



医療情報セキュリティにおける JAHS標準類の位置づけ2020年度版

医療システム部会
セキュリティ委員会

•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

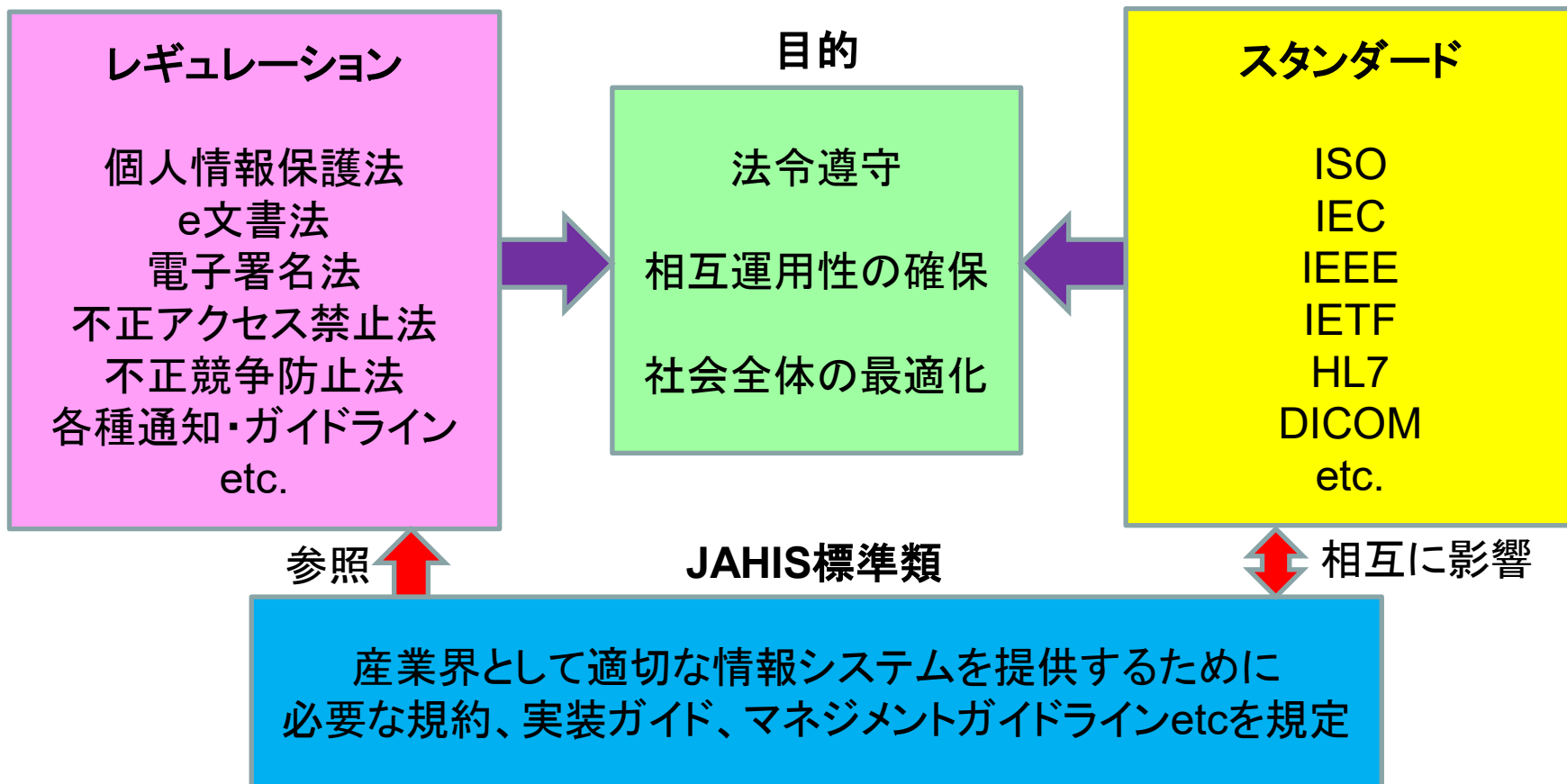
2. 国の規制との関係

3. 国際標準(特にISO/TC215)との関係

を示した上で、2021年3月31日時点の各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、医療サービスや情報システムサービスの視点ではない。

最近の課題
情報システムサービスとしての、クラウドに関するガイドラインの準拠性を示す開示書の策定要望が有識者会議などで生じている。

17-008 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ログのメッセージを規定

20-005 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

医療情報システム/サービスの安全管理GL対応状況を自ら説明するための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スラーとして考慮すべき事項を規定

18-001 HPKI対応ICカードガイドライン

HPKI証明書・私有鍵をICカードに格納した場合のHPKI格納領域へのアクセスメソッドを規定

18-006 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フォーマット並びに手続きを規定

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

18-004 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

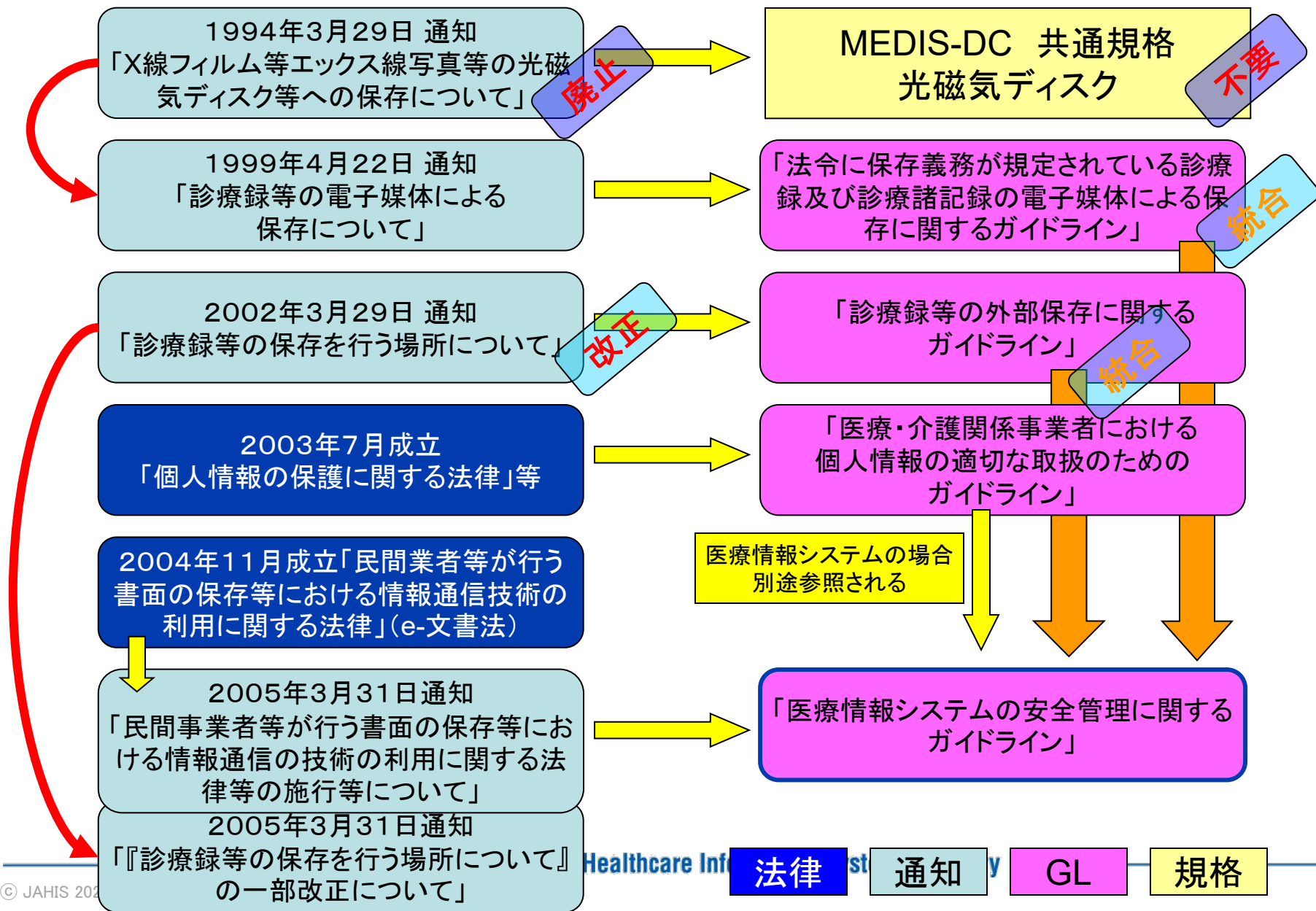
病院内の複数システムにおいてシングルサインオンを実現するための要求事項とリスクアセスメントの考え方を記載

16-103 セキュアトークン実装ガイド・機器認証編

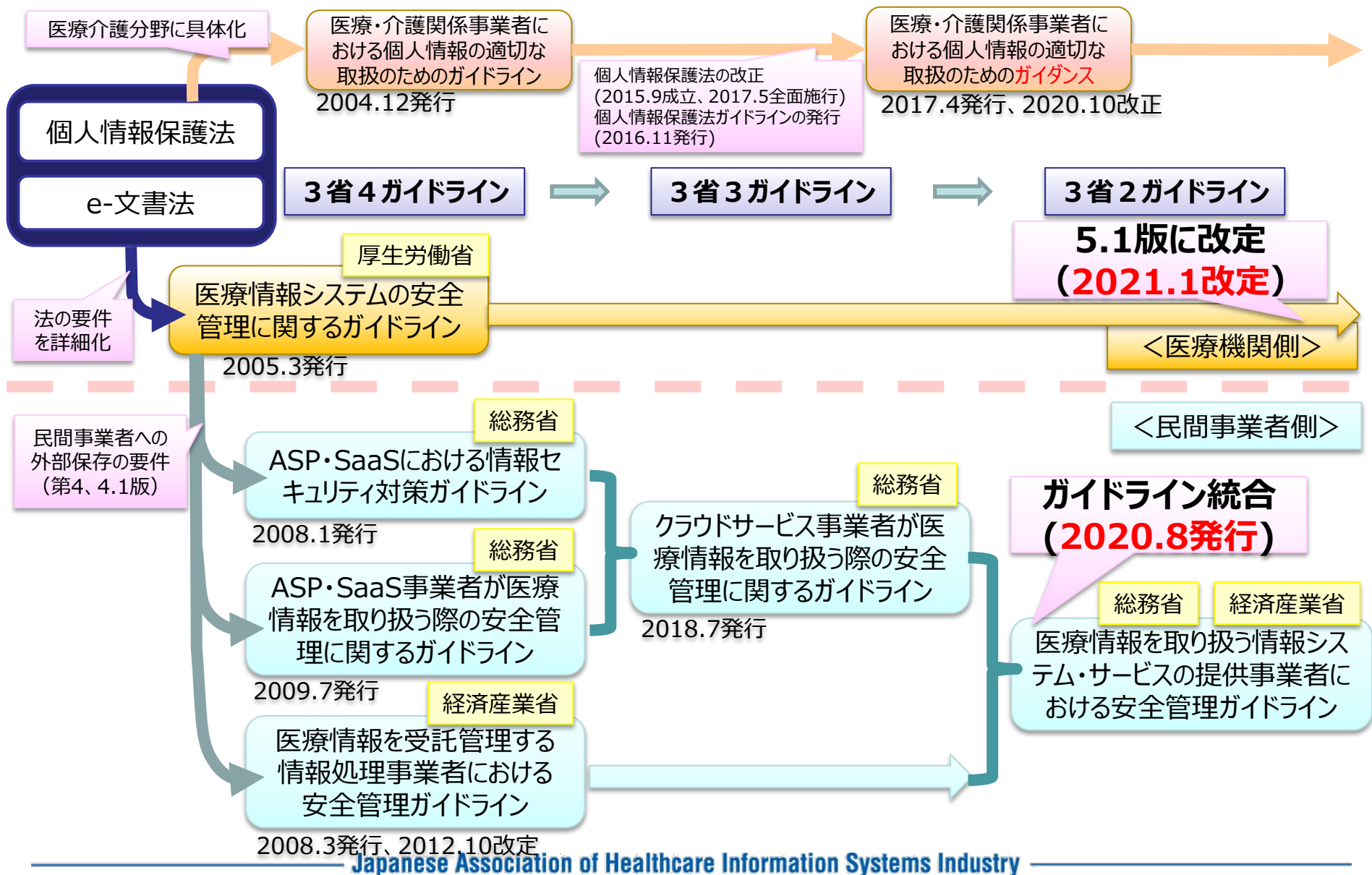
医療機関内における無線接続機器の機器認証のためのクルデンシャルをセキュアに格納・利用するための考慮事項を記載

17-105 セキュアトークン実装ガイド・ノード認証編

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



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5月	第5版	サイバー攻撃の多様化・巧妙化、地域医療連携や医療介護連携等の推進、IoT等の新技術やサービス等の普及への対応。改正個人情報保護法(平成29年5月全面施行)対応。
令和3年1月	第5.1版	サイバー攻撃の多様化・巧妙化、スマートフォンや各種クラウドサービス等の普及、各種ネットワークサービスへの動向への対応。各種ガイドラインとの整合性、個人情報に関する状況等への対応。



JAHIS 安全管理GLとJAHIS標準の関係

17-008 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

20-005 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

安全管理ガイドラインのシステム/サービス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

18-001 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

18-006 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

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

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/TS11633-1,TR11633-2のベースの規格となった。

18-001 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、日本医師会等のHPKI対応ICカード発行時のベースの規格となった。

18-006 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CAAdES、XAdES、PAdES規格(14533)を参照標準とし、本JAHIS標準と完全整合する形でISO17090-4改定が行われた。

14-005 HPKI電子認証ガイドライン

本JAHIS標準と完全整合する形で電子認証の要求事項をまとめたISO17090-5として国際標準として発行された。