

PS 3 . 1 5 - 2 0 0 1 翻訳  
医療におけるデジタル画像と通信 ( D I C O M )  
巻 1 5 : セキュリティプロファイル

PS 3.15-2001  
Digital Imaging and Communications in Medicine (DICOM)  
Part 15: Security Profiles

Published by

National Electrical Manufacturers Association

1300 N. 17th Street

Rosslyn, Virginia 22209 USA

© Copyright 2000 by the National Electrical Manufacturers Association. All rights including translation into other languages, reserved under the Universal Copyright Convention, the Berne Convention or the Protection of Literacy and Artistic Works, and the International and Pan American Copyright Conventions.

## 解説

この文書は、DICOM Committee が作成し、NEMA が発行した下記の規格を検討用として翻訳したものである。

PS 3.15-2001

Digital Imaging and Communications in Medicine (DICOM)

Part 15: Security Profiles

File name: 01\_15dr.pdf

翻訳 繁村 直

翻訳登録： 2002.9.8

ファイル名 P15j0129.doc

|                            |          |            |
|----------------------------|----------|------------|
| access control             | アクセス制御   | JIS X 5004 |
| audit trail                | 監査証跡     | JIS X 5004 |
| authentication             | 認証       | JIS X 5004 |
| authorization              | 許可       | JIS X 5004 |
| certificate                | 証明書      | JIS X 5004 |
| channel                    | 通信路      | JIS X 5004 |
| confidentiality            | 機密性      | JIS X 5004 |
| data origin authentication | データ発信元認証 | JIS X 5004 |
| encryption                 | 暗号化      | JIS X 5004 |
| integrity                  | 完全性      | JIS X 5004 |
| key                        | かぎ       | JIS X 5004 |
| policy                     | 方針       | JIS X 5004 |
| Privacy                    | プライバシー   | JIS X 5004 |
| security policy            | 安全保護方針   | JIS X 5004 |
| tampering                  | 改ざん      |            |

## 目次

|  |     |
|--|-----|
| 目次.....                                    | iii |
| まえがき.....                                  | 1   |
| 1 適用範囲と適用分野.....                           | 2   |
| 2 引用規格.....                                | 3   |
| 3 定義.....                                  | 4   |
| 3.1 参照モデル定義.....                           | 4   |
| 3.2 参照モデルセキュリティアーキテクチャー定義.....             | 4   |
| 3.4 セキュリティ定義.....                          | 4   |
| 3.5 DICOM序文と概要定義.....                      | 5   |
| 3.6 DICOM適合性定義.....                        | 5   |
| 3.7 DICOM情報オブジェクト定義.....                   | 5   |
| 3.8 DICOMサービスクラス定義.....                    | 5   |
| 3.9 DICOM通信サポート定義.....                     | 5   |
| 3.10 DICOMセキュリティプロファイル定義.....              | 5   |
| 4 記号と省略形.....                              | 6   |
| 5 規約.....                                  | 7   |
| 6 セキュアプロファイルの概要.....                       | 7   |
| 6.1 セキュア使用プロファイル.....                      | 7   |
| 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.....           | 7   |
| 6.3 デジタル署名プロファイル.....                      | 7   |
| 6.4 媒体保存セキュリティプロファイル.....                  | 8   |
| 付属書A セキュア使用プロファイル(規格).....                 | 9   |
| A.1 オンライン電子保存セキュア使用プロファイル.....             | 9   |
| A.1.1 SOPインスタンス状態.....                     | 9   |
| A.2 基本デジタル署名セキュア使用プロファイル.....              | 11  |
| 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.....           | 11  |
| 付属書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).....      | 13  |
| 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.....      | 13  |
| 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.....       | 14  |
| 付属書C デジタル署名プロファイル(規格).....                 | 15  |
| C.1 基本RSAデジタル署名プロファイル.....                 | 15  |
| C.2 生成者RSAデジタル署名プロファイル.....                | 15  |
| C.3 許可RSAデジタル署名プロファイル.....                 | 16  |
| 付属書D 媒体保存セキュリティプロファイル(規格).....             | 17  |
| D.1 基本DICOM媒体セキュリティプロファイル.....             | 17  |
| 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..... | 17  |
| 索引.....                                    | 18  |

## まえがき

A C R (American College of Radiology) と N E M A (National Electrical Manufacturers Association) は、医療におけるデジタル画像と通信 ( D I C O M ) のための規格を開発するために合同委員会を組織した。この D I C O M 規格は、N E M A の手続きに従って開発された。

この規格は、欧州の C E N T C 2 5 1 として日本の J I R A を含む他の標準化組織との連絡の中で、また米国の I E E E , H L 7 , として A N S I を含む他の組織による論評を得て、開発された。

D I C O M 規格は、次の文書の中で確立された指針を用いて、複数の巻の文書として構成される。

— ISO/IEC Directives, 1989 Part 3: Drafting and Presentation of International Standards.

この文書は、次の巻から構成される D I C O M 規格の一つの巻である。

- P S 3 . 1 : 序文と概要
- P S 3 . 2 : 適合性
- P S 3 . 3 : 情報オブジェクト定義
- P S 3 . 4 : サービスクラス仕様
- P S 3 . 5 : データ構造と符号化
- P S 3 . 6 : データ辞書
- P S 3 . 7 : メッセージ交換
- P S 3 . 8 : メッセージ交換のためのネットワーク通信支援
- P S 3 . 9 : メッセージ交換のための 2 点間通信支援
- P S 3 . 1 0 : 媒体保存とファイルフォーマット
- P S 3 . 1 1 : 媒体保存応用プロファイル
- P S 3 . 1 2 : 媒体相互交換のための媒体フォーマットと物理媒体
- P S 3 . 1 3 : プリント管理二点間通信サポート
- P S 3 . 1 4 : グレースケール標準表示関数
- P S 3 . 1 5 : セキュリティプロファイル
- P S 3 . 1 6 : 内容マッピング資源

これらの巻は、関係したしかし独立した文書である。それらの開発レベルおよび承認状態は異なることがある。追加の巻が、この複数の巻の規格に加えられることがある。P S 3 . 1 はこの規格の現在の巻の基本参照文献として使用される。

## 1 適用範囲と適用分野

D I C O M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プロファイルを明記する。適切なセキュリティ方針への忠実な支持はセキュリティの任意の水準で明らかに必要であるが、D I C O M規格はセキュリティ方針の問題に取り組まない。規格は、応用エンティティ間のD I C O M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することができる機構を単に提供する。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、D I C O M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機構を含んでいるが、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安全な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D I C O M経由で情報を相互交換することに合意する場合、彼らは本質的に、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、彼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あるいは変造を検知するための、あるいは、通信チャンネルを横断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機構を提供する。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、自由にこれらの機構の何れかを利用することができる。

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あるい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、あるいは、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に注意すること。応用エンティティがD I C O M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、あるいは監査証跡を生成する際に、局所あるい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、あるい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持っているとして仮定する。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。この時に、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えない、それは将来の何時かでの考慮する題目であることがあるけれども。

さらにこの規格は、T L S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 . 5 0 9 かり証明書にセキュアアクセスを持つ、あるいは安全に得ることができると仮定する。さらにこの規格は、応用エンティティが、それが受信するX . 5 0 9 証明書を有効にする手段を持っていると仮定する。確認機構は局所的に管理された事務局、公に利用可能な事務局あるい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、I S C L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機構（例えばスマートカード）にアクセスすると仮定する。そのような鍵管理と配布機構の性質と使用は、特定現場で使用されるセキュリティ方針の一部であることがあるけれども、D I C O Mの適用範囲外である。

## 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んでいる。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。

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 Directives, 1989 Part 3 - Drafting and Presentation of International Standards

ISO/IEC 10118-1:1998 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、<ftp://ftp.esat.kuleuven.ac.be/pub/bosselaer/ripemd>で同様に入手可能である。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る、そして1993と2000、二組の補正を含めて2001に改訂された。ITU-Tは、以前はCCITTとして知られていた。

RFC 2246, 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。

RFC-2313 PKCS #1: RSA Encryption, Version 1.5, March 1998.

RFC 2437 PKCS #1 RSA Cryptography Specifications Version 2.0

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

RFC-2630 Cryptographic Message Syntax, June 1999

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

### 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ー定義

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、あるいは処理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生成および保存、配布、削除、保管、応用」である。
- e. デジタル署名 Digital Signature  
注：定義は、「データ単位の受取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、例えば受取人によって、データ単位に追加されたデータ、あるい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 の中で定義される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 の中で定義される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あるい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，P S 3 . 1 の中で定義される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，P S 3 . 2 の中で定義される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，P S 3 . 3 の中で定義される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，P S 3 . 4 の中で定義される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 ( S O P ) 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，P S 3 . 8 の中で定義される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んでいる。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。

|                  |  |
|------------------|--|
| <b>ACR</b>       | American College of Radiology  |
| <b>AE</b>        | Application Entity   |
| <b>ANSI</b>      | American National Standards Institute  |
| <b>CEN TC251</b> | Comite European de Normalisation-Technical Committee 251-Medical Informatics |
| <b>CBC</b>       | Cipher Block Chaining  |
| <b>CCIR</b>      | Consultative Committee, International Radio                                  |
| <b>DES</b>       | Data Encryption Standard   |
| <b>DICOM</b>     | Digital Imaging and Communications in Medicine                               |
| <b>ECMA</b>      | European Computer Manufacturers Association                                  |
| <b>EDE</b>       | Encrypt-Decrypt-Encrypt  |
| <b>HL7</b>       | Health Level 7   |
| <b>IEEE</b>      | Institute of Electrical and Electronics Engineers                            |
| <b>IEC</b>       | International Electrical Commission  |
| <b>IOD</b>       | Information Object Definition  |
| <b>ISCL</b>      | Integrated Secure Communication Layer  |
| <b>ISO</b>       | International Standards Organization   |
| <b>JIRA</b>      | Japan Industries association of RAdiological systems                         |
| <b>MAC</b>       | Message Authentication Code  |
| <b>MD-5</b>      | Message Digest - 5   |
| <b>MEDIS-DC</b>  | Medical Information System Development Center                                |
| <b>NEMA</b>      | National Electrical Manufacturers Association                                |
| <b>PDU</b>       | Protocol Data Unit   |
| <b>RSA</b>       | Rivest-Shamir-Adleman  |
| <b>SCP</b>       | Service Class Provider   |
| <b>SCU</b>       | Service Class User   |
| <b>SHA</b>       | Secure Hash Algorithm  |
| <b>SOP</b>       | Service-Object Pair  |
| <b>SSL</b>       | Secure Sockets Layer   |
| <b>TLS</b>       | Transport Layer Security   |
| <b>UID</b>       | Unique Identifier  |

## 5 規約

節3 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 セキュアプロファイルの概要

実装は、セキュリティプロファイルのどれでもへの適合を個々に主張することがある。さらにそれは、一より多くのセキュリティ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、一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

実装は一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機構の記述
- 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機構
  - 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機構の記述
  - 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タ
- d. 実装がサポートする完全性検査機構の記述

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、一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あるい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、デジタル署名を生成するか確認するために使用される機構：
  - 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機構。
  - 4 . 証明されたタイムスタンプタイプ (0400,305) および証明されたタイムスタンプ (0400,310) 属性のためのすべての必要条件。
- d . 署名者を識別するためのすべての特別の必要条件。
- 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、一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、一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 D I C O M ファイルのタイプへの制限。
- c . D I C O M 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。

## 付属書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：
    - a) SOPクラスUID(0008,0016)およびSOPインスタンスUID(0008,0018)
    - b) 知られている場合には、インスタンス生成日付(0008,0012)およびインスタンス生成時刻(0008,0013)
    - c) SOPインスタンス状態(0100,0410)
    - d) SOP許可日時(0100,0420)
    - e) ある場合は、SOP許可コメント(0100,0424)
    - f) 許可装置証明番号(0100,0426)
    - g) 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)
    - h) 知られている一般装置モジュールの任意の属性
    - i) 存在する任意のオーバーレイデータ
    - j) 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S O P 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S O P 許可コメント (0100,0424) 属性を加えることがある。
- c. S O P インスタンス状態がオリジナル ( O R ) か、オーソライズドオリジナル ( A O ) である場合、S O P インスタンスを保持する一つの応用エンティティだけがある。そのようなS O P 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、S O P インスタンス状態がオリジナルか ( O R ) 、オーソライズドオリジナル ( A O ) である場合、S O P 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に同様に適合する別の応用エンティティにそのS O P 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. 転送に関与する二つの応用エンティティは互いを確証する、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S O P 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S O P 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S O P インスタンスまたはS O P 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S O P 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、S O P インスタンスのその局所コピーに下記の一つを行う：
    - a) S O P インスタンスを削除する、
    - b) 無指定 ( N S ) にS O P インスタンス状態を変更する、
    - c) S O P インスタンス状態がオーソライズドオリジナル ( A O ) だった場合は、オーソライズドコピー ( A C ) にS O P 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、S O P インスタンス状態がオーソライズドオリジナル ( A O ) あるいはオーソライズドコピー ( A C ) であるS O P 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S O P 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. 転送に関与する二つの応用エンティティは互いを認証する、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、S O P インスタンス状態を無指定 ( N S ) あるいはオーソライズドコピー ( A C ) にセットする。S O P インスタンスU I D 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S O P 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、あるい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には、
  - 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、あるい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あるい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、あるい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) にセットする。
- 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 インスタンスを格納する、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、あるいは前述の変更に伴うグループ長さ属性への変更より他は、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生成する実装は、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. 可能な場合にはどこでも、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一以上の新しいデジタル署名を生成する。

## 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 インスタンスを格納し転送する実装は、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いかなる実装もデジタル署名を扱うときに下記の規則に従う：

- 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インスタンスを格納する。

- 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。

## 付属書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T L S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T L S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機構を利用する。表B.1-1は、T L S内の対応する機能が応用エンティティによってサポートされる場合、サポートされる機構を指定する。そのプロファイルは、T L Sの機能（エンティティ認証、暗号化、完全性検査）のすべてをサポートすることは実装に要求しない。T L S通信路の確立の間に折衝によって同意される場合は、他の機構が使用されることがある。

表B.1-1 T L S機能のための最小機構

| サポートするT L S機能                           | 最小機構                   |
|---|------------------------|
| 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T L S接続を受諾するI Pポート、あるいはこのポート番号が選択されるか構成される機構は、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：基本T L S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T L S上のD I C O M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機構を示す。

プロファイルは、T L Sセキュアトランスポートコネクションを確立する方法、あるいは、同位エンティティ認証の間に交換された任意の証明書の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。証明書所有者の同一性は、監査ログサポートのために、あるいは何らかの外部アクセス権制御フレームワークに基づいてアクセスを制限するために、応用エンティティが使用することができる。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には、上位層アソシエーションはそのセキュア通信路を使用することができる。

注：トランスポートの効率に影響を与えるP D UサイズとT L Sレコードサイズの間には相互作用があることがある。許される最大T L Sレコードサイズは、許される最大P D U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 - A B O R T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T L S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機構を利用する。応用エンティティは、表B.2-1の中で指定された機構を選択するためにISCLを使用する。応用エンティティは、最小として、エンティティ認証機構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機構を使用することがある。

表B.2-1 ISCL機能のための最小機構

| サポートするISCL機能                   | 最小機構  |
|--------------------------------|---|
| 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、あるいは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健全性検査を実行することができる。

実装がISCL接続を受諾するIPポート、あるいはこのポート番号が選択されるか構成される機構は、適合性宣言の中で指定される。このポートは、他のタイプの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機構を示す。

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せられる。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には、上位層アソシエーションはそのセキュア通信路を使用することができる。

注：トランスポートの効率に影響を与えるPDUサイズとISCLレコードサイズの間に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。

## 付属書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、デジタル署名を生成するために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べきかの仕様あるい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キーを使用して暗号化されるMACを生成するためにRIPEMD-160、MD5、SHA-1ハッシュ関数の一つを使用する。デジタル署名の確認者は、指定された三種類のハッシュ関数（RIPEMD-160、MD5、SHA-1）のいずれによって生成されたMACも使用することができる。

注： MD5の使用はその発明者、RSAによって推奨されない。下記を参照：

<ftp://ftp.rsasecurity.com/pub/pdfs/bulletn4.pdf>

RFC 2437 (PKCS#1) の中で指示されるように、署名されるMACは、RSAキー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」あるいは「MD5」、「SHA1」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）と同様に秘密鍵に関連した公開鍵は、X.509 (1993) 署名証明書の中で送信される。証明書タイプ (0400,0110) 属性の値は「X509\_1993\_SIG」にセットされる。X.509証明書が生成され、確認され、配布される方法は、サイト特定の方針が決定する。サイトはX.509証明書を直接発行し配布することがある、あるいは認証機関のサービスを利用することがあるが、証明書生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生成される。

### C.2 生成者RSAデジタル署名プロファイル

DICOM SOPインスタンスの生成者は、生成者RSAデジタル署名プロファイルを使用して、署名を生成することがある。このプロファイルによって生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生成以来変更されていないことを確認するために使用することができる、生涯データ保全性チェックとして、貢献する。生成者RSAデジタル署名プロファイルを支援する実装は、それが作成するすべてのSOPインスタンスで生成者RSAデジタル署名を含んでいることがある；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、実装は生成者RSAデジタル署名を生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あるいはカーブ、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文書一般およびSR文書内容モジュールあらゆる属性
- h . 存在する波形および波形注釈モジュールのあらゆる属性

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、生成者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鍵は、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。

生成者RSAデジタル署名は、他のデジタル署名との直接の関係を持たない。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、生成者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 許可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、許可RSAデジタル署名プロファイルを使用して署名を生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することができる、生涯データ保全性チェックとして役立つ。

最低、実装は許可RSAデジタル署名を生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 . そ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あるいはカーブ、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あらゆる属性
- g . 存在する波形および波形注釈モジュールのあらゆる属性

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あるい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同一性を決定し、彼らの証明書を取得する。

許可RSAデジタル署名は、他のデジタル署名との直接の関係を持たない。しかしながら、生成者デジタル署名のような他のデジタル署名は、許可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。

## 付属書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、内容暗号化用の Triple-DES，および Triple-DES 内容暗号化かぎのかぎ移送のための RSA の使用を明示する。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 を使用し，署名アルゴリズムとして RSA を使用して，一つ以上のデジタル署名で署名される DICOM ファイル，あるいは
- デジタル署名の適用なしで，ダイジェストアルゴリズムとして SHA-1 でダイジェストされる DICOM ファイル。

#### 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、RFC 2630 に定義された暗号メッセージ構文の Enveloped-data content type を含む。包まれたデータは、Triple-DES 内容暗号鍵の鍵の移送に、RSA[RFC 2313]を使用する。Triple-DES キーの長さは、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、RFC-2630 の中の RSA かぎ移送のための仕様に従って行なわれる。

Enveloped-data content type の暗号化された内容は、下記の選択である：

- 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]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には、署名アルゴリズムとして RSA[RFC 2313]が使用される。

- 注： 1．Triple-DES 内容暗号化かぎの RSA かぎ移送は、欧州予備標準 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あるいは制限は、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。

## 索引

|                  |        |
|------------------|--------|
| (0008,0012)..... | 10     |
| (0008,0013)..... | 10     |
| (0008,0016)..... | 10     |
| (0008,0018)..... | 10     |
| (0020,000D)..... | 10     |
| (0020,000E)..... | 10     |
| (0100,0410)..... | 10     |
| (0100,0420)..... | 10, 11 |
| (0100,0424)..... | 10, 11 |
| (0100,0426)..... | 10, 11 |