

実行の抑制等も効果が大きい。

(5) ネットワーク上からの不正アクセス

ネットワークからのセキュリティでは、クラッカーやコンピュータウイルスや不正アクセスを目的とするソフトウェアの攻撃から保護するための一つ手段としてファイアウォールの導入がある。

ファイアウォールは「パケットフィルタリング」、「アプリケーションゲートウェイ」、「ステートフルインスペクション」等の各種方式がある。またその設定によっても動作機能が異なるので、単にファイアウォールを入れれば安心ということにはならない。単純なパケットフィルタリングで十分と考えるのではなく、それ以外の手法も組み合わせて、外部からの攻撃に対処することが望ましい。システム管理者はその方式が何をどのように守っているかを認識すべきである。このことは、医療機関等の外部から医療機関等の情報システムに接続される PC 等の情報端末に対しても同様であるが、その考え方と対策については、「6.9 情報及び情報端末の持ち出しについて」を参照されたい。

不正な攻撃を検知するシステム (IDS : Intrusion Detection System) もあり、医療情報システムと外部ネットワークとの関係に応じて、IDS の採用も検討すべきである。また、システムのネットワーク環境におけるセキュリティホール (脆弱性等) に対する診断 (セキュリティ診断) を定期的 to 実施し、パッチ等の対策を講じておくことも重要である。

無線 LAN や情報コンセントが部外者により、物理的にネットワークに接続できる可能性がある場合、不正なコンピュータを接続し、ウイルス等を感染させたり、サーバやネットワーク機器に対して攻撃 (サービス不能攻撃 DoS : Denial of Service 等) を行ったり、不正にネットワーク上のデータを傍受したり改ざんする等が可能となる。不正な PC に対する対策を行う場合、一般的に MAC アドレスを用いて PC を識別する 경우가多いが、MAC アドレスは改ざん可能であるため、そのことを念頭に置いた上で対策を行う必要がある。不正アクセスの防止は、いかにアクセス先の識別を確実に担保するかが重要であり、特に、“なりすまし”の防止は確実に行わなければならない。また、ネットワーク上を流れる情報の窃視を防止するために、暗号化等による”情報漏えい”への対策も必要となる。

(6) その他

無線 LAN は、看護師等が情報端末を利用し患者のベッドサイドで作業する場合等に利便性が高い反面、通信の遮断等も起こる危惧があるので、情報の可用性が阻害されないように留意する必要がある。また、無線電波により重大な影響を被るおそれのある機器等の周辺での利用には注意が必要である。

最近では、電力線搬送通信 (PLC : Power Line Communication) が利用可能になった。しかし、医療機関等において PLC を利用する場合、医療機器に対する安全性が確認されておらず、厚生労働省医薬食品局から「広帯域電力線搬送通信機器による医療機器への影