医療情報の外部保管の可能性とガイドライン

有限会社　夢見堂
石川浩太

はじめに

医療機関における医療情報の取り扱いに対する考え方が、ここ数年変わりつつある。電子カルテやフィルムレスの導入などの電子化が進み、医療従事者の情報へのアクセス方法が大きく変わり、パソコンおよびモニタなどの情報端末を使用する方法が一般化した。ぼう大な情報に対し瞬時にアクセスでき、医療サービスの向上に資すると考えられているが、一方で、紙やフィルムなどでは発生し得なかったさまざまな課題や問題点に直面している。

電子情報システムは、その特性により個人情報が瞬時に、大量に漏洩する恐れがある。医療機関においてみずからIT 専門家を配置してシステム管理を行っている例はいまだ少なく、経験のない医療従事者がシステム管理を強いられている病院も多い。PACS においては、医療機器の大幅な性能向上により、医療画像などの情報発生量は飛躍的な増加を続けており、システムストレージを圧迫している。また、システムの老朽化に伴い、更新時期にさしかかっている医療機関においては、データの移行、システムの更新に伴う仕様変更や運用の見直しなど、ぼう大な作業に疲弊している例も多い。このように、電子化の利便性を享受するには多大な労力を要する場合があり、その有用性に対し慎重に見極めを行う賢い医療機関が増えつつある。必要なサービス（いわゆる ASP・SaaS サービス）をネットワーク経由に利用し、医療情報データを外部保管することができれば、医療機関はシステム資産の保有や管理の必要がなくなり、多くの労力を軽減できる。また、専門家にシステム管理を委託することで、安全性の向上や効率的運用に伴う管理コストの削減も期待できる。システムの更新やデータの移行などの作業も原則的には発生しなくなる。さらに、遠隔読影サービスを提供している機関、地域医療連携やパーソナルヘルスレコードの実現と親和性が極めて高い (**図1**)。ただし、医療情報を外部保存する場合、事故が起こった場合の責任の所在のあいまいさや結果の重大性の観点から、院内における医療情報システムの安全管理に加え、特段の注意を払う必要がある。

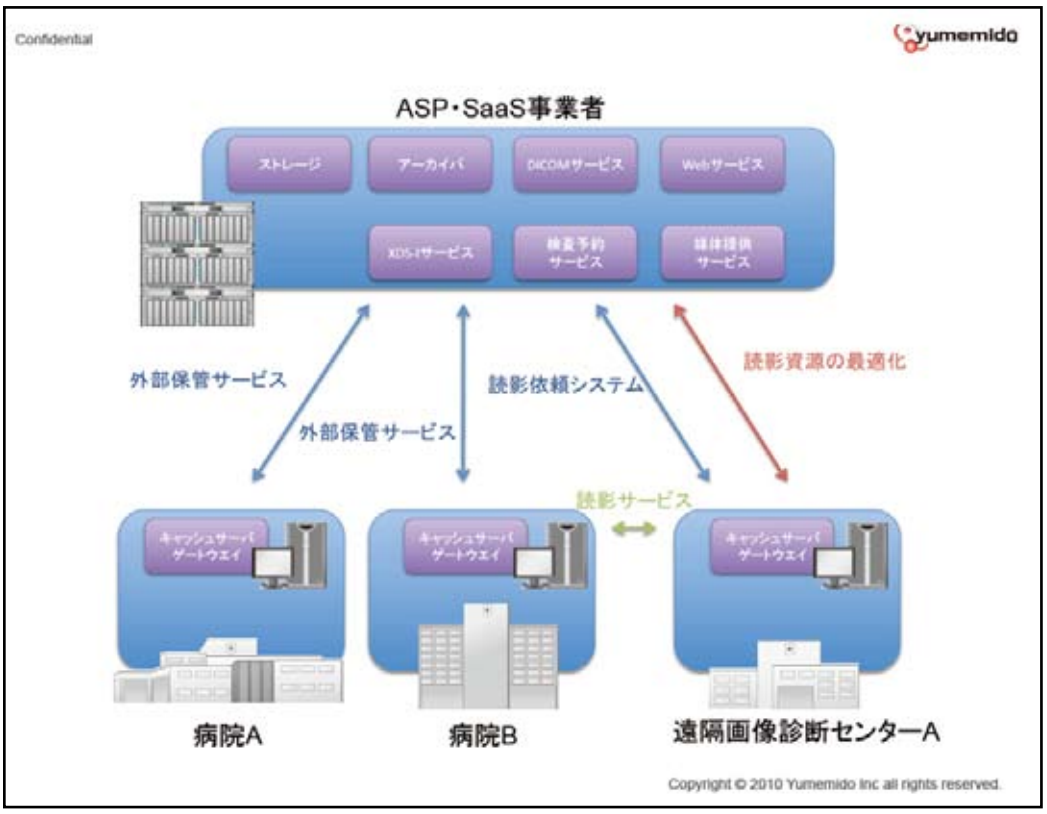

図1　ASP・SaaS 事業者と医療機関の役割分担
ASP・SaaS 事業者のサービスを利用することで、医療機関や遠隔画像診断センターが施設間のシステム連携の調整作業を行うことなく、有機的に医療サービスを提供できるようになる。

このようななか、本年２月、厚生労働省から「医療情報システムの安全管理に関するガイドライン」（以下、本ガイドライン）が改訂され、第 4.1 版として公開された[1]。本改訂は、平成 21 年７月に総務省が「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」を策定し、平成 20 年７月に経済産業省が告示した「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」（平成 20 年７月 24 日　経済産業省告示第 167 号）の整備などにより、外部保存に対する対応方法が明確になったとの指摘に基づくものである。今回は本ガイドラインの第４、６、８章を中心に紹介する。今後増加するであろう ASP・SaaS などのサービスの活用における留意点としてほしい。

電子的な医療情報の管理責任（本ガイドライン第４章）

第４章の中で、「医療にかかわるすべての行為は医療法等で医療機関等の管理者の責任で行うことが求められており、医療情報の取扱いも同様である」と述べられており、医療機関等の管理者に対し、法律的な責任、義務を課すことで、適切な取り扱いを求めている。一方、医療情報が電子化されたことで「紙の媒体やフィルムなどに比べてその動きが一般の人にとってわかりにくい」「漏えいなどの事態が生じた場合に、一瞬かつ大量に情報が流出する可能性が高い」「さらに医療従事者が情報取扱の専門家とは限らないため、その安全な保護に慣れていないケースが多い」という問題点が発生することも同時に指摘している。さらに、電子化された医療情報が医療機関等の施設内にとどまって存在するという状況のみならず、ネットワークを用いた交換・共有・委託などが考えられる状況下においては、本管理責任がネットワーク上のサービスを提供する事業者やネットワークを提供する通信事業者等にもまたがることになり、その責任の範囲を明確化する必要が発生し、「責任分界」という概念を用いて整理する必要が発生する。

通常運用においては、管理者は説明責任、運用責任、定期的に見直し必要に応じて改善を行う責任を負うとしている。説明責任とは電子的に医療情報を取り扱うシステムの機能や運用方法が、その取り扱いに関する基準を満たしていることを患者らに説明することである。本責任を果たす要件としては、システムの仕様や運用方法の明確な文書化、定期的監査、監査結果の文書化、監査結果の問題に対する対応、対応記録の文書化を求めている。管理責任をはたすためには、請負事業者に対し管理状況の定期的報告を求めることと、責任所在の明確化などの監督を行うことが必要である。また、個人情報保護法上の責任者の選任も求めている。改善責任では、情報保護に関する技術の日進月歩性により現在の情報保護体制が陳腐化する恐れがあり、それを適宜見直して改善する必要性を求めている。

事後責任においては、管理者は説明責任と善後策を講ずる責任を負うとしている。いったん事故が発生した場合、医療機関等の管理者はその事態発生を公表することと、原因およびそれに対する対処法について説明することを求めている。善後策を講ずる責任としては、原因究明、損害補償、再発防止策が含まれる。

責任分界（本ガイドライン第４章）

委託と第三者提供では責任分界が異なるため、整理する必要がある。第三者提供においては、適切な第三者提供がなされる限り、その後の情報保護に関する責任は医療機関等の管理者から離れることになり、その後は提供を受けた第三者に生ずることになる。一方、委託の場合、管理責任の主体はあくまでも医療機関等の管理者である。医療機関等の管理者は、患者に対する関係では、受託する事業者の助けを借りながら前述の「説明責任」・「管理責任」・「定期的に見直し必要に応じて改善を行う責任」をはたす義務を負うことになる。そのため医療機関等の管理者は、契約のなかに以下の内容を含めて受託する事業者に対応することが求められる。

① 通常運用の説明責任をはたすため、情報提供義務・説明義務を課す。
② 通常運用の運用責任をはたすため、委託先事業者の管理の実態を理解し、その監督を適切に行う仕組みを作る。
③ 通常運用の改善責任をはたすため、当該システムの運用管理の状況を定期的に監査し、問題点を洗い出し、改善すべき点があれば改善していく責任の分担の明確にする。
④ 通常運用の改善責任をはたすため、情報保護に関する技術進展に配慮した定期的な再評価・再検討の義務を課す。
⑤ 通常運用の改善責任をはたすため、対策をとる際の医療機関等との協議の義務を課す。
⑥ 事故後の説明責任をはたすため、事業者の情報提供や分析義務を課す。
⑦ 事故後の善後策を講ずる責任をはたすため、原因追及と再発防止策の提案義務を課す。

⑧ 事故後の善後策を講ずる責任をはたすため、損害填補責任の分担を明記する。

実際に医療情報について何らかの事故が生じた場合、事故が医療情報の処理を委託した事業者の責任による場合、適切な委託契約に基づき、受託する事業者の選任・監督に適切な注意を払っていれば、法律上、医療機関等の管理者の善管注意義務ははたされていると理解される。とはいえ、医療機関等では医療情報の管理を医療機関等の管理者の責任において行うことが求められているので、医療情報に関する事故の原因究明、被害者への損害填補、さらに再発防止について、少なくとも責任の一端を負わなければならない。また、現実的にも、受託する事業者が医療情報のすべてを管理しているとは限らないため、事故を契機として、医療情報保護の仕組み全体について善後策を講ずる責任は医療機関等の管理者が負わざるを得ない。同様に、患者に対して善後策を講ずる責任を免れるものではないことは留意する必要がある。

遠隔画像診断など医療機関等の業務の一部を委託することに伴い、情報が「一時的に外部に保存」される場合においても、医療機関の管理者は業務委託先に対して、受託する事業者の選定に関する責任や（セキュリティなどの）改善指示を含めた管理責任があるとともに、情報の保存期間の規定などの管理監督を行う必要がある。

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（本ガイドライン第６章）

医療情報をネットワークを利用して外部と交換する場合、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「なりすまし」「改ざん」および「盗聴」などの脅威に対して対策を講じる必要がある。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サービスとしては、おもに専用回線、ISDN 等の公共回線、IP-VPN や一部の Internet-VPN などがある。この場合、物理的もしくは論理的にインターネットから隔離されているため、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。しかし、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。「改ざん」を検知するための方法としては、電子署名を用いることなどが想定される。

一方､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サービス（例えばインターネット）を利用する場合は、特段の注意が必要になる。この場合、通信上の脅威に備えることを医療機関等の責任において行わなければならない。SSL-VPN や IPSec などの技術が用いられるが、内在するリスクが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。

診療録及び診療諸記録を外部に保存する際の基準（本ガイドライン第８章）

現在の技術を十分活用し、かつ注意深く運用すれば、ネットワークを通じて診療録などを医療機関等の外部に保存することが可能である。この場合、受託する事業者が、真正性を確保し、安全管理を適切に行うことにより、外部保存を委託する医療機関等の経費節減やセキュリティ上の運用が容易になる可能性がある。しかし、患者らの情報が瞬時に大量に漏えいする危険性も存在し、この場合被害者の苦痛や権利回復が困難であることが多く、通常求められる安全管理上の体制と同等以上の体制を確保した上で、患者に対する保健医療サービスなどの提供に当該情報を利活用するための責任を果たせることが必要となる。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保存する場合のガイドラインを以下に示す。

(ア) 医療機関等が、外部保存を受託する事業者と、その管理者や電子保存作業従事者等に対する守秘に関連した事項や違反した場合のペナルティも含めた委託契約を取り交わし、保存した情報の取り扱いに対して監督を行えること。

(イ) 医療機関等と外部保存を受託する事業者を結ぶネットワーク回線の安全性に関しては「6.11 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」を遵守していること。

(ウ) 受託事業者が民間事業者等に課せられた経済産業省の「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」や総務省の「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」等を遵守することを契約等で明確に定め、少なくとも定期的に報告を受ける等で確認をすること。

(エ) 保存された情報を、外部保存を受託する事業者が契約で取り交わした範囲での保守作業に必要な範囲での閲覧を超えて閲覧してはならないこと。なお保守に関しては、「6.8 情報システムの改造と保守」を遵守すること。
(オ) 外部保存を受託する事業者が保存した情報を分析、解析等を実施してはならないこと。匿名化された情報であっても同様であること。これらの事項を契約に明記し、医療機関等において厳守させること。
(カ) 保存された情報を、外部保存を受託する事業者が独自に提供しないように、医療機関等は契約書等で情報提供について規定すること。外部保存を受託する事業者が提供に係るアクセス権を設定する場合は、適切な権限を設定し、情報の漏えい、異なる患者の情報を見せたり、患者に見せてはいけない情報が見えたり等の誤った閲覧が起こらないようにさせること。
(キ) 医療機関等において（ア）から（カ）を満たした上で、外部保存を受託する事業者の選定基準を定めること。少なくとも以下の 4 点について確認すること。

(a) 医療情報等の安全管理に係る基本方針・取扱規程等の整備
(b) 医療情報等の安全管理に係る実施体制の整備
(c) 実績等に基づく個人データ安全管理に関する信用度
(d) 財務諸表等に基づく経営の健全性

さらに推奨されるガイドラインを以下に示す。
(ク) トラブル発生時のデータ修復作業等緊急時の対応を除き、原則として委託する医療機関等のみがデータ内容を閲覧できることを担保すること。
(ケ) 外部保存を受託する事業者に保存される個人識別に係る情報の暗号化を行い適切に管理することや、外部保存を受託する事業者の管理者といえども通常はアクセスできない制御機構をもつこと。具体的には、「(a) 暗号化を行う」、「(b) 情報を分散保管する」という方法が考えられる。その場合、非常時等の通常とは異なる状況下でアクセスすることも想定し、アクセスした事実が医療機関等で明示的に識別できる機構を併せもつこと。

個人情報の保護の観点から必要とされるガイドラインを以下に示す。
(コ) 適切な委託先の監督を行うこと。診療録等の外部保存を受託する事業者内の個人情報保護については「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」において考え方が示されている。
(サ) 外部保存実施に関する患者への説明。診療録等の外部保存を委託する施設は、あらかじめ患者に対して、必要に応じて患者の個人情報が特定の外部の施設に送られ、保存されることについて、その安全性やリスクを含めて院内掲示等を通じて説明し、理解を得る必要がある。

おわりに

医療機関が個別にコンピュータシステムを導入し管理することは、一般的に効率が悪い。医療機関は、財務の健全化のみならず医療サービスの向上に資するために、外部保管サービスおよび ASP・SaaS サービスの利用を考える時期にきていると思われる。現状のシステムの見直しや更新に際し、これらのサービスの導入の可能性も合わせて考慮すべきである。

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