6.9　情報及び情報機器の持ち出しについて

B. 考え方

昨今、医療機関等において医療機関等の従業者や保守業者による情報及び情報機器の持ち出しにより、個人情報を含めた情報が漏えいする事案が発生している。

情報の持ち出しについては、ノートパソコンのような情報端末やフロッピーディスク、USB メモリのような情報記録可搬媒体が考えられる。また、情報をほとんど格納せず、ネットワークを通じてサーバにアクセスして情報を取り扱う端末（シンクライアント）のような情報機器も考えられる。

まず重要なことは、「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」の「6.2.2　取扱情報の把握」で述べられているように適切に情報の把握を行い、「6.2.3　リスク分析」を実施することである。

その上で、医療機関等において把握されている情報もしくは情報機器を持ち出してよいのか、持ち出してはならないのかの切り分けを行うことが必要である。切り分けを行った後、持ち出してよいとした情報もしくは情報機器に対して対策を立てなくてはならない。

適切に情報が把握され、リスク分析がなされていれば、それらの情報や情報機器の管理状況が明確になる。例えば、情報の持ち出しについては許可制にする、情報機器は登録制にする等も管理状況を把握するための方策となる。

一方、自宅等の医療機関等の管轄外のパソコン（情報機器）で、可搬媒体に格納して持ち出した情報を取り扱う時に、コンピュータウイルスや不適切な設定のされたソフトウェア（Winny 等）、外部からの不正アクセスによって情報が漏えいすることも考えられる。この場合、情報機器が基本的には個人の所有物となるため、情報機器の取り扱いについての把握や規制は難しくなるが、情報の取り扱いについては医療機関等の情報の管理者の責任において把握する必要性はある。

このようなことから、情報もしくは情報機器の持ち出しについては組織的な対策が必要となり、組織として情報もしくは情報機器の持ち出しをどのように取り扱うかという方針が必要といえる。また、小規模な医療機関等であって、組織的な情報管理体制を行っていない場合でも、可搬媒体や情報機器を用いた情報の持ち出しは想定されることからリスク分析を実施し、対策を検討しておくことは必要である。

ただし、この際留意すべきは、可搬媒体や情報機器による情報の持ち出し特有のリスクである。情報を持ち出す場合は、可搬媒体や情報機器の盗難、紛失、置き忘れ等の人による不注意、過誤のリスクの方が医療機関等に設置されている情報システム自体の脆弱性等のリスクよりも相対的に大きくなる。

従って、情報もしくは情報機器の持ち出しについては、組織的な方針を定めた上で、人的安全対策をさらに施す必要がある。