福県医発第２３３９号(地)
平成２０年　３月２８日

各　医　師　会　長　殿

福　岡　県　医　師　会
会長　横　倉　義　武
(公印省略)

オンライン請求に係る通知等の一部改定について

オンライン請求に関しましては、「保険医療機関又は保険薬局に係る光ディスク等を用いた費用の請求等に関する取扱いについて」（平成１８年４月１０日保総第04010001 号)、「「レセプトのオンライン請求に係るセキュリティに関するガイドライン」等の策定について」（平成１８年４月１０日保総第 0401002 号。以下、「オンライン請求ガイドライン」という。）により取り扱われていますが、今般、請求に用いる回線について、インターネット上で高水準のセキュリティを確保する手段である、ＩＰｓｅｃとＩＫＥを組み合わせた請求方式が追加された旨、日本医師会より通知がありましたので、貴会会員へ周知方よろしくお願いいたします。

なお、今回の改定にあたっても、日本医師会としてはオンライン請求の「義務化」には断固反対であり、その姿勢は何ら変るものではありませんが、「手挙げ」を希望される医療機関が一部独占的企業の電気通信回線を利用せざるを得ない状況を打開するため、今般の改定に対応してこられました。

小郡三井医師会より

担当理事　毛利康茂・島田昇二郎
会長　丸山　泉

医療

日医発第１０７８号（保206）
平成２０年３月４日

都道府県医師会長　殿

日本医師会長
唐澤

オンライン請求に係る通知等の一部改定について

オンライン請求に関しましては、「保険医療機関又は保険薬局に係る光ディスク等を用いた費用の請求等に関する取扱いについて」（平成１８年４月１０日保総発第04010001号）、「「レセプトのオンライン請求に係るセキュリティに関するガイドライン」等の策定について」（平成１８年４月１０日保総第0410002号。以下、「オンライン請求ガイドライン」という。）により取り扱っているところでありますが、今般、請求に用いる回線について、インターネット上で高水準のセキュリティを確保する手段である、IPsecとIKEを組み合わせた請求方式が追加されましたので、ご連絡申し上げます。

従来のオンライン請求では、請求に用いる電気通信回線がIP-VPNもしくはISDNに限定されており、一部企業の回線を利用するしかなく、独占的な取り扱いがなされておりました。

今般の改定は、同じく厚生労働省が作成した「「医療情報システムの安全管理に関するガイドライン 第２版」（平成１９年３月３０日医政発第0330033号、以下「安全管理ガイドライン」という。）とオンライン請求ガイドラインの整合性を確保することで、高水準のセキュリティを確保した電気通信回線を活用できることとし、また、請求にあたって請求専用のコンピューターを準備する必要性をなくすものです。

請求にあたりまして、医療機関に新たな機材購入に係る投資と回線に係る一部企業の独占を排除するために、本会としてもこれらの是正を厚生労働省と協議した結果、今般の改定となりました。

なお、今般の改定にあたっても、本会としてはオンライン請求の「義務化」には断固反対しており、その姿勢は何ら変わるものではありません。

本会としては、オンライン請求は実施を希望する医療機関が「手挙げ」で参加すべきものであり、一律の義務化はあってはならないと考えております。

従いまして、「義務化」には明確に反対しつつ、「手挙げ」を希望される医療機関が一部の独占的企業の電気通信回線を利用せざるを得ない状況を打開するため、今般の改定に対応して参りましたことを併せて申し添えさせていただきます。

今回の改定内容は下記のとおりでありますので、貴会会員にご周知くださいますよう、よろしくお願い申し上げます。

記

１．保険医療機関又は保険薬局に係る光ディスク等を用いた費用の請求等に関する取扱いについて（平成２０年２月２０日保総発第 0220001 号）

療養の給付、老人医療及び公費負担医療に関する費用の請求に関する省令」（昭和５１年厚生省令第３６号）の一部施行及び安全管理ガイドラインの策定に伴い、取扱い通知における「保険医療機関又は保険薬局に係る光ディスク等を用いた費用の請求に関する取扱要領」を別添のとおり改定し、平成２０年５月請求分から適用することとされた。

改正の内容は、安全管理ガイドラインの策定に伴い、医療機関等の利用者の責任においてオンラインによるレセプトの提出及び受取を行う回線の選択肢を拡大するほか、届出様式等について所要の改正を行ったもの。

２．「レセプトのオンライン請求に係るセキュリティに関するガイドライン」等の改定について（平成２０年２月２０日保総発第 0220003 号）

「安全管理ガイドライン」の策定に伴い、別添１のとおりオンライン請求ガイドラインを改正し、平成２０年５月請求分から適用することとされた。

３．光ディスク等を用いた費用の請求に関して厚生労働大臣が定める方式及び規格並びに電子情報処理組織の使用による費用の請求に関して厚生労働大臣が定める事項及び方式について（平成２０年２月２０日保発第0220004号）

療養の給付、老人医療及び公費負担医療に関する費用の請求に関する省令（昭和５１年厚生省令第３６号）第三条第一項及び附則第四条第二項の規定に基づき、光ディスク等を用いた費用の請求に関して厚生労働大臣が定める方式及び規格並びに電子情報処理組織の使用による費用の請求に関して厚生労働大臣が定める事項及び方式（平成１８年４月１０日保発第0410006号の別紙）について一部変更された。

変更点は、別紙の別添１－１、別添１－２及び別添１－３それぞれの第２章の１中「IP-VPN接続」の次に「、または、オープンなネットワークにおいてはIPsec（IETF(Internet Engineering Task Force)において標準とされた、IP(Internet Protocol)レベルの暗号化機能。認証や暗号のプロトコル、鍵交換のプロトコル、ヘッダー構造など複数のプロトコルの総称）とIKE(Internet Key Exchange；IPsecで用いるインターネット標準の鍵交換プロトコル）を組み合わせた接続」が加えられた。

（添付資料）

１．保険医療機関又は保険薬局に係る光ディスク等を用いた費用の請求等に関する取扱いについて（平成２０年２月２０日保総発第0220001号）

２．「レセプトのオンライン請求に係るセキュリティに関するガイドライン」等の改定について（平成２０年２月２０日保総発第0220003号）

３．光ディスク等を用いた費用の請求に関して厚生労働大臣が定める方式及び規格並びに電子情報処理組織の使用による費用の請求に関して厚生労働大臣が定める事項及び方式について（平成２０年２月２０日保発第0220004号）

福岡県医師会
受
20.2.1
4750

別添

「写」

保総発第 0220001 号
平成２０年２月２０日

地方社会保険事務局長　殿
都道府県民生主管部（局）
　国民健康保険主管課（部）長　殿
都道府県老人医療主管部（局）
　老人医療主管課（部）長　　殿
地方厚生（支）局長　　殿

厚生労働省保険局総務課長

保険医療機関又は保険薬局に係る光ディスク等を用いた
費用の請求等に関する取扱いについて

標記については、「保険医療機関又は保険薬局に係る光ディスク等を用いた費用の請求等に関する取扱いについて」（平成１８年４月１０日保総発第 04010001 号。以下「取扱い通知」という。）により取り扱っているところであるが、今般、「療養の給付、老人医療及び公費負担医療に関する費用の請求に関する省令」（昭和５１年厚生省令第３６号）の一部施行及び「医療情報システムの安全管理に関するガイドライン　第２版」（平成１９年３月３０日医政発第 0330033 号。以下「医療情報システムガイドライン」という。）の策定に伴い、取扱い通知における「保険医療機関又は保険薬局に係る光ディスク等を用いた費用の請求に関する取扱要領」を別添のとおり改定し、平成２０年５月請求分から適用することとしたので通知する。

今回の改正は、医療情報システムガイドラインの策定に伴い、医療機関等の利用者の責任においてオンラインによるレセプトの提出及び受取を行う回線の選択肢を拡大するほか、届出様式等について所要の改正を行ったものであるので、関係者への周知及び指導について、よろしくお取り計らい願いたい。

（別添）

保険医療機関又は保険薬局に係る電子情報処理組織等を用いた費用の請求に関する取扱要領

1　電子情報処理組織による診療（調剤）報酬の請求の届出

保険医療機関又は保険薬局（以下「保険医療機関等」という。）は、療養の給付、老人医療及び公費負担医療に関する費用の請求に関する省令（以下「請求省令」という。）の定めるところにより、診療（調剤）報酬の請求に当たって、電子情報処理組織を使用する場合、又は使用しているプログラム等を変更する場合は、あらかじめその旨を審査支払機関に届け出る（別添１参照）こと。

なお、保険医療機関等で電子情報処理組織の使用による費用の請求が厚生労働大臣の定める方式に適合しているかどうかを事前に確認したい場合は、審査支払機関に依頼（別添２参照）して確認試験を受けることができるものであること。

2　電子情報処理組織による診療（調剤）報酬の請求に関する方法

(1)　保険医療機関等は、診療（調剤）報酬請求書情報及び診療（調剤）報酬明細書情報について、厚生労働大臣の定める方式に従って入出力装置から入力して審査支払機関の電子計算機に備えられたファイルに所定の期日までに記録すること。ただし、電気通信回線に障害が生じたときその他の事情により、電子情報処理組織による請求が特に困難と認められる場合には、後記４(2)または、診療（調剤）報酬請求書及び診療（調剤）報酬明細書により請求すること。

(2)　返戻照会に係る再請求分がある場合は、平成２０年度内の別に定める日までの間、当月請求の電子情報処理組織の使用による費用の請求分と区分し、審査支払機関が返戻した現行の紙レセプトに準じて出力した紙レセプト（以下「出力紙レセプト」という。）に請求省令に定める診療（調剤）報酬請求書を添えて提出すること。

3　保険医療機関等への連絡

(1)　入出力装置から入力して審査支払機関の電子計算機に備えられたファイルに記録された診療（調剤）報酬請求書情報及び診療（調剤）報酬明細書情報等について、読み取り不能が発生した場合は、受付処理結果リストにより連絡すること。

(2)　診療（調剤）報酬請求点数の算定誤り、審査による査定等、請求点数に異動が生じた場合は、増減点連絡書により連絡すること。

(3)　記載事項の不備等事務的理由による返戻及び審査委員会の返戻照会は、平成２０年度内の別に定める日までの間、入出力装置から入力して審査支払機関の電子計算機に備えられたファイルに記録された請求情報に基づき作成した出力紙レセプトにより行うこと。

4　光ディスク等による診療（調剤）報酬の請求の届出

(1)　請求に関する届出

保険医療機関等は、請求省令の定めるところにより、診療（調剤）報酬の請求に当たって厚生労働大臣の定める方式に従って記録した厚生労働大臣の定める規格に適合するフレキシブルディスク又は光ディスク（以下「光ディスク等」という。）を使用する場合、又は使用しているプログラム等を変更する場合は、あらかじめその旨を審査支払機関に届け出る（別添３参照）こと。

なお、保険医療機関等で作成する光ディスク等が、厚生労働大臣の定めた記録条件仕様等に適合しているかどうかを保険医療機関等が事前に確認したい場合は、審査支

払機関に依頼（別添４参照）して確認試験を受けることができるものであること。

(2)　請求に関する方法

①　保険医療機関等は、診療（調剤）報酬請求書情報及び診療（調剤）報酬明細書情報を記録した光ディスク等を正・副２枚作成し、正本に所要の事項を記載したラベル（別添５参照）を貼付のうえ、保険医療機関等が所在する都道府県の審査支払機関に所定の期日までに提出すること。

②　光ディスク等の提出に当たっては、破損等を防止するため、保護ケースを使用すること。

③　光ディスク等の副本は、保険医療機関等で保管すること。
なお、審査支払機関に提出した正本が傷等の理由から読み取りができない場合、正本に代えて提出するものであること。

④　返戻照会に係る再請求分がある場合は、当月請求の光ディスク等の請求分と区分し、審査支払機関が返戻した出力紙レセプトに診療（調剤）報酬請求書を添えて提出すること。

(3)　保険医療機関等への連絡

①　提出された光ディスク等について、読み取り不能が発生した場合は、受付エラー連絡票により連絡すること。

②　診療（調剤）報酬請求点数の算定誤り、審査による査定等、請求点数に異動が生じた場合は、増減点連絡書により連絡すること。

③　記載事項の不備等事務的理由による返戻及び審査委員会の返戻照会は、光ディスク等に記録された請求情報に基づき作成した出力紙レセプトにより行うこと。

５　保険者等への請求

保険者等への請求は、平成２３年３月３１日までの間は、保険者等の選択により以下のいずれかの方法で行うこと。

(1)　診療（調剤）報酬明細書情報を、電子情報処理組織を使用して保険者等の電子計算機に備えられたファイルに記録する。

(2)　診療（調剤）報酬明細書情報を記録した光ディスク（ＤＶＤ－Ｒ又はＣＤ－Ｒ）を提出する。

(3)　出力紙レセプトを提出する。

ただし、平成２３年４月１日以降の保険者等への請求は、(1)の方法で行うこと。

６　再審査の申出及び請求の取下げ申出

再審査の申出及び請求の取下げ申出は、出力紙レセプトにより行うこと。

別添　1

電子情報処理組織の使用による費用の請求に関する届出

電子計算機を使用して厚生労働大臣の定める方式に従って電子情報処理組織の使用による費用の請求を（　開始　・　変更　）することに関し、「療養の給付、老人医療及び公費負担医療に関する費用の請求に関する省令」の規定に基づき届け出ます。

なお、審査支払機関のオンライン請求システム利用規約に同意します。

平成　　年　　月　　日

住所

開設者

氏名　　㊞

（審査支払機関名）　　御中

医療機関（薬局）コード		点数表区分	医科　・　調剤
保険医療機関（薬局）名		電話番号	
保険医療機関（薬局）所在地		郵便番号	－（　　）
レセコンのプログラム名称		請求開始・変更年月	平成　　年　　月請求分から
レセコンのソフトメーカー名（プログラムの作成者の氏名）		パソコンの基本ソフト（ＯＳ）・ブラウザ	
オンライン請求システムに係る安全対策の規程（セキュリティ・ポリシー）	有　・　無		
電気通信回線	ＩＰ－ＶＰＮ接続	ＩＳＤＮ ダイヤルアップ接続 （　　－　　－　　）	インターネット接続（IPsec+IKE） （ＩＰｓｅｃ＋ＩＫＥ提供事業者名　　）
確認試験の実施	有　・　無		
備考			

※受付印

作成要領

1　この様式は、保険医療機関等が電子情報処理組織の使用による費用の請求を開始又は使用しているプログラム等を変更する場合、審査支払機関に医科及び調剤別に作成し提出する。

2　電子情報処理組織の使用による費用の請求を開始又は変更しようとするとき、その別を○で囲む。

3　「点数表区分」欄には、医科及び調剤の別を○で囲む。

4　「医療機関（薬局）コード」、「保険医療機関（薬局）名」、「電話番号」、「保険医療機関（薬局）所在地」及び「郵便番号」欄には、保険医療機関届で届け出た記載内容を記入する。

5　「レセコンのプログラム名称」欄には、レセコンのソフトの名称及びシリーズ名を記入する。

6　「レセコンのソフトメーカー名」欄には、レセコンのソフトメーカー名又はプログラムの作成者の氏名を記入する。

7　「請求開始・変更年月」欄には、電子情報処理組織の使用による費用の請求を開始又は変更しようとするときに、当該診療（調剤）報酬の請求年月を記入する。

8　「パソコンの基本ソフト（ＯＳ）・ブラウザ」欄には、オンライン請求システムの送信機器の基本ソフト名及びブラウザ名を記入する。

≪記載例≫

ＯＳ：ウィンドウズ Vista　　ブラウザ：インターネットエクスプローラ 7

9　「オンライン請求システムに係る安全対策の規程（セキュリティ・ポリシー）」欄には、安全対策の規程の有・無を○で囲む。

10　「電気通信回線」欄には、電気通信回線への接続方法がＩＰ－ＶＰＮ接続、ダイヤルアップ接続及びインターネット接続(IPsec+IKE)（IPsec（IETF(Internet Engineering Task Force)において標準とされた、IP(Internet Protocol)レベルの暗号化機能。認証や暗号のプロトコル、鍵交換のプロトコル、ヘッダー構造など複数のプロトコルの総称）と IKE（Internet Key Exchange；IPsec で用いるインターネット標準の鍵交換プロトコル）を組み合わせた接続に限る。）の別を○で囲む。

なお、ダイヤルアップ接続（ＩＳＤＮ）の場合は、専用電話番号を、インターネット接続（IPsec と IKE を組み合わせた接続に限る。）の場合は、提供事業者名を記入する。

11　「確認試験の実施」欄には、確認試験の有・無を○で囲む。

別添　2

平成　　年　　月　　日

（審査支払機関名）御中

住　所
開設者
氏　名

電子情報処理組織の使用による費用の請求に係る確認試験依頼書

電子情報処理組織の使用による費用の請求を開始するにあたり、確認試験を受けたいので次のとおり依頼します。
なお、審査支払機関のオンライン請求システム利用規約に同意します。

点数表区分	医科　・　調剤		
医療機関（薬局）コード		電話番号	
保険医療機関（薬局）名			
保険医療機関（薬局）所在地	〒		
レセコンのプログラム名称			
レセコンのソフトメーカー名（プログラムの作成者の氏名）			
パソコンの基本ソフト（ＯＳ）・ブラウザ			
オンライン請求システムに係る安全対策の規程	有　・　無		
電気通信回線	ＩＰ-ＶＰＮ接続	ISDN ﾀﾞｲﾔﾙｱｯﾌﾟ接続（　－　－　）	インターネット接続（IPsec+IKE）〔IPsec＋IKE提供事業者名　〕
備考			

《　作成要領　》

1　本依頼書は、保険医療機関（薬局）で電子情報処理組織の使用による費用の請求が厚生労働大臣の定める方式に適合しているかどうか事前に確認したい場合、保険医療機関（薬局）の所在する審査支払機関に医科及び調剤別に作成し提出する。

2　本依頼書の提出期日は確認試験を実施する月の前月２０日までとする。

3　「点数表区分」欄には、医科及び調剤の別を○で囲む。

4　「医療機関（薬局）コード」、「電話番号」、「保険医療機関（薬局）名」及び「保険医療機関（薬局）所在地（郵便番号を含む。）」欄には、保険医療機関届で届け出た記載内容を記入する。

5　「レセコンのプログラム名称」欄には、ソフトの名称及びシリーズ名を記入する。

6　「レセコンのソフトメーカー名」欄には、ソフトメーカー名又はプログラムの作成者の氏名を記入する。

7　「パソコンの基本ソフト（ＯＳ）・ブラウザ」欄には、オンライン請求システムの送信機器の基本ソフト名及びブラウザ名を記入する。
≪記載例≫　ＯＳ：ウィンドウズ　Vista　　ブラウザ：インターネットエクスプローラ　7

8　「オンライン請求システムに係る安全対策の規程」欄の有・無を○で囲む。

9　「電気通信回線」欄には、電気通信回線への接続方法がＩＰ－ＶＰＮ接続、ダイヤルアップ接続及びインターネット接続(IPsec+IKE)（IPsec（IETF(Internet Engineering Task Force)において標準とされた、IP(Internet Protocol)レベルの暗号化機能。認証や暗号のプロトコル、鍵交換のプロトコル、ヘッダー構造など複数のプロトコルの総称）とIKE（Internet Key Exchange；IPsecで用いるインターネット標準の鍵交換プロトコル）を組み合わせた接続に限る。）の別を○で囲む。
なお、ダイヤルアップ接続（ＩＳＤＮ）の場合は、専用電話番号を、インターネット接続（IPsecとIKEを組み合わせた接続に限る。）の場合は、提供事業者名を記入する。

別添３

光ディスク等を用いた費用の請求に関する届出

厚生労働大臣の定める方式に従って記録した厚生労働大臣の定める規格に適合する光ディスク等を用いた費用の請求を　開始／変更　することに関し、「療養の給付、老人医療及び公費負担医療に関する費用の請求に関する省令」の規定に基づき届け出ます。

平成　　年　　月　　日

住所

開設者

氏名　　印

（審査支払機関名）　　御中

医療機関（薬局）コード		点数表区分	医　科・ＤＰＣ・調　剤
保険医療機関（薬局）名		電話番号	
保険医療機関（薬局）所在地		郵便番号	－
プログラム名称			
ソフトメーカー名 （プログラムの作成者の氏名）			
請求開始・変更年月	平成　　年　　月請求分から		※　受付印
電子媒体	ＦＤ	ＭＯ	ＣＤ－Ｒ
記録形式	ＭＳ-ＤＯＳ/ＣＳＶ形式		
備考			

別添３

作成要領

１　この様式は、光ディスク等を用いた費用の請求を開始又は変更しようとするとき、保険医療機関（薬局）の所在する審査支払機関に医科、ＤＰＣ及び調剤別に作成し提出する。

２　光ディスク等を用いた費用の請求を開始又は変更しようとするとき、その別を○で囲む。

３　「点数表区分」欄には、医科、ＤＰＣ及び調剤の別を○で囲む。

４　「医療機関（薬局）コード」、「保険医療機関（薬局）名」、「電話番号」、「保険医療機関（薬局）所在地」及び「郵便番号」欄には、保険医療機関届で届け出た記載内容を記入する。

５　「プログラム名称」欄には、ソフトの名称及びシリーズ名を記入する。

６　「ソフトメーカー名」欄には、ソフトメーカー名又はプログラムの作成者の氏名を記入する。

７　「請求開始・変更年月」欄には、光ディスク等を用いた費用の請求を開始又は変更しようとするときに、当該診療（調剤）報酬の請求年月を記入する。

８　「電子媒体」欄には、記録する電子媒体を○で囲む。

別添　4

平成　　年　　月　　日

（審査支払機関名）　御中

住　所
開設者
氏　名

光ディスク等を用いた費用の請求に係る確認試験依頼書

光ディスク等を用いた費用の請求を開始するにあたり、確認試験を受けたいので次のとおり依頼します。

点数表区分	医科・ＤＰＣ・調剤	依頼回数	新規・　回目
医療機関（薬局）コード		電話番号	
保険医療機関（薬局）名			
保険医療機関（薬局）所在地	〒		
プログラム名称			
ソフトメーカー名 （プログラムの作成者の氏名）			
電子媒体	ＦＤ	ＭＯ	ＣＤ-Ｒ
見込件数	入院　・	入院外　・	
備考			

《　作成要領　》

1　本依頼書は、保険医療機関（薬局）で作成する光ディスク等が厚生労働大臣の定めた記録条件仕様等に適合しているか事前に確認したい場合、保険医療機関（薬局）の所在する審査支払機関に医科、ＤＰＣ及び調剤別に作成し提出する。

2　本依頼書の提出期日は確認試験を実施する月の前月２０日までとする。

3　「点数表区分」欄には、医科、ＤＰＣ及び調剤の別を○で囲む。

4　「依頼回数」欄には、新規又は何回目の確認試験依頼か記入する。

5　「医療機関（薬局）コード」、「電話番号」、「保険医療機関（薬局）名」及び「保険医療機関（薬局）所在地（郵便番号を含む。）」欄には、保険医療機関届で届け出た記載内容を記入する。

6　「プログラム名称」欄には、ソフトの名称及びシリーズ名を記入する。

7　「ソフトメーカー名」欄には、ソフトメーカー名又はプログラムの作成者の氏名を記入する。

8　「電子媒体」欄には、記録する電子媒体を○で囲む。

9　「見込件数」欄には、確認試験を受ける際の見込件数を記入する。

別添５

電子媒体への表記

電子媒体への表記については、記録形式、点数表区分、医療機関（薬局）コード、保険医療機関（薬局）名称、診療（調剤）月分、提出年月日及び媒体枚数（請求枚数及び当該媒体の順）並びに支払基金又は国保連の別を記載する。

なお、確認試験で提出する電子媒体へは、貼付ラベルの余白に「試験用」と朱記する。

１　ＦＤ・ＭＯへの貼付ラベル

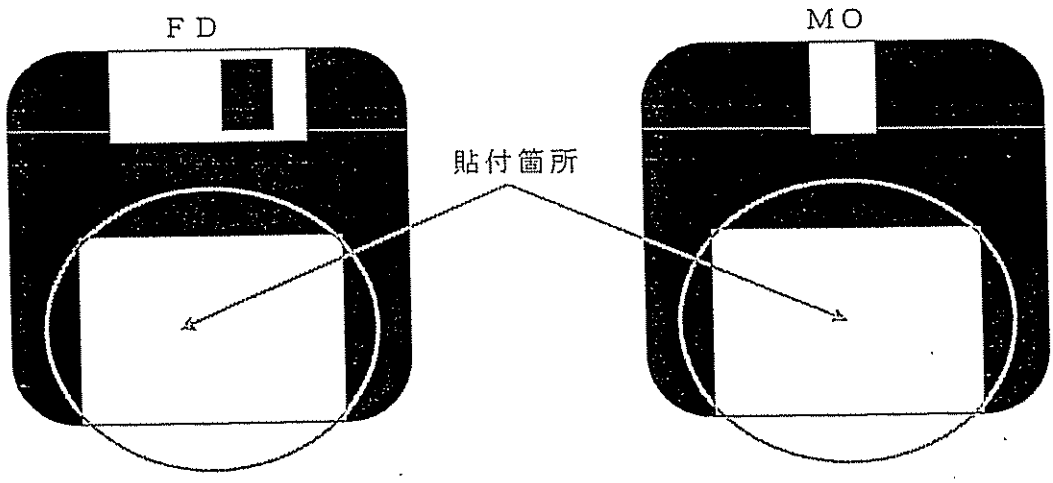
ＭＳ－ＤＯＳ／ＣＳＶ形式（ＦＤ・ＭＯ用）

ＭＳ－ＤＯＳ／ＣＳＶ（医科・ＤＰＣ・調剤）

医療機関（薬局）コード			
保険医療機関（薬局）名称			
診療（調剤）月分	年	月分	
提出年月日	年	月	日
媒体枚数	枚中	枚目	

支払基金
・
国保連

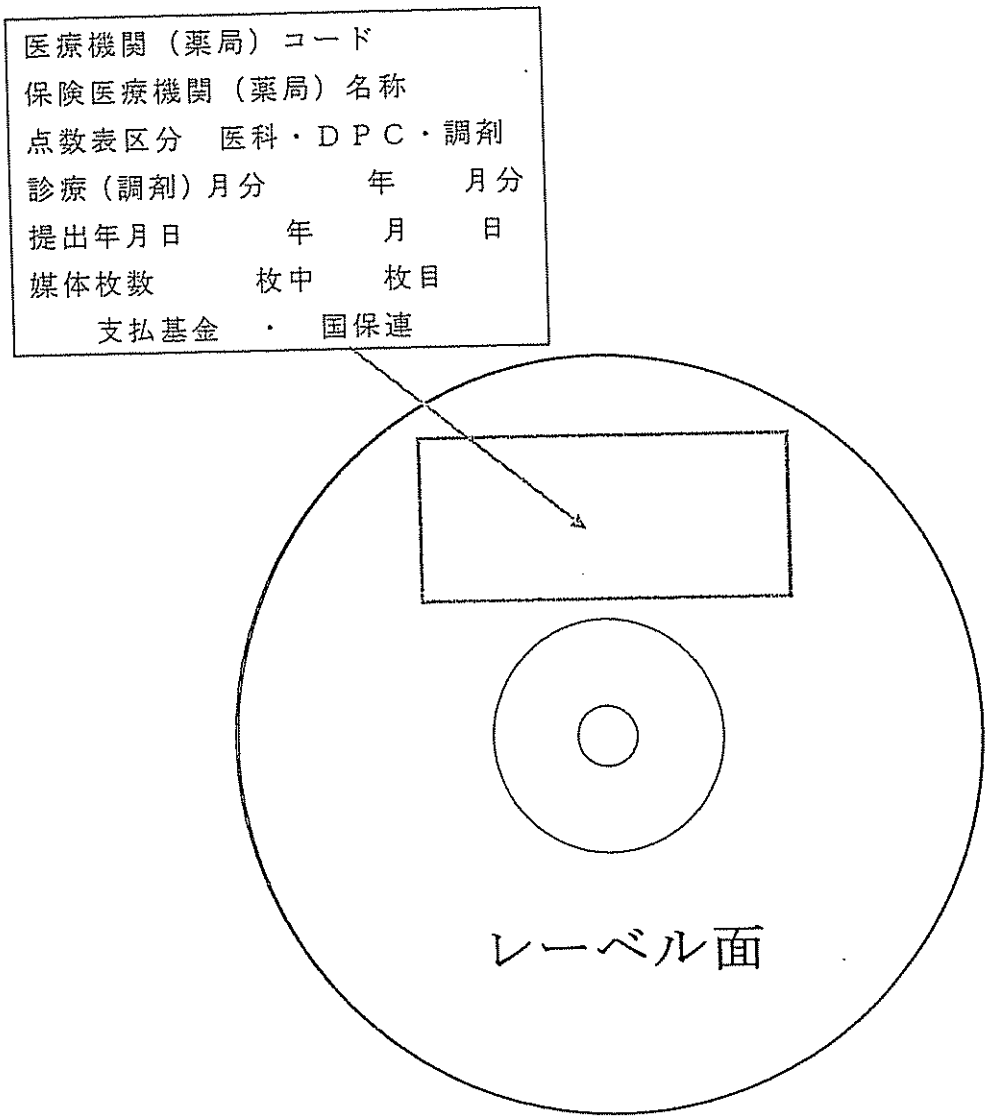
ＦＤ及びＭＯへのラベルの貼付箇所



別添５

２　ＣＤ－Ｒへの表記

レーベル面にシール等を貼付せずに、フェルトペン等により記入すること。



別添

「写」

保総発第 0220003 号
平成２０年２月２０日

地方社会保険事務局長　　殿
都道府県民生主管部（局）
　国民健康保険主管課（部）長　殿
都道府県老人医療主管部（局）
　老人医療主管課（部）長　　殿
地方厚生（支）局長　殿

厚生労働省保険局総務課長

「レセプトのオンライン請求に係るセキュリティに関する
ガイドライン」等の改定について

標記については、「「レセプトのオンライン請求に係るセキュリティに関するガイドライン」等の策定について」（平成１８年４月１０日保総第 0410002 号）により取り扱っているところであるが、今般、「医療情報システムの安全管理に関するガイドライン　第２版」（平成１９年３月３０日医政発第 0330033 号。以下「安全管理ガイドライン」という。）の策定に伴い、別添１のとおり「レセプトのオンライン請求に係るセキュリティに関するガイドライン」（以下「レセプトガイドライン」という。）を改正し平成２０年５月請求分から適用することとしたので通知する。

また、このレセプトガイドラインに則った「レセプトのオンライン請求システムに係る安全対策の規程例（保険医療機関及び保険薬局用）」及び「レセプトのオンライン請求システムに係る安全対策の規程例（保険者用）」をそれぞれ別添２、別添３のとおり改定したので通知する。

関係者への周知につき遺漏のないよう配慮されたい。

別添１

レセプトのオンライン請求に係る
セキュリティに関するガイドライン

平成２０年２月

厚　生　労　働　省

目　次

I 総則 1

1 目的 1
2 適用範囲 3
3 位置付け 4
4 構成 5
5 見直し 5

II セキュリティに関するガイドライン 6

1 組織・体制 6
(1) 責任者の任命 6
(2) 責任の所在 6
(3) 連絡体制 7
2 情報の分類と管理 7
(1) 情報の管理責任 7
(2) 情報の分類 7
(3) 情報の分類に応じた管理方法 8
3 物理セキュリティ 8
(1) 医療機関及び薬局の送信機器の設置場所 8
(2) 審査支払機関の送受信機器の設置場所 8
(3) 保険者の受信機器の設置場所 8
4 人的セキュリティ 8
(1) すべての人員の基本的な責務 9
(2) 機関の長の責務 9
5 技術的セキュリティ 9
(1) レセプトデータの機密性の確保 9
(2) 伝送相手の正当性の確保 9
(3) 伝送事実の正当性の確保 9
(4) システムの機密性の確保 9
(5) 伝送経路の機密性の確保 10
(6) 伝送の完全性の確保 10
(7) 他システムと接続する場合の要求事項 10
6 運用 10
(1) 開発規程 10
(2) 管理運用規程 10
(3) 開発及び試験環境と運用環境の分離 11
7 規程遵守 11
(1) セキュリティポリシー 11
8 規程に対する違反への対応 11
9 評価・見直し 11
(1) 監査証跡の保管 11
(2) 監査の実施 11
(3) 監査結果に基づく措置 11

Ⅰ　総則

1　目的

情報システムの導入は、事務処理の効率化、利便性の向上等のメリットをもたらすことを目指している。しかし、そのメリットの反面、適切な対策が欠如したまま導入した場合には、データの漏洩、消失及び破壊や、情報システムの停止など、事務処理に多大な影響を与える可能性がある。診療報酬明細書等（以下単に「レセプト」という。）に係る電子情報処理組織の使用による費用の請求に関わるシステム（以下「オンライン請求システム[1]」という。）についても決して例外ではなく、特に患者の氏名や傷病名等の慎重な取扱いを要する個人情報[2]を伝送するシステムであるため、適切な対策を講じる必要がある。

このような観点から、本ガイドラインは、レセプトのオンラインによる提出及び受取（以下「オンライン請求」という。）に際し、レセプトに含まれる個人情報を適切に保護するとともに、オンライン請求業務の円滑な遂行に資することを目的として、オンライン請求業務及びオンライン請求システムに携わる人または組織が遵守すべき事項を示すものである。

※留意事項

病院、診療所、薬局（以下「医療機関等」という。）は、情報システムの導入にあたっては、「診療録等の保存を行う場所について」（平成１４年３月２９日付け医政発0329003 号・保発第 0329001 号厚生労働省医政局長・保険局長通知）、「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」（平成１６年法律第149 号）、「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ドライン」（平成１６年１２月２４日付け医政発第 1224001 号、薬食発第 1224001 号、老発第1224002 号厚生労働省医政局長・医薬食品局長・老健局長通知）、「個人情報の保護に関する法律」（平成１５年法律第５７号）、「医療情報システムの安全管理に関するガイドライン　第２版」（平成１９年３月３１日付け医政発第 0330033 号厚生労働省医政局長通知。以下「安全管理ガイドライン」という。）等の関連法令及びガイドラインを参照して適切に導入する必要がある。「安全管理ガイドライン」は、医療に関わる情報を扱うすべての情報システムと、それらのシステムの導入、運用、利用、保守及び廃棄にかかわる人または組織を対象としている。

レセプトを扱うオンライン請求システムは、医療に関わる情報を扱う情報システムであり、したがって、「安全管理ガイドライン」に沿って導入、運用、利用、保守及び廃棄が行われるべきものと考えられる。一方、オンライン請求に際し、レセプトに含まれる個人情報を適切に保護するとともに、オンライン請求業務の円滑な遂行に資することを目的として、オンライン請求システムに携わる人または組織が特に遵守すべき事項もある。また、

---

[1] オンライン請求システム：レセプトをオンラインを活用した電子的手法により提出及び受取を行うためのシステムをいう。単にシステムと記述されている場合は、送信機器、送受信機器又は受信機器等のハードウェアとデータベース及び専用アプリケーション等のソフトウェアの総称をいう。

[2] 個人情報：個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。

オンライン請求業務及びオンライン請求システムに携わる人または組織には、医療機関等だけではなく、医療機関等からレセプトを受取って審査支払を行う審査支払機関及び保険者も含まれる。

このため本ガイドラインは、「安全管理ガイドライン」に沿ってオンライン請求システムの導入、運用、利用、保守及び廃棄が行われることを前提とし、オンライン請求業務及びオンライン請求システムに携わる人または組織に求められる要件を規定するものである。

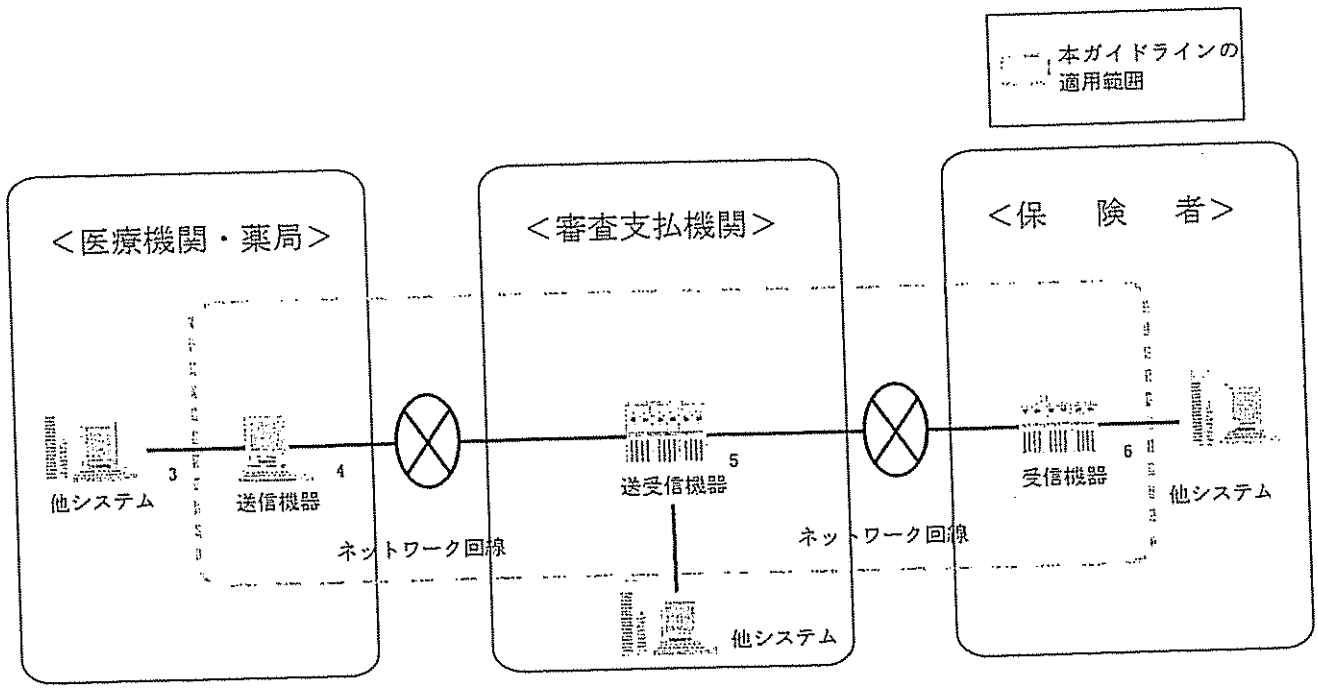
2　適用範囲

本ガイドラインは、オンライン請求システムの導入、運用、利用、保守及び廃棄にかかわる人または組織を対象とし、医療機関等だけではなく、審査支払機関及び保険者も対象になる。

また、本ガイドラインは、オンライン請求システムにおいて伝送されるレセプトをその対象とする。

したがって、物理的手法による搬送などの従来からの請求と、これら請求に付随する業務は、本ガイドラインの対象には含まれない。

本ガイドラインの対象範囲を、図１に示す。



[図　１：ガイドライン対象範囲]

---

[3] 他システム：オーダリングシステム及び人事給与システム等、医療機関等で利用しているシステムあるいは、審査支払機関及び保険者が利用している業務システムをいう。

[4] 送信機器：レセプト等を主に送信する機器の総称をいう。機器とは、例えばパソコン、ネットワーク機器及び外部記憶装置等がある。

[5] 送受信機器：レセプト等を主に送受信する機器の総称をいう。機器とは、例えばサーバ、パソコン、ネットワーク機器、外部記憶装置、バックアップ装置及び無停電電源装置等がある。

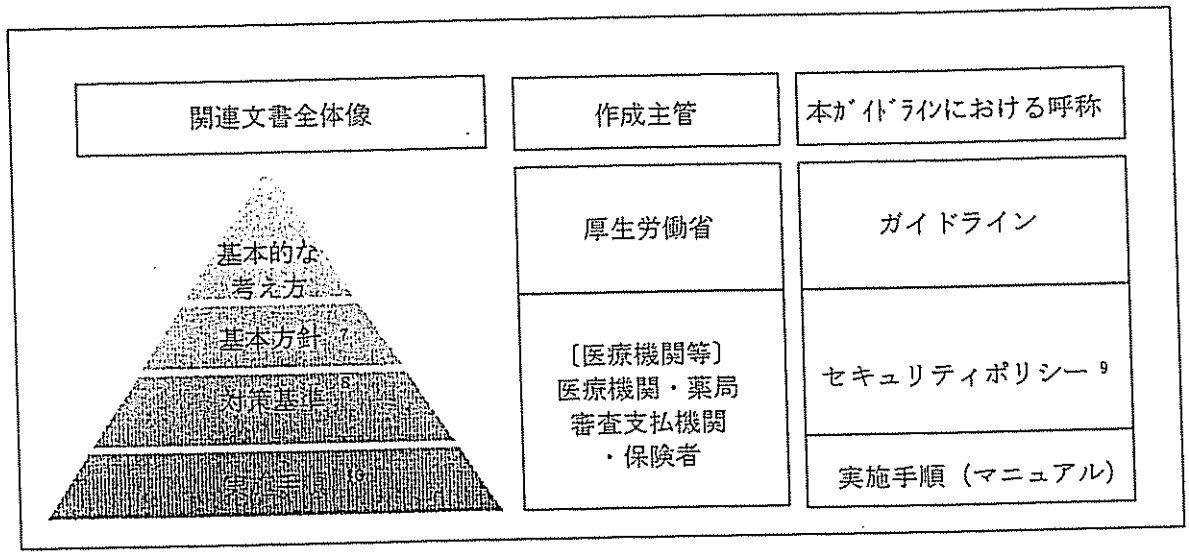
[6] 受信機器：レセプト等を主に受信する機器の総称をいう。機器とは、例えばパソコン、ネットワーク機器及び外部記憶装置等がある。

3　位置付け

本ガイドラインは、前項の適用範囲に基づき、レセプトのオンライン化に関するセキュリティについて基本的な考え方を示すものであり、オンライン請求業務に携わる人または組織及びオンライン請求システムが最低限満たすことが必要と考えられる項目を示している。

オンライン請求を実施しようとする医療機関、薬局、審査支払機関並びに保険者は、本ガイドラインの内容に基づき、その組織においてどのように目的を達成していくかを示した基本方針等を作成することが求められる。また、本ガイドライン以外の対策についても、必要に応じて導入することが望ましい。

本ガイドラインの位置付けを、図２に示す。



[図　２：ガイドラインの位置付け]

---

[7] 基本方針：医療機関等におけるセキュリティ対策に対する根本的な考え方を表わすもので、医療機関等がどのような情報資産をどのような脅威からなぜ保護しなければならないのかを明らかにし、医療機関等の情報セキュリティに対する取組姿勢を示すものをいう。

[8] 対策基準：基本方針に定められた情報セキュリティを確保するために遵守すべき行為及び判断等の基準、つまり、基本方針を実現するために何をやらなければいけないかを示すものをいう。

[9] セキュリティポリシー：医療機関等が所有する情報及び情報システム等の情報資産のセキュリティ対策について、総合的・体系的かつ具体的にとりまとめたものをいう。情報資産への脅威に対する対策について、基本的な考え方並びに情報セキュリティを確保するための体制、組織及び運用を含めた規定。基本方針及び対策基準からなるもの。

[10] 実施手順：セキュリティポリシーには含まれないものの、対策基準に定められた内容を具体的な情報システム又は業務において、どのような手順に従って実行していくのかを示すものをいう。

4　構成

本ガイドラインの構成を、表１に示す。

[表　１：ガイドラインの構成]

構　　成	概　　要
組織・体制	オンライン請求業務に関わる組織の責任と役割について記述する。
情報の分類[11]と管理	オンライン請求業務に関わる情報等の分類と分類に応じた管理方法について記述する。
物理セキュリティ	オンライン請求システムで使用される送信機器、送受信機器又は受信機器の設置される環境が備える設備要件について記述する。
人的セキュリティ	オンライン請求業務に関わる人員の役割と責任、人員に対する教育について記述する。
技術的セキュリティ	オンライン請求システムが備えるセキュリティ機能要件について、ハードウェア、ソフトウェア及びネットワークの観点で記述する。
運用	オンライン請求システムの管理運用に関する整備すべき文書及び遵守事項について記述する。
規程遵守	オンライン請求システムを導入するにあたり整備すべき文書について記述する。
規程に対する違反への対応	オンライン請求システムの運用時における規程違反に対する対応について記述する。
評価・見直し	オンライン請求に関わる業務、システム、文書に対する評価及び見直しについて記述する。

5　見直し

本ガイドラインは、情報通信に関する環境の変化、オンライン請求の状況その他の事情を勘案し、必要に応じ見直しを行うものとする。

---

[11] 情報の分類：情報資産に対し、機密性、完全性、可用性の３つの側面から重要性及び開示範囲の分類を行ったものをいう。この分類は、情報資産をどのように扱い、保護するかを決めるための判断基準となり、これに基づき要求されるセキュリティ水準が定められる。

II　セキュリティに関するガイドライン

1　組織・体制

（1）　責任者の任命

機関の長[12]は、情報セキュリティの確保する体制を確立するため、「医療情報システムの安全管理に関するガイドライン 第2版 第10章」に準じて、オンライン請求システムに従事する人員の情報セキュリティに関する役割と責任を定義し、責任者を任命すること。

（2）　責任の所在

機関の長は、システムを適切に運用するため、「医療情報システムの安全管理に関するガイドライン 第2版 第6.3章」、「医療情報システムの安全管理に関するガイドライン 第2版 第6.9章」及び「医療情報システムの安全管理に関するガイドライン 第2版 第6.10章」に準じて、医療機関、薬局、審査支払機関及び保険者のそれぞれの責任の所在を明確にしておくこと。

（3）　連絡体制

機関の長は、システム障害等における組織間の連絡を円滑に行うため、医療機関、薬局、審査支払機関及び保険者との連絡体制を明確にし、遵守すること。

---

[12] 機関の長：医療機関、薬局、審査支払機関及び保険者において、オンライン請求業務に関するすべての責任を有する最高意思決定者をいう。

2　情報の分類と管理

（1）　情報の管理責任

機関の長は、オンライン請求システムで取り扱う情報について、「医療情報システムの安全管理に関するガイドライン 第2版 第10章」に準じて、管理責任を明確にするため、管理責任者を定めること。

（2）　情報の分類

機関の長は、オンライン請求システムで取り扱う情報について、組織内で重要度の度合を共有するため、「医療情報システムの安全管理に関するガイドライン第2版 第6.2.2章」に準じて、情報の分類を定めること。

（3）　情報の分類に応じた管理方法

機関の長は、オンライン請求システムで取り扱う情報について、重要度の度合に応じた適切な取り扱いを行うため、「医療情報システムの安全管理に関するガイドライン 第2版 第6.3章」に準じて、情報の分類に応じた管理方法について定めること。

3　物理セキュリティ

（1）　医療機関及び薬局の送信機器の設置等

医療機関及び薬局は、医療機関及び薬局の責任において「医療情報システムの安全管理に関するガイドライン 第2版 第6.4章」に準じて、送信機器を設置し、運用すること。

（2）　審査支払機関の送受信機器の設置等

審査支払機関は、審査支払機関の責任において「医療情報システムの安全管理に関するガイドライン 第2版 第6.4章」及び「医療情報システムの安全管理に関するガイドライン 第2版 第6.9章」に準じて、送受信機器を設置し、運用すること。

（3）　保険者の受信機器の設置等

保険者は、保険者の責任において「医療情報システムの安全管理に関するガイドライン 第2版 第6.4章」に準じて、送受信機器を設置し、運用すること。

4　人的セキュリティ

（1）　すべての人員の基本的な責務

オンライン請求業務に携わるすべての者は、「医療情報システムの安全管理に関するガイドライン 第2版 第6.6章」に準じて、オンライン請求業務におけるセキュリティを確保するように努めること。

（2）　機関の長の責務

機関の長は、「医療情報システムの安全管理に関するガイドライン 第2版 第6.6章」に準じて、その機関におけるオンライン請求業務に関する最終的な責任を有する者として、オンライン請求業務におけるセキュリティを確保するように努めること。

5　技術的セキュリティ

（1）　レセプトデータの機密性の確保

オンライン請求業務に携わるすべての者は、「医療情報システムの安全管理に関するガイドライン 第2版 第6.10章」に準じて、レセプトデータを正当な権限を有さない者から適切に保護すること。

（2）　伝送相手の正当性の確保

オンライン請求業務に携わるすべての者は、「医療情報システムの安全管理に関するガイドライン 第2版 第6.10章」に準じて、伝送相手が正当な相手であることを相互に認証する機能を有すること。

（3）　伝送事実の正当性の確保

オンライン請求業務に携わるすべての者は、伝送相手が、レセプトデータの送受信に関する事実を確認できるようにすること。レセプトデータの送受信に関する事実を確認できるようにするとは、例えばデジタル署名付きデータの送付と受領確認データの返送、データの送付に関する受領確認データをお互いに送信、送信ログ及び受信ログの保管などがある。

（4）　システムの機密性の確保

オンライン請求業務に携わるすべての者は、「医療情報システムの安全管理に関するガイドライン 第2版 第6.5章」及び「医療情報システムの安全管理に関するガイドライン 第2版 第6.10章」に準じて、システムの機密性を確保すること。

（5）　伝送経路の機密性の確保

オンライン請求業務に携わるすべての者は、「医療情報システムの安全管理に関するガイドライン 第2版 第6.10章」に準じて、医療機関、薬局、審査支払機関及び保険者を接続するネットワーク回線において、許可されていない者による盗聴及び漏洩に対する機密性を確保する機能を有すること。

（6） 伝送の完全性の確保

オンライン請求業務に携わるすべての者は、「医療情報システムの安全管理に関するガイドライン 第2版 第6.9章」に準じて、ネットワーク回線の切断、ネットワーク機器の故障等の不測の事態にでも対処できる機能を有すること。伝送時における不測の事態に対処するとは、例えばレセプトデータの伝送中にネットワーク障害等が起きた場合、送信機器でネットワークの切断を検知して伝送を中止するようなことである。

（7） 他システムと接続する場合の要求事項

オンライン請求業務に携わるすべての者は、「医療情報システムの安全管理に関するガイドライン 第2版 第6.10章」に準じて、オンライン請求システムを利用及び運用すること。他システムとネットワーク接続する場合は、他システムからの悪影響を遮断すること。

6 運用

（1） 開発規程

審査支払機関は、「医療情報システムの安全管理に関するガイドライン 第2版 第10章」に準じて、オンライン請求システムの開発におけるセキュリティの方針や対策等について明文化し、遵守すること。

（2） 管理運用規程

審査支払機関は、「医療情報システムの安全管理に関するガイドライン 第2版 第10章」に準じて、オンライン請求システムの管理運用におけるセキュリティについて明文化し、遵守すること。

（3） 開発及び試験環境と運用環境の分離

オンライン請求システムの開発及び試験環境は、「医療情報システムの安全管理に関するガイドライン 第2版 第10章」に準じて、運用環境から分離すること。

7　規程遵守

（1）　セキュリティポリシー

ア　医療機関、薬局、審査支払機関及び保険者は、「医療情報システムの安全管理に関するガイドライン 第2版 第6.2章」に準じて、前記1　～6　において規定した事項を実行するためのオンライン請求システムに関わるセキュリティポリシーを策定し、運用すること。

イ　審査支払機関は、オンライン請求システムの安全な運用を図るため、利用規約を定めることができることとし、医療機関、薬局及び保険者は、その利用規約を遵守すること。

8　規程に対する違反への対応

機関の長は、自らの機関で規定した内容に対する違反があった場合の対処について明確にし、厳正に対応すること。

9　評価・見直し

（1）　監査証跡の保管

審査支払機関は、「医療情報システムの安全管理に関するガイドライン 第2版 第10章」に準じて、オンライン請求システムの監査に必要な情報や記録を保管すること。

（2）　監査の実施

審査支払機関は、「医療情報システムの安全管理に関するガイドライン 第2版 第10章」に準じて、システム及び業務に従事する人員とは独立した監査人を任命して監査に関する規程を策定し、オンライン請求についてシステム、文書及び業務が適切であるか定期的に監査を行うこと。

（3）　監査結果に基づく措置

審査支払機関における機関の長は、「医療情報システムの安全管理に関するガイドライン 第2版 第6.2章」に準じて、監査人より監査結果の報告を受け、指摘事項に対する是正措置を講じること。

別添２

レセプトのオンライン請求システムに係る安全対策の規程例
（保険医療機関及び保険薬局用）

○○機関（医療機関名又は、薬局名）

１　目的

この規程（以下「本規程」という。）は、○○機関（以下「当機関」という。）において、オンライン請求システムで使用される機器、ソフトウェア及び運用に必要な仕組み全般について、その取り扱い並びに管理に関する事項を定め、患者の氏名や傷病名等の慎重な取り扱いを要する個人情報を適切に保護し、業務を円滑に遂行できることを目的とする。

２　組織・体制

・　当機関にオンライン請求システム管理者（以下「システム管理者」という。）を置き、機関の長をもってこれに充てる。
・　機関の長は必要な場合、システム管理者を別に指名することができる。
・　オンライン請求システムを円滑に運用し、責任の所在を明確にするため、オンライン請求システムに関する情報管理及び運用について、それぞれを担当する責任者（情報管理責任者及び運用責任者）を置く。
・　情報管理責任者及び運用責任者は、機関の長が指名することができる。
・　システム管理者は緊急時及び災害時の連絡、復旧体制並びに回復手順を定め、非常時においても参照できるように保存し、保管する。

３　情報の分類と管理

・　情報管理責任者は、オンライン請求システムで取り扱う情報について、組織内で重要度の度合いを共有するため、各々の情報の機密性を踏まえ、次の重要性分類に従って分類する。

厳秘：機密性が極めて高い情報の種別（例；レセプトデータ）
秘密：特定の範囲に限り開示することができる機密性が高い情報の種別
（例；実施手順（マニュアル））
公開：広く一般に公開可能である情報の種別

・　オンライン請求システムで取り扱う情報について、ファイル名又は記録媒体等に情報の分類が分かるように表示をする等適切な管理を行わなければならない。

4　送信機器の設置場所等

・　オンライン請求システムの送信機器を設置する場所を、パーティション等で仕切るか又は送信機器に覆いをするか等により、関係者以外の者が機器に接しないようにする。

5　利用者の責務

・　利用者は、本規程及びオンライン請求システムの実施手順（マニュアル）に定められている事項を遵守すること。

・　利用者は、システム管理者の許可を得ず、送信機器及び記録媒体等を部屋外への持ち出しをしないこと。

・　利用者は、オンライン請求システムを正しく利用するための教育と訓練を受けること。

・　利用者は、職務上知り得た個人情報を漏らさないこと。その職を辞した後も、同様である。

・　利用者は、個人情報の漏洩及び改竄が生じた場合、並びにそれらが生じる恐れがある場合には、速やかに運用責任者に連絡し、その指示に従うこと。

・　利用者は、情報セキュリティ対策について不明な点、遵守することが困難な点等については、速やかにシステム管理者に相談し、指示を仰ぐこと。

・　利用者は、関係者以外の者が不正にオンライン請求システムを利用できないようにユーザID及びパスワード等を、適切に管理すること。

6　システム管理者の責務

・　システム管理者は、オンライン請求システムに関する送信機器の設定変更、更新を行う管理者権限等これらの運用における最終的な責任を負うこと。

・　システム管理者は、送信機器やソフトウェアに変更があった場合においても、利用者がオンライン請求業務の遂行を継続的にできるよう環境を整備すること。

・　システム管理者は、オンライン請求システムを正しく利用させるため、利用者の教育と訓練を行うこと。

7　ソフトウェアの管理

・　運用責任者は、送信機器にコンピュータウィルス対策ソフトウェアをインストールするとともに、定期的にコンピュータウィルスのチェックを行い、感染の

防止に努める。

・　オンライン請求システムの送信機器は、オンライン請求業務（レセプト作成業務等を含む。）及びオンライン請求業務の遂行上必要となる業務に使用する。したがって、これらの業務に必要とするソフトウェア以外のソフトウェアはインストールしない。

8　運用

・　システム管理者は、オンライン請求システムの取り扱いについて実施手順（マニュアル）を整備し、利用者に周知の上、常に利用可能な状態にしておく。

・　運用責任者は、ネットワークの不正な利用を発見した場合には、直ちにその原因を追求し対策を実施する。

9　規程に対する違反への対応

システム管理者は、本規程で定めた事項及び自らの機関で別に規定した事項に対する違反があった場合の対処について明確にし、厳正に対応する。

10　評価・見直し

システム管理者は、本規程で定めた事項及び自らの機関で別に規定した事項を評価し、定期的に見直す。

11　その他

その他、本規程の実施に関し必要な事項がある場合については、機関の長がこれを定める。

12　適用年月日

本規程は平成〇年〇月〇日より適用する。

別添３

レセプトのオンライン請求システムに係る安全対策の規程例
（保険者用）

○○機関（保険者名）

１　目的

この規程（以下「本規程」という。）は、○○機関（以下「当機関」という。）において、オンライン請求システムで使用される機器、ソフトウェア及び運用に必要な仕組み全般について、その取り扱い並びに管理に関する事項を定め、被保険者（及び被扶養者）の氏名や傷病名等の慎重な取り扱いを要する個人情報を適切に保護し、業務を円滑に遂行できることを目的とする。

２　組織・体制

・　当機関にオンライン請求システム管理者（以下「システム管理者」という。）を置き、機関の長をもってこれに充てる。
・　機関の長は必要な場合、システム管理者を別に指名することができる。
・　オンライン請求システムを円滑に運用し、責任の所在を明確にするため、オンライン請求システムに関する情報管理及び運用について、それぞれを担当する責任者（情報管理責任者及び運用責任者）を置く。
・　情報管理責任者及び運用責任者は、機関の長が指名することができる。
・　システム管理者は緊急時及び災害時の連絡、復旧体制並びに回復手順を定め、非常時においても参照できるように保存し、保管する。

３　情報の分類と管理

・　情報管理責任者は、オンライン請求システムで取り扱う情報について、組織内で重要度の度合いを共有するため、各々の情報の機密性を踏まえ、次の重要性分類に従って分類する。

厳秘：機密性が極めて高い情報の種別（例；レセプトデータ）
秘密：特定の範囲に限り開示することができる機密性が高い情報の種別
（例；実施手順（マニュアル））
公開：広く一般に公開可能である情報の種別

・　オンライン請求システムで取り扱う情報について、ファイル名又は記録媒体等に情報の分類が分かるように表示をする等適切な管理を行わなければならない。

4　受信機器の設置場所等

・　オンライン請求システムの受信機器を設置する場所を、パーティション等で仕切るか又は受信機器に覆いをするか等により、関係者以外の者が機器に接しないようにする。

5　利用者の責務

・　利用者は、本規程及びオンライン請求システムの実施手順（マニュアル）に定められている事項を遵守すること。

・　利用者は、システム管理者の許可を得ず、受信機器及び記録媒体等を部屋外への持ち出しをしないこと。

・　利用者は、オンライン請求システムを正しく利用するための教育と訓練を受けること。

・　利用者は、職務上知り得た個人情報を漏らさないこと。その職を辞した後も、同様である。

・　利用者は、個人情報の漏洩及び改竄が生じた場合、並びにそれらが生じる恐れがある場合には、速やかに運用責任者に連絡し、その指示に従うこと。

・　利用者は、情報セキュリティ対策について不明な点、遵守することが困難な点等については、速やかにシステム管理者に相談し、指示を仰ぐこと。

・　利用者は、関係者以外の者が不正にオンライン請求システムを利用できないようにユーザID及びパスワード等を、適切に管理すること。

6　システム管理者の責務

・　システム管理者は、オンライン請求システムに関する受信機器の設定変更、更新を行う管理者権限等これらの運用における最終的な責任を負うこと。

・　システム管理者は、受信機器やソフトウェアに変更があった場合においても、利用者がオンライン請求業務の遂行を継続的にできるよう環境を整備すること。

・　システム管理者は、オンライン請求システムを正しく利用させるため、利用者の教育と訓練を行うこと。

7　ソフトウェアの管理

・　運用責任者は、受信機器にコンピュータウィルス対策ソフトウェアをインストールするとともに、定期的にコンピュータウィルスのチェックを行い、感染の防止に努める。

・　オンライン請求システムの受信機器は、オンライン請求業務及びオンライン請求業務の遂行上必要となる業務に使用する。したがって、これらの業務に必要とするソフトウェア以外のソフトウェアはインストールしない。

8　運用

・　システム管理者は、オンライン請求システムの取り扱いについて実施手順（マニュアル）を整備し、利用者に周知の上、常に利用可能な状態にしておく。

・　運用責任者は、ネットワークの不正な利用を発見した場合には、直ちにその原因を追求し対策を実施する。

9　規程に対する違反への対応

システム管理者は、本規程で定めた事項及び自らの機関で別に規定した事項に対する違反があった場合の対処について明確にし、厳正に対応する。

10　評価・見直し

システム管理者は、本規程で定めた事項及び自らの機関で別に規定した事項を評価し、定期的に見直す。

11　その他

その他、本規程の実施に関し必要な事項がある場合については、機関の長がこれを定める。

12　適用年月日

本規程は平成〇年〇月〇日より適用する。

（参考）

医療情報システムの安全管理に関するガイドライン

第２版（抜粋）

平成１９年３月

厚生労働省

6　情報システムの基本的な安全管理

情報システムの安全管理は、刑法等で定められた医療専門職に対する守秘義務等や個人情報保護関連各法（個人情報保護法、行政機関の保有する個人情報の保護に関する法律（平成１５年法律第５８号)、独立行政法人等の保有する個人情報の保護に関する法律（平成１５年法律第５９号)）に規定された安全管理・確保に関する条文によって法的な責務として求められている。守秘義務は医療専門職や行政機関の職員等の個人に、安全管理・確保は個人情報取扱事業者や行政機関の長等に課せられた責務である。安全管理をおろそかにすることは上記法律に違反することになるが、医療においてもっとも重要なことは患者等との信頼関係であり、単に違反事象がおこっていないことを示すだけでなく、安全管理が十分であることを説明できること、つまり説明責任を果たすことが求められる。この章での制度上の要求事項は個人情報保護法の条文を例示する。

A. 制度上の要求事項
（安全管理措置） 法第二十条　個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。 （従業者の監督） 法第二十一条　個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない。 （委託先の監督） 法第二十二条　個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

6.1　方針の制定と公表

「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ドライン」でも個人情報保護に関する方針を定め公表することが求められているが、情報システムの安全管理も個人情報保護対策の一部として考えることができるため、上記の方針の中に情報システムの安全管理についても言及する必要がある。

少なくとも情報システムで扱う情報の範囲、取扱いや保存の方法と期間、利用者識別を確実に行い不要・不法なアクセスを防止していること、安全管理の責任者、苦情・質問の窓口を含めること。

6.2 医療機関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

6.2.1 ISMS 構築の手順

ISMS の構築は PDCA モデルによって行われる。JIS Q27001:2006 では PDCA の各ステップを次の様に規定している。

ISMS プロセスに適用される PDCA モデルの概要

Plan－計画 (ISMS の確立)	組織の全般的方針及び目的に従った結果を出すための、リスクマネジメント及び情報セキュリティの改善に関連した、ISMS 基本方針、目的、プロセス及び手順の確立
Do－実施 (ISMS の導入及び運用)	ISMS 基本方針、管理策、プロセス及び手順の導入及び運用
Check－点検 (ISMS の監視及び見直し)	ISMS 基本方針、目的及び実際の経験に照らした、プロセスのパフォーマンスのアセスメント（適用可能ならば測定）、及びその結果のレビューのための経営陣への報告
Act－処置 (ISMS の維持及び改善)	ISMS の継続的な改善を達成するための、ISMS の内部監査及びマネジメントレビューの結果又はその他の関連情報に基づいた是正処置及び予防処置の実施

P では ISMS 構築の骨格となる文書（基本方針、運用管理規程など）と文書化された ISMS 構築手順を確立する。
D では P で準備した文書や手順を使って実際に ISMS を構築する。
C では構築した ISMS が適切に運用されているか、監視と見直しを行う。
A では改善すべき点が出た場合に是正処置や予防処置を検討し、ISMS を維持する。

上記のステップをより身近にイメージできるようにするために、医療行為における安全管理のステップがどのようにおこなわれているかについて JIPDEC（財団法人 日本情報処理開発協会）の「医療機関向け ISMS ユーザーズガイド」では次のような例が記載されている。

【医療の安全管理の流れ】

事故やミスの発見と報告
「ヒヤリ、ハット事例」や「インシデントレポート」による事故やミスの発見と報告

↓

原因の分析
- 「プロセスアプローチ」によって医療行為をプロセスと捉え、事故やミスの起きた業務全体を一つ一つの単体プロセス（動作）に分解し、フロー図として目に見える形にする。
  （例えば注射を例にプロセスに分解すれば、①医師が処方箋を出し、②処方箋が薬剤部に送られ、③薬剤部から処方が病棟に届けられ、④病棟では看護師が正しく準備し、⑤注射を実施する、となる）
- 作成したフロー図を分析し、どのプロセスに原因があったのかを調べる。

↓

予防／是正策
- 再発防止のための手段を検討と実施（手順の変更、エラーチェックの仕組み導入、職員への教育の徹底など）

上記を見ると、主にD→C→Aが中心になっている。これは医療分野においては診察、診断、治療、看護などの手順が過去からの蓄積によってすでに確立されているため、あとは事故やミスを発見したときにその手順を分析していくことで、どこを改善すればよいかがおのずと見え、それを実行することで安全が高まる仕組みが出来上がっているためと言える。

反面、情報セキュリティではIT技術の目覚しい発展により、過去の経験の蓄積だけでは想定できない新たなセキュリティ上の問題点や弱点が常に存在し得る。そのため情報セキュリティ独自の管理方法が必要であり、ISMSはそのために考え出された。ISMSは医療の安全管理と同様PDCAサイクルで構築し、維持して行く。

逆に言えば、医療関係者にとってISMS構築はPのステップを適切に実践し、ISMSの骨格となる文書体系や手順などを確立すれば、あとは自然にISMSが構築されていく土壌があると言える。

Pのステップを実践するために必要なことは何かについて次に述べる。

6.2.2 取扱い情報の把握

情報システムで扱う情報をすべてリストアップし、安全管理上の重要度に応じて分類を行い、常に最新の状態を維持する必要がある。このリストは情報システムの安全管理者が必要に応じて速やかに確認できる状態で管理されなければならない。

安全管理上の重要度は、安全性が損なわれた場合の影響の大きさに応じて決める。少なくとも患者等の視点からの影響の大きさと、継続した業務を行う視点からの影響の大きさを考慮する必要がある。この他に医療機関等の経営上の視点や、人事管理上の視点等の必要な視点を加えて重要度を分類する。

一般に医療に係る情報が個人識別可能な状態で安全性に問題が生じた場合、患者等にきわめて深刻な影響を与える可能性があり、もっとも重要度の高い情報として分類される。

6.2.3 リスク分析

分類された情報ごとに、管理上の過誤、機器の故障、外部からの侵入、利用者の悪意、利用者の過誤等による脅威を列挙する。医療機関等では一般に他の職員等への信頼を元に業務を進めているために、同僚等の悪意や過誤を想定することに抵抗がある。しかし、情報の安全管理を達成して説明責任を果たすためには、たとえ起こりえる可能性は低くても、万が一に備えて対策を準備する必要がある。また説明責任を果たすためには、これらのリスク分析の結果は文書化して管理する必要がある。この分析の結果えられた脅威に対して、6.3～6.10 の対策を行うことになる。

特に安全管理や個人情報保護関連各法で原則禁止されている目的外利用の防止はシステム機能だけでは決して達成できないことに留意しなければならない。システムとして可能なことは人が正しく操作すれば誰が操作したかを明確に記録しつつ安全に稼動することを保障するのが限界である。したがって人の行為も含めた脅威を想定し、運用規程を含めた対策を講じることが重要である。

医療情報システムとして上記の観点で留意すべき点は、システムに格納されている電子データに関してだけでなく、入出力の際に露見等の脅威にさらされる恐れのある個人情報を保護するための方策を考える必要がある。以下にさまざまな状況で想定される脅威を列挙する。

① 医療情報システムに格納されている電子データ
- (a) 権限のない者による不正アクセス、改ざん
- (b) 権限のある者による不当な目的でのアクセス、改ざん
- (c) コンピュータウイルス等の不正なソフトウェアによるアクセス、改ざん

② 入力の際に用いたメモ・原稿・検査データ等
- (a) メモ・原稿・検査データ等の覗き見
- (b) メモ・原稿・検査データ等持ち出し
- (c) メモ・原稿・検査データ等のコピー
- (d) メモ・原稿・検査データの不適切な廃棄

③ データを格納した可搬型媒体等

(a) 可搬型媒体の持ち出し

(b) 可搬型媒体のコピー

(c) 可搬型媒体の不適切な廃棄

(d) 非可搬型媒体（ハードディスクを搭載したパーソナルコンピュータ等（以下、PC等という。）の不適切な廃棄

④ 参照表示した端末画面等

(a) 端末画面の覗き見

⑤ データを印刷した紙やフィルム等

(a) 紙やフィルム等の覗き見

(b) 紙やフィルム等の持ち出し

(c) 紙やフィルム等のコピー

(d) 紙やフィルム等の不適切な廃棄

⑥ 医療情報システム自身

(a) サイバー攻撃によるIT障害

- 不正侵入
- 改ざん
- 不正コマンド実行
- 情報かく乱
- ウイルス攻撃
- サービス不能（DoS：Denial of Service）攻撃
- 情報漏えい　等

(b) 非意図的要因によるIT障害

- システムの仕様やプログラム上の欠陥（バグ）
- 操作ミス
- 故障
- 情報漏えい　等

(c) 災害によるIT障害

- 地震、水害、落雷、火災等の災害による電力供給の途絶
- 地震、水害、落雷、火災等の災害による通信の途絶
- 地震、水害、落雷、火災等の災害によるコンピュータ施設の損壊等
- 地震、水害、落雷、火災等の災害による重要インフラ事業者等におけるITの機能不全

これらの脅威に対し、対策を行うことにより、発生可能性を低減し、リスクを実際上問題のないレベルにまで小さくすることが必要になる。

6.3 組織的安全管理対策（体制、運用管理規程）

B. 考え方

安全管理について、従業者の責任と権限を明確に定め、安全管理に関する規程や手順書を整備運用し、その実施状況を確認しなければならない。これは組織内で情報システムを利用するかどうかにかかわらず遵守すべき事項である。組織的安全管理対策には以下の事項が含まれる。

① 安全管理対策を講じるための組織体制の整備
② 安全管理対策を定める規程等の整備と規程等に従った運用
③ 医療情報取扱い台帳の整備
④ 医療情報の安全管理対策の評価、見直し及び改善
⑤ 事故又は違反への対処

管理責任や説明責任を果たすために運用管理規程はきわめて重要であり、必ず定めなければならない。運用管理規程には必ず以下の項目を含めること。

- 理念（基本方針と管理目的の表明）
- 医療機関等の内部の体制、外部保存に関わる外部の人及び施設
- 契約書・マニュアル等の文書の管理
- 機器を用いる場合は機器の管理
- 患者等への説明と同意を得る方法
- 監査
- 苦情の受け付け窓口

C. 最低限のガイドライン

1. 情報システム運用責任者の設置及び担当者（システム管理者を含む）の限定を行うこと。ただし小規模医療機関等において役割が自明の場合は、明確な規程を定めなくとも良い。
2. 個人情報が参照可能な場所においては、来訪者の記録・識別、入退を制限する等の入退管理を定めること。
3. 情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成すること。
4. 個人情報の取扱いを委託する場合、委託契約において安全管理に関する条項を含めること。

5. 運用管理規程等において次の内容を定めること。

(a) 個人情報の記録媒体の管理（保管・授受等）の方法

(b) リスクに対する予防、発生時の対応の方法

6.4 物理的安全対策

B. 考え方

物理的安全対策とは、情報システムにおいて個人情報が入力、参照、格納される、情報端末やコンピュータ、情報媒体等を物理的な方法によって保護することである。具体的には情報の種別、重要性と利用形態に応じて幾つかのセキュリティ区画を定義し、以下の事項を考慮し、適切に管理する必要がある。

① 入退館（室）の管理（業務時間帯、深夜時間帯等の時間帯別に、入室権限を管理）
② 盗難、窃視等の防止
③ 機器・装置・情報媒体等の物理的な保護

C. 最低限のガイドライン

1. 個人情報が保存されている機器の設置場所及び記録媒体の保存場所には施錠すること。
2. 個人情報を入力、参照できる端末が設置されている区画は、業務時間帯以外は施錠等、権限者以外立ち入ることが出来ない対策を講じること。
   ただし、本体策項目と同等レベルの他の取りうる手段がある場合はこの限りではない。
3. 個人情報の物理的保存を行っている区画への入退管理を実施すること。
   - 入退者には名札等の着用を義務付け、台帳等に記入することによって入退の事実を記録すること。
   - 入退者の記録を定期的にチェックし、妥当性を確認すること。
4. 個人情報が存在するPC等の重要な機器に盗難防止用チェーンを設置すること。
5. 離席時にも端末等での正当な権限者以外の者による窃視防止の対策を実施すること。

D. 推奨されるガイドライン

防犯カメラ、自動侵入監視装置等を設置すること。

6.5 技術的安全対策（略）

6.6 人的安全対策

B. 考え方

医療機関等は、情報の盗難や不正行為、情報設備の不正利用等のリスク軽減をはかるため、人による誤りの防止を目的とした人的安全対策を策定する必要がある。これには守秘義務と違反時の罰則に関する規定や教育、訓練に関する事項が含まれる。

医療情報システムに関連する者として、次の５種類を想定する。

(a) 医師、看護師等の業務で診療に係わる情報を取扱い、法令上の守秘義務のある者
(b) 医事課職員、その事務委託者等の診療を維持するための業務に携わり、雇用契約の元に医療情報を取扱い、守秘義務を負う者
(c) システムの保守業者等の雇用契約を結ばずに診療を維持するための業務に携わる者
(d) 患者、見舞い客等の医療情報にアクセスする権限を有しない第三者
(e) 診療録等の外部保存の委託においてデータ管理業務に携わる者

このうち、(a) (b)については、医療機関等の従業者としての人的安全管理措置、(c)については、守秘義務契約を結んだ委託業者としての人的安全管理措置の２つに分けて説明する。

(d)の第三者については、そもそも医療機関等の医療情報システムに触れてはならないものであるため、物理的安全管理対策や技術的安全管理対策によって、システムへのアクセスを禁止する必要がある。また、万が一、第三者によりシステム内の情報が漏洩等した場合については、不正アクセス行為の禁止等に関する法律等の他の法令の定めるところにより適切な対処等をする必要がある。

(e)については、いわゆる「外部保存」の委託先の機関等に該当するが、これに関しては、その主旨と実施の詳細を８章に記述する。

(1) 従業者に対する人的安全管理措置

C. 最低限のガイドライン

医療機関等の管理者は、個人情報に関する施策が適切に実施されるよう措置するとともにその実施状況を監督する必要があり、以下の措置をとること。

1. 法令上の守秘義務のある者以外を事務職員等として採用するにあたっては、雇用及び契約時に守秘・非開示契約を締結すること等により安全管理を行うこと。
2. 定期的に従業者に対し教育訓練を行うこと。
3. 従業者の退職後の個人情報保護規程を定めること。

D. 推奨されるガイドライン

1. サーバ室等の管理上重要な場所では、モニタリング等により従業者に対する行動の管理を行うこと。

(2) 事務取扱委託業者の監督及び守秘義務契約

C. 最低限のガイドライン

1. プログラムの異常等で、保存データを救済する必要があるとき等、やむをえない事情で病院事務、運用等で、外部受託業者を採用する場合は、医療機関等の内部における適切な個人情報保護が行われるように、以下のような措置を行うこと。

   ① 包括的な委託先の罰則を定めた就業規則等で裏づけられた守秘契約を締結すること
   ② 保守作業等の医療情報システムに直接アクセスする作業の際には、作業者・作業内容・作業結果の確認をおこなうこと。
   ③ 清掃等の直接医療情報システムにアクセスしない作業の場合においても、作業後の定期的なチェックを行うこと。
   ④ 委託先事業者が再委託を行うか否かを明確にし、再委託を行う場合は委託先と同等の個人情報保護に関する対策及び契約がなされていることを条件とすること。

2. プログラムの異常等で、保存データを救済する必要があるとき等、やむをえない事情で外部の保守要員が診療録等の個人情報にアクセスする場合は、罰則のある就業規則等で裏づけられた守秘契約等の秘密保持の対策を行うこと。

6.7 情報の破棄（略）

6.8 情報システムの改造と保守

B. 考え方

医療情報システムの可用性を維持するためには定期的なメンテナンスが必要である。メンテナンス作業には主に障害対応や予防保守、ソフトウェア改訂等があるが、特に障害対応においては、原因特定や解析等のために障害発生時のデータを利用することがある。この場合、システムのメンテナンス要員が管理者モードで直接医療情報に触れる可能性があり、十分な対策が必要になる。具体的には以下の脅威が存在する。

- 個人情報保護の点では、修理記録の持ち出しによる暴露、保守センター等で解析中のデータの第三者による覗き見や持ち出し等
- 真正性の点では、管理者権限を悪用した意図的なデータの改ざんや、オペレーションミスによるデータの改変等
- 見読性の点では、意図的なマシンの停止や、オペレーションミスによるサービス停止等
- 保存性の点では、意図的な媒体の破壊及び初期化や、オペレーションミスによる媒体の初期化やデータの上書き等

これらの脅威からデータを守るためには、医療機関等の適切な管理の下に保守作業が実施される必要がある。すなわち、①保守会社との守秘義務契約の締結、②保守要員の登録と管理、③作業計画報告の管理、④作業時の病院関係者の監督、等の運用面を中心とする対策が必要である。

また、安全な情報システムの構築を推進するため、システム全体の構成管理を適切に行い、定期的にシステム評価を実施し、最新のセキュリティ技術や標準を適切に取り入れ、客観的に評価された暗号、製品等を導入することも重要である。

なお、保守作業によっては保守会社からさらに外部委託業者に修理等を依頼することが考えられるため、保守会社との保守契約の締結にあたっては、再委託先への個人情報保護の徹底等について保守会社と同等の契約を求めることが重要である。

C. 最低限のガイドライン

1. 動作確認で個人情報を含むデータを使用するときは、明確な守秘義務の設定を行うとともに、終了後は確実にデータを消去する等の処理を行うことを求めること。
2. メンテナンスを実施するためにサーバに保守会社の作業員がアクセスする際には、保守要員個人の専用アカウントを使用し、個人情報へのアクセスの有無、およびアクセスした場合は対象個人情報を含む作業記録を残すこと。これはシステム利用者を模して操作確認を行うための識別・認証についても同様である。

3. そのアカウント情報は外部流出等による不正使用の防止の観点から適切に管理することを求めること。
4. 保守要員の離職や担当変え等に対して速やかに保守用アカウントを削除できるよう、保守会社からの報告を義務付けまた、それに応じるアカウント管理体制を整えておくこと。
5. 保守会社がメンテナンスを実施する際には、日単位に作業申請の事前提出することを求め、終了時の速やかな作業報告書の提出を求めること。それらの書類は医療機関等の責任者が逐一承認すること。
6. 保守会社と守秘義務契約を締結し、これを遵守させること。
7. 保守会社が個人情報を含むデータを組織外に持ち出すことは避けるべきであるが、やむ得ない状況で組織外に持ち出さなければならない場合には、置き忘れ等に対する十分な対策を含む取扱いについて運用管理規程を定めることを求め、医療機関等の責任者が逐一承認すること。
8. リモートメンテナンスによるシステムの改造や保守が行なわれる場合には、必ずメッセージログを採取し、当該作業の終了後速やかにメッセージログの内容を医療機関等の責任者が確認すること。
9. 再委託が行なわれる場合は再委託先にも保守会社と同等の義務を課すこと。

D. 推奨されるガイドライン

1. 詳細なオペレーション記録を保守操作ログとして記録すること。
2. 保守作業時には病院関係者立会いのもとで行うこと。
3. 作業員各人と保守会社との守秘義務契約を求めること。
4. 保守会社が個人情報を含むデータを組織外に持ち出すことは避けるべきであるが、やむ得ない状況で組織外に持ち出さなければならない場合には、詳細な作業記録を残すことを求めること。また必要に応じて医療機関等の監査に応じることを求めること。
5. 保守作業にかかわるログの確認手段として、アクセスした診療録等の識別情報を時系列順に並べで表示し、かつ指定時間内でどの患者に何回のアクセスが行われたかが確認できる仕組みが備わっていること。

6.9 災害等の非常時の対応

B. 考え方

医療機関等は医療情報システムに不具合が発生した場合でも患者安全を配慮した医療サービスの提供が最優先されなければならない。

ここでは、「6.2.3 リスク分析」の「⑥医療情報システム自身」に掲げる自然災害やサイバー攻撃による IT 障害などの非常時に、医療情報システムが通常の状態で使用が出来ない事態に陥った場合における留意事項について述べる。

「通常の状態で使用できない」とは、システム自体が異常動作または停止になる場合と、使用環境が非定常状態になる場合がある。

前者としては、医療情報システムが損傷を被ることにより、システムの縮退運用あるいは全面停止に至り、医療サービス提供に支障発生が想定される場合である。

後者としては、自然災害発生時には多数の傷病者が医療サービスを求める状態になり、医療情報システムが正常であったとしても通常時のアクセス制御下での作業では著しい不合理の発生が考えられる場合である。この際の個人情報保護に関する対応は、「生命、身体の保護のためであって、本人の同意を得ることが困難であるとき」に相当すると解せられる。

(1) 非常時における事業継続計画(BCP : Business Continuity Plan)

非常事態が発生している最中では適切な意思決定は望み難いので、事前にできるだけ多くの意思決定を準備しておくことが望ましい。非常事態を事前に適切に分類することは難しく、可能な限り計画内容を事前演習などで検証することが望ましい。

医療施設として定められる BCP においては、医療情報システムについての計画を含め、全体としての整合性が必要である。

以下に、BCP としての策定計画と運用に関する一般項目を参考に掲げる。

① BCP として事前に周知しておく必要がある事項

事前に対応策を知ってもらい、信頼してもらっておくべきである。

- ポリシと計画
  何が「非常事態」なのかを理解し、定義すべきである。
- 非常事態検知手段
  災害や故障の検知機能と発生情報の確認手段
- 非常時対応チームの連絡先リスト、連絡手段および対策ツール
- 非常時に公にすべき文書および情報

② BCP 実行フェーズ

災害や事故の発生（或いは発生の可能性）を検知してから、BCP 実行か通常の障

害対策かの判断を行い、BCP 発動と判断した場合は関係者の召集、対策本部等の設置、関係先への連絡･協力依頼を行い、システムの切替／縮退等の準備を行う。例えば、ネットワークから切り離したスタンドアロンでの使用や、紙での運用等が考えられる。
業務委託先との間の連絡体制や委託先と一体となったトラブル対処方法等が明示されるべきである。
具体的項目は、「基本方針の策定」、「発生事象の確認」、「安全確保・安否確認」、および「影響度の確認」である。

③ 業務再開フェーズ
BCP を発動してから、バックアップサイト・手作業などの代替手段により業務を再開し、軌道に乗せるまでフェーズで、代替手段への確実な切り替え、復旧作業の推進、要員などの人的資源のシフト、BCP 遂行状況の確認、BCP 基本方針の見直しがポイントである。
最も緊急度の高い業務（基幹業務）から再開する。
具体的項目は「人的資源の確保」、「代替施設および設備の確保」、「再開／復旧活動の両立」、および「リスク対策によって新たに生じるリスクへの対策」である。

④ 業務回復フェーズ
最も緊急度の高い業務や機能が再開された後、さらに業務の範囲を拡大するフェーズで、代替設備や代替手段を継続する中での業務範囲の拡大となるため、現場の混乱に配慮した慎重な判断がポイントとなる。
具体的項目は「拡大範囲の見極め」、「業務継続の影響確認」、「全面復旧計画の確認」および「制限の確認」である。

⑤ 全面復旧フェーズ
代替設備・手段から平常運用へ切り替えるフェーズで、全面復旧の判断や手続きのミスが新たな業務中断を引き起こすリスクをはらんでおり、慎重な対応が要求される。
具体的項目は「平常運用への切り替えの判断」、「復旧手順の再確認」、「確認事項の整備」および「総括」である。

⑥ BCP の見直し
正常な状態に復帰した後に、BCP に関する問題点や見直しを検討することが必要である。実際の非常事態においては、通常では予想し得ないような事象が起こることも少なくない。実際の対応における成功点、失敗点を率直に評価、反省し、BCP

の見直しを行い、次の非常時に備えることが重要である。

(2) 医療システムの非常時使用への対応

① 非常時用ユーザアカウントの用意

- 停電、火災、洪水への対策と同様に、正常なユーザ認証が不可能な場合の対応が必要である。医療情報システムは使用可能であっても、使用者側の状況が定常時とは著しく違い、正規のアクセス権限者による操作が望めない場合に備えなくてはならない。例えば、ブレークグラスとして知られた方法では、非常時の使用に備えたユーザアカウントを用意し、患者データへのアクセス制限が医療サービス低下を招かないように配慮している。ブレークグラスでは非常時用ユーザアカウントは通常時の明示的な封印、使用状態に入ったことの周知、使用の痕跡を残すこと、定常状態に戻った後は新しい非常時ユーザアカウントへ変更をすることを基本としている。

② 災害時は、通常時とは異なる人の動きが想定される。例えば、災害時は、受付での患者登録を経ないような運用を考慮するなど、必要に応じて非常時の運用に対応した機能を実装すること。

上記の様な非常時使用への対応機能の用意は、関係者に周知され非常時に適切に用いる必要があるが、逆にリスクが増えることに繋がる可能性がある。不用意な使用を行わないために管理・運用は慎重でなくてはならない。

C. 最低限のガイドライン

1. 医療サービスを提供し続けるためのBCPの一環として"非常時"と判断する仕組み、正常復帰時の手順を設けること。すなわち、判断するための基準、手順、判断者、をあらかじめ決めておくこと。
2. 正常復帰後に、代替手段で運用した間のデータ整合性を図る規約を用意すること。
3. 非常時の情報システムの運用
   - 「非常時のユーザアカウントや非常時用機能」の管理手順を整備すること。
   - 非常時機能が定常時に不適切に利用されることがないようにし、もし使用された場合には使用されたことが多くの人にわかるようにする等、適切に管理および監査をすること。
   - 非常時用ユーザアカウントが使用された場合、正常復帰後は継続使用が出来ないように変更しておくこと。
4. サイバー攻撃で広範な地域での一部医療行為の停止など医療サービス提供体制に

支障が発生する場合は、別途定める所管官庁への連絡を行うこと。

6.10　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

B. 考え方

ここでは、組織の外部と情報交換を行う場合に、個人情報保護およびネットワークのセキュリティに関して特に留意すべき項目について述べる。外部と診療情報等を交換するケースとしては、地域医療連携で医療機関、薬局、検査会社等と相互に連携してネットワークで診療情報等をやり取りする、診療報酬の請求のために審査支払機関等とネットワークで接続する、ASP（Application Service Provider）型のサービスを利用する場合等が考えられる。

外部と医療情報を外部ネットワークを利用して交換する場合、送信元から送信先に確実に情報を送り届ける必要があり、「送付すべき相手に」、「正しい内容を」、「内容を覗き見されない方法で」送付しなければならない。すなわち、送信元の送信機器から送信先の受信機器までの間の通信経路において上記内容を担保する必要があり、送受信データに対する「盗聴」および「改ざん」、ネットワークに対する「侵入」および「妨害」などの脅威から守らなければならない。

ただし、本ガイドラインでは、これら全ての利用シーンを想定するのではなく、ネットワークを通じて医療情報を交換する際のネットワークの接続方式に関して幾つかのケースを想定して記述を行う。また、ネットワークが介在する際の情報交換における個人情報保護とネットワークセキュリティは考え方の視点が異なるため、それぞれの考え方について記述する。

なお、医療機関等が法令による義務の有無に関わらず、個人情報を含む医療情報の保存を外部に委託する場合は、情報の不適切な二次利用を防止する等、特段の個人情報保護に関する配慮が必要なため、８章に別途まとめて記述を行う。

B-1. 責任分界点の明確化

医療情報を外部に提供することは個人情報保護法上、委託と第三者提供の２種類があり、遵守すべき事項が異なる。

委託の場合、管理責任は提供元医療機関等にあり、契約と監督で管理責任を果たす責務があり、説明責任・結果責任を負わなければならない。提供先機関は契約遵守と報告義務を負う。

第三者提供の場合、提供元は同法第２３条で規定された例外を除き、「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ドライン」のⅢ－５－（３）－①のア～エに相当する場合は同ガイドラインで明記された方法で黙示の同意、それ以外の場合は明示の同意を得なければならない。また提供先は同法第１５条、第１６条にしたがって利用目的を特定し、同法および「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ドライン」にしたがって個人情報保護を達成する責務を負う。これらの要件を満たして提供された情報に対して提供元は責任を負わない。

オンラインで情報を提供する場合、情報の主体である患者と情報が乖離する。患者と乖離している間は情報を取り扱う事業者のどれかが責任を負う必要があり、どの事業者が責任を負っているかが明確で誤解のないものでなければならない。また患者にとっての苦情の申し入れ先や開示等の要求先が明白でなければならない。

提供元医療機関等、オンラインサービス提供事業者、回線提供事業者、提供先機関または提供先になる可能性がある事業者等が関係事業者になりえる。以下の原則で責任分界点を考える必要がある。

まず、提供元医療機関等と提供先機関は通信経路における責任分界点を定め、不通時や事故発生時の対処も含めて契約などで合意する必要がある。その上で、自らの責任範囲において、オンラインサービス提供事業者や回線提供事業者と管理責任の分担について責任分界点を定め、委託する管理責任の範囲および、サービスに何らかの障害が起こった際の対処をどの事業者が主体となって行うかを明らかにする必要がある。ただし、前述のように結果責任、説明責任は委託の場合は提供元事業者、第三者提供の場合は提供元医療機関等または提供先機関にあり、オンラインサービス提供事業者や回線提供事業者に生じるのは管理責任の一部のみであることに留意する必要がある。

回線事業者の提供する回線の発信元との責任分界点以前に適切に暗号化され、送信先との責任分界点以降に復号される場合は、回線事業者は盗聴の脅威に対する個人情報保護上の責務とは無関係である。ただし、改ざん、侵入、妨害の脅威に対する管理責任の範囲や回線の可用性等の品質に関しては契約で明らかにすること。

オンラインサービス提供事業者の管理範囲の開始される責任分界点に情報が到達する以前に適切に暗号化され、管理範囲の終了する責任分界点以降に復号される場合は、オンラインサービス提供事業者は盗聴の脅威に対する個人情報保護上の責務とは無関係である。ただし、改ざん、侵入、妨害の脅威に対する管理責任の範囲やサービスの可用性等の品質に関しては契約で明らかにすること。

法令で定められている場合などの特別な事情により、オンラインサービス提供事業者および回線提供事業者のいずれかに暗号化されていない医療情報が送信される場合は、オンラインサービスもしくは回線において盗聴の脅威に対する対策を施す必要があるため、当該医療情報の通信経路上の管理責任を負っている医療機関等はオンラインサービス提供事業者もしくは回線提供事業者と医療情報の管理責任についての明確化をおこない、オンラインサービス提供事業者もしくは回線提供事業者に対して管理責任の一部もしくは全部を委託する場合はそれぞれの事業者と個人情報に関する委託契約を適切に締結し、監督しなければならない。

提供元医療機関等と提供先機関が１対１通信である場合、または１対Ｎであってもあらかじめ提供先または提供先となる可能性がある機関を特定できる場合は委託または第三者提供の要件にしたがって両機関等が責務を果たさなければならない。

提供元医療機関等と提供先機関が１対Ｎ通信で、提供先機関が一つでも特定できない場

合は原則として医療情報を提供できない。ただし法令で定められている場合等の例外を除く。

リモートログイン機能を用いたデータアクセスには、代表的用途としてシステムメンテナンスを目的とした遠隔保守のためのアクセスが考えられる。しかし、制限がゆるいと一時保存しているディスク上の個人情報を含む医療情報の不正な読み取りや改ざんが行われる可能性もある。

他方、リモートログイン機能を全面的に禁止してしまうと、遠隔保守が不可能となり、保守に要する時間等の保守コストが増大する。適切に管理されたリモートログイン機能のみに制限しなければならない。

B-2. 医療機関等における留意事項

ここでは「B-1. 責任分界点の明確化」で述べた責任の内、ネットワークを通じて診療情報等を含む医療情報を伝送する場合の医療機関等における留意事項を整理する。

まず、医療機関等で強く意識しなくてはならないことは、情報を伝送するまでの医療情報の管理責任は医療機関等にあるということである。これは、情報の送信元である医療機関等から、情報が通信事業者の提供するネットワークを通じ、適切に送信先の医療機関等に受け渡しされるまでの一連の流れ全般において適用される。

ただし、誤解のないように整理しておくべきことは、ここでいう管理責任とは電子的に記載されている情報の内容であり、その記載内容や記載者の正当性の保持（真正性の確保）のことを指す。つまり、後述する「B-3. 選択すべきネットワークのセキュリティの考え方」とは対処すべき方法が異なる。例えば、同じ「暗号化」を施す処置としても、ここで述べている暗号化とは、医療情報そのものに対する暗号化を施す等して、仮に送信元から送信先への通信経路上で通信データの盗聴があっても第三者がその情報を判読できないようにしておく処置のことを指す。また、改ざん検知を行うために電子署名を付与することも対策のひとつである。一方、「B-3. 選択すべきネットワークセキュリティの考え方」で述べる暗号化とはネットワーク回線の経路の暗号化であり、情報の伝送途中で情報を盗み見られない処置を施すことを指す。

このような視点から見れば、医療機関等において情報を送信しようとする場合には、その情報を適切に保護する責任が発生し、次のような点に留意する必要がある。

①「盗聴」の危険性に対する対応

ネットワークを通じて情報を伝送する場合には、この盗聴に最も留意しなくてはならない。盗聴は様々な局面で発生する。例えば、ネットワークの伝送途中で仮想的な迂回路を形成して情報を盗み取ったり、ネットワーク機器に物理的な機材を取り付けて盗み取る等、明らかな犯罪行為であり、必ずしも医療機関等の責任といえない事例も想定される。一方で、不適切なネットワーク機材の設定により、意図しない情報漏洩や誤送信等も想定され、

このような場合には医療機関等における責任が発生する事例も考えられる。

このように様々な事例が考えられる中で、医療機関等においては、万が一、伝送途中で情報が盗み取られたり、意図しない情報漏洩や誤送信等が発生した場合でも、医療情報を保護するために適切な処置を取る必要がある。そのひとつの方法として医療情報の暗号化が考えられる。ここでいう暗号化とは、先に例示した通りであり、情報そのものの暗号化のことを指している。

どの程度の暗号化を施すか、また、どのタイミングで暗号化を施すかについては伝送しようとする情報の機密性の高さや医療機関等で構築している情報システムの運用方法によって異なるため、ガイドラインにおいて一概に規定することは困難ではあるが、少なくとも情報を伝送し、医療機関等の設備から情報が乖離する段階においては暗号化されていることが望ましい。

さらに、この盗聴防止については、例えばIDとパスワードを用いたリモートログインによる保守を実施するような時も同様である。その場合、医療機関等は上記のような留意点を保守委託業者等に確認し、監督する責任を負う。

②「改ざん」の危険性への対応

ネットワークを通じて情報を伝送する場合には、正当な内容を送信先に伝えることも重要な要素である。情報を暗号化して伝送する場合には改ざんへの危険性は軽減するが、通信経路上の障害等により意図的・非意図的要因に係わらず、データが改変されてしまう可能性があることは認識しておく必要がある。

また、後述する「B-3. 選択すべきネットワークセキュリティの考え方」のネットワークの構成によっては、情報を暗号化せずに伝送する可能性も否定できず、その場合には改ざんに対する対処は確実に実施しておく必要がある。なお、改ざんを検知するための方法としては、電子署名を用いる等が想定される。

③「なりすまし」の危険性への対応

ネットワークを通じて情報を伝送する場合、情報を送ろうとする医療機関等は、送信先の医療機関等が確かに意図した相手であるかを確認しなくてはならない。逆に、情報の受け手となる送信先の医療機関等は、その情報の送信元の医療機関等が確かに通信しようとする相手なのか、また、送られて来た情報が確かに送信元の医療機関等の情報であるかを確認しなくてはならない。これは、ネットワークが非対面による情報伝達手段であることに起因するものである。

そのため、例えば通信の起点と終点で医療機関等を適切に識別するために、公開鍵方式や共有鍵方式等の確立された認証の仕組みを用いてネットワークに入る前と出た後で相互に認証する等の対応を取ることが考えられる。また、改ざん防止と併せて、送信元の医療機関等であることを確認するために、医療情報等に対して電子署名を組み合わせることも

考えられる。

また、上記の危険性がサイバー攻撃による場合の対応は「6.9　災害等の非常時の対応」を参照されたい。

B-3. 選択すべきネットワークのセキュリティの考え方

ネットワークを介して外部と医療情報を交換する場合の選択すべきネットワークのセキュリティについては、責任分界点を明確にした上で、医療機関における留意事項とは異なる視点で考え方を整理する必要がある。ここでいうネットワークとは、医療機関等の情報送信元の機関の外部ネットワーク接続点から、同じく医療機関等の情報を受信する機関の外部ネットワーク接続点までのことを指し、医療機関等の内部で構成されるLANは対象とならない。ただし、「B-1. 責任分界点の明確化」でも触れた通り、接続先の医療機関等のネットワーク構成や経路設計によって意図しない情報漏洩が起こる可能性については留意をし、確認をする責務がある。

ネットワークを介して外部と医療情報を交換する際のネットワークを構成する場合、まず、医療機関等としては交換しようとする情報の機密度の整理をする必要がある。「B-2. 医療機関等における留意事項」では情報そのものに対する暗号化について触れているが、同様の観点から、情報の機密度に応じてネットワーク種別も選択しなくてはならない。基本的に医療情報をやり取りする場合、確実なセキュリティ対策は必須であるが、例えば、機密度の高くない情報に対して過度のセキュリティ対策を施すと、高コスト化や現実的でない運用を招く結果となる。つまり、情報セキュリティに対する分析を行った上で、コスト・運用に対して適切なネットワークを選択する必要がある。この整理を実施した上で、ネットワークにおけるセキュリティの責任分界点がネットワークを提供する事業者となるか、医療機関等になるか、もしくは分担となるかを契約等で明らかにする必要がある。その際の考え方としては、大きく次の2つに類型化される。

- 回線事業者とオンラインサービス提供事業者がネットワーク経路上のセキュリティを担保する場合

  回線事業者とオンラインサービス提供事業者が提供するネットワークサービスの内、これらの事業者がネットワーク上のセキュリティを担保した形で提供するネットワーク接続形態であり、多くは後述するクローズドなネットワーク接続である。また、現在はオープンなネットワーク接続であっても、Internet-VPNサービスのような通信経路が暗号化されたネットワークとして通信事業者が提供するサービスも存在する。

  このようなネットワークの場合、通信経路上におけるセキュリティに対して医療機関等は最終的な結果責任を負うにせよ、管理責任の大部分をこれらの事業者に委託できる。もちろん自らの医療機関等においては、善良なる管理者として注意義務を払い、組織的・物理的・技術的・人的安全管理等の規程に則り自医療機関等のシステムの安全管理を確

認しなくてはならない。

- 回線事業者とオンラインサービス提供事業者がネットワーク経路上のセキュリティを担保しない場合

例えば、インターネットを用いて医療機関等同士が同意の上、ネットワーク接続機器を導入して双方を接続する方式が考えられる。この場合、ネットワーク上のセキュリティに対して回線事業者とオンラインサービス提供事業者は責任を負わない。そのため、上述の安全管理に加え、導入されたネットワーク接続機器の適切な管理、通信経路の適切な暗号化等の対策を施さなくてはならず、ネットワークに対する正確な知識のない者が安易にネットワークを構築し、医療情報等を脅威にさらさないように万全の対策を実施する必要がある。

そのため、例えば情報の送信元と送信先に設置される機器や医療機関内に設置されている情報発信端末、端末に導入されている機能、端末の利用者等を確実に確認する手段を確立したり、情報をやり取りする機関同士での情報の取り扱いに関する契約の締結、脅威が発生した際に備えて、通信事業者がネットワーク経路上のセキュリティを担保する場合よりも厳密な運用管理規程の作成、専任の担当者の設置等を考慮しなくてはならない。

このように、医療機関等において医療情報をネットワークを通じて交換しようとする場合には、提供サービス形態の視点から責任分界点のあり方を理解した上でネットワークを選定する必要がある。また、選択するセキュリティ技術の特性を理解し、リスクの受容範囲を認識した上で、必要に応じて説明責任の観点から患者等にもそのリスクを説明する必要がある。

ネットワークの提供サービスの形態は様々存在するため、以降では幾つかのケースを想定して留意点を述べる。

Ｉ．クローズドなネットワークで接続する場合

ここで述べるクローズドなネットワークとは、業務に特化された専用のネットワーク網のことを指す。この接続の場合、いわゆるインターネットには接続されていないネットワーク網として利用されているものと定義する。このようなネットワークを提供する接続形式としては、「①専用線」、「②公衆網」、「③閉域 IP 通信網」がある。

これらのネットワークは基本的にインターネットに接続されないため、通信上における「盗聴」、「侵入」、「改ざん」、「妨害」の危険性は比較的低い。ただし、「B-2. 医療機関等における留意事項」で述べた物理的手法による情報の盗聴の危険性は必ずしも否定できないため、伝送しようとする情報自体の暗号化については考慮が必要である。また、ウイルス対策ソフトのウイルス定義ファイルや OS のセキュリティパッチ等を適切に適用し、コンピュータシステムの安全性確保にも配慮が必要である。

以下、それぞれの接続方式について特長を述べる。

①専用線で接続されている場合

専用線接続とは、2地点間においてネットワーク品質を保ちつつ、常に接続されている契約機関専用のネットワーク接続である。通信事業者によってネットワークの品質と通信速度（「帯域」という）等が保証されているため、拠点間を常時接続し大量の情報や容量の大きな情報を伝送するような場合に活用される。

ただし、品質は高いといえるが、ネットワークの接続形態としては拡張性が乏しく、かつ、一般的に高コストの接続形態であるため、その導入にあたってはやり取りされる情報の重要性と情報の量等の兼ね合いを見極める必要もある。

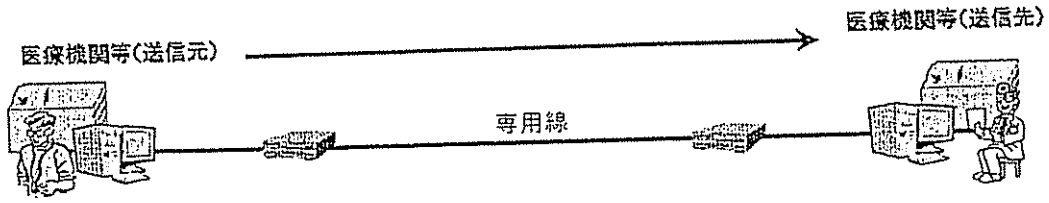


図 B-3-① 専用線で接続されている場合

②公衆網で接続されている場合

公衆網とはISDN（Integrated Services Digital Network）やダイアルアップ接続など、交換機を介した公衆回線を使って接続する接続形態のことを指す。

ただし、ここで想定する接続先はインターネットサービスプロバイダ（以下、ISP）に接続する接続方法ではなく、情報の送信元が送信先に電話番号を指定して直接接続する方式である。ISPを介して接続する場合は、ISPから先がいわゆるインターネット接続となるため、満たすべき要件としては後述する「Ⅱ．オープンなネットワークで接続する場合」を適用する。

この接続形態の場合、接続先に直接ダイアルしてネットワーク接続を確立するため、ネットワークを確立する前に電話番号を確認する等の仕組みを導入すれば、確実に接続先と通信ができる。

一方で、電話番号を確認する仕組みを用いなかったことによる誤接続、誤送信のリスクや専用線と同様で拡張性が乏しいこと、また、現在のブロードバンド接続と比べ通信速度が遅いため、大量の情報もしくは画像等の容量の大きな情報を送信する際に適用範囲を適切に見定める必要がある。

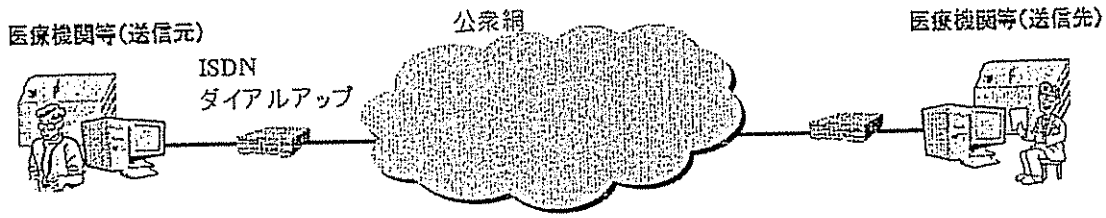


図 B-3-② 公衆網で接続されている場合

③閉域 IP 通信網で接続されている場合

ここで定義する閉域 IP 通信網とは、通信事業者が保有する広域ネットワーク網と医療機関等に設置されている通信機器とを接続する通信回線が他のネットワークサービス等と共用されていない接続方式を言う。このような接続サービスを本ガイドラインでは IP-VPN (Internet Protocol-Virtual Private Network) と呼び、クローズドなネットワークとして取り扱う。これに適合しない接続形態はオープンなネットワーク接続とする。主な利用形態としては、企業間における本店・支店間での情報共有網を構築する際に、遠隔地も含めた企業内 LAN のように利用され、責任主体が単一のものとして活用されることが多い。

この接続方式は、専用線による接続よりも低コストで導入することができる。また、帯域も契約形態やサービスの種類によっては確保できるため、大量の情報や容量の大きな情報を伝送することが可能である。

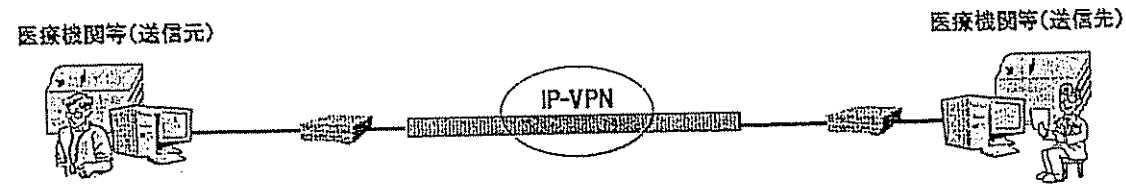


図 B-3-③-a 単一の通信事業者が提供する閉域ネットワークで接続されている場合

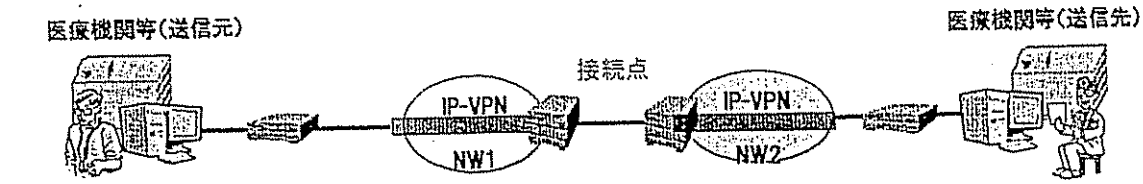


図 B-3-③-b 中間で複数の閉域ネットワークが相互接続して接続されている場合

以上の３つのクローズドなネットワークの接続では、クローズドなネットワーク内では外部から侵入される可能性はなく、その意味では安全性は高い。しかし、接続サービスだけでは一般に送られる情報そのものに対する暗号化は施されていない。また異なる通信事

業者のネットワーク同士が接続点を介して相互に接続されている形態も存在し得る。接続点を介して相互に接続される場合、送信元の情報を送信先に送り届けるために、一旦、送信される情報の宛先を接続点で解釈したり新たな情報を付加したりする場合がある。この際、偶発的に情報の中身が漏示する可能性がないとは言えない。電気通信事業法があり、万が一偶発的に漏示してもそれ以上の拡散は考えられないが、医療従事者の守秘義務の観点からは避けなければならない。そのほか、医療機関等から閉域IP通信網に接続する点など、一般に責任分界点上では安全性確保の程度が変化することがあり、特段の注意が必要である。

そのため、クローズドなネットワークを選択した場合であっても、「B-2. 医療機関等における留意事項」に則り、送り届ける情報そのものを暗号化して内容が判読できないようにし、改ざんを検知可能な仕組みを導入するなどの措置を取る必要がある。

Ⅱ. オープンなネットワークで接続されている場合

いわゆるインターネットによる接続形態である。現在のブロードバンドの普及状況から、オープンなネットワークを用いることで導入コストを削減したり、広範な地域医療連携の仕組みを構築したりする等、その利用範囲が拡大して行くことが考えられる。この場合、通信経路上では、「盗聴」、「侵入」、「改ざん」、「妨害」等の様々な脅威が存在するため、十分なセキュリティ対策を実施することが必須である。また、医療情報そのものの暗号化の対策を取らなければならない。

ただし、B-3の冒頭で述べたように、オープンなネットワークで接続する場合であっても、回線事業者とオンラインサービス提供事業者がこれらの脅威の対策のためネットワーク経路上のセキュリティを担保した形態でサービス提供することもある。医療機関等がこのようなサービスを利用する場合は、通信経路上の管理責任の大部分をこれらの事業者に委託できる。そのため、契約等で管理責任の分界点を明確にした上で利用することも可能である。

一方で、医療機関等が独自にオープンなネットワークを用いて外部と個人情報を含む医療情報を交換する場合は、管理責任のほとんどは医療機関等に委ねられるため、医療機関等の自己責任において導入する必要がある。また、技術的な安全性について自らの責任において担保しなくてはならないことを意味し、その点に留意する必要がある。

オープンなネットワーク接続を用いる場合、ネットワーク経路上のセキュリティの考え方は、「OSI (Open Systems Interconnection) 階層モデル※」で定義される7階層のうち、どこの階層でセキュリティを担保するかによって異なってくる。OSI 階層モデルを基本としたネットワーク経路上のセキュリティの詳細については「「医療情報システムの安全管理に関するガイドライン」の実装事例に関する報告書（保健・医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアム；HEASNET）；平成19年2月」が参考になる。

※OSI 階層モデル（Open System Interconneciton）

開放型システム間相互接続のことで、異種間接続を実現する国際標準のプロトコール。

第7層	アプリケーション層	FTPやMail等のサービスをユーザに提供
第6層	プレゼンテーション層	データを人に分かる形式、通信に適した形式に変換
第5層	セッション層	データ経路の確立と開放に関係する層
第4層	トランスポート層	データを確実に届ける為に規定されている層
第3層	ネットワーク層	アドレス管理と経路の選択だめの層
第2層	データリンク層	物理的通信経路の確立するために規定されている層
第1層	物理層	ビットデータを電気的、物理的に変換。機器の形状・特性を規定している層

例えば、SSL-VPN を用いる場合、5 階層目の「セッション層」と言われる部分で経路の暗号化手続きがなされるため、正しく経路が暗号化されれば問題ないが、経路を暗号化する過程で盗聴され、適切でない経路を構築されるリスクが内在する。一方、IPSec を用いる場合は、2 階層目もしくは 3 階層目の「ネットワーク層」と言われる部分より下位の層で経路の暗号化手続きがなされるため、SSL-VPN よりは危険度が低いが、経路を暗号化するための暗号鍵の取り交しに IKE（Internet Key Exchange）といわれる標準的手順を組み合わせる等して、確実にその安全性を確保する必要がある。

このように、オープンなネットワーク接続を利用する場合、様々なセキュリティ技術が存在し、内在するリスクも用いる技術によって異なることから、利用する医療機関等においては導入時において十分な検討を行い、リスクの受容範囲を見定める必要がある。多くの場合、ネットワーク導入時に業者等に委託をするが、その際には、リスクの説明を求め、理解しておくことも必要である。

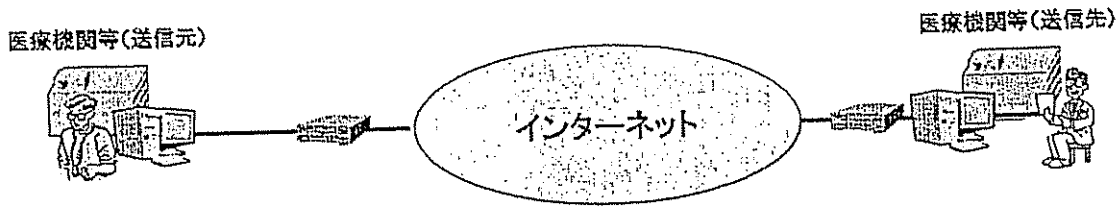


図 B-3-④　オープンネットワークで接続されている場合

（患者等に診療情報等を提供する場合）

診療情報等の開示が進む中、ネットワークを介して患者（または家族等）に診療情報等を提供する、もしくは医療機関内の診療情報等を閲覧する可能性も出てきた。本ガイドラインは、医療機関等間における情報のやり取りを想定しているが、今後、このような事例も十分想定される。そのため、ここでその際の考え方について触れる。ただし、ここで触れる考え方は、医療機関等が自ら実施して患者等に情報を提供する場合であり、第 8 章で定める診療録及び診療諸記録を外部に保存している場合は、第三者に委託しており、委託

先が情報提供を行うことになるため想定しない。

ネットワークを介して患者等に診療情報等を提供する場合、第一に意識しておかなければならないことは、情報を閲覧する患者等のセキュリティ知識と環境に大きな差があるということである。また、一旦情報を提供すれば、その責任の所在は医療機関等ではなく、患者等にも発生する。しかし、セキュリティ知識に大きな差がある以上、情報を提供する医療機関等が患者等の納得が行くまで十分に危険性を説明し、その提供の目的を明確にする責任があり、説明が不足している中で万が一情報漏洩等の事故が起きた場合は、その責任を逃れることはできないことを認識しなくてはならない。

また、今まで述べてきたような専用線等のネットワーク接続形態で患者等に情報を提供することは、患者等が自宅に専用線を敷設する必要が生じるため現実的ではなく、提供に用いるネットワークとしてはオープンネットワークを介することになる。この場合、盗聴等の危険性は極めて高く、かつ、その危険を回避する術を患者等に付託することも難しい。

医療機関等における基本的な留意事項は、既に B-1 や B-2 で述べられているが、オープンネットワーク接続であるため利活用と安全面両者を考慮したセキュリティ対策が必須である。特に、患者等に情報を公開しているコンピュータシステムを通じて、医療機関等の内部のシステムに不正な侵入等が起こらないように、システムやアプリケーションを切り分けしておく必要がある。そのため、ファイアウォール、アクセス監視、通信の SSL 暗号化、PKI 個人認証等の技術を用いる必要がある。

このように、患者等に情報を提供する場合には、ネットワークのセキュリティ対策のみならず、医療機関等内部の情報システムのセキュリティ対策、情報の主体者となる患者等へ危険性や提供目的の納得できる説明、また非 IT に係わる各種の法的根拠等も含めた幅広い対策を立て、それぞれの責任を明確にした上で実施しなくてはならない。

C. 最低限のガイドライン

1. ネットワーク経路でのメッセージ挿入、ウイルス混入などの改ざんを防止する対策をとること。
   施設間の経路上においてクラッカーによるパスワード盗聴、本文の盗聴を防止する対策をとること。
   セッション乗っ取り、IP アドレス詐称などのなりすましを防止する対策をとること。
   上記を満たす対策として、例えば IPSec と IKE を利用することによりセキュアな通信路を確保することがあげられる。

2. データ送信元と送信先での、拠点の出入り口・使用機器・使用機器上の機能単位・利用者の必要な単位で、相手の確認を行う必要がある。採用する通信方式や運用

規程により、採用する認証手段を決めること。認証手段としてはPKIによる認証、Kerberosのような鍵配布、事前配布された共通鍵の利用、ワンタイムパスワードなどの容易に解読されない方法を用いるのが望ましい。

3. 施設内において、正規利用者への成りすまし、許可機器への成りすましを防ぐ対策をとること。これに関しては、医療情報の安全管理に関するガイドライン「6.5 技術的安全対策」で包括的に述べているので、それを参照すること。

4. ルータなどのネットワーク機器は、安全性が確認できる機器を利用し、施設内のルータを経由して異なる施設間を結ぶ VPN の間で送受信ができないように経路設定されていること。安全性が確認できる機器とは、例えば、ISO15408で規定されるセキュリティターゲットもしくはそれに類するセキュリティ対策が規定された文書が本ガイドラインに適合していることを確認できるものをいう。

5. 送信元と相手先の当事者間で当該情報そのものに対する暗号化などのセキュリティ対策を実施すること。たとえば、SSL/TLSの利用、S/MIMEの利用、ファイルに対する暗号化などの対策が考えられる。その際、暗号化の鍵については電子政府推奨暗号のものを使用すること。

6. 医療機関間の情報通信には、当該医療機関等だけでなく、通信事業者やシステムインテグレータ、運用委託事業者、遠隔保守を行う機器保守会社など多くの組織が関連する。
そのため、次の事項について、これら関連組織の責任分界点、責任の所在を契約書等で明確にすること。

- 診療情報等を含む医療情報を、送信先の医療機関等に送信するタイミングと一連の情報交換に係わる操作を開始する動作の決定
- 送信元の医療機関等がネットワークに接続できない場合の対処
- 送信先の医療機関等がネットワークに接続できなかった場合の対処
- ネットワークの経路途中が不通または著しい遅延の場合の対処
- 送信先の医療機関等が受け取った保存情報を正しく受信できなかった場合の対処
- 伝送情報の暗号化に不具合があった場合の対処
- 送信元の医療機関等と送信先の医療機関等の認証に不具合があった場合の対処
- 障害が起こった場合に障害部位を切り分ける責任
- 送信元の医療機関等または送信先の医療機関等が情報交換を中止する場合の対

処

また、医療機関内においても次の事項において契約や運用管理規程等で定めておくこと。

- 通信機器、暗号化装置、認証装置等の管理責任の明確化。外部事業者へ管理を委託する場合は、責任分界点も含めた整理と契約の締結。
- 患者等に対する説明責任の明確化。
- 事故発生時における復旧作業・他施設やベンダとの連絡に当たる専任の管理者の設置。
- 交換した医療情報等に対する結果責任の明確化。
  個人情報の取扱いに関して患者から照会等があった場合の送信元、送信先双方の医療機関等への連絡に関する事項、またその場合の個人情報の取扱いに関する秘密事項。

7. リモートメンテナンスを実施する場合は、必要に応じて適切なアクセスポイントの設定、プロトコルの限定、アクセス権限管理等を行って不必要なログインを防止すること。
   また、メンテナンス自体は「6.8 章　情報システムの改造と保守」を参照すること。

8. 回線事業者やオンラインサービス提供事業者と契約を締結する際には、脅威に対する管理責任の範囲や回線の可用性等の品質に関して問題がないか確認すること。また上記１および４を満たしていることを確認すること。

10　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きわめて重要であり、運用管理規程は必ず定めなければならない。

A. 制度上の要求事項

1)　平成16年の「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ドライン」

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

－－－個人情報の取扱いに関する明確かつ適正な規則を策定し、それらを対外的に公表することが求められる。

－－－個人情報の取扱いに関する規則においては、個人情報に係る安全管理措置の概要、本人等からの開示等の手続き、第三者提供の取扱い、苦情への対応等について具体的に定めることが考えられる。

Ⅲ　4 (2) ①個人情報保護に関する規程の整備、公表

－－－個人情報保護に関する規程を整備し、－－－。

個人データを取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。

2)　その他の要求事項

○診療録等の電子保存を行う場合の留意事項

(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。

①　運用管理を総括する組織・体制・設備に関する事項

②　患者のプライバシー保護に関する事項

③　その他適正な運用管理を行うために必要な事項

(施行通知　第三)

○電子媒体により外部保存を行う際の留意事項

(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。

(外部保存改正通知　第３)

B. 考え方

運用管理規程には、システムの導入に際して、「法令に保存義務が規定されている診療録及び診療諸記録の電子媒体による保存に関する基準」や「診療録等の外部保存を行う際の基準」を満足するために技術的に対応するか、運用によって対応するかを判定し、その内容を公開可能な状態で保存する旨を盛り込まなければならない。

医療機関等には規模、業務内容等に応じて様々な形態があり、運用管理規程もそれに伴い様々な様式・内容があると考えられるので、ここでは、本書の 6 章から 9 章の記載に従い、定めるべき管理項目を記載してある。(1) に電子保存する・しないに拘らず必要な一般管理事項を、(2) に電子保存の為の運用管理事項を、(3) に外部保存のための運用管理事項を、(4) にスキャナ等を利用した電子化、そして終わりに運用管理規程の作成にあたっての手順を記載している。

電子保存を行う医療機関等は (1) (2) (4) の管理事項を、電子保存に加えて外部保存をする医療機関等では、さらに (3) の管理事項を合わせて採用する必要がある。

C. 最低限のガイドライン

以下の項目を運用管理規程に含めること。本指針の 6 章から 9 章において「推奨」に記されている項目は省略しても差し支えない。

(1) 一般管理事項

① 総則

a) 理念

b) 対象情報

② 管理体制

a) システム管理者、機器管理者、運用責任者の任命

b) 作業担当者の限定

c) マニュアル・契約書等の文書の管理

d) 監査体制と監査責任者の任命

e) 苦情の受け付け窓口の設置

f) 事故対策

g) 利用者への周知法

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

監査証跡の取組方については、「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～（(財) 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
b) 情報保存装置、アクセス機器の設置区画の管理・監視
c) 委託契約における安全管理に関する条項
d) 個人情報の記録媒体の管理（保管・授受等）
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
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利用者識別と認証、アクセス権限管理、アクセスログ取得と監査、時刻同期、ウイルス等不正ソフト対策

⑤ 教育と訓練

a) マニュアルの整備
b) 定期また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

⑥ 業務委託の安全管理措置

a) 業務委託契約における守秘条項
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データ参照
  - 保守要員専用のアカウントの作成及び運用管理
  - 作業時の病院関係者の監督
  - 保守契約における個人情報保護の徹底
  - メッセージログの採取と確認

⑦ 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

⑧ 災害等の非常時の対応

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規程

c) 非常時の機能と運用規程

d) 報告先と内容一覧

⑨ 外部と医療情報を交換する場合

a) 安全を技術的、運用的面から確認した文書の管理

b) リスク対策の検討文書の管理

c) 責任分界点を定めた契約文書の管理

d) リモートメンテナンスの基本方針

⑩ 規程の見直し

運用管理規程の定期的見直し手順

(2) 電子保存の為の運用管理事項

① 真正性確保

a) 作成者の識別及び認証

b) 情報の確定手順と、作成責任者の識別情報の記録

c) 更新履歴の保存

d) 代行操作の承認記録

e) 一つの診療録等を複数の医療従事者が共同して作成する場合の管理

f) 機器・ソフトウェアの品質管理

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

- 診療目的
- 患者説明
- 監査
- 訴訟

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

c) 記録媒体、設備の劣化による読み取り不能または不完全な読み取りの防止策

d) 媒体・機器・ソフトウェアの整合性不備による復元不能の防止策

e) 万が一に備えての考慮対策

f) 情報の継続性の確保策（例えば、媒体の劣化対策等）

g) 情報保護機能策（例えば、バックアップ等）

④ 相互利用性確保

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」

可搬型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「医療機関等としての管理事項」を作成すること。

① 管理体制と責任

a) 委託に値する事業者と判断した根拠の記載
受託機関が医療機関等以外の場合には、8.1.2「外部保存を受託する機関の限定」に記された要件を参照のこと。

b) 委託元での管理責任者

c) 受託機関への監査体制

d) 保存業務受託機関との責任分界点

e) 受託機関の管理責任、説明責任、結果責任の範囲を明文化した契約書等の文書作成と保管

f) 事故等が発生した場合における対処責任、障害部位を切り分ける責任所在を明文化した契約書等の文書作成と保管
受託機関が医療機関等以外の場合には、8.1.2「外部保存を受託する機関の限定」に記された要件を参照のこと。

② 外部保存契約終了時の処理

受託先に診療録等が残ることがない様な処理法

a) 受託先に診療録等が残ることがないことの受託先との契約、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

c) リモートログイン制限機能

④ 見読性確保

a) 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

b) 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

＊ 上記事項は推奨

⑤ 保存性確保

a) 外部保存を受託する機関での保存確認機能

b) 標準的なデータ形式及び転送プロトコルの採用

＊ 上記事項は推奨

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

d) 電気通信回線や外部保存を受託する機関の設備の劣化対策

e) 電気通信回線や外部保存を受託する機関の設備の互換性確保

＊ 上記事項は推奨

f) 情報保護機能

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

受託機関が医療機関等以外の場合には、8.1.2「外部保存を受託する機関の限定」に記された要件を参照のこと。

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 患者への説明と同意

a) 診療開始前の同意

b) 患者本人の同意を得ることが困難であるが、診療上の緊急性がある場合

c) 患者本人の同意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

⑨ 受託機関への監査項目

a) 保存記録（内容、期間等）

b) 受託機関側での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の同一性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(実施者または管理者)の電子署名及び認証業務に関する法律(電子署名法)に適合した電子署名

④ スキャナ読み取り電子情報への正確な読み取り時刻の付加

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

＜運用管理規程の作成にあたって＞

運用管理規程は、電子保存及び外部保存の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。即ち、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。

勿論、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ける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。

具体的な作成手順は以下のとおりである。

ステップ 1：全体の構成及び目次の作成

全体の章立てと節の構成を決める場合に、付表の「運用管理項目」、「実施項目」から選

択し、医療機関等ごとの独自性を一部変更する方法で全体の構成を作成する。

この際、電子保存及び外部保存のシステムに関する運用管理規程だけではなく、医療情報システム全体の総合的な運用管理規程の構成とすることが重要である。

ステップ２：運用管理規程文の作成

運用管理規程文の作成には、付表の「運用管理規程文例」から選択し、医療機関等ごとの独自性を一部変更する方法で作成する。

特に、大規模／中規模病院用と小規模病院／診療所用では、運用管理規程文の表現が大きく異なることを想定して、付表に「対象区分」欄を設けている。大規模／中規模病院の場合は、対象区分のＡとＢの運用管理規程文例を選択し、小規模病院／診療所の場合は、対象区分のＡとＣの運用管理規程文例を選択することを推奨する。

ステップ３：全体の見直し及び確認評価

運用管理規程の全体が作成された段階で、医療機関等の内部の関係者等にレビューを行い、総合的視点で実施運用が可能か評価し改善する。

なお、運用管理規程は単に策定すれば良いと言うものではなく、策定（Plan）された管理規程に基づいた運用（Do）を行い、適切な監査（Check）を実施し、必要に応じて改善（Action）していかねばならない。この PDCA サイクルを適切に廻しながら改善活動を伴う継続的な運用を行うことが重要である。

別添

「写」

保発第 0220004 号
平成２０年２月２０日

都道府県知事　殿
地方社会保険事務局長　殿
地方厚生（支）局長　殿

厚生労働省保険局長

光ディスク等を用いた費用の請求に関して厚生労働大臣が定める方式及び規格並びに電子情報処理組織の使用による費用の請求に関して厚生労働大臣が定める事項及び方式について

療養の給付、老人医療及び公費負担医療に関する費用の請求に関する省令（昭和５１年厚生省令第３６号）第三条第一項及び附則第四条第二項の規定に基づき、光ディスク等を用いた費用の請求に関して厚生労働大臣が定める方式及び規格並びに電子情報処理組織の使用による費用の請求に関して厚生労働大臣が定める事項及び方式（平成１８年４月１０日保発第 0410006 号の別紙。以下「別紙」という。）について下記のとおり一部変更したので、通知する。

記

１．　変更内容について

別紙の別添１－１、別添１－２及び別添１－３それぞれの第 2 章の１中「IP-VPN 接続」の次に「、または、オープンなネットワークにおいてはIPsec（IETF(Internet Engineering Task Force)において標準とされた、IP(Internet Protocol)レベルの暗号化機能。認証や暗号のプロトコル、鍵交

換のプロトコル、ヘッダー構造など複数のプロトコルの総称）とIKE（Internet Key Exchange；IPsecで用いるインターネット標準の鍵交換プロトコル）を組み合わせた接続」を加える。

2．　適用日について

平成２０年５月１日から適用することとする。