○医療情報セキュリティに関連してJAHIS セキュリティ委員会が発行している JAHIS 標準類一覧
(2021年 3 月現在)

各関連 JAHIS 標準類に関して以下の項目をまとめている。

1. タイトル:
2. 発行年月:
3. 種別:JAHIS 標準か JAHIS 技術文書
4. 概要:
5. 目的:
6. 他の JAHIS 標準類との関係:
7. 国のガイドライン等のレギュレーションとの関係:
8. 国際標準化団体等の標準類との関係:
9. 国内標準化団体や関連団体との関係:
10. 管轄 WG:
11. 改訂などの計画:

文書一覧(目次)

1. タイトル：
13-009　JAHISヘルスケア分野における監査証跡のメッセージ標準規約 Ver.2.0
2.発行年月：2014年3月
3.種別：JAHIS標準

4.概要：
個人情報保護法、医療－介護関係事業者における個人情報の適切な取り扱いのためのガイドラインおよび医療情報システムの安全管理に関するガイドラインに対応した監査証跡の取り扱いについて、最低限の要件とメッセージ内容を規定した標準規約である。DICOM PS3.15 Security and System Management Profiles A.5. Audit Trail Message Format Profile および ISO 27789 Audit Trail for EHR との 整合性がとられている。

5.目的：
本規約においては監査証跡のうち「医療情報システムに関する安全管理のガイドライン」において求められている業務アプリケーションの監査ログのログメッセージ規約を策定している。本規約において 規定する監査ログは以下の目的で利用されることを想定している。
(1) 個人情報へのアクセス履歴の確認
(2) 医療機関が説明責任を果たすために利用
(3) 副次的効果としての目的外アクセスの抑止
(4) 情報システムのセキュリティ監査

6.他の JAHIS標準類との関係：
「17-008　JAHIS保存が義務付けられた診療録等の電子保存ガイドライン Ver.3.3」、
「17-107　JAHIS IHE-ITIを用いた医療情報連携基盤実装ガイド本編 Ver.3.1」で参照されている。

7.国のガイドライン等のレギュレーションとの関係：
本規格は「医療情報システムの安全管理に関するガイドライン」の要求事項を踏まえた記載となって いる。

8.国際標準化団体等の標準類との関係：
ISOで策定された監査証跡の規格と整合性を取るものであり、DICOM規格との互換性もある。
－IS27789:2013 Audit Trail for EHR
－DICOM PS 3.15 Security and System Management Profiles、PS 3.16 Content Mapping Resource

9.国内標準化団体や関連団体との関係：
特になし

10.管轄WG：
監査証跡WG

11.改訂などの計画：
本編の改訂中である。

1.タイトル：
　14-005　JAHIS HPKI 電子認証ガイドライン V1.1
2.発行年月：2014 年 9 月
3.種別：JAHIS 標準

4.概要：
電子認証の互換性の確保、及びなりすまし防止のために、認証に求められる署名の生成、検証及び証明書検証において最低限行わねばならないことについて明確に定める。
また検証では医療分野特有の検証要件として、HPKIのポリシへの準拠性を確認できることが必要であることを明確に定める。これにより証明書内に記載された国家資格等の識別を活用することができる。ユースケースを想定し、ユースケースに応じた利用方法を提示する。
認証のフレームワークについての規定は行わないが、一般的な利用方法として想定される、SSL クライアント認証ならびに独自のクライアント機能による認証を例にした実装要件を提示する。

5.目的：
認証用HPKI を利用することで、相互運用性の確保、国家資格等の属性認証、外部の医療認証基盤システムの利用などを可能にするためのガイドラインを示す。
システム構築ベンダーにとって参考となるユースケースを示し、実装の一助とする。

6.他の JAHIS 標準類との関係： 本規格は独立した標準類である。
関連規格として「18-001　JAHIS HPKI対応ICカードガイドラインVer.3.0」がある。

7.国のガイドライン等のレギュレーションとの関係：
医療情報システムの安全管理に関するガイドラインの6.5章の認証を HPKI で行う際の要件を記載している

8国際標準化団体等の標準類との関係：
ISO17090-5　策定の際のベースの規格となっている。

9.国内標準化団体や関連団体との関係：
規格策定に当たり、日本医師会との意見交換を実施し、日医認証サービスとの整合を取っている。

10.管轄 WG：
HPKI 電子署名規格作成 WG

11.改訂などの計画：
現在改定の計画はない。

1. タイトル：
　16-003　リモートサービスセキュリティガイドラインVer.3.0
2. 発行年月：2016年06月
3. 種別：JAHIS標準

4. 概要：
リモートサービスとは、医療機関内の機器やシステムと保守ベンダとをネットワークで結び、定期的な保守管理サービスを遠隔で行うことをいう。このリモートサービスにより、機器やシステムの故障時における障害発生から復旧までのダウンタイム短縮など、より円滑な運用が可能となる。
情報セキュリティの視点からこのリモートサービスを安全に行うために、その一つの手段として情報セキュリティマネジメント（以下、ISMS）という考え方を選択することで、情報セキュリティに関するリスクを最小限に抑えるためのコントロールを示すことができる。本ガイドラインは、新規にリモートサービスを設計する際や、現状のリモートサービスを再度検討いただくために活用されたい。

5. 目的：
リモートサービスへのISMSの適用には詳細なリスク評価とリスクコントロールが必要となり、実際のサービスインまでに莫大な労力と時間が要求される。そのため、本JAHIS標準では代表的なリモートサービスのモデルにより分析を行っており、それぞれの脅威に対する代表的な対策を示している。リモートサービスにおいて情報セキュリティ対策の見直し、あるいはISMSを構築する際に活用されることを期待している。リモートサービスを既に実施している保守ベンダや、新規にリモートサービスを設計する方々を主な対象としている。

6. 他のJAHIS標準類との関係：
リモートサービスを題材にして、ISMSの構築手順や、脅威や脆弱性に対するリスクアセスメントの手法を提示している。
17-008　JAHIS保存が義務付けられた診療録等の電子保存ガイドラインVer.3.3
18-004　JAHISシングルサインオンにおけるセキュリティガイドラインVer.2.0

7. 国のガイドライン等のレギュレーションとの関係：
・厚生労働省「医療情報システムの安全管理に関するガイドライン」の
「6.8章　情報システムの改造と保守」に該当する項目

8. 国際標準化団体等の標準類との関係：
・日本規格協会　JIS Q 27001:2014(ISO/IEC 27001:2013) 情報技術－セキュリティ技術－
情報セキュリティマネジメントシステム－要求事項
・日本規格協会　JIS Q 27002:2014(ISO/IEC 27002:2013) 情報技術－セキュリティ技術－
情報セキュリティマネジメントの実践のための規範
・文書の記述から日本固有の法令、制度等に係る部分を取り除き、「ISO TS 11633 Health informatics － The Information security management for remote maintenance of medical devices and medical information systems Part 1」および「ISO TR 11633 Health informatics － The Information security management for remote maintenance of medical devices and medical information systems Part 2」として国際標準となった。

9. 国内標準化団体や関連団体との関係：
・JIRAと合同WGとして運用している。本規格はJIRAの標準文書であるJESRAとしても出版されている。

10. 管轄WG：

医療システム部会　セキュリティ委員会　JAHIS-JIRA合同リモートサービスセキュリティ作成WG

11. 改訂などの計画:
参照しているJIS Q 27001および27002の改訂に合わせ、本JAHIS標準の改訂を実施する。

1.タイトル：
20-005　JAHIS「製造業者/サービス事業者による医療情報セキュリティ開示書」ガイド　Ver.4.0
2.発行年月：2021年3月
3.種別：JAHIS標準

4.概要：
各製造業者/サービス事業者の医療情報システムのセキュリティ機能に関する説明のための標準書式がなく、その記載レベルも一様ではなかった。この状況は、医療機関等側にとって各システム/サービス間の整合性を取る際の支障であり、製造業者/サービス事業者にとっても各医療機関で独自に策定した書式に対応することもまた、業務の効率化の妨げとなっていた。
そこで、日本での標準となるよう製品/サービスのセキュリティに関する書式を作成し、その書式に関して説明したものが本ガイドである。

5.目的：
対象読者は医療機関等に医療情報システムを提供する製造業者/サービス事業者。
本ガイドの使用は強制されるものではないが、厚生労働省「医療情報システムの安全管理に関するガイドライン」第5.1版への適合性を説明する標準ツールとなることを期待する。

6.他のJAHIS標準類との関係：
17-008 JAHIS保存が義務付けられた診療録等の電子保存ガイドラインVer.3.3
16-003 リモートサービスセキュリティガイドラインVer.3.0

7.国のガイドライン等のレギュレーションとの関係：
厚生労働省「医療情報システムの安全管理に関するガイドライン」：6～9章
6.2章で、情報のリストアップやリスク分析及び対策において本ガイドのチェックリストが参考になると紹介されている。

8.国際標準化団体等の標準類との関係：
MDS2は根幹となる部分が米国HIPAA法ではあるが、概念的にはMDS2が元となった。
MDS2とはHIMSS/NEMAにより策定された米国における医療情報システムのチェックリスト。
正式名称：Manufacturer Disclosure Statement for Medical Device Security

9.国内標準化団体や関連団体との関係：
JIRAと合同WGとして運用している。本規格はJIRAの標準文書であるJESRAとしても出版される。
Ver.4.0では、サービス事業者も対象に加えたためASPIC、JEITAからオブザーバとして参画していただいた。

10.管轄WG：
JAHIS-JIRA合同開示説明書WG（MDS-WG）

11.改訂などの計画：
Q&A集に関しては必要に応じて随時更新を行う。
医療機関等向けの「ユーザーズガイド」の発行。

1.タイトル：
17-008　JAHIS保存が義務付けられた診療録等の電子保存ガイドライン　Ver.3.3
　　厚生労働省「医療情報システムの安全管理に関するガイドライン　第5版」対応
2.発行年月：2017年12月
3.種別：JAHIS標準

4.概要：
診療録等の電子保存を推進するガイドラインとして、厚生労働省の「医療情報システムの安全管理に　関するガイドライン」、総務省の「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン」及び、経済産業省の「医療情報を受託管理する情報処理事業者向けガイドライン」が発行されている。
これに対して、各ベンダが自社のシステムに実装する立場から、各ガイドラインに示されている要件を技術的な対策と運用的な対策に整理し、より細かく具体的に示している。

5.目的：
本ガイドラインは、システムにどの機能を実装することが望ましいかをJAHISの立場から具体的に示し、各ベンダがどのような仕様で開発したらよいか考える基準を示すことを目標とした。

6.他のJAHIS標準類との関係：
下記の標準と対象項目が重なる部分が有り、内容の確認を相互に行なっている
17-006 JAHIS「製造業者による医療情報セキュリティ開示書」ガイド Ver3.0a
16-003 JAHISリモートサービスセキュリティガイドライン Ver.3.0

7.国のガイドライン等のレギュレーションとの関係：
本標準は以下の3省ガイドラインを補完するガイドラインである。
・厚生労働省
医療情報システムの安全管理に関するガイドライン 第5版 2017年5月
・経済産業省
　医療情報を受託管理する情報処理事業者向けガイドライン 第2版 2012年10月
・総務省
　クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン(第1版) 2018年7月

8.国際標準化団体等の標準類との関係：
特に無し

9.国内標準化団体や関連団体との関係：
特に無し

10.管轄WG：
電子保存WG

11.改訂などの計画：
総務省・経済産業省のガイドライン統合（2020年8月に第1版発行）と厚生労働省のガイドライン改定（2021年1月に第5.1版発行）が行われたため、本ガイドラインの改定対応中である。（改定Aの承認番号：20-008）

1. タイトル:
18-001 JAHIS HPKI 対応 IC カードガイドライン Ver 3.0
2. 発行年月:2018 年 5 月
3. 種別:JAHIS 標準

4.概要:
電子署名および電子認証を目的とした HPKI で使用される IC カード、及び IC カードの利用環境に対する要求事項を定めている。
- IC カード機能・仕様
- IC カードのセキュリティ要件
- IC カードを利用する端末の機能
- IC カードを利用する端末のセキュリティ要件
- 相互運用性を確保するための IC カード内の PKI アプリケーションの仕様
- 相互運用性を確保するための IC カードを利用する際のインタフェースの仕様

電子署名用の要件及び仕様に関しては第1版、電子認証の要件及び仕様に関しては第 2 版で定めている。

5. 目的:
保健医療福祉分野において導入されている HPKI は、複数の事業者が認証サービスを提供する可能性がある。HPKI で重要となる秘密鍵や公開鍵を含むクレデンシャルは IC カード等の安全な媒体に格納して利用することとなるが、事業者毎に格納する IC カードの仕様が異なっていると利用するソフトウェアやシステムに支障をきたす恐れがある。本標準は、異なる仕様の IC カードが混在することで生ずる混乱を防ぐために、異なる事業者が発行した HPKI 対応の IC カードでの相互運用性を確保するための仕様を定めたものである。主たるターゲットは HPKI 認証事業者、PKI ライブラリの開発を行うベンダーであるが、PKI ライブラリを利用するシステムベンダーにも有用である。

6. 他の JAHIS 標準類との係:
本規格は、08-002 HPKI 対応 IC カードガイドライン及び 10-002 HPKI 対応 IC カードガイドライン 第 2 版を合わせて改定したもので、独立した標準類である。関連規格として
18-006 JAHIS ヘルスケア PKI を利用した医療文書に対する電子署名規格 Ver.2.0
14-005 JAHIS HPKI 電子認証ガイドライン V1.1
がある。

7. 国のガイドライン等のレギュレーションとの関係:
本ガイドラインは、次の保健医療福祉分野PKI認証局に準拠するためのポリシの「6.2 私有鍵の保護及び暗号モジュール技術の管理」の要件を踏まえた記載となっている。
－保健医療福祉分野PKI認証局署名用証明書ポリシ 1.6版(令和 2 年 12月)
－保健医療福祉分野PKI認証局認証用(人)証明書ポリシ 1.5版(令和 2 年 12 月)
－保健医療福祉分野PKI認証局認証用(組織)証明書ポリシ 1.1版(平成 22 年 3 月)

8. 国際標準化団体等の標準類との関係:
以下の JIS を参照している。
JIS X 19790:2015 セキュリティ技術 － 暗号モジュール 有効のセキュリティ要求事項
JIS X 6320-4:2017 IC カード－第 4 部: 交換のための構成、セキュリティ及びコマンド
JIS X 6320-8:2006 IC カード－第 8 部: セキュリティ処理コマンド
JIS X 6320-15:2006 IC カード－第 15 部 暗号情報アプリケーション

9.国内標準化団体や関連団体との関係：特になし

10. 管轄 WG：
セキュアトークン WG

11. 改訂などの計画
なし。

1.タイトル：
18-004　JAHISシングルサインオンにおけるセキュリティガイドライン Ver.2.0
2.発行年月：2018年12月
3.種別：JAHIS標準

4.概要：
本ガイドラインは、シングルサインオンの概念を整理し利用可能な技術的選択肢を解説することにより、シングルサインオン技術を採用したシステムの運用を行う場合に想定されるリスクとその対応への考え方（セキュリティリスクアセスメントと要求事項）を提示するものである。
『医療機関内で運用管理されている各種の情報システム』、及び『地域連携システムなど医療機関外で運用管理されているシステム』の両方のシングルサインオンにおけるセキュリティリスクアセスメントと要求事項を適用範囲としている。

5.目的：
医療機関とベンダーが、医療情報システムにてシングルサイオンを用いたシステムを構築する際にどのようなセキュリティ対策を行うべきかを提示し、適切なセキュリティ対策を講じることが出来ることを目的としている。

6.他のJAHIS標準類との関係：
本ガイドラインは独立した標準類である。

7.国のガイドライン等のレギュレーションとの関係：
本ガイドラインは、医療情報システムの安全管理に関するガイドラインの要求事項を踏まえた記載となっている。

8.国際標準化団体等の標準類との関係：
　特になし

9.国内標準化団体や関連団体との関係：
本ガイドラインは、日本医師会電子認証センター等が運営する医療認証基盤との整合を取っている。

10.管轄WG：
シングルサインオンWG

11.改訂などの計画：
　2020年8月より、米国を中心に規格化が進んでいるFHIRの実装を意識したガイドラインの改版作業を実施している。FHIRのセキュリティ要件、ユースケース例をリスクアセスメント対象に追加し、FHIRにおいて、シングルサインオン実装の際に利用が推奨されている OAuth 2.0、及び、OpenID Connectを対象プロトコルとして、新たに改版を行う計画で進めている。

1.タイトル：
18-006　JAHISヘルスケアPKIを利用した医療文書に対する電子署名規格 Ver.2.0
2.発行年月：2019年2月
3.種別：JAHIS標準

4.概要：
電子署名の互換性の確保、及び不正な署名の流通防止のために、署名の生成、検証及び証明書検証において最低限行わねばならないことについて明確に定める。
通常の署名検証に加えて医療分野特有の検証要件として、HPKIのポリシへの準拠性を確認できることが必要であることを明確に定める。
電子保存において必要となる長期真正性担保のために長期署名フォーマットを採用することとする。
また、相互運用性向上のために長期署名フォーマットの利用方法を規定したJIS規格に準拠する形で規格を作成する。
署名対象文書のフォーマットについては限定しない。

5.目的：
本規格は保健医療福祉分野における電子署名を行うに際して、相互運用性と署名検証の継続性を確保するために策定されたものである。主たるターゲットは PKIライブラリの開発を行うベンダーであるが、PKIライブラリを利用するシステムベンダーにも有用である。

6.他のJAHIS標準類との関係：
本規格は独立した標準類である。

7.国のガイドライン等のレギュレーションとの関係：
本規格は電子署名法、e-文書法に準拠しており、医療情報システムの安全管理に関するガイドラインの6.12章の要求事項を踏まえた記載となっている。

8.国際標準化団体等の標準類との関係：
ETSIのCAdES、XAdES規格をベースに策定された以下のJIS規格を参照標準とし、ISO17090-4策定の際のベースの規格となっている。
「CMS利用電子署名(CAdES)の長期署名プロファイル」 JIS X 5092:2008
「XML署名利用電子署名(XAdES)の長期署名プロファイル」 JIS X 5093:2008
「Long term signature profiles for PDF Advanced Electronic Signatures (PAdES)」
ISO14533-3:2017

9.国内標準化団体や関連団体との関係：
規格策定に当たり、日本医師会との意見交換を実施し、HPKI発行側との整合を取っている。

10.管轄WG：
HPKI電子署名規格作成WG

11.改訂などの計画：
ETSIにてJSONに対する電子署名規格としてJAdESの検討が行われているとの情報があり、必要があれば整合性確保のための改定を実施する。

1. タイトル：
16-103　JAHISセキュアトークン実装ガイド・機器認証編 Ver.1.0
2. 発行年月：2017年3月
3. 種別：JAHIS技術文書

4. 概要：
セキュアトークンは、ノード（ネットワークに接続され、ネットワークを介して通信を行うネットワークを構成するコンピュータ、ルータ、サーバ等の要素）の識別及び認証に用いられるクレデンシャルを安全に格納すると共に、クレデンシャルを利用するための媒体である。本ガイドは、Wi-Fiによって医療機器を施設内ネットワークに接続する場合に「医療情報システムの安全管理に関するガイドライン」の最低限のガイドライン（C項）及び推奨されるガイドライン（D項）を満たすための方法や例を示すとともに、そこで利用されるセキュアトークンに関して、ユースケース、セキュアトークンの要件、運用上の要件、相互運用の要件を明らかにしている。

5. 目的：
本ガイドは、医療施設等の院内ネットワークにWi-Fiを用いて医療機器等の接続を行う際に、医療情報システムを安全に運用するために策定されたものである。主たるターゲットはWi-Fiを用いて医療情報システムを構築する医療関連施設のシステム管理者、医療情報システムを開発するベンダー、Wi-Fi機能を搭載した医療機器等を開発するベンダーである。

6. 他のJAHIS標準類との関係：
17-105　JAHISセキュアトークン実装ガイド・ノード認証編Ver.1.1

7. 国のガイドライン等のレギュレーションとの関係：
厚生労働省：医療情報システムの安全管理に関するガイドライン
6.5章C項14及びD項6

8. 国際標準化団体等の標準類との関係：
以下の標準等を参照している。
・IEEE Std 802.1X-2010 - IEEE Standard for Local and metropolitan area networks--Port-Based Network Access Control, February 2010
・RFC 2315, PKCS #7: Cryptographic Message Syntax Version 1.5, March 1998
・RFC 7292, PKCS #12: Personal Information Exchange Syntax v1.1, July 2014
・RFC 2986, PKCS #10: Certification Request Syntax Specification Version 1.7, November 2000
9. 国内標準化団体や関連団体との関係：
特になし

10. 管轄WG：
医療システム部会　セキュリティ委員会　セキュアトークンWG

11. 改訂などの計画：
本編の改定の予定はない。

1. タイトル：
JAHISセキュアトークン実装ガイド・ノード認証編Ver.1.1
2. 発行年月：2017年6月
3. 種別：JAHIS技術文書

4. 概要：
セキュアトークンは、ノード（ネットワークに接続され、ネットワークを介して通信を行うネットワークを構成するコンピュータ、ルータ、サーバ等の要素）の識別及び認証に用いられるクレデンシャルを安全に格納すると共に、クレデンシャルを利用するための媒体である。本ガイドでは、ノード認証に用いられるセキュアトークンに必要とされる機能、相互運用で必要となる仕様を明らかにすると共に、運用上で要求される事項を説明している。

5. 目的：
本ガイドは、セキュアトークンを適応することで医療機関等の施設認証の基盤が円滑に導入・運営されることを目的としている。そのため、本ガイドの主たるターゲットは、医療機関等の情報処理システム管理担当者、認証基盤を利用したシステムベンダーである。

6. 他のJAHIS標準類との関係：
本ガイドは、14-103 JAHISセキュアトークン実装ガイドを改定したものであり、独立した標準類である。関連規格として次のJAHIS標準及びガイドがある
18-001 HPKI対応ICカードガイドライン Ver 3.0
18-004 JAHIS シングルサインオンにおけるセキュリティガイドラインVer 2.0
16-003 JAHISリモートサービスセキュリティガイドラインVer.3.0
16-103 JAHISセキュアトークン実装ガイド・機器認証編Ver.1.0

7. 国のガイドライン等のレギュレーションとの関係：
なし

8. 国際標準化団体等の標準類との関係：
以下のJISを参照している。
JIS X 19790:2007 セキュリティ技術 - 暗号モジュール 有効のセキュリティ要求事項

9. 国内標準化団体や関連団体との関係：
なし

10. 管轄WG：
セキュアトークンWG

11. 改訂などの計画：
なし