Digital Health Task Force
-2024年の振り返り-

Dec 12, 2024 EBC代表者会議

Tomohiko Matsukawa

EBC, MEDICAL EQUIPMENT & DIAGNOSTICS COMMITTEE

DHTFについて

DHTFは上位の診療報酬部会、薬事部会双方と連携して活動するTFとして機能します。
特に現在様々な局面で議論が進んでいるプログラム医療機器について、承認/認証に係る法整備や診療報酬上の取り扱いなど部会単体で扱うには難しい内容などにおいて、部会と意見調整を行う集団に位置付けられます。
現状としては、サイバーセキュリティ（MDS/SDS関連）の意見交換や無体物QMSについての勉強会開催（PMDA共催）を検討しています。

- サイバーセキュリティについて

サイバーセキュリティ　意見募集

- 「製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）」における課題
　→　一方でMDS/SDSについて、設置管理医療機器等の大型機器を想定したようなチェックリストとなっており、対応しづらい項目が多いという企業さんがいらっしゃいます

【意見募集】
MDS/SDSにて対応に困っている企業さんはいらっしゃいますか？
・どんな点が対応しづらいですか？
・病院から指摘されて困った経験はありませんか？

- 「医療情報システムの安全管理に関するガイドライン　第6.0版」における課題（会員より提起）
・ガイドライン「13.ネットワークに関する安全管理措置」において、セキュアなネットワークは「専用線・IKE＋IPsec・IP-VPN」について

【意見募集】
インターネットVPNにおいてIKE＋Ipsec以外のプロトコルで接続をすでに開始しており、変更が難しく、病院への説明で困っているという企業さんはいらっしゃいますか？

MDS/SDS関連

【MDS】

１．どんな点が対応しづらいですか？

①想定対象が電カル・オーダーリングシステムであるため装置と合っていない

②クライアント-サーバを前提とした構成を想定されているが装置の構成には合っていない

③扱う情報の機微レベルが電カル想定で掛かれており機微レベルが低い装置に合っていない

④ガイドラインはリスクベースであるがMDS/SDSはYES/NOでの判定のため多くの医療機関等がチェック内容が全てYESでなければガイドラインに準拠したことにならないと誤解されている

⑤MDS/SDSはチェックリストであるため100点満点でなければならないように誤解させるテンプレートになってしまっており、各内容についてリスクの測定をしない状態で結果が判定されてしまう

⑥装置はV&Vを実施する必要があるため、PCのようにユーザ側のアプリケーションを自由に入れるようにはできない

⑦複数の装置から成る製品についてどのように記載すれば良いか分からない

２．病院から指摘されて困った経験はありませんか？

テンプレートがチェックリストであるため100点満点でなければガイドラインを遵守していないと指摘を受けている

MDS/SDS関連

【SDS】
１．どんな点が対応しづらいですか？
①装置自体はサービスではないため対象のサービスの同定が困難
→同定しても病院の納得を得難い
②「機器」という言葉がサーバを想定していると読み取れるが医療機器がどのように該当するのか分からない
→結果、弊社としての解釈で作成しているのが現状

２．病院から指摘されて困った経験はありませんか？
該当なし

【対応部門について】
QAが担当部門として対応することとしましたが、QMSと一体化するには範囲が異なり、少し無理があるように思えます。
医療機関からもQAが統括していると安心すると安易に判断されているようです。
何かサービスを行っている部門もしくはプロマネが所属している部門が統括するべき！というような通知やガイドラインは示されませんでしょうか？
→ 安易にQAが主体とならない様にできないものか

VPN関連

【対応部門について】

１．ガイドラインの記載が限定されておりその他の方式を提案する余地が無い
　→システム運用編１３②には「原則として医療機関等が経路等を管理する、セキュアなネットワークを利用すること。」と記載されているが原則ではなく必須であると理解されてしまっている

２．全世界展開しているため個々の病院への閉域網/VPNによる接続は対応コストが大きくなりすぎるため難しい

３．閉域網接続の要求が根強いためそれ以外の接続方式の交渉が難航するか拒否されることがある

４．閉域網でもVPNでもなく、オープンネットワークでTLSを利用していても十分な対策の実施によりリスクを有意に低減できていれば問題無いものであるが、方式が限定されているためリスクベースのコミュニケーションを実施できない

MDS/SDSについて深堀り

- MDS/SDS 関連

【MDSについて】
・MDS 5.0 （発行間近）、出し直し等の対応は発生するか？
→ 厚労省ガイドライン6.0には対応できているからOK
→ 今後発生しないとは限らない
・MDSの解釈は各社で行うため、バラつきがある
→ 医療機関から解釈差について質問される
→ 業界団体として解釈のスタンダードを決めて回答の方向性を示した方が良いのでは？

【MDS/MDS2 の運用】
・MDS2は世界的に使っているので本社がしっかり作成している。 MDSの置き換えとしてつかえるのであればかなり良い
・MDS/SDSが国際整合したものではない。
→ 文書体系がなってない、法的根拠もない
→ 個情法等を寄せ集めたものとは思うが使いづらい
・QAとして対応すべき絶対な物ではあることは認識するが、求められているものが細かい
→ 手間が大きくて本来やるべきことがひっ迫しがち

【IMDRF/ISO81001等の国際標準などとの関連について】
・MDSはIMDRFよりも細かい部分に言及している可能性
・ISO81001に適合していればOKとなれば相当楽になる

MDS/SDS　議論結果

- MDS/SDS 関連

【方針整理】

MDSの使用について、医療機器はMDS以外でもMDS2やISO 81001-5-1 への適合をもって対策が取られているとする形に持っていけないか？

【目標】

官民対話、定期会合、定期意見交換会にEBC要望として入れ込む

【ベース】

・MDS2

承認/認証時に提出をしており、MDSへの読み替えが発生しない国際標準であること

・ISO 81001-5-1

QMS調査に載っている　→　PMDAから適合チェックされている

MDSは定期的な適合チェックはされていない

【当面の研究課題】

・MDS、MDS2、IMDRFガイダンス、ISO81001-5-1、ISO 80001-2-2など関連規格の水平比較

・内容を鑑みた官民対話的なもの以外のルート模索（規制改革推進会議への打ち込みなど）

サイバーセキュリティ関連通知・ガイドライン

通知
・20211224_医療機器のサイバーセキュリティの確保及び徹底に係る手引書について
・20220301_医療機器等に関するサイバーセキュリティ対策の強化について(要請)
・20230331_医療機関における医療機器のサイバーセキュリティ導入に関する手引書について
・20230331_医療機器のサイバーセキュリティ導入に関する手引書の改訂について
・20231010_医療機関等におけるサイバーセキュリティ対策の取組みについて
・20240115_医療機器サイバーセキュリティに関する不具合等報告の基本的考え方について
・20240131_医療機器のサイバーセキュリティに関する質疑応答集（Q&A）について
・20240328_医療機器のサイバーセキュリティを確保するための脆弱性の管理等について
・20240423_医療機器のサイバーセキュリティ対策に関連する一部変更に伴う軽微変更手続き等の取扱いについて

IMDRFガイダンス（原則＋レガシー・SBOM）
・医療機器サイバーセキュリティの原則及び実践
・レガシー医療機器のサイバーセキュリティの原則及び実践
・医療機器サイバーセキュリティのためのソフトウェア部品表の原則及び実践

3省2ガイドライン
・医療情報システムの安全管理に関するガイドライン 第6.0版
・医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン 1.1版

JIS T 81001-5-1（IEC 81001-5-1:2021）
MDS/SDS/MDS2

今後の活動方針

- MDS/SDS 関連
  ・8月に「製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）」の新版リリース済
  → この内容について精査、引き続きサイバーセキュリティについて検討

- QMS 関連
  ・無体物に関するQMSについての勉強会
  → SaMDにフォーカスをあてた無体物に関するQMSについてPMDAとの勉強会開催を検討中