別紙 3

A 大学病院へのヒアリング（要約）

目　的：医療情報システムに関して先進的に実践している医療機関でのサイバーセキュリティ対策および医療機器のサイバーセキュリティ対策に関する状況把握や課題について意見交換を行う。

いただいた主な意見：

○医療機器メーカが MDS 2 等のセキュリティ情報を開示すべき（現在はできていない）。MDS 2 を集めただけでは判断材料にならない。その使い方を明示すべき。

○セキュリティ対策は 1 か 0 かではなく、環境の変化についても継続的に対応する必要がある。

○セキュリティに偏りすぎ。実は BCP としてどうするかが主目的であり、セキュリティはリスクファクターの一つでしかない。全体でどう対応するか？が重要である。

○第三者機関なようなところで、まとめてペンテスト（ペネトレーションテスト　脆弱性を検証するテスト手法の 1 つ。侵入テストとも呼ばれる）を実施するのも一つの案。

○セキュリティ開示文書について、JIRA　JAHIS の書式でも対応されていない。さらには、そのような団体に参画していない企業をどうするかも課題である。

○CIFS/1.0（Common Internet File System）を使っているのも医療ぐらいなので、そのあたりから医療機器のサイバーセキュリティ確保のためには改善が必要である。

○サイバーセキュリティ対策を自分できるのが理想であるが、人材がいない。医療情報技師がいればある程度は対応できる。そのためにも、簡単にできる方法を広める必要がある。ペンテストのサーバを配ることや、共通ソフトを配る等が必要である。

○情報システムは点数で評価できない。導入したらお金がかかる。管理するための　CSIRT、ペンテストにもお金がかかる。ネットワーク設備についても同様で、医療の収益だけだと無理がある。

○医療機器も含めてサイバーセキュリティ確保のためには、医療情報技師の拡充、診療情報管理士の拡充が必要であるが、併せてキャリアパスの検討も必要である。

○医療情報技師であれば、医療に関する知識テストもあり医療のことも知っている。IT パスポート試験には医療は入っていないし、セキュリティも入っていない。その上の資格だとレベルが高すぎ、裾野は広がらない。

○サイバーセキュリティ確保のための人材育成⇒病院運営に必要なレベル、運用マネージャーレベルが必要

○ペンテストをアウトソースすると高い。 1 台いくらという世界。脆弱性の確認については、それほど高度な技術は必要なし。最低限できてないというレベルが判別できれば良い。各医療機関でベンチマークできると良いのではないか。それによって、保険の掛け金が安くなるとかの仕組みも必要。サイバーセキュリティの対策費やサイバー攻撃による減収まで対応できるよう

な保険も今後必要となるのではないか。

○医療機関の経営者が認識すること、共通指標で評価し、自己評価ができる仕組みが必要ではないか。

○医療機器系、部門システムのサイバーセキュリティ対策は希薄。

○現在ようやく、不要なサービスをとめたりしている。ひどい場合には、ファイヤーウォールの設定もしていないし、アップデートの確認などもしていない。チェックリストで点検、端末全数把握できるような仕組みが必要。

○医療機器メーカには、ネットワーク接続前に確認しても、仕様と言われる。導入時見て、指摘しても改善されない。（できない）PMDA はセキュリティの中身の評価ができていない。承認の段階でネット―ワーク、セキュリティを併せて確認してもらわないと、いざネットワークに医療機器を接続して使用するときに、問題が生じることになる。厚生労働省や PMDA 単独ではなく、他省と連携して、専門分野が得意な省庁と連携してセキュリティは別基準で対応する必要があるのではないか。

○実際に DDos 攻撃をモニタ機器に行ったところ、ICU でバイタルサインのモニタリングが実際に停止した。しかし、製造販売業者については、その対策は承認の関係でできず、新製品では対応されている。使用する環境への配慮が足らないがそれでも、製造販売承認は下りてしまう。

○サイバーセキュリティについては、ランサムだけではない。DDos の方が怖い。医療機器のサイバー攻撃の可能性については海外では結構報告例がある。検査データの改ざんもあり得る。医療機器導入の際にその情報が情報部門にも共有され、サイバーセキュリティの観点からも確認している。基本的には、ネットワーク機器は全て情報部門で管理しているが、チェックをして指摘はするものの、その後の管理などそれ以上はできていない。

○ネットワークに接続される医療機器のポートスキャンだけでも実施した方が良い。メーカに確認する必要があるが、何番ポート使っているかも現時点では開示されていない。医療機器側の義務として、そのような情報を開示してもらう必要もある。実際のポートスキャンについては、フリーでソフトもある。サイバーセキュリティ対策の初歩としては、ポートのスキャンが基本。可能であれば、攻撃を加えて動作状況を確認することもできる。

○医療機器のサイバーセキュリティに関して、医療機関の管理者として知っているべき要件や具体にやることについての推奨を出した方が良いのではないか。