医療情報セキュリティにおける
JAHIS標準類の位置づけ

2017年3月版
医療システム部会
セキュリティ委員会

はじめに

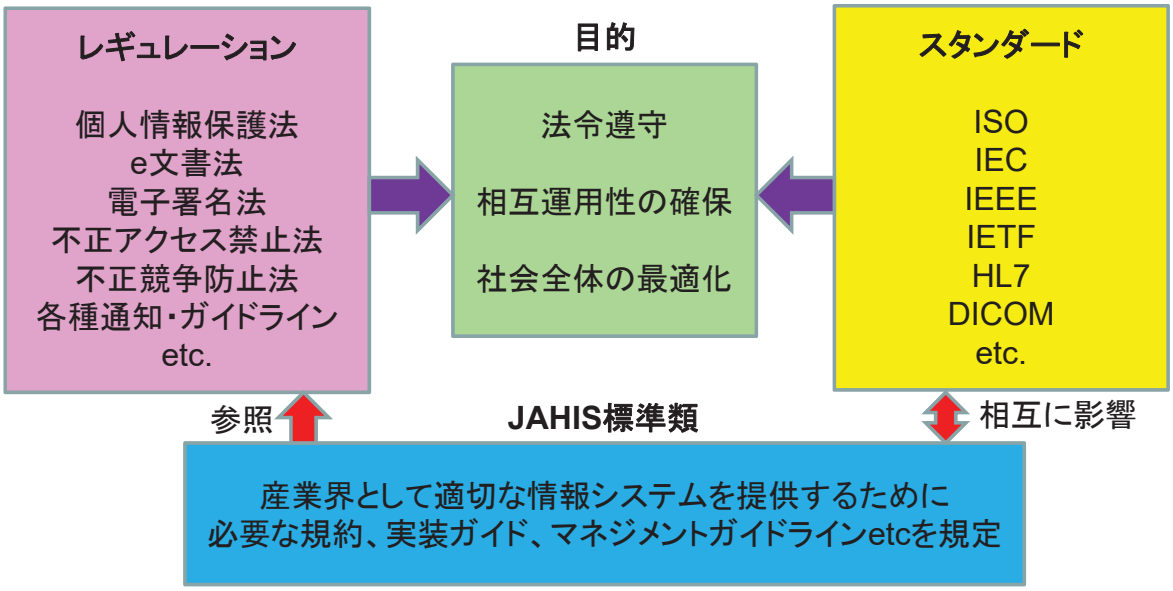
•本ドキュメントはセキュリティ委員会が策定、メンテナンスを行っているJAHIS標準類について、

1. 策定における考え方
2. 国の規制との関係
3. 国際標準（特にISO/TC215）との関係

を示した上で、各JAHIS標準類の概要を上記観点から概説したものである。

本ドキュメントは毎年度末（毎年３月）に年度内の成果を反映した改訂版を発行する予定である。

ヘルスケアセキュリティ分野における レギュレーションとスタンダード



セキュリティ委員会のJAHIS標準類策定における考え方

レギュレーションにおいては、
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」を遵守することを念頭に置いた規約、ガイドラインを制定する

スタンダードにおいては、
ISOとの整合性を確保するため、JAHIS標準類のISOへの提案や、ISO規格のJAHIS標準類への取り込みを実施する

工業会組織であるため、視点はあくまでベンダーの視点であり、医療サービサーや情報システムサービサーの視点ではない。

最近の課題

情報システムサービサーとしての、クラウドに関する問い合わせや、標準化の要請が増えつつある。

セキュリティ関連のJAHIS標準

15-001　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	電子保存・外部保存システムにおける技術的対策としてベンダーが整備すべきものを規定
13-009　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	医療情報システムにおける監査証跡としての監査LOGのメッセージを規定
14-008　製造業者による医療情報セキュリティ開示書ガイド	医療情報システムの技術的対策の実装内容をベンダーが自ら説明するフォーマットを規定
16-003　リモートサービスセキュリティガイドライン	リモート保守などのリモートサービスを実施する際のサービサーとして考慮すべき事項を規定
8-002、10-002　HPKI対応ICカードガイドライン	HPKI証明書をICカードに格納した場合のHPKIへのアクセスメソッドを規定
12-007　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	HPKIを利用して否認防止のための電子署名を行う際の手続きを規定
14-005　HPKI電子認証ガイドライン	HPKIを利用して本人確認などの認証を行う際の考慮すべき事項を規定

セキュリティ関連のJAHIS標準

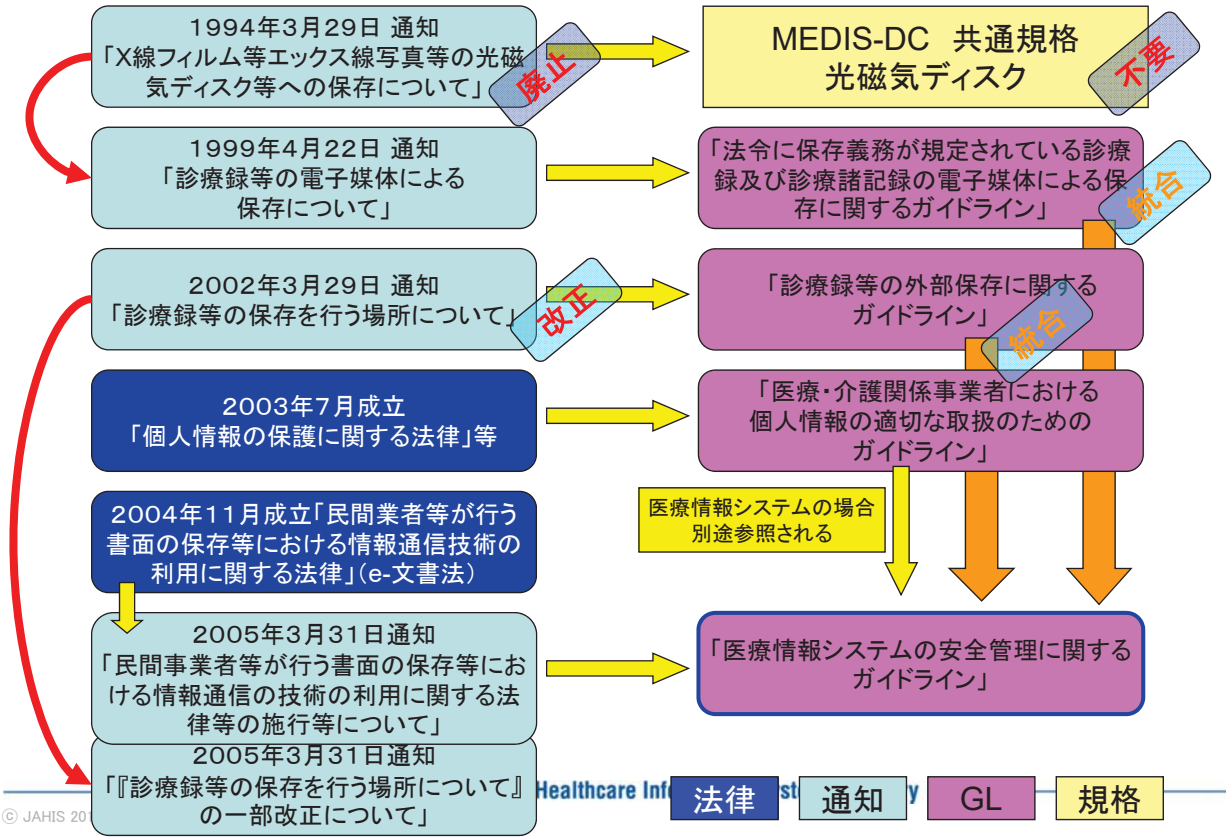
16-002　シングルサインオンにおけるセキュリティガイドライン	病院内の複数システムにおいてシングルサインオンを実現するための要求事項とリスクアセスメントの考え方を記載

Japanese Association of Healthcare Information Systems Industry
ⓒ JAHIS 2017

セキュリティ関連のJAHIS技術文書

16-103　セキュアトークン 実装ガイド機器認証編	医療機関内おける無線接続機器の機器認証のためのクルデンシャルをセキュアに格納・利用するための考慮事項を記載
14-103　セキュアトークン 実装ガイド	医療機関内、施設間などにおけるノード認証のためのクルデンシャルをセキュアに格納・利用するための考慮事項を記載

医療情報システムの安全管理に関するガイドライン制定の経緯



安全管理ガイドライン改訂履歴

年月	版	内容
平成17年3月	初版	電子保存、外部保存のGL統合。個人情報保護のための情報システム運用管理を含む。
平成19年3月	第2版	外部施設とのネットワーク接続に関する要件、災害時等の非常時対応追加。
平成20年3月	第3版	医療情報を取り扱う際の責任分担とルール、無線LAN、モバイル端末の要件追加。
平成21年3月	第4版	電子保存の要求事項のB項、C項、D項大幅見直し。外部保存の民間事業者受託基準の明確化。
平成22年2月	第4.1版	外部保存通知の改正に伴い、改定を実施。
平成25年10月	第4.2版	調剤済み処方箋および調剤録等の外部保存が認められたことから改定。モバイル端末の取扱いについて明確化。
平成28年3月	第4.3版	「電子処方せんの運用ガイドライン」対応。

平成29年3月時点

安全管理GLとJAHIS標準の関係

15-001　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	安全管理ガイドラインの技術的対策として要求されているC項、D項を網羅的に記載
13-009　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	安全管理ガイドラインの6．5章C6.の要求事項を満たすように規定されている
14-008　製造業者による医療情報セキュリティ開示書ガイド	安全管理ガイドラインの技術的対策として要求されているC項への対応状況を記載可能
16-003　リモートサービスセキュリティガイドライン	安全管理ガイドラインの6．5章、6．8章、6．11章の要求事項を踏まえた記載となっている
8-002、10-002　HPKI対応ICカードガイドライン	安全管理ガイドラインの6．5章に対応しているが直接の関係はない
12-007　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	安全管理ガイドラインの6．12章の要求事項を踏まえた記載となっている
14-005　HPKI電子認証ガイドライン	安全管理ガイドラインの6．5章の認証をHPKIで行う際の要件を記載している

JAHIS ヘルスケアセキュリティにおける国際標準

ISO/TC215WG4（Health Informatics Security）

活動スコープ

ヘルスケア情報領域におけるセキュリティとプライバシー保護に関する標準の策定を以下のために行う。

（1） ヘルスケア情報の完全性、機密性、可用性の保持と拡大

（2） 患者安全に悪影響を与えるものからのヘルスケア情報システムの防護

（3） 個人情報に関わるプライバシー保護

（4） ヘルスケア情報システムの利用者に対する責任の明確化

セキュリティ委員会は主として（1）、（3）に関連する規格を担当している
なお（2）については安全性品質企画委員会が担当している

JAHIS JAHIS標準と国際標準との関係

13-009 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	RFC3881,DICOM3.0Part15を参照標準とし、ISO27789のベースの規格となった。 ISO27789出版を受け完全に整合するよう改訂。
16-003 リモートサービスセキュリティガイドライン	SPC White Paperを参考にJIRAが立案し、JAHISと合同でメンテナンスを実施している。 ISO/TR11633のベースの規格となった。 ISO/TR11633出版を受け整合するよう改訂。
8-002、10-002 HPKI対応ICカードガイドライン	ISO/IEC7816-4,8,15を参照標準とし、日本医師会のHPKI対応ICカード発行時のベースの規格となった。
12-007 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	ISOのCAdES、XAdES規格（14533）を参照標準とし、ISO17090-4策定の際のベースの規格となった。
14-005 HPKI電子認証ガイドライン	電子認証の要求事項をまとめるためJAHISが立案し、ISO17090-5として国際標準策定作業中（現在はFDIS）。

○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

（2017 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）

JAHIS 標準

JAHIS 技術文書

１．タイトル：
08-002　HPKI 対応 IC カードガイドライン
10-002　HPKI 対応 IC カードガイドライン 第 2 版
２．発行年月：2008 年 6 月（第 1 版）、2010 年 6 月（第 2 版）
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 標準類との関係：
本規格は独立した標準類である。
関連規格として
12-007　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.1.1
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（平成 27 年 2 月）
・保健医療福祉分野ＰＫＩ認証局認証用（人）証明書ポリシ（平成 27 年 2 月）
・保健医療福祉分野ＰＫＩ認証局認証用（組織）証明書ポリシ（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 19790:2007 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
JIS X 6320-4:2009 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：
「ＨＰＫＩ対応ＩＣカードガイドラインVer.3.0」として、両版の統合と最新化の作業を実施中。

１．タイトル：
12-007　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.1.1
２．発行年月：2013 年 3 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。
関連規格として「10-002　HPKI 対応 IC カードガイドライン 第 2 版」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

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：
本編の改定予定はないが、PDF 電子署名に関する規格を PAdES 編として WG にて原案策定中である。

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 IS27789 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：
「15-001　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．３．２」、「14-104　JAHIS IHE-ITI を用いた医療情報連携基盤実装ガイド本編 Ver2.0」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：
本編の改定予定はない。

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 5 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「10-002　HPKI 対応 IC カードガイドライン 第 2 版」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：
本編は ISO17090-5 出版時に整合性を取るために改訂する可能性がある。

１．タイトル：
14-008　「製造業者による医療情報セキュリティ開示書」ガイド　Ver.2.0
２．発行年月：2014 年 11 月
３．種別：JAHIS 標準

４．概要：
各製造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には標準的記載方法がなく、その記載レベルもさまざまになっている。この状況は、医療機関側にとって、各システム間の整合性を取る際の支障であり、各医療機関で独自に策定した書式にその都度製造業者が対応することもまた、業務の効率化の妨げとなっている。
そこで、日本での標準となるよう製品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に医療情報システムを提供する製造業者。
本ガイドの使用は強制されるものではないが、将来的に DICOM Conformance Statement のように医療情報システムのセキュリティ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：
本書の初版はタイトルが「13-003 製造業者による医療情報セキュリティ開示説明書」と異なり、安全管理ガイドラインの６章のみに対応していたが、Ver.2 では７～９章にも対応している。
15-001　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.3.2
14-003　リモートサービスセキュリティガイドライン Ver.2.1

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」：６～９章

８．国際標準化団体等の標準類との関係：
根幹となる部分が米国 HIPAA 法ではあるが、概念的には MDS^2 が元となった。
※MDS^2 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 としても出版されている。

１０．管轄 WG：
JAHIS-JIRA 合同開示説明書 WG（MDS-WG）

１１．改訂などの計画：
SPC に送付するため Ver.2 の英語化が作業中、安全管理ガイドライン 4.3 版が出版されたタイミングで内容の検討を行い必要であれば改訂作業を開始する。

１．タイトル：

15-001　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.3.2

２．発行年月：2015 年 7 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「ASP･SaaS 事業者が医療情報を取り扱う際の安全管理ガイドライン」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

14-008 JAHIS 製造業者による医療情報セキュリティ開示書ガイド Ver2.0, 2014 年 11 月

14-003JAHIS リモートサービスセキュリティガイドライン Ver.2.1,2014 年 07 月

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 4.2 版　2013 年 10 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

ASP・SaaS 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 1.1 版 2010 年 12 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：

安全管理ガイドライン改定版の出版が予想されており、内容の検討を２月から開始した。

１．タイトル：
16-002　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.1.0
２．発行年月：2016 年 6 月
３．種別：JAHIS 標準

４．概要：
病院内の複数システムにおいてシングルサインオンを実現するための要求事項とリスクアセスメントの考え方を記載している JAHIS 標準である。

５．目的：
本規格は保健医療福祉分野におけるシングルサインオンを実現するに際し、代表的なユースケースと技術方式を選定しリスクアセスメントを行なうことにより、シングルサインオンが安全に運用されることを目的に策定されたものである。主たるターゲットは医療情報システムを導入するベンダーであるが、医療情報システム開発を行うベンダーにも有用である。

６．他の JAHIS 標準類との関係：
ISMS リスクアセスメント手法を参考にした以下のガイドラインと関係している。
・JAHIS 標準 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」の
「6.5 章　技術的安全対策」内の「(1)利用者の識別及び認証」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
・国際標準化機構(ISO)、国際電気標準会議(IEC)　ISO/IEC 27005:2014 情報技術－セキュリティ技術－情報セキュリティのリスクマネジメント

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　シングルサインオン WG

１１．改訂などの計画：

JAHIS 標準　16-002「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.1.0」に対し、スコープ外としていた「外部ネットワークに存在する地域連携サービス」と「電子カルテ等の院内システム」をスコープ内（ユースケースに追加する）として、新たに改版を行う予定である。

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。
15-001　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.3.2
16-002　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.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：
・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 TR 11633 Health informatics — The Information security management for remote maintenance of medical devices and medical information systems Part 1&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：14-103　ＪＡＨＩＳセキュアトークン実装ガイド
２．発行年月：2015 年 2 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：
本規格は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
10-002　HPKI 対応 IC カードガイドライン 第 2 版
12-105　シングルサインオン実装ガイド
14-003　JAHIS リモートサービスセキュリティガイドライン Ver.2.1

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：

「16-103 JAHIS セキュアトークン実装ガイド･機器認証編 Ver.1.0」が発行されたため、ノード認証編として改訂の予定。

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：

14-013　JAHIS セキュアトークン実装ガイド　（ノード認証編として改定予定）

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 11 及び D 項 7

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：

機器認証編の発行に合わせて、「14-013　JAHIS セキュアトークン実装ガイド」をノード認証編として改訂の予定。