特集1
今そこにある危機
放射線診療のBCPを考える
Business Continuity Plan

# 4. 医療機関におけるサイバー攻撃に対するBCP

武内　彬正／前原　諒一　厚生労働省医薬・生活衛生局医療機器審査管理課

## 医療情報システムのサイバーセキュリティ対応と医療機器

現在，医療機関においては，患者カルテなどを含むさまざまな医療情報が電子化され，医療機関のネットワークの中で取り扱われる状況にある。医療情報の集積・処理を扱う医療情報システムは，情報通信技術の発達に伴い，事務情報処理の向上だけでなく，診察の迅速化や医療従事者の負担軽減，ひいては，医療の安全性や質の向上に資するものとなっている。

医療情報システムは，これまで大規模な医療施設において普及が進んでいたところであるが，近年では，中小規模のクリニックまで医療情報システムの普及が進んでいる状況にある[1]。

医療情報システムは，患者個人の氏名や既往歴，服薬状況のほかにも，各種治療データや主治医の情報なども共に扱われる可能性があるため，漏えいや改ざん，システム破壊のリスク対策として，情報セキュリティ対応が求められている。

医療情報システムに関する情報セキュリティ上の脆弱性を利用されたサイバー攻撃の事例として，2020年9月には，ドイツ・デュッセルドルフ大学病院において，ランサムウエア感染によるシステム障害が発生し，救急患者の受け入れ停止となり，受け入れ予定の患者を別施設へ搬送する必要が生じた事例がある[2]。また，同じく2020年9月には，米国・Universal Health Services（以下，UHS）において，ランサムウエア感染が発生し，全米のUHS施設でコンピュータおよび電話システムが停止した事例がある[3]。

わが国では，電子カルテシステムなどの基幹システムを対象に，患者情報の保護などを目的とした「医療情報システムの安全管理に関するガイドライン　第5版」[4]が公表されている。当該ガイドラインでは，医療情報を扱うシステムと，それらシステムにかかわる人または組織を対象として，情報セキュリティマネジメントシステム（information security management system：ISMS）の実践に加えて，組織的，物理的，技術的および人的な対策，そしてシステムが不正侵入などのサイバー攻撃を受けた際の非常時の対応について示している。

このように，医療情報システムについては，情報セキュリティ対応が進められているところであるが，医療情報システムに対する情報通信の入出力を行う医療機器についてもセキュリティ対応を実施する必要がある。本稿では，医療機関におけるサイバー攻撃に対するBCP（business continuity plan：事業継続計画）について，医療情報システムに対する情報通信の入出力を行う医療機器の観点から，医療機器のサイバーセキュリティ対応に関連する規制の現状などについて概説する。なお，本稿中には筆者らの個人の見解が含まれており，該当箇所については厚生労働省の正式な見解ではないことに留意いただきたい。

## 医療機器の規制とサイバーセキュリティ対策

### 1. 医療機器のサイバーセキュリティ対策の必要性

internet of things（IoT）技術を利用する情報通信機器が多く登場したことに伴い，医療機関の医療情報システムが単一のネットワークで結ばれ，さらには，患者の診療や治療に関する情報の入力または出力を担う医療機器も，ネットワークに接続（有線または無線による別を問わず，USB媒体などの記憶媒体を介した間欠的データ通信も含む）される機会が増加していることから，医療機器の外部からの不正侵入や不正操作などのサイバーセキュリティリスク（サイバーリスク）を考慮する必要がある。

医療機器のサイバーリスクとしては，医療機関などのネットワークに接続されたほかのコンピュータなどがサイバー攻撃を受けた場合には，ネットワークを介して医療機器がサイバー攻撃を受けるリスク，また，医療機器がサイバー攻撃を受けた場合には，当該医療機器が接続されたネットワークを介してほかの医療機関の基幹システムに障害を引き起こすリスクが挙げられる。これらのサイバーリスクに対し，医療機器の製造販売業者は，適切な設計や開発の管理をいっそう厳重に実施するとともに，製品の販売


〈0913-8919/21/￥300/ 論文 /JCOPY〉