「安全管理GL」第5版

運用管理規程を中心に

2017.11.20

(一社)保健医療福祉情報安全管理適合性評価協会(HISPRO)
野津　勤

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　2017.5.30

各章の構成

- A:制度上の要求事項
  法律・通知・他の指針など
- B:考え方
  要求事項の解説および原則的な対策
- C:最低限のガイドライン
  Aの要求事項を満たすための必須実施事項
- D:推奨されるガイドライン
  説明責任の観点から実施したほうが理解が得やすい対策

【10章】運用管理規程に関する事項について記載されている。

巻末の3つの付表は安全管理上の要求事項を満たすための技術的対策と運用的対策の関係を要約したもので、運用管理規程の作成に活用されることを期待して作成した。安全管理対策は技術的対策と運用的対策の両面でなされて初めて有効なものとなるが、技術的対策には複数の選択肢があることが多く、採用した技術的対策に対して、相応した運用的な対策を行う必要がある。付表は以下の項目からなる。

1.運用管理項目：安全管理上の要求事項で多少とも運用的対策が必要な項目

2.実施項目：上記管理項目を実施レベルに細分化したもの

3.対象：医療機関等の規模の目安　A＝全、B＝大中、C＝小

4.技術的対策：技術的に可能な対策（一つの実施項目に対して選択可能な対策を列挙した）

5.運用的対策：上記4. の技術的対策を行った場合に必要な運用的対策の要約

6.運用管理規程文例：運用的対策を規程に記載する場合の文例

1.運用管理項目：真正性確保
2.実施項目：入力者及び確定者の識別及び認証
3.対象：B
4.技術的対策：利用者識別子、パスワード等による識別と認証
5.運用的対策：
- 利用者識別子とパスワードの発行、
- パスワードの最低文字数、有効期間等の規程
- 認証の有効回数、超過した場合の対処
- 入力者及び確定者への認証操作の義務付け
- 識別子、パスワードの他人への漏えいやメモ書きの禁止
- 入力者及び確定者への教育
- 緊急時認証の手順規程

6.運用管理規程文例：
- システム管理者は、電子保存システムの入力者及び確定者の登録を管理し、そのアクセス権限を規定し、不正な利用を防止すること。
- パスワードの最低文字数、有効期間等を別途規定すること。
- 認証の有効回数、超過した場合の対処を別途規定すること。
- 入力者及び確定者は、自身の認証番号やパスワードを管理し、これを他者に利用させないこと。
- 入力者及び確定者は、電子保存システムの情報の参照や入力（以下「アクセス」という。）に際して、認証番号やパスワード等によって、システムに自身を認識させること。
- システム管理者は、電子保存システムを正しく利用させるため、入力者及び確定者の教育と訓練を行うこと。

4.1 医療機関等の管理者の情報保護責任について

運用責任に拘わる組織体制
規程通り行われている事の監査
日々の運用＝教育

(1)通常運用における責任について

①説明責任
電子的に医療情報を取り扱うシステムの機能や運[illegible]
満たしていることを患者等に説明する責任である。
・システムの仕様や運用方法を明確に文書化すること
・仕様や運用方法が当初の方針のとおりに機能しているかどうかを定期的に監査すること
・監査結果をあいまいさのない形で文書化すること
・監査の結果問題があった場合は、真摯に対応すること
・対応の記録を文書化し、第三者が検証可能な状況にすること

②管理責任
・管理に関する最終的な責任の所在を明確にする等の監督を行うこと

さらに、個人情報保護法上は、以下の事項を定め、請負事業者との対応に当たる必要がある。
個人情報保護の責任者を定めること
電子化された個人情報の保護について一定の知識を有する責任者を決めること

③定期的に見直し必要に応じて改善を行う責任
情報保護に関する技術は日進月歩であるため、
・・問題点を洗い出し、改善すべき点があれば改善すること
そのために医療機関等の管理者は、医療情報保護の仕組みの改善を常にこころがけ、
現行の運用管理全般の**再評価・再検討を定期的に行う必要**がある。

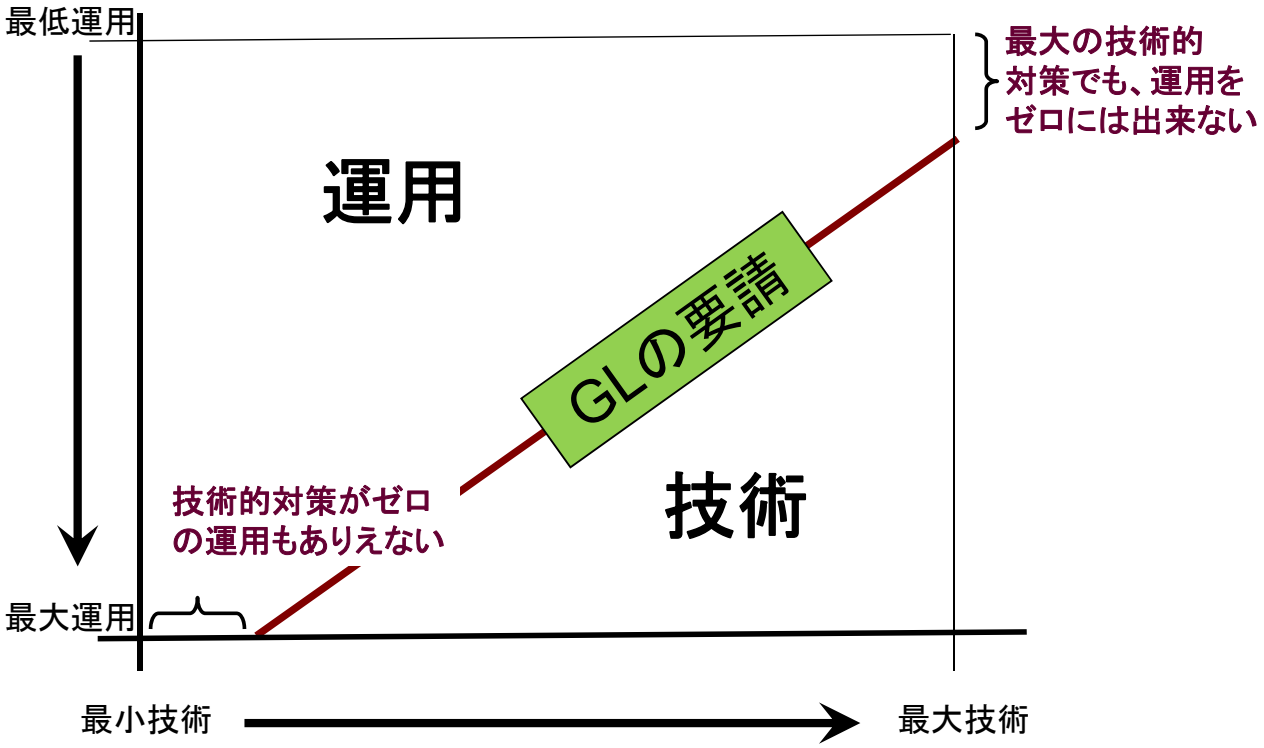
4.4 技術的対策と運用による対策における責任分界点

情報システムの安全を担保するためには、**「技術的な対応（対策）」と「組織的な対応（運用による対策）」の総合的な組み合わせによって達成**する必要がある。
技術的な対応（対策）は医療機関等の総合的な判断の下、主にシステム提供側（ベンダ）に求められ、組織的な対応（運用による対策）は利用者側（医療機関等）の責任で実施される。
総合的な判断とは、リスク分析に基づき、経済性も加味して装置仕様あるいはシステム要件と運用管理規程により一定レベルの安全性を確保することである。この選択は安全性に対する脅威やその対策に対する技術的変化や医療機関等の組織の変化を含めた社会的環境変化により異なってくるので、その動向に注意を払う必要がある。
総合的な判断を下し、医療機関等が責任を果たすためには、ベンダへ要求する技術要件あるいは**ベンダが要求する運用条件**を明確にして、ベンダとの責任分界点を明確にする必要がある。
運用管理規程は、医療機関等として総合的に作成する場合と医用画像の電子保存のように部門別や装置別に作成される場合がある。基準を満たしているか否かを判断する目安として、10章と付表を参考にして、「基準適合チェックリスト」等を作成して整理しておく必要がある。
このようなチェックリストは第三者へ説明責任を果たす際の参考資料に利用できる。

6.3 組織的安全管理対策
運用管理規程は極めて重要であり、
必ず定めなければならない。

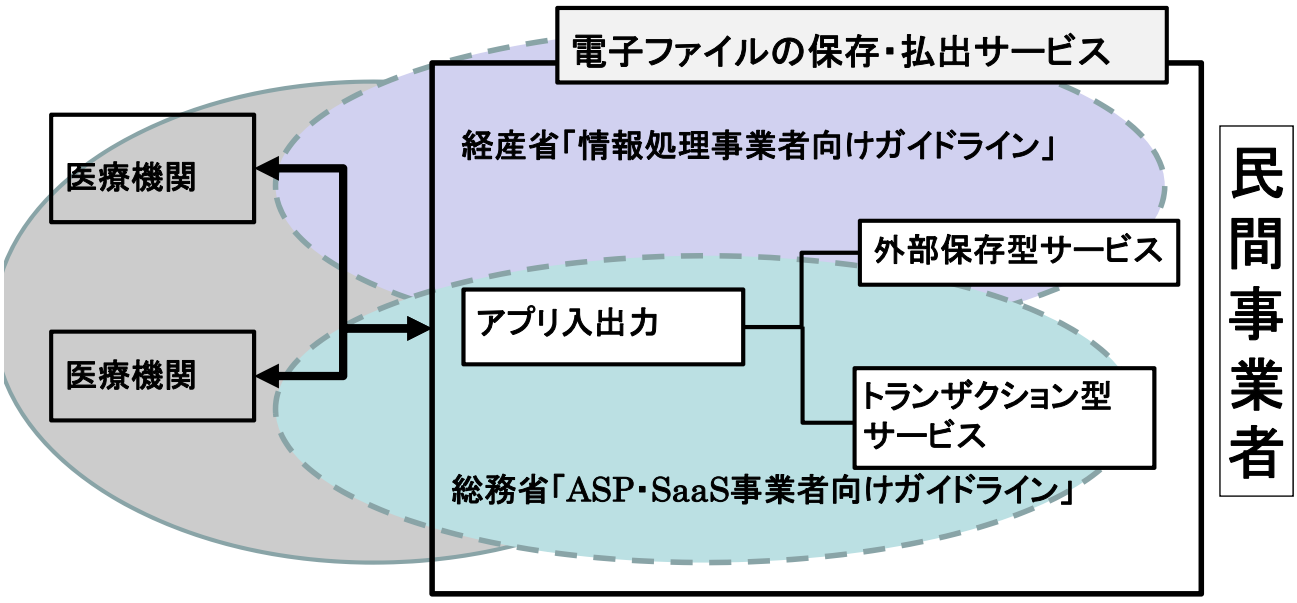
運用と技術の組み合わせ
導入に当たっての契約・評価
　MDSの活用、HISPRO評価の利用
ベンダが求める運用条件

ガイドラインの要請には技術と運用の組み合わせで 対応



民間事業者による医療情報の「外部保存サービス」、「ASP・SaaSサービス」

「安全管理GL」6章ネットワーク　8章業者の選定



10章運用管理について

「運用管理」において運用管理規程は管理責任や説明責任を果たすために極めて重要であり、運用管理規程は必ず定めなければならな

運用管理規程は必須の存在

「医療・介護関係事業者における個人情報の適

Ⅰ　6. 医療・介護関係事業者が行う措置の透明性の確保と対外的明確化

Ⅲ　4(2)①個人情報保護に関する規程の整備、公表

　　ーーー個人情報保護に関する規程を整備し、ーーー。

　個人データを取り扱う情報システムの安全管理措置に関する規程等についても同様に整備を行うこと。

診療録等の電子保存を行う場合の留意事項（施行通知　第3）

1　施設の管理者は診療録等の電子保存に係る運用管理規程を定め、これに従い実施すること。

2　運用管理規程には以下の事項を定めること。

運用管理を総括する組織・体制・設備に関する事項

患者のプライバシー保護に関する事項

その他適正な運用管理を行うために必要な事項

電子媒体により外部保存を行う際の留意事項（外部保存改正通知　第3）

1　外部保存を行う病院、診療所等の管理者は運用管理規程を定め、これに従い実施すること。なお、既に診療録等の電子保存に係る運用管理規程を定めている場合は、適宜これを修正すること。

2　1の運用管理規程の策定にあたっては、診療録等の電子保存に係る運用管理規程で必要とされている事項を定めること。

10章運用管理について

（5）運用管理規程の作成に当たって

運用管理規程は、システムの運用を適正に行うためにその医療機関等ごとに策定されるものである。すなわち、各々の医療機関等の状況に応じて自主的な判断の下に策定されるものである。もちろん、独自に一から作成することも可能であるが、記載すべき事項の網羅性を確保することが困難なことが予想されるため、付表1～付表3に運用管理規程文案を添付する。

付表1は電子保存する・しないに拘らず一般的な運用管理の実施項目例、

付表2は電子保存における運用管理の実施項目例であり、

付表3はさらに外部保存の場合において追加すべき運用管理の実施項目例である。

従って、外部保存の場合は、付表1から付表3の項目を運用管理規程に盛り込むことが必要となる。

「運用管理規程」が1冊の独立した文書である必要性はない。実際の運用に当たって使用される管理規程を定めた文書類の中に、本ガイドラインで記載され本章にまとめられた内容が記載されていれば良い。しかし、日常運用あるいは見直しと改定のことを考慮し、業務単位に分かりやすくまとまっていることが大事である。

　運用管理規程書を作成する場合の推奨手順は以下のとおりである。

作成の参考として付表がある

以下、運用管理規程で決めるべき事項

（1）**一般管理事項**

①総則

a)理念（基本方針と管理目的の表明）

b)対象情報

情報システムで扱う全ての情報のリストアップ

安全管理上の重要度に応じた分類

リスク分析

ISMS
リスク分析

c)　情報システムにおいて採用し変更をフォローすべき標準規格

②管理体制

a)システム管理者、機器管理者、運用責任者、安全管理者、個人情報保護責任者等

b)マニュアル・契約書等の文書の管理体制

c)監査体制と監査責任者

d)患者及びシステム利用者からの苦情・質問の受け付け体制

e)事故対策時の責任体制

f)システム利用者への教育・訓練等の周知体制

③管理者及び利用者の責務

a)システム管理者や機器管理者、運用責任者の責務

b)監査責任者の責務

c)利用者の責務

監査証跡の取り組み方については、「個人情報保護に役立つ監査証跡ガイド」～あなたの病院の個人情報を守るために～（医療情報システム開発センター）を参考にされたい。

④一般管理における運用管理事項

a)来訪者の記録・識別、入退の制限等の入退管理規程

b)情報保存装置、アクセス機器の設置区画の管理・監視規程

c)情報へのアクセス権限の決定方針

d)個人情報を含む記録媒体の管理（保管・授受等）規程

e)個人情報を含む媒体の**廃棄の規程**

f)リスクに対する予防、発生時の対応方法

g)情報システムの安全に関する技術的と運用的対策の分担を定めた文書の管理規程

システムの導入に際して、技術的に対応するか、運用によって対応するかを判定し、その内容を文書化し管理する旨の規程。

技術的対応の検討のための情報収集には、6.2章Bで紹介している「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」を参考にされたい

MDSの利用を

h)技術的安全対策規程

利用者識別と認証の方法

ICカード等セキュリティ・デバイス配布の方法

情報区分と**アクセス権限管理**及び人事異動等に伴う見直し

アクセスログ取得と監査の手順

時刻同期の方法

ウイルス等不正ソフト対策

ネットワークからの不正アクセス対策

パスワードの管理

i)IoT機器の利用に関する事項
　IoT機器の貸し出しに関するリスク受容の合意
　異常時の患者及び医療機関等の役割、連絡先
　異常の検知方法
　セキュリティ上重要なアップデートの方法
　使用終了後又は停止中の不正接続対策
j)無線LANに関する事項
　無線LAN設定（アクセス制限、暗号化等）
　電波障害のおそれがある機器の使用制限
k)電子署名・タイムスタンプに関する規程
　対象となる発行文書、電子署名付き受領文書の取扱規程　　運用管理規程

IoTに関する事項の新設

委託事業者における運用管理規程

⑤業務委託（システムの運用・保守・改造）の安全管理措置
a)業務委託契約における安全管理・守秘条項
b)再委託の場合の安全管理措置事項
c)システム改造及び保守での医療機関等関係者による作業管理・監督、作業報告確認
　保守要員専用のアカウントの作成及び運用管理
　作業時のデータアクセス範囲の確認
　アクセスログの採取と確認
　※リモートメンテナンスには下記⑦も参照。

⑥情報及び情報機器の持ち出しについて
a)持ち出し対象となる情報及び情報機器の規程
b)持ち出した情報及び情報機器の運用管理規程
c)持ち出した情報及び情報機器への安全管理措置
d)盗難、紛失時の対応策
e)利用者への周知徹底方法

⑦外部の機関と医療情報を提供・委託・交換する場合
a)安全を技術的、運用的面から確認する規程
b)リスク対策の検討文書の管理規程
c)情報処理関連事業者等との通常運用時、事故対処時それぞれでの責任分界点を定めた契約文書の管理と契約状態の維持管理規程
リモートメンテナンスの基本方針
d)保守事業者によるリモートメンテナンス体制の安全性確認
e)**従業者による医療機関等の外部からアクセスする場合の運用管理規程**
　アクセスに用いる機器の安全管理

BYODの扱い
SNSの利用

⑧災害、サイバー攻撃等の非常時の対応
a)BCPの規程における医療情報システムの項
b)システムの縮退運用管理規程
c)**非常時の機能と運用管理規程**
d)報告先と内容一覧

⑨教育と訓練
a)マニュアルの整備
b)定期又は不定期なシステムの取扱い及びプライバシー保護やセキュリティ意識向上に関する研修
c)従業者に対する人的安全管理措置
医療従事者以外との守秘契約
従事者退職後の個人情報保護規程
⑩監査
a)監査の内容
b)監査責任者の任務
c)**アクセスログの監査**
⑪規程の見直し
a)運用管理規程の定期的見直し手順

（2）電子保存のための運用管理事項
①真正性確保
a)入力者及び確定者の識別及び認証
b)記録の確定手順と、識別情報の記録
c)更新履歴の保存
d)代行入力の承認記録
e)機器・ソフトウェアの品質管理、動作状況の内部監査規程

②見読性確保
a)情報の所在管理
b)見読化手段の管理
c)見読目的に応じた応答時間とスループット
d)システム障害対策
冗長性
バックアップ
緊急対応

③保存性確保
a)ソフトウェア・機器・媒体の管理（例えば、設置場所、施錠管理、定期点検、ウイルスチェック等）
ウイルスや不適切なソフトウェア等による情報の破壊及び混同等の防止策
b)不適切な保管・取扱いによる情報の滅失、破壊の防止策
バックアップ、作業履歴管理
c)記録媒体、設備の劣化による読み取り不能又は不完全な読み取りの防止策
d)媒体・機器・ソフトウェアの不整合による復元不能の防止策
システムの移行時のデータベースの不整合、機器・媒体の互換性不備に備えた
システム変更・移行時の業務計画の作成規約

④相互運用性確保
a)システムの改修に当たっての、データ互換性の確保策
b)システムの更新に当たっての、データ互換性の確保策

(3)**ネットワークによる外部保存に当たっての「医療機関等としての管理事項」**
可搬媒体による外部保存、紙媒体による外部保存に当たっては、本項を参照して管理事項を作成すること。

①管理体制と責任
a)委託する事業者選定規約、選定時に「適合」と判断した根拠記載の規程
民間事業者等との契約に基づいて確保した安全な場所に該当する機関を選定する場合には、データセンター等の情報処理関連事業者が**経済産業省が定めた「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」**や**総務省が定めた「ASP・SaaS における情報セキュリティ対策ガイドライン」及び「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」**に準拠していることを確認する規程
b)医療機関等における管理責任者
c)**受託事業者への監査体制**
d)受託事業者、回線事業者等との責任分界点
e)受託事業者、回線事業者等の管理責任、説明責任、定期的に見直し必[illegible]応じて改善を行う責任の範囲を明文化した契約書等の文書作成と保管
f)不都合な事態が発生した場合における対処責任、障害部位を切り分け[illegible]存在を明文化した契約書等の文書作成と保管
g)外部に保存を委託する文書の選定基準

外部保管事業者の
選定・管理
暗号鍵預託の管理

②外部保存契約終了時の処理
a)受託事業者に診療録等が残ることがない処理方法の規程
受託事業者に診療録等が残ることがないことの契約、管理者による確認

③真正性確保
a)相互認証機能の採用
b)電気通信回線上で「改ざん」されていないことの保証機能

④見読性確保
a)施設内保存と同項目(2)②の確認
b)緊急に必要になることが予測される医療情報の見読性の確保手段(推奨)
c)緊急に必要になるとまではいえない医療情報の見読性の確保手段(推奨)

⑤保存性確保
a)外部保存を受託する事業者での保存確認機能
施設内保存と同項目(2)③④の確認
b)標準的なデータ形式及び転送プロトコルの採用(推奨)
c)データ形式及び転送プロトコルのバージョン管理と継続性確保

⑥診療録等の個人情報を電気通信回線で伝送する間の個人情報の保護
a)秘匿性の確保のための適切な暗号化
b)通信の起点・終点識別のための認証

⑦診療録等の外部保存を受託する機関内での個人情報の保護
a)外部保存を受託する機関における個人情報保護
b)外部保存を受託する機関における診療録等へのアクセス禁止
c)障害対策時のアクセス通知
d)アクセスログの完全性とアクセス禁止

⑧患者への説明
a)診療開始前の説明方法
b)患者本人の理解を得ることが困難であるが診療上の緊急性がある場合の説明方法
c)患者本人の理解を得ることが困難であるが診療上の緊急性が特にない場合の説明方法

⑨受託事業者に対する監査項目
a)保存記録（内容、期間等）
b)受託事業者における管理策とその実施状況監査

（4）スキャナ等により電子化して保存する場合
①スキャナ読み取りの対象文書の規程
②スキャナ読み取り電子情報と原本と同等であることを担保する情報作成管理者の任命
③スキャナ読み取り電子情報への作業責任者（実施者又は管理者）の電子署名法に適合した電子署名・タイムスタンプ
④診療等の都度、スキャンするタイミングに関する規程
⑤過去に蓄積された文書を電子化する場合の、実施手順規程