セキュリティーの基礎

「安心」は人によって異なるが、守るべき最低限の基準は存在するはずである。このような最低限の安全基準は、一般に法律・規則や指針で定められていることが多い。保健・医療・福祉分野でも、例えば米国ではHIPAA Security StandardsやPrivacy Standardsが存在する。しかし、わが国では法律・規則や指針はいまだ十分に整備されてはいない。基準の整備は今後の課題であるが、医療の現場は日々電子化が進んでおり、整備されるのを待つわけにもいかない。原則に従って基本的な対策を取る必要がある。最低限の「安心」は、米国の例でも分かるように、一定の基準に従った情報の安全性とプライバシー保護によって達成される。

情報の安全性は可用性、機密性、真正性を確保することで達成するとされている。本稿でそれぞれの技術的な側面を詳細に述べることは紙数の関係でできないので、概略を述べる。技術的には診療情報に特有なことは少なく、詳細は他分野において研究や実用化されている技術手法が参考になる。

1．可用性

可用性の確保とは、情報が必要なときに確実に利用できることを保障することである。情報システムでこれを厳密に追求すると、冗長かつ高価なシステムを導入しなければならない。一概に必要と言っても、必要性には程度がある。例えば大規模な震災で医療機関自体が破壊されたとき、紙で運用されているカルテが取り出せないからと言って、診療しないわけにはいかない。一方で、社会インフラや医療機関の設備に何も障害がないのに、前回受診時のカルテが取り出せず、そのために診療方針を誤れば、医療過誤と言わざるを得ない。

つまり可用性とは、状況に応じて診療に必要な情報が確実に利用できることと考えることができる。診療情報システムを設計・導入する場合、状況を分類し、状況に応じた可用性の目標をしっかり定める必要がある。

2．機密性

機密性は、原理的には不要・不正なアクセスを防止し、正当な権利を有する利用者や施設だけがアクセスできることを保障することである。しかし、診療情報の場合はいくつかの複雑な問題がある。

まず「正当な権利」が問題で、診療情報に誰がアクセスしてよいか、ということは微妙な問題を含む。診療情報は、一般に患者の健康の維持・回復という目的があって収集されるわけで、この目的にかなう利用は正当と考えることができる。しかしこれは原則であり、現場にはさまざまな状況が生じ得る。必要と考えて収集した情報が不必要である場合もあれば、偶然収集した情報が重要となる場合もある。

さらに情報の主権という点から考えると、診療情報は本質的に患者の個人情報であり、患者が情報の主権者である。従って、情報のコントロール権は患者にある。では、すべての患者が積極的に診療情報をコントロールしたいかと言えば、そうではない。自主的に関与する以上は責任が生じるが、疾病や健康に対する知識格差が存在するために、ある限度内で医療機関に委任することを望むことが一般的であろう。問題は、この「ある限度」であり、これには明確な基準が存在しないということである。問題を複雑にすることを恐れずに言えば、「ある限度」は医療機関と患者の信頼関係にも依存する。

3．真正性

真正性は、情報操作の責任者が明確であり、いったん作成された情報が不正または偶発的に内容を変更されないことを保障することである。

電子化情報は、1ビットでも違えば内容が大きく異なったり、再現できなかったりする。また、手書き情報における筆跡のような作成操作の個性は、検出が困難である。現在では、責任者を明確にするためにデジタル署名を用いることが多く、またこれをうまく活用することで、短期間での不正な内容の変更は検出可能である。ただし、診療情報は長期に利用されることがあり、また法的にも一定の保存期間が定められている。単にデジタル署名を採用するだけでは必要な期間の真正性確保は難しい。署名延長技術を用いるか、固定媒体と監視運用などを組み合わせる必要がある。

このように論じてくると、真正性は可用性や機

密性と比べて技術的には容易に対応可能に見えるが、実際は利用者の識別方法や、どの時点をもって情報が「作成された」とするかは運用の問題であり、施設の状況や診療形態で大きく変わることが分かる。

運用とシステム機能

前項で、セキュリティー対策を基礎的な項目に分類することはできるが、いずれの項目も単純な技術的対策では困難であることを述べた。では、どうすればよいであろうか。

本来、診療情報は情報システム内にだけ存在すれば目的を達成されるものではない。情報システムのなかに存在する情報が医療従事者に認識され、状況によっては、患者やほかの保健医療機関に伝えられて初めて情報の存在目的が達成される。セキュリティーの「安心できる状態」を目指す以上は、情報システム内にある場合もそうでない場合も、同様にセキュリティーが確保されている必要がある。

つまり、システム内だけでセキュリティーを考えても意味がない。情報が使われる状況を、システム内外を含めて考慮する必要がある。また、情報システムのセキュリティーは、情報システム利用者の運用上の努力と相補的である。運用上厳しい制限を設けて、それが確実に順守されればシステム機能は軽くて済むし、システム機能を充実させれば運用上の負担は減る。しかし、どのような運用を行っても、セキュリティーが達成される診療情報システムは存在しない。これは、情報がシステム外でも活用されることを考えれば自明である。

従って、運用設計とシステム設計は密に連携して行う必要がある。運用設計が実施されるための制度的な仕組みも必須である。一般に、運用側に負担をかければ利用者に厳しい制限と規律の順守が強く求められ、システム側に負担をかければ導入や維持経費が増加する。情報システムの導入や維持に利用可能な経費を十分に勘案しなければ、経済的な面から安全性が破綻(たん)することもあり得る。

セキュリティー方針

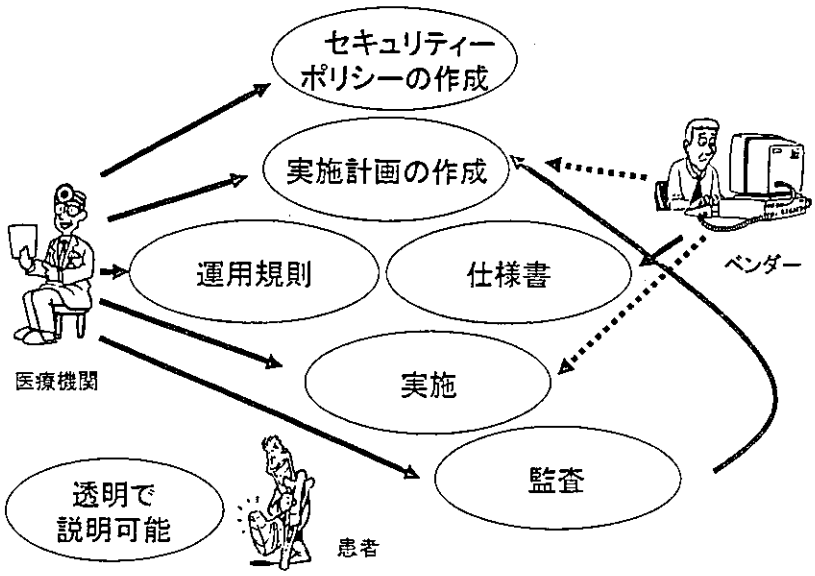
運用とシステム機能は相補的であり、どちらか一方だけでは診療情報システムを導入した場合のセキュリティー確保が不可能であることを示した。しかし運用は医療機関側が責任を持ち、システム機能は一般には契約に従って導入ベンダーや維持業者が責任を持つ。責任主体が分かれることは、特に患者の「安心」にとって不明瞭な要素となる。患者は医療機関を受診するのであって、情報システムに関連した業者を意識することは通常はあり得ない。従って患者から見れば、実情はどうであれ、安全の責任主体は医療機関以外にはない。ここに「ねじれ」を残しては、安心は獲得できない。責任は医療機関にあることを明瞭にする必要がある。しかし一方では、医療機関は一般にIT技術の専門家ではなく、導入された情報システムの詳細に責任を取ることは現実的ではない。責任関係があいまいで理解し難いものであれば「安心」は獲得できないので、明快に示し得るものにする必要がある。

一般に、このような責任関係の明確化を目的として、次のような方法が取られる。まず、患者から見て自明の責任主体がセキュリティーの基本方針を作成し、公表する。この基本方針は言わば宣言であり、医療機関が患者の診療情報のセキュリティーに責任を持つことを明記し、さらに情報の主権者である患者から委任を受けるための利用目的や保管方法、患者からの質問や苦情の受付方法を明記する。

次に、基本方針を実現するための実施計画を作成する。実施計画には医療機関内でのセキュリティー確保を実現するための体制を規定し、情報の運用形態を列挙し、それぞれについて運用とシステムに求める要件の概略を記載する。また計画どおりの運用が行われるための教育や監査、違反があった場合の対策などを記載する。

実施計画に基づき、運用規則とシステム仕様書を作成する。重要なことは、これらの方針や計画、規則、仕様書をすべて文書として整備することで、最初は結構大きな作業となるが、一度整備すれば

図1　セキュリティー対策の実現方法



重要な資産になる。

このように段階的に文書を整備することで、その時点でのセキュリティー対策が常に説明可能になり、責任関係も明確にすることができる。

監査と発展的反復

基本方針やそれに従った実施計画や運用規則、仕様書が整備されても、実際に実施した場合、計画どおりにいくとは限らない。予想外の情報の利用が起こることもあるし、運用規則が厳し過ぎて診療に差し支えることもあるかもしれない。このようなあいまいさや無理を残しておくと、セキュリティー対策はいずれ破綻する。これを防止するためには、定期的に基本方針が実現されているかどうか、実現や継続に困難や無理がないかをチェックする、つまり監査を行う必要がある。監査は計画的に行うべきで、実施計画に含まれるべきであろう。そして監査の結果、問題があればその原因を速やかに修正し、次の監査で検証を行う。これを繰り返すことで、セキュリティー対策は向上することになる。

ここで注意しなければならないことは、問題があっても基本方針は変更してはならないという点である。基本方針は、例えば医療機関の合併のように組織そのものが大きく変化する場合か、法律の制定のように社会的な要請が大きく変化した場合以外には通常は変更されない。言い換えれば、そのような場合以外に変更の必要がないように基本方針を作成しなければならない。

実施計画以降を修正し検証を繰り返して、基本方針の確実な実現を図らなければならない。全体を図1に示す。このような方法は、PDCAサイクル(計画、実施、チェック、評価サイクル)と呼ばれることがある。

参照基準の作成

「安心」を得るための方法論について論じてきたが、一般の医療機関にとって、基本方針や実施計画と言われてもなじみのあるものではない。ひな型が必要である。現在セキュリティーに関しては、ISMSやBS-7799、ISO/IEC17799などの一般的な基準は存在するが、医療機関向けのガイドラインはまだ存在しない。関係者の努力に期待したい。

【参考文献】

1)医療の個人情報保護とセキュリティ(編集:開原成允, 樋口範雄), 有斐閣, 東京, 2003.