Part 1 ―ガイドラインを読み解く
医療従事者が知っておくべき医療情報受託ガイドラインのポイント

小尾　高史　東京工業大学総合理工学研究科
大山　永昭　東京工業大学像情報工学研究所

（おび　たかし）
1995年東京工業大学大学院総合理工学研究科物理情報専攻博士後期課程満期退学。同大学工学部附属像情報工学研究施設教務職員を経て，97年同助手。2003年同大学総合理工学研究科物理情報システム専攻助教授。2008年に同准教授となり，現在に至る。専門分野は，医療画像処理，情報セキュリティ。博士（工学）。

（おおやま　ながあき）
1982年東京工業大学大学院総合理工学研究科物理情報工学専攻博士課程修了。83年同大学工学部附属像情報工学研究施設助手。86年から87年までアリゾナ大学放射線科研究員（画像再構成についての研究）。88年東京工業大学工学部附属像情報工学研究施設助教授，93年同教授となり，現在に至る。専門分野は医用画像工学，光情報処理。工学博士。

はじめに

医療情報の電子化は，医療分野の情報化を進める上できわめて重要なことであるが，他方，意図しない情報漏えいなどの危険性があり，いったん個人医療情報が漏えいした場合，個人の権利・利益が大きく侵害されるとともに，その回復が非常に困難である。

このような状況において，個人情報保護法およびそれに基づく医療分野でのガイドライン策定が進められ，現在，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4.1版」（以下，医療情報システムガイドラインという）[1]，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」[2]，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」（以下，医療情報受託ガイドラインという）[3]が整備されている。本稿では，これらのガイドラインの関係に配慮しながら，主として医療情報受託ガイドラインに関して，医療関係者が押さえるべきポイントを解説する。

安全管理上の要求事項

医療情報受託ガイドラインは，2008年3月に厚生労働省により改訂された医療情報システムガイドライン第3版[4]を受けて，2008年7月に経済産業省により策定されたものであり，医療機関から医療情報を受託する情報処理事業者が講ずべき安全管理措置について定められたガイドラインである。全3章からなるが，2章が医療情報受託事業者における安全管理上の要求事項となっており，医療情報受託ガイドラインの骨子となる。以下では，2章の内容について目次順に沿って主なポイントを示すので，医療機関などが受託事業者を選定，契約する場合などに役立てていただきたい。

1. 医療情報受託事業者に対する公正な第三者認証取得の奨励

医療情報受託ガイドラインには，医

療情報受託事業者がガイドラインの記述に沿ってISMS（Information Security Management System）認証を取得する際の注意点が記述されている。したがって，医療機関が実際に医療情報の保存などを委託するために情報処理事業者を選定，委託する際は，事業者が作成した適用宣言書などを用いて，候補となる事業者がISMS認証を取得していることを確認することが必要である。さらに委託後も，定期的に監査結果の提供を求め，適切な安全管理策を講じているかを確認することが必要である。

2. 情報資産管理の実施

情報処理事業者は，自己の保有する医療情報システムだけでなく，医療機関などから委託された情報についても，資産管理台帳を作成管理することが必要であるとされている。また，受託した情報を適切に分類し，区分管理を実施するために必要となる要求事項が示されており，これは，2.7節に記述されているグループ管理に基づく情報へのアクセス制御を実現するために必要な要件となっている。これらについても，医療機関などは受託事業者が作成管理する関連書類などを用いて，必要な要件を満たしていることを確認することが必要である。

3. 組織的安全管理策

情報処理システムを構成するハードウエア，ソフトウエアについて責任者を定め，それを文書化し管理すること，情報処理の安全管理に関する手順書の作成や，運用管理規定の整備などが組織的安全管理策の要件として挙げられている。ここで，これらの手順書，規定については，この節以降で記述されている入退出管理やアクセス管理などにかかわる手順書，規定の策定を含んでいることに注意が必要である。

4. リスク評価

医療情報受託ガイドラインでは，主として情報の伝達経路におけるリスク評価の必要性が述べられている。ISMS認証を導入している事業者は，リスクアセスメントを実施しているため，それを基本としてより詳細なリスク評価を行う必要がある。そして，その結果を踏まえて，情報処理事業者は，リスク対応措置の内容を医療機関などと協議し，その内容について合意することが必要である。この時，医療機関などは，自己が実施する医療情報に対するリスクアセスメントの内容と情報処理事業者が行うリスク対応の内容との間に，整合性がとれているかを確認することが重要である。

5. 物理的安全対策

物理的安全対策では，情報システムを格納する建物の管理，入退出管理の実施，データの盗難の防止などの措置に関する要件が挙げられている。特に，医療情報処理設備専用のサーバラックの設置要求や入退室管理おける2要素認証の実施など，厳格な安全対策を求めている点が特徴である。本件についても，医療機関などは受託事業者が要件を満たしていることを確認することが必要である。

6. 技術的安全対策

技術的対策は，医療情報受託ガイドラインにおいてもっとも多くのページを割いている部分であり，システム保守，ネットワーク，情報交換，バックアップ施設，使用するアプリケーション，個人データおよびそれを取り扱う医療情報システムへのアクセス制御，不正ソフトウエア対策，医療情報システムの監視，ID管理等，医療情報に対する技術的な安全管理措置に必要な各種要件が挙げられている。

ここで挙げられている要件については，安全性の担保だけではなく，サービスの品質にかかわるものも多いため，医療情報受託ガイドラインに記載されていない事項については，情報処理事業者と医療機関などとの間であらかじめ合意し，その内容を契約書もしくはSLA（Service Level Agreement）などに明文化することが必要である。

また，医療情報受託ガイドラインには，物理的安全対策について入退出管理などでICカードなどを利用した2要素以上の認証を要求している反面，情報システムに対するアクセス制御時にはパスワード認証に関する要求事項しか記述されていない。しかしながら，医療情報システムガイドラインでは，推奨される認証手段として，ID＋バイオメトリクス，あるいはICカードなどのセキュリティデバイス＋パスワード，またはバイオメトリクスなどを利用した2要素認証の採用が示されている。そのため，医療機関などは，情報処理事業者が用いている情報システムについて，この点を十分に考慮することが望まれる。

7. 人的安全対策

人的安全対策としては，従業者に対して業務上秘密と指定された個人データの非開示契約の締結や教育・訓練などを行うことを求めている。これらの点についても，受託事業者の対策を確認することが必要である。

8. その他

このほか医療情報受託ガイドラインには，情報の破棄，事業継続計画なども記載されている。これらの内容は，通常，適用宣言書に記載されるため，医療情報を委託する医療機関は，ガイドラインに沿って適用宣言書が作成されているかを委託前に確認することが必要である。

ガイドライン参照時の留意点

ここでは，医療情報受託ガイドラインを参照する上で留意すべき点について述べる。

医療情報受託ガイドラインで想定する情報処理システムは，インターネットに直接接続されることはないものとされており，現時点ではファイアウォールなどを介して情報処理システムをインターネットに間接的に接続することも想定していない。したがって，現時点で医療機関などは，情報処理業者の保有するシステムを利用して患者などへ直接的に情報提供を行うことや，PHRなどの外部健康情報管理システムとの連携を実施することはできないと解釈される。しかしながら，医療情報システムガイドライン第4.1版や「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」では，患者に情報を閲覧させる場合の要求事項が記述されていることから，今後医療情報受託ガイドラインにおいても，このような利用形態に対応するよう改訂が進められることが期待される。

また，現在の医療情報受託ガイドラインは，主として正常運用時を想定した内容となっており，医療情報に何らかの不都合な事態が生じた場合に講じるべき対策については，詳細に触れられていない。しかし，医療情報システムガイドラインに記載されているように，委託事業者および医療機関などは連携して「説明責任」と「善後策を講じる責任」を果たす必要があることから，障害などが生じた場合に責任をいかに分担するか，言い換えると責任範囲とその分界点などを明確にし，あらかじめ双方で合意するとともに，委託契約に明記する必要があることに十分注意すべきである。

おわりに

医療情報受託ガイドラインは，医療情報システムガイドライン第3版をベースとしているため，一部ほかのガイドラインと整合性がとれていない箇所があり，今後その改訂が行われると予想される。当然ながら医療情報受託ガイドラインの目的は，医療情報の安全性担保を図るためのものであるが，患者のプライバシー保護だけでなく，医療情報の活用による医療の質の向上などへつなげていくことが重要である。今後，医療情報を活用する際に，どのようにして安全性を担保すればよいかという点を含めたガイドラインへと発展していくことを期待する。

●参考文献
1) 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4.1版．2010.（http://www.mhlw.go.jp/shingi/2010/02/dl/s0202-4a.pdf）
2) 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.（http://www.soumu.go.jp/main_content/000095031.pdf）
3) 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．2008.（http://www.meti.go.jp/policy/it_policy/privacy/080724iryou-kokuzi.pdf）
4) 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3版．2008.（http://www.mhlw.go.jp/shingi/2008/07/dl/s0730-18g.pdf）

TOPICS

「健康情報活用基盤（PHR）構築のための標準化及び実証事業」の成果報告会を開催

経済産業省は，「健康情報活用基盤（PHR）構築のための標準化及び実証事業」の成果報告会を2月14日（月）に科学技術館（東京都千代田区）で開催する。

同実証事業は，2008年度から3年間の計画で進められてきたが，最終年度を終えるにあたり，最終成果を報告するシンポジウムを開催する。実証事業では，総務省，厚生労働省と連携して，PHRの構築と運用に必要な技術的・制度的な要件の検討を中心に取り組んできた。

報告会開催にあたって，同事業の全体委員会委員長を務める山本隆一氏（東京大学大学院情報学環・准教授）は，事業の意義について次のようにコメントしている。

「糖尿病や高脂血症などの生活習慣に起因する疾患が増加する中，わが国では，医療は社会保障的な位置付けとなっているが，今後，欧米のような自己責任での健康管理が重要となる。慢性疾患では，長期的な生活習慣の改善が重要だが，個人が独力で取り組むのは困難で，個人の健康情報を一元的に集約し，自己管理を行える環境を構築し必要に応じて第三者に開示して，健康維持・向上を行うためのサポートが受けられる環境を構築・実証するために立ち上げたのが本事業だ」

個人が健康情報を管理する時代へ

シンポジウムでは，4つの実証コンソーシアムからの成果報告，「医療・健康情報を個人が管理する時代に向けて」と題したパネルディスカッションなどが行われる。山本氏は，シンポジウムで発表される成果が，今後の医療・健康情報の活用の方向性を示すと期待する。

「本事業によって，個人が自分の健康状態を自己責任において管理し，必要に応じて健康サービス産業のサポートが受けられる環境が整備された。これまで机上検討のみであった，健康情報活用基盤や，当該基盤を活用した健康サービス産業のあり方や可能性を示すことができた。“どこでもMY病院”や“シームレスな地域連携医療”などにおいても，健康情報の管理・活用は強調されている。本事業成果は，今後のわが国の医療健康情報の活用と新たな産業の発展について考察する上で非常に有益な成果だと言えるだろう」

問い合わせおよびプログラムの詳細は，アクセンチュア（http://www.accenture.com/jp/phr）まで。

Part 2 ―安全管理のための認定・サービス

HISPROが提供する医療情報システムの安全管理の事業

喜多　紘一　保健医療福祉情報安全管理適合性評価協会理事長

（きた　こういち）
保健医療福祉情報安全管理適合性評価協会（HISPRO）理事長。株式会社東芝医用機器事業部（現・東芝メディカルシステムズ株式会社），国際医療福祉大学特任教授，財団法人医療情報システム開発センター審議役兼プライバシーマーク付与認定審査室長，東京工業大学統合研究院特任教授を経て現在に至る。厚生労働省医療情報ネットワーク基盤検討会構成員を務める。

はじめに

「新たな情報通信技術戦略」において，「地域の絆の再生」として「『どこでもMY病院』構想の実現」あるいは「シームレスな地域連携医療の実現」が掲げられている。また，「地域医療再生基金」の「地域医療における情報連携のモデル的プラン」の中では，「地域医療連携情報システム（XDS：Cross-Enterprise Document Sharing）」が紹介されている。

こうした地域連携システムを実現するためには，ネットワークを通じた情報システムの活用が必要になり，従来の院内システムに比べて，高度な知識と技術が要求される。ほかの分野では，利用者はサーバを保有せずに利用料を払えば，ネットワークサービスを受けられるASP（Application Service Provider）・SaaS（Software as a Service）の利用が進められ，利用者のシステム管理の負担を軽減させている。しかし，医療情報システムは，ネットワークや情報処理機器のセキュリティの確保がより重要であり，医療機関などや関係者には格別の安全管理措置が義務づけられている。こうした要求が，ネットワークを通じたASP・SaaSサービスを医療分野で活用するには，高いハードルとなっていた。

このような状況の中で，総務省，経済産業省によって「医療情報システムの安全管理に関するガイドライン　第4.1版」（厚生労働省）[1]に沿った各種ガイドライン[2)~5)]が整備され，医療施設の外で医療情報を取り扱う場合の対応方法が明確化されてきた。

これを踏まえ，2010年2月に外部保存通知[6]が改正された。上記の各種ガイドラインの順守を前提に，これまで外部保存に係る場所のうち，「医療機関等が震災対策等の危機管理上の目的で確保した安全な場所」という箇所が「医療機関等が民間事業者等との契約に基づいて確保した安全な場所」に改正され，ASP・SaaSの利用への道が開かれた。

しかし，こうしたサービスを利用する場合，医療機関などはそのサービスが，自施設の置かれた脅威に合った安全対策がなされたものであり，各種ガイドラインに適合しているか確認する必要があり，それなりの知識と時間が要求される。こうした状況で，システムサービス提供者の提供するサービスが，各種ガイドラインなどに適合しているかをユーザー視点で評価することを目的とした，日本医師会，日本薬剤師会，日本歯科医師会，および日本医療情報学会の4団体を社員とする，一般社団法人保健医療福祉情報安全管理適合性評価協会（以下，HISPROという）[7]が設立された。HISPROの設立により，ユーザーが評価する場合の負担の軽減ばかりでなく，システムサービス提供者も自分の提供するネットワークサービスがガイドラインに適合しているかを客観的に提示し，サービスの透明性を図れるようになった。

本稿では，HISPROの趣旨や概要，現在の活動状況について，医療関係者向けにポイントをご解説する。

HISPROの業務

図1に業務イメージを示す。HISPROはユーザーの立場で，チェックリストに基づいてネットワークやサーバの各種ガイドラインへの適合性を評価する。行政，社会保険診療報酬支払基金（以下，支払基金という）や医療機関などは，その評価を自己組織内で判断して，各種認定や必要な指導・アドバイスのための材料に活用する。

HISPROの業務としては，最初に「支払基金等へのレセプトオンライン請求用IPsec＋IKEサービス」を対象とする適合性評価から始め，現在4社7製品の評価を行った。現在，支払基金のホームペー

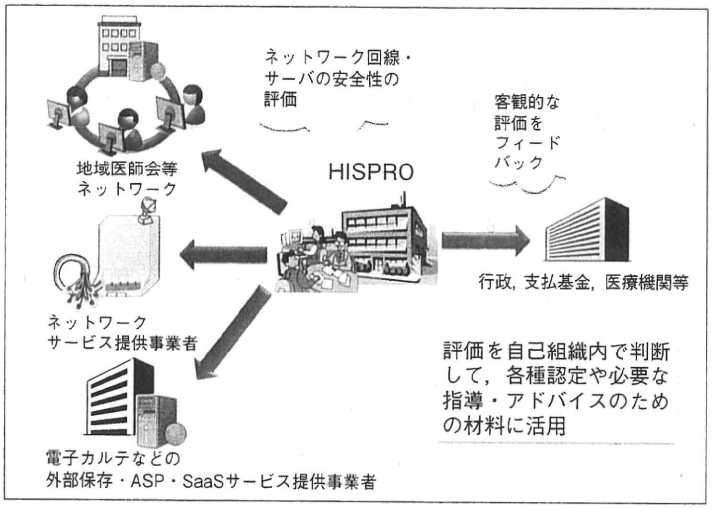

図1　HISPROの業務イメージ

表1　「支払基金等へのレセプトオンライン請求用IPsec＋IKEサービス」に対するチェックシート概要

要件			確認項目	対応策	確認エビデンス
大分類	中分類	小分類			
サービス全体	サービス内容，サービス仕様（責任分界点），情報の管理，事業継続，運用				
サービス拠点	物理的セキュリティ 技術的セキュリティ（拠点内部・外部侵入・監視・端末＆サーバ）				
接続サービス	サービス内容 終端装置のセキュリティ 通信変換拠点内での管理 接続の方式				
その他	サービスの共有				

ジ（http://www.ssk.or.jp/index.html）に，診療報酬請求に関して，インターネットに接続するための「IPsec＋IKEサービス提供事業者」として，HISPROのホームページの評価結果がリンクされている。今後，支払基金用などのネットワーク以外の「IPsec＋IKEサービス」にも広げることや，外部保存，ASP・SaaSへも適合性評価の対象を広げる準備を進めている。

HISPROの適合性評価の申請単位は，商品販売名，あるいは型式名ごととしている。したがって，サービス提供の形態が評価ずみのOEM製品でも，ユーザーに販売しているシステムサービス提供者がそれぞれ申請する必要がある。もちろん，直接ユーザーに販売するのではなく，OEMとして提供するサービス提供事業者の場合も申請可能である。その場合，ユーザーへ販売するシステムサービス提供者との責任分界点と，その運用を明確にする必要がある。

これは，ユーザーの購入対象品が評価ずみかどうかを商品名などでHISPROのホームページ（http://www.hispro.or.jp/）で確認することになるので，評価一覧との対応づけを明確にするためである。さらに，販売システムサービス提供者のセキュリティに対する運用も重要な評価要素で，OEM製品の適合だけではセキュリティ対策は不十分と考えているからである。

評価のポイント

表1に「支払基金等へのレセプトオンライン請求用IPsec＋IKEサービス」に対するチェックシート概要を示す。大分類および中分類項目のみを示しているが，実際に使用するチェックリストには，小分類としてガイドラインに対応した細かい要件と，それに対する具体的確認項目がある。システムサービス提供者は，それに対して自社のサービスでどのように対応しているかを記入し，その対応をしていることを何で確認したかエビデンスを記入して，適合性評価申請を行う。評価員は，これを見てガイドラインへの対応程度を評価する。さらに必要に応じ，ヒアリングや現地調査を行う。

HISPROの評価として重要視していることは，サービス内容に関する責任分界点の明確化と，ユーザーが実施すべきセキュリティ対策の順守事項への注意喚起である。これは不動産や投資を行うときの重要事項説明義務と似ている。すなわち，サービス利用に関する禁止事項を明確化し，それを利用者に対して要求事項としてサービス仕様に明記し，契約者と確認していることを要求している。

おわりに

HISPROの役割を果たしていくためにはシステムサービス提供者が提供するサービス種別ごとに各種ガイドラインへの適合性を評価するので，サービスの種別に合わせたチェックリスト作成と評価員の参加が必要になる。関心のある方の積極的な参加とご協力をお願いしたい。

今後，医療機関などがシステムサービスを利用する場合，投資家に対するムーディーズの格付けなどのように，HISPROの評価結果を参考にして，自施設にあったサービスを安心して導入いただけるようになることを想定している。これにより，民間事業者との契約に基づいたASP・SaaSの利用が進展し，地域連携システムの発展につながることを期待したい。

●参考文献

1）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4.1版．2010.（http://www.mhlw.go.jp/shingi/2010/02/s0202-4.html）
2）総務省：ASP・SaaSにおける情報セキュリティ対策ガイドライン．2008.（http://www.soumu.go.jp/menu_news/s-news/2008/pdf/080130_3_bt3.pdf）
3）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．2009.（http://www.soumu.go.jp/main_content/000030806.pdf）
4）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．2008.〔2008年7月24日付公示（号外第161号）〕（http://www.meti.go.jp/policy/it_policy/privacy/080331iryou-hontai.pdf）
5）経済産業省：SaaS向けSLAガイドライン．2008.
6）厚生労働省医政局長，厚生労働省保険局長：「診療録等の保存を行う場所について」の一部改正について．医政発0201第2号，保発0201第1号，2010.（http://www.meti.go.jp/press/20080121004/03_guide_line_set.pdf）
7）保健医療福祉情報安全管理適合性評価協会（HISPRO）ホームページ（http://www.hispro.or.jp/）