JAHIS
健康で豊かな国民生活を保健医療福祉情報システムが支えます

平成29年度 業務報告会

セキュリティ委員会　活動報告

2018年2月2日

セキュリティ委員会

副委員長　　江崎　智

本日のテーマ

電子保存ガイドラインVer.3.3の対応概要

厚労省から安全管理ガイドライン第5版が
2017年5月に公開されました。
これに対応して、電子保存ガイドラインをVer.3.3として
更新しましたので紹介します。

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

厚労省安全管理GL／JAHIS電子保存GL　更新状況

厚労省　安全管理ガイドライン		JAHIS 電子保存GL
平成26年3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27年7月 Ver．３．２
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。	対応無し
平成29年1月30日 第4.4版(案) パブコメ公示	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。	↓ 平成29年12月 Ver．３．３
平成29年5月30日 パブコメ結果公表	意見提出者数36 件、意見数49 件 (BYOD, SNS, パスワード定期変更等)	
平成29年5月30日 第5版	版数を第4.4版(案)から第5版と変更して公開 ・パブコメのコメント検討結果反映 ・改正個人情報保護法(平成29年5月全面施行)対応。	

安全管理ガイドライン第5版の改定概要

- 医療機関等を対象とする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として、関連する1 章、6 章等を改定するとともに、第4.2 版の公表以降に追加された標準規格等への対応を行った。
- また、改正個人情報保護法や「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」等への対応を行った

安全管理ガイドライン第5版　改定内容一覧

#	改訂内容
1	電子カルテの代行入力を時間経過で自動確定することへの言及
2	「製造業者による情報セキュリティ開示書」ガイドへの言及
3	モバイルデバイスへの対応
4	標的型攻撃への対応
5	TLS1.2によるオープンネットワーク接続への言及
6	小規模医療機関が遵守すべき項目の明確化
7	医療情報システムの対象範囲の検討
8	IoTセキュリティへの対応
9	2要素認証の採用
10	電子署名の採用
11	わかりやすさへの対応
12	規格変更への対応

5

電子保存ガイドライン Ver.3.3

#	目次
1	はじめに
2	概要
3	主な用語
4	適用範囲
5	ベンダーの責任のあり方
6	情報システムの基本的な安全管理
7	電子保存の要求事項について
8	診療録及び診療諸記録を外部に保存する際の基準
9	診療録等をスキャナ等により電子化して保存する場合について

6

以下、電子保存ガイドラインver.3.3での
主な改定箇所を説明します。

4.2. 本ガイドラインの対象システム及び対象情報

安全管理ガイドライン第5版において、「医療機関等」の範囲を明確化した。
具体的には「1．はじめに」に追記された。

「本ガイドラインは、病院、一般診療所、歯科診療所、助産所、薬局、訪問看護ステーション、介護事業者、医療情報連携ネットワーク運営事業者等（以下「医療機関等」という。）・・・

電子保存ガイドラインでは、システムの例として「介護システム」を追記した。

以下に対象となる可能性があるシステムの例を示す。

- 電子カルテシステム
- オーダエントリシステム
- 診療部門システム（看護支援システム、手術システムなど）
- 臨床・病理検査システム
- 医用画像システム
- 放射線システム
- 調剤録を電子保存するシステム
- 介護システム

6.1. 医療機関等における情報セキュリティマネジメントシステム(ISMS)の実践

6.1.2. 取扱い情報の把握

- 運用的対策
  - 医療情報システムで扱う情報について重要度に応じて分類し、提示できるようにしておくことが望ましい

6.1.3. リスク分析

- 運用的対策
  - 「製造業者による医療情報セキュリティ開示書(MDS)」を積極的に医療機関等に提出することが望ましい

安全管理ガイドライン第5版において
情報システムで扱われている情報のリストアップやリスク分析及び対策において、その装置のベンダから技術的対策等の情報を収集することが重要である。その際、JAHIS標準及び日本画像医療システム工業会規格となっている「『製造業者による医療情報セキュリティ開示書』ガイド」で示されている「製造業者による医療情報セキュリティ開示書チェックリスト」が参考になる。
とB項に明記された。

MDS：Manufacturer Disclosure Statement for Medical Information Security

6.2. 技術的安全対策

(3)パスワード以外を使用した認証

- 技術的対策
  - 認証にバイオメトリックスを使用する場合には、認証に使用する身体的特徴情報が読取装置の外部へ出ない構造か、身体的特徴情報を暗号化してから読取装置の外部へ送り出す構造のものを使用すること。
- 運用的対策
  - 二つの独立した要素の組み合わせとして、公開情報となっているIDと取得すると誰でも利用できるUSBトークンのように比較的容易に他人が入手可能な要素同士のみの組み合わせは避けるよう医療機関等に推奨すること。

安全管理ガイドライン第5版において
　認証に用いる手段としては、・・・（途中略）・・・利用者しか持ち得ない2つの独立した要素を用いて行う方式（2要素認証）を採用することが望ましい。
　認証技術の端末等への実装状況等を鑑み、本ガイドライン第5版の公表から約10年後を目途に「C. 最低限のガイドライン」とすることを想定する。」
とB項に明記された。

6.2. 技術的安全対策

安全管理ガイドライン第5版において

IoTについて「(6)医療等分野におけるIoT機器の利用」が新たに追加され、情報セキュリティの観点から医療機関等が順守すべき事項が規定されている。

IoT機器とは
　「センサ等で自動的に情報を取得し、若しくは他の機器が自動的に取得した情報を中継し、ネットワークを通じて他の医療情報システムに送信する機器」
と記載されている。

C項(1)リスク分析の実施と運用管理規程の策定
C項(2)セキュリティ対策を十分に行うことが難しいウェアラブル端末や在宅設置のIoT機器を患者等に使用する際はリスク受容について合意。異常時の連絡方法
C項(3)製品出荷後の脆弱性対応
C項(4)使用が終了した又は不具合のために使用を停止したIoT機器の対策
D項(1)IoT機器・システムのそれぞれの状態や他の機器との通信状態の収集・把握

6.2. 技術的安全対策

(12)その他

3)IoT機器の利用時の対策

- 技術的対策
  - IoT機器を含むシステムが単独でそれぞれの状態を把握できることが望ましい
  - 大量のログ管理やログの暗号化を行う等の対策を講じることが難しい機器・システムの場合、上位のシステムに監視装置を設置する等、システムやサービス全体での対策を検討することが望ましい
- 運用的対策
  - ウェアラブル端末や在宅設置の機器を貸し出す際は、情報セキュリティ上のリスクについて事前に患者等へ説明し、リスク受容について合意すること。
  - IoT機器に異常や不都合が発生した場合の問い合わせ方法を確立すること。
  - 使用を終えた又は停止した機器は電源を切り、接続を遮断すること。

6.4. 情報システムの改造と保守

安全管理ガイドライン第5版において
　モバイルデバイスへの対応が記載された。

電子保存ガイドラインでは、モバイルデバイスへの対応として、下記を追記した。

1)　ログ管理　及び　リモートメンテナンス
(イ) リモート保守に関する技術的対策については、「リモートサービスセキュリティガイドラインVer.3.0」（JAHIS標準16-003）を参照すること。

3) 個人情報を含むデータの組織外への持ち出し
(キ) 持ち出し機器でBYOD（個人の所有する、あるいは、個人の管理下にある端末の業務利用）を行う場合は、管理者により適切に設定された機器を用い、個人による設定変更を禁止すること。

6.5. 情報及び機器の持ち出しについて

安全管理ガイドライン第5版において

「公衆無線LANは6.5章C-11の基準を満たさないことがあるため、利用できない。ただし、公衆無線LAN しか利用できない環境である場合に限り、利用を認める。利用する場合は6.11章で述べている基準を満たした通信手段を選択すること。」

とC項に明記された。（赤字の部分が追加された）

「個人の所有する、あるいは個人の管理下にある端末の業務利用（以下「BYOD」という。）」

BYODという用語が使用されるようになった。（「個人の所有する、あるいは個人の管理下にある端末」という記述は4.3版でも有り）

6.6. 災害、サイバー攻撃等の非常時の対応

安全管理ガイドライン第5版において

「(3)サイバー攻撃を受けた際の非常時の対応」が新たに追加され、サイバー攻撃に対する事前・事後の対応について改定されている。

「標的型メール攻撃等により医療情報システムがコンピュータウイルス等に感染した場合、関係先への連絡手段や紙での運用等の代替手段を準備すること。」

とC項に明記された。連絡先として厚生労働省の電話番号も明記されている。

6.7. 外部と個人情報を含む医療情報を交換する場合の安全管理

(10)オープンなネットワークを利用してHTTPSを利用する際の安全対策

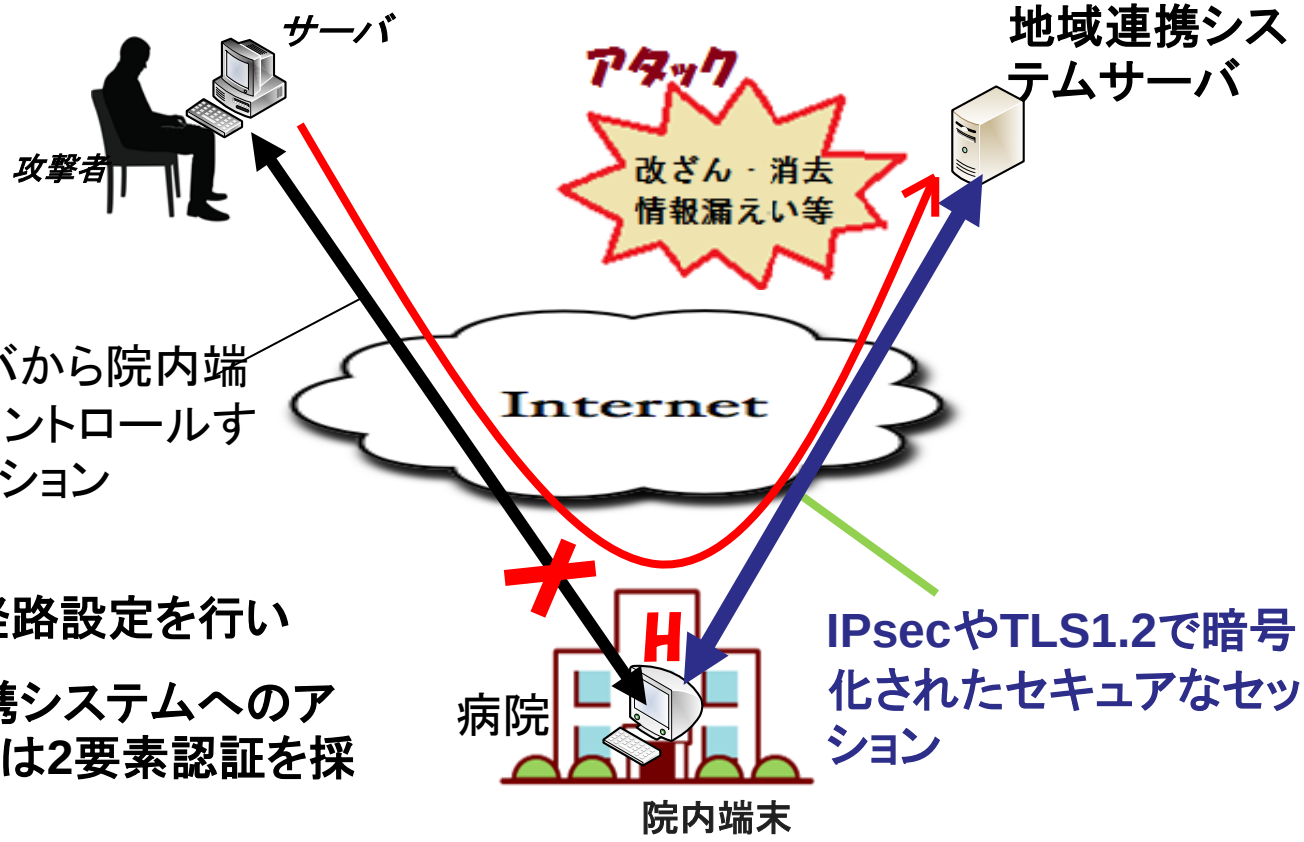
- 技術的対策
  - セッション間の回り込み対策が必要とされる。
    - ルータ等の設定で接続可能なサイトを限定する。
    - 基幹系、情報系のネットワークを分離する。

安全管理ガイドライン第5版において
「オープンなネットワークを介してHTTPSを利用した接続を行う際、IPsecを用いたVPN接続等によるセキュリティの担保を行っている場合を除いては、SSL/TLSのプロトコルバージョンを**TLS1.2**のみに限定した上で、クライアント証明書を利用したTLSクライアント認証を実施すること。」
とC項に明記された。

『「医療情報システムの安全管理に関するガイドライン 第4.3版」に関するQ&A』では既にTLS1.2のみに限定する旨の記載がある。Q&Aはガイドラインの理解を深める役に立つ。
http://www.mhlw.go.jp/file/06-Seisakujouhou-12600000-Seisakutoukatsukan/PDF_11.pdf

6.7. 外部と個人情報を含む医療情報を交換する場合の安全管理

セッション間の回り込みを防ぐには・・・



6.8 法令で定められた記名・押印を電子署名で行なうことについて

(1) 電子署名に用いる電子証明書について

- 技術的対策
  - 保健医療福祉分野PKIの電子証明書（HPKI）⇒JAHIS推奨

【推奨理由】
医師等の国家資格保有者の署名が求められる場合に推奨する。HPKIは電子証明書に保健医療福祉分野の国家資格を格納しており、署名者の国家資格の確認ができる。他の電子証明書では国家資格の確認は別途必要となる。

  - 認定特定認証業者の発行する電子証明書→推奨しない
  - 公的個人認証サービスの電子証明書→推奨しない

安全管理ガイドライン第5版において
「保健医療福祉分野において国家資格を証明しなくてはならない文書等への署名は、この保健医療福祉分野PKI認証局の発行する電子署名を活用することが**推奨される**。」
とC項に明記された。（前版の表記は「望ましい」）

7.1.1. 入力者及び確定者の識別及び認証

安全管理ガイドライン第5版において
電子カルテ等の入力における関係者の役割や責任を明確にした。

変更前:「利用者を正しく識別し、認証を行うこと。」
変更後:「入力者及び確定者を正しく識別し、認証を行うこと。」

- 1）　本人認証、識別
  技術的対策
  (エ)　入力者及び確定者の識別及び認証が可能で、また、入力者と確定者が異なる場合は、確定者の識別及び認証が可能なシステムであること。

7.1.4. 代行入力の承認機能

安全管理ガイドライン第5版において

代行入力の承認機能の項で
「一定時間後に記録が自動確定するような運用の場合は、作成責任者を特定する明確なルールを策定し運用管理規程に明記すること。」
という記載が削除された。

- 代行入力の場合は一定時間後に記録が自動確定するような運用を行ってはならない。

代行入力でない場合は
「一定時間後に記録が自動確定するような運用の場合は、作成責任者を特定する明確なルールを策定し運用管理規程に明記すること。」
という記載は残っている。

健康で豊かな国民生活を保健医療福祉情報システムが支えます

ご清聴ありがとうございました