケンス	(0008,1111)	N	Y	X/Z/D		K							
参照された SOP インス タンス MAC シーケンス	(0400,0403)	N	Y	X									
参照された SOP インス タンス UID	(0008,1155)	N	Y	U		K							

属性名	タグ	廃止 (PS 3.6 から)	規格合 成 IOD (PS 3.3 から)	基礎プ ロファ イル	保持安 全個人 オプシ ョン	保持 UID オ プシ ョン	保持装 置識別 オプシ ョン	保持患 者特性 オプシ ョン	保持経 時フル 日付オ プシ ョン	保持経 時修正 日付オ プシ ョン	記述消 去オプ ション	構造化 目次消 去オプ ション	グラフ 消去オ プシ ョン
ファイル中の参照された SOP インスタンス UID	(0004,1511)	N	N	U		K							
参照スタディシーケンス	(0008,1110)	N	Y	X/Z		K							
参照医師のアドレス	(0008,0092)	N	N	X									
参照医師の識別シーケンス	(0008,0096)	N	Y	X									
参照医師の名前	(0008,0090)	N	Y	Z									
参照医師の電話番号	(0008,0094)	N	N	X									
住居のある地域	(0010,2152)	N	N	X									
参照 UID の関連するフレーム	(3006,00C2)	N	Y	U		K							
リクエスト属性シーケンス	(0040,0275)	N	Y	X							C		
要求された造影剤	(0032,1070)	N	N	X							C		
要求された手続きコメント	(0040,1400)	N	N	X							C		
要求された手続きの記述	(0032,1060)	N	Y	X/Z							C		
要求手続き ID	(0040,1001)	N	N	X									
要求手続き位置	(0040,1005)	N	N	X									
要求された SOP インスタンス UID	(0000,1001)	N	N	U		K							
要求する医師	(0032,1032)	N	N	X									
要求サービス	(0032,1033)	N	N	X									

属性名	タグ	廃止 (PS 3.6 か ら)	規格合 成 IOD (PS 3.3 か ら)	基礎プ ロファ イル	保持安 全個人 オプシ ョン	保持 UID オ プショ ン	保持装 置識別 オプシ ョン	保持患 者特性 オプシ ョン	保持経 時フル 日付オ プショ ン	保持経 時修正 日付オ プショ ン	記述消 去オプ ション	構造化 目次消 去オプ ション	グラフ 消去オ プショ ン
責任を負う組織	(0010,2299)	N	Y	X									
責任者	(0010,2297)	N	Y	X									
結果コメント	(4008,4000)	Y	N	X							C		
結果分配リストシーケンス	(4008,0118)	Y	N	X									
結果 ID 発行者	(4008,0042)	Y	N	X									
レビューアの名前	(300E,0008)	N	Y	X/Z									
予定された人間の実行者シーケンス	(0040,4034)	N	N	X									
予定患者施設住居	(0038,001E)	Y	N	X									
予定実施医師識別シーケンス	(0040,000B)	N	N	X									
予定実施医師名	(0040,0006)	N	N	X									
予定処理手順終了日付	(0040,0004)	N	N	X					K	C			
予定処理手順終了時間	(0040,0005)	N	N	X					K	C			
予定処理手順記述	(0040,0007)	N	Y	X							C		
予定処理手順位置	(0040,0011)	N	N	X			K						
予定処理手順修正日時	(0040,4010)	N	N	X					K	C			
予定処理手順開始日	(0040,0002)	N	N	X					K	C			

属性名	タグ	廃止 (PS 3.6 から)	規格合 成 IOD (PS 3.3 から)	基礎プ ロファ イル	保持安 全個人 オプシ ョン	保持 UID オ プシ ョン	保持装 置識別 オプシ ョン	保持患 者特性 オプシ ョン	保持経 時フル 日付オ プシ ョン	保持経 時修正 日付オ プシ ョン	記述消 去オプ ション	構造化 目次消 去オプ ション	グラフ 消去オ プシ ョン
予定処理手順 開始日時	(0040,4005)	N	N	X					K	C			
予定処理手順 開始時間	(0040,0003)	N	N	X					K	C			
予定ステーシ ョン AE タイ トル	(0040,0001)	N	N	X			K						
予定ステーシ ョン地理的地 域コードシ ーケンス	(0040,4027)	N	N	X			K						
予定ステーシ ョン名前	(0040,0010)	N	N	X			K						
予定ステーシ ョンネームコ ードシーク ェンス	(0040,4025)	N	N	X			K						
予定スタディ 位置	(0032,1020)	Y	N	X			K						
予定スタディ 位置 AE タイ トル	(0032,1021)	Y	N	X			K						
シリーズ日付	(0008,0021)	N	Y	X/D					K	C			
シリーズ記述	(0008,103E)	N	Y	X							C		
シリーズイン スタンス UID	(0020,000E)	N	Y	U		K							
シリーズ時間	(0008,0031)	N	Y	X/D					K	C			
サービスエピ ソード記述	(0038,0062)	N	Y	X							C		
サービスエピ ソード ID	(0038,0060)	N	Y	X									
喫煙状態	(0010,21A0)	N	N	X				K					
SOP インス タンス UID	(0008,0018)	N	Y	U		K							
ソース画像シ ーケンス	(0008,2112)	N	Y	X/Z/U*		K							
ソース認識番 号	(3008,0105)	N	Y	X			K						
特別ニーズ	(0038,0050)	N	N	X				C					
収集開始日付 時間	(0018,9516)	N	Y	X/D					K	C			
ステーション 名	(0008,1010)	N	Y	X/Z/D			K						

属性名	タグ	廃止 (PS 3.6 から)	規格合 成 IOD (PS 3.3 から)	基礎プ ロファ イル	保持安 全個人 オプシ ョン	保持 UID オ プシ ョン	保持装 置識別 オプシ ョン	保持患 者特性 オプシ ョン	保持経 時フル 日付オ プシ ョン	保持経 時修正 日付オ プシ ョン	記述消 去オプ ション	構造化 目次消 去オプ ション	グラフ 消去オ プシ ョン
保存媒体ファ イル- セット UID	(0088,0140)	N	Y	U		K							
スタディコメ ント	(0032,4000)	Y	N	X							C		
スタディ日付	(0008,0020)	N	Y	Z					K	C			
スタディ記述	(0008,1030)	N	Y	X							C		
スタディ ID	(0020,0010)	N	Y	Z									
スタディ ID 発行者	(0032,0012)	Y	N	X									
スタディイン スタンス UID	(0020,000D)	N	Y	U		K							
スタディ時間	(0008,0030)	N	Y	Z					K	C			
同期評価基準 系 UID	(0020,0200)	N	Y	U		K							
対象 UID	(0018,2042)	N	Y	U		K							
電話番号 (試 行)	(0040,A354)	Y	N	X									
テンプレート 拡張作成者 UID	(0040,DB0D)	Y	N	U		K							
テンプレート 拡張組織 UID	(0040,DB0C)	Y	N	U		K							
テキストコメ ント	(4000,4000)	Y	N	X									
テキスト文字 列	(2030,0020)	N	N	X									
UTCから時間 帯オフセット	(0008,0201)	N	Y	X					K	C			
トピック著者	(0088,0910)	Y	N	X									
トピックのキ ーワード	(0088,0912)	Y	N	X									
トピック主題	(0088,0906)	Y	N	X									
トピックタイ トル	(0088,0904)	Y	N	X									
追跡 UID	(0062,0021)	N	Y	U		K							
トランザクシ ョン UID	(0008,1195)	N	N	U		K							
UID	(0040,A124)	N	Y	U									
言葉のソース (試行)	(0040,A352)	Y	N	X									
言葉ソース ID コードシーケ ンス (試行)	(0040,A358)	Y	N	X									

属性名	タグ	廃止 (PS 3.6 か ら)	規格合 成 IOD (PS 3.3 か ら)	基礎プ ロファ イル	保持安 全個人 オプシ ョン	保持 UID オ プシ ョン	保持装 置識別 オプシ ョン	保持患 者特性 オプシ ョン	保持経 時フル 日付オ プシ ョン	保持経 時修正 日付オ プシ ョン	記述消 去オプ ション	構造化 目次消 去オプ ション	グラフ 消去オ プシ ョン
検証観察者識別コードシーケンス	(0040,A088)	N	Y	Z									
検証観察者名前	(0040,A075)	N	Y	D									
検証観察者シーケンス	(0040,A073)	N	Y	D									
検証組織	(0040,A027)	N	Y	X									
訪問コメント	(0038,4000)	N	N	X							C		

E.1.2 再識別化(Re-identifier)

アプリケーションは、アプリケーションが、保護された SOP インスタンスから保護を削除できる場合、再識別化(Re-identifier)としてのアプリケーションレベル機密性プロファイルへの適合を要求してもよい。条件は受信者かぎが、SOP インスタンスの暗号化属性シーケンス(0400,0500)内の 1 つ以上の暗号化内容(0400,0520)属性を解読するため要求されるが、それが利用可能であることである。この文脈中の保護の削除は次のプロセスとして定義される：

1. アプリケーションによって、受信者かぎを用いて、暗号化属性シーケンス(0400,0500)内の暗号化内容(0400,0520)属性の 1 つのインスタンスは解読されなければならない。また、バイトの結果ブロックを DICOM データセットに解読されなければならない。これに用いるのは、暗号化内容転送構文 UID(0400,0510)中で指定された転送構文である。このプロファイルへの適合を主張する再識別は、暗号化内容を解読できなければならない。これに用いるのは AES または Triple-DES の何れかであり、このプロファイルの中で指定されたあらゆるかぎ長さを用いる。

注

アプリケーションが、暗号化属性シーケンス(0400,0500)内の暗号化内容(0400,0520)属性の 2 つ以上のインスタンスを解読できる場合、アプリケーションの裁量により何れか 1 つのインスタンスを選ぶ。

2. アプリケーションは、解読されたデータセットの修正属性シーケンス(0400,0550)の単一のアイテムに含まれる属性をすべて、主なデータセットの中へ移動させなければならない。そのとき主なデータセット中にある「ダミー値」の属性を置換する。

注

1. 再識別はオリジナルの SOP インスタンスの完全な再構成を意味しない。なぜなら保護されている属性すべてが暗号化属性データセットの一部になるよう要求されることはないからである。オリジナルの UID が暗号化属性データセットの一部である場合、それらはオリジナルの無防備の SOP インスタンスへのアクセスを獲得するのに使用可能かもしれない。
2. 解読できない暗号化データセットの存在は、メッセージ中の属性値のうちいくつかまたはすべてがリアルではない（それらはダミーである）ことを示す。したがって、受信者は、メッセージ中のどの値も診断的に適切であると考えてはならない。
3. 属性患者識別削除(0012,0062)は、置換されるかまたはデータセットに、NO の値を用いて追加されなければならない。また匿名化(De-identifier)方法(0012,0063)および匿名化(De-identifier)方法コードシーケンス(0012,0064)は削除されなければならない。

E.1.3 適合要求事項

アプリケーションレベル機密性プロファイルへの適合を要求するアプリケーションの適合性宣言書は、次項を記述しなければならない：

- どの属性が保護の間に削除されるか；

- どの属性がダミー値と取り替えられるか。また、ダミー値はどのように生成されるか；
- どの属性が暗号化された属性データセットに含まれて後日に再識別されるか。および関連の詳細事項、つまり暗号化の実施のためにかぎがどのように選択されるか；
- 多数の SOP インスタンスが保護される場合である（例えば、多数のスタディをまとめて、同じスタディが 2 度以上処理された場合の一貫した置換など）、アプリケーションは、参照のための置換値の参照完全性をどの範囲まで保証できるか、例えば、SOP インスタンス UID、評価基準系 UID などである；
- どの属性および属性値が SOP インスタンスの保護の間に挿入されるか；
- どの転送構文が暗号化された属性データセットの符号化／復号化のために支援されるか；
- どのオプションが支援されるか；
- 追加の制限（例えば、公開かぎのためのかぎサイズ）。

E.2 基礎アプリケーションレベル機密性プロファイル

このプロファイルは治験および他のシナリオでの使用を意図する。その場合に匿名化(De-identifier)が要求される。例えば、教育用ファイルの生成、その他の種類の出版、画像および関連情報の登録（例えば、腫瘍内科学または放射線量の登録）への提出である。

この基礎アプリケーションレベル機密性プロファイルは、非常に保守的なアプローチを定義する。それは次のものと関係する情報をすべて削除する：

- 患者の識別および人口統計的特性
- 責任者または家族の識別
- 手続きに関与する人員の識別
- 手続きを命じるかまたは行うことに関与する組織の識別
- インスタンスをマッチさせるために使用できる追加情報。これはオリジナル、例えば、UID、日付および時間にアクセスできる場合である。
- プライベート属性

これはその情報が、表 E.1-1 に述べるグラフィックスまたはオーバーレイを含む非ピクセルデータ属性中にある場合である。

注

もしピクセルデータ消去オプションも指定されなければ、このプロファイルはピクセルに焼き付けられた情報にアドレスしない。

属性経時時間情報修正(0028,0303)は、「REMOVED」の値を用いてデータセットに追加されなければならない。これは保持経時時間情報オプションの何れも適用されない場合である。

E.3 基礎アプリケーションレベル機密性オプション

様々なオプションが、基礎アプリケーションレベル機密性プロファイルに適用可能であると定義される。これらのオプションのうちのいくつかは、追加情報の削除を要求し、これらのオプションのうちのいくつかは、本来削除される情報の保持を要求する。

次のオプションが定義され、これらは追加情報の削除を要求する：

- ピクセルデータ消去オプション
- 認識視覚特徴消去オプション
- グラフィックス消去オプション
- 構造化内容消去オプション
- ディスクリプタ消去オプション

次のオプションが定義され、本来削除されるが特定用法に必要とされる情報の保持を要求する：

- 保持経時時間情報のフル日付つきオプション
- 保持経時時間情報の修正日付つきオプション
- 保持患者特性オプション
- 保持装置識別オプション
- 保持 UID
- 保持安全個人オプション

E.3.1 ピクセルデータ消去オプション

このオプションがアプリケーションレベル機密性プロファイルに追加され指定される場合、情報がピクセルデータ(7FE0,0010)に焼き付けられ、プロファイルおよび他の指定オプションによって削除を指定された属性情報に対応するとき、それも削除されなければならない。表 E-1-1 に述べるとおりである。

これは、人間のオペレータの介在またはオペレータによる承認を要求するかもしれない。

属性焼き付け注釈(0028,0301)は、「NO」の値を用いてデータセットに追加されなければならない。

注

1. この能力は特定のオプションとして呼ばれる。なぜならそれは実装するのに実際上非常に厄介かもしれないし、そのような注釈の中で第一に焼き付けないモダリティの大部分には不必要であるからである。一方で、例えばコンピュータ断層撮影は、そのような焼き付け注釈を含まない。他方で、超音波映像は慣例的にそれを含む。
2. 画像処理および光学文字認識の技術は、焼き付けテキストの存在および位置を検知するために使用できる。既知の識別情報に対するマッチングも応用できる。しかしそのテキストが識別情報かまたは他の種類の情報が決めることが重要である。このオプションへの適合は、識別情報の削除を要求する。それがどのように達成されるかを問わない。情報は、非ピクセルデータ中の保持を他のオプション（例えば、身体特性、日付またはディスクリプタ）によって要求されているから、ピクセルデータの方に焼き付け保持される必要はない。したがって、焼き付けテキストをすべて削除する最も保守的なアプローチは、適合する。これにより、追加の有用な情報、例えばローカライズ配置およびマニュアルグラフィック注釈が犠牲になるかもしれない。
3. 保存されたピクセル値は変更されることになっている（抹消される）；オーバーレイ若しくはグラフィックの注釈を重ね合わせるか、またはピクセルデータ値を隠すためシャッタを置くことは十分ではない。なぜならそれらは受信システムによって無視されないかもしれないからである。
4. このオプションが意図するのは、画像蓄積 SOP インスタンスのトップレベルデータセットに生じるピクセルデータ(7FE0,0010)属性に当てはまることである。ピクセルデータ(7FE0,0010)の別の標準的用法はアイコン画像シーケンス(0088,0200)内にある。それは表 E-1-1 に既に述べられ、削除を要求するとして注記されている。このオプションは、トップレベルデータセット以外の位置に生じるピクセルデータ(7FE0,0010)のピクセル値を手動または自動で処理する能力を要求しない。しかし、それはその能力を禁止しない。プライベート属性内に生じるピクセルデータ(7FE0,0010)が削除される。なぜならそのような属性は、安全であると知られていないからである。

E.3.2 認識視覚特徴消去オプション

このオプションがアプリケーションレベル機密性プロファイルに追加されて指定される場合、十分な視覚情報が1組のインスタンスのピクセルデータ内にあり、個人がインスタンス自体からまたは1組のインスタンスの再構成から認識できるとき、ピクセルデータの十分な削除または歪曲が認識を防ぐために応用されなければならない。

これは、人間のオペレータの介在またはオペレータによる承認を要求するかもしれない。

属性認識視覚特徴(0028,0302)は「NO」の値を用いてデータセットに追加されなければならない。

注

1. それが実装するのに実際上非常に厄介かもしれないし、解剖学的部位と物理療法の大部分には不必要であるので、この能力は特定のオプションとして呼ばれる。
2. 顔写真の場合、視覚的に識別されるリスクが明白であるので、多数の技術が匿名化(De-identifier)のため十分に確立されている。例えば、目を黒い四角で隠すなどである。
3. 頭部および頸部全体の高解像度の横断画像の場合、示唆されているのは、ピクセルデータの 3D ボリュームまたは表面レンダリングが十分であり、いくつかの状況の下で識別（または、個人の制約された部分集合に対するマッチング）ができることである。
4. このオプションを応用すると、ピクセルデータが集められた目的に対し使用不能になるかもしれない。したがって、それを使用する場合、匿名化(De-identifier)と、適切な倫理承認および「説明と同意」の入手に基づく有用性と兼ね合いが必要になる。例えば、歯の画像の場合を考慮しなければならない。
5. 参照された患者写真シーケンスは基本プロファイルの一部として削除されるため、認識視覚特徴消去オプションのサポートはその属性に対する要件を追加しない。

E.3.3 グラフィックス消去オプション

様々な規格および規格拡張 SOP クラスのインスタンス（例えば、画像、表示状態および他の合成 SOP インスタンス）は、グラフィックス、テキスト注釈またはオーバーレイとして符号化された識別情報を含むかもしれない。これは、構造化した報告書 SOP クラスに含まれる情報を含まない。

このオプションがアプリケーションレベル機密性プロファイルに追加されて指定される場合、情報がグラフィックス、テキスト注釈またはオーバーレイで符号化され、プロファイルおよび他の指定情報によって削除を指定された属性情報に対応するとき、それも削除されなければならない。表 E.1-1 に述べるとおりである。

これは人間のオペレータの介在を要求するかもしれない。

注

1. この能力は特定のオプションとして呼ばれる。なぜならそのようなグラフィックス、テキスト注釈またはオーバーレイをすべて削除する方が実際的かもしれないからである（このオプションのないプロファイルによって要求されるように）。
2. 焼き付けピクセルデータ注釈に関しては、テキストが識別情報かまたは他の種類の情報が決めることが重要である。情報は、他のオプション（例えば、身体特性、日付またはディスクリプタ）によって非ピクセルデータ中で保持されるよう指定されるので、グラフィックス、テキスト注釈またはオーバーレイ中で保持されることは必要とされない。

E.3.4 構造化内容消去オプション

構造化レポート SOP クラスのインスタンスは、内容アイテム中で符号化された内容シーケンス(0040,A730)の中に識別可能な情報を含むかもしれない。他の SOP クラスのインスタンスは、収集文脈シーケンス(0040,0555)または標本調製シーケンス(0040,0610)の中に同様の方法で符号化された構造化内容を含むかもしれない。

このオプションがアプリケーションレベル機密性プロファイルに追加されて指定される場合、情報が SR 内容アイテムまたは収集文脈または標本調製シーケンスアイテムの中で符号化され、プロファイルおよび他の指定オプションによって削除を指定される属性情報に対応するとき、それも削除されなければならない。

注

1. 例えば、画像診断報告書に責任を負う「観察者」は、SR 中の観察内容関連の内容アイテム中で明示的に識別されるかもしれない。
2. このオプションを実装しない匿名化(De-identifier)は、構造化レポートを匿名化(De-identifier)しようとするとき著しいリスクを引き起こす。内容シーケンス中に識別情報をもたないと分かっているインスタンスを匿名化(De-identifier)するため使用するだけの場合は、その限りでない。

E.3.5 ディスクリプタ消去オプション

たとえ多くの属性が、特定の目的、例えばスタディまたはシリーズの記述のため DICOM 規格に定義されていても、オペレータが管理する平文を含むものは、識別を含む非体系的な情報を含むかもしれない。

このオプションがアプリケーションレベル機密性プロファイルに追加されて指定される場合、情報がテキストまたは文字列属性に埋込まれ、プロファイルおよび他の指定オプションによって削除を指定された属性情報に対応するとき、それも削除されなければならない。表 E. 1-1 に述べるとおりである。

注

1. 例えば、オペレータは人の名前または患者の人口統計若しくは身体特性をスタディ記述(0008,1030)に含めるかもしれない。なぜならそれらのモダリティのユーザーインターフェースが他のフィールドを提供しないから、または、他のシステムがそれらを表示しないからである。例えば、記述は「CT 胸腹骨盤-55F Dr. Smith」を含むかもしれない。
2. そのようなテキスト文字列を人間が介在せずに消去する一つのアプローチは、有用で安全な値だけを抽出し保持し、他の値をすべて廃棄することである。例えば、文字列で「CT 胸腹骨盤-55F, Dr. Smith」がスタディ記述(0008,1030)中にあれば、「CT 胸腹骨盤」を検知し保持し、残りを廃棄するのが実用的である。国際的な設定では、これは保持するのに安全な単語の広範囲な辞書を要求するかもしれない。例えば「Buik」はオランダ語で腹、「λεκάνη」はギリシャ語で骨盤である。別の可能性は、そのような情報を抽出し、情報を他の属性(そうでなければ不在または空いている)、例えば、解剖部位シーケンス(0008,2218)で符号化することである。しかしながら、文字列の値が、異なる用途であり、識別的で記述的である可能性が考慮される必要がある。例えば「Dr. Hand」または「M.Genou」。
3. 表 E.1-1 は、リスクがあると知られている特定の属性を呼び出す。しかし実装者は文字データを含む可能性のある属性を考慮したいかもしれない。もっともこのオプションはこれが行われることを必要としない。例えば、SH, LO, ST, LT および UT 値表現はすべて恐らく誤用される。符号列 (CS) は一般にリスクがない。しかし既知の定義語および数値に照らしてのチェックを行うことができるかもしれない。非常に異常であるが、DS または IS の文字列さえ誤用されることがある。また、法的な数字だけが使用されるようチェックする。PN 属性は明らかにリスクがある。OB VR は保持安全個人オプションの中で議論される。
4. このオプションが指定するのは、何を削除する必要があるかであり、何を保持する必要があるかではない。それはアプリケーション次第で異なる。技法記述のような情報を保持することが望ましいかもしれない。しかし、例えば、診断のような他の情報は、治験の解釈に影響するので、廃棄することが望ましいかもしれない。例えば、1つのアプローチは、記述およびコメント属性を、シリーズ記述(0008,103E)以外はすべて削除することである。なぜならこの属性は、識別または診断情報を含むことは稀であるが、収集技法に関する有用な情報の信頼できる源であるからである。それはモダリティ装置プロトコルから自動的に実装される。もっとも注2に述べるように、それは今までどおり消去できる。
5. ディスクリプタが特に異常な手順または条件に関する情報を含む場合、それは、他の人口学的情報と共に、画像化の被験者の人数を減らすかもしれないことを認識することが望ましい。しかしながら、条件または他の異常な身体特徴が画像自体の読影から明白な場合、これはある程度まで真実である。例えば、特定の月にフィラデルファアで何人の接着双胎が生まれたか。

クリーニングの方法は適合性宣言書に述べられなければならない。

E.3.6 保持経時時間情報オプション

日付と時間は、それらが画像化の被験者であり得る可能な人数を制約するので、識別が漏洩する可能性があるとして認められる。もっとも当該個人に関する他の情報へのアクセスがあり、照合できる場合に限る。

しかしながら、目的を達成するため日付と時間の存在を必要とするアプリケーションがある。これは、治療の治験において特に真実である。治験の目的が評価項目の経時変化を測定することである。さらに、しばしば必要なことは、画像からの情報を他の情報源、例えば臨床および検査データと照合することであり、日付と時間が一貫している必要がある。

2つのオプションがこれらの要求事項をアドレスするよう指定される：

- 保持経時時間情報のフル日付つきオプション
- 保持経時時間情報の修正日付つきオプション

保持経時時間情報のフル日付つきオプションが、アプリケーションレベル機密性プロファイルに追加されて指定される場合、属性中の日付および時間は保持されなければならない。表 E.1-1 に述べるとおりである。属性経時時間情報修正 (0028,0303)は「UNMODIFIED」の値を用いてデータセットに追加されなければならない。

保持経時時間情報の修正日付オプションが、アプリケーションレベル機密性プロファイルに追加されて指定される場合、表 E.1-1 に列記された属性中の日付および時間が修正されなければならない。日付と時間は次の方法で修正されなければならない。

- 再識別とマッチする可能性を縮小するように日付を集積するかまたは変形する。
- アプリケーションに必要な程度まで、異なる日付に得られた画像の総体の経時時間関係を保存する。
- アプリケーションのための画像分析に必要な程度まで、画像と現実のイベントとの間の細かい時間関係を保存する。

属性経時時間情報修正(0028,0303)は「MODIFIED」の値を用いてデータセットに追加されなければならない。

注

1. 日付は種々の手段で集積する。例えば、すべての日付を月の第1日に設定する、すべての月を年の第1月に設定するなどである。それはアプリケーションに必要な精度によって異なる。
2. 日付および時間をすべてダミー値に修正できる。それには日付および時間を任意のエポックに関してシフトする。したがって精密な経時時間関係を1組のスタディ中で保持する。これは組全体を同時に匿名化(De-identifier)するときか、または別の機会にこのプロセスを繰り返すためある種の写像またはデータベースを維持するときである。
3. 日付および時間の変形は一緒に考慮することが望ましい。真夜中をはさむスタディを扱うためである。
4. 時間は、分析に要する計算を乱さぬよう変形することが望ましい。例えば、PET SUVのための注入時間開始と収集時間との比較、または動的造影スタディからの時間強度値の抽出である。

日付修正の方法は適合性宣言書に述べられなければならない。

E.3.7 保持患者特性オプション

患者の身体特性は、記述的でありそれ自体は識別情報でないが、識別が漏洩する可能性があるとして認められる。なぜなら身体特性は画像化の被験者の人数を制約するからである。もっとも当該個人に関する他の情報へのアクセスがあり、それと照合できる場合に限る。

しかしながら、そのような身体特性を要求するアプリケーションがある。画像を分析するのに必要な計算を行い、目的を果たすアプリケーションである。1つのそのようなクラスのアプリケーションは、代謝指標に関連するもの、例えば、PET 標準摂取率(SUV)またはDEXA若しくは身体成分のMRI指標であり、それらは、体重、体表面積または除脂肪体重に基づく。

このオプションがアプリケーションレベル機密性プロファイルに追加されて指定される場合、年齢、性別、身長および体重および属性中にある他の特性に関する情報が保持されなければならない。表 E.1-1 に述べるとおりである。

保持された属性のクリーニングの方法は適合性宣言書に述べられなければならない。

E.3.8 保持装置識別オプション

収集を行うために使用された装置の識別に関する情報は、識別の漏洩の可能性をもっていると認められる。なぜならそれが画像化の被験者であり得る可能な個人の数に制約するかもしれないからである。もっとも当該個人に関する他の情報へのアクセスがあり、それと装置情報を照合できる場合に限る。

しかしながら、分析かまたは解釈を行うことをそのような装置情報に要求するアプリケーションがある。空間かまたは他の異質のための矯正の種類は、特定装置の製品番号の知識を要求するかもしれない。特定装置が以前に限定された(例えば、ファントムで)という確認が必要かもしれない。さらに、規制目的または登録目的のために使用された装置の記録を維持する必要があるかもしれない。しかし、収集サイトは適切な電子監査証跡を維持しないかもしれない。

このオプションがアプリケーションレベル機密性プロファイルに追加されて指定される場合、属性中の装置の識別に関する情報が保持されなければならない。表 E.1-1 に述べるとおりである。

E.3.9 保持 UID オプション

個人は一意的な確認自体をもたないが、DICOM モデル中のスタディ、シリーズ、インスタンスおよび他のエンティティは、全体的に一意的な UID を割当てられる。一方で、これらの UID は個人に文脈から直接写像できないが、オリジナル画像、または UID を含むオリジナル画像のデータベースへのアクセスを与えられると、個人の身元を回復することは可能である。

しかしながら、オリジナル画像への監査証跡を維持する能力を要求するアプリケーションがある。また、他のメカニズムがあるけれども、それらはよくスケールせず確実に実装されないかもしれない。このオプションは次の判断の場合に提供される。つまり UID 経由でオリジナルの情報へのアクセスを獲得するリスクが、それらを保持する有益性に比べて小さいことである。

このオプションがアプリケーションレベル機密性プロファイルに追加されて指定される場合、UID が保持されなければならない。表 E.1-1 に述べるとおりである。

注

1. DICOM エンティティの UID は、プライバシー規制によって禁止される一意的な ID と同じではない。
2. UID は「ルート」の階層的スキームを使用して、生成される。それは知識の豊富な人によってルートのオリジナルの譲受人に追跡できる。その生成は典型的に装置メーカーであるが、時々装置を使用する組織である。
3. UID と、オリジナル画像か PACS データベースとをマッチさせるリスクを評価する場合、たとえ UID が変更されても、ピクセルデータ自体は同様のリスクを示すと思うべきである。具体的には、匿名化(De-identifier)された画像のピクセルデータは、オリジナル画像のピクセルデータとマッチさせることができる。そのようなマッチングは、ピクセルデータのあらかじめ計算されたハッシュ値を比較することによって非常に加速できる。焼き付け識別を削除すれば、ピクセルデータを変更できるかもしれない。しかし、ピクセルデータのサブ部位に対してマッチさせることは、ほとんど確かに可能である(例えば、画像の中央部)。画像への雑音の追加でさえ再識別を防ぐには十分ではない。なぜなら統計マッチング技術を使用できるからである。結局、何れかの使用可能なピクセルデータが匿名化(De-identifier)の間に保持される場合、オリジナル画像にアクセスすることにより、再識別はほとんど常に可能である。Ergo (UID の置換)は、UID が保持される場合より、画像がより徹底的に匿名化(De-identifier)されたと誤信すべきでない。
4. このオプションにかかわらず、実装者は、構造的で規格によって定義され、インスタンス関連のものに対立するものとしての UID を削除しないように注意することが望ましい。例えば、匿名化(De-identifier)目的のために SOP クラス UID を削除または置換しない。
5. 実装クラス UID(0002,0012)は保持される UID 属性のリスト中に含まれていない。なぜならそれはファイルメタ情報(PS3.10 を参照)の一部であり、それはファイルが匿名化(De-identifier)の間に保存または修正されるとき常に、完全に置換されるからである。セクション E.1.1 を参照。

E.3.10 保持安全個人オプション

定義によって、プライベート属性は機密情報を含むが、多くの場合その性質がベンダーにのみ知られていて、公には文書化されない。

しかしながら、いくつかのプライベート属性は、希望されるアプリケーションに必要なかもしれない。例えば、特定の技術情報、例えば、CT のヘリカルスパンピッチ若しくはピクセル値変換、または PET SUV のリスケール係数は、プライベート属性にのみ利用可能かもしれない。なぜならそのような情報は規格属性に定義されていないか、または収集装置が製造された後に DICOM 規格に追加されたからである。

このオプションがアプリケーションレベル機密性プロファイルに追加されて指定される場合、識別漏洩から安全であると匿名化(De-identifier)によって知られているプライベート属性は、保持されなければならない。一緒に、保持されたプライベート属性を完全に定義するよう要求されるプライベート作成者 ID も、保持されなければならない; 他のすべてのプライベート属性は削除されるか、プライベートデータ要素特性シーケンス(0008,0300)内に存在する場合は非特定化アクション(0008,0307)が推奨する要素特有の方法で保持されなければならない(PS3.3 セクション C.12.1 を参照)。

属性が安全であると知られているか否かは以下によって判断してよい:

- ブロック特定情報ステータス(0008,0303)において、「SAFE」値とともにプライベートデータ要素のブロックに存在、または非特定プライベート要素(gggg,0004)に個々にリストアップされている（プライベートデータ要素特性シーケンス(0008,0300)内; PS3.3 セクション C.12.1 を参照)
- 表 E.3.10-1 安全なプライベート特性に存在
- 適合性宣言書にて文書化
- その他の手段。

このオプションが指定されない場合、プライベート属性はすべて削除されなければならない。表 E.1-1 に述べるとおりである。

注

1. 安全であると思われたプライベート属性のサンプルリストを以下に示す。ベンダーは、これらが安全であると保証しない。またこれらを特別のソフトウェアバージョン（将来の製品も含んで）の中で送る約束はしない。

表 E.3.10-1. 安全なプライベート属性

データ要素	プライベート作成者	VR	VM	意味
(7053,xx00)	Philips PET Private Group	DS	1	SUV 係数－ 保存されたピクセル値にリスケール傾斜を乗じる。この係数が SUVbw になる。単位は g/l である
(7053,xx09)	Philips PET Private Group	DS	1	放射能濃度係数－ 保存されたピクセル値にリスケール傾斜を乗じる。この係数が MBq/ml になる。
(00E1,xx21)	ELSCINT1	DS	1	DLP
(01E1,xx26)	ELSCINT1	CS	1	ファントムタイプ
(01E1,xx50)	ELSCINT1	DS	1	収集時間
(01F1,xx01)	ELSCINT1	CS	1	収集タイプ
(01F1,xx07)	ELSCINT1	DS	1	テーブル速度
(01F1,xx26)	ELSCINT1	DS	1	ピッチ
(01F1,xx27)	ELSCINT1	DS	1	回転時間
(0019,xx23)	GEMS_ACQU_01	DS	1	テーブル速度[mm/回転]
(0019,xx24)	GEMS_ACQU_01	DS	1	中央スキャンタイム[秒]
(0019,xx27)	GEMS_ACQU_01	DS	1	回転速度（ガントリー周期）
(0019,xx9E)	GEMS_ACQU_01	LO	1	内部パルスシーケンス名
(0043,xx27)	GEMS_PARM_01	SH	1	「n.nnn:1」形式のスキャンピッチ比
(0045,xx01)	GEMS_HELIOS_01	SS	1	検出器中のマクロ列の数
(0045,xx02)	GEMS_HELIOS_01	FL	1	ISO センターのマクロの幅
(0903,xx10)	GEIIS PACS	US	1	拒絶画像フラグ
(0903,xx11)	GEIIS PACS	US	1	重要なフラグ
(0903,xx12)	GEIIS PACS	US	1	機密フラグ
(2001,xx03)	Philips Imaging DD 001	FL	1	拡散 B 係数
(2001,xx04)	Philips Imaging DD 001	CS	1	拡散方向
(0019,xx0C)	SIEMENS MR HEADER	IS	1	B 値
(0019,xx0D)	SIEMENS MR HEADER	CS	1	拡散指向性

データ要素	プライベート作成者	VR	VM	意味
(0019,xx0E)	SIEMENS MR HEADER	FD	3	拡散勾配方向
(0019,xx27)	SIEMENS MR HEADER	FD	6	B マトリックス
(0043,xx39)	GEMS_PARM_01	IS	4	B 値の ^{※1} の値
(0043,xx6F)	GEMS_PARM_01	DS	3-4	スキャナーテーブルエントリ + 選択された傾斜磁場コイル
(0025,xx07)	GEMS_SERS_01	SL	1	連続した画像
(7E01,xx01)	HOLOGIC, Inc.	LO	1	コーデックのバージョン
(7E01,xx02)	HOLOGIC, Inc.	SH	1	コーデックの内容タイプ
(7E01,xx10)	HOLOGIC, Inc.	SQ	1	高解像度のデータシーケンス
(7E01,xx11)	HOLOGIC, Inc.	SQ	1	低解像度のデータシーケンス
(7E01,xx12)	HOLOGIC, Inc.	OB	1	コーデックの内容
(0099,xx01)	NQHeader	UI	1	バージョン
(0099,xx02)	NQHeader	UI	1	分析したシリーズ UID
(0099,xx04)	NQHeader	SS	1	リターンコード
(0099,xx05)	NQHeader	LT	1	リターンメッセージ
(0099,xx10)	NQHeader	FL	1	MI
(0099,xx20)	NQHeader	SH	1	ユニット
(0099,xx21)	NQHeader	FL	1	ICV
(0199,xx01)	NQLeft	FL	1	左皮質下白質
(0199,xx02)	NQLeft	FL	1	左皮質灰白質
(0199,xx03)	NQLeft	FL	1	左第 3 脳室
(0199,xx04)	NQLeft	FL	1	左第 4 脳室
(0199,xx05)	NQLeft	FL	1	左第 5 脳室
(0199,xx06)	NQLeft	FL	1	左側脳室
(0199,xx07)	NQLeft	FL	1	左下側脳室
(0199,xx08)	NQLeft	FL	1	左下 CSF
(0199,xx09)	NQLeft	FL	1	左小脳白質
(0199,xx0a)	NQLeft	FL	1	左小脳灰白質
(0199,xx0b)	NQLeft	FL	1	左海馬
(0199,xx0c)	NQLeft	FL	1	左扁桃核
(0199,xx0d)	NQLeft	FL	1	左視床
(0199,xx0e)	NQLeft	FL	1	左尾状
(0199,xx0f)	NQLeft	FL	1	左被殻
(0199,xx10)	NQLeft	FL	1	左淡蒼球
(0199,xx11)	NQLeft	FL	1	左腹側間脳
(0199,xx12)	NQLeft	FL	1	左側坐核
(0199,xx13)	NQLeft	FL	1	左脳幹
(0199,xx14)	NQLeft	FL	1	左外側 CSF
(0199,xx15)	NQLeft	FL	1	左 WM 下
(0199,xx16)	NQLeft	FL	1	左その他
(0299,xx01)	NQRight	FL	1	右皮質下白質
(0299,xx02)	NQRight	FL	1	右皮質灰白質

データ要素	プライベート作成者	VR	VM	意味
(0299,xx03)	NQRright	FL	1	右第3脳室
(0299,xx04)	NQRright	FL	1	右第4脳室
(0299,xx05)	NQRright	FL	1	右第5脳室
(0299,xx06)	NQRright	FL	1	右側脳室
(0299,xx07)	NQRright	FL	1	右下側脳室
(0299,xx08)	NQRright	FL	1	右下CSF
(0299,xx09)	NQRright	FL	1	右小脳白質
(0299,xx0a)	NQRright	FL	1	右小脳灰白質
(0299,xx0b)	NQRright	FL	1	右海馬
(0299,xx0c)	NQRright	FL	1	右扁桃体
(0299,xx0d)	NQRright	FL	1	右視床
(0299,xx0e)	NQRright	FL	1	右尾状
(0299,xx0f)	NQRright	FL	1	右被殻
(0299,xx10)	NQRright	FL	1	右淡蒼球
(0299,xx11)	NQRright	FL	1	右腹側間脳
(0299,xx12)	NQRright	FL	1	右側坐核
(0299,xx13)	NQRright	FL	1	右脳幹
(0299,xx14)	NQRright	FL	1	右外側CSF
(0299,xx15)	NQRright	FL	1	右WM下
(0299,xx16)	NQRright	FL	1	右その他
(2005,xx0D)	Philips MR Imaging DD 001	FL	1	スケールインターセプト
(2005,xx0E)	Philips MR Imaging DD 001	FL	1	スケールスロープ
(0119,xx00)	SIEMENS Ultrasound SC2000	LO	1	音響メタ情報バージョン
(0119,xx01)	SIEMENS Ultrasound SC2000	OB	1	共通の音響メタ情報
(0119,xx02)	SIEMENS Ultrasound SC2000	SQ	1	マルチストリームシーケンス
(0119,xx03)	SIEMENS Ultrasound SC2000	SQ	1	音響データシーケンス
(0119,xx04)	SIEMENS Ultrasound SC2000	OB	1	トランザクションごとの音響管理情報
(0119,xx05)	SIEMENS Ultrasound SC2000	UL	1	音響データオフセット
(0119,xx06)	SIEMENS Ultrasound SC2000	UL	1	音響データ長
(0119,xx07)	SIEMENS Ultrasound SC2000	UL	1	フッターオフセット
(0119,xx08)	SIEMENS Ultrasound SC2000	UL	1	フッター長
(0119,xx09)	SIEMENS Ultrasound SC2000	SS	1	音響ストリーム番号
(0119,xx10)	SIEMENS Ultrasound SC2000	SH	1	音響ストリームタイプ
(0119,xx11)	SIEMENS Ultrasound SC2000		1	ステージタイマー時間
(0119,xx12)	SIEMENS Ultrasound SC2000		1	ストップウォッチ時間
(0119,xx13)	SIEMENS Ultrasound SC2000	IS	1	量率
(0119,xx21)	SIEMENS Ultrasound SC2000	SH	1	
(0129,xx00)	SIEMENS Ultrasound SC2000	SQ	1	MPR ビューシーケンス
(0129,xx02)	SIEMENS Ultrasound SC2000	UI	1	ブックマーク UID

データ要素	プライベート作成者	VR	VM	意味
(0129,xx03)	SIEMENS Ultrasound SC2000		1	平面の原点ベクトル
(0129,xx04)	SIEMENS Ultrasound SC2000		1	行ベクトル
(0129,xx05)	SIEMENS Ultrasound SC2000		1	列ベクトル
(0129,xx06)	SIEMENS Ultrasound SC2000	SQ	1	可視化シーケンス
(0129,xx07)	SIEMENS Ultrasound SC2000	UI	1	ブックマーク UID
(0129,xx08)	SIEMENS Ultrasound SC2000	OB	1	可視化情報
(0129,xx09)	SIEMENS Ultrasound SC2000	SQ	1	アプリケーション状態シーケンス
(0129,xx10)	SIEMENS Ultrasound SC2000	OB	1	アプリケーション状態情報
(0129,xx11)	SIEMENS Ultrasound SC2000	SQ	1	参照されたブックマークシーケンス
(0129,xx12)	SIEMENS Ultrasound SC2000	UI	1	参照されたブックマーク UID
(0129,xx20)	SIEMENS Ultrasound SC2000	SQ	1	シネパラメータのシーケンス
(0129,xx21)	SIEMENS Ultrasound SC2000	OB	1	シネパラメータのスキーマ
(0129,xx22)	SIEMENS Ultrasound SC2000	OB	1	シネパラメータ値
(0129,xx29)	SIEMENS Ultrasound SC2000	OB	1	
(0129,xx30)	SIEMENS Ultrasound SC2000	CS	1	生データオブジェクトタイプ
(0139,xx01)	SIEMENS Ultrasound SC2000	SL	1	フィジオキャプチャROI
(0149,xx01)	SIEMENS Ultrasound SC2000	FD	1-n	BROI ポイントのベクトル
(0149,xx02)	SIEMENS Ultrasound SC2000	FD	1-n	ストリップストリームの開始/終了タイムスタンプ
(0149,xx03)	SIEMENS Ultrasound SC2000	FD	1-n	可視 R 波のタイムスタンプ
(7FD1,xx01)	SIEMENS Ultrasound SC2000	OB	1	音響画像およびフッターデータ
(7FD1,xx09)	SIEMENS Ultrasound SC2000	UI	1	量バージョン ID
(7FD1,xx10)	SIEMENS Ultrasound SC2000	OB	1	量のペイロード
(7FD1,xx11)	SIEMENS Ultrasound SC2000	OB	1	ペイロード後
(7FD1,xx01)	SIEMENS SYNGO ULTRA-SOUND TOYON DATA STREAMING	OB	1	パディング
(7FD1,xx09)	SIEMENS SYNGO ULTRA-SOUND TOYON DATA STREAMING	UI	1	バージョン ID
(7FD1,xx10)	SIEMENS SYNGO ULTRA-SOUND TOYON DATA STREAMING	OB	1	量のペイロード
(7FD1,xx11)	SIEMENS SYNGO ULTRA-SOUND TOYON DATA STREAMING	OB	1	ペイロード後

2. プライベート属性を安全に保持する 1 つのアプローチは、VR が明示的に符号化されるか、データ辞書から既知である場合（例えば、公表された DICOM 適合性宣言書または以前に遭遇したインスタンスから由来し、新しい明示的な VR インスタンスが受け取られたとき恐らく適応してデータ辞書を拡張することにより）、数値の特性だけを含む属性を保持することである。例えば、保持するのは US, SS, UL, SS, FL および FD 二成分値並びに IS および DS 文字列値であって有効な数値の特性だけを含むものである。仮定できることは、他の文字列値表現は、ベンダーから安全であるとの明確な確認がない状態では不安全である；符号列（CS）は例外かもしれない。OB 値表現でのバルクの二成分のデータは特に不安全であり、機密フォーマットヘッダー全体を 2 進法またはテキスト若しくは XML 形式でしばしば含み、それは患者の名前および他の識別情報を含む。

保持される安全なプライベート属性は適合性宣言書に述べられなければならない。

F ネットワークアドレス管理プロファイル

F.1 基本ネットワークアドレス管理プロファイル

基本ネットワークアドレス管理プロファイルは、DHCP を利用し IP パラメータを機械のために遠隔に割当てて管理するサービスを提供する。DHCP サーバは機械に IP アドレスを割当てる規則を確立するように手動で構成される。規則は機械割当てによる明示的な機械かもしれないし、IP アドレスのブロックの割当てかもしれない。そのブロックは機械がネットワークに着脱される時ダイナミックに割当てられる。DHCP クライアントはその IP アドレスを得ることができ、様々な関連するパラメータ、例えば、NTP サーバアドレスを DHCP サーバから操業開始の間を得る。DHCP サーバは、ダイナミックに DNS サーバを IP アドレスと DNS ホスト名と間の新しい関係を用いて更新する。

DNS クライアントは、DNS ホスト名を DNS サーバに与えることによりもう一つのホストのために IP 番号を得て、IP 番号をレスポンスで受け取ることができる。このトランザクションは、他のプロファイルの中で、または基本ネットワークアドレス管理プロファイルに適合しない実装の中で使用されてもよい。

基本ネットワークアドレス管理プロファイルが当てはまるのは、アクタ DHCP サーバ、DHCP クライアント、DNS サーバおよび DNS クライアントである。必須およびオプションのトランザクションは、以下の表とセクションの中で述べる。

表 F.1-1. 基本ネットワークアドレス管理プロファイル

アクタ	トランザクション	オプション性	セクション
DHCP サーバ	DHCP サーバを構成する	M	F.1.2
	DHCP サーバを見つけて使用する	M	F.1.3
	リースを維持する	M	F.1.4
	ホスト名を解決する	M	F.1.1
	DDNS 協調	O	F.1.5
DHCP クライアント	DHCP サーバを見つけて使用する	M	F.1.3
	リースを維持する	M	F.1.4
DNS サーバ	DDNS 協調	O	F.1.5
	ホスト名を解決する	M	F.1.1
DNS クライアント	ホスト名を解決する	M	F.1.1

F.1.1 ホスト名を解決する

F.1.1.1 適用範囲

DNS クライアントは、DNS ホスト名を DNS サーバに与えて、IP 番号をレスポンスで受け取ることによってホストのために IP 番号を得ることができる。

F.1.1.2 ユースケース／役割

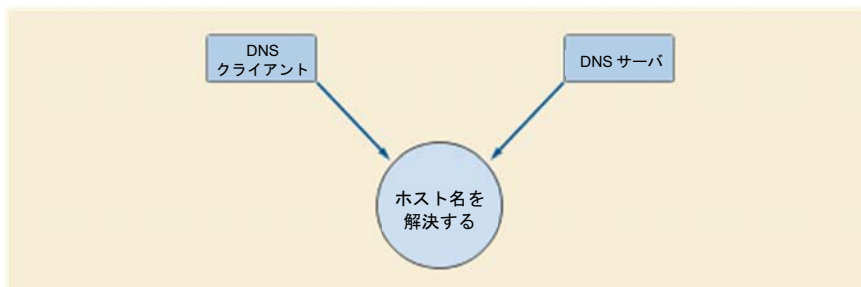


図 F.1-1. ホスト名を解決する

アクタ： DNS クライアント

役割： IP アドレスを必要とし、DNS ホスト名もっている。

アクタ： DNS サーバ

役割： DNS ホスト名を与えられた時、現在の IP アドレスを提供する。

F.1.1.3 参照される標準

DNS プロトコルのファミリーのための標準およびそれらの関係を、図 F.1-2 に示す。トランザクション、トランザクション図形などの詳細は、参照される RFC の内に含まれている。

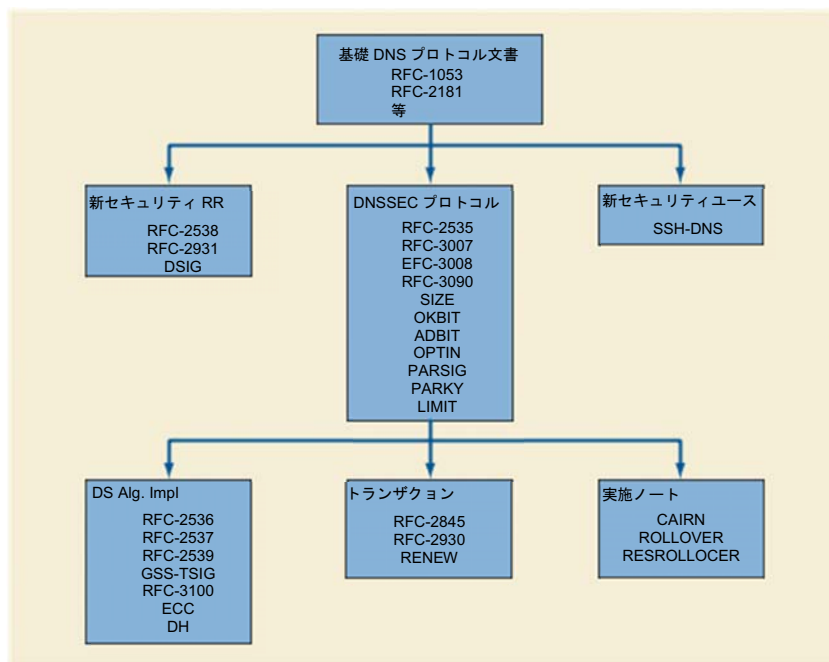


図 F.1-2. DNS 参照標準

F.1.1.4 DNS セキュリティ考察 (参考)

セキュリティの問題は、インターネットエンジニアリング特別対策本部(IETF: Internet Engineering Task Force)およびその様々なワーキンググループにより積極的に開発されつつある。そのセキュリティ関連 RFC および草案は図 F.1-2 に特定される。これらのうちのいくつかは完成している。他のものはまだ草案の段階にある。基本ネットワークアドレス管理プロファイルは、DNS クライアントによる DNS セキュリティ拡張の支援用の特定要求事項を含んでいない。

基本ネットワークアドレス管理プロファイルは、セキュリティ環境の外部で使用されるべきでない。最小限、次のものが存在することが望ましい：

- a. 承認された外部ホストだけが DNS サービスに使用されることを保証するためのファイアウォールまたはルーター保護。
- b. VPN および他のアクセスのための協定は、DNS クライアントが、承認された DNS サーバだけを VPN の上で使用することを要求することが望ましい。

他のネットワークセキュリティ手続き、例えば、自動侵入検知は、いくつかの環境において適切かもしれない。この最小限以上のセキュリティ特長は、ローカルのセキュリティ方針によって確立されることが望ましく、それらは DICOM の範囲外である。

選択されたセキュリティの目的は、インサイダー攻撃に対する脅威の範囲を制限することである。DNS システムはホスト名および IP アドレスだけを開示する。したがって、盗聴に対する懸念はほとんどない。その保護は、偽のサーバまたはクライアントによる DoS 攻撃に曝されるのを制限することである。

F.1.1.5 DNS 実装考察（参考）

クライアントキャッシュは更新中に混乱を引起すかもしれない。多くの DNS クライアントは、DNS 更新をチェックすることは非常に稀であり、DNS 変更を何時間も何日間も反映しないかもしれない。手動のステップは即時の更新を引き起こすために必要かもしれない。キャッシュと更新との管理のための詳細は、DNS クライアントおよび DNS サーバが異なると、変わる。しかし、DNS キャッシュと更新伝達遅延は著しい要因である。また、実装はこれらの問題を管理するメカニズムをもっている。

DNS サーバ失敗管理が考慮されることが望ましい。重複サーバおよび予備ホストファイルは、可能なエラー管理手段の例である。

F.1.1.6 サービス発見の支援

DNS サーバは、構成管理を支援する補足オプション情報を提供してもよい。この情報の仕様および支援される追加の RFC についてはセクション H.2 を参照すること。

F.1.2 DHCP サーバを構成する

F.1.2.1 適用範囲

DHCP サーバはサイト管理によって次のように設定可能でなければならない。

- DHCP クライアントは追加および削除することができる。
- DHCP クライアント構成は、修正され後日のトランザクションの中で使用される属性のため値を設定できる。
- DHCP クライアント用の固定の IP アドレスの事前配分が支援される。

この標準は、この配置がどのようにして行われることになっているか明示していない。

注

ほとんどの DHCP サーバは、従来システムのための推移プロセスを単純化するために、固定の IP アドレスの事前配分を支援する。一方でこれにより特定装置を DHCP に切り替えることができ、他方で以前に割当てられた IP アドレスを保持できる。これにより IP アドレスの中央サイト管理を使用でき、同時に、固定の IP アドレスを要求する従来システムとの互換性を壊すことがない。

F.1.2.2 ユースケース／役割

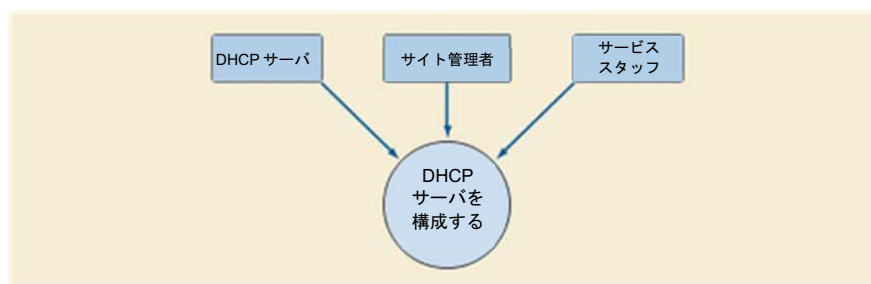


図 F.1-3. DHCP サーバを構成する

アクタ： DHCP サーバ

役割： 内部設定ファイルを維持する。

アクタ： サイト管理者

役割： 配置情報を更新し、クライアントとサーバのデスクリプションを追加、修正、削除する。

アクタ： サービススタッフ

役割： 新しいネットワークをインストールする場合は多くの装置のために、単一の装置をインストールまたは修正する場合は個々の装置のために、最初の配置要求事項を提供する。

F.1.2.3 参照される標準

無し

F.1.3 DHCP サーバを見つけて使用する

F.1.3.1 適用範囲

これは正常な操業開始プロセスの支援である。DHCP クライアントシステムは起動し、そして起動プロセスの非常に初期に、それは DHCP サーバを見つけ、DHCP サーバのうちの 1 つをそのサーバとして選び、各種情報を得るためにそのサーバに問い合わせ、その問い合わせの結果を使用して DHCP クライアント自己配置を継続する。DHCP サーバは、オプションとして各種情報、例えば、サーバ位置、正常なルートを提供してもよい。このトランザクションは、どんな情報かが適合 DHCP サーバにより提供されなければならないか、およびどんな情報が適合 DHCP クライアントにより要求されなければならないかを特定する。適合 DHCP サーバは、このオプション情報を提供することを要求されない。

F.1.3.2 ユースケース／役割

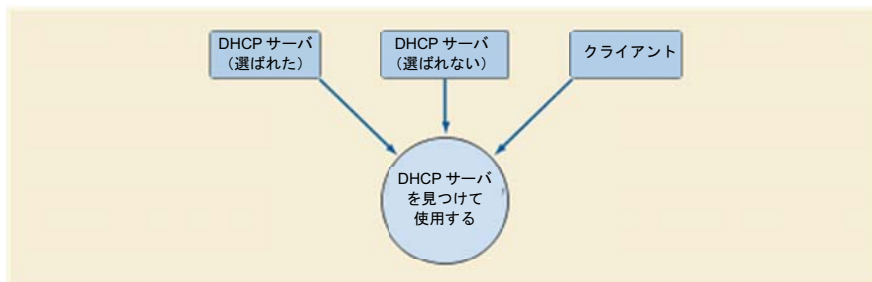


図 F.1-4. DHCP サーバを見つけて使用する

アクタ： DHCP サーバ

役割： DHCP 収集問い合わせに回答する。多数のアクタが存在するかもしれない。DHCP クライアントは 1 つを選択する。

アクタ： DHCP クライアント

役割： DHCP サーバのための問い合わせ。1 つの回答するサーバを選ぶ。

F.1.3.3 参照される標準

RFC2131 DHCP プロトコル

RFC2132 DHCP オプション

RFC2563 自動構成管理

F.1.3.4 相互作用図

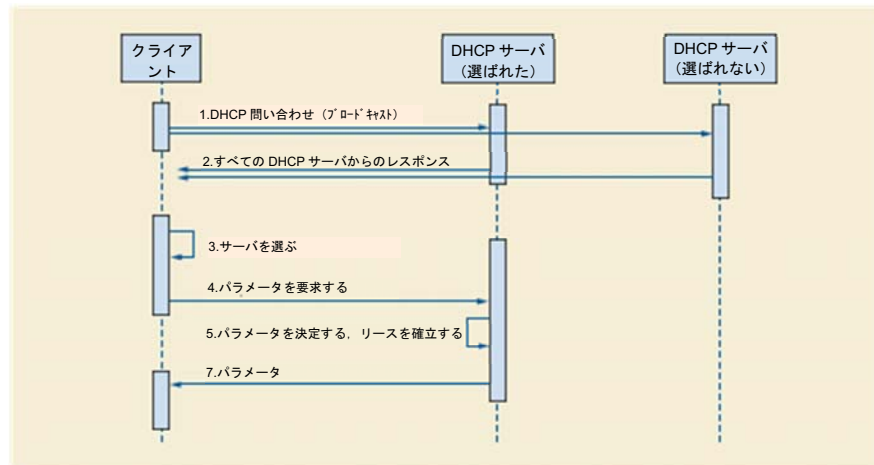


図 F.1-5. DHCP 相互作用

DHCP クライアントは、RFC2131 (DHCP プロトコル)、RFC2132 (DHCP オプション)、RFC2563 (自動構成管理) およびそれらの参照される RFC に適合しなければならない。

DHCP クライアントは利用可能な DHCP サーバを問い合わせなければならない。それは、使用するべき DHCP サーバを選ばなければならない。

DHCP クライアントは IP 割当てを問い合わせなければならない。DHCP サーバは現在の DHCP 構成に従って IP パラメータを決定し、これらのパラメータに対するリース契約を確立し、この情報で答えなければならない。(リースメンテナンスおよび終了については下記を参照。) DHCP クライアントは、これらのパラメータを TCP/IP スタックに適用しなければならない。DHCP クライアントは内部リースメンテナンス活動を確立しなければならない。

DHCP クライアントは、クライアントシステムによって使用される追加のプロファイルによって要求された時、表 F.1-2 で列記されたオプション情報を問い合わせなければならない。DHCP サーバがこの情報を提供しなければ、初期設定値が DHCP クライアントによって使用されなければならない。

表 F.1-2. DHCP パラメータ

DHCP オプション	概要	初期設定
NTP	List of NTP servers	Empty list
DNS	List of DNS servers	Empty list
Router	Default router	Empty list
Static routes		Nil
Hostname		Requested machine name
Domain name		Nil
Subnet mask		Derived from network value
Broadcast address		Derived from network value
Default router		Nil
Time offset		Site configurable
MTU		Hardware dependent
Auto-IP permission		From NVRAM

DHCP クライアントは、この情報を DHCP クライアントマシン内の他のアクタに利用可能にしなければならない。

F.1.4 リースを維持する

F.1.4.1 適用範囲

DHCP クライアントは、通常 RFC に従って IP リースを維持する。時々、サーバはリースを更新しない。非書換えは通常ネットワークサービスオペレーションの一部である。IP リースの損失は、停止する IP アドレスを使用して、接続を要求する。

F.1.4.2 ユースケース／役割

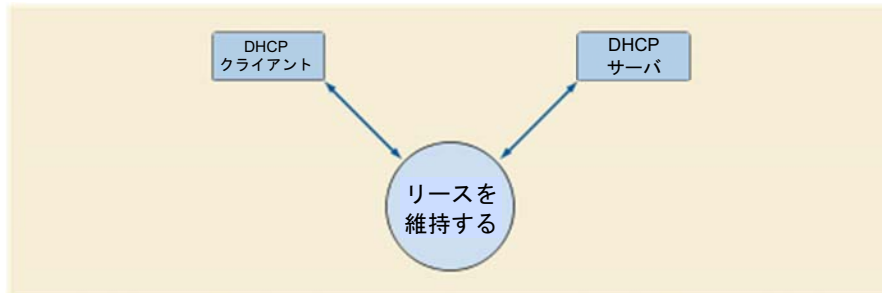


図 F.1-6. リースを維持する

アクタ： DHCP クライアント

役割： リース書換えおよび終了を備えた取引。

アクタ： DHCP サーバ

役割： 更新するかリースを意図的に終了させること（時々ネットワークサービスオペレーションの一部として行われた）。

F.1.4.3 参照される標準

RFC2131 DHCP プロトコル

RFC2132 DHCP オプション

F.1.4.4 正常な相互作用

DHCP クライアントは、RFC2131 および RFC2132 の中で指定するとおり、リースを IP アドレス上で DHCP プロトコルに従って維持しなければならない。DHCP サーバは失敗するかもしれないか、またはリースを更新しないことを選ぶかもしれない可能性がある。

更新されずに、DHCP リースが終了する場合、まだ活発な DICOM 接続も異常終了するかもしれない（AP 異常終了）。

注

通常、リースの延期要求と実際のリースの終了との間（典型的には数分および数日の間）には期間がある。そのアプリケーションは、これを利用し、AP 中断の急なシャットダウンではなく緩慢なアソシエーションリリースを行うかもしれない。

F.1.5 DDNS 協調

F.1.5.1 適用範囲

DHCP サーバは、IP とホスト名の割当てを DNS サーバと調整してもよい。これにより IP アドレスの動的な割当てが可能となり、DHCP クライアントへのアクセスが他のシステムにより干渉されることがない。他のシステムは、同意されたホスト名（それを DHCP は管理しクライアントに提供することができる）を利用し、DNS ルックアップにより現在の IP アドレスを得る。

DHCP サーバは、適切なホスト名/IP 関係を DNS データベースの中で維持するために関連 DNS サーバを維持し更新する場合、基本ネットワークアドレス管理プロファイルのこのオプション部に適合する。

F.1.5.2 ユースケース／役割

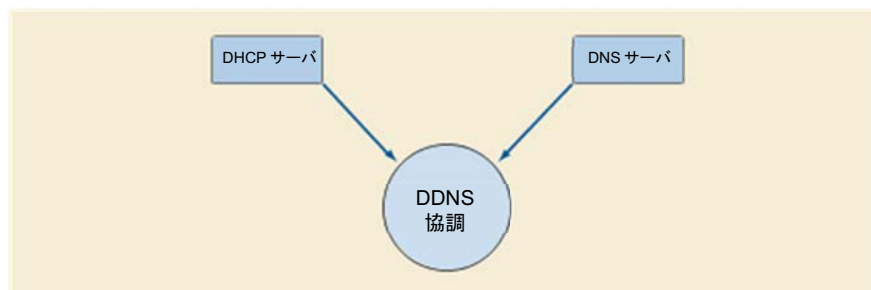


図 F.1-7. DDNS 協調

アクタ： DHCP サーバ

役割： DHCP 収集問い合わせに応答し、IP アドレスをクライアントに割当てた。

アクタ： DNS サーバ

役割： ネットワークのための DNS サービスを維持する。

F.1.5.3 参照される標準

RFC2136 ドメイン・ネーム・システム中の動的な最新版

F.1.5.4 イベントの基礎コース

DHCP サーバが IP アドレスを DHCP クライアントに割当てた後、DHCP サーバは DDNS を使用して、DNS サーバに、ホスト名が DHCP クライアントに割当てられ、それが割当てられた IP アドレスを与えられたことを通知する。DNS サーバは DNS データベースを更新する。このホスト名のための事後の DNS 問い合わせが、割当てられた IP アドレスを与えられるようにするためである。IP アドレスに対するリースが更新なしで終了する場合、DHCP サーバは、IP アドレスとホスト名がもはや有効ではないことを DNS サーバに通知する。DNS サーバは DNS データベースからそれらを削除する。

F.1.6 DHCP セキュリティ考察（参考）

基本ネットワークアドレス管理プロファイルには、2つの分野のセキュリティ上の問題がある：

- DHCP クライアント／サーバ取引に対する DoS 攻撃からの保護。
- DHCP サーバから DDNS サーバへの更新プロセスに対する DoS 攻撃からの保護。

基本ネットワークアドレス管理プロファイルはセキュリティ環境外で使用されるべきでない。最小限、次のものが存在することが望ましい：

- 承認されたホストだけが DHCP と DNS のサービスに使用されることを保証するファイアウォールまたはルーター保護。
- VPN および他のアクセスのための協定は、病院ネットワークの DNS クライアントは、VPN 上の承認された DHCP または DNS のサーバだけを使用することを要求するべきである。

他のネットワークセキュリティ手続き、例えば、自動侵入検知は、いくつかの環境において適切かもしれない。この最小限以上のセキュリティ特長は、ローカルのセキュリティ方針によって確立されることが望ましく、それらは DICOM の範囲外である。

選択されたセキュリティの目的は、インサイダー攻撃に対する脅威の範囲を制限することである。DHCP と DNS のシステムはホスト名および IP アドレスだけを開示する。したがって、盗聴に対する懸念はほとんどない。その保護は、偽のサーバまたはクライアントによる DoS 攻撃に曝されるのを制限することである。特定の DNS セキュリティ拡張はセクション F.1.1.4 に述べられている。このプロファイルは DHCP セキュリティ延期を利用しない。なぜならそれらが提供する追加セキュリティは非常に限定され、かつ攻撃がインサイダーの DoS 攻撃であるからである。侵入検知および他のネットワークレベル保護メカニズムは、DHCP プロセスのための最も有効な次のレベル保護である。

DNS 最新版はこのプロファイルにおいてオプションであり、DHCP サーバおよび DNS サーバは、相互に受理可能なセキュリティプロセスに達することはできないという可能性を提供するものである。このオプションの支援は、開発中の DNS セキュリティプロトコルの支援を要求するかもしれない。DNS セキュリティプロファイル標準および草案の議論については、セクション F.1.1.4 を参照すること。

F.1.7 DHCP 実装考察（参考）

DHCP 構成ファイルは、企業内情報通信網ハードウェア構成の文書化の非常に有用な形式になり得る。それは、新しい設置のために前もって準備することができ、クライアントが追加されるとともに更新することができる。すべての機械（DHCP を利用しない機械も含む）の情報を含むことにより、偶発的な IP アドレスの矛盾および同様のエラーを回避する。

ほとんどの DHCP サーバは構成能力をもっているため、クライアントに提供される IP アドレスおよび他の情報を管理できる。これらの管理は、要求された機械名または MAC アドレスに基づいて、特定の IP アドレスなどを機械に予め割付けることができる。その結果、これらの予め割付けられた IP アドレスは、これらの特定の機械が同じ IP アドレスを常に割当てられることを保証する。DNS を利用しない従来システムは、DHCP サーバがそれらのサービスに IP アドレスを予め割付けた場合、IP アドレスを備えた固定テーブルを使用し続けることができる。

F.1.8 適合

LDAP クライアントのための適合性宣言書は、ローカルの AE タイトルを構成するために LDAP を使用することを記述しなければならない。最新版 LDAP サーバオプションへの適合は、LDAP サーバに送信された最新版中のすべての構成要素オブジェクト属性に対する値と一緒に、指定されなければならない。LDAP を使用して遠隔の装置アドレスおよび能力を構成することも記述されなければならない。LDAP 問い合わせを使用して遠隔の装置コンポーネントオブジェクト属性を得た場合、問い合わせが指定されなければならない。

注

特に、特定のシステムアクタ（例えば、イメージアーカイブ、または行われたプロセスステップマネージャ）のために AE タイトル、TCP ポートおよび IP アドレスを得る LDAP の使用、さらに、遠隔装置のための LDAP 情報はどのように運用上の使用に選ばれるかについては、詳述されることが望ましい。

G 時間同期プロファイル

G.1 基本時間同期プロファイル

基本時間同期プロファイルは、多数のコンピュータ上の時計を同期させるサービスを定義する。このプロファイルは、他の多くの分野でこの目的に使用されたネットワーク時間プロトコル (NTP) サービスを使用する。NTPにより、ローカル時間ソースを提供するローカルサーバへの同期および様々な外部時間サービスへの同期が可能である。正確さと精密さの管理は明示的にはプロトコルの一部ではない。それらは、時計ハードウェアおよびネットワーク位相の選択によって大部分決定される。

NTPのための実装戦略の広範囲な議論は <http://www.ntp.org> で得ることができる。

基本時間同期プロファイルは、次のアクタに当てはまる。つまり DHCP クライアント、DHCP サーバ、SNTP クライアント、NTP クライアントおよび NTP サーバである。必須およびオプションのトランザクションは、以下の表とセクションの中で述べる。

表 G.1-1. 基本時間同期プロファイル

アクタ	トランザクション	オプション性	セクション
NTP サーバ	時間を維持する	M	G.1.2
	NTP サーバを見つける	O	G.1.1
NTP クライアント	時間を維持する	M	G.1.2
	NTP サーバを見つける	O	G.1.1
SNTP クライアント	時間を維持する	M	G.1.2
DHCP サーバ	NTP サーバを見つける	O	G.1.1
DCHP クライアント	NTP サーバを見つける	M	G.1.1

G.1.1 NTP サーバを見つける

NTP 自動構成用および NTP 自動発見用のオプションの NTP プロトコル要素は、設置を著しく単純化することができる。これらのための NTP 仕様は、それらがクライアントとサーバの両方に本当にオプションであるように定義される。クライアントがこれらのサービスを利用して、NTP サーバを自動的に見つけることができない場合、クライアントは、サーバを見つけるために DHCP オプション情報または手動で構成された情報を使用することができる。これらのサービスの支援は勧められるが必須ではない。

このトランザクションは、設備の特定のモデルが自動発見を支援するか否かを文書化する手段として主に存在する。これにより設置と操作は、DHCP および設備設置手続きを予め計画することができる。

G.1.1.1 適用範囲

これは、正確な時間を必要とするか、またはそのタイムスタンプを別のシステムのタイムスタンプと同期させる必要のあるあらゆるクライアントに適用する。同期の正確さは、特定のサイトでのネットワークと NTP のサーバの構成および実装の詳細によって決定される。

NTP と SNTP の両方のクライアントは、情報が DHCP によって提供され、自動発見を使用しても NTP サービスが見つからない場合、NTP サーバ情報を利用しなければならない。マニュアル構成はバックアップとして提供されなければならない。自動発見または DHCP が好まれる。

G.1.1.2 ユースケース／役割

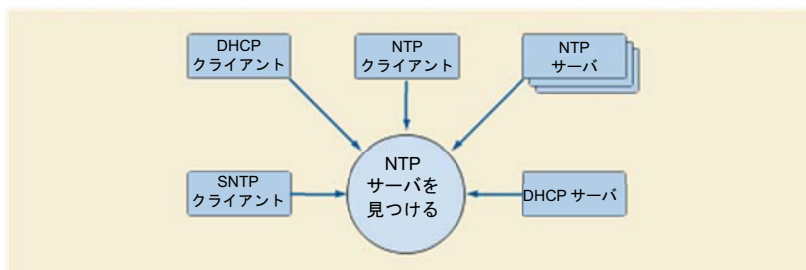


図 G.1-1. NTP サーバを見つける

DHCP サーバ	UTC オフセットを提供し、NTP サーバのリストを提供する。
DHCP クライアント	UTC オフセットおよび NTP サーバのリストを受け取る。
NTP クライアント	クライアント時計を維持する。
SNTP クライアント	クライアント時計を維持する。
NTP サーバ	外部時間サーバである。これらは、他の時間サーバに接続しているかもしれないし、全国時間ソースと同期しているかもしれない。

G.1.1.3 参照される標準

RFC1305 ネットワーク時間プロトコル (NTP) 標準仕様

RFC2030 簡易 NTP

G.1.1.4 イベントの基礎コース

DHCP サーバは、NTP サーバのリストを提供したかもしれない。または、オプションの NTP 発見メカニズムによってそれが得られるかもしれない。このリストが空であり、手動で構成された NTP サーバアドレスが存在しない場合、クライアントはその内部時計を時間ソースとして選択しなければならない（以下を参照）。リストが空でない場合、クライアントはそれらのすべての NTP サーバと時間同期を維持することを試みなければならない。クライアントは、RFC1305 に定義されるマルチキャスト、メニーキャスト、ブロードキャストのオプションを使用することを試みるかもしれない。クライアントは、これらが利用可能でない場合に、2 点間同期オプションを利用しなければならない。同期は RFC1305 (NTP) または RFC2030 (SNTP) のいずれかに適合しなければならない。

アプリケーションが 1 秒平均誤差よりよい時間同期を要求する場合、クライアントは NTP を使用することが望ましい。SNTP は、より正確な時間同期を保証することができない。

DHCP サーバは、機械でのローカル時間と UTC との間の UTC オフセットを提供したかもしれない。これが見当らなければ、UTC オフセットは装置固有の方法（例えば、サービス、CMOS）で得られる。UTC オフセットが提供される場合、クライアントは UTC とローカル時間との間を変換するためにこのオフセットを使用しなければならない。

G.1.1.5 代替パス

もし DHCP サーバからの UTC オフセット情報がなければ、NTP クライアントは、そのプリセットまたはサービスセット UTC オフセットを使用するであろう。

もし NTP 時間サーバが存在しなければ、NTP クライアントはその内蔵電池時計を UTC のソースとして選択する。これらには本質的なエラーがあるかもしれない。また、これは多重システムがあって NTP ソースがない場合、多重システムは互いに同期することを試みないということも意味する。

G.1.1.6 仮定

ローカルのバッテリークロックタイムは UTC に設定されるか、または、ローカルのオペレーティングシステムは、適切な支援を得て、両方のバッテリークロックタイム、NTP クロックタイムおよびシステムクロックタイムを管理する。NTP 時間は常に UTC にある。

G.1.1.7 事後条件

クライアントはその選択された時間ソースと同期し続ける。1 つ以上の NTP サーバをもつ環境では、これはよい時間同期になる。NTP サーバが存在しない場合、選択されたソースは、付随する全エラーにもかかわらず、内部クライアント時計になる。

G.1.2 時間を維持する

G.1.2.1 適用範囲

これは、正確な時間を必要とするか、またはそのタイムスタンプを別のシステムのタイムスタンプと同期させる必要のあるあらゆるクライアントに適用する。同期の正確さは、特定のサイトでのネットワークと NTP のサーバの構成および実装の詳細によって決定される。

G.1.2.2 ユースケース／役割

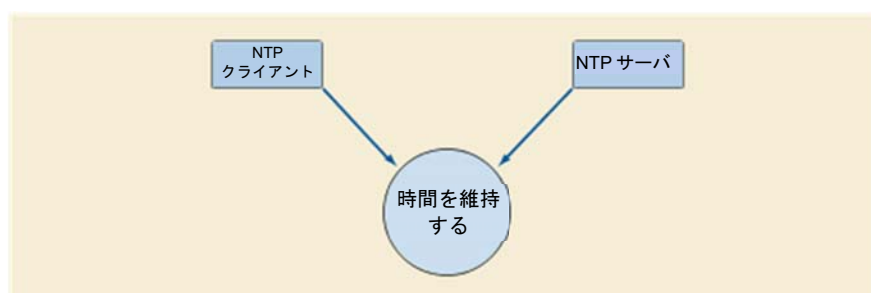


図 G.2-1. 時間を維持する

NTP/SNTP クライアント クライアント時計を維持する。

NTP サーバ 外部時間サーバである。これらは、他の時間サーバに接続しているかもしれないし、全国時間ソースと同期しているかもしれない。

G.1.2.3 参照される標準

RFC1305 ネットワーク時間プロトコル (NTP) 標準仕様

RFC2030 簡易 NTP

G.1.2.4 イベントの基礎コース

すべての完全細目は RFC1305 および RFC2030 にある。NTP オペレーション用の最も一般的で最も必要な最小限のモードが、クライアントとサーバ間のメッセージのピンポンを確立する。クライアントは、リクエストをサーバに送信する。サーバは時間関連フィールドに応答を書き入れる。また、クライアントは、現在の時間の最適な推定を行う。RFC は失われたメッセージ、推定方式などの問題に対処する。一旦時計が同期すれば、これらのピンポン交換は典型的にはおよそ 1000 秒の間隔で安定する。

クライアントマシンは、典型的には時間推定を使用して内部オペレーティングシステムクロックを維持する。その後、このクロックは、時間情報を必要とするアプリケーションによって使用される。このアプローチは、同期時間と非同期時間との間のアプリケーション可視の違いを除去する。RFC は、適切な実装の指針を提供する。

G.1.3 NTP セキュリティ考察 (参考)

基本時間同期プロファイルはセキュリティ環境の外部で使用しない方が望ましい。最小限、次のものが存在することが望ましい：

- ファイアウォール、またはルーター保護であって、承認されたホストだけが NTP サービスに使用されることを保証するもの。
- VPN および他のアクセスのための協定は、承認された NTP サーバだけを VPN の上で使用することを要求することが望ましい。

これにより、リスクがインサイダーの DoS 攻撃に限定される。このサービス拒否攻撃は時間同期の改ざんであり、システムが不正確な時間を報告するように仕向ける。NTP プロトコルは、協定することができる安全なトランザクション能力を組込む。このプロファイルが仮定することは、上記の保護が十分であるとし、安全なトランザクションのサポートを要求しないが、しかし、それらは実装により支援されるかもしれないことである。SNTP クライアントは、安全なトランザクションの使用をサポートしない。

外部ネットワークの時間ソースのセキュリティに関し特別の懸念をもつサイトは、GPS からラジオに基づいた時間同期を利用することを選ぶかもしれない。GPS とラジオの時間ソースを選ぶ場合、注意しなければならないことは、特定の時間ソースによって提供される精度および安定性を確立することである。GPS と電波源の根本的な時間精度は素晴らしいが、しかし、いくつかの受信機は低い精度での使用を意図しており、正確な結果や安定した結果を提供しない。

G.1.4 NTP 実装考察（参考）

NTP サーバは常に NTP および SNTP クライアントの両方を支援する。違いは同期精度の一つであり、コミュニケーション互換性ではない。理論上、NTP クライアントおよび SNTP クライアントの両方がクライアント上で同時に動くことができるが、これは推奨されない。SNTP 最新版は単に時間精度を下げる。他の時間プロトコルクライアント、例えば、IRIG も使用されている場合、これらのクライアントは、NTP クライアントと調整し同期問題を回避しなければならない。

RFC-1305 には、NTP サーバや故障したサーバなどへの断続的なアクセスの管理に関する仕様書が含まれている。NTP プロセスが始まる場合、NTP サーバは存在する必要がないし使用可能である必要もない。NTP は、バックアップおよびよりよい精度を提供するために多数のサーバの使用を支援する。RFC1305 は、NTP クライアントによって使用されるメカニズムを指定する。サイト www.ntp.org は、バックアップおよび多数のサーバ構成のための、最も有効な構成に関する広範囲な指針および参照を提供する。

ローカルのバッテリークロックおよびクライアントオペレーティングシステムは適切に UTC を意識しなければならない。NTP 同期は UTC にある。これは混乱の源であり得る。なぜならいくつかのコンピュータは、ハードウェアクロックがローカル時間に設定されて構成され、オペレーティングシステムが UTC に（不正確に）設定されるからである。これは一般的なエラーであり、装置がクロックを同期させることを試みる場合だけ明白になる。

G.1.5 適合

NTP サーバおよび NTP クライアントのための適合性宣言書は、安全なトランザクションが支援されるかどうか述べなければならない。

NTP サーバのための適合性宣言書は、それがさらに NTP クライアントかどうか述べなければならない。

H アプリケーション構成管理プロファイル

H.1 アプリケーション構成管理プロファイル

アプリケーション構成管理プロファイルは、アクタ、つまり LDAP サーバ、LDAP クライアントおよび DNS サーバに適用する。必須およびオプションのトランザクションは、以下の表とセクションの中で述べる。

表 H.1-1. アプリケーション構成管理プロファイル

アクタ	トランザクション	オプション性	セクション
LDAP サーバ	問い合わせ LDAP サーバ	M	H.1.4.2
	LDAP サーバを更新する	O	H.1.4.3
	LDAP サーバを維持する	M	H.1.4.4
LDAP クライアント	LDAP サーバを見つける	M	H.1.4.1
	問い合わせ LDAP サーバ	M	H.1.4.2
	LDAP サーバを更新する	O	H.1.4.3
DNS サーバ	LDAP サーバを見つける	M	H.1.4.1

H.1.1 データモデルコンポーネントオブジェクト

図表の標準の定義はセクション H.1.3 で得ることができる。このセクションは、その図表に定義されたオブジェクトおよび情報の追加の有益な記述を与えて、DICOM システム挙動に関する規範的な陳述をする。

アプリケーション構成データモデルには次のコンポーネントオブジェクトがある：

装置	装置の記述
ネットワーク AE	ネットワークアプリケーションエンティティの記述
ネットワーク接続	ネットワークインタフェースの記述
転送能力	ネットワーク AE に支援された SOP クラスおよびシンタックスの記述

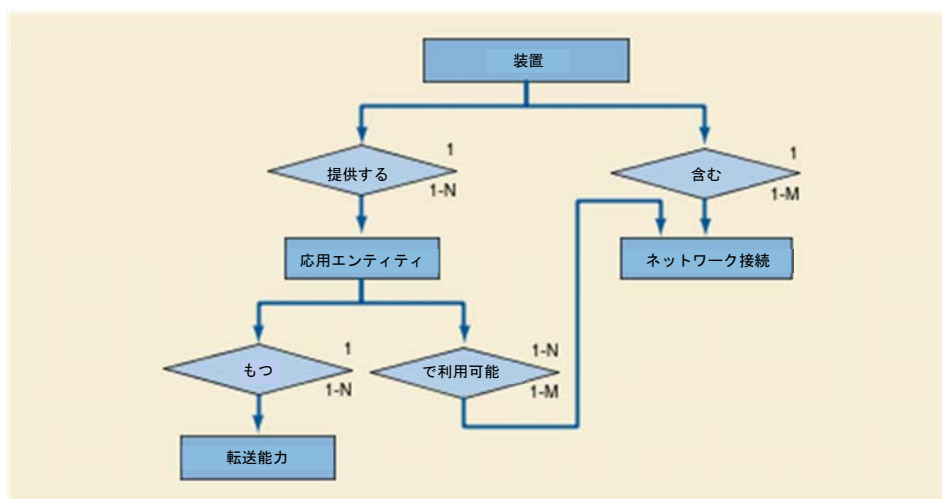


図 H.1-1. アプリケーション構成データモデル

さらに、多くの他のオブジェクトが LDAP スキーマの中で使用される（セクション H.1.2 および図 H.1-2 を参照）：

DICOM 構成ルート	DICOM 構成階層のルート
DICOM 装置ルート	DICOM 装置階層のルート
DICOM 一意的 AE タイトル登録簿ルート	DICOM 一意的 AE タイトル登録簿のルート
DICOM 一意的 AE タイトル	AE タイトル登録内の一意的 AE タイトル

LDAP は、図表に対する拡張がローカルのニーズ（つまり、オブジェクトは単一構造および多重補助 LDAP クラスを実施するかもしれない）を支援することを可能にする。DICOM は、クライアント支援にそのような拡張を義務付けない。サーバは、そのような拡張をローカルの目的のため支援してもよい。DICOM クライアントは拡張を受理または無視してもよいが、それらの存在をエラーと考えるべきではない。

H.1.1.1 装置

「装置」とは、特定の物理的なインスタンスではなくタスクを行うために組織されたコンポーネントのセットである。単純な装置の場合、データモデル装置に対応する 1 つの物理デバイスがあるかもしれない。しかし複雑な設備の場合、1 つの「装置」に多くの物理的な部分があるかもしれない。

「装置」とは、物理的なエンティティの集まりであり、その集まりはアプリケーションエンティティの集まりを支援する。それはこれらのエンティティと一意的に関連があり、逆もまた真である。それはネットワーク接続とも一意的に関連があり、逆もまた真である。単純なワークステーションが 1 つの CPU、電源接続およびネットワーク接続を備えていれば、「装置」はワークステーションである。

複雑な装置の一例は、多数のコンピュータのネットワークから構築されたサーバであり、コンピュータは多数のネットワーク接続および独立した電源接続をもっている。これは 1 つのアプリケーションエンティティおよび多数のネットワーク接続を備えた 1 つの装置である。このようなサーバが設計されるのは、個々のコンポーネントのコンピュータの置換を、オペレーションを乱すことなく行うためである。アプリケーション構成データモデルは、この内部構造を何ら記述しない。それが記述するのはネットワーク接続およびネットワーク可視のアプリケーションエンティティである。これらの複雑な装置は、非常に高い利用可能性のために通常設計されているが、システムシャットダウンの異常なイベントの場合、「装置」は、シャットダウンされるすべての部分に相当する。

表 H.1-2. 装置オブジェクトの属性

情報フィールド	重複度	概要
装置名	1	この装置の一意的名前 (LDAP データベースの範囲内の)。それは法的な LDAP 名に限定され、DICOM AE タイトル制限によって制約されない。
記述	0..1	装置の自由なテキスト記述。
製造業者	0..1	この装置によって作成された SOP インスタンスの中の製造業者(0008,0070)の値と同じにすることが望ましい。
製造業者モデル名	0..1	この装置によって作成された SOP インスタンスの中の製造業者モデル名(0008,1090)の値と同じにすることが望ましい。
ソフトウェアバージョン	0..N	この装置によって作成された SOP インスタンスの中のソフトウェアバージョン(0018,1020)の値と同じにすることが望ましい。
ステーション名	0..1	この装置によって作成された SOP インスタンスの中のステーション名(0008,1010)の値と同じにすることが望ましい。
装置製造番号	0..1	この装置によって作成された SOP インスタンスの中の装置通し番号(0018,1000)の値と同じにすることが望ましい。
主要な装置タイプ	0..N	装置のタイプを表し、収集モダリティに最も適用可能である。適用可能な場合、タイプは、CID30「DICOM 装置」のコード値(0008,0100)リストから選ばれることが望ましい。
施設名	0..N	この装置によって作成された SOP インスタンスの中の施設名(0008,0080)の値と同じにすることが望ましい。
施設アドレス	0..N	この装置によって作成された SOP インスタンス中の施設アドレス(0008,0081)属性の値と同じにすることが望ましい。
施設部門名	0..N	この装置によって作成された SOP インスタンスの中の施設の部門名(0008,1040)の値と同じにすることが望ましい。

情報フィールド	重複度	概要
患者 ID の発行者	0..1	この装置によって作成された SOP インスタンス用の患者 ID(0010.0021)の発行人のための初期設定値。ワークリストまたは他のソースで受け取った値によって無視されるかもしれない。
関連する装置参照	0..N	DICOM 構成階層の外の関連装置記述の DN。DICOM 装置オブジェクトを他の図表から実証された追加の LDAP オブジェクトにリンクするために使用でき、また別の管理上の目的に使用できる。
認可されたノード証明書参照	0..N	この装置に接続することを認可されるノードの証明書用の DN。DN は DICOM 構成階層内に存在する必要はない
このノード証明書参照	0..N	このノードのための公の証明書の DN。DN は DICOM 構成階層内に存在する必要はない
ベンダー装置データ	0..N	装置固有のベンダー構成情報
インストール済み	1	ネットワークにこの装置が現在インストールされているかどうかを示すブーリアン。(これは事前構成、モバイルのバンおよび同様の状況に有用)

「認可されたノード証明書参照」の意図は、この装置との通信を認められるノード証明書のリストを LDAP サーバが供給できるようにすることである。これらは公の証明書だけにすることが望ましい。このリストは完全である必要はない。他のネットワークピアは他のメカニズムによって認可されてもよい。

「このノード証明書参照」の意図は、LDAP サーバがこのノードに証明書を供給できるようにすることである。これらも LDAP から独立して扱われてもよい。

注

装置は多数の主要な装置タイプエントリをもってもよい。それは多機能の装置、例えば、PET と CT の組合せかもしれない。それはカスケード装置、例えば、画像取り込みおよび超音波かもしれない。

表 H.1-3. 装置オブジェクトの子オブジェクト

情報フィールド	重複度	概要
ネットワークアプリケーションエンティティ	1..N	この装置で利用可能なアプリケーションエンティティ (セクション H.1.1.2 を参照)
ネットワーク接続	1..N	この装置のためのネットワーク接続 (セクション H.1.1.3 を参照)

H.1.1.2 ネットワークアプリケーションエンティティ

ネットワーク AE はネットワーク上のサービスを提供するアプリケーションエンティティである。ネットワーク AE は使用される特定のネットワーク接続にかかわらず同じ機能的な能力をもつ。選択されたネットワーク接続に基づいた機能的な違いがある場合、これらは別々のネットワーク AE である。他の内部構造に基づいた機能的な違いがある場合、これらは別々のネットワーク AE である。

表 H.1-4. ネットワーク AE オブジェクトの属性

情報フィールド	重複度	概要
AE タイトル	1	このネットワーク AE のための一意的 AE タイトル
記述	0..1	アプリケーションエンティティの自由なテキスト記述
ベンダーデータ	0..N	AE の特定のベンダー構成情報
アプリケーションクラスタ	0..N	関連するアプリケーションの部分集合に対しローカルに定義された名前。例えば「神経放射線学」
好ましいコールド AE タイトル	0..N	アソシエーションの開始のために好まれる AE タイトル
好ましい呼出し AE タイトル	0..N	アソシエーションの受理のために好まれる AE タイトル。

情報フィールド	重複度	概要
アソシエーションアクセプタ	1	ブール値。ネットワーク AE がアソシエーションを受理できる場合に真であり、できない場合に偽である。
アソシエーションイニシエータ	1	ブール値。ネットワーク AE がアソシエーションを受理できる場合に真であり、できない場合に偽である。
ネットワーク接続参照	1..N	この AE のためのネットワーク接続オブジェクトの DN
支援された文字セット	0..N	それが受け取るデータセットに対しネットワーク AE によって支援された文字セット。値は PS3.3 の中で特定文字セット用の定義語(0008,0005)から選ばなければならない。値が存在しない場合、これはネットワーク AE が初期設定文字レパートリだけ (ISO IR 6) を支援することを示唆する。
インストール済み	0..1	ブール値。AE がネットワークにインストールされる場合に真である。存在しなければ、AE のインストールされたステータスに関する情報は、装置から継承される。

「アプリケーションクラスタ」の概念は、システムのローカルのクラスタを定義するメカニズムを提供する。構成管理のユースケースは 2 つのものを要求する。一つはネットワーク位相から独立している DICOM アプリケーションの「ドメイン」能力である。他の一つは DNS および他の TCP レベルプロトコルによって使用される管理上のドメインである。アプリケーションクラスタは多重価値であり、異なる目的のための多数のクラスタ生成の概念を可能にする。アプリケーションクラスタは、問い合わせの範囲を制限するために、問い合わせの一部として使用されると予想される。

「好ましいコールド AE タイトル」の概念の意図は、サイト管理者がアソシエーションを始める場合コミュニケーションパートナーとして使用するため好まれる AE の限定的な初期設定セットを定義できることである。この能力が特に役立つのは、大きな中央管理サイトが構成可能性を単純化し、かつ特定のワークフローシナリオ用の構成 AE の数を制限するときである。例えば、AE のセットは、クライアント装置がその構成優先に適應するために、割当てられたプリンタの AE タイトル、アーカイブ、RIS および QA ワークステーションを含む。「好ましいコールド AE タイトル」の概念は、リストに無記載の AE へのアソシエーション開始を禁止しない。リストに無記載の AE へのアソシエーションは必要ならば始めることができる。

「好ましい呼出し AE タイトル」の概念の意図は、サイト管理者がアソシエーションを受理する場合に好まれる AE の初期設定セットを定義できることである。「好ましい呼出し AE タイトル」概念は、リストに無記載の AE からアソシエーションを受理することを禁止しない。

「ネットワーク接続参照」は個別のネットワーク接続オブジェクトへのリンクである。参照されたネットワーク接続オブジェクトは AE オブジェクトの兄弟である（つまり両方とも同じ装置オブジェクトの子供である）。

表 H.1-5. ネットワーク AE オブジェクトの子オブジェクト

情報フィールド	重複度	概要
転送能力	1..N	このネットワーク AE に対する転送能力。セクション H.1.4 を参照

H.1.1.3 ネットワーク接続

「ネットワーク接続」は、1 つのネットワーク装置上の 1 つの TCP ポートについて記述する。これは、TCP 接続に使用され、ここでは DICOM アソシエーションが 1 つ以上のネットワーク AE と交渉できる。それはホスト名および TCP ポート番号を指定する。ネットワーク接続は多数のネットワーク AE を支援するかもしれない。ネットワーク AE 選択は、コールド AE タイトルおよび呼出し AE タイトルに基づいたアソシエーション交渉の間に起る。

表 H.1-6. ネットワーク接続オブジェクトの属性

情報フィールド	重複度	概要
一般名	0..1	ネットワーク接続オブジェクトの任意の名前。意味のある名前または文字の任意の一意的なシーケンスであり得る。RDN として使用できる。 注 「cn」属性タイプは基本的な LDAP に定義されたタイプで、一般名の同意語である。

情報フィールド	重複度	概要
ホスト名	1	これは特定の接続に対する DNS 名である。これは接続のための現在の IP アドレスを得るために使用される。任意のクライアント DNS ユーザーにとって明白であるために、ホスト名は十分に限定されなければならない。
ポート	0..1	AE がリスンする TCP ポート。(これは、単にアソシエーションを始めるネットワーク接続には見当らないかもしれない。)
TLS CipherSuite	0..N	この特定接続で支援される TLS CipherSuites。TLS CipherSuites は RFC2246 文字列表現を使用して記述されなければならない。(例えば「TLS_RSA_WITH_RC4_128_SHA」)
インストール済み	0..1	ブール値。ネットワーク接続がネットワークにインストールされる場合、真である。存在しなければ、ネットワーク接続のインストールされたステータスに関する情報は、装置から継承される。

アソシエーションを受理できるネットワーク接続に TLS CipherSuite を含む場合、その意味は、ネットワーク接続中のアソシエーションを成功裡に確立するためには TLS プロトコルを使用しなければならないということである。

単一のネットワーク AE を多数のネットワーク接続で利用してもよい。これは、利用可能性または性能上の理由でサーバにおいてしばしば行われる。例えば、各階が 1 階当たり単一のハブネットワークにつながれている病院では、主なサーバはハブの各々に対して直接接続されているかもしれない。これは、よりよい性能および信頼性を提供する。サーバが特定の物理的なネットワーク接続に基づいた挙動を変更しなければ、これらの多数のネットワーク接続のすべてで利用可能なネットワーク AE をもっていると言える。また、ネットワーク AE は、同じネットワークハードウェアポート上の多数の TCP ポートで目に見え、そして各 TCP ポートは個別のネットワーク接続として表される。これにより、例えば、TLS 安全 DICOM ポートおよび従来の不安全 DICOM ポートが同じ AE により支援されることが可能になる。

H.1.1.4 転送能力

ネットワーク AE オブジェクトはそれぞれ 1 つ以上の転送能力をもつ。転送能力はそれぞれ次のものを指定する。つまりネットワーク AE が支援できる SOP クラス、それが利用できるモード (SCP または SCU)、およびそれが利用できる転送構文である。ネットワーク AE が同じ SOP クラスを SCP および SCU モードの両方で支援する場合、それは、2 つの転送能力オブジェクトをその SOP クラスに対してもつ。

表 H.1-7. 転送能力オブジェクトの属性

情報フィールド	重複度	概要
一般名	0..1	転送能力オブジェクトの任意の名前。意味のある名前または文字の任意の一意的なシーケンスであり得る。RDN として使用できる。
SOP クラス	1	SOP クラス UID
役割	1	「SCU」または「SCP」のいずれか
転送構文	1..N	SCU として要求されるか、または SCP として提示される転送構文

H.1.1.5 DICOM 構成ルート

この構造のオブジェクトクラスは、DICOM 構成階層のルートを表す。このタイプの単一のオブジェクトだけが組織的なドメイン内に存在することが望ましい。DICOM 構成階層のルートを見つけるために、クライアントはこのクラスのオブジェクトを探索できる。

表 H.1-8. DICOM 構成ルートオブジェクトの属性

情報フィールド	重複度	概要
一般名	1	構成ルートの名前。RDN として使用されることが望ましい。名前は「DICOM 構成」でなければならない。
記述	0..1	自由なテキスト記述。

表 H.1-9. DICOM 構成ルートオブジェクトの子オブジェクト

情報フィールド	重複度	概要
装置ルート	1	DICOM 装置階層のルート
一意的 AE タイトル登録簿ルート	1	一意的 AE タイトル登録簿のルート

H.1.1.6 装置ルート

この構造のオブジェクトクラスは、DICOM 装置階層のルートを表す。このタイプの単一のオブジェクトだけが DICOM 構成ルートの子供として存在することが望ましい。DICOM 装置階層のルートを見つけるために、クライアントはこのクラスのオブジェクトを探索できる。

表 H.1-10. 装置ルートオブジェクトの属性

情報フィールド	重複度	概要
一般名	1	装置ルートの名前。RDN として使用されることが望ましい。名前は「装置」でなければならない。
記述	0..1	自由なテキスト記述。

表 H.1-11. 装置ルートオブジェクトの子オブジェクト

情報フィールド	重複度	概要
装置	0..N	この組織的なドメイン内にインストールされた個々の装置

H.1.1.7 一意的 AE タイトル登録簿ルート

この構造のオブジェクトクラスは、一意的 AE タイトル登録簿階層のルートを表す。このタイプの単一のオブジェクトだけが DICOM 構成ルートの子供として存在することが望ましい。一意的 AE タイトル登録簿のルートを見つけるために、クライアントはこのクラスのオブジェクトを探索できる。

表 H.1-12. 一意的 AE タイトル登録簿ルートオブジェクトの属性

情報フィールド	重複度	概要
一般名	1	一意的 AE タイトル登録簿ルートの名前。RDN として使用されることが望ましい。名前は「一意的 AE タイトル登録簿」でなければならない。
記述	0..1	自由なテキスト記述。

表 H.1-13. 一意的 AE タイトル登録簿ルートオブジェクトの子オブジェクト

情報フィールド	重複度	概要
一意的 AE タイトル	0..N	この組織的なドメイン内にインストールされた一意的 AE タイトル（セクション H.1.1.8 を参照）

H.1.1.8 一意的 AE タイトル

この構造オブジェクトクラスは一意的アプリケーションエンティティタイトルを表す。このタイプのオブジェクトは、単に一意的 AE タイトル登録簿ルートの子供として存在することが望ましい。このオブジェクトクラスの唯一の目的は一意的 AE タイトルの配分を可能にすることである。AE タイトルに関連した運用上の情報はすべて、個別のネットワーク AE オブジェクト内に維持される。

表 H.1-14. 一意的 AE タイトルオブジェクトの属性

情報フィールド	重複度	概要
AE タイトル	1	一意の AE タイトル。

H.1.2 アプリケーション構成データモデル階層

LDAP 構造は命名されたオブジェクトの階層で構築される。この階層はサイトが変わると変わる。DICOM 構成管理機能は、この階層内のそのオブジェクトを予測可能な方法で見つける必要がある。この理由で、3つの特定オブジェクトクラスが、DICOM 階層の一番上の3つのオブジェクトのために定義される。これらの3つのオブジェクトクラスは、このツリー関係において LDAP 階層の他の場所で使用されてはならない。

階層の DICOM 部分は、クラス `dicomConfigurationRoot` のルートオブジェクトで始まらなければならない、そして一般名は「DICOM 構成」である。このオブジェクトの下に2つの他のオブジェクトがなければならない：

- 一つはクラス `dicomDevicesRoot` のオブジェクトであり、一般名は「装置」である。これは、オブジェクトのツリーのルートであり、オブジェクトはセクション H.1.1 のアプリケーション構成データモデル構造に相当する。
- 他の一つはクラス `dicomUniqueAETitlesRegistryRoot` のオブジェクトであり、一般名は「一意の AE タイトル登録簿」である。これはオブジェクトの水平なツリーのルートである。これらのオブジェクトの各々は、現在割当てられている AE タイトルのうちの1つで指定される。これは、利用可能な AE タイトルを見つけるためのメカニズムである。

3つのオブジェクトクラス、つまり `dicomConfigurationRoot`、`dicomDevicesRoot` および `dicomUniqueAETitleRegistryRoot` が、LDAP クライアントによって使用される、その目的は LDAP 階層内に DICOM 構成情報のローカルのルートを確認することであり、ルートは他の多くの目的に使用されるかもしれない。

注

システム起動中に、DICOM 構成アプリケーションは、オブジェクトクラス `dicomConfigurationRoot` のエントリの LDAP 検索を行い、次に、それが直下に `dicomDevicesRoot` と `dicomUniqueAETitlesRegistryRoot` のエントリをもつことを確認する。この構成をそれが見つける場合、それはローカルの LDAP ツリーの内の十分な位置を保存し、DICOM ツリーのルートとしてそれを使用できる。

`dicomUniqueAETitlesRegistryRoot` の真下のオブジェクトは、DICOM AE タイトルに必要な一意性を提供するために使用される。`dicomUniqueAETitle` オブジェクトには一意の AE タイトルを表す単一の属性がある。新しい AE タイトルが必要な場合、一時的な新しい名前が選択される。新しい名前は、LDAP クリエイト設備の使用により保存され、その目的はクラス `dicomUniqueAETitle` のオブジェクトを作成することであり、AE タイトルオブジェクトの下で新しい名前をもつ。この名前が既に使用されていれば、クリエイトは失敗する。そうでなければ、これはその名前を保存する。LDAP 問い合わせは、現在割当てられた AE タイトルのリストを得るために使用できるが、それは `dicomUniqueAETitlesRegistryRoot` オブジェクトの下のすべての名前のリストを得ることにより可能になる。

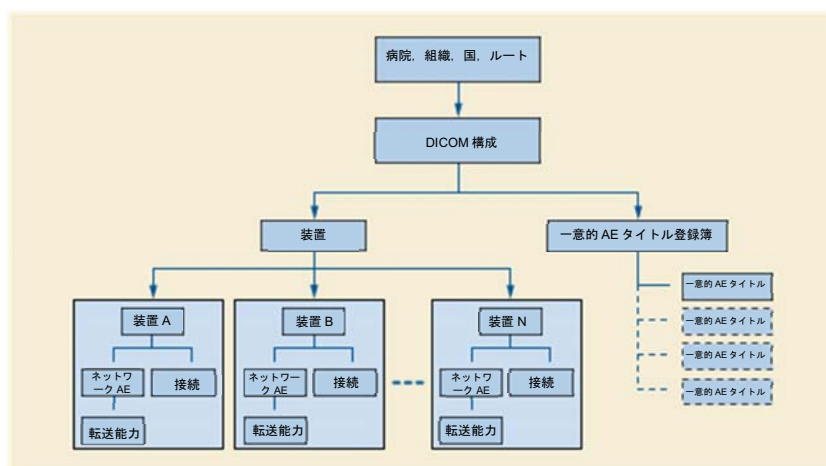


図 H.1-2. DICOM 構成階層

注

1. LDAP はルートおよび相対的な階層的命名システムをオブジェクトのために使用する。すべてのオブジェクト名は、階層全体の中で完全に一意である。これは、「一意的 AE タイトル登録簿」の下のオブジェクトの名前が一意であることを意味する。さらに、それは、ネットワーク AE および接続の名前がそれらの階層文脈内にあることを意味する。例えば、図 H.1-2 中のネットワーク AE のうちの 1 つのための DN は次のとおりである：

dicomAETitle=CT_01, dicomDeviceName=Special Research CT, cn=Devices, cn=DICOM Configuration, o=Some town Hospital

2. 理論上、多数の独立した DICOM 構成階層が 1 つの組織内に存在することがある。そのようなネットワーク中の LDAP サーバはローカルな装置アクセスを抑制することが望ましく、それは DICOM 構成クライアントは、各クライアントに見える唯一の DICOM 構成階層をもつようにするためである。
3. 2 つの組織の合併は、DICOM 構成階層を合併することを手動の構成管理に要求する。AE タイトル、役割における矛盾および他の矛盾が恐らくあるであろう。

H.1.3 オブジェクトおよび属性用の LDAP スキーマ

個々の LDAP 属性情報は、以下の図表の初めのコメントの中で要約される。オブジェクトと属性の形式上の定義は、以下の図表にある。この図表は、補足図表の定義により拡張され、それは補助のクラス、この図表に由来したサブクラスまたはその両方を定義する。

アプリケーション構成データモデルおよび DICOM 構成階層のための正式の LDAP スキーマは次のとおりである：

```

# 3 Attribute Type Definitions
#
# The following attribute types are defined in this document:
#
# Name          Syntax  Multiplicity
# -----
# dicomDeviceName      string  Single
# dicomDescription     string  Single
# dicomManufacturer    string  Single
# dicomManufacturerModelName  string  Single
# dicomSoftwareVersion string  Multiple
# dicomVendorData      binary  Multiple
# dicomAETitle         string  Single
# dicomNetworkConnectionReference  DN      Multiple
# dicomApplicationCluster  string  Multiple
# dicomAssociationInitiator  bool    Single
# dicomAssociationAcceptor  bool    Single
# dicomHostname        string  Single
# dicomPort            integer Single
# dicomSOPClass        OID     Single
# dicomTransferRole    string  Single
# dicomTransferSyntax  OID     Multiple
# dicomPrimaryDeviceType  string  Multiple
# dicomRelatedDeviceReference  DN      Multiple
# dicomPreferredCalledAETitle  string  Multiple
# dicomTLSCipherSuite  string  Multiple
# dicomAuthorizedNodeCertificateReference  DN      Multiple
# dicomThisNodeCertificateReference  DN      Multiple
# dicomInstalled       bool    Single
# dicomStationName     string  Single
# dicomDeviceSerialNumber  string  Single
# dicomInstitutionName  string  Multiple
# dicomInstitutionAddress  string  Multiple
# dicomInstitutionDepartmentName  string  Multiple
# dicomIssuerOfPatientID  string  Single
# dicomPreferredCallingAETitle  string  Multiple
# dicomSupportedCharacterSet  string  Multiple
#
# 3.1 dicomDeviceName      string  Single
#

```

```
# This attribute stores the unique name (within the scope of the LDAP database)
# for a DICOM Device.
#
# It is a single-valued attribute.
# This attribute's syntax is 'Directory String'.
# Its case is not significant for equality and substring matches.
#
attributetype ( 1.2.840.10008.15.0.3.1
  NAME 'dicomDeviceName'
  DESC 'The unique name for the device'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE )

# 3.2 dicomDescription          string  Single
#
# This attribute stores the (unconstrained) textual description for a DICOM entity.
#
# It is a single-valued attribute.
# This attribute's syntax is 'Directory String'.
# Its case is not significant for equality and substring matches.
#
attributetype ( 1.2.840.10008.15.0.3.2
  NAME 'dicomDescription'
  DESC 'Textual description of the DICOM entity'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE )

# 3.3 dicomManufacturer        string  Single
#
# This attribute stores the Manufacturer name for a DICOM Device.
# Should be identical to the value of the DICOM attribute Manufacturer (0008,0070) [VR=LO]
# contained in SOP Instances created by this device.
#
# It is a single-valued attribute.
# This attribute's syntax is 'Directory String'.
# Its case is not significant for equality and substring matches.
#
attributetype ( 1.2.840.10008.15.0.3.3
  NAME 'dicomManufacturer'
  DESC 'The device Manufacturer name'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE )

# 3.4 dicomManufacturerModelName  string  Single
#
# This attribute stores the Manufacturer Model Name for a DICOM Device.
# Should be identical to the value of the DICOM attribute Manufacturer
# Model Name (0008,1090) [VR=LO]
# contained in SOP Instances created by this device.
#
# It is a single-valued attribute.
# This attribute's syntax is 'Directory String'.
# Its case is not significant for equality and substring matches.
#
```



```
attributetype ( 1.2.840.10008.15.0.3.4
  NAME 'dicomManufacturerModelName'
  DESC 'The device Manufacturer Model Name'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE )
```

```
# 3.5 dicomSoftwareVersion      string  Multiple
#
# This attribute stores the software version of the device and/or its subcomponents.
# Should be the same as the values of Software Versions (0018,1020) in
# SOP instances created by this device.
#
# It is a multi-valued attribute.
# This attribute's syntax is 'Directory String'.
# Its case is not significant for equality and substring matches.
#
```

```
attributetype ( 1.2.840.10008.15.0.3.5
  NAME 'dicomSoftwareVersion'
  DESC 'The device software version. Should be the same as the values of Software
  Versions (0018,1020) in SOP instances created by this device.'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

```
# 3.6 dicomVendorData          binary   Multiple
#
# This attribute stores vendor specific configuration information.
#
# It is a multi-valued attribute.
# This attribute's syntax is 'Binary'.
# Neither equality nor substring matches are applicable to binary data.
#
```

```
attributetype ( 1.2.840.10008.15.0.3.6
  NAME 'dicomVendorData'
  DESC 'Arbitrary vendor-specific configuration information (binary data)'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.5 )
```

```
# 3.7 dicomAETitle             name    Single
#
# This attribute stores an Application Entity (AE) title.
#
# It is a single-valued attribute.
# This attribute's syntax is 'IA5 String'.
# Its case is significant.
#
```

```
attributetype ( 1.2.840.10008.15.0.3.7
  NAME 'dicomAETitle'
  DESC 'Application Entity (AE) title'
  EQUALITY caseExactIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
  SINGLE-VALUE )
```

```
# 3.8 dicomNetworkConnectionReference  DN      Multiple
#
# This attribute stores the DN of a dicomNetworkConnection object
# used by an Application Entity.
#
# It is a multi-valued attribute.
```

```
# This attribute's syntax is 'Distinguished Name'.
#
attributetype ( 1.2.840.10008.15.0.3.8
  NAME 'dicomNetworkConnectionReference'
  DESC 'The DN of a dicomNetworkConnection object used by an Application Entity'
  EQUALITY distinguishedNameMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )

# 3.9 dicomApplicationCluster      string  Multiple
#
# This attribute stores an application cluster name for an Application
# Entity (e.g., "Neuroradiology Research")
#
# It is a multi-valued attribute.
# This attribute's syntax is 'Directory String'.
# Its case is not significant for equality and substring matches.
#
attributetype ( 1.2.840.10008.15.0.3.9
  NAME 'dicomApplicationCluster'
  DESC 'Application cluster name for an Application Entity (e.g., "Neuroradiology Research")'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

# 3.10 dicomAssociationInitiator   bool    Single
#
# This attribute indicates if an Application Entity is capable of initiating
# network associations.
#
# It is a single-valued attribute.
# This attribute's syntax is 'Boolean'.
#
attributetype ( 1.2.840.10008.15.0.3.10
  NAME 'dicomAssociationInitiator'
  DESC 'Indicates if an Application Entity is capable of initiating network associations'
  EQUALITY booleanMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
  SINGLE-VALUE )

# 3.11 dicomAssociationAcceptor    bool    Single
#
# This attribute indicates if an Application Entity is capable of accepting
# network associations.
#
# It is a single-valued attribute.
# This attribute's syntax is 'Boolean'.
#
attributetype ( 1.2.840.10008.15.0.3.11
  NAME 'dicomAssociationAcceptor'
  DESC 'Indicates if an Application Entity is capable of accepting network associations'
  EQUALITY booleanMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
  SINGLE-VALUE )

# 3.12 dicomHostname              string  Single
#
# This attribute stores a DNS hostname for a connection.
#
# It is a single-valued attribute.
# This attribute's syntax is 'Directory String'.
```

Its case is not significant for equality and substring matches.

#

```
attributetype ( 1.2.840.10008.15.0.3.12
  NAME 'dicomHostname'
  DESC 'DNS hostname'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE )
```

3.13 dicomPort integer Single

#

This attribute stores a TCP port number for a connection.

#

It is a single-valued attribute.

This attribute's syntax is 'Integer'.

#

```
attributetype ( 1.2.840.10008.15.0.3.13
  NAME 'dicomPort'
  DESC 'TCP Port number'
  EQUALITY integerMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
  SINGLE-VALUE )
```

3.14 dicomSOPClass OID Single

#

This attribute stores a SOP Class UID

#

It is a single-valued attribute.

This attribute's syntax is 'OID'.

#

```
attributetype ( 1.2.840.10008.15.0.3.14
  NAME 'dicomSOPClass'
  DESC 'A SOP Class UID'
  EQUALITY objectIdentifierMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.38
  SINGLE-VALUE )
```

3.15 dicomTransferRole String Single

#

This attribute stores a transfer role (either "SCU" or "SCP").

#

It is a single-valued attribute.

This attribute's syntax is 'Directory String'.

Its case is not significant for equality and substring matches.

#

```
attributetype ( 1.2.840.10008.15.0.3.15
  NAME 'dicomTransferRole'
  DESC 'Transfer role (either "SCU" or "SCP")'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE )
```

3.16 dicomTransferSyntax OID Multiple

#

This attribute stores a Transfer Syntax UID

#

It is a multi-valued attribute.

This attribute's syntax is 'OID'.

```
#
attributetype ( 1.2.840.10008.15.0.3.16
  NAME 'dicomTransferSyntax'
  DESC 'A Transfer Syntax UID'
  EQUALITY objectIdentifierMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.38 )

# 3.17 dicomPrimaryDeviceType      string  Multiple
#
# This attribute stores the primary type for a DICOM Device.
# Types should be selected from the list of code values (0008,0100)
# for Context ID 30 in DICOM Part 16 when applicable.
#
# It is a multiple-valued attribute.
# This attribute's syntax is 'IA5 String'.
# Its case is significant.
#
attributetype ( 1.2.840.10008.15.0.3.17
  NAME 'dicomPrimaryDeviceType'
  DESC 'The device Primary Device type'
  EQUALITY caseExactIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

# 3.18 dicomRelatedDeviceReference  DN      Multiple
#
# This attribute stores a reference to a related device description outside
# the DICOM Configuration Hierachy. Can be used to link the DICOM Device object to
# additional LDAP objects instantiated from other schema and used for
# separate administrative purposes.
#
# This attribute's syntax is 'Distinguished Name'.
# It is a multiple-valued attribute.
#
attributetype ( 1.2.840.10008.15.0.3.18
  NAME 'dicomRelatedDeviceReference'
  DESC 'The DN of a related device description outside the DICOM Configuration Hierachy'
  EQUALITY distinguishedNameMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )

# 3.19 dicomPreferredCalledAETitle  string  Multiple
#
# AE Title(s) to which associations may be preferably initiated.
#
# It is a multiple-valued attribute.
# This attribute's syntax is 'IA5 String'.
# Its case is significant.
#
attributetype ( 1.2.840.10008.15.0.3.19
  NAME 'dicomPreferredCalledAETitle'
  DESC 'AE Title(s) to which associations may be preferably initiated.'
  EQUALITY caseExactIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

# 3.20 dicomTLSCipherSuite          string  Multiple
#
# The attribute stores the supported TLS CipherSuites.
# TLS CipherSuites shall be described using a RFC-2246 string representation
# (e.g., "TLS_RSA_WITH_RC4_128_SHA").
#
# It is a multiple-valued attribute.
```

```
# This attribute's syntax is 'IA5 String'.
# Its case is significant.
#
attributetype ( 1.2.840.10008.15.0.3.20
  NAME 'dicomTLSCipherSuite'
  DESC 'The supported TLS CipherSuites'
  EQUALITY caseExactIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

# 3.21 dicomAuthorizedNodeCertificateReference DN Multiple
#
# This attribute stores a reference to a TLS public certificate for a DICOM
# node that is authorized to connect to this node. The certificate
# is not necessarily stored within the DICOM Hierarchy
#
# This attribute's syntax is 'Distinguished Name'.
# It is a multiple-valued attribute.
#
attributetype ( 1.2.840.10008.15.0.3.21
  NAME 'dicomAuthorizedNodeCertificateReference'
  DESC 'The DN of a Certificate for a DICOM node that is authorized to connect to this node'
  EQUALITY distinguishedNameMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )

# 3.22 dicomThisNodeCertificateReference DN Multiple
#
# This attribute stores a reference to a TLS public certificate for
# this node. It is not necessarily stored as part of
# the DICOM Configuration Hierachy.
#
# This attribute's syntax is 'Distinguished Name'.
# It is a multiple-valued attribute.
#
attributetype ( 1.2.840.10008.15.0.3.22
  NAME 'dicomThisNodeCertificateReference'
  DESC 'The DN of a related device description outside the DICOM Configuration Hierachy'
  EQUALITY distinguishedNameMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )

# 3.23 dicomInstalled          bool    Single
#
# This attribute indicates whether the object is presently installed.
#
# It is a single-valued attribute.
# This attribute's syntax is 'Boolean'.
#
attributetype ( 1.2.840.10008.15.0.3.23
  NAME 'dicomInstalled'
  DESC 'Indicates if the DICOM object (device, Network AE, or Port) is presently installed'
  EQUALITY booleanMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
  SINGLE-VALUE )

# 3.24 dicomStationName      string  Single
#
# This attribute stores the station name of the device.
# Should be the same as the value of Station Name (0008,1010) in
# SOP instances created by this device.
#
# It is a single-valued attribute.
```

```
# This attribute's syntax is 'Directory String'.
#
attributetype ( 1.2.840.10008.15.0.3.24
  NAME 'dicomStationName'
  DESC 'Station Name of the device. Should be the same as the value of Station
    Name (0008,1010) in SOP instances created by this device.'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE)

# 3.25 dicomDeviceSerialNumber      string  Single
#
# This attribute stores the serial number of the device.
# Should be the same as the value of Device Serial Number (0018,1000)
# in SOP instances created by this device.
#
# It is a single-valued attribute.
# This attribute's syntax is 'Directory String'.
#
attributetype ( 1.2.840.10008.15.0.3.25
  NAME 'dicomDeviceSerialNumber'
  DESC 'Serial number of the device. Should be the same as the value of Device Serial
    Number (0018,1000) in SOP instances created by this device.'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE)

# 3.26 dicomInstitutionName         string  Multiple
#
# This attribute stores the institution name of the device.
# Should be the same as the value of Institution Name (0008,0080)
# in SOP Instances created by this device.
#
# It is a multi-valued attribute.
# This attribute's syntax is 'Directory String'.
#
attributetype ( 1.2.840.10008.15.0.3.26
  NAME 'dicomInstitutionName'
  DESC 'Institution name of the device. Should be the same as the value of Institution
    Name (0008,0080) in SOP Instances created by this device.'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

# 3.27 dicomInstitutionAddress      string  Multiple
#
# This attribute stores the institution address of the device.
# Should be the same as the value of Institution Address (0008,0081)
# attribute in SOP Instances created by this device.
#
# It is a multi-valued attribute.
# This attribute's syntax is 'Directory String'.
#
attributetype ( 1.2.840.10008.15.0.3.27
  NAME 'dicomInstitutionAddress'
  DESC 'Institution address of the device. Should be the same as the value of Institution
    Address (0008,0081) attribute in SOP Instances created by this device.'
  EQUALITY caseIgnoreMatch
```

SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15)

3.28 dicomInstitutionDepartmentName string Multiple

#

This attribute stores the institution department name of the device.
Should be the same as the value of Institutional Department Name (0008,1040)
in SOP Instances created by this device.

#

It is a multi-valued attribute.

This attribute's syntax is 'Directory String'.

#

attributetype (1.2.840.10008.15.0.3.28

NAME 'dicomInstitutionDepartmentName'

DESC 'Institution department name of the device. Should be the same as the value of Institutional
Department Name (0008,1040) in SOP Instances created by this device.'

EQUALITY caseIgnoreMatch

SUBSTR caseIgnoreSubstringsMatch

SYNTAX 1.3.6.1.4.1.1466.115.121.1.15)

3.29 dicomIssuerOfPatientID string Single

#

This attribute stores the Default value for the Issuer of Patient ID (0010,0021)
for SOP Instances created by this device. May be overridden by the values
received in a worklist or other source.

#

It is a multi-valued attribute.

This attribute's syntax is 'Directory String'.

#

attributetype (1.2.840.10008.15.0.3.29

NAME 'dicomIssuerOfPatientID'

DESC 'Default value for the Issuer of Patient ID (0010,0021) for SOP Instances created by this device.
May be overridden by the values received in a worklist or other source.'

EQUALITY caseIgnoreMatch

SUBSTR caseIgnoreSubstringsMatch

SYNTAX 1.3.6.1.4.1.1466.115.121.1.15)

3.30 dicomPreferredCallingAETitle string Multiple

#

AE Title(s) to which associations may be preferably accepted.

#

It is a multiple-valued attribute.

This attribute's syntax is 'IA5 String'.

Its case is significant.

#

attributetype (1.2.840.10008.15.0.3.30

NAME 'dicomPreferredCallingAETitle'

DESC 'AE Title(s) to which associations may be preferably accepted.'

EQUALITY caseExactIA5Match

SYNTAX 1.3.6.1.4.1.1466.115.121.1.26)

3.31 dicomSupportedCharacterSet string Multiple

#

The Character Set(s) supported by the Network AE for data sets it receives.

Contains one of the Defined Terms for Specific Character Set (0008,0005).

If not present, this implies that the Network AE supports only the default

character repertoire (ISO IR 6).

#

It is a multiple-valued attribute.

This attribute's syntax is 'IA5 String'.

```

# Its case is significant.
#
attributetype ( 1.2.840.10008.15.0.3.31
  NAME 'dicomSupportedCharacterSet'
  DESC 'The Character Set(s) supported by the Network AE for data sets it receives.'
  EQUALITY caseExactIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

# 4 Object Class Definitions
#
# The following object classes are defined in this document. All are
# structural classes.
#
# Name                Description
# -----
# dicomConfigurationRoot    root of the DICOM Configuration Hierarchy
# dicomDevicesRoot          root of the DICOM Devices Hierarchy
# dicomUniqueAETitlesRegistryRoot root of the Unique DICOM AE-Titles Registry Hierarchy
# dicomDevice                Devices
# dicomNetworkAE             Network AE
# dicomNetworkConnection    Network Connections
# dicomUniqueAETitle         Unique AE Title
# dicomTransferCapability    Transfer Capability

#
# 4.1 dicomConfigurationRoot
#
# This structural object class represents the root of the DICOM Configuration Hierarchy.
# Only a single object of this type should exist within an organizational domain.
# Clients can search for an object of this class to locate the root of the
# DICOM Configuration Hierarchy.
#
objectclass ( 1.2.840.10008.15.0.4.1
  NAME 'dicomConfigurationRoot'
  DESC 'Root of the DICOM Configuration Hierarchy'
  SUP top
  STRUCTURAL
  MUST ( cn )
  MAY ( description ) )

#
# 4.2 dicomDevicesRoot
#
# This structural object class represents the root of the DICOM Devices Hierarchy.
# Only a single object of this type should exist as a child of dicomConfigurationRoot.
#
objectclass ( 1.2.840.10008.15.0.4.2
  NAME 'dicomDevicesRoot'
  DESC 'Root of the DICOM Devices Hierarchy'
  SUP top
  STRUCTURAL
  MUST ( cn )
  MAY ( description ) )

#
# 4.3 dicomUniqueAETitlesRegistryRoot
#
# This structural object class represents the root of the Unique DICOM AE-Titles
# Registry Hierarchy.

```



```
# Only a single object of this type should exist as a child of dicomConfigurationRoot.
```

```
#  
objectclass ( 1.2.840.10008.15.0.4.3  
  NAME 'dicomUniqueAETitlesRegistryRoot'  
  DESC 'Root of the Unique DICOM AE-Title Registry Hierarchy'  
  SUP top  
  STRUCTURAL  
  MUST ( cn )  
  MAY ( description ) )
```

```
#  
# 4.4 dicomDevice  
#  
# This structural object class represents a DICOM Device.  
#
```

```
objectclass ( 1.2.840.10008.15.0.4.4  
  NAME 'dicomDevice'  
  DESC 'DICOM Device related information'  
  SUP top  
  STRUCTURAL  
  MUST (  
    dicomDeviceName $  
    dicomInstalled )  
  MAY (  
    dicomDescription $  
    dicomManufacturer $  
    dicomManufacturerModelName $  
    dicomSoftwareVersion $  
    dicomStationName $  
    dicomDeviceSerialNumber $  
    dicomInstitutionName $  
    dicomInstitutionAddress $  
    dicomInstitutionDepartmentName $  
    dicomIssuerOfPatientID $  
    dicomVendorData $  
    dicomPrimaryDeviceType $  
    dicomRelatedDeviceReference $  
    dicomAuthorizedNodeCertificateReference $  
    dicomThisNodeCertificateReference ) )
```

```
#  
# 4.5 dicomNetworkAE  
#  
# This structural object class represents a Network Application Entity  
#
```

```
objectclass ( 1.2.840.10008.15.0.4.5  
  NAME 'dicomNetworkAE'  
  DESC 'DICOM Network AE related information'  
  SUP top  
  STRUCTURAL  
  MUST (  
    dicomAETitle $  
    dicomNetworkConnectionReference $  
    dicomAssociationInitiator $  
    dicomAssociationAcceptor )  
  MAY (  
    dicomDescription $  
    dicomVendorData $  
    dicomApplicationCluster $  
    dicomPreferredCalledAETitle $
```

```
dicomPreferredCallingAETitle $
dicomSupportedCharacterSet $
dicomInstalled ) )
```

```
#
# 4.6 dicomNetworkConnection
#
# This structural object class represents a Network Connection
#
```

```
objectclass ( 1.2.840.10008.15.0.4.6
NAME 'dicomNetworkConnection'
DESC 'DICOM Network Connection information'
SUP top
STRUCTURAL
MUST ( dicomHostname )
MAY (
  cn $
  dicomPort $
  dicomTLSCipherSuite $
  dicomInstalled ) )
```

```
#
# 4.7 dicomUniqueAETitle
#
# This structural object class represents a Unique Application Entity Title
#
```

```
objectclass ( 1.2.840.10008.15.0.4.7
NAME 'dicomUniqueAETitle'
DESC 'A Unique DICOM Application Entity title'
SUP top
STRUCTURAL
MUST ( dicomAETitle ) )
```

```
#
# 4.8 dicomTransferCapability
#
# This structural object class represents Transfer Capabilities for an Application Entity
#
```

```
objectclass ( 1.2.840.10008.15.0.4.8
NAME 'dicomTransferCapability'
DESC 'Transfer Capabilities for an Application Entity'
SUP top
STRUCTURAL
MUST (
  dicomSOPClass $
  dicomTransferRole $
  dicomTransferSyntax )
MAY (
  cn ) )
```

H.1.4 トランザクション

H.1.4.1 LDAP サーバを見つける

H.1.4.1.1 適用範囲

RFC2782 サービス (DNS SRV) の位置を指定するための DNS RR が指定するのは、機械の名前を要求するメカニズムおよびネットワークサービスを提供する機械の基本的な記述である。DNS クライアントは、特定のサービス名をオファーするとして登録されるすべての機械のための記述を要求する。この場合、要求されたサービス名は「LDAP」である。DNS サーバは多数の名前で単一のリクエストに対して答えてもよい。

H.1.4.1.2 ユースケース／役割

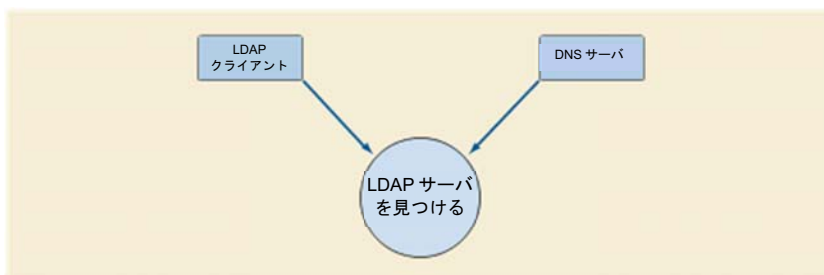


図 H.1-3. LDAP サーバを見つける

DNS サーバ LDAP サーバのリストを提供する。

LDAP クライアント LDAP サーバにリストを要請する。

H.1.4.1.3 参照される標準

RFC2181 DNS 仕様書の解明

RFC2219 ネットワークサービスのための DNS エイリアスの使用

RFC2782 サービスのロケーションを指定する DNS RR (DNS SRV)

他の RFC は、RFC2181, RFC2219 および RFC2782 からの参照によって含まれている。

H.1.4.1.4 相互作用図

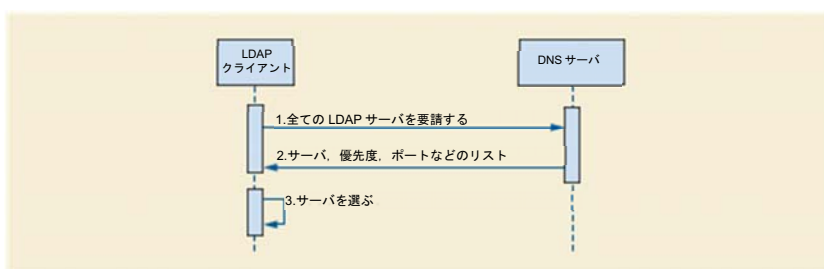


図 H.1-4. LDAP サーバを選ぶ

DNS クライアントは、利用可能なすべての LDAP サーバのリストを要求しなければならない。クライアントは優先度、キャパシティ、位置の情報を DNS によって提供され、それを使用してサーバを選ぶ。(RFC2782 は、これらのパラメータの適切な使用を勧める。) LDAP サーバがないか、または DNS サーバが SRV RR リクエストを支援しないことがあり得る。

注

1. 多数の LDAP サーバが共通の複製 LDAP データベースへのアクセスを提供するが、これは一般に支援される構成である。これにより、LDAP サーバは、最良の性能およびフォールトトレランスに適切な場所に位置することができる。DNS サーバ応答情報は、最も適切なサーバを選ぶ指針を提供する。
2. 多数の LDAP サーバは異なるデータベースも提供するかもしれない。この状況で、クライアントは、いくつかのサーバを調べて、DICOM 構成データベースを支援するサーバを見つけなければならないかもしれない。同様に、単一の LDAP サーバが多数の基礎 DN を支援してもよいし、クライアントは、これらの DN の各々をチェックしてどれが DICOM を支援するツリーであるか決める必要がある。

H.1.4.1.5 代替パス

クライアントは、DNS サーバが LDAP サーバ位置を提供しない場合、使用される LDAP サーバを手動で初期設定選択するメカニズムをもつてもよい。

H.1.4.2 LDAP サーバを問い合わせる

H.1.4.2.1 適用範囲

RFC2251「軽量ディレクトリアクセスプロトコル (v3)」は、LDAP スキーマに対応するデータベースの問い合わせをするメカニズムを指定する。LDAP クライアントは、リクエストを LDAP 問い合わせ言語で構成でき、そして LDAP サーバは単一のリクエストに対する結果で応答する。

H.1.4.2.2 ユースケース／役割

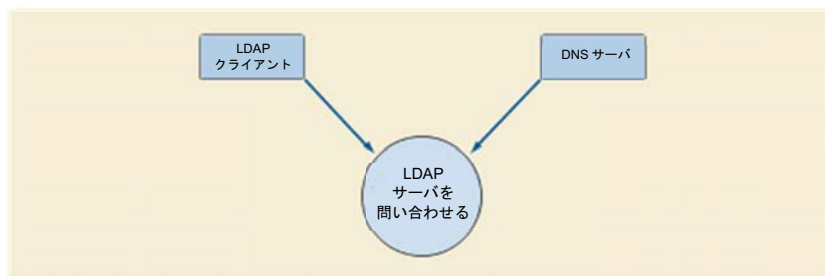


図 H.1-5. LDAP サーバを問い合わせる

LDAP サーバ 問い合わせ応答を提供する。

LDAP クライアント LDAP 情報を要求する。

H.1.4.2.3 参照される標準

RFC2251 軽量ディレクトリアクセスプロトコル (v3)。LDAP 支援は、参照によって起動された他の RFC への適合を要求する。

H.1.4.2.4 相互作用記述

LDAP クライアントは、LDAP を使用して種々の問い合わせおよびカスケード問い合わせをする。LDAP クライアントおよびサーバはアプリケーション構成データモデルを支援しなければならない。

注

多数の LDAP サーバが共通の複製 LDAP データベースへのアクセスを提供するが、これは一般に支援される構成である。これにより、LDAP サーバは、最良の性能およびフォールトトレランスに適切な場所に位置することができる。LDAP サーバのために選ばれた複製規則は、可視データ完全性に影響する。LDAP により、データベースの一貫しない見方が更新中および複製中に可能になる。

H.1.4.3 LDAP サーバを更新する

H.1.4.3.1 適用範囲

RFC2251「軽量ディレクトリアクセスプロトコル (v3)」は、LDAP スキーマに対応するデータベースを更新するメカニズムを指定する。LDAP クライアントは、更新を LDAP 問い合わせ言語で構成でき、そして LDAP サーバは単一のリクエストに対する結果で答える。更新要求はセキュリティの理由から拒絶されるかもしれない。

H.1.4.3.2 ユースケース／役割

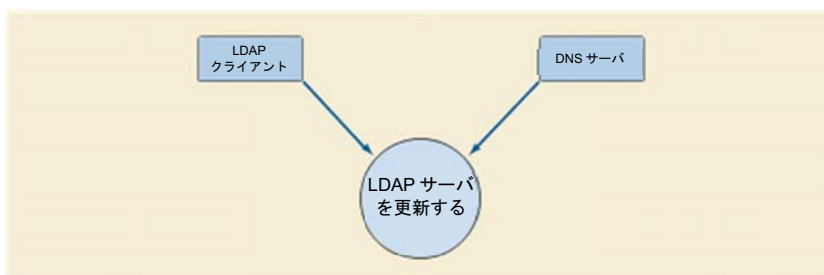


図 H.1-6. LDAP サーバを更新する

LDAP サーバ データベースを維持する。

LDAP クライアント LDAP 情報を更新する。

H.1.4.3.3 参照される標準

RFC2251 軽量ディレクトリアクセスプロトコル (v3)。LDAP 支援は、参照によって起動された他の RFC への適合を要求する。

H.1.4.3.4 相互作用記述

LDAP クライアントは、LDAP データベースを更新するよう要求するかもしれない。LDAP クライアントは、上記のデータモデルを支援しなければならない。LDAP サーバは、セキュリティの理由で更新要求を拒絶することを選択してもよい。LDAP サーバは、更新要求を許可する場合、上記のデータモデルを支援しなければならない。

注

多数の LDAP サーバが共通の複製 LDAP データベースへのアクセスを提供するが、これは一般に支援される構成である。これにより、LDAP サーバは、最良の性能およびフォールトトレランスに適切な場所に位置することができる。LDAP サーバの構成における複製規則の選択が不適当な場合、AE タイトルオブジェクトを作成する時に AE タイトルの一意性が損なわれる。

H.1.4.3.5 ネットワーク AE 生成のための特別更新

新しいネットワーク AE の生成は特別な処置を必要とする。次のステップに従わなければならない：

- a. 暫定の AE タイトルが選択されなければならない。様々なアルゴリズムが可能であり、ランダムな名前の生成、プリセットされた名前テンプレートから始まり、カウンタフィールドをインクリメントすることに及ぶ。クライアントは、このプロセスの一部として現在使用されている名前の完全なリストを得るために一意的 AE タイトル登録簿サブツリーに問い合わせてもよい。
- b. 新しい一意的 AE タイトルオブジェクトは、暫定の名前をもった階層の一意的 AE タイトル登録簿部分の中に作成されなければならない。LDAP サーバは、階層中の特定のポイントで名前の一意性を強制する。
- c. 新しいオブジェクト生成が成功した場合、これは新しいネットワーク AE のために使用される AE タイトルでなければならない。
- d. 新しいオブジェクト生成が非一意的な名前により失敗する場合は、a)に返り、別の名前を選択する。

H.1.4.4 LDAP サーバを維持する

LDAP サーバは、LDAP データベース内容を維持する個別の手動または自動の手段を支援しなければならない。LDAP サーバは、LDAP データベースの更新のために RFC2849 ファイル形式メカニズムを支援しなければならない。LDAP クライアントまたはサービスインストレーションツールは、LDAP サーバデータベースを手動で更新するために RFC2849 フォーマットファイルを提供しなければならない。LDAP サーバは、セキュリティ理由でクライアントネットワーク更新を拒絶してもよい。その場合、保守プロセスは、LDAP データベースを維持するために使用される。

手動の更新手続きが指定される要求事項は次のことだけである、つまり少なくとも RFC2849 からの最小限の LDAP 情報交換ファイル形式が支援されることである。この情報を転送するための正確なメカニズムは、ベンダーおよびサイトに固有である。いくつかの状況、例えば、AE タイトルの生成では、純粋に手動の更新メカニズムの方が交換ファイルより容易かもしれない。

適合性宣言書はこの情報の転送に利用可能なメカニズムを文書化しなければならない。典型的なメカニズムは次のものを含んでいる：

- a. フロッピーディスク
- b. CD-R
- c. SSH
- d. 安全な FTP
- e. FTP
- f. 電子メール
- g. HTTPS

注

1. LDAP データベースを維持するための多くの自動および半自動のツールがある。多くの LDAP サーバが GUI インタフェースおよび更新ツールを提供する。これらのツールの詳細は DICOM の適用範囲の外にある。LDAP RFC2849 は少なくとも最小限のデータ交換能力を要求する。さらにこれらのファイルを作成し維持するための XML に基づいたツールがある。
2. このメカニズムは、個々の機械の更新よりは単一の予め計画されたネットワーク構成の設定により、新しいネットワーク設置の準備に高度に有効かもしれない。

H.1.5 LDAP セキュリティ考察（参考）

H.1.5.1 脅威の評価

LDAP に基づいた構成メカニズムの脅威および価値は、次のカテゴリに分類される：

- a. AE 一意性メカニズム
- b. 発見（および更新）ネットワーク AE 記述
- c. 発見（および更新）装置記述

これらは各々が、攻撃に対し異なる脆弱性を示す。これらは次のとおりである：

- a. 能動的攻撃
 1. AE タイトル一意性メカニズムは、莫大な数の偽の AE タイトルを作成することにより攻撃され得る。これは LDAP サーバに対するサービス拒否（DoS）攻撃であり得る。それは DICOM オペレーションを乱す確率が低い。
 2. ネットワーク AE 情報は悪意をもって更新され得る。これは適切なサーバを見つけることに干渉し DICOM オペレーションに干渉するであろう。それは接続を悪意のあるノードに導く。もっとも TLS 認証を DICOM 接続のために使用すれば、そのような不当な誘導を検知する。TLS 認証が整備されているとき、これは DoS 攻撃になる。
 3. 装置記述は悪意を持って修正され得る。これは適切な装置動作に干渉するであろう。

b. 受動的攻撃

1. AE タイトルの現在のリストを得る際に、攻撃者に明白な値はない。これは、これらの AE タイトルがどこで、またはどんな設備上で展開されるかを示さない。
2. ネットワーク AE 情報および装置記述は、脆弱なシステムの位置の決定において価値があるかもしれない。特定のベンダーからの特定のモデルの設備が、特定の攻撃に弱いことが知られている場合、ネットワーク AE 情報はその設備を見つけるために使用できる。

H.1.5.2 利用可能な LDAP セキュリティメカニズム

LDAP のためのセキュリティメカニズムは、実際の実装において高度に可変である。それらは管理制約とプロトコル実装との混合物である。セキュリティ方法に対する広く利用可能なオプションは次のとおりである：

- a. 匿名のアクセス、これはネットワーク上でこの機能を行うことに対し制約がない場合である。
- b. ベーシック、これはこの機能へアクセスする前にユーザー名とパスワードの交換がある場合である。その交換は覗き見、なりすまし、中間者攻撃に弱い。
- c. TLS、これは接続確立中に SSL/TLS 交換がある場合である。
- d. 手動、これはネットワークアクセスが許されず、機能をサーバで手動で、またはサーバで半自動で行わなければならない場合である。半自動手段により、独立して交換されたファイル（例えば、フロッピー経由）の使用、それと一緒にサーバでの手動コマンドが可能である。

独立して管理されるかもしれない機能のカテゴリは、次のとおりである：

- a. 読取り関連、これは LDAP ディレクトリのツリーの一部を読むか、問い合わせるか、他の方法で得る。
- b. 更新関連、これはディレクトリのツリーの中に以前に存在していたオブジェクトを修正する。
- c. クリエイト、これはディレクトリのツリーに新しいオブジェクトをクリエートする。

最後に、これらの規則は、総合的な LDAP 構造内の異なるサブツリーに対して、異なる方法で適用されるかもしれない。アクセス制御リスト（ACL）、機能的制御などの特別の詳細は、異なる LDAP 実装の間で多少変わる。

H.1.5.3 推奨（参考）

LDAP サーバは、AE タイトルリストに対し、および構成情報の残りに対し、異なる制限を指定できることが望ましい。相互運用性を容易にするため、表 H.1-15 は、アクセス制御に対するいくつかのパターンを定義する。それらはネットワーク環境のためのリスクの異なる査定に対応する。

表 H.1-15. LDAP セキュリティパターン

	TLS	TLS—手動	ベーシック	ベーシック—手動	匿名	匿名—手動
AE タイトルを読む	匿名, TLS	匿名, TLS	匿名, ベーシック	匿名, ベーシック	匿名	匿名
AE タイトルを作成する	TLS	手動	ベーシック	手動	匿名	手動
読取り構成	TLS	TLS	ベーシック	ベーシック	匿名	匿名
更新構成	TLS	手動	ベーシック	手動	匿名	手動
作成構成	TLS	手動	ベーシック	手動	匿名	手動

TLS このパターンが提供するものは、クライアントとサーバとの間の SSL/TLS 認証および暗号化である。それは設置の間に補足設定を必要とする。なぜなら TLS 証明書情報がクライアントマシン上とサーバ上にインストールされる必要が生じるからである。一旦証明書がインストールされたならば、その後クライアントは十分な更新オペレーションを行ってもよい。

TLS—手動 このパターンは情報への読取りアクセスのために SSL/TLS 管理を提供し、更新と生成の機能を行うよう手動の介入に要求する。

ベーシック	このパターンは、LDAP データベースへのアクセスを得るために、LDAP のベーシックなセキュリティを利用する。それはクライアント設定中にパスワードの設置を必要とする。暗号化保護は提供しない。一旦パスワードが設置されていれば、その後、クライアントは更新を行うことができる。
ベーシック-手動	このパターンは、構成情報への読取りアクセスのためのベーシックなセキュリティ保護を利用し、更新と生成の機能を行うことを手動の介入に要求する。
匿名	このパターンは、ネットワーク上のすべての機械への十分な読取り/更新アクセスを許す。
匿名-手動	このパターンは、ネットワーク上のすべての機械への十分な読取りアクセスを許すが、更新と生成を行うことを手動の介入に要求する。

クライアントまたはサーバの実装は、多数のパターンを支援するように構成できる。これは適合主張で文書化されることが望ましい。その後、特定のサイトで使用される特定の構成は、設置時に決定できる。

H.1.6 実装考察（参考）

LDAP データベースは文書化ツールとして使用できる。管理機械および従来機械の構成を両方とも文書化することにより、アップグレードを単純化し、手動で構成される従来設備の誤り率を縮小させる。

LDAP データベース内のルックアップを行うクライアントのための様々な可能な実装戦略がある。例えば、特定 AE への DICOM アソシエーションを始める前に、クライアント実装は次のことができる：

- LDAP データベースに問い合わせる特定の AE タイトルのホスト名とポートを得ることを、DICOM アソシエーションの開始直前に行う。
- AE タイトル、ホスト名およびポート情報のローカルキャッシュを維持し、LDAP データベースに問い合わせることは、特定の AE タイトルがローカルなキャッシュ内に見つからなかった場合だけにする。

ローカルなキャッシュを維持する利点は、パフォーマンス（頻繁なルックアップを回避できるから）および信頼性（LDAP サーバが一時的に利用不可能な場合）の向上などである。キャッシュの不利な点は、時間が経過するにつれて陳腐化することである。クライアント実装は、ローカルに貯えられた情報を除去する適切なメカニズムを提供することが望ましい。

クライアントキャッシュは更新中に混乱を引き起すかもしれない。手動のステップは即時の更新を引き起こすために必要かもしれない。LDAP データベース複製はさらに遅れと矛盾を導入するかもしれない。データベース複製は、更新が直ちに生じるように手動の介入を要求するかもしれない。

クライアントキャッシュ問題をほぼ解消する 1 つの戦略は、ネットワークアソシエーション情報の後に再度新しい DNS および LDAP 情報を再度得ることである。多くの場合、古くなったキャッシュ情報の最初の徴候は、陳腐化した構成情報の使用によるアソシエーション失敗である。

いくつかの LDAP サーバは「DN を修正する」オペレーションを支援しない。例えば、そのようなサーバの装置を改名する場合には、ツリーコピーオペレーションが、新しい名前を使用する新しいオブジェクトツリーを作成するために必要かもしれない。次に古いオブジェクトツリーを除去する。そのような改名の後、装置はそれ自身の構成情報、例えば、装置通し番号を見つける場合、他の属性を使用して探索する必要があるかもしれない。

H.1.7 適合

LDAP クライアントまたは LDAP サーバ実施のための適合性宣言書は、それが支援するセキュリティパターンを指定しなければならない。

H.2 DNS サービス発見

H.2.1 適用範囲

サービス発見メカニズムは、装置がそれらの存在を発表し、かつネットワーク上の他のサービスの存在に関する情報を求める手段を提供する。これらのメカニズムの多くは DNS に基づく。

DNS サービス発見 (DNS-SD)、マルチキャスト DNS (mDNS) および DNS 動的更新のようなプロトコルの正確な使用は、DICOM によって参照された RFC 中に定義されている。このセクションは、DNS SRV 記録の中でそのような目的に使用される名前、および随伴パラメータを符号化する DNS TXT 記録を標準化する。

自己発見に関連したセキュリティ問題は、適用範囲の外にある。DNS セキュリティ問題に関する参考議論については、セクション F.1.1.4 を参照すること。

H.2.2 ユースケース／役割

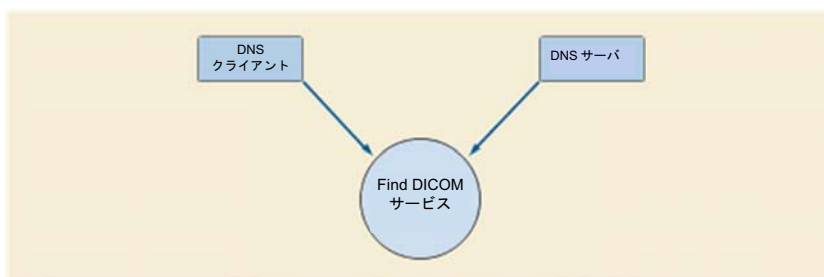


図 H.2-1. Find DICOM サービス

DNS サーバ DICOM アソシエーションアクセプタのリストを提供する。

DNS クライアント DICOM アソシエーションアクセプタのリストを要求する。

H.2.3 参照される標準

RFC2136 DNS 動的更新 <http://tools.ietf.org/html/rfc2136>

RFC2181 DNS 仕様書の解釈 <http://tools.ietf.org/html/rfc2181>

RFC2219 ネットワークサービスのための DNS エイリアスの使用 <http://tools.ietf.org/html/rfc2219>

RFC2782 サービスのロケーションを指定する DNS RR (DNS SRV) <http://tools.ietf.org/html/rfc2782>

RFC6762 マルチキャスト DNS <http://tools.ietf.org/html/rfc6762>

RFC6763 DNS ベースのサービス発見 <http://tools.ietf.org/html/rfc6763>

DNS 自己発見 <http://www.dns-sd.org/>

DICOM アソシエーションアクセプタを広告するために DNS SRV の中で使用される名前は、支援された SOP クラスにかかわらず、次のとおりでなければならない。

- 「dicom」、不安全な DICOM 通信用
- 「dicom-tls」、ベーシックな TLS の安全なトランスポート接続プロファイル用
- 「dicom-iscl」、ISCL トランスポート接続プロファイル用
- 「dicomweb」、セキュアでない http での DICOM ウェブサービス用
- 「dicomweb-tls」、https での DICOM ウェブサービス用

注

これらの選択は、サービスへの IP ポートの写像を定義するために IANA で登録された名前と一致している。それはこの用法には伝統的なものである。選択「dicom」が「acr-nema」代案ではなく使用されるのは、明瞭さのためである。DNS SRV サービスタイプにおける使用法による黙示のポート選択はない、なぜならポートが明示的に伝えられるからである。

DNS TXT 記録は次のパラメータを含んでいるかもしれない：

- AET=<アプリケーションエンティティタイトル>, ここでは値<アプリケーションエンティティタイトル>がコールドアプリケーションエンティティタイトルとして使用され、それは装置へのアソシエーションを始める場合である。

- PrimaryDeviceType=<主要な装置タイプ>, ここでは値<主要な装置タイプ>は, 表 H.1-2「装置オブジェクトの属性」で定義されたとおりである。
- DICOMWebPath= <サービス>, ここでは値 <サービス>は PS3.18 に定義されたとおり DICOM ウェブサービスのルートパスを構成する要素である。

DNS TXT 記録, DNS TXT 記録の AET パラメータが存在しない場合, インスタンス名であって DICOM サービス発見に使用される DNS SRV 記録中のサービスタイプに先行するものは, AET でなければならない。

注

さらなるパラメータは指定されない, 例えば, 支援された SOP クラスまたは他の情報を示すパラメータである。なぜなら UDP データグラムとして符号化された DNS 記録のサイズが, 厳密に制限されているからである。また, さらに, 計画されたマルチキャスト使用法は, 必要最小限の情報の交換を奨励している。既存の DICOM アソシエーション交渉メカニズムは, 提示された SOP クラスを調査するために使用できる。これは一旦 IP アドレス, ポート番号および AET が既知の場合である。主要な装置タイプが供給される。なぜならユーザーに装置のタイプを示すことが有用であり, それはアソシエーションの確立中には伝えられないからである。

H.2.4 例

DNS SRV 記録例 :

- _dicomweb-tls._tcp.examplehospital.org 86400 IN SRV 10 60 443 dicomweb.examplehospital.org.

TXT 記録例 :

- dicomweb.examplehospital.org IN TXT "DICOMWebPath=apps/dicom-rs"

上記の例は結合して以下の DICOM ウェブサービスへのルートを定義する :

- https://dicomweb.examplehospital.org:443/apps/dicom-rs

